大学共同利用機関法人自然科学研究機構
情報セキュリティ対策基準

２０２５年３月２７日

大学共同利用機関法人

自然科学研究機構

目　次

はじめに

「大学共同利用機関法人自然科学研究機構情報セキュリティ対策に関する基本規程」（平成28年９月23日自機規程第111号。以下「基本規程」という。）第５条第３項の規定に基づき、以下のとおり大学共同利用機関法人自然科学研究機構情報セキュリティ対策基準（以下「対策基準」という。）を定める。

対策基準は、原則、役職員等全員に適用する。

第１章から第５章は情報を扱う者すべてが理解・実践する必要がある。

第６章から第７章は、特に情報セキュリティ対策関係者（最高情報セキュリティ責任者、総括情報セキュリティ責任者、機関最高情報セキュリティ責任者、情報セキュリティ責任者、副情報セキュリティ責任者、CSIRT、情報セキュリティ管理者、情報システム管理者、情報システム担当者等）が理解・実践する必要がある。

対策基準の用語は、基本規程第３条各号に掲げるもののほか、【別紙】の用語の定義に掲げるものによる。

第１章　総則

1.1 対策基準の目的

情報セキュリティの基本は、情報の重要度に応じた「機密性」「完全性」「可用性」を確保することであり、大学共同利用機関法人自然科学研究機構（以下「機構」という。）が自らの責任において情報セキュリティ対策を講ずることとする。

対策基準は、「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（令和５年度版）」（令和５年７月４日サイバーセキュリティ戦略本部）に準拠するとともに、法令及び基準、政府決定等の改正に合わせ、必要に応じ逐次見直すこととする。

1.2 対策基準の適用対象

(1) 対策基準において適用対象とする者は、原則として全ての役職員等とする。

(2) 対策基準において適用対象とする情報は、以下の情報とする。

① 役職員等が職務上使用することを目的として調達し、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において利用・生成された情報又はそれらの外部電磁的記録媒体に記録された情報（当該システムに対し入出力された書面に記載された情報を含む。）

② その他のシステムにより利用・生成され、又は外部電磁的記録媒体に記録された情報（当該システムに対し入出力された書面に記載された情報を含む。）であって、役職員等が職務上取り扱う情報

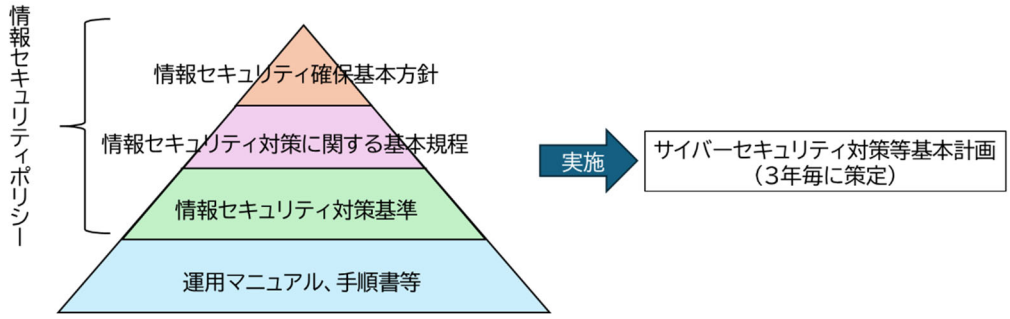
③ ①及び②のほか、調達し、又は開発したシステムの設計又は運用管理に関する情報

(3) 対策基準において適用対象とする情報システムは、対策基準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。

(4) 機構は策定した対策基準で定める対策を実施するため、必要に応じ運用マニュアル、手順書等（以下「マニュアル等」という。）を整備する。

1.3 対策基準の位置づけ

対策基準は下図のとおり位置づける。



第２章　情報セキュリティ対策の基本的枠組み

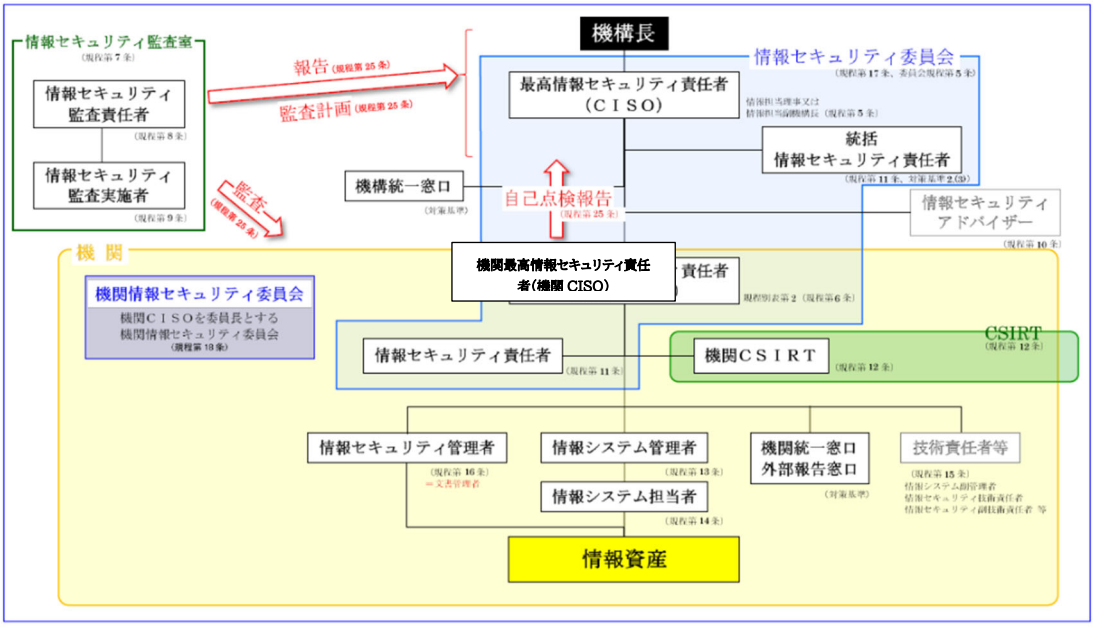
2.1 組織・体制

(1) 目的・趣旨

情報セキュリティ対策に係る全ての役職員等の権限と責務を明確にし、必要となる組織・体制を整備する。特に最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）は、組織内を統括し、組織全体として情報セキュリティ対策が計画的に実施されるよう努めなければならない。

(2) 情報セキュリティ対策推進体制・職務・職責

情報セキュリティ対策の推進体制



① CISO（基本規程第５条）

(a) CISOは、機構における全ての情報資産の開発、管理、運用及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

(b) CISOは自らを補佐させるため、統括情報セキュリティ責任者を置く。統括情報セキュリティ責任者は、機構事務局の情報セキュリティ責任者とする。

(c) CISOは、情報セキュリティ戦略の意思決定を行った際には、機関最高情報セキュリティ責任者（以下「機関CISO」という。）を通じてその内容を関係部局等に適切に通知するものとする。

(d) CISOは、情報セキュリティインシデント（以下「インシデント」という。）の発生又は発生するおそれを認知した場合は、速やかに必要な対応を取るとともに、文部科学省等に報告する。

(e) CISOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有し

た専門家を情報セキュリティアドバイザーとして置く。情報セキュリティアドバイザーは、CISOに対して情報システムに関する技術的事項、インシデントへの対処その他必要な指導・助言を行うものとする。

(f) CISOは、情報セキュリティに関する状況を把握するとともに、情報セキュリティリスクを分析・評価し、「サイバーセキュリティ対策等基本計画」（以下「基本計画」という。）を策定するとともに、それを着実に実施する。

② 機関CISO（基本規程第６条）

(a) 機関CISOは、CISOを補佐するとともに、基本規程別表第２に規定する所掌する機関（以下「所掌機関」という。）における情報資産の開発、管理、運用及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

(b) 機関CISOは、自らを補佐させるため、情報セキュリティ責任者を指名する。

(c) 機関CISOは、インシデントの発生又は発生するおそれを認知した場合は、速やかに必要な対応を取るとともに、CISO等に報告しなければならない。

(d) 機関CISOは、基本規程第13条第１項に基づき情報システム管理者を指名する。当該情報システム管理者に重要サーバ（外部公開サーバ及び機密性３以上の情報を格納している等の重要な情報を扱うサーバをいう。以下同じ。）を管理させようとする場合は、その資質について機関CISOが指名する者又は機関CSIRT（以下「重要サーバ管理資格確認者」という。）による確認を実施のうえ、その結果を尊重し、指名しなければならない。

③ 統括情報セキュリティ責任者（基本規程第11条）

統括情報セキュリティ責任者は、CISOを補佐するとともに、緊急時における連絡の中核としての役割を持つ。そのため、CISO、機関CISO、統括情報セキュリティ責任者、情報セキュリティ責任者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

④ 情報セキュリティ責任者（基本規程第11条）

(a) 情報セキュリティ責任者は機関CISOを補佐するとともに、所掌機関のネットワーク及び情報システムにおける開発、運用、情報資産の管理並びに情報セキュリティ対策に関して、情報セキュリティポリシー及び実施規則並びにこれらに基づきCISO及び機関CISOが定める手順書等（以下「情報セキュリティポリシー等」という。）に基づき指示を行う権限及び責任を有する。

