NISD-K304-111

政府機関の情報セキュリティ対策のための統一管理基準（平成 24 年度版）

平成 24 年 4 月 26 日

情報セキュリティ政策会議

目次

第 1.1 部　総則

1.1.1.1 本統一管理基準及び統一技術基準の位置付け

(1) 政府機関の情報セキュリティ対策の強化における本統一管理基準及び統一技術基準の位置付け

府省庁の情報セキュリティの確保については、それぞれの府省庁が自らの責任において対策を講じていくことが原則である。しかし、政府機関全体の情報セキュリティ対策を強化・拡充するためには、「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枠組みを構築し、それぞれの府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要である。そこで本統一管理基準及び政府機関の情報セキュリティ対策のための統一技術基準」（以下「統一技術基準」という。）は、政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

(2) 本統一管理基準及び統一技術基準の改訂

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、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。本統一管理基準及び統一技術基準については、それぞれの府省庁がその特性を踏まえた上で省庁対策基準及び実施手順の整備に活用し、また情報セキュリティ対策の評価に使用することにより、本統一管理基準及び統一技術基準の内容を追加・修正等すべきことが明らかになることが考えられる。また、情報技術の進歩に応じて、本統一管理基準に記載する情報セキュリティ対策を変更することも必要となり得る。

このため、本統一管理基準の見直しを定期的に行い、必要に応じて項目の追加やその内容の充実等を図ることによって、その適用性を将来にわたり維持するものとする。また、府省庁においては、本統一管理基準及び統一技術基準が更新された場合、その内容をそれぞれの省庁対策基準に適切に反映させる必要がある。

(3) 法令等の遵守

情報及び情報システムの取扱いに関しては、法令及び規則等（以下「関連法令等」という。）においても規定されているため、情報セキュリティ対策を実施する際には、本統一管理基準及び統一技術基準のほか関連法令等を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本統一管理基準及び統一技術基準では、あえて関連法令等の遵守について明記していない。また、情報セキュリティ対策に係る内容について定めた既存の政府決定等についても同様に遵守すること。

1.1.1.2 本統一管理基準及び統一技術基準の使い方

(1) 全体構成

本統一管理基準及び統一技術基準は、部、節及び項の 3 つの階層によって構成される。

本統一管理基準は、組織全体で情報セキュリティ対策を推進する組織・体制の整備、情報のライフサイクルの各段階における情報セキュリティ対策、情報システムに関連のある規程類の整備等について遵守すべき事項を定めており、統一技術基準は技術的な内容であり改訂頻度が高いものとして情報システムに求められるセキュリティ要件等について遵守すべき事項を定めている。

本統一管理基準では、「総則」、「組織と体制の整備」、「情報についての対策」、「情報処理についての対策」、「情報システムについての基本的な対策」を、統一技術基準では、「情報セキュリティ要件の明確化に基づく対策」、「情報システムの構成要素についての対策」、「個別事項についての対策」をそれぞれ部として分類している。

さらにそれぞれの部において、内容に応じて節として対策項目に分け、その下に項として対策基準を定めている。具体的には以下のとおり。

(a) 第 1.1 部 総則

(b) 第 1.2 部 組織と体制の整備

「組織と体制の整備」では、組織全体として情報セキュリティ対策を実施するに当たり、実施体制や評価手順、違反や例外措置等、組織としての運用に関係する各行政事務従事者の権限と責務を明確にするために整備すべき事項を本統一管理基準において定めている。

(c) 第 1.3 部 情報についての対策

「情報についての対策」では、情報の作成、利用、保存、移送、提供、消去等といった情報のライフサイクルに着目し、各段階において各行政事務従事者が情報を保護するために業務の中で常に実施すべき事項を本統一管理基準において定めている。

(d) 第 1.4 部 情報処理についての対策

「情報処理についての対策」では、情報システムの利用において実施すべき事項と、要管理対策区域外での情報処理及び府省庁支給以外の情報システムによる情報処理において制限すべき事項を本統一管理基準において定めている。

(e) 第 1.5 部 情報システムについての基本的な対策

「情報システムについての基本的な対策」では、統一技術基準で定められる遵守事項が適切に実施されるように、情報システムの計画、構築、運用、移行、廃棄及び見直しといった情報システムのライフサイクルの各段階において実施すべき事項と、情報システムに係る情報セキュリティを確保するために規定として整備すべき事項を本統一管理基準において定めている。

(f) 第 2.1 部 総則

(g) 第 2.2 部 情報セキュリティ要件の明確化に基づく対策

「情報セキュリティ要件の明確化に基づく対策」では、情報システムにおいて、アクセス制御の観点等、導入すべきセキュリティ機能を示すとともに、セキュリティホール、不正プログラム及びサービス不能攻撃等の脅威を防ぐために、情報システムにおいて実施すべき事項を統一技術基準において定めている。

(h) 第 2.3 部 情報システムの構成要素についての対策

「情報システムの構成要素についての対策」では、電子計算機及び通信回線等の個別の情報システムの特性及びライフサイクルの観点から、情報システムにおいて実施すべき事項を統一技術基準において定めている。

(i) 第 2.4 部 個別事項についての対策

「個別事項についての対策」では、新たな技術の導入等に際し特に情報セキュリティ上の配慮が求められる個別事象に着目し、遵守すべき事項を統一技術基準において定めている。

(2) 対策項目の記載事項

本統一管理基準及び統一技術基準では、府省庁が行うべき対策について、対策項目ごとに遵守事項を示す。

(3) 「対策レベルの設定」に係る変更点

「政府機関の情報セキュリティ対策における統一管理基準」（平成 23 年 4 月 21 日策定、NISD-K304-101）及び「政府機関の情報セキュリティ対策における統一技術基準」（平成 23 年 4 月 21 日策定、NISD-K305-101）までは、各対策項目で対策の強度に段階を設けていた。この段階を「対策レベル」と呼び、採るべき遵守事項を「基本遵守事項」又は「強化遵守事項」としていた。

そして、「基本遵守事項」を「保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項」、「強化遵守事項」を「特に重要な情報とこれを取り扱う情報システムにおいて、府省庁が、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項」と定義し、「強化遵守事項」については、各府省庁において省庁対策基準の策定時に、府省庁の情報システム及び業務の特性を踏まえ、省庁対策基準への採用を選択することとしていた。

今後は、従来の「基本遵守事項」及び「強化遵守事項」の区分を廃止して「遵守事項」とする。「遵守事項」は、省庁対策基準において、保護すべき情報とこれを扱うシステムにおいて、必須として実施すべき対策事項とする。なお、必要性の有無を検討し、必要があると判断した際に実施する対策事項については、実施の必要性の有無の検討を必須とし、対策の実施についてはそれぞれの府省庁の判断とする。

1.1.1.3 情報の格付の区分及び取扱制限の種類

(1) 格付及び取扱制限

行政事務で取り扱う情報については、その目的や用途により、取扱いに慎重を要する度合いは様々であり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、情報の格付の区分及び取扱制限の種類を定めるものとする。

