【2023 年度】海外サイバーセキュリティ・プライバシー政策動向の解説

2024 年 5 月

JCIC 客員研究員　古澤一憲

【2023 年度】海外サイバーセキュリティ・プライバシー政策動向の解説 について

JCIC では、サイバーセキュリティとプライバシー政策に関連した最新の海外動向をまとめ、メールマガジン形式で全会員とオブザーバー組織などに「JCIC 海外ニュース」を毎週配信している。

配信したニュースは翌月に JCIC のウェブサイトに掲載し、広く閲覧できるようにしている。この海外ニュース配信は、基本的にセキュリティ事故や脆弱性情報、技術情報は取り扱うことはせず、海外の政策動向を中心に配信することで、日本企業のビジネス視点での施策検討の一助となることを目的とするものである。

今回のコラムでは、2023 年度（2023 年 4 月～2024 年 3 月）に配信した 168 件の JCIC 海外ニュースを分析し、2024 年度の政策動向を占う重要な出来事を解説する[1]。

まず、2023 年度の海外サイバーセキュリティ・プライバシー政策動向のまとめとして全体を俯瞰した解説を行い、次に各トレンド別に代表的なニュースの振り返りを行う。

1.　2023 年度の主要なサイバー政策動向のまとめ

2023 年度のサイバー政策動向は、サイバーセキュリティの安全保障問題化という大きな流れが継続し、より破壊的な方向へのエスカレーションの兆候と経済安全保障や外交関係への影響の強まりを示す事例が多く見られた。デジタル機器や生成 AI への規制についても、これまで以上にサイバーセキュリティの論点が重視されている。

JCIC では 2023 年度の主要なトレンドとしてサイバー大国同士のつばぜり合いと周囲への波紋、デジタル保護主義の新しい段階、サイバー犯罪に対する国際捜査の成果、AI 規制におけるサイバーセキュリティの 4 点に着目する。

サイバー大国同士のつばぜり合いと周囲への波紋

2023 年度は、サイバー大国である米英や中露間でサイバーセキュリティの関係性において相互に直接的な影響を及ぼす行動が増加し、かつてないほどの緊張の高まりを見せた。

中国の国家支援型サイバー攻撃は、2010 年代においては機密情報の窃取が中心であり、重要インフラの安定稼働に影響を及ぼすような破壊的サイバー攻撃の実行は限定的であった。しかし、2020 年代に入ってから明らかに状況が変化し、米国の重要インフラを直接標的とした破壊的サイバー攻撃の数が増してきた経緯がある。2023 年度は特に Volt

[1] 2022 年度以前のまとめはこちらから：https://www.j-cic.com/reports.html#org_ovrvw1c

Typhoon と呼称される攻撃グループによる一連の破壊的サイバー活動に焦点があてられた。米英はこれを中国による国家支援型サイバー活動であると帰属を明言、「現代における決定的な脅威」であると位置づけた。数年にわたり米国の上下水道管理システムや衛星通信システムへのサイバー攻撃に関与し、不正な制御指令を発する一歩手前まで侵害を実行したと強く非難した。

一方ロシアは、破壊的サイバー攻撃こそウクライナとの紛争へのリソース配分を重視している様子が伺えるが、2024 年に実施される米国大統領選の中間選挙を見据えた偽情報の流布に関するトピックが多く見られた。米国は偽情報の流布を民主主義インフラへの破壊工作とみなし警戒を強めており、米国サイバー軍からも敵対的プロパガンダとしての対応についてレポートが発行された。

これらの緊張の高まりを受け、米政府は敵対的な国家を名指しした上での法整備や新組織の設立、サイバー予算の大幅拡大といったこれまで以上に強力なサイバー安全保障政策を次々と打ち出した。また、民間企業への規制や働きかけの強化、経済安全保障政策への影響も見られた。

民間企業の視点から特に着目すべきポイントのひとつが、サイバー版「大きな政府」とでも言うべき政策の質の変化である。政府組織から民間企業に対しての注意喚起やガイドラインの提示といった形に留まらず、民間企業の具体的な行動を要求する規制等が世界的に増加している。

象徴的な例として取り上げたいのが、米国での「セキュリティ・バイ・デザイン」というコンセプトにおける含意の変化である。従来この言葉はソフトウェア開発のベストプラクティスとしての意味合いが強かった。しかし、ソフトウェアサプライチェーンを狙ったサイバー攻撃の激化をうけ、政府がソフトウェアベンダーらに対して社会的責任を果たすことを強く要請するという政策的側面が強調されるよう変化している。23 年 11 月には、2020 年に大規模なサイバー攻撃事案の原因となった SolarWinds 社が適切なサイバーセキュリティ対策状況の開示を行わなかったとして、米国証券取引委員会が同社の CISO を提訴したという発表もあった。ソフトウェアサプライチェーンは国際的エコシステムであり、米国企業に限らず日本を含む諸外国の企業にも大きく影響する議論となるだろう。

他にも、重要インフラ事業者に対する監督官庁の権限強化や上場企業のインシデント報告要件の厳格化といった民間企業のセキュリティ対応の質の担保に政府からの介入を強める施策が各国で発表された。特に欧州中央銀行は監督下の銀行を対象に復旧能力テストを実施するという積極性を見せた。日本国内でも政府と重要インフラ事業者との連携を図る政策が種々実行されているところであるが、安全保障の議論が施策の方向性について与える影響に注目したい。

経済安全保障の観点では、サイバー安全保障とのつながりを伺わせる民間ビジネスへの政府介入が多く見られた。米国では、24 年 3 月の中国企業の Byte Dance 社に対する TikTok 事業売却を強制する法案（その後 4 月に下院通過）や 24 年 1 月に開始されたファッション EC の SHEIN に対する慎重なサイバーセキュリティ審査などが代表的な事例といえる。背景には、米国民の行動やプロファイルに関するデータが選挙への他国からの介入に利用されることへの懸念があると指摘されている。他方、中国の側も半導体メーカーのマイクロン社製品をサイバーセキュリティ審査で不合格とし

たほか、24 年 5 月から施行される予定の改正国家機密保護法においてセキュリティ製品を抜き打ち検査の対象に位置付けるなどしており、製品やサービスの流通への影響が両国で相互に拡大している。

これらの流れは 2024 年度も継続するものと考えられ、周辺国への影響も増してくるだろう。現時点では英国に米国と協調する行動が目立つが、その他の同盟国との協力関係の強化も推し進められると予想される。日本におけるセキュリティクリアランス法制などへの影響も考えられるだろう。また、中露の関係性や中東諸国などのスタンスも注視すべきである。

デジタル保護主義の新しい段階

近年のデータ主権の尊重は、消費者の権利保護という本来の目的以外にもインターネットサービスの提供に地域や国家の単位で異なる規制の枠組みを導入するという形でビジネス環境に大きな影響を与えてきた。EU 一般データ保護規則（GDPR）をはじめとする域外事業者への強力な罰則規定を組み込んだデータ保護規制は、巨大グローバル IT 企業へのカウンターとしても重要な役割を果たし続けている。デジタル保護主義とも形容される本トレンドにおいて、2023 年度に印象的であったトピックは、デジタルデバイスに対する規制の拡大とデータ流通を委縮させないための現実的な規制への調整である。

デジタルデバイスに対する規制の拡大として象徴的な動向は、23 年 7 月に発表された米国におけるスマートデバイス向けセキュリティラベル表示プログラム（サイバートラストマーク）と 24 年中に施行予定の欧州サイバーレジリエンス法に対応する機器認証制度の 2 つだろう。いずれも脆弱な IoT 機器が攻撃者によってボットネット化される脅威やスマートデバイスを通じた盗聴リスクなどが背景にある。しかし、米国のサイバートラストマークが市場メカニズムによりマークを付与された製品が競争力を高めることを狙いとする一方で、欧州サイバーレジリエンス法は GDPR 同様に企業のグローバル売上に連動した罰金制度を運用する点で違いがある。24 年 1 月にはコモンクライテリアに基づく認証スキームが EU サイバーセキュリティ認証フレームワークに対応した初のスキームとして発表された。チップやハードウェア、ソフトウェアなど個別の構成要素ごとに認証を取得可能な体系となっており、IT 機器産業に携わる広範な事業者を対象としている。これまでデータ保護規制が IT 産業に与えた影響がものづくりのサプライチェーンを対象に拡張される構図であり、制度の内側と外側に保護主義的な違いをもたらす可能性があるだろう。

もう一点のデータ流通を委縮させないための現実的な規制への調整は、各国で続いた GDPR 水準のデータ保護規制の導入による民間企業の混乱やビジネスの停滞を緩和する意図が見て取れる。23 年 7 月に長らく中断していた EU と米国間のデータプライバシー要件の十分性認定があらたな枠組みにおいて合意されたことを筆頭に、中国や韓国ではデータの国外移転に関する法規をより事務的なレベルで明確にすることで事業者の委縮効果を軽減する措置がとられた。保護主義的政策における最大の副作用である経済効率の低下に対する調整弁とも考えることができるだろう。