(b) 情報セキュリティ責任者は、所掌機関における情報セキュリティ対策に関して、情報セキュリティポリシー等に基づき、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、指導及び助言を行う権限を有する。

(c) 情報セキュリティ責任者は、所掌機関等における共通的なネットワーク、情報システム等の情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

(d) 情報セキュリティ責任者は、緊急時における連絡に資するため、機関CISO、情報

セキュリティ責任者、機関CSIRT、情報セキュリティ管理者、情報システム管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

(e) 情報セキュリティ責任者は、情報システム管理者の権限執行を監視するため、必要な点検等を実施する権限を有する。

(f) 情報セキュリティ責任者は、所掌機関におけるネットワーク及び情報システム（外部電磁的記録媒体を除く。）に係る情報資産台帳（以下「情報資産台帳」という。）並びに所掌機関における外部電磁的記録媒体に係る管理台帳（以下「外部電磁的記録媒体管理台帳」という。）を整備しなければならない。

(g) 情報資産台帳には、名称、設置場所、分類・格付け、個人情報保存の該非、特定個人情報保存の該非、内蔵電磁的記録媒体の暗号化、使用者等、管理上必要な項目を含めなければならない。

(h) 外部電磁的記録媒体管理台帳には、機密性分類及び使用者等、管理上必要な項目を含めなければならない。

⑤ 副情報セキュリティ責任者（基本規程第11条）

機関CISOは、情報セキュリティ責任者からの要請に基づき、必要であると認めた場合は、任命期間及び所掌範囲を指定して、副情報セキュリティ責任者を指名することができる。

⑥ CSIRT（基本規程第12条）

(a) 機構におけるインシデントマネジメントを実施するため、各機関に機関CSIRTを置く。機関CSIRTは、各機関のインシデント発生予防（脆弱性情報等の収集・共有を含む。）、対策、監視、インシデント発生時及び発生後の対応等を行う。

(b) 機関CSIRTは、インシデント対策について、機関CISO及び情報セキュリティ責任者並びに情報システム管理者へ助言を行うことができる。

また、情報セキュリティ責任者及び情報システム管理者から要請があった場合は、これに応じなければならない。

(c) 機関CSIRTは、インシデントの発生又は発生するおそれを認知し、直ちに対処が必要と判断した場合は、機関CISO及び情報セキュリティ責任者の指示の有無にかかわらず即時に、システムの緊急停止及びネットワーク遮断などの対応を行う又は命じることができる。

(d) 機関CSIRTにチームリーダーを置くことができ、機関CISOが指名する者をもって充てる。チームリーダーは、機関CSIRTの総括及び調整等を行う。

(e) チームリーダーは、機関CSIRTとして情報セキュリティ上、緊急に必要と認める場合は、CISOと調整の上、役員及び機関の長に直接意見を具申することができる。

(f) チームリーダーは、特に必要と認めるサーバについては、情報システム管理者に依頼して監査をすることができる。その結果、問題等が見受けられる場合はサーバ管理者に是正等を要請することができる。その際は、速やかに機関CISOへ報告しなければならない。

(g) チームリーダーは所掌機関における重要サーバ管理者の力量について確認する必要があると判断した場合は、その理由を明示し、機関CISOに再確認又は交代を要求することができる。

(h) 機構に機関のチームリーダーを統括する統括チームリーダーを置き、事務局等のチームリーダーをもって充てる。統括チームリーダーは、インシデントの内容に関し、情報収集するため、CISOの了解を得て、組織外CSIRT及びJPCERTコーディネーションセンター（JPCERT/CC）並びに独立行政法人情報処理推進機構（IPA）等に連絡することができるものとする。

(i) 統括チームリーダーは、機関CSIRTとの連携、組織外CSIRTとの連携及び情報共有を図るほか、毎年度機構で生じたインシデント及びヒヤリハットを取り纏め、CISOへ報告しなければならない。

⑦ 情報セキュリティ管理者（基本規程第16条）

(a) 情報セキュリティ管理者はその所掌する課室、研究グループ等のネットワーク及び情報システムで取り扱う情報（基本規程第３条第５号。以下「所掌取扱情報」という。）の分類・格付け及び情報セキュリティ対策に関する権限及び責任を有する。

(b) 情報セキュリティ管理者は、所掌取扱情報に対するインシデント又はそのおそれを認知した場合は、⑬(b)に規定する機関統一窓口へ速やかに報告を行い、機関CISO又は情報セキュリティ責任者の指示を仰がなければならない。

(c) 情報セキュリティ管理者は、機密性３以上の情報を扱う場合は、当該取扱部署、研究グループ等における当該情報の取扱上の注意点等をまとめたマニュアルを整備しなければならない。

⑧ 情報システム管理者（基本規程第13条）

(a) 情報システム管理者は、基本規程第３条第１号から第４号及び第６号に定める所掌範囲のネットワーク、情報システム、情報施設・設備、電磁的記録媒体及びシステム関連文書（以下「所掌情報システム等」という。）の管理、開発、変更、運用、見直し等及び情報セキュリティに関する権限及び責任を有する。

(b) 情報システム管理者は、所掌情報システム等に係る情報セキュリティ実施手順の維持・管理の責任を有する。

(c) 情報システム管理者は、所掌するネットワーク及び情報システムに係る情報資産台帳を整備しなければならない。

(d) 情報システム管理者は、重要サーバを管理する際は、機関CISOから重要サーバ管理者として指名を受けなければならない。

(e) 重要サーバ管理者は、重要サーバに関するシステム構成カタログ等を整備し、機関CISOへ提出しなければならない。機関CISOは、機関CSIRTが閲覧可能な状態にしなければならない。

(f) 重要サーバ管理者は、重要サーバに対してソフトウェアをインストールしよう

とする場合（委託業者等が行う場合を含む。）は、その必要性やシステム構成カタログ、保守請負業者等の緊急連絡先一覧等を提示し、あらかじめ機関CISOの許可を得なければならない。重要サーバを新規に設置する場合（設置済みのサーバを新たに重要サーバとして扱うこととなる場合を含む。）も同様とする。

(g) 重要サーバ管理者は、所掌する重要サーバの引き継ぎにあたっては、「重要サーバ引継ガイドライン」に従ってこれを行わなければならない。

(h) 情報システム管理者は、他の情報システム管理者から協力要請や相談があった場合は、可能な範囲で対応しなければならない。

(i) 機関CISOは、情報システム管理者によるサポートを目的とする役職員等向けの技術相談窓口を整備し、周知しなければならない。

⑨ 情報システム担当者（基本規程第14条）

(a) 情報システム担当者は、情報システム管理者の指示等に従い、所掌情報システム、外部電磁的記録媒体等の管理、開発、運用、更新等の作業を行う。

(b) 情報システム担当者は、情報システム管理者の指示等に従い、情報資産台帳及び外部電磁的記録媒体管理台帳を整備する。

⑩ 情報セキュリティ委員会（基本規程第17条）

(a) 情報セキュリティ委員会は、「大学共同利用機関法人自然科学研究機構情報セキュリティ委員会規程」（平成28年９月23日自機規程第112号）第２条の規定に従い、機構における情報システムの運用、情報資産の管理、情報セキュリティ対策の状況を確認するとともに、基本計画の実施状況、基本規程第25条に定める監査（以下「監査」という。）の結果及び基本規程第26条に定める自己点検（以下「自己点検」という。）の結果を確認する。

(b) 情報セキュリティ委員会は、基本計画の進捗状況、監査及び自己点検結果等に基づき、必要に応じてCISOに改善策を提言する。

(c) CISOは、情報セキュリティ委員会に対して、基本計画等に関する意見を求めることができる。

⑪ 機関情報セキュリティ委員会（基本規程第18条）

各機関において、個別に対策すべき情報セキュリティ対策を行うため、機関に機関CISOを委員長とする機関情報セキュリティ委員会を置き、機関における情報セキュリティに関する重要な事項を審議・決定する。

⑫ 兼務の禁止（基本規程第19条）

(a) 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

(b) 情報セキュリティ監査にあたっては、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(c) ②(d)に規定する重要サーバ管理資格確認者と、資質確認を受ける情報システム管理者は、やむを得ない場合を除き、同一人であってはならない。

⑬　情報セキュリティに関する統一的な窓口及び外部から通報を受けるための窓口

(a) 機構の情報セキュリティに関する統一的な窓口（機構統一窓口）は、事務局総務課とする。

(b) 機関におけるインシデントの統一的な窓口（機関統一窓口）及び機構における情報システム等の情報資産に関するインシデントについて外部から通報を受けるための窓口（外部通報窓口）として、下記のとおり設置する。

機関等区分 （基本規程別表第２）	機関統一窓口	外部通報窓口
国立天文台	情報セキュリティ室	総務課総務係
核融合科学研究所	情報通信システム部情報ネットワークグループ	管理部総務企画課企画・評価係
岡崎３機関等	岡崎３機関等機関統一窓口担当	岡崎統合事務センター総務部総務課図書・ITソリューション係
事務局等	事務局総務課企画評価係	事務局総務課企画評価係

※　ただし、組織運営通則第２条の２の各号に掲げる共創戦略統括本部、アストロバイオロジーセンター及び生命創成探究センターについて、機関等の施設に設置された研究室等は、当該機関等が窓口となる。

(c) 機関CISOは、機関統一窓口及び外部通報窓口を整備する。当該窓口がインシデントについて部局等より報告を受けた場合には、状況を確認し、速やかに機関CISOへ報告する。

