

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

これまでの議論の整理（案）

令和6年8月6日

内閣官房

サイバー安全保障体制整備準備室

目次

- I. 官民連携の強化 3
- II. 通信情報の利用 7
- III. アクセス・無害化 13
- IV. 横断的課題 17

I. 官民連携の強化

0 対応能力向上のための官民連携の必要性

① 重要インフラ等への攻撃の高度化

- ・ サイバー攻撃は一段と巧妙化、高度化、複雑化、組織化されていることが顕在化している。
- ・ 攻撃の高度化に伴い、近年の攻撃は単純なインディケータ情報の共有では検知や対策が困難になってきている。
- ・ 現状、インシデントの報告窓口は複数存在しており、一刻を争う状況の中で、報告コストを下げるため、窓口の一本化やフォーマットの統一が求められる。

② 重要インフラ等のデジタル化

- ・ 重要インフラのDXが進んだ結果、インターネット等への依存が高まり、サイバーセキュリティのリスクも高まった。
- ・ 重要インフラを守ることの大きな目的は、国民視点でサービスが持続的に提供されるということ。

③ 社会全体の強靱化の必要性

- ・ サプライチェーン全体を考慮したとき、国家のレジリエンスを確保するためには、数の上で90%以上を占める中小企業の対策は絶対的に必要。
- ・ セキュリティ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。
- ・ 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。

1 高度な攻撃に対する支援・情報提供

① 政府の役割について

- ・ 重要インフラは、国民視点でサービスを継続できることが大事。
- ・ 人口減少社会において、社会全体の強靱性（レジリエンス）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。
- ・ 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、社会全体の強靱性（レジリエンス）を最大化できるよう、リスクコミュニケーションや支援を行うべきではないか。
- ・ 被害企業から情報を報告してもらうには、インセンティブの設計が大事。いわゆる「平時・有事」の区別なく、状況に応じて、政府が情報を受け取るだけでなく、率先して情報を示していくなどの姿を見せることにより、官民双方向の情報共有を促進すべきではないか。

② 提供されるべき情報について

- ・ 経営者、実務者、アナリストといった階層ごとに適切な情報を提供することが必要。
- ・ 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た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国際情勢、地政学といった視点からの情報も共有すべきではないか。
- ・ 近年の攻撃は、単純なインディケータ情報の共有では検知や対策が困難であり、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（マルウェアのふるまいに関する情報や攻撃者のツール・テクニック）の提供も必要ではないか。
- ・ 攻撃者の動向として、サイバー攻撃の資金源となっている仮想通貨の移動を分析することも有効ではないか。

③ 情報提供の方法について

- ・ 抜本的に強化した新しいNISCのもとに、官民の協議会を置く体制が考えられる。
- ・ 情報提供の主体について、JPCERT/CC、IPA、警察、経済産業省等のそれぞれの観点があることは理解するが、有事においては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、ワンボイスで行うべきではないか。
- ・ インテリジェンス活動等を含めて政府が分析した情報を、必要な共有先に柔軟に共有すべきではないか。
- ・ 情報の提供先は必ずしも重要インフラに限られず、情報ごとに提供範囲などを定義するべきではないか。
- ・ セキュリティクリアランスがあると海外との連携、官民の情報共有が行いやすくなることなどが期待できるため、最大活用を考えてほしい。
- ・ 公開範囲に応じてどのような情報を出すかといった、情報の区別の定義や情報公開に関する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はないか。
- ・ 安全・安心なサイバー空間を構築するためには、トラストに立脚した相互運用性が不可欠。このため、政府による制度設計においては友好国との間での平仄と相互運用性に配慮すべきではないか。
- ・ 海外や国内の取組が進んでいるISAC(Information Sharing and Analysis Center)の事例を調べ、ISAC間のノウハウ共有を政府が支援してはどうか。
- ・ 情報共有基盤の開発に当たっては国内技術による自立性に留意すべきではないか。

2 ソフトウェア等の脆弱性対応

① ベンダの責務について

- ・ 毎年、多くの脆弱性が公表され、約3万件にも上るが、攻撃に悪用されているのはそのうち1%未満。悪用されている脆弱性に優先的に手当てをすることが重要ではないか。

