座談会
Round-table Discussion

わが国のサイバー・レジリエンス強化に向けた課題と方策

近年、国内の重要インフラや企業活動を標的とするサイバー攻撃が増大・高度化する中、わが国では2025年5月にサイバー対処能力強化法及び同整備法が成立した。今後は「能動的サイバー防御」の枠組みのもと、官民連携の強化や通信情報の適切な利用などを通じて、平時から有事まで一体的に対応できる環境を整備し、わが国全体のサイバー・レジリエンス強化を図ることが求められる。

そこで本座談会では、わが国のサイバー・レジリエンス強化に向けて、官民連携のもとで取り組むべき課題や方策について議論する。

岩村有広〈司会〉
いわむら　ありひろ
経団連常務理事

蓮見祥子
はすみ　さちこ
スターバックスコーヒージャパン
サイバーセキュリティ部部長
元国連CISOグループ共同議長

飯田陽一
いいだ　よういち
内閣サイバー官

遠藤信博
えんどう　のぶひろ
経団連副会長
サイバーセキュリティ委員長
日本電気特別顧問

篠田佳奈
しのだ　かな
BLUE代表取締役

サイバー・レジリエンス 強化に向けた 官民の取り組み

サイバーセキュリティをめぐる経団連の取り組み

岩村　初めに自己紹介も兼ねて、これまで取り組まれてきたことや、現在注力されている活動について、お聞かせいただけますでしょうか。

遠藤　私はこれまで経団連のサイバーセキュリティ委員長として、様々な活動に携わってきました。政府関連では、サイバーセキュリティ戦略本部の発足時から約10年にわたり審議に参画し、現在も引き続き連携させていただいています。

　日本では、２０１０年頃から徐々にサイバーセキュリティにかかわる危機意識が高まり始め、２０２０年東京オリンピック・パラリンピックの開催を見据え、２０１４年「サイバーセキュリティ基本法」の成立、２０１５年「サイバーセキュリティ戦略」の策定など、政策面の対応が進む一方、ＡＩの進展などを背景に、２０１０年代後半頃から一気にサイバー攻撃が活発化しました。社会活動を維持するうえで、サイバーセキュリティが極めて重要な要素となる中、経団連は、経営者が意識を高めない限り企業のサイバーセキュリティ対策は進まないとの問題意識のもと、２０１８年に「経団連サイバーセキュリティ経営宣言」を公表、経営層に対策を推進するよう呼びかけました。

　その後、コロナ禍によって社会・経済活動が変化する中でサイバー攻撃が増加し、事業活動や国民生活に深刻な影響を及ぼす事例が増えました。こうした状況も踏まえ、経団連は、２０２１年に誰もが主体的に危機意識を持って取り組む「Cybersecurity by All」（全員参加によるサイバーセキュリティ）の実現に向けて提言を公表し、翌２０２２年には、先ほどの経営宣言を「経団連サイバーセキュリティ経営宣言2・0」としてアップデートしました。具体的には、サプライチェーン全体を見据えたレジリエンス強化に向け、①経営課題としての認識、②経営方針の策定と意思表明、③社内外体制の構築・対策の実施、④対策を講じた製品・システムやサービスの社会への普及、⑤安心・安全なエコシステムへの貢献、という五つの柱を掲げ、企業に行動を促しています（図表1および19ページ参照）。

　また、国際連携の取り組みでは、２０２４年に経団連は英国政府に招かれるかたちで「日英サイバー協力ミッション」を派遣し、同国政府関係者と非常に有益な意見交換を行い、英国国家サイバー諮問委員会（ＮＣＡＢ）とは協力覚書も交わしました。サイバー攻撃への防御は、もはや個々の企業だけの問題ではありません。ミッション等の議論を通じて、日本全体としてのサイバー分野のレジリエンス力を高めていかなければならないことを、改めて認識しています。

図表１　経団連のこれまでの取り組みと主な提言

経団連では、サプライチェーン全体を俯瞰した
サイバーセキュリティ強化に向けた３本柱の取り組み
（産業横断／官民連携／国際連携）を推進

2018.3.16　サイバーセキュリティ経営宣言
- ✓ 東京オリンピック・パラリンピック競技大会までが重点取り組み期間
- ✓ 経営課題としてサイバーセキュリティを認識

2019.10.31　サイバーリスクハンドブック
- ✓ 全米取締役協会が作成した“Cyber Risk Oversight Handbook”の日本版
- ✓ 企業の取締役等が果たすべき役割等について、五つの原則を提示

2021.7.13　全員参加によるサイバーセキュリティの実現に向けて
- ✓ 政府の新たなサイバーセキュリティ戦略策定の動きを捉えた提言
- ✓ 誰もが主体的に危機意識を持って取り組む「Cybersecurity by All」実現に向けた三つの視点を提示

2022.10.11　サイバーセキュリティ経営宣言2.0
- ✓ サプライチェーン全体を俯瞰したサイバーセキュリティの強化

出所：経団連事務局作成

〝人間らしいサイバーセキュリティ〟とは

蓮見　私は、これまで、グローバル企業の金融機関やＯＥＣＤでＩＴやセキュリティに携わり、その後は国連機関のＣＩＳＯ（最高情報セキュリティ責任者）として、国や組織をまたいだサイバー対応に取り組んできました。

