

安全保障を 考える

ここに掲載された意見等は、執筆者個人のもので、本会の統一の見解ではありません。

重要インフラのサイバー防御における官民連携

研究班 住田和明

1 はじめに

2024年6月7日、能動的サイバー防御（Active Cyber Defense、以下「ACD」という）を行う上で必要な法整備などについて議論する「サイバー安全保障分野での対応能力の向上に向けた有識者会議」（以下、「有識者会議」という）が設置され、8月7日に「議論の整理」が公表された。通信の秘密¹、不正アクセス禁止法など、これまでに指摘されていた壁を乗り越え、個人情報や通信事業者による活動の安全を確保するために必要な提言が数多くなされており、ACDに関連する法整備や対応能力の向上を達成するために必要な道筋が示された。今後、実際にACDを行うにあたっては、法整備に加え、NISC（National center of Incident readiness and Strategy for Cybersecurity、内閣サイバーセキュリティセンター）、警察、自衛隊のACD能力及び体制を抜本的に強化するほか、平素の情報収集、重要インフラ等の民間事業者及び電気通信事業者（以下、「通信事業者等」という）との連携、米国や同志国との連携などによりACDの実効性を確保することが不可欠である。

国民生活及び社会経済活動は、様々な重要インフラによって提供されるサービスによって支

¹ 憲法第21条2項は、「検閲は、これをしてはならない。通信の秘密はこれを侵してはならない」としている。

えられており、これを防護することは安全保障上の最重要事項である。重要インフラサービス提供の支障事案の主な原因は、自然災害、管理不良、サイバー攻撃などが挙げられるが、中でもサイバー攻撃は近年増加の一途を辿っている。有識者会議がサイバー攻撃について「実空間への影響が重大化・深刻化」、「サイバー攻撃に用いられる手法の高度化・巧妙化が進展」などと指摘²している通り、重要インフラ単独でサイバー攻撃から安全を確保することは難しく、NISC、警察、自衛隊など政府の実動組織及び通信事業者等との連携が必要である。

このような観点から本稿では、安全保障上の懸念を生じさせる重大なサイバー攻撃から重要インフラを防御するために不可欠な官民連携の現状を概観するとともに、緊密な官民連携を達成するための施策について考察する。

2 重要インフラに対するサイバー攻撃

(1) 重要インフラのサイバー防御

ロシアによる本格的な侵略に先立って、ウクライナの重要インフラが大規模なサイバー攻撃に晒された。ロシアは侵略開始の1年以上前からウクライナの政府機関や重要インフラのシステムに侵入してサイバー攻撃を準備、侵略開始の一ヶ月程度前から破壊的なサイバー攻撃を開始し、侵略前日には約300のシステムを対象とした大規模な破壊的サイバー攻撃を実施したとされる³。「重要インフラのサイバーセキュリティに係る行動計画（以下、「行動計画」という）」では、重要インフラ分野として、情報通信、金融、電力など15分野を特定⁴している。その機能が停止、低下又は利用不能な状態に陥った場合、わが国の国民生活や社会経済活動に極めて深刻な影響を及ぼすことから、重要インフラに対するサイバー攻撃を早期に検知して障害の発生を未然に防ぐとともに、障害が生じた場合には迅速に復旧し、サービスの提供を継続しなければならない。

国家安全保障戦略では、重要インフラを含む民間事業者等がサイバー攻撃を受けた場合の政府への情報連絡や通信事業者等が提供する通信情報を活用して攻撃者による悪用が疑われるサーバー等を検知するほか、国、重要インフラに対する安全保障上の懸念を生じさせる重大なサイバー攻撃については、可能な限り未然に攻撃者のサーバー等へ侵入して無害化できるよう、政府に対し必要な権限を付与するとしている。このために必要な措置として「官民連携の強化」、「通信情報の活用」、「アクセス・無害化措置」を挙げているが、これらを可能

² 第1回有識者会議（令和6年7月1日）において内閣官房サイバー安全保障体制整備準備室が提出した資料

³ 「サイバー安全保障分野での対応能力の向上に向けて」（R6.6.7 第1回有識者会議資料）

⁴ 「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の15分野

とするためには、強力な情報収集・分析・対処調整機能を有する新たな司令塔を設置するとともに、通信の秘密、不正アクセス禁止法、サイバーセキュリティ基本法、各種業法などの整理が必要である。また防衛省・自衛隊は、ACD を含むサイバー安全保障分野における政府全体での取組と連携し、重要なシステム等を中心に常時継続的にリスク管理を実施する態勢に移行し、我が国全体のサイバーセキュリティに貢献する体制を抜本的に強化するとして、このために必要な取組を行っている。

(2) 重要インフラに対するサイバー攻撃手法等と対処

近年、中国やロシア、北朝鮮は積極的に APT (Advanced Persistent Threat、持続的標的型) 攻撃を行っており、情報窃取や暗号資産 (仮想通貨) 窃取の他、重要インフラに対する攻撃やプロパガンダの流布なども行っている。APT 攻撃は特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃であり、従来の標的型攻撃に比して長期間、持続的に攻撃を行う。ウクライナ戦争で重要インフラの情報を窃取したロシアの APT28 や、中国の政府系サイバー攻撃グループ APT31、北朝鮮当局の下部組織とされる Lazarus Group などが知られている。

2023 年 5 月、マイクロソフト社はグアム、ハワイ、および米軍基地周辺にある米国の重要インフラを標的とした Volt Typhoon というグループによるサイバー攻撃を報告し、世界の注目を集めた。中国の国家背景があるとされる Volt Typhoon は、グアムや米国本土などの国民生活や社会経済活動の基盤となる重要インフラを対象として 2021 年半ばから活動しており、攻撃により影響を受ける組織は、通信、製造、公益事業、運輸、建設、海事、政府、情報技術、教育の広範な分野に及んでいる。攻撃の踏み台としてインターネットに公開されていた脆弱な SOHO (Small Office Home Office、小規模事務所や自宅で働く職場形態) デバイスに KV Botnet と呼ばれるボットネット⁵を感染させ、米国のコンピュータネットワーク機器関連会社である Cisco Systems 及び NetGear のサポートが終了してアップデートができなくなった脆弱なデバイスを複数経由して標的のシステムに LotL (Living off the Land、環境寄生型) 攻撃を行っていた。LotL はシステムに侵入した後、OS 等にあらかじめ組み込まれている機能を利用してセキュリティ製品からの検知を回避しながら攻撃する。マルウェアを使わずユーザーになりすまして正規ツールを駆使する攻撃手法で、1 回あたりの攻撃時間が短く範囲も限定的であることなどから、システムがサイバー攻撃を受けた際に残る IoC (Indicator of Compromise、痕

⁵ ボット (様々な作業を自動化するプログラム) に感染したコンピュータと攻撃者の命令を送信する指令サーバーによって構成されたネットワーク。攻撃者はボットネットに接続したコンピュータに対して一斉に同じ指令を与えることができる。