- このうちゼロデイ脆弱性について、官民が連携してゼロデイ脆弱性を早期認知・対処できるよう、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深めるべきではないか。また、ゼロデイ攻撃を早期に認識するためには、ハニーポットなどの観測基盤の強化が必要ではないか。
- 安全な製品開発や脆弱性の対応に関するベンダの責任を規定すべきではないか。
- 攻撃を受けたソフトウェアベンダからユーザーに被害が拡散する「サプライチェーン攻撃」を防ぐため、海外事例等も参考に、安全性のテスト基準などベンダの規律を設定し、セキュアな製品の提供や脆弱性情報の報告等を求めるべきではないか。
- SBOM (Software Bill of Materials) やセキュアバイデザイン・セキュアバイデフォルトを推進すべき。
- IoT機器等の中小ベンダは資源が限定的であり、厳しい価格競争も踏まえると、単にベンダだけに責任を負わせるのではなく、セキュアな製品開発・供給にあたっての支援も検討すべきではないか。

② 脆弱性情報等の提供について

- 平時から脆弱性対応を行うには、影響を受ける機器が国内にどれだけあるかを把握しておくことが重要ではないか。
- 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べきではないか。
- アメリカで悪用が認められた脆弱性 (KEV) がカタログとして公表されているが、日本やアジアでのみよく使われているソフトウェアの情報は掲載されない。事業者等が膨大な脆弱性情報の中から優先順位を付けられるよう、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はないか。
- 豪州では、資産情報を予め登録させることで、登録情報と適合した脆弱性情報が速やかにフィードバックされる仕組みとなっており、これは、迅速な情報提供を実現する取組の一つだと考えている。
- 日本においても、国民生活等の基盤となる事業者については、政府が資産情報を把握し、関連するゼロデイ情報等を速やかに提供する枠組みを構築すべきではないか。
- 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負担になってしまうことに留意すべき。

3 政府の情報提供・対処を支える制度

① インシデント報告の義務化、情報共有を促進する仕組みについて

- 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れば、継続的なサービス提供のため、影響の大きさに応じ、インシデント報告を義務化し、情報共有を促進すべきではないか。デジタルインフラと電力は特に重要なインフラとして扱うべきではないか。

- ・ インフラ以外の事業者についても、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、官民の会議体を設置するなど、情報共有を促進する仕組みを設けるべきではないか。
- ・ その制度設計に際しては、屋上屋を架すような制度は避けるべきであり、ISACやサイバーセキュリティ協議会、JPCERT/CCやIPA等の既存枠組の効果を検証すべきではないか。また、現場レベルで官民の対応者が集結できる仕組みが必要ではないか。

② インシデント報告の迅速化について

- ・ 行政へのインシデント報告は、これまで監督省庁へ行われてきたが、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。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はないか。
- ・ 事業者には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になってきている。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はないか。

③ 報告された情報の取扱いについて

- ・ 報告を行う被害企業の負担を考慮すると、報告先の一元化に加えて、報告フォーマットの統一化も必要。この際、フォーマット以上の情報が入手できないことを防ぐため、一定のバッファを設ける等の工夫もすべきではないか。
- ・ 情報提供を行う民間企業の立場からすると、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いと、リスクが高すぎて情報提供できないのではないか。
- ・ 情報提供については、明確な規律が必要ではないか。報告された情報は、経営上機微な情報を含み得るため、慎重に取り扱うべき。報告された情報の利用目的を明確化し、情報の不用意な流出や、制裁目的での利用防止を規定すべきではないか。
- ・ 提供された情報はセンシティブ情報として慎重に取り扱うべきであるが、工夫により業種や攻撃の種類等がある程度分かる形で注意喚起に活用することも必要。

II. 通信情報の利用

1 攻撃実態解明のための通信情報利用の必要性

- 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。
- このような状況で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、ボットネットワーク*等の攻撃の実態を把握することが必要。

*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り、これらの通信機器（ボット）を多数、多段的に組み合わせて構成された攻撃用のネットワーク（ボットネットワーク）を利用することが通常。しかも、これらボットの多くは、国外に所在すると考えられている。

- アクセス・無害化を行うに当たっての判断のためにも、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。
- 平時からの分析が必要であり、令状主義*に基づく個別かつ司法的なコントロールでは、通信情報の利用と通信の秘密の保護という両方の目的を適切に果たすことができない。

*例えば、電話番号やメールアドレスなどにより特定され傍受令状に記載された通信手段に対して傍受を行う「犯罪捜査のための通信傍受に関する法律」（通信傍受法）が該当する。なおここでいう「令状」は憲法第35条第2項「権限を有する司法官憲が発する各別の令状」を指すが、外国法制での「令状」あるいは「許可状」は、司法府ではなく行政府の発行するものを指す場合がある。