日英サイバー協力ミッション　NCABメンバーとミッション一行

覚書署名式（右からバーバー NCAB共同議長、ダウデン副首相、遠藤副会長）

　現在は企業のサイバーセキュリティに携わっていますが、有事と平時、国際と国内、官と民、それぞれの現場に立ってきた経験があります。

　こうした現場で感じるのは、どれほど制度や技術が整っていても、人の判断が追い付かなければサイバーセキュリティは機能しない、ということです。ルールや体制があっても、現場で適切に判断ができなければ、動けません。この経験から、〝人間らしいサイバーセキュリティ〟の構築を提唱しています。「人は迷う存在だ」という前提のもと、その迷いをどう支え、判断や行動を後押しする構造や仕組みをどのようにつくるかが重要だという考え方です。このような考え方を立場や組織を超えて共有していくために、学会での論文発表や講演活動、コラム執筆などを通じて、日々起きている現場の出来事を多くの人が共有できる言葉にして伝えていく取り組みも行っています。

　政策や技術が現場を動かすまでには長い距離があり、非常に難しいと感じています。これが国内外、様々な現場で見てきての実感です。今日は、現場の視点から、「能動的サイバー防御」について考えていければと思います。

現場の教育、若手の人材発掘・育成が重要

篠田　弊社は、国際的な情報セキュリティ会議である「CODE BLUE」を運営しています。CODE BLUEは、国内外からトップクラスの情報セキュリティ専門家を招き、国や言語の垣根を越えた情報交換と交流の機会を提供する国際会議です。年1回、過去13回開催し、講演に加え、実践的なワークショップを行っています。２０２５年は港湾、宇宙、ＩＣＴ、自動車、医療機器といった重要なインフラ分野について、海外の先駆的な取り組みを日本に紹介しました。また、25歳以下の方の登壇や学生スタッフを交えた運営など、協賛企業や参加者と若い世代とのネットワークづくりや、業界に入る前の準備の機会を提供しています。こうした取り組みが、将来のセキュリティ人材の育成につながることを期待しています。

飯田陽一
内閣サイバー官
（併）国家安全保障局次長

1989年、東京大学工学部卒業。同年、通商産業省（現経済産業省）入省。製造産業局航空機武器宇宙産業課長、貿易経済協力局貿易管理部長などを経て、2020年貿易経済協力局長、2022年内閣官房内閣審議官（国家安全保障局）、2024年内閣サイバーセキュリティセンターセンター長代理、2025年から内閣サイバー官（現職）

このほか、2025年に「インターナショナル・サイバーセキュリティ・チャレンジ（ICC）」という国際サイバー競技会を国家サイバー統括室（NCO）と共同開催したり、セキュリティ・キャンプ協議会と共に、セキュリティ・キャンプの全国大会をモデルにした1週間の合宿形式で欧州・アジア約10カ国からのサイバーセキュリティ人材が研鑽を積む「グローバル・サイバーセキュリティ・キャンプ（GCC）」を開催したりしています。

情報処理推進機構（IPA）の産業サイバーセキュリティセンター（ICSCoE）で重要なインフラ企業のセキュリティ担当者を対象とした研修の講師支援をスポットで約10年間務める中で、重要なインフラを支える現場の方々が抱える悩みや、人材育成の難しさを実感しています。

今般の能動的サイバー防御に関する法整備の検討に際しても、有識者会議[注1]に参画し、微力ながら意見を述べてきました。

大きな転換点を迎えるサイバーセキュリティ

飯田　私は、経済産業省で日本の安全保障を支える宇宙・航空・防衛等の産業分野を担当してきたほか、経済安全保障にかかわる法整備や政策展開に携わってきました。

現在は、内閣サイバー官として、サイバー安全保障の分野において、政府が民間の事業活動にどこまで関与すべきかといった点を含め、様々な政策を担当しています。

今、サイバーセキュリティは大きな転換点を迎えています。これまで政府の関与のあり方は、民間主導を基本とし、政府の関与はサイバースペースやITイノベーションの促進に限定されてきました。政府の役割は最小限とし、サイバーセキュリティ基本法をベースに、民間の活動を後押しする環境整備に注力してきたのです。

しかし、皆さまもご認識の通り、この数年で状況は大きく変わりました。民間だけで、サイバー空間を自由で公正、かつ安全な空間として維持できるかといえば、もはやそのような状況ではなくなってきました。そこで、政府はどこまで民間のサイバー空間に関与すべきなのかを改めて議論し、今回のサイバー対処能力強化法及び同整備法[注2]の制定につながりました。

サイバーセキュリティの強化は、政府の立場から見ても、まだ手探りの段階です。制度や法律は整いましたが、それを実際の運用に落とし込み、機能させていくためには、なお多くのプロセスが必要だと感じています。今日の議論では、そうしたプロセスの中で、われわれ政府側がまだ気付いていない視点や課題について、皆さまから教えていただきたいと考えています。

国内外のサイバー事案の教訓

社会全体で脅威に立ち向かう

岩村　続いて、サイバー空間をめぐる脅威の変化や、そこから見えてくる課題について、皆さまのお考えを伺います。まずは政府の立場から、国家安全保障や経済安全保障の観点も含めて、飯田内閣サイバー官からお話しいただけますでしょうか。

飯田　サイバー空間はボーダーレスで、誰もがアクセスできる自由な空間です。国際的なルールや国内ルールは存在するものの、それを悪用する側にとっては非常に都合のいい空間でもあります。サイバー犯罪はもちろん、国家を狙った不法行為が横行しているのが現状です。こうした中で、政府でなければ対応できない領域が存在します。その対応をどのように実行するのかを示そうとしたのが、サイバー対処能力強化法及び同整備法です。

