資料１－２

サイバー安全保障分野での
対応能力の向上に向けた提言

令和６年１１月２９日

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

目次

１　はじめに

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は、「国家安全保障戦略」（令和４年 12 月 16 日閣議決定）に基づき、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、当該分野における新たな取組の実現のために必要となる法制度の整備等について検討を行うために立ち上げられ、本年６月初頭から約６か月間にわたり全体会議を４回、テーマ別での会合を９回開催した。

具体的には、まず、第１回全体会議で重点的に検討すべき点、検討に当たって留意すべき点などについて議論を行ったうえで、「官民連携の強化」、「通信情報の利用」及び「アクセス・無害化」のそれぞれについてテーマ別会合を開催し、集中的な議論を行うこととした。

また、第２回全体会議では経済界からのヒアリングを実施し、政府に求める役割や、いかなる制度や枠組みが望ましいかなどについて意見を求めた。

そして、第３回全体会議にて、この間に行われたテーマ別会合の議論の状況について事務局から報告を受けるとともに、上記３テーマ及びそれぞれのテーマについて議論を行う中で明らかになった横断的課題について、「これまでの議論の整理」として示し、その内容を公表した。

以後、この「これまでの議論の整理」を基礎とし、有識者会議としての提言に向けた議論の深化・収れんを行い、最後の全体会議において、とりまとめの議論を行った。

以上の検討の結果について、以下のとおり提言する。

２　実現すべき具体的な方向性

（１）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ほか、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日常的に行われているなど、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、重要インフラ事業者等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、官のみ・民のみでの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、サイバー攻撃による業務継続性への影響を減じ、社会全体の強靭性を高め、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、政府機関、重要インフラ事業者、製品ベンダその他サプライチェーンに関与する全ての者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。

そのためには、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」など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、事業者間の相互依存関係を考慮しつつ、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、適切な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、情報共有を行う場合には、TLPなど情報共有ポリシーを設定することに加え、攻撃の背景や目的に関する情報などのうち、特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティクリアランス制度を活用する等、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（NISC）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、官民だけでなく、民間事業者間の情報共有も重要であるが、業種によってはISACによる情報共有の体制が十分でない場合もあることから、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。

また、こうした情報提供のあり方については、サイバー攻撃の動向や民間事業者等のニーズを踏まえて不断に見直していくべきである。

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等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、製品ベンダや関連サービス提供者による解消手段の開発・提供等と、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、製品ベンダ等が、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法的責務として規定すべき**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、製品ベンダ等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（「経済安全保障推進法」）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、製品ベンダ等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も必要となる。

このほか、海外事例等も参考に、SBOM（Software Bill of Materials）の国際的な相互運用を前提とした活用推進、安全性のテスト基準など製品ベンダ等の規律の設定、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、ベンダに対する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、ユーザに対する適切な設定・運用の慫慂も行うべきである。

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が、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も留意すべきである。

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 NISC 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事業者についても、重要インフラ事業者については、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、**その他の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、報告基準・内容の明確化を進めるべき**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る事を検討していくべきである。

一方、情報提供を行う被害組織等の立場からすると、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、サイバーセキュリティ以外の目的での利用防止を図るべきである。

（２）通信情報の利用

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、国内の通信事業者が役務提供する通信に係る情報（以下この提言において「通信情報」という。）の利用*について述べる。

＊同戦略では通信情報の「活用」と表現されているが、本提言では、個人情報保護法等の規定での表現にも倣い、通信情報の「利用」の語を採用する。

①　攻撃実態の把握のための通信情報利用の制度の必要性

世界全体で政府機関や重要インフラ等を標的にしたサイバー攻撃による脅威が急速に高まりつつあり、日本でも実際に、政府機関がサイバー攻撃を受けるなどで、被害が深刻化している。攻撃者は、攻撃元を隠蔽するため、一般利用者の通信機器をマルウェアに感染させるなどして乗っ取った「ボット」に対し、「C2 サーバ*」から指令を送る手法を用いることが通例であり、これらボットやC2サーバは、多数、多段的に組み合わせて構成されることもある。しかも、これらボットや C2 サーバの多くは、日本の執行管轄権の及ばない国外に所在すると考えられている。

＊C2(Command And Control)サーバとは、クラウド・ホスティングサービス上等で、マルウェアに感染させるなどして乗っ取った通信機器（ボット）を操作し、情報の収集や攻撃等の指令を出すサーバのこと。

このような状況では、通常の情報収集の手段では、どのような攻撃がどこから行われるかを事前に知ることが困難であり、攻撃を受ける側での防御に限界があるとともに、アクセス・無害化等の能動的な防御も難しい。そのため、被害を未然に防止するためには、通信情報を分析することにより、ボットやC2サーバで構成される攻撃用のインフラの実態を把握し、防御を可能とすることが必須であり、特に、アクセス・無害化を行うに当たっては、今まで以上に、サイバー攻撃に関する詳細で十分な量の観測・分析の積み重ねが必要である。

この点、政府が他人間の通信に係る情報を取得する制度として、例えば、犯罪捜査のための通信傍受に関する法律（以下「通信傍受法」という。）による通信傍受があるが、これは、一定の要件の下、裁判官が発する傍受令状により、犯罪関連通信の傍受を行うという犯罪捜査の手段である。犯罪捜査は、犯罪があると思料するとき、その犯人及び犯罪の証拠を発見・収集・保全して、犯罪と犯人を解明することを目的とするものであり、このことを前提に、裁判官は、犯罪の嫌疑、犯罪関連通信が行われる蓋然性等を判断し、傍受すべき通信の手段、内容等を特定して傍受令状を発するものである*。しかしながら、今般実現されるべき**通信情報の利用は、重大なサイバー攻撃による被害を未然に防ぐため、また、被害が生じようとしている場合に即時に対応するため、具体的な攻撃が顕在化する前**、すなわち前提となる犯罪事実がない段階**から行われる必要**がある。したがって、通信情報を取得しようとする時点では、いかなる具体的態様でサイバー攻撃が発生するかを予測することはできず、あらかじめそのサイバー攻撃に関係する通信手段、内容等を特定することは通常は困難であるから、犯罪捜査とは異なる形で通信情報を取得し利用する必要があり、被害の防止と通信の秘密の保護という両方の目的を適切に果たすためには、**これまで我が国では存在しない新たな制度による通信情報の利用が必要**とされると考えられる。

