独立行政法人Ａ機構の
情報セキュリティ対策のための管理基準
(政府機関統一管理基準 K304-101 版ベース)
解説書

本書において、空色マーカ部分は、必ず書き換えが必要な箇所、黄色マーカ部分は、書き換えについて検討をするとよいと思われる箇所をマークしたものです。これらが書き換えを要するすべてではありませんが、参考にしてください。

独立行政法人Ａ機構

目次

第 1.1 部　総則

1.1.1.1 本管理基準及び技術基準の位置付け

(1) 本管理基準及び技術基準の位置付け

～～～～～。

(2) 本管理基準及び技術基準の改訂

～～～～～。

(3) 法令等の遵守

～～～～～。

解説：B 省が所管する独立行政法人等群における既存の決定等については本書別添資料 A.1.3 を参照。

1.1.1.2 本管理基準及び技術基準の使い方

(1) 全体構成

本管理基準及び技術基準は、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、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、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職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、各段階において各職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、独立行政法人Ａ機構外での情報処理及び独立行政法人Ａ機構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、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、遵守すべき事項を技術基準において定めている。

(2) 対策項目の記載事項

本管理基準及び技術基準では、対策項目ごとに遵守事項を示す。

(3) 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、本管理基準及び技術基準においては、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、独立行政法人Ａ機構が、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

以上により、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。

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

職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、職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。

解説：情報の格付及び取扱制限の実施方法については、「行政機関の保有する情報の公開に関する法律」（以下「情報公開法」という。）に基づき独立行政法人Ａ機構において定めている「処分に係る審査基準」や文書管理規程等を参考に決めるとよい。

なお、情報の格付及び取扱制限については、独立行政法人Ａ機構における情報セキュリティ対策基準の施行日以後に作成又は入手した全ての情報について適用するものであり、施行日前に作成又は入手した情報について一括して処理することを求めているものではない。しかし、施行日前に作成又は入手した情報についても、適宜その決定を行うことが望ましいことから、当該情報を施行日以後取り扱う際に、格付及び取扱制限を行う必要がある。

(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管理基準の遵守事項で用いるが、独立行政法人Ａ機構において、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、独立行政法人Ａ機構の対策基準における格付区分と遵守事項との関係が本管理基準及び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、他の独立行政法人Ａ機構との情報のやり取りをする際に、自身の格

付区分が本管理基準及び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、他の独立行政法人A機構に情報を提供する際に、本管理基準及び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	職務で取り扱う情報のうち、機密が損なわれることにより、職務の遂行に支障を及ぼすおそれがある情報であって、情報を格付けした者だけが、当該情報についての参照を許可される者を特定する必要のある情報
機密性２情報	職務で取り扱う情報のうち、機密が損なわれることにより、職務の遂行に支障を及ぼすおそれがある情報であって、情報について参照を許可された者が、（機密保持契約書締結等による）予め定めた手続きに従うことで、当該情報について開示することができる情報
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。

解説：機密性の格付については、文書管理規程上の秘密文書に相当する機密性を要する情報であり、職務従事者のうち、特定の者だけがアクセスできる状態を厳密に確保されるべき情報は機密性３情報に、秘密文書には相当しないが、情報公開法に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報等、職務従事者以外がアクセスできない状態を最低限確保されるべき情報は機密性２情報に、それ以外の情報は、機密性１情報に決定することを基本とする。

例えば、従来「取扱注意」等と表示されてきたような資料は、機密性２情報に決定することが考えられるが、その内容によっては、機密性１情報に決定した上で取扱制限を決定することで十分な場合も考えられる。

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	職務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、職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。

解説：完全性の格付については、情報が改ざん、誤びゅう又は破損されていない状態を確保されるべき情報は完全性２情報に、それ以外の情報は、完全性１情報に決定することを基本とする。

例えば、原本に相当する情報を完全性２情報に、複製に相当する情報（例えば、電子メールに添付されるファイル等）を完全性１情報に決定すること等が考えられる。

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	職務で取り扱う情報（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、職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。

解説：可用性の格付については、情報が滅失又は紛失されていない状態及び情報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されるべき情報は可用性２情報に、それ以外の情報は可用性１情報に決定することを基本とする。

なお、可用性２情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。

(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。

解説：付表を用いて定める場合の例については本書別添資料 A.1.2 取扱制限の種類に係る付表例を参照。

1.1.1.4 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、本管理基準及び技術基準に基づき、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) 本管理基準及び技術基準がＢ省が所管する独立行政法人等群の情報セキュリティ対策のための管理基準及び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) 実際の運用が本管理基準及び技術基準に準拠していること。（運用の準拠性確認）

(c) 独立行政法人Ａ機構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、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、本管理基準及び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、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、独立行政法人Ａ機構の責任において運用することが大前提であるが、Ｂ省が所管する独立行政法人等群全体としての情報セキュリティ対策推進の観点から、独立行政法人Ａ機構は対策の実施状況及び監査結果についてＢ省政策評価広報課に報告を行うこととする。また、独立行政法人Ａ機構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。

1.1.1.5 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。
- 「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。
- 「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職務従事者以外の者に請け負わせることをいう。
- 「可用性」とは、情報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。
- 「職務従事者」とは、職員（独立行政法人Ａ機構において職務に従事している国家公務員）及び独立行政法人Ａ機構の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、独立行政法人Ａ機構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、職務の遂行に支障を及ぼすものをいう。
- 「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、本管理基準及び技術基準における「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。
- 「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、独立行政法人Ａ機構基準及び独立行政法人Ａ機構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、独立行政法人Ａ機構外に、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、職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】

● 「独立行政法人Ａ機構外」とは、職務従事者の各々が所属する独立行政法人が管理する組織又は施設の外をいう。

● 「独立行政法人Ａ機構外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び独立行政法人Ａ機構管理又は他組織管理）及び通信回線装置を問わず、職務従事者の各々が所属する独立行政法人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。

● 「独立行政法人Ａ機構外での情報処理」とは、職務従事者の各々が所属する独立行政法人の管理部外で職務の遂行のための情報処理を行うことをいう。なお、オンラインで独立行政法人Ａ機構外から職務従事者の各々が所属する独立行政法人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。

● 「独立行政法人Ａ機構支給以外の情報システム」とは、職務従事者の各々が所属する独立行政法人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、独立行政法人Ａ機構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。

● 「独立行政法人Ａ機構支給以外の情報システムによる情報処理」とは、職務従事者の各々が所属する独立行政法人が支給する情報システム以外の情報システムを用いて職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、職務従事者の各々が所属する独立行政法人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。

- 「独立行政法人Ａ機構内」とは、職務従事者の各々が所属する独立行政法人が管理する組織又は施設の内をいう。
- 「独立行政法人Ａ機構内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び独立行政法人Ａ機構管理又は他組織管理）及び通信回線装置を問わず、職務従事者の各々が所属する独立行政法人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、職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、職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

趣旨（必要性）

情報セキュリティ対策は、それに係る全ての職務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。具体的には、

・最高情報セキュリティ責任者の設置とその役割
・情報セキュリティ委員会の設置とその役割
・情報セキュリティ監査責任者の設置とその役割
・情報セキュリティ責任者の設置とその役割
・情報システムセキュリティ責任者の設置とその役割
・情報システムセキュリティ管理者の設置とその役割
・課室情報セキュリティ責任者の設置とその役割
・情報セキュリティアドバイザーの設置とその役割

についての遵守事項を定めるものである。

遵守事項

(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。最高情報セキュリティ責任者は、ＩＴ総括責任者とすること。

解説：独立行政法人Ａ機構における情報セキュリティ対策の最高責任者を置くことを定めた事項である。

情報セキュリティ対策の実現には、職務従事者一人一人の意識の向上や責務の遂行はもちろんのこと、組織的な取組の推進や幹部の責任を持った関与が必須であり、独立行政法人Ａ機構における最高責任者の設置とその役割の明確化が重要である。なお、本管理基準で規定する各役割についてはイメージ図（本書別添資料 A.1.1）を参考にされたい。

(b)　最高情報セキュリティ責任者は、独立行政法人Ａ機構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。

解説：最高情報セキュリティ責任者は、独立行政法人Ａ機構内における情報セキュリティ対策の推進体制が十分機能するように管理するとともに、独立行政法人Ａ機構対策基準の決定や評価結果による見直しに関する承認

等を行う。

(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、委員長及び委員を置くこと。情報セキュリティ委員会は、部局長会議とすること。

解説：独立行政法人Ａ機構における独立行政法人Ａ機構対策基準の策定等を行う機能を持つ組織の設置について定めた事項である。

情報セキュリティ対策の運用を円滑に進めるには、委員会を設置し組織全体で取り組むことが重要である。最高情報セキュリティ責任者は、委員長を兼務することが可能である。

なお、実務を担当する下位委員会を設置し、又は既存の情報システム管理部門に情報セキュリティ対策の運用を統括する機能を持たせる等して、部門横断的な連携の仕組みを確立することが望まれる。

(b) 情報セキュリティ委員会は、管理基準に準拠して、情報セキュリティに関する独立行政法人Ａ機構対策基準を策定し、最高情報セキュリティ責任者の承認を得ること。

解説：全部門的に定めるべき独立行政法人Ａ機構対策基準策定に関する情報セキュリティ委員会の役割を定めた事項である。

(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。情報セキュリティ監査責任者は、監事とすること。

解説：独立行政法人Ａ機構において策定した独立行政法人Ａ機構対策基準に基づき監査を行う責任者を置くことを定めた事項である。

情報セキュリティ監査責任者は、情報セキュリティ責任者が所管する組織における情報セキュリティ監査を実施するため、情報セキュリティ責任者と兼務することはできない。

監査の実効性を確保するために、情報セキュリティ責任者より職務上の上席者を情報セキュリティ監査責任者として置くことが望ましい。

情報セキュリティ監査責任者は、独立行政法人Ａ機構内の情報セキュリティに関する情報を共有するために、情報セキュリティ委員会にオブザーバとして参加することが望まれる。

情報セキュリティ監査責任者の業務を補佐するために、独立行政法人Ａ機構の内部及び外部の担当者を置く必要性を検討することが望まれる。また、業務の実効性を担保するために外部組織の活用も考えられる。

なお、独立行政法人Ａ機構において、監査責任者を補佐する立場として監査副責任者等を独自に設置することを妨げるものではない。

(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

【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人置くこと。管理を行う単位を全部門情報システム運用委員会の各情報システム運用小委員会とし、情報セキュリティ責任者は、各小委員会委員長とし、統括情報セキュリティ責任者は、ＩＴ総括責任者補佐とすること。

解説：組織内での役割の明確化のため、情報セキュリティ対策の運用について管理を行う単位を決めることを定めた事項である。

「管理を行う単位」は、部、局（外局、地方支分局等含む。）ごとや情報システムごと等が挙げられる。情報セキュリティ責任者は、独立行政法人Ａ機構の実施手順を策定するとともに、組織内での情報セキュリティ対策の運用実態を十分踏まえ、実務レベルでの管理の仕組みを確立し、全ての職務従事者への責務の周知や教育を行う等、個別対策を機能させる環境を整備することが重要である。

(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、技術基準に準拠して、情報セキュリティに関する独立行政法人Ａ機構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。

解説：全部門的に定めるべき独立行政法人Ａ機構対策基準における技術的側面の基準策定に関する統括情報セキュリティ責任者の役割を定めた事項である。また、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。なお、情報セキュリティ責任者等が委任に基づき技術基準を策定する場合は、最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告することが望ましい。

(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。

解説：「雇用の開始、終了及び人事異動等に関する管理の規定」とは、現実の人事配置状況と情報システム上のアクセス権の付与状況等の不整合や、採用及び異動時等における適切な教育の不十分さを原因とする情報セキュリティの侵害を回避することを目的とする規定のことである。

具体的には、

・人事担当課又は各課室から、情報システム所管課に人事異動に関する情報が提供される連絡体制

・人事異動の情報に基づき、アクセス権の変更、職務従事者の教育等の

情報セキュリティ関係業務を適切に実施するための手順
等を整備することが求められる。
これには、転出に伴うアカウントの失効、情報システムへのアクセス権の変更の管理等も含まれる。

(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

【基本遵守事項】

(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。情報システムセキュリティ責任者は、各情報システム運用小委員会の技術責任者とすること。

解説：各情報システムにおいて、計画、構築、運用等のライフサイクル全般を通じて必要となるセキュリティ対策の責任者を置くことを定めた事項である。
情報システムのセキュリティ要件は計画段階において決定されることから、情報システムセキュリティ責任者は新規の情報システムについては計画段階までに置かなければならない。
独立行政法人Ａ機構内 LAN システムのような全部門的なシステム、特定部門における個別業務システム、その他独立行政法人Ａ機構の全ての情報システムを、情報システム単位にセキュリティ対策の運用の責任の所在を明確にすることが重要である。
「所管する単位における情報システムごとに」と記載しているが、所管する単位ごとに１人あるいは情報システムごとに１人に限るものではなく、所管する単位内に複数の情報システムセキュリティ責任者を置いてもよいし、複数の情報システム群をまとめて、情報システムセキュリティ責任者を置いてもよい。
なお、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にすること。

(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

【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。

解説：各情報システムにおいて、その管理業務ごとのセキュリティ対策の実施を管理する者を置くことを定めた事項である。

計画、構築、運用等の情報システムのライフサイクルやサーバ、データベース、アプリケーション等の装置・機能ごとに必要に応じて設置する必要がある。

情報システムセキュリティ管理者は、情報セキュリティ責任者によって定められた手順や判断された事項に従い、対策を実施する。

(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

【基本遵守事項】

(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。

解説：課室単位での情報セキュリティ対策の事務を統括する者を置くことを定めた事項である。

課室情報セキュリティ責任者は、所管する事務や職務従事者における情報の取扱い等に関して、その是非を判断し、情報の持ち出しや公開等についての責任を有する者であり、課室長若しくはそれに相当する者であることが望ましい。情報セキュリティ責任者が各課室で 1 人任命し、統括情報セキュリティ責任者に報告するものである。

(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) 情報セキュリティアドバイザーの設置

【基本遵守事項】

(a) 最高情報セキュリティ責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くこと。

解説：情報セキュリティに関する専門家を情報セキュリティアドバイザーとして置くことを定めた事項である。

独立行政法人Ａ機構における情報セキュリティ対策については、情報システムに関する技術や事案に対する対処等の専門的な知識及び経験が必要となるため、独立行政法人Ａ機構対策基準の策定・導入から運用、評価、見直しまで専門的な助言を行う専門家を活用することが重要である。

情報セキュリティアドバイザーについては、高度な国家安全保障、治安に係る分野においては、内部人材を充てることもできる。またこの場合、情報セキュリティアドバイザーは情報セキュリティ責任者等の各責任者を兼務することができる。

なお、CIO（情報化統括責任者）補佐官は情報セキュリティアドバイザーを兼務することができる。この場合、CIO 補佐官に情報セキュリティ担当を設けることが望ましい。

(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。

解説：情報セキュリティアドバイザーの業務を明確化するため、最高情報セキュリティ責任者に、情報セキュリティアドバイザーの業務の内容について定めることを求める事項である。

情報セキュリティアドバイザーの業務として、情報セキュリティ対策に係る様々な事務への助言等が想定されるが、その事務として例えば、

・情報セキュリティ施策の全般的な計画策定
・情報セキュリティ教育の計画立案、教材開発及び実施
・各種規定の整備
・情報システムに係る技術的事項
・情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定
・職務従事者に対する日常的な相談対応
・緊急時対応
・自己点検の計画立案と実施
・情報セキュリティの監査の計画立案と実施

等が想定される。

これらの事務を行う最高情報セキュリティ責任者、情報セキュリティ監査責任者、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、課室情報セキュリティ責任者等が定められた事項を遂行するために、情報セキュリティアドバイザーが専門的な知識及び経験に基づき行う助言等の内容を定める。

1.2.1.2 役割の割当て

趣旨（必要性）

情報セキュリティ対策に係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、情報セキュリティが確保されていることが確認、証明されたことにはならない。情報セキュリティを確立するためには、兼務してはいけない役割が存在する。また、承認や許可事案においては、情報セキュリティ対策に係る組織体制に加えて、職務上の権限等から、当該組織体制上の承認等を行う者の上司が承認等をすべき場合がある。

これらのことを勘案し、本項では、情報セキュリティ対策に係る役割の割当てに関する対策基準として、兼務を禁止する役割、上司による承認・許可についての遵守事項を定める。

遵守事項

(1) 兼務を禁止する役割の規定

【基本遵守事項】

(a) 職務従事者は、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

解説：承認又は許可する役割の者自らが、申請をする場合には、その申請について自らが承認又は許可することはできない。このため、組織・体制及び申請手続を整備するに当たっては、このことに十分留意する必要がある。

(2) 上司による承認・許可

【基本遵守事項】

(a) 職務従事者は、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。

解説：承認や許可事案の内容によっては、承認権限者等が承認等の可否の判断を行うことが適切でない場合も想定される。このような場合は、その上司に申請し承認等を得ることになる。

なお、「兼務を禁止する役割の規定」を遵守する必要がある。したがって、自らが承認権限者の上司であったとしても、当該上司は自らに係る承認等の事案について自らが承認等してはならない。

(b) 職務従事者は、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。

解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。例えば、機密性３情報、完全性２情報又は可用性２情報について、独立行政法人Ａ機構外での情報処理や独立行政法人Ａ機構支給以外の情報システムによる情報処理を課室情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得すること等が求められる。