情報の格付及び取扱制限は、その作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュ

リティ対策を明確にするための手段であることから、適切に実施される必要がある。

また、情報の格付及び取扱制限を実施することで、情報の利用者に対し、日々の情報セキュリティ対策の意識を向上させることができる。具体的には、情報を作成又は入手するたびに格付及び取扱制限の判断を行い、情報を取り扱うたびに格付及び取扱制限に従った対策を講ずることで、情報と情報セキュリティ対策が不可分であることについての認識を継続的に維持する効果も生ずるため、行政事務従事者にその内容を理解し遵守するように周知すること。

(2) 格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、それぞれにつき格付の区分の定義を示す。

格付としては、以下に記載のものを本統一管理基準の遵守事項で用いるが、それぞれの府省庁において、適宜変更又は追加して構わない。しかし、変更又は追加する場合には、それぞれの府省庁の対策基準における格付区分と遵守事項との関係が本統一管理基準及び統一技術基準での関係と同等以上となるように準拠しなければならない。また、変更又は追加した場合には、他の府省庁との情報のやり取りをする際に、自身の格付区分が本統一管理基準及び統一技術基準で用いた格付区分とどのように対応するかを伝達する方法について定めなければならない。例えば、他の府省庁に情報を提供する際に、本統一管理基準及び統一技術基準で用いた格付区分を記載する方法が考えられる。

(a) 情報の格付の区分は、機密性、完全性及び可用性について、それぞれ以下のとおりとする。

機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

格付の区分	分類の基準
完全性２情報	行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。
また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

(3) 取扱制限の種類

情報について、機密性、完全性及び可用性の３つの観点から区別し、それぞれにつき取扱制限の種類について基本的な定義を定める。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。

(a) 情報の取扱制限の種類は、機密性、完全性及び可用性について、それぞれ定めるものとする。なお、取扱制限の種類については適宜定めることができる。

1.1.1.4 情報取扱区域における管理及び利用制限

(1) 情報取扱区域

情報セキュリティを確保するためには、適切な対策が講じられている区域で行政事務を行うことが必要不可欠である。そのため、執務室や会議室、サーバ室等の管理に当たっては、それらの区域でどのような行政事務が行われるのかを想定し、それに応じて必要となる管理対策を決定し、適切な措置を講ずる必要がある。

また、それらの区域の利用に当たっては、用途や施されている管理対策に応じて、必

要な制限を利用者に求めることも情報セキュリティを確保する上で必要となる。

さらに、このような対策を有効なものとするためには、行政事務を行う者が、それらの区域に求められる管理対策及び利用の制限について正しく認識でき、取り扱う情報の重要性に応じて適切な区域を選択できるようにする必要がある。

これらのことから、それぞれの府省庁の内外において情報を取り扱う区域を「情報取扱区域」とし、それらの区域のうち、求める対策の観点から「クラス」の区分を定めるものとする。

(2) 情報取扱区域のクラスの決定

情報取扱区域について、求める対策の基準ごとに「クラス」の区分を定める。

(a) 情報取扱区域におけるクラス及びクラスにおける区分の基準を、それぞれ以下のとおりとする。

クラス	区分の基準
クラス 3	クラス 2 より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域
クラス 2	クラス 1 より強固な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域
クラス 1	最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域
クラス 0	クラス３、クラス２及びクラス１以外の区域であり、情報セキュリティを確保するため、利用制限対策を実施する必要がある区域

なお、クラス 1 以上の区域を「要管理対策区域」という。

(3) 情報取扱区域のクラス別管理及び利用制限

各府省庁は、定めた情報取扱区域について、クラス 0 からクラス 3 の区域においてクラス別に講ずる管理対策（以下「クラス別管理」という。）及び対策が講じられた区域におけるクラス別の利用制限対策（以下「クラス別利用制限」という。）を決定し、それらに基づいて適切に対策を講ずるものとする。

なお、統一管理基準及び統一技術基準において定めるクラス別管理及び利用制限は、最低限の管理対策及び利用制限対策であるため、それぞれの府省庁において、名称の変更、クラスの追加並びに実施する管理対策及び利用制限対策の変更又は追加を適宜実施

して構わない。ただし、変更又は追加する場合には、それぞれの府省庁の対策基準で求める情報取扱区域における情報セキュリティ水準が、本統一管理基準及び統一技術基準において求める情報セキュリティ水準と同等以上となるように準拠しなければならない。

(4) 情報取扱区域の個別管理及び個別利用制限

情報取扱区域について、決定したクラスの区分において必要な対策が不足していると認められる区域、又はクラスとは別の区分で対策を講ずる必要のある区域があるときは、求める情報セキュリティ水準を確保又は向上させるため、定められたクラス別管理及び利用制限にかかわらず、当該区域ごとに個別の管理対策（以下「個別管理」という。）及び個別の利用制限対策（以下「個別利用制限」という。）を決定することができる。

1.1.1.5 評価の方法

情報セキュリティ対策は、一過性のものとはせず、遅滞なく継続的に取組を実施できるものであることが重要である。そのためには、府省庁においては本統一管理基準及び統一技術基準に基づき、定期的又は事案等の発生の状況に応じて情報セキュリティ監査を行い、以下のことを確認する必要がある。

(a) 省庁対策基準が統一管理基準及び統一技術基準に準拠した内容となっていること。（設計の準拠性確認）

(b) 実際の運用が省庁対策基準に準拠していること。（運用の準拠性確認）

(c) 省庁対策基準の内容がリスクに応じて適切であること、効率的な内容であること、あるいは実現困難な内容となっていないこと。(設計の妥当性確認)

(d) 実際の運用がリスクに応じて有効で効率的であること。（運用の妥当性確認）

特に、府省庁の情報セキュリティ監査においては、設計及び運用の準拠性確認をその第一の目的とする。ただし、監査の過程において、設計及び運用の妥当性に関連して改善すべきと思われる点が発見された場合には、それを要検討事項にすることが望ましい。なお、本統一管理基準及び統一技術基準においては、実施すべき者を具体的に示して遵守事項を定めているため、対策の実施状況については各自の役割に応じた自己点検を実施することとする。情報セキュリティ対策においては、各自がそれぞれの役割を十分に実行することが不可欠であり、各自における対策の実効性を確保するために、自己点検を活用するものである。したがって、各府省庁が監査を行う際には、その自己点検の適切さを確認し、運用の準拠性確認に用いるものとする。また、監査を通じて把握した対策の実施状況と自己点検の結果に相違点があれば、相違点が発生した原因の分析及び自己点検結果の修正を行い正確な実施状況を把握するものとする。

情報セキュリティ対策の実施については、原則として、それぞれの府省庁の責任において運用することが大前提であるが、政府機関全体としての情報セキュリティ対策推進の観点から、府省庁は対策の実施状況及び監査結果について内閣官房情報セキュリティセンターに報告を行うこととする。また、それぞれの府省庁に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。さらに、内閣官房情報セキュリティセンターは、本統一管理基準及び統一技術基準に関する評価指標に基づき、府省庁の情報セキュリティ関係規程の整備状況及び対策実施状況について定期又は必要に応じて検査し、評価することとする。なお、対象となる情報システムの範囲については内閣官房情報セキュリティセンターが府省庁と協議して定めるものとする。

