# 政府機関の情報セキュリティ対策における政府機関統一基準の策定と運用等に関する指針

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
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強化・拡充を図るため、「政府機関の情報セキュリティ対策強化に関する基本方針（平成１７年９月１５日付情報セキュリティ政策会議決定）」に基づき、政府機関が行うべき情報セキュリティ対策の統一的な基準を策定し、これを運用する上で必要となる事項を示すものである。

### １－２　本指針で使用する主要な用語の説明

本指針において次に掲げる用語の定義は、それぞれ次に定めるところによる。

(1) 「府省庁」とは、内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省をいう。

(2) 「情報セキュリティポリシー」とは、組織内の情報セキュリティを確保するための方針、方策及び体制等を包括的に定めた文書をいう。
(3) 「政府機関統一基準」とは、政府機関の情報セキュリティ対策の横断的な取組みの一環として、各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために、各府省庁が最低限行うべき情報セキュリティ対策を定めた政府の統一的な基準をいう。
(4) 「省庁基本方針」とは、各府省庁の情報セキュリティ対策の基本的な方針をいう。
(5) 「省庁対策基準」とは、政府機関統一基準に準拠した各府省庁のすべての情報資産に共通する情報セキュリティ対策の基準をいう。
(6) 「省庁基準」とは、各府省庁がそれぞれ策定する情報セキュリティポリシーであり、省庁基本方針と省庁対策基準からなる。
(7) 「実施手順」とは、省庁基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた文書をいう。
(8) 「統一基準個別ガイドライン群」とは、省庁基準に基づいて、各府省庁が実施手順を作成する際に参照すべきガイドラインの総称であり、原則として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。）が策定する文書をいう。

## ２　政府機関の情報セキュリティ対策の在り方

### ２－１　各府省庁の情報セキュリティ対策の進め方

各府省庁の情報セキュリティの確保については、自らの管理下にある情報資産に責任を持ち、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に、当該府省庁が有する情報資産に関して、個人的裁量でその扱いが判断されることのないように、組織として意思統一し、明文化された文書として省庁基準及び実施手順を策定し、当該規程の適切な運用に努める。

なお、各府省庁は、省庁対策基準を策定する際に、政府機関統一基準を踏まえ、記載内容に不備が生じないようにする必要がある。

また、センターは、各府省庁の実施手順策定に当たり、記載内容の不備の防止と策定作業の効率化に資するよう、各府省庁と協力して、統一基準個別ガイドライン群を策定する。

### ２－２　センターによる対策実施状況の検査と評価

情報セキュリティ対策の評価は、各府省庁の責任において行われることが原則であるが、政府として、これを更に効果的かつ効率的に実施し、政府機関全体としての情報セキュリティ水準の向上を図るためには、客観的に比較検証することが可能な判断基準による評価が重要である。

同時に、情報セキュリティ対策は、一過性のものではなく、遅滞なく継続的に取組みを実施できるものであることが重要である。

これらのことから、センターは、政府機関統一基準に基づき、各府省庁の省庁基準、実施手順及びその他の情報セキュリティ関係規程の整備状況並びに対策の実施状況を、総合

的、客観的、統一的な視点で、定期的に、又は必要に応じて検査及び評価を実施し、必要に応じて対策改善を促す。

なお、各府省庁は、センターが検査及び評価を実施する場合、これに協力する。

## ３　省庁基準に基づく情報セキュリティ対策

### ３－１　省庁基準に関する留意点

(1) 組織としてどのような基本方針の下に情報セキュリティを確保していくのかを明確にすること

情報資産がさらされている脅威（例えば、盗聴、侵入、改ざん、破壊、窃盗、漏えい、サービス不能攻撃等）から保護すべき情報資産を明らかにするとともに、情報資産ごとにその重要性、利用環境等を考慮した脅威（リスク）の分析を行う。その際保護すべきものとされた特定の情報資産と当該情報システムに要求される情報セキュリティの水準が、情報セキュリティ対策を考える基礎となる。

また、情報セキュリティ対策を講ずるための体制を確立し、情報システムを運用・管理する者、利用する者、当該情報システムの情報セキュリティ対策の責任者等、１つの情報システムに複数の者が関わることを十分認識した上で、それぞれの権限と責任の範囲を明確化することにより、組織として情報セキュリティ対策が適切に進められるようにする必要がある。