＊これは、「捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。」と規定する憲法第３５条第２項等が定める令状主義の趣旨に沿うものである。なお、外国法制での「令状」あるいは「許可状」は、通信手段、内容等を特定せずに行政府の発行するものを指す場合がある。

これは、我が国にとっては新たな挑戦となる事項であるが、先進主要国では既に、国家安全保障等の観点から通信情報を利用していると考えられ、かつ、通信情報の利用が安全保障目的のインテリジェンス活動の中核となっており、現在は、サイバー攻撃対策としても、用いられていると考えられる。この点、少なくとも米国及び英国については、サイバー攻撃対策としても成果を挙げているとの政府の公表情報があることは、特筆される。また、それ以外にも、少なくともドイツ、フランス及び豪州において、サイバー攻撃対策を含むと考えられる国家安全保障等の目的で通信情報の利用を可能とする制度が存在することが確認できる。

これらの国における**サイバー攻撃対策の通信情報利用の手法としては、個別具体的な対象を事前に特定せずに一定量の通信情報を収集するが、その全てを分析するのではなく、**通信の宛先や送受信者に関する情報及び通信コンピュータ等に一定の動作をするよう指令を与える情報など、**コミュニケーションの本質的な内容ではないデータに注目する方法（②で「☆の方法」として参照する）が一般的にとられている**と考えられ、また、これを可能とするため、一定の条件の下、安全保障上の必要性等がある場合に、政府による通信情報の利用を統制しながら、利用を許容する法律が整備されている状況にある。そして、政府による通信情報の利用には、通信事業者等の協力が必要とされ、これらの国では、通信事業者等に対する法律上の義務付けが行われるとともに、政府からのコスト負担によっても、協力の実施が確保されていると考えられる。加えて、政府においても、通信情報の取得と分析について、一定の技術と能力が必要とされると考えられる。

このような先進主要国の状況を踏まえると、**我が国でも、**重大なサイバー攻撃への対策（以下「重大サイバー攻撃対策」という。）のため、**一定の条件の下での通信情報の利用を検討することが必要**である。また検討に当たっては、安全保障の観点から、海外に依存することなく日本独自の情報収集が必要と考えられることに留意すべきである。他方で国際的な観点からも、先進主要国と連携しながら通信情報を利用する*ことで日本は大きな役割を果たせると考えられるものであり、日本が重大サイバー攻撃対策の能力を高めることは、国際的にも要請されていると言えると考えられる。

＊これは、日本政府が新たな制度により利用する通信情報が無制限に他国と共有されるべきことを意味するものでは全くない。他国との情報の共有は、必要かつ合理的な程度となることが確保されるよう、制度上適切に制限されるべきである。

②　通信情報の利用の範囲及び方式

通信情報の利用による効果と通信の秘密への影響は、利用の範囲及び方式の内容によって、変わり得る。そのため、通信の秘密を保障する憲法との関係での許容性を具体的に検討するには、まず先に、重大サイバー攻撃対策という目的を達成する観点から、通信情報の利用のあるべき範囲や方式について、検討する必要がある。その際、通信情報の分析は、問題を未然に防ぐ予防のための分析であるため、過去になされた行為について真実を解明することを目的とする犯罪捜査とは方法が異なり、「最初は広く、懸念が見つかったら深く」という考え方が妥当である。また、制度全体として重大サイバー攻撃対策の観点で弱点がないものとなるよう検討していくべきである。

具体的にはまず国外の通信か、国内の通信か、という観点では、**攻撃用のインフラを構成するボットや C2 サーバの多くは国外に所在することから、国外が関係する通信について、通信情報を分析する必要が特にある**と考えられる。

そして、多くが国外所在と考えられるそうした攻撃用のインフラの実態把握が必要であることに鑑み、まず、「外外通信（国内を経由して伝送される国外から国外への通信）」については、先進主要国と同等の方法（①の☆の方法）の分析をできるようにしておく必要がある。

加えて、国外に所在する潜在的な攻撃者から国内に対して攻撃がなされるという状況を踏まえ、「外内通信（国外から国内への通信）」及び「内外通信（国内から国外への通信）」についても、被害の未然防止のために必要な分析をできるようにしておくべきと考えられる。

このうち、国外からの攻撃に関係する通信が含まれる「外内」通信だけでなく「内外」通信まで分析する必要性が想定されるのは、例えば、国内でマルウェア等に感染したコンピュータが国外の攻撃元に通信を送信している場合である。

また、外内通信及び内外通信の分析は、我が国への国際的な信頼の失墜につながり得る、国内の領域にボット等が所在し攻撃の一端となるような事例の発生の未然防止や、国際社会における国内の領域で行われている行為の説明責任を果たすことにもつながるものである。

分析の対象とする必要がある情報の範囲について、通信情報は、ⅰ）電気通信設備等を識別する情報、ⅱ）コンピュータ等に一定の動作をするよう指令を与える情報、ⅲ）その他機械的な情報、ⅳ）個人のコミュニケーションの本質的内容に関わる情報、に主に分類できるが、このうちⅳ）は重大サイバー攻撃対策のためには特に分析する必要があるとまでは言えない。すなわち、メールの中身を逐一全て見るようなことは、重大サイバー攻撃対策としては適当とは言えない行為である。加えて、収集したデータ全てについて人間の目で判断することは不可能であり、またプライバシー保護等の観点から適切でもない。重大サイバー攻撃対策に必要な情報を取り出すため、機械的にデータを選別するとともに、検索条件等で絞っていくなどの工夫が必要である。

