独立行政法人国立青少年教育振興機構情報セキュリティポリシー

令和４年３月３０日
ＣＩＳＯ　裁　定

目次

第1部　総則

1.1 情報セキュリティポリシーの目的・適用範囲

(1)　情報セキュリティポリシーの目的

この情報セキュリティポリシー(以下「ポリシー」という)は、「政府機関の情報セキュリティ対策のための統一規範(サイバーセキュリティ戦略本部決定)」に基づく政府機関における統一的な枠組みの中で、独立行政法人国立青少年教育振興機構情報システムの整備及び利用に関する規程第６条の規定に基づき、独立行政法人国立青少年教育振興機構(以下「機構」という。)が情報セキュリティ確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めるものとする。

(2)　ポリシーの適用対象

(a)ポリシーにおいて適用対象とする者は、全ての職員等とする。

(b)ポリシーにおいて適用対象とする情報は、以下の情報とする。

（ア）職員等が職務上使用することを目的として機構が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)

（イ）その他の情報システム又は外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)であって、職員等が職務上取り扱う情報

（ウ）(ア)及び(イ)のほか、職員等が調達し、又は開発した情報システムの設計又は運用管理に関する情報

(c)ポリシーにおいて適用対象とする情報システムは、ポリシーの適用対象となる情報を取り扱う全ての情報システムとする。

(3)　ポリシーの改定

情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、情報技術の進歩に応じて、ポリシーを定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。

(4)　法令等の遵守

情報及び情報システムの取扱いに関しては、ポリシーのほか法令及び基準等(以下「関連法令等」という。)を遵守しなければならない。なお、これらの関連法令等は情

報セキュリティ対策にかかわらず当然に遵守すべきものであるため、ポリシーでは、あえて関連法令等の遵守について明記していない。また、情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。

(5)　対策項目の記載事項等

ポリシーでは、機構が行うべき対策について、部、節、及び項の３階層にて対策項目を分類し、各項に対して遵守事項を示している。

遵守事項は、ポリシーにおいて必ず実施すべき対策事項である。機構は、内閣官房内閣サイバーセキュリティセンターが別途策定する政府機関等の対策基準策定のためのガイドライン及び政府機関統一基準適用個別マニュアル群において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、策定するものとする。なお、ポリシーは「政府機関の情報セキュリティ対策のための統一基準(以下、統一基準という。)」に準拠した構成としているが、統一基準では各項に対して遵守事項のほか、目的・趣旨が示されており、職員等はこれを踏まえて遵守事項を実施するものとする。

1.2 情報の格付の区分・取扱制限

(1)　情報の格付の区分

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、ポリシーの遵守事項で用いる格付の区分の定義を示す。

格付の定義を変更又は追加する場合には、ポリシーにおける格付区分と遵守事項との関係が「政府機関の情報セキュリティ対策のための統一基準」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、他機関へ情報を提供する場合は、自身の格付区分とポリシーにおける格付区分の対応について、適切に伝達する必要がある。

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	独立行政法人における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン(平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。)に定める秘密文書に相当する機密性を要する情報を含む情報又は上記に準ずる情報
機密性２情報	独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報

機密性１情報	独立行政法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

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

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報(書面を除く。)のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業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、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

(2) 情報の取扱制限

「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、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを職員等に確実に行わせるための手段をいう。

職員等は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。機構は、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある。

1.3 用語定義

ポリシーにおいて次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

●「アプリケーション・コンテンツ」とは、アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

● 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化(Windows の BitLocker 等)、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

● 「Web(ウェブ)会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像または音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

【か】

● 「外部サービス」とは、機関等外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において機関等の情報が取り扱われる場合に限る。

● 「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

● 「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して機関等に向けて独自のサービスを提供する事業者は含まれない。

● 「外部サービス利用者」とは、外部サービスを利用する機関等の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

● 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。

● 「機関等内通信回線」とは、一つの機関等が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該機関等の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。機関等内通信回線には、専用線やVPN 等物理的な回線を機関等が管理していないものも含まれる。

●「機器等」とは、情報システムの構成要素(サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部電磁的記録媒体等の総称をいう。

●「基盤となる情報システム」とは、他の機関等と共通的に使用する情報システム(一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。)をいう。

● 「業務委託」とは、機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、

全て含むものとする。ただし、当該業務において機関等の情報を取り扱わせる場合に限る。

●「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、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、情報システム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、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

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

●「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

【さ】

●「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、機構が調達又は開発するものをいう。

●「CYMAT（サイマット）」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team(情報セキュリティ緊急支援チーム)の略。

●「CSIRT（シーサート）」とは、機構において発生した情報セキュリティインシデントに対処するため、機構に設置された体制をいう。Computer Security Incident Response Team の略。