跡情報)をほとんど残さない。将来再侵入して本格的な攻撃活動を行うための攻撃準備と言える。このようなサイバー攻撃は既に我が国に対しても行われ、重要インフラやサプライチェーン上にある脆弱な機器等に潜伏して再攻撃を準備している可能性がある。2024年1月、FBIは裁判所の許可を得て Volt Typhoonが複数メーカーの SOHO ルーター等に仕込んだ KV Botnet を強制的に除去したと発表した。これを踏まえ 2 月には米国の CISA (Cybersecurity and Infrastructure Security Agency、サイバーセキュリティ社会基盤安全保障庁)、NSA (National Security Agency、米国家安全保障局)、FBI 及びファイブアイズ⁶が共同でアドバイザリー⁷を発表した。Volt Typhoon の事案に参画した米国の機関等に該当する組織は我が国にもあるものの、所要の権限が付与されておらず、現状では米国のような対応はできない。国家レベルで組織的に対処した例として参考にしつつ、我が国の実情に適った ACD を実現してもらいたい。

3 ACDのための官民連携

(1) NISCの強化と官官連携

2023年5月、NISC及び警察庁は、連名で重要インフラ事業者等のウェブサイトへのDDoS攻撃に関する注意喚起を行い、リスク低減に向けたセキュリティ対策の実施を呼び掛けた。その2か月後の7月、名古屋港統一ターミナルシステム(NUTS)がランサムウェアに感染し、名古屋港全コンテナターミナルの作業停止を余儀なくされ、約3日間にわたりコンテナの搬入・搬出作業が停止した。リモート接続機器の脆弱性が悪用され、そこから不正なアクセスを受けたと報告されている⁸。本事案は保守用VPN(Virtual Private Network、仮想専用線)を通じて物理サーバーにランサムウェアが侵入してサーバー情報が暗号化されたもので、保守作業に利用する外部接続部分のセキュリティ対策が見落とされ、重要インフラにおけるサーバー機器及びネットワーク機器の脆弱性対策が不十分であったと分析されている⁹。更に、原因を分析するためのログがバックアップの対象になっておらず暗号化被害によって原因分析ができなかったこと、復旧対応によるログの消失が発生したこと等が報告されており¹⁰、ネットワークを含む事前の脆弱性対策、原因の特定による被害拡大の阻止までを見据えた被害復旧手順

⁶ 米、豪、加、ニュージーランド、英の5か国による機密情報を含む幅広い情報を共有するための枠組み

⁷ PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure ; Volt Typhoon の活動を緩和するために今日取るべき行動として、インターネットに接続するシステムにパッチを適用すること、フィッシングに強いMFA(Multi Factor Authentication、多要素認証)を実装することなどを提示した。

⁸ 「NUTSシステム障害の経緯報告」(2023.7.5、名古屋港運協会等)

⁹ コンテナターミナルにおける情報セキュリティ対策等委員会資料

¹⁰ 「名古屋港コンテナターミナルのサイバー攻撃におけるインシデント対応について」(2024.7.26、国土交通省 最高情報セキュリティアドバイザー 北尾 辰也)

を徹底するなど ICT (Information and Communication Technology、情報通信技術) 部門の BCP (Business Continuity Plan、事業継続計画) である ICT-BCP の実効性を高めるとともに、ICT-BCP とビジネスそのものの BCP を整合させなければならない。本事案が生じた当時、行動計画で定める重要インフラサービス 14 分野には、港湾運送業を含む「物流」はあったものの「港湾」の規定はなく、本事案を契機として「港湾」が追加され 15 分野になった。重要インフラに係るサイバーセキュリティの重要性、対策強化の必要性は認識されているが、現場レベルにおける対策はなかなか進捗しない。一方、その 2 か月後に NISC と警察庁は米国の NSA、FBI 及び CISA とともに、中国を背景とするサイバー攻撃グループ BlackTech (ブラックテック) によるサイバー攻撃に関する合同の注意喚起を発出した。サイバー犯罪分野における NISC と警察庁との連携が進み、国内にとどまらず米国等、国外のサイバー関連機関等との連携にも及んでいる証左であり、サイバー犯罪分野における官官連携は強化されてきた。

現在、ACD 関連法案の策定と並行して NISC の強化が図られており、従前から指摘されていた実動組織の強化として職員を約 90 名から約 175 名に倍増するものの、これまで以上に警察及び自衛隊の役割が重要になることは間違いない。現在の NISC は総務省、経済産業省、警察庁、防衛省などの各省庁からの出向者が実務を担っていることから、現場レベルでの人的交流は図られているものの、警察と自衛隊が組織的に連携してサイバー攻撃対処に当たることはない。ACD 法 (仮称) によって自衛隊に何らかの平素の任務が付与された場合、NISC、警察及び自衛隊の 3 つの組織が平素から有事にいたるまで切れ目なく、緊密に連携することが求められる。重要インフラは 15 分野に区分され、金融庁、総務省、厚生労働省、経済産業省及び国土交通省の 5 省庁が所管していることから、重要インフラに対するサイバー攻撃が同時多発的に行われた場合、ACD に当たる省庁間の連携は複雑になり容易ではない。新 NISC による司令塔としての統制、重要インフラ所管省庁と事態対処省庁との緊密な連携、警察や自衛隊の選択と集中による効率的な運用などが重要となる。特にサイバー攻撃の無害化¹¹に際しては、状況に応じて警察のサイバー特別捜査隊や自衛隊のサイバー防衛隊等が投入されるものと考えられるが、勢力が限られていることから、15 分野の重要インフラの中から攻撃者の特定状況、被害の程度、国民生活や社会経済活動等に及ぼす影響などの状況を勘案して決定された優先順位に基づいて対処することになる。この際、当該優先順位をどのように決定し、どの組織がいかなる指揮・統制システムで無害化活動を行うか、その際の官官連携、官民連携の要領などについて予め定めておくこと、当該活動に必要な法改正などが必要である。

¹¹ 確認された攻撃サーバー等を無効化するなどの措置。有識者会議に提出された資料では「特定の APT が用いる技術の弱体化等の取組」、「サイバー犯罪者の海外サーバーの無効化」などの例示がある。

この他、各省庁の事案発生に伴い政府として一体となった対応が必要となる情報セキュリティに係る事象にはCYMAT (Cyber Incident Mobile Assistant Team、情報セキュリティ緊急支援チーム) が対応に当たっている。CYMAT は要請に応じて各府省庁の登録要員が出動して支援する互助組織で、各府省庁から指名を受け、情報セキュリティに関する技能・知見・関心を有する所属職員を、要員として内閣官房に併任している。要員の派遣が困難な府省庁は、要員育成等の観点から研修員の枠で参加するなどしているが、いずれにしても現行の体制は十分ではなく、各省庁は現職ポストに関係なく、コンピュータやサイバーセキュリティに知見のある職員を積極的に指名して CYMAT の拡充を図るとともに、全府省庁横断的な連携要領などについて改めて検証し、有事を想定した演習等を通じて実力を高めておく必要がある。

