○サイバーセキュリティ対策実施細則

（平成29年4月3日細則(情)第11号）

改正　令和2年1月31日細則(情)第1号　令和3年3月31日細則(総)第9号
令和4年3月31日細則(情)第1号　令和5年3月31日細則(情)第6号
令和6年3月13日細則(情)第5号　令和6年7月31日規程(総)第17号
令和6年8月9日細則(情)第16号　令和7年2月27日細則(情)第1号

目次

第1編　総則

第1章　目的・定義・適用範囲

(目的)

第1条　本細則は、独立行政法人国際協力機構サイバーセキュリティ対策に関する規程(平成29年規程(情)第14号。以下「規程」という。)第23条の規定に基づき、独立行政法人国際協力機構(以下「機構」という。)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に係る対策基準を定めることを目的とする。

(適用範囲)

第2条　本細則の適用対象とする者は、規程第3条第1項に定める役職員等及び情報取扱事務従事者とする。

2　本細則の適用対象とする情報は、以下の各号の情報とする。

(1)　役職員等及び情報取扱事務従事者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当該情報システムに入力された書面に記載された情報を含む。）

(2)　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当該情報システムに入力された書面に記載された情報を含む。）であって、役職員等及び情報取扱事務従事者が職務上取り扱う情報

(3)　前各号に掲げるもののほか、機構が調達し、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

3　前項の適用範囲外の情報についての管理は、独立行政法人国際協力機構法人文書管理規程(平成16年規程(総)第31号。以下「法人文書管理規程」という。)の定めるところによる。

4　本細則の適用対象とする情報システムは、第2項に定める情報を取り扱う全ての情報システムとする。

(用語定義)

第3条　本細則における用語の定義は、次のとおりとする。

(1)　「部等」とは、独立行政法人国際協力機構組織規程(平成16年規程(総)第4号。以下「組織規程」という。)第4条に定める本部の部、室、事務局及び研究所、組織規程第50条に定める国内機関、組織規程第57条に定める在外事務所、組織規程第2条第2項に定める支所及び出張所をいう。

(2)　「課等」とは、組織規程第6条第1項及び第6項に定める本部の課、部内室及びチーム並びに組織規程第53条第1項に定める国内機関の課をいう。

(3)　「機密性」とは、情報に関して、アクセスを認められた者のみが、これにアクセスできる特性をいう。

(4)　「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

(5)　「可用性」とは、情報へのアクセスを認められたものが、必要時に中断することなく、情報にアクセスすることができる特性をいう。

(6)　「アプリケーション・コンテンツ」とは、機構が開発し提供する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。

(7)　「運用規程」とは、規程第2条第3号に規定する運用規程をいう。

(8)　「外部委託」とは、業務委託及びクラウドサービス利用の双方を指す。なお、業務委託に際し、委託先が当該業務遂行を目的としてクラウドサービスを調達・利用する場合、再委託に相当することとなる。

(9)　「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。

(10)　「機構ドメイン名」とは、jica.go.jpで終わるドメイン名のことをいう。

(11)　「機構内通信回線」とは、機構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、機構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。機構内通信回線には、専用線やVPN等物理的な回線を機構が管理していないものも含まれる。

(12)　「機構外通信回線」とは、通信回線のうち、機構内通信回線以外のものをいう。

(13)　「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。

(14)　「業務委託」とは、機構の業務の一部又は全部について、委任、準委任、請負といった契約形態を問わず、契約をもって外部の者に実施させることをいう。ただし、当該業務において機構の情報を取り扱わせる場合に限る。

(15)　「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11年法律第89号）第49条第1項若しくは第2項に規定する機関、国家行政組織法（昭和23年法律第120号）第3条第2項に規定する機関又はこれらに置かれる機関をいう。

(16)　「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（SaaS（Software as a Service）、PaaS（Platform as a Service）及びIaaS（Infrastructure as a Service）を含む。）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。なお、本細則におけるクラウドサービスは、機構外の一般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クラウドサービスであって、当該サービスにおいて機構の情報が取り扱われる場合に限るものとする。

(17)　「クラウドサービス管理者」とは、クラウド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クラウドサービスに係る管理を行う機構の役職員等をいう。

(18)　「クラウドサービス提供者」とは、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。

(19)　「クラウドサービス利用者」とは、クラウドサービスを利用する機構の役職員等及び情報取扱事務従事者又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。

(20)　「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及びマウス等の周辺機器を含む。)であって、原則として、機構が調達し、又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。

(21)　「物理的なサーバ装置」とは、物理的なハードウェアを有するサーバ装置をいう。

(22)　「サイバーセキュリティ戦略本部監査」とは、サイバーセキュリティ基本法第26条第1項第2号に基づきサイバーセキュリティ戦略本部が実施する監査をいう。

(22)の2　「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 Assistant Team（情報セキュリティ緊急支援チーム）の略である。

(23)　「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の略である。

(24)　「実施手順」とは、規程第2条第4号に規定する実施手順をいう。

(25)　「情報」とは、本細則第2条第2項に定めるものをいう。
(26)　「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う。以降、本細則においては、特に断りのない限り、機構が調達し、又は開発するもの（管理を外部委託しているシステムや政府共通利用型システムを含む。）をいう。
(27)　「情報セキュリティインシデント」とは、日本産業規格情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語（JIS Q 27000:2019）における情報セキュリティインシデントをいう。

参考：JIS Q 27000:2019（抄）

・情報セキュリティインシデント（3.31）

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

・情報セキュリティ事象（3.30）

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

(28)　「情報セキュリティ関係規程」とは、規程第2条第5号に規定する情報セキュリティ関係規程をいう。
(29)　「情報セキュリティ対策推進体制」とは、規程第2条第6号に規定する情報セキュリティ対策推進体制をいう。
(30)　「政府共通利用型システム」とは、他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム及び他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムをいう。
(31)　「政府共通利用型システム管理機関」とは、政府共通利用型システムを構築・運用する機関等をいう。
(32)　「政府共通利用型システム利用機関」とは、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する機関等及び政府共通利用型システムが提供する機器等を利用する機関等をいう。
(33)　「対策推進計画」とは、規程第8条第1項に規定する対策推進計画をいう。
(34)　「端末」とは、情報システムの構成要素である機器のうち、役職員等及び情報取扱事務従事者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並びに直接接続され一体として扱われるキーボード及びマウス等の周辺機器を含む。)であって、原則として、機構が調達し、又は開発するもの（その形態を問わず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（以下「モバイル端末」という。）及び政府共通利用型システムが提供するものを含む。）をいう。
(35)　「機構支給以外の端末」とは、情報システムの構成要素である機器のうち、役職員等および情報取扱事務従事者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並びに直接接続され一体として扱われるキーボードおよびマウス等の周辺機器を含む。）であって、機構が調達し、又は開

