Cybercrime Investigation Body Of Knowledge

第2版

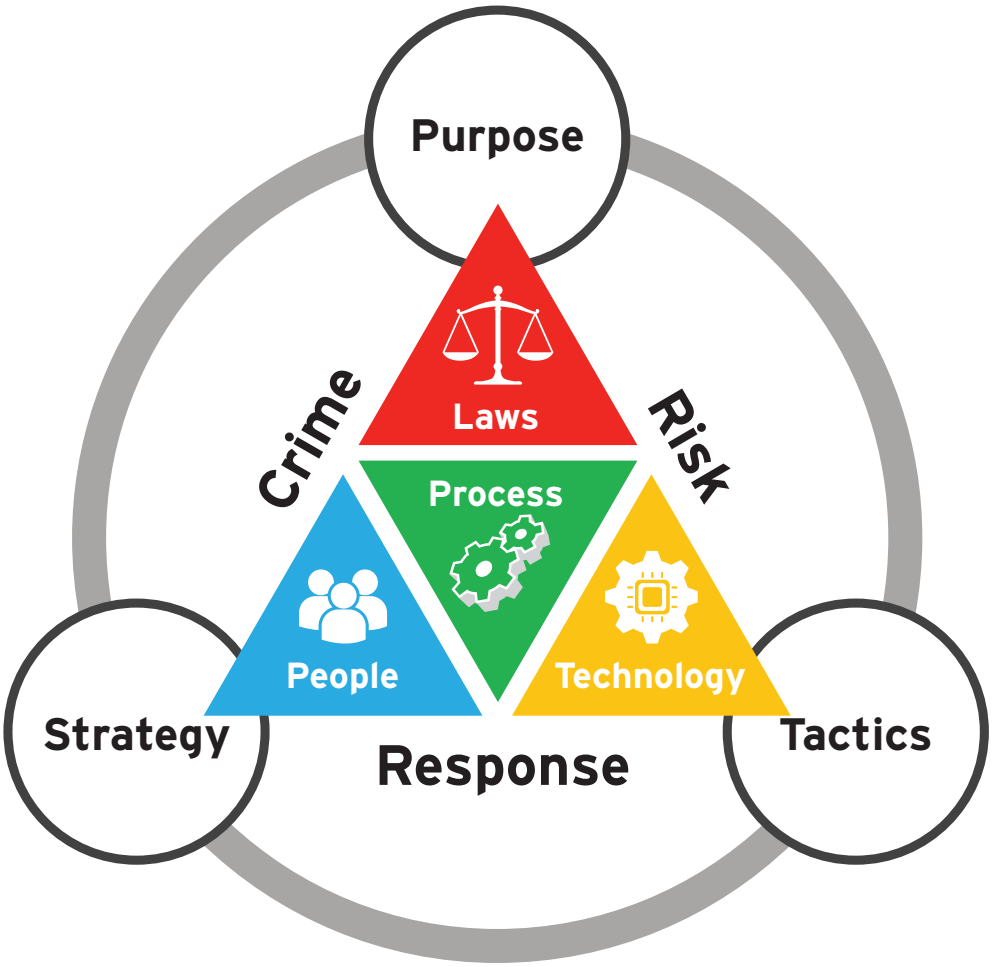
Cybercrime Investigation Body Of Knowledge

第2版

A Guide to the

Cybercrime Investigation Body of Knowledge

（CIBOKガイド第2版）



製造業者や販売業者が自社製品を区別するために使用する名称の多くは、商標として主張されている。本書にそれらの名称が記載され、出版社が商標の主張を認識している場合は、名称の頭文字が大文字になるか、またはすべて大文字で印刷される。

著者および出版社は本書の作成に細心の注意を払っているが、いかなる種類の明示的または黙示的な保証も行わず、誤りや脱落についていかなる責任も負わない。本書に含まれる情報またはプログラムの使用に関連する、または使用に起因する付随的損害または派生的損害を含む、直接損害以外の損害についてもいかなる責任も負わない。

この出版物の無断転載を禁ずる。この出版物は著作権で保護されており、禁止されている複製、検索システムへの保存、または電子的、機械的、コピー、録音など、いかなる形式や手段による送信も、それらを行う場合は、事前に発行者から許可を得る必要がある。

Copyright © 2025
Cybercrime Investigation Knowledge Forum
https://www.cibok.org/en/cikf/
All Rights Reserved

初版　2017 年 1 月
第 2 版　2025 年 5 月

CIBOK Ver.2.0の発刊にあたり

サイバー犯罪は、現代社会においてますます深刻な問題となっています。技術の進化とともに、サイバー犯罪者たちはその手法を高度化し、私たちの生活や社会基盤に重大な影響を及ぼすようになりました。その被害額は年々増加しており、企業、政府機関、個人を問わず、多くの人々がその脅威に直面しています。この現実を踏まえ、CIBOK（Cybersecurity Incident Management Body of Knowledge）は、サイバー犯罪の脅威に対応するための実践的な知識体系として、Ver.2.0への改定を実施しました。

改定の背景にはいくつかの重要な理由があります。第一に、サイバー犯罪が社会全体に及ぼす影響がますます深刻化していることが挙げられます。サイバー犯罪の手口は多様化し、その範囲も広がっています。企業情報の窃取やランサムウェア攻撃といった従来の手法に加え、国家レベルのサイバー攻撃やAIを活用した新しい脅威も現れています。このような状況下では、最新の情報と効果的な対策を迅速に共有し、適切な対応策を講じることが求められます。

第二に、サイバーセキュリティ分野における専門家が増えている一方で、特にサイバー犯罪に特化した知識や経験を持つ人材は依然として不足しています。多くの技術者がセキュリティ対策を担っていますが、彼らが直面するサイバー犯罪の脅威は、単なる技術的な問題を超え、法的、社会的、倫理的な視点を必要とする複雑な課題です。この課題に対応するために、CIBOK Ver.2.0では、時代の変化に即した内容の改定を行い、専門家だけでなく、幅広い層にとって有益な情報を提供することを目指しました。

第三に、サイバー犯罪の影響は法執行機関や専門家に限らず、私たちすべての人々に及んでいます。サイバー犯罪に直接関与しない人々であっても、その影響を受ける可能性がある現代社会では、全ての人が基本的な知識を持つことが重要です。そのため、本書では、サイバー犯罪の基礎的な理解から、組織や個人が取るべき具体的な対応策までを網羅し、法執行機関やセキュリティ専門家だけでなく、一般の読者にも分かりやすく有益な内容を提供しています。

さらに、CIBOK Ver.2.0は、500ページを超える対策集として、これまで以上に充実した内容を提供しています。この膨大な情報量は、現代のサイバー犯罪対策に必要な多くの知識をカバーするためのものです。また、多くの皆様に活用いただけるよう、本書は英語版と日本語版の同時発刊を行います。これにより、国内外問わず広範な読者層に向けた情報共有を可能とし、グローバルなサイバーセキュリティ対策の推進を目指します。

ビジネスの持続的成長を維持し、組織全体のバランスや戦略との整合性を考慮することも、対策を検討する上で益々重要となっています。CIBOK Ver.2.0は、これらの課題を解決するために、以下の点に重点を置いています。

1. **最新のサイバー犯罪動向の包括的な解説**：新たに発生している脅威や、犯罪手法の進化についての詳細な分析を提供。
2. **実践的なインシデント管理プロセスの強化**：サイバー犯罪への対応策を具体的に示し、実務に活かせるガイドラインを充実化。
3. **幅広い層へのアクセス可能性の向上**：専門用語の解説や、日常生活にも適用できる防犯対策を盛り込むことで、読者層を拡大。

本書が目指すのは、サイバー犯罪の脅威を正確に理解し、適切に対応するための道しるべとなることです。読者一人ひとりがサイバーセキュリティに関する知識を深め、より安全な社会の実現に向けて貢献できることを願っています。一般の企業人である読者にも、犯罪の手口を知ることで予防や迅速な対処の手段を学び、捜査官の行動や意識を知ることでより緊密な連携ができるようになってもらえれば幸いです。

CIBOK編纂委員会委員長　西野　弘

序文

著者の一人から、サイバーセキュリティ調査に関するこの貴重で包括的かつ詳細な本の序文を書くよう依頼されたとき、もちろん私は「はい」と答えた。私は著者たちと一緒に仕事をし、彼らの献身と情熱を体験した。彼らは全員、それぞれの分野の専門家であり、キャリアのほとんどを世界中でサイバー犯罪と戦うことに費やしてきたため、比類のない実践的な知識と経験を持っている。彼らは世界的な戦士であり、「最高の中の最高」であり、この素晴らしいリソースをまとめるために集合的に知識を共有している。

最初に思ったことは、このようなことを依頼されて光栄だということだった。次に、読者の皆さんにこの本で共有されている洞察と知識の重要性を理解してもらい、必読の書にするにはどうしたらよいかと考えた。経験豊富な専門家であろうと、サイバーセキュリティ調査のキャリアを始めたばかりであろうと、本書は皆さんを含め、誰にとっても役立つ内容である。本書は、この分野での実用的知識を増やし、強化してくれるであろう。

これからあなたは、サイバー犯罪捜査の知識を増やすための、非常に興味深く、やりがいのある旅に出ようとしている。サイバー犯罪者、国家主体の攻撃者、悪質な行為者、悪質な集団と、サイバー犯罪と闘い、組織犯罪グループを壊滅させることに注力しているあなたのような人々との間の差は広がっている。これらのサイバー犯罪者やグループは、ほとんどの場合、罰を受けることなく活動しており、捕まることをほとんど恐れていない。彼らの方法と戦術は非常に洗練されており、非常に儲かる。サイバー犯罪の背後にいる人物を特定し、そのネットワークインフラを特定し、それらを壊滅させることは簡単ではない。サイバー犯罪は狡猾で、ほとんどの場合、国境がない。

業界や法執行機関の垣根を越えて、情報を協力しながら世界規模で共有し、その情報をインテリジェンスに変えることが最も重要である。事件を立証するために必要なすべての情報を収集するには、何年もかかることがある。事件を立証し、起訴するには、信頼できる組織、業界、連邦法執行機関との世界的な協力とコーディネートが必要だ。

その特に良い例が、2014 年の GameOver ZeuS（GOZ）のテイクダウンである。GOZ は、感染したコンピュータから銀行情報や認証情報を盗むように設計された、極めて巧妙なマルウェアだった。これは 1 億ドルを超える銀行詐欺被害を引き起こし、CryptoLocker ランサムウェア攻撃の主な手段として使用された。必要な情報をすべて収集し、技術インフラを詳細に把握、ボットネットのテイクダウンの根拠となる証拠を収集し、起訴状を作成するまでに 2 年以上かかった。これには、戦略的な運用計画、多国間のコーディネート、協力が必要だった。

このテイクダウンは米国連邦捜査局（FBI）が主導した。FBI は米国の民間企業や高度な技術を持つ企業、米国の連邦政府機関、そして世界中の 10 を超える法執行機関と連携し、この高度なボットネットを取り締まり、破壊するために組織的にかつ共同で取り組んだ。

2014 年、ペンシルベニア州ピッツバーグの連邦大陪審は、ロシア連邦アナパのエフゲニー・ミハイロヴィッチ・ボガチェフ（Evgeniy Mikhailovich Bogachev）に対し、GameOver ZeuS ボットネットの管理者としての役割を担っていたとして 14 件の起訴状を公開した。彼は FBI のサイバー最重要指名手配リストに載せられ、逮捕または有罪判決につながる情報には 300 万ドルの懸賞金がかけられた。この金額は当時としては前代未聞だった。

現在、エフゲニー・ミハイロビッチ・ボガチェフは、本名を名乗ってロシアで働き、生活する自由な人間である。彼はサイバー犯罪捜査と刑事訴追の困難さの壁によって守られている。

サイバー犯罪に関するすべての必要な証拠を集めて、起訴することは非常に困難で時間がかかる。場合によっては、犯罪者が特定の国で保護され、法の裁きを免れて活動していることもある。捜査過程で

のミスは、この困難さをさらに増すため、捜査官はそれを避けることが不可欠である。本書「サイバー犯罪捜査の知識体系」（Cybercrime Investigation Body of Knowledge）は、捜査過程において成功する可能性を高めるためのものである。

2017 年に「サイバー犯罪捜査の知識体系」（Cybercrime Investigation Body of Knowledge）の初版が発行されて以来、サイバー犯罪や犯罪者の能力、技術、手法を加速させる数多くの技術的進歩があった。その 1 つが人工知能（AI）である。サイバーセキュリティ、サイバー捜査、全体的なセキュリティに対して、予防的かつ積極的なアプローチを取ることがこれまで以上に重要になっている。サイバーセキュリティのあらゆる分野において、不断の警戒とデューデリジェンスが重要である。

サイバー犯罪は被害者のいない犯罪ではない。私たち全員がサイバー犯罪と戦い、全体的なセキュリティを維持する役割を担っている。この取り組みは好奇心旺盛な人のためのものではなく、熱意のある人のためのものである。サイバー犯罪に関する知識と専門知識を増やし、情報を共有するためのグローバルな集団的、協力的な取り組みによってのみ、安全なサイバーの未来を築くことができる。

サイバーセキュリティ捜査に関する知識を深めたいと考えている人にとって、この本は貴重なリソースとなると確信している。ぜひ読んでみてほしい。あなたの優れた仕事が、多くのサイバー犯罪の訴追に貢献することを願っている。

マリア・J・ベロ
2024 年 5 月 20 日

マリア・ヴェロ（Maria Vello）は、脅威インテリジェンスとサイバー犯罪捜査の発展のために公的部門と民間部門の橋渡しをしてきた数十年の経験を持つサイバー犯罪捜査のベテランである。マリアは、米国の National Cyber Forensics Training Alliance（NCFTA）の元社長兼 CEO であり、英国の Cyber Defense Alliance（CDA）の元 CEO でもある。

執筆者

編集長

シェーン・ショック（Shane Shook, PhD）は、情報セキュリティと対応業務のベテランとしてよく知られており、政府と業界のIT リスク管理問題に30年近く携わっている。彼はフォレンジックアナリストを率い、ほとんどの業界セクターで最も悪名高い侵害事件の多くにおいて専門家の証言を提供してきた。また、関連する（国際的なおよび米国の）連邦、民事、商業紛争で専門家の証人を務めてきた。現在は、いくつかの新興セキュリティ技術企業の諮問委員会に所属している。彼は、数冊の本の寄稿者および編集者であり、基調講演やゲスト講演を頻繁に行っている。

CIBOKのこの版の著者と寄稿者

アーロン・ゴールドスタイン（Aaron Goldstein）は、サイバー詐欺対応のリーダーであり研究者である。複雑で大規模なサイバー侵害事件の経験があり、あらゆる規模の環境を保護するための戦略的なソリューションを提供してきた。

アルベルト・カサレス（Alberto Casares）は、脅威インテリジェンスの研究者兼アナリストであり、Constella Intelligence のCTO として、アイデンティティ脅威の検出と対応に重点的に取り組んでいる。スペイン産業省の支援を受けた複数の研究開発プロジェクトを主導しており、グラナダ大学のサイバーセキュリティ修士課程のサイバーセキュリティ教授でもある。

アントニア・ニシオタ（Antonia Nisiota, PhD）は、セキュリティ態勢管理、脅威ハンティング、コンピュータおよびメモリフォレンジックを専門とするサイバーセキュリティオペレーションセンターのリーダーであり、研究者であり、アナリストである。

ビリー・グヴェイア（Billy Gouveia）はSureFire, Inc. のCEO 兼創設者である。サイバー詐欺対応、情報収集と分析、およびテクノロジーの分野で20年以上の経験を持っている。

ブラッドリー・ポッテイガー（Bradley Potteiger, PhD）は、ArmsCyber の共同設立者兼最高技術責任者である。米国国防総省を含む政府機関や業界団体で、情報収集、サイバー防御、分析、技術開発の経験がある。ゼロトラスト、自動移動標的型防御、欺瞞技術、サイバーセキュリティの回復原理を活用したアクティブディフェンス法の専門的経験を重ねてきた。メリーランド大学とジョンズホプキンス大学応用物理学研究所で、サイバーセキュリティ、自律走行車のセキュリティとプライバシー、選挙の完全性、宇宙システム、国家安全保障などのテーマについて教鞭をとり、学術研究を行っている。

クリス・コールター（Chris Coulter）は、政府、業界、個人のコンピュータ犯罪捜査を主導してきた法医学調査官およびインシデント対応者である。彼は、法医学コンピュータ捜査における証拠取得の複雑な方法を簡素化するために開発し市場に提供した技術の特許保有者である（デジタル法医学取得キットおよびその使用方法 - 米国US 13/019,796）。サイバーセキュリティサービスおよび製品における企業リーダーシップの経験、PwC、Stroz Friedberg LLC、MIT Labs、IRS などでの監査および調査経験もある。

ダン・ガンター（Dan Gunter）は、IT およびOT ネットワークに特化したサイバー脅威ハンティングおよびフォレンジック企業であるInsane Cyber の創設者兼CEO である。彼は、石油・ガス、および世界的なエ

ネルギー企業のクライアントとの仕事を通じて、OT および産業用制御システムのサイバーセキュリティ研究とインシデント対応の豊富な経験を有している。また、AFCERT および CYBERCOM チームで USAF サイバー戦闘士官を務めたこともある。

デビッド・エマーソン（David Emerson）は、複数の製品およびサービス企業で最高情報セキュリティおよびテクノロジーの役職を務め、豊富なリーダーシップ経験がある。彼は、クライアントの安全なプログラムと運用体制の確保を支援するマネージドセキュリティサービスプロバイダーである SolCyber の CTO である。

エリン・ジョー（Erin Joe）は、Google の CISO オフィスに所属する Mandiant の上級管理職である。FBI で上級管理職として 25 年のキャリアを経て、サイバー犯罪の捜査と危機対応の経験を活かすため Mandiant と Google に入社した。

ヒデキ・ニノミヤ（Hideki Ninomiya）は、株式会社オリエントの CEO 兼創設者である。日本の製薬業界やその他の業界において、IT リーダーシップ、サイバーセキュリティ、サイバー犯罪分析、リスクアドバイザリーサービスについて豊富なキャリアを積んできた。また、サイバー リスク、セキュリティ組織、セキュリティ体制の開発について、企業の役員会にアドバイスを行っている。

ヒロシ・ニシノ（Hiroshi Nishino）は、本書 CIBOK の編纂委員会委員長であり、HI イニシアティブ株式会社の代表取締役である。1991 年株式会社ブロシードを設立し、PMBOK、lTlL、COPC など多くのグローバルスタンダート知識体系のマネジメントシステムの日本導入を行い、PMl や it SMF、ClKF などの推進団体の設立に寄与した。また、2001 年より政府の IT 調達改革に関わり、政府の各委員会にて、総合入札方式や ClO 補佐官制度、人財育成などの提言や実践を行った。その他兼務する役職に以下がある。特定非営利法人 CeFIL 副理事長、デジタルビジネスイノベーションセンター共同設立者、国際刑事警察機構（インターポール）グローバルサイバー犯罪専門家委員会委員一般社団法人サイバー犯罪捜査・調査ナレップフォーラム、共同設立者・理事、筑波大学大学院情報生命学術院システム情報工学非常勤講師、富山大学教養教育科目非常勤講師。

イアン（イフタック）アミット（Ian（Iftach）Amit）は、セキュリティおよびソフトウェア業界の経験豊かなマネージャーであり、企業セキュリティから小売、エンドユーザーソフトウェア、大規模なバックエンドシステムまで、情報セキュリティのさまざまな分野で豊富な経験がある。彼は、低レベルの技術的専門知識から企業のセキュリティポリシー、法規制遵守、戦略まで、幅広い経験を持つ情報セキュリティの専門家である。イアンは、BlackHat や DefCon で頻繁に講演しており、PTES（ペネトレーションテスト実行標準）、IL-CERT、および Tel-Aviv DEFCON グループ（DC9723）の創設メンバーである。

カリム・ヒジャジ（Karim Hijazi）は、サイバーセキュリティとインテリジェンスの分野で 30 年以上の実務経験を持つ投資家兼サイバーセキュリティインテリジェンスのリーダーである。彼は、世界的なボットネットとそれが政府機関や民間企業に与える影響に対処するために、複数のサイバーインテリジェンスサービス会社を設立した。

キャスリン・シー（Kathryn Shih）は、Akamai Technologies、Amazon Web Services、Google などの組織でクラウドおよび人工知能プログラムの開発と管理の専門知識を習得した、サイバーセキュリティアナリスト、投資家、実務家である。

ケリー・ロバートソン（Kelly Robertson）は、30 カ国以上で 30 年以上のサイバーセキュリティの専門的経

験を有しています。SAIC、Nokia、Juniper Networks、White Hat Security、Atos、Horizon3.ai など、大手 ICT およびサイバーセキュリティ企業で、技術面および市場面で重要な役職を歴任しました。実践的な技術プログラム開発、トレーニング、市場定義活動における彼の貢献は、本版で提示される視点に役立っています。彼はシュック博士の長年の友人であり同僚でもあり、効果的なプログラムとプロセスを通じてサイバーリスクを認識し、対処するというテーマの推進に 20 年以上協力してきました。

マリア・ヴェロ（Maria Vello）は、脅威インテリジェンスとサイバー犯罪捜査の発展のために公的部門と民間部門の橋渡しをしてきた数十年の経験を持つサイバー犯罪のベテランである。マリアは、米国の National Cyber Forensics Training Alliance（NCFTA）の元社長兼 CEO であり、英国の Cyber Defense Alliance（CDA）の元 CEO でもある。

マーク・マリソン（Mark Mullison）はアライドユニバーサルの最高技術責任者であり、通信、教育、物理的セキュリティ業界において 30 年以上のテクノロジーおよびサイバーセキュリティのリーダーシップ経験がある。

ニール・ビニー（Neil Binnie, PhD）は、世界的な建設、不動産、航空宇宙の分野での経験を持つシニアサイバーセキュリティエグゼクティブである。

ノリアキ・ハヤシ（Noriaki Hayashi）は、日本のトレンドマイクロ株式会社のシニアリサーチャーである。さまざまなコンピューティングプラットフォームとテクノロジーの高度なスキルを持つ認定管理者およびシステムエンジニアでもある。17 年以上のシステム管理およびセキュリティの経験があり、プログラムおよびプロジェクト管理、セキュリティ研究、脅威対応などの分野での実績を持っている。

オマロラ・ファグブル（Omalola Fagbule, PhD）は、サイバーセキュリティ啓発の専門家であり、人間の動機と認識を理解することに重点を置いた研究者である。彼女は、スタッフを教育し、組織の意識を高めるために、サイバー犯罪者の動機と行動に対処するトレーニングプログラムと資料を開発している。

パトリック・A・ウェスターハウス（Patrick A. Westerhaus）は 2016 年にウェルズファーゴに入社し、企業情報セキュリティ（EIS）、サイバー脅威フュージョンセンター（CTFC）のチームを率いて、金融機関のサイバー、詐欺、マネー ロンダリングのリスクを軽減する企業プログラムの開発を目指してデータの統合と分析に取り組んでいる。ウェルズファーゴに入社する前は、KPMG で詐欺およびフォレンジック業務に携わり、過去 12 年間は FBI に勤務し、本部サイバー部門の監督特別捜査官にまで昇進した。FBI 在職中、パトリックは企業・政府詐欺、公共汚職、テロ対策、防諜、サイバー詐欺・窃盗の捜査を指揮し、最後には NCIJTF の仮想通貨チームに所属していた。パトリックはゴンザガ大学で会計学の経営学士号、ジョージワシントン大学でセキュリティ管理のフォレンジックサイエンスの修士号、スタンフォード大学で国際セキュリティの大学院修了書を取得している。パトリックは CPA でもあり、CFE および CAMS 認定資格も保持している。

サトシ・シミズ（Satoshi Shimizu）は、サイバー犯罪捜査ナレッジフォーラムの創設者であり、本書「サイバー犯罪捜査の知識体系」（Cybercrime Investigation Body of Knowledge）の初版の編集者である。トレンドマイクロの日本事業部の地域 CISO として、また日本サイバー犯罪対策センターのディレクター、トレンドマイクロとのインターポールの提携プロジェクトのディレクターとして、テクノロジーとサイバーセキュリティ製品およびプログラムの開発をリードしてきた豊富なキャリアを持っている。彼は、世界的なサイバー犯罪と戦うための国際的なインテリジェンスと対応の取り組みの定義に貢献してきた。

スコット・マクレディ（Scott McCready）はSolCyberのCEOであり、FireEye、Symantec、NTT、EDSなど、世界的に有名なセキュリティ企業向けにサイバーセキュリティ製品やサービスの提供を指揮してきた。

サイモン・マリス（Simon Mullis）は、FireEye、Palo Alto Networks、Taniumでチームを率い、最高技術責任者としてVenari Securityを共同設立した、経験豊富なサイバーセキュリティ製品やサービスのエグゼクティブである。また、サイバーセキュリティの業界および公共部門のニーズを代表し、ヨーロッパや北米のテクノロジーおよびセキュリティカンファレンスで講演を行っている。

タミー・アーチャー（Tammy Archer）は、世界的な自動車流通サービス企業Inchcape PLCのCISO、およびHSBCの元CISOとして、サイバーセキュリティのリーダーシップに関する豊富な経験を持っている。以前は、英国政府で外務省のCISO、英国国防省、英国海軍に勤務していた。
ワジ・ヤシン（Wajih Yassine）は、GoogleおよびCylanceの顧客サポートで経験を積んだ上級サイバーセキュリティおよびフォレンジックエンジニアである。クラウドおよび企業フォレンジックツールの開発に貢献してきた。

この版に寄稿していただいた以下の企業に特に感謝申し上げる。

株式会社オリエント - 日本
トレンドマイクロ株式会社 - 日本
Acora - イギリス
Surefire Cyber - アメリカ
SolCyber - アメリカ
Insane Forensics - アメリカ
Forgepoint Capital - アメリカ

CIBOKの初版にご協力いただいた以下の方々にも引き続き感謝申し上げる。

クレイグ・W・ソーラム（Craig W. Sorum）は、連邦捜査局（FBI）のベテランで、テキサス州エルパソ、ワシントンD.C.、アイオワ州シーダーラピッズ、ミネソタ州ミネアポリスの現地事務所に配属され、数百件の国内および国際サイバー犯罪捜査を指揮し、監督した。クレイグは、現場捜査官として重要なサイバー捜査で表彰され、FBIHQのFBI法執行オンラインユニットの責任者としての功績により、政府内のトップITマネージャーに贈られる"Federal 100 Award"の受賞者に選ばれた。捜査局を退役した後、クレイグは「フォーチュン500」に入る防衛・航空宇宙企業に情報セキュリティ担当シニアマネージャーとして勤務し、すべてのサイバー捜査と脅威インテリジェンス問題を担当した。クレイグは現在、サイバー セキュリティ管理コンサルタントとして働いている。

デイヴィッド・コーウェン（David Cowen）は、SANS認定インストラクター、CISSP、およびGIAC認定フォレンジック検査官である。1999年からデジタルフォレンジックとインシデント対応に携わり、公共部門と民間部門の何千ものシステムを対象に調査を行ってきた。これらの調査には、内部脅威の暴露から民事訴訟の専門家証人としての活動やサイバー犯罪者を刑務所に送るための証拠の提供まで、あらゆることが含まれている。デイヴィッドは、デジタルフォレンジックに関する3シリーズの書籍、"Hacking Exposed Computer Forensics"（第1版～第3版）、"Infosec Pro Guide to Computer Forensics"、および"Anti Hacker Toolkit"（第3版）を執筆している。

エリック・ジマーマン（Eric Zimmerman）は、Krollのサイバーセキュリティおよび調査部門の上級副社長

である。エリックは、複雑な法執行機関の調査、コンピュータフォレンジック、専門家の証言、コンピュータシステムの設計、アプリケーションアーキテクチャなど、サイバー領域において非常に深く幅広い専門知識を持っている。彼は、その仕事について数多くの評価を受けており、受賞歴のある著者であり、サイバー関連のトピックに関する人気の高い講師であり、プレゼンターである。Kroll に入社する前、エリックは連邦捜査局（FBI）の特別捜査官であり、犯罪および国家安全保障関連のコンピュータ侵入、児童に対する犯罪（児童ポルノの製作、配布、所持）、知的財産の窃盗および関連犯罪の捜査を専門としていた。

ジョン・ジョリー（John Jolly）は、幅広い業界での経験を持つ、熟練したサイバーセキュリティエグゼクティブである。ジョンは、ゼネラル・ダイナミクスのサイバーセキュリティ部門の副社長兼ゼネラルマネージャーを務め、商業インシデント対応業務を含む幅広い製品とサービスのポートフォリオを担当していた。ジョンは、メリーランド大学ボルチモア郡校で優秀な成績でコンピュータサイエンスの学士号を取得し、ペンシルベニア大学ウォートン校でも優秀な成績で財務の MBA を取得している。

ジュディス・H・ジェルマノ（Judith H. Germano）は、サイバーセキュリティガバナンスとデータプライバシー問題について企業に助言することを専門とする法律事務所 Germano Law LLC の創設メンバーである。ジェルマノ氏はニューヨーク大学ロースクールの非常勤教授であり、ニューヨーク大学（NYU）サイバーセキュリティセンターのシニアフェローでもある。そこで彼女は、サイバーセキュリティの新たな問題と解決策に焦点を当てた企業幹部と政府高官から成るタスクフォースを率いている。以前は、ニュージャージー州連邦検事局で経済犯罪担当チーフを務め、連邦検察官として 11 年間勤務した。連邦検事局に入局する前は、ニューヨーク市の多国籍法律事務所 Shearman & Sterling LLP に勤務していた。ジェルマノ氏の著書には、"A New Era of Collaboration" や "After the Breach: Cybersecurity Liability Risk" などがある。

ルーク・デンボスキー（Luke Dembosky）は、Debevoise & Plimpton のサイバーセキュリティ& データプライバシーグループのパートナーであり、以前は司法省国家安全保障局で国家安全保障担当の司法次官補を務めていた。14 年間以上司法省に勤務し、司法省のコンピュータ犯罪および知的財産セクションの訴訟担当副主任など、さまざまな役職を務めた。デンボスキー氏は、主要なサイバー事件や関連する法律上および政策上の問題に関して、司法省、FBI、シークレットサービス、国家安全保障会議、その他の機関の指導部に定期的に顧問を務めてきた。2013 年のロシアとのサイバー協定、および 2015 年にオバマ大統領と中国の習近平国家主席が署名した歴史的な 5 項目の合意の交渉に参加し、国連でのサイバーに関する議論で司法省の共同代表を務めました。彼は最近、サプライチェーンに対するテクノロジーリスクへの対応に重点を置く ABA 公共契約法セクションの副議長に任命された。デンボスキー氏は、業界全体にわたるサイバーセキュリティ脅威共有プラットフォームを確立するというホワイトハウスの取り組みの一環として、ISAO 向けの内部ガバナンス ガイダンスの開発を主導する情報共有および分析組織ガバナンス ワーキンググループの共同議長でもある。

フィリップ・フォドチャック（Philip Fodchuk）は、Suncor の企業全体の情報セキュリティプログラムを率いている。Suncor では、組織の情報セキュリティ体制の成熟と強化を担当し、サイバーセキュリティインシデント対応機能を指揮している。以前は、Deloitte の企業リスクサービスグループ内のサイバーセキュリティプラクティスのパートナーだった。その任務では、エネルギーおよび資源部門の危機管理のグローバルリーダーを務め、Deloitt のサイバーセキュリティインシデント対応のカナダ側のリーダーだった。フィリップは、王立カナダ騎馬警察（RCMP）およびカルガリー警察の警察官として、テクノロジー犯罪、サイバーセキュリティ、インシデント対応の問題に携わっていた。20 年にわたる多様な経験を持つフィリップは、サイバーセキュリティ、デジタルフォレンジック、インシデント管理、組織危機の問題に関する戦略への対応、管理、開発の専門家と見なされている。

CIBOK 目次

CIBOK Ver.2.0 の発刊にあたり 3
序文 4
執筆者 6

序章：本書に対する序言 25

本書の対象読者 26
ヒント 27
「CIBOK」の概念 28
なぜ「CIBOK」なのか 28
図 1-1. サイバー犯罪捜査フレームワーク 28
「CIBOK」とは何か 29
本書の目的とは 29
CIBOK を確立する 5 つの目的 29
図 1-2. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 30
表 1-1.「実行」を支える「関連」フレームワーク 31
図 1-3. サイバー犯罪捜査およびインシデント調査部門のマクロフレームワーク 32
サイバー犯罪とその捜査 33
サイバー犯罪とは 33
図 1-4. b/d/r ダイナミクス 33
表 1-2. サイバー空間で発生する有害行為のカテゴリ 34
表 1-3. サイバー空間で行われた有害行為によって生じる被害者の損害のカテゴリ 34
表 1-4. サイバー空間における被害者のリスクのカテゴリ 34
サイバー犯罪捜査およびインシデント調査とは 34
表 1-5. サイバー犯罪捜査およびインシデント調査活動のカテゴリ 35
表 1-6. サイバー空間における犯罪の特性 35
刑事政策及び民間の事業ドメインに立脚する戦略と計画 36
価値創造のフレームワーク 36
図 1-5. サイバー犯罪捜査およびインシデント調査班へのフレームワークの適用 36
サイバー犯罪捜査およびインシデント調査部門の構成 38
伝統的な捜査組織体制におけるサイバー部門の検討 38
図 1-6. 基本的な従来の犯罪捜査組織の体制 38
図 1-7. カテゴリ型組織 39
図 1-8. マトリクス型組織 39
図 1-9. 複合型組織 40
サイバー犯罪捜査およびインシデント調査 41
図 1-10. サイバー犯罪捜査およびインシデント調査班の構成図 41
管理 42
知見収集 42
調査 42
事件対応 43
証拠 43
説明責任 43
予防啓発 43

後方支援 43
総務人事 43
表 1-7. CI 実行フレームワークと CI 任務の関係、必要なスキルと経験 44
表 1-8. CI 任務知識領域に対する CI 実行フレームワークの関連性 45
表 1-9. CIBOK 階層構造 46

第 1 章：サイバー犯罪とその捜査 47

はじめに 48
サイバー犯罪とその捜査におけるトピックス分類 49
図 1-1.「サイバー犯罪とその捜査」知識領域におけるトピックスの分類 49
サイバー犯罪の定義 49
犯罪の道具としての技術 50
図 1-2. 世界サイバー犯罪指数を用いたサイバー犯罪の地理的分布のマッピング 52
犯罪の攻撃対象としての技術 52
犯罪から目をそらす手段としての技術 53
コンピュータ犯罪を規定する法律 54
サイバー犯罪の管轄権の問題 55
サイバー犯罪に関する条約 56
MLAT 57
外交的手法 57
規制 58
CERT 58
図 1-3. サイバー犯罪ガバナンス 58
サイバー犯罪捜査のベストプラクティス 59
多面的なアプローチ 60
内部体制 60
外部のリソース 61
Chapter 1：CIBOK の分類法との関係 62
図 1-4. サイバー犯罪捜査における実行フレームワーク 62
表 1-1. CIBOK の分類法 63
第 1 章：レビュー 64
ケーススタディ 1：世界最大のボットネットの解体 65

第 2 章：サイバー犯罪の分類 67

はじめに 68
サイバー犯罪の種類におけるトピックス分類 71
図 2-1.「サイバー犯罪の種類」知識領域におけるトピックスの分類 71
サイバー犯罪とは 71
図 2-2. 従来型犯罪とサイバー犯罪の比較（出典：米国会計検査院 2007） 73
道具としての技術 74
表 2-1.「高齢者を狙った金銭詐欺トップ 10」 77
攻撃対象としての技術 79
（犯罪から）目をそらす手段としての技術 84
サイバー犯罪の目的、動機、スキル 85
サイバー詐欺師 85

ネットいじめ 86
ハクティビスト 86
児童の性的搾取犯 86
テロ行為 86
コンピュータハッカー 87
APT チーム 87
第 2 章：CIBOK の分類法との関係 88
図 2-2. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 88
表 2-1. CIBOK の分類法 89
表 2-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 89
第 2 章：レビュー 91
ケーススタディ 2：サイバー犯罪の「ABC」 92

第 3 章：サイバー犯罪のアーティファクト 95

はじめに 96
サイバー犯罪のアーティファクトにおけるトピックス分類 99
図 3-1.「サイバー犯罪のアーティファクト」知識領域におけるトピックスの分類 99
サイバー犯罪の侵害兆候とは 99
図 3-2.「サイバーキルチェーン」モデル 100
図 3-3. サイバー犯罪のインジケーター 101
MITRE ATT&CK フレームワーク 102
図 3-4. Mitre ATT&CK（™）フレームワークのディテールの深さの図解 102
図 3-5. 敵対者エミュレーション計画のサンプル 103
MITRE D3FEND フレームワーク 103
アーティファクト 104
攻撃 104
事前調査 105
不正アクセス 105
脆弱性攻撃／攻撃成功 105
サイバー犯罪活動のステージ 106
表 3-1. サイバー犯罪活動 106
標的の決定 106
アクセスの提供 106
列挙 107
サービスの決定 107
サービスの管理 107
サービスの維持／防御 107
サービスの冗長化 107
難読化 108
代替サービス 108
目的達成 108
「環境寄生型（LotL）攻撃」 109
LOLBins の主な特徴 109
よく使われる LOLBins： 110
LOLBin リスク軽減と脅威検出： 110
サイバー犯罪のアーティファクト 112

図 3-6. インジケーターとアーティファクトの関連性 112
外部のアーティファクト 113
インターネット 113
ディープウェブ 113
ダークウェブ 113
ソーシャルメディア 114
従来型メディア 114
図 3-7. サイバー犯罪における外部のアーティファクト 114
犯罪ネットワーク 114
内部のアーティファクト 115
システム 115
従業員 115
コミュニケーション 116
図 3-8. 内部のアーティファクト 116
暗号化 116
第 3 章：CIBOK の分類法との関係 117
図 3-9. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 117
表 3-2. CIBOK の分類法 118
表 3-3. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 118
第 3 章：レビュー 120
ケーススタディ 3：現代の攻撃 120
図 3-10. 不正アクセスされたホストのサプライチェーンエコノミクス 121

第 4 章：サイバー犯罪のスコープ 125

はじめに 126
サイバー犯罪のスコープにおけるトピックス分類 129
図 4-1.「サイバー犯罪のスコープ」知識領域におけるトピックスの分類 129
サイバー犯罪のスコープとは 129
図 4-2. サイバー犯罪のスコープ 130
図 4-3. サイバー詐欺／不正組織 132
図 4-4. ダークネットでの取り扱い品目 135
図 4-5. ダークネットのプロファイル 136
quickly evolved 137
サイバー犯罪の特性 138
図 4-6. サイバー犯罪の特性 141
偶発的なもの 142
標的型 142
進化型 142
サイバー犯罪で狙われるリスク 145
図 4-7. サイバー犯罪の動機の傾向 146
図 4-8. サイバー犯罪で用いられる手法の動向 146
表 4-1. サイバー犯罪と従来型犯罪の関係 147
図 4-9. 特性およびリスクとスコープの関係 148
金融・金銭面 148
ブランド面 149
業務面 149

従業員 150
公的組織 vs 民間組織 151
図 4-10. 公的組織と民間組織でのリスク優先順位に関する比較 151
第 4 章：CIBOK の分類法との関係 152
図 4-11. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 152
表 4-2. CIBOK の分類法 153
表 4-3. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関 153
第 4 章：レビュー 155
ケーススタディ 4：インサイダーが市場をハッキングするとき 155

第 5 章：証拠の情報源 157

はじめに 158
サイバー犯罪のアーティファクトにおけるトピックス分類 159
図 5-1.「証拠の情報源」知識領域におけるトピックスの分類 159
証拠の情報源とは 160
図 5-2. 証拠の情報源をとりまく関係 160
証拠の外部情報源 161
図 5-3. 日本サイバー犯罪対策センターの対応モデル 161
脅威インテリジェンス 162
フォーラムおよび掲示板 165
ボットネットコントロールパネル 165
証拠の内部情報源 166
図 5-4. 証拠の内部情報源 166
ネットワーク 166
コンピュータ端末 168
Windows プリフェッチアーティファクトのデジタルフォレンジック分析 173
機能性 173
よくある誤解の訂正 174
デジタルフォレンジック分析における活用 174
クラウドコンピューティングの深層 177
クラウドコンソール 177
クラウドストレージ 177
仮想マシン 177
コンテナ 178
Kubernetes（クバネティス） 178
マネージドサービス 179
DFIR のためのオープンソースツールの活用 179
図 5-5. オープンソース DFIR ツール 181
図 5-6. 非 Kubernetes インストールと OSDFIR インフラの比較 182
図 5-7. 完全に展開された OSDFIR インフラストラクチャ スタック 183
サービス 183
図 5-8. Windows イベントログのコンテンツ 184
第 5 章：CIBOK の分類法との関係 192
図 5-9 サイバー犯罪捜査およびインシデント調査における実行フレームワーク 192
表 5-1. CIBOK の分類法 193
表 5-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 193

第 5 章：レビュー 195
ケーススタディ 5：フォレンジック技術を用いた Mirai ボットネットの分析 195
図 5-10. Mirai ボットネット 196
図 5-11. Mirai ボットネットのトポロジー 197
表 5-3. Mirai の不正アクセスを受けたデバイスの上位ベンダー 197
表 5-4. Mirai の不正アクセスを受けた Mirai デバイスの上位種類 197
表 5-5. Mirai の不正アクセスを受けたデバイスのデフォルトログイン認証情報の例 198
Mirai ボットネットのフォレンジック分析 198
図 5-12. ラボラトリーフォレンジック手順の例 199
調査結果と意味 199

第 6 章：証拠収集の手段 201

はじめに 202
サイバー犯罪のアーティファクトにおけるトピックス分類 203
図 6-1.「証拠収集の手段」知識領域におけるトピックスの分類 203
証拠収集の手段とは 203
図 6-2. トリアージに基づく証拠収集 205
証拠の自動収集 206
システム全体（アラート型ロギング） 206
図 6-3. システム全体アラートの IoC の例 207
図 6-4. アラートの STIX アーキテクチャ 208
図 6-5a. アラート型ロギング 209
図 6-5b. Crowdstrike Falcon Overwatch のアラート型ロギング 209
スウィープ・ディスカバリー（一掃検知） 210
図 6-6. 証拠収集での段階的アプローチ 211
図 6-7a. 異常なセキュリティー掃による証拠の収集と集約 212
図 6-7b. CrowdStrike Falcon による証拠の収集と集約 212
手作業による証拠収集 212
図 6-8. 証拠収集の手段 214
ネイティブツール 214
図 6-9. TASKLIST（PSAPI の使用） 215
図 6-10. サードパーティのツールで PSAPI を使用するコード例 215
図 6-11a. Linux のネイティブ NET 統計（未加工） 216
図 6-11b. Linux のネイティブ NET 統計（変換済み） 216
図 6-12a. NETSTAT でネットワーク統計を得るためにサードパーティスクリプトで PS を使用しているコード例（netstat.py） 217
図 6-12b. NETSTAT でネットワーク統計を得るためにサードパーティスクリプトで PS を使用しているコード例（netstat.py） 217
図 6-13. Windows の IPCONFIG 218
図 6-14. Windows PowerShell の Get-NetAdapter 219
図 6-15. Windows と Linux の netstat -ano 219
図 6-16. Windows の tasklist /m と Linux の ps -df 219
図 6-17. Windows の netstat -anob と Linux の ss -ltp 220
図 6-18. Linux の tcpdump 220
図 6-19. Windows の netsh trace 221
図 6-20a. Microsoft Message Analyzer でトレースログを開いているところ 221
図 6-20b. Microsoft PktMon.exee 222

図 6-20c. PktMon.etl の Microsoft ネットワークモニター変換 222
図 6-21. Windows PowerShell のファイルシステムメタデータ 223
図 6-22. Linux（Ubuntu）の lsw メタデータ 224
図 6-23. Windows の robocopy と Linux の dd 225
図 6-24. Windows のイベントビューアー 226
図 6-25. Windows の WEVTUTIL クエリユーティリティ例 226
図 6-26. Windows の TypedURLs（履歴） 226
図 6-27. Windows の REGEDIT によるエクスポート 227
図 6-28. Windows PowerShell の例 227
図 6-29a. PSRecon 228
図 6-29b. WinDBG（メモリダンプ解析用に SwishDbgExt.dll を使用） 229
サードパーティ製ツール 229
図 6-30. 捜査官・調査員が収集するもの 230
図 6-31. nmap 231
図 6-32. TCPView 231
図 6-33. Wireshark 232
図 6-34. Autorun と Process Exploler（PROCEXP.EXE） 233
図 6-35. RawCopy と FGET 233
図 6-36. osTriage 234
図 6-37. Google Rapid Response 235
図 6-38. 各種フォレンジック（犯罪捜査）レビューツール間の類似点 236
図 6-39. ロギング 237
フォレンジックにおける証拠の完全性 238
図 6-40. フォレンジックにおける証拠の完全性 238
図 6-41. Windows と Linux のネイティブハッシング 239
手順の文書化 239
ツールの認定 240
証拠分析担当者取得すべき認証資格 240
サイバー犯罪の種類別の証拠収集要件 241
標的別 242
分類別 242
表 6-1. 分類別の証拠収集 243
証拠収集の手引き 243
証拠収集における課題 245
CoC（Chain of Custody 証拠の保全・マネジメントの連鎖） 247
表 6-2. 証拠の連鎖のログ 247
分類／管轄別の保有 247
証拠の廃棄 248
第 6 章：CIBOK の分類法との関係 248
図 6-42. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 248
表 6-3. CIBOK の分類法 249
表 6-4. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 249
第 6 章：レビュー 251
ケーススタディ 6：複雑な IT ／ OT 環境における証拠収集 251
図 6-43. OT ネットワークと Triton/Trisis 攻撃対象の例図 252
図 6-44. トリトン／トライシス攻撃目標のバデューモデル 252

第 7 章：証拠分析の方法 257

はじめに 258
証拠分析の方法におけるトピックス分類 259
図 7-1.「証拠分析の方法」知識領域におけるトピックスの分類 259
集約 259
証拠収集 259
図 7-2. DFIR プロセス 260
脅威インテリジェンス（TI） 260
図 7-3. 脅威インテリジェンスのライフサイクル 261
図 7-4. DIKWP ピラミッド 261
図 7-5. 痛みのピラミッド 262
調査におけるデータ要素 263
表 7-1. IOC として蓄積されたデータ要素 264
表 7-2. 被害者の「有責性（Culpability/Culpabilité）」に基づく分類方法 264
表 7-3. プログラムの解析手法 267
分析フレームワーク 268
データモデリング 268
表 7-4. データモデリングにより警察活動にもたらされるメリット 268
表 7-5. 構造化データ（Structured Data）、半構造化データ（Semi-structured Data）および非構造化データ（Unstructured Data） 269
表 7-6. メタデータの種類 270
データの保存とマネジメント 270
機械学習とデータマイニング 272
表 7-7. 共通機械学習アルゴリズム 272
表 7-8. データマイニングにおける代表的な分析モデル 272
表 7-9. データマイニングにおいて使用されるツール 273
データビジュアライゼーション 273
データ品質テスト 274
表 7-10. データの完全性を確認するためのチェック技法 274
表 7-11. データ型の一例 275
表 7-12. 欠損値の構造 275
表 7-13. 欠損値の削除または補完方法 276
表 7-14. 外れ値を検出するアプローチ 276
自動化 276
表 7-15. データベースの種類 276
表 7-16. ケン・コリアーによって開発されたデータマイニングソフトウェアの評価基準 277
品質保証と品質マネジメント 277
結果との関係 278
脅威プロファイル 278
表 7-17. アクター分類（Actor Classes） 279
表 7-18. 犯行動機（Actor Motivations） 279
表 7-19. 行為者の熟練度 279
帰属属性（Attribution Profile） 279
表 7-20. 帰属属性 280
影響度の分析（Impact Analysis） 280
表 7-21. 影響度の分析 280
暗号通貨とブロックチェーンのフォレンジック機能 280

第 7 章：CIBOK の分類法との関係 282
図 7-6. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 282
表 7-22. CIBOK の分類法 283
表 7-23. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 283
第 7 章：レビュー 285
ケーススタディ 7：サーバー侵入の試み 285

第 8 章：最終処理 289

はじめに 290
最終処理におけるトピックの分類 292
図 8-1.「最終処理」知識領域に含まれるトピックの分類 292
最終処理（サイバー犯罪事件の解決とは） 292
図 8-2. サイバー犯罪の最終処理のモデル 293
事件の捜査と対応組織 293
コミュニケーション 295
図 8-3. 最終処理に向けたコミュニケーション 295
内部 295
表 8-1. 内部コミュニケーション 295
外部 295
図 8-4. CSIRT による情報の共有 296
表 8-2. 外部コミュニケーション 298
手段 298
図 8-5. コミュニケーションプラン 300
技術的な修復 300
役割の割り当て 300
表 8-3. RACI 標準 301
アクション：処置 301
表 8-4. 技術的な修正に関するアクション 301
手続きによる修復 305
図 8-6. 手続きによる修正 305
捜査・調査 305
表 8-5. 電子メールの収集に関係する送達の要件（米国の例） 307
図 8-7. サイバー犯罪の環境 308
図 8-8. 組織的サイバー犯罪 309
図 8-9.「サイバー犯罪条約第 185 号」の調印国 310
逮捕 310
犯罪捜査に役立つインテリジェンス構築 312
起訴 313
表 8-6. 証人の種類 314
サイバー犯罪の発見／防止に関する学びと改善 314
図 8-10. 最終処理の改善 315
第 8 章：CIBOK の分類法との関係 316
図 8-11. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 316
表 8-7. CIBOK の分類法 317
表 8-8. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 317
第 8 章：レビュー 319
ケーススタディ 8：インシデントの解決 320

第 9 章：サイバー犯罪情報の共有 323

はじめに 324
サイバー犯罪情報の共有におけるトピックス分類 325
図 9-1.「サイバー犯罪情報の共有」知識領域におけるトピックスの分類 325
サイバー犯罪の情報共有とは 326
フレームワーク 327
図 9-2. サイバー犯罪情報の共有フレームワーク 327
強固な基盤の重要性： 327
図 9-3. ケースマネジメントのフレームワーク 328
共有コミュニティへの展開： 328
図 9-4. AIS を使用した TAXII による共有方法 330
法的留意事項 330
管轄権 330
犯罪の種類 331
配信 332
標準化 332
図 9-5. 情報共有の基準 332
マネジメント 332
場所 334
図 9-6. 米国における情報共有の位置相関図 335
第 9 章：CIBOK の分類法との関係 336
図 9-7. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 336
表 9-1. CIBOK の分類法 337
表 9-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 337
第 9 章：レビュー 339
ケーススタディ 9：モバイルアプリケーション決済詐欺 339

第 10 章：管理フレームワーク 343

はじめに 344
管理フレームワークにおけるトピックス分類 345
図 10-1.「マネジメントフレームワーク」知識領域におけるトピックスの分類 345
サイバー犯罪捜査・調査のマネジメントフレームワークとは？ 346
戦略およびガバナンス 347
全体的な方向性（ビジョン、ミッション、目的など） 347
戦略の策定 347
図 10-2. CI PDCA プロセス 349
図 10-3. サイバー犯罪捜査の OODA ループプロセス 349
図 10-4. サイバーインシデント対応活動と判断 350
表 10-1. サイバー犯罪捜査職務の企画立案 352
パフォーマンスの見直し 353
組織計画／予算編成 354
予算戦略の構築 354
図 10-5. サイバー犯罪捜査の予算編成戦略 355
リスクアセスメント 355
リスクマネジメント 356
図 10-6. COBIT リスクマネジメントプロセス 357

図 10-7. COBIT 5 プロセス参照モデル 357
リスク軽減 360
表 10-2. 軽減のためのリスク査定 361
図 10-8. OWASP リスクランキング 362
予算編成 362
予算消化率マネジメント 363
リソース使用率マネジメント 364
図 10-9. 簡単な予算消化率マネジメントの例 364
予算マネジメントプロセスの改善 364
人事 365
人事組織の規定 365
職務分掌 366
図 10-10. 3 ラインモデル 367
表 10-3. セキュリティ活動に必要な機能の例 368
人材利用計画 368
人材パフォーマンスのマネジメント 368
必要となる知識・スキルの定義 369
図 10-11. プロジェクト GLACY モデルでの技能とサイバー犯罪捜査職務との関係 369
採用と雇用 369
表 10-4. 活動内容別のサイバー犯罪捜査官の採用 370
技能パフォーマンスの目標 370
知識とスキルの検証 370
パフォーマンスのマネジメント 370
組織パフォーマンスの測定基準 371
組織の監査 371
業務プロセスの測定基準 371
業務プロセスの監査 371
パフォーマンスの測定と改善 371
人材のマネジメント 372
集団力学（グループダイナミクス） 372
学習する組織の構築 372
コーチング 372
チームビルディング 372
モチベーションのマネジメント 373
多文化環境のマネジメント 373
ツールのマネジメント 373
戦略的要求に対するツールの選択 373
戦術的要求に対するツールの選択 374
ツール利用率マネジメントとパフォーマンスの見直し 374
ツールのトレーニングと認定 374
第 10 章：CIBOK の分類法との関係 375
図 10-12. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 375
表 10-5. CIBOK の分類法 376
表 10-6. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 376
第 10 章：レビュー 378
ケーススタディ 10：サイバーセキュリティリスクのオーナーシップ 379

第 11 章：実践的サイバーリスク管理 381

はじめに 382
実践的なサイバーリスクマネジメントにおけるトピックス分類 383
図 11-1. 実践的なサイバーリスクマネジメント領域におけるトピックス分類 383
実践的なサイバーリスクマネジメントとは 383
リスクマネジメントとサイバーリスク 384
リスクの所在の明確化 384
リスクオーナーシップの明確化 384
表 11-1.「脅威」、「脆弱性」、「サイバーリスク」の関連性 385
図 11-2. サイバーリスクの脅威の起源 386
リスクシナリオ 387
図 11-3. 蝶ネクタイ図 387
リスクシナリオの作成 387
図 11-4. 犯罪進行シナリオの例 388
図 11-5. リスクシナリオを特定するためのサンプルテンプレートの例 388
代表的なリスクマネジメントフレームワーク 388
表 11-2. セキュリティマネジメントフレームワーク 388
表 11-3. リスクマネジメントフレームワーク 389
サイバーリスクマネジメントの実践 389
保護すべき資産を特定する 389
影響を特定する 390
表 11-4. 米国 FIPS199 の潜在的影響 391
リスク発生シナリオの特定 391
図 11-6. フォールトツリー分析チャートの例 392
インシデント発生後のリスクシナリオの特定 393
図 11-7. 影響の木チャートの例 394
リスク評価 394
表 11-5. 定量的評価のためのリスクマトリックスの例 395
図 11-8. イベントツリーを用いた犯罪成功確率の分析 396
図 11-9. 脆弱性対応のための OODA ループ 396
リスク対応 397
図 11-10. リスク対応の選択肢 397
図 11-11. リスクプロファイル、リスクキャパシティ、およびリスクアペタイトの関係 398
図 11-12. ALARP 398
図 11-13. 費用便益分析を用いた ALARP の計算 399
リスクモニタリング 399
図 11-14. サイバーセキュリティ PDCA ＋ OODA 399
図 11-15. リスク再評価の入力例 400
リスクレポートと見直し 400
11 章：CIBOK の分類法との関係 402
図 11-16. サイバー犯罪捜査およびインシデント調査における実行フレームワーク 402
表 11-6. CIBK の分類法 403
表 11-7. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係 403
第 11 章：レビュー 405
ケーススタディ 11：インサイダーデータ盗難 406
フォレンジック分析結果： 407

付録 409

主要な用語と定義 410
参考書目 422
Index 434
あとがき 438

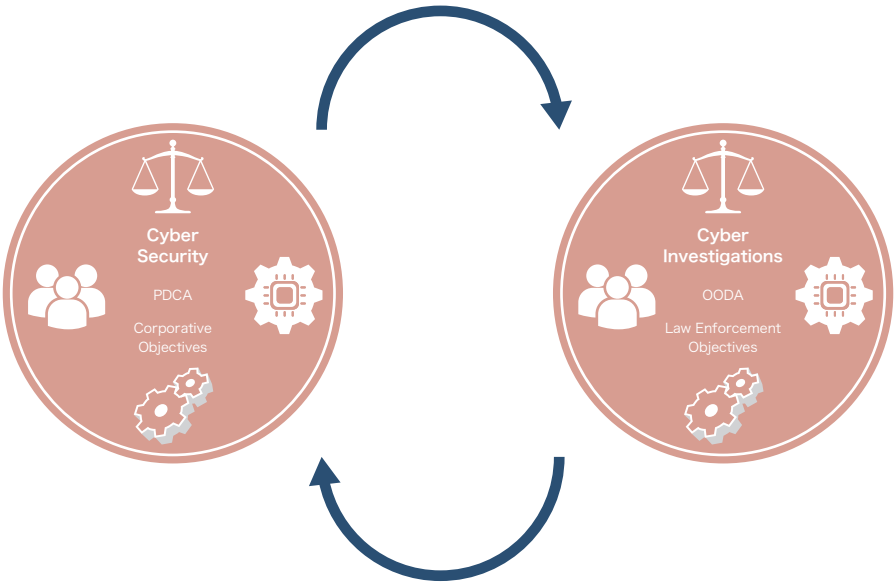
序 章

本書に対する序言

本書の対象読者

本書の対象読者は以下のグループおよび個人であるが、民間組織の最高情報セキュリティオフィサー（CISO）、リスク管理チーム、インシデント対応（IR）対応チーム（CSIRT）も含まれる。

- 犯罪捜査を行う警察組織や法執行機関（検察、裁判所等）、同様の職務執行組織（捜査権、逮捕権等の警察権が認められている組織等）の職員、組織の不正行為を捜査する職員、犯罪捜査の経験があるが「サイバー犯罪」に不慣れな者。
- 新たに組織内にサイバー犯罪捜査チームの組成を任命された責任者。
- すでに犯罪捜査の実働組織をマネジメントした経験があり、今後、サイバー犯罪捜査部門への配属が見込まれる幹部研修生。
- 短期的に高い効果を発揮するサイバー犯罪捜査官をトレーニングするプログラムの研究・開発・指導を行う者。



Same coin, different focus

ヒント

緑の卵とスパムメール - 効率的なインシデント対応

かつて、コンピュータに
誰も知らないユーザーが作成したデータがありました
それは存在しない誰かに盗まれました
そして、それが事件を拡大させたのです

他の 2 台のコンピュータにはマルウェアが感染し
別の 1 台はブラックリストに登録された IP アドレスとの
異常な通信を行っていました
だから誰もがロジック・ボムを心配しました。

… ドロッパーやダウンローダー、トロイの木馬などのマルウェア、
さらには匿名のハッカー集団、中国やサイバー攻撃で知られるシャムーンなどの脅威が
次々に心配されていたのですが …

しかし、一瞬でも立ち止まって
全体をじっくり考えようとする人はいませんでした。

実は、そのコンピュータにアクセスしたのは、
その夜、経理部のボブでした。
なぜなら、同僚のトムが昇進したことに、
ボブが納得できなかったからです。

ところが、会社は中国のハッカーを疑い、
イランがなぜ関与しているのかを調査し、
ベンダーに多額の資金を投入していました。
しかし、実際には、もっとシンプルな方法で
問題を解決できたはずだったのですが …

何が起きたのかよく見て
あせって結論を出すのはやめよう
問題の原因がマルウェアだと決めつけないで
コトの真相に辿りつけたことでマルウェア感染の原因を作ってしまったボブは罪を免れました。

シェーン・シュック (Shane Shook, PhD) による
https://blogs.blackberry.com/en/2013/07/green-eggs-and-spam-efficient-incident-response

「CIBOK」の概念

なぜ「CIBOK」なのか

サイバーセキュリティは、組織に対するサイバーリスクを特定し、軽減することを目的とする組織のマネジメント機能である。組織が業務遂行する際には常にリスクと背中合わせであり、そうしたリスクを低減するためのリスクコントロールはポリシー、プロシジャーによって定義され、トレーニングによって業務に関わるメンバーへの周知・浸透が図られている。また、IT は組織のリスク管理機能をサポートし、組織が顧客（下流）に継続的にサービスを提供する能力に対するリスクを軽減し、市場、株主、パートナーに対する経営陣の義務を履行できるようにする。

IT が組織の要件をサポートするように進化するにつれて、テクノロジーをツールとして活用する方法、企業が使用する IT をターゲットにする方法、サイバー手段によって組織の機能を妨害する方法にも、関連する進化が生じた。最高情報責任者（CIO）は、組織の戦略に参加する役員会に席を得て、情報保護やインフラストラクチャセキュリティなどの IT サポートを通じて業務の継続性を確保する責任を負う。CIO をサポートするために、最高情報責任者（CISO）の役割が創設され、戦略および戦術計画とリソース管理を監督することになる

IT の急速な進歩とそれに伴う脅威により、市場情報（無償および有償の）が進化し、組織に新たなリスクをもたらすと同時に、新たなスキル、知識、経験の要件も発生している。その結果、組織に発生する問題調査および情報ニーズをサポートするために、サイバー犯罪捜査官および民間におけるインシデントレスポンスチーム（CSIRT）の役割が生まれた。本書『サイバー犯罪捜査の知識体系』（CIBOK）は、法執行機関や企業のリスク管理者、IT 管理者、インシデント対応チームなどを支援するために、サイバー犯罪捜査官のスキル、背景、要件を説明することを目的としている。

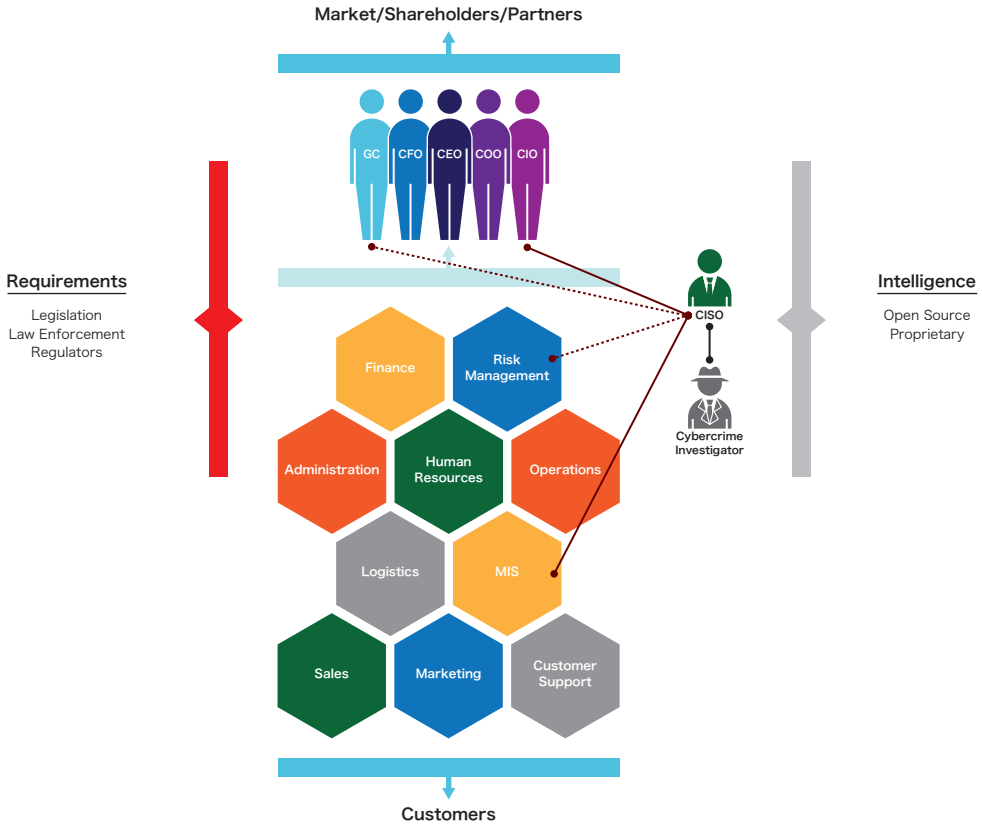


図 1-1. サイバー犯罪捜査フレームワーク

「CIBOK」とは何か

本書の目的とは

CIBOK の目的は、有能で熟練したサイバー犯罪捜査官および CSIRT メンバーが捜査活動で実践するベストプラクティスを示すことである。

目的は、サイバー犯罪捜査およびインシデント調査で一般的に習得しなければならない知識、スキル、アプローチを体系的に分類および整理した利用しやすい分類法を示すことである。このため、各トピックに関する説明は、読者がトピックに関連する参考資料を見つけるのに必要な範囲に限定されている。知識体系自体はこのドキュメント内には記載されていないが、参考資料から見つけることができる。

CIBOKを確立する5つの目的

本書は、次に示す 5 つの目的に従って作成されている。

1. 各国の法律に左右されず、世界中で一貫したサイバー犯罪捜査への常識的なアプローチを普及・推進する。
2. サイバー犯罪捜査およびインシデント調査の範囲内で、プロジェクト管理、コンピュータサイエンス、デジタルフォレンジックにおける他の体系化された慣習的慣行の詳細なデモンストレーションを提供する。
3. サイバー犯罪捜査およびインシデント調査において実践すべき内容を特徴付けして実証する。
4. トピックを実際に活用する手段を提供する。
5. サイバー犯罪捜査およびインシデント調査訓練のカリキュラムの開発および個人の知識とスキルが高いレベルにあることを実証する。

第 1 の目的（世界的な規模での一貫したサイバー犯罪捜査およびインシデント調査に関する知識）を達成するために、本書は世界中の著者（査読者を含む）の参加を得て作成された。

第 2 の目的（サイバー犯罪捜査およびインシデント調査の範囲内で体系化されたその他の慣習的慣行の詳細な実証）を達成するために、特定の資料が実行可能なフレームワークとして含まれている。これらの資料は、サイバー犯罪捜査およびインシデント調査実行フレームワーク（図 1-2 に例示されている 8 つの知識領域で構成）に従って分類されている。

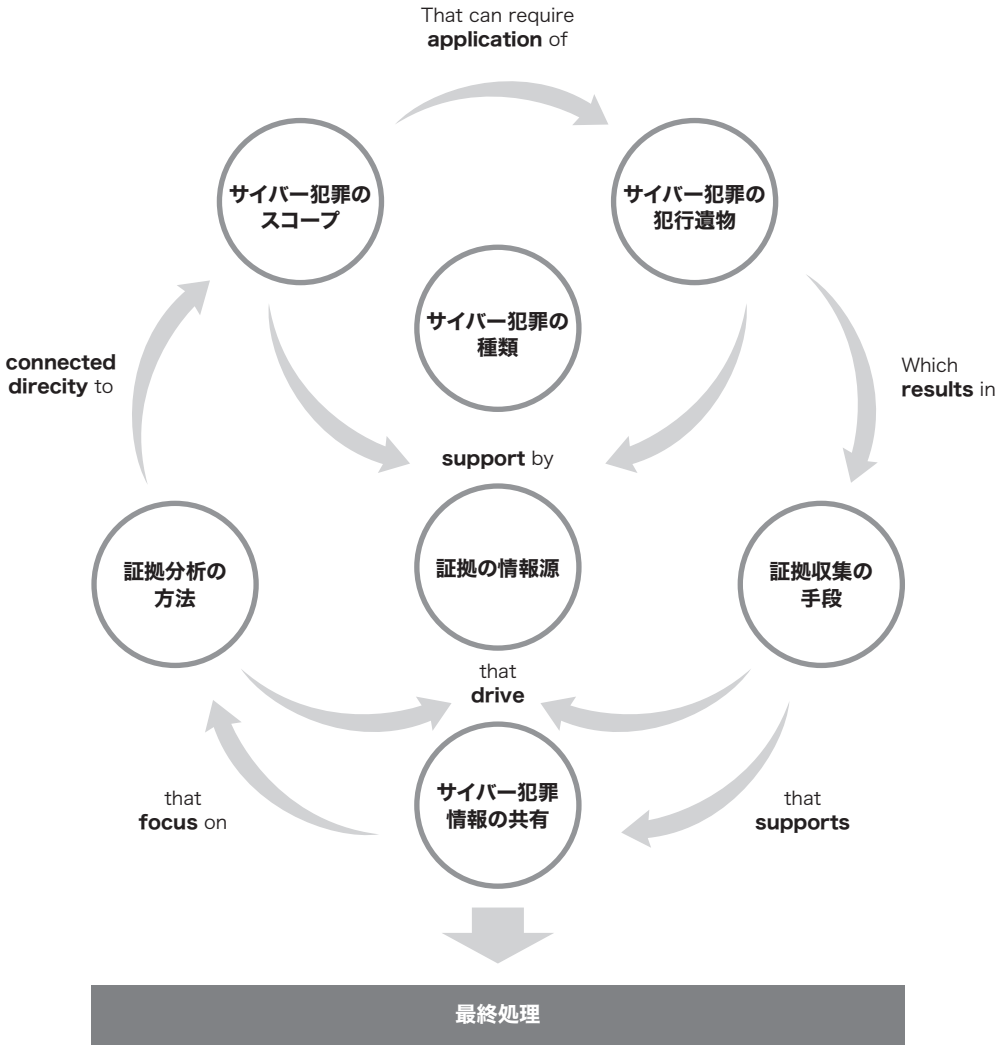


図 1-2. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

範囲を詳細化するにあたって、サイバー犯罪捜査およびインシデント調査と関連する業務慣行を特定することが重要である。本書では、表 1-1 に例示されている 6 つのフレームワークを使用して、関連する領域を示す。これらの関連するフレームワークに関する包括的な知識の習得は、効果的な業務慣行に必要であるが、本書の範囲外である。

例えば、すべての新人警察官や新たに CSIRT メンバーとなった者（サイバー分野であるか否かを問わず）に求められる知識やスキルは「警察官としての基礎」フレームワークとして定義されており、各国の法制度で定められた警察官の正式な要件を満たすことで民間においても各組織の事業ドメインに沿った導入教育、基礎教育などにより役割を担う上での必要なスキルを習得することができる。

本書では、警察官としての基礎知識を習得していること、民間組織のメンバーとしての基礎教育を受けていることを前提条件としているため、こうした基盤となるような知識そのものについては言及していない。これらのフレームワークを構成する 13 の法執行機関としての知識領域を参考情報として以下に示す。知識領域は各国の法制度によって異なるという点に留意すること。基礎フレームワークを取得する場合は、警察学校やその他の研修・研究機関での研修を通じて正式な認定が実施され、通常 600〜1000 時間のテストも含まれる。

表 1-1.「実行」を支える「関連」フレームワーク

フレームワーク名	知識領域
警察政策 戦略＆統制フレームワーク	矯正政策、被害者学などもその範疇に含み、サイバー分野における刑事法にまつわる諸政策について警察組織が戦略を定義または立案するため、または警察政策の遂行が健全かつ有効に運用されているかどうかを保障するためのフレームワーク
資金調達および 予算管理フレームワーク	警察戦略の遂行を支える上で必要な財務機能を明確にし、歳出を適正にコントロールすることで、限られた資金や資源を、必要とされる施策に対し効率的に配分し、確実かつ効果的に成果を生むためのフレームワーク
効果的なポリシング＆ 防犯管理フレームワーク	優先順位を付けることが困難である「秩序維持」というミッションに対し、どのような良質な「警察サービス（Policing Services）」を提供することで、ステークホルダーの要求を満たすことができ、社会的な達成を得ることができるのか検討するためのフレームワーク
サイバー犯罪捜査 実行フレームワーク （Cybercrime Investigation Execution Framework）	サイバー犯罪の分類（Type of Cybercrime）
	サイバー犯罪の関連技術（Cybercrime Artifact）
	サイバー犯罪のスコープ（Scope of Cybercrime）
	証拠の情報源（Source of Evidence）
	収集の手段（Method of Collection）
	分析の手段（Method of Analysis）
	情報共有（Information Sharing）
	最終処理（Resolution）
基礎 （Foundations）	コンピュータエンジニアリング
	コンピュータサイエンス
	システムエンジニアリング
	プロジェクトマネジメント
警察官としての基礎 （Police Officer Core）	行政手続き（Administrative Procedures）
	憲法（Constitutional Law）
	倫理とプロフェッショナリズム（Ethics and Professionalism）
	犯罪に関する人間行動（Human Behavior）
	警察活動とパトロール（Policing and Patrol）
	国土安全保障（Homeland Security）
	法執行（Law Enforcement）
	犯罪捜査（Criminal Investigation）
	報告書作成（Report Writing）
	初動対応（First Responder）
	防衛戦略（Defensive Tactics）
	銃火器（Firearms）
	体力鍛錬と健康維持（Physical Training and Wellbeing）

サイバー犯罪捜査およびインシデント調査に貢献する捜査部門が使用するこれら 6 つの枠組みは、図 1-3 に示されているように、犯罪部門を管理するための「**マクロフレームワーク**」を形成している。

本書の各章では、マクロフレームワークがミクロレベルで分析および定義され、日常的なサイバー犯罪捜査およびインシデント調査活動が刑事政策に与える影響を測定するために捜査官が習得する必要がある主な活動と手順が示されている。

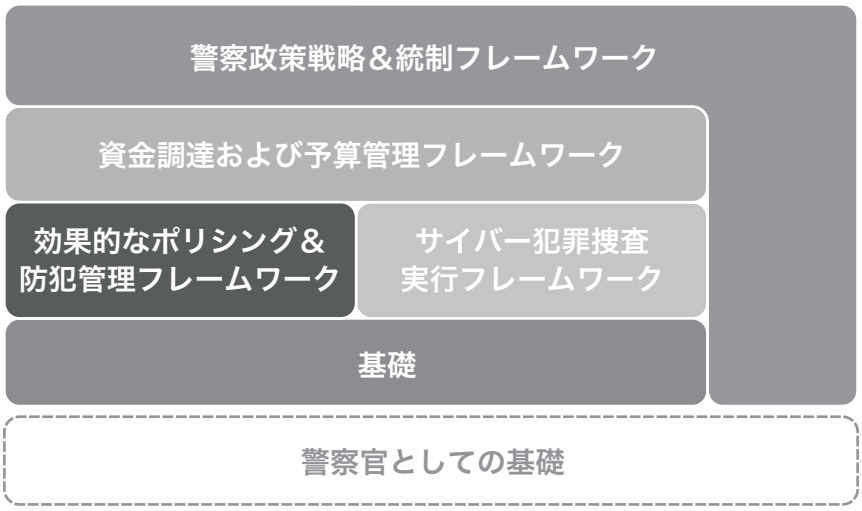


図 1-3. サイバー犯罪捜査およびインシデント調査部門のマクロフレームワーク

第 3 の目的（サイバー犯罪捜査およびインシデント調査で実践すべき内容の特徴付けと実証）を達成するために、各知識領域の組織構造を分類する。

第 4 の目的（トピックを実際に活用するための手段の提示）を達成するために、本書では、8 つの知識領域（図 1-2 に表示）のそれぞれについて信頼できる参考資料と共に、管理フレームワークと実用的なサイバーリスク管理へのアプローチを示す 2 つの章（それぞれ第 10 章と第 11 章）を提供する。

第 5 の目的（サイバー犯罪捜査およびインシデント調査の研修カリキュラムの開発と個人の知識および技能が高いレベルであることを示す）を達成するため、サイバー犯罪捜査およびインシデント調査に従事する捜査官が現在使用している知識および技能を職務分析としてまとめている。そうすることにより、一般的に受け入れられている知識基準が確立され、基準に基づく筆記、口頭陳述、実技評価、観察などの客観的かつ信頼性の高い方法を使用して捜査官の能力を評価することができる。

サイバー犯罪とその捜査

サイバー犯罪とは

サイバー分野に限らず、法律で何を犯罪と規定するかは国によって異なる。また、歴史的背景によっても何を犯罪とみなすべきかは変化する。そこで、本書では「**サイバー犯罪**」を以下のように定義する。

サイバー犯罪とは、**サイバー空間**（コンピュータ、コンピュータ・ソフトウェア、コンピュータ・ネットワーク、またはシステムを制御する組み込みソフトウェアを含む）に関わる行為であって、社会の集団意識の中で強く定義された様々な規範に違反するものと定義される。

サイバー空間はネットワークからなる新しい**社会領域**である。この領域は、すでに市民生活の隅々にまで浸透しており、サイバー空間を利用できる他の領域は、地域的・地球的規模で拡大している。サイバー空間は、陸、海、空、宇宙を含む実際の「領域」における様々な活動を支える必要不可欠なインフラを提供する。国家の管轄外の領域（国際水域、国際空域など）と同様に、人類共有の財産として認識することができ、その結果、サイバー空間における犯罪活動は、従来の犯罪とは異なる。

「**犯罪学**」や「**刑事政策**」において考慮すべき犯罪要素を、「**b/d/r ダイナミクス**」を用いて図 1-4 に示す。

犯罪とは、「**個人**」が「**被害者**」に「**損害**」を与える有害な「**行為**」を犯した場合、それに対して「**社会**」から「**反応**」が起こることである。

$$\mathbf{I - b \cdot d - V}$$
$$\mathbf{r}$$
$$\mathbf{|}$$
$$\mathbf{S}$$

（訳注：I= 個人、b= 行為、d= 損害、V= 被害者、r= 反応、S= 社会）

図 1-4. b/d/r ダイナミクス

図 1-4 に示されているように、「社会」を構成する国によって「反応」は異なる。したがって、国によって犯罪の定義が異なるのは必然である。さらに、捜査・調査においては、「行為」だけでなく「被害」によって捜査対象を絞り込む必要がある。その上で、捜査を介して個人を発見し、証拠を確保しなければならない。

サイバー空間における横領や不正行為が、既に法律で規定されている犯罪行為を実現するための手段として利用されているに過ぎない場合がある。法執行機関としては、従来の捜査部門との連携が、こうした有害行為の捜査を加速させるかどうかを早急に見極めることが不可欠である。そのため、表 1-2 に示されているように、サイバース空間で発生する有害行為のカテゴリを定義する必要がある。

表 1-2. サイバー空間で発生する有害行為のカテゴリ

攻撃対象としての技術（Technology as a Target）	サイバー空間の出現以前には存在し得なかった、被害者に損害を与える行為
犯罪の道具としての技術（Technology as an Instrument）	サイバー空間、その技術を手段として悪用することで、被害者に損害を与える行為
（犯罪から）目をそらす手段としての技術（Technology as a Distraction）	サイバー空間、その技術を捜査からかく乱することを目的とする技術として悪用することで、調査員（Investigator）や事件対応員（Responder）から標的のシステムや情報から引き離す行為
他の犯罪に付随する技術（Technology Is Incidental to Other Crimes）	サイバー空間、その技術により、資金洗浄（Money Laundering）や不法な銀行取引（Unlawful Banking Transactions）、電子コミュニケーションサービスを介した違法活動の支援、記録の改ざんによる犯歴の消去や投薬量の変更などによる殺人などに悪用する行為
普及技術と関連した犯罪（Crime Associated with the Prevalence of Technology）	サイバー空間、その技術により、ソフトウェアの違法コピーまたは偽造（コンピュータプログラムの著作権侵害）、偽造機器、闇市場におけるコンピュータ機器やプログラム、および技術設備に対する盗難する行為

表 1-3 と表 1-4 はサイバー空間で発生する有害行為による被害者への被害とリスクを分類したものである。

表 1-3. サイバー空間で行われた有害行為によって生じる被害者の損害のカテゴリ

人身傷害	**財産的損害**	消極損害	サイバー犯罪を受けたことにより、生じた事故対応費用、責任に対する損害賠償
		積極損害	サイバー犯罪を受けたことにより、IT 機器等が機能停止などに陥り、それによって生じた逸失利益、事業継続費用、または喪失した市場機会に対する損害
	精神的損害	サイバー犯罪を受けたことに対する苦痛（名誉毀損、信用毀損）の損害	

表 1-4. サイバー空間における被害者のリスクのカテゴリ

分類名	詳細
可用性（Availability）リスク	システムダウンなどがもたらす損害
パフォーマンス（Performance）リスク	システムの処理能力が低下することによる損害
市場（Market）リスク	ブランドの毀損や市場における信頼の喪失による損害
不正（Fraud）リスク	金融・有価証券として保護すべき情報の窃盗によってもたらされる損害
コンプライアンスリスク	法令やガイドラインを遵守しないことがもたらす損害
セキュリティリスク	セキュリティ対策の不備がもたらす損害
安全性（Safety）リスク	システム運用により人員の危険をさらす損害

サイバー犯罪捜査およびインシデント調査とは

本書では、**「サイバー犯罪捜査（Cybercrime Investigation）およびインシデント調査」**を次のとおり、定義する。

> 犯罪がサイバースペースで行われたとみなされた場合に、起訴を提起し維持するための犯罪証拠の発見、収集、保存、確保に関わる行為（民間の場合も同様に、犯罪証拠の発見、収集、保存、確保に関わる行為とする）。被害を受けた側のインシデントマネジメントとして、被害の確定とその保全。

これらの活動は、一般的に、表 1-5 に示されているように、**「事前予防調査」**と**「事後対応調査」**の 2 つに分類することができる。

表 1-5. サイバー犯罪捜査およびインシデント調査活動のカテゴリ

事前予防捜査 (Proactive Investigation)	法執行機関が犯罪を企てている容疑者を予見し、その逮捕を目的に行われる捜査活動である。このタイプのオペレーションでは「**洞察（Intelligence）**」の構築が活動開始の端緒となる
事後対応捜査 (Reactive Investigation)	犯罪発生後に法執行機関が容疑者の証拠について収集・確保を行い、その逮捕を目的に行われる活動である。このタイプのオペレーションでは市民からの「**通報（Report）**」または捜査官による「**警ら（Patrol）**」が活動開始の端緒となる

サイバー犯罪捜査およびインシデント調査活動の本質は、従来の捜査活動と同じである。いずれの捜査活動においても、捜査官は関係各国の法律、規制、条約を遵守しなければならない。さらに、捜査活動においては、個人の自由や権利を不当に侵害することなく、事実を解明し、問題を解決するために捜査権限を誠実かつ公正に行使することが不可欠である。

しかし、表 1-6 に示されているように、サイバー犯罪には従来の犯罪とは異なる特徴がいくつかある。

表 1-6. サイバー空間における犯罪の特性

1. 時間的・地理的無限定性	サイバー空間はネットワークで結合している社会領域である。このため、身体の所在としての地理的位置（犯罪の実行地、証拠の所在地、被害発生地）にとらわれずに、また同期的にも非同期的にもやりとりが可能となった
2. 被害の不特定多数性	サイバー空間は不特定多数の者に対して情報を発信することができ、短時間の内に不特定多数の者に影響を及ぼしやすい
3. 無痕跡性	サイバー空間はすべてデジタルデータのやりとりである。その記録を保存するための措置を特に講じない限り、その痕跡は残らない。また、その記録が保存されている場合にも、改ざんや消去、暗号化、難読化が容易である
4. 匿名性	サイバー空間は相手方の顔や声を容易に偽ることが可能で、筆跡、指紋等の物理的な痕跡も残らない。相手方が本人であるかどうかの確認は、デジタルデータに依存して行われる

これらの特性により、サイバー犯罪に関わる捜査活動はあらゆる分野で改革を必要としている。ここでは 2 つの重要な側面が示される。

第 1 の側面は、サイバー犯罪捜査およびインシデント調査活動における協力とコーディネートである。伝統的な犯罪のほとんどは、一つの司法管轄区内で行われる。そのため、関連する捜査活動は、犯罪者と被害者が同じ領域内に存在することを前提に構築されてきた。サイバー空間は、個人の存在や企業の経済活動の多様化をもたらし、従来は当然と考えられていた様々な境界（国民国家の枠組みなど）を崩し続けている。こうした変化は、犯罪捜査活動をより困難なものにしている。例えば、犯罪者が犯行後すぐに別の管轄区域に逃亡する事例や、同一犯者が広範囲で連続して犯行に及ぶ場合も報告されている。

また、サイバースペースをインフラとして利用することで、**組織犯罪グループ**の組織力が高まり、国際的な活動を拡大し、外国へ進出するようになっている。さらに、テクノロジーを標的とした新しいタイプのサイバー犯罪（表 1-2 に示されている「標的としてのテクノロジー」）を扱う新興犯罪組織も出現している。

そのため、サイバー犯罪の捜査は、常に複数の管轄区域にまたがる活動を前提としている。事件発生後の初動対応を迅速かつ的確に行うためには、警察の管轄区域をまたがる捜査を行う「**広域捜査班**」の編成が不可欠であり、国際的な主権間の調整・連携にも留意する必要がある。

第 2 の側面は、サイバー犯罪捜査およびインシデント調査活動中の犯罪者による「**証拠隠滅**」である。適法な手段で得られた証拠でなければ、公訴を提起し、公判を維持することは困難である。特にサイバー犯罪については、中核捜査機関を通じた外部からの「**検証**」によって得られる証拠には限界がある。サイバー空間における行為はすべてデジタルデータのやり取りであるため、そのデータを保存するための具体的な措置が取られない限り、痕跡は残らない。また、専門的な知識を持つ者による内部の「**鑑定**」でな

ければ得られない証拠もある。

したがって、サイバー犯罪捜査およびインシデント調査に携わる捜査官は、先入観にとらわれることなく、根拠のない憶測を排除し、有形の**「物的証拠」**だけでなく、デジタル証拠も扱う必要がある。被疑者や関係者の**「目撃証言」**を過大評価してはならない。サイバー空間では、誤解や思い込みによる衝突が起きることもある。基礎捜査を論理的に徹底し、あらゆる証拠の発見と収集に努めなければならない。

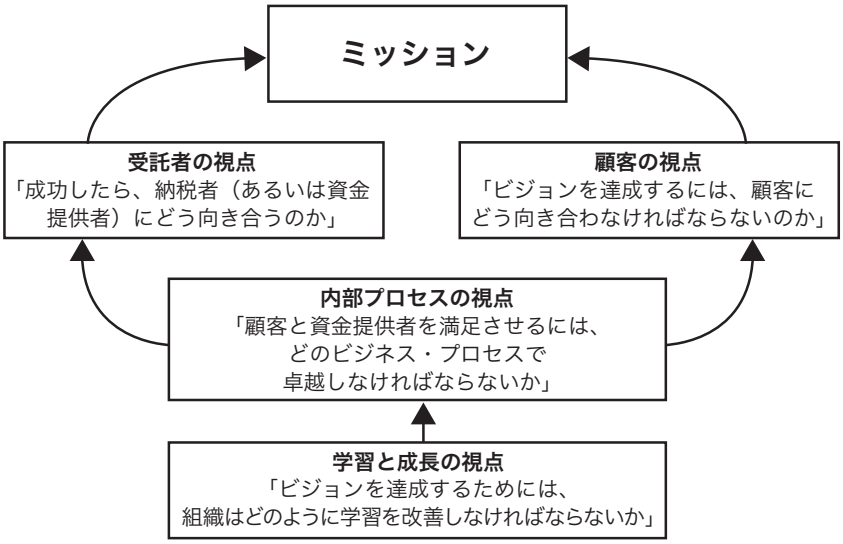
捜査を行うにあたり、入手可能なすべての情報と照合された資料に基づいて総合的に判断しなければならない。そのためには、幅広い知識と技術力を実践的に活用する必要がある。しかし、捜査官は、自らの能力を過信したり、自らの判断だけに頼ってはならない。捜査官の倫理を常に意識し、組織の力で総合的に捜査を進めることが不可欠である。

刑事政策及び民間の事業ドメインに立脚する戦略と計画

価値創造のフレームワーク

法執行機関のサイバー犯罪捜査およびインシデント調査部門にとっての究極の成功は「ミッション」の達成である。民間企業においても同様である。図 1-5 は、ミッションから戦略を導き出すためのフレームワークを示している。

「ミッション」（最も重要な長期目標）は、質の高い警察サービスを提供することで「ステークホルダー」の満足度を高めることである。したがって、ミッションは図 1-5 に示すフレームワークの最上位に位置付けられる。



『戦略マップバランスト・スコアカードによる戦略策定・実行フレームワーク復刻版』
ロバート・S. キャプラン（著）、デビッド・P. ノートン（著）、櫻井通晴（監訳）、伊藤和憲（監訳）、長谷川恵一（監訳）

図 1-5. サイバー犯罪捜査およびインシデント調査班へのフレームワークの適用

法執行機関が掲げるミッションの幅は広く多様である。例えば、**「国際刑事警察機構（INTERPOL）」**は、次のミッションを掲げている。

Preventing and fighting crime through enhanced cooperation and innovation on police and

security matters
警察と治安に関する協力とイノベーションの強化を通じて犯罪を防止し、犯罪と闘う

INTERPOL などの法執行機関の任務は、**「秩序の維持」**など社会的意義の高い内容を含んでいる。その結果、達成基準は優先順位を決めるのが難しい社会的指標になる。

ミッションを達成するための条件を計画するには、まず**「顧客の視点」**、つまり、ステークホルダーが**「サイバー犯罪班」**に何を求めているか、そしてその要求を満たし社会的成果を達成する**「警察サービス」**の質がどのようなものかを検討する。

- ステークホルダーの定義（捜査官、納税者、資金提供者、警察長官、議会、協力する民間企業など）
- ステークホルダーのセグメンテーション
- ステークホルダーに何を提供すべきか
- ステークホルダーの声をどのように把握し、戦略に反映させるか

「受益者の視点」には、納税者や資金提供者などの重要なステークホルダーの戦略目標が反映される。顧客とは異なり、資金提供者は必ずしも警察サービスの受益者ではない。サービス受益者になることもあるが、そうならないことも多い。

図 1-5 に示されているフレームワークは、**「学習と成長の視点」**によってサポートされる**「内部プロセスの視点」**の実行を通じて、法執行機関が成功するためのルートを示している。

法執行機関が使用するリソースは決して無尽蔵ではない。リソースは、捜査官、納税者、寄付者、警察長官、議会、協力する民間企業などのステークホルダーからの提供に依存している。しかし、財務基準は、必ずしも機関がミッションを遂行しているかどうかの適切な指標ではない。社会指標と財務指標の間に明確な関係がない限り、ミッションから戦略を導き出すフレームワークに財務の視点を含めるべきではない。

サイバー犯罪捜査およびインシデント調査部門の構成

伝統的な捜査組織体制におけるサイバー部門の検討

図 1-6 は、基本的な従来の犯罪捜査組織の体制を図示したものである。サイバー犯罪捜査官は、社会や組織の要請に応じて、伝統的な組織体制に対して、警察サービスの提供を行う必要がある。

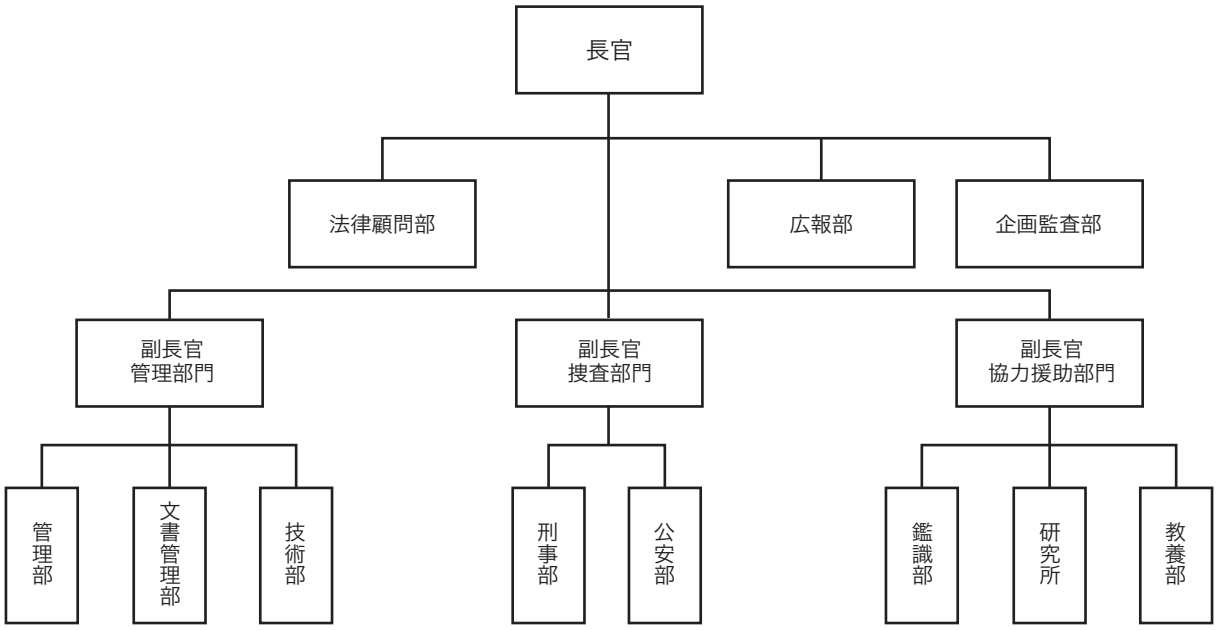


図 1-6. 基本的な従来の犯罪捜査組織の体制

サイバー部門とサイバー捜査官は、インシデントを解決するために、従来の捜査部門と連携できなければならない。

長官は「**サイバー犯罪班**」の任務を指揮する役割を担う。この役職は組織の形態によって異なるが、ここでは便宜上、この人物を「指揮官」と定義する。

指揮官に与えられる権限、資源、人員は組織構造によって異なる。しかし、いずれの場合も指揮官が組織のトップと質の高いコミュニケーションを実現することが不可欠である。

組織の構造の大きさは、組織の長や指揮官、または法律によって規定される範囲に依存する。

図 1-7 に示されている「**カテゴリ型組織**」は、刑事部や公安部などの専門の「部」に分かれ、その下に「課」がある組織の例である。これらの部は、犯罪のカテゴリ（重罪、麻薬、銃器、詐欺など）に焦点を当てた「セクション」に分かれている。サイバー犯罪班は、指揮官が統制する組織としてこれらのセクションの下に配置される。これらの部署やセクションを分類する場合は、各国の法制度を参照する必要がある。

カテゴリ型組織構造では、サイバー犯罪班の責任範囲はカテゴリ部門の領域に限定される。その結果、少ない人員でユニットを立ち上げることができる。図 1-7 が示すように、複数のセクションにまたがる共同ユニットもあれば、特定のセクション専用のユニットもある。いずれの場合も、ユニットの範囲は限られているため、複数のセクションが同時に同様の機能を担当するユニットの設置を要求する場合がある。同様の機能を担当するユニットが分散している場合、それらのユニット間のコミュニケーションが問題になる。

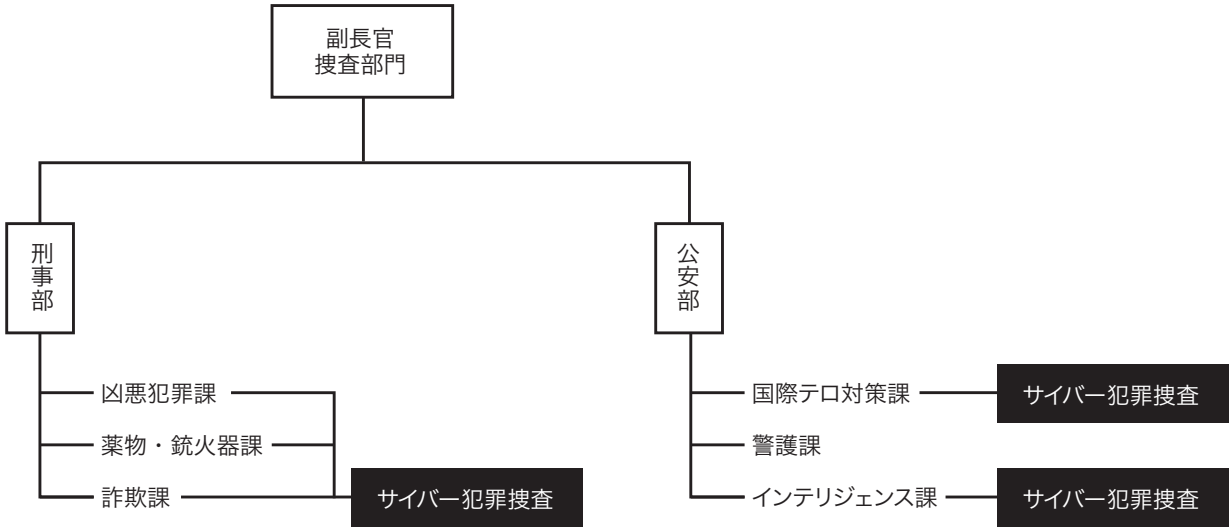


図 1-7. カテゴリ型組織

図 1-8 に示されているように、**「マトリクス型組織」**では、サイバー犯罪捜査およびインシデント調査班は専門の「部」として設置される。サイバー犯罪班は、指揮官が統括する組織として部の下に置かれる。

マトリクス型 s2 組織では、ユニットの責任範囲はすべての部門領域に拡大する。したがって、より強力な権限、リソース、および人員を保持する必要がある。さらに、部門間の連絡担当者として任命される要員は、その部門に関する専門知識を有しているべきである。図 1-7 では、これらの班は「協力支援部門」の下部組織として図示されているが、場合によっては「捜査部門」の下部組織となることもある。サイバー犯罪班の設置場所を決定する際には、各国の法制度と各部門の活動轄範囲を考慮する。

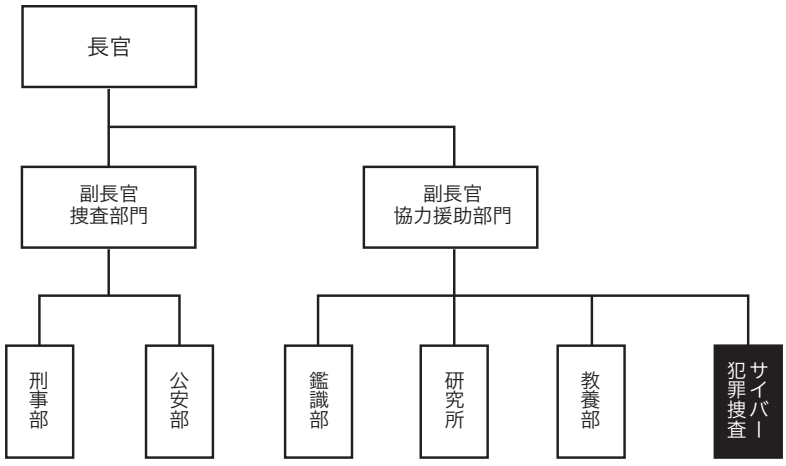


図 1-8. マトリクス型組織

図 1-9 に例示されている**「複合型組織」**は、カテゴリ型とマトリクス型の組み合わせである。サイバー犯罪捜査およびインシデント調査班は、専門部署としてだけでなく部署の下部組織としても存在する。

複合型組織では、ユニットの責任範囲を調整することが可能である。平時は、ユニットはカテゴリー型組織として活動し、緊急時には、プロジェクトチームが別途編成され、別の指揮官が任命されることがある。

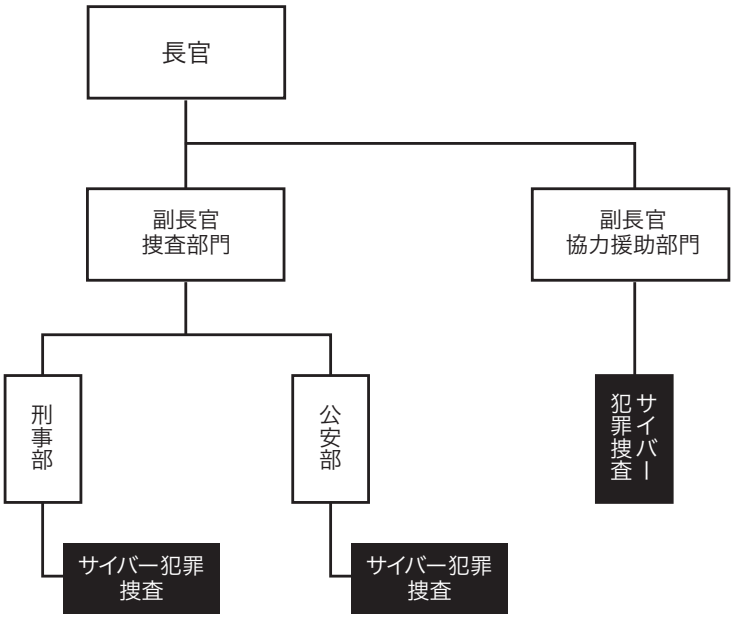


図 1-9. 複合型組織

サイバー犯罪捜査およびインシデント調査班は、従来の組織システムにサービスを提供し、他の部隊と協力して相互理解と機能性を促進することで成功を収めている。サイバー犯罪捜査およびインシデント調査には、分野を超えたメンバーや部署間のコミュニケーションが不可欠である。

すべての組織構造において、以下の主要な要素に関する相互連携が行われなければならない。

- サイバー犯罪捜査およびインシデント調査の戦略的重要性
- サイバー犯罪捜査およびインシデント調査の成熟度
- サイバー犯罪捜査およびインシデント調査の管理体制

国際的なサイバー犯罪の増加に対応するため、法執行機関や民間企業は、官民協力、効率的なコミュニケーション、外部資源の使用に備えておかなければならない。現在、捜査機関と民間企業との連携は、テクノロジー主導のアプローチが主流となっている。この連携を強化し、効果的な経営を可能にするために、組織の経営幹部は企業のリスク管理能力の開発を監督しなければならない。

第 10 章と第 11 章（この版で新たに追加）では、企業が適切な情報セキュリティ能力を確立するための管理フレームワークを紹介して適用し、以下のトピックを取り扱っている。

- 国際的な課題としてのサイバー犯罪や情報ガバナンスに関連する課題についての理解を深め、適切な対策を探る。
- 組織の整合性部門と IT 部門の間の責任分担を明確にし、ガバナンスの問題に対応する。
- ビジネス戦略との整合性を考慮しながら、セキュリティ活動とリスクに対するリソースを適切に優先順位づけして割り当てる。
- セキュリティ対応とサプライチェーン管理において共通の価値観を共有し、一貫性のあるガバナンスを維持する。
- 急速に進化するサイバーセキュリティ状況において、現実的な基準を設定するための柔軟な枠組みを確立する。

企業のサイバーリスク管理フレームワークは、法執行機関とより適切に協力するために、各国のサイバー犯罪に関する様々な期待、法律、その他の慣行から生じる障壁を企業が克服するのに役立つ。この枠組みを実施することで、企業はサイバー犯罪に対してより効果的に対応し、国際社会の安全と繁栄の維持にさらに十分に貢献できるようになる。表 1-9 は、管理フレームワークを含む包括的な CIBOK 分類法と、戦略的、戦術的、および手続き的知識領域との関係を示している。

サイバー犯罪捜査およびインシデント調査

図 1-10 は、典型的なサイバー犯罪捜査およびインシデント調査班の構成を示している。各国の法律や協力機関、兼任する職員などによって構成は変わる。ここでは、サイバー犯罪捜査およびインシデント調査班に必要な機能体制と人材を明確にする。

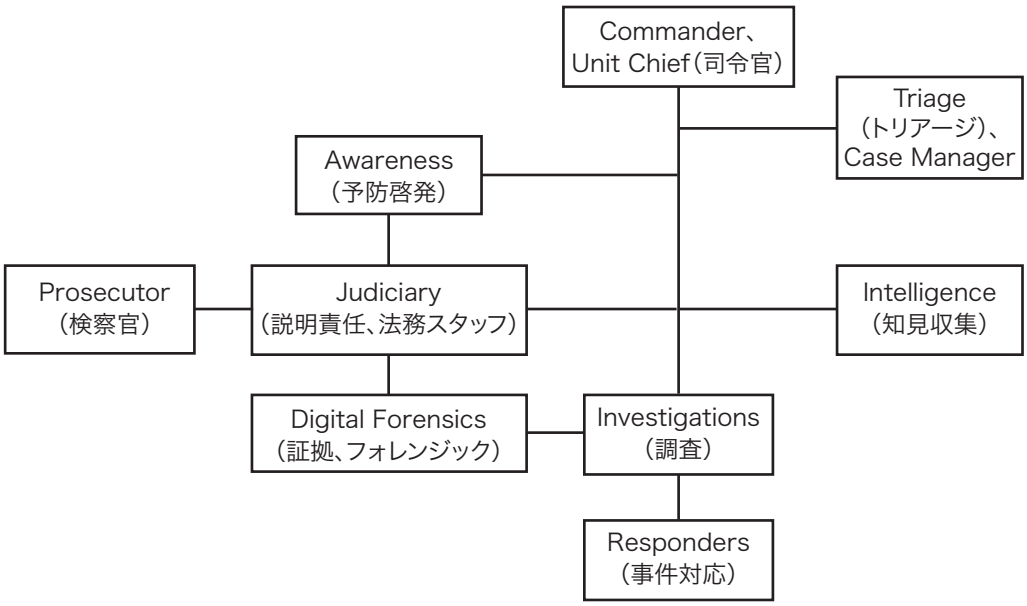


図 1-10. サイバー犯罪捜査およびインシデント調査班の構成図

典型的なサイバー犯罪捜査およびインシデント調査班には、多数の専門家が含まれている。適切な能力やスキルを有する人材を直ちに確保できない場合は、組織外から人材を求めることも検討する必要がある。さらに、スタッフの訓練についても考慮すべきである。

業務内容は専門家によって異なる。しかし、班は常に共通の任務を達成することを目的として編成されるべきである。したがって、専門分野と責任を明確にして、サイバー犯罪捜査およびインシデント調査班のミッションに貢献すべきである。サイバー犯罪捜査班および民間におけるインシデント対応チーム（CSIRT など）では、以下の専門分野が一般的に取り扱われる。

1. 捜査管理（Management/Executive）、Commander/Unit Chief/Triage/Case Manager
2. 知見収集（Intelligence）
3. 調査（Investigations）
   a. 事件対応（Responders）
   b. 証拠（Digital Forensics）

4. 説明責任（Judiciary）
5. 予防啓発（Public Relation、Awareness）
6. 後方支援（Support）
7. 総務人事（Administrative）

管理

管理者とは、複雑なインシデント調査において関連するステークホルダーとの調整を行い、意思決定責任を負う調査員を指す。

この機能では、捜査官や民間の調査員はサイバー犯罪捜査およびインシデント調査に関する活動計画を策定し、中期的な予測に基づいて人員を管理する。マネジメント層は犯罪捜査組織内のサイバー犯罪捜査およびインシデント調査班の期待と能力を理解しているため、この専門分野はサイバー犯罪捜査官にどのような情報、ツール、訓練を提供すべきかを決定することができる。

さらに、経営陣は分野間のサイバー犯罪やサイバー攻撃に関する情報を社外のステークホルダーと共有することができる。

個別のサイバー犯罪については、捜査本部長や民間においては経営陣が包括的な観点から複数のサイバー犯罪捜査およびインシデント調査にどのように関与し、優先順位を決め、人員とリソースを割り当てるかを判断し、ケースマネージャーとトリアージ機能を担当する。

さらに、サイバー犯罪における犯罪傾向のベクトルは「国から国へ」、「大規模組織から小規模組織へ」、「類似業種間へ」と高度化および多様化している。経営陣はこれらの傾向を把握し、関連する情報共有を推進することができる。

CIBOK では、分類法において、「管理者（Manager）」を「経営者（Executive）」の活動として扱っている。

知見収集

知見収集は、さまざまな情報を駆使して全体の方向性や傾向を把握し、効果的な捜査戦略や資産配分を考える捜査官である。

この機能は、アナリストによって報告されたサイバー犯罪の予測やデータの統計処理（データの取得、収集、抽出、クリーンアップ、分析、モデリング）を実行する。知見収集捜査官は、捜査・調査に使用できるさまざまな情報源（経済環境、マクロ／ミクロ経済など）から作戦知見収集を構築できる知識と技術的スキルを持っている。

平常時には、この機能により情報収集の範囲を拡大し、収集したデータに標準化されたデータ構造やモデルを適用して、アーカイブするためのデータ管理システムを構築することができる。

調査

調査は、警察組織においてサイバーに関するさまざまな事柄を扱う捜査官である。この職務はリサーチに関する知識とスキルを必要とする。

これらの捜査官はサイバー犯罪の技術的側面に精通しており、コンピュータサイエンスとネットワーク調査に堪能であり、他の捜査官と連携して犯罪者の逮捕を可能にする情報を提供することができる。

平時には、この機能はジュニアレベルやインシデント対応捜査官向けのトレーニングプログラムの開発をサポートし、一般の人々向けのサイバー犯罪意識向上トレーニングを開発することもできる。

事件対応

事件対応は、治安維持を目的としたサイバー空間での捜査パトロールを担当する捜査官である。

この機能は技術的な知識を十分に使いこなす。事件対応は最初に対応し、最初に犯罪現場を訪れ、犯罪を報告する。犯罪現場では、事件対応は入手可能な「デジタル証拠」を特定し、その証拠の潜在的な影響を確認する。事件対応の報告書は、経営陣がさまざまな調査における優先順位を決定するのに役立つ。

証拠

証拠とは、サイバー犯罪事件において物理的なデジタル機器から「デジタル証拠」を収集し、回復する責任を負う捜査官である。

この機能は、コンピュータサイエンスとネットワーク調査の基本的なバックグラウンドを必要とする。証拠の捜査官は、「証拠の原則」に関する知識と技能を持ち、「デジタル証拠」を特定できなければならない。

この機能は、容疑者による改ざん、削除、または暗号化によって難読化された証拠の復元を試みる。

訴訟段階では、この機能は、質問書を作成したり、関連するデータを提出したりすることで、説明責任機能の調査官を支援する。

説明責任

説明責任捜査官は、実体法と手続法に基づいて、手段、許容性、証明価値の観点から「デジタル証拠」を整理し、基礎資料を作成する責任がある。この役割は、サイバー犯罪に関する警察の手続きにおける説明責任を監督し、警察の捜査に関する実体法と手続き法を理解する。説明責任捜査官は、「証拠」や「調査」を担当する捜査官と同等レベルの知識と技術力を必要とする。

国際的な主権間の調整を必要とする広範な調査においては、説明責任捜査官は状況を熟知している他の地域の説明責任捜査官と連携することができる。

予防啓発

予防啓発捜査官は、サイバー犯罪防止の取り組みを担当する。

この職務では、捜査官はサイバー犯罪を可能にした機会を分析する。これらの捜査官は、犯罪防止環境計画に基づいて国民の意識を高めるためにサイバー犯罪防止情報を提供する知識とスキルを必要とする。

この機能は、調査や説明責任捜査官と連携し、サイバー犯罪の実態に合わせた効果的な犯罪予防策を立案する。これらの捜査官は、国家政府や関係団体と連携しながら、被雇用者、起業家、地域住民の間での意識改革を促進するために、広報活動や啓発、教育機会、情報共有を推進することもできる。

後方支援

この機能は、提供されるサービスに特有の IT および施設サポート活動を含む。

総務人事

この機能は、事務、人事、予算管理、および提供されるサービスに特有の関連活動を含む。

これらの各機能は、「サイバー犯罪捜査およびインシデント調査の実行フレームワーク」と明確な関係を持っている。各フレームワークについては、表 1-7 に示されているように、各機能が必要とするスキルと経験のレベルが、「高」、「中」、「低」（または「適用しない」）と記述される。「サイバー犯罪操作」

と「管理」はプログラム活動であり、これらの活動を実施する機能と混同しないように注意すること。

高 = 知識領域に関するポリシーと手順の開発および解釈に関する詳細な理解と実践的な経験。
中 = 関連する知識領域のポリシー、手順、および関連テクノロジーを活用する他者の適用と管理を通じて得られる知識と経験。
低 = ポリシー要件を満たすために知識とスキルを適用し、関連する手続きガイダンスに従い、知識領域で関連テクノロジーを活用する能力。
適用不可 = 関連する知識ドメインの機能には適用されない。

さらに、各フレームワークについては、各機能で使用される関連知識ドメインが、表 1-8 に示されているように、戦略的（Strategic／計画された長期目標）、戦術的（Tactical／計画された付随的または対応活動）、および手続き的（Procedural／手順、ツール、およびテストによってサポートされる活動）として記述されている。

表 1-7. CI 実行フレームワークと CI 任務の関係、必要なスキルと経験

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 1-8. CI 任務知識領域に対する CI 実行フレームワークの関連性

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

表 1-9. CIBOK 階層構造

戦略的知識、スキルおよび経験														
		戦術的知識、スキルおよび経験												
					手続き上の知識、スキルおよび経験									
サイバー犯罪とその捜査	**サイバー犯罪の種類**	**サイバー犯罪の目的**	**サイバー犯罪者のプロファイル**	**サイバー犯罪組織**	**兆候**	**ステージ（段階）**	**サイバー犯罪の犯行遺物**	**サイバー犯罪のスコープ**	**証拠の情報源**	**証拠収集の手段**	**証拠分析の方法**	**最終処理**	**サイバー犯罪情報の共有**	**管理フレームワーク**
法令等	道具	破壊	反社会的	ハッカー	攻撃	標的の決定	インターネット	偶発的なもの	OSINT	自動	収集	組織	分類	戦略および統制
管轄権および政策・方針等	攻撃対象	妨害	搾取型	サービスプロバイダ	事前調査	アクセスの提供	ディープウェブ	標的型	PROPINT	手作業	集約	コミュニケーション	権限	企画立案および予算編成
ベストプラクティス	かく乱	窃盗 / 詐欺	破壊型	サービス登録者（利用者）	不正アクセス	列挙	ダークウェブ	進化型	各種フォーラム	手順	関連付け	技術的な修正	通知	人事
		スパイ	無政府主義者	犯罪行為者	脆弱性攻撃 / 攻撃成功	サービスの決定	ソーシャルメディア	金融・金銭面	ボットネットコントロールパネル	標的別の要件	データモデリング	手続きによる修正	場所	パフォーマンスの管理
			窃盗 / 詐欺			サービスの管理	従来型メディア	ブランド面	ネットワーク	分類別の要件	ETL			人材の管理
			スパイ			サービスの維持 / 防御	犯罪ネットワーク	業務面	ホスト		データ品質			ツールの管理
						サービスの冗長化	システム	従業員	サービス		自動			
						難読化	従業員	公的組織			品質保証 / 品質管理			
						代替サービス	コミュニケーション	民間組織			分析			
						目標の達成					解釈			
											第二者による調査・検証			

第1章

サイバー犯罪とその捜査

はじめに

犯罪は常に社会の一要素である。犯罪はさまざまな理由で行われ、関連する目的を支援するために行われることもある。犯罪行為の影響は、妥当な罰則に値すると社会によって解釈される。

犯罪は、活動を容易にするためにツールを利用する人間によって行われる。サイバー犯罪は、その目的でコンピュータを使用する人間によって行われる。

企業がネットワークやインターネットで接続される以前は、侵入はハンマーやピッキング、盗まれたバッジや警報システムのコード、または割れた窓によって行われていた。今日の企業侵入者は、スピアフィッシングメール、ウェブサービスへのSQLインジェクション攻撃、ソーシャルエンジニアリング手法を使用する。不法侵入という意味では犯罪は同じだが、その目的を達成するために使われるツールが違う。結局のところ、犯罪は人間によって行われるものである。

2014年以降、サイバー犯罪は進化したが、依然として被害者を犠牲にして犯罪者に利益をもたらす客観的な結果を達成することを意図していることには変わりはない。これらの犯罪は、個人情報や財務データなどの機密情報の盗難から、コンピュータシステム（およびデータ）の妨害や破壊まで多岐にわたる。

今日のデジタル時代には、あらゆる規模の企業がサイバー犯罪の被害に遭う危険にさらされている。全米中小企業協会が2013年に実施した調査によると、中小企業の44%がサイバー攻撃を経験しており、これらの攻撃による平均コストは1件あたり9,000ドルだった[1]。2016年までにその数字は50%に上昇し、被害を受けた企業の60%がその後に廃業した。2023年現在、データ侵害1件あたりの世界の平均コストは445万米ドルだった[2]。

企業が心配しなければならないのは金銭的な損失だけではない。サイバー犯罪は企業の評判を傷つけ、顧客の信頼を損なう可能性もある。サイバー犯罪は、システムや人に対して物理的な損害をもたらす可能性もある。アメリカの病院に対するランサムウェア攻撃に関する2023年の調査[3]では、2016年から2021年の間に、これらの攻撃による被害のゆえに最大67人のメディケア患者が死亡したことが示唆された。これは、企業がサイバー脅威から身を守るための対策を講じることがなぜそれほど重要なのかを冷静に思い出させるものである。

教育と啓発はサイバー犯罪から身を守るための重要な対策である。企業は自社の利益を守るためにこれらを優先しなければならない。企業は従業員に対し、「最善の」セキュリティ慣行だけでなく、何がサイバー犯罪を構成するかについても教育すべきである。これには、フィッシングメールやマルウェア攻撃などの潜在的なリスクを強調し、従業員がサイバー犯罪を特定して防止できるように、これらのタイプのサイバー犯罪の例を示すことも含む。進化するサイバー脅威に先手を打つために、企業がセキュリティプロトコルやシステムを定期的に見直して更新することも重要である。

サイバー犯罪を防止するためのもう一つの重要な側面は、企業内にサイバーセキュリティの文化を作り出すことである。これは、すべての従業員が会社の（依存する）テクノロジーと関連情報のセキュリティを維持する責任を負うという考え方を育成することを意味する。

本章では、サイバー犯罪に関連する法的原則と、サイバー犯罪がどのように定義され、捜査され、訴追されるのかを探る。また、調査および起訴の方法に影響を与える自己統治の問題や管轄権の指針（お

1 https://www.prnewswire.com/news-releases/nsba-economic-report-small-business-outlook-vastly-improved-300037112.html

2 https://www.statista.com/statistics/987474/global-average-cost-data-breach/

3 McGlave、Claire、Neprash、Hannah、Nikpay、Sayeh、「ハッキングで粉々に?ランサムウェア攻撃が病院と患者に与える影響」（2023年10月4日）。SSRNを参照。https://ssrn.com/abstract=4579292またはhttp://dx.doi.org/10.2139/ssrn.4579292

よび制約）についても検討する。実行者がプログラムとポリシーを適用可能なフレームワークに合わせることができるように、組織および調査機関の役割と責任が説明される。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- 法廷や法令における「サイバー犯罪」の定義とは
- サイバー犯罪捜査を管轄するのはだれか
- 2013 年以降に制定されたサイバー犯罪法とは
- サイバー犯罪捜査における「ベストプラクティス」とは

サイバー犯罪とその捜査におけるトピックス分類

「サイバー犯罪とその捜査」知識領域におけるトピックスの分類を図 1-1 に示す。

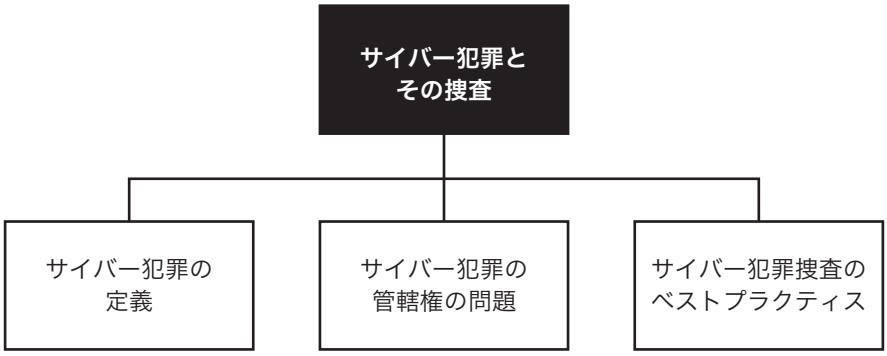


図 1-1.「サイバー犯罪とその捜査」知識領域におけるトピックスの分類

サイバー犯罪の定義

現在の（一般的な）定義では、サイバー犯罪を定義する 2 つの大きなカテゴリがある[4]。コンピュータを犯罪の道具または手段として扱うカテゴリと、コンピュータや電子的資産を犯罪の標的または被害者として扱うカテゴリである。最初のカテゴリでは、コンピュータ（またはコンピューティング技術）は、犯罪者が犯罪行為を実行できるようにするツールまたは手段である。例えば、児童虐待者はコンピュータを使用して、虐待しようとしている幼い被害者を特定、追跡、および誘い込むかもしれず、泥棒はコンピュータを使用して銀行口座にアクセスし、資金を不正に送金するかもしれず、悪質な競合他社はコンピュータを使用して、他者の保護された機密ビジネス情報を盗むかもしれない。逆に、銀行はしばしば「分散型サービス拒否」（DDos）攻撃を受け、顧客サービス機能が中断され、ビジネスが影響を受ける。このタイプの攻撃は、コンピュータや電子的資産が標的となっていることを反映している。

4　世界中の多くの法執行機関は、カナダ王立騎馬警察と同様の方法でサイバー犯罪を定義している。http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canadaの“Defining Cybercrime from a Law Enforcement Perspective”（法執行機関の観点から見たサイバー犯罪の定義）を参照。

最近登場した関連する第3のカテゴリは、コンピュータが捜査官を犯罪の実際の真の目的から目をそらすための仕掛けや、証拠を改竄する手段として利用されるケースである。これは依然としてコンピュータをツールとして使用することを意味するが、場合によっては、標的のコンピュータや電子的資産に偶然に損害を与えることもある。例えば、攻撃者は、金融マネジメントシステムを標的にして電信送金詐欺を実行する目的で組織のコンピュータネットワークにアクセスするが、活動の過程で、調査員や対応者が他の活動の分析に集中できないようにするために、ネットワーク内の他のコンピュータにランサムウェアを展開するかもしれない。

犯罪の道具としての技術

私たちの日常生活、金融関係の手続き、ビジネスライフのあらゆる側面でコンピュータ、モバイルデバイス、自動化テクノロジーがますます使用されるようになるにつれ、これらのテクノロジーが使用される犯罪の数も増え続けている。今日では、犯罪を実行するために必要な人物や情報にアクセスするには、コンピュータを使うのが最も効率的な手段であることが多い。また、オンラインや仮想サービスなどの電子ツールを通じて犯罪を行うことで、犯人は (1) 地理的範囲、(2) スピード、(3) 匿名性という付加利益を得ることができる。これらの利点は犯罪者にとって有利であるが、被害者や法執行機関にとってはさらなる課題をもたらす。以下にそれらの例を示す。

(1) 地理的に広範囲な犯行

ネットワークとサイバー空間は、犯罪者が世界中の遠隔地から被害者や情報にアクセスして世界規模で犯罪を行うのを可能にする。これには、被害者や法執行機関の手が届きにくい世界の地域から犯罪を行う能力が含まれる。その結果、被害企業、法執行機関および政府は、地理的境界を越えたサイバー犯罪の捜査と対処のために国際的な関係と手順を確立しなければならない。この分野では過去10年間に大きな進歩があったが、各国の多様な法律や法的枠組み、サイバーセキュリティ問題に関する成熟度や理解度の差、犯罪に対処する独自の方法などをよりよく調整し理解するためには、まだ多くの課題が残っている。これについては、本書で論じられているように、サイバー犯罪とサイバー犯罪者を検出、捜査、起訴するための思慮深い対応計画と効率的かつ効果的な国際調整チャネルを開発する必要がある。

(2) 短期間のうちに実行される犯行

従来は相当な時間がかかった犯罪でも、現在はコンピュータとサイバー空間を使えばはるかに早く実行できるようになっている。実際、わずか数秒の間に、盗んだ金を電磁的に外国へ送金する、膨大な量のデータを取得または削除する、何百万枚もの違法な児童ポルノ画像を全世界に発信するといった犯行が可能である。このような高速で行われる犯罪過程においては、被害者や法執行機関は、サイバー犯罪がいつどのように発生し、どのように対応すべきかを迅速に特定して、機敏かつ迅速に対応する準備が求められる。したがって、サイバー犯罪捜査官と彼らが活動する組織や政府にとって、多種多様なサイバーインシデントを捜査するための効率的かつ効果的な手段を開発し、実践し、必要に応じて支援を求めることができる官民両セクターの専門家のネットワークを（事前に）構築することが不可欠である。

(3) 匿名による犯行

数秒から数分で世界中のどこからでも犯罪を実行し、被害者に接触し、情報にアクセスできることに加えて、サイバー犯罪者はコンピュータを使って自分の身元や所在地を容易に隠すことができ

る。これは、特定の犯罪行為を、その行為の責任者である個人、組織、および（場合によっては）国家に絞り込もうとするサイバー犯罪捜査官にとって、大きな問題を引き起こす。コンピュータを通じて個人の身元や所在地を隠す手段は長年にわたって発展しており、法執行機関が犯罪者を発見するための新しい改良された方法を開発する一方で、犯罪者が発見を逃れるための新しい手段を採用するというイタチごっこが生じている。さらに、コンピュータは、サイバー犯罪者が自分たちの身元を隠すだけでなく、法を遵守する国民、他の犯罪者、組織犯罪グループ、さらには他の政府などが犯罪行為に関与しているように見せかけて、法執行機関を欺くことも可能にする。このように、匿名性という概念はサイバー犯罪において常に存在するものであり、捜査官は、サイバー犯罪者の傾向や慣行に関する技術的な洗練度を維持すること、サイバー犯罪の最新の手法や手段を常に把握すること、技術的な捜査手段と従来の捜査手段の両方を適宜用いて、さまざまな角度から犯罪行為を捜査することが求められる。

サイバー犯罪者にとってこのような利点があり、法執行機関にとって課題があることを考えれば、コンピュータを道具とする犯罪が急増しているのは驚くべきことではない。例えば、日本の警察庁は、「2015 年 3 月のオンライン犯罪の可能性に関する問い合わせは前年比で約 40% 増加し」、また「2014 年の違法なオンライン銀行送金による金銭的被害はおよそ 29 億円または 2400 万米ドルに達した」[5] と報告した。米国司法省は、「サイバー犯罪はわが国が直面する最大の脅威のひとつであり、国家安全保障、経済的繁栄、公共の安全に多大な影響を及ぼす。テクノロジーの進化と同様に、法執行機関にとっての脅威の範囲と課題も急速に拡大している」[6] と報告している。ある調査によると、2015 年に米国の調査対象組織が被ったサイバー犯罪の年間平均コストは 1,500 万ドルで、2014 年の 1,270 万ドルから増加した。[7] 同調査によると、2015 年に組織が被ったサイバー犯罪の世界的なコストは 770 万ドルで、コストが最も高かったのは米国、ドイツ、日本の順だった。[8] ユーロポールは最近「サイバー犯罪はより攻撃的で対立的になっている」と報告した。サイバー犯罪問題はヨーロッパだけでなく世界中で拡大し続けている。[9]

興味深いことに、サイバー犯罪の世界的地理をマッピングした 2024 年の調査 [10]（サイバー犯罪情報および捜査の専門家の調査に基づく）では、多くの国にサイバー犯罪者がいる一方で、サイバー犯罪の地理を影響（犯罪の発生と影響、および攻撃者の専門性と技術力）の観点から示す「サイバー犯罪指数」で測定したところ、比較的少数の国にサイバー犯罪の脅威（活動と犯罪者）の大部分が集中していることがわかった。ロシア、ウクライナ、中国、米国、ナイジェリアなど、一握りの国々が、世界に大きな影響を与えるサイバー犯罪の脅威の大部分を占めている。図 1-2 は、指数にマッピングされた国を示している。

5　トレンドマイクロの「日本のアンダーグラウンド」レポート、p.4（US$1＝119.74円の為替レートを使用）※要Update。http://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdfを参照。
6　国司法省のウェブサイト。https://www.justice.gov/usao/priority-areas/cyber-crimeを参照。
7　Ponemon Institute、「2015年サイバー犯罪コスト調査:米国」、2015年10月9日、http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-statesを参照。
8　Ashley Carman、「調査:サイバー犯罪の平均コストが2015年に再び上昇し、770万ドルに」、SC Magazine。http://www.scmagazine.com/ponemon-and-hp-release-annual-cybercrime-cost-study/article/443433/を参照（Ponemon Instituteの調査を引用）。
9　ユーロポール、インターネット組織犯罪脅威評価（IoCTA）2015、ユーロポールの欧州サイバー犯罪センター（EC3）による。https://www.europol.europa.eu/IoCta/2015/overview.htmlを参照。
10　https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312

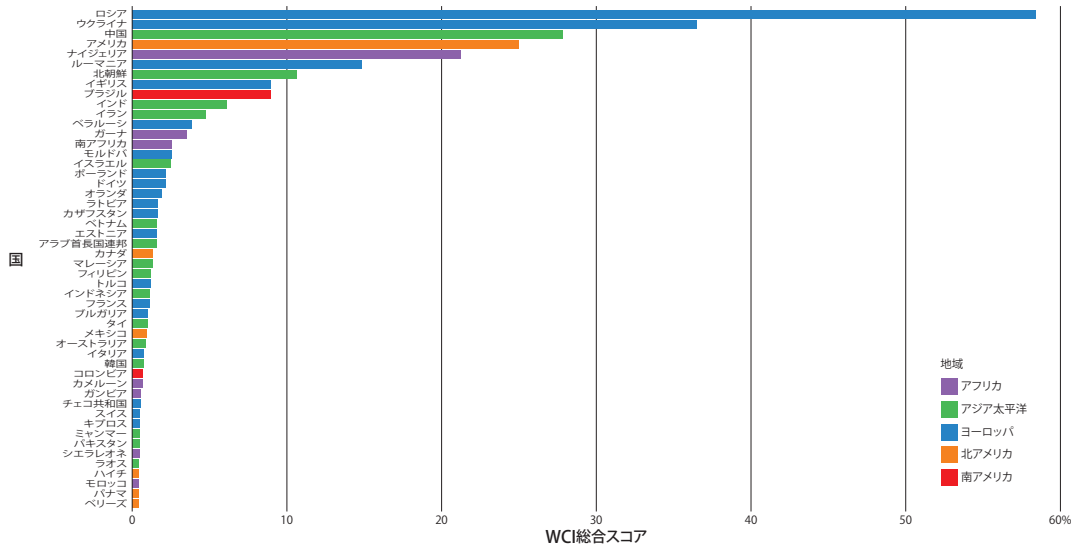


図 1-2. 世界サイバー犯罪指数を用いたサイバー犯罪の地理的分布のマッピング

サイバー犯罪は違法薬物取引よりも利益が大きいとみなされており、[11] インターネットを利用する人が増えるにつれて、日本やその他の国々を含めて世界中で拡大し続けると予想されている。[12] コンピュータが犯罪の道具となるこのカテゴリのサイバー犯罪では、多くの場合、犯人が高度な技術的スキルや知識を持っている必要はない。しかし、本書で解説されているように、コンピュータを利用した犯罪の捜査方法や対応方法をしっかりと理解することで、法執行機関や被害者たりえる企業や組織は、サイバー犯罪者を特定し、捜査し、阻止する場合に有利になる。

犯罪の攻撃対象としての技術

コンピュータまたは関連技術（個別にホストされているか、多数のコンピュータに分散されているアプリケーションサービスなど）が犯罪の標的または被害者である場合であり、通常、加害者側と犯罪を捜査する側の双方に、技術に関するより高度な知識が必要となる。このカテゴリは、システムのオペレーションを停止させたり動作を著しく低下させたりする DDoS 攻撃、コンピュータやシステムにマルウェアを感染させるネットワーク侵入、電子データを破損、削除、改ざんし、システムの運用を妨害するその他の手段など、コンピュータシステムそのものに対する攻撃を含む。

家庭内の温度調節から医療機器の機能、さらには国の水道や電力網、国際線のフライトパターンというような重要なインフラの運用まで、我々はあらゆる面でテクノロジーに依存し続けており、コンピュータを攻撃する犯罪の潜在的な範囲はより大規模なものになっている。さらに、これらの犯罪による潜在的な被害は今や壊滅的なものとなっている。このような犯罪は、単一のコンピュータに対する単独の行為者による個人攻撃から、組織的犯罪企業や敵対する国家によって実行される多国籍組織や国に対する大規模な脅威まで、多岐にわたる。これらの犯罪による潜在的な被害は、個人や企業に影響を与える些細な不便や「不具合」から、データの消失、公衆衛生や安全に対する重大な脅威、そして本格的なサイバー戦争にまで及ぶことがある。

国のインフラや企業運営のあらゆる側面を効率的にマネジメントするためのコンピューターへの依存

11　例えば、ロバート・デスレフス著、フォーチュン誌、2015年5月1日「サイバー攻撃が麻薬取引よりも利益を生むようになった理由」、http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/を参照。

12　例えば、トム・リーブ著、SC Magazine（英国）、2016年10月15日「サイバー犯罪被害の急増に直面する日本」http://www.scmagazineuk.com/japan-facing-explosion-in-cyber-crime-claims-report/article/446174/.を参照。また、トレンドマイクロの「日本のアンダーグラウンド」レポートについて論じているhttp://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdfを参照。

が拡大していることを考慮すると、この分野のサイバー犯罪は今後も飛躍的に増加する可能性が高い。例えば、サイバー犯罪者は「ランサムウェア」を使用してコンピュータシステムへの攻撃をますます多く仕掛けるようになっており、システムや電子データを「人質」に取って、「身代金」または金銭の支払いなしには元通りに利用できないような攻撃を仕掛けている。2015 年、米国連邦捜査局は、被害者に推定 2,400 万ドルの損害を与えたランサムウェア攻撃に関する 2,453 件の被害報告を受けた。[13] ランサムウェアによる攻撃は日本でも著しく増加している。トレンドマイクロの報告によると、2015 年に日本企業から報告されたランサムウェア感染件数は 650 件で、これは 2014 年に報告されたランサムウェア攻撃件数の 16 倍以上であり、2016 年の最初の 3ヶ月間だけで、日本企業はすでに 740 件のランサムウェアを報告しており、この問題が拡大し続けていることを示している。[14] ランサムウェアの問題は、ヨーロッパやその他の地域でも広がっている。4 カ国の 500 社を対象としたある調査によると、2015 年には約 40% の企業がランサムウェアの標的になり、調査対象となった英国企業全体の 54% が標的になったことが示された。[15]

IoT（Internet of Things）の進化により、コンピュータを狙った犯罪も増加し続けると予想され、それにより、拡大する接続デバイスのネットワークを通じてテクノロジーが私たちの生活のあらゆる側面に浸透し、（さまざまな程度で）自律的なコンピュータ機能が多くの日常生活に影響を与えている。例えば、家庭内の空調やセキュリティ、自動車の機能や特徴、家電製品、スマートフォンやその他のポータブルデバイス、健康関連のデバイスや機器などが犯罪のターゲットにされ得る。[16] これらの犯罪の潜在的な範囲、被害、複雑さを考慮し、コンピュータシステムを標的としたサイバー犯罪を防止、検出、起訴する方法をしっかりと理解することが不可欠である。

犯罪から目をそらす手段としての技術

前述のように、テクノロジーは犯罪の道具として、あるいは犯罪の標的として使われるだけでなく、偶然にも両方の目的で使用されることもある。複雑な犯罪の中には、証拠を隠蔽したり捜査を混乱させるために「偽旗（false flag）」や注意をそらす手法が用いられる場合もある。より伝統的な（サイバーではない）犯罪では、宝石店強盗から捜査員の注意をそらすために、犯罪者が犯行現場とは別の場所にある高校に火を放つようなものである。

コンピュータが犯罪の妨害手段として使用される場合、犯罪者は通常は最初に標的の環境を調査して、単純なコンピュータ犯罪に対してターゲットとなる組織による事案対処能力を推し量る。場合によっては、事前調査をせず、単純にかく乱と目的の攻撃行動を同時に起こすこともある。どちらの場合であれ、サイバー犯罪者は、組織のコンピュータシステムやアプリケーションの窃盗、破壊、妨害など、標的とする目的とは無関係のツールを展開したり、コンピュータを攻撃したりすることで、自分たちの活動を偽装しようとする。このような場合、コンピュータへの侵入や操作（あるいは破壊）の明白な証拠があるために、マルウェアを使わずに行われた認証情報やコンピュータの不正利用といった、より捉えにくい証拠を見落としやすくなる。また、目くらましのためによく利用されるものとは全く無関係なツールを

13 David FitzpatrickおよびDrew Griffin、「ランサムウェア犯罪の波が拡大」、2016年4月4日、CNN、http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/を参照。

14 Shusuke Murai、「ランサムウェアが日本のオンライン環境に多大な損害をもたらす」、The Japan Times、2016年6月6日、http://www.japantimes.co.jp/news/2016/06/06/reference/ransomware-making-costly-inroads-into-online-japan/#.V8mgEztrrwwを参照（トレンドマイクロのレポートを引用）。

15 Alex Hern、「ランサムウェアの脅威が増加、企業の約40%が攻撃を受ける」、The Guardian、2016年8月3日、https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attackedを参照。

16 「モノのインターネット」（IoT:Internet of Things）は、インターネット対応デバイスの進化するネットワークであり、相互に通信し、日常生活に影響を与えるさまざまな方法で電子的に機能する。現在、多くのデバイスが存在し、急速に拡大しているこの分野ではさらに多くのデバイスが開発されている。

使用することもある。実際、「目立つもの」は目立たないものよりも捜査されることが多く、犯罪者はこれを利用するのである。したがって、サイバー犯罪を捜査する際には、犯罪の動機と目的を検証し、入手可能なすべての証拠を客観的に検討することが極めて重要である。

コンピュータ犯罪を規定する法律

コンピュータ関連の犯罪行為を定義し、捜査し、起訴する際には、従来の刑法だけでなく、コンピュータ特有の法律も考慮して、これらの法律が手近な行為に適用されるかどうか、またどのように適用されるかを判断することが有益である。これは、テクノロジーをツールとして使って行われる犯罪と、テクノロジーが具体的な標的となる犯罪の両方に当てはまる。例えば、窃盗、銀行詐欺、通信詐欺、児童搾取、知的財産の保護、およびその他の犯罪に関する国または地域の刑法の法律は、コンピュータ関連の犯罪にも適用されることが多い。これらの法律の多くは、コンピュータが存在するはるか以前に制定されたものであるが、その他の法律も制定され、一部は改正され、これらの長年にわたる法律に対するコンピュータ関連の違反を明示的に想定した特定の条項が含まれている。

さらに、日本や米国を含む多くの国では、コンピュータへの不正アクセスを規制する特定の法律を制定している。[17] 例えば、日本では、1999 年に制定されて 2000 年から施行されている「不正アクセス禁止法」（法律第 128 号）は、不正のコンピュータアクセスを犯罪としており、最高 1 年の懲役および最高 50 万円の罰金を規定している。[18] 米国では、「コンピュータ不正行為防止法」（アメリカ合衆国法典第 18 編、第 1030 条）が、コンピュータへの不正アクセスを犯罪として取り締まり、最高 1 年の禁固刑（軽犯罪）から無期懲役（故意にコンピュータに損害を与え、死に至らしめた場合）までの刑罰を科す。[19] イギリス、ドイツ、シンガポールなどの政府も、独自のコンピュータ不正使用法を制定している。[20] しかし、コンピュータに特化した法律を制定する際の課題のひとつは、技術も人々の使い方も急速に変化することである。また、サイバー犯罪の種類と範囲、そしてそれらの犯罪による潜在的な被害は、法律が改正されるよりもはるかに速いスピードで広がり続けている。このため、コンピュータに特化した法律は、制定後すぐに時代遅れにならないよう、十分な柔軟性と適応性を備えていることが重要である。

●多様な視点

サイバー犯罪の捜査において、発生した行為を定義しようとする際には、デジタルデータおよび情報のフォレンジック分析を含む技術的なコンピュータベースのアプローチと、関係者への聞き取り調査、文書・通信・銀行記録、またはその他の関連データの確認を含むより伝統的な捜査アプローチの両方を組み合わせて証拠を収集することが最も効果的である。証拠がどのように明らかになるかに応じて、捜査官と検察官は、起訴すべき適用法令に関して偏見を持たないようにすべきである。彼らは、事件の証

17 不正アクセス禁止法、1999年法律第128号、http://www.cybercrimelaw.net/Japan.htmlを参照。例えば、Takato Natsui「日本におけるサイバー犯罪:最近の事例、立法上の問題および展望、2003年」、http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdfを参照。Ryan Handerhan「日本とアメリカのコンピュータ犯罪政策」、2010年、http://repository.cmu.edu/cgi/viewcontent.cgi?article=1067&context=hsshonorsを参照。

18 日本の不正アクセス禁止法の英語の暫定翻訳については、http://www.cyberlawdb.com/gcld/wp-content/uploads/2010/04/computer_access.pdfを参照。

19 米国コンピュータ詐欺および濫用防止法（合衆国法典第18編、第1030条）の本文については、https://www.law.cornell.edu/uscode/text/18/1030を参照。この法律および関連する米国法の説明は、Charles Doyle、議会調査局、「サイバー犯罪:合衆国法典第18編第1030条および関連する連邦刑法の概要」、2014年10月15日、https://www.fas.org/sgp/crs/misc/RS20830.pdfを参照。

20 例えば、Clemens Louis、「Comparison of Computer Misuse Acts Around the World」（英国、ドイツ、シンガポールのコンピュータ不正使用法の比較）http://www.rechtsanwalt-louis.de/european_computer_misuse_acts.htmを参照。Michela Menting, "Cybercrime Laws by Country and Other Resources,"（国別のサイバー犯罪法とその他のリソース）2011年10月、http://www.academia.edu/1125166/Cybercrime_Laws_By_Country_and_Other_Resources_DOC.を参照。

拠に基づいて、従来の刑法、コンピュータ犯罪に特化した法律、または従来の法律とコンピュータに特化した法律の両方の組み合わせのどれが最も効果的で適切であるかを検討すべきである。この分析を行う際には、検察官は、起訴された法律に応じて適用される可能性のある罰則も考慮する必要がある。

例えば、犯人は銀行のコンピュータ システムに不法にアクセスして銀行から資金を流用し、犯罪を隠蔽するために銀行記録を操作するかもしれない。これは、保護されたコンピュータへの不法アクセスを犯罪とするコンピュータ特有の法律に該当する場合がある。またこの行為には、窃盗や詐欺に適用される法律が適用される可能性もある。さらに、銀行詐欺を規定する法律が同様に適用される場合、行為に対する刑罰がより重くなる（陪審員への説明も簡潔になる）可能性がある。また、国の法律によっては、捜査官や検察官が犯罪行為を窃盗、詐欺、不法なコンピュータ侵入として、またはこれら３つすべてとして定義することで、どのような証拠を収集できるか、どのような手段（盗聴など）で収集できるか、他の司法管轄区から関連する可能性のある証拠を入手できるか、裁判でどのような証拠を提出できるか、などが変わってくる場合がある。また、犯罪行為を起訴するために使用される法律は、被告人が他の司法管轄区で逮捕され、そこから引き渡されるかどうか（および引き渡しの方法）に影響する可能性がある。国によっては、伝統的な刑法犯罪に基づいて被告人を引き渡すが、認知度の低いコンピュータ特有の犯罪については引き渡さない場合もある。

さらに、サイバー犯罪は法廷においては新しい分野であり、関連する技術的背景や理解も大きく異なるため、起訴される特定の刑法に直接適用されるように、何が、どのように、誰によって起きたかを具体的に定義する明確な方法で犯罪と証拠を説明することが重要である。この場合、犯罪を実行する際に使用される専門用語や手順を、裁判官または陪審員（職業裁判官であれ、裁判員制度下の一般裁判員であれ）が理解できる方法で定義することがしばしば必要になる。したがって、サイバー犯罪を定義し、被告人を起訴するために最も適切な法律を選択することに加えて、犯罪行為、コンピュータ特有の方法、犯罪を実行するために使用された手段、さらには被告人の犯人としての身元を確立することなどを、さまざまなレベルの技術的知識を持つ人々が理解できる方法で十分に説明することも重要である。

サイバー犯罪の管轄権の問題

サイバー犯罪は、その国の一般的な刑法、コンピュータに特化した法律、またはその両方の組み合わせに基づいて起訴される可能性があるが、複雑な管轄権の問題がしばしば存在する。というのも、サイバー犯罪に関しては、加害者、被害者、犯罪行為の発生場所が地理的な境界を超えることが多いからである。また、サイバー犯罪や関連行為を規制すべきかどうか、どのように規制すべきか、どの程度まで規制すべきかについても、多くの国で見解が異なっている。例えば、ある国では特定の活動がサイバー犯罪に該当する可能性がある一方で、別の州では同じ行為が刑事違反に該当しないということがある。この例としては、ネットいじめ、リベンジポルノ、知的財産の盗難といった新たな状況が挙げられる。さらに、刑事事件における証拠の収集、使用、保存に関する国内法令や手続きはしばしば異なる。もう一つの重大な問題は、サイバー犯罪者がしばしば迅速に行動し、証拠がすぐに消えてしまう一方で、どのような情報をどのような手段で共有できるか、また各国の法執行機関がどのように協力するのが最善なのかが明確ではないために、国際的な捜査が遅れがちになるということである。

国家または地方自治政府が犯罪または犯罪者に対して管轄権を持つかどうかを判断するには、さまざまな基準が考えられる。これらには、犯罪が行われた場所、加害者の国籍、被害者の国籍、犯罪によって影響を受けた包括的な国家的または国際的利益、あるいは被告人が現在どこにいるかを考慮するもの

が含まれる。[21] しかし、サイバー犯罪の状況では、「どこで」犯罪が行われたかを定義することさえかなり難しい場合がある。それは、加害者の１人または複数が犯罪を実行した際に物理的に所在していた場所、被害者または犠牲者が所在していた場所、アクセスされたコンピュータシステムや情報が所在していた場所、またはこれらすべての潜在的な管轄区域である可能性がある。サイバー犯罪は世界各地で行われることが多いため、複数の司法管轄区が犯罪行為に管轄権を持つことは珍しくない。また、何がどのように起こったかを判断するために必要な証拠が、複数の司法管轄区に存在することも珍しくない。

最初の問題として、サイバー犯罪では、犯人の身元と居場所を特定することが著しく困難な場合がある。インターネットの大きな利点は、プライバシーや表現の自由を妨げることのない匿名性を生み出すということである。しかし、その匿名性には潜在的なリスクが伴う。特に、犯罪行為者がだれなのか、そしてどこにいるのかを突き止めるのが難しくなるため、犯罪者はその匿名性を利用して、捕らえられることなく犯行を行えると考えている。

かつて、銀行強盗は襲う銀行に赴き、その所在地からバッグに詰めた有形の資金を移動していたため、銀行がある街やその周辺から捜査を開始するのは理にかなっていた。今や、銀行のコンピュータシステムは世界中のどこからでもアクセス可能であり、資金移動やデータへのアクセスは数秒以内に行われ、侵入から数分以内にデータを世界中に転送し、転売することができる。サイバー犯罪に対処するには、被害者、法執行機関、検察官による、さらに機敏で洗練された対応が必要になっている。侵入やその他のコンピュータ犯罪が発生したことを被害者または法執行機関が早く検知して報告し、法執行機関と被害者が協力して何がどのようにして盗まれたのかを迅速に特定できれば、犯人を特定して犯罪による被害を軽減できる可能性が高くなる。

さらに、被害を受けた企業や組織、行政機関でサイバー犯罪を捜査する者は、犯罪者がしばしばサイバー空間内での自分の実際の居場所を特定しにくくする手段を取ることに留意しなければならない。例えば、犯罪者は、犯罪者のコンピュータから直接銀行のシステムを攻撃するのではなく、まず１つ以上の他のコンピュータシステムに（違法にまたはその他の方法で）アクセスし、それらのシステムを介して悪質な犯罪トラフィックを送って、自分の位置を隠すことがある。他のコンピュータシステムを介したこれらの「ホップと呼ばれる犯罪行為の中継」は複数の国で発生する可能性があり、その結果、検出、逮捕、管轄権の決定がさらに困難になる。さらに、サイバー犯罪者はコンピュータシステムにしばらく留まり、そのシステムにマルウェアを感染させて目的のデータにアクセスする手段を調べ、侵入の痕跡を完全に隠し、どのデータが取得されたのか、どのように取得されたのかを隠蔽する方法で最も効果的に情報や資金を得ることがよくある。これにより、事件に対応する法執行機関にはさらなる課題が生じることになる。というのも、真の犯人がどこにいるのかを理解し、発生した行為を完全に把握するには、時間、労力、そして高度な知識が必要となる場合があるからである。

サイバー犯罪は複雑なため、多くのサイバー犯罪の複雑な管轄権の問題と国際的な性質を理解することが重要である。また、捜査官は、管轄権の障害が存在するにもかかわらず、サイバーインシデントに最善の対応をするために、何がどこで起こったのかを最もよく理解するための技術的な手がかりを探すこと（第５章で解説）および利用可能な国際協力および情報共有の手段にアクセスする方法を知ること（第９章で解説）が重要である。

サイバー犯罪に関する条約

サイバー犯罪に対処するための共通の国際刑事政策を見つける取り組みの一環として、欧州評議会は2001年に、日本、米国、カナダ、南アフリカの積極的な参加を得て、ブダペスト条約としても知られ

21　例えば、Armando Cottim、「サイバー犯罪、サイバーテロ、管轄権:サイバー犯罪に関するCOE条約第22条の分析」、ヨーロッパ法学ジャーナル、http://www.ejls.eu/6/78UK.htm（さまざまな管轄権理論について議論）を参照。

る「サイバー犯罪に関する条約」を策定した。米国と日本はそれぞれ2006年と2012年にこの条約を批准し、この条約は米国では2007年、日本では2012年に発効した。[22] 2024年6月現在、72か国がこの条約を批准しており、さらに2か国が署名しているが、まだ批准には至っていない。[23] この条約は、コンピュータ関連の詐欺、著作権侵害、児童ポルノ、ヘイトクライム、ネットワークセキュリティ違反に特に焦点を当てている。参加国は、サイバー空間の状況を含むこうした行為を犯罪とする国内法を制定することに合意している。この条約はまた、コンピュータ関連の証拠を入手し、保存し、サイバー犯罪の捜査と訴追を支援するための国際協力を強化するための枠組みを設定することを目指している。

この条約は画期的なものであり、増大するサイバー犯罪の脅威に対処するために各国がより統一された解決策を模索するために結集した代表的な例であると考えられた。しかし、この条約の有効性には限界がある。それは、サイバー犯罪とその被害を特定し、調査し、対処するためには各国と被害者の独自の内部プロセス、立場、法律、専門知識をさらによく理解する必要があるためである。例えば、プライバシー保護の範囲や、それがコンピュータを使用した潜在的な犯罪に関する証拠を収集する方法や手段を決定するために捜査官が講じることができる措置にどのような影響を与えるかなどについては、国内および各国間では依然として多くの異なる見解が残っている。また、サイバー犯罪に対処するために利用可能な潜在的な法律に関する教育と理解を深める必要もある。さらに、コンピュータを犯罪の手段や標的として利用する行為を定義するための、現在の状況に即した柔軟な法律が不足しており、このことが各管轄区域にわたるサイバー犯罪の定義と対処における課題を生み出している。

MLAT

サイバー犯罪捜査における国際的な証拠収集に影響を与える管轄権の問題に対処するもう一つの方法は、相互刑事援助条約（MLAT）を利用することである。MLATは、サイバー犯罪やその他の犯罪の捜査における国境を越えた協力を可能にするために、多くの国の間に存在する。MLATにより、検察官は刑事事件で使用するために他国の検察官に情報を要求して入手することが可能になる。しかし、大きな障害の1つは、MLATSを使用して証拠を収集するには時間がかかり、場合によっては完了までに何年もかかることである。サイバー犯罪とサイバー犯罪者の素早い行動を考えると、MLATに従って情報を入手するための官僚的な手続きが取られる前に、証拠と犯人はすでに消えてなくなっている場合が多い。しかし、サイバー犯罪捜査に関しては、特定の国の間では大きな改善が見られ、MLATプロセスを通じてより正式に情報が提供される前の第一歩として、非公式な形で情報を保存し共有することが可能になった。

外交的手法

サイバー犯罪によって影響を受けることが多い複雑な国際問題を踏まえると、サイバー犯罪に対する国際的な対応を可能にするための外交手段を理解することも重要である。企業がサイバー被害とその対策について認識を深めるにつれ、外交的な協議や協力のチャネルが強化されるようになる。この分野での成功の良い例は、2012年にDDoS攻撃を通じて金融機関を狙ったサイバー犯罪に対する国際的な対応である。いくつかの国が関与する国際的な協力を通じて、政府代表者は外交交渉に従事し、公共および民間のセクターは技術的および法的協力を受け入れて、攻撃が行われたインターネットのノードやアク

22 欧州評議会のウェブサイト、サイバー犯罪に関する条約、条約185、署名国リストのページ、http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signaturesを参照。
23 同上。

セスポイントを遮断することで攻撃を阻止するのに貢献した。[24]

規制

考慮すべきもう一つの管轄上の問題は、政府による各種規制と業界または企業の自主的なセキュリティガイドラインの両方の観点から見た規制の問題である。急速に進化するサイバーセキュリティの性質を考えると、適切な基準や十分なセキュリティのための枠組みをあまり具体的に特定することは現実的ではなく、多くの法域の法律は、この文脈で対処すべき問題に遅れをとっている。したがって、多くの管轄区域で規制当局がサイバーセキュリティを監督する役割を担っており、一部の業界では、犯罪攻撃に対して最も脆弱なシステムやデータを保護するために、業界固有の規制を導入している。また、サイバー攻撃の予防、検知、対応、被害軽減のための適切なセキュリティを確保するため、より高度な自己評価と自主規制を自ら行う企業も増えている。サイバー犯罪者から身を守るための適切なサイバーセキュリティの重要性について社会の知識が深まるにつれ、サイバー犯罪をより適切に定義し、国家的な規模および世界的な規模でサイバー犯罪を最も効果的に捜査および訴追する方法に関するさらなる指針を提供する法律や基準が今後も発展し続けると思われる。

CERT

管轄の障壁を越えて情報共有を改善し、さまざまな国の法執行機関が協力できるようにする取り組みの一環として、民間企業と政府の両方がサイバー犯罪に対処するための関係を築いてきた。これらには、日本、米国、EU、および世界各地に存在するコンピュータ緊急対応チーム調整センター（CERT）が含まれる。[25] さらにFBIは、サイバー犯罪に対応し、コミュニケーションおよび協力を促進するために、世界各国に法務担当官を配置している。本書で後述されているように、国際協力のための手段は他にも存在する。

図 1-3. サイバー犯罪ガバナンス

サイバー犯罪の管轄ガバナンスの相関関係を図1-3に示す。捜査の実施方法に関する組織の方針は、関連する要件に応じて適合させることができる。

24 http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdfサイバーセキュリティ情報の共有と連携の重要性と有効性、およびそのための効果的な手段について論じたJudith H. Germanoの「サイバーセキュリティ パートナーシップ、官民連携の新時代」、http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdfを参照。

25 たとえば、Japan CERTのウェブサイトの英語版、https://www.jpcert.or.jp/english/を参照。

サイバー犯罪捜査のベストプラクティス

サイバー犯罪の可能性がある事象が発生した際、最初にそれに気付くのは被害者、法執行機関、または第三者である。個人や企業の被害者が、システムが正常に作動していないこと、データや資金が紛失していること、子供が行方不明になっていることに気づくこともある。また、「ランサムウェア」を使用したサイバー犯罪の増加傾向に伴い、サイバー犯罪者がコンピュータまたはシステムを電子的に制御し、解除のために身代金を支払わない限り関連データを破壊するというメッセージを被害者が受け取る場合もある。その他の場合としては、企業の内部システム制御により、潜在的なサイバー犯罪が発生したことが企業に警告されることがある。これには、コンピュータシステム上の不審な動きを電子的に報告する技術的制御や、会社の情報を含んでいるノートパソコンの盗難を報告するための手順を従業員が知っていて、それに従うなどのガバナンス制御が含まれる場合がある。これらは、被害者がまず犯罪を察知し、その後、法執行機関に問題を報告するかどうか（およびどのように報告するか）を決定する犯罪のほんの一例である。

また、サイバー犯罪が発生したことをまだ知らない企業や個人に対する特定の攻撃に関する情報を法執行機関が受け取ることもあり、その場合、法執行機関は被害者に通知することがある。法執行機関は、業界における潜在的なサイバー犯罪の傾向に関する情報を受け取ったり入手したりして、企業の被害者に接触することがある。その他の場合として、法執行機関は、監視または別の調査で得られたデータに基づいて、企業がサイバー攻撃の被害を受けたと判断することもある。法執行機関にとって有益な情報源の１つは、児童に対する犯罪、クレジットカード詐欺、その他の金融犯罪、その他の犯罪に関与するサイバー犯罪者が使用する違法なチャットルームやウェブサイトを密かに監視することである。法執行機関にとってもう一つの有益な情報源は、外国の管轄区域にある他の法執行機関である。例えば、他の司法管轄区での無関係な調査によって、特定の町や国の特定の児童のビデオや画像が、小児性愛者が利用するピアツーピアネットワークで取引されていることが明らかになるかもしれない。国際的な調査により、システムを侵害したりデータを盗み出したりするために繰り返し使用されるコードや、法執行機関に知見を提供するその他の国際的な傾向や情報も明らかになっている。

サイバー犯罪を検知する第三の方法は、サイバー犯罪に関する情報や洞察を提供する第三者からの報告である。たとえば、クレジットカード処理会社は、被害を受けた同じ小売店で使用された一連のクレジットカードに関連する不正行為を検出する場合がある。友人や顧客が、個人または企業から送信されたと称する疑わしいメッセージを受け取ることがあるが、実際には、被害者のアカウントまたはシステムをハッキングしたサイバー犯罪者から送信されたものである。顧客は、企業のウェブサイトの特定の機能、または企業のオンラインシステムの公開されているその他の部分にアクセスする際に問題が発生する可能性がある。報道記者やその他の情報源は、特定の企業から違法に取得されたデータがインターネットのダークウェブ（違法取引や盗難データの闇市場の電子版）で提供されているという報告を見たり受け取ったりすることがある。企業のシステムに対する定期的な第三者によるフォレンジック調査により、システムが侵害されていることが検出される場合がある。民間企業または民間および公共のセクター部門の団体が参加する業界ベースの情報共有グループは、特定の管轄区域で発生したサイバー犯罪に関する関連情報を公開する場合がある。これらのグループの中には、個人的な人脈に基づく非公式の緩やかな結びつきの団体もあれば、本書で情報共有について後述するように（第９章）、より正式な会員制の団体もある。

これらは、サイバー犯罪を検知するさまざまな方法のほんの一例にすぎない。犯罪がどのように発覚するかにかかわらず、個人の被害者、その内部および外部の技術アドバイザーや法律アドバイザー、法執行機関の捜査官や検察官の間で強固で信頼できるコミュニケーションラインを確立することが重要で

ある。これは、犯罪行為が可能な限り早期に発見され、適切な人物または団体に報告され、被害者、その技術アドバイザー、専門アドバイザー、法執行機関といった関係者が、被害を予防、発見、軽減し、加害者を阻止するための行動をとるために十分な実践と知識を有することを保証するために必要である。