2025年末には、この法律を踏まえて、これまでとは視点を変えるかたちで新たなサイバーセキュリティ戦略をまとめました。個別のサイバー攻撃全てを防ぐことは現実的には非常に困難です。しかし、攻撃者側にとって攻撃を続けるコストが増大し、「割に合わない」と感じさせることはできます。こうした考え方で、サイバー攻撃による被害をできるだけ小さくする、あるいは抑止するために、攻撃者に継続的にコストを負わせていく。これを民間や国際社会とも連携しながら強化していくのが今回の戦略のポイントです。

この戦略は、政府だけ、企業だけ、あるいは日本の外で外国だけが対応しても成立しません。日本全体、つまり一人ひとりが意識しなければ意味がありません。そこで、2月1日から開始したサイバーセキュリティ月間では「サイバーはひとごとじゃない」をテーマに、サイバー攻撃の被害を自分ごととして捉え、行動につなげてもらうための情報発信や、普及啓発を行いました。

社会全体のレジリエンスを高めていくためには、個々人のレベルまで立ち返り、サイバーに関する意識を高め、具体的な行動を取ることが重要です。そして、サイバーセキュリティの技術や人材を社会全体として育成し、適切に処遇し、エコシステムが循環するような戦略を描いています。今後は、この戦略を現場でどう実装していくかについて、最前線の現場の方々と意見交換をし、連携を深めていきたいと考えています。

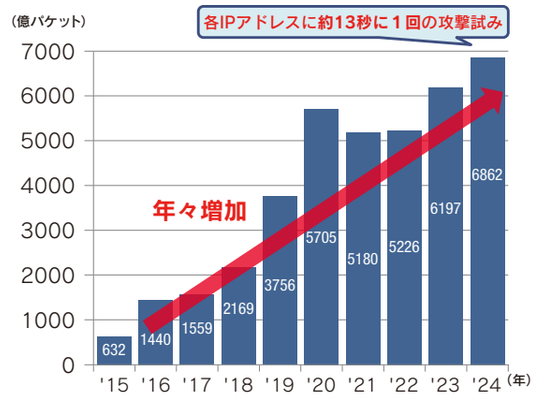
現在、サイバーセキュリティの脅威として強く感じていることの一つは、攻撃の量が圧倒的に増えていることです（図表2）。政府に対しても、不正アクセスは増加の一途をたどっています。今後、AIを使うことで、攻撃のスピードも量も、さらに加速度的に増えていくでしょう。

重要インフラ事業者の場合は、ランサムウエア攻撃やDDoS（分散型サービス妨害）攻撃のほかにも、事前にシステムに侵入・潜伏し、タイミングを見て全体を停止させる高度な攻撃も増えています。こうした攻撃の質的変化や、標的の広がりを見ても、社会全体で取り組む必要があると感じています。

高度化する攻撃、弱点を意識して対応

岩村　続いて、民間の立場から見た課題認識について、まずは経済界・経営者の立場から、

図表2　サイバー攻撃関連通信数の推移



情報通信研究機構（NICT）が観測したサイバー攻撃関連通信数の推移
出所：内閣官房国家サイバー統括室資料より抜粋

（注1）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

（注2）**サイバー対処能力強化法及び同整備法**：重要電子計算機に対する不正な行為による被害の防止に関する法律（令和7年法律第42号）
重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和7年法律第43号）

遠藤信博
経団連副会長、サイバーセキュリティ委員長、知的財産・国際標準戦略委員長
日本電気特別顧問

1981年東京工業大学大学院理工学研究科博士課程修了、工学博士。同年、日本電気入社。モバイルネットワーク担当役員、経営企画担当常務などを経て、2010年代表取締役執行役員社長、2016年代表取締役会長、2022年６月から特別顧問（現職）

遠藤副会長にお伺いします。

遠藤　サイバー攻撃の量が増加している背景として、まずはＡＩを含むコンピューティングパワーの向上が挙げられます。企業は、リモート性やリアルタイム性といったＩＣＴが持つ価値を取り込み、サイバー空間を効果的に活用することで、事業の高度化や効率化を進めてきました。一方で、言い換えれば、企業によるサイバー空間への依存度が年々高まってきたということでもあり、攻撃者側から見れば、価値ある資産が集中しているサイバー空間が必然的に攻撃対象となるわけです。これが、攻撃の量が増えている大きな背景だと考えています。

もう一つ、近年特に意識すべき点は、地政学とサイバーセキュリティの相関関係が非常に強くなっていることです。軍事目的のツールとしてサイバー攻撃が使われる可能性が高まっているといわれていますので、民間企業であっても、地政学を踏まえた対応が求められる時代になっています。

２０２３年には、港湾施設がサイバー攻撃を受け、機能が停止し、復旧に約3日を要した事例がありました。ライフラインや物流施設等が攻撃を受けると、その機能停止により、関連する様々な領域に影響が波及します。攻撃の量が増えているだけでなく、影響の度合いが大きく、かつ広範囲になっている点も、サイバー空間への依存性が高くなっていることの表れでしょう。

さらに、攻撃手法そのものも変化しています。最近では、サイバー攻撃の分業化が進み、それぞれの領域に精通した専門家が役割を分担し、最後に交渉者が現れるような、非常に専門性の高い攻撃へと進化しているといわれています。一方で、昔から変わっていないのは、攻められるのは企業の弱点の部分であるということでもあり、攻撃者側から見れば、価値ある資産が集中しているサイバー空間が必然的に攻撃対象となるわけです。これが、攻撃の量が増えている大きな背景だと考えています。