発するもの以外をいう。
(36)　「物理的な端末」とは、物理的なハードウェアを有する端末をいう。
(37)　「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。
(38)　「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（ハブ、スイッチ、ルータ、ファイアウォール等を含む。）をいう。
(39)　「物理的な通信回線装置」とは、物理的なハードウェアを有する通信回線装置をいう。
(40)　「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、通信回線に接続する機能又は内蔵電磁的記録媒体を備えているものをいう。
(41)　「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。
(42)　「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。
(43)　「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。
(44)　「要管理対策区域」とは、機構の事業所、又は機構外の組織から借用している施設等、機構の管理下にある区域であって、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。

(改正)

第4条　情報セキュリティ水準を適切に維持していくために、情報技術の進歩に応じて、本細則を定期的に点検し、必要に応じ規定内容の追加・修正等の改正を行う。

(法令等の遵守)

第5条　情報及び情報システムの取扱いに関して、関連法令等、規程第2条第1項第2号に定める機構情報セキュリティポリシー(以下「機構ポリシー」という。)及び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を遵守する。

(機構の対策基準)

第6条　本細則で目的別に定める機構が行うべき対策については、「政府機関等のサイバーセキュリティ対策のための統一基準群」(令和5年7月4日決定。以下「統

一基準群」という。)に含まれる統一基準及び「政府機関等の対策基準策定のためのガイドライン」（以下「ガイドライン」という。）に例示される対策又はこれと同等以上の対策を講ずることとする。第12条第2項に定める統括情報セキュリティ責任者は、各対策において実施すべき基本的な対策事項（以下「基本対策事項」という。）を含む運用規程及び実施手順を別に定める。

第2章　情報の格付の区分・取扱制限

(情報の格付の区分)

第7条　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、本細則で用いる格付の区分を用いる。

2　格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本細則で定めるセキュリティ水準と同等以上の水準で取り扱われるようにするものとする。

3　他機関等へ情報を提供するときは、機構の対策基準における格付区分と本統一基準における格付区分の対応について適切に伝達するため、本条に定める格付及び取扱制限を明示する。

4　機密性についての格付の定義は以下のとおりとする。

(1)　機密性3情報とは、機構における業務で取り扱う情報のうち、法人文書管理規程第2条第10号に定める極秘区分に該当する情報かつ他の機関等から提供された「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。）」に定める秘密文書としての取り扱いを要する情報とする。

(2)　機密性2情報とは、機構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「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であって、「機密性3情報」以外の情報とする。

(3)　機密性1情報とは、機構における業務で取り扱う情報のうち、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とする。

(4)　機密性2情報及び機密性3情報を「要機密情報」という。

5　完全性についての格付の定義は、以下のとおりとする。

(1)　完全性2情報とは、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とする。

(2)　完全性1情報とは、完全性2情報以外の情報（書面を除く。）とする。

(3)　完全性2情報を「要保全情報」という。

6　可用性についての格付の定義は、以下のとおりとする。

(1)　可用性2情報とは、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とする。

(2)　可用性1情報とは、可用性2情報以外の情報（書面を除く。）とする。

(3)　可用性2情報を「要安定情報」という。

7　要機密情報、要保全情報又は要安定情報に一つでも該当する情報は、「要保護

情報」という。

（情報の取扱制限）

第8条　「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役職員等及び情報取扱事務従事者に確実に行わせるための手段をいう。

2　役職員等及び情報取扱事務従事者は、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。

3　取扱制限に関する基本的な定義は、取り扱う情報に応じて、機密性、完全性及び可用性の3つの観点から、第12条第2項に定める統括情報セキュリティ責任者が別に定める。

第2編　情報セキュリティ対策の基本的枠組み

第1章　導入・計画

第1節　組織・体制の整備

（最高情報セキュリティ責任者の統括業務）

第9条　最高情報セキュリティ責任者は、次に掲げる業務を統括する。

(1)　情報セキュリティ対策推進のための組織・体制の整備

(2)　機構ポリシーの決定、見直し

(3)　対策推進計画の決定、見直し

(4)　情報セキュリティインシデントに対処するために必要な指示その他の措置

(5)　情報セキュリティ監査の結果を踏まえた改善計画の策定等の必要な措置の指示

(6)　前各号に掲げるもののほか、情報セキュリティに関する重要事項

2　最高情報セキュリティ責任者は、必要に応じて、最高情報セキュリティ副責任者1人を選任する。最高情報セキュリティ副責任者は、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 機構の情報セキュリティに関する事務を統括する。

（情報セキュリティ委員会）

第10条　最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、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。

2　情報セキュリティ委員会の委員長、副委員長及び委員は、最高情報セキュリティ責任者が情報セキュリティを推進する役職員等又は各部の代表者から指名する。

3　委員の構成は、次のとおりとし、必要に応じ、他の役職員等又は第三者の専門家を出席させることができる。

(1)　委員長　情報システム部（情報セキュリティ及び個人情報保護）担当理事

(2)　副委員長　情報システム部長

(3)　委員　総務部長、人事部長、財務部長、企画部長、国内事業部長、国際協力調達部長、青年海外協力隊事務局長

4　情報セキュリティ委員会は、次に掲げる事項を審議する。

(1)　機構ポリシー

(2)　対策推進計画
(3)　前各号に掲げるもののほか、情報セキュリティに関し必要な事項
5　情報セキュリティ委員会は、事務局を情報システム部計画課に置き、計画課長を事務局長とする。
(情報セキュリティ監査責任者の設置)
第11条　機構は、情報セキュリティ監査に関する業務を統括する情報セキュリティ監査責任者を置き、監査室長をもって充てる。
(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)
第12条　最高情報セキュリティ責任者は、部等における情報セキュリティ対策に関する業務を統括する者として、情報セキュリティ責任者１人を置き、部等の長をもって充てる。ただし、研究所においては副所長をもって充てる。
2　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を統括情報セキュリティ責任者とし、情報システム部長をもって充てる。
3　情報セキュリティ責任者は、第51条第1項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業務を統括する区域情報セキュリティ責任者１人を置く。
4　情報セキュリティ責任者は、課等ごとに情報セキュリティ対策に関する業務を統括する課等情報セキュリティ責任者１人を置く。
5　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業務の責任者として、情報システムセキュリティ責任者を兼ねる。
(最高情報セキュリティアドバイザーの設置)
第13条　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く。
2　最高情報セキュリティアドバイザーの業務内容は、統括情報セキュリティ責任者が最高情報セキュリティ責任者と協議のうえ定める。
(情報セキュリティ対策推進体制の整備)
第14条　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を整備し、以下の各号を含む役割を規定する。
(1)　情報セキュリティ関係規程及び対策推進計画の策定に係る事務
(2)　情報セキュリティ関係規程の運用に係る事務
(3)　例外措置に係る事務
(4)　情報セキュリティ対策の教育の実施に係る事務
(5)　情報セキュリティ対策の自己点検に係る事務
(6)　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務
2　機構は、情報セキュリティ対策推進体制の責任者を置き、情報システム部長をもって充てる。
(情報セキュリティインシデントに備えた体制の整備)
第15条　最高情報セキュリティ責任者は、CSIRTを整備し、その役割を定める。
2　CSIRTは専門的な知識又は適性を有すると認められる者で構成する。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責任者を置き、情報システム部長をもって充てる。また、CSIRT責任者は、CSIRT内の業務統括及び外部との連携等を行う役職員等を定める。

