政府機関の情報セキュリティ対策の強化に関する基本方針

平成１７年９月１５日
情報セキュリティ政策会議決定

１　基本認識

（１）現状認識

産業・経済活動から行政上の諸活動、国民生活に至る様々な分野において、情報技術に支えられた社会基盤が厚みを増しているが、今後、この社会基盤が健全に発展していくためには、その安全性及び信頼性の確保・向上が不可欠である。

こうした中、昨今、政府機関に対するサービス不能攻撃（ＤｏＳ攻撃）、国民生活及び社会経済活動の基盤である重要インフラにおける IT 障害や、民間事業者におけるインターネットを介した個人情報等の重要情報漏洩の発生等、様々な問題が増大する傾向にあるが、これら情報セキュリティに対する脅威の増大に対して、社会の至るところで、情報セキュリティ対策は質的にも量的にも拡充・強化が避けられない状況となっている。

重要インフラの一つである政府・行政サービスについて見れば、政府機関が有する各情報システムが取り扱う情報には、国家として高い機密性を有する情報を始め、国民や企業に関する情報等、その漏えい、改ざん又は破壊等が発生した場合には極めて重大な結果を招くおそれがあるものが多数含まれている。また、長時間のシステム停止があってはならない情報システムもあり、政府機関の情報セキュリティの確保は、個人の権利・財産の保護から、経済活動、行政機能の維持、さらには安全保障に至る様々な分野に関係する重要課題であるといえる。

（２）政府の取組みの現状と課題

政府機関の情報セキュリティ対策については、平成 12 年 7 月 18 日に情報セキュリティ対策推進会議が決定した「情報セキュリティポリシーに関するガイドライン」（以下「旧ガイドライン」という。）に基づき、各府省庁（内閣官房、内閣法制局、人事院及び公正取引委員会を含む。以下同じ。）がそれぞれ自らの責任において独自に情報セキュリティポリシーを策定し対策を実施してきた。これにより、情報セキュリティに関する意識の定着と、各府省庁の情報セキュリティ水準の向上という点で一定の成果を挙げているが、旧ガイドラインは各府省庁において実際に実施される対策の整合化・共通化を目指したものではないことから、現状では、各府省庁の対策内容及びその水準はまちまちである。また、情報セキュリティに関する専門家が各府省庁においても極めて不足していることもあって、政府機関全体として十分な情報セキュリティ水準が確保されているとは言い難い状況にある。

このような状況を踏まえて、政府機関全体としてより高い情報セキュリティ水準を確保するための取組みを進めるためには、各府省庁のより一層の協力体制を前提とした情報セキュリティ対策の枠組みを構築することが必須となっている。具体的には、まず、各府省庁における情報セキュリティ水準の斉一的な引上げを図るため、各府省庁が行うべき情報セキュリティ対策の統一的な基準（以下「政府機関統一基準」という。）を策定し、各府省庁の特性を踏まえつつ、各々の対策を講ずることが必要である。さらに、各府省庁が共同で行うべき対策等も充実させ、政府機関全体として対策レベルの向上に努めるべきである。

政府機関の情報セキュリティ対策をこのような協力枠組みで進めていく場合、政府機関以外の者との関係も重要である。すなわち、政府機関の情報システムは電子申請等の仕組みを通じて民間、地方公共団体及び独立行政法人とも接点を持つことから、それらに対する関係に配慮し、またそれらに対する範となる対策であることが求められる。また、今日では、一般的に政府機関と民間はともに情報セキュリティの観点から見れば類似のシステムを運用していることからも、政府機関の情報セキュリティ対策は政府機関以外の者にとって参照する価値があることが求められる。このことは、さらに、世界最先端のＩＴ（情報技術）国家の実現に向けた取組みの一環という視点で考えれば、国際的に意義のある取組みとすべきである。

２　対策強化のための基本方針

１の基本認識を踏まえ、政府の情報セキュリティ政策の一環として、各府省庁は以下に示す統一的・横断的な情報セキュリティ対策を推進することにより、政府機関全体として高いレベルで水準のそろった情報セキュリティを確保し、もって国民が信頼できる電子政府の実現及び継続的かつ安定的な行政機能の維持に努めることとする。

（１）政府機関統一基準の策定

各府省庁は、情報セキュリティ対策の整合化・共通化を促進することとする。情報セキュリティ政策会議（以下「政策会議」という。）は、このために必要な政府機関統一基準について定め、以後、技術や環境の変化を踏まえ、毎年その見直しを行うものとする。

（２）各府省庁での情報セキュリティポリシー等の見直し

各府省庁は、自らの組織の情報セキュリティ対策について責任を持って取り組むことを原則としたうえで、政府機関統一基準を踏まえ、現行の情報セキュリティポリシー及び情報システム関係実施手順等について必要な見直しを行うことによって、政府機関全体として整合性のある情報セキュリティ対策を促進する。

（３）各府省庁での自己点検等

各府省庁は、情報セキュリティ対策の実施状況を自ら定期的に検査し、必要に応じて、対策の改善を行う。

（４）政府全体でのＰＤＣＡサイクルの確立

内閣官房情報セキュリティセンター（以下「センター」という。）は、各府省庁の対策の実施状況を、政府機関統一基準に基づき、必要な範囲で検査し、評価する。これをもとに、政策会議は各府省庁の対策の改善を勧告し、政府機関統一基準等の改善に結びつけることで、政府全体としての PDCA サイクル(Plan・Do・Check・Act サイクル)を確立する。

（５）情報セキュリティ確保に有効な制度等の活用の促進

各府省庁は、安全な情報システムの構築を推進するため、客観的に評価された暗号・製品等の導入、外部監査の実施、外部委託先の情報セキュリティ管理体制の確認等情報セキュリティ確保のために必要な措置を講ずる。また、センターは、各府省庁におけるこれらの取組みを促進する。

（６）独立行政法人等のセキュリティ対策の改善

各府省庁は、政府機関統一基準を踏まえ、所管の独立行政法人等の情報セキュリティ水準の向上を促進する。

（７）新たな脆弱性等に対するセンターと府省庁との連携

センターは、政策会議庶務協力省庁及び重要インフラ所管省庁との日常の連絡を強化し、新たな脆弱性等の情報を把握し、それら脆弱性等と収集した攻撃情報等を分析し、各府省庁に適宜適切な情報提供を行う。

（８）情報セキュリティ人材の育成の支援・促進

センターは、政府機関の情報セキュリティ対策を円滑に推進していく上で必要な情報セキュリティ知識のある職員が政府機関全体として著しく不足している状況にかんがみ、職員の人材育成・人材確保のため支援を行うとともに、希望する各府省庁に対し、情報システム構築段階等における情報セキュリティ面からの設計支援を行う。

（９）その他、政府全体での中長期的な対策の強化

上記各項のほか、センターは、情報セキュリティに関する要求仕様の共通化、年度途中での緊急事態対応に向けた取組み等、政府機関が全体として協力して行うべき情報セキュリティ対策の実施を図る。

上記のうち、（１）から（４）の対策については、各府省庁がセンターと協力して総合的かつ体系的に行うことが必要であるため、政策会議は指針を策定して実施枠組みを明確にするものとする。