なお、ⅰ）からⅲ）に当たる、特に分析する必要があると考えられる情報（コミュニケーションの本質的な内容ではない通信情報）は、いわゆる「メタデータ」に限られるものではないと考えられる。

③　通信の秘密との関係

通信情報の利用の範囲と方式に関する以上の結論を踏まえつつ、憲法第２１条第２項後段の通信の秘密との関係を以下検討する。

コミュニケーションの本質的内容に関わる情報は、特に分析する必要がないが、一方で、分析対象となるそれ以外の通信情報（コミュニケーションの本質的な内容ではない通信情報）も、憲法上の通信の秘密として適切に保護されなければならないものである。しかしながら、通信の秘密であっても、法律により公共の福祉のために必要かつ合理的な制限を受けることが認められているところ、通信情報の利用は、国民の安全かつ平穏な生活という基本的な価値を守るために必要であるという考え方の下、先進主要国*を参考にしながら、具体的な制度設計の各場面において、通信の秘密との関係を考慮しつつ丁寧な検討を行うべきである。抽象的な議論のみで「許容される」あるいは「許容されない」との結論を得ることは適切ではない。

＊例えば英国及びドイツでは、通信情報の利用と通信の秘密又は人権との関係について、関連の判決等により、整理が図られている。

以上を踏まえて検討するに、通信情報の利用については、現代的なプライバシーの保護や独

立機関等の議論を組み合わせるとともに、通信の秘密の保障と公共の福祉の両方が整合し、かつ、実効性のある防御を実現できるという緻密な法制度を、分かりやすい議論を積み上げて、作り上げていくことが必要であると考えられる。また、その際は、実体的な規律とそれを遵守するための組織・手続的な仕組み作りが必要であり、加えて、明確で詳細なルールとなるよう考慮することが適当である。その上で、サイバー空間における攻撃手法の変化等の状況に応じ新たなルールが必要となる、法制の整理の見直しが必要となるといった場合が発生し得ることにも配意が必要である。

さらに、先進主要国の制度を俯瞰し、通信情報の取得及び情報処理のプロセス全体で、どこにどのような統制や規律が必要となり得るか、という視点で整理した場合、取得及び情報処理のプロセスとしては、先進主要国の法律では、おおむね共通する実施過程として、準備・承認、通信事業者への措置、処理・分析、提供・共有等、保存・廃棄を認めることができると考えられ、また、独立機関による監督があることも共通している。このため、こうした仕組みを参考としながら、重大サイバー攻撃対策という我が国における今般の政策目標を踏まえつつ、日本の社会やこれまでの法制度と連続的で整合的な仕組みを導入していくことを考える必要がある。中でも、独立機関は重要であり、各国の司法制度等との関係や日本の他法での類例を考慮しながら、具体的な組織の在り方が検討されるべきである。とりわけ、独立機関による監督の制度設計は、②の内容を踏まえて、精緻なものとする必要があると考えられる。

④　同意がある場合の通信情報の利用

なお、③で述べた議論は通信当事者（通信の利用者）の同意がない場合の通信情報の利用を前提としたものである。通信の秘密の制限に対する通信当事者の有効な同意がある場合の通信情報の利用は、同意がない場合とは異なる内容の制度により実施することも可能であると考えられる。攻撃の対象となり得る重要インフラ等を通信当事者とする通信情報を利用することは有用と考えられるところ、その同意の在り方は更に検討がされる必要があるが、制度により規格化された内容による同意を必要に応じ制度により促していくことが方法として考えられ、その観点から重要インフラ等の中でも重要な社会的基盤を有すると考えられる事業者（例：基幹インフラ）については、協議に応じる義務を課すことも視野に入れるべきである。またその際、規格化の一部として、通信当事者の同意のある利用であっても、独立機関の監督等のガバナンスの仕組みが用意されることが検討されるべきである。

⑤　電気通信事業者の協力

先進主要国と同等の方法による通信情報の利用を実現していくに当たっては、その運営する設備から通信情報を送出し政府に提供することとなる電気通信事業者の協力が必須である。

電気通信事業者の協力は通信情報の利用という通信の秘密に対する制限を伴う措置への協力となるが、これは政府の責任の下で行う公益のためのものであり、協力を行う電気通信事業者は、社会の安全に貢献しているとして、肯定的に評価されるべきである。社会的な非難に曝されるようなことがあってはならない。

また、通信情報の利用による重大サイバー攻撃対策という社会的に重要な施策が持続可能なものとなるよう、電気通信事業者が直面し得る訴訟等のリスク及び通信ネットワーク運営に対

する負担について、先進主要国の例も参考にしながら、回避策を十分に検討していくべきである。加えて、通信ユーザの利便性低下やコスト負担が生じるようなことも避けられるべきである。

電気通信事業者の設備から通信当事者の同意なく通信情報が政府に送出されるという、通信の秘密の制約となり得る協力の是非は、既存法令の解釈運用に委ねるのではなく、法整備により、法律の規定に基づき政府の責任で判断すべきものとすることが必要である。これをより広い視野でみれば、政府と民間の適正な連携が重要ということができるものであり、その点でも、電気通信事業者の設備から政府への通信情報の送出の適正性が確保され、同時に協力する電気通信事業者の直面し得るリスクの軽減につながり得るような監督の在り方を含め、独立機関などのガバナンスの仕組みを十分に考えていくべきである。