多くのサイバー犯罪は新しいものであり、進化しているため、サイバー犯罪が発生したときに何をすべきか、つまり、いつサイバー犯罪被害を誰に誰が報告すべきか、次に何が起こるかをより深く理解することは、多くの被害者と政府にとって依然として有益である。このような理解は、潜在的なサイバー犯罪被害者に対する教育と支援活動の改善に取り組む各国政府によって改善されてきた。また、被害者の側においても、発生した可能性のある脅威や被害に対処するために法執行機関と協力する利点に加え、サイバー犯罪の種類や潜在的な被害に関する知識と認識が深まり、状況は改善した。しかし、この分野ではやるべきことはまだ多い。

多面的なアプローチ

地域、地方、世界規模でのサイバー犯罪を最もよく理解して対応するには、官民両セクターが協力して取り組む多面的な取り組みが最善のアプローチであることを捜査官は認識しなければならない。多くの場合、特定のセクター内（およびもっと広い範囲）の企業は、被害を抑え、加害者を特定し、サイバー犯罪に対処するためのベストプラクティスを確立するために、互いに情報を共有することができる。これにより、潜在的な攻撃の手法や手段、システムを強化する最善の方法、サイバー犯罪を防止、検出、対応するための利用可能な防御策に関する認識を高めることができる。企業間や企業同士の協力に加え、情報共有や協力のための官民プログラムを通じてサイバー犯罪に対処することは、公式および非公式の関係レベルの両方において大きなメリットがある。

重要な第一歩として、多くの企業が企業全体のサイバーセキュリティ戦略を含むコーポレートガバナンスのシステムを確立し、強化している。サイバー攻撃のレベルが高まり、それが引き起こす重大な被害が拡大していること、また、サイバー犯罪を防止し訴追する政府の能力がある程度限られていることを認識すると、これは不可欠なものになっている。前述のように、サイバー犯罪が発生したと最初に認識・判断するのは被害企業であることが多い。というのは、多くの民間企業は、サイバー脅威を特定し、対処することができる、より大きなリソース、自社システムへの特定のアクセスとシステムそのものに対する理解を有しているからである。とは言え、政府は、潜在的なサイバー脅威や傾向に関する幅広い知識を頻繁に提供しており、サイバー犯罪に対処する上で貴重なアドバイザリーを提供している。政府はまた、捜索令状や押収令状、アドバイザリー、逮捕令状や起訴などを通じて、証拠を収集しサイバー犯罪者を特定するための積極的な手段を講じることもできるが、これらの対処方法はいずれも民間では利用できない。これらすべての視点とツールを組み合わせると、増大するサイバー犯罪の問題に対処する上で重要な役割を果たすことができる。

内部体制

企業内では、コンピュータシステムと情報のセキュリティと脆弱性に関する洞察力を持つ社内（および社外）の専門家と、企業内のリスクマネジメントの最終責任を負う上級マネジメント職との間で効果的なコラボレーションに基づく明確なコミュニケーションラインを確立することが重要である。長年にわたり、多くの企業の技術的側面やコンピュータ関連の脆弱性といった情報は、上級マネジメント職に直接報告する機会を持たない情報技術部門に委ねられていた。さらに、上級マネジメント職は、会社のデータやコンピュータシステムのセキュリティに関して関心や知識が不足していることがしばしばあった。サイバー犯罪とその潜在的な危害が大幅に増加するにつれて、多くの組織は、サイバーセキュリティに関する強力な社内企業ガバナンスシステムが重要であるだけでなく、組織の健全性、さらには存続に

とって不可欠であることを認識するようになった。サイバー犯罪が増加し、組織、その顧客、そして一般市民に対してすら壊滅的な影響を与える可能性があることを踏まえると、このような認識と、サイバーセキュリティに対処するための人的および予算の割り当てがますます必要になっている。したがって、組織のトップ意思決定者は、適切なシニアリーダーをアサインしサイバーセキュリティのリスクと対応を適切に認識し、対応できるようにしなければならない。

外部のリソース

組織内のコミュニケーションやガバナンス体制に加え、サイバー犯罪の検知や対応を支援する外部リソースやコミュニケーションチャネルを確立することも必要である。これには、会社の機能の定期的な監査を支援する外部のフォレンジック調査会社や法律の専門家などと関係を構築すること、経営層がサイバー脅威や傾向を十分に認識できるように定期的な最新情報やガイダンスを提供すること、侵害が発生した場合に（必要に応じて）支援することなどが含まれる。また、業界パートナー、分野特有の組織、政府リソース間で情報共有やサイバー犯罪対応のための関係を構築することも重要である。これらの関係については、本書の「解決」（第8章）と「情報共有」（第9章）の章で詳しく説明されている。[26]

26 http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdfサイバーセキュリティ情報の共有と連携の重要性と有効性、およびそのための効果的な手段について取り上げた、Judith H. Germanoの「サイバーセキュリティ パートナーシップ、官民連携の新時代」、http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdfも参照。

Chapter 1:CIBOK の分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

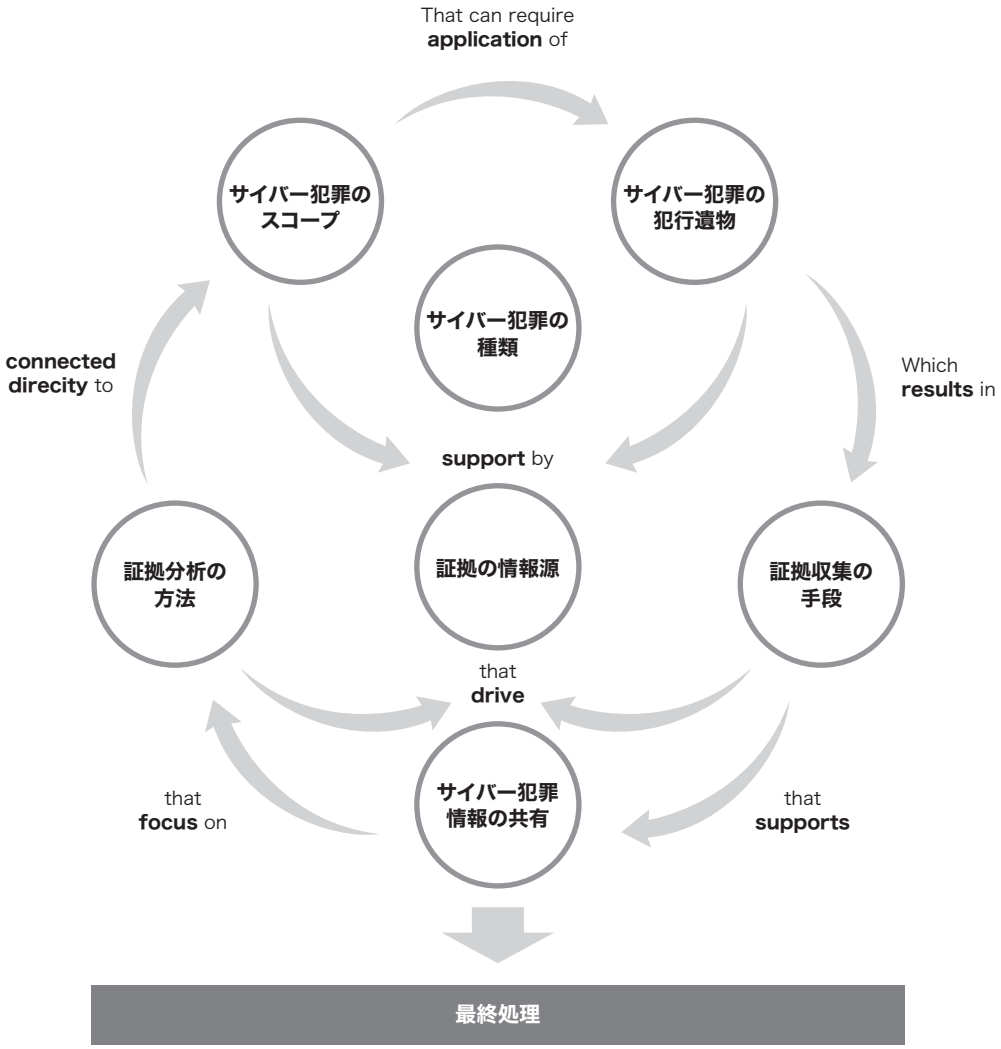


図 1-4. サイバー犯罪捜査における実行フレームワーク

実行フレームワークとスキルおよび知識の CIBOK 分類法（表 1-1）との関係は、機能要件が関連する役割によって異なることを示している。このフレームワークには、CIBOK で説明されている活動が含まれている。サイバー犯罪の種類を決定することから始まり、犯罪の範囲（被害者への影響）と、犯罪が何であったかを証拠資料から説明する成果物を詳述する。証拠がどのように収集されて分析されるかは、犯罪の範囲（と種類）の理解を深めるのに役立ち、情報源と収集・分析方法を組み合わせることは、情報の共有と事件の解決に役立つ。

これらの活動は、組織の CI 機能（サイバー犯罪調査・対応機能）を構成する特定の役割（幹部、情報、捜査、司法、広報、支援、事務）に関連している。

大規模な組織では、役割は個人またはチームに割り当てられ、小規模な（または発展途上の）組織では、そうした役割を外部組織にゆだねることができる（例えば、法執行機関における司法関係はリスクマネジメントまたは顧問弁護士の役割に組み合わされ、法執行機関のサイバー犯罪捜査チームは情報セキュリティマネジメント者の役割に組み合わされるなど）。このような、サイバー犯罪に対処するために必要となる組織の役割は、組織の戦略、戦術、および手続き上のマネジメント活動との関係で定義される。

表 1-1. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解が含まれる。捜査管理機能は関連情報の共有の承認を行い、サイバー犯罪の捜査における決定と、組織が防護体制を改善するためのリスクマネジメント手続きを監督する。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査管理の各役割にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。捜査の進み具合は利用可能な情報源から収集され、分析された知見に依存する。

調査 – 利用可能な情報源にあるアーティファクトや証拠を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。知見収集、説明責任、予防啓発、捜査管理の各機能にあ

る者が、サイバー犯罪の影響を識別するのを支援する。識別にあたっては、その犯罪に関連する目的の特性（および達成の段階）に対する評価を用いる。捜査の進め方は利用可能な証拠とその種類に依存する。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。知見の収集、捜査手続きに関する指導を行い、関連方針および法規制に基づいて分析結果を解釈して、捜査マネジメントや予防啓発の各機能を支援する。関係者による捜査の手段はこの指導に依存する。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。サイバー犯罪捜査の結果は被害者および類似の組織、個人におよぶ関連リスクを解決する機会を提供する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的および手続き的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第1章:レビュー

1. **法廷や法令における「サイバー犯罪」の定義とは**
   答え：コンピュータを使用して行われた犯罪。
   例：ツールとして、ターゲットとして、気をそらすものとしてのコンピュータ。

2. **サイバー犯罪捜査を管轄するのはだれか**
   答え：国際協定、交渉による協定、国内法。
   例：サイバー犯罪に関する条約（欧州評議会、条約 185）、相互刑事援助条約（MLAT：Mutual Legal Assistance Treaties）、米国コンピュータ詐欺および濫用防止法（CFAA：Computer Fraud and Abuse Act）。

3. **2013 年以降に制定されたサイバー犯罪法とは**
   答え：UNCTAD の報告書によると、2014 年時点で 117 か国がサイバー犯罪法を施行しており、そのうち 82 か国は発展途上国であった（出典：https://unctad.org/press-material/global-mapping-cyberlaws-reveals-significant-gaps-despite-progress）。
   例：
   - *米国サイバーセキュリティ情報共有法（CISA）：この法律は、米国政府と技術・製造企業の間でインターネットトラフィック情報を共有することを許可する。これは 2014 年 7 月 10 日に米国上院で提出され、2015 年 10 月 27 日に上院で可決された。*
   - *2014 年米国サイバーセキュリティ強化法：2014 年 12 月 18 日に法律として署名されたこの法律は、サイバーセキュリティを改善し、サイバーセキュリティ研究の人材育成と教育、および国*

民の意識と備えを強化するための継続的な自発的な官民パートナーシップを規定する。

- *2015 年連邦取引所データ侵害通知法：この法律はデータ漏洩に対処するもので、2015 年に成立した。*
- *ナイジェリア：法律を調和させ、実質的なサイバー犯罪法を施行するために、2015 年サイバー犯罪（禁止、防止など）法が施行された。*
- *カタール：サイバー犯罪に関する捜査権限、証拠および手続きの規則、国際協力、相互法的援助、犯罪人引き渡し、サービスプロバイダの義務に対処するため、2014 年法律第 14 号サイバー犯罪防止法が制定された。*

4. サイバー犯罪捜査における「ベストプラクティス」とは

答え：コンピュータ（またはコンピューティングデバイス）を使用して行われた「犯罪」の証拠を客観的に評価すること。内部プロトコルおよび外部リソースを含む多面的なアプローチを活用すること。

例：DDoS 対スピアフィッシング（CFAA）、DDoS、通信詐欺、ランサムウェア。組織の対応と捜査手順、管轄区域のガイダンス、業界のインテリジェンスを含む。

ケーススタディ1:世界最大のボットネットの解体

- **犯罪**：コンピュータ詐欺、コンピュータ詐欺の共謀、通信詐欺の共謀、マネーロンダリングの共謀
- **容疑者**：アクセスブローカー（ボットマスター）
- **手段**：マルウェア、サービスとしてのサイバー犯罪（CaaS; ボットネットの侵害されたデバイスへのアクセスの販売）
- **動機**：個人的な（金銭的な）利益
- **機会**：ソフトウェアや VPN アプリのダウンロードに関するセキュリティ意識やサイバーハイジーンマネジメントの欠如、サイバー犯罪者の間での CaaS（Crime as a Service）アクセスブローカーのニーズ

2024 年 5 月、米国司法省は、国際的な法執行機関による連携捜査を通じて、世界最大規模とされ「911 S5」として知られているボットネットを解体したと発表した。[27] この調査活動により、ボットネットのインフラが破壊され、そのマネジメント者（「ボットマスター」）とされる中国人の YunHe Wang が逮捕された。

司法省の起訴状によると、2014 年から 2022 年にかけて、Wang はマルウェアを作成して拡散させ、世界中の何百万台もの Windows コンピュータ（米国内の 61 万 3000 台以上を含む 1900 万以上のユニークな IP アドレスに関連けられた）を侵害してボットネットを形成した。Wang は、ボットネットの侵害されたデバイスへのアクセス権（プロクシ経由）を他のサイバー犯罪者に販売し、約 9,900 万ドルの利益を得た。これらのサイバー犯罪者は、購入したアクセス権を利用して、多数のサイバー攻撃、大規模な詐欺、児童搾取、嫌がらせ、爆破脅迫、輸出違反などの犯罪を実行した。

27 https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation

●マルウェア配布とボットネットマネジメント

Wang は、自身が運営する無料 VPN サービス（MaskVPN や DewVPN など）にマルウェアを埋め込んだり、**「Pay-per-install service」（海賊版やライセンスまたは著作権で保護された素材を含むことが多い）**で提供されるソフトウェアにマルウェアをバンドルしたりするなど、さまざまな方法でマルウェアを展開して拡散させたとされている。いったん侵入されると、感染したデバイスは約 150 台の専用サーバーのネットワークを通じてマネジメントおよび制御され、そのうち約半数は米国のサービスプロバイダーからリースされていた。これらのサーバーは、アプリケーションの展開とマネジメント、コマンドと制御、911 S5 サービスの運用、および有料顧客（犯罪者）へのアクセス提供を促進した。

●911 S5によって可能になる犯罪行為

ボットネットのプロキシ IP アドレスへのアクセス権を購入すると、犯罪者は身元（および場所）を隠してさまざまな犯罪を行うことができる。ボットネットによって提供されたアクセスに関連する犯罪は多岐にわたり、ストーカー行為や嫌がらせ、個人情報の盗難、爆破脅迫、違法輸出、児童搾取などの犯罪に加え、詐欺検出システムを回避して金融機関や政府プログラムから数十億ドルを盗む金融犯罪（失業保険の不正請求を含む）も含まれていた。

●捜査、逮捕、ボットネットのテイクダウン

法執行機関は当初、ボットネットの侵害された IP アドレスへのアクセスによって有効になっていた盗まれたクレジットカードを使ったマネーロンダリングと密輸の計画を捜査しているときに、911 S5 を特定した。さまざまな法執行機関による数年にわたる国際的な取り組みの後、Wang は最終的にマルウェアの展開、ボットネットの運用、マネーロンダリングに関連する刑事告訴で逮捕された。米国、シンガポール、タイ、ドイツの法執行機関による協調的な取り組みにより、911 S5 に関連する多数のドメインが押収され、さらにはボットネットの再構築の試みに関連する新しいドメインとサービス（クラウドルーターと呼ばれる）も押収された。70 以上のサーバーと 23 のドメインが押収され、多数の悪質なバックドアが閉鎖された。

捜査官はさらに Wang の数軒の住居と 3,000 万ドル相当の資産を押収し、さらに 3,000 万ドル相当の没収可能な資産を特定した。米財務省はまた、ボットネットに関与したとして Wang およびその仲間の Jingping Liu と Yanni Zheng、そして Wang に関係のある 3 つの団体に金融制裁を課した。Wang は現在、コンピュータ詐欺共謀罪、通信詐欺共謀罪、マネーロンダリング共謀罪、実質的コンピュータ詐欺罪で起訴されている。すべての罪で有罪になれば、最高で懲役 65 年の刑が彼に科せられる。

911 S5 ボットネットのテイクダウンは、世界的なサイバー犯罪との闘いにおける意義深い成果であることは間違いない。しかし、さらに重要なことは、大規模なサイバー犯罪活動に関連する広範な影響と、サイバー犯罪者が身元を隠して犯罪活動を加速させるために使用する戦術の進化に加えて、世界中の複数の機関の協力的な努力をこの案件が実証していることである。これはまた、現代のサイバー犯罪の世界的な広がりと広範囲な定義も強調している。

第2章

サイバー犯罪の分類

はじめに

過去において、企業による不当行為に対する社会的抗議やデモは、建物の前でプラカードを掲げる組織化された団体の専売特許であった。今日では、このような社会的抗議は、ソーシャルメディアを介したり、企業のマーケティング情報（ウェブサイトなど）を改ざんしたりすることによって行われる。このようなデモの目的は、企業の製品やサービスへの顧客アクセスを妨害したり、従業員の業務遂行能力を低下させたりすることだった。今日、同じ目的は、システムを消去したり使用不能にしたりするためのサービス拒否攻撃や妨害行為によって達成されている。かつて恐喝は、企業が依存している公表されたくない情報とアクセスやサービスをコントロールすることで行われていた。今日では、それもランサムウェアによって簡単に実行されている。スパイ活動（民間または政府による）は常に存在していたが、今日では、リモートアクセスや盗聴を可能にするバックドア型トロイの木馬によって容易に行われている。

サイバー犯罪は 2014 年から 2023 年にかけて大きく進化し、より巧妙になり、頻発し、影響力を増している。サイバー犯罪の進化は、攻撃の多様性の増加、サイバー犯罪者が使用する手法の高度化、個人、企業、国家への影響の規模の拡大によって特徴づけられている。この時期における最も重要な傾向の一つは、ランサムウェア攻撃の増加である[28]。被害者のデータを暗号化し、その解除と引き換えに身代金を要求するランサムウェアは、金銭を得るためのツールから地政学的に重要な武器へと進化した。現在進行中のウクライナとロシアの紛争のような国家間の紛争におけるランサムウェアの使用は、サイバー戦争が拡大していることを明確に示している。

さらに、フィッシングは依然として一般的なサイバー犯罪であり、2022 年にはフィッシングの被害者がオンライン犯罪の被害者全体の半数を占めている[29]。サイバー犯罪者は、暗号通貨関連の攻撃などの新しいトレンド、テクノロジー、戦術を取り入れて、フィッシングやメールのなりすましの戦術も進化させている[30]。

人工知能などの新技術の台頭により、攻撃者の手口はより巧妙になっている[31]。たとえば、サイバー犯罪者は ChatGPT を使用して、ウェブサイトのレイアウトを設計し、クレデンシャルを盗むオブジェクトとクレデンシャルを転送するオブジェクトの両方を組み込むことで、簡単に攻撃を構築することができる。[32] サイバー犯罪者は、セキュリティシステムを回避するために、保護が脆弱なサードパーティのネットワークを悪用することもある。

サイバー犯罪の影響も飛躍的に増大している。サイバー犯罪による経済的損失は 2001 年以降は 570 倍以上に増加しており、22 年間で少なくとも 7,303,267 人の被害者と 364 億ドルの損失が発生している。サイバー犯罪の世界的なコストは、2015 年の 3 兆ドルから 15%増加し、2025 年には 10.5 兆ドルに達すると予想されている[33]。

COVID-19 のパンデミックは、リモートワークやデータの保護方法に関する不確実性により、サイバー犯罪を増幅させた。その結果、窃盗や横領からデータのハッキングや破壊まであらゆるものを含むサイバー犯罪が 600% 増加した[34]。

サイバー犯罪の脅威が増大していることに対応して、サイバーセキュリティは広範囲な優先事項と

28 https://heimdalsecurity.com/blog/the-history-of-ransomware/
29 https://surfshark.com/research/data-breach-impact/statistics
30 https://www.embroker.com/blog/top-cybersecurity-threats/
31 https://nordlayer.com/blog/evolution-of-cyber-threats-over-10-years/
32 Roy、S.S.、Naragam、K.V.、Nilizadeh、S.（2023）。ChatGPTを使用したフィッシング攻撃の生成。arXivプレプリント arXiv:2305.05133。
33 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
34 https://www.embroker.com/blog/cyber-attack-statistics/

なっている。政府、企業、個人は、新たな脅威に迅速に適応し、データとシステムを保護するためにサイバーセキュリティ対策に投資しなければならなかった。

サイバー空間が助長する犯罪の「種類」とは？本章では、サイバー犯罪の進化を探る。ビジネスの中断や敵対的なブランド攻撃を助長するためにサイバーツールがどのように使用されたか、そして犯罪者が達成しようとする真の目的から捜査官の注意をそらすためにサイバーツールがどのように使用されているか（時にはサイバーツール自体を用いて）を探る。こうした目的とそれを支える動機、脅威の実行者と被害者のプロファイル、サイバー犯罪者の識別特性も提供される。サイバー犯罪に関わる「人的要因」には特に注目が集まる。これは、犯罪の実行と予防の両方に重要な役割を果たし、影響を与える。サイバー犯罪に関連する人的要因は以下に由来する。

1. **犯罪者**：サイバー犯罪者は、衝動性、スリルの追及、共感力の欠如など、特定の心理的特性を示すことが多い。これらの特性は、個人や企業に与えるかもしれない損害を含め、自分の行動の結果に対する関心の欠如につながる可能性がある。また、多くのサイバー犯罪者は高度な知性と創造性を発揮し、セキュリティシステムの脆弱性を見つけ、洗練された攻撃方法を開発する[35]。サイバー犯罪にはリスクが伴うが、サイバー犯罪者は金銭的な利益、個人的な満足感、イデオロギー的な理由などの動機によって、想定される結果を回避する。これらは多くの場合、心理学の行動理論によって実証される。例えば、健康促進や疾病予防プログラムの指針として使える理論モデルである健康信念モデル（HBM）は、サイバー犯罪にも応用できる。モデルの2番目の要素である「認識された重大性」は、「健康状態の深刻さに関する個人の評価」と説明されており、喫煙の結果の重大さを評価することによって、個人が喫煙を決断する可能性があることを意味する。サイバーセキュリティに当てはめると、これはサイバー犯罪者が結果の重大さを評価して、情報に基づいた判断で被害者を攻撃していることを示している。
2. **被害者**：サイバー犯罪の過程では、人間の意思決定が重要な役割を果たす。例えば、ソーシャルエンジニアリングは、サイバー犯罪者が人間の信頼を悪用して機密情報を入手し、さらなるサイバー犯罪を可能にする操作手法である。電子メールや電話などの通信手段を偽装し、個人を騙してパスワードや個人情報を暴露する[36]。短期記憶、疲労、物忘れなど、人間の本性に関連する行動も、セキュリティインシデントの一因となる可能性がある。例えば、疲労している従業員は、フィッシングメールの可能性を評価して確認することを忘れ、フィッシングメールに埋め込まれたランサムウェアをクリックして、自分のマシンに感染させる可能性がある。
3. **インサイダー脅威**：インサイダー脅威は、公的領域と私的領域の両方に影響を及ぼす複雑でダイナミックなリスクである。インサイダーとは、組織の一員であり、業務を遂行するために、施設、システム、ネットワーク、または人々への一定のレベルのアクセス権を付与された個人である[37]。インサイダー脅威は直接的または間接的であり、サイバー行為を含む様々な形で顕在化する可能性がある。
4. **予防と対応**：サイバー犯罪者の心理を理解することで、個人や企業はより適切に自分自身を守ることができる。サイバー犯罪の背後にある動機を認識することにより、個人や企業は関連するリスクを軽減するための措置を講じることができる。予防策は、従業員を監視してハッカーの行動を早期に発見することだが、これは現代企業にとって困難な課題である[38]。従業員の行動を変えるための従来のアプローチは、サイバーセキュリティにおいては人間が最も弱い部分であることを前提とされ

35 https://www.linkedin.com/pulse/psychology-cybercriminals-understanding-mind-hacker-sharma/
36 https://terranovasecurity.com/what-is-social-engineering/
37 https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
38 https://www.wallix.com/blog/the-psychology-of-the-cyber-criminal/

る傾向があった。しかし、リチャード・H・ターラー（Richard H. Thaler）とキャス・R・サンスティーン（Cass R. Sunstein）によって提唱された行動経済学のナッジ理論は、サイバーセキュリティに適用できる有望な代替アプローチを示している。それは、「ソフトで父権主義的なナッジ」は、人々の選択肢を制限することなく、彼らの最善の利益になる意思決定を支援することができるというものである。[39] サイバーセキュリティでは、ナッジとは、特定のセキュリティ動作に影響を与えるように設計されたセキュリティ通知、メッセージ、プロンプトのことである。それは、最も重要な場合に正しいセキュリティ決断へと人々を導く。ナッジは、終業時にソフトウェアの更新を促すメッセージとして機能することがある。それは、最新のセキュリティ意識向上トレーニングモジュールを完了するためのリマインダーかもしれない。効果的なナッジは、パーソナライズされていることが多い。例えば、「従業員の皆様」というような全体に向けたメールではなく、「ジョー・ブログズ様」というように、受信者の名前で始めるのである。パーソナライズされたナッジは個人の注意を引き、人々を正しい行動に導きやすくする。[40]

サイバー犯罪を理解し、防止し、対応するためには、人的要因が不可欠である。これらは犯罪者の行動、被害者の脆弱性、予防と対応の戦略に影響を与える[41]。

本章で提供される定義は、サイバー犯罪が反映する脅威の種類を明確にすることにより、組織のポリシー開発者が監査と評価のトピック、および防御と保護のメカニズムを決定するのに役立つ。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- 「サイバー犯罪」とは
- サイバー犯罪の目的と動機とは
- サイバー犯罪者のプロファイルとは
- サイバー犯罪者の組織構成とは
- サイバー犯罪者が保有するスキルや知識とは
- 2014 年以降のサイバー犯罪の進化経緯とは
- サイバー犯罪と人的要因の関係とは

39 https://blog.thinkcyber.co.uk/introduction-to-nudge-theory-for-security-awareness

40 https://www.cybsafe.com/blog/security-nudges-behavioral-research/#:~:text=What%20is%20a%20cybersecurity%20nudge,day%2C%20prompting%20a%20software%20update

41 Leukfeldt, R. and Holt, T. (2021). The Human Factor of Cybercrime (Routledge Studies in Crime and Society) 1st Edition; Routledge Studies in Crime and Society

サイバー犯罪の種類におけるトピックス分類

「サイバー犯罪の種類」知識領域におけるトピックスの分類を図 2-1 に示す。

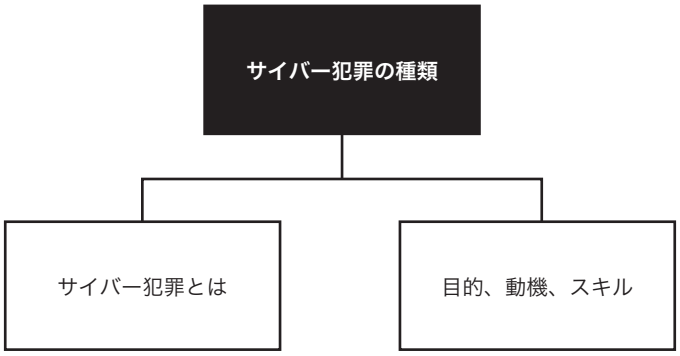


図 2-1.「サイバー犯罪の種類」知識領域におけるトピックスの分類

サイバー犯罪とは

サイバー犯罪は、序章で「サイバー空間を巻き込み、社会の集合意識の強力で確定的な諸状態を冒涜する行為」と定義した。サイバー犯罪は、インターネットやコンピュータを使用した一連の犯罪行為や詐欺行為、および社会活動を指す言葉として広く使用されている。挙動に関する社会的ルールは常に変化しており、そこには常識的儀礼と合わせて、実際の犯罪になる可能性のある受け入れがたい挙動まで含まれる。

「第 1 章サイバー犯罪とその捜査」では、幅広く解釈できる要約説明を行った。

「サイバー犯罪とは … コンピュータ（またはコンピューティングデバイス）をツールとして、あるいは標的にされた被害者として、あるいは注意をそらす目的で行われる犯罪である」

他の定義では、以下の定義のように、ツールや関与する活動をより詳細に説明して列挙している。

「サイバー犯罪は、インターネットのコンポーネント（チャットルーム、E メール、掲示板、ウェブサイト、オークションなど）を 1 つ以上使用して、計画に関連した金融機関やその他機関に対して、不正行為を行う、または詐欺で得た収益を送金する一連の不正な企てである。また、サイバー犯罪には、迷惑メールの生成、コンピュータへのウイルスやスパイウェアのダウンロード、インターネットを介した他人への嫌がらせ、児童ポルノ、オンラインでの売春誘惑行為も含まれる。おそらく、サイバー犯罪の最も顕著な形態は、犯罪者がインターネットを使用して他人から個人情報を盗み出すなりすましだ。」[42]

インターネットがだれにでも利用できるほど普及を遂げたことで、ウェブサイト（World Wide Web）は、多くの人々にとってビジネスチャンス拡大のための新しい道を切り開くに至っている。オンラインショッピング、E メール、インスタントメッセージング、そしてその他のサービスは、中小企業が世界

42 http://definitions.uslegal.com/c/cybercrimes/

に打って出るための競争力を高めている。「サイバー空間」によって、中小企業は地域市場にとらわれることなく、物理的な限界すら取り除く存在としてその意義を見いだしている。この傾向は世界的なCOVID-19パンデミックによって加速され、その間に中小企業の70%がデジタル技術の導入を加速するか、あるいは業務のデジタル化の度合いを高めた。[43]

サイバー空間以前は、犯罪活動の大半は一度に一つの場所で行われていた。詐欺師が地元の被害者を騙したとき、当局は犯罪が行われた時点で詐欺師が管轄区域内に物理的に存在していたことを知っていた。サイバー空間と新技術により、*サイバー犯罪者は複数の司法管轄区で複数の犯罪を同時に行うことができる。*[44]

多くの人は言う。「インターネットの良い点は、だれでも利用できるところである」と。逆に、法の執行機関やセキュリティの専門家はこう言う。「インターネットの悪い点は、だれでも利用できてしまうところである」と。犯罪者は、サイバー空間が自分たちの活動の新たな領域だと分かった。サイバー空間は、より効率的に拡大できる詐欺スキーム（企み）のため、また性的捕食者や小児性愛者が自分の家で子供たちを犠牲にするためにチャンスを与えてしまった。コンピュータハッカーは、リモート操作でネットワークに不正侵入し、システムをシャットダウンし、情報を破壊し、機密情報を盗み出すことができる。

サイバー犯罪は、文字どおりサイバー空間があればどこででも存在し、1日24時間、週7日いつでも稼働することができる。たとえば、サイバー犯罪者は英国の大企業にフィッシングメールを送信し、それと同時に、米国の中小企業や慈善団体にもフィッシングメールを送信することができる。これらはすべて遠隔地から行われる。たとえ犯罪者が寝ていても、自動化プロセスとホストされたウェブサイトは作業を行い続ける。マルウェアは、疑いを持たないユーザーが目的のリンクをクリックするまで、感染した正規サイトのウェブページで待ち伏せすることができる。チャットルームは昼夜問わずビジー状態となり、小児性愛者が性的搾取を目的に幼い子供たちを探す間に、詐欺師は**ロマンス詐欺**や投資詐欺を行う。サイバー空間は、多くの犯罪をグローバル化し、そして新たな犯罪を生み出したことで、世界を変えてしまった。たとえば、サイバー犯罪者は、人間の脆弱性と怠惰の増大を悪用して、新型コロナウイルス感染症（COVID-19）を利用した。個人が企業ポリシーや管轄権を持たずに自宅にいること、また企業が危機的状況にあり、受信する通信の正当性を検証する時間やリソースがほとんどないことを犯罪者は認識し、フィッシング、スミッシング（テキストメッセージによるフィッシング）、ヴィッシング（音声通信によるフィッシング）攻撃を巧妙化し、頻度も高めた。

サイバー犯罪者は、社会の相互接続性のおかげでより容易に利用できるようになった手段、動機、機会を利用する[45]。たとえば、新型コロナウイルス感染症（COVID-19）のパンデミックの後、公的機関になりすました詐欺師がいるという報告があった。サイバー攻撃者は、悪意を持って世界保健機関（WHO）および組織、スーパーマーケット、航空会社[46]を標的にし、COVID-19の治療法[47]を提供した。これらの例は、サイバー攻撃に対する脆弱性が広がっており、セクターを越えて影響を受けやすいことを示している。

---

43 Parker, C., Bingley, S. and Burgess, S.（2023）. 危機時の中小企業のデジタル対応の性質。情報と組織、33（4）、p.100487。

44 Al-Musib, N.S.、Al-Serhani, F.M.、Humayun, M.、Jhanjhi, N.Z.、2023.「ビジネスメール詐欺（BEC）攻撃」Materials Today: Proceedings、81、pp.497-503。（訳注: "Materials Today: Proceedings"は科学雑誌の名前）

45 （Pasculli, 2020）

46 （Threat Team, 2020）

47 Gervais, J.（2020）.これらのコロナウイルス詐欺に注意すること。[オンライン]Us.norton.com。参照先:<https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>[2020年9月1日アクセス]。

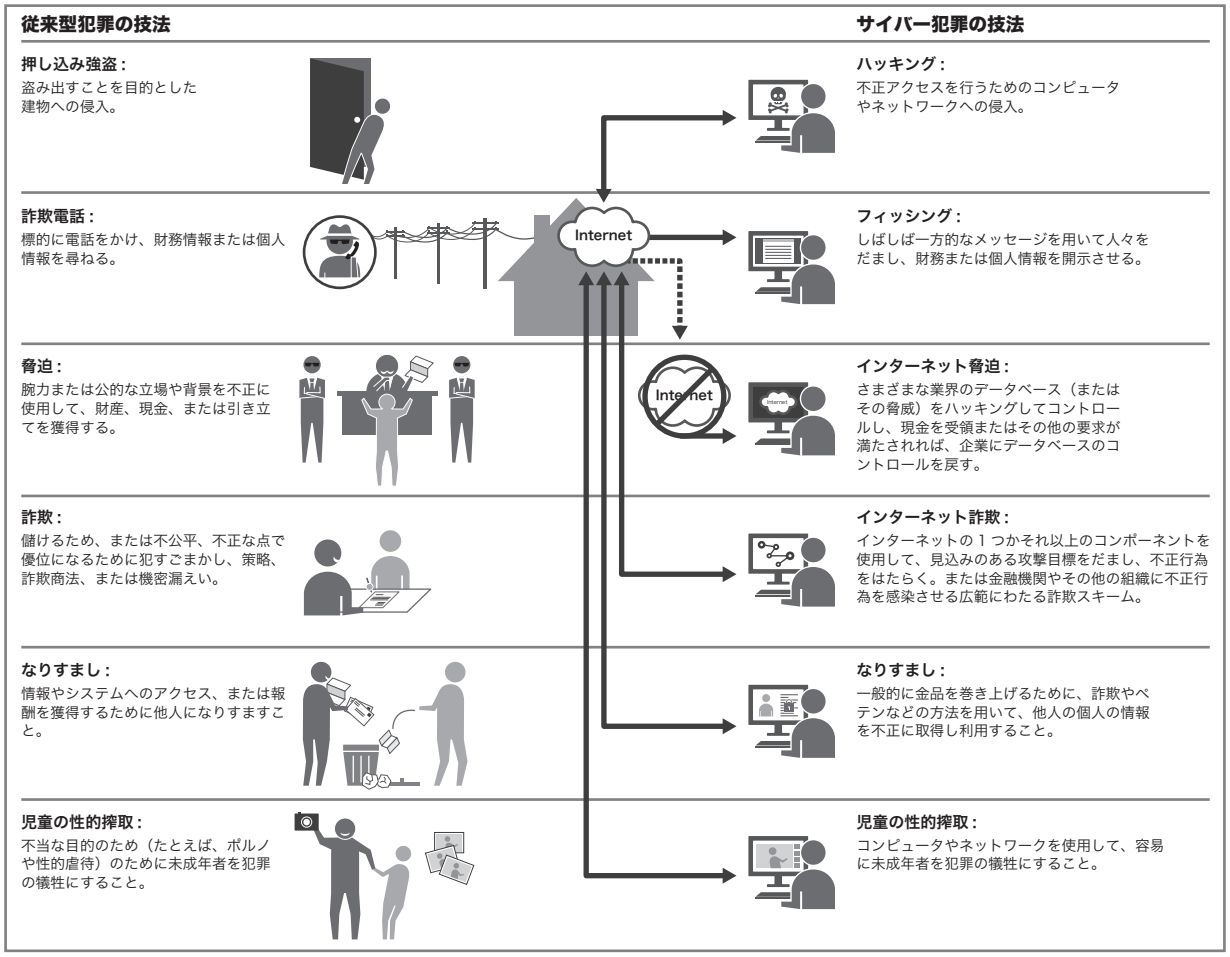


図 2-2. 従来型犯罪とサイバー犯罪の比較（出典：米国会計検査院 2007）[48]

サイバー捜査官は、どのような犯罪や活動が誰によって行われたのかを最終的に特定する必要がある。サイバー犯罪の被害者、動機、目的、そして犯罪を行うのに必要な技術的スキルを調査することで、加害者を特定する分野を絞り込むことができる。被害者学を研究すると、なぜ個人や企業が標的にされたのか、また、対象者の動機や目的は何であったのかということを捜査官が特定できるようになる。以下の質問は、被害者、動機、目的を検討する際に調査員が尋ねそうなことである。被害者は、出会い系サイトを定期的に利用しているのか？あるいは被害者は政府と国防契約を結んでいる契約者なのか？被害者に対してどのような種類のサイバー詐欺やサイバー攻撃が行われたのか？犯罪を起こすにはどのようなスキルが必要なのか？犯人はチャットルームでソーシャルエンジニアリングスキルを使用しているのか？それとも、極めて高い動機を持ち、検出されずに被害者のネットワークにアクセスできる高度なスキルを有するハッカーなのか？被害者は 10 代かそれとも年配者か？被害者は性的搾取の標的になっているのか、それとも多額の退職金を持っているからなのか？

サイバー犯罪とサイバー犯罪者は、それぞれ異なる動機と意図に支配されていることに留意することが重要である。幸いなことに、心理学研究は行動や動機を説明するのに役立つ理論をいくつか提供しており、それらはサイバー犯罪にも応用できる。例えば、健康信念モデル（HBM）は[49]、病気に対する脆弱性と病気の重症度が組み合わさって「脅威」を形成し、脅威の認知が行動を動機付けると提唱している。HBM によると、脅威の認知が行動を促すが、実行される特定の行動は、脅威に対抗するために利用可

48　米国会計検査院、「サイバー犯罪、公的機関および民間組織がサイバー脅威への対応で直面する課題」、GAO-07-705（2007）、出典:http://www.gao.gov/products/GAO-07-705

49　参考文献:Rosenstock, I.M., 2000.健康信念モデル。

能な行動のオプションに関する信念によって決定される。特定の行動は、その行動によって得られると認識される利点（つまり、病気の脅威を軽減する可能性）が、その行動によって得られると認識される障害（コスト、不便さ、恥ずかしさ、不快感など）を上回る場合にのみ採用される。同じ理論は、企業におけるサイバーセキュリティの行動を調査する際にも適用できる。その場合、サイバーセキュリティの方針や行動は、認知された利点（サイバー脅威を軽減する可能性）が認知された障害（コスト、不便さなど）を上回った場合にのみ採用される可能性がある。

第１章で解説されているように、コンピュータ（またはコンピューティングデバイス）は、犯罪の道具（または「手段」）として、犯罪の標的として、あるいは犯罪から目をそらすものとして、サイバー犯罪に使われることがある。より一般的には、「仮想」サービスやアプリケーションなど、それらが表現するテクノロジーは、本章で解説されるサイバー犯罪の種類を考慮する際は、同じカテゴリを反映する。

道具としての技術

サイバー空間や技術の悪用が、犯罪者に新たなツールボックスを提供することになり、長らく用いてきた詐欺スキームやその他の犯罪活動と同じ犯罪を実行できるようになった。これらの新たなツールのお陰で、犯罪者は大規模な標的確保がより容易になり、また逮捕を逃れるよう自分たちの行動や痕跡の隠蔽ができるようになった。

サイバー犯罪者はまた、これらのツールを使用して個人を操作し、許可されていないあるいは違法なタスクを実行させる。これらの取り組みは人間の心理を利用しようとするものであり、正しく適用すればサイバー犯罪活動に役立てることができる。[50] 例えば、あるフィッシング詐欺では、犯罪者は住宅購入手続き中の人物を監視し、その人物の事務弁護士を装った後、自分の口座に５万ポンドを振り込むよう要求した。[51] これらの攻撃に関する重要な観察からわかることは、犯罪者が他人を信頼する意思、親切心、不安やストレスが意思決定に与える影響、個人のニーズや欲求、意思決定における素朴さなど、さまざまな人間の心理的特性を利用しようとしていることである。[52] 住宅購入の例では、犯罪者はまず住宅購入というストレスの多いプロセスを狙い、次に勧誘者になりすまして資金の送金を要求できる特定の瞬間を待った。メールの文面は、購入を確実にするために資金をすぐに送金することの重要性を強調していた。さらに、住宅購入者が購入予定の物件を失うことへの恐れ、住宅購入に対する一般的な不安、そして（本物と思いこんだ）弁護士に対する住宅購入者の信頼が、資金移転につながった要因であることは間違いない。

サイバー犯罪者は、摘発を回避し、法執行機関による証拠収集をより困難にするために、他国を経由することによって、物理的な司法権に対してサイバー空間を活用することができる。犯罪者がテクノロジーを利用した初期の例として、タイプライターではなくコンピュータプリンタを使って被害者に書面を送ったことが挙げられる。電子プリンタを使用すると、ボイラールーム詐欺の文書作成プロセスの生産性と効率性が向上するだけでなく、犯罪者が文書の作成者として追跡されることを回避するのにも役立つ。法執行機関の研究室の技術者が、誘拐、身代金要求、恐喝などの詐欺計画に関する事件を解決するために、タイプライターのキーを特定して照合できることを犯罪者が気付いたときにこの改変が生じた。

---

50 Nurse, J.R.、2018。「サイバー犯罪とあなた:犯罪者の攻撃方法と悪用しようとする人的要因」arXivプレプリント arXiv:1811.06624。

51 iTVニュース:電子メールで50,000ドルを騙し取られる。http://www.itv.com/goodmorningbritain/news/scammed-out-of-50000-over-email（2015） scammed-out-of-50000-over-email（2015）

52 Nurse, J.R.、2018。「サイバー犯罪とあなた:犯罪者の攻撃方法と悪用しようとする人的要因」arXivプレプリント arXiv:1811.06624。

- **詐欺スキーム：**

  詐欺スキームは、常に虚偽の表示と策略に基づいている。スキームの範囲は、配送されることのない偽商品から実現することのない偽投資話にまで至る。今日では、これと同様の策略や虚偽の表示は、ソーシャルエンジニアリングとして知られている。ソーシャルエンジニアリングは、会話、チャット、メール、投稿、通信など想像できるあらゆる方法で実行される。犯罪者は、電話中、詐欺やフィッシング詐欺のスパムメールの勧誘、ウェブサイトの投稿などで策略を使う。改ざんされたウェブサイトには、被害者を騙してリンクをクリックさせ、コンピュータにマルウェアをダウンロードさせるリンクが掲載されている場合がある。オンラインの詐欺スキームでは、特にサイバー空間で個人、企業、または組織のオンライン ID について、正当なものと同等の雰囲気を醸し出すのが容易な場合には、誰に対しても犯行をはたらくことができる。今日、サイバー犯罪者はフィッシングメールやソーシャルエンジニアリングの戦術を使用して、個人を騙して暗号通貨ウォレットの認証情報を公開させたり、不正なアドレスに資金を送金させたりしている。いったんこれらの認証情報を入手すると、その情報を使用して被害者のウォレットから資金を盗むことができる。

  心理学的な観点から見ると、ソーシャルエンジニアリングとは、望ましい結果を達成するために人々の意思決定に影響を与えることである。その成功は心理欺瞞の結びつきにあり、人間の思考プロセスに存在する認知バイアスを利用することに依存することが多い。ソーシャルエンジニアは、人間の推論には欠陥があることを知っており、ターゲットの心理的ヒューリスティックを操作して体系的な間違いを起こさせ、協力するよう説得する。[53]

- **ナイジェリア詐欺スキーム**[54]**：**

  ナイジェリアの（手紙または）詐欺計画は当初、米国郵便公社を通じて個人的な手紙を送ったり、迷惑電話をかけたり、意図したターゲットにファクスで通信を送信したりすることによって実行された。技術の進歩により、E メールという、より強力で費用対効果の高い配信ツールが開発された。これらの詐欺行為は、相続詐欺や恋愛詐欺から、国営宝くじ当選詐欺や投資スキームまで多岐にわたる。サイバー空間が登場する前は、サイバー犯罪者は詐欺を企てるたびに、紙、封筒、郵便料金、長距離電話料金といった投資コストを負担していた。彼らの努力が報われたか否かに関わらず、標的とされた被害者を狙うたびにコストが発生した。技術が進歩するにつれ、サイバー犯罪者は手紙をファクスで送信するようになり、実際の手紙を送るコストを回避し、印刷コストを標的の被害者に転嫁するようになった。使用されたツールに関係なく、詐欺を実行するために米国郵政公社を配送手段として利用したことは、郵便詐欺法（合衆国法典第 18 編第 1341 条）違反であり、連邦犯罪となった[55]。犯罪者が手紙や郵便サービスから電話やファクシミリ機器に移行したとき、彼らの計画は有線通信詐欺法（合衆国法典第 18 編第 1343 条）により連邦政府によって起訴された[56]。スキームの実現方法や計画手法に関わらず、詐欺は詐欺である。郵便詐欺と電信詐欺のいずれの違反行為も、コンピュータ犯罪に対して、当初は知能犯罪として捜査されていた。

  それ以来、電子メールは、何千人もの潜在的な被害者にスパム電子メール詐欺を効率的に配信するために犯罪者に利用されてきた。最近、サイバー犯罪者は生成 AI を利用することにより、ChatGPT などのツールを使用して標的を絞ったフィッシングメールを効率的に作成し、生成 AI ツールからのアラートや警告を回避できるようになった。たとえば、サイバー犯罪者は、米国の法律事務所の CEO をターゲットにしたフィッシングメールの作成を依頼するテキストを ChatGPT

53 Bosworth, S., Kabay, M. ,& Whyne, E. (2014).Computer security handbook (6thed.). NewYork: Wiley
54 https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud
55 https://www.law.cornell.edu/uscode/text/18/1341
56 https://www.law.cornell.edu/uscode/text/18/1343

に入力するだけである。ChatGPT からの最初の応答では出力を防止して要求者に警告する場合があるが、犯罪者は単純なフレーズを使用してツールを操作し、出力を生成することができる。生成 AI を活用することにより、サイバー犯罪者はフィッシングメールによくあるエラー（スペルミスなど）を簡単に減らし、詐欺の特定を困難にすることができる。

コンピュータアプリケーションを使用すると、サイバー犯罪者は、本物のように見えるロゴや参照情報を使用して精巧な文書を作成できる。詐欺師はまた、ニュースで大きく報道される危機的状況も利用する。地震や「ジカウイルス」[57] のような大惨事は、犯罪者が他人を利用する機会を提供する。人々は騙されて偽の災害基金に寄付したり [58]、欺瞞的な広告に引っかかってジカウイルスから身を守るリストバンドを購入したりしがちである [59]。詐欺師は、クリスマスのような国際的な祝祭日も利用する。というのは、人々は普段よりも興奮し、警戒心が薄れ、より安い買い物を求める可能性が高いからである。詐欺師は、ギフトカードを改ざんし、消費者が使用する前に資金を流出させる「ギフトカード流出」を行うこともありうる。[60]

銀行強盗が強盗をする前に銀行を調査したり調査したりするのと同じように、詐欺師はサイバー犯罪を行う前に、悪用できる潜在的な被害者を特定する。犯罪者は、ターゲットを特定するための**情報ツール**としてインターネットを使用する。Facebook、Instagram、TikTok、LinkedIn、出会い系サイトを利用すると、**ロマンス詐欺**や**金銭誘導（豚の屠殺）**の潜在的なターゲットを特定するのに役立つ。これらの情報源を使用してターゲットのペルソナやプロファイルを構築すると、犯罪者は自己紹介文や挨拶文を作成して、信頼関係を構築するのに役立つ。これらの手法は、存在しない恋愛や投資への期待を利用して被害者から金銭を奪い取ろうとするソーシャルエンジニアリングの策略である。今日、ロマンス詐欺と金融詐欺には一般的に共通点がある。どちらも情緒的な弱点を悪用し、ソーシャルエンジニアリング戦術を利用して、被害者から暗号通貨ウォレットの情報や資産を入手し、偽りの口実や見せかけで被害者を誘惑し、悪意のある人物に対して進んで資金を提供するように仕向け、デジタル資産を盗む。これらの策略は、悪意のある人物が信頼関係の構築や性格の発達などのさまざまなソーシャルエンジニアリング手法を利用して、最終的に資金や資産の移転につながる要求を行うため、数週間または数か月にわたって展開されることがある。

インターネットの情報収集力は、犯罪者が年齢によって被害者をターゲットにするのにも役立つ。犯罪者が名前や電子メールアドレスのリストを持っていれば、それらをウェブブラウザに入力し、無料の身元調査を提供するリンクをたどるだけで、サービスに加入することなく人物の年齢を判定できる。**高齢者詐欺**では高齢者がターゲットである。というのは、高齢者は老後の蓄えがあり、若者よりもソーシャルエンジニアリングが容易に行えるからだ。

振り込め詐欺 [61] は、大半の祖父母が孫に抱いている愛情ある支援関係を悪用したソーシャルエンジニアリングによる詐欺である。この手法は、まず年齢ごとに潜在的攻撃目標を特定するために専用のツールを使用し、電話番号を探り出して電話をする。そして、オンライン送金システムが、詐欺師への送金ツールとして利用される。

このスキームは、孫の短期的な金銭的危機を脱せられるよう祖父母に送金させる詐欺行為が関わってくる。犯人は、孫（高齢者）がいる可能性があると特定された人の電話番号に電話をかけることから始める。犯人側は、詐欺をはたらくにあたって何も知識は必要がない。ここで振り込め詐

57 http://www.cdc.gov/zika/about/
58 http://www.fraud-magazine.com/article.aspx?id=4294978232
59 https://www.ftc.gov/news-events/press-releases/2016/05/marketers-mosquito-shield-bands-pay-300000-barred-making
60 https://www.foxbusiness.com/lifestyle/gift-card-draining-scam-what-it-is-and-how-to-protect-yourself
61 http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf

欺の展開手法について説明する。

発信者：「あっ、おじいちゃん、僕だよ、だれだか分かる？」

被害者：「あぁ、この声はマシューだろう」

発信者：「そう、そのとおり。実は、友達とカナダに向かっている途中でヒッチハイクの男の子を乗せたんだよ。すると、警察が彼を尋問してマリファナを持っていることが分かったんだ。僕たちみんなが逮捕されて、保釈されるのに500ドルが必要って。状況が余計に悪くなるから、父さんと母さんには知らせたくないんだよ。おじいちゃん、助けてよ」

そして、詐欺の標的は国際送金サービスのような振替システムを使用して送金するように指示をされる。

表2-1は、高齢者を狙った最も一般的な金融詐欺の概要を示している。

表2-1.「高齢者を狙った金銭詐欺トップ10」[62]

1	高齢者向け医療保険制度 / 健康保険詐欺
2	偽造処方箋
3	葬儀 & 墓地詐欺
4	偽のアンチエイジング（老化防止）商品
5	テレマーケティング / 電話勧誘詐欺
6	インターネット詐欺
7	投資詐欺
8	住宅オーナー/ リバースモゲージ（持家担保年金）詐欺
9	賞金 & 宝くじ詐欺
10	振り込め詐欺

- **いじめと脅迫：**

  「お願いします」「ありがとうございました」というような基本的な社会規範は、特定の社会的状況における適切な対応として幼児に教えられる。子供たちは、いじめが許される行為ではないことも学ぶ。いじめはもともと、被害者が本来行わないであろうことを強制される**身体的な脅迫**として定義されていた。押したり、叩いたり、被害者から物を奪ったりすることはいじめとみなされた。いじめは、加害者が被害者に対し、自分の身体的な力を行使して、被害者を自分の意のままにしようとしたときに発生した。

  サイバー空間は**ネットいじめ**の遊び場であり、学校だけでなく職場にも広がる可能性がある。テキストメッセージ、ビデオ、写真を送ったり、誰かについて真実でない話を広めたりすることは、すべてネットいじめの一部である。ソーシャルメディアは物理的な場所に関係なくすべての人を結びつけるので、いじめる側が他人を威圧する力は、もはや物理的な威嚇だけにとどまらない。さらに、ネットいじめは昼夜を問わず、どこからでも匿名で送信できるテキストメッセージやソーシャルメディアへの投稿によって発生する可能性がある。いじめは、サイバース空間であるか否かを問わず、被害者に長期的な身体的および心理的影響を与える可能性がある。そのため、ほとんどの州

62 https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

でネットいじめや電子ハラスメントに関する法律が制定されている。

脅しや脅迫によって被害者が何かを強要されるいじめと同様に、テクノロジーの悪用によって犯罪者やその脅迫の実践のためにツールが利用されるようになった。**恐喝**とは、通常は金銭などのような価値のあるものを、力、威嚇、または脅迫によって入手することである。1990年代後半、マイクロソフトのビル・ゲイツ会長は、500万ドルを払わなければゲイツと妻、娘、そして同僚のスティーブ・バルマーが狙撃兵の銃弾で殺されるという脅迫状を受け取った。最初の脅迫は、シカゴ近郊のイリノイ州パラタインからゲイツ氏に郵送された恐喝状の中にあった。身元を隠すため、恐喝者はゲイツに対し、今後の通信にはアメリカオンライン（AOL）の特定の掲示板システム（BBS）を使用するよう指示した。その後の手紙やBBSへの投稿を通じて、FBIは関連する期間中に800人が特定のBBSにアクセスし、そのうち79人がシカゴ地域で登録されていたことを突き止めた。犯人が新たな連絡手段として使用するフロッピーディスクを送りつけてきたとき、FBI法医学検査官はデータを回収し、最終的にその結果犯人としてイリノイ州パラタインのアダム・プレッチャーの身元を特定した。その後プレッチャーは逮捕および起訴されて、懲役70か月の判決を言い渡された[63]。

サイバー空間ではまた、性的に露骨な自分の写真を他人に送る**セクスティング**から発展した新しい形の恐喝も発生している。犯罪者はチャットルームで女性と親しくなり、挑発的なヌード写真やビデオを送るよう説得する。被害者が後悔し、これ以上の送信を続けることを拒否すると、犯罪者は画像やビデオを両親、教師、友人、教会のメンバーに送ると脅し、従わせようとする。成人女性が脅迫され、犯罪者と性的関係を続けるよう強要された。

時には、関係が悪化して別れた後、執念深いパートナーが、元パートナーの同意を得ていないポルノ写真やビデオをインターネット上に公開することがある。これが**リベンジポルノ**と言われるものである。

児童の性的搾取は、最も多発している犯罪行為のひとつであり、テクノロジーとサイバー空間を悪用して飛躍的に増加してきた。児童ポルノ（CP）や未成年者への性的虐待に関与する人物は、長年にわたり世間の注目を浴びてこなかった。一般の人々は、このような性癖を持つ人々の数や、発生した事件の数を知らなかった。何年もの間、ほとんどの人々は、こうした加害者がレインコートを着た不審人物ではなく、家族や被害者から信頼されている身近な人物であることがほとんどであることに気づかなかった。犯罪は何十年もの間、報告されなかった。犯罪者はフィルム現像店で写真を現像するリスクを冒すことができなかったため、CP写真は通常ポラロイドカメラで撮影された。ビデオはさらに少なく、米国郵便公社を通じて送られた茶色の小包として犯罪者の間でのみ共有されていた。

米国郵政検査局は、この種の事件を調査した最初の連邦機関であった。サイバー空間を通じて行われる多くの犯罪と同様に、インターネットは、以前は限定されていた物理的および地理的領域を超えて、被害者層を大幅に拡大した。1990年代、デジタル写真の技術と手頃な価格、そしてインターネットを介した匿名での画像取引が可能になり、犯罪者にとって新たな機会が爆発的に増えた。この種のメディアは利用しやすくて匿名性が高く、ネット上で個人的に同好の士とつながることができるため、多くの小児性愛者や痴漢が闇から姿を現した。**インターネットチャットルーム**の出現もまた、こうした犯罪者たちに悪用され、自宅で遠隔操作される若い被害者たちをソーシャルエンジニアリングで手なずけようとしている。米国郵政検査局によると、10歳から17歳までの子どもの7人に1人が、インターネットを通じて性的な勧誘を受けたり、声をかけられたりした経験

63　http://community.seattletimes.nwsource.com/archive/?date=19980711&slug=2760562

があるという[64]。このことを親に報告したのはわずか12%だった。

攻撃対象としての技術

犯罪者がより洗練され、新しいテクノロジーを使いこなすようになると、テクノロジーそのものが標的となり、サイバー空間の出現以前には存在しなかった新しい犯罪が出現した。

- **カードスキマー：**

  カードスキマーは、テクノロジーがクレジットカードの取り扱いを変えたことから生まれた。歴史的に、クレジットカードのアカウント情報の窃盗は「ゴミ箱漁り」によって行われていた。犯罪者は、企業のゴミを漁り、クレジットカードがカーボンコピー用紙に印刷され、顧客が署名した後に廃棄されたカーボン伝票を探していた。伝票の1枚は顧客に渡され、1枚は店舗で保管され、1枚は預金項目として銀行に送られ、それぞれの用紙の間に挟まれていたカーボン紙はゴミ箱に捨てられていた。当時のクレジットカードには磁気データテープが付いていなかったのだ。廃棄されたカーボン紙には、口座名義人の名前、口座番号、カードの有効期限が記載されていた。誰にも気づかれることなくこの情報を手に入れた犯罪者は、電話で商品を注文し、空き家に発送させ、配達員宛てのメモをドアに残し、不在の場合にはどこに荷物を置くべきかを指示した。犯人につながる痕跡はなかった。この種の「ゴミ箱漁り」詐欺に対する短期的な解決策は、カーボンレスのクレジットカード伝票を使用することだった。

  クレジットカード処理の技術が進化するにつれ、必要なデータはカード裏面の磁気テープに保存され、販売者がカードをスワイプすると販売時点情報管理（POS）レジスターで読み取られるようになった。その後、データはサイバー空間に送られ、クレジットカード発行会社とベンダーの銀行に中継され、すぐに配信される。このプロセスにより、口座保有者のデータは電子的に読み取られて送信されるため、犯罪者がデータを入手することがより困難になり、セキュリティが向上する。

  テクノロジーが進歩し続けるにつれて、犯罪者の活動環境も変化した。口座情報を盗むためにはクレジットカードに物理的にアクセスしなければならなかったため、犯罪者は新しいカード処理技術をターゲットにする必要があった。犯罪者は独自のカードリーダー、つまり**「スキマー」**を使って情報を取得し始めた。たとえば、レストランではウェイターがあなたのカードを持って行き、数分後にカードを返す。これにより、犯罪者はポケットやレジの近くに保管しておいたスキマーでカードのデータをスキミングして取り込むための機会を余裕をもって得ることになる。その後、磁気テープを作成して新しいプラスチックカードに貼り付けて、e複製カードを作ることができる。

  カードスキミング装置は、ATMやガソリンスタンドの給油機に偽装して設置されることもある。顧客（被害者）がスキミング装置でカードをスワイプすると、装置（例えばATMや給油機などの）リーダーが単に故障したようにしか見えないため、顧客はデータが盗まれたことに気づかない。さらに、被害者はATMやガソリンスタンドに一人でいることが多いので、何が起こったのか理解できない場合もある。その後、犯罪者はスキマーを取り外し、複数のクレジットカードからデータを入手することができる。2015年、ベライゾンの2016年データ侵害調査報告書によると[65]、ペイメントカードスキミング事件の70%が犯罪組織によるものであったとされている。

  サイバー空間が出現する以前は、合併計画、製品の研究開発プロジェクト、企業広報などの業務記録を傍受したり入手したりすることは困難だった。スパイ活動と同様、犯罪者はまず、目的のデータや情報を保有する企業や組織を見つけ、その施設に侵入して標的の情報を探し出す方法を探

64 http://docplayer.net/16377727-A-u-s-postal-inspector-s-guide-to-internet-safety-for-children.html
65 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

り、捕まることなくデータを盗み出すことに成功しなければならなかった。情報が社内データシステムに保存されている場合、これはさらに困難になる。

かつて、スパイ機関はマイクロカメラを使って文書を撮影していた。この小さな装置は、隠すのも持ち運ぶのも簡単だった。50 枚撮りのフィルムロールが、後日、秘密裏にハンドラーまたはケースオフィサーに届けられる。文書を電子的に保存して転送することが簡単にできるようになり、このような活動の状況は大きく変化した。これらのテクノロジーにより、以前は（ほとんどの場合）物理的に不可能だった大規模なデータ窃盗が可能になった。

1 ギガバイト（GB）のサムドライブやフラッシュメモリー（USB メモリ）には、約 65,000 件の Word 文書または 10,000 件の PDF 文書を保存できる。8 ギガバイトのサムドライブを使用すれば、犯罪者は、520,000 件の Word 文書をその場から簡単に盗み出し、持ち去り、宅配便で配送することができる。さらに、ファイル転送プログラムを使用すると、100Mbps のファーストイーサネットで、520,000 件の文書をその場所から取り出すのに 1 分半もかからない。一方、USB が出現する前は、スパイは、5,000 枚の文書が入った 8.5 インチ × 11 インチの紙を 104 ケース被害現場から発見されないように物理的に持ち出さなければならなかった。今日の内部関係者は、Dropbox™、Google Drive、その他のオンラインストレージサービスを使用して、雇用主や侵入したネットワークからデータを取り出すことができる。盗まれたデジタル情報（それが内部脅威であれ外部脅威であれ）について議論する際に留意すべき重要な違いは、犯罪者が盗むのはオリジナルの記録ではなく電子コピーなので、盗まれた記録が元の場所に残っており、盗難を検出して証明することが困難になるということである。

コンピュータ捜査・調査の初期には、東欧のハッカーが**コンピュータへの侵入**を開始し、その後に**恐喝**を行っていた。サイバー犯罪者は、企業のネットワークに不正にアクセスし、機密情報を盗み出し、次のような婉曲的な脅迫を記載したメールを送信する。「当社はウクライナのコンサルティングセキュリティ会社です。御社のシステムのセキュリティスキャンを無料で実施しました。私たちは脆弱性を発見しましたが、それを有料で修正いたします。弊社の信頼性を証明するために、お客様のシステムが危険にさらされているかもしれないという弊社の主張を裏付けるための情報を添付しました」これらには、CEO のアカウントからの機密メールやアカウントとパスワードのリスト、あるいはハッカーが被害者の内部ネットワークにアクセスしたことを証明するあらゆる添付ファイルが含まれていた。メッセージには、「弊社に依頼する必要はありませんが、他の誰かがこれらのセキュリティホールを見つけて他の目的に使用しないという保証はできません」といった、暗黙の脅迫が続く。言い換えれば、犯罪者は「金を払え、さもなければ報いを受けることになる」と言っていたのだ。

- **社内関係者による脅迫の脅威：**

セキュリティ会社によると、**内部関係者による脅迫の脅威**が増加している。サイバー空間では、従業員は元の雇用主に対してネガティブキャンペーンを展開できるようになった。解雇されて不満を抱いた従業員が作成したウェブサイトを削除するために身代金が支払われた。約 200 人がこのウェブサイトに参加し、同社とその経営陣を中傷するコメントを投稿した。コメントの中には機密情報を含むものもあれば、捏造されたものや真実ではないものもあった。

不満を持ったあるいは退職した従業員による内部データの盗難も、組織や企業にとってサイバー犯罪のリスクである。従業員は、新しい雇用主の下で仕事を始める際に、知的財産情報を盗んで持ち出すかもしれない。不満を抱いた従業員は、情報を公に漏らして会社困らせたり、製品製造に使用されているシステムに損害を与えて現従業員に身体的損害を与えるなどして、復讐や報復を企てることがある。

- **マルウェア：**

  マルウェアとは、悪意のあるソフトウェアを指す言葉で、ウイルス、トロイの木馬、ワーム、スパイウェア、ランサムウェアなどを含む。マルウェアはコンピュータシステムに感染し、ルーチン（ルーチンが複数の場合もある）を自動的に実行するために使用される。例えば、マルウェアはバックドアをインストールし、被害者のコンピュータにリモートアクセスできるようにしたり、ユーザー名やパスワードを収集して攻撃者に情報を送信したりするかもしれない。その他のマルウェアは、児童ポルノ画像や、コンピュータソフトウェア、音楽、ビデオなどの著作権保護された素材を提供するために、被害者のコンピュータ上に配信システムを構築することがある。マルウェアは**ルートキット**をインストールすることもできる。ルートキットとは、被害者のコンピュータのオペレーティングシステムを変更し、主要な機能を自分の機能に置き換えることで、ステルス性を維持し、検出されずに存在し続けるソフトウェアである。マルウェアはまた、被害者のコンピュータを制御するために使用され、ゾンビコンピュータとして電子メールスパムを送信したり、分散型サービス拒否（DDoS）攻撃のエージェントとして使用されたりする。

  マルウェアは、実行可能プログラムとして、またはマルウェアをホストするウェブサイトへのリンクとして電子メールに配信されることがある。攻撃者は、受信者が添付ファイルを開いたり、リンクをクリックしたりするようにソーシャルエンジニアリングしなければならない。ウイルス対策ソフトは、電子メールの添付ファイルとして送信される実行可能プログラムをブロックすることができる。ただし、マルウェアを含む可能性のあるウェブページへのリンクは、電子メールシステムではなくウェブブラウザを介してコードが侵入してくるため、コンピュータへの別の扉を開いてしまう。電子メールの添付ファイルは、PDF や Microsoft Word 文書など、どのようなタイプのファイルでもかまわない。実行可能プログラムは文書ファイル内に隠されている。Microsoft Word 文書には、マクロの形で隠されたコードが含まれている場合がある。受信者が Word でマクロを有効にすると、マルウェアが実行される。多くの場合、マルウェアはセキュリティプログラムに偽装され、マルウェアを削除すると言われているが、実際にはマルウェアをインストールしてしまう。マルウェアは、攻撃者が必要とするほぼすべてのアクションを実行できる。

  ランサムウェアとスケアウェアは、経済的利益を目的として広く使用されている 2 種類の悪意のあるコードである。**ランサムウェア**は、被害者のコンピュータのデータを暗号化してデータにアクセスできなくするマルウェアである。犯人は、データを使用可能な状態に復元する暗号キーや暗号コードを提供する前に、恐喝金を要求する。ランサムウェアは通常、"CryptoLocker" [66] のようなトロイの木馬の添付ファイルとして電子メールメッセージに含まれて配信される。これらの活動は高度に自動化されており、犯罪者はボットネットを使用してマルウェアを配布し、被害者のデータを復号化するキーをリモートサーバーに提供し、指定された時間内に支払いが行われない場合はキーを自動的に消去するようにタイマーが設定されている。身代金の支払いは、Bitcoin（ビットコイン）やその他のデジタル通貨を使って行うことができ、被害者が支払う金額は、個人の場合は 100〜300 ドル、その他の団体の場合は数千ドルに及ぶ。これまでは 1 対 1 のビジネスだったマルウェアの市場が進化している。今日、開発者はランサムウェア・アズ・ア・サービス（Ransomware as a Service）を販売し、犯罪者には無償でマルウェアを提供する一方、受け取った身代金の 40〜50% を**上納させている**。2016 年の調査によると [67]、ロシアのランサムウェアのリーダーの平均年収は 9 万ドルである。被害者の負担は増大している。2015 年、FBI のインターネット犯罪苦情センター（IC3）

66 http://www.trendmicro.com/vinfo/us/security/definition/ransomware
67 https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf

は、ランサムウェアによる被害を受けた 2,453 人の被害者から通報を受け、その経済的損失は合計 1,620,814 ドルになった[68]。

スケアウェアは、虚偽の説明に基づいて、ウイルス対策保護などの不要なソフトウェアを被害者に購入させるようにソーシャルエンジニアリングするために使用される悪意のあるコードである。トライデントトリビューナル作戦は、約 96 万人の標的にスケアウェアを配信し、偽のセキュリティソフトウェアを購入させて 7,100 万ドル以上の損害を与えた国際犯罪者組織に焦点を絞った法執行機関のタスクフォースだった[69]。この計画は、消費者を騙して彼らのコンピュータを悪質なスケアウェアに感染させるというものだった。このスケアウェアは、被害者のコンピュータが多数のマルウェアに感染しているというポップアップ警告を表示し、存在しない問題を解決するために偽のアンチウイルス・ソフトウェアを購入するよう被害者に強要した。この事件には、FBI とウクライナ、ドイツ、オランダ、イギリス、ラトビア、カナダ、ルーマニア、キプロス、デンマーク、オーストリアの法執行機関が関与した。

- **サービス拒否（DoS）攻撃：**

  サービス拒否（DoS）は、被害者のサービスを過負荷により能力ダウンさせるために使われる攻撃手法である。攻撃者は、標的のマシンやネットワークにジャンクデータリクエストを殺到させてそれらを圧倒する（まるで消防ホースから水を飲むようなものである）。あまりにも多くのデータ要求がリソースを消費するため、正規ユーザーはサービスへのアクセスができなくなる。分散型サービス拒否（DDoS）攻撃は、異なる IP アドレスの数千または数百万のマシンが、標的となるシステムに継続的なデータ要求を殺到させ、正規ユーザーや顧客のサービスを拒否する。DDoS 攻撃には感染した数百万台のゾンビマシンが関与し、攻撃の時間とターゲット IP アドレスを特定する指揮統制マシンからの指示を受けるために待機していることがある。

  ハクティビストはサイバー活動家である。彼らは、DDoS 攻撃でウェブサイトをシャットダウンすることにより、社会の変化や不正と思われるものに対して電子的に直接行動を起こす。最もよく知られているハクティビスト集団のひとつが、「**Anonymous（アノニマス）**」である。Anonymous は、政府、企業、宗教のウェブサイトに対して、注目を集めたいくつかの DDoS 攻撃を行ったとされている。アサンジの復讐作戦は、2010 年後半にウィキリークス（WikiLeaks）が米国の外交秘密を公表するのを阻止しようとしたことに抗議して、Anonymous が複数の金融機関やクレジットカード会社に対して行った協調 DDoS 攻撃である。ジュリアン・アサンジ（Julian Assange）は、リークされた文書や通信を公開するウィキリークスの創設者であり発行者である。米国政府による法的脅迫を受けて、Amazon.com はウィキリークスを自社のサーバーから削除し、MasterCard、Visa および PayPal はウィキリークスへのサービスを停止した。これに抗議して、Anonymous は MasterCard、Visa および PayPal のメインサイトに対して DDoS 攻撃を仕掛け、サイトは一時ダウンし、推定 550 万ドルの損害を被った。[70]

- **個人情報窃盗：**

  個人情報窃盗とは、他人の個人識別情報（PII）を経済的利益のために利用することを指す。PII とは、個人の氏名、生年月日、ソーシャルセキュリティナンバーなどのことである。米国においては個人情報窃盗だけでは FBI は犯罪と見なさない。犯罪は、窃盗犯がその情報を使って何をした

68 https://pdf.ic3.gov/2015_IC3Report.pdf
69 https://www.justice.gov/opa/pr/payment-processor-scareware-cybercrime-ring-sentenced-48-months-prison
70 https://nakedsecurity.sophos.com/2013/01/27/not-so-anonymous-anonymouses-head-off-to-prison-over-paypal-DDoS/

かによって決まる。PII が銀行口座の開設やアクセス、クレジットカードや住宅ローンの申し込み、不動産や自動車の購入に使用された場合、実際の犯罪が発生し、加害者に利益がもたらされる。米連邦取引委員会（FTC）の報告によると、2020 年には 2019 年の 2 倍にあたる約 140 万件の個人情報窃盗事件の報告を受けた。失業保険給付金を狙った個人情報窃盗は、2019 年に記録された 12,900 件に対し、約 394,280 件であった。[71] 場合によっては、PII データはコンピュータ侵入によって取得され、犯罪者は数千人または数百万人の PII を得ることになる。このような場合、侵入または許可されたアクセスは、その後の PII の使用と同様に犯罪となる。

- **テロ行為：**

  FBI は**テロ行為を（米国連邦規則集 28 編 0.85 節に従い）**[72]「政治的または社会的目的を推進するために、政府、市民、またはその一部を威嚇または強制するために、人または財産に対して武力または暴力を不法に行使すること」と定義している。テロリストはインターネットとテクノロジーを利用して世界規模の接続性を活用し、自らの目的と活動に対する支援を獲得する。彼らはテクノロジーを使ってプロパガンダを広め、新しいメンバーを募集する。彼らはイデオロギーに基づいて暴力を振るうよう新兵を急進化させ、商品を販売するサイト、支援者からの寄付、送金システム、慈善団体などを通じて活動資金を調達するためにサイバース空間を利用することができる。テクノロジーは、世界中の視聴者と募集プール、そして活動を計画し実行するための安全な通信を提供する。

- **コンピュータ不正侵入：**

  コンピュータ不正侵入は、技術を道具としてもターゲットとしても使用し、システムに保存されている価値のあるものを取得するためのハイテク電子窃盗と見なすことができる。この種の不正侵入者を示す一般的な用語は、ハッカーである。ハッカーとは、脆弱性や弱点を突いてセキュリティ技術を突破し、ネットワークにアクセスする者のことである。ハッカーの被害者には、金融機関、政府、医療施設、Facebook、Target、Home Depot、民主党全国委員会、さらには 2016 年米国大統領候補のヒラリー・クリントン（Hillary Clinton）まで、あらゆる人々が含まれる。

- **標的型サイバー攻撃：**

  標的型サイバー攻撃（APT）の活動とは、被害者のネットワークを攻撃して不正アクセスを行い、そのアクセスを維持し、長期間にわたって検知されないようにするものである。APT 攻撃は、外国政府が支援するハッカー集団に関連するのが最も一般的だが、社会的過激派や組織的犯罪集団の場合もある。これらのグループは訓練を受けており、十分な資金があり、スタッフやインフラなどの十分なリソースを備えている。多くの人は、APT チームをハッカーの「代表チーム」とみなしている。彼らはアクセスを得るためにさまざまなテクニックを使用する。

  APT 攻撃者は、悪意のあるコードを含む添付ファイルや、チームによって侵害されたウェブサイトへのリンクを含む電子メールメッセージを介して**スピアフィッシング**を使用することが多く、これらによってネットワークへの最初のアクセスを得ることができる。一旦侵入すると、彼らは足場を広げるために弱点を探す。彼らは、電子メール サーバーなどのサービスで追加のアカウントを取得するために使用できるツールやマルウェアをダウンロードする。Outlook のような電子メールクライアントはサーバーを継続的にチェックしているため、ハッカーは数分で何百ものアカウントとパスワードを取得することができる。この時点で、彼らはマルウェアを削除し、将来の使用の

71 https://www.cpomagazine.com/cyber-security/identity-theft-doubled-during-the-pandemic-as-fraudsters-targeted-covid-19-relief-payments/

72 https://www.law.cornell.edu/cfr/text/28/0.85

ために新しいアカウントを抜き出す。その後、彼らはデータを探し始める。多くのユーザーが重要な情報をメールに保存しているため、メールアカウントは、プロジェクトや開発、人事、連絡先に関する優れた情報源となる。彼らはまた、他の保管場所を探し、盗み出す情報の収集を開始する。中国などの国々は、防衛情報だけでなく、ビジネスやベンダーの情報にも関心を持っている。現実的には、自国に情報を提供するような諜報活動は、外国企業とのビジネス交渉において大きな利点となる。

- **マネーロンダリング：**
  今日の**マネーロンダリング**活動では、サイバー犯罪者が違法行為から得た資金を洗浄するために暗号通貨を使用することが多い。不正資金を仮想通貨に変換し、その後、複数の取引所や取引を経由して、ミキシングやタンブリング、その他のオンチェーン隠蔽技術を用いて再び法定通貨に戻すことで、犯罪者は資金の出所を隠し、最終的に資金を金融システムに戻して、さらにプレイスメント（犯罪収益を金融システムに組み込む段階）やレイヤリング（資金の出所を不明瞭化する段階）の手法を用いることができる。

- **暗号通貨詐欺と不正行為：**
  イニシャル・コイン・オファリング（ICO）や暗号通貨投資スキームの増加により、詐欺師が投資家を騙す機会が発生している。投資詐欺、偽の ICO、株価操作詐欺などはすべて、暗号通貨にまつわる誇大広告を悪用して、無防備な個人を騙してきた。

- **クリプトジャッキング：**
  クリプトジャッキングとは、疑うことを知らないユーザーのコンピュータやデバイスの処理能力を乗っ取って、本人の同意なしに暗号通貨をマイニングすることである。サイバー犯罪者はマルウェアを配布したり、あるいは脆弱性を悪用して被害者のデバイスにマイニングソフトウェアをインストールしたりして、電気代の増加やデバイスのパフォーマンスの低下を引き起こす。

- **SIM スワッピング：**
  SIM スワッピング攻撃では、通常、集中化された暗号通貨交換アカウントが侵害され、脅威の行為者が実質的に SIM 情報を交換する。これは、悪意の行為者が使用する電話に携帯電話番号を移し、新たに受信されるモバイルのテキストメッセージや通話を受け取るという行為を指している可能性がある。このスワッピングにより、脅威の行為者は SMS ベースの 2 要素認証（2FA）コードを傍受できるようになる。多くの場合、被害者が個人のメールアカウントに同様の SMS ベースの 2 要素認証を設定していれば、悪意の行為者が被害者のメールアカウントにもアクセスでき、その結果、被害者の暗号通貨交換アカウントに不正にアクセスできるようになる。その時点で、暗号通貨資産はハッカーの暗号通貨ウォレット（または別の関連リポジトリ）に流出する。

（犯罪から）目をそらす手段としての技術

DDoS 攻撃はまた、サイバーセキュリティやインシデント対応の担当者の注意を、攻撃者が仕掛けている本当の攻撃からそらすためにも使われてきた。DDoS 攻撃は、前述のように、マシンやネットワークを圧倒し、正当な目的で利用できないようにするために設計されている。しかし、他の DDoS 攻撃は、実際には他の不正な活動を隠すための策略にすぎないにもかかわらず、攻撃ベクトルであるように見せるためにあるように見せている。。DDoS 攻撃では、攻撃者がマルウェアを忍び込ませてアクセスを維持したりデータを流出させたりしている間に、ウェブサイトやセキュリティチームの労力を消費すること

が多い。Neustar が 2015 年に発表した調査[73]によると、DDoS 攻撃はより小規模でしかもより頻繁に行われるようになっており、被害者は DDoS 攻撃が収まった後に初めてマルウェアが仕込まれていてデータが盗まれていたことに気付かされる。

第 1 章で説明したように、ランサムウェアは、DDoS の代わりにビジネスを妨害したり、対応者の注意を目的の犯罪からそらしたりするために使用されることがある。例えば、2016 年には、あるハッカー集団が[74]、フォーチュン 500 社の競合他社に雇われ、ランサムウェアを仕掛け、製品の市場投入を妨害したと主張した。

多くの場合、アドウェア、スケアウェア、ランサムウェア、さらには複雑なバックドア型トロイの木馬マルウェアなど、企業の情報セキュリティ監視・検知ソフトウェアやネットワーク・ツールにアラームを発するような明らかな「侵害のインジケーター」を持つマルウェアが使用される一方で、偶然にも他のあまり目立たないツール（多くの場合、すでに存在する正規のネットワーク管理ツール）が、サイバー犯罪者が目的を達成するために必要なアクセスや機能を提供している。調査の目をごまかすためのテクノロジーの利用は増加傾向にあり、サイバー犯罪を捜査し、犯罪者の動機とプロファイル、関連する範囲と被害者への影響を理解するために目的を切り分けるプロセスに、さらなる複雑さを生み出している。

サイバー犯罪の目的、動機、スキル

サイバー犯罪者のプロフィールは、その動機、目的、スキルによって異なる。これは行動科学の専門家にとっては新しい分野であり、実際、連続殺人犯のプロファイリングによって行動学は世間の注目を浴びるようになった。こうした研究では、暴力犯罪者のプロフィールは 30 歳から 40 歳の年齢範囲を示す場合がある。被害者によっては、被害者と同じ人種と推測されることもある。犯罪現場は、組織的であれ無秩序であれ、犯罪者の教育レベルや犯行の手口を示している場合がある。

サイバーの観点から見ると、動機は、ハッカーになろうとする「スクリプトキディ（Script Kiddies）」から、40 代の小児性愛者の男性、不満を抱く従業員、海外の組織犯罪集団、政府が支援するプロのハッカーチームまで多岐にわたる。サイバー犯罪者の年齢は様々で、13 歳のハッカーもいれば 50 代のハッカーもいる。不満を抱いた従業員が次の就職先のためにデータを盗む場合、その年齢は関係ない。通信中の言語は、犯人が外国出身で翻訳プログラムを使用していることを示している場合もある。金銭、復讐、セックス、秘密、恐喝、ゆすり、いじめ、社会活動、スパイ、自慢する権利などはすべて、サイバー犯罪者の動機となり得る。

サイバー詐欺師

詐欺計画を継続するためのツールとしてテクノロジーを使用する**サイバー詐欺師**は、経済的利益を動機としている。彼らの目的は、被害者から金をだまし取ることである。彼らは社会的に適応力があり、ソーシャルエンジニアリングや操作技術に長けている。テクノロジーのスキルはそれほど高くはないが、計画を達成するためにそれを効果的に使うことができる。彼らはナイジェリアの犯罪組織（必ずしもナイジェリアにいるとは限らない）のように組織化され、チームとして行動することができる。2014 年 12 月、警察はジョージア州アトランタ郊外で**ロマンス詐欺**や懸賞詐欺を行っていた 100 人以上のメン

73 https://www.neustar.biz/resources/whitepapers/DDoS-attacks-protection-report-us-2015
74 http://motherboard.vice.com/read/ransomware-gang-claims-fortune-500-company-hired-them-to-hack-the-competition

バーからなるナイジェリア人犯罪組織を発見した。[75]

ネットいじめ

ネットいじめの動機は、復讐、退屈、嫉妬、同調圧力、優越感、匿名性、被害者になりたくないという願望などである。これらの犯罪者は、ハイテクなコンピュータの専門家ではないが、記録を残さず消えるメッセージを送信するために使用できるアプリについて詳しい場合がある。このようないじめグループは非公式に組織されており、恒久的な階層構造はない。

ハクティビスト

ハクティビストの動機は政治的目的である。彼らは、言論の自由、人権、情報の自由に関わる問題についての認識を広めるためにテクノロジーを利用し、社会変革に取り組むことに価値を置いている。ハクティビストは組織化される傾向があるが、アノニマスグループのように構造化されたヒエラルキーがあるとは限らない。彼らはハッカー出身である傾向があり、自分たちの目的を支援するためにアクセス権を得たり、情報を公開したりすることに長けている。例えば、アノニマスは DoSer のダウンロード可能なプログラム[76]を公開し、他の人がターゲットに対する DDoS 攻撃に参加できるようにしたとされている。こうすることで、コンピュータスキルのない同好の士が DDoS 攻撃に参加し、抗議行動に参加することができる。

児童の性的搾取犯

児童の性的搾取犯は、性的満足を動機としている。小児性愛者は子どもに対する性的嗜好を持っているが、それを行動に移さない者もいる。他の犯罪者は小児性愛者ではないため、子供に性的魅力を感じないかもしれないが、子供はより扱いやすく、時には都合の良い獲物であるため、子供を（オンラインでも対面でも）標的にする。これらの犯罪者の中には非常に熟練し組織化された者もいるが、そうでない者もいる。オンライン上の匿名性を維持するために多大な労力を費やし、通信やデータ転送に暗号化されたチャンネルを使うなどして、メディアを交換する相手に注意を払っている者もいる。孤独を好む者たちは、どのソフトウェアを使うべきか、どこでデジタルメディアを気付かれずに入手または取引できるかなど、知識を共有してくれる同じような考えを持つ同志をオンラインで見つける。これらの犯罪者たちは、犯罪に対する連邦政府の罰則が厳しいため、慎重になっている場合が多い。

テロ行為

テロ行為は、政府の政策や政治、宗教、イデオロギーの変化に影響を与えるために、人々や財産に対して行われる脅迫や暴力行為と定義されている。**テロリスト集団**は洗練されており、よく組織化されており、技術にも精通している。彼らは、政府がサイバー空間を通じて彼らを追跡し、勧誘や過激化プログラム、さらには作戦計画やコミュニケーション活動を阻止するために、多大な資源を費やし、高度な訓練を受けた技術者を雇用していることを知っている。彼らの動機と目的は、プロパガンダを広め、特定の社会や価値観に敵対する過激な宗教的または政治的イデオロギーを採用する意思のある人々を過激化させることである。彼らはまた、海外での戦いに参加したり、国内でテロリストになるための人材を募集しようとしている。プロファイル分析は、これらの暴力的過激派は非常に多様であり、標準的な対象プロファイルに当てはまらないことを示している。しかし、多くの人は、テロ組織に加わるためには、

75 http://www.cbs46.com/story/25551165/police-international-nigerian-crime-ring-operates-out-of-atlanta-suburbs

76 http://anonhacktivism.blogspot.com/2013/06/dos-tools-2.html

次の3つの要素が必要とされるという点で一致している。それは、不満、イデオロギー／物語、そして動員があることである。サイバー空間は、特定のグループ（または民族）の迫害などの不満やそのイデオロギー／物語に関する世界的なプロパガンダを促進することによって、テロリストの勧誘者を支援する。サイバー空間によって促進される3番目の要素は動員であり、過激派はオンラインで同じ考えを持つ人々と交流し、行動を起こして暴力行為を実行する動機を得ることができる。

コンピュータハッカー

自分のスキルをテストし、セキュリティプログラムの動作を理解するためにシステムに侵入するコンピュータハッカーは、倫理的ハッカーまたは**ホワイトハットハッカー**と呼ばれる。彼らは組織化されており、組織によってネットワークを侵害する権限を与えられた専門家である。彼らの目的は、データやシステムを盗んだり破壊したりすることではなく、その活動を契約上の侵入テストを行うことである。その後、セキュリティ上の問題を組織に報告し、その解決方法を提案する。

ブラックハットハッカーとは、個人情報窃盗を目的としてクレジットカード番号や個人識別情報（PII）を盗むために不正アクセスを行うハッカーである。これが本当のコンピュータ犯罪者である。彼らの目的と動機は、個人的利益、金銭的利益または別の何らかの利益を得ることであり、場合によっては大混乱を引き起こすことである。彼らは気に入らない企業や団体に対してDDoS攻撃を行い、ハッキング技術やネットワークのセキュリティシステムを突破することに非常に熟練している。

グレーハットハッカーは、ホワイトハットハッカーとブラックハットハッカーの中間に位置する。これらのハッカーはコンピュータの専門家であり、所有者の知識や同意なしにシステムに侵入することがあるが、ブラックハットハッカーのような悪意や邪悪な意図はない。彼らは、発見したセキュリティ問題を、サイト所有者に直接報告するのではなく、公共のフォーラムで報告することがある。

「**スクリプトキディ（Script Kiddie）**」は、インターネットでハッキングについて学び、既存のスクリプトや他の人によって作成されたコードを実行してみる。というのは、自分でコードを書くスキルがないからである。彼らはコードをコピーし、それが実際にどのように機能し、何をするのかを完全に理解することなく実行する。攻撃対象は必ずしも特定の組織ではなく、むしろIPアドレスであるため、どのシステムを攻撃しているのかさえ気づかないこともある。スクリプトキディは、単独行動を好み、組織化を避ける傾向があり、意図や自覚がないまま、システムに損害を与えることがある。これらの個人は、主に仲間の間で注目を集めるために自己宣伝を動機としている。彼らはインターネットリレーチャット（IRC）を通じて得た情報やスクリプトを仲間と共有することもある。

APTチーム

APTとは、サイバー犯罪者が明確な目標と目的を持って行う「標的型サイバー攻撃（Advanced Persistent Threat）」活動を指す。**APTチーム**は、最も洗練された献身的なハッカー集団である。高度な訓練を受け、十分な資金を持つ彼らの目的は、組織化されたサイバー犯罪グループ、競争市場の利害関係者、および／または国家政府組織である可能性のあるタスクマスターによって指示される（そして時には、これらのグループ間の明確な違いが定義されていない場合もある）。彼らは、防衛兵器計画、競争力のある医学研究、物流サプライチェーン情報、あるいは市場に先駆けて取引を可能にする「インサイダー情報」など、非公開／保護情報を入手する任務を負っている。彼らが収集したあらゆる情報は、彼らの組織やタスクマスターにとって価値のあるものである。例えば、APTチームは、自国の関係者と取引を希望する企業との交渉会議の前に、ターゲットの従業員や製品、事業計画、ベンダーとの関係、財務／証券実績に関する企業データを収集することがある。この種の情報は、ターゲット企業の弱点を把握するなど、大きな利点をもたらし、組織は後でその弱点を利用して自らの利益のために利用する方法を立案することができる。

第2章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

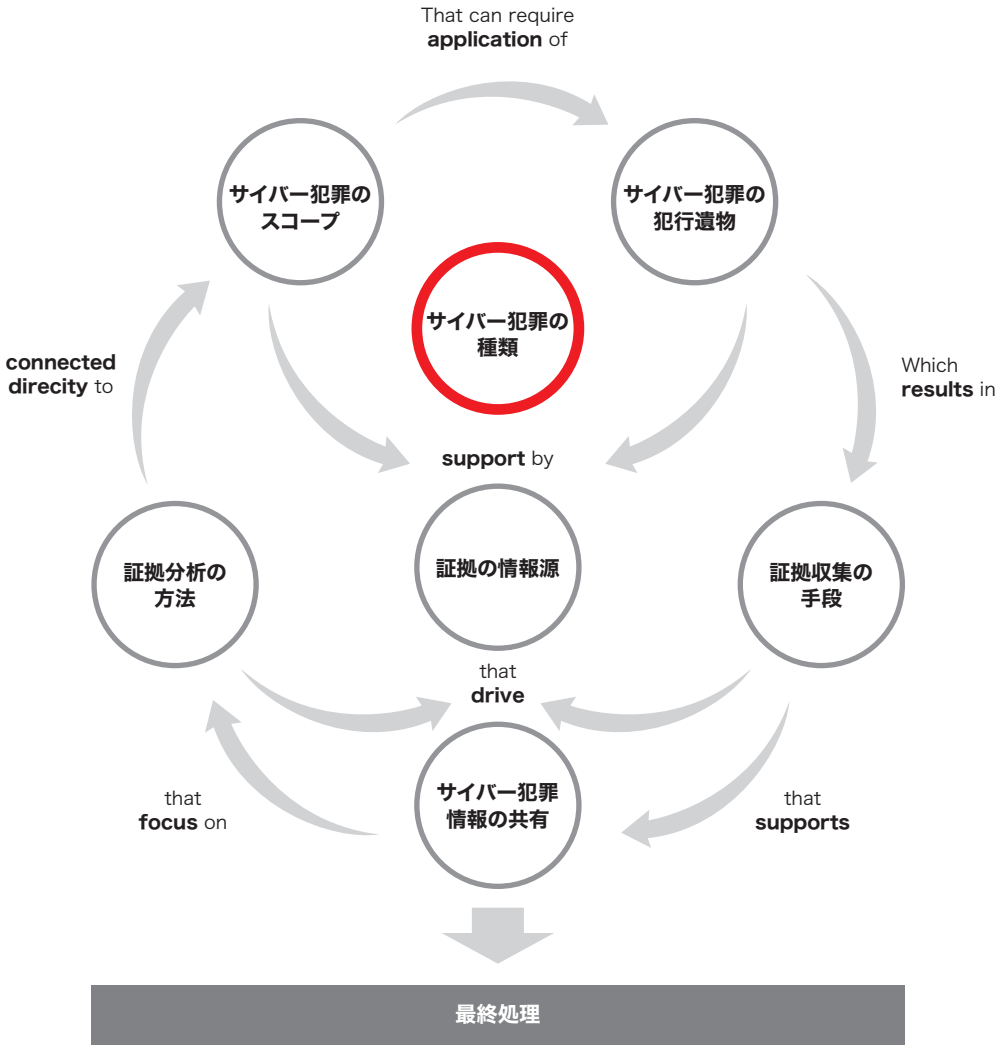


図 2-2. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークとスキルおよび知識の CIBOK 分類法（表 2-1）との関係は、機能要件が関連する役割によって異なることを示している。

表 2-1. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 2-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査管理の機能は、組織のためにサイバー犯罪の性質と種類を説明する。捜査管理の機能は、サイバー犯罪者の組織方法に応じて、サイバー犯罪者の関連する動機と意図された目的を戦術的に理解すべきである。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査管理の各役割にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。

調査 – 利用可能な情報源にあるアーティファクトを駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。知見収集、説明責任、予防啓発、捜査管理の各機能にある者が、サイバー犯罪の影響を識別するのを支援する。識別にあたっては、その犯罪に関連する目的の特性（および達成の段階）に対する評価を用いる。サイバー犯罪の種類は、証拠によって決定する。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。知見の収集、捜査手続きに関する指導を行い、関連方針および法規制に基づいて分析結果を解釈して、捜査管理や予防啓発の各機能を支援する。捜査のアプローチだけでなく、実行されたサイバー犯罪の種類に応じて、法令に関する指導や情報を共有する。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪の種類に応じて、方針に基づきながら、何を、だれに、いつ、伝えるのかを決定する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第2章:レビュー

1. 「サイバー犯罪」とは

答え：コンピュータを使用して行われた犯罪。

例：ツールとして、ターゲットとして、または捜査・調査の目をそらすものとしてのコンピュータ。

2. 犯罪の目的と動機とは

答え：個人または組織を混乱させたり損害を与えたりする競争的または個人的な利害関係。

例：破壊活動、妨害行為、窃盗／詐欺、スパイ活動。

3. サイバー犯罪者のプロファイルとは

答え：目的を達成するためにコンピュータや関連サービスを雇ったり利用したりする犯罪者の持つ技術的能力。

例：反社会的、恐喝主義者、破壊主義者、無政府主義者、泥棒、スパイ。

4. サイバー犯罪者の組織構成とは

答え：個人として、または同様の動機や方向性を持つグループとして、目標を達成する。

例：ハッカー、サービスプロバイダ、サービス加入者、客観的な犯罪の加害者。

5. サイバー犯罪者が保有するスキルや知識とは

答え：対象となるシステム、プロセス、または人物に関する技術的および手順的な知識。

例：スクリプトキディ、雇われハッカー、APT アクター、不正なトレーダー／出納係／従業員。

6. 2014 年以降のサイバー犯罪の進化経緯とは

答え：より洗練され、より頻繁に、よりインパクトのあるものと進化している。

例：選択または利便性のターゲット、サービスとしてのボットネット、ダークウェブサービス、ランサムウェアが 600% 増加。

7. サイバー犯罪と人的要因の関係とは

答え：サイバー犯罪の加害と予防の両方に影響を与えるもの。

例：被害者学、加害者の目的、結果、およびインシデント対応。

ケーススタディ2:サイバー犯罪の「ABC」

- **犯罪**：支払い詐欺
- **容疑者**：IT 管理者
- **手段**：許可されたアクセスの不正使用
- **動機**：個人的な利益
- **機会**：不適切な財務システム管理

サイバー犯罪行為が犯罪として訴追されるためには、法律に違反しなければならない。これは、サイバー犯罪者の責任を追及する上で最大の障害のひとつである。この問題を説明するには、まずサイバーセキュリティの ABC を理解しなければならない。

- (A) ttack（攻撃）：攻撃とは、被害者のネットワーク、システム、デバイスへのアクセスを試みることである。攻撃は、侵入や窃盗を試みるというような物理的な犯罪の代表例である。
- (B) reach（侵害）：侵害とは、脆弱性（脆弱な暗号化や設定、証明書やアカウントの乗っ取り、不十分なサイバーセキュリティシステムなど）を悪用して、被害者のネットワーク、システム、デバイスに不正にアクセスすることである。侵害は、強盗のような物理的な犯罪の代表例である。サイバー犯罪においては、侵害は多くの場合（企業の利用規約やその他のポリシーによる）ポリシー違反であるが、通常は犯罪として体系化されていない。
- (C) ompromise（不正アクセス）：不正アクセスとは、被害者のネットワーク、システム、またはデバイスへのアクセスを利用して、データの盗難、恐喝（ランサムウェア経由）、システムの混乱などの目的を達成することである。不正アクセスは、窃盗、詐欺、横領、財産の破壊などのような物理的な犯罪の代表例である。

攻撃において、アクセスブローカーはアクセスを悪用し、認証情報を操作してコンピュータを攻撃し、アクセスを維持し、そのアクセスを販売することで、コンピュータ詐欺および不正使用防止法に違反する。ブローカーからアクセス権を購入するサイバー犯罪者は、被害者のシステムを不正にアクセスして情報を盗んだり、恐喝を働いたりする犯罪を行う。ただし、環境を操作したり変更したりすることなく、システムに侵入してアクセス権を行使する **APT アクター**は、環境にアクセスしたことだけが罪となる。攻撃と不正アクセスでは明らかな犯罪が行われているが、侵入ではそうではない。不正アクセスに関心を持つ第三者を支援するためにアクセスを利用して利益を得ている執拗な脅威の行為者を起訴するのは非常に困難である。さらに、法執行機関はサイバー犯罪を誤って起訴することがよくある。検察官は与えられた罪状に基づいて捜査を行うため、法令に適合しない罪状がサイバー犯罪者に何らかの罰則をもたらす可能性は低い。

これらの複合的な課題は、サイバー事件の複雑さと、サイバー犯罪捜査官とサイバーセキュリティ専門家の双方がサイバー犯罪の捜査と起訴を調整する必要性を示している。

ケーススタディ：サイバー犯罪の複雑さ

会社の最高財務責任者（CFO）が横領と思われる取引を承認した記録がある事件の捜査のために**サイバー犯罪の調査員**が雇われた。事件を報告して捜査を要請した CFO は、支払いがどのように行われたかは知らなかったと主張した。

調査員はまずネットワークログを分析し、IT 管理者がパスワードスニッファーを使って CFO のコンピュータと財務システム間の暗号化された認証情報を取得していたことを発見した。その後、管理者はフリーウェアを使用してパスワードを解読し、CFO のコンピュータの RDP セッションを介して請求書を作成した。さらに捜査を進めると、同じ IT 管理者のための偽の法人の海外口座に支払いが行われていたことも判明した。

調査員はさらに取引を分析し、CFO の認証情報が請求書の作成と支払いの承認の両方に関連していることを突き止めた。CFO は通常、請求書を自分で作成しないため、これは疑念を引き起こした。その作業は買掛金担当者が実行し、支払いには通常、整合性を確保するために 2 人の担当者が関与する。同社の IT スタッフにインタビューした後、調査員は現在の IT 管理者が以前は会計手続きに精通した監査役であったことを知り、容疑者を特定して関係する法執行機関に通報した。法執行機関は管理者を尋問し、彼の自宅のコンピュータを分析したところ、その時点で管理者は犯罪を自白した。

当初は CFO による横領のように見えたが、実際は管理者による窃盗だった。捜査では、同社には 2 要素認証、第三者の承認なしに CFO が支払いを投稿した場合の警告、およびその他のセキュリティ対策が欠けていたことも明らかになった。このケーススタディは、犯罪の第一印象が必ずしもすべての事実を物語るわけではないこと、また、犯罪を行う機会を犯罪者に与えないように組織が強力なセキュリティ対策を講じなければならないことの両方を示している。

第3章

サイバー犯罪のアーティファクト

はじめに

あらゆる犯罪は証拠を残す。犯罪は単独の行為ではなく、いくつもの行為が積み重なって違法行為となる。したがって、捜査官や組織の管理職が犯罪者の手口である「TTP」（Tactics, Techniques and Procedures：戦術、技術および手順）を理解していれば、サイバー犯罪の計画や準備、管理から実行を反映する形跡や手がかりを得ることができる。無差別に行われたかまたは計画的に行われたかにかかわらず、それらの痕跡は犯罪の特性を識別するのに役立つ。このような痕跡は一般に「インジケーター」や「アーティファクト」と呼ばれる。

サイバー犯罪捜査およびインシデント調査の文脈では、インジケーターとアーティファクトの違いは以下のとおりである。

不正アクセスのインジケーター（IoC）と攻撃のインジケーター（IoA）

- 不正アクセスのインジケーター（IoC）とは、データ侵害、侵入、またはサイバー攻撃が発生したことを示す動作またはデータのことである。これらは、システムの脆弱性を特定し、サイバー攻撃の発生を確認する上で非常に重要である。
- 攻撃のインジケーター（IoA）は、攻撃で使用されるマルウェアやエクスプロイトの種類を問わず、攻撃者が何を達成しようとしているのかを検出することに重点を置いている。

アーティファクト

- デジタルアーティファクトは、エンドユーザーの活動に基づいて残される項目である。これらは、実際に何が起こったかを示すより優れたインジケーターであり、個人の意図や心境など、コンテンツでは決して明らかにできない詳細を示すことができる。

IoC や IoA は、サイバー攻撃の発生を確認し、攻撃者の意図を検出するために使用される。一方、アーティファクトは、実際に何が起こったかを示す、より優れたインジケーターであり、IoC や IoA で示される情報よりも多くの情報を明らかにすることができる。インジケーターは、ネットワーク、エンドポイント、アイデンティティサービス、およびデバイスの使用状況のモニタリングを通じて観察される。アーティファクトは、このようなインジケーターの動作分析と、関連する機器やログのデジタルフォレンジック調査を通じて発見される。

過去 10 年間で、組織が IoC と IoA の両方を検出して対応するために使用されるインテリジェンスを作成、管理、維持、およびキュレートする方法には、さまざまな傾向があった。

- 高度化の進行：IoC はより洗練されて包括的になり、IP アドレス、ドメイン、ファイルハッシュだけでなく、様々なタイプのインジケーターを包含するようになった。今日、IoC は、行動パターン、戦術、技術、手順（TTP）、脅威の行為者とその動機に関する文脈情報とともに、Mutex[77]、Imphash[78]、Fuzzy Hash[79] といった、より難解なインジケーターを含むことが多い。

77 Lenny Zeltser - “Looking at Mutex Objects for Malware Discovery & Indicators of Compromise” https://www.sans.org/blog/looking-at-mutex-objects-for-malware-discovery-indicators-of-compromise/

78 Mandiant - “Tracking Malware with Import Hashing” https://www.mandiant.com/resources/blog/tracking-malware-import-hashing

79 Niklolaos Sarantinos et al - “Forensic Malware Analysis: The Value of Fuzzy Hashing Algorithms in Identifying Similarities” https://ieeexplore.ieee.org/document/7847157

- 脅威インテリジェンスプラットフォームとの統合：IoC と脅威インテリジェンスプラットフォームの統合は組織では一般的になっており、信頼できるソースから収集・集約・整理された IoC にアクセスし、セキュリティインフラに組み込むことができる。事前予防脅威ハンティング、リアルタイムのアラート、自動化されたレスポンス・アクションが、IoC によってますます促進されている。

- コンテキスト分析の重視：正当なインジケーターと悪意のあるインジケーターを区別するために、IoC の文脈分析が重視されるようになってきている。文脈分析では、IoC をネットワークトラフィックログ、エンドポイント遠隔測定、ユーザー行動分析などの追加データソースと関連付けて、潜在的脅威の重大性と関連性を正確に判断する。

- 共有とコラボレーション：組織間、産業部門間、および国境を越えて IoC を共有することで、サイバー脅威に対するコラボレーションと集団的防御が向上した。情報共有分析センター（ISAC）や政府主催の脅威インテリジェンス共有プログラムのような取り組みは、IoC や実用的なインテリジェンスの交換を促進し、世界的な規模でサイバーセキュリティ態勢を強化する。

- 脅威ハンティングに焦点：IoC は、セキュリティチームがネットワーク内の侵害の兆候を積極的に探す事前予防脅威ハンティング活動において、重要な役割を果たす。調査の出発点として IoC を活用することにより、組織は従来の検出メカニズムを回避する可能性のあるステルス性のある脅威や脆弱性を発見することができる。

しかし、IoC の使用には欠点も予想される。

- 既知の指標への過度の依存：IoC は、主に悪意のある活動の既知のパターンに基づいており、新規の脅威や以前には見られなかった脅威を検出できない場合がある。洗練された敵対者は、戦術、手法、手順（TTP）を変更したり、既知の IoC では表示されないカスタムメイドのマルウェアや関連インフラを使用したりすることで、検知を回避することができる。

- 偽陽性と偽陰性：IoC は、偽陽性（良性の活動を悪意があると誤って識別する）または偽陰性（実際の脅威を検出できない）を生成する可能性があり、過検知によるオペレーションの疲弊やインシデント対応の非効率性につながる。IoC の動的な性質は、誤報を最小限に抑え、正確な検出を確実に行うために、継続的な調整と検証を必要とする。

- 限定範囲：IoC は、既知の脅威に関連する特定の指標のスナップショットを提供するが、敵対者の動機、戦術、および目的に関するより広範な文脈や情報が欠けている場合がある。IoC ベースの検知は、この限界を克服するために、脅威インテリジェンス分析とサイバーセキュリティリスクの文脈的理解で補完されるべきである。

- 古くなった IoC：脅威の行為者は検知を逃れるために戦術やインフラを頻繁に変更するので、IoC の寿命は限られている。古くなった IoC は、新たな脅威を特定する上でもはや適切でも効果的でもない場合があり、継続的な更新と脅威インテリジェンスフィードの充実が必要になる。このキュレーション（収集・集約・整理）プロセスは困難になることがあり、使用するインジケーターの妥当性を確保するために努力しなければならない。

- プライバシーと法的懸念：IoC、特に個人を特定できる情報（PII）や機密データを含むIoCを共有することは、特に規制のある業界やデータ保護規制の厳しい管轄区域において、プライバシーや法的な懸念を引き起こす可能性がある。組織は、外部当事者とIoCを交換する場合、適用されるプライバシー法および情報共有契約を遵守しなければならない。

IoCは依然としてサイバーセキュリティ防御の貴重な要素であるが、その効果的な活用には、IoCの長所、限界、そしてより広範な脅威の状況を考慮したバランスの取れたアプローチが必要である。

本章では、活動のステージ（段階）を示す証拠として、また犯罪に関係のある活動の兆候または属性として評価可能なサイバー犯罪のアーティファクトについて詳細に説明する。さらに、捜査官・調査員がこういったアーティファクトを発見するのに役立つ内外の情報源について説明し、加えて組織の意思決定者や管理職が包括的な監査や評価のプログラム、または防衛・防御システムおよび手順を構築するのを支援する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の兆候とは
- サイバー犯罪のアーティファクトと兆候の違いとは
- サイバー犯罪活動におけるステージ（段階）とは
- 捜査官が使用できるサイバー犯罪のアーティファクトの種類とは
- 捜査官がサイバー犯罪のアーティファクトと兆候を見つけられる場所はどこか

サイバー犯罪のアーティファクトにおけるトピックス分類

「サイバー犯罪のアーティファクト」知識領域におけるトピックスの分類を図 3-1 に示す。

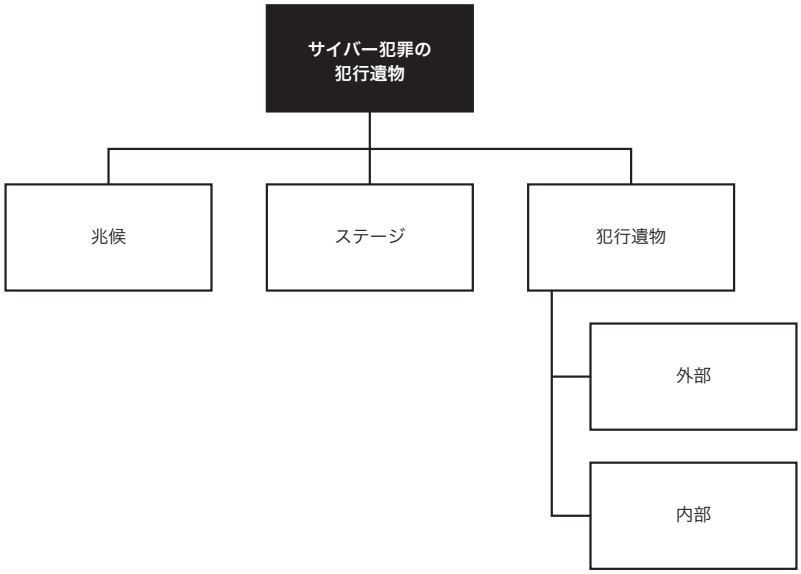


図 3-1.「サイバー犯罪のアーティファクト」知識領域におけるトピックスの分類

サイバー犯罪の侵害兆候とは

アーティファクトと証拠は互いに関係のある用語であるが、同じものを意味しない。アーティファクトとは、犯罪者が何かを「操作する」ことによって作成されるものである。たとえば、Microsoft Word の文書やその文書に関係するメタデータ（Word では、作成者や会社名、回覧先などの個人情報や、非表示のデータ（変更履歴、バージョン、注釈、隠し文字、隠しプロパティなど）が自動で保存される、またはユーザがその文書を作成したり使用したりした履歴に関するレジストリのエントリなどに相当するデータである。一方、証拠とはアーティファクトの集合である。たとえば、あるファイル内の保護情報をリムーバブルメディア（取り外し可能な媒体）上の文書に複製するといった問題と、そのアーティファクトが「どのように」関係しているのかを説明するのが証拠である。

サイバー犯罪のアーティファクトは分離・独立していることもあれば、互いに関係し合い、依存し合う場合もある。それらは技術的に構造化された場所に存在することもあれば、そうでない場所に存在することもある。たとえばコンピュータのディスクの内容であることもあれば、メモや動画記録といった、人間がやりとりを交わした結果（を記録したもの）のこともある。

サイバー犯罪のアーティファクトは関連する活動を実行するのに使われた資源や手段を明らかにする。したがって、それらに関連するものは活動の段階（ステージ）と目的に関連するインジケーターである。また、アーティファクトには内部のアーティファクトと外部のアーティファクトがあり、これらを各種の情報源（「第 5 章 証拠の情報源」で説明）から収集しなければならない。

サイバー犯罪捜査官および CSIRT メンバーのほとんどは攻撃の細部に焦点を当てる。すなわち、標的が脆弱性に対する攻撃を受けた結果生じるファイルやインターネットアドレス、ドメイン名、ハッシュ値やその他の兆候を探す。脆弱性に対する攻撃を示すこれらのインジケーターを、一般的には「不

正アクセスのインジケーター」（IoC：Indicators of Compromise）と呼ぶ。ただし、サイバー犯罪捜査官およびCSIRTメンバーがこれらの細部に焦点を当てるのは、彼らの責任範囲や経験、知識が、防御と調査を任されたシステムと関係するものに限られているからである。サイバー犯罪捜査官およびCSIRTメンバーは、自らの責任範囲がもっと広範囲であり、細部だけでなく包括的な範囲の知識が必要とされていることを認識する必要がある。

つまり、サイバー犯罪の実行前から存在していた大きいフレームワークを理解することが大切だということである。サイバー犯罪活動の過程で発生する計画、準備、および実行は、それぞれインターネットの広い範囲（どの程度広いかはサイバー犯罪のスコープによる）に「不正アクセスのインジケーター（IoC）」と呼ばれるインジケーターを残すことになる。これらのインジケーターを発見できれば、単一の標的に対する攻撃にとどまらず、犯罪を練り上げた人物またはグループの範囲や資産、影響を受けた被害者のシステムまたは従業員の範囲など、分析員がはるかに多くを理解するのを助ける。

不正アクセスのインジケーターとは、アーティファクトが関連する活動を指す。（同種の）インジケーターを説明するのに最も一般的なフレームワークはロッキードマーチン社によって開発されたもので、「サイバーキルチェーン」と呼ばれている[80]。このモデルは、最初のターゲットの特定から目的の達成に至るまで、攻撃者が実行する行動を関連付ける。

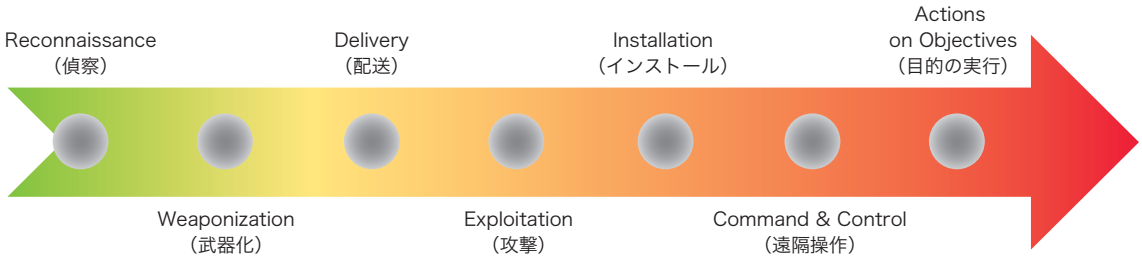


図 3-2.「サイバーキルチェーン」モデル[81]

サイバーキルチェーンモデルは単独の犯罪行為者または組織が実行する一連のできごとを示すのには効果的である。ただ、第2章で述べたサイバー犯罪組織とサイバー犯罪者のプロファイルが進化したことに伴い、サイバーキルチェーンが具体的に当てはまるケースも減ってきている。このモデルは活動を記述しているが、活動の組織や目的を表現していない。今日のサイバー犯罪は、その目的を達成するために関与しているのが個人のこともあれば、独立した組織、あるいは互いに関係のある複数組織のこともある。また、サイバー犯罪の標的となる側も、単独で標的となる場合以外に、顧客やパートナーも含めて標的となる場合がある。現在では攻撃と事前調査の活動のかなりの部分が第三者によって実行されており、侵害活動は技術的能力を有している外部の労働力に「外注」されている場合が少なくない。そのため、同時に何人もの行為者がそれぞれ異質でばらばらの目的を達成すべく行動している。

サイバー犯罪とその組織、手段、（狙いや目的別の）プロファイルは複雑である。そこで、サイバー犯罪の「ステージ（段階）」を達成するために実行されている活動からインジケーターを切り離した新しいモデルを示したのが次の図である。

80　エリック·M·ハッチンス（Eric M. Hutchins）、マイケル·J·クロッパート（Michael J. Cloppert）、およびロハン·M·アミン（Rohan M. Amin）博士、「敵対者のキャンペーンと侵入キル チェーンの分析に基づくインテリジェンス主導型コンピュータ ネットワーク防御」。http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdfを参照。

81　「サイバーキルチェーン」はロッキード·マーティン社の商標登録されている。

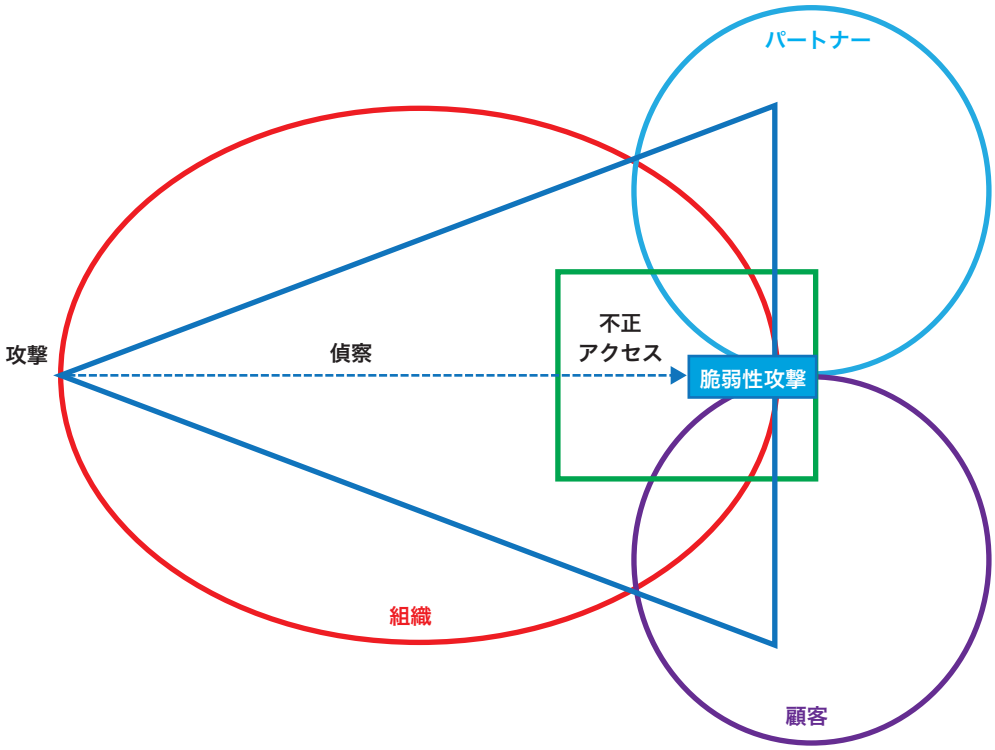


図 3-3. サイバー犯罪のインジケーター

不正アクセスのインジケーターとは、サイバー犯罪の各「段階」において目的を成功裏に達成する方法を指す。行為者はそれぞれ異なる目的を持っている。例えば、銀行決済ネットワークからの金融詐欺を意図する犯罪者は、ハッカーを雇って銀行をターゲットにし、銀行へのアクセスを提供する可能性がある。また、銀行の手続きを模倣してそのアクセスを悪用する不正な銀行技術者や、不正送金によって盗まれた資金を洗浄するためのオフショア銀行口座を使用する可能性もある。このシナリオの各行為者はサイバー犯罪を行っており、それぞれが最終的なサイバー犯罪（詐欺）の段階の目標を達成するための手順を踏んでいる。ただし、関連する不正アクセスのインジケーター（コンピュータで見つかった純粋に技術的な成果物を指す別の概念）は、さまざまな行為者と同様に固有である（ただし、さまざまな行為者が偶然にまたは同時に、少なくとも同じボットネットインフラ採用することがある）。今日のサイバー犯罪は複雑であるため、捜査から犯罪の指標や活動段階を把握しない限り、犯罪を行為者に帰属させることは非常に困難である。

サイバー攻撃と防御のさまざまなフェーズをマッピングして管理するための追加モデルと代替モデルが、過去 10 年間で広く使用されるようになった。特に、攻撃手法と対策にそれぞれ重点を置いた MITRE ATT&CK[82] モデルと D3FEND[83] モデルを理解しなければならない。

MITRE Corporation[84] は、サイバーセキュリティの防御策を理解して改善するための 2 つの補完的なフレームワーク、ATT&CK フレームワークと D3FEND フレームワークを開発した。これらのフレームワークは、サイバー脅威を特定して緩和するための構造化された方法を提供し、サイバーセキュリティの専門家に貴重なガイダンスを提供する。

82 https://attack.mitre.org/
83 https://d3fend.mitre.org/
84 https://www.mitre.org/

MITRE ATT&CKフレームワーク

MITRE ATT&CK（敵対的戦術、手法、および共通知識）は、現実世界の観察に基づいた敵対的戦術と手法に関する、世界的にアクセス可能な知識ベースである。これは、民間部門、政府、サイバーセキュリティ製品およびサービスコミュニティにおける特定の脅威モデルと方法論の開発の基盤として使用される。このフレームワークは、サイバーセキュリティの実践に共通の分類法を提供するように設計されており、脅威の検出、分析、対応のためにより構造化されたアプローチを可能にする。以下の詳細が提供される。

- 戦術と手法：**犯罪者・攻撃者**の行動は、達成しようとしている目的を表す戦術と、その目的を達成する方法を詳述する手法に分類される。この分類は、防御側が敵の行動の背後にある「方法」と「理由」を理解するのに役立つ。
- マトリックス：エンタープライズ、モバイル、クラウドなど、さまざまな環境向けのさまざまなマトリックスがカバーされている。各マトリックスは環境の特定の側面に焦点を当てており、より的を絞ったセキュリティ対策を可能にする。
- 緩和策：それぞれの手法ごとに、その手法の有効性を阻止するまたは制限するための緩和策が提案されている。これらの緩和策は、組織がセキュリティ体制を改善するために実施できる実用的な対策である。
- グループとソフトウェア：既知の敵対者グループと、それらが一般的に使用するソフトウェアに関する情報が含まれており、防御側が攻撃を識別して原因を特定するのに役立つ。

図 3-4. Mitre ATT&CK (™) フレームワークのディテールの深さの図解

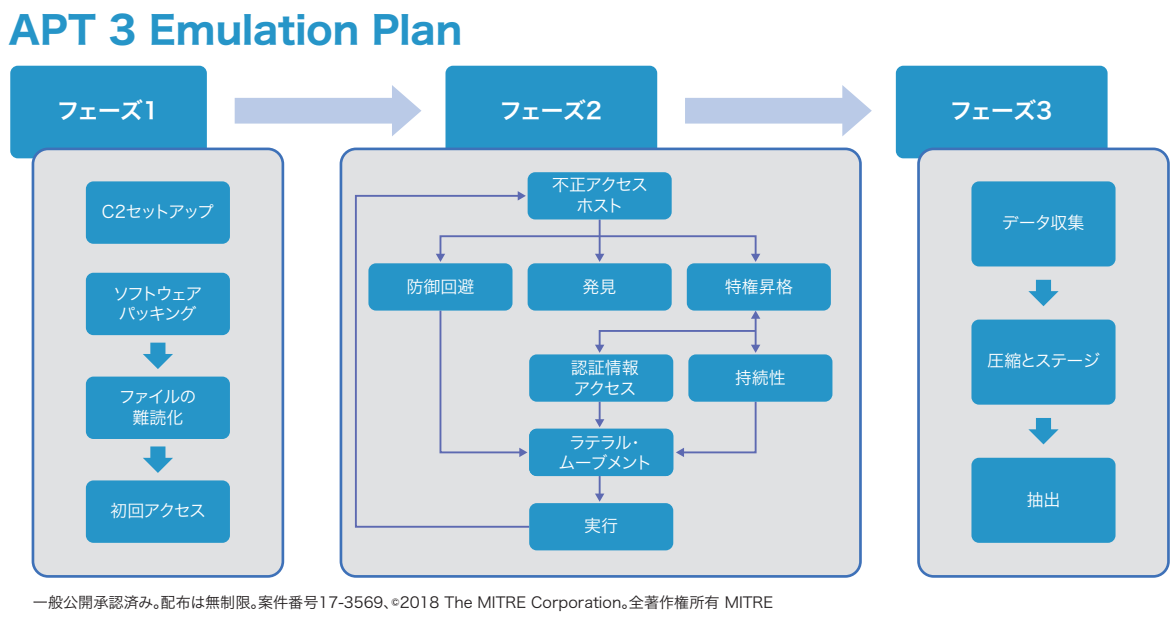
敵対者エミュレーション計画

攻撃チームと防御側の両方にとっての ATT&CK の価値を実証するために、MITRE は敵対者エミュレーション計画（Adversary Emulation Plans）[85] を開発した。これらの文書は、公開されている脅威インテリジェンスと ATT&CK フレームワークの潜在的な用途を示す青写真として機能する。これらの計画の目標は、ATT&CK で概説されているように、レッドチームが敵の戦術をより効果的に再現できるようにすることで、ネットワークと防御のテストを強化することである。この取り組みは、特定の不正ア

85 https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/adversary-emulation-library/

クセスのインジケーター（IoC）やツールへの狭い焦点を超えて、ATT&CK 行動分析の開発とともに、製品と環境のテストの改善を目指す幅広い取り組みに貢献する。

現在の脅威インテリジェンスレポートでは、マルウェア分析、初期侵入、コマンド＆コントロール（C2）戦略が強調されることが多い。しかし、攻撃者がどのようにテクニックをリンクさせ、あるいはキーボードから直接操作を行うかについての詳細な洞察は乏しい。利用可能な脅威インテリジェンスから構築されたこれらのエミュレーションプランは、このような制限を引き継いでいる。このギャップに対処するため、包括的なレッドチーム演習の経験から、ATT&CK 戦術を統合する以下のアプローチが提案される。これらの計画を策定するにあたり、これらの APT に対するエミュレーション戦略の可能性を調査するために、ATT&CK にカタログ化されている特定の APT（Advanced Persistent Threat）グループが分析された。このプロセスは、APT が使用するツールの機能を特定し、それらのアクションを模倣する代替方法を提案することを含んでいた。その目的は、実行時にある程度の柔軟性を保ちながら、オペレーターが特定の敵対者の一般的な手口を模倣できるようにすること、つまり、文書化された戦術、技術、手順（TTP）と行動を遵守できるようにすることである。一般的なレッドチーミングプラットフォームの類似アクションに適用可能なコマンドの「チートシート」を介して、さらなるサポートが提供される。下記の高レベル図は、APT3 エミュレーション戦略を構築するためのフレームワークを示している。



一般公開承認済み。配布は無制限。案件番号17-3569、©2018 The MITRE Corporation。全著作権所有 MITRE

図 3-5. 敵対者エミュレーション計画のサンプル

エミュレーション計画の例は MITRE から入手可能であり、さまざまな脅威の行為者が採用するアプローチや方法論についての洞察が得られる [86]。

MITRE D3FENDフレームワーク

MITRE D3FEND は、サイバーセキュリティ対策に重点を置いた補完的なフレームワークである。ATT&CK が攻撃者の行動を概説しているのに対し、D3FEND はそれらの行動に対する防御方法についての情報を提供している。これは、ATT&CK に記載されている戦術や手法を軽減または防止する防御手法を詳しく説明することで、組織のサイバーセキュリティ体制を強化するように設計されている。そ

86 https://attack.mitre.org/groups/G0022/

の詳細は以下のとおりである。

- 対策手法：対策は、ATT&CK が攻撃手法をリストする方法と同様に、構造化された形式で記載される。これらの対策は ATT&CK テクニックに直接マッピングされており、特定の敵対者の行動から防御する方法に関する明確なガイドを提供する。
- 分類法：サイバーセキュリティ対策の分類法が導入され、強化、検出、隔離、（囮などで犯罪者を）欺くこと、不法侵入者立ち退きなどの領域に分類される。この分類は、包括的なサイバーセキュリティ戦略の立案と実施に役立つ。
- 技術的特異性：さまざまな対策の実施と有効性に関する技術的な詳細が示され、さまざまな状況においてどのように適用できるかについての指針が提供される。

ATT&CK フレームワークと D3FEND フレームワークは共に、サイバー脅威を理解して対抗するための包括的なアプローチを提供する。特定の敵対者の行動とそれに対応する防御策を詳述することにより、サイバーセキュリティの専門家はサイバーセキュリティ戦略をより適切に計画、実施、評価できるようになる。

アーティファクト

犯罪者は検出を回避するために、被害者が通信するインターネットアドレスやファイル名などの単純なものを変更するので、不正アクセスのインジケーターに関連する技術的なアーティファクトは急速に変わる可能性がある。サイバー犯罪のインジケーターは、犯罪者が利用したシステム全体に残され、監視システムや履歴記録によって捕捉されます。これは、インターネットなどの公共システムと、個人または企業のコンピュータなどのプライベートシステムの両方を含む。IoC はサイバー犯罪が行われるたびに関連するアーティファクトから作成され、犯罪者が将来行うかもしれない変更に関係なく保存される。IoC 間の重複により、個々のアーティファクトだけではなく犯罪に調査を集中することで、キャンペーンを犯罪組織に帰属させるプロセスを開始できるようになる。

これを現実世界の組織犯罪に当てはめると、たとえば犯罪活動は従来の犯罪に例えることができる。例えば、ある組織犯罪グループが悪徳、誘拐、恐喝に関与していた場合、それらは 1 つのグループによる 3 つの個別の作戦になる。犯罪の実行方法は異なるため、犯罪の種類ごとにインジケーターは異なるが、人、交通、インフラなど、犯罪の種類間で共有される可能性のある共通の要素はある。サイバー犯罪の世界でも、ランサムウェア、クレジットカードの窃盗、スパイ行為に関与するグループがあれば、同じことが当てはまる。それぞれの犯罪には異なるインジケーターがあるかもしれないが、組織的な活動を明らかにするためにグループ化できる共通点があるかもしれない。

攻撃

作戦の目的によって、攻撃方法は異なる。他のアクションを実行する前に、攻撃者は目的を念頭に置き、それを達成するための手段を持っているはずである。例えば、攻撃者に金銭的な動機があって、可能な限り広範囲に攻撃しようとする場合、敵対的な広告で人気のあるウェブサイトにアクセスする人を標的にする広告ベースの攻撃を計画するかもしれない。特定の企業のみに興味を持つような、より的を絞ったシナリオの場合、攻撃者はリサーチやソーシャルエンジニアリングを活用して、既知の従業員のメールアドレスを収集したり、スピアフィッシングのリンクを介して従業員が最もクリックしたくなるトピックを特定したりする可能性が高くなる。

より高度な攻撃者は、標的が購入したハードウェアや提携を発表した企業を調査し、外部ネットワークに不正アクセスするのに使用できる新しいエクスプロイト（ゼロデイと呼ばれる）の開発に資金を提

供し、その後内部に侵入する可能性がある。攻撃行為の痕跡はインジケーターとみなされるが、それは標的のメカニズムの性質によって、次のことがわかるからである。

1. 特定の組織が標的として狙われたのか、それとも無差別か
2. 攻撃の対象は何だったのか（ユーザグループ、国家、その他）
3. グループの動機は何だったのか
   a. 金銭目的（ランサムウェア、カード詐欺、クレデンシャル（認証）情報窃盗）
   b. スパイ活動（長期にわたる遠隔操作や情報抜き取りが絡む標的型攻撃）
   c. 妨害・破壊工作（サービスやサーバの削除および無効化）
   d. ハクティビズム（ウェブページの改ざんやサービス妨害（DoS）攻撃）

事前調査

サイバー犯罪のインジケーターは、攻撃者が標的に関する情報をどのように収集するかに応じて、複数のソース（第5章で詳述）から見つけることができる。サイバー攻撃の事前調査は、かつては単に標的の境界防御を調査してその弱点を特定するものと考えられていた。今日では、企業やその従業員、所在地、使用されているテクノロジーに関する膨大な量のデータが公開されているため、攻撃者は攻撃活動を開始する前に、潜在的な弱点に関する知識を迅速に得ることができる。

不正アクセス

不正アクセス行為があると、ほとんどの人がまずそこからサイバー犯罪のインジケーターやアーティファクトを探し始めようとする。というのは、それは被害者組織にとって最もわかりやすく、見つけやすい（目立つ）活動だからである。サイバー犯罪の種類によっては、信頼できる「シグネチャ」が発見されると、組織が影響を受けるシステムやアプリケーションを検索できるようにする不正アクセス行為のインジケーターが構成されることがある。ウイルス対策やマルウェア対策の企業、そして侵入防御やネットワーク監視の技術は、以前に確認された攻撃者の活動の兆候を検出する機能を提供しており、場合によっては、その活動がどの作戦と相関関係にあるかを判断することもできる。

技術的なインジケーター以外にも、攻撃者の洗練度のレベルや明らかな習慣も有用なインジケーターとなる。コモディティ型マルウェアは、犯罪組織によって広く使用されている（また、犯罪組織に販売されている）が、資金力のある組織化されたグループを反映するような洗練されたレベルの独自のマルウェアが出現することもある。このような場合、攻撃は標的型であり、ボットネットを単に拡大する以上の重要な目的が犯罪キャンペーンに存在すると考えられる。

脆弱性攻撃／攻撃成功

脆弱性攻撃は、影響が確定できるまでは予測するのが最も難しいカテゴリである。脆弱性攻撃は、攻撃者が侵入に成功し、選択肢を検討し、目的（金銭窃盗、スパイ活動、破壊活動など）を実行することを意味する。脆弱性攻撃の目的は単純な場合もある。被害者ネットワーク上の多数のシステムがランサムウェアによって使用不能になった場合、目的は恐喝か妨害行為である。被害者のネットワークから大量のデータが盗まれた場合、その目的はスパイ活動（産業スパイ、国家スパイ）か窃盗である。第1章と第2章で論じたように、明らかな不正アクセス行為は、犯人が実際に持っていた目的の理解から目をそらす可能性がある。世界にはさまざまな犯罪グループが活動しており、その目的も多岐にわたります。捜査官が自問しなければならないのは「なぜ？」である。結局のところ、彼らは何に興味を持ち、どのようにそれを追求し、誰が利益を得たのかを捜査官は自問するべきである。

サイバー犯罪活動のステージ

以下のステージは、サイバー犯罪の実行中に発生する構成要素の活動を含んでいる。これらの活動に関連するアーティファクトは、関連する記述との関連において評価されるべきである。前述したように、これらの活動は、それらを実行するサイバー犯罪者や組織のプロファイルや利益／目的に応じて、独立していたり、重複していたり、調整されていたりする場合がある。これらの活動は、先に図 3-2 で説明したサイバーキルチェーンに類似しているが、単一の組織内であれ、相互に依存するサイバー犯罪者の利益によるものであれ、サイバー犯罪がどのように「共有サービス」の経済の規模と運営に発展してきたかに関連するように拡大されている。

表 3-1. サイバー犯罪活動

サイバー犯罪のステージ	説明
標的の決定	意図的もしくは機会のある標的を識別
アクセスの提供	「仮想プライベート」アクセスを提供
攻撃対象の状況をカタログ化	アクセスの種類、ホスト、サービス、データ、ビジネス部門、アプリケーションおよびデータ保存場所のクレデンシャル（認証）情報／権限などを記録
犯罪サービスの定義づけ	アクセス / 情報の登録利用者に対して提供するサービスを定義する
犯罪サービスの管理	不正アクセスが可能なホストやサービス、資格情報、その他情報の利用を管理する
サービスの維持／（検出技術に対する）防御	アクセスを防御し、可用性が高く安全なサービスを確保する
サービスの冗長化	アクセス手段を冗長化して維持する
難読化	アーティファクト／証拠の削除や各種のかく乱技法によってアクセスの種類（およびその範囲）を分かりにくくする
代替サービス	第三者に対して代替サービスを構築して提供する
目標の達成	ボットネットの拡大、利用者向けのサービス調達、破壊工作、破壊活動、窃盗などの目標を達成する

標的の決定

標的の決定とは、どの被害者が最終的に最良の結果をもたらすかを犯罪組織が判断することである。コモディティ型マルウェア（ランサムウェア、認証情報の窃盗、ボットネットファーミング）の場合、これは直接的な標的の決定よりも、どのメカニズムが最も多くの標的（スパム、フィッシング、悪意のある広告）を集めるかを特定することの方が重要かもしれない。スパイ活動、**支払いに利用されたカード**の窃盗、あるいは通信詐欺に関連する標的型攻撃の場合、攻撃者は、盗んだ情報の売却や金銭の授受といった金銭的利益という形で、自分たちの努力に見合う最高の結果をもたらす被害者を特定するため、これはより具体的になる。

アクセスの提供

アクセスを提供する際、サイバー犯罪者は自分たちのニーズに対して「仮想プライベートネットワーク」アクセスを提供する何らかのインフラを構築するか、リースしなければならない。多くの人々は、コマンド＆コントロール（C2）を誤解しており、敵対する外国からのあらゆる通信は攻撃者のインフラであると思い込んでいるが、パブリッククラウドコンピューティングや世界規模のホスティングサービスの出現により、どのネットワークでも標的となる被害者へのアクセスを容易にしたり、提供したりする可能性がある。攻撃者が、「未必の故意」となる行為者（悪い結果を望んではいないけれども、その結果が起きることを「仕方がない」として受け入れている状況）と想定される、すでに侵害されたシステムを利用して、自分たちの悪意あるインフラをホストする場合、これはさらに大きな問題となる。ボット

ネットに制御されているコンピュータの70%が「企業のファイアウォールの内側にある」と推定する人もいる。これは、既知のC2ネットワークのことである。関連システムの大半はすでに危険にさらされており、管理された環境に存在している。これらのシステムは、オンデマンドでアクセスを提供することができる。

列挙

サイバー犯罪者は標的とするホストへのアクセスに成功すると、そのホストで利用可能なアクセスの種類とサービスを記録する。関連ホストの「カタログ」は、（組織のIT管理者が開発・使用する資産管理データベースと同様に）独自の目的で開発されることもあれば、その全部または一部を購読者に提供することもある。不正アクセスされたホストへのアクセスを競合関係にある加入者に販売しようとする第三者によるボットネットの拡張がますます増えている。ホスト タイプ、サービスの構築と構成、認証情報、組織リソースに対する権限は、それぞれ関連カタログ内の貴重な商品である。

サービスの決定

サイバー犯罪者は、ホスト、サービス、アプリケーション、認証情報、組織、パートナー、顧客などに対するアクセス権を決定すると、不正アクセスされたホストまたは資産に構築するサービスの種類を定義する。当初、サービスは単なるリモートアクセスだが、その後は自分の犯罪組織やCaaSのサブスクライバーの関心に応じて進化し、より高度なサービスを含むようになる。

サービスの管理

サイバー犯罪者がアクセス権を獲得し、カタログ（およびサービス提供）を開発することに成功すると、他の情報技術リソースと同様に、加入者に提供されるアクセスを管理しなければならない。インフラが拡大するにつれて、システムをメンテナンスし、リソースを追加し、パッチを当てる必要がある。こうした行為のアーティファクトから、攻撃者のインフラが押収されると、攻撃者の身元、目的、組織に関する情報が明らかになる場合がある。

サービスの維持／防御

サイバー犯罪者のインフラが拡大し、セキュリティツールや研究者・リサーチャーによって検出されるようになると、被害者組織や自警団が攻撃者に対して報復を試みることもある。犯罪者は、被害者、自警団、その他の攻撃者による攻撃から自身のインフラを守ろうとする。

サービスの冗長化

今日、悪意のあるソフトウェアパッケージの多くは、それらを提供する犯罪ネットワークを通じて商業的にサポートされている。それらは日々洗練され、能力が高まっている。サイバー犯罪者は、マルウェアのようなカスタムツールでサービスの冗長性を引き起こし、また、既存のサービスを悪用して再構成し、サービスへのアクセスや管理が利用できるようにしようとする。

つまり、特定のインターネットアドレスへのアクセスを単に拒否するという従来のアプローチでは、サイバー犯罪者がアクセスを継続するのを防ぐのにもはや十分ではないということである。多くの場合、コマンド＆コントロールネットワーク（アドレス）へのアクセスを即座にブロックすることよりも、サイバー犯罪者が利用する多様な通信手段や方法を特定することの方が重要である。犯罪被害への対処の活動においては、サイバー犯罪者のすべてのアクセスを阻止したい被害者組織と捜査官が対立することがあるが、活動の範囲と能力が理解されるまで、有意義な犯罪対処を保証することはできない。

難読化

サイバー犯罪者が継続的に発達させてきた能力のひとつとしては「難読化」がある。難読化とは、明らかに不正なソフトウェアまたはネットワークトラフィックを他のデータに紛れ込ませ、無害または読み取り不可能なように見せかけることである。やり方としては、一般的なエンコード方式（例：Base64[87]）や換字式暗号（ROT13[88] など）または、公開鍵暗号方式（PGP[89] など）を使ってデータを暗号化し、不正なソフトウェアが把握されないように保護するといった方法がある。サイバー犯罪者のインフラが生成するネットワークトラフィックも同様で、ドメイン名の変換要求や通常のウェブページへのアクセス、あるいは Dropbox や Gmail などの正規サービスを指揮統制通信に利用するように見せかけることができる。

代替サービス

サイバー犯罪者が特定の活動のために標的への不正アクセスを実行し、その目的を果たしてからはじめて、そのアクセスが後から役に立ちそうだと気付くことも多い。こういった場合、サイバー犯罪者は新たな目的を持った別の活動を開始するまで潜伏したり、独自の目的を持つ他の犯罪組織にそのアクセスを売ったりすることがある。繰り返しになるが、これまでに確認されたもの以外にも、さまざまな攻撃者が多様なサービスを利用する可能性がある。これは、被害者またはその周囲の WiFi や、相互接続されたアプリケーションサービスなど、革新的なソリューションを含んでおり、彼らの活動（およびツール）を難読化し、彼らの行動によって生成されたネットワークトラフィックが被害者ネットワーク上で決して見られないようにしている。

目的達成

最後のステージは、サイバー犯罪者がその目的を達成したときに発生する。発生したサイバー犯罪の種類によっては、それが標的にとって分かりやすいもの（ランサムウェア、破壊工作、窃盗、その他）の場合もある。ベンダーやパートナー、ジャーナリストなど、第三者から発生を知らされることもあれば、発生したことに一切気付かないままのこともある。同一の犯罪組織から 3 年間も不正アクセスされ続け、何回も犯罪行動を許してしまっていたことに気付かなかった被害者も珍しくない。

87 https://tools.ietf.org/html/rfc4648
88 http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf
89 http://www.pgpi.org/doc/pgpintro/

「環境寄生型（LotL）攻撃」

注目すべきサイバー犯罪の傾向の一つは、既存の合法的なツールを使って攻撃を行い、組織内で横方向に移動することである。「Living off the Land」攻撃または「LotL」[90]として知られるこれらの方法はファイルレス方式であり、すなわち、これは標的のシステム内にコードやスクリプトをインストールする必要はないことを意味する。この方法で利用できるネイティブツールには、PowerShell や Windows Management Instrumentation などがある。

レジストリ常駐型マルウェアとして知られる悪意のあるソフトウェアは、Windows レジストリに埋め込まれて、悪意のあるコードをシステムのレジストリに直接挿入することができる。それはオペレーティングシステムの起動時に開始するようにプログラムすることができるため、持続性を確保して長期間検出されないようにすることができる。一方、メモリーオンリーのマルウェアは、システムのメモリー内でのみ動作し、検知を回避する一方で、偵察、横移動、データ流出など、さまざまな悪意のある活動のための秘密のエントリポイントとして機能する。

ランサムウェア戦術の分野では、システムに侵入するための主な方法としてファイルレス手法が採用されている。悪意のあるコードを文書に埋め込み、正規のソフトウェアツールを活用することによって、攻撃が実行され、ファイルを暗号化し、重大な混乱を引き起こす。ランサムウェアグループが好んで使用するツールの中には、PowerShell、PsExec、Windows Management Instrumentation（WMI）、Mimikatz、Cobalt Strike などがある。

LotL の脅威の行為者は、正当なユーザー認証情報を盗んでビジネスメール詐欺を実行する。これらの詐欺は、アカウント認証情報などの機密情報を盗み出し、追加のシステムを偵察し、正規のツールを乗っ取り、さらなる悪意のある活動のために永続的なアクセスを確立することを目的としている。

「LOLBins」とは、「Living Off The Land Binaries」の略で、オペレーティングシステムや一般的に使用されているアプリケーションにネイティブな、悪意のない合法的なシステムツールを指し、攻撃者はこれを悪用することで、検知を回避しながら悪意のある活動を行うことができる。この用語は、同様に悪用される可能性のあるスクリプトやバッチファイルを指す「LOLScripts」にも拡張できる。これらの概念は、より広範な「Living Off The Land」戦術に関連しており、前述のように、攻撃者は合法的にプリインストールされたツールを使用して操作を実行し、セキュリティシステムが悪意のある活動を検出することを困難にする。

LOLBinsの主な特徴

- 回避とステルス：攻撃者は通常のネットワーク活動に紛れ込むことができ、セキュリティツールやシステム管理者に対してその行動が疑わしくないように見せる。この方法は、ウイルス対策ソフトウェアによってフラグが立てられる可能性のあるカスタムマルウェアを使用する場合と比較して、検出される可能性を低くする。
- 機能の悪用：ファイルのダウンロード、実行、永続性の確立、特権の昇格、防御の回避、データの流出など、攻撃者にとって有用なさまざまな機能を実行することができる。例えば、Windows のコマンドプロンプト（cmd.exe）と PowerShell（powershell.exe）は、スクリプトを実行したり、インターネットからファイルをダウンロードしたり、システム設定を変更したりできる強力なツールである。
- 外部ツール不要：LOLBin は既にシステム内に存在するか、一般的にインストールされているアプ

90 https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/threat-actors-leverage-legitimate-tools-in-lotl-attacks

リケーションであるため、攻撃者はツールをアップロードする必要がなく、フットプリントが減少し、従来のウイルス対策システムやエンドポイント検出対応（EDR）システムに捕捉される可能性も減る。
- 防御側の課題：これらのツールの合理的な性質は、防御側にとって課題を示す。というのは、これらのツールをブロックしたり制限したりすると、通常のシステムやユーザーの操作が妨害される可能性があるからである。これは、正当な使用と悪意のある使用を区別するための行動分析と背景に焦点を当てた、より洗練された検出技術を必要とする。

よく使われるLOLBins:

- Windows：Cmd.exe、PowerShell（powershell.exe）、Certutil.exe（ファイルのダウンロードまたはデコード用）、Bitsadmin.exe（バックグラウンドファイル転送用）、および Regsvr32.exe（コードの実行とユーザーアカウント制御のバイパス用）。
- Linux/Unix：Curl または Wget（ファイルのダウンロード用）、Cron（タスクのスケジュール用）、Bash（スクリプトとコマンドの実行用）。
- macOS：Osascript（AppleScripts やその他のスクリプトの実行用）、Curl/Wget、Launchd（永続化用）。

LOLBinリスク軽減と脅威検出:

LOLBin の悪用リスクを軽減するには、厳格なアプリケーションのホワイトリスト化、プロセス実行パスとコマンドライン引数の監視とログ記録、動作検出戦略の採用、攻撃者が初期アクセスを取得するために使用するフィッシングやその他の戦術に関するユーザー教育などの戦略を組み合わせる必要がある。検出と対応の戦略も、進化する攻撃者の戦術に応じて調整されなければならない。

LOLBin は、いくつかの注目を集めたサイバー侵害や攻撃で利用されてきた。これらのツールの使用法が報告の中心となることはあまりないが、攻撃者がさまざまな段階でこれらのツールを活用していることを示す文書は数多く存在する。下記にいくつかの例を示す。

- WannaCry ランサムウェア攻撃（2017 年）：拡散と被害の主な方法は EternalBlue エクスプロイトと DoublePulsar バックドアによるものだったが、WannaCry ランサムウェア攻撃は Windows に組み込まれたツールも操作に活用していた。例えば、vssadmin を使ってシャドーコピーやバックアップを削除してファイルの復元を防いだ。これは、被害者に身代金を支払うよう圧力を強めるためにランサムウェアの実行者がよく使う戦術である。
- SolarWinds Orion サプライチェーン攻撃（2020 年）：この巧妙かつ広範囲に及ぶ攻撃では、敵が SolarWinds 社の Orion ソフトウェアのビルドシステムを侵害し、顧客に配布されるアップデートに悪意のあるコードを挿入した。侵害後の段階では、攻撃者は PowerShell などのさまざまな LOLBin を使用して、従来のマルウェアのシグネチャを監視していたセキュリティツールからのアラートをトリガーすることなく、コマンドの実行、横方向への移動、データの抽出を行った。
- NotPetya 攻撃（2017 年）：NotPetya は、初期感染では EternalBlue エクスプロイトを使用した破壊的なマルウェアの突発的な発生だった。感染後、PsExec（正規の Microsoft ツール）や WMIC（Windows Management Instrumentation Command-line）などの LOLBin を利用して横方向に移動し、ネットワーク全体に拡散した。これらのツールを使用することで、攻撃者はリモートマシン上のシステム特権を使用してマルウェアを実行することができた。
- Stuxnet（2010 年発見）：イランの核開発プログラムを標的にしたサイバー兵器 Stuxnet は、Windows の正規の機能や特徴（LNK ファイルやプリントスプーラサービスなど）を利用してペイ

ロードを拡散および実行した。これらはスタンドアロンバイナリではないが、検出を回避するためのより広範な LotL 戦略を反映している。

- APT29/Cozy Bear 作戦：ロシア政府に帰属する脅威グループ APT29 は、サイバースパイ作戦でさまざまな LOLBin を使用していると報告されている。certutil.exe などのツールは、悪意のあるペイロードをダウンロードするために使用されており、PowerShell は、インメモリペイロードの実行、データ収集、および抽出のために広く使用されており、暗号化されたコマンドを頻繁に活用して活動を難読化している。

これらの例は、LOLBins の使用がサイバー攻撃における多様性とステルス性を可能にすることを示している。攻撃を可能にして迅速化するためのネイティブツールの使用は、ブルーチームとネットワーク防御者にとって、IoC とアーティファクトの適用をより困難にする場合がある。これは、これらのツールの合法的な使用と悪意のある使用を区別する際に防衛側が直面する課題と、攻撃の兆候を示す異常な動作を検出するための高度な監視および分析機能の必要性を強調している。

サイバー犯罪のアーティファクト

「アーティファクト」という用語は理解が難しいかもしれない。アーティファクトは証拠でもなければ、単純にインジケーターでもない。これらはソース内に存在するが、サイバー犯罪活動において人間、コンピュータ、またはその組み合わせの相互作用によって作成された個別のオブジェクトである。アーティファクトは2つのカテゴリに分類される。1つは被害者のコンピュータネットワークの外部にあるものであり、もう1つは犯罪者の行為の結果として被害者のコンピュータネットワーク内に含まれるものである。

サイバー犯罪のインジケーターは犯罪者の意図を反映するが、アーティファクトは犯罪者の行動の痕跡、すなわち、メモ、ファイルや通信の断片、録音、メッセージ、現在は使用されていない忘れられた（ダーク）ウェブページのキャッシュなどを表す。インジケーターとアーティファクトの組み合わせは、サイバー犯罪者が追跡または実行した犯罪の証拠につながる。

以下の図は、インジケーターとアーティファクト、証拠、ソース（第5章で説明）との関連性を示している。

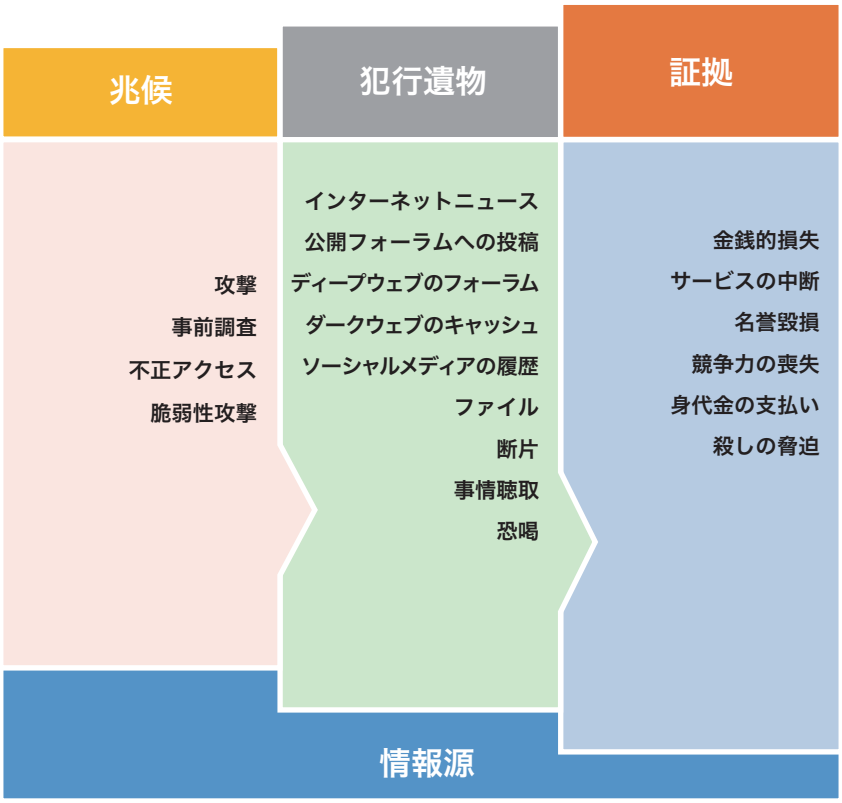


図 3-6. インジケーターとアーティファクトの関連性

外部のアーティファクト

外部のアーティファクトは、標的となったネットワーク外に存在する証拠またはインテリジェンスの情報源である。組織によっては、関連情報源にどのようなインジケーターやアーティファクトが存在するかを積極的に調べ、インテリジェンスを収集している場合がある。脅威インテリジェンスサービス企業は技術的情報と市場情報といった情報源からデータを収集し、緊急リスクや進行中の活動を組織が把握できるよう、これらのデータを販売している。こういった民間の情報源に加えて、特定のデータ情報源（ディープウェブのサイトや取引市場、チャットルームなど）を監視している極秘情報提供者（組織が雇うセキュリティ調査員など）や秘密諜報部員がサイバー犯罪活動に関する有益なアーティファクトを取り出すことができる場合もある。

インターネット

インターネットは、Google や Bing などのインターネット検索エンジンによって捕捉されたワールドワイドウェブ（WWW：World Wide Web）のアクセス可能な公開領域を表している。インターネットアドレスあるいはドメイン名をだれが購入したかなどの履歴情報は、domaintools.com といった企業が提供している他、「WHOIS[91]」の記録を見れば、そのようなサービスが物理的にどこでホストされているのか分かる。攻撃者が何らかの形の通貨で支払いを行っていた場合、これらのサービスから一連の捜査で数少ないアーティファクトが出てくるかもしれない。現実世界における支払い絡みの捜査で必ず調べるのと同じように、送金や支払いが行われたなら、そこから支払い元を突き止めて、背後のつながりを解明できるようになる。特筆すべきは、過去 10 年間の暗号通貨の台頭により、犯罪者は捜査を回避および迂回する大きな能力とツールを手に入れ、高度な匿名性で資金を送金および移動できるようになったことである。

ディープウェブ

ディープウェブは、Google のクローラーや検索エンジンなどのサービスではアクセスできないインターネットのすべての領域を表している。これは、犯罪者が情報を交換するプライベートなディスカッションフォーラムや、Google などのサービスによるコンテンツのインデックス作成を制限する匿名の通信ウェブサイトに犯罪者が盗んだデータを販売する市場などを含むことがある。ディープウェブサイトは目に見えない場所に隠れているため、アクセス可能ではあるが（ただし、適切なソフトウェアを使用した場合のみ）、サイバー犯罪者以外では広く宣伝または議論されていない。ディープウェブサイトは通常、調査で収集されたヒントや HUMINT（**ヒューマンインテリジェンス**）を通じて暴露される。いずれにせよ、サイバー犯罪者はディープウェブサイトが暴露されたことを知ると、すぐに別のサイトに移る可能性がある。つまり、ディープ ウェブサイトの価値は、長期的な作戦追跡と犯罪者（およびその目的）を特定するために監視することにあり、閉鎖を試みることにはあまり意味がない。

ダークウェブ

ダークウェブとは、匿名ネットワーク TOR[92] のような隔離されたリポジトリで利用可能なリソースのコレクションと、アーカイブサービス（「Wayback Machine[93]」や Google Cache など）を通じてのみ利用可能な、廃止または放棄された情報の両方を表す。TOR を使用すると、個人は実際の位置を公開せずに

91 https://www.whois.net/
92 https://www.torproject.org/
93 https://archive.org/web/

通信できるため、サイバー犯罪者（および単にプライバシーを求めているユーザー）は私的に通信できる。

ソーシャルメディア

ソーシャルメディアは、公共のコミュニケーションと情報共有サービスを表す。現在最も人気のあるソーシャルメディアサイトには、Facebook、YouTube、X（以前は「Twitter」として知られていた）、Instagram、Snapchat などがあり、多くの公開（および非公開）オプションが利用可能である。ソーシャルメディアは、被害者をターゲットにしたり、一般大衆に伝えたり、被害者を挑発したり、私的な通信ネットワークを提供したり、犯罪グループ間の通信を容易にしたりするために利用されるため、サイバー犯罪に関連している。

従来型メディア

従来型メディアは依然として存在しており、記者の中には犯罪組織を追跡して潜入したり、犯罪組織から連絡を受けて社会的な抗議や偽情報の拡散、あるいは「ファン」と思われる人々からの称賛を得るなどの目的を達成しようとする者もいる。

