

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）
概 要

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

国家安全保障戦略（抄）	2
Ⅰ 官民連携の強化	5
Ⅱ 通信情報の利用	9
Ⅲ アクセス・無害化	13
Ⅳ 横断的課題	17

- サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。
- サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、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。

【略】

武力攻撃に至らないものの、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、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

- (ア) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。
- (イ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。
- (ウ) 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について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

I . 官民連携の強化

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>

- 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、日本全体の強靱性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。
 - 情報共有は社会全体の強靱性を高める上で最重要であり、被害組織が情報提供するインセンティブの設計が必要。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はないか。
-

<② 提供されるべき情報について>

- 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、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の提供も必要ではないか。
-

<③ 情報提供の方法について>

- 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はないか。
- 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、ワンボイスで行うべきではないか。また、友好国との間での相互運用性に配慮すべきではないか。

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>

- ❑ 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。
 - ❑ 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とともに、観測基盤を強化すべきではないか。
 - ❑ 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。
 - ❑ 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>

- ❑ 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。
- ❑ 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。
- ❑ 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。

3. 政府の情報提供・対処支援を支える制度

<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、ISACやサイバーセキュリティ協議会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>

- 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。
- 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。

Ⅱ．通信情報の利用

1. 通信情報の利用の必要性

- ❑ 一般利用者の乗っ取られた通信機器で構成されるボットネットワーク等の攻撃の実態を把握するためには、通信情報の分析が必要。また、その分析は、平時から行うことが必要ではないか。
- ❑ 国家安全保障等の観点からサイバー攻撃対策のためにも通信情報を利用している先進主要国の状況に鑑み、日本でも、重大なサイバー攻撃への対策のため独自の分析を行えるよう、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はないか。
- ❑ 通信情報利用は先進主要国との連携でも有意義。日本の能力向上は国際的にも要請されている。

2. 通信情報の利用の範囲と方式

- ❑ 外国が関係する通信の分析が特に必要。日本を経由する外国から外国への通信（トランジット通信）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。
- ❑ 個人の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あるとまでは言えないのではないか。メールの中身を逐一全て見るようなことは適当ではないのではないか。
- ❑ 収集したデータ全てを人間の目で判断することは不可能かつ不適切。機械的な選別等が重要ではないか。最初は広く、懸念が見つければ深くとの考え方が妥当ではないか。
- ❑ データ分析の技術、能力、設備等も重要。

３．通信の秘密との関係

- 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。
- 具体的な制度設計の各場面において、丁寧な検討を行うべき。
- 先進主要国を参考にしながら、緻密な法制度を、作り上げていくことが必要ではないか。
- 定められた規律の遵守を確保するための仕組みが必要ではないか。明確で詳細なルールも重要ではないか。
- 情報処理の各プロセス（実施過程）でどのような統制や規律が必要なのか、整理していくべき。
→ 先進主要国では、準備・承認、電気通信事業者への措置、処理・分析、共有、廃棄等の一連の実施過程が法律で定められ、独立機関が監督
- 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。
- なお、通信の秘密の制限に対する通信利用者の有効な同意がある場合の通信情報の利用は、憲法上許容される。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。

4. 電気通信事業者の協力

- ❑ 協力を行う電気通信事業者は社会の安全のために貢献しているとして肯定的に評価されるべき。
- ❑ 電気通信事業者に求められる協力が、電気通信事業者の実施可能な範囲内になるよう、明確化していく必要があるのではないかな。
- ❑ 電気通信事業者が直面し得るリスクや負担等について回避策を十分に検討していくべき。
法整備により、国の責任で取り組むとすることが必要ではないかな。
- ❑ 官民の適正な連携のためにも、独立機関等のガバナンスの仕組みを検討することが必要ではないかな。

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。
- ❑ 運用の詳細などまで全てを公開することは性質上難しいと考えられるが、適切な情報公開は行われるべき。
- ❑ 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な。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な。
- ❑ 通信情報の利用の必要性について、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な。
- ❑ 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な。

Ⅲ. アクセス・無害化

１．実効的な制度構築の必要性

- ❑ 無害化措置は、我々が価値創造を行う安全なサイバー空間を守る観点で必要。
- ❑ 新制度は、被害の未然防止を目的とする重要なものであり、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と。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、行政作用法として規律されるのが妥当ではないかと。また、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と。
- ❑ 事象や状況の変化に臨機応変に対応し、講じるべき措置を変化させていく現場対応的な力が必要ではないかと。個別の要件を法定し、あらかじめメニュー化された措置を講じる制度はなじまず、むしろ、状況に応じた措置を即時的に実施する現行の警察官職務執行法を参考とすべきではないかと。その際には、執行に係る全体のプロセスやシステムも参考とすべきではないかと。
- ❑ 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と。