もう一つ、近年特に意識すべき点は、地政学とサイバーセキュリティの相関関係が非常に強くなっていることです。軍事目的のツールとしてサイバー攻撃が使われる可能性が高まっているといわれていますので、民間企業であっても、地政学を踏まえた対応が求められる時代になっています。

２０２３年には、港湾施設がサイバー攻撃を受け、機能が停止し、復旧に約3日を要した事例がありました。ライフラインや物流施設等が攻撃を受けると、その機能停止により、関連する様々な領域に影響が波及します。攻撃の量が増えているだけでなく、影響の度合いが大きく、かつ広範囲になっている点も、サイバー空間への依存性が高くなっていることの表れでしょう。

さらに、攻撃手法そのものも変化しています。最近では、サイバー攻撃の分業化が進み、それぞれの領域に精通した専門家が役割を分担し、最後に交渉者が現れるような、非常に専門性の高い攻撃へと進化しているといわれています。一方で、昔から変わっていないのは、攻められるのは企業の弱点の部分であるということです。企業の中核のシステムではなく、周辺システムや地方拠点の端末等を足掛かりに侵入するケースも少なくありません。だからこそ、企業側も自らの脆弱性を意識したうえで、これを克服する方法論を考える必要があります。例えば、ＡＩを活用し、どこに、どのような異常があるのかを常にモニタリングするなど、進化する攻撃に対応した取り組みが求められています。

現場での対応を止めないためには権限や指揮統制の明確化が重要

岩村　国連でのご経験やグローバル企業でのサイバーセキュリティ対策を担ってこられた立場から、蓮見部長のお考えをお聞かせ下さい。

蓮見　組織の中で判断が止まる構造は、国や企業を問わず非常によく似ています。これは特定の国や企業に限った話ではなく、複数のインシデントに対応してきた中で共通して感じることです。

現場での経験から二つの課題があります。

一つ目は、企業内の権限設計です。インシデントが起きると、現場には技術的に対応できる人がいますし、次々と情報も集まってきますので、着々と対応を進めることができます。ただしそれをどこまで現場で動かしてよいのか、誰が最終的に決めるのか、権限が曖昧になることがあります。この原因は、平時の延長線上に非常時の判断範囲が設計されていないためで、結果として重要な判断ほど組織の上層部に上がるうち、対応のスピードが失われ、判断そのものが止まってしまいます。

蓮見祥子
スターバックスコーヒージャパン サイバーセキュリティ部部長
元国連CISOグループ共同議長

南クイーンズランド大学にて情報処理学修士・MBAを修了。国際金融機関、OECD、国連機関（UNIDO、ICAO、UN Women、IOM）、国内大手製造業・大手金融機関において25年以上にわたり情報処理、サイバーセキュリティと組織リスク管理に従事。CISOおよび国連CISOグループ共同議長を歴任。2025年からスターバックスコーヒージャパンサイバーセキュリティ部部長。$(ISC)^2$ CISSP、CCSP、ISACA CISA、CRISC、CISM、ICF認定プロフェッショナル・コーチ、メンタルケア専門心理士

二つ目は、インシデント発生時の指揮統制です。多くの組織で見られるのが、誰が指揮を執るのかが明確でないケースです。情報を集め、分析まではできても、その先の次に何をするのか、対応は進んで見えても、意思決定が行われず、そこで止まってしまいます。

現場では、この状況をよく目にします。

この二つの課題に共通しているのは、平時の業務や組織のあり方と、インシデント対応が切り離され、特別なものとして扱われている点です。有事専用のルールを作っても、いざ事が起こると人はすぐには動けません。平時の権限設計や指揮統制、判断の仕方の延長線上に、有事対応をどう位置付けるか。それが一番の課題だと、私は感じています。

篠田　今のお話は非常に興味深く、私も同様の課題をICSCoEで米国企業と実施した演習の中で目にしたことがあります。10年ほど前のことです。化学プラントでサイバー攻撃が原因と見られる物理的インシデントが発生し、ＣＩＳＯである受講生に判断が迫られる場面がありました。その際、ＣＩＳＯが上長に判断を委ね、さらにその上へと判断が回されている間に、被害が拡大していく状況でした。もちろん、発生直後に詳細な原因がわからないのは当然ですが、限られた情報の中でも判断する力、そして普段から有事を想定して体制設計や訓練がなされているかが重要であることを実感しました。あれから10年がたち、状況はかなり改善されているとは思います。ちなみに別の受講者は模範的な対応を示しました。違いについてご本人もおっしゃっていましたが、その方は部下をサイバーセキュリティの国際会議に参加させ、最新の攻撃動向や事例の報告に日頃から触れていたことで、シミュレーションが自然と頭の中でできていたのではないか、とのことでした。

飯田　権限委譲は、判断の起点が複層的になっている場合が難しいと思います。サイバー空間で何かが起きている場合の判断と、フィジカル空間で例えば火事などの物理的な事象が起きている場合の判断、二つのエンドポイントがあると思います。企業でも政府でも、この二つを組み合わせて判断することに、われわれは慣れていません。