1.1.1.6 用語定義

【あ】

- 「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。
- 「移送」→「情報の移送」を参照。
- 「委託先」とは、情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を請け負った者をいう。

【か】

- 「外部委託」とは、情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を府省庁外の者に請け負わせることをいう。
- 「可用性」とは、情報及び関連資産へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。
- 「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- 「機器等」とは、情報機器等及びソフトウェアをいう。
- 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。
- 「行政事務従事者」とは、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）及びそれぞれの府省庁の指揮命令に服している者（個々の勤務条件にもよるが、例えば、派遣労働者等）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をいう。
- 「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況等を考慮して、１つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードという。
- 「記録媒体」とは、情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面、書類その他文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、電子計算機や通

信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、CD-R、DVD、MO、USB メモリ、フラッシュメモリ等の外部電磁的記録媒体がある。

● 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

● 「サービス」とは、サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能群をいう。

● 「最少特権機能」とは、管理者権限を実行できる範囲を管理作業に必要な最少の範囲に制限する機能をいう。

● 「識別」とは、情報システムにアクセスする主体を特定することをいう。

● 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

● 「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、行政事務の遂行に支障を及ぼすものをいう。情報の格付では、要機密情報に相当する。

● 「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

● 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本統一管理基準及び統一技術基準における「主体認証」については、公的又は第三者による証明に限るものではない。

● 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

● 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。
代表的な主体認証情報格納装置として、IC カード等がある。

● 「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。

● 「情報」とは、情報システム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又は

情報システムから出力した情報を記載した書面をいう。）及び情報システムに関する設計書が含まれる。

- 「情報システム」とは、情報処理及び通信に係るシステムをいう。
- 「情報セキュリティ関係規程」とは、省庁対策基準及び省庁対策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実施手順をいう。
- 「情報の移送」とは、要管理対策区域外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。
- 「情報の抹消」とは、廃棄した情報が漏えいすることを防止するために、全ての情報を復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態ではない。
- 「ソフトウェア」とは、電子計算機を動作させる手順及び命令を電子計算機が理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム上で動作するアプリケーションを含む広義の意味である。

【た】

- 「端末」とは、行政事務従事者が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆる PC のほか、PDA 等も該当する。
- 「通信回線」とは、これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みであり、物理的なものと論理的なものがある。
- 「通信回線装置」とは、回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。
- 「電子計算機」とは、コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。
- 「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。

【は】

- 「府省庁外」とは、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の外をいう。
- 「府省庁外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び府省庁管理又は他組織管理）及び通信回線装置を問わず、行政事務従事者の各々が所属する府省庁が管理していない電子計算機が接続され、当該電子計算機間の通信に利用する論理的な通信回線をいう。
- 「府省庁支給以外の情報システム」とは、行政事務従事者の各々が所属する府省庁が支給する情報システム以外の情報システムをいう。いわゆる私物の PC のほか、当該府省庁への出向者に対して出向元組織が提供する情報システムも含むものとする。

● 「府省庁支給以外の情報システムによる情報処理」とは、行政事務従事者の各々が所属する府省庁が支給する情報システム以外の情報システムを用いて行政事務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、行政事務従事者の各々が所属する府省庁の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

● 「府省庁内」とは、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の内をいう。

● 「府省庁内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び府省庁管理又は他組織管理）及び通信回線装置を問わず、行政事務従事者の各々が所属する府省庁が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。

● 「不正プログラム」とは、コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。

● 「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるように措置することをいう。なお、情報ごとに格付を記載することにより明示することを原則とするが、その他にも、当該情報の格付に係る認識が共通となる措置については、明示等に含むものとする。例えば、特定の情報システムについて、当該情報システムに記録される情報の格付を規定等に明記し、当該情報システムを利用する全ての者に当該規定を周知することができていれば明示等に含むものとする。

【や】

● 「要安定情報」とは、可用性２情報をいう。

● 「要機密情報」とは、機密性２情報及び機密性３情報をいう。

● 「要管理対策区域」とは、施設及び環境に係る管理対策が講じられている区域であって、情報取扱区域におけるクラス１以上の区域をいう。

● 「要管理対策区域外」とは、情報取扱区域におけるクラス０の区域をいう。

● 「要管理対策区域外での情報処理」とは、行政事務従事者が情報取扱区域におけるクラス０の区域において行政事務の遂行のための情報処理を行うことをいう。なお、オンラインで府省庁外から行政事務従事者の各々が所属する府省庁の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。

● 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。

● 「要保全情報」とは、完全性２情報をいう。

【ら】

- 「例外措置」とは、行政事務従事者がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。
- 「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。
- 「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

第 1.2 部　組織と体制の整備

1.2.1　導入

1.2.1.1 組織･体制の整備

遵守事項

(1) 最高情報セキュリティ責任者の設置
  (a) 最高情報セキュリティ責任者を１人置くこと。
  (b) 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に関する事務を統括すること。

(2) 情報セキュリティ委員会の設置
  (a) 最高情報セキュリティ責任者は、情報セキュリティ委員会を設置し、委員長及び委員を置くこと。
  (b) 情報セキュリティ委員会は、統一管理基準に準拠して、情報セキュリティに関する省庁対策基準を策定し、最高情報セキュリティ責任者の承認を得ること。

(3) 情報セキュリティ監査責任者の設置
  (a) 最高情報セキュリティ責任者は、情報セキュリティ監査責任者を１人置くこと。
  (b) 情報セキュリティ監査責任者は、最高情報セキュリティ責任者の指示に基づき、監査に関する事務を統括すること。

(4) 情報セキュリティ責任者の設置
  (a) 最高情報セキュリティ責任者は、情報セキュリティ対策の運用に係る管理を行う単位を定め、その単位ごとに情報セキュリティ責任者を置くこと。そのうち、情報セキュリティ責任者を統括する者として統括情報セキュリティ責任者を１人置くこと。
  (b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者の指示に基づき、統一技術基準に準拠して､情報セキュリティに関する省庁対策基準における技術的側面の基準を策定すること。なお、当該基準の策定については、最高情報セキュリティ責任者が指定した者に委任することができる。
  (c) 情報セキュリティ責任者は､所管する単位における情報セキュリティ対策に関する事務を統括すること。
  (d) 統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定を整備すること。
  (e) 情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定に従った運用がなされていることを定期的に確認すること。
  (f) 最高情報セキュリティ責任者は、情報セキュリティ責任者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を連絡すること。

(g) 統括情報セキュリティ責任者は、全ての情報セキュリティ責任者に対する連絡網を整備すること。

(5) 情報システムセキュリティ責任者の設置

(a) 情報セキュリティ責任者は、所管する単位における情報システムごとに情報システムセキュリティ責任者を、当該情報システムの計画段階までに置くこと。

(b) 情報システムセキュリティ責任者は、所管する情報システムに対するセキュリティ対策に関する事務を統括すること。

(c) 情報セキュリティ責任者は、情報システムセキュリティ責任者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を報告すること。