1.2.1.3 違反と例外措置

趣旨（必要性）

独立行政法人Ａ機構において情報セキュリティを継続的に維持するためには、万一違反があった場合に、定められた手続に従って、適切に対処する必要がある。

また、情報セキュリティ関係規程の適用が職務の適正な遂行を著しく妨げる等の理由により、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採用すること又は規定を実施しないことを認めざるを得ない場合についても、定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できるものでなければ、当該規程の実効性を確保することが困難となる。

これらのことを勘案し、本項では、違反と例外措置に関する対策基準として、違反への対処方法及び例外措置の適用方法についての遵守事項を定める。

遵守事項

(1) 違反への対処

【基本遵守事項】

(a) 職務従事者は、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。

解説：独立行政法人Ａ機構において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉するための事項である。独立行政法人Ａ機構においては、例規への違反を知った者にはこれを報告する義務が課されており、情報セキュリティ関係規程への違反においては、各規定の実施に責任を持つ情報セキュリティ責任者に報告することとなる。

情報セキュリティ関係規程への重大な違反とは、当該違反により独立行政法人Ａ機構の業務に重大な支障を来すもの又はその可能性のあるものをいう。

(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。

解説：情報セキュリティ関係規程への違反があった場合に、違反者及び当該規

程の実施に責任を持つ者を含む必要な者に対して、情報セキュリティを維持するために必要な措置を講ずることを求める事項である。重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、問題の早期解決、拡大防止の必要がある。例えば、情報セキュリティ関係規程について再度周知する方法が考えられる。

(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。

解説：情報セキュリティ関係規程への違反があった場合に、違反の事実を、その内容、結果、業務への影響、社会的評価等を含めて、最高情報セキュリティ責任者に報告することを求める事項である。

(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。

解説：例外措置の適用の申請を受けた際に審査を遅滞なく実施できるように、許可権限者を定め、審査手続を整備しておくための事項である。緊急を要して申請される場合は、遂行に不要の遅滞を生じさせずに審査を速やかに実施する必要がある。そのため、申請の内容に応じ、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、情報システムセキュリティ責任者、情報システムセキュリティ管理者又は課室情報セキュリティ責任者の中から許可権限者を定めておくことが重要である。

(b) 職務従事者は、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、職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。職務従事者は、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

解説：例外措置を職務従事者の独断で行わせないための事項である。

職務従事者は、定められた審査手続に従い例外措置の適用を申請し、許可を得てから、例外措置を講ずる。ただし、職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て許可を得ること。

職務従事者は、例外措置の適用を希望する場合には、当該例外措置を適用した場合の被害の大きさと影響を検討、分析する必要がある。その上で、例外措置の適用が必要であると判断した場合は、リスクを低減させるための補完措置を提案し、適用の申請を行う必要がある。

(c) 許可権限者は、職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

解説：許可権限者に、例外措置の適用の申請を適切に審査させるための事項である。

審査に当たっては、例外措置の適用を許可した場合のリスクと不許可とした場合の職務遂行等への影響を評価した上で、その判断を行う必要がある。例外措置の適用審査記録の報告を受け、最高情報セキュリティ責任者は適用審査記録の台帳を整備することとなるが、これは、将来、許可をさかのぼって取り消す場合に、該当する申請を全て把握し、一貫性をもって取り消すために必要となる。

（ア）の「役割名」には、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、情報システムセキュリティ責任者、情報システムセキュリティ管理者又は課室情報セキュリティ責任者のいずれかを記載する。

(d) 職務従事者は、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。

解説：例外措置の適用の終了を確認するための事項である。
例外措置の適用期間が終了した場合及び期間終了前に適用を終了する場合には、許可を受けた職務従事者が、許可権限者に終了を報告しなければならない。

(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。

解説：例外措置の適用期間を、許可を受けた者に遵守させるための事項である。
必要な措置としては、許可を受けた者が報告を怠っているのであればそれを督促すること、許可を受けた者が例外措置の適用を継続している場合にはその延長について申請させそれについて審査すること、が挙げられる。

(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。

解説：最高情報セキュリティ責任者に、例外措置の適用審査記録の台帳を維持・整備することを求める事項である。例外措置の適用を許可したとしても、それが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採用すること又は遵守事項を実施していないことに変わりはない。もしも、例外措置を適用していることにより重大な情報セキュリティの侵害が発生した場合には、同様の例外措置を適用している者に対して、情報セキュリティの侵害発生の予防について注意を喚起したり、例外措置適用の許可について見直しをしたりする等の対処を検討する必要がある。そのためには、例外措置を適用している者や情報システムの現状について、最新の状態のものを集中して把握する必要がある。

1.2.2　運用

1.2.2.1 情報セキュリティ対策の教育

趣旨（必要性）

情報セキュリティ関係規程が適切に整備されているとしても、職務従事者にその内容が周知されず、職務従事者がこれを遵守しない場合には、情報セキュリティ対策の水準の向上を望むことはできない。このため、全ての職務従事者が、情報セキュリティ対策の教育を通じて、情報セキュリティ関係規程に関する理解を深め、情報セキュリティ対策を適切に実践できるようにすることが必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の教育に関する対策基準として、統括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による教育体制の整備に係る規程及び職務従事者による教育の受講についての遵守事項を定める。

遵守事項

(1) 情報セキュリティ対策の教育の実施

【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、職務従事者に対し、その啓発をすること。

解説：統括情報セキュリティ責任者に情報セキュリティ対策の啓発の実施を求める事項である。

(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、職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。

解説：統括情報セキュリティ責任者に情報セキュリティ対策の教育のための資料を整備することを求める事項である。

教育の内容については、独立行政法人Ａ機構の実情に合わせて幅広い角度から検討し、職務従事者が対策内容を十分に理解できるものとする必要がある。

そのためには、独立行政法人Ａ機構の情報セキュリティに係る網羅的な資料ではなく、受講する者が理解しておくべき事項に制限した資料を教育に用いるべきである。すなわち、資料の作成においては、遵守事項を遵守すべき者ごとに整理し、受講する者が遵守する必要がない事項は極力含まないように配慮する必要がある。

なお、遵守すべき事項以外であっても、教育内容に含めることが望ましい情報セキュリティ対策の例として、違反の監視機能に係る説明が挙げられる。これは、当該機能の存在を周知することで、その違反についての抑止効果を期待できる場合があるためである。

(c)　統括情報セキュリティ責任者は、職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。

解説：情報セキュリティ対策の教育の最低限の受講回数等について定めた事項である。

なお、情報セキュリティ事案の発生等、情報セキュリティ環境の変化に応じて、適宜、教育を行うことが重要である。計画の作成に際しては、関係する教育計画を参照し、効率性に注意するとともに人材育成にも留意すること。

(d) 統括情報セキュリティ責任者は、職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。

解説：着任、異動した職務従事者に対して、早期に情報セキュリティ対策の教育を受講させることによって、当該職務従事者の情報セキュリティ対策の適正な実施を求める事項である。

なお、異動した後に使用する情報システムが、異動前と変わらない等、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。

(e) 統括情報セキュリティ責任者は、職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。

解説：情報セキュリティ対策の教育の受講状況について把握できる仕組みを整備することを求める事項である。

(f) 統括情報セキュリティ責任者は、職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。

解説：計画された教育の実施に向けて、情報セキュリティ対策の教育を受講していない職務従事者を課室情報セキュリティ責任者に通知することを定めた事項である。

(g) 課室情報セキュリティ責任者は、職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。

解説：課室情報セキュリティ責任者が、職務従事者に情報セキュリティ対策の教育を受講させる責務について定めた事項である。

なお、例えば、受講時間を確保する等の職務従事者が受講できるための環境を整備することも必要である。

(h) 課室情報セキュリティ責任者は、職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。職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。

解説：情報セキュリティ対策の教育を受講しない者への対策を定めた事項である。

なお、計画された教育を受講しない職務従事者は、その遵守違反について責任を問われることになる。

(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、職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。

解説：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情報セキュリティ対策の教育の受講状況を報告することを求める事項である。

(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、職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。

解説：実際に情報セキュリティ対策のための模擬的に事務を行うことにより、情報セキュリティ関係規程に係る知識・技能等を習得するために実施する訓練の内容及び体制を整備することを求める事項である。
なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。

(2) 情報セキュリティ対策の教育の受講

【基本遵守事項】

(a) 職務従事者は、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。

解説：職務従事者が、情報セキュリティ対策の教育に関する計画に従って、これを受講することを求める事項である。

(b) 職務従事者は、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。

解説：着任、異動した職務従事者が、確実に情報セキュリティ対策の教育を受講するための事項である。

(c) 職務従事者は、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。

解説：情報セキュリティ対策の教育を受講できない理由についての報告をしないままで、計画された教育を受講しない場合には、職務従事者は、その遵守違反について責任を問われることになる。

(d) 職務従事者は、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。

解説：職務従事者が、情報セキュリティ対策の訓練に関する規定に従って、これを受講することを求める事項である。

1.2.2.2 障害・事故等の対処

趣旨（必要性）

情報セキュリティに関する障害・事故等が発生した場合には、早急にその状況を検出し、

被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、障害・事故等の影響や範囲を定められた責任者へ報告し、障害・事故等の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準として、障害・事故等の発生に備えた事前準備、発生時における報告と応急措置、原因調査と再発防止策についての遵守事項を定める。

遵守事項

(1) 障害・事故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障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生した場合、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備すること。

解説：最高情報セキュリティ責任者に障害・事故等に対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配意することが求められる。

なお、情報セキュリティに関する障害・事故等とは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。

また、「インシデント」とは、JIS Q 27002:2006（ISO/IEC 17799:2005）における情報セキュリティインシデントと同意である。

(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職務従事者に周知すること。

解説：窓口についての周知は、情報セキュリティ対策の教育の中で行うとともに、窓口の連絡先を執務室内に掲示する等して、緊急時に職務従事者がすぐに参照できるようにすることが必要である。情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。

(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対処手順を整備すること。

解説：対処手順として障害・事故等の発生時において緊急を要する対処等の必要性に備えて、通常とは異なる例外措置の承認手続を設けることもあわせて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなことがないよう検討すること。

対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を職務従事者が記録すべきことを定めることも考えられる。

(d) 統括情報セキュリティ責任者は、障害・事故等に備え、職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。

解説：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及び情報システムセキュリティ管理者の連絡網を整備しているものである（管理基準 1.2.1.1）が、障害･事故等が発生した場合に速やかに対応するため、「緊急」連絡網を加えて整備することを定める事項である。

緊急連絡網には、1.2.1.1 において整備を求める連絡網とは異なり、該当する職務従事者の自宅や携帯電話の番号等の個人情報が含まれることも想定され、この場合、それぞれの連絡網の取扱いが異なることに注意する必要がある。

なお、緊急連絡網には当該システムに係る責任者及び管理者のほか、大規模な障害・事故等に備えて最高情報セキュリティ責任者も含める必要がある。

(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。

解説：実際に障害・事故等への対処を模擬的に行うことにより、対応力を強化するために実施する訓練の内容及び体制を整備することを求める事項である。

なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。

(f) 職務従事者は、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。

解説：職務従事者が、障害・事故等への対処の訓練に関する規定に従って、これに参加することを求める事項である。

【強化遵守事項】

(g) 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必要に応じ、統括情報セキュリティ責任者は、障害・事故等について独立行政法人Ａ機構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独立行政法人Ａ機構外に公表すること。

解説：独立行政法人Ａ機構における情報セキュリティ対策の不備について外部の者が発見したり、独立行政法人Ａ機構において管理する電子計算機がサービス不能攻撃を外部に行った場合等、独立行政法人Ａ機構を取り巻く外部に対して、関連業務に支障を生じさせたり、情報セキュリティ上の脅威を与えたりした際に、その連絡を外部から受ける体制についても整備し、連絡先を独立行政法人Ａ機構の外部に公表することを求める事項である。

(2) 障害・事故等の発生時における報告と応急措置

【基本遵守事項】

(a) 職務従事者は、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、情報セキュリティ責任者にその旨を報告すること。

解説：障害・事故等が発生した場合に、職務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害・事故等への対処を開始することができるようにすることを求める事項である。

なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。

(b) 職務従事者は、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。

解説：職務従事者の判断による被害拡大防止策が常に適切なものであるとは限らないため、障害・事故等への対処手順に従うことを求める事項である。

(c) 職務従事者は、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。

解説：対処手順が想定していない障害・事故等が発生した場合、職務従事者は対処の指示を受けるまでの間も障害・事故等の拡大防止に努めることを求める事項である。

(3) 障害・事故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・事故等が発生した場合には、障害・事故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。

解説：情報セキュリティ責任者に対して、障害・事故等の原因を究明し、それに基づき障害・事故等の再発防止策を策定することを求める事項である。

(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。

解説：障害・事故等の再発防止策を講ずることを、最高情報セキュリティ責任者に求める事項である。

1.2.3　評価

1.2.3.1 情報セキュリティ対策の自己点検

趣旨（必要性）

情報セキュリティ対策は、それに係る全ての職務従事者が、各自の役割を確実に行うことで実効性が担保されるものであることから、全ての職務従事者自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要である。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

これらのことを勘案し、本項では、自己点検に関する対策基準として、自己点検に関する年度計画の策定とその実施に関する準備、自己点検の実施、結果の評価及び自己点検に基づく改善についての遵守事項を定める。

遵守事項

(1) 自己点検に関する年度計画の策定

【基本遵守事項】

(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。

解説：自己点検を実施するに当たり、その実施頻度、実施時期、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である。

実施頻度については、自己点検は年に２度以上実施することが望ましいが、例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては半年に一度の頻度で実施する等、様々な選択肢が考えられる。

実施時期については、例えば、当初は毎月 10 項目ずつ自己点検し、職務従事者の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。

確認及び評価の方法については、例えば、単純に実施したことを確認するほか、遵守率を確認する等、数値評価により客観性を持った評価とすることが望ましく、様々な選択肢が考えられる。

実施項目の選択については、例えば、当初は全ての職務従事者が容易に遵守できる項目のみを自己点検し、職務従事者の意識が高まった後、遵守率が低いと想定される項目を実施するように変更する等、様々な選択肢が考えられる。

なお、職務従事者自らが行う自己点検を原則とするが、システム的な仕組みを用いてパッチやパターンファイルの更新状況を把握したり、実際の文書を確認することによりその整備状況を把握する等、自己点検と同等以上の信頼性を有する方法が存在する場合には、代替方法としてそれ

を採用しても良い。

(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、職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。

解説：各職務従事者が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、情報セキュリティ責任者は、職務従事者ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することを求める事項である。

(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、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、職務従事者に対して、自己点検の実施を指示すること。

解説：年度自己点検計画に基づき、情報セキュリティ責任者自らも含めた職務従事者に対して、自己点検の実施に関し指示することを求める事項である。

(b) 職務従事者は、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。

解説：情報セキュリティに関わる職務従事者に対して、自己点検を実施し、自らが実施すべき対策事項について、実施の有無を確認することを求める事項である。

(4) 自己点検結果の評価

【基本遵守事項】

(a) 情報セキュリティ責任者は、職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。

解説：職務従事者による自己点検の結果について、情報セキュリティ責任者が評価することを求める事項である。

なお、評価においては、自己点検が正しく行われていること、独立行政法人Ａ機構対策基準に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った評価とすることが望ましい。例えば、自己点検実施率や、独立行政法人Ａ機構対策基準遵守率、要改善対策数/対策実施数等の準拠率の把握が挙げられる。

(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。

解説：情報セキュリティ責任者による自己点検が適切に行われていることを、統括情報セキュリティ責任者が評価することを求める事項である。

(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。

解説：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を求める事項である。

(5) 自己点検に基づく改善

【基本遵守事項】

(a) 職務従事者は、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。

解説：自己の権限の範囲で改善可能である問題点については、情報セキュリティに関わる全ての職務従事者自らが自己改善することを求める事項である。

(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。

解説：自己点検の結果により明らかとなった問題点について、最高情報セキュリティ責任者が情報セキュリティ責任者に対して改善することを求める事項である。

1.2.3.2 情報セキュリティ対策の監査

趣旨（必要性）

情報セキュリティの確保のためには、本管理基準及び技術基準に準拠して独立行政法人A機構対策基準が適切に策定され、かつ、情報セキュリティ関係規程が適切に運用されることによりその実効性を確保することが重要であって、その準拠性と妥当性の有無が確認されなければならない。そのためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の監査に関する対策基準として、監査計画の策定とその実施に関する指示、個別の監査業務における監査実施計画の策定、監査の実施に係る準備、監査の実施及びその結果に対する対処についての遵守事項を定める。

遵守事項

(1) 監査計画の策定

【基本遵守事項】

(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。

解説：監査の基本的な方針として、年度監査計画を策定し、承認を受けることを求める事項である。年度監査計画には、次の事項が含まれる。

・重点とする監査対象及び監査目標（情報漏えい防止、不正アクセス防止等）

・監査実施期間

・監査業務の管理体制

・外部委託による監査の必要性及び範囲

・監査予算

なお、以前実施した監査結果で明らかになった課題及び問題点の改善状況について、監査を実施する場合には、年度監査計画に盛り込むこと。

(2) 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。

解説：年度監査計画に従って監査を実施することを求める事項である。

(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。

解説：年度監査計画において実施する監査以外に、独立行政法人Ａ機構内外における注目すべき事案の発生又は情報セキュリティ対策の実施内容について重大な変更が生じた場合に、必要に応じて臨機応変に監査を実施することを求める事項である。

(3) 個別の監査業務における監査実施計画の策定

【基本遵守事項】

(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。

解説：監査の基本的な方針に基づいて、実施すべき監査についての詳細な計画を策定することを求める事項である。監査実施計画には、次の事項が含まれる。(経済産業省 情報セキュリティ監査基準　実施基準ガイドライン Ver1.0 等を参考)