例えば、サイバー攻撃が原因で事業が停止している場合、復旧のめどが立たない中で、別の方法で事業を動かす判断をどうするのか。サイバーの復旧作業と事業自体の復旧作業を並行して行うのは、非常に難しい判断だと思います。事業部とサイバーセキュリティの部門の対立も想定して、権限を誰に、どう分配するかが問われていると感じています。

遠藤　まさにその通りだと思います。判断と昧になることがあります。この原因は、平時の延長線上に非常時の判断範囲が設計されていないためで、結果として重要な判断ほど組織の上層部に上がるうち、対応のスピードが失われ、判断そのものが止まってしまいます。

篠田佳奈
BLUE 代表取締役

セキュリティエンジニアとしての実務、暗号・セキュリティ分野の調査研究、新規事業開発支援を経て、情報セキュリティ国際会議Black Hat Japanの企画・運営に従事。2007年から、米国サイバー犯罪対策組織APWGのアジア・リエゾンを務める。セキュリティ・キャンプ協議会国際連携WGにおいて、Global Cybersecurity Camp（GCC）や国家サイバー統括室と共同主催する国際的なサイバーセキュリティ人材育成競技International Cybersecurity Challenge（ICC）などを通じた次世代人材育成を主導。世界トップクラスの国際会議CODE BLUE発起人。千葉工業大学変革センター研究員

ファクターを洗い出し、そのファクターごとに担当者を割り振ってリーダーが答えをまとめます。プロセスが確実に走るための仕組みをチームで訓練することも必要だと思います。

リーダーシップの観点でいえば、米国の海軍兵学校では、科学（S）、技術（T）、工学（E）、数学（M）を学ぶSTEM教育が行われ、卒業時には理学士号（Bachelor of Science）が授与されます。科学技術教育を通じて、課題を見つけ出し、それを解決するためのリーダーシップを発揮できる人材を育てるという強い信念があるのだと思います。戦場では、毎日が新しい事象の連続で、新しい課題に直面します。論理的に考え、課題を見つけ、対応するための要素を洗い出し、それを人に割り当て、最終的に意思決定を行うリーダーの存在が非常に重要になります。このようなコンピテンシーを育てる教育や訓練は、サイバーセキュリティの分野でインシデントに対処することを想定した場合にも通じるものがあるのだと思います。

守りは弱点の克服に尽きる

岩村　篠田代表は、国際コミュニティの視点から、現在の課題をどのように捉えていますか。

篠田　皆さまご指摘の通り、AIの進展やコンピューター性能の向上により、サイバー攻撃の能力は高まっています。加えて、以前は国家を主な対象とするアクターと、金銭目的のランサム等サイバー犯罪アクターは比較的明確に分かれていましたが、近年では両者の活動領域が重なり合う傾向も指摘されています。その結果、攻撃者側の意図を分析すること自体が、以前にも増して難しくなっています。

ではどのように守っていくかといえば、弱点を克服することに尽きると思います。

日本は自然災害が多いことから、平時から物理的な災害対応・復旧に向けた備え、公衆衛生対策などが非常に優れています。言い換えれば、〝守る文化〟が根付いているのです。そこは弱点克服に有利な点と考えます。一方で、サイバー攻撃による災害は原因や影響範囲が見えにくいという点が、物理的災害との大きな違いです。これが非常に厄介な点です。侵入・潜伏された攻撃痕跡などは日頃からログを収集して分析できるような脅威ハンティングができる体制を設計していくことも大切だと考えます。

弱点の克服という観点では教育の役割も大切です。例えば、情報通信研究機構（NICT）が実施している実践的サイバー防御演習は、目の前の情報を基に方向性を定める行為です。結論までの時間を短くするための判断もあれば、着実に次のステップに進めるための判断もあります。個人で決めきれない場合には、複数人で話し合って、課題を解くためのとが重要だと考えています。

能動的サイバー防御に関する評価と期待

攻撃を未然に防ぐための情報収集と分析

岩村　サイバー対処能力強化法及び同整備法に基づく能動的サイバー防御の枠組みについて、皆さまの評価や、今後の運用に向けた期待、留意点等についてお伺いします。

まずは、法制度の実現に尽力された飯田内閣サイバー官から、能動的サイバー防御の狙いや具体的な枠組みについて、ご説明いただけますでしょうか。

飯田　この制度の目的は、サイバー攻撃によって国家安全保障にかかわる重大な被害が生じる前に先手を打って未然に防止すること、また万一攻撃を受けて被害が発生し始めた場合でも、耐えきれない規模にまで拡大しないよう途中で阻止することにあります。そのためには、まず国内外で行われているサイバー攻撃について、誰が、どのような戦術で行っているのかという情報を集めることです。NCOにサイバー攻撃の阻止に必要な情報をいかに多く集められるかに着眼し、制度を設計しています。

今回は三つの柱を立てました（図表3）。一つ目が「官民連携の強化」です。具体的には、攻撃対象になり得る重要なコンピューターの

「CYDER」という教育プログラムがあります。これは総務省が政府機関や自治体向けに整備したもので、遠隔教育から始まり、教材や演習環境まで一体で設計されています。現在では対象を広げつつあります。重要インフラ事業者などにもさらに裾野を広げ、省庁の垣根を越えて連携しながら、日本全体のサイバーセキュリティ体制をより強靭にしていくことが望ましいと考えます。

また、ICSCoEでは、空港、電力、鉄道、自動車など、重要インフラ分野にかかわる方々が垣根を越えて集まり、1年間かけて学びます。その結果、横のつながりが生まれ、10年単位で見ると大きなコミュニティができます。これは非常に良い取り組みであり、こちらについても省庁の枠を超えて、必要とする多くの関係者に教育の門戸が開かれることを期待しています。