●「実施手順」とは、ポリシーに定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

●「情報」とは、「1.1(2)　ポリシーの適用範囲」の(b)に定めるものをいう。
●「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機構が調達又は開発するもの(管理を外部委託しているシステムを含む。)をいう。
●「情報セキュリティインシデント」とは、JIS Q 27000:2014 における情報セキュリティインシデントをいう。
●「情報セキュリティ関係規程」とは、ポリシー及び実施手順を総称したものをいう。
●「情報セキュリティ対策推進体制」とは、機構の情報セキュリティ対策の推進に係る事務を遂行するため、機構に設置された体制をいう。
●「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。
●「職員等」とは、機構の業務に従事している役職員その他機関等の指揮命令に服している者であって、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。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。
●「政府ドメイン名」とは、.go.jp で終わるドメイン名のことをいう。日本国の政府機関、独立行政法人、特殊法人（特殊会社を除く。）が登録（取得）することができる。

【た】
●「対策基準」とは、機構における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
●「端末」とは、情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、機構が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機構が調達又は開発するもの以外を指す「機構支給以外の端末」がある。また、機構が調達又は開発した端末と機構支給以外の端末の双方を合わせて「端末（支給外端末を含む)」という。
●「通信回線」とは、複数の情報システム又は機器等(機構が調達等を行うもの以外のものを含む。)の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機構の情報システムにおいて利用される通信回線を総称し

たものをいう。通信回線には、機構が直接管理していないものも含まれ、その種類(有線又は無線、物理回線又は仮想回線等)は問わない。

●「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

●「テレワーク」とは、情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。

●「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

【は】

●「不正プログラム」とは、コンピュータウイルス、ワーム(他のプログラムに寄生せず単体で自己増殖するプログラム)、スパイウェア(プログラムの使用者の意図に反して様々な情報を収集するプログラム)等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

【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する措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

●「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

●「要管理対策区域」とは、機構の管理下にある区域(機構が外部の組織から借用している施設等における区域を含む。)であって、取り扱う情報を保護するために、

施設及び執務環境に係る対策が必要な区域をいう。

第2部　情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1　組織・体制の整備

(1)　最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置

(a)機構における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者を１人置くこととし、総務担当理事をもって充てる。

(b)最高情報セキュリティ責任者を助けて機構における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機構のセキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置く。

(2)　情報セキュリティ委員会の設置

(a)最高情報セキュリティ責任者は、ポリシー等の審議を行う機能を持つ組織として、機構の情報セキュリティ対策推進体制及びその他業務を実施する部等の代表者を構成員とする情報セキュリティ委員会を置く。情報セキュリティ委員会は、ポリシーの審議を行い、最高情報セキュリティ責任者の承認を得るものとする。

(3)　情報セキュリティ監査責任者の設置

(a)最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこととし、監査室長をもって充てる。

(4)　統括情報セキュリティ責任者、情報セキュリティ責任者等の設置

(a)最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこととし、本部部長及び各施設所長を、青少年教育研究センターにあっては研究センター長をもって充てる。

　そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する者として、統括情報セキュリティ責任者１人を置くこととし、総務企画部長をもって充てる。

(b)情報セキュリティ責任者は、3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者１人を置く。

(c)情報セキュリティ責任者は、本部課室及び施設ごとに情報セキュリティ対策に関する事務を統括する課室等情報セキュリティ責任者 1 人を置くこととし、本部課

長及び各施設次長を、青少年教育研究センターにあっては副センター長を、本部にあって室を設置している場合は室長をもって充てる。ただし、本部に参事及び主幹を置いている場合は、参事及び主幹もこれに充てる。

(d)情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、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企画に着手するまでに置くこととし、情報システムを所管する本部課長及び各施設次長をもって充てる。

(e)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とし、情報システムを所管する本部課及び各施設の課長補佐又は係長をもって充てる。

(5)　最高情報セキュリティアドバイザーの設置

(a)最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定める。

(6)　情報セキュリティ対策推進体制の整備

(a)最高情報セキュリティ責任者は、機構の情報セキュリティ対策推進体制を整備し、その役割を規定する。

(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推進体制の責任者を定める。

(7)　情報セキュリティインシデントに備えた体制の整備

(a)最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化する。

(b)最高情報セキュリティ責任者は、職員等のうちから CSIRT に属する職員等として専門的な知識又は適性を有すると認められる者を選任する。そのうち、機構における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置く。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定める。

(c)最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

(8)　兼務を禁止する役割

(a)職員等は、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とする。

（ア）承認又は許可(以下本項において「承認等」という。)の申請者と当該承認等を行う者(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