(d) CISOは、インシデント等に関し外部へ報告する際には、外部通報窓口への連絡手段を公表しなければならない。

⑭　情報関係相談窓口等

(a) 各機関において、役職員等からの日常の相談に応じる体制を構築する。

(b) 機構に各機関の情報システム及び情報セキュリティの関係者による連絡会（以下「情報基盤連絡会」という。）を置き、定期的に、情報システム、情報資産、情報化推進及び情報セキュリティに関する情報収集と技術的検討を行う。

2.2 資産管理

(1) 目的・趣旨

情報セキュリティ対策を講じるにあたって、自組織の資産の状況を把握することが重要である。資産の把握が不十分な状況では、把握できていない資産が存在することによる対策の漏れや、網羅的な対策がなされず情報システムに脅威が存在し続ける可能性がある。

さらに、インシデントが発生した際、資産が正しく管理されていないとインシデントに対応するための情報収集に時間を要するなど、インシデントへの対処が遅れる等の可能性がある。

(2) 遵守事項

① 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、情報資産台帳及び外部電磁的記録媒体管理台帳に整備する。

② 情報の格付けの区分

情報資産には格付けを行い、格付け区分に従い適切な対応を行う。格付けの区分は基本規程第20条に定めるとおりとし、その運用の原則は下表のとおりとする。個別の情報資産は、情報セキュリティ管理者が格付けを行う。

情報資産の分類基準、取扱制限及び具体的な情報資産

機密性による情報資産の分類	分類基準	取扱制限	具体的な情報資産
機密性4（極秘）	国の安全保障に関わるもの，特定個人情報など，内容が漏洩した場合，機構の業務への影響が深刻かつ重大な情報資産	機密性3の取扱制限に加えて，機関CISOの許可がある場合を除き下記の措置 ・複製及び配付禁止 ・指定場所以外でのアクセスの禁止 ・運用は，スタンドアロン又は独立したネットワークの範囲に限定	①国の安全保障にかかわる情報（国防、外交等） ②特定個人情報（マイナンバーやマイナンバーに対応する符号）を含む情報
機密性3（秘密）	機構で取り扱う情報資産のうち，秘密文書に相当する機密性を要する情報資産	機密性2の取扱制限（例外措置を除く。）に加えて，機関CISOの許可がある場合を除き下記の措置 ・機構の資産である情報システム端末以外での作業の原則禁止 ・必要以上の複製及び配付禁止 ・電磁的記録媒体の施錠可能な場所への保管	①個人情報（住所、氏名。生年月日、メールアドレス、顔画像等）を含む情報 ②予算要求・予算執行計画、調達計画、人事採用計画等機構又は機関の運営に関わる重要な情報で情報セキュリティ管理者が指定したもの ③国から機構又は機関限りとして提示された情報 ④発表・公開する以前の研究データ、論文情報等研究責任者が指定したもの
機密性2（機構外秘）	機構の業務で取り扱う情報資産のうち，秘密文書に相当する機密性は要しないが，漏えいにより，個人の権利が侵害され又は機構業務の遂行に支障を及ぼすおそれがある情報資産（本分類区分で取扱うことを本人が承諾した個人情報を含む。）	・保管場所の制限，保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信，情報資産の運搬・提供時における暗号化・パスワード設定又は鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定	①機構内又は機関内だけで提示される情報で機構又は機関外に対して、秘匿性がある情報 ②漏えいにより，個人の権利が侵害され又は機構業務の遂行に支障を及ぼすおそれがある情報資産 ③研究データ、論文情報等で機構外秘と研究責任者が指定したもの
機密性1	公表済みの情報，公表しても差し支えない情報等，機密性2以上の情報資産以外の情報資産		

2.3 情報セキュリティ関係マニュアル等の整備と運用

(1) 目的・趣旨

機関の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、機関として遵守すべき対策の基準を、情報セキュリティに係るリスク評価の結果等を踏まえた上で定めるとともに、計画的に対策を実施することが重要である。

そのため、対策の実施に必要な具体的なマニュアル等を定めるとともに、定期的に状況の把握と検証を行う。

(2) 遵守事項

① リスク評価の実施

CISOは、自己点検の結果、情報セキュリティ監査の結果、内部監査等を勘案した上で、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、リスク評価を行う。

② 対策基準の策定

CISO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として実効性のある対策基準を定める。

また、対策基準は、機関の業務、取り扱う情報、保有する情報システムに関するリスク評価の結果及び対策基準や基本計画の見直し結果を踏まえた上で定める。

③ 基本計画の策定

CISOは、情報セキュリティ委員会における審議を経て、基本計画を定め計画的に実施する。

④ マニュアル等の策定

各機関の情報セキュリティ責任者は、必要に応じマニュアル等を整備するとともに、その実施状況を機関CISOに報告する。

また、マニュアル等は情報基盤連絡会で共有を図る。

⑤ 例外措置

基本規程、対策基準、マニュアル等(以下「関係規程等」という。)を遵守することが困難な状況において、業務の適正な遂行を著しく妨げるなどの理由により、やむを得ず規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことが必要な場合、機関CISOの許可を得なければならない。機関CISOがその許可をした場合は、速やかにCISOに報告する。

⑥ 違反への対処

役職員等は、関係規程等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。

それを受け、情報セキュリティ責任者は、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、機関CISOへ報告し、機関CISOは統括

情報セキュリティ責任者を通じて、CISOに報告する。CISOは必要な対応を行う。

2.4 教育

(1) 目的・趣旨

関係規程等が役職員等に認知されて情報セキュリティが確保されることはもとより、その水準の向上を目指す必要がある。このため、全ての役職員等が関係規程への理解を深められるよう、適切に教育を実施する。

また、近年のインシデントの増加等に鑑み、各機関は、情報セキュリティの専門性を有する人材を育成する。

(2) 遵守事項

① 教育実施計画の策定、教育対象者の整理

(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、基本計画に従って、教育実施計画を策定し、その着実な実施を図る。なお、情報セキュリティの状況の変化に応じ役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。

(b) 情報セキュリティ責任者は、教育対象となる者を抽出し、必要な教育を施さなければならない。

② 教育の実施

(a) 情報セキュリティ責任者は、教育実施計画に基づき、役職員等に対して、関係規程等に係る教育を適切に受講させる。役職員等は、指示に従って、必要な時期に教育を受講する。

(b) 情報セキュリティ責任者は、「2.1 組織・体制」(2)の情報セキュリティ対策推進体制に属する役職員等に必要な専門的教育を受講させる。

(c) (a)及び(b)の教育の実施結果は、機関CISO及びCISOに報告する。その際、教育の実施状況を分析・評価した結果を添付する。

第３章　情報の取扱い

3.1 情報の取扱い

(1) 目的・趣旨

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下本章において「利用等」という。）を行う必要があり、情報のセキュリティの確保のためには、当該情報を利用等する全ての役職員等が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。

このため、役職員等は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付け及び取扱制限の明示等を行い、その段階において対策を講ずる必要がある。なお、法人文書管理の観点については「大学共同利用機関法人自然科学研究機構法人文書管理規程」（平成16年４月１日自機規程第50号）に則って取り扱う。

(2) 遵守事項

①　情報の格付け及び取扱制限の決定・明示等

(a) 役職員等は、情報の作成時及び機関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、格付け及び取扱制限の定義に基づき格付け及び取扱制限を決定し、明示等する。

(b) 役職員等は、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け及び取扱制限の決定がなされている場合には、原則として、元となる情報の機密性に係る格付け及び取扱制限を継承する。

(c) 役職員等は、修正、追加、削除その他の理由により、作成及び入手時に決定した情報の格付け及び取扱制限を見直す必要があると考える場合には、情報セキュリティ管理者の承認を得る。

②　情報の利用・保存

(a) 役職員等は、利用する情報に明示等された格付け及び取扱制限に従い、当該情報を適切に取り扱う。特に機密性４の情報について要管理対策区域外で業務を行う場合は、必要な安全管理措置を講じた上で、情報セキュリティ管理者の許可を得る。

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

ア　情報を機器等に保存する場合は、インターネットによる漏洩を防止する措置を取るとともに、暗号化による保護を行う。

イ　当該情報を保存した機器等については、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。

(c) 機密性２以上の情報を扱うUSBメモリ等の外部電磁的記録媒体の利用は、原則として機関からの支給品とし、支給品以外の利用は、情報セキュリティ管理者の許可を得る。

(d) 役職員等は、機密性２以上の情報の移動にUSBメモリ等の外部電磁的記録媒体を用いる際には、情報の暗号化を行う。

③ 情報の提供・公表

(a) 役職員等は、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) 役職員等は、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、その提供先において、当該情報に付された格付け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) 役職員等は、機密性２以上の情報を閲覧制限の範囲外の者に提供する場合には、情報セキュリティ管理者の許可を得る。

④ 情報の運搬・送信

(a) 役職員等は、機密性４の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、情報の格付け及び取扱制限に応じて、暗号化措置等安全確保のための適切な措置を講ずる。

(b) 役職員等は、電子メール（外部サービス及びクラウドサービスを用いる場合を含む。）により機密性２以上の情報を送信・共有するときは、以下のとおり取り扱うものとする。