米国では、情報共有や教育の面で軍と民間の連携が強く、軍の教育機関が民間と協力し、多くのステークホルダーを巻き込んでインシデントレスポンスを学ぶ、といった取り組みも行われています。私たちが招聘したNPOの中にも、軍での経験を活かし、地域社会のセキュリティ向上に取り組んでいる人たちがいます。このような、守りを強化する取り組みを官民共に連携し、継続し、広げていくこ

図表3　能動的サイバー防御のポイント

出所：内閣官房国家サイバー統括室資料より抜粋

製品名等をあらかじめ届け出していただくこと、そして実際に攻撃を受けた企業や組織から、攻撃に関する情報を提供していただくことを想定しています。特に基幹インフラ事業者は、国民生活を支える極めて重要な存在です。どのようなシステムを保有しているのかを可能な範囲で把握し、実際に攻撃を受けたときに、その内容について情報提供をお願いすることになります。

二つ目が「通信情報の利用」です。サイバー空間上の通信情報を収集・分析することで、攻撃者を検知します。例えば、外国からインターネットを通じて機械的に送信されるサイバー攻撃や、すでに被害が起きている場合、その通信情報をモニタリングします。そして、攻撃者の戦略や戦術を分析し、サイバー攻撃の司令塔となるC2サーバー(注3)がどこにあるのか、それに指示を出している攻撃主体は誰なのかを把握することを、今回の法律では非常に重視しています。

三つ目が「アクセス・無害化措置」です。これまでの国内法制では、政府がこうした措置を実施することは必ずしも認められてきませんでしたが、今回、範囲を広げました。具体的な措置の範囲はケース・バイ・ケースでしょう。「アクセス・無害化措置」という方法だけではなく、民間に対する注意喚起や効果的な防御法の提示を行う場合もあれば、外交的配慮を踏まえつつ、攻撃者を名指しで非難する、いわゆる「パブリック・アトリビューション」を行う場合もあるでしょう。

官民情報共有の一体感をさらに深化

遠藤　能動的サイバー防御は、これまでよりやや踏み込んだ領域を含めた情報の共有化を目指すものであり、非常に有意義な制度だと思っています。情報は共有されてこそ大きな価値を持ちます。日本国内で、情報をリアルタイムに官民で共有する仕組みを構築することは、非常に重要だと思います。

一方で民間の課題としては、サイバー攻撃を正確かつリアルタイムに政府に伝えられるかどうかという点があります。今回、インシデント報告のフォーマットが統一され、報告窓口の一本化も進められています。実務上、非常に有効な取り組みであると考えており、感謝しています。

今後は、この制度が実際に稼働する中で、企業側に生じるメリットを、より明確にフィードバックしていただけることを期待しています。例えば、民間には中々届かない海外で起きている事象も含めた情報共有や、それに対する対応策や注意点についても情報共有がなされれば、民間側から情報提供に協力する意義や、そのメリットの大きさを感じられるようになると思います。

また、今回の取り組みで官民の一体感が醸成されることが期待されますが、さらにその先、この一体感をベースとした具体的な活動につなげられると良いと思います。例えば、先ほどお話に出たJCSCoEには受講者のOB／OG組織があり、どこかで問題が起きたときに、OB／OGが支援できないかといった議論が行われています。このように、産学官が一体となって解析や分析を行うことが当たり前になれば、より高度でスピード感のある課題解決が可能になり、民間の人材にとっても社会に対する自らの役割の一つだと感じられるのではないでしょうか。

サイバー・レジリエンスの向上は、国民一人ひとりが自分ごととして捉え、自らが答えをつくるという認識を持ち、それが広く共有されることで進むものだと思います。そうした環境をつくり上げていくことこそが、能動的サイバー防御の制度の先に期待される姿だと思います。アクティブ・ディフェンスという言葉は、攻撃に対する対応だけでなく、われわれ自身がアクティブになる必要があるという意味も含まれるのだと思います。

CODE BLUEにおける活動（セキュリティ人材の育成・ネットワークづくり）

(注3)C2サーバー：マルウエアに感染した端末を遠隔操作するため、攻撃者が指令を送るサーバー

民も官も遠慮なく熱を持って解決に向かいたい

篠田　ICSCoEを起点にサイバーセキュリティ人材が産業横断で迅速に対応できる仕組みには、皆さまも熱意をお持ちですし、期待しています。

コミュニティの形成という点では、例えば英国では民間でできないことを政府がサポートする、という非常にシンプルな方針を採っています。CODE BLUEのようなカンファレンスを政府が実施しています。民間だけでは弱かった点を補いながら、情報共有し、官民協働で国を守っています。


CODE BLUEにおける活動（国境を越えたセキュリティコミュニティとの交流）

官民連携を機能させるという観点では、米国の取り組みは非常によくできていると常々感じています。政府で働いていた人が民間に移り、NPOを立ち上げて政府では対応できない部分を支援し、また政府に戻るなど、人材が行き来しています。

米国で開催される世界最大級のセキュリティイベントDEF CONには、ホワイトハッカー、政府関係者、軍関係者など数万人が集まります。そこでは、最新のトレンドが共有されるだけでなく、攻撃の犯行主体や手口、目的を特定する、いわゆる「アトリビューション」についても、立場を超えて議論が交わされます。こうした、率直に話せるコミュニティが理想だと思います。