(b)職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ることとする。

2.1.2 情報セキュリティポリシー・情報セキュリティ対策推進計画の策定

(1) 情報セキュリティポリシーの策定

(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における審議を経て、統一基準に準拠した情報セキュリティポリシーを定めること。また、情報セキュリティポリシーは、機構の業務、取り扱う情報及び保有するシステムに関するリスク評価の結果を踏まえた上で定める。

(2) 情報セキュリティ対策推進計画の策定

(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における審議を経て、情報セキュリティ対策を総合的に推進するための計画(以下「対策推進計画」という。)を定める。また、対策推進計画には、機構の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めるものとする。

(ア) 情報セキュリティに関する教育
(イ) 情報セキュリティ対策の自己点検
(ウ) 情報セキュリティ監査
(エ) 情報システムに関する技術的な対策を推進するための取組
(オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.2 運用

2.2.1 情報セキュリティ関係規程の運用

(1) 情報セキュリティ対策の運用

(a)統括情報セキュリティ責任者は、機構における情報セキュリティ対策に関する実施手順を整備(本統一基準で整備すべき者を別に定める場合を除く。)し、実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告する。

(b)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、終了及び人事異動時等に関する管理の規定を整備する。

(c)情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該

体制の役割に応じて必要な事務を遂行する。

(d)情報セキュリティ責任者又は課室情報セキュリティ責任者は、職員等より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告する。

(e)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係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告する。

(2) 違反への対処

(a)職員等は、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は、情報セキュリティ責任者にその旨を報告する。

(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とともに、統括情報セキュリティ責任者を通じて、違反者の任命権者及び最高情報セキュリティ責任者に報告する。

2.2.2 例外措置

(1) 例外措置手続の整備

(a)最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者(以下「許可権限者」という。)及び、審査手続を定める。

(b)統括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、許可権限者に対して、定期的に申請状況の報告を求める。

(2) 例外措置の運用

(a)職員等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請する。ただし、業務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、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、事後速やかに届け出る。

職員等は、申請の際に以下の事項を含む項目を明確にする。

(ア)申請者の情報(氏名、所属、連絡先)

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

(ウ)例外措置の適用を申請する期間

(エ)例外措置の適用を申請する措置内容(講じる代替手段等)

(オ)例外措置の適用を終了したときの報告方法

(カ)例外措置の適用を申請する理由

(b)許可権限者は、職員等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。

(c)許可権限者は、以下の項目を含む例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者に報告する。

(ア)決定を審査した者の情報(氏名、役職名、所属、連絡先)

(イ)申請内容

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

(ウ)審査結果の内容

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

(d)統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

2.2.3 教育

(1) 教育体制の整備・教育実施計画の策定

(a)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係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

(b)統括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職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直す。

(2) 教育の実施

(a)課室等情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を適切に受講させる。

(b)職員等は、教育実施計画に従って、適切な時期に教育を受講するものとする。

(c)課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及びCSIRT に属する職員等に教育を適切に受講させるものとする。

(d)課室情報セキュリティ責任者は、教育の実施状況を記録し、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。

(e)統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告する。

2.2.4 情報セキュリティインシデントへの対処

(1) 情報セキュリティインシデントに備えた事前準備

(a)統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機構関係者への報告手順を整備し、報告が必要な具体例を含め、職員等に周知する。

(b)統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の機構外との情報共有を含む対処手順を整備する。

(c)統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業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。

(d)統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備する。

(e)統括情報セキュリティ責任者は、情報セキュリティインシデントについて機構外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機構外の者に明示する。

(f)統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認する。

(2) 情報セキュリティインシデントへの対処

(a)職員等は、情報セキュリティインシデントの可能性を認知した場合には、機構の報告窓口に報告し、指示に従うものとする。

(b)CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

(c)CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告する。

(d)CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧

告を行う。

(e)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情報セキュリティインシデントを認知した場合には、機構で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処する。

(f)情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処する。

(g)CSIRT は、機構の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、文部科学省に連絡する。

(h)CSIRT は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行う。

(i)CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行う。

(j)CSIRT は、情報セキュリティインシデントに関する対処の内容を記録する。

(k)CSIRT は、情報セキュリティインシデントに関して、機構を含む関係機関と情報共有を行う。

(l)CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行う。

(3) 情報セキュリティインシデントの再発防止・教訓の共有

(a)情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それ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。

(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情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示する。

(c)CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有する。

2.3 点検

2.3.1 情報セキュリティ対策の自己点検

(1) 自己点検計画の策定・手順の準備

(a)統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定

する。

(b)情報セキュリティ責任者は、年度自己点検計画に基づき、職員等ごとの自己点検票及び自己点検の実施手順を整備する。

(c)統括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、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直す。