デジタル機器のセキュリティ認証制度の本格的な施行は 2024 年度以降に予定されており、モノのサプライチェーンにどのような形で具体的な影響が生じてくるかを確認できるのはこれからになるだろう。しかし、保護主義的な施策は経済的なデメリットと不可分であるため、データ保護規制と同様に相互認定やバランスをとる施策の動向にも同時に目を配ることが現実的な対応を適時に計画するために重要となるだろう。

サイバー犯罪に対する国際捜査の成果

高度に組織化されたサイバー犯罪グループによる被害は、国家を背景とした標的型サイバー攻撃と並ぶ主要な脅威であり続けている。しかし、攻撃者の特定から帰属の言及といったプロセスに政治的な要因を含むことから根源的な対応が難しい国家による攻撃と異なり、サイバー犯罪への対応は国際協調が大きな成果を生み出しつつある。

2023 年度も大きな最大手ランサムウェア犯罪グループ LockBit の幹部メンバーの逮捕、認証情報を窃取するマルウェアとして猛威を振るった Qakbot のインフラの差し押さえ、ダークウェブ市場 Genesis Market の閉鎖など多くの成果が国際捜査連携によって成し遂げられた。サイバー犯罪では被害が発生した国と異なる国に攻撃者が潜伏していることが常であるため、容疑者の身柄を確保する段階まで捜査を進めるためには国際連携が極めて重要となる。一定の沈黙の後にグループの活動再開や再編が見られるケースも多く必ずしも犯罪グループの活動そのものを停止する成果ではないという見方もあるが、サーバの差し押さえやメンバーの逮捕は確実に組織の体力を削ぐものであり、大きな前進といえるだろう。[2024.5.9 追記] FBI、ユーロポールなどから LockBit 主催者（「LockBitSupp」として知られていた）と見られるロシア人の身元を特定、制裁措置を開始した旨が公表された。[2]

また、今年度の特筆すべき事項として、LockBit に対する国際捜査の一環で日本の警察庁が開発した復号ツールが配布され、被害組織の救済に一役買ったことを挙げるべきだろう。2022 年にサイバー局が発足してからおよそ 2 年、国内外で様々な改革が進められている最中であるが、サイバー犯罪への国際的な対処の取り組みに協調し、目に見える成果を発揮している事実は頼もしく、今後の活躍にも期待をしたい。

AI 規制におけるサイバーセキュリティの議論

前年度から引き続き、2023 年度も生成 AI 技術は目覚ましい進化を遂げ、これに付随した議論や政策に関する情報も慌ただしく飛び交うこととなった。

生成 AI に関する論点の全体を対象とした基本方針は各国の方針の違いを浮き彫りにした。米国バイデン大統領が 10 月に公布した「AI の安全性に関する大統領令」では、多くの領域で AI のリスク管理策を政府のリーダーシップのもと進めつつ積極的な法規制の導入には慎重姿勢であり、基本的にはこれまでのソフトロー路線を継続している。EU では長く議論されてきた「AI 法」が 2024 年 3 月に成立した。AI をリスクの大きさで分類し、レベルに応じた要求事項を定めている。最上位には「許容できないリスク」と禁止事項が定められ、その次のレベルである「ハイリスク AI」では重要

[2] https://www.justice.gov/usao-nj/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

インフラや医療システムなどユースケースに制限が設けられることが規定された。また、中国では 23 年 7 月に「生成式人工知能サービス管理暫定弁法」が発表されたが、生成 AI の開発やサービスの提供にあたって、社会主義の核心的価値観の堅持すること、社会にもたらされ得る悪影響を抑制するための効果的な措置を講ずることといった国家への影響をコントロールすることに重点をおいている点に特徴がある。
こうした状況の中で日本は「広島 AI プロセス」を主宰するなど国際的議論の取りまとめを担いながら、国内では AI 事業者ガイドラインを策定するなど意欲的な働きをみせている。取りまとめ役という性質上、各国の姿勢に対してバランスのよい立ち回りを意識した国内制度設計が志向されるものと考えられ、国際的にビジネスを行う企業にとってはそれぞれのルールを把握したうえでの対応が求められることになりそうだ。

また、2023 年度は AI の議論においてサイバーセキュリティの論点の整理が進んだ年でもあった。AI に関する包括的な議論の一部としてではなく、AI へのサイバー攻撃を想定したセキュリティの議論と AI を悪用したサイバー攻撃を専門的に扱ったレポートやガイドラインが次々と発行された。AI の適正な利用に関する他の論点と比較した際、サイバーセキュリティの論点は AI 自身に対する脅威を扱うものであり、もし AI 自身のセキュリティが侵害されてしまえば公平性や透明性、安全性といったその他の原則が成り立つ基盤そのものが破壊されかねない点に決定的な違いがある。
また、セキュリティと AI といういずれも高度に専門的な技術的知見が要求される特徴のあるデュアルメジャー領域であるため、今後も個別に切り出された論点として専門的な検討が進む可能性は高いだろう。JCIC はこれに先駆けて「AI とセキュリティの論点とリスクシナリオの整理[3]」をレポートとして発刊している。AI セキュリティ領域の論点把握の参考としてご参照いただきたい。

まとめと 2024 年度の展望

全体的なトレンドとして大国間の地政学的な緊張の高まりを反映したサイバー空間上の衝突の増加と各国のサイバー防衛力の強化は継続するだろう。米英を中心に既に様々な計画は打ち出されており、今後はその実装と他国への波及的影響がポイントになると考えられる。デジタル規制においても、データ規制・デジタル機器・AI と様々な側面で国際的なパートナーシップとけん制関係が複雑に絡み合うことになるだろう。ある国同士が安全保障上の目標を共有しながらもデータに関する理念の違いからビジネス上の対立構造を招くような事態はそこかしこで発生するはずだ。

そして、24 年度の特筆すべきイベントとして挙げられるのは選挙だろう。11 月の米国大統領選の中間選挙に加え、6 月には欧州議会選挙が予定されており大きな節目となる。選挙戦における偽情報工作の影響や選挙結果が国家レベルのサイバー政策に与える影響など様々な面を注視する必要がある。日本国内でも 7 月の東京都知事選や解散があった場合の衆院選など大型の選挙イベントに対し、サイバーセキュリティ視点での議論が活発になる可能性がある。

[3] https://www.j-cic.com/pdf/report/AI-Security-Risk_JP.pdf

企業の視点からは、政府からの安全保障上のサイバーセキュリティ要請についての対応を検討することに加え、デジタル規制がビジネス環境に与える影響について機敏に適応していく必要があるだろう。現在の複雑な環境下では地域ごとのデジタル規制をビジネス戦略に反映するといった粒度は既に十分でないと考えられ、テーマごとに各国の姿勢や協力もしくは対立関係を把握し、対応をアップデートしていくことが望まれる。情報収集の質とそれを適切な対応に結び付けるためのサイクルは引き続き重要事項であり続ける。

最後にこれまで論じてきたポイントとは異なる着眼点から、情報セキュリティリスクの再評価について言及したい。JCIC ニュースクリップでは海外ニュースを扱う主旨から、国際的に影響のある政策やサイバー脅威を中心に取り上げている。しかし、ミスや内部犯行を原因とする情報セキュリティインシデントもまた各国企業で発生し続けている。

企業のサイバーセキュリティ対策への認識が高まり対策が進んでいる現状は歓迎されるべきものである。しかし、相対的に情報セキュリティ対策への重要性が見落とされてしまっていないかについては懸念がある。主に外部からの悪意あるサイバー攻撃への対応を想定するサイバーセキュリティでは、脅威の分析と即応性が重視される。企業の情報管理を PDCA サイクルで計画的に改善する情報セキュリティ管理とはその特徴や必要なリソース等も異なるもので新旧や優劣で論じられるべきものではない[4]。サイバーセキュリティ対策と情報セキュリティ対策の概念に誤解が生じていないか、人材の適正や育成、その他リソースの配分といった視点から今一度確認をする価値はあるだろう。

2. 各トレンドの代表的なニュースの振り返り

1） サイバー大国同士のつばぜり合いと周囲への波紋

1-a) 米国から中国への強力な反応に関するニュース

2023 年 6 月 20 日 米国司法省、国家安全保障局内に国家安全保障サイバー部門の新設を発表

米国司法省（DOJ）は、国家安全保障局内に新しい国家安全保障サイバーセクションである「NatSec Cyber」を創設することを発表した。今回の部門新設は 2022 年 7 月にモナコ司法副長官が行った包括的サイバーレビューの結果に基づいており、既に議会の承認を得ている。

NatSec Cyber は、悪意のあるサイバー活動を妨害する司法省の能力を強化するとともに、敵対的な国家による高度なサイバー攻撃の脅威に対処するための司法省内外のパートナーシップを推進する。

https://www.justice.gov/opa/pr/justice-department-announces-new-national-security-cyber-section-within-national-security

https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-g-olsen-delivers-remarks-hoover-institution-announcing

[4] 情報セキュリティとサイバーセキュリティの概念の成り立ち、歴史的な経緯については JCIC コラム「サイバーセキュリティと情報セキュリティの狭間にて」もご参照いただきたい。https://www.j-cic.com/pdf/report/InformationSecurity_Cybersecurity.pdf

