資料４－３

政府機関の情報セキュリティ対策のための統一基準（２００５年項目限定版）

平成１７年９月１５日

情報セキュリティ政策会議決定(案)

目次

第１部　総則

1.1.1 本統一基準の位置付け

(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基準の位置付け

各府省庁の情報セキュリティの確保については、各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強化に関する基本方針（平成１７年９月 XX 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、各府省庁の情報セキュリティ水準の斉一的な引き上げを図ることが必要である。そこで本統一基準は、この政府機関統一的な枠組みの中で、各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捉え、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。本統一基準については、これを各府省庁においてそれぞれの府省庁の特性を踏まえた上で情報セキュリティ対策基準（以下「省庁対策基準」という。）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、各府省庁においては、本統一基準が更新された場合、その内容を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、法令及び規制等（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、これらの関係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。

1.1.2 本統一基準の使い方

(1) 本統一基準と省庁対策基準との関係

本統一基準は、すべて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。各府省庁においては、本統一基準で定められた以上の情報セキュリティ確保を目標として、現行の情報セキュリティ関係規程について必要な見直しを行うものとする。したがって、各府省庁において、本統一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。各府省庁は、各府省庁の特性を踏まえつつ、情報セキュリティ関係規程に盛り込むべき内容を決定し、本統一基準を直接参照する、本統一基準をそのまま取り込む、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。

(2) 適用対象範囲

本統一基準が適用される対象範囲を以下のように定める。

(a) 本統一基準は、「情報」を守ることを目的に作成されている。本統一基準において「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、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。

(b) 本統一基準は、行政事務従事者のうち、情報及び情報システムを取り扱う者に適用される。なお、本統一基準中、特に断りがないものを除き、「行政事務従事者」とは、情報及び情報システムを取り扱う行政事務従事者をいう。

(c) 本統一基準における「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）、防衛庁、金融庁、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、国土交通省及び環境省をいう。

(3) 全体構成

本統一基準は、部、節及び項の３つの階層によって構成される。

本統一基準は、情報セキュリティ対策を「組織と体制の構築」、「情報についての対策」、「セキュリティ要件の明確化に基づく対策」、「情報システムについての対策」、「個別事項についての対策」に部として分類し、さらに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。

(a) 「組織と体制の構築」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、違反や例外措置などの組織として構築すべき課題を取り上げ、組織としての運用に関係する各職員の権限と責務を明確にする。

(b) 「情報についての対策」では、情報の作成、利用、保存、移送、提供及び消去等といった情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、各職員が業務の中で常に実施する情報保護の対策を示す。

(c) 「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など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遵守すべき

事項を定め、情報システムにおいて講ずべき対策を示す。

(d) 「情報システムについての対策」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、それぞれ遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。

(e) 「個別事項についての対策」では、業務の外部委託や政府部外での情報処理等の、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、それぞれ遵守すべき事項を定める。

(4) 対策項目の記載事項

本統一基準では、各府省庁が行うべき対策基準について対策項目ごとに、遵守事項を示す。

(5) 対策レベルの設定

情報セキュリティ対策においては、対象となる情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様ではない。また、該当する情報システム及び業務の特性に応じて、各対策項目で適切な強度の対策を実施すべきである。したがって、本統一基準においては、各対策項目で対策の強度に段階を設け、採るべき遵守事項を定めている。この段階を「対策レベル」と呼び、以下のように定義する。

(a) 「基本遵守事項」は、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

(b) 「強化遵守事項」は、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、各府省庁において、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

以上より、各府省庁は、基本遵守事項以上の対策を実施することとなるが、当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない。

なお、対策項目によっては、強度にかかわらず実施されるべき対策もあるため、その場合には対策レベルは設けていない。

(6) 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みを実施できるものであることが重要である。したがって、各府省庁においては本統一基準に基づき、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) 各府省庁の基準が統一基準に準拠した内容となっていること。(設計の遵守性確認)

(b) 実際の運用が各府省庁の基準に準拠していること。(運用の遵守性確認)

(c) 情報セキュリティ関係規程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、各府省庁の情報セキュリティ監査においては、設計及び運用の遵守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（整備）及び運用（実施）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、自己点検を活用することによって、各自における対策の実効性を確保するためである。したがって、各府省庁が監査を行う際には、その自己点検の適正さを確認し、運用の実施状況の把握に用いるものとする。

また、情報セキュリティ対策の実施については、原則として、各府省庁の責任において運用することが大前提であるが、政府全体としての情報セキュリティ対策推進の観点から、各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。さらに、内閣官房情報セキュリティセンターは、本統一基準の評価指標に基づき、各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的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各府省庁と協議して定めるものとする。

1.1.3 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。
- 「アプリケーション」とは、オペレーティングシステム上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。
- 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。
- 「暗号化」とは、第三者に容易に解読されないよう、あらかじめ定められた演算を施しデータを変換することをいう。
- 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したハードウェア、ソフトウェア、ファームウェア及びそれらの組合せをいう。
- 「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。
- 「委託先」とは、情報システムに関する企画、開発、保守及び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。
- 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。
- 「ウェブサーバ」とは、HTTP サーバアプリケーション、当該サーバアプリケーションで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のよう

にウェブサーバと一体として動作するハードウェアをいう。

- 「受渡業者」とは、安全区域内で職務に従事する行政事務従事者との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

【か】

- 「外部委託」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を政府部外の者に請け負わせることをいう。
- 「外部記録媒体」とは、情報機器から取り外しすることが可能な記録装置（磁気テープ、磁気ディスク、光ディスク、カセットテープ、MO、フロッピーディスク及び USB メモリ等）をいう。
- 「可用性」とは、情報へのアクセスを認可された者が、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。
- 「可用性１情報」とは、可用性２情報以外の情報をいう。
- 「可用性２情報」とは、行政事務で取り扱う情報のうち、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。
- 「完全性１情報」とは、完全性２情報以外の情報をいう。
- 「完全性２情報」とは、行政事務で取り扱う情報のうち、その改ざん、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をいう。
- 「機密性」とは、情報に関して、アクセスを認可さ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。
- 「機密性１情報」とは、機密性２情報又は機密性３情報以外の情報をいう。
- 「機密性２情報」とは、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、直ちに一般に公表することを前提としていない情報をいう。
- 「機密性３情報」とは、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をいう。
- 「強制アクセス制御 (MAC：Mandatory Access Control)」とは、主体が客体に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それを保護すべき対象ではないものとすることはできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。
- 「行政事務従事者」とは、政府職員、請負業者、外部委託先その他行政事務の遂行に係る者のうち、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をいう。
- 「業務用電子メール」とは、各府省庁が運営又は外部委託した電子メールサーバによ