(2) 省庁基準に基づく情報セキュリティ対策の実施サイクルに従った間断ない取組みを行うこと

各府省庁にとって情報セキュリティ対策は、省庁基準を策定することによって完結する一過性のものではなく、省庁基準の策定及びそれに続く継続的な取組みによって意味をなすものである。したがって、図１に示す省庁基準に基づく情報セキュリティ対策の実施サイクルに従った間断ない取組みが必要である。このように、情報セキュリティの水準を適切に維持していくためには、策定した省庁基準を導入し、確実に運用していくとともに、その効果を的確に評価し、それに応じて省庁基準の見直しを図ることが重要である。

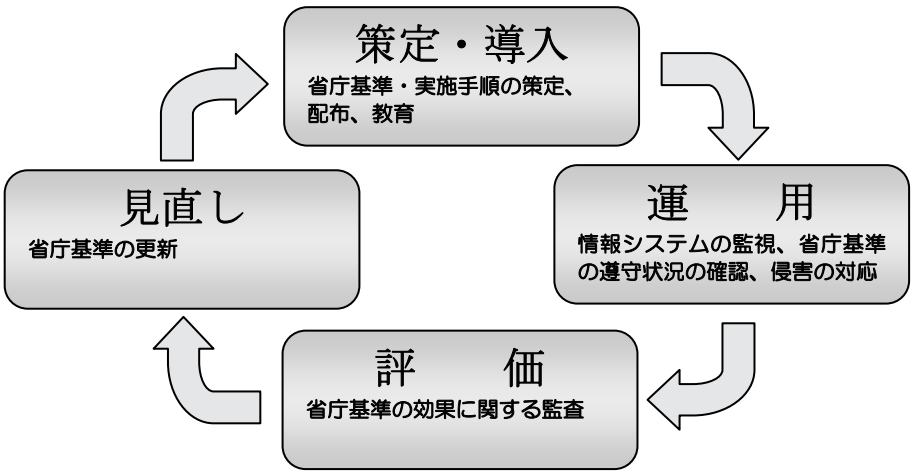


図１：省庁基準に基づく情報セキュリティ対策の実施サイクル

## ３－２　策定

省庁基準を策定する手続及び省庁基準に定めるべき事項の原則は次のとおりとする。

(1) 策定手続の概要

省庁基準は、図２に示すとおり、各府省庁において、①策定のための組織・体制を確立し、その組織・体制の下で、②省庁基本方針を策定し、③リスク分析に基づき、④対策基準の策定を行い、⑤各府省庁内において意思統一及び明文化するものとする。

また、各府省庁においては、それぞれの省庁基準に従い、⑥実施手順を策定することとなる。

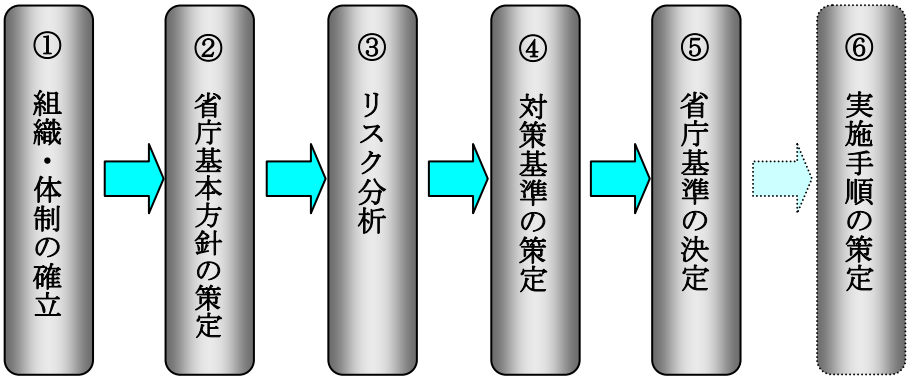


図２：ポリシー策定手続の概要

なお、策定した対策基準及び実施手順並びにリスク分析結果等の関連文書類は、攻撃者にとっての手掛かりとなり得る情報が含まれていることが多いため、その取扱いには注意が必要である。