2023 年 7 月 25 日 米国 CISA、選挙コミュニティ支援のため地方選挙セキュリティアドバイザーを設立

米国 CISA は、選挙コミュニティへの支援強化の一環で地方選挙セキュリティアドバイザー制度を設立した。

これまでは重要インフラ向けにセキュリティアドバイザーを配置していたが、今後は 10 の地方に専任の選挙セキュリティアドバイザーを設置する予定。

CISA は、選挙セキュリティアドバイザーは、州や地方の選挙管理者と CISA との間にさらに強力な関係性を構築するのに役立ち、過去数年間に CISA が行ってきた地方支援の取り組みをより発展させるものになると述べた。

https://www.cisa.gov/news-events/news/cisa-establishes-regional-election-security-advisors-strengthen-front-line-support-election

https://www.cisa.gov/director-easterlys-remarks-national-association-state-election-directors-summer-conference

2023 年 10 月 5 日 米国サイバー軍、敵対的なプロパガンダを特定する方法を公開

米国サイバー軍は、敵対的なプロパガンダを特定する方法に関する記事を公開した。敵対的な偽情報キャンペーンや影響力作戦は、その起点を知ることで特定できると説明している。

偽情報を広めるためにはボット、サイボーグ、トロール、ソックパペット、アンプリファイアなどと呼ばれる偽情報アクターが使われる。これらのアクターを特定するためには、最近作成したアカウントで繰り返し投稿が行われていること、フォロワーが 100 人未満のアカウントで個人的な更新がないこと、実在のユーザーを模倣しているかどうかといった観点で特定が可能だとしている。

また、偽情報を特定する方法としてプロパガンダのエコシステムを検出することを挙げ、そのことが信頼できる情報源を検証することにもなるという。Global Engagement Center が公開したウェブサイト Disarming Disinformation (www.state.gov/disarming-disinformation/) には、すでに特定されているプロパガンダエコシステムを説明するリソースが公開されている。

https://www.cybercom.mil/Media/News/Article/3551070/dont-be-a-target-how-to-identify-adversarial-propaganda/

2024 年 1 月 31 日 米国 CISA 長官、下院特別委員会で中国のサイバー脅威から国家を守るための取組について発言

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）の長官であるジェン・イースタリー氏が、米国と中国共産党の戦略的競争に関する下院特別委員会で中国がもたらすサイバー脅威から国家を守るための CISA の取り組みについて発言した。「CISA、NSA、FBI、業界パートナーによって中国の悪質な活動が明らかになったことから、CISA はこの脅威が現実的かつ緊急であることを認識し、現在行動している」と述べた。

サイバーセキュリティによって国家安全保障は重大な岐路にあるとの見解を示し、緊急の呼びかけをおこなった。

https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

2024 年 3 月 19 日 米国 CISA ら、中国の Volt Typhoon によるサイバー活動について共同ファクトシートを発表

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、国家安全保障局（NSA）、連邦捜査局（FBI）、その他多くの国際パートナー（オーストラリア、カナダ、英国、ニュージーランド当局など）と共同で、ファクトシート「中国の国家支援型サイバー活動：重要インフラリーダーのための行動」を発表した。Volt Typhoon の活動に関連する詳細な情報を提供し、特に米国の通信、エネルギー、輸送システム、上下水道システム部門の組織に対して、どのように侵害に成功したかを解説している。

また、Volt Typhoon がもたらす緊急のリスクを重要インフラのリーダーに向けて警告し、脅威活動から組織を保護するために優先すべき行動のガイダンスを提供している。

https://www.cisa.gov/news-events/alerts/2024/03/19/cisa-and-partners-release-joint-fact-sheet-leaders-prc-sponsored-volt-typhoon-cyber-activity

https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders

2024 年 3 月 20 日 米国下院、「外国敵対勢力から米国人のデータを保護する法案」を全会一致で承認

米国下院は、「外国敵対勢力から米国人のデータを保護する法案（H.R.7520）」を全会一致で承認した。この法案は、データブローカーと呼ばれる個人データの販売で利益をあげている組織もしくは個人が、「外国敵対勢力」が支配する企業・団体・個人に対して米国人の機密データを販売・共有することを禁止するもの。外国敵対勢力の定義は合衆国法典の規定を参照しており、現在は北朝鮮、中国、ロシア、イランの名が挙げられている。

背景として、米国では 2024 年 2 月に「懸念国家による悪用から米国人の機密データを保護するための大統領令」が発令され、司法省・国土安全保障省・保健福祉省・国防省などに予防措置を命じていた。

違反した場合は連邦取引委員会（FTC）法違反として扱われ、FTC には違反 1 件につき罰金 5 万ドル（約 750 万円）以上の民事罰を請求する権利が与えられる。発効日は法案の制定日から 60 日後として定義されている。

同法案における機密データとして位置付けられた情報には次のようなものがある。政府発行の ID、個人の健康医療情報、財務情報、生体遺伝子情報、位置情報、私的通信情報、デバイスやアカウント情報、性的嗜好情報、デバイス内の情報・ログ・写真・動画、17 歳未満の個人情報、人種・宗教、オンライン活動情報、軍隊情報、他。

https://clerk.house.gov/Votes/202491

https://energycommerce.house.gov/posts/

https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/evo-media-document/DATA_BROKERS_01_xml_0.pdf

https://www.justice.gov/opa/pr/justice-department-implement-groundbreaking-executive-order-addressing-national-security

1-b) 米国と他国によるサイバー安全保障に係る共同リリース

2023 年 9 月 27 日 日米両国、中国を背景とする攻撃グループ BlackTech に対する共同勧告

米国 NSA、FBI、CISA および日本の警察庁、内閣サイバーセキュリティセンターは、中国を背景とするサイバー攻撃グループ「BlackTech」に対する共同勧告を発表した。

現在、BlackTech による政府や防衛、科学技術、メディア、電機電子、通信、製造業などの事業体が利用するルーターのファームウェアへ潜伏を試みるサイバー活動が観測されていることを報告し、注意を促している。

戦術的分析の詳細では、BlackTech の今回の手口と特徴を次のように説明している。

（1）ルーターの設定を変更・ログ機能を無効化して隠蔽 （2）ルーターのファームウェアを変更してバックドアの永続性を確立 （3）ルーターのドメイン管理機能を悪用して海外子会社と国内本社のネットワーク間を横移動 （4）様々な OS とネットワークの通常活動に偽装して EDR 製品による検出を回避

また、推奨される対応として、多国籍企業はすべての子会社との接続の見直し、アクセスの検証、ゼロトラストモデルの導入をして潜在的な侵害の範囲を限定する必要性があると強調している。

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3539209/us-and-japanese-agencies-issue-advisory-about-china-linked-actors-hiding-in-rou/

https://media.defense.gov/2023/Sep/27/2003309107/-1/-1/0/CSA_BLACKTECH_HIDE_IN_ROUTERS_TLP-CLEAR.PDF

https://www.cisa.gov/news-events/alerts/2023/09/27/nsa-fbi-cisa-and-japanese-partners-release-advisory-prc-linked-cyber-actors

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a

2023 年 9 月 29 日 米国 CISA と英国 NCSC、市民社会のサイバーセキュリティについて戦略対話を開始

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）と英国国家サイバーセキュリティセンター（UK-NCSC）は、国境を越えた脅威にさらされている市民社会のサイバーセキュリティに関する戦略対話の初会合を開催した。戦略対話では、8 カ国（米国と英国に加えて、オーストラリア、カナダ、エストニア、日本、ニュージーランド、ノルウェー）が集まり、市民社会のサイバーセキュリティを推進する方法を議論した。特に高リスクコミュニティ（HRC）のサイバーレジリエンスを支援する将来の取り組みの優先順位を議論し、各参加国が取り組んでいくことを確認した。

https://www.cisa.gov/news-events/news/cisa-and-uk-ncsc-hold-inaugural-meeting-strategic-dialogue-cybersecurity-civil-society-under-threat

2023 年 10 月 16 日 米国財務省、アラブ首長国連邦とのサイバーセキュリティ協力覚書を締結

米国財務省およびアラブ首長国連邦（UAE）サイバーセキュリティ評議会は、サイバーセキュリティ協力に関する二国間覚書（MoU）が締結されたことを発表した。

2021 年 11 月に米国財務副長官がアラブ首長国連邦を訪問した際に金融セクターの重要インフラを保護するための二国間パートナーシップ確立の必要性が議論され、今回の MoU 締結のきっかけとなった。

国際金融の健全性を守るためにサイバーセキュリティに関する協力を深めることを目的とし、具体的には以下の分野での協力を強化する。

・サイバー脅威およびインシデントに関する情報を含む、金融セクター関連情報の共有

・サイバーセキュリティ分野での協力を促進するためのスタッフの研修と調査訪問

・国境を越えたサイバーセキュリティ演習実施などの能力開発活動

https://home.treasury.gov/news/press-releases/jy1808

2023 年 11 月 9 日 米韓当局、サイバー脅威情報とベストプラクティスの共有について覚書を締結

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）はと韓国国家情報院（NIS）は、両国間でのサイバー脅威情報とサイバーセキュリティのベストプラクティスの共有に関する覚書に署名した。