(d) 統括情報セキュリティ責任者は、全ての情報システムセキュリティ責任者に対する連絡網を整備すること。

(6) 情報システムセキュリティ管理者の設置

(a) 情報システムセキュリティ責任者は、所管する情報システムの管理業務において必要な単位ごとに情報システムセキュリティ管理者を置くこと。

(b) 情報システムセキュリティ管理者は、所管する管理業務における情報セキュリティ対策を実施すること。

(c) 情報システムセキュリティ責任者は、情報システムセキュリティ管理者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を報告すること。

(d) 統括情報セキュリティ責任者は、全ての情報システムセキュリティ管理者に対する連絡網を整備すること。

(7) 課室情報セキュリティ責任者の設置

(a) 情報セキュリティ責任者は、各課室に課室情報セキュリティ責任者を 1 人置くこと。

(b) 課室情報セキュリティ責任者は、課室における情報セキュリティ対策に関する事務を統括すること。

(c) 情報セキュリティ責任者は、課室情報セキュリティ責任者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を報告すること。

(d) 統括情報セキュリティ責任者は、全ての課室情報セキュリティ責任者に対する連絡網を整備すること。

(8) 区域情報セキュリティ責任者の設置

(a) 統括情報セキュリティ責任者は、要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う区域の単位を定め、その単位ごとに区域情報セキュリティ責任者を置くこと。

(b) 区域情報セキュリティ責任者は、所管する単位における区域ごとの情報セキュリティ対策に関する事務を統括すること。

(c) 統括情報セキュリティ責任者は、全ての区域情報セキュリティ責任者に対する連絡網を整備すること。

(9) 最高情報セキュリティアドバイザーの設置
  (a) 最高情報セキュリティ責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くこと。
  (b) 最高情報セキュリティ責任者は、情報セキュリティ対策等の実施において最高情報セキュリティアドバイザーが行う業務の内容について定めること。

1.2.1.2 役割の割当て

遵守事項

(1) 兼務を禁止する役割の規定
  (a) 行政事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。
    (ア) 承認又は許可事案の申請者とその承認又は許可を行う者（以下本項において「承認権限者等」という。）
    (イ) 監査を受ける者とその監査を実施する者

(2) 上司による承認・許可
  (a) 行政事務従事者は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をすること。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。
  (b) 行政事務従事者は、前事項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずること。

1.2.1.3 違反と例外措置

遵守事項

(1) 違反への対処
  (a) 行政事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合には、各規定の実施に責任を持つ情報セキュリティ責任者にその旨を報告すること。
  (b) 情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせること。
  (c) 情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、最高情報セキュリティ責任者にその旨を報告すること。
(2) 例外措置

(a) 情報セキュリティ委員会は、例外措置の適用の申請を審査する者（以下本項において「許可権限者」という。）を定め、審査手続を整備すること。

(b) 行政事務従事者は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に例外措置の適用を申請すること。ただし、行政事務の遂行に緊急を要する等の場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。行政事務従事者は、申請の際に以下の事項を含む項目を明確にすること。

(ア) 申請者の情報（氏名、所属、連絡先）

(イ) 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）

(ウ) 例外措置の適用を申請する期間

(エ) 例外措置の適用を申請する措置内容（講ずる代替手段等）

(オ) 例外措置の適用を終了した旨の報告方法

(カ) 例外措置の適用を申請する理由

(c) 許可権限者は、行政事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。また、決定の際に、以下の項目を含む例外措置の適用審査記録を作成し、最高情報セキュリティ責任者に報告すること。

(ア) 決定を審査した者の情報（氏名、役割名、所属、連絡先）

(イ) 申請内容

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

(ウ) 審査結果の内容

- 許可又は不許可の別
- 許可又は不許可の理由
- 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を許可した期間
- 許可した措置内容（講ずるべき代替手段等）
- 例外措置を終了した旨の報告方法

(d) 行政事務従事者は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了した時に、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

(e) 許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必

要な措置を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

(f) 最高情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずること。

1.2.2 運用

1.2.2.1 情報セキュリティ対策の教育

遵守事項

(1) 情報セキュリティ対策の教育の実施

(a) 統括情報セキュリティ責任者は、情報セキュリティ関係規程について、行政事務従事者に対し、その啓発をすること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ関係規程について、行政事務従事者の役割に応じて教育すべき内容を検討し、教育のための資料を整備すること。

(c) 統括情報セキュリティ責任者は、行政事務従事者の役割に応じて毎年度最低１回、受講できるように、情報セキュリティ対策の教育に係る計画を企画及び立案するとともに、その実施体制を整備すること。

(d) 統括情報セキュリティ責任者は、行政事務従事者の着任時又は異動時に、その役割に応じて新しい職場等で３か月以内に受講できるように、情報セキュリティ対策の教育を企画及び立案するとともに、その実施体制を整備すること。

(e) 統括情報セキュリティ責任者は、行政事務従事者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。

(f) 統括情報セキュリティ責任者は、行政事務従事者の情報セキュリティ対策の教育の受講状況について、課室情報セキュリティ責任者に通知すること。

(g) 課室情報セキュリティ責任者は、行政事務従事者に情報セキュリティ対策の教育を受講させること。

(h) 課室情報セキュリティ責任者は、行政事務従事者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。行政事務従事者が当該勧告に従わない場合には、統括情報セキュリティ責任者にその旨を報告すること。

(i) 統括情報セキュリティ責任者は、毎年度１回、最高情報セキュリティ責任者及び情報セキュリティ委員会に対して、行政事務従事者の情報セキュリティ対策の教育の受講状況について報告すること。

(j) 統括情報セキュリティ責任者は、情報セキュリティ関係規程について、行政事務従事者に対する情報セキュリティ対策の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

(2) 情報セキュリティ対策の教育の受講

(a) 行政事務従事者は、毎年度最低１回、情報セキュリティ対策の教育に関する計画に従って、情報セキュリティ対策の教育を受講すること。

(b) 行政事務従事者は、着任時又は異動時に新しい職場等で、情報セキュリティ対策の教育の受講方法について課室情報セキュリティ責任者に確認すること。

(c) 行政事務従事者は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではない場合には、その理由について、課室情報セキュリティ責任者を通じて、

統括情報セキュリティ責任者に報告すること。

(d) 行政事務従事者は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って情報セキュリティ対策の訓練に参加すること。

1.2.2.2 障害・事故等の対処

遵守事項

(1) 障害・事故等の発生に備えた事前準備

(a) 最高情報セキュリティ責任者は、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。）の発生に対応するために以下の役割及び機能を有する体制を整備すること。