⑥　国民の理解を得るための方策とその他の検討課題等

以上において通信情報の利用の必要性と許容性について論じたが、通信情報の利用の実現に当たっては、こうした議論のほかにも、国民の理解を得ていく観点が重要であり、そのため、制度の在り方や制度の運用に関する透明性を確保していく視点が重要である。通信の秘密を守るという側面もある国家の活動であるがゆえに、「手の内」を全てさらしてしまえばその活動目的の達成を損ねてしまうことから、運用の詳細などまで全てを公開することは性質上難しく、非公開とすべき範囲が一定程度存在すると考えられる。他方で、不必要な権力の濫用が行われる可能性を排除するためにも、その活動の透明性を高めていくことも同時に行う必要があり、これらの両立を果たしていくために、例えば定期的な報告書の公表などの方法で、大枠の適切な情報公開は行われるべきである*。その上で、情報の公開が難しい部分を独立機関の監督で補う必要があると考えられ、その意味でも、独立機関の構成や業務の在り方が重要である。

＊適切な情報公開の前提として、公文書等の管理に関する法律等にのっとった適切な行政文書の作成及び保存等が実施されるべきことは当然である。

加えて、通信情報の利用の必要性について、固定電話からサイバースペースへの通信の形態の変化や各国の制度の導入の経緯を説明するとともに、急速に高まりつつあるサイバー攻撃による脅威から平穏な通信を守るために通信情報を利用するのであり、これによりサイバーセキュリティが強化され、ひいては通信の自由及び通信の秘密の保護の強化が図られるという側面があることも説明していくことで、理解を得ていくことも重要ではないかと考えられる。また、重大サイバー攻撃対策としての通信情報の利用では、コミュニケーションの本質的内容に関わる情報までは分析しないと考えられることもあり、得られた情報は積極的に活用していくことが適切と考えられるところ、分析した情報を活用するなどして、企業・国民にとって便益がある仕組みとすることも重要である。かかる活用において、政府が取得した通信情報が重大サイバー攻撃対策以外の不当な目的で利用されないことが前提となることは論をまたない。

最後に、以上のほか、今後のあり得る検討課題等について述べる。まず、政府における司令塔となる部門と実施を担当する部門など、独立機関以外の関係組織の役割についても明確化を図り、必要な制度的手当てを行うべきである。また、分析の実務面については、構造化されていないデータの分析を含め、データを分析する技術・能力と設備が必要と考えられるところ、民間企業と協力することも考えられる。さらに、取得した通信情報の分析の際に、インテリジェンス情報も含め政府部内各組織の収集した多様な情報と併せて分析していくことも必要では

ないかと考えられる。また、諸外国の事例を引き続き踏まえていくことが必要であり、場合によっては、継続的に検討していくことも必要ではないかと考えられる。

（3）アクセス・無害化

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、重大なサイバー攻撃について未然に対処するための攻撃者サーバ等へのアクセス・無害化についての権限付与*について述べる。

＊同戦略では「侵入」・無害化と表現されているが、本提言では、ネットワークにおける活動であることをより客観的に示す表現として、「アクセス」の語を採用する。

＊同戦略において、能動的サイバー防御は、武力攻撃には至らないものの、国、重要インフラ等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のおそれがある場合に、これを未然に排除し、また、発生した場合の被害拡大を防止するために導入するものとされているところ、この項の「アクセス・無害化」についても、武力攻撃事態に至らない状況下における対処を念頭に置いている。

①　サイバー空間の特徴を踏まえた実効的な制度構築の必要性

近年、サイバー攻撃は巧妙化・高度化している。具体的には、サイバー攻撃は、複雑化するネットワークにおいて、国内外のサーバ等を多数・多段的に組み合わせ、サーバ等の相互関係・攻撃元を隠匿しつつ敢行されている。また、ゼロデイ脆弱性の活用等により、高度な侵入が行われるほか、侵入後も高度な潜伏能力により検知を回避するなど、高度化している。このため、サイバー攻撃の特徴としては、現実空間における危険とは質的に異なり、**実際にある危険が潜在化し認知しにくい**ということが挙げられる。また、潜伏の高度化等により、**攻撃者の意図次第でいつでもサイバー攻撃が実行可能**であるとともに、ネットワーク化の進展により、**一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれ**がある。

もとより、これまで、政府等においては、サイバー攻撃に対して防御側での対処のほか、攻撃側への対処として、サーバ等の管理者と連携した任意のテイクダウン、パブリックアトリビューション、攻撃手口の公表等を積極的に行ってきたところであるが、上記のような状況のほか、外国においてもアクセス・無害化の取組が行われていることなどを踏まえれば、これまでの取組に加え、**武力攻撃事態に至らない状況下において、重大なサイバー攻撃による被害の未然防止・拡大防止を目的とした、攻撃者サーバ等へのアクセス・無害化を行う権限を政府に付与することは必要不可欠であり、我々が価値創造するための安全なサイバー空間を守る観点から極めて重要な取組**と考えられる。

新たな権限を制度化するに当たっては、**既存の法執行システムとの接合性や連続性を意識**しつつも、**サイバー空間の特徴を踏まえた実効的な制度とする必要**がある。**新たな制度の目的が、被害の未然防止・拡大防止であることを踏まえると、インシデントが起こってから令状を取得し、捜査を行う刑事手続では十全な対処ができないと考えられ、新たな権限執行には、緊急性を意識し、事象や状況の変化に臨機応変に対処可能な制度とする必要がある。**法形式としては、具体的な権限執行法（作用法）として構想されるべきものと考えるが、個別の要件を法定し、あらかじめ具体的な手法を法律上にメニューとして用意するという形の法制度ではなく、目前に存在する危険に対して、**状況に応じた危害防止のための措置を即時的に実施することを可能とする法制度とすべきである。**他方、こうした**措置は、比例原則を遵守し、必要な範囲で実施されるものとする必要がある**。