署名された覚書に基づき、米国と韓国はそれぞれ次のことを実施する。

・サイバーセキュリティの脅威に対応するための技術的能力とメカニズムについて定期的に協議し、それぞれの緊急対応チーム（CERT）間のコミュニケーションを強化する

・重要インフラのサプライチェーンの回復力に関して協力する

・共同演習、専門家レベルの交流、トレーニングを通じて、サイバーおよび重要インフラ領域全体でベストプラクティスを共有する

・AI などの新しいテクノロジーを管理するポリシーに関するベストプラクティスを共有する

https://www.cisa.gov/news-events/news/cisa-signs-memorandum-understanding-republic-korea-share-cyber-threat-information-and-cybersecurity

2024 年 2 月 26 日 英国 NCSC とファイブアイズ同盟国、ロシアの高度標的型攻撃グループによるクラウド環境への攻撃に警鐘

英国の国家サイバーセキュリティセンター（NCSC）とファイブアイズのパートナー（米国、オーストラリア、カナダ、ニュージーランドの当局）は、ロシアの対外情報庁（SVR）を背景とする高度標的型攻撃グループ「APT29」が、クラウドホスト環境に移行した組織を標的とするために、情報窃取の戦術を更新したとしてその詳細を報告するとともに警戒を促した。

今回のアナウンスでは、攻撃者がクラウド環境への初期アクセスを獲得するためにクラウドサービス自体への攻撃もスコープに入れた手口を用いる点に進化が見られるとしている。多要素認証疲れと呼ばれる不正アクセス手法や家庭用ルーターを悪用したアクセス元偽装の手口などの詳細が解説され、これらの攻撃を検知するための助言がまとめられている。

https://www.ncsc.gov.uk/news/uk-allies-expose-evolving-tactics-of-russian-cyber-actors

https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access

1-c) サイバー安全保障を起点とする大きな政府政策

2023 年 4 月 13 日 米国 CISA ら、共同文書「サイバーセキュリティリスクのバランスをシフトする」を公開

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、連邦捜査局（FBI）、国家安全保障局（NSA）、およびオーストラリア、カナダ、イギリス、ドイツ、オランダ、ニュージーランドのサイバーセキュリティ当局との共同ガイダンス「サイバーセキュリティリスクのバランスをシフトする（セキュリティ・バイ・デザイン アンド デフォルト の原則とアプローチ）」を公開した。

このガイダンスは、技術的な推奨事項に加えて、製品を開発、構成、および出荷する前に、ソフトウェア開発企業がソフトウェアセキュリティを設計プロセスに組み込む際の指針となる原則について概説している。

また、技術を提供する側がサイバーセキュリティに対する説明責任を負い、業界のパートナーと協力してセキュリティ・バイ・デザイン アンド デフォルトの慣行を促進するための組織向けアドバイスも含まれている。

セキュリティ・バイ・デザイン アンド デフォルトの 3 つの指針の内容は以下の通り。

「1.セキュリティの負担を顧客だけに追わせるべきではなく、ソフトウェア開発企業が責任を持って製品を改善しなければならない」「2.透明性と説明責任を受け入れる。安全でセキュアな製品を提供することに誇りを持ち、他のメーカーと差別化する必要がある」「3.目標を達成するために、組織とリーダーシップを構築する」

https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default

https://www.ncsc.gov.uk/news/uk-and-international-partners-share-advice-to-help-turn-dial-on-tech-product-security

2023 年 7 月 26 日 米国 SEC、重大なサイバーインシデントを 4 日以内に開示するよう義務付ける新規則

米国 SEC は新たなサイバーセキュリティ規則を採択し、重大なサイバーインシデントの 4 日以内の開示やサイバーリスク管理に関する情報の年次開示を義務付ける。規則は、連邦官報への掲載から 30 日後に発効する。

新規則の下では、米国の上場企業は発生したサイバーインシデントが「重大」であると判断した時点から 4 日以内に開示しなければならない。また、インシデントの特徴、範囲、時期、影響または「合理的に起こりうる重大な影響」に関する詳細を Form 8-K に従って開示することを求められる

さらに、サイバーリスク管理について、サイバー脅威のリスクに対する取締役会のガバナンス、重大なリスクの評価と管理における経営陣の役割と専門知識についての説明が求められることとなり、Form 10-K に従った年次報告が義務付けられる。

なお、米国で事業を行う他国の非公開企業に対しても、重大なサイバーインシデントは Form 6-K に、サイバーリスク管理情報については Form 20-F に従い同等の開示を行うことを求めている。

https://www.sec.gov/news/press-release/2023-139

https://www.sec.gov/files/rules/final/2023/33-11216.pdf

2023 年 9 月 19 日 米国土安全保障省、重要インフラ事業者のサイバーインシデント報告の調和に向けた勧告を発表

米国国土安全保障省（DHS）は、連邦政府が国の重要インフラをより適切に保護するためにサイバーインシデントの報告を合理化し、調和させる方法に関する一連の実用的な推奨事項の概要を発表した。

これらの推奨事項は、重要インフラパートナーの負担を軽減し、連邦政府がサイバーインシデントの傾向をより適切に特定できるようにするための明確な道筋を提供するとともに、組織が攻撃を防止、対応、回復できるように支援する。

議会に提出された報告書による勧告は、画期的な「重要インフラのためのサイバーインシデント報告法（CIRCIA）」の要件である。主な勧告には、報告可能なサイバーインシデントのモデル定義、タイムライン、トリガーの確立、連邦機関が採用できるサイバーインシデント報告フォームのモデル作成、単一の報告ウェブポータルの可能性の評価を含むサイバーインシデントに関する情報の報告と共有の合理化などが含まれる。

https://www.dhs.gov/news/2023/09/19/dhs-issues-recommendations-harmonize-cyber-incident-reporting-critical

2023 年 11 月 10 日 米国証券取引委員会、証券法などへの違反で SolarWinds 社および CISO を告発

米国証券取引委員会（SEC）は、サイバーセキュリティリスクに関連した詐欺防止規定と報告・内部統制規定違反で SolarWinds 社および同社 CISO のブラウン氏を告発した。

同社製品の SolarWinds Orion を標的としたサイバー攻撃「SUNBURST」への対応に関連して、1933 年証券法と 1934 年証券取引法の詐欺防止規定、および証券取引法報告と内部統制規定の違反があるとして、ニューヨーク南部地区連邦裁判所に訴状を提出した。SolarWinds 社とブラウン氏は、IPO から攻撃発覚までの間にサイバーセキュリティ対策に欠陥があることを認識していたにも関わらず対策を過大評価し、SEC に提出した書類でも既知のリスクを過小評価または開示せず、結果として投資家を欺いたと主張している。

訴状はサイバーセキュリティにおける CISO の役割を理由に、ブラウン氏に対して恒久的な差止命令による救済、予見利息を伴う遺贈、民事処罰、役員および取締役の資格停止を求めている。

https://www.sec.gov/news/press-release/2023-227

2023 年 12 月 8 日 中国 CAC、「サイバーセキュリティインシデント報告管理弁法（案）」を公開

中国国家インターネット情報弁公室（CAC）は、「サイバーセキュリティインシデント報告管理弁法（案）」を公開した。中国国内でネットワークの構築・運営、サービス提供する事業者に対し、サイバーセキュリティに危害を及ぼすインシデントの報告義務を規定したもの。

「サイバーセキュリティインシデント分類ガイドライン」におけるインシデント分類が 重大／特に重大 に該当する場合は、通報から 1 時間以内に管轄当局へ『ネットワークセキュリティインシデント情報報告書』の提出が必要。特に、重要情報インフラの 重大／特に重大な インシデントは、通報から 1 時間以内に、国家インターネット情報部門と国務院公安部門への報告義務がある。非重要インフラ運営者の場合は地方のインターネット情報部門へ、犯罪行為の疑いが

ある場合は公安への報告が必要。1 時間以内にインシデントの原因、影響、傾向等が把握できない場合は、組織名や発生した施設などを部分報告した後、24 時間以内にその他の状況を報告することも可能。

http://www.cac.gov.cn/2023-12/08/c_1703609634347501.htm

2024 年 1 月 3 日 欧州中央銀行、銀行向けにサイバー攻撃からの復旧能力テスト実施を発表

欧州中央銀行（ECB）は直接監督下にある銀行 109 行を対象に、サイバー攻撃時の効果的な緊急対策が講じられているかどうかを判断するため、初の復旧能力テストを実施すると発表した。

今回の取り組みは、2023 年 11 月に発表された銀行の IT リスク管理に関する ECB の評価を受けたもの。テストでは、銀行がサイバー攻撃を防ぐ能力ではなく、銀行の通常業務を中断させる攻撃が成功したシナリオをシミュレートする。銀行が攻撃を受けた後の緊急時対応手順や緊急時対応計画の発動、通常業務の復旧など、サイバー攻撃にどの程度対処し、復旧できるかが評価される。