3　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。

（兼務を禁止する役割）

第16条　役職員等及び情報取扱事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しない。

(1)　承認又は許可(以下本条において「承認等」という。)の申請者及び当該承認等を行う許可権限者

(2)　監査を受ける者及びその監査を実施する者

2　役職員等及び情報取扱事務従事者は、承認等を申請する場合において、自らが許可権限者であるときその他許可権限者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、当該許可権限者の上司又は適切な者に承認等を申請し、承認等を得る。

第2節　資産管理

（情報システム台帳の整備）

第17条　統括情報セキュリティ責任者は、原則として、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。

第3節　情報セキュリティ関係規程の整備

（リスク評価の実施）

第18条　最高情報セキュリティ責任者は、機構の目的等を踏まえ、自己点検の結果、情報セキュリティ監査の結果、サイバーセキュリティ戦略本部監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価する。

（本細則の策定）

第19条　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、これと同等以上の情報セキュリティ対策が可能となるように本細則を定める。また、本細則は、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、並びに本細則及び対策推進計画の見直し結果を踏まえた上で定める。

（運用規程及び実施手順の策定）

第20条　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運用規程（本細則で最高情報セキュリティ責任者が整備すると定める場合を除く。）及び実施手順(本細則で整備すべき者を別に定める場合を除く。)を整備し、運用規程及び実施手順に関する業務を統括し、並びに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。

2　統括情報セキュリティ責任者は、役職員等の雇用の開始、雇用の終了若しくは人事異動の際又は情報取扱事務従事者の業務の開始、若しくは終了の際に、情報セキュリティに関して必要となる事務について運用規程を整備する。

（対策推進計画の策定）

第21条　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、対策推進計画を定める。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次に掲げる取組の方針・重点及びその実施時期を全て含める。

(1)　情報セキュリティに関する教育
(2)　情報セキュリティ対策の自己点検
(3)　情報セキュリティ監査及び 過年度の監査結果（サイバーセキュリティ戦略本部監査の結果を含む。）を踏まえた取組
(4)　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
(5)　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　前項第3号の情報セキュリティ監査については、最高情報セキュリティ責任者は予め情報セキュリティ監査責任者の意見を徴する。

第2章　運用

第1節　情報セキュリティ関係規程の運用

（情報セキュリティ対策の運用）

第22条　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。

2　情報セキュリティ責任者又は課等情報セキュリティ責任者は、役職員等及び情報取扱事務従事者から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。

3　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。

（違反への対処）

第23条　役職員等及び情報取扱事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ責任者にその旨を報告する。

2　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、最高情報セキュリティ責任者に報告する。

第2節　例外措置

（例外措置手続の整備）

第24条　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し、許可する者(以下本節において「許可権限者」という。)及び審査手続を定める。

2　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。

（例外措置の運用）

第25条　役職員等及び情報取扱事務従事者は、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、当該規定の趣旨を十分尊重した取扱いを行う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。

2　許可権限者は、役職員等及び情報取扱事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定する。

3　許可権限者は、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。

4　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。

第3節　教育

（教育体制等の整備・教育実施計画の策定）

第26条　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。

2　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役職員等及び情報取扱事務従事者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。

（教育の実施）

第27条　課等情報セキュリティ責任者は、役職員等及び情報取扱事務従事者に対して、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。

2　役職員等及び情報取扱事務従事者は、教育実施計画に従って、適切な時期に教育を受講する。

3　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に属する役職員等に教育を適切に受講させる。

4　課等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。

5　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。

第4節　情報セキュリティインシデントへの対処

（情報セキュリティインシデントに備えた事前準備）

第28条　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が必要な具体例を含む報告手順を整備し、役職員等及び情報取扱事務従事者に周知する。

2　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。

3　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。

4　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。

5　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。

6　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。

（情報セキュリティインシデントへの対処）

第29条　役職員等及び情報取扱事務従事者は、情報セキュリティインシデントの可能性を認知した場合には、機構の報告窓口（情報システム部）に報告し、指示に従う。

2　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。
3　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。
4　CSIRT責任者は、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。また、CSIRT責任者は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該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へ確認を指示する。
5　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、情報システム部長が別途定める対処手順及びCSIRTの指示又は勧告に従って、適切に対処する。
6　政府共通利用型システムを利用している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政府共通利用型システムに関するものである場合には、当該政府共通利用型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に従い、適切に対処する。
7　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警察への通報・連絡等を行う。
8　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、対処全般に関する指示、勧告又は助言を行う。
9　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。
10　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。

（情報セキュリティインシデントに係る情報共有）

第30条　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、外務省に連絡する
2　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。
3　CSIRTは、情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告を行う。

（情報セキュリティインシデントの再発防止・教訓の共有）

第31条　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及び統括情報セキュリティ責任者に報告する。
2　最高情報セキュリティ責任者は、前項の定めに従い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。
3　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関係する情報セキュリティ責任者等に共有する。

第3章　点検

第1節　情報セキュリティ対策の自己点検

（自己点検計画の策定・手順の準備）

第32条　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。
2　情報セキュリティ責任者は、年度自己点検計画に基づき、役職員等及び情報取扱事務従事者ごとの自己点検票及び自己点検の実施手順を整備する。
3　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、役職員等及び情報取扱事務従事者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。
（自己点検の実施）
第33条　情報セキュリティ責任者は、年度自己点検計画に基づき、役職員等及び情報取扱事務従事者に自己点検の実施を指示する。
2　役職員等及び情報取扱事務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。
（自己点検結果の評価・改善）
第34条　情報セキュリティ責任者は、自らが担当する部等に特有の課題の有無を確認するなどの観点から役職員等及び情報取扱事務従事者による自己点検結果を分析し、評価する。また、その評価結果を統括情報セキュリティ責任者に報告する。
2　統括情報セキュリティ責任者は、機構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。
3　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。