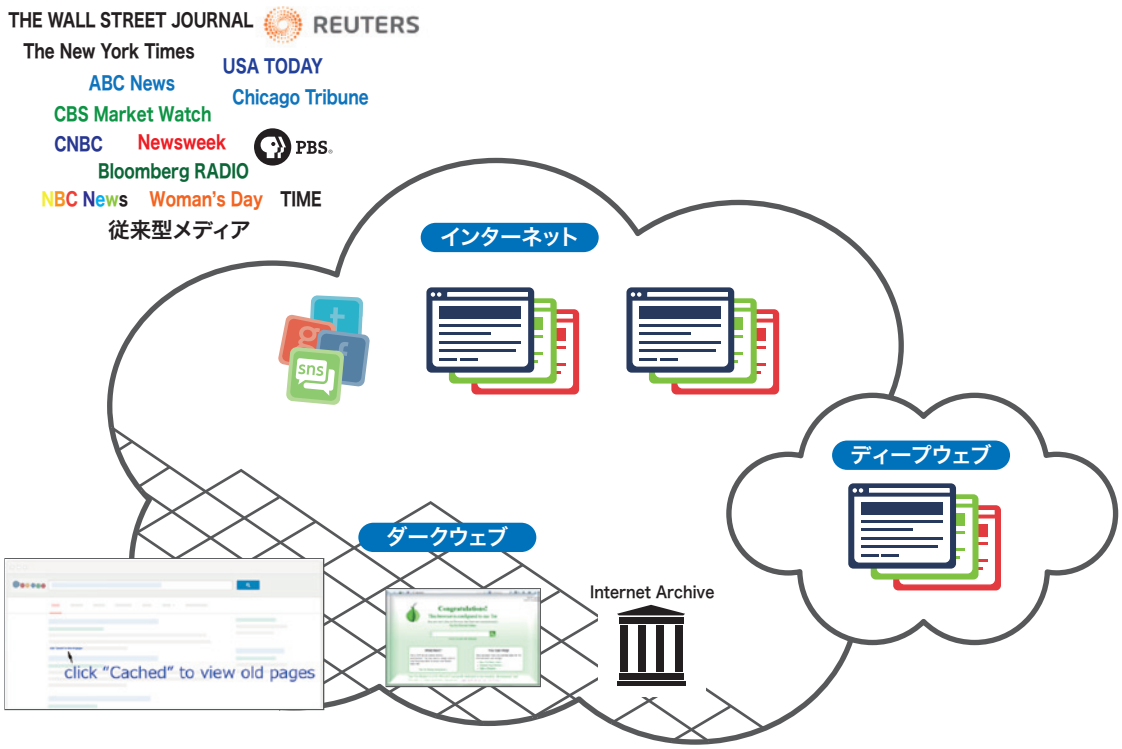


図 3-7. サイバー犯罪における外部のアーティファクト

犯罪ネットワーク

ほとんどの法執行機関は、犯罪ネットワークへの潜入を試みるために、情報提供者、潜入捜査官、または購入した脅威情報サービスを通じて、HUMINT を収集し、開発する。犯罪者が情報を交換したり、単に同じグループの他のメンバーと話し合って新しい作戦を調整したりするディープウェブ、ダークウェブ、その他の隠れたコミュニティは、捜査官や情報収集にとって特に価値がある。

内部のアーティファクト

最も分かりやすく記録されているアーティファクトは標的のコンピュータ内に存在している。これらは、システム、人員、通信の3つのカテゴリに分類できる。具体的な情報源については、第5章で詳しく説明する。

システム

個々のコンピュータやアプリケーションからのアーティファクトは、揮発性の高い順番に従って複数のソースから取得されることがある。アーティファクトの順序が高いほど、通常のシステム操作と使用によって破壊されるまでの寿命が短くなる。

- **メモリ** - プログラムがメモリに読み込まれると割り当て済みのセグメントが上書きされるため、メモリの中にあるアーティファクトは最も揮発性が高い。メモリは一時的な格納場所であり、ファイルの利用やプログラムを終了すると必要に応じてメモリ空間が解放され、コンピュータをシャットダウンするとアクティブメモリは削除される。
- **ログファイル** - オペレーティングシステムとその関連アプリケーションによっては、サイバー犯罪行動が明らかになるようなアーティファクトが標的システム上のログファイルとして存在している可能性がある。ただし、ログファイルは修正・削除が可能であり、構成によっては一定時間の経過後、または指定したファイルサイズの制限に従って、ホストシステムが自動的にログファイルを上書きまたは削除してしまうことがある。
- **構成設定** - 通常は基本設定を格納する仕組み（Microsoft の Windows ではレジストリ、macOS では plist と呼ばれる）に保存されている。これらのファイルにはアプリケーションの構成が保存されており、サイバー犯罪行動の各種ステージに関係するアーティファクト（コマンドの実行履歴やサービス設定）を含んでいる場合がある。
- **オペレーティングシステムおよびファイルシステム** – オペレーティングシステムおよびファイルシステムの中にはユーザーの活動履歴を記録しているものがある。コンピュータを使うユーザーにとって便利な機能として開発されたものが、フォレンジック調査官による過去の利用歴の調査に役立つことになる。これらのアーティファクトが収められている場所によっては、データが一定期間保存される場合（例：インターネット履歴）もあれば、保存されるエントリ数の上限が決まっている場合（例：最近使ったファイル）もある。一方、攻撃者が何らかのアンチフォレンジック技法またはツールを使って自身の行動を分からなくなるようにしない限り、データが記録されたままとなる場合もある。これらは他の何らかのプロセスによって削除されるか、ユーザーが削除しない限りはストレージに残るように設計されており、最も揮発性の低いアーティファクトである。

従業員

従業員は、サイバー犯罪に関連するさまざまな種類のアーティファクトを提供できる。異常な振る舞いを最初に察知した被害者は観察した情報を提供したり、捜査官が犯罪の時間軸を組み立てるために事情聴取で協力したりできる。標的となった組織の従業員は、ログファイルや物理的・論理的なアクセス記録だけでなく、システムの利用および構成に関する異常で気付いた事柄も提供できる。また、恐喝やランサムウェアによる要求、脅迫的なコミュニケーションなどのサイバー犯罪についても、これらに関連して観察した事柄や体験した事柄を従業員から得られる。

コミュニケーション

コミュニケーションまたはネットワークのアーティファクトはさまざまな場所に存在している可能性がある。例としては、請求記録や、ルータおよびスイッチの構成詳細、ホストの構成設定、サービス履歴ログ、ネットワークトラフィック記録などがある。また、不正アクセスのインジケーターに関するイベントを相関させる、セキュリティ情報およびイベント管理システム（SIEM：Security Information and Event Management）で見つかる場合もある。捜査官・調査員の多くが構成設定や請求記録に注目するのを忘れがちである（ネットワークセキュリティやアーキテクチャ管理に携わる従業員からの事情聴取についても同様である）が、これらの情報源はサイバー犯罪者によって実行されている行為や犯罪の範囲を理解するのに重要なアーティファクトを提供できる場合がある。

被害者によっては、記録デバイスを介して接続するネットワーク接続ごとに何が起きたのかを要約して記録するネットワークフロー（NetFlow などの）データが残っている場合がある。最近のほとんどのネットワークデバイスは、ネットワークフローデータを捕捉して、ネットワークのどこかに置かれたレシーバーに送信できるようになっている。被害者組織のほとんどは、品質管理を目的とする運用および保守の機能としてネットワークフローを見ているため、脅威に気付いていない場合でもこのデータが存在する場合がある。

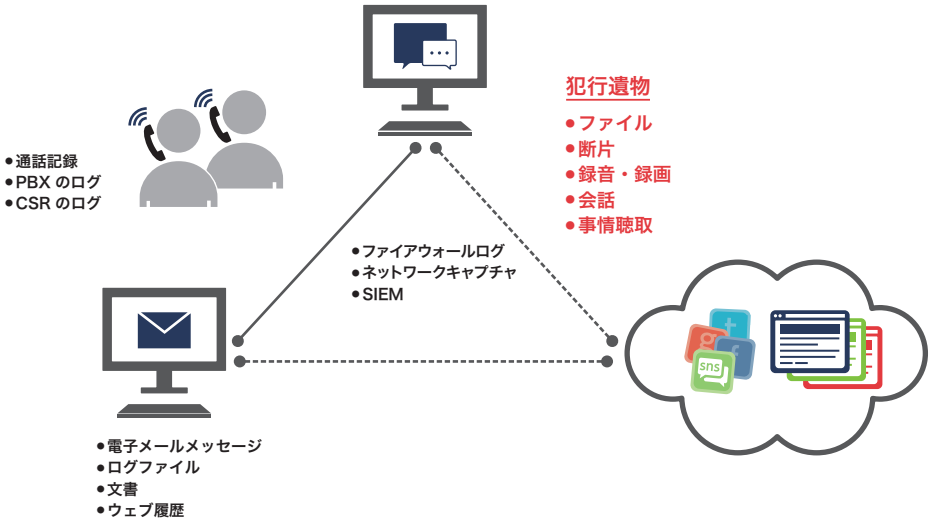


図 3-8. 内部のアーティファクト

暗号化

SSL の後継である TLS に代表されるトランジット暗号化の利用が飛躍的に伸びたのは、Let's Encrypt[94] などのサービスを通じて、プログラムで簡単に証明書を作成できるようになったからである。暗号化は一般的に有益であり、エンドユーザーやトランザクションのプライバシーを含む様々な重要な利点を提供する。しかし、ネットワーク脅威検知の障害になることもある。

暗号化の使用は過去 10 年間で大幅に増加しており、2014 年には 50% 程度であったものが、現在では 90% 以上に伸びているという情報もある [95]。ユーザーセッションの復号化、セキュリティ検査、再暗号化を容易にするために、TLS や SSL の復号化機能を導入する組織が増加している。これは複雑でコストがかかり、規模を拡大するのは困難である。

94　https://letsencrypt.org/
95　https://transparencyreport.google.com/https/overview?hl=en

第3章:CIBOKの分類法との関係

すでに述べたように、CIBOK 分類の実行フレームワークは、組織内におけるサイバー犯罪捜査の機能と有用性を理解するのに必要な各知識範囲の相関関係を表している。サイバー犯罪の捜査プロセスは、犯罪の範囲（および関連するアーティファクト）に応じて利用可能な証拠源の種類を決定することに依存し、証拠の収集と分析の実用的な方法によってサポートされる。被害者と公共および民間組織間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

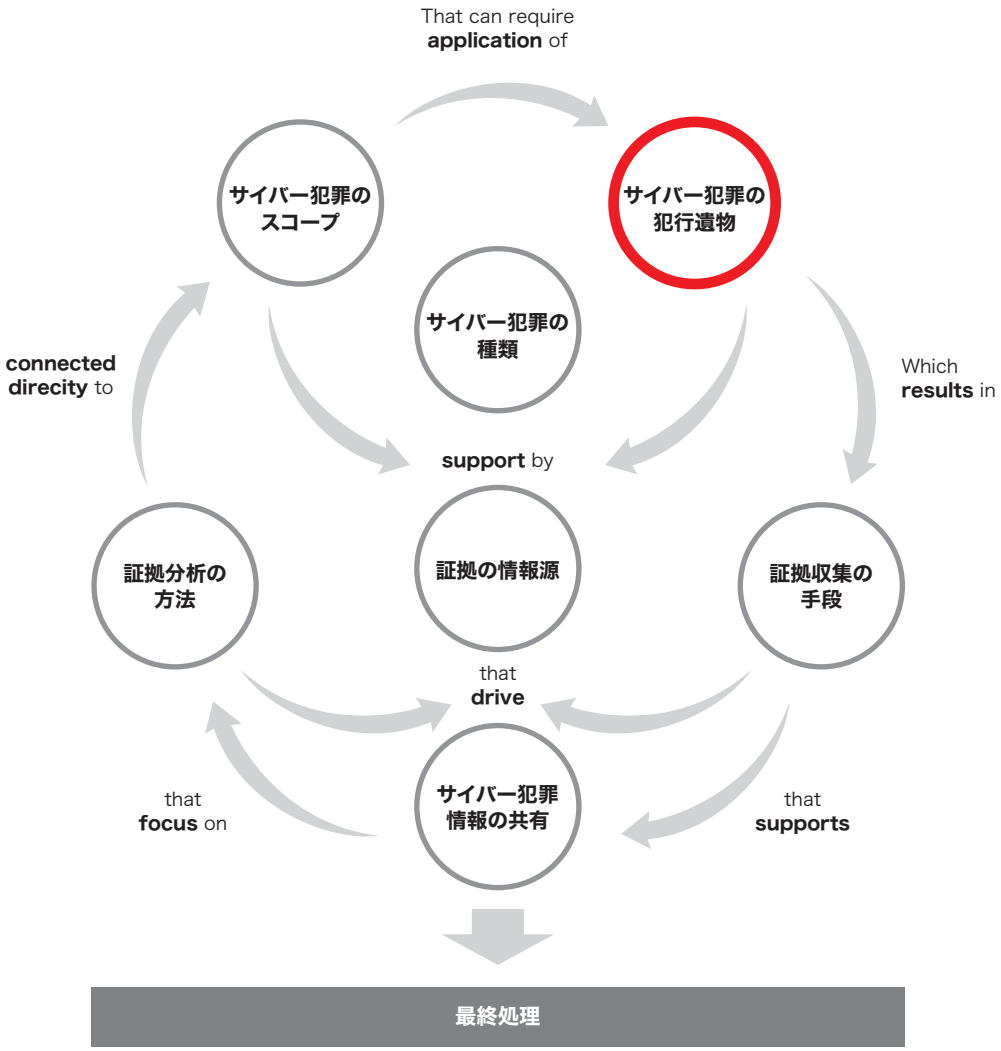


図 3-9. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと CIBOK のスキルおよび知識の分類（表 3-2）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 3-2. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 3-3. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査管理の機能は、組織に対してサイバー犯罪の特性と種類を説明する。また自組織に対するリスクを識別するインジケーターおよびアーティファクトを戦略的に理解し、捜査を支援するためにそのような情報を見つける方法を理解する必要がある。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査管理の各役割にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集の機能は戦術的であるが、捜査官がアーティファクトを収集して証拠を犯罪活動に結び付けるのを支援するような、サイバー犯罪のインジケーターに関する高度な認識が必要である。

調査 – 利用可能な情報源にあるアーティファクトや証拠を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。知見収集、説明責任、予防啓発、捜査管理の各機能にある者が、サイバー犯罪の影響を識別するのを支援する。識別にあたっては、その犯罪に関連する目的の特性（および達成の段階）に対する評価を用いる。サイバー犯罪の種類は、信頼できる方法で発見され、分析されたアーティファクトに応じた証拠によって決まる。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。知見の収集、捜査手続きに関する指導を行い、関連方針および法規制に基づいて分析結果を解釈して、捜査管理や予防啓発の各機能を支援する。証拠を見つけるために発見または追求されるインジケーターやアーティファクトに関係するため、捜査のアプローチは法令に定められた指針によって決まる。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。予防啓発の機能は、少なくともサイバー犯罪のインジケーターについて戦術的に理解し、組織やステークホルダーにリスクを正確に伝え、組織が実行する対応活動（調査を含む）についても知らせなければならない。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第3章:レビュー

1. **サイバー犯罪のインジケーターとは**
   答え：組織に対する脅威。
   例：保護された情報の暴露、システムまたはサービスの中断、経済的損失、証券パフォーマンスの操作、恐喝メッセージ。

2. **サイバー犯罪のアーティファクトとインジケーターの違いとは**
   答え：インジケーターは活動の種類を反映し、アーティファクトは詳細を提供する。
   インジケーター：活動の種類や兆候、攻撃者が行っている行動や進行状況を把握するための手がかり。例、「攻撃」「不正アクセス」「事前調査」。アーティファクト：攻撃者の活動によって生成された具体的な痕跡や証拠であり、ファイル、ログ、ツール、コマンドの出力などが含まれ、攻撃の実施やその影響を具体的に明確に示す。例、攻撃者が使用したマルウェアのファイルや、不正アクセス時に変更されたログファイルなどがアーティファクト。

3. **サイバー犯罪活動におけるステージ（段階）とは**
   答え：さまざまな理由で実行される関連活動。
   例：標的の決定、アクセスの提供、カタログ作成、サービス定義／管理／サポート／防御、サービス冗長性、難読化、代替サービス、目標の達成。

4. **捜査官が使用できるサイバー犯罪のアーティファクトの種類とは**
   答え：パブリックとプライベート。
   例：ログファイル、ファイルの断片、通信／録音、インタビュー、オペレーティングシステムの設定など。

5. **捜査官がサイバー犯罪のアーティファクトとインジケーターを見つけられる場所はどこか**
   答え：外部と内部の情報源。
   例：インターネット、（ディープ／ダーク／ソーシャル）ウェブ、HUMINT、従来のメディア、システム、従業員、通信。

ケーススタディ3:現代の攻撃

- **犯罪**：個人情報（認証情報）の盗難、不正アクセス
- **容疑者**：イランの脅威の行為者 UNC1549
- **手段**：ソーシャルエンジニアリング、マルウェア
- **動機**：政治的目標（潜在的なスパイ活動、データ盗難、動的戦争攻撃を可能にする）
- **機会**：不適切なメールフィッシングセキュリティとセキュリティ意識、政情不安

異なるタイプの脅威グループ間の境界線が曖昧になることで、サイバー犯罪の複雑さがさらに加わる。歴史的に、脅威の行為者は、金銭的利益を動機とするクライムウェアを使って犯行を行う者、情報収集

や地政学的敵対勢力の混乱を狙うステートスポンサード攻撃者、特定の社会的または政治的目的を推進するハクティビストなど、いくつかのグループに分かれていた。今日、これらのグループの境界線はますます曖昧になっている。

過去 20 年の間に、これらの各カテゴリに属する脅威の行為者やグループの例は数多くある。これは、2011 年のシリア電子軍[96]や 2000 年代初頭の古典的なロシアビジネスネットワーク（RBN）[97]、中国のスパイグループ UNC3886[98]や国家に隣接する APT グループ[99]などの最近の多数の攻撃者、Blackcat、Cl0p、LockBit、Black Basta などの現代の広範なランサムウェアグループを含んでいる。「ペイパーインストール」とマルウェア配布のコモディティ化の初期の兆候[100]からかなり経過した後も、この傾向はマルウェア・アズ・ア・サービス（MaaS）の提供が広まり、衰えることなく続いている[101]。

キーボードの向こうに人間がいるという事実を忘れてはならない。マルウェアは単なるツールであり、本当の脅威はそれを操作する人間である。最近の AI の進歩の観点からすると、捜査官は AI を利用した攻撃の設計、方法論、高度なツール、機械学習の背後にいる人間についても考慮しなければならない。

脅威の行為者が犯罪を行う真の動機を見極めるのは難しい。例えば、ブルーチームが集団的なスキルを駆使して、ある環境で 5 台の侵害されたホストを検出できる場合があり、これらのすべてに同様のマルウェアファミリのバイナリが埋め込まれていることがある。不正アクセスの原因が行為者やどのような犯罪作戦によるものと確信できるだろうか？不正アクセスされたホストの所有権が脅威の行為者間で移転される傾向があり、サイバー犯罪のインフラが商品化されていることを考えると、不正アクセスの原因となった特定の脅威の行為者の動機や望ましい結果を理解することは非常に困難である。不正アクセスされたホストによってもたらされるリスクは、責任を負う敵対者しだいで大きく異なる。

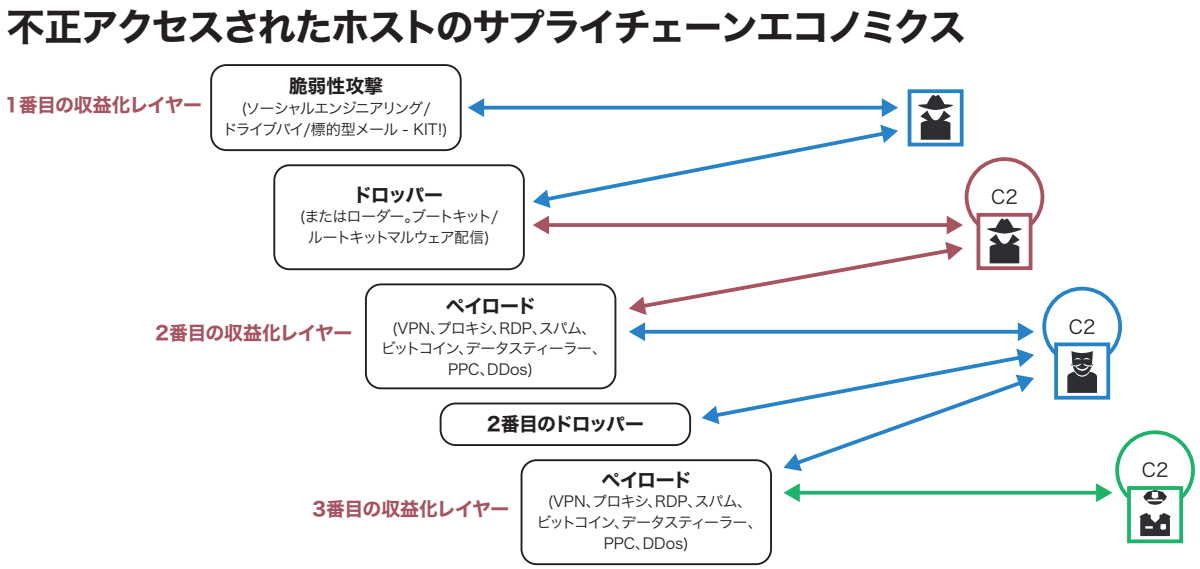


図 3-10. 不正アクセスされたホストのサプライチェーンエコノミクス

96 https://www.bugcrowd.com/glossary/syrian-electronic-army/
97 https://en.wikipedia.org/wiki/Russian_Business_Network
98 「中国のスパイグループUNC3886が2021年後半からCVE-2023-34048を悪用していることが判明」、Mandiant、2021年10月3日。https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021を参照。[アクセス日: 2024年2月2日]
99 https://www.mandiant.com/resources/insights/apt-groups
100 「ペイパーインストール」の測定:マルウェア配布のコモディティ化」2011。https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdfを参照。
101 https://securelist.com/malware-as-a-service-market/109980/

マルウェアのコモディティ化と、想定される攻撃者の動機を理解することの難しさの例を、前頁の図3-10に示す。この例では、最初の脆弱性攻撃によって標的のホストが不正にアクセスされ、その後、複数のドロッパー（またはローダー）とペイロードがエンドポイントに配信される。最終的な結果として、侵害されたホストにアクセスできるのは4人の異なる脅威の行為者である。

先に説明したように、サイバー攻撃の帰属は、攻撃者が「LOLbins」などの高度な技術を使用して自分の身元や所在地を隠すため、さまざまな要因によって非常に複雑になる可能性がある。

以下の事項は、当初の帰属が後に疑問視されたり修正されたりしたサイバー攻撃の例を示している。

- ソニーピクチャーズハッキング（2014年）：ソニーピクチャーズへのハッキングは、金銭的にも風評的にも大きな損害をもたらし、当初はさまざまなハッカー集団や不満を持つ従業員によって行われたのではないかとの憶測があった。FBIや他の機関によるさらなる調査は、攻撃に使用された戦術、技術、手順（TTP）に基づき、この攻撃は北朝鮮によるものであると判断した。

- オリンピック作戦／Stuxnet（2010年）：スタックスネットは当初、監視制御およびデータ収集（SCADA）システムを標的とした、起源がはっきりしない非常に高度なコンピュータワームであると考えられていた。また、スタックスネットはイランの核開発計画に損害を与えるために設計されたものであることも判明した。後に、このワームの背後にはアメリカとイスラエルがいたと報道された（現在では広く信じられている）。スタックスネットは複雑で標的が特定されているため、発見当初はその本質と起源が不明瞭だった。

- WannaCryランサムウェア攻撃（2017年）：世界中の何十万台ものコンピュータに影響を与えたWannaCryランサムウェア攻撃の直後、犯罪組織や国家を含む潜在的な犯人に関するさまざまな説が広まった。さらに分析を進めると、同グループによるものとされる以前のマルウェアとのコードの類似性に基づき、この攻撃が北朝鮮と関連のあるラザルスグループによるものであることを示す証拠が特定された。

これらの事例は、特に攻撃者がLOLbinなどの技術を巧みに利用して通常のネットワーク活動に紛れ込む場合、サイバー攻撃の帰属を特定するには複雑な調査作業が必要であることを強調している。このような手法は、攻撃者が目的を達成するのに役立つだけでなく、攻撃者を正確に特定するための調査作業を大幅に妨げる。

これらの事例は、社内パートナーまたは外部パートナーの能力を問わず、組織が定義、準備、実践したインシデント対応計画と専門知識を持つ必要性も強調している。攻撃に対して迅速かつ効果的に対応する能力は、被害を最小限に抑え、復旧を早めることができる。

ケーススタディ：現代の攻撃の詳細な例

2024年2月、マンディアント（Mandiant）はイスラエルと中東の航空宇宙および防衛部門を標的とした攻撃の詳細を記した文書を公開したが[102]、その後、この攻撃はイランの脅威の行為者UNC1549によるものとされた。この作戦で使用された戦術には、カスタマイズされた雇用をテーマにした罠や、C2用のクラウドサービスの利用などがあり、防止、検出、対応の面でネットワークセキュリティチームに大きな課題をもたらす可能性がある。

犯罪行為を隠すために複数の回避手法が使用された。Microsoft Azureのインフラ、ソーシャルエン

102 https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

ジニアリングスキーム、および2つの独自の個別のマルウェアインスタンス（MINIBUS と MINIBIKE）も広く使用された。さらに、「LIGHTRAIL」と呼ばれるカスタムの「トンネラー」が使用され、犯罪行為をさらに隠蔽して難読化した。

このキャンペーンの攻撃ライフサイクルは、攻撃者が侵入してマルウェアツールを埋め込むために使用する複雑な手法を示す。

1. 攻撃者は、電子メールやソーシャルメディアのメッセージを介してフィッシング攻撃を仕掛け、偽のウェブサイトに誘導するリンクを配信する。これらのウェブサイトは、イスラエルとハマスの紛争に関連するコンテンツや、航空、航空宇宙、サーマルイメージングなどの技術・防衛分野をターゲットにした詐欺的な求人情報などを掲載している。不正な求人情報により、攻撃者は認証情報を窃取することができる。さらに、フィッシングリンクをクリックすると、有害なソフトウェアがダウンロードされる。

2. 感染プロセスでは、前述のサイトから悪意のあるパッケージが被害者のデバイスに直接転送される。パッケージは下記の2つの主要コンポーネントを含むアーカイブである：

    - MINIBIKE または MINIBUS：感染したシステムに包括的な不正アクセスを提供することができる、異なるタイプのマルウェア。MINIBIKE は 2022 年頃に登場し、MINIBUS は 2023 年頃に登場した。どちらもコマンド実行に加えて、データの抽出とアップロードを可能にする。

    - 正規のアプリケーション OneDrive のように見えるように設計されたおとりアプリケーション（MINIBIKE の場合）、またはハマスに拘束されているイスラエル人に関する情報を表示する特注のアプリケーション（MINIBUS の場合）のいずれかである。MINIBUS アプリケーションは、ユーザーを詐欺サイト birngthemhomenow[.]co[.]il に誘導することもある。

この攻撃で使用された IoC と IoA の広範なリストは、Mandiant によって概説されている。注目すべきは、ファイルハッシュ、レジストリキーと値、特定のブラウザのユーザーエージェント、永続化メカニズム、専用の C2 インフラ、および C2 URL が見られることであり、これらはすべて、攻撃に使用されたツールのその後のバージョン間では異なっている。これは、国家による攻撃を実行するために使用される手法の複雑さと幅広さを強調している。

第4章

サイバー犯罪のスコープ

はじめに

ある人物が銃撃を受けた。これは状況によっては犯罪かもしれないし、そうでないかもしれない。ある人物が意図的な銃撃を受けた。これでも犯罪でない可能性がある。その人物が撃たれた場所は戦場ではなく、住宅地であった。まだ、状況は明確でない。その人物は、デモに参加している群衆の中にいて、意図的な銃撃を受けた。もしかすると、発砲者には自己防衛といった正当な理由があっただろうか。撃たれた人物は、デモに参加している群衆に向かって演説していた。あるいは、犯罪かもしれない。撃たれたのは、マーティン・ルーサー・キングであった。

いかなる犯罪も、行動と意図、その行為による影響によって定義される。犯罪の特性も同じ基準によって定義される。区別に使われるのは、基本的に犯罪の「スコープ」である。上記のような犯罪は、撃たれた人物が戦場にいる兵士だった場合や、マーティン・ルーサー・キング（キング牧師）ではなく、デモに居合わせた人物だった場合には違うものになる。これは、単純に、犯罪行為の影響はスコープが幅広いからである。犯罪の脅威または（既遂の場合）結果は、犯罪の目的と達成手段によって変わる。

次のシナリオで、もっと一般的なサイバー犯罪を説明しよう。セキュリティシステムが警告を発し、あるビルにだれかが適切な暗証番号を使わずに侵入したことを知らせたとする。警察が対応に駆け付け、ドアが開いているのを発見する。さらに調べてみると、窓ガラスの一枚が割られ、内側からドアが開けられたことが判明した。ビルに入ったすぐのところにホームレスが寝ているのを警察が見つける。

同じシナリオで、今度はホームレスがいるホールから奥のオフィスルームで明かりがついているのに気付いたとする。1台のコンピュータは電源がオンになっていて（他のコンピュータはすべてがオフなので不審である）、コンピュータのデスクトップにあるフォルダの1つが開いている。「2016年の合併」という名前のファイルが選択された状態で「コピー完了」というダイアログボックスが画面に表示されている。ホームレスに対する尋問で、ホームレスが屋外の寒さから逃れて安全に寝られる場所を求めてビル内に入ってきたときには、すでにドアが開いていたことが分かる。

どれも人騒がせな犯罪に聞こえるかもしれないが、残念ながら、これらはサイバー空間のTTP（Tactics, Techniques and Procedures：戦術、技術および手順）によって遂行される代表的な犯罪の種類である。殺人や社会転覆、不法侵入、知的財産窃盗、恐喝など、あらゆる種類の犯罪がサイバー技術で可能となる。しかしながら、これらの犯罪がおよぼす影響の決定的要素となるのは、最終的に、犯罪の実行と結果におけるスコープである。

すでに使えなくなったボットネットサービスへの加入を試行させる無差別なコンピュータ感染は、サイバー犯罪者が企業内のコンピュータに感染を広げ、ボットネットの、感染端末を無人操作機に仕立て挙げて利用する標的型コンピュータ感染とはまったく別物である。後者はサイバー犯罪者が情報を盗む、企業の業績データを盗聴する、企業システムへのアクセスをボットネットの登録利用者に販売するといったことを行う。また、コンピュータをボットネットに組み込むためのコンピュータ侵入は、ボットネットに利用者として登録し、そこで得た非公開情報をもとにインサイダー取引を行おうとする不正トレーダーとは異なる。

2013年以降、サイバー犯罪の範囲は大幅に拡大し、攻撃の動機が進化し、攻撃実行者が技術的に高いスキルを持たなくても実行可能となったことで、犯罪活動が増加している。サイバー犯罪を実行する動機は、依然として本質的には主に金銭的なものである。しかし、技術的アプリケーションを使用して、知的財産、非公開の市場情報、国家機密の窃盗などに関する高度な犯罪を実行する能力は、破壊活動、イデオロギー、命令、エゴ、憎悪などの動機とともに、それに応じてすべて成長してきた。さらに、金融サービスにおける暗号通貨の大幅な市場成長と広範な採用により、ランサムウェアは、より広範な目的を達成しようとする犯罪者や国家に支援された行為者にとって好ましいツールセットへと進化した。

下記の例は、2013 年から 2024 年までのサイバー犯罪の状況の変化と今後の見通しを示している。

1. **金銭的的利益**：サイバー犯罪の主な動機は依然として金銭的利益であり、詐欺と窃盗が主な目的である。ハッカーは、資格情報のリプレイ、フィッシング、ソーシャルエンジニアリング、インサイダーのオンラインリクルートなど、さまざまな手法を使って、クレジットカード情報、オンライン小売、銀行口座、暗号通貨ウォレット、ゲームのログイン、および関連する個人識別情報（PII）を収集、販売、または自分自身のために使用し、金銭的利益を得ている[103]。オンライン口座乗っ取りによる個人への単純な詐欺、ペテン、詐欺の域を越える金融犯罪は、インサイダー取引、電信詐欺（ビジネスメール詐欺）、モバイルバンキング預金詐欺、暗号通貨の直接窃盗など、高度な金融犯罪行為へと発展している。[104]
2. **イデオロギー／秩序**：サイバー犯罪者の中には、イデオロギーに動機づけられた者もいるため[105]、それが彼らをより困難な脅威にし、犯罪の範囲を評価することが困難になることがある。イデオロギーは、政治的、環境的、あるいは宗教的な思想の過激化によって動機付けられることが多くなっている。国家が支援する攻撃（戦争行為、すなわち重要インフラの破壊行為を含む）や組織的または分散的な犯罪集団によるハッキング活動が増加している一方で、ハッカーが軍隊や諜報機関に雇用されているため直接の命令に従うケースも増加しており、サイバー犯罪の背後にある職業上の動機とともにイデオロギー的原則と過激化が高まっていることが示されている[106] [107]。例えば、企業や国家が知的財産の研究開発、特にテクノロジー（量子コンピューティング、人工知能（AI）、ロボット工学、ブロックチェーンなど）、輸送、医療、防衛、宇宙機能などに多大な投資を行っているため、さまざまな競争、金融、国家安全保障の目的を促進する**民間の企業に対する攻撃**を行うために雇われた国家支援者や犯罪行為者によるデータ窃盗の動機がますます高まっている。
3. **不正アクセス**：インサイダーの脅威や（犯罪者に）脅された従業員も、サイバー攻撃の動機となる場合がある。意見の相違や個人的な利益により、従業員が組織のセキュリティを危険にさらすことがある[108]。
4. **エゴ**：承認や達成に対する欲求もサイバー犯罪者の動機となる。一部のハッカーは、主要なシステムへの不正アクセスに成功することで評判を高めようとし、より複雑なハッキングを遂行するためにお互いを駆り立てている[109]。バグ報奨金プログラムが大幅に増加したため、ハッカーが攻撃を実行した動機が単なるエゴなのか、それとも脆弱性やシステムへの不正アクセスを公表しない代わりに被害者が金銭を支払うことを期待する金銭的動機もあるのかを判断することが難しくなっている。
5. **憎悪**：サイバーストーカー、ネットいじめ、なりすまし、セクストーション、リベンジポルノなど、個人に対するサイバー犯罪は、憎悪や苦痛や危害を与えたいという欲求がしばしば動機となっている[110]。この種のサイバー犯罪の増加は、ソーシャルメディアの爆発的な利用やプラットフォーム、ハードウェア、ソフトウェアの強化（携帯電話、カメラ、ビデオ編集、ディープフェイクなど）にも直接関連している。

103 https://www.coretech.us/blog/6-motivations-of-cyber-criminals
104 https://www.fraud-magazine.com/article.aspx?id=4295019793
105 https://www.sophos.com/en-us/cybersecurity-explained/threat-actors
106 https://stratixsystems.com/what-are-the-motivations-for-cyber-attacks/
107 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
108 https://stratixsystems.com/what-are-the-motivations-for-cyber-attacks/
109 https://www.coretech.us/blog/6-motivations-of-cyber-criminals
110 https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

サイバー犯罪の範囲は 2013 年から 2024 年の間に大きく変化し、攻撃の割合、侵害によって盗まれた記録の数、金銭的な影響も増加している。サイバー犯罪の動機が変化したことにより、脅威の状況はより複雑かつ困難なものとなり、サイバーセキュリティ対策の継続的な適応と改善が必要となっている。内部者が支援するサイバー犯罪が一般的になり[111]、サプライ チェーンが組織のセキュリティに対する大きな弱点となっていることから[112]、テクノロジーを利用して財務的および経済的な競争上の利益を達成する機会もまた魅力的であることが証明されている。

サイバー犯罪者、特にランサムウェアグループとその関連メンバーは、攻撃を実行するのが簡単であること、および関係者や共謀者全員を捕らえて責任を取らせようとする執行当局にとっての課題が増大していることから、日々大胆さを増している。抑止力の欠如が、グループによる重要なインフラや商業の分野への攻撃を招いている。2024 年だけでも、銀行取引システム、主要な医療提供者の支払いシステム、州政府や地方政府などへの攻撃が観測されている。攻撃の規模、範囲、範囲は拡大し続けており、発生する経済的破壊への対応がますます困難になっている。

同時に、サイバーセキュリティ業界は急速な成長を遂げており、求人数は増加し、熟練した専門家が不足している。サイバー犯罪の頻度と影響が増大していることを反映し、サイバーセキュリティに対する世界的な優先度が高まっており、企業、組織、そして一般の人々がサイバーセキュリティを受け入れることが不可欠となっている[113]。

サイバー犯罪の世界的なコストは、2025 年までに年間 10 兆 5,000 億ドルに達すると推定され、経済的な富の大幅な移転を意味し、イノベーションと投資に大きなリスクをもたらす[114]。サイバー犯罪の状況の変化は、増大する脅威と効果的に闘うための強固なサイバーセキュリティ対策、意識の向上、熟練した労働力の必要性を強調している。さらに、捜査官は、実行されている「犯罪」を考慮せずに「サイバー」の技術的な詳細だけに焦点を当てるのではなく、サイバー犯罪のあらゆる側面を考慮して、犯罪行為の全範囲を完全に理解し、捜査し、解決する必要がある。

本章では、サイバー犯罪の理解と評価における「スコープ」の概念を探る。犯罪の性質、標的化の目的（TTP が促進する設計された目的を達成するため）、および公的組織と民間組織の違いについて説明する。本章は、組織が調査を指示するためのガバナンス基準を定義し、防御と保護のための関連するポリシー、システム、手順を策定するのに役立つ。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪にはどのような「特性」があるか
- サイバー犯罪が標的とする組織機能にはどのようなものがあるか
- インサイダーとサプライチェーンはサイバー犯罪の脅威と影響をどのように拡大してきたのか
- そのような機能に対するリスクは、官と民の組織でどのように異なるか

111 https://www.code42.com/blog/insider-threat-examples-in-real-life/
112 https://www.bluevoyant.com/knowledge-center/supply-chain-attacks-7-examples-and-4-defensive-strategies
113 https://ung.edu/continuing-education/news-and-media/cybersecurity.php
114 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

サイバー犯罪のスコープにおけるトピックス分類

「サイバー犯罪のスコープ」知識領域におけるトピックスの分類を図 4-1 に示す。

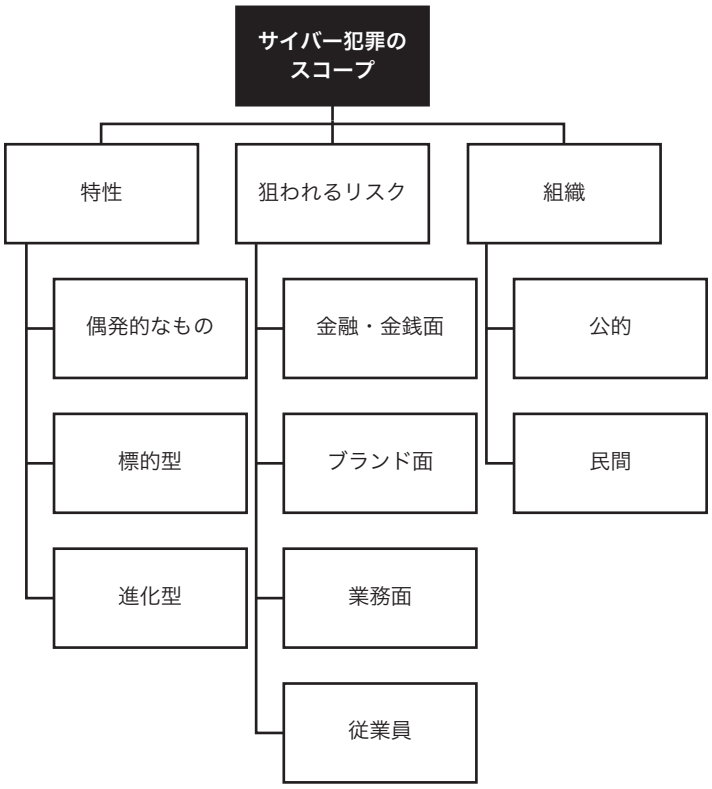


図 4-1.「サイバー犯罪のスコープ」知識領域におけるトピックスの分類

サイバー犯罪のスコープとは

サイバー犯罪のスコープは、サイバー犯罪組織の規模と、被害者または被害を受けたコンピュータのスコープに関係する。サイバー犯罪はそれぞれ異なる特性を持っており、攻撃者が狙う組織的または個人的リスクの点に違いがある。したがって、被害者のスコープも異なる。たとえば、サードパーティの（標的を釣るためにスパムやフィッシング、水飲み場型攻撃を使う）ボットネット開発者は、通常小規模または独立した仮想プラットフォーム運用者で、組織の規模は小さい。ただし、目的がばら撒き型の（ドライブバイダウンロード攻撃のような）不正アクセスの場合には、標的のスコープが非常に広いこともある。逆に、ボットネット開発者が提供するアクセスを利用する側が大規模な組織を持っており、開発者や管理者のみならず高いスキルを有するビジネス経験・知識を有する要員がいて、標的組織の経理・財務システムやプロセスといったリソースを目標として、標的型攻撃を仕掛ける場合がある。そのような場合は、標的のスコープは狭いが潜在的リスクは大きい。「第 2 章 サイバー犯罪の種類」および「第 3 章 サイバー犯罪のアーティファクト」で述べたように、サイバー犯罪の種類とアーティファクトは複雑であるが、究極的にサイバー犯罪のスコープを（影響の分析のために）判断する際は、実行された犯罪の目的は何か、、だれが利益を得るのかに依存する。

標的のコンピュータおよびネットワークに対する攻撃または不正アクセスの評価で、捜査官がスコー

プの問題を見落とすことが少なくない。相互接続しているときはパートナーやベンダーのネットワークも含めて、IT 環境全体を評価すれば明らかな犯罪も、目立たないインジケーターに注目しすぎると、犯罪を近視眼的に（狭い見方で）捉え、誤解してしまうことがある。捜査官がサイバー犯罪のスコープを判断するための、組織全体的な証拠の情報源および証拠の収集と分析の手段については、「第 5 章 証拠の情報源」から「第 7 章 証拠分析の方法」で説明する。

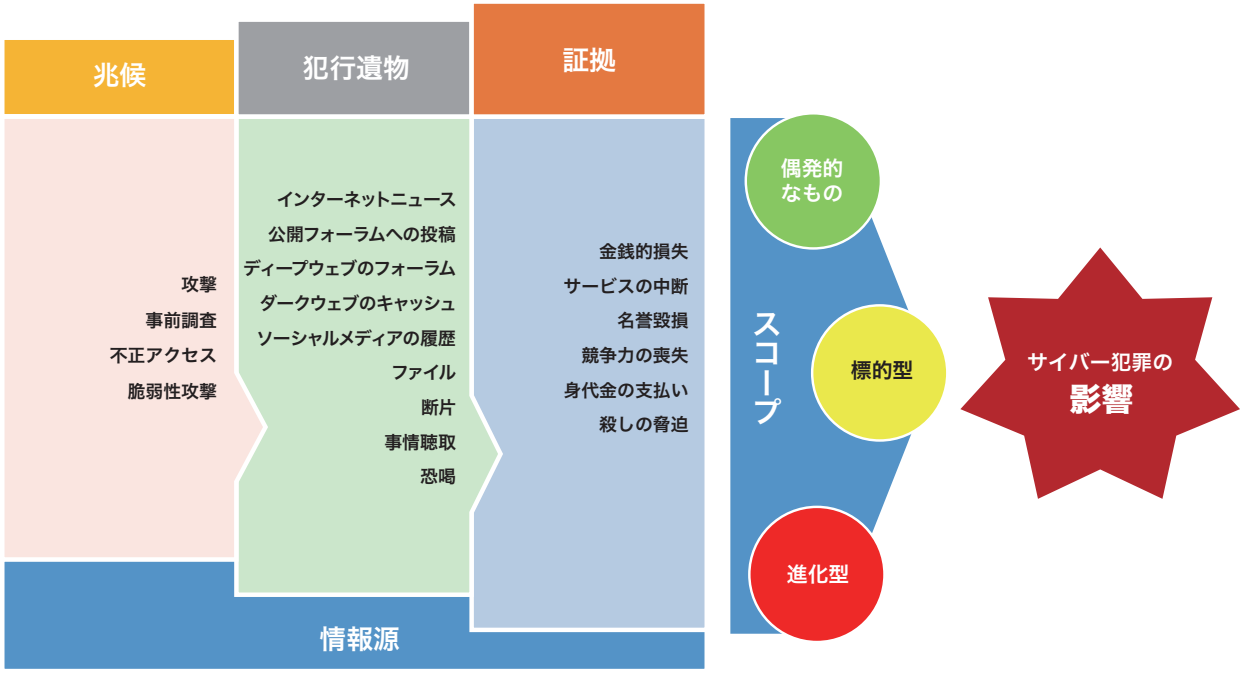


図 4-2. サイバー犯罪のスコープ

技術の進歩によってデジタル時代が到来した。個人も組織も毎日の生活や仕事の効率を向上する手立てとして技術に依存し、重要視している。そして、新しいアプリケーション、よりよいアプリケーションを生み出そうとする絶え間ない競争によって、世界はフラット化した。世界中で大勢の人々が技術の利便性と力を活用している。その多くはインターネット接続を使った利用である。コミュニケーションやエンターテインメント、ショッピング、学習、銀行取引、ヒーリングから創作に至るまで、さまざまな需要を満たしている。人の暮らしは間違いなく進歩しており、相互に結ばれた世界は繁栄と機会を我々にもたらした。

我々の暮らしを改善してきた技術的進歩（この場合はインターネット）のほとんどは、不正な目的でそれらの技術を利用する機会を生み出すことが多い。歴史的に、物理的な世界の建物や警備員、国境、水路といった存在に加えて、法執行機関による物理的な証拠の収集や法制度上の共通性によって、国際犯罪を抑える戦いが繰り広げられてきた。仮想世界の拡大は、犯罪を実行する機会を増加させた[115]。詐欺、窃盗、スパイ、恐喝といった従来と同じ種類の犯罪を実行する新しい方法は、その大きさ、規模、スコープのいずれにおいても拡大しており、文字どおり「ネットワーク技術による犯罪行為または有害行為の変容」であるとされている[116]。

データ侵害によって盗まれた数十億件もの記録により、サイバー犯罪に参加できる人々の数が増加し、組織的および非組織的なサイバー犯罪グループの規模が大幅に拡大した。最近のできごとで分かったこ

115 Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Doubleday.
116 Tabansky, L. (2012). Cybercrime: A National Security Issue? Military and Strategic Affairs, 4(3), 117-136.

とは、金銭目的のサイバー犯罪活動には、各種の仕事をそれぞれ担当部署に割り振って実行している集団が存在するということである。そういった担当部署にはリクルートによって集められた人材ネットワークが属しており、「運び屋（ミュール）」と呼ばれることが多い。運び屋はサイバー活動には関係しないが、金銭目的のサイバー犯罪で最後の部分を成し遂げるのに必要である。その活動の一環としては、西側社会の法執行機関に非協力的な国に存在する銀行口座に盗んだ金のプレースメント、レイヤリング、およびインテグレーション（すなわち、資金洗浄）を行う活動が含まれる。

FBI は、2010 年の声明で高度に組織化された不正行為の各種機能（下記）を特に挙げ、サイバー犯罪がいかに成長しているかを示した[117]。

- コーダーやプログラマーがマルウェアや攻撃コード、その他犯罪の実行に必要なツールを作成する。
- 頒布者やベンダーが盗んだデータを取引・売買し、その他の専門業者から提供される商品を保証する。
- 技術者がサーバやインターネットサービスプロバイダ（ISP：Internet Service Provider）、暗号化などの犯罪インフラストラクチャおよび支援技術を保守する。
- ハッカーが攻撃に使える脆弱性をアプリケーションやシステム、ネットワークから探し、管理者アクセス権限または従業員名簿へのアクセスを取得する。
- 詐欺の専門家がフィッシングや会社幹部のホエーリング、スパム、ドメイン乗っ取りなどのソーシャルエンジニアリングスキームを考えて実行に移す。
- 協力者が不正なコンテンツを保存するサーバやサイトなどを置く「安全な」施設を提供する。これには、手の込んだボットネットおよびプロキシネットワークが使われることが多い。
- 入金役が振込口座を管理し、名義や口座の情報を有償で他の犯罪者に提供する。また、個人の金の運び屋である「マネーミュール」を仕切るのも、通常はこの入金役である。
- マネーミュールは請け負ったとおりに不正行為の利益を第三者に送金する。その金はさらに安全な場所に送金される。
- 出納役はデジタル通貨サービスを通じて、さらには複数の国の通貨を通じて不正な利益を移転し、資金洗浄する。
- 組織の幹部は標的を選び、メンバーを集めて上記の業務に割り当て、さらには犯罪行為で得た利益を配分する。

組織的犯罪における運用の規模が大きいことは、関与している人員が上記で述べたさまざまな役割や業務にあたっていることから明らかである。再利用可能なツールおよびインフラストラクチャを作成していることからも、犯罪者がどれほど広いスコープの標的を狙い、金銭詐欺や窃盗目的で攻撃を仕掛けようとしているのかが分かる。サイバー詐欺／不正組織[118]がどのように活動しているかを示した図を以下に示す。

117 Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An Analysis of the Nature of Groups Engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

118 https://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-scam.htmlgraphic

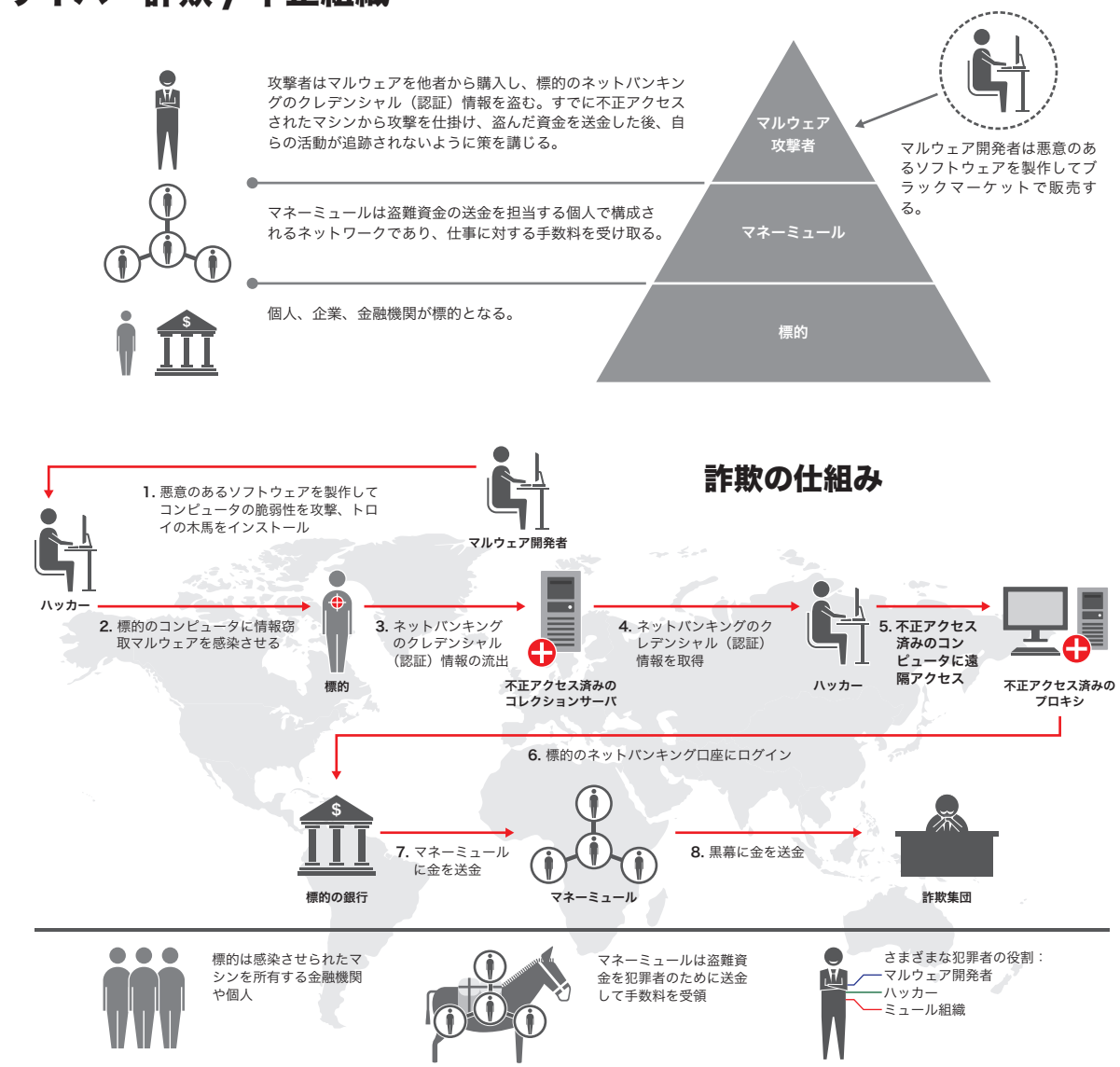


図 4-3. サイバー詐欺／不正組織

「マフィア」のような犯罪ファミリーを思い起こさせる構造モデルと同程度に高度に組織化されているサイバー詐欺組織がどれほど存在し、活動しているかは不明である。例えば 2015 年に起きた米国人事管理局（OPM：U.S. Office of Personnel Management）[119] での金銭的な動機による、ニュースの見出しを独占するような大規模な事件とか、大規模なデータ侵害の責任者を特定し、裁判にかけるようなことは、法執行機関にとっては捉えどころない困難な作業であることが判明している。このように金銭やデータを目的とする大型事件の首謀者を突き止めて法廷の下に連れ出すことは、法執行機関にとって非常に困難を極める仕事である。国際銀行間通信協会（SWIFT：Society for Worldwide Interbank Financial Telecommunication）を通じてバングラデシュ銀行が金を盗まれた事件 [120] と、ハッカーが盗んだ内部情報をもとに証券取引を行った罪を認めた株式トレーダーの 2 つのサイバー犯罪事件 [121] は、サイバー犯罪に使われているサイバーツールが一段と新しいものになり進化しているという点よりも、詐欺や窃盗といった犯罪を実行するために、商業や金融など市場を支える種類のシステムが攻撃を受けているという

119　https://www.opm.gov/cybersecurity/cybersecurity-incidents/
120　http://www.reuters.com/investigates/special-report/cyber-heist-federal/
121　http://fortune.com/2015/12/21/trader-pleads-guilty-in-insider-trading-hacking-case/

点を浮き彫りにしている。この事実によってサイバー犯罪は規模が拡大し、サイバー犯罪の標的も、直接的な標的のみであったのが間接的な標的にまでスコープが広がった。

これによって浮かび上がってくる点として重要なのは次のとおりである。

- ハッカーは、後に続く犯罪目的を実際に果たす実行犯と同一人物とは限らない。
- 極めて儲かる犯罪を実行する機会や能力が発達している。
- これらの犯罪を実行するのに必要なビジネス的知識のレベルが高いことから、幅広い知識と技能を持つ人物が犯罪に携わっていることが分かる。
- 法執行機関や関連調査は、犯罪の特性やスコープに合わせて犯罪の目的に焦点を当てるべきであり、ツールや偶発的な活動を目的の文脈外で解釈してはならない。

ほとんどの人は、サイバー犯罪者の数と、不正ソフトウェアを作成できる人の数は同じだと思っている。犯罪の行為者がサイバー犯罪世界の総人口の一定割合を占めているのは事実であるが、他方、サイバー犯罪者によっては、自分で不正ツールを作れるという特技を生かし、作成したツールを Google や Bing といった主要検索エンジンからでは見つからないインターネットの裏世界で販売する者もいる。この裏のインターネットは人々が毎日閲覧している表の部分（検索エンジンに登録されている部分）よりも広く、ディープウェブおよびダークウェブと呼ばれている。

「第 3 章 サイバー犯罪のアーティファクト」で述べたように、ディープウェブとダークウェブは「ダークネット」とも呼ばれている。ダークネットには「eBay」のようなオークションサイトが無数にあり、さまざまな不正ツール類が取引されている。たとえば、脆弱性攻撃キットやマルウェア、不正アクセス可能なネットワークインフラストラクチャ（サーバーやコンピュータなど）の他、窃取された銀行口座の認証情報やクレジットカード番号、個人情報（PII：Personally Identifiable Information）、進行中の合併や吸収などの企業機密情報が含まれたデータベースへのアクセス権などが売られている。こういった品目は、医療保険会社（例：Anthem BlueCross）[122] や法律事務所 [123]、小売チェーン（例：Home Depot）[124] に侵入するなど、他の違法活動を通して取得される。

ハッキングがもはや単なるイベントではないことは明らかである。これは、ハッカーがネットワークやデータソースにアクセスするのを支援するために、無数の方法やツールを適用することから始まるプロセスである。マルウェア、フィッシング、ランサムウェア、およびその他のアプローチは、標的を絞ったり、チャンスを狙ったりする目的で使用される。侵入後、盗まれたデータはソーシャルメディア、オープンウェブのダンプサイト、ダークネットマーケットプレイス、およびその他の媒体で宣伝され、そこでパッケージ化、再パッケージ化されて販売される。注目すべきは、このような犯罪的な商取引が、最初のネットワーク侵害から数週間、数カ月、あるいは数年後に行われる可能性があることである。ダークウェブ市場の動態に関する説明は、サイバー犯罪の範囲を適切に定義するために捜査官が考慮しなければならない複雑さを明らかにする。

ハッカーは金銭的利益を得るため、または将来的にもっと価値のある情報を入手するために情報を盗む。成功したビジネスモデルと同様に、金銭は需要と供給に基づいて市場価格で商品（この場合は盗まれたデータ）と交換される。盗まれたデータに対する需要は、利益率が高く、法執行機関による措置のリスクが比較的低いため、飛躍的に増加している。ただし、二次犯罪者が投資の利益を得るためには、販売される窃盗情報、侵害されたコンピュータ、またはシステムアクセスが使用可能で有効でなければ

122 http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/
123 http://fortune.com/2016/04/04/panama-papers-law-firm/
124 http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

ならない。同様に、使用可能で有効なデータを提供するというハッカーの評判は、ハッカー自身の投資収益にとって不可欠である。国家レベルのハッカーでさえ、評判の良いサイバー犯罪者から有用かつ有効な情報を得ようとする。評判はサイバー犯罪業界にとって生命線であるため、ハッカーは盗んだデータの品質と有効性を慎重に管理する。

最も優れたハッカーは、盗んだデータを配布用に蓄積する手段を講じた後、サイバーセキュリティプロトコルでは通常検出されない方法（電子メールへの簡単なログイン、口座残高の確認、支払いカードへの少額の請求など）を使用して、情報の有効性をテストする。データの検証には時間がかかるが、いったん認証されると、そのデータはさまざまな犯罪目的（詐欺、インサイダー取引、スパイ活動など）でパッケージ化および再パッケージ化される可能性がある。最後に、ハッカーはデータをインターネットのマーケットプレイスやその他の媒体で販売する。最初のハッキングからハッキングされた情報の将来の使用までのこの時間の経過により、ハッカーと犯罪者のビジネス上の関わりにギャップが生じる。このギャップは、ハッカーが売却するデータの種類に特化し、より目の肥えた犯罪市場に対応する中で拡大を続け、結果としてサイバー犯罪の規模と範囲をますます拡大させている。

データやアクセスの買い手、売り手、再販業者による犯罪経済の急成長は、さまざまな方法と目的でデータを盗むハッカーによって促進されている。これは、フィッシング作戦を実行するハッカー、システムを暗号化しデータを盗むために第2段階のマルウェアを利用するランサムウェアギャングのために第1段階のボットネットマルウェアへのアクセスを促進するハッカー、システムに侵入しデータを流出させるハッカー、国家行為者の標的パッケージの作成を可能にするためにソーシャルメディアサイトを持続的にスキャンしスクレイピングするツールセットを運用するハッカーなどを含む。盗まれた情報や不正アクセスされたコンピュータやネットワークへのアクセスを利用して、詐欺、窃盗、スパイ行為などの犯罪行為に手を染めるのは、2013年以降、被害者や金銭的被害が記録的に増加しているバイヤーである。

サイバーコミュニティではサイバー犯罪サービス（CaaS）[125]としても知られる犯罪サブスクリプションマーケットプレイスの拡大は、Silk Roadと呼ばれるフォーラムの責任者に対する捜査が公表されて以来、急速に進んでいる[126]。サービスとしてのCaaSモデルは拡大し、サイバー犯罪組織は、合法的なビジネスに必要なすべての機能（コールセンター、支払いプロトコルなど）とプロセスを備えたビジネスモデルを成熟させている。CaaS組織はハッカーを雇用し、通常の組織の従業員と同様にインセンティブを与え、コールセンターの担当者を雇用して顧客にサービスを提供し、管理と構造、収益目標、組織目標の明確な階層を作成します。CaaSのビジネスは、それ自体が産業に発展した。

CaaSモデルにおける最大の成長分野は、ランサムウェアである。暗号化マルウェアを作成するグループのすべてではないにせよ、そのほとんどは、ネットワークアクセスを獲得してデータを盗み、ペイロードを展開することを任務とするアフィリエイトメンバーにツールセットを貸し出している。その後、身代金を支払うための暗号通貨のアドレスが被害者に提供され、その代金は悪質なソフトウェアを作成したグループと山分けされる。この収益分配モデルで犯罪活動を組織化することで、犯罪者にとって事業継続性が生まれ、当局がすべての責任者を追及することが難しくなる。それほどセンセーショナルではなく、あまり広く宣伝もされていないCaaSモデルのデモンストレーションが、米国の銀行で毎日のように行われている。このサイバー犯罪は米国を拠点とするストリートギャングによって実行され、彼らはその後銀行詐欺で得た収益を他の犯罪行為に利用している。詐欺の手口は次のように機能する。

携帯電話のバンキングアプリケーションのリモートデポジットキャプチャー機能は、ソーシャル

125　http://resources.infosecinstitute.com/cybercrime-as-a-service/
126　https://www.rt.com/usa/silk-road-bitcoin-shut-650/

メディアを通じて勧誘された参加者の銀行口座に不正な小切手を振り込むために使用される。ギャングのメンバーは、以前は Facebook として知られていた Meta を通じて、主にナイジェリアのサイバー犯罪者と協力し、過去のデータ侵害から得たデータを使って作成した偽の小切手を購入し、入金している。小切手は通常、暗号通貨を使って購入される。偽造小切手を預け入れると、ギャングは複数の場所にある現金自動預け払い機（ATM）の近くにメンバーを配置し、小切手が偽造であると判断される前に口座にある資金をすべて引き出す。自分の口座が詐欺に利用された参加者は、その後、オンラインで口座が乗っ取られたと主張して銀行に苦情を申し立てる。多くの場合、銀行は偽の小切手を預ける前に元の残高の資金を返却する。

CaaS により構成される経済圏は法執行機関にとって闘うべきもう一つの課題ではあるが、情報収集の基礎として匿名化されたプレゼンスを確立し、オンライン潜入捜査を展開し、そして最も重要なこととして、電子情報（ELINT）事象を文脈化し、意味を与えるために必要なタイプの情報、すなわち人的情報（HUMINT）を発見し、評価し、採用する機会を特定するユニークな機会を生み出す。このような種類のインテリジェンスの力を借りて、捜査官はサイバー犯罪組織の目的や規模、標的のスコープに関する知識を評価し、発展させることができる。

以下の図は、ダークネット[127]での活動が確認されている種類の情報、サービス、製品、および犯罪行為者の概要を示している。

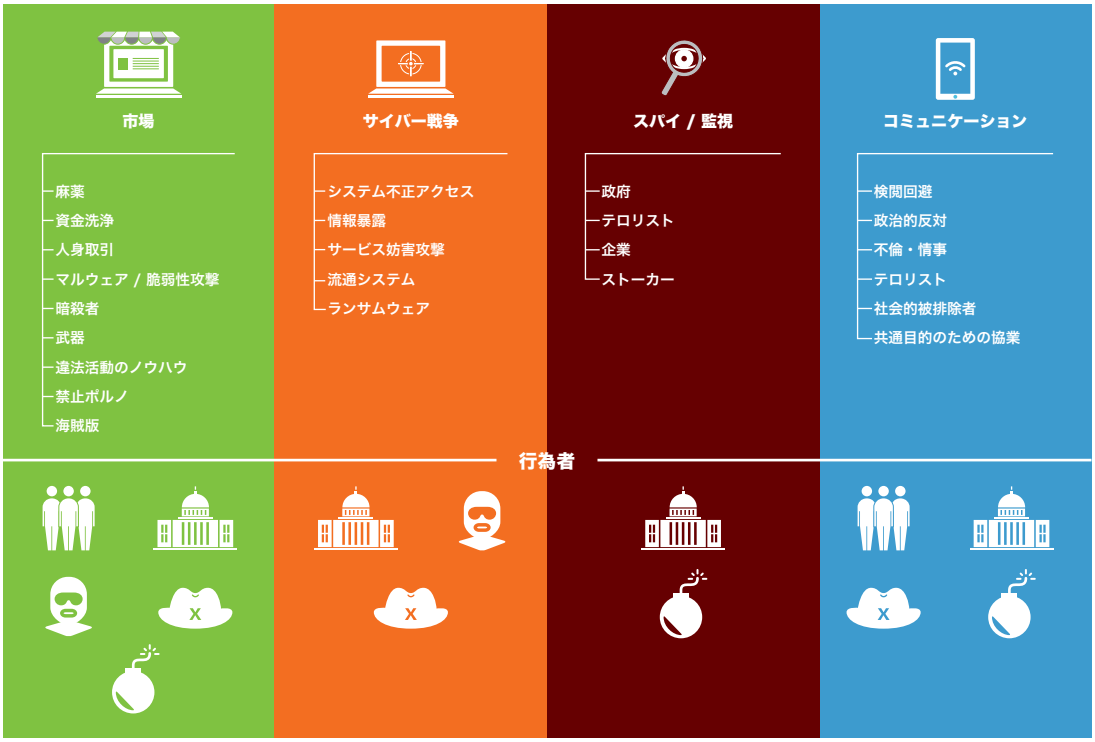


図 4-4. ダークネットでの取り扱い品目

127 https://www.linkedin.com/pulse/darknet-deep-web-explained-bradley-w-deacon, originally found at http://http://www.batblue.com/the-darknet/

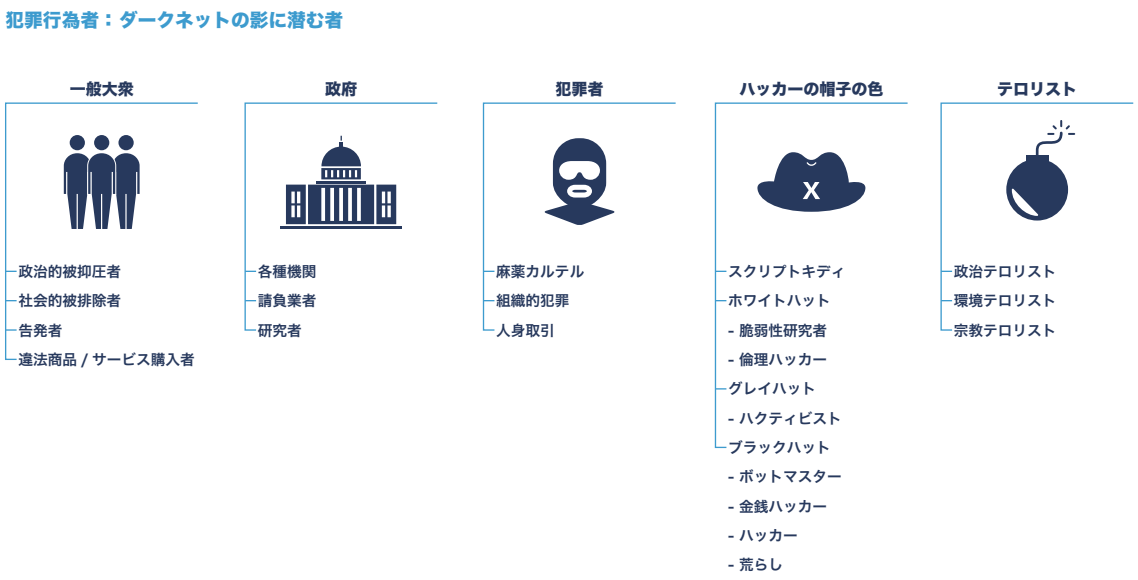


図 4-5. ダークネットのプロファイル

オンラインの世界になって窃盗や詐欺、妨害活動といった犯罪の実行が容易になり、犯人が捕まらずじまいの場合も多い。オンラインであれば、世界中の異なる司法管轄区に個人や集団が散らばったままでも簡単に仕事ができ、その後解散して身を隠すことができるからである。犯罪活動との関係が以前よりも隠しやすいため、大規模な経済的被害を与えられるようになっている。これは、暗号通貨（ビットコインなど）などの発明と、それが前述のダークネットの仮想地下市場において重要な役割を果たしているからである。サイバー犯罪者がさまざまな目的のためにコンピュータ技能を使う機会を得たことで、極めて高度な法執行機関であっても対応が難しくなっている。

この混乱は、リソースを混ぜ合わせ、悪意のあるソフトウェアツールを使用し、（相互接続）ネットワークインフラストラクチャを共有し、ペーパーカンパニーを利用し、偽の（または盗まれた）ID の下で銀行口座を管理し、犯罪を実行する洗練された犯罪者に利用され、法執行機関は犯罪を捜査すべきかどうか、どのように捜査すべきかを判断するために多大な時間を費やすことを余儀なくされている。その「方法」については、第 1 章で述べたように複雑な管轄権の問題があり、テクノロジーや関連するサイバー犯罪の進化に追いついていない手続きに阻まれることもある。

今日のサイバー犯罪の複雑さを完全に理解するには、デジタル資産、特に暗号通貨の進化する役割と使用について深く議論する必要がある。暗号通貨は消費者や金融機関に広く採用されるようになり、最近の米国証券取引委員会（SEC）によるビットコイン（BTC）上場投資信託の承認により、資本市場でも広く採用されるようになった。Mastercard 社の CipherTrace によると、「暗号通貨の時価総額は、2019 年 1 月 1 日の約 1,350 億ドルから、2022 年 3 月 31 日には 2.1 兆ドル弱にまで増加しており、これは 1,456% の増加である。暗号通貨の時価総額は 2021 年 11 月に 3 兆ドル近くでピークに達し、その時点でビットコインは史上最高値の 68,790 ドルを記録した」[128] Ciphertrace による報道以来、ビットコインは最近 70,000 ドルの閾値を超え、時価総額の史上最高記録を更新した。

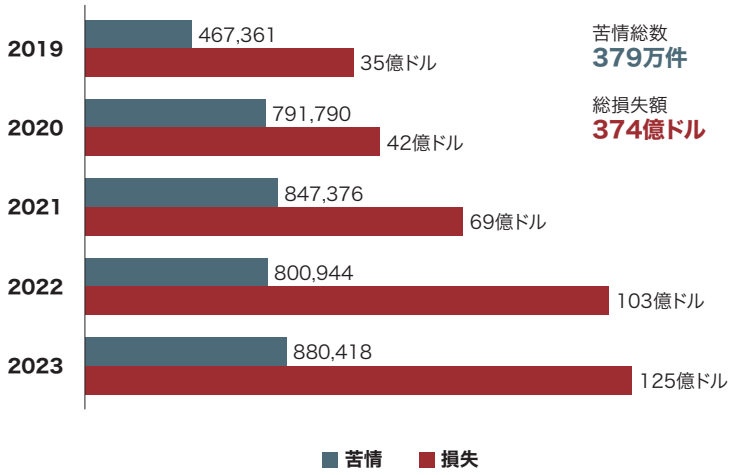
暗号通貨市場が拡大すると同時に、業界全体でインサイダー取引、詐欺、破産手続きが急増し、サイバー犯罪者、テロリスト集団、国際組織犯罪による暗号通貨の大幅な導入も進んだ。暗号通貨は、ほとんどのサイバー犯罪者の活動にとって不可欠なものとなっている。これらの通貨が提供する匿名性の高さは、法執行機関が取引を個人や不換紙幣の清算口座を仲介する交換業者にまでさかのぼって追跡することを困難にしている。これにより、ダークネット上での麻薬密売、武器販売、ハッキングツールの販

128　暗号通貨犯罪とマネーロンダリング対策、CipherTrace、Mastercard、2022年6月レポート

売などの違法行為に暗号通貨が一般的に使用されるようになり、他の犯罪の中でもランサムウェア攻撃の増加が促進された。暗号通貨の非中央集権的な性質は、こうした取引が従来の法執行機関の手の届かないところで行われることを可能にしている。

デジタル資産と暗号通貨が業界やエコシステム全体で急速に採用され続けるにつれて、重要な調査結果を特定して報告するためにデジタルフォレンジックと暗号通貨に関連するデータの詳細な調査を統合することがますます不可欠になる。ブロックチェーン取引の複雑さを理解し、所有権と個人への帰属を追跡する能力は、詐欺、盗難、恐喝、詐欺行為、その他の違法行為に関連するイベントを調査する上で非常に重要である。全体的に、暗号通貨は数多くの利点を提供する一方で、その分散化と匿名性という性質は、サイバー犯罪と戦う法執行機関にとって課題も示す。暗号通貨の人気と採用が拡大するにつれ、サイバー犯罪者が暗号通貨を違法な目的で利用し続ける可能性が高く、サイバー犯罪の範囲がさらに拡大するであろう。

捜査官や諜報機関がサイバー犯罪組織の規模を把握できない限り、実行される犯罪の影響を受ける標的のスコープを理解することはできない。サイバー犯罪の拡大を裏付ける証拠は、連邦捜査局（FBI）の2023年の最新の米国インターネット犯罪苦情センター（IC3）年次報告書に記載されている[129]。報告書から抜粋した以下のグラフは、2019年から2023年までの苦情件数と被害額、2023年の各種サイバー犯罪の影響、被害者の年齢層別の影響をまとめたものである。



quickly evolved

129 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

サイバー犯罪の特性

サイバー犯罪捜査においては、サイバー犯罪者によって使われたネットワークインフラストラクチャ（すなわち、サーバやIPアドレス、ウェブサイト、ドメインなど）の識別と無力化、マルウェアがどのような機能でどのような挙動なのかの調査（すなわち、リバースエンジニアリング）に過度な注意が向けられ、焦点が当てられてきた。こういった捜査活動は重要ではあるが、それは犯罪活動の規模とスコープを判別するという場合においてのみである。これらの捜査活動は捜査を支援する分析員が行うべきである。これによって得られた情報は、捜査進行（または捜査結果の解釈）の基礎として使うのではなく、データポイントとして用いるか、捜査における事実としてリストアップして使う。

サイバー犯罪捜査およびインシデント調査の開始のきっかけとなるのは、ほとんどの場合、公式の発表や組織による自主的な報告、法執行機関の通知である。情報は、ヒューミント（HUMINT）、シギント（SIGINT：SIGnals INTelligence、通信や電子信号等を介した諜報活動およびそれによって得られる情報）、一般に公開されている調査結果をはじめ、さまざまな情報源からもたらされる（「第5章 証拠の情報源」で説明）。場合によっては、組織内のセキュリティ監視ツールが発したアラートに対応する形で捜査が始まることもある。被害者との初期の接触プロセスにおいては、被害者組織が官民のどちらかに関係なく、以下の質問一覧（注：すべてを網羅しているわけではない）に対する詳細な答えを得ることが極めて大切である。大部分は被害者が協力的でなければ得られない質問であるが、調査の方法論とアプローチを決定するのに役立つ材料となる。

1. 組織のだれが、いつ標的となったのか？
2. 標的にされたシステムの種類は？
3. それらのシステムが使われているビジネス部門は？
4. 機密データやアプリケーションに不正アクセスはあったか、そしてあった場合のリスクは？
5. 標的にされたシステムはその後どのように使われたか。たとえば、他のシステムにアクセスするための踏み台に使われたか？使われた場合、上記の質問に対する答えは？
6. このインシデントで最も心配なことは何か。たとえば、非公開の保護情報の消失、ブランド価値／評判の低下、経済的損失、事業の中断、訴訟、その他？
7. 攻撃者を名乗る相手から連絡はあったか？あった場合、相手の要求は？
8. 証拠収集目的で必要な法的書類（召喚令状、国家安全保障書簡、同意文書など）を届けるために連絡をとるべき組織側の窓口はだれか？

このアプローチは、従来の詐欺や窃盗、マネーロンダリング（資金洗浄）、スパイ、その他の犯罪捜査を行うときとおおむね同じである。サイバー犯罪の性質に応じて範囲を定義することは、誰が犯罪を行ったのか、あるいはもっと重要なことは、なぜ彼らが犯罪を行ったのかを証明するためにほとんど不必要な手続きに時間と資源を浪費することを避けるために、決定的に重要になる。調査チームが犯罪の本当の特性（ほとんどの場合、システムへの単なる不正アクセスではない）を正しく識別できれば、いっそう意味のある法律を適用するための構造を構築できる。なぜなら、特に米国の法律においては、送金詐欺や資金洗浄といった犯罪に対する刑罰の方が、不正アクセスや「コンピュータ詐欺と濫用に関する法律」（CFAA：Computer Fraud and Abuse Act）違反よりも重いからである[130]。

よく知られた商用マルウェアでさえ、複雑なサイバー犯罪を容易にこなせるほど進化しているため、

130　第1章と第2章で説明したとおり。

先に掲げた一覧のような質問をサイバー犯罪捜査で尋ねることが以前にも増して重要である。不正アクセスされた後、マルウェアによってすでに不正アクセスされている他のコンピュータのネットワークに加えられたコンピュータはすべて「ボットネット」に所属することになる。ボットとは「マルウェアの一種で、ボットに感染したコンピュータやモバイル機器、**IoT 機器**は、攻撃者による操作が可能となる。この方法で同一の攻撃者の管理下に組み入れられたマシン群あるいはネットワーク化されたマシン群を『ボットネット』と呼ぶ」[131]。ボットネットは自動タスクを実行可能で、DDoS や、スピアフィッシング攻撃用の電子メールスパム送信など、さまざまな種類のサイバー犯罪で悪用される。複数の独立したサイバー犯罪者が使うこともあれば、互いに連携しているサイバー犯罪者が使うこともある。商用ツールの出現でだれにでもボットネットを構築できるようになり、商用サービスによってだれもがボットネットを運用できる。

マルウェアには数多くの種類があるが、その多くは「ボットネットマルウェアの元祖」と呼ばれる「Zeus」の派生形である。マルウェア Zeus はもともとダークネット上の多数のフォーラムで販売されていたが、2011 年にインターネット上で公開され、無償で利用／開発が可能となった [132]。ボットネットの規模がそれ以来世界中で爆発的に拡大したのはおそらく偶然ではない。この広く普及したボットネットマルウェアの（有償および無償の）派生バージョンが絶え間なく公開されている。先に述べたように、CaaS が成長したのは、基盤となるインフラストラクチャが使えるようになり、CaaS に関心を持つサイバー犯罪者が出てきたためである。これらのサービスは利用が登録制となり、マネージドアクセス方式で不正アクセスが可能なコンピュータを使える形に進化した。*「A Dummies Guide to 'Insider Trading' via Botnet」（初心者にも分かるボットネットを使った「インサイダー取引」ガイド）*[133] と題する記事でボットネットの進化の歴史が説明されており、CaaS プロバイダが提供するサービスが単純なものから複雑なものまで紹介されている。この記事の要点をいくつか下記に示す。

もともと、ボットのネットワークが設計され使用されたのは、犯罪の作戦活動に参加するノードをできるだけ多数集めるためであった。従来のボットネットは、以下の活動を実行するために侵入とデータの窃盗に注力していた。

- システムの遠隔操作
- サービスの中断／停止
- 個人情報窃盗（ID／個人の信用情報／ネットバンキング情報）
- 年月を経て、ボットネットは他にも以下のサービスを取り込むようになった。
- 窃取した情報のドキシング（Doxing、個人情報をウェブ公開して公にさらす）／列挙（Cataloging）／販売
- 企業システムに対するオンデマンド型の攻撃およびアクセス提供
- システム上へのサードパーティ製マルウェアのインストール（リモートアクセスツールやランサムウェア）

現在では、以下のマネージドサービスもボットネットで提供されている。

- 匿名通信のルーティングおよび掲示
- 利用登録式ネットワーク／コンピュータへのアクセス管理
- 24 時間／365 日の技術サポートを含むヘルプデスクサービス

131　https://www.fssecure.com/en/web/labs_global/botnets
132　https://github.com/Visgean/Zeus
133　https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet/

- ペイメントサービス（電磁的資金転送または「暗号」資産（仮想通貨）取引）
- ダークウェブ製品およびサービスを扱う市場

これらのボットネットの背後にいる「ボットマスター」と呼ばれる行為者たちは、アクセスの貸し出しを通じて上記のような運用で大型の共同作戦に加担し、同時に個人的な利益をあげている。従来のボットネットは「オーナーによる運用」であったが、ボットネットが儲かるとの評判が知れ渡るようになるにつれて組織化が進んだ。もとはボットマスターがサービスを決めていたのが、商品やサービスが利用者の求める形に進化した結果、顧客志向の産業へと発展した。多岐にわたる登録利用者の要望は、一般的に最近のボットネットで提供されているマルウェアに反映されており、これには下記の種類がある[134]。

- 個人情報収集ツール：一般消費者を標的とするツールで、スパムまたはフィッシングによって拡散される場合が多い。なりすましや個人的な金融信用詐欺、ネットバンキング詐欺、ネットトレーディング詐欺に使えるクレデンシャル（認証）情報やその他の個人情報（PII）を狙う。
- 企業情報収集ツール：企業の従業員や役員を標的とするツールで、通常はフィッシングを介して行われるが、ソーシャルエンジニアリング技法の助けも借りる。ソーシャルエンジニアリングで組織内の個人やビジネス部門を狙い、人事情報やクレデンシャル（認証）情報（およびコンピュータアクセス情報）を盗み取って、ERP システムや電子小切手決済（ACH）、電子送金（EFT）を使った金融詐欺や窃盗をはたらく。
- 市場情報収集ツール：スピアフィッシング、または「水飲み場型攻撃」といった巧妙なマーケティング技法を使い、悪意のある広告を表示する。広告の表示先は特定業種の読者がよく利用するウェブサイトや、登録申請またはソーシャルメディアを介した紹介で相互に信頼できる利用者同士の輪を作るビジネスネットワーキングサービスである。通常、これらは民間企業の役員や弁護士・会計士、金融サービス機関、関連のメディアサービスを標的とする。情報収集ツールは、インサイダー取引に役立つ保護情報や機密情報の窃取を容易にする。

上記に使われているマルウェアの設計は共通であり、異なるのは、だれを標的とするのか、各種情報を窃取するためにどのような指示を行うのか、どの C&C サーバーと通信するのか、といった点だけである。**犯罪の種類を特徴付けるのは、もはやどのツールが使われているかではなく、活動の証拠である。**証拠が存在する場所は、基本的に次の 3 か所である。すなわち、窃取された情報が保存され、登録利用者に対するアクセスが提供されている C&C サーバーと、詐欺が実行された被害者の預金（または取引）口座、不正利用の評価に使える履歴が残っている被害者コンピュータの中のアーティファクトである。

残念ながら、歴史的に見て、多くのサイバー犯罪（例：組織内への侵入）捜査は、コンピュータが標的となったことを証明することに焦点が当てられてきた。そのため、システムへのアクセスを確保した後、使われたコードの種類を調べることによって、「だれが侵入したのか」を突き止めようとする点に力を入れすぎていた。サイバーコミュニティにおいては、これを「アトリビューション」と呼ぶ。サイバーセキュリティ調査会社やサイバーインシデント対応会社の多くは、インシデント調査レポートで、だれが攻撃を行ったのか、または本当の目的は何であったのかという結論を出すために、証拠となる情報をほとんど示すことができていない。インシデント調査レポートのようなマーケティング資料は、意外にも不幸な結果として、法執行機関や民間組織の多くにおいて、ほとんど犯罪捜査の経験がない分析員に基づいて調査方法が定められ、拙速な調査結果が出されるという傾向を顕著にした。

先に述べたように、侵入イベントの技術面にのみ焦点を当てたのでは視野が狭くなり、実際に起きた

134　https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet-part-2/

犯行が何であったのかを特定できなくなる可能性がある。「目的」に基づく帰属、すなわち犯人が狙っているもの（再販を含めた各種目的の業務妨害、詐欺、窃盗、社会的ひずみ、機密、個人情報（PII）、クレデンシャル（認証）情報）によってだれが利益を得るのかを考えることにより、捜査の特性をスコープ内で適切に評価および定義できるようになるからである。コードの「識別」に基づく帰属は非常に難しく、ヒューミント（HUMINT）やシギント（SIGINT）、場合によっては資金洗浄インテリジェンス（MLINT：Money Laundering INTelligence）、オープンソースインテリジェンス（OSINT：Open Source INTelligence、オシント）など、他のところで収集された証拠との関連性を見たり、それらの証拠の助けを借りたりしなければ帰属は決められない。捜査で収集および分析する技術的アーティファクトはインシデントのリスクを把握するのに重要な場合があり、これは特にサイバー犯罪者が狙っていた情報または機能が、証券取引または送金などの管理されたビジネス機能の場合に当てはまる。ただし、エリント（ELINT）のみに基づいて個人を識別するのが捜査の焦点となっている場合、捜査の効力とスコープが狭くなりすぎ、他の政府機能や商業、社会の安定に対するリスクを完全に見落としてしまうかもしれない。

スコープの問題をよく表しているのが2016年の一連の「SWIFTハッキング」事件である[135]。この事件では、ボットネットマルウェアに帰属する不正アクセスを介して銀行間専用の支払いネットワークアプリケーションが不正に利用され、数千万ドルもの送金詐欺が実行された。盗まれた金の転送と資金洗浄にオフショア口座[136]が利用され、その後、手を組んでいたサイバー犯罪者らによって現金が引き出された。このサイバー犯罪はボットネットによる銀行への侵入をはるかにしのぐ内容で、銀行のプロセスや手続きに関する具体的な知識を有する人物の他、明らかに異種の組織（ボットマスターおよび登録利用者）が絡んでいた。これらの活動は異なる犯罪組織によって何度も繰り返されているため、今のところ規模は不明である。一方、スコープの方は、不正送金詐欺を通じて送金および窃取された金額から明らかである。

伝統的犯罪は、だれが「手段、動機、および機会」を持っているか、そしてだれが利益を得るのかによって評価される。サイバー犯罪では、捜査官は最初にスコープを評価しなければならない。そのためには、「特性」を把握することが何よりも重要である。サイバー犯罪の特性を以下の図に示す。

図 4-6. サイバー犯罪の特性

135　http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C
136　http://www.theregister.co.uk/2016/06/28/swift_victim_ukraine/

偶発的なもの

偶発的なサイバー犯罪は、著名ブランドを騙ったメッセージを不特定多数へ配信するようなスパムキャンペーンなどの標的を「引っかける」ためのツールを開発し、利用するときの後知恵または結果として実行される犯罪である。このときの標的は意図的に狙うのではなく、特定の層／業種の人物が他者よりも興味を持っているテーマやサイト全般に注目する。通常、偶発的サイバー犯罪は単純な「コンピュータ詐欺と濫用に関する法律」（CFAA）違反、つまりは「不正侵入」などの不正アクセスである。

標的型

偶発的サイバー犯罪とは対照的に、標的型サイバー犯罪は意図的なもので、特定の対象または人物を狙う。言い換えれば、攻撃の標的は個人のこともあれば、組織機能（経理、法務、人事、IT、その他）のこともある。標的型サイバー犯罪はフィッシングやホエーリング（組織の幹部を狙う）、水飲み場型攻撃など類似のツールを使うが、標的とするのは競合上の利益または相当に大きな利益を生む特定の個人または組織、集団である。

標的型のサイバー犯罪は一段と具体的な目的や目標を持っている。たとえば、転覆（評判または運営を崩壊させる）や窃盗（情報の窃取、保護情報をもとに市場機会を利用する、金銭を盗む）、破壊活動（アクセスや利用の停止、事業の中断）などである。この場合は、システムや施設、従業員が個別に、あるいは同時に、目標を達成するための標的となり得ることに注意が必要である。

進化型

進化型のサイバー犯罪は偶発的活動と標的型活動が組み合わさった結果、発生するものである。たとえば、すでに述べたように、特定の銀行で詐欺をはたらこうとするサイバー犯罪者であれば、その銀行が所有するコンピュータへの不正アクセスをすでに成功させている独立したサードパーティハッカーがいるダークネットへ行き、ボットネットサービスに登録して、BaaS（Banking as a service）サービスプロバイダカタログに加えられている不正アクセスサービスを利用するだけでよい。

サイバー犯罪は、必ずしもボットネットやカスタムツール、すなわち巧妙に用意された攻撃を使って組織外部からのみ行われるものではない。サイバー犯罪捜査官が見落としがちな問題の元がいることを忘れてはならない。つまり、第三者が不正アクセスして犯罪を実行できるように、インサイダーが何らかの役割を果たした可能性である。インサイダーとは、銀行口座情報、経済データ、軍事機密への電子アクセスを支援するために犯罪組織や外国の諜報組織によって採用された組織内の個人を指す。彼らは、すべての組織が日々機能するために依存しているサプライチェーンに存在する。サプライチェーンは、組織が商取引を行ったり、公共に奉仕する使命を遂行したりするために必要な人材（例：請負業者や下請け業者）、プロセス（例：データストレージサービス）、サプライヤー、およびテクノロジ（例：ソフトウェア）として定義される。

インサイダーとサプライチェーンは、サイバー犯罪の脅威、影響、範囲をいくつかの方法で大幅に拡大した。

1. **インサイダーの脅威**：特に重要な情報技術システム、ERP システム、データベース、財務／財務報告、研究開発（R&D）などへの内部アクセス権を持つ従業員や個人は、重大なリスクをもたらし、悪用の標的になることが多い。インサイダーは、意図的であれ無意識であれ、機密情報を漏らしたり、権限を悪用したり、承認されていないソフトウェア・サービスを利用したりする可能性があり、巧妙なフィッシング攻撃を受けやすい。彼らはデータ窃盗、企業スパイ、破壊工作、詐欺などの悪質な行為に関与する可能性がある。インサイダーはシステムに正当にアクセスできることが多く、従来のセキュリティ対策を回避する可能性があるため、インサイダーによる脅威の検出、軽減、調

査は特に困難である。膨大なデータに簡単にアクセスできるため、サイバー犯罪者はアクセスの対象となる個人の記録を作成するために必要なものをすべて持っている

ネバダ州ラスベガスにある MGM リゾーツに対する 2023 年のランサムウェア攻撃は、インサイダーの脅威を利用した攻撃の完璧な事例である。MGM リゾーツの推定損失額は数億ドルに上る。この攻撃は、Scattered Spider（別名 Roasted 0ktapus、UNC3944 または Storm-0875）として知られるランサムウェアグループによって実行され、以下のように実行された。

> 「ソーシャルエンジニアリング攻撃によって、脅威の行為者は MGM の環境に潜り込み、足場を築くことができた。パスワードの再利用というありふれた間違いのせいで、攻撃者は以前のデータ侵害で使用したユーザー名とパスワードを手に入れていた。攻撃者は、価値の高いユーザーの LinkedIn プロフィールから収集した追加情報を使って、ヘルプデスクを騙してユーザーの多要素認証（MFA）をリセットさせようとした。彼らは成功した。」[137]

悪意のあるインサイダーには、データ損失や事業中断の原因となる不満を持つ従業員も含まれる。2013 年のシティバンクの案件がそうだった。

> 「2013 年 12 月 23 日午後 6 時 3 分頃、従業員が故意にコードとコマンドをシティバンクグローバルコントロールセンターの中核となる 10 台のルータに送信し、そのコードを送信することで 9 台のルータの実行中の設定ファイルを消去し、その結果、北米全土のシティバンクネットワークの約 90% への接続が失われた。」[138]

2. **サプライチェーン攻撃**：サプライチェーン攻撃は、サードパーティのベンダー、サプライヤー、またはサービスプロバイダーを標的にして、組織のシステムまたはデータに不正にアクセスする。攻撃者は通常、サプライ チェーンの脆弱性を悪用するか、不正アクセスされた認証情報を通じてアクセスし、信頼できるネットワークやクラウド環境に侵入して、ソフトウェア、ハードウェア、またはファームウェアの完全性を侵害する。サプライチェーン攻撃は広範囲にわたる結果をもたらし、複数の組織や業界に影響を及ぼす可能性がある。たとえば、信頼できるベンダーによって配布されて不正アクセスされたソフトウェアアップデートは、広範囲にわたるデータ侵害やシステム障害を発生させることがある。

   より有名で破壊的なサプライチェーン攻撃の 1 つは、ソフトウェア会社 SolarWinds の侵害によって発生した。攻撃は 2019 年 9 月に始まったものの、2020 年 12 月まで発見されなかった。サイバースパイ行為でロシア政府と結びついていると思われる脅威の行為者が、どのように攻撃を実行したかの概要は以下のとおりである。

   > 「脅威の行為者は、プラットフォームのソフトウェアコンパイルプロセスをハイジャックし、デジタル署名された正規の Orion ソフトウェアアップデートの中にバックドアを設置した。これらの有害なアップデートは数か月にわたって何千人もの顧客に配布された。脅威の行為者はこれらのバックドアのいくつかを悪用して、司法省や国土安全保障省などの米国政府機

137 https://www.cyberark.com/resources/blog/the-mgm-resorts-attack-initial-analysis
138 http://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shut-down-90-of-firms-networks-across-america

関や、FireEye やマイクロソフトなどのテクノロジー大手に侵入した。」[139]

攻撃の規模、範囲、範囲はまだ完全には解明されていないが、おそらく諜報機関のために活動しているロシアの攻撃者が得た情報とアクセスは、その後の情報収集とスパイ活動に利用されるだろうし、実際に利用されている可能性が高い。この攻撃は米国の複数の政府機関に壊滅的な影響を及ぼしたため、米国証券取引委員会（SEC）は 2023 年 10 月に SolarWinds を訴えた。[140]

捜査官は、**犯罪者・攻撃者**が目的とする犯罪を達成する際に、サプライチェーンの各側面がどのように攻撃を受ける可能性があるかを考慮する必要がある。たとえば、官民の多くの組織が、世界中に拠点を置く IT 製品・サービス会社を雇い、利益率の高いビジネス分野を支える大型アプリケーションを作らせている。これらの企業が自社の真の所有者と、政府情報機関（または、競合他社、あるいは犯罪組織）との関係、協力関係を長期間偽り続けることがある。このような企業は、**ベンダーや関連請負業者を雇う前に徹底的な審査プロセスをほとんど採用しておらず、ソフトウェア開発需要の増加に付け込み、審査されていない。**これらの手続き上の脆弱性により、悪質な企業は契約を取得し、システムを開発し、顧客組織が自社のテクノロジーに依存し続けるようにすることが可能になったが、その一方で、サポート対象の組織に関連する他のパートナー、顧客、ベンダーなど、保護された情報へ**いつでもアクセスできる状況が整ってしまった。**そのような会社の従業員や関係者がサイバー犯罪をはたらくと、そのアクセスおよび活動のスコープは非常に広いものとなる。

3. **攻撃対象領域の拡大**：インサイダーとサプライチェーンはいずれも、サイバー犯罪者に新たな侵入口を提供することで、組織の攻撃対象領域を拡大する。インサイダーは、外部の攻撃者が容易に侵害できない機密データやシステムにアクセスできる可能性がある一方、サプライチェーンパートナーは複数の組織とつながっている可能性があるため、攻撃者はネットワーク間を行き来し、連携した攻撃を仕掛けることができる。新型コロナウイルス感染症（Covid-19）のパンデミックによる在宅勤務の急速な拡大、クラウド環境の急速な導入、BYOD デバイスの許可された使用により、攻撃者が悪用するエントリポイントの数が拡大している。もはや、組織が自社発行のデバイス、サーバー、ルータ、スイッチ、および所有する建物内のインターネット／イントラネットアクセスに限定してネットワークやインフラの在庫を簡単に把握、管理、制限できる時代ではない。セキュリティチームが完全に管理できない脆弱性のポイント［家庭用ルータ、モノのインターネット（IoT）機器、ゲームシステムなど］は、悪いセキュリティ習慣（家庭用ルータのデフォルトパスワードの使用など）により、これらのシステムに簡単にアクセスできるため、サイバー犯罪者に悪用されている。これらのデバイスは、サイバー犯罪者が他のシステムにアクセスするための出発点となる。

139 https://www.techtarget.com/searchsecurity/ehandbook/SolarWinds-supply-chain-attack-explained-Need-to-know-info

140 https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html

サイバー犯罪で狙われるリスク

サイバー犯罪は匿名性が高いため、サイバー犯罪者が「組織犯罪」なのか、それとも「国家」による行為なのかを判別するために多大な努力が払われてきた。また、捜査をどこで行うかを決める際には、だれが標的となったのか（例：金融機関）、またはどのようなサイバーツールが使われたのか（例：バンキング型トロイの木馬）のみに基づいて決定されてきた[141]。

サイバー犯罪者によって使われるツール、戦術、および手順は、彼らの目標達成を助けるものでしかない。残念ながら、証券詐欺や市場操作など、金融関係の目的が、金融から競争、評判、政治までをも含むその他の計画を助けている可能性があるという考えは、ほとんど検討されない。また、サイバー犯罪者が用いる戦略が進化し、サイバーツールと戦術の組み合わせによって、インシデント分析員や捜査官らの目を犯罪の真の目的からそらすこともあるので、事態はさらに複雑になっている。この手法は多くの分散型サービス妨害攻撃（DDoS）[142]の他、「第2章」で説明したランサムウェアでも使われている。仮想世界では比較的新しい手法であるが、現実世界で犯罪者が使う攪乱とまったく同じ行為であり、例としてはデモの最中に強盗をはたらくケースがある。

従来は単独のサイバー犯罪に使われていた手法を組み合わせることにより、新たな種類の不正活動を行うモデルが出現している。たとえば、事業の中断を狙う、競合他社よりも優位に立つなどの目的で、DDoSやランサムウェアを提供しているサービスにユーザー登録して利用することもできる。なかには、ある会社に雇われて、同業の競合他社による対抗製品の出荷を遅らせるために、ランサムウェア「JIGSAW」を仕掛けたことがあるサイバー犯罪者もいるという[143]。これと同じ種類の活動でもうひとつの例としては、米国のメジャーリーグ野球チームのスカウト部長が他チームの選手データベースと電子メールシステムに不正侵入したとして、法執行機関が動いた事件がある[144]。進化したサイバー犯罪の最も顕著な例の一つとして、不正トレーダー集団がハッカーを雇って非公開の財務情報や営業実績情報を盗み出し、「差金決済取引」市場で先物取引を行い、最終的に1億ドル以上の不法利益を得たという事例がある[145]。使い方が簡単なサイバーツールが手に入るようになり、技術をほとんど理解していない人物でもサイバー空間で犯罪をはたらけるようになった。

トレンドマイクロ、Dell SecureWorks、インテルセキュリティ／マカフィー、ベライゾンといったサイバーセキュリティ対策企業は毎年、モニタリングと調査に基づいて、官民の組織、ひいては経済に大きな影響を与えるサイバー犯罪の種類を予測している。ベライゾンが公開した「2016年度データ漏洩／侵害調査報告書[146]」によれば「データ漏洩の89%はその動機が金銭またはスパイ目的です」とある。

ベライゾンのレポートからの抜粋として、サイバー犯罪の「動機」と「手法」の図を以下に示す。

141 http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans
142 http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html
143 https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf
144 http://www.cbsnews.com/news/former-st-louis-cardinals-executive-pleads-guilty-to-hacking-houston-astros
145 http://www.forexfraud.com/forex-articles/sec-terminates-cyber-fraud-ring-that-netted-$100-million-in-cfd-trading.html
146 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

攻撃してくる理由は？
敵の目的は？　金銭、盗んだ金、現金、悪銭、拝金…もうおわかりでしょうか。直接的ではなくとも最終的には「金」に行き着くのです。2013 年度の DBIR では、「金銭目的」の王座が「スパイ目的」に奪われることが予測されました。それは実現したのでしょうか。いいえ、現実とはならなかったのです。スパイ目的の件数が最大となった時でもその差はあまりに大きく、金銭目的の独占的地位は揺るぎませんでした。金銭目的はスパイ目的や愉快犯など他の動機をはるかにしのいでいます。

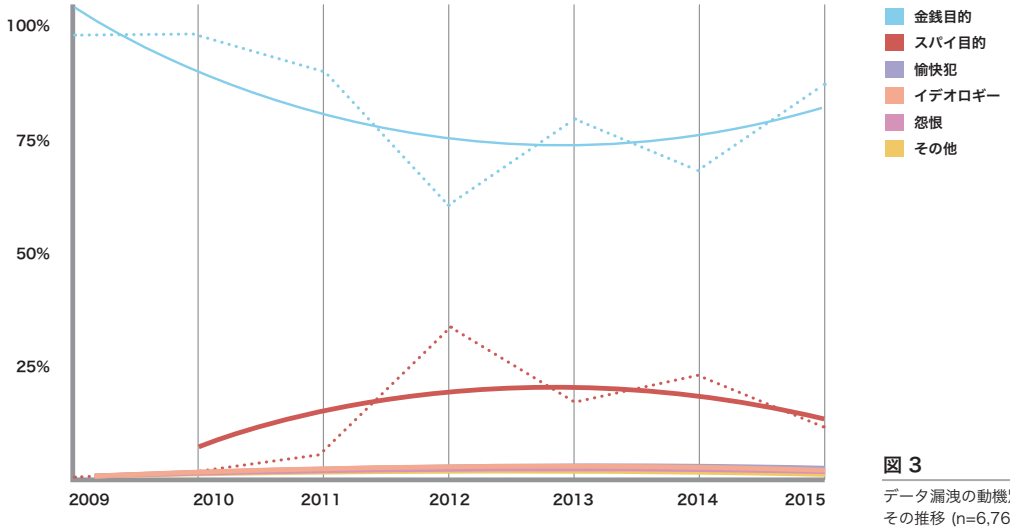


図 3
データ漏洩の動機別割合とその推移 (n=6,762)

図 4-7. サイバー犯罪の動機の傾向

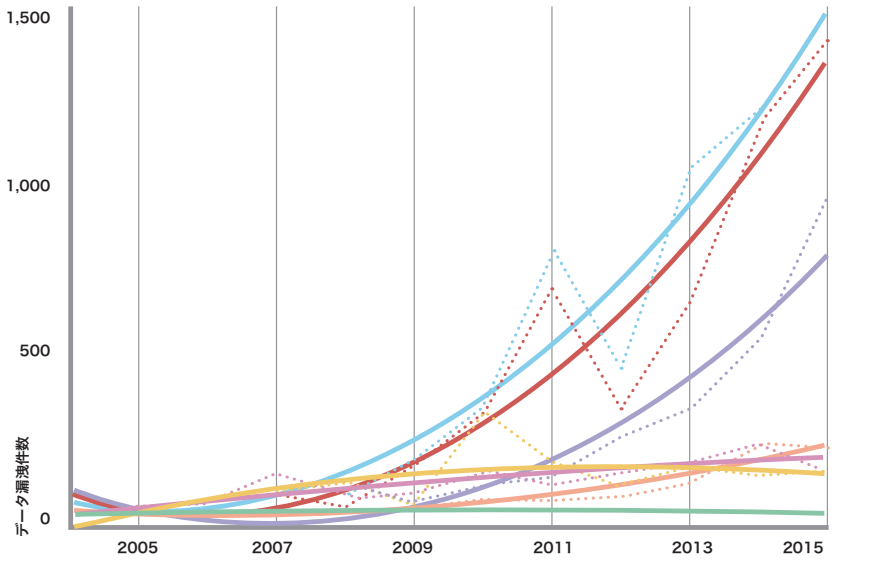


図 4
データ漏洩の脅威カテゴリ別件数とその推移 (n=9,009)

図 4-8. サイバー犯罪で用いられる手法の動向

コンピュータとインターネット（ツール）を使って目的を達成するサイバー犯罪は、2007 年以降、爆発的に増加した（基礎データおよび分析の詳細はベライゾンレポートのデータを参照）。2010 年以降、目的はほとんど変わっていない。金銭目的の犯罪とスパイ目的の犯罪は反対の傾向にあり、2013 年以降は金銭目的が上昇に転じている（同時に、同レポートで見る限り、スパイ目的はわずかに減少している）。技術が新しい種類の犯罪を作ったわけではない。単に、詐欺や盗難、資金洗浄、スパイなどの犯罪が行われる方法に変化をもたらしただけである。技術はツールをもたらしたものの、ハッキングにはリスクまたは脆弱性を標的とした目的が必要である。攻撃対象の脆弱性には、手続き上のもの、技術的なもの、人に関するものがある。

捜査官が「**何を**」、「**どのようにして**」、「**いつ**」といった事柄に答えることができなければ、「だれが」犯罪を行ったのかを正しく証明することも、反証することもできない。ただし、サイバー犯罪の目的を

達成するために狙われたリスクを判別するという行為は、捜査の最初の段階だけで行われる独立した作業ではない。ほとんどの捜査においては、収集した証拠の種類によって軌道を修正する。また、捜査のアプローチを見直すことも多い。したがって、サイバー犯罪の特性と、サイバー犯罪の目的を達成するために脆弱性攻撃を仕掛けようとされているリスクに応じて捜査の「スコープ」を決定することが特に重要である。これによって、捜査を効率的かつ効果的な最終処理へと導くことができる。捜査におけるこれらの原理は、サイバー犯罪の場合でも同様に大切である。実際、ほとんどの事件で捜査が五里霧中で始まることを考えれば、今まで以上に重要である。

ほとんどのサイバー犯罪捜査は、マルウェアによる事件（種類、システム属性、および機能）やコンピュータ（場合によってはネットワーク上の複数のコンピュータ）への侵入または不正なアクセス権限の取得といった行為について、犯罪に使われたツールによってのみ、調査の特性を決めようとする傾向がある。アクセス権限の取得に使われたツールのみを対象として捜査の特性を決めたり、焦点を当てたりしても、「**だれが**」犯罪を行ったのかをはっきりさせるという捜査で最も大切な目的はまず果たせない。物理的な犯罪で言えば、殺人捜査のスコープを、使われた凶器の種類を立証することだけに限定してしまうようなものである。あるいは、ホワイトカラー犯罪の捜査の例であれば、詐欺計画で使われた電話の種類だけを立証するようなものである。

サイバー犯罪においてはそれぞれを個別に分類しようとする傾向があるため、活動ごとに名前が付けられている。標的型サイバー攻撃、分散型サービス妨害攻撃、マルウェア、ランサムウェア、ドキシング、ドライブバイダウンロード攻撃、水飲み場型攻撃、スパム、フィッシング標的型攻撃メール、ビジネスメール詐欺（BEC：Business Email Compromise）、アドウェア、エクスプロイトキット、情報窃盗、コネクトバック通信、その他の新しい専門用語が登場し、法執行機関の職員にとっては理解が難しい頭痛の種となっている。

一般的に、サイバー犯罪関連の新語は、それぞれ対応する従来型の既存犯罪活動またはその道具がある。以下にいくつかの例を示す。

表 4-1. サイバー犯罪と従来型犯罪の関係

サイバー犯罪用語	対応する従来型犯罪または犯罪に使用される道具等
標的型サイバー攻撃（APT：Advanced Persistent Threat）	スパイ
分散型サービス妨害（DDoS：Distributed Denial of Service）攻撃	不法監禁（ビジネス）
マルウェア	違法銃器
ランサムウェア	恐喝
バンキングトロジャン	銀行強盗
ドキシング（Doxing）	ハラスメント、嫌がらせ
ドライブバイダウンロード攻撃	車からの銃撃
水飲み場型攻撃	詐欺
フィッシングおよびスパム	電話マーケティング詐欺
標的型攻撃メール / ソーシャルエンジニアリング	なりすまし
ビジネスメール詐欺（BEC：Business Email Compromise）	詐欺
アドウェア	虚偽広告
エクスプロイトキット	家宅侵入
情報窃盗	窃盗
コネクトバック通信	違法な盗聴

サイバー犯罪者には目的がある。ソーシャルメディアで注目を浴びてはいるが、サイバー犯罪はいた

ずらのためにだけ攻撃を実行しているわけではない[147]。彼らの動機は単純な場合もあるが、複雑なことの方が多い。それは、集団（あるいは、結び付きの弱いものから強いものを含む組織）の活動を推進する人物についても同様である。アナーキズムを標榜する悪党個人でさえ目的を持っている。これらの目的のため、サイバー犯罪者が攻撃を加える対象となるのがリスクあるいは脆弱性である。サイバー犯罪の特性と、一般的に標的となるリスクとスコープの関係を示したのが以下の図である。

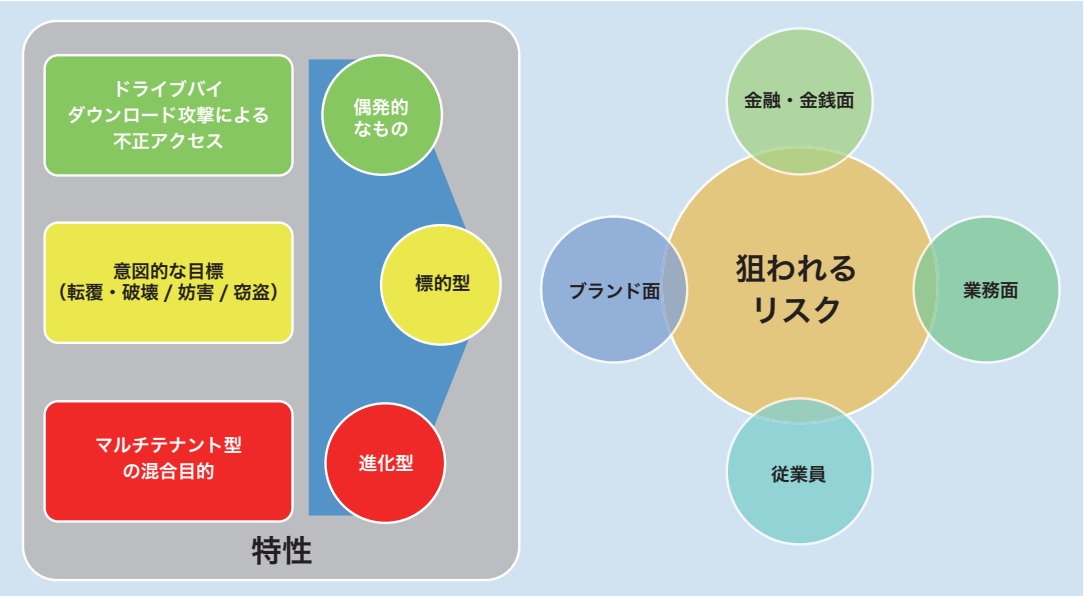


図 4-9. 特性およびリスクとスコープの関係

標的組織（または個人）が狙われる可能性のある個別の脆弱性は多数存在する。しかしながら、独立したサイバー犯罪者か、それとも組織かあるいは金銭的に援助を受けている（国家または何らかの目的のために雇われた）かには関係なく、サイバー犯罪者の主たる狙いをリスク分類としてまとめると以下のとおりである。

金融・金銭面

金融・金銭面のリスクには、民間金融機関の契約やプロセスに直接関係するもの以外に、投資市場に関係するものもある。このようなリスクの例としては、個人、企業、公共、および投資市場の口座や証券を狙って窃取または詐欺／詐称をはたらく目的の脆弱性攻撃がある。金銭の窃盗および詐欺は銀行や証券会社、取引所で発生する可能性がある。通貨としては、法定通貨（Fiat Currency）または仮想通貨の他、信用証券が関係する場合もある。金融・金銭面のリスクとしては、組織または個人が負っている金銭関係の契約義務や資産関係の要件を満たせなくさせるような目的を持った攻撃がある。ときには、金融機関の口座から金を盗む単純な窃盗の場合もあれば、株式、債権、商品先物取引（例：ヘッジファンドがトレードにおける保険として使用する「ショート」または「ロング」のポジション[148]）など、公開される証券に関する市場マインド（および信頼）を左右する可能性のある企業の業績報告の不正操作や非公開情報に基づくインサイダー取引の場合もある。

金融サイバー犯罪のスコープは不正アクセス活動の特性によって変わる。偶発的な不正アクセスでシステムから取得して利用可能となった固有識別子がボットマスターへと送られ、ボットマスター自身に

147 http://arstechnica.com/security/2015/01/come-for-the-lulz-stay-for-the-hacktivism-a-new-book-on-anonymous-reviewed/
148 http://www.investopedia.com/university/hedge-fund/strategies.asp

よって使用されたり、それらを欲しがる第三者に販売されたりする。2014 年以降、組織的サイバー犯罪集団（およびサイバー犯罪を装った国家）の主な焦点となっている標的型および進化型の不正アクセスは大きなリスクである。金融サイバー犯罪のスコープに入るのは個人または組織であるが、連携の有無次第でパートナーや顧客が含まれる場合もある。標的のプロファイルおよび市場アクセス、市場における重要性によって、市場全体（金融および商品）が金融サイバー犯罪によるリスクの対象となる可能性がある。

ブランド面

サイバー犯罪者は、直接的（競争）または間接的（株式市場）な影響を与えることを目的として、標的のブランド価値または市場における信頼の低下を狙うことが多い。ブランドの脆弱性を狙う究極の目的は、非公開で潜在的に気まずいまたは有害な情報を暴露し、その結果として意図した何らかの利益を得ようとすることである。これには、経営者の個人情報や給与[149]、個人的なコミュニケーションの内容をドキシングするといった単純なものから、WikiLeaks[150] などのフォーラムで機密情報を暴露するなどの例がある。

ブランド型サイバー犯罪のスコープは、ほとんどが企業の契約や売上情報、業績データ、人事情報、経営者または顧客のコミュニケーションに照準を当てたものである。通常、ブランドの脆弱性を標的とするサイバー犯罪は標的型であるが、2012 年以降は進化型の活動が増えている。その背景には、標的型攻撃で構築されたインフラストラクチャに、他の集団がめぼしいと感じる何らかの残存価値が残っており、アクセス（収集された情報またはカタログ化された情報源のこともある）がダークネットサービスを通じて提供されていることがある。ブランド型サイバー犯罪は標的だけでなく、関連する従業員、顧客、およびパートナーにも影響を与えることがある。

業務面

さまざまな動機を持つサイバー犯罪によって最も一般的に標的とされるのが業務面の脆弱性である。コンピュータが 1 台あれば、ダークネットのサービスに登録したり、ありふれたボットネットを構築したりして、だれでも標的組織に対して DDoS 攻撃をかけられる。同様に、商品化されたツールと、標的組織のシステムに関して一般に公開されている情報を使えば、ほぼだれでも標的型攻撃や不正アクセス活動を実行できる。マルウェアの多くは一般的に入手可能で、ダークネットサイトからカスタマイズ機能付きのものを購入することもできる。そのため、だれにでも業務面の脆弱性に対する攻撃を仕掛けることができるのである。業務に対する攻撃の目的は、基本的にシステムおよび組織プロセスを中断、妨害あるいは破壊することである（恐喝が絡む場合には人が対象となることもある）。DDoS 不要な空白削除攻撃の他には、ランサムウェアやワイパー攻撃、ルータまたは電子メール／ウェブサービスのハッキング、「IP-PBX オーバーロード」による攻撃[151] などが、業務面の脆弱性を攻撃するのによく使われる。

一般的に、サイバー犯罪者が業務面の脆弱性を攻撃するのは活動家としての目的、または競合上の目的を果たすためであるが、それ以外には、標的組織の調査員や対応員の注意を目立つサイバー犯罪に引き付けておいて、第三者が別の目的を果たしやすくする場合もある。したがって、業務面を攻撃するサイバー犯罪のスコープは、組織全体もしくは業種、あるいは、CaaS による金融・金銭目的またはブランド・競合目的から目をそらすためのかく乱の場合がある。インシデントでは、目の前で起こっている事柄だけでなく、その他に何が起こった可能性があるかを踏まえて評価を行う必要がある。現在のサイ

149 http://time.com/3615160/sony-hack-salaries/
150 https://wikileaks.org/
151 http://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf

バー犯罪活動においては、業務面を攻撃するサイバー犯罪がかく乱としてよく使われているため、捜査官は「それ以外に」何が起こっているかを常に調査しなければならない[152]。

従業員

サイバー犯罪者が攻撃をもくろむ対従業員リスクには、恐喝といった直接的な脅威の他、間接的な脆弱性がある。後者の例としては、個人情報を窃取し、その人物になりすまして金融／証券詐欺をはたらくといったケースがある。従業員リスクがサイバー犯罪者に攻撃される場合、その期間は短いこともある。たとえば、ボットネットマルウェアによって識別情報が盗まれ、詐欺（または情報の窃取）目的で企業システムとアプリケーションが使われてしまう場合である。

従業員を狙うサイバー犯罪のスコープは、活動の特性によって変わる。たとえば、システムと資格情報の偶発的不正アクセスは、ソーシャルエンジニアリングで使われる、ほぼあらゆる種類のマルウェアおよび一般的なフィッシングの「餌」（フィッシングの手口）で発生する。標的型の不正アクセス活動は、対話が発生するソーシャルエンジニアリング（あるいは、偽のヘルプデスクからの電話やメッセージ内の不正なリンクに疎いといったセキュリティの教育および認知度における人の脆弱性）に依存する。不正アクセスのスコープにおいて最も注意する必要があるのは進化型の活動である。なぜなら、そのような活動は、サイバー犯罪者が目的を達成する際に、組織の特定の個人または部門を標的とするときに使った、選ばれたインテリジェンスに基づいているからである。標的となる人物の数は少なくなることが多いが、使用される手法は一段と難解（捜査官が気づきにくく）になり、サイバー犯罪者に対する利益の帰属が不明になる一方で標的の組織または個人に対する影響が明確に大きくなる。

152 http://www.computerweekly.com/news/4500253349/Most-DDoS-attacks-hiding-something-more-sinister-Neustar-warns

公的組織 vs 民間組織

ここまでの項で説明したリスクの多くは公的組織（例：政府）と民間組織（企業など）に共通するものである。とはいえ、両組織間には、リスク分類の考え方と重要性において根本的な違いが存在する。

相違点は、発生するサイバー犯罪について、両組織における優先順位と、それぞれの組織の対応（または予防）能力が異なることである。シェイン・シュック（本書の編集長）は、この違いについて、2014 年の記事で次のように述べている。[153]

「それが基本的に意味するのは、公的組織においては、予防できる活動と、捕捉・調査すべき活動とを分けるということである。民間機関においては、リスクのしきい値が異なる。すなわち、『サイバーセキュリティリスク管理』を、何がビジネス（健康と安全、金融、競合、ブランド、法務、業務といった諸問題）に影響するのかというビジネス判断と絡めることになる。官民両機関の組織はいずれもこれらの点に関係があるが、リソースや手段、法的管轄権の点で組織の調査能力に基本的な違いがある」

以下の図（同記事より引用）は、それぞれの組織におけるリスクの優先順位を示している。金融面および業務面のリスクは公的機関の優先順位に含まれていないが、それらは管理上の基礎的関心事であり、民間組織が絶えず管理している市場絡みの関心事とは異なっている。

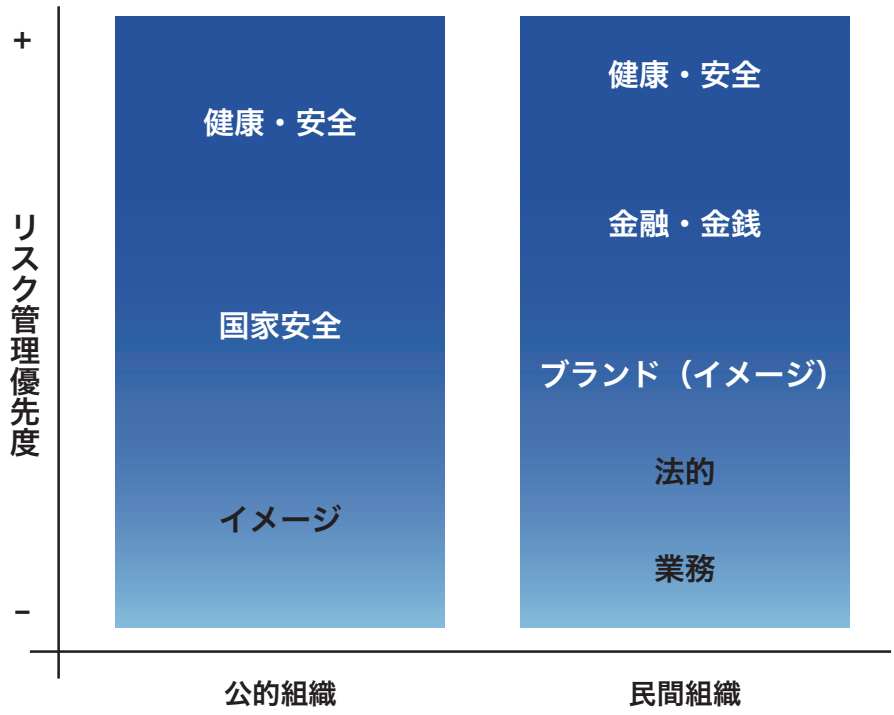


図 4-10. 公的組織と民間組織でのリスク優先順位に関する比較

153 https://info.cylance.com/incident-response-and-malware

第4章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

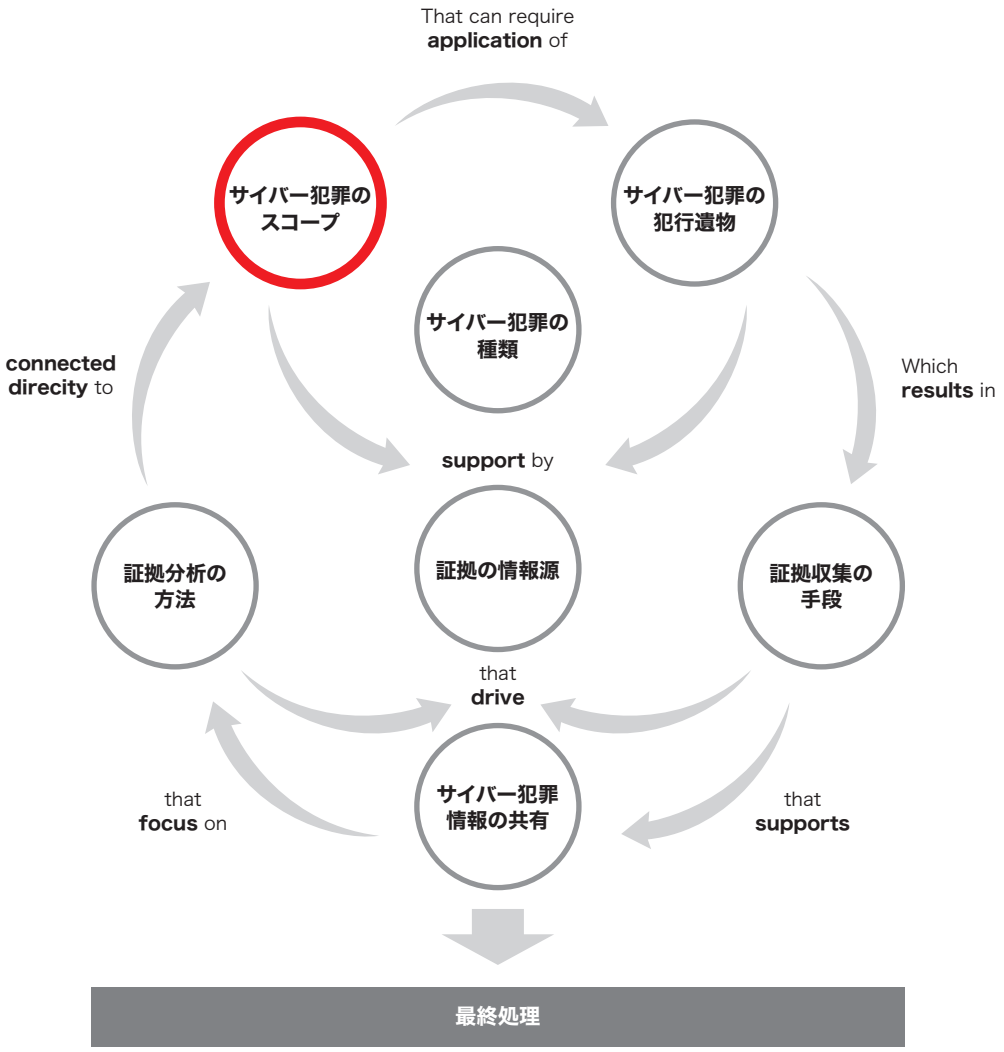


図 4-11. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 4-2）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 4-2. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 4-3. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。また、組織に対してサイバー犯罪の特性と種類を説明する。またサイバー犯罪者がどのように組織化されているかに応じて、彼らが狙った特性およびリスクと意図した目標を、戦略的に理解する必要がある。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査管理の各役割にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。利用可能な証拠の情報源を駆使して知見収集が集めた情報は、サイバー犯罪の特性とスコープ、目標を判断する上で不可欠な情報源となる。

調査 – 利用可能な情報源にあるアーティファクトや証拠を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。知見収集、説明責任、予防啓発、捜査管理の各機能にある者が、サイバー犯罪の影響を識別するのを支援する。識別にあたっては、その犯罪に関連する目的の特性（および達成の段階）に対する評価を用いる。サイバー犯罪の種類と影響を受けたシステム、組織機能、および従業員のスコープは、証拠によって決まる。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。知見の収集、捜査手続きに関する指導を行い、関連方針および法規制に基づいて分析結果を解釈して、捜査管理や予防啓発の各機能を支援する。法令に関する指導は捜査のアプローチだけでなく、実行されたサイバー犯罪の種類に応じた情報共有にも影響する。説明責任の活動においては、サイバー犯罪活動のスコープを判別して把握することが戦略的に必須である。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪のスコープに応じて、方針に基づきながら、また、どの組織・職務・人員が影響を受けるのかを考慮しながら、何を、だれに、いつ、伝えるのかを決定する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第4章:レビュー

1. **サイバー犯罪にはどのような「特性」があるか**
   答え：偶発的、標的型、進化型。
   例：ドライブバイフィッシング／水飲み場型攻撃、標的型ホエーリング、CaaS への登録。

2. **サイバー犯罪が標的とする組織機能にはどのようなものがあるか**
   答え：金融・金銭、ブランド、業務面、従業員。
   例：財務実績、競争力のあるマーケティング、物流とサプライチェーン、人事。

3. **インサイダーとサプライチェーンはサイバー犯罪の脅威と影響をどのように拡大してきたのか**
   答え：信頼されたリソースを通じた容易なアクセスにより、影響を制御することが困難になる。
   例：Tesla、SolarWinds、JPMC（JP Morgan Chase Bank）の市場操作。

4. **そのような機能に対するリスクは、官と民の組織でどのように異なるか**
   答え：財務リスクと業務リスクは公的機関では特に詳述されていない。
   例：公的機関は予算配分をコストセンターとして活用するのに対し、民間組織は予算を収益／費用関連として損益に配分する。

ケーススタディ4:インサイダーが市場をハッキングするとき

- **犯罪**：市場操作、偽情報
- **容疑者**：銀行取引担当幹部
- **手段**：許可されたアクセスの不正使用
- **動機**：個人的な利益
- **機会**：不適切な金融システム管理

8 年間に及ぶ数千件の違法取引が絡んだ画期的な事件で、JP モルガン・チェース & カンパニー（JP モルガン）の元貴金属トレーダーであるグレッグ・スミスとマイケル・ノワックの 2 人は、詐欺、価格操作未遂、スプーフィングの罪で最近有罪判決を受けた[154]。

実行前にキャンセルするつもりの注文を出すことで、彼らは市場の反対側で実行したい注文の価格を操作して、貴金属先物契約の実際の需要と供給に関する**誤解を招く偽情報**を市場に効果的に注入することができた。

3 週間の裁判の結果、両被告は、価格操作未遂、スプーフィング、商品詐欺、金融機関に影響を与えた電信詐欺など、複数の罪状で有罪判決を受けた。これらの有罪判決は、商品市場の健全性に対する国民の信頼を損なったウォール街の金融機関に責任を負わせようとする司法省のより広範な取り組みの一環である。

スミスとノワックは、JP モルガンの貴金属部門の他のトレーダーらとともに、2008 年 5 月から

154 https://www.justice.gov/opa/pr/former-jp-morgan-traders-convicted-fraud-attempted-price-manipulation-and-spoofing-multi-year

2016年8月にかけて詐欺的な計画を画策した。これは、実行前にキャンセルするつもりの注文を発注し、市場の反対側で実行する予定の注文の価格を操作するというものだった。一般に「スプーフィング」と呼ばれるこの行為は、貴金属契約の実際の需要と供給に関する虚偽の情報を市場に注入するために行われた。

影響を受けた契約は、ニューヨーク商品取引所（NYMEX）と米国商品取引所（COMEX）を通じて取引された。この操作の影響は市場に広範囲に及び、商品市場の健全性に対する投資家の信頼を損なった。

スミスとノワックの有罪判決に加え、ジョン・エドモンズとクリスチャン・トランツという他の二人の元トレーダーも関連事件で有罪判決を受け、組織内でのこの不正行為の規模が強調された。注目すべきは、2020年9月、JPモルガンが貴金属先物取引と米国債先物取引の市場での違法取引に関連して電信詐欺を犯したのを認めたことである。その結果、同社は3年間の起訴猶予契約を締結し、刑事罰金、刑事不当利得返還、被害者補償を含む9億2000万ドル以上の支払いに同意した。

この事件は市場健全性の重要性を強調し、このような巧妙な詐欺行為がもたらす深刻な結果を実証している。これは、非倫理的な市場操作行為に伴う法的リスクと風評リスクを金融機関に厳しく思い出させるものである。市場健全性を維持し、投資家の信頼を守る上での規制当局と法執行機関の重要な役割も、この事例から明らかである。

第5章

証拠の情報源

はじめに

第 3 章では、サイバー犯罪活動におけるステージおよび TTP（Tactics, Techniques and Procedures：戦術、技術および手順）に関係するインジケーターに基づき、サイバー犯罪のアーティファクトについて考察した。すでに述べたように、犯罪では必ず証拠が残る。証拠によっては、一般に公開されている情報源に残るものもある。なぜなら、サイバー犯罪はインターネット上の共有サービスを使って実行されることが多く、分散型の行動（他者に雇われて実行する行動や、組織的犯罪集団による行動）であったり、さまざまな形で繰り返されたりすることが理由で、TTP が、情報を共有する捜査官と分析員に見えてしまうからである。それ以外の証拠は、システムや従業員、関連の活動ログなど、内部（被害者）の情報源からしか得られないものである。

2013 年以降、（第三者のインフラとしての）クラウドサービスやサブスクリプションサービスが成長し、採用されるようになったことで、デジタル証拠の範囲にも変化が生じている。デスクトップ、ノートパソコン、タブレット、スマートフォンなどのサーバーやエンドユーザーコンピューティングデバイスに加えて、IaaS、PaaS、SaaS の構成と使用履歴のログも、現代のサイバー犯罪捜査における重要な証拠の情報源である。

消費者によるペイメントカードの盗難、銀行口座詐欺、ビジネス電子メールの漏洩、取引システムの操作や詐欺、ユーザーアカウントの乗っ取りやサービスソフトウェアの脆弱性の悪用に関連するその他の犯罪など、サイバー犯罪に関連する重大なデータやサービスの漏洩が露見している。

さらに、組織がサイバー犯罪を妨害、破壊、窃盗の脅威として認識するようになるにつれ、攻撃や侵害に対応し、侵害を調査するために、監視・検知の防御ツールを採用するようになった。その後、脅威の行為者は、認識可能なバックドア型トロイの木馬やその他のマルウェアをインストールする代わりに、**環境寄生型**アプローチを取り、ファイルレスツールやスクリプトを使用する方向にますます手法を変更している。オペレーティングシステムとアプリケーションサービスの観測可能性、ネットワーク監視、メモリフォレンジックの必要性は、サイバー犯罪インシデントを調査する際の証拠の情報源を拡大した。

すべてのサイバー犯罪がエンドユーザーコンピュータの操作に限定されるわけではない。「モノのインターネット」（IoT）には、産業用オートメーションシステムやビルオートメーションシステムのほか、コールセンター、フルフィルメントおよび出荷センター、交通管制、物流管理など、さまざまな産業機能をサポートするオペレーティングシステムが含まれる。2013 年以降、これらのシステムに対する攻撃が相関的に増加している。これらの機能とそれをサポートするシステムが関与するサイバー犯罪を捜査するためには、証拠の情報源についてさらに考慮する必要がある。

本章では、捜査官がサイバー犯罪のスコープ、影響、および行動を理解するために利用できる内外の証拠の情報源について考察する。この情報は、組織の意思決定者および管理職が防衛と予防に関する方針やシステム、手続きを決定するための監査と評価の基準を設ける際の助けとなる。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪を識別する証拠の情報源にはどのようなものがあるか
- 証拠は組織内外のどこで見つけることができるか
- 証拠の情報源別に、内容、信頼性、および構造はどのように異なるのか

サイバー犯罪のアーティファクトにおけるトピックス分類

「サイバー犯罪のアーティファクト」知識領域におけるトピックスの分類を図 5-1 に示す。

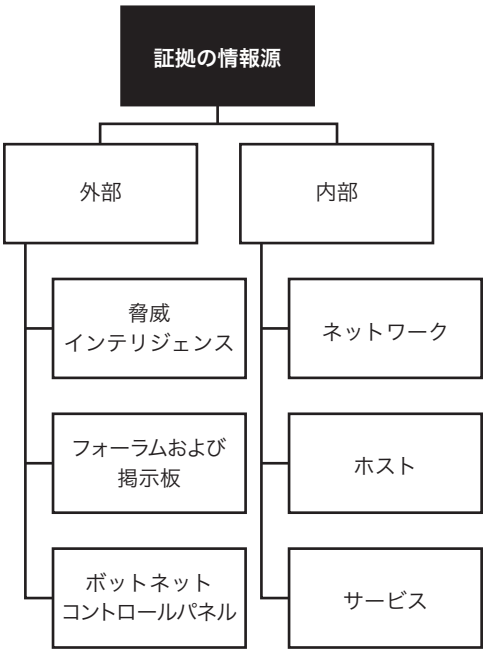


図 5-1.「証拠の情報源」知識領域におけるトピックスの分類

証拠の情報源とは

証拠の特定に役立つインジケーターとアーティファクトについては、サイバー犯罪の性質と種類に応じて、前の章で説明した。本章では、インジケーターやアーティファクトといった情報をどこで見つけ、捜査を助ける証拠としてどう使えるのかを解説する。

証拠の情報源には外部の情報と内部の情報があり、捜査とインテリジェンスの収集、関連する分析によって得られる。情報が完全かどうかは、データを収集し、相関させ、分析によって理解できるかどうかにかかっている。したがって、サイバー犯罪事件に関する有用な情報を得るには、完全で、時を得た証拠の情報源が必要である。次の図は、サイバー犯罪捜査（または検知と予防）に役立つ一般的な証拠の情報源で、組織が利用できるものの例を示している。

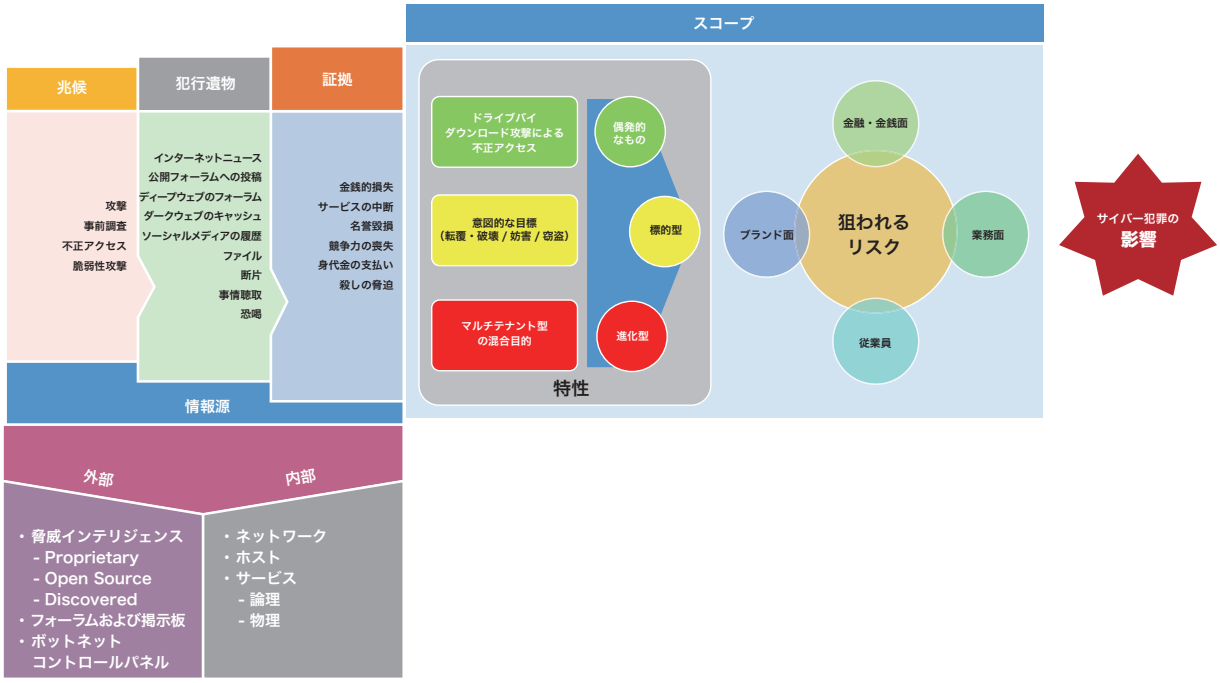


図 5-2. 証拠の情報源をとりまく関係

サイバー犯罪事件は毎回、内容が異なる。そのため、具体的な証拠の情報源も変わる。コンピュータとその通信ネットワークにはサイバー犯罪者が実行した活動のアーティファクトや兆候が残るため、いくつかの証拠の全般的分類を調べることが捜査・調査上役に立つ。捜査官・調査員は利用可能な証拠の情報源のすべてを検証し、実行された犯罪をスコープ（第 4 章を参照）に応じて適切に評価することが重要である。捜査官は、ログに残された情報をどのように入手し、利用可能な情報源を使ってインテリジェンスをどのように追跡して獲得するかを注意深く考えなければならない。

証拠の外部情報源

サイバー犯罪捜査およびインシデント調査において、証拠の外部情報源は特に重要である。入手可能な情報源を考慮する場合、外部の情報源とは、被害者の所属する組織外から発信された証拠と定義される。証拠の外部情報源は、サイバー犯罪活動の特定に役立つ幅広い関連データポイントを提供する。これらの情報源にアクセスするには、ほとんどの場合、オンラインで一般にアクセス可能な（場合によってはよりプライベートな）データソースを追跡し、監視する必要がある。これらの活動の大半はデジタル情報収集に限定されるが、ごく一部には HUMINT を必要とするものもある。

外部情報源には、捜査・調査をサポートする関連可能な多くの異種情報源が含まれる。例えば、日本サイバー犯罪対策センター（JC3）は、以下のように説明される産官学協力組織である。「産業界、学術界、公共部門の間で協力の枠組みを構築することにより、サイバー空間の脅威を軽減することを目指す非営利団体である。JC3 は、産業界、学術研究機関、法執行機関のそれぞれの強みを生かし、警察の捜査権を強化することで、サイバー脅威への先制的かつ包括的な対応を推進する。JC3 の最終的な目的は、世界中の関係機関の協力と情報共有を促進し、あらゆる脅威の発生源を突き止め、その被害を局限化または最小化できるようにすることである」。[155]

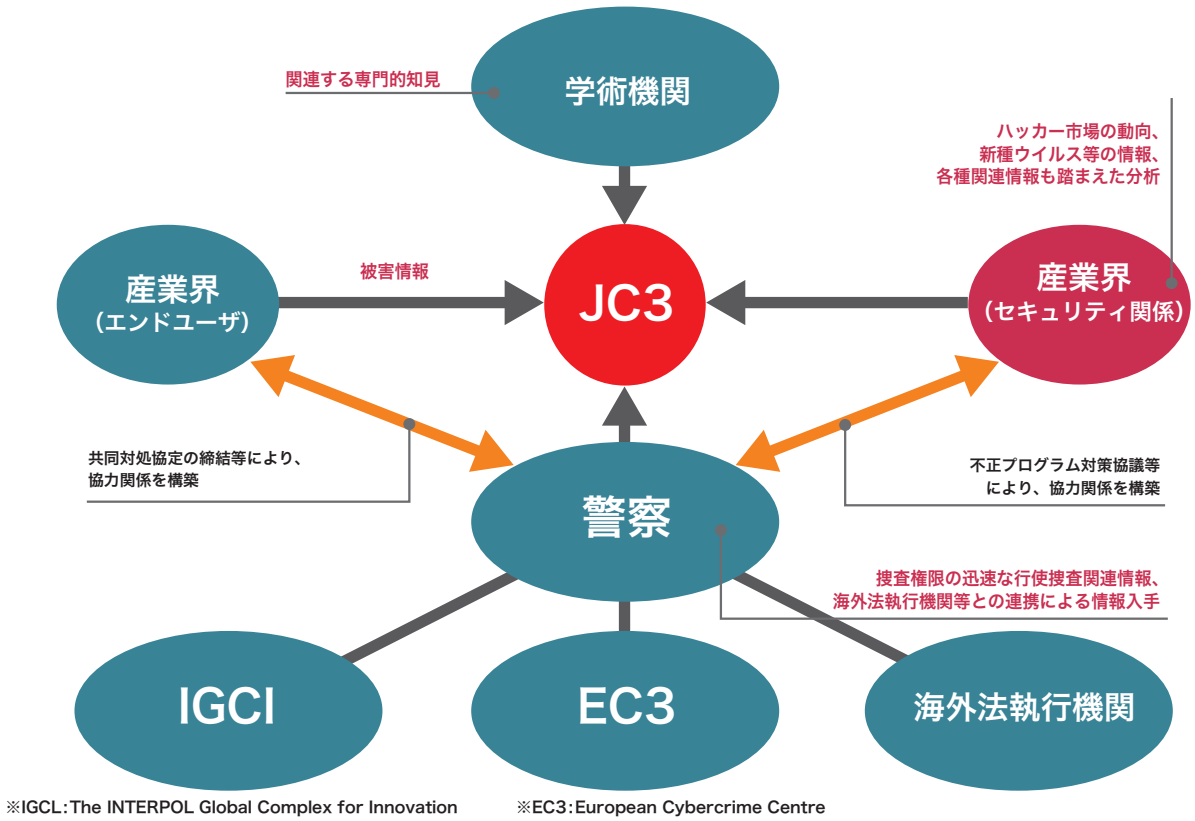


図 5-3. 日本サイバー犯罪対策センターの対応モデル

サイバー犯罪の捜査で一般的に使われる証拠の外部情報源には、主要なカテゴリが 3 つある。1 つめのカテゴリは、サードパーティベンダーによってパッケージ化された脅威インテリジェンス、または、オープンな情報源もしくは独自の情報源（組織独自の脅威インテリジェンス活動を含む）を通じて配布

155 http://www.nec.com/en/global/solutions/cybersecurity/efforts/index.html

される脅威インテリジェンスである。2つめはハッカーやCaaS（Crime as a Service）プロバイダが利用するフォーラムで、3つめは見落とされがちなカテゴリであるが、ボットマスターやサイバー犯罪者がC2通信とサブスクリプションサービスのために使用するボットネットコントロールパネルである。

脅威インテリジェンス

捜査官には使える外部の情報源が多数ある。とはいえ、情報をどのように入手し、処理すれば高品質なインテリジェンスになるかを習得するには時間と経験が必要である。情報を収集し、価値（信頼性および適合性）を評価してから、さらに意図または観察した犯罪目的のスコープに照らし合わせて解釈しなければ情報は「生」のインテリジェンスであり、よくてもリスクインテリジェンスにしかならない。生のインテリジェンスを解釈し、証拠となる情報源を発見するための捜査手続きに応用することだけが、脅威を明らかにするのである。

実際には、「脅威インテリジェンス」という包括的な用語は、悪意のあるソフトウェアのハッシュのコレクション、悪意のあるコードをホストしているURL、C&Cサーバーに関連するIPアドレス（上記を参照）などの単純なIoCから、あらゆるものを指す。他に脅威インテリジェンスが提供すべき情報としては、脅威コミュニティ／行為者特有のTTPや、組織のネットワーク監視およびホスト動作に適用可能な行動パターン（脆弱性攻撃、水平移動、C&Cサーバー、データ抜き取りに関するもの）、その他保護対象組織に狙いが定められた独特のアーティファクトなどがある。証拠収集で確実に犯罪証拠やIoCの検知および識別を体系的に扱うようにするのであれば、一般的な脅威インテリジェンスサービス／フィードのほとんどが利用できる。より高度なインテリジェンスサービスでは、保護対象の組織のプロファイルを作成するために、またさらに重要なことに、組織に関連する脅威コミュニティを特定して全般的にプロファイルするために、追加の微調整が必要になることがしばしばある。第4章ですでに述べたように、HUMINTやELINTからは、特殊なインテリジェンスの情報源を得られる。

●情報 vs インテリジェンス

脅威インテリジェンスは、捜査を助ける詳細を提供する証拠の情報源として重要な役割を果たすことがある。あふれんばかりの情報を抱えている分析員にとって、課題は情報とインテリジェンスをどうやって区別するかである。情報とは、いわばあらゆる情報源から集めたデータをまとめたものである。それは、関連性があるかどうかわからない、フィルタリングされていない生のデータを指す。情報は真偽が定かではないから、批判的な目で評価する必要がある。捜査官は、決して情報のみに基づいて行動してはならない。

他方、インテリジェンスとは、信頼できる情報源から提供された情報であり、その正確さと関連データが保証された評判の高い実績あるものである。通常、いかなる行動（中断、阻止、または改善）を計画するよりも先に、訓練された複数の分析員がインテリジェンスによって評価する。

あらゆる形のインテリジェンス収集技術がすでに数世紀前から存在しているが、サイバー脅威インテリジェンスに関しては、最近の技術革新によってさまざまな能力が登場し、入手可能となった。成長が進むサイバー脅威インテリジェンス分野からは、ますます大量のPROPINT（PROPrietary INTelligence、プロプライエタリインテリジェンス）および情報源が生み出されており、低料金で一般に提供されている。オープンソースインテリジェンス（OSINT）と呼ばれる他の情報源も、同様に信頼できる情報を無料で提供している。信頼性がそれほど高くないその他の情報源は、インテリジェンスの「ヒント」や検証されていない情報を提供しており、噂情報（RUMINT）として知られている。

●インテリジェンス共有グループ

法執行機関や政府機関の中には、情報共有サービスとして脅威インテリジェンスを公開提供している

機関が複数ある。前述の JC3 モデルと同様に、米国 FBI は InfraGard[156] という組織と提携しており、サイバー脅威から自身や組織を守ることに関心を持つ一般市民がインテリジェンスを共有できるようにしている。これらのグループには会員資格が必要だが、会費は伝統的に無料か、脅威インテリジェンス・ベンダーが提供するものよりもかなり低価格で提供されている。政府が支援するインテリジェンスに頼る場合に留意しなければならないことの一つは、有料のサービスよりも情報が古い場合が多いということだ。

●脅威インテリジェンスの種類

情報源から入手できる主要インテリジェンスにはいくつかの種類がある。インテリジェンスの質と信頼性は情報源に応じて異なるが、インテリジェンスは大まかに 4 つの分野に分類できる：

- **戦術的インテリジェンス** - 戦術的インテリジェンスは、攻撃者のツール、戦術、および手順（TTP）に関係する。これらのインジケーターは、特定のツールや方法がどの種類の脅威に帰するかを判断するのに役立つ。

- **技術的インテリジェンス** - 技術的インテリジェンスは、通常、マルウェアや通信プロトコルに関連する侵害のインジケーターを含む。例えば、悪意のあるファイルや通信は、ユニークな特徴を持っていたり、サイバー犯罪組織に帰することができる監視活動に関連していたりする場合がある。

- **運用上のインテリジェンス** - 運用上のインテリジェンスは、直近の活動環境と脅威の行為者の能力および意図に焦点を当てる。近く計画されている攻撃または進行中の不正アクセスに関する具体的な詳細は運用上のインテリジェンスにあたる。

- **戦略的インテリジェンス** – 戦略的インテリジェンスに含まれるのは、上層部がリスクを評価し、組織の脅威対応体制および予算を計画するときに有用な大局的詳細である。

●PROPINT（Proprietary Intelligence、プロプライエタリインテリジェンス）

PROPINT は上述のインテリジェンス共有グループやその他のベンダーのサービスから有益な情報を提供する。商品としてのサイバー犯罪脅威インテリジェンスは成長中の分野であるが、その品質はさまざまである。

- **ベンダー** - FS-ISAC（金融）、H-ISAC（医療）、RH-ISAC（小売）など、いくつかの民間企業や関連グループが、独自のインテリジェンスへの管理されたアクセスを顧客に提供している。これらのインテリジェンス情報源は、完全性や比較可能性に大きなばらつきがあり、無料で入手できるオープンソースインテリジェンスが含まれている場合もあれば、含まれていない場合もある。

- **セキュリティ関連団体／法執行機関** - 非営利団体（政府系または民間）のセキュリティおよび法執行機関等は、加入条件に合致する登録利用者に対して PROPINT を提供し、利用を認めている。これらの情報源から得られるインテリジェンスには、生のインテリジェンスから古いインテリジェンスが入り交じっている（機密性や取り扱いの制限などが原因である）。

156 https://www.infragard.org/

●OSINT（Open Source Intelligence、オープンソースインテリジェンス）

オープンソースインテリジェンスは、一般に入手可能な情報源から収集される。必ずしも信頼性が確認されたインテリジェンスではないものの、「クラウドソーシング」によって構築された、無償のデータ情報源である。OSINT は利用可能な外部ソースからいくらでも収集できるが、多くの場合、以下の分野から得られる。

- **検索エンジン** - 最もよく使われ、広く利用されている情報源の一つが検索エンジンである。情報は検索エンジンによってインデックス登録され、アクセス可能なインターネット ページを継続的にスキャンしてインデックス登録するため、サイト所有者がデータを削除しても情報は保持される。検索エンジンを利用するだけで、膨大な量のデータを解析し、非常に具体的なインテリジェンスを何点も集められる。捜査官の多くは、検索結果を絞り込める高度な機能を検索エンジンで駆使している。検索にカスタム構文を使うこの手法は「**ドーキング（Dorking）**[157]」（または、Google ハッキング）と呼ばれることが多い。

  - **人物検索** – 人物検索サービスは個人の識別に特化したサービスで、できるだけ多くの公開情報源をまとめる。人物検索サービスでは、資産所有者や法的記録に関するものを含む公的記録をかき集めるといったことがしばしば行われる。これらの検索サービスは、被疑者グループまたは個人に関する追加の詳細を見つけるのに驚くほど効果的である。

  - **画像検索** – 画像検索（および画像逆引き検索）サービスは多くの検索エンジンで提供されている機能である。これらの機能により、捜査官は、共有されたソーシャルメディアのプロフィールやウェブページ内で、（信頼度に基づいて）同時に出現する画像を発見することができる。多くの場合、サイバー犯罪の証拠には、ビデオチャットの断片や写真の背景など、テクノロジーの使用による「結果として生じるアーティファクト」が含まれることがある。画像検索サービスは、そのような重要な詳細を発見するために活用することができる。

- **ソーシャルメディア** - 2013 年以降、ソーシャルメディアは劇的に普及した。ソーシャルメディアを使えば、個人や組織に関する情報を集めて、捜査用のプロファイルを構築できる。加えて、ソーシャルメディアサービスの利用者は、自身の情報へのアクセスを制限する法を十分に理解していないため、その情報が検索エンジンの結果に表示されることがある。これらの詳細は、捜査官が容疑者を識別して彼らの狙いを明らかにする他、容疑者が連絡を取り合っている可能性のある人物を見つけるのにも役立つことがある。ときには、サイバー犯罪者がソーシャルメディアサービスを使って、自身の高度なハッカー技術（1337 h4x0r skillz、エリートハッカースキル）を売り込んだり、標的や法執行機関を挑発したりする（ソーシャルネットワークにおける匿名性をよく知らずに、あるいは誤解してそのような行動をとることがある）。

●発見／噂情報（RUMINT）

RUMINT は、観察、秘密情報提供者、インタビュー、マルウェアや通信のリバースエンジニアリング分析、フォーラムや同様の情報源の偵察や監視など、多くの情報源からもたらされる。情報源が信頼できるものであって、体系的かつ有用なインテリジェンスを繰り返し得られると判断できるまでは、それは「RUMINT」である。その後は、信頼性等が確認できなければ RUMINT のままであり、確認できた

157 https://www.exploit-db.com/google-hacking-database/

場合にはPROPINTまたはOSINTの情報源集に組み込めるときもある。

フォーラムおよび掲示板

ハッカーや犯罪者はインターネット上で交流し、情報交換を行う。このようなコミュニケーションを促進するために使用される手段は、多くの場合、さまざまなレベルのアクセス制御を備えたオンラインフォーラムである。これには、関連部分にアクセスするためにログイン情報を作成するだけでよい「オープン」フォーラムという簡単なものから、参加するためには既存のフォーラムメンバーで評判の良い人が新しいフォーラムメンバーの保証人になる必要があり、多くの場合、新しいメンバーはハッキング（またはその他の犯罪）能力と犯罪行為の証拠を提示しなければならない、厳しく制限され審査されたフォーラムまでが含まれる。

フォーラムや掲示板はサイバー犯罪者が好んで使う通信手段である。これらのフォーラムは、多くの違法または非合法なサービスや商品を提供していることがある。攻撃者たちが協力し、有用な詳細を列挙するために、フォーラムで今後の標的について話し合うことは珍しくない。これらのフォーラムを監視すれば、捜査に役立つインテリジェンスを収集でき、準備中の攻撃または不正アクセスの実行を未然に防げる。フォーラムは重要なインテリジェンスを得られる極めて有効な情報源であるが、フォーラムのメンバーは、法執行機関やセキュリティ調査員が内部に潜入していないかを警戒している。その結果、秘密情報提供者またはフォーラムのメンバーから得られるHUMINTの方が頼りになる場合もある。

ボットネットコントロールパネル

ほとんどのサイバー犯罪活動は、乗っ取られたりあるいは不正アクセスされた資産（コンピュータやモバイルデバイス）を制御するために、何らかの集中管理機能を備えたツールを利用している。サイバー犯罪者がインターネットやネットワーク接続を介して資産に直接（仮想的に）アクセスできたとしても、その活動の規模は、隠蔽目的か必要性かにかかわらず、通常、多数の分散コンピュータやデバイスへのアクセスに依存する。

アクセス制御と「ボットネット」のメンテナンスは、特定のタスクを自動化するコントロールパネルを備えたC&Cサーバーによってサポートされる。これらのタスクは、サイバー犯罪活動のリモート制御と運用サポートのためにカスタム構成でボットネット内のコンピュータを関与させるためのマルウェアツールをオンデマンドで配信することを含む。コントロールパネルには、ボット「ドローン」（ボットネットの制御下にあるコンピュータ）に対する構成変更を実行するためのスクリプトリポジトリもある。さらに、コントロールパネルはドローンから盗まれた構成（および標的）の詳細やデータ、音声／ビデオ録画などの情報も保存する。一部のコントロールパネルは、盗んだ情報を他のストレージホストにルーティングするだけで、コントロールパネルのホストサーバーの場所を難読化するためにさまざまな中間プロキシとルートを組み込む場合がある。

ボットネットコントロールパネルは、マルウェアの使用に関する具体的な詳細（タスク実行用のスクリプトとリモートアクセスおよび制御用のコンパイル済みツールの両方）、被害者の識別情報（IPアドレス、システム構成／ビルド、コンピュータ名など）、被害者のデータ（スクリーンショット、ビデオ／オーディオ録音、ファイルなど）、ボットネットの動作（および期間）に関連するメタデータが含まれるアーティファクトを含むため、重要な証拠の情報源となる可能性がある。また、コントロールパネルには通信の構成詳細が含まれている場合もある。これがあれば、捜査官は犯罪者の組織全体を見渡しながら、各地にまたがるサイバー犯罪活動（および目標）のスコープを明らかにできるかもしれない。これまで法執行機関は、C&Cサーバーを捕捉することでボットネットを単に中断または「テイクダウン」しようとするだけであった。しかし、コントロールパネルは、実行可能な（または許可されている）場合に捜査官が活用すべき、重要な詳細な証拠および情報源であることが明らかになっている。

証拠の内部情報源

潜在的な証拠の情報源を調査するときは、捜査中に組織のネットワークシステムに存在する利用可能なすべての情報源とデータを考慮することが重要である。従来の犯罪現場と同様に、内部の証拠は、捜査官が犯罪現場を離れることなく証拠として使用できるものとして定義される。デジタルフォレンジックでは、犯罪現場は疑わしいシステムと通信するシステムやネットワーク機器とみなされる。ただし、デジタルフォレンジックはサイバー犯罪捜査における活動のひとつにすぎない。捜査官は、組織内の物理的な証拠（施設や設備）および人的な証拠の情報源を考慮しなければならない。

情報セキュリティに関するコミュニティの発展に伴い、レイヤごとのセキュリティアプローチをとる「多層防御」モデルを採用する企業が増えている。これは、組織内のリスクの高い領域を特定し、インシデントを防止または検出するための適切なセキュリティ管理とメカニズムを導入することを含むが、それをもってサイバー犯罪から完全に逃れられるものではない。組織の IT ネットワーク内で重要な場所の数か所に防御を構築すれば、単独の攻撃媒介またはセキュリティメカニズムの機能不全が全体的な影響を引き起こしたとしても、それを軽減できる。

組織は情報技術（IT：Information Technology）に加えて、施設や生産活動を支える制御技術（OT：Operations Technology）を導入している。OT は、電力、水、環境制御、セキュリティ／安全システムなどの単純な制御システムである場合もあれば、関連機器の操作と保守を行うためにプログラマブルロジックコントローラー（PLC）やリモートターミナルユニット（RTU）を使用する複雑な生産管理機器を含むこともある。情報セキュリティとそれに対応するサイバー調査のポリシーと手順では、IT と OT の両方を認識して組み込む必要がある。

次の図は、捜査官が評価すべき証拠の内部情報源の概略を示している。

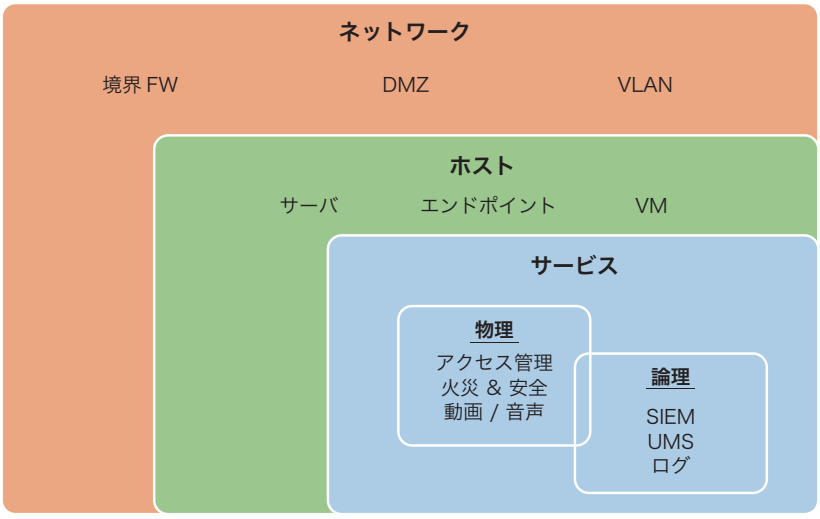


図 5-4. 証拠の内部情報源

ネットワーク

組織のネットワークはいくつかの要素によって構成されている。これらは、境界、サービス、ネットワークゾーン、仮想および物理的な「ローカルエリアネットワーク」（LAN/VLAN）、および組織の通信を容易にするために必要に応じてファイアウォール、ルータ、ブリッジを使用して物理的または論理的な分離によって各ゾーンを互いに分離する「非武装地帯」（DMZ）を含む。ネットワークはデータだけ