さらに、代表 28 行が重点評価を受け、サイバー攻撃への対処方法についてさらなる詳細の提出を求められる。他の監督活動との連携が十分かどうかも評価される。

テスト結果は、2024 年に行われるより広範な監督当局のレビューと評価に利用される。主な成果は 2024 年夏に公表される予定。

https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.en.html

https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl231115.en.html

2024 年 2 月 12 日 米国 FCC、通信事業者に対して攻撃発見から 7 日以内の報告を義務付ける規則を確定

連邦通信委員会（FCC）は、通信事業者に対して攻撃発見から 7 営業日以内に FCC へ報告することを義務付け、データ漏洩があれば FBI と米国秘密情報局にも報告することを求める規則を確定した。加えて、通信事業者が顧客へ通知するまでの必須待機期間を廃止し、対象データの侵害について連邦機関への通知した後、漏えいがあったとみられる日から 30 日以内に顧客へ通知することを義務付ける。

本規則は、情報漏えい通知規則の適用範囲を拡大し、CPNI（Customer Proprietary Network Information）だけでなく、すべての PII（Personally Identifiable Information）を対象とする。電気通信事業者における「情報漏えい」の定義を拡大し、不注意による顧客情報へのアクセス、使用、開示を含めるという提案が採択された。また、電気通信事業者以外にも、相互接続された VoIP サービス事業者および電気通信中継サービス事業者は、機密性の高い顧客情報を保護する義務において説明責任を果たし、顧客が自身を保護する手段を提供する必要があるとして、FCC がこれらの事業者にも本規則を適用する権限があるという結論を示した。

https://www.federalregister.gov/documents/2024/02/12/2024-01667/data-breach-reporting-requirements

2024 年 3 月 7 日 米国 CISA、オープンソースエコシステムの安全性を確保するための新たな取り組みを発表

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、オープンソースソフトウェア（OSS）コミュニティのリーダーを招集した 2 日間の OSS セキュリティサミットの中で、オープンソースエコシステムの安全性を確保するための新たな取り組みを発表した。サミットでは、オープンソースの脆弱性への対応に関する机上演習やパッケージマネージャーのセキュリティに関するラウンドテーブルディスカッションが行われた。

CISA はパッケージリポジトリと緊密に連携し、パッケージリポジトリが遵守すべきセキュリティ原則の採用を促進していく考えを示した。これは、オープンソースセキュリティ財団（OpenSSF）のセキュリティ保護ソフトウェアリポジトリワーキンググループが 2 月に公開したベストプラクティス集で、セキュリティ成熟度の自己評価のための枠組みなどが解説されている。

https://www.cisa.gov/news-events/news/cisa-announces-new-efforts-help-secure-open-source-ecosystem

https://www.cisa.gov/news-events/alerts/2024/02/08/cisa-partners-openssf-securing-software-repositories-working-group-release-principles-package

https://repos.openssf.org/principles-for-package-repository-security

1-d) サイバー安全保障から経済安全保障への波及

2023 年 4 月 17 日 英国政府の「オンライン安全法案」に対し、WhatsApp、Signal など 5 社が公開書簡で抗議

メッセージングアプリ大手の WhatsApp、Signal などの 5 社は、英国政府が現在検討中のオンライン安全法案への抗議を示す共同書簡を一般公開した。

5 社は、提出された草案が採用されれば本来意図された受信者以外がメッセージの内容を盗聴することを防ぐプライベートメッセージングサービスのエンドツーエンド暗号を解読するようテクノロジー企業へ強制し、エンドツーエンド暗号を実質的に非合法化するために利用される可能性があると批判した。また、通信規制当局である OFCOM が個人メッセージの積極的スキャンを強制することが可能となり、ユーザーのプライバシーが損なわれかねないと抗議した。

https://blog.whatsapp.com/an-open-letter

https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation

https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk

2023 年 5 月 11 日 米国政府、Rockwell Automation China のソフトウェアに対するセキュリティ調査を開始

米国のオートメーション大手 Rockwell Automation が、同社の中国拠点からの不正アクセスの可能性について米国政府から調査を受けていると報じられた。

大連にある同社施設のひとつから、米国の重要インフラや軍事施設などへのアクセスを可能にする脆弱性の有無が確認されているという。

調査は初期段階にあり、当該施設に勤務している従業員に着目しており、エネルギー省、国防省、司法省の商事訴訟部門など様々な関係者が調査対象になっているという。Rockwell の広報担当者は、ソフトウェアが侵害されたという報告

はないとし、中国で製造されたコードも必ず米国での脆弱性試験を経て提供されていると説明した。Rockwell は米軍や米国の重要インフラ事業者向けに広くサービスを提供しており、報道の翌日同社の株価は 1%以上低下した。

https://www.wsj.com/articles/automation-giant-faces-u-s-government-probe-over-china-operations-e12c831f?mod=latest_headlines

https://www.reuters.com/technology/rockwell-automation-faces-us-government-probe-over-china-ops-wsj-2023-05-10/

https://au.investing.com/news/stock-market-news/rockwell-automation-facing-us-investigation-over-operations-in-china--wsj-432SI-2865106

2023 年 5 月 21 日 中国 CAC、米大手半導体メーカーマイクロン社製品のサイバーセキュリティ審査不合格を発表

中国国家インターネット情報弁公室（CAC）は、米大手半導体メーカーのマイクロン社の製品がサイバーセキュリティ審査において不合格になったと発表した。

今回の審査は本年 3 月に実施通達が出されていたもので、実施の理由について CAC は「中国国内で販売される製品のサイバーセキュリティ上の問題により、中国の重要情報インフラの安全が脅かされることを防ぐことが目的であり、国家安全の維持のために必要な措置」と説明していた。

審査結果には「同社製品には深刻なサイバーセキュリティ上の問題があり、中国の重要情報インフラのサプライチェーンへの潜在的なリスクと、中国の国家安全保障に影響を及ぼすことが判明した」と記載されている。さらに、サイバーセキュリティ法等に基づき、中国国内の重要情報インフラの運営者に対してマイクロン製品の購入中止が要請された。

http://www.cac.gov.cn/2023-05/21/c_1686348043518073.htm

http://www.cac.gov.cn/2023-03/31/c_1681904291361295.htm

2024 年 1 月 17 日 中国発ファストファッション EC の「SHEIN」、米国での IPO に向けサイバーセキュリティ審査開始

中国発のファストファッション EC プラットフォームの運営を手掛ける「SHEIN」に対し、米国市場での新規株式公開（IPO）のためのサイバーセキュリティ審査がされた。SHEIN は、中国政府に対して米市場での IPO の承認を申請しており、これに応じて中国のサイバーセキュリティ規制当局である CAC が審査を開始した形。

SHEIN は現在 150 以上の国や地域でサービスを展開しているが、中国国内におけるデータの取り扱いと共有、国外へのデータ流出、国外からの不正アクセスに対する保護能力などについて調査が進められているという。調査対象のデータについては従業員や取引先の管理に関するものも含まれるという。

米誌報道によれば、IPO 手続きの一環として SHEIN がワシントンの規制当局に開示することになる中国関係のデータの種類についても中国当局は関心を持っているとみられている。

https://www.cnbc.com/2024/01/17/china-launches-security-review-of-shein-ahead-of-ipo.html

https://www.wsj.com/world/china/fashion-giant-faces-new-ipo-hitch-chinas-cybersecurity-police-70c57561

https://www.reuters.com/business/retail-consumer/shein-files-with-chinese-regulator-planned-us-float-sources-2024-01-12/

https://www.asiafinancial.com/shein-facing-cybersecurity-review-in-china-ahead-of-us-ipo

2024 年 3 月 13 日 米国議会下院、中国 ByteDance 社に対し TikTok 事業の売却を迫る法案を可決

米国議会下院は、中国 ByteDance 社が運営する動画共有アプリ TikTok を「敵対国による安全保障上の脅威」と認定し、180 日以内に米国内事業を売却しない場合にアプリ配信などを禁止する法案を可決した。法案は今後上院で審議されることになる。

TikTok の周 CEO は、TikTok 事業を守るために法的措置を含めた対応を検討中であるとコメントした。また、中国商務省も翌 14 日の記者会見で米国の姿勢が市場経済と公平競争の原則に反すると非難し、外国企業の不当な抑圧をやめない場合は中国の国益を守るためのあらゆる措置を講じると述べた。

https://edition.cnn.com/2024/03/13/politics/house-vote-tiktok-ban-bill/index.html

https://edition.cnn.com/2024/03/14/tech/china-reactions-tiktok-potential-ban-intl-hnk/index.html

2） デジタル保護主義の新しい段階

2-a) デジタルデバイスへの規制の拡大

2023 年 6 月 6 日 英国政府、調達法の修正案を提出　国家安全保障に危険を及ぼすサプライヤーを調査する専門部署を設置

米国サイバーセキュリティ・インフラセキュリティ庁は、中国製の無人航空機システム（UAS）に関するサイバーセキュリティガイダンスを発表した。

英国政府は、調達法の修正案を提出し、調達に関係する国家安全保障部門を内閣府に設置することを提案する。

同部門は、情報機関と緊密に連携しながら国家安全保障にリスクをもたらす可能性のあるサプライヤーを調査し、公的調達から排除すべきか評価する。

リスクが認められたサプライヤーを防衛や国家安全保障などの特定分野の調達から追放することを求める一方、機密性のない分野では調達の継続を認める新たな権限の設置も提案されている。

