資料１－１

新たなサイバーセキュリティ戦略
～政府機関等のサイバーセキュリティ対策の抜本的強化～

平成27年8月

内閣官房内閣サイバーセキュリティセンター

政府機関等のサイバーセキュリティ対策の抜本的強化（1/3）

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、所要の法改正を含め、抜本的な強化を図る。

（注）「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に盛り込み、積極的かつ総合的に推進する。

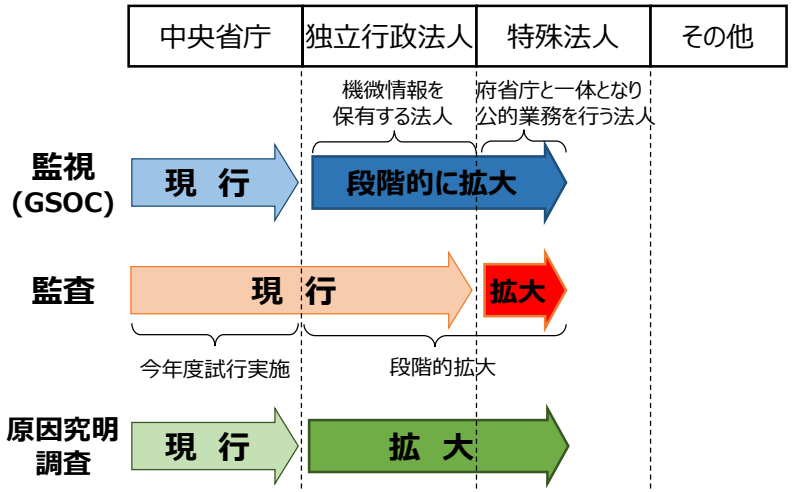
1．NISCの機能強化

■ GSOCの大幅な機能強化

- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化

■ 業務対象の拡大等

- 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大（所要の法改正について速やかに検討）



■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携（所要の法改正について速やかに検討）

■ NISCの要員強化

- 高度セキュリティ人材の民間登用等による対処能力の一層の強化

政府機関等のサイバーセキュリティ対策の抜本的強化（2/3）

２．政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対処に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

政府機関等のサイバーセキュリティ対策の抜本的強化（3/3）

3． その他の重要課題への取組強化

■ 重要インフラに関する取組強化（本年中を目途に具体策を決定）

- 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
- 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善

■ セキュリティ人材の育成のための演習環境の整備（本年度中に人材育成総合強化方針(仮称)を策定）

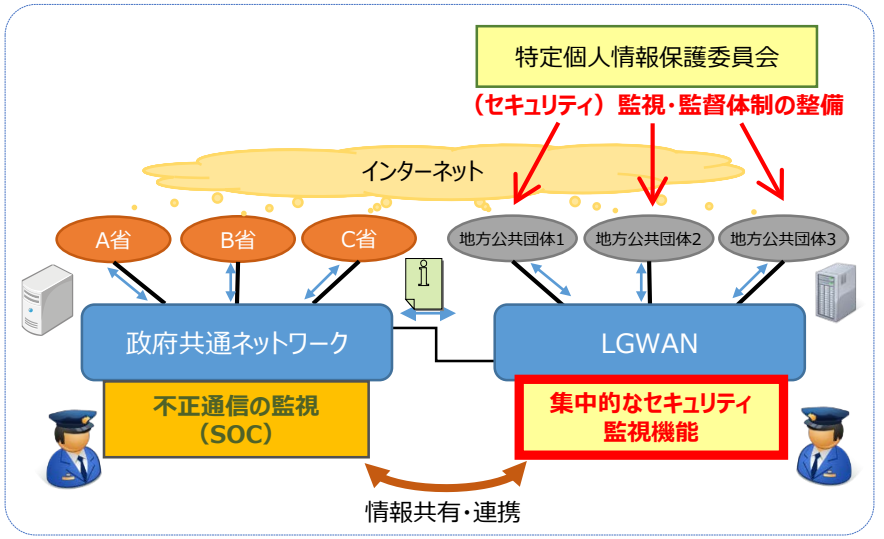
- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 即応予備チームの体制整備

- 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備（法改正について速やかに検討）

■ マイナンバー制度の円滑な導入に向けた対策の強化

- 特定個人情報保護委員会において、関係機関と連携して監視・監督体制を整備（本年度中を目途）
- 総合行政ネットワーク（LGWAN）について集中監視機能を設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知体制を整備
- 官民連携を実現する認証連携のための枠組みの取組方針を策定（本年中を目途）



■ 事案対処に関する取組強化

- サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
- 対処機関における能力の質的・量的向上