でなく、電話や動画、音声の通信も担う（つまり、PBX／電話システムネットワークは、LANまたは境界ネットワークサービスに統合される場合もあれば、完全に別個の場合もある）。これらの通信を担当するアーキテクチャは共存している場合もあれば、別個の場合もある（すなわち、PBX／電話システムのネットワークがLANまたは境界ネットワークサービスに統合されている場合や、まったく別個の場合がある）。ネットワーク設備は本質的にコンピュータであり、オペレーティングシステムとサービス構成、保守用のツールもしくは機能を有している。ルータ、ファイアウォール、PBX、監視カメラシステムなど、ネットワーク機器のそれぞれは、捜査官・調査員が分析に組み込むべき潜在的な証拠の情報源である。少なくとも、いずれのネットワークシステムも活動履歴ログを有している。これらのシステムでネットワーク記録（またはパケットキャプチャ）ツールを使える場合には、サイバー犯罪活動に使われたC&Cサーバーの通信プロトコルや通信方式、通信時刻、アドレスといった通信関連のアーティファクトを捜査官が把握するのを助ける。

どのログが捜査・調査で役に立つかを評価するときは、ネットワークベースのツールやアプリケーション、セキュリティアプライアンスなどをどのように駆使すれば調査官が証拠を見つけられるかを考えることが大切である。これらのデバイスのほとんどは、毎日発生するイベントやアクションを記録するように構成できる。このようなログを正しく保存すれば、ネットワークからキャプチャしたアーティファクトに基づいて、ネットワーク内の水平移動や不正アクセスされたシステム（およびアプリケーション／認証情報）のスコープ、サイバー犯罪の特性を識別する上で極めて重大な情報となる。捜査の助けとなる有用な証拠またはアーティファクトは以下のネットワーク設備から得られる可能性がある。

- **境界ファイアウォール** – 境界ファイアウォールは組織とリモート（外部）サービスとの間で交わされる通信について、外部からの受信と内部からの送信の証拠を提供する。使用された通信プロトコルの種類、ポリシーで許可されている（または方針に違反する）サービスの構成、通信の頻度／タイミングは役立つ詳細であり、不正アクセスのインジケーターを明確にして活動のヒントとなるインテリジェンスを提供する。また、これらの情報は関連コミュニティまたは公共機関（各種ISACや法執行機関）との共有においても役に立つインテリジェンスである。

- **ネットワークプロキシ** – ネットワークプロキシはユーザーとサービス間の行動履歴を提供する。通常、ウェブプロキシは悪意のあるウェブサイトやビジネスに必要ないと思われるコンテンツから組織の利用者を守るために導入されている。また、普通は、発信元コンピュータのアドレス、接続時刻、コンテンツの種類、リモートサービスとそのアドレス、通信方向など、通信に関するアーティファクトで鍵となる詳細をログに記録している。記録された詳細は、特定のウェブサイトにアクセスした人物を捜査官が識別したり、容疑者の活動を評価したりするのに利用できる。

- **DMZ** – ネットワーク非武装地帯（DMZ：DeMilitaraized Zone）とは、ローカルエリアネットワーク（LAN）を他のネットワーク／リモートネットワークから隔離するための物理的もしくは論理的ネットワークである。通常、DMZに置かれたシステムはインターネットに接続されており、ウェブサーバやアプリケーションの不正アクセスが絡むインシデントにおいては、常に捜査の対象となる。DMZのログで一般的に確認できる活動には、脆弱性のスキャンや脆弱性攻撃の試行、DMZから内部ネットワークのホストへの侵入がある。DMZログは侵入のみを検知するように構成されていることが多い。ところが、サイバー犯罪の証拠を収集する際は、アウトバウンド（内部から外部方向への）検知を行う方が、実際にはインテリジェンスの詳細として価値が高い。なぜなら、それによって捜査官はサイバー犯罪に関連するシステムへとたどり着くことができ、意図または目標の評価を行えるからである。

- **ゾーン／VLAN スイッチ／ルータ／ブリッジ** – 組織で異なる機能を分担するネットワークは、セキュリティ上の理由から「ゾーン」または仮想 LAN（VLAN）にセグメント化（分割）されることが多い。ネットワークセグメント間で通信を行うには、異なるセグメントの橋渡し（ブリッジ）を担当する設備が必要となる。これらのネットワーク機器には構成（および変更）履歴があり、セグメント間の転送接続を、日時や転送元／転送先アドレスといった情報を伴うログに記録する場合もある。これらはサイバー犯罪に関係する証拠を特定できる有用なアーティファクトを提供することがある。

- **VPN** – 仮想プライベートネットワーク（VPN）のルータはリモートで仕事をする人が内部ネットワークのホストに接続するのを可能とする。接続履歴の詳細はルータとホストの両方でログに記録される。

- **PBX/VM/IVR** – 構内交換機（PBX）は音声メール（VM）や音声自動応答（IVR）サービスを備えていることが多く、電話システムを介して交わされた通信のログや、記録された／利用可能な情報へのリモートアクセスに関する役立つログを保存している場合がある。これらのシステムは、「サポート詐欺」や恐喝が絡むサイバー犯罪において、重要な証拠の情報源となり得る。

- **安全／セキュリティシステム** – 火災や落雷、物理的な入退室の管理、緊急通知サービスをつかさどるのが安全システムやセキュリティシステムである。通常、これらのシステムは、イベントの発生時間に基づいて制御コードやバッジ／入退室者のアクセス ID を伴う詳細をログに記録する。このログは、捜査官がサイバー犯罪に関連する物理的なイベント活動を把握するのに役立つ。

- **DCS（RTU/DCU）** – 分散制御システム（DCS）には、産業制御システム（ICS）の運用を制御するリモートターミナルユニット（RTU）およびデータコンセントレータユニット（DCU）が含まれている。また、生産およびロジスティックスを制御するプログラマブルロジックコントローラ（PLC）の他、電力、水道、空調、エレベータ、および自動ドアを管理するビル管理システム（BMS）も DCS に含まれる。捜査で見落とされることが少なくないが、通常、これらのシステムはアクセスしたアカウントの履歴（日時、資格別など）の他、接続元のホストアドレスや、場合によっては関連プロトコルの詳細もログに保持している。これらのログから見つかるアーティファクトは、「インサイダーの脅威」活動が捜査で問題視されている場合に、他のサイバー犯罪のアーティファクトとの関連性を見ることで役に立つ。

ネットワークパケットをキャプチャ（PCAP）してファイルに記録できる機器も検査の必要がある。これらの機器はネットワーク活動のデジタルレコーダーの役割を果たし、捜査官がネットワーク活動を再現するのに役立つ。PCAP ファイルのフォレンジック分析は、年月の経過とともに大きく進歩している。現在では、パケットキャプチャから VVoIP（Voice and Video over IP）やその他の通信のデータストリームを復元できるようになっている。時には通信が暗号化されていたとしても、PCA ではユーザー名やパスワードといった重要情報も得られることがある。

コンピュータ端末

エンドポイントシステムには、あらゆるサイバー犯罪捜査に関わる情報が多数含まれている。通常、エンドポイントは露出度が高いため、組織にとってのリスクも高い。エンドポイントのほとんどは、電子メールやウェブブラウジングといった脆弱性攻撃を受けがちなサービスをどこからでも利用できる。

証拠という意味で注目すべき重要な領域が何かを明らかにすることで、捜査に関連する情報領域の体系的な分析の手順を捜査官は構築できる。

企業環境においては、システムの健全性を管理および保守するさまざまなツールが全エンドポイントシステムにあらかじめインストールされている。アンチウイルスなどのソフトウェアは、マルウェア活動や、システムで検知された疑わしい活動に関するログファイルを保存していることが多い。不正アクセスされたホストにマルウェアの履歴がある場合、捜査官はインシデントの時間軸を再評価しなければならない場合がある。ホストベースのファイアウォールなどのファイルは、疑わしいネットワークアクティビティ、ブルートフォース攻撃、悪意のあるバックドアの存在などに関する詳細な情報も提供することができる。ソフトウェアの導入記録にも、その他の有用な証拠の情報源が含まれている場合があり、これらの記録には、システムパッチや構成履歴が保存されていることがある。

●ウェブ履歴

一般的に、ウェブの閲覧活動は貴重な証拠の情報源である。これにより、捜査官はユーザーの活動を特定し、マルウェア感染、違法コンテンツ、その他の情報などの疑わしい活動がインシデントの背景となる可能性があるかどうかを判断することができる。ブラウザのキャッシュに保存されている追加のアーティファクトで、ウェブメールを含むウェブサイトの再構築も可能となる場合がある。ブックマークやお気に入りといった項目によって、ユーザーがウェブで普段どのような活動を行っているかを捜査官が把握できる。場合によっては、保存されたパスワードをウェブ履歴またはブラウザ設定から復元できることもある。これらのパスワードを発見できれば、それまで見つからなかった追加の証拠をつかめる場合もある。

●チャットおよびメッセージングの履歴

チャットとメッセージングは幅広く利用されているプログラムであり、人気アプリケーションがどのように、また、どこに履歴を保存しているかを理解しておくと、捜査で非常に役立つ。チャット履歴、添付ファイル、および関連するアーティファクトの再構築を試みるフォレンジック分析ツールがいくつかある。

●電子メールおよびカレンダーのアーティファクト

電子メールやカレンダーのアーティファクトを検証すれば、人物やグループの間の関係を明らかにするのに非常に役立つ。電子メールの記録はローカルシステムに保存されているオフラインメールボックスの中から取り出せることが多い。また、対象人物のメールボックスをホストしているサーバーからも取得できる。悪意のある電子メールの配信は、エンドポイントシステムを感染させるのによく使われる手法である。電子メールのメタデータおよびリンクや添付ファイルを含むコンテンツを分析すれば、種類によっては攻撃や侵入の発見につながる場合がある。

●アドレス帳および連絡先の内容

容疑者がだれと接触したか、あるいは普段からどういった人物と連絡を取り合っているかが分かれば、非常に参考になる。状況によっては、この情報をもとに、ある利用者の別名が判明したり、電子メールやソーシャルメディア、電話、フォーラムその他の連絡手段が分かったりする場合もある。

●隠しファイルおよびシステムファイル

Windows システムには「隠しファイル」や「システムファイル」の属性を持つファイルが多数ある。しかし、これらのファイルが例外的な場所にあるのであれば、容疑者が残したアーティファクトの可能性

があるため、捜査で調べる必要がある。ファイルに隠し属性を与える作業は簡単なものの、容疑者がなぜ、システムの他のユーザーからファイルを隠したいのかを捜査官は考慮する必要がある。これらのファイルは意識的に表示するようにしないと、ディレクトリの一覧やファイルシステムビューアーには表れないため、普通のユーザーには見落とされがちである。

●圧縮アーカイブ

圧縮アーカイブ（.zip、.rar、.7z、その他）ファイルと、それらに関連する履歴は、潜在的なデータの抜き取りや、サイバー犯罪者が残したツールの識別に役立つ。ハッカーは、検知を回避するために、使用するツールを圧縮ファイルに保存することが多い。さらに、データの抜き取りには分割圧縮ファイルがよく使われる。これは、大きなデータセットを小さな圧縮ファイルに分割することで、ネットワークセキュリティツールによる検知を回避するためである。

●暗号化ファイル

暗号化ファイルは、捜査との関連性がないかを調べて判断する必要がある。サイバー犯罪者は、検知を回避する目的で暗号化ツールを使うことがよくある。暗号化ファイルは復号できるとは限らないが、何か有益な情報がないかを見つけるために調べる価値はある。圧縮アーカイブはしばしば暗号化されている。

●削除されたファイルとごみ箱

「ごみ箱」や「ゴミ箱」（オペレーティングシステムによって名前が異なる可能性がある）に削除済みファイルがある場合は、これらを調べなければならない。削除されたファイルにアクセスできなくなった場合は、フォレンジックツールを使用してそれらのファイルを復元できることがある。場合によっては、他のファイルやアーティファクトからファイルの削除履歴を復元できることもあるので、調べる必要がある。ファイルが削除された場合は特に、だれが削除したのか、ファイルのコンテンツは何だったのかといった情報は有益で、サイバー犯罪の証拠特定を助ける。

●テンポラリファイルおよびテンポラリディレクトリ

アプリケーションの多くは、プログラムに使われているデータを書き込む場所として、テンポラリディレクトリを使用する。そういったデータのファイルと関連情報の断片は、テンポラリディレクトリ内にあるデータを調べると見つかることがある。たとえば、ワープロソフトは、アプリケーションでハングした場合にテンポラリファイルを作成する。テンポラリファイルには、サイバー犯罪のアーティファクトまたは目標が記述された有益なコンテンツが含まれている場合がある。

●仮想マシン

被疑ホストに仮想マシンが見つかった場合には、フォレンジック分析を行うべきシステムが新たに1台見つかったのと同じように扱う必要がある。仮想技術が普及したため、エンドポイントシステムとサーバーのどちらにも、仮想マシンが置かれるようになっている。仮想システムは物理マシンと同様のフォレンジックアーティファクトを有し、ディスク構造全体が分析対象となる。仮想マシンがサスペンド状態で見つかったときは、ローカルディスク上のファイル内に仮想マシンのメモリが保存されていることもある。仮想マシンからは、サイバー犯罪に関する有益な詳細とアーティファクトが見つかる可能性がある。

●アプリケーションおよびシステムのバックアップファイル

アプリケーションおよびシステムのバックアップがしっかりしていると捜査官の信頼は高い。適切なシステムバックアップがあれば、捜査官は被疑システムの「過去のスナップショット」を追加で検証できる。バックアップによって、以前に削除された情報を見つけられる可能性がある。たとえば、携帯電話のバックアップがコンピュータに作成されている場合、そのバックアップがなければ見つからないような証拠につながるアーティファクトが得られるかもしれない。テキストメッセージや通話記録など、バックアップファイルに保存されている活動が例として挙げられる。

●画像およびデジタルメディア

捜査の種類によっては、システム内に存在する画像およびデジタルメディアコンテンツを調べる必要がある。システムの不正利用があったような場合には、ビジネスに不要な違法コンテンツなどの媒体がないかを調べると役立つことがある。ピアツーピア（P2P）ネットワークから取得されたファイルや、P2P ネットワークとの通信に使われるアプリケーションは、マルウェアが仕込まれていないかや、著作権上の問題がないかを分析しなければならない。

●完全削除ツール

完全削除ツールは、フォレンジック捜査官によってファイルが復元されないようにするためのツールである。これらのツールは、最初に対象ファイルを削除し、次にディスク上のデータを数回にわたって上書きし、復元を不可能にする。完全削除ツールの中には、合法的な利用目的として、特に共有したくない秘密データを削除するものもある。ただし、こういったツールが見つかった場合には、組織の方針に照らし合わせて正当な理由があるのかどうかを確認しなければならない。

●リモートアクセスファイル

「Microsoft ターミナルサービスクライアント」（MSTSC）、「仮想ネットワーククライアント」（VNC）、Secure Shell（SSH）、Public TTY（PuTTY）、Citrix、「LogMeIn」、「WebEx」、および「GoToMyComputer」などのシステムツールまたはアプリケーションのリモートアクセス構成および履歴キャッシュファイルは、有用な履歴を提供し、場合によっては、それらの使用に関連する画像や成果物も提供する。こういったアーティファクトは、サイバー犯罪の証拠を見つけて評価するにあたって、貴重な証明となる詳細をもたらすことがある。

●システム構成設定

不正アクセスされたホスト内の証拠の情報源として、オペレーティングシステムの構成やユーザサービスの構成からはフォレンジックに使える詳細が豊富に得られる。ほとんどのフォレンジック分析および調査の情報は Microsoft の Windows に関するものである。理由は単純で、サイバー犯罪（DDoS 攻撃またはマルウェア等の配布を除く）に関係する不正アクセスのほとんどは、Windows オペレーティングシステムまたは関連のアプリケーションの脆弱性に対するものか、ソーシャルエンジニアリングを通じてユーザーの行動にうまく付け込んだものだからである。

Windows 系オペレーティングシステム用のレジストリハイブはいずれもシステム活動に関する情報の主要情報源であり、サイバー犯罪の証拠を特定するための分析で着目すべきである。Windows オペレーティングシステムがインストールされているコンピュータのレジストリは本質的に、オペレーティングシステムやアプリケーション、ユーザー、ハードウェア機器の構成情報を保存している階層型データベースである。

設定または使用履歴に関する情報を含むレジストリキーには、「最終書き込み時刻」を表す有益なアー

ティファクトが含まれている。この情報は従来の表示技法では確認できないが、フォレンジック手順の助けを借りれば、捜査を支援する有益な情報を得られる。

以下の Microsoft の Windows オペレーティングシステムのレジストリキーには、有用な証拠の情報源が含まれている。

- **HKEY_CURRENT_USER（HKCU）** – ログオンユーザの構成情報が含まれている。このレジストリハイブに存在する可能性のあるアーティファクトの例としては、フォルダおよび表示のオプション、コントロールパネルの設定、その他ユーザーごとの活動履歴がある。

- **HKEY_LOCAL_MACHINE（HKLM）** - オペレーティングシステムで必要となるハードウェアごとの情報が含まれる。このレジストリハイブから得られる主要アーティファクトの例としては、マウントされているドライブの情報や、システムおよびアプリケーションの構成キーがある。HKLM のサブツリーには、持続型サービス（トロイの木馬など不正なサービスを含む）をサポートするリソースの構成に不可欠な情報が含まれている。

- **SYSTEM** - 主として Windows オペレーティングシステムの設定や、DHCP リースの詳細などを含むネットワーク情報、マウントされているファイルシステムに関する情報などを保存するのに使われる。SYSTEM キーにはオペレーティングシステムに読み込まれているハードウェアドライバに加え、プラグアンドプレイデバイスの列挙（履歴）に関する情報も保存されている。インシデントごとの Run キーも、SYSTEM レジストリハイブ内に固定で構成されている。

- **SOFTWARE** - すべてのユーザーが使えるようにインストールされている個別アプリケーションの詳細に関する変数型構成が保存されている。

- **SAM** - ユーザーアカウント管理およびローカルシステムのセキュリティ設定に関する詳細情報が保存されている。暗号化（ハッシュ化）されたユーザーパスワードも SAM キー内に保存されている。

- **SECURITY** - 現在のユーザーが所属しているドメインのセキュリティデータベースに関する情報が保存されている。

- **NTUSER.DAT** - ユーザーのアプリケーションおよびプロファイルに関する構成設定と使用履歴が保存されている。使用履歴には、マウントされているネットワーク共有や取り外し可能なストレージメディアおよびデバイス、アプリケーションおよびファイルのアクセス履歴、固定サービスまたはスケジュールされたサービスの詳細が含まれている。

- **Most Recently Used Lists（MRU：最近使用したリスト）** - レジストリのあちこちに存在しており、ユーザーがとった活動に関する追加の情報を得られる。捜査官がコンピュータの利用状況を評価するのに使える MRU キーにはいくつか異なる種類のキーがある。MRU キーには、使用された文書またはその他のファイルに関する情報や、使用活動に関係するタイムスタンプなどの情報が保存されている。

●メタデータ

メタデータとは「データに関する属性情報」である。メタデータには、ファイルの属性や、ファイルと

ユーザまたはオペレーティングシステムとの関係、ストレージ／デバイスの構成に関係する情報などがある。たとえば、文書には作成日、所有者、および編集者などのプロパティを説明するメタデータが含まれている。マスターファイルテーブル（MFT：Master File Table）またはオペレーティングシステムのジャーナルファイルには「インデックス」メタデータが含まれており、ユーザとのやりとりを行うファイルシステムをオペレーティングシステムが参照するのを助ける。これは、非常に重要な証拠の情報源となる。

●Windowsプリフェッチ／スーパーフェッチファイル

Microsoft Windows のプリフェッチファイルは、アプリケーションデータを要求される前にメモリにロードすることで、Windows とアプリケーションの起動パフォーマンスを向上させるように設計されている。**プリフェッチ**は当初 Windows XP で導入され、その後 Windows オペレーティングシステムの後続バージョンに統合された。プログラムが実行された回数や最後の実行のタイムスタンプなどの詳細は、プリフェッチファイルに保存される。

プリフェッチファイルは、アプリケーションプロセスの実行時に偶然発生したファイルやアクティビティに関する詳細な手がかりを含んでいる。そのため、**あまりにも頻繁に注目される不正アクセスの単純なインジケーターとは対照的に、プリフェッチファイルは、**不正アクセスの他のアーティファクトを検討するための重要なコンテキストを捜査官・調査員に提供することができる。

調査全体の文脈で証拠の情報源を考慮した場合に利用できる情報の深さを示すために、次のセクションでは、プリフェッチアーティファクトの潜在的な有用性について概説し、それに関する一般的な誤解を訂正し、調査中にそれをどのように活用できるかを明らかにする。

Windowsプリフェッチアーティファクトのデジタルフォレンジック分析

機能性

プリフェッチプロセスは通常、アプリケーションの起動後最初の約 10 秒以内に実行され、アプリケーションが相互作用するファイルとディレクトリを監視して、その後の起動を最適化することを目的としている。プリフェッチファイル名は、**<実行ファイル名>-<プリフェッチハッシュ>.pf** という構造になっている。この場合、「実行ファイル名」は元のアプリケーションのファイル名を 29 文字に切り詰めたものであり、「プリフェッチハッシュ」は元のファイルパスに基づいて計算される。プリフェッチファイルは **C:\Windows\Prefetch** ディレクトリに保存され、各プリフェッチファイル（*.pf）は、ファイルパス、コマンドラインパラメーター、前回の実行時間、アクセスされたディレクトリ、他のファイルとの相互作用など、特定のアプリケーションの実行に関するデータをキャプチャする。

アプリケーションが再実行されると、そのファイルに関連付けられた既存のプリフェッチファイルが参照され、パフォーマンスが向上する。同じファイルが更新され、現在の実行に関する情報が反映される。

Windows 7 およびそれ以前のバージョンでは、オペレーティングシステムは最大 128 個のプリフェッチファイルを保存することができ、Windows 8 およびそれ以降のバージョンでは、この限度は合計 1,024 個のプリフェッチファイルまで増加した。

よくある誤解の訂正

プリフェッチアーティファクトについては、よくある誤解がいくつかある。以下は、それらの誤解を正すための説明の一覧である。

- Windows Server オペレーティングシステムでは、プリフェッチはデフォルトで有効になっていない。

- プリフェッチは、アプリケーションの実行中にアクセスされるすべてのファイルをキャプチャするわけではない。その代わりに、アプリケーションの起動後の最初の期間（約 10 秒以内）にアクセスされるファイルとディレクトリに焦点を当て、頻繁にアクセスされるリソースをプリロードすることで、その後の起動を最適化することを目的とする。

- プリフェッチはアプリケーションの起動プロセス中にアクセスされたファイルを記録する。これは、ダイナミックリンクライブラリ（DLL）や、アプリケーションによってロードされた他のリソースを含むことがあるが、それらは必ずしも直接実行されるわけではない。

- プリフェッチのファイル名に含まれる 8 文字のハッシュは、アプリケーションのファイルパスとコマンドラインパラメーターに基づいて計算される。このことから、コマンドライン引数のバリエーションにより、単一のアプリケーションに対して複数のプリフェッチ ファイルが作成される可能性が高くなる。

- プリフェッチは、アプリケーションの実行を正確に反映しない場合がある。例えば、プリフェッチファイルを手動で削除したり破損したりした場合や、アプリケーションがプリフェッチプロセスをバイパスした場合などである。

デジタルフォレンジック分析における活用

捜査官・調査員は、アプリケーションの実行に関する一般的に信頼できる証拠としてプリフェッチを活用することができる。プリフェッチ ファイルの作成時刻（B[158]）は、以前のプリフェッチファイルが元の場所から削除またはコピーされていないと仮定すると、バイナリがシステム上で最初に実行された時刻を示すことができる。プリフェッチ ファイルの最終変更時刻（M[159]）は、バイナリがシステム上で最後に実行された時刻を示すことができる。いずれの場合も、プリフェッチ処理時間を考慮して、作成時刻と変更時刻から 0〜10 秒の差分を減算する必要がある。一般的に、小さいアプリケーションは大きいアプリケーションよりも読み込みが速い。

プリフェッチファイルを解析することにより、アプリケーションの実行中にアクセスされたファイルやディレクトリに関する貴重な洞察を得ることができる。これは、マルウェアを調査し、悪用の試みを特定するという状況において、特にマルウェアがアプリケーション内のライブラリコンポーネントとして自身をロードしようとするシナリオで顕著である。

Windows Prefetch は、Windows システム上のアプリケーションの実行パターンに関する洞察を提供し、捜査官・調査員にとって貴重なアーティファクトとして機能する。その機能、よくある誤解、および活用のベストプラクティスを理解することで、捜査官・調査員はプリフェッチアーティファクトを効

158　Birth（誕生）- NTFSファイルシステムでのファイル作成時刻を示す
159　Modified（変更）- ファイルの変更日時を示します

果的に活用し、Windows イベントログや Shimcache のプロセス実行データのような他のシステムソースと相関させ、アプリケーションイベントのより正確なタイムラインを再構築することができる

●ページングファイルおよびハイバネーションファイル

Microsoft Windows は「pagefile.sys」という名前のメモリキャッシュファイルを使用し、物理メモリに入りきらない部分のメモリを保存している。捜査官・調査員はページングファイルを確認してアーティファクトを見つけ、場合によってはファイルを回復することもできる。また、Windows は、コンピュータが休止モードに入るときに利用される「hiberfil.sys」と呼ばれる類似のキャッシュメカニズムも使用する。このプロセスは、アクティブメモリ（RAM）をディスク上の「hiberfil.sys」に保存する。コンピュータを再起動／再開すると、ハイバネーションファイルは内容をメモリに復活させる。これらのファイルは法医学における解剖のように分析され、システム状態、アプリケーションの使用、一時ファイルの内容、サービス／通信の構成と使用の詳細など、揮発性メモリのアーティファクトを特定できるため、これらはすべて証拠の特定に役立つ。

●揮発性メモリのアーティファクト

アクティブメモリ（RAM）からアーティファクトを抽出して分析するため、これまでに数多くの手段がフォレンジック分析員らによって編み出されてきた。ランダムアクセスメモリとは、「揮発性」のコンピュータ用データストレージの 1 つである。つまり、RAM 内の情報は一時的なものであり、ある時点でのシステムの構成やユーザーの活動に関する情報の簡単な「スナップショット」のみが提供される。

揮発性メモリのアーティファクトにはさまざまな種類の情報が含まれている可能性があるので、これを念頭に置くことが大切である。アプリケーション、ユーザー、またはシステム機能に関するアクティブな詳細が利用可能である。たとえば、暗号化キーやパスワード、その他の認証トークンが存在する。その他の揮発性メモリ アーティファクトには次のものがある。

- **実行中のプロセス** - システムで実行中の全プロセスとその構成、関連リソースの使用状況である。この情報は、「タスクマネージャー」を見るのと似ている。各プロセスにはプロセス ID が割り振られ、（認証された）プロセスの所有者がいる。

- **過去および現在のネットワーク接続** - ポートやトラフィックの宛先を含む現在および過去のネットワーク接続（およびネットワークサービスの設定）は、疑わしい接続、または本来使われるべきでないポート上の活動を識別するのに役立つ。

- **ユーザー名およびパスワード** - メモリには、アプリケーションおよびサービスで使用されるユーザー名およびパスワード情報が（現在使用されている場合にはクリアテキストで、また一時用途ではハッシュ化された形で）保存されている。

- **暗号化キー** - 暗号化ファイルおよびマウントポイントは常に対応する復号キーを参照し、アクティブメモリに保持されている。

- **開いているレジストリキー** - レジストリハイブはオペレーティングシステムが機能するために必要であり、システムの実行中はハイブがアクティブメモリに読み込まれた状態となる。メモリ内のハイブを分析することにより、特定のプロセスおよびシステム活動をユーザーまたはセキュア ID（SID）トークンと関連付けることができる。マルウェアも、不正アクセスしたホスト上に居座るた

めにレジストリを使う種類のものが多いため、疑わしいキーがあれば調査に値する。そういったキーは、再起動されてもシステムに残るよう、実行キー（またはその他のキー）を使おうとするマルウェアの存在を示している可能性がある。

- **スクリーンショット／コンソール履歴** - メモリ分析技法を使えば、メモリを取得した時点で残っているスクリーンショットや、ダイアログボックスまたはコマンドラインから入力したコマンドなどのコンソール履歴を復元できる。スクリーンショットによって、メモリ取得時点でシステムを利用中だったユーザーについて、その時点で他にどのようなアプリケーションが実行中であったかを判断したり、スクリーン上にその他の情報が映っていたりするのを見つけたりできることがある。

- **復号されたアプリケーション／展開されたアプリケーション** - おそらく、マルウェアのリバースエンジニアリングを行う際のメモリ分析の最も価値のある側面の１つは、復号または展開されたアプリケーションおよびファイルセグメントを捉えられる点である。元々暗号化されているプログラムファイルは、いずれも復号しなければ正しく実行できない。これらのアーティファクトは、マルウェアのユーティリティまたはリソースの依存関係の他、ボットネットのコントロールパネルが通信に使う C&C サーバーのアドレスおよびプロトコルなど、重要な詳細を明らかにする場合がある。

- **メモリ常駐型（ファイルレス）マルウェア** - メモリ常駐型（ファイルレス）マルウェアは増加傾向にあり、マルウェアの使用を示すファイルをハードディスク上に残さないため、従来の方法で検知および検疫するのがかなり難しい。メモリ常駐型マルウェアは、アンチウイルスソフトウェアをはじめとする多くのエンドポイント防御／検知ソフトウェアを回避する。感染システムのメモリを分析すれば、悪意のあるファイルがメモリに読み込まれてプロセスを維持していたり、実行中のプロセスに直接挿入されていたりするのを識別できる可能性がある。

●クラウドトレージ

サイバー犯罪者の間でクラウド型のバーチャルコンピューティングおよびストレージシステムを利用する動きが広まっており、この傾向は続くと考えられる。クラウドコンピューティングは、証拠としてディスクを物理的に取得する場合のような利便性を提供しない。仮想サーバーとアプリケーションに割り当てられているメモリは他の仮想サービスと共有されるため、クラウドベースのメモリ取得は困難である。

クラウドベースのプロセスと論理メモリをキャプチャするために利用できる便利な方法はまだある。しかしながら、捜査官・調査員が活動している管轄区域とは別のところに仮想サーバーが存在していることが多い。クラウドストレージ型システムが捜査･調査の範囲内にある場合、捜査官･調査員は、データへのアクセス可能性、利用可能なログ、契約またはサービス レベル契約、および証拠収集プロセスを支援または妨げる可能性のある管轄上の制限を考慮すべきである [160]。

160　関連情報については第1章を参照。

クラウドコンピューティングの深層

クラウドコンピューティングが広く採用されていることを考えると、その基礎となる要素をより深く検討する必要がある。クラウドテクノロジーはこれまでにない柔軟性と拡張性を提供する一方で、捜査官・調査員にとって独特の課題も示す。

Google Cloud Platform（GCP）、Amazon Web Services（AWS）、および Microsoft Azure などのクラウドプロバイダーは、命名規則が若干異なるものの、同様のサービスを提供している。これらのサービスは以下のものを含む。

クラウドコンソール

クラウドコンソールは、特定のクラウドサービスプロバイダーのリソースをマネジメントおよび構成するための主要なインターフェースとして機能する。これは、管理者がインフラを監視するための集中型ダッシュボードを提供する。クラウドコンソールは、ユーザーの活動、API コール、および設定変更をログに記録し、システムイベントやユーザーの操作に関する貴重な洞察を提供する。各クラウドプロバイダーは、それぞれ独自にデフォルトのログ設定や保存期間の設定を行っており、プロバイダーによっては、これらのサービスに対して料金を課す場合があるということに留意する必要がある。その結果、顧客はコストを削減するためにログ記録を無効にする可能性があり、これは調査中に考慮しなければならない要因である。

クラウドコンソールと API へのアクセスは、IAM（Identity and Access Management）ポリシーによって制御される。基本的に、IAM はユーザーまたはサービスアカウントに付与される権限を決定し、クラウド環境内の特定のリソースに対してどのようなアクションを実行できるかを指示する。これは、クラウドプロジェクトへの不正アクセスに関する調査の際に重要な証拠となり、攻撃者が行った活動に関する洞察を提供する。

クラウドストレージ

各クラウドプロバイダーは、クラウドストレージサービスを独自に実装している。例えば、GCP は Google Cloud Storage（GCS）を、AWS は S3 バケットを、Microsoft Azure は Azure Blob Storage を提供している。クラウドストレージバケットは、データへのアクセスを規制するそれぞれの IAM ポリシーによってマネジメントされる。さらに、これらのバケットは、公共のウェブサイトやドキュメントをホスティングするなどの目的で、パブリックアクセスができるように構成することも可能である。これらのストレージサービスに関連する一般的なリスクは、すべてのパブリックユーザーにアクセスを許可するなど、誤った IAM ポリシーの設定によるデータの偶発的な流出である。

クラウドプロバイダーは、ネットワークファイル共有（NFS）や MySQL や Redis のようなマネージドサービスなどの代替ストレージオプションを提供する。インシデントが発生した場合、クラウドプロジェクトにデータが含まれているかどうか、どこに保存されているか、保存されているデータの性質を理解することが重要である。

仮想マシン

仮想マシン（VM）は、クラウドプロバイダーのデータセンターでホストされている物理マシン内に、分離されたコンピューティング環境を構築することを可能にする。VM の基礎となるディスクのスナップショットをキャプチャして、従来のフォレンジックツールを使って分析できるオリジナルの証拠を保存することができる。クラウド環境で一般的なファイルシステム形式には、NTFS、XFS、ext4 がある。

コンテナ

Docker のようなプラットフォームによって普及したコンテナは、分離とリソースマネジメントが追加されたプロセスである。コンテナは名前空間を使用して分離を提供し、cgroup を使用してリソースの使用量を制限および監視する。名前空間は、プロセスがシステム上で参照できるリソースを制限する Linux カーネルの機能である。cgroup は、プロセスの集合（CPU、ディスク、ネットワークなど）のリソース使用量を制限、マネジメントおよび分離する Linux カーネルのもう 1 つの機能である。

コンテナは特権または非特権として実行できる。特権コンテナのコンテナユーザー識別子（UID）0 は、ホストの UID 0 にマッピングされる。UID 0 は、実質的にシステムへのルートレベルのアクセス権である。一方、非特権コンテナは、コンテナ UID 0 をコンテナ外部の非特権ユーザーにマッピングし、自身が所有するリソースに対してのみ特別な許可を持つ。

Docker はクライアントサーバーアーキテクチャを使用する。このアーキテクチャでは、クライアントはユーザーが Docker デーモン（**dockerd**）にコマンドを送信できるようにし、Docker デーモンはリクエストを検証してランタイムエンジン **containerd** に送信する。次に、containerd は必要な分離の設定を支援し、コンテナの作成と実行を支援する **runc** にリクエストを送信する。Windows ベースのオペレーティング システムでも同様のアプローチが期待できる。名前空間と cgroup は Linux 実装であるため、主な違いは Windows カーネルが仮想化をマネジメントする方法にある。このメカニズムのさらなる洞察については、脚注の Windows コンテナーフォレンジックブログ [161] を参照のこと。

調査の観点から、コンテナはプロセスとして実行されているため、それぞれにプロセス ID（PID）が関連付けられる。インストールディレクトリには、いくつかの便利なアーティファクトも含まれている。Windows の場合、Docker のデフォルトのインストールは通常 **C:\Program Files\Docker** であり、Containerd のデフォルトのインストールは通常 **C:\Program Files\containerd** である。Linux の場合、Docker のデフォルトインストールは通常 **/var/lib/docker** であり、Containerd のデフォルトインストールは通常 **/var/lib/containerd** である。これらのディレクトリに含まれるファイルを手作業で調べることもできるが（cat や grep など）、コンテナ化された環境の調査は、コンテナの最後の既知の良好な状態と変更点との差分を取得できれば簡単である（例：docker diff を使用）。Docker Explorer や Container Explorer など、コンテナイメージを分析できるオープンソースのツールもある。

Kubernetes（クバネティス）

K8s としても知られる Kubernetes（クバネティス）は、コンテナ化されたアプリケーションのデプロイ、スケーリング、マネジメントを自動化するためのオープンソースのシステムである。Docker と K8s はどちらもコンテナ技術だが、機能は異なる。K8s は、複数のサーバーにわたってコンテナのマネジメントを簡素化するため、通常は本番環境の展開に適している。K8s のコンテナは、**ポッド**と呼ばれる論理的なグループ単位で実行される。K8s 内では、一般的に**ノード**と呼ばれるクラスター（マシンのグループ化）全体で、1 つまたは複数のコンテナをポッドとしてまとめて実行およびスケーリングできる。Docker デーモンに類似した K8s コントロールプレーンは、ポッドをいつどこで実行するかを決定し、トラフィックルーティングをマネジメントし、リソース使用率または事前に定義されたメトリクスに基づいてポッドをスケーリングする。

K8s クラスターを調査するには、K8s のコントロールプレーンのログと複数のノードに分散されたポッドを確認する必要がある。K8s の重要な課題は、クラスター内で動作するポッドとノードの動的な状態であり、その後、環境内で動作する攻撃者を軽減することである。例えば、資格情報が暴露され、攻撃者が K8s コントロールプレーンにアクセスして悪意のあるデプロイメントをスケジュールできるよ

161 https://osdfir.blogspot.com/2021/07/windows-container-forensics.html

うになったとする。分析では、悪意のあるポッドがどのノードにデプロイされたかを特定し、K8s の自動スケーリングによって削除されたかどうかを判断する。ノードが利用可能な場合、捜査官は基盤となるディスクのスナップショットを取得し、その後ポッド（ノード内で動作しているコンテナ）を調査できる。このような攻撃を軽減するには、ユーザーの認証情報をリセットし、K8s コントロールプレーンから悪意のあるデプロイメントを削除し、影響を受けるすべてのノードとそれらがアクセスしたデータを特定する必要がある。

ノード上に通常存在するアーティファクトは、**CRI-O Containerd**、および **Dockerd** などの基盤となるコンテナエンジンを含む。ポッドレベルのログは、Linux インストールの場合はデフォルトで **/var/log/pods** に保存され、Windows 環境の場合は **C:\var\log\pods** に保存される。

マネージドサービス

マネージドサービスと SaaS（Software as a Service）アプリケーションは、業務の合理化とコラボレーションの強化を目指す組織にとって不可欠なツールになっている。従来のオンプレミスのソフトウェア導入とは異なり、SaaS アプリケーションはサードパーティプロバイダーによってホストされマネジメントされるため、社内のインフラを維持する必要がない。捜査官・調査員にとって、SaaS アプリケーションは、法律違反・社内規定違反、ビジネス メール詐欺（BEC）、フィッシング、詐欺、その他の犯罪に関する多くの捜査における重要な証拠の情報源である。

注目すべきは、Microsoft 365（O365）と Google Workspace が最も有名な SaaS 製品であることである。Microsoft 365 は、MicrosoftOutlook、Office、Sharepoint、OneDrive など、クラウド上でホストされる一連の生産性ツールを提供する。ログは、Microsoft 365 セキュリティアンドコンプライアンスセンターで入手可能である。さらに、Microsoft Purview（以前は Azure Purview として知られていた）は、ユーザーの O365 データのデータガバナンスと eDiscovery を推奨している。

Google が提供する Google Workspace は、Gmail、Google Drive、Google Docs を含む同様のクラウドベースの生産性ツールを提供している。ログは Google Workspace のマネジメントコンソールで参照可能である。さらに、Google Vault は、Google Workspace の情報ガバナンスおよび eDiscovery ツールとして機能する。Vault を使用すると、ユーザーの Google Workspace データを保持、保留、検索、エクスポートすることができる。

O365 と Google Workspace の両環境を調査するには、ユーザー活動のログ、電子メールのヘッダーとやり取り、およびファイル共有の許可を分析する必要がある。

DFIRのためのオープンソースツールの活用

クラウドサービスの普及が進むにつれ、クラウドベースのデジタル脅威も増加する。組織はセキュリティインシデントに迅速かつ効果的に対応できる必要がある。インシデントレスポンスの重要な要素の 1 つは、脅威を分析し対応するための適切なツール群を手元に置くことである。

デジタルフォレンジックとインシデントレスポンス（DFIR）の領域では、調査プロセスのさまざまな側面に対応する数多くのツールがある。商用ソリューションは堅牢な機能セットと献身的なサポートを提供するが、商用ツールは、場合によってはドングルを必要とするライセンスのため、クラウド環境への展開が面倒なことがある。オープンソースのツールは、そのアクセシビリティと柔軟性、そしてデジタルフォレンジックの専門家の活気あるコミュニティの共同作業により、人気を得ている。

オープンソースの DFIR ツールは幅広い機能を網羅し、それぞれがフォレンジック調査において異なる目的を果たしながらも相互に関連した役割を果たす。オープンソースの DFIR ツールは多岐にわたるが、いくつかの主要なカテゴリが存在している（複数のカテゴリに当てはまるツールもある）。

- **収集**：ディスクイメージまたは個々のアーティファクトを取得するには、いくつかの方法がある。dd や FTK Imager のような従来の方法は、完全なディスクイメージをキャプチャするために採用することができ、Google Rapid Response（GRR）や Unix-like Artifacts Collector（UAC）のような特殊なツールは、アーティファクトのサブセットを取得するために利用することができる。ただし、ホストシステム上で収集のためにバイナリを実行するのは、フォレンジック調査に適切なアプローチではない。適切な方法の選択は、法的義務と適用される規則に基づいて決定されるべきである。

- **ライブ解析**：このプロセスでは、メモリの解析と監視、およびホストのライブ解析が行われる。これらのタスクによく使われるツールには、YARA と GRR がある。これらのツールは、アクティブなプロセス、開いているネットワーク接続、システム構成設定などの一時的なデータを抽出することを可能にする。これは、スクリプトベースの脅威を含む、メモリに常駐するマルウェアを特定するために非常に価値のあるリアルタイムの洞察を提供する。

- **データ処理**：システムログ（syslog や Windows イベントログ）、Windows レジストリハイブ、アプリケーション固有のログ、その他のソースを含むホストから取得したデジタルアーティファクトを解析し、関連付けるために Plaso（log2timeline）や Bulk Extractor などの専門ツールが使用される。Plaso で利用可能なパーサーについては、参考ドキュメント [162] を参照のこと。

- **タイムライン解析**：様々なツールがデジタルアーティファクトのタイムライン解析を支援し、時にはアーチファクトのプロセッサーとアナライザーの両方の役割を果たす。注目すべき例としては、Autopsy と Timesketch があり、どちらもアーティファクトとタイムラインの解析に広く利用されている。状況によっては、コマンドラインツールの「cat」または「grep」を使用すると、最も早く結果が得られることがある。

- **不正アクセスのインジケーター（IoC）の追跡**：マルウェア情報共有プラットフォーム（MISP）や Yeti などのオープンソースプラットフォームは、フォレンジック調査中に特定された IoC の追跡を容易にする。IoC を共同作業環境に一元化することにより、これらのツールはフォレンジックの専門家が捜査全体にわたって IoC を追跡することを可能にする。

調査を解決する際に、さまざまな目的で使用される DFIR ツールが多数存在するため、複数のオープンソース DFIR ツールの導入と統合を効率化するソリューションが必要である。これにより、効果的なインシデント対応インフラストラクチャの設定、維持、拡張に必要な時間と労力が削減される。

この問題を解決することを目的とした有望な新しいリポジトリの 1 つが、OSDFIR Infrastructure[163] である。これは、Kubernetes における複数のオープンソース DFIR ツールのデプロイと統合を自動化するための Helm チャートのセットと簡略化された手順を提供するオープンソースのリポジトリである。

このリポジトリは、以下のようないくつかのよく知られているオープンソース DFIR ツールのデプロイをサポートしている。

162 https://plaso.readthedocs.io/en/latest/sources/user/Parsers-and-plugins.html
163 https://github.com/google/osdfir-infrastructure

図 5-5. オープンソース DFIR ツール

- **Timesketch** - データ内のパターンを特定するためのアナライザーを備えた、共同で行うフォレンジックタイムライン分析のためのツールであり、Plaso、JSONL、または CSV ファイルのインポートに対応し、以下のようなツールとの組み込み統合をサポートする。
  - **DFIQ**：デジタルフォレンジックに関する調査上の質問とそれに答えるためのアプローチ用
  - **Sigma**：タイムライン全体にわたって実行される検出およびハンティングルール用
  - **Unfurl**：URL グラフ解析用
  - **Yeti**：タイムライン全体にわたって利用可能なすべての情報の検索用

- **Turbinia** - 大規模なフォレンジック証拠処理を自動化し、一般的な問題の発見を支援し、以下のような多くのツールとの統合を組み込む。
  - **Plaso（および dfVFS、libyal、SleuthKit などの関連プロジェクト）**：さまざまなソースからデータを抽出し、相関性のあるスーパータイムラインにまとめる。
  - **Container Explorer**：コンテナレベル処理用
  - **Docker Explorer**：docker コンテナレベル処理用
  - **Fraken**：マルチスレッド YARA スキャン用
  - **Libcloudforensics**：クラウドプラットフォームからの証拠のマウント用
  - **dfDewey**：ファイルや生のディスクから文字列を収集し、検索できるようにインデックスを作成する文字列抽出、インデックス作成、および検索ツール用。
  - Bulk Extractor や一般的なアーティファクトの分析ジョブなど、他にも多くの機能がある。

- **Yeti** - DFIR および脅威インテリジェンス追跡用であり、対応者は内部および外部システムからの CTI（観測情報、TTP、キャンペーンなど）を保存および分析することが可能。

- **GRR** - リモートライブフォレンジックに焦点を当てたインシデント対応フレームワーク。

- **dfTimewolf** - フォレンジック収集、処理、およびデータエクスポートを調整し、ツール間でデータを渡すためのフレームワーク。以下に例を示す。
  - クラウドディスクのコピーを作成し、そのディスクを Turbinia に提出してさらなる処理を行い、Plaso が作成したタイムラインを Timesketch に提出する。
  - GRR からファイルシステムのタイムラインを取得し、Turbinia を使用して Plaso を実行することによりタイムラインを処理し、作成されたタイムラインを GRR にインポートする。

OSDFIR インフラストラクチャは、複数のオープンソース DFIR ツールの導入、統合、メンテナンス、スケーリングを合理化することで、ギャップを埋めるのに役立つ。これには以下のような重要な利点がある。

- **展開時間の短縮**：展開には数分しかかからないため、対応者はより重要なタスクに集中できる。
- **一貫した構成を提供**：統合は自動的に行われるため、構成ミスや人為的エラーのリスクが軽減される。
- **認定デプロイメント**：複数のツールのドキュメントを確認する必要がなくなり、多くの DFIR ツールについて一元的に学ぶことができるため、リソースの共有による複雑さが軽減される。
- **簡単なスケーリング**：最小限のリソースにインストールでき、任意のコンポーネントを 1 つのコマンドでモジュール方式でスケーリングできる。Kubernetes の自動スケーリングは強力な機能である。

OSDFIR インフラストラクチャの利点は、多くのステップを必要とする現在のプロセスと、OSDFIR インフラストラクチャによる簡素化された一回の展開とを比較した下図にまとめられている。

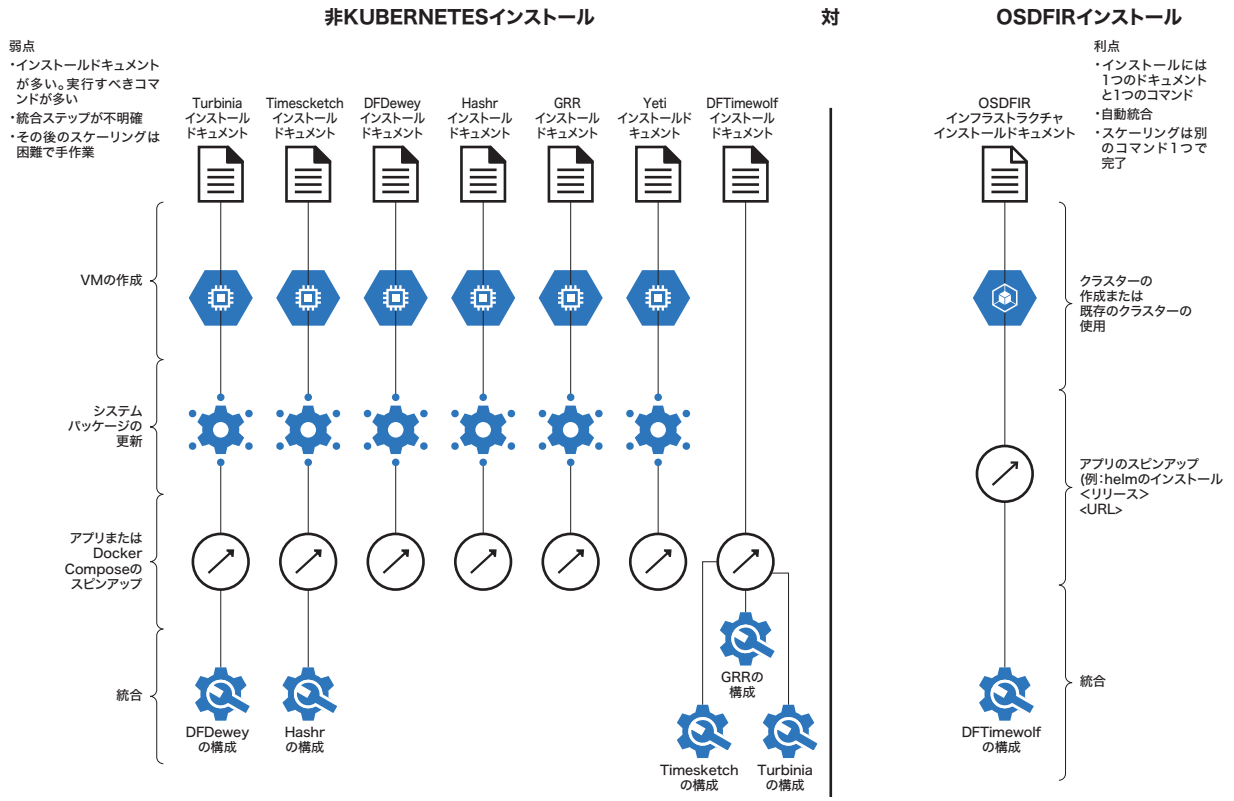


図 5-6. 非 Kubernetes インストールと OSDFIR インフラの比較

下記の図は、完全に展開された OSDFIR インフラスタックの構成を表している。

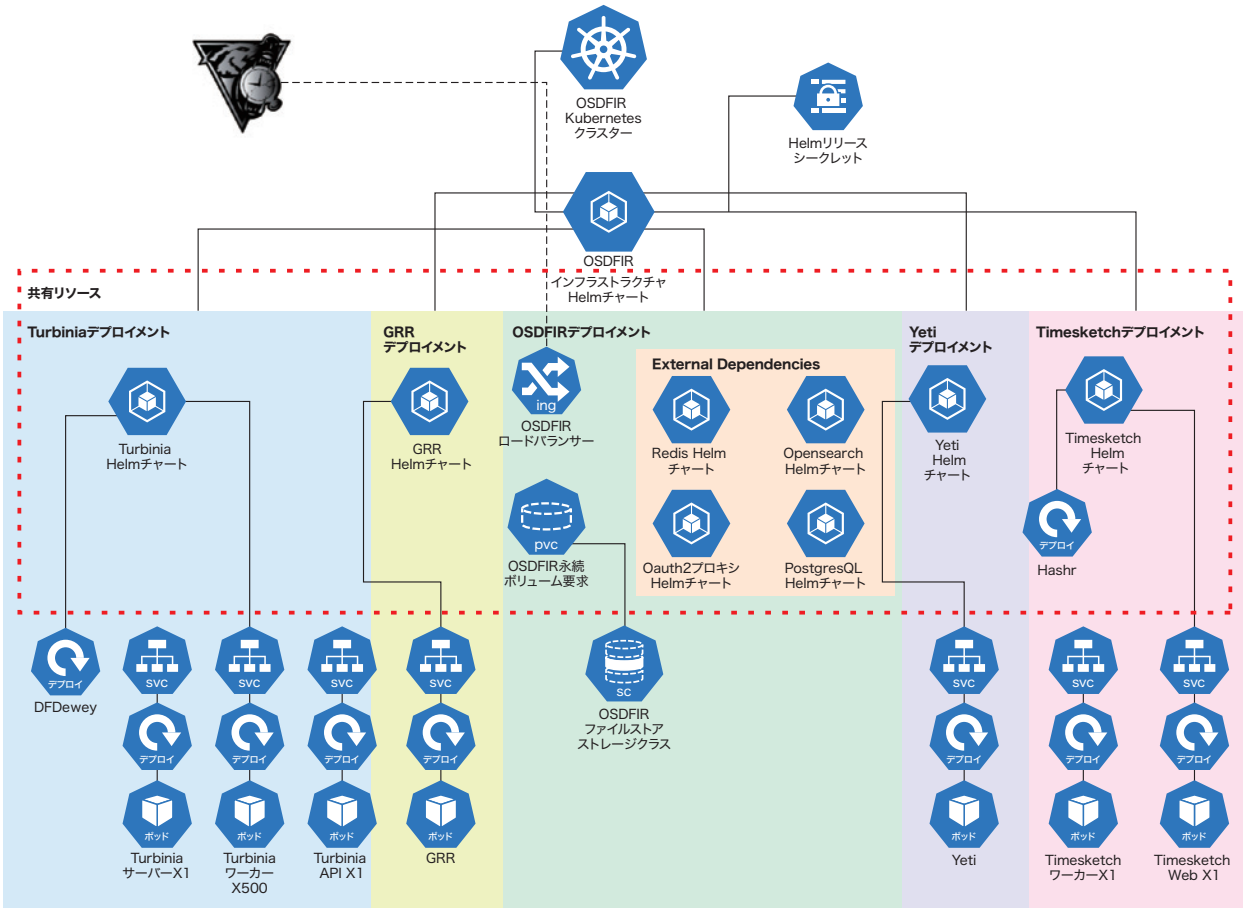


図 5-7. 完全に展開された OSDFIR インフラストラクチャ スタック

OSDFIR インフラストラクチャは最初は複雑に見えるかもしれないが、Helm クライアントと K8s クラスターがセットアップされると、インフラストラクチャ全体のデプロイは（必要なアップグレードを含めて）単一のコマンドプロセスになる。このプロジェクトは、詳細なドキュメントを提供し、安全なデフォルトインストールを実装することで、このプロセスを合理化することに専念する。すべてのアプリケーションはデフォルトでローカルで実行されるため、インストール後に Helm チャートで提供されるインストール後の手順に従って、ユーザーはそれらのアプリケーションにアクセスできる。

サービス

ロギングシステムとインフラストラクチャは、調査において最も魅力的な側面ではないかもしれないが、インシデント中に発生した活動を再構築したり、イベントのタイムラインを構築したりする上で、しばしば重要である。ログソースの関連性を評価する際に考慮しなければならないログマネジメントには、多くの側面がある。ログの可用性と整合性は捜査・調査の基本である。本項では、ログマネジメントの主要な特性の多くを検討し、各ログがどのように活用されるか、また捜査官が現場で遭遇する可能性のある一般的な問題についての洞察を提供する。

●イベントログ

Microsoft Windows のイベントログは、「Windows ログ」と「アプリケーションとサービスログ」の 2 つに大別できる。「Windows ログ」分類内には、さらにいくつかに分類されたログが存在する。

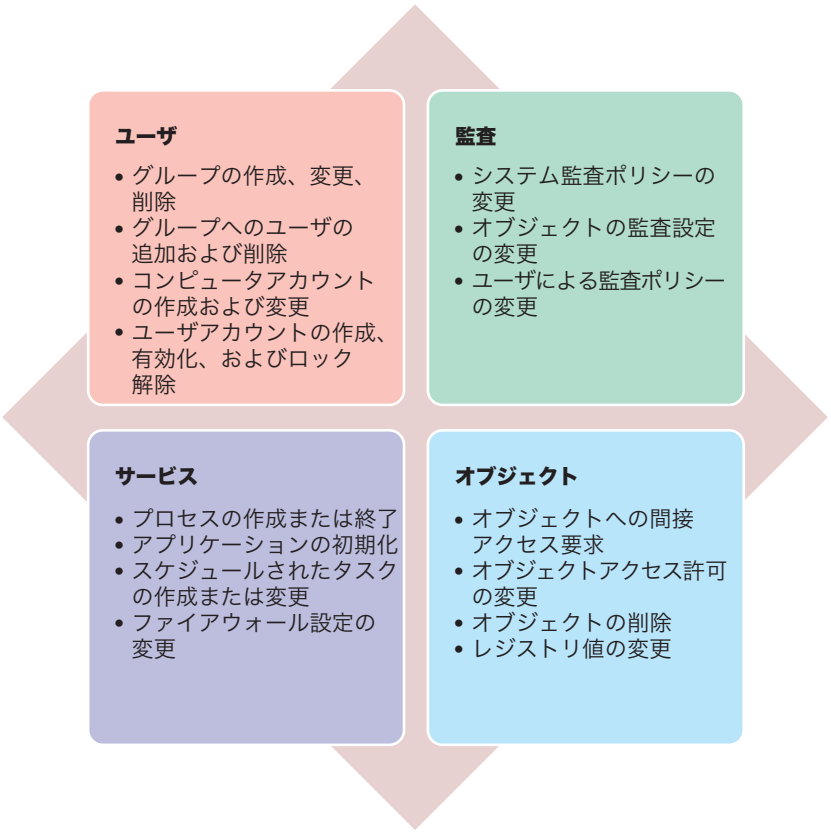


図 5-8. Windows イベントログのコンテンツ [164]

Windows イベントログの詳細な分類には次のものがある。

- **アプリケーションログ** – アプリケーションログにはプログラムまたはアプリケーションによって記録されたイベントログが含まれる。アプリケーションログに記録されるのは、アプリケーションのバックアップ失敗やアンチウイルスサービスによるマルウェアの検知である。アプリケーションのログ記録はプログラムごとにマネジメントされており、すべてのアプリケーションがイベントを生成するというわけではない。捜査官・調査員がアプリケーションログを調査するときは、記録されているのはどの種類の活動かを確認した上で、疑わしい活動を調査しなければならない。

- **システムログ** – システムログには、Windows オペレーティングシステムによって記録されたイベントログが含まれる。システムログに記録されているのは、システムの起動およびシャットダウン、時刻の変更などのイベントである。デバイスドライバ関連の活動もシステムイベントログファイルに記録される。

- **セキュリティログ** – セキュリティログには、アプリケーションサービスおよび関連のユーザー活動を含む、システムの重要な活動に関係する監査情報が含まれる。アカウントのログオンおよびログオフ、昇格の他、特権アクセス要求などのイベントもこれに含まれる。これらの監査ログは「成功」または「失敗」のいずれかとして記録される。

- **セットアップログ** – セットアップログには、オペレーティングシステムのインストールに関係する

164 http://www.thinkmind.org/index.php?view=article&articleid=icimp_2016_2_20_30032

情報が含まれる。

アプリケーションタイプとサービスログは Windows で収集されるイベントログとしては新しい分類である。これらのログは、Windows 7 以降を実行しているシステムにしか存在しない。これらのログは、システム上で発生するアクションについて、より詳細な情報を提供する。イベントログの収集源は他にもいくつかあるが、以下に主要な分類を掲げる。

- **マネジメント** – マネジメントイベントログは主としてマネジャーおよびサポート担当者向けのログである。これらのイベントログは、特にアプリケーションまたはサービスが正常に機能していることを確認するために記録される。

- **使用可能** – 通常、使用可能イベントは問題または事象の分析と診断に使用される。使用可能ログに含まれるイベントの中には、システム上のハードウェアの取り付けまたは取り外しといった貴重な情報が含まれている場合がある。

- **分析** – 通常、分析ログは、アプリケーションの状態の変化をイベントとしてログに記録し、アプリケーションの動作を監視するために使われる。特定の問題は分析ログに記録され、アプリケーションの開発の問題またはバグを示している場合がある。

- **デバッグ** – 一般的に、デバッグログには、トラブルシューティング目的で問題を切り分けるためにシステムで試行する作業に関係する詳細な活動ログが含まれる。

● セキュリティログに表示されるログオンタイプ

Windows のログオンイベントは、セキュリティログの中で最もよく調査の対象となる証拠の情報源である。証拠を正しく解釈するには、ログオンタイプの違いを理解しておく必要がある。各ログオンイベントの詳細には、イベントの「ログオンタイプ」が記録されている。システムの活動を適切に再現するには、これらの個々の活動を理解することが大切である。

- **ログオンタイプ 2：Interactive** – ユーザーがコンソールからのアクセスによりシステムにログオンしようとしたときにトリガーされる対話型のログオンイベントである。これは通常、ユーザーが物理的にシステムのローカルキーボードおよびマウスを使って認証するときに発生する。

- **ログオンタイプ 3：Network** – ユーザーがネットワーク認証を介してシステムにアクセスしようとしたときに記録されるネットワークログオンイベントである。これは通常、ユーザーがターゲットシステム上の共有ファイルや共有プリンタにアクセスしようとするときに発生する。ネットワークサービス認証もこのタイプのログオンを使用する場合がある。

- **ログオンタイプ 4：Batch** – 保存済み資格情報を使ってスケジュールされたタスクが実行されるときに記録されるイベントである。他に、スケジュールされたジョブがログオンタイプ 4 として記録される場合もある。

- **ログオンタイプ 5：Service** – サービスアカウントを使用して実行するスクリプトまたはプロセスがログオンタイプ 5 として記録される。

- **ログオンタイプ 7：Unlock** – ユーザーがシステムを再度使い始めるときに、キーボードとマウスを使ってロックを解除すると記録されるイベントである。ターゲットシステムでロック画面が有効になっている場合にのみトリガーされる。

- **ログオンタイプ 8：NetworkClearText** – ログオンタイプ 3 に似ているが、ユーザーアカウントのパスワードがクリアテキストで渡されたときのイベントである。これは、インターネットインフォメーションサービスの対話型ログインや、アプリケーションへの暗号化されていない（クリアテキストの）ログインにも使用される。

- **ログオンタイプ 9：NewCredentials** – NewCredentials ログオンタイプは、ユーザーが別のアカウントを使うときのログオンタイプである。典型的な例としては、スケジュールされたタスクが実行される場合や、「Run As」コマンドでプロセスを開始する場合がある。

- **ログオンタイプ 10：RemoteInteractive** – RemoteInteractive ログオンタイプは、「RDP」サービスを使用したリモートデスクトップ経由のシステムへのアクセスに関連付けられている。なお、VNC や類似のアプリケーションは代わりにタイプ 3 を利用する。

- **ログオンタイプ 11：CachedInteractive** – キャッシュに保存されている資格情報を使ってユーザーのドメイン認証が行われた場合に記録されるイベントである。最も一般的なシナリオは、システムがドメインサーバーにアクセスできない場合である。その後、ユーザーはシステムに保存されているキャッシュされた資格情報に対して認証される。

●ログ情報源の識別

ほとんどすべてのオペレーティングシステムが基礎部分に監査システムやログシステムを有している。たとえば先述したように、Microsoft Windows ベースのホストは包括的なイベントログ機能を備えており、活動を調査してインシデントの時間軸を構築するときに非常に貴重な証拠の情報源となる。イベントログを使えば、ユーザーアカウントの活動や、ほとんどのアプリケーションの動作情報に関する疑問点を解決するのに役立つだけでなく、ログオンおよびログオフの活動や、その他の疑わしい活動を識別するのを助ける。

●ログのローカル保存および集中保存

ほぼすべてのアプリケーションが何らかのログを作成するため、ログを適切に保存し、ログへの安全なアクセスを提供するには、大規模なストレージとインフラストラクチャを用意する必要がある。証拠の情報源を特定するためには、組織のログ構造や方針を理解することが非常に重要な側面である。

ログの保存には、大きく分けて主に 2 つの方法がある。

- **ログのローカル保存**とは、システムのありとあらゆるログを当該システム内に保存（ローカルに保存）することである。これは効果的な保存方法ではあるが、数十、あるいは数百といった単位のシステムのログを調査しなければならない場合には、全情報源へのアクセスを整理するのが複雑になるため、ログの回収作業に極めて時間がかかる。証拠収集の手段を検討するときは、分析用のログファイルを集めるのに必要な労力がどれくらいかに注意しなければならない。リソース要件を削減するために、これらのログの収集を自動化すると便利な場合がある。

- **集中保存**は、ログ保存のもう 1 つの構成方法である。ログファイルがローカルファイルシステム上に作成された後、ログファイルはログコレクターに転送され、集中ログサーバーに保存される。いくつものログを複数のシステムから集めてまとめたいときに、特に便利な方法である。

●ログの保持期間

潜在的な証拠の情報源を識別する際のもう 1 つの重要な問題は、ログ記録インフラストラクチャの保持期間を明確にすることである。捜査官・調査員がログの情報源を調べると、ログが十分に過去に遡っていないことや、関心のあるログがシステム上で利用できなくなっていることがわかったという事態があまりにも多い。経験豊富な捜査官・調査員であれば、捜査のできるだけ早い段階で、利用可能なログの保持期間を調べる。

通常、組織がログの保持期間を設定するときに、決定的要素となるのがストレージ容量の制限である。数千台単位のホストを保有している組織の場合、必要最小限のログを保存できる容量を超えるストレージを持っていない可能性がある。他に調べるべき事柄としては、法規制に定められている記録保持期間などのコンプライアンス要件がある。規制対象となっている組織によっては、ログの保持期間要件が定められている場合がある。この情報を活用することで、ポリシー違反や証拠隠匿を示す可能性のあるログ記録インフラストラクチャの欠陥があるかどうかを識別できる。

●ログの改ざん

標準的なログ記録で鍵となる問題のひとつは、ログが改ざんされたり、削除されたりしていないかを判断するのが非常に難しいという点である。どちらのシナリオも調査の結果に直接影響を与える可能性があるため、常に考慮する必要がある。ログの改ざんには、意図的な改ざんと、捜査過程における過失によるログファイルまたは記録の改ざんがある。

ログの改ざんを防ぐために、これらの活動を識別するための保護手段が開発されている。Microsoft Windows には、アクセス許可に基づいた制限が実装されており、ユーザーがイベントログを丸ごと削除するのを防ぐことができる。ユーザーが他の方法でログを消去したとしても、その行為自体が活動の記録を示す新たなログのエントリを作成することになる。そういったログは、捜査・調査において非常に重要な証拠の情報源となり得る。

ただし、ユーザーがシステム（SYSTEM または「root」）で最高レベルの権限を取得できるようにする脆弱性が依然として多く存在する。場合によっては、ユーザーは個々のレコードごとに、またはログ全体を削除することによって、ログエントリを変更および削除できる。特定の種類のマルウェアも、検出を回避するために、アンチフォレンジックメカニズムの一部としてこれらの手法を利用する。

多くの組織に採用されているもうひとつの保護機構は、集中ログ機能を活用する方法である。集中ログを使用するシステムでは、指定されたログファイルはシステム上にローカルに保存されず、通常はネットワーク接続を介してリモートログサーバーに送信される。ログソースがログ転送を停止した場合や、改ざんが疑われる場合に警告を発するように構成できる。集中ログアプリケーションの中には、ログが変更されていないことを確認するために、送信時と保存後の両方でログファイルの暗号化ハッシュが可能である。経験豊富な捜査官は、イベント、アプリケーション、またはシステム ログの可用性に関してどのような質問をするかを決定する際に、これらすべての点を考慮する。

●ログレベル

ほとんどのログ記録フレームワークは複数のログプロファイル（ログレベル）に対応しており、システム所有者がログシステムの主要特性を構成できるようにしている。ログレベルの大半は各ログに記録可能なデータ量と、どのイベントをログに記録するかをカスタマイズできるようになっている。すべての

アプリケーションがこれらの主なログレベルを使用するわけではないが、ほとんどが同様のログ構造を有している。捜査官・調査員はログレベルの違いを理解することで、どの種類の情報を最初に調べるべきかといった優先順位を決められる。

- **デバッグ** – 一般的に、「デバッグ」は最も詳細なログレベルである。問題の識別やトラブルシューティングを行うために、可能な限りの詳細を記録するように設計されているのがデバッグである。デバッグに設定されているログには、API キーやアクセストークン、その他アプリケーション特有の情報など、追加の情報を含んでいる場合がある。

- **情報** – ログレベルの「情報」は、アプリケーションの毎日の運用に役立つ詳細を出力するのに使われることが多い。通常、情報のログはアプリケーションの動作に関する特定の（細かい）詳細を表示する。

- **警告** – システムまたはアプリケーションの例外や、その他の主要ログイベントを扱うことの多いログレベルである。警告イベントは、たとえば構成ファイルが見つからないなど、重要であっても重大ではないエラーを知らせる。

- **エラー** – エラーログレベルは、あらゆる未処理の例外を記録する。アプリケーション実行中のあらゆるエラーや想定外の挙動がこのログに記録される。

- **致命的** – 致命的レベルは、アプリケーションで FATAL（致命的な）例外をトリガーする例外に特に使用される。これらのログは、アプリケーションの問題や、アプリケーションがクラッシュした理由、起動しなかった理由をすぐに識別するために使われる。

●SIEM技術を使った高度な相関

SIEM（Security Information and Event Management）システムは、関連システムのログデータやその他の情報源から集めたイベントを相関させて、潜在的なセキュリティリスクを識別するアプリケーションまたはアプライアンスである。一般的に、SIEM 技術はログマネジメントとデータ集約を、リアルタイムの監視およびアラートと組み合わせたものとなっている。これらの機能は、ネットワーク内のリスク活動を半自動的に識別するために利用できる高度な検知機構を提供する。SIEM のダッシュボードからイベントの相関関係を確認できるため、捜査官・調査員は注目すべきシステムや活動を簡単に見つけられる。

●サーバーログとシステムログ

ほとんどのアプリケーションやサービスは、捜査・調査の証拠として使える少なくとも基本レベルのログ記録機能を提供する。「Active Directory」（AD、アクティブディレクトリ）や DNS、VPN といったサービスには、捜査・調査のスコープ内で考慮すべき重要な証拠の情報源が含まれている可能性がある。他のアーティファクトと同様、これらのサービスおよびアプリケーションで適切なログを記録するには構成を設定しなければならない。設定によっては、十分な文脈を得られない最小限のログになったり、必要以上に詳細なために分析が難航したりしてしまう。

●Active Directory

Active Directory はドメインベースのネットワークサービスで、ユーザー情報やセキュリティ方針、

組織全体に分散しているリソースへのアクセスに関するマネジメントを自動化する。Active Directoryのログには、注目すべきホストのアーティファクトに関係する詳細な記録が含まれており、ユーザーおよびホストベースの活動を識別するのに役立つ。Active Directoryは大半の組織が全社的に使用しているため、証拠の情報源として大変有益である。Active Directoryには調査して特に役立つアーティファクトが複数ある。

Active Directoryサーバーの「NTDS.DIT94」ファイル[165]には組織の詳細が含まれている。これに含まれるユーザーごとの情報としては、アカウントの最終ログインの他、「UserAccountControl」フィールドに設定できる各種フラグなどがある。注目すべき主要なフラグ項目について以下に概要を説明する。

- **SCRIPT** - このフラグを設定すると、ログオンスクリプトが存在する場合には、ユーザーログオン時に実行する。
- **ACCOUNTDISABLE** - このフラグを設定すると、Active Directoryでユーザーアカウントが無効となる。
- **PASSWD_NOTREQD** - このフラグを設定すると、アカウントのパスワードが不要となる。
- **PASSWD_CANT_CHANGE** - ユーザーが自身のアカウントのパスワードを変更できなくなる。
- **INTERDOMAIN_TRUST_ACCOUNT** - 他のドメインを信頼しているアカウントを信頼するのを許可する。
- **SERVER_TRUST_ACCOUNT** - 当該ドメインのメンバーであるドメインコントローラのコンピュータアカウントであることを示す。

NTDS.DITファイルには各ユーザーのパスワードハッシュ（LMハッシュとNTハッシュの両方）が暗号化形式で含まれる[166]。Active Directoryの設定および構成には、疑わしい活動または権限の昇格を捜査官が識別するのに使えるような重要情報が含まれている場合がある。

●DNSのログ

DNSのログも、捜査で非常に重要な情報源となり得る。残念ながらDNSのログはサイズと量が大きくなるため、ほとんどの組織がDNS要求を記録していない。もし記録されているなら、さまざまな種類の疑わしい活動を識別できる。以下は、DNSログ記録によって可能になる機能の一部であり、証拠の情報源としての相対的な価値を示している。

- **不正アクセスのインジケーター** – DNS解決要求（自動または手動）は、OSINTやPROPINTといった情報源との関連性を調べ、既知のC&Cサーバーとの合致がないかを確認できる。
- **インテリジェンスマイニング** – 完全修飾ドメイン名（FQDN：Fully Qualified Domain Name）やトップレベルドメイン（TLD：Top Level Domain）などの登録詳細、登録者ID、関連メタデータ

165 https://technet.microsoft.com/en-us/library/cc961761.aspx
166 http://ntdsxtract.com/downloads/ntdsxtract/ntds_forensics.pdf

の類似に基づいて、追加の C&C につながる可能性のあるインテリジェンスを発見できる可能性がある。

- **シンクホール**[167] – 悪意のある DNS が見つかった場合（または見つかった時）、FQDN または TLD を DNS シンクホールで設定して、感染したホストを捜査員・調査員が発見するのを支援したり、サイバー犯罪の通信や関連活動を分析するために PCAP をキャプチャしたりできる。

●パスワードと証明書のマネジメント

パスワードと証明書をマネジメントするサーバーは、当然のことながら、極めて機密性が高く、「王国への鍵（Key to the Kingdom）」とも呼ばれる。これらの情報が保存されているシステムへの不正アクセスは大きなインシデントにつながる恐れがある。パートナーネットワークやベンダー／サービスプロバイダのクライアントサポートネットワークなど、組織が共有（保護）リソースおよびインフラストラクチャを使っている場合は特に重大になりかねない。これらの種類の技術がもたらす利点のひとつは、通常、システムと関連プロセスには強力な監査機能やレポート機能が組み込まれていることである[168]。捜査官・調査員は、パスワードまたは証明書マネジメントサーバーから利用可能なログと監査記録またはレポートを要求し、それらを潜在的な証拠ソースとして確認すべきである。

●VPNのログ

VPN 技術や VPN プロバイダは数多く存在するが、VPN ログは捜査において優秀な情報源となり得る。サイバー犯罪者はユーザーの認証情報を何らかの方法で取得し、組織の VPN サービスを介してアクセスを試みることが多い。利用可能な VPN ログを分析することで、捜査官・調査員はその情報をエンドポイントホストまたはその他のサービスのログソース上のアーティファクトからのユーザーの活動と関連付けることができる。これらの情報源を分析すれば、注目すべきアーティファクトが複数見つかることもある。たとえば、位置情報技術を使って個々の接続元 IP アドレスを調べれば、部外者を識別できるかもしれない。ユーザーが普段は家庭内から企業 VPN にログインするのに、夜中の不審な時間帯に海外からユーザーアカウントにログインしていたら、それはそのユーザーの認証情報が不正にアクセスされていることを強く示すインジケーターである。

●物理的なセキュリティと監視

物理的なセキュリティ監視のログもまた、捜査官・調査員が考慮すべき潜在的な証拠の情報源である。施設や設備への不正なアクセスを防ぐには、適切なアクセスマネジメントが必要である。ログや、物理的なアクセスおよび関連活動の調査を行うことができれば捜査で大きく役立つ。

- **入退室マネジメントシステム** – 物理的な場所や立ち入り禁止地区は、入退室を許可する人物を定めることが大切である。基本的には、適切な資格を有している人物以外はだれもマネジメント区域に入れないようにしなければならない。物理的な入場ゲートや入退室マネジメントシステムは、捜査官が調査して疑わしい活動を識別するのに使える監査ログを記録していることが多い。アクセスログは、被疑者個人やグループのプロファイルを作成するときにも役立つ。捜査官はこれらのログを使用して、ユーザーの通常のアクティビティを確認し、異常を特定する場合がある。

167 https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523
168 例えば、ペイメントカード業界のベンダー／クライアントのコンプライアンス要件:https://www.pcisecuritystandards.org/pci_security/

- **火災報知システムと安全マネジメントシステム** – 通常、犯罪をはたらくのに最も適したタイミングは、法執行機関や緊急対応担当者が他の事柄で手を離せないときである。サイバー犯罪が発生したときは、火災報知システムや安全マネジメントシステムのログに、同時の応答サービス通知が示されているかどうかを判断することが有益である。

- **音声および動画による監視** – 監視カメラや CCTV、その他の音声／動画監視システムは、悪意を持ったインサイダーがサイバー犯罪に関与しているときに役立つ証拠の情報源となる。

第5章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

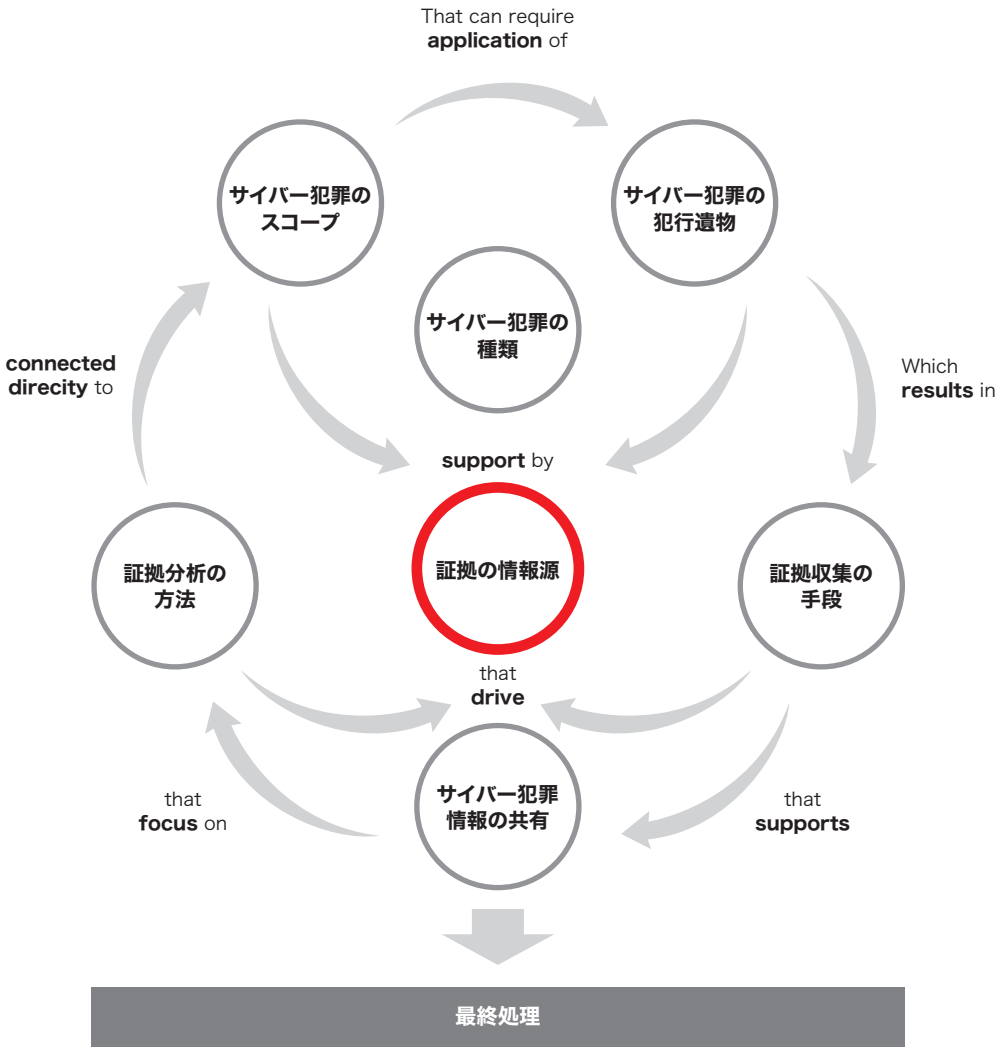


図 5-9 サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 5-1）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 5-1. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 5-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査マネジメント – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査マネジメントの機能は、組織に対してサイバー犯罪の特性と種類を説明する。またサイバー犯罪の目的と関連組織のプロファイルを特定するために、利用可能な証拠の情報源を戦略的に理解する必要がある。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各役割にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、サイバー犯罪に関係する証拠の情報源を識別し、発展させて、監視および収集する上で不可欠な戦術的情報源となる。

調査 – 利用可能な情報源にある犯行遺物や証拠を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。知見収集、説明責任、予防啓発、捜査マネジメントの各機能にある者が、サイバー犯罪の影響を識別するのを支援する。識別にあたっては、その犯罪に関連する目的の特性（および達成の段階）に対する評価を用いる。サイバー犯罪の種類は証拠によって決まる。調査の捜査官は、サイバー犯罪活動とその目的を特定するために、証拠の情報源から見つけることのできる兆候や犯行遺物について、戦術的な理解を必要とする。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。知見の収集、捜査手続きに関する指導を行い、関連方針および法規制に基づいて分析結果を解釈して、捜査マネジメントや予防啓発の各機能を支援する。法令に関する指導は捜査のアプローチだけでなく、実行されたサイバー犯罪の種類に応じた情報共有にも影響する。説明責任は、サイバー犯罪を明らかにするのに役立つ証拠の情報源について、戦術的な理解を必要とする。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪の種類に応じて、方針に基づきながら、何を、だれに、いつ、伝えるのかを決定する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。後方支援は証拠の情報源の収集および分析を支援する。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第5章:レビュー

1. **サイバー犯罪を識別する証拠の情報源にはどのようなものがあるか**
   答え：外部と内部。
   例：HUMINT/ELINT、コンピュータ、サーバー、モバイルデバイス、PBX システムなど。

2. **証拠は組織内外のどこで見つけることができるか**
   答え：脅威情報源、ハッカーフォーラム、ボットネットコントロールパネル、ネットワーク、ホスト、サービスログ。
   例：OSINT/PROPINT/RUMINT、SIEM、メタデータ、レジストリ設定、VPN ログ。

3. **証拠の情報源別に、内容、信頼性、および構造はどのように異なるのか**
   答え：構造化対非構造化および揮発性対永続性。
   例：ログ対プロセスメモリの詳細。

ケーススタディ5:フォレンジック技術を用いたMiraiボットネットの分析

- **犯罪**：不正アクセス、業務妨害
- **容疑者**：ボットマスター
- **手段**：マルウェアとボットネットの開発、認証情報の悪用
- **動機**：BaaS（Botnet as a Service）の評判と金銭的利益

最近の歴史上最も破壊的な分散型サービス拒否（DDoS）攻撃のいくつかを引き起こした Mirai ボットネットは、サイバー犯罪捜査におけるフォレンジック技術の応用を理解するための注目すべきケーススタディとして役立つ。

Mirai ボットネットの洗練された攻撃メカニズムは、様々な著名なターゲットに大きな影響を与えた。注目すべき被害者の中には、大手 DNS プロバイダの Dyn も含まれていた。2016 年 10 月の Dyn への攻撃は、Twitter、Reddit、Netflix、Spotify を含む多数の著名なウェブサイトのサービスを妨害し、米国とヨーロッパ全域で広範なインターネット停止をもたらした。もう一つの重要な被害者は、フランスの大手ウェブホスティングサービスプロバイダーである OVH で、ピーク時には毎秒 1 テラビットを超えるトラフィックの集中攻撃に直面しました。さらに、サイバーセキュリティジャーナリストのブライアン・クレブスが運営するブログ「Krebs on Security」は、史上最大規模の DDoS 攻撃の 1 つを経験し、ネットワークプロバイダにセキュリティプロトコルの見直しと防御の再評価を迫った。

サイバーセキュリティ企業 Imperva[169] による 2016 年の調査では、これらの事象に関連して、Mirai ボットネットによって活用されて感染した IoT デバイスのグローバルな性質が描かれている。それを下記の図に示す。

169　Source: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

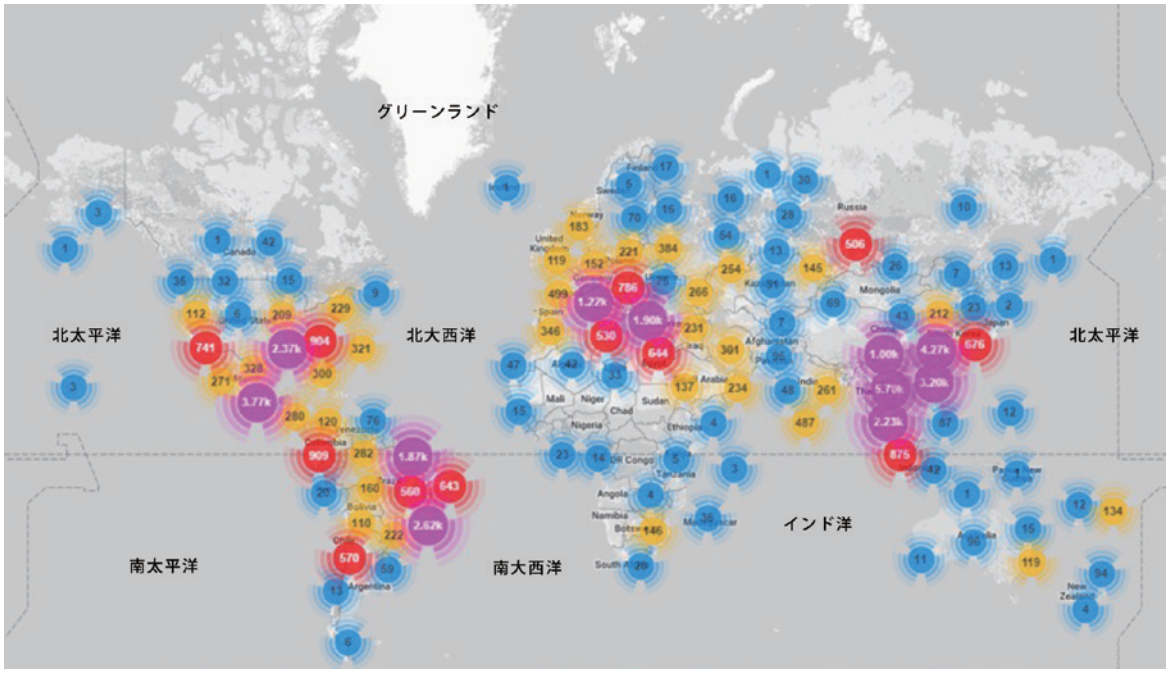


図 5-10. Mirai ボットネット

Mirai が特に狡猾なのは、デフォルトのログイン認証情報を悪用して IoT デバイスに侵入し、それらをゾンビに変えて大規模な攻撃を仕掛ける手法である。Mirai ボットネットは、インターネットに接続されたカメラ、ルータ、DVR などの日常的な物体を含むカテゴリであるモノのインターネット（IoT）デバイスに感染することによって動作する[170]。Mirai はブルートフォース攻撃法を利用してこれらのデバイスを制御する。工場出荷時のログイン認証情報が残っている IoT デバイスをスキャンすることで、Mirai はそれらのデバイスに簡単に侵入することができる。いったん感染すると、「ボット」とも呼ばれる不正アクセスされたデバイスは、ボットネットの作成者が運営するコマンドアンドコントロールサーバーによって制御される。

Mirai ボットネットのトポロジーとその全体的な範囲を以下の図に示す[171]。

170　https://storage.googleapis.com/gweb-research2023-media/pubtools/3982.pdf
171　https://www.sciencedirect.com/science/article/pii/S2666281720300214?via%3Dihub

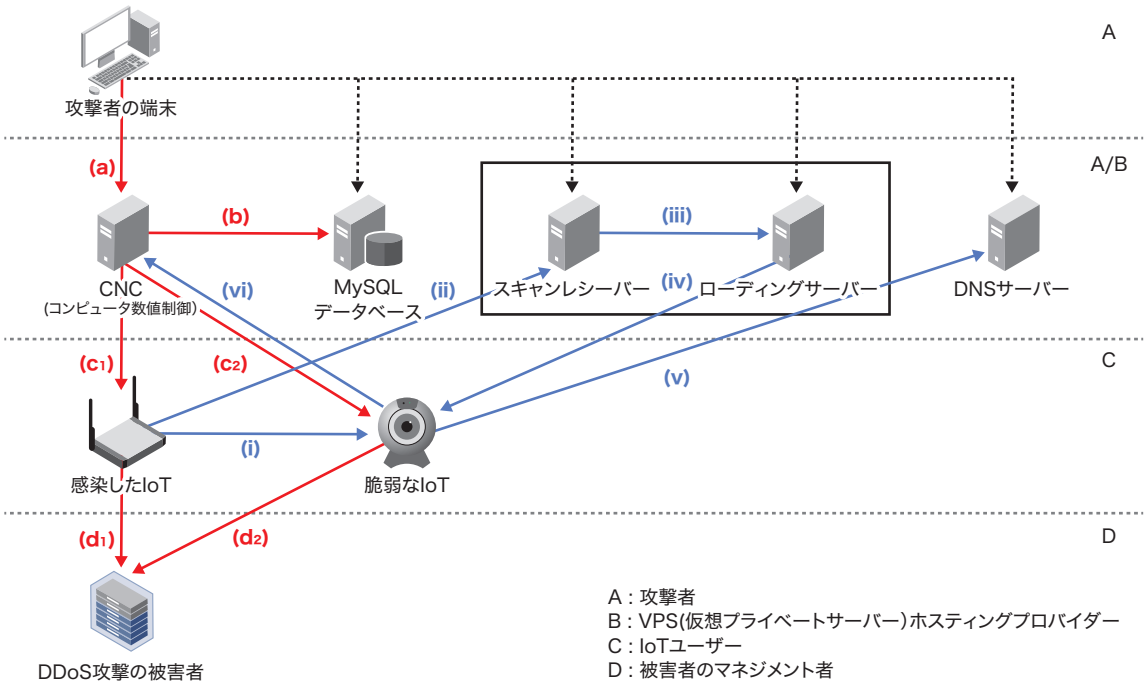


図 5-11. Mirai ボットネットのトポロジー

表 5-3. Mirai の不正アクセスを受けたデバイスの上位ベンダー

CWMP (28.30%)		Telnet (26.44%)		HTTPS (19.13%)		FTP (17.82%)		SSH (8.31%)	
Huawei	3.6%	Dahua	9.1%	Dahua	3.4%	D-Link	37.9%	MikroTik	3.4%
ZTE	1.0%	ZTE	6.7%	MultiTech	26.8%	MikroTik	2.5%		
		Phicomm	1.2%	ZTE	4.3%	ipTIME	1.3%		
				ZyXEL	2.9%				
				Huawei	1.6%				
その他	2.3%	その他	3.3%	その他	7.3%	その他	3.8%	その他	1.8%
不明	93.1%	不明	79.6%	不明	20.6%	不明	54.8%	不明	94.8%

表 5-4. Mirai の不正アクセスを受けた Mirai デバイスの上位種類

CWMP (28.30%)		Telnet (26.44%)		HTTPS (19.13%)		FTP (17.82%)		SSH (8.31%)	
ルータ	4.7%	ルータ	17.4%	カメラ／DVR	36.8%	ルータ	49.5%	ルータ	4.0%
		カメラ／DVR	9.4%	ルータ	6.3%	ストレージ	1.0%	ストレージ	0.2%
				ストレージ	0.2%	カメラ／DVR	0.4%	ファイアウォール	0.2%
				ファイアウォール	0.1%	メディア	0.1%	セキュリティ	0.1%
その他	0.0%	その他	0.1%	その他	0.2%	その他	0.0%	その他	0.0%
不明	95.3%	不明	73.1%	不明	56.4%	不明	49.0%	不明	95.6%

表 5-5. Mirai の不正アクセスを受けたデバイスのデフォルトログイン認証情報の例 [172]

ユーザー名／パスワード	メーカー	裏付けとなる証拠へのリンク
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Mirai の特徴的な技術的側面は、ドメイン名生成アルゴリズム（DGA）を使用していることである。このアルゴリズムは、コマンドアンドコントロールサーバー用に複数のドメイン名を定期的に生成し、被害者側がボットネットとボットの通信を妨害することを困難にする。さらに、ボットネットは、UDP フラッド、TCP ACK フラッド、HTTP POST 攻撃など、さまざまなタイプの DDoS 攻撃ベクトルを用いて、ネットワークリソースを圧迫し、標的のサービスを無力化する。これらのベクトルは、標的となるシステムの脆弱性に基づいて特別に選択され、攻撃によって引き起こされる影響と混乱を最大化する。また、Mirai はモジュラーアーキテクチャを採用しており、新しい機能や攻撃能力を迅速に組み込むことができる。このモジュール方式により、ボットネットは進化するセキュリティ対策に適応し、悪意のある活動を効果的に継続することができる。

著名なサイバー犯罪研究者のブライアン・クレブスは、2016 年の Mirai ボットネット攻撃を受けて調査を行った。彼は、後に米国当局が Mirai の作成者として拘束および起訴した複数の人物 [173] を特定した。特筆すべきは、それぞれが米国市民であり、当局に協力することで懲役刑を免れ、5 年間の保護観察処分と関連する金銭的損害の賠償を命じられたことである [174]。

残念なことに、Mirai のソースコードが GitHub に公開されたことで、「OMG」、「ZHtrap」、「Mukashi」など、後にいくつかの変種が作成される結果になった [175]。

Miraiボットネットのフォレンジック分析

Mirai ボットネットの構築と運用を理解するには、Mirai ボットネットのトポロジーを理解し、不正

172 https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/
173 https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
174 https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/
175 https://heimdalsecurity.com/blog/mirai-botnet-phenomenon/

にアクセスされたデバイスから十分な運用上のインテリジェンスを収集する必要がある。実際の設定と「偽」の設定を関連付けるために、各デバイスの複数のソースから証拠を収集することも重要である。特には、IoT 環境では、事後にそのような証拠を入手することが難しい場合があり、代わりに実験室での分析を実施し、その結果を使用してネットワークおよび動作プロセスの検出シグネチャを開発する必要がある。

ラボラトリーフォレンジック手順の詳細な例は、2020 年に実施された研究に示されている [176]。

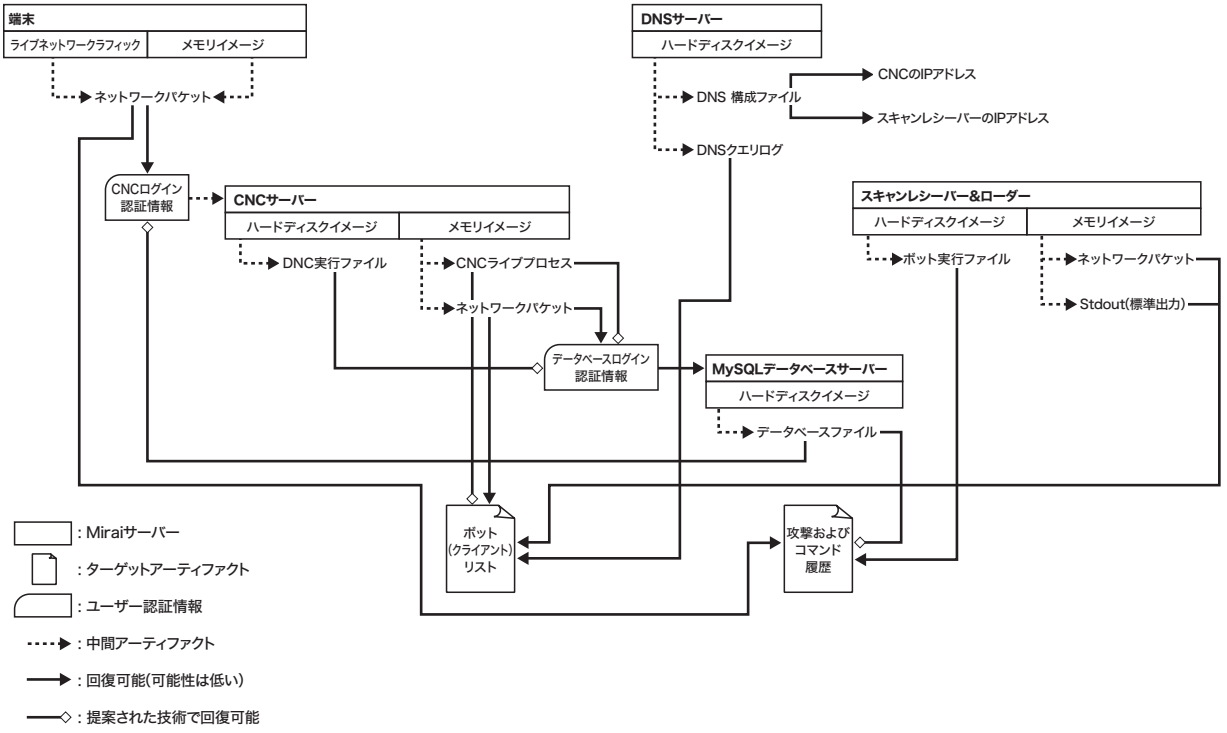


図 5-12. ラボラトリーフォレンジック手順の例

重要なのは、その研究で、ボットネットの分散アーキテクチャを理解するには、Mirai ボットネットのいくつかの段階をフォレンジック的に取得する必要があることが判明したことである。フォレンジック手順の共通点は、不正にアクセスされた各デバイスからのライブメモリとネットワーク通信の取得、バイナリーリバースエンジニアリング、プロセスと通信の分析などである。特に、通信構成を生成するためのプロセスメモリの分析が重要だった。

調査結果と意味

参照記事で概説されているように、Mirai ボットネットのフォレンジック調査により、その手口に関する重要な知見が明らかになった。これは、その伝播メカニズム、攻撃ベクトル、C2 通信戦略についてのより深い理解を含む。Mirai ボットネットのフォレンジック分析は、ライブネットワークトラフィック、メモリダンプ、バイナリリバースエンジニアリング、および公開リリースのソースコード分析など、いくつかの異なる関連した証拠ソースを含む、高度で多面的な調査手法を採用する必要性を強調している。このような情報は、緩和戦略の策定、IoT セキュリティプロトコルの強化、規制方針への情報提供にとって非常に貴重である。

176 https://www.sciencedirect.com/science/article/pii/S2666281720300214

第6章

証拠収集の手段

はじめに

デジタル証拠をそのソースから収集することは、証拠自体の分析と同じくらい重要である。多くの場合、証拠収集プロセスは厳しい精査の対象となり、不適切な証拠収集や取り扱いにより訴追が失敗した例は歴史上数多くある。犯罪の性質、捜査官・調査員の捜査・調査範囲、情報源を特定または認識する際の（捜査官またはセキュリティチームの）人的ミス、さまざまな種類のデータにアクセスするために使用されるテクノロジーなど、いくつかの要因によって、入手可能な情報源からどのような証拠を取得できるかが決まる。相互接続されたデバイス、クラウドサービス、および自動同期アカウントが急増しているため、捜査官が証拠を収集するための複数のソースを利用できる可能性があることに注意することが重要である。

これまでの章では、「モノのインターネット」全体のコンピューティングデバイスと通信デバイスの急増、そして産業用オペレーティングシステムやその他の機能オペレーティングシステムを含む従来の企業ネットワークの拡大について述べてきた。前述したように、クラウド（IaaS/PaaS/SaaS）の成長と採用は、サイバー犯罪の範囲、性質、目的を評価する上で、証拠ソースに関するさらなる考慮も必要としている。

証拠の情報源の規模が劇的に拡大するにつれ、サイバー犯罪を評価および証明するために必要な証拠を収集および保存するための自動化の必要性も高まっている。

本章では、証拠収集の自動化された方法と手動の方法について検討する。本章では次に、調査対象のサイバー犯罪の種類に基づいた証拠収集の違いについて説明する。さらに、本章は、証拠収集の効果的な方法を開発するための参考フレームワークを捜査官に提供し、組織のマネジメント者が防御と保護のための方針、システム、および手順を定義するのを支援する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の証拠はどのように収集できるか
- 証拠はどのように収集すべきか
- 証拠の信頼性を確保するためにどのような措置や手段を講じるべきか
- サイバー犯罪の種類によって証拠や関連する手法はどのように異なるのか

サイバー犯罪のアーティファクトにおけるトピックス分類

「証拠収集の手段」知識領域ににおけるトピックスの分類を図 6-1 に示す。

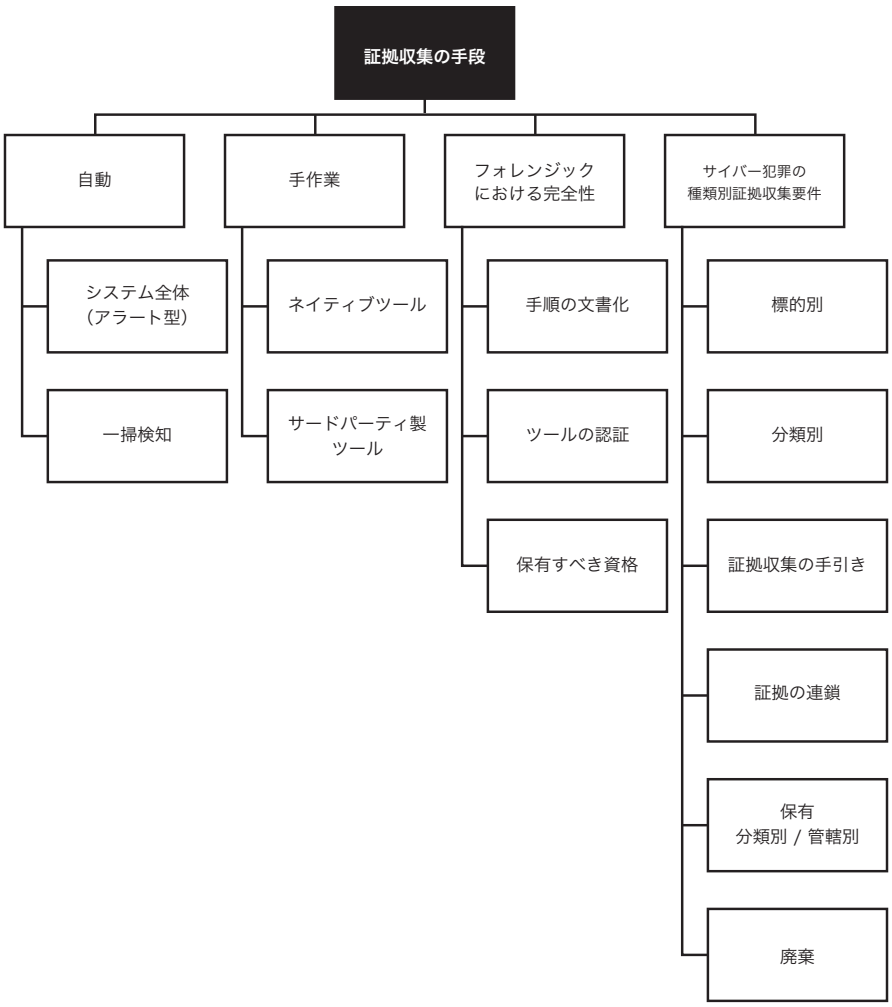


図 6-1.「証拠収集の手段」知識領域におけるトピックスの分類

証拠収集の手段とは

今日、捜査官・調査官がサイバー犯罪の範囲、目的、TTP を特定できるように、デジタルソースから証拠を収集する方法がいくつかある。歴史的に、ネットワークセキュリティの役割を担う捜査官は、IoC アラートを伝播する特定のシステムに関連する証拠ソースに焦点を当ててきた。捜査官・調査官はその後、付随的な証拠を調べるために他の関連する「関心のあるシステム」を特定するが、時折、重要なデータやアーティファクトが誤解され、不完全な情報に基づいた結論につながることもある。IoC の追跡に基づく証拠収集方法は、糸がどこにつながるか、どのくらい長いかがわからないため、「yarn ball（毛糸だま）」と呼ばれることもある。その結果、リソースのコスト（人、ツール、時間、および関連する経済的費用）は「毛糸だま」と同じくらい長くなる可能性がある問題をさらに複雑にしているのは、調査官がようやくこの「毛糸だま」を解きほぐせたとしても、企業の SIEM がすでに求めていたデータを削除してしまっている可能性があるという点だ。

サイバー犯罪の範囲を特定するには、より効率的な手順が必要である。コンピュータを調査し、担当者にインタビューし、ログソース（つまり、第5章で説明した証拠の情報源）を確認するアプローチの有効性は、スケーラブルでありながら包括的な証拠収集のプロセスにかかっている。これを容易にするために、「トリアージ」アプローチを使用すべきである。トリアージに基づく証拠収集とは、証拠の種類と場所をより迅速に特定するために、段階的アプローチでシステム、ツール、収集活動を使用することを指す。これにより、証拠の量、複雑さ、範囲、そして捜査の全容を理解することができる。このような証拠は、情報源と調査源の両方に基づくアーティファクトとデータから導き出される。情報源は、インタビューの実施のほか、法執行機関（または法執行機関に準ずる組織）が公開した、あるいは情報セキュリティの研究者やアナリストが作成した「オープンソース」および「独自」の情報の確認が含むことがある。

捜査官・調査員は、捜査・調査に関連する技術的証拠の関連情報源を特定し、保存しているだけでなく、無関係と判断された情報源は、法的に有効な分析プロセスに基づいて評価されたことを説明できることが重要である。

トリアージに基づく証拠収集のプロセスには下記の3つの段階がある。これは捜査官・調査員（または監査人 - このプロセスはリスクアセスメントとマネジメントの目的もサポートするため）が、証拠収集の対象となる特定のシステムを特定するのに役立つ。

1. **スイープ・ディスカバリー（一掃検知）**：トリアージプロセスは、対象となるITエステート内のすべてのマネジメント対象（またはアクセス可能な）ホストの評価から始まる。これには、ネットワークやセキュリティレポート（SIEMなど）のログと関連付けることができるエンドポイントホストのデータを収集することを含む。第1段階では、「関心のあるシステム」に対する調査活動に重点を置く。
2. **捜査・調査**：第2段階では、ポリシーまたは手続き上の指示に従って特定の証拠を保存するため、深い技術分析や収集が必要なデータのサブセットに関するメタデータを収集し、捜査の範囲をさらに絞り込む。
3. **スイープ・ディスカバリー（一掃検知）、捜査・調査、収集**：証拠をトリアージするプロセスは多くのソースから取得できる、特定の目的を果たすためのその有用性は、収集プロセスの信頼性と、分析を通じて証拠が伝える情報の完全性に依存する。

下記の図6-2はトリアージに基づく証拠収集の概念を示している。

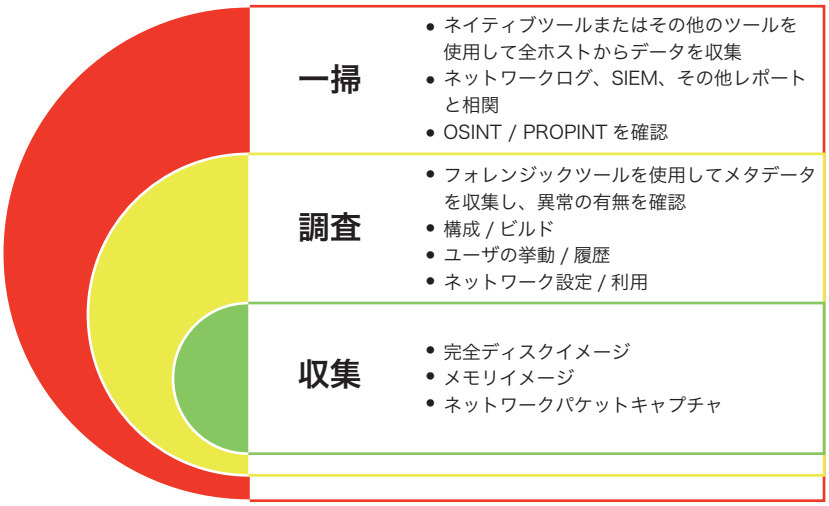


図 6-2. トリアージに基づく証拠収集

このトリアージアプローチにより、捜査官・調査員はサイバー犯罪の目的に関連して解釈できるデータを収集することができる。例えば、企業アカウントからの盗難が発生した場合、このアプローチによって操作官・調査員は、導入されたツール（マルウェアなど）が関係するシステムや認証情報で使用されたかどうかを識別することができる。

トリアージ型のアプローチでは、証拠の収集に自動化された方法と手作業による手段を活用する。例えば、エンドポイントのアーティファクト発見と証拠収集の負担を軽減するために、多くの組織が自動化を採用している。このような場合、情報収集手法を伝えるというよりも、サイバー犯罪捜査・調査や組織のサイバーセキュリティ体制を支援するツールがなぜ存在するのかを理解するために、以下の情報が役立つ場合がある。[177]

これらの慣行は、一般的に次のように受け入れられている。

- 証拠の特定
- 証拠の収集と取得
- 証拠の保全と保証
- 証拠の処理
- 証拠の分析
- 報告

これらの実践は、以下のような国内的、国際的、専門的な基準によって支えられている。

- ISO/IEC 27037[178]：「デジタル証拠の識別、収集、取得、保全に関するガイドライン」
- ISO/IEC 27041[179]：「インシデント調査方法の適切性及び妥当性を保証するためのガイドライン」
- NIST SP 800-86[180]：「フォレンジック技術をインシデントレスポンスに統合するためのガイド」。

177 特定の成果物とツールについて説明するが、この章は概念を示すことのみを目的としており、証拠収集のための指示やツールの推奨を行うものではないことに注意すること。
178 https://www.iso.org/standard/44381.html. Published 2012 and last confirmed as current in 2018.
179 https://www.iso.org/standard/44405.html. Published 2015 and last reviewed and confirmed as current in 2021.
180 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf. Published 2006.

- SWGDE[181]：「デジタル証拠に関する科学ワーキンググループ」
- NIST CFTT[182]：「コンピュータフォレンジックツールテストプログラム」

いずれの場合も、捜査官は適用可能な基準を確認し、必要に応じて関連するガイドライン、実践、手順を適用すべきである。

証拠の自動収集

市販のオープンソースのサイバーセキュリティツールを使用することにより、捜査官はさまざまなソースからデータを取得し、そのデータを分析し、その証拠価値を判断できる。警告メカニズムによって関連するアーティファクトを識別して強調表示するようにプログラムされたインジケーターに従って、さまざまなテクノロジーがアーティファクトを収集する。サイバーセキュリティアナリストや捜査官は、ツールを使って、手動でなければできない証拠収集の方法を自動化することもできる。

システム全体（アラート型ロギング）

組織が採用すべき必須の技術の1つは、不正アクセスのインジケーター（IoC）を記録するアラートベースのシステムである。第3章に記述されているように、IoCは、イベントの日時、パターンマッチ（暗号ハッシュまたはヒューリスティック行動シグネチャ）、および潜在的なインシデントに関する有用な詳細を提供することができる関連メタデータのようなアーティファクトを反映する。下記のIoCの例は、「Careto」マルウェアのエンドポイント検出のアラート条件を示している[183]。

181 https://www.swgde.org/documents/published-by-committee/forensics
182 https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt
183 https://conf.splunk.com/session/2014/conf2014_FredWilmot_Splunk_Security.pdf

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="8ddb7d26-b275-446c-bbaa-387e6b29135b" last-modified="2014-02-12T02:21:38"
xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Careto "The Mask" Espionage Campaign</short_description>
  <description>This IOC detects activity revealed in the Kaspersky report
  unveiling the mask. The Mask is an advanced threat actor that has been
  involved in cyber-espionage operations since at least 2007. The name "Mask"
  comes from the Spanish slang word "Careto" ("Ugly Face" or ?Mask?) which
  the authors included in some of the malware modules. The main targets of
  Careto fall into several categories: Government institutions, Diplomatic /
  embassies, Energy, oil and gas, Private companies, Research institutions,
  Private equity firms, and Activists. The Mask?s implants can intercept
  network traffic, keystrokes, Skype conversations, analyse WiFi traffic, PGP
  keys, fetch all information from Nokia devices, screen captures and monitor
  all file operations.</description>
  <authored_by>@iocbucket</authored_by>
  <authored_date>2014-02-12T01:05:09</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="d8799972-a5b1-49de-a4e4-a3691a732b4d">
      <IndicatorItem id="8d6b0f66-0351-4ca0-b21c-19c895b25bbc"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">linkconf.net</Content>
      </IndicatorItem>
      <IndicatorItem id="a9d87fad-e313-48cc-b858-d8caaad2edcb"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">redirserver.net</Content>
      </IndicatorItem>
      <IndicatorItem id="4d5623fc-66c4-45c6-8804-3c0737c30a35"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">swupdt.com</Content>
      </IndicatorItem>
      <IndicatorItem id="de7165e5-f647-4f81-b82e-5c4f0a210e5e"
      condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">shlink32.dll</Content>
```

図 6-3. システム全体アラートの IoC の例

この IoC は、カスペルスキーの報告書で明らかになった、マスクの活動を検出する。「マスク」は、少なくとも 2007 年以来サイバースパイ活動に関与している高度な脅威アクターである。「マスク」という名前は、スペイン語の俗語「Careto」（「醜い顔」または「マスク」）に由来しており、作成者はこれをマルウェアモジュールの一部に含めた。Careto の主なターゲットは、政府機関、外交官／大使館、エネルギー、石油、ガス、民間企業、研究機関、未公開株式投資会社、活動家など、いくつかのカテゴリに分類される。「マスク」のインプラントは、ネットワークトラフィック、キーストローク、Skype の会話を傍受し、WiFi トラフィックや PGP キーを分析し、Nokia デバイスからすべての情報を取得し、画面をキャプチャし、すべてのファイル操作を監視することができる。

製品によって使用する IoC モデリング言語は異なるが、一般的には各製品は同様の情報に対して警告を発する。最もよく使われている IoC 標準の例としては、構造化脅威情報表現（STIX）[184]、信頼できる指標情報自動交換（TAXII）[185]、および「OpenIoC」[186] がある。下記の図 6-4 は STIX アラートアーキテクチャを示している。

184　https://stixproject.github.io/
185　https://taxiiproject.github.io/
186　http://www.openIoCIoC.org/

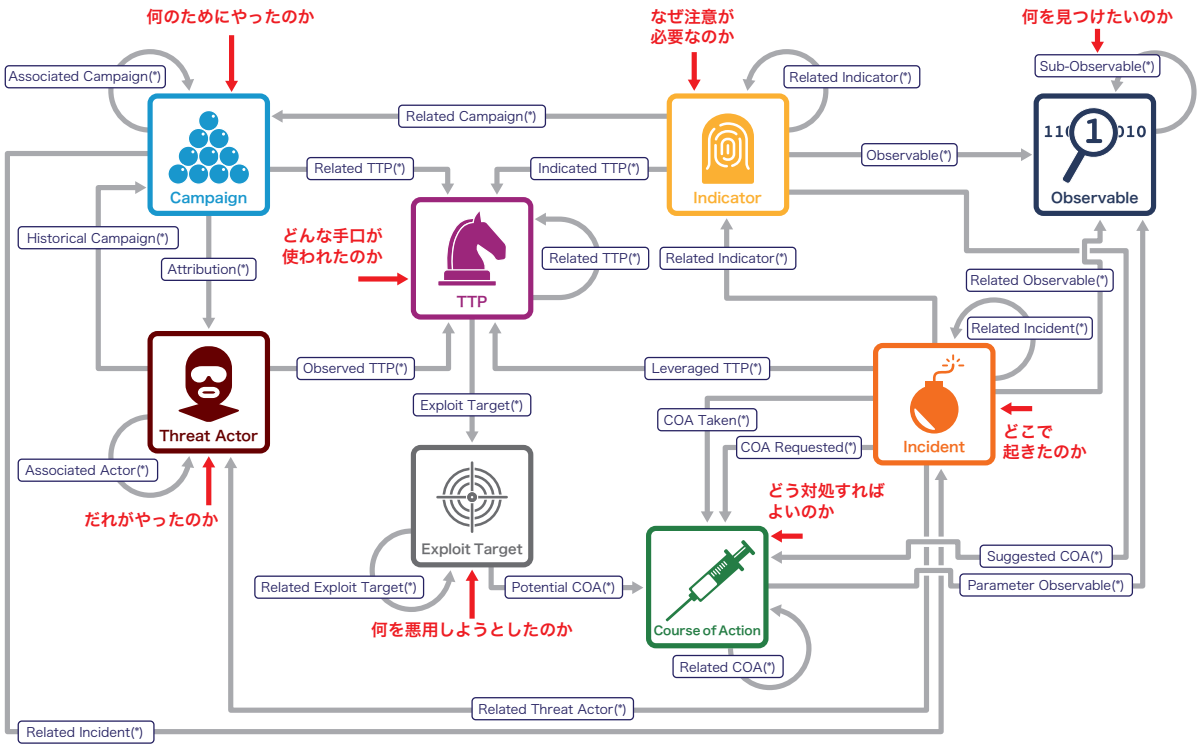


図 6-4. アラートの STIX アーキテクチャ

これらの IoC 標準は、情報共有を目的とした共通の交換方法として設計された。交換形式の共通化により、多くのサイバーセキュリティ製品および調査製品は、脅威インテリジェンスを体系的に統合し、それらが監視する環境における悪意のある活動の独立した（場合によっては相互依存的な）検出を向上させることができる。

一部の製品は、情報の保存や交換において、限られた「承認済みの」パートナーソリューションとの間で、依然として独自のプロトコルを使用している。ただし、これらの製品であっても、多くの場合、共通の IoC 形式に統合され、集中型／統合型のログ記録システムが IoC 情報を関連付けてアラートを生成できるようになる。これらのログ システムでは、サイバー犯罪活動の文脈型アーティファクトをログに記録するためのプロファイルが自動化され、体系的な証拠収集がサポートされる。

監視対象のエンドポイントや証拠ソースからのデータを集約する SIEM や同様のコンソールは、証拠の体系的な収集と分析にも使用できる（第 7 章で説明）。しかし、証拠収集には、標準的な製品に設定されているかどうかわからないコンテキストが必要であり、最近では、サイバーセキュリティ、コンプライアンス、リスクマネジメント、サイバー犯罪捜査の要件をサポートする他のワークフローソリューションも登場している。

図 6-5a. アラート型ロギング

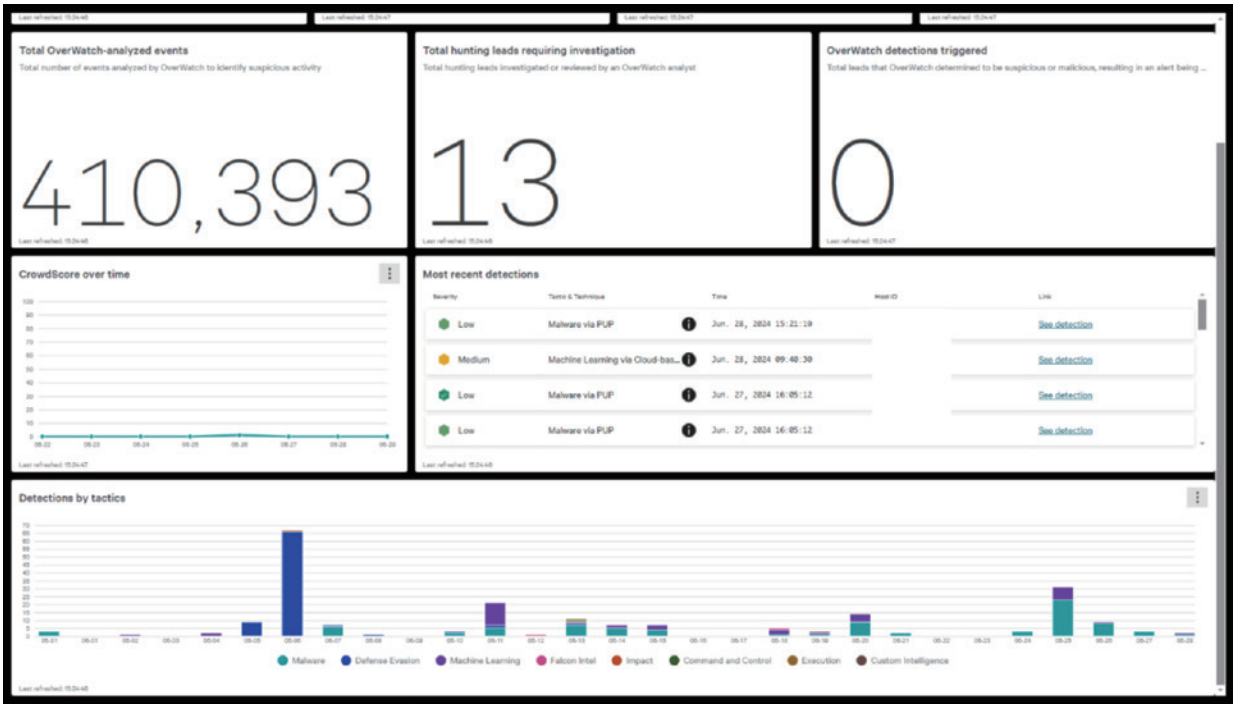


図 6-5b. Crowdstrike Falcon Overwatch のアラート型ロギング

捜査官・調査員にとって重要な考慮事項の１つは、探している情報が記録されているかどうかである。もう１つは、関連するシステムが特定の活動を正確に相関付けるための参照視点を持っているかどうかである。現代のネットワークセンサーはしばしばネットワークトラフィックを記録し、ホストセンサーはホストトラフィックを記録するため、捜査官・調査員が不正なイベントを適切に特定するには、これら２つのデータソースをしばしば相互に関連付ける必要がある。ログの忠実性は、ログ記録システムを適切に構成し、その出力を確認して、調査の質問に回答し、追加の調査の手がかりを生成する際に保存されたログの正確性と有用性を保証するための副産物である。捜査官・調査員は、どのようなログ記録

メカニズムが実施されているか、何がログに記録されているか、それらのログはどこに保存されているか、誰がそれらのログにアクセスしたかを判断し、それらのログの保持ポリシーを確認すべきである。捜査・調査で何も見つからなかったと宣言する前に、利用可能なログを確認してこれらの質問をし、答えを出さなければならない。これは、さまざまな独自のセキュリティ製品から標準化された「syslog」スタイルのメッセージングを使用して、上記の図 6-5 に示している。警告システムのベースとなるイベントのログファイルを調べるとき、または証拠を見つけるために実際の収集を実行するときは、まずログ記録がどのように構成されているかという疑問を最初に検討しなければならない。ログ構成の証明は、収集した証拠に添付されるべきである。

アラート型のロギングの有効性は、適格なインテリジェンスと監査されたシステマティックな手順の融合に依存する。これらは、TTP の変化とともに進化するサイバー犯罪の証拠の範囲、種類、性質について適切な視点が理解されるようにマネジメントされなければならない。効果的なプログラムは、これらの観点とそれを支える自動化のバランスを組み込み、組織が調査を効率化し、回復と解決活動のプロセスを迅速に開始するのに役立つ。インテリジェンスと情報の共有は、サイバー犯罪の認識向上に貢献する IoC の独自のソースを提供するいくつかの組織によって増強され、広範囲に及ぶオープンソースのコミュニティベースのプラットフォームに成長した。ただし、第 4 章で説明したように、IoC は組織に対するリスクの文脈で理解されるまでは「脅威インテリジェンス」ではない。

スウィープ・ディスカバリー（一掃検知）

捜査官・調査員は、サイバー犯罪のスコープを迅速に判断し、保存する証拠の情報源を特定しなければならない。企業環境では、犯罪現場が大規模で分散していることがある。サイバー犯罪が広がる速度と多くのコンピューティング環境の複雑さの両方を考慮すると、スキャンまたは「一掃検知」の初期トリアージ段階は捜査官・調査員の助けとなる。

デジタル資産をスキャンする最初の段階は、さまざまなソースを列挙して、IoC やその他のアーティファクトが存在する可能性のある場所を特定するのに役立つ。これにより、捜査官・調査員は収集と分析活動を、まず関連するシステムに集中させることができる。一掃検知を実行する際には、既存のオペレーティングシステムやサードパーティのソフトウェア ツール、スクリプト、ログファイルを使用するのが一般的である。多くの場合、これは、当初は無関係または関連性がないと考えられていた証拠の情報源を特定するために、デジタル資産全体をスキャンすることになる。

適切に構成された一掃検出プロセスには、ホストベース（エンドポイント）およびネットワーク（外部接続またはその他の重要な接続）の監視を含む、さまざまなソースからのデータが含まれる。ホストベースのシステムソースの例としては、ウイルス対策ログ、イベント ログ、syslog、プロセス監視ログなどがある。その他の有用な情報源としては、コンフィギュレーション情報（オペレーティングシステムやアプリケーションのバージョンなど）、ファイルシステムのリスト（完全なもの、特定のもの）、ユーザープロファイルやシステムやアプリケーションによる使用権限、ネットワークコンフィギュレーション設定やホストベースの通信サービス、永続サービスやスケジュールサービスのコンフィギュレーション、共有リソースの接続などがある。証拠の信頼性を確保し、必要に応じて捜査の過程を弁明するためには、科学捜査的に健全な方法でこれらのアーティファクトを収集することが重要である。

スウィートディアスカバリーは EnCase や AccessData のような一般的なフォレンジックツール [187] を使って実行されることが多いが、F-Response[188] のようなツールや、セキュリティコミュニティで共有されている無料のツールを使って実行することもできる [189]。**スウィートディアスカバリー**は、捜査官・調査

187 https://www.guidancesoftware.com/ and http://accessdata.com/solutions/digital-forensics/ad-enterprise
188 https://www.f-response.com
189 https://github.com/AJMartel/IRTriage

員が証拠を特定するのに十分な生データを収集することを目的としている。そのため、エンドポイントで実行され、抽出、変換、ロード（ETL）のために収集される最も単純なオペレーティングシステムのコマンドでさえ、この種のデータを提供することができる。ウイルス対策ソフトウェアやエンドポイント構成管理ソフトウェアは通常、次のようなデータの収集をサポートする。

- オペレーティングシステムや「ユーザースペース」ファイルのディレクトリの一覧出力（dir　や lsof）
- ネットワークの設定および構成（netstat、ipconfig/ifconfig、arp など）
- アクティブプロセスとそのリソース（tasklist または ps）
- ホストの構成の詳細（msconfig または ls）
- イベントログの詳細（wevtutil または cat）

証拠収集プロセスを漏斗の観点から考えると分かりやすい。漏斗の一番上は最も収集しやすいデータを表す（一掃）。漏斗が狭くなるにつれ、データ収集と分析の両方に、より多くの労力が必要となる。さらに、漏斗が狭くなるにつれてデータの精度（完全性とコンテキスト）が高まり、より綿密な捜査が可能になる。この段階的アプローチを下記の図 6-6 に示す。

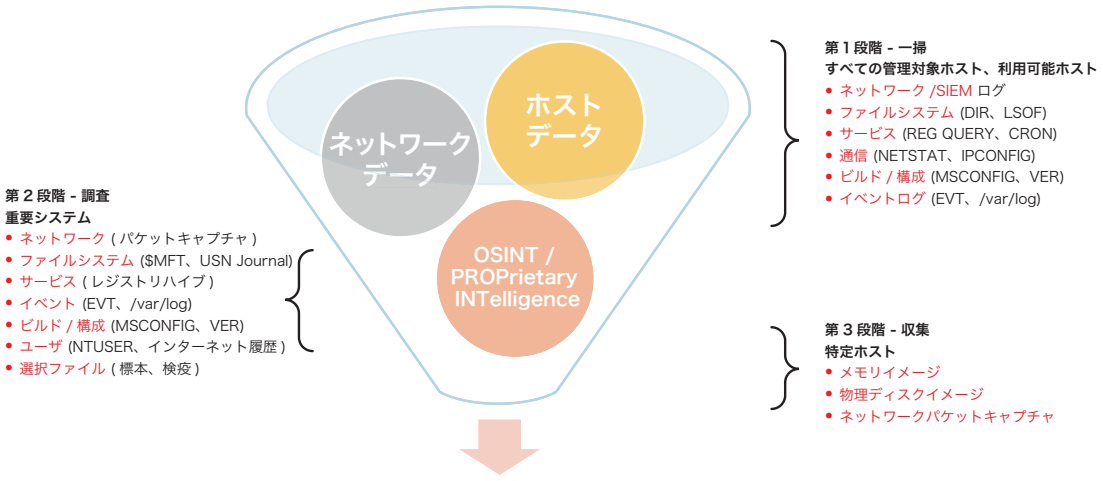


図 6-6. 証拠収集での段階的アプローチ

効率的な証拠収集プロセスでは、ETL データ分析技術を活用して、スケーラブルな証拠処理を可能にする。データベース内でデータを収集し相関させることで、関心のあるシステムを特定するために常に「ソースに戻る」のとは対照的に、偶然の成果物や指標を迅速に特定することができる。このプロセスを通じて、IoC が発見されて確認されると、同じ挙動を示した環境内の他のホストを探すために、データリポジトリを大規模に照会することができる。これにより、フィードバックまたは「OODA」ループ [190] が実現し、IoC とスキャンルールを継続的に追加および更新して、インシデントの範囲を徹底的に把握できるようになる。

一掃によってレビュー対象としてフラグが付けられたシステムは、ログファイル、ホストとサービスの構成設定と変更履歴、ファイルシステム リスト、揮発性システムデータ、ユーザー活動の詳細など、

190　観察、方向付け、決定、行動 – 計画、実行、確認、行動（PDCA）とは対照的

第5章で説明されているような重要なフォレンジックアーティファクトを収集することで、さらに詳しく調査することができる。下記の図6-7は、さらなる調査と収集の準備が整った一掃集計データの例を示している。

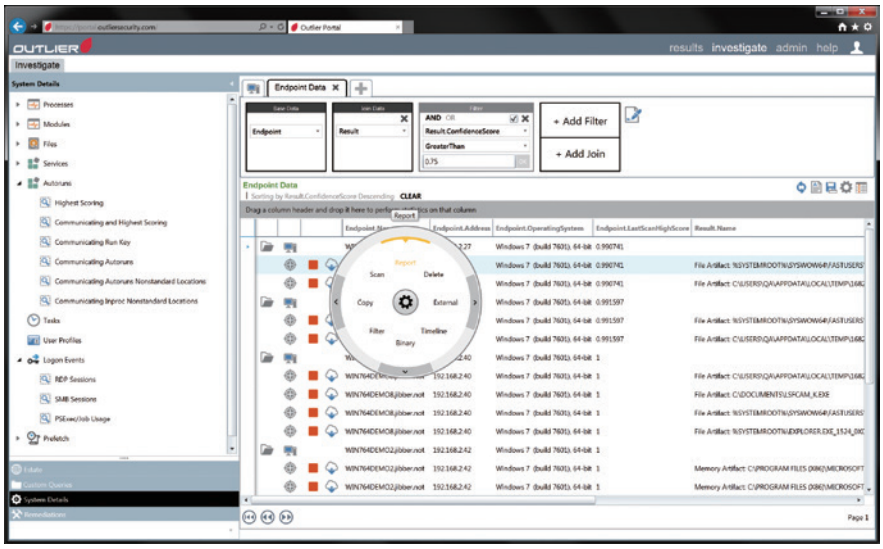


図 6-7a. 異常なセキュリティー掃による証拠の収集と集約

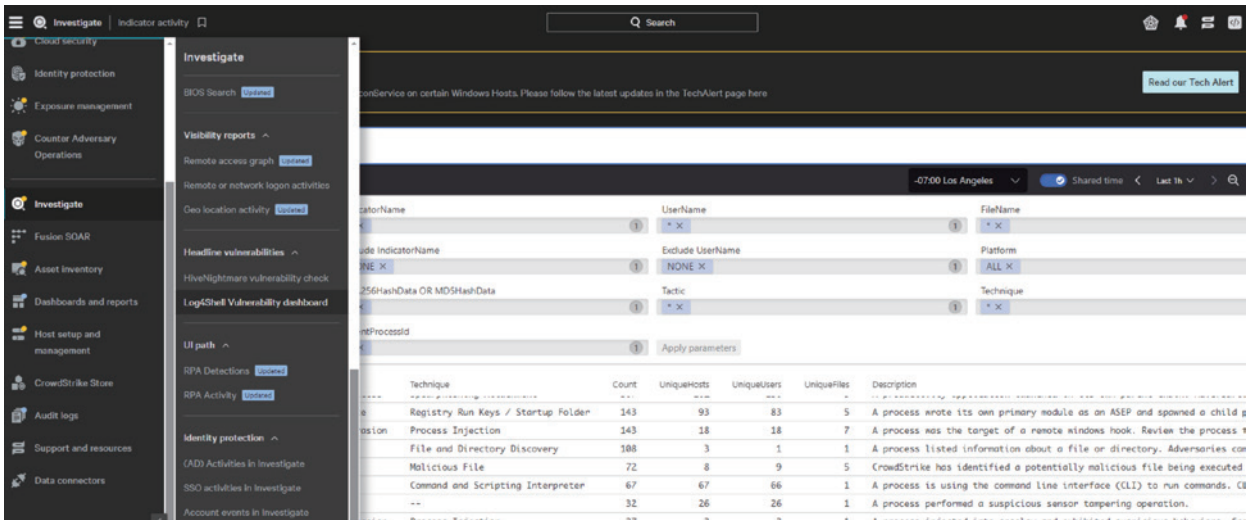


図 6-7b. CrowdStrike Falcon による証拠の収集と集約

手作業による証拠収集

スウィープ・ディスカバリー（一掃検知）アプローチを使用して調査対象のシステムが特定されると、犯罪の証拠を発見するために、構成と使用履歴に関する具体的な情報が必要になる場合がある。自動化されたエンタープライズツールやソフトウェアアプリケーションは証拠の収集と分析に役立つが、結論を導き出したり、法的および／または規制上の要件を満たしたりするには、体系的なアラートや包括的な証拠から得られる詳細が不十分な場合がある。調査対象のシステムが特定されたら、特定のアーティファクトを収集すべきである。証拠収集に関する組織または捜査・調査方針について、まず重要な判断を下さなければならない。

証拠分析員は、コンピュータから収集することのできるアーティファクトの分量にして1% 未満に対しおよそ 95% の時間を費やしている。一般的に、得られるアーティファクトは次のとおりである。

1. ネットワーク接続やアクティブプロセス（およびそのリソース）のように揮発性のシステム情報
2. 揮発性のアクティブな物理メモリページ
3. ファイルシステムの内容（ファイル、プログラム、および履歴／ログを含む）
4. ハードウェア構成（ディスクボリュームや接続機器を含む）
5. ソフトウェア構成（オペレーティングシステムやエンタープライズ管理アプリケーション、ユーザアプリケーションを含む）

関連するアーティファクトは、メタデータまたはコンテンツ指向の取得方法のいずれかを使用して収集することができる。適切な方法は、捜査官・調査員が従わなければならない収集の方針や指示によって異なる。

メタデータ指向のデータ収集（すなわち、調査、第2段階）は、**証拠分析担当者**が95%の時間を費やす1% のアーティファクトに適用される。これは、ネイティブツールからファイル、ログコンテンツ、揮発性システム情報に関するメタデータを取得することに重点を置いている。このようなメタデータを評価する際の分析官の主な関心は、イベントの時系列とサイバー犯罪活動を説明する相対的証拠を特定することであるため、（特定のログ以外の）ファイルのコンテンツ自体は収集されない。たとえば、Microsoft Windows コンピュータ用のメタデータ指向の取得には、通常、以下のファイルが含まれる。

- $MFT と $UsnJrnl
- レジストリハイブ（システム、ソフトウェア、セキュリティ、およびSAM）
- ユーザー履歴（NTUSER.DAT、USRCLASS.DAT、およびインターネットエクスプローラー（INDEX.DAT）他）
- EVT/EVTX ログ（アプリケーション、セキュリティ、およびシステム）
- アンチウイルスログ
- 揮発性のシステムデータ（tasklist、netstat、arp、ipconfig、autorun のエントリ）

同様の情報は、Mac OSX、Linux、その他のオペレーティングシステムからもメタデータ指向の取得のために収集することができる。このような簡易に取得を行う主な理由は、捜査に役立つ十分な証拠を迅速かつ効率的に収集するためである。一掃検知の収集と同様に、この収集はエンタープライズツールで支援することができ、データベース分析による ETL は、一人一人のシステム分析者が利用できない証拠の偶然性や詳細を効率的に明らかにすることができる。

場合によっては、ポリシーまたは技術的なニーズにより、証拠の収集をサポートするために、より完全なコンテンツ指向の取得が必要になることもがある。この「第3段階」（つまり、収集）は、多くの場合、規制上の義務に基づく弁護士または組織のリスク管理ポリシーにより、完全なディスクイメージング（物理ハードドライブおよび場合によってはアクティブメモリコンテンツのビット単位のフォレンジックコピー）が要求される場合がある。その他の状況においては、追加的な技術分析またはコンテンツ解析を行うために、「メモリイメージ」を収集しなければならない場合がある。このような場合、リモートホストに接続できるエンタープライズフォレンジックツールセットを使用するか、コンピュータから物理的にイメージを収集する以外に選択肢はほとんどない。コンテンツ指向の収集は、特定の（そして限られた）スキル、ツール、時間、関連コストが必要となるため、リソースの割り当てという点で最もコストがかかる。一掃検知とメタデータ指向の証拠取得では、収集された企業情報の規模で ETL とデー

タ分析を採用できる。コンテンツ指向の取得では通常、取得されたイメージと分析は 1 対 1 の関係になる。

サイバー犯罪のスコープと影響を判断するためのこれらの段階におけるコストや効率は様々であるため、組織は、経験する可能性のあるサイバー犯罪の種類に応じて、証拠提出に関する規制や法的義務など、管轄区域の要件を見直す必要がある（第 2 章参照）。これらの要件は、利用可能なスキル、知識、経験、ツールと照らし合わせて検討されるべきである。要件とリソースの組み合わせにより、知的で効率的な証拠収集のための指針となるポリシーと手順が形成されるはずである。

各業界や法執行機関におけるベストプラクティスには、以下のようなものがある。

1. 異常な活動のパターン／IoC から潜在的なサイバー犯罪を警告するための体系的な収集の使用。
2. 企業のコンピュータと関連エンドポイントを定期的に一掃し、関心のあるシステムや異常なユーザー行動を発見する。
3. 証拠を調査するためのメタデータ指向のアーティファクトの手動取得。
4. ポリシーで要求される場合にのみ、サイバー犯罪の証拠の保全および／または調査のためにコンテンツ指向のアーティファクトを取得する。

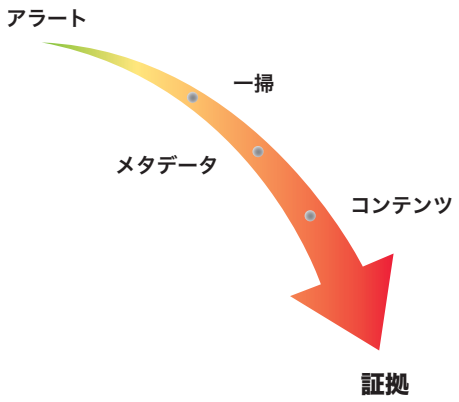


図 6-8. 証拠収集の手段

ネイティブツール

「手動収集」アプローチでは、ネイティブツールとサードパーティツールを使用して証拠を収集する。ネイティブツールは、管理者やユーザー（権限設定による）がコンピュータのサービス、構成、使用履歴に関する情報を照会できるオペレーティングシステム内のユーティリティを含んでいる。サードパーティのツールは同様の情報を提供できるが、そのツールが作られた設計目的に基づいて、コンピュータからのデータの独立したアーティファクトを関連付ける機能を持っている。ネイティブツールとサードパーティツールは、多くの場合コンパイルされたプログラムとしてスクリプト化された命令を使用して、オペレーティングシステムとファイルシステムの詳細への API 関数の呼び出しを利用する。偶然ではないが、マルウェアも API 関数の呼び出しを使用して、リモートアクセス、プログラミング、情報アクセス、コンピュータの制御など、同様の機能目的を達成している。

一例としては、オペレーティングシステム情報収集ツールでは、PSAPI と NETAPI という 2 つの主要な API が一般的でよく使用されている。プロセスステータス（PS）API には、プログラムで使用できるネイティブ関数と、プロセスに関する情報のクエリが含まれている。例えば、下記の図 6-9 は、API 命令セットを含む「PSAPI.DLL」のリソース呼び出しを介して「TASKLIST.EXE」コマンドによって行わ

れる関数の呼び出しを示している[191]。

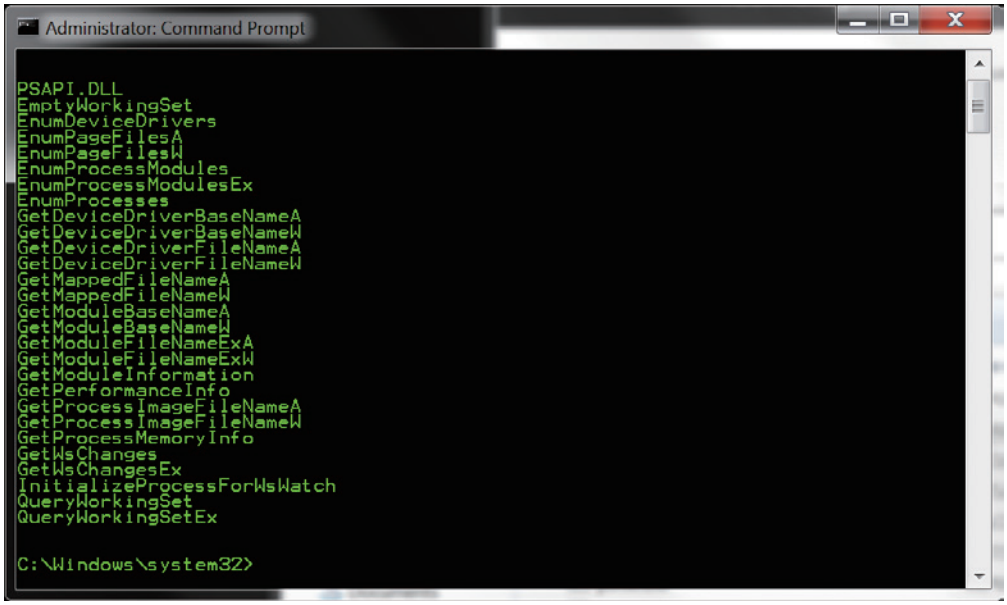


図 6-9. TASKLIST（PSAPI の使用）

ネットワーク（NET）API は、ネットワーク統計（NETSTAT.EXE）[192]、ネットワーク管理（NETSH.EXE）[193]、および使用詳細（NET.EXE）に対して同様の機能呼び出しを提供する。ここで説明したユーティリティはどのオペレーティングシステムにも同様の機能を持つものが存在し、ネイティブツールとサードパーティツールのどちらでも基本的な証拠収集に使えるようになっている。たとえば、下の図 6-10 に示す Google Rapid Response[194] インシデント対応ツールキットのソースコードは、プログラムが依存する「含まれている」リソースライブラリを詳述している。

```
934 lines (762 sloc)  27.6 KB
1  // Copyright 2012 Google Inc
2  // All Rights Reserved.
3  //
4  //
5  // This windows service installation code is inspired from the MSDN article:
6  // http://msdn.microsoft.com/en-us/library/windows/desktop/bb540475(v=vs.85).aspx
7
8  #include "grr/client/nanny/windows_nanny.h"
9  #include <shellapi.h>
10 #include <psapi.h>
11 #include <stdio.h>
12 #include <tchar.h>
13 #include <time.h>
```

図 6-10. サードパーティのツールで PSAPI を使用するコード例

NETSTAT などの一般的なユーティリティがなくても、経験豊富なシステム分析官は、図 6-11a と図 6-11b に示すように、簡単な方法で対象のシステム[195]から常に有用な情報を収集することができる。ただ

191 https://msdn.microsoft.com/en-us/library/windows/desktop/ms684884(v=vs.85).aspx
192 https://msdn.microsoft.com/en-us/library/windows/desktop/bb525390(v=vs.85).aspx
193 https://msdn.microsoft.com/en-us/library/windows/desktop/aa370675(v=vs.85).aspx
194 https://github.com/google/grr
195 Note that the addresses are displayed as reverse HEXIDECIMAL format（0100007F = 127.0.0.1）

し、32 ビットおよび 64 ビットのプロセス情報、特にリソース（DLL と共有オブジェクト）は、ネイティブツール（および多くのサードパーティツール）では同じようにアクセスできないことに注意することが重要である。収集された証拠の分析では、この点を考慮すべきである。

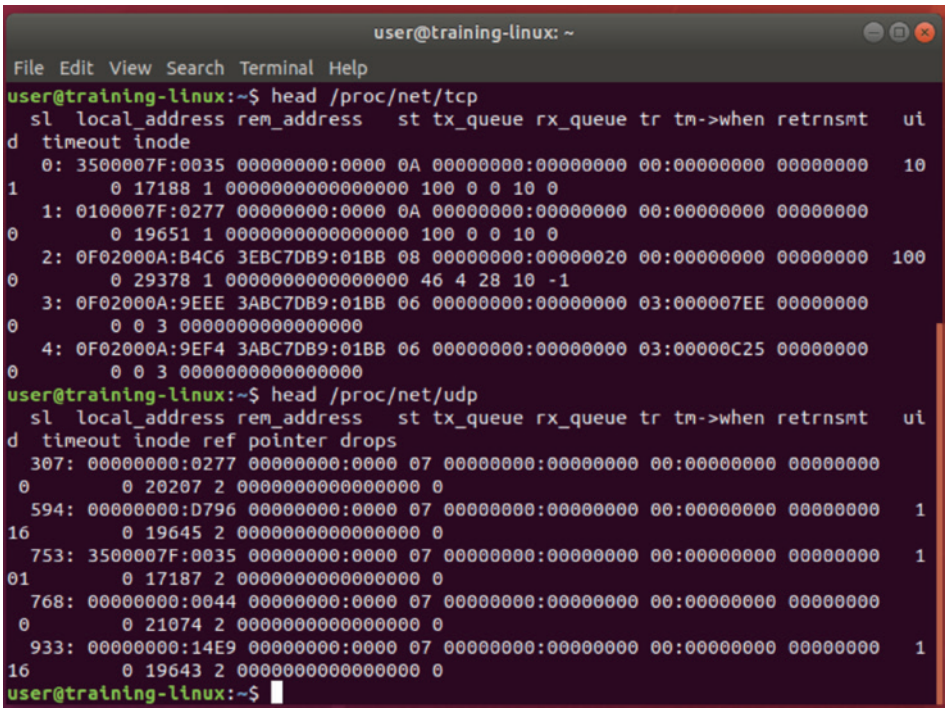


図 6-11a. Linux のネイティブ NET 統計（未加工）

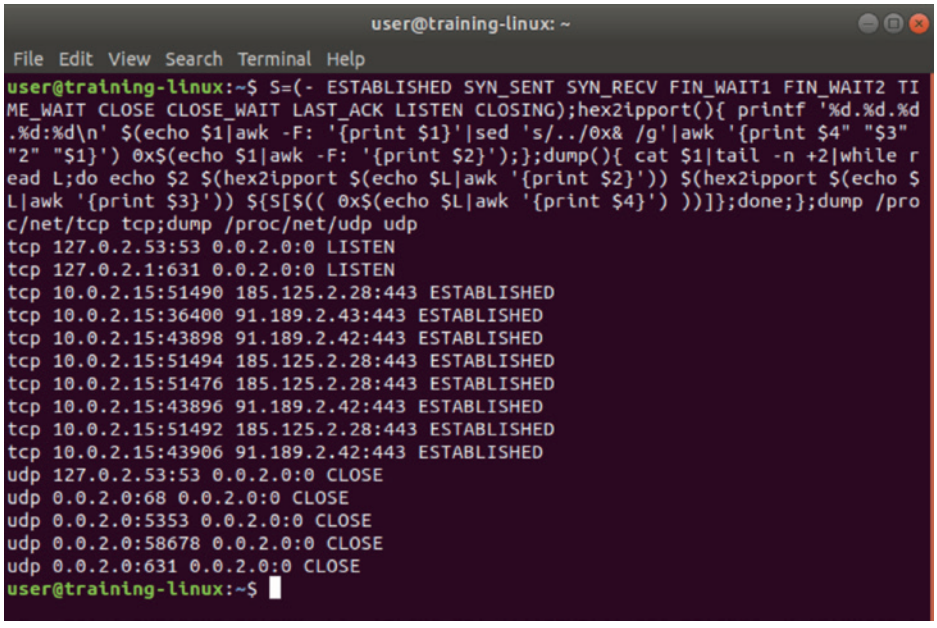


図 6-11b. Linux のネイティブ NET 統計（変換済み）

上述のとおり、NETAPI 情報はサードパーティツールからも呼び出すことが可能である。下記の図 6-12 では、Linux 用の Python スクリプトを使用して、PS 呼び出しからネットワーク接続統計を返している[196]。

196 https://github.com/da667/netstat/blob/master/netstat.py

241 lines (211 sloc) | 7.7 KB

```python
#!/usr/bin/python

import pwd
import os
import re
import glob

PROC_TCP4 = "/proc/net/tcp"
PROC_UDP4 = "/proc/net/udp"
PROC_TCP6 = "/proc/net/tcp6"
PROC_UDP6 = "/proc/net/udp6"
PROC_PACKET = "/proc/net/packet"
TCP_STATE = {
        '01':'ESTABLISHED',
        '02':'SYN_SENT',
        '03':'SYN_RECV',
        '04':'FIN_WAIT1',
        '05':'FIN_WAIT2',
        '06':'TIME_WAIT',
        '07':'CLOSE',
        '08':'CLOSE_WAIT',
        '09':'LAST_ACK',
        '0A':'LISTEN',
        '0B':'CLOSING'
        }

def _tcp4load():
    ''' Read the table of tcp connections & remove the header  '''
    with open(PROC_TCP4,'r') as f:
        content = f.readlines()
        content.pop(0)
    return content
```

図 6-12a. NETSTAT でネットワーク統計を得るためにサードパーティスクリプトで PS を使用しているコード例 (netstat.py)

```
user@training-linux: ~
File  Edit  View  Search  Terminal  Help

user@training-linux:~$ python netstat.py
['0:', 'systemd-resolve', '127.0.0.53:53', '0.0.0.0:0', 'LISTEN', None, None]
['1:', 'root', '127.0.0.1:631', '0.0.0.0:0', 'LISTEN', None, None]
['2:', 'root', '10.0.2.15:34762', '34.120.237.76:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['3:', 'root', '10.0.2.15:36452', '23.192.228.22:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['4:', 'root', '10.0.2.15:39428', '34.149.100.209:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['5:', 'user', '10.0.2.15:56684', '140.82.113.21:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['6:', 'root', '10.0.2.15:36174', '185.125.190.17:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['7:', 'user', '10.0.2.15:35738', '185.199.108.154:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['8:', 'root', '10.0.2.15:52992', '34.107.221.82:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['9:', 'user', '10.0.2.15:40864', '23.192.228.24:80', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['10:', 'root', '10.0.2.15:57994', '34.120.5.221:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['11:', 'root', '10.0.2.15:58196', '192.229.211.108:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['12:', 'user', '10.0.2.15:44718', '34.107.243.93:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['13:', 'root', '10.0.2.15:38852', '142.251.214.132:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['14:', 'user', '10.0.2.15:33536', '35.201.103.21:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['15:', 'root', '10.0.2.15:39432', '34.149.100.209:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['16:', 'root', '10.0.2.15:35826', '34.117.188.166:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['17:', 'root', '10.0.2.15:52990', '34.107.221.82:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['18:', 'root', '10.0.2.15:50672', '72.247.211.9:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['19:', 'user', '10.0.2.15:55426', '185.199.109.133:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['20:', 'root', '10.0.2.15:44704', '34.107.243.93:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['21:', 'user', '10.0.2.15:54264', '34.120.208.123:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['22:', 'root', '10.0.2.15:40658', '142.251.32.35:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['23:', 'user', '10.0.2.15:34050', '185.199.108.133:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
```

図 6-12b. NETSTAT でネットワーク統計を得るためにサードパーティスクリプトで PS を使用しているコード例 (netstat.py)

ネイティブツールまたはサードパーティツールを使用してホストにアクセスして証拠を収集する方法は多数ある。組織は、サイバー調査機能を計画するとき、あるいは外部に委託するときに、現実的な決断を下さなければならない。多くの場合、スキルとツールの間にはトレードオフがある。高価なツールは、安価で経験の浅いスタッフに取って代わることはできないが、高価で経験のあるスタッフは高価なツールを必要としないかもしれない。幸いなことに、経験の浅いスタッフでも、どのような情報をなぜ収集するのかを理解していれば、スタッフを支援するネイティブツールやサードパーティツールが数多くある。

● ネットワーク

Windows と Linux[197] のいずれのシステムにも、ネットワーク構成と接続の状態を照会するユーティリティが含まれている。下記の図 6-13 に示されているように、これには、ハードウェアのネットワークアドレス情報（ipconfig）に加え、サービスや状態（netstat）が含まれる。

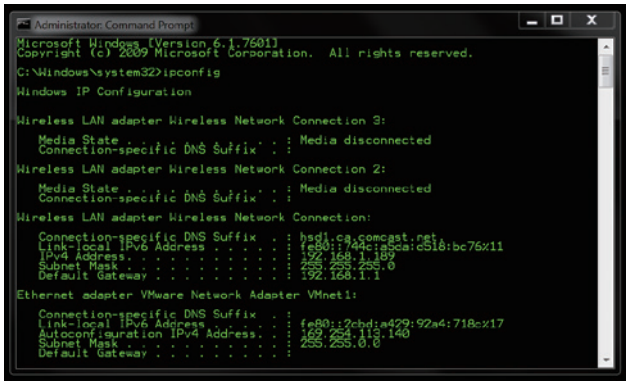


図 6-13. Windows の IPCONFIG

PowerShell などのツールは、証拠を探し出すための幅広いアーティファクトを収集するのに非常に優秀である（最近になり、PowerShell は Linux もサポートするようになっている[198]）。PowerShell はスクリプトやプログラミング言語ではないが、情報収集を含む自動管理タスクをサポートしている。PowerShell スクリプトが返すデータは、一か所に集めて異常がないかを分析するのに使える。PowerShell で収集できるデータは、オペレーティングシステムの詳細、インストールされているプログラム、実行中のプロセス、ネットワーク情報、開いているファイル、ネットワーク共有、ファイアウォールの設定などを含む。PowerShell は、C# などの任意の Microsoft.net Framework 言語を使用して拡張できるため、より複雑な PowerShell 機能を作成することが可能である。PowerShell 管理ユーティリティは、Microsoft が発行するパッチごとに更新されるため、一部の機能（図 6-15 に示す Windows8.1/2012 に同梱されている Get-NetAdapter など）ではスクリプトの作成が必要になる場合がある[199]。

197 Linux は、いくつかのUnixオペレーティングシステムやOSX（Apple）のほか、さまざまなモバイル、ネットワーク、さらにはDCS機器（DCU/RTUなど）にサービスを提供するオペレーティングシステムとも類似しているため、この章全体ではデモンストレーションの目的で使用されています。

198 https://blogs.msdn.microsoft.com/powershell/2015/05/05/powershell-dsc-for-linux-is-now-available/

199 https://blogs.technet.microsoft.com/heyscriptingguy/2014/01/15/using-powershell-to-find-connected-network-adapters/

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\e> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                    ------- ------       ----------             ---------
Bluetooth Network Conn... Bluetooth Device (Personal Area Netw...       5 Disconnected 5C-F3-70-74-6E-C0          3 Mbps
Ethernet 2                Intel(R) Ethernet Connection (2) I219-V       3 Disconnected 78-24-AF-D9-C8-4B          0 bps
VMware Network Adapte...8 VMware Virtual Ethernet Adapter for ...      19 Up           00-50-56-C0-00-08        100 Mbps
VMware Network Adapte...1 VMware Virtual Ethernet Adapter for ...      12 Up           00-50-56-C0-00-01        100 Mbps
Ethernet 3                Cisco AnyConnect Secure Mobility Cli...       4 Not Present  00-05-9A-3C-7A-00          0 bps
Ethernet                  Realtek PCIe GBE Family Controller          13 Up           78 24 AF 47 71 59          1 Gbps


PS C:\Users\e>
```

図 6-14. Windows PowerShell の Get-NetAdapter

アクティブプロセスに関するネットワーク統計は、関連するサービス構成を特定するのに非常に便利である。捜査官・調査員が利用できる簡単なテクニックは、下記の図 6-15 と図 6-16 に示すように、プロセス識別子（PID）により NETSTAT と PS（TASKLIST または LSOF）出力を関連付けることである。マルウェアは、svchost.exe や dllhost32.exe などの正規のサービスプロセスをフックすることが知られているため、関連する出力に開いているファイルを含めることも有効である。

