資料２－４

## ○　官民連携の強化

本章では、国家安全保障戦略において能動的サイバー防御の実現のための検討事項とされていた措置のうち、官民連携の強化について述べる。

### ①　サイバー攻撃が発生した場合の対応能力向上のための官民連携の必要性

我が国のサイバーセキュリティ対策は、JPCERT/CC の設立(1996 年)や内閣官房情報セキュリティ対策推進室の設置（2000 年)、サイバーセキュリティ基本法の制定（2014 年）など四半世紀の歴史を有する。その間、**サイバー攻撃の態様は大きく変化し、今なお巧妙化・高度化が続いている**。

当初のサイバー攻撃は、データの大量送信によるウェブサイトの閲覧支障等、公開サーバを対象とするものが主であった。しかし、近年では、**政府や企業の内部システムからの情報窃取、ランサムウェアによるデータの暗号化・身代金要求等が大きな問題となっている**。更に、**有事において重要インフラ等の機能を停止させることを目的とした高度な侵入・潜伏能力を備えたサイバー攻撃に対する懸念が急速に高まっている**。

特に、**重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家を背景とした形でも平素から行われているなど、安全保障上の大きな懸念となっており、官民ともに、サイバーの世界は常に有事であるとの危機意識を持った対応が求められる**。加えて、**社会全体でデジタルトランスフォーメーションが進んだ結果、各組織が自らのサイバーセキュリティを確保しようとすれば、そのサプライチェーン全体のセキュリティを確保することが必要**となっている。このような状況に鑑みれば、官民いずれの組織であれ、**単独でサイバーセキュリティを確保することは極めて困難**である。すなわち、サイバー攻撃から社会全体の強靭性を維持し、もって国民の生命、身体及び財産の安全を確保するためには、**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**であると言える。

ここで、官民が連携を進めるためには、特に**社会全体での情報共有を進めることが最重要**となる。**サイバーセキュリティ基本法においては、民間事業者は自主的かつ積極的にサイバーセキュリティの確保に努めるもの**とされ、また、**国や産業界等は相互に連携してサイバーセキュリティに取り組むこと**とされている。同時に、情報提供や助言が国の役割の一つとされているところ、上記の懸念に対応するためには、重要インフラ事業者等をはじめとする**産業界をサイバー安全保障の「顧客（カスタマー)」としても位置づけることが重要**となる。さらに、脆弱性解消手段の開発前に悪用が先行する「ゼロデイ攻撃」から国民生活を守るためには、システム開発やセキュリティ監視等を担う**ベンダとの連携をより一層深める必要**がある。

これらの問題意識を背景に、具体的な施策のあり方について、以下、「②高度な攻撃に対する支援・情報提供」「③ソフトウェア等の脆弱性対応」「④政府の情報提供・対処を支える制度」に分けて述べる。

### ②　高度な攻撃に対する支援・情報提供

情報共有は社会全体の強靭性を高める上で最重要であり、**被害組織が情報を提供するためのインセンティブの設計を行う**とともに、サイバー攻撃による業務継続性への影響や事業者間の

相互依存関係を考慮し、重要インフラ事業者等は勿論のこと、これに限らず、リスクコミュニケーションや支援が行われるべきである。欧米主要国では、情報提供が政府の役割として明確に位置づけられているところであるが、我が国においても、いわゆる「平時・有事」の区別なく、状況に応じて、政府が率先して情報提供し、官民双方向の情報共有を促進すべきである。

提供される情報については、高度な侵入・潜伏能力を備えた攻撃に対し、事業者等が具体的行動を取れるよう、攻撃者の動向を踏まえつつ、専門的なアナリスト向けの技術情報に加え、経営層が判断を下す際に必要な、攻撃の背景や目的なども共有されるべきである。その際、攻撃者の動向を把握するため、ダークウェブからの情報のほか、ランサムウェア攻撃等で支払われた仮想通貨の移動を分析することも有効である。

また、高度な攻撃はIPアドレスやマルウェアのハッシュ値などの指標（インディケータ）のみでは検知や対策が困難であり、情報の被提供者がシステムの作動状況から侵害の痕跡を探索する「脅威ハンティング」を効率的に行えるよう、攻撃者の手法に関する具体的情報の提供も必要である。

こうした情報の多くは、広く一般に注意喚起されるべき性質のものである一方、政府のインテリジェンス情報や企業秘密に関わるものも存在することから、セキュリティ・クリアランス制度の活用や、情報共有ポリシーの設定により、適切な情報管理と情報共有を両立する仕組みを構築すべきである。具体的な仕組みとしては、現在のサイバーセキュリティ協議会を改組し、新たな情報共有枠組を設けることも考えられる。

加えて、現在、内閣サイバーセキュリティセンターのほか、警察・経済産業省・JPCERT/CC・情報処理推進機構等が個別に情報発信を行っているが、特に緊急性の高い情報発信について機関ごとに差異が生じないよう、ワンボイスで行われるべきである。また、現場レベルで官民の対応者が集結できる仕組みや、国産技術の活用、友好国との間での相互運用性にも配慮すべきである。