(2) 警察のサイバーセキュリティと官民連携

現在の我が国のサイバーセキュリティは犯罪防止・対策の観点から警察が大きな役割を担っている。2022年4月に施行された「警察法の一部を改正する法律」に基づき、サイバー事案について捜査指導、解析、情報集約・分析、対策等を一元的に所掌するサイバー警察局が新設され、サイバー事案の取締りが一層強化された。このほか警察庁、管区警察局などの情報通信部¹²に、都道府県警察のサイバー事案対策部門を技術的な面から支援するサイバーフォースを設置している。サイバーフォースは、個々の重要インフラ事業者等に対する脅威情報の提供や助言、サイバーテロ対策協議会との連携、共同対処訓練を実施するなどして、官民連携の強化に努めており、サイバー事案発生時には都道府県警察と連携し、被害状況の把握、被害拡大の防止、証拠保全等について技術的な緊急対処を行っている。特に警察庁のサイバーフォースセンターは、全国のサイバーフォースの司令塔の役割を担っており、サイバー事案発生時においては緊急対処を行う拠点として機能するほか、24時間体制でサイバー事案の予兆・実態把握、標的型メールに添付された不正プログラム等の分析、全国のサイバーフォースに対する指示等を行う。またサイバーフォースセンターでは、リアルタイム検知ネットワークシステムによりサイバー事案の予兆・実態等を把握している。同システムは、インターネット上にセンサーを設置し、当該センサーに対して送られてくる通信パケットを収集・分析することにより、インターネットに接続された各種機器の脆弱性の探索行為、当該脆弱性を悪用した攻撃、不正プログラムに感染したコンピュータの動向等、インターネット上で発生している各種事象等を把握することができる。

¹² 管区警察局情報通信部（四国警察支局情報通信部を含む。以下同じ。）、東京都警察情報通信部、北海道警察情報通信部、府県情報通信部（四国警察支局の管轄区域内の県情報通信部を含む。以下同じ。）及び方面情報通信部

警察による官民連携の観点では、日本サイバー犯罪対策センターとの連携、サイバー防犯ボランティアに対する支援、サイバーテロ対策協議会等を標的としたサイバー事案への対策の推進など、多方面にわたる官民連携に取り組んでいる。また、情報窃取の標的となるおそれの高い先端技術を有する全国約8,600の事業者等（2023年現在）との間で情報窃取を企図したサイバー攻撃に関する情報共有を行うサイバーインテリジェンス情報共有ネットワークを構築しており、このネットワークを通じて事業者等から提供された情報を集約するとともに、その他の情報を総合的に分析し、事業者等に対して分析結果に基づく注意喚起を行っている。重要インフラについては、サイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成するサイバーテロ対策協議会を全ての都道府県に設置し、個別訪問によるサイバー攻撃の脅威や情報セキュリティに関する情報提供、民間有識者による講演、参加事業者間の意見交換や情報共有を行うほか、共同対処訓練やサイバー攻撃対策セミナーを実施して緊急対処能力の向上に努めている。

(3) 防衛省・自衛隊の官民連携

国家防衛戦略では防衛省・自衛隊のサイバーセキュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進するとしている。2013年、防衛省はサイバーセキュリティに関心の深い防衛産業10社程度（保全の関係から詳細は明らかにされていない）をメンバーとするサイバーディフェンス連携協議会（DDC）を設置した。防衛省がハブとなり、防衛産業間において情報共有を実施することにより、情報を集約し、サイバー攻撃の全体像の把握に努めることとしている。防衛省・自衛隊が任務を遂行するためには防衛産業が正常に機能していることが不可欠であり、このために必要な防衛省と企業間、企業相互（防衛省がハブとなって提供）の間で情報を共有するとともに、標的型メール攻撃など防衛産業に特徴のあるサイバー攻撃についてベストプラクティスの共有を実施することなどを目的としている。重要インフラについて、自衛隊による防護等の計画はあるもののサイバー防御に係る連携はなく、本協議会を拡充するか、新たに重要インフラを対象とした協議会を設ける等、情報共有などサイバー防御に係る連携に取り掛かる必要がある。

防衛省のサイバー対策やACDの実施に当たっては通常より高いレベルの秘密情報を扱うこととなる。本年5月に成立・公布された重要経済安保情報保護活用法¹³により我が国においてもようやくセキュリティクリアランス制度が確立される。内閣官房の解説によるとサイバー脅

¹³ 重要経済安保情報の保護及び活用に関する法律（令和6年法律第27号）。1年以内に施行されることになっている。

威・対策等に関する情報¹⁴等についても、一定のものを重要経済安保情報として有効期限付きで指定するとされている。本制度の適用により、防衛省・自衛隊と通信事業者等との間でもこれまで以上に高いレベルの秘密保全が保証され、サイバー領域における防衛省・自衛隊と通信事業者等の連携強化が期待される。このような中、防衛省は一般幹部候補生（陸自）に、サイバー等の専門分野に特化した採用区分を新設し、2025年度から募集を開始するという。報道によると人材確保のために採用時身体検査基準を緩和するなど一般の自衛官とは異なる制度として要員の確保を目指すようであるが、通信事業者等でさえ採用に苦しむ中、高いスキルのサイバー要員を十分に揃えることは厳しいであろう。また常に最新の状態を維持すべく更新を要するサイバー専用機器なども、通常の防衛力整備では更新が間に合わない。人事異動を含め、様々な要因によって生ずる恐れのあるリスクを補完し、最新の技術力に追随するためにも通信事業者等との連携はますます重要になってくる。ところで、平素の業務における通信事業者等との連携や現在のCDCの活動は、本格的な武力攻撃事態を想定したものとはなっていない。通信事業者等を対象としていない自衛隊法第103条¹⁵やサイバー空間における文民保護などについても整理しておかなければならない。有事において重要インフラ等をサイバー防御するためには、平素からリモートによる連携に習熟し、いざという時に現場に出動した自衛官と通信事業者等の技術者等が、サイバー空間において連携できるようにしておくなどの措置を講じておかなければならない。

ロシアによるウクライナ侵略では、サイバー攻撃による被害は国内の重要インフラはもとより他国にも拡大していった。また、重要インフラに対するサイバー攻撃は、国外のボットやC2 (Command and Control、(遠隔攻撃用の) コマンド&コントロール) サーバー (以下、「ボット等」という) などを踏み台として行われる可能性が高い。このようなサイバー攻撃に対処するためには、グローバルに展開する国内外の通信事業者等や、ボット等が所在する国の協力が不可欠である。米国はウクライナにおいて HFOs (Hunt Forward Operations、ハント・フォワード作戦) を行った。HFOs は、パートナー国の要請に応じて USCYBERCOM が実施する防衛的サイバー作戦で、派遣された HFOs チームは、パートナー国の同意を得た上で重要インフラなどのネットワークに監視器材を接続し、悪質なサイバー活動を監視・検出する。HFOs で探知した知見やマルウェアは CISA、FBI、通信事業者等とも共有され、じ後の対応に活用される。