- 海外に依存することなく、日本独自の情報収集が必要。
- 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のではないかと考えられる。日本がサイバー防御の能力を高めることは、国際的にも要請されていると考えられる。
- 先進主要国では、国家安全保障等の観点から、テロ防止等のほか、サイバー攻撃対策のためにも、通信情報を利用していると考えられる。その状況は、おおむね次のとおりと考えられるところ、これを踏まえると、我が国でも、重大なサイバー攻撃への対策のため、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。

- 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いる。
- 従来はテロ防止のために行われていたが、現在は、サイバー攻撃対策としても、用いられている。（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）。
- 個別具体的な調査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手法がとられている
- 取得と分析には一定の技術及び能力が必要とされる。
- 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。

- 通信事業者等の協力が必要。法律上の義務付けとともに、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。

2 通信情報の利用の範囲及び方式

- 外国が関係する通信については、国外に日本の国家権力が及ばないこともあり、分析する必要が特にあると考えられる。
- 日本を經由して伝送される外国から外国への通信である「トランジット」の通信を分析してよいかについては、先進主要国と同等の方法の分析をできるようにしておく必要があるのではないか。
- 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。
- 通信情報は、①電気通信設備等を識別する情報、②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、③その他機械的な情報、④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④は特に分析する必要がありとまでは言えないのではないか。すなわち、メールの中身を逐一全て見るようなことは、サイバー防御では適当とは言えない行為である。
- 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。サイバー防御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はないか。
- 問題を未然に防ぐ予防のための分析であるため、既遂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はないか。
- 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・能力と設備が必要ではないか。民間企業と協力することも考えられるのではないか。
- 諸外国の事例を勉強し、分析の範囲等を理解した上で設計し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。

3 通信の秘密との関係

- いわゆるメタデータなど、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。
- 一方で、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。
- 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。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。
- 先進主要国を参考にしながら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はないか。
- 実体的な規律とそれを遵守するための組織・手続き的な仕組み作りが必要であり、

また、明確で詳細なルールとなるよう考慮することが適当ではないか。

- 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（別添参照）。
- 通信情報の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、整理していくべき。
- 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のではないかと。また、独立機関による監督があることも共通している。
- 独立機関は重要。各国の司法制度等との関係や日本の他法での類例を含め、検討していくべきではないか。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として導入していくことを考える必要があるのではないかと。
- なお、以上の議論は通信当事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。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、そもそも憲法上許容されると考えられる。その場合の同意の在り方は更に検討していく必要があるが、制度により規格化された内容による同意が方法として考えられるのではないかと。

4 電気通信事業者の協力

- 公益のため政府によるサイバー攻撃対策の通信情報の利用に協力を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。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。
- 通信情報の利用による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。
- 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。
- 行政や民間の解釈に委ねるのではなく、法整備により、国の責任で取り組むことが必要。
- 政府と民間の適正な連携が重要。その点でも、独立機関などのガバナンスの仕組みを考えていくべき。

5 国民の理解を得るための方策

- 国民の理解を得ていくため、制度の在り方の議論を深めることや透明性を確保していく視点が重要。
- 「手の内」を知られないようにしなければならない必要から全てを公開することは難しいと考えられるが、大枠の情報の公開は行われるべきではないか。
- 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のではないかと。その

意味でも、独立機関の構成や業務の在り方が重要ではないか。

- 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ことで、理解を得ていくことも重要ではないか。
- 今回検討する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必要ではないため、得られた情報は積極的に活用していくことが適切ではないか。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はないか。