り提供される電子メールサービスをいう。

- 「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、利用状況などを考慮して、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をいう。
- 「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。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
- 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造又は提供元等から公開されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公開されたセキュリティホール等が該当する。
- 「公開されていないセキュリティホール」とは、ソフトウェアの提供元等からセキュリティホール情報が公開されていないようなセキュリティホールのことであり、パッチなども提供されていないことが想定される。

【さ】

- 「サーバ装置」とは、通信回線等を経由して接続してきた電子計算機に対して、自らが保持しているサービスを提供する電子計算機をいう。
- 「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。
- 「サービス不能攻撃」とは、セキュリティホールを悪用しサーバ装置若しくは通信回線装置のソフトウェアを動作不能にさせること、又はサーバ装置、通信回線装置若しくは通信回線の容量を上回る大量のアクセスを意図的に行い通常の利用者のサービス利用を妨害する攻撃をいう。
- 「最小特権機能」とは、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。
- 「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、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。
- 「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、磁気テープカードやＩＣカード等がある。
- 「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、省庁基準及び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実施手順をいう。
- 「情報セキュリティ対策」とは、情報に関してその機密性、完全性及び可用性を維持することをいい、策定・導入、運用、評価、見直しの各サイクルで実施すべき情報セキュリティに関する取組みの全体をいう。
- 「情報の移送」とは、府省庁外に、電磁的に記録された情報を送信すること及び情報を記録した外部記録媒体や PC 並びに書面に印刷された情報を運搬することをいう。
- 「政府職員」とは、人事発令を受けて行政事務に従事する者をいう。
- 「セキュリティホール」とは、オペレーティングシステム又はアプリケーション等に存在し、それら自身や処理する情報のセキュリティが侵害される原因となる可能性のある問題をいう。
- 「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】

- 「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。
- 「耐タンパー性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。
- 「端末」とは、端末を利用する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をいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、電子計算機間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線をいう。
- 「通信回線装置」とは、回線の接続のために設置され、電子計算機により通信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。

- 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。
- 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。
- 「電子メールサーバ」とは、電子メールの利用者に対する電子メールの送受信のサービス及び電子メールの配送を行うアプリケーション並びにそのアプリケーションを動作させる電子計算機をいう。
- 「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、読後廃棄等をいう。

【は】

- 「パッチ」とは、発見された問題点を解決するために提供される修正用のファイルをいう。提供元によって、パッチ、ホットフィクス、サービスパック等名称が異なる。
- 「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組み合わせにより主体認証を行う方法である。
- 「府省庁外」とは、政府職員の各々が所属する府省庁が管理する庁舎の外をいう。
- 「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、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。
- 「府省庁外での情報処理」とは、府省庁の管理部外で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政府職員の各々が所属する府省庁の情報システムに接続して、情報処置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。
- 「府省庁支給以外の情報システム」とは、政府職員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 の他、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、府省庁支給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、たとえば、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、政府職員の各々が所属する府省庁が管理する庁舎の内をいう。
- 「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、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。
- 「付与」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。

【ま】

- 「無線 LAN」とは、無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a、802.11b、802.11g、Bluetooth 等が挙げられる。
- 「明示」とは、情報を取り扱うすべての者が当該情報の格付け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、情報ごとの格付けの記載を原則とするが、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けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。
- 「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。

【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。

【A～Z】

- 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネットなどの公衆回線を私設通信回線として広域化するための技術をいう。

第２部　組織と体制の構築

2.1　導入

2.1.1 組織・体制の確立

(1)　最高情報セキュリティ責任者の設置

【基本遵守事項】

(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、自らが所属する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。

(c) 最高情報セキュリティ責任者は、必要に応じ、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。

(2)　情報セキュリティ委員会の設置

【基本遵守事項】

(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、委員長及び委員を任命すること。

(b) 情報セキュリティ委員会は、情報セキュリティに関する省庁基準を策定し、最高情報セキュリティ責任者に承認を得ること。

(3)　情報セキュリティ監査責任者の設置

【基本遵守事項】

(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、省庁基準に基づき監査を行うこと。

(4)　情報セキュリティ責任者の設置

【基本遵守事項】

(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人指名すること。

(b) 情報セキュリティ責任者は、所管する部門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) 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策定し、最高情報セキュリティ責任者の承認を得ること。

(d) 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。

(e) **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。**

(f) **統括情報セキュリティ責任者は、すべ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**

【基本遵守事項】

(a) **情報セキュリティ責任者は、所管する部門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情報セキュリティ対策の管理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、すべ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**

【基本遵守事項】

(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、すべ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**

【基本遵守事項】

(a) **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) **課室情報セキュリティ責任者は、就任した時又は交代した時は、統括情報セキュリティ責任者にその旨を申告すること。**

(d) **統括情報セキュリティ責任者は、すべ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。**

2.1.2 役割の分離

(1) 兼務を禁止する役割の規定

【基本遵守事項】

(a) 情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
(ア) 承認又は許可事案の申請者とその承認者又は許可者
(イ) 監査を受ける者とその監査を実施する者

2.1.3 違反と例外措置

(1) 違反への対応

【基本遵守事項】

(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採らせること。
(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、違反者の任命権者及び統括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

【基本遵守事項】

(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ための手続きを整備すること。
(b) 行政事務従事者は、例外措置を適用する場合には、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又は情報システムセキュリティ管理者を通じて統括情報セキュリティ責任者に対して、例外措置の適用を申請し、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適用箇所（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（講じる代替手段等）
(オ) 例外措置の適用を終了したときの報告方法
(カ) 例外措置の適用を申請する理由
(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情報システムセキュリティ管理者は、行政事務従事者による例外措置の適用の申請を、定められた手続きに従って審査し、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整備し、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（講じる代替手段等）**
- **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適用箇所（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、それを終了したときに、当該例外措置の許可を与えた者にその旨を報告すること。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) **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情報システムセキュリティ管理者は、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、必要な対応を講ずること。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。**

(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を実施する者からの求めに応ずること。**

2.2 運用

2.2.1 情報セキュリティ対策の教育

(1) 行政事務従事者に対する情報セキュリティ対策教育の実施

【基本遵守事項】

(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（委託先の行政事務従事者を除く。以下この項において同じ。）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、行政事務従事者に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、行政事務従事者が毎年度最低１回、受講できるように、情報セキュリティ対策の教育を企画、立案し、その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、異動時に新しい職場等で３ヶ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、立案し、その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。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。

(g) 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。

【強化遵守事項】

(h) 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訓練の内容及び体制を整備すること。

(2) 行政事務従事者による情報セキュリティ対策教育の受講義務

【基本遵守事項】

(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規定に従って、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、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と思われる場合には、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。

【強化遵守事項】

(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。

2.2.2 事故及び障害の対応

(1) 障害等の発生に備えた事前準備

【基本遵守事項】

(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事故及び障害等（以下「障害等」という。）が発生した場合、被害の拡大を防ぐとともに、障害等から復旧するための体制を整備すること。

