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

平成２８年９月２３日
一部改正　平成２８年１２月２２日
一部改正　平成３０年３月１日
一部改正　平成３０年１１月１日
一部改正　平成３１年３月２７日
一部改正　令和元年７月２５日
一部改正　令和元年９月１０日
一部改正　令和元年１２月１日
一部改正　令和２年７月９日
一部改正　令和２年１２月４日
一部改正　令和３年６月２４日
一部改正　令和４年５月３０日
一部改正　令和４年１１月２４日
一部改正　令和５年４月１日
最高情報セキュリティ責任者決定

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，以下のとおり対策基準を定める。

なお，本対策基準の用語は，基本規程第３条各号に掲げるもののほか，本対策基準「1.3 用語定義」に規定するものとする。

目次

1. 対象範囲

本対策基準が対象とする情報資産は，基本規程第４条に規定する情報資産とする。

1.1. 基本規程第４条第１項ただし書きに規定する CISO が対策基準で定めるもの

基本規程第４条第１項ただし書きに規定する CISO が対策基準で定めるものは，以下のとおりとする。

(1) 外来者，宿泊施設における宿泊者等に対して，機構がインターネットアクセスを提供することを目的として，機構のネットワークから物理的又は論理的に隔離するとともに，機構が管理するグローバル IP アドレスを利用することなく，ネットワークやインターネットに接続するように構成された LAN の使用。ただし，当該 LAN を設置した情報システム管理者は，使用者に対して，当該 LAN を使用したことによって生じたいかなる損害についても機構は責任を負わない旨を明示しなければならない。

(2) 大学共同利用機関法人自然科学研究機構固定資産等貸付要領に基づきネットワーク，情報システム，情報施設・設備及び電磁的記録媒体の貸付を行う場合において，次のいずれかに該当する場合。ただし，機密性２以上に格付けされている情報資産については，貸付の際に原則として「情報資産廃棄ガイドライン」の「２）論理的破壊（データ破壊）」又は「３）論理的破壊（暗号化キーの廃棄）」を実施したうえで貸し出すものとし，返却時には借主にこれに準じる形で論理的破壊を行ったうえで返却させるとともに，借主の論理的破壊の不備による情報漏洩を考慮して，返却後の当該情報資産から借主に係る情報の漏洩が発生しても借主の責に帰すことを契約書等に明記すること。

① 法人に貸付を行う場合において，借主が適用となるセキュリティポリシーを示す場合。ただし，この場合においては貸付契約書等に適用となる当該法人のセキュリティポリシーを明記するなど，齟齬が生じないようにすること。

(3) 役職員以外の者へのサービスの提供等

役職員以外の者に対して，機関 CISO 若しくは情報システム管理者及び情報セキュリティ管理者が認めた範囲における，次のいずれかに掲げるサービスの提供等。ただし，適用は役職員以外の者に限る。

① 機密性１の情報へのアクセス

② 機密性２以上の情報を含まないネットワーク（論理分離を含む），情報システム及び電磁的記録媒体の利用

③ 役職員以外の者からの情報収集等を目的とした情報システムの利用（情報の入力及びファイルのアップロードにかかるものに限る）

1.2. 対応規定

本基準で定める文言への対応要件は，各項目において別途付記がある場合を除き，原則として以下のとおりとする。

(1) 必須という意

「しなければならない」,「ものとする」という用語は，その項目が絶対要件であることを意味する。一方,「してはならない」という用語は，その項目が禁止事項であることを意味する。

(2) 任意である意

「できる」という用語は，その項目が任意の要件であることを意味する。

(3) 即時に対応する意

「即時に」,「直ちに」という用語は，事象把握時から，可能な限り即時にということを意味する。「速やかに」という用語は，数時間以内で可能な限り早くということを意味する。

(4) 滞りなく対応する意

「遅滞なく」という用語は，数日以内ということを意味する。

1.3. 用語定義

(1) サーバ　ネットワークで, 他のコンピュータ等からの要求や指示を受け, 情報や処理結果を返す役割を持つコンピュータ（電子メールサーバ，ウェブサーバ，コンテンツサーバ，DNS サーバ，ファイルサーバ，データベースサーバ，認証サーバ，メインフレーム，Proxy サーバ，ネットワークアクセスサーバなど）をいう。

(2) 端末　デスクトップ PC，ノート PC，スマートフォン，タブレット端末，及びこれに類するものをいう。

(3) モバイル端末　移動させて使用することを目的とした端末（ノート PC，スマートフォン，タブレット端末等）をいう。（ネジ止めする等，固定して使用するものは含まれない。）

(4) 機器等　情報システムから外部サービスを除いたものをいう。

(5) 通信回線装置　DCE（モデム，TA，DSU，ONU 等），中継装置（ハブ，スイッチ，ルータ等），侵入検知・防御装置（IDS，IPS，UTM，FW，WAF 等）及びこれに類するものをいう。

(6) 特定用途機器　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, 入退館システム，センサー等の特定の用途に使用される情報システム特有の構成要素であって，通信回線に接続されている，又は内蔵電磁的記録媒体を備えているもの及びその他の IOT 機器をいう。

(7) 外部電磁的記録媒体　外付け又は取り外しを前提とした電磁的記録媒体（HDD，フラッシュメモリ（SSD，USB メモリ，SD カード等），光学メディア（Blu-ray，DVD，

CD 等)，磁気メディア（LTO 等))，その他内臓メモリを有す IC レコーダなどをいう。

(8) セキュリティトークン　情報システムにおける認証に用いられる物理デバイス（スマートカード，USB トークン，非接触型トークン等）をいう。

(9) 暗号化消去　本対策基準の情報資産廃棄ガイドラインにおける「論理的破壊（暗号化キーの廃棄)」に同じ。

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

(11) クラウドサービス　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 DaaS（Desktop as a Service)， SaaS（Software as a Service)，PaaS（Platform as a Service)，IaaS（Infrastructure as a Service）等をいう。

(12) 外部サービス　自然科学研究機構外の者が一般向けに情報システムの一部又は全部の機能を提供するもの（クラウドサービス，検索サービス，翻訳サービス，地図サービス，ソーシャルメディアサービス，インターネット回線接続サービス，ホスティングサービス，リモートデスクトップサービス等）をいう。ただし，当該サービスにおいて自然科学研究機構の情報が取り扱われる場合に限る。

(13) 外部サービス管理者　外部サービスの管理者として機関 CISO から指名された当該外部サービスに係る管理を行う情報システム管理者をいう。

(14) 外部サービス提供者　外部サービスを提供する事業者をいう。外部サービスを利用して自然科学研究機構に向けて独自のサービスを提供する事業者は含まれない。

(15) 外部サービス利用者　外部サービスを利用する自然科学研究機構の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

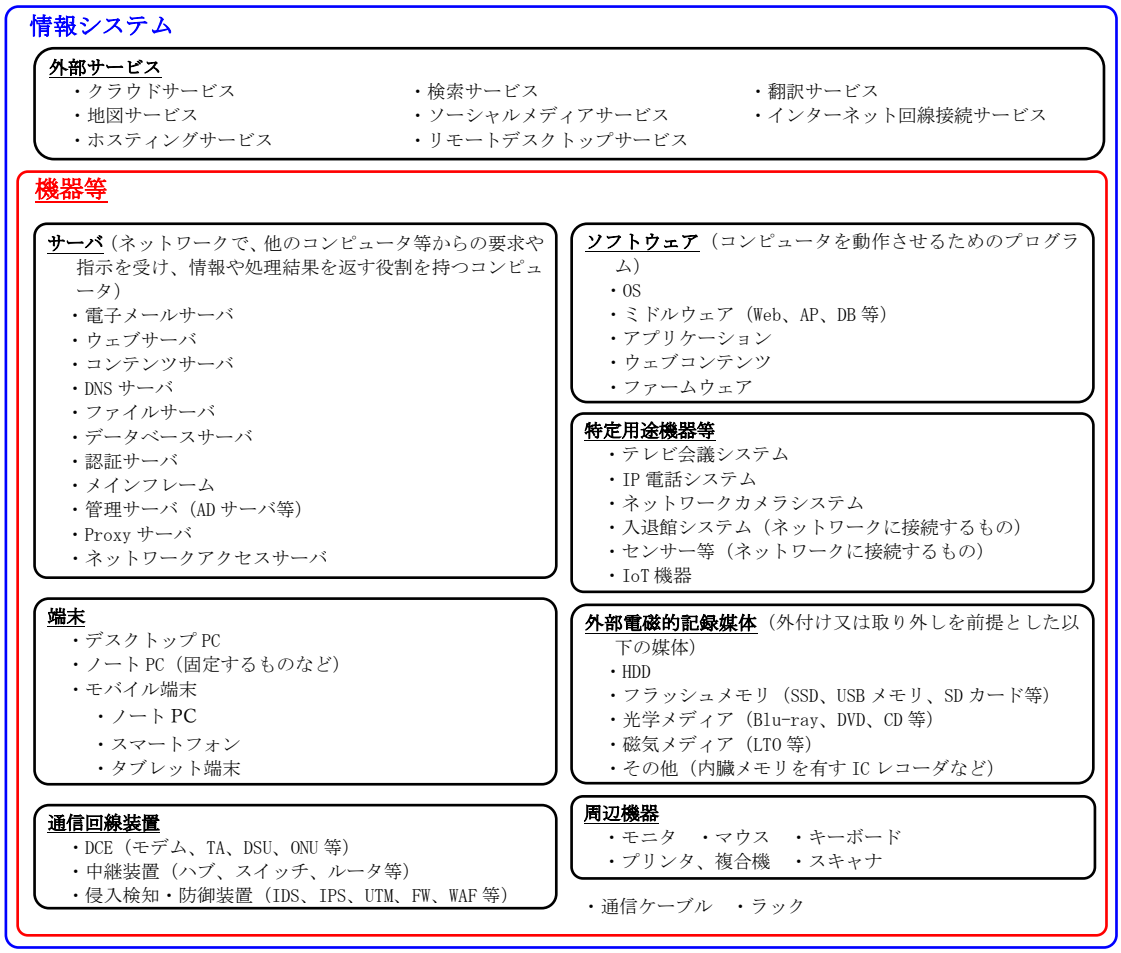
(16) 業務委託　自然科学研究機構の業務の一部又は全部について，契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず，全て含むものとする。ただし，当該業務において自然科学研究機構の情報を取り扱わせる場合に限る。

(17) 情報の抹消　情報資産廃棄ガイドラインに基づき，電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は，復元が困難な状態とはいえず，情報の抹消には該当しない。

(18) テレワーク　情報通信技術（ICT＝Information and Communication Technology）を

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

1.4. 情報システム等の概念図



1.5. 役職員等及び共同利用・共同研究者等が注意すべき情報セキュリティに関する基本的事項

役職員等及び共同利用・共同研究者等は，本対策基準に記載の無い事項や，疑義が生じた場合は，情報セキュリティ管理者又は情報システム管理者に確認したうえで業務を遂行しなければならない。

情報セキュリティ管理者及び情報システム管理者は，本対策基準に記載の無い事項や，疑義が生じた場合は，情報セキュリティの基本に立ち返り，次の事項を確認したうえで，必要に応じて情報セキュリティ責任者に相談するなど，適切に対応しなければならない。

① 基本規程第３条第８号に掲げる情報セキュリティ（機密性，完全性及び可用性を維持すること）が確保されていること。

② 機密性，完全性及び可用性の格付け等を考慮し，必要な「真正性」,「責任追跡性」,「否認防止」,「信頼性」が確保されていること。
③ 悪用防止が措置されていること。

2. 組織体制・職務・職責

(1) 最高情報セキュリティ責任者（基本規程第５条）

① 最高情報セキュリティ責任者（CISO: Chief Information Security Officer, 以下「CISO」という。）は，自然科学研究機構（以下「機構」という。）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。
② 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。
③ CISO は，情報セキュリティインシデントを認知した場合には，その重要度や影響範囲等を勘案し，総務，個人情報保護及び広報の各担当理事（当該担当として機構長が副機構長を指名した場合は当該副機構長をいう。以下同じ。）と連携して文部科学省，総務省等の所轄省庁及び報道機関への通知・公表対応を即時に行わなければならない。
④ 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ことができる。（基本規程第１０条）情報セキュリティアドバイザーは, CISO に対して情報セキュリティに関する助言（情報システムに関する技術的事項，情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言）・支援等を行うものとする。
⑤ CISO は，全体方針，個別取組，工程表からなる複数年を見通した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。）案を策定するものとし，役員会の審議に付すものとする。
⑥ 基本計画の策定に当たっては, 機構を取り巻く脅威及び内在する脆弱性等を洗い出し，情報セキュリティリスクを分析・評価した上で決定しなければならない。
⑦ 決定した基本計画は，CISO がその進捗状況を把握するとともに，総務担当理事，財務担当理事及び事務局における当該担当課長と情報共有し，機構における情報セキュリティ対策の強化を進めるものとする。
⑧ CISO は，必要がある場合は，代理者を指名することができる。この場合，CISO は機関最高情報セキュリティ責任者に対して，代理者の氏名，代理期間，連絡先を通知しなければならない。

(2) 機関最高情報セキュリティ責任者（基本規程第６条）

① 機関最高情報セキュリティ責任者（以下「機関 CISO」という。）は，CISO を補佐しなければならない。
② 機関 CISO は，基本規程別表第２に規定する所掌する機関等（以下「所掌機関等」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。

③ 機関 CISO は，所掌機関等において，情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には，CISO 及び統括情報セキュリティ責任者へ速やかに（深刻な場合（その可能性がある場合を含む。）には直ちに）報告を行わなければならない。

④ 機関 CISO は，必要がある場合は，代理者を指名することができる。この場合，機関 CISO は CISO，2.(3)に定める統括情報セキュリティ責任者及び所掌機関等における関係者に対して，代理者の氏名，代理期間，連絡先を通知しなければならない。

⑤ 機関 CISO は，指名責任を負うことに注意して情報セキュリティポリシーに基づき指名する。特に情報システム管理者の指名にあたっては，その資質が情報セキュリティインシデントに直結することを考慮して指名しなければならない。

⑥ 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場合において，当該情報システム管理者に重要なサーバ（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。なお，重要サーバ管理資格確認者が条件付きで認めた場合は，当該条件付きで指名をすることができる。

⑦ 前項における条件には，情報システム管理者配下の情報システム担当者の資質を含めて認めることを含む。ただし，当該情報システム担当者の退職や異動により条件が変った場合は，情報システム管理者は機関 CISO に連絡のうえ，改めて前項の資質確認を受けなければならない。

⑧ ⑥により指名された情報システム管理者（以下「重要サーバ管理者」という。）以外の情報システム管理者に重要なサーバを管理させようとする場合については，前項を準用する。

⑨ 機関 CISO は，必要により随時に，重要サーバ管理資格確認者に重要サーバ管理者の資質を確認させ，必要に応じて条件付与，指名取消等の措置を講じることができる。

⑩ 機関 CISO は，重要サーバ管理者から重要なサーバにインストールするソフトウェアについて申請があった場合は，これを審査したうえで許可を与えるものとする。また，許可の際には必要に応じて取るべき対策を明示しなければならない。

⑪ 機関 CISO は，必要に応じて，前項における審査を委任することができる。

⑫ 機関 CISO は，重要サーバ管理者が所掌する重要なサーバを後任へ引継ぐにあたり実施する事項についてのガイドライン（以下「重要サーバ引継ガイドライン」という。）を整備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）

① CISO 直属の情報セキュリティ責任者として事務局の情報セキュリティ責任者をもっ

て充て，統括情報セキュリティ責任者と位置付ける。

② 統括情報セキュリティ責任者は CISO を補佐しなければならない。

③ 統括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，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 統括情報セキュリティ責任者は，緊急時には CISO に直ちに報告を行わなければならない。

⑤ 統括情報セキュリティ責任者は，必要がある場合は，代理者を指名することができる。この場合，統括情報セキュリティ責任者は CISO 及び機関 CISO に対して，代理者の氏名，代理期間，連絡先を通知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）

① 情報セキュリティ責任者は機関 CISO を補佐しなければならない。

② 情報セキュリティ責任者は，所掌機関等のネットワーク及び情報システムにおける開発，設定の変更，運用，見直し等に関して，また，その他情報資産の管理等に関して，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。

