2023 年 10 月

シリーズ 「日本のサイバーセキュリティ政策史」第 5 回

結果を保証する「重要インフラのサイバーセキュリティに係る行動計画」

サイバーセキュリティ政策分野に詳しい三角育生氏が日本の同政策史をひもとくシリーズ。第 5 回は、前内閣サイバーセキュリティセンター（NISC）重要インフラ担当内閣参事官の結城則尚氏をお迎えし、話をうかがいます。サイバーの問題が社会安全に直結し、脅威が高度化・巧妙化する時代、継続的サービスが求められる重要インフラのセキュリティに必要な取り組みとは。経営責任や障害対応体制の強化など、これまでにない訴求を盛り込む「重要インフラのサイバーセキュリティに係る行動計画」はどのような考えで策定されたのか──。

【出席者】

結城 則尚 氏
三井物産セキュアディレクション株式会社 イノベーション戦略部 シニアアドバイザー（前内閣参事官内閣官房 内閣サイバーセキュリティセンター（NISC）重要インフラグループ）

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

サイバーの問題が社会安全に直結する時代に

三角 今回は「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日サイバーセキュリティ戦略本部決定。以下、第5次行動計画）を取り上げたいと思います。第5次行動計画策定において、当時、重要インフラ担当内閣参事官としてその中枢におられた結城さんに、背景や狙いについて話をうかがいます。まず、第5次行動計画を立案した経緯や意図などについて教えていただけますか。

結城 それは不正アクセスによる日本年金機構からの個人情報流出事件に遡ります。流出の問

題が公表されたのは 2015 年 6 月 1 日でした。5 月 25 日に官邸で安倍晋三総理大臣（当時）が出席される中、2015 年 1 月に完全施行されたサイバーセキュリティ基本法（2014 年成立）に基づく初の「サイバーセキュリティ戦略案」をパブリックコメント（意見公募）にかけることが決定されて間もなくのことです。これは安倍政権への挑戦と考えて、関係者一体となって対処しました。

また、内閣サイバーセキュリティセンター（NISC）がサイバーセキュリティ基本法に基づき 2015 年 1 月に設置されて早々に起きた事案です。当時 NISC では、所属グループ、上下関係を越えて当時参事官だった三角さんとも一緒に、標的型攻撃等への対応について常に頭のトレーニングをしていましたね。特に若手が熱血漢で、毎日あちこちで熱い議論がありました。こうした中で、実際の事案が発生しました。まさに被害が現認された事案に対する初のインシデントハンドリングでした。職員一丸となって、わずか 2 カ月半で報告書をまとめることができました。報告書は、原子力安全規制での事故・トラブル対応の経験を踏まえ、わかりづらいサイバー事案を国民の方々にできるだけわかりやすく、共感できるものにするよう心掛けました。結果として、この報告書は多方面から引用され、設置されたばかりの NISC の存在を示せたのではと思います。

その後、WannaCry（ワナクライ）、NotPetya(ノットペティア)、BadRabbit （バッドラビッド)といったランサムウエア攻撃が日本にも押し寄せてきました。同時期に、IoT の爆発的普及により、あらゆるものがネットにつながるようになり、従来サイバー空間だけだった問題が、現実の社会安全に直結する時代となりました。最近の例では、2022 年夏に、大手携帯キャリアの手順書ミスにより 86 時間通信障害が発生しました。現代社会においては、携帯電話は社会基盤化しており、緊急通報ができないといった電話機能のほか、IoT 回線としても使用されていることから、物流システムに障害が発生しました。一昔前なら、「携帯電話が使えない」で済んだものが、現在では、大きな社会混乱につながるようになってきたことを示す事例ではないかと思います。

サイバーセキュリティとは何か

三角　そうした状況において、第 5 次行動計画を改定することになったということですね。

結城　そうです。その意図や内容を紹介する前に、「セキュリティ」についていろいろな解釈があるので、共通認識を得ておきたいと思います。

英国の国際問題戦略研究所（IISS）が 2021 年 6 月 21 日にレポート “Cyber Capabilities and National Power: A Net Assessment” を発表しました。各国のサイバー能力と国家の能力をアセスメントした結果、日本は最下位のレイヤーにランクされたとする内容です。