(b) 統括情報セキュリティ責任者は、障害等について行政事務従事者から情報セキュリティ責任者への報告手順を整備し、当該報告手段をすべ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､障害等が発生した際の対応手順を整備すること。

(d) 統括情報セキュリティ責任者は、障害等に備え、要保護情報を取り扱う情報システムのうち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、その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の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

【強化遵守事項】

(e) 統括情報セキュリティ責任者は、障害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) 障害等の発生時における報告と応急措置

【基本遵守事項】

(a) 行政事務従事者は、障害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、情報セキュリティ責任者にその旨を報告すること。

(b) 行政事務従事者は、障害等が発生した際の対応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。

(c) 行政事務従事者は、障害等が発生した場合であって、当該障害等について対応手順がないとき及びその有無を確認できないときは、その対応についての指示を受けるまで、障害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。

(3) 障害等の原因調査と再発防止策

【基本遵守事項】

(a) 情報セキュリティ責任者は、障害等が発生した場合には、障害等の原因を調査し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等についての報告を受けた場合には、その内容を審査し、再発防止策を実施するために必要な措置を講ずること。**

2.3 評価

2.3.1 情報セキュリティ対策の自己点検

(1) 自己点検に関する年度計画の策定

【基本遵守事項】

(a) 最高情報セキュリティ責任者は、年度自己点検計画を整備すること。

(2) 自己点検の実施に関する準備

【基本遵守事項】

(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準備すること。

(3) 自己点検の実施

【基本遵守事項】

(a) 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し、自らが実施すべき情報セキュリティに対する対策項目の実施の有無を確認すること。

(4) 自己点検結果の評価

【基本遵守事項】

(a) 行政事務従事者は、実施した自己点検の結果について、各自、情報セキュリティ責任者による評価を受けること。

(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による自己点検が行われていることを確認し、評価すること。

(5) 自己点検に基づく改善

【基本遵守事項】

(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、自己点検の結果を評価し、情報セキュリティ責任者に改善を指示すること。

2.3.2 情報セキュリティ対策の監査

(1) 監査計画の整備

【基本遵守事項】

(a) **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承認を得た上で、年度情報セキュリティ監査計画を整備すること。**

(2) **情報セキュリティ監査の実施に関する指示**

【基本遵守事項】

(a) **最高情報セキュリティ責任者は、年度情報セキュリティ監査計画に従って、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、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案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立案**

【基本遵守事項】

(a) **情報セキュリティ監査責任者は、年度情報セキュリティ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立案すること。**

(4) **情報セキュリティ監査を実施する者の要件**

【基本遵守事項】

(a) **情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼すること。**

(b) **情報セキュリティ監査責任者は、必要に応じて、府省庁外の者に監査の一部を請け負せること。**

(5) **情報セキュリティ監査の実施**

【基本遵守事項】

(a) **情報セキュリティ監査を実施する者は、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適切に実施すること。**

(b) **情報セキュリティ監査を実施する者は、情報セキュリティ関係規程が統一基準に準拠しているか否かを確認すること。**

(c) **情報セキュリティ監査を実施する者は、被監査部門において実施されている自己点検が年度自己点検計画に基づき正しく行われているか否か、情報セキュリティ関係規程に基づき機器の設定が行われているか否かを確認すること。また、必要に応じて、自己点検記録の査閲、機器の設定状況の点検等により、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認すること。**

(d) **情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存すること。**

(e) **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)　情報セキュリティ監査結果に対する対応

【基本遵守事項】

(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、指摘事案に対する対応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事案について、対応計画を報告すること。

(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。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

(1) セキュリティ対策の見直し

【基本遵守事項】

(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、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行うこと。**

第３部　情報についての対策

3.1　情報の格付け

3.1.1 情報の格付け

(1)　情報の格付け

【基本遵守事項】

(a) **情報セキュリティ委員会は、行政事務で取り扱う情報について、機密性、完全性及び可用性の観点による当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること。**

3.2　情報の取扱い

3.2.1 情報の作成と入手

(1)　業務以外の情報の作成又は入手の禁止

【基本遵守事項】

(a) 行政事務従事者は、行政事務の遂行以外の目的で、情報システムに係る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けの決定と取扱制限の検討

【基本遵守事項】

(a) 行政事務従事者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

(b) 行政事務従事者は、府省庁外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

(3)　格付けと取扱制限の明示

【基本遵守事項】

(a) 行政事務従事者は、情報の格付けを、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し、必要に応じて取扱制限についても明示すること。

(4)　格付けと取扱制限の継承

【基本遵守事項】

(a) 行政事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

(5)　格付けと取扱制限の変更

【基本遵守事項】

(a) 行政事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

(b) 行政事務従事者は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

3.2.2 情報の利用

(1) 業務以外の利用の禁止

【基本遵守事項】

(a) 行政事務従事者は、行政事務の遂行以外の目的で、情報システムに係る情報を利用しないこと。

(2) 格付け及び取扱制限に従った情報の取扱い

【基本遵守事項】

(a) 行政事務従事者は、利用する情報に明示された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示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) 要保護情報の取扱い

【基本遵守事項】

(a) 行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を府省庁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再配付しないこと。

【強化遵守事項】

(e) 行政事務従事者は、機密性３情報には、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、情報の格付けを下げる必要性があると思料される場合には、格付けの変更に必要な処理を行うこと。

(f) 行政事務従事者は、書面に印刷された機密性３情報には、一連番号を付し、その所在を明らかにしておくこと。

3.2.3 情報の保存

(1) 格付けに応じた情報の保存

【基本遵守事項】

(a) 情報セキュリティ責任者又は情報システムセキュリティ責任者は、電子計算機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。

(b) 行政事務従事者は、情報の格付けに応じて、情報が保存された外部記録媒体を適切に管理すること。

(c) 行政事務従事者は、情報の格付けに応じて、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、及び情報システムの設計書等情報システムに係る書面を、適切に管理すること。

【強化遵守事項】

(d) 行政事務従事者は、要機密情報を電子計算機又は外部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、要保全情報及び要安定情報について、バックアップを取得すること。

(2) 情報の保存期間
【基本遵守事項】
(a) 行政事務従事者は、電子計算機又は外部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。

3.2.4 情報の移送

(1) 情報の移送に関する許可及び届出
【基本遵守事項】
(a) 行政事務従事者は、機密性３情報を移送する場合には、情報セキュリティ責任者又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情報を移送する場合には、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。

(2) 情報の送信と運搬の選択
【基本遵守事項】
(a) 行政事務従事者は、要機密情報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決定し、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。

(3) 移送手段の選択
【基本遵守事項】
(a) 行政事務従事者は、要機密情報を移送する場合には、安全確保に留意して、当該要機密情報の移送手段を決定し、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。

(4) 書面に記載された情報の保護対策
【基本遵守事項】
(a) 行政事務従事者は、要機密情報が記載された書面を移送する場合には、情報の格付けに応じて、安全確保のための適切な措置を講ずること。