別添 英国及びドイツにおける通信情報の利用と通信の秘密又は人権との関係

・ 英国

- 調査権限法により、安全保障上の必要性等がある場合に、「運用目的」を特定した上で、分析や外部提供等の制限及び独立機関の監督の下、海外関連通信（英諸島外の個人による送受信される通信）について、「不特定型」の通信情報の利用が可能。
- 情報収集活動について幅広く規律する調査権限法は、英国がEU離脱後も欧州評議会加盟国であり、議院内閣制という共通項もあるため、特に我が国の参考となり得る。
- EU法でも、欧州人権条約でも、国家安全保障や重大犯罪への対処のために、人権の制約をする場合があることを認めている。
- 関連判決では、調査権限とプライバシー等の人権の関係について、権限の範囲及び人権制約に関して明確かつ詳細なルールを定めなければならないとの判断が共通している。
(EU司法裁判所の6判決、欧州人権裁判所の1判決と英国国内裁判所の1判決)
- 「不特定型」の通信情報の利用は加盟国が自国の安全保障への脅威を特定するために不可欠な重要性を有しているとして、正当で必要である旨を認める判決もある。
- 権限の濫用・誤用の防止だけでなく、権限の内容・手法が権限の目的にふさわしいかという視点 (fit for purpose) も重要とされる。すなわち、国家主権が侵害されると人権の存立基盤が失われるため国家安全保障には不可欠な価値がある一方で、国家安全保障が人権侵害を引き起こす場合には民主主義国家としての正当性が失われることになるため、効果的・効率的な調査権限と人権保障の両面に関して、明確かつ詳細な規定を置く必要があると考えられるもの。
- 独立機関であるIPCO（調査権限コミッショナー事務局）は、調査権限の全てのプロセスについて監督した結果として、エラー（誤り）の状況の記載を含む年次報告を公表している。

・ ドイツ

- 連邦情報局法*により、安全保障上の必要性があり、重大な危険分野(マルウェアによる国際的犯罪・テロ・国家攻撃、重要インフラに対する脅威等)に関する情報の入手のために必要な場合に、分析や外部提供等に対する制限と独立機関の監督の下、外国の電気通信について「不特定型」の通信情報の利用が可能。

*事務局資料では「連邦情報庁法」と称している場合がある。

- 1968年に基本法(憲法)が改正され、「通信の秘密」の制限が4つの条件*の下で認められ得るということが明記された。

*法律の根拠に基づくこと、安全保障等に役立つこと、本人に対して非通知の場合はその旨が法定されること、国民代表の選任した機関及び補助機関による事後審査を行うこと。

- 外国の通信の不特定型の収集・利用と「通信の秘密」との関係については、連邦憲法裁判所の判決において、一定の措置を講じなければ、通信の秘密に対する制約が正当化できないとされている。
- 同判決で最も重点が置かれたのは狭義の比例性審査であり、通信の秘密の保護とその制限によって守られる安全という2つの法益の単純なバランスではなく、制度設計に関する具体的要件について審査が行われた。その結果、継続的で独立した事前・事後の監督・統制、透明性・法的保護・監督に関する基準などの約10項目の重要な考慮要素が示された。
- 独立機関の権限と機能が特に重要なポイント。同判決を受けて連邦情報局法が改正され、2022年1月、新たな独立機関として「独立統制評議会」(UKRat)が設立。通信情報利用の開始前に審査を行う司法機関類似の統制機関と事後の統制をする行政的統制機関から構成される新たな方式の独立機関であり、連邦情報局の通信情報の利用その他の情報収集活動(技術的監視)に対する包括的な統制を実施。
- 独立機関は、基本的には、連邦情報局が保有するすべての記録にアクセスできる。独立機関には、厳しい守秘義務がある。
- 議会の役割は、俯瞰的なもの。ドイツでは議会統制委員会がこの役目を担っているが、選挙の結果に応じてその構成員が変わることもあり、個別の行政活動を統制するという事にはならない。

