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管理基準及び政府機関統一技術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　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
　１－２　本指針で使用する主要な用語の説明
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
　２－２　複数の府省庁で共通的に使用する基盤とな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
　２－３　センターによる対策実施状況の検査と評価
　２－４　情報セキュリティに関する障害・事故等への対応
３　省庁基準に基づく情報セキュリティマネジメント
　３－１　省庁基準に関する留意点
　３－２　計画
　３－３　実施
　３－４　評価
　３－５　改善
４　政府機関統一管理基準及び政府機関統一技術基準に関する取組
　４－１　政府機関統一管理基準及び政府機関統一技術基準の策定と運用等
　４－２　政府機関統一基準適用個別マニュアル群の策定と提供

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のための統一規範」（平成 23 年４月 21 日付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、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、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関若しくはこれらに置かれる機関をいう。

(2)「情報」とは、情報処理及び通信に係るシステム（以下「情報システム」という。）内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。したがって、作業途上の文書も適用対象であり、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

(3)「情報資産」とは、組織における情報セキュリティ対策の対象となるものであり、次に掲げるものをいう。

（ア）情報

（イ）情報システム及び電磁的記録媒体等

（ウ）ソフトウェア

（エ）組織及び人

(4)「リスク」とは、不確かさによって結果が目的からかい離することでもたらされる影響をいう。起こり得る事象（周辺状況の変化を含む。）の結果とその起こりやすさとの組み合わせで表される。

(5)「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、情報セキュリティの計画、実施、評価及び改善を行うことをいう。

(6)「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。（図１を参照のこと。）

(7)「政府機関統一管理基準」とは、政府機関統一規範に基づき、政府機関の情報セキュリティ対策の横断的な取組の一環として、情報セキュリティ対策の内容の整合化・共通化を促進するため、それぞれの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。

(8)「政府機関統一技術基準」とは、政府機関統一管理基準に記載された情報セキュリティ対策を実施する上での具体的な技術的基準をいう。

(9)「省庁基本方針」とは、政府機関統一規範に準拠した、それぞれの府省庁における情報セキュリティ対策の基本的な方針をいう。

(10)「省庁対策基準」とは、政府機関統一管理基準及び政府機関統一技術基準に準拠し

た、それぞれの府省庁における全ての情報資産に適用する情報セキュリティ対策の基準をいう。

(11) 「省庁基準」とは、それぞれの府省庁が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。

(12) 「実施手順」とは、省庁基準に定められた対策の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。

(13) 「政府機関統一基準適用個別マニュアル群」とは、省庁基準に基づいて、それぞれの府省庁が実施手順を作成する際に参照すべき文書(実施手順、規程及びマニュアル等)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。