・監査の実施時期

・監査の実施場所

・監査実施者及び担当職務の割当て

・準拠性監査（情報セキュリティ関係規程に準拠した手続が実施されていることを確認する監査）のほか、必要に応じて妥当性監査（実施している手続が有効な情報セキュリティ対策であることを確認する監査）を

行うかについての方針
・実施すべき監査の概要（監査要点、実施すべき監査の種類及び試査の範囲を含む。）
・監査の進捗管理手段又は体制
なお、被監査部門に対し監査の内容や範囲を明確化するために、監査実施期間、監査実施者の氏名、監査対象等を含む事項に関して、情報セキュリティ監査責任者より事前通知することが望ましい。
また、本管理基準においては、監査業務に対して監査を別途実施することを必須とはしてない。しかし、監査実施者が監査過程で被監査者を監査すること以外のことを実施した場合には、その実施に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、監査実施計画を策定する際は、監査実施者が実施することが情報セキュリティ対策の向上になり得ることや、何らかの作業を効率的に行えるとしても、それを安易に監査実施計画の中に取り込むべきではない。

(4) 監査の実施に係る準備
【基本遵守事項】
(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。
解説：情報セキュリティ監査責任者に、独立行政法人Ａ機構において監査業務を実施するに当たり、必要となる者を情報セキュリティ監査実施者に指名することを求める事項である。
情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。
例えば、情報システムを監査する場合には、当該情報システムの構築をした者は、その監査をしないこととする。また、情報資産の運用状況に関する監査を行う場合には、当該情報資産を運用している者はその監査をしないこととする。
(b) 情報セキュリティ監査責任者は、職務従事者以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、職務従事者以外の者に監査の一部を請け負わせること。
解説： 情報セキュリティ監査責任者に、監査を実施するに当たり、必要に応じて監査対象システムの詳細情報を有する組織、独立行政法人Ａ機構内の情報システム部門に加えて外部専門家の支援を受けることを求める事項である。
組織内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮し、外部委託に関する対策基準に従うこと。また、情報セキュ

リティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。

(5) 監査の実施

【基本遵守事項】

(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。

解説：情報セキュリティ監査実施者が適切に監査を実施することを求める事項である。

(b) 情報セキュリティ監査実施者は、独立行政法人Ａ機構対策基準が管理基準及び技術基準に準拠していることを確認すること。

解説：独立行政法人Ａ機構対策基準が管理基準及び技術基準に準拠して設計されていることの確認を求める事項である。

(c) 情報セキュリティ監査実施者は、実施手順が独立行政法人Ａ機構対策基準に準拠していることを確認すること。

解説：独立行政法人Ａ機構における実施手順が独立行政法人Ａ機構対策基準に準拠して設計されていることの確認を求める事項である。

(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。

解説：被監査部門における実際の運用が、独立行政法人Ａ機構の情報セキュリティ関係規程に準拠して実施されていること（運用の準拠性）の確認を求める事項である。運用の準拠性の確認は、自己点検の適正性の確認によることが実効性の高い方法であると考えられる。

監査に当たっては、自己点検結果に基づく担当者への質問、記録文書の査閲、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、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の妥当性を確認することも求められる。例えば、監査対象によっては脆弱性検査、侵入検査等のその他の方法によっても確認することができる。

(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。

解説：監査報告書の根拠となる監査調書を適切に作成することを求める事項である。

監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等を綴り込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては組織の外部の第三者から入手した資料等を含むことがある。

(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。

解説：監査結果を報告書として文書化した上で、最高情報セキュリティ責任者へ確実に提出をすること求める事項である。
なお、本監査は、独立行政法人Ａ機構対策基準が管理基準及び技術基準に準拠しているか、実際の運用状況が情報セキュリティ関係規程に準拠して行われているか等、準拠性の監査を意図したものであるが、監査の過程において、遵守内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言提案を監査報告書に含めることが望ましい。

(6) 監査結果に対する対処

【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、指摘されたことに対する対処の実施を指示すること。

解説：監査報告書において指摘された課題及び問題点に対する改善を図るため、最高情報セキュリティ責任者へ被監査部門の情報セキュリティ責任者に対する対処実施の指示を求める事項である。

(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。

解説：監査報告書において指摘された課題及び問題点が、他の監査対象にも同種の課題及び問題点として存在する可能性が高い場合又は同種の課題及び問題点の存在を緊急に確認する必要性が高い場合には、想定される他の監査対象についても同様に調査を実施する必要がある。そのため、最高情報セキュリティ責任者から情報セキュリティ責任者に対する確認の指示を求める事項である。

(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。

解説：監査報告書や監査調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ことについて、対処計画の策定及び報告を求める事項である。監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成することが可能な対処目標を提示することが重要である。また、その課題及び問題点が人為によるものである場合には、情報セキュリティ責任者は、提示された対処目標を情報セキュリティ対策の教育方法や教育施策に反映することが必要である。

(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。

解説：情報セキュリティ監査責任者から報告された監査報告書において、課題

とその改善に対する助言意見等の指摘を受けた場合には、既存の情報セキュリティ関係規程の見直しを検討することを求める事項である。
検討の結果、情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。

1.2.4　見直し

1.2.4.1 情報セキュリティ対策の見直し

趣旨（必要性）

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティレベルは維持できなくなる。このため、情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、作成、導入、運用、評価の各段階において、適時見直しを行う必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策の見直しに関する対策基準について定める。

遵守事項

(1) 情報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。

解説：情報セキュリティ関係規程を整備した者は、新たなセキュリティ脅威の出現、自己点検及び監査の評価結果等を踏まえつつ、情報セキュリティ対策に支障が生じないように見直しを行う時期を判断する必要がある。情報セキュリティ関係規程を見直した者は、他部門へも影響があると思われる場合、同種の課題及び問題点の有無を確認するように連絡することを推奨する。

(b)　職務従事者は、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。

解説：職務従事者自らが整備したものではない情報セキュリティ関係規程について、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を求める事項である。

(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。

解説：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に、その是非を検討し、必要な措置を講ずることを求める事項である。例えば、職務従事者からの相談が妥当であると思料する場合に情報セキュリティ関係規程の見直しを行ったり、逆に職務従事者の理解不足が原因であると思料する場合は、再教育の措置を講ずること等が考えられる。

1.2.5　その他

1.2.5.1 外部委託

趣旨（必要性）

職務従事者以外の者に情報処理業務を委託する場合（外部の設備を利用した役務提供も含む）には、独立行政法人Ａ機構が委託先を直接管理することができないため、独立行政法人Ａ機構内で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報処理業務を外部委託する際は、委託先においても独立行政法人Ａ機構の独立行政法人Ａ機構対策基準と同等の対策を実施させるべく、委託先への要求事項を定める必要がある。

これらのことを勘案し、本項では、外部委託に関する対策基準を定める。具体的には、

・情報セキュリティ確保のための独立行政法人Ａ機構内共通の仕組みの整備
・委託先に実施させる情報セキュリティ対策の明確化
・委託先の選定
・外部委託に係る契約
・外部委託の実施における手続
・外部委託終了時の手続

についての遵守事項を定めるものである。

適用範囲

本項は、独立行政法人Ａ機構による貸借、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独立行政法人Ａ機構内共通の仕組みの整備

【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。

解説：外部委託の対象としてよい範囲としてはいけない範囲を判断する基準を独立行政法人Ａ機構として整備することを定めた事項である。独立行政法人Ａ機構内の情報システム及び関連する業務に関し、網羅性を確保しつつ統一的な基準で当該範囲を設定することが重要である。

また、データの所在については、海外のデータセンター等に情報を保存

する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。例えば、「行政機関の保有する個人情報の保護に関する法律」で定義する個人情報については、国内法が適用される場所に制限する必要があると判断すること等が考えられる。

(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。

解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。

統括情報セキュリティ責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、独立行政法人A機構対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。

選定基準としては、例えば、委託先が独立行政法人A機構対策基準の該当項目を遵守し得る者であること、独立行政法人A機構対策基準と同等の情報セキュリティ管理体制を整備すること、独立行政法人A機構対策基準と同等の情報セキュリティ対策の教育を実施すること等が挙げられる。

また、独立行政法人A機構の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を独立行政法人A機構内で統一的に整備することが重要である。

なお、本基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施に反映することが必要である。

【強化遵守事項】

(c) 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必要に応じ、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。

解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。

評価方法の整備には、例えば、ISO/IEC 27001 等に基づく認証制度の活用や、国際規格を踏まえ、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用が考えられる。

(2) 委託先に実施させる情報セキュリティ対策の明確化

【基本遵守事項】

(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。

解説：委託先に実施させる情報セキュリティ対策の内容を具体的に定めることを求める事項である。

外部委託に係る業務において納入される成果物（特に情報システム）に関しては、委託先における情報セキュリティ対策が適切に実施されてい

ることがその後の情報システム等の運用におけるセキュリティレベルの維持及び向上の前提となることから、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、周知しておくことが重要である。

なお、課室情報セキュリティ責任者が外部委託に係る業務について責任を負う場合には、例えば、課室において保有する情報の加工・処理を外部委託により行う場合がある。

(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。

解説：委託先に請け負わせる業務における情報セキュリティの侵害発生時の対処方法を独立行政法人Ａ機構として整備することを定めた事項である。

情報セキュリティの侵害の業務に対する影響度の大きさや機密性、完全性及び可用性の要求度に応じて、対処の緊急性等を考慮することが重要である。

(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。

解説：委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであること、及び履行が不十分である場合に速やかに適切な対処をすべきであることにかんがみ、これらのための方法の整備を求める事項である。

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としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。

周知する情報セキュリティ監査の内容には、請け負わせる業務のうちで監査の対象とする範囲、実施者（独立行政法人Ａ機構が指定する第三者、委託先が選定する第三者、独立行政法人Ａ機構又は委託先において当該業務を行う部門とは独立した部門）、実施方法（情報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先候補の情報セキュリティポリシーとの整合性等を委託先候補が判断するために必要と考えられる事項を含める。

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としては、例えば、独立行政法人Ａ機構及び委託先が改善について協議を行い、合意した改善策を実施させること等が考えられる。

また、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自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。

(3) 委託先の選定

【基本遵守事項】

(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。

解説：委託先の選定時における手続等の遵守に関して定めた事項である。

【強化遵守事項】

(b) 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必要に応じ、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、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に従って、委託先の候補者の情報セキュリティ水準を確認し、委託先の選定における評価の一要素として利用すること。

解説：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に基づく評価結果を、委託先の選定における評価の一要素として利用することを求める事項である。

(4) 外部委託に係る契約

【基本遵守事項】

(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

解説：情報セキュリティの観点から、外部委託に係る契約に含めるべき事項を定めた事項である。

機密保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報を守るべきであることから、これを記載する必要がある。

情報セキュリティ監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む、委託先と合意した事項を契約に含める。

サービスレベルに関しては、セキュリティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、事故発生時の対処方法等を決定し、委託先に保証させることが重要である。

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自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。

(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、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

解説：外部委託に係る契約者双方の責任の明確化と合意形成に基づく委託先からの確認書等の提出に関し定めた事項である。

必要に応じて、当該委託業務に携わる委託先の者の特定や、当該者が実施する取組内容を、委託先に確認することが重要になる。

特に、情報システムの構築及びソフトウェア開発等の外部委託の場合には、成果物における情報セキュリティ対策の実施が、その作成プロセスと不可分であることが想定されるため、遂行される業務全体の責任者を報告させることが重要である。

(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。

解説：外部委託契約の継続、特に随意契約に関し、都度審査することを定めた事項である。

また、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自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。

(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。

解説：委託契約の実施中の契約変更に関して定めた事項である。変更がある場合にはその是非を審査し、必要に応じて、契約変更をする等の対応が必要である。

また、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自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。

(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。

解説：委託先がその委託内容を再委託することは、セキュリティレベルの低下を招くことが懸念されることから原則として避けるべきである。一方、委託先がその委託内容を再委託する場合には、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を定めた事項である。

情報セキュリティを十分に確保するためには、委託先自体が業務を実施する場合に求めるべき水準と同一水準の情報セキュリティ対策を再委託

先においても確保させる必要がある。

(5) 外部委託の実施における手続

【基本遵守事項】

(a) 職務従事者は、委託先に要保護情報又は重要な設計書を提供する場合、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。

解説：委託契約開始から終了に至るまでに行う委託先への情報の提供を必要最小限に止め、また、提供に伴う要保護情報の漏えいや滅失等を防止するための措置の実施を求める事項である。

委託先への情報の提供における遵守事項は、本管理基準の「1.3.1.4 情報の移送」及び「1.3.1.5 情報の提供」の定めに準ずるが、例えば機密性３情報を提供する場合には、当該外部委託について責任を負う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許可を得ること、また、機密性２情報を提供する場合には、これらの者のいずれかに届け出ることが必要となる。委託先の選定基準や情報セキュリティの侵害時の対処方法を整備した上で、当事者間の情報の授受において上記の措置に従うことにより情報セキュリティを確保することが重要である。

(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。

解説：請け負わせた業務の実施中に情報セキュリティの侵害が発生した場合に、契約に記載した対処方法に従い、委託先に必要な措置を講じさせることを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に求める事項である。

(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。

解説：委託先に請け負わせた業務の実施中に、契約に記載した方法に従い、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を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に求める事項である。

委託先における情報セキュリティ対策の履行状況の確認に際し、情報セキュリティ監査を利用することとした場合には、契約に記載した監査の範囲及び実施方法に従い、独立行政法人Ａ機構自らが情報セキュリティ監査を行う以外に、第三者又は委託先に情報セキュリティ監査を行わせ

ることが考えられる。

(6) 外部委託終了時の手続

【基本遵守事項】

(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。

解説：外部委託に係る業務の終了時における情報セキュリティ対策の確認に関して定めた事項である。

委託先に請け負わせた業務において情報セキュリティ対策が契約に従い適切に実施されていることが、その後の運用におけるセキュリティレベルの維持及び向上の前提となる。このため、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、委託先において実施さ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の判断に加えることが重要である。

1.2.5.2 業務継続計画との整合的運用の確保

趣旨（必要性）

独立行政法人Ａ機構においては、「中央省庁業務継続ガイドライン 第１版」（平成 19 年 6 月、内閣府）に基づき、業務の継続に重大な支障を来し、あるいは外部の人々の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。他方では、業務継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、独立行政法人Ａ機構の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。

これらのことを勘案し、本項では、業務継続計画と情報セキュリティ対策の整合的運用の確保及び不整合の報告に関する対策基準を定める。

適用範囲

BCP を整備し、又は整備を予定している独立行政法人等に適用する。

遵守事項

(1) 業務継続計画と情報セキュリティ対策の整合性の確保

【基本遵守事項】

(a) 情報セキュリティ委員会は、独立行政法人Ａ機構において業務継続計画又は独立行政法人Ａ機構対策基準を整備する場合には、業務継続計画と独立行政法人Ａ機構対策基準との整合性の確保のための検討を行うこと。

解説：業務継続計画と独立行政法人Ａ機構対策基準は、特定の事態に対して、それぞれの体系において定められることがあり得る。当該事態の例として、情報システムの稼動を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画及び独立行政法人Ａ機構対策基準のそれぞれで定める対策に矛盾があると、双方の遵守を求められる独立行政法人Ａ機構組織及び職務従事者は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画と独立行政法人Ａ機構対策基準の間で整合性を確保するよう検討を行うことが必要である。

本管理基準の 1.2.1.1 項で情報セキュリティ委員会は独立行政法人Ａ機構対策基準の策定を求められているが、その策定及び見直しの際に、独立行政法人Ａ機構が業務継続計画で定め、又は定めることが予定されている要求事項を情報セキュリティ委員会が把握した上で、業務継続計画の整備計画を担当する者と協議し双方の定めを調整する必要がある。また、業務継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が独立行政法人Ａ機構対策基準に影響するかどうかを確認し、必要があれば、独立行政法人Ａ機構対策基準の改訂を行う等して、業務継続計画との整合の確保に努めなければならない。

(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、独立行政法人Ａ機構において業務継続計画の整備計画がある場合には、全ての情報システムについて、当該業務継続計画との関係の有無を検討すること。

解説：業務継続計画と情報セキュリティ関係規程との整合性を確保する前提として、独立行政法人Ａ機構の情報システムのうち、業務継続計画と関係のある情報システムを特定することを求める事項である。

(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、独立行政法人Ａ機構において業務継続計画の整備計画がある場合には、当該業務継続計画と関係があると認めた情報システムについて、以下に従って、業務継続計画と独立行政法人Ａ機構対策基準に基づく共通の実施手順を整備すること。

(ア) 通常時において業務継続計画と独立行政法人Ａ機構対策基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。

解説：例えば、事態発生時には、業務の継続以外の対応として、独立行政法人Ａ機構の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障をきたすおそれがある。このため、セキュリティ確保の面で配慮を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、施設全体の入館管理だけでなく、各執務室や各職務従事

者の卓上の情報セキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。
また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ずる必要がある。

（イ）事態発生時において業務継続計画と独立行政法人Ａ機構対策基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定を整備すること。