第2節　情報セキュリティ監査

（情報セキュリティ監査計画の策定）
第35条　情報セキュリティ監査責任者は、対策推進計画を参酌して監査計画を策定し、理事長の承認を得るものとする。
2　前項の規定にかかわらず、理事長の命により、又は理事長の承認を得て、情報セキュリティ監査責任者は臨時に監査を実施することができる。
（監査の実施）
第36条　監査は、独立行政法人国際協力機構内部監査規程第7条に基づき実施し、結果を理事長に報告する。また、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に監査結果を共有する。
（監査結果に応じた対処）
第37条　最高情報セキュリティ責任者は、監査報告の内容を踏まえ、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。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示する。
2　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、機構内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。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

3　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、自らが担当する部等に特有の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。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

第4章　見直し

第1節　情報セキュリティ対策の見直し

（情報セキュリティ対策の見直し）

第38条　最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、本細則や対策推進計画の必要な見直しを行う。

（情報セキュリティ関係規程等の見直し）

第39条　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、情報セキュリティ監査並びにサイバーセキュリティ戦略本部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、機構ポリシーについて必要な見直しを行う。

2　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、情報セキュリティ監査並びにサイバーセキュリティ戦略本部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運用規程及び実施手順を見直し、又は運用規程及び実施手順を整備した者に対して規定の見直しを指示し、見直した結果について最高情報セキュリティ責任者に報告する。

3　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、情報セキュリティ監査並びにサイバーセキュリティ戦略本部監査等の結果等を踏まえて機構内で横断的に改善が必要となる情報セキュリティ対策の運用に係る見直しについて、機構内の職制及び職務に応じた措置を実施し、又は情報セキュリティ責任者又は情報システムセキュリティ責任者に対してその実施を指示し、措置の結果について最高情報セキュリティ責任者に報告する。

（対策推進計画の見直し）

第40条　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自己点検、情報セキュリティ監査並びにサイバーセキュリティ戦略本部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5章　独立行政法人におけるセキュリティ対策

（機構を所管する行政機関からの助言）

第41条　最高情報セキュリティ責任者は、情報セキュリティ対策を適切に推進するため、所管省庁と密接な連携を要する事項や専門的知見を要する事項について、外務省へ助言を求める。

第3編　情報の取扱い

第1章　情報の取扱い

第1節　情報の取扱い

（情報の取扱いに係る規定の整備）

第42条　統括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、役職員等及び情報取扱事務従事者へ周知する。

(1)　情報の格付及び取扱制限についての定義
(2)　情報の格付及び取扱制限の明示等についての手続
(3)　情報の格付及び取扱制限の継承、見直しに関する手続

(情報の目的外での利用等の禁止)

第43条　役職員等及び情報取扱事務従事者は、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。

(情報の格付及び取扱制限の決定・明示等)

第44条　役職員等及び情報取扱事務従事者は、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。

2　役職員等及び情報取扱事務従事者は、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。

3　役職員等及び情報取扱事務従事者は、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「決定者等」という。)に確認し、その結果に基づき見直す

(情報の利用・保存)

第45条　役職員等及び情報取扱事務従事者は、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。

2　役職員等及び情報取扱事務従事者は、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、情報セキュリティ責任者の許可を得る。

3　役職員等及び情報取扱事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずる。

4　役職員等及び情報取扱事務従事者は、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。役職員等及び情報取扱事務従事者は、機密性3情報を機器等に保存する際、以下の各号の措置を講ずる。ただし、機構において、機密性3情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

(1)　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。
(2)　当該情報に対し、暗号化による保護を行う。
(3)　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。

5　役職員等及び情報取扱事務従事者は、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。

(情報の提供・公表)

第46条　役職員等及び情報取扱事務従事者は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認する。

2　役職員等及び情報取扱事務従事者は、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。
3　役職員等及び情報取扱事務従事者は、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、情報セキュリティ責任者の許可を得る。
4　役職員等及び情報取扱事務従事者は、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。
（情報の運搬・送信）
第47条　役職員等及び情報取扱事務従事者は、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。役職員等及び情報取扱事務従事者が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課等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。ただし、他の機関等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。
2　役職員等及び情報取扱事務従事者は、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。役職員等及び情報取扱事務従事者が、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、課等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。ただし、機構が、機密性3情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。
（情報の消去）
第48条　役職員等及び情報取扱事務従事者は、電磁的記録媒体に保存された情報が業務上不要となった場合は、速やかに情報を消去する。
2　役職員等及び情報取扱事務従事者は、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。
3　役職員等及び情報取扱事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にする。
（情報のバックアップ）
第49条　役職員等及び情報取扱事務従事者は、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。
2　役職員等及び情報取扱事務従事者は、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。
3　役職員等及び情報取扱事務従事者は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄する。

第2章　情報を取り扱う区域の管理

第1節　情報を取り扱う区域の管理

（要管理対策区域における対策の基準の決定）
第50条　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。
2　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

を全て含む対策の基準を運用規程として定める。

(1)　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

(2)　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

(区域ごとの対策の決定)

第51条　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、施設及び環境に係る対策を行う単位ごとの区域を定める。

2　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。

(要管理対策区域における対策の実施)

第52条　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。役職員等及び情報取扱事務従事者が実施すべき対策については、役職員等及び情報取扱事務従事者が認識できる措置を講ずる。

2　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。

3　役職員等及び情報取扱事務従事者は、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。

4　役職員等及び情報取扱事務従事者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編　外部委託

第1章　業務委託

第1節　業務委託

(業務委託に係る運用規程の整備)

第53条　統括情報セキュリティ責任者は、業務委託に係る次の内容を全て含む運用規程を整備する。

(1)　委託先への提供を認める情報及び委託する業務の範囲を判断する基準（以下本節において「委託判断基準」という。）

(2)　委託先の選定基準

(業務委託実施前の対策)

第54条　情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施する。

(1)　委託する業務内容の特定

(2)　委託先の選定条件を含む仕様の策定

(3)　仕様に基づく委託先の選定

(4)　契約の締結

(5)　委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

2　情報セキュリティ責任者は、以下を全て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、その旨を仕様に含める。

(1)　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

(2)　委託先における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制

(3)　情報セキュリティインシデントへの対処方法
(4)　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
(5)　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

3　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。
(1)　情報セキュリティ監査の受入れ
(2)　サービスレベルの保証

4　情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱う。

5　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、本条第2項及び第3項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。

6　情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求める。
(1)　仕様に準拠した提案
(2)　契約の締結
(3)　委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

7　情報セキュリティ責任者は、以下を全て含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること
(1)　当該委託業務に携わる者の特定
(2)　当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

(業務委託実施期間中の対策)

第55条　情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施する。
(1)　委託判断基準に従った要保護情報の提供
(2)　契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認
(3)　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役職員等又は情報取扱事務従事者より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

2　情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求める。
(1)　情報の適正な取扱いのための情報セキュリティ対策
(2)　契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告
(3)　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又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置

を含む対処

(業務委託終了時の対策)

第56条　情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施する。

(1)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(2)　委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