(2) 自己点検の実施

(a)情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示する。

(b)職員等は、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。

(3) 自己点検結果の評価・改善

(a)情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を統括情報セキュリティ責任者に報告する。

(b)統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を最高情報セキュリティ責任者に報告する。

(c)最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受ける。

2.3.2 情報セキュリティ監査

(1) 監査実施計画の策定

(a)情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定める。

(b)情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定める。

(2) 監査の実施

(a)情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告する。

（ア）ポリシーに統一基準を満たすための適切な事項が定められていること
（イ）実施手順がポリシーに準拠していること
（ウ）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

(3) 監査結果に応じた対処

(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示する。

(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からの改善の指示のうち、機関等で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。

(c) 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からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

(1) 情報セキュリティ関係規程の見直し

(a) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、ポリシーについて必要な見直しを行う。

(b) 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。

(2) 情報セキュリティ対策推進計画の見直し

(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及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行う。

第3部 情報の取扱い

3.1 情報の取扱い

3.1.1 情報の取扱い

(1) 情報の取扱いに係る規定の整備

(a)統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、職員等へ周知する。

（ア） 情報の格付及び取扱制限についての定義

（イ） 情報の格付及び取扱制限の明示等についての手続

（ウ） 情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報の目的外での利用等の禁止

(a)職員等は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等すること。

(3) 情報の格付及び取扱制限の決定・明示等

(a)職員等は、情報の作成時及び機構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し、明示等するものとする。

(b)職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び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ものとする。

(c)職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者(決定を引き継いだ者を含む。)又は決定者の上司(以下この項において「決定者等」という。)に確認し、その結果に基づき見直すものとする。

(4) 情報の利用・保存

(a)職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱う。

(b)職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、課室等情報セキュリティ責任者の許可を得ることとする。

(c)職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずる。

(d)職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理する。なお、職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずる。

（ア） 機器等に保存する場合は、インターネットやインターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用する

（イ） 当該情報に対し、暗号化による保護を行う

（ウ） 当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずる

(e)職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従う。

(5) 情報の提供・公表

(a)職員等は、情報を公表する場合には、当該情報が機密性 1 情報に格付けされるものであることを確認する。

(b)職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従う。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずる。

(c)職員等は、機密性３情報を閲覧制限の範囲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。

(c)職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録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。

(6) 情報の運搬・送信

(a)職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、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。職員等が、機密性３情報を要管理隊せく区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

(b)職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、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。職員等が、機密性３情報を機構外通信回線（インターネットを除く）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信する。

(7) 情報の消去

(a)職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速や

かに情報を消去する。

(b)職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消する。

(c)職員等は、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。

(8) 情報のバックアップ

(a)職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施する。

(b)職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理する。

(c)職員等は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄する。

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

(1) 要管理対策区域における対策の基準の決定

(a)統括情報セキュリティ責任者は、要管理対策区域の範囲を定める。

(b)統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定める。

（ア）許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

（イ） 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。

(2) 区域ごとの対策の決定

(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た対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定める。

(b)区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。

(3) 要管理対策区域における対策の実施

(a)区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施する。職員等が実施すべき対策については、職員等が認識できる措置を講ずる。

(b)区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずる。

(c)職員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従

って利用する。また、職員等が機構外の者を立ち入らせる際には、当該機構外の者にも当該区域で定められた対策に従って利用させる。

第4部 外部委託

4.1 業務委託

4.1.1 業務委託

(1) 業務委託に係る規定の整備

(a)統括情報セキュリティ責任者は、業務委託に係る以下の内容を含む規定を整備する。

（ア） 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下「委託判断基準」という。）

（イ）委託先の選定手続き、選定基準及び委託先が具備すべき要件（委託先職員に対する情報セキュリティ対策の実施を含む。）

(2) 業務委託に係る契約

(a)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って業務委託を実施する。

(b)情報セキュリティ責任者又は課室情報セキュリティ責任者は、業務委託を実施する際には、選定基準及び選定手続に従って委託先を選定する。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含める。

（ア）委託先に提供する情報の委託先における目的外利用の禁止

（イ）委託先における情報セキュリティ対策の実施内容及び管理体制

（ウ）委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先、又はその他の者によって、機構の意図せざる変更が加えられないための管理体制

（エ）委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

(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、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含める。

（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

(d)情報システムセキュリティ責任者又は課室等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よう、上記(b)(c)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し、機構の承認を受けるよう、仕様内容に含める。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断する。

(3) 業務委託における対策の実施

(a)情報システムセキュリティ責任者又は課室等情報セキュリティ責任者は、契約に基づき、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。

(b)情報システムセキュリティ責任者又は課室等情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせる。

(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、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認する。