解説：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に、業務継続計画と自らが担当する実施手順の整合性の確保を求める事項である。整合性を確保するための対応には、通常時の運用において実施するものと、事態発生時に実施するものがある。事態発生への対応として、業務継続計画及び独立行政法人Ａ機構対策基準のそれぞれにおいて事態発生時における情報システムの稼動水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対策を実施手順において具体的に定める等が想定される。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。
これらの目標及び対策を業務継続計画及び情報セキュリティ関係規程の双方で定めることとなるため、相互の整合性を確保するための規定の整備が必要となる。
また、事態発生時には、情報システムの主体認証情報（パスワード）を設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。しかしながら、個人が管理しているパスワードの共用（共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。このため、個人が管理しているパスワードを聞き出したり、共用するために管理者において控えを管理する手順を業務継続計画で安易に認めるべきではなく、これに代わる手順を十分検討する必要がある。
手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、ついで、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生

時用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容を記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。

(2) 業務継続計画と情報セキュリティ関係規程の不整合の報告

【基本遵守事項】

(a) 職務従事者は、独立行政法人A機構において業務継続計画の整備計画がある場合であって、業務継続計画と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。

解説：本来、業務継続計画と情報セキュリティ関係規程が定める要求事項との整合性については、上記(1)及び(2)の遵守事項を適正に実施することで担保されるものである。しかしながら、業務継続計画の対象となる状況においては、事前に想定していなかった様々な不整合が発生すると考えられる。業務継続計画の重要性を考慮すると、万が一、不整合について、情報セキュリティ委員会等が事前に想定できなかった場合にも、それを迅速に改善できるようにしておくべきである。

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

趣旨（必要性）

職務においては、その事務の遂行のために複数の者が共通の情報を利用する場合がある。この際、利用者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し、又は入手した段階で、全ての利用者において認識を合わせるための措置が必要となる。

これらのことを勘案し、本項では、情報の作成及び入手に関する対策基準として、業務以外の情報の作成又は入手の禁止、情報の作成又は入手時における格付と取扱制限の決定、格付と取扱制限の明示等、格付と取扱制限の加工時における継承についての遵守事項を定める。

遵守事項

(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)　職務従事者は、職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。

解説：職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を求める事項である。

(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

【基本遵守事項】

(a)　職務従事者は、情報の作成時及び職務従事者以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。

解説：作成又は入手した情報について、以降、適切な情報セキュリティ対策が実施されるように、機密性、完全性及び可用性の格付及び取扱制限を決定することを求める事項である。

情報の格付が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障害・事故等の直接の原因となった人物のほか、情報の格付及び明示等を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、職務従事者が、情報の格付及び取扱制限とその明示等を確実に行うことは重要である。

なお、格付及び取扱制限の決定をする際は、要件に過不足が生じないように十分注意しなければならない。格付及び取扱制限として決定する要

件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなって事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを職務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。
特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。
例えば、本来要機密情報とする情報を要機密情報に格付けないことは不適切であるが、逆に、本来要機密情報ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けることも不適切であることに注意すること。
また、取扱制限については必要性の有無を検討し、その結果指定しないという決定を行っても差し支えない。
電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から、格付及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した格付及び取扱制限に基づき、その指定を行うこと。
なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。

(b) 職務従事者は、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。

解説：元の情報の修正、追加、削除のいずれかにより、格付又は取扱制限を変更する必要が生じた場合には、格付及び取扱制限の再決定を行う必要がある。
例えば、以下のような場合が考えられる。
・機密性の低い情報に機密性の高い情報を追加したことによって、情報の機密性が上がる場合
・機密性の高い情報から機密に該当する部分を削除したことによって、情報の機密性が下がる場合
なお、情報の格付及び取扱制限は、独立行政法人Ａ機構対策基準に沿った対策を適正に実施するための基礎となる重要な事項であることについては、前記のとおりである。このため、これらを変更するに当たっても適正な手続により実施する必要がある。情報の格付及び取扱制限の変更には、大別して再決定と見直しがある。
再決定した場合には、再決定後の新たな格付等の決定者は再決定した者となる。見直しについては、1.3.1.2 情報の利用（4）を参照のこと。

(3) 格付と取扱制限の明示等

【基本遵守事項】

(a) 職務従事者は、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。

解説：作成者又は入手者によって格付及び取扱制限が決定された情報に対して、以降、他者が当該情報を利用する際に必要とされる情報セキュリティ対策の内容を示すため、情報の格付及び取扱制限の明示等を行うことを求める事項である。「明示等」とは、情報を取り扱う全ての者が当該情報の格付及び取扱制限について共通の認識となるように措置することをいい、情報ごとの格付の区分及び取扱制限の種類を当該情報に記載することによる明示を原則とする。なお、格付の区分及び取扱制限の種類を記載していたとしても、当該ファイルを参照する者が、その内容を参照する際に格付の区分及び取扱制限の種類を特段の手順なく視認することができない状態（例えば、文書ファイルのプロパティ設定に格付の区分を記載することや、文章閲覧時に画面表示はされず印刷しかされないヘッダ部分に記載すること等）については、記載しても明示に当たらない。

格付及び取扱制限の明示等は、当該情報が、電磁的ファイルとして取り扱われることが想定される場合にはファイル名自体又は情報内容の中に、外部電磁的記録媒体に保存して取り扱うことが想定される場合には外部電磁的記録媒体に、書面に印刷されることが想定される場合には書面のヘッダ部分等に、それぞれ記載する必要がある。

既に書面として存在している情報に対して格付や取扱制限を明示等する場合には、手書きによる記入又はスタンプ等による押印が必要である。

なお、原則として各書面それぞれに明示等すべきであるが、取り扱う単位がフォルダ単位や冊子単位の時には、その単位ごとに明示等することも可能である。

なお、格付及び取扱制限の明示等とあわせて、情報の作成者又は入手者の氏名、所属、連絡先等を記載することも有益である。

明示等を行うに当たっては、格付の区分及び取扱制限の種類を記載することによる明示が原則であるが、以下のような場合に明示等を簡便化してもよい。

① 格付及び取扱制限の明示等を簡便化できる場合

特定の情報（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）の格付及び取扱制限を規定等により明記し、当該情報にアクセスする全ての者に当該規定を周知している場合は、格付の区分及び取扱制限の種類について記載することを省略することができる。

具体的な例としては、次のような場合が考えられる。

・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の区分及び取扱制限を規定等により明記し、当該情報システムの利用者にあらかじめ周知している場合。

・取り扱う情報の格付が機密性１、完全性１及び可用性１の場合には、記載による明示を簡便化できることを規定等により周知している場合。ただし、格付及び取扱制限の明示等を簡便化した場合には、以下の事項に注意する必要がある。

格付及び取扱制限の明示等を簡便化した場合の注意事項

① 格付及び取扱制限の決定を認識できない者への情報の提供

格付の区分及び取扱制限の種類が記載されていない要保護情報を、格付及び取扱制限の決定内容を認識できない職務従事者に提供する必要が生じた場合（例えば、他独立行政法人Ａ機構に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限の種類を記載した上で提供しなければならない。

② 取扱制限の明示等を簡便化した場合における取扱制限の追加・変更

例えば、簡便化に係る規定等により、特定の文書ファイルについて、取扱制限の種類の記載を省略している場合において、当該ファイルのうち一部のファイルについて取扱制限を追加するときは、追加する取扱制限の種類のみを記載すること。また、取扱制限を解除する場合は、当該解除する取扱制限を「送信可」「印刷可」等のように記載することが考えられる。

ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記すること。

(4) 格付と取扱制限の加工時における継承

【基本遵守事項】

(a) 職務従事者は、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。

解説：作成の際に参照した情報又は入手した情報が既に機密性に係る格付又は取扱制限の指定がされている場合には、元となる格付及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、引用した新たな情報において適切な格付及び取扱制限を決定すること。

1.3.1.2 情報の利用

趣旨（必要性）

職務においては、その遂行のために多くの情報を利用するが、利用者の認識不足等により情報を不適切に取り扱うと、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。このリスクに対応するため、職務の遂行において、情報は、格付等に応じて定められた手続に従い、適切に利用しなければならない。

これらのことを勘案し、本項では、情報の利用に関する対策基準として、業務以外の利用の禁止、格付及び取扱制限に従った情報の取扱い、格付及び取扱制限の複製時における継承、格付及び取扱制限の見直し、要保護情報の取扱いについての遵守事項を定める。

遵守事項

(1) 業務以外の利用の禁止

【基本遵守事項】

(a) 職務従事者は、職務の遂行以外の目的で、情報を利用しないこと。

解説：職務の遂行以外の目的で、情報を利用しないことを求める事項である。

(2) 格付及び取扱制限に従った情報の取扱い

【基本遵守事項】

(a) 職務従事者は、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。

解説：情報に明示等された格付及び取扱制限に従って、適切に取り扱うことを求める事項である。

(3) 格付及び取扱制限の複製時における継承

【基本遵守事項】

(a) 職務従事者は、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。

解説：複製の際に元となる情報が既に機密性に係る格付又は取扱制限の明示等がされている場合には、元となる格付及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、複製した新たな情報において適切な格付及び取扱制限を決定すること。

(4) 格付及び取扱制限の見直し

【基本遵守事項】

(a) 職務従事者は、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。

解説：利用する元の情報への修正、追加、削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。

また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は同人の上司に相談し、その是非を検討することになる。

ただし、元の決定者等のいずれかによる再決定がない限り、当該情報の利用者がそれらの者に無断で、格付又は取扱制限を変更することは許されない。

見直しにより元の決定者等に相談することが必要となる例として以下のような場合が考えられる。

・作成時には非公開だった情報が正規の手続によって公開されることで機密性が失われた場合（時間の経過により変化した場合）

・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合

・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合

・格付及び取扱制限を決定した時の判断が不適切であったと考えられる場合

・行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等における情報の取扱いに変更がある場合

相談を受けた決定者等は、次項(b)に基づいて所要の措置を講ずることになる。

(b) 職務従事者は、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。

解説：いずれの理由であっても、適切な格付又は取扱制限がなされていない場合は、情報セキュリティ対策が適正に実施されないおそれが生ずるため、適切な格付又は取扱制限に変更することを求める事項である。

また、同一の情報が異なる格付又は取扱制限とならないように、変更以前に当該情報を参照した者に対しても、格付又は取扱制限が変更された旨を周知させることに努める必要がある。

当該情報を直接提供した相手やそれを参照したと思われる者を特定することが困難な場合には、わかる範囲で構わない。

(5) 要保護情報の取扱い

【基本遵守事項】

(a) 職務従事者は、職務の遂行以外の目的で、要保護情報を独立行政法人Ａ機構外に

持ち出さないこと。

解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、職務従事者が職務の遂行以外の目的で要保護情報を独立行政法人Ａ機構外へ持ち出すことを禁止する事項である。

なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。

(b) 職務従事者は、要保護情報を放置しないこと。

解説：第三者による不正な操作や盗み見等を防止することを求める事項である。例えば、離席する際には、ロック付きスクリーンセーバーを起動するあるいはログオフして、画面に情報を表示しないこと、また、机の上に書類を放置して長時間離席しない、印刷した書面を速やかに回収し出力トレイに放置しないこと等を徹底する必要がある。

(c) 職務従事者は、機密性３情報を必要以上に複製しないこと。

解説：不必要な複製によって情報漏えいの危険性が高くなることを考慮し、必要以上に機密性３情報を複製しないことを求める事項である。

なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ） 第６項 では、「 「極秘」の文書の複製は、絶対に行なわないこと。「秘」の文書は、指定者の承認をうけて複製することができること。」と定めている。

なお、これを徹底させる手段として、「複製禁止」の取扱制限の明示等が挙げられる。

(d) 職務従事者は、要機密情報を必要以上に配付しないこと。

解説：情報漏えいを未然に防ぐため、要機密情報の配付は最小限にとどめることを求める事項である。

なお、これを徹底させる手段として、「配付禁止」の取扱制限の明示等が挙げられる。

【強化遵守事項】

(e) 特に重要な情報において必要に応じ、職務従事者は、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。

解説：秘密としての管理を求められる期間を明記することにより、必要以上の秘密管理を防止するための事項である。

なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ） 第５項 では、「秘密文書には、秘密にしておく期間を明記し、その期間が経過した時は、秘密の取扱いは、解除されたものとする。ただし、その期間中秘密にする必要がなくなったときは、その旨を通知して秘密の解除を行うものとすること。」と定めている。

(f) 特に重要な情報において必要に応じ、職務従事者は、機密性３情報である書面には、一連番号を付し、その所在を明らかにしておくこと。

解説：機密性３情報である書面に一連番号を付与し、個別に所在管理を行うことを求める事項である。
配付時に一連番号を付与することによって、当該機密性３情報を受領した者に、一定の管理義務を要請する効果も期待できる。
なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ） 第 4 項 では、「 「極秘」の文書には、必ず一連番号を付し、その所在を明らかにしておくこと。」と定めている。

1.3.1.3 情報の保存

趣旨（必要性）

職務においては、その事務の継続性を確保する等の必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。

これらのことを勘案し、本項では、情報の保存に関する対策基準として、格付に応じた情報の保存及び保存期間における取扱い又は保存期間満了後の取扱期間についての遵守事項を定める。

遵守事項

(1) 格付に応じた情報の保存

【基本遵守事項】

(a) 職務従事者は、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。

解説：電磁的記録媒体に保存された情報、書面又は重要な設計書に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切に保存することを求める事項である。
例えば、職務従事者が書面又は重要な設計書を保存する場合は、安全区域内の棚に保存したり、必要なく情報の参照等をさせないために、施錠のできる書庫・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報（パスワード）によるロック機能を利用して、当該媒体の利用を防止することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。
一方、職務従事者が要保護情報に関する情報処理を行う場合は、例えば、安全区域に設置された情報システム上に保存すること等が考えられる。また、職務従事者が許可を得て、個人で利用する ASP・SaaS サービスの外部の情報システムを用いて、要保護情報に関する情報処理を行う場合は、独立行政法人Ａ機構対策基準と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適

用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。

(b) 職務従事者は、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。

解説：電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める事項である。

電磁的記録媒体に保存された情報には電子計算機等を利用してアクセスすることになるため、アクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができ、これらを選択し組み合わせて、適切なアクセス制御を実現する。

情報システムに職務従事者自らがアクセス制御設定を行う機能が装備されている場合には、職務従事者は、当該情報の格付及び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行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性２情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。例えば、上書き禁止の属性を付与する方法としては、ファイルに対する書込権限者の制限、又はファイルのセキュリティ設定でパスワード設定した上での読取専用の設定等がある。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、職務従事者が取扱上注意することで、その指示を遵守することになる。

(c) 職務従事者は、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。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。

方法としては、文書作成アプリケーションによるパスワード保護オプション、圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。

なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

(d) 職務従事者は、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。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、その暗号化を行うことを求める事項である。

暗号化を行うと情報の復号ができる者を限定することとなり、独立行政

法人A機構内において情報の機密性を高めるために有効である。また、万一 PC、光ディスク、USB メモリ等の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。
情報を暗号化する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(e) 職務従事者は、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。

解説：要保全情報を電磁的記録媒体に保存する場合、その改ざんのおそれを勘案し、必要に応じて電子署名を付与することを求める事項である。
情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(f) 職務従事者は、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。

解説：情報のバックアップ又は複写の取得を求める事項である。
バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。障害・事故等に備えて適切な頻度で復元の演習も行い、職務従事者に習熟させる。
なお、バックアップした記録媒体の紛失・盗難により情報が漏えいするおそれがあるため、必要に応じて、その情報を暗号化することが望ましい。

(g) 職務従事者は、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。

解説：バックアップ又は複写の適切な保管を求める事項である。
例えば、バックアップ又は複写を防火金庫に保管することや、同時被災に備えて遠隔地に保管すること等が考えられる。

(2) 情報の保存期間

【基本遵守事項】

(a) 職務従事者は、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。

解説：電磁的記録媒体に保存された情報に関して、情報セキュリティ確保の観点から保存期間を定めている場合に、当該保存期間に従って管理することを求める事項である。
職務従事者は、情報セキュリティ上、必要な期間は確実に情報を保存するとともに、その期間を経過した場合には当該情報を速やかに消去してリスクの増大を回避する必要がある。また、当該情報が記載されている

行政文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか、利用の制限についての意見を付す等して移管するものとする。その際、本管理基準及び技術基準における遵守事項に従いつつ、例えば、職務従事者でパスワードを設定していた場合は、解除する等して移管先がその内容を参照できるように配慮すること。

1.3.1.4 情報の移送

趣旨（必要性）

職務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部電磁的記録媒体及び PC の運搬、書面の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。

これらのことを勘案し、本項では、情報の移送に関する対策基準として、情報の移送に関する許可及び届出、情報の送信と運搬の選択、移送手段の決定、記録媒体及び電磁的記録の保護対策についての遵守事項を定める。

遵守事項

(1) 情報の移送に関する許可及び届出

【基本遵守事項】

(a) 職務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書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。

解説：機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する際に課室情報セキュリティ責任者の許可を求める事項である。

なお、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望ましい。

(b) 職務従事者は、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。

解説：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際に課室情報セキュリティ責任者に届け出ることを求める事項である。

なお、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情報である書面を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望ましい。また、届出を必要としない移送を定める際

には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(2) 情報の送信と運搬の選択

【基本遵守事項】

(a) 職務従事者は、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。

解説：要保護情報の安全確保に留意した移送を求める事項である。

届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(3) 移送手段の決定

【基本遵守事項】

(a) 職務従事者は、要保護情報又は重要な設計書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。

解説：多種多様な移送手段の中から要保護情報又は重要な設計書を安全に移送するための手段の選択を求める事項である。

「移送手段」とは、送信については独立行政法人Ａ機構内通信回線、信頼できるプロバイダ、VPN 及び暗号メール(S/MIME)等、運搬については信頼できる運送業者や、情報セキュリティ責任者が指定する運送役務及び職務従事者自らによる携行等が挙げられる。なお、「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、電子メールの暗号化の方式の１つである。