③ 情報セキュリティ責任者は，所掌機関等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指示を行う権限及び責任を有する。

④ 情報セキュリティ責任者は，所掌機関等における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，情報セキュリティに関する指導及び助言を行う権限を有する。

⑤ 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。

⑥ 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（以下「機関緊急連絡網」という。）を整備しなければならない。

⑦ 機関緊急連絡網は，年１回以上の見直しを行うとともに，変更が生じた場合には，機関 CISO 及び統括情報セキュリティ責任者にこれを提出するものとする。

⑧ 情報セキュリティ責任者は，所掌機関等において所有している情報システムについて，緊急時等における連絡体制の整備，情報セキュリティポリシーの遵守に関する意見の集約及び役職員等及び共同利用・共同研究者等に対する教育，訓練，助言及び指示を行う。

⑨ 情報セキュリティ責任者は，必要がある場合は，代理者を指名することができる。こ

の場合，情報セキュリティ責任者は所掌機関等における機関 CISO 及び関係者に対して，代理者の氏名，代理期間，連絡先を通知しなければならない。

⑩ 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。

⑪ 情報セキュリティ責任者は，所掌機関等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。）並びに所掌機関等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。

⑫ 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。

⑬ 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）

① 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。

② 情報セキュリティ責任者は，①に規定する機関 CISO への要請を行なおうとする場合は，副情報セキュリティ責任者の任命期間，及び自身の所掌機関等において分掌させる範囲を，明示しなければならない。

③ ①に規定する任命期間は，最長で２年間とし再任を妨げない。また，副情報セキュリティ責任者が機構の職員としての資格を喪失した場合は，当該日の前日をもって任命期間を満了するものとする。

④ 副情報セキュリティ責任者は，指定された所掌範囲及び任命期間における情報セキュリティ責任者としての職権と職責を有し，情報セキュリティ責任者はこれを失うものとする。

⑤ 機関 CISO は，副情報セキュリティ責任者を置いた場合は，直ちに CISO，統括情報セキュリティ責任者及び関係者に対して，副情報セキュリティ責任者の氏名，連絡先を通知しなければならない。

⑥ 情報セキュリティ責任者は，副情報セキュリティ責任者を統括するものとする。

⑦ ①の要請は，副情報セキュリティ責任者がこれを行うことはできない。また，機関 CISO は，所掌範囲に副情報セキュリティ責任者を重複して指名することはできない。

(6) CSIRT（基本規程第１２条）

① CSIRT は，機構におけるインシデントマネジメントの中核を担う組織であり，コンピュータセキュリティインシデント（情報システムの運用におけるセキュリティ上の問題として捉えられる事象をいい，NIST（National Institute of Standards and

Technology）の定義に同じ。）に対応するものとする。

② 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。

③ 機関 CSIRT は，コンピュータセキュリティ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助言の要請があった場合は,これに応じなければならない。

④ 機関 CSIRT は，インシデント発生（発生する恐れの場合を含む。）の際には，当該インシデントに関して自らの属する機関 CISO の権限を行使することができるとともに,被害や攻撃の防止を目的として，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ものとする。

⑤ 機関 CSIRT にチームリーダーを置き，機関 CISO が指名する者をもって充てる。

⑥ チームリーダーは，機関 CSIRT の対応等に関し，総括及び調整等を行う。

⑦ CSIRT に統括チームリーダーを置き,基本規程別表第２に規定する事務局等のチームリーダーをもって充てる。

⑧ チームリーダーは，機関 CSIRT として情報セキュリティ上必要と認める場合は，役員及びその所掌における大学共同利用機関法人自然科学研究機構組織運営通則（平成１６年通則第１号。以下「組織運営通則」という。）第６条第１項第１号に規定する機関の長，第１７条第３項に規定する局長，第２条の２第１項に規定する機構直轄の研究施設の長に対して，意見を具申することができる。ただし，役員へ意見を具申する場合は，統括チームリーダーと調整しなければならない。

⑨ 機関 CSIRT は，特に重要と認める重要なサーバについては全て，その他の重要なサーバについては不作為抽出等により検査対象を定め，定期的に当該サーバの設定等を確認し，問題が見受けられる場合は，当該サーバの重要サーバ管理者に是正等の指示を行うとともに，機関 CISO へ報告しなければならない。

⑩ 機関 CSIRT は，そのチームリーダーが所掌機関等における重要サーバ管理者の資質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 に再確認を要求することができる。

⑪ 統括チームリーダーは，コンピュータセキュリティインシデントの内容を勘案し，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（以下「組織外 CSIRT 等」という。）に連絡することが妥当と認められる場合は，CISO 及びコンピュータセキュリティインシデントを起した機関 CISO の了承を得てこれを行うものとする。

⑫ 統括チームリーダーは必要に応じて，コンピュータセキュリティインシデントを起した機関 CSIRT のチームリーダーに⑧に掲げる組織外 CSIRT 等への連絡を依頼するこ

とができる。

⑬ 統括チームリーダーは，機関 CSIRT 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を取り纏め，CSIO 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）

① 情報セキュリティ管理者はその所掌する課室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。

② 情報セキュリティ管理者は，所掌取扱情報に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には，2.(13)②に規定する「機関統一窓口」へすみやかに報告を行い，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。

③ 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，当該取扱部署における当該情報の取扱上の注意点等をまとめた「取扱手順書」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）

① 情報システム管理者は，所掌するネットワーク（基本規程第３条第１号），情報システム（基本規程第３条第２号），情報施設・設備（基本規程第３条第３号），電磁的記録媒体（基本規程第３条第４号）及びシステム関連文書（基本規程第３条第６号）（以下「所掌情報システム等」という。）の管理，開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

② 情報システム管理者は，所掌情報システム等における情報セキュリティに関する権限及び責任を有する。

③ 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。

④ 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。

⑤ 情報システム管理者は，所掌する外部電磁的記録媒体に係る外部電磁的記録媒体管理台帳を整備しなければならない。

⑥ 情報システム管理者は，機関 CISO から重要サーバ管理者として指名を受けていない場合は，重要なサーバを管理してはならない。

⑦ 重要サーバ管理者として指名された情報システム管理者は，重要な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。

⑧ 重要サーバ管理者は，重要な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等を提示し，機関 CISO へ申請のうえ，許可を得なければならない。

⑨ 前項の機関 CISO の許可は，重要なサーバを新規に設置する場合（設置済みのサーバ

を新たに重要なサーバとして扱うこととなる場合を含む。）に準用する。

⑩ 重要サーバ管理者は，所掌する重要なサーバの引継ぎにあたっては，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。

⑪ 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。

⑫ 情報システム管理者は，所掌する情報システムにかかる保守請負業者等の緊急連絡先一覧を整備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）

① 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，所掌情報システム等の管理，開発，設定の変更，運用，更新等の作業を行う。

② 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，外部電磁的記録媒体の管理を行う。

③ 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の記載を行う。

(10) 情報セキュリティ委員会（基本規程第１７条）

① 情報セキュリティ委員会は，毎年度，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。）の結果を確認しなければならない。

② 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ことができる。

③ 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）

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

(12) 兼務の禁止（基本規程第１９条）

① 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。

② 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。

③ 2.(2)⑥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報告を受けるための窓口

① 機構の情報セキュリティに関する統一的な窓口（以下「機構統一窓口」という。）は，

事務局総務課企画評価係とする。

② 機関における情報セキュリティインシデントの統一的な窓口（以下「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情報セキュリティインシデントについて，外部から報告を受けるための窓口（以下「外部報告窓口」という。）として，下記のとおり設置する。

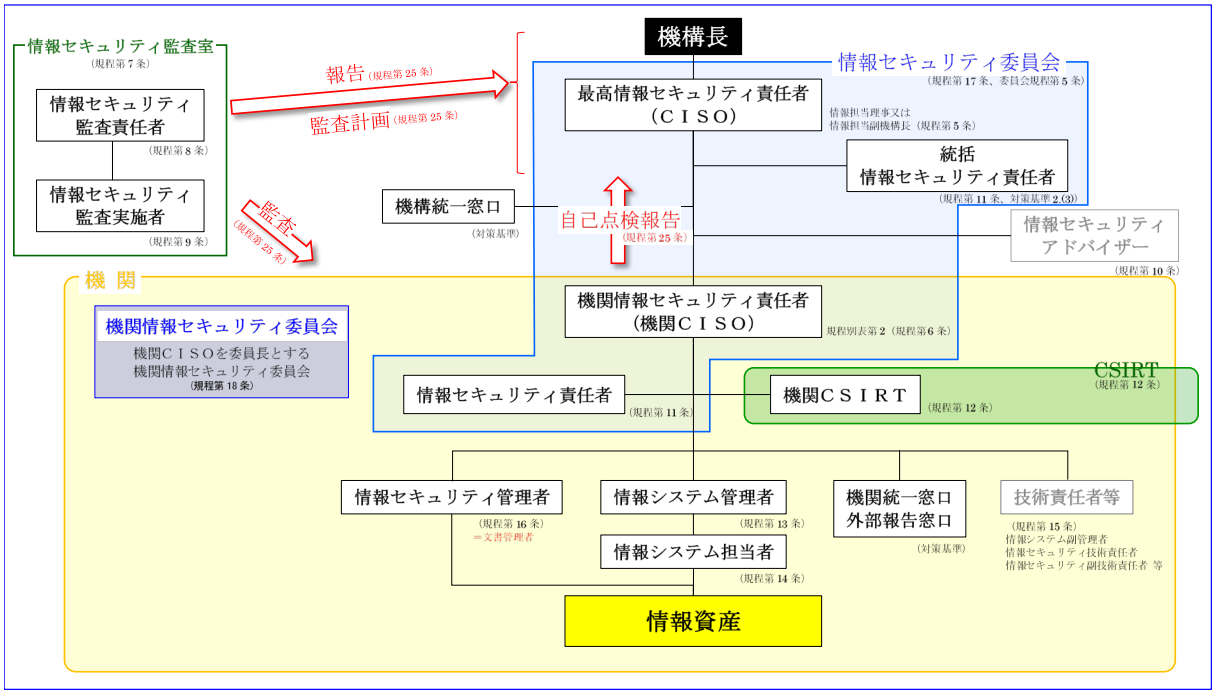
機関等区分 （基本規程別表第２）	機関統一窓口	外部報告窓口
国立天文台	情報セキュリティ室	総務課総務係
核融合科学研究所	情報システム・セキュリティセンター情報セキュリティグループ	管理部総務企画課企画・評価係
岡崎３機関等	岡崎３機関等機関統一窓口担当	岡崎統合事務センター総務部総務課情報サービス係
事務局等	事務局総務課企画評価係	事務局総務課企画評価係

※ ただし，組織運営通則第２条の２第１号に掲げる共創戦略統括本部及び同条第２号に掲げるアストロバイオロジーセンターについて，機関等の施設に設置された研究室等については，当該機関等の窓口となるので注意すること。

③ 機関 CISO は，機関統一窓口及び外部報告窓口を整備し，当該窓口が情報セキュリティ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，その状況を確認し，自らへの報告が行われる体制を整備する。

④ 機関 CISO は，外部報告窓口への連絡手段を公表しなければならない。

情報セキュリティ対策に関する基本規程　統制図



(14) 情報システム管理者相談窓口

機関 CISO は，情報システム管理者のサポートを目的とする技術相談窓口を整備し，周知しなければならない。

3. 情報資産の分類と管理方法

(1) 情報資産の分類

機構における情報資産は，基本規程第２０条に基づき，機密性，完全性及び可用性により分類・格付けし，基本規程別表第１に定めた取扱制限を行うものとする。

① 分類・格付けの細分化

機関 CISO は，別途定めることにより，基本規程別表第１に規定する情報資産の分類・格付けを細分化し，基本規程及び本対策基準の規定を満たす範囲で，取扱制限等を適用することができる。

細分化にあたっては，基本規程別表第１の分類に枝番号を付すことにより行うものとする。

(2) 情報資産の管理

① 管理責任

（ア）情報セキュリティ管理者は，その所掌する情報資産について管理責任を有する。

（イ）情報資産（基本規程第３条第５号及び第６号に該当するものに限る。以下「情報データ資産」という。）が複製又は伝送された場合には，複製等された情報資産も（１）

の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員等（機構が定める就業規則に基づき雇用されている全ての者をいう。以下同じ。）は，以下の（ア）に掲げる情報資産について，情報資産の分類・格付けを情報セキュリティ管理者の指示に従って表示し，必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。ただし，情報資産の格付けが１（機密性１，完全性１，可用性１）の場合は，当該表示を省略することができるものとする。

情報システム管理者は，以下の（イ）及び（ウ）に掲げる情報資産について，情報資産の分類・格付けを表示しなければならない。ただし，機密性２以下，完全性１及び可用性１については，当該表示を省略することができるものとする。（機密性２以下を省略可能としているのは，情報資産廃棄ガイドラインにより適切に廃棄されることを前提としていることに留意すること。）

（ア）基本規程第３条第５号（ネットワーク及び情報システムで取り扱う情報）及び同条第６号（システム関連文書）

ファイル（データ）については，ファイル名等に表示する。印刷文書については，当該文書の上余白等に表示する。

（イ）基本規程第３条第２号（情報システム）

性能，使用条件等に影響しない範囲で，筐体のベゼル部分など，確認し易くかつ剥がれ難い場所にラベル等で表示する。

（ウ）基本規程第３条第４号（電磁的記録媒体）

電磁的記録媒体の筐体又は外装の任意の場所にラベル等で表示する。

ただし，内蔵電磁的記録媒体について，当該記録媒体を収容している筐体に表示している場合は，当該記録媒体に表示する必要はない。

③ 情報の作成

（ア）情報を作成する者は，情報セキュリティ管理者の指示に従い，情報の作成時に（１）の分類に基づき，当該情報の分類と取扱制限を定めなければならない。

（イ）情報を作成する者は，作成途上の情報についても，紛失や流出等を防止しなければならない。また，情報の作成途上で不要になった場合は，当該情報を消去しなければならない。

（ウ）情報セキュリティ管理者又は情報システム管理者は，情報を基本規程第３条第４号に該当する情報資産へ長期保管する場合は，機密性分類に応じた取扱制限，アクセス権限の管理及びサービス継続性等に留意するとともに，改竄や消去に対する対策を講じなければならない。

④ 情報資産の入手

（ア）機構の役職員等が作成した情報資産を入手した者は，入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）機構の役職員等以外の者が作成した情報資産を入手した者は，情報資産の分類に基づき，当該情報の分類と取扱制限を定めなければならない。

（ウ）情報資産を入手した者は，入手した情報資産の分類が不明な場合，情報セキュリティ管理者に判断を仰がなければならない。

⑤ 情報資産の利用

（ア）情報資産を利用する者は，機関 CISO の許可がある場合を除き，業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は，情報資産の分類に応じ，適切な取扱いをしなければならない。

（ウ）情報資産を利用する者は，同一の電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合，最高度の分類に従って，当該電磁的記録媒体を取り扱わなければならない。

⑥ 情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は，情報資産の分類に従って，情報資産を適切に保管しなければならない。

（イ）情報セキュリティ管理者又は情報システム管理者は，情報データ資産を記録した電磁的記録媒体を長期保管する場合は，書込禁止の措置（DVD-R 等の WORM(Write Once Read Many)メディアにより改竄や消去に対する対策を講じることを含む。）を講じなければならない。

（ウ）情報セキュリティ管理者又は情報システム管理者は，利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は，自然災害を被る可能性等を考慮し，その可能性が低い区域に保管したり，異なる場所での多重保管をする等必要な対策を講じなければならない。

（エ）情報セキュリティ管理者又は情報システム管理者は，機密性３以上，完全性２以上，可用性２以上の全てを満たす情報を記録した電磁的記録媒体を保管する場合，耐火，耐熱，耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦ 情報の送信

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以上の情報を送信する者は，当該情報について，別紙２「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。