三角　指標の立て方によって結果は異なります。当時は、日本の防衛政策におけるサイバー対処について、国の方針の書きにくさがあったわけですから、Defense が計算されればどうしてもランクは下がりますね。

結城　その通りです。では、民生用である日本の重要インフラ防護は実際、弱いのでしょうか。それぞれ見ていくと、電力については、日本は停電継続時間及び停電回数が極めて少なく、米国、フランス、英国、ドイツなどのサイバー先進国と比較しても桁違いに少ないことがわかります。通信


結城氏

については、インターネット利用率や携帯電話加入者数が各国と比して、日本は極めて高い状況にあります。鉄道については、日本は輸送密度が高いにもかかわらず、極立って高い安全性を誇り、定時運行については、ずば抜けた成績です。現時点の日本の重要インフラサービス水準は、世界に誇るレベルとなっているのですが、このことがあまり知られていません。他方、サイバーセキュリティのお手本とされることが多い米国をはじめとするサイバーセキュリティ先進各国は、重要インフラサービスの安定性の水準は高くないため、サイバーセキュリティ強化による障害対策を行う必要があるのではと受け止めています。

三角　今のところは、日本は比較的に安定していると言えますね。

結城　これまではその通りです。ところが、既に世の中は大きく変わってきており、急速に進む少子高齢化、人材不足、技術伝承不足が表面化してきています。その対策として、システム化、自動化が進み、相互接続性・依存性を高めていく必要があり、IoT 化、オープン化がいっそう加速化することにより、サイバー依存度が急速に増加してきていきます。また、東西デカップリング、新型コロナウイルス(SARS-CoV-2)パンデミック、ロシアのウクライナ侵攻など、最近の世界情勢の急激な変化によってサプライチェーンの不安定性が高まっています。さらに、持続可能な開発目標（SDGs）の機運が世界的に高まり、低コスト化、省力化など、従来のやり方では、どんどん余裕がなくなってきています。しかし、こうした時代の趨勢には逆らえません。アンテナを高くして、時代の変化に柔軟に対応していくことが求められます。既に、日本において、サイバーセキュリティ対策をいっそう高めていくことが必須であることは周知の通りです。

サイバーセキュリティとは何か、とざっくりと説明が求められる場合、MotoGP(世界のオートバイレスの最高峰)を引用することがあります。MotoGP で優勝するためには、レーサーが多く並走する複雑なコースを速く、安全に走破する必要があります。安全第一でゆっくり走ったら走破できても勝てませんし、度量を超えて速く走れば転倒し、走破できません。レーサーは、搭乗する車体特性を熟知し、常に「上振れリスク」と「下振れリスク」を踏まえ、最適なリスク環境を保って操縦する技量が求められます。また、レーサーだけでは優勝できません。最適な車体の性能の確保はもちろんのこと、監督の下、戦略を立てて、支えるチームがあって、車体の状態をモニタリングしながら、レース中に最適なメンテナンスを短時間で終えるための手順とスキルを十分発揮できるチームワーク等、全てが整ってこそ勝利につながります。よく、セキュリティは、「ブレーキだ」と指摘されますが、「ブレーキ」があるからこそ、安全確実なスピードが出せ、優勝に導く大きな要因となります。すなわち、「サイバーセキュリティ」は、激変する社会情勢の中で、業務を安定させ、競争に勝ち続けるために欠くことのできないものと考えています。

サイバー攻撃はサイバーセキュリティを損なう要因の一つに過ぎない

三角　私もよくスポーツカーのブレーキに例えますが、同感です。

結城　「情報セキュリティ」について、JIS Q 27000:2019 では以下のように定義されています。「情報の機密性・完全性・可用性（CIA）を維持すること」。機密性（Confidentiality）とは、アクセスを認可された者だけが情報に確実にアクセスできること。完全性（Integrity）とは、情報資産が完全な状態で保存され、内容が正確であること。そして、可用性（Availability）とは情報資産が必要になったとき、利用できる状態にあることです。