(ア) 障害・事故等に対応する責任者の決定

(イ) 障害・事故等の発生の報告

(ウ) 障害・事故等の発生報告の受付

(エ) 関係する部門への障害・事故等の発生に関する速やかな連絡

(オ) 応急措置の実施（被害の拡大防止）

(カ) 障害・事故等からの復旧

(キ) 原因調査の実施

(ク) 再発防止策の策定及び実施

(ケ) 再発防止策の実施の確認

(b) 統括情報セキュリティ責任者は、障害・事故等について報告手順を整備し、当該報告手段を全ての行政事務従事者に周知すること。

(c) 統括情報セキュリティ責任者は、障害・事故等が発生した際の府省庁内及び府省庁外との情報共有を含む対処手順を整備すること。

(d) 統括情報セキュリティ責任者は、障害・事故等に備え、行政事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

(e) 統括情報セキュリティ責任者は、障害・事故等への対処の訓練の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

(f) 行政事務従事者は、障害・事故等への対処の訓練に関する規定が定められている場合には、当該規定に従って、障害・事故等への対処の訓練に参加すること。

(g) 統括情報セキュリティ責任者は、障害・事故等について府省庁の外部から報告を受けるための窓口を設置し、その窓口への連絡手段を府省庁外に公表すること。

(2) 障害・事故等の発生時における報告と対処の流れ

(a) 行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に報告することができない場合は、定められた報告手順に従

って、最高情報セキュリティ責任者に報告すること。

(b) 障害・事故等に対応する責任者は、被害の拡大防止等を図るための応急措置の実施及び障害・事故等からの復旧に係る指示又は勧告を行うこと。

(c) 行政事務従事者は、障害・事故等が発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

(d) 行政事務従事者は、障害・事故等が発生した場合であって、当該障害・事故等について対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、障害・事故等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

(e) 最高情報セキュリティ責任者は、報告を受けた障害・事故等について、定められた対処手順に従って、府省庁内外の関係部門と情報共有を行うこと。

(3) 障害・事故等の原因調査と再発防止策

(a) 情報セキュリティ責任者は、障害・事故等が発生した場合には、障害・事故等に対応する責任者が実施した内容も踏まえ、障害・事故等の原因を調査するとともに再発防止策を策定し、その結果を報告書として最高情報セキュリティ責任者に報告すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティ責任者から障害・事故等についての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。

(4) 障害・事故等の発生するおそれがある場合の対処

(a) 最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ責任者又は障害・事故等に対応する責任者は、障害・事故等の発生するおそれがある場合においては、本項の各遵守事項に準じて、必要な措置を講ずること。

(b) 行政事務従事者は、障害・事故等の発生するおそれがある場合においては、前事項による報告手順や対処手順等に基づき、適切な措置を講ずること。

1.2.3 評価

1.2.3.1 情報セキュリティ対策の自己点検

遵守事項

(1) 自己点検に関する年度計画の策定

(a) 統括情報セキュリティ責任者は、年度自己点検計画を策定し、最高情報セキュリティ責任者の承認を得ること。

(2) 自己点検の実施に関する準備

(a) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

(3) 自己点検の実施

(a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定める年度自己点検計画に基づき、行政事務従事者に対して、自己点検の実施を指示すること。

(b) 行政事務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施すること。

(4) 自己点検結果の評価

(a) 情報セキュリティ責任者は、行政事務従事者による自己点検が行われていることを確認し、その結果を評価すること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ責任者による自己点検が行われていることを確認し、その結果を評価すること。

(c) 統括情報セキュリティ責任者は、自己点検の結果を最高情報セキュリティ責任者へ報告すること。

(5) 自己点検に基づく改善

(a) 行政事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、情報セキュリティ責任者にその旨を報告すること。

(b) 最高情報セキュリティ責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には情報セキュリティ責任者に改善を指示すること。

1.2.3.2 情報セキュリティ対策の監査

遵守事項

(1) 監査計画の策定

(a) 情報セキュリティ監査責任者は、年度監査計画を策定し、最高情報セキュリティ

責任者の承認を得ること。

(2) 監査の実施に関する指示

(a) 最高情報セキュリティ責任者は、年度監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度監査計画で計画されたこと以外の監査の実施を指示すること。

(3) 個別の監査業務における監査実施計画の策定

(a) 情報セキュリティ監査責任者は、年度監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定すること。

(4) 監査の実施に係る準備

(a) 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

(b) 情報セキュリティ監査責任者は、府省庁外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、府省庁外の者に監査の一部を請け負わせること。

(5) 監査の実施

(a) 情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施すること。

(b) 情報セキュリティ監査実施者は、省庁対策基準が統一管理基準及び統一技術基準に準拠していることを確認すること。

(c) 情報セキュリティ監査実施者は、実施手順が省庁対策基準に準拠していることを確認すること。

(d) 情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していることを確認すること。

(e) 情報セキュリティ監査実施者は、監査調書を作成すること。

(f) 情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、最高情報セキュリティ責任者へ提出すること。

(6) 監査結果に対する対処

(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、被監査部門の情報セキュリティ責任者に対して、指摘されたことに対する対処の実施を指示すること。

(b) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の

課題及び問題点があることを確認する必要があると判断した場合には、他の部門の情報セキュリティ責任者に対しても、同種の課題及び問題点の有無を確認するように指示すること。

(c) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、対処計画を策定し、報告すること。

(d) 最高情報セキュリティ責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。

1.2.4　見直し

1.2.4.1 情報セキュリティ対策の見直し

遵守事項

(1) 情報セキュリティ対策の見直し

(a) 情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。

(b) 行政事務従事者は、情報セキュリティ関係規程に課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談すること。

(c) 情報セキュリティ関係規程を整備した者は、情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合は、必要な措置を講ずること。

1.2.5 その他

1.2.5.1 外部委託

適用範囲

本項は、府省庁による貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次に掲げる営業品目に該当するものに適用する。

- ソフトウェア開発（プログラム作成、システム開発等）
- 情報処理（統計、集計、データエントリー、媒体変換等）
- 賃貸借
- 調査・研究（調査、研究、検査等）

遵守事項

(1) 情報セキュリティ確保のための府省庁内共通の仕組みの整備

(a) 統括情報セキュリティ責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。

(b) 統括情報セキュリティ責任者は、委託先の選定基準及び選定手続を整備すること。

(2) 委託先に実施させる情報セキュリティ対策の明確化

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、委託先候補に事前に周知すること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法を整備し、委託先候補に事前に周知すること。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先における情報セキュリティ対策の履行状況を確認するための方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を整備し、委託先候補に事前に周知すること。

(3) 委託先の選定

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、選定基準及び選定手続に基づき、委託先を選定すること。

(4) 外部委託に係る契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を含む外部委託に伴う契約を取り交わすこと。また、必要

に応じて、以下の事項を当該契約に含めること。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めさせること。

(ア) 当該委託業務に携わる者の特定

(イ) 遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託契約の継続に関しては、選定基準及び選定手続に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。

(d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の提供する役務(情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。)の変更に関しては、選定基準及び選定手続に基づき、その是非を審査すること。

(e) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保される措置を委託先に担保させること。

(5) 外部委託の実施における手続

(a) 行政事務従事者は、委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。

(ア) 委託先に情報を提供する場合は、安全な受渡し方法によりこれを実施し、提供した記録を取得すること。

(イ) 外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消（全ての情報を復元が困難な状態にすることをいう。以下同じ。）させること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、取り交わした契約の対処方法に従い、委託先に必要な措置を講じさせること。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り交わした契約の対処方法に従い、委託先における情報セキュリティ対策の履行状況を確認すること。