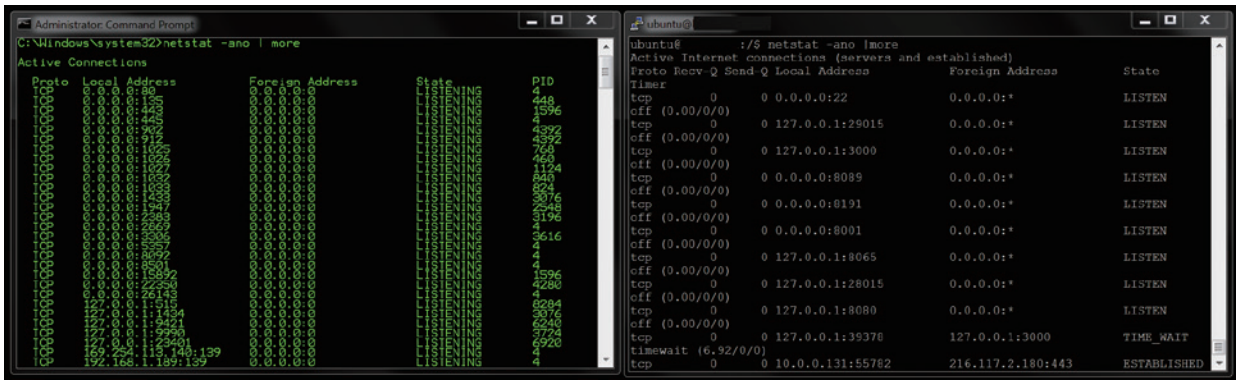


図 6-15. Windows と Linux の netstat -ano

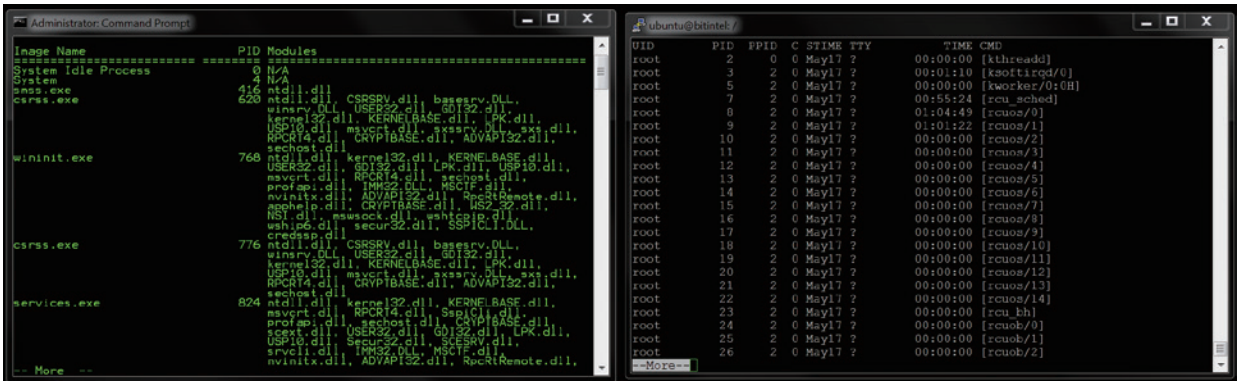


図 6-16. Windows の tasklist /m と Linux の ps -df

もう 1 つの（より単純な）手段としては、図 6-17 に示されているように、ネットワーク接続の情報別にプロセス ID を表示する方法がある。

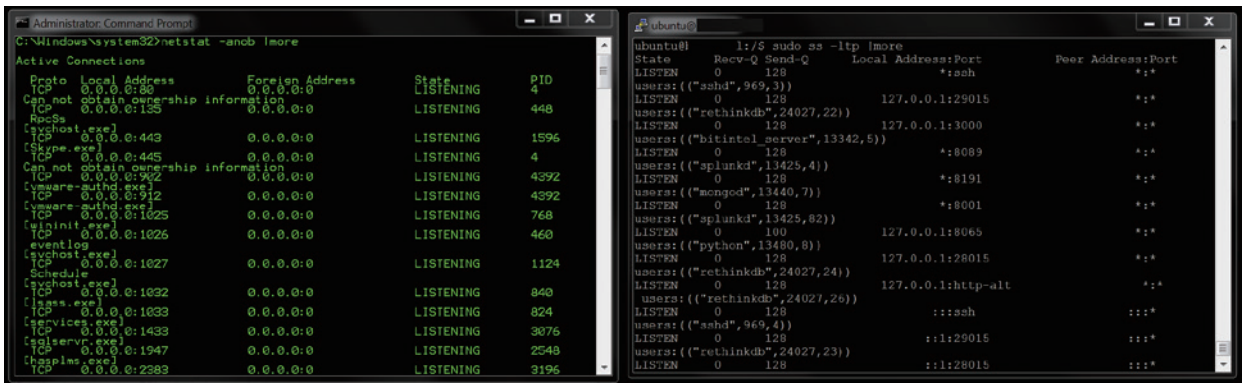


図 6-17. Windows の netstat -anob と Linux の ss -ltp

ネットワークパケットキャプチャから得られる情報も、証拠を調べるのに非常に役立つアーティファクトである。下記の図 6-18 に示されているように、Linux システムには「tcpdump」と呼ばれるユーティリティが含まれており、これを使えば指定したインターフェース上のネットワークトラフィックを収集できる。この収集をテキストエディタや「Wireshark」[200] などのツールで分析して、ネットワーク通信を調査することができる。

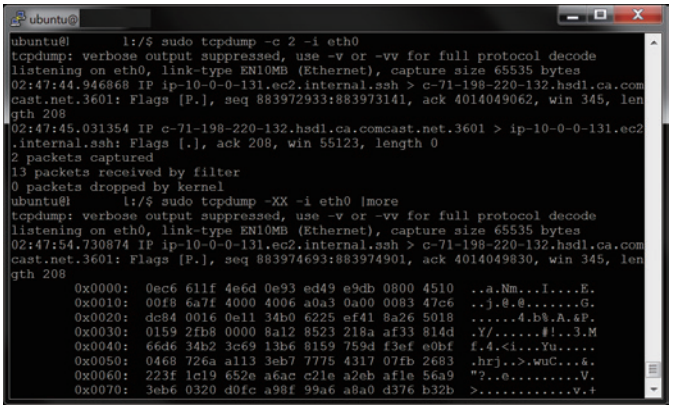


図 6-18. Linux の tcpdump

Windows も同様のユーティリティ（NETSH）があり、プロセスや関連情報を含むネットワークサービスと設定に関するネットワーク情報をオンデマンド（またはスケジュールどおり）で収集できる。下記の図 6-18 に示されているように、Windows のパケットキャプチャは、「ETL」（イベントトレースログ）ファイル形式や生データを圧縮した形で格納している CAB ファイル形式の他、独自の XML（Extensible Markup Language）形式で保存可能となっている。図 6-20 に示されているように、XML ファイルは任意の XML リーダーで開けるが、Microsoft はアクティビティファイルをレビューするためのユーティリティ[201] も無料で提供している。

200 https://www.wireshark.org/
201 https://www.microsoft.com/en-us/download/details.aspx?id=44226

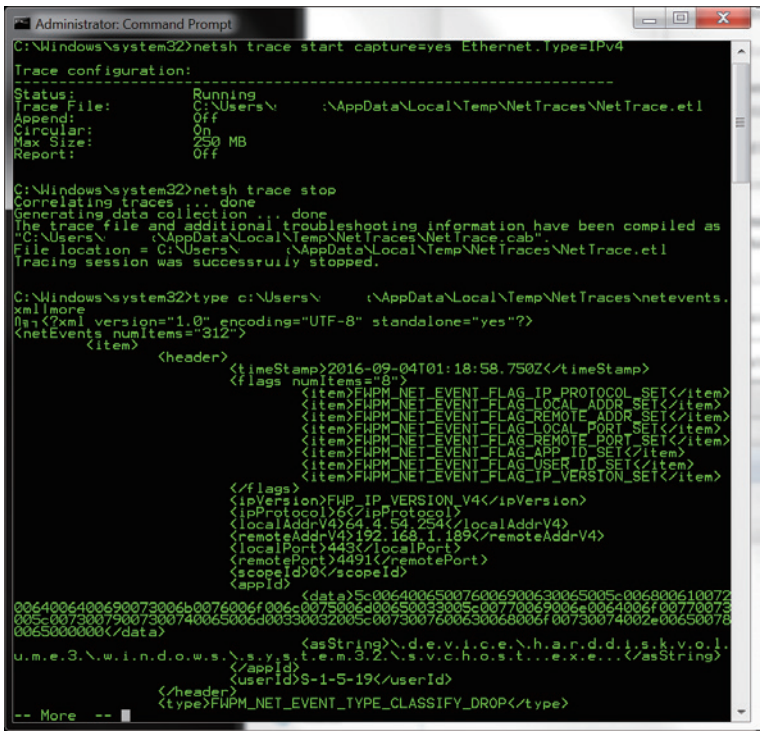


図 6-19. Windows の netsh trace

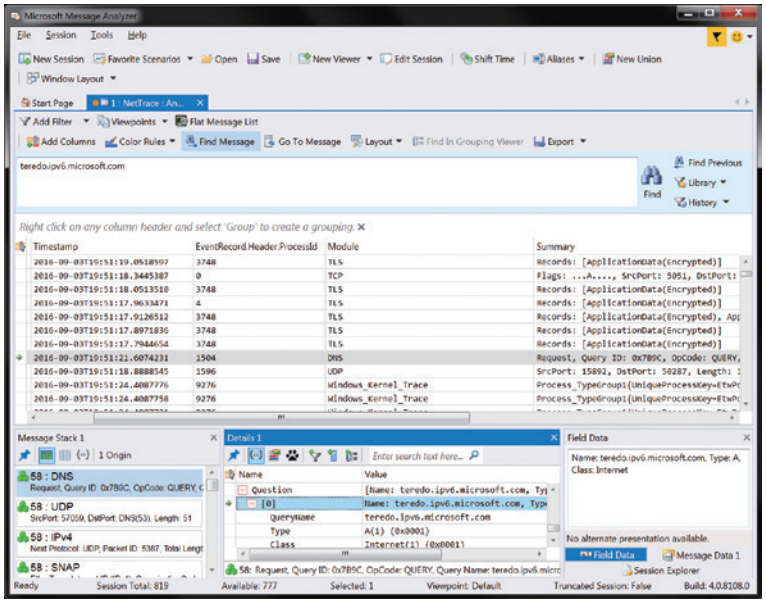


図 6-20a. Microsoft Message Analyzer でトレースログを開いているところ

Windows の NETSH Trace ユーティリティは Windows 10 のリリースで廃止され、「PKTMON」という新しいユーティリティがリリースされた。pktmon が実行されると、デバイス上のすべてのネットワークインターフェイス上のすべてのパケットを PktMon.etl というファイルに記録し、パケットの最初の 128 バイトだけを記録する。パケット全体と特定のイーサネットデバイスからのものだけをログに記録するには、-p 0（パケット全体をキャプチャ）と -c 13（ID が 13 のアダプターからのものだけをキャプチャ）の引数を使うことができる。キャプチャを停止すると、レビュー用にログファイルが ETL 形式で作成される。適切なビューア（Microsoft Network Monitor）または ETL コンバータツールが必要である。

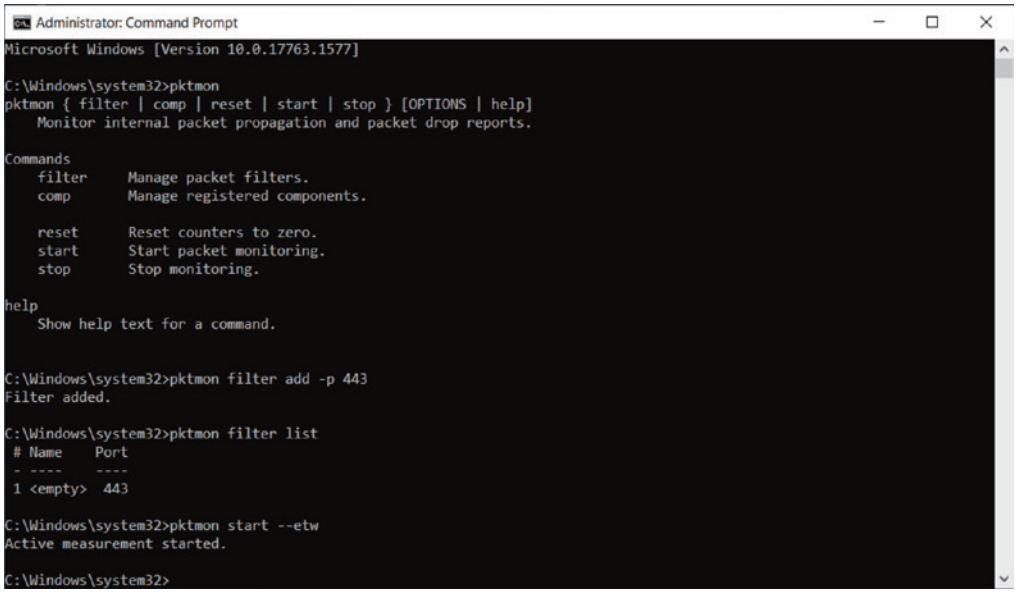


図 6-20b. Microsoft PktMon.exee

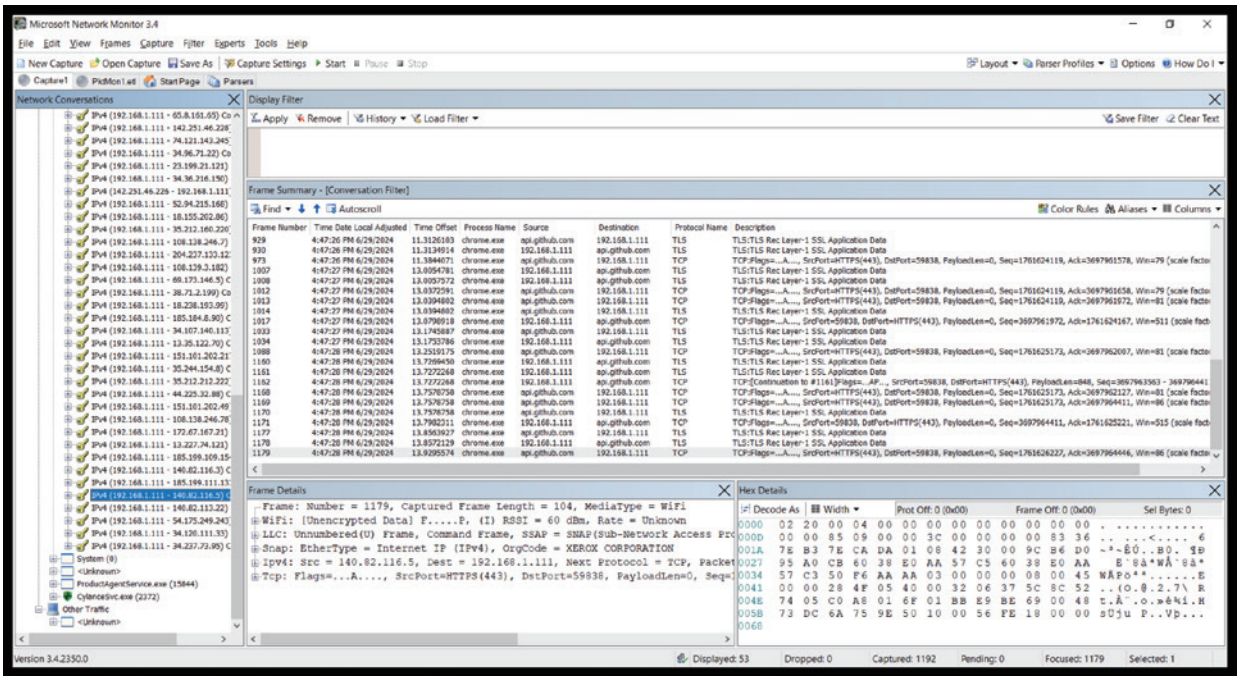


図 6-20c. PktMon.etl の Microsoft ネットワークモニター変換

●ホストのメタデータ

すでに説明したように、メタデータとは「データに関する情報」である。ファイルのコンテンツ自体は含まれないが、種類、作成者、編集者、作成日時と変更日時（または削除日時）、管理権限、共有履歴、およびアプリケーション、構成、使用履歴などのシステムとサービスに関する関連情報などの内容に関する情報が含まれる。メタデータは、コンピュータがどのように構成され、どのように使用されてきたか、あるいはサイバー犯罪とどのように関連しているかを捜査官・調査員が理解するのに役立つため、収集することが重要である。

ホストメタデータの最も単純な例は、上記で NET および PSAPI ユーティリティを使用して示した。「TASKMGR」、「MSCONFIG または MSINFO32」、「SCHTASKS」、「AT」、および「REG（QUERY）」など、他の多くの同様のツールは、Windows コンピュータから簡単に収集できる重要なメタデータ

アーティファクトを提供する。Linux や mac OS X にも同様のユーティリティが存在する。すでに説明したように、これらのユーティリティは基本的に、ネイティブツール（PowerShell、.NET、VBScript、AutoIT、BASH、AWK など）を使用した API とスクリプトを活用して設計されたタスクを実行し、同じタスクを実行できるだけでなく、捜査官・調査員の ETL 形式のニーズに役立つカスタム出力も可能にする。

捜査官・調査員は主にファイルのメタデータに興味を持つであろう。保存場所における各ファイルの作成、変更、最終書き込み、削除の詳細に関するファイルシステム履歴（およびファイルに対する権限を持つユーザーを管理する属性）は、コンピュータの重要な使用（または誤用）履歴を特定する上で重要である。Windows では、「DIR」コマンドから一部の情報を提供できるが、出力はコマンドのフラグに制約されており、「システム情報」（SI）の日付／時刻のみを返す。この日付／時刻は、ファイル作成日を変更するためにマルウェアがよく使用するユーティリティでは変更されない、より情報量の多い「ファイルシステム注記」（FN）の日付／時刻とは異なる。PowerShell は、より完全な詳細を提供することができ（下記の図 6-21 を参照）、Visual Basic スクリプトは、FileSystem（FS）API から情報を返すことができる。

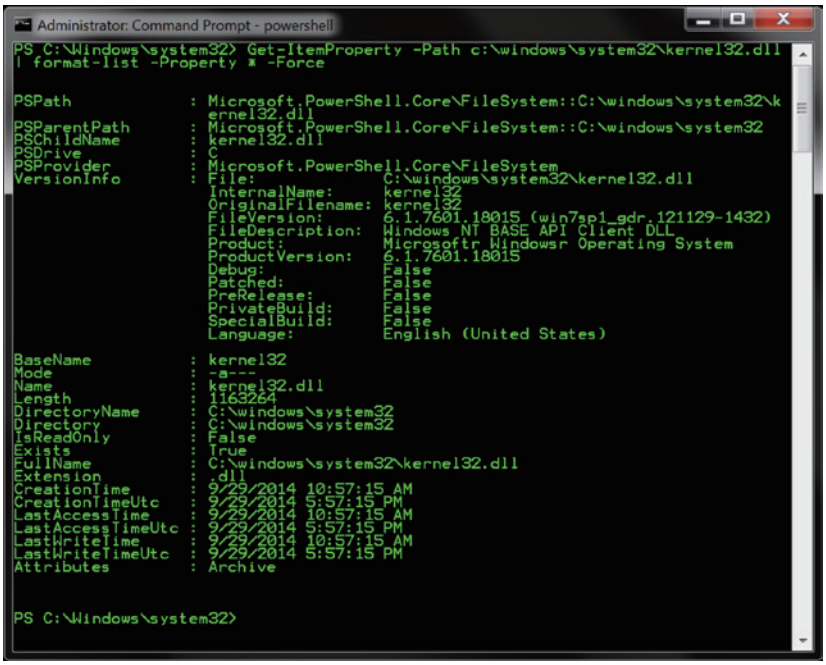


図 6-21. Windows PowerShell のファイルシステムメタデータ

Linux および macOS X からも同様のメタデータを得られるが、一致するアーティファクトの詳細を収集するにはいくつかのコマンドを組み合わせる必要がある。「stat」コマンドを実行すれば「ls-l」と同様にファイルに関する基本的なメタデータを得られるが、いくつかのメタデータの詳細をひとつのコマンドで返す機能 [202] をプログラムすれば、証拠を収集するのに活用できる。Linux メタデータのスナップショットについては、下記の図 6-22 を参照。

202 http://superuser.com/questions/554291/viewing-extended-file-properties-via-command-line-in-linux

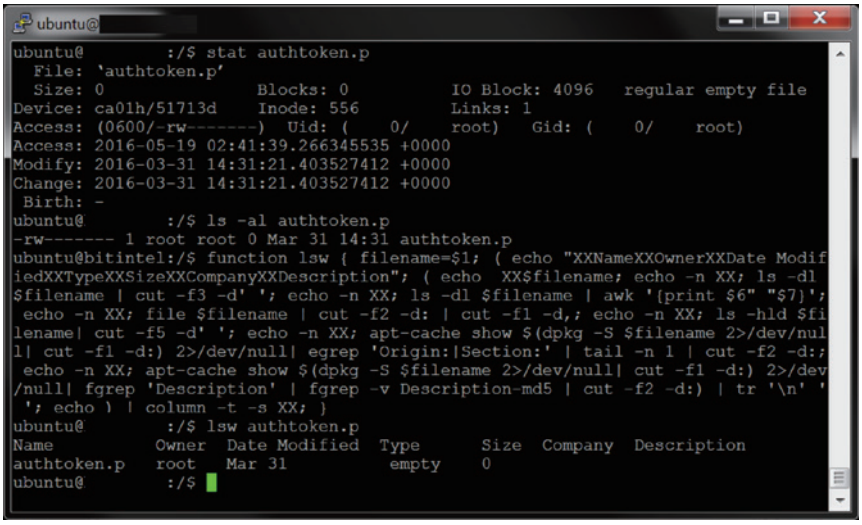


図 6-22. Linux (Ubuntu) の lsw メタデータ

Windows には「Windows Management Instrumentation Command-line」(WMIC)[203] と呼ばれるレガシーユーティリティも含まれている。WMIC コマンドは、ハードウェア、ネットワーク、アプリケーションの構成や関連する詳細など、システムに関する豊富な詳細情報を返すことができる。たとえば、「wmic startup」コマンドを使うと、コンピュータの再起動時に自動実行されるよう設定されているコマンドやプログラムが返される。PowerShell、WMIC、および多くの Windows コマンドを使用して、リモートホストにアクセスし、情報を収集することもできる。

●ホストのファイルとコンテンツ

ファイルのコンテンツが証拠として信頼できるよう、その整合性を維持することが重要である。標準的な「コピー」ユーティリティは、署名の詳細(暗号ハッシュ値を含むメタデータ)を変更するため、証拠収集のためにファイルをコピーする場合は避けるべきである。幸いなことに、Linux は、ほぼすべてのサードパーティ製デジタルフォレンジックユーティリティの基礎となる、基本的なフォレンジックディスクイメージングユーティリティを含んでいる。コピー機能は、メタデータプロパティを保持しない Windows の「COPY.EXE」プログラムと同じ名前なので、やや紛らわしい。逆に、Windows の「ROBOCOPY.EXE」および「XCOPY.EXE」コマンドは、API を適切に利用する。そのため、一般に、Linux では「dd」を、Windows では「ROBOCOPY /DATSOU」を使用することが推奨される(下記の図 6-23 を参照)。転送可能性のために、ファイルは圧縮する必要があり、ファイルが収集されるたびに暗号ハッシュ署名を計算して文書化する必要があることに留意する。

203 http://ss64.com/nt/wmic.html

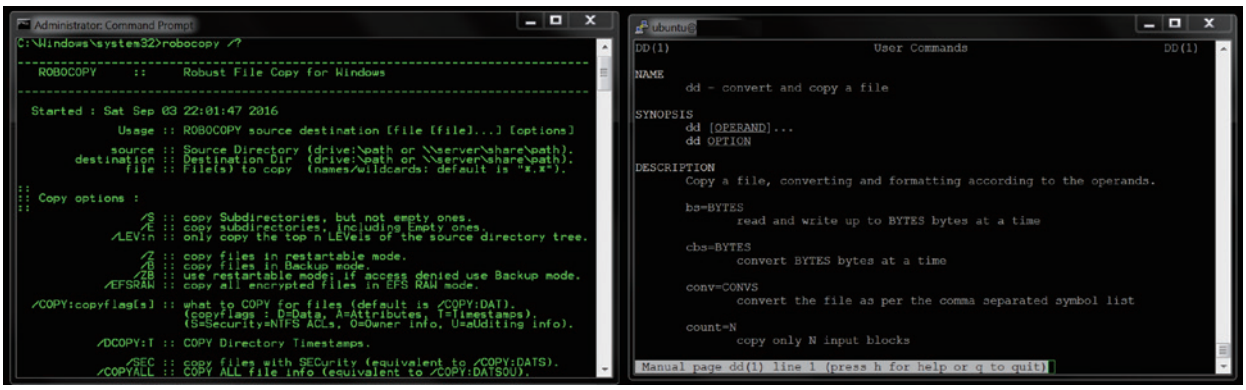


図 6-23. Windows の robocopy と Linux の dd

特定のアーティファクトとサイバー犯罪との関係を確かめる上で重要な内容を含むある種のファイルは、システム操作によってロックされる可能性があり、コピー操作ではアクセスできなくなる。これには、「inode」（属性とディスクブロック位置）によるファイルのインデックスを含むマスター／ジャーナルファイルシステム情報が含まれる。これまでに紹介したコマンドを使えばロックされたファイルから情報を解析できる他、robocopy または dd コマンドでその他の必要な作業も行える。ロックされたファイルシステムのログ、レジストリのハイブ、ユーザー設定／履歴ファイルなど、特にメタデータアーティファクトの収集には、ネイティブコマンドの代わりに有用なサードパーティ製のフォレンジックコピーユーティリティを使用する必要がある。これについては、後述の「サードパーティツール」のセクションで詳しく説明する。

●ログ

アプリケーションの多くは、役に立つログをさまざまな場所に作成している。これらのログは、独自のフォーマットである場合もあれば、「正規化」された（テキストや XML などの）フォーマットである場合もある。サードパーティアプリケーションのログファイルは「.LOG」または「.DB」を拡張子に使用することが多い。あるいは、Linux または類似オペレーティングシステムの場合は「LOG」という単語が名前に使われている。しかし、Windows のログファイルは、「Event」（EVT/EVTX）または「Data」（DAT）の拡張子とフォーマットを使用する。これらのファイルは、データファイル用の「REG」やイベントログ用の「WEVTUTIL」などのネイティブツールで抽出することができる。ネイティブツールで稼働中のオペレーティングシステム上のログファイルから情報を収集する場合は、グラフィカルアプリケーション（Windows イベントビューアまたは RegEdit（下記の図 6-24 を参照）を利用してデータを転送可能なフォーマットにエクスポートするか、同じ結果を達成するために適切なコマンドまたはスクリプト命令を使用する必要がある。

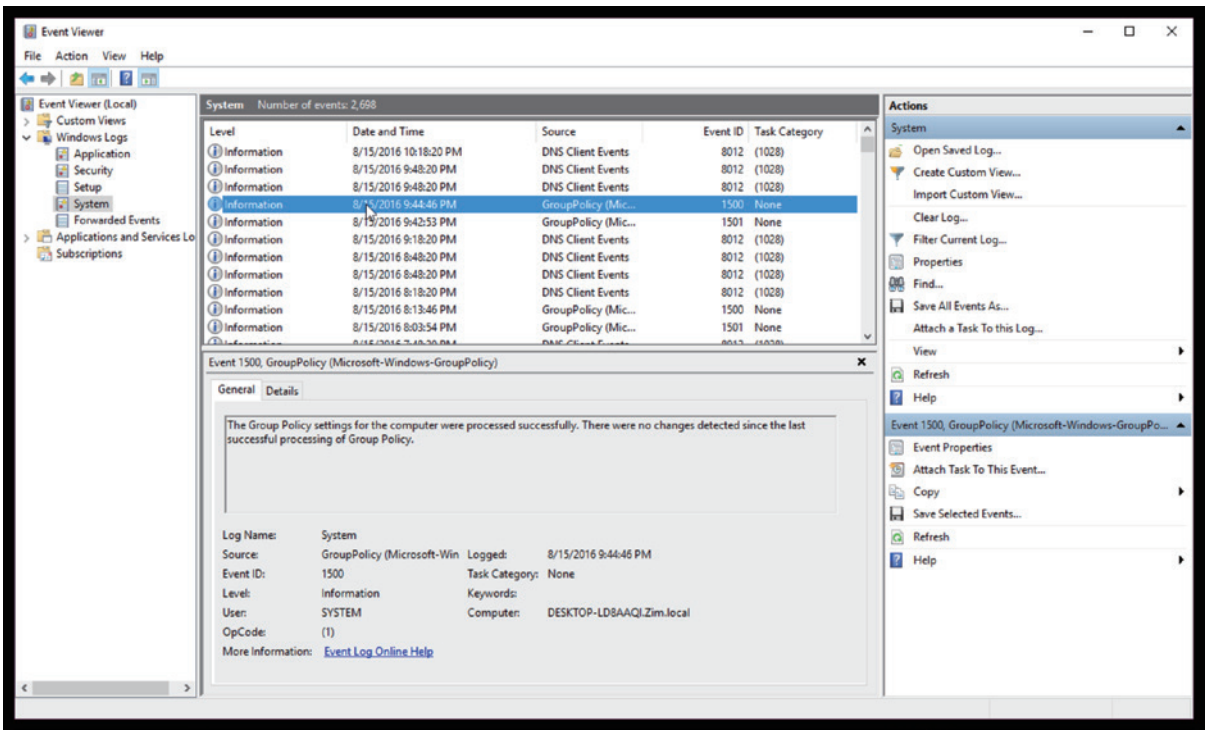


図 6-24. Windows のイベントビューアー

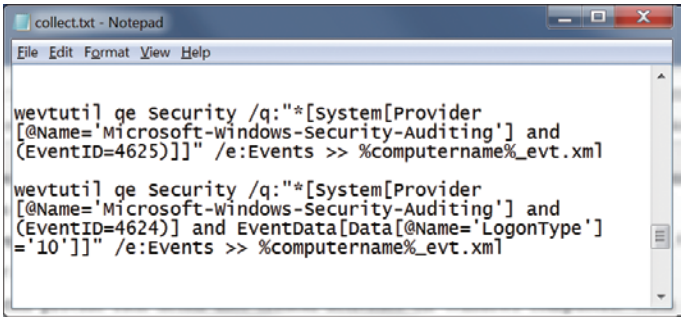


図 6-25. Windows の WEVTUTIL クエリユーティリティ例

通常、Linux の場合は標準テキスト形式で /var/log にログが保存される。単純な「grep」または「cat」コマンドでログの詳細を閲覧できる他、Linux では使用中のログファイルもコピーが可能である。

Windows レジストリのデータファイルには広範な情報が含まれているが、分析官が時系列を決定するのに十分なリテラルデータを含むように収集するのは困難な場合がある。レジストリのクエリまたはエクスポートコマンドを使用すれば、下記の図 6-26 および図 6-27 に示されているように、サービスの構成やインターネットの使用履歴など、有益な情報が得られる。

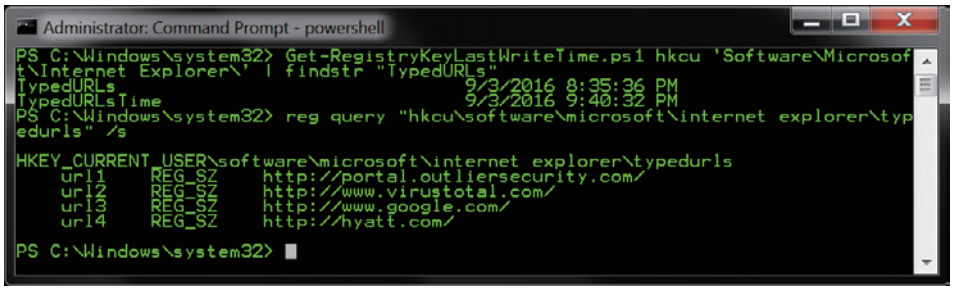


図 6-26. Windows の TypedURLs（履歴）

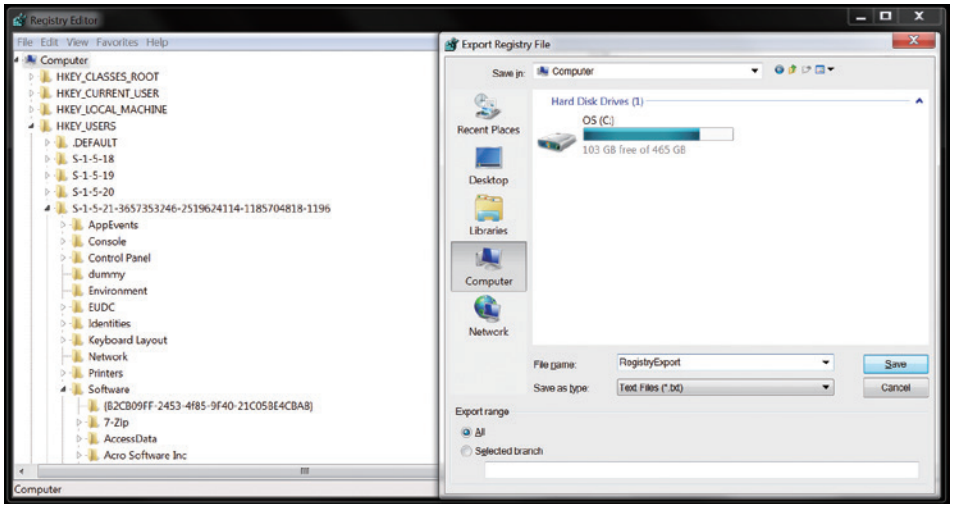


図 6-27. Windows の REGEDIT によるエクスポート

日時情報の抽出には、やや手間がかかる。PowerShell のスクリプトは便利なツール[204]で、すでに述べたように、Windows ネットワーク内のローカルまたはリモートのホスト情報を収集できる。

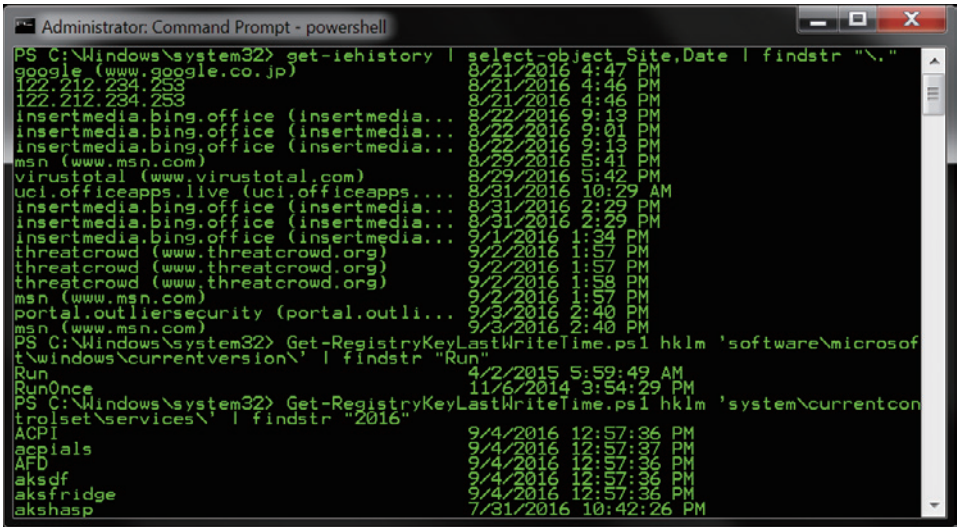


図 6-28. Windows PowerShell の例

Windows7 がリリースされて以来、Windows で PowerShell が標準化され（以前のバージョンでも利用可能だったが、オプションのインストールのみ）、Linux をサポートするために最近リリースされたことで、オペレーティングシステムのネイティブ機能を使用した多くの有用な証拠収集方法が作成された。「PSRecon サフィックス」と「Get-Memory-Dump サフィックス」が 2 つの良い例である。

PSRecon[205] は上述のネイティブテクニックのいくつかを使用し、ローカルまたはリモートのコンピュータからホスト情報を収集する。これはインシデント対応用に設計されているが、効果的な手動収集ユーティリティでもある。分類上はサードパーティツールであるが、「Apache（アパッチ）」ライセンス下でフリーソフトウェアとしてリリースされている[206]。証拠収集にネイティブツールをどのように使う

204 https://gallery.technet.microsoft.com/scriptcenter/Get-RegistryKeyLastWriteTim-63f4dd96 and https://richardspowershellblog.wordpress.com/2011/06/29/ie-history-to-csv/
205 https://github.com/gfoss/PSRecon/blob/master/psrecon.ps1
206 https://tldrlegal.com/license/apache-license-2.0-(apache-2.0)

かについて、非常に役立つ詳細が提供されるスクリプトである。下記の図 6-29 を参照。

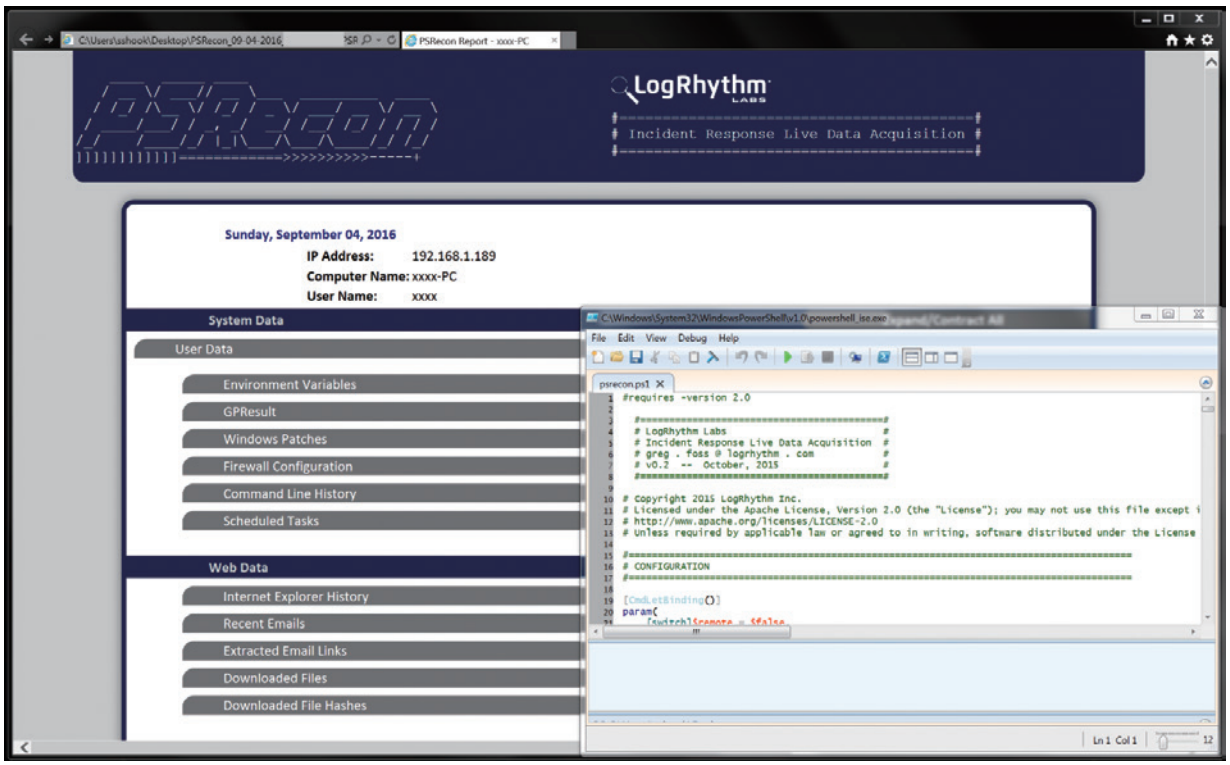
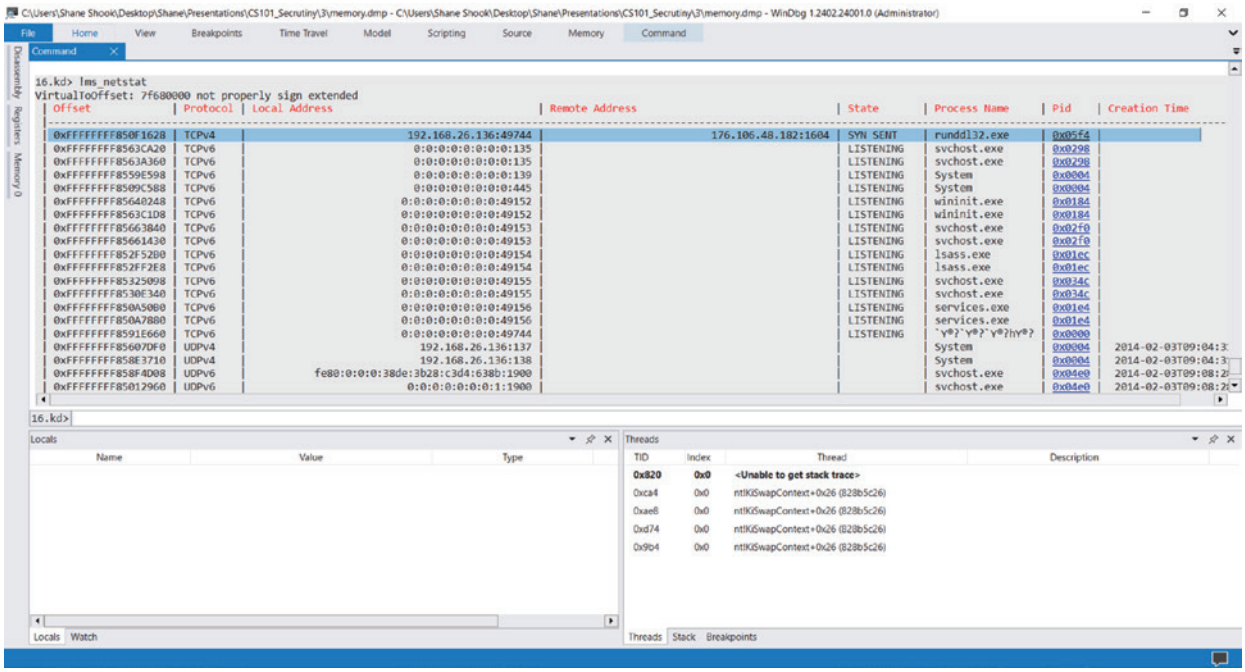


図 6-29a. PSRecon

Get-Memory-Dump[207] は Microsoft がリリースしたモジュールで、Windows コンピュータの稼働中メモリから Windows のクラッシュダンプ形式による取得が可能となる。Windows デバッガ（WinDBG）[208] を使ってダンプ・ファイルを確認したり、Volatility[209] のようなサードパーティ製ツールを使って、アクティブなプロセス情報、ネットワーク情報、ユーザー履歴、開いているファイル、サービス構成などの情報をメモリダンプから抽出したりすることができる。これらのメタデータと実際のファイル内容（取得の際にメモリ内に読み込まれている場合）は、PowerShell を使えばローカルまたはリモートのコンピュータから簡単かつ包括的に収集できる。Linux にも、/dev/（crash または mem）内にメモリダンプファイルを作成する同様の方法が存在する。使用する前に、これらのコンセプトをテストすることをお勧めする。

207 https://gallery.technet.microsoft.com/scriptcenter/Get-MemoryDump-c5ab38d8
208 https://msdn.microsoft.com/en-us/library/windows/hardware/ff539316(v=vs.85).aspx
209 http://www.volatilityfoundation.org/#!releases/component_71401



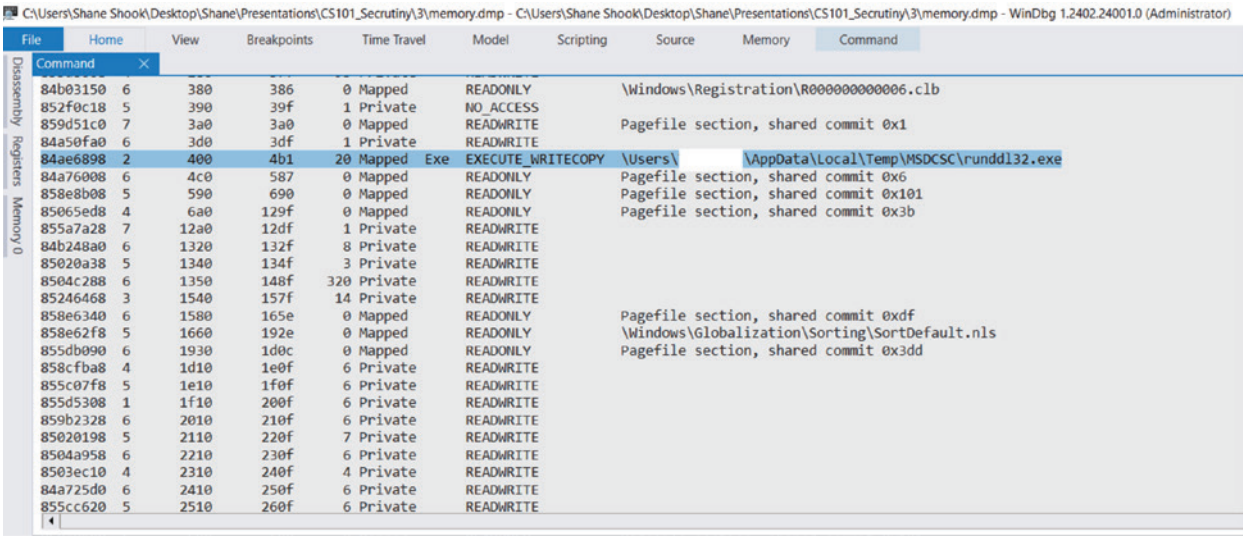


図 6-29b. WinDBG（メモリダンプ解析用に SwishDbgExt.dll[210] を使用）

サードパーティ製ツール

上述したように、ネイティブツールは、サイバー犯罪の証拠を収集する際に、多くの偶発的なアーティファクトを容易に集めることができる。収集を実行する証拠分析官が API をどこで、いつ、どのように効果的に使用するかを理解していれば、すべてのエンドポイントに存在するスクリプトユーティリティを使用してネイティブオペレーティングシステム API を活用することで、集中的な収集を実現することもできる。アーティファクトや証拠を収集するこれらのネイティブな方法の代わりに、同じ（または同種のパッケージの）API を活用する多くのサードパーティツールは、証拠収集を簡素化することができる。

210 https://github.com/MagnetForensics/SwishDbgExt

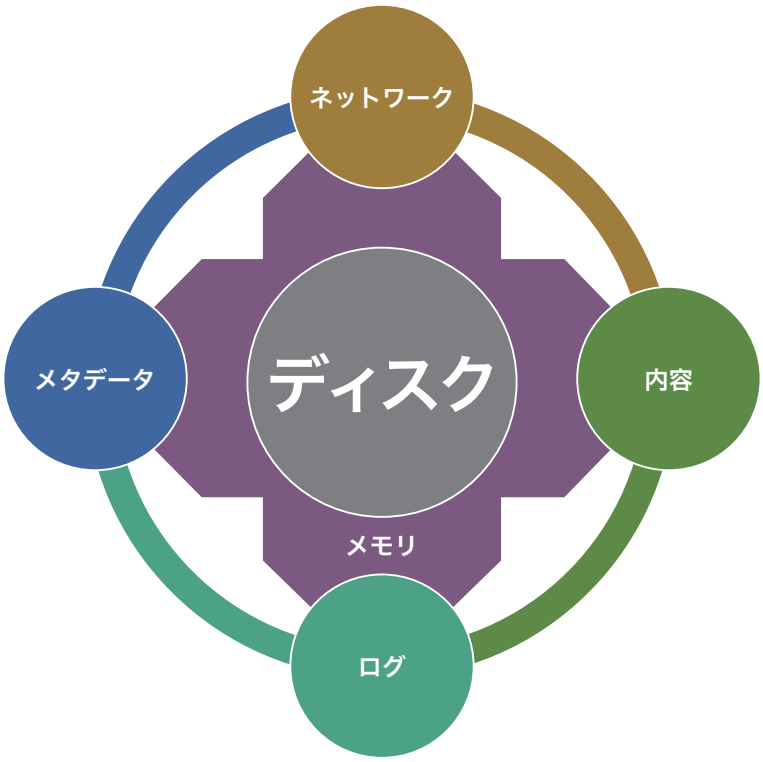


図 6-30. 捜査官・調査員が収集するもの

サードパーティのツールは、多くの場合、スピード、利便性、および不具合修正や機能リクエストなどのコミュニティ利用の利点を提供する。本項では、調査において一般的に使用され、必要に応じて法的手続きにおける証拠を作成するのに適していると思われるサードパーティツールの例をいくつか示す。

●ネットワーク

ネットワーク情報は、NetworkMiner[211]、nmap[212]、tcpview[213]、WireShark[214] などのツールによって収集できる。「Network Mapper」(nmap) は、アドレスまたは範囲によってホストまたは指定されたネットワークをスキャンできるオープンソースツールである。Nmap はネットフローを生成しないが、外部で識別されたサービス構成とホスト情報を一覧表示する。Nmap は、コマンドラインからアプリケーションとして、またはさまざまなオペレーティングシステムでグラフィカルに実行される。下記の図 6-31 を参照。

211 https://www.netresec.com/?page=NetworkMiner
212 https://nmap.org/
213 https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx
214 https://www.wireshark.org/

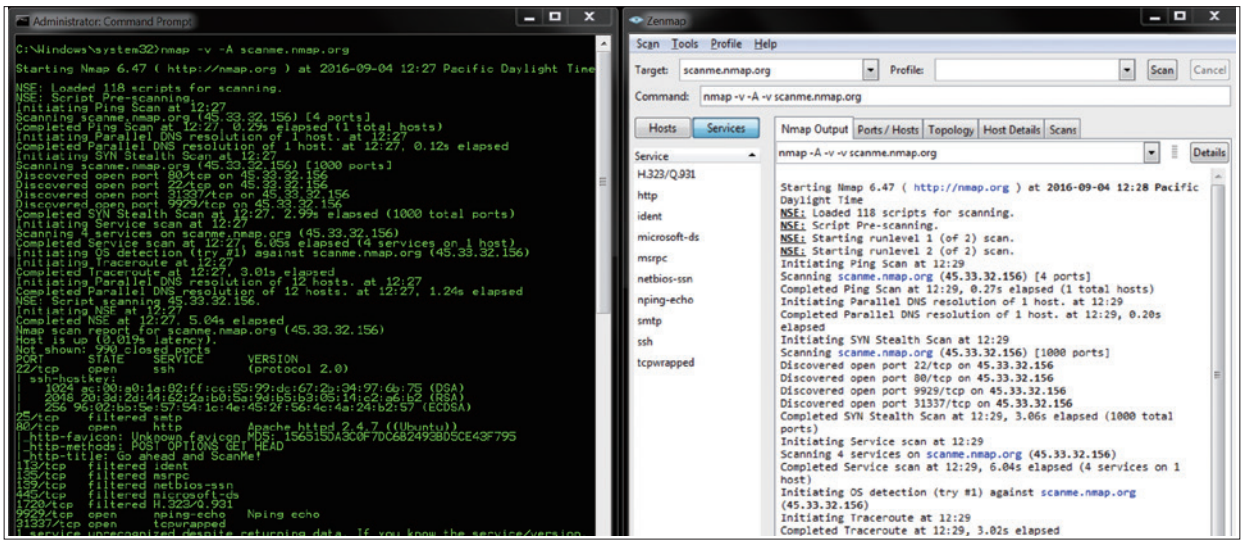


図 6-31. nmap

TCPView は Windows および Linux に含まれているプロセスやネットワーク API ツールを組み合わせたようなツールである。これは、2016 年に Microsoft が自社製品に追加したツールの中でも非常に人気の高い「SysInternals Suite」[215] の著者であるマーク・ラシノビッチによって書かれたものである。TCPView は BSD Unix の同名のユーティリティに似ており、Solaris やその他の Unix ベースのオペレーティングシステムにも移植されている [216]。これは、先に説明した「tcpdump」（および NETSH TRACE）の出力結果を簡略化したものである。

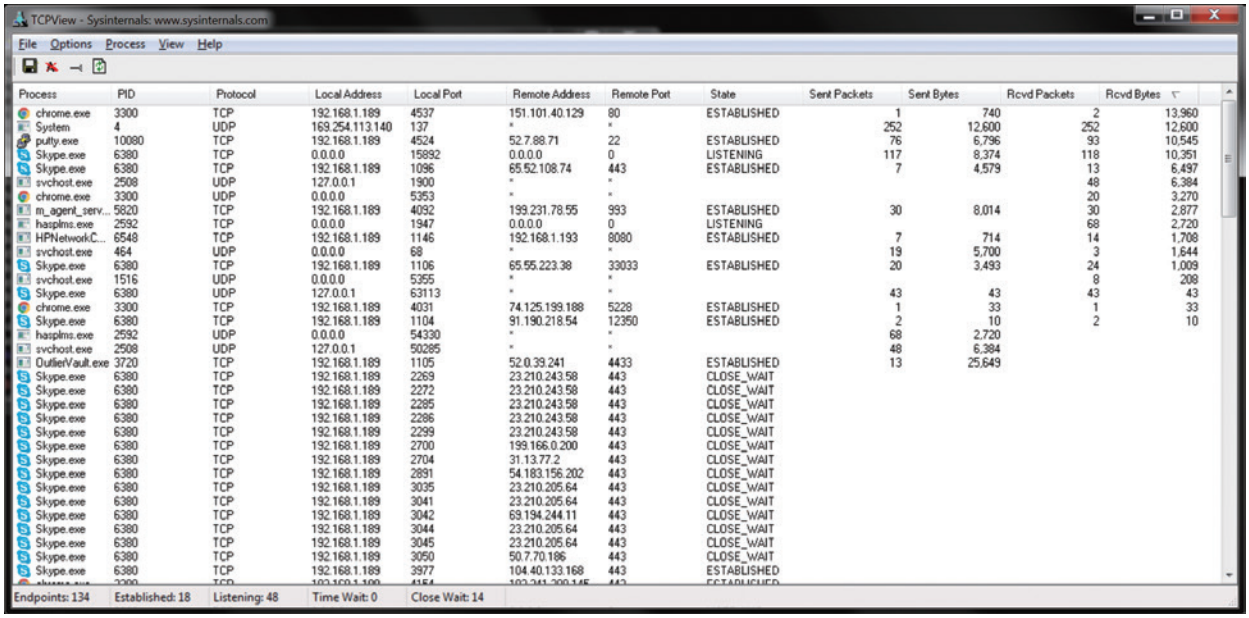


図 6-32. TCPView

Wireshark も tcpdump に似ているが、TCPView とは異なり、ネットワークパケットと接続情報を完全に（または指定されたコマンドによって限定的に）キャプチャする。Wireshark はパケットキャプチャ

215 https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

216 Linuxには、TCPViewや、NetActView、iftopなどの類似のユーティリティのさまざまな実装があるが、単純な「lsof -i」コマンドでも、TCPViewが提供するものと同様の情報が返される。

ライブラリー(libpcap)[217]を使用している。「Libcap」は、Windows向けにはWinPCap[218]として移植されている。Wiresharkは、視覚的またはプログラム的に、多くの多様なソースフォーマット、プロトコル、および通信のコンテンツタイプをキャプチャし、分析するために捜査官・調査員が使用することができる。Wiresharkで監視されたコンピュータ間で転送されたファイル、またはtcpdumpやその他のネットワークパケットキャプチャファイルに含まれるファイルは、パケットキャプチャが接続メタデータだけでなくコンテンツの詳細も収集するように設定されているかどうかに応じて、完全なコンテンツで抽出することができる。tcpdump/PCAPの分析を可視化し、支援するソフトウェアは、オープンソースのものからプロプライエタリで無償、それに有償のものまで、他にも多数存在するが、ネットワークのアーティファクトおよび関連する証拠を収集するのに不可欠なツールはWiresharkに含まれている。

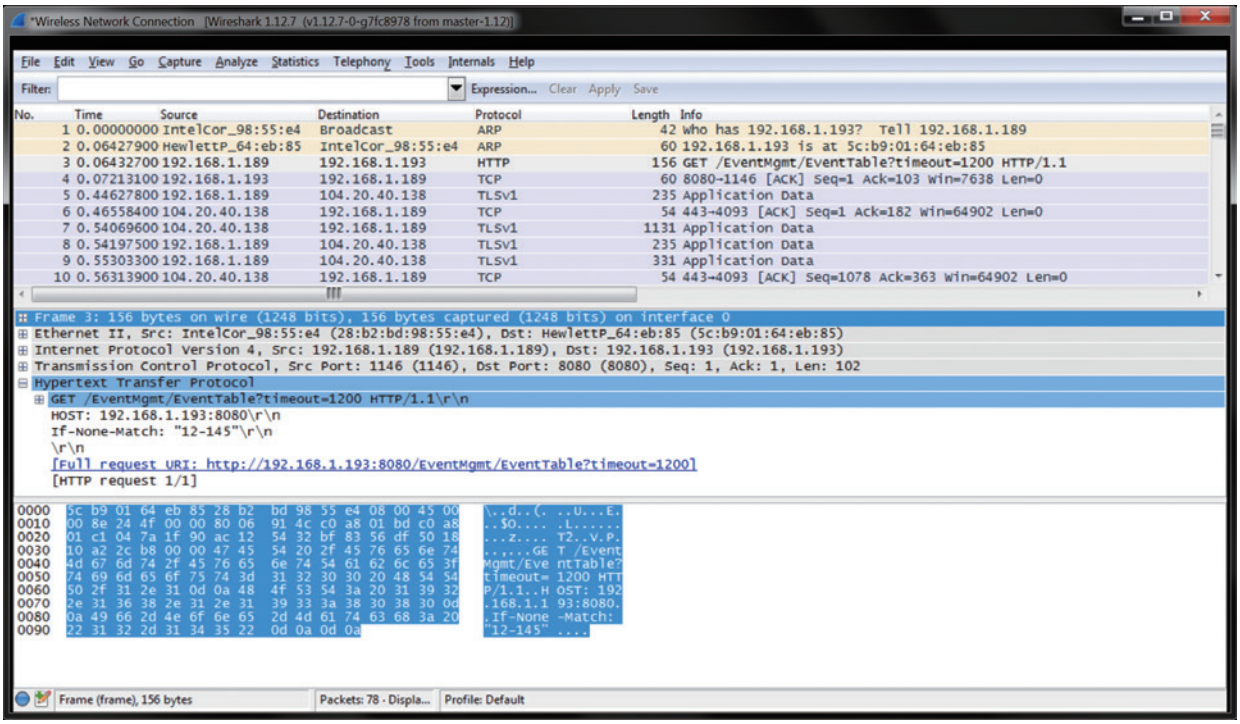


図 6-33. Wireshark

●ホストのメタデータ

ホストのメタデータを収集するツールの種類は幅広い。Sysinternals Suiteには、開かれているファイルのハンドルやシステム構成、実行中のプロセス、自動実行(Autorun)、その他に関する情報を収集するユーティリティがいくつか含まれている(下記の図6-34を参照)。ただし、ホストメタデータの収集は、主に、$MFTおよび$USNJrnl、オペレーティングシステムおよびユーザーのレジストリハイブ、インターネット履歴、Windowsイベントログなど、アクティブシステムでの操作によってロックされているWindowsシステムファイルの収集を含む。処理用にこれらのメタデータファイルをローカルまたはリモートから収集できる特殊ツールには、「RawCopy」[219]や「FGET」[220]などがある(下記の図6-35を参照)。

217 http://www.tcpdump.org/
218 https://www.winpcap.org/
219 https://github.com/jschicht/RawCopy
220 http://opensecurityresearch.com/files/FGET.zip

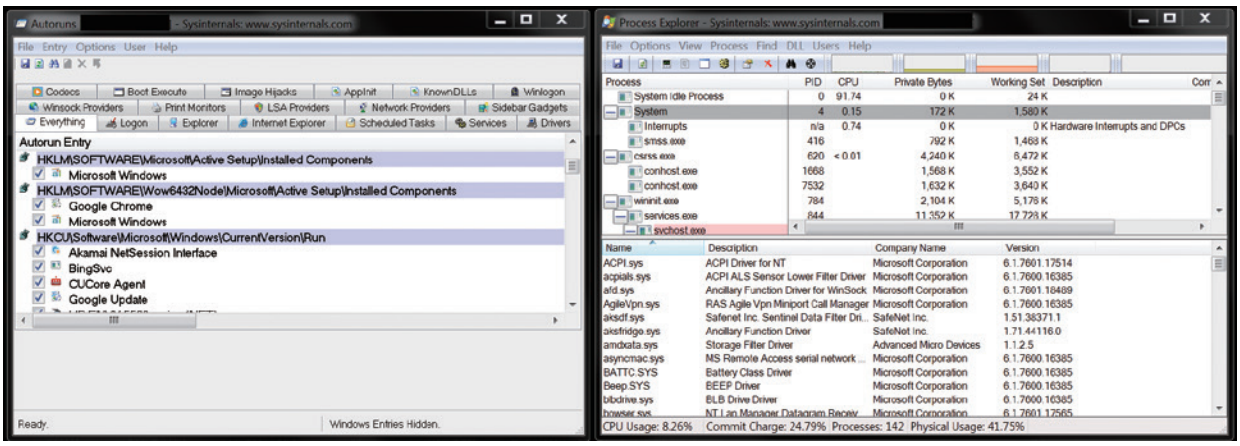


図 6-34. Autorun と Process Exploler（PROCEXP.EXE）

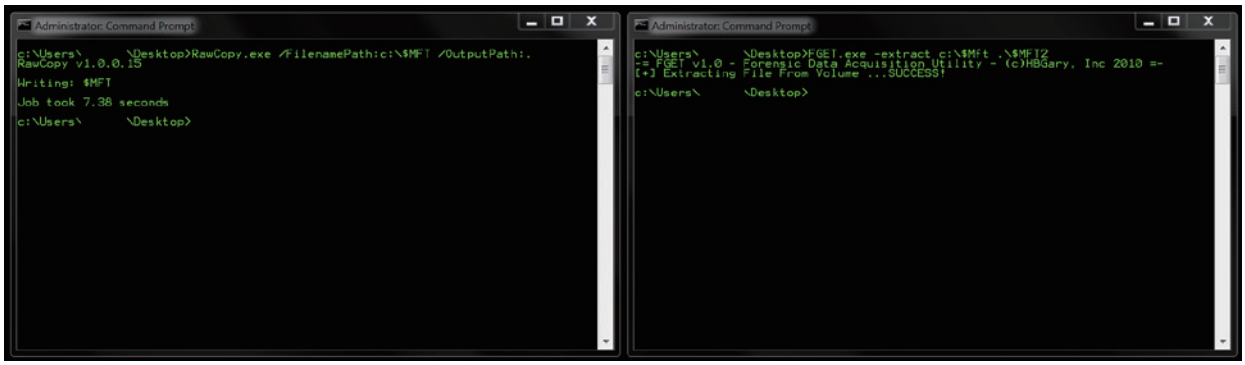


図 6-35. RawCopy と FGET

ロックされているファイルを収集するのに使える無料のサードパーティ製ツール（PowerShell スクリプト[221]を含む）はいくつかあり、**インシデントレスポンスチームの分析者**によってさまざまなフォーラムで議論が交わされている[222]。Joachim Schicht の RawCopy や Greg Hoglund の FGET など、どのようなツールが使用される場合でも、メタデータ分析のために収集する必要があるファイルには、少なくとも次のものが含まれる。

- $MFT と $UsnJrnl
- レジストリハイブ（システム、ソフトウェア、セキュリティ、および SAM）
- ユーザー履歴（NTUser.DAT、USRClass.DAT、およびインターネット – すなわち、Index.DAT など）
- EVT/EVTX ログ（アプリケーション、セキュリティ、およびシステム）
- アンチウイルスログ
- 揮発性のシステムデータ（TASKLIST、NETSTAT、ARP、IPCONFIG、および Autorun のエントリ）
- （任意）Pagefile.sys および Hiberfil.sys
- （任意）メモリダンプ

幸いなことに、インシデントレスポンスチームの分析者が他の「トリアージ」ツールを利用できるよう

221　https://github.com/clymb3r/PowerShell/tree/master/Invoke-NinjaCopy
222　例えば、see http://journeyintoir.blogspot.com/2013/09/tools-to-grab-locked-files.htmlを参照。

になった。そのため、これらのアーティファクトを一度に1つずつ収集する必要はない。最も人気のあるものには、「Google Rapid Response」（GRR）フレームワーク[223]、「PowerForensics」デジタルフォレンジックフレームワーク[224]、「osTriage」[225]、Brimor Labsの「Live Response Collection Toolkit」[226]などがある。図6-36にosTriageのスクリーンショットを示す。

これらのツールはインストールして使うか、単純に適切なコマンドラインから呼び出して使える（たとえば、PowerForensicsまたは既述のPSReconであれば、PowerShellを「管理者」として実行し、呼び出せる）。

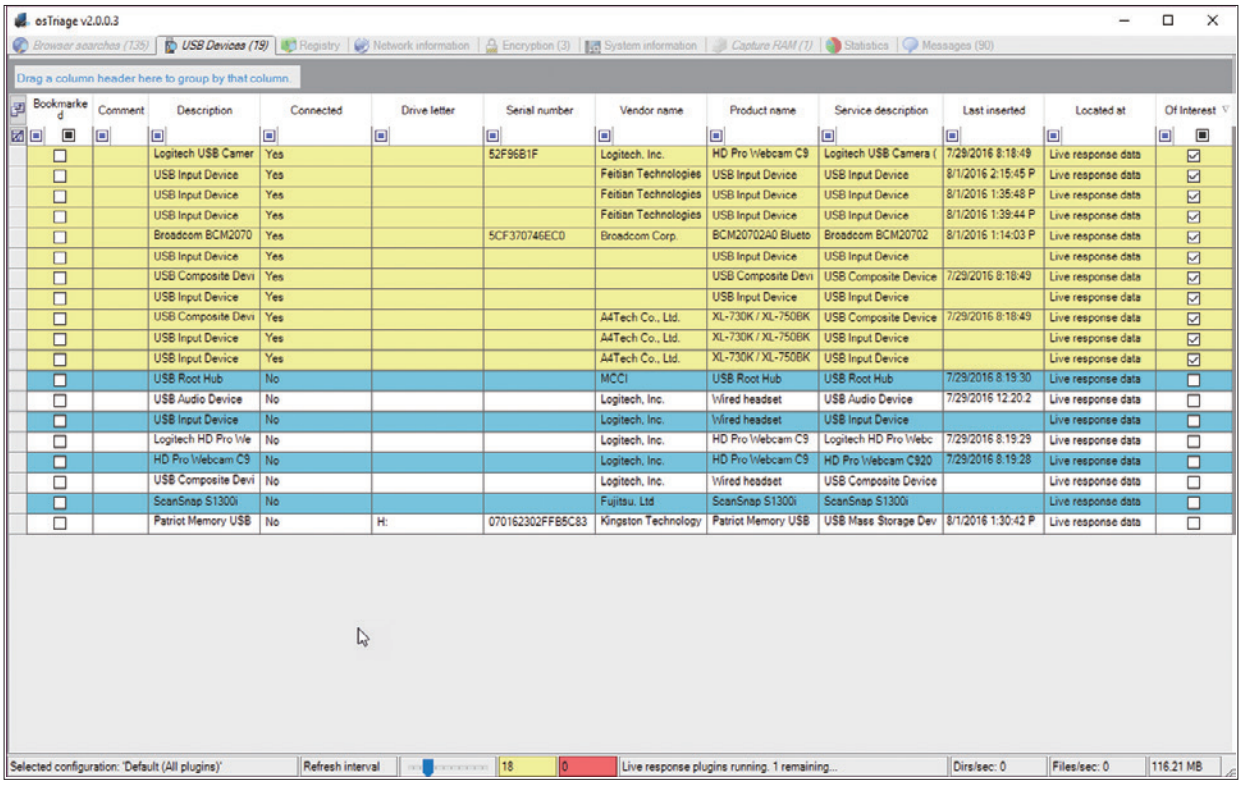


図6-36. osTriage

これらのツールを使えば、捜査官・調査員は稼働中のコンピュータから揮発性のデータを収集できる。また、1つまたは複数のドライブにわたって、さまざまな種類のファイルやアーティファクトを検索することもできる。検索ごとに詳細なレポートが生成され、結果を検証することができる。前述したように、これらのツールキットは、各オペレーティングシステムにあるビルトインユーティリティ、カスタムスクリプト、またはプログラミングと、その他の自由に利用できるツールを組み合わせたものである。これらのツールを組み合わせることで、証拠収集の第2段階（調査）で必要なより深い分析をサポートし、対象となるシステムにサイバー犯罪の実際の証拠が含まれているか、組織のポリシー違反などその他の異常が含まれているか、あるいは無関係であるかを判断することができる。

ライブフォレンジックが実行されると、実行中のシステムに変更が加えられることに注意することが重要である。捜査官・調査員は実行中の環境にツールを導入しなければならず、そうすることでコンピュータに新たな成果物が追加されるため、これは避けられない。たとえば、ライブレスポンスデータ

223 https://github.com/google/grr
224 https://github.com/Invoke-IR/PowerForensics
225 https://feeble-industries.com/forums/
226 https://www.brimorlabs.com/tools/

を収集するために使用されるソフトウェアを含むマシンに接続されたUSBデバイスに関連するレジストリエントリなどである。捜査官・調査員は、自らの行為によって、原証拠にどのような変更を加えたか（もし加えたのであれば）、また使用した具体的なツールを明確にし、説明できることが重要である。実際のフォレンジック分析シナリオでは、ソース証拠の変更は避けられない可能性があるが、捜査官・調査員sが変更の責任（および変更の理由）を説明できない場合、証拠が法的手続きから除外され、捜査官・調査員の報告書や証言の信頼性に影響を与える可能性がある。

●ホストのファイルと内容

ホストファイルやコンテンツのフォレンジック収集は、前述のように、FGETやPowerForensicsのような特定の手動ツールで実行できる。これらのユーティリティは、ETLで消費して大規模な結果を効率的に処理できる「軽量」コレクションのメタデータの取得を支援することを目的としている。また、伝統的に企業のフォレンジック収集需要に応えてきたソフトウェアも別に存在する。これらのツールは基本的に「Hard Disk Duplicator」(DD、ディスクデュープリケーター）が基礎となっている。大規模収集ツールで最も普及しているのは、「FTK Imager142」[227]、「EnCase143」[228]、および「X-Wcays」[229]などである。ただし、Google Rapid Response（GRR）も大規模な収集をサポートしており（下記の図6-37を参照）、これらの収集ツールはいずれも、必要に応じて揮発性データ、ディスク、メモリコンテンツを収集できることに注意することが重要である。

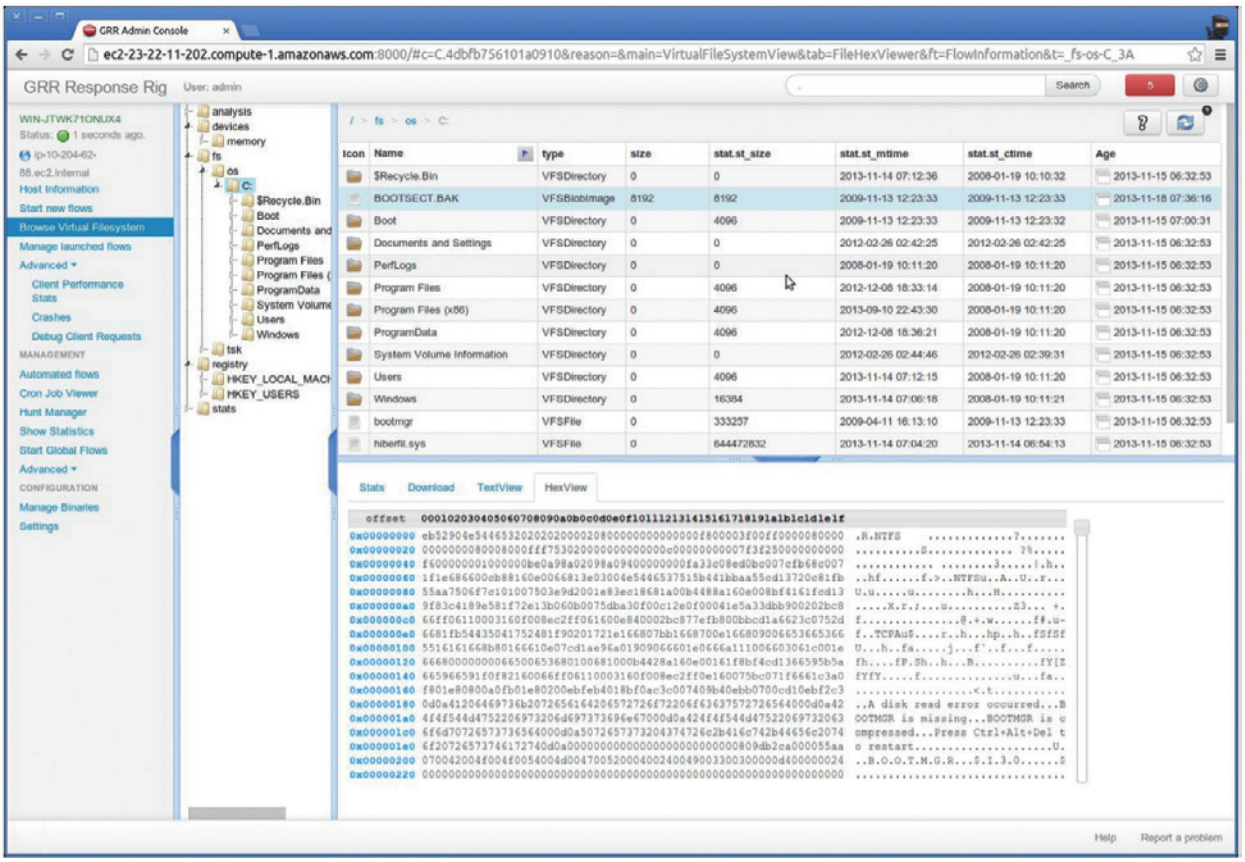


図 6-37. Google Rapid Response

227 http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
228 https://www.guidancesoftware.com/encase-forensic
229 http://www.x-ways.net/forensics/index-m.html

FTK Imager、EnCase 収集ツール、DD、X-Ways、および GRR はすべて収集ユーティリティであり、それぞれ同様の分析レビューツールを備えている（下記の図 6-38 を参照）。EnCase と X-Ways は無料ではないが、他のツールは無料である。各製品には多少の違いはあるものの、各製品で作成される収集ファイルは裁判所（および業界慣行）で認められた形式で標準化されていることを捜査官・調査員は認識しておくべきである。つまり、無料のツールを使用して分析を実行できるということである。レビューツールによっては、アクセスや利用が難しい機能もあるが、収集されるファイル形式は標準化されているため、捜査官・調査員や分析官のスキルや経験に応じて、組織は無料または高価なソフトウェアのいずれでも同じ結果を得ることができる。

無償のツールは経験が豊富なデジタルフォレンジックの捜査官・調査員や分析員に広く活用されている。特に、GRR、様々な PowerShell フレームワーク、そして「SleuthKit」（「Autopsy」[230] レビューツールを含む）は、サイバー犯罪の調査に使用されるツールや手順の改善に熱心な熟練した分析人材のコミュニティの貢献によって支えられている。

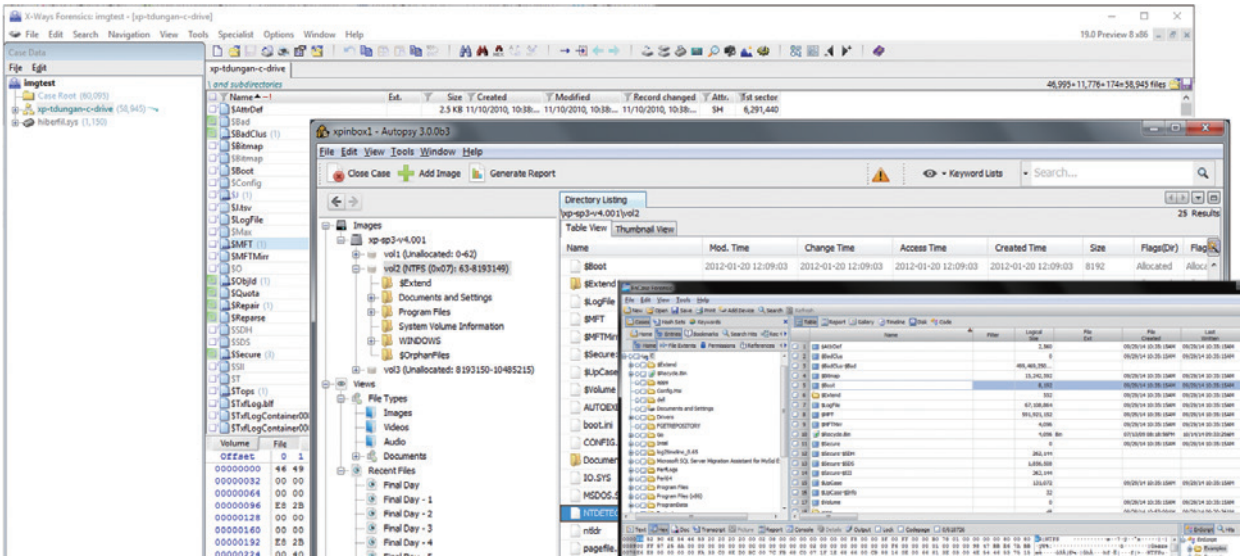


図 6-38. 各種フォレンジック（犯罪捜査）レビューツール間の類似点

メモリダンプの収集には、ディスクのデジタルコピーに使用するのと同じツールを使用できる。メモリ収集には、Windows 用の「Fast Dump Professional Edition」（FDPRO）[231] や「MoonsolsDumpIt」[232]、Linux 用の「LiME」[233]、Apple/OSX 用の「OSXPmem」[234] などの他の一般的なツールも使用される。いったんメモリが収集されると、Volatility や「ReKall」[235] などのツールを利用して、ネットワーク接続、実行中のプロセス、メモリにロードされたファイル、オペレーティングシステムやアプリケーションの設定、ユーザー履歴の詳細、その他のフォレンジックに関連する情報を抽出することができる。

●ログ

サードパーティ製ユーティリティによるログファイルの収集は、さまざまな方法で実現できる。ログは、イベントを書き込んだり、Splunk や ArcSight などの SIEM システムに定期的に内容をコピーした

230 http://www.sleuthkit.org/autopsy
231 http://www.countertack.com/products
232 http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7
233 http://code.google.com/p/lime-forensics/
234 http://www.rekall-forensic.com/docs/Tools/
235 http://www.rekall-forensic.com/

りするように設定できる。また、前節で述べたのと同じツールキットを使うことで、ログにリモートアクセスして検索し、その情報を抽出することもできる（あるいは、ログファイル全体をコピーすることもできる）。証拠収集ソフトウェアと同様に、ログ収集および相関ソフトウェアは無料または有料で利用できる。本質的な違いは、ソリューションを設計、プログラミング、展開、サポートするために必要なスキルが異なる。。

現在、ログ収集および統合（処理用）ソリューションとして最もよく知られているのは、1つは「Elastic」のオープンソースソリューションである「Elastic Stack」（以前は「ELK」と呼ばれ、Elasticsearch、Logstash、Kibanaの頭文字をとったものであるが、現在は「Beats」も含まれている）[236]で、これは必要なストレージおよび処理機器（別途調達する必要がある）以外は無料で使用できる。もう1つは「Splunk」[237]である。これは、一部の（制限のある）条件では無料だが、基本的に処理するデータの量に応じてライセンスが付与されるため、高額な料金になることがある。Splunkには大規模な開発者コミュニティ（オープンソースとプロプライエタリソース）があり、コミュニティでは多くのカスタマイズされたソリューションやサポートが利用可能である。

前述したように、証拠を確認するには、ログファイルとその構成ファイルの両方を収集する必要がある。ログソースからどのような情報が入手できるか、また、構成の不備や技術的な理由（多くの場合、妨害行為）によりどのような情報が入手できないかを理解しておくことが重要である。

サイバー犯罪の潜在的な証拠を特定するには、以下のソースからログを収集して分析する必要がある。

- エンドポイントのコンピュータやサーバー／サービス（Active Directory／DNS／プロキシなど）
- ネットワークスイッチ、ブリッジ、ルータ、ファイアウォール
- 電話システム、警報システム、入退室管理システム
- その他のITおよびOT（Operational Technology）システム（ビル管理、ICS、DCSなど）

収集したログは統合した後、品質のテストと関連性の確認を行い、証拠分析の手順で役に立つよう相関システムで処理する必要がある。下記の図6-39は、ロギングとログ管理の範囲を詳細に示している。

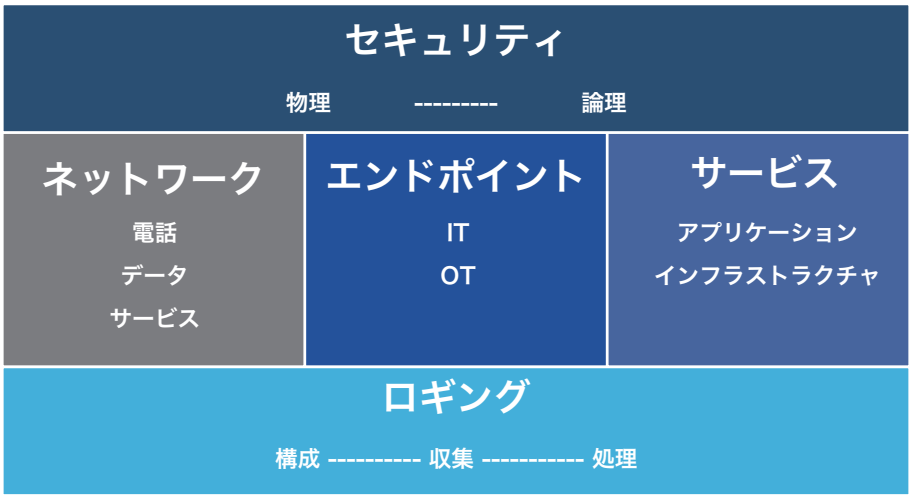


図 6-39. ロギング

236 https://www.elastic.co/products
237 http://www.splunk.com/

フォレンジックにおける証拠の完全性

証拠を収集する手段は、その再現性と実証性、検証性が確保されていなければならない。同じ入力が与えられて、プロセスが何回実行されるか、誰がアクションを実行するかに関係なく、同じ出力が確実に生成される場合、そのプロセスは再現性がある。使用されたツールと方法を他の人が確認して、結果や結論がどのように得られたかを理解できる場合、そのプロセスは実証可能である。異なるツールや方法を、信頼できる手順で同じ入力に適用し、同じ出力を生成できる場合、そのプロセスは検証可能である。フォレンジック分析に確実な証拠を収集するための方法を開発し、関連するツールやスタッフを設計または選択する場合、これらは非常に重要な考慮事項である。

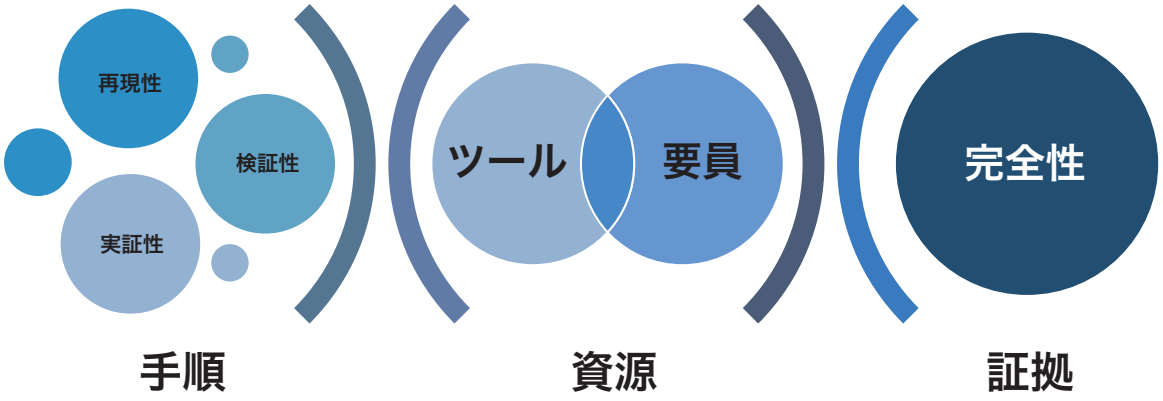


図 6-40. フォレンジックにおける証拠の完全性

「フォレンジック」とは、犯罪の証拠収集・分析に使われる科学的試験またはテクニック（技法）を指す。伝統的な犯罪捜査においては、証拠の収集に加え、法医学、心理学、病理学、機械学、弾道学、会計学などの分野の経験が必要である。サイバー犯罪の登場で、サイバー空間におけるフォレンジック分析の経験も必要になってきている。

サイバー犯罪捜査・調査は、IT 要員や情報セキュリティ要員でさえも、一般的には「通常の業務上」（in the normal course of business）は行わない種類の活動である（「in the normal course of business」は訴訟において証拠／証言の有効性を審理する際に頻出する言い回しである）。サイバー犯罪捜査は「完全性」を保証するフォレンジック手順に依存する。完全性は、大量の（職員および専門家による）証言と証拠収集手順の信頼性を確保した上で、その両方を証明できる能力で成り立つ。

フォレンジックにおける（デジタルの）技術的証拠に関して言えば、「ブラックボックス型」のアプローチは、組織の各種需要をサポートする IT や情報セキュリティのプロセスでは広く使われているものの、サイバー捜査では不十分である。「証明」できることが必須の条件であり、完全性なくしてこれは実現できない。

実証性のあるプロセスは、あるツールがどのような出力を生み出しているのかをある程度可視化するのに役立つため、捜査官・調査員は必要に応じて、ある結論をどのように導き出したのかを説明できる。言い換えれば、捜査官・調査員は、純粋に「ブラックボックス」的なアプローチに頼ることを避け、その代わりに、証拠の収集と変換のテクニック、およびそれらのテクニックによってどのように結論に到達できたかを説明し、実証できるようにすべきである。

例としては、ファイルやハードドライブのイメージの暗号化ハッシュの使用、あるフォレンジックツールを別のフォレンジックツールや文書化された仕様と照合して検証することなどが挙げられる。

暗号ハッシュ関数52は、基本的に数学的な「チェックサム」を計算する方法であり、ファイル入力のようなデータのストリームをプログラムされたアルゴリズムに取り込み、「ハッシュ署名」として固定値を返す。署名は一意であり、対象のファイルに少しでも変更を加えれば、その後の試験でアルゴリズムから返される値も変わる。言い換えれば、ハッシュ関数は可変長のデータ（ファイルの内容など）を固定長のデータ（サイズ）に対応させる任意のアルゴリズムである。ハッシュ署名は、証拠収集の過程でファイルが改変されていないことを示す信頼性のある証明として広く利用されている。また、ある捜査官・調査員が結論を導き出すために使った同じファイルが、別人による検証にも使えるという証明にもなる。

ハッシュ署名は、署名によるメッセージの暗号化とは異なるので注意が必要である。ファイルのハッシュ化は、ファイルの暗号化とはまったく関係がない。これは、ファイルを表す一意の署名にすぎない（多くの場合、冗長になるファイル名とは異なる）。収集された証拠を検証するために最もよく利用されるハッシュ関数は、MD5とSHA256である。WindowsとLinuxには、スクリプト[238]を利用してハッシュを計算する機能が組み込まれている（図6-41を参照）が、前述の収集ツールを含め、他の多くのツールでもこれらの機能が利用できる。収集された証拠の完全性を証明できないと、サイバー犯罪の捜査が妨げられる可能性があるため、使用されるツールに関係なくハッシュを計算する機能が重要である。

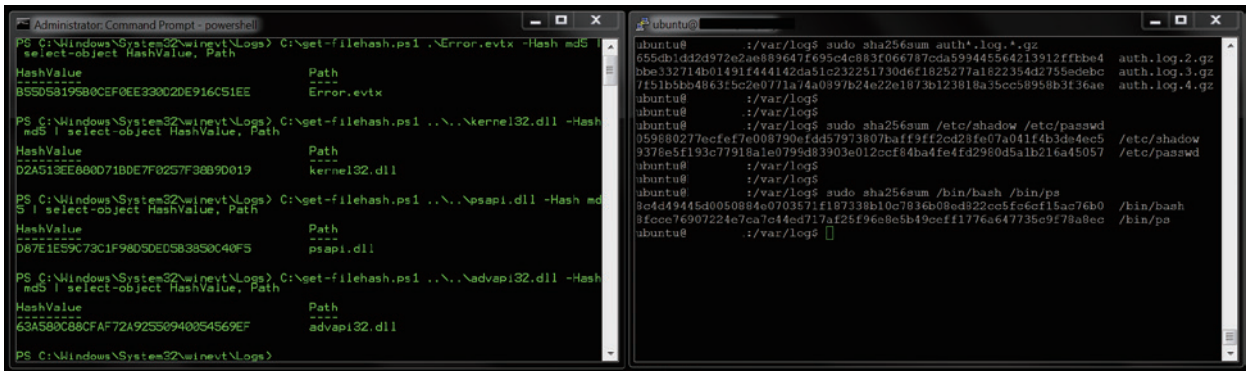


図6-41. WindowsとLinuxのネイティブハッシング

手順の文書化

証拠収集においては極めて具体的な文書化が求められる。文書化は、証拠の完全性を確保するのに役立つという側面もあるが、証拠収集は犯罪捜査全体を支えるプロセスの一部であるため、それは不可欠なものでもある。特定されたすべての要件（再現可能、実証可能、検証可能）を満たす文書化されたフォレンジック分析手順には、どの証拠分析官でも従うことができ、一貫した結果を生み出すことができる。ただし、これは、文書化されたプロセスによって捜査官・調査員が自分の行っている作業を理解する必要がなくなることを示唆するものではない。文書に含めるべき内容の例としては、証拠の収集にあたる捜査官・調査員、その支援を行う要員、収集された証拠を最終的に破棄するか、他の関係当局へ引き渡すまでの取り扱いに携わる要員すべての氏名や資格が挙げられる。

文書化には、特定の情報源や定められたアーティファクトになぜ価値があるのか、それが一般的にどのように解釈されているのか、その他の関連する文脈の概要を含めることができる。これにより、証拠収集にまつわる詳細な情報はサイバー犯罪捜査・調査に続く可能性のある解決や起訴において他の当事者を支援することができるため、より良い報告書の作成、裁判や法的手続きの準備が可能になる。

証拠収集に関する手順を文書化する際は、少なくとも以下を記載する必要がある。

238 Windows PowerShell 5.0にはGet-Filehash CMDLETが組み込まれている。PowerShellの古いバージョンではhttp://poshcode.org/5815などの適切なスクリプトが必要になる。同様のスクリプトは、http://mwganson.freeyellow.com/md5/md5.vbsで説明されているように、Visual Basicスクリプト（および.NETを使用）で実行できる。

- 利用可能な証拠の情報源 – インテリジェンス収集、要員、システムなど
- 収集の手段 – 要員（社内、サードパーティの支援）、ツール、プロセスなど
- 収集および取り扱いの方針 – 法務、リスク管理、コミュニケーションに関する指針など

文書化された手順は、組織内で人員が入れ替わる際の業務の継続性もサポートする。収集手順を徹底的に文書化することで、組織のプロセスに不慣れな人の学習曲線を大幅に短縮できる。

ツールの認定

フォレンジックによる証拠収集に使用されるツールは認証されるべきである。認証は、資格のある社内スタッフまたは第三者によって定期的に監査および更新される文書化された手順を通じて簡単に管理できる。文書化は、ベンダーが提供する製品が同様の状況でいつ、どのように使用されたかに関する製品情報によっても裏付けられるが、ツールの具体的な使用方法や使用条件は、法的手続きでは常に問題になる。したがって、証拠収集のために使用されるツールは、組織の手順に従って使用されるか、少なくとも証拠収集プロセスにおけるツールの使用方法を具体的に説明できるスタッフによって使用されるべきである。

裁判所がフォレンジックツールを認定するわけではないことに注意することが重要である。むしろ、検察官が使用した手順（およびその手順に従った理由）が裁判所で精査され、裁判において提示されるデータが証拠として認められるかどうかが判断される。裁判手続きは、これまで議論されたすべての項目がまとめられる場所である。捜査官・調査員が定められたプロセスに従い、収集の情報源と方法を理解していれば、裁判所にすべてを明確に説明することができ、信頼できる証人、場合によっては専門家の証人とみなされるための要件を満たすことができる。

第三者によるツール認証は、しばしば、組織が特定のツールを選択する際の出発点として機能することができるが、資格のある捜査官・調査員による内部テストや検証に取って代わることがあってはならない。認証のもう一つの側面は、調査員が特定のツールの使用について認定を受けることです。

これは、オンラインテストを受けることから、ツールの熟練度だけでなく、さらに重要なことには、フォレンジックの概念と技術に関する包括的なデモンストレーションまで、さまざまな場合がある。捜査官・調査員はツールに「使われる」ことになってしまわないよう、ツールを活用できるように努めるべきである。言い換えれば、ツールが役に立つかどうかは使用者次第ということでもある。ツールが誤って使用される場合、あるいは捜査官・調査員がツールをいつ、なぜ使用すべきか（または使用すべきでないか）を理解していない場合、ツールは要件に対して適切に信頼できるものにはならない。フォレンジックツールや業界認定は、特定の製品や標準的な手法に精通していることを示す役割を果たすことが多い。ただし、認定を唯一のよりどころとして、証拠収集における捜査官・調査員の能力を判断すべきではない。

証拠分析担当者取得すべき認証資格

IT または関連技術スタッフがキャリアを通じて取得できる認定資格は数多くある。高等教育（大学の学位）を必要とするものもあるが、ほとんどは、科目または技術の習熟度を証明することを目的とした業界またはベンダーの認定資格である。ただし、現実には捜査官・調査員は認定資格を取得していない[239]。その代わり、彼らの経験、実践、方法、知識は、認定を受けている多くの人々がまだ時間と機会をかけて身につける必要がある価値を提供している。

239 http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications

SANS FOR 408（Windows Forensic Analyst[240]）、SANS FOR 508（Advanced Digital Forensics and Incident Response[241]）、SANS FOR 572（Advanced Network Forensics and Analysis[242]）など、ベンダーに依存しない業界認定資格は多種多様である。これらのコースは豊富な資料を提供し、各コースは関連するテストと認定資格で完結する。最も一般的なベンダー認定資格は、AccessData Certified Examiner（ACE）と EnCase Certified Examiner（EnCE）の 2 つだが、下記のようなベンダーに依存しない認定資格も業界では一般的である。

- **CCE** – International Society of Forensic Computer Examiners/Certified Computer Examiner（国際法医学コンピュータ検査官協会／公認コンピュータ検査官）
- **CHFI** – International Council of E-Commerce Consultants/Computer Hacking Forensic Investigator（国際電子商取引コンサルタント協会／コンピュータハッキングフォレンジック捜査官・調査員）
- **CFCE** – International Association of Computer Investigative Specialists/Certified Computer Forensic Examiner（国際コンピュータ調査専門家協会／認定コンピュータフォレンジック検査官）
- **GCFE** – Global Information Assurance Certification/Certified Forensic Examiner（グローバル情報保証認定／認定フォレンジック検査官）
- **GCFA** - Global Information Assurance Certification/Certified Forensic Analyst（グローバル情報保証認定／認定フォレンジック分析官）
- **CSFA** – CyberSecurity Institute/Cyber Security Forensic Analyst（サイバーセキュリティ研究所／サイバーセキュリティフォレンジック分析官）

証拠収集を行うスタッフは、細部にこだわり、簡潔に記述でき、複雑な技術的概念をさまざまな対象者に説明できる能力を備えているべきである。例えば、他の検察官に調査結果を提示する場合、同じ技術的背景を持たない弁護士や経営陣に調査結果を提示する場合よりも多くの（そして異なる）詳細を含むことになる。

サイバー犯罪の種類別の証拠収集要件

サイバー犯罪の種類によって証拠の要件が異なるため、収集要件も異なる。サイバー犯罪の種類は、標的（および対応する範囲）とカテゴリ（犯罪の意図または目的）によって定義される。サイバー犯罪の標的や分類は、従来の犯罪にそのまま対応している。収集される証拠の種類は、多くの場合、検察官が法廷で事件を証明するために使用する必要があるものによって決まる。インシデントレスポンスの調査員や捜査官が任務とする証拠収集は、標的と犯罪意図のカテゴリによって優先順位をつけるべきである。人体の安全に関わる事例は、そうでない事例よりも必ず優先度が高くなる。たとえば、差し迫ったテロの脅威や誘拐は、金融詐欺や知的財産の盗難よりも優先度が高くなる。

以下の項では、収集すべき証拠の種類と、サイバー犯罪の各ターゲットやカテゴリを調査する際に考慮すべき優先事項について説明する。必要に応じて、収集する証拠の例についても示す。

240 https://www.sans.org/course/windows-forensic-analysis
241 https://www.sans.org/course/advanced-incident-response-threat-hunting-training
242 https://www.sans.org/course/advanced-network-forensics-analysis

標的別

先の章で述べたように、サイバー犯罪は犯罪を行う新しいメカニズムを反映している。（情報源や捜査成果物の）証拠収集の目的のために、サイバー犯罪の種類は、犯罪のターゲットに応じて文脈化することができる。ある種の証拠は、すべてのサイバー犯罪に共通し、収集、処理、分析に必要である。しかし、検察官は、一部の証拠の情報源と関連アーティファクトについて、重点的に評価し、さらに特定の収集を要請することがある。

●個人

個人を標的とするサイバー犯罪は、個人情報（PII：Personally Identifiable Information）を悪用する。そのため、その人物のコンピュータやモバイルデバイスの使用履歴が最良の証拠源となる。一般的なアーティファクトである $MFT またはファイルシステムの変更履歴以外に、NTUSER.DAT（または bash の履歴と関連ファイル）や plists、電子メールが格納されているファイル（PST や OST ファイルなど）、インターネットブラウザの履歴を調べ、時間軸を分析して知見の情報源と一致する IoC（不正アクセスのインジケーター）の有無を確認する必要がある。

●組織

組織を標的にしたサイバー犯罪の目的は、個人を標的にした犯罪ほど単純ではないかもしれない。標的となった性質と範囲は、ホストとネットワークのデータを含むインテリジェンスと調査したソースから得た証拠の包括的な分析によってのみ決定できる。分析においては、どの組織単位が（もしあれば）、どのような目的で標的になっているかを見極めることに重点を置くべきである。たとえば、情報源から企業が知的財産の盗難の標的になっていることが判明した場合、調査では財務または人事アプリケーションではなく、関連する知的財産の開発と保管に重点を置くべきである。（先に述べたような）手続き的な調査ステップでも、他の利害関係システムを明らかにすることは可能であるが、目的のターゲット設定に応じて収集と分析の優先順位をつけることで、効率的なリソース利用を確保することができる。

●業界

組織を標的とする場合と同様に、業界セグメントを標的とする場合も、サイバー犯罪の目的に関連する証拠の収集が必要になる。セキュリティ自動化ツール（アラートやその他の目的）を使用して IoC を作成し、活用するには、同業組織や業界コミュニティの情報源を含む OSINT および PROPINT からのインテリジェンス収集に特に重点を置くことが最も重要である。

●国家

国家を標的にした攻撃は、通常、国防や政治に関する情報、通信、作戦のネットワークや管理システムに向けられる。このような活動の目的は、主にスパイ活動、破壊活動（再構成または誤報による）、または妨害行為／破壊を行うことである。このようなケースの証拠収集は、特定の業界、組織、または人物を詳細に示すことができる情報データと、捜査官・調査員がフォレンジック証拠を入手する際に役立つ関連する技術的指標に焦点を当てるべきである。

分類別

サイバー犯罪は、標的の規模に応じた一定の目的を達成するために行われる。下記の表は、組織やサイバー捜査官・調査員が収集ガイダンスの方針と手順に組み込むべきいくつかのカテゴリを示している。

表 6-1. 分類別の証拠収集

分類	目的	証拠の情報源
健康および人体の安全	健康医療サービス、救急対応サービス	• 動画 / 音声、安全システムの録画 / ログ • 通話記録 / 録音 • 証人からの事情聴取 • ユーザエンドポイントおよびアプリケーションサービス（電子メール / チャット / その他）の画像 • ユーザのネットワーク共有
	人体に対する危害	
	児童犯罪	
	誘拐	
	個人情報窃盗	
	器物または施設の損壊	
強盗 / 窃盗	恐喝	• 通話記録 / 録音 • 証人からの事情聴取 • エンドポイント / サーバおよびアプリケーションサービス（電子メール / チャット / その他）の画像 • 市場の知見、OSINT、PROPINT
	個人の金融財産	
	組織の金融財産	
	業界の財務業績 / 経済活動	
	市場の財務業績 / 経済活動	
ビジネス	ソフトウェア知的財産	• 通話記録 / 録音 • 証人からの事情聴取 • エンドポイント / サーバの画像
	その他知的財産（設計、設計図など）	
テロリズムおよび国家安全	破壊工作、転覆、恐怖	•（必要に応じて）上記のすべて

●証拠の取り扱い

証拠を取り扱うときは、それが裁判で使われるものであるということを常に理解しておく必要がある。したがって、最初の収集から検査プロセス、そしてその証拠を所有者に返却するまでの証拠取り扱いのすべての段階を適切に文書化することが極めて重要である。プライバシー、情報の機密性、アクセス制御に関わる収集方法に関するポリシーは、法的制限に基づいて決定する必要がある。

証拠収集の手引き

サイバー犯罪に対処する際に収集される証拠には、（標準的な組織的プロセスを通じて）サイバー犯罪の発見時またはそれが疑わしい時に収集される付帯的な証拠、物理的な捜査令状または同様の行動の結果として現場で収集される証拠、召喚状、電子捜査令状、またはその他の法的プロセスを通じて収集される証拠の 3 種類がある。

物理的な捜索令状の場合、まず適切な法的書類を入手してインターネットサービスプロバイダーに提出し、プロバイダーが証拠を収集してそれを要求機関に返却するまでに、数日から数週間かかることが多い。このような事情がある場合は、（適切な法的権限が付与されている場合）要請される証拠を保有または管理している組織に保全要請を送付することが推奨される。保全要請では、求められている情報の所有者に要請を知らせないことを明確にすべきである（管轄の要件に従って）。証拠を保有する会社が、その要求について情報の所有者に伝えた場合、調査が危険にさらされる可能性がある。例えば、対象者が証拠を修正または破壊しようとするかもしれない。

●付帯的証拠の収集

偶発的な証拠収集とは、基本的に、組織のプロセスや関連技術によって発生する「通常の業務過程」での知見および証拠の収集のことである。組織の方針に例外が記述されていない限り、そのような追加的な証拠収集は行われるべきではない。そのような例外には、ヘルプデスク、IT、監査、セキュリティ、または通常の業務中に検出された異常に関連する証拠を収集し保存するために、疑わしい活動を調査行動にエスカレーションする関連手順が含まれる場合がある。このようなエスカレーション手続きは、他の業務活動がその後の証拠収集の妨げになったり、偶発的な改ざんのために証拠の信頼性が低下したりしないように、組織のリスク管理方針に組み込まれるべきである。ヘルプデスクや IT スタッフが「手助け」をしようとしても、証拠収集の方法に関する要件（目的と制限）を理解していない場合、これは残念

なことだが、捜査官・調査員が直面する非常に一般的な状況である。

●物理的に行う証拠収集

デジタル証拠の収集は、血液、紙の記録、武器などの、より伝統的な証拠収集と多くの点で似ている。証拠が発見された場所や環境条件は、時には証拠そのものの内容と同じくらい（あるいはそれ以上に）重要である。

方針として、捜査官・調査員は場所を確保したら、捜索を行う前に現場のビデオを撮り、環境を記録すべきである。写真も使用できるが、ビデオの方が多くの場合より迅速で、詳細をより多く保存できる。これは、ビデオでは（写真と比較して）調査員がより効率的に収集できる情報が多く提供されるからである。「前」の状態を記録した後、場所内の特定の領域に固有の文字や番号などの指定を与えるべきである。全体的な場所のスケッチも作成でき、捜査後の参照を容易にするために、識別子をスケッチに記録することができる。

捜索を開始したら、証拠を発見するたびに捜査官・調査員は所見を徹底的に文書に記録すべきである。これは、証拠が発見されたエリア、そのエリア内での場所、誰が証拠を発見したかを記録することを含む。デジタル証拠を収集する前に、デジタル機器の状態を観察すべきである。例としては、デバイスの電源が入っているかどうか、デバイスが何に接続されているか、などが挙げられるが、これらに限定されるものではない。要約すると、デジタル証拠を収集する前に、デバイスの写真を撮影し、下記の具体的な情報を文書化すべきである。

- 物品の発見者
- 見つけた日時
- 発見現場／エリア
- 機器の状態（電源オン、接続済みなど）
- メーカー、モデル名、製造番号、その他機器を識別するための詳細

証拠が発見されるたびに、それを保管人に届けるべきである。それぞれの品物は専用のビニール袋に入れられ、固有の番号が付けられ、番号は袋と押収品の目録の両方に記載される。収集すべきデバイスの電源がオンになっている場合は、画面に表示されている内容や実行中のプロセスなど、デバイスから入手可能な揮発性データを収集すると便利な場合がよくある。写真では画面に表示されている内容が明確に示されていない場合は、画面の写真と表示されている内容の詳細なメモを書き留めておくべきである。デバイスの初期状態が記録されたら、デバイスの電源がオフになった場合に失われる揮発性データを収集するために、デバイスをトリアージすべきである。osTriage、PSRecon、その他のライブ レスポンス ツール（前述のとおり）などのツールを使用すると、捜査官・調査員は揮発性データと不揮発性データの両方を迅速に収集し、それを便利な形式で提示して、定められたデバイスで次に何をすべきかを即座に決定できる。

デバイスのトリアージは、デバイスが暗号化されているかどうかの判断など、多くの重要な証拠収集技術を自動化する。これは、強力な暗号化がますます一般的になりつつあるため、非常に重要である。このようなデバイスが適切に取り扱われない場合、またデバイスの電源が途中でオフになった場合、後でデータにアクセスすることが困難になったり、不可能になったりすることがある。また、トリアージは、容疑者や目撃者との事情聴取の際に、現場で活用できる豊富なリアルタイムのインテリジェンスを提供することもできる。例えば、トリアージデータは、ネットワーク内の他のホスト（または他の場所）との接続を示すかもしれず、その後の収集と分析によって有用な証拠が得られる可能性がある。トリアージプロセスは、閲覧履歴、最近使用したファイルやプログラムなどのリストを提供することができ

る。その情報は、追加の証拠としてインタビューに組み込むこともできる。

捜査が終了したら、その資産を所有している人に目録を見せ、何が収集されたかを確認させるべきである。確認が完了したら、目録を作成した人と押収された品物の所有者が目録受領書に署名する必要がある目録の署名者には、目録の写しを渡すべきである。捜索令状の許可を示す書類の写し（陳述書を除いて）も渡すこと。また、送達用の写しが渡されたことを示すために、目録の領収書と捜索令状を写真に撮っておくことも推奨される。理想的には、捜査官・調査員は、目録と捜査令状の送達用の写しの両方を持つ目録に署名した人物の写真を撮るべきである。これにより、それらの文書のコピーが提供されなかったという主張の可能性が排除される。

●電子的証拠の収集

このカテゴリの証拠は、組織が召喚状や捜索令状などの法的手続きに供される結果をもたらす。電子資料は、電子メールアカウント、サーバーまたはエンドユーザーコンピュータ、アプリケーション履歴ログおよび相関する設定ファイル、またはコンピュータ／メモリ画像およびネットワークパケットキャプチャのような単純なものかもしれない。電子証拠収集によって返却される情報の種類や形式は、召喚状の対象者や、要求された資料をどのように返却することにしたか、あるいは捜査令状に従って捜査官・調査員がどのように証拠を押収、収集、文書化したかによって、大きく異なる場合がある。何が返されるかに関係なく、一貫した方法で処理されるべきである。下記の情報は、提供者から受け取った時点で、報告書、証拠追跡システム、または同様のリポジトリに記録する必要がある。

- 証拠が届いた日時
- 提供者に対するデータの収集を求めた法的手続き
- 届けられた資料の概要（写真と詳細な目録を含む）
- 配達人または代理人を含む証拠提供者の身元と住所

作業する証拠分析官のために、電子証拠の作業コピーを作成すべきである。調査目的で証拠のコピーを作成する場合を除き、収集されたオリジナルの証拠を扱うことは決して推奨されない。証拠をコピーし、証拠のフォレンジック調査上の整合性を保護するための特別な手順、たとえばファイルシステムまたはボリュームデータの改変を防止する「書き込みブロッカー」、あるいはそれに代わる特定の文書（コピー手順のビデオが添付されている場合もある）を使用する必要がある。証拠の完全性を検証するため、証拠原本および作成された各コピーのハッシュ署名も文書化されるべきである。

たとえ法執行機関がサイバー犯罪捜査に関与していない場合でも、組織のセキュリティおよび捜査活動においては、これらの手続きに従うことがベストプラクティスである。これらの手順を関連するポリシーに文書化することで、リスク管理部門、IT 部門、および関連する部門が、サイバー犯罪の証拠収集において法執行機関からの要請をサポートするための要件を理解するのにも役立つ。

証拠収集における課題

組み込みデバイスの急増により、現代の証拠収集には特有の課題が生じている。この章で紹介されている方法とツールは、ユーザーがデバイスに簡単にアクセスでき、システムアーキテクチャとオペレーティングシステムアーキテクチャが一般的なアプリケーションをサポートする従来のエンドポイントに対する包括的なアプローチを表している。しかし、モノのインターネット（IoT）や産業用モノのインターネット（IIoT）デバイスの台頭により、さらに高度な抽出・分析ツールが必要になることが多い。

モノのインターネット（IoT）デバイス

デフォルトでは、IoT デバイスは簡素化されたカーネルを含んでいることが多く、デバイスファイルシステムへのアクセスは制限されている。その結果、クラウドサービスやウェブサイトでの管理に頼ることが多くなる。しかし、多くの IoT ベンダーは、データ収集が可能なハードウェアデバッグポートまたは限定的なローカルインターフェースを構築している。

IoT デバイスは、アンドロイドから他の Linux 型亜種まで、様々なオペレーティングシステムを実行する。IoT デバイスにアクセスできたとしても、生成される証拠は、デバイスの構成や容量制限、特定のデバイスで稼働中の機能によって大きく異なる可能性がある。IoT や組み込みデバイスでは、「BusyBox」と呼ばれる、コマンドラインコマンドの数が限られた、簡素化されたソフトウェアスイートをよく見かける。IoT デバイスでの証拠収集は、すべてのデバイスが同じコマンドを有効にした状態で出荷されるわけではないため、デバイスの BusyBox インスタンスにあるコマンドを使用してどのようなデータを抽出できるかを知ることに依存する場合が多い。ウェブインターフェースが公開されているデバイスの場合、捜査官・調査員は NGINX やデバイス上で動作している他のウェブサーバからウェブサーバのアーティファクトを引き出せることが多い。

産業用制御システムと産業用モノのインターネット（IIoT）デバイス

産業用制御システム（ICS）デバイスと産業用モノのインターネット（IIoT）デバイスは、産業環境で動作するように設計された IoT デバイスのサブクラスである。これらのカテゴリの産業用デバイスには、センサー、アクチュエータ、ヒューマンマシンインターフェースデバイス、その他のエンドポイントデバイスが含まれる。

センサーは、産業プロセスの状態を監視して、プロセスが意図したとおりに実行されていることを確認し、安全システムの場合には、プロセスの整合性、可用性、安全性を保護するために調整が必要であることをシステム全体に迅速に反応して警告する。

アクチュエータは物理世界で動作し、何らかの形の物理的変化を引き起こす。例としては、ロボット、モーター、および物理的またはプロセス制御の変更が可能なその他のデバイスなどがある。

ヒューマンマシンインターフェースには、工場のオペレーターやその他の担当者が産業プロセスを監視および制御するために使用するデバイスが含まれる。

産業用デバイスでは、証拠収集が簡単な場合もあれば、そうでない場合もある。例えば、ヒューマンマシンインターフェースは、Microsoft Windows の異なるバージョンを頻繁に使用する。従来のエンドポイントシステムに Windows がインストールされている場合、捜査官・調査員はシステムから直接従来の Windows アーティファクトを収集できる可能性がある。ただし、ヒューマンマシンインターフェースデバイスが組み込みシステム上にある場合など、アクセスのためにベンダーとの調整を必要とするベンダー管理システムでは、課題が生じる場合がある。例えば、Siemens は組み込みシステムに Windows CE を搭載した Simatic HMI シリーズを製造している。この場合、このエンドポイントから証拠を収集するのはそれほど簡単ではないかもしれず、捜査官・調査員はどのようなログやデータソースにアクセスできるかを判断しなければならない場合がある。

プログラマブルロジックコントローラ（PLC）は、証拠収集にとってさらに大きな課題を示す。これらのデバイスの多くは、Blackberry の QNX や WindRiver の VxWorks などのリアルタイムオペレーティングシステム（RTOS）の派生版を実行する。このような状況では、アクセス方法もアーティファクトも Windows エンドポイントのものとは大いに異なる。PLC または組み込みデバイスからの収集には、デバイス上のデバッグポート（存在する場合）にアクセスする方法に関する知識など、ある程度のハードウェアリバースエンジニアリングのスキルが必要になる場合がある。一部のデバイスでは、Joint Test Action Group（JTAG）ポートが露出しており、これにより組み込みデバイスへのデータアクセスや操作

が可能になることがある。別の場合では、データの収集にメーカーとの協力が必要になる場合もある。ソフトウェアプロービングを通じて組み込み型産業用デバイスからデータを収集することも可能になるかもしれない。例えば、Microsoft は ICS システムから特定の情報を調べるための ICSpector というオープンソースツールを開発した[243]。

CoC（Chain of Custody 証拠の保全・マネジメントの連鎖）

証拠が押収された後、その証拠は指定の証拠保管施設に安全に搬送され、安全に保管されるべきである。法執行手続きにおいては、この活動は、その手続きに従って証拠を収集する捜査官の裁量に委ねられる。組織的な調査においては、証拠品施設も使用のために指定されるべきであり、物理的／論理的なアクセス制御をマネジメントする関連ポリシー、および証拠品を預ける者と本来の証拠品取り扱いに関するその活動に関する関連記録を保持すべきである。証拠保管施設が利用できない場合、押収された証拠が安全に保管され、目録／領収書に署名した個人の保管下にあることを確実にするため、押収された証拠を所持する者は、十分な注意を払うべきである。押収された各品目については、前述のとおり前述のとおり証拠の保全（マネジメントの連鎖）を準備すべきである。

証拠が引き渡されたら（または電子証拠ケースマネジメントシステムでチェックアウトされたら）、受取人は、証拠がいつ、誰によって、どのようにアクセスされたか、またその理由を詳細に記した「マネジメント記録」に署名すべきである。例を表 6-2 に示す。

表 6-2. 証拠の連鎖のログ

氏名	理由	日時	受領者氏名	場所	日時
スティーブ・アレン	現場から搬送	2016-08-27 13:47	マイク・ロジャース ID#1234	証拠品ロッカー	2016-08-27 15:00
マイク・ロジャース	調査のため出庫	2016-08-28 08:27	スティーブ・アレン ID#6789	受付	2016-08-28 08:27
スティーブ・アレン	証拠品保管施設に返却	2016-08-30 09:52	マイク・ロジャース ID#1234	証拠品ロッカー	2016-08-30 09:52

証拠のコピーは他の証拠品と同様に追跡され、それに応じて証拠の保全（管理の連鎖）が用いられる。

分類／管轄別の保有

事件が解決するまで、証拠（原本とコピー〔「派生証拠」と呼ばれることもある〕の両方）は保管し、関連する証拠の保全（管理の連鎖）を維持すべきである。事件解決までの期間は、裁判の結果に応じて数か月から数年にわたる場合がある。事案が司法手続き（必要に応じて上訴や再審査を含む）を経るにつれて、数十件から数百件分の証拠を保管するための十分な保管場所と資源を確保するための準備と計画を立てなければならない。法的な保管に加えて、規制上の要件により、個人の健康に関する情報、プライバシー情報、財務情報、保護すべき産業に関する情報、機密情報、または類似の情報が含まれる場合、特定の証拠の保管方法が定義される場合がある。このような問題があるため、組織は、SIEM やその他のロギングや監査データなどの偶発的な証拠を収集するためのポリシーや手順を決定する際には、特に注意を払うべきである。場合によっては、非公開情報の収集に、保持および取り扱い要件（世界の一部の地域では開示など）が発生することがある。

243　https://github.com/microsoft/ics-forensics-tools

証拠の廃棄

ほとんどの場合、事件が終結すると、証拠の原本は持ち主に返却される。このプロセスは、証拠が押収されたときと同様の方法で目録に記録されるべきである。証拠が誰かに返却されるとき、目録にはそれを返却する法執行官と証拠を受け取った人が署名する。この目録は、証拠が返却されたことを示すため、事件簿に記載されるべきである。証拠を所有者に返却できない場合は、いかなる資料も適切な手段で破棄し、それに応じてその破棄を文書化しておくべきである。

第 6章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪のスコープ（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

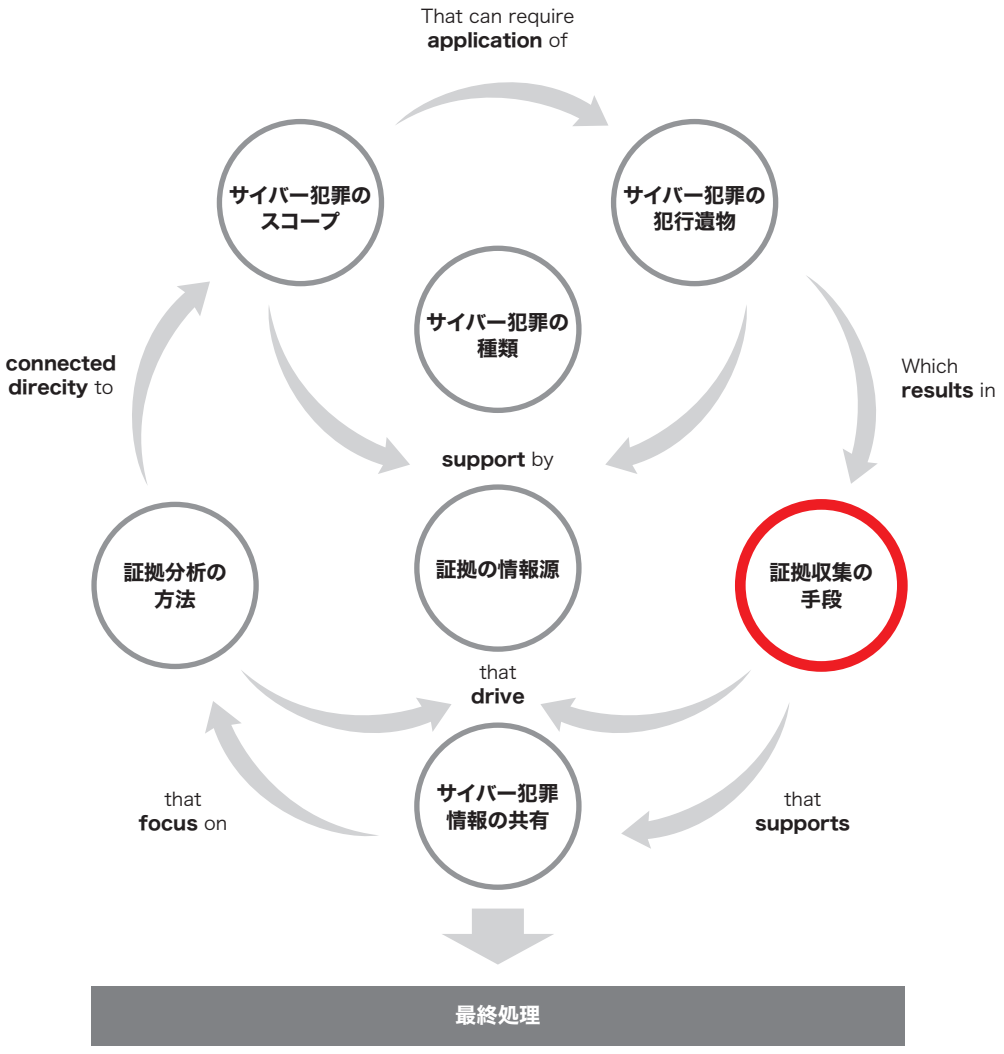


図 6-42. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

表 6-3. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 6-4. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 6-3）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査マネジメントの機能は、組織に対してサイバー犯罪の特性と種類を説明する。証拠の収集および取り扱いの手段に関する法的方針については、手続き的な理解を必要とする。また、関連方針の策定とマネジメントについて、戦略的な責任を持つべきである。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。知見収集スタッフは、証拠収集方法（および制限）に関する手順的な理解と、証拠を収集する方法に関する戦術的な知識を持っているべきである。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。捜査官・調査員は、証拠収集方法（および制限）に関する手順を理解し、証拠を収集する戦術的な知識を持っているべきである。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制および法律のガイドラインは、政策立案者に情報を提供するための調査のアプローチ、および証拠の収集に関する方法と制限を決定する。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。この機能には、責任ある情報開示の場と情報共有の方法を戦略的に理解することも必要である。捜査と分析を通じて判明したサイバー犯罪の種類に応じて、方針に基づきながら、何を、だれに、いつ、伝えるのかを決定する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第6章:レビュー

1. **サイバー犯罪の証拠はどのように収集できるか**
   答え：自動的におよび手作業で。
   例：情報収集、調査およびインタビューによる。

2. **サイバー犯罪の証拠はどのように収集すべきか**
   答え：体系的に（アラート駆動型）、スウィープ・ディスカバリー（一掃検知）、ネイティブおよびサードパーティのツール。
   例：SIEM、ネットワーク PCAP、フェーズ 1／2／3 収集。

3. **証拠の信頼性を確保するにはどのような手段または手順に従うべきか**
   答え：計画／文書／使用手順、リソース、および証拠。
   例：再現可能／検証可能／実証可能、スタッフ／ツール、完全性。

4. **サイバー犯罪の種類によって、証拠や関連手段はどのように異なるか**
   ターゲット別およびカテゴリ別。
   例：範囲と目的に応じて。

ケーススタディ6:複雑なIT／OT環境における証拠収集

- **犯罪**：個人情報（認証情報）の盗難、不正アクセス
- **容疑者**：国家の脅威の行為者
- **手段**：ソーシャルエンジニアリング（スピアフィッシング）、ハードウェアおよびソフトウェアのリバースエンジニアリング、マルウェア
- **動機**：スパイ活動、重要インフラの運営妨害、（安全システムの妨害による）物理的損害や危害を与える意図の可能性

公共事業だけでなく、大規模な上下水道、石油、ガス、その他の化学精製プロセスをサポートする運用技術環境は、サイバー インシデントが発生すると二重に危険な状況である。技術システムの中断の可能性だけでなく、安全システム、そして人命も危険にさらされることになる。サウジアラビアの石油化学製油所で「Triton/Trisis」マルウェアが使用されたという悪名高い事件が 2017 年に明らかになったが、使用されて数か月後のことであり、後に判明したように、脅威アクターが最初にアクセスしたのは（2014 年）から実際には数年後のことであった[244]。

産業環境内の安全システムは、人命への悪影響を防ぎ、産業プロセスの整合性を確保し、産業プロセ

244 https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-trisis-malware-mystifies-industrial-community/#:~:text=TRISIS%20malware%20was%20first%20detected,place%20to%20prevent%20plant%20shutdowns.
https://www.darkreading.com/cyberattacks-data-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known

ス内の生産を最適化するために、産業環境内の潜在的に危険な状況を継続的に監視、警告し、頻繁に反応する。

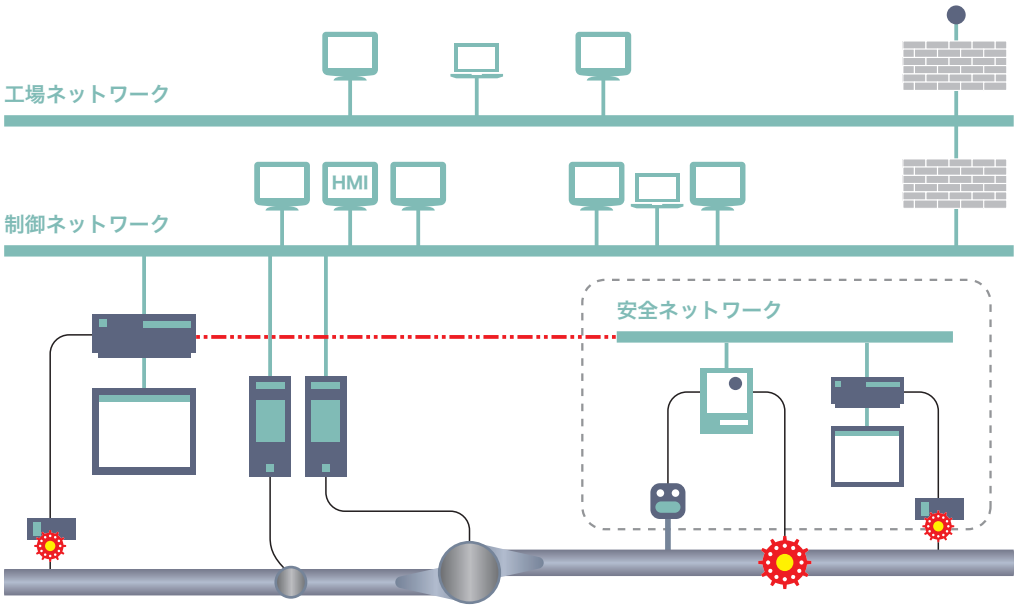


図 6-43. OT ネットワークと Triton/Trisis 攻撃対象の例図 [245]

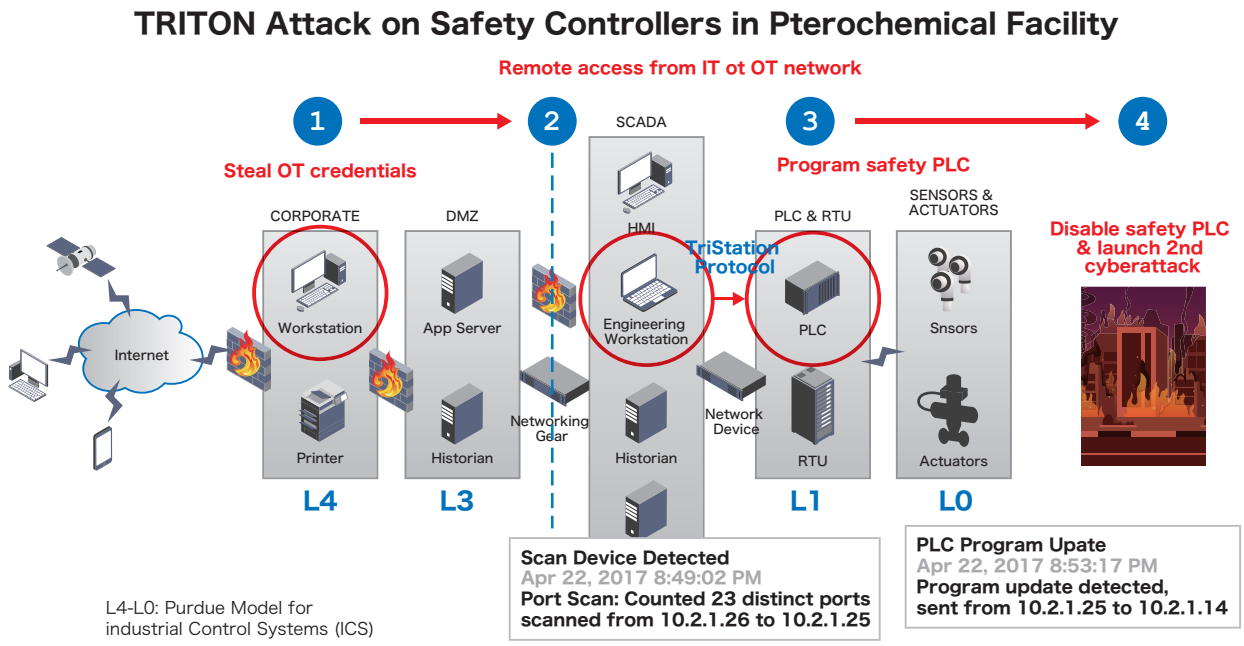


図 6-44. トリトン／トライシス攻撃目標のパデューモデル [246]

2017 年、世界はサウジアラビアの製油所の産業安全システムへの前代未聞の侵入事件を知った。米国司法省の起訴状によると [247]、侵入は少なくとも 2014 年 8 月にさかのぼり、国家と関係のある攻撃者が米国および世界中のエネルギー施設を標的にしていた。攻撃のタイムライン、関連する手順、および IT/

245 https://www.sans.org/blog/triton-trisis-in-search-of-its-twin/
246 https://www.microsoft.com/en-us/security/blog/2020/11/25/go-inside-the-new-azure-defender-for-iot-including-cyberx/
247 https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

OT 環境に対する複雑な攻撃においてフォレンジック捜査官がどのように証拠を収集し評価するかについての洞察を提供する。

- 2014 年、攻撃者は製油所内のコンピュータに不正侵入し、足がかりを築いた

この足がかりにより、攻撃者は検出テストを実行することができた。攻撃者は、変更されたオープンソースのセキュリティツール（cryptcat を含む）をアップロードして通信を確立し、製油所内の産業プロセスにアクセスしてそれに対する機能を構築し始めた。（注：2014 年から 2017 年の間にはオープンレポートにギャップが存在する。）

- 2017 年 5 月、攻撃者が cryptcat をアップロードし、安全システムに関連する技術ファイルにアクセスしているのが再び確認された。

フォレンジック分析観点から、捜査官・調査員はアップロードされたバイナリの MACB ファイル変更記録を通じて 2014 年から 2017 年までのタイムラインを構築した。

- 2017 年 5 月下旬、攻撃者は環境内に存在する特定の古いヒストリアンソフトウェアの調査を開始した。

産業環境では、ヒストリアンソフトウェアは性能評価とコンプライアンスの両方のために、特定のプロセス特性を記録している。ヒストリアンソフトウェアには、産業プラント内外のユーザーがアクセスすることが多いため、多くの場合、ヒストリアンソフトウェアはピボットポイントとして機能し、多くの産業用サイバーセキュリティファイアウォールや監視ツールを通過することができる。ヒストリアンソフトウェアの調査において、攻撃者は製油所内の安全システムのログファイル形式について深い知識を得た。

- 2017 年 5 月 29 日、攻撃者は盗んだ認証情報を使ってエンジニアリングワークステーションにアクセスし、将来のアクセスのためにバックドアを設置し、作戦をさらに強化した。

産業用ネットワークの文脈では、エンジニアリングワークステーションは、組み込み産業用デバイスと産業プロセスの他の部分の両方を設定するためのソフトウェアを含む、最も一般的な古い Windows システムである。エンジニアリングワークステーションは、環境に大きな変更を加えるためのソフトウェアを持っており、そのような変更が発生する場所でもある。エンジニアリングワークステーションがプロセスを変更するという予想される性質はデバイスのネットワークプロファイルに存在する可能性があるが、メンテナンスウィンドウと実稼働ウィンドウを区別できるデバイスは、そのようなネットワークトラフィックに基づいてトリガーされるべきである。エンジニアリングワークステーションは Windows システムであることが多いため、フォレンジック証拠は他のアクティブディレクトリドメインに接続されたマシンと一致する。

- 2017 年 6 月 2 日、攻撃者は安全システムの物理的なプログラムキーを回避して、組み込み型安全システムへの攻撃に方向転換した。

多くの安全システムには、安全システムを「オフ」、「プログラム」、または「実行」の状態に設定でき

る物理的なキーがある。オフ状態では、安全システムはアプリケーションを実行しない。実行状態では、デバイス上のアプリケーションのみが実行されるが、特定の変更は制限される。プログラム状態では、プロセスは実行されないが、設定の変更が行われる場合がある。攻撃者によって標的にされた安全システムの場合、物理キーは存在していたが、安全システムはソフトウェアレジスタに依存しており、キーはそのソフトウェアレジスタの状態を駆動していただけである。攻撃者は正規のバイナリにパッチを適用し、キーの物理的な状態に関係なく、Triconex デバイスをリモートでプログラムモードに切り替えることができるようにした。

これまでの攻撃の段階は、Windows エンドポイントを標的とする攻撃者の典型的な能力と行動と一致していたが、この段階でのピボットは、著しい巧妙さの向上を表していた。安全システムは、単にログインするだけではない組み込みデバイスである。このような能力を開発するには、ソフトウェアとハードウェアの両方のリバースエンジニアリングのスキルが必要である。安全システムの取得と構成にも、多大な資金と知識が必要である。プログラマブルロジックコントローラは eBay やその他のウェブサイトで簡単に見つけることができるが、安全システム全体を探して組み立てるのは非常に困難である。攻撃者はまた、どのシステムを標的にするかを知るために、十分なネットワーク認識を持っていなければならなかった。フォレンジック分析の観点からは、リアルタイムオペレーティングシステムを実行する安全システムのオペレーティングシステムにアクセスすることも困難である。

- 2017 年 7 月 17 日、攻撃者はキーロガーをインストールし、ユーザーのログイン認証情報を収集した。2017 年 8 月、攻撃者は製油所の安全システムに高度な産業向けの機能を配信した。

2017 年 8 月 4 日、攻撃者が多数の安全システムに安全システムマルウェアを展開した後、マルウェアのバグによって装置の 1 つが障害を引き起こし、製油所の緊急停止を引き起こした。攻撃者は、インシデント対応手法を理解するために、標的の組織内の業務システムへのアクセスを継続した。このマルウェアは後に Triton/Trisis/Hatman と名付けられ、安全システムへの侵入が公に知られるようになった初めての事例になった。この事件以前に起きた注目すべき主要な産業事件としては、2005 年から 2010 年にかけてイランの核濃縮を標的とした Stuxnet ウイルスや、2015 年と 2016 年にウクライナの送電・配電変電所への侵入などがある。産業への影響はなかったが、工業用地への侵入に繋がる多くのシステムへの不正アクセスが発生した。

インシデント対応者や捜査官・調査員は、この侵入のいくつかの主要な特徴に注意すべきである。

まず、侵入はスピアフィッシングと従来の Windows システムを標的とした攻撃の組み合わせから始まった。

第二に、この攻撃は数年にわたって発生しており、2014 年に収集されたフォレンジック分析証拠と、活動が活発化した 2017 年の間には大きなノウハウ面でのギャップがあった。攻撃者は、単に同じ日にアクセスして不正なアクセス権限を昇格させたわけではない。

第三に、攻撃者による準備、計画、開発の量は非常に多かった。攻撃者は、ビジネスの技術的側面と運用的側面の両方を研究するために、何年にもわたってアクセスしていた。ログファイルの形式とターゲットの特定のシステムに関する情報が、この操作の重要なデータポイントになった。

第四に、攻撃者はこのリサーチの一部を標的の環境で行ったが、ほぼ間違いなく、組み込み安全システム用のマルウェアを構築し、検出エンジニアリングテストを行うことができるテスト環境にアクセスすることができていた。攻撃者は最終的にはミスを犯したが、従来のマルウェアを使用して何年も、また特定のセキュリティシステムに特化したマルウェアを使用して何か月も環境に潜伏することに成功した。

第五に、脅威が発見されたのはネットワークやホストの検知によるものではなく、産業用マルウェア

自体の失敗によるものであった。多くの産業環境では、導入が簡単でメンテナンスが比較的少ないパッシブ・ネットワーク モニタリングが使用されている。Trisis は cryptcat（およびその他の方法）による検出を回避したが、これは受動的なネットワーク監視だけではこのようなさまざまな方法による攻撃を検出するのが困難であることを証明している。ホストベースの IoC・IoA は、捜査官・調査員がイベントのタイムラインを再構築するための唯一の情報源として機能した。証拠収集を実行するときは、環境内で利用可能なネットワークおよびホストソースを認識し、より完全なタイムラインを構築するために追加の収集をいつ展開する必要があるかを把握することが重要である。

2017 年のサウジアラビアの石油精製所への Trisis の侵入は、産業オペレーションへの侵入と、従来のデバイスと組込みデバイスの両方が存在する環境への侵入に対処する際のホストとネットワークの両方のデータ収集の重要性を示す驚くべきケーススタディである。この侵害は、高度な技術を持ち、十分なリソースを持つ攻撃者によって実行されたが、観察された手法の多くは、一般的な攻撃者の戦術、テクニック、手順が含まれており、多くの調査で参考となる可能性がある。

第7章

証拠分析の方法

はじめに

「証拠分析の方法」の知識領域では、特定のデータ検証方法を通じて証拠が集約され、分析される。サイバー犯罪の捜査官・調査員は決して証拠を偶然の一致として扱わない。サイバー犯罪捜査にはデータサイエンスに基づく分析コントロールが必要である。これらの分析コントロールは、効果的な証拠分析フレームワークにおける必須要素として定義されなければならず、テスト、品質保証、結果の開示を含む。

この知識領域を通じて、サイバー犯罪捜査官はサイバー犯罪を「スコープ（scope）」、「ステージ（stages）」、「種類（types）」別に検討し、組織に関連するリスクと脅威を特定することができる。この領域は、「脅威の行為者（threat actors）」（企業や組織に脅威をもたらすサイバー犯罪者）の「プロファイル（profiles）」や彼らが行う「活動（activities）」に関する影響分析も含む。

この知識領域は、サイバー犯罪捜査官に、証拠分析の効果的な方法を開発するための重要な基本フレームワークを提供する。これらのフレームワークは、システム管理者が予防と保護に関連する「ポリシー（policies）」、「システム（systems）」、「手続き（procedures）」を定義するのにも役立つ。

この知識領域は、「証拠の情報源」（第5章）および「証拠収集の手段」（第6章）と密接に関連する3つのトピック、すなわち集約、分析フレームワーク、および結果の解釈に分かれている。サイバー犯罪捜査官にとって、入手可能な情報源から適切な証拠を収集することが重要であるのと同様に、サイバー犯罪の範囲を評価するためには証拠分析が重要である。一般に、調査には制約があり、技術やその他のリソースは、証拠分析の効率と効果を高めるために、評価スコープに応じて配分されるべきである。

「証拠分析の方法」の知識領域は、本書におけるサイバー犯罪捜査・調査およびその知識領域での他のすべての側面と関連している。この知識領域を学ぶことで、読者は以下のことを理解できるようになる。

- サイバー犯罪の証拠分析のために、どのように証拠を集約、分析すべきか
- 効率的なデータマネジメントと分析フレームワークをどのように定義すべきか
- どのように分析結果を入力し、サイバー犯罪のスコープを関連付けすべきか
- 「脅威（threats）」、「行為（activities）」、および「脅威の行為者（threat actors）」に関連する影響分析はどのように解釈すべきか

証拠分析の方法におけるトピックス分類

「証拠分析の方法」知識領域におけるトピックスの分類を図 7-1 に示す。

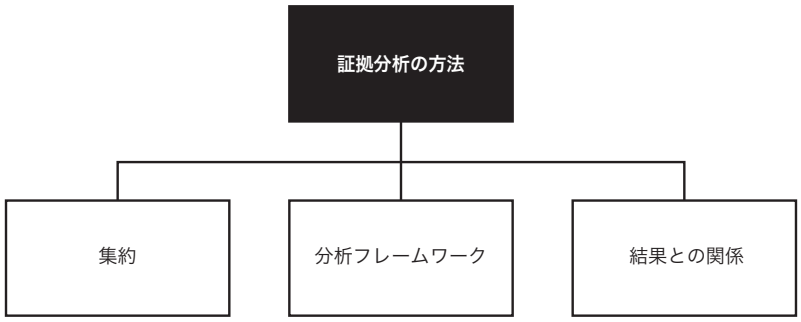


図 7-1.「証拠分析の方法」知識領域におけるトピックスの分類

集約

集約では、「証拠収集（Collected Evidence）」、「脅威インテリジェンス（Threat Intelligence）」、および「調査におけるデータ要素（Data Elements in an Investigation）」の定義を扱う。多くの場合、サイバー空間に散らばった単一の情報のみを使用して事実を証明することは難しい。その結果、断片的な個々の情報を多面的に集約することが不可欠となる。サイバー犯罪捜査・調査で収集された証拠を集約することで、「脅威インテリジェンス（Threat Intelligence）」に昇華させることができ、その情報に基づいて意思決定のサイクルを生み出すことができる。

証拠収集

「証拠収集」とは、不正な行為を行った、または不正な行為に関与した個人または組織を特定するための基礎的証拠の収集である。

収集された証拠は、目撃者、専門家、関係者の証言である**「人的証拠（personal evidence）」**と、目に見える**「物的証拠（physical evidence）」**の 2 つのカテゴリに分けられる。

いずれのタイプの証拠を収集する場合も、将来の法的手続きにおけるその用途を理解することが不可欠である。言い換えれば、証拠は適切かつ合法的な手段のみを使用して収集されなければならない。捜査官・調査員は、収集された証拠の信頼性を保証するために、その証拠が改ざんされていないことを証明できるべきである。

サイバー犯罪の捜査・調査において、極めて重要な「電子データ」は、有形の文書にはない**「揮発性（Volatility）」**の影響を受ける。このような証拠は、誤った操作により紛失または改変された場合、その証拠能力が失われることがある。このため、**CoC** はサイバー犯罪捜査において重要な概念と手順になっている。

CoC は、証拠にアクセスして取り扱うことができたすべての人々の記述を要求している。この仕組みは、証拠がいつ、どこで収集され、どこに保管され、誰が保護・マネジメントしたかを明らかにすることで、証拠の信頼性を保証する。サイバー犯罪捜査・調査における CoC に関する具体的な詳細については、「証拠収集の方法」の知識領域（第 6 章）を参照のこと。

正式な捜査・調査の一環としての証拠収集と、（インシデント）検知とインシデントレスポンスを支援するためのテレメトリ収集の違いを、捜査官・調査員が理解することも重要である。図 7-2 は DFIR（デジタルフォレンジックとインシデントレスポンス）のプロセスを示している。以下に示すように、検知段階が最初に行われ、特定された違反の結果として、インシデントレスポンスの一環として調査が開始される場合がある。検知段階では、アナリストは EDR ツールのような様々なコントロールやメカニズムを通じて利用可能なテレメトリを使用するが、法廷に認められるような方法でテレメトリを収集し、検証する必要はない。一方、法執行機関による捜査段階では、第 6 章で述べるように、証拠が適切に収集されるよう適切な措置を講じる必要がある。従って、検知に使用できるテレメトリが必ずしも証拠として認められるわけではない。このような問題は、各組織のフォレンジック準備計画において考慮される必要がある。

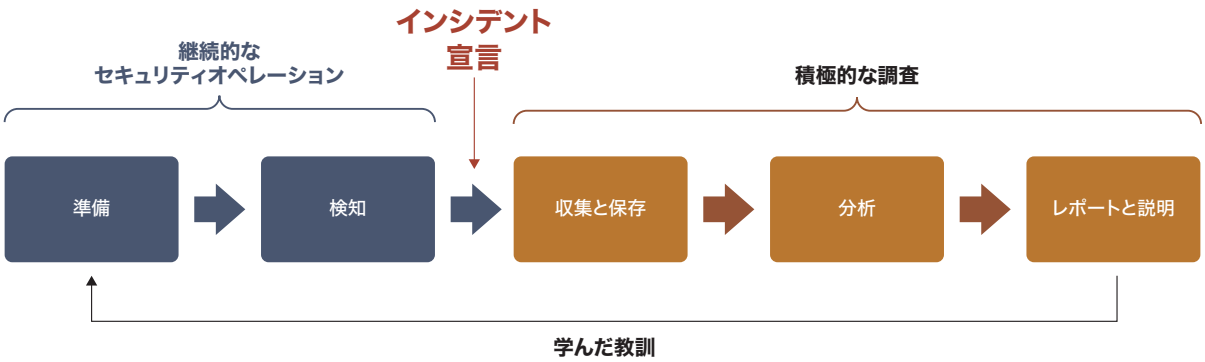


図 7-2. DFIR プロセス

脅威インテリジェンス（TI）

TI またはサイバー脅威インテリジェンス（CTI）は、脅威の実行者とその動機、目的、ターゲット、および手法に関連する収集、処理、分析されたデータから得られる情報である。TI は、組織がサイバーインシデントやサイバー対応型犯罪に備え、防御し、対応することを可能にする。

図 7-3 に示すように、TI のライフサイクルは、収集するインテリジェンスの種類を特定することから始まる（計画と指示の段階）。次に、収集の段階で生データが収集される。**生**データは、数字、文字、図、画像、音声などを通じて、実証された事実を示しているに過ぎない。これらのデータポイントは、組織の外部または内部、あるいは公開または非公開など、さまざまなソースから取得できる。しかし、生データは直接利用できるものではなく、**情報**を抽出するには、データを処理し、変換し、構造化し、濃縮するために、さまざまなテクニックを使用しなければならない。その際、分析手法を適用できるように情報を処理しなければならない（処理段階）。処理段階では、手作業による処理やキュレーションから、自然言語処理や機械学習技術まで、さまざまな手法が導入される。情報が処理されると、情報の分析（分析段階）によって**知識**が生成され、パターン、傾向、洞察が特定され、組織のさまざまな機能によって普及されて利用できるようになる（普及段階）。最後に、情報に基づいた意思決定と行動を行うための**叡智**、つまりより高いデータ品質を実現できる。これらの概念は、図 7-4 のデータ情報知識知恵ピラミッド（DIKWP）にも示されている。また、調査のある段階で脅威インテリジェンスを収集し、後の段階で使用することができることも注目に値する。

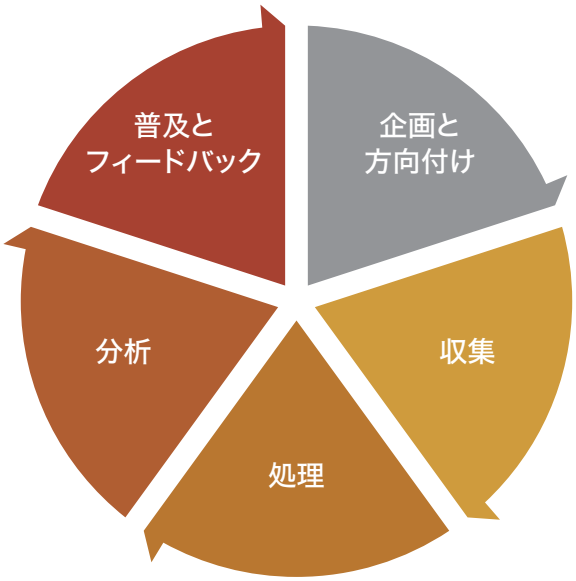


図 7-3. 脅威インテリジェンスのライフサイクル

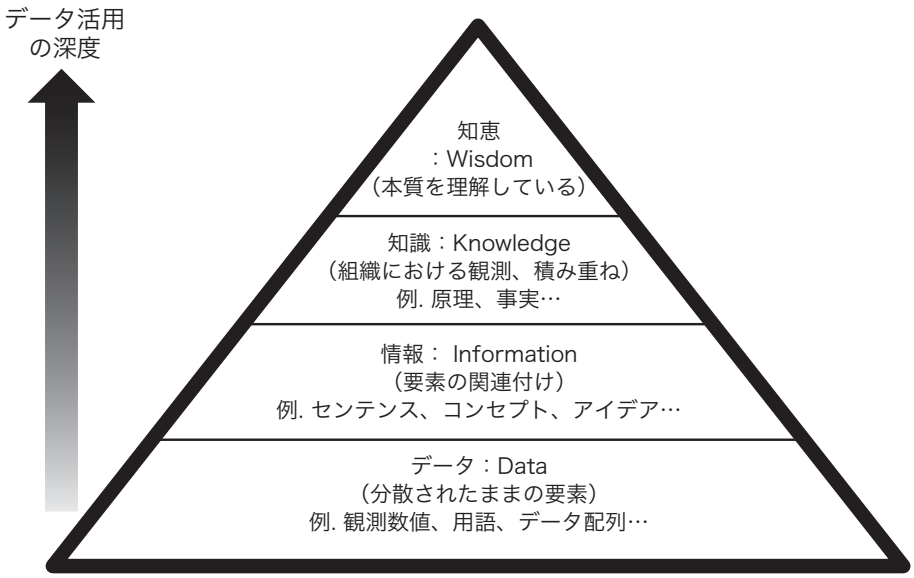


図 7-4. DIKWP ピラミッド

前述したように、脅威インテリジェンスは内部または外部ソースに由来する。内部情報は、過去または現在のインシデントや調査、収集された証拠、または組織に関する既存の知識から生成されることがある。外部のインテリジェンスは、一般に公開されているものから入手することも、独自の／商業的なプラットフォームから入手することもできる。外部情報は通常、企業にとってあまり重要ではない多様な情報を提供する。たとえば、同様のインシデントが同様の（ただし同一ではない）組織に影響を与えた場合などである。一方、内部情報は、より忠実で質の高い、少量の情報を提供する傾向がある。しかし、企業に直接関連し、フォレンジック調査や企業全体の姿勢に大きな利益をもたらす可能性のある外部インテリジェンスが 1 つある。それはブランドインテリジェンスである。ブランドインテリジェンスとは、漏えいした認証情報、侵害された資産、期限切れの証明書、データ漏えいなど、企業に直接影響を与えるリスクについて外部インテリジェンスを監視するプロセスを指す。

TI は、不正アクセスのインジケーター（IoC）、戦術・技術・手順（TTP）、および状況の 3 種類の情報に分類できる。IoC とは、システムが侵害された可能性があることを示す情報の断片を指す。IoC は

外部から入手することも、内部調査中に特定することもできる。IoC は、悪意のあるファイルやネットワーク接続のハッシュから、脅威の行為者が特定の目的で使用する既知の悪質な IP やレジストリキーまで様々である。このような指標の価値は時間の経過とともに薄れていくことに注意することが重要である。捜査官や分析官は、常に批判的思考を働かせ、各 IoC に利用可能な特性を利用して、それが調査に適用できるかどうかを判断すべきである。たとえば、調査中のインシデントの 1 年前に IP が悪意のあるものとして特定されていた場合、IoC の価値は低くなる。

各 IOC は、さまざまなプロパティに関連付けられている。IoC には複数の形式が提案され、使用されている。捜査官・調査員は、包括性を保証するために、いくつかの形式を組み合わせて使用すべきである。一般的な IoC の形式には以下のものがある。

- **STIX（Structured Threat Information eXpression）**（脅威情報構造化記述形式）
- **MISP（Malware Information Sharing Platform & Threat Sharing）**（マルウェア情報共有プラットフォームと脅威共有）
- **YARA（Yet Another Recursive Acronym）**（マルウェアを識別して分類する方法の 1 つ）
- **CybOX（Cyber Observable eXpression）**（サイバー攻撃観測記述形式）
- **OpenIOC（Open Indicators of Compromise）**（オープンな不正アクセスのインジケーター）
- **TAXII（Trusted Automated eXchange of Indicator Information）**（信頼できる指標情報の自動交換）

戦術、技術、手順（Tactics, Techniques, and Procedures：TTPs）は、サイバーセキュリティに導入された軍事・諜報分析に由来する用語である。**戦術**とは、脅威の行為者の戦術的目標、つまり彼らがなぜ行動を起こすのかを指す。**技術**は活動の実行方法を表す。例えば、脅威の行為者は既存のコマンドアンドコントロールチャネルを使用してデータを流出させるかもしれない。**手順**は、技術の特定の実装を記述するために使用される。TTP の知識ベースとして最もよく知られ、利用されているのは、マサチューセッツ工科大学（MIT）が 2013 年に発表した MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）[248] である。

状況インテリジェンスは、時系列で観察される傾向や地政学的状況などの抽象的な情報を表す。

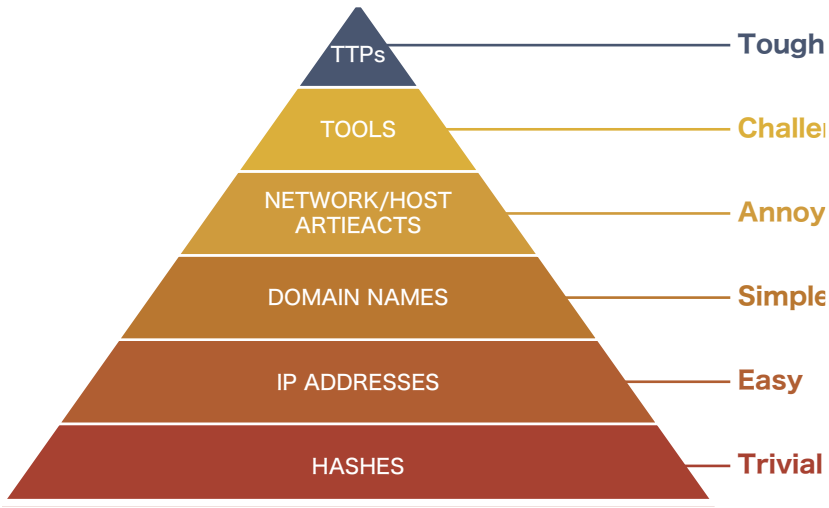


図 7-5. 痛みのピラミッド

248 https://attack.mitre.org/

しかし、すべての種類のTIが同じ価値を持つわけではない。デビッド・J・ビアンコ（David J Bianco）が作成した**「痛みのピラミッド」**[249]（図7-5）は、さまざまな種類の指標や知識が、いかに価値、適用可能性、調達や変更の難しさにおいて異なるかを表している。これは、ある種類のインジケーターが他のインジケーターより優れているということを意味するものではない。それぞれのインジケーターには長所と短所があり、さまざまな機能に応じてさまざまな方法で使用されることを意図している。

具体的には、ピラミッドの下位レベルは、ハッシュ値やIPアドレスなど、収集は簡単だが価値の低い指標を含んでいる。これらの指標は識別しやすいが、その価値は簡単に失われてしまう。たとえば、攻撃者は悪意のあるファイルのハッシュを変更するだけで、インジケーターを無効にすることができる。ピラミッドの中央には、ネットワークとホストのアーティファクトとツールが含まれる。前者は、ネットワークプロトコル、ユーザーエージェント、レジストリキーまたはディレクトリを含む場合があり、一方、後者は、横方向の移動、データの流出などのさまざまなタスクを達成するために脅威の行為者が使用する実際のツールとユーティリティを含む。このような指標は分析が必要なため収集が難しく、また、新しいツールの購入や開発、普及のための新しい作戦などに資金や時間などのリソースを必要とするため、修正も難しい。

TTPは、犯罪者が使用する可能性のある技術的な詳細だけでなく、全体的な方法、目的、目標も表すため、収集するのが最も難しい指標としてピラミッドの頂点に位置する。説明したように、TIはあらゆる組織のさまざまな業務や活動に適用できる。さまざまな種類の脅威インテリジェンスは、それぞれ異なる機能をサポートすることができ、運用的、戦略的、技術的、および戦術的の4つの機能カテゴリに分類することができる。

- **技術的インテリジェンス**は、IoCや脆弱性などの情報に重点を置いている。これは主に、SOC（セキュリティオペレーションセンター）やその他の技術チームが検出、分析、対応に使用することを目的としている。
- **戦術的インテリジェンス**は、新たな脆弱性など、即座に対策を講じる必要のある緊急の脅威を表す。
- **運用上のインテリジェンス**は、ピラミッドの上位レベル、すなわちTTPの情報に焦点を当てている。この種のインテリジェンスは、脅威ハンターやコンテンツ開発者からフォレンジック捜査官まで、さまざまな機能によって消費される場合がある。
- **戦略的インテリジェンス**は、状況インテリジェンスや新たな脅威や傾向を含む、脅威の状況に関するより広い見地を表す。組織の利害関係者がンテリジェンスに基づいた意思決定を行い、組織のリスクマネジメントをサポートすることができる。

調査におけるデータ要素

フォレンジック調査とサイバーセキュリティの検出および対応機能との間には、根本的な違いがある。フォレンジック調査における出力と方法論は、法廷に提出できる形で文書化される必要がある。本項では、表7-1に示すように、完全または部分的なデジタル犯罪捜査・調査に含まれる最も重要なデータ要素を示す。IoCとしてのデータの蓄積は、これらすべての要素にとって不可欠である。

249 https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

表 7-1. IOC として蓄積されたデータ要素

IOC として蓄積すべきデータ要素	
被害者プロフィール（Victimology）	被害者はなぜその犯罪において被害に遭ったのか
	被害者は加害者に知られていたのか
	被害者が犯罪被害の標的となり得る可能性は何かあったのか
	犯罪者がこの犯罪におよんだ場合にどのようなリスクをとることになるのか
犯行現場の指標（Crime Scene Indicators）	犯行現場
	犯行時刻
	クライムウェア
フォレンジックによる発見（Forensic Finding）	データフォレンジック
	アプリケーションフォレンジック（含むリバースエンジニアリングの結果）
	ネットワークフォレンジック

●被害者プロファイル

「**被害者プロファイル（Victimology）**」は、被害者に関するプロファイル情報である。なぜ、被害者が犯罪の標的となったのか考察することが重要である。サイバー犯罪によるデータまたはインフラの破壊が行われた場合には、標的となったデジタル資産を含め記録する必要がある。被害者プロファイルに注目することで、捜査官・調査員は標的とされた理由の評価が可能となり、犯罪者の動機につながる情報を得ることができる。また、被害者に関する情報を収集することで、捜査官・調査員は被害者のプロファイルを脅威の行為者のプロファイルや TTP と関連付けることができる。これにより、リソースの使用効率を高め、対応に必要な時間を改善し、帰属をサポート（リソースの使用状況や影響の特定を容易に）することができる。

サイバー犯罪を分析する際に特に重要なのは、以下の 4 つの質問である。

1. 被害者はなぜ被害に遭ったのか
2. 被害者は加害者に知られていたのか
3. 被害者が標的にされた可能性はあるか
4. 加害者はこの犯罪を犯すに当たりどのようなリスクをとることになるのか

なお、ベンジャミン・メンデルソーンは、被害者の「**有責性（Culpability）**」に基づく分類方法[250]を表 7-2 のとおり示している。

表 7-2. 被害者の「有責性（Culpability/Culpabilité）」に基づく分類方法

責任制の重さ	概要
完全に責任のない被害者	嬰児殺害や嬰児誘拐における嬰児、無差別爆破事件の巻き添えなど
責任の少ない被害者	犯罪場面に消極的に参加している。侮辱し心理的苦痛を与えて加害者の害意を誘発した被害者、危険を容易に察知して逃げられたはずであるにも関わらず犯行地に赴いた強姦の被害者など
加害者と同程度に責任のある被害者	自発的に犯罪場面に参加している。嘱託・承諾殺人における被殺者、喧嘩口論で互いに挑発し合った結果の殺傷事件の被害者など
加害者よりも責任のある被害者	被害者の挑発が加害の主たる要因と認められる。相手方の家族を殺すなどと脅したために攻撃された殺傷事件の被害者など
最も責任のある被害者	不法な攻撃を加えたため正当防衛にあって殺傷されたものなど

250　ベンジャミン·メンデルソーン、「生物心理社会科学の新たな分野:被害者学」、国際犯罪学および警察技術レビュー、第10巻、1956年、95-109ページ。

●犯行現場のインジケーター

「**犯行現場のインジケーター（Crime Scene Indicators）**」は、犯行現場を構成する要素である。捜査官・調査員は犯行現場を押さえたとき、注目すべきポイントを理解することが重要である。