「セキュリティが厳しすぎて、使いにくい」という話をよく耳にします。この場合の「セキュリティ」は、もっぱら「機密性」を指しているのであり、セキュリティの構成要素である「可用性」が劣後しているように感じます。現に「機密性」に重点を置き過ぎ、「可用性」が劣っているシステムの使用者が、使いにくいとして、別のシステムにデータを転送して作業を行い、セキュリティ事故を起こした事例があります。

では、サイバーセキュリティ基本法において、「サイバーセキュリティ」はどう定義されているか。第 2 条で以下のように記されています。「『サイバーセキュリティ』とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏洩、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう」（注：太字は発言者による）。

つまり、サイバー攻撃はサイバーセキュリティを損なう要因の一つであって、すべてではないということです。その点、各国が定義する「サイバーセキュリティ」の中でも、日本のサイバーセキュリティ基本法の定義が最も明確化されています。

以上を踏まえて、第5次行動計画を見ていきます。

考えるべきことは、サービス停止という結果を防ぐこと


三角氏

三角　第5次行動計画は障害対応体制の強化や経営責任など、これまでにない内容を含んでいます。その背景を解説いただけますか。

結城　まず、日本のサイバーセキュリティ政策の歴史を振り返ると、2010 年代までとそれ以降で大きく要素が変わっています。2010 年代までは、ファイアウォールやアンチウィルスといった共通の防護で十分対応できていました。

三角　世界的には、2010 年頃の Google などへの Operation Aurora と名付けられた攻撃の事件対応のあたりから変わってきました。日本社会で大きく認識を変える契機となったのは、2011 年に発生した大手重工メーカーの事案です。結果の社会的イン

パクトや、事前の対策中心では足りないことなどが、広く認識されるようになりました。

結城　そうですね。その後、米国のソニー・コンピュータエンタテインメント（SCE）へのサイバー攻撃の被害のひどさが問題となるなど、最初に述べた通り、サイバーセキュリティが単にネットワークだけではなく、組織全体や経済・社会に影響するようになりました。そこで守り方もリスクベースに大きく舵を切ることになります。

こうした中、第5次行動計画では、「障害対応体制の強化」を取り組む項目の最前面に出しました。その理由は、日本におけるサイバー事案が目立ち始めてきていますが、現段階が、組織をあげて対応すれば、実効性を上げることができるラストチャンスだからです。

日本で重要インフラ障害が目立ち始めたのは 2018 年頃からです。2018 から 21 年にかけて複数医療機関に対するランサムウエア攻撃、2019 年に複数自治体が利用するクラウドサービスのシステム障害、そして 2021 年に重要インフラ事業者等が利用する業務委託先に対するランサムウエア攻撃が発生しています。これら事案は、脆弱性の放置、インシデントハンドリングの不備が主な原因であり、組織的に対応していれば防げた可能性が高いと思われます。

三角　似たような重要インフラ障害が繰り返し発生しましたね。

結城　他社の障害事案から学ぶことがなかったということです。障害対応体制の強化は急務です。

2019 年 9 月には、消費税率改定に間に合わせるべく大手スーパーチェーンが新しいスマホ決済サービスを導入しましたが、せっかくのビジネスチャンスを「セキュリティ・バイ・デザイン」と運用開始後の事案対応に弱さがあったことから、開始 1 カ月でサービス廃止となってしまいました。その約 1 年後、大手通信キャリアの電子決済サービスにおいて、利用者範囲拡大に伴うリスク増加に十分対応できていなかったため、不正送金が多数発生し、一時的にサービス停止となりました。将来性のある新しいサービスを導入しても、セキュリティ対策が十分でなかったことによる停止事案が、事業者の枠を超えて繰り返されているのは、日本の経済・社会発展にとって好ましいことではありません。業界を超えて他社の失敗を自分事として学ぶことが重要と考えます。新規事業については、企業内ではトップシークレット扱いで開発されるのだと思いますが、その際、セキュリティが劣後されがちなのではないでしょうか。「セキュリティ・バイ・デザイン」は新規事業において、投資リスクを下げることを示す事例と言えると思います。