さらに、民間事業者間の情報共有も重要であることから、セプターカウンシルの活用など、ISAC間のノウハウ共有を政府が支援することも考えられる。

### ③　ソフトウェア等の脆弱性対応

システムへの不正侵入に悪用し得る脆弱性は、開発段階でいかに注意しても発生するものであり、解消手段の開発前に悪用が先行する「ゼロデイ脆弱性」の悪用が散見されるほか、海外では、攻撃を受けた製品ベンダから利用者に被害が拡散する「サプライチェーン攻撃」の被害も深刻化している。

このため、製品ベンダによる解消手段の開発と、利用者による適用をサイクルとして回し続ける必要があるところ、利用者が自らの利用するソフトウェア等のリスクを適切に理解しないまま使用し続けると、予期せず深刻な被害をもたらし得るものであることから、脆弱性情報の提供やサポート期限の明示など、製品ベンダが、利用者に対し適切にリスクコミュニケーションを行うべき旨を規定すべきである。その際、政府によって、侵害有無の調査方法や緩和策など、ベンダが提供すべき情報を整理することも求められる。

同時に、毎年多くの脆弱性が公表されるなか、利用者が膨大な脆弱性情報の中から優先的に

対応すべきものを特定できるよう、政府は、米国政府が公表している「既知の悪用された脆弱性カタログ」を参考に、国内で悪用されている脆弱性情報を一元的に分かりやすく発信すべきである。

ゼロデイ脆弱性については、利用者自身による発見・対応は困難である一方、パッチの開発・公表までに一定期間を要することから、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（以下「経済安全保障推進法」という。）の特定社会基盤事業者（以下「基幹インフラ事業者」という。）については、インターネットとの接点となるVPN装置など、その保有する特定重要設備に関連する一定の機器について、機種名等の届出を求めた上で、当該機器に関するゼロデイ攻撃を含めた攻撃関連情報の迅速な提供や、製品ベンダに対する必要な対応の要請ができる仕組みを整えるべきである。また、ゼロデイ攻撃を早期に認識するためのハニーポットなどの観測基盤の強化が必要となる。

このほか、海外事例等も参考に、SBOM（Software Bill of Materials）の活用推進、安全性のテスト基準など製品ベンダの規律の設定、脆弱性情報の報告等も求めるべきであるが、IoT機器ベンダを中心に資源が限定的な中小ベンダも多く、厳しい価格競争も踏まえると、単にベンダに責任を負わせるのではなく、セキュアな製品開発・供給、脆弱性対応にあたっての助言や支援も行うべきである。

また、外部からのスキャンによって脆弱性を把握し、注意喚起をすることも効果的と考えられる。なお、精度が低い場合には、注意喚起の対象となった組織の過度な負担になってしまうことに留意すべきである。

**④　政府の情報提供・対処を支える制度**

以上のような情報提供・支援のためには、政府としても、サイバー攻撃に関連する情報の収集や分析を十全に行う必要がある。現在、我が国では、重要インフラ事業者等については、重要インフラのサイバーセキュリティに係る行動計画（以下「重要インフラ行動計画」という。）のもと、個別業法に基づき所管省庁に報告されたインシデントについて、各所管省庁を経由する形で内閣サイバーセキュリティセンターに集約されている。一方で、米国、英国、豪州等では、近年、サイバー対応組織の一元化が行われるとともに、インシデント報告の義務化が進められている。

重要インフラのデジタル依存度が増していることを踏まえ、継続的なサービス提供のため、重要インフラ事業者等の中でも、サイバー攻撃が発生した場合において、国家及び国民の安全を損なう事態が生じるおそれがある基幹インフラ事業者に対して、インシデント報告を義務化し、情報共有を促進すべきである。また、その中でもデジタルインフラと電力は、特に重要なインフラとして、より緊密な情報連携を行うことが考えられる。

基幹インフラ事業者に該当しない重要インフラ事業者等についても、従来どおり、重要インフラ行動計画に基づく情報集約を行うほか、機微技術を保有する者等についても、国内外での情報窃取事案や、サプライチェーンにおける重要性等に鑑みれば、インシデント発生時の報告を条件に②の情報共有枠組への参画を認めるなど、情報を共有する仕組みを設けるべきである。

サイバー攻撃被害拡大の防止の観点からは、政府へのインシデント報告は速やかに行われることが重要であり、事業者に負担をかけずに効率的に情報収集し、フィードバックするという

仕組みが重要である。これまで所管省庁へ行われてきているものの、所管省庁におけるセキュリティ担当者のリソースの不足からリアルタイム性が損なわれる可能性がある。そこで、被害組織の負担軽減と政府の対応迅速化を図るため、インシデント報告先の一元化や報告様式の統一化、速報の簡素化を進めるべきである。また、サイバー攻撃の有効な対処には、数分・数十分というタイムスケールでの迅速な情報収集・共有が必須であり、インシデント報告において自動化技術を活用すべきである。

一方、情報提供を行う民間企業の立場からすると、報告された情報は、経営上機微な情報を含み得る一方、他の企業への提供や公表など、提供された情報がどのように取り扱われるのかの予測が立たなければ、安心して情報提供することが困難となる。このため、情報提供に関する明確な規律が必要であり、報告された情報の利用目的の明確化、機密情報の流出防止策、サイバーセキュリティ以外の目的での利用防止を規定すべきである。