「サイバーセキュリティ戦略」(案)概要

資料 2-1

1. 環境の変化

サイバー空間と実空間の「融合・一体化」
► 情報通信技術の普及・高度化・利活用の進展

サイバー空間を取り巻く「リスクの深刻化」
► リスクの甚大化・拡散・グローバル化

2. 基本的な方針

(1) 目指すべき社会像:「サイバーセキュリティ立国」の実現

国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、
「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、
サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現

(2) 基本的な考え方

① 情報の自由な流通の確保 ► 表現の自由やプライバシーの保護等が確保され、経済成長等を享受
② 深刻化するリスクへの新たな対応 ► リスクの変化に迅速・的確に対応できる多層的な取組が必要
③ リスクベースによる対応の強化 ► 動的対応力を通じ、リスクの性質を踏まえた対応の強化が必要
④ 社会的責務を踏まえた行動と共助 ► 多種多様な主体が各々の役割を発揮し、相互連携・共助が必要

(3) 各主体の役割

① 国 ► サイバー空間の外交・防衛・犯罪対策、政府機関等における対策強化・対処態勢整備 等
② 重要インフラ事業者等 ► 現行10分野の取組強化、新たな分野における必要な対策の実施 等
(10分野:情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む)、医療、水道、物流)
③ 企業や教育・研究機関 ► 情報共有等の集団的対策、産学連携による高度技術・人材の供給 等
④ 一般利用者や中小企業 ►「他者に迷惑かけない」認識醸成やリテラシー向上など自律的取組、情報共有 等
⑤ サイバー空間関連事業者 ► 製品等の脆弱性への対応、インシデント認知・解析、国際競争力の強化 等

3. 取組分野

2015年度までの3年間、以下に掲げる取組を実施。

(1)「強靱な」サイバー空間の構築

※GSOC: Government Security Operation Coordination team
CSIRT: Computer Security Incident Response Team
CYMAT: Cyber Incident Mobile Assistant Team

① 政府機関等における対策：情報システム等に関する対策及びサイバー攻撃への対処態勢を一層強化

例
- 政府共通プラットフォームによる情報システムのクラウド化、技術標準化等を通じ、攻撃等に強いシステム基盤構築。
- 国家機密等に関する情報及び情報システムの重要度等に応じてセキュリティ対策を重点化。
- 国の安全に関する重要な情報の国以外の事業者による取扱い、独立行政法人等におけるセキュリティ強化。
- GSOCを抜本的に強化し、監視対象を拡大するとともに、インシデント情報を効果的に収集・活用。
- CYMAT、CSIRT等の間の連携強化により、政府内におけるインシデント情報共有・即応体制を一層強化。
- 大規模サイバー攻撃事態等を想定した対処訓練を毎年度実施するなど対処態勢を強化。

② 重要インフラ事業者等における対策：政府機関等における対策に準じた取組

例
- 重要インフラ事業者等とサイバー空間関連事業者との間の、攻撃情報等の情報共有を促進。
- GSOCが保有するインシデント情報等を重要インフラ事業者等と共有するための仕組みを整備。
- 重要インフラの範囲及び対応の在り方等を検討し、対策をとりまとめた新たな「行動計画」を策定。

③ 企業・研究機関等における対策：インシデントの認知・情報共有の強化、CSIRT構築促進や演習等

例
- セキュリティ投資促進のためのインセンティブ検討等により、中小企業等におけるサイバー攻撃認知機能等を強化。
- 演習用テストベッドを利用した実践的な防御演習等により、企業等におけるサイバー攻撃への対応能力を向上。
- 企業・研究機関等のCSIRT構築促進・連携強化を図り、インシデント発生時の対応能力を向上。

④ サイバー空間の衛生：個々の主体による対策に加え、社会全体が参加した予防的対策実施

例
- 「サイバー・クリーン・デー」（仮称）の新設などサイバー空間の衛生確保を国民運動化。
- 悪性サイトにアクセスしようとする一般利用者に対するISP等による注意喚起等を行うための仕組みを構築。
- セキュリティ目的の通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方を検討。

⑤ サイバー空間の犯罪対策：　対処能力強化や民間事業者等の知見の活用等による対処態勢強化

例
- 日本版NCFTAの創設、アンチウイルスベンダーとの情報共有枠組みの構築等の取組を強化。
- サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討。