(5) 電磁的記録媒体に記録された情報の保護対策

【基本遵守事項】

(a) **行政事務従事者は、要機密情報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、電子ファイルを移送する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないかを確認すること。**

【強化遵守事項】

(d) **行政事務従事者は、要機密情報を移送する場合には、適切な強度の暗号化を行った上で、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こと。**

3.2.5 情報の提供

(1) 情報の公表

【基本遵守事項】

(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情報に格付けされるものであることを確認すること。**

(2) 他者への情報の提供

【基本遵守事項】

(a) **行政事務従事者は、機密性３情報を府省庁外の者に提供する場合には、情報セキュリティ責任者又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情報を府省庁外の者に提供する場合には、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。**

(c) **行政事務従事者は、要機密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、当該要機密情報が、自らが所属する府省庁の付した情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。**

3.2.6 情報の消去

(1) 電磁的記録の消去方法

【基本遵守事項】

(a) **行政事務従事者は、電子計算機、通信回線装置及び外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にすること。**

(b) **行政事務従事者は、初期化されていない電子計算機、通信回線装置及び外部記録**

媒体を利用する場合には、これらに保存された情報を復元が困難な状態にする必要性の有無を検討し、必要があると認めたときは，データ消去ソフトウェア又はデータ消去装置を用いて、すべての情報を復元が困難な状態にすること。

【強化遵守事項】

(c) **行政事務従事者は、電子計算機、通信回線装置及び外部記録媒体について、設置環境等から必要があると認められる場合は、データ消去ソフトウェアを用いて、当該電子計算機等の要機密情報を復元が困難な状態にし、当該電子計算機等に残留する要機密情報を最小限に保つこと。**

(2) **書面の廃棄方法**

【基本遵守事項】

(a) **行政事務従事者は、要機密情報が記録された書面を廃棄する場合には、復元できない方法を用いること。**

第４部　情報セキュリティ要件の明確化に基づく対策

4.1　情報セキュリティについての機能

4.1.1 主体認証

(1)　主体認証機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、すべ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性があると判断すること。

(b) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムには、識別及び主体認証を行う機能を設けること。

(c) 情報システムセキュリティ管理者は、主体認証を行う必要があると認めた情報システムであって、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

(ア) 主体認証情報を保存する場合には、その内容の暗号化を行うこと。

(イ) 主体認証情報を通信する場合には、その内容の暗号化を行うこと。

(ウ) 保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。

(d) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を情報システムに設けること。

(ア) 利用者が定期的に変更しているか否かを確認する機能

(イ) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

(e) 情報システムセキュリティ責任者は、利用者から主体認証情報又は主体認証情報格納装置を他者に使用された又は使用される危険性がある旨の報告を受けた場合には、直ちに当該主体認証情報又は主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を情報システムに設けること。

(f) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、知識による主体認証方式を用いる場合には、以下の機能を情報システムに設けること。

(ア) 利用者が、自らの主体認証情報を設定する機能

(イ) 利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

(g) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、生体情報による主体認証方式を用いる場合には、当該生体情報

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。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

(h) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、知識、所有、生体情報以外の主体認証方式を用いる場合には、以下の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。

(ア) 正当な主体以外の主体を誤って主体認証しないこと。（誤認の防止）

(イ) 正当な主体が本人の責任ではない理由で主体認証できなくならないこと。（誤否の防止）

(ウ) 正当な主体が容易に他者に主体認証情報を付与及び貸与ができないこと。（代理の防止）

(エ) 主体認証情報が容易に複製できないこと。（複製の防止）

(オ) 情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）

(カ) 主体認証について業務遂行に十分な可用性があること。（可用性の確保）

(キ) 新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）

(ク) 主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

【強化遵守事項】

(i) 情報システムセキュリティ責任者は、複数要素（複合）主体認証方式で主体認証を行う機能を情報システムに設けること。

(j) 情報システムセキュリティ責任者は、ログオンした利用者に対して、前回のログオンに関する情報を通知する機能を情報システムに設けること。

(k) 情報システムセキュリティ責任者は、不正にログオンしようとする行為を検知又は防止する機能を情報システムに設けること。

(l) 情報システムセキュリティ責任者は、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。

(m) 情報システムセキュリティ責任者は、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を情報システムに設けること。

(n) 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共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を情報システムに設けること。

(2) 行政事務従事者における識別コードの管理

【基本遵守事項】

(a) 行政事務従事者は、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、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、あらかじめ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。

【強化遵守事項】

(e) 管理者権限を持つ識別コードを付与された者は、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。

(3) 行政事務従事者における主体認証情報の管理

【基本遵守事項】

(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) 知識による主体認証情報を用いる場合には、当該主体認証情報について以下の要件を満たすこと。

(ア) 行政事務従事者は、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) 行政事務従事者は、自己の主体認証情報を他者に教えないこと。

(ウ) 行政事務従事者は、主体認証情報を忘却しないように努めること。

(エ) 行政事務従事者は、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) 行政事務従事者は、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。

(c) 所有による主体認証を用いる場合には、主体認証情報格納装置について以下の要件を満たすこと。

(ア) 行政事務従事者は、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) 行政事務従事者は、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) 行政事務従事者は、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。

4.1.2 アクセス制御

(1) アクセス制御機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、すべ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。

(b) 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムには、アクセス制御を行う機能を設けること。

【強化遵守事項】

(c) 情報システムセキュリティ責任者は、利用者等の属性以外に基づくアクセス制御を行う必要があると認めた情報システムには、当該アクセス制御の機能を追加すること。

(d) 情報システムセキュリティ責任者は、強制アクセス制御を行う必要があると認めた情報システムには、当該機能を設けること。

(2) 行政事務従事者による適正なアクセス制御

【基本遵守事項】

(a) 行政事務従事者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

4.1.3 権限管理

(1) 権限管理機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、すべ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。

(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は、権限管理を行う機能を設けること。

【強化遵守事項】

(c) 情報システムセキュリティ責任者は、最小特権機能を情報システムに設けること。

(d) 情報システムセキュリティ責任者は、主体認証情報の再発行を自動で行う機能を情報システムに設けること。

(e) 情報システムセキュリティ責任者は、デュアルロック機能を情報システムに設けること。

(2) 識別コードと主体認証情報の付与管理

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、共有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、権限管理について、以下の事項を含む手続きを明確にすること。**

(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き

(イ) 主体認証情報の初期配布方法及び変更管理手続き

(ウ) アクセス制御情報の設定方法及び変更管理手続き

(c) **情報システムセキュリティ責任者は、権限管理を行う者を定めること。**

(d) **権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。**

(e) **権限管理を行う者は、識別コードを発行する際に、それが共有識別コードか、共有ではない識別コードかの区別を利用者に通知すること。ただし、共有識別コードは、情報システムセキュリティ責任者が、その利用を認めた情報システムでのみ付与することができる。**

