資料 1-3

政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（案）

平成 17 年９月 15 日
平成 21 年２月３日改定
平成 22 年５月 11 日改定
平成 23 年４月 21 日改定
平成 24 年４月 26 日改定
平成 26 年　月　日改定
情報セキュリティ政策会議決定

目次

１　本指針の位置付け等

１－１　本指針の位置付け

本指針は、「政府機関の情報セキュリティ対策のための統一規範」（平成 23 年４月 21 日情報セキュリティ政策会議決定。以下「政府機関統一規範」という。）に基づき別に定める「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（平成 26 年○月○日情報セキュリティ政策会議決定。以下「政府機関統一基準」という。）の策定及びその運用等のために必要な事項について示すものである。

１－２　本指針における用語の意義

本指針における用語の意義は、政府機関統一規範に定める用語のほか、それぞれ次に定めるところによる。

(1) 「情報セキュリティマネジメント」とは、組織の取組の方針に基づいて、情報セキュリティ対策の導入・計画、運用、点検及び見直しを行うことをいう。

(2) 「対策基準策定ガイドライン」とは、各府省庁が政府機関統一基準に準拠した府省庁対策基準を策定するために参照するガイドラインをいう。

(3) 「政府機関統一基準群」とは、政府機関統一規範、本指針、政府機関統一基準及び対策基準策定ガイドラインの総称をいう。

(4) 「実施手順」とは、府省庁対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

(5) 「政府機関統一基準適用個別マニュアル群」とは、各府省庁が実施手順等を作成する際に参考とするため、内閣官房情報セキュリティセンター（National Information Security Center、以下「NISC」という。）が策定する文書の総称をいう。

２　政府機関の情報セキュリティ対策の在り方

２－１　府省庁における情報セキュリティ対策の進め方

(1) 情報セキュリティマネジメントの進め方

府省庁における情報セキュリティの確保については、国民、企業等からの情報セキュリティ確保に関する要求や期待を踏まえた上で、自らが取り扱う情報の管理に責任を持ち、それぞれの業務や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則である。

各府省庁は、この原則に基づき、情報セキュリティ対策を適切に推進するため、以下の観点を踏まえた情報セキュリティマネジメントを行う。

・最高情報セキュリティ責任者の指揮

府省庁に、府省庁ポリシーの策定及び運用その他の情報セキュリティの事務を統括するとともにその責任を負う者として、最高情報セキュリティ責任者を置く。

最高情報セキュリティ責任者は、府省庁における情報セキュリティ対策の推進を指揮し、その方向性を明確化するとともに、情報セキュリティ対策に必要な人員・予算等の資源配分の方針を決定する。

・情報セキュリティ対策の推進のための組織・体制の確立

情報セキュリティ対策を効率的かつ実用的に推進するためには、取り扱う情報や業務、組織等の特性を踏まえる必要があることから、各府省庁において部門横断的に取り組むことが重要である。

したがって、府省庁対策基準その他の情報セキュリティに関する重要な事項の審議や報告等を行うため、府省庁の情報セキュリティを推進する部局及びその他の部局の代表者を構成員とする委員会等の組織を設ける。

(2) 情報セキュリティ対策の実施

各府省庁は、組織として意思統一して情報セキュリティ対策を実施するため、各府省庁において府省庁ポリシーを策定するとともに、その適切な運用に努め、一定のセキュリティ水準を確保する。また、重要な業務、情報等に対しては詳細にリスクを把握した上で対策を講ずる。

なお、リスクを把握し、情報セキュリティ対策を実施する手法について、政府機関において適用されているガイドライン等が存在する場合は、それらに沿って実施することが求められる。