(4) 業務委託における情報の取扱い

(a)職員等は、委託先への情報の提供等において、以下の事項を遵守する。

（ア）委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供する。

（イ）提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させる。

（ウ）委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室等情報セキュリティ責任者に報告する。

4.2 外部サービスの利用

4.2.1 要機密情報を取り扱う場合

(1) 外部サービスの利用に係る規程の整備

(a) 統括情報セキュリティ責任者は、以下を含む外部サービス（要機密情報を取り扱う場合）の利用に関する規定を整備すること。

（ア） 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 4.2 節において「外部サービス利用判断基準」という。）
（イ）外部サービス提供者の選定基準
（ウ）外部サービスの利用申請の許可権限者と利用手続
（エ）外部サービス管理者の指名と外部サービスの利用状況の管理

(2) 外部サービスの選定（クラウドサービスの場合）

(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、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

(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、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、業務に特有のリスクが存在する場合には、必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びに外部サービスとの情報セキュリティに関する役割及び責任の範囲を踏まえてセキュリティ要件を定め、外部サービスを選定すること。

(3) 外部サービスの選定（クラウドサービス以外の場合）

(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、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

(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、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

（ア） 外部サービスの利用を通じて機関等が取り扱う情報の外部サービス提供者における目的外利用の禁止
（イ） 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ）外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制

（エ）外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

(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、外部サービスの利用を通じて機関等が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（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

(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、外部サービスの利用を通じて機関等が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて機関等の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

(f) 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、外部サービス提供者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よう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

(g) 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、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

(h) 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、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

(i) 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、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

(4) 外部サービスの利用に係る調達・契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

(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、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

(5) 外部サービスの利用承認

(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、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

(b) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

(c) 利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

(6) 外部サービスを利用した情報システムの導入・構築時の対策

(a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止

(b) 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

(7) 外部サービスを利用した情報システムの運用・保守時の対策

(a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

（ア）外部サービス利用方針の規定

（イ）外部サービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）外部サービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）外部サービスを利用した情報システムの事業継続

(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、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

(c) 外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

(8) 外部サービスを利用した情報システムの更改・廃棄時の対策

(a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

（ア）外部サービスの利用終了時における対策
（イ）外部サービスで取り扱った情報の廃棄
（ウ）外部サービスの利用のために作成したアカウントの廃棄

(b) 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

4.2.2 要機密情報を取り扱わない場合

(1) 外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備すること。

（ア）外部サービスを利用可能な業務の範囲
（イ）外部サービスの利用申請の許可権限者と利用手続
（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理
（エ）外部サービスの利用の運用手順

(2) 外部サービスの利用における対策の実施

(a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で要機密情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、

当該外部サービスの利用において適切な措置を講ずること。

(b) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

第5部 情報システムのライフサイクル

5.1 情報システムに係る文書等の整備

5.1.1 情報システムに係る台帳等の整備

(1) 情報システム台帳の整備

(a)統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備する。

(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、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告する。

(2) 情報システム関連文書の整備

(a)情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備する。

（ア） 情報システムを構成するサーバ装置及び端末関連情報

（イ） 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情報

（ウ） 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

（エ） 情報セキュリティインシデントを認知した際の対処手順

5.1.2 機器等の調達に係る規定の整備

(1) 機器等の調達に係る規定の整備

(a)統括情報セキュリティ責任者は、機器等の選定基準を整備する。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機構が確認できることを加える。

(b)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・検査手続きを整備する。

5.2 情報システムのライフサイクルの各段階における対策

5.2.1 情報システムの企画・要件定義

(1) 実施体制の確保

(a)情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわた

って情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求める。

(b)情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機構が定める運用管理規程等に応じた体制の確保を、最高情報セキュリティ責任者に求める。

(c)最高情報セキュリティ責任者は前二項で求められる体制の確保に際し、情報システムを統括する責任者の協力を得ることが必要な場合は、当該システムを統括する責任者に当該体制の全部または一部の整備を求める。

(2)　情報システムのセキュリティ要件の策定

(a)情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム(クラウドサービスを含む。)から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定する。

（ア）情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

（イ）情報システム運用時の監視等の運用管理機能要件(監視するデータが暗号化されている場合は、必要に応じて復号すること)

（ウ）情報システムに関連する脆弱性についての対策要件

(b)情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定する。

(c)情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定する。

(d)情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定する。

(3)　情報システムの構築を業務委託する場合の対策

(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を業務委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させる。

（ア）　情報システムのセキュリティ要件の適切な実装

（イ）　情報セキュリティの観点に基づく試験の実施

（ウ）　情報システムの開発環境及び開発工程における情報セキュリティ対策

(4)　情報システムの運用・保守を業務委託する場合の対策

(a)情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させる。

(b)情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させる。

5.2.2　情報システムの調達・構築

(1)　機器等の選定時の対策

(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選定における判断の一要素として活用する。

(2)　情報システムの構築時の対策

(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において、情報セキュリティの観点から必要な措置を講ずる。

(b)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保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。