¹⁴ 我が国の重要なインフラ事業者の活動を停止又は低下させるようなサイバー攻撃等の外部からの行為が実施された場合を想定した政府としての対応案の詳細に関する情報 (内閣官房公表資料から抜粋)

¹⁵ 自衛隊法第103条では、自衛隊の行動に係る地域以外の地域において都道府県知事は、自衛隊の任務遂行上特に必要があると認めるときは医療、土木建築工事又は輸送を業とする者に対して業務従事を命ずることができるが、通信事業者は含まれておらず、有事における通信インフラ等の保守整備機能が確保できていない。

ACD の実効性を高める上でも、平時やグレーゾーン事態において米国等による HF0s 作戦の受け入れの可否を検討するとともに、自衛隊についても状況により国内の重要インフラなどに対して HF0s のような活動を行える法的枠組み、制度や体制などを整える必要がある。

警察は犯罪対策の観点から様々な取組を推進し民間等との連携を図っているが、自衛隊はサイバーに関する平時任務を有しておらず、サイバーセキュリティが自組織に限られることから警察のような枠組みや実績はない。サイバーセキュリティに関し、中央では NISC を介するなどして極めて限定的な人的交流等はあるものの、地方における自衛隊と警察の間にサイバーセキュリティに関する連携はない。自衛隊に平素の情報収集、監視、無害化などの任務が付与された場合、中央レベルはもとより重要インフラの所在する現場レベル（方面総監部と管区警察局等）においても、POC（Point of Contact、連絡窓口）の設置、重要インフラに対するサイバー攻撃に関する情報共有や重大インシデント発生に際しての連携要領、ACD に際して自衛隊が本格的な無害化措置を行う場合の情報共有や対処における役割分担などを定め、平素からの交流や事態対処演習などを通じて連携を深めておくことが必要である。

(4) サイバーセキュリティにおける官民連携の現状

有識者会議で「人口減少社会において、社会全体の強靱性を維持するためには、官民が連携してサイバーセキュリティの確保に努めていくことが必要であり、そのためには情報共有が最も重要」と指摘している通り、官民連携において情報の共有は極めて重要である。

重要インフラに対するサイバー攻撃に対しては、新 NISC と重要インフラ所管省庁が緊密に連携して重要インフラに係る政府としての情報共有体制を確立するとともに、重要インフラ事業者、サイバーセキュリティ関係機関、通信事業者等、組織・分野の枠組みを超えたオールジャパンによる情報共有体制を構築し、強化しなければならない。現在、サイバー攻撃の送信元に関する情報の共有や、送信元が特定できない場合において送信元を特定するための調査研究等の業務を行う第三者機関を総務大臣が認定する制度として「認定送信型対電気通信設備サイバー攻撃対処協会」があるが、制度開始当初から大手電気通信事業者を含む4社で推移しており、更なる強化が必要であろう。この他、情報共有の観点から今後ますます重要な役割を担うものと期待される組織としてサイバーセキュリティ協議会（以下「協議会」という）が挙げられる。協議会はサイバーセキュリティ基本法に基づいて組織された法定の情報共有体制であり、国の行政機関、重要社会基盤事業者、サイバー関連事業者や教育研究機関など官民の多様な主体が相互に連携し、早期の段階から対策情報等を共有することにより、サイバー攻撃による被害の拡大を防ぐことなどを目的としている。協議会のメンバーは、

国の関係行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業、大学・教育研究機関等の中で協議会の活動に賛同する者とされており、運営委員会の承認を得なければならない¹⁶。協議会には守秘義務¹⁷が課されており、これにより通信量の急激な増加、サーバー等のハングアップ、特定のサイトへの接続が遅いなど「いつもとは何か違う」といった極めて初期の不確かな段階であっても、安心して情報提供や相談を行うことが可能となっている。情報提供者による情報共有範囲の設定や、監督官庁等を情報共有範囲から除外することなども可能であるほか、情報提供義務の発動要件を大規模なサイバー攻撃、同意がある場合等に限定するなど、参加者の活動リスクを軽減している。このような制限等は、これまで活動の活性化を妨げていた要因を洗い出し、これを法律改正等によって改善することにより、既存の情報共有体制の活動を補完し、これらと有機的に連携しつつ従来の枠を超えた情報共有体制を構築していくことを目標として設けられた規定である。他方、情報提供者が情報共有範囲を設定できる点や監督官庁等を情報共有範囲から除外可能とするなど、情報共有には一定の制限が存在するため、重要インフラに対するサイバー攻撃が予測され、あるいは既にサイバー攻撃が行われた段階において本当にこれで十分か検証し、情報共有の義務化などについて見直さなければならない。

協議会は早期警戒情報の提供システム「CISTA¹⁸」を有する他、「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づく情報共有体制、サイバー情報共有イニシアティブ、日本サイバー犯罪対策センター、サイバーセキュリティ対処調整センター、重要インフラ分野の各セプター、ISAC¹⁹等、主要な情報共有組織が多数参加しており適切な連携が可能とされているが、現場の下部組織は複数の体制に加入して活動することとなり、情報共有のための活動に伴う負担軽減を考慮する必要がある。極めて信頼度が高く、重要な役割を有する協議会であるが、ACD体制の構築に際しては情報共有範囲や情報連絡の速達、情報発信のワンボイス化、他セキュリティ組織等との関連性を考慮しつつ、改めてサイバーセキュリティに係る情報共有の「核」として位置づけ、ACDの実効性を確保する観点から情報連絡・提供の流れを整理した方がよいものと思われる。

他にも官民連携に欠かせない組織として一般社団法人ICT-ISACがある。ISACとは特定の業界に特化した情報共有と分析を行う組織を指し、他に電力ISAC、医療ISAC、金融ISAC、交通ISACなどがある。ICT-ISACはICT分野のサイバーセキュリティに関する観測・分析や共同対処を目

¹⁶ 協議会の目的達成または活動に支障を生じるおそれがある場合は承認しない場合があるとされている。

¹⁷ 罰則（サイバーセキュリティ基本法）により担保された高度な守秘義務によって情報提供者名等の漏洩を防止している。

¹⁸ Collective Intelligence Station for Trusted Advocates、JPCERT/CCが運営する早期警戒情報に関する提供システム