(f) **権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に則した場合に限定して付与すること。**

(g) **権限管理を行う者は、退職等により行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者の識別コードを無効にすること。また、人事異動等の必要時に、不要な識別コードの有無を点検すること。**

(h) **権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をすること。**

【強化遵守事項】

(i) **権限管理を行う者は、単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみを付与すること。**

(j) **権限管理を行う者は、付与した識別コードをどの主体に付与していたかの記録について、保存すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。**

(k) **権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。**

(3) 識別コードと主体認証情報における代替措置の適用

【基本遵守事項】

(a) **情報システムセキュリティ管理者は、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、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を**

停止させること。

4.1.4 証跡管理

(1) 証跡管理機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、すべ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。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、証跡管理を行う必要があると判断すること。

(b) 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た情報システムには、証跡管理のために証跡を取得する機能を設けること。

(c) 情報システムセキュリティ責任者は、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。

(d) 情報システムセキュリティ責任者は、証跡が取得できない場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。

(e) 情報システムセキュリティ責任者は、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、サーバ装置に取得した証跡についてはアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

【強化遵守事項】

(f) 情報システムセキュリティ責任者は、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。

(g) 情報システムセキュリティ責任者は、セキュリティ侵害の可能性を示す事象を検知した場合は、監視要員等にその旨を即時に通知する機能を情報システムに設けること。

(2) 行政事務従事者による証跡の取得と保存

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、情報システムセキュリティ責任者が情報システムに設けた機能を利用して、証跡を記録すること。

(b) 情報システムセキュリティ管理者は、取得した証跡の保存期間を定め、当該保存期間が満了する日まで保存すること。

(c) 行政事務従事者は、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行うこと。

(3) 取得した証跡の点検、分析及び報告

【強化遵守事項】

(a) 情報セキュリティ責任者又は情報システムセキュリティ責任者は、取得した証跡

を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ統括情報セキュリティ責任者若しくは情報セキュリティ責任者に報告すること。

(b) 監視要員等は、セキュリティ侵害の可能性を示す事象を検知した旨の通知を受けた場合には、あらかじめ定められた措置を採ること。

(4) 証跡管理に関する利用者への周知

【基本遵守事項】

(a) 情報セキュリティ責任者又は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をすること。

4.1.6 暗号と電子署名 鍵管理を含む）

(1) 暗号化機能及び電子署名の付与機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱うすべての情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

(b) 情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。

(c) 情報システムセキュリティ責任者は、要保全情報（書面を除く。以下この項において同じ。）を取り扱うすべての情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。

(d) 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。

(e) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与に用いるアルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行うこと。この際、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。なお、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。

【強化遵守事項】

(f) 情報システムセキュリティ責任者は、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。

(g) 情報システムセキュリティ責任者は、複数のアルゴリズムを選択可能とすること。

(h) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与に使用されるアルゴリズムのうち、少なくとも一つは電子政府推奨暗号リストの中から選択すること。

(i) 情報システムセキュリティ責任者は、選択したアルゴリズムが、ソフトウェアやハードウェアへ適切に実装されているか否かを確認すること。

(j) 情報システム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を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。

(2) 暗号化及び電子署名の付与に係る管理

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、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、鍵の生成手順及び有効期限を定めること。

(b) 情報システムセキュリティ責任者は、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、鍵の保存媒体及び保存場所を定めること。

(c) 情報システムセキュリティ責任者は、電子署名を付与した場合には、その正当性を検証するための情報又は手段を署名検証者へ提供すること。

【強化遵守事項】

(d) 情報システムセキュリティ責任者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップの取得方法及び鍵の預託方法を定めること。

(e) 情報システムセキュリティ責任者は、選択したアルゴリズムの危殆化に関する情報を常時収集すること。

(3) 暗号化機能及び電子署名を付与する機能の利用

【基本遵守事項】

(a) 行政事務従事者は、要機密情報を移送する場合又は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。

(b) 行政事務従事者は、要保全情報を移送する場合又は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。

(c) 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を付与された場合には、これを他者に知られないように自己管理すること。

(d) 行政事務従事者は、暗号化された情報の復号に用いる鍵を付与された場合には、そのバックアップを取得すること。

4.2 情報セキュリティについての脅威

4.2.1 セキュリティホール対策

(1) 情報システムの構築時

【基本遵守事項】

(a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の機種並びに当該電子計算機及び通信回線装置が利用しているオペレーティングシステム、ソフトウェア又はファームウェア等の種類及びバージョンに関する書面を整備すること。

(b) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の構築又は運用開始時に公開されたセキュリティホールの対策を実施すること。

【強化遵守事項】

(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、要安定情報を取り扱う情報システムについては、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。

(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、セキュリティホールが公開されていない段階においても電子計算機及び通信回線装置上でその対策を実施すること。

(2) 情報システムの運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の機種並びに当該電子計算機及び通信回線装置が利用しているオペレーティングシステム、ソフトウェア又はファームウェア等の種類及びバージョンに変更があった場合には、関連する書面を更新すること。

(b) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、管理対象となる電子計算機及び通信回線装置等に関連する公開されたセキュリティホールの情報を適宜入手すること。

(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、入手したセキュリティホール情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。

(ア) 対策の必要性
(イ) 対策方法
(ウ) 対策方法が存在しない場合の一時的な回避方法
(エ) 対策方法又は回避方法が情報システムに与える影響
(オ) 対策の実施予定
(カ) 対策テストの必要性

(キ) 対策テストの方法
(ク) 対策テストの実施予定

(d) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

(e) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者等を記録すること。

(f) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、信頼できる方法で対策用ファイルを入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

【強化遵守事項】

(g) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

(h) 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、入手したセキュリティホール情報及び対策方法に関して、他の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と共有すること。

4.2.2 不正プログラム対策

(1) 情報システムの構築時

【基本遵守事項】

(a) 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た行政事務従事者に対する留意事項を含む日常的実施事項を定めること。

(b) 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、電子計算機にアンチウイルスソフトウェア等を導入すること。

(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、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。

【強化遵守事項】

(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、想定される不正プログラムの感染経路において、異なる業者のアンチウイルスソフトウェア等を組み合わせ、導入すること。

(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、不正プログラムが通信により拡散することを防止するための対策を実施すること。

(2) 情報システムの運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段

の対処が必要な場合には、行政事務従事者にその対処の実施に関する指示を行うこと。

(b) 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る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。

(c) 行政事務従事者は、アンチウイルスソフトウェア等にかかわ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。

(d) 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。

(e) 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すべ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。

(f) 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、必ず不正プログラム感染の有無を確認すること。

(g) 行政事務従事者は、ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

(h) 情報セキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。

【強化遵守事項】

(i) 情報セキュリティ責任者は、アンチウイルスソフトウェア等では検知されない新種の不正プログラムに感染した等、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくこと。