また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(4) 記録媒体の保護対策

【基本遵守事項】

(a) 職務従事者は、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。

解説：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おける情報セキュリティ対策を求める事項である。

職務従事者は、外部電磁的記録媒体、PC、書面又は重要な設計書等を運搬する場合には、例えば、外見ではその内容が要機密情報であると知ら

れないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。

(5) 電磁的記録の保護対策

【基本遵守事項】

(a) 職務従事者は、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。

解説：移送手段の種別を問わず、受取手以外の者が要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。

方法としては、文書作成アプリケーションによるパスワード保護オプション及び圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。

なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

(b) 職務従事者は、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。

解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。情報を暗号化する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(c) 職務従事者は、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。

解説：要保全情報を移送する場合、必要に応じて電子署名の付与を行うことを求める事項である。情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(d) 職務従事者は、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。

解説：要保全情報を移送する場合、必要に応じてバックアップを取得することを求める事項である。

(e) 職務従事者は、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。

解説：要安定情報を移送する場合、必要に応じて所要の措置を講ずることを求める事項である。

【強化遵守事項】

(f) 特に重要な情報において必要に応じ、職務従事者は、要機密情報である電磁的記録を移送する場合には、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こと。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。
要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。
この考え方は、専門用語で秘密分散技術といわれ、例えば、１個の電子情報についてファイルを２個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方を 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で郵送する方法が挙げられる。

1.3.1.5 情報の提供

趣旨（必要性）

職務においては、その事務の遂行のために職務従事者以外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがある。

これらのことを勘案し、本項では、情報の提供に関する対策基準として、情報の公表及び他者への情報の提供についての遵守事項を定める。

遵守事項

(1) 情報の公表

【基本遵守事項】

(a) 職務従事者は、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。

解説：公表すべきでない情報の公表を防止することを求める事項である。
独立行政法人Ａ機構の業務においては、保有する情報をウェブサイト等により広く外部の人々に提供する場合がある。この場合には、公表しようとする情報に対する格付の適正さを再度検討し、必要に応じて格付の変更等を行った上で、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必要がある。
なお、情報セキュリティ関係規程の定めによらず、当該情報が法律の規定等で公表が禁じられたものでないことは別途確認する必要がある。

(b) 職務従事者は、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。

解説：職務従事者が意図せず情報を漏えいすることを防止するための事項である。
例えば、公開する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作

成履歴が残っていることがないように除去することが考えられる。また、電子ファイル上でアプリケーションの機能を用いて特定の部分の情報を黒塗りしたとしても、当該部分の情報の閲覧が可能となる場合があることに留意し、黒塗りされた部分の情報そのものの削除や置換えを行うことも検討する必要がある。

(2) 他者への情報の提供

【基本遵守事項】

(a) 職務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を職務従事者以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。

解説：機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を職務従事者以外の者に提供する際に課室情報セキュリティ責任者の許可を得ることを求める事項である。

(b) 職務従事者は、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情報である書面を職務従事者以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。

解説：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情報である書面を職務従事者以外の者に提供する際に課室情報セキュリティ責任者に届け出ることを求める事項である。

届出を必要としない提供を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(c) 職務従事者は、要保護情報又は重要な設計書を職務従事者以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。

解説：要保護情報又は重要な設計書を職務従事者以外の者に提供する場合において遵守すべきことを定める事項である。

要保護情報又は重要な設計書を職務従事者以外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。

確実に伝達する方法として、提供先が管理基準及び技術基準に準じた組織の場合には、管理基準及び技術基準による情報の格付及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付の区分だけを示すのでは不十分である。なぜなら、提供先においては当該格付区分がどのように取り扱われるべきものであるかが認識できないからである。

格付の区分（例えば、「機密性２」と記載する）で示すのであれば、当該格付の区分の定義について提供先にあらかじめ周知しておくか、格付の

区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す（例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要がある。

職務従事者は、格付及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付及び取扱制限に従った取扱いを確保するため、提供する前に、明記が不要とされている情報の格付及び取扱制限を当該書面又は電磁的記録に明記すること。

(d) 職務従事者は、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。

解説：職務従事者が意図せず情報を漏えいすることを防止するための事項である。

例えば、提供する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作成履歴が残っていることがないように除去することが考えられる。

1.3.1.6 情報の消去

趣旨（必要性）

職務において利用した電子計算機、通信回線装置及び外部電磁的記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報を消去する際に、適切な措置が講じられていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されない。

これらのことを勘案し、本項では、情報の消去に関する対策基準として、電磁的記録の消去方法及び書面の廃棄方法についての遵守事項を定める。

遵守事項

(1) 電磁的記録の消去方法

【基本遵守事項】

(a) 職務従事者は、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。

解説：電磁的記録媒体を廃棄する場合に、全ての情報を復元が困難な状態にすることを求める事項である。

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。また、ファイルの情報自体へ別の情報を

上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、内蔵電磁的記録媒体及び外部電磁的記録媒体に記録されている全ての情報を適切な方法で復元が困難な状態にする必要がある。

抹消するための方法としては、例えば、次の方法が挙げられる。

・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを個々に抹消する方法

・ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法

・媒体を物理的に破壊する方法

なお、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。

・FD 等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等して情報を記録している内部の円盤を破壊する方法

・CD-R/RW、DVD-R/RW 等の光学媒体の場合には、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法

(b) 職務従事者は、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。

解説：電磁的記録媒体に保存された不要な情報を抹消することを求める事項である。

長期にわたり利用された内蔵電磁的記録媒体及び外部電磁的記録媒体には、要機密情報が断片的に残留した状態となっているおそれがある。そのため、電磁的記録媒体を用いて職務従事者以外の者に情報を提供する場合や、担当者間による業務の引継ぎを伴わず、別の業務に機器等を引き継ぐことが想定される場合には、データを抹消する必要がある。

【強化遵守事項】

(c) 特に重要な情報において必要に応じ、職務従事者は、電磁的記録媒体について、設置環境等から必要があると認められる場合は、当該電磁的記録媒体の要機密情報を抹消すること。

解説：無人の執務室に設置されていたり、設置場所及び利用場所が確定していない電子計算機、通信回線装置及び外部電磁的記録媒体等、安全といえない環境で利用される電子計算機等に要機密情報を残留させないことを求める事項である。職務従事者は、要機密情報が保存された電子ファイル又は空き領域に残留する情報を抹消すること。

(2) 書面の廃棄方法

【基本遵守事項】

(a) 職務従事者は、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。

解説：電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却又は溶解等により、復元が困難な状態にすることを求める事項である。なお、廃棄すべき書類が大量である等の理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。

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

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。

なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。

遵守事項

(1) 識別コードの管理

【基本遵守事項】

(a)　職務従事者は、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。

解説：自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、なりすまし行為であることを認識する必要がある。仮に、悪意がない行為であっても、他者の識別コードを使って情報システムを利用することは、安易に許容されてはならない。

例えば、何らかの障害により自己の識別コードの利用が一時的に不可能になった場合には、まず、当該情報システムを使って行おうとしている業務について、他者へ代行処理依頼することを検討すべきであり、仮に他者の許可を得たとしても、当該者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを用いて、情報システムを利用するということは制限されなければならない。また、業務の継続のために、他者の識別コードを用いることが不可避の場合には、例外措置の承認を行う際に本人の事前の了解に加えて、情報システムセキュリティ管理者の了解を得ることが最低限必要である。極めて緊急性が高い場合には、他者の識別コードを利用していた期間とアクセスの内容を、事後速やかに、情報システムセキュリティ管理者に報告しなければならない。情報システムセキュリティ

管理者は、その理由と利用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えるのが望ましい。
いずれの場合も、用いる識別コードの本人からの事前の許可を得ずに、その者の識別コードを用いて、情報システムを利用することは禁止されるべきである。
遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。

(b) 職務従事者は、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。

解説：共用する識別コードについても情報システムセキュリティ管理者から各本人に個別に付与されるものであり、付与された者がそれを他者に付与、貸与してはならない。また、情報システムセキュリティ管理者が明示的に共用識別コードとしているもの以外の識別コードを、共用してはならない。
遵守事項に「主体認証に用いるために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。

(c) 職務従事者は、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。

解説：ほとんどの場合には、識別コード自体は必ずしも秘密ではないが、積極的に公開したり、公然となるような放置はしないようにすることを求める事項である。
本来、主体認証のためには、主体認証情報が用いられるが、識別コード自体も秘密にすることによって、不正に主体認証される可能性をより低くすることが可能となる。そのため、識別コードについても適切に管理することが求められる。

(d) 職務従事者は、職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。

解説：識別コードを利用する必要がなくなった場合に、職務従事者自らが情報システムセキュリティ管理者へ届け出ることを求める事項である。ただし、例えば、人事異動等によって、職務従事者の識別コードが大規模に変更となる場合や、その変更を情報システムセキュリティ管理者が職務従事者自らからの届出によらずして把握できる場合等、職務従事者自らの届出が不要となる条件を情報システムセキュリティ責任者が定めても

良い。

【強化遵守事項】

(e) 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必要に応じ、職務従事者は、管理者権限を持つ識別コードを付与された場合には、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。

解説：管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用することを求める事項である。

例えば、情報システムのオペレーティングシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更等をしないときには、administrator 権限なしの識別コードを使用し、設定変更をするときにだけ administrator 権限で再ログインすることを遵守しなければならない。

なお、本遵守事項は、実際には繁雑な操作を必要とする場合があるため、最少特権機能が設けられている場合は、これを遵守するべきであるが、当該情報システムで取り扱う情報の重要性等を勘案し、必要に応じて選択されたい。

(2) 主体認証情報の管理

【基本遵守事項】

(a) 職務従事者は、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。

解説：職務従事者は、自らの主体認証情報自体の露呈や主体認証情報に関連する情報の露呈又はそれらが露呈した可能性がある場合には、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へ報告することを求める事項である。

(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。

解説：自らが発見したり、報告を受けたりして、主体認証情報の他者使用又は危険発生を知った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が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるログオン制限等がある。

(c) 職務従事者は、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。

解説：職務従事者は、例えば自己の主体認証情報を内容が分かる状態で付箋に記入して貼付するようなことを行ってはならず、主体認証情報を入力する際に周囲からの盗み見に注意を払ったり、管理者を名乗って主体認証

情報を聞き出す行為に注意したりする等、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。

解説：職務従事者が他者に処理代行させるために自己の主体認証情報を教示しないことを求める事項である。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関連があいまいとなる可能性があり、アクセス制御、権限管理、証跡管理その他のセキュリティ対策の基礎が崩壊する可能性がある。また、教示された側にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己の主体認証情報は他者に「教えない」ことを徹底すべきである。

(ウ) 主体認証情報を忘却しないように努めること。

解説：他者が容易に見ることができないような措置（施錠して保存する等）や、他者が見ても分からないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取ることそのものを禁ずるものではない。むしろ、忘れることのないようにもしなければならない。

なお、本人の忘却によって主体認証情報を初期化（リセット）する場合に備えて、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。

(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。

解説：辞書に載っている単語、利用者の名前や利用者個人に関連する情報から簡単に派生させたもの等、容易に推測されるものを用いてはならない。また、使用する文字種として、数字だけでなく、アルファベットの大文字及び小文字、更に特殊記号等も織り交ぜて主体認証情報を構成することが望ましい。

(オ) 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。

解説：定期的な変更の要求を自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達する等の運用によって対処することでも差し支えない。

(d) 職務従事者は、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。

解説：所有による主体認証方式では、それを取得した者が正当な主体として主体認証されることになるため、他者に使用されることがないように、また、紛失等で、その可能性がある場合の報告を徹底する必要がある。異動等により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、これを返却する必要がある。

(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。

解説：利用者の指紋情報等、主体認証情報として生体情報を取り扱う場合には、個人のプライバシーに配慮し、個人情報として厳格な管理が求められる。管理方法としては、元の生体情報が再現できないように保存すること等が考えられる。

(3) 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、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。

解説：原則として、識別コードは、情報システムへアクセスする主体へ個別に付与することになる。しかしながら、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必要がある場合には、当該情報システムごとに利用許可の判断をすることを求める事項である。

(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

解説：情報システムへアクセスする主体に対して、識別コード及び主体認証情報を付与する際の関連手続を明確に定めることを求める事項である。また、情報システムへアクセスする主体ごとに、確実にアクセス権を設定するため、関連手続を明確に定めることを求める事項である。

(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。

解説：権限の管理については、情報システムのセキュリティ保護上、非常に重要な役割を果たすため、権限管理を行う者を定める事項である。

(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

【基本遵守事項】

(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職務従事者から、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。

解説：情報システムを利用する職務従事者においては、何らかの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合が想定される。例えば、知識による主体認証方式であれば主体認証情報（パスワード）を忘れた場合、所有による主体認証方式であれば携帯するのを忘れた場合、指紋による主体認証方式であれば指を怪我した場合等が挙げられる。

それらの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合には、代替手段の使用に関する許可申請をすることができる。情報システムセキュリティ管理者は、その申請を受理した時には、その申請が正当な利用者からの許可申請であること及び許可申請の理由が妥当であること等を確認した上で、その必要性を判断し代替手段を提供することを求める事項である。なお、代替手段としては、例えば、当日限り有効とした暫定的な識別コード及び主体認証情報の提供や、当該情報システムから切り離された代替 PC の提供、情報システムを利用しない業務環境の提供等が想定されるが、情報システムセキュリティ管理者が情報セキュリティ保護の観点に加えて職務従事者本人による業務執行の緊急性、効率性、利便性及び当該情報システムの可用性等も考慮して、適正な代替手段を準備しておくこと。

なお、代替手段の提供に当たっては、その申請理由と使用期間、使用者等を記録として残すことが望ましい。

(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。

解説：自らが発見したり、報告を受けたりして、識別コードの不正使用を知った場合には、他の項目で定められている障害・事故等の対処に係る遵守事項とともに、本遵守事項の対処を実施する。

なお、不正使用による被害が甚大であると予想される場合には、例えば、全ての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得することが望ましい。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行することが望ましい。

1.4.2　情報処理の制限

1.4.2.1 独立行政法人A機構外での情報処理の制限

趣旨（必要性）

職務においては、その事務の遂行のため、独立行政法人Ａ機構外において情報処理を実施する必要が生ずる場合がある。この際、独立行政法人Ａ機構外での実施では物理的な安全対策を講ずることが比較的困難になることから、職務従事者は、施設内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

これらのことを勘案し、本項では、独立行政法人Ａ機構外での情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

遵守事項

(1) 安全管理措置についての規定の整備

【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独立行政法人Ａ機構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。

解説：統括情報セキュリティ責任者が、独立行政法人Ａ機構外において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を求める事項である。ただし、情報処理の種類により個別の規定を設けても構わない。独立行政法人Ａ機構外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通した通信の形態、関与する独立行政法人Ａ機構内外の者等に応じた措置を示した規定を整備する必要がある。

(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独立行政法人Ａ機構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。

解説：統括情報セキュリティ責任者が、独立行政法人Ａ機構外に要保護情報を取り扱う情報システムを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を求める事項である。持ち出す情報システム及び持ち出し先等を具体的に想定して規定を整備する必要がある。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

(a)　職務従事者は、機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ機構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。

解説：機密性３情報、完全性２情報又は可用性２情報に係る情報処理を独立行政法人Ａ機構外で行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。

当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。
なお、「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(b) 職務従事者は、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独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、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、各々の責任の範囲において届出を必要としない独立行政法人Ａ機構外での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(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、独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構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を求める事項である。
「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(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情報について独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構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報告の有無を確認し、措置を講ずること等を求める事項である。
状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、職務従事者に改めて許可を得るようにさせること。

(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、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独立行政法人Ａ機構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。

解説：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

て独立行政法人Ａ機構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、期間の延長が必要な状況であれば職務従事者に改めて届出をさせる等の措置を講ずることを求める事項である。

(f) 職務従事者は、要保護情報について独立行政法人Ａ機構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。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を独立行政法人Ａ機構外で情報処理することを最小限にとどめることを求める事項である。

(g) 職務従事者は、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独立行政法人Ａ機構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。

解説：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独立行政法人Ａ機構外に持ち出す職務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該持ち出しの業務上の必要性については課室情報セキュリティ責任者の、当該持ち出しの安全性については情報システムセキュリティ責任者の許可を得ることとなる。

(h) 職務従事者は、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独立行政法人Ａ機構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。

解説：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独立行政法人Ａ機構外に持ち出す職務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、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、各々の責任の範囲において届出を必要としない独立行政法人Ａ機構外への持ち出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(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独立行政法人Ａ機構外への持ち出しに係る記録を取得すること。

解説：要保護情報を取り扱う情報システムの独立行政法人Ａ機構外への持ち出しに係る記録を取得することを求める事項である。

「持ち出しに係る記録」には、持ち出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(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独立行政法人Ａ機構

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。

解説：情報システムを独立行政法人Ａ機構外に持ち出すことを許可した期間が終了した時に報告の有無を確認すること等を求める事項である。
状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、職務従事者に改めて許可を得るようにさせること。

(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独立行政法人Ａ機構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。

解説：届出期間が長期にわたる場合等、必要に応じて、独立行政法人Ａ機構外への持ち出しの状況を確認することを求める事項である。
状況を確認した際に、期間の延長が必要な状況であれば、職務従事者に改めて届出をさせること。

(l) 職務従事者は、要保護情報を取り扱う情報システムを独立行政法人Ａ機構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。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を取り扱うシステムを独立行政法人Ａ機構外に持ち出すことを最小限にとどめることを求める事項である。

(3) 安全管理措置の遵守

【基本遵守事項】

(a) 職務従事者は、要保護情報について独立行政法人Ａ機構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。