¹⁹ Information Sharing and Analysis Center、業界内での情報共有・連携の取組推進を図る組織

的として、ISP（Internet Service Provider、接続サービスを提供する通信事業者等）、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者を含む幅広い分野の事業者によって設立されたもので、多様な事業者が業界の枠を超えて連携・協調する組織として活動している。2019年には総務省から「認定送信型対電気通信設備サイバー攻撃対処協会」の認定を受け、NOTICE（National Operation Towards IoT Clean Environment、次項で詳述）プロジェクトにおいても NICT（National Institute of Information and Communications Technology、国立研究開発法人情報通信研究機構）の観測情報を基に ISP に対処を要請するなどの調整役を担っている。活動は経路情報共有 WG、DoS 攻撃即応 WG、IoT セキュリティ WG、サイバーセキュリティ協議会対応 WG、国内外 ISAC 連携など、多くの Working Group に区分して取り組まれている。それぞれの WG に責任会社が指定されているが、この責任会社には日本を代表する IT 企業等が就いており、サイバーセキュリティ、特に民間の技術力や組織力を活用するという観点から欠かせない存在になっている。他方、活動は通信事業者等の自主性によるものとなっているが、①官民連携の強化、②情報共有基盤の整備、③他の国内 ISAC（金融 ISAC、電力 ISAC、交通 ISAC など）との連携強化、④米国の ISAC（IT-ISAC、Communications ISAC、National Council of ISACs など）をはじめとする諸外国との連携強化等、活動を強化するための取組は通信事業者等のみでできるものではない。現在の ICT-ISAC は総務省との関係が深い。新たに創設される新 NISC との関係強化・再整理するなど、官側との連携を抜本的に強化して諸課題の解決に取り組むことが重要である。

4 重要インフラのサイバーセキュリティにおける官民連携の実態

(1) Volt Typhoon 事案に対する我が国の対応

2024年6月25日、JPCERT/CC（Japan Computer Emergency Response Team Coordination Center、一般社団法人JPCERT コーディネーションセンター）は、「Operation Blotless²⁰攻撃キャンペーンに関する注意喚起」を公表した。Operation Blotless 攻撃のうち、多くの公開情報が出ている Volt Typhoon による LotL 攻撃のように、明確に侵害の有無を判断できないケースを想定した上での「推奨対策（中長期的な対策）」について、①メーカーからの脆弱性情報が直接エンドユーザーに届かないケースや代理店などを経由して伝達が遅延するケースについて可能な限り速やかに重要な脆弱性情報を入手できるよう伝達経路や確認方法の見直しを行うこと、②脆弱性情報入手後の速やかな対策や回避策を適用できるよう運用保守を担当する組織やグル

²⁰ LotL 戦術を用いて長期間・断続的に攻撃キャンペーンを行う APT

ープの中での対応体制について確認することと紹介している。重要インフラを防護する上で、脆弱性に関する情報は極めて重要であるものの、サプライチェーンを含む周辺環境に至るまで情報を行き届かせることは難しく、推奨対策を徹底する方策を講じる必要がある。

総務省は、2018年からNICT、ICT-ISAC、ISPなどの協力を得てNOTICEを推進している。NOTICEはサイバー攻撃に悪用されるおそれのあるIoT機器をNICTで調査し、NOTICEに協力しているISPのネットワークに直接接続されているIoT機器を定期的に観測し、悪用のおそれがあると特定したIoT機器のグローバルIPアドレスや脆弱性などの情報をISPに通知、通知を受けたISPは当該IoT機器の管理者・利用者に対して、電子メールや郵便で注意喚起を実施するというものである。当初、2023年度末までとされていたID・パスワードに脆弱性があるIoT機器の調査を2024年度以降も継続し、NOTICEの枠組みを通じた注意喚起を継続することとなった。他方、重要インフラを構成するネットワークは複雑かつ広範囲で、サプライチェーン上にある無数のIoT機器はサイバー攻撃の絶好の標的であり、その脆弱性を完全に除去することは難しい。例えば、NOTICEの観測対象はインターネットに接続されたルーターやネットワークカメラなどのIoT機器のみであり、その先のSOHOや工場内などのプライベートネットワークに繋がっているPC、スマホ、家電などの情報を収集するものではない。注意喚起も電子メールや郵便で行なうものとなっており、速達や徹底の観点から見直しが必要と思われる。

米国のCISAは、重要インフラの監視システム内のカメラにVolt Typhoonの攻撃者がアクセスできるようになっていた事例があったと分析しており、我が国の重要インフラについても予期しない機器から制御システム等に関するクリティカルな情報が抜き取られ、時が来れば大きなダメージを与える攻撃が行われる可能性がある。排除し尽くせない脆弱な機器に対して有効な対策をとることは困難であるが、これを打開すべく、2023年にNICT法を改正し、新たな業務としてファームウェア²¹に脆弱性があるIoT機器の調査をNICTの業務²²として位置付け、NOTICEの枠組みを通じてルーターやネットワークカメラなどのIoT機器の乗っ取りや、IoTボットネットへの対処を総合的に推進する取組を開始している。これによりNOTICEは注意喚起を行うものから、IoT機器の乗っ取りやIoTボットネットへの対処を総合的に推進する役割を担うようになった。このようにNOTICEは重要インフラを防護する上で極めて重要な取組であり、我が国の重要インフラ周辺に残る脆弱性あるIoT機器を一掃する安全保障上の重要案件の一つとして国家的取組に格上げすべきである。

²¹ 電子機器に組み込まれたコンピュータシステム（ハードウェア）を制御するためのソフトウェア

²² NICTが行うパスワード設定などに不備のあるIoT機器を観測するための行為（機器にID・パスワードを入力するなどの行為）は「特定アクセス行為」として「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」に定められたものであり、不正アクセス禁止法における「不正アクセス」には該当しない。

(2) 重要インフラに対するサイバー攻撃への対応

重要インフラ事業者はサイバーセキュリティインシデントが発生した場合、適用される業法に基づく法的義務としての対応が求められる。サイバーセキュリティ基本法により事業継続のための努力義務が求められており、国民生活や社会経済活動に重大な影響を及ぼす重要インフラに対するサイバー攻撃について、行動計画等に基づいて NISC や重要インフラ所管省庁等が中心となって対処体制を強化することとされている。重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関する情報のうち定められたケース²³に該当する場合には、重要インフラ所管省庁を通じて NISC に対する情報連絡を行う。

2020 年 11 月 26 日、NISC から「ランサムウェアによるサイバー攻撃について(注意喚起)」が公開²⁴された。対応策の全体像を把握する上で参考になることから一部を掲載する。