4.2.3 サービス不能攻撃対策

(1) 電子計算機、通信回線装置及び通信回線がインターネットからのアクセスを受ける情報システムの構築時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要とするサーバ装置及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

【強化遵守事項】

(b) 情報システムセキュリティ責任者は、サービス不能攻撃を受けた場合、通信回線装置や通信回線を共用している他サービスや内部からインターネットへのアクセスにも影響を及ぶことを考慮して通信回線装置及び通信回線の構築を行うこと。

(c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監

視対象を特定し、監視方法を定めること。

(d) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除又は低減する対策装置を導入すること。**

(e) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。**

(f) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機、通信回線装置及び通信回線を冗長構成にすること。**

(g) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービスを提供しているサーバ装置や通信回線装置だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を定めておくこと。**

(2) **電子計算機及び通信回線がインターネットからのアクセスを受ける情報システムの運用時**

【強化遵守事項】

(a) **情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。**

(b) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、前事項の記録をサービス不能攻撃の検知精度向上等に反映すること。**

(c) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、定期的にサービス不能攻撃の対策の見直しを行うこと。**

第５部　情報システムについての対策

5.1　施設と環境

5.1.1 電子計算機及び通信回線装置を設置する安全区域

(1)　立入り及び退出の管理

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。**

【強化遵守事項】

(b) **情報システムセキュリティ責任者は、安全区域をセキュリティレベルが異なる区域から物理的に隔離し、立入り及び退出が可能な場所を制限する措置を講ずること。**

(c) **情報システムセキュリティ責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。**

(d) **情報システムセキュリティ責任者は、安全区域から退出する者の主体認証を行うための措置を講ずること。**

(e) **情報システムセキュリティ責任者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ､及び安全区域から退出させない措置を講ずること。**

(f) **情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を承認する手続きを整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載した書面を整備すること。**

(g) **情報システムセキュリティ責任者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の書面へ反映させること。また、当該変更の記録を保存すること。**

(h) **情報システムセキュリティ責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。**

(2)　訪問者及び受渡業者の管理

【強化遵守事項】

(a) **情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。**

(b) **情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。**

(c) **情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の行政事務従事者が訪問者の安全区域への立入りについて承認するための措置を講ずること。**

(d) **情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。**

(e) **情報システムセキュリティ責任者は、安全区域内において訪問相手の行政事務従事者が訪問者に付き添うための措置を講ずること。**

(f) **情報システムセキュリティ責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。**

(g) **情報システムセキュリティ責任者は、訪問者の立入りを監視するための措置を講ずること。**

(h) **情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。**

(ア) 安全区域外で受渡しを行うこと。

(イ) 業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、電子記録媒体、書面に触れることができない場所に限定し、行政事務従事者が立ち会うこと。

(3) **電子計算機及び通信回線装置のセキュリティ確保**

【強化遵守事項】

(a) **情報システムセキュリティ責任者は、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。**

(b) **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は、設置及び利用場所が確定している電子計算機及び通信回線装置を所定の設置場所から移動できない措置を講ずること。**

(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情報システムについては、安全区域内で利用するモバイル PC の盗難を防止するための措置を講ずること。**

(d) **情報システムセキュリティ責任者は、行政事務従事者が離席時に電子計算機及び通信回線装置を不正操作及び盗み見から保護するための措置を講ずること。**

(e) **情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。**

(f) **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は、情報システムで利用する電源ケーブル又は通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。**

(g) **情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電磁波による情報漏えい対策の措置を講ずること。**

(4) **安全区域内のセキュリティ管理**

【基本遵守事項】

(a) **行政事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。**

【強化遵守事項】

(b) **行政事務従事者は、情報システムセキュリティ責任者の承認を得た上で、情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。**

(c) **情報システムセキュリティ責任者は、安全区域への持込み及び安全区域からの持出しについて、持込み及び持出しをした者、日時、物品及び事由を含む事項について記録すること。**

(d) **情報システムセキュリティ責任者は、情報システムに関連しない電子計算機、通信回線装置、電子記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。**

(e) **行政事務従事者は、要保護情報を含む電子記録媒体及び書類については、机上に放置したままで、離席しないこと。**

(f) **情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。**

(5) **災害及び障害への対策**

【強化遵守事項】

(a) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。**

(b) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、安全区域内において災害及び障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。**

5.2　電子計算機

5.2.1 電子計算機共通対策

(1)　電子計算機の設置時

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。**

(b) **情報システムセキュリティ責任者は、すべての電子計算機に対して、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ための文書を整備すること。**

(c) **情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。**

(d) **情報システムセキュリティ責任者は、利用者が電子計算機にログオンする場合には主体認証を行うように電子計算機を構成すること。ただし、識別コードを複数の利用者で共有することにつき合理的な理由がある場合であって、情報システムセキュリティ責任者の承認を得たとき、及び主体認証機能を付加できない端末の場合であって、利用者が電子計算機を専有するときは、この限りでない。**

(e) **情報システムセキュリティ責任者は､ログオンした利用者の識別コードに対して、権限管理を行うこと。**

(f) **情報システムセキュリティ責任者は、電子計算機上で動作するオペレーティングシステム及びアプリケーションに存在する公開されたセキュリティホールから電子計算機を保護するための対策を講ずること。**

(g) **情報システムセキュリティ責任者は、攻撃者により送り込まれる公開された不正プログラムから電子計算機を保護するための対策を講ずること。**

(h) **情報システムセキュリティ管理者は、電子計算機関連文書を整備すること。**

(i) **情報システムセキュリティ責任者は、電子計算機を安全区域に設置すること。ただし、情報セキュリティ責任者の承認を得た場合は、この限りでない。**

(j) **情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にすること。**

(2)　電子計算機の運用時

【基本遵守事項】

(a) **情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。**

(b) **情報システムセキュリティ責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。**

(c) **行政事務従事者は、行政事務の遂行以外の目的で電子計算機を利用しないこと。**

(d) 情報システムセキュリティ責任者は、電子計算機を管理する行政事務従事者及び利用者を変更した場合には、当該変更の内容を、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ための文書へ反映すること。また、当該変更の記録を保存すること。

(e) 情報システムセキュリティ責任者は、電子計算機のセキュリティレベルを維持するため、公開されたセキュリティホールから電子計算機を保護するための対策を講ずること。

(f) 情報システムセキュリティ責任者は、電子計算機のセキュリティレベルを維持するため、攻撃者により送り込まれる公開された不正プログラムから電子計算機を保護するための対策を講ずること。

(g) 情報システムセキュリティ管理者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

【強化遵守事項】

(h) 情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されているすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある電子計算機を検出した場合には、当該不適切な状態の改善を図ること。

(i) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、情報システムにおいて基準となる時刻に、すべての電子計算機の時刻を同期すること。