この点、従前から、災害時の避難措置や危険物による切迫した事態への対処など、必要に応じて関係機関が相互に連携することを含め、危害防止のために臨機応変かつ組織的に対処する際に機能してきた警察官職務執行法を参考としつつ、その適正な実施を確保するための検討を行うべきである。また、サイバー空間の特性を踏まえた必要な調整が図られるべきであるとともに、法制度のみならず執行に係る全体のプロセスやシステムも参考とすべきと考えられる。

また、平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるなどのサイバー攻撃の特性から、制度全体としては、事態を細かく区切り事態を認定するという従来の事態認定方式ではなく、武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度の構築が必要と考えられる。

② 措置の実施主体

サイバー空間の脅威は深刻であり、これへの対処は喫緊の課題である。先に述べたように、これまでに様々な主体が様々な取組を実施してきたところではあるものの、新たな取組であるアクセス・無害化の措置の性格や、新たな執行制度を既存の法執行システムとの接合性や連続性をもつものとして構成すべきとの考え方を踏まえ、権限の執行主体は、現に組織統制、教育制度等を備え、サイバー脅威への対処に関する権限執行や武力攻撃事態等への備えを行っている、警察や防衛省・自衛隊とし、その保有する能力・機能を十全に活用すべきである。これらの組織が執行権限の主体となることについては、諸外国において、同種のアクセス・無害化を担っている主体がインテリジェンス機関、軍、法執行機関であることを考慮すれば、国際的なスタンダードにも合致するものである。

その上で、今般の措置は武力攻撃事態に至らない状況下における対処となることから、まずは警察が、公共の秩序維持の観点から特に必要がある場合には自衛隊もこれに加わり、共同で実効的に措置を実施できるような制度とすべきものと考えられる。

③ 措置の対象

サイバー脅威の深刻性と対処の困難性は、質的な要因と量的な要因の両方に起因するものである。②の措置の実施主体の能力や機能の向上を強力に進めて行くことは極めて重要であるが、その上でもなお能力やリソースが限られることを勘案すべきであり、措置を講じる事案の優先順位を考える必要がある。具体的には、アクセス・無害化の対象としては、社会全体の機能維持（レジリエンス）と安全保障能力の基盤確保という安全保障上の必要性を念頭に、国の安全や国民の生命・身体・財産に深く関わる国、重要インフラのほか、事態発生時等に自衛隊や在日米軍の活動が依存するインフラ等に対するサイバー攻撃を重点とすべきものと考えられる。

他方、昨今のサイバー空間やデジタル技術の急速な発展等を踏まえると、措置の対象を上記に限定することは必ずしも適当でなく、必要性が認められる場合には、適切にアクセス・無害化が実施できるような仕組みとなるよう、留意すべきである。

④ アクセス・無害化と国際法との関係

サイバー脅威は国境を越えて発現する。攻撃主体や攻撃に用いられるサーバなどの機器が海

外に所在し、国境を越えて我が国に重大なサイバー脅威をもたらす場合においては、アクセス・無害化は国境を越えて実施され得るものであるところ、アクセス・無害化と国際法との関係を整理する必要がある。

この点、アクセス・無害化の対象サーバ等が海外に所在した場合において、同措置が当該国に対する主権侵害に当たるか否かは、個別の措置についてどういう影響が生じるかを踏まえた上で、措置の目的、あるいは相手方の対象の性質を加味して個別具体的に判断される必要があり、どのような行為が他国の主権侵害に当たるかをあらかじめ確定しておくことは困難である。

このため、アクセス・無害化の国際法上の評価について一概に述べることは困難であるが、当該措置がそもそも国際法上禁止されてない合法的な行為に当たる場合も考えられるほか、他国の主権侵害に当たり得るものである場合であっても、国際法上の違法性が阻却される場合がある。

その違法性阻却事由としては、「対抗措置（Countermeasures）」や「緊急状態（Necessity）」（※）が考えられるが、「対抗措置（Countermeasures）」については、相手国の先行する違法行為の存在や被害の程度との均衡性を証明しなければならないなどの点を踏まえると、実務上、援用する違法性阻却事由としては、「緊急状態（Necessity）」の方が援用しやすいものと考えられるが、こうした国際法上許容される範囲内でアクセス・無害化が行われるような仕組みについて検討すべきである。

※　対抗措置（Countermeasures）
　国際違法行為により被害を受けた国が、その限りにおいて、当該行為の責任を負う相手国に対して、その行為を中止させ、自国が受けた被害の回復を図る際に、被った被害と均衡する措置を一定の条件の下で措置をとる場合に違法性阻却が認められるという考え方

※　緊急状態（Necessity）
　当該措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、当該行為が相手国又は国際共同体の不可欠の利益を深刻に侵害せず、状態の発生に寄与していない場合に違法性阻却が認められるという考え方

国連憲章全体を含む既存の国際法はサイバー行動にも適用されるという、国連総会で承認され、我が国としても確認している基本的な立場を前提に、国際法のサイバー行動への具体的な適用に関して形成されつつある一定程度の共通認識を踏まえながら、海外に所在する攻撃者サーバ等へのアクセス・無害化を講じることとすべきである。その一方で、アクセス・無害化に関する国際法は未だ発展途上であることを踏まえれば、今後、我が国が目指すアクセス・無害化の制度導入とその執行は、我が国の国家実行として国際法規則の形成に影響を与える事項であることから、サイバー空間での活動の特徴を踏まえ、慎重な法制度の発展が図られるべきであるとともに、サイバー行動に係る国際法の議論に我が国として積極的に参画・貢献していくべきものと考える。

⑤　制度構築に当たっての留意点

アクセス・無害化の制度については、サイバー空間の特徴を踏まえた実効的なものとする必要があるが、そのほか、制度構築に当たって留意すべき点は以下のとおりである。

まず、アクセス・無害化は、上述のサイバー攻撃の特性を踏まえ、実効性確保の観点から、専門的能力を有する者により、具体的な状況に応じ臨機応変な判断で適切な手法が選択され実施されるべきものと考える。政治によるマイクロマネジメントと権限行使の主体への白紙委任