機密性３以上の情報については，原則として電子メールによる情報の送信を禁止する。

⑧ 情報データ資産等の運搬

（ア）車両等により機密性２以上の情報データ資産及び情報データ資産を記録している情報資産（以下「情報データ資産等」という。）を運搬する者（運搬を委託する場

合を含む。）は，機密性２の情報データ資産等については必要に応じ，機密性３以上の情報データ資産等については必ず，情報データ資産等の不正利用を防止するための措置（鍵付きのケース等に格納し，暗号化ガイドラインに基づく情報データ資産の暗号化及びストレージパスワードの設定を行う等）を講じなければならない。

（イ）機密性３以上の情報データ資産等を運搬する者（運搬を委託する場合を含む。）は，運搬にあたって措置する保全対策及び情報漏洩時の影響並びにその他必要な事項を情報セキュリティ管理者に明示し，許可を得なければならない。

⑨ 情報データ資産の提供・公表

（ア）情報データ資産を外部に提供する者は，機密性２の場合は必要に応じて，機密性３以上の場合は必ず，別紙２に掲げる「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。

（イ）機密性２以上の情報データ資産を外部に提供する者は，機関 CISO が定めた情報資産及び機構の規程，規則，その他契約等により別途取扱いの定めがある場合を除き，情報セキュリティ管理者に許可を得なければならない。

⑩ 情報資産の廃棄

（ア）機密性２以上の情報資産を廃棄する者は，情報を記録している電磁的記録媒体が不要になった場合，当該電磁的記録媒体を別紙１「情報資産廃棄ガイドライン」に従い廃棄しなければならない。なお，内蔵電磁的記録媒体の破損等によりこれを交換した場合，交換前の内蔵電磁的記録媒体は外部電磁的記録媒体に準じて外部電磁的記録媒体管理台帳に記録するものとする。

（イ）情報システム管理者は，機密性３以上として格付けされた基本規程第３条第２号に規定する情報システム又は第４号に規定する電磁的記録媒体に該当する情報資産を廃棄した場合は，当該情報資産の廃棄に関する記録（日時，担当者及び処理内容（情報資産廃棄ガイドラインに基づく破棄の方法，委託した場合は委託先等，及びエビデンス））を作成し，当該情報資産台帳又は外部電磁的記録媒体管理台帳の写しを添付のうえ，所属の情報セキュリティ管理者へ提出するものとする。情報セキュリティ管理者は当該記録を３０年間（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における「法人文書ファイル等の移管又は廃棄の状況が記録された帳簿」に同じ。）保管するものとする。

4. 物理的セキュリティ

4.1. サーバ等の管理

(1) 機器の取付け

情報システム管理者は，サーバ等の機器の取付けを行う場合，火災，水害，埃，振動，

温度，湿度等の影響を可能な限り排除した場所に設置し，容易に取り外せないよう適切に固定する等，必要に応じて適切な措置を講じるものとする。

(2) サーバの冗長化

情報システム管理者は，ネットワーク，情報システム及び情報施設・設備の可用性等を考慮し，合理性のある冗長構成とするように努力しなければならない。

(3) 機器の電源

① 情報システム管理者は，情報セキュリティ責任者及び施設管理部門と連携し，サーバ等の機器の電源について，電源供給体制を確認し，その体制において停電の可能性がある場合は，必要に応じて当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けるものとする。

② 情報システム管理者は，情報セキュリティ責任者及び施設管理部門と連携し，落雷等による過電流による影響がある場合はサーバ等の機器を保護するための措置を講じるものとする。

(4) 通信ケーブル等の配線

① 情報セキュリティ責任者及び情報システム管理者は，施設管理部門と連携し，通信ケーブル及び電源ケーブルの損傷等を防止するために，必要に応じて対策を講じなければならない。

② 情報セキュリティ責任者及び情報システム管理者は，パブリックスペース等通信ケーブルへアクセス可能な場所は，保護対策を講じなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は，適切な認証や接続制限が適用されている場合又は予め情報セキュリティ責任者が定めた方法による接続である場合を除き，ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する，接続口をロックする又は接続しても当該機器がネットワークに繋がらないようにする等，適切に管理しなければならない。

④ 情報セキュリティ責任者及び情報システム管理者は，必要に応じて，自ら又は情報システム担当者及び契約により操作を認められた業務委託事業者以外の者が配線を変更，追加できないような措置を施さなければならない。

(5) 機器の定期保守及び修理

① 情報システム管理者は，可用性２以上のサーバ等の機器については，必要に応じて自ら又は委託により，定期的に保守点検を実施しなければならない。

② 情報システム管理者は，機密性３以上の分類に該当するデータを格納する電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合において，機構の監視が届かない場所（当該事業者のサービス拠点等）において行う場合は，内容を消去した状態又は当該電磁的記録媒体を取り外した状態で行わせなければならない。これらの措置を講じることができない場合，情報システム管理者は，外部の事業者に故障を修理させ

るに当たり，修理を委託する事業者との間で，守秘義務契約を締結するほか，秘密保持体制の確認などによりセキュリティを担保しなければならない。

(6) 機構外へのサーバの設置

情報セキュリティ責任者及び情報システム管理者は，機構が所有又は借上する不動産以外にサーバを設置する場合，機関 CISO の承認を得なければならない。また，定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(7) 機器の廃棄・譲渡等

情報システム管理者は，機密性２以上の分類に該当するデータを格納する機器を廃棄，リース返却，譲渡等をする場合，「情報の抹消」を講じなければならない。

ただし，他の国立大学法人等に譲渡する場合において，譲渡先において適切な情報セキュリティポリシーが適用されることが確実であって，機構の各種規程に違反せず，かつ機関 CISO の承諾が得られた場合にはこの限りではない。

4.2. 情報管理区域（情報システム室等）の管理

(1) 情報管理区域の構造等

① 情報管理区域とは，ネットワークの基幹機器及び重要な情報システムを設置し，当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 情報セキュリティ責任者及び情報システム管理者は，原則として情報管理区域を２階以上に設けるものとし，やむを得ず地階又は１階に設ける場合は，外部からの侵入が容易にできないように配慮しなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は，施設管理部門と連携して，情報管理区域から外部に通ずるドアは必要最小限とし，鍵，監視機能，警報装置等によって許可されていない立入りを防止するように努力しなければならない。

④ 情報セキュリティ責任者　及び情報システム管理者は，情報システム室内の機器等に，必要に応じて転倒及び落下防止等の耐震対策，防火措置（コンピュータ専用消火器等の設置），防水措置等を講じなければならない。

⑤ 情報セキュリティ責任者及び情報システム管理者は，施設管理部門と連携して，情報管理区域を囲む外壁等の床下開口部を全て塞ぐように努力するものとする。

⑥ 情報セキュリティ責任者及び情報システム管理者は，情報管理区域に配置する消火薬剤や消防用設備等が，機器等及び電磁的記録媒体に影響を与えないようなものとするように配慮しなければならない。

⑦ 情報セキュリティ責任者及び情報システム管理者は，施設管理部門と連携して，情報管理区域の電源について，空調（排熱）設備及び情報システムの運転維持に関して配慮したものとしなければならない。

(2) 情報管理区域の入退室管理等

① 情報システム管理者は，IC カード，指紋認証等の生体認証等により，原則として情報管理区域への入退室を許可された者のみに制限し，入退室のログを記録するものとする。

② 役職員等及び業務委託事業者は，情報管理区域に入室する場合，身分証明書等を携帯し，求めにより提示しなければならない。

③ 情報システム管理者は，外部からの訪問者が情報管理区域に入る場合には，必要に応じて以下の対策を講じるものとする。

（ア）立入区域を制限

（イ）情報管理区域への入退室を許可された役職員等の立会い

（ウ）外部訪問者が外見上役職員等と区別できる措置

④ 情報システム管理者は，機密性３以上の情報資産を扱うシステムを設置している情報管理区域について，当該情報システムに関連しない端末，通信回線装置，電磁的記録媒体等を許可なく持ち込ませないようにしなければならない。

(3) 機器等の搬入出

① 情報システム管理者は，搬入する機器等が，既存の情報システムに与える影響について，あらかじめ職員又は業務委託事業者に確認を行わせなければならない。

② 情報システム管理者は，情報システム室の機器等の搬入出について，職員を立ち会わせなければならない。

4.3. 通信回線及び通信回線装置の管理

① 情報セキュリティ責任者及び情報システム管理者は，所掌するネットワーク及び当該情報施設・設備の通信回線及び通信回線装置を，施設管理部門と連携し，適切に管理しなければならない。また，通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

② 情報セキュリティ責任者は，外部へのネットワーク接続を必要最低限に限定し，できる限り接続ポイントを減らさなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は，所掌する機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合，必要なセキュリティ水準を検討の上，適切な回線を選択しなければならない。また，必要に応じ，送受信される情報の別紙２「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。

④ 情報セキュリティ責任者及び情報システム管理者は，所掌するネットワーク及び当該情報施設・設備に使用する回線（LAN ポートを含む。）について，必要に応じて伝送途上に情報が破壊，盗聴，改ざん，消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤ 情報セキュリティ責任者は，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

る通信回線について，継続的な運用を可能とする回線を選択しなければならない。また，必要に応じ，回線を冗長構成にする等の措置を講じなければならない。

4.4. 職員等の端末の管理

(1) 情報システム管理者による端末の管理

① 情報システム管理者は，盗難防止のため，必要に応じて執務室等の施錠管理等（端末をセキュリティワイヤー等により固定することを含む。）の物理的措置を講じなければならない。機密性２以上の情報資産を一度でも記録したことがある電磁的記録媒体については，情報を保存する必要がなくなった時点で速やかに「情報の抹消」を行わなければならない。

② 情報システム管理者は，情報システムへのログインに際しては，パスワードの入力又は生体認証等によりセキュリティを確保するように設定しなければならない。また，利用者に強固なパスワードを守らせるために，原則としてパスワード管理ポリシー（パスワードに必要な桁数，文字種，複雑さなど）を設定するとともに，不正アクセス対策として，アカウントロック，パソコンロック（画面ロック）等の機能を有効に機能するように設定しなければならない。

③ 情報システム管理者は，必要に応じて端末の電源起動時のパスワード（BIOS/UEFI パスワード，ストレージパスワード等）を併用しなければならない。

④ 情報システム管理者は，取り扱う情報の重要度を鑑みて，必要に応じてユーザー認証に多要素認証，生体認証等を用いるものとする。

⑤ 情報システム管理者は，端末が内蔵する電磁的記録媒体の暗号化機能（ファイルシステムの暗号化機能を含む。）を有効にし，これを利用しなければならない。端末にセキュリティチップが搭載されている場合，その機能を有効に活用するように配慮しなければならない。また，役職員等は外部電磁的記録媒体の使用に当たっては，原則として機密性２のデータについては，これを暗号化するものとし，機密性３以上のデータを記録する場合は，当該媒体全体が暗号化されているものを用いなければならない。

⑥ 情報システム管理者は，機構の資産であるモバイル端末の機構外での業務利用の際は，その電磁的記録媒体について暗号化しなければならない。なお，既に機密性２以上の情報が保存された非暗号化状態にあるモバイル端末については，記録された領域全体の論理的破壊が行われない場合は，暗号化したとしても，未破壊領域にかかる情報を復元できる可能性があり，この点にかかる論理的保証が必要であることに留意すること。

⑦ ⑤及び⑥に規定する暗号化にあたっては，原則として別紙２「暗号化ガイドライン」を遵守するものとする。

(2) 職員等による端末の管理

職員等は，情報システム管理者の許可を得て，自身が使用する機構の資産である端末

及び電磁的記録媒体について，管理者（以下「自己管理者」という。）となることができる。この場合は，当該機器について情報システム管理者としての義務と責任を負う。また，当該機器の管理については，4.4.(1)「情報システム管理者による端末の管理」を準用するほか，これを廃棄・資産の譲渡等を行う場合について，4.1.(7)を準用する。

5. 人的セキュリティ

5.1. 職員等の遵守事項

(1) 職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員等は，情報セキュリティポリシー等を遵守するとともに，自ら情報セキュリティの向上に努めなければならない。また，情報セキュリティ対策について不明な点，遵守することが困難な点等がある場合は，速やかに情報セキュリティ管理者に相談し，指示を仰がなければならない。

② 職務以外の目的での使用の禁止

職員等は，就業規則第１５条第２号に基づき，機関 CISO の許可無く職務以外の目的で情報資産の外部への持ち出し，ネットワークの利用，情報システムへのアクセス，基本規程第４条第１項第１号及び第３号に該当しない情報システムへの転送，電子メールアドレスの使用及びインターネットの利用を行ってはならない。

③ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

職員等は，機構の資産であるモバイル端末や電磁的記録媒体等を外部に持ち出す場合は，情報セキュリティポリシーを遵守するとともに，特に基本規程別表第１の分類による取扱制限，本対策基準 3.(2)⑧に掲げる情報資産の運搬，4.4.(1)②及び 4.4.(1)⑥に注意しなければならない。

④ 機構の資産である情報システム以外（私物を含む。）の端末及び電磁的記録媒体等（以下「支給外端末等」という。）の業務利用

ＣＩＳＯが特に定める場合を除き，本項に基づく支給外端末等の業務利用により生じた損害（当該端末の故障，マルウェア感染など）については，機構はその責を負わない。一方で，職員等の善管注意義務違反により発生した情報漏洩等により機構が損害を被った場合，機構は当該損害額を上限として損害賠償請求を行うことができるものとする。

職員等は，このことを十分に認識したうえで，以下の（ア）・（イ）の許可申請を行わなければならない。

（ア）職員等は，支給外端末等を原則として機密性２以上の情報資産を扱う職務に利用してはならない。ただし，職務上必要であり，機密性２及び機密性３の情報の場合は，情報セキュリティ管理者の許可を得て利用することができる。この場合，

当該許可を申請した職員等は，当該支給外端末等を業務利用するうえで生じるマルウェア感染等のリスクを認識するとともに，当該申請対象の支給外端末等に情報セキュリティポリシーが適用される（当該端末の内蔵電磁的記録媒体にかかる暗号化等，情報セキュリティポリシーの準拠を含む。）ことについて同意したものと見做す。

情報セキュリティ管理者は，機密性３にかかる許可を与える場合は，（イ）に掲げる事項を満たしていることを確認しなければならない。

（イ）職員等は，機密性３の情報資産については，基本規程別表第１「機密性による情報資産の分類」の取扱制限に定める機関ＣＩＳＯの許可がある場合を除き，私物の端末及び電磁的記録媒体等による情報処理及び保管を行ってはならない。ただし，機関ＣＩＳＯは，当該規定に基づき機密性３の情報資産の支給外端末等による業務利用の許可を与えようとする場合は，情報漏洩（内部不正によるものを含む。）のリスクを十分に低減するための基準を定めなければならない。

（ウ）職員等は，支給外端末等をネットワーク及び情報システムへ接続する場合は，接続するネットワーク及び情報システムを所掌する情報システム管理者が定めた手順を遵守するとともに，当該情報システム管理者の指示に従わなくてはならない。また，情報セキュリティインシデントが生じた場合に，支給外端末等が原因として疑われる場合は，支給外端末等の精査について，情報システム管理者に協力しなければならない。

（エ）情報セキュリティ管理者は（ア）に基づき許可を与える場合は，当該支給外端末等が情報セキュリティポリシーに準拠することを確認したうえで許可を与えるものとする。許可を与えた支給外端末等については，記録簿を整備し，職員等氏名，当該端末の形式，Serial No，許可日，解除日，許可期間等必要な情報を記録しなければならない。

（オ）職員等は，支給外端末等を用いて業務を行う必要が無くなった場合又は情報セキュリティ管理者が許可した期間を満了した場合，速やかに機構の情報の消去（暗号化消去が好ましい）を行い，情報セキュリティ管理者へ報告するものとする。

⑤ 端末におけるセキュリティ設定変更の禁止

職員等は，端末のソフトウェアに関するセキュリティ機能の設定を，明らかにセキュリティを強化する設定変更を除き，情報システム管理者の許可なく故意に変更してはならない。

⑥ 机上の端末等の管理

職員等は，端末，電磁的記録媒体及び情報が印刷された文書等について，第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように，離席時の端末のロックや電磁的記録媒体，文書等の容易に閲覧されない場所への保管等，適切な措置を講じなければならない。

⑦ 退職時等の遵守事項

職員等は，異動，退職等により業務を離れる場合には，利用していた機構の情報資産を，返却しなければならない。また，その後も業務上知り得た機密性 2 以上の情報を漏らしてはならない。