Ⅲ. アクセス・無害化

1 サイバー空間の特徴を踏まえた実効的な制度構築

- 今回の無害化措置は、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で、必要な措置だと考えている。
- 行政法的には、特に制度の中に置かれる手法の定め方が、制度の実効性を左右する重要なポイント。単なる理念法や理念的な組織法のレベルにとどまるものではなく、関係組織、関係主体の具体的な権限執行法として構想されること、従来の法執行システムと接合的で連続的な仕組みとして構想すべきではないか。
- 措置には、事前の予防に当たる作用から何か起こったときの措置まで幅広い措置が含まれ得る。作用法にしていくという視点からは、①要件を書ききり、命令により実施、②許可・令状の仕組みを導入し、実施、③警察官職務執行法のように、即時に実施の大きく3つのやり方が考えられる。
- アクセス・無害化措置は平素からの活動が基盤となるものであるとともに、緊急性を意識した、迅速かつ臨機応変な対応が特に重要。その意味で、現場対応の力、Improvisationのスピリットが求められる。
- 能動的サイバー防御の主たる目的は被害の未然防止にある。インシデントが起こってから令状を取得し捜査を行う、刑事手続の令状審査では対処できないのではないか。無害化に当たっては、政治・外交等の手段も活用していく必要があることも踏まえると、行政的作用法で規律されるのが妥当ではないか。
- 措置に当たっては、その場その場での判断で適切な手法を選択して実施していく必要があり、臨機応変さが重要。そのため、法制度整備に当たっては、あらかじめ具体的な無害化の手法を法律上にメニューとして用意するという形の条文化は難しいのではないか。具体的な活動の内容を要件と効果で規定して羅列するのではなく、目前に存在する危険に対して、危害防止のための措置を即時執行として行うことを可能としている警察官職務執行法を参考とすべきではないか。
- 警察官職務執行法を参考とするに当たっては、その背景や周辺にある警察制度、警察官の教練、日常の警らの活動、様々な制度の中で即時執行を可能にしているという視点が重要である。サイバー空間においても、無害化措置という手法単体ではなく、連続するプロセスにおいて段階的な権限行使をしていく中で、無害化措置というものをどう位置付け、どう正当性を担保していくのか等の一連のプロセスとして議論していくべきではないか。
- 現実空間とサイバー空間における危険の顕在化には相当の違いがあるため、現行の警察官職務執行法そのままというのは難しく、法制度設計においては、サイバー空間の特性を踏まえた調整が必要であることには留意が必要。
- サイバー攻撃事案はボーダーレスで融合しているため、総合的評価が必要であり、個別要件の明示は困難なのではないか。
- 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、事態を細かく区切り事態を認定するという従

来の事態認定の方式ではなく、平素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ではないか。

2 措置の実施主体

- ・ 諸外国の無害化措置の実行・運用主体が軍、法執行機関、インテリジェンス機関であることを考慮すると、日本国内においては防衛省や自衛隊、警察等が保有する能力を活用すること、その能力を高度化することが極めて重要ではないか。

3 措置の対象

- ・ 無害化措置を講じる事案の優先順位付けを考える必要がある。能力やリソースが限られることを勘案すれば、対処すべき事案の優先順位を付けていくことが大事。
- ・ 無害化措置の対象としては、国民の生命・安全に関わる重要インフラや有事において自衛隊や在日米軍の活動が依存する通信・電力などのインフラ等が優先順位が高いのではないか。
- ・ 対象事案である「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」もののスコープとしては、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ものを重視すべきではないか。

4 アクセス・無害化措置と国際法との関係

- ・ 様々な措置についてどういう影響が生じるかを踏まえた上で、目的、あるいは相手方の対象の性質を加味して違法性を考えなければならないが、具体的にどの行為が主権侵害に当たるか、確定することは困難。
- ・ 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等の点から、違法性阻却事由として対抗措置を援用することが有用かどうかはやや疑問。現時点での評価としては、緊急避難の方が違法性阻却事由として援用しやすいのではないか。
- ・ アクセス・無害化措置は国家実行として国際法規則の形成に影響を与える事項なのだということを考えてほしい。サイバー空間での活動の特徴を踏まえ、慎重に法制度の発展が図られるべきではないか。

5 制度構築に当たっての留意点

- ・ 無害化措置の執行は、その場その場での判断で適切な手法を選択して実施していく必要がある一方、比例原則を遵守し、必要な範囲で実施されるものであるべき。
- ・ アクセス・無害化措置の実施には世論の支持、そして世論の支持を得るためには手続の公正性・透明性の確保が不可欠であって、さらに、サイバー防御とプライバシー保護の両立も考えていかなければならない。サイバー防御には事前審査の時間を取れない場合もあろうが、現場で即時実力行使できるように警察・自衛隊に執行権

限を行使する権限を与える場合、独立性を持った機関が事後監査を行うこととすべきではないか。

- 全く関係のない人のパソコンを無害化措置の対象にしてしまった場合、マルウェアに感染しているパソコンのプログラムを消去したことによって、そのパソコン自体が使用できなくなってしまった場合など、無害化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に、こういったセーフティネットがあるのか議論しておく必要があるのではないか。
- 権限とポリシーの関係について、個別のアクセス・無害化措置のオペレーションは、政治が個別に確認・承認するというものではないと思料。サイバー攻撃における緊急性・切迫性を踏まえ、様々な分野における専門家が、チームでオペレーションを回していく必要。他方、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、適切な「ポリシー」の下で専門家集団がオペレーションを回せるようにする必要があるのではないか。