解説：職務従事者に対して、独立行政法人Ａ機構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を求める事項である。

(b) 職務従事者は、機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ機構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。

解説：職務従事者に対して、独立行政法人Ａ機構外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。

(c) 職務従事者は、要保護情報を取り扱う情報システムの独立行政法人Ａ機構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。

解説：職務従事者に対して、情報システムの独立行政法人Ａ機構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を求める事項である。
定められた安全管理措置の内容としては、例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリ

ーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、操作を実施できなくすること等が考えられる。

(d) 職務従事者は、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独立行政法人Ａ機構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。

解説：職務従事者に対して、独立行政法人Ａ機構外へ情報システムの持ち出しが終了したことを、その許可を与えた者に報告することを求める事項である。

1.4.2.2 独立行政法人A機構支給以外の情報システムによる情報処理の制限

趣旨（必要性）

職務においては、その遂行のため、独立行政法人Ａ機構支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、独立行政法人Ａ機構が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できない。

これらのことを勘案し、本項では、独立行政法人Ａ機構支給以外の情報システムによる情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

遵守事項

(1) 安全管理措置についての規定の整備

【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独立行政法人Ａ機構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。

解説：職務従事者が所有する個人の PC 等を用いて要保護情報に関する情報処理を行う場合であっても、独立行政法人Ａ機構支給の情報システムと同程度のセキュリティ対策を施す必要があるため、その安全管理措置についての規定を整備することを求める事項である。ただし、情報システムの種類により個別の規定を設けても構わない。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

(a) 職務従事者は、機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ機構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。

解説：機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ

機構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、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。

独立行政法人Ａ機構支給以外の情報システムによる機密性３情報、完全性２情報又は可用性２情報の情報処理を許可する場合は、その期間については、最長で１年間にすることが望ましい。ただし、期間の延長が必要な状況であれば、職務従事者に改めて許可を得るようにさせること。

(b)　職務従事者は、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独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構支給以外の情報システムによる機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、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、各々の責任の範囲において届出を必要としない独立行政法人Ａ機構支給以外の情報システムによる情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(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、独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構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を求める事項である。

「独立行政法人Ａ機構支給以外の情報システムによる情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(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情報について独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構支給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、報告の有無を確認すること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、職務従事者に

改めて許可を得るようにさせること。

(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、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独立行政法人Ａ機構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。

解説：届出期間が長期にわたる場合等、必要に応じて、独立行政法人Ａ機構支給以外の情報システムによる情報処理の状況を確認することを求める事項である。状況を確認した際に、期間の延長が必要な状況であれば、職務従事者に改めて届出をさせること。

(3) 安全管理措置の遵守

【基本遵守事項】

(a) 職務従事者は、要保護情報について独立行政法人Ａ機構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。

解説：職務従事者が所有する個人の PC 等、独立行政法人Ａ機構支給以外の情報システムを用いて要保護情報に関する情報処理を行う場合であっても、独立行政法人Ａ機構支給の情報システムと同程度のセキュリティ対策を施す必要があるため、職務従事者に安全管理措置を講ずることを求める事項である。

(b) 職務従事者は、機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ機構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。

解説：職務従事者が機密性３情報、完全性２情報又は可用性２情報について独立行政法人Ａ機構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、その報告を求める事項である。

独立行政法人Ａ機構支給以外の情報システムの利用許可を与えた者は、その終了報告を受け、独立行政法人Ａ機構支給以外の情報システムによる情報処理の状況を把握することが可能となる。その結果、独立行政法人Ａ機構支給以外の情報システムを、本来必要とされる期間を超えて利用している場合には、これを検知し、利用実態を是正することが可能となる。

【強化遵守事項】

(c) 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必要に応じ、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独立行政法人Ａ機構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直接確認すること。

解説：情報システムセキュリティ責任者に対して、許可又は届出を受理した要

保護情報を取り扱う独立行政法人Ａ機構支給以外の情報システムについて、独立行政法人Ａ機構支給の情報システムと同程度のセキュリティ対策が施されていることの確認を求める事項である。
確認する頻度は、情報処理の開始時や一定期間経過後等、独立行政法人Ａ機構の特性に応じて設定することが望ましい。また、当該情報システムが固定されている等の理由で、情報システムの運搬が不可能な場合には、当該情報システムが設置されている現地に赴いて確認することが望ましい。
なお、あらかじめ情報システムセキュリティ責任者が認めた場合には、情報システムセキュリティ責任者が指定した者に確認させることも考えられる。その際には、情報システムセキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。

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

趣旨（必要性）

情報システムは、目的業務を円滑に遂行するため、その計画、構築、運用、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせてセキュリティ対策を実施する必要がある。

これらのことを勘案し、本項では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。

遵守事項

(1) 情報システムの計画

【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。

解説：情報システムを統括する責任者（情報化統括責任者（ＣＩＯ））が確立した体制が、セキュリティ維持の側面からも実施可能な体制（人員、機器、予算等）となるように求める事項である。

なお、「情報システムを統括する責任者」とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を想定している。

(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、外部の人々・企業と独立行政法人Ａ機構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。

解説：情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。

「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。

具体的なセキュリティ要件については、独立行政法人Ａ機構対策基準において技術基準に対応して定められた事項、本管理基準の「1.5.2　情報システムに係る規定の整備と遵守」に対応するものも含めた独立行政法人Ａ機構の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。
決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。
また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが発生しないようにすること。
なお、物理的に分割されたシステムに限らず、論理的に分割されたシステムも同様に考慮すること。「論理的に分割されたシステム」とは、一つの情報システムの筐体上に複数のシステムを共存させることを目的として、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。

(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。

解説：情報システムのセキュリティ要件を満たすために必要な対策を定めることを求める事項である。
情報システムにおいて必要な対策としては、独立行政法人Ａ機構対策基準において技術基準に対応して定められた事項、本管理基準の「1.5.2　情報システムに係る規定の整備と遵守」に対応するものも含めた独立行政法人Ａ機構の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件に基づく対策がある。

(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の有無を検討し、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。

解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択肢がある場合、ISO/IEC 15408 に基づく 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ものを選択することを求める事項である。第三者による情報セキュリティ機能の客観的な評価によって、安全性の高い情報システムの構築が期待できる。

製品分野として当該認証を取得する必要性の判断については、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ることが望ましい。なお、国際承認アレンジメント（CCRA）参加国における ISO/IEC 15408 に基づく認証取得製品又は実質的に CC 認証取得製品とセキュリティ機能上同等であると確認されている製品（上記のリストを参照）を活用することが考えられる。

(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。

解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。

情報セキュリティの侵害とは、要保護情報について機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。

監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、独立行政法人Ａ機構の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の安全区域への立ち入り等があり得る。

また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。

（１）設ける監視機能を定める。監視機能には、以下の例がある。

・独立行政法人Ａ機構外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能（侵入検知システム等による）

・不正プログラム感染や踏み台に利用されること等による独立行政法人Ａ機構外への不正な通信を監視する機能

・独立行政法人Ａ機構内通信回線への PC の接続を監視する機能

・PC への外部記録媒体の挿入を監視する機能

・サーバ装置等の機器の正常な動作を監視する機能

・安全区域への人の出入を監視する機能

（２）監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。

（３）監視によりプライバシーを侵害する可能性がある場合は、当該職務従事者等への説明について定める。

(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。

解説：情報システムセキュリティ責任者に、セキュリティの観点での試験等の実施により当該情報システムがセキュリティ要件を満たすことを確認し、

運用段階への導入の方法、体制、作業手順、スケジュール、期間、教育やトラブル対処について手順を整備することを求める事項である。

【強化遵守事項】

(g) 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必要に応じ、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に重要なセキュリティ要件があると認めた場合には、当該情報システムの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、情報システムを更改し、又は構築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。

解説：重要なセキュリティ要件がある情報システムについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を受けることを求める事項である。

「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。情報システムの構築が終了するまでにセキュリティ設計仕様書について、ST 評価及び ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。

なお、情報システムの構築を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。

(2) 情報システムの構築及び運用

【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。

解説：情報システムのセキュリティ要件に基づき機器等の購入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についての対策及び監視を実施し、情報システムを構築、運用することを求める事項である。

(3) 情報システムの移行及び廃棄

【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。

解説：情報システムの移行及び廃棄を行う場合に、情報システムを構成する機

器の扱い、情報の格付等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を講ずることを求める事項である。

(4) 情報システムの見直し

【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。

解説：情報システムのセキュリティ対策について、必要に応じて見直しとそれに必要な措置を求める事項である。見直しを行う時期は、新たなセキュリティ脅威の出現、運用、監視等の状況により判断する必要がある。

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

趣旨（必要性）

独立行政法人Ａ機構の情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うためには、情報システムの管理のために必要な情報を文書として整備する必要がある。また、独立行政法人Ａ機構全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するためには、独立行政法人Ａ機構が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備し、維持管理していく必要がある。

これらのことを勘案し、本項では、独立行政法人Ａ機構における情報システムに係る文書整備及び台帳整備に関する情報セキュリティの対策基準を定める。

遵守事項

(1) 情報システムの文書整備

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、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職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職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
- 通信回線の利用部署

(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

解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、

障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として整備することを定めた遵守事項である。文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。
所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。
電子計算機、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアにセキュリティホールが存在することにより使用上のリスクが高まった場合に、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。
電子計算機の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システム構成要素の管理状況を確実に把握できるようにするとともに、障害・事故等を防止する責任の所在を明確化するために必要な事項である。
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、及び通信回線の利用部署の記載は、通信回線の管理状況を把握するために必要な事項である。
情報システムに係る仕様書又は設計書は、情報セキュリティ対策実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。
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は、当該構成要素のセキュリティを維持する目的で管理者が実施するべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。
障害・事故等が発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。
・業務継続計画で定める当該情報システムを利用する業務の重要性
・情報システムの運用等の外部委託の内容
また手順に記載される内容として、例えば以下が想定される。
・障害・事故等の内容・影響度の大きさに応じた情報連絡先のリスト
・情報システムを障害・事故等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準
・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項
・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

ムに感染した場合等に支援を受けるための外部の専門家の連絡先
なお、統括情報セキュリティ責任者が整備する対処手順（1.2.2.2(1)(c)を参照）により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。

(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。

解説：所管する情報システムの運用管理において、適切なセキュリティ対策を行うことを求める遵守事項である。

(2) 情報システムの台帳整備

【基本遵守事項】

(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) 管理課室及び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) 接続する独立行政法人A機構外通信回線の種別
(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) 管理課室及び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

解説：独立行政法人A機構全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するため、独立行政法人A機構が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備することを求める事項である。

情報システム名、管理課室及び当該情報システムセキュリティ責任者の氏名・連絡先の記載は、独立行政法人A機構が所管する全ての情報システムを把握し、当該情報システムに係る管理責任を把握するために必要な事項である。

システム構成の記載は、情報システムを構成する電子計算機、通信回線及び通信回線装置に関する事項である。当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、独立行政法人A機構としての情報セキュリティ対策を行うために一元的に把握

する必要があると判断する事項を含める必要がある。
接続する独立行政法人Ａ機構外通信回線の種別、取り扱う情報の格付及び取扱制限に関する事項の記載は、当該情報システムを設置し、また運用管理することによるセキュリティ上のリスクを独立行政法人Ａ機構として把握するために必要な事項である。なお、取り扱う情報の格付及び取扱制限に関する事項については、情報システムを構成する電子計算機等について機器別又は機器の形態・目的別に記載することが望ましい。
当該情報システムの設計・開発、運用、保守に関する事項の記載は、実施責任者若しくは実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。
また、情報処理業務を外部委託する場合は、役務名、管理課室及び当該情報システムセキュリティ責任者の氏名・連絡先、契約事業者、契約期間、役務概要、ドメイン名（インターネット上で提供される役務等を利用する場合）、取り扱う情報の格付及び取扱制限に関する事項を記載した決裁に係る書類を集約し、容易に参照できるようにすることで、台帳の代替とすることも可能である。
なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該台帳を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。

(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。

解説：独立行政法人Ａ機構の各情報システムを所管する情報システムセキュリティ責任者が、情報システムに係る台帳に記載の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を求める事項である。
台帳における網羅性の維持のため、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た際、又は更改した際には、速やかに台帳に記載の事項を報告する必要がある。なお、台帳の最新性の維持のため、台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、台帳を更新する必要があるが、その報告の方法やタイミングについては、独立行政法人Ａ機構ごとに定めることが望ましい。

1.5.2.2 機器等の購入

趣旨（必要性）

機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要なセキュリティ機能が装備されていない場合及び購入後にセキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等で取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

この課題に対応するため、機器等を購入する際は、独立行政法人Ａ機構の独立行政法人Ａ機構対策基準に準拠した機器等の購入を行うべく、購入先への要求事項を定める必要がある。

これらのことを勘案し、本項では、機器等の購入に関する対策基準として、統括情報セキュリティ責任者による機器等の購入に係る規定の整備、情報システムセキュリティ責任者による当該規定の遵守についての遵守事項を定める。

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

【基本遵守事項】

(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。

解説：機器等の選定に先立って、機器等の選定基準を整備することを求める事項である。

統括情報セキュリティ責任者は、機器等の選定基準の整備に当たっては、機器等が独立行政法人Ａ機構対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。

選定基準としては、機器等が独立行政法人Ａ機構対策基準の該当項目を満たし、独立行政法人Ａ機構のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を独立行政法人Ａ機構内で統一的に整備することが重要である。

なお、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の購入に反映することが必要である。

(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。

解説：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、当該機能を有する製品の中でも ISO/IEC 15408 に基づく 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製品の優遇を選定基準の一つとすることを求める事項で

ある。
第三者による情報セキュリティ機能の客観的な評価のある製品を選定することによって、より信頼度の高い情報システムが構築できる。

(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。

解説：機器等の納入時の確認・検査に関する手続を定めるものである。
特に、確認・検査手続では、納入された機器等が定められた選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加える手続を組み込む必要がある。
具体的な確認・検査の方法として、必要なセキュリティ機能の実装状況（機器等に最新のパッチが適用されているかどうか、アンチウイルスソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）及び機器等に不正プログラムが混入していないことを、購入先からの報告で確認すること等が挙げられる。

(2) 機器等の購入に係る規定の遵守

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、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。

解説：整備された選定基準に従って、機器等に必要なセキュリティ機能が実装されていること等を確認し、これを機器等の選定における判断の一要素として利用することを求める事項である。

(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。

解説：情報セキュリティ対策の視点を加味して定められた納入時の確認・検査手続に準拠して、納入された機器等の納品検査を行うことを求める事項である。

1.5.2.3 ソフトウェア開発

趣旨（必要性）

ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、当該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脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、アクセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。

加えて、開発するソフトウェアの処理に対するセキュリティホールの混入（設計及び作成時のミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発

者により意図的に埋め込まれること等）についての防止対策も必要となる。

これらのことを勘案し、本項では、ソフトウェアを開発する際の対策基準として、統括情報セキュリティ責任者によるソフトウェア開発に係る規定の整備、情報システムセキュリティ責任者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) ソフトウェア開発に係る規定の整備

【基本遵守事項】

(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。

解説：本遵守事項では、統括情報セキュリティ責任者が情報システムセキュリティ責任者に求める規定を整備することとしているが、別途規定を整備することとはせずに、独立行政法人A機構対策基準内において情報システムセキュリティ責任者に対する遵守事項として（ア）～（セ）の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく情報システムセキュリティ責任者となることに留意すること。

(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。

解説：ソフトウェア開発を実施する体制が、セキュリティ維持の側面からも実施可能な開発体制（人員、機器、予算等）を確保することを求める事項である。

なお、開発体制の確保に当たっては、情報システムを統括する責任者に要求することとなる。ここで、情報システムを統括する責任者とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を指す。

(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。

解説：ソフトウェア開発を委託先に行わせる場合には、ソフトウェア開発を実施する者に実施の責任を負わせるセキュリティに係る要件を選択し、それを委託先に保証させることを求める事項である。「委託先に実施について保証させる」手段は、契約（付随する確認書等を含む。）によることとなる。

(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。

解説：ソフトウェア開発に係る情報資産を保護するための手順及び環境を定めることを求める事項である。「手順」とは、例えば、仕様書及びソースコード等の成果物に対してソフトウェアのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツールを指し、「環境」とは、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用する電子計算機の設置場所及びアクセス制御の方法等を指す。

なお、ソフトウェア開発を外部委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。

(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。

解説：運用中の情報システムを利用してソフトウェアの作成及び試験を行うことにより、運用中の情報システムに悪影響が及ぶことを回避することを求める事項である。これは運用中の情報システム全体ではなく一部だけの場合も同様である。例えば、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにすること等も含まれる。

(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。

解説：開発するソフトウェアに必要となるセキュリティ機能について、その設計を適切に行うとともに、設計書に明確に記録することを求める事項である。

なお、汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、全てを独自開発する場合であっても、外部から察知される脅威（例えば、ＳＱＬインジェクション、バッファオーバーフロー等）は存在するため、開発するソフトウェアの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。

(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。

解説：「管理機能」とは、真正確認及び権限管理等のセキュリティ機能を管理するための機能のほか、故障、事故及び障害等の発生時に行う対処及び復旧に係る機能、事故発生時の証跡保全の機能等を指し、これらの必要性をソフトウェアの設計時から検討することにより、必要がある場合にはソフトウェアに組み込むことを求める事項である。