英国政府は 2022 年 11 月に、中国の国家情報法の適用を受ける企業が製造した監視カメラを政府の機密性の高い現場から撤去するスケジュールを公表することを約束していた。これを受けて中国国営の CCTV メーカーのキットが撤去される予定で、米国とオーストラリアではすでに中国製カメラの撤去が命じられている。

https://www.gov.uk/government/news/procurement-bill-strengthened-to-protect-national-security

https://bills.parliament.uk/bills/3159

https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386?module=inline&pgtype=article

2023 年 6 月 21 日 米国国土安全省、国土安全保障調達規則の改正に関する最終規則を発表

米国国土安全保障省（DHS）は、国土安全保障調達規則（HSAR）の改正に関する最終規則を発表した。この最終規則は、機密情報以外の重要情報（CUI）の保護を目的に既存の条項の改定と新しい条項の追加を行うものである。

新条項は、一般的な CUI 取り扱い要件、連邦情報システムに対する運用権限要件、インシデントの報告と活動の要件、政府関連ファイルおよび情報の無毒化という 4 つの要件を規定している。

連邦情報システムに対する運用権限要件では、請負業者の情報システムが政府に代わって運用されていると政府が判断した場合、その情報システムは連邦情報システムとみなされ、NIST SP 800−53 の適用対象となる。それ以外の場合は、SP 800-171 が適用される。

また、インシデントの報告要件では、個人識別情報 （PII）または機密個人識別情報 （SPII）に関係するインシデントは発見から 1 時間以内に報告することを求める。その他のインシデントは発見から 8 時間以内に報告する必要がある。

https://www.federalregister.gov/documents/2023/06/21/2023-11270/homeland-security-acquisition-regulation-safeguarding-of-controlled-unclassified-information

2023 年 7 月 18 日 米国ホワイトハウス、スマートデバイス向けサイバーセキュリティラベル表示プログラムを発表

米国ホワイトハウスは、米国民が安全でサイバー攻撃に対して脆弱性を持たないスマートデバイスをより簡単に選択できるように目的で、サイバーセキュリティ認証・セキュリティラベル表示プログラムを発表した。

提案された「サイバートラストマーク」プログラムは、スマート冷蔵庫、スマート電子レンジ、スマートテレビ、スマート空調システム、スマートフィットネストラッカーなどを含む消費者向けデバイス全体のサイバーセキュリティの水準を引き上げることが狙い。Amazon、Best Buy、Google、LG Electronics USA、Logitech、Samsung Electronics などのデバイスメーカー、小売業者らがプログラムの支持を表明し、推進の取り組みを発表している。

無線通信機器の規制を所掌する連邦通信委員会（FCC）は、プログラムについてのパブリックコメントを募集し、2024 年までに実施したいとの考えを示している。

https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/

https://docs.fcc.gov/public/attachments/DOC-395185A1.pdf

2024 年 1 月 17 日 米国 CISA、「中国製無人航空機システムに関するサイバーセキュリティガイダンス」を発表

米国サイバーセキュリティ・インフラセキュリティ庁は、中国製の無人航空機システム（UAS）に関するサイバーセキュリティガイダンスを発表した。

米国において UAS への依存度が高まっていることをうけ、重要インフラ事業者とそのパートナー組織向けに中国製 UAS がもたらす脅威に警鐘を鳴らすことを目的としているという。知的財産や機密情報を標的とする中国の積極的なサイバー作戦に関する緊急注意を促し、適切なサイバーセキュリティ対策なしに UAS が運用された場合に起こり得る結果

の概要とネットワークや機密情報に対するリスクを低減するための推奨策を案内している。CISA は、UAS を調達・運用するすべての組織がガイダンスを確認し、リスクを軽減するための行動を取るように奨励した。

https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators

https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-chinese-manufactured-uas

2024 年 1 月 31 日 欧州委員会、コモンクライテリアに基づく EU サイバーセキュリティ認証スキームを採択

欧州連合サイバーセキュリティ庁（ENISA）によって起草されたコモンクライテリアに基づく欧州サイバーセキュリティ認証スキーム（EUCC）が、EU サイバーセキュリティ認証フレームワーク内の最初のスキームとして欧州委員会に採用された。

新しいスキームの下で ICT サプライヤーは、EU 域内の共通認識となる評価プロセスを経て、技術コンポーネント（チップ、スマートカード）・ハードウェア・ソフトウェアなどに EUCC 認証を取得することができる。現在 ENISA は、EUCC の他にも 2 つのサイバーセキュリティ認証スキーム（クラウドサービスに関する EUCS、5G セキュリティに関する EU5G）に取り組んでいる。

https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme

2024 年 2 月 27 日 中国全人代、改正国家機密保護法を採択 5 月 1 日から施行

中国全人代は国家機密保護法の改正案を採択し、5 月 1 日から施行すると発表した。2010 年 4 月以来となる同法の改定は、中国からみた内外情勢の変化と科学技術の発展によりもたらされる新たな課題への対処をめざす目的があると説明している。

科学技術の自立と改善が中国の国力と国家安全の礎という見解に基づき、国家機密・主権・発展利益の保護のために秘密保護技術の革新を支援するための新規定が追加された。また、国家機密保持規定に従ったシステム計画・構築・運用・維持・定期的なリスク評価の実施と監督体制を整えることが義務付けられた。さらに、セキュリティ製品と技術設備を「国家機密の保護における不可欠かつ重要な技術支援」と位置づけ、秘密保護規定と基準の遵守に関する抜き打ち検査や再検査の制度を定めている。

http://www.npc.gov.cn/npc/c2/c30834/202402/t20240228_434899.html

http://www.npc.gov.cn/npc/c2/c30834/202402/t20240228_434897.html

http://www.npc.gov.cn/npc/c2/c30834/202402/t20240228_434895.html

2-b) データ流通を委縮させないための現実的な規制への調整

2023 年 7 月 10 日 欧州委、米国との新データプライバシーフレームワークの十分性を認定、7 月 11 日より発効

欧州委員会は、米国との間に新たなデータプライバシーフレームワークの十分性を認定した。米国当局が 7 月 3 日に最終化した「新たなデータプライバシーの枠組み（新 DPF）」を、欧州委が認定した形。新 DPF は、米国大統領令

（EO.14086）に基づく形で作成されており、欧州委はデータ保護審査裁判所（DPRC）の設置などにより米国の諜報機関による域内の個人データへのアクセスを必要かつ適切なものに制限し、拘束力のある救済措置が導入されていると評価。新 DPF は米国に移転される個人データに対して欧州経済領域（EEA）と同等の保護レベルを提供するものであると結論付け、7 月 11 日に発効した。

今後、新 DPF に違反してデータ収集されたと米国の DPRC が判断した場合は、当該組織にデータの削除を命じることができる。EU の個人が米国組織により不当にデータが取り扱われたと判断した場合には、無償の解決支援制度や仲裁パネルを利用できる。

新 DPF は、この枠組みに参加している米国組織へのデータ移転を対象としている。米国の組織はプライバシーの保護義務を遵守することで参加可能となる。

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

https://www.dataprivacyframework.gov/s/data-protection-authorities

2023 年 9 月 5 日 韓国国務院、個人情報保護法施行令の改正を承認　9 月 15 日より一部施行

韓国国務院は同国の個人情報保護法施行令の改正を承認し、9 月 15 日より一部施行することを発表した。

一部施行される「個人情報保護法およびその改正施行令」には、様々な分野にわたる個人情報処理基準を統一する規則が盛り込まれている。個人情報の処理過程で遵守すべき事項に多くの変化が予想されることから、韓国個人情報保護委員会は改正事項を入念に確認するよう注意喚起した。改正施行令による主な変更点は以下の通り。なお、個人情報の転送要求などの事項は、10 月から段階的に立法予告が行われる予定。

1. 公共安全や緊急救助時も情報主体である国民の権利を原則保障
2. 映像およびオン／オフラインの情報処理をデジタル基準に一元化（「同一行為同一規制原則」）
3. 主要公共システム運営機関などにおける個人情報処理の安全性確保措置
4. 個人情報の国外移転と課徴金制度に国際基準を反映（違反に関連した事業の売上から全体売上に基準を変更。中小向けには分割納付を考慮）