(6) 外部委託終了時の手続

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。

1.2.5.2 業務継続計画及び情報システム運用継続計画との整合的運用の確保

遵守事項

(1) 業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保

(a) 情報セキュリティ委員会は、府省庁において業務継続計画、情報システム運用継続計画又は省庁対策基準を整備する場合には、業務継続計画及び情報システム運用継続計画と省庁対策基準との間の整合性の確保のための検討を行うこと。

(b) 統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画及び情報システム運用継続計画を整備する場合には、全ての情報システムについて、当該業務継続計画及び情報システム運用継続計画との関係の有無を検討すること。

(c) 統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画及び情報システム運用継続計画を整備する場合には、当該業務継続計画及び情報システム運用継続計画と関係があると認めた情報システムについて、業務継続計画及び情報システム運用継続計画との整合性を考慮し、必要な措置を講ずること。

(ア) 通常時において業務継続計画及び情報システム運用継続計画と省庁対策基準との整合的運用が可能となるよう必要な措置を講ずること。

(イ) 事態発生時において業務継続計画、情報システム運用継続計画及び省庁対策基準との整合的運用が可能となるよう実施手順の整備等の必要な措置を講ずること。

(2) 業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の不整合の報告

(a) 行政事務従事者は、府省庁において業務継続計画及び情報システム運用継続計画と整備する場合であって、業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。

1.2.5.3 情報取扱区域

遵守事項

(1) 情報取扱区域のクラス、管理及び利用制限の決定

(a) 統括情報セキュリティ責任者は、情報取扱区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限対策を決定すること。なお、決定する内容は、統一技術基準 2.3.1.1（別表 1 及び別表 2 を含む。）に定める。

(b) 情報セキュリティ責任者は、要管理対策区域については、当該区域を管理又は利用する行政事務従事者がクラスについて認識できる措置を講ずること。
(c) 区域情報セキュリティ責任者は、個別の管理対策及び利用制限対策を決定する必要性の有無を検討し、必要と認めた場合は、当該対策を決定し、統括情報セキュリティ責任者に報告すること。

(2) 情報取扱区域の管理
(a) 区域情報セキュリティ責任者は、要管理対策区域を管理する場合には、統括情報セキュリティ責任者が定めた当該区域のクラスを確認し、統一技術基準 2.3.1.1（別表 1 を含む。）に定める管理対策を講ずること。また、個別の管理対策を決定している場合には、同様に対策を講ずること。

(3) 情報取扱区域における利用制限
(a) 区域情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた情報取扱区域のクラスを確認し、統一技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策を講ずること。なお、個別に利用制限対策を決定している場合には、同様に講ずること。
(b) 行政事務従事者は、情報を取り扱う場合には、統括情報セキュリティ責任者が定めた情報取扱区域のクラスを確認し、統一技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策に従って利用すること。なお、個別の利用制限対策を決定している場合には、同様に従うこと。

第 1.3 部　情報についての対策

1.3.1　情報の取扱い

1.3.1.1 情報の作成と入手

遵守事項

(1) 業務以外の情報の作成又は入手の禁止

(a) 行政事務従事者は、行政事務の遂行以外の目的で、情報を作成し、又は入手しないこと。

(2) 情報の作成又は入手時における格付と取扱制限の決定

(a) 行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に格付及び取扱制限の定義に基づき、格付及び取扱制限を決定すること。

(b) 行政事務従事者は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の格付及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。

(3) 格付と取扱制限の明示等

(a) 行政事務従事者は、情報の格付及び取扱制限を決定（再決定を含む。以下同じ。）した際に、当該情報の参照が許されている者が認識できる方法を用いて明示等すること。

(4) 格付と取扱制限の加工時における継承

(a) 行政事務従事者は、情報を作成する際に、参照した情報又は入手した情報が既に格付又は取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

1.3.1.2 情報の利用

遵守事項

(1) 業務以外の利用の禁止

(a) 行政事務従事者は、行政事務の遂行以外の目的で、情報を利用しないこと。

(2) 格付及び取扱制限に従った情報の取扱い

(a) 行政事務従事者は、利用する情報に明示等された格付に従って、当該情報を適切に取り扱うこと。格付に加えて取扱制限の明示等がなされている場合には、当該取扱

制限の指示内容に従って取り扱うこと。

(3) 格付及び取扱制限の複製時における継承
(a) 行政事務従事者は、情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

(4) 格付及び取扱制限の見直し
(a) 行政事務従事者は、情報を利用する場合に、元の格付又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付又は取扱制限そのものを見直す必要があると思料する場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下この項において「決定者等」という。）に相談すること。
(b) 行政事務従事者は、自らが格付及び取扱制限の決定者等である情報に対して、見直しの必要があると認めた場合には、当該情報の格付又は取扱制限を再決定し、それを明示等すること。また、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知すること。

(5) 要保護情報の取扱い
(a) 行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を要管理対策区域外に持ち出さないこと。
(b) 行政事務従事者は、要保護情報を放置しないこと。
(c) 行政事務従事者は、機密性３情報を必要以上に複製しないこと。
(d) 行政事務従事者は、要機密情報を必要以上に配付しないこと。
(e) 行政事務従事者は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。
(f) 行政事務従事者は、情報を機密性３情報と決定した書面のうち、必要なものには、一連番号を付し、その所在を明らかにしておくこと。

1.3.1.3 情報の保存

遵守事項

(1) 格付に応じた情報の保存
(a) 行政事務従事者は、情報の格付及び取扱制限に応じて、情報を適切に保存すること。
(b) 行政事務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。
(c) 行政事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワ

ードを設定すること。

(d) 行政事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(e) 行政事務従事者は、要保全情報を電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

(f) 行政事務従事者は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。

(g) 行政事務従事者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。

(2) 情報の保存期間

(a) 行政事務従事者は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

1.3.1.4 情報の移送

遵守事項

(1) 情報の移送に関する許可及び届出

(a) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を移送する場合には、課室情報セキュリティ責任者の許可を得ること。

(b) 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面を移送する場合には、課室情報セキュリティ責任者に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

(2) 情報の送信と運搬の選択

(a) 行政事務従事者は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

(3) 移送手段の決定

(a) 行政事務従事者は、要保護情報を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２

情報である書面の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

(4) 記録媒体の保護対策

(a) 行政事務従事者は、要機密情報が記録又は記載された記録媒体を運搬する場合には、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

(5) 電磁的記録の保護対策

(a) 行政事務従事者は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。

(b) 行政事務従事者は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(c) 行政事務従事者は、要保全情報である電磁的記録を移送する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

(d) 行政事務従事者は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めたときは、情報のバックアップを取得すること。

(e) 行政事務従事者は、要安定情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送する等の措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

(f) 行政事務従事者は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いる必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

1.3.1.5 情報の提供

遵守事項

(1) 情報の公表

(a) 行政事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

(b) 行政事務従事者は、電磁的記録を公表する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。

(2) 他者への情報の提供

(a) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を府省庁外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。