情報セキュリティ管理者は，職員等の退職時に，機構の機密性２以上の情報を持ち出さないこと及び在職時に知りえた機構の機密性２以上の情報にかかる機密保持等を確保するため，退職時機密保持誓約書を提出させ，保管するものとする。ただし，機関 CISO が認める場合は，情報セキュリティ管理者に代わり，機構の人事担当が代理して取得，保管することができるものとする。

⑧ 機構が提供するネットワーク以外のネットワーク利用

職員等は，機構が提供するネットワーク以外のネットワークを業務で利用する場合は，接続する情報システム（支給外端末等を含む）に適切なセキュリティ対策（外部から当該情報システムへ利用可能なサービス，ポート等を制限するなど）を講じるとともに，通信が盗聴されている可能性を考慮し，通信の暗号化状況に注意して利用しなければならない。

⑨ 職員等は，機構のネットワークに接続されている機器に外部ネットワークから接続する場合（以下「リモートアクセス」という。）は，機関ＣＩＳＯの規定に基づき接続するものとし，これ以外の接続方法を用いてはならない。

⑩ テレワーク

職員等は，原則として機構が支給する端末を用いてテレワークを行うものとし，その遂行にあたっては，情報セキュリティ管理者及び情報システム管理者の指示に従うとともに，以下に掲げる事項について遵守しなければならない。

- テレワークの実施前に，テレワークで使用する端末の OS 及びソフトウェアのセキュリティ更新を実施し，当該端末を最新の脆弱性対策パッチが適用された状態に維持すること。
- テレワークの実施前に，不正プログラム対策ソフトウェアのパターンファイルを最新にすること。
- 自宅以外の場所でテレワークを行う場合は，セキュリティワイヤーを用いるなど，紛失・盗難対策を講じること。
- 当該端末を接続するネットワークについては，機構が提供した場合はこれを使用することを原則とする。
  機構が提供しない場合においても，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ネットワークの利用は極力避けること。（ネットワーク機器の管理状況によっては，脆弱性等により，DNS データベースの改ざんや，盗聴などの可能性がある。）
- 職員等は，画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選

定すること。

(2) 非常勤及び臨時職員への対応

① 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は，非常勤及び臨時職員に対し，採用時に情報セキュリティポリシー等のうち，非常勤及び臨時職員が守るべき内容を理解させ，また実施及び遵守させなければならない。

② 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は，非常勤及び臨時職員の採用の際，情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

(3) 情報セキュリティポリシー等の掲示

CISO 及び機関 CISO は，職員等が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならない。

(4) 業務委託事業者に対する説明

情報セキュリティ管理者又は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の開発・保守等を業務委託事業者に発注する場合，業務委託事業者から再委託を受ける事業者も含めて，情報セキュリティポリシー等のうち業務委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

5.2. 教育・研修・訓練

(1) 情報セキュリティに関する教育・研修・訓練

① CISO 及び機関 CISO は，定期的に情報セキュリティに関する教育・研修・訓練を実施しなければならない。

② CISO 及び機関 CISO は，CSIRT 及び重要サーバ管理者に対する教育・研修・訓練については，特に配慮して実施しなければならない。

(2) 教育・研修計画の策定及び実施

① CISO は，機構全体として実施する役職員等に対する情報セキュリティに関する教育・研修計画を策定し，情報セキュリティ委員会に報告しなければならない。

② 機関 CISO は，各機関において実施する役職員等に対する情報セキュリティに関する教育・研修計画を策定し，情報セキュリティ委員会に報告しなければならない。

③ 役職員等は，CISO 及び機関 CISO の定めた教育・研修計画の参加について，最大限の努力を払わなければならない。

④ CISO 及び機関 CISO は，必要に応じて，教育・研修に参加しなかった者に対して情報資産の一部又は全部を使用禁止とする等の措置を講じるものとする。

⑤ 機関 CISO は，新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

⑥ CISO 及び機関 CISO が定める教育・研修計画は，統括情報セキュリティ責任者，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及びその他職員等に対して，それぞれの役割及び情報セキュリティに関する理解度等に配慮したものにしなければならない。

⑦ CISO 及び機関 CISO は，毎年度１回，情報セキュリティ委員会に対して，教育・研修計画の実施状況及び役職員等の教育・研修への参加状況について報告しなければならない。

(3) 緊急時対応訓練

① CISO 及び機関 CISO は，緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は，ネットワーク及び各情報システムの規模等を考慮し，訓練実施の体制，範囲等を定め，また，効果的に実施できるようにしなければならない。

② 機関 CSIRT は，インシデントレスポンス訓練を定期的に実施し，対応能力向上に努めなければならない。

(4) 教育・研修・訓練への参加

全ての役職員等は，定められた教育・研修・訓練に参加しなければならない。

5.3. 情報セキュリティインシデントの報告

情報セキュリティインシデントの報告経路において，出張等により当該者が不在の場合は，代理者が，代理者が指名されていない場合は直近上位者が対応にあたるものとする。

(1) 職員等の情報セキュリティインシデントの報告（機関統一窓口）

本項において，外部への情報漏洩，外部からの不正アクセス等，外部に起因するセキュリティインシデントについては，重要であるものとして扱う。

① 職員等は，情報セキュリティインシデントを確認した場合，又はインシデントの恐れがあることを認めた場合は，機関統一窓口に直ちに報告しなければならない。

② 報告を受けた機関統一窓口は，直ちに機関 CSIRT 及び情報セキュリティ責任者に報告しなければならない。

③ 機関統一窓口から報告を受けた機関 CSIRT は，情報システム管理者と協力し，直ちに対応しなければならない。

④ 機関統一窓口から報告を受けた情報セキュリティ責任者は，直ちに機関 CISO に報告しなければならない。

⑤ 情報セキュリティ責任者から報告を受けた機関 CISO は，当該インシデントの重要性を判断し，重要と判断したもの（以下「重要案件」という。）は直ちに，重要ではないと判断したもの（以下「非重要案件」という。）は速やかに，情報セキュリティ責任者及び機関 CSIRT に対応を指示しなければならない。

⑥ 機関 CISO から指示を受けた情報セキュリティ責任者は，重要案件は直ちに（非重要案件は速やかに）情報セキュリティ管理者へ必要な対応を指示しなければならない。

⑦ 情報セキュリティ責任者から指示を受けた情報セキュリティ管理者は，重要案件は直ちに（非重要案件は速やかに）対応しなければならない。
⑧ 機関 CSIRT は，直ちに状況を確認し，重要案件は直ちに（非重要案件は速やかに）機関 CISO 及び情報セキュリティ責任者に状況報告を行わなければならない。
⑨ 情報セキュリティ管理者は，重要案件は直ちに（非重要案件は速やかに）当該インシデントに起因する情報漏洩に関して，情報セキュリティ責任者へ状況報告しなければならない。
⑩ 情報セキュリティ管理者から報告を受けた情報セキュリティ責任者は，重要案件は直ちに，非重要案件は速やかに機関 CISO へ状況報告するものとする。
⑪ 機関 CISO は，機関 CSIRT 及び情報セキュリティ責任者の状況報告を受け，当該インシデントの重要度を再評価し，重要案件は直ちに（非重要案件は速やかに）当該機関長，CISO 及び統括情報セキュリティ責任者へ報告しなければならない。

(2) 外部からの情報セキュリティインシデントの報告（外部報告窓口）
① 外部報告窓口は，機構が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて，外部から連絡を受けた場合，直ちに機関 CSIRT 及び情報セキュリティ責任者に報告しなければならない。
② 外部報告窓口から報告を受けた機関 CSIRT は，情報システム管理者と協力し，直ちに対応しなければならない。
③ 外部報告窓口から報告を受けた情報セキュリティ責任者は，直ちに機関 CISO に報告しなければならない。
④ 情報セキュリティ責任者から報告を受けた機関 CISO は，直ちに情報セキュリティ責任者及び機関 CSIRT に対応を指示しなければならない。
⑤ 機関 CISO から指示を受けた情報セキュリティ責任者は，直ちに情報セキュリティ管理者に対応を指示しなければならない。
⑥ 情報セキュリティ責任者から指示を受けた情報セキュリティ管理者は，直ちに対応しなければならない。
⑦ 機関 CSIRT は，直ちに状況を確認し，機関 CISO 及び情報セキュリティ責任者に状況報告を行わなければならない。
⑧ 情報セキュリティ管理者は，直ちに当該インシデントに起因する情報漏洩に関して，情報セキュリティ責任者へ状況報告しなければならない。
⑨ 情報セキュリティ管理者から報告を受けた情報セキュリティ責任者は，直ちに機関 CISO へ状況報告しなければならない。
⑩ 機関 CISO は，機関 CSIRT 及び情報セキュリティ責任者の状況報告を受け，当該インシデントの重要度を再評価し，重要案件は直ちに（非重要案件は速やかに）当該機関長，CISO 及び統括情報セキュリティ責任者へ報告しなければならない。

(3) 情報セキュリティインシデント原因の究明及び記録並びに再発防止等

① 機関 CSIRT は，情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者，情報システム管理者等と連携し，これらの情報セキュリティインシデント原因を究明し，記録を保存しなければならない。また，必要に応じて復旧計画を策定するとともに，できる限り速やかに原因究明と再発防止策案を策定し，機関 CISO 及び情報セキュリティ責任者へ提出しなければならない。

② 機関 CISO は，機関 CSIRT からの原因究明と再発防止策案の提出を受け，機関としての原因究明と再発防止策を策定し，当該機関長，CISO 及び統括情報セキュリティ責任者に報告するとともに，情報セキュリティ責任者に再発防止措置を指示しなければならない。

(4) CISO の報告

機関 CISO から報告を受けた CISO は，重要案件であると判断した情報セキュリティインシデントについては，その経緯，原因究明結果及び再発防止策等について役員会に報告するものとする。

(5) 情報セキュリティインシデント情報の共有

CISO 及び機関 CISO は,機構内で発生した情報セキュリティインシデントについて，可能な限り詳細な情報をホームページ等を用いて役職員等に開示し，情報共有を図らなければならない。

(6) 情報セキュリティインシデントの公表

CISO は，情報セキュリティインシデントの内容を検討し，必要と認めた場合は速やかに情報セキュリティインシデントの公表を行うものとする。

5.4. ID 及びパスワード等の管理

(1) セキュリティトークンの取扱い

① 職員等は，自己の管理するセキュリティトークンに関し，次の事項を遵守しなければならない。

（ア）認証に用いるセキュリティトークンは，情報システム管理者の許可なく，職員等間で共有してはならない。

（イ）認証に必要な場合を除き，セキュリティトークンを端末のスロット等から外し，鍵付きの引き出し等安全な場所に保管しておかなければならない。

（ウ）セキュリティトークンを紛失した場合には，速やかに情報システム管理者に報告し，指示に従わなければならない。

② 情報システム管理者は,セキュリティトークンの紛失等の報告を受けた場合は直ちに,当該セキュリティトークンによる認証を無効化しなければならない。

③ 情報システム管理者は，セキュリティトークンを切り替える場合，切り替え前のセキュリティトークンによる認証を無効化しなければならない。また，必要に応じて切替

え前のセキュリティトークンを回収し，破砕するものとする。

(2) ID の取扱い

職員等は，自己の管理する ID に関し，次の事項を遵守しなければならない。

① 自己が利用している ID は，他人に利用させてはならない。

② 共用 ID を利用する場合は，情報システム管理者が認めた場合を除き，共用 ID の利用者以外に利用させてはならない。

(3) パスワードの取扱い

職員等は，自己の管理するパスワード（秘密鍵の展開用パスフレーズを含む）や公開鍵暗号における秘密鍵（以下「秘密鍵」という。）に関し，別紙３「パスワードガイドライン」及び次の事項を遵守しなければならない。

① パスワードは，他者に知られないように管理しなければならない。また，公共交通機関やパブリックスペースなど，パスワードの入力過程が他人に漏れる可能性が高い場所では，パスワードの漏えいに十分に注意しなければならない。

② パスワードは原則として記号，英小文字，英大文字，数字のうちから２種類以上を組み合わせ，１２文字以上の長さ又はこれと同等以上の複雑さを有するものとする。(パスワード長は，できるだけ長い方が良い。）また，自己から推定できる文字列，辞書等に掲載される文字列の組み合せ，文字と数字の置き換え等，探索・推定が容易なパスワードにしてはならない。

③ パスワード又は秘密鍵が流出した又はそのおそれがある場合には，即時に変更を行うとともに，情報セキュリティ管理者に速やかに報告しなければならない。ただし，Web アプリケーション等，セッション管理されているものは，セッションを破棄したうえでパスワードの変更を行わなければならないことに注意すること。

④ 複数の情報システムを扱う職員等は，原則として機密性３以上の情報システムに関しては，同一のパスワードや秘密鍵をシステム間で用いてはならない。ただし，二段階認証，多要素認証及び生体認証を併用する場合を除く。）

⑤ 原則として仮のパスワードは，最初のログイン時点で変更しなければならない。

⑥ 情報システム管理者が認めた場合を除き，職員等間でパスワード及び秘密鍵を共有してはならない。

5.5. 共同利用・共同研究者等の扱い

(1) 適用範囲

基本規程第４条第１項各号に定めるもの。

(2) 本対策基準における適用

職員等を共同利用・共同研究者等と読み替え適用する。ただし，自然科学研究機構の就業規則に該当する事項及び機関 CISO が定める場合を除く。

(3) 同意書

機関 CISO は，必要に応じて，共同利用・共同研究者等に対し，情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

6. 技術的セキュリティ

6.1. コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

① 情報システム管理者は，容量超過などによる可用性の障害を考慮する等，必要に応じて職員等が使用できるファイルサーバ（Network Attached Storage を含む。以下同じ。）の容量を設定し，職員等に周知しなければならない。

② 情報システム管理者は，ファイルサーバを想定される利用状況に応じたグループの単位で構成し，職員等が他グループのフォルダ及びファイルを閲覧及び使用できないようにする等，アクセス権限を適切に設定しなければならない。

③ 情報システム管理者は，個人情報，人事記録等，特定の職員等しか取り扱えないデータについて，別途フォルダを作成する等の措置を講じ，担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

(2) バックアップの実施

情報システム管理者は，ファイルサーバ等に記録された情報について，サーバの冗長化対策に関わらず，必要に応じて定期的にバックアップを実施しなければならない。

バックアップデータについては，当該ファイルサーバ等の機密性の格付けを鑑みて，情報管理区域に保管する等，盗難・紛失対策を行うものとする。

また，ランサムウェア対策として，完全性の格付け等の重要度を鑑みて，必要に応じてネットワークから隔離して保管するものとする。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は，他の団体と情報システムに関する認証情報等の機密性２以上の情報及び機密性２以上の情報を取り扱うソフトウェアにより情報を交換する場合，その取扱いに関する事項をあらかじめ定め，機関 CISO の許可を得なければならない。

(4) システム管理記録及び作業の確認

① 情報システム管理者は，所掌する情報システムの運用において実施した作業について，作業記録を作成しなければならない。

② 情報システム管理者は，所掌する重要なサーバ及びその他重要と考える情報システム及びネットワークにおいて，システム変更等の作業を行った場合は，必要に応じて作業内容について記録を作成し，詐取，改ざん等をされないように適切に管理しなければならない。

③ 情報セキュリティ責任者，情報システム管理者又は情報システム担当者及び契約によ

り操作を認められた業務委託事業者等が情報システムに係る重要な又は影響の大きなシステム変更等の作業を行う場合は，必要に応じて２名以上で作業し，互いにその作業を確認しなければならない。

(5) 情報システム仕様書等の管理

情報セキュリティ責任者及び情報システム管理者は，ネットワーク構成図及び情報システム仕様書について，記録媒体に関わらず，業務上必要とする者以外の者の閲覧及び紛失等がないよう，適切に管理しなければならない。

(6) 情報システムの利用記録の採取（ログの取得）等

① 情報システム管理者は，情報セキュリティの確保に必要な記録を取得し，以下の期間保存しなければならない。ただし，（ア）～（ウ）について，２０２０年３月３１日までは別途機関 CISO が定めることができる。