(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。

解説：ソフトウェアの設計について、脆弱性の原因となる設計の不具合をなくすために、設計レビューの実施を求める事項である。

一般にソフトウェア開発における設計レビューには、①レビュー対象内にあるエラーの発見を第一目的とし、開発責任者等が実施する確認手法（インスペクション）、②開発担当者自身が開発関係者を集め、レビュー対象プログラムを実行の流れに従って追跡し確認する手法（ウォークスルー）等があり、これらを、いつ、誰が、何に対して実施するのか、といったことを定める必要がある。

(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。

解説：ソフトウェアの内部及び入出力するデータについて、処理の誤りや意図的な改ざん等を検出するための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等を組み込むことを求める事項である。

「データの妥当性」とは、例えば、HTML タグや JavaScript、SQL 文等として機能する不正な文字列や通信過程において生じたデータ誤り等、適切なデータ処理の障害になる情報がデータ内に含まれない状態であることを意味している。データの妥当性を確認する方法として、不正な文字列を変換し、又は削除する機能（いわゆるサニタイジング）の付加、チェックデジット（検査数字）による処理の正当性を確認する機能の付加等がある。

(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。

解説：重要なセキュリティ要件があるソフトウェアについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を行うことを求める事項である。

「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入

手がなされることである。ソフトウェアの開発が終了するまでにセキュリティ設計仕様書について、ST 評価及び ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。
なお、ソフトウェア開発を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。

(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。

解説：ソフトウェア開発者が悪意を持って脆弱性を持つソースコードを組み込んでしまうことを防ぐための変更管理や、ソースコードが流出することを防ぐための閲覧制限のためのアクセス制御、ソースコードの滅失及び毀損等に備えたバックアップの取得等を求める事項である。

(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。

解説：ソフトウェア開発者が意図せずに脆弱性の存在するソフトウェアを作成してしまわないように、ソフトウェア開発者が実施するコーディングに関する規定を定めるように求める事項である。
「コーディングに関する規定」とは、コードの可読性の向上や記述ミスの軽減のため、ソフトウェア開発担当者間のコードの記述スタイルのガイドラインとして、使用を控える構文、使用禁止語等を定めたいわゆるコーディング規約に相当する規定を指す。例えば、バッファオーバーフローによる情報の改ざんを防ぐために、データを更新する処理を実行する場合には、そのデータ量が適正であることを確認する処理を付加することを義務付ける等の規定が挙げられる。

(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。

解説：ソースコードレビューの範囲及び方法について定めることを求める事項である。例えば、脆弱性の原因となるソースコードについては、開発言語ごとに典型的なパターンが知られていることから、これらについては静的解析ツール、又はソースコードレビュー等による検証が挙げられる。
なお、ソースコードレビューについては、開発するソフトウェアだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。

(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。

解説：セキュリティの観点から必要な試験がある場合にその試験の項目及び試験方法を定めることを求める事項である。攻撃が行われた際にソフトウェアがどのような動作をするかを試験する項目として想定しており、具体的には、バッファオーバーフローが発生しないか、想定の範囲外のデータの入力を拒否できるか、DoS 攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、といった項目が挙げられる。

なお、セキュリティ機能の試験だけにとどまらず、ソフトウェアの試験計画全般について、セキュリティホールの有無、必要なチェック機能の欠如等について、単体試験、結合試験、統合試験等の複数の試験を通じて、必要な試験が網羅されるよう留意することが望ましい。

(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。

解説：「実施記録」とは、試験の項目、実施結果、実施時に判明した不具合及び当該不具合の修正の記録等を指し、これらを保存することにより、セキュリティホールを発見した場合の対処に利用できるようにすることを求める事項である。

(2) ソフトウェア開発に係る規定の遵守

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、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。

解説：ソフトウェア開発を行う情報システムセキュリティ責任者が、独立行政法人A機構で整備したソフトウェア開発に係る規定を遵守して、ソフトウェアの開発を行うことを定めた事項である。

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

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

一方、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。また、主体認証情報の機密性と完全性、及びアクセス制御情報の完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、主体認証・アクセス制御・権限管理・証跡管理・保

証等の必要性判断等に関する対策基準として、統括情報セキュリティ責任者による主体認証・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、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による当該規定の遵守、情報システムセキュリティ責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。

なお、1.4.1.1 において識別コードと主体認証情報の管理等に関する判断基準を、技術基準 2.2.1.1~2.2.1.5 においても主体認証・アクセス制御・権限管理・証跡管理・保障等の導入等に関する対策基準を定めている。

遵守事項

(1) 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

【基本遵守事項】

(a) 統括情報セキュリティ責任者は、独立行政法人Ａ機構における主体認証・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。

解説：本遵守事項では、統括情報セキュリティ責任者が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に求める規定を整備することとしているが、別途規定を整備することはせずに、独立行政法人Ａ機構対策基準内において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に対する遵守事項として（ア）～（カ）の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく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となることに留意すること。

(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。

解説：主体認証を行う前提として、情報システムセキュリティ責任者に、各情報システムについて、アクセスする主体の主体認証を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、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。

解説：アクセス制御を行う前提として、情報システムセキュリティ責任者は、各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しなければならない。要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。

なお、アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。

http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf

(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。

解説：権限管理を行う前提として、情報システムセキュリティ責任者に、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。

なお、アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与（発行、更新及び変更を含む。以下この項において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。

(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。

解説：証跡管理を行う前提として、情報セキュリティ責任者に、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を求める事項である。

情報セキュリティは、独立行政法人Ａ機構の内部及び外部からの不正アクセス、不正侵入、誤操作又は不正操作等の様々な原因により損なわれることがある。また、職務の遂行以外の目的でウェブの閲覧や電子メールの送受信がなされるおそれもある。万一問題が発生した場合にはその実行者を特定する必要があるため、一連の事象を情報システムで証跡として取得し、保存する必要がある。

証跡として多くの情報を取得すれば、事後追跡及び事前抑止の効果は高まる。その反面、多くの証跡を取得する場合には、情報システムの処理能力及び記憶容量を多く消費することになる。情報セキュリティ責任者は、この両面に配慮し、また情報システムの重要度や取り扱う証跡管理情報の機密性も考慮して、証跡として取得する情報と、証跡を取得する箇所を決定する必要がある。

証跡には、以下のような管理記録が考えられる。

・識別コードの発行等の管理履歴
・各識別コードへのアクセス権設定の管理履歴
・それらの権限管理者の許認可そのものの管理履歴

また、証跡として、上記の他に以下のような利用記録や監視記録等を含めることも考えられる。

・利用者による情報システムの操作記録
・操作する者、監視する者及び保守する者等による情報システムの操作記録

・ファイアウォール、侵入検知システム（Intrusion Detection System）等通信回線装置の通信記録
・プログラムの動作記録
なお、証跡管理を行う必要性の有無の判断に当たっては、情報システムの側面だけではなく、組織的な側面からの検討も必要であるため、情報セキュリティ責任者によるものとしている。

(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。

解説：証跡を取得する場合に、取得する情報項目及び証跡の保存期間を適切に定めることを求める事項である。
以下に示す例は一般的に取得すべき基本的な情報項目であるが、限られた情報量で実効性のある証跡を取得するように設計することが重要である。
証跡に含める情報項目の例：
・事象の主体である者又は機器を示す識別コード等
・事象の種類（ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等）
・事象の対象（アクセスした URL（ウェブアドレス）、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等）
・日付、時刻
・成功、失敗の区別、事象の結果
・電子メールのヘッダ情報、通信内容
・通信パケットの内容
・操作する者、監視する者及び保守する者等への通知の内容
また、保存期間は、１つの情報システムであっても取得する箇所や情報項目により異なることもあり得る。
情報セキュリティに関する問題を事後に追跡し、また事前に抑止するという証跡管理の目的に照らして、保存期間を定めることになる。

(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。

解説：証跡の取得等について、あらかじめ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説明を行うことを求める事項である。
取得、保存する証跡には、情報システムの管理者、操作員及び利用者等の行動に関する情報が記録される。そのため、証跡を取得、保存し、事後に参照、点検、分析する可能性があることを、利用者に説明する必要がある。なお、証跡を証拠として活用する際の正当性を高めるためにも

周知することが望ましい。

(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。

解説：要保護情報を取り扱う情報システムについて、情報が適切な状態であることを保証するための対策の必要性の有無を検討することを求める事項である。

(2) 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

【基本遵守事項】

(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、独立行政法人A機構における主体認証・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。

解説：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が、独立行政法人A機構で主体認証・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遵守して、情報システムの導入を行うことを定めた事項である。

(3) 取得した証跡の点検、分析及び報告

【強化遵守事項】

(a) 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必要に応じ、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、又は情報セキュリティ責任者に報告すること。

解説：取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずることにより、情報セキュリティを維持し、あるいはその侵害を早期に検知することを求める事項である。

取得した証跡は、その全てを定期的に精査することは一般には困難であり、その一部を重点あるいは指標として点検及び分析することが有効である。重点項目の内容と証跡の量を定期的に点検し、その範囲で通常とは異なる状況が見られた場合に更に詳細な点検及び分析を行うことも考えられる。

証跡の点検、分析及び報告を支援するための自動化機能が設けられていれば、これを利用することにより、作業を効率的かつ確実に行うことができる。

情報セキュリティの侵害が特定された場合は、復旧及び再発防止のために必要な対策を採らなければならない。

1.5.2.5 暗号と電子署名の標準手順

趣旨（必要性）

情報システムの利用において、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐためには、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、職務従事者による個別判断で選択されることのないよう、独立行政法人A機構で標準となる手順を定めることが重要である。

これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、統括情報セキュリティ責任者による暗号と電子署名に係る規定の整備、職務従事者による当該規定の遵守についての遵守事項を定める。

なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。

遵守事項

(1) 暗号と電子署名に係る規定の整備

【基本遵守事項】

(a) 統括情報セキュリティ責任者は、独立行政法人A機構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。

解説：独立行政法人A機構内の情報システムにおける暗号化及び電子署名について、使用を認めるアルゴリズム及び方法を統括情報セキュリティ責任者が定めることを求める事項である。アルゴリズム及び方法は、暗号及び電子署名の使用場面等に応じて整備することも可能である。例えば、電子メールの暗号化に関してアルゴリズムを定めるとともにその方法を S/MIME とし、ウェブサーバとブラウザの通信の暗号化に関してアルゴリズムを定めるとともに方法を SSL とする。他に、データベースのデータ暗号化や、電子申請における電子署名等についても、アルゴリズム及び方法を定めることが考えられる。

職務従事者は、文書の作成、電子メールの送受信等に汎用のソフトウェアを日常的に使用しているが、これらのソフトウェアでは、暗号化及び電子署名について、複数のアルゴリズムを用意し、設定画面等で利用者が選択できるようにしている場合がある。そのような場合には、職務従

事者は、（ア）にもとづき電子政府推奨暗号リストに記載されたアルゴリズムを選択して使用することになる。
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、情報システムセキュリティ責任者は、本遵守事項に基づき統括情報セキュリティ責任者が定めたアルゴリズム及び方法を使用する。
暗号化又は電子署名を行う特定の箇所について見ると、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、複数のアルゴリズムを実装し、使用可能とする場合がある。この場合には、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、電子政府推奨暗号リストに記載されたアルゴリズムを少なくとも一つ含めることを求める。
もしも(イ)について規程策定者がこの部分を緩和するには、「ただし・・・」以後の文を強化遵守事項に移すよりも、たとえば、（１）遵守事項文章はこのままとして、運用上で包括的な例外承認手続きを実施するか、（２）遵守事項文章の「電子政府推奨暗号リスト」の箇所を「電子政府推奨暗号リスト又は情報セキュリティ委員会における検証済み暗号リスト」などと添削するなどして、『いずれかの手続きにしたがって技術的に予め検証された暗号を選択すること』を義務付けることが望ましい。

(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。

解説：アルゴリズムが危殆化した場合に備えて、情報システムの停止等の緊急避難的な対応計画を策定することを求める事項である。対象となるアルゴリズムは、用途に応じて変わることに留意すること。

(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)及び(イ)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

解説：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を定めることによって、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の適正な管理を求める事項である。
暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵の生成手順や有効期限等が定められている時は、安全性を検討の上、これを準用することが可能である。
また、電子署名の有効期限については、当該有効期限満了までの間、その正当性を検証可能なものとする必要がある。

(イ) 鍵の保存手順

解説：鍵の保存手順を保存方法及び保存場所を含めて定めることによって、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の適正な管理を求める事項である。
鍵の保存方法としては、電磁的記録媒体に保存することが考えられるが、それをどのように保存するかの方法や、保存する際に電磁的記録媒体以外の記録媒体と併用することの是非等についても定める必要がある。
暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵を保存する電磁的記録媒体や保存場所が定められている時は、安全性を検討の上、これを準用することが可能である。
情報システム共通として鍵の保存手順を定める場合には、統括情報セキュリティ責任者が直接それを定めることが考えられる。あるいは、情報システムごとに鍵の保存手順を個別に定めるのであれば、各情報システムセキュリティ責任者にそれを定めさせることについて、定めるという方法でもよい。

【強化遵守事項】

(c) 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必要に応じ、統括情報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のバックアップの取得手順又は鍵の預託手順（以下「鍵のバックアップ手順等」という。）を定めること。

解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、鍵のバックアップ手順等を定めることを求める事項である。
例えば、復号に用いる鍵を紛失し、又は消失した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得し、又は信頼できる第三者へ鍵情報を預託する等の対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。
なお、本遵守事項における鍵のバックアップ手順等は、前事項の鍵の管理手順等に含めて整備することも可能である。

(d) 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必要に応じ、統括情報セキュリティ責任者は、独立行政法人Ａ機構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。

解説：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書を GPKI が発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。

(2) 暗号と電子署名に係る規定の遵守

【基本遵守事項】

(a) 職務従事者は、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。

解説：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、独立行政法人Ａ機構で定めたアルゴリズム及び方法を遵守することを求める事項である。

(b) 職務従事者は、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。

解説：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が露呈した場合、暗号化された情報の漏えいや電子署名の偽造等のおそれがある。そのため、職務従事者による鍵情報の保護を求める事項である。

【強化遵守事項】

(c) 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必要に応じ、職務従事者は、暗号化された情報の復号に用いる鍵について、定められた鍵のバックアップ手順等に従い、そのバックアップを取得すること。

解説：鍵の書換え、紛失、消失等により、その完全性、可用性が侵害された場合には、暗号化により保護されている情報を復号することが困難となり、可用性が損なわれる可能性がある。そのため、職務従事者による鍵のバックアップを求める事項である。

1.5.2.6 独立行政法人A機構外の情報セキュリティ水準の低下を招く行為の防止

趣旨（必要性）

独立行政法人Ａ機構が、独立行政法人Ａ機構外の情報セキュリティ水準の低下を招くような行為をすることは、独立行政法人Ａ機構外に対して適切な行為でないことは当然であって、その行為が他者の情報セキュリティ水準を低下させることによって、独立行政法人Ａ機構を取り巻く情報セキュリティ環境を悪化させるため、独立行政法人Ａ機構にとっても好ましくない。

これらのことを勘案し、本項では、独立行政法人Ａ機構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対策基準として、統括情報セキュリティ責任者による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の整備、職務従事者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) 措置についての規定の整備

【基本遵守事項】

(a) 統括情報セキュリティ責任者は、独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構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して、統括情報セキュリティ責任者が、規定を整備することを求める事項である。

独立行政法人Ａ機構外の情報セキュリティ水準の低下を招く可能性のある行為としては、例えば、以下のものが挙げられる。

（ア）不適切なソフトウェア及びサービスの使用要求：電子行政サービス（例えば、独立行政法人Ａ機構のウェブによるコンテンツの提示等を言う。以下同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービスへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。

（イ）ソフトウェアの不適切な設定要求：電子行政サービスを利用するために、利用者の環境にインストールされているソフトウェア（独立行政法人Ａ機構が直接提供していないソフトウェア（例えば、クライアント PC の OS やウェブブラウザ等）以下同じ。）について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。

（ウ）ソフトウェア等の不適切な削除要求：独立行政法人Ａ機構のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。

「明示的に要求する行為」とは、「『このような設定を変更してください。』等のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけではなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。

以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。

・ソフトウェアを実行させる場合：電子行政サービスのためのソフトウェアを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windows の「.exe」ファイル等）、ランタイム環境実行型（例えば、Java アプレットや Windows の ActiveX ファイル等）、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの全てを含む。

・HTML メール等を送信する場合：独立行政法人Ａ機構から HTML メール等（利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形

式を用いたメールのこと。）を送信する場合に注意する必要がある。

これらの場合については、結果的に利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある。実行させるソフトウェアの提供については、オンラインによる提供（ウェブへの掲載、メールの添付等）について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については電子署名を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。
やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。
また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。

ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。
また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名（コード署名）が必要な場合には、政府認証基盤（GPKI）で発行したコード署名証明書を利用することが望ましい。
なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。
（ア）（イ）については、当該電子行政サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該電子行政サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める等の方法を考えることができる。
例えば、電子行政用ウェブのアプリケーションを利用するために、利用者の PC 上にあらかじめ標準的にインストールされているソフトウェアがバージョンＡであったとする。その後、そのソフトウェアの最新バージョンがＢに更新され、また、バージョンＡについて脆弱性が公開された場合には、バージョンＢで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョンＡだけで動作するような設計では、利用者に脆弱性の

あるバージョンＡを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンＢでも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。

(2) 規定の遵守

【基本遵守事項】

(a) 職務従事者は、独立行政法人Ａ機構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。

解説：独立行政法人Ａ機構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独立行政法人Ａ機構の役割を定めた事項である。職務従事者は、組織及び個人として措置を講ずることが重要である。