の双方を避ける観点から、政府としての適切な方針の下で、専門的能力を有する者らによりオペレーションを回せるようにする必要がある。

加えて、こうした政府の**アクセス・無害化の取組には、国民の理解を得ることが重要**である。アクセス・無害化の実施に当たっては、措置対象への影響の考慮、公正性・透明性の確保、プライバシー保護との両立が不可欠であるところ、**アクセス・無害化の適正性を確保するための枠組みを検討する必要**がある。この点については、既存の法執行システムとの整合性も考慮しつつ、措置の迅速性とその公正性・適正性の両立の観点から、例えば、措置の実施について幹部職員が関与することや独立した立場から専門的知見も取り入れた事後的な監督を受けることなども考えられる。

さらに、仮に、結果的に関係のないサーバ等を無害化の対象にしてしまった場合、不正プログラムを消去したことによってそのサーバ等自体が使用できなくなってしまった場合など、意図せず、措置を行うことで達成しようとしていたものとは異なる結果に至った場合の対応についても十分検討しておく必要がある。

⑥　運用面の留意点を含めた今後の検討課題

サイバー安全保障分野での対応能力を向上させるという目標の実現に向けては、アクセス・無害化に係る制度の構築に加え、アクセス・無害化を効果的かつ実効的なものとしていくため、その運用においても以下の点に留意すべきである。

まず、アクセス・無害化の実施に当たっては、**恒常的な情報収集やサイバー空間に限らないオールソースデータの蓄積・活用を含む総合的な情報収集が必要**であり、その際には、**官民協力・国際協力も重要**となる。こうした情報収集においては、公開情報の収集に加え、**警察や防衛省・自衛隊、その他の関係機関等による多様な能力を活用することを前提とし、サイバー空間に限らず、必要なインテリジェンスを収集・分析し、関係機関間で相互に共有しながら活用していくことが重要**である。

また、アクセス・無害化を優先的に実施すべき事象か否かを判断するに当たっては、攻撃グループにも、国家を背景とする高度な攻撃を行うグループからそうでないものまで存在することから、アクセス・無害化の権限がより効果的に運用されるには、攻撃グループの属性を把握することが必要である。

加えて、攻撃側のインフラは多重的なものであり、インフラが第三国に存在する場合もあるほか、正規のサービスの悪用やずさんな管理のサービスのように中間地帯があるところ、関係国を含む多様な主体との連携も重要となる。

このほか、アクセス・無害化については、臨機応変な対応を可能としつつも、政府としての適切な方針の下で行われる必要がある。特に強度の高い措置の実施を選択するに際しては、政治、外交等の他の枠組みの可能性を追求するなど、**政府全体としての総合的な判断が求められるとともに、その判断の下で実施主体が措置を講ずることが必要となる場合もあることから、政府においてリーダーシップを発揮するための司令塔の存在が極めて重要**となる。

このように情報収集からアクセス・無害化に至るまでには、司令塔や措置の実施機関を始め、関係機関が相互に連携する必要があると同時に、迅速かつ臨機応変な対応を必要とするアクセ

ス・無害化の実効性を確保するため、関係機関が有機的かつ円滑に連携することが可能な組織体制の整備を図っていく必要がある。

さらに、今後の検討課題として、アクセス・無害化を実施していくに当たっては、多岐にわたる高度な専門性を有する人材の育成・確保に取り組んでいく必要がある。

司令塔となる組織に関していえば、地政学の分析や通信ネットワークの分析の専門家、ネットワークの中を通る情報のアナリスト、無害化に関する技術的理解を有する人材等、**多様な機能・人材が集まり、総合力を発揮することにより、状況の把握と予測を行うことができ、無害化を含むサイバー脅威への対処の戦略ができあがることに留意し、司令塔たる組織にはそのために必要な人材・能力を構築すべき**である。

また、アクセス・無害化の実行組織に関していえば、**個別のアクセス・無害化のオペレーションは、専門的能力を有する者らにより回していくことが必要**となるが、効果的なアクセス・無害化を行うためには、**極めて高度な専門性を有する人材の育成が必要不可欠**である。

こうした人材の育成・確保に当たっては、司令塔組織・実行組織双方の立場を経験し、マクロ・ミクロ双方の視点を有する人材を育成していくことがそれぞれの組織にとって有用であることも踏まえつつ、また、**官民交流の中で人材を教育していくことも含め、全体としてどのように人材を育成していくのか検討を進めていく**ことが求められる。

（4）横断的課題

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各措置に加えて、普段から対応することが求められる横断的な課題について述べる。

①　サイバーセキュリティ戦略本部・NISC・関係省庁が連携した施策の推進

深刻化するサイバー攻撃の脅威に対処するには、事案発生時に加えて、普段から対策を強化して備えることが重要であり、これまでサイバーセキュリティ基本法に基づき、サイバーセキュリティ戦略本部（以下「戦略本部」という。）が設置され、NISC を事務局として、政府機関等や重要インフラを中心に、総合的かつ効果的な対策の推進が図られてきたところである。そこで、能動的サイバー防御の実現と併せて、各組織における普段からの対策を抜本的に強化するため、戦略本部の在り方等を含め、見直しを行うことが求められる。

まず、戦略本部が一般的な政策立案や助言に加え、事案発生に備えた普段からの対策について、政府としてより責任を持って意思決定を行っていくには、その構成の在り方から検討すべきである。具体的には、大臣と有識者を戦略本部の構成員としている現在の構成を改め、**基本的な方針や枠組みを大臣による戦略本部で決定し、それに対して普段から助言をする民の有識者からなる組織が別途存在するという形が考えられる**。また、諸外国の取組も参考に、官が主導しつつも、民とあるべき姿をディスカッションする場を平常的に設けることが、サイバーセキュリティ対策の価値を高め、改善に資することになる。