(2) 策定のための組織・体制

情報セキュリティは各府省庁の責任において確保されなければならないものであり、組織横断的な取組みが必要であるため、省庁基準の策定には、幹部職員の関与が不可欠である。省庁基準の策定及び運用その他各府省庁の情報セキュリティの全体に対する責任の所在を明らかにするため、最高情報セキュリティ責任者を定め、必要に応じてその実務を行う者を任命することとする。効率的かつ実用的な省庁基準を策定するには、情報システムを運用する部門のほか、人事・会計部門等を含めた組織横断的な検討体制を確保するとともに、担当者だけではなく幹部職員で構成する委員会等の組織（以下「情報セキュリティ委員会」という。）を設ける必要がある。このため、省庁基準においては、情報セキュリティ委員会の目的、権限、名称、業務、構成員等を定める。

(3) 省庁基本方針の策定

各府省庁は、情報資産に求められる情報セキュリティの確保のため、情報セキュリティ対策の目的、対象範囲など、各府省庁の情報セキュリティに対する基本的な考

え方を示した省庁基本方針を定める。

なお、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。

(4) リスク分析

リスク分析とは、保護すべき情報資産を明らかにし、それらに対するリスクを評価することであり、図３に示すとおり、①情報資産の調査、②情報資産の重要性の分類、③情報資産を取り巻く脅威の調査、及び④脅威の発生頻度・発生時の被害の大きさの分析を行うことであり、これにより、⑤当該情報資産に要求される情報セキュリティ水準が設定される。適切な情報セキュリティ対策を実行するためには、各情報資産に要求される情報セキュリティ水準が的確に設定されることが重要であることから、リスク分析は、適切な情報セキュリティ対策に結び付くように確実に行われなければならない。

なお、情報資産に変更があったとき、又は情報資産を取り巻く脅威に変化が生じたときには、当該情報資産についてリスク分析を再度行い、その結果を踏まえ、必要に応じて省庁基準の見直しを行う。また、定期的な省庁基準の評価・見直しの際にも、必要に応じてリスク分析から見直す必要がある。また、リスク分析の際に発見された情報資産に対する情報セキュリティ対策の問題点のうち、早急に対応する必要のあるものについては、速やかに措置を講ずる必要がある。

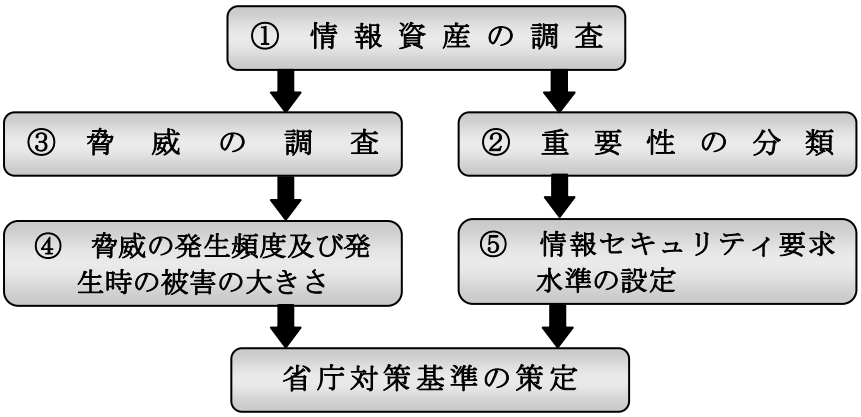


図３：リスク分析の手続

(5) 省庁対策基準の策定

リスク分析の結果に基づき検討した各情報資産に対する個々の情報セキュリティ対策について、省庁対策基準を定める。

なお、政府機関統一基準は、各府省庁に必要とされる情報セキュリティ対策を原則として包含する形で策定されるものである。このことは、専門的知識が必要とされる正確なリスク分析と対策の選定作業を、政府機関統一基準に準拠することで容易とする効果がある。