優れたコミュニティの共通点は熱意があることです。その熱量を目指して人は集まり、物事を成し遂げていきます。高度成長期の日本も、〝なんとかせねばならん〟という強い思いが社会を動かしました。サイバーセキュリティの問題も、まさに今がその局面ではないでしょうか。民も官も遠慮することなく、双方が熱意を持って、インタラクティブな対話を重ねて解決に向かうべきだと思います。理想的には、普段から立場を超えて、遠慮なく交流できる関係が築かれ、政府と民間企業と

で行き来できる環境に、日本もなるとよいと思います。

現場が動きやすくなる仕組みが大切

蓮見　篠田さんがおっしゃる通り、サイバーセキュリティの現場には、熱意を持った方が多くいます。能動的サイバー防御が成立したとき、現場では大変喜んでいました。官民一体で備えていくことを重視するのは、現場の思いも同じです。

　実務の立場から見ると、一番のポイントは、情報の量や精度そのものよりも、それが現場でどのように使われるかだと思います。国連やグローバル企業でサイバー対応をして難しさを感じたのは、技術的な対応ではなく、役割や責任のあり方、全体の動かし方です。情報は集まり、専門家も集まる。しかし、誰がどう判断し、どう動くのかが明確でないと、前に進めません。

　私が期待しているのは、制度の細かな運用手続き以上に、官と民がそれぞれどこまでを自分たちの役割として動かすのか、役割分担と意思決定のラインが平時から共有されていくことだと思っています。

　そこが共有されていけば、官民連携は特別なものではなく、日常の延長線上で自然と使われるようになります。そうなったとき、能動的サイバー防御は、現場が動きやすくなる仕組みになっていくのだと思います。

飯田　私も同感です。一方で懸念しているのは、制度ができたことで、企業も政府も制度の範囲内だけ、法定されたこと以外は対応せず、結果として形骸化することです。制度は最低限を定めたものであり、その余白や行間を現場の熱意で膨らませるエコシステムが重要です。

　アクセス・無害化措置は法的に認められましたが、それ以外の様々な取り組みを自由に考えるきっかけにしなければいけません。情報提供についても、確実に提供いただける範囲が定まったというだけであり、お互いに信頼関係を築くことで、さらに多くの情報提供があるかもしれませんし、政府側からも多くの情報をフィードバックできるのではないかと思います。こうした膨らみがなければ、このサイバー対処能力強化法は失敗しかねません。情報は作りましたが、形式的に履行するだけでは能動的サイバー防御とはいえないと思います。ぜひお力添えをいただければと思います。

遠藤　アクティブ・ディフェンスや情報共有が、企業にとっても大きな価値として実感できる仕組みであることが重要です。参加者が一つひとつの活動に価値を見いだせば、必ず次につながります。

　また、官民連携をより長期的な視点で考えると、将来の日本の人口減少に対する対処の問題があります。将来、人口規模が縮小したときに、政府頼みの姿勢で機能を維持し続けられるでしょうか。例えば、世界トップレベルのサイバーセキュリティを持つフィンランドの人口は５６３万人ほどですが、官民が一体となって実現しています。日本も将来を見据え、官民一体、産学官一体で仕組みを動かす訓練を重ねていく必要があると思います。そして、蓮見さんがおっしゃるように、平時から当たり前に機能する仕組みになれば、人口減少の中でも機能を高めたまま維持し続けることができるはずです。この視点で方法論を含め議論していくことが、中長期的に重要になってくるのではないでしょうか。

サイバー・レジリエンス強化に向けて

能動的サイバー防御に定義はなく、取り得るオプションを広げていくことが必要

岩村　最後に、サイバー・レジリエンス強化に向けて、官民が最優先で取り組むべきアクションについて、改めてご意見をいただきます。

蓮見　皆さまのお話を伺い、官と民、立場は違っても目指している方向は同じだと強く感じました。繰り返しになりますが、現場の視点から、改めて三つ共有させていただきます。

　第1に、平時の役割と動き方を曖昧にしないことです。有事になってから何かを決めようとすると、どうしても動きは鈍くなります。平時の延長線上で、どのように動くか、どこまで動くか、誰が動くか、その前提を少しずつでも言語化していけば、サイバー・レジリエンスの強化につながります。

　第2に、官民連携を特別な対応にしないことです。イベント化してしまうと、現場はかえって動きにくくなります。日常の業務や対話の延長として、自然につながっていく関係性をつくること。この積み重ねが、有事における円滑な対応を支える力になります。

　第3に、制度は守るものではなく、使うものだと考えることが重要です。能動的サイバー防御は、枠組みを整えること自体が目的ではなく、現場がいかに動きやすくなるかを実現するためのものです。その視点で、官民が互いに制度と向き合いながら、磨いていく必要があります。私自身も、本日議論したことを現場に持ち帰って、考え続けていきたいと思います。

飯田　能動的サイバー防御には、明確な定義があるわけではありません。取り得るアクションには、無限の可能性があります。政府だけではなく、産学官、さらには国際的な連携も含めて、能動的に対応できるオプションを広げていきたいと考えています。

　アクセス・無害化措置はあくまで上限で、そこに至るまでには様々な対応が考えられます。民間だけで対応する場合もあれば、官民連携、あるいは国際連携で対応する場合もあるでしょう。そうした選択肢をどれだけ多く持てるかが、この国の将来のサイバー・レジリエンスの行方を左右すると考えています。