ア 機密性２及び３の情報を送信・共有するときは、当該情報について「暗号化ガイドライン」に基づく暗号化を行わなければならない。ただし、機関が運用しているクラウドサービス（Microsoft365及びGoogle Workspaceのコアサービスに限る。）を用いて情報を共有する場合は、この限りではない。

イ 機密性２及び３の情報を送信・共有する際には、相手先の再確認、送信遅延設定、共有時間の設定等誤送信に対する対策を行う。

ウ 情報の送信・共有先が管理権限を有するなど信頼性を確保できるBox等のサービスについては、機密性２及び３を送信・共有することができるものとする。

エ 機密性４の情報については、機関CISOの許可がある場合を除き、情報の送信・共有を禁止する。

以上は【別表】を参照のこと。なお、運用にあたり別途マニュアルを定める。

⑤ 情報の消去

(a) 役職員等は、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) 役職員等は、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) 役職員等は、機密性２以上の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。

⑥ 情報のバックアップ

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

(b) 役職員等は、取得した情報のバックアップについて、格付け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。

3.2 情報を取り扱う区域の管理

(1) 目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。

また、災害の発生による情報システムの損傷等の可能性もあることから、情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

(2) 遵守事項

情報システム管理者は、要管理対策区域の範囲を特定し、これを受けて、情報セキュリティ責任者は要管理対策区域を定める。情報システム管理者は、許可されていない者の立入りを制限する等、入退管理対策を実施する。

3.3 インシデントへの対処

(1) 目的・趣旨

インシデントを認知した場合には、CISOに早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる。

また、インシデントの対処が完了した段階においては、原因について調査するなどにより、インシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげる。

(2) 遵守事項

① インシデントに備えた事前準備

(a) 情報セキュリティ責任者は、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関及び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、役職員等に周知する。

(b) 情報セキュリティ責任者は、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。

(c) 情報セキュリティ責任者は、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ホームページ等に明示する。

(d) CISOは機関CISOと協力し、インシデントへの対処訓練を定期的に実施し、対応手順等が適切に機能することを確認する。

② インシデントへの対処

(a) 役職員等は、インシデントの可能性を認知した場合には、機関の報告窓口に報告し、指示に従う。

(b) 機関CSIRTは、報告されたインシデントの可能性について状況を確認し、インシデントであるかの評価を行う。

(c) 機関CSIRTチームリーダーは、インシデントであると評価した場合、情報セキュリティ責任者及び機関CISO並びにCISOに速やかに報告する。

(d) 機関CSIRTは、インシデントに関係する情報システム管理者及び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、機関CSIRTは、同様の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管理者へ確認を指示する。

(e) 情報システム管理者は、所管する情報システムについてインシデントを認知した場合は、速やかに機関CSIRTに報告し、機関CSIRTの指示に従い対処する。

(f) 機関CSIRTは、認知した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、情報セキュリティ責任者及び機関CISO並びにCISOと協議し、警察への通報・連絡等を行う。

(g) 機関CSIRTは、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等を行うとともに、対処の内容を記録する。

③ インシデントに係る情報共有

(a) CISOは、インシデントに関して、速やかに文部科学省に報告を行う。

(b) インシデントにより、個人情報や特定個人情報の漏えい等が発生した場合、CISOは、必要に応じて個人情報保護委員会へ報告を行う。

(c) CISOは、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。

(d) 機関CSIRTチームリーダーは、インシデントに関して情報基盤連絡会で情報共有するとともに、機関情報セキュリティ委員会及び機構の情報セキュリティ委員会に報告する。

3.4 点検

3.4.1 情報セキュリティ対策の自己点検

(1) 目的・趣旨

情報セキュリティ対策の実効性を担保するためには、関係規程の遵守状況や実施すべき対策事項を実際に実施しているか否かを確認するとともに、組織全体の情報セキュリティ水準を確認することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

(2) 遵守事項

自己点検計画の策定・評価・改善

① 統括情報セキュリティ責任者は、基本計画に基づき年度自己点検実施要領を策定する。

② 情報セキュリティ責任者は、年度自己点検実施要領に基づき、自己点検を実施し、分析及び評価をする。情報セキュリティ責任者は、自己点検結果及び情報セキュリティの状況の変化に応じた見直しを機関CISO及びCISOに報告し、次年度の年度自己点検実施要領に反映させる。

③ CISOは、機関の自己点検結果を機構全体として評価し、自己点検の結果により明らかになった問題点について、必要に応じ基本計画に反映するとともに、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。

3.4.2 情報セキュリティ監査

(1) 目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。情報セキュリティ監査は、機構の情報セキュリティ対策の改善に係るPDCAサイクルを円滑に機能させるためにも重要である。

機構においては、機関情報セキュリティ責任者を監査責任者とした情報セキュリティ監査室を編成し、年１回、機構事務局等及び各機関のいずれかを対象に、情報セキュリティ監査を実施する。監査責任者は、機構事務局等及び各機関の持ち回りとする。当該年度監査対象外の場合においては、これまでの監査指摘事項への対応状況に関する監査（フォローアップ監査）を実施する。

(2) 遵守事項

監査実施計画の策定、実施、報告、改善措置

① 監査責任者は、基本計画に基づき監査実施計画を定める。必要な場合は、追加の

監査実施計画を定めることができる。

② 監査責任者は、監査実施計画に基づき、監査を実施し、結果を監査報告書としてCISO及び機構長に報告する。

③ CISO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及び完了時の報告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。

第４章　情報システムの利用

4.1 情報システムの利用

(1) 目的・趣旨

役職員等は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用することから、インシデントを引き起こさないよう、情報セキュリティポリシーをはじめマニュアル等を遵守するとともに、利用にあたっては常に細心の注意を払う必要がある。

(2) 遵守事項

① 情報システムの利用に係る規定の整備

(a) 情報システム管理者は、必要に応じ、業務で利用する情報システムのマニュアル等を整備し、利用者に周知する。

(b) 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マニュアルを定める。

② 情報システムの利用時の基本的対策

(a) 役職員等は、業務の遂行以外の目的で情報システムを利用してはならない。

(b) 役職員等は、情報システム管理者が接続許可を与えたネットワーク以外に機関の情報システムを接続してはならない。ただし、業務の必要により自宅のWi-Fi、外部Wi-Fiサービス（公共交通機関（鉄道や航空機等）や商業施設及び宿泊施設等が提供するサービス）を利用する場合は、その安全性を認識し、VPN接続、セキュリティソフト利用や接続サイトを精選する等、十分な安全対策を講じる。

(c) 役職員等は、機関のネットワークに、情報システム管理者の接続許可を受けていない情報システムや機器等を接続してはならない。

(d) 役職員等は、業務の遂行において、情報システム管理者により利用が認められていないソフトウェアを利用してはならない。ただし、当該ソフトウェアを職務上の必要により利用する場合は、情報システム管理者の承認を得る。

(e) 役職員等は、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。

(f) 役職員等は、機密性４の情報が記録された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には、情報セキュリティ管理者の許可を得る。

(g) 役職員等は、業務の遂行において、機関CISOの利用承認を得ていないクラウドサービスを利用してはならない。

③　電子メール・ウェブの利用時の対策

(a) 役職員等は、業務において電子メールを送受信する場合には、それぞれの機関が運営し、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) 役職員等は、業務において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、機関より付与されたメールアドレスを使用する。

(c) 役職員等は、会議の参加申し込み等、閲覧しているウェブサイトに表示されるフォームに個人情報を入力して送信する場合には、送信内容が暗号化されることや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を確認する。

(d) 役職員等は、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って対処するとともに、機関統一窓口に通報し、指示を仰ぐ。

(e) 役職員等は、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ことのないよう、情報システム管理者に相談する。

(f) 役職員等は、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。

④ 識別コード（ログインID)・認証情報（パスワードなど）の取扱い

(a) 役職員等は、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てはならない。

(b) 役職員等は、自己に付与された識別コードを適切に管理する。

(c) 役職員等は、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) 役職員等は、自己の認証情報の管理を徹底する。

⑤ 暗号・電子署名の利用時の対策

(a) 役職員等は、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、鍵長及び方法に従う。

(b) 役職員等は、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) 役職員等は、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。

⑥ 不正プログラム感染防止

役職員等は、情報システム（支給外端末を含む。以下本項において同じ。）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、感染したと思われる情報システムのネットワークへの接続を速やかに切断し、自らの判断で復旧等を行わずに機関統一窓口に通報し、指示を仰ぐ。

⑦ ウェブ会議サービスの利用時の対策

(a) 役職員等は、定められた利用手順に従い、ウェブ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。

(b) 役職員等は、ウェブ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。

⑧　クラウドサービスを利用した機関外の者との情報の共有時の対策

役職員等は、機関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機密性２以上の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当該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。

また、役職員等は、機関外の者と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機密性２以上の当該情報は速やかに削除する。

4.2 テレワーク

(1) 目的・趣旨

政府が推進する働き方改革では、柔軟な働き方に対応しやすい環境整備が求められていることから、役職員等が業務を遂行する上で、必ずしも勤務地に出勤する必要はなく、自宅等から遠隔で業務を遂行する形態に対応することや、大規模災害時や感染症対策として勤務地への出勤が抑制されるような状況下における業務の遂行の観点も含めて、テレワークの実施のための対策が必要である。