デジタル基準への一元化について、デジタル基準では（1）個人情報の利用・提供内容の通知、（2）14 歳未満の個人情報の収集、（3）個人情報の流出などの申告・通知、（4）安全措置基準、（5）制裁 の 5 点が定められている。今回の施行令では、ドローンや自律走行車など移動型映像情報処理機器を通じて業務目的の映像撮影をする際、撮影事実を十分に知らせた場合（案内板、音声などによる告知）には、情報主体が拒否の意思を示さない限り撮影可能とする例が示された。

https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9145

2023 年 9 月 28 日 中国国家インターネット弁公室、「国境を越えるデータの流れの規制と促進に関する規定」の草案を公開

中国国家インターネット弁公室（CAC）のインターネットデータ管理局は、「国境を越えるデータの流れの規制と促進に関する規定」の草案を公開した。

今回の草案では、本規定はデータや個人情報の国外提供に関する「安全評価弁法」「標準契約弁法」に優先するものと位置付けられ、安全評価の申告、標準契約の締結、個人情報保護認証の合格に関する例外条件が複数定められている。例えば、（1）本人が当事者となる契約を締結・履行するために、個人情報を国外に提供しなければならない場合（海外からの買い物、支払、航空券予約など）（2）従業員の個人情報を国外に提供する必要がある場合（3）1 年以内に国外に個人情報を提供する見込みがある場合（取り扱う情報の規模により条件が異なる）（4）自由貿易試験区でネガティブリスト（データ輸出安全評価、個人情報輸出標準契約、個人情報保護認証の管理範囲に含める必要のあるデータのリスト）を作成し、当局の承認を得ている場合 等を例外として扱う案となっている。

http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm

2024 年 1 月 17 日 米国連邦取引委員会、データプライバシーとセキュリティに関するグローバル協定へ参加

米国連邦取引委員会（FTC）は、データプライバシーとセキュリティに関する多国間協定「Global CAPE」への参加に合意した。Global CAPE は、APEC（アジア太平洋経済協力会議）の越境プライバシー規則である「APEC CBPR」を補完するために創設された協定で、新たに APEC 以外の国も参加できるようになった。FTC は、Global CAPE に参加することで加盟各国の個人情報保護当局とは個別に覚書を締結することなく、データプライバシーおよびセキュリティ法執行の問題に関する調査協力、情報共有などを行うことが可能となる。

https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-signs-multilateral-arrangement-bolster-cooperation-privacy-data-security-enforcement

https://www.globalcbpr.org/wp-content/uploads/Global-CAPE-2023.pdf

2024 年 3 月 22 日 中国国家インターネット情報局、「国境を越えるデータの流れの促進と規範に関する規定」を発表

中国国家インターネット情報局（CAC）は、「国境を越えるデータの流れの促進と規範に関する規定」を発表した。

データの越境移転に関する制度に関連する「重要データ」の申告基準を最適化したもの。

管轄部門や当局が対象のデータを重要データとして通知・公表していない場合、データ越境移転安全評価の申告が不要であることを明確にした。さらに、次の事項に該当する場合も安全評価の申告、個人情報輸出標準契約、個人情報保護認証が免除されることが明文化された。

・貿易、国際輸送、学術協力、国境を越えた製造・販売で収集・生成された中国国外で提供されるデータで個人情報や重要なデータを含まない場合

・国外で収集・生成した個人情報が処理のために国内に持ち込まれ、再び国外提供される場合で、処理中に国内の個人情報や重要なデータを含まない場合

・契約の締結・履行の当事者が個人情報を国外に提供する必要がある場合

・国境を越えた人事管理で従業員情報の国外提供が真に必要な場合

・重要情報インフラ事業者であらず、当年 1 月 1 日以降に国外提供した（機微でない）個人情報の累計が 10 万人未満の場合

また、安全評価の有効期間と延長申請、データ安全保護義務や監督責任などの詳細についても規定された。

https://www.cac.gov.cn/2024-03/22/c_1712776612187994.htm

https://www.cac.gov.cn/2024-03/22/c_1712776612187994.htm

https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm

3） サイバー犯罪に対する国際捜査の成果

2023 年 4 月 5 日 ユーロポール、盗まれた認証情報を販売していたダークウェブ市場「Genesis Market」を閉鎖

ユーロポールは、米国連邦捜査局（FBI）とオランダ国家警察など計 17 カ国と協力して行った捜査により、ダークウェブ市場「Genesis Market」を閉鎖したと報告した。

Genesis Market は、サイバー犯罪で窃取された認証情報を扱う最大級の市場のひとつだった。押収された Genesis Market のシステムインフラからは、150 万を超えるボット、200 万を超える ID などが発見されたという。

このボットは、購入するとボットが収集したフィンガープリント、Cookie、ブラウザに保存された自動入力データなどのデータにアクセスできるようになる。また、情報の収集はリアルタイムで行われ、購入者にはパスワードの変更情報などが通知される仕組みだった。ボットの販売価格は数ドルから数百ドルの範囲で、最高価格帯のものにはオンラインバンキングのアカウント情報が含まれていた。

https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

2023 年 8 月 29 日 米国司法省ら、多国間連携で Qakbot マルウェアを解体

米国司法省らは、Qakbot として知られるボットネットおよびマルウェアの解体に成功した。米国、フランス、ドイツ、オランダ、英国、ルーマニア、ラトビアの当局による多国籍作戦（The Operation "Duck Hunt"）を実行し、52 台のサーバーと約 900 万ドル（約 13 億円）相当の暗号資産を押収したと発表した。

Qakbot は、被害者のコンピュータに感染すると、ランサムウェアなどの追加のマルウェアを感染したコンピュータに配送する機能があり、近年、Conti、ProLock、Egregor、REvil、MegaCortex、Black Basta など、多くのランサムウェア犯罪グループによって初期感染手段として使用されていた。

https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

2023 年 10 月 21 日 ランサムウェア犯罪グループ Ragnar Locker のメンバーが国際捜査連携により逮捕

ユーロポールは、ランサムウェア犯罪グループ「Ragnar Locker」のメンバーを 11 カ国の法執行機関と司法当局の連携によって逮捕したと発表した。

逮捕作戦は主に 10 月 16 日から 20 日の機関に実行された。チェコ、スペイン、ラトビアでの捜索を経てフランスのパリで容疑者が逮捕され、チェコの自宅で家宅捜索が行われた。さらに、Ragnar Locker ランサムウェアが稼働していたシステムインフラはオランダ、ドイツ、スウェーデンでも押収され、関連するダークウェブサイトはスウェーデンで閉鎖された。この国際的な捜査は、フランスが主導し、チェコ、ドイツ、イタリア、日本、ラトビア、オランダ、スペイン、スウェーデン、ウクライナ、米国の法執行機関の協力のもと行われたという。

https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop

2024 年 2 月 1 日 インターポール、国際捜査によりランサムウェア犯罪等に利用された大量のサーバーを解体

インターポールは、フィッシング・マルウェア・ランサムウェア攻撃を対象とした国際捜査活動により、約 1,300 個の不審な IP アドレスやドメインを押収、31 人を拘束し、70 人の容疑者を特定したと報告した。

Operation Synergia と名付けられたこの活動は 2023 年 9 月から 11 月にかけて実施され、インターポール加盟国 50 カ国以上の 60 の法執行機関が参加したという。警官らが容疑者の家宅捜索やサーバーや電子機器の差し押さえを実施し、特定されたコマンドアンドコントロール（C2）サーバーのおよそ 70%を停止する成果を挙げている。

インターポールは、国際法執行機関、各国当局、民間部門のパートナーがベストプラクティスを共有したうえで積極的な行動をとったことが成功要因とみている。今回の作戦では、シンガポールと香港の警察機構が多くの成果をあげたほか、南スーダン、ジンバブエ、ボリビア、クウェートといった国々が各地域で重要な役割を果たした。また、INTERPOL の民間パートナーである Group-IB、Kaspersky、TrendMicro、Shadowserver、Team Cymru は、作戦全体を通じて脅威インテリジェンスの提供と分析の支援を行った。

https://www.interpol.int/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats

2024 年 2 月 20 日 国際捜査協力によりランサムウェア犯罪グループ LockBit の関係者を逮捕、サイトを一時停止 日本警察による復号ツールも公開（24 年 5 月に主催者の身元特定、制裁措置へ）

米国司法省は、米英を中心とした 10 カ国の捜査当局が共同作戦を実施し、ランサムウェア犯罪グループ LockBit のメンバーとみられるロシア人 2 名を逮捕、運営サイトを押収したと発表した。LockBit はこれまで 2 千以上の組織が合計 1 億 2 千万ドル（約 180 億円）の被害に遭ったとされる世界最大級の規模のグループで、RaaS（ランサムウェアアズアサービス）として様々な実行グループにデータ暗号化マルウェアや暴露サイトのサービスを提供していた。

押収したサイトのデータには、被害者から盗んだデータや暗号資産、複合キーなどが含まれていたという。摘発後、運営サイトは各国当局による共同凍結メッセージに差し替えられ、日本の警察庁が開発した復号ツールも被害者救済のための案内として掲載された。

その後、2 月 27 日に LockBit 主催者がバックアップからサイトを復旧し、事態の説明と FBI への報復を行う旨のメッセージを発した。システムを改善したうえで RaaS サービスを再開する意向を示しているが、識者は LockBit はダメージをうけており、彼らのサービスを利用する実行犯グループからも不信感を持たれた可能性があると指摘している。
https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/

4） AI 規制におけるサイバーセキュリティの議論

2023 年 6 月 14 日 欧州議会、欧州 AI 法案に関する共通見解を採択　法案の最終検討へ（24 年 3 月に可決）

欧州議会、欧州 AI 法案に関する共通見解を採択した。今後は欧州議会、欧州連合理事会、欧州委員会が EU 法案の内容を交渉する三者対話（トリローグ）の枠組みに進む。