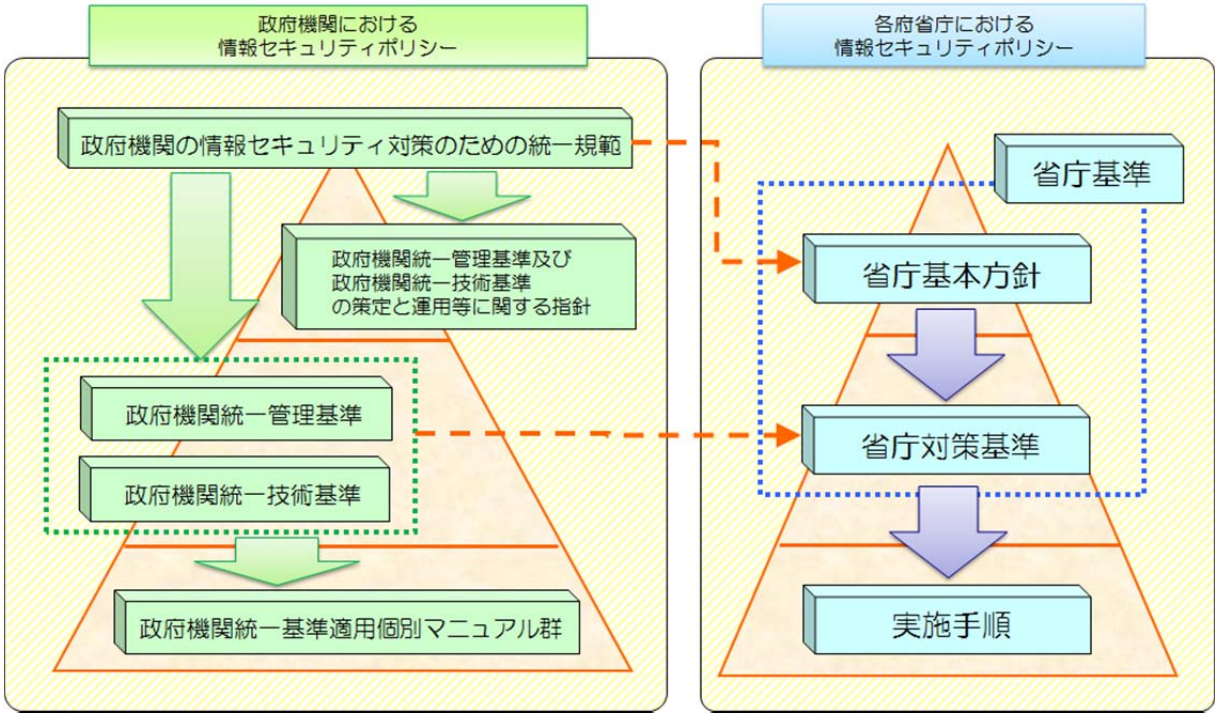

図１：政府機関及び各府省庁における情報セキュリティポリシー

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

それぞれの府省庁における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。

それぞれの府省庁は、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て情報セキュリティに係るリスクの評価を行うものとする。その上で、リスク対応の選択肢（低減、受容、共有又は回避）を選び、当該選択肢を具体化する情報セキュリティ対策を定め、これらを明文化した文書として省庁基準及び実施手順を策定し、これらの適切な運用に努める。

ここで、府省庁においては、政府機関統一規範並びに政府機関統一管理基準及び政府機関統一技術基準で定められた以上の情報セキュリティの確保を目的として、省庁基準及び実施手順を策定するとともに、その後、必要な見直しを行うものとする。したがって、府省庁において、政府機関統一管理基準及び政府機関統一技術基準で定められている内容を合理的な理由なく省庁対策基準に反映させないということはあってはならない。それぞれの府省庁は、その特性を踏まえつつ、省庁対策基準に盛り込むべき内容を決定するとともに、政府機関統一管理基準及び政府機関統一技術基準については、これを直接参照する、そのまま取り込む、又は構成や表現を変えて盛り込む等の方法により適切に反映させるものとする。なお、省庁対策基準から政府機関統一技術基準に相当する技術的側面の基準を分離し、省庁対策技術基準として別途策定してもよい。

また、センターは、それぞれの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、府省庁と協力して、政府機関統一基準適用個別マニュアル群を策定する。

情報システムの調達に当たっては、必要なセキュリティ対策を確実に実施するため、要求仕様に要件として記載することになる。

２－２　複数の府省庁で共通的に使用する基盤とな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基盤となる情報システム（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する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抜けや漏れの防止を図ることが必要であり、また、一部の情報システムの障害・事故等が他の情報システムに及ぼす影響等も踏まえ、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することが必要である。

このため、基盤となる情報システムを整備し運用管理する府省庁、及びこれと連携して運用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を運用管理する実施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の在り方について検討するとともに、情報セキュリティ対策を確実かつ迅速に調整・実施できる体制とする必要がある。

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、各府省庁における

情報セキュリティ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。

これらにより、基盤となる情報システムについても、情報セキュリティ対策の実施及び点検等、情報セキュリティマネジメントが適切に実行されることが必要である。

２－３　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、それぞれの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、遅滞なく継続的な取組が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、政府機関統一規範並びに政府機関統一管理基準及び政府機関統一技術基準に基づき、それぞれの府省庁の省庁基準、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、又は必要に応じて検査及び評価を実施し、必要に応じて改善を促す。

なお、それぞれの府省庁は、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。

２－４　情報セキュリティに関する障害・事故等への対応

情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生又はそのおそれがある場合には、早急にその状況を検出又は確認し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、障害・事故等の影響や範囲に関する責任者への報告及び府省庁内外の関係部門との情報共有により、障害・事故等の発生現場の混乱や誤った指示の発生等を最小限に抑えるとともに、被害の拡大防止や再発防止を講ずることが重要である。