(2) 遵守事項

実施環境における対策

①　情報システム管理者は、テレワークの実施に際し、機関外のネットワークを経由して機関の情報システムへリモートアクセスする形態による場合は、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　情報システム管理者は、リモートアクセスする端末を許可されたものに限定するとともに、原則として多要素又は生体認証を講じるものとする。

③　情報システム管理者は、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。

④　情報システム管理者は、テレワーク実施前及び実施後に役職員等が確認するべき項目を定め、役職員等に当該項目を確認させる。

⑤　役職員等は、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。

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。

⑥　役職員等は、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外ネットワークを利用してテレワークを行ってはならない。ただし、業務の必要により自宅のWi-Fi、外部Wi-Fiサービス（公共交通機関（鉄道や航空機等）や商業施設及び宿泊施設等が提供するサービス）を利用する場合は、その安全性を認識し、VPN接続、セキュリティソフト利用や接続サイトを精選する等、十分な安全対策を講じる。

4.3 ソーシャルメディアによる情報発信

(1) 目的・趣旨

各機関において、積極的な広報活動等を目的としたソーシャルメディアの利用が一般的になっていることから、公的なアカウントであることを国民が確認できるようにする必要がある。

また、機関のアカウントを乗っ取られた場合、利用しているソーシャルメディアが予告なく停止した際に必要な情報を発信できない事態が生じた場合や、なりすましによる誤情報の拡散に備え、ホームページとの連携等の対応を取るなど、非常時の情報発信方法を確保しておく必要がある。

なお、ソーシャルメディアの利用に際しては、機密性１の情報以外を取り扱ってはならない。

(2) 遵守事項

ソーシャルメディアによる情報発信時の対策

① 情報セキュリティ責任者は、ソーシャルメディアの利用について、アカウント管理を含め、実態を把握する。

(a) 機関のアカウントによる情報発信が実際の機関のものであると明らかとするために、アカウントの管理と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。

(b) 不正アクセスの対策を講ずるために運用手順を定めたうえで、機関CISOに許可を得る。

② 役職員等は、可用性２以上の情報の提供にソーシャルメディアを用いる場合は、機関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。

4.4 サプライチェーンリスクへの対応

(1) 目的・趣旨

ハードウェア製品を意図的に不正改造したり、情報システム又はソフトウェアに不正なプログラムを埋め込んだりするなど、機構の意図しない変更を攻撃者が情報システム又は機器等に加えることにより、機密情報を窃取するなどのサプライチェーンリスクを軽減するため、情報に関するシステム・機器・役務等の調達時における仕様書に記載する事項を仕様書追加要件として定める。

(2) 遵守事項

「情報セキュリティ上のサプライチェーンリスクに対応するための仕様書追加要件」(令和６年２月１日情報化推進委員会・情報セキュリティ委員会決定)による。

4.5 情報システムの運用継続計画

(1) 目的・趣旨

情報システムの停止が大学や研究コミュニティの安全や利益に重大な脅威をもたらす可能性のある業務は、地震、火災、感染症、インシデント等の危機的事象発生時でも継続させる必要があることから、「事業継続計画（BCP)」を策定し運用する。

(2) 遵守事項

「事業継続計画（BCP)」(令和５年10月１日制定)において、情報システムにおける事業継続に関して定めており、非常事態発生時等において遵守する。

第５章　外部委託

5.1 業務委託

(1) 目的・趣旨

情報システムやアプリケーションの開発・管理・運用等に関し、機関外の者に業務を委託する際は直接の情報セキュリティ管理が困難なため、委託先が機密性２以上の情報を適切に保護するよう、調達仕様書に要求事項を定め、契約条件に含めることが必要である。特に業務実施途中において機構側の意図しない変更が加えられないよう、委託する業務の範囲や責任範囲を明確にし、双方で情報セキュリティ対策について合意することが重要である。なお、業務委託はクラウドサービスなど様々な形態があることから、それぞれ特有のリスクを考慮し、適切なセキュリティ対策を実施する必要がある。

＜業務委託の例＞

・情報システムの開発及び構築業務の委託
・アプリケーション・コンテンツの開発業務の委託
・情報システムの運用業務の委託
・業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
・プロジェクト管理支援業務の委託
・調査・研究業務（調査、研究、検査等）の委託
・ウェブサイトの運用業務の委託

(2) 遵守事項

① 業務内容を特定し、委託先の選定条件を含む仕様を策定し、機構の調達手続きに従って、委託先の選定、契約締結を行う。仕様書策定時に調査が必要な場合は、調査対象者との間で秘密保持契約（NDA）を締結する。

② 機密性２以上の情報を取り扱う場合は、業務の履行状況及び情報セキュリティ対策の履行状況の定期的確認を行うとともに、インシデント発生時の必要な措置についてあらかじめ対応策等について聴取を行う。

③ 業務終了時には、仕様書に定める事項の他、セキュリティ対策の実施確認を行う。

また、委託先において取り扱われた情報の返却、廃棄又は抹消の確認を行う。

④ サプライチェーンリスクに対応するため、「4.4 サプライチェーンリスクへの対応」を実施する。

5.2 クラウドサービス

(1) 目的・趣旨

クラウドサービスの利用においては、そのセキュリティ対策の直接的な確認が困難

なため、機密性３以上の情報を取り扱う場合、クラウドサービスの特性を理解し、クラウドサービス提供者へのガバナンスの有効性やセキュリティ確保のための事項を考慮する必要がある。よって、機関とクラウドサービス提供者間の役割と責任分担を明確にし、セキュリティ要件を満たすクラウドサービスの選定が求められる。

また、クラウドサービスを利用する際のセキュリティ対策は、情報システムのライフサイクル全般（情報システムの導入・構築、運用・保守、契約終了）において行う必要がある。クラウドサービスのサービス内容は非常に早いサイクルで変化しており、構築時には想定していなかった脅威や脆弱性が発生する可能性もあることから、情報セキュリティ対策の定期的な確認と見直しによりセキュリティ要件の追加及び修正を実施することが求められる。

さらに、クラウドサービスへのアクセス権限については、役職員等の業務やクラウドサービスの利用環境等の変化に応じて、定期的な確認による見直しをすることが重要である。

＜クラウドサービスの例＞

・仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
・データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
・ウェブ会議サービス
・ソーシャルメディア
・検索サービス、翻訳サービス、地図サービス

(2) 遵守事項

① クラウドサービスの選定

原則として、「政府情報システムのためのセキュリティ評価制度（ISMAP）」（内閣サイバーセキュリティセンター）に基づく「ISMAP等クラウドサービスリスト」に掲載されたサービスから調達を行う。ただし、「ISMAP等クラウドサービスリスト」以外のサービスを利用するときは、セキュリティリスクを明らかにし、必要な対策等を明示して、機関CISOの許可を得る。

② クラウドサービスの利用時・終了時における対策

クラウドサービスを活用するため、選定・利用のためのマニュアルを定めるとともに、必要な事項は、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013年度版」（経済産業省）を準用する。

なお、クラウドサービス終了時は、「5.1 業務委託」の遵守事項を準用する。

第６章　情報システム構成要素のセキュリティ対策

6.1 端末のセキュリティ対策

6.1.1 端末

(1) 目的・趣旨

業務用端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等に注意する必要がある。

また、役職員等の不適切な利用や過失等の内的要因による不正プログラム感染等のインシデントが発生するおそれがあることから、常にソフトウェアのアップデート、防御用のソフトウェアの導入等適切なセキュリティ対策を講ずるとともに、役職員等に利用を認めるソフトウェアや接続を認める機器等を定めておくことが重要である。

さらに、盗難・紛失等による情報漏えいを考慮した対策を講ずる。

(2) 遵守事項

端末の導入時の対策

① 役職員等は、あらかじめ情報システム管理者が接続を認めた機器等以外はネットワークに接続してはならない。

② 情報システム管理者は、端末ごとに必要なセキュリティ対策を実施する。

また、業務で利用するソフトウェアの脆弱性について情報収集し、対策を実施する。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 情報システム管理者は、多様なソフトウェアを利用することにより脆弱性が増大しないよう、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。

④ 役職員等は情報システム管理者が設定したセキュリティ対策ソフトを活用するとともに、機密性２以上の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脅威から保護するため物理的な対策を講ずる。

⑤ 情報システム管理者は、運用を終了した端末は、「情報資産廃棄ガイドライン」に基づき、速やかに電磁的記録媒体の全ての情報を抹消する。

6.1.2 テレワーク等での端末利用時の対策

(1) 目的・趣旨

テレワークの実施等において、役職員等が機関外で業務を行う場合は、盗み見や盗難・紛失などのリスクが増えることから、それに対抗するための措置を定めて周知する必要がある。特に端末の盗難、紛失、不正プログラムの感染等による情報窃取を防止するため技術的な措置が必要である。

また、役職員等が機構外のネットワークを用いて情報システムにリモートアクセス

をする場合は、リモートアクセス特有の攻撃等に対抗するためのセキュリティ対策を実施する必要がある。

(2) 遵守事項

① 情報セキュリティ責任者は、テレワーク等において業務端末を用いて機密性２以上の情報を取り扱う場合について、これらの端末や利用したネットワークから情報が漏えいするなどのリスクを踏まえた実施手順を定める。