このため、各府省庁は、省庁基準を策定するに当たって、各情報資産の特質を踏まえ

た上で政府機関統一基準に準拠することとする。

(6) 省庁基準の決定

策定された省庁基準案については、情報セキュリティ分野の専門家による評価、関係部局の意見等を踏まえ、その妥当性を確認する手続を経ることが必要である。

省庁基準には、関係部局からの意見を反映させるための手続を定め、省庁基準の決定に当たっては、各府省庁としての意志決定を必要とすることを定める。

## ３－３　導入

(1) 実施手順の作成

実施手順においては、省庁基準に記述された内容を具体的な情報システムや業務においてどのような手順に従って実行するかについて定める。この実施手順は、省庁基準を遵守しなければならない者全員について、取り扱う情報、実施する業務、及び利用する情報システム等に応じて情報セキュリティを確保するために、何をどのようにすべきか、あるいは、何をしてはならないかを示すマニュアルに該当するものである。したがって、各府省庁は、統一基準個別ガイドライン群を参考にしながら、業務を実施する環境に応じて、情報システムごとに又は業務ごとに適切な実施手順の作成を行い、必要に応じて改訂することとする。

なお、実施手順については、対策基準に基づき個別の目的のために作成し、評価・見直しなどの実施サイクルを柔軟に行うことが有効であることから、情報セキュリティ委員会による承認を受けることなく、情報システムを管理する者等において策定、更新及び廃止することを可能とする必要がある。

(2) 省庁基準及び実施手順の周知

情報セキュリティ対策を実効性のあるものにするには、省庁基準を関係者に周知する必要がある。また、実施手順については、当該手順を実行する者に周知する必要がある。

外部委託業者等についても十分に該当部分を周知するとともに、省庁基準の遵守についてあらかじめ合意させることが必要である。

## ３－４　運用

省庁基準を確実に運用していくためには、そのための組織・体制を確立するとともに、省庁基準に従って対策が適切に遵守されているか否かを確認することが必要である。

また、情報セキュリティ侵害の発生に備えて、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直しを適切に実施する必要がある。

## ３－５　評価（監査）

各府省庁は情報セキュリティ対策を実施するに当たり、客観的な視点から省庁基準に基づいた対策が適切に行なわれていることが重要であり、このため監査、評価を適切に実施することが必要である。その場合、情報システムに係る技術的、物理的及び人的情報セキュリティに関する事項にとどまらず、それに関係する情報自体のセキュリティをも含む総合的な監査、評価を実施することが必要である。

外部の機関を活用して監査を行う場合、当該機関に情報システムの弱点が知られる危険を伴うことを十分留意した上、信頼性について慎重な検討を行い、機関の選定を行うことが必要である。

### ３－６　見直し

省庁基準の更新においては、省庁基準と実態との相違を十分考慮することが重要であることから、関係部局から意見聴取等を行い、実態把握を行うことが望ましい。また、省庁基準を更新する際には、必要に応じてリスク分析の見直しを行うなど、実態に即したものとすることが重要である。さらに、日頃から新たな攻撃方法の情報収集に努め、省庁基準の更新に活用することも必要である。

また、新たな省庁基準項目を策定した際には、その内容を周知徹底する必要がある。

なお、各府省庁は、各府省庁の情報セキュリティに係る検査・評価等の結果を踏まえて政府機関統一基準が見直された場合、これに即して省庁基準の見直しを行う必要がある。

## ４　政府機関統一基準に関する取組み

### ４－１　政府機関統一基準の策定と運用等

政府機関統一基準の原案はセンターが策定する。また、政府機関統一基準は、新たな脅威の発生や各府省庁における運用の結果を踏まえて、原則として毎年見直し、必要に応じ改訂を行う。

なお、政府機関統一基準の策定については、次の点に留意する。

(1) 政府機関統一基準は、各府省庁に必要とされる情報セキュリティ対策を原則としてすべて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、各府省庁が無理なく準拠できるよう、各府省庁の実情を踏まえて策定する。

(3) 政府機関統一基準の策定に当たっては、国際的な基準等との整合性に必要な配慮を払う。

### ４－２　統一基準適用個別ガイドライン群の策定と提供

統一基準適用個別ガイドライン群については、各府省庁が実際に省庁基準を適用する際に作成する文書（実施手順、規程及びマニュアル等）の参考となるものとして、センターが各府省庁と協力して策定する。また、当該ガイドライン群は、新たな脅威の発生や各府省庁における運用の結果を踏まえて、重要性かつ緊急性のある項目から優先的に作成又は改正し、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日付情報セキュリティ対策推進会議決定）は廃止する。