採択された AI 法案は「高リスクの AI アプリケーション」を全面的に禁止する条文を含む。欧州議会は高リスク AI を「人々の健康、安全、基本的権利または環境に重大な危害を及ぼす AI システム」と定義した。これには「有権者に影響を与えるために使用される可能性のあるシステム」や「4500 万人以上のユーザーを持つ SNS 企業が使用する推薦システム」などが該当する。また、性別や人種のような機微な情報を使用する生体分類システムや犯罪捜査システムの禁止についても議論された。

議会は今後、基盤となる AI モデルの提供者に対して、潜在的なリスクを評価・軽減した上で、欧州市場にリリースする前に EU のデータベースへの登録を義務付ける予定。また、ChatGPT のような生成 AI システムには、コンテンツが AI によって生成されたことの開示を義務化し、ユーザーが AI 生成物を区別可能とすることを目指す。
https://multimedia.europarl.europa.eu/en/webstreaming/press-conference-by-roberta-metsola-ep-president-brando-benifei-and-dragos-tudorache-rapporteurs-on_20230614-1400-SPECIAL-PRESSER
https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

2023 年 6 月 14 日 米 MITRE、「AI セキュリティのための良識ある規制の枠組み」を発表

米国の非営利研究機関 MITRE は、AI セキュリティ規制について議論したレポート「AI セキュリティのための良識ある規制の枠組み」を発表した。AI 規制の潜在的な選択肢を検討し、AI の開発と利用を形作るためのガードレールを確立する方法を提唱することが目的とされている。

レポートの特徴として、AI がもたらすメリットを維持しながら安全性を担保するために、システム工学の高度な専門知識を適用するというアプローチをとっている。従来のソフトウェア保証要件に加えて AI 保証要件を満たすことを求め

るという基本提言に加え、業界別の固有ユースケースに基づいた保証の必要性にも言及している。また、検証の視点から、AI システムの監査可能性や自動化された AI セキュリティテストなどを検討することを求めている。

https://www.mitre.org/news-insights/publication/sensible-regulatory-framework-ai-security

2023 年 7 月 13 日 中国国家インターネット情報弁公室ら、「生成式人工知能サービス管理暫定弁法」を発表

中国国家インターネット情報弁公室（CAC）、科学技術部、工業情報化部、公安部など 7 部門は、生成 AI サービスの管理に関する暫定的な行政法規「生成式人工知能サービス管理暫定弁法」を発表した。8 月 15 日より施行される予定。この弁法は、生成 AI のサービス提供・使用、訓練データやデータラベリング要件などを明確化するもの。

中国国民に対してコンテンツ（テキスト、画像、音声、映像など）を生成する AI 技術を開発・応用・提供する組織に適用される。また、「インターネット情報サービス深層生成管理規定」（2023 年 1 月 10 日施行）に基づき、生成されたコンテンツへのマーク付け、違法コンテンツの適時処分、セキュリティ評価やアルゴリズムの提出に関する法的責任も定義した。要件の概要は次の通り：

1. 生成 AI サービスの提供・利用にあたっては社会主義の核心価値観を堅持すること
2. アルゴリズム設計、学習データ選択、モデル生成・最適化、サービス提供の各過程において社会にもたらされ得る悪影響を抑制するための効果的な措置を講じること（例：学習データに存在する差別的なコンテンツ、アルゴリズムが特定の特徴値を好むこと、アノテーション担当者の主観的判断などの要因を排除）
3. 知的財産権と他者の正当な権利と利益の尊重
4. 生成 AI サービスの透明性を高め、生成されたコンテンツの真正性を保証すること

http://www.cac.gov.cn/2023-07/13/c_1690898326795531.htm

http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

http://www.cac.gov.cn/2023-07/13/c_1690898326863363.htm

2023 年 7 月 26 日 FBI 長官、サイバー脅威サミットで人工知能に関する FBI の立場を表明

FBI のレイ長官は、主催したサイバー脅威サミットの基調講演で、サイバー犯罪者が人工知能を武器化しており、機械学習モデルが洗練されるにつれ生じる脅威もより深刻化すると警告した。一方で「捜査で収集した膨大なデータをトリアージして優先順位を付ける」など、捜査を支援するために人工知能を活用する方法を模索していることにも触れた。また、外国情報監視法（FISA）第 702 条によって FBI に与えられた権限が世界中でサイバー犯罪を取り締まる能力の鍵であると述べた。その際、第 702 条が情報収集を許可しているのは外国の諜報監視対象者に関する情報のみであり、米国国民の情報収集は許可されていないと強調した。そして、米国民と経済をサイバー脅威から守る上での官民パートナーシップが重要であると訴え、協力を呼びかけた。

https://www.fbi.gov/news/stories/fbi-director-lays-out-bureau-s-stance-on-artificial-intelligence-at-cyber-threat-summit

2023 年 9 月 12 日 米国国家安全保障局ら、ディープフェイクの脅威に関するサイバーセキュリティ情報シートを公開

米国国家安全保障局（NSA）、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）は合同で、ディープフェイクの脅威、技術、使用傾向の概要を示すサイバーセキュリティ情報シート（CSI）「組織に対するディープフェイクの脅威の文脈化」を発表した。

ディープフェイクのような合成メディアからの脅威は指数関数的に増加しており、国家安全保障システム（NSS）、国防総省（DoD）、国防産業基盤（DIB）、国家重要インフラの所有者や運営者など、現代のテクノロジーや通信の利用者にとって、ますます大きな課題となっている。

合成メディアをめぐる社会的関心には、偽情報を広めるように設計された偽情報操作も含まれる。偽情報操作は、混乱、不安、不確実性を引き起こし、政治的、社会的、軍事的、経済的な問題について、大衆に影響を与える。CISA らは、組織がディープフェイクの脅威に備え、識別し、防御し、対応するための推奨される手順とベストプラクティスについて、CSI を参考にするよう促している。

https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats

https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF

2023 年 11 月 23 日 米国 CISA と英国 NCSC、安全な AI システム開発のための国際ガイドラインを発表

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）および英国国家サイバーセキュリティセンター（NCSC）は、安全な AI システム開発のための国際ガイドラインを発表した。このガイドラインは、G7 の加盟国すべてを含む世界の 21 の当局や機関と協力して策定された。AI システム開発に関するガイドラインとしては世界的に合意された初めての文書となる。

AI システム開発ライフサイクルの 4 つを主要領域 (安全な設計、安全な開発、安全な導入、安全な運用と保守) に分類し、各領域で組織の AI システム開発プロセスに対するサイバーセキュリティリスクを軽減するのに役立つ考慮事項と緩和策を説明している。

https://www.cisa.gov/news-events/news/dhs-cisa-and-uk-ncsc-release-joint-guidelines-secure-ai-system-development

https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

2024 年 1 月 4 日 米国 NIST、AI システムへの攻撃と緩和策の分類と用語に関するレポートを発行

米国国立標準技術研究所（NIST）は、AI システムへの攻撃と緩和策の分類と用語に関するレポート「Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations（NIST.AI.100-2）」を発行した。

AI システムは信頼できないデータにさらされると誤動作する可能性があり、攻撃者によって悪用されている。今回のレポートでは、これらの攻撃の種類と緩和策が取りまとめられた。攻撃の種類は、攻撃者の目標や目的、能力、知識などの複数の基準に従って 4 つの主要なカテゴリに分類されている。各分類の概要は次の通り。

・回避攻撃（AI システムがデプロイされた後に行われるもので、入力に手を加えてシステムの反応を変えようとする）

・ポイズニング攻撃（悪意のあるデータを導入することでトレーニング段階で AI モデルの汚染が発生する）

・プライバシー攻撃（AI を悪用するために、学習したデータに関する機密情報を知ろうとする）

・不正使用攻撃（ウェブページやオンライン文書などのソースに不正な情報を挿入し、AI がそれを学習してしまう）

https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

2024 年 1 月 24 日 英国 NCSC、AI がサイバー脅威に与える短期的な影響を評価

英国国家サイバーセキュリティセンター（NCSC）は、AI がサイバー脅威に与える短期的な影響の評価についてレポートを公表した。

NCSC は、AI は今後 2 年間でほぼ確実にサイバー攻撃の量を増加させるが、サイバー脅威に与える影響は均一的なものではないと評価した。サイバー攻撃者は既に様々な場面で AI を使用しているが、特に偵察とソーシャルエンジニアリングの能力を向上させ、検出を難しくする点で影響が大きいと指摘している。また、AI の支援によって未熟なサイバー攻撃者が不正アクセスや情報収集を行うことが容易になり、世界的なランサムウェアの脅威の拡大に寄与する可能性が高いとの分析を示した。

短期的には AI を高度に活用したサイバー攻撃の実行は高い能力を持つ一部の国家アクターに限られるという見通しを示しつつも、2025 年を目途により広い範囲で AI を用いたサイバー攻撃が広まると警鐘を鳴らしている。

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

https://www.ncsc.gov.uk/pdfs/report/impact-of-ai-on-cyber-threat.pdf

以上