② 情報セキュリティ管理者は、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必要な対策を行う。

6.1.3 機関支給以外の端末の導入及び利用時の対策

(1) 目的・趣旨

役職員等は、その業務の遂行にあたっては、機関から支給された端末を用いるのが原則である。しかしながら、出張等や危機事象発生時の際に、やむを得ず機関支給以外の端末を利用して業務を行う場合、当該端末の情報セキュリティ水準が対策基準を満たさないおそれがある。このため、当該端末の利用について、あらかじめ情報セキュリティ管理者の許可を得る必要がある。情報セキュリティ管理者は、当該端末の管理をその所有者が行うこととなり、機関において管理ができないことへのリスクを勘案し、その利用の可否を判断する必要がある。

(2) 遵守事項

機関支給以外の端末を利用する場合は、あらかじめ情報セキュリティ管理者の許可を得る。情報セキュリティ管理者は、許可する際には、当該端末の利用範囲とそのセキュリティ基準を達成できることを確認する。

6.1.4 アプリケーション・コンテンツの作成・運用時の対策

(1) 目的・趣旨

業務においては、情報の提供、諸手続等のサービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招かないよう、機関で情報セキュリティ対策を講じておく必要がある。

また、利用者に提供するサービス（クラウドサービスを含む。）は通常インターネットを介して利用するものであるため、特に機構外利用者にとっては、そのサービスが、機関が提供する正規のものであると確認できることが重要である。

さらに、アプリケーション・コンテンツの開発・提供を業務委託する場合については、「5.1 業務委託」を遵守する必要がある。

(2) 遵守事項

アプリケーション・コンテンツのセキュリティ

① 役職員等は、アプリケーション・コンテンツの開発・作成を自ら行うときは、情報システム管理者と調整し、情報セキュリティ水準の低下を招かぬよう措置する。外部に委託する際には、その内容をセキュリティ要件として調達仕様に含める。

② 情報システム管理者は、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。

③ 情報システム管理者は、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。

④ 情報システム管理者は、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。

⑤ 情報システム管理者は、機構外利用者向けに提供するウェブサイト等が機関提供のものであることを機構外利用者が確認できるように、機構や機関のドメイン名を使用する。

⑥ 情報システム管理者は、機構外利用者が検索サイト等を経由して機関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。

6.2 サーバ装置

(1) 目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置は、ネットワーク等を介して不正プログラム感染や不正侵入を受けるなどの可能性が極めて高い。

また、サーバ装置には大量の情報が保存され、同時に多くの者が利用することから、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

(2) 遵守事項

① サーバ装置の導入時の対策

(a) 情報システム管理者は、機密性２以上の情報を取り扱う物理的な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) 情報システム管理者は、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、可用性２以上の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) 情報システム管理者は、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。

(d) 情報システム管理者は、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。

(e) 情報システム管理者は、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。

(f) 情報システム管理者は、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。

(g) 情報システム管理者は、可用性２以上の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。

② サーバ装置の運用時の対策

(a) 情報システム管理者は、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。

(b) 情報システム管理者は、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) 情報システム管理者は、サーバ装置上での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。

(d) 情報システム管理者は、可用性２以上の情報を取り扱うサーバ装置について、「事業継続計画 (BCP)」における危機事象発生時に適切な対処が行えるよう運用をする。

③ サーバ装置の運用終了時の対策

情報システム管理者は、サーバ装置の運用を終了する際に、「情報資産廃棄ガイドライン」に基づき、サーバ装置の電磁的記録媒体の全ての情報を抹消する。

6.3 電子メール

(1) 目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する役職員等が巻き込まれるリスクもある。これらの問題を回避するためには、利用リスクを管理するとともに、適切な電子メールサーバの管理が必要である。

(2) 遵守事項

電子メールの対策

① 情報システム管理者は、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 情報システム管理者は、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認証を行う機能を備える。

③　情報システム管理者は、電子メールのなりすましの防止策ため、原則としてDMARC、DKIM及びSPFを導入する。ただし、機関CISOが認めた場合はこの限りでない。

④　情報システム管理者は、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。

6.4 ウェブサーバ

(1) 目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが必要である。

(2) 遵守事項

ウェブサーバのセキュリティ対策

①　情報システム管理者は、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こととし、多用途の利用は避ける。

②　情報システム管理者は、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　情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定する。

④　情報システム管理者は、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及び電子証明書による認証の対策を講じる。

6.5 ドメインネームシステム（DNS）

(1) 目的・趣旨

インターネット上のホスト名や電子メールで使われるドメイン名と、IPアドレスとの対応づけ（正引き、逆引き）を管理するために使用されているドメインネームシステム（DNS：Domain Name System）には、機関が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNSクライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。

また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等のDNSクライアントが悪意あるサーバに接続させられるなどの被害

に遭う可能性がある。

さらに、電子メールのなりすまし対策の一部はDNSで行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNSサーバの適切な管理が必要である。

(2) 遵守事項

DNSのセキュリティ対策

① 情報システム管理者は、重要な情報システムの安定運用を確保するため、情報システムの可用性に応じた適切な名前解決の冗長化措置を講ずる。特に外部公開される情報システムや業務継続に重要な役割を持つシステムについては、DNSサーバの冗長化、フェイルオーバー構成、キャッシュDNSの導入等により、名前解決の可用性を確保する。

② 情報システム管理者は、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 情報システム管理者は、コンテンツサーバにおいて、機関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。

④ 情報システム管理者は、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。

⑤ 情報システム管理者は、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。

⑥ 情報システム管理者は、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。

6.6 データベース

(1) 目的・趣旨

対策基準におけるデータベースとは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、機密性２以上の情報を保管するサーバ装置とする。

機密性２以上の情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び役職員等の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、そのようなデータは攻撃者の標的となりやすいことから注意する必要がある。

(2) 遵守事項

データベースのセキュリティ対策

① 情報システム管理者は、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 情報システム管理者は、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。

③ 情報システム管理者は、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 情報システム管理者は、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。

⑤ 情報システム管理者は、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。

6.7 複合機・特定用途機器

(1) 目的・趣旨

プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機は、機関内ネットワークや公衆電話網等のネットワークに接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、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用途機器は、インターネットに接続する機能を備える、いわゆるIoT機器となっている場合が多くある。例えばネットワークカメラシステムの構成要素である機器のうちインターネットに接続する機能を備えるカメラや、環境モニタリングシステムの構成要素である機器のうちインターネットに接続する機能を備えるセンサーが挙げられる。近年、IoT機器の脆弱性をついた攻撃が数多く発生しており、IoT機器が踏み台となって他の情報システムへの攻撃に利用されるなど、社会的問題となってきている。このため、これらの機器に対する情報セキュリティ対策が必要となる。

したがって、複合機やIoT機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講ずることが重要である。

(2) 遵守事項

① 複合機

(a) 情報システム管理者は、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け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) 情報システム管理者は、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インシデントへの対策を講ずる。

(c) 情報システム管理者は、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

情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、ネットワークへの接続形態等により脅威が存在する場合には、「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」（IPA）を参考に適切なセキュリティ基準を満たす製品を選定する等、当該機器の特性に応じた対策を講ずる。

また、必要に応じ、機関内での利用ガイドラインを策定し、リスクの高い機器については、ネットワーク分離やアクセス制御の強化を行うものとする。

6.8 ネットワーク

(1) 目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続されたネットワークを介して行われる場合がほとんどであることから、ネットワークに対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。ネットワークの運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムは時間経過とともに、利用条件の変化や攻撃手法の変化も想定されることから、継続的な情報セキュリティ対策を実施することが重要である。

(2) 遵守事項

① ネットワークの導入時の対策

(a) 情報システム管理者は、ネットワーク構築時に、当該ネットワークに接続する情報システムにて取り扱う情報の格付け及び取扱制限に応じた適切な回線種別を選択し、インシデントによる影響を回避するために、ネットワークに対して必要な対策を講ずる。

(b) 情報システム管理者は、ネットワークにおいて、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) 情報システム管理者は、機密性３以上の情報を取り扱う情報システムをネットワークに接続する際に、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) 情報システム管理者は、役職員等がネットワーク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。機関内ネットワークへ機関支給以外の端末を接続する際も同様と

する。

(e) 情報システム管理者は、可用性２以上の情報を取り扱う情報システムが接続されるネットワークについて、当該ネットワークの継続的な運用を可能とするための措置を講ずる。

② 機関外ネットワークの接続時の対策

(a) 情報システム管理者は、機関内ネットワークにインターネット回線、公衆ネットワーク等の機関外ネットワークを接続する場合には、機関内ネットワーク及び当該機関内ネットワーク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。

(b) 情報システム管理者は、機関内ネットワークと機関外ネットワークとの間及び機関内ネットワーク内の不正な通信の有無を監視するための措置を講ずる。

(c) 情報システム管理者は、保守又は診断のために、機関外ネットワークから機関内ネットワーク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。

(d) 情報システム管理者は、電気通信事業者のネットワークサービスを利用する場合には、当該ネットワーク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。

③ ネットワークの運用時の対策

(a) 情報システム管理者は、経路制御及びアクセス制御を適切に運用し、ネットワーク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。

(b) 情報システム管理者は、機関内ネットワークと機関外ネットワークとの間及び機関内ネットワーク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。

(c) 情報システム管理者は、保守又は診断のために、機関外ネットワークから機関内ネットワーク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。

(d) 情報システム管理者は、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ネットワークについて、共有先の他の情報システムを保護するため、当該ネットワークとは別に独立した閉鎖的なネットワークに構成を変更する。