重要インフラサービスにおいて、「サービス停止」は、それ自体の目的からの逸脱であり、最も避けなければならないものです。重要インフラサービスは、「結果の保証」が一義的な目的であり、停止した原因がサイバー攻撃なのか、故障なのかには関係がないのです。原因が何であるかにかかわらず、停止による社会混乱にどのように対処するかが重要であることは言うまでもありません。

経営層の関与は不可欠

三角　第5次行動計画では、障害対応体制を強化する上で、経営層を含めた組織一丸となった対応が必要であることを指摘し、また組織統治に必要な観点として、サイバーセキュリティと経営層の責任を明記しています。体制が適切でなかったために情報漏洩等があって会社に損害が生じ

た場合、「損害賠償責任を問われ得る」とまで記されています。この点を強調した意図は何でしょう。

結城　最近のサイバー事案はサイバー部門だけで閉じていないことが特徴の一つです。組織全体のマネジメントと CSIRT（Computer Security Incident Response Team）の連携が弱いように見えます。組織に存在するリスクを、どうしたら組織内で共有できるのかということが課題と考えています。

ある大手金融機関で、2002 年にシステム障害が発生したにもかかわらず、その後 20 年間ガバナンス問題が改善されなかったことにより大規模なシステム障害に至った事案があります。第三者委員会の報告書によると、「障害に共通する原因として、危機対応力や IT システム統制の弱さ等がある」ということです。サイバー攻撃ではなく、ガバナンス問題で大規模障害に至る事例です。また、先ほど触れた 2021 年の重要インフラ事業者等が利用する業務委託先に対するランサムウエア攻撃では、約 7 億 5,000 万円の特別損失を計上しました。脆弱性対策に必要な予算と被害額を比較すれば、サイバーセキュリティ対策への投資の有効性を経営者が認知する機会になったと言われています。

三角　第 5 次行動計画では、組織統治の重要性についてこれまで以上に訴求していますね。

結城　組織全体に影響を及ぼす事案は、組織全体で対応しないと対処できなくなってきているからです。2010 年以降、特に最近は、サイバーセキュリティに対し経営リスクとして取り組む時代になってきています。IT 依存度が高まり、使用方法は複雑化し、新規ビジネスの開発機会が増大するにつれ、IT 障害が、国民経済、生命財産に影響を与えるようになり、サービス提供事業者の経営問題に発展しかねない事案が発生しているからです。一方、外部調達しているシステムやサービスに関しては、供給者の連携が不可欠になってきています。事業者だけで対処できる範囲を超えている実状を考慮する必要があります。

また、重要インフラ防護体制の役割の責任を明記し、従来とは異なる組織統治のアプローチを訴求しています。「経営層、CISO、戦略マネジメント層、システム担当者等の組織全体及びサプライチェーン等に関わる事業者における役割と責任を明確にした上で、サイバーセキュリティの専門的・技術的な問題点と、経営層が抱えている事業運営の問題点を融合させることが必要である」（「第 5 次行動計画」11 頁。太字は発言者による）と明記し、しかしながら、経営層がサイバーセキュリティの専門的な知見を必ずしも有するとは限らないため、サイバーセキュリティの知見を有する人材を経営層に取り込むという、より実効的、現実的な選択を示しています。