✓ **犯行現場：**

多くのサイバー犯罪は、各分野の専門家を使った分業体制で成り立っている。その結果、1つのインシデントが複数の分野関係していることがある。例えば、マルウェアによる不正情報売買事件では、マルウェアの開発拠点、マルウェア配布の踏み台となる改ざんされたウェブサイト、マルウェア拡散を目的としたスパムメールの悪質な配信に利用されたボットネット、犯人が利用するC2サーバー、マルウェアに感染したホストコンピュータ、コンピュータから盗み出された情報が売買される市場などが明らかになる。これは、評価すべき犯罪現場が少なくとも6箇所あることを意味する。

サイバー犯罪捜査官・調査員は、物理的な場所を完全に把握するだけでなく、デジタル識別情報（MACアドレス、IPアドレス、デジタル証明書、URL、ネットワークアドレス、インターネットサービスプロバイダなど）、犯罪現場で発見されたサービスの特徴（無料、有料、利用登録に必要な情報など）を収集して記録すべきである。

✓ **犯行時刻：**

犯行時刻からは、犯罪者の動機や行動パターンに関する洞察を得ることができる。また、時系列を評価することで、犯罪者の習熟度や犯罪に関するリスク、さらなる証拠入手の可能性などを把握することも可能である。

サイバー犯罪捜査官・調査員が犯行時刻を特定するにあたって有益なのは、ログである。ログは、コンピュータのセキュリティに関する情報を含む「セキュリティソフトウェアログ」、システムの使用状況ログを含む「オペレーティングシステムログ」、および「アプリケーションログ」に分けることができる。

ソフトウェアのログを扱う際には、タイムスタンプの不一致の可能性を考慮すべきである。ソフトウェアログは、すべてのログ項目のタイムスタンプを設定するために、それらが保存されているホストコンピュータの時計を参照する。したがって、ホストコンピュータの時計が不正確であれば、ログのタイムスタンプも不正確になる。特に、複数のホストから取得したログを分析する際にタイムスタンプに矛盾がある場合、捜査官・調査員が注意しないと、インシデントに関する調査の洞察が的外れになる可能性がある。

犯行時刻に関連する追加情報は、マルウェア解析やコンピュータフォレンジックによって得られるかもしれない。

✓ **クライムウェア：**

「**クライムウェア（Crimeware）**」とは、犯罪行為のために作成または使用されるソフトウェアの総称である。よく知られた例としては、不正または有害な行為を行う意図で作成された悪意のあるソフトウェアである「**マルウェア（Malware）**」がある。しかし、サイバー犯罪において考慮すべきソフトウェアはマルウェアだけに限らない。捜査官・調査員は、合法的な目的で作成されたソフトウェアやオペレーティングシステムに属するソフトウェアが犯罪行為に悪用される場合もあることを考慮する必要がある。したがって、サイバー犯罪捜査官・調査員はまず、捜査・調査対象のクライムウェアが以前から犯罪現場に存在していたものなのか、それとも犯人が持ち込んだものなのかを特定しなければならない。

例えば、ネットワークへの侵入に成功した犯罪者は、侵入したホストコンピュータから情報（プロセス情報、ネットワーク情報、OS情報）を収集するために、タスクリスト、ver、

ipconfig、systeminfo といった WindowsOS の標準コマンドを使用する。これらは犯罪者が持ち込んだソフトウェアの断片ではなく、犯罪現場にもともと存在していたフトウェアの断片である。この手法は "Living off the Land（LotL）" と呼ばれ、犯罪者が自分の行動を合法的な活動に混ぜ込み、より長く発見されずに済むためによく使用される。

さらに重要な傾向として、最近のソフトウェアは必ずしもホストコンピュータでマネジメントおよび使用されるわけではなく、クラウドベースであることが多い。**「クラウドコンピューティング」**は広く普及しており、インターネットなどのネットワークを通じて利用されるサービスを含んでいる。最も一般的な 4 つのクラウドコンピューティングサービスは、"Software as a Service"（SaaS）、"Platform as a Service"（PaaS）、"Infrastructure as a Service"（IaaS）および "Function as a Service"（FaaS）である。クラウドコンピューティングの種類によって、制御と所有権のレベルは異なる。そのため、捜査官・調査員は対応する証拠を収集および分析するためのクラウド技術を理解し、その限界を考慮することが重要である。

捜査官・調査員は、クラウドコンピューティングへの物理的なアクセスが不可能なために識別が困難なケース（犯罪現場で証拠が残らない）に加えて、クラウド環境で使用されているソフトウェアがクライムウェアとして悪用されるケースに遭遇する可能性がある。このような困難な状況でも、クラウドサービスにアクセスしたブラウザのキャッシュ情報や、クラウドコンピューティングアクセスのためにホストコンピュータに生成される一時ファイルによって、正確な再現と分析が可能になる。正規の手続きとして承認される方法を通じて IoC を取得することも可能である。さらに、ソフトウェアを構成するプログラムの分析を通じて、さらなる IoC を得ることも可能である。これらの方法の具体的な詳細については、後述の「フォレンジックによる発見 - アプリケーションフォレンジック」の項を参照のこと。

●フォレンジックによる発見

「フォレンジックによる発見」とは、犯罪の発生を法的に証明するために、犯罪に関連する「物的証拠」を分析する際に得られた発見を指す。この発見は、「被害者プロファイル」と「犯行現場のインジケーター」を補足するデータとなる。これは犯罪の特徴に関する客観的事実を実証し、検証された IoC となり、最高の評価を受ける。

一連の発見に対しては、厳格なデータ保護と CoC を通して情報の整合性を保護することが不可欠である。

デジタルフォレンジックは、分析対象となるデータに応じて 3 つのカテゴリに分類できる。

✓データフォレンジック：

分析対象は、デジタル機器（モバイルデバイスや IoT デバイスを含む）で使用されるファイル記憶媒体、ファイルシステム、またはファイルである。データを分析する際にはファイルシステムを考慮する必要があり、削除されたファイルや既存のファイルの履歴データを保存することができる。このデータは、サイバー犯罪捜査にとって極めて重要な情報を含んでいる可能性がある。

✓メモリフォレンジック：

分析対象は、特定の時点でデジタル機器から収集されたメモリダンプである。メモリダンプは、アクティブなプロセスやネットワーク接続から、プロセスに注入されたマルウェアや暗号鍵まで、さまざまな情報を含んでいる。メモリは揮発性であるため、データを保持するためにはできるだけ早く回収することが重要である。

✓クラウドフォレンジック：

分析対象はクラウド環境である。場合によっては、クラウドフォレンジックには、この項で述べたフォレンジックの調査結果や手順が1つ以上含まれる。例えば、クラウドでホストされている仮想マシンのファイルディスク解析や、クラウド固有のログが含まれる。同様に、クラウド環境からの認証ログもアプリケーションフォレンジックと見なすことができる。いずれにせよ、クラウドフォレンジックスは、クラウドコンピューティングの利用が増加していることや、それに伴う課題があることから、フォレンジック準備において特別なカテゴリとして考慮すべきである。

✓ **アプリケーションフォレンジック：**

分析対象はOSを含むプログラムである。分析中は関連データの揮発性を考慮する必要がある。揮発性データは時間の経過とともに変化する可能性があるため、収集中は順序と時系列が重要になる。

さらに、表7-3に示す3つの方法を使用してソフトウェアを構成するプログラムを分析すると、捜査官は新しいIoCを発見できる可能性がある。

表 7-3. プログラムの解析手法

解析手法	詳細
表層解析	プログラムを実行せずにファイルに記録された情報の確認
動的解析	プログラムを実際に実行し、デバッガなどのツールを併用しながらその動作を確認
静的解析	ソースコードを解析する 逆アセンブル、逆コンパイルなどリバースエンジニアリングの手法によってコードレベルで機能を確認

これら解析手法によって得られるIoCとして、プログラムの重複実行を防止するMutexや、C&Cとしてターゲットにしている URL、ブラウザの通信を偽装するようなHTTPリクエストの文字列、サーバーを偽装するようなHTTPレスポンスの文字列といったプログラムとして機能するための情報が挙げられる。

また、プログラムがコンパイルされた時刻が特定できれば、犯行が計画された時刻や犯行が行われた時間帯（犯行場所）を推測できる可能性がある。さらに、（プログラム内のASCII文字として抽出された）文字列情報を分析することで、犯人の開発環境や使用言語（コンピュータ言語または会話における話し言葉）など、犯人の身元に関する仮説を立てることができる。

✓ **ネットワークフォレンジック：**

分析対象は、ネットワークを通過するパケットである。このデータを分析する際には、各TCP/IPプロトコルなどのプロトコルスイートのレイヤー構造を考慮しなければならない。多くの場合、関連する活動は、ユーザー（被害者または犯罪者）に最も近いレイヤー、つまりアプリケーションレイヤーで発見される。

分析フレームワーク

分析フレームワークでは、「データモデリング（Data Modeling）」、「データマイニング（Data Mining）」、「抽出・変換・ロード（Extraction, Transformation, and Loading）」、「データ品質テスト（Data Quality Testing）」、「自動化（Automation）」、「品質保証と品質マネジメント（Quality Assurance and Control）」の定義を扱う。

サイバースペースへの依存度が高まっている現代の世界では、サイバー犯罪だけでなく従来の犯罪においても入手可能な電子データの多様化が進んでいる。このような環境では、データ分析を担当するリサーチャーは、科学的な「分析フレームワーク」を用いて、大量のデータの中から価値のあるデータを見つけ出さなければならない。サイバー犯罪捜査・調査において分析フレームワークを活用することで、犯罪の背景にある主な要因を特定することができる。その結果、情報に基づく意思決定サイクルが確立される。

データモデリング

「データモデリング（Data Modeling）」とは、定義されたルールに基づいて、データを一連のオブジェクト（データベースではテーブル自体をオブジェクト、列を項目、行をレコードと呼ぶことが多い）とそれらの相互関係として構造的に表現する技法を指す。このプロセスには、エンティティ（データモデルの構成要素のひとつ）、属性、エンティティ間の関係、および制約の定義が含まれる。

警察活動においては、捜査活動全体を支援する目的で、データに基づくデータモデリングを実施すべきである。これは、捜査官が「脅威の行為者」に関する仮説を立て、彼らが行う「活動」の因果関係を推論するのに役立つはずである。データモデリングは、捜査官がこれまで不明だった関係性を特定し、さらに効率的な方法で処理と視覚化を行うのにも役立つ。ただし、モデリングは調査の技術的な分析に限定されるものではない。モデリングは、予算計画や警察政策などの分野でマネジメント者が活用することもできる。

表 7-4 は、警察活動においてデータモデリングを行うことにより得られるメリットを示している。

表 7-4. データモデリングにより警察活動にもたらされるメリット

捜査活動の最適化	最適な資源の割り当て
	捜査範囲の評価と優先順位付け
事件の解決	「脅威アクター（Threat Actors）」の推定や、逮捕
	犯罪者の起訴
治安の向上	市民に対する情報提供と啓発
	危険予測地域に対する巡回強化
将来に向けた犯罪予防	必要となる資源の計画
	効果的な戦略と戦術の開発
	政策提言

●データ種別

犯罪捜査ではさまざまなデータが扱われるが、データは大きく分けて「**構造化データ（Structured Data）**」、「**半構造化データ（Semi-structured Data）**」および「**非構造化データ（Unstructured Data）**」の 3 つに分類することができる。

表 7-5. 構造化データ（Structured Data）、半構造化データ（Semi-structured Data）および非構造化データ（Unstructured Data）

構造化データ	あらかじめ定義され、構造化された形式で編成されたデータ。このような形式の例としては、データベースやスプレッドシートがあり、これらはすべて分類された要素を持ち、それらの要素間の関係を定義することができる
半構造化データ	データベースのような正式な構造で整理されてはいないが、階層構造やある程度の構造に従っているデータ。半構造化データの例としては、XML ファイルや JSON ファイルなどがあり、様々なシステムのイベントロギングによく使用される
非構造化データ	構造化された形式でフォーマットされておらず、定義された方法で処理できないデータ。例としては、ドキュメント、電子メール、写真、ビデオなどがある

例えば、麻薬密売人が逮捕され、彼のコンピュータが押収されたとしよう。コンピュータ上の電子メール記録（非構造化データ）を分析した結果、いくつかの不審なやり取りが特定された。さらに、押収されたコンピュータから削除されたファイルの復元も試みられる。その結果、日付、名前、価格を示すスプレッドシート（構造化データ）が発見される。そうすれば、薬物の販売ネットワークを特定するための作戦を拡大することが可能になる。

構造化データや半構造化データは、その構造上、様々な方法で容易に処理することができるが、非構造化データはその逆であることがわかる。従って、コンピュータ上で文書や情報の意味を正確に解釈するためには前処理が必要であり、これはデータを整理する前に行わなければならない。非構造化データの処理をサポートする方法は、下記のように多数ある。

- **メタデータの抽出**：メタデータはデータそのものではなく、対象データに関する情報を記述した関連情報である。メタデータの種類と例を表 7-6 に示す。

- **テキストマイニング**：テキスト分析とも呼ばれるテキストマイニングは、洞察と情報を抽出し、その後このリストの他の方法を使用してさらに処理することを目的としてテキストデータを処理することを含む。

- **画像とビデオの分析**：これは、構造化データを抽出して解釈するための画像とビデオの処理に重点を置いている。画像とビデオの分析には、光学文字認識（OCR）、画像分類、オブジェクト検出などの技術が含まれる。

- **オーディオ分析**：オーディオと話し言葉を処理し、その後、音声認識やオーディオ分類などの他の方法を適用してさらに分析する。

- **自然言語処理（NLP）**：これは、人間と同じように「理解」することを目的とした言語分析に焦点を当てたものである。NLP はテキストマイニングとともに広く使われているが、この種のデータに限定されるものではなく、画像や音声など他の前処理済みデータにも適用できることに留意すべきである。**感情**分析や固有表現抽出（NER：Named Entity Recognition ）など、その他のタスクも NLP に含まれることがよくある。

- **機械学習とデータマイニング**：これらの分野はどちらもアルゴリズムを使用してデータを分析および抽出する、機械学習はデータから学習して予測や決定を下すことを目的としており、データマイ

ニングはデータを探索し、パターンを発見し、情報を抽出することを目的としている。どちらの分野も、非構造化データ分析の他の多くの手法をサポートしており、この項の後半で説明する。

表 7-6. メタデータの種類

メタデータの種類	詳細	例示
システムメタデータ	ファイルシステムが扱う種類やサイズ、作成日、所有者、アクセス権といった情報	• デジタル写真ファイルにおける Exif • Microsoft Office ファイル（Word / Excel / PowerPoint）におけるプロパティや個人情報
カスタムメタデータ	データに付随する日時、宛先などの情報	• 通話記録、電子メールにおける「To」や「From」 • 通話記録における通話時間 • 携帯電話における IMEI 情報
リッチメタデータ	画像からの OCR や、音声からの音声認識によりテキストに変換された情報	• 通話音声をテキスト化した情報 • 画面キャプチャに含まれるテキスト情報

データの保存とマネジメント

データの保存は、フォレンジック調査だけでなく、情報システム全般にとって重要な部分である。データレイクとデータウェアハウスの両方を、この目的のために使うことができる。主な違いは、データレイクが生の非構造化データの保存を可能にするのに対し、データウェアハウスは事前にクリーニング、変換、必要に応じて加工された構造化データの保存にしか使用できないという点である。本項では、データウェアハウスに焦点を当てる。というのは、データウェアハウスは、以下の理由により、捜査システムの要件をサポートするのに適していることが多いからである。

1. 履歴データマネジメントと傾向分析をサポートする能力
2. 構造化データのみを使用するため、データレイクと比較して分析（クエリ）性能が向上
3. 完全性と正確性の要件を満たすデータの一貫性と品質

「データウェアハウス」とは、複数の情報源から抽出・再構築されたデータを格納し、情報分析や意思決定に利用される大規模データベースのことである。提唱者であるウィリアム・H・インモン（William H. Inmon）は、データウェアハウスを「経営者の意思決定プロセスを支援するための、サブジェクト志向で、統合され、時間経過による変動がなく、不揮発性のデータの集合体」と定義している。

結果として、データウェアハウスの 3 つの主要な特徴は、「時間差異（時間の経過に伴う変化を包括的に把握できる）」、「主題指向」、「統合」である。システムのリソースには限りがあるため、1 つのシステムですべての犯罪に関連する「取引データ」を継続的に収集することは不可能である。そのため、現実のシステムを構築する際には、必要なデータを得るスピードを考慮した視点から、定期的にデータを絞り込んで収集するシステムを構築したり、作業の専門性などの効率性を考慮した視点から、個々の機能別にシステムを構築したりすることが一般的である。これらのタイプのシステムは利便性に優れている。

しかし、サイバー犯罪捜査が行われる現場では、長期的な視点で犯罪動向を分析しなければならない場合もある。このような状況では、過去のデータが含まれていないデータベースは犯罪傾向の分析には使用できない。したがって、データウェアハウスは過去のデータも逐次的に保存する必要があり、これを**「時間差異」**と呼ぶ。

さらに、サイバー犯罪捜査のデータベースは分類によって構築される。これは、「IP アドレス」、「URL」、「WHOIS」、「マルウェアハッシュ値」などの各 IoC に加えて、「脅威の行為者」、「手口」、「TTP（戦術、技術、手順）」のデータベースの構築を必要とする。システムごとにデータ形式やシリアルナンバーなどが異なるため、そのままでは使用できない。そのため、これは「事件」や「犯罪グループ」などの種類ご

とに統合されている。データウェアハウスでは、これは**「サブジェクト指向」**の構成である。最後に、異なるシステムに分散しているデータを１つのデータベースに集めて結合することを**「統合」**と呼ぶ。

データウェアハウスにデータを保存するための手法は**「ETL（抽出、変換、ロード）」**と呼ばれる。ETL は、NIBRS（National Incident-Based Reporting System）などのソースからデータを**「抽出」**し、必要に応じて**「変換」**し、データウェアハウスなどのターゲットシステムに「ロード」する連続的なプロセスである。操作の順序により、ETL プロセスの最後にあるデータはすべて構造化されているため、データレイクではなくデータウェアハウスにデータを保存するのが最適な選択であることに注意する。

●抽出

「抽出」プロセスでは、データをシステム（情報源）から抽出し、処理可能な状態に変換する。このプロセスはインスタンス化と呼ばれる。インスタンス化によって、フィールドのタイプや値などの情報がインポートされ、それを指定することができるようになる。モデリングを用いた意思決定やデータ収集の結果、データ抽出が見直されることがある。

犯罪捜査における情報源としては、インシデントデータ、関係機関からの報告書データ、所轄データ、個人データのほか、犯罪歴などの組織に関わるデータ、警察活動から得られるデータなどがあり、組織によっては「RMS（記録マネジメントシステム）」などのデータベースに蓄積されるデータもある。犯罪捜査における具体的な情報源については、「第５章 証拠の情報源」を参照のこと。

- ✓インシデントデータ：「事件犯罪報告書（Incident Crime Report）」、「逮捕報告書（Arrest Reports）」、および「出動要請記録（Call for Service Records）」
- ✓関連組織からの報告データ
- ✓所轄データ
- ✓犯罪歴など個人または組織に関するデータ
- ✓警察活動を通じて得られたデータ

●変換

「変換」プロセスでは、複数の情報源から抽出されたデータが結合され、一定のルールに従って処理され、不正な場合は拒否される。このプロセスは、データの選択、整理、コンパイル、結合、および書式設定を含む。

- ✓異なるシステムのデータを統合
- ✓フィールド値の異なる型の統一
- ✓欠損値、不正な値、または極端な値の定義
- ✓データの選択
- ✓分析に必要な形式にデータを再構成
- ✓関連フィールドを変換する

●ロード

「ロード」プロセスでは、「変換」プロセスで作成されたデータファイルがデータウェアハウスにインポートされる。このプロセスによって、情報分析と意思決定のためのデータベースが作成されることになる。

機械学習とデータマイニング

「機械学習」と**「データマイニング」**は、どちらも大規模なデータセットの分析をサポートし、科学捜査の効率を高める分野である。これらの用語は混同されることが多く、性質は異なるが、組み合わせると相乗的に機能する。**「機械学習」**は、アルゴリズムを使用して（トレーニングして）データから学習し、高い精度で予測および分類する人工知能の分野である。これにより、このようなアルゴリズムは、明示的なプログラミングを必要とせずに、予測や行動を起こすことができる。機械学習アルゴリズムはさまざまな種類の分析に利用され（多くはこの章の前半で説明されている）、その 1 つがデータマイニングである。これについては後ほど詳しく説明する。

機械学習では、アルゴリズムはデータセットでトレーニングされる。データセットには、各データポイントに出力ラベルが割り当てられている「ラベル付き」のものと、「ラベルなし」のものがある。モデルはデータから学習する「トレーニング」段階を経てから、別のデータセットに対して性能を評価される。機械学習アルゴリズムの最も一般的なタイプを表 7-7 に示す。

表 7-7. 共通機械学習アルゴリズム

モデル名	得られる結果
教師あり学習	モデルはラベル付けされたデータで学習され、分類などのアプリケーションに使用される
教師なし学習	モデルは、パターンや構造を特定する目的で、ラベル付けされていないデータに対して学習される。クラスタリングや異常検知は教師なし学習の一例である
半教師あり学習	教師ありモデルと教師なしモデルの利点を活用するために、ラベル付けされたデータとラベル付けされていないデータの両方がトレーニング中に使用される
強化学習	強化は、報酬やペナルティを与えるフィードバックループ（エージェント）を含む。モデルは「試行錯誤」方式で学習する
ディープラーニング	ディープラーニングは、生物学にヒントを得た多層構造の人工ニューラルネットワーク（ディープネットワーク）を使用する。画像処理、自然言語処理（NLP）、大規模言語モデル（LLM）などがディープラーニングの応用例である

「データマイニング」とは、データを探索し、有用な洞察やパターンを掘り出す技術である。データ分析を担当する捜査官は、統一性のない大量のデータを、より使いやすい形式に変換し、統計に基づくツールを用いてデータと隠れたインジケーターとの相関関係を発見することで、犯罪捜査を支援して貢献する。

分析モデルを用いたデータマイニングでは、事前に仮説を立てて必要なデータを収集することで分析を行う。次に、検証を予測事象と組み合わせ、適切な解析モデルを選択する。表 7-8 はデータマイニングで使用される分析モデルを示している。さらに、使用されるツールを表 7-9 に示す。

表 7-8. データマイニングにおける代表的な分析モデル

モデル名	得られる結果
相関分析・アソシエーション分析（Association Analysis）	X が起きるときには Y も起きやすい
クラス分類（Classification）	X の属性から、そのクラス C を予測
クラスタリング（Clustering Analysis）	似ているもの同士を集約する
回帰分析（Regression Analysis）	X の属性から、数値変数 Y を予測
異常または外れ値の検出	予期しない観察、つまり他のデータポイントとは著しく異なるデータポイントを特定する

表 7-9. データマイニングにおいて使用されるツール

ツール名	詳細
データビジュアライゼーション **・ヒストグラム** **・散布図**	データの傾向または分布を把握し、外れ値の有無を確認するとともに、最適な分析手法を決定し、図形やグラフィックの形式でレポートを作成する
多様なデータへの対応 **・テキスト解析（Text Analysis）、形態要素解析（Morphological Analysis）** **・空間分析（Spatial Analysis）** **・パターン認識（Pattern Recognition）、画像処理（Computer Vision）**	非構造化データを調べ、捜査における重要なインサイトを導き出す

これに対して、機械学習を用いたデータマイニングでは、事前の仮説は必要ない。その代わりに、コンピュータはデータから学習し、相関関係を導き出す。機械学習で得られた分析結果から新たな考察や示唆を得ることは難しいが、スパムメールの判定やクレジットカードの不正利用の検知など、自動化が求められる分野ではすでに活用されている。機械学習は、分類、再帰、クラスタリング、ルール抽出などの犯罪捜査分野での活用が期待されている。

データマイニングと機械学習はどちらも、画像やドキュメントの処理から認証やアプリケーションログの動作分析まで、さまざまなタスクに使用できる。これらは、さまざまな方法でフォーマットされたデータや欠落したセグメントで構成されている場合であっても、捜査官が大規模なデータセットからデータを分析し、洞察を特定したり、イベントを再構築したりするのに役立つ。ただし、これらの分析モデルとツールを通じて得られた結果をすぐに信頼すべきではないことに注意することが重要である。発見された結果は「正確性」、「信頼性」、および「実用性」の観点から検討する必要がある。

データビジュアライゼーション

データビジュアライゼーション、またはグラフビジュアライゼーションは、調査結果の分析と解釈において強力なツールとなりうる。データビジュアライゼーションとは、データとその中の関係を表すチャートやグラフを構築することを指す。データビジュアライゼーションにより、捜査官はパターンを特定し、攻撃やデータの欠落が及ぼす影響を理解することができる。チャートやグラフの一般的な例をいくつか下記に示す。

- **ノード**はネットワーク内のホストを、その状態（不正アクセスあり、不正アクセスなし、不明）に応じて色分けしたもので、ノード間のリンクは対応する証拠に沿った通信を表す。これらを記述したチャートやグラフなどを更新することで、捜査官はさらに不正サクセスされたホストや潜在的な横の動きを特定し、攻撃の影響を評価することができる。
- ユーザーログインと各ログインのソース IP アドレスはノードとして表され、各ユーザーはそのユーザーが認証した IP ノードにリンクされる。さらに詳しい情報は、IP の国によって異なる色でグラフやチャートに表示することができる。これによって捜査官は、基準外の国からログインしている異常値ユーザーや、多すぎる IP アドレスからログインしている異常値ユーザーを発見することができる。
- ノードは実体と証拠を表す。例えば、BEC（Business Email Compromise：ビジネスメール詐欺）の調査において、関係するユーザーと侵害の証拠をグラフやチャートで表現し、それらの関係をリンクで示すことを考えてみる。これにより、捜査官は調査結果を要約できるだけでなく、分析におけるギャップを発見し、仮説を構築することができる。

最後に、**タイムライン**はあらゆる調査の一部となるべきデータビジュアライゼーションである。タイ

ムラインは調査結果を時系列で表示する。これは、グラフビジュアライゼーションと同様に、分析の複数の目的を果たし、証拠と結論の提示にも役立つ。

データ品質テスト

「**データ品質検査（Data Quality Testing）**」とは、犯罪捜査の結果を精査し、その妥当性を評価するための測定を行うことである。

犯罪現場からは様々な種類のデータが提供される。代表的な例を下記に示す。

- CSV（Comma Separated Values）：複数のフィールドを区切り文字であるカンマ「,」記号で区切ったテキストファイルデータ
- TSV（Tab Separated Values）：複数のフィールドを区切り文字であるタブ記号で区切ったテキストファイルデータ
- Microsoft Excel/Access などのアプリケーションファイル
- Oracle Database/Microsoft SQL Server/MySQL などのデータベースファイル
- IBM i2/LexisNexis CaseMap などの分析ソフトウェアのデータファイル

データファイルの中には相互に互換性のある形式もある。いずれにせよ、捜査官にとって最初の仕事は、受け取ったデータファイルが読めるかどうかを確認することである。

次に、受信したデータの「**完全性（Integrity）**」をチェックしなければならない。代表的なチェック方法を表 7-10 に示す。

表 7-10. データの完全性を確認するためのチェック技法

チェック方法	効果
ニューメリックチェック（Numeric Check）	数値として扱う必要のあるデータに、文字など数値として扱えないものが含まれていないかをチェック
シーケンスチェック（Sequence Check）	対象とするデータが一定の順序でならんでいるかをチェック
リミットチェック（Limit Check）	データが適正な範囲内にあるか、上限値を超えていないか、下限値を下回っていないかをチェック
フォーマットチェック（Format Check）	データの形式が一定の形式に従っているかをチェック
照合チェック	登録済みでないデータの入力を避けるため、入力されたデータが登録済みのデータと一致するかをチェック
論理チェック	入力データが、関係する他のデータと矛盾がないかをチェック 貸借対照表（Balance Sheet）のように借方と貸方のそれぞれの合計が一致しなければならないデータにおいて、借方と貸方を個別に計算し、それぞれの合計が一致するかをチェック
重複チェック	一意であるべきデータなどが、重複して登録されていないかをチェック

●データの標準化

捜査を助けるためにデータ分析を開始する場合、捜査官とマネジメント者は、どのようなデータセットをどの程度の分析の対象とするかについて、あらかじめ合意しておくべきである。

計画段階では、指定された捜査シナリオに適合する傾向を特定するために、データを体系化し、科学的な分析フレームワーク内で整理する必要がある。これを「**データラングリング（Data Wrangling）**」と呼ぶ。

データを「**グループ化（Grouping）**」して「**要約（Summarization）**」することで、データ全体の概観を把握することができる。これにより、後から調査中に外れ値が見つかった場合でも、その概観を参考に

することができる。

分析の一貫性を確保するために、すべてのデータは標準化されなければならない。この目的のために、一部のデータフィールドの標準フォーマットへの変換が必要となる場合がある。いくつかの典型的なデータ形式を表 7-11 に示す。

表 7-11. データ型の一例

データ型名	特徴
連続型	0–100 のように、数値の範囲を記述する。連続値は、整数、実数、または日付 / 時間なども含む
カテゴリ型	値の数字が不明な場合に、文字列値に用いられる。インスタンス化されていないデータとも呼ばれる
フラグ型	true と false、Yes と No、0 と 1 など、特性の有無を示す 2 つの異なる値を持つデータで使用される
名義型	複数の異なる値を持つデータを記述するために使用される。それぞれの値は、「North/South/East/West」などのセットのメンバーとして処理される
順序型	LOW、NORMAL、HIGH などの固有の順位のある複数の値を持つデータを記述する

データの品質をチェックすると、場合によっては不整合が発見されることがある。このような不整合データを「削除」や「補完」などの手段で対処するプロセスを**「データクレンジング（Data Cleansing）」**と呼ぶ。

矛盾したデータは安易に削除すべきではない。というのは、数値の範囲外のデータであっても、意思決定のプロセスにおいては大きな意味を持つ場合があるからである。サイバー犯罪捜査に関連するデータの取り扱いにおいて、捜査官は違法取引の価値を扱っていることを常に念頭に置かなければならない。**「欠損値」**とは、一貫性のないデータのことで、特定のケースで特定の項目の値が欠損していることに起因する。この問題を解決する有効な方法は、欠損に至ったパターンを考察することである。典型的な欠損値構造を表 7–12 に示す。

表 7-12. 欠損値の構造

MCAR（Missing Completely at Random）（完全に無作為に欠損）	値がランダムに欠損している。他の値に依存せずに欠損している
MAR（Missing at Random）（無作為に欠損）	値が観測データに依存して欠損している
MNAR（Missing Not at Random）（無作為ではない欠損）	値が欠損データ自身に依存して欠損している

欠損値の状況については、「削除」か「補完」のどちらかの方法で対処しなければならない。MCAR の場合、各データポイントの損失確率は他のデータに依存しないため、欠損データを削除することができる。これに対して、MAR または MNAR の場合、削除を実行すると不均衡が生じるリスクがある。このような状況には、欠損値を補完することで対処する必要がある。

代表的な欠損値の削除または補完方法を表 7-13 に示す。

表 7-13. 欠損値の削除または補完方法

欠損処理		内容
削除	リストワイズ法	欠損値を持つサンプルの削除
	ペアワイズ法	相関係数や分散等の算出によって、2 変数のいずれかが欠損値を持つサンプルを削除
補完	単一代入法	平均値や他の変数による予測値を補完
	多重代入法	欠損値に代入したデータセットを複数作成し、各データセットに対して分析を実行し、その結果を統合することにより欠損値を補完
	完全情報最尤推定法 (Full Information Maximum Likelihood Method)	サンプルごとに欠損パターンに応じた尤度関数を仮定して最尤推定を実施し得られる多変量正規分布を用いて平均値や分散共分散行列を推定

「外れ値データ（Outlier Data）」とは、観測データや値から大きく外れた矛盾したデータの項目を指す。捜査官は、採用された値がどの範囲に入るかを決定しなければならない。これは、分析の結果得られた提案を反映した施策がどのようなユーザーをターゲットにしているか、また、結果を達成するためにどの程度の有効な分析が必要かによって決まる。

代表的な外れ値を検出するアプローチについて、表 7-14 に示す

表 7-14. 外れ値を検出するアプローチ

アプローチ	概要
統計に基づく方法 (Statistical Approaches)	データは統計的なモデルに従って発生すると考え、そのモデルに従わないデータを外れ値とする
空間的な近さに基づく方法 (Proximity-based Method)	他のデータと比べ、近傍点への近接度合いが著しく異なるデータを外れ値とする
クラスタリングに基づく方法 (Clustering-based Method)	データをクラスタリングする際に、小さいクラスターに所属するデータを外れ値とする

自動化

「自動化（Automation）」とは、コンピュータリソースを用いることによって、手作業の調査では実施しきれない量の情報について、複数の異なる分析フレームワークを実行し、異なる角度から分析を実行することである。

●データベース

データベースは分析フレームワークのインフラストラクチャである。データベースには、リレーショナル（RDBS）と非リレーショナル（NoSQL（Not only SQL））という 2 つの主要なカテゴリがある。非リレーショナルデータベースはさらにいくつかのカテゴリに分類できる。最も一般的なデータベースの種類を表 7-15 に示す。

表 7-15. データベースの種類

データベースの種類	データ保持形式	例
RDBS（リレーショナルデータベース）	表（行と列）	MySQL, PostgreSQL, Oracle
NoSQL データベース		
KVS（キーバリューストア）	キーとバリューのペア	Redis, DynamoDB
ドキュメント指向データベース	表（行と動的な列）	MongoDB, CouchDB
グラフデータベース	キーとバリューのペア	Neo4j, OrientDB
時系列データベース	キーとバリューのペア	Druid, eXtremeDB
ワイドバリューストア	行と列	Apache Cassandra, Bigtable

RDBは、不可分性、一貫性、独立性、永続性（ACID：Atomicity, Consistency, Isolation, and Durability）の特性に準拠した構造を持ち、データの一貫性に重点が置かれている。このタイプのデータベースは、行と列を持つテーブルを使ってデータを保持する。これに対して、NoSQLは、基本的に可用性の高さ、ソフト状態、最終的な一貫性（BASE：Basically Available、Soft-state、Eventual Consistency）の特性に準拠した構造を持ち、データの使いやすさに重点が置かれている。表7-15に見られるように、NoSQLデータベースには、キーと値のペアやドキュメントからグラフ構造まで、データを保持するためにさまざまな方法を使用する複数のタイプがある。いずれの場合も、システムが必要とする処理特性に合ったデータベースを選択する必要がある。

●データ分析ソフトウェア

多数のデータ分析ソフトウェアパッケージが利用可能である。これらの中には、犯罪捜査のデータ分析用に設計された専門ソフトウェアパッケージがある。多くの場合、捜査官はすでに自分の組織で使われているソフトウェアを使うことにした。新しいソフトウェアを使用するケースを支援するために、ケン・コリアー（Ken Collier）が開発したデータマイニングソフトウェアの評価基準を参考資料として表7-16に示す。

表 7-16. ケン・コリアーによって開発されたデータマイニングソフトウェアの評価基準

パフォーマンス	さまざまなデータソースを処理する能力
機能性	プログラムに含まれたデータマイニングのための多様な性能、技術的手法、方法論
利便性	有用性や機能性を失うことなく、さまざまなレベルや種類のユーザに適合する能力
補助作業の支援	ユーザがデータマイニングを支えるさまざまなタスクを実行できる能力

Microsoft ExcelやGoogle Spreadsheetなどのプログラムは、最も多くの組織で使用されているデータ分析ソフトウェア製品であると言われている。しかし、これらは扱えるデータ数に制約があり、機能制御も限定的であるため、複数ソースからのデータのブレンディングやクリーニング、高度な可視化など、統計処理に対する高度な要求に応えることができない。

「R」や「Python」などのプログラミング言語は、書籍やライブラリなどの多数の査読済みリソースによって大きく進歩しており、あらゆる捜査官の武器として非常に柔軟なツールになり得る。これらは、繰り返し可能なタスクの自動化、さまざまなデータタイプ（CSVファイルからPCAPファイルまで）の分析、データマイニングと機械学習の手法の適用、タイムラインの視覚化と作成に役立つ。さらに、組織内にすでに導入されているツールのアプリケーションプログラミングインターフェイス（API）の利用も可能になる。これにより、すでに導入されているツールと対話する際の拡張性を確保しながら、調査時間を短縮できる。ネットワークに展開されたツールからのテレメトリを使用する場合は、CoC（管理の連鎖・証拠の保全）とデータの整合性を確実にすることが重要であることに留意すべきである。

品質保証と品質マネジメント

「品質保証とマネジメント（Quality Assurance and Control）」とは、分析フレームワークに関連して、経験豊富で熟練した人が指導とアドバイスを提供することで最終出力の品質を保証できるプロセスとして定義される。分析フレームワークの出力を評価する基準は、**「精度（Precision）」**、**「信頼性（Reliability）」**、および**「実用性（Practicality）」**を伴う。

精度は、分析フレームワークの出力が、提供された属性と密接な関係があるかどうかを示す指標である。分析フレームワーク内で実行されるデータ標準化プロセスでは、不整合データに関してデータクリーニングが実行される。このため、精度を測定する際には、不整合データに関してさらに調査や研究

を行う必要があるかもしれない。

信頼性は、異なるデータセットに対する分析フレームワークの性能を示す。提供されたデータに関係なく、一般的なパターンまたは同じタイプの出力が生成されることが判明した場合、分析フレームワークの評価は信頼性が高いと判断できる。

実用性は、分析フレームワークによって有用な情報が提供されるかどうかを示す。

一般的に、品質保証と品質マネジメントはデータの標準化プロセスと密接に関係している。

●品質維持に向けた計画の普及

品質保証と品質マネジメントのプロセスでは、目標レベルと優先順位を事前に決定すべきである。頻繁に使用される情報や犯罪捜査に大きな影響を与える情報には、高い優先順位が与えられるべきである。捜査官は、使用する予定のない情報を削除することも検討すべきである。

データの一貫した維持は、分析を担当する捜査官だけで達成されるものではない。これは、捜査に携わるすべての捜査官によって達成されるべきものである。したがって、データをマネジメントするための正しいポリシーと手順に関する定期的なトレーニングを実施することが不可欠である。

データは常に変化する。データの変化に応じて、品質マネジメントプロセスを定期的に見直す必要がある。

●品質維持に向けた監視

データ品質は適切にマネジメントされなければ、急速に悪化する。古い情報や誤った情報の流通を防ぐため、データの除去を含む定期的なモニタリングを実施すべきである。一貫したデータを維持するためには、レポートやダッシュボードなど、必要なときに誰でも確認できる自動データマネジメントシステムをあらかじめ構築しておく必要がある。

結果との関係

「結果との関係」では、「脅威プロファイル（Threat Profile）」、「帰属プロファイル（Attribution Profile）」、および「影響分析（Impact Analysis）」の定義を扱う。犯罪捜査では、発見された証拠がすべて決定的なものとは限らない。しかし、限られた証拠項目の間に関連性を持たせることで、文脈を見いだすことができ、それが情報に基づいて意思決定のサイクルを生み出す。

脅威プロファイル

「脅威プロファイル（Threat Profile）」とは、犯罪シナリオ、「脅威の行為者」の関与、およびその脅威に関する情報をまとめたものと定義される。

発生した脅威を分析し、表 7-17 に分類される「行為者クラス（Actor Class）」、表 7-18 に示される「行為者の動機（Actor Motivations）」、および表 7-19 に示される「行為者の熟練度（Actor Sophistication）」を記録することにより、サイバー犯罪捜査官はこれらの条件間の相互作用を説明することができる。これは捜査官が警察当局に犯罪状況の理解を伝えるのに役立ち、警察の活動を分析するためにも使用できる。

これらの項目を発展させ、サブカテゴリを作ることでより詳細な内容を発展させる今後の研究が必要であることは注目に値する。

表 7-17. アクター分類（Actor Classes）

Actor Classes
競合（Competitors）
不満を持つ顧客（Disgruntled Customer / User）
ハクティビスト（Hacktivists：社会的・政治的な主張を目的としたハッキング活動を行う犯罪者）
内部犯行（Insiders）
組織犯罪（Organized Crime）
スクリプトキディ（Script Kiddies：興味本位で第三者に被害を与える犯罪者）
諜報員（State Actor / Agency）
テロリスト（Terrorists）

表 7-18. 犯行動機（Actor Motivations）

Actor Motivations	Sub-category
金銭・経済（Financial or Economic）	
イデオロギー、観念（Ideological）	汚職（Corruption）
	反体制（Anti-Establishment）
	環境保護（Environmental）
	民族主義（Ethnic / Nationalist）
	情報公開主義（Information Freedom）
	宗教（Religious）
	人権（Human Rights）
産業（Industrial）	
軍事（Military）	
便乗（Opportunistic）	
政治（Political）	
名声（Prestige）	

表 7-19. 行為者の熟練度

Actor Sophistication
イノベーター（Innovator）
エキスパート（Expert）
練習生（Practitioner）
初心者（Novice）
志願者（Aspirant）

帰属属性（Attribution Profile）

「属性プロファイル」は、犯罪者または犯罪者がリクルートされる予備グループに関する情報で構成される。ビジネス関係や人的ネットワークの中には多くのリスクが隠れている。したがって、帰属属性を分析および記録し、隠れた脅威の理解を促進することによって、これらのリスクを明らかにすることが重要である。

記録すべき予備グループは、パートナーや家族など、リスクの高い個人やグループを含む。さらに、**「AML（マネーロンダリング対策）」**や**「CFT（テロ資金供与対策）」**の観点から、**「PEP（重要な公的地位にある者）」**も監視（モニタリング）する必要がある。表 7-20 は、非常に信頼性の高い情報源から得られる、極めてプライベートな属性情報を示している。

公開記録の情報の集約から得られた調査結果をまとめることも重要である。予備的な集団犯罪歴がない場合、公開情報の利用は捜査において強力な手がかりとなる。

表 7-20. 帰属属性

帰属属性
写真（Photo）
姓（Last Name）
名（First Name）
性別
婚姻の状況（Marital status）
つづり字異形、代替スペル
別名（Alias）
ネイティブキャラクター名
勤務先
肩書
誕生日（Date of Birth）
出生地（Place of Birth）
出生国（Country of Birth）
国籍（Nationality）
現住所（Current Address）
電話番号
メールアドレス
ソーシャルメディアアカウント
パスポート番号（Passport No.）
運転免許証番号（およびその他の公的な個人文書に関する番号）

影響度の分析（Impact Analysis）

「影響度の分析」は、被害者に関する情報と、不正にアクセスされたまたは使用されたシステムやユーザーなどの数など、サイバー犯罪の影響範囲を示す情報で構成される。影響度の分析をシステムごと、ユーザーごと、または関連する標準形式で文書化することが重要である。これにより、捜査官は類似した詳細を迅速に比較できる。案件マネジメントシステムの使用は、関連分析の支援に役立てることができる。

表 7-21 に示されているように、アーティファクトは影響分析のためのインシデントのタイムラインを記述するために、その発生日または変更日に従って記録されるべきである。緊急処置および修復処置のための対応勧告は、組織の方針および管轄のガイダンスに従って文書化されるべきである。

表 7-21. 影響度の分析

影響度の分析事項
影響下にあるシステム数
影響下にあるユーザー数
影響下にある情報
事件の時系列に基づくアーティファクト
事件解決のための処置
（a）緊急対応
（b）是正処置（再発防止）

暗号通貨とブロックチェーンのフォレンジック機能

最後に議論する価値のある話題は、犯罪取引をわかりにくくするために暗号通貨の使用が最近になって増加しているということである。こうした傾向を前提とすると、特に法執行機関が犯罪に基づく資金の移動に対する妨害、資産没収・押収のために裁判所に正式に捜査令状を提出する必要があるシナリオでは、主要なアーティファクト、取引履歴、違法行為のインジケーターを特定する上で、詳細なデジタ

ルフォレンジックと分析技術の使用がますます重要になっている。デジタルフォレンジックと分析は、暗号通貨に関連する一見複雑に見える取引を解明する上で重要な役割を果たしており、多くの場合、特注のオープンソースであり業界も認めるツールと方法論を活用して、取引を追跡し、所有権を特定し、行動パターンを確立する。例えば、イーサリアムブロックチェーンと非代替トークン（NFT）をイーサリアムと Ronin チェーン間で転送するためのアプリである Ronin Bridge の悪用により、2022 年にイーサリアム（ETH）と USDC トークンが 6 億 2500 万ドル強奪された[251]。

デジタル金融資産に関わる問題を調査する際の中心的な課題の 1 つは、暗号通貨取引の匿名性である。デジタルウォレットの所有権を特定するのは難しい場合があるが、ブロックチェーンフォレンジックソフトウェアの機能は進化しており、チェーン上で観察できる内容を文脈化するための追加の洞察が含まれるようになっている。

法執行機関やサイバー犯罪捜査官は、高度な技術を使用して取引を特定の団体や個人に結び付ける独自の立場にある。これには、ブロックチェーンデータの分析、ウォレットアドレスの追跡、主要な行動パターンの特定、評判の良い企業から収集されたディープウェブおよびダークウェブのリソースを含む追加の OSINT ツールの活用が含まれ、詐欺、盗難、恐喝事件の背後にいる行為者の特定に役立つ。高度な分析を統合することで、疑わしい活動に関与した個人が残したデジタル痕跡を包括的に把握できるようになる。

251　https://www.fraud-magazine.com/article.aspx?id=4295019793

第7章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

図 7-6. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 7-22）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 7-22. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 7-23. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査マネジメント – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査マネジメントの機能は、組織に対してサイバー犯罪の特性と種類を説明する。同機能は証拠の収集および取り扱いの手段に関する法的方針について、手続き的な理解を必要とする。また、関連するポリシーの定義とマネジメントについて戦略的な責任を負う必要がある。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。知見収集スタッフは、証拠分析方法（および制限）に関する手順的な理解と、証拠を処理する方法に関する戦術的な知識を持っているべきである。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。捜査官・調査員は、証拠分析・報告の方法（および制限）に関する手順を理解し、証拠を処理する戦術的な知識を持っているべきである。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制および法律のガイドラインは、政策立案者に情報を提供するための調査のアプローチ、および証拠の分析に関する方法と制限を決定する。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。この機能には、責任ある情報開示の場と情報共有の方法を戦略的に理解することも必要である。捜査と分析を通じて判明したサイバー犯罪の種類に応じて、方針に基づきながら、何を、だれに、いつ、伝えるのかを決定する。

後方支援 – 知見収集と捜査活動を支援するために、サイバー犯罪のスコープと手段について、戦術的な理解を必要とする。

総務人事 – 捜査の目的と、証拠の収集および分析に関する組織の能力について、手続き的な理解を必要とする。

第7章:レビュー

1. **サイバー犯罪の証拠分析のために、どのように証拠を集約、分析すべきか**
   答え：分析のためにETL方式でデータベースに集約する。
   例：ログの標準化と、種類、関係、エンティティを定義するEDM（Enterprise Data Management）。

2. **どのように効率的なデータマネジメントと分析フレームワークを定義すべきか**
   答え：品質マネジメントチェックによるスケーラブルで反復的に実施する。
   例：データ品質に関するQCテスト、QAアナリストによるクエリーレビュー、セカンドパーティによる結果レビュー。

3. **どのように分析結果を入力し、サイバー犯罪の範囲を関連付けすべきか**
   答え：通知／共有機能を備えたケース管理システム内で記録する。
   例：日付XXのケース1は日付YYのケース4に関連し、IoCはZZと共有される。

4. **「脅威」、「活動」、および「脅威の行為者」に関連する影響分析はどのように解釈すべきか**
   答え：個人情報だけでなく、サイバー犯罪の被害者やシステムの範囲と目的に応じて行う。
   例：何が、いつ、どのように、どこで行われ、どれだけの人々やシステムに影響を与えたかは、具体的に誰がそれを行ったかよりも重要である。なぜかというと、犯罪の（スコープと目的を）定義する際に捜査官を助けるために、分析によって明らかになる究極の証拠であり、容疑者を特定するための手段／動機／目的を決定することができるからである。

ケーススタディ7:サーバー侵入の試み

- **犯罪**：不正なコンピュータアクセス
- **容疑者**：不明
- **手段**：マルウェア、環境寄生型（LotL）攻撃
- **動機**：不明 - 潜在的な経済的利益
- **機会**：漏洩した特権ユーザーの資格情報やセキュリティ保護されていないサーバーのパスワードストレージへのアクセス

第三者のマネージドセキュリティサービスプロバイダーにセキュリティ監視を委託している法律事務所がセキュリティ警告を受け取る。セキュリティプロバイダーは、企業のバックアップサーバーの1つでRDP（リモートデスクトップ）経由でログインするために使用されているサービスアカウントに関連して起こり得る不正アクセスのインジケーターについて法律事務所に通知する。利用可能なログにより、これは失敗したログインであったことが確認されるが、アクティビティの種類、発生元、および時間はアカウントのベースラインと一致していない。内部エスカレーションの後、これは予期していなかったことが確認され、認証情報とサーバーが不正アクセスされたと判断された。法律事務所がサーバーに保存している機密性の高い顧客データのため、重大なインシデントの可能性が宣言され、法律事務所が事前に定められたインシデント対応計画が実行される。その結果、関係するエンティティは分離され、

必要に応じて修復され、第三者の捜査官がこの案件に割り当てられる。この時点で分かっているのは、RDP 接続に使われているサービスアカウント、接続元デバイス、接続先サーバーだけである。調査に役立つデータをさらに収集するために、調査員は下記の作業を行う。

- 独自の脅威インテリジェンスツールを活用して、法律事務所に関する外部情報を検索する。この結果、法律事務所のユーザーの複数の漏洩した認証情報が特定される。しかし、これらの認証情報のどれが内部アプリケーション用で、どれが外部サービス用かは明確ではない。その後、漏洩した認証情報を集めて企業のパスワード・ポリシーと比較することで、認証情報リストがフィルタリングされる。
- 法律事務所の資産内にすでに導入されている EDR 機能を活用して、利用可能なすべてのデバイスから永続化メカニズムとプロセス、ネットワーク、ファイルアクティビティに関連するイベントを収集する。これにより、相当な規模のデータセットが生成され、これを効率的に分析すれば、インシデントに関する貴重な IoC や不正アクセスの範囲に関する最初の見解が得られるかもしれない。

次に、収集されたデータセットに対して複数の分析方法が使用される。ドメイン、IP、ハッシュは、まず既知の IoC と相互参照され、脅威インテリジェンスが形成される。そして、少数のデバイスにのみ存在する異常値を特定するために、イベントの統計分析が実行される。捜査官は、調査中に法律事務所の資産の大部分にアクセスできるため、異なるタイプの資産（サーバーとエンドユーザーデバイスなど）のベースラインの作成が可能になり、通常とは異なる事象をより効率的に特定することができる。

分析により、手作業で確認する必要がある少数の重要なイベントが生成される。手作業による調査により、捜査官は下記の IoC を確認する。

- いくつかの EUC（End User Computing）資産と 1 つのサーバー資産の「C:\Temp」ディレクトリに未知の実行可能ファイル「fox.exe」がある。
- fox.exe 実行ファイルがデバイス上で存続する Windows サービス。
- 実行可能ファイルが接続を開始した IP のリスト。

この時点で、調査員は発見された情報を会社と第三者のセキュリティプロバイダーに提供する。これにより、下記のことが保証される。

- 不正アクセスされたデバイスは、被害を抑えるために隔離される。
- 不正アクセスされたデバイスに対して、ハードディスクとメモリの科学捜査的な回収が行われる。
- IoC は、会社のセキュリティマネジメント（IP のブロックなど）を強化し、監視を強化するために使用される。

収集された証拠から、調査員は「fox.exe」実行ファイルの 3 つのバリエーションを抽出し、分析のために別のチームに渡す。分析が行われている間、調査員は収集したディスクイメージとメモリサンプルを分析し、以前に発見された流出した認証情報と関連付ける。不正アクセスされたデバイスの 1 つは、最近ダークウェブで認証情報が流出したユーザーの主要な業務用デバイスであることが確認されている。調査員は、このユーザーおよび他のすべての EUC 資産デバイスのプライマリユーザーのすべての認証アクティビティを要求する。この結果、漏洩した認証情報が公表された 2 日後に、ユーザーのベースラインと一致しない IP からのユーザーのログインが特定される。

これらの調査結果は、このデバイスがペイシェントゼロ（感染源）であった可能性を示しており、攻

撃者が他のデバイスに対して別の方法で侵入を拡大した可能性があることを示唆している。さらに、ディスクの分析では、不正アクセスされたユーザーの Windows プロファイルが他の EUC デバイス上に表示されたが、サーバー上には表示されなかった。これは、ペイシェントゼロのユーザー認証情報が、EUC 以外のデバイスへの横方向の移動を許可していないことを示している。デバイス上のさまざまな Windows イベントを分析すると、不正アクセスされたユーザーのアカウントを使用した予期しない RDP アクティビティとログインが示される。これにより、攻撃者が EUC デバイス間をどのように移動したかは確認されるが、サーバーにどのように移動したかは確認されない。

さらに、実行可能ファイルの分析により、これは、メモリへの他のツールの読み込みや、正当なプロセスへの挿入などのさまざまな回避メカニズムの使用を含む、さまざまなコマンドのリモート実行を可能にするモジュール型マルウェアの一種であると結論づけられた。収集したメモリダンプを使用して、調査員は注入された複数のプロセスを特定し、注入されたコードを抽出する。さらに分析を進めると、認証情報へのアクセスや既知の悪意のあるツールのリストが作成される。不正アクセスされたサーバーに焦点を当て、調査員は悪意のあるプロセスが実行されていたドメインマネジメント者アカウントを 1 つ特定する。これまでと同様に、新たな調査結果はさらなる封じ込め措置のために企業に提供される。

どのようにして特権アカウントが不正にアクセスされたのかは、証拠からは明らかではない。しかし、あるサーバー上のファイルの分析を通じて、調査員は、会社のバックアップサーバーの 1 つに RDP 経由でログインしようとする際に使用されたオリジナルのサービスアカウントのパスワードを含むプレーンテキストファイルを発見した。会社の IT チームとさらに連絡を取り、パスワード変更ログを確認したところ、サービスアカウントのパスワードは最近（悪意のあるログイン失敗の前に）変更されており、そのためプレーンテキストファイルには以前のパスワードが含まれていたことが判明した。最後に、特定された TTP と IoC（IP、ハッシュ、ファイル名、侵害されたアカウント）に基づくと、他のデバイスが不正にアクセスされたようには見えず、インシデントは封じ込められたようである。調査員は、期待される手順に従って、適切な文書と報告書を作成する。

第8章 最終処理

はじめに

サイバー犯罪への効果的な対応を理解するには、インシデントを「どのように」解決するかだけでなく、「誰が」最終処理に関与すべきか、「いつ」関与すべきかを問う必要がある。サイバー犯罪の解決には、技術的にも手続き的にも、評価、調査、理解、是正のための組織的努力が必要である。効果的な解決策とは、単にハッキングされたシステムを交換することではない。これは、インシデントが発生するずっと前から始まる。まず、組織が保護すべき情報資産を特定し、直面するリスクを評価することで、防御のためにどのように時間とリソースを投資すべきかを決定する。また、サイバー犯罪を防止し、または対応するために、組織のセキュリティ態勢を向上させるための計画とテストが必要となる。その後、これは啓発や予防および防御されるべき「通常の業務過程」における活動も含む。

サイバーセキュリティの観点から通常のビジネスの流れを理解することは、さまざまな種類の混乱がもたらす影響を測定するビジネス影響評価を実施することを意味する。この評価には、重要なシステム、プロセス、データの特定に加え、サイバー攻撃による潜在的な財務上、評判上、運用上の影響も含めるべきである。これらの資産の重要性と潜在的な脆弱性（および関連する影響）を理解することで、組織は資産を保護するためのリソースと取り組みの優先順位をより適切に設定できる。

サイバーセキュリティのビジネス影響評価（BIA）の主な構成要素は下記のとおりである。

1. **重要資産の特定**：これは、組織の情報資産を特定し、優先順位を付けて、コアビジネス機能におけるその重要性を理解することを含む[252]。
2. **影響度の分析**：BIA は、販売の遅れ、経費の増加、規制上の罰金、顧客の不満など、重要な事業運営の中断による潜在的な影響を評価することに重点を置く[253]。
3. **リスク分析とマネジメント**：BIA はリスク分析と継続的なリスクマネジメントの基盤として機能し、組織がリソースを効果的に割り当て、適切なセキュリティ対策を実施するのに役立つ[254]。
4. **復旧戦略と緊急時対応計画**：これは、レジリエンス戦略の策定、緊急時対応計画の作成、バックアップ計画、緊急時対応、復旧プロトコルなどの対策による混乱の緩和を含む[255]。
5. **リソースの相互依存性**：リソースの相互依存関係と機密データの流れを理解することは、インシデントが業務に与える影響を評価し、復旧時間の要件を確立する上で極めて重要である[256]。

これらの要素を考慮することによって、組織はサイバー攻撃の潜在的な影響をより深く理解し、混乱を最小限に抑えて効果的に回復するための戦略を策定できる。

BIA が完了したら、組織はサイバー脅威要因から直面する「ABC」（Attack、Breach、Compromise）に対して業務を保護するために、適切な防御策を実施する必要がある。

予防策に加えて、組織は徹底したインシデント対応計画を立てる必要がある。これは、サイバー攻撃の検知と対応を担当する専門チームの設置や、攻撃を封じ込め、その影響を軽減するための明確な手順を含む。この計画の有効性を保証するために、計画を定期的にテストして更新することが重要である。

さらに、クラウドコンピューティングの台頭やサードパーティベンダーの利用増加に伴い、企業は自

252 https://clearwatersecurity.com/blog/business-impact-analysis-a-critical-process-for-to-improve-resiliency-in-wake-of-a-cyber-attack/
253 https://www.techtarget.com/searchstorage/definition/business-impact-analysis
254 https://www.cybersaint.io/blog/cybersecurity-risk-management-framework-key-components
255 https://www.cm-alliance.com/cybersecurity-blog/the-importance-of-business-impact-analysis-in-cybersecurity
256 https://coreitx.com/blogs/8-elements-of-a-business-impact-analysis-bia-for-compliance

社のネットワークだけでなく、パートナーやサプライヤーのネットワークも保護することが重要になっている。これは、これらの事業体のセキュリティ慣行に関するデューデリジェンス、強固な契約上の合意、およびこれらの事業体のシステムに侵害の兆候がないかどうかの定期的な監視を伴う。

効果的なサイバーセキュリティのもう１つの側面は、最新の脅威と脆弱性に関する情報を常に把握しておくことである。これは、業界のニュースや進歩をフォローし、会議や講習会に出席し、サイバーセキュリティ専門家のオンラインコミュニティなどに参加することによって実現できる。

さらに、従業員は、組織のネットワークのセキュリティを維持し、攻撃を防止し、侵害を緩和し、組織内外から発生する可能性のある不正アクセスを阻止し、調査する上で重要な役割を果たす。企業にとって、フィッシングメールの見分け方、強力なパスワードの作成方法、そして最も重要な点として、何かおかしい点やミスがあった可能性がある場合にいつどのように報告するかなど、安全なコンピューティングの実践に関するトレーニングと教育を定期的に提供することが重要である。組織はまた、機密情報にアクセスできるのは許可された人員だけであることを保証するために、厳密なアクセス制御手段を導入すべきである。

本章では、サイバー犯罪の調査と対応に用いられる役割、任務、活動、手順について説明する。また、サイバー犯罪のスコープ、アーティファクト、ソース、証拠が、組織または管轄のポリシーに従ってインシデントを解決するプロセスにどのように関係するかについても説明する。サイバー犯罪は種類によって影響が異なるため、調査や解決の手法もそれぞれ異なる。

本章ではさらに、多くの司法管轄区で見られるベストプラクティスと責任に関連する考慮事項に従って、サイバーインシデントに対応し、脆弱性を是正するための提案された枠組みを調査員に提供する。これは、組織のマネジメント者が防御と保護に関連するポリシー、システム、および手順を定義するのにも役立つ。

本章で取り上げた多くの問題や行動の法的・規制的意味合いは、司法管轄区域によって異なることに注意することが重要である。本章の目的は法的助言を提供することではなく、そのようなものとして依拠されるべきではない。むしろ、事実と現地で適用される法律をサイバーインシデント対応に適用する際に、調査員が考慮すべき法的および実務的な検討事項の概要を提供することを意図している。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の調査と最終処理の機能はどのように組織すべきか
- ビジネス影響評価の構成要素とは
- サイバーセキュリティの ABC とは
- サイバー捜査と最終処理の各段階においてどのようなコミュニケーション手段と権限を確立すべきか
- サイバー犯罪の捜査と最終処理の計画に関与すべき人物および関与のタイミングとは
- 最終処理のために整備すべきツール類、人員、および手順とは

最終処理におけるトピックの分類

「最終処理」知識領域に含まれるトピックの分類を図 8-1 に示す。

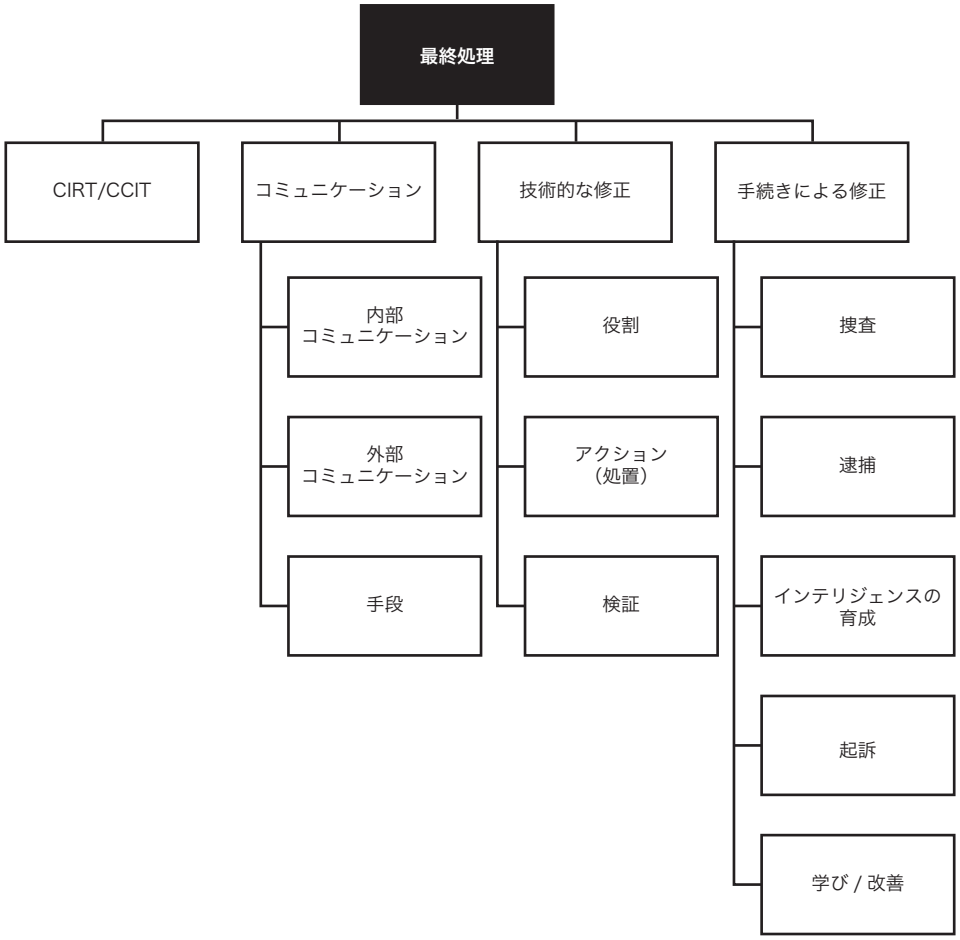


図 8-1.「最終処理」知識領域に含まれるトピックの分類

最終処理（サイバー犯罪事件の解決とは）

サイバー犯罪「インシデント」における最終処理には、いくつかのものが含まれる。組織のサイバーインシデント対応は、技術的な対応にとどまらず、インシデントに関連するリスクの増大と責任をマネジメントすることまで包含しなければならない。最終処理とは、多様で分散したリソース（および異なるミッションや業務目標）を持つ組織の活動と、独自のリソースと目的を持つ法執行機関／諜報機関の活動との橋渡しをすることである。

大規模なサイバーインシデントが国民に衝撃や驚きを与える時代はとうに過ぎ去った。近年、大規模な情報漏えいが多発しているため、世間、規制当局、メディア、弁護士は、企業の経営陣に対してサイバーセキュリティに対する認識と予防措置を求めている。

端的に言えば、私たちは今、サイバーインシデントの予防と対応における「責任」の段階、あるいは広い意味での「説明責任」の段階に入っている。法執行機関の捜査官や諜報／防諜機関の職員にとって、この新たな現実は、民間団体がサイバー犯罪の報告を積極的に行う可能性や、捜査官へのアクセスや証拠

の提供の度合いについて、特有の影響を及ぼす。

最終処理の取り組みは、技術的な対応にとどまるものではない。組織や被害者が利用できるコミュニケーションや技術的／手続き的な救済措置を考慮するものである。このような是正措置は、組織のポリシーに従って行われることもあれば、法的証拠の収集や加害者の訴追を伴う適用法によって規定されることもある。伝統的な犯罪であれ、サイバー犯罪であれ、それが犯罪の本質である。

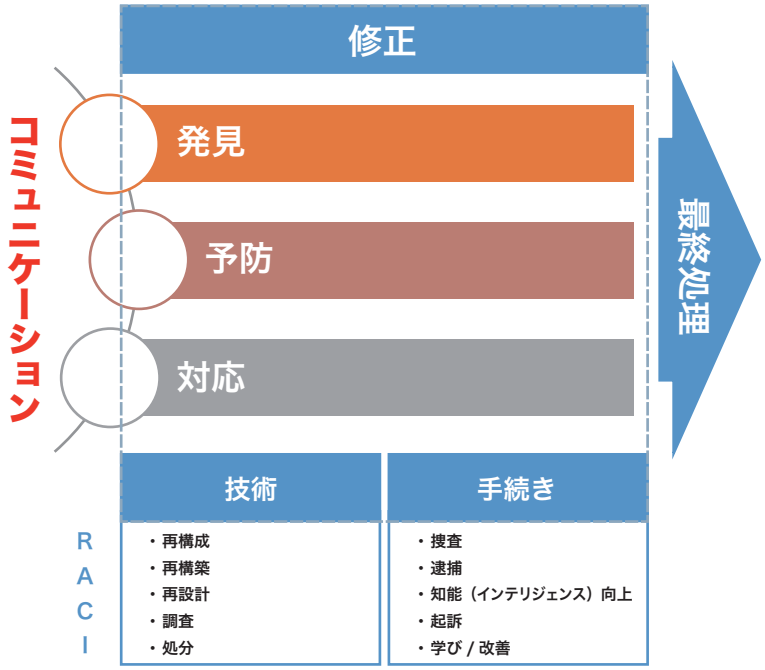


図 8-2. サイバー犯罪の最終処理のモデル

事件の捜査と対応組織

組織におけるサイバーセキュリティインシデント対応チーム（CSIRT）は、業務の継続性、ビジネス機能のセキュリティ上のニーズ、情報のガバナンスと保護など、企業のサイバーセキュリティのニーズに対応するために発展してきた。CSIRT モデルは、Critical Incident Response Teams（CIRT）と Computer Emergency Response Teams（CERT）に由来しており、これらは「サイバー」の概念よりもずっと前から存在していた概念である。CIRT は主に法執行機関で誕生したもので、緊急事態やその他のインシデントが報告されたときに迅速に対応できるよう、才能、スキル、スタッフ、機器、および関連する管轄区域のポリシーと作成遂行上の許可を得るスキームを組織化するという現場の対応者のニーズによって推進された。時が経つにつれて、この概念は民間企業や他の公共部門の組織によって同様の機能を説明するために採用された。CERT は、1998 年に大規模なコンピュータウイルスがインターネットに接続されているコンピュータを攻撃した後に出現した CIRT のコンセプトの進化形であり、このようにして最初の CERT（カーネギーメロン大学のコンピュータ緊急対応チーム - コーディネーションセンター[257]）が誕生した。時が経つにつれて、CERT は、しばしば CSIRT または CIRT（「サイバー」インシデントレスポンスチーム）と改名され、公共部門と民間部門の両方の組織で、事業継続と情報セキュリティの計画とガバナンスに採用されてきた。CCIT（サイバー犯罪捜査チーム）という名称が使われるこ

257　https://en.wikipedia.org/wiki/Computer_emergency_response_team

ともある。

調査、証拠収集、報告のための方針と手順を文書化することが、インシデント対応の成功に不可欠である。経営陣は、インシデントを完全に調査し、データの流出を最小限に抑えるためにCSIRTに期待する。CSIRTは、攻撃者がどのようにしてアクセスしたのか、ネットワーク内でどのように、どこに移動したのか、どのようなデータを探し収集したのか、データはどこで流出されたのか、どのようなデータがどのような経路で実際に持ち出されたのかを究明することを期待されている。CSIRTは、侵入者によって悪用されたセキュリティ上の弱点を特定する。その弱点は、ゼロデイマルウェアやパッチ未適用のシステムから、ネットワークにアクセスできる従業員やベンダーに対するフィッシングやソーシャルエンジニアリングまで多岐にわたる。CSIRTは、侵害を受けた他のシステムを特定し、証拠収集目的でそれらのマシンのイメージを作成し、再構成によって再構築して強化してから、ネットワークに復元することが求められる。

経営陣によるCIRTへの支援と信頼は不可欠である。企業のレピュテーションは、有能で効率的なCIRTを持つことによって守られる。組織は、日常業務を遂行するために、他社、ベンダー、下請け業者、政府からのデータなどを所有し、保存している。TargetやAmazonなどの消費者向け企業は、顧客のクレジットカードデータと個人を識別可能な情報（PII）を預かっている。そのようなデータを保護する企業の能力に対する消費者の信頼が失われれば、人々はその企業との取引を中止するだろう。同様に、政府／防衛産業では、多くの請負業者が製品製造のための研究開発プロジェクトで他社と協力し、広範なサプライチェーン関係を維持している。これらの関係にはすべて契約上の義務があり、データ侵害が発生した場合に企業の責任が拡大する可能性がある。企業は最初のサイバー攻撃を生き延びるかもしれないが、その後の存続は顧客が組織を引き続き信頼できるブランドと見なすかどうかに大きく左右される。

経営陣は、自社のITインフラが法的要件に準拠していること、そしてCSIRTが継続的に監視、調査し、全員のデータを守るためにセキュリティの継続的改善に取り組むことを証明できなければならない。これらの目標を達成するためには、責任と説明責任を持つ社内外のリソースを組織化し、ツール、スタッフ、手順によってサポートしなければならない。

コミュニケーション

サイバー犯罪が発生した場合、組織にとってまず第一に考慮すべきはコミュニケーションである。多くの組織は、インシデントの発見、予防、対応に重点を置いているが、これらすべての機能にわたってコミュニケーションが必要である。誰が、誰と（組織内外で）、どのような情報を共有するべきか、なぜ、どのように情報を伝えるべきかが主な関心事である。

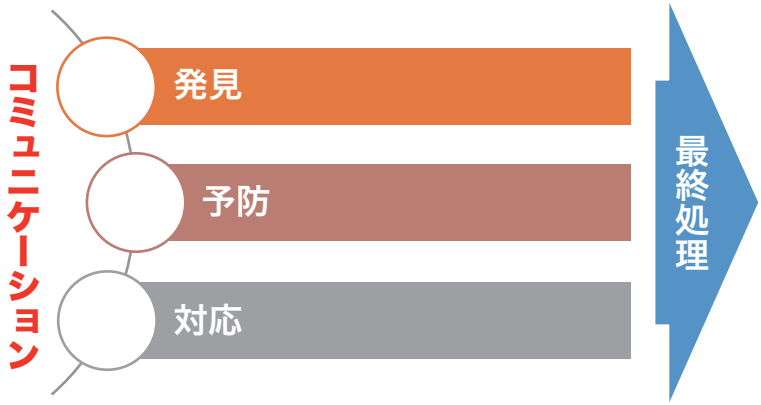


図 8-3. 最終処理に向けたコミュニケーション

内部

CSIRT プロセスは、通信の経路、各経路がコミュニケーション先の対象者に提供する必要な情報（形式、内容、タイミング、配信方法を含む）、および誰がそのコミュニケーションを行うべきかを定めるべきである。これは「レッドブック」通知プロセスと呼ばれることもある。法執行機関やその他の捜査官は、被害者への通知手続きや連絡について、同様のプロセスを定めるべきである。

内部通知には通常、以下の内部組織対象者が関与し、対象者はその通知またはプロセスへの関与に関連する方法に応じて編成される。

表 8-1. 内部コミュニケーション

通知手段	対象者
技術警告	捜査官
案件管理	捜査官、CSIRT、各種業務部門（リスク管理、法務、IT/IS など）
レッドブック	各種業務部門、幹部スタッフ
共有ポータル	各種業務部門（IT/IS）
STIX/TAXII などの IOC ソース	各種業務部門（IT/IS）
監査報告書 [258]	CSIRT、各種業務部門（影響を受ける各部門の長、監査、ガバナンス）

外部

組織には、インシデントの解決プロセスを通じて通知し、コミュニケーションを取るべき複数の対象者がいる。社内の対象者の他に、関連する社外の関係者も存在する。その中には、組織に利害関係を持つ「第二者的関係者」（社外弁護士や株主など）もいれば、組織に影響を及ぼす事故によって影響を受ける可能性のある「第三者的関係者」（一般市民、業界、法執行機関、保険会社など）もいる。場合によっ

258　この文脈での「監査レポート」は、「事後レポート」のほか、定期的なパフォーマンス改善テストとレポートも含むことに留意。

ては、第二者と第三者の境界線が明確でないことがある。しかし、重要な問題は、内部の対象者に加えて、CSIRT にはレッドブックの計画とプロセスで対処する必要がある多くの外部対象者がいることである。

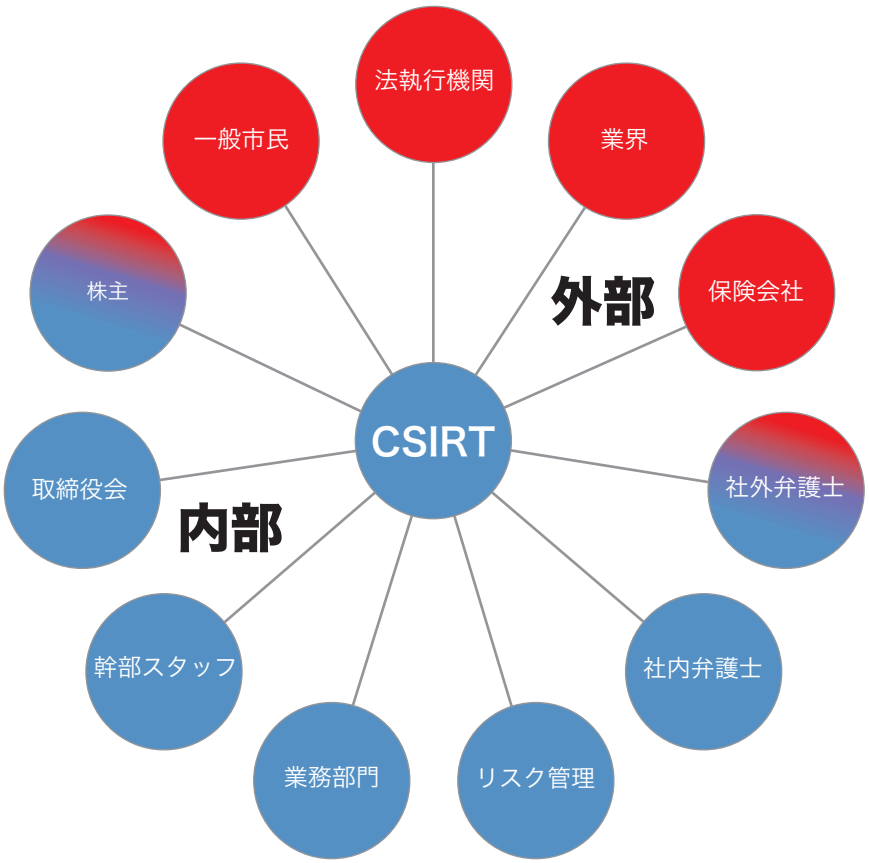


図 8-4. CSIRT による情報の共有

理想的な状況では、法執行機関のサイバー犯罪捜査官は、重大事件が発生したときに被害者とは初対面ではないことが好ましい。近年、FBI や米国シークレットサービスなどの捜査機関は、事件が発生するより以前から、企業に対して指導を行う（さらには、一般コンシューマのコンピュータ利用者たちに情報を提供する）ために多大な努力を払ってきた。侵害の前に関係を確立することで、捜査機関はサイバー犯罪に関連する進化する脅威を説明できるだけでなく、潜在的な対応を合理化し、ある程度の親近感と信頼を提供することができる。米国の国家サイバーフォレンジック & トレーニングアライアンス（NCFTA：U.S. National Cyber Forensics & Training Alliance）[259]、日本のサイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）[260]、英国の国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）[261] などの官民データ共有センターは、脅威情報の交換、協力関係の構築、企業と政府双方の準備レベルの向上など、協力のための重要なプラットフォームとなっている。

一般企業や政府内の「姉妹機関／部局」であっても、法執行機関との関係の程度については慎重である。歴史的に、法執行機関との交流のほとんどは、提出された召喚状や令状に基づくものであり、技能と利益を一致させるための積極的な関係構築の努力に基づくものではなかった。被害者はサイバー犯罪を法執行機関に報告するのを非常に躊躇することが多い。そうすることで、社会への公表や恥辱、顧客

259　https://www.ncfta.net/
260　https://www.jc3.or.jp/
261　https://www.ncsc.gov.uk/

や取引先の信頼の失墜、規制当局による制裁、第三者情報の保護に失敗した場合の責任、そして最終的には事態をコントロールできなくなることなど、さまざまな結果を招くことを彼らは恐れている。法執行機関ごとにサイバー犯罪に関する技術的能力や理解度のレベルが異なるため、捜査官との好ましい関係性構築も阻害されている。法執行機関が、企業の社内技術チームだけでなく企業の経営層やリーダーシップ層とも関係を築くために継続的に時間と労力を費やすと、協力的で生産的な関係が生まれる。公的機関（法執行機関を含む）も民間組織も、それぞれがサイバー犯罪に対処するためのリソースやインテリジェンスや捜査結果の可視性が限られていることを徐々に認識し始めている。

さらに、一般的な法執行チームとインシデント対応する従業員の両方に精通している被害者は、捜査に積極的に協力する可能性がはるかに高くなる。少なくとも、被害者は重大な事故が発生したときに誰に電話すればよいかを知ることができ、貴重な時間を費やして適切な応急処置担当者を探す手間を省くことができる。企業の被害者から多大な協力が得られない場合、法執行機関は通常、強制的な法的手続きを用いて被害者に情報を開示させることを余儀なくされる。これは、捜査官が重要な証拠を収集（および理解）する能力を直接的に妨げる可能性があり、効果のない技術的解決を試みる組織によるミスにつながる可能性がある。

多くの場合、サイバー犯罪の被害者は、法執行機関に通報するかどうかの選択権を持っていない。被害者がネットワークへの侵入者を発見するまでにかかる平均時間は数か月にも及ぶため、盗まれたデータがブラックマーケットや別の場所で発見されることが多くある。そのため、事件について最初に知るのは捜査官やセキュリティリサーチャー、またはメディアである場合が多くなり、これにより証拠収集が指示されることになる。多くの場合、企業には事件を公表することを義務付けられる情報漏洩報告や被害者への通知義務があり、これにより事件の開示が必要となる。例えば、欧州連合（EU）の一般データ保護規則（GDPR：General Data Protection Regulation）[262] は、個人データの侵害を発見してから 72 時間以内に適切な規制当局に報告することを義務付けている。

誰にどのような情報を通知し、どのような見返りを期待するかは、サイバー犯罪の被害者となった組織（または個人）にとって重要な検討事項である。世界のほとんどの地域の地方警察は、通常、不法侵入、物品や財産の盗難、人に対する暴力などの物理的な犯罪にのみ対応する。連邦政府機関はサイバー犯罪に対処する任務を負っているが、解決を支援する情報を連邦政府機関にどうやって伝えるかは依然として周知されていないため、よくある質問となっている。

例えば、米国では FBI がサイバー犯罪の連絡と対応の主要な窓口となっている。他の国では、それほど明確ではない。多くの国では、サイバー犯罪などの地理的に広範囲にわたる問題に対処するための訓練を受けたリソースや全国的な組織がなく、代わりにインターポール（国際刑事警察機構　INTERPOL）やユーロポール（欧州刑事警察機構　EUROPOL）に頼っている。どちらの国際警察機関（の集合体）も、サイバー犯罪の捜査と対応の調整能力を有しているが、関連法の施行と関連する訴追は、被害者が物理的に所在する国、あるいは加害者が逮捕された国の国内裁判所が行う。

保険会社、投資家、またはビジネス取引の相手方に対して、企業が契約上開示義務を負っている場合にも、必要な開示が発生する可能性があるが、これらの状況のいずれも、必ずしもより広範な公開を伴うものではない。これらの状況のいずれにも当てはまらない場合、組織はサイバー犯罪を報告するかどうかを独自に決定することができるが、多くの組織は報告を拒否する。これは主に、インシデントを公表することに伴う責任の懸念によるもので、規制当局に情報を引き渡すこと（したがって、法的特権と、米国法で認められている「弁護士の作業成果物」による保護を放棄すること）と、規制手続きや民事訴訟でその情報が企業に不利に使用されることとの間の矛盾によって部分的に煽られている。

責任に関する懸念は依然として重大な問題であるが、犯罪を報告することで得られる潜在的なメリッ

262　https://gdpr.eu/

トを考慮し、報告に伴うリスクと比較検討すべきである。法執行機関を関与させることの最も明らかな利点は、何が起こったのか、誰が犯罪の背後にいるのかを判断するのに大きく役立つ可能性のある能力と組織的知識が追加されるということである。米国などの市場では、優れたスキルとサイバー犯罪の手法やツールを調査する豊富な経験を備えた強力なフォレンジックリソースが多数存在し、技術的能力がより利用しやすくなっているのは事実である。しかし、これらのリソースには、証拠の提出を強制したり、世界中の法執行機関との関係を活用したりする能力はない。

特に事件発見直後に法執行機関を関与させることのもう１つの利点は、企業が規制当局、顧客保険会社、メディアなどに対して責任ある行動を取ったと主張できるようになることである。調査の過程で後に違反が公になった場合、組織にとって大きな恥辱となる可能性がある。特に、違反が第三者に影響を及ぼす場合、法執行機関を積極的に関与させることは、関連するインシデントを開示する潜在的なリスクに見合う価値があるかもしれない。

法執行機関は、定期的な（一般およびセクター別の）脅威に関するブリーフィングと最新情報を実施することで、被害企業との協力関係を構築する機会を活用すべきである。このアプローチにより、捜査中、法執行機関と被害者団体はより効果的に協力することができる。

特定の情報は組織によって保護されるべきである。システム警告／技術警告、案件管理情報、レッドブック情報の開示は、調査員や組織機能がリスクと関連する対応を決定する過程で成果物として使用する「作業成果物」であるため、不適切である。これらのアーティファクトは捜査官や検察官によっても使用されるため、特権資料として扱われるべきである。

表 8-2. 外部コミュニケーション

通知手段	対象者
技術警告	法執行機関（要求のあった場合）
案件管理	法執行機関（要求のあった場合）
レッドブック	法執行機関（要求のあった場合）
共有ポータル	法執行機関、業界ソース、メディア、一般市民
STIX/TAXII などの IOC ソース	法執行機関、業界ソース、その他ソース
監査報告書 [263]	株主、メディア、一般市民

手段

本章ではサイバーインシデントの解決に焦点を当てるが、組織がサイバーリスクを管理し、侵害に効果的に対応する能力は、事前の準備によって大きく左右されることに留意することが重要である。効果的な準備には、下記のようないくつかの不可欠な要素がある。

- 組織が保護しなければならないデータのカテゴリ、それらのデータの保存場所、およびそれらの保護方法を決定することにより、組織の情報資産（システムとスタッフ）をマッピングする。残念ながら、多くの IT 部門は、サーバー、クラウドコンテナ、アプリケーションなどの資産と重要なビジネスプロセス間のリンクを理解していない。この整合性を確立することが、リスク管理と効果的な準備の重要な部分である。このプロセスは、組織の物理的・論理的情報処理資産（サーバー、ノートパソコン、クラウドコンテナなど）と、それらの接続性（ネットワークレイアウト）、「サービスオーナー」のマッピングを含む。この情報は、組織の IT サービスカタログや構成管理データベー

263 Note that “Audit Reports” in this context include “After Action Reports” as well as periodic performance improvement testing and reporting.

ス（CMDB）に格納されていることが多いが、サイバー犯罪者にとって価値の高いターゲットであるため、サイバーセキュリティの観点から見直す必要があり、適切に保護されるべきである。

- 組織の最も貴重な情報資産の保護を強化し、特定のカテゴリの日常的な情報への制限を緩和してより高速なアクセスを可能にする、多層的な技術セキュリティプランを作成する。現代のサイバー攻撃はしばしば巧妙であり、多種多様な戦術、技術、手順（TTP）を駆使することがある。そのため、成熟したサイバーセキュリティ体制下では、セキュリティ運用チームとインシデント対応チーム（IRT）がベースラインからの逸脱を調査できるように、「通常の」活動がどのようなものかを把握するための効果的な監視機能を備えているべきである。
- サイバーインシデントのトリアージと処理方法を決定する手順を含むインシデント対応計画（IRP：Incident Response Plan）を開発する。
- IRP を継続的に実施するために、組織内の複数の専門分野の代表者を含むインシデント対応チーム（IRT：Incident Response Team）を設置する。
- IRT と組織の上級役員が模擬侵害への対応をテストする定期的な訓練を通じて IRP を実践する。近年、多くのサイバー攻撃で発見されたことの１つは、インシデントレスポンスチーム（IRT）の技術メンバーとビジネスメンバーを訓練することで、実際の脅威に対処する際の効率が向上するということである。実際の攻撃が訓練とまったく同じになる可能性は低いが、「筋肉の記憶」と「対応への自信」が大きな違いを生むことがある。
- サイバーセキュリティとサイバー犯罪の脅威、およびパスワードの管理、不審な電子メールの処理、その他の重要な安全対策に関する従業員の責任について従業員を教育する。従業員には、サイバー攻撃が疑われる場合、あるいは実際にあった場合にどのように対応するか、例えば、懸念がある場合は誰に直ちに連絡するかなどの訓練も欠かせない。多くのサイバー専門家は、インシデントの初期段階を「ゴールデンアワー」（医療業界から引用）と呼んでいる。これは、攻撃者が持続性と管理者権限を獲得する前に、組織が新たなサイバー攻撃を撃退する可能性を大幅に高めることができる重要な期間である。

組織は、重大なサイバーインシデントに直面する前に、これらの対策を実施するために時間とリソースを投資すべきである。実際、多くの業界では、これらの措置の多くが規制要件になったり、サイバー保険契約によって義務付けられたりしている。CSIRT チームを持つ企業は、内部および外部のコミュニケーション対象とその方法を含む関連するコミュニケーション計画を策定すべきである。対象者は、何が重要であるか、関連するスケジュール、関連する詳細レベル、および処理のために情報をどのように分類する必要があるかなどの具体的な情報を受け取るべきである。この文脈では、情報の分類とは、機密性、優先度、および第９章で詳しく説明される方針または法律を管理することを指す。

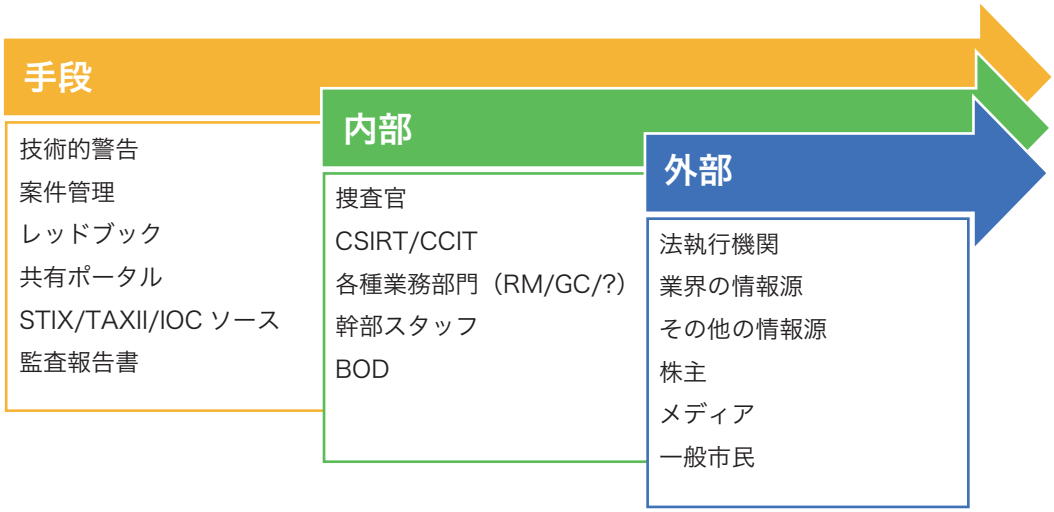


図 8-5. コミュニケーションプラン

技術的な修復

サイバーインシデントの修復は、不正アクセスされたコンピュータをサービスから削除し、イメージを再作成してサービスに戻すという IT 部門の単なる技術的な対応ではない。むしろ、技術的な修復は、根本原因の分析、コンピュータが使用されている環境（ネットワークとユーザー）、他のコンピュータやサーバー／サービスとの関係、調査対象のサイバー犯罪の性質の調査を伴う。たとえば、貴重な情報を得るために、不正アクセスされたホストをあえてそのままにして攻撃者の動向を監視することが必要な場合（または調査員が監視するように指示されている場合）があり、コンピュータを再構築するだけではその活動が妨げられることになる。

役割の割り当て

多くの IT および IS 担当者がよく取る残念な対応として、単純に「脅威」を排除しようとし過ぎるものがある。これは、（脅威がどのように、またはどの状況で使用されていたかに関わらず）ツールやマルウェアを「脅威」として宣言するベンダーの影響で、メディアによりしばしば誤解が強調されてしまうからである。このような対応ではなく、適切な手順に従い、問題の説明、ビジネスリスクとの関連付け（リスクのカテゴリと種類による）、および技術的なアラートまたはケースマネジメントシステムを介して適切な情報の受領者へ通知することが推奨される。強力な CSIRT の原則を実践している組織では、インシデント調査員または案件の分析者に警告を発する方法（およびツール）を持っており、その後、エスカレーションを行うべきかどうかが決定される。エスカレーションが発生した場合、関連する業務部門に、想定される潜在的リスクまたは文書化されたリスクを認識させ、組織の方針および関連する法的／規制要件に従って、修復工程と密接に関連するビジネスへの影響について相談すべきである。

サイバー犯罪（またはあらゆるインシデント）の修復における意思決定の基準は、「RACI」と呼ばれる一般的な組織計画およびリスク管理の頭字語を参照している。下記の表 8-3 に詳細を示す。

表 8-3. RACI 標準

役割	意味	例
実行責任者（Responsible）	タスクを実行することに責任を持つ	CSIRT リーダーが事業 / 業務の継続性を脅かす可能性のある重大なインシデントを幹部にエスカレートする
説明責任者（Accountable）	タスクの進捗や状況（結果）がどのようになっているのか説明することに責任を持つ	方針に従い、インシデントの捜査官が適切な証拠物保管の連続を確保する
協業先（Consulted）	タスク実行を支援するアドバイスなどを行う	経理 /ERP アプリケーションまたはデータにアクセスするバックドア型のトロイ / マルウェアなど（不正プログラム）が発見された場合、CFO または業務部門の管理者と相談する。ユーザ権限やアクセス履歴などの具体的情報を点検し、関連リスクを判断する
報告先（Informed）	タスクの進捗や状況（結果）の最新情報を受け取る	一般公開されていない情報または個人情報への不正アクセス、あるいはそのような情報を格納しているシステムへの不正アクセスが検知された場合、ただちに委員会に報告する

アクション:処置

組織がサイバー犯罪の事件や捜査を解決するために行う行動は、事件により組織が抱えることになるリスクという点ではサイバー犯罪そのものと同じくらい大きな影響を及ぼす可能性がある。不適切な解決策に対する法的および規制上の罰則は、場合によっては非常に具体的な開示要求を含み、組織に経済的影響を与えたり、幹部、スタッフ、または関連するサポートベンダーの訴追につながることさえある。同様に、メディアや公的情報源への不適切または無責任な情報開示は（意図的か否かを問わず）、競争市場や組織とその経営幹部に対する評価に悪影響を与える可能性がある。

IRP およびコミュニケーション計画に関連する役割の割り当てを明確に定義し、テストとシナリオ計画を通じて技術的な修復アクションを含めることが重要である。ガイダンスは、関連する RACI とともに、下記の例を含むアクションについて CSIRT が検討すべき推奨事項とともに文書化する必要がある。

表 8-4. 技術的な修正に関するアクション

アクション	条件の例	RACI
再構成	2 週間を超えて業務から離れていたユーザのアカウントと権限は再構成する	MIS（A）、IT（A）、IS（R）、部門管理職（C、I）
再構築	マルウェアが仕込まれたコンピュータは、CSIRT のリリース後、再構築する	MIS（A）、IT（R）、IS（A、I）、部門管理職（C、I）、CSIRT（R、A）
再設計	ネットワークアーキテクチャまたはリソースのマッピングが行われた証拠が見つかった場合は、CSIRT によるエスカレーションを行い、ネットワークセグメントとサポート ACL を再設計し、実装する	MIS（A）、IT（R）、IS（C）、部門長（C、I）、幹部（C、I）、CSIRT（R、A）
調査	組織の基準からかけ離れた構成となっている IT/OT 資産については、悪用を示す潜在的な証拠がないかを調査する	MIS（A）、IT（R）、IS（A、I）、部門管理職（C、I）、CSIRT（R、A）
処分	年次監査後 90 日以内に利用されなかった、または何らのサービスも提供しなかった IT/OT 資産は処分させる	MIS（A）、IT（A）、IS（R）、部門管理職（C、I）

● 初期検討事項

被害を受けた企業がサイバーインシデントへの初期対応をどのように行うかは、いくつかの理由から、被害者にとっても法執行機関にとっても極めて重要である。企業はサイバーインシデントを IT の問題としてだけでなく、法律やコンプライアンスの問題としても考えることが重要である。たとえば、侵害の疑いの証拠を保全しておくことは特に重要である。そうすることで、法律に基づく侵害開示義務に関する法的判断を支援したり、規制当局に対してインシデントの処理方法を文書化したり、民間当事者による請求に的確に対応したり、必要に応じて、攻撃者を特定して阻止するための貴重な手がかりや捜査の手掛かりを法執行機関に提供したりすることができる。第 6 章で論じたように、証拠収集の方法は、証拠を収集して保存するための体系的、自動化された、および手動の機能（その文書化と処理を含む）を

含むべきである。このような証拠は不安定なことが多いため、証拠に関連付ける関連アーティファクトの自動または手動取得をサポートするツールを迅速に認識して使用することが重要である。特に大規模な環境では、スイープ検出方法によるサンプリングと、関連する体系的な（アラートベースの）アーティファクトログ記録は、従来のフォレンジック手順で収集される膨大な量の技術的アーティファクトを削減するのに役立つ。本書の他の章でも述べたように、アーティファクトと証拠のソースを理解し、効率的な収集（および分析）方法を活用することで、組織はサイバーインシデントを解決することができる。

●証拠を保全しながらネットワークを保護する

侵入者が組織のネットワーク内に残っているかどうかをできるだけ早く判断し、攻撃者が被害者側の対応状況や意思決定された内容をトレースして、それに対抗してくる可能性があるシステムについて、内部調査やその他のセキュリティ対策に関する議論を継続する必要があるかどうかを判断することが重要である。組織は、内部通信が「クリーン」であるとみなされるまで、承認された安全な帯域外通信プラットフォームの使用を検討する必要がある。インシデントに関連するすべての議論は、安全な通信プラットフォームで維持されるべきであり、個人的なアカウントから行われるべきではない。

アクセス時間と場所を含むネットワークログにアクセスすることは、不正アクセスされたシステムを特定し、現在も続いている侵害を排除するために不可欠である。ログは、侵入者がどのデータにアクセスしたか、また企業のネットワークから何が削除または「持ち出された」かを判断する上でも重要である。

前の章で述べたように、侵入と流出のポイントは、データが削除されたネットワークの同じ部分とは限らない。通常、攻撃者は被害者のネットワーク内を横方向に移動して貴重なデータソースを特定しようとし、盗んだユーザー権限を昇格させてネットワークへの完全な管理アクセスを取得しようとする。だからこそ、ネットワークの境界を守ることは重要ではあるが、それだけでは不十分である。その代わりに、ファイアウォールやその他の境界対策は、検知ソフトウェアツール、ネットワークのセグメンテーション、アクティビティロギング、ネットワーク内の異常な横の動きに関する重要なデータを特定して捕捉するその他の手段と組み合わせる必要がある。これらの詳細は、潜在的なサイバー犯罪の範囲と性質を確定するのに役立つ。

法執行機関の観点からは、証拠の保全も重要な問題である。被害者のネットワークからのインシデントデータがなければ、法執行機関の捜査員の仕事ははるかに困難になる。これにより、法執行機関が被害者のネットワークへの直接アクセスを要求し、独自にフォレンジックアーティファクトの復元を試みることの必要性も高まる可能性がある。米国では、ほとんどの連邦捜査官がデジタル証拠の入手と取り扱いに関する特別な訓練を受けている。さらに、米国の主要な法執行機関はすべて、ユーザーが削除したデータのマイニングを含む、フォレンジック・ラボまたは現場でのコンピュータシステムの非常に詳細な調査の実施を専門とするコンピュータフォレンジックの専門家に投資している。

検査官は、可能な限り、収集した証拠のコピーで作業し、公判で使用できなくなるような改変を加えないよう注意する。被害者のネットワークでのインシデントを調査する場合、最も高度な訓練を受けた捜査官であっても、ネットワークに精通している被害者組織のIT担当者の現地での支援を受けることは有益である。単一のデバイスの調査とは異なり、大規模な企業ネットワークでのインシデントの調査には通常、稼働中のネットワーク環境内で証拠となる「アーティファクト」を特定してキャプチャすることを含む。証拠収集の間は、コンピュータや関連するネットワーク機器などを実行中の状態のままにしておくことを強く推奨する。

多くの組織には、IT部門とは異なる機能を実行するサイバー犯罪対処要員がおり、重要な証拠を保全するために犯罪現場に慎重に近づき、証拠の取り扱いと保管の連鎖に注意を払い、法執行機関が何を要求するかを予測するスキルを有している。さらに、自動化されたソフトウェアツールは、関連するイン

シデントデータを保全用に確保するのにますます役立つようになっている。全体的なインシデント対応計画の一環としてネットワーク上にこれらのツールを導入するリソースを持つ組織は、調査中の時間とリソースの効率化というメリットを享受できる。これらのソリューションは、もはや高価なものではない。第6章で説明したように、無料のツールでも同じ目的を果たすことができ、多くの場合、高価なツールと同じくらい簡単に導入して活用できる。これらは今日のあらゆる組織にとって実用的であり、証拠保存のための重要な時間と労力を節約できる。

第6章で説明したように、証拠収集のためのCoC（証拠の保全・管理の連鎖）を確立し、文書化することが重要である。最良証拠の原則とは、原本は原本のコピーよりも優れた証拠であり、原本が存在し、それを提出できる場合にはコピーは認められないという法的原則がある。しかし膨大なログファイルなどのデジタル証拠の場合、多数のシステムからオリジナルの全てを含んだログ、ファイル、ハードドライブを提供することは現実的ではない。さらに、多くの大規模ネットワークでは仮想マシンが使用されているため、取り外して複製し、法執行機関に提出できるハードドライブそのものが存在しない。したがって、収集された証拠がいかなる形であれ修正されたり変更されたりしないことを保証するプロセスが重要である。フォレンジックソフトウェアは収集プロセスを自動化できる。CSIRTの調査員が証拠の収集と分析の手順を文書化している限り（また、必要に応じて証言する意思と能力がある限り）、収集された証拠から無関係なデータを除外した後、ログファイル内の特定のトランザクションをより大きなデータセットから抽出できる。したがって、調査員は、法廷手続き中の精査に耐えられることを確認するために、収集およびCoCプロセスを弁護士とともに検討する必要がある。

●インシデント対応の文書化

企業がサイバーインシデントへの対応をどのように文書化するかは、法的な観点から極めて重要である。サイバー犯罪の兆候を特定するプロセスは、アラートベースのログ記録と、証拠を収集するための関連ツールおよび手順を使用して体系的である必要がある。これらの手順は証拠の取り扱いを含んでいなければならず、特に「ケースマネジメント」の文書化を含むべきである。決定と措置が後の確認のために正式に記録されるように、CSIRTに正式な記録担当者を配置することを強く推奨する。調査がログシステムからの警告によって開始されるか、弁護士のアドバイスによって開始されるかにかかわらず、文書化は基本的に標準的な組織手順と同じであるべきである。

可能な限り、企業の法務部門もしくは顧問弁護士が調査を指揮し、弁護士・依頼者間の秘匿特権および（米国の場合）弁護士の作業成果物の保護が調査の概要と結論に及ぶべきである。このアプローチは、事件に関する企業関係者との面談・聞き取り調査を含む、調査のすべての重要なステップに適用すべきである。特権と作業成果物の保護は訴訟で困難に直面する可能性があり、絶対確実とは程遠いものであるが、企業が機密性の高い分析作業を保護する大きな可能性をもたらす。基礎となる事実自体は秘匿特権の対象にはならず、証人は法廷で直接証言を求められる可能性があるが、何が起こったのかを理解するための企業自身の努力と、その事実が漏洩からどのように保護されるかを理解するための努力は、多くの場合、秘匿特権の対象となる。一般的に、社外弁護士は社内弁護士よりも（はるかに）強力な特権保護を受ける。その理由は単純で、社内弁護士は調査に必然的に影響する組織の経営管理機能を代表しているからである。

調査結果の書き方にも注意を払うことが重要である。CSIRTの調査員や外部のフォレンジックベンダーは、自分たちの作業が終わってからずっと後に起こる可能性のある民事訴訟や規制手続きに、自分たちが書いた内容がどのような影響を与えるかを考慮しないことがある。そのため、報告書の文言は、報告書が最終版になる前に弁護士が評価すべきものである。結果が慎重に書かれ、誇張された表現、不必要に拡大された範囲、不当に独断的な結論が避けられているのを確認することは、企業の行動が民事訴訟、規制当局、メディアなどによって試される際に、さらに別の保護の役割を果たすことになる。

これらの法的考慮事項は、被害者がサイバー犯罪をいつ報告するか、また捜査官にどのような証拠を引き渡すことに同意するかに影響するため、法執行機関にとって重要な意味を持つ。証拠を文書化する際のベストプラクティスは、事実に基づいて簡潔に記述すること、「現時点の理解に基づく」などの用語を使用すること（解釈は文書化に含めるべきではないーこれは専門家の証人と裁判所の領域である）、そして絶対的な言葉で述べないことである。CISRT の調査員は何事についてもすべてを知ることはできないので、文書化されている記載内容は、調査員がその時点で観察し、行っていることに過ぎないことを認識すること。同じことをする調査員は他にも必ずいるであろう。

●法執行機関に対する証拠の提出

上記のような責任に関する懸念があるため、サイバー犯罪の被害企業は、法執行機関に提供する情報に注意しなければならない。特権や作業成果物の保護を損なわず、また将来的に会社を不必要に責任にさらすことなく、法執行機関が職務を遂行するために必要な情報を提供するよう、あらゆる努力を払うべきである。ただし、情報は必ずしもデータを意味するわけではない。

情報とデータは異なる。場合によっては、規模や機密性／責任の問題により、捜査官と組織の法的責任が侵害されないように、承認された専門家によってのみデータが要約されることもある。例えば、ほとんどの場合、法執行機関は企業のネットワーク上で行われる通信の内容を必要としないため、要求すべきではない。代わりに、法執行機関は、侵入がどのように、いつ、どこで発生したかを判断するために必要なログデータやその他のコンテンツの中身自体は含まない情報のみを必要とすることがほとんどである。ただし、フィッシングメールの内容など、攻撃者の身元や手口に関する手がかりとなる可能性がある例外もいくつか存在する。米国法および多くの国際法では、犯罪自体の一部である通信が、被害者が法執行機関にこれらの項目を提供する際に法的障壁となることはほとんどないが、法的ガイダンスを求め、ネットワークデータと通信を法執行機関に提供する根拠を文書化すべきである。

●サイバー捜査・調査はITやISではない

サイバー犯罪捜査・調査における重要な違いは、これは単なる情報セキュリティや技術上の欠陥の調査ではなく、犯罪の捜査であるという認識を組織が持つことである。サイバー犯罪はシステムやアプリケーションの設定ミスから発生することもあるが、客観的な結果を伴う意図的な法律違反である。管理者のコンピュータの「バンキング型トロイの木馬」感染を IT/IS の問題と見なすのは正しくなく、その単一のシステムを再構築しても、侵入者が何らかの方法で最初にネットワークに侵入し、選択的にトロイの木馬をインストールして金銭窃盗や詐欺を働いたという、より重要な問題を解決できないかもしれない。調査にはさまざまな措置が必要だ。

手続きによる修復

手続きによる修正は、技術的な修正と同様に重要である。組織がサイバー犯罪インシデントをどのように解決するかは、基本的に犯罪の性質とスコープに依存する。手順による修復のプロセスは、下記の図 8-6 で可視化されおり、本項で説明する。

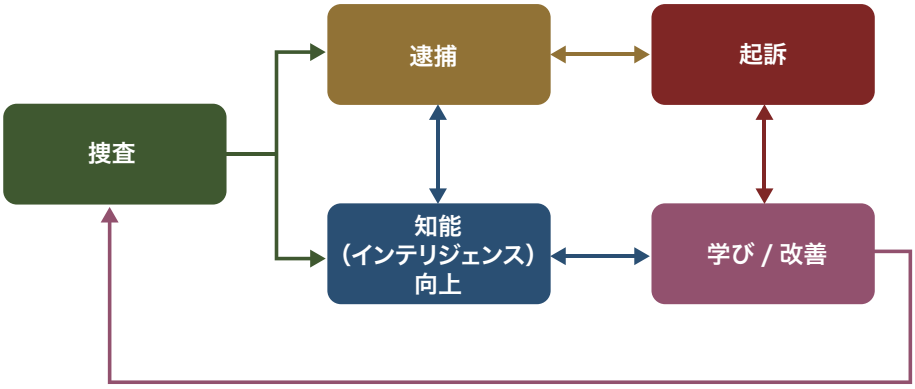


図 8-6. 手続きによる修正

捜査・調査

サイバー犯罪の調査は、SIEM のアラートを確認して感染したコンピュータからマルウェアを駆除するだけではない。調査は、効果的な解決を達成できるようにサイバー犯罪のスコープと目的を決定することを含む。場合によっては、簡単な修復が実現可能であり、組織のポリシーで、そのような場合に発生する可能性のある条件を定義する必要がある。簡単な修復が可能ではない場合、特に非公開情報、個人情報、または保護された情報が許可なくアクセスされた（または共有された／盗まれた）場合、特定の調査手順を実行しなければならない。それらの手続きは、特権のもとで証拠の収集および取り扱いのプロセスに従い、適切な CoC の文書化と共に行われるべきである。

●証拠の情報源の見直し

被害者のネットワークを保護するための初期対応（サイバー犯罪者によるアクティブな侵害やバックドアアクセスが残っていないことの確認、技術的な修復手順の文書化、重要な証拠の収集）の後、調査では証拠の情報源を検討して犯罪の意図や利益を判断しなければならない。被害者のネットワークから収集された手がかりは、多くの場合、第 5 章で説明した他の情報源からの情報と組み合わせることができる。たとえば、下記のような情報である。

- **既知のマルウェア**サンプル、IoA（攻撃指標）、その他の「シグネチャ」データなど、他の事件で捜査官が収集したデータ。サイバー犯罪者は通常、複数の被害者に対する一連の攻撃で同じツール、インフラ、手法を使用するため、捜査官は被害者のネットワークから収集した証拠と比較できる貴重な情報をすでに持っていることが多い。
- フォレンジックサービスを提供する企業を含む、サイバーセキュリティリサーチコミュニティが発表した分析。たとえば、セキュリティリサーチャーたちは、さまざまなマルウェア活動や、ボットネット（ボットマスターの管理下にある侵害されたコンピュータのネットワーク）を含むサイバー犯罪者のインフラストラクチャの詳細な分析を発表しており、ボットネットは、DDoS 攻撃攻撃から盗まれたデータの流出まで、あらゆることを実行するために使用されている。この種の情報は、

Virustotal[264] などのコミュニティ情報ソースや同様のサービスも含むことがある。

- サイバー犯罪者が使用する中間「ホップポイント」の無実の所有者である通信サービスプロバイダや、盗難資金の洗浄に使用される金融機関などの**第三者**から取得した証拠。第三者のデータの中には、現地の法律に基づいて同意によって取得できるものもあるが、ほとんどの司法管轄区では、法執行機関は召喚状、裁判所命令、捜索令状、その他の強制的な法的手続きを取得して第三者に送達しなければならない。これらのサービスは、関連情報の提供を強制するだけでなく、法的な権限なしに顧客データを開示したことによるプライバシー侵害の申し立てから第三者を保護するように設計されている。
- 新規および既存の**潜入捜査**を通じて、また秘密情報提供者などの活動参加者の協力を通じて得られた証拠。これは重要性を増している分野であるが、関連する司法管轄区に依存する重大な法的懸念も伴う。
- **他国の捜査官**から得られた証拠。サイバー犯罪の証拠が1か国に限定されることはめったにないため、外国の法執行機関との協力が極めて重要である。

最後の3つのカテゴリについては、以下で詳しく説明する。

●第三者が保有する証拠

被害者のネットワークからの手がかりを利用して、法執行機関の捜査官は他の潜在的な証拠源の手がかりを特定できる場合がある。サイバー犯罪の黎明期には、IP アドレス（または一連のアドレス）を取得し、それをたどることで、犯罪に使われたコンピュータに直接たどり着くことがよくあった。今日では、攻撃者は通常、国際的／管轄権の境界線を越え、VPN サービスなどの暗号化された通信チャネルを活用する一連のサードパーティ「ホップ」を使用する。これにより捜査は複雑化し、「デジタルの痕跡」だけでなく、金銭的な痕跡、他の事件との類似性、インフラや関係者に関する既存の知識、独創的な潜入捜査も考慮する必要が生じる。したがって、捜査官は、（犯罪から得られた）手がかりとなる第三者の情報源の初期リストを作成し、それらの情報源から証拠を収集するためにどのような法的手段が利用できるかを判断すべきである。

米国では、サイバー犯罪捜査官が利用できる法的手段は、サイバー犯罪以外の事件で利用できるものとほぼ同じである。ある司法管轄区で利用可能な法的権限については、一冊の本や講義で十分に扱えるほどの内容であるが、一般的な概要として、米国における主な証拠収集手段には以下のようなものがある。

- **大陪審の召喚令状**：召喚令状は**裁判所命令**と同じものではない。これは、大陪審の権限に基づいて検察官が発行し、裁判所によって執行される法的拘束力のある証拠請求である。召喚令状を受け取った当事者がそれに従わなかったり、召喚令状の合法性に異議を申し立てたりする場合、裁判所がそれらの問題を判断する。米国では、サイバー犯罪事件において、召喚令状は、特定のアカウントの加入者の名前、住所、請求情報など、基本的な非コンテンツ情報を要求するために使用される。ウェブログのデータなど、より広範な非コンテンツデータは、通常、召喚状では取得できず、裁判所命令が必要である。
- **捜索令状**：捜索令状は、示された「相当な理由」（すなわち、特定の場所に犯罪の証拠が存在するという合理的な確信）に基づいて裁判所によって発行され、権限のある法執行官が、令状に記載された特定のカテゴリの証拠を探すために、物理的な場所に立ち入ること、または物理的なコンピュー

264 https://www.virustotal.com

タまたはデバイス／機器を捜索することを許可する。コンピュータ証拠の文脈では、捜索令状はコンテンツを含む保存されたデータを取得するために使用されるが、ライブ通信におけるコンテンツを傍受することは許可されない。

- **盗聴命令**：盗聴は、ライブ通信を傍受するために多くの司法管轄区で長い間使用されてきた。米国では当初、盗聴は組織犯罪事件で数十年前から使われていたが、今では麻薬事件で一般的に使われ、サイバー犯罪事件でも増えている。通信相手のプライバシーへの重大な侵害のため、米国の法律では、無関係な通信を傍受するリスクを最小限に抑える計画があり、裁判所に頻繁に最新情報を報告することを条件に、必要性が示された場合にのみ盗聴を許可している。

証拠の収集と提出に関する法的要件は、時に混乱を招くことがあるため、弁護士の助言に基づいて常に明確にしておくべきである。ただし、その助言は、CISRT スタッフの職務と要求される職能を定義する運用方針として整備する必要がある。例えば、下記の ECPA サービスガイダンス（表 8-5）では、電子メールを参照しているが[265]、これはサイバー犯罪の捜査で必要となる可能性のある証拠の 1 つの情報源にすぎない。

表 8-5. 電子メールの収集に関係する送達の要件（米国の例）

通信の種類	収集のために法執行機関が用意する必要のある送達	根拠法
送受信経路上のメール	令状	合衆国法典第 18 編第 2516 条
家宅内のコンピュータに保存されているメール	令状	合衆国憲法修正第 4 条
リモートストレージに保存されているメール（開封済みのもの）	召喚令状	合衆国法典第 18 編第 2703 条
リモートストレージに保存されているメール（未開封で保存期間が 180 日以下のもの）	令状	合衆国法典第 18 編第 2703 条
リモートストレージに保存されているメール（未開封で保存期間が 180 日を超えるもの）	召喚令状	合衆国法典第 18 編第 2703 条

●潜入捜査

2000 年代初頭から、盗まれたクレジットカード情報やその他のデータが取引された 1990 年代初期の闇市場の「カードフォーラム」を基盤として、サイバー犯罪者グループが形成され始めた。時が経つにつれて、これらのグループは、高い価値のハッキング標的に挑むために必要なさまざまな専門スキルを持つ個人を集め、驚くほど洗練されたレベルに達している。最近では、盗まれた内部情報を利用した取引、産業用制御システムの操作、SWIFT[266] などの銀行決済ネットワークでの電子決済／電信送金の実行など、専門的なタスクのために得た不正アクセスを可能とする仕掛けを最大限に活用するために、一部のグループがスキームに専門知識を追加している。実際、世界のトップクラスのサイバー犯罪グループは、大多数の国の能力に匹敵する組織犯罪グループである。これは主に、サイバー犯罪による収益を受け取る人々が示した利益によって推進されている。サービスとしてのサイバー犯罪（CaaS）（前述のとおり）は、要求に対する市場の反応の成長を表している。CaaS を利用することで、加入者はある程度の匿名性を保ったまま不正アクセスを可能とする仕掛けやメリットを得ることができる。

265　https://epic.org/privacy/ecpa/
266　https://www.swift.com/

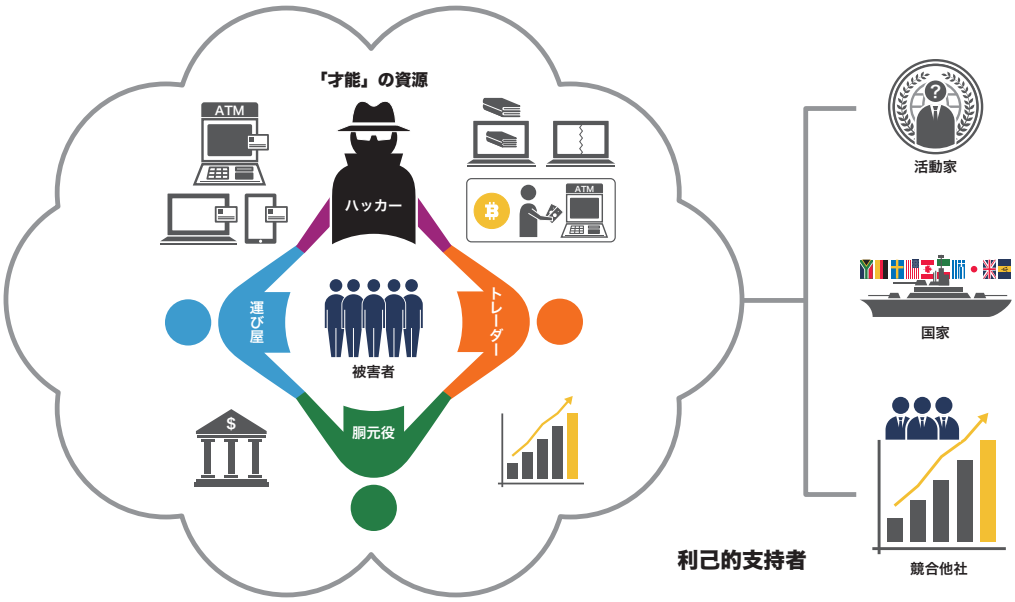


図 8-7. サイバー犯罪の環境

サイバー犯罪が組織犯罪へと発展していることを踏まえ、米国の法執行機関は何年も前から、従来の組織犯罪グループに対して行ってきたのと同じタイプの潜入捜査活動を開始している。これには、マフィアグループや麻薬組織に対して一般的に用いられる盗聴やその他の侵略的な捜査手法の使用を含め、グループメンバーの活動を特定し、追跡する長期的な戦略も含まれる。警察が長年マフィアや麻薬事件で行ってきたように、これはグループ自体に潜入したり、他の方法でメンバーと「潜入」活動で関与したりすることを伴う場合もある。

このような伝統的なケースと同様に、サイバー犯罪においても、特定され逮捕される可能性が最も高いのは、グループの下位のメンバーであり、多くの場合、スキームのより露出度の高い「現金化」部分に関与している者である。いわゆる「金の運び屋」やその他の下位のメンバーは、いったん逮捕されれば、グループの他のメンバーの特定を支援するため、法執行機関の監視および監督の下で協力してスキームを継続することを選択できる。この取り組みにおいて極めて重要な法的手段となるのが、司法取引である。司法取引とは、協力そのものと引き換えに、被告の刑を軽減する（または非公開の審理を含む裁判所への協力の記録を残す）ことである。これらの手法を使用することで、米国の法執行機関はサイバー犯罪グループの通信に合意に基づいてアクセスし、その将来の活動に関する貴重な洞察を得ることに成功した。

潜入捜査が重要な意味を持つ理由の１つは、サイバーが目的達成の手段に過ぎないことがあるからである。組織化されたサイバー犯罪では、加害者はハッカーではなく、組織化された活動に関連するあらゆる関係者である可能性がある。たとえば、一部の CaaS サイバーパートナーシップでは、イニシャルアクセスブローカーが恐喝グループに窃取したクレデンシャル情報を売ることがある。このような場合、恐喝グループが犯人であり、アクセスブローカーによって支援されているという構図となる。グループのメンバーのかなりの割合が特定されると、通常は起訴内容が公開され、犯罪グループは解散することになる。メンバーの中には起訴を逃れて他の計画を続ける者もいるかもしれないが、彼らの活動は大幅に妨害され、捕まるのではないかという真の恐怖を経験する可能性が高い。

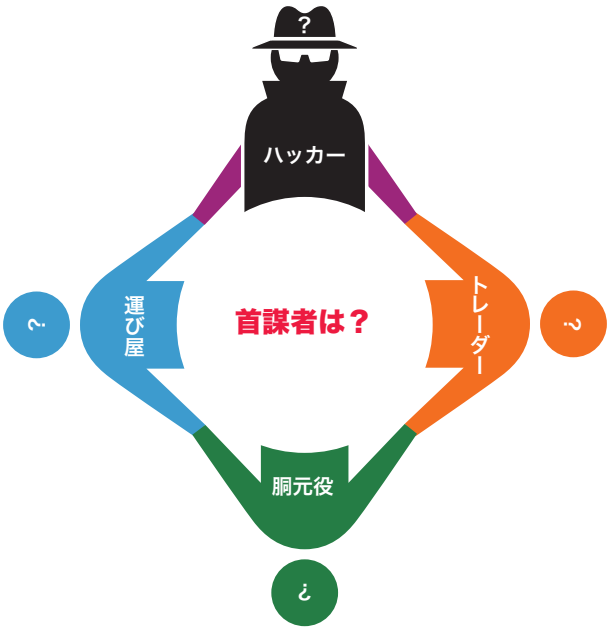


図 8-8. 組織的サイバー犯罪

潜入捜査には、考慮すべき重要な法的問題が存在する。例えば、サイバー犯罪事件では、犯罪に使われるサーバーや被告が他国に所在している可能性があることが重要な考慮事項となる。もう一つの検討事項は、法執行機関が関与する犯罪行為の種類である。背後にいる犯罪者を特定するために詐欺計画を短期間継続させることは、コストとリスクに見合う価値があるかもしれないが、潜入捜査員が監視する中でオンライン児童ポルノ組織を継続させることは別の問題かもしれない。潜入捜査員が負うリスクとその管理方法を考慮することも重要である。これらおよびその他の多くの重要な法的および実際的な問題は、現地の法律に従って慎重に検討されなければならない。

しかし、最終的には、許容される慣行のパターンが現れ始め、法的に擁護できる効果的な潜入捜査を計画し、実行するための基本的なロードマップを捜査官に提供する。組織は、明確なルールとガイドライン、および厳格で一貫性のある審査システムを確立し、提案されたすべての操作が安全性、法律、ポリシーの考慮事項に従って厳重に評価され、承認された場合は潜入捜査官の行動は監視されて文書化されるようにすべきである。このようなレビューと監視には、サイバーセキュリティとプライバシーの問題に関する専門知識を持つ監督者を関与させることが賢明である。このような活動の設計（そして、重要な点として、承認）に法律顧問と法執行機関が確実に含まれる必要がある。

●他国からの証拠収集

サイバー犯罪が完全に一つの司法管轄区域内で発生することはほとんどない。上記で説明した証拠収集のための法的権限に加えて、捜査官は他の国からの支援や正式な証拠を要請する必要が生じることがよくある。第 1 章で説明したように、正式な証拠の要求は、通常、ブダペストサイバー犯罪条約[267]または国家間の相互刑事援助条約（MLAT）の条項に従って行われる。これらの条約には一般的に共通の条項が含まれており、たとえば次のようなものがある。条約が適用される犯罪の種類を正式に列挙したリスト、「二重犯罪性」（要請の根拠となる犯罪に類似する犯罪規定が受領国にも存在する必要性）、および国家安全保障上の例外（受領国が国家安全保障上の理由から要請された証拠を提供しない決定を下せる権限）などである。

267　http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

ブダペストサイバー犯罪条約の「条約第 185 号」は、特定のサイバー犯罪の定義および関連する法執行機関間の調整に関する署名国の相互合意を規定している。これは決して「世界的」な条約ではない。署名国はわずか 49 カ国で、批准して協定を締結した国は 49 カ国（署名国はすべて批准国ではない）だけである。ただし、27 カ国が留保を表明し、25 カ国が宣言を行った。[268]

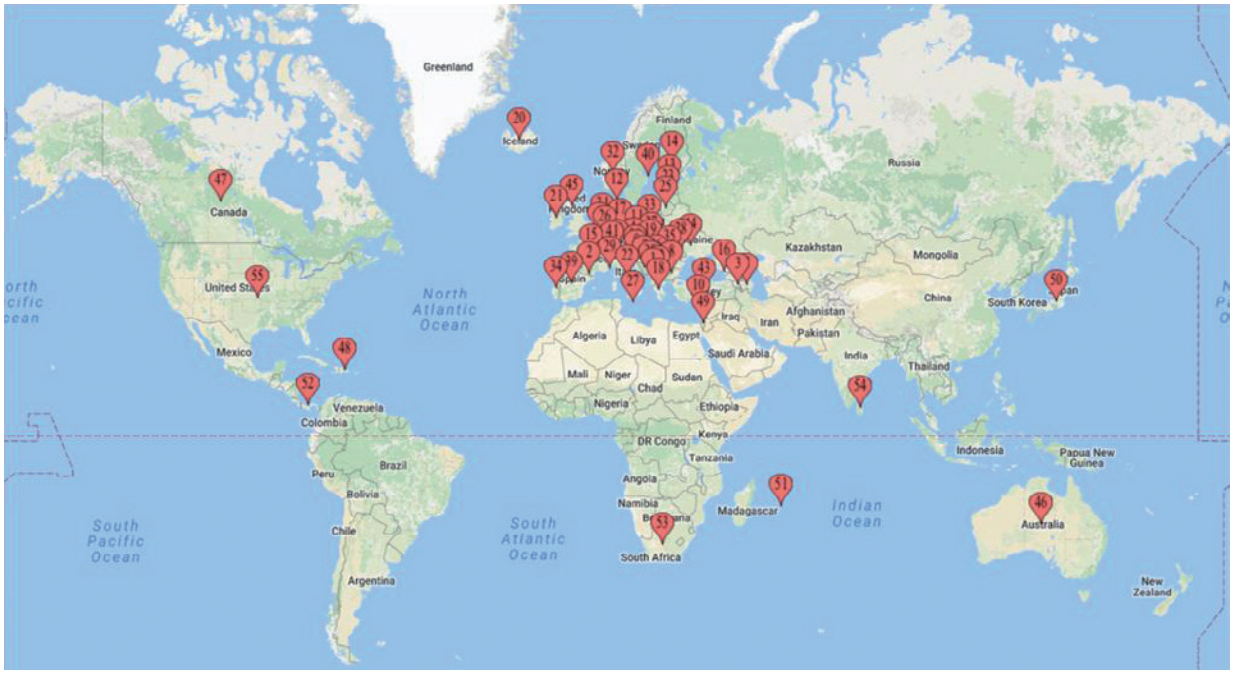


図 8-9.「サイバー犯罪条約第 185 号」の調印国

MLAT の要請の送付と返答のプロセスは、非常に官僚的で時間がかかることで有名である。要求された証拠を受け取るまでの典型的な期間は数か月だが、信頼関係や同様の法的枠組みを持つ国では、より迅速に要求に応じることができる。欠点はあるものの、MLAT は裁判で使用できる正式な認証済みの証拠を他国から入手する唯一の手段であることが多いため、しばしば必要な手順となる。しかし、光速で活動し、通信チャネルを絶えず変更する傾向があるサイバー犯罪者を特定して阻止するために十分な速さで証拠を入手するには、これらはあまり効果的ではない。これらの目標を達成するために、許可された捜査官は「警察チャンネル」を通じて活動し、法執行機関に進行中の犯罪に関する警察情報を提供するよう依頼したり（これは国家安全保障情報とは異なり、全く別の問題である）、現地の法律に基づいて積極的な捜査措置を講じたりする。

場合によっては、現地の法執行機関が管轄権の根拠を特定して国内で独自の捜査を開始し、そのような措置を講じ、その結果を要請した外国の捜査官と共有することができる。同様のアプローチは、他の多くの種類の重大な国境を越えた事件、特に犯罪を阻止するための行動をとるのに何ヶ月も待つという選択肢がないテロ対策事件でも採用されている。このような場合、裁判のための正式な証拠交換は後日に行われる可能性があり、当面の優先事項は深刻な被害を阻止することである。現場での迅速な情報交換と行動のための警察のチャンネルと、最終的な法廷での正式な MLAT プロセスという 2 つの経路で進めることによってのみ、法執行機関はサイバー犯罪者を阻止する能力を最大限に高めることができる。

逮捕

容疑者を逮捕することと、犯罪で起訴することは関連しているが、異なる概念である。逮捕の手続き

268　http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

は、犯罪の容疑者を探し出し、身柄を拘束することを含む。起訴は逮捕と同時に行われる場合もあれば、そうでない場合もある。どちらかが先に行われる場合もあるが、逮捕されても起訴に至らない場合もある。

加害者、被害者、コンピュータインフラがさまざまな国に存在し、サイバー犯罪が司法管轄権を越える傾向があることから、告訴できる司法管轄権が複数存在することが多い。このような決定は、実際の状況に大きく左右される。例えば、被告人がハッキング行為を行った司法管轄区の市民であり、それが別の司法管轄区の被害者に影響を与えた場合、その司法管轄区の当局は、自国民の一人を引き渡すよりも、その事件を起訴することを好むことが多い。実際、いくつかの司法管轄区では、憲法または政策により自国民の引き渡しを禁止している（米国にはそのような一般的な禁止規定はない）。

他方、被害者がいる司法管轄区の当局は、特に被害者の証言やその他の国内証拠が事件の中心となる場合、その司法管轄区の裁判所で起訴手続きを進めることが最も適切に正義を実現するという強い主張を持っている。また、異なるが関連性のある犯罪の訴追を、両方の司法管轄区で進めることも可能であるが、実際問題として、1つの手続が終了するのを待つことに伴う遅延（上訴手続を含むが、これには長い時間がかかることがある）が、この方法を困難にすることがある。

●起訴における検討事項

現在、多くの司法管轄区ではコンピュータハッキングに特化した刑法が制定されている。米国では、関連する連邦法は「コンピュータ不正行為防止法」（CFAA：Computer Fraud and Abuse Act）として知られている。[269] CFAAの中心にあるのは、「承認なしに、または承認を得ている権限を超えて、コンピュータにアクセスする行為」という概念である。CFAAは（1986年に制定されたため）かなり古くなっており、デジタル犯罪が蔓延する現代では陳腐化が見られるが、その中に含まれる概念は今のところ存続している。そうは言っても、多くの検察官は、詐欺、マネーロンダリング、個人情報の盗難、知的財産の盗難、犯罪の共謀など、ハッキングに特化しない他の刑法違反でコンピュータハッカーの有罪判決の獲得に成功している。

他のほとんどのサイバー犯罪法は、不正アクセスに焦点を当てるのではなく、サイバー犯罪活動の目的や意図（現在でも「ハッキング」と大まかに定義されている）に焦点を当てている。場合によっては、これらの犯罪はCFAAに基づくコンピュータハッキング罪よりも立証が容易であり、あるいは、事件の事実と状況に応じてより重い罰則が認められ、CFAAに違反した罪に加えて、またはCFAAの罪の代わりに起訴される可能性がある。

被告の活動に対処するために、最も容易に証明可能な要素を持つ刑法を特定することに加え、以下の点についても考慮する必要がある。すなわち、可能な刑罰、特定の罪状が含まれる場合に裁判で提示が必要となる証拠の性質と範囲、損害の証明方法とその必要性、証拠の基となる捜索や押収、その他の証拠収集技術の正当性を保護できるかどうかなどである。また、特定の証拠が公の場で提示された場合、被害者の観点からどのような敏感な問題が生じる可能性があるかを理解しておくことも通常は賢明なことである。検察官は被害者に起訴状を作成したり編集したりする権利を与えることはできないが、被害者を二重に苦しめないように被害者の利益を考慮することはできるし、そうすべきである。実際、不必要に繊細な証言を要求する軽率な告発によって、あるいはネットワーク システムなどに関する被害者からのその他の証拠によって、彼らは再度被害を受ける可能性がある。これらの問題を慎重に検討することで、被害者や法執行機関との良好な経験を知った他の人々が、将来の事件で協力する可能性が最大限に高まる。

269 https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf

● サイバー犯罪における逮捕に特有の問題

サイバー犯罪の容疑者を逮捕する際、捜査官は、逮捕時に被告人が物理的に所持していたデジタル証拠だけでなく、何が起こっているかに被告人が気づいた後に遠隔で変更できる（または他の誰かに変更を指示できる）証拠も保全するよう細心の注意を払うべきである。もう一つの重要な考慮事項は、犯人が所有するデバイスが暗号化されてしまう可能性があるという事実である。また、デバイスが勝手にタイムアウトして、捜査官が貴重な証拠を確保する機会を失うこともある。これは、ランサムウェアの攻撃者による意図的な行為、あるいはコンピュータの「シャットダウン」設定などの意図しない設定の問題によって発生する可能性がある。これらの理由から、逮捕に伴う通常の安全上の懸念に加えて、捜査官は逮捕時にデジタル証拠を保存するための戦略を慎重に計画しなければならない。この新たな現実は、すべての捜査官がデジタル証拠の取り扱いに関する基本的な訓練を受けるべきであるということを意味する。通常、被害者のコンピュータネットワーク上でサイバー事件に取り組む場合と同様に、捜査官は、コンピュータフォレンジックのツール、方法、ルールについて特別な訓練を受けた逮捕チームのメンバーを少なくとも１人は確保したいと考える。

被疑者が所持している機器を法執行機関が押収してアクセスすることには多くの法的問題があるため、法執行機関は、逮捕計画の初期段階から検察官を関与させ、可能な限りこれらの問題を事前に検討できるようにすべきである。

犯罪捜査に役立つインテリジェンス構築

最も熟練したサイバー犯罪者は、時間の経過とともにさまざまな手口を駆使しながら、サイバー犯罪を職業とする傾向があると認識することが重要である。サイバー犯罪には、かなりの量のリサーチとテストを通じて新しい技術や方法を学ぶことが必要であり、サイバー犯罪者はサイバー犯罪を行おうとして失敗することもある。技術は攻撃手法とともに変化していくだろうが、最も深刻なサイバー犯罪の背後にいる人々は、関係を築いた相手と「ビジネス」を続ける傾向がある。そのため、法執行機関は、あらゆるサイバーインシデントから残されたデジタルの痕跡を単に追跡するだけでなく、一連のサイバー犯罪に関与した個人に注意を払う長期的な視点も持たなければならない。これらの個人を特定すること（つまり、「帰属」を行うこと）は、通常、短期的な課題ではなく、サイバー犯罪者と彼らが使用するインフラストラクチャの関係をマッピングし、活動パターンを探し、サイバー犯罪グループ内部からの洞察を提供するための情報源と秘密捜査活動を開発することを伴う。捜査官は、これらの個人やグループに関する知識を深めることにより、サイバー犯罪者を特定し、逮捕する上で有利な立場に立つことができる。

最も優秀なサイバー犯罪捜査官や検察官は、専門的なトレーニングを積み、世界中の他の捜査官やそれぞれの管轄区域の潜在的な被害者との重要な関係を構築しながら、それを職業とする傾向もある。こうした信頼関係は、サイバー犯罪の捜査や法執行活動を成功させるための基盤になる。サイバー犯罪に対処するための専門知識と能力の構築に真剣に取り組む捜査官は、基礎から最先端の問題まであらゆることが議論される主要な会議に参加するなど、他の管轄区域の法執行機関との訓練の機会を活用すべきである。しかし、知識を構築することよりもさらに価値があるのは、専門知識の交換を通じて築かれる仕事上の関係であろう。

また、捜査官は知識の限界も認識しなければならない。これは帰属に関して特に重要である。インシデント発生後の調査に基づく帰属は、進行中のサイバー犯罪の開始または活動を（監視を通じて）特定するインテリジェンスに基づく帰属に比べて、個人の正確な識別情報を返す可能性が低くなる。調査における関連するプライバシー問題には、虚偽の告発や誤った帰属（公開された場合）が含まれ、これが名誉毀損、中傷、あるいは「偽りの光」などの民事請求や不法行為の訴訟につながる可能性がある。

もちろん、サイバー犯罪の混乱は政府だけでなく、おそらくそれ以上に、インターネットインフラの

大部分を管理する民間部門にも存在する。米国では、企業同士および政府との間でサイバー脅威データを共有するよう促す動きがあり、これは脅威指標をマシン間で共有することで、理想的にはリアルタイムで調整できる、より優れた防御を実現することを目的としている。サイバー犯罪との戦いにおける人的要素がなくなることはないが、戦いに投入されるツールが増えるほど、攻撃される面積が減り、被害も少なくなる。企業や政府がシステムや防御の設計と保護をより上手に行うようになるにつれ、サイバー犯罪者ははるかに多くの労力とリソースを費やすことを余儀なくされるだろう。彼らの活動は、犯人を特定し、逮捕や告発につなげるための遺物や証拠をより多く残すことになる。

起訴

米国の裁判官や陪審員は、民事裁判だけでなく、刑事裁判でも検察側と弁護側の両方が法廷で提示するコンピュータ証拠を見ることに慣れている。しかし、他の多くの法域では、このタイプの証拠は新しいものである可能性があり、関係する弁護士は、証拠がどのように取得されたか、それが本物として信頼できる理由、そしてそれが正確に何を意味するかを説明するために追加の時間を計画する必要があるかもしれない。

米国でも、これは依然として実践的なアプローチである。幸いなことに、ソーシャルメディアとスマートフォンの時代により、コンピュータ技術は多くの国民の日常生活の一部となっているため、裁判でそのような証拠を扱う可能性に怯える人はほとんどいない。しかし、問題は、テクノロジーによってユーザーインターフェイスが非常に便利で汎用的に活用できるようになったため、ウェブサイトにアクセスしたり、電子メールを送信したり、ソーシャルメディアアカウントに何かを投稿したりするときに、舞台裏で何が起こっているのかを多くの人がまだ理解していないことである。

検察官と捜査官は、このような例を通じて、裁判官や陪審員に舞台裏の仕組みや、その結果残された遺物（手がかり）について教えるべきである。彼らは通常、日常生活で大きな特徴となっているテクノロジーについて学ぶことに非常に熱心な人が多いことに気がつくだろう。

裁判でより複雑なコンピュータフォレンジック調査の証拠を提出する際には、さらに大きな課題が生じる。フォレンジック証拠を提出する際の証言者は通常、管轄地域の法律に基づいて専門家として認められた人物によって行われる。この課題の一部は、裁判で召喚される可能性のあるさまざまなタイプの証人に関する混乱に起因している。下記の表は、その明確な詳細を示している。

表 8-6. 証人の種類

種類	説明
捜査官	法執行機関に所属する職員。自らの観察や行為に限定される、事実に基づく証言を行う。自らが作成または確認した文書によって裏付けを行う
事実証人	実質的に証言を行う専門家で、対象システム、プロセス、または添付として作成された文書に関連して個人的に事実に基づく経験を持つ。法執行機関の職員が事実証人の役目を果たすことは多い（事実についてのみ）。組織に従事し、さまざまなプロセスや機能、システムを担当する主任またはプログラマーが、各人の個人的知識に関係する特定の問題については、事実証人の役目を果たすことがある
鑑定証人	それぞれの事件において、事件の問題点となる知識分野の専門家として「適格」であると裁判所によって指定される証人。原告と被告の両陣営の弁護士、さらに裁判所の尋問を受ける。また、裁判所を通してであるが、陪審員の尋問を受ける場合もある。鑑定証人の採否を最終的に判断するのは裁判官である。裁判では、技術的な概念や被害の評価に関する説明は鑑定証人に任される。鑑定証人は、各々の知識、経験、教育に基づいて意見を述べる
一般人の証人	一般人の証人は、弁護士や裁判所からの質問に対して答えを述べる証人である。答えは観察に基づいて述べられる。法執行機関の職員は一般人の証人となってもよい
専門コンサルタント	弁護士による裁判の準備や証拠の収集および分析、点検を支援するコンサルタントが専門コンサルタントである。弁護士の指導の下ではなく、会社のために働くコンサルタントは、指定の専門コンサルタントではない。専門コンサルタントは事実証人となってもよい
供述人	供述人は、宣誓の下、供述証言を行う。状況によって、一般人の証人、鑑定証人、事実証人として証言する（証人として提示された資格が未承認の場合もある）
原告 / 被告	弁護士によって代表される裁判の当事者である
被害者	犯罪の被害者で、供述人または一般人の証人となることがある

証人（事実証人または専門家）に、手元の証言を提出する資格を与えるかどうかは、最初に行う戦術的な判断である。米国では、フォレンジック調査による証拠が特に複雑な場合（あるいはそれを得るために非常に複雑な方法が用いられた場合）を除き、捜査官は通常、事実に基づいた証言を行うことができる。このような状況において、弁護側は通常、フォレンジックコピー（「イメージ」）の信憑性を確認する。この信憑性は、検査されたコピーが押収された当時のデバイスの内容と同一であることを示す暗号ハッシュ値の比較によって容易に証明される。

訴訟で問題となっている証拠のデジタル検査プロセスがより技術的になるほど、資格を有する専門家の証言が必要になる可能性が高くなる。このような場合、証言台で豊富な経験を持つコンピュータ検査官が、技術的な概念を素人に理解しやすいように説明する方法を学んでいるにもかかわらず、その検査官は専門用語で話す傾向があるという事実に検察官は敏感になるべきである。検察官にとって重要なのは、特定のデジタルアーティファクトを生成する厳格で信頼できるプロセスを陪審員に示すことである。これは通常、事実証人と専門家証人による証言によって行われる。最良の専門家証言は、結果に対して真に不可知論的であり、証人が特定の結果を主張しているようには見えない。

サイバー犯罪の起訴は、以下の点を通じて裁判所や陪審員を説得できるかどうかに依存している。

- 法に則った証拠の収集と信頼性の高い解析手法
- 特定の法律に違反していることを実証できる解析結果
- 証人による事実および意見の提示
- 被害者に対する（潜在的または実際の）関連被害

サイバー犯罪の発見／防止に関する学びと改善

どのようなプロセスでも、成熟度を向上させることで改善できるものである。これはサイバー犯罪を解決するプロセスでも同様である。組織は、関連する問題を解決するプロセスで直面した問題だけでなく、成功についても文書化すべきである。また、ステークホルダー（RACI）が必要に応じて支援や意思決定に価値をもたらす実用的な情報を入手できるよう、常にコミュニケーションの改善を図る必要があ

る。改善とは、規模の効率性と関連リソースの経済性を生み出すことである。

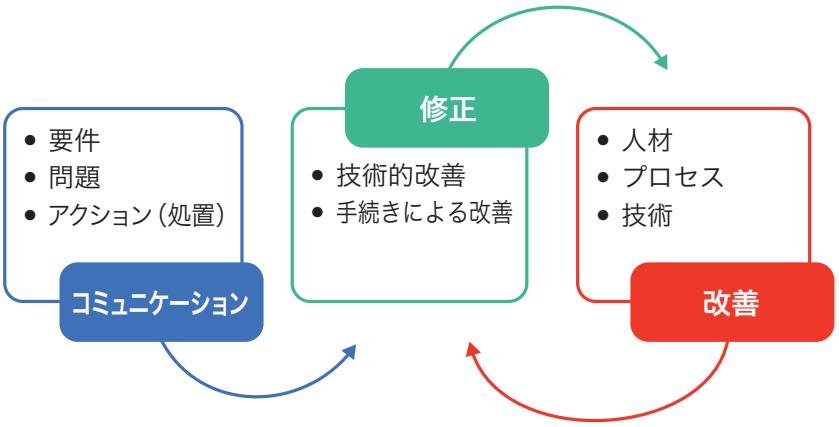


図 8-10. 最終処理の改善

CSIRT がインシデントに対応していく中で、コミュニケーションの障壁や手順の欠陥に対応しなければならない場合がある。これらの戦術的改善は、事後のレビューとプログラムの改善のために文書化されるべきである。サイバー犯罪インシデントを検知、防止、または対応するための組織の戦略的能力は、実践と経験によって向上する。

第8章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

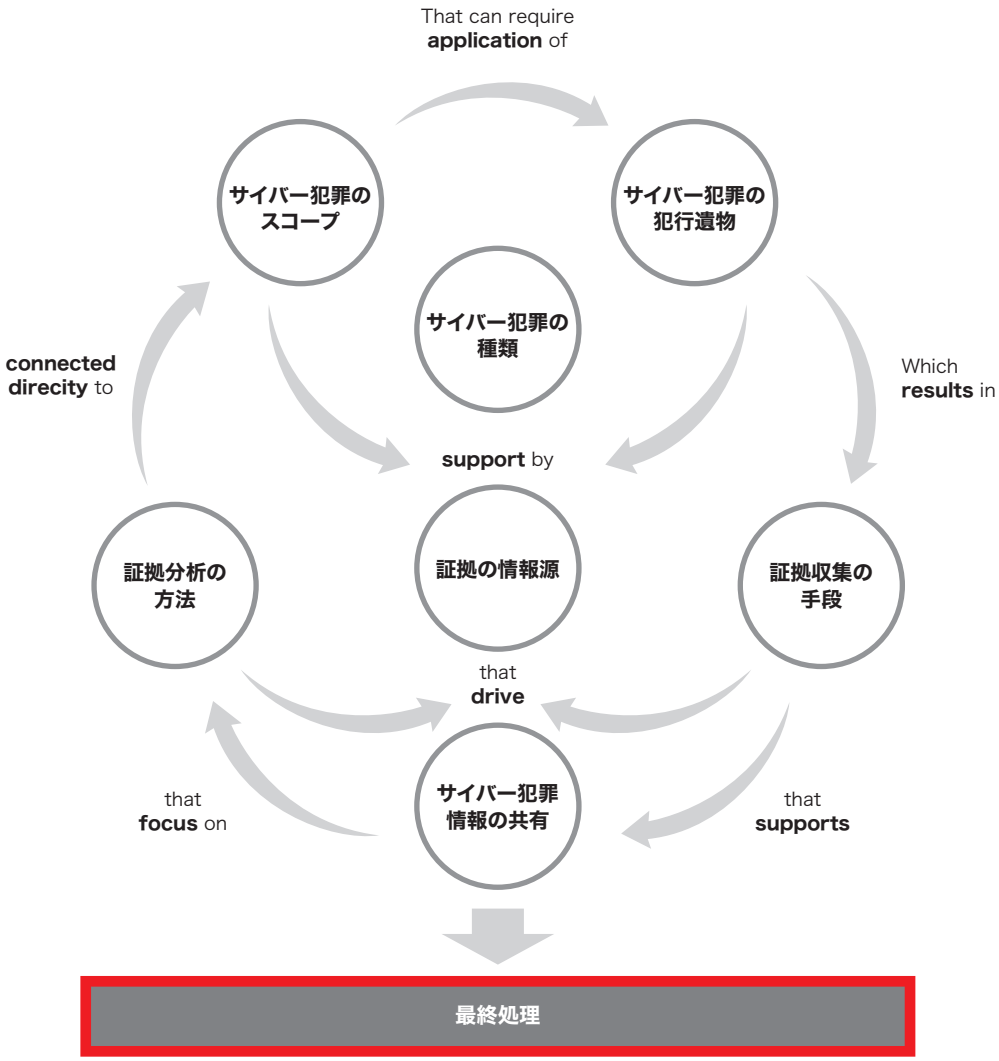


図 8-11. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 8-7）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 8-7. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 8-8. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査マネジメント – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査管理の機能は、組織に対してサイバー犯罪の特性と種類を説明する。捜査管理の機能は、解決活動を計画し、文書化し、指示すべきである。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査管理の各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。サイバー犯罪インシデントの効果的な解決を達成するために、知見収集は情報源を監視し、該当する IoC を供給または発見することによって捜査当局を支援すべきである。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。捜査官は、司法当局の起訴を支援するために、必要な証拠の収集と取り扱い、分析に関する戦術的知識を実証し、必要な技術的および手続き的改善において組織を支援しなければならない。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制および法律のガイドラインは、サイバー犯罪事件を解決するための効果的な起訴および／または是正活動だけでなく、調査へのアプローチを指示する。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪のスコープに応じて、方針に基づきながら、また、どの組織・職務・人員が影響を受けるのかを考慮しながら、何を、だれに、いつ、伝えるのかを決定する。予防啓発は、法的制限に従って、適切な外部機関との効果的なコミュニケーションを確保するために、司法当局と調整しなければならない。

後方支援 – 情報収集と捜査活動を支援するため、サイバー犯罪の捜査範囲と方法について手続き上の理解を必要とする。

総務人事 – 証拠を収集および分析するために、手順の理解、調査の意図、組織能力を必要とする。

第8章:レビュー

1. **サイバー犯罪の捜査と最終処理の機能はどのように組織すべきか**
   答え：CIRT による。経営幹部と事業部門のスポンサーシップを含む。
   例：CIRT リーダー、社内／社外顧問。

2. **ビジネス影響評価の構成要素とは**
   答え：資産目録、リスク登録簿、緊急時対応計画、リソース相互依存マップ。
   例：CMDB、リスク登録、BCP/DRP など。

3. **サイバーセキュリティの ABC とは**
   答え：リソースや資産への攻撃、制御の侵害、機能やデータの不正アクセス 。
   例：フィッシング、侵入攻撃、ソーシャルエンジニアリング、バックドア型トロイの木馬、InfoStealers、詐欺など。

4. **サイバー捜査と最終処理の各段階においてどのようなコミュニケーション手段と権限を確立すべきか**
   答え：体系的および偶発的なコミュニケーション（IRP およびレッドブックを含む）。
   例：RACI の再構成、再構築、再設計、レビュー、廃止。

5. **サイバー犯罪の調査と最終処理の計画に関与すべき人物および関与のタイミングとは**
   答え：RACI を使用して役割を決定する。調査員、CIRT、専門家、弁護士など。コミュニケーション、修復、改善を含むべきである。
   例：プロセス全体を通じてコミュニケーションを取り、ガイダンスと感度／リスクに従って修正し、学んだ教訓により改善する。

6. **最終処理のために整備すべきツール類、人員、および手順とは**
   答え：アラート、デジタル証拠収集、および CIRT（調査員と専門家も含む）。
   例：ネットワークを保護し、証拠を収集し、犯罪を捜査・起訴し、検知・対応し、または将来の事件を防止する。

ケーススタディ8:インシデントの解決

- **犯罪**：業務妨害
- **容疑者**：従業員
- **手段**：ランサムウェア
- **動機**：破壊工作
- **機会**：機密性の高い業務へのアクセス

ジョン・スミスという名の自動車組立ライン作業員が、会社の製造・組立ネットワークにランサムウェアを展開しようとしたとして告発された。最初の告発は、ネットワーク上で検出された不審な動きと、第三者のサービスプロバイダが監視していた会社のサイバーセキュリティシステムによって、従業員のコンピュータにフラグが立てられたことが原因だった。しかし、調査が進むにつれ、告発を裏付ける証拠が不完全で不正確であることが次第に明らかになり、複雑で物議を醸す状況になった。

サイバーセキュリティチームの初期の分析では、サードパーティのサイバーセキュリティサービスプロバイダによってスミスのワークステーションに関連付けられた侵害の兆候に基づいてランサムウェアが展開されたことが示唆された。SIEM のインシデントログには、従業員が自分のコンピュータに USB ドライブを挿入してランサムウェアをインストールしたことが示されており、組立ネットワーク内の他のコンピュータに感染する可能性があるため、直ちに警告が出され、迅速な対応が求められた。それに応じて、同社の IT 部門はスミスのワークステーションを隔離し、さらなる調査が行われるまで彼を停職処分とした。この迅速な決断は、データを暗号化して生産ラインを停止させ、多大な経済的損害と業務上の損害を引き起こす可能性のあるランサムウェアの潜在的な脅威の重大さによって促された。

停職処分の後、スミスのワークステーションの包括的なフォレンジック分析が行なわれた。フォレンジックチームは高度なツールと方法論を利用して、従業員のコンピュータからデータを抽出して分析した。このプロセスでは、ワークステーションのアクティビティログ、ファイル履歴、ネットワーク接続のあらゆる側面が精査され、SIEM データと比較された。

フォレンジック分析による初期の調査結果は、第三者のサイバーセキュリティサービスプロバイダが以前に出した結論と矛盾していた。スミスのワークステーションから収集された証拠は、いくつかの重要な領域で矛盾を示した。まず、コンピュータ上でランサムウェアが発見されたが、EDR ソフトウェアによって検出され、無効化されていた。さらに、フォレンジックの証拠は、第三者からの SIEM ログと矛盾していた。ワークステーションから得られたフォレンジック証拠は、スミスが単に Chrome ブラウザを開いて近くの惣菜販売店を Google で検索しただけであることを明確に示していた。Google の検索リンクを選択すると、使用していた Chrome ブラウザの（パッチが適用されていない）バージョンの脆弱性を悪用した悪質な広告がブラウザから返された。そのため、ランサムウェアが自動的にダウンロードされてインストールが試みられた。実際、そのワークステーションでスミスや他の誰かが USB を使ったことはなかった。

SIEM ログを調べると、冗長なプロセスや時間に関連する特定の異常が詳細に記録されていた。分析の結果、ログは実際には 2 台の異なるコンピュータの組み合わせであり、それぞれが異なる時間に監視されていた異なるプロセスを実行していたが、同じ IP アドレスが割り当てられていたことが判明した。SIEM ログは IP アドレスと時間の相関関係によってホストを識別するように設定されていたが、統合されたログに含まれる 2 台の個別のコンピュータの情報には、独立した組織ネットワークセグメントから同じ IP が割り当てられていた。USB デバイスの使用は時間的には偶然であったが、別のワークステーションの事務職のユーザーによるものであり、不審な点はなかった。これらの新事実はスミスの疑いを

晴らした。

もう一つの重要な発見は、フォレンジックチームが実施したマルウェア分析から得られた。ランサムウェアのサンプルは既知の亜種のいくつかのシグネチャと一致したが、さらに詳しく調べたところ、この特定の亜種は組織の EDR によって適切に検出されたことが明らかになった。

この徹底的な調査の結果は、企業と業界全体にとっていくつかの重要な教訓をはっきりと示した。第一に、サイバーセキュリティ調査における包括的なフォレンジック手法の必要性が強調され、個人に対する懲罰的措置が取られる前に、最初の調査結果が綿密に検証することの重要性が認識された。第二に、第三者のサイバーセキュリティサービスプロバイダがどのデータを信頼すべきかを正しく理解することの重要性が実証された。

調査結果を考慮し、会社はいくつかの是正措置を講じた。スミスは正式な謝罪により復職し、この事件をきっかけに会社のサイバーセキュリティ戦略とインシデント対応プロトコルの再評価が行われた。IT 部門は高度な監視ツールを導入し、組み立てネットワークをインターネットや組織の他の機能領域から分離し、高度なサイバー脅威をより効果的に検出して対応するための定期的なトレーニングセッションを定期的に実施した。さらに、会社は防御を強化し、将来このような誤解が生じないようにするために、外部のサイバーセキュリティ専門家との協力体制を開始した。

結局のところ、スミスの事例は、産業界におけるサイバー関連の調査に内在する複雑さと課題を示している。これは、サイバーセキュリティインシデントに対して系統的かつ証拠に基づいたアプローチを取ることの重要性を強調し、正義が確実に遂行され、貴重な従業員が不当に巻き込まれないことを保証することが大切であることを表している。

第9章

サイバー犯罪情報の共有

はじめに

サイバー犯罪が行われると、通常、意図的に（ウェブページの改ざん、機密情報の公開など）、あるいは意図に反して（センサーが記録したIPアドレス、マルウェアのバイナリなど）、活動の証拠が残される。法執行機関やその他の捜査官が最初に犯罪に対応する際、特に攻撃者が痕跡を隠そうとして高度な技術を使用した場合や、当初の活動がかなり前に開始されていた場合には、最初に入手できる情報が乏しい場合がある。整備されたインシデントレスポンス（IR：Incident Response）プロセスに従い、確実に分析過程の適切な管理を行い、これまでの章で説明したフォレンジックやIR手法を用いることで、付加情報や証拠が生成される。このようなデータは、攻撃者が使用した戦術、技術、手順（TTP）の詳細や、帰属（犯罪の背後にいる個人またはグループの特定）、または動機の理解や帰属に役立つ情報を含んでいる場合がある。

これらの証拠は、捜査官が将来の事件の経験を積み、分析や起訴の効率を高めるのに役立つ。しかし、証拠は特定の被害者に関するアーティファクトのみを示すに過ぎない。今日の知識、スキル、リソース（インフラでさえも）のシェアリングエコノミー、およびサイバー犯罪の組織、単一の被害者の場所で発見された成果物から、サイバー犯罪者の特定や効果的な訴追を可能にするのに十分な情報が得られる可能性は低い。サイバー犯罪捜査において情報共有が非常に重要なのは、主にこのような理由からである。このような証拠を共有すれば、組織が初期の活動の成果物や指標を特定するのに役立ち、それに対応すれば、その後の犯罪を未然に防ぐことができる。特定の種類の犯罪では、プライバシーの機密性や、起訴のための追加証拠の発見に不可欠な捜査の詳細の故に、共有できる情報の種類が必然的に制限される。言い換えれば、サイバー犯罪を阻止するのに役立つ情報であっても、それがすべて共有されるとは限らないということである。

2013年以降、サイバー犯罪の情報共有はさまざまな方法や場を通じて拡大している。サイバーリスクと脅威を説明するための新しいモデルが定義され、影響情報の共有は、組織にとってサイバー犯罪のリスク指標の即時性を理解するための有用なツールとなっている。情報の迅速な伝達は、サイバー攻撃の可能性を防ぐだけでなく、発生した攻撃による被害を軽減するためにも重要である。

サイバー犯罪情報を共有する最も一般的な方法の1つは、官民パートナーシップである。このようなパートナーシップは、政府機関と民間組織との協力関係を伴い、サイバー脅威とリスクのより包括的な理解を可能にする。両者が協力することで、潜在的な攻撃や脆弱性に関する重要な情報を共有することができ、より効果的な予防と対応戦略がもたらされる。さらに、このような協力関係はしばしば進行中の調査にも及び、リアルタイムで情報を共有することで、攻撃に関する両者の理解を深め、攻撃者の手口や攻撃の根本原因、さらにはその背後にいる人物を特定するために利用することができる。

サイバー犯罪との戦いにおいて極めて重要な要素は、関係者間で機密情報を安全に伝送するために、信頼できるプラットフォームやネットワークを活用することである。これらのプラットフォームは技術の進歩により大きく進化し、現在では暗号化されたメッセージングアプリや安全な通信チャネルを通じてリアルタイムのコミュニケーションやコラボレーションを促進する高度に洗練された機能をサポートしている。暗号化を組み込むことで、安全なテキスト交換が保証されるだけでなく、音声通話が傍受されることも防止する。このリアルタイムの暗号化通信は、すべての関係者が瞬時に安全に情報を交換し、新たなサイバー脅威に迅速かつ効果的に対応できるようにするために不可欠である。リアルタイムで安全に通信する能力は、サイバー防衛戦略の有効性を高め、進化するサイバー脅威に迅速に適応し、その脅威を軽減することを可能にする。

本章では、サイバー犯罪情報の共有の方法と限界について説明する。特に、犯罪の種類による管轄権と分類の制限、および関連情報の公開と共有の権限について説明する。また、共有される情報の文書化

や適格性、および共有のタイミングと目的に関するガイダンスも提供される。本章では、そのような要求に従って情報を共有するための参照フレームワークを捜査官に提供する。また、これは組織の管理者が、防御と保護のための関連するポリシー、システム、手順を定義する際にも役立つ。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪情報を共有する理由は何か
- 誰がサイバー犯罪情報を社内外で共有すべきか
- 共有する情報の種類および共有する時期を規定する要件は何か
- どの場所で、どのようにサイバー犯罪情報を共有すべきか