2　情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求める。

(1)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(2)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

第2節　情報システムに関する業務委託

(情報システムに関する業務委託における共通的対策)

第57条　情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに機構の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定する。

2　情報システムセキュリティ責任者は、委託先の選定に際し、以下を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託先の選定条件に加え、その旨を仕様に含める。

(1)　委託先企業若しくはその従業員、再委託先企業若しくはその従業員又はその他の者によって、情報システムに機構の意図せざる変更が加えられないための管理体制

(2)　委託先の資本関係、役員等の情報、委託事業の実施場所並びに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（情報処理安全確保支援士等）及び研修実績等)、実績及び国籍に関する情報提供

(情報システムの構築を業務委託する場合の対策)

第58条　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、契約に基づき、以下を全て含む対策の実施を委託先に求める。

(1)　情報システムのセキュリティ要件の適切な実装

(2)　情報セキュリティの観点に基づく試験の実施

(3)　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

(情報システムの運用・保守を業務委託する場合の対策)

第59条　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、契約に基づき、委託先に実施を求める。

2　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、契約に基づき、委託先に速やかな報告を求める。

(機構向けに情報システムの一部の機能を提供するサービスを利用する場合の対

策）

第60条　情報システムセキュリティ責任者は、機構外の一般の者が機構向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加える。

2　情報システムセキュリティ責任者は、業務委託サービスの中断や終了時に円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを委託先の選定条件に加え、仕様にも含める。

(1)　取り扱う情報の可用性区分の格付に応じた、業務委託サービス中断時の復旧要件

(2)　取り扱う情報の可用性区分の格付に応じた、業務委託サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

3　情報システムセキュリティ責任者は、業務委託サービスの利用を通じて機構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委託先を選定し、必要に応じて機構の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を委託先の選定条件に含め、仕様にも含める。

4　情報システム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、業務委託サービスを選定する。また、業務委託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。

5　情報システム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、業務委託先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。

6　情報システムセキュリティ責任者は業務委託サービスを利用する場合には統括情報セキュリティ責任者へ当該サービスの利用申請を行う。

7　統括情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定する。

8　統括情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名する。

第2章　クラウドサービス

第1節　クラウドサービスの選定（要機密情報を取り扱う場合）

（クラウドサービスの選定に係る運用規程の整備）

第61条　統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程を整備する。

(1)　クラウド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（以下本章において「クラウドサービス利用判断基準」という。）

(2)　クラウドサービス提供者の選定基準

(3)　クラウドサービスの利用申請の許可権限者と利用手続

(4)　クラウドサービス管理者の指名とクラウドサービス利用状況の管理

（クラウドサービスの選定）

第62条　情報システム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、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討する。
2　情報システム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クラウドサービス提供者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、以下を全て含むセキュリティ要件を定める。
(1)　クラウドサービスに求める情報セキュリティ対策
(2)　クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
(3)　クラウドサービスに求めるサービスレベル
3　情報システムセキュリティ責任者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則としてISMAP等クラウドサービスリストからクラウドサービスを選定する。
(クラウドサービスの利用に係る調達)
第63条　情報システムセキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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。
2　情報システムセキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得る。また、調達仕様の内容を契約に含める。
(クラウドサービスの利用承認)
第64条　情報システムセキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行う。
2　利用申請の許可権限者は、前項におけるクラウドサービスの利用申請を審査し、許可の可否を決定する。
3　利用申請の許可権限者は、クラウドサービスの利用申請を許可した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名する。

第2節　クラウドサービスの利用（要機密情報を取り扱う場合）

(クラウドサービスの利用に係る運用規程の整備)
第65条　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備する。
2　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備する。
3　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備する。
(1)　クラウドサービスの利用終了時における対策
(2)　クラウドサービスで取り扱った情報の廃棄
(3)　クラウドサービスの利用のために作成したアカウントの廃棄
(クラウドサービスの利用に係るセキュリティ要件の策定)
第66条　クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づ

き、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認する。

2　クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定する。

（クラウドサービスを利用した情報システムの導入・構築時の対策）

第67条　クラウドサービス管理者は、第65条第1項で定めた運用規程を踏まえて、前条第2項において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずる。また、導入・構築時に実施状況を確認・記録する。

2　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載する。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告する。

3　クラウドサービス管理者は、クラウドサービス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、クラウドサービスの運用開始前までに以下の全ての実施手順を整備する。

(1)　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(2)　クラウドサービスを利用した情報システムの運用・監視中における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

(3)　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

（クラウドサービスを利用した情報システムの運用・保守時の対策）

第68条　クラウドサービス管理者は、第65条第2項で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録する。

2　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正する。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告する。

3　クラウドサービス管理者は、クラウドサービス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。

（クラウドサービスを利用した情報システムの更改・廃棄時の対策）

第69条　クラウドサービス管理者は、第65条第3項で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずる。また、クラウドサービスの利用終了時に実施状況を確認・記録する。

第3節　クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

（要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備）

第70条　統括情報セキュリティ責任者は、以下を全て含む要機密情報を取り扱わない場合のクラウドサービスの利用に関する運用規程を整備する。

(1)　クラウドサービスを利用可能な業務の範囲

(2)　クラウドサービスの利用申請の許可権限者と利用手続
(3)　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理
(4)　クラウドサービスの利用の運用規程

(要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施)

第71条　情報セキュリティ責任者は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、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利用申請の許可権限者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請する。

2　利用申請の許可権限者は、情報セキュリティ責任者が利用を申請するクラウドサービスの定型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かどうかについての確認の結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定する。

3　利用申請の許可権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録する。

4　クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずる。

第3章　機器等の調達

第1節　機器等の調達

(機器等の調達に係る運用規程の整備)

第72条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備する。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。

2　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。

第5編　情報システムのライフサイクル

第1章　情報システムの分類

第1節　情報システムの分類基準等の整備

(情報システムにおける分類のための運用規程の整備)

第73条　統括情報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インシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である情報システムの分類基準を運用規程として整備する。

(情報システムの分類基準に基づいた情報セキュリティ対策に係る運用規程の整備)

第74条　統括情報セキュリティ責任者は、情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を運用規程として整備する。

(情報システムの分類基準に基づいた分類の実施)

第75条　統括情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ、その結果を報告

させる。
2　前項の報告を受けた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発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には情報システムセキュリティ責任者に修正の指示を行う。
（情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用規程の見直し）
第76条　統括情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた情報セキュリティ対策の具体的な対策事項の運用規程について定期的な確認による見直しをする。
2　統括情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認する。