(3) 電子計算機の運用終了時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要機密情報を取り扱う電子計算機については、電子計算機の運用を終了する場合に、データ消去ソフトウェア又はデータ消去装置の利用、若しくは物理的な破壊又は磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にすること。

5.2.2 端末

(1) 端末の設置時

【基本遵守事項】

(a) 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、端末にインストールしてはならないソフトウェアを定めること。

(b) 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モバイル PC については、府省庁外で使われる際にも、府省庁内で利用される端末と同等の保護手段が有効に機能するように構成すること。

(c) 行政事務従事者は、モバイル PC を利用する必要がある場合には、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の承認を得ること。

(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、要機密情

報を取り扱うモバイル PC については、内蔵記録媒体に保存される情報の暗号化を行う機能を付加すること。

【強化遵守事項】

(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、行政事務従事者が情報を保存できない端末を用いて情報システムを構築すること。

(2) 端末の運用時

【基本遵守事項】

(a) モバイル PC を利用する行政事務従事者は、要保護情報を取り扱う情報モバイル PC については、盗難防止措置を行うこと。

(b) 行政事務従事者は、要機密情報を取り扱うモバイル PC については、モバイル PC を府省庁外に持ち出す場合に、当該モバイル PC の内蔵記録媒体に保存されている要機密情報の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、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接続許可を与えた通信回線以外に端末を接続しないこと。

5.2.3 サーバ装置

(1) サーバ装置の設置時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、サーバ装置へのリモートログインについて、通信回線で送受信される情報の機密性を確保すること。

(b) 情報システムセキュリティ責任者は、主たるサービスの提供に必要のないサービスを停止し、また、必要なサービスであっても、利用しない機能を無効化して提供すること。

(2) サーバ装置の運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、サーバ装置の構成の変更を監視すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定すること。

(b) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

(c) 情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

(d) 情報システムセキュリティ管理者は、サーバ装置の障害について、障害発生日、障害を受けたサーバ装置、障害の内容、対策及び復旧作業内容並びに作業者を含

む事項を記録すること。

【強化遵守事項】

(e) **情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。**

(f) **情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム性能を監視し、当該サーバ装置に関するトラブルの発生を検知すること。**

(g) **情報システムセキュリティ責任者は、サーバ装置上で記録されるログについて、記録対象、記録項目、保存期間及び保存方法を含む事項を定め、当該ログの記録と保管を情報システムセキュリティ管理者に実施させること。**

(h) **情報システムセキュリティ管理者は、記録されたログの内容を定期的に確認、分析し、情報セキュリティ事象の発生を推測し又は検知すること。**

5.3 アプリケーションソフトウェア

5.3.1 通信回線を介して提供するアプリケーション共通対策

(1) サービスの導入時

【基本遵守事項】

(a) 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、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規定を整備すること。

(2) サービスの運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、サービスのセキュリティ維持に関して整備した規定に基づいて、日常的及び定期的に運用管理を実施すること。

(b) 行政事務従事者は、通信回線を介して提供されるサービスを私的な目的のために利用しないこと。

5.3.2 電子メール

(1) 電子メールの導入時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

【強化遵守事項】

(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの送受信時における行政事務従事者の主体認証を行う機能を備えること。

(2) 電子メールの運用時

【基本遵守事項】

(a) 行政事務従事者は、業務遂行にかかわる情報を含む電子メールを送受信する場合には、業務用電子メールを利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

(b) 行政事務従事者は、受信したメールを電子メールクライアントにおいてテキストとして表示すること。

5.3.3 ウェブ

(1) ウェブの導入時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。

(b) 情報システムセキュリティ責任者は、ウェブサーバからウェブクライアントに不必要な情報を送信しないように情報システムを構築すること。

(c) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、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。

【強化遵守事項】

(d) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。

(e) 情報システムセキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。

(2) ウェブの運用時

【基本遵守事項】

(a) 行政事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

【強化遵守事項】

(b) 情報システムセキュリティ責任者は、行政事務従事者が閲覧することが可能なホームページを制限し、定期的にその見直しを行うこと。

5.4 通信回線

5.4.1 通信回線共通対策

(1) 通信回線を構築する場合

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。

(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

(c) 情報システムセキュリティ責任者は、通信回線及び通信回線装置関連文書を整備すること。

(d) 情報システムセキュリティ責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

(e) 情報システムセキュリティ責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。

(f) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の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。

(g) 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は､通信回線に利用する物理的な回線のセキュリティを検討し､選択すること。

(h) 情報システムセキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

(i) 情報システムセキュリティ責任者は、通信回線装置に存在する公開されたセキュリティホールから通信回線装置を保護するための対策を講ずること。

(j) 情報システムセキュリティ責任者は、通信回線装置を安全区域に設置すること。また、損傷及び盗聴を含む脅威から通信ケーブルを保護するための対策を講ずること。

(k) 情報システムセキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

【強化遵守事項】

(l) 情報システムセキュリティ責任者は、通信を行う電子計算機の主体認証を行うこと。

(m) 情報システムセキュリティ責任者は、通信回線を用いて送受信される情報を記録すること。

(n) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについ

ては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること。

(2)　通信回線を運用する場合

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、通信回線を利用する電子計算機の識別コード及び電子計算機を利用する者と当該利用者の識別コードの対応並びに通信回線の利用部局を含む事項の管理を行うこと。

(b) 情報システムセキュリティ管理者は、通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項を変更した場合には、当該変更の内容を通信回線及び通信回線装置関連文書へ反映すること。また、当該変更の記録を保存すること。

(c) 情報システムセキュリティ責任者は、通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項の他者による変更を監視すること。また､当該変更によって生ずる通信回線のセキュリティへの影響を特定すること。

(d) 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の確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。

(e) 行政事務従事者は、情報システムセキュリティ責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。

(f) 情報システムセキュリティ責任者は、通信回線装置のセキュリティレベル維持のため、公開されたセキュリティホールから通信回線装置を保護するための対策を講ずること。

(g) 情報システムセキュリティ責任者は、情報システムにおいて基準となる時刻に、すべての通信回線装置の時刻を同期するための措置を講ずること。

(3)　通信回線の運用停止時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線装置の利用を停止する場合には、通信回線装置の内蔵記録媒体の情報を復元が困難な状態にすること。

5.4.2 府省庁内通信回線の管理

(1)　府省庁内通信回線を構築する場合

【強化遵守事項】

(a) 情報システムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認するための措置を講ずること。

(2)　府省庁内通信回線を運用する場合

【強化遵守事項】

(a) 情報システムセキュリティ責任者は、通信要件の変更に際し又は定期的に、アクセス制御の設定の見直しを行うこと。

(b) 情報システムセキュリティ責任者は、定期的に、通信回線及び通信回線装置のセキュリティホールを検査すること。

(c) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況を確認、分析し、情報セキュリティ事象の発生を推測又は検知すること。