このため、各府省庁は、障害・事故等への対応として、障害・事故等の発生に備えた体制や対処手順等の整備、発生時における報告と応急措置・復旧等、障害・事故等の原因調査と再発防止策を講ずる。センターは、各府省庁の障害・事故等への政府一体となった対応の中核となる機関として、各府省庁への技術的な支援及び助言を行うとともに、各府省庁間の情報共有の結節点として、各府省庁間の連携・調整を行う。各府省庁は、障害・事故等が発生又はそのおそれがある場合には、センター及び府省庁内外の関係部門との情報

共有により、被害の未然又は拡大防止及び再発防止のための措置を講ずる。

３　省庁基準に基づく情報セキュリティマネジメント

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

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情報セキュリティに係るリスク評価を行う。その際保護すべきものとされた特定の情報資産とこれ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) 省庁基準の適用範囲を明確にすること

省庁基準が適用される情報資産、組織（者）、場所・区域の範囲及びその境界を外部委託の観点も含めて明確にする。境界外で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等により、その境界が妥当であることを確認することも重要である。

適用範囲を定めるに当たっては、下記（ア）～（エ）を考慮する。

（ア）情報

省庁基準を適用する情報の範囲は、本指針１－２(2)の定義に従う。特に、情報システムの外部の電磁的記録媒体に記録された情報も対象となること、また、情報の作成・入手の時点から対象となることに留意し、府省庁の事務に基づく具体例を含む説明を示す必要がある。

（イ）組織（者）

省庁基準を適用する者の範囲は、政府職員（府省庁において行政事務に従事している国家公務員をいう。）及びそれぞれの府省庁の指揮命令に服している者のうち、それぞれの府省庁の管理対象である情報及び情報システムを取り扱う者（以下「行政事務従事者」という。）とする。この範囲について、府省庁の事務に基づく具体的な説明を示す必要がある。

（ウ）場所・区域

省庁基準を適用する場所・区域の範囲は、行政事務従事者の各々が所属する府省庁が管理する組織又は庁舎とする。特に、外出時の情報の持ち出し等、府省庁が管理する組織又は庁舎以外の場所・区域について適用範囲とする場合には、府省庁の事務に基づく具体的な説明を示す必要がある。

（エ）外部委託

府省庁の事務における情報の保有及び取扱いを外部に委託する場合は、府省庁が管理する組織又は庁舎以外の場所・区域で委託先に情報を保有させ又は取り扱わせる場合であっても、当該委託関係を省庁基準の適用範囲に含めて、これを管理する。省庁基準において、府省庁と委託先のそれぞれの責任を含む委託先管理の原則を示す必要がある。

(3) 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を行うこと

それぞれの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基づく継続的な取組によって意味をなすものである。したがって、図２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、これに基づく情報セキュリティ対策を実施していくことが重要である。そして、それとともに、対策の実施状況及び効果並びにその結果としての情報セキュリティの状態を的確に評価し、評価の結果に応じて省庁基準及び対策の実施について改善を図ることが重要である。

