情報セキュリティ　アドバイザリーボード

資料3－2－7

課題
高度化・複雑化するサイバー攻撃の社会的な脅威の増大

ICT基盤の強化

Mission－使命
「みんなの安心を守る」
世界最高水準のサイバーセキュリティ環境を実現！

Vision －目標
Ⅰ. 動的防御プロセス連携の確立
Ⅱ. リスク認識に基づく対応の強化（事故前提社会）
Ⅲ. 国際連携によるサイバー空間政策の推進

取組の方向性

◇サイバーセキュリティの研究開発拠点（CYREC）の構築
◇悪性サイトへのアクセス等に対する注意喚起等の実施
◇ASEAN諸国等との共同プロジェクトの実施

「情報セキュリティ　アドバイザリーボード」では、情報セキュリティを取り巻く環境の変化に迅速かつ的確に対応するための取組の方向性として、「総務省における情報セキュリティ政策の推進に関する提言」（平成25年4月5日公表）を取りまとめ。

本提言の浸透

本提言に基づき、情報セキュリティ政策の基本的な考え方、方策等を情報セキュリティ政策会議（議長：内閣官房長官）に提案し、政府の基本戦略である「サイバーセキュリティ戦略（仮称）」（案）に反映。

「総務省における情報セキュリティ政策の推進に関する提言」
基本的な考え方
◇ 情報の自由な流通の確保、過度な規制によらない信頼できるサイバー空間の構築
◇動的防御プロセス連携を確立による適時適切な意思決定
◇ リスク認識に基づく対応の強化（事故前提社会）
◇国際連携によるサイバー空間政策の推進

反映

「サイバーセキュリティ戦略（仮称）」（案）
基本的な方針
◇ 情報の自由な流通の確保
◇ 深刻化するリスクへの新たな対応
◇ リスクベースによる対応の強化
◇ 社会的責務を踏まえた行動と共助

その他、情報セキュリティ対策の方策として、国際連携、官民連携、省庁間連携、個人や中小企業が自律的に対応を促す仕組み作り等が重要であることを提案し、これらについても具体的な取組として「サイバーセキュリティ戦略（仮称）」（案）に反映。

本提言に基づいた政策の推進

本提言に基づき、早期に実施可能な施策について速やかに着手。

○ 動的防御連携プロセスの確立
高度化・複雑化するサイバー攻撃に対応するために、国内の英知を結集したサイバーセキュリティの研究開発拠点（CYREC, Cybersecurity Research Center）を（独）情報通信研究機構に構築。平成25年4月より本格稼働。

○ 国際連携によるサイバー空間政策の推進
◇ 平成25年4月、新藤総務大臣がインドネシアを訪問し、「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議の開催」（平成25年9月予定）をはじめとした情報セキュリティ分野における両国間の協力について合意。
◇ 「日米サイバー対話」（平成25年5月　東京）として、日米のサイバー空間政策について政府一体となった最初の会合を実施し、サイバー空間での規範形成を含めた取組の共有と双方の連携を確認。

（参考）「総務省における情報セキュリティ政策の推進に関する提言」の概要（平成25年4月5日公表）

Ⅰ．情報の自由な流通の確保

人間の尊厳、自由、民主主義等の核心的な価値を推進するサイバー空間の構築による経済成長の促進。

Ⅱ．過度な規制によらない信頼できるサイバー空間の構築

イノベーションや経済成長を起こすサイバー空間の堅持。

Ⅲ．動的防御プロセス連携の確立

高度化・複雑化するサイバー攻撃に対応するためには、PDCAという一連のサイクルが終わる前に、常に、動的に、適時適切な意思決定を行うプロセスの構築が必要。

動的防御プロセス連携

それぞれのプロセスにおいて得られた知見を常時他のプロセスに反映

①モニタリング（検知・解析）（Observe）
◇継続的なモニタリングによるサイバー攻撃の検知
◇サイバー攻撃の目的・意図を判別するための情報収集

②情勢判断（Orient）
◇攻撃の目的・意図を識別した上で、自組織に対する影響を把握

③意思決定（Decide）
◇サイバー攻撃に対する措置に関する迅速かつ的確な意思決定

④行動（Act）
◇問題解決やリスク要因の排除の実施

総務省の取組

官民連携	悪性サイトの検知機能の強化	サイバー攻撃解析協議会による観測データ等の蓄積
国際連携	PRACTICE※1による諸外国とのサイバー攻撃情報の共有	
技術開発・人材育成	NICT「サイバー攻撃対策総合研究センター（CYREC※2）」による解析能力の向上	サイバー攻撃の防御モデルの確立・実践演習の実施※3

政府自身の防御体制の構築

- 政府情報システムの情報セキュリティ対策の強化。
- 職員訓練の充実。

※1　諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを国際的に構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験プロジェクト。

※2　Cybersecurity Research Center

※3　演習用テストベッドを利用した官民のLAN管理者等を対象に実践的な防御演習を実施。対象やその手法の提供等は、官庁・大企業にとどまらず、地方公共団体や中小企業に拡大。

Ⅳ．リスク認識に基づく対応の強化（事故前提社会）

自律的な対応を促す仕組みづくりの構築。

個人
- 通信事業者によるマルウェアの感染や悪性サイトへのアクセスに対する注意喚起等の実施。
- スマホのアプリについて、個人がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みの構築。

中小企業
- 情報セキュリティ投資促進税制等のインセンティブの検討。
- システムの共同利用など全体として低コストの情報セキュリティ対策の実現に向けた対策の推進。

Ⅴ．国際連携によるサイバー空間政策の推進

我が国の経済成長を見据えた戦略的な国際連携の推進。

グローバルなインターネット環境の安全の確保
- 共同プロジェクト推進等のASEAN諸国等との連携による情報セキュリティ環境の向上。

日本企業のグローバル展開への貢献
- 情報セキュリティの名の下で行われる過度な規制の撤廃に向けて省庁の枠を超えて連携。

国際的なサイバー空間の規範形成への主導的な取組
- 顔が見える外交を展開し、先導的に国際的なサイバー空間の規範形成をリード。