1.5.2.7 ドメイン名の使用についての対策

趣旨（必要性）

独立行政法人Ａ機構では、行政に係る情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサーバ、電子メール等を用意し、外部の人々等の利用に供している。これらのサービスはインターネットを介して利用するものであるため、外部の人々等にとっては、そのサービスが実際の独立行政法人Ａ機構のものであると信頼できることが重要である。一方、インターネット上のサービスの特定はドメイン名（例えば、nisc.go.jp のこと。）が重要な役割を果たしており、独立行政法人Ａ機構において一貫したドメイン名を使用することにより、万一独立行政法人Ａ機構以外の者による悪用や詐称がなされた場合にも外部の人々が気付くための条件を整備する必要がある。

これらのことを勘案し、本項では、独立行政法人Ａ機構におけるドメイン名の使用に関する対策基準として、統括情報セキュリティ責任者によるドメイン名の使用についての規定の整備、職務従事者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) ドメイン名の使用についての規定の整備

【基本遵守事項】

(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、以下の事項を職務従事者に求める規定を整備すること。

解説：本遵守事項では、統括情報セキュリティ責任者が職務従事者に求める規定を整備することとしているが、別途規定を整備することとはせずに、独立行政法人Ａ機構対策基準内において職務従事者に対する遵守事項として（ア）～（ウ）の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく

職務従事者となることに留意すること。

(ア) 職務従事者は、職務従事者以外の者（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、以下の独立行政法人Ａ機構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独立行政法人Ａ機構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。

解説：アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.example.go.jp/）や FTP サーバ（例えば、ftp://ftp.example.go.jp/）等へのアクセスを促すことをいう。上記には、ウェブページの閲覧に必要なソフトウェア（プラグインを含む）を入手できる政府ドメイン名以外のウェブサイトを告知する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先（例えば、null@example.go.jp）への送信等を促すことをいう。

本遵守事項における告知にあたる場合とは、情報提供のきっかけが独立行政法人Ａ機構側にある場合で、告知にあたらない場合とは、情報提供のきっかけが独立行政法人Ａ機構側にない場合である。例えば、職務従事者以外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらず、本遵守事項の対象とはならない。なお、いずれの場合についても媒体の種類（郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。

「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。

なお、在外公館のように国外在住の者を対象とし、かつ、現地のルール

に従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。
政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなものが考えられる。
（例）
・この告知についてのお問い合わせは、null@example.go.jp までご連絡ください。
・この告知で案内しているウェブサイトは○○○協会が運営しており、独立行政法人A機構が運営しているものではありません。
・この告知で案内しているウェブサイトのアドレスについては、2007 年 12 月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。

(イ) 職務従事者は、職務従事者以外の者に対して、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、独立行政法人A機構外の者にとって、当該職務従事者が既知の者である場合を除く。

解説：送信に使用する電子メールのドメイン名として政府ドメインの使用を求める遵守事項である。
また、電子メールの送信元として政府ドメイン名を使用するに当たっては、その送信に用いる電子メールサーバは、当該政府ドメイン名にかかる DNS サーバの MX レコードで指定している IP アドレスのサーバである必要がある。
なお、送信元として使われる電子メールアドレスを外部に告知する場合には、適切なドメイン名で告知するように、事前に準備する必要がある。

(ウ) 職務従事者は、職務従事者以外の者に対して、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。

解説：職務従事者以外の者にアクセスさせることを目的として情報を保存するサーバとは、主としてウェブサーバのことをいう。
（ア）により政府ドメイン名以外のドメイン名を告知することを禁止しているが、告知していなくとも、独立行政法人A機構としての情報を政府ドメイン名以外のドメイン名のウェブサーバに保存していると、インターネット上の検索サービス等により表示される場合がある。そのような場合には、なりすましをしようとする者が、独立行政法人A機構からの情報を装った内容を保存したウェブを作成して、検索されるのを待ち伏せするという方法によるなりすましが考えられる。普段から政府ドメイン名のウェブサーバだけを使うことで、検索結果が政府ドメイン名以外である場合に、そこに保存されている情報の真偽について独立行政法人A機構以外の者が注意を心がけやすくできる。

なお、既存のウェブサーバ等においてこれら以外のドメイン名のサーバの使用が避けられない場合には、本遵守事項に対する例外措置を必要な期間に限り適用し、かつ、政府ドメイン名のサイトから当該ドメイン名を案内することにより、新規に告知するドメイン名について（ア）を遵守すること。
また、政府ドメイン名以外のウェブサーバの使用を停止した後も、当該ドメイン名を不正に利用されないように管理することに注意しなければならない。具体的には、そのような用途に使用した当該ドメイン名については、使用後も登録管理を一定期間維持することを求める規定を設ける必要がある。

(2) ドメイン名の使用についての規定の遵守
【基本遵守事項】
(a) 職務従事者は、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。
解説：全ての職務従事者が、インターネットを経由した行政サービスの提供に当たり、独立行政法人Ａ機構で整備したドメイン名の使用についての規定を遵守して、政府ドメイン名等のドメイン名を適切に使用することを定めた事項である。
なお、ウェブサイトの構築・管理等の「ドメイン名の使用」を伴う業務を外部委託する場合は、職務従事者が委託先への要求事項に含める必要がある。
そのような業務の外部委託は、情報システム部門以外の者が担当となる場合があるため、それらの者にも本遵守事項を周知すること。

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

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。不正プログラムへの感染を防止するためには、情報システムを利用する全ての職務従事者が、アンチウイルスソフトウェア等を活用して不正プログラムの検知・除去に努めるほか、ファイルの閲覧や実行、外部ファイルの取り込み等において十分な注意を払う必要がある。

これらのことを勘案し、本項では、不正プログラム感染の回避を目的とした対策基準として、統括情報セキュリティ責任者による不正プログラム対策に係る規定の整備、職務従事者による当該規定の遵守について遵守事項を定める。

遵守事項

(1) 不正プログラム対策に係る規定の整備

【基本遵守事項】

(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、以下の措置を職務従事者に求める規定を整備すること。

解説：本事項では、統括情報セキュリティ責任者が職務従事者に求める規定を整備することとしているが、別途規定を整備することとせずに、独立行政法人A機構対策基準内において直接に職務従事者に対する遵守事項として（ア）～（キ）の事項を定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく職務従事者となることに留意すること。

(ア) 職務従事者は、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。

解説：不正プログラムに感染したソフトウェアを実行した場合には、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に労力を要するため、不正プログラムとして検知された実行ファイル等の実行を禁止する事項である。

なお、アンチウイルスソフトウェア等が全ての現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行うことが望ましい。予防措置とは、例えば、差出人が不明な電子メールに添付された不審なファイルを実行しないこと、ウェブクライアントのセキュリティ設定を不必要に低下させないこと、不審なウェブサイトを閲覧しないこと等である。

(イ) 職務従事者は、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。

解説：アンチウイルスソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。

自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。

また、最新の状態に維持する方法としては、端末ごとに利用者が自動化の設定をする方法のほか、情報システムセキュリティ責任者等が管理する端末を一括して自動化する方法もあるため、情報セキュリティ責任者が適切な方法を選択すること。同様に(ウ)～(オ)の事項は、情報セキュリティ責任者が適切な方法を選択すること。

(ウ) 職務従事者は、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。

解説：人為による対策の漏れや遅れを回避するために、不正プログラム対策の中で自動化が可能なところは自動化することを求める事項である。
ファイルの作成、参照等のたびに検査を自動的に行う機能をオンに設定し、その機能をオフにしないことが必要である。

(エ) 職務従事者は、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。

解説：定期的に不正プログラムの有無を確認することを求める事項である。
前事項の自動検査機能が有効になっていたとしても、検査した時点における不正プログラム定義ファイルでは検知されない不正プログラムに感染している危険性が残る。このような危険性への対策として、定期的に全ての電子ファイルを検査する必要がある。

(オ) 職務従事者は、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。

解説：外部とやり取りするデータやソフトウェアには、ウェブの閲覧やメールの送受信等のネットワークを経由したもののほか、USB メモリや CD-ROM 等の外部電磁的記録媒体によるものも含む。
不正プログラムの自動検査による確認ができていればそれで差し支えない。

(カ) 職務従事者は、不正プログラム感染の予防に努めること。

解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等が全ての不正プログラムを検知できるとは限らないことに注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないこと等がある。

(キ) 職務従事者は、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、必要な措置を講じること。

解説：不正プログラムに感染したおそれがある電子計算機については、他の電子計算機への感染等の被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講じることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等をすることが挙げられる。

(2) 不正プログラム対策に係る規定の遵守

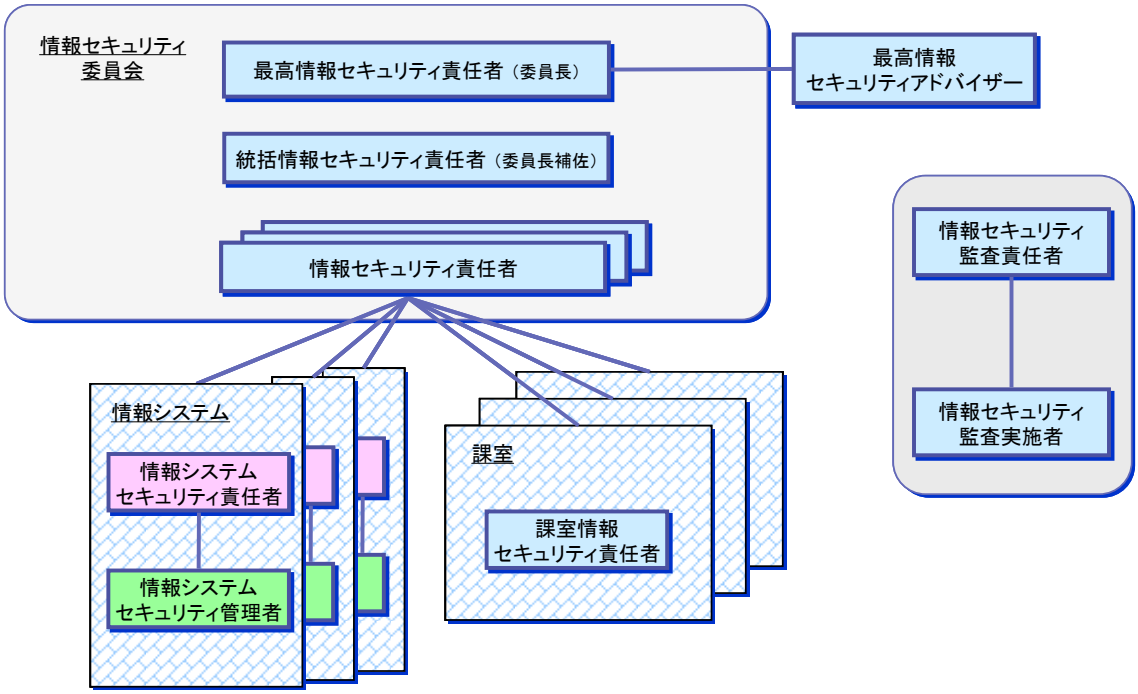
【基本遵守事項】

(a) 職務従事者は、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。

解説：全ての職務従事者が、不正プログラム対策に係る規定に基づき、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を定めた事項である。

A.1 解説書別添資料

A.1.1 組織・体制イメージ図



A.1.2 取扱制限の種類に係る付表例

解説：取扱制限の例として以下の表に記載のものを想定したが、独立行政法人A機構において、このうちから必要な取扱制限の種類を採用し、また、不足している場合は適宜追加して構わない。
取扱制限は必要に応じて指定するものであるから、規程では例示するだけとして、「情報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る」という目的を果たせるのであれば、記載する表現方法を一律に定めないという運用方法でも構わない。例えば、「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」等と記載しても目的を果たせると考えられる。

機密性についての取扱制限の定義

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配付について	配付禁止、配付要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日迄○○禁止

上記の指定方法の意味は以下のとおり。
・「○○禁止」
当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
・「○○要許可」
当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
・「暗号化必須」
当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。
・「○○限り」
当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「セキュリティセンター限り」「政策会議委員会出席者限

り」等、参照を許可する者が分かるように指定する。
・「〇月〇日迄〇〇禁止」
例えば、〇月〇日迄複製を禁止したい場合、「〇月〇日迄複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

解説：上記の「〇〇要許可」の補足説明では「〇〇する行為を禁止」とは明言をせずに、「許可を得る必要がある」とすることで、暗黙に「許可を得なければ禁止」という文章例を示した。そうではなく、はっきりと「〇〇する行為を禁止するが、許可を得ることにより〇〇することができる」といった表現等も考えられる。分かりやすく、簡便な表現であることが望ましい。
「複製禁止」の指定は、機密性の確保を目的とする以外に、知的財産権保護として指定することにも使用することができる。同様に、「暗号化必須」の指定も機密性だけではなく、完全性のために指定することに役立つ。その旨を補足することで、職務従事者による運用の適切性を増すことができる。

完全性についての取扱制限の定義

取扱制限の種類	指定方法
保存期間について	〇〇まで保存
保存場所について	〇〇において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

情報の保存期間の指定の方法は、以下のとおり。
保存を要する期日である「年月日」又は期日を特定できる用語に「まで保存」を付して指定する。
例）平成〇〇年７月３１日まで保存
例）平成〇〇年度末まで保存
完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。
例）年度内保存文書用共有ファイルサーバに保管
例）３カ年保存文書用共有ファイルサーバに保管

可用性についての取扱制限の定義

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

復旧許容時間の指定の方法は以下のとおり。
復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。
例） １時間以内復旧
例） ３日以内復旧
可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、各自ＰＣのファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。
例）課室共有ファイル保存必須
例）各自ＰＣ保存可

A.1.3 情報セキュリティ対策に関するＢ省が所管する独立行政法人等群における決定等

〔B 省が所管する独立行政法人等群における決定〕

・行政文書の管理方策に関するガイドライン（平成 12 年２月 25 日、各省庁事務連絡会議申し合わせ）

・国の行政機関における情報システム関係業務の外注の推進について（平成 12 年３月 31 日行政情報システム各省庁連絡会議了承）

・各省庁の調達におけるセキュリティ水準の高い製品等の利用方針（平成 13 年３月 29 日行政情報化推進各省庁連絡会議了承）

・各府省の情報システム調達における暗号の利用方針（平成 15 年２月 28 日　行政情報システム関係課長連絡会議了承）

・電子政府推進計画（平成 18 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定）

・行政情報の電子的提供に関する基本的考え方（指針）（平成 16 年 11 月 12 日　各府省情報化統括責任者（CIO）連絡会議決定）

・業務・システム最適化指針（ガイドライン）（平成 18 年３月 31 日　各府省情報化統括責任者（CIO）連絡会議決定）

・情報システムに係る政府調達の基本指針（平成 19 年３月１日　各府省情報化統括責任者（CIO）連絡会議決定）

・国家公務員身分証明書のＩＣカード化（平成 16 年２月６日　e-Japan 戦略 II 加速化パッケージ）

・中央省庁業務継続ガイドライン　第１版（平成 19 年６月　内閣府）

・行政文書の管理の徹底について（平成 19 年 12 月 14 日　関係省庁連絡会議申合せ）

・今後の行政文書の管理に関する取組について（平成 20 年 11 月 25 日　行政文書・公文書等の管理・保存に関する関係省庁連絡会議申合せ）

・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（平成 22 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定）

・IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト（平成 23 年 4 月 21 日　経済産業省）

〔法律〕
・行政機関の保有する情報の公開に関する法律（平成十一年五月十四日法律第四十二号）

・行政機関の保有する個人情報の保護に関する法律（平成十五年五月三十日法律第五十八号）

・公文書等の管理に関する法律（平成二十一年七月一日法律第六十六号）

注）詳細については、原文を参照すること。

A.1.4 用語解説

【あ】

- 「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、定められた演算を施しデータを変換することをいう。
- 「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。

【か】

- 「業務継続計画」とは、中央省庁業務継続ガイドライン 第1版（平成 19 年 6 月、内閣府）に基づき独立行政法人A機構において策定する BCP（Business Continuity Plan: 事業継続計画）をいう。

【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。
- 「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。

【た】

- 「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。
- 「ドメインネームシステム（DNS)」とは、ドメイン名やホスト名と IP アドレスとの

対応関係を管理するデータベースシステムである。

● 「ドメイン名」とは、サーバ装置や通信回線装置に付与した IP アドレスを、扱いやすいように英数字及び一部の記号を用いて表したものをいう。例えば、nisc.go.jp のこと。

【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。

● 「踏み台」とは、第三者によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

【ら】

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

【A～Z】

● 「ASP・SaaS サービス」とは、「Application Service Provider（ASP）」及び「Software as a Service（SaaS）」の略で、インターネットを経由して、アプリケーション機能を利用するサービスをいう。例えば、レンタルウェブサーバの利用、インターネットを経由したウェブアプリケーションの利用等が挙げられる。

● 「BCP（Business Continuity Plan: 事業継続計画）」とは、組織において特定する事業の継続に支障を来すと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。狭義には、このうちの事態発生後の事業の維持を主とした計画をいう。

● 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させる電子計算機をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の二種類に分けることができる。

● 「ST 確認」とは、評価機関による ST 評価の評価結果が妥当であることを認証機関（独立行政法人 情報処理推進機構）が検証し、確認することをいう。

● 「ST 評価」とは、セキュリティ設計仕様書(ST:Security Target)が IT セキュリティ評価基準(ISO/IEC 15408)に適合していることを IT セキュリティ評価方法 CEM（Common Methodology for Information Technology Security Evaluation）に則って、ST の評価を行うことが可能な機関が評価することをいう。

● 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等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。