さらに、リスクに応じた対応を具体的に訴求しています。ISO31000:2018 のリスクの定義は「目的に対する不確かさの影響」です。「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」（以下、第 3 次行動計画）ではリスクを「目的に対する不確かさの影響」としていたものの、新しい概念であったことから、従来から用いられてきた「損失の大きさ×発生頻度」をどちらかといえば主体としてきました。第5次行動計画では ISO31000 の定義に明確に切り替えました。定義に従えば、「目的」が決まらないと組織の「リスク」を決めることができません。目的は経営層が決めるものなので、経営層の関与が不可欠となります。また、米国立標準技術研究所（NIST）が策定し、世界的に活用されている「サイバーセキュリティフレームワーク（CSF）」によれば、組織のリスクを明確にするためには、組織が提供するサービスの特徴や組織がどうありたいのかといった組織の特性

（プロファイル）を当初に明らかにする必要があります。

日本では、自然災害によるリスクに対しても留意が必要です。日本におけるシステムダウンによるサービスの停止事案の原因は、先ほど指摘した管理ミスのほか、自然災害が多いことが特徴です。2018 年台風 21 号による関西国際空港の浸水、また 2019 年台風 19 号による房総半島全域停電が発生し、その地域に立地するシステム停止に至っています。繰り返しになりますが、重要インフラの目的は、サービスの継続的な提供です。緊急時対応、浸水対策、バックアップ対策などシステム側でもあらかじめ考えておく必要があります。サイバー攻撃しか対応しないとなれば、強靭性が劣後します。

加えて、重要インフラ事業者等がリスク情報を活用して自らの組織に最適な防護対策を実現するアプローチを示しています。すなわち、自組織が現状分析を行うことによって、重要インフラサービスの継続的提供にかかるリスクを明確にし、対応の程度にメリハリをつけ、効果的な自組織に適した具体的な対策の決定を行うことで可能になるとしています。

プロファイルから始めよ

三角　その点、すなわちプロファイルで定義される組織の「AsIs（現在）」と「ToBe（目標）」をはっきりさせるべきことについて今回強調していますね。行動計画の内容が、これまでの ISO 基調から NIST 基調に切り替えたなという印象です。

結城　NIST の CSF のイメージです。

NIST の CSF は、「特定（Identify）」「防御（Protect）」「検知（Detect）」「対応（Respond）」「復旧（Recover）」の 5 項目からなることは、ほとんどの方が知っていると思われます。他方、それらを組織固有のリスクに応じて有効に活用するためには、「コア（Core）」（それぞれの項目に対するサイバーセキュリティ対策）と「ティア（Tier）」（それぞれの項目に対するサイバーセキュリティ対策の深さ）については、「プロファイル」（組織の現状［As Is］把握と目標［To Be］に基づく組織の特性）によって、メリハリをつけて最適な対策をとるものであることが十分に理解されているとは言えない状況です。

米国で CSF に関する研修を受けた際、コアとティアだけを見て発表している参加者に対して、講師が「ストップ！ストップ！」と言ってドンドンと黒板を叩いて、「みなさん、プロファイルが決まらなければリスクは特定できないでしょう」と助言する場面がありました。あのときパチンと叩かれた感じがしました。そうだ、日本で決定的に欠けているのは「プロファイル」だ。だから、リスクアセスメントが容易ではなく、メリハリがつけられないのだと。

これが今回の行動計画で最も訴求したい内容です。

三角　プロファイルから始めるのは、実務からするとやりやすいと思います。実際に実務で優先順位付けしようとすると、まず、自分たちは何をする組織か、何をしようとしているのか、というところからスタートすることになります。

結城　プロファイルを明確にして、自分たちの組織に合ったコアとティアを定め、ティアについてはどの程度までやるのかを決める。同様のことを PDCA サイクルで説明することもできます。リスク

