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

概　要

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

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

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**させるための**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４度の全体会議及び９度のテーマ別会合にて検討し、**提言とりまとめ**。

実現すべき具体的な方向性

（１）官民連携の強化

- **国家をも背景とした高度なサイバー攻撃への懸念の拡大**、デジタルトランスフォーメーションの進展を踏まえると、**官のみ・民のみでのサイバーセキュリティ確保は困難**。インフラ機能など社会全体の強靱性を高めるため、**産業界をサイバー安全保障政策の「顧客」としても位置づけ**、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。

- 高度な侵入・潜伏能力を備えた攻撃に対し事業者が具体的行動を取れるよう、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。情報共有枠組みの設置や、クリアランス制度の活用等により、情報管理と共有を両立する仕組みを構築すべき。

- これらの取組を効果的に進めるため、システム開発等を担う**ベンダとの連携を深める**べき。脆弱性情報の提供やサポート期限の明示など、**ベンダが利用者と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位置づけるべき。

- 経済安保推進法の**基幹インフラ事業者によるインシデント報告を義務化**するほか、その**保有する重要機器の機種名等の届出**を求め、攻撃関連情報の迅速な提供や、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。基幹インフラ事業者以外についても、インシデント報告を条件に情報共有枠組みへの参画を認めるべき。**被害組織の負担軽減と政府の対応迅速化**を図るため、**報告先や様式の一元化、簡素化**等を進めるべき。

（２）通信情報の利用

- **先進主要国は国家安保の観点からサイバー攻撃対策のため事前に対象を特定せず一定量の通信情報を収集し、分析**。我が国でも、重大なサイバー攻撃対策のため、一定の条件下での**通信情報の利用を検討すべき**。

- **国外が関係する通信**は分析の必要が特に高い。まず、①**外外通信(国内を経由し伝送される国外から国外への通信)**は**先進主要国と同等の方法の分析が必要**。加えて、 ②攻撃は国外からなされ、また、国内から攻撃元への通信が行われるといった状況を踏まえ、**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。

- **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は言えない**。**機械的にデータを選別し検索条件等で絞る等の工夫が必要**。

- **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。先進主要国を参考に明確で詳細なルールとなるよう考慮し、緻密な法制度を作るべき。その際、**取得及び情報処理のプロセス**について**独立機関の監督**が重要。

- なお、**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。その際、制度により、基幹インフラ事業者の協議の義務化等で、必要に応じ、同意を促すことが考えられる。

- 性質上**非公開とすべき範囲はある**が**適切な情報公開**は行われるべき。**公開困難な部分を独立機関の監督で補う**べき。

（３）アクセス・無害化

- サイバー攻撃の特徴（①危険の認知の困難性、②意図次第でいつでも攻撃可能、③被害の瞬時拡散性）を踏まえ、**被害防止を目的**としたアクセス・無害化を行う権限は、**緊急性を意識**し、**事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき**。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。その際、執行のシステム等を含め、従前から機能してきた**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**。

- 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サイバー攻撃の特性から、**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**とすべき。

- アクセス・無害化の措置の性格、既存の法執行システムとの接合性等を踏まえ、**権限の執行主体**は、**警察や防衛省・自衛隊**とし、その能力等を十全に活用すべき。**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が**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**。

- 権限行使の対象は、**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、事態発生時等に自衛隊等の活動が依存するインフラ**等へのサイバー攻撃に重点を置く一方、**必要性が認められる場合に適切に権限行使できる仕組み**とすべき。

- 国際法との関係では、他国の主権侵害に当たる行為をあらかじめ確定しておくことは困難。他国の主権侵害に当たる場合の違法性阻却事由としては、実務上は対抗措置法理より**緊急状態法理の方が援用**しやすいものと考えられるが、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を検討すべき。

（４）横断的課題

- 脅威の深刻化に対し、**普段から対策の強化・備えが重要**であり、**サイバーセキュリティ戦略本部の構成等を見直す**とともに、NISCの発展的改組に当たり政府の司令塔として強力な情報収集・分析、対処調整の機能を有する組織とすべき。

- 重要インフラのレジリエンス強化のため、行政が達成すべきと考える**セキュリティ水準を示し、常に見直しを図る制度**とするとともに、政府機関等についても**国産技術を用いたセキュリティ対策を推進**し、**実効性を確保する仕組み**を設けるべき。

- 政府主導でセキュリティ人材の定義の可視化を行い、関係省庁の人材の在り方の検討を含め、非技術者の巻き込みや人材のインセンティブに資する**人材育成・確保の各種方策を自ら実践**しながら、**官民の人材交流を強化**すべき。

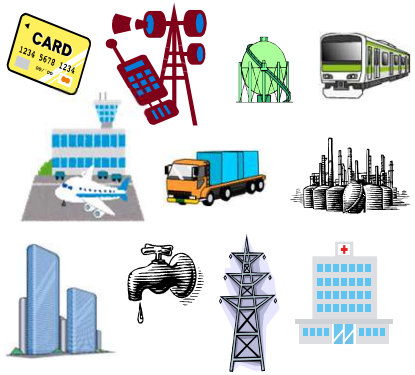
- サプライチェーンを構成する中小企業等のセキュリティについて、意識啓発や支援拡充、対策水準等を検討すべき。

【参考】全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築

守る対象（例）

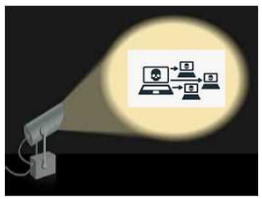


情報窃取

Internet

攻撃サーバ

通信事業者



通信情報の利用
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を利用

機能停止

官民連携の強化
官民の情報共有により、事案の未然防止、対処支援強化を図る

アクセス・無害化措置
確認された攻撃サーバ等に対し、 必要に応じ無害化

政　　府