２．措置の実施主体・措置の対象

- ❑ 諸外国での無害化措置の実行・運用主体を考慮すると、日本国内においては防衛省・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。
- ❑ 能力やリソースが限られることを勘案し、措置を講じる事案の優先順位付けを考える必要があり、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。
- ❑ 対象事案のスコープは、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を重視すべきではないか。

３．措置と国際法との関係

- ❑ 措置により生じる影響、措置の目的、対象の性質等を加味して国際法上の違法性を考えなければならず、具体的にどの行為が他国の主権侵害に当たるかをあらかじめ確定することは困難。
- ❑ 他国の主権侵害に当たる場合の国際法上の違法性阻却事由として、実務上は対抗措置法理よりも緊急避難法理の方が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。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。

4. 制度構築に当たっての留意点

- ❑ 無害化措置は、臨機応変な執行を可能としつつも、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。
- ❑ 透明性や公正性の担保、プライバシー保護、また、サイバー攻撃の特性に応じた執行の観点から、アクセス・無害化措置の適正性を確保する制度の検討（独立した立場からの監督など）、意図しない結果が生じた際の対応、現場における執行権限の必要性等に配慮すべきではないか。
- ❑ 個別のオペレーションに政治が個別に承認するのではなく、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。

5. 運用に当たっての留意点

- ❑ 攻撃インフラの多重性・サイバー攻撃の技術的複雑性を踏まえ、関係国との国際連携・協力が重要。
- ❑ アクセス・無害化措置に当たっては、平素からの、また、サイバーに限られない情報収集が重要。関係機関等による多様な機能・能力を活用すべき。
- ❑ 強度の高い措置の実施に際しては、国内法的な文脈のみならず政治、外交など他の枠組の活用可能性を追求し、それを踏まえた総合的判断が必要であり、司令塔の存在が極めて重要。
- ❑ アクセス・無害化措置を実施する体制構築には、様々な分野における高い専門性を有する専門家が必要。そのためにも人材の教育、登用、待遇、官民交流を含めた全体のシステムに配慮すべき。

IV.横断的課題

(サイバーセキュリティ戦略本部の在り方、政府等での対策強化、人材育成ほか)

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

- ❑ 事案発生時の役割や基本的な方針等を決定する役割等を踏まえて、有識者等が助言をする別の組織を設けることを含め、サイバーセキュリティ戦略本部の構成の在り方等を検討すべきではないか。
- ❑ 関係省庁や地方公共団体等と戦略本部との役割分担や責任範囲を整理するとともに、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。

2. 重要インフラ事業者等の対策強化

- ❑ デジタル空間における位置づけ等を踏まえた重要インフラ分野の範囲等を検討すべきではないか。
- ❑ サービスの継続とサプライチェーンを含めたレジリエンス強化の観点を踏まえて、政府が普段から重要インフラ等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、必要な連携や優先度等を踏まえた対応ができるように備えるべきではないか。
- ❑ 基準・ガイドライン等の手法を活用し、分かりやすく取り組むべき事項の明確化が必要ではないか。
- ❑ 基準等については常に見直しを図るとともに、基準に対する取組状況を把握し、優れた取組を展開することを含め、実効性を高める仕組みを検討すべきではないか。

3. 政府機関等の対策強化

- ❑ 政府機関等のシステムに対する不正な活動を監視・制御する技術の導入や分析の向上等、政府機関等のサイバーセキュリティ水準を強固にするための取組を進めるべきではないか。
- ❑ 政府機関等の対策強化に当たっては、諸外国の取組を参考にするほか、国産セキュリティ製品・技術も活用していくべきではないか。

4. サイバーセキュリティ人材の育成・確保

- ❑ サイバーセキュリティに関わる人材は、技術者に限られるものではない。経営等に関わる者も含めた、広く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）付けや資格による可視化等を通じて育成・確保等を進めるべきではないか。
- ❑ 企業・組織からの視点だけでなく、現場に携わる人からの視点も取り込み、キャリアパスの明示、経営層の理解の促進等により、魅力あるキャリアとする方策についても検討すべきではないか。
- ❑ 人材の定義等の枠組みを通じ、産学官での人材交流・流動化を進めるべきではないか。また、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についても検討すべきではないか。

5. 中小企業を含めた対策強化

- ❑ 社会全体の強靱性を高める観点で、基幹インフラのサプライチェーンなど中小企業のセキュリティ対策について、ツールの提供などを含めた支援を検討すべきではないか。
- ❑ 大企業が下請け企業のセキュリティ対策を要請することに関して、サプライチェーンセキュリティに関する独占禁止法等の明確な整理を行うべきではないか。

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。
- ❑ 安全保障の観点から、国産のセキュリティ技術の育成・展開が重要であり、大学等で開発された技術等を活かしたエコシステムの構築を図るべきではないか。
- ❑ サイバーセキュリティ対策の重要性を広く理解いただくための取組が必要ではないか。