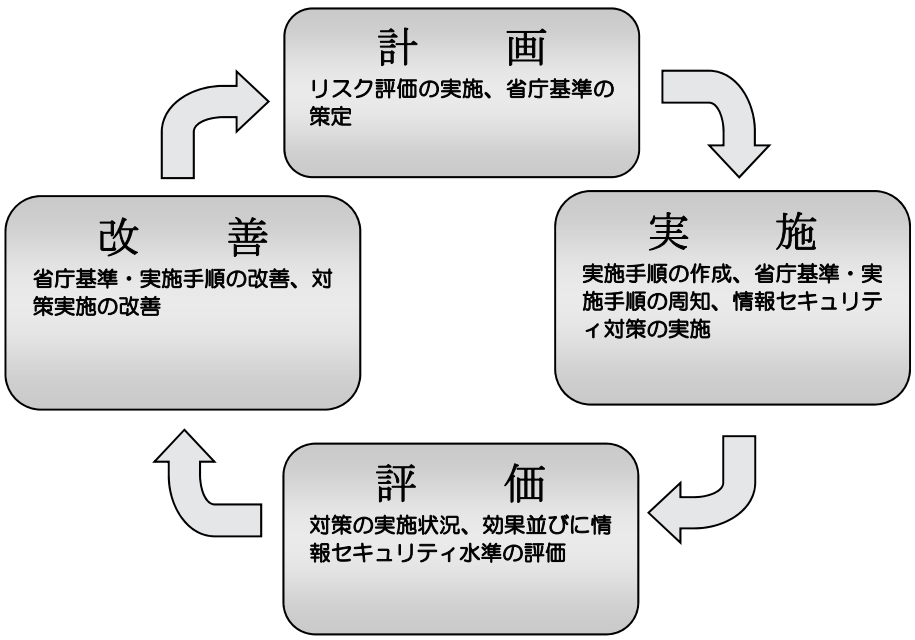

図２：省庁基準に基づく情報セキュリティ対策の実施サイクル

３－２　計画

省庁基準及び実施手順を策定する手続及び定めるべき事項の原則は次のとおりとする。

(1) 省庁基準及び実施手順の策定手続の概要

省庁基準は、図３に示すとおり、それぞれの府省庁において、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リスク評価に基づき、④省庁対策基準の策定を行い、⑤それぞれの府省庁内において意思統一及び明文化した省庁基準を決定するものとする。

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

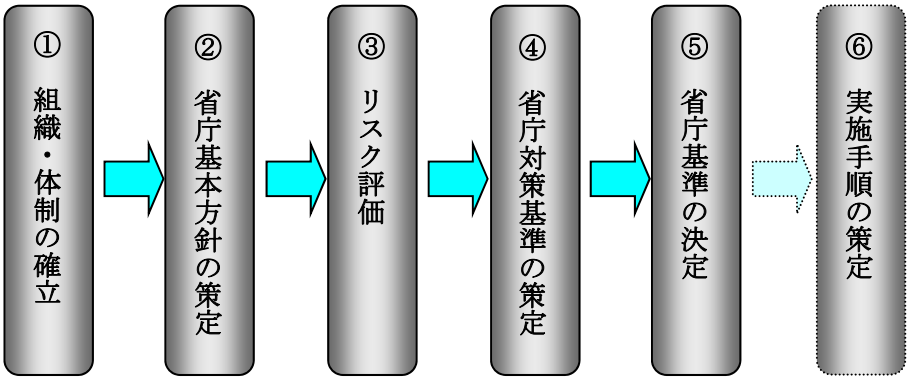

図３：省庁基準及び実施手順の策定手続の概要

なお、策定した対策基準及び実施手順並びにリスク評価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) 省庁基準策定のための組織・体制

情報セキュリティはそれぞれの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それぞれの府省庁における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

それぞれの府省庁は、情報資産に求められる情報セキュリティを確保するため、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) リスク評価及びリスク対応

情報セキュリティにおいてリスク評価とは、保護すべき情報資産を明らかにし、それらに対する情報セキュリティに係るリスクを評価することであり、図４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・脆弱性の調査を行い、③情報資産を取り巻く脅威・脆弱性の調査に基づき、④脅威の発生頻度、脆弱性の程度及び発生時の被害の大きさの分析を行うことと、②情報資産の重要性の分類に基づき、⑤情報セキュリティ要求水準の設定を行うことである。

なお、リスクの大きさについては、事故の発生頻度と発生時の被害の大きさの積として表す方法があるが、その場合、リスクによっては定量的に評価することが困難な場合が少なくないことにも留意する必要がある。

情報セキュリティにおいてリスク対応とは、保護すべき情報資産について求める情報セキュリティ水準を達成するための措置として、リスクの低減、受容、共有又は回避のいずれか又は組み合わせを選択し、かつ情報セキュリティ対策を決定することをいう。情報セキュリティ対策実施の制約等により、求める情報セキュリティ水準を超えるリスクを受容するとの判断もあり得る。