第2章　情報システムのライフサイクルの各段階における対策

第1節　情報システムの企画・要件定義

（実施体制の確保）
第77条　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。
2　最高情報セキュリティ責任者は、前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（独立行政法人国際協力機構情報システム管理規程(平成20年9月30日規程(情)第25号)第3条の2第1項に定める情報システム部担当理事）の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求める。
（情報システムの分類基準に基づいた分類の実施）
第78条　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、情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告する。
（情報システムのセキュリティ要件の策定）
第79条　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を勘案し情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、以下の全て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。
(1)　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
(2)　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)
(3)　情報システムに関連する脆弱性及び不正プログラムについての対策要件
(4)　情報システムの可用性に関する対策要件
(5)　情報システムのネットワーク構成に関する要件
2　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。
3　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、経済産業省が公表する「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。
4　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が取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要求する情報システムについては、情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等へ助言を求め、業務の特性や情報システムの特性を踏まえて、上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いかを確認する。

第2節　情報システムの調達・構築

（情報システムの構築時の対策）

第80条　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。
2　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　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、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。
4　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、以下を全て含む情報システム関連文書を整備する。
(1)　情報システムを構成するサーバ装置及び端末関連情報
(2)　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
5　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、以下を全て含む実施手順を整備する。
(1)　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
(2)　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
(3)　情報システムが停止した際の復旧手順

（納品検査時の対策）

第81条　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、仕様書等に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。
2　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へ移行する際に、当該情報システムの開発事業者から運用保守事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。

第3節　情報システムの運用・保守

（情報システムの運用・保守時の対策）

第82条　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監視を含むセキュリティ機能を適切に運用する。
2　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し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直す。
3　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、情報システム台帳及び関連文書の内容に変更が生じた場合、情報システム台帳及び関連文書を更新又は修正する。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告する。
4　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　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、危機的事象発生時に適切な対処が行えるよう運用をする。

第4節　情報システムの更改・廃棄

（情報システムの更改・廃棄時の対策）

第83条　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、以下を全て含む措置を適切に講ずる。
(1)　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
(2)　情報システム廃棄時の不要な情報の抹消（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）

第5節　情報システムについての対策の見直し

（情報システムについての対策の見直し）

第84条　情報システムセキュリティ責任者は、対策推進計画に基づき情報システムの情報セキュリティ対策を適切に見直す。
2　情報システムセキュリティ責任者は、機構内で横断的に改善が必要となる情報セキュリティ対策の見直しを適時検討し、必要な改善指示に基づき、情報セキュリティ対策を適切に見直す。また、措置の結果については、統括情報セキュリティ責任者へ報告する。

第3章　情報システムの運用継続計画

第1節　情報システムの運用継続計画の整備・整合的運用の確保

（情報システムの運用継続計画の整備・整合的運用の確保）

第85条　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場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討する。
2　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に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であるかを定期的に確認する。
3　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に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直す。

第4章　政府共通利用型システム

第1節　政府共通利用型システム利用時の対策

（政府共通利用型システム利用時の体制の整備）

第86条　情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程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。

2　統括情報セキュリティ責任者は、政府共通利用型システムが提供する機器等の提供を受けこれを役職員等が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに政府共通利用型システム利用管理者を指名する。

3　政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程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。

（政府共通利用型システム利用時の情報セキュリティ対策）

第87条　情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システム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、適切にセキュリティ要件を策定し、運用する。

2　情報システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

（政府共通利用型システム利用時の機器等の管理）

第88条　政府共通利用型システム利用管理者は、政府共通利用型システムが提供する機器等の提供を受けてこれを役職員等が利用する場合は、当該政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程及び実施手順を整備する。

2　政府共通利用型システム利用管理者は、提供を受けた政府共通利用型システムの機器等を把握するために必要な文書を整備する。

3　政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、政府共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知する。

4　政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

第6編　情報システムの構成要素

第1章　端末

第1節　端末

（端末の導入時の対策）

第89条　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物理的な端末について、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。
2　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を定め、それ以外のソフトウェアは利用させない。
3　情報システムセキュリティ責任者は、端末に接続を認める機器等を定め、接続を認めた機器等以外は接続させない。
4　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として策定した内容に従い、端末に対して適切なセキュリティ対策を実施する。
5　情報システムセキュリティ責任者は、端末において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対策を実施する。
(端末の運用時の対策)
第90条　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について、定期的に見直しを行う。
2　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。
(端末の運用終了時の対策)
第91条　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。
第2節　要管理対策区域外での端末利用時の対策
(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。）の導入及び利用に係る運用規程の整備)
第92条　統括情報セキュリティ責任者は、機構が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）を役職員等及び情報取扱事務従事者が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実施手順として定める。
2　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物理的な端末（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運用規程を整備する。
3　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構外通信回線に接続した機構が支給する物理的な端末を機構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、当該端末から機構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技術的な措置に関する運用規程を定める。
(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。）の導入及び利用時の対策)
第93条　情報システムセキュリティ責任者は、機構が支給する物理的な端末(要管理対策区域外で使用する場合に限る。)を役職員等及び情報取扱事務従事者が用いて要機密情報を取り扱う場合は、当該端末について前条第2項の技術的な措置を講ずる。
2　情報システムセキュリティ責任者は、要管理対策区域外において機構外通信回

線に接続した機構が支給する物理的な端末を機構内通信回線に接続させる際、当該端末について前条第3項の技術的な措置を講ずる。

第3節　機構支給以外の端末の導入及び利用時の対策

（機構支給以外の端末の利用可否の判断）

第94条　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け及び取扱制限、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。

（機構支給以外の端末の利用に関する運用規程等の整備）

第95条　統括情報セキュリティ責任者は、役職員等及び情報取扱事務従事者が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の許可等の手続を実施手順として定める。

2　統括情報セキュリティ責任者は、役職員等及び情報取扱事務従事者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、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などのリスクを踏まえた利用手順及び許可手続を実施手順として定める。

3　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、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を含めた安全管理措置に関する運用規程を整備する。

4　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構外通信回線に接続した機構支給以外の端末を機構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、当該端末から機構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運用規程及び許可手続に関する実施手順を定める。

（機構支給以外の端末の利用に関する責任者の策定）

第96条　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。

（機構支給以外の端末の利用時の対策）

第97条　役職員等及び情報取扱事務従事者は、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。

2　役職員等及び情報取扱事務従事者は、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、第95条第2項で定める利用手順に従う。

3　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、第95条第3項に定める安全管理措置を講じ、又は役職員等及び情報取扱事務従事者に講じさせる。

4　役職員等及び情報取扱事務従事者は、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。

第2章　サーバ装置

第1節　サーバ装置

（サーバ装置の導入時の対策）

第98条　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、物理的なサーバ装置の盗難、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。
2　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。
3　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を定め、それ以外のソフトウェアは利用させない。
4　情報システムセキュリティ責任者は、サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させない。
5　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として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施する。
6　情報システムセキュリティ責任者は、サーバ装置において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対策を実施する。
7　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は、適切な方法でサーバ装置のバックアップを取得する。
（サーバ装置の運用時の対策）
第99条　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について定期的な確認による見直しを行う。
2　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。
3　情報システムセキュリティ責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講ずる。
4　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、危機的事象発生時に適切な対処が行えるよう運用をする。
（サーバ装置の運用終了時の対策）
第100条　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。