（ア）対外（インターネット）接続部であるゲートウェイのログは，原則として全てのログを２年間以上保存するものとする。

（イ）重要なサーバのログ（関係するものを含む。）は原則として１年間以上保存するものとする。

（ウ）上記（ア），（イ）に掲げるものを除き，機密性３以上の情報を保存している端末については，そのアクセスログ等を原則として１年間以上保存するものとする。

（エ）その他の機器については，原則として 30 日以上とする。ただし，必要に応じて機関 CISO が別に定めることができる。

② 前項のログは，30 日を越えるものについては，完全性を担保しつつ，外部電磁的記録媒体に保存することができる。ただし，機関 CISO が別の方法を定めた場合は，これによるものとする。

③ ①に掲げるログとして取得する項目は，追跡可能性を考慮し，誰が（又は端末が），いつ，どの情報資産にアクセスしたかなど，不正アクセス等に備えて適切な項目としなければならない。ただし，機関 CISO が別の取得項目を定めた場合は，これによるものとする。

④ 情報システム管理者は，取得したログを定期的に点検又は分析する機能を設ける等，必要に応じて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しなければならない。

⑤ 機関 CISO は，必要に応じて，ログが取得できなくなった場合の対処等，その他の必要な事項について定め，情報システム管理者に適切にログを管理させるための措置を講じなければならない。

(7) 障害記録

① 情報システム管理者は，職員等からのシステム障害の報告，システム障害に対する処理結果又は問題等について，障害記録を作成しなければならない。

② 情報システム管理者は，システム障害が情報セキュリティインシデントに起因すると判断した場合は，直ちに機関統一窓口に通報するものとする。

(8) ネットワークの接続制御，経路制御等

① 情報セキュリティ責任者及び情報システム管理者は，所掌機関等におけるネットワークに対するフィルタリング及びルーティングについて，設定の不整合が発生しないように，ファイアウォール，ルータ等の通信ソフトウェア等を設定しなければならない。

② 情報セキュリティ責任者及び情報システム管理者は，所掌機関等におけるネットワークについて，不正アクセスを防止するため，ネットワークに適切なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムの分離等

情報システム管理者は，来訪者が利用できるシステム（1.1.(1)に掲げる LAN を除く）について，必要に応じて他のネットワーク及び情報システムと物理的又は論理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

① 情報システム管理者は，所掌するネットワークを外部ネットワークと接続しようとする場合には，機関 CISO 及び情報セキュリティ責任者の許可を得なければならない。

② 情報システム管理者は，接続しようとする外部ネットワークに係るネットワーク構成，機器構成，セキュリティ技術等を詳細に調査し，機構内の全てのネットワーク，情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は，ウェブサーバ等をインターネットに公開する場合，機構内ネットワーク（基本規程第３条第１号及び第４条に該当するネットワークをいう。以下同じ。）への侵入を防御するために，当該サーバ等を外部のネットワーク又は DMZ（非武装地帯）等適切なセグメントに設置しなければならない。

④ 情報システム管理者は，接続した外部ネットワークのセキュリティに問題が認められ，情報資産に脅威が生じることが想定される場合には，情報セキュリティ責任者の判断に従い，速やかに当該外部ネットワークを物理的又は論理的に遮断しなければならない。

⑤ 機関 CISO は，職員等に対して外部のネットワークから機構のネットワーク内（DMZ は含まない）の情報システムに対するアクセスを提供することを目的として VPN 等（リモートアクセスツール（Chrome リモートデスクトップ，SoftEther VPN など）を含む。）を構築する場合は，規定を整備しなければならない。

⑥ 情報セキュリティ責任者及び情報システム管理者は，機関 CISO の規定に従い VPN を構築・運用する場合は，以下の点に十分配慮しなければならない。

- 6.2(1)①に掲げるアクセス制御及び VPN 装置に対する不正アクセスの検知

- 利用可能なプロトコルの制限
- VPN によりアクセス可能な内側のネットワークの範囲の制限（IP による制限など）

⑦ 情報セキュリティ責任者及び情報システム管理者は，必要に応じて，機関 CISO が規定した以外の方法による役職員等の VPN 等の利用を禁止する技術的な措置（リモートアクセスで使用するアウトバウンド通信を遮断するなど）を講じなければならない。

(11) 複合機のセキュリティ管理

① ネットワークに接続する複合機を調達する場合における，当該複合機が備える機能，及び管理方法等については，機関 CISO が別に定める場合を除き，当該ネットワークに接続するサーバに必要なセキュリティ要件（運用終了時に実施するデータ消去の要件等を含む。）に準じるものとする。

② 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情報セキュリティインシデントへの対策を講じなければならない。

③ 情報システム管理者は，複合機の運用を終了する場合，①により規定したセキュリティ要件に従って，複合機の持つ電磁的記録媒体の全ての情報を情報資産廃棄ガイドラインに基づき，抹消又は再利用できないようにする等情報漏洩に対処するための必要な対策を講じなければならない。

(12) 特定用途機器のセキュリティ管理

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，通信回線への接続形態等により，何らかの脅威が想定される場合は，当該機器の特性に応じた対策を実施しなければならない。

(13) 無線 LAN（Wi-Fi）（以下「無線 LAN」という。）の設置及び盗聴対策

① 情報システム管理者は，無線 LAN を設置する場合は，機関 CISO が定めた方法により設置する場合を除き，情報セキュリティ責任者（機関 CISO が別途の定めをした場合は当該者）の許可を得るとともにレイヤー２の無線通信路に対して別紙２「暗号化ガイドライン」に基づく暗号化等，事実上解読が困難とされる暗号化，認証方式を適用しなければならない。また，必要に応じて次の対策を講じるものとする。

- 無線 LAN 通信の暗号化
- IEEE 802.1X による無線 LAN へのアクセス主体の認証
- 無線 LAN 回線利用申請手続の整備
- 無線 LAN 機器の管理手順の整備
- 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

② 無線 LAN の運用にあたっては，総務省が定めるガイドライン等に準拠するように配

慮するとともに，情報セキュリティ責任者の指示に従って，必要なセキュリティ対策を講じなければならない。

(14) 電子メールのセキュリティ管理

① 電子メールサーバ（電子メールサービスを含む。）を運用している情報システム管理者（以下「電子メールシステム管理者」という。）は，権限のない利用者により，外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう，電子メールサーバ等の設定を行わなければならない。また，侵害拡大防止，及び監視強化を目的とした内部対策を講じなければならない。

② 電子メールシステム管理者は，フィッシングメール及びスパムメール等と思われる異常メールの受信又は送信を検知できるようにシステムを構築するものとする。

③ 電子メールシステム管理者は，異常メールの送受信を検知した場合は，メールのフィルタリングやメールサーバの運用を停止する等，必要な対策を講じなければならない。また，必要に応じて，当該メールの廃棄，検疫等の措置を取ると共に，機関統一窓口へ報告を通じて機構内へ情報共有を図らなければならない。

④ 電子メールシステム管理者は，電子メールの利活用途に応じて電子メールの送受信容量の上限（各個人の１日あたりの送受信件数の上限や総量等）を設定し，上限を超える電子メールの送受信を制限する等，バルクメール等の送信を防ぐ措置を講じなければならない。

⑤ 電子メールシステム管理者は，システム開発や運用，保守等のため機構に常駐している業務委託事業者の作業員等に対して，契約等に基づき電子メールアドレスを付与する場合は，情報セキュリティポリシーを遵守させる等，電子メールアドレス利用について，業務委託事業者との間で利用方法を取り決めなければならない。

(15) 電子メールの利用制限

① 職員等は機関 CISO が定める場合及び情報セキュリティ責任者の許可を得た場合を除き，原則として自動転送機能を用いて，電子メールを転送してはならない。

② 職員等は，業務上必要のない送信先に電子メールを送信してはならない。

③ 職員等は，複数人に電子メールを送信する場合，電子メールが非公開の個人情報に該当する場合がある点に注意し，必要に応じて他の送信先の電子メールアドレスが分からないようにする等の対策を講じなければならない。

④ 職員等は，機密性２以上の電子メールを誤送信した場合，情報セキュリティ管理者に報告しなければならない。ただし，機密性２情報について誤送信した相手が役職員等及び共同利用・共同研究者等である場合にはこの限りではない。

(16) 電子署名・ハッシュ値・時刻認証・暗号化

① 職員等は，情報資産の分類により定めた取扱制限に従い，外部に送るデータの機密性又は完全性を確保することが必要な場合には，別紙２「暗号化ガイドライン」に従い，

暗号化又はパスワード設定等を行うとともに，基本規程別表第１「完全性による情報資産の分類」の取扱制限に注意して，送信しなければならない。

② 職員等は，暗号化を行う場合は，原則として別紙２「暗号化ガイドライン」を遵守しなければならない。また，復号のための鍵は，暗号化した情報とは別に保管・送信する等，適切に管理しなければならない。ただし，管理方法を機関 CISO が別に定めた場合は，これによらなければならない。

③ 電子署名を用いる場合には，電子署名の正当性を検証するための情報又は手段を，署名検証者へ安全に提供しなければならない。ただし，提供方法を機関 CISO が別に定めた場合は，これによらなければならない。

(17) 無許可ソフトウェアの導入等の禁止

① 職員等は，業務上の必要があり，機関 CISO が定めた場合又は当該機器を所掌する情報システム管理者（自己管理者を含む。以下本項において同じ。）の許可を得た場合に限り，ソフトウェアを導入することができる。なお，導入する際は，情報システム管理者は，必要に応じてソフトウェアのライセンスを管理しなければならない。

② 職員等は，不正にコピーしたソフトウェアを利用してはならない。

③ 職員等は，①に基づきソフトウェアを導入する場合において，提供元が真正であることを確認し，提供元が不明瞭なソフトウェアの導入には，マルウェアの混入するリスクがあることを理解し，当該ソフトウェアの第三者による評価の調査等を行い，必要に応じて当該機器を所掌する情報システム管理者への事前相談等を行わなければならない。

(18) 機器構成の変更の制限

職員等は，業務上，端末に対し機器の改造及び増設・交換を行う必要がある場合には，当該機器を所掌する情報システム管理者の許可を得なければならない。

(19) 無許可でのネットワーク接続の禁止

職員等は，機関 CISO が定めた方法による場合を除き，情報セキュリティ責任者又は情報システム管理者の許可なく端末を機構内ネットワークに接続してはならない。

(20) 職務以外の目的でのインターネット利用の禁止

職員等は，機関 CISO が定める場合を除き，機構の情報資産を用いて職務以外の目的でインターネットを利用（WEB の閲覧やインターネット上のサービスの利用を含む。）してはならない。

6.2. アクセス制御

(1) アクセス制御

① アクセス制御等

情報システム管理者は，所掌するネットワーク又は情報システムごとにアクセスす

る権限のない職員等がアクセスできないように，システム上制限しなければならない。

アクセス制御にかかる認証方式について，特に外部サービスにおける認証方式については以下の方式の導入を検討するものとする。

- 二段階認証又は多要素認証方式による主体認証
- 常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ，ゼロトラストセキュリティ等と呼称される。）を用いたセキュリティ設計
- CASB(Cloud Access Security Broker)の導入
- デバイス認証による端末アクセス制御

② 利用者 ID の取扱い

情報システム管理者は，利用者 ID を適切に管理しなければならない。

情報システム管理者は，役職員等及び共同利用・共同研究者等が，異動・退職等により当該身分を失うに至った場合は，原則として 1 月以内に当該利用者 ID の削除又は停止を行うものとする。ただし，必要に応じて機関 CISO は別段の取り扱いを定めることができるものとするが，この場合においては，当該利用者が情報セキュリティインシデントを発生させ，機構に損害を与えた場合等を考慮して適切に定めるとともに，当該利用者から遵守の署名を得る等の対策を講じなければならない。

（ア）情報システム管理者は，利用者の登録，変更，抹消等の情報管理，職員等の異動，出向，退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

（イ）職員等は，業務上必要がなくなった場合は，利用者登録を抹消するよう，情報システム管理者に通知しなければならない。

（ウ）情報システム管理者は，機関 CISO が定める場合を除き，利用されていない ID が放置されないように定期的及び随時に点検しなければならない。

③ 特権を付与された ID の管理等

（ア）情報システム管理者は，管理者権限等の特権を付与された ID を利用する者を必要最小限にしなければならない。

（イ）情報システム管理者は，特権を付与された ID 及びパスワードの変更について，業務委託事業者に行わせてはならない。ただし，契約に基づき管理を委託しているネットワーク及び情報システムにおける当該業務委託事業者が使用する ID 及びパスワードを除く。

（ウ）情報システム管理者は，機関 CISO が定める場合を除き，原則として特権を付与された初期設定の ID（例：Administrator，root など）は無効化しなければならない。ID が無効化できない場合は，5.4.(3)に基づきパスワードを初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

① 職員等は，外部から内部のネットワーク又は情報システムにアクセスする場合は，機関 CISO が定める方法によるものとする。業務上必要であり，機関 CISO が定める方

法では目的を達成できない場合は，情報セキュリティ責任者（独自に LAN を構築している情報システム管理者の当該 LAN に関する事項については，当該情報システム管理者とする。以下本項において同じ。）の許可を得なければならない。

② 情報セキュリティ責任者は，機関 CISO が定める場合を除き，内部のネットワーク又は情報システムに対する外部からのアクセスを，アクセスが必要な合理的理由を有する必要最小限の者に制限しなければならない。

③ 情報セキュリティ責任者は，外部からのアクセスを認める場合，システム上利用者の本人確認を行う機能を確保しなければならない。

④ 情報セキュリティ責任者は，外部からのアクセスを認める場合，通信途上の盗聴を防御するために別紙２「暗号化ガイドライン」に基づく暗号化等の措置を講じなければならない。

⑤ 情報セキュリティ責任者及び情報システム管理者は，テレワーク等を目的として外部からのアクセスに利用するモバイル端末を職員等に貸与する場合，セキュリティ確保のために必要な措置を講じなければならない。

⑥ 職員等は，持ち込んだ又は外部から持ち帰ったモバイル端末を機構内のネットワークに接続する前に，マルウェアやウイルスに感染していないことを，ウイルス対策ソフトウェア等により確認するとともに，セキュリティパッチの適用状況等についても確認しなければならない。

⑦ 情報セキュリティ責任者は，公衆通信回線（移動通信網，公衆無線 LAN 及びインターネット接続サービス等）又はトンネル通信等を，機構内ネットワークに接続することは原則として禁止しなければならない。ただし，やむを得ず接続を許可する場合は，利用者の ID 及びパスワード，生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等，情報セキュリティ確保のために必要な措置等を講じなければならない。

⑧ 職員等は，①の規定に基づく接続である場合を除き，機構外から機構内ネットワークに接続してはならない。

(3) 自動識別の設定

情報システム管理者は，原則としてネットワークで使用される機器について，機器固有情報等によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

(4) ログイン時の表示等

情報システム管理者は，ログイン時におけるメッセージ，ログイン試行回数の制限，アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により，正当なアクセス権を持つ職員等が自身のアカウントが不正に利用されていないことを確認することができるように，可能な限りシステムを設定しなければならない。

(5) パスワードに関する情報の管理

① 情報システム管理者は，職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため，オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は，これを有効に活用しなければならない。

② 情報システム管理者は，機関 CISO が定める場合を除き，原則として職員等に対してパスワードを発行する場合は，仮のパスワードを発行し，ログイン後直ちに仮のパスワードを変更させなければならない。

(6) 特権による接続時間の制限

情報システム管理者は，特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

6.3. システム開発，導入，保守等

(1) 情報システムの調達

① 情報システム管理者は，情報システム開発，導入，保守等の調達に当たっては，調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 情報システム管理者は，情報システムの調達に当たっては，当該製品のセキュリティ機能を調査し，情報セキュリティ上問題のない（ソフトウェアの場合はセキュリティメンテナンスサポート中のものであることを含む。）ことを確認しなければならない。

③ 情報システム管理者は，機器等をリース契約で調達する場合は，契約終了に伴う返却時の情報の抹消方法について，原則として情報資産廃棄ガイドラインに基づき実施されるように仕様に規定するものとし，情報の抹消や廃棄を委託する場合は，その履行状況の確認手段について，以下を例とする対策を行うこと。