把握をする際、PDCA ではなく、順番を C から始めて CAPD サイクルへと着手点の転換を提案します。

こうして改善実施計画を作った上で、経営層のコミットメントをもって実施を確実にしましょうと説明しています。

失敗経験の共有を

三角　経営層にコミットメントの重要性が理解されにくいと思います。サイバーセキュリティへの問題意識を、どうやったら経営層に持ってもらえると思いますか。

結城　失敗経験者あるいはそれをよく知る人に話をしてもらうことではないでしょうか。私自身も現場技術者だった 20 代、安全確保に必要なプロセスを時間の制約で飛ばしてしまい、プラント故障を引き起こした経験をしています。また、先日、ある企業経営者の方が「安全を軽視したことによって、実害が発生し、それをきっかけに、それまでの勢いに戻らなくなる場合がある」とおっしゃっていました。重い言葉だなと思って聞きました。失敗して、「あのときこうすればよかった」という事例が多く見られます。失敗したことは、なかなか言い出しにくいものですから、失敗から得られた教訓が生かせず、同様のことが繰り返されることは、社会にとっての損失と考えています。

2022 年 2 月、大手自動車企業の仕入先がランサムウエア攻撃を受け、同企業の全工場の操業を停止した事案がありました。この事態を重く受け止め、政府による注意喚起の文書が公表されました。リスク低減のための措置、インシデントの早期検知、そしてインシデント発生時の適切な対処・復旧の 3 つについてまとめられています。しかし、こうした注意喚起は以前から発出されてきています。どんなに注意喚起しても、実行されなければ意味を持ちません。

私は、米連邦政府で原子力安全規制に従事した経験があります。その時に感心したのは、連邦政府からの注意喚起には「Action Required」(注意喚起に対する対応を事業者に求め、必要に応じて報告させるもの)と「No Action Required」(注意喚起のみ)の 2 種類があることでした。ランサムウエア攻撃は、繰り返し発生しており、原因を調査すると同様であることがほとんどです。こうした事案に対しては、「Action Required」の注意喚起とすべきではないか。サイバーセキュリティ政策は、徐々に保安規制でのグッドプラクティスを参照することが必要になってきているのではと感じています。

三角　義務的な報告を求めるには法的な裏付けが必要かと思います。その場合に「Action Required」を発出できる重要インフラなどの対象を決めておくことになるでしょうね。

結城　重要インフラ 14 分野は、業所管省庁の下にあり、適用される業法に基づき、こう

した注意喚起を発出することは可能と考えています。なお、行動計画に基づき、各事業者はプロファイルを明確にして、メリハリをつけた実効的なサイバーセキュリティ対策を講じることが期待されています。その際には、先程の CSF が参考になると思います。米国は、日本で第 3 次行動計画を策定していた 2013 年に初版を発行しており、当時三角さんから「このような文書が米国から発出されたけれど参考にならないだろうか」と紹介されました。しかし、恥ずかしながら、当時は理解の範囲を超えていました。ほぼ 10 年遅れですが、ようやく日本も追いついたと思うと同時に、米国の先進性を痛感しています。

三角　米国はいろいろな事案が生じていますし、実務的に政府に対してフィードバックが入っていると思います。そうしたことから先進的に対応しているということではないかと思います。われわれが実際に同様の立場に立つと、課題に直面した際に考えて行動している内容が、既に米国のドキュメントに書かれてあったりしますね。

日本の最大の課題は、人口及び労働者数が減少し、これから急速にデジタル化・ネットワーク化が進んだとき、デジタルの基幹産業が国内に十分にないことかと思います。サービスやプロダクトの大半が海外からの買い物となってしまうので、本質がブラックボックスのような状況でシステムを組まざるをえなくなる可能性があります。

結城　そうですね。

三角　システムの組み方のプラクティスをよく分析しないと、どこにリスクが潜むかわかりません。そこをどういう風に見ますか。

結城　設計思想を十分に把握し、冗長性をどのように確保しているかなどを確認する必要があります。原子力施設の安全設計では、多重化、多様化、予防、緩和などが重要なポイントとなっており、参考になると思います。

三角　やはり、強靭な重要インフラ維持のためにも、日本としてしっかりとした充実したサプライチェーンの構築が必要だと考えます。

本日は、第5次行動計画において、いろいろと新しい機軸が示された意図、背景についてよくわかりました。どうもありがとうございました。

(2023 年 8 月 1 日収録。取材・構成：一般社団法人 日本サイバーセキュリティ・イノベーション委員会[JCIC])