第2節　電子メール

（電子メールの導入時の対策）
第101条　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。
2　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。
3　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。
4　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ずる。

第3節　ウェブ

（ウェブサーバの導入・運用時の対策）
第102条　情報システムセキュリティ責任者は、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、ウェブサーバが備える機能のうち、必要な機能のみを利用する。
2　情報システムセキュリティ責任者は、ウェブサーバ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。
3　情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を行う主体を限定する。
4　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転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化の機能及び電子証明書による認証の対策を講ずる。

第4節　ドメインネームシステム（DNS）

（DNSの導入時の対策）
第103条　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。
2　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。
3　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。
（DNSの運用時の対策）
第104条　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。
2　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。
3　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。

第5節　データベース

（データベースの導入・運用時の対策）
第105条　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。
2　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に、措置を講ずる。
3　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。
4　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に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。
5　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。

第3章　複合機・特定用途機器

第1節　複合機・特定用途機器

（複合機）

第106条　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。

2　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。

3　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。

（IoT機器を含む特定用途機器）

第107条　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。

第4章　通信回線

第1節　通信回線

（通信回線の導入時の対策）

第108条　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。

2　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。

3　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。

4　情報システムセキュリティ責任者は、役職員等及び情報取扱事務従事者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。

5　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。

（機構外通信回線の接続時の対策）

第109条　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当該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。

2　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及び機構内通信回線内の不正な通信の有無を監視するための措置を講ずる。

3　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、機構外通信回線から機構内通信回線に接続された機器等に対して行われるリモートメンテナンス

に係る情報セキュリティを確保する。
4　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。
（通信回線の運用時の対策）
第110条　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確認及び見直しを行う。
2　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及び機構内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをする。
3　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、機構外通信回線から機構内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認による見直しをする。
4　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。

第2節　通信回線装置

（通信回線装置の導入時の対策）
第111条　情報システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、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。
2　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に関する事項を含む実施手順を定める。
3　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として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施する。
4　情報システムセキュリティ責任者は、通信回線装置において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対策を実施する。
（通信回線装置の運用時の対策）
第112条　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・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管する。
2　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を構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管する。
3　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等を調査し、認識した脆弱性等について対策を講ずる。
（通信回線の運用終了時の対策）
第113条　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。

第3節　無線LAN

（無線LAN環境導入時の対策）

第114条　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。

第4節　IPv6 通信回線

（IPv6通信を行う情報システムに係る対策）

第115条　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。

2　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、IPv6通信による情報セキュリティ上の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。

（意図しないIPv6通信の抑止・監視）

第116条　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5章　ソフトウェア

第1節　情報システムの基盤を管理又は制御するソフトウェア

（情報システムの基盤を管理又は制御するソフトウェア導入時の対策）

第117条　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情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講ずる。

2　情報システムセキュリティ責任者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備する。

(1)　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(2)　情報システムの基盤を管理又は制御するソフトウェアで発生した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

（情報システムの基盤を管理又は制御するソフトウェア運用時の対策）

第118条　情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施する。

(1)　情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(2)　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

第6章　アプリケーション・コンテンツ

第1節　アプリケーション・コンテンツの作成・運用時の対策

（アプリケーション・コンテンツの作成に係る運用規程の整備）

第119条　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運用規程を整備する。

（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）

第120条　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のセキュリティ要件を定め、仕様に含める。

2　情報システムセキュリティ責任者は、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、前項に掲げる内容を調達仕様に含める。

（アプリケーション・コンテンツの開発時の対策）

第121条　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、セキュリティ要件として定めた仕様に加えて、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。

（アプリケーション・コンテンツの運用時の対策）

第122条　情報システムセキュリティ責任者は、利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直す。

2　情報システムセキュリティ責任者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずる。

3　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やウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずる。

第2節　アプリケーション・コンテンツ提供時の対策

（機構ドメインの使用）

第123条　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、機構ドメイン名を使用できない場合を除き機構ドメイン名を情報システムにおいて使用する。

2　情報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の作成を業務委託する場合においては、機構ドメイン名を使用するよう調達仕様に含める。

（不正なウェブサイトへの誘導防止）

第124条　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。

（アプリケーション・コンテンツの告知）

第125条　役職員等及び情報取扱事務従事者は、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、必要な対策を講ずる。

2　役職員等及び情報取扱事務従事者は、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編　情報システムのセキュリティ要件

第1章　情報システムのセキュリティ機能

第1節　主体認証機能

（主体認証機能の導入）

第126条　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。

2　情報システムセキュリティ責任者は、申請及び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。

3　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。

（識別コード及び主体認証情報の管理）

第127条　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を適切に付与し、管理するための措置を講ずる。

2　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。

第2節　アクセス制御機能

（アクセス制御機能の導入）

第128条　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。

2　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。

第3節　権限の管理

（権限の管理）

第129条　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必要最小限の範囲で適切に設定するよう、措置を講ずる。

2　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。

3　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不要なアクセス権限が付与されていないか定期的に確認する。

第4節　ログの取得・管理

（ログの取得・管理）

第130条　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並びに不正侵入及び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。

2　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。

3　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。

第5節　暗号・電子署名

(暗号化機能・電子署名機能の導入)

第131条　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、以下全ての措置を講ずる。

(1)　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。

(2)　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。

2　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」に基づき、情報システムで使用する暗号、電子署名のアルゴリズム、鍵長及びそれらを利用した安全なプロトコルを定める。また、その運用方法について定める。

3　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、鍵長及び運用方法に、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。

(暗号化・電子署名に係る管理)

第132条　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、以下の全ての措置を講ずる。

(1)　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。

(2)　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又は鍵長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、役職員等及び情報取扱事務従事者と共有を図る。

第6節　監視機能

(監視機能の導入・運用)

第133条　情報システムセキュリティ責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装する。

2　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において、情報システムに実装された監視機能を適切に運用する。

3　情報システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直す。

第2章　情報セキュリティの脅威への対策

第1節　ソフトウェアに対する脆弱性対策

（ソフトウェアに関する脆弱性対策の実施）

第134条　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。

2　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。

3　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対策の状況を定期的及び適時に確認する。

4　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態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。

第2節　不正プログラム対策

（不正プログラム対策の実施）

第135条　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。

2　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。

3　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。

第3節　サービス不能攻撃対策

（サービス不能攻撃対策の実施）

第136条　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。以下本条において同じ。)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。