6.9 ネットワーク装置

(1) 目的・趣旨

インターネット等の外部ネットワークからアクセス可能なネットワーク装置においては、ソフトウェアの脆弱性を悪用された不正アクセスの被害を受ける可能性があ

る。そのため、ネットワーク装置におけるソフトウェアの脆弱性対策は、迅速かつ適切に対処することが求められる。

また、ネットワーク装置は端末やサーバ装置などの経路制御やアクセス制御に用いるため、情報システムの構築時からリスクを十分検討し、必要なセキュリティ対策を実施しておく必要がある。

さらに、運用時においても、脅威動向の変化等に応じた継続的な対策を実施することが重要である。

(2) 遵守事項

① ネットワーク装置の導入時の対策

(a) 情報システム管理者は、物理的なネットワーク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。

(b) 情報システム管理者は、ネットワーク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。

(c) 情報システム管理者は、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、ネットワーク装置に対して適切なセキュリティ対策を実施する。

(d) 情報システム管理者は、ネットワーク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。

② ネットワーク装置の運用時の対策

(a) 情報システム管理者は、ネットワーク装置の運用・保守に関わる作業等によりネットワーク装置の設定変更等を実施する場合は、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。

(b) 情報システム管理者は、可用性２以上の情報を取り扱う情報システムを構成するネットワーク装置については、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。

(c) 情報システム管理者は、ネットワーク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。

③ ネットワーク装置の運用終了時の対策

情報システム管理者は、ネットワーク装置の運用を終了する場合には、当該ネットワークを構成するネットワーク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、当該ネットワーク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。

6.10 無線LAN

(1) 目的・趣旨

無線LANは、有線のネットワーク及びネットワーク装置において想定される脅威に加え、電波を利用するために有線と比較して通信の傍受等が容易であることに起因する脅威への対策が必要である。

(2) 遵守事項

① 無線LAN環境導入時の対策

情報システム管理者は、無線LAN技術を利用して機関内ネットワークを構築する場合は、ネットワーク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。その際、WPA3を必須とし、WPA2は例外的に許容する。WEPやWPA1は非推奨とする。IEEE 802.1X 認証を推奨し、PSK方式の使用は可能な限り制限する。

② 無線LAN環境の適切なアクセス制御とログ監視を実施する。

6.11 NAS

(1) 目的・趣旨

NAS（Network Attached Storage）は、組織内のデータ共有やデータバックアップに利用されるが、適切なアクセス制御や暗号化が施されていない場合、情報漏洩や不正アクセスのリスクが高まる。そのため、NASの導入・廃棄に関する基準を明確にすることが必要である。

(2) 遵守事項

① アクセス制御

(a) NASへのアクセスは認証機能を導入し、利用者ごとに権限を制限する。

(b) 最小限の原則を適用し、不要なアクセス権限を付与してはならない。

(c) 匿名アクセスをしてはならない。

(d) 退職者、異動者が発生した場合は速やかにこれに対応する。

② データの暗号化

(a) 機密性２以上の情報を保存するNASはデータ暗号化を必須とする。

(b) NASの通信経路はTLS1.2以上の暗号化プロトコルを使用する。

(c) 暗号鍵の管理は、情報システム管理者が責任をもち、安全なストレージを利用する。

③ ログ管理

(a) NASのアクセスログ（認証・変更）を取得し、１年以上保管する。

(b) 改ざん防止措置を講じ、ログの適切な監視を行う。

(c) 異常なアクセスや不正アクセスの兆候が検知された場合は、機関統一窓口を通

じて機関CSIRTに報告する。

④ バックアップの保全

NASは定期的にバックアップを取得し、リストア可能な状態を維持する。

⑤ 廃棄時の対応

(a) NASを廃棄する際は、記録媒体のデータを完全消去又は物理破壊する。

(b) データの完全削除を行った証明（消去ログ・破壊証明書等）を取得し、一定期間保管する。

⑥ ファームウェア・セキュリティ更新

(a) NASのファームウェアを定期的に更新し、既知の脆弱性を修正する。

(b) 不要なサービスは無効化し、セキュリティリスクを最小限に抑える。

6.12 IPv6ネットワーク

(1) 目的・趣旨

近年では、サーバ装置、端末及びネットワーク装置等にIPv6技術を利用する通信（以下「IPv6通信」という。）を行う機能が標準で備わっているものが多く出荷されている。IPv6通信プロトコルでは、グローバルIPアドレスによるパケットの直接到達性などを考慮する必要があり、設定不備によっては運用者が意図しないIPv6通信が通信ネットワーク上で動作し、結果として、不正アクセスの手口として悪用されるおそれもある。このため、必要な対策を講じていく必要がある。

(2) 遵守事項

① IPv6通信を行う情報システムに係る対策

(a) 情報システム管理者は、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) 情報システム管理者は、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。

② 意図しないIPv6通信の抑止・監視

情報システム管理者は、サーバ装置、端末及びネットワーク装置を、IPv6通信を想定していないネットワーク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、当該ネットワークから受ける不正な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。

6.13 情報システムの基盤を管理又は制御するソフトウェア

(1) 目的・趣旨

情報システムの基盤を管理又は制御するソフトウェアは、情報システムを制御する上でセキュリティ上の重要な機能を有している。そのようなソフトウェアは悪用や不正アクセスされた場合、被害が広範囲に及ぶ可能性がある。したがって、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利用する端末やサーバ装置、ネットワーク装置等及びソフトウェア自体において、必要なセキュリティ対策を実施する必要がある。

また、当該ソフトウェアを利用する際の操作ミスや設定不備などを防ぐためには、当該ソフトウェアの利用者や管理者が利用するソフトウェアを利用するための手順を整備することも重要である。

さらに、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悪用した攻撃を防ぐにはソフトウェアの脆弱性対策が特に重要となる。当該ソフトウェアに関係する脆弱性に関する情報を製品ベンダや脆弱性情報提供サイト等からの通知を受け取るようにするとともに、公開された脆弱性についての影響度と緊急度に応じてセキュリティパッチ等を適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。

(2) 遵守事項

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及び運用時の対策

① 情報システム管理者は、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、ネットワーク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 情報システム管理者は、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。

(a) 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

(b) 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インシデントを認知した際の対処手順

③ 情報システム管理者は、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。

(a) 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

(b) 脅威やインシデントを迅速に検知し、対応するための対策

第７章　情報システムのセキュリティ要件

7.1 情報システムのセキュリティ機能

7.1.1 認証機能

(1) 目的・趣旨

情報又は情報システムへのアクセスを制御するためには、認証機能の導入が必要である。その際、なりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、機関等の情報システムにおいて、役職員以外にサービスを提供する場合は、利用者が情報システムへのアクセスの主体となることにも留意して、認証情報を適切に保護しなければならない。

(2) 遵守事項

① 認証機能の導入

(a) 情報システム管理者は、情報システムや情報へのアクセスを特定し、それが正当であることを検証する必要がある場合、その識別及び認証を行う機能を設ける。

(b) 情報システム管理者は、外部からの申請、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、認証に係る要件を策定する。

(c) 情報システム管理者は、認証を行う場合、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（ログインID）及び認証情報（パスワードなど）の管理

(a) 情報システム管理者は、情報システムへのアクセスに対して、識別コード及び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) 情報システム管理者は、役職員等が退職するなど、情報システムを利用する必要がなくなった場合は、当該役職員等の識別コード及び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。

7.1.2 アクセス制御機能

(1) 目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

(2) 遵守事項

アクセス制御機能の導入

① 情報システム管理者は、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け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 情報システム管理者は、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。

7.1.3 アクセス権限の管理

(1) 目的・趣旨

情報システムのアクセス制御機能を適切に運用するためには、主体毎に最小限の権限を設定し、付与することとし、不必要な権限を与えないことが重要である。

また、情報に対して権限を付与する場合も同様に、知る必要のある主体に対してのみ権限を付与とすることが重要である。なお、権限の管理が不適切になると、情報又は情報システムへ不正アクセスや情報漏洩のリスクを高める。特に管理者権限は特権を持つため、悪意ある第三者等に奪取されると情報等の漏えい、改ざんや不正プログラムによって業務継続が生じる可能性も生じる。

また、これらの不正アクセスや不正プログラム等を検知又は防止するための設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

(2) 遵守事項

権限の管理

① 情報システム管理者は、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 情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び認証情報が、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 情報システム管理者は、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。

7.1.4 ログの取得・管理

(1) 目的・趣旨

情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等のインシデント及びその予兆を検知するための重要な材料となるものである。

また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ロ

グは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、さらには改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

(2) 遵守事項

ログの取得・管理

① 情報システム管理者は、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。

② 情報システム管理者は、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、ログの保存期間を次のとおりとする。

(a) ゲートウェイ（対外接続部）のログ：原則２年間以上

(b) 重要なサーバのログ（関係するものを含む。）：１年間以上

(c) 機密性３以上の情報を保存する端末のアクセスログ：１年間以上

(d) その他の機器のログ：原則30日以上とし、必要に応じて機関CISOが別途定めることができる。

(e) 取得したログは、以下の要件を満たすものとする。

ア 外部電磁的記録媒体に保存する場合は、完全性を担保する。

イ 誰が（又はどの端末が）、いつ、どの情報資産にアクセスしたかを追跡可能な項目とする。

ウ 情報システム管理者は、ログ取得不能時の対応やその他必要な事項についてマニュアル等を作成する。

7.1.5 暗号・電子署名

(1) 目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズム及び鍵長に加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズム又は鍵長が危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