サイバー犯罪情報の共有におけるトピックス分類

「サイバー犯罪情報の共有」知識領域におけるトピックスの分類を図 9-1 に示す。

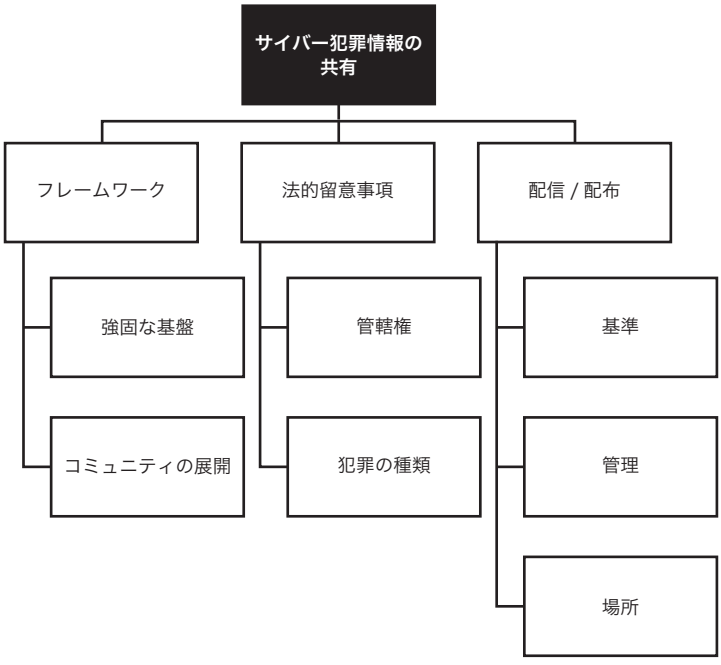


図 9-1.「サイバー犯罪情報の共有」知識領域におけるトピックスの分類

サイバー犯罪の情報共有とは

情報共有を検討する場合、**情報**と**証拠**を区別することが重要である。**情報**とは、捜査の過程で発見または生成されたデータのことである。**情報**は、関連する民事または刑事訴訟において事実または事柄を証明（または反証）することを意図または提供された場合に証拠となる。特定のマルウェアが一般的に特定の脅威の行為者[270]に起因するという事実は有用な**情報**だが、そのアーティファクトがサイバー犯罪者または関連組織の活動、意図、および利益とどのように関連しているかを含む（法的およびその他の解決）要件を満たすまでは**証拠**にはならない。一例として、特定のマルウェアサンプルを識別するシグネチャなどのIoCは単なる**情報**（アーティファクト）であり、コンテキストと影響を確立できない限り**証拠**にはならない。これは、経験豊富な捜査官が時間をかけて学ぶ重要な認識である。サイバー犯罪との関連性の分析ではなく、アーティファクトの評判に基づいた誤った帰属を推定することは、誰の役にも立たない。

●メリットと制限:

捜査・調査過程で生成された証拠と情報の共有は、次の５つの点から非常に重要である。

1. 実行されたサイバー犯罪の特性に応じて、情報と証拠を共有することは、インシデントレスポンス専門家や組織の防御担当者にとっては、軽減措置、被害防止対策、犯罪からの復旧の計画や戦略の策定に役立つ。
2. 収集または生成された情報や証拠は、将来の攻撃を防止する際に、組織の防御者にとって必ず役に立つ。
3. 情報と証拠は、攻撃者から保護したり、攻撃による被害を修復したりする際に、より大規模な防御者同士のコミュニティにとって役立つ場合がある。
4. 情報や証拠は、被害者組織を民事訴訟で保護するのに役立つ場合がある。
5. 情報や証拠は、法執行機関にとっては、攻撃者が特定できた場合、攻撃者の刑事訴追をうまく進めるのに役立つ場合がある。

情報共有においては、上記すべてが重要な理由となる一方で、役に立つサイバー犯罪情報でも共有すべきではない、または共有できない、あるいは制限せざるを得ないシナリオもある。特に、起訴において情報を証拠として使用する意図がある場合、プライバシーの問題が関与する場合（たとえば、PPI：Personal Privilege Information、すなわち、個人の特権情報）、共有によって企業や取引上の機密がうっかりさらされる可能性がある場合、そして共有が法的に禁じられる場合が、それに該当する。たとえば、米国で2015年に施行された「サイバーセキュリティ情報共有法（CISA：Cybersecurity Information Sharing Act of 2015）」では、組織に対して、情報共有の前に、特に脅威の検知指標に対して「個人情報」を見直し、取り除くことを求めている。[271]

270　http://www.threatgeek.com/2016/06/dnc_update.html
271　https://www.congress.gov/bill/114th-congress/senate-bill/754/text - see section 104（d）(2)（A）&（B）

フレームワーク

企業の情報共有戦略と詳細なプロセス実装を開発するには、企業の特定のミッションまたはビジネス目的の文脈で、情報共有の利点と限界（上記で説明したように）の両方を考慮しなければならない。どの企業も、独自の経済的有用性の文脈でトレードオフを考慮しなければならず、その結果、同じような企業が似て非なる情報共有アプローチを選択する可能性がある。本章の残りの部分では、これらのメリットや制限との関連における情報共有の参照フレームワークについて記述している。この参照フレームワークは、サイバー犯罪捜査官・CSIRT の調査員と、防御と保護のための関連ポリシー、システム、手順を定義する責任を負う組織管理者の双方にとって有用である。

サンプルフレームワークを下記のモデルで説明する（図 9-2）。サイバー犯罪に関する情報の分類は、関連する管轄要件と、そのような情報共有をどれだけ迅速かつ完全に実行する必要があるかという考慮事項によって決定される。誰がどのように情報を共有するために公開できるかについての権限も説明されている。次に、通知要件（被害者、規制当局、業界など）をサポートするために、共有される情報の正確性と信頼性の判断が行われる。最後に、サイバー犯罪情報が共有されるべき場所について、公開条件も含めて詳述される。

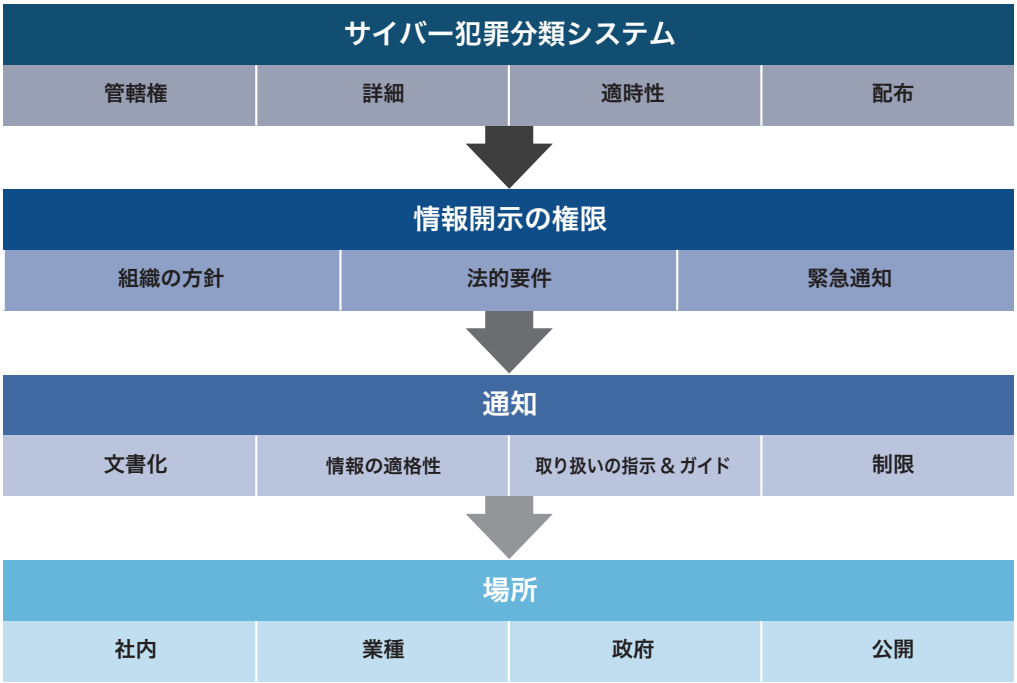


図 9-2. サイバー犯罪情報の共有フレームワーク

強固な基盤の重要性:

サイバー犯罪は、標的や被害者に対して何らかの行動を起こそうとする個人やグループが表明する意図や動機から始まるという点では、他の種類の犯罪と変わらない。サイバー犯罪捜査官の目標は、可能であれば起訴するための証拠を作成し、過去の経験から学んで将来の予防措置に役立てることである。

適切なセキュリティ対策（夜間にドアや窓を施錠する、アラームをオンにする、不審な活動に注意するなど）を講じることで予防的な制御を実現することは多くの場合可能だが、ほとんどの企業にとっての課題は、急速に進化する高度な脅威に直面して攻撃対象領域を管理することであり、サイバー犯罪者は防御側に対して非対称的な優位性を持っている。簡潔に言えば、十分な時間とリソースがあれば、サ

イバー犯罪者は「家」への侵入に成功する可能性が高い。

このため、「インシデントを敷地内から排除する」ための強固なインシデント対応プロセスが重視されるのは明らかだが、見落とされがちな（あるいはあまり理解されていない）のは、日常業務の過程で情報を日常的に記録し、記録しておくことの重要性である。事件履歴を追跡し、IoC や関連する活動パターン、意図、容疑者、関連などの詳細を含む組織は、将来の調査で構築できるコンテキストを作成する。ケースマネジメントシステムが非常に重要なのはこういう理由である。STIX/TAXII や同様の方法によって、ケースマネジメント情報を体系的に共有することができれば、インテリジェンスの共有と使用に参加する地域社会に利益をもたらすインテリジェンスを開発することができる。

例えば、3ヶ月前に特定の IP アドレスから検出されたポートスキャンは、今日同じ IP からフィッシングの試みが発見されたときに新たな意味を持つ。案件履歴により、捜査官・調査員は一見異なる情報の断片を結び付けて、動機や帰属をより深く理解し、犯罪者の行動を共有することができる。したがって、企業に関する情報を定期的に収集することで、調査と解決を最適化するために必要なコンテキストが提供される。この定期的なデータ収集は、情報共有フレームワークの基盤を形成している。実際、日々の業務、使用パターン、システムやプロセスの脆弱性を悪用する潜在的または実際の攻撃の観測など、自社の企業について収集するデータは、収集して利用できる最も重要な情報である。企業内でこの情報を共有することは、効果的な防衛のために非常に重要である。この重要な案件管理フレームワークの視覚化については、下記の図 9-3 を参照のこと。

図 9-3. ケースマネジメントのフレームワーク

今日の企業では、この基礎情報は通常、無数のセンサーによって収集され、堅牢でルーチン化された反復可能な IR プロセスによってさらに背景情報が追加される。収集された情報と生成された証拠は、適切なセキュリティコントロールにより、調査員と防御担当者がアクセスできるデータベースに保存されるべきである。このデータベース機能は、内部で開発することも、外部から取得することも可能であり、データモデル、保持、保存、アクセシビリティに関する決定が、情報共有フレームワークの最初の基礎層を形成するトレードオフを構成する。

共有コミュニティへの展開:

企業が、自社内での情報収集と共有を可能にする、十分に検討された基盤レイヤーを確立した後、上で説明した情報共有のメリットを実現するための次の論理的なステップは、より広範なコミュニティ内で情報を共有することである。十分な互恵関係がある限り、サイバー犯罪情報を外部と共有することは、捜査官・調査員や防御担当者にとって多くの利点を生み出す可能性がある。脅威行為者や犯罪者は、複数の標的に不正アクセスしようとする際に、しばしば同じ手法や慣行を使用するため、脅威の行為者の活動やその手法や慣行に関する情報をタイムリーに共有することは、まだ攻撃を受けていない潜在的なコミュニティメンバーにとって非常に有益である。この情報を共有する能力は、犯罪の性質や使用され

る捜査手続きに影響される。このような複雑な検討はひとまず置いておくとして、サイバー犯罪情報の日常的な相互交換は、通常、下記のような方法で行われている。

1. 収集または開発された情報が共有される可能性があることを示す方針決定
2. 法律や規則によって定められる個人情報の削除、または匿名化
3. 情報を提供する企業または政府機関に関連する機密情報の削除または匿名化
4. 情報を共有する適切なフォーラムと書式に関する決定

日常的な情報共有であっても、関連法令、適用される規制上の決定、およびベストビジネスプラクティスを遵守するように設計された、十分に理解されているガバナンスポリシーによってサポートされなければならないため、上記のステップ1は極めて重要である。通常、データは上記の手順2および／または3で説明したように匿名化されるが、匿名化の詳細は、情報をどこでどのように共有するかについての手順4の決定に影響されるという注意点がある。

手順4に関しては、主に自動セキュリティシステムでの使用を目的とした既知の悪意のあるIP、URL、ファイルハッシュなどの比較的単純な侵害指標（IoC）から、対象となるアクター、キャンペーン、手法、および慣行を特定して説明する、人間が使用できるように設計された詳細な分析レポートまで、さまざまな形式で情報が共有される可能性がある。この種の詳細なレポートは、通常、攻撃をリアルタイムでブロックするのには役立たないが、組織全体の姿勢とポリシーを検討する際には非常に重要である。例えば、組織が、組織のプロセスの脆弱性を悪用することに焦点を当てた、その業界をターゲットにした特定の作戦を認識している場合、その組織は、関連するプロセスを調整することで対応し、従業員に対する集中的なトレーニングを通じて意識を高める時間があるかもしれない。

情報共有フォーマットのフレームワークのサンプルについては、下記の図9-4を参照のこと。

手順4では情報を共有する場所を決定する。オプションは以下のとおりである。

1. 組織が加入している特定のサービスを中心に発展したコミュニティ内での共有。たとえば、組織が特定のベンダーの脅威インテリジェンスを購読している場合、その同じベンダーを介して情報を共有することを選択し、代わりに他のコミュニティメンバーの情報を受け取ることができる。この種の共有は、IRやSOCのオペレーションで観測される日常的なIoCに最も一般的に有効であろう。
2. 特定の業種を中心に構築されたコミュニティ内での共有。たとえば、全米ISAC協議会（NCI）の下に、20以上の情報共有分析センター（ISAC）が設立されている。[272] これらのISACは、自動化された指標や脅威の共有から、日常的な報告や予定された調整および交換会議まで、各セクター内の活動を調整する。ISAC内での共有はサイバー犯罪情報に限らず、物理的セキュリティ脅威データも共有プロセスに組み込まれている。モノのインターネット（IoT）が拡大するにつれて、物理的なセキュリティ情報の統合の重要性は高まり続けている。ISACは、NCIにおいて、政府および民間セクター（特に重要インフラ）全体の復旧、緩和、および修復活動を調整する責任を負うUS-CERTの一部門である国家サイバーセキュリティおよび通信統合センター（NCCIC）によっても代表されている。
3. 共有は、防御担当者の幅広いコミュニティにおいて公然と行われることがある。たとえば、他の捜査官や防御担当者が確認できるように、観察されたTTPの詳細を公開することを選択する者もいる。また、特定の種類のサイバー犯罪事件の識別、封じ込め、調査、復旧に関するベストプラクティスで構成されるワークフローを共有することを選ぶ者もいる。

272　http://www.nationalisacs.org/member-isacs

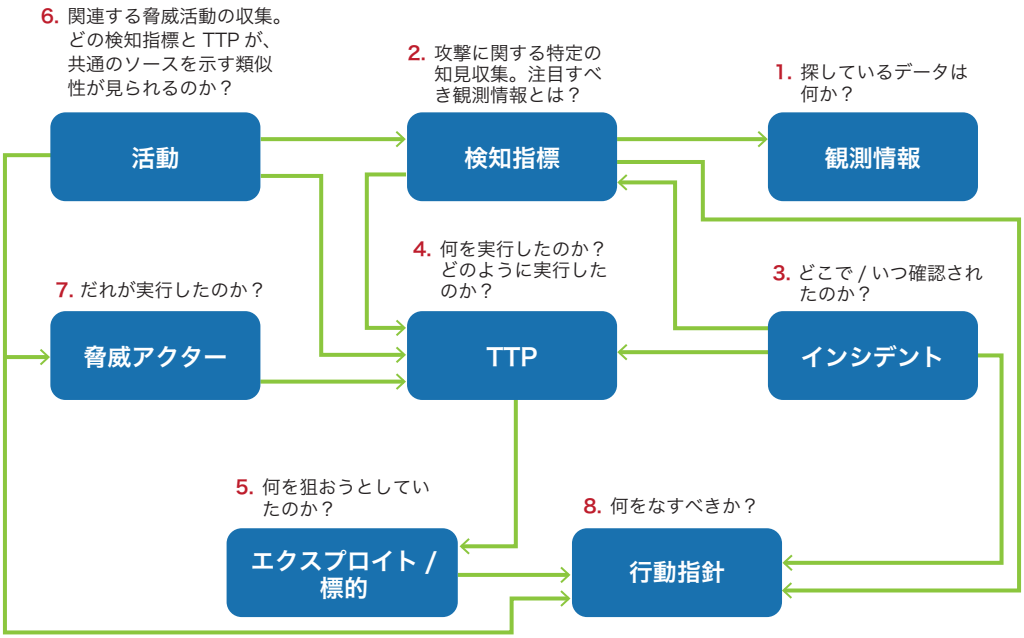


図 9-4. AIS を使用した TAXII による共有方法 [273]

法的留意事項

サイバー犯罪情報をコミュニティ内で広くタイムリーに共有することには多くの利点があるが、共有する際には法的な配慮が必要であり、いくつかの非常に重要な制限が生じる。

管轄権

サイバー犯罪の容疑に関連する情報の共有を検討する場合、最も重要な最初の問題は、管轄権を持つ者を決定することである。管轄権がなければ、検察官には捜査権限がなく、裁判所には判決を下す権限がない。刑事事件または民事事件における管轄権は、行為が行われた場所または被害者がいた場所によって決定される。たとえば、米国では、ある行為がメリーランド州で行われた場合、連邦法に違反していない場合は、メリーランド州が管轄権を持つが、連邦法にも違反しているのであれば、連邦裁判所も管轄権を持つことがある。このモデルは物理的な世界ではうまく機能するが、オンラインで行われる犯罪では、被害者がある管轄区に住み、加害者は別の管轄区に住み、犯罪を実行するために使用されたリソース（被害者にマルウェアを提供したコンピュータなど）が第 3 の管轄区に存在する場合があるという、独特の課題が生じる。サイバー犯罪者は、自分の本当の身元や所在地を隠すために、匿名プロキシやヘッダースプーフィングなどの技術的手段を使用することが多いため、適切な管轄権の決定はさらに複雑になる。

管轄権の決定は、起訴能力に影響するだけでなく、証拠をどのように収集する必要があるか、どの証拠を共有できるか、誰と証拠を共有できるか、証拠をどのくらいの期間保持する必要があるかなどの証拠規則にも影響を与えるため、極めて重要である。また、管轄権に影響を与える具体的な詳細は、捜査開始時には不明であるが、証拠が明らかになるにつれて判明する可能性もある。たとえば、企業の知的財産の盗難は、一見するとドイツから行われたように見えるかもしれないが（記録された IP アドレスを

273 https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

ざっと調べた結果）、調査の過程で得られた追加の証拠が、実際には犯人の本当の所在地はロシアであったことが示す場合がある。

犯罪の種類と規模も、最終的に誰が管轄権を持つかに影響を及ぼす可能性があり、特に連邦レベルでは、複数の機関（FBI、シークレットサービス、DHS（国土安全保障省）、ATF、FTC、SEC）がそれぞれ複数の法令に基づいて、犯された犯罪の種類に応じて管轄権を主張する権限を持っている。第6章では、知的財産の窃盗、個人情報の窃盗、テロリズム／国家安全保障、ランサムウェア／恐喝など、さまざまな種類のサイバー犯罪について詳しく論じている。

米国では、FBIとシークレットサービスの2つが最も突出した連邦機関である。どちらも広範な管轄権を持ち、しばしば重複している。FBIは通常、テロ、国家安全保障、知的財産窃盗と密接な関連がある、または潜在的に左記と関連がある問題で主導権を握る。問題が通貨や銀行の詐欺に関係する場合、2001年の愛国者法によって与えられた広範なサイバー犯罪権限に基づき、シークレットサービスが主導する可能性が高い。[274] アルコール・タバコ・火器局（ATF）（武器や軍需品の密売に関する問題）、証券取引委員会（SEC）（証券法違反に関する問題）、連邦取引委員会（FTC）（消費者詐欺や貿易詐欺に関する問題）など、他の機関が関連分野に関わる犯罪の捜査を主導するが、FBIは少なくともそれらの活動を支援することになる。

現実的な問題として、管轄権はしばしば、犯罪を追及するための利用可能な資源によって、法令と同様に決定される。愛国者法は、シークレットサービスに広範な管轄権を付与することに加え、電子犯罪タスクフォース（ECTF）も設立した。ECTFは、全国約30か所でサイバー犯罪を捜査し、訴追するためにリソースと知識を共有する地方、州、連邦機関で構成された合同タスクフォースである。[275] このようにリソースを出し合うことで、捜査機関は複数の管轄区域の広範囲の人々やコミュニティに影響を与える犯罪に、より効果的に対抗できるようになる。他の国も同様の国内取り決めをしており、サイバー犯罪が国際的な司法権の問題を含んでいる場合には、それらの他の国も参加している。第1章と第8章で述べたように、ブダペストサイバー犯罪条約（「条約185」）とMLATは、各国がこのような捜査に利用する協定の種類を形成している。

犯罪の種類

犯罪の種類は、どのような詳細が共有されるかにも影響する。例えば、IDや機微な個人情報の窃盗に関わる犯罪では、CISAの下では、共有される情報は被害者のPIIを除外しなければならない。PIIは、DHSとDOJ（司法省）によって「特定個人の個人情報または特定個人を識別する情報」と定義されている。[276] このガイダンスにもかかわらず、共有によって身元が開示される状況もある。例えば、標的となったEメールやIPアドレスを開示することは許されない場合でも、発信元のEメールやIPアドレスなど、フィッシングの脅威の発信元に関する識別情報を共有することは許される場合がある。また、DDoS攻撃で使用されたIPアドレスを開示することは、状況によってはそのアドレスと特定の個人を関連付ける可能性があるとしても、一般的には許可される。多くの種類のサイバー犯罪において、CISAやその他の連邦プライバシー法に基づく責任を負うことなく、有用な指標（マルウェアファイルの名前やハッシュ、犯罪の発信元となったドメインやIPなど）や、一般的な感染や攻撃の方法（スピアフィッシング、感染したUSBデバイスなど）を共有することは比較的簡単である。

犯罪が国家安全保障に関わる問題（機密情報の窃盗や送信など）である場合、捜査官は通常、適切に許

274 https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf
275 https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf
276 https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

可されたコミュニティ以外で機密情報や証拠を共有することは許されない。IP（知的財産）の盗難が発生した場合、企業は、コミュニティ内の他のユーザーに警告し、同様の攻撃を防ぐために、標的または盗まれた情報の種類に関する詳細を公開することを選択する場合がある。

配信

攻撃が検出されてから数日または数週間後に共有された情報は、他の防御者や捜査官にとって役立つには遅すぎる可能性があるため、共有の適時性も非常に重要である。このような理由により、および共有できる情報量が膨大であることから、可能な場合は自動化された配布方法が望ましい。上述したように、脅威交換を通じて脅威インジケーターを自動的に共有できるメカニズムがいくつかある。

標準化

ここ数年の間に、サイバー脅威情報を共有するための標準的な形式と仕組みが開発され、広く採用されるようになった。[277] これらの情報共有における標準化は、タイムリーで実用的な情報共有を促進し、多くの企業環境で迅速に運用することができる。下の図 9-5 は、3 つの一般的な基準を示している。

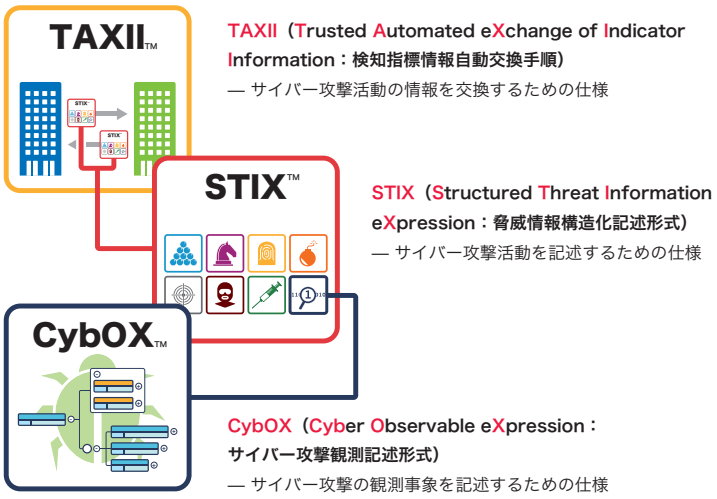


図 9-5. 情報共有の基準

法律または規制制度の一環として必要な内部機密性、共有組織の知的財産を保護するための内部レビュープロセス、または単に共有する情報を完全に開発するのにかかる時間の長さなどの理由で、情報を即時に共有できない場合がある。別の例として、脆弱性を共有すると重大な損害が発生する可能性がある場合が挙げられる。研究者が新しいゼロデイエクスプロイトを発見した場合、責任ある開示の原則では、脆弱性を公表する前にパッチを適用できるよう、脆弱性の対象となるソフトウェアを所有または責任を負う組織にまずその脆弱性を共有する必要があると指示している。

マネジメント

管轄区域に関連する情報共有のさまざまな法的制限、共有の可否がある具体的な詳細、およびサイバー犯罪のカテゴリーは、情報公開の適切なマネジメントプロセスの確立が不可欠な環境を生み出して

277　https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

いる。すべての組織（公的組織および民間組織）は、ポリシーを確立し、文書化し、推進し、それに従うべきである。完全な方針は、下記の主要な構成要素を含んでいなければならない。

すべての組織—公的機関および民間企業—は、方針を策定し、文書化し、推進し、遵守する必要がある。

完全な方針には、以下の主要な要素が含まれていなければならない。

- 開示される情報の種類
- 開示できない情報の種類
- PII（個人情報）、IP アドレス、機密データ、あるいは法律、規定、または方針によって開示が禁止されているものが含まれないように、情報から該当部分を除去する方法
- 開示前に情報を見直す人（または組織）
- 情報を受け取る権限のある人（または組織）
- 情報開示の権限を持つ人（または組織）
- 開示する情報の周知に使用する仕組み

マネジメント方針で、次のような主要な州および連邦政府の法律や規制に準拠するようにしておくことは重要である。

- ECPA（Electronic Communications Privacy Act of 1986：電気通信におけるプライバシー保護法）－通信の傍受方法、格納される情報の収集方法、非コンテンツデータ（電話番号など）の収集方法が規定されている。
- CISA（Cybersecurity Information Sharing Act of 2015：サイバーセキュリティ情報共有法）－民間企業が連邦政府とサイバーセキュリティ情報を共有することを奨励するために責任保護を行う。
- CIIA（Critical Infrastructure Information Act of 2002：重要インフラストラクチャ情報法）
- CCPA（Cable Communications Policy Act of 1984：ケーブル通信政策法）－ケーブル通信プロバイダが収集する PII を規定している。
- COPPA（Children's Online Privacy Protection Act：児童オンラインプライバシー保護法）－児童を対象としたウェブサイトで収集される PII について規定している。
- GLBA（Gramm-Leach-Bliley Act：グラム・リーチ・ブライリー法）－金融サービスプロバイダについて規定している。
- FERPA（Family Educational Rights and Privacy Act：家庭教育の権利とプライバシーに関する法）－教育機関向について規定している。
- HIPAA（Health Insurance Portability and Accountability Act：医療保険の携行性と責任に関する法律）－ 医療提供者について規定している。

民間企業の場合、マネジメント方針は適用される規制を遵守していることを保証しなければならない。連邦取引委員会（FTC）は民間企業を規制し、データセキュリティ違反の証拠を発見した場合は強制措置を講じる。FTC は、「企業のデータセキュリティ対策は、保有する消費者情報の機密性と量、データ操作の規模と複雑さ、セキュリティの向上と脆弱性の軽減に利用できるツールのコストを考慮して、合理的でなければならない」という一般的な基準を適用している。[278] 2023 年現在、FTC はこの基準を満た

278 https://www.ftc.gov/datasecurity

さない民間企業に対して89件のデータセキュリティ訴訟を起こしている。[279]

金融面では、証券取引委員会（SEC）が取引所（規制SCI）[280]とブローカーディーラー（規制S-P）[281]を規制し、取引システムと情報の整合性、およびPIIの保護を確保している。SECは、サイバーセキュリティに関する規制やその他の基準を満たしていない企業に対して強制措置を講じることが可能であり、実際にそのようにしている。2つの顕著な例は、100万ドルの罰金[282]をもたらしたモルガンスタンレーに対する強制措置と、10万人以上の個人に影響を与えたPII開示に関連する金融サービス会社との和解である。[283]

通常のマネジメント手順を無効にしたり、ポリシー違反や規制違反の可能性が生じたりするような方法で緊急通知を行う必要がある状況が発生することがある。一例としては、ダムや航空管制システムなどの重要なインフラを危険にさらす攻撃など、標準的な開示手順を経ることで個人または個人のグループに身体的危害が及ぶ可能性がある計画的な攻撃の検出が挙げられる。このような状況を見越して、情報の共有と開示のマネジメントポリシーには、緊急時に迅速にエスカレーションできる例外プロセスと、情報を共有しなかった際に1人以上の個人に重大な身体的危害が発生するかもしれないと合理的に予想される場合など、同時または事後に承認を求めることができる事前定義された例を含める必要がある。このような状況では、マネジメント手順の目標は、脅威を回避するために必要な最低限の情報のみを共有すべきである。

マネジメント手順では、ポリシー、規制、または法律で要求される決定や通知に関する問題と記録の保持も規定すべきである。これは、決定がいつ行われたか、誰が決定したか、誰に通知されたか、その他の重要なイベントのタイミングに関する文書と記録を含む。これらの記録は、外部監査人または規制機関が主導するマネジメント手順のコンプライアンスを実証できるように、監査可能な形式で保存されるべきである。

共有される情報には、情報の作成者、共有の意図または根拠、情報の取得方法や使用方法に関する条件、情報の取り扱いに関する指示または制限、および情報をいつどのように処分しなければならないかを明確に示す通知が添付されるべきである。

例えば、情報は劣化しやすいため、2週間後には、情報源や方法の開示や防御戦術に関連するその他のリスクが、情報を保持することによるメリットを上回ってしまうことがある。この場合、情報の使用期限を限定し、破棄や廃棄の指示するような通知書を作成することは可能だろう。別の場合では、情報は機密扱いとなり、許可された組織としか共有されないことがある。時には、特定の産業部門のみを対象とし、情報はその業界のISACに参加している企業と共有される場合もある。自動共有の場合、このような通知は、使用事例や共有される情報の種類に基づいてスクリプト化または事前定義される場合があるが、通知は存在し、文書化され、十分に理解されているべきである。

場所

情報共有についての議論は、情報共有が行われる場所についてもまとめなければ終わらない。先に挙げた場所は米国の組織にとっていくつかの提案を示しているが、一般的には組織は次のようなコミュニティを検討すべきである。

279 https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update
280 https://www.sec.gov/spotlight/regulation-sci.shtml
281 https://www.sec.gov/spotlight/regulation-s-p.htm
282 https://www.sec.gov/news/pressrelease/2016-112.html
283 https://www.sec.gov/news/pressrelease/2015-202.html

- 防御者と捜査官をサポートするための企業の**内部**コミュニティ。上記の情報共有フレームワークの基本的な要素で説明したように、社内で情報を収集して交換することは、共有の他の側面を構築するための重要な基盤となる。
- **業界セクター**内のコミュニティ。たとえば、この章の前半のコミュニティに関する議論で取り上げたように、ISAC[284] の 1 つまたはその他の特別なまたは正式な共有組織など。
- 防御者や捜査官の広範な**コミュニティ**。組織は、TIP（脅威インテリジェンス・プロバイダー）経由の自動フィードであれ、公表された報告書やブログであれ、情報、指標、分析を広く公表することによって、これらのコミュニティと共有することができる。

米国政府内では、情報共有は通常、国土安全保障省（DHS）を通じて行われる。そのような DHS プログラムの 1 つは、自動指標共有すなわち AIS[285] である。AIS プログラムは、前述の STIX および TAXII 基準を用いた「高度検知指標共有」を提供している。PII の最小化と保護に関するガイドラインに従って AIS プログラムを使用して情報を共有する組織は、特に PII の開示と、共有された情報の結果として政府が開始する可能性のある規制措置に関連する、特定の重要な法的保護が与えられる。下記の図 9-6 を参照のこと。

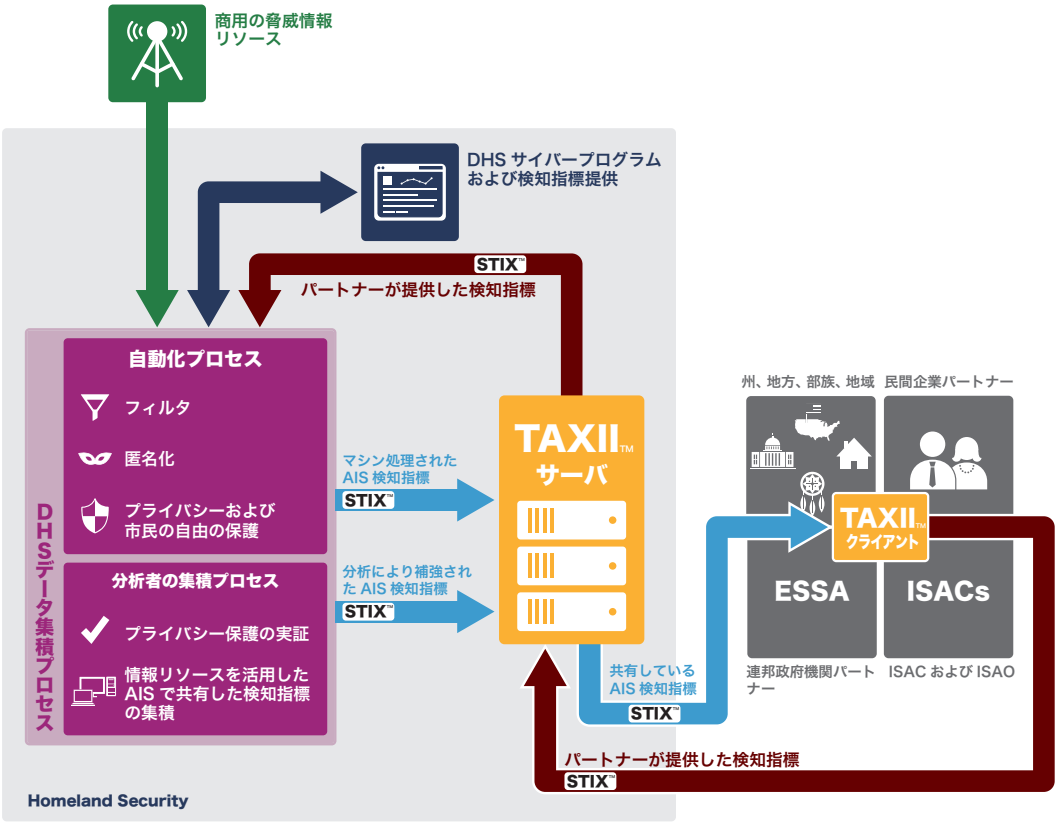


図 9-6. 米国における情報共有の位置相関図

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪の捜査プロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、犯罪の種類、利用可能な証拠の情報源を決定す

284 http://www.nationalisacs.org/member-isacs
285 https://www.dhs.gov/ais

ることに依存し、証拠の収集と分析における実践的手段によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

第9章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

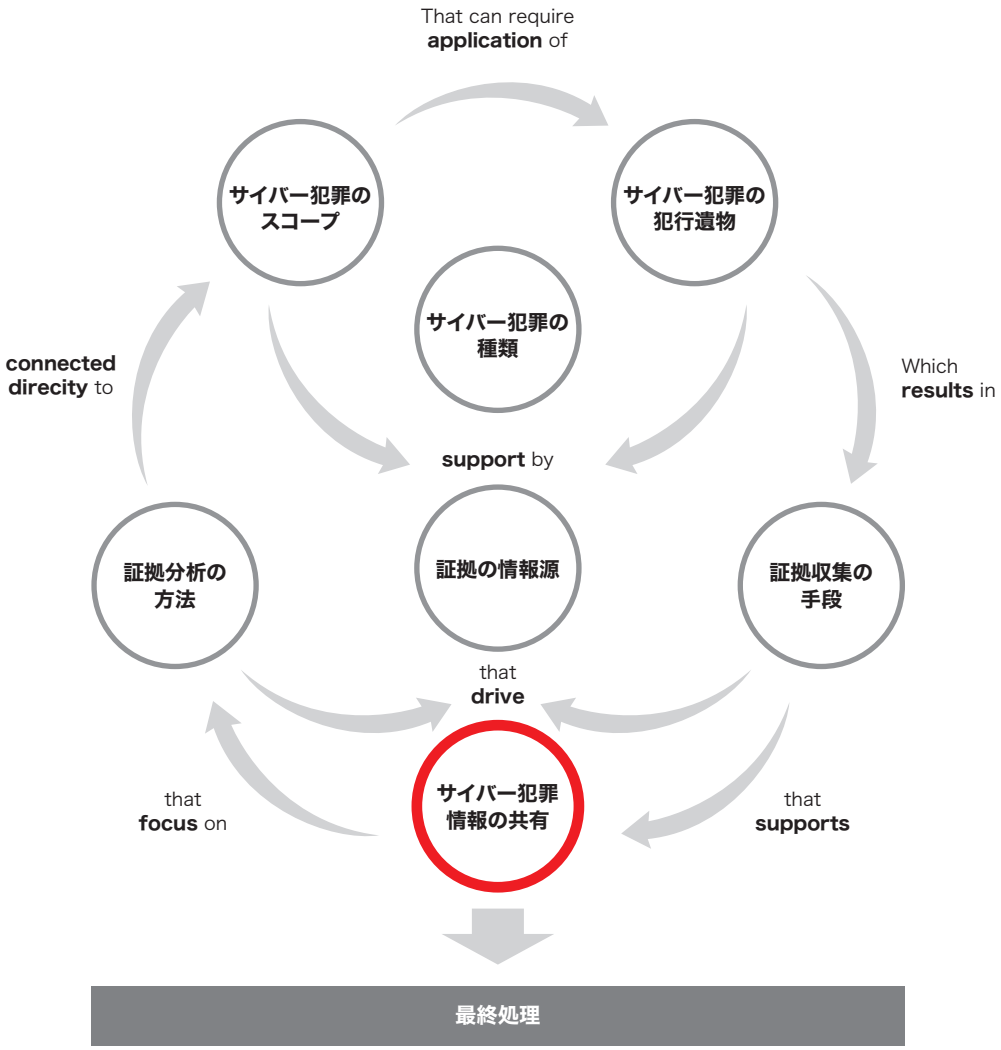


図 9-7. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークとスキルおよび知識の CIBOK 分類法（表 9-1）との関係は、機能要件が関連する役割によって異なることを示している。

表 9-1. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 9-2. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査管理 – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査マネジメントの機能は、共有すべき情報とその普及／配布方法をマネジメントすべきである。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。知見収集は、組織の方針で指定された場合を除き、情報を収集するが、配布すべきではない。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。捜査官は情報を収集し分析すべきだが、共有するのは組織の方針に従った場合のみである。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制や法律に関する指針は、情報の共有に対する制限や罰則を規定する。これは、司法機関が捜査官および知見収集機能に関する方針を定義するのを支援し、経営陣に必要事項を伝える際に役立つ。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪のスコープに応じて、方針に基づきながら、また、どの組織・職務・人員が影響を受けるのかを考慮しながら、何を、だれに、いつ、伝えるのかを決定する。予防啓発は、法的制限に従って、適切な外部機関との効果的なコミュニケーションを確保するために、司法当局と調整しなければならない。

後方支援 – 情報収集と捜査活動を支援するため、サイバー犯罪の捜査範囲と方法について手続き上の理解を必要とする。

総務人事 – 証拠を収集および分析するために、手順の理解、調査の意図、組織能力を必要とする。

第9章:レビュー

1. **サイバー犯罪情報を共有する理由は何か**
   答え：組織内外の他の捜査官・調査員を支援し、実戦的に役立つ知識を増やす。
   例：攻撃を受けた組織は、類似した TTP や反映された IoC を経験した他の組織から恩恵を受けることができる。

2. **誰がサイバー犯罪情報を社内外で共有すべきか**
   答え：権限を持つ者のみ。
   例：RACI によって異なるが、一般的には法務部門と広報。

3. **共有する情報の種類および共有する時期を規定する要件は何か**
   答え：標準化と統制。
   例：STIX/TAXII/CybOX（Cyber Observable eXpression）、GLBA、HIPAA など。

4. **どのようにどんな場所でサイバー犯罪情報を共有すべきか**
   答え：社内、業界の関連団体、コミュニティ。
   例：組織のその他の機能、ISAC、OSINT/PROPINT フォーラム。

ケーススタディ9:モバイルアプリケーション決済詐欺

- **犯罪**：情報（個人情報）の盗難と詐欺
- **容疑者**：アクセスブローカーと少人数グループ
- **手段**：ソーシャルエンジニアリング、フィッシング、暴露された認証情報、マルウェア（情報窃取）
- **動機**：詐欺を行う
- **機会**：不十分なセキュリティ対策（フィッシングに対するセキュリティ意識の欠如、不適切なパスワードマネジメント、弱い身元確認など）が原因で、メールアカウントやユーザー認証情報が侵害される。

2024 年、ある捜査官は、法執行機関から、世界的企業のモバイル決済アプリケーションの顧客に影響を与える詐欺事件の捜査に協力するよう要請を受けた。被害者の認証情報が盗まれ、モバイル決済アプリケーションを通じて不正な支払いを行うために使用された。一部の支払いは対面で行われたが、攻撃者は不正な購入も行い、それを米国の住所に発送していた。

調査の過程では、高度な帰属および分析技術の研究と活用が行われ、さまざまなツールと強化された OSINT が活用された。調査結果の詳細は以下のとおりである。

●初期データの収集と共有

法執行機関から提供された初期情報は、漏洩した電子メールアカウント、疑わしい IP アドレス、不正取引の詳細などを含んでいた。このデータは、構造化されたインシデント対応プロセスに従って捜査官と共有され、適切な証拠の連鎖を確保し、正確な分析を可能にした。

●外部ソースとの連携

その後、捜査官は、法執行機関、グローバル企業、捜査官の間の既存のパートナーシップの一部であるデータ侵害データベースと脅威インテリジェンスツールにアクセスした。これらの情報源は、不正アクセスされた認証情報と IP アドレスに関する追加の文脈と裏付けを提供した。

●確立されたフレームワークの活用

捜査は、タイムリーで安全な情報共有の重要性を強調するサイバー犯罪情報共有フレームワーク（CISF）に従って行われた。このフレームワークは、捜査官が情報を効果的に収集、分析、および配布するのに役立った。

●匿名化とコンプライアンス

2015 年のサイバーセキュリティ情報共有法などの法的要件と規制要件に準拠するために、PII と機密性の高い企業データは、共有される前に匿名化された。これにより、共有データがプライバシーや知的財産を侵害することがなくなった。

●安全な通信チャネル

捜査官は、暗号化されたメッセージングアプリと安全な通信チャネルを使用して、法執行機関やグローバル企業と情報を交換した。新たな脅威に迅速かつ効果的に対応するには、リアルタイムの暗号化通信が不可欠だった。

●リアルタイムの情報共有

同様に、捜査官はグローバル企業のセキュリティチームとリアルタイムの更新情報や調査結果を共有し、関連する脅威に対応するために防御戦略を迅速に適応できるようにした。場合によっては、交換される情報の機密性と完全性を確保するために、安全なメッセージングアプリを使用して安全なリアルタイム通信回線が確立された。共有された情報は、フィッシング攻撃に使用される悪意のある IP や電子メールアドレスなどの IoC を含んでいた。

●リサーチ方法

グローバル企業から提供された情報を受け取った後、捜査官はさまざまなソースを検索し、不正アクセスされた電子メール、デバイス、IP アドレスを分析した。見つかった各結果は、クライアントから提供されたオリジナルのデータであるかのように、徹底的に分析された。参照した情報源は下記のとおり。

- **データ侵害データベース**：分析された電子メールとプレーンテキストのパスワードが複数回公開されていることが検出され、パスワードが更新されていなかったり、サービス間で共有されていたりすると、アカウントを完全に制御するのが可能になる。さらに分析を進めると、Badoo の侵害（2016 年に最初に発見）が、暴露されたすべてのアカウントに共通する参照ポイントであることが判明した。
- **OSINT ツール**：ソーシャルネットワークがフィッシング攻撃メールに関連付けられ、そのメールは米国のマーケティングおよび広告の専門家のものであることが特定された。
- **脅威インテリジェンスツール**：攻撃に使用された一部の IP アドレスから悪意のあるアクティビティと疑わしい大量のトラフィックが検出され、マルウェアとの接触の可能性があることが示された。

●調査概要

その後の分析により、攻撃者が侵入やユーザーのデバイスに感染したインフォスティーラーファミリーを通じて、どのようにしてこの世界的な企業の顧客の電子メールアカウントを制御したかが明らかになった。攻撃者は乗っ取ったメールアカウントを使用して顧客の支払いプラットフォームにアクセスし、グローバル企業のアプリケーションのパスワードとPINをリセットし、不正アクセスされたメールアカウントにリセットメールを送信して詐欺的な取引を実行した。

攻撃者は、侵入やインフォスティーラーを利用するだけでなく、攻撃を補完し、より多くの被害者を狙うフィッシング活動を開始し、電子メールでグローバル企業の顧客に連絡して個人の認証情報（グローバル企業のプラットフォームで使用されるIDとPIN）を要求した。攻撃者は侵害されたアカウントのリストを使用して、最終的にさまざまなデバイスからグローバル企業のプラットフォームにアクセスし、銀行口座の詳細が記載されたアカウントを切り替えて詐欺的な支払いを実行した。

捜査官は、複数のモバイルデバイスが不正操作に使用されたという証拠に基づいて、攻撃は小規模なグループによって実行された可能性があると判断した。この情報は、支払いが実際に行われた場所の防犯カメラの画像やビデオで確認できる。詐欺が行われた物理的な場所に現れずに、別の犯罪者（または複数の犯罪者達）が遠隔で技術的な操作を指示していた可能性もある。

●結論と提言

調査の結果、この詐欺は、電子メールの認証情報を盗むインフォスティーラー（ソーシャルエンジニアリングを介して）に感染した顧客のデバイスによって実行され、攻撃者に繰り返しアクセスを許してしまっていたことが明らかになった。このリスクを軽減するために、顧客は不正アクセスされたデバイスからマルウェアを削除し、電子メールと支払いプラットフォームの両方のパスワードを変更することが推奨された。さらに、電子メールとグローバル企業のアプリケーションに2要素認証（2FA）を導入し、使用をクライアントのモバイルデバイスのみにリンクすることが推奨された。

捜査官は、NIST SP 800-63の要求要件にに従い、新規ユーザーまたはパスワード変更時のパスワード漏洩をチェックし、以前に漏洩したパスワードの使用を防止するための追加のセキュリティ検証を実装することも助言した。

第10章 管理フレームワーク

はじめに

官民に関係なく、どのような組織であってもリソースには限りがあり、その中で各種機能とそれに関連する手続きを支えている。リソースは規模の効率と応用の範囲を考えてマネジメントしなければならない。組織にとって、サイバー犯罪におけるインシデント対応や調査、最終解決は比較的新しい活動であって、これまでは一般的な機能（経理や総務、情報サービス、顧客サポートのように）として設置されてはいなかった。

組織機能としてのサイバーセキュリティは比較的新しい要素である。実行機能は、法務、IT、マネジメントを含む複数の戦略的組織機能にマトリックス化されており、運用の能力は、IT やマネジメントなどの共有サービス機能とビジネスユニット、およびそれぞれの機能要件と規制要件との間で交渉される。

2013 年以降、サイバー犯罪とその事業継続性への影響（業務への直接的影響と市場パフォーマンスへの間接的影響の両方）に対する認識が高まるにつれ、より高い可視性と防御戦略（能動的と受動的の両方）の必要性もそれに応じて進化してきた。これにより、ファーストパーティおよびサードパーティのサイバーセキュリティマネジメント構造、戦略、および関連ツールに変化が生じた。セキュリティオペレーションセンター、サイバー緊急時対応マネジメント計画、サイバーインシデント対応計画は、取締役会レベルの説明責任を伴う業界の義務になっている。事業の優先順位との整合性を確保するために、サイバー犯罪の調査機能を組織のリスクマネジメント機能に統合する必要性が高まっている。

本章では、サイバー犯罪捜査機能のマネジメントフレームワークを構成、計画および実行するための構造と枠組みについて説明する。情報サービスがあらゆる組織機能をサポートするように拡大し、マネジメントフレームワークが進化したのと同様に、サイバーツールで実行された犯罪やサイバーTTP によって促進された犯罪は、組織が調査し、防御し、関連する手順とツールで定義する新しい次元のものとなっている。階層型およびマトリックス型の組織構造についての説明は、サイバー調査機能および人員が実行する活動の在り方に関連付けられる。さらに、テクノロジーとビジネスの間のギャップを埋めるために、サイバー犯罪捜査機能はリスクマネジメントのベストプラクティスと統合される。

本章では、そのような要件に応じて効果的に証拠を収集する方法を作り上げるための参照フレームワークを捜査官・調査員向けに提示する。さらに、防衛と予防に関連する方針やシステム、手続きを、組織のマネージャー職が定める上で参考となる情報を提供する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪捜査・調査および最終解決の機能（以下 CI 機能）の目的は何か
- 本機能はどのように組織し、マネジメントすべきか
- 本機能の戦略的な目標は何か
- 本機能はガバナンス機能やマネジメント機能とどのように関係すべきか
- その機能に必要なリソース（スタッフ、ツール、コミュニティ）は何か
- 本機能のスタッフ割り当て、マネジメント、指導／統制にはどのような技術的・経験的要件があるか
- 本機能（およびそのスタッフ）のパフォーマンスはどのように測定すべきか
- 組織をうまく機能させるには、どのような組織コミュニケーションと戦略的な関与を、組織のどのチャネルに組み込むべきか
- サイバー犯罪とその捜査・調査および最終解決の機能は組織のどの幹部機能の配下とすべきか

管理フレームワークにおけるトピックス分類

下記の図は、「マネジメントフレームワーク」知識領域のトピックス分類を示している。

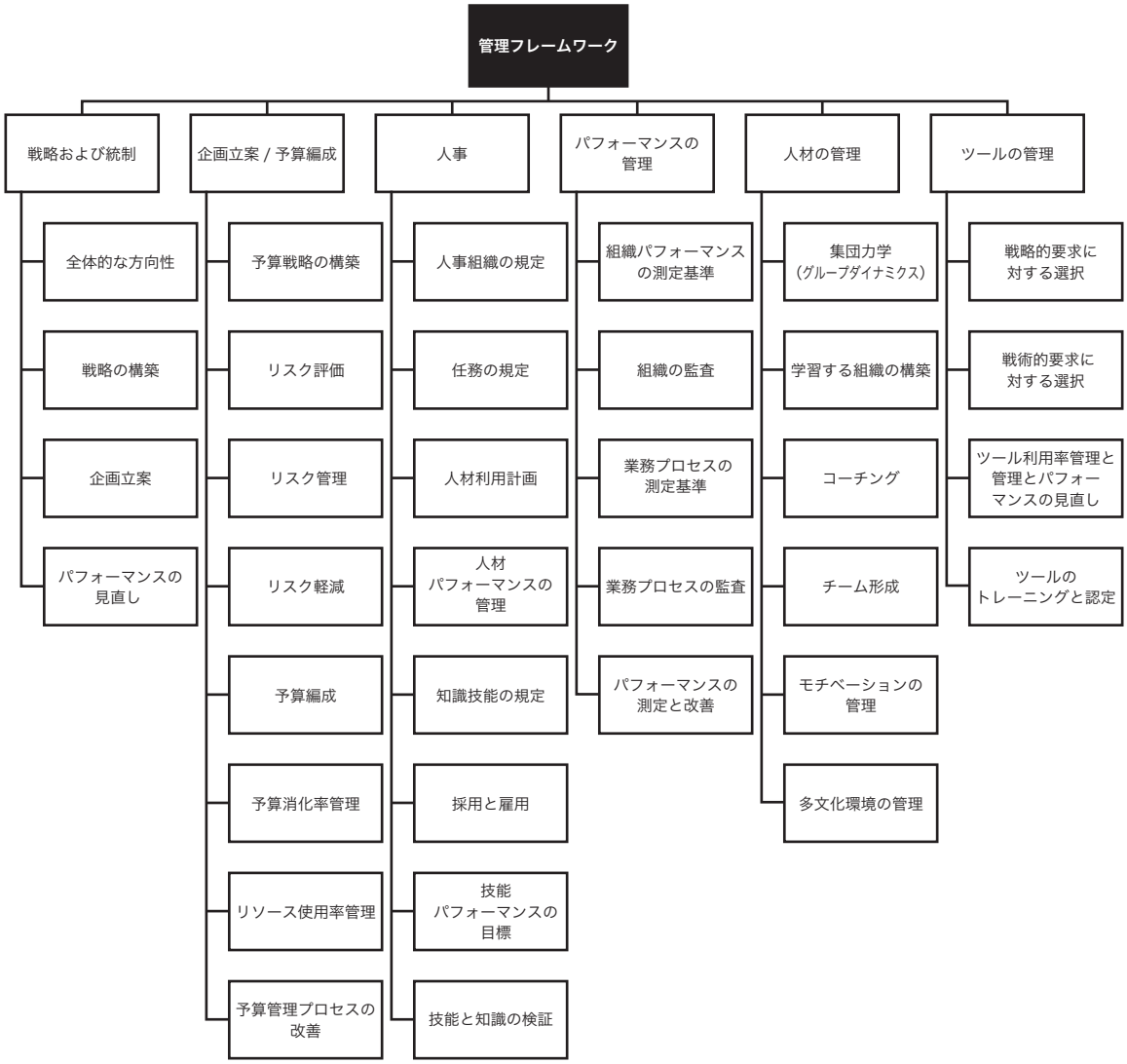


図 10-1.「マネジメントフレームワーク」知識領域におけるトピックスの分類

サイバー犯罪捜査・調査のマネジメントフレームワークとは?

会社組織は、風評リスク（レピュテーショナルリスク）、法的な通知義務、そして比較的新しい「脅威情報の共有」の指令といった相反する要素に直面しており、これらの理解が極めて重要である。これらは今日のほとんどの企業にとって現実的な原動力であり、これらの要件を理解することは、公的機関であれ民間企業であれ、サイバー犯罪の捜査・調査速度の向上に役立つ。

前述のように、サイバーインシデントの対応と調査は新しい活動ではないが、プライバシー侵害[286]に関連する報告義務や罰金などによる政府の監視が強化されたことで、潜在的な責任を考慮して、調査機能の適切な計画とマネジメントの重要性が高まっている。もう一つの複合的な要素は、最近の民間部門のサイバーセキュリティ情報共有指令[287]であり、これは過去および進行中のサイバー犯罪活動に関連する組織内に含まれる調査インテリジェンスを認めている。さらに複雑な要因は、サービスとしてのサイバー犯罪（CaaS）の進化である。例えば、高度な技術を持った犯罪者がダークウェブを通じて商品やサービスを交換して犯罪を行う場合、従来の技術指向のITセキュリティマネジメントやインシデント調査の枠組みでは不十分である。何を、どのように行うかのみに焦点を当てるだけでは、適切なリソースの割り当てと効果的な対応を検討することはもはや不可能である。代わりに、犯罪や違反の背景を把握した上で、誰が、なぜ行うかに焦点を当てて、犯罪の目的、動機、目標を調査しなければならない。

サイバー犯罪解決の要素と融合したサイバーセキュリティインシデント対応と調査という新たに評価された役割は、これまで共通の機能として組織化されていなかった組織にとって比較的新しい活動である（財務、マネジメント、情報サービス、顧客サポートと比較した場合）。サイバーセキュリティとサイバー犯罪の捜査は、多くの共通の技術的および手続き的方法、ツール、トレーニングを共有している。しかし、マネジメント機能と目標に関しては必ずしも同じことが当てはまるわけではない。というのは、サイバーセキュリティは、事業継続と情報保護を主な目標としてビジネス機能をサポートするITとMISのサポート機能だからである。サイバー調査は主にリスクマネジメントをサポートするものであり、IT手順とは大きく異なる特定のインテリジェンスと証拠の生成および管理手順を備えている。

進化するサイバー脅威に効果的に対処する既存のサイバーセキュリティフレームワークやガイドラインは数多く存在するが、提案された対策や制御をすべて実装するには膨大な資金と人的リソースが必要となり、取締役会や経営幹部にその有効性を証明するのは非常に困難である。そのため、ビジネスリーダー、利害関係者、セキュリティ部門、サイバー調査機能の間で、ビジネス戦略に関するリスクプロファイルと優先順位の整合性を保証することが重要である。この議論の根底にあるのは、組織内で何を保護すべきかについて共通の理解を確立する必要性である。このことを理解しない場合、調整が不十分で分散した対策や取り組みによって組織のリソースに負担がかかり、結果としてより多くの投資と採用が必要になる。リスクをマネジメントするためのリソースの不適切な配分は非常に多く見受けられる事態であり、その結果、最も重要な事業戦略上の主要業績評価指標（KPI）と切り離された「サイバー犯罪調査機能」が生じてしまい、資産、データ体制、および認証情報などのID、衛生マネジメントの低下などの影響を招くことになる。

サイバー犯罪捜査・調査マネジメントフレームワークは、サイバー犯罪捜査・調査機能の目的、役割、範囲、目標を明確にすることで、これらすべての課題に対処する。

---

286 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC and http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

287 https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

戦略およびガバナンス

サイバー犯罪捜査・調査の目的を組織の機能として戦略的能力に組み込むには、その目的を理解しなければならない。戦略には、CI 機能、その有用性、組織方法、および責任ある構造の定義が必要である。サイバー犯罪捜査・調査は単なるセキュリティまたは IT の機能ではない。

全体的な方向性（ビジョン、ミッション、目的など）

CI 機能の目的は、根本原因分析フレームワーク[288]を利用して、サイバー行為者が行った犯罪やサイバーツールによって明らかにされた犯罪の捜査・調査要件を意思決定者が理解できるように支援し、必要なリスク認識ポリシーとトレーニング（および必要なツール、人員、サポート）を計画し、組織に装備して、それらのリスクを防止またはマネジメントできるようにすることである。

CI を戦略的機能として位置付け、組織の役割に組み込むには、組織はビジネスニーズや戦略、所有資産、資産の活用により提供される価値に応じて、保護する対象（マネジメント範囲やリスクシナリオ）を定義しなければならない。保護対象を明確にすることで、CI 機能の目的が明確になり、割り当てられた責任を果たすための効率的な構造と方法論が決定される。

民間部門におけるガバナンスの重要性により、すでに多くの企業が取締役会を含む上級マネジメント層と統合されたサイバーセキュリティマネジメントシステムを導入している。さらに、世界経済フォーラム（WEF：World Economic Forum）は、全米取締役協会（National Association of Corporate Directors）およびインターネットセキュリティアライアンス（Internet Security Alliance）と協力して、企業がサイバー犯罪に対してより強靭になるよう支援するサイバーリスクに関する取締役会のガバナンス原則（Cyber Risk Board Governance Principles）を作成した。サイバーリスクマネジメントは経営課題として扱うべきであるというコンセンサスが形成されており、この傾向は今後さらに強まると予想され、民間部門における CI 機能のさらなる調整が必要になる。

その CI 機能が組織のスタッフや意思決定者に示すべきビジョンは、経験と専門知識に裏打ちされた能力を発揮し、その機能を支える業務を遂行する姿であるべきだ。。民間組織では、CI ビジョンは経営戦略や事業戦略に基づいていなければならない。CI 機能のミッションは、最終的には事業中断のリスクを軽減し、同時に、抑止または是正措置（ポリシー、手順、トレーニング、技術的能力を含む）を通じて将来の再発を防ぐ修正措置を通してインシデントを解決することである。組織がそのミッションとビジョンを実現するためのリソースは限られている。CI 機能の戦略を策定する前に、経営マネジメントと戦略に沿ったサイバーリスクとテクノロジーリスクを理解する必要がある。これにより、サイバー犯罪者のターゲットと目的を理解し、ビジネスの優先順位を考慮し、CI 機能とビジネスリスクマネジメント活動を統合した効率的で有意義なリソース割り当てが可能になる。

戦略の策定

説明された目標（ビジョン、ミッション、および目的）を達成するには、組織はリスクマネジメント、情報セキュリティ、法務の領域にわたって CI 機能を整合させる必要がある。すなわち、アセスメントを通じて犯罪を特定し、（管轄区域および組織的による）承認された手順を通じて調査し、技術的および組織的なポリシーと修復努力を通じて解決するのである。そのためには、CI 機能の戦略の策定が必要である。

このような戦略的活動と必要な取り組みの必要性は、法執行機関などの公共組織においても 2013 年に

288 https://en.wikipedia.org/wiki/Root_cause_analysis

欧州連合と欧州評議会によって研究開発活動として資金提供された「GLACY」（サイバー犯罪に関する世界的行動、英：Global Action on Cybercrime、仏：*Action globale sur la cybercriminalite*）[289] と呼ばれる計画委員会で説明されている。関連するプロジェクト報告書「法執行機関訓練戦略プロジェクト地域別戦略」[290] では、プロジェクトに期待される成果として、以下の戦略目標が挙げられている。

- 意思決定者の関与
- 立法の調和
- 司法トレーニング
- 法執行機関の役割
- 国際協力
- 情報共有
- 進捗評価

これらの目標は公共政策や政府／法執行機関の指示のために定義されたものであるが、ビジネス用語で簡単に翻訳すると、民間部門の組織にも一般的に適用できる。

- 意思決定者の関与
- トレーニングとコミュニケーションを通じたサイバーリスクの予防啓発
- 組織におけるサイバーリスクマネジメントの方針と手順の策定
- スタッフ配置、トレーニング、CI およびリスクマネジメントの人員の備え
- 組織とサイバー犯罪捜査・調査機能のパフォーマンス測定
- 業界および法執行機関との情報共有
- 監査と継続的改善

これらの目標は、下記のような有益な結果をもたらす。

- ビジネスニーズを満たす新しいテクノロジーの導入
- 価値を生まない取り組みの排除
- 最適化された IT アーキテクチャや監視性の改善などを含む、既存の IT およびセキュリティ投資の価値の向上
- リソース利用に関する可視性の向上
- 最適化された人員構成

CI 機能の組織戦略を策定するには、従来のビジネス機能を適応させて、サイバーリスクの認識（前の項で説明したとおり）によるリスク軽減と、調査および解決による修復を組み込むことができるようなコミュニケーションが必要である。サイバーリスクは一般的に状況に応じて認識され、競合するソースへのリソースの緊急割り当てによって戦略的な組織機能が不整合になることがよくある。したがって、CI 機能が実行するために構築する必要がある解決策を通じて、サイバーインシデント対応の目的を理解するための参照フレームワークを持つことは有益である。これらの活動を、各活動の焦点となる目標を含め、順を追って以下の図で示す。

289 http://www.coe.int/cybercrime
290 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168030287b

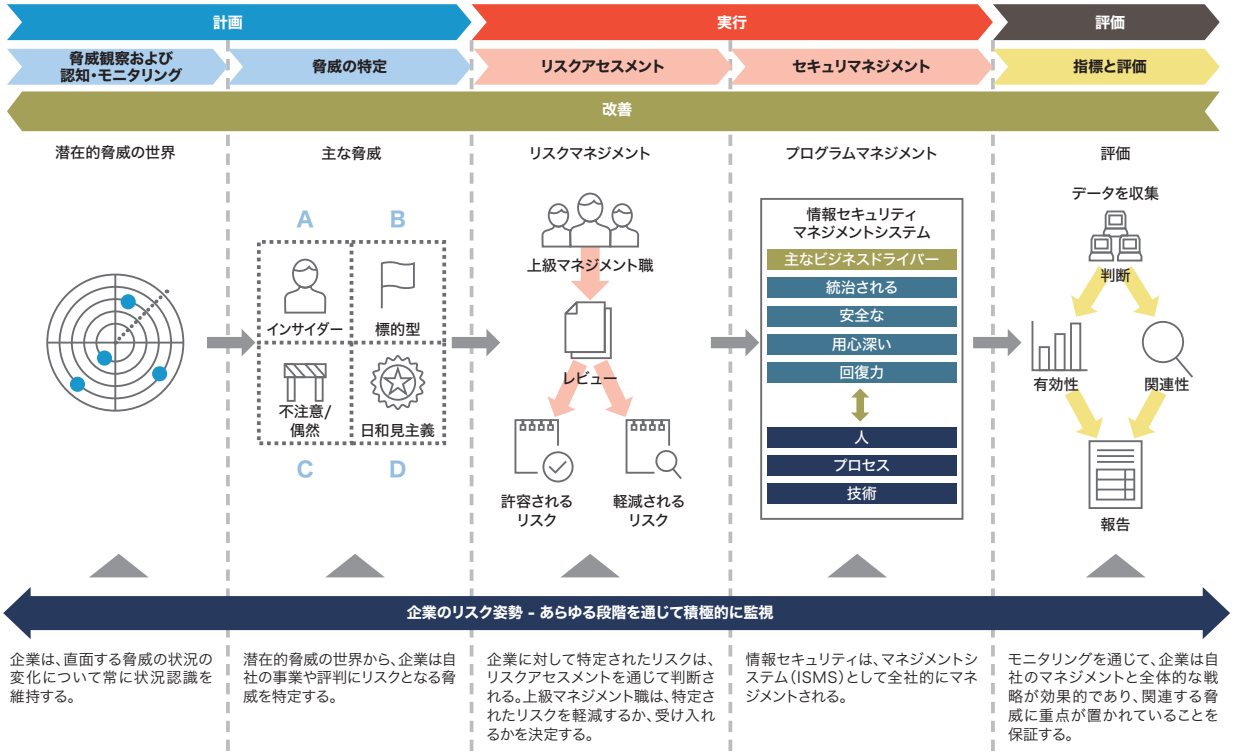


図 10-2. CI PDCA プロセス

前述の図に描かれているように、CI 機能は、組織のサイバーリスクの認識とインシデントに対して PDCA（Plan、Do、Check、Act／計画、実行、評価、改善）を実行する戦略的リスクマネジメント機能をサポートするために、さまざまな目標を持っている。この図は、CI 機能の活動を静的に示すのではなく、組織全体の戦略目標をサポートするための継続的な改善プロセスを示している。これらの活動には、リスクマネジメント目標を協力して達成するために、さまざまな組織要素を含めなければならない。CI 機能は組織の PCDA 構成要素として計画されるべきであるが、OODA（Observe、Orient、Decide、Act／観察、判断、決定、実行）の連続ループとしても機能する。このモデル[291]はもともと軍事目的で作られたものだが、さまざまな形でビジネス戦略の目的にも応用されてきた。サイバー調査に適用する場合、一般的な IT/IS 用語として、以下に示すように「検知」（Detect）、「対応」（Respond）、「修正」（Remediate）、「改善」（Improve）として文脈化することができる。

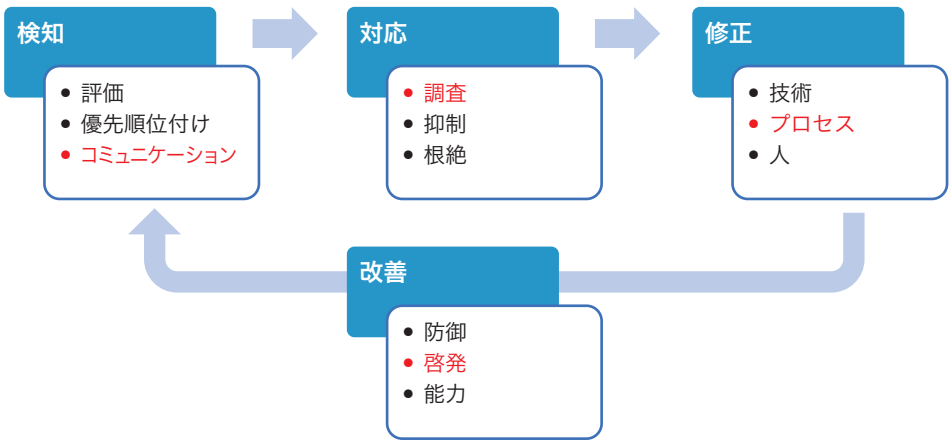


図 10-3. サイバー犯罪捜査の OODA ループプロセス

291　http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html

●検知

「検知」では、CI 機能はコミュニケーションを通じて組織の意思決定者を関与させ、リスクのカテゴリ（情報窃盗、破壊行為、恐喝、盗難、名誉毀損など）と組織への影響の範囲（金銭、業務、従業員、企業ブランドなど）別にリスクの性質を理解させなければならない。例えば、既知のボットネットアドレスとの悪意ある通信に関する SIEM アラートを通じて発見された「バンキング型トロイの木馬」が IT サポートに従事しているユーザーのコンピュータにインストールされていると（調査を通じて）判断された場合、そのリスク（およびそれに対応する組織リソースの割り当て）はマルウェアが財務マネジメント担当者のコンピュータにインストールされていた場合とは異なる[292]。そのため、評価されたリスクは検出時の証拠によって優先順位が付けられ、組織のポリシーと手順に従って適切な対応をとるために経営部門に伝えられる。これはリスクアセスメントの一例であり、トロイの木馬はどちらの場合も同じマルウェアであるが、リスクの性質と適切な対応はその固有のコンテキストに基づいて異なる。

●対応

「対応」目標では、CI 機能は、リスクの性質、範囲、影響を十分に理解するための調査を通じて、サイバーリスクを封じ込めるか、または根絶するかを決定しなければならない。例えば、法執行機関は、調査目的を裏付けるために必要な証拠を収集するまで、検出されたバックドア型トロイの木馬やボット登録ツールを組織から削除しないように要求する場合がある（または、組織がアーキテクチャやポリシーの弱点をより適切に認識するために、悪意のある侵入の意図を理解したいと考える場合もある）。このような場合、リスクをマネジメント可能な影響範囲内に収める必要があるが、封じ込めまたは根絶を追求する決定は、その後の活動に情報を提供する効果的な調査に大きく依存する。前の章で述べたように、対応活動は、リソースの要件と割り当てに関する決定を通知するための評価と調査を通じて情報を収集することを含む。下記の図は関連する状況を示している。

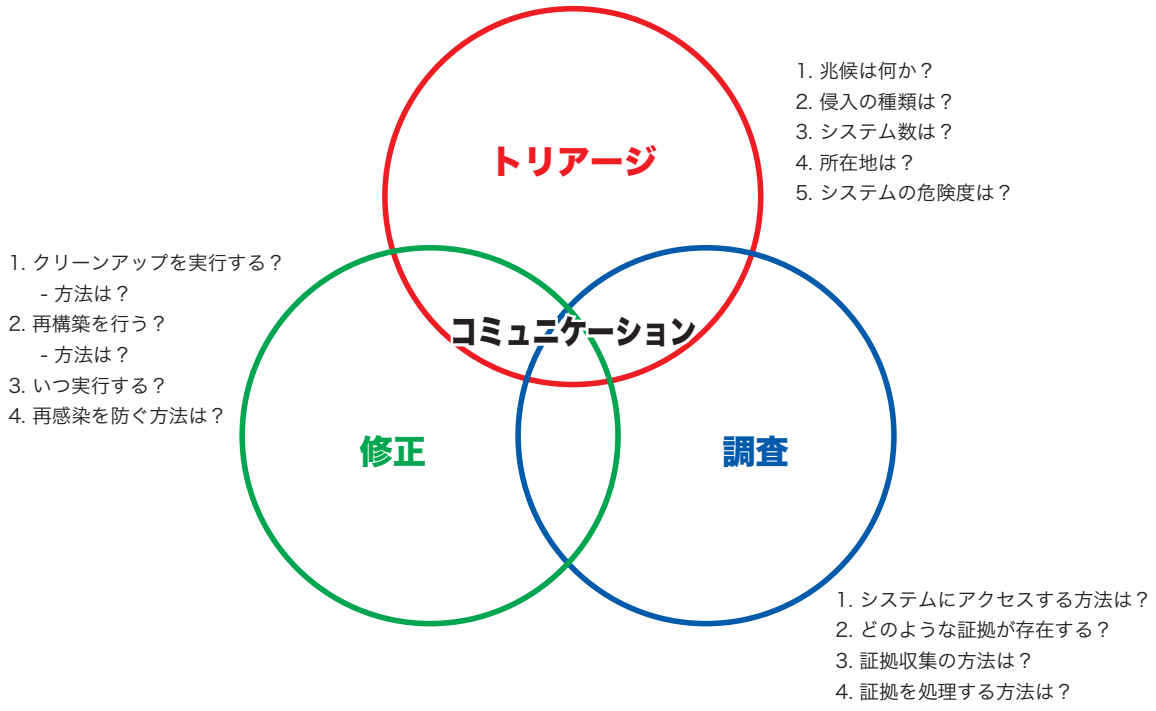


図 10-4. サイバーインシデント対応活動と判断

292　これは、組織のシステム上のバンカー型トロイの木馬が、組織内の他の高関心／リスクコンピュータに侵入するために使用できないという意味ではない。これは、単に通信に関するリスク評価の例である。

●修復

「修復」目標では、人的要因（人）や技術的ソリューションよりもプロセスにおける修復が優先される。例えば、1台のコンピュータにつながるIoCに基づいて、その1台のコンピュータから悪意のあるワームを単に駆除するだけでは不十分な場合がある。ワームはさまざまな形態をとり、ネットワーク内で悪意のある操作を実行する可能性がある。したがって、ワームを識別するプロパティに基づいて（一致するIoCだけを探すことなく）、すべてのコンピュータからワーム自体だけでなく関連するマルウェアも削除する方が効果的かもしれない。臨機応変な考え方や状況に応じたセキュリティツールの選択を含むプロセスは、サイバーリスクの効率的な修復を可能にする効果的な検知と対応活動をサポートする。

非常に多くの場合、組織は検出されたサイバーインシデントやリスクを修復するためにツールに頼りがちである。このアプローチは、問題のツールが正しく構成され、実際に脅威を検出できる限り、うまく機能する。この「ベンダーのジレンマ」は、ますます複雑化するサイバー犯罪への取り組みを通じて、過去10年間にわたって続いてきた概念である。本質的に、このジレンマは疫学と共通する問題を抱えている。つまり、新しいウイルスが発見されると、最初に感染した集団に壊滅的な影響を与える可能性がある。しかし、科学者がサンプルを入手し、それを分析するのに十分な時間があれば、適切なワクチンを開発できることはよくある。初発症例が確認されてからワクチンが利用可能になるまでが、一般の人々にとって最も重大かつ危険な期間ということになる。

この概念をインシデント対応、調査、サイバー犯罪の解決に適用すると、厳しい現実が示される。ベンダーのツールに厳密に依存すると、昨日の脅威のみを検出したり、昨日の脅威から保護したりすることしかできなくなる。サイバー攻撃者は、サイバー捜査官やインシデント対応者と同等かそれ以上に、ベンダーのツールについて熟知している。このことにより、攻撃者はベンダーのツールがTTPを検出できないような攻撃を開発しようとするであろう。

組織を保護するためのツールは、それを使用する人々の技量に依存しており、要件に対するツールの構成（および機能／適合性）によって制限される。例えば、アンチウイルスは、組織や個人のコンピュータ内のマルウェアを検出して修復するために一般的に使用され、信頼されているツールである。アンチウイルス、さらには「次世代マルウェア対策」やEDRツールでさえも、サービスだけでなく、それらが使用するシグネチャ、ポリシー、またはモデルの関連定義ファイル、または特定の修復タスク用に定義される明示的なルールも更新とパッチの適用が必要であり、そうしないと意図通りに機能しない。

アンチウイルスエージェントがホストコンピュータ上で適切に構成されていない場合、他のホストと一貫して更新／パッチが適用されていない場合、または正確で一貫性のある定義ファイルがない場合は、そのツールは実際にサイバーリスクを引き起こし、意図的にまたは単に回避によって悪用される可能性がある。これは、組織が（ニーズに合わない修復ツールに）依存していることと、ツールが設計目的を果たせないことが原因で発生する。

こうしたことは、アンチウイルスコミュニティ内で簡単に見つかり、理解されている。攻撃者は、アンチウイルスツールの検出機能を無効にするために、マルウェアを絶えず修正して操作している。さらに、攻撃者はVirusTotalなどの人気サイトを使用して検知されるかのテストを実施し、独自のマルウェアが手動で検出されてしまうかどうかを判断する。このように攻撃者によって検出を回避されてしまうという制限は、アンチウイルスのコミュニティだけに存在するものではなく、IDS（不正侵入検知システム）やIPS（不正侵入防御システム）などの幅広い技術に共通している現実である。ここからジレンマが始まる。ベンダーツールの弱点が明らかになっているにもかかわらず、そして敵対者がまさにあなたの環境を守るために頼っているツールを対象に攻撃を試行し、調整している可能性が高いという事実があるにもかかわらず、それらのツールなしでは決してやっていけないのだ。

場合によっては、担当者がベンダーツールの機能やその性能の限界を完全に理解する機会、ツールに関するトレーニングを受けた経験がなかったり、データ要素を手作業で調べるためのベンダー以外のス

キルやプロセスを持っていなかったりすることがある。特に、証拠の取り扱い方、優先順位の決め方、適切な手順と対応についての理解が不足していると、致命的なエラーが発生し、証拠の記録が破損する可能性がある。またサイバーリスクのマネジメントを任されている場合、これは別の種類の「サイバーリスク」をもたらす恐れがある。したがって、CI 機能におけるサイバーリスクに対する重要な修復機能を開発するための効果的なツールの選択と実装／マネジメント、熟練した人材の採用、および関連するトレーニングとパフォーマンス評価のプロセスは、関連する修復プロセスと相互依存関係にある。したがって、修復プロセスの定義が必要である。

●改善

あらゆる効果的な戦略には、継続的な改善目標が含まれる。継続的な改善目標を実現する主な要因は、CI 中核領域以外のさまざまな専門知識を持つ機能横断型グループである。過去の失敗（および成功）から学ばなければ、組織は将来の目標を効果的に計画することはできない。これは CI 機能にも当てはまる。改善目標は、認識を高めることで戦略の策定と実行をサポートする。改善点を知るということは、組織の防御と能力を向上させるための偶発的な活動である。改善点の認識は、インシデント調査や関連する技術的修復の結果として得られる場合もあるが、技術的な防御や人材育成の改善に使用されると、CI 機能の進化に役立つ戦略的な支援活動になる。例えば、セキュリティ態勢（組織のサイバーハイジーンと脅威ハンティング活動を含む）の可視化は、数値目標による改善目標の設定に役立つ。また、技術的防御と人材育成の改善に使用すると、CI 機能を戦略的に支援することもできる。上で説明した機能横断的なグループを活用することで、この取り組みの成果物が CI の単一の声ではなく、リスク、IT、法律、その他の一般的なビジネス言語で共有されるため、より広範な改善提案の採択が進みやすくなり加速できる。

インシデントが検出され、調査され、修復され、組織の能力が向上したら、その結果をフィードバックループとして体系的に活用して、新たな検出や調査のその他の側面の改善に役立てるべきである。このフィードバックループは継続的な改善を保証する。

組織の CI 機能の企画立案は、戦略的組織要素によって定義されるミッションと目的によって記述される目標と目的に依存する。一般に、組織の企画立案には、次の表に示す 4 つの主要な機能が必要になる。

表 10-1. サイバー犯罪捜査職務の企画立案

機能	説明	活動
企画立案	将来を展望	組織の目的を達成するための詳細なアクション計画を策定
組織	効果的な組織の構築	リソースの配分および組織を決定
指導	有能な人材を育成	コミュニケーションをとる、モチベーションを与える、鼓舞する、生産性が高くなるよう育成するなど、要員との関係構築
管理	学習と改善	改善に向けたパフォーマンス評価

これらのコアとなる活動は、サイバー調査の機能とマネジメントの役割を説明している。企画立案は、限られた資源を組織化し、それらを効率的かつ効果的に配分することによって、目標を決定するための意思決定の枠組みと、目標を達成するための方法を提供する。リーダーシップは学問的に教えられるものではなく、身をもって学ぶものである。特に、高度に技術的な活動（CI がそうであるように）においては、リーダーシップはオフィスからマネジメントされるのではなく、実践を通じて「示される」のが最善である。もちろん、マネジメントは重要な活動であり、組織のリソース（時間、人材、資金、また

は技術）の消費には説明責任が必要である。これについては、この章の後半で詳しく説明する。しかし、リーダーシップは、スタッフが自身のスキルと知識を開発支援を伴うことが特に重要である。過去の経験から学ぶことは、成長を促すことを支援する役割も持つ。

パフォーマンスの見直し

組織能力の有効性は、次の領域におけるパフォーマンスの客観的評価によって測定される。(1) 中核となる活動、(2) 追加される要件に対応するための適応性、(3) スキルとリソースの活用の効率、(4) 組織の同様のリソース機能との比較評価、(5) 変化の履歴の記録とポリシー／手順／スタッフの変更の相関率、(6) 組織による CI リーダーシップ（トップダウンとボトムアップ）への信頼度合。

1. CI 機能のコアとなる活動は、前述の検出、対応、修復、改善の目標を含む。これらの要素は、「投資収益率」や「投資価値」などの測定可能な値を説明するビジネス影響に関する記述に変換する必要がある。

2. 案件の必要条件に応じて追加の必要条件や短期目標が発生する可能性があり、高業績の組織は、必要に応じて変更を容易にするためにプロセスとスキルを適応させる。

3. チーム編成と「ベストプラクティス」（外部と内部の両方）の採用を通じて手順とスキルが向上するにつれ、規模と範囲の効率性が生まれる。

4. すべての技術的機能は、組織の他のスキルベースの機能における同様の客観的基準と比較することができる。このような比較パフォーマンス分析は、組織機能を向上させるための測定基準値、または差分分析のための基準セット（場合によってはその両方）を決定するのに有用である。

5. 高度な技術を要する環境では、トレーニングや新しい熟練労働者の採用を通じて、積極的なスキルとツールの開発が必要となる。グループまたは機能としてのパフォーマンスの向上は、技術スキルの進化に合わせて手順を相関的に変更することで実現されるが、変更は責任を持ってマネジメントする必要がある。

6. パフォーマンスは、最終的には組織がそのリーダーに対して抱く信頼を反映する。経験から得た確かな技術力と知識を発揮するリーダーは、スタッフから高く評価される。同様に、リソースの効率的な活用と戦略目標の達成を実証するリーダーは、経営幹部から高く評価される。

組織計画／予算編成

予算とコストおよびリソースの割り当て計画がなければ、組織の機能は存在できない。サイバー調査は、歴史的に、通常の業務過程で組織が偶発的に負担する運営コストをもたらしてきた。しかし、適切に計画された組織機能では、必要な施設、機器（ソフトウェアを含む）、戦略的なベンダー契約、および人員に対する予算計画とマネジメントされた実行により、付随するコストの多くを軽減できる。

予算戦略の構築

高度な技術を要する組織能力としてのCI機能には、従来の組織機能に比べて高額な予算が必要である。しかし、前述したように、組織の手順や採用／トレーニングが進化するにつれて、プロセスの効率化によってその費用は削減される。CIは通常、情報技術（IT）コンポーネント機能であるが、内部監査や法務部門などのリスクマネジメント機能に対してドットラインレポートと説明責任を負っている場合がよくある。法執行機関では、CIは通常、2つの非常に異なる要素に分かれている。1つはコンピュータが犯罪を支援するために使用されるもの（殺人事件、行方不明事件など）、もう1つはコンピュータが犯罪の対象となるもの（ネットワーク侵入、マルウェアなど）である。ただし、公的機関であれ民間企業であれ、セキュリティ調査活動としてのCI予算戦略策定の一般的な慣行は、IT予算の10～15%である。

悪意のある内部関係者や、ITまたはセキュリティ／リスクマネジメントポリシーに違反する組織に所属するユーザーが関与するような状況では、IT予算の10～15%の追加コストが、他の組織機能に「チャージバック／ビジネス影響コスト」として割り当てられることがある。「チャージバック」の例として、財務ユーザーが悪意のあるリンクをクリックしてトロイの木馬型のバックドアをインストールし、その後、企業の口座から資金を盗むために使用されるフィッシング攻撃による被害に対して発生したコストは、当該のユーザーが所属する財務部門に対して請求される可能性がある。ただし、組織によっては、情報セキュリティサポートのコストをIT部門に一般化することを選択する場合がある。ただし、後者の場合でも、調査と修復の費用は財務部門に請求されることがある。

調査活動の結果として訴訟が発生した場合にも、「ビジネス影響コスト」が発生する。一般論として、司法当局に対応する場合、ネットワーク侵入の被害者は、経済的損失を明確に説明できなければならない。これには、調査に費やされた時間、回復／軽減に費やされた時間、およびネットワークが利用できないことによるビジネス損失が含まれる。

マネジメントフレームワーク活動としてIC機能のOODAループに関連付けられた予算戦略開発（IT予算の割合として）のモデルを下記に示す。

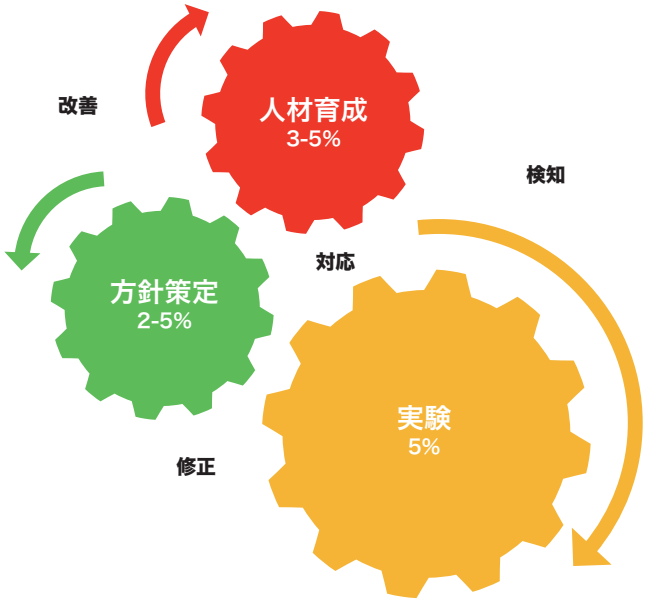


図 10-5. サイバー犯罪捜査の予算編成戦略

戦略的なビジネス機能に対するより具体的な標的設定（事業継続の妨害、貴重な知的財産の窃取、幹部や市場地位の強要など）が進むにつれて、**各ビジネス機能における対応する予算配分**も同様に、サイバー調査と修復に関連する運営費を確保されるべきである[293]。市場競争においてビジネスが成功すればするほど、悪意のある部外者や内部者から標的にされる可能性が高くなる。

リスクアセスメント

情報セキュリティとそれに関連する人的資源に関するリスクの評価に関しては、すでに多くのモデルが組織内で定義され、採用されている。一般的な基準は、国際標準化機構（ISO）27001 の「サイバーセキュリティリスク評価」[294] である。ISO 27001 規格は、下記のような審査基準で 10 件のリスク分野を取り扱っている。

1. 取締役会主導の情報リスクマネジメント体制
2. 安全な在宅勤務とモバイル勤務
3. ユーザーの教育と意識向上
4. ユーザー権限マネジメント
5. リムーバブルメディアの管理
6. アクティビティ監視
7. 安全な構成
8. マルウェア対策
9. ネットワークセキュリティ
10. インシデントマネジメント

293 業界の研究成果としてさまざまな配分モデルが紹介されている。たとえば、グローバルなファイナンスオペレーション企業の多くと政府組織が利用している老舗のソフトウェア会社であるSASが公開しているモデルもそのひとつである。https://www.sas.com/en_us/insights/articles/risk-fraud/a-modern-cybersecurity-strategy-building-a-budget.html。本書で提示している10～15%はSASの提案と似通っているが、サイバー犯罪捜査の予算戦略にチャージバック条件をとり入れている。

294 http://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security.aspx

重大なことは、ISO 27001 には現在、CI 機能、その必要な能力、またはその関連する活動の審査が含まれていないことである。「インシデントマネジメント」の基準は、インシデントを特定して対応するための戦術的な活動と組織能力のみを対象としており、以前に CI 戦略として概説された集合的な目標は扱っていない。NIST SP 800 シリーズ [295]、PCI[296]、BSI[297]、OCIE[298] などの他の標準も、サイバーリスク評価を IT セキュリティの概念としてのみ扱っており、サイバー犯罪活動が達成しようとする犯罪目的（または競争的ビジネス目的）との明確な整合性には言及していない。したがって、これらのセキュリティ特化のガイドラインよりも ISO31000 リスクマネジメントのガイダンスを適用する方が適切となるが、これは ISO 27001、ISO 20000[299]（ITIL[300] とも関連）および ISO 22301[301]「事業継続性」で扱われる課題も吸収できる。

CI 機能をサポートする最も近い既存の規格は、NIST SP 800-86[302] である。ただし、現在のところ、この規格は関連するコンピュータまたはデバイスの収集、調査、分析、および報告を含むサイバー調査のためのフォレンジック技術と手順のプロセスのみを記載している。それは、説明した CI 機能の「対応」（Respond）目標を構成するアクティビティにすぎない。

CI 機能のリスク評価基準を定義して採用するためには、国際的な協力組織によってさらなる開発が行われる必要がある。推奨される行動方針は、ISO 31000 のフレームワークの下で ISO 20000/22301/27001 の抜粋を活用することであるが、前述の CI 目標「検出、対応、修復、改善」に重点を置くべきである。CI 機能のリスク評価も、「情報および関連技術の制御目標」（COBIT）[303] などの ITIL/ITSM（IT サービスマネジメント）ガイダンスに従って含めるべきである。CI リスク評価のサンプル分類は付録 A に含まれている。

リスクマネジメント

COBIT5 は、企業 IT のリスクマネジメントのための推奨フレームワークを提供しており、これを CI 機能に採用し、適切な IT セキュリティマネジメントフレームワークに統合することができる。COBIT フレームワークは、下記のようなマネジメントのための 7 つのリスク原則を定義している。

- 事業体の目標との関連性
- 事業体のリスクマネジメントとの整合性
- IT リスクの費用対効果のバランス
- 公正かつオープンなコミュニケーションの推進
- 「経営トップの姿勢」の確立と説明責任
- 日常業務の一部としての機能
- 一貫性のあるアプローチ

リスク原則は、測定可能で、組織の同様の技術的機能に匹敵する信頼性の高い客観的な結果に貢献できる、リスクマネジメントに対する構造化されたアプローチを提供することを目的としている。COBIT

295 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
296 https://www.pcisecuritystandards.org/
297 http://www.bsigroup.com/en-GB/Cyber-Security/
298 https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
299 http://www.itgovernance.co.uk/iso20000.aspx
300 http://www.itgovernance.co.uk/itil.aspx
301 http://www.itgovernance.co.uk/bc_dr.aspx
302 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
303 http://www.isaca.org/cobit/pages/default.aspx

フレームワークは、次の図に示すプロセスで、一連の「リスクシナリオ」を使用して、組織の IT リスクを検出しそれに対応する能力を示す。

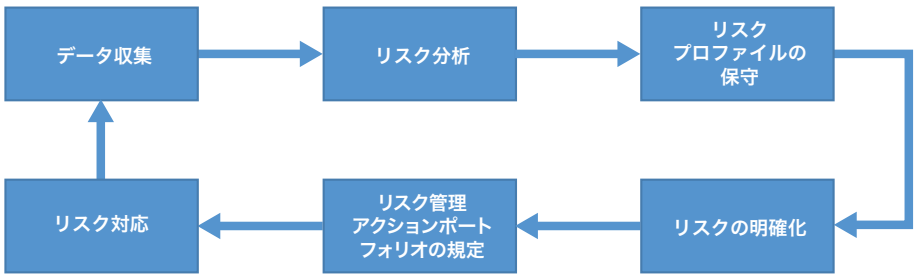


図 10-6. COBIT リスクマネジメントプロセス

COBIT リスクマネジメントプロセスには、IT（さらにはサイバー）リスクに関する検出から対応までのフィードバックループがある。ただし、マネジメントプロセスは、前述した修復や改善のプロセスは含んでいない。COBIT リスクマネジメントプロセスは下記の図で説明されている [304]。

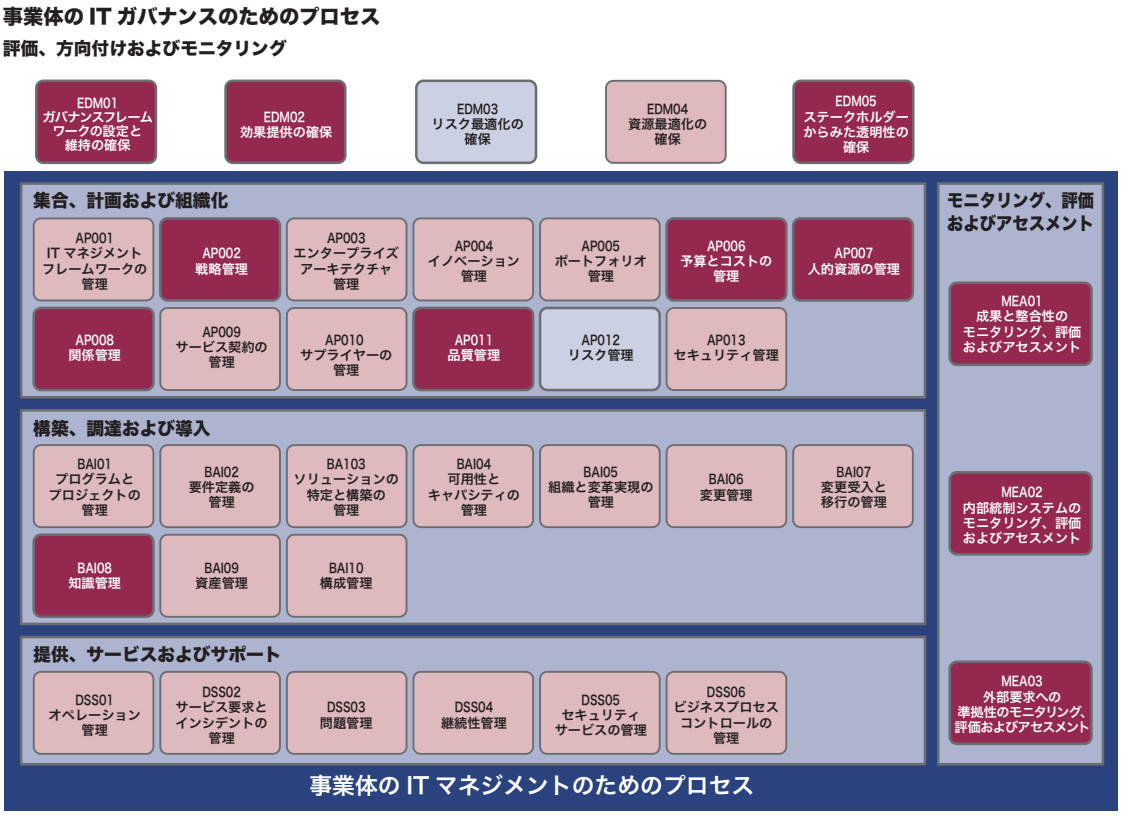


図 10-7. COBIT 5 プロセス参照モデル

図に描かれているように、COBIT5 フレームワークの焦点は IT サービスマネジメントであり、リスクマネジメントに特化していない。これはマネジメントのためのフレームワークを提供するが、ISO27001 と同様に、フレームワークは CI 機能の要件に合わせて調整すべきである。組織の種類に応じて、CI 機能は IT の構成アクティビティである場合もあれば、それ自体が機能ユニットである場合や、調査ユニットの支援アクティビティという場合もある。したがって、「万能」なリスクマネジメントフ

304 http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-5-Risk_res_Eng_1213.ppt

レームワークは存在しない。しかし、COBIT5 フレームワークのリスクシナリオの焦点は、サイバー犯罪に焦点を当てた CI 活動に匹敵するものであり、サイバーリスクを種類やカテゴリー別に調査し、対処する活動には役立つ、他のガイダンスとの明確な違いがある。

前述されているように、テクノロジーの急速な発展とビジネスへの浸透、およびそれに伴う影響とリスクは、近年、CIO/CISO の執行権限と責任（本章の後半で詳述）と、その役割が適切に遂行されなかった場合に生じる可能性のあるビジネスへの影響と損失との間に不均衡を引き起こしている。このような傾向を受けて、ガバナンスとマネジメントの役割と執行責任を分離し、より効果的な役割分担を通じてより健全な企業経営を目指す動きが提唱されている。COBIT2019[305] フレームワークは COBIT5 フレームワークを更新したもので、この概念を実践的に説明し、ガバナンス機能とマネジメント機能の役割と責任をそれぞれ定義している。

●ガバナンス

- 利害関係者のニーズ、状況、選択、焦点を評価し、組織のビジョンと戦略に基づいて目標が合意されていることを確認する。
- 優先順位付けと意思決定により、組織の目標と戦略に最も合致するプロジェクトとイニシアチブに最高の優先順位が与えられ、組織のリソースと整合されて最適化される。
- 目標に対する組織のパフォーマンスとコンプライアンスの遵守が適切に監視されていることを確認する。

取締役会は、取締役会長のリーダーシップの下、ガバナンス全体の実施に責任を負う。ガバナンスが失敗する主な理由は、マネジメント体制の不備、スポンサーシップの欠如、戦略変更に対する柔軟性の欠如、ビジネスとの整合性を無視したリスクの特定への完璧主義的な集中であることに留意すべきである。これらの特徴は、リーダーシップチームの積極的な関与によって是正されなければならない。

●経営マネジメント

経営陣は、ガバナンスによって指定された目標を実現するために、様々な活動の戦略策定、予算編成、リソースマネジメントに加え、活動の計画・構築・実行・評価に責任を負う。最高経営責任者（CEO）のリーダーシップのもと、経営幹部が経営執行の責任を負う。

COBIT フレームワークは、ビジネスリスクと IT／セキュリティリスクを整合させ、企業 IT のリスクマネジメントを支援するのに役立つ。ただし、それを適用するには、専門的なスキルセットとフレームワークの知識が必要である。多くの場合、その内容の複雑さゆえに、実際に適用するのは困難である。バランスよく実施しなければ、「マネジメントのためのマネジメント」のようなマネジメント上のオーバーヘッドが発生する場合がある。不必要なオーバーヘッドは、ガバナンス関連の活動を通じて評価されるべきである。企業経営において、限られた資源に優先順位をつけ、最適な配分を実行するために有効なアプローチが 2 つある。

- ビジネスとの整合：簡素化された COBIT フレームワークを使用して、ビジネス戦略とサイバーセキュリティ活動を整合させる。
- リスクのプロファイリング：リスクを分類し、効果的なリスクシナリオを展開させるために、ビジネスリスクとサイバーリスク（サイバー犯罪者の目的の視点に基づく）を整合させる。

305　https://www.isaca.org/resources/cobit

効果的に組み合わせてマネジメントすれば、サイバーセキュリティに関連するリスクを体系的かつ実践的に調整し、組織の経営目標と優先順位を明確にすることができる。その結果、組織はサイバーセキュリティ活動の一貫性を保ち、CI 機能が有効になり、信頼性と客観的な結果が生まれる。活動に対する広範な主要業績評価指標（KPI）を活用することにより、詳細で測定可能な目標を設定できる。

ガバナンスとマネジメントの目標を設定する際、ビジネス目標との整合性を確保するために COBIT の推奨事項すべてに準拠すると、コストや時間がかかりすぎる可能性があるため、簡素化され調整された COBIT フレームワークを使用することが推奨される。COBIT フレームワークは、各組織内で内容と深さによって個別に定義されなければならないコンポーネントで構成される。組織内に熟練したガバナンスの専門家がいれば、本格的な COBIT フレームワークを採用することができる。ただし、多くの場合、指定された COBIT レビュー手順、設計要素、ガバナンスシステムコンポーネントを抽出して利用することは、利用可能なリソースを使用しながらビジネスの整合性を確保するのに役立つ。ビジネスにおける調整は CIO または CISO が主導すべきであり、下記の手順が含まれる。

●利害関係者の推進力とニーズを理解する

利害関係者の推進力とニーズの理解は、取締役会およびリーダーシップチームとの面談を通じて、懸念事項、重大なリスク、および主要な問題を特定することによって達成される。

●企業、ガバナンス、マネジメント目標の設定

企業目標を設定する際は、利害関係者の推進要因やニーズを取り入れるだけでなく、COBIT の設計要因にある以下の項目を取り入れることができ、明確な目標、特定されたギャップ、アクション項目を含める必要がある。

- ビジネスの背景と企業戦略の理解
- リスクプロファイル
- 業界の法律や規制の遵守
- 脅威の状況
- IT セキュリティ組織の機能の役割
- IT とセキュリティの問題

●目標の調整

目標の調整は、マネジメントするアクティビティを企業目標に合わせてマッピングすることを伴う。COBIT ガバナンスシステムが提示するコンポーネントは、適切かつ信頼できる方法で活動をサポートして実施するのに必要な能力が存在することを保証するために使用されるべきである。これにより、ビジネスと IT の連携が可能になる。組織能力が不十分な場合は、資源配分、追加投資、優先順位の調整を解決するために、取締役会、CEO、またはその他のリーダーシップに問題をエスカレーションすべきである。組織能力には下記のような観点のものがある。

- プロセス
- 組織構造
- 人材、スキル、および個々人の能力
- データ
- 原則、ポリシー、手順
- 文化、倫理、行動

- サービス、インフラストラクチャ、アプリケーション

経営目標を効果的に設定するためには、目標設定の前に、目標整合プロセスで現状、理想的な状態、活動に関する既存のギャップを明確にする必要がある。CIO または CISO は、経営目標を達成する責任を負うべきである。可能ならば、企業の戦略、規制、脅威の状況の変化に応じて目標を柔軟に調整できるように、3〜6 か月ごとに進捗状況を評価すべきである。

ガバナンスの目標を設定するには、経営目標の評価を行い、下記の要件を満たす準備ができているかどうかを判断しなければならない。

- 組織が規定するフレームワークの設定と維持
- 約束された利益の実現
- リスクプロファイリングで可視化されたリスクの軽減
- リソースの最適化
- 利害関係者へのコミットメント

取締役会およびガバナンスを担当するリーダーシップチームは、この評価を行った後、事業責任者、CIO、CISO、およびその他のエグゼクティブリーダーに指示を与えることができる。取締役会は、定期的な監査と連動して、定量的および定性的な指標に関するガバナンス目標を監視し、それらが正しく実行され、約束された利益が実現されていることを確認しなければならない。

リスク軽減

リスクマネジメントにはリスク評価分類法を採用することが不可欠だが、どのリスクを軽減するか（制御によるか、根絶によるか）を判断するには、意思決定者が理解できる評価方式または基準が必要である。リスクの軽減は、コントロール（およびコントロールの失敗）の概念を理解することにかかっている。ほとんどの CI 機能の調査員が（多くの場合、組織の方針や圧力によって）技術的な根本原因を探るが、システムの欠陥、プログラムの欠陥、ルールの不順守が侵害の原因となっていることの方が一般的である。例えば、ユーザーがアプリケーション間でパスワードを再利用したり、単にデスクを離れるときにコンピュータをロックしなかったりというような場合である。

調査という観点からすれば、根本原因分析が非常に重要なのはこのためである。技術的な根本原因を体系的な原因と区別し、そこから得られた教訓を文書化すると、リスクについて実証的な議論を可能にする傾向が現れ始める。すべてのプロセスは、人、プロセス、テクノロジー、リソース、および関連するアクティビティを含む。このため、体系的なリスクを是正せずに放置することはできない。さもなければ組織はインシデントに苦しみ続けることになる。

一般的に使用されるリスク評価の方程式は下記のとおりである。

$$\text{リスク} = (\text{発生確率} \times \text{影響の大きさ}) / \text{軽減能力}$$

その数式を再構築することにより、リスクを軽減する組織の能力は、リスク条件（またはシナリオ）の発生確率にその（推定される）影響を掛け、その値をリスクで割った結果として示されるべきである。

$$\text{軽減能力} = (\text{発生確率} \times \text{影響の大きさ}) / \text{リスク}$$

ただし、数学では答えが得られないこともある。リスクは、確率、影響、軽減能力の主観的な推定に

よって決定される経験的な値であるため、決して単純な計算ではない[306]。リスク軽減計算を活用しようとする組織は、カテゴリリスク（サイバー犯罪の種類やカテゴリなど）に応じてリスク分類の尺度を採用する必要がある。

規模はシンプルで一般的なものとし、1〜3（高／中／低）または1〜10の規模にすべきである。オーストラリア／ニュージーランドのISO31000：2009規格「リスクマネジメント - 原則とガイドライン[307]」は、リスクをマネジメントするための5つのステップを規定している。

1. 文脈を確立する
2. リスク特定
3. リスク分析
4. リスク評価
5. リスク対応

ISO31000は技術マネジメントに適用されるが、記載されている基準には、以下に示す一般的な図[308]のようなリスク計算の例が含まれている。

表 10-2. 軽減のためのリスク査定

全体的なリスクの重要度				
影響の大きさ	高	中	高	最重要
	中	低	中	高
	低	覚書	低	中
		低	中	高
	可用性レベル			

リスクアセスメントを実施する際には、特定されたリスクの計算上の重大性を評価し、組織に影響を及ぼす可能性（確率）に応じて軽減すべきである。しかし、一般的なITと比較すると、CIのリスク評価にはより複雑な要素が関係している。

IT資産のリスクは、以下の図のようなリスクの「ランク付け」によって評価されることが多い[309]。

306 一部のITセキュリティリスクの計算式では、「リスク＝（（脅威 x 脆弱性）/対策）x 影響」が使用されることに注意すること。ただし、前述のように、これらの値は主観的に決定される。
307 https://www.standards.govt.nz/search-and-buy-standards/standards-information/risk-managment/
308 https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
309 https://www.owasp.org/index.php/Application_Threat_Modeling

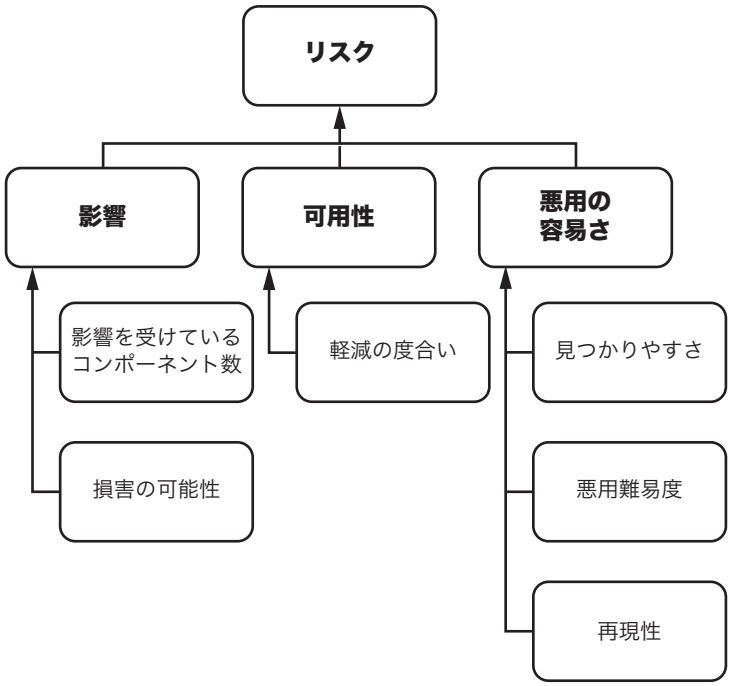


図 10-8. OWASP リスクランキング

リスクマネジメントに対する COBIT5 シナリオアプローチは、OWASP（The Open Web Application Security Project）方法論と組み合わせて、サイバー犯罪のシナリオをタイプとカテゴリ別に定義し、リスク軽減基準を定義することができる。例えば、フィッシングに関連するリスクに関するユーザートレーニングや認識が限られている組織では、そのリスクを軽減する組織の能力がユーザーのリスク認知とトレーニングによって制限されるため、サイバーリスクが発生する可能性が高くなる。したがって、リスクを評価するためのテストシナリオとして、CI 機能がフィッシング演習を実施し、経営陣に結果を報告することができる。この報告には、リンクをクリックしたり関連するバックドアをダウンロードしたりしたユーザーの数（ただし、そのような活動を報告しなかったもの）などの結果を共有することが含まれる。

OWASP 基準の簡単なテストを 1 つでも実行することで、CI 機能は、そのようなアクティビティの潜在的な影響（調査または例を通じて）を、そのシナリオの成功の可能性に関するカテゴリの詳細とともに説明できる。このようなシナリオは、サイバー犯罪行為者によって行われた攻撃や不正アクセスの過去および現在のタイプを反映しているべきである。

予算編成

CI 機能を計画するための予算戦略については既に述べたとおりであり、CI 機能を他の組織との関連性の中でどのように編成するかに応じて、調査コストを組織機能または支援活動に関連付けるための異なるモデルが提示されている。しかし、人件費やツールや設備関連コストは別として、CI は通常、専門的なリサーチ施設を必要とし、認証取得などに関連費用がかかる場合がある。したがって、予算計画は人件費だけでなく関連経費も含んでいるべきである。

The Guide to Computer Forensics and Investigations 第 5 版[310] *は次のことを推奨している。*

310　ネルソン、B.、フィリップス、A.、ステュアート、C.、(2016)。コンピュータフォレンジックと調査ガイド、第5版、コーステクノロジー。http://www.utc.edu/center-information-security-assurance/468--ch03.pptも参照のこと。

1. 費用の内訳を日ごと、四半期ごと、1年ごとの経費にまとめる。
2. 過去の調査費用を使用して、予想される将来の費用を推定する。
3. リサーチラボの経費には以下のものが含まれる[311]。
   a. ハードウェア
   b. ソフトウェア
   c. 設備スペース
   d. 訓練された人員
4. リサーチラボで検査することになりそうなコンピュータ事例の数を推定する。
   a. 検査することになるであろうコンピュータの種類を識別する。
5. 技術の変化を考慮する。
6. 統計を用いて発生しやすそうな種類のコンピュータ犯罪を判断する。
7. この情報を用いてリサーチラボに必要となるものと、それらにかかる費用をあらかじめ計画する。
8. 統一犯罪報告書（Uniform Crime Reporting）の統計を確認する[312]（※中表記に）。
9. 特殊なソフトウェアを利用して実行された犯罪を識別する。
10. 民間企業がリサーチラボを開設する場合は下記の点を確認する。
    a. ハードウェアおよびソフトウェアの資産目録
    b. 前年に報告された問題
    c. コンピューティング技術の将来の発展

このガイドは、「購入するソフトウェアやハードウェアを選択する際には、タイムマネジメントが大きな問題となる」とも述べている。前述したように、採用とトレーニングは、組織がCI機能の効率を高めるのに役立つ。しかし、トレーニングとツールのコストは相互に関連しており、どちらも必要なコストであり、一方の費用を削減するには、他方のマネジメントされた費用の増加が必要となる。ただし、熟練した人材は常にツールよりも優れた投資である。というのは、ツールは限られた目的でしか活用できない一方で、人材はケースの要件により柔軟に対応できるからである。したがって、常にツールよりもトレーニングに投資すべきである。

また、仕事の労働要素を考慮することも重要である。高度なスキルを要する作業には、多くの（比較的）低レベルのサポート、中レベルの分析と開発／トレーニング、そして少量の（しかしより重要な）高レベルの調査とレポート作成を伴う。予算計画には、調査における効用を要素として組み込むべきである。

民間部門のIT予算は通常、収益の割合、または組織内のITユーザー1人あたりのコストとして反映される。公共部門の組織は、収益ではなく費用ベースで運営されている。民間部門のCI機能は一般にITサポートコストに「まとめられる」ため、正確な数字を見積もるのは難しい。ただし、法執行機関などの公共部門の組織は予算要求を公表している。

予算消化率マネジメント

予算の消化率は、予算元帳（単式記帳）に対して「時間と経費」システムによって実行されるべきである。施設、ツール、教育、交通費、関連経費、およびCI機能に割り当てられた人員の時間当たり（または人日当たり）の時間を借方として処理すべきである。他の組織機能に対する時間や経費のチャージバックは、利用可能であれば、同様の方法で貸方として台帳に計上されるべきである。

311 ASCLAD認証やヨーロッパの同等の認証は高額である。これを要求する管轄区域が増えている。http://what-when-how.com/forensic-sciences/accreditation-of-forensic-science-laboratories/

312 http://www.fbi.gov/ucr/ucr.htm

従業員による時間と経費の報告は、少なくとも毎週、可能であれば毎日行うべきである。関連する「エンタープライズリソースプランニング」（ERP）ソフトウェアは、予算計画および追跡／実績の目的で、組織全体の共有サービスとして活用されるべきである。マネジメント費（施設費、設備費、および関連費用、ならびにチャージバック活動による貸方勘定）は、「損益」活動として実施し、経営幹部への週次報告、月次見直し、および組織的コストマネジメントのための四半期ごとの業績公表を行うべきである。緊急の予算リスクに対応したり、将来の要件を削減するための効率性を報告したりするために、半年ごとおよび年間の予算見直しを実行すべきである。

多くのCI機能は法的調査に関連しているため、スタッフは少なくとも1時間ごとに時間報告を行うことが推奨される。場合によっては、税務上の目的で、15分単位の経費や内訳をさまざまなカテゴリ別に報告する必要が生じることもある。

リソース使用率マネジメント

リソースの利用（ツール、設備、人員）は、時間と経費の追跡方針および関係する各種手順と関連付けるべきである。米国で技術者追跡の目的で使用される一般的な数値は、「請求可能な」時間または期待稼働率の1人年当たり2,000時間である。ただし、仕事の満足度を高く保つためには、その数値に関連するリソース効用マトリックスを組み込む必要がある。そうしないと、組織はそれに応じた離職率に直面することになる。パフォーマンスは予算マトリックスで測定されるべきである。

		Hours				
	Hours per year	2,000				
Personnel		Target Utilization	%utilization	# of Staff	$Full Cost	Cost
	Executive	400	20%	1	$ 225,000	$225,000
	Administrative Staff	-	0%	1	$ 50,000	$ 50,000
	Senior Staff	700	35%	2	$ 180,000	$360,000
	Managerial Staff	1,200	60%	4	$ 145,000	$580,000
	Experienced Staff	1,700	85%	4	$ 140,000	$560,000
	Junior Staff	1,800	90%	8	$ 120,000	$960,000
	Interns	1,000	50%	2	$ 60,000	$120,000
Training						
	Annual Policies	80				
	Industry	80				
	Professional/Skills	160				
	Personal Development	80				
Tools						
	Hardware					
	Software					
	Facilities					
Travel						
	Training					
	Remote Sites					
	Legal Support					

図 10-9. 簡単な予算消化率マネジメントの例

予算マネジメントプロセスの改善

時間と経費は予算計画に従って追跡調査されるため、業績は組織のリーダーによって計画され合意された予算戦略と比較されるべきである。コストマネジメントやリソース要件を調整するために、サポートされている組織機能への関連リソース割り当てをチャージバックする機会も検討されるべきである。月次および四半期ごとの業績レビューは機能分野の幹部が実施し、半年ごとおよび年次の業績は戦略計画のサポートのために組織のリーダーに報告すべきである。

人事

人材はあらゆる組織の中心である。どれほど多くのツール、プロセス、手順、ルールが定義され、実施されたとしても、リーダーシップを発揮する人々とそのリーダーシップに従う人々がいなければ、組織は成り立たない。サイバー調査などの高度に技術的な分野では、人材を募集、雇用、維持することが困難である。彼らのスキルや才能（そしてさらに重要なのはその経験）を求める市場は、非常に競争が激しい。これらのリソースの不足と、組織がサイバー犯罪を効果的に防御したり、サイバー犯罪の事件を調査するのを支援するという点におけるそれらの職務の重要性について、慎重な検討が行われるべきである。

人事組織の規定

CI 機能に必要な人材には、経営幹部、マネジメント職、シニア（エキスパート）、およびジュニアスタッフが含まれる。サイバー調査は進化するテクノロジーを伴うため、インターンを（限定的な関与の）スタッフポジションに含めることも強く推奨される。インターンは、CI 機能とスタッフの能力を向上させるための斬新な知識源として、また潜在的な才能の採用プールとして機能する。知識とスキルに基づいた階層構造が提案されているが、タスク指向のマトリックス型リソース活用において、シニアおよび経験豊富なスタッフとジュニアスタッフが並行して関与する。これは、（警察や連邦法の執行活動において、ジュニアレベルの捜査官をシニアレベルの捜査官と組ませるのと同様に）技能と経験の向上を保証する。幹部および経営スタッフは、分野の経験を有しているべきであるが、関連する人材要件（調査、情報収集、科学的・技術的捜査・調査、および関連する法務および広報サポート活動）に応じて、CI 機能での経験に基づいて配置する必要がある。

本書の冒頭で説明されているように、サイバーセキュリティは、組織のリスクを特定して軽減するために設計された IT 機能である。サイバーセキュリティは「サイバーセキュリティリスクマネジメント」と考えることができる。その正確な性質は組織によって異なるが、基本的には経営と事業戦略、そして事業自体をサイバーリスクから守ることを目的としたエンタープライズリスクマネジメントの領域である。経営マネジメント機能として、事業全体のリスクを軽減する責任を負い、顧客、市場、株主、投資家に対する経営マネジメント（EMS）責任を果たす。

これらのタスクを適切に実行するために、組織では、戦略的なマネジメント役割として最高情報責任者（CIO）と最高情報セキュリティ責任者（CISO）の役職を設けることが増えている。さらに、サイバーセキュリティ機能の中核メンバーは、ガバナンスに関しては取締役会や経営幹部、マネジメントに関しては最高業務責任者（CBO：Chief Business Officer）を含む経営幹部にまで拡大した。

テクノロジーの急速な発展とビジネスへの浸透の結果、サイバーインシデントの数と影響の規模は拡大している。同時に、CIO や CISO の権限や責任は、ビジネスへの影響や損失とのバランスが取れておらず、多くの企業で不均衡なリスクマネジメントが行われている。リスクマネジメントを積極的に行うには、企業はビジネス全体への影響の観点からサイバーリスクを理解し、経営幹部を含む役割と責任を見直し、取締役会などのガバナンス責任を明確にし、リーダーシップを重視したマネジメント体制に移行する必要がある。

CISO は、多種多様なセキュリティ活動を監督し、さまざまなセキュリティ機能の目標を設定する責任を負い、その目標を達成するための組織戦略や人材戦略、予算を策定する。したがって、CISO には単なるセキュリティの専門家以上の存在が求められる。マネジメントやビジネス戦略を含むビジネス領域を十分に理解していなければならない。CISO がセキュリティの目的だけを追求する行動をとれば、セキュリティチームはいずれビジネスチームと対立することになる。したがって、CISO は経営戦略や事業

戦略に沿ったセキュリティ戦略を策定しなければならない。EC-Council University は、「成功するための CISO の 6 つの鍵」[313] として以下を挙げている。

1. CISO はビジネス上の戦略目標と「セキュリティに関する計画」をと計画を整合させる
2. CISO が成功するためにはリーダーシップスキルが必要
3. CISO は部門間の調整と権限委譲に責任を負う
4. 継続的な学習は CISO の重要な特徴である
5. CISO は C レベルの幹部である
6. CISO がベンチマークを作成する

いったんサイバーインシデントが発生すると、組織内のリソースだけでインシデント調査を完了できることはめったにない。多くの組織は外部の専門家と協力せざるを得ない。しかし、多くは外部の専門家と協力するための準備やプロトコルの理解が不足しており、協力が迅速かつ円滑に行われず、サイバー犯罪の捜査に必要な証拠が損なわれている。幸いなことに、物理的なセキュリティ対応において警察、法執行機関、企業の間で連携が成功している例が頻繁に発生しており、その連携によって次のような潜在的なメリットを垣間見ることができる。

- 弱い立場の人が被害に遭うのを防ぐための教育と指導
- 効果的な予防策と対策
- 被害を最小限に抑えるための事故への早期対応
- 組織の評判を守る能力を強化
- 適切な証拠保全、捜査、逮捕を通じて犯罪を抑止

組織は、効果的な社内 CI 機能を促進するだけでなく、調査中に社内スタッフと一緒に作業する外部関係者との有益な協力関係を確保するための措置を講じることが不可欠である。

職務分掌

法執行機関などの公的組織と、民間企業における CI 機能の役割のうち法務および広報機能については官民で異なっている。一方、捜査・調査、諜報／情報収集、フォレンジックやマネジメントに関する役割は官民に共通している。職務の内容は、組織が過去に直面したサイバー犯罪や将来直面すると予測されるサイバー犯罪の種類とカテゴリによって決まり、組織が対処するリソース要件に従って定義されるべきである。

従来、セキュリティのガバナンスとマネジメントは分離されておらず、すべてのセキュリティ対策と責任を担当する専任のセキュリティチームを備えた集中型の構造が一般的だった。今日、サイバー脅威がビジネスに及ぼす影響が増大するにつれ、セキュリティ チームに委任される権限と責任は、ビジネスへの影響の規模と深刻度に釣り合わないことが多くなっている。したがって、COSO（トレッドウェイ委員会組織委員会）[314] の 3 ラインモデル [315] に基づいたマネジメント構造は、組織内の責任と役割のより効果的な分担を促進するのに役立つ可能性がある。

313　EC Council Universityブログ - 成功するためのCISOの6つの重要な特性。https://blog.eccu.edu/6-key-characteristics-of-a-successful-ciso/
314　COSO（トレッドウェイ委員会スポンサー組織委員会）トレッドウェイ委員会組織委員会https://www.coso.org/
315　IIAの3つの防衛ラインモデル～3つの防衛ラインの最新版、2020年、内部監査人協会。

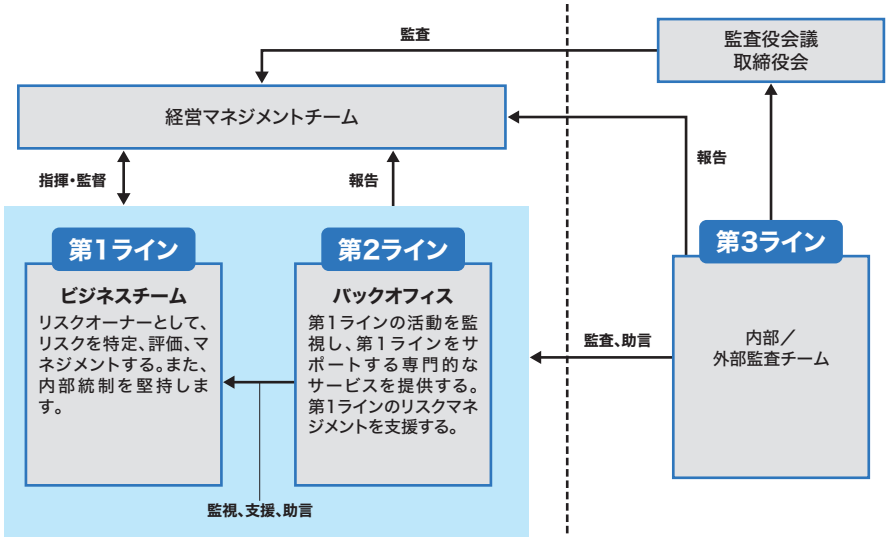


図 10-10. 3 ラインモデル

●第1ライン:ビジネス部門

第 1 ラインは、事業の性質、その推進、利益と損失、および事業に対するリスクからの潜在的な影響を最も正確に認識することができる。事業に関連するリスクのオーナーとして、リスクを評価し、特定し、マネジメントし、リスクに関するガバナンスを維持する責任を負わなければならない。第 1 ラインがセキュリティやリスクマネジメントの専門知識を持っていることはほとんどないため、第 2 ラインによるサポートが必要になる。

●第2ライン:間接マネジメント部門

第 2 ラインは、セキュリティマネジメント施策（ポリシーやルール策定、ソリューション導入および運用）、セキュリティ監視（SOC：Security Operation Center）、インシデント対応、情報収集および共有、IT インフラマネジメント、資産マネジメント、リスク評価、アカウントマネジメント、アクセス権マネジメント、アプリケーションマネジメント、脆弱性対応、災害復旧、セキュリティ教育・啓蒙・訓練など、高度な専門性を必要とするセキュリティ関連機能で構成される。これらすべての機能には組織全体の関与が必要だが、第 2 ラインはこれらのタスクの実行を主導する。

重要なのは、第 2 ラインは、保護すべきビジネス目標と価値に関する意見の相違を避けるために、これらのタスクを第 1 ラインのリスク認識と優先順位と一致させる必要があることである。整合が行われない場合、第 2 ラインはビジネスの進行を遅らせる内部の敵として認識される可能性がある。敵対的な構造や言説は組織の脆弱性の原因となる可能性があるため、第 2 ラインは過度にリスク回避を主張し過ぎないためにビジネスニーズに敏感でなければならない。

●第3ライン:内部監査部門

第 3 ラインは、主にセキュリティ監査とコンプライアンス監査を通じて、組織内の第 1 ラインと第 2 ラインのセキュリティ対策を客観的に評価し、主にセキュリティおよびコンプライアンス監査を通じて組織の独立性を維持しなければならない。

さらに、社内のリソースやキャパシティが不十分と判断される場合は、専門知識を持つ外部プロバイダーへの委託が必要になることもある。セキュリティ監視（SOC）やインシデント調査（フォレンジック調査）のような高度なセキュリティスキルを必要とする機能は、信頼できる外部の専門家に委託することができる。

委託先パートナーと組織の目標を戦略的に結びつけるには、ガバナンスや経営目標に関連する情報やKPIを共有することが重要である。外部の委託先パートナーの活動に関するKPIが調整されていない場合、限られたリソースが消費され、ビジネスクリティカルなリスクや攻撃ベクトルが見過ごされることになる。サイバーセキュリティ活動に従事するサプライチェーンパートナー全体に、ビジネスと整合した優先事項を適用することで、セキュリティ監視とインシデント対応の強固な実施とマネジメントが可能になる。

下記の図は、3ラインモデルに沿って、委託先パートナーをNIST CSFの必要なセキュリティ機能の5つのコア機能カテゴリ（IPDRR：Identify, Protect, Detect, Respond, Recover）に統合している。セキュリティ活動と機能は、役割と責任を明確にするために、各組織の状況に応じてマネジメントされるべきである。

表 10-3. セキュリティ活動に必要な機能の例

	特定	防御	検知	対応	回復
第1ライン	資産、アカウント（ID）、デバイス、アプリケーションマネジメント／リスクアセスメント	脆弱性対応、セキュリティポリシーのガバナンス	危機マネジメント、事業継続マネジメント		
	サプライチェーンマネジメント、リスクマネジメント、製品／サービスセキュリティ、研修、啓発				
第2ライン	資産、アカウント（ID）、デバイス、アプリケーションマネジメント（共通）	セキュリティマネジメント、監視、脆弱性対応（共通）	インシデント対応、ディザスタリカバリ、情報共有		
	Learn and improve Evaluate performance for improvement				
第3ライン	セキュリティ監査				
外部	セキュリティ監査	ソリューションを提供		インシデント対応	

人材利用計画

前述した予算追跡の例で描かれたように、人的資源の組織におけるさまざまな利用レベルの計画が必要である。職務の上級職に進むにつれて、管理業務やその他の組織的活動（法執行機関の広報や民間企業の戦略計画など）は増えるため、資源の活用率は低下する傾向にある。しかし、その一方で、業務遂行の効率は向上する。高度な技術を要する仕事では、社内外を問わず、利用できる人材プールが限られている。したがって、組織は職務に応じた人材の効果的な活用を理解すべきである。

人材パフォーマンスのマネジメント

高度なスキルを必要とする仕事における人材のパフォーマンスは、以下の要素を指標として測定されるべきである。すなわち、①方針への遵守、②リーダーシップ能力（技術的スキル、タスク管理、人的管理、またはそれらの組み合わせ）に対する主観的な信頼度、③資源活用計画の目標達成度といった客観的な要素である。

CI機能の予算管理では、日次（または少なくとも週次）の時間・経費報告が求められるため、週次・月次のパフォーマンス評価を活用目標に照らして提供する必要がある。また、リーダーシップの主観的な評価と、方針遵守（違反の有無や影響を含む）に関する客観的な評価は、四半期ごとおよび年次で実施すべきである。さらに、年次のパフォーマンス評価は、給与および福利厚生の見直しと関連付けることで、組織の戦略的計画の要件と整合させることが望ましい。

必要となる知識・スキルの定義

CI 機能の主な仕事は、調査（人的および技術的）、インテリジェンス（偵察、監視、情報ソース開発）、フォレンジック（コンピューター／モバイル デバイスおよびネットワーク）マネジメントまたはサポート（広報や司法など）を含む。調査、インテリジェンス、フォレンジックなどの主要な CI 活動には、共通の技術的基盤と、上級レベルまたは専門家の要件を満たすための特定の経験と高度な知識が必要である[316]。

少なくとも、主要なコンピュータオペレーティングシステムとインターネットプロトコルに関する実用的な知識と、関連する調査または評価ツール（テスト、証拠収集、フォレンジックおよびデータ分析の実行用）の操作方法は、主要な CI 活動を行なう者の要件となる。

マネジメント職、経営職、幹部職員の役職にも、ビジネス機能に関する教育とトレーニングが必要である。司法担当・法務担当や広報を含むその他のサポート機能は、集中的な学業や業界特有のトレーニングや実務経験に支えられた高度な専門スキルである。

主要な CI 活動のためのスキルセットは、人的資源の計画と活用のための役割に沿った知識と経験の要件に従って定義されるべきである。プロジェクト GLACY が提供する以下のモデルは、CI 活動が関連するサイバー犯罪の種類とカテゴリー別に、職務上の役割に従って必要となる知識・スキルの要件を示している。

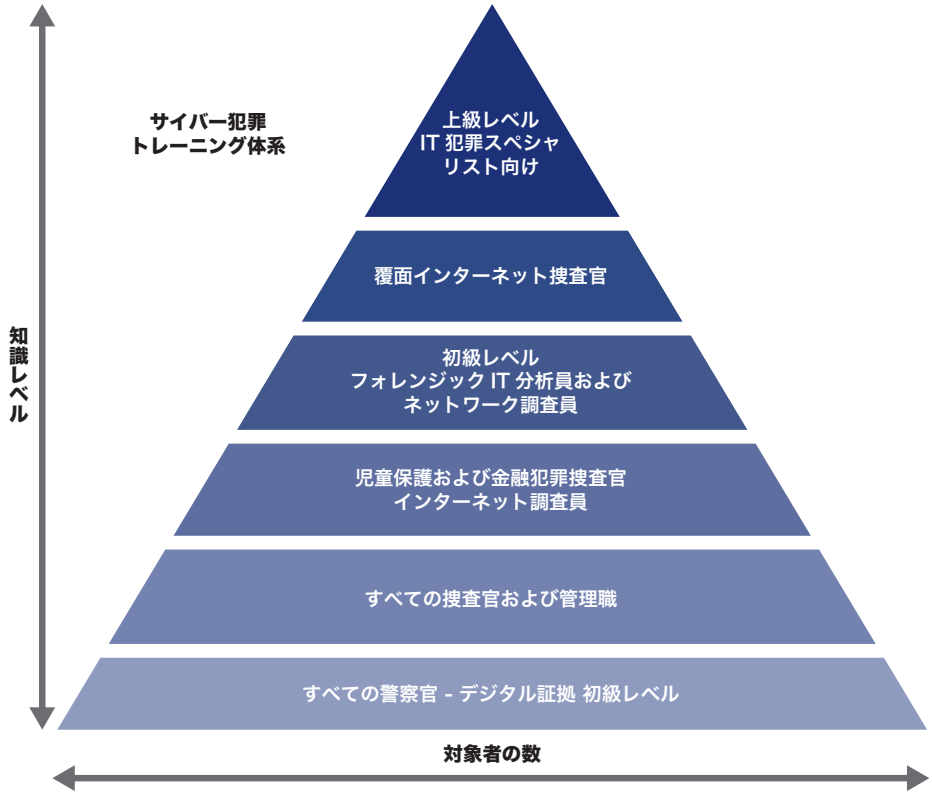


図 10-11. プロジェクト GLACY モデルでの技能とサイバー犯罪捜査職務との関係

採用と雇用

前述したように、開発された CI 機能は、潜在的な才能を見極める手段（および進化するテクノロジーに関する最新の知識の提供）として、インターンを人材計画に組み込むべきである。高度な技術と専門知識を必要とする仕事の分野では、従業員の離職率が高い。このため、継続的な募集と雇用は計画的な

316　CIにおける「専門家」の要件には、報告または証言（証言録取書または法廷での証言）が含まれる場合がある。

活動であるべきであり、マネジメント職や幹部職員の業績目標とすべきである。

大学からのインターン採用により、組織に利益をもたらす意欲的で経験を求めており、そして適用力のある人材が提供される。一方では、職業学校や軍隊、または経験豊富な（そして「任務訓練を受けた」）人材を採用すると、実社会での経験だけがもたらすことのできる必要な現場経験と実践的なスキルが得られる。連邦／地域／地方の法執行機関、軍隊、または関連する CI 機能からの同様の経験は、特定の機能にとって優れた教育および経験の源となる。どちらも、公共部門と民間部門の組織全体で、採用と雇用に重点を置くべき必要な人材プールである。次のマトリクスは、CI 活動を中心とした採用の簡単な計算方法を提供する。

表 10-4. 活動内容別のサイバー犯罪捜査官の採用

機能	教育	求められる経験
捜査管理	大学	深い経験（任意の CI 活動における）、官民
調査	大学または連邦	深い～中程度の経験、官民
知見収集	大学および連邦	深い経験、官（官の経験有りが望ましい）
証拠	大学または職業学校または業界	中程度の経験、官民
総務人事	大学または職業学校または業界	中程度～浅い経験、官民
説明責任	大学または業界	深い経験、官民（民間の経験有りが望ましい）
予防啓発	業界または連邦	深い経験、官（官の経験有りが望ましい）
後方支援	業界または連邦	中程度の経験、官民

技能パフォーマンスの目標

技能パフォーマンス目標は、要員が実施する必要な活動の測定、および定期的な研修（上級スタッフの場合はトレーナーとしての実施、その他のスタッフの場合は受講）による関連する研修成果の測定について算出されるべきである。これには、スタッフが現在職務で担っている経験レベルや、昇進を希望している場合は年次業績評価で予想される成果も考慮する必要がある。

知識とスキルの検証

高度に専門的な分野であるため、特に上級レベルでは、組織内で人員が遂行する CI 活動に応じて適切なスタッフ配置を確保するために、募集時、採用時、および雇用のパフォーマンス「テスト」期間の終了後に、知識とスキルの検証を実施すべきである。技術的スキルの検証は、可能であれば、指導を受けた上級スタッフが作業セッションで行うことが望ましい。一方で、リーダーシップの適性や能力は、幹部／マネジメント職や若手スタッフによる客観的な調査を通じて評価すべきである。

司法、事務管理、および後方支援のスタッフの技能と知識は、組織内の同等の活動に携わる職員によって検証される必要があるが、役割への適性の最終的な判断は、採用マネジメント者を通じて CI 機能の幹部職員に委ねられるのが適切である。

パフォーマンスのマネジメント

パフォーマンスのマネジメントは、あらゆる組織機能にとって重要な戦略的報告活動である。CI 機能を成長または発展させるためには、リーダーシップは、確立された基準や計画に対する測定可能なパフォーマンスを明確に示すことができなければならない（彼らはその作成に参加すべきである）。

組織パフォーマンスの測定基準

サイバー犯罪は個人や組織を標的としており、その調査・捜査は「通常の業務」を構成する活動ではないため（組織が対応することがある程度通常の業務になってはいるが）、CI 機能の成功を測定したり、パフォーマンスの弱点を特定したりすることは困難である。CI 機能が関係する戦術的および戦略的リスクについては、前述の組織計画およびマネジメントのセクションで論じられた。組織パフォーマンスの測定基準は、CI 機能が支援するよう割り当てられた組織またはユニットとして、リスクマネジメント又は他の組織のパフォーマンス基準に従って適用されるべきである。

組織の監査

CI 機能の監査は、戦略的な予算編成および計画活動について組織に情報を提供するために、リソースの計画、割り当て、および計画に対する実績に従って、月次、四半期、および少なくとも年次ベースで実行されるべきである。監査は、CI 機能が実施責任を負うプロセスを含むマネジメント手順に関するテスト計画に従って実施されるべきである。

業務プロセスの測定基準

CI 機能の運用プロセス指標は、一般に、組織全体の指標と同じ基準に従って決定されるべきである。例えば、金融と IT は一般に CI 活動と同様のスキルと知識の強度を必要とする技術分野である。どちらも組織のサポート機能であり、定義された（監査可能な）リスクマネジメントプロセスを備えている。前述の COBIT フレームワークは、リスクとそれに対応する運用目標のパフォーマンスを測定する手段を提供する。公共部門の CI 機能活動（法執行捜査官など）においては、業務プロセスの指標は、公共部門の偶然の役割（法医学病理学者対コンピュータ科学者、HUMINT 対 ELINT 情報専門家など）とより類似しているはずである。

業務プロセスの監査

どのような業務でもパフォーマンスを測定できる。実施される作業には、関連するプロセスと手順、および活動報告（時間、経費、リソース利用など）が必要である。したがって、あらゆる業務を監査して、手順と運用ガイダンスに準拠しているかどうかを確認できる。CI スタッフが実行する活動は、証拠の収集と処理、司法・法務担当または広報の報告とコミュニケーションを含むインシデント調査および情報公開手順などの特定の運用プロセスを定義する。手順は、職員が行う CI 活動に対して明確に定義されるべきであり、運用プロセスは、ポリシーの遵守を確認するために、また、関連する手順を改善するための要件や機会を特定するために、定期的に実施されるべきである。監査は透明性があり、レビューに対してオープンであるべきである。

パフォーマンスの測定と改善

業務プロセスや手順を定期的に監査することで、スタッフのパフォーマンスは標準化され、（資源の配分や利用における）規模の効率性が得られるはずである。規模の効率性が得られない場合は、人事または業務の弱点を特定し、是正するために、人事と関連する業務プロセスの両方について追加監査を実施すべきである。監査することによって、スタッフと組織の両方のパフォーマンスを向上させることができる。

人材のマネジメント

人材マネジメントは単なる「リソースマネジメント」活動ではない。人間には動機や欲望がある。高度なスキルを持つ技術専門家は、成功すること、認められて報酬を得ること、同僚やスタッフに知的に挑戦すること、教育の機会を求めることへの動機を持っている。技術的な組織や機能で人をマネジメントするということは、信頼を獲得し、知識を証明し（「知らない」ことを認めることも含む）、模範を示してリーダーシップを発揮することを意味する。

集団力学（グループダイナミクス）

前述のとおり、CI 機能は高度に専門的な分野であり、人材計画と組織化には、効率的な組織パフォーマンスを実現するために、才能、経験、そしてマネジメントを統合することが求められる。シニアスタッフとジュニアスタッフをタスク指向でペアにすることで、スキルや経験の向上のためのメンタリングアプローチを通じた協力が確保される。マネジメント職・幹部職員とシニアスタッフ・ジュニアスタッフを交互に配置することで、個人および専門職の開発目標を推進する機会（および選択肢）が提供される。組織の人材計画におけるこれらの設計は、均質なグループダイナミクスを生み出し、オープンな対話、仕事のパフォーマンスの技術的な一貫性、サービスの長期化、組織の戦略目標へのスタッフの関与を促進することを意図している。

学習する組織の構築

学習する組織とは、強力なグループダイナミクスとオープンなコミュニケーションで構成され、パフォーマンスを測定して強み、弱み、改善の機会を特定する組織である。前述のように役割を交互に配置して構築すると、CI 機能は組織の構造に学習を組み込む。これにより継続的な改善が可能になる。

コーチング

マネジメントスタッフ、ジュニアスタッフへのコーチング、高度に技術的なリスクマネジメント活動をサポートする活動が重要である。サイバー犯罪被害の可能性を認識している組織、またはサイバー犯罪の実際の影響を経験した組織は、ビジネスだけでなく組織の人員やアーキテクチャの複雑さを必然的に理解しなければならないスタッフの離職を許容することはできない。したがって、コーチングは CI 活動の機能であるだけでなく、CI が他の戦略目標をサポートする組織の共同作業でもあるべきである。

例えば、金融犯罪を専門とする CI 捜査官は、コンピューターフォレンジック捜査官だけでなく、会計士やマネジメント者からも指導を受け、収集した証拠を分析する際の理解力を高めるために、その分野特有のリスクに対する理解と認識を深めるべきである。そのような捜査官が財務調査の経験を積むにつれて、仕事の効率は上がり、活動の業務中断は減少し（関連する組織の業績が向上する）、結果的に組織にとっての価値（他のスタッフのスキルや知識を開発する価値も含む）が高まる。このような捜査官が、CI 機能だけでなく、彼らがサポートするビジネス機能（財務）からも適切な指導を受けられない場合、彼らは組織を去り、開発に費やされた時間と費用も一緒に去ってしまう可能性がある。

チームビルディング

リーダーシップには支持者が必要である。フォロワーは単に割り当てられるのではなく、導かれることを自ら望まなければならない。それは、支持者がリーダーに求める知識、スキル、経験が実証されることによって可能になる。真のリーダーは、ジュニアスタッフ（あるいは他のスタッフ）から、自身のスキルや知識を伸ばす機会を求められる存在である。顧客が製品やサービスを 2 回目に購入するまでは

「真の意味の顧客」とはならないのと同じように、スタッフが1回目だけでなく2回目にもにリーダーに従うことを選んだときに”リーダー”が誕生する。

CI活動におけるチームビルディングは、組織を支援し、関連するリスクのマネジメントを手助けする機能的要件を中心とした人材計画の機能であるべきである。チームビルディングは、フォロワーが評価できるリーダーを確保するための人事パフォーマンスマネジメントの機能でもなければならない。そうしないと、離職が発生し、業務のパフォーマンスが低下する。

モチベーションのマネジメント

すべての個人には成功するための個人的な動機と職務上の動機がある。健康と安全という基本的な動機であれ、自己実現[317]という高度な動機であれ、それらは個人的な動機である。適切にマネジメントされた組織は、業務パフォーマンス要件の範囲内で個人のニーズを満たす計画を立てる。これは、機能的なスキルと知識を、許容できるレベルの利用で人材を募集、雇用、雇用するための予算計画に一致させることによって部分的に達成される。これは、役割に応じた適切な組織計画と、それに伴うコーチングやメンタリングによっても達成される。

高度なスキルを持つ人材は業界で高い需要があり、批判や否定的なフィードバックに対して非常に敏感になることがよくある。適切にマネジメントされた組織は、軽蔑的なフィードバックなしにパフォーマンスを向上させるリーダーシップとマネジメント方針の雰囲気を作り出す。

多文化環境のマネジメント

複雑な仕事には、複雑な頭脳と、環境や文化に広く触れることで得られる幅広い経験が必要である。サイバー犯罪は、特定の地域だけで行われるものでもなく、特定の人種や特定の集団だけが行うものでもない。おそらく他のどの仕事よりも、CI機能には多文化環境とオープンマインドで進歩的なスタッフが求められる。サイバー犯罪の発生源とその被害者のために、CIスタッフはしばしば関連捜査を支援するために出張する必要がある。同様のオープンマインドで統合された文化的経験は、CI機能のパフォーマンスを向上させるのに役立つ。

ツールのマネジメント

仕事に適したツールを選択することは重要な計画活動である。ツールは業務の効率化を促進し、サイバー犯罪捜査・調査に関連する偶発的な費用のための第三者契約サポートによる時間と費用を削減することができる。

戦略的要求に対するツールの選択

ビジネスの戦略的目標は、インフラストラクチャーの要件を定義し、その要件は一般的に、組織がその目標を達成するために必要なサポート（方針、手順、技術、人員）を定義する。安全なコミュニケーション、活動の文書化と情報マネジメント、非公開データおよび私的データの安全なマネジメント、競争上の秘密の保護といった戦略的組織能力には、それに対応するCI要件がある。

戦略的要求をサポートするために、組織は少なくとも下記のツールに投資すべきである。

317　マズローの欲求階層を参照:http://www.simplypsychology.org/maslow.html

1. 境界ネットワークと通信（電子メールと音声）監視ツール
2. マルウェア対策とマルウェア対策用のソフトウェアとハードウェア
3. セキュリティ情報とイベントマネジメント（SIEM）用のソフトウェア
4. フォレンジックコンピュータ、モバイルデバイス、メモリ、ネットワーク取得ツール
5. データの保持と分析用ツール

戦術的要求に対するツールの選択

組織をサポートするために戦略的なツールが毎日活用されるが、より散発的な戦術的なニーズも発生するため、それについても計画されるべきである。少なくとも、組織は組織の要求をサポートするために、下記の戦術的ツールに投資すべきである。

1. 迅速に展開できるフォレンジックキット
2. メモリ分析ソフトウェア
3. （ネットワークとホスト）スキャンと評価用のソフトウェアとハードウェア
4. オープンソースおよびプロプライエタリのインテリジェンスソフトウェアまたはサービス
5. 録音（オーディオおよびビデオ）機器またはサービス
6. 「サンドボックス」ソフトウェアおよびハードウェアまたはサービス
7. 「シンクホール」ソフトウェアまたはサービス
8. リバースエンジニアリングおよび分析ソフトウェア
9. マルウェア／マルウェア検出ソフトウェア
10. 双方向無線機または「クリーン」な携帯電話およびモバイル機器（iPad など）

ツール利用率マネジメントとパフォーマンスの見直し

ツールの価値は、資産としての活用によってのみ測定できる。棚から取り出されることのないツールは、組織にとって換算する価値のないコストである。タスクの遂行に重要でありながら、十分に設定されていないために利用できないツールは、組織にとって効率や生産性に影響を及ぼす機会費用となる。ビジネスの戦略的要求をサポートするツールは、関連する予算計画に従って追跡されるべき IT 投資である。しかし、戦術的ツールの使用は、時間と経費の報告において、担当者による利用指標を通じて追跡されるべきである。少なくとも四半期ごとに、CI スタッフはユーティリティとパフォーマンスのレビューを実施し、関連のツールが十分であるか、改善できるか、または CI インベントリから削除できるかを判断する必要がある。

ツールのトレーニングと認定

組織（または支援される機能）の戦略的及び戦術的ニーズを支援するために選択されたツールに関するスタッフのトレーニングは、CI 機能の効率的な予算計画と実行にとって重要である。いくつかの認定資格は、業界のトレーニングソースから入手可能であるが、役割に基づく認定資格は、戦略的機能目標（検知、対応、修復、改善）を支援する CI 活動に従って、組織によって定義されるべきである。（内部および／または外部の）認証取得のための研修目標は、文書化されて人事計画の業績評価指標に含まれるべきである。

第10章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

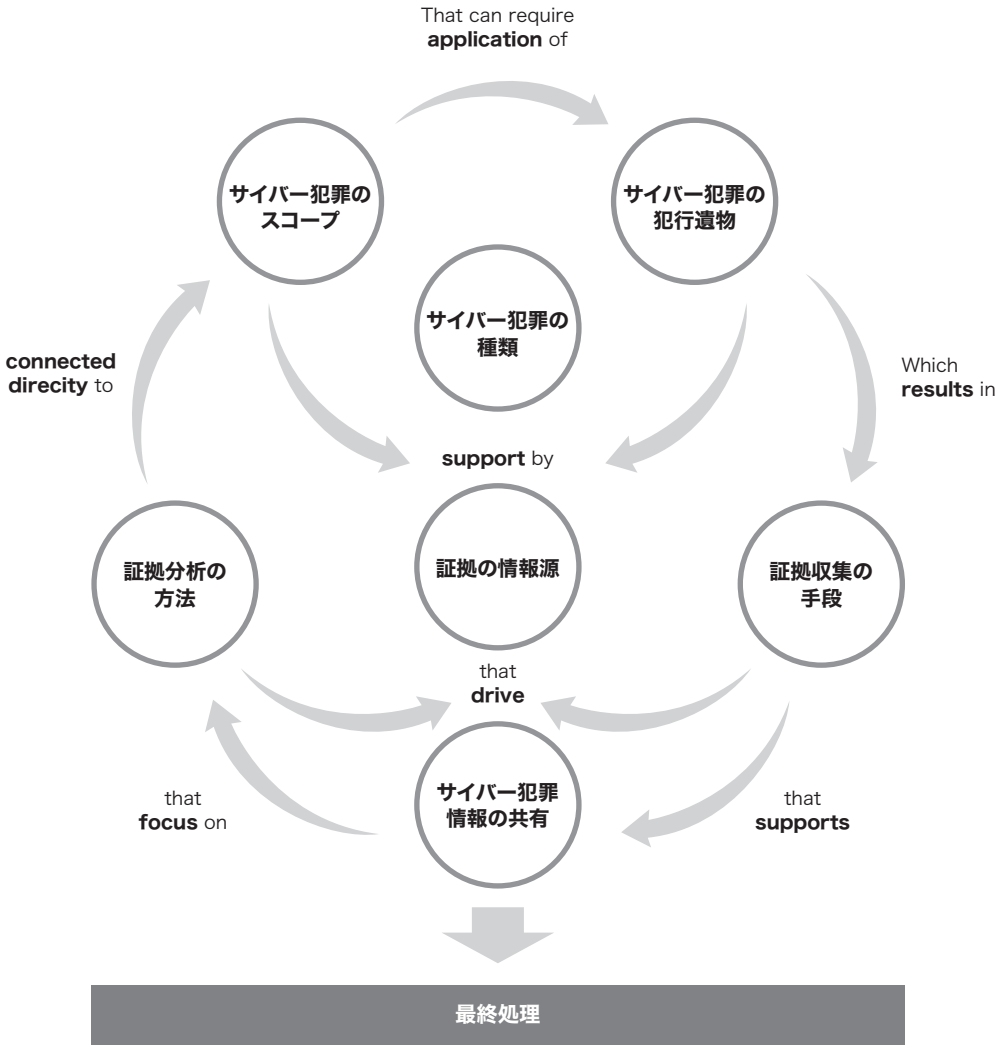


図 10-12. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 10-5）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 10-5. CIBOK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 10-6. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査マネジメント – サイバー犯罪とその捜査・調査に関する手順と方針、捜査・調査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査管理・インシデント管理の機能は、組織に対してサイバー犯罪の特性と種類を説明する。捜査管理・インシデント管理の機能は方針、手順、計画を策定し、（人的、その他の）資源とその継続的な開発をマネジメントすべきである。

知見収集 – 利用できる証拠の情報源から得られる知見を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、スコープ、目的を判断するための重要な情報源である。知見収集スタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。調査スタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

説明責任 – 捜査・調査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制や法律に関する指針は、情報の共有に対する制限や罰則を規定する。シニアスタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、広報の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪のスコープに応じて、方針に基づきながら、また、どの組織・職務・人員が影響を受けるのかを考慮しながら、何を、だれに、いつ、伝えるのかを決定する。シニアスタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

後方支援 –情報収集と捜査・調査活動を支援するため、サイバー犯罪の捜査範囲と方法について手続き上の理解を必要とする。

総務人事 –証拠を収集および分析するために、手順の理解、調査の意図、組織能力を必要とする

第10章:レビュー

1. **サイバー犯罪捜査・調査および最終解決の機能の目的は何か**
   答え：警告を調査したりまたは法的要請への対応を指示すること。
   例：PII マネジメントシステムの侵害、財務データにアクセスするためのユーザーアカウントの悪用など。

2. **本機能はどのように組織し、マネジメントすべきか**
   答え：経験豊富なスタッフによる戦略的運営。
   例：経験豊富な捜査官によるリスクマネジメントの補助機能として。

3. **機能の戦略的目標は何か**
   答え：検出、対応、修復、改善。
   例：リソース（人材、時間、資金、ツール／機器）を計画して割り当てる。

4. **機能のリソース要件（スタッフ、ツール、コミュニティ）は何か**
   答え：経験、技術的なもの／標準的な実務で承認または使用されているもの／業界や研究におけるもの。
   例：捜査管理・インシデント管理、知見収集、調査、広報、後方支援、総務人事、ハードウェア／ソフトウェア／処理システムおよび設備。

5. **スタッフを配置し、マネジメントし、指導または統括するために必要な技術的および経験的な要件は何か**
   答え：シニア、ミドルレベル、スタッフ、インターン。
   例：教育、知識、技能、（事件／調査）経験。

6. **本機能（およびそのスタッフ）のパフォーマンスはどのように測定すべきか**
   答え：方針と結果に対する基準による。
   例：方針とスタッフの育成の成功に応じて。

7. **組織をうまく機能させるには、どのような組織コミュニケーションと戦略的な関与を、組織のどのチャネルに組み込むべきか**
   答え：計画、パフォーマンス指標。
   例：機能的および戦略的なレポート作成における（人材、予算、ツール）。

8. **サイバー犯罪とその捜査・調査および最終解決の機能は組織のどの幹部機能の配下とすべきか**
   答え：リスクマネジメント。
   例：必要に応じてCIO、GC（General Counsel）、GA（General Affairs）との調整／マトリックス報告。

ケーススタディ10:サイバーセキュリティリスクのオーナーシップ

- **犯罪**：情報窃盗
- **容疑者**：アクセスブローカー
- **手段**：USB スティックを使ったソーシャルエンジニアリング
- **動機**：従業員のセキュリティ意識とセキュリティアーキテクチャをテストする
- **機会**：企業幹部による支援

2015 年、東京に本社を置くグローバル企業の CIO は、ソーシャルエンジニアリングやフィッシングなどによるデータ損失に関する会社のセキュリティ体制を評価するため、サイバー犯罪調査員を雇った。議論を重ねた結果、捜査官は企業本社で実行される簡単な USB ドロップ演習を開発した。この演習の目的は、会社の従業員のサイバーセキュリティ意識向上トレーニングの有効性を判断すると同時に、(エンドポイントからネットワークまでの) セキュリティ アーキテクチャの適切性をテストすることだった。

まず、捜査官はウクライナのクラウドサーバーに登録されたウェブサービスを作成した。その後、Windows コンピュータに USB スティックを挿入すると、インフォスティーラーが自動的に実行されるようにプログラムされた。インフォスティーラーは、日時、IP アドレス、ホスト名、ユーザー名、オペレーティングシステム、ブラウザービルドなどのデータを収集するように構築された。USB が Windows デバイスに挿入されると、インフォスティーラーは、この情報を固有のデバイス識別子とともに、前述のクラウドサーバーに登録されている DNS に送信する。DNS はダイナミック DNS プロバイダーからのものであり、登録は再利用された証明書により使用して 1 か月未満だった。

インフォスティーラーマルウェアは 40 本の新しい USB スティックにコピーされ、それぞれの USB スティックには会社のロゴと重要でないシリアル番号が付けられていた。USB スティックに保存されていたファイルは、「autorun.inf」という名前のインフォスティーラーマルウェアと、空白の Word 文書だけだった。捜査官は、会社のロゴが印刷された封筒に入れた USB スティック 10 個を、無作為に選んだ本社の幹部宛に送った (幹部のリストは、基本的なインターネット検索でまとめられた)。残りの 30 本の USB スティックは本社に持ち込まれ、一般見学の際に、捜査官がコーヒー休憩室のバスケットに 20 本を入れ、残りの 10 本を廊下や机の上に無造作に置いた。

その後、捜査官がウクライナでホストされているクラウドサーバーを監視すると、2 週間以内に 40 個の USB スティックすべてが企業本社から少なくとも 1 台のコンピュータの情報を通信していたことがわかった。場合によっては、USB スティックがパソコンでも使用されていた。合計で、89 台の異なるコンピュータと 45 人の異なるユーザーの情報が、わずか 40 個の USB スティックの初期配備から Web サーバーに伝達された。

その後、企業のセキュリティ部門と調査を行ったところ、従業員の意識向上トレーニングで不明な USB やデバイスの使用に対する注意が強調されていたにもかかわらず、USB スティックに関するヘルプデスクへの問い合わせは記録されていないことが判明した。さらに、東京本社からウクライナの Web サービスへの通信が通常の履歴パターンに基づくと極端な異常値であったにもかかわらず、同社のセキュリティアーキテクチャはネットワークの異常を検出しなかった。この会社では DNS や証明書履歴／警告システムを採用しておらず、USB スティック上の自動実行ファイルが 10 年以上にわたって重大なマルウェアの脅威となることが知られていたにもかかわらず、同社のコンソールログにはウイルス対策アラートが 5 件しか発見されなかった。

演習の結果に基づき、同社は従業員のセキュリティ意識を向上させ監視するためのセキュリティポリシーおよび支援ツール、さらにネットワークやエンドポイント通信およびデータ損失防止対策に投資した。

第11章

実践的サイバーリスク管理

はじめに

サイバー犯罪捜査・調査部門の最終的な目的は、そのマネジメントシステムをビジネス戦略および企業のリスクマネジメントと整合させながら、ミッションクリティカルな資産を保護し、業務中断のリスクを軽減することである（第 10 章で説明）。理想的には、組織はサイバーリスクマネジメントおよび IT サービスマネジメント機能を、企業の戦略的機能に基づいたビジネス戦略に組み込み、企業全体のマネジメントと整合する包括的なフレームワークによってマネジメントすべきである。しかし、企業マネジメントの範囲が広いため、これには強力なリーダーシップと膨大なリソース（および時間）が必要になる。これは理想的なアプローチではあるが、必ずしも実現できるとは限らない。

本章では、サイバーリスクマネジメントをビジネス戦略要件と実際に統合するアプローチを提案する。

- ビジネスリスクマネジメントの認識と整合性の向上
- 脅威（およびその原因）、脆弱性、リスク、および影響についての共通の定義と理解
- サイバー犯罪捜査・調査部門の戦略と活動（特に目的と範囲）の整合性の向上
- サイバーリスクマネジメントのための組織能力の向上
- 調査中の案件についての法的および手続き上の両方のニーズに対応するための、サイバーリスクマネジメントに関する特定の技術要件（例：調査のためにログを保持する期間）
- リスクの優先順位付けに基づくインシデントレスポンスとリソース配分の改善
- 重大なインディケーターを特定するための、偽旗作戦などの誤誘導戦術の正確な識別