- 組織のネットワークと外部との接続点の堅牢性について確認のうえ、対策（セキュリティパッチの迅速な適用、不要なポートやプロトコルを外部に開放しない等）が必要
- リモートアクセス環境を構成する製品、迅速なアップデートや適切な設定が行われているか確認（迅速なセキュリティパッチの適用、VPN 機器やクラウドサービスに対する多要素認証の導入）が必要。特に VPN に対するセキュリティ対策に留意
- 自組織で使用している PC やサーバー等の OS、アプリケーション等が常に最新化されているか確認
- 必要な機器にウイルス対策ソフトが導入され、パターンファイルが最新化されているか確認する。また定期的なスキャンが実行される設定になっているか確認
- 重要なデータに対する定期的なバックアップの設定を確認。バックアップに当たっては、ランサムウェア感染時でもバックアップが保護されるように留意
- バックアップで取得したデータをもとに、実際に復旧できることを確認
- 公開された場合、業務に支障が生じるような機微データや個人情報等に対して、特別なアクセス制御や暗号化を実施
- システムの再構築を含む復旧計画が適切に策定できているか確認
- サーバー、ネットワーク機器、PC 等のログの監視を強化。振る舞い検知、EDR(Endpoint Detection and Response)、CDM(Continuous Diagnostics and Mitigation)等を活用
- データの暗号化及び公開を想定した対処態勢、対処方法、業務継続計画等を含むランサムウェアへの対応計画が適切に策定できているか確認

また、経済産業省は 2023 年に「ASM 導入ガイダンス」を公表²⁵した。ASM (Attack Surface Management、攻撃対象領域管理) は組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスで、不正侵入経路となりうるポイントを把握することができる。これにより組織自身が把握していない端末機器や意図しない設定ミスを攻撃者の視点で発見し、リスクを低減する効果

²³ ①法令等で重要インフラ所管省庁への報告が義務付けられている場合、②関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合、③そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合

²⁴ <https://www.nisc.go.jp/pdf/policy/kokusai/press-1221.pdf>

²⁵ <https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf>

を期待できる。NIST (National Institute of Standards and Technology、アメリカ国立標準技術研究所) の定義によると、Attack Surface とは、攻撃者の視点からサイバー攻撃が行われる可能性があるデジタル資産やサービス、環境を指し、クライアント端末、モバイル端末、IoT デバイス、サーバー、VPN といったネットワーク機器の他、ソフトウェア、クラウドサービス、サプライチェーンを構成するサービスなど広範囲に及ぶ。従前の ASM では外部公開されている Attack Surface を重視する傾向にあったが、LotL などサイバー攻撃の高度化により、組織内への侵入を前提とした対策がとられるようになってきた。外部公開されている Attack Surface のみならず、攻撃者に悪用されうる内部のデジタル資産を全て含めた対策が求められる。

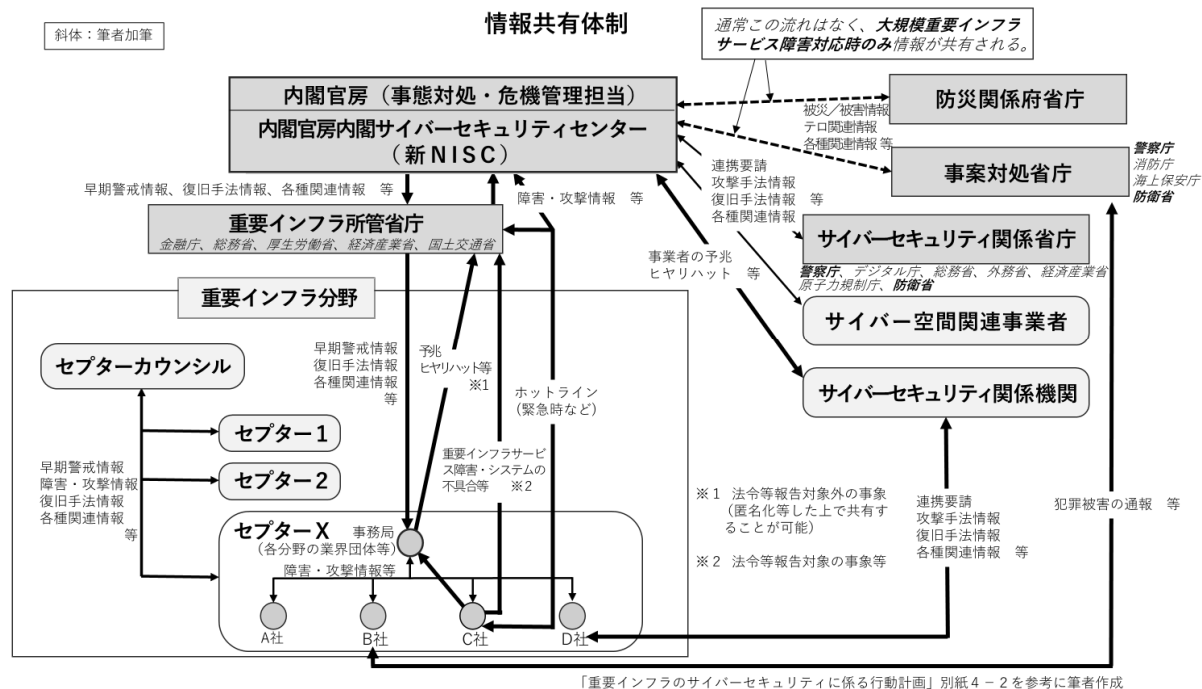
重要インフラのような巨大なネットワークでは、サプライチェーンが脆弱な鎖となり、組織全体に深刻な被害を及ぼす危険性がある。ASM はドメイン名が分かればリスク評価ができることから、自社のみならず子会社・関連会社・サプライヤーのセキュリティ対策状況の把握・管理が可能となり、サプライチェーン全体のサイバーリスク対策につながる。

米国は CISA による 2022 年の通知において、政府機関に対して 1 週間ごとに自動化された資産探索を実行し、そこで見つけた資産の脆弱性について 2 週間ごとに一覧化を行うこととしている。我が国においても重要インフラのサイバーセキュリティを推進するにあたり、ASM について企業の自主性に任せるのではなく、国として総合的に取り組むべき課題である。特に重要インフラ所管省庁は、所管する企業に対して ASM を早期に導入して IoT 機器などのリスクを低減し、継続的に脆弱性を排除するよう指導することが必要である。また、重要インフラに対してサイバー攻撃が行われた場合、JPCERT/CC から注意喚起や個別通知が通知されるものの、中小規模の事業者や個人にはなかなか情報が伝わり難い。重要インフラのサプライチェーン上にある脆弱な機器や、侵害されている可能性のある機器の利用者にしっかり情報を届け、現場が行う対策のために必要な支援を行うことが、重要インフラ及びサプライチェーン全体のサイバーリスク対策において極めて重要である。

(3) 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情報共有と対応

重要インフラに係る情報共有に関しては、基本法第 12 条に基づいて定めている「サイバーセキュリティ戦略」において情報共有体制の拡充が打ち出されており、行動計画に基づいて具体的な取組が進められている。重要インフラは高度にシステム化するとともに、サプライチェーンの複雑化等に伴い、関係主体間での相互連関・連鎖性が深く、ある重要インフラにおける障害が複数の重要インフラや重要インフラサービス障害に至る可能性が高い。被害を受けた主体単独によるサイバーセキュリティ対策には限界があり、相互依存性のある重要イ