【出席者略歴】

結城 則尚（ゆうき のりひさ）氏

1984 年東北大学工学部機械工学科卒業。1985 年同大学院中退後、新潟県庁入庁。県営発変電プラント等の運転、保守、設計、建設業務に従事。1996 年経産省に移籍。原子力発電の安全設計審査業務を開始。以後、安全検査、事故調査、電力安全、製品安全業務に従事(~2013 年)。その過程で米国原子力規制委員会(US NRC)原子炉規制局へ派遣され、米国の原子力安全規制(1998～99 年)、国際原子力機関(IAEA)専門家として、国際マネジメント規格策定、国際審査業務に従事するとともに、組織事故、原子力事故等の事故調査を行い、報告書を多数作成。NISC 重

要インフラ担当、基本戦略担当(2013～22 年)。2015 年に発生した日本年金機構個人情報漏洩事案原因究明報告書等、事故報告書を数多く担当。現在、三井物産セキュアディレクション株式会社イノベーション戦略部シニアアドバイザー、産業技術総合研究所サイバーフィジカルセキュリティ研究センター客員研究員などを務める。

三角　育生（みすみ　いくお）氏
1987 年通商産業省入省。内閣サイバーセキュリティセンター(副センター長等)や経済産業省(サイバーセキュリティ・情報化審議官等)等において、サイバーセキュリティ、安全保障貿易管理といった行政に長く携わり、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法制定・改正、日本年金機構のインシデント対応等に従事。2020 年 7 月退官。2022 年 4 月～東海大学情報通信学部長・教授。博士(工学)、MA in Management。

1 「重要インフラのサイバーセキュリティに係る行動計画」策定の背景・提言
(1)現状認識：重要インフラを取り巻く環境は予断を許さない状況まできている。
(2)課題の明確化：管理を適切にすれば防げた類似障害が繰り返し発生していることを踏まえ経営層を含め組織的な対応が必要である。
(3)提言：「第４次行動計画」における有効な取り組みは維持しつつ、特に以下の２点に留意すべきである。
①障害対応体制の強化のあり方の抜本的な見直し。すなわち、現在の「経営層の働きかけ」から、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載する。また、サイバーセキュリティ基本法が公布・施行されたことを踏まえ、各関係主体の責務の境界を明確化する。
②将来の環境変化を先取りし、サプライチェーン等を含め包括的に対応する。

出所)「重要インフラ行動計画改訂への提言」概要（2021 年 10 月 25 日、サイバーセキュリティ戦略本部 重要インフラ専門調査会 政策部会資料） https://www.nisc.go.jp/pdf/council/cs/ciip/dai26/26shiryou05.pdf

２ 「重要インフラのサイバーセキュリティに係る行動計画」の概要

（1）官民連携による重要インフラ防護の推進

・任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現

・官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

※NISC による総合調整（重要インフラ所管省庁、重要インフラ［全 14 分野］、関係機関等）

（2）「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

・障害対応体制の強化

・安全基準等の整備及び浸透

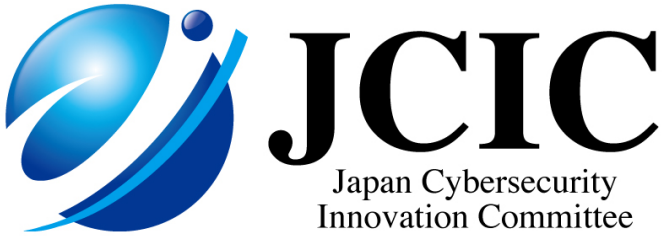
・情報共有体制の強化

・リスクマネジメントの活用

・防護基盤の強化

出所）「重要インフラのサイバーセキュリティに係る行動計画」（概要）

https://www.nisc.go.jp/pdf/policy/infra/cip_policy_abst_2022.pdfß



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com