さらに、既存のマネジメントフレームワーク（COBIT など）のサイバー犯罪調査活動の範囲への統合について示す。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- リスクマネジメントフレームワークは実際にどのように実施できるか
- リスクマネジメントの実務は、ビジネス要件や業務とどのように整合させるべきか
- リスクマネジメントは、サイバー脅威、脆弱性、リスクとどのように関連するのか
- 保護が必要な資産はどのように特定すべきか
- リスクシナリオはどのように作成され、評価されるべきか
- リスクはどのように評価されるべきか
- リスク対応はどのように実施されるべきか
- リスクレベルは、いつ、どのように監視されるべきか
- リスク報告は、いつ、どのように経営陣に提示されるべきか

実践的なサイバーリスクマネジメントにおけるトピックス分類

下記の図は、「実践的なサイバーリスクマネジメント」知識領域のトピックス分類を示している。

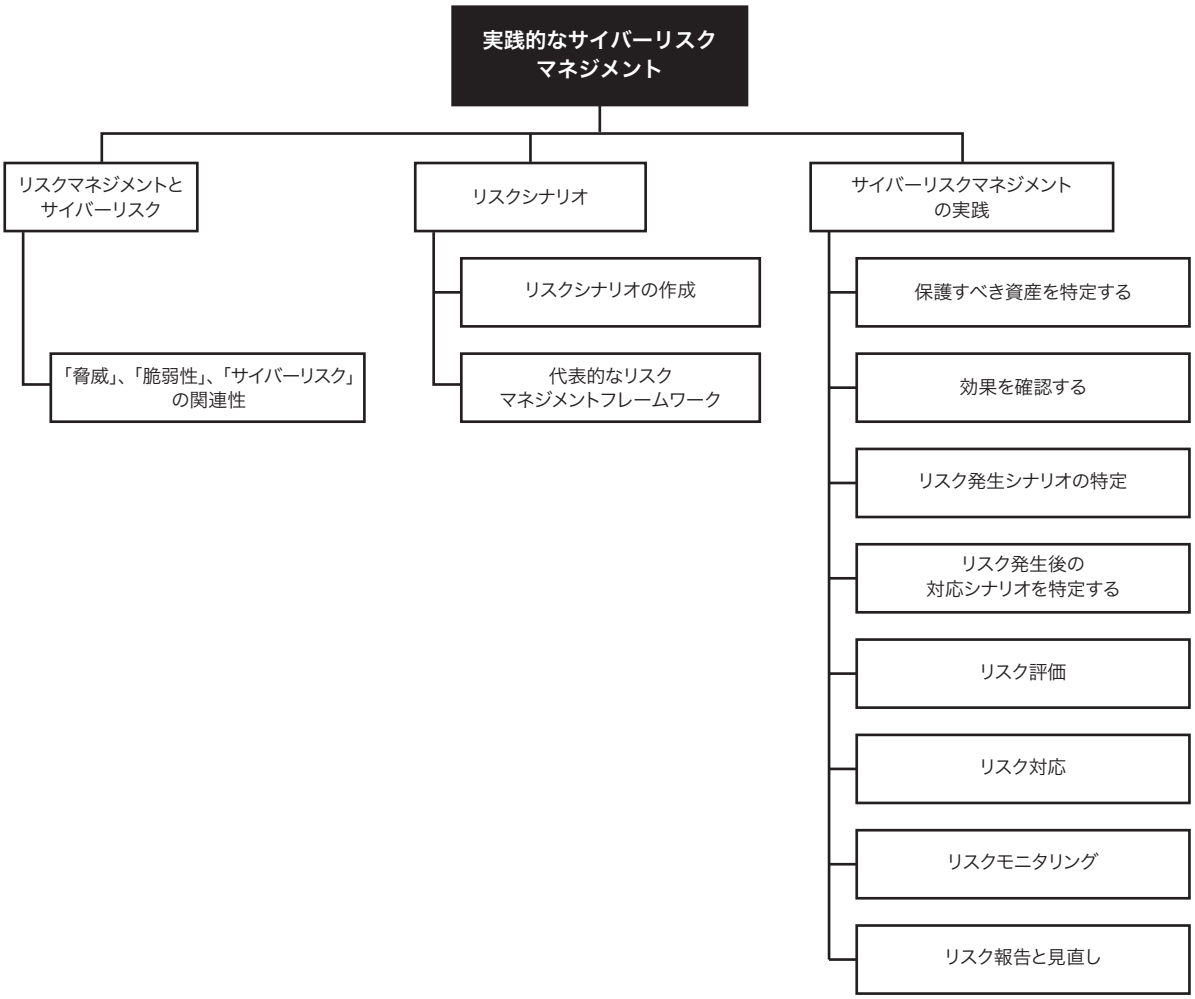


図 11-1. 実践的なサイバーリスクマネジメント領域におけるトピックス分類

実践的なサイバーリスクマネジメントとは

サイバーセキュリティは、セキュリティチームだけでなく、全社的な活動を伴うものであり、その目的は下記のように定義できる。

- 企業資産（情報または情報システム）とそれに関連するリスクの特定（IDENTIFY）
- リスクを軽減するためのセキュリティ管理施策の取り組み（PROTECT）
- 脅威の兆候の可能な限り早期の検知（DETECT）
- インシデントへの適切な対応（RESPOND）
- 適切なインシデント対応による（マイナスの）影響の最小化（RECOVER）

上記の目的を達成するために重要なのは、リスクマネジメントである。本章は、企業のサイバーセキュ

リティ活動における効果的なリスクマネジメントに対処するための実践的なアプローチを示す。

リスクマネジメントとサイバーリスク

サイバーリスクマネジメントの背景を説明するためには、まずリスクプロファイリングを理解することが不可欠である。これは、ガバナンスとマネジメント範囲、目標設定、目標の整合性を支える不可欠なものである。リスクプロファイリングの鍵は、「リスクの所在」と「リスクのオーナーシップ」を明確にすることにある。すべての利害関係者は、ビジネスの整合性を確保するために、これらの要素について共通の理解を持つ必要がある。

リスクの所在の明確化

適切な判断を行い、リスクに効果的に対応するためには、「守るべきものの価値」を正確に理解した人がオーナーでなければならない。「リスクマネジメント」の意味は一般的に広く、組織内のさまざまな分野が複雑に関連しているため、認識されているすべての範囲と活動を調整しながらリスクをマネジメントすることは困難である。その結果、サイバーセキュリティ活動では、ビジネスへの影響との相関関係や因果関係が無視される傾向がある。これは、ビジネス部門の関与がほとんどなく、ビジネスをほとんど理解していない IT 部門とセキュリティ部門にすべての意思決定の責任を委ねている場合に特に当てはまる。例えば、攻撃者の目的や、どの組織資産が標的となり保護が必要かを理解せずに、マルウェア感染や不正アクセスなどのイベントのみに焦点を当てた技術分析を行うと、サイバー犯罪調査において誤った結論を導くことがある。

また、セキュリティ部門や内部統制部門の関与が弱かったり、業務部門がリスクを認識できなかったりして、リスクマネジメントやリスクへの対応が不十分になる場合もある。これは既存のガイドラインやフレームワークの盲点によって引き起こされ、リソースの制約やガバナンス構造の欠陥がある企業でよく発生する。

これらの問題に対処するには、以下の 3 つのリスクグループを「頂上事象」（フォールトツリー分析における最高リスクレベルのカテゴリー）として識別し、より効果的なマネジメントと説明責任を可能にするために、ビジネスと関連付けるべきである。

- 情報漏洩：例えば、顧客データベースからの情報漏洩
- 業務妨害：例えば、企業システムのシャットダウン
- 金融詐欺：例えば、詐欺に騙された経理担当者が権限のない受取人に対して行う支払い

リスクオーナーシップの明確化

リスクがピーク時の事象と事業との関連性によって定義される場合、説明責任はより明確になる。上級マネジメント職およびビジネスマネジメント職は、リスクの最終評価、対策の実施、インシデント発生後の対応など、組織のリスクに関する最終的な意思決定に責任を負う必要がある。ビジネスをサポートする一部の機能が、契約や定義されたサービスレベルを通じて請負業者、委託先パートナー、またはセキュリティ部門に委託されている場合でも、情報漏洩やサービス停止による影響（ビジネス、顧客、パートナー組織への影響）に対する責任はビジネスマネージャーにある。情報漏洩の場合は、COO（Chief Operational Officer）やセールスマネージャーが該当する。業務妨害の場合は、これは業務の責任者になる。金融詐欺の場合、財務部門の責任者がこれにあたる。

ピーク時の事象をビジネスにマッピングしなければ、リスク分析の作業負荷は過大になり、リスク評価は失敗する可能性が高くなる。IT セキュリティは頻繁にこの罠に陥る。特定のリスクの担当者を明確に特定しなければ、リスクの影響を判断することは不可能であり、非効率的な対策や投資につながる。合意は、リスクがビジネスに関連し、責任が定義されている場合にのみ可能である。

●「脅威」、「脆弱性」、「サイバーリスク」の関連性

リスクの定義が曖昧で多様なため、リスクマネジメントに関する議論が混乱しがちだが、その意味を確認することが重要である。リスクは、フィッシングメールなどの脅威や、（組織内のシステム、デバイス、あるいは人の）脆弱性が悪用されることによって引き起こされる。典型的なランサムウェアインシデントの場合、リテラシーの低い従業員（脆弱性）がフィッシングメールを開いて添付ファイル（脅威）をクリックすることにより、恐喝、データ漏洩、データ盗難（リスク）が引き起こされる。下記の図は、この関係の概略を示している。

表 11-1.「脅威」、「脆弱性」、「サイバーリスク」の関連性

脅威（脅威源）	脆弱性	リスク
フィッシングメール	リテラシーの低い従業員	• マルウェア感染による情報漏洩 • ランサムウェア感染による恐喝や妨害行為
エクスプロイト	パッチ未適用のシステム	• マルウェア感染による情報漏洩 • ランサムウェア感染による恐喝や妨害行為
悪意のあるウェブサイト	リテラシーの低い従業員によるアクセス 検出できないセキュリティソフト	• マルウェア感染による情報漏洩 • ランサムウェア感染による恐喝や妨害行為
なりすまし犯罪者	緩いアクセス制御	• ネットワークへの侵入
サプライヤー	サプライヤーの未熟なセキュリティマネジメント	• サプライヤーによる情報漏洩

脅威は、その発生源によって、図 11-2 に示すように、1）意図的、2）偶発的、または 3）第三者のいずれかに分類できる。意図的な脅威は、発生源によって、a）攻撃し、結果として生じる犯罪のためのバックドアを作成し、盗んだデータを恐喝者に販売する犯罪アクセス ブローカーやデータ ブローカーなどの外部の人物またはグループ、または b）明確な目的を持つ能動的な犯罪者、または外部の犯罪者によって犯罪を強いられる受動的な犯罪者である可能性のある内部の人物またはグループに分類することもできる。

偶発的な脅威は意図的なものではない。典型的な例としては、ソフトウェア、プロセス、または IT サービス操作におけるミスが挙げられる。

脅威は第三者から発生する場合がある。例えば、高度な標的型攻撃は、最初にソフトウェアサプライチェーン内の最も脆弱で相互接続されたサプライヤーネットワークをターゲットにし、関連する顧客組織を侵害するという目標を追求する場合がある。通常、サプライチェーンは複雑であるため、ソフトウェアサプライチェーン全体をセキュリティスクマネジメントに含めるには、膨大なリソースと時間が必要である。

資産マネジメント（情報、システム、アクセス権を含む）やセキュリティ監査が不十分な場合も、未知の脅威や未確認の脅威（未分類の脅威）をもたらす可能性がある。

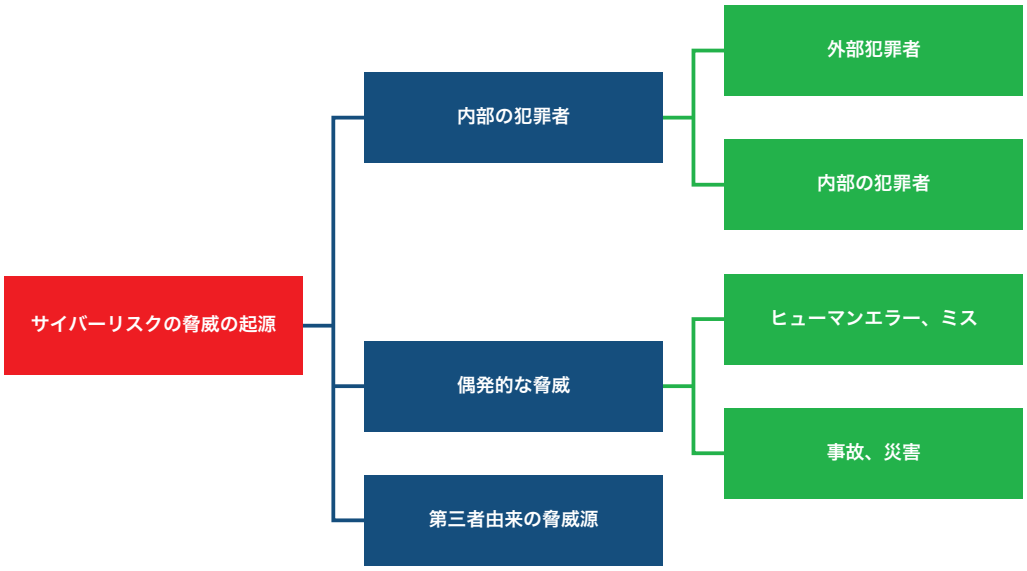


図 11-2. サイバーリスクの脅威の起源

リスクが現実のものとなると、悪影響は被害を受けた組織だけでなく、サイバー空間だけでなく現実世界にまで及ぶ可能性がある。例えば、2021 年に Colonial Pipeline に対して行われたランサムウェア犯罪により、米国の複数の州でガスと石油の供給が中断された。この場合、重要な業務運営の中断と恐喝（身代金の支払い）が組織にとってのリスクだった。

一般的に、リスクは次のように分類できる。

- 情報の盗難または漏洩
- 事業運営の妨害
- 金銭の盗難
- 名誉毀損（サイバースペースでのコミュニケーションによる）
- ネガティブキャンペーン

組織は、投資を導き、リスクを軽減するために、企業戦略や事業戦略マネジメントをこれらのリスクの潜在的影響と一致させる必要がある。歴史的に、多くの組織はサイバーリスク軽減活動をビジネス戦略と統合することに失敗してきた。サイバーリスクマネジメントの目的は、情報とシステムを保護するだけでなく、ビジネス自体を保護することである。したがって、リスクの潜在的影響はビジネス自体にリンクされている必要があり、リスク軽減はコストではなく投資になる。

リスクマネジメントフレームワークを次のように適用することで、組織はサイバーセキュリティと CI 活動に企業の優先事項を反映できるようになる。このアプローチにより、組織は調査中に法執行機関と効果的に連携し、ビジネスの優先事項を保護し、チーム間のスムーズな連携が可能になる。これを可能にするには、次のセクションで説明するように、組織はまずビジネス リスクを明確かつ明確に定義する必要がある。

リスクシナリオ

リスクマネジメントは、2つの主要な活動に分類できる。第1はリスクアセスメントで、リスクの特定、リスク分析、リスク評価で構成される。第2はリスク対応である。

リスクアセスメントの目的は、リスクがどのように発生するか、またリスクが現実化した場合の影響の大きさを特定することである。リスク対応の目的は、リスクへの対応方法を確立し、組織が許容できる範囲でリスクの影響を軽減することである。リスクアセスメントとリスク対応を組み合わせることで、次の蝶ネクタイ チャート図で視覚化されるリスク シナリオが作成される。

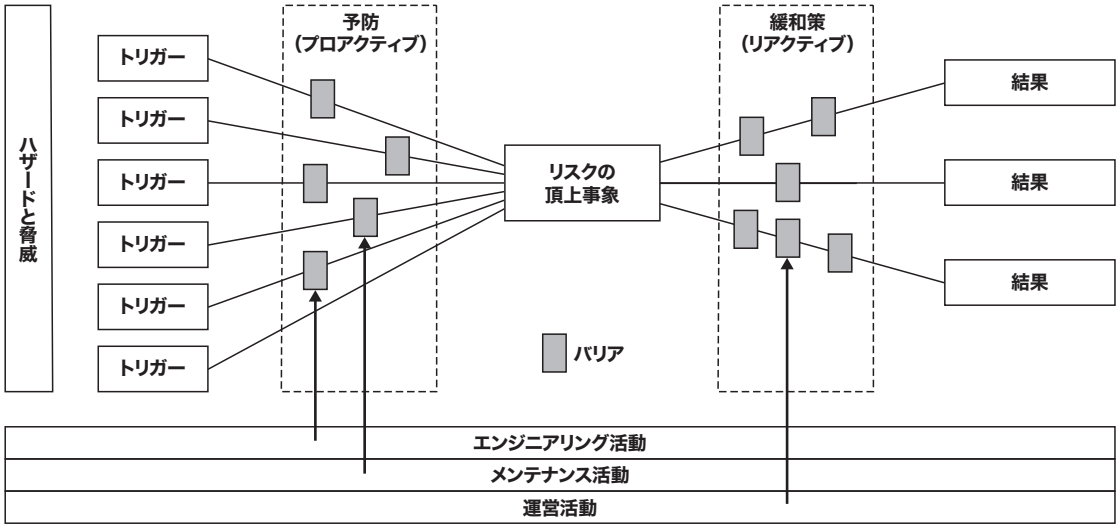


図 11-3. 蝶ネクタイ図 [318]

リスクシナリオの作成

上記の図に示すように、リスクシナリオには、予防的活動を必要とする脅威、危険なイベントそのもの、インシデント発生後の緩和活動、インシデントの顛末が含まれる。このアプローチは、定義されたリスクシナリオを既存の企業のリスクマネジメントの優先事項に統合し、より効果的なリソースの割り当てと意思決定をサポートするビジネス継続性マネジメント（BCM）の実践に適用できる。

ただし、選択した頂上事象が抽象的すぎると、分析が曖昧で不確実になり、利害関係者を納得させられない曖昧な評価結果が生まれる。選択したイベントの範囲は大きすぎたり小さすぎたりしてはならない。範囲が誤って調整されていたり、ビジネスの優先事項と一致していなかったりすると、リスクマネジメントプロセスを受け入れてその価値を認める利害関係者はほとんどいなくなる。

したがって、リスクシナリオは2つのフレームワークに基づいて作成する必要がある。まず、サイバー犯罪者が実際に犯罪目的を追求する方法を中心に定義し、侵入、ネットワーク内での準備、最終ターゲットを探すためのネットワーク内での横方向の移動、犯罪目的の実行という4つの主要なプロセスに分ける。

318 （Rausand, Marvin. - リスク評価:理論、方法、およびアプリケーション。ホーボーケン、ニュージャージー:John Wiley&Sons、2011年。p.120、図5.3）

図 11-4. 犯罪進行シナリオの例

さらに、**誰が何にどのように影響を与えるか**を尋ねる簡略化されたテンプレートを使用してリスクシナリオを作成する必要がある。

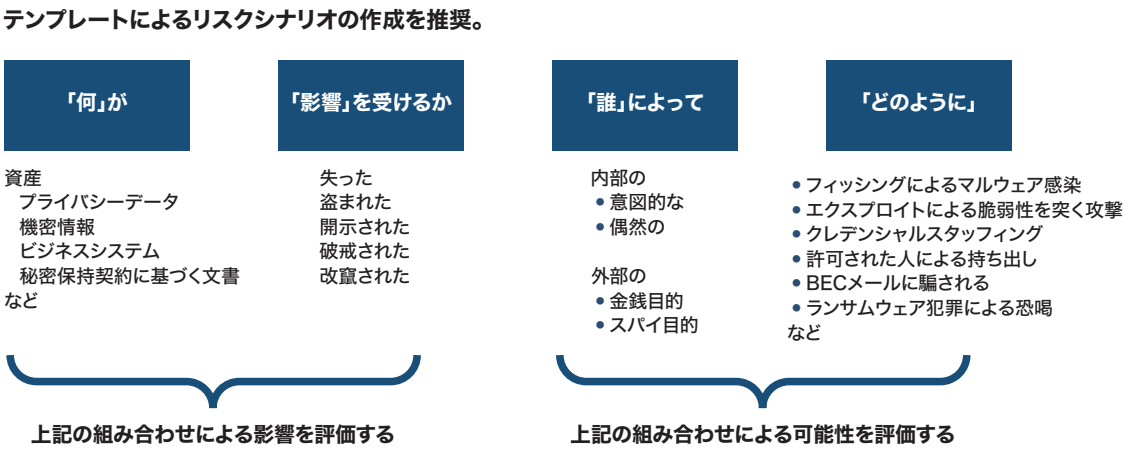


図 11-5. リスクシナリオを特定するためのサンプルテンプレートの例

リスクシナリオの特定は、特定、分析、評価、対応、監視からなる一般的なリスクマネジメントフレームワークにおける「特定」及び「分析」に相当する。

代表的なリスクマネジメントフレームワーク

サイバーリスクシナリオを作成した後、調整のためにリスクマネジメントフレームワークを選択する必要がある。既存のフレームワークを適用する方が簡単な場合が多いため、多くの組織は COBIT または IEC/ISO27001 の利用を選択している。ただし、これらのフレームワークは主に IT サービスマネジメントに重点を置いており、サイバーリスクマネジメントと CI 活動に合わせて調整しなければならない。

表 11-2. セキュリティマネジメントフレームワーク

フレームワーク	適用のメリットとポイント
IEC/ISO 27001（ISMS）	総合的な組織構造とマネジメントシステムを構築するためのアプローチを参照する
NIST RMF	サイバーリスクマネジメントライフサイクルに特に適応するフレームワーク
NIST CSF	セキュリティマネジメントに実践的に適応できる 5 つのコアと成熟度モデル
NIST SP 800-171	サプライヤーとして、要求される NIST SP 800-53 のうちの 14 ファミリーへの適合
NIST SP 800-53/ ISO27002	複数のファミリに分かれたセキュリティ制御を実施する方法に関する実用的なガイドライン

表 11-3. リスクマネジメントフレームワーク

フレームワーク	ポイント
ISO31000	基本プロセス（特定 - 分析 - 評価 - 対応）
ISO27001/ISO27005	サイバーセキュリティリスクに特化した分析および評価アプローチ
NIST SP800-30	サイバーセキュリティリスクに特化した分析および評価アプローチ
OWASP リスク評価	安全な Web 開発に特化したリスク評価など
脅威モデリング	ISO 31000 とその技法を定義した ISO 31010 に基づくリスク定量化方法
NIST RMF	情報資産と情報システムに焦点を当ててリスクに対処するモデル
STAMP/STPA/FRAM	複雑な技術分野の組み合わせからなるエコシステムにおける安全性

フレームワークの選択と適応において、最も考慮すべきことは、リスクをいかに最善に扱うかということである。組織ごとに資産、ビジネスの優先順位、戦略は異なる。したがって、リスクマネジメントシステムは、C レベルのリーダーシップの指導の下でビジネスニーズに合わせなければならない。リスクマネジメントの利害関係者間で価値観、優先順位、定義が異なると、リスクに関する議論は効果的ではなくなる。まず、共通のスコープ、定義、目標、フレームワークを確立する必要がある。

サイバーリスクマネジメントの実践

前述のように、サイバーセキュリティは下記の企業活動を含む。

- ビジネスとその戦略にとって重要な資産を特定し、そのリスクを定義する
- 資産を保護するために適切なリスク軽減（セキュリティマネジメント）に取り組む
- インシデントと顕在化したリスクをできるだけ早く検出する
- インシデントに適切に対応する
- 損害を制御し、回復力（レジリエンス）を強化する

これらの活動は、サイバーリスクからビジネスを保護するためにビジネス戦略と整合させなければならない。しかし、リスクマネジメントに関する既存のセキュリティガイドラインのほとんどは実際に運用するとなると非現実的なことである。これらのガイドラインのスコープは、ビジネスの整合を考慮せずにサイバーリスクのみに焦点を当てており、セキュリティ専門家が唯一のリスクマネジメント関係者として割り当てられている。サイバーリスクマネジメントを日常のビジネス慣行に実装するには、より実用的なアプローチが必要である。

保護すべき資産を特定する

リスクマネジメントの最初のステップは、保護が必要な資産（情報、データ、またはシステム）を特定することである。資産は、データとシステムが絶えず変更されることを考慮して、実践的に分類されなければならない。資産の特定の目的は、各ファイル単位で保護することではなく、ビジネス自体を保護することである。この点では、資産をグループ化し、それらをビジネス構造にリンクさせるカテゴリ化が役立つ。たとえば、アウトソーシング契約と秘密保持契約は、注文契約（契約文書のサブグループであり、法的機密情報のサブグループ）の下にグループ化できる。

法的機密情報 - 契約書類 - **発注契約書**

- アウトソーシング契約書
- 秘密保持契約書

資産の分類にはツリー構造を利用することが推奨される。資産の共有カテゴリは、オンプレミスかクラウドベースかに関係なく、多くの場合、共通のサーバーに保存すべきである。というのは、同じレベルにリスクを調整しようとすると、それらの資産を守るための共通のセキュリティコントロール（監視、アクセス制御、マルウェア対策など）が必要となるからである。共通のセキュリティコントロールではリスク対策が不十分となる資産は「リスクレベル高」のグループカテゴリを作成しておくと、そのカテゴリに対してのみ追加のリスクアセスメント活動が必要となる（つまり、すべての資産をつぶさに評価するという膨大なリソースと時間の消費を軽減できる）。「シャドーIT」が広範で従業員の行動が制御されていない組織では、従業員が簡単に許可されていない場所にドキュメントを保存できるため、このように実践時の効率化を実現できるようなカテゴライズのアプローチを行うことが困難になる。コンプライアンスとセキュリティプロセスを強化していくためには、資産の分類を効果的に行わなければならない。

影響を特定する

資産分類ツリー構造を作成する際には、リスクの影響と資産の機密性、整合性、可用性（CIA トライアド）を考慮する必要がある。影響度が異なる資産（リスクが顕在化した場合）は、一緒に分類すべきではない。利害関係者間の不一致を避けるために、影響度の共通定義が必要である。下記に例を示す。

- 大規模：影響は組織にとって重大なもの（たとえば、事業の破綻）
- 中規模：影響は事業に損害を与え、1 四半期より長く続く
- 小規模：影響は 1 四半期以内に回復する

影響の大きさの定義は個人的な偏見を避けるべきであり、下記に示すように、FIPS199（連邦情報処理標準 199）などの既存のガイドラインによってサポートされる。

表 11-4. 米国 FIPS199 の潜在的影響

	潜在的な影響		
セキュリティ目標	低	中	高
機密性 ***個人のプライバシーや専有情報を保護するための手段を含む、情報へのアクセスと開示に対する認可された制限を維持する***	情報の不正な開示は、組織の運営、組織の資産、または個人に限定的な悪影響を及ぼすことが予想される	情報の不正な開示は、組織の運営、組織の資産、または個人に重大な悪影響を及ぼすことが予想される	情報の不正な開示は、組織の運営、組織の資産、または個人に重大または壊滅的な悪影響を及ぼすことが予想される
完全性 ***不適切な情報の変更や破壊を防ぎ、情報の否認不可性と真正性を確保することを含む***	情報の不正な変更または破壊は、組織の運営、組織の資産、または個人に限定的な悪影響を及ぼすことが予想される	情報の不正な変更または破壊は、組織の運営、組織の資産、または個人に重大な悪影響を及ぼすことが予想される	情報の不正な変更または破壊は、組織の運営、組織の資産、または個人に重大または壊滅的な悪影響を及ぼすことが予想される
可用性 **情報を利用するためのタイムリーで信頼性の高いアクセスを確保する**	情報または情報システムがアクセスできなくなると、組織の運営、組織の資産、または個人に限定的な悪影響を及ぼすことが予想される	情報または情報システムがアクセスできなくなると、組織の運営、組織の資産、または個人に重大な悪影響を及ぼすことが予想される	情報または情報システムがアクセスできなくなると、組織の運営、組織の資産、または個人に重大または壊滅的な悪影響を及ぼすことが予想される

リスク発生シナリオの特定

資産を分類したら、次のステップは、リスクシナリオのセクションで説明したように、資産がどのように侵害される可能性があるかを特定することである。ここでは、実際のリスクマネジメントの取り組みをガイドするための追加の詳細を示す。

●共通シナリオ

共通シナリオは、重要な側面とパターンを共有している。たとえば、従業員の PC が侵入の入り口である場合、サイバー犯罪者はその PC を利用して犯罪活動の基盤を作り、その後の活動の基盤を（ボットネットなど経由で）拡大して、ネットワーク内でより簡単に外部からコントロールする可能性がある。ネットワーク内を横方向に移動して、標的の資産にアクセスし、盗む可能性がある。このような場合、どの従業員の PC が不正アクセスされたかに関係なく、シナリオの詳細はそれほど変わらないかもしれない。PC のセキュリティ管理施策は、ネットワーク管理施策と同様に全従業員間で共通可能性がある。このような組織全体に共通するシナリオを定義する主なステークホルダーは、3 ライン防御モデル（第 10 章で説明）の第 2 ライン、つまりセキュリティ専門チームであるべきだ。

ただし、たとえば従業員がネットワークにアクセスするデフォルトのパスワードを持つ未承認の SaaS サービスや IoT デバイスを使用する場合、共通化されて定義されるシナリオには隠れた側面があるかもしれない。したがって、共通シナリオを定義する前に、アタックサーフェスの可視化（可能ならば、ある程度自動化）を追求することが重要である。共通シナリオには、従業員が必ずしもセキュリティ ルールに従わない可能性を考慮した条件を含めるべきである。

●個別シナリオ

いくつかのシナリオは個別的であり、共通シナリオではカバーできない。例えば、業務部門で特定の用途を持つ SaaS アプリケーション、マーケティング部門が構築した Web サーバー、工場の制御システムなどのシナリオなどである。このような場合、第 1 ラインチーム（ビジネスセクション）がリスクアセスメントを実施すべきである。

クラウド移行がより一般的になり、ビジネスプロセスの変更がより急速に起こるようになると、より

多くの個別のシナリオが生み出され続けるであろう。未知の個別のシナリオの数を制限するには、定期的および不定期の両方のアセスメント活動が必要である。定期的アセスメントは、PDCA サイクルに合わせる必要がある。不定期アセスメントは、重大な脆弱性が発見された時、組織（人員とプロセス）に大きな変更があった時、重大なインシデントやルール違反などが発生した時などのように定義されたイベントによってトリガーされるべきである。

●分析の方法

テンプレートなどを使って作成するリスクアセスメントシートは、分析されたリスクシナリオの最終成果物である。このようなアセスメントを効率的に実施するためのテンプレートの作成には、根本原因分析や品質マネジメントに使用される（ツリー構造、いわゆる「アタックツリー」を使用）フォールトツリー分析（FTA）などのシナリオ特定ツールが役立つ。例えば、FTA では、「頂上事象」は、すべてのビジネスセクションで使用される顧客データベースのデータ漏洩であるかもしれない。頂上事象の下に主要なカテゴリが作成され、詳細な分析が開始される。例えば、頂上事象は、外部の犯罪者、内部の犯罪者、事故やミス、またはサプライヤーなどの第三者によって引き起こされる可能性がある。以下に FTA のサンプルを示す。

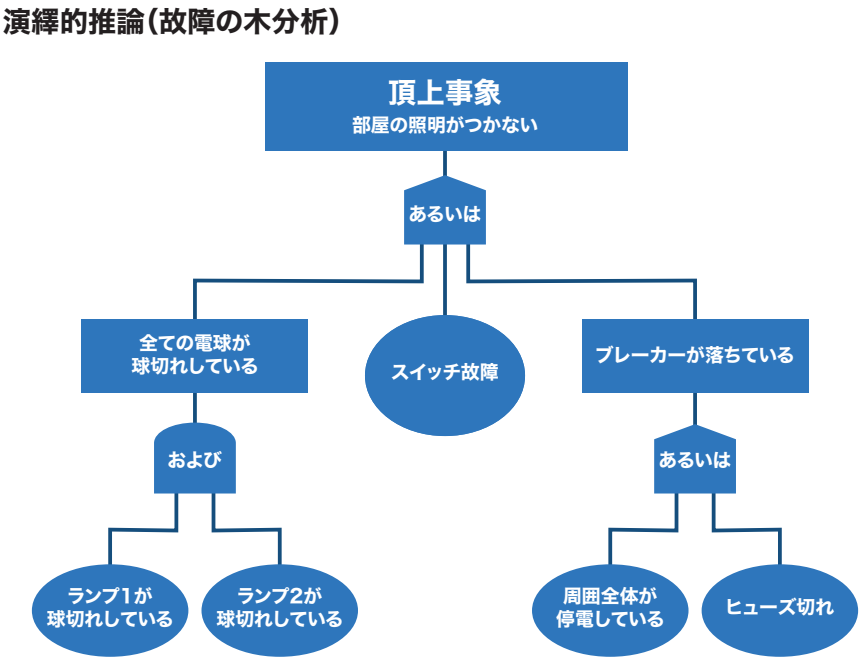


図 11-6. フォールトツリー分析チャートの例

●注目すべき点

サイバー犯罪者は、さまざまな方法を使ってネットワークを標的にし、侵害を企てる。リスクシナリオを適切に作成するには、方法論のニュアンスを把握することが重要である。MITRE ATT&CK は、MITRE Corporation が提供するリソースで、観察されたサイバー犯罪の手法を文書化し、ほとんどの分析に十分な詳細情報を提供している。ただし、高度な技術的知識を必要とする過度に詳細まで分析を試みることは避け、第 2 ラインセキュリティスペシャリストに過度の負担をかけない実践的なアプローチを可能にする必要がある。同時に、前述のように、詳細が少なすぎることも避ける必要がある。シナリオは、技術的な詳細をあまり多く含んで作成せずに、主要な側面に基づいて記述するという絶妙なバランスを実現しなければならない。結局のところ、リスクマネジメントの目的は、実践的な取り組みを通

じてビジネスを保護することである。たとえば、リスクシナリオは次のように記述できる。「犯罪者はなりすましのアカウントでログインし、VPN などの正当なツールを使用して、標的のデータにアクセスして盗みだす」。組織は、そのような犯罪者の行為が既存のセキュリティ管理施策とプロセスによって検出されブロックされるかどうか、また、そうでない場合はどのような是正手順が必要かを判断する必要がある。

インシデント発生後のリスクシナリオの特定

組織は、リスクの発生シナリオと、インシデントが発生したときの対応方法も特定すべきである。この場合も、シナリオを過度に増やし過ぎないようにグループ化する必要がある。開始点として、下記のグループが推奨されます。

●初期侵攻段階

侵害の兆候を非常に早い段階で検出できれば、対応シナリオが効果的に機能し、被害をほぼ完全に軽減できる可能性がある。たとえば、SDN（Software Defined Network）による自動ネットワーク切り替えによって犯罪者がダミーの囮の標的に誘導されたり、組織が犯罪者がアクセス権を取得する前にアクセス権をリセットできれば、データの盗難を防ぐことができる。犯罪者の行為による影響をよく観察することで、犯罪者の目的を特定することもできる。ただし、犯罪者を泳がせて様子を見るよりは、検出後にただちにブロックすることが最善のアプローチになることが多い。

●ネットワーク内の活動の段階

犯罪者がネットワークにアクセスしてから数日後に検出が行われた場合、侵入に要した時間の長さを特定することが重要である。この情報は、犯罪者がすでに目的を遂行してしまったかどうかを判断するのに役立つ。さらに、対応シナリオでは、どの資産が影響を受けたか、どの程度の損害が発生したか（侵害、改竄、盗難など）を特定する必要がある。この調査の側面は、感染したマシンのクリーンアップの前に行う必要がある。というのは、感染したマシンには調査に不可欠なアーティファクトが含まれているからである。クリーンアップが実行されると、アーティファクトを収集することはほぼ不可能になる。

例えば、ログデータは多くの調査において重要なアーティファクトである。セキュリティソフトなどのアラートによる検出があった場合、クリーンアップ活動によってログデータが失われると、組織はインシデントの本質を完全に理解できず、インシデントによるその後の影響に備えることができなくなる。例えば、機密情報が盗まれた場合、ビジネス戦略に影響が出る可能性がある。特権アクセスを持つ従業員の資格情報が盗まれた場合、その資格情報を使用して別のスパイ活動が開始されたり、機密情報が一般に公開されて組織の評判が損なわれたりすることがある。

犯行のある程度進行してしまった後で検知されたインシデント対応の場合、法執行機関とどのように連携するのが最善か、また関係者（内部および外部の両方）とどのようにコミュニケーションをとるかを検討することも重要である。被害を受けた組織は自社のネットワーク内でしか調査できないため、サードパーティ環境内の重要なアーティファクトは法執行機関が調査しなければならないことが一般的である。

●データ侵害後の段階

犯行の最終目的が遂行されてしまった後に検知されたインシデントの場合（たとえば、ランサムウェアグループが盗んだデータを公開した後に企業がデータ盗難を検出した場合）、犯罪がまだ進行中かどうかを判断することが重要である。ここでの例では、分散型犯罪活動と CaaS の共通性を考えると、ランサムウェアの関連する別の犯罪グループ（ransomware as a service の加入者を含む）が盗まれたデー

タにアクセスして、さらに恐喝を行う可能性がある。このシナリオのスコープは、効果的な対応を展開するために、サイバー犯罪者の技術的な方法に加えて組織的な戦略を理解する必要があることを強調している。

●対応シナリオを作成する方法

影響の木分析（ETA：Event Tree Analysis）は、インシデント対応シナリオの開発をサポートする優れたツールである。ETA は「トリガーイベント」から始まり、イベント（およびその結果）がどのように進行するかを検討し、各結果に決定ポイントを設定する。たとえば、トリガーイベントが組織の SOC からのアラートである場合、対応の初期段階は、インシデントが発生したかどうか（または発生しなかったかどうか）とそれに関連する影響を特定するためのトリアージである。インシデント（または犯罪）のすべての段階がどのように進行するかを特定することは、効果的な対応を行う上で重要である。幸いなことに、イベントの結果には特定のパターンがある傾向があり、組織は過去のインシデントから学ぶことができる。前述のように、インシデントが検出される段階（最初の侵入、ネットワーク内のアクティビティ、およびデータ侵害後）に基づいて、3 つの主要なシナリオパターンがある。したがって、組織は 3 つのパターンに対応する 3 つの一般的な対応シナリオを作成し、そこからより具体的なシナリオを作成すべきである。

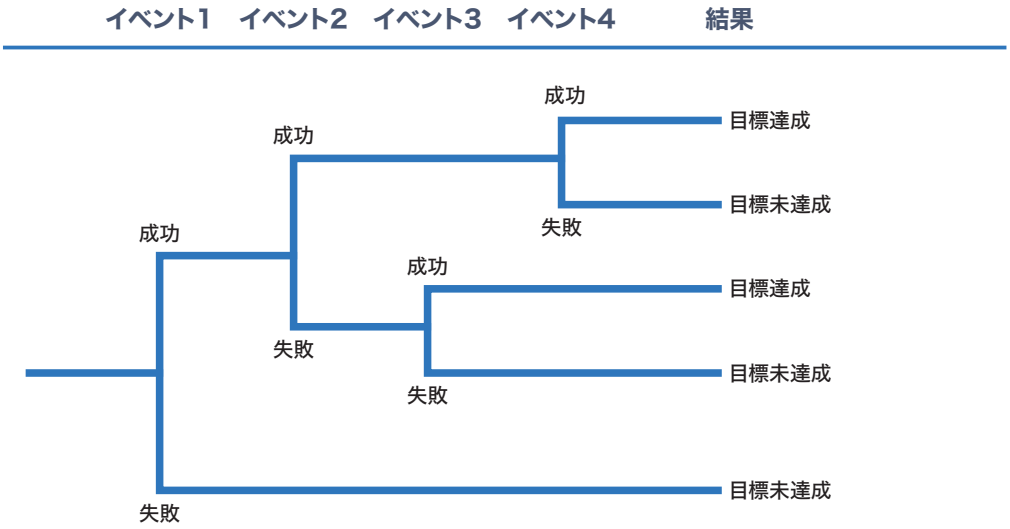


図 11-7. 影響の木チャートの例

リスク評価

リスクシナリオを特定したら、次のステップはリスクの評価である。一般的なリスクマネジメントガイドラインでは、リスクは、影響の大きさに発生の可能性（確率）を掛け、それを組織のリスク軽減能力で割ることで決定される。ただし、第 10 章で述べたように、サイバーリスクは必ずしも簡単に定義できるわけではない。例えば、サイバー犯罪者の行動が予測できない場合、確率は必ずしも簡単には決定できない。さらに、重大な脆弱性が講評されたような場合、確率は増加する。これは、リスクが静的ではなく動的な尺度であることを証明している。

いずれにせよ、リスクは、リスクを防止または軽減する組織の能力によって計算される必要がある。たとえば、組織がリスクシナリオを特定し、適切なセキュリティ制御を適用する能力（3 ラインモデルに従って、第 1 ラインと第 2 ラインの防御の連携を通じて）を備えている場合、リスクを軽減できる。

●シナリオごとのリスク値

リスク評価は、前述のとおり、発生シナリオを特定することから始めるべきである。しかし、セキュリティ対策を実施した後に評価を進めることもできる。対策の有効性は、対策の実施前と実施後のリスク値の差によって識別できる。

●セキュリティマネジメント

多くのセキュリティ管理施策は、関連するテクノロジー、人材、プロセスの点において、組織横断的に共通である（ファイアウォール、IDS/IPS、マルウェア対策ソフトウェア、EDR など）。共通の管理施策は、デフォルト的であり資産リスクを十分に機能を果たすとは限らないが、特定のリスクシナリオに合わせてカスタマイズして調整できる。これは、コスト効率の高いリスクマネジメントを実現するための重要なステップである。さらに、単一の管理施策のみでは通常、リスクの発生を十分に防ぐことはできないため、階層化された防御における制御の組み合わせが重要である。

●定量的評価

リスクの定量的値は、合理的かつ科学的なアプローチには有益である。ただし、定量的値は実際には複雑になることがある。例えば、リスク報告者がリスクを 80/100 と定量化したとしても、報告先の幹部が 100 点満点のスコアを理解していない場合（つまり、共通の値を伝えていない場合）、定量化は役に立たない。定量的値を使用する前に、指標システムに関する共通の理解を深める必要がある。以下に示すリスクマトリックスアプローチは、リスクを定性的に評価するためのよく知られた一般的なシステムである。

表 11-5. 定量的評価のためのリスクマトリックスの例

リスクマトリックスアプローチ（RMA）

リスク値			重大度				
確率			壊滅的	危険	大規模	小規模	無視できる
			5	4	3	2	1
	頻繁	5	25	20	15	10	5
	時々	4	20	16	12	8	4
	Remote	3	15	12	9	6	3
	あり得ない	2	10	8	6	4	2
	極めてあり得ない	1	5	4	3	2	1

組織が総合的なリスクマネジメントを実施できるほど成熟すると、前述の FTA や ETA などのツールを定量的リスク評価と統合できる。ただし、サイバーリスクには常に人的要因が伴うため、定量的指標はセキュリティ制御の有効性を評価する際に最適であり、組織が犯罪者の標的になるかどうか、その確度を判断する際に最適ではない。

下記の ETA の例では、フィッシングメールがトリガーイベントである。ツリーには、メールがメールゲートウェイでブロックされる可能性、受信者がメールを開く可能性、受信者が添付ファイルを開く可能性、セキュリティソフトウェアが脅威を検出してブロックする可能性が示されている。これは、組織のセキュリティ制御の脆弱性と弱点を特定するための便利なアプローチである。

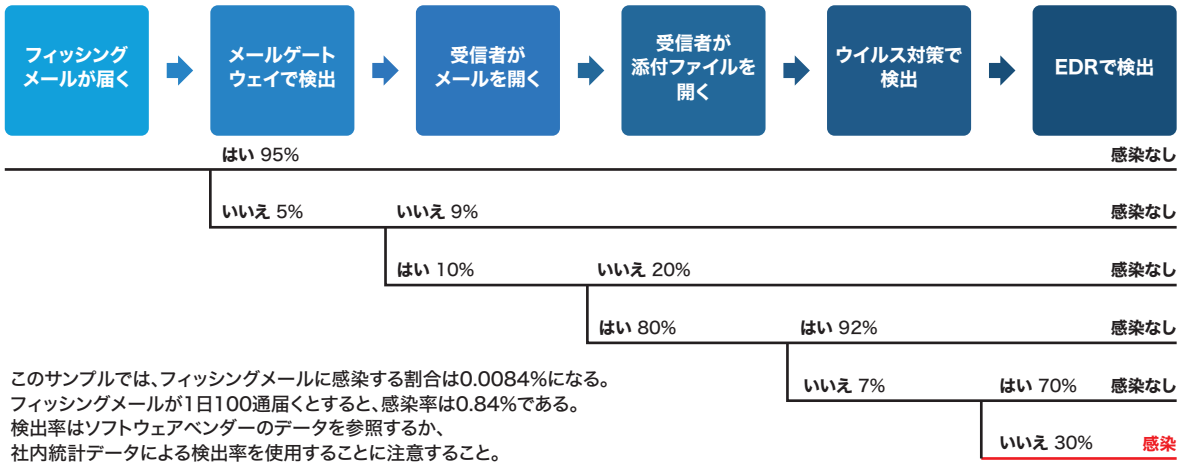


図 11-8. イベントツリーを用いた犯罪成功確率の分析

●脆弱性への対処

既存のサイバーセキュリティリスクマネジメントガイドラインの中には、脆弱性を考慮することを推奨しているものもある。しかし、脆弱性はまだ認識されていない場合や動的に変化する場合もあるため、リスク評価で脆弱性を考慮することは必ずしも現実的ではない。脆弱性情報に PDCA サイクルを使用するよりも、より短いサイクルで即時の対応を可能にする OODA ループの方が有益である。これにより、関連するシステムや資産に影響を与える脆弱性（または複数の脆弱性）を評価段階で完全に把握できていなくてもリスク評価を進めることができる。OODA ループにより、セキュリティ運用でリスクを迅速に評価し、意思決定（システムのシャットダウンやソフトウェアのパッチ適用など）を行うことができる。

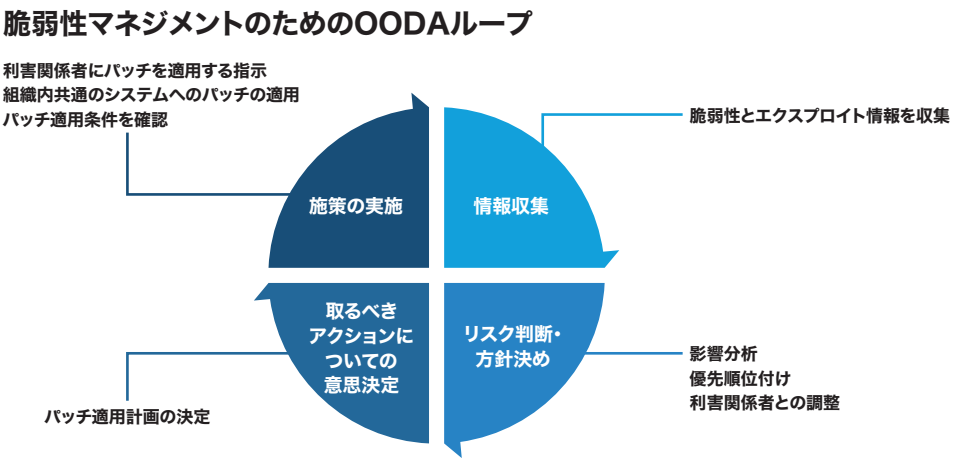


図 11-9. 脆弱性対応のための OODA ループ

リスク対応

リスクアセスメント（シナリオ／発生の特定、対応策の確立、リスクの評価）の後、リスク対応を決定しなければならない。リスク対応には、1）除去、2）低減、3）移転、4）受容の 4 つの選択肢がある。前述のように、セキュリティ管理施策によってリスクを軽減することはできるが、除去することはできない。また、被害者はリスクを第三者に完全に移転することはできない。下記の図は、確率と影響度に関連する 4 つのタイプのリスク対応の概要を示している。

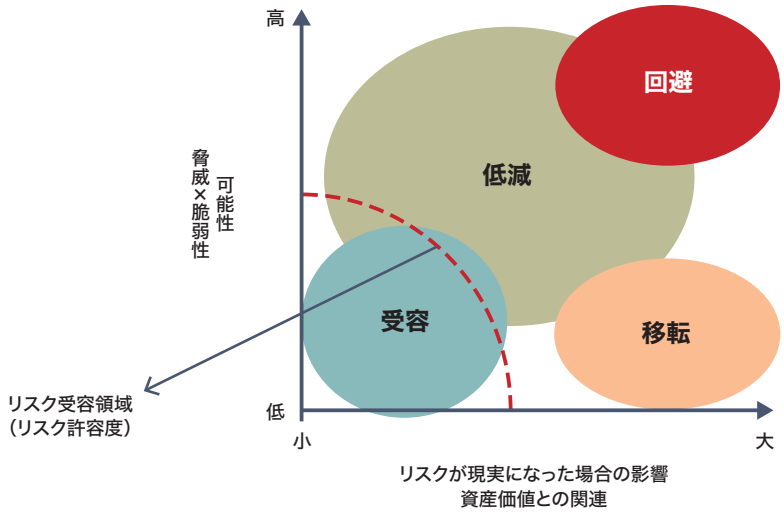


図 11-10. リスク対応の選択肢

リスク対応に関する決定は、コスト（リスクの軽減または受容、プロジェクト スケジュールの遅延など）を考慮する必要があるため、説明責任のあるビジネス利害関係者を関与させるべきである。さらに、説明責任のある利害関係者が決定を合理化できない場合、最終的に間違った決定を下した場合に、決定の背景を理解していないことで、（ブランドの評判などに）さらなる損害を与える可能性がある。したがって、意思決定者は、ビジネスチーム（3 線モデルでいう「第 1 線」）の資産（情報、データ、またはシステム）の所有者である必要があり、第 2 線（セキュリティスペシャリスト、リスクマネジメントチームなど）は、関連情報を提供して意思決定者の決定をサポートすべきである。意思決定者がセキュリティチームにいる場合、リスクを受け入れる可能性は低く、リスク軽減のコストが増加し、セキュリティ管理施策をさらに実装するにつれてプロジェクトが遅れることになる。

下記の用語は、リスクマネジメントを進める意思決定者をサポートするのに役立つ。

- **リスクキャパシティ**：コスト、リソース、あるいは社内外の関係者からのサポートを必要とする点で、組織が保持できる最大限のリスク。たとえば、リスクのコストをカバーするための資金が利用可能であれば、それは許容できる可能性がある。ただし、リスクの影響を定量的に特定することは困難であり、リスク容量のみに基づいた決定は推奨されない。
- **リスクプロファイル**：サイバーリスクや災害リスク、人的リスクなど、その他の種類のリスクを含む、事業の過程で組織が被るリスクの総量。リスクプロファイルでは、質的リスクを量的に変換する必要がある。たとえば、ランサムウェアによる事業中断に対応するためにどれだけの資金が必要かということなどである。
- **リスクアペタイト**：ビジネス目標に沿って、組織が敢えて取ろうとするリスクの量。たとえば、現在開発中のアプリケーションのリリース日に間に合わせるためのスケジュールが厳しく、ユーザーに多大な影響を与える可能性のあるバグがいくつかある場合、ビジネス関係者は、許容できるリス

クの量に基づいて、アプリケーションを予定どおりにリリースするかどうかを決定する。この場合、組織はリリース後すぐに自動パッチ適用でバグを修正する緩和計画を実施し、リスク期間を最小限に抑えることができる。リスク許容度は、ビジネスとセキュリティの両方の観点から考慮しなければならない。

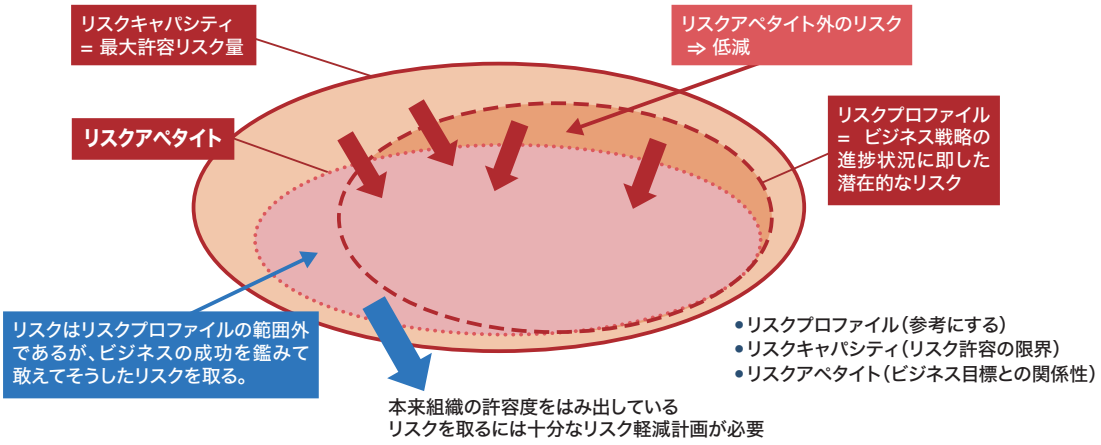


図 11-11. リスクプロファイル、リスクキャパシティ、およびリスクアペタイトの関係

- **リスクアペタイトの限界値**：組織がポリシー、戦略目標、セキュリティ目標に沿ったリスクマネジメントの基準に従って敢えて取ることを厭わない最大許容リスク。これは、リスクマネジメントの意思決定を導く重要なベンチマークである。リスクアペタイトの限界値を確立するには、リスクマネジメントの成熟度が必要である。
- **ALARP（As Low As Reasonably Practicable：合理的に実行可能な限り低く抑える）**：リスクを低減しなければならないレベルを表す概念。ALARP 領域とは、合理的に実行できるレベルを意味しており、実際にリスクを全て除去することはできず、また低減するためのコストや日程、リソースが対象の事業の価値に対して釣り合わない場合にはリスクを取る（許容する）ことの方が合理的という考え方である。例えば、月に 100 万円の売り上げが見込めるシステムの抱えるリスク低減に 100 万円を超えるコストが必要。ALARP は、組織が特定のリスクマネジメント決定を下した方法と理由を説明するのに役立つフレームワークを提供する。

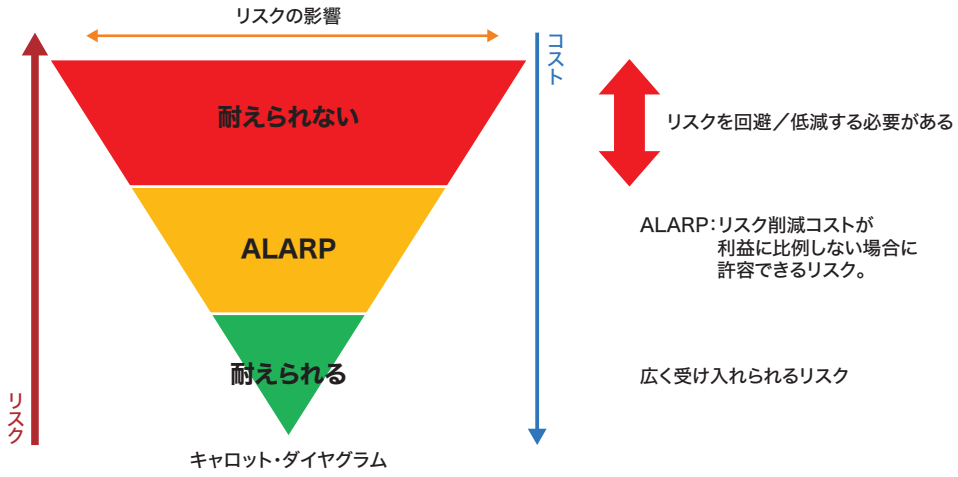


図 11-12. ALARP

費用便益分析（CBA：Cost Benefit Analysis）を使用すると、リスク削減のコストがリスクのコストと一致するポイントを特定して、ALARP を決定することができる。この方法で CBA を適用するには、定量的なリスク評価を活用しなければならない。

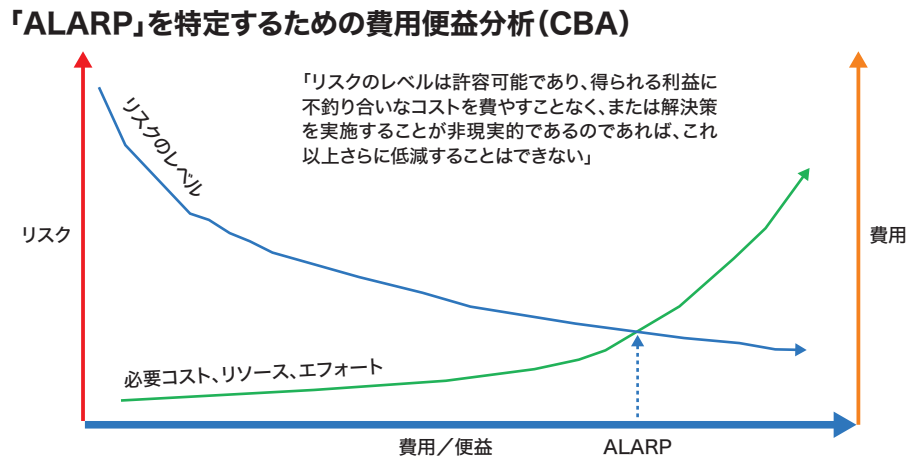


図 11-13. 費用便益分析を用いた ALARP の計算

リスクモニタリング

リスクマネジメントの最後のフェーズは、リスクレベル（およびそれが許容可能かどうか）をモニタリングして、すでに適用したリスク低減のための各種施策の有効性を確認することである。このフェーズは、リスク低減策自体のの価値を実証する上で非常に重要である。リスクモニタリングは、PDCA サイクルの「チェック」フェーズに相当する。

評価されたリスクシナリオに影響を与える変更が頻繁に発生し、リスクレベルが上昇することに注意することが重要である。例えば、重要な資産を含む企業の特定の業務運用システムを標的とする新しい悪意のあるツールが見つかった場合などである。これにより、最初のリスク評価が完了したときよりもリスクレベルが高くなる状況が発生する。そのため、リスクモニタリングを定期的に（リスク削減アクションの前、期間中、後に）実施して、変化するリスクレベルを可視化するリアルタイムのリスクダッシュボードシステムに通知すべきである。

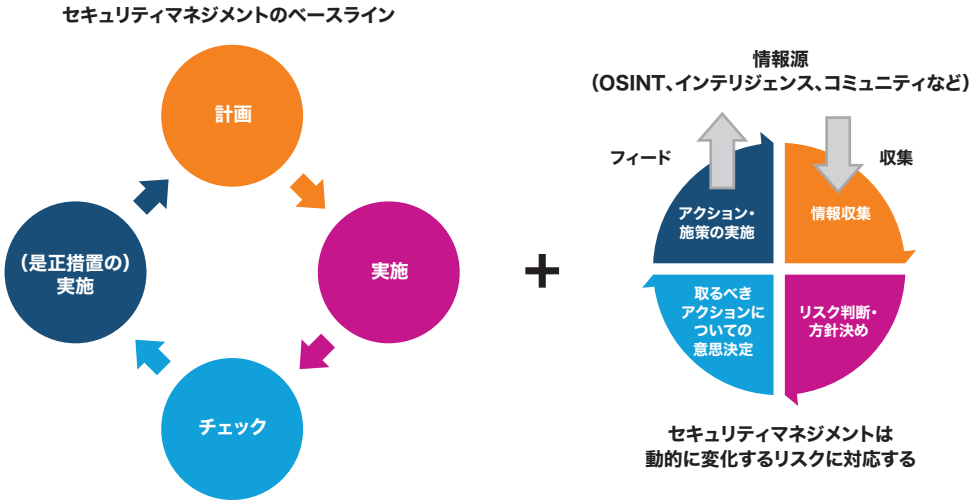


図 11-14. サイバーセキュリティPDCA ＋ OODA

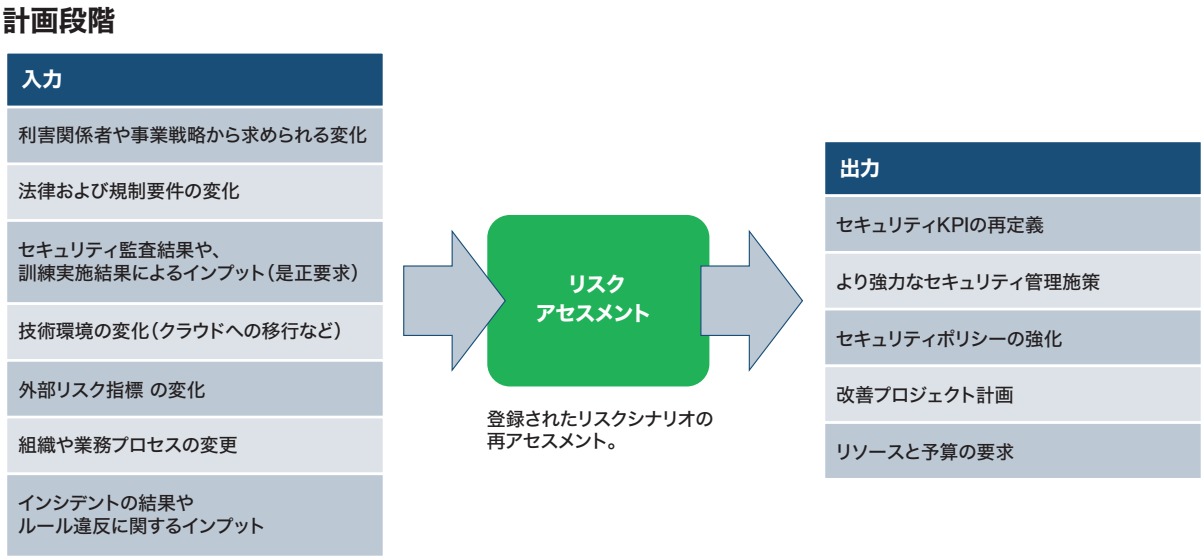


図 11-15. リスク再評価の入力例

リスクの動的な性質を最適に把握するには、リスクレベルを再評価（再査定）するためのトリガーを活用すべきである。トリガーには下記のものがある。

- リスクの影響（例：CIA トライアドによる影響度の大きさ）が変化する場合
- セキュリティインシデントが発生した場合
- 大規模な脆弱性が報告された場合
- 大規模な組織変更または役割変更が発生した場合
- 大規模なシステム変更が実施された場合
- 大規模な業務プロセス変更が発生した場合
- 法的規制または政府要件が発効した場合

リスクレポートと見直し

リスクマネジメントの進捗状況、有効性、従業員の目標を確認するための可視化システムは不可欠である。しかし、多くの組織は、リスクマネジメントの結果をビジネスおよび経営幹部の関係者に伝える際に課題に直面する。最も一般的な課題には、下記のようなものがある。

1. 経営陣がセキュリティチームの報告を理解していない
2. リスク報告の内容が取締役会で議論されない
3. ビジネス環境の変化（頻繁かつ急速な変化にもかかわらず）に応じてリスクシナリオのレビューが実施されていない

CISO（最高情報セキュリティ責任者）は、これらの問題を解決する上で重要な役割を果たす。CISO は組織およびビジネス要件を考慮し、経営幹部およびビジネス関係者向けのセキュリティレポートを要約・意訳すべきである。セキュリティ関連のアクティビティ（担当チームに関係なく）の KPI を策定し、刹那的な／受動的なサイバーセキュリティアクティビティを回避するために高レベルのビジネスニーズと整合させる必要がある。CISO は、適切なリスクガバナンスの重要な側面である、経営幹部が適切な決定を下しているかどうかを取締役会が確認できるように支援すべきである。

成熟度モデルは、リスクマネジメントコミュニケーションに役立つ追加の考慮事項である。例え

ば、重要インフラ企業向けの NIST のサイバーセキュリティフレームワーク（米国国立標準技術研究所 - NIST CSF）[319] と米国国防総省が開発した CMMC（サイバーセキュリティ成熟度モデル認証）フレームワーク [320] は、どちらも組織のセキュリティレベルを評価するために成熟度モデルを推奨している。注目すべきは、どちらのモデルも、組織がサイバーセキュリティをどのようにマネジメントするかに焦点を当てており、リスクをアセスメントに特定する方法に焦点を当てていないということである。成熟度モデルとリスクシナリオベースのアセスメントを組み合わせることで、リスクの視覚化とレビューを強化できる。

下記の戦術は、CISO がリスク報告を経営幹部に効果的に伝えるのに役立つ。

1. 「マルウェア感染リスク」（リスクシナリオの一部に過ぎない）ではなく、「マルウェア感染による情報漏洩」（ビジネスに何が起こるか、その影響を強調）を報告すべきである。
2. リスクの定量的な価値を伝えるには、「コスト」や「必要なリソース」などの、理解しやすくビジネスに即したリスク指標を使用する必要がある。さらに、セキュリティ KPI を BSC（バランスト スコアカード）やその他のパフォーマンスマネジメントフレームワークに実装すべきである。
3. 経営幹部への報告は定期的に（月次、少なくとも四半期ごとに）実施すべきである。報告内容では、リスクの説明に加えて、経営幹部に求められることとセキュリティに求められることについて対話を促す必要がある。

319 https://www.nist.gov/cyberframework
320 https://dodcio.defense.gov/CMMC/About/

11章:CIBOKの分類法との関係

前述したように、CIBOK 分類法の実行フレームワークは、組織におけるサイバー調査の機能と有用性を理解するために必要な知識領域間の相互関係を詳述している。サイバー犯罪を捜査するプロセスは、犯罪の範囲（および関連するアーティファクト）に応じて、利用可能な証拠源の種類を決定することに依存し、証拠収集と分析の実践的な方法によって支えられている。被害者と官民両セクター間の責任ある情報共有は、組織がサイバー犯罪事件を解決するのに役立つ。

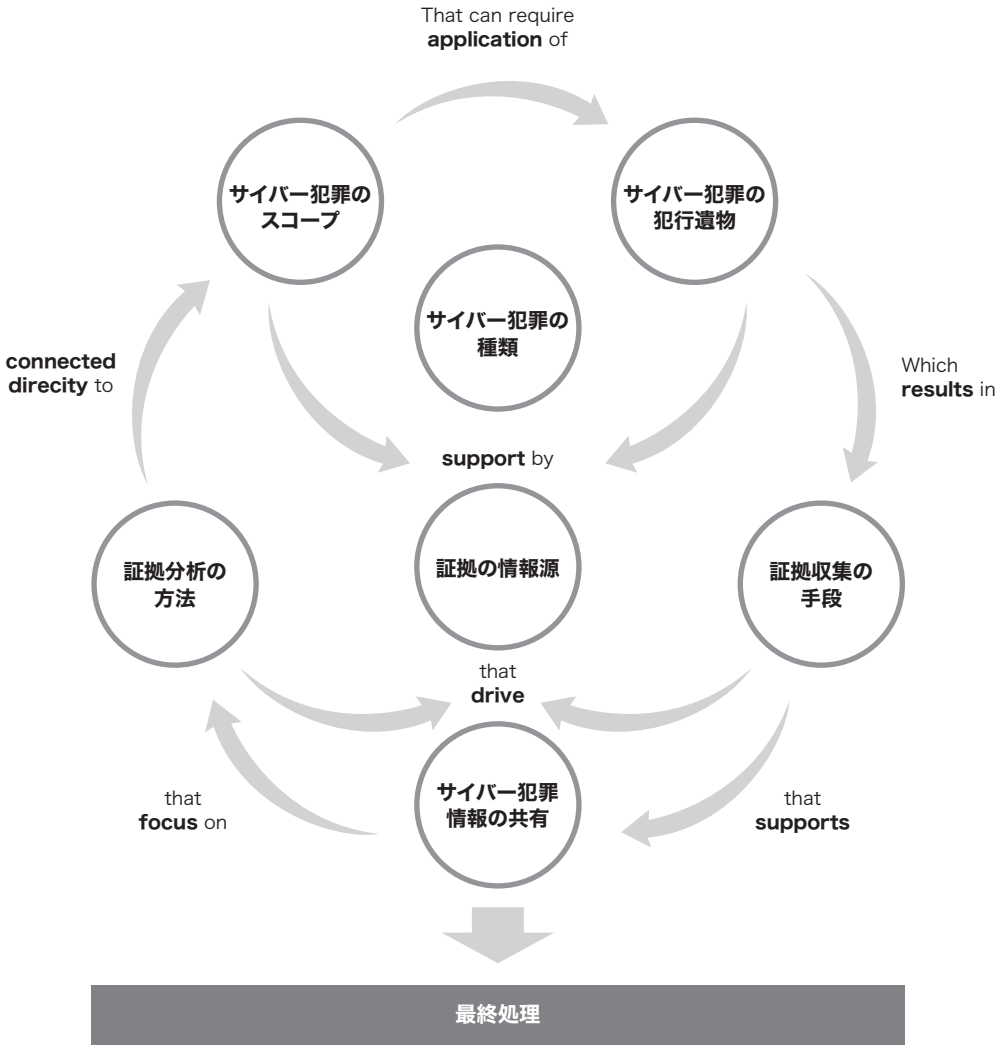


図 11-16. サイバー犯罪捜査およびインシデント調査における実行フレームワーク

実行フレームワークと、CIBOK のスキルおよび知識の分類（表 11-6）との関係は、さまざまな役割によって機能上の要件が異なることを示している。

表 11-6. CIBK の分類法

	要求されるスキルおよび経験						
CIBOK のフレームワーク	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	高	高	高	高	低	低	–
サイバー犯罪の種類	高	高	高	高	高	低	低
サイバー犯罪の目的	高	高	高	高	高	低	低
サイバー犯罪者のプロファイル	高	高	高	高	高	–	–
サイバー犯罪組織	高	高	高	高	高	–	–
兆候	高	高	高	低	低	低	–
ステージ（段階）	高	高	高	中	中	低	–
サイバー犯罪の犯行遺物	中	高	高	–	–	低	–
サイバー犯罪のスコープ	中	高	高	中	中	低	–
証拠の情報源	中	高	高	中	–	低	–
証拠収集の手段	中	高	高	中	–	低	低
証拠分析の方法	中	高	高	中	–	低	低
最終処理	高	中	高	中	中	低	低
サイバー犯罪情報の共有	中	高	高	高	高	低	低
管理フレームワーク	高	低	中	低	低	低	中

表 11-7. サイバー犯罪捜査およびインシデント調査における実行フレームワークと CIBOK の分類法との関係

	捜査管理	知見収集	調査	説明責任	予防啓発	後方支援	総務人事
サイバー犯罪とその捜査	S	T	T	S	T	P	P
サイバー犯罪の種類	S	T	T	S	S	T	P
サイバー犯罪の犯行遺物	S	T	T	T	P	T	P
サイバー犯罪のスコープ	S	T	T	S	T	T	P
証拠の情報源	S	T	T	T	P	T	P
証拠収集の手段	S	T	T	P	P	T	P
証拠分析の方法	S	T	T	P	P	T	P
最終処理	S	T	T	S	T	P	P
サイバー犯罪情報の共有	S	P	P	T	T	P	T
管理フレームワーク	S	P	P	P	P	P	T

＜凡例＞
S：戦略（Strategic）
T：戦術（Tactical）
P：手続き（Procedural）

捜査マネジメント – サイバー犯罪とその捜査に関する手順と方針、捜査対象となっているサイバー犯罪の種類を戦略的に理解する必要がある。これには、犯罪の実行（または目的達成）段階における、関連目標、スコープ、証拠の情報源に対する理解を含む。捜査マネジメントの機能は、組織に対してサイバー犯罪の特性と種類を説明する。捜査マネジメントの機能は方針、手順、計画を策定し、（人的、その他の）資源とその継続的な開発をマネジメントすべきである。

知見収集 – 利用できる証拠の情報源を駆使し、サイバー犯罪のスコープと影響を戦術的に理解し、その手順についても理解する。調査、説明責任、予防啓発、捜査マネジメントの各機能にある者が、被害者が（証拠から、または情報・市場心理の分析から見て）どのようなリスクにさらされているのかを理解するのを支援する。知見収集は、入手可能な証拠に基づいてサイバー犯罪の性質、範囲、目的を判断するための重要な情報源である。知見収集スタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

調査 – 入手可能な情報源のアーティファクトと証拠に基づいて、サイバー犯罪の範囲と影響について戦術的および手順的な理解を必要とする。この機能は、関連する目標の評価された性質（および達成段階）に従ってサイバー犯罪の影響を評価する諜報、司法、広報、および経営の役割を支援する。調査スタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

説明責任 – 捜査プロセスにおける法的・手続き的な許容度と限界を戦略的に理解する必要がある。この機能は、法律、規制、および関連ポリシーに従って情報収集、調査手順、分析結果の解釈を指導することにより、経営および広報の役割を支援する。規制や法律に関する指針は、情報の共有に対する制限や罰則を規定する。シニアスタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

予防啓発 – サイバー犯罪の種類と目標、プロファイル、構造に加え、自らの組織を戦略的に理解する必要がある。また、予防啓発の機能は、責任ある開示を行うために、情報共有を行う場所や手段を戦術的に理解しなければならない。捜査と分析を通じて判明したサイバー犯罪のスコープに応じて、方針に基づきながら、また、どの組織・職務・人員が影響を受けるのかを考慮しながら、何を、だれに、いつ、伝えるのかを決定する。シニアスタッフは手順を理解し、組織の方針に従うべきである。シニアスタッフは、スキルと知識の開発についてジュニアスタッフを支援すべきである。

後方支援 – 情報収集と捜査活動を支援するため、サイバー犯罪の捜査範囲と方法について手続き上の理解を必要とする。

総務人事 – 証拠を収集および分析するために、手順の理解、調査の意図、組織能力を必要とする。

第11章:レビュー

1. **保護が必要な資産はどのように特定すべきか**
   答え：資産分類。
   例：ツリー構造を使って資産を分類する。

2. **リスクシナリオを定義する責任者は誰か**
   答え：第1ライン／ビジネス部門（個人）、第2ライン／セキュリティ専門家（共通）。
   例：フォルトツリー分析または影響の木分析（インシデント発生後）の使用を通じて。

3. **リスクマネジメントの有効性はどのように測定すべきか**
   答え：定性的評価。
   例：リスクマトリックスアプローチ。

4. **リスク低減に必要な投資レベルはどのように決定されるのか**
   答え：ALARP。
   例：費用便益分析（CBA）を利用する。

5. **リスクシナリオの再評価の一般的なトリガーは何か**
   答え：リスクレベルを変えるもの。
   例：リスク影響（CIAの観点での）の変化、セキュリティインシデント、脆弱性、組織または役割の変更、システムの変更、業務運営の変更、法的要求・監督官庁による規制などの変更。

6. **リスク評価の結果はいつ経営陣に報告すべきか**
   答え：少なくとも四半期ごと、できれば毎月の頻度で。
   例：CISOがビジネスニーズに合わせたセキュリティKPIを採用し、取締役会がリスクマネジメントの意思決定を評価できるように支援する（リスクガバナンス）。

ケーススタディ11:インサイダーデータ盗難

- **犯罪**：データ窃盗、企業スパイ
- **容疑者**：従業員
- **手段**：許可されたアクセスの不正使用
- **動機**：個人的な利益
- **機会**：不十分な資産セキュリティ

大手製薬会社の上級研究科学者が、競合他社からのオファーを受け入れることにした。製薬研究開発の幅広い経験を持つ彼は、処方、FDA（アメリカ食品医薬品局）申請、助成金情報など、雇用主の成功に不可欠な機密情報や専有情報にアクセスできた。同僚の支援を受けながらも彼の退職は不吉な方向へと進み、会社は企業スパイ活動の影響と格闘することになった。

競合企業への入社を決意した研究者は、一連の行動を起こし、企業の機密保持および倫理基準に重大な違反を犯した。正式に辞職を発表する前の2か月間、研究者は専有文書にアクセスし、個人のクラウドストレージアカウントに転送した。その情報は下記のものを含んでいた。

- 開発中の詳細な医薬品処方。
- 彼の雇用主の市場戦略にとって重要なFDAへの申請内容。
- 助成金情報と研究データ。

さらに、彼は、機密事項の議論や戦略計画を含む数百件の社内メールを仕事用アカウントから個人用メールに転送していた。これらのメールには、共同作業での議論、会議メモ、独自の研究目的やビジネス戦略を明かす機密文書が含まれていた。これらの活動を調査した結果、下記のことが明らかになった。

1. **機密文書へのアクセス**：彼は自分の認証情報を使用して、数週間にわたって機密情報を体系的に収集した。データマネジメントが不十分だったため、彼の認証情報によって組織全体の情報に無制限にアクセスできた。
2. **個人用クラウドストレージへのデータ転送**：彼は仕事用のラップトップを使用して機密文書を個人用クラウドストレージアカウントにアップロードし、どこからでもアクセスできる雇用主の専有情報のリポジトリを作成した。
3. **メール転送**：彼は何百通もの仕事関連のメールを自分の個人用メールアカウントに転送した。この行為は、文書だけでなく重要な社内の議論や計画も含まれていたため、特に損害が大きかった。
4. **データ削除の試み**：会社支給のラップトップを返却する前に、彼は自分の痕跡を隠そうとした。彼は自分の閲覧履歴を削除し、無料のデータ消去ソフトウェアを使用して自分のユーザー履歴を消去し、自分の活動の証拠を消そうとした。

雇用主のIT部門は、通常の人事プロトコルを使用して、研究科学者が会社を去る最後の数日間に記録したデータ使用ログに異常を発見した。これらの活動に疑いを持ったチームは、外部コンサルタントの支援を受けて徹底的なフォレンジック調査を実施し、彼の行動の範囲を明らかにした。

フォレンジック分析結果:

- **削除されたデータの復元**：彼の努力にもかかわらず、IT チームは削除されたファイルを正常に復元し、外部ソースへの大量のデータ転送を示すログを取得した。
- **クラウドストレージアクセスの検出**：ログには、外部クラウドストレージサービスに繰り返しアクセスしたことが示されており、データ流出の時系列と一致していた。また、企業のクラウドデータアクセスログを調査したところ、移籍先の競合他社に関連することが判明した IP アドレスから情報をダウンロードするために、彼の認証情報が使用された追加のデバイスについても記載されていた。
- **電子メール転送パターン**：電子メールサーバーのログには、彼の個人アカウントへの電子メールの不審な転送パターンが示されていた。

元従業員の行為は、倫理基準および契約上の守秘義務に対する重大な違反にあたる。このような行為は、以下の重大な法的影響を及ぼす。

1. **秘密保持契約（NDA）違反**：従業員の行為は、秘密情報を権限のない第三者に転送または開示することを明確に禁じている NDA および雇用契約に直接違反していた。
2. **企業スパイ活動**：雇用主の競争力を弱める組織的な試みとして競合他社に独占情報を故意に転送することは、企業スパイ活動に該当し、厳しい法的罰則が科せられる。
3. **知的財産権侵害**：医薬品の処方と FDA 申請書類を流用することで、会社の研究開発努力による独自の創作物を保護することを目的とした知的財産法に違反した。

元研究者の行動によってもたらされたかなりのリスクに直面して、会社はいくつか対応を開始した。

- **即時の法的措置**：会社は、契約違反、コンピュータ詐欺および不正使用、企業スパイ、知的財産窃盗の罪で元従業員に対して法的救済を求めた。これには、盗まれた情報を新しい雇用主が利用することを防ぐための差止命令を求めることも含まれていた。
- **セキュリティ対策の強化**：会社はデータアクセスプロトコルを見直して強化し、より厳格なアクセス制御、データ監視、多要素認証プロセスを導入して、将来の信頼の悪用を防止した。
- **規制当局への通知**：会社は関係する規制当局に違反を通知し、法的義務の遵守と、公衆衛生および市場慣行への潜在的な影響の報告における透明性を確保した。

この事例は、特に従業員の異動時に企業の機密情報を保護することの重要性を強調している。これは、企業スパイや内部脅威に関連するリスクを軽減するために、組織が堅牢なセキュリティプロトコル、継続的な監視、迅速な対応を通じて警戒を維持する必要があることを強く警告するものである。

付録

主要な用語と定義

Access controls—Measures that establish privileges, determine authorized access, and prevent unauthorized access.

Active digital footprint—Created by data provided by the user of a computing device or application.

Advanced fee fraud—A computer-related fraud involving a request for an advance fee to complete a transfer, deposit or other transaction in exchange for a larger sum of money.

Advanced persistent threats (APTs)—Individuals and/or groups that persistently target an entity.

Anonymity—The shielding of one's identity to enable individuals to engage in activities without revealing themselves and/or their actions to others.

Anonymizers—These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as anonymous proxy servers.

Anonymous proxy servers—These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as anonymizers.

Anti-digital forensics—Tools and techniques used to obfuscate cybercrime investigation and digital forensics efforts. Also known as antiforensics.

Appellations of origin—Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as geographical indications.

Application and file analysis—Type of analysis that is performed to examine applications and files on a computer system to determine the perpetrator's knowledge of and intent and capabilities to commit cybercrime.

Artifacts—traces and clues that reflect the planning, organization, conduct, and commission of cybercrime.

Asset—Something that is considered important and/or valuable.

Attribution—The determination of who and/or what is responsible for a cybercrime.

Attribution profiles—information about criminals or the preliminary groups from which they are recruited.

Automation—the use of computers to perform analysis on data of such volume that it cannot be performed manually, using a variety of analytical frameworks, and to carry out analysis from different viewpoints.

Availability—Data, services, and systems are accessible on demand.

Backdoor—A secret portal used to gain unauthorized access to systems.

Back-tracing—The process of tracing illicit acts back to the source of the cybercrime. Also known as traceback.

Best evidence—The original piece of evidence or an accurate duplicate of the original.

Big data—large volumes of structured and unstructured data that can be consolidated and analyzed to reveal information about associations, patterns, and trends.

Black-Hat hackers—hackers that gain unauthorized access in order to steal credit card numbers or Personally Identifiable Information (PII) for identity theft; seek personal gain, financial or otherwise, and to raise havoc in some cases; use DDoS attacks and code malware; and are very skilled in hacker techniques and getting past security systems in networks.

Botherder—Controller of bot-infected digital devices.

Botnet—a group or network of bots under the control of the same attacker.

Bot—type of malware that an attacker can use to control an infected computer or mobile device.

Brute force attack—The use of a script or bot to guess user credentials.

Bulletproof hosting—A service that enables criminals to utilize servers to commit cybercrime, store illicit content, and protect illicit content from being accessed by law enforcement authorities and/or being taken offline.

Business continuity plan—Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as emergency management plan.

Catphishing—False or misleading promises of love and companionship designed to scam individuals out of their time, money and/or other items.

Censorship—The prohibition of information, visual depictions, and written or oral communications that are prohibited by law and/or their suppression by a government, community, or group because they are unlawful and/or viewed as harmful, unpopular, undesirable, or politically incorrect.

Chain of custody—A detailed log about the evidence, the condition of the evidence, its collection, storage, access, and transfer and reasons for its access and transfer, is essential to ensure the admissibility of digital evidence in most courts of law.

Child grooming—Enticement of children or solicitation of children for sexual purposes.

Child sex trafficking—Acting in some manner that recruits, leads, causes, maintains, and/or otherwise facilitates the commercial sexual exploitation of children.

Child sexual abuse material (CSAM) —The representation of child sexual abuse and/or other sexualized acts using children.

Child sexual abuse to order—Viewers of child sexual abuse can be actively involved in abuse by communicating with the child, the sexual abuser, and/or facilitator of the child sexual abuse and requesting specific physical acts and/or sexual acts to be performed on and/or performed by the child.

Circumstantial evidence—Evidence that infers the truth of a matter.

Clearnet—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Surface Web or Visible Web.

Clou—internet hosted servers that provide virtualized computing and storage services and resources.

Code of ethics—Guidelines covering right and wrong conduct to inform decision-making.

Collected evidence—the collection of a foundation to identify an individual or organization that has committed a wrongful act or participated in the act.

Commercial sexual exploitation of children—A term used to describe a range of activities and crimes that involve the sexual abuse of children for some kind of remuneration of any monetary or non-monetary value.

Computer data—Any form of representation of information that is processed by a system of a digital device. Also known as computer information or data.

Computer Emergency Response Team—A team that provides support for cybersecurity incidents. Also known as Computer Security Incident Response Team.

Computer information—Any form of representation of information that is processed by a system of a digital device. Also known as computer data or data.

Computer network—Two or more computers that send and receive data between them.

Computer Security Incident Response Team (CSIRT) —A team that provides support for cybersecurity incidents. Also known as Computer Emergency Response Team.

Computer system—A stand-alone or networked device that performs data processing among other functions.

Confidentiality—Systems, networks, and data are protected, and only authorized users can access them.

Confirmation bias—The process whereby individuals look for and support results that support their working hypothesis and dismiss results that conflict with their working hypothesis.

Content data—Words in written communications or spoken words.

Coordinated vulnerability disclosure—The practice of harmonized information sharing and disclosure of vulnerabilities to relevant stakeholders along with the tactics used for its mitigation.

Copyrights—Creative products, such as artistic and literary works, protected by law.

Crime displacement—When a crime that was intended for one target is committed on another target because of security measures in place.

Crime reconstruction—This process seeks to determine who was responsible for the crime, what happened, where did the crime occur, when did the crime take place, and how the crime unfolded, through the identification, collation, and linkage of data. Also known as event reconstruction.

Crime scene indicators—elements that comprise a crime scene.

Crimeware—general term for software created or used for criminal acts.

Critical infrastructure—Designated essential sectors that are considered fundamental to the proper functioning of society.

Cryptocurrency—A form of digital currency secured utilizing advanced encryption.

Cryptomarkets—A website utilizing cryptography to protect users of the site.

Crytopjacking—A tactic whereby the processing power of infected computers is used to mine cryptocurrency for the financial benefit of the person (or persons) controlling the bot-infected digital devices.

Cyber organized crime—A term used to describe a continuing criminal enterprise that rationally works to profit from illicit activities that are in demand online.

Cyber organized criminals—A structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the United Nations Convention against Transnational Organized Crime of 2000, which operate in whole or in part online, in order to obtain, directly or indirectly, a financial or other material benefit.

Cyber proxies—The use of intermediaries to contribute directly or indirectly to a cyber dependent crime intentionally targeting a state.

Cyberbullying—The use of information and communication technology by children to annoy, humiliate, insult, offend, harass, alarm, stalk, abuse or otherwise attack another child or children.

Cybercrime investigations—acts involving the discovery and preservation, and collection and securing of evidence to file and maintain a prosecution when a crime is deemed to have taken place in cyberspace.

Cybercrime taxonomy—the systematic classification and organization of entire areas regarding the knowledge, skills and approaches that must be commonly mastered in the implementation of cybercrime investigations.

Cybercrime—acts involving cyber space (including computers, computer software, computer networks, or embedded software controlling systems) that violate various strongly defined norms in society's collective consciousness.

Cyber-dependent crime—A cybercrime that would not be possible without the Internet and digital technologies.

Cyber-enabled crimes—A cybercrime facilitated by the Internet and digital technologies.

Cyberespionage—The use of information and communication technology by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national security, economic competitiveness, and/or military strength.

Cyberharassment—The use of information and communication technology to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse an individual (or individuals).

Cybersecurity—The collection of strategies, frameworks, and measures that are designed to identify threats and vulnerabilities of systems, networks, services, and data to these threats; prevent the exploitation of vulnerabilities; mitigate the harm caused by materialized threats; and safeguard people, property, and information and communication technology.

Cybersecurity posture—A term used to describe the cybersecurity capabilities of a country, organization or business.

Cybersmearing—Posting or otherwise distributing of false information or rumours about an adult or child to damage the victim's social standing, interpersonal relationships, and/or reputation.

Cyberspace—An environment accessed by Internet-enabled digital technology within which online activities take place.

Cyberstalking—The use of information and communication technology to commit a series of acts over a period of time designed to harass, annoy, attack, threaten, frighten, and/or verbally abuse an individual (or individuals).

Cyberterrorism—The cyber-dependent crimes perpetrated against critical infrastructure to cause some form of harm and to provoke fear in the target population.

Cyberwarfare—Cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack.

Dark Web—The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as darknet.

Darknet—The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as Dark Web.

Data—Any form of representation of information that is processed by a system of a digital device. Also known as computer data or computer information.

Data hiding analysis—Type of analysis that searches for hidden data on a system.

Data mining—The retrieval of information from data sets.

Data modeling—the technique of organizing data (targeted items and events) on the basis of consistent rules.

Data preservation—Requests are made to service providers by law enforcement in an effort to retain data before it is deleted or altered in any way.

Data protection—The safeguarding of personal information and regulates its collection, storage, analysis, use, and sharing.

Data protection by design—Privacy measures embedded in the design of systems and technologies. Also known as privacy by design.

Data quality testing—putting the results of criminal investigation under scrutiny and measuring to assess their appropriateness.

Data warehouse—a large scale database for storing data extracted and rebuilt from multiple information sources that is used for information analysis and decision-making.

Deep Web—The part of the World Wide Web that is not indexed by search engines and is not easily accessible and/or available to the public.

Denial of service (DOS) attack—A cybercrime that interferes with systems by overwhelming servers with requests to prevent legitimate traffic from accessing a site and/or using a system.

Design patents—A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as industrial designs.

Deterrence—Discouraging illicit activity through punishment.

Digital evidence—Data obtained from information and communication technology. Also known as electronic evidence.

Digital footprint—Data left behind by ICT users that can reveal information about them, including age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history and concerns, psychological disorders, employment status, affiliations, relationships, geolocation, routines, and other activities.

Digital forensic process—The search, retrieval, preservation, and maintenance of digital evidence; description, explanation and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability and relevance to the case; and the reporting of evidence pertinent to the case.

Digital forensics—A branch of forensic science that applies matters of law to information and communication technology and digital evidence.

Digital piracy—The illegal download of a movie from a third-party website that does not have the right to distribute the copyrighted work.

Direct evidence—Evidence that establishes a fact.

Disinformation—The deliberate spreading of false information.

Disinhibition—The process whereby an individual demonstrates a lack of social restraint with regards to online behavior.

Dissociative anonymity—Individuals' detachment of their online behavior from their offline behavior due to the anonymity afforded to them when utilizing the Internet and digital technology.

Dissociative imagination—Individuals' view of cyberspace as a forum within which the rules of everyday interactions, codes of conduct, social norms, and/or laws do not apply, disinhibiting the individual to act in a manner contrary to offline rules of everyday interactions, codes of conduct, social norms, and/or laws.

Distributed Denial of Service (DDoS) attack—The use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers to prevent legitimate users' access.

Dogpiling—A tactic whereby users within an online space bombard victims with offensive, insulting, and threatening messages to silence the target, force them to take back what they said and/or apologize, or to force them to leave the platform.

Domain name—A pseudonymous representation of an IP address in an Internet (or web) browser.

Domain Name System (DNS)—Enables Internet access by translating domain names to IP address.

Doxing—Personal information about individuals posted online to cause the individual some form of harm.

Doxware—A form ransomware that perpetrators use against victims that releases the user's data if ransom is not paid to decrypt the files and data.

Dual criminality—A clause in treaties requiring acts to be considered illegal in cooperating countries.

Electoral fraud—The use of unlawful tactics to influence elections.

Electronic Discovery (eDiscovery)—The process of searching, identifying, and preserving digital data for use as evidence in a legal proceeding.

Electronic evidence—Data obtained from information and communication technology. Also known as digital evidence.

Emergency management plan—Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as business continuity plan.

Encryption—Measure that blocks third party access to users' information and communications by encoding data using a factorial method.

Event reconstruction—This process seeks to determine who was responsible for the event, what happened, where did the event occur, when did the event take place, and how the event unfolded, through the identification, collation, and linkage of data. Also known as crime reconstruction.

Expected utility theory—A theory that holds that people engage in actions when the expected utility from these actions is higher than the expected utility of engaging in other actions.

Fake news—Propaganda and disinformation masquerading as real news.

Fifth domain—A term used to describe cyberspace as another domain of warfare.

File carving—Search based on content identifiers.

Firewall—A security measure that restricts the free flow of information by blocking unauthorized network traffic data.

First responders—Individuals who respond first to the scene and are responsible for securing evidence at the scene.

Forensic relevance—The relevance of forensic data is determined by whether the digital evidence: links or rules out a connection between the perpetrator and the target and/or the crime scene; supports or refutes perpetrator, victim and/or witness testimony; identifies the perpetrator (s) of the cybercrime; provides investigate leads; provides information about the method of operation of the perpetrator; and shows that a crime has taken place.

Forensic—scientific tests or techniques used in the detection of crime.

Full vulnerability disclosure—Publicly publishing the software or hardware vulnerability through online forums and websites before a fix is available.

Functional analysis—The assessment of the performance and capabilities of systems and devices involved in events.

General deterrence—Punishment designed to send the message to others that similar illicit behavior will receive similar severe punishment.

Geographical indications—Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as appellations of origin.

Gray-Hat hackers—hackers in the middle ground between White-Hat and Black-Hat hackers; computer experts who may hack into a system without the knowledge or consent of the owner but lack malicious or evil intent; they may report security issues that they find to a public forum as opposed to the site owner directly.

Hacking—Unauthorized access to systems, networks, and data.

Hard drive—An internal, persistent memory in a computer.

Hash—A calculated cryptographic value used to identify evidence.

Hearsay—Out of court statements.

Human flesh search engine—A term used to describe online users work together to identify a target and perpetrate coordinated online abuse against the target.

Identity management—The process of authenticating users' identities, identifying associated privileges, and granting user access based on these privileges.

Identity-related crime—A perpetrator unlawfully assumes and/or misappropriates the identity of the victim and/or uses the identity and/or information associated with the identity for illicit purposes.

Image-based sexual abuse—A form of sexual violence whereby sexually explicit images and/or videos of the victims are intentionally created, distributed, or threatened to be distributed without the consent of the victims. This may be to cause some form of harm to the victim and/or to benefit the perpetrator in some way (e.g. monetary gain, sexual gratification, social status building and more).

Imaging—Creating a duplicate copy of the content of the digital device.

Impact analysis—consists of information about victims and the scope of cybercrime as indicated by the number of systems, users, etc. that were accessed or used without authorization.

Incident detection—The process of identifying threats by actively monitoring assets and finding anomalous activity.

Industrial control systems—Systems that command and control critical infrastructure processes.

Industrial designs—A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as design patents.

Information warfare—The collection, distribution, modification, disruption, interference with, corruption, and degradation of information to gain some advantage over an adversary.

Inoculation theory—This theory holds that the way to inoculate individuals from persuasion attempts of others is to expose them to these attempts and given them tools they need to resist these attempts.

Insider Threat—employees, contractors, consultants, or partners who have access and use of internal information technology and services resources and exhibit inappropriate or malicious behaviors.

Integrity—Data is accurate and trustworthy and has not been modified.

Intellectual property (IP) —Products of creativity, such as works, innovations, creations, original expression of ideas, and secret business practices and processes, that individuals have rights to as prescribed by law.

Internet governance—The creation and application of Internet principles, rules, and procedures by various stakeholders to guide the use of the Internet and shape its development.

Internet of Things (IoT)—an evolving, rapidly expanding network of internet-enabled devices that can

communicate with each other and function electronically in a variety of ways impacting daily life.

Internet penetration rate—The portion of the population in an area that uses the Internet.

Internet Protocol address (IP address)—A unique identifier assigned by an Internet service provider to an Internet-connected digital device to connect to the Internet.

Internet service provider (ISP)—Provides Internet services to a computer system or a system of another digital device.

Internet trolls—Individuals that purposely post rude, aggressive, and offensive remarks designed to create discord and discontent online.

Interpersonal cybercrime—Cybercrimes committed by individuals against other individuals with whom they are interacting, communicating, and/or having some form of real or imagined relationship.

Intrusion detection systems (IDS)—A cybersecurity measure that enables the detection of cyberattacks and unauthorized access and use of systems, networks, data, services, and related resources.

Jurisdiction—A state's power and authority to enforce laws and punish non-compliance with laws.

Key performance indicators (KPIs)—Measures that are used to determine progress towards the realization of the strategic objectives of the national cybersecurity strategy.

Keyword searches—Search based on terms provided by the investigator.

Knowledge management—The process of identification and assessment of knowledge needs and the utilization of knowledge assets.

Letters rogatory—Written requests from national courts for evidence from a foreign country.

Logical extraction—The search for and acquisition of evidence from the file system location.

Malware—malicious software used to infect computer systems and automatically execute its routine; includes terms such as viruses, Trojans, worms, spyware, and ransomware.

Memory resident malware—unique malware that leaves no files on the hard disk to indicate it has been used to facilitate cybercrimes, making traditional detection and mitigation much more difficult.

Metadata—information about data; attributes of files and their relationship to users or operating system and storage/device configurations.

Microlaundering—A form of money-laundering whereby the perpetrators launder a significant amount of money through multiple small transactions.

Misinformation—False or inaccurate information.

Missing data—inconsistent data resulting from the value of a certain item in a certain case being missing.

Money mules—Individuals who either knowingly or unknowingly commit crimes and/or cybercrimes by obtaining and transferring illicit goods, engaging in illicit services, and/or illegally receiving or transferring money for others for remuneration.

Money-laundering—The concealment of illicit proceeds through a combination of legitimate and illegitimate transactions.

Morphing—A victim's face or head superimposed on the bodies of others for the purpose of defamation, pornography, and/or sexual abuse.

Mutual legal assistance treaty (MLAT)—An agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences proscribed by both parties under national law.

Net neutrality—Requires all data, irrespective of source, to be treated equally.

Neutralization techniques—Techniques used to overcome or minimize negative emotions associated with the engagement in illicit activity.

Non-content data—Data about the content. Also known as metadata.

Online child sexual abuse—The use of information and communication technology as a means to sexually abuse children.

Online child sexual exploitation—The use of information and communication technology as a means to sexually exploit children, where child sexual abuse and/or other sexualized acts using children involve an exchange of some kind.

Online impersonation—The impersonation of victims by creating accounts with similar names and, by making use of existing images of the victims.

Organized crime—A continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand.

Ownership and possession analysis—Type of analysis that is used to determine the person who created, accessed, and/or modified files on a computer system.

Passive digital footprint—Data that is obtained and unintentionally left behind by the users of the Internet and digital technology.

Patent—Exclusive right granted for an invention (innovation or creation), which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem.

Patent trolls—These individuals neither create nor invent anything; they merely purchase patents to license them to others, and sue any person, group, or organization infringing their acquired patents.

Pedophile—A person sexually interested in children.

Personal autonomy—The ability to make choices and act in ways of their own choosing free from coercion.

Pharming—The creation of a fake, duplicate website that is designed to trick users to input their login credentials.

Phishing—The sending of an email to targets with a website link for users to click on, which might either download malware onto the users' digital devices or sends users to a malicious website that is designed to steal users' credentials.

Physical extraction—The search for and acquisition of evidence from the location within a digital device where the evidence resides.

Preventive law—Legal rules that focus on regulation of risk and seek to prevent crime or at the very least mitigate the damage that could be caused in the event of a crime.

Privacy—The right to be left alone and be free from observation; the capacity to keep one's thoughts, beliefs, identity, and behavior secret; and the right to choose and control when, what, why, where, how, and to whom information about oneself is revealed and to what extent information is revealed.

Privacy by design—Privacy measures embedded in the design of systems and technologies. Also known as data protection by design.

Procedural law—Legal rules that cover the processes and procedures to be followed to apply substantive law, the rules to enable the enforcement of substantive law, and the rules and standards in criminal justice proceedings.

Proxy server—An intermediary server that is used to connect a client with a server that the client is requesting resources from.

Pseudonymization—The process whereby identifying data in a record is replaced by artificial identifiers.

Quality assurance and control—the process whereby, in relation to an analytical framework, an experienced and skilled person, by giving guidance and advice, can guarantee the quality of the final output.

Ransomware—Malware designed to take users' system, files, and/or data hostage and relinquish control back to the user only after ransom is paid.

Recovery—The identification, creation, and ultimate implementation of measures for resilience and the restoration of systems, networks, services, and data that were unavailable, harmed, damaged, and/or compromised during the incident.

Relational analysis—The determination of the individuals involved and what they did, and the association and relationships between these individuals.

Resilience—The ability to withstand disruptions, adapt to changing conditions, and recover from incidents of ICT and protect the confidentiality, integrity, and availability of systems, networks, services, and data.

Responsible vulnerability disclosure—The practice of not disclosing the vulnerability until a fix is provided by the responsible organization.

Revenge porn—when a revengeful partner publishes nonconsensual pornographic photos and videos on the Internet of their former partner.

Risk—The impact of a threat and its probability of occurring.

Risk assessment—The evaluation of the probability of a threat, its impact, and the exposure of an asset to this threat.

Risk treatment—Responses to risks.

Roasting—Individuals willingly posting images and/or videos of themselves on online and inviting others to post insults about them.

Rootkit—software that will modify the operating system of a victim computer and replace key functions with its own functionality in order to maintain a stealthy presence and remain undetected.

Routine activity theory—A theory that holds that crime occurs when two elements are present - a motivated offender and a suitable target, and one element is absent—a capable guardian.

Scope of cybercrime—the scale of cybercrime organizations as well as the scope of victims or their associated computers.

Script—A computer program.

Service provider—Provides services to a computer system or a system of another digital device.

Sexting—Self-generated sexually explicit material.

Sexting—sending sexually explicit photos of oneself to others.

Sextortion—A form of cyberharassment whereby the victim is threatened with the release of sexually explicit content if the demands of the perpetrator are not met.

Situational crime prevention—Measures used to prevent and reduce crime.

Smishing—Phishing via text messaging. Also known as SMS phishing.

SMS phishing—Phishing via text messaging. Also known as smishing.

Social dilemma—When individuals' decisions are based on self-interest rather than the interest of the group or collective, even when the utility of engaging in the collective interest is higher than the utility of engaging in self-interest.

Social engineering—A tactic whereby a perpetrator tricks the target into divulging information or performing another action.

Social engineering fraud—Tricking the victim into revealing or otherwise providing personal information and/or funds to the perpetrator.

Solipsistic introjection—The fictional image of others created by users' perceptions of others and their traits absent contextual data, including the relationships they have with them based on imagined rather than real information.

Sovereignty—A country's right to exercise authority over its own territory.

Spam—Sending of unsolicited emails.

Spearphishing—The sending of emails with infected attachments or links that are designed to dupe the receiver into clicking on the attachments or links.

Specific deterrence—Punishing individuals who commit crime to cease further illicit activity if the punishment received outweighs the benefits of committing the crime.

Spyware—Malware designed to surreptitiously monitor infected systems and collect and relay information back to creator and/or user of the spyware.

Stalkerware—A form of spyware that can run on a victim's computer, smartphone or other Internet-enabled digital device and collect and relay all the user's actions on these devices, from emails and text messages sent and received, to photographs taken and keystrokes.

Standard operating procedures—Documents that include the policies and sequential acts that should be followed to investigate cybercrime and handle digital evidence on information and communication technology.

Steganography—The stealthy concealment of data by both hiding content and making it invisible.

Substantive law—Legal rules that govern behaviour and responsibilities of those over whom the state has jurisdiction.

Surface Web—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Clearnet or Visible Web.

Swappers—Semiautomated cryptocurrency exchanges.

Temporal analysis—The determination of the time events occurred and the sequence of these events.

Territorial sovereignty—The state's complete and exclusive exercise of authority and power over its geographic territory.

Terrorism—threats or violent acts against people or property to affect government policy or political, religious, or ideological change.

Threat—A circumstance that could cause harm.

Threat actors—cyber criminals who give rise to threats to enterprises and organizations.

Threat profile—comprises a crime scenario, the threat actors, and information about the threat.

Time-frame analysis—Type of analysis that seeks to create a timeline or time sequence of actions using time stamps that led to an event or to determine the time and date a user performed some action.

Traceback—The process of tracing illicit acts back to the source of the cybercrime. Also known as back-tracing.

Trade secret theft—The theft of a trade secret offline and/or online to gain an unfair competitive advantage.

Trade secrets—Valuable information about business processes and practices that are secret and

protect the business' competitive advantage.

Trademark counterfeiting—Intentional unauthorized use of a trademark to label good or service that does not originate from the trademark owner.

Trademarks—Identifiers that distinguish the source of a good or service.

Traffic data—Data transmitted over a computer network (or network).

Trojan horse—Malware designed to look like legitimate software in order to trick the user into downloading the program, which infects the users' system to spy, steal and/or cause harm.

Unallocated space—Space that is available for use because content was deleted, or space was never used.

Usability—Ease with which digital devices can be used.

Victimology—profile information related to the victim.

Virus—Malware that requires user activity to spread.

Vishing—Phishing via telecommunications.

Visible Web—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Clearnet or Surface Web.

Vulnerability—Exposure to harm.

Watering-hole attack—Placing malware on the most frequented websites of targets to ultimately infect their systems and gain unauthorized access to them.

Web crawlers—Applications designed to traverse the World Wide Web to achieve specific objectives.

Whaling—Pretending to be higher level executives in a company, lawyers, accountants, and others in positions of authority and trust, in order to trick employees into sending them funds.

White-Hat (or ethical) hackers—hackers who break into systems to test their skills and to figure out how security programs work; professionals who have been authorized by an organization to compromise its network, report any security issues, and make recommendations on how to fix them.

Worm—Stand-alone malicious software that spreads without the need for user activity.

Write blocker—Designed to prevent the alteration of data during the copying process.

Zero day—Previously unknown vulnerability that is exploited once identified.

参考書目

#mum cryptolabs. (2004, September 25). On the 2ROT13 Encryption Algorithm. Retrieved from http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf

114th U.S. Congress, Senate Bill 754, Cybersecurity Information Sharing Act of 2015. (2015, October 28). Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/754/text

ACCESSDATA Forensic Toolkit (FTK). (2016). Retrieved from http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

ACCESSDATA. (n.d.). Network investigation and incident response. Retrieved from http://accessdata.com/solutions/digital-forensics/ad-enterprise

AJMartel. (2016, April 21). IRTriage. GitHub. Retrieved from https://github.com/AJMartel/IRTriage

Akerlof, G. and Shiller, R. 2015. Phishing for phools. In Phishing for Phools. Princeton University Press.

Apache License 2.0. (n.d.). Retrieved from https://tldrlegal.com/license/apache-license-2.0- (apache-2.0)

Archambeault, William O. and Betty J. Archambeault. Computers in Criminal Justice Administration and Management: Introduction to Emerging Issues and Applications. Cincinnati: Anderson Publishing Co., 1984.

Arkin, Stanley, et al. Prevention and Prosecution of Computer and High Technology Crime. New York: Matthew Bender and Co., 1988.

Ashford, W. (2015, September 15). Most DDoS attacks hiding something more sinister, Neustar warns.

Associated Press. (1998, July 11). Man who threatened gates sentenced to prison - Extortion letter told

ATT&CK. 2015. MITRE ATT&CK. MITRE. Retrieved from https://attack.mitre.org/

Autopsy. (2016). Retrieved from http://www.sleuthkit.org/autopsy

Barta, C. (2011, December). NTDS.DIT forensics. Retrieved from http://ntdsxtract.com/downloads/ntdsxtract/ntds_forensics.pdf

Barufaldi, D. (n.d.). Hedge funds: Strategies. Investopedia. Retrieved from http://www.investopedia.com/university/hedge-fund/strategies.asp

Bash, K. (2015, May 5). PowerShell DSC for Linux is now available! [Blog post]. Retrieved from https://blogs.msdn.microsoft.com/powershell/2015/05/05/powershell-dsc-for-linux-is-now-available/

BatBlue. (n.d.). The Darknet – The underground for the underground. Retrieved from http://www.batblue.com/the-darknet/

Bequai, August. Computer Crime. Lexington, MA: Lexington Books, 1978.

Bequai, August. How to Prevent Computer Crime: A Guide For Managers. New York: John Wiley and Sons, 1983.

Bequai, August. Technocrimes. Lexington, MA: Lexington Books, 1987.

Bequai, August. Technocrimes-The Computerization of Crime and Terrorism. Lexington, MA: Lexington Books, 1986.

Bequai, August. "Technocrimes-Why the Cops Can't Cope." Law Enforcement Technology. March/April 1987: 28.

Bequai, August. White Collar Crime. Lexington, MA: Lexington Books, 1977.

Boyd, J. (n.d.). Summary of OODA model. Retrieved from http://www.valuebasedmanagement.net/

methods_boyd_ooda_loop.html
Brezinski, D., Killalea, T. (2002, February). Guidelines for evidence collection and archiving. Retrieved from https://tools.ietf.org/html/rfc3227
BriMor Labs Tools. (2016). Retrieved from https://www.brimorlabs.com/tools/
British Standards Institution. (n.d.). Cyber security. Retrieved from http://www.bsigroup.com/en-GB/Cyber-Security/
Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8 (1), 1-20.
Bruneau, G. (2010). DNS Sinkhole. Retrieved from https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523
Carman, A. (2015, October, 6). Study: Average cost of cybercrime rises again in 2015 to $7.7 million. SC Magazine. Retrieved from http://www.scmagazine.com/ponemon-and-hp-release-annual-cybercrime-cost-study/article/443433/
CBS News. (2016, January 8). Former St. Louis Cardinals executive pleads guilty to hacking Houston Astros. Retrieved from http://www.cbsnews.com/news/former-st-louis-cardinals-executive-pleads-guilty-to-hacking-houston-astros
Centers for Disease Control and Prevention. (2016). About Zika: What we know. Retrieved from http://www.cdc.gov/zika/about/
Cisco Snort. (n.d.). Retrieved from http://www.snort.org
Cleveland, T. (n.d.). SEC terminates cyber-fraud ring that netted $100 million in CFD trading. Forex Fraud. Retrieved from http://www.forexfraud.com/forex-articles/sec-terminates-cyber-fraud-ring-that-netted-$100-millionin-cfd-trading.html
Cluley, G. (2016, July 28). Citibank IT guy deliberately wiped routers, shut down 90% of firm's networks across America. Tripwire. Retrieved from
http://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shutdown-90-of-firms-networks-across-america
clymb3r. (2015, September 30). PowerShell – Invoke-NinjaCopy. GitHub. Retrieved from https://github.com/clymb3r/PowerShell/tree/master/Invoke-NinjaCopy
Computer emergency response team. (n.d.). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Computer_emergency_response_team
Consumer Federation of America. (n.d.). Protect yourself from the "grandparent scam." Retrieved from http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf
Cottim, A. (2010). Cybercrime, cyberterrorism and jurisdiction: An analysis of Article 22 of the COE Convention on Cybercrime. European Journal of Legal Studies. Retrieved from http://www.ejls.eu/6/78UK.htm
Council of Europe. (2016). Action against cybercrime. Retrieved from http://www.coe.int/cybercrime
Council of Europe. (2016). Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
Council of Europe. (2016)., Details of Treaty No.185, Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
CounterTack Products. (2016). Retrieved from http://www.countertack.com/products
da667. (2015, November 2). Netstat. GitHub. Retrieved from https://github.com/da667/netstat/blob/

master/netstat.py

Danyliw, R. Meijer, J., Demchenko, Y. (2007, December). The incident object description exchange format. Retrieved from https://tools.ietf.org/html/rfc5070

Das, K. N., Spicer, J. (2016, July 21). How the New York Fed fumbled over the Bangladesh Bank cyber-heist. Reuters Investigates. Retrieved from http://www.reuters.com/investigates/special-report/cyber-heist-federal/

David, W. and Pattavina, A. 2005. The Internet as a conduit for criminal activity. In Information technology and the criminal justice system. Sage.

Deacon, B. W. (2015, September 20). The Darknet (Deep Web) explained. LinkedIn Pulse. Retrieved from https://www.linkedin.com/pulse/darknet-deep-web-explained-bradley-w-deacon

D3FEND. 2022. D3FEND™, A knowledge graph of cybersecurity countermeasures. MITRE. Retrieved from https://d3fend.mitre.org/

Delhi_Cybercrime_Unit. 2022. Custom fraud via social networking sites. Special Cybercrime Unit, India. Retrieved from https://cyber.delhipolice. gov.in/socialmediacrimes.html

destijl. (2016, November 20). GRR rapid response: Remote live forensics for incident response. GitHub. Retrieved from https://github.com/google/grr

Dethlefs, R. (2015, May 1). How cyber attacks became more profitable than the drug trade. Fortune. Retrieved from http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/

Directive (EU) 2016/680 of the European Parliament and of the Council. (2016, April 27). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

Doyle, C. (2014, October 15). Cybercrime: A sketch of 18 U.S.C. 1030 and related federal criminal laws. Washington, DC: Congressional Research Service, Library of Congress. Retrieved from https://www.fas.org/sgp/crs/misc/RS20830.pdf

Ducklin, P. (2013, Jan 27). Not-so anonymous Anonymouses head off to prison over PayPal DDoS. Naked Security. Retrieved from https://nakedsecurity.sophos.com/2013/01/27/not-so-anonymous-anonymouses-head-off-to-prisonover-paypal-ddos/

elastic Products. (2016). Retrieved from https://www.elastic.co/products Electronic Privacy Information Center. (2016). Electronic Communications Privacy Act (ECPA). Retrieved from https://epic.org/privacy/ecpa/

Europol's European Cybercrime Centre (EC3). (2015). Europol, Internet Organised Crime Threat Assessment (IOCTA) 2015. Retrieved from https://www.europol.europa.eu/iocta/2015/overview.html

Farivar, C. (2015, January 2). Come for lulz, stay for hacktivism: A new book on Anonymous, reviewed. Ars Technica. Retrieved from http://arstechnica.com/security/2015/01/come-for-the-lulz-stay-for-the-hacktivism-a-new-book-on-anonymous-reviewed/

Federal Bureau of Investigation. 2021. FBI Internet crime report 2021. Federal Bureau of Investigation. Retrieved from https://www.documentcloud.org/documents/21504639-fbi-internet-crime-report-2021

Federal Bureau of Investigation. (2010, October). Cyber theft ring [graphic]. Retrieved from https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-graphic

Federal Bureau of Investigation. (n.d.). Nigerian letter or "419" fraud. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud

Federal Bureau of Investigation. (n.d.). Uniform crime reporting. Retrieved from https://ucr.fbi.gov/

Federal Trade Commission. (2016, May 24). Marketers of "mosquito shield bands" to pay $300,000, barred from making misleading pest-control claims under settlement with FTC. Retrieved from https://www.ftc.gov/news-events/press-releases/2016/05/marketers-mosquito-shield-bands-pay-300000-barred-making

Federal Trade Commission. (n.d.). Cases tagged with data security. Retrieved from https://www.ftc.gov/enforcement/cases-proceedings/terms/249

Federal Trade Commission. (n.d.). Data security. Retrieved from https://www.ftc.gov/datasecurity

FEEBle Industries Forum. (n.d.). Retrieved from https://feeble-industries.com/forums/

Findings from Analysis of DNC intrusion malware. (2016, June 20). Retrieved from http://www.threatgeek.com/2016/06/dnc_update.html

Finkle, J. (2016, August 31). Exclusive: SWIFT discloses more cyberthefts, pressures banks on security. Reuters. Retrieved from http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C

Fitzpatrick, D., Griffin, D. (2016, April 4). "Ransomware" crime wave growing. CNNMoney. Retrieved from http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/

Flashpoint. (2016, June 2). Ransomware as a service: Inside an organized Russian ransomware campaign. Retrieved from https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf

ForensicsWiki – Hashing. (2009, May 5). Retrieved from http://www.forensicswiki.org/wiki/Hashing

Franceschi-Bicchierai, L. (2016, July 22). Ransomware gang claims Fortune 500 company hired them to hack the competition. Motherboard. Retrieved from http://motherboard.vice.com/read/ransomware-gang-claims-fortune-500-company-hired-them-to-hack-the-competition

F-Response. (n.d.). Retrieved from https://www.f-response.com

Frizell, S. (2014, December 2). Sony executives' salaries leaked in devastating hack. Time. Retrieved from http://time.com/3615160/sony-hack-salaries/

F-Secure. (2016). Evaluation the customer journey of crypto-ransomware and the paradox behind it. Retrieved from https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf

F-Secure. (n.d.). Botnets. Retrieved from https://www.f-secure.com/en/web/labs_global/botnets

Ganson, M. (2015, July 20). .vbs script for computing and displaying md5 hashes. Retrieved from http://mwganson.freeyellow.com/md5/md5.vbs

Germano, J. H. (2014). CyberSecurity partnerships: A new era of public-private collaboration. New York, NY: The Center on Law and Security, New York University School of Law. Retrieved from http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

gfoss. (2016, April 18). PSRecon. GitHub. Retrieved from https://github.com/gfoss/PSRecon/blob/master/psrecon.ps1

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Toronto, Ontario: Doubleday Canada.

Google hacking database (GHDB). (n.d.). Retrieved from https://www.exploit-db.com/google-hacking-

database/

Greene, T. (2015, Sep 17). Under DDoS attack? Look for something worse. Network World. Retrieved from http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html

Guidance Software EnCase Forensic. (n.d.). Retrieved from https://www.guidancesoftware.com/encase-forensic

Guidance Software. (n.d.). Retrieved from https://www.guidancesoftware.com/

Hacking tools: June 2013 [Blog post]. (2013, June) Retrieved from http://anonhacktivism.blogspot.com/2013/06/dos-tools-2.html

Handerhan, R. (2010). Japanese and American computer crime policy: A comparative study. Carnegie Mellon University Research Showcase. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1067&context=hsshonors

Harrell, C. (2013, September 12). Tools to grab locked files [Blog post]. Retrieved from http://journeyintoir.blogspot.com/2013/09/tools-to-grab-locked-files.html

Hern, A. (2016, August 3). Ransomware threat on the rise as "almost 40% of businesses attacked." The Guardian. Retrieved from https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

Holt, T. 2018. Regulating cybercrime through law enforcement and industry mechanisms. The ANNALS of the American Academy of Political and Social Science 679, 1 (2018).

Hutchins, E. M., Cloppert, M. J., Amin, R. M. (2014, April 3). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

IBM. 2022. X-Force Threat Intelligence Index 2022. International Business Machines Corporation (IBM). Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ

IC3. 2000. Internet Crime Complaint Center IC3. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/

IC4. 2022. National Cyber Crime Reporting Portal. Ministry of Home Affairs, India. Retrieved from https://cybercrime.gov.in/

InfraGard. (n.d.). Retrieved from https://www.infragard.org/

Internet Archive. (2014). Retrieved from https://archive.org/web/

Introduction to TAXII. (2012, November). Retrieved from https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

ISACA. (2013). COBIT 5 for risk. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-5-Risk_res_Eng_1213.ppt

ISACA. (2016). What is COBIT 5? Retrieved from http://www.isaca.org/cobit/pages/default.aspx

IT Governance. (n.d.). Business continuity, disaster recovery and ISO22301. Retrieved from http://www.itgovernance.co.uk/bc_dr.aspx

IT Governance. (n.d.). Cyber security risk assessments (10 steps to cyber security). Retrieved from http://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security.aspx

IT Governance. (n.d.). ISO/IEC 20000: The international standard for service management. Retrieved from http://www.itgovernance.co.uk/iso20000.aspx

IT Governance. (n.d.). ITIL – IT Infrastructure Library for IT Service Management (ITSM) – ITIL 2011. Retrieved from http://www.itgovernance.co.uk/itil.aspx

Japan Computer Emergency Response Team Coordination Center [English version]. (2016). Retrieved from https://www.jpcert.or.jp/english/

Japan Cybercrime Control Center. (n.d.). Retrieved from https://www.jc3.or.jp/

Japan, Unauthorized Computer Access Law, Law No. 128 of 1999. (n.d.). Retrieved from http://www.cybercrimelaw.net/Japan.html

jaredcatkinson. (2016, November 15). PowerForensics. GitHub. Retrieved from https://github.com/Invoke-IR/PowerForensics

jdevaney. (2013, February 19). Viewing extended file properties via command line in Linux. Stack Exchange, Super User. Retrieved from http://superuser.com/questions/554291/viewing-extended-file-properties-via-command-line-in-linux

Josefsson, S. (2006, October). The Base16, Base32, and Base64 Data Encodings. Retrieved from https://tools.ietf.org/html/rfc4648

jschicht. (2016, June 27). RawCopy. GitHub. Retrieved from https://github.com/jschicht/RawCopy

Leyden, J. (2016, June 28). SWIFT hackers nick $10m from Ukraine bank. The Register. Retrieved from http://www.theregister.co.uk/2016/06/28/swift_victim_ukraine/

Loader, B. and Thomas, D. 2013. Cybercrime: Security and surveillance in the information age. Routledge.

Lockheed Martin. 2022. Cyber Kill Chain. Lockheed Martin Corporation. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Louis, C. (n.d.). Comparison of computer misuse acts around the world. Retrieved from http://www.rechtsanwalt-louis.de/european_computer_misuse_acts.htm

McGuire, M. 2019. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In The human factor of cybercrime. Routledge.

McLeod, S. (2016). Maslow's hierarchy of needs. Simply Psychology. Retrieved from http://www.simplypsychology.org/maslow.html

MEIT. 2016. Information Technology Act 2000. Goverment of India. Retrieved from https://www.meity.gov.in/content/information-technology act-2000

Mendelsohn, B. (1956). Une nouvelle branche de la science bio-psycho-sociale: La victimologie. Revue Internationale de Criminologie et de Police Technique, Vol.10, pp.95-109.

Menting, M. (2011). Cybercrime laws by country & other resources. Retrieved from http://www.academia.edu/1125166/Cybercrime_Laws_By_Country_and_Other_Resources_DOC

Microsoft Message Analyzer. (n.d.). Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=44226

Microsoft TechNet. (n.d.). Directory data store. Retrieved from https://technet.microsoft.com/en-us/library/cc961761.aspx

Microsoft. (n.d.). Crash dump analysis using the Windows debuggers (WinDbg). Retrieved from https://msdn.microsoft.com/en-us/library/windows/hardware/ff539316 (v=vs.85).aspx

Microsoft. (n.d.). Microsoft Interflow. Retrieved from https://technet.microsoft.com/en-us/library/dn750892.aspx

Microsoft. (n.d.). NetStatisticsGet function. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/bb525390 (v=vs.85).aspx

Microsoft. (n.d.). Network management functions. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/aa370675 (v=vs.85).aspx

Microsoft. (n.d.). Process status API. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/ms684884 (v=vs.85).aspx

MITRE Corporation. (2016). Cyber Observable eXpression (CybOX). Retrieved from http://cybox.mitre.org

MITRE Corporation. (2016). Structured Threat Information eXpression (STIX). Retrieved from https://stixproject.github.io/

MITRE Corporation. (2016). Trusted Automated eXchange of Indicator Information (TAXII). Retrieved from https://taxiiproject.github.io/

Moonsols (n.d.). Retrieved from http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

Murai, S. (2016, June 6). Ransomware making costly inroads into online Japan. The Japan Times. Retrieved from http://www.japantimes.co.jp/news/2016/06/06/reference/ransomware-making-costly-inroads-into-online-japan/#.V8mgEztrrww

National Council of ISACs. (2016). Retrieved from http://www.nationalisacs.org/member-isacs

National Council on Aging. (n.d.). Top 10 financial scams targeting seniors. Retrieved from https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

National Cyber-Forensics & Training Alliance. (2016). Retrieved from https://www.ncfta.net/

National Institute of Standards and Technology, U.S. Department of Commerce. (2012, September). Guide for conducting risk assessments. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology, U.S. Department of Commerce. (2006, August). SP 800-86, Guide to integrating forensic techniques into incident response. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Natsui, T. (2003). Cybercrimes in Japan: Recent cases, legislations, problems and perspectives. NetSafe II Conference, Auckland, New Zealand. Retrieved from http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf

NEC. (n.d.). NEC's superior internal systems are proof in themselves. Retrieved from http://www.nec.com/en/global/solutions/cybersecurity/efforts/index.html

Nelson, B., Phillips, A., Steuart, C. (2016). Guide to computer forensics and investigations (5th ed.). Retrieved from http://www.utc.edu/center-information-security-assurance/468--ch03.ppt

Network Associates. (1999). Introduction to Cryptography, Chapter 1. Retrieved from http://www.pgpi.org/doc/pgpintro/

Neustar. (2015). U.S. DDoS attacks and protection report, April 2015. Retrieved from https://www.neustar.biz/resources/whitepapers/ddos-attacks-protection-report-us-2015

Nmap. (n.d.). Retrieved from https://nmap.org/

Nurse, J. 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624 (2018).

Open Security Research. (n.d.). Retrieved from http://opensecurityresearch.com/files/FGET.zip

OpenIOC. (n.d.). Retrieved from http://www.openioc.org/

OWASP. (n.d.). Application threat modeling. Retrieved from https://www.owasp.org/index.php/

Application_Threat_Modeling
OWASP. (n.d.). OWASP risk rating methodology. Retrieved from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
Paganini, P. (2013, August 7). Cybercrime as a service. Infosec Institute. Retrieved from http://resources.infosecinstitute.com/cybercrime-as-a-service/
Parks, J. (2013). Fraudulent charities in the wake of disaster. Fraud Magazine. Retrieved from http://www.fraud-magazine.com/article.aspx?id=4294978232
Parker, Donn B. "Computer-Related White Collar Crime." In Geis, Gilbert, and Ezra Stotland, eds. White Collar Crime: Theory and Research. Beverly Hills: Sage, 1980.
PCI Security Standards Council. (2016). Retrieved from https://www.pcisecuritystandards.org/
Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., and Aiken, M., 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences 2, 2 (2022).
Ponemon Institute, LLC. (2015). 2015 Cost of cybercrime study: United States [Blog post]. Retrieved from http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states
PowerShell Code Repository – Get-FileHash. (n.d.). Retrieved from http://poshcode.org/5815
proofpoint. 2022. Multi-Persona Impersonation. proofpoint. Retrieved from https://www.proofpoint.com/au/blog/threat-insight/ta453-uses-multipersona-impersonation-capitalize-fomo
Prox, B. (2014, December 18). Get-RegistryKeyLastWriteTime. Retrieved from https://gallery.technet.microsoft.com/scriptcenter/Get-RegistryKeyLastWriteTim-63f4dd96
Reeve, T. (2015, October 15). Japan facing explosion in cyber-crime, claims report. SC Magazine (U.K.). Retrieved from http://www.scmagazineuk.com/japan-facing-explosion-in-cyber-crime-claims-report/article/446174/
Rekall. (n.d.). Retrieved from http://www.rekall-forensic.com/
The Pmem Memory acquisition suite. (n.d.). Retrieved from http://www.rekall-forensic.com/docs/Tools/
Reuters. (2015, December 21). Trader pleads guilty in insider trading, hacking case. Fortune. Retrieved from http://fortune.com/2015/12/21/trader-pleads-guilty-in-insider-trading-hacking-case/
Reuters. (2016, April 4). The "Panama Papers" law firm responds to the massive data hack. Fortune. Retrieved from http://fortune.com/2016/04/04/panama-papers-law-firm/
Richet., JL., 2013. Laundering Money Online: a review of cybercriminals methods. arXiv preprint arXiv:1310.2368 (2013).
Riley, C. (2015, February 6). Insurance giant Anthem hit by massive data breach. CNN Tech. Retrieved from http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/
Root cause analysis. (n.d.). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Root_cause_analysis
Royal Canadian Mounted Police. (2014). Cybercrime: an overview of incidents and issues in Canada - Defining cybercrime from a law enforcement perspective. Retrieved from http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec2
RT. (2013, October 2). FBI seizes "Silk Road" black market domain, arrests owner. Retrieved from https://www.rt.com/usa/silk-road-bitcoin-shut-650/
Russinovich, M. (2011, July 25). TCPView v3.05. Retrieved from https://technet.microsoft.com/en-us/

sysinternals/tcpview.aspx

Samani, R., Beek, C. (2015, November 20). A dummies guide to "insider trading" via botnet [Blog post]. Retrieved from https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet/

Samani, R., Beek, C. (2015, November 23). A dummies guide to "insider trading" via botnet, part 2 [Blog post]. Retrieved from https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet-part-2/

SANS Institute. (n.d.). FOR408: Windows Forensic Analysis [Course]. Retrieved from https://www.sans.org/course/windows-forensic-analysis

SANS Institute. (n.d.). FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting [Course]. Retrieved from https://www.sans.org/course/advanced-incident-response-threat-hunting-training

SANS Institute. (n.d.). FOR572: Advanced Network Forensics and Analysis [Course]. Retrieved from https://www.sans.org/course/advanced-network-forensics-analysis

Sarkar, H. 2022. Cybercrime Navigator. In collaboration with C3I Centre and Microsoft India. Retrieved from https://cybercrime.c3ihub.org/

SecureLogix. (2014, October 21). The surging threat of telephony denial of service attacks. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf

Shaw, S. (n.d.). A modern cybersecurity strategy: Building a budget. SAS Institute. Retrieved from http://www.sas.com/en_us/insights/articles/risk-fraud/a-modern-cybersecurity-strategy-building-a-budget.html

Shook, S. (n.d.). Green eggs & SPAM - Efficient incident response. Retrieved from https://info.cylance.com/incident-response-and-malware

Siddaway, R. (2011, June 29). IE history to CSV [Blog post]. Retrieved from https://richardspowershellblog.wordpress.com/2011/06/29/ie-history-to-csv/

Sidel, R. (2014, September 18). Home Depot's 56 million card breach bigger than Target's. The Wall Street Journal. Retrieved from http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

Sieber, Ulrich. The International Handbook on Computer Crime. New York: John Wiley and Sons, 1986.

Sloan, Irving J. The Computer and the Law. New York: Oceana Publications, 1984.

Somers, L. E. Economic Crimes-Investigative Principles and Techniques. 1984.

Splunk. (2016). Retrieved from http://www.splunk.com/

Standards New Zealand. (2016). Risk management. Retrieved from https://www.standards.govt.nz/search-and-buy-standards/standards-information/risk-managment/

Steptoe & Johnson LLP. (2016, January 21). Comparison of U.S. state and federal security break notification laws. Retrieved from http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

SWIFT. (2016). Retrieved from https://www.swift.com/

Sylve, J. (2016, August 20). LiME. GitHub. Retrieved from http://code.google.com/p/lime-forensics/

Tabansky, L. (2012). Cybercrime: A national security issue? Military and Strategic Affairs, 4 (3), 117-136.

Tang, R. (2015, October 4). Get-MemoryDump. Retrieved from https://gallery.technet.microsoft.com/

scriptcenter/Get-MemoryDump-c5ab38d8
Tcpdump & Libpcap. (2016). Retrieved from http://www.tcpdump.org/
The Scripting Guys. (2014, January 15). Using PowerShell to Find Connected Network Adapters [Blog post]. Retrieved from https://blogs.technet.microsoft.com/heyscriptingguy/2014/01/15/using-powershell-to-find-connected-network-adapters/
The Tor Project. (n.d.). Retrieved from https://www.torproject.org/
The Volatility Foundation. (n.d.). Releases. Retrieved from http://www.volatilityfoundation.org/#!releases/component_71401
The White House, Office of the Press Secretary. (2015, February 13). Executive Order promoting private sector cybersecurity information sharing. Retrieved from
https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
Title 18 U.S. Code, Section 1030 - Crimes and criminal procedure. (n.d.). Retrieved from https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-se c1030.pdf
Title 18 U.S. Code, Section 1030 - Fraud and related activity in connection with computers. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1030
Title 18 U.S. Code, Section 1341 - Frauds and swindles. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1341
Title 18 U.S. Code, Section 1343 - Fraud by wire, radio, or television. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1343
Title 28 U.S. Code of Federal Regulations, Section 0.85 - General functions. (n.d.) Retrieved from https://www.law.cornell.edu/cfr/text/28/0.85
Tittel, E., Lemons, M., Kyle, M. (n.d.). Introduction: Information security and cybersecurity certifications. TechTarget. Retrieved from http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications
Tittel, E., Lindros, K. (2016, November 7). Best computer forensics certifications for 2017. Tom's IT Pro. Retrieved from http://www.tomsitpro.com/articles/computer-forensics-certifications,2-650.html
Tixteco, M., Tixteco, L., Perez, G., Medina, L. (2016, May 22). Intrusion detection using indicators of compromise based on best practices and Windows event logs. ICIMP 2016: The Eleventh International Conference on Internet Monitoring and Protection. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=icimp_2016_2_20_30032
Trend Micro. (2015, August 31). A brief history of notable online banking trojans. Retrieved from http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans
Trend Micro. (2016). Ransomware. Retrieved from http://www.trendmicro.com/vinfo/us/security/definition/ransomware
U.S. Computer Emergency Readiness Team. (n.d.). Information sharing specifications for cybersecurity. Retrieved from https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
U.S. Department of Homeland Security and Department of Justice. (2016, June 15). Guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015. Retrieved

from https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

U.S. Department of Homeland Security. (2016, June 21). Automated Indicator Sharing (AIS). Retrieved from https://www.dhs.gov/ais

U.S. Department of Homeland Security. (n.d.). U.S. Secret Service, electronic crimes task forces. Retrieved from https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf

U.S. Department of Justice, Federal Bureau of Investigation. (2015). 2015 Internet crime report. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

U.S. Department of Justice. (2012). Payment processor for scareware cybercrime ring sentenced to 48 months in prison. Retrieved from https://www.justice.gov/opa/pr/payment-processor-scareware-cybercrime-ring-sentenced-48-months-prison

U.S. Government Accountability Office. (2007). Cybercrime: Public and private entities face challenges in addressing cyber threats. Retrieved from http://www.gao.gov/products/GAO-07-705

U.S. Office of Personnel Management, Cybersecurity Resource Center. (2015). Cybersecurity incidents. Retrieved from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

U.S. Patriot Act. (2001, Jan 3). Retrieved from https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

U.S. Postal Inspection Service. (2008). A U.S. Postal Inspector's Guide to Internet Safety for Children. Retrieved from http://docplayer.net/16377727-A-u-s-postal-inspector-s-guide-to-internet-safety-for-children.html

U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations. (2015, September 15). OCIE's 2015 Cybersecurity Examination Initiative. Retrieved from https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

U.S. Securities and Exchange Commission. (2015, September 22). SEC charges investment advisor with failing to adopt proper cybersecurity policies and procedures prior to breach. Retrieved from https://www.sec.gov/news/pressrelease/2015-202.html

U.S. Securities and Exchange Commission. (2016, June 8). SEC: Morgan Stanley failed to safeguard customer data. Retrieved from https://www.sec.gov/news/pressrelease/2016-112.html

U.S. Securities and Exchange Commission. (2016, March 18). Regulation S-P. Retrieved from https://www.sec.gov/spotlight/regulation-s-p.htm

U.S. Securities and Exchange Commission. (2016, October 14). SEC Spotlight: Regulation SCI. Retrieved from https://www.sec.gov/spotlight/regulation-sci.shtml

United States Department of Justice, Offices of the United States Attorneys. (n.d.). Cyber crime. Retrieved from https://www.justice.gov/usao/priority-areas/cyber-crime

Urano, A. (2015). The Japanese underground: A TrendLabs research paper. Retrieved from http://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdf

US Legal Definitions. (n.d.). Cybercrimes law and legal definition. Retrieved from http://definitions.uslegal.com/c/cybercrimes/

Verizon. (2016). Verizon's 2016 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

VirusTotal. (n.d.). Retrieved from https://www.virustotal.com

Visgean. (2014, February 23). Zeus. GitHub. Retrieved from https://github.com/Visgean/Zeus

Vormetric Data Security. (2015). 2015 Vormetric insider threat report. Retrieved from https://www.vormetric.com/campaigns/insiderthreat/2015/pdf/insiderthreatreport-retail-0224.pdf

WGCL-TV/CBS 46. (2014, May 19). Police: International Nigerian crime ring operates from Atlanta suburbs. Retrieved from http://www.cbs46.com/story/25551165/police-international-nigerian-crime-ring-operates-out-of-atlanta-suburbs

What-when-how. (n.d.). Accreditation of forensic science laboratories. Retrieved from http://what-when-how.com/forensic-sciences/accreditation-of-forensic-science-laboratories/

WHOis.net. (2015). Retrieved from https://www.whois.net/

WikiLeaks. (n.d.). Retrieved from https://wikileaks.org/

Wilmot, F., Lindow, B. (2014). Threat intelligence: STIX and stones will break your foes. Splunk .conf2014. Retrieved from https://conf.splunk.com/session/2014/conf2014_FredWilmot_Splunk_Security.pdf

Windows Management Instrumentation Command (WMIC.exe). (n.d.). Retrieved from http://ss64.com/nt/wmic.html

Windows Sysinternals. (2016). Retrieved from https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

WinPcap. (n.d.). Retrieved from https://www.winpcap.org/

Wireshark. (n.d.). Retrieved from https://www.wireshark.org/

X-Ways Forensics: Integrated Computer Forensics Software (n.d.). Retrieved from http://www.x-ways.net/forensics/index-m.html

YARA Project. (n.d.). Retrieved from https://code.google.com/p/yara-project

Index

A

Active Directory 188, 189
AML（マネーロンダリング対策） 136, 279

B

b・d・r ダイナミクス 33
BEC 72, 147, 179, 273, 388
Bitcoin 81, 134, 429

C

CaaS 65, 107, 134, 135, 139, 149, 155, 162, 307, 308, 346, 393,
CFAA 64, 65, 138, 142, 311
CFT（テロ資金供与対策） 279
Chain of Custody（証拠の保全） 247, 411
CSIRT 19, 26, 28, 29, 30, 41, 99, 100, 293, 294, 295, 296, 299, 300, 301, 303, 315, 327, 412

D

DDoS ... 49, 52, 57, 65, 81, 82, 84, 85, 86, 87, 121, 139, 145, 147, 149, 150, 171, 195, 197, 198, 305, 331, 410, 414, 422, 424, 426
Deep Web 414, 424
DoS 52, 57, 65, 81, 82, 84, 85, 86, 87, 105, 139, 145, 147, 149, 150, 171, 195, 197, 198, 305, 331, 410, 414, 422, 424, 426, 428

E

ETL 46, 211, 213, 220, 221, 223, 235, 271, 285,

H

HUMINT 113, 114, 120, 135, 138, 141, 161, 162, 165, 195, 371

I

IC3 ..... 81, 82, 137, 426, 432
IoC（侵害兆候、不正アクセスのインジケーター） 96, 97, 98, 100, 103, 104, 111, 123, 162, 189, 203, 206, 207, 208, 210, 211, 214, 242, 255, 261, 262, 263, 264, 267, 270, 285, 286, 287, 295, 296, 318, 326, 328, 329, 339, 340, 351
IoT（モノのインターネット） 53, 144, 196, 202, 245, 246, 266, 329, 391, 416

M

MLAT（Mutual Legal Assistance Treaties 相互刑事援助条約） 57, 58, 309, 310, 331, 417
MLINT：Money Laundering INTelligence） 141

O

OSINT 141, 162, 164, 165, 189, 195, 205, 211, 242, 243, 281, 339, 340, 399

P

PEP 279
PII（個人識別情報） ... 82, 83, 87, 98, 127, 133, 140, 141, 242, 294, 331, 333, 334, 335, 340, 378, 410

R

RACI 19, 300, 301, 314, 319, 339
RUMINT 162, 164, 195

S

SIEM 116, 166, 188, 195, 203, 204, 205, 208, 211, 236, 247, 251, 305, 320, 350, 374
SIGINT 138, 141

T

Technology as a Target（攻撃対象としての技術） 34
Technology as an Instrument（犯罪の道具としての技術） 34
Threat Actors（脅威アクター） 268
Threat Profile（脅威プロファイル） 278
TTP（戦術、技術、手順） 270
Victimology 264, 421

い

インサイダー取引 126, 127, 134, 136, 139, 148
インターネット犯罪苦情センター（IC3） 81, 137
インテリジェンス 5, 6, 7, 8, 9, 15, 18, 19, 39, 65, 96, 97, 100, 103, 113, 135, 141, 150, 159, 160, 161, 162, 163, 164, 165, 167, 181, 189, 190, 199, 208, 210, 240, 242, 244, 259, 260, 261, 262, 263, 286, 292, 293, 305, 312, 328, 329, 335, 340, 346, 369, 374, 399

お

オープンソースインテリジェンス（OSINT） 162

か

カードスキマー 79
外交的手法 12, 57, 58
階層構造 12, 86, 269, 365
学習と成長の視点 36, 37
仮想通貨 8, 84, 140, 148
カテゴリ型組織 11, 38, 39
鑑定 35
鑑定証人 314

き

起訴 4, 19, 34, 48, 50, 53, 54, 55, 60, 65, 66, 75, 78, 92, 156, 198, 239, 252, 268, 292, 293, 305, 308, 310, 311, 313, 314, 318, 319, 324, 326, 327, 330
帰属属性 18, 279, 280
揮発性 115, 175, 195, 211, 213, 233, 234, 235, 244, 259, 266, 267, 270
キャンペーン 80, 100, 105, 123, 142, 181, 329, 386
脅威アクター 207, 251, 268, 330
脅威プロファイル 278

く

クライムウェア 120, 264, 265, 266

け

警察学校 30
警察官としての基礎 30, 31, 32
警察政策 31, 32, 268

こ

広域捜査班 35
攻撃対象としての技術 12, 34, 52, 79, 434
構造化データ 18, 268, 269, 270, 273
後方支援 42, 43, 44, 45, 63, 64, 89, 90, 118, 119, 153, 154, 193, 194, 249, 250, 283, 284, 317, 318, 337, 338, 370, 376, 377, 378, 403, 404
個人識別 82, 87, 127
個人情報窃盗 82, 83, 87, 139, 243
コンピュータ詐欺と濫用に関する法律（CFAA） 138, 142

さ

サービス拒否（DoS）攻撃 82
サービスとしてのサイバー犯罪（CaaS） 307
最高情報責任者 28, 439
最高情報セキュリティ責任者 365, 400
サイバーキルチェーン 13, 100, 106
サイバー空間 11, 33, 34, 35, 36, 43, 50, 57, 69, 71, 72, 74, 75, 77, 78, 79, 80, 86, 87, 126, 145, 161, 238, 386, 438
サイバー詐欺師 12, 85
サイバー犯罪 3, 4, 5, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 80, 84, 85, 87, 88, 89, 90, 91, 92, 95, 96, 98, 99, 100, 101, 104, 105, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 170, 171, 176, 190, 191, 192, 193, 194, 195, 198, 202, 203, 204, 205, 208, 210, 213, 214, 222, 225, 229, 234, 236, 237, 238, 239, 241, 242, 243, 245, 248, 249, 250, 251, 258, 259, 264, 265, 266, 268, 270, 275, 278, 280, 281, 282, 283, 284, 285, 290, 291, 292, 293, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 323, 324, 325, 326, 327, 328, 329, 330, 331, 335, 336, 337, 338, 339, 340, 344, 346, 347, 348, 349, 351, 352, 355, 356, 358, 361, 362, 365, 366, 369, 370, 371, 372, 373, 375, 376, 377, 378, 379, 382, 384, 391, 392, 394, 402, 403, 404, 438
サイバー犯罪に関する条約 12, 56, 57, 64
サイバー犯罪捜査（Cybercrime Investigation） 34
サイバー犯罪班 37, 38, 39
サイバー犯罪捜査官 21, 26, 28, 29, 38, 42, 50, 51, 92, 99, 100, 142, 258, 265, 278, 281, 296, 306, 312, 327, 370
詐欺師 72, 76, 84, 85

し

資金洗浄インテリジェンス（MLINT） 141
事件対応 11, 34, 41, 43
事後対応捜査 35
事前予防捜査 35
児童の性的搾取 13, 73, 78, 86
重要な公的地位にある者（PEP） 279
受託者の視点 36
証拠隠匿 187
証拠収集 30, 44, 45, 46, 57, 62, 63, 74, 88, 89, 117, 118, 138, 152, 153, 162, 176, 186, 192, 193, 201, 202, 203, 204, 205, 206,208, 211, 212, 214, 215, 224, 227, 229, 234, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246,, 248, 249, 250, 251,255, 258, 259, 282, 283, 294, 297, 301, 302, 303, 306, 309,

311, 316, 317, 319, 328, 336, 337, 350, 369, 375, 376, 402, 403
証拠の連鎖 203, 247, 339
侵害兆候 99
人的証拠 259

す

スクリプトキディ 85, 87, 91, 136, 279
スケアウェア 81, 82, 85
スパム 27, 75, 81, 106, 121, 129, 131, 139, 140, 142, 147, 265, 273
スピアフィッシング 65, 83, 104, 139, 140, 251, 254, 331

せ

脆弱性 13, 22, 60, 69, 70, 72, 80, 83, 84, 92, 96, 97, 99, 101, 105, 112, 121, 122, 127, 130, 131, 132, 133, 135, 136, 143, 144, 146, 147, 148, 149, 150, 158, 160, 162, 167, 168, 171, 187, 198, 263, 290, 291, 324, 328, 329, 332, 333, 361, 367, 368, 382, 383, 385, 388, 392, 394, 395, 396, 400, 405, 438
説明責任 11, 41, 42, 43, 44, 45, 63, 64, 89, 90, 118, 119, 153, 154, 193, 194, 249, 250, 283, 284, 292, 294, 301, 317, 318, 337, 338, 344, 353, 354, 356, 370, 376, 377, 384, 397, 403, 404, 439
戦術 4, 21, 28, 41, 44, 45, 63, 64, 66, 68, 75, 76, 89, 90, 96, 97, 102, 103, 109, 110, 118, 119, 122, 126, 145, 153, 154, 158, 163, 193, 194, 249, 250, 255, 261, 262, 263, 268, 270, 283, 284, 299, 314, 315, 317, 318, 324, 334, 337, 338, 345, 356, 371, 374, 376, 377, 382, 401, 403, 404
戦術、技術、手順 96, 126, 158, 270
潜入捜査 114, 135, 306, 307, 308, 309
戦略 ... 28, 31, 32, 36, 37, 40, 44, 45, 46, 60, 63, 70, 89, 103, 104, 110, 111, 118, 145, 153, 193, 199, 249, 268, 283, 290, 308, 312, 317, 321, 324, 326, 327, 337, 340,344, 345, 346, 347, 348, 349, 352, 353, 354, 357, 358, 359, 360, 362, 364, 376, 382, 403

そ

相互刑事援助条約（MLAT） 57, 58, 309, 310, 331, 417
捜査管理 ..... 41, 44, 45, 63, 89, 90, 118, 119, 153, 154, 193, 249, 250, 283, 317, 3!8, 337, 338, 370, 376, 377, 378,, 403,
総務人事 12, 42, 43, 44, 45, 63, 64, 89, 90, 118, 119, 153, 154, 193, 194, 249, 250, 283, 284, 317, 318, 337, 338, 370, 376, 377, 378, 403, 404
ソーシャルエンジニアリング 48, 73, 75, 76, 81, 82, 85, 104, 120, 121, 127, 140, 143, 147, 150, 171, 251, 319, 339, 379
ソーシャルメディア 14, 68, 77, 112, 114, 123, 127, 130, 133, 134, 140, 147, 164, 169, 280, 313
組織犯罪集団 85

た

ダークウェブ ... 14, 59, 91, 112, 113, 114, 130, 133, 140, 281, 286, 346
ダークネット 14, 133, 135, 136, 139, 142, 149

ち

チェックサム 239
知見収集 41, 44, 45, 63, 89,, 90, 118, 119, 153, 154, 193, 194, 249, 250, 283, 284, 317, 318, 330, 337, 338, 370, 376, 377,378, 403, 404
抽出、変換、ロード（挿入） 271
調査 4, 6, 9, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45, 48, 49, 50, 51, 53, 54, 57, 59, 61, 62, 63, 65, 73, 74, 76, 78, 79, 80, 81, 85, 88, 89, 90, 91, 92, 93, 96, 97, 98, 100, 103, 104, 105, 112, 113, 115, 116, 117, 118, 119, 120, 122, 128, 130, 133, 137, 138, 140, 145, 147, 149, 150, 151, 152, 153, 154, 158, 160, 161, 165, 166, 167, 171, 173, 174, 175, 176, 177, 178, 179, 180, 181, 183, 184, 185, 186, 187, 188, 189, 190, 192, 193, 194, 195, 199, 202, 203, 204, 205, 208, 209, 210, 211, 212, 213, 214, 218, 219, 220, 222, 223, 230, 232, 234, 235, 236, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 253, 254, 255, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 270, 273, 274, 276, 277, 279, 281, 282, 283, 284, 286, 287, 290, 291, 293, 294, 298, 299, 300, 301, 302, 303, 304, 305, 312, 313, 314, 316, 317, 318, 319, 320, 321, 324, 326, 327, 328, 329, 331, 335, 336, 337, 338, 339, 340, 341, 344, 346, 347, 348, 349, 350, 351, 352, 354, 355, 356, 357, 358, 360, 362, 363, 364, 365, 366, 367, 369, 370, 371, 372, 373, 375, 376, 377, 378, 379, 382, 384, 386, 393, 402, 403, 404, 406, 407,438

て

ディープウェブ 14, 112, 113, 114, 130, 133, 160, 281
データウェアハウス 270, 271
データマイニング 18, 268, 269, 272, 273, 277
データモデリング 18, 268
データ品質テスト 18, 268, 274
デジタルデータ 35, 54
テロ行為 83, 86

テロ資金供与対策 279

と

道具としての技術 12, 34, 50, 74
ドーキング 164
ドキシング 139, 147
ドライブバイダウンロード 147
トリアージ.....16, 41, 42, 204, 205, 233, 244, 299, 350, 394

な

ナイジェリアの手紙 75
内部プロセスの視点 36
難読化.....13, 35, 43, 103, 106, 108, 111, 120, 123, 165

ね

ネットいじめ 13, 55, 77, 78, 86, 127

は

破壊.....4, 46, 48, 53, 59, 65, 68, 72, 87, 91, 92, 105, 106, 108, 110, 115, 126, 127,128, 141, 132, 143, 148, 149, 158, 160, 195, 242, 243, 264, 320, 350, 391
ハクティビスト 13, 82, 86, 121, 136, 279
外れ値..... 272, 273, 274, 276
ハッシュ署名 224, 239, 245
犯行遺物..... 30, 44, 45, 46, 62, 63, 88, 89, 99, 112, 116, 117, 118, 130, 152, 153, 160, 192, 193, 194, 248, 249, 282, 283, 316, 317, 336, 337, 375, 376, 402, 403
犯行現場の指標 264
犯罪学.....33, 264

ひ

被害者プロフィール 264
非構造化データ 18, 268, 269, 270, 273
ビジネスメール詐欺 72, 109, 127, 147, 273
ビットコイン 81, 121, 136
ヒューミント 138, 141
標的型サイバー攻撃 83, 87, 147

ふ

ファーミング 106, 436
フィッシング.....48, 65, 68, 69, 72, 73, 74, 75, 76, 83, 104, 106, 110, 120, 123, 127, 129, 131, 133, 134, 139, 140, 142, 147, 150, 155, 179, 251, 254, 291, 294, 304, 319, 331, 339, 340, 341, 354, 362, 379, 385, 388, 395, 396
フォレンジック 6, 8, 9, 10, 15, 16, 17, 18, 22, 29, 41, 54, 59, 61, 115, 137, 158, 166, 168, 169, 170, 171, 172, 173, 174, 175, 177, 178, 179, 180, 181, 182, 187, 195, 198, 199, 203, 205, 206, 210, 212, 213, 224, 225, 234, 235, 236, 238, 240, 241, 242, 245, 253, 254, 260, 261, 263, 264, 265, 266, 267, 270, 280, 281, 296, 298, 302, 303, 305, 312, 313, 314, 320, 321, 324, 356, 362, 366, 367, 369, 372, 374, 406, 407, 438
複合型組織 11, 39, 40, 436
不正アクセス 13, 14, 16, 54, 73, 83, 87, 92, 96, 100, 101, 103, 104, 105, 106, 107, 108, 112, 116, 120, 121, 123, 127, 129, 130, 132, 133, 134, 135, 138, 139, 141, 142, 143, 148, 149, 150, 160, 163, 165, 167, 171, 173, 175, 177, 180, 189, 195, 197, 198, 206, 251, 254, 261, 262, 273, 285, 286, 287, 291, 300, 301, 302, 307, 311, 319, 328, 341, 362, 384, 391
不正アクセス禁止法 54
物的証拠.....36, 259, 266
ブラックハットハッカー.....87
振り込め詐欺 76, 77
分散型サービス妨害攻撃（DDoS） 145

ほ

ボットネット 4, 12, 15, 16, 65, 66, 81, 91, 101, 105, 106, 107, 126, 129, 131, 134, 139, 140, 141, 142, 149, 150, 159, 160, 162, 165, 176, 195, 196, 197, 198, 199, 265, 305, 350
ホワイトハットハッカー.....87

ま

マクロフレームワーク 11, 31, 32
マトリクス型組織 11, 39
マネーミュール 131, 132
マネーロンダリング 65, 66, 84, 136, 138, 279, 311
マネーロンダリング対策（AML） 136, 279
マルウェア 4, 27, 48, 53, 56, 65, 66, 72, 75, 81, 83, 84, 85, 96, 97, 103, 105, 106, 109, 110, 120, 121, 122, 123, 131, 132, 133, 134, 135, 138, 139, 140, 141, 146, 147, 149, 150, 158, 163, 164, 165, 169, 171, 174, 175, 176, 180, 184, 187, 195, 205, 206, 214, 219, 223, 251, 254, 262, 265, 266, 270, 285, 287, 294, 301, 305, 321, 324, 326, 330, 331, 339, 340, 341, 350, 351, 354, 355, 374, 379, 384, 385, 388, 390, 395, 401

み

水飲み場型攻撃 129, 140, 142, 147, 155
ミッション...20, 31, 36, 37, 41, 292, 327, 347, 352, 382

め

メタデータ.....17, 18, 99, 165, 169, 172, 173, 189, 195, 204, 205, 206, 213, 214, 222, 223, 224, 225, 228, 230, 232, 233, 235, 269, 270

も

モノのインターネット ...53, 144, 196, 202, 245, 246, 329

ゆ

有責性.....18, 264

よ

予防啓発.....11, 41, 42, 43, 44, 45, 63, 64, 89, 90, 118, 119, 153, 154, 193, 194, 249, 250, 283, 284, 317, 318, 337, 338, 348, 370, 376, 377, 403, 404

ら

ランサムウェア.... 3, 4, 48, 53, 59, 65, 68, 81, 82, 85, 92, 104, 105, 106, 108, 109, 110, 115, 121, 122, 126, 128, 133, 134, 135, 137, 143, 145, 147, 149, 312, 320, 331, 385, 386, 388, 397

り

リベンジポルノ 55, 78, 127

倫理的ハッカー 87

れ

レジストリキー 123, 171, 172, 175, 262, 263

連邦捜査局（FBI） 4, 9, 10, 137

［制作協力］
編集：篠田健二
制作：エステム（谷口宏佳、横野 保）
翻訳：藤井比呂志

あとがき

『サイバー犯罪捜査の知識体系（CIBOK）』第２版の制作に携われたことを大変光栄に思います。本書の完成にあたっては、執筆者、査読者、寄稿者の皆様の並々ならぬ努力、豊富な専門知識、そして鋭い洞察力が結集されており、深く感謝申し上げます。その内容の広範さと奥深さは、私たちが共有するサイバー犯罪捜査という進化し続ける分野における複雑な課題と重大な責任を如実に物語っています。

本書には、世界中の熟練した専門家が寄稿しており、彼らは高度な技術的・捜査的経験と、国境を越えた洗練された脅威に立ち向かうために不可欠なグローバルな連携の精神を兼ね備えています。

●物理的セキュリティとサイバー脅威の融合

私たちは、世界有数のセキュリティ企業において、テクノロジーリーダーとして物理的脅威とサイバー脅威が急速に融合しつつある現実を日々目の当たりにしています。私たちの組織は、重要インフラ、金融機関、国際的な物流ネットワーク、そして公共空間の保護を支援していますが、これらの現場では、もはや物理的な侵入とサイバー攻撃を明確に分けて捉えることが難しくなってきています。

サイバー空間と物理空間におけるリスクは相互に作用し、一方の領域で発生した事象が、他方の領域に瞬時に波及する時代となりました。サイバー犯罪と物理的犯罪の境界線は曖昧になりつつあり、将来的には完全に融合する可能性すらあります。今、私たちはデジタルリスクとフィジカルリスクの交差点に立っていることを認識しなければなりません。

●犯罪の現実

現実は極めて明確です。バールを用いた犯行であれ、キーボードを通じた侵入であれ、犯罪は犯罪です。バックドアからの物理的侵入も、漏洩したクレデンシャルを用いたデジタル侵入も、目的、影響、そして対応の緊急性において本質的な違いはありません。

いずれの領域においても、安全性の確保、予防、調査、原因の特定、解決という一連のプロセスは、同じ厳密さと倫理観、そして人々や資産、コミュニティを守るという強い使命感をもって臨まれるべきです。

サイバー脅威の捜査においては、フォレンジックツールや検出技術の活用にとどまらず、デジタル証拠の重みを理解し、公正な観点から行動を精査する視座が必要です。サイバー攻撃者もまた、物理的犯人と同様に、その行動には意図を示す痕跡やパターンが必ず残されるという認識が求められます。

●インサイダー脅威への対応

インサイダーによる脅威は、物理的・サイバー的両面の脆弱性を巧妙に突く存在です。信頼された従業員や第三者は、アクセスバッジを使って制限区域に入るのと同様に、正規の認証情報を用いてファイアウォールを突破する可能性があります。

こうした脅威に対する捜査では、物理的な行動とサイバー的な行動を別個の出来事として切り離すのではなく、ひとつの統合された脅威ベクトルとして捉える視点が重要です。CIBOK が提唱する包括的アプローチは、分類体系、証拠の取り扱い、調査のフレームワークを通じて、まさにこのような学際的対応の必要性に応えるものです。

●次世代のための基盤

本書は、捜査官のみならず、強靭かつ知的で、統合されたセキュリティプログラムの設計・実行・監督を担うテクノロジーリーダー、経営幹部、セキュリティ専門家にとっても有益な指針となることでしょう。

テクノロジーリーダーとは、単なる技術者ではありません。私たちは「信頼」の管理者です。不正行為や窃盗、妨害、過失などによってこの信頼が損なわれたとき、私たちにはそれに毅然と対処する責任があります。

被害の本質と影響を理解し、適切な措置を講じることこそが、私たちの義務であり、CIBOK はその取り組みに規律と目的を与えてくれます。

このガイドブックは、サイバー防衛と刑事司法の未来を担う次世代の捜査官やリーダーにとって、不可欠な基礎資料です。物理空間とデジタル空間の境界がますます曖昧になっていく中、私たちは対応力を進化させ、犯罪がどこで発生しようとも、常に説明責任を追及し続ける姿勢を持ち続けるべきです。

マーク・マリソン
最高技術責任者（CTO）
アライド・ユニバーサル

ディアナ・スティール
北米最高情報責任者（CIO）
アライド・ユニバーサル