（ア）リース契約の調達仕様書に記載し，契約内容にも含める。

（イ）リース契約終了時に伴う情報の抹消について，役務提供契約を別途締結する。

(2) 情報システムの開発

① システム開発における責任者及び作業者の特定

情報システム管理者は，システム開発の責任者及び作業者を特定しなければならない。また，必要に応じてシステム開発のための規約を策定し，関係者間で共有しなければならない。

② システム開発における責任者，作業者の ID の管理

（ア）情報システム管理者は，システム開発の責任者及び作業者が使用する ID を管理し，開発完了後，開発用 ID を削除しなければならない。

（イ）情報システム管理者は，システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③ システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は，システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）情報システム管理者は，利用を認めたソフトウェア以外のソフトウェアが導入されている場合，アンインストール又はオペレーティングシステムのロールバック等により，当該ソフトウェアをシステムから排除しなければならない。

(3) 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は，原則としてシステム開発，保守及びテスト環境とシステム運用環境を分離しなければならない。

（イ）情報システム管理者は，システム開発・保守及びテスト環境からシステム運用環境への移行について，システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ）情報システム管理者は，移行の際，情報システムに記録されている情報資産の保存を確実に行い，移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（エ）情報システム管理者は，導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

② テスト

（ア）情報システム管理者は，新たに情報システムを導入する場合，既に稼働している情報システムに接続する前に開発した組織と導入する組織がそれぞれ独立した受入テストを行う等，十分な試験を行わなければならない。

（イ）情報システム管理者は，運用テストを行う場合，原則としてあらかじめ擬似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は，個人情報及び機密性の高い情報を，テストデータに使用してはならない。

③ 脆弱性等の点検

情報システム管理者は，導入する情報システムの脆弱性に関して以下の点検を行わなければならない。

（ア）情報システムで使用されているソフトウェア（組込のソフトウェア部品の場合もある。）のバージョンを確認し，脆弱性が無いこと，EOL（End Of Life）ではないことを確認する。

（イ）ソフトウェアに包含されているサンプルプログラム（特に Web サーバのフレームワークなど）について，不要であれば削除する等，無効化する。

（ウ）必要に応じて，脆弱性診断ツール等を用いた診断を行う。

④ 導入時の対策

情報セキュリティ管理者及び情報システム管理者は，機密性３以上の情報を保管す

る情報システムを導入（格付を変更する場合を含む。）する際は，機器の盗難，情報の不正な持ち出し，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連帯して講じるものとする。

(4)　システム開発・保守に関連する資料等の整備・保管

情報システム管理者は，以下の資料等を取得・作成し，適切に保管しなければならない。

① システム開発・保守に関連する資料及びシステム関連文書

② システムのテスト結果（一定期間保管）

③ 情報システムに係るソースコード

④ 情報システムに使用されているソフトウェアの管理簿

情報システム管理者には，情報システム（自ら開発するもの及び委託により開発するものを含む。）の構築時にソフトウェアを効率的に開発するために使用するソフトウェアフレームワークやソフトウェア部品が情報システムに組み込まれて納入される場合があることを考慮のうえ，これらについても脆弱性対策の状況を随時又は定期的に確認することが求められる。これを確実に実施するための管理簿を作成しておくことが望ましい。

(5)　情報システムにおける入出力データの正確性の確保

① 情報システム管理者は，情報システムに入力されるデータについて，範囲，妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 情報システム管理者は，故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に，これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③ 情報システム管理者は，情報システムから出力されるデータについて，情報の処理が正しく反映され，出力されるように情報システムを設計しなければならない。

(6)　情報システムの変更管理

情報システム管理者は，情報システムを変更した場合，プログラム仕様書等の変更履歴を必要に応じて作成しなければならない。

(7)　開発・保守用のソフトウェアの更新等

情報システム管理者は，開発・保守用のソフトウェア等を更新，又はパッチの適用をする場合，他の情報システムとの整合性を確認しなければならない。

(8)　システム更新又は統合時の検証等

情報システム管理者は，システム更新・統合時に伴うリスク管理体制の構築，移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6.4. 不正プログラム対策

(1) 情報セキュリティ責任者の措置事項

情報セキュリティ責任者は，基幹及び共通ネットワークにおける不正プログラム対策として，次の事項を措置しなければならない。

① 外部ネットワークから受信したファイルは，インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い，不正プログラムのシステムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは，インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い，不正プログラムの外部への拡散を防止しなければならない。

③ 攻撃に用いられる C&C サーバについて情報を収集し，FW，IPS，Proxy，GW 等を用いて外部への通信を制限する（C&C サーバへの接続拒否を含む。）等の出口対策を実施しなければならない。

④ コンピュータウイルス等の不正プログラム情報を収集し，必要に応じ職員等に対して注意喚起しなければならない。

⑤ 所掌するサーバ及び端末に，原則として（メインフレームや一部のスマートフォンなど，不正プログラム対策ソフトウェアが提供されていない場合を除く。以下 6.4 において同じ。）コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。また，不正プログラム対策ソフトウェアのパターンファイルは，常に最新の状態に保たなければならない。

⑥ 業務で利用するソフトウェアは，スタンドアロン又は完全に隔離されたネットワーク内で使用する場合を除き，パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。ただし，次に掲げる場合を除く。

（ア）重要なサーバについては情報システム管理者が必要と考えるセキュリティ対策を提示し，情報セキュリティ責任者の承認を得た場合

（イ）重要なサーバ以外については，情報システム管理者が必要と考えるセキュリティ対策を行う場合

⑦ 情報セキュリティ責任者は，前記により承認した情報システムについては，これを把握し，定期的に運用状況を確認しなければならない。

(2) 情報システム管理者の措置事項

情報システム管理者は，不正プログラム対策に関し，次の事項を措置しなければならない。

① 情報システム管理者は，その所掌するサーバ及び端末に，原則としてコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

② 不正プログラム対策ソフトウェアはメーカーのサポート期間内のものとし，そのパターンファイルは，常に最新の状態に保たなければならない。

③ 情報システム管理者は，インターネットに接続していないシステムにおいて，電磁的記録媒体を使う場合，コンピュータウイルス等の感染を防止するために，自身が管理している媒体以外を職員等に利用させない等，必要な措置を講じなければならない。また，不正プログラムの感染，侵入が生じる可能性が著しく低い場合（メインフレームや一部のスマートフォンなど，不正プログラム対策ソフトウェアが提供されていない場合を含む。）を除き，不正プログラム対策ソフトウェアを導入し，定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

④ 必要に応じて，端末及びサーバの活動を監視し，不正プログラム等の検知や対処を行う EDR（Endpoint Detection and Response（エンドポイントでの攻撃検出対応））ソフトウェアの導入及び MSS（Managed Security Service）を利用した SOC（Security Operation Center）業務の委託を検討しなければならない。

(3) 職員等の遵守事項

職員等は，不正プログラム対策に関し，次の事項を遵守しなければならない。

① 端末において，不正プログラム対策ソフトウェアが導入されている場合は，情報システム管理者の承諾がある場合を除き，当該ソフトウェアの設定を変更してはならない。

② 外部からデータ又はソフトウェアを取り入れる場合には，原則として不正プログラム対策ソフトウェアによるチェックを行わなければならない。ただし，これが困難な場合において，不正プログラム等による問題が生じないことが合理的に説明できる場合を除く。また，ソフトウェアを取り入れる場合は，6.1.(17)の規定を遵守しなければならない。

③ 以下に掲げるメールを受信（メールフィルタ等により迷惑メールとマークされたり，隔離されたりした場合を除く。）した場合は，直ちに機関統一窓口へ報告し，指示に従うものとする。

- 自身では容易に判断できない疑わしいメール
- メールの内容（本文に自機関の名前が記載されている，本文に記載された URL が自機関のドメインを誤認させるなど）から判断して自組織を標的としていると考えられるメール
- その他，自組織において危険であると考えられるメール

④ 端末に対して，不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。ただし，情報システム管理者が不要であると判断した場合を除く。（シンクライアントで読み取り専用ドライブの場合などが想定される。）

⑤ 添付ファイルが付いた電子メールを送受信する場合は，不正プログラム対策ソフトウェアでチェックを行わなければならない。なお，暗号化されたファイルの場合は，復号化しなければチェックできない点に留意し，前記②に基づきチェックしなければならない。

⑥ 情報セキュリティ責任者及び機関 CSIRT 等が提供する不正プログラムに関する情報

を，常に確認しなければならない。

⑦ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は，速やかに機関統一窓口へ報告を行い，その指示に従いながら，状況の保存とともに必要に応じて以下の対応を行わなければならない。

（ア）有線 LAN に接続する機器の場合

LAN ケーブルの即時取り外しを行わなければならない。

（イ）無線 LAN により通信を行う機器の場合

無線 LAN を切断するなど，直ちに利用を中止し，通信を行わない設定への変更を行わなければならない。

(4) 専門家の支援体制

情報セキュリティ責任者は，実施している不正プログラム対策では不十分な事態が発生した場合に備え，外部の専門家の支援を受けられるようにしておかなければならない。

6.5. 不正アクセス対策

(1) 情報セキュリティ責任者及び情報システム管理者の措置事項

情報セキュリティ責任者及び情報システム管理者は，不正アクセス対策として，必要に応じて以下の事項を措置しなければならない。

① 情報システムにおける使用しないポートは，原則としてこれを閉鎖又は利用不能にしなければならない。

② 不要なサービスについて，機能を削除又は停止しなければならない。

③ ウェブサーバに関しては，不正アクセスによるウェブページの改ざんを防止するために，不正アクセス検出ツールや，データの書換えを検出し情報セキュリティ責任者及び情報システム管理者へ通報するように設定するなど，適切な対策を講じなければならない。

④ 重要なシステム設定ファイル等について，定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤ 情報セキュリティ責任者は，機関統一窓口と連携し，監視，通知，外部報告窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

(2) 攻撃の予告

機関 CISO 及び情報セキュリティ責任者は，サーバ及び通信回線装置に攻撃を受けることが明確になった場合，当該システムの停止を含む必要な措置を講じなければならない。また，関係機関と連絡を密にして情報の収集に努めなければならない。

(3) 記録の保存

機関 CISO 及び情報セキュリティ責任者は，サーバ及び通信回線装置に攻撃を受ける等，当該攻撃が不正アクセス禁止法違反等の犯罪（ソーシャル・エンジニアリングによ

るもの等を含む）の可能性がある場合には，必要に応じて攻撃の記録を保存するとともに，警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

基幹ネットワークを管理している情報システム管理者は，LAN に接続している端末からの LAN 内のサーバ及び通信回線装置に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

情報セキュリティ責任者及び情報システム管理者は，職員等による不正アクセスを発見した場合は，当該職員等が所属する課室等の情報セキュリティ管理者に通知し，適切な処置を求めなければならない。

(6) サービス不能攻撃

情報セキュリティ責任者及び情報システム管理者は，外部からアクセスできる情報システムに対して，第三者からサービス不能攻撃（DoS，DDoS，smarf，SYN フラッド，DNS amp 等をいう。）を受け，利用者がサービスを利用できなくなることを防止するため，情報システムの可用性を確保する対策を可能な限り講じなければならない。

(7) 標的型攻撃

情報セキュリティ責任者及び情報システム管理者は，情報システムにおいて，標的型攻撃による内部への侵入を防止するために，役職員等への教育や注意喚起，OS のポリシー設定等による自動再生無効化等の人的対策や入口対策を講じなければならない。また，内部に侵入した攻撃を早期検知して対処するために，通信をチェックする等の内部対策を講じなければならない。

(8) DDoS（Distributed Denial of Service）対策

重要なコンテンツサーバ（ウェブサーバを含む）については，コンテンツデリバリーネットワーク（CDN）サービスの利用を検討する。

6.6. セキュリティ情報の収集・脆弱性対策

(1) 脆弱性に関する情報の収集・共有及びソフトウェアの更新等

情報セキュリティ責任者及び情報システム管理者は，コンピュータソフトウェア等の脆弱性に関する情報を収集し，必要に応じ，関係者間で共有しなければならない。また，当該脆弱性の緊急度・深刻度に応じて，以下の対策を実施しなければならない。

① セキュリティパッチが提供されている場合はこれを適用する。ハイリスクの場合は，原則として直ちに適用しなければならない。ただし，セキュリティパッチの適用に大きなリスクを伴う場合（ベンダーや保守請負者が適用を推奨しない場合を含む）は，当該脆弱性の緩和策を実施し，脆弱性が解消されるまでリスク管理を行うものとする。

② セキュリティパッチが提供されていない場合は，当該脆弱性の緩和策を実施する。

③ ハイリスクな脆弱性に対し，セキュリティパッチが提供されておらず，対策も取り得ない場合は，システムを停止する。

(2) 不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ責任者は，不正プログラム等のセキュリティ情報を収集し，必要に応じ対応方法について，職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

情報セキュリティ責任者及び情報システム管理者は，情報セキュリティに関する情報を収集し，必要に応じ，関係者間で共有しなければならない。また，情報セキュリティに関する社会環境や技術環境等の変化によって，所掌する情報資産に対して新たな脅威を認識した場合は，セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

(4) 機関 CSIRT による情報の収集及び共有

機関 CSIRT は，コンピュータソフトウェアの脆弱性，不正プログラム等のセキュリティ情報及び情報セキュリティに関する幅広い情報を収集・分析し，必要に応じて所掌組織内への注意喚起及び情報提供を行わなければならない。また，必要に応じて各機関 CSIRT 間で情報共有を行うものとする。

7. 運用

7.1. 情報システムの監視

① 情報セキュリティ責任者及び情報システム管理者は，セキュリティに関する事案を検知するため，機密性３以上の情報システムについては，連携してこれを常時監視しなければならない。

② 情報セキュリティ責任者及び情報システム管理者は，連携してログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は，連携して外部 WAN と常時接続するシステムを常時監視しなければならない。

7.2. ネットワークの監視

① 基本規程第２３条第１項に定めのあるネットワーク監視者（以下「ネットワーク監視者」という。）を除き，役職員等はネットワークの通信データを傍受・監視してはならない。ただし，ネットワーク監視者は，配下の情報システム担当者に対して自己の権限に基づき，ネットワークの通信データの傍受・監視を行わせることができる。

② 基本規程第２３条第２項に定める対策基準で定める場合とは，機構又は機構外に対する重大なセキュリティ侵害を防止するために CISO 又は機関 CISO が認めた場合とし，伝達可能な範囲は必要最小限とし，被伝達者について，他者への伝達を禁止するとと

もに，伝達内容，伝達先を記録しなければならない。

③ 前規定にかかわらず，機構又は機構外に対する重大なセキュリティ侵害を防止するために緊急を要す場合，ネットワーク監視者は自己の判断により対応することができる。ただし，事後に CISO 又は機関 CISO の承認を得なければならない。

7.3. 情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

① 情報セキュリティ責任者及び情報セキュリティ管理者は，情報セキュリティポリシーの遵守状況について確認を行い，問題を認めた場合には，速やかに機関 CISO に報告しなければならない。

② 機関 CISO は，発生した問題について，適切かつ速やかに対処しなければならない。

③ 情報システム管理者は，ネットワーク，サーバ及び通信回線装置のシステム設定等における情報セキュリティポリシーの遵守状況について，定期的に確認を行い，問題が発生していた場合には適切かつ速やかに対処しなければならない。

(2) 端末及び電磁的記録媒体等の利用状況調査

情報セキュリティ責任者（情報セキュリティ責任者から調査を行う者として指名された者を含む。）及び機関 CSIRT は，不正アクセス，不正プログラム等の調査のために，職員等が使用している端末及び電磁的記録媒体等のログ，電子メールの送受信記録等の利用状況を調査することができる。

(3) 職員等の報告及び協力義務

① 職員等は，情報セキュリティポリシーに対する違反行為を発見した場合，直ちに機関統一窓口に報告を行わなければならない。

② 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ責任者が判断した場合は，緊急時対応計画に従って適切に対処しなければならない。

③ 職員等は，情報セキュリティポリシーに基づき実施する情報セキュリティ監査責任者，情報セキュリティ監査実施者，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及び情報システム管理者の調査等に対して，即時に協力・対応する義務を負う。