(b) 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である

電磁的記録又は機密性２情報である書面を府省庁外の者に提供する場合には、課室情報セキュリティ責任者に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた提供については、この限りでない。

(c) 行政事務従事者は、要保護情報を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。

(d) 行政事務従事者は、電磁的記録を提供する場合には、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。

1.3.1.6 情報の消去

遵守事項

(1) 電磁的記録の消去方法

(a) 行政事務従事者は、電磁的記録媒体を廃棄する場合には、全ての情報を抹消すること。

(b) 行政事務従事者は、電磁的記録媒体を他の者へ提供する場合には、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

(c) 行政事務従事者は、電磁的記録媒体について、設置環境等から要機密情報を抹消する必要性の有無を検討し、必要と認めたときは、当該電磁的記録媒体の要機密情報を抹消すること。

(2) 書面の廃棄方法

(a) 行政事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

第 1.4 部　情報処理についての対策

1.4.1　情報システムの利用

1.4.1.1 情報システムの利用

遵守事項

(1) 識別コードの管理

(a) 行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと。

(b) 行政事務従事者は、自己に付与された識別コードを他者が主体認証に用いるために付与及び貸与しないこと。

(c) 行政事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。

(d) 行政事務従事者は、行政事務のために識別コードを利用する必要がなくなった場合は、その旨を情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、情報システムセキュリティ責任者が定めている場合は、この限りでない。

(e) 情報システムセキュリティ責任者は、管理者権限を持つ識別コードを付与された行政事務従事者に、管理者としての業務遂行時に限定して当該識別コードを利用させる必要性の有無を検討し、必要と認めたときは、管理者としての業務遂行時に限定して当該識別コードを利用させること。

(f) 行政事務従事者は、管理者権限を持つ識別コードを付与され、かつ情報システムセキュリティ責任者が求めた場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

(2) 主体認証情報の管理

(a) 行政事務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

(b) 情報システムセキュリティ責任者又は情報システムセキュリティ管理者は、主体認証情報が他者に使用され、又はその危険が発生したことを知った場合には、必要な措置を講ずること。

(c) 行政事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

(ア) 自己の主体認証情報を他者に知られないように管理すること。

(イ) 自己の主体認証情報を他者に教えないこと。

(ウ) 主体認証情報を忘却しないように努めること。

(エ) 主体認証情報を設定するに際しては、容易に推測されないものにすること。

(オ) 異なる識別コードに対して、共通の主体認証情報を用いないこと。
(カ) 情報システムセキュリティ管理者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。

(d) 行政事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。
(ア) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。
(イ) 主体認証情報格納装置を他者に付与及び貸与しないこと。
(ウ) 主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。
(エ) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者又は情報システムセキュリティ管理者に返還すること。

(e) 情報システムセキュリティ責任者は、主体認証のために取得した情報を本人から事前に同意を得た目的以外の目的で使用しないこと。

(3) 識別コードと主体認証情報の付与管理
(a) 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。
(b) 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。
(ア) 主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続
(イ) 主体認証情報の初期配布方法及び変更管理手続
(ウ) アクセス制御情報の設定方法及び変更管理手続
(c) 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。

(4) 識別コードと主体認証情報における代替手段等の適用
(a) 情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった行政事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。
(b) 情報システムセキュリティ責任者及び情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用を知った場合には、直ちに当該識別コードによる使用を停止させること。

1.4.2 情報処理の制限

1.4.2.1 要管理対策区域外での情報処理の制限

遵守事項

(1) 安全管理措置についての規定の整備

(a) 統括情報セキュリティ責任者は、要保護情報について要管理対策区域外での情報処理を行う場合の安全管理措置についての規定を整備すること。

(b) 統括情報セキュリティ責任者は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合の安全管理措置についての規定を整備すること。

(2) 許可及び届出の取得及び管理

(a) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。

(b) 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

(c) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、要管理対策区域外での要保護情報の情報処理に係る記録を取得すること。

(d) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(e) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

(f) 行政事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。

(g) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。

(h) 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないと

した場合は、この限りでない。

(i) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得すること。

(j) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(k) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを要管理対策区域外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

(l) 行政事務従事者は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持ち出しにとどめること。

(3) 安全管理措置の遵守

(a) 行政事務従事者は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずること。

(b) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

(c) 行政事務従事者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずること。

(d) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

1.4.2.2 府省庁支給以外の情報システムによる情報処理の制限

遵守事項

(1) 安全管理措置についての規定の整備

(a) 統括情報セキュリティ責任者は、要保護情報について府省庁支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

(2) 許可及び届出の取得及び管理

(a) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。

(b) 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

(c) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。

(d) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(e) 情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

(3) 安全管理措置の遵守

(a) 行政事務従事者は、要保護情報について府省庁支給以外の情報システムによる情報処理を行う場合には、当該情報システムについて定められた安全管理措置を講ずること。

(b) 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムによる情報処理を終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

(c) 情報システムセキュリティ責任者は、要保護情報を取り扱う府省庁支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に確認すること。

第 1.5 部　情報システムについての基本的な対策

1.5.1　情報システムのセキュリティ要件

1.5.1.1 情報システムのセキュリティ要件

遵守事項

(1) 情報システムの計画

(a) 情報システムセキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

(b) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。この場合、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の活用又はそれと同等以上の検討を行った上で決定すること。また、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムにおいては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づき決定すること。

(c) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。

(d) 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。

(e) 情報システムセキュリティ責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。

(f) 情報システムセキュリティ責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。

(2) 情報システムの構築及び運用

(a) 情報システムセキュリティ責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めたセキュリティ対策を行うこと。

(3) 情報システムの移行及び廃棄

(a) 情報システムセキュリティ責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。

(4) 情報システムの見直し

(a) 情報システムセキュリティ責任者は、情報システムのセキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

1.5.2 情報システムに係る規定の整備と遵守

1.5.2.1 情報システムに係る文書及び台帳整備

遵守事項

(1) 情報システムの文書整備

(a) 情報システムセキュリティ責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。

(ア) 当該情報システムを構成する電子計算機関連事項

- 電子計算機を管理する行政事務従事者及び利用者を特定する情報
- 電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン
- 電子計算機の仕様書又は設計書

(イ) 当該情報システムを構成する通信回線及び通信回線装置関連事項

- 通信回線及び通信回線装置を管理する行政事務従事者を特定する情報
- 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン
- 通信回線及び通信回線装置の仕様書又は設計書
- 通信回線の構成
- 通信回線装置におけるアクセス制御の設定
- 通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応
- 通信回線の利用部門

(ウ) 情報システムの構成要素のセキュリティ維持に関する手順

- 電子計算機のセキュリティ維持に関する手順
- 通信回線を介して提供するサービスのセキュリティ維持に関する手順
- 通信回線及び通信回線装置のセキュリティ維持に関する手順

(エ) 障害・事故等が発生した際の対処手順

(b) 情報システムセキュリティ管理者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理においてセキュリティ対策を行うこと。