※NCFTA: National Cyber-Forensics and Training Alliance

(1)「強靭な」サイバー空間の構築 ［続き］

⑥ サイバー空間の防衛：国家レベルのサイバー攻撃から我が国に係るサイバー空間を守るための対応強化

例
- 重要インフラ等の情報システムに対する攻撃における自衛隊など非常時における関係機関の役割を整理し、必要な体制・機密情報等の共有システムや制度の整備等を行うとともに、個別具体的な国際法の適用も併せて整理。
- 武力攻撃の一環としてサイバー攻撃が行われた場合に対処する任務を負う自衛隊等の能力・態勢等を強化。

(2)「活力ある」サイバー空間の構築

① 産業活性化：海外製品等への依存度が高い我が国のサイバーセキュリティ産業の国際競争力強化

例
- 国際標準化や評価・認証の国際的な相互承認枠組み作りに積極的に関与するとともに、産業制御システムの評価・認証機関を設立。
- 新たな技術が採用された製品等の政府による積極的な調達。

② 研究開発：リスクの変化に適切に対応できる、創意と工夫に満ちたセキュリティ技術の創出

例
- サイバー攻撃の検知や高度解析等の向上に向けた技術の研究開発等を加速させ、最先端の研究開発を保持・向上。
- 潜在型マルウェア等多様・高度化するサイバー攻撃に対し、有効な革新的技術を確立するため、先端技術を開発。

③ 人材育成：高度かつ国際的なセキュリティ人材の育成

例
- ソフトウェア関連分野における優れた個人を発掘等するための合宿研修や実践的技能を競うコンテスト等を官民で連携実施。
- グローバルに活躍できる人材の育成等のため、国際会議への参加や海外の専門大学院等への留学を支援。

④ リテラシー向上：一般国民のリテラシーの向上

例
- 初等中等教育において、情報セキュリティを含む情報モラルやソフトウェアのプログラミングに関する教育、デジタル教科書の活用など実践的な取組を推進。高齢者に対するセキュリティ啓発のためのサポーター等を育成・活用。
- スマートフォンのアプリについて、一般利用者がリスクを認知し、利用等の判断を行う自ら行える仕組みを構築。

(3)「世界を率先する」サイバー空間の構築

① 外交：基本的な価値観を共有する国等とのパートナーシップ関係の多角的構築・強化

例
- サイバー空間を利用した行為に対する国連憲章や国際人道法等の個別具体的な国際法の適用について引き続き検討。
- 米国等との間で、サイバー領域での具体的対処の在り方、国際的なルール作りといった分野における議論を深化。

② 国際展開：ASEAN等とともに成長できる関係を構築し、サイバー攻撃への対応能力構築の支援

例
- 諸外国と連携してサイバー攻撃に関する情報収集ネットワークを構築し、攻撃の発生予知、即応等に関する研究開発を実施。
- 官民連携によるボットウイルス対策など国内における成功事例の紹介や共同プロジェクト、机上演習等を実施。

③ 国際連携：国境を越えるサイバー攻撃に関するインシデントへの対応・連携の強化

例
- 外国捜査機関等とのサイバー犯罪に係る情報交換を継続的に行うとともに、連携強化等のため、職員を派遣。
- 相互不信による不測事態回避のため、我が国の基本的な立場等を共有するとともに、インシデント発生した場合の相互の連絡体制等を平時から構築し、国際共同研究や複数国間におけるサイバー攻撃対応演習等を実施。

4. 推進体制等

- NISCについて権限等の必要な組織体制を整備し、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組・機能強化
- 政府機関や重要インフラ事業者等におけるサイバー攻撃関連情報の共有促進のための枠組み整備
- 取組を進めるにあたっての具体的な中長期（2015年度・2020年）の目標の管理

例
- 2015年度までに、政府機関等におけるサイバー攻撃関連情報の共有体制のカバー率向上、マルウェア感染率や国民の不安感の改善、国際インシデント調整の対応連携が可能な国等の３割増
- 2020年までに、国内の情報セキュリティ市場規模の倍増、セキュリティ人材の不足割合の半減

- 2015年度までの3年間を戦略の対象とし、年次計画の策定・評価等を実施
- 国際分野における総合的な対応を推進するための方針を策定