④ 職員等は，自己の保有する技術上の専門的知識等について，情報セキュリティ責任者及び機関 CSIRT から協力を依頼された場合は，協力する義務を負う。

⑤ 情報セキュリティ監査室が行う監査業務（外注により実施する脆弱性検査を含む。）について，役職員等は協力する義務を負う。

7.4. 侵害時の対応等

(1) 緊急時対応計画の策定

機関 CISO は，情報セキュリティインシデント，情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置を迅速かつ適切に実施するために，緊急時対応計画を定めておき，セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には，以下の内容を定めなければならない。

① 関係者の連絡先
② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

(3) 事業継続計画との整合性確保

CISO は，自然災害，大規模・広範囲にわたる疾病等に備えて策定された自然科学研究機構事業継続計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

機関 CISO は，情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ，必要に応じて緊急時対応計画を見直さなければならない。

7.5. 例外措置

(1) 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は，情報セキュリティ関係規定を遵守することが困難な状況で，機構の運営等事務の適正な遂行を継続するため，遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には，機関 CISO の許可を得て，例外措置を取ることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は，機構業務の遂行に緊急を要する等の場合であって，例外措置を実施することが不可避のときは，当該措置の実施後速やかに機関 CISO に報告しなければならない。

(3) 例外措置の申請書の管理

機関 CISO は，例外措置の申請書及び審査結果を適切に保管し，定期的に申請状況を確認しなければならない。

7.6. 法令遵守

職員等は，職務の遂行において使用する情報資産を保護するために，関係法令，並びに機構が定める諸規程を遵守し，これに従わなければならない。

特に，下記の法令及び機構が定める規程に注意すること。

① 著作権法（昭和４５年法律第４８号）
② 不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
③ 個人情報の保護に関する法律（平成１５年法律第５７号）
④ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）
⑤ 刑法（明治４０年法律第４５号）におけるコンピュータ犯罪防止法
⑥ 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成１３年法律第１３７号）
⑦ 特定電子メールの送信の適正化等に関する法律（平成１４年法律第２６号）
⑧ 大学共同利用機関法人自然科学研究機構個人情報保護規程（平成１７年自機規程第５４号）
⑨ 大学共同利用機関法人自然科学研究機構特定個人情報取扱規程（平成２７年自機規程第１０６号）

そのほか，個人情報を電子的に収集・管理する場合においては，次の点を遵守すること。

・ 個人情報の保護に関する法律及び大学共同利用機関法人自然科学研究機構個人情報保護規程の規定に基づき収集時に利用目的を明示しなければならない。
・ 利用目的には情報の取扱いが分かるように記載し，本人の同意を得るものとする。
・ 電子的手段以外で収集した個人情報は，利用目的を達成する範囲でのみ電子化することができる。

7.7. 懲戒処分等

(1) 懲戒処分等

① 情報セキュリティポリシーに違反した職員等及びその監督責任者は，その重大性，発生した事案の状況等に応じて，機構の就業規則による懲戒処分の対象とする。
② 共同利用・共同研究者等が，故意又は重過失により情報セキュリティポリシーに違反し，機構に損害を与えた場合は，当該事案にかかる機構が被った損害額について，契約等に基づき損害賠償請求を行う場合がある。また，当該共同利用・共同研究者等の監督責任者は，その重大性，発生した事案の状況等に応じて，機構の就業規則による懲戒処分の対象とする。
③ 情報セキュリティ監査責任者，情報セキュリティ監査実施者，CSIRT の職務遂行に対

して，役職上の立場を利用した妨害行為やハラスメント，強要等を行った職員等は，その重大性等を勘案し，機構の就業規則による懲戒処分の対象とする。ただし，情報セキュリティ監査責任者，情報セキュリティ監査実施者，CSIRT は，合理的な説明責任を負うものとし，緊急を要すると判断した場合における関係者への詳細な説明は，事後であっても構わないものとする。

④ 機関 CISO 及び情報セキュリティ責任者の職務遂行に対し，在職中の立場や社会的立場を背景とした妨害行為やハラスメント，強要等を行った共同利用・共同研究者等は，CISO 又は機関 CISO から指示された場合には，自然科学研究機構の情報資産の使用を停止するとともに，保管している自然科学研究機構の情報を削除又は返還をしなければならない。ただし，当該措置に不服がある時は，当該措置が無効である根拠を明示して CISO へ申し立てを行うことができる。

(2) 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には，速やかに次の措置を講じなければならない。

① 情報セキュリティ責任者が違反を確認した場合は，情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し，適切な措置を求めなければならない。

② 情報システム管理者等が違反を確認した場合は，違反を確認した者は速やかに情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し，適切な措置を求めなければならない。

③ 情報セキュリティ管理者の指導によっても改善されない場合，情報セキュリティ責任者は，当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに，情報セキュリティ責任者は，職員等の権利を停止又は剥奪した旨を機関 CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

8. 外部委託

本項については、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（令和３年度版）第４部 外部委託の各項目における「目的・趣旨」に準じるものである。

8.1. 業務委託

(1) 業務委託事業者の選定基準

① 情報セキュリティ管理者及び情報システム管理者は，業務委託事業者の選定に当たり，委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 情報セキュリティ管理者及び情報システム管理者は，情報セキュリティマネジメントシステムの国際規格の認証取得状況，情報セキュリティ監査の実施状況等を参考にし

て，事業者を選定しなければならない。

③ 情報セキュリティ管理者及び情報システム管理者は，クラウドサービスを利用する場合は，ISMAP 等を参考とし当該サービスで取り扱う情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

④ 基本規程別表第１「機密性による情報資産の分類」の機密性４及び機密性３分類における取扱制限に基づき，機関 CISO の許可により業務委託を行おうとする場合は，自機関で当該業務を行うことに比して同等又はそれ以上の情報セキュリティが担保される事が確認できることを示した書類を提示したうえで，機関 CISO の許可を得なければならない。また，当該委託に個人情報又は特定個人情報が含まれている場合は，大学共同利用機関法人自然科学研究機構個人情報保護規程（平成１７年自機規程第５４号）及び大学共同利用機関法人自然科学研究機構特定個人情報取扱規程（平成２７年自機規程第１０６号）を遵守できるものでなければならない。

(2) 契約項目

情報セキュリティ責任者，情報セキュリティ管理者及び情報システム管理者は，情報システムの運用，保守等を業務委託する場合には，業務委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約が締結されるようにしなければならない。

・機構の情報セキュリティポリシー等の遵守
・業務委託事業者における情報セキュリティ対策の実施内容及び管理体制
・委託事業者の実施に当たり，委託先企業若しくはその従業員，再委託先又はその他の者によって，機構の意図せざる変更が加えられないための管理体制
・業務委託事業者の資本関係・役員等の情報，業務委託事業の責任者及び委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報，委託内容，委託事業の実施場所・作業場所の特定
・提供されるサービスレベルの保証
・業務委託事業者にアクセスを許可する情報の種類と範囲，アクセス方法
・業務委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還，廃棄等
・委託業務の定期報告及び緊急時報告義務
・委託業務事業者の情報セキュリティインシデントへの対処方法
・委託業務事業者の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，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
・機構による監査，検査の受け入れ
・機構による情報セキュリティインシデント発生時の公表

・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

(3) 再委託の可否

情報セキュリティ責任者，情報セキュリティ管理者及び情報システム管理者は，委託業務事業者がその役務内容を一部再委託する場合は，再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう，上記契約項目の措置の実施を事業者に担保させるとともに，再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し，機構の承認を受けるよう，仕様内容に含めること。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こと。

(4) 業務委託における対策の確認・措置等

情報セキュリティ管理者及び情報システム管理者は，業務委託事業者において，以下に掲げる点を，機密性２の情報資産については必要に応じて，機密性３以上の情報資産については必ず，定期的に確認し，必要に応じて前記契約項目の契約に基づき措置するとともに，その内容を情報セキュリティ責任者に報告しなければならない。また，情報セキュリティ責任者は，報告内容の重要度を鑑み，必要に応じて機関 CISO に報告しなければならない。

① 契約に基づき，委託先における情報セキュリティ対策の履行状況を確認すること。
② 委託した業務において，情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合は，委託事業を一時中断するなどの必要な措置を講じた上で，契約に基づく対処を委託先に講じさせること。
③ 委託した業務の終了時に，委託先において取り扱われた情報が確実に返却，又は抹消されたことを確認すること。

(5) 業務委託における情報の取扱い

職員等は，委託先への情報の提供等において，以下の事項を遵守すること。

① 委託先に要保護情報を提供する場合は，提供する情報を必要最小限とし，あらかじめ定められた安全な受渡し方法により提供すること。
② 提供した要保護情報が委託先において不要になった場合は，これを確実に返却又は抹消させること。
③ 委託業務において，情報セキュリティインシデント，情報の目的外利用等を認知した場合は，速やかに情報セキュリティ責任者，情報セキュリティ管理者又は情報システム管理者に報告すること。

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

(1) 外部サービスの利用承認及び外部サービス管理者の指名

① 情報セキュリティ責任者及び又は情報セキュリティ管理者は，外部サービスを利用する場合には，機関 CISO の承認を得ること。

② 機関 CISO は，外部サービスの利用申請を承認した場合は，承認済み外部サービスとして記録し，当該サービスの運用・管理を目的として，外部サービス管理者を指名しなければならない。

(2) 外部サービス導入時の対策

基本規程別表第１「機密性による情報資産の分類」の取扱制限に定める機関ＣＩＳＯの許可に基づき，外部サービスで機密性３以上の情報を扱う場合，機関ＣＩＳＯは，6.3(3)④と同等の対策が実施されることを確認するものとする。

(3) 外部サービスの利用に係る規定の整備

① 機関 CISO は，以下を含む外部サービス（要機密情報を取り扱う場合）の利用に関する規定を整備すること。

（ア）外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）

（イ）外部サービス提供者の選定基準

本選定基準は，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）クラウドサービスリストに掲載されているサービスとし，当該サービス以外を選定する場合に整備するものとする。

（ウ）外部サービスの管理及び利用手続

機関 CISO は，外部サービス管理者を指名した場合は，当該外部サービス管理者に委任することができる。

(4) 外部サービス（クラウドサービス）（以下「クラウド外部サービス」という。）の選定

① 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，取り扱う情報の格付及び取扱制限を踏まえ，外部サービス利用判断基準に従ってクラウド外部サービスの利用を検討すること。

② 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，クラウド外部サービスで取り扱う情報の格付及び取扱制限を踏まえ，外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また，業務に特有のリスクが存在する場合には，必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

③ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，取り扱う情報の格付及び取扱制限並びに外部サービス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セキュリティ要件を定め，クラウド外部サービスを選定すること。

(5) 外部サービス（クラウドサービス以外）（以下「非クラウド外部サービス」という。）の選定

① 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，取り

扱う情報の格付及び取扱制限を踏まえ，外部サービス利用判断基準に従って非クラウド外部サービスの利用を検討すること。

② 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，非クラウド外部サービスで取り扱う情報の格付及び取扱制限を踏まえ，外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また，以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

（ア）外部サービスの利用を通じて機構が取り扱う情報の外部サービス提供者における目的外利用の禁止

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

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

（エ）外部サービス提供者の資本関係・役員等の情報，非クラウド外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績に関する情報提供

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，非クラウド外部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を検討し，外部サービス提供者の選定条件に含めること。

④ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，非クラウド外部サービスの利用を通じて機構が取り扱う情報の格付等を勘案し，必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，非クラウド外部サービスの利用を通じて機関等が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し，必要に応じて機関等の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

⑥ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，外部サービス提供者がその役務内容を一部再委託する場合は，再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう，外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに，再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し，機構の承

認を受けるよう，外部サービス提供者の選定条件に含めること。また，外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，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，非クラウド外部サービスを選定すること。また，非クラウド外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

⑧ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，非クラウド外部サービスの特性を考慮した上で，非クラウド外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう，情報の流通経路全般を見渡した形でセキュリティ設計を行った上で，情報セキュリティに関する役割及び責任の範囲を踏まえて，セキュリティ要件を定めること。

⑨ 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，情報セキュリティ監査による報告書の内容，各種の認定・認証制度の適用状況等から，外部サービス提供者の信頼性が十分であることを総合的･客観的に評価し判断すること。

(6) 外部サービスの利用に係る調達・契約

① 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，外部サービスを調達する場合は，外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

② 情報セキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，外部サービスを調達する場合は，外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し，調達仕様の内容を契約に含めること。

(7) 外部サービスを利用した情報システムの導入・構築時の対策

① 機関 CISO は，外部サービスの特性や責任分界点に係る考え方等を踏まえ，以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

② 外部サービス管理者は，前項において定める規定に対し，構築時に実施状況を確認・記録すること。

(8) 外部サービスを利用した情報システムの運用・保守時の対策

① 機関 CISO は，外部サービスの特性や責任分界点に係る考え方を踏まえ，以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定するこ

と。

（ア）外部サービス利用方針の規定

（イ）外部サービス利用に必要な教育

（ウ）取り扱う資産の管理

（エ）不正アクセスを防止するためのアクセス制御

（オ）取り扱う情報の機密性保護のための暗号化

（カ）外部サービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）外部サービスを利用した情報システムの事業継続

② 情報システムセキュリティ責任者，情報セキュリティ管理者及び外部サービス管理者は，外部サービスの特性や責任分界点に係る考え方を踏まえ，外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

③ 外部サービス管理者は，前各項において定める規定に対し，運用・保守時に実施状況を定期的に確認・記録すること。

(9) 外部サービスを利用した情報システムの更改・廃棄時の対策

① 機関 CISO は，外部サービスの特性や責任分界点に係る考え方を踏まえ，以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

（ア）外部サービスの利用終了時における対策

（イ）外部サービスで取り扱った情報の廃棄

（ウ）外部サービスの利用のために作成したアカウントの廃棄

② 外部サービス管理者は，前項において定める規定に対し，外部サービスの利用終了時に実施状況を確認・記録すること。

8.3. 外部サービスの利用（機密性１の情報のみを取り扱う場合）（以下「パブリック外部サービス」という。）

(1) パブリック外部サービスの利用に係る規定の整備

① 機関 CISO は，機構としてパブリック外部サービスに外部サービス管理者を指名する場合など，必要であると認められた場合は，以下を含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備すること。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの管理及び利用手続

(2) パブリック外部サービスの利用上の注意点

① 役職員等は，利用する外部サービスの約款，その他の提供条件等から，利用に当たってのリスクが許容できることを確認するとともに，当該外部サービス利用上の責任を負うことを理解した上で，約款による外部サービスの利用を外部サービス提供者に申請し，適切な措置を講じた上で利用しなければならない。

8.4. 外部サービス（ソーシャルメディアサービス）の利用

① 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サービスを利用する場合，情報セキュリティ対策に関して下記の対策を講じるとともに，必要に応じてソーシャルメディアサービス運用手順を定めるものとする。

（ア）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ことを明らかにするために，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とともに，当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で，不正アクセス対策を行うこと

② ソーシャルメディアサービスで発信できる情報は，機密性１の情報に限る。

③ 情報セキュリティ責任者は，利用するソーシャルメディアサービスの責任者を定めなければならない。

9. 評価・見直し

9.1. 監査対応

(1) 監査実施計画の立案及び実施への協力

被監査部門は，監査の実施に協力しなければならない。

(2) 監査結果への対応

CISO は，監査結果に基づく指摘事項を踏まえ，所管する機関 CISO 及び情報セキュリティ責任者に対し，当該指摘事項への対処を指示しなければならない。また，指摘事項を所管していない情報セキュリティ責任者に対しても，同種の課題及び問題点がある可能性が高い場合には，当該課題及び問題点の有無を確認させなければならない。また，機関 CISO は，必要に応じて，情報セキュリティ管理者及び情報システム管理者に対する適切な措置を講じるものとする。

(3) 情報セキュリティポリシー及び関係規程等の見直し等への活用

CISO 及び機関 CISO 並びに情報セキュリティ委員会は，監査結果を情報セキュリティポリシー等の見直し，その他情報セキュリティ対策の見直し時に活用しなければならない。

9.2. 自己点検

(1) 定期自己点検計画

基本規程第２６条に基づき，機関 CISO は，情報システム管理者，情報セキュリティ管理者，役職員等及び共同利用・共同研究者等が行う自己点検計画（点検項目等を含む。）を定め，情報セキュリティポリシー等の遵守状況等について，自己点検（以下「定期自