ンフラによる分野横断的な情報共有や対策が求められる。下図は「重要インフラのサイバーセキュリティに係る行動計画」別紙第 4-2 に筆者が加筆したものである。図から分かる通り、新 NISC と防災関係府省庁、事案対処省庁（警察庁、消防庁、海上保安庁、防衛省）との間の情報共有は大規模重要インフラサービス障害対応時のみとされている。



行動計画に基づく情報共有の手引書によると、重要インフラにおける「システム²⁶の不具合等に関する情報」には重要インフラサービス障害の未然防止、拡大防止・迅速な復旧、原因等の分析・検証による再発防止の3つの側面が含まれる。また、その流れには、重要インフラ事業者等から重要インフラ所管省庁に連絡し、それを重要インフラ所管省庁が NISC に連絡する「情報連絡」と、サイバーセキュリティ対策に資するための情報を NISC から重要インフラ所管省庁に提供し、それを重要インフラ所管省庁が重要インフラ事業者等に対して提供する「情報提供」がある。これらは基本法に基づいて構築されたものであるものの、法令等で義務付けられている訳ではなく、重要インフラ事業者の自主的な協力によって成り立っている。また、これまで外部との接続がないとして安全と考えられていた制御システム等においてもサイバー攻撃が確認されていることから、これらに対する脅威や脆弱性等の共有についても対策を講ずるべきである。

²⁶ ここでいう「システム」には、いわゆる情報系システムに限らず、各重要インフラ分野のプラントやシステム監視等でも用いられる制御システムや IoT 等も含む。

行動計画に基づく情報共有は「システムの不具合等に関する情報」を対象としているが、これは事象（不具合）の情報であって、原因別に区分されたものではない。不具合等の原因は①サイバー攻撃等の「意図的な原因²⁷」、②操作ミス等の「偶発的な原因」、③災害や疾病等の「環境的な原因」、④「その他の原因」の4つに分類されているが、グレーゾーン事態ではサイバー攻撃による被害を②～④だと誤って認識させるような「振る舞い」をする可能性もあり、真に実効性あるサイバー防御を行うためには、①の「意図的な原因」を検知する体制を重点的に強化することが必要である。

重要インフラ事業者等の情報共有を担う組織としてセプター（CEPTOR²⁸）がある。法令等で報告が義務付けられていない事象などについては、情報連絡元の匿名化等を行った上でセプター事務局を經由して重要インフラ所管省庁に報告することが可能とされている。情報共有のための情報連絡様式に記載する情報には、企業情報や機微情報等が含まれることから、適切なTLP（Traffic Light Protocol、情報共有範囲）を設定することとされており、RED、AMBER+STRICT、AMBER、GREEN、CLEARに区分されている。

情報共有範囲（TLP）

区 分	情報共有先
RED	受信者個人に限定
AMBER+STRICT	ある組織のみに共有を限定
AMBER	限定公開、情報の受信者は Need to know の原則に基づき組織内やそのクライアント ²⁹ にのみ共有できる。
GREEN	限定公開、情報の受信者はコミュニティ ³⁰ 内に情報を共有できる。
CLEAR	公開

事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者等に対する情報共有は GREEN からとなっており、迅速な事態対処を踏まえた情報共有として適切かどうか再考が必要と思われる。また、TLP は情報連絡の各段階において報告者（重要インフラ事業者等、セプター事務局、重要インフラ所管省庁など）が設定することになっており、過重な設定により情報共有先を狭めてしまうと、事態対処が遅延する場合なども考えられる。情報発信者が情報共有範囲に含まれない対象の追加を求める場合は、当該対象を共有範囲に含めることができるとされているが、そのような場

²⁷ 不審メール等の受信、ユーザーID等の偽り、DDoS 攻撃等の大量アクセス、情報の不正取得内部不正、適切なシステム運用等の未実施

²⁸ Capability for Engineering of Protection, Technical Operation, Analysis and Response

²⁹ ある組織からサイバーセキュリティのサービスを受ける人々や事業者

³⁰ 共通の目標、慣習、非公式な信頼関係を持つ集団

合に迅速な対応を行うため、継続的な担当者の養成、実際的な訓練の実施などが重要である。

NISC は、重要インフラ事業者や重要インフラ所管省庁などの関係部署から提供される幅広いシステムの不具合等に関する情報を集約、分析等して情報を提供する。情報は提供元が特定されないよう、情報を加工するなど、不利益を被らないための適切な措置を講じた上で NISC から重要インフラ所管省庁を通じてセプター事務局、あるいは必要に応じて直接重要インフラ事業者等に提供される。一刻を争うようなサイバー攻撃を受けた際、このような流れをいかにスムーズかつ迅速に行うかが重要となる。

サイバーセキュリティ対策には経営層やそれに近い職位の高い意識と強いリーダーシップが求められる。2022 年にトレンドマイクロ株式会社と株式会社日経リサーチが行った「サイバーセキュリティに関する調査」によると、CISO (Chief Information Security Officer、最高情報セキュリティ責任者) または CSO (Chief Security Officer : 最高セキュリティ責任者) を社内に設置している企業は 38.7%、CISO/CSO とは異なるセキュリティトップの配置を含めると 73.3%にのぼり、いずれも設置していないという回答は 24.3%であった。CISO/CSO の内訳は経営者が 7.3%、役員クラスが 64.5%、計 7 割以上が経営に関与する重要なポジションを担っているとされ、サイバーセキュリティの体制は整ってきたが、未だ設置のない企業に対して CISO/CSO の設置を促す必要がある。CISO/CSO を通じて社内における意識の高揚やサイバーセキュリティに関する取組の強化を行うためには、CISO/CSO に対する継続的な最新情報の提供が重要である。政府はサイバーセキュリティ基本法施行令に基づき、関係行政機関の最高情報セキュリティ責任者等 (CISO/CSO、局長等が兼任) 相互の緊密な連携の下、サイバーセキュリティ戦略本部にサイバーセキュリティ対策推進会議 (以下「推進会議」という。) を設置した。推進会議の実質的な運営は同会議に置かれたサイバーセキュリティ対策推進専任審議官等会議 (以下「専任審議官等会議」という。) が担っており、メンバーは各府省庁に設置されたサイバーセキュリティ・情報化審議官 (部長級、原則として専任) となっている。サイバーセキュリティ・情報化審議官は各府省庁の CISO/CSO を直接補佐し、各府省庁におけるサイバーセキュリティ対策の実質的な司令塔であることから、専任審議官等会議と重要インフラ及びサイバー関連事業者等の CISO/CIO 間の連携を具体化するなど、政府と重要インフラ等の CISO/CIO 間の連携を強化して、サイバーセキュリティの実効性を確保することが重要である。

(4) 自助、共助及び公助

行動計画ではサイバーセキュリティのための情報共有について「自助ありきの共助」としており、「官」の役割 (公助) は「自助と共助(互助)を促進させるための公助」とした上で情