(3) 複数の府省庁で共通的に使用する情報システムにおける情報セキュリティ対策の進め方

複数の府省庁で共通的に使用する情報システム（一府省庁でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）については、これを使用する各府省庁の情報システムと連携して運用管理を行うものであることから、府省庁の間での情報セキュリティ対策の遺漏防止を図る必要がある。また、基盤となる情報システムと連携する一部の情報システムにおける情報セキュリティインシデントが他の情報システムに影響を及ぼす可能性等も踏まえ、情報セキュリティマネジメントを適切に実行し、情報システム全体としての情報セキュリティ水準を適切に確保しなければならない。

このため、基盤となる情報システムを整備し、運用管理を行う府省庁及び基盤となる情報システムと連携する情報システムを管理する府省庁（以下「整備・運用管理府省庁」という。）は、基盤となる情報システムの運用管理を行う体制を整備するに当たっては、各府省庁の責任と役割分担を明確化するとともに、情報セキュリティ対策を確実かつ迅速に調整・実施できる体制にする必要がある。

また、整備・運用管理府省庁は、基盤となる情報システムの情報セキュリティを確保するための方策等について包括的に定めた文書を整備するに当たっては、各府省庁の府省庁ポリシーとの関係について検討し、適切な運用管理が行われるよう、以下の事項等を整理するものとする。

・各府省庁間の責任分界
・平常時及び非常時の協力・連携体制
・非常時の具体的対応策　等

以上の検討・実施に当たっては、府省庁間での十分な合意形成を図るとともに、情報セキュリティ対策の円滑かつ迅速な実施に支障を来さないように留意する必要があ

る。

なお、基盤となる情報システムの情報セキュリティ対策を共通的に行うため、基盤となる情報システムを整備し、運用管理を行う府省庁は、当該基盤となる情報システムと連携する情報システムを管理する府省庁と協議の上、基盤となる情報システムの情報セキュリティについて、各府省庁が定める府省庁ポリシーの定めにかかわらず、府省共通的な規程を定めることができるものとする。

２－２　政府機関全体としての情報セキュリティ対策の進め方

情報セキュリティ対策は、一過性のものではなく、継続的な取組が必要であることから、客観的に比較検証することが可能な判断基準による点検を実施することが重要である。

情報セキュリティ対策の実施状況の点検は、各府省庁の責任において行われることが原則であるが、政府機関全体として、これを更に効果的かつ効率的に実施するため、NISC は、政府機関統一基準群に基づき各府省庁が定める情報セキュリティ関係規程等の整備状況及び対策の実施状況並びに各府省庁の情報セキュリティマネジメントの状況について、総合的、客観的及び統一的な視点で、定期的に、又は必要に応じて点検を実施する。また、NISC は、これら点検により情報セキュリティ対策の実施等に係る課題を把握し、それを踏まえて政府機関全体の取組について、今後の方向付けや改善を行う。

なお、各府省庁は NISC が行う政府機関全体の点検に協力することとし、NISC は、当該点検の結果及び今後の取組の方向性を取りまとめ、情報セキュリティ政策会議に報告後、その概要を公表するものとする。

２－３　情報セキュリティインシデントの対応

(1) 情報セキュリティインシデントの情報共有

情報セキュリティインシデントに対し、政府機関全体として迅速かつ的確に対処するためには、情報セキュリティインシデントに関する情報が府省庁内外の関係部門と適時・適切に共有されることが重要である。

そのため、各府省庁は、情報セキュリティインシデントの認知時には、当該情報セキュリティインシデントに係る情報を速やかに NISC に連絡するとともに、平時においても、収集した情報セキュリティインシデントに関する情報を NISC に連絡する。NISC は、平時から各府省庁や外部の関係機関との情報共有の結節点となり、収集・集約された情報を情報セキュリティインシデントに対する被害の未然防止又は拡大防止、応急措置・復旧のための措置及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う。

(2) 情報セキュリティインシデントの対処

各府省庁は、情報セキュリティインシデントの認知時には、自らが設置した CSIRT（Computer Security Incident Response Team の略であり、府省庁において発生した