(3)　納品検査時の対策

(a)情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認する。

(b)情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階に移行する際に、当該情報システムの開発事業者から運用保守業者へ引継がれる

項目に、情報セキュリティ対策に必要な内容が含まれていることを確認する。

5.2.3　情報システムの運用・保守

(1)　情報システムの運用・保守時の対策

(a)情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用する。

(b)情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する機構との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用する。

(c)情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理する。

5.2.4　情報システムの更改・廃棄

(1)　情報システムの更改・廃棄時の対策

(a)情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずる。

（ア）　情報システム更改時の情報の移行作業における情報セキュリティ対策

（イ）　情報システム廃棄時の不要な情報の抹消

5.2.5　情報システムについての対策の見直し

(1)　情報システムについての対策の見直し

(a)情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。

5.3 情報システムの運用継続計画

5.3.1　情報システムの運用継続計画の整備・整合的運用の確保

(1)　情報システムの運用継続計画の整備・整合的運用の確保

(a)統括情報セキュリティ責任者は、機構において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は、非常時における情報セキュリティに係る対策事項を検討する。

(b)統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持

改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認する。

第6部 情報システムのセキュリティ要件

6.1 情報システムのセキュリティ機能

6.1.1 主体認証機能

(1) 主体認証機能の導入

(a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。

(b) 情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。

(c) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずる。

(2) 識別コード及び主体認証情報の管理

(a) 情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずる。

(b) 情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずる。

6.1.2 アクセス制御機能

(1) アクセス制御機能の導入

(a) 情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設ける。

(b) 情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。

6.1.3 権限の管理

(1) 権限の管理

(a) 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適

切に設定するよう、措置を講ずる。

(b)情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずる。

6.1.4 ログの取得・管理

(1) ログの取得・管理

(a)情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

(b)情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理する。

(c)情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

6.1.5 暗号・電子署名

(1) 暗号化機能・電子署名機能の導入

(a)情報システムセキュリティ責任者は、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、以下の措置を講ずる。

（ア）要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

（イ）要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

(b)情報システムセキュリティ責任者は、 暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定める。

（ア） 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗

号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させる。

（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、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用する。

（ウ） 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定める。

（エ）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、管理手順を定める。

(c)情報システムセキュリティ責任者は、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、かつ適用可能な公的な公開鍵基盤が存在する場合は、それを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定める。

(2) 暗号化・電子署名に係る管理

(a)情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずる。

（ア）電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供する。

（イ） 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図る。

6.2 情報セキュリティの脅威への対策

6.2.1 ソフトウェアに関する脆弱性対策

(1) ソフトウェアに関する脆弱性対策の実施

(a)情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施する。

(b)情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施する。

(c)情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性情報を定期的に確認する。

(d)情報システムセキュリティ責任者は脆弱性対策の状況の定期的な確認により脆弱性対策が講じられていない状況が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずる。

6.2.2 不正プログラム対策

(1) 不正プログラム対策の実施

(a)情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

(b)情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずる。

(c)情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行う。

6.2.3 サービス不能攻撃対策

(1) サービス不能攻撃対策の実施

(a)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム(インターネットからアクセスを受ける情報システムに限る。以下この項において同じ。)については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。

(b)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築する。

(c)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視する。

6.2.4 標的型攻撃対策

(1) 標的型攻撃対策の実施

(a)情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策(入口対策)を講ずる。

(b)情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻

撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策及び出口対策)を講ずる。

6.3 アプリケーション・コンテンツの作成・提供

6.3.1 アプリケーション・コンテンツの作成時の対策

(1) アプリケーション・コンテンツの作成に係る規定の整備

(a)統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機構外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備する。

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a)情報システムセキュリティ責任者は、機構外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含める。

(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと

(イ) 提供するアプリケーションが脆弱性を含まないこと

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと

(エ) 電子証明書を用いた署名等と、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること

(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること

(カ) サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

(b)職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項各号に掲げる内容を調達仕様に含める。

6.3.2 アプリケーション・コンテンツ提供時の対策

(1) 政府ドメイン名の使用

(a)情報システムセキュリティ責任者は、機構外向けに提供するウェブサイト等が実際の機構提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用する。ただし、次に掲げる場合を除く。

（ア） 指定法人が政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することができないドメイン名を使用する。

（イ） 教育機関である法人が、高等教育機関向けのドメインを使用する場合。この場合において、当該法人は、あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断する。

（ウ）4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合

(b)職員等は、機構外向けに提供するウェブサイト等の作成を業務委託する場合においては、前項各号列記以外の部分、同項（ア）及び（イ）の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含める。

(2) 不正なウェブサイトへの誘導防止

(a)情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機構のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずる。