報共有における「共助」を推進することとしている。サイバーセキュリティにおける情報共有はあくまでも重要インフラ事業者等の自主的な取組が前提となっている。このような前提の下、情報共有体制を強化するためには、協議会やICT-ISACの情報収集・分析能力を強化するとともに役割を見直し、分野間連携や業界を超えた連携等により通信事業者等自身の対処能力を高めることが第一である。一方、サイバーセキュリティ対策は企業・経営者自らが主体性を持って取組む「自助」が前提であるものの、サイバー攻撃が高度化・複雑化する中で組織単独での対策には限界があり、特に中小企業が単独で CSIRT (Computer Security Incident Response Team、シーサート) のようなインシデント対応組織を設置することは難しい。このため、お互いが助け合う「共助」の部分強化するための「公助」による支援が不可欠である。

企業間での情報共有を促す場・手法として、重要インフラで構成されるセプターカウンスル、重要インフラの各業界における情報共有・分析組織が重要になってくる。「共助」のための枠組みとして、同じ業種に属する企業間の協力組織である ISAC や、重要インフラ企業が業種横断で協力を行う産業横断サイバーセキュリティ検討会、企業 CSIRT の連合体である日本シーサート協議会 (NCA) などがこれにあたる。このようなサイバーセキュリティ関係機関は、企業から独立した中立的な観点から、国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっているとされており、政府も行動計画などにおいて情報共有体制におけるメインプレーヤーのひとつとしての活動を期待しているが、そのためには政府と通信事業者等がお互いの立場・役割を尊重し、それぞれの強みを活かしながら一体となって情報共有関係を構築する必要がある。

ボット等が国内ネットワーク上にある場合、通信事業者等との連携によってその所在を検知することは可能であり、米国が Volt Typhoon の攻撃に対処した例などはこれに該当する。他方、現実に攻撃者が踏み台とするボット等は海外のネットワーク上に所在するケースが圧倒的に多く、これに対処するためには海外の通信事業者等及びボット等が所在する国の協力が不可欠である。

米国の CISA は 2021 年 8 月に JCDC (Joint Cyber Defense Collaborative、統合サイバー防衛連携) を設立した。これは CISA が中心となり、米軍のサイバーコマンド、NSA、FBI、国家情報局などの政府機関に加え、ICT 関連企業、重要インフラ企業からなる官民一体型の組織で、官民合同のサイバー防衛計画、サイバーセキュリティ情報の融合、重要インフラ、及び国家重要機能へのリスクを低減するためのサイバー防衛ガイダンスの普及を主導する。我が国からは 2023 年 1 月に日本電信電話株式会社 (NTT) がアジアで最初のメンバーとして加入している。

我が国においても 2021 年に策定されたサイバーセキュリティ戦略において、自助共助では

対応できないような事象に対して、国がインシデント対応とその後の再発防止や改善に向けた政策措置を一体的に推進するための総合的な調整を担う機能として、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（CSIRT/CERT）の枠組みの強化を図りつつ、それが一層果たされるよう検証による向上・充実強化を図るとされた。現在の CSIRT/CERT は NISC となっている。NISC はナショナルサートの総合調整役として、①政策対応、②対処調整、③情報収集・対処、④情報集約・分析の各機能を具備するために、2022年6月に体制を見直し、更に国家安全保障戦略を踏まえ抜本的に強化されることになっている。平素のサイバーセキュリティや ACD を実効性あるものにするためには、警察や自衛隊、通信事業者等との緊密な連携は不可欠であり、将来的には新 NISC の下、重要インフラのサイバーセキュリティに関連する政府機関、ISP、重要インフラ事業者等に防衛省・自衛隊を加えた米国の JCDC のような体制についても検討すべきである。

5 まとめ

重要インフラのサイバー防御における官民連携について考察してきたが、総括すると下記の 5 点に集約される。

- ① 重要インフラのサイバー防護は守備範囲が広く、組織や仕組みが複雑で分かり難い。緊急性の高い情報発信は、発信機関ごとに差異が生じないように、ワンボイスで行う³¹など窓口を一本化するとともに、AI 等の導入による業務の簡素化等、再整理が必要
- ② 官官連携について、組織上、法制上の縦割り観が否めない。ACD は新 NISC、警察及び自衛隊の能力強化と通信事業者等との緊密な連携が鍵であり、JCDC のような官民一体型の体制について検討が必要
- ③ 官民連携や情報共有の枠組みはサイバーセキュリティ基本法をベースとしながら数多く構築されているものの、迅速性や徹底といった観点から整理統合するなど、見直しが必要
- ④ サイバー情報の収集や分析、事案発生に伴う対処における通信事業者等の役割は極めて大きいものの、企業の自主性に依存している。国家による基盤提供や予算措置などについて考慮するとともに、重要な情報連絡については義務化なども検討が必要
- ⑤ NOTICE や ASM は国家レベルで取組むべき重要施策と位置づけ、政府主導で取組むことが必要

³¹ 有識者会議「これまでの議論の整理（案）概要」（令和6年8月6日、内閣官房）から引用

巨大な重要インフラ分野を対象とし、官民連携に必要な体制や規則、業務手順などの複雑性を排して簡明かつシームレスなものを整えることは容易ではない。これを実現するためには新 NISC によるリーダーシップの発揮が不可欠であり、そのための体制整備や権限付与を惜しんではならない。また、重要インフラに対するサイバー攻撃が発生した場合、多くの所管省庁や重要インフラ事業者が参入することになるが、迅速な対処を求めれば求めるほど、事態は拡大・複雑化し、多くの確認や指示が行きかうなどして、いわゆる「エリートパニック³²」に陥る危険性がある。過去の大震災等に際しても見られた現象で、一刻を争うサイバー防御においては絶対に起こしてはならない。政府部内で情報提供や注意喚起を適切に行うとともに、サイバー事態における窓口を一本化し、その代替手段を明確にすること、現職の大臣や政策責任者、企業トップ等の参加によるリアリティのある演習などにより対処のための練度と覚悟を整えておくことが、事態に際して冷静さを保持し、的確に対処する力となる。

重要インフラは国民生活、社会経済活動にとって極めて重要であり、トライアンドエラーを繰り返しながら官民連携の実効性を高め、安全保障上の懸念を生じさせるような重大なサイバー攻撃を阻止・排除して、重要インフラの安全を確保してもらいたい。

³² 災害時などに、権力層にあるエリートたちが「一般の人がパニックを起こすのではないかと恐れ、エリート自身がパニックを起こすという考え方。アメリカのノンフィクション作家レベッカ・ソルニットの著書「災害ユートピア」で紹介された概念で、一般人によるパニックよりも、エリートたちのこうした過剰反応こそが社会に重大な影響を与えるとする。

[著者プロフィール]



住 田 和 明 (すみだ かずあき)

1984年 防衛大学校（機械工学科）卒業

同年陸上自衛隊に入隊

第2師団長

統合幕僚副長

東部方面総監

陸上総隊司令官を歴任し、

2019年退官