また、NISC については、サイバー安全保障分野の政策を一元的に総合調整する**政府の司令塔として発展的に改組するに当たり、インテリジェンス能力を高め、技術・法律・外交等の多様な分野の専門家を官民から結集し、強力な情報収集・分析、対処調整の機能を有する組織とす**

る必要がある。その際、NISC や関係する政府機関のほか、重要インフラに位置づけられている地方公共団体等を含め、それぞれの役割と責任範囲を明確に整理することが求められる。さらに、官と官の連携強化の観点からは、関係省庁のサイバーセキュリティ部局が物理的に同じ場所で協働できるよう、基盤となるしっかりとしたインフラ（建物、スペース、勤務環境、セキュリティ等）の確保を図るべきと考えられる。

②　重要インフラ事業者等の対策強化

重要インフラ事業者等においては、国民視点でサービス提供を継続できることが肝要であり、重大なサイバー攻撃に対処するためには、日常の運用をはじめとする攻撃が発生する前の段階から防護を強固にし、実際の攻撃発生時におけるインフラの補完・代替・復旧等の計画をはじめとしたレジリエンスの強化に取り組む必要がある。

この点、まず、**国民視点でサービス継続が求められる重要インフラ分野の防護範囲を定義するにあたっては、重要性の優先順位とともに、新しい分類やデジタル空間の構造*を踏まえた検討が不可欠**である。また、政府として、普段から重要インフラの国民生活や社会経済に対する影響度や相互依存関係を適切に把握しておき、重大なサイバー攻撃の発生時にどのように連携するか、優先度のガイドラインを作って対応できるよう備える必要がある。

＊例えば、国民生活や経済活動における衛星測位関連システム（GPS や準天頂衛星システム（QZSS））の役割は増大しているほか、事業者等の DX により、クラウドサービス等、デジタルアーキテクチャがあらゆる環境の基盤になっている。

また、重要インフラのレジリエンスの強化のためには、**普段から求められるサイバーセキュリティ対策の質の保証の観点から、基準、ガイドラインという手法により、行政が達すべきと考える水準を分かりやすく示し、制度的に誘導していくことが必要**である。この点、近年、欧米主要国では、特に重要な事項として事業者等が実施すべき対策につき、政府が優先順位をつけてベースラインを明示する取組が行われていることも参考になる。基準等については、**重要インフラの日々のシステム運用に携わる技術者等の関係者の声を聞き、第三者の視点からも適切なものとなるよう常に見直しを図る**とともに、遵守の実効性を確保するため、認証、資格の活用や遵守状況の公表など、実効性を高める仕組みを設けることが考えられる。併せて、**重要インフラ分野の中で優れた取組があれば、監督権限やリソースの差も考慮しつつ、他の分野に展開することも有効**である。

さらに、重要インフラ事業者等のサプライチェーンを構成する中小企業のレジリエンス強化のためには、政府が基準等を策定するのみならず、その実行に必要なリソース支援、政府調達要件への採用等の方法論を用意し、それらを中小企業が活用できるようにすることも求められる。

なお、重要インフラ分野の防護範囲の決定や基準等の策定は、戦略本部でなされているところ、我が国や諸外国で重要インフラとなっている分野を所管する大臣全てが構成員となっていない点について見直しを図ることも考えられる。

③　政府機関等の対策強化

政府機関においては、重大なサイバー攻撃事案の発生時においても、その機能を維持することが不可欠となる。国家安全保障戦略では「世界最先端の概念・技術等を常に積極的に活用す

る」ことが掲げられているが、政府機関等の情報システム内で行われる不正活動を監視・制御する技術の導入を進め、今まで以上にサイバー攻撃に関する膨大かつ詳細な状況の観測・分析の積み重ねを行っていくことが必要となる。

また、政府機関が自らのサイバーセキュリティ水準を強固にすることが必要であり、例えば、政府機関等の脅威対策やシステムの脆弱性等を随時是正するため、府省横断的なリスク評価結果や注意喚起についての対応が個々の政府機関に委ねられている点を改め、対応の実効性を確保する仕組みを制度として設けることが重要である。

これら政府機関等の対策の強化にあたっては、日本発のサイバーセキュリティ関係のソフトウェアや中核的なセキュリティ技術がほとんどなく、公に使われているものもないという我が国の状況を踏まえると、国家安全保障の観点からも政府主導で高品質な国産セキュリティ製品、サービス供給の強化を支援すべきと考えられる。その際、大学等で開発された技術等の社会実装と、知見のフィードバックによる更なる技術開発の促進というエコシステムの構築を図ることも重要となる。また、欧米主要国では、政府が公共機関や国民向けに、セキュリティ対策を強化するための多様な支援サービスを提供している例もあり、現行法制度下でも実施可能な施策は積極的に取り入れることが望ましいと考えられる。

④　サイバーセキュリティ人材の育成・確保

重要インフラ事業者等や政府機関等における事案発生時の対応や普段からの対策強化に当たっては、サイバーセキュリティ人材の育成・活用の促進が不可欠である。国家のサイバーセキュリティの力とは、その国におけるサイバーセキュリティ人材の層の厚さであるとも考えられ、人材の重要性が叫ばれて久しいが、セキュリティ分野に実際に人材が流入するような状況にはなっていない。これまでにも幅広い取組がなされてきたところであるが、依然として大幅な不足が指摘されるサイバーセキュリティ人材の育成を官民で効果的に行っていくためには、まずは、政府が官民の人材育成の取組をしっかり把握した上で、産学官の共通認識を醸成するため、政府主導で技術者に限らず、経営等に関わる者も含めたサイバーセキュリティに関わる人材の定義（役割、知識、技術等）付けや資格の活用による可視化等を行うとともに、必要な人数・規模を含めた政府の人材育成に対する姿勢をメッセージとして示すべきである。