　そのためには、官民の間で日常的なコミュニケーションを重ねていくことが不可欠です。定例的なものでも不定期であっても、必要なときにはいつでもコミュニケーションを取れる環境をつくることが重要です。それは制度で保証されるのではなく、制度が土台を築き、そのうえでプラスアルファとして、コミュニケーションの機会を増やしていくことが極めて大事だと思います。

　こうした点を踏まえると、まず変わらなければならないのは、官の側です。政府が情報共有や対話に対して臆することなく、民間の経営者から技術者まで幅広く様々な方と意見を交わしていく。そのマインドセットが、最も大事なことだと考えています。

サイバー・レジリエンスの強化には人材育成も欠かせない

遠藤　今のお二人のお話で十分に語られていますが、企業にとっても大きな価値として実感できる仕組みであることが重要です。参加者が

撮影：田山達之

ると思いますが、補足として考えていただきたい点があります。一つ目は、中小企業の存在です。日本の企業の99・7％は中小企業（注4）であり、そこのサイバーセキュリティが十分でなければ、日本全体のレジリエンス力は高まりません。中小企業はサプライチェーンを通じて大企業とも密接につながっています。日本国全体のレジリエンス力を考えた場合、中小企業を意識しながら答えをつくっていく努力が不可欠です。

次に、人材育成です。ＩＰＡにはICSCoEがあり、ＮＩＣＴにもサイバーセキュリティ研究所に人材育成の機能があります。私自身、両方に携わり、現在はＮＩＣＴのアドバイザーも務めていますが、非常に良いプログラムがたくさんあります。これらを一般化し、誰もが活用できるようにしていただきたいと考えています。さらに、先ほど篠田代表からお話があったＣＹＤＥＲのほかにも、SecHack365という25歳以下を対象とした人材育成プログラムでは、非常に優秀な人材が育っています。こうした人材を活用するための仕組み、例えば卒業生が民間企業や政府の中でより活躍しやすくなる仕組みを整えることを考える必要があります。

日本では、サイバーセキュリティ分野のビジネスはまだ少なく、利用されているソフトウエアの多くは海外製です。しかし、日本に開発能力がないわけではありません。人材を活用しながら、国産のサイバーセキュリティビジネスを育てていく仕組みを官民連携で整えることも、国家のレジリエンス強化の観点から重要ではないでしょうか。

アクティブ・ディフェンスをより進める際には、実効性あるセキュリティクリアランスの仕組みが必要になってくると思います。共有可能な情報の幅の広がりに応じて、官民でレジリエンスを強化するための一つの方策になると思います。

篠田　遠藤副会長がおっしゃる通りで、官の側が省庁の垣根を越えることは非常に大事です。SecHack365やＣＹＤＥＲはいずれも総務省の予算で、あくまで総務省の範囲内で完結しています。一方、ICSCoEは経済産業省の所管で、会議の場で国土交通省の港湾関係者を呼びたいと提案すると、戸惑われることもあります。こうした垣根は、ぜひ越えていただきたいところです。10年かけて開発したプログラムを様々なところで展開してほしいと思っています。

また先ほど話題に出た人口減少の問題については、私も懸念しています。これは一企業が背負える問題ではなく、日本国として耐え、乗り越えていかなければなりません。そのためには国際連携も必要でしょう。例えばシンガポールは小さな国なので、国際連携を重視しています。今年は、日本とシンガポールの国交樹立60周年にあたりますし、２０２７年からはシンガポールはＡＳＥＡＮの議長国となります。その一環として、シンガポールの学生を60～80人ほど日本に招き、人材育成の観点で一緒に何かできないかという提案も受けています。日本も、こうした国際連携をもっと考えていく必要があると思います。今後もこの国のために、粛々と取り組んでいきたいと思います。

岩村　本日は、ありがとうございました。

（２０２６年２月４日　経団連会館にて）

（注４）出所：2021年経済センサス・活動調査

Declaration of Cyber Security Management 2.0
経団連サイバーセキュリティ経営宣言 2.0

2022年10月
一般社団法人　日本経済団体連合会

新型コロナウイルス感染症を受けた社会経済活動の変容やデジタルトランスフォーメーション（ＤＸ）の進展に伴い、各産業にとどまらず社会全体でサイバー空間とフィジカル空間の融合が進んでいる。一方、サイバー攻撃を受けた際の被害がフィジカル空間にも波及し、事業活動や国民生活に甚大な影響を及ぼす事例が後を絶たない。取引先や海外子会社等のサプライチェーンを経由したサイバー攻撃も増加傾向にある。また、地政学的緊張の高まりがサイバー空間にも波及する中、サイバーセキュリティは国家安全保障に関わる最重要領域の一つとなっている。

こうした状況下、Society 5.0 for SDGsの実現に向けた価値創造やバリューチェーンの構築、さらにはリスクマネジメントの観点から、実効あるサイバーセキュリティ対策を講じることは、いまやすべての企業にとって、経営のトッププライオリティと言っても過言ではない。

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献すべく、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識

- 経営者自らが最新情勢への理解を深めることを怠らず、DXを進めるうえで必須となるサイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
- 経営者自らがデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題として認識し、リーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

- 特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行う。
- 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

- 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
- 経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
- サイバーセキュリティ対策のガイドライン・フレームワークの活用や、政府によるサイバーセキュリティ対策支援活動との連携等を通じて、取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

- 製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

- 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
- 各種情報を踏まえた対策に関して注意喚起することによって、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に寄与する。