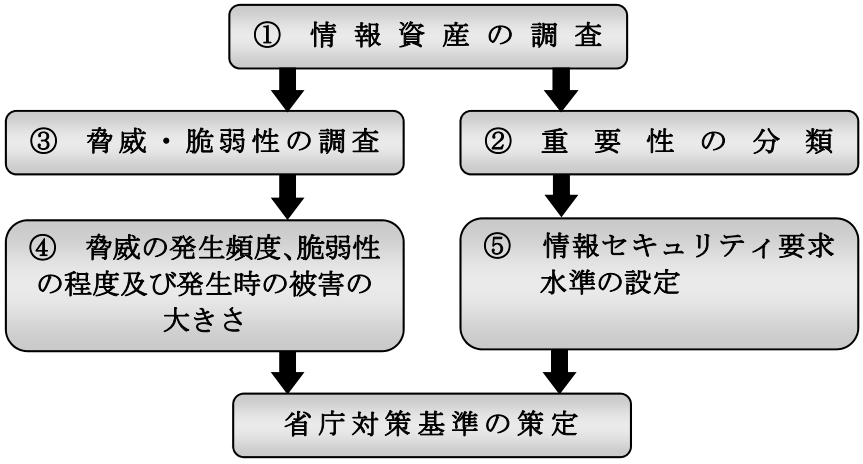

図４：リスク分析の手続

(5) 省庁対策基準の策定

リスク評価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、政府機関統一管理基準及び政府機関統一技術基準は、それぞれの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。これにより、専門的知識が必要とされる正確なリスク評価と対策の選定作業が、政府機関統一管理基準及び政府機関統一技術基準に準拠することで容易となるという効果がある。

このため、それぞれの府省庁は、省庁対策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管理基準及び政府機関統一技術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、府省庁としての意思決定を必要とすることを定める。

３－３　実施

実施手順の作成、省庁基準及び実施手順の周知及び運用は次のとおりとする。

(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、それぞれの府省庁は、政府機関統一基準適用個別マニュアル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・見直し等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。

委託先についても委託する業務に該当する事項を周知するとともに、これを契約に含めて行わせることが必要である。

(3) 省庁基準及び実施手順の運用

省庁基準及び実施手順で定めた情報セキュリティ対策を、定めた組織・体制の下で実施する。これには、情報の作成及び入手から消去までのライフサイクルに基づく管理、情報システムの利用管理、情報システムの計画から廃棄及び見直しまでのライフサイクル管理、緊急時対応及びその訓練を含む。

３－４　評価

情報セキュリティ対策についてその適正を確保するため、それぞれの府省庁は、情報セキュリティ対策の実施状況、効果並びに対策実施の結果としての情報セキュリティの状態を評価することが必要である。

評価を行うべき契機に、年度等定期、外部の脅威の変化、府省庁の業務や取り扱う情報の変化、情報セキュリティ事故やひやり事案の発生等がある。

なお、評価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、このため評価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。

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。

また、それぞれの府省庁において情報セキュリティ報告書を作成し、自組織の情報セキュリティ対策の取組状況を公表する。

３－５　改善

評価の結果、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、及び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、リスク評価を行い、リスク対応として省庁基準の改正、実施手順の改正、省庁基準又は実施手順の教育による周知徹底、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対応を採ることとなる。また、改善の処置の結果については、意図された目的が達成されていることを確認する必要がある。

なお、それぞれの府省庁は、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管理基準及び政府機関統一技術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　政府機関統一管理基準及び政府機関統一技術基準に関する取組

４－１　政府機関統一管理基準及び政府機関統一技術基準の策定と運用等

政府機関統一管理基準及び政府機関統一技術基準の原案はセンターが策定する。また、政府機関統一管理基準は、新たな脅威の発生やそれぞれの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、必要に応じて改訂を行う。政府機関統一技術基準は、新たな脅威の発生や技術の変化等の政府外環境の変化への対応が必要な場合に見直しを行い、必要に応じて改訂を行う。

なお、政府機関統一管理基準の策定については、次の点に留意する。

(1) 政府機関統一管理基準は、府省庁において必要とされる情報セキュリティ対策を原則として全て包含するものとして策定する。

(2) 政府機関統一管理基準は、責任体制、実施体制及び対策内容について、それぞれの府省庁が無理なく準拠できるよう、府省庁の実情を踏まえて策定する。

(3) 政府機関統一管理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　政府機関統一基準適用個別マニュアル群の策定と提供

政府機関統一基準適用個別マニュアル群については、それぞれの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それぞれの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訂し、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。