(3) アプリケーション・コンテンツの告知

(a)職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずる。

(b)職員等は、機構外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つ。

第7部 情報システムの構成要素

7.1 端末・サーバ装置等

7.1.1 端末

(1) 端末の導入時の対策

(a)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端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。

(b) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

(2)　端末の運用時の対策

(a)情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

(b)情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図る。

(3)　端末の運用終了時の対策

(a)情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消する。

(4)　機構が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策

(a)統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。

(b) 統括情報セキュリティ責任者は、要機密情報を取り扱う機構が支給する端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する規定を整備すること。

(c) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

(d) 情報システムセキュリティ責任者は、職員等が機構が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、当該端末について本条(b)の技術的な措置を講ずること。

(5)　機構支給以外の端末の導入及び利用時の対策

(a) 最高情報セキュリティ責任者は、機構支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機構が講じる安全管理措置、当該端末の管理は機構ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機構における機構支給以外の端末の利用の可否を判断すること。

(b) 統括情報セキュリティ責任者は、職員等が機構支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続を定めること。

(c) 統括情報セキュリティ責任者は、職員等が機構支給以外の端末を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。

(d) 統括情報セキュリティ責任者は、要機密情報を取り扱う機構支給以外の端末について、以下の安全管理措置に関する規定を整備すること。

（ア） 盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置

（イ） 不正プログラムの感染等により情報窃取されることを防止するための利用時の措置

(e) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機構支給以外の端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

(f) 情報セキュリティ責任者は、機構支給以外の端末を用いた機構の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定めること。

(g) 端末管理責任者は、職員等が機構支給以外の端末を用いて要機密情報を取り扱う場合は、当該端末について本条(d)(ア)の安全管理措置を講ずること。

(h) 端末管理責任者は、要機密情報を取り扱う機構支給以外の端末について、前項の規定にかかわらず本条(d)(ア)に定める安全管理措置のうち自ら講ずることができないもの、及び本条(d)(イ)に定める安全管理措置を職員等に講じさせること。

(i) 職員等は、要機密情報を取り扱う機構支給以外の端末について、前項において本条(d)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び本条(d)(イ)に定める安全管理措置を講ずること。

(j) 職員等は、機構支給以外の端末を用いて機構の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。

(k) 職員等は、情報処理の目的を完了した場合は、要保護情報を機構支給以外の端末から消去すること。

7.1.2 サーバ装置

(1) サーバ装置の導入時の対策

(a)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サーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物

理的な脅威から保護するための対策を講ずる。

(b)情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保する。

(c)情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

(d)情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずる。

(2) サーバ装置の運用時の対策

(a)情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

(b)情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。

(c)情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずる。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

(d)情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能となるよう、必要な措置を講ずる。

(3) サーバ装置の運用終了時の対策

(a)情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消する。

7.1.3 複合機・特定用途機器

(1) 複合機

(a)情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定する。

(b)情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対

策を講ずる。

(c)情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消する。

(2) IoT 機器を含む特定用途機器

(a)情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずる。

7.2 電子メール・ウェブ等

7.2.1 電子メール

(1) 電子メールの導入時の対策

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

(b)情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備える。

(c)情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずる。

(d)情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講じる。

7.2.2 ウェブ

(1) ウェブサーバの導入・運用時の対策

(a)情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずる。

（ア）ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること

（イ）ウェブコンテンツの編集作業を担当する主体を限定すること

（ウ） 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること

（エ）ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること

(オ)インターネットを介して転送される情報の盗聴及び改ざん防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じる。

(b)情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。

(2)　ウェブアプリケーションの開発時・運用時の対策

(a)情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずる。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行う。

7.2.3　ドメインネームシステム(DNS)

(1)　DNS の導入時の対策

(a)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずる。

(b)情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずる。

(c)情報システムセキュリティ責任者は、コンテンツサーバにおいて、機構のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずる。

(2)　DNS の運用時の対策

(a)情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持する。

(b)情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認する。

(c)情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずる。

7.2.4　データベース

(1)　データベースの導入・運用時の対策

(a)情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。

(b)情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずる。

(c)情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずる。

(d)情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講

ずる。

(e)情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をする。

7.3 通信回線

7.3.1 通信回線

(1) 通信回線の導入時の対策

(a)情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。

(b)情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。

(c)情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずる。

(d)情報システムセキュリティ責任者は、職員等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずる。機構内通信回線へ機構支給以外の端末を接続する際も同様とする。

(e)情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置する。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。

(f)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずる。

(g)情報システムセキュリティ責任者は、機構内通信回線にインターネット回線、公衆通信回線等の機構外通信回線を接続する場合には、機構内通信回線及び機構内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。

(h)情報システムセキュリティ責任者は、機構内通信回線と機構外通信回線との間で送受信される通信内容を監視するための措置を講ずる。

(i)情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備する。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