(2) 遵守事項

① 暗号化機能・電子署名機能の導入

(a) 情報システム管理者は、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、以下の全ての措置を講ずる。

ア　機密性３以上の情報を取り扱う情報システムについては、原則として暗号化機能を設ける。

イ　完全性２以上の情報を取り扱う情報システムについては、必要に応じて電子署名の付与及び検証を行う機能を設ける。

(b) 情報システム管理者は、原則として、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及び電子署名のアルゴリズム及び鍵長並びに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実施手順を定める。

(c) 情報システム管理者は、機関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。

② 暗号化・電子署名に係る管理

情報システム管理者は、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。

(a) 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。

(b) 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、役職員等と共有を図る。

7.1.6 監視機能

(1) 目的・趣旨

情報システムにおけるインシデントや不正利用等の速やかな認知や、情報セキュリティ対策の実効性を確認するためには、適切に監視機能を実装し、運用することが重要である。

また、監視機能の実装に当たっては、情報システムの特性や当該情報システムで取り扱う情報の格付け等を踏まえて、監視対象や監視内容を定める必要がある。

(2) 遵守事項

監視機能の導入・運用

① 情報システム管理者は、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、監視機能を実装し、適切に運用する。

② 情報システム管理者は、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。

7.2 情報セキュリティの脅威への対策

7.2.1 ソフトウェアに関する脆弱性対策

(1) 目的・趣旨

機関の情報システムに対する脅威としては、第三者が情報システムに侵入し機関の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に個人情報等の重要な情報の漏えい等が発生した場合、社会に多大な影響を及ぼすとともに、信用が失われる。

このような攻撃では、情報システムを構成するサーバ装置、端末及びネットワーク装置のソフトウェアの脆弱性を悪用されることが多い。したがって、機関の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

(2) 遵守事項

ソフトウェアに関する脆弱性対策の実施

① 情報システム管理者は、サーバ装置、端末及びネットワーク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 情報システム管理者は、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、端末及びネットワーク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 情報システム管理者は、サーバ装置、端末及びネットワーク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 情報システム管理者は、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、端末及びネットワーク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。

7.2.2 不正プログラム対策

(1) 目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を

及ぼすおそれがある。

このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

(2) 遵守事項

不正プログラム対策の実施

① 情報システム管理者は、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 情報システム管理者は、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 情報システム管理者は、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。

7.2.3 サービス不能攻撃対策

(1) 目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能とする攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、機関の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。近年ではインターネットに接続されたいわゆるIoT機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできるDDoS対策代行サービスの活用等を検討する。

(2) 遵守事項

サービス不能攻撃対策の実施

① 情報システム管理者は、可用性３の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、端末及びネットワーク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 情報システム管理者は、可用性３の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 情報システム管理者は、可用性３の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、ネットワーク装置又はネットワークから監視対象を特定し、監視する。

7.2.4 標的型攻撃対策

(1) 目的・趣旨

標的型攻撃は、特定の組織に狙いを絞り、入念な調査を行った上で、その組織に最適な手法で執拗に行われる攻撃であり、不正侵入や情報奪取等が主な目的である。未知の手段を用いることもあり、完全に検知及び防御することは困難との前提に立ち、入口、組織内部、出口の各段階で多重防御の情報セキュリティ対策を講じる必要がある。

また、関連組織を狙った間接的な攻撃も確認されており、広範な対策が必要である。

(2) 遵守事項

標的型攻撃対策の実施

① 情報システム管理者は、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 情報システム管理者は、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。

7.3 ゼロトラストアーキテクチャ

7.3.1 動的なアクセス制御の実装時の対策

(1) 目的・趣旨

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の機関外ネットワークと組織内ネットワークである機関内ネットワークとの境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であるが、クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信し、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される。）への情報セキュリティ対策が不足していないか適宜確認する必要がある。

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方であり、積極的に推進する。

ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体、アクセス元やアクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。

(2) 遵守事項

① 動的なアクセス制御における責任者の設置

機関CISO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、情報システム管理者を選任する。

② 動的なアクセス制御の導入方針の検討

情報システム管理者は、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。

③ 動的なアクセス制御の実装時の対策

(a) 情報システム管理者は、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。

(b) 情報システム管理者は、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。その際、都度認証（リアルタイム認証）又は定期的な再認証とし、動的なリスク評価を実施する。

さらに、利用デバイスのコンプライアンスチェック（デバイス証明書、脆弱性診断）を組み込む。機密性の高いリソースへは、アクセスリスクに応じた多要素認証を適用する。

7.3.2 動的なアクセス制御の運用時の対策

(1) 目的・趣旨

テレワークの拡大やクラウド・バイ・デフォルト原則によって、リソースの利用形態は日々変化していることを踏まえ、動的なアクセス制御の運用時には、実装時に検討した対策内容が正しく機能しているかどうか確認し、必要に応じてアクセス制御ポリシーを見直すことが重要である。

また、動的なアクセス制御の前提となるリソースの信用情報を収集する中でリスクが検出された場合は、当該リスクを低減するための措置が必要となる。

(2) 遵守事項

① 動的なアクセス制御の実装方針の見直し

情報システム管理者は、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。

② 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

情報システム管理者は、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。

【別表】3.1(2)④(b) 機密性２以上の情報の送信・共有

		機関内	機構内(機関間)	機構外(大学、企業、個人等)
機密性1	メール送信	可	可	可
	クラウドファイル共有	**可**	**可**	**可**
	ファイル転送アプリ	可	可	可
機密性2	メール送信	可(要暗号化)	可(要暗号化)	可(要暗号化)
	クラウドファイル共有※	**可**	**可**	可
	ファイル転送アプリ	可(要暗号化)	可(要暗号化)	可(要暗号化)
機密性3	メール送信	不可	不可	不可
	クラウドファイル共有※	**可**	**可**	可
	ファイル転送アプリ	不可(そもそもクラウド※利用が前提)	機関CISO許可により可(要暗号化)	機関CISO許可により可(要暗号化)
機密性4	メール送信	原則禁止 (「情報セキュリティ対策に関する基本規程」別表第1(情報の分類・格付けと取扱制限)に「機関CISOの許可がある場合を除き」と例外規定あり。)		
	クラウドファイル共有			
	ファイル転送アプリ			
	クラウドファイル共有※：Microsoft365及びGooglework spaceのコアサービスに限る。			

【別紙】用語の定義

対策基準における用語の定義は、下記に定めるところによる。
なお、基本規程と解釈に齟齬があるときは、基本規程を優先する。

【あ】

- 「アプリケーション・コンテンツ」とは、機関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。

【か】

- 「関係規程等」とは、基本規程、対策基準、マニュアル等を総称したものをいう。
- 「機関」とは、基本規程別表第２に掲げる機関等をいう。
- 「機関外ネットワーク」とは、ネットワークのうち、機関内ネットワーク以外のものをいう。
- 「機関内ネットワーク」とは、一つの機関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ネットワークであって、当該機関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。機関内ネットワークには、専用線やVPN等物理的な回線を機関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、ネットワーク装置、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。
- 「基本規程」とは、対策基準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運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。
- 「業務委託」とは、機関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の情報を取り扱わせる場合に限る。
- 「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。クラウドサービスの例としては、SaaS（Software as a Service)、PaaS（Platform as a Service)、IaaS（Infrastructure as a Service）等がある。なお、対策基準におけるクラウドサービスは、機関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関の情報が取り扱われる場合に限るものとする。
- 「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。

【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、ネットワーク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、機関が調達又は開発するものをいう。

  また、物理的なハードウェアを有するサーバ装置を「物理的なサーバ装置」という。
- 「サイバーセキュリティ等基本計画」とは、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。
- 「CSIRT(シーサート)」とは、機関において発生したインシデントに対処するため、当該機関に設置された体制をいう。Computer Security Incident Response Teamの略。
- 「実施手順」とは、対策基準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や手続をいう。
- 「情報」とは、対策基準の「1.2 対策基準の適用対象」の(2)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、機関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 27000:2019における情報セキュリティインシデントをいう。
- 「情報セキュリティ対策基準」とは、機関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。
- 「情報セキュリティ対策推進体制」とは、機関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、当該機関に設置された体制をいう。

【た】

- 「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、機関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、機関が調達又は開発するもの以外を指す「機関支給以外の端末」がある。

  また、機関が調達又は開発した端末と機関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。

  さらに、物理的なハードウェアを有する端末を「物理的な端末」という。
- 「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、ネットワークに接続する

機能を備え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。

【ま】

・「明示等」とは、情報を取り扱う全ての者が当該情報の格付けについて共通の認識となるようにする措置をいう。明示等には、情報ごとに格付けを記載することによる明示のほか、当該情報の格付け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、その格付け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。

【や】

・「役職員等」とは、役員、機構と直接雇用関係にある者、共同研究・受託研究により機構の施設で業務を行っている者、機構において研究・研修を行う学生等をいう（一時的来訪者、警備・清掃等の業務委託でネットワークを利用しない者を除く。）。
・「要管理対策区域」とは、機関の管理下にある区域（機関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。