具体的な育成・確保のための方策としては、雇用する側の視点として、長期的なキャリアパスの明示、待遇の改善、経営層の理解の促進、人材の重要性の周知、企業等の組織への当該分野人材採用のための支援等が必要となる。その際、非技術者の巻き込みも重要となるため、専門用語だけでなく、分かりやすい比喩や統計データの活用などにより、サイバーセキュリティ対策の重要性について、経営層を含めた非技術者にも広くわかりやすく説明することが求められる。一方、制度面や給与面だけでなく、サイバーセキュリティを担う人材のインセンティブも重要であり、現場でサイバーセキュリティの実務に携わる人の生の声を聞き、それらを集約して政策に活かすことも重要である。これらの観点から、CISO を重要視することは、組織のセキュリティ強化とともに、魅力的なキャリアパスを提示することにつながる。このほか、若年層から教育を行うことも重要である。

また、サイバー攻撃に関する情報や危機感の共有によるトラストの醸成等を目的として、NISC 等の政府機関との官民人材交流を強化すべきであり、政府においては、上記の各種方策を

自ら実践することはもとより、任期の長期化等を含め、関係省庁のサイバーセキュリティ部局の人材の在り方についても検討すべきと考えられる。さらに、海外では産学間の移動も多く、民間の優秀な人材が大学で学び、さらに専門的な能力を身につけるという流れが存在し、我が国においても、大学における教育や人材育成の取組を重視しつつ、産学官での人材交流・流動化を推進することが重要となる。

⑤　中小企業や地域における対策強化とその他の検討課題等

サイバー攻撃は、セキュリティ対策が十分でないところが狙われることがあるため、サプライチェーンの弱点を突いたサイバー攻撃が増加しているなど、その被害は重要インフラ事業者等に限らず、中小企業等にも及んでいる。社会全体の強靭性を高める観点からは、我が国において数の上で 90%以上を占める中小企業や地域の企業を含むサプライチェーン全体での対策が必要であるが、資金や人材等のリソースが限られている中小企業が自らのみでセキュリティ対策を進めていくことは困難である。

そのため、**中小企業等のセキュリティ対策については、必要性に関する意識啓発や政府によるツールの提供などを含めた支援拡充の検討のほか、大企業による下請企業のセキュリティ対策の支援・要請に係る独占禁止法等の明確な整理、サプライチェーン企業の対策水準の検討を行うべき**であると考えられる。

また、中小企業等については、サイバーセキュリティの対策・情報共有を実施できる人材育成が必要と同時に、政府がそのような中小企業等の活動を支援しつつ情報連携を行う施策を検討することが望ましいと考えられる。

最後に、本提言には、本章の横断的課題を中心に、制度整備によらず、速やかに具体的な施策や枠組みを検討すべき指摘も含まれている。**政府においては、これらの指摘について、戦略本部の場の活用も含めて、検討に着手すべき**と考えられる。

3　参考資料

（参考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　構成員一覧

（五十音順）

上沼　紫野	LM 虎ノ門南法律事務所弁護士
遠藤　信博	日本電気株式会社特別顧問
落合　陽一	筑波大学デジタルネイチャー開発研究センター長/准教授
川口　貴久	東京海上ディーアール株式会社主席研究員
川添　雄彦	日本電信電話株式会社代表取締役副社長 副社長執行役員 一般社団法人 電気通信事業者協会参与 一般社団法人 ICT-ISAC 理事
酒井　啓亘	早稲田大学法学学術院教授
佐々江　賢一郎	公益財団法人 日本国際問題研究所理事長
宍戸　常寿	東京大学大学院法学政治学研究科教授
篠田　佳奈	株式会社 BLUE 代表取締役
辻　伸弘	SB テクノロジー株式会社プリンシパルセキュリティリサーチャー
土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
野口　貴公美	一橋大学副学長、法学研究科教授
丸谷　浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表 兼 名古屋支社代表
村井　純	慶應義塾大学教授
山岡　裕明	八雲法律事務所弁護士
山口　寿一	株式会社読売新聞グループ本社代表取締役社長
吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院教授

（参考２）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の開催状況

第１回会議：令和６年６月７日（金）
議事：（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について
　　（２）討議
　第１回テーマ別会合
　　令和６年６月１９日（水）、２０日（木）　通信情報の利用に関するテーマ別会合
　　令和６年７月１日（月）　アクセス・無害化措置に関するテーマ別会合
　　令和６年７月３日（水）　官民連携に関するテーマ別会合

第２回会議：令和６年７月８日（月）
議事：（１）経済三団体からのヒアリング
　　（２）質疑応答
　　（３）テーマ別会合の開催状況[報告]
　第２回テーマ別会合
　　令和６年７月２３日（火）　官民連携に関するテーマ別会合
　　令和６年７月２４日（水）　アクセス・無害化措置に関するテーマ別会合
　　令和６年７月２６日（金）　通信情報の利用に関するテーマ別会合

第３回会議：令和６年８月６日（火）
議事：（１）テーマ別会合について[報告]
　　（２）これまでの議論の整理[報告]
　　（３）自由討議
　第３回テーマ別会合
　　令和６年８月２６日（月）　通信情報の利用に関するテーマ別会合
　　令和６年８月２７日（火）　アクセス・無害化措置に関するテーマ別会合
　　令和６年９月２日（月）　官民連携に関するテーマ別会合

第４回会議：令和６年１１月２９日（金）
議事：（１）テーマ別会合について[報告]
　　（２）サイバー安全保障分野での対応能力の向上に向けた提言（案）
　　（３）自由討議

（了）