(j)情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保する。

(k)情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておく。

(2) 通信回線の運用時の対策

(a)情報システムセキュリティ責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずる。

(b)情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の 見直しを行う。

(c)情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図る。

(d)情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更する。

(3) 通信回線の運用終了時の対策

(a)情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずる。

(4) 無線 LAN 環境導入時の対策

(a)情報システムセキュリティ責任者は、無線 LAN 技術を利用して機構内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる。

7.3.2IPv6 通信回線

(1) IPv6 通信を行う情報システムに係る対策

(a)情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択する。

(b)情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずる。

（ア）グローバル IP アドレスによる直接の到達性における脅威

（イ）IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

（ウ）IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

（エ）アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

(2) 意図しない IPv6 通信の抑止・監視

(a)情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずる。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

(1) 情報システムの利用に係る規定の整備

(a)統括情報セキュリティ責任者は、機構の情報システムの利用のうち、情報セキュリティに関する規定を整備する。

(b)統括情報セキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定める。当該手順には以下の事項を含めること。

（ア）職員等は機構が支給する外部電磁的記憶媒体、又は本項に規定する利用手順において定められた外部電磁的記憶媒体を用いた情報の取扱いの遵守を契約により機構との間で取り決めた機構外の組織から受け取った外部電磁的記憶媒体を使用する

（イ）自組織以外の組織から受け取った外部電磁的記憶媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記憶媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講じる

(c)統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記憶媒体を要管理対策区域外に持ち出す際の許可手続きを定める。

(2)　情報システム利用者の規定の遵守を支援するための対策

(a)情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築する。

(3)　情報システムの利用時の基本的対策

(a)職員等は、業務の遂行以外の目的で情報システムを利用しない。

(b)職員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機構の情報システムを接続しない。

(c)職員等は、機構内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しない。

(d)職員等は、情報システムで利用を禁止するソフトウェアを利用しない。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得る。

(e)職員等は、接続が許可されていない機器等を情報システムに接続しない。

(f)職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずる。

(g)職員等は、機構が支給する端末（要管理対策区域外で使用する場合に限る）及び機構支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従う。

(h)　職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

（ア）　機構が支給する端末（要管理対策区域外で使用する場合に限る）　機密性３情報、要保全情報又は要安定情報

（イ）　機構支給以外の端末　要保護情報

(i)　職員等は、要管理対策区域外において機構外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機構内通信回線に接続する場合には、定められた安全管理措置を講ずる

(j)職員等は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得る。

(k)職員等は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等

の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、課室情報セキュリティ責任者の許可を得る。

(4)　電子メール・ウェブの利用時の対策

(a)職員等は、要機密情報を含む電子メールを送受信する場合には、それぞれの機構が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用する。

(b)職員等は、機構外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用する。ただし、当該機構外の者にとって、当該職員等が既知の者である場合、電子メールを受信する機構等外の者が、職員等から送信された電子メールであることを認知できる場合は除く。

(c)職員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する。

(d)職員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わない。

(e)職員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認する。

(f)職員等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認する。

（ア）　送信内容が暗号化されること

（イ）　当該ウェブサイトが送信先として想定している組織のものであること

(5)　識別コード・主体認証情報の取扱い

(a)職員等は、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。

(b)職員等は、自己に付与された識別コードを適切に管理する。

(c)職員等は、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。

(d)職員等は、自己の主体認証情報の管理を徹底する。

(6)　暗号・電子署名の利用時の対策

(a)職員等は、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。

(b)職員等は、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。

(c)職員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

(7) 不正プログラム感染防止

(a)職員等は、不正プログラム感染防止に関する措置に努める。

(b)職員等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断するなど、必要な措置を講ずる。

(8) Web 会議サービスの利用時の対策

(a)職員等は、機構の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

(b)職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

8.1.2 ソーシャルメディアサービスによる情報発信

(1) ソーシャルメディアサービスによる情報発信時の対策

(a)統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

（ア） 機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

（イ） パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

(b)職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

8.2.1 テレワーク

(1) 実施規定の整備

(a)統括情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策に係る規定を整備すること。なお、原則としてテレワークは機関等が支給する端末で行

うよう定めること。

(2)　実施環境における対策

(a)情報システムセキュリティ責任者は、テレワークの実施により機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対するセキュリティを確保すること。

(b) 情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行うこと。

(c) 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じること。

(d)情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。

(3)　実施時における対策

(a)情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等がチェックするべき項目を定め、職員等に当該チェックを実施させること。

(b)職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。

職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。

雑則

このポリシーに定めるもののほか、必要な事項は、CISO が定める。

附則

このポリシーは、令和４年３月３０日から施行する。附則