(d) 情報システムセキュリティ管理者は、府省庁内通信回線上を送受信される通信内容を監視すること。

(3)　回線の対策

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、VPN を利用する場合には、以下に挙げる事項を含む措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) VPN 経由でアクセスすることが可能な通信回線の範囲の制限

(カ) VPN 接続方法の機密性の確保

(キ) VPN を利用する電子計算機の管理

(b) 情報システムセキュリティ責任者は、無線ＬＡＮを利用する場合には、以下に挙げる事項を含む措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) 無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限

(カ) 無線 LAN に接続中に他の通信回線との接続の禁止

(キ) 無線 LAN 接続方法の機密性の確保

(ク) 無線 LAN に接続する電子計算機の管理

(c) 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセスを利用する場合には、以下に挙げる事項を含む措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信を行う者又は発信者番号による識別及び主体認証

(ウ) 主体認証記録の取得及び管理

(エ) リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限

(オ) リモートアクセス中に他の通信回線との接続の禁止

(カ) リモートアクセス方法の機密性の確保
(キ) リモートアクセスする電子計算機の管理

5.4.3 府省庁外通信回線との接続

(1)　府省庁内通信回線を府省庁外通信回線と接続する場合
【基本遵守事項】

(a) **情報システムセキュリティ責任者は、情報セキュリティ責任者の承認を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。**
(b) **情報セキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。**

(2)　府省庁外通信回線と接続している府省庁内通信回線を運用する場合
【基本遵守事項】

(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の確保が困難な事由が発生した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線に構成を変更すること。**
(b) **情報システムセキュリティ責任者は、通信回線の変更に際し又は定期的に、アクセス制御の設定の見直し行うこと。**
(c) **情報システムセキュリティ責任者は、定期的に、府省庁外通信回線から通信することが可能な府省庁内通信回線及び通信回線装置のセキュリティホールを検査すること。**
(d) **情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況を確認、分析し、情報セキュリティ事象の発生を推測又は検知すること。**
(e) **情報システムセキュリティ管理者は、府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容を監視すること。**

第６部　個別事項についての対策

6.1　個別事項

6.1.1 外部委託

(1)　府省庁内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

(a) 統括情報セキュリティ責任者は、外部委託の対象とする情報システム及び委託先による部門内の情報資産へアクセスすることが可能な範囲を明確化すること。

(b) 統括情報セキュリティ責任者は、委託先の選定手続、選定基準及び委託先が具備すべき要件（委託先職員に対する情報セキュリティ対策の実施を含む。）を整備すること。

【強化遵守事項】

(c) 統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

(d) 統括情報セキュリティ責任者は、前事項の評価方法に従って、求める情報セキュリティ要件に対する委託先の候補者の情報セキュリティ水準を確認し、委託先の選定基準の一要素として利用すること。

(2)　委託先に適用する情報セキュリティ対策の整備

【基本遵守事項】

(a) 情報システム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手順を整備すること。

(b) 情報システムセキュリティ責任者は、委託先の情報セキュリティ対策への履行状況を確認するための評価基準を策定し、遵守すべき情報セキュリティ対策の履行が不十分である場合の措置に関して委託先に事前に通知すること。

(3)　外部委託の実施における手続きの遵守

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、外部委託を実施する際に、情報セキュリティ関係規程に基づく情報セキュリティ対策の遵守、機密の保持（情報の目的外利用の禁止等を含む。）、委託先に請け負わせる業務における情報セキュリティ侵害発生時の対処手順の遵守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措置の遵守を含む外部委託に伴う契約書等を取り交わすこと。また、必要に応じて、以下の事項を含めること。

(ア) 情報セキュリティ監査を受け入れること。

(イ) 提供されるサービスレベルに関して委託先に保証させること。

(b) 情報システム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に含めること。

(ア) 遵守すべき情報セキュリティ対策を実現するために、委託先における所属職員が実施する具体的な取組内容

(イ) 外部委託した業務の作業に携わる者の特定とそれ以外の者による作業の禁止

(c) 情報システムセキュリティ責任者は、外部委託契約の継続に関しては、選定手続、選定基準及び委託先が具備すべき要件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は、委託先の提供するサービス（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、選定手続、選定基準及び委託先が具備すべき要件に基づき、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は、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負する合理的理由が認められる場合は、その限りではない。

(f) 行政事務従事者は、委託先が要機密情報を取り扱う場合、以下の実施手順に従うこと。

(ア) 委託先に情報を移送する場合は、不要部分のマスキングや暗号化等安全な受け渡し方法により実施し、移送した記録を保存すること。

(イ) 外部委託の業務終了等により情報が不要になった場合には、確実に返却又は廃棄させること。

6.1.2 府省庁外での情報処理の制限

(1) 安全管理措置の整備

【基本遵守事項】

(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府省庁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

【基本遵守事項】

(a) 行政事務従事者は、要保護情報（機密性２情報を除く。）について府省庁外で情報処理を行う場合には、情報セキュリティ責任者又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情報について府省庁外で情報処理を行う場合には、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。

(c) **情報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（機密性２情報を除く。）について府省庁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、対応を講ずること。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情報について府省庁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、対応を講ずること。**

(f) **行政事務従事者は、要保護情報について府省庁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、要保護情報（機密性２情報を除く。）を取り扱う情報システムを府省庁外に持ち出す場合には、情報セキュリティ責任者又は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情報を取り扱う情報システムを府省庁外に持ち出す場合には、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。**

(i) **情報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府省庁外への持出しに係る記録を取得すること。**

(j) **情報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（機密性２情報を除く。）を取り扱う情報システムを府省庁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、対応を講ずること。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情報を取り扱う情報システムを府省庁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、対応を講ずること。**

(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府省庁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出しにとどめること。**

(3) **安全管理措置の遵守**

【基本遵守事項】

(a) **行政事務従事者は、要保護情報（機密性２情報を除く。）について府省庁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、要保護情報（機密性２情報を除く。）について府省庁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府省庁外への持出しに**

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、要保護情報（機密性２情報を除く。）を取り扱う情報システムを府省庁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。

6.1.3 府省庁支給以外の情報システムによる情報処理の制限

(1) 安全管理措置の整備

【基本遵守事項】

(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

【基本遵守事項】

(a) 行政事務従事者は、要保護情報（機密性２情報を除く。）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、情報セキュリティ責任者又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、情報セキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。

(c) 情報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（機密性２情報を除く。）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、対応を講ずること。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、対応を講ずること。

(3) 安全管理措置の遵守

【基本遵守事項】

(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、原則として、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、要保護情報（機密性２情報を除く。）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。

6.2 その他

6.2.1 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

(1) 措置の徹底

【基本遵守事項】

(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。

(b) 行政事務従事者は、原則として、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を講ずること。