6 運用に当たっての留意点

- しっかりとした状況自体の把握と同時にprediction（予測）が必要。同時に無害化のための戦略を立てる必要。その観点からいうと、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、無害化する能力等、多様な機能・人材が集まり、円滑な情報共有が行われることによって、無害化措置の戦略ができあがると考えている。そのための機能や必要な人材・能力の明確化、そして多様な人材が一緒になって無害化の戦略を作るエコシステムが重要。
- 攻撃側のインフラは、攻撃者が直接的に管理・運用するコア部分に加えて、それを取り巻く関連のリソース、サービスから成り立って多重的なものと理解。そのため、攻撃者とそれ以外という二値ではなく、その間には、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、様々なグラデーションの中間地帯があると思われる。
- インシデントが発生した場合に、攻撃側の追及を行い、アクセス・無害化措置を行っていくことになるが、攻撃側・被害側ともに必ずしもどの国に属しているかがマッチするものではなく、サイバー攻撃の技術的な複雑さが増している。サイバー攻撃を実施する国の特定には不確実性をはらむため、中継ネットワークが所在する国との連携が重要。
- 攻撃者のグループも、国家を背景とする高度な攻撃を行うグループから、ティーンネージャーの小遣い稼ぎのような攻撃もある。そうしたものの区別を早い段階でしておくことで、より適切な運用に資するのではないか。攻撃グループのアトリビューションが必要。
- 無害化措置そのものや優先順位付けに不可欠なのがインテリジェンスである。主要なサイバー脅威の動向、つまり中国、ロシア、北朝鮮、ランサムウェア犯罪集団がどのような動機や狙いで能力を開発しているかをしっかりと見極めて、彼らが嫌がることをやっていく、コストを課していくため、必要なインテリジェンスをサイバー空間に限らず収集、分析し、政策判断に活かしていくことが重要であると考えている。

- 公開情報のみの収集には限界。政府によるダークウェブにおける情報収集やゼロデイ脆弱性の購入等にも踏み込んでいく必要があるのではないかと。
- アクセス・無害化の実施に当たっては、平素からの情報収集やサイバー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重要。
- アクセス・無害化を検討する上では、総合的な情報収集と官民協力・国際協力が重要。サイバー空間に限らないオールソースデータの蓄積・活用や平素からの情報活動が大きな役割を果たす。平素からの情報収集は警察、自衛隊、情報機関などによる多様な能力を活用することを前提とし、サイバー空間を含めて積極的に行われる必要。
- 無害化措置の中でも、強度の高い措置の実施に際しては、政治、外交など他の枠組みの活用可能性を追求し、それを踏まえた総合的な判断が求められる場合もあることから、司令塔の存在が極めて重要となる。
- アクセス・無害化措置を実施する体制作りを進める上で、極めて高い専門性を有する専門家の協力が必要であり、その活用が必須。他方、こうした専門家が政府のアクセス・無害化措置に協力するに当たって危険に晒されることもあり得るため、こうした協力する人材を保護する、プロテクションシステムが重要であり、こうしたシステムが政府に協力するインセンティブにもなり得る。
- 「アクセス・無害化措置」の体制を構築するには極めて高度な専門家・人材の育成が必要。無害化のための専門家は通常の教育で育てるものではなく、一旦教育をして1-2年の実践教育が必要と思っている。それを念頭に置いた教育システムの構築も無害化の対応の一つとして用意する必要がある。どういう領域にどういう人数が必要かを明示化することで、教育システムの組み方も変わる。また、人材の給与・待遇改善・待遇の明確化をサポートすることも重要。
- ソフトウェア・ハードウェアを含め日本としての自律が必要。また、官民交流の中で人材を教育していくことも含め、全体での人材育成のシステム構築が求められる。
- アクセス・無害化措置の実施に関し、判断を下すCommanderと、実行するOperatorがいるという単純な状況とは異なり、緊急時に短い期間で対応しなければならない場面がある。その観点でいえば、サイバー対処の現場には、法律家等含めて各分野に精通した人材がいることが重要ではないかと。