2　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。

3　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、監視を行う。

第4節　標的型攻撃対策

（標的型攻撃対策の実施）

第137条　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。

2　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。

第3章　ゼロトラストアーキテクチャ

第1節　動的なアクセス制御の実装時の対策

(動的なアクセス制御における責任者の設置)

第138条　統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用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選任する。

(動的なアクセス制御の導入方針の検討)

第139条　情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定める。

(動的なアクセス制御の実装時の対策)

第140条　情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成する。

2　情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行う。

第2節　動的なアクセス制御の運用時の対策

(動的なアクセス制御の実装方針の見直し)

第141条　情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しをする。

(リソースの信用情報に基づく動的なアクセス制御の運用時の対策)

第142条　情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を行う。

第8編　情報システムの利用

第1章　情報システムの利用

第1節　情報システムの利用

(情報システムの利用に係る規定の整備)

第143条　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実施手順を整備する。

2　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実施手順を定める。

3　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録媒体を要管理対策区域外に持ち出す際の許可手続を定める。

(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)

第144条　情報システムセキュリティ責任者は、役職員等及び情報取扱事務従事者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。

(情報システムの利用時の基本的対策)

第145条　役職員等及び情報取扱事務従事者は、業務の遂行以外の目的で情報シス

テムを利用しない。
2　役職員等及び情報取扱事務従事者は、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。
3　役職員等及び情報取扱事務従事者は、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。
4　役職員等及び情報取扱事務従事者は、業務の遂行において、利用が認められていないソフトウェアを利用しない。また、当該ソフトウェアを業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。
5　役職員等及び情報取扱事務従事者は、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。
6　役職員等及び情報取扱事務従事者は、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。
7　役職員等及び情報取扱事務従事者は、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録媒体を要管理対策区域外に持ち出す場合には、課等情報セキュリティ責任者の許可を得る。
8　役職員等及び情報取扱事務従事者は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しない。

（端末（支給外端末を含む）の利用時の対策）

第146条　役職員等及び情報取扱事務従事者は、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。
2　役職員等及び情報取扱事務従事者は、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、課等情報セキュリティ責任者の許可を得る。
(1)　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
(2)　機構支給以外の端末　要保護情報
3　役職員等及び情報取扱事務従事者は、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、定められた措置を講ずる。

（電子メール・ウェブの利用時の対策）

第147条　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、要機密情報を含む電子メールを送受信する場合には、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。
2　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、機構外の者と電子メールにより情報を送受信する場合は、機構ドメイン名を使用できない場合を除き、当該電子メールのドメイン名に機構ドメイン名を使用する。
3　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、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。
4　役職員等及び情報取扱事務従事者は、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。

5　役職員等及び情報取扱事務従事者は、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。

6　役職員等及び情報取扱事務従事者は、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、以下の全ての事項を確認する。

(1)　送信内容が暗号化されること。

(2)　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。

(識別コード・主体認証情報の取扱い)

第148条　役職員等及び情報取扱事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しない。

2　役職員等及び情報取扱事務従事者は、自己に付与された識別コードを適切に管理する。

3　役職員等及び情報取扱事務従事者は、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。

4　役職員等及び情報取扱事務従事者は、自己の主体認証情報の管理を徹底する。

(暗号・電子署名の利用時の対策)

第149条　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム、鍵長及び方法に従う。

2　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理する。

3　役職員等及び統括情報セキュリティ責任者が別に定める一部の情報取扱事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

(不正プログラム感染防止)

第150条　役職員等及び情報取扱事務従事者は、不正プログラム感染防止に関する措置に努める。

2　役職員等及び情報取扱事務従事者は、情報システム(機構支給以外の端末を含む。)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(機構支給以外の端末を含む。)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。

(Web会議サービスの利用時の対策)

第151条　役職員等及び情報取扱事務従事者は、定められた利用手順に従い、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。

2　役職員等及び情報取扱事務従事者は、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。

(クラウドサービスを利用した機構外の者との情報の共有時の対策)

第152条　役職員等及び情報取扱事務従事者は、機構外の者と情報の共有を行うこ

とを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずる。
2　役職員等及び情報取扱事務従事者は、機構外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除する。

第2節　ソーシャルメディアによる情報発信

（ソーシャルメディアによる情報発信時の対策）

第153条　統括情報セキュリティ責任者は、機構が管理するアカウントでソーシャルメディアを利用することを前提として、以下を全て含む情報セキュリティ対策に関する運用規程などを定める。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。

(1)　機構のアカウントによる情報発信が実際の機構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。

(2)　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。

2　役職員等及び情報取扱事務従事者は、要安定情報の国民への提供にソーシャルメディアを用いる場合は、機構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。

第3節　テレワーク

（運用規程の整備）

第154条　統括情報セキュリティ責任者は、テレワークの実施時の情報セキュリティ対策に係る運用規程を整備する。なお、原則としてテレワークは機構が支給する端末で行うよう定める。

（実施環境における対策）

第155条　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構外通信回線を経由して機構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情報セキュリティを確保する。

2　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。

3　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ずる。

4　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。

（実施時における対策）

第156条　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役職員等及び情報取扱事務従事者が確認するべき項目を定め、役職員等及び情報取扱事務従事者に当該項目を確認させる。

2　役職員等及び情報取扱事務従事者は、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。また、自宅以外でテレワークを実施する場合

には、離席時の端末(支給外端末を含む。)の盗難に注意する。
3　役職員等及び情報取扱事務従事者は、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構外通信回線を利用してテレワークを行わない。

附　則

1　この細則は、平成29年4月3日から施行し、平成29年4月1日から適用する。
2　この細則により、細則の実施に係る細目の決定を理事長から授権又は委任される者（以下「授権者」という。）が異なることとなる場合であって、この細則の施行の際、現に制定済の準内部規程等の細目（以下「準内部規程等」という。）があるときは、当該準内部規程等に相当する準内部規程等が新たな授権者により別途制定されるまでの間、現に制定済の準内部規程等を当該新たな授権者により制定されたものとみなす。

附　則(令和2年1月31日細則(情)第1号)

この細則は、令和2年1月31日から施行する。

附　則(令和3年3月31日細則(総)第9号)

この細則は、令和3年4月1日から施行する。

附　則(令和4年3月31日細則(情)第1号)

この細則は、令和4年4月1日から施行する。

附　則(令和5年3月31日細則(情)第6号)

この細則は、令和5年4月1日から施行する。

附　則(令和6年3月13日細則(情)第5号)

この細則は、令和6年4月1日から施行する。

附　則(令和6年7月31日規程(総)第17号)

この細則は、令和6年8月1日から施行する。

附　則(令和6年8月9日細則(情)第16号)

この細則は、令和6年8月9日から施行する。

附　則(令和7年2月27日細則(情)第1号)

この細則は、令和7年2月27日から施行する。