情報セキュリティインシデントに対処するため、当該府省庁に設置された体制をいう。以下同じ。）を中心として、早急にその状況を確認し、被害の拡大防止、応急措置・復旧のための措置を講ずる。

NISC は、各府省庁における情報セキュリティインシデントへの政府一体となった対応の中核となる機関として、各府省庁間の連携・調整を行う。また、CSIRT の能力向上の支援等、各府省庁へ技術的な支援及び助言を行い、各府省庁の求めに応じて情報セキュリティ緊急支援チーム（Cyber Incident Mobile Assistance Team（CYMAT））による支援を行う。

３　府省庁における情報セキュリティマネジメント

３－１　導入・計画

(1) 府省庁基本方針の策定

各府省庁は、情報セキュリティ対策の目的、対象範囲等、情報セキュリティに対する基本的な考え方を示した府省庁基本方針を定める。

府省庁基本方針の策定に当たっては、対象となる情報、情報システム、組織（者）、場所・区域の範囲及びその境界について、外部委託の観点も含めて明確にするとともに、対象範囲外においては、他の主体により情報セキュリティ対策が講じられていることを確認するなどにより、その境界が妥当であることを確認することが重要である。

なお、府省庁基本方針は、情報セキュリティに対する基本的な方向性を決定付けるものであることから、頻繁に更新される性質のものではないことに留意する必要がある。

(2) 府省庁対策基準の策定

各府省庁は、府省庁基本方針に基づき、政府機関統一基準に準拠して府省庁対策基準を定める。府省庁対策基準には、政府機関統一基準の規定を遵守するための対策事項について、対策基準策定ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて検討の上、定めることとする。また、脅威の変化等に迅速に対応するために政府機関共通の情報セキュリティ対策が個別に決定されている場合にはそれを反映する。

(3) 対策推進計画の策定

各府省庁は、最高情報セキュリティ責任者の指揮の下、情報セキュリティに係るリスク評価の結果を踏まえ、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を策定する。対策推進計画は、教育訓練、情報システムに対する技術的な対策を含め、各府省庁における情報セキュリティに関する一連の取組を俯瞰（ふかん）できるものとする。

３－２　運用

各府省庁は、対策推進計画に基づき、行政事務従事者に対する教育訓練を実施し、府省庁ポリシーの浸透を図るとともに、情報システムに対する技術的な対策を強化するなど、情報セキュリティに関する取組を実施する。

３－３　点検・見直し

各府省庁は、対策推進計画に基づく取組について、年度ごとに実施状況を把握し点検するとともに、必要に応じて見直しや改善を行う。

各府省庁は、情報セキュリティ対策について、その適正性を確保するため、情報セキュリティ対策の実施状況、効果及び対策実施の結果としての情報セキュリティの状態を点検することが必要である。

なお、点検は客観的な視点から行なわれていると認められることが重要であり、このため点検対象の部門や者から独立した組織又は部門による監査を含めることが必要である。

点検の結果、求める情報セキュリティ水準が達成されていないと判断された場合又は情報セキュリティ対策の実施状況や効果が不十分であると判断された場合は、それについて、再発防止を考慮した改善を実施しなければならない。改善においては、府省庁対策基準等の改正、教育による府省庁対策基準等の周知徹底、情報システムや機器の更新、情報セキュリティの重要性に係る啓発等の措置を講ずることとなる。改善措置の結果については、意図した目的が達成されていることを確認する必要がある。

最高情報セキュリティ責任者は、対策推進計画に照らして自府省庁の情報セキュリティマネジメントの状況を総合的に評価し、情報セキュリティに係る取組をより一層推進するため、今後の情報セキュリティマネジメントの方向性、資源配分の見直しを行う。