IV. 横断的課題

- 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
 - ・ サイバーセキュリティ戦略本部は、一般的な政策立案や助言だけでなく、事案が発生したときに、司令塔として関連省庁に指示を出す組織だとすれば、有識者の関わり方を含めて、構成の在り方を検討すべきではないか。
 - ・ NISCやサイバーセキュリティに関係するその他政府機関等、それぞれの役割と責任範囲を明確に整理すべきではないか。
 - ・ 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。
 - ・ 基本的な方針や枠組みをサイバーセキュリティ戦略本部で決定し、それに対して普段から助言をする組織が別途存在するという形も考えられるのではないか。
 - ・ 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、改善に資するのではないか。
 - ・ 地方公共団体についても、政府が横断的な指令塔としての役割を果たせるようにすべきではないか。

- 2 重要インフラ事業者等の対策強化
 - ・ 重要インフラの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て考えるべき。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。
 - ・ 重要インフラは、国民視点でサービスを継続できることが大事であり、インフラの補完・代替・復旧など全体の大きな計画の中でどのように備えるべきか考えるべき。
 - ・ 政府が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、有事の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べきではないか。
 - ・ 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には、政府が方法論を用意して、それを中小企業が活用する取組が必要ではないか。
 - ・ 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、誘導していく手法が重要。また、基準等については関係者の声を聞き、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考えていくことが重要ではないか。
 - ・ 重要インフラ分野の中で優れた取組があるなら、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考えられるのではないか。
 - ・ サプライチェーン全体のレジリエンス強化に向けて、ガイドラインの策定のみならず実行に必要なリソース支援、政府調達要件への採用等も検討すべきではないか。

3 政府機関等の対策強化

- まず取り組むべきこととして、各組織におけるサイバーセキュリティ水準を強固にすることが必要。
- 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・分析の積み重ねが必要。
- 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。
- 英国では、公共機関や国民向けに多様なサービスを提供しており、現行法制度下でも実施可能な施策は取り入れるべきではないか。
- 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ではないか。

4 サイバーセキュリティ人材の育成・確保

- 産学官の共通認識を醸成するため政府主導で人材定義の可視化を検討するとともに、必要な人数・規模についてもメッセージを示すべきではないか。
- 人材の育成・確保については、資格の活用や、非技術者の巻き込みも重要ではないか。
- 適切な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必要ではないか。
- サイバーセキュリティ人材の待遇の改善、経営層の理解の促進、長期的なキャリアパスの提示、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策が必要ではないか。
- サイバーセキュリティ人材の確保のためには、若年層の教育も重要ではないか。
- CISOを組織で重要視すべき。CISOを置くことで組織のセキュリティが強化されるとともに魅力的なキャリアパスを提示することになる。
- 官民の流動化を進めるうえで、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が重要ではないか。現場に携わる人の生の声を聞き、それを集約して政策に活かすことも重要。
- 海外では産学間の移動も多い。民間の優秀な人材が大学に来て、さらに専門的な能力を身につけるといった流れは重要。
- 情報や危機感の共有によるトラストの醸成を目的として、NISC等の政府機関との官民人材交流に関する枠組みを導入すべきではないか。
- 関係省庁のサイバーセキュリティ部局の人材の任期の長期化等を検討すべきではないか。

5 中小企業を含めた対策強化

- 社会はサプライチェーンで価値を創出。中小企業の強靭性を高めないと、社会全体の強靭性は高まらない。
- 特にIoT機器などは、大企業だけが製造に関わっているのではなく、リソースが限られている中、家庭用製品は厳しい価格競争にも晒されている。対策を企業だけに任せるのは難しく、メーカーをサポートするなどの対策が必要ではないか。
- 情報共有を行う内容の調査ができる人材育成が必要と同時に、調査を支援してくれるのであれば報告するという企業からの情報を拾い上げる仕組みも検討する必要があるのではないか。
- 基幹インフラのサプライチェーンを含め、中小企業の限られたリソースを考慮したツールの提供など、中小企業の事業継続・セキュリティ対策の支援をお願いしたい。
- サプライチェーンにおいて、大企業が下請けとなる中小企業のセキュリティ対策を要請したり、逆に支援したりすることが競争法上の問題とならないか、整理することが必要なのではないか。

6 その他の論点

- 政府の司令塔は、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べきではないか。
- 大学発のよい技術を社会実装するとともに、その知見が研究にフィードバックされることで、更なる技術開発につながるが、日本では、このサイクルが機能せず、大学発の中核的なセキュリティ技術が少ないのではないか。
- サイバー分野の投資に対して税制優遇を行うことが考えられるのではないか。
- 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やサービスの供給を支援すべきではないか。
- 適切な比喻や統計データの活用などにより、幅広い層にサイバーセキュリティの重要性について発信することは重要。

(了)