(2) 情報システムの台帳整備

(a) 統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。

(ア) 情報システム名

(イ) 管理課室、当該情報システムセキュリティ責任者の氏名及び連絡先

(ウ) システム構成

(エ) 接続する府省庁外通信回線の種別

(オ) 取り扱う情報の格付及び取扱制限に関する事項

(カ) 当該情報システムの設計・開発、運用、保守に関する事項

また、情報処理業務を外部に委託する場合は、以下の事項を記載した台帳を整備

すること。

(キ) 役務名

(ク) 管理課室、当該情報システムセキュリティ責任者の氏名及び連絡先

(ケ) 契約事業者

(コ) 契約期間

(サ) 役務概要

(シ) ドメイン名（インターネット上で提供されるサービス等を利用する場合）

(ス) 取り扱う情報の格付及び取扱制限に関する事項

(b) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項について統括情報セキュリティ責任者に報告すること。

1.5.2.2 機器等の購入

適用範囲

本項は、機器等の購入（購入に準ずるリース等を含む。以下同じ。）に適用する。

遵守事項

(1) 機器等の購入に係る規定の整備

(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。

(b) 統括情報セキュリティ責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。

(c) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

(2) 機器等の購入に係る規定の遵守

(a) 情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。

(b) 情報システムセキュリティ責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。

1.5.2.3 ソフトウェア開発

遵守事項

(1) ソフトウェア開発に係る規定の整備

(a) 統括情報セキュリティ責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を情報システムセキュリティ責任者に求めるための規定を整備すること。

(ア) 情報システムセキュリティ責任者は、セキュリティに係る対策事項（本項(1)(a)(ウ)から(セ)の遵守事項をいう。）を満たすことが可能な開発体制を確保すること。

(イ) 情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（本項(1)(a)(ウ)から(セ)の遵守事項をいう。）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

(ウ) 情報システムセキュリティ責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。

(エ) 情報システムセキュリティ責任者は、ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。

(オ) 情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。

(カ) 情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。

(キ) 情報システムセキュリティ責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

(ク) 情報システムセキュリティ責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。

(ケ) 情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価及び ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書のST評価及びST確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

(コ) 情報システムセキュリティ責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取

得すること。

(サ) 情報システムセキュリティ責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。

(シ) 情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

(ス) 情報システムセキュリティ責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する試験項目及び試験方法を定め、これに基づいて試験を実施すること。

(セ) 情報システムセキュリティ責任者は、情報セキュリティの観点から実施した試験の実施記録を保存すること。

⑵ ソフトウェア開発に係る規定の遵守

(a) 情報システムセキュリティ責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。

1.5.2.4 主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順

遵守事項

⑴ 主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備

(a) 統括情報セキュリティ責任者は、府省庁における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を、以下の事項を含めて定めること。

(ア) 情報システムセキュリティ責任者は、全ての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要があると判断すること。

(イ) 情報システムセキュリティ責任者は、全ての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。

(ウ) 情報システムセキュリティ責任者は、全ての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。

(エ) 情報セキュリティ責任者は、全ての情報システムについて、証跡管理を行う必要性の有無を検討すること。

(オ) 情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。

(カ) 情報システムセキュリティ責任者は、証跡を取得する必要があると認められた情報システムにおいては、情報システムセキュリティ管理者及び利用者等に

対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

(キ) 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについて、保証のための対策を行う必要性の有無を検討すること。

⑵ 主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の遵守

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、府省庁における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定に基づいて、情報システムの導入を行うこと。

⑶ 取得した証跡の点検、分析及び報告

(a) 情報システムセキュリティ責任者は、証跡を取得する必要があると認められた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析することの必要性の有無を検討し、必要と認めたときは、当該措置を講じ、その結果に応じて必要な情報セキュリティ対策を講じ、又は情報セキュリティ責任者に報告すること。

1.5.2.5 暗号と電子署名の標準手順

遵守事項

⑴ 暗号と電子署名に係る規定の整備

(a) 統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び運用方法を、以下の事項を含めて定めること。

(ア) 電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。

(ウ) アルゴリズムが危殆化した場合の緊急対応計画の必要性の有無を検討し、必要と認めたときは、緊急対応計画を定めること。

(b) 統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）から（ウ）の手順（以下「鍵の管理手順等」という。）を定めること。

(ア) 鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等

(イ) 鍵の保存手順

(ウ) 鍵のバックアップ手順

(c) 統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズ

ム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。

(2) 暗号と電子署名に係る規定の遵守

(a) 行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

(b) 行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

(c) 行政事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

1.5.2.6 府省庁外の情報セキュリティ水準の低下を招く行為の防止

遵守事項

(1) 措置についての規定の整備

(a) 統括情報セキュリティ責任者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。

(2) 措置についての規定の遵守

(a) 行政事務従事者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。

1.5.2.7 ドメイン名の使用についての対策

遵守事項

(1) ドメイン名の使用についての規定の整備

(a) 統括情報セキュリティ責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）の使用について、以下の事項を行政事務従事者に求める規定を整備すること。

(ア) 行政事務従事者は、府省庁外の者（国外在住の者を除く。以下本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。

- .go.jp で終わるドメイン名

  ただし、電子メール送信又は政府ドメイン名のウェブページでの掲載に限り以下の条件を満たす場合には、政府ドメイン名以外のドメイン名を府省庁以外のものとして告知してもよい。

  具体的には、電子メールの送信においては以下の条件を全て満たすことが必要である。

- 告知内容についての問い合わせ先として政府ドメイン名による電子メールアドレスを明記しているか、又は政府ドメイン名による電子署名をしていること。
- 告知するドメイン名を管理する組織名を明記すること。
- 告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。

  また、政府ドメイン名のウェブページでの掲載においては以下の条件を全て満たすことが必要である。

- 告知するドメイン名を管理する組織名を明記すること。
- 告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。

(イ) 行政事務従事者は、府省庁外の者に対して、送信に使用する電子メールのドメイン名は、政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合を除く。

(ウ) 行政事務従事者は、府省庁外の者に対して、アクセスさせることを目的として情報を保存するためにサーバを使用する場合には、政府ドメイン名のサーバだけを使用すること。

(2) ドメイン名の使用についての規定の遵守

(a) 行政事務従事者は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。

1.5.2.8 不正プログラム感染防止のための日常的実施事項

遵守事項

(1) 不正プログラム対策に係る規定の整備

(a) 統括情報セキュリティ責任者は、不正プログラム感染の回避を目的として、以下の措置を行政事務従事者に求める規定を整備すること。

(ア) 行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

(イ) 行政事務従事者は、アンチウイルスソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

(ウ) 行政事務従事者は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にすること。

(エ) 行政事務従事者は、アンチウイルスソフトウェア等により定期的に全ての電子ファイルに対して、不正プログラムの有無を確認すること。

(オ) 行政事務従事者は、外部からデータやソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

(カ) 行政事務従事者は、不正プログラム感染の予防に努めること。

(キ) 行政事務従事者は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講ずること。

(2) 不正プログラム対策に係る規定の遵守

(a) 行政事務従事者は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。