３－１から３－３に掲げる府省庁における情報セキュリティマネジメントの全体像について、２－２及び２－３に掲げる政府機関全体の取組と合わせて図１に示す。

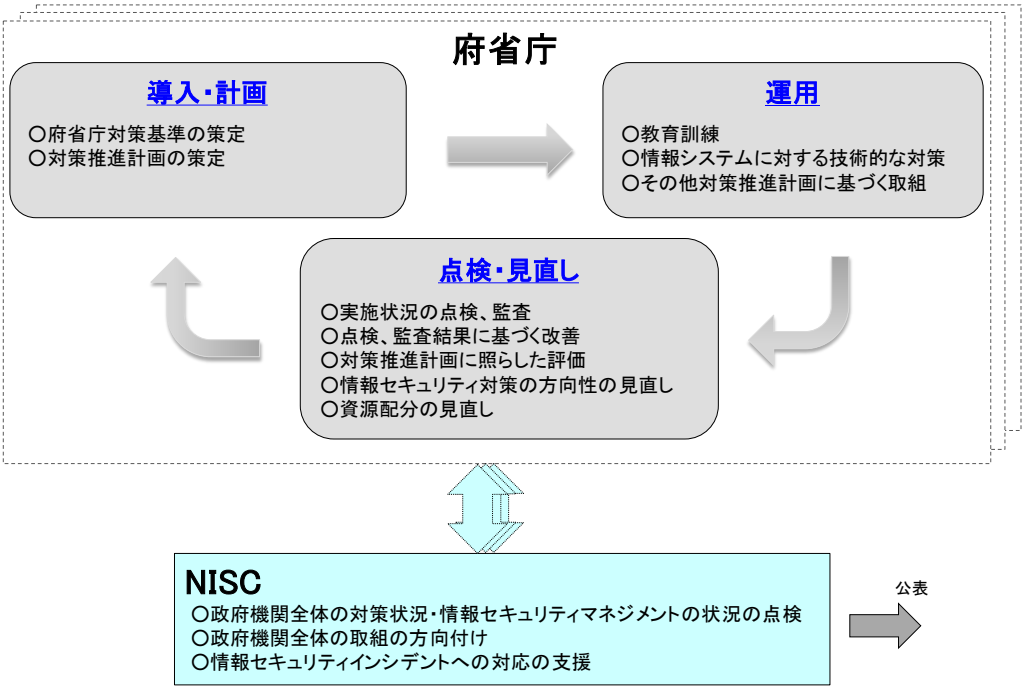

図１　府省庁における情報セキュリティマネジメントの全体像

４　政府機関統一基準に関する取組

４－１　政府機関統一基準の策定等

政府機関統一基準の原案はNISCが策定し、情報セキュリティ政策会議において決定する。また、新たな脅威の発生や府省庁における運用の状況を定期的に点検した結果を踏まえて、必要に応じて改訂を行う。

なお、NISCは、政府機関統一基準の策定又は改訂に当たっては、次の点に留意する。

(1) 政府機関統一基準は、原則として、全ての府省庁において共通的に必要とされる情報セキュリティ対策を包含するものとして策定する。

(2) 政府機関統一基準は、責任体制、実施体制及び対策内容について、各府省庁が準拠できるように、各府省庁の実状を踏まえて策定する。

(3) 政府機関統一基準は、国際的な基準等との整合性に配慮して策定する。

４－２　対策基準策定ガイドラインの策定等

対策基準策定ガイドラインは、各府省庁において府省庁対策基準を策定する際に参照すべきものとして、脅威の変化、技術の進歩等を踏まえ、各府省庁と協議の上、NISCにおいて決定し改訂する。

４－３　政府機関統一基準適用個別マニュアル群の策定等

政府機関統一基準適用個別マニュアル群については、NISCが各府省庁と協力して策定する。また、当該マニュアル群は、新たな脅威の発生や各府省庁における運用の状況を

踏まえて、重要性及び緊急性の高い項目から優先的に作成又は改訂し、各府省庁に提供する。

附則　「情報セキュリティポリシー策定ガイドライン」（平成１２年７月１８日情報セキュリティ対策推進会議決定）は廃止する。