己点検」という。）を毎年度１回以上行わせるものとする。

ただし，共同利用・共同研究者等の定期自己点検の実施については，機関 CISO の判断により，一部又は全部について省略することができる。

(2) 情報システム管理者及び情報セキュリティ管理者の自己点検

① 情報システム管理者は，定期自己点検を実施した場合は，所掌するネットワーク，情報システム（外部電磁的記録媒体を除く）及び外部電磁的記録媒体の一覧（情報資産台帳及び外部電磁的記録媒体管理台帳を用いることができる。)に自己点検結果を記し，問題が見つかった場合は改善策を付記のうえ，機関 CISO へ報告しなければならない。

② 情報セキュリティ管理者は，定期自己点検を実施した場合は，その結果を記すとともに，問題が見つかった場合は改善策を付記のうえ，機関 CISO へ報告しなければならない。

③ 情報システム管理者及び情報セキュリティ管理者は，必要に応じて随時に自己点検を行うものとし，問題が見つかった場合は改善策を付記のうえ，機関 CISO へ報告しなければならない。

④ 情報システム管理者及び情報セキュリティ管理者は，役職員等及び共同利用・共同研究者等から情報セキュリティ上の問題等について報告があった場合は，必要に応じて改善を図るとともに，機関 CISO へ報告しなければならない。

(3) 役職員等及び共同利用・共同研究者等の自己点検

① 役職員等は，定期自己点検及び随時に自己点検を行わなければならない。また，情報セキュリティ上の問題となる(可能性を含む)点について気付いた事項がある場合は，情報セキュリティ管理者又は情報システム管理者へ報告するものとする。

② 共同利用・共同研究者等は，定期自己点検（機関 CISO から実施の指示があった場合に限る）及び随時に自己点検を行うものとし，点検結果に基づき，自己の権限の範囲内で改善を図らなければならない。また，情報セキュリティ上の問題となる（可能性を含む）点について気付いた事項がある場合は，情報システム管理者又は情報セキュリティ管理者へ報告するものとする。

(4) 定期自己点検結果報告

機関 CISO は，定期自己点検の結果報告を取り纏め，機関情報セキュリティ委員会に報告するものとする。

(5) 自己点検結果の活用

① 役職員等は，自己点検の結果に基づき，自己の権限の範囲内で改善を図らなければならない。

② 機関 CISO 及び機関情報セキュリティ委員会は，この点検結果を所掌の情報セキュリティポリシー等の見直し，その他情報セキュリティ対策（研修等を含む。）の見直し時に活用しなければならない。

③ 機関 CISO は，自己点検に基づく点検結果及び対策について，CISO に報告しなければならない。

④ CISO は，基本規程第２７条に基づき，情報セキュリティポリシー及び実施規則の見直しを行うものとする。

9.3. 情報セキュリティポリシー及び関係規程等の見直し

CISO，機関 CISO，情報セキュリティ委員会及び機関情報セキュリティ委員会は，情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ，情報セキュリティ体制を含む情報セキュリティポリシー等について毎年度及び重大な変化が発生した場合は随時に評価を行い，必要があると認めた場合，改善を行うものとする。

情報セキュリティポリシー等の見直しにあたっては，機密性３以上の重要情報の洗い出しを徹底しこれらを把握するとともに，リスク評価と分析に基づき，セキュリティ対策方針を定め，実施するものとする。

10. 附 記

(1) 大学共同利用機関法人自然科学研究機構情報システム運用基準（平成２０年４月１日情報化統括責任者決定）は，廃止する。

(2) 本対策基準は，特に定めのある場合を除き，平成２８年９月２３日から施行する。

(3) 前項にかかわらず，施行日以前に運用・稼動している情報資産にかかる設定等について，本対策基準を適用することが困難な場合（多額に費用がかかる場合を含む。）は，機密性３以上の情報を保存している情報資産及び特に定めのある場合を除き，本対策基準の適用を平成３０年３月３１日まで猶予するものとする。ただし，可能な限り速やかに改善する努力を払うとともに，情報セキュリティについて注意を払わなければならない。

(4) 本対策基準の重要サーバ管理者にかかる規定，及び別紙２「暗号化ガイドライン」については，２０２０年４月１日から適用するものとする。ただし，これより早期に適用することを妨げない。

別紙１

情報資産廃棄ガイドライン

情報資産を廃棄する場合は，以下いずれかの方法によらなければならない。

１）物理的破壊

破砕・溶解・焼却等，情報資産を物理的に破壊し，復旧を不可能とする方法。

２）論理的破壊（データ破壊）

記録されている磁気等による情報を，消磁等により破壊し，復旧を不可能とするもの。

米国国家安全保障局方式（NSA）又は米国陸軍方式（複数回の乱数・ヌルデータを複数回書き込み，ベリファイする等）等，一般にデータを抹消することが確認された手法を用いて情報を破壊する機能を有するソフトウェアやハードウェアを用いて，情報の復元を不可能とする方法。

ただし，USB メモリ等の半導体メモリについては，確実に論理的破壊が保障されない限り，物理的破壊によらなければならない。

３）論理的破壊（暗号化キーの廃棄）

十分な強度で暗号化（「暗号化ガイドライン」に準拠するものとする。）されている情報について，当該暗号化キーを廃棄することにより復旧を不可能とするもの。

前項の１）物理的破壊 及び ２）論理的破壊（データ破壊）が困難な場合（人事異動等で再度使用する場合を含む）において，記録されている情報（過去に記録した情報を含む）が機密性３以下の情報であり，かつ十分な強度を有す暗号化手法にて暗号化されている場合は，暗号化キーを完全に消去又は廃棄し，併せて当該媒体を初期化（フォーマット等）することにより，論理的破壊が行われたこととして取り扱うものとする。

補足：本ガイドラインにおける「物理的破壊」及び「論理的破壊（データ破壊）」について具体的な方法として，以下に例示する。

■ 物理的破壊

- 媒体を物理的に破壊する方法
  - フロッピーディスク等の磁気媒体の場合
    当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法。
  - USB メモリ，SSD 等のフラッシュメモリ媒体の場合
    当該媒体を切断するなどして情報を記録している内部のメモリチップを破壊する方法。（この方法を用いる場合，ハードディスク向けの一般的な物理的破壊方法では，裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できな

いことに注意が必要である。）

- CD-R/RW，DVD-R/RW 等の光学媒体の場合
  カッター等を利用してラベル面側から同心円状に多数の傷を付け，情報を記録している記録層を破壊する方法
- 媒体全般
  メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法

■ 論理的破壊（データ破壊）

一般的には「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり，ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態にある。電磁的記録媒体に記録されている情報を抹消するための方法としては，例えば，次の方法が挙げられる。

- データ抹消ソフトウェア（もとのデータに異なるランダムなデータを１回以上上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法。
  この方法を用いる場合，ソリッドステートドライブ（以下「SSD」という。）等のフラッシュメモリタイプの電磁的記録媒体は，データ書き込み回数に制限（寿命）があることからウェアレベリングと呼ばれるディスク領域全体を均一に使用する機能を持っており，データ抹消ソフトウェアによる上書きを実施しても実際にはデータの書き込みが行われず，消去すべき情報がそのまま残ってしまう領域が発生する可能性があることに注意が必要である。同様に，データ抹消ソフトウェアがハードディスクの不良セクタ用の退避領域にアクセスすることができない場合，そこに存在する情報が残る可能性があることにも注意が必要である。
- 暗号化消去を行う方法
- ATA コマンドの「Enhanced SECURITY ERASE UNIT」コマンドを使用する方法
- ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
  この方法を用いる場合，ハードディスクの磁気記録方式（水平磁気記録方式又は垂直磁気記録方式）に対応した消磁装置を用いる必要があることに注意が必要である。

なお，ファイルの情報に別の情報を上書きした場合であっても，特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があることに留意する必要がある。

情報の抹消を外部の民間事業者等へ業務委託する場合は，情報が適正に抹消されたことを証明する資料の提出を求める，職員等による立ち合いを行う等，委託先での履行状況を確認することが重要である。

別紙２

暗号化ガイドライン

情報セキュリティポリシーにおける情報の暗号化においては，原則として下記に掲げるもの及び暗号技術検討会及び関連委員会（以下「CRYPTREC」という。）により安全性及び実装性能が確認された「電子政府における調達のために参照すべき暗号のリスト」（以下「CRYPTREC 暗号リスト」[1]という。）における「電子政府推奨暗号リスト」に基づく暗号技術又は秘密分散技術を適用するものとする。ただし，機密性２以下の情報について，互換性の問題がある場合は，CRYPTREC 暗号リストにおける「運用監視暗号リスト」に基づく暗号技術を使用することができる。

なお，暗号化する際に設定するパスワードやパスフレーズ（以下「暗号化鍵」という。）は，十分な長さと複雑さを有することが求められる。また，暗号化鍵を暗号化された情報と同じ経路で送信等したり，第三者が容易に知り得る方法で送信等したりしてしまうと，第三者によって情報が復号されるおそれが高くなると考えられることから，暗号化鍵は事前の面会時に共有したり，暗号化された情報とは別の方法で送信するなどにより秘匿性を確保しなければならない。

※　「電子政府推奨暗号リスト」について，脆弱性が発見された暗号技術がある場合や，暗号技術には問題ないが，パスワードから暗号鍵を導出する際に電子政府推奨暗号リストに記載されていないアルゴリズムが使われていたり，脆弱性がある場合は，同リストにおける他の暗号方式を用いる等の対応を行うこと。

※　暗号化鍵を要する場合は 5.4.(3)②に掲げるパスワードの規定を遵守すること。

※　「秘密分散技術」とは，秘匿すべき情報を複数のデータに分割することで，そのうちの一つを窃取しても元の情報を一切復元できないようにする技術をいう。この分割されたデータのそれぞれを異なる経路で運搬・送信することにより情報漏えいを防止することができる。なお，秘密分散技術自体が暗号技術の一種であるため，分割されたデータをさらに暗号化する必要はない。

このガイドラインの記述にかかわらず，機関 CISO は必要に応じて，別途暗号化ガイドラインを定めることができる。

記

1.　TLS　TLS1.2 以上
（HTTPS,SMTPS,LDAPS,FTPS,IMAPS,POP3S 等のプロトコルで用いられる。）

[1] https://www.cryptrec.go.jp/list.html

TLS 暗号設定ガイドライン（CRYPTREC, 2020 年 7 月）を参照し，「推奨セキュリティ型」又は「高セキュリティ型」を用いること。（特に機密性３以上を扱う場合は，原則として「高セキュリティ型」を用いること。）

2. WPA2
   （暗号化方式：TKIP 又は AES）
3. PGP
4. Microsoft Office 暗号化
5. Acrobat
   ただし，「AcrobatX 及びそれ以降（暗号化レベル：256-bit AES）」とする。
6. Windows の BitLocker，Mac の FileVault，ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive））及びこれと同等のもの。

別紙３

パスワードガイドライン

パスワードについては，その要件として，類推困難であることが求められる。また，パスワードの管理も重要である。本パスワードガイドラインは，この点を説明することを目的とする。

１）パスワードについて

パスワードは，通常利用者本人が設定するものであり，利用者の個人情報などが含まれる場合が考えられる。

一方で，業務上の使用において，外部サービスからパスワードが漏洩したり，人事異動やインシデントが発生した場合の調査において，開示することが求められる可能性がある。

従って，業務で使用するパスワードはこのことを念頭にし，非常時には開示できるものとしなければならない。

２）パスワードの機密性について

パスワードは，システムへのサインイン（又はログイン）に使用するものについては，原則として機構の情報ではなく，本人に帰するものである。従って機構の機密性の概念は存在しない。しかしながら，当該パスワードの漏洩により，機構の情報資産に被害が生じる可能性がある。従って，役職員等は自己のパスワードに善管注意義務があることに留意し，適切に管理する必要がある。また，パスワードが漏洩した（疑いがある場合も含む）場合は，速やかに機関 CSIRT や情報セキュリティ管理者，関係する情報システム管理者へ報告すること。

なお，機構の情報の暗号化に用いているパスワードについては，機構の情報となる。

３）パスワード長について

5.4.(3)②の規定を遵守すること。[2]

４）類推困難であることについて

類推困難であるためには，以下を満たす必要がある。

A). 複雑であること

（NG な例:「0123456789」,「abcdefg01234」,「qwertyuio」（キーボードの並び順））

[2] ただし，可能であれば，より十分な長さと複雑さを有するものとして，パスワードエントロピーとして 100 ビットを要する（パスワードの解析に 2 の 100 乗回の試行を要する）ものとすることが望ましい。これは例えば，英大文字・英小文字・数字（62 種の文字）を用いたランダム生成では 17 文字以上とすることや，利用者が記憶しやすい単語を用いる場合は，11 万語の辞書から 6 語，2 万語の辞書から 7 語程度を用いるものとなる。

B). 総当たり攻撃（ブルートフォースアタック）に耐性があること
（NG な例: 「0000000」「ZZZZZZZZ」）
C). 辞書攻撃に耐性があること
（NG な例: 「ILoveYou」「p@ssw0rd」「password123」）
D). 複数のシステムやサービスで同じパスワードにしない
（NG な例:PC のログインパスワードと，クラウドサービスのパスワードが同じ）
E). 類推攻撃に耐性があること
（NG な例: 「パスワードにアカウント名や電話番号，生年月日，車のナンバー，職員番号などが含まれる」「あるシステムのパスワードから類推できるパスワードを，別のシステムのパスワードにしている」）
F). パスワードリスト攻撃耐性があること。
過去に盗難や情報漏えいで流出したパスワードを使用しない。

5）パスワードをファイルに保存する場合の注意点

パスワードは, 漏洩した際のリスクを低減するため, 極力共用しないことが望ましい。

一方で，必要なパスワードの数が多くなった場合に，これをテキストファイル等に記述し，暗号化することなく保存することはリスクが大きいため，ファイルで保存する場合はファイルの暗号化機能を用いる必要がある。（ファイルの暗号化については，暗号化ガイドラインに従うものであること。）

この場合においても，パスワードを完全にファイル記述することは望ましくない。

対策として，パスワードに４～６文字程度の共通部分を設け，当該部分は暗記し，それ以外の部分のみ記述することが有効である。（共通部分は，多種多様なシステムのパスワードに対応させるには英数のみとする必要があるかも知れない。）ただし，共通部分が漏洩するとパスワードエントロピーが小さくなる（パスワードとしての有効な文字数が減る）ため，共通部分を除外しても十分なパスワード長と類推困難性を有すことが好ましい。また，共通部分のパスワードが漏洩した場合（可能性を含む），全てのパスワードを変更する必要がある。

なお, パスワードを記載したファイルを,「パスワード」,「Password」等の名称で保存すべきではない。（ファイル名に含む場合も同じ。）脆弱性等により攻撃者の侵入を許した場合，攻撃者はこのようなキーワードでファイルを検索することが知られている。

6）情報システム管理者の注意点

情報システム（外部サービスを含む）を導入する際は，その情報システムの機密性や性質を考慮し，以下の点に注意すること。

A). ユーザーが管理するパスワードが増えないよう，2 要素認証等を備えた既存の認証基盤に認証を委任することなどを検討する。その際，認証基盤から発行されたトークン

等が漏洩しないように，セキュリティには十分配慮する。

B). パスワード認証のみに依存せず，WebAuthn（FIDO2 を含む）や 2 要素認証等の認証方法を検討する。

C). ユーザーにパスワードを設定させる画面では，①類推が容易なパスワードを受け付けないようにする。②パスワード選定の際の注意書きを表示する。③ランダムに生成されたパスワードを提案する。などの機能を検討する。

D). 認証の際は，総当たり攻撃ができないよう，試行回数を制限したり，試行間隔を長くするなどの対策を検討する。

E). システムに保存する認証情報は，直接当該情報を保存するのではなく，ハッシュ値を保存し，ハッシュ値の算出にあたっては，ソルトを加えて算出する。また，ログなどにはパスワードは出力しないなどして，当該情報システムからのパスワード漏洩のリスクに備える。

別紙４

参考とすべき資料等

1. 規範・基準
   - サイバーセキュリティ基本法（平成 26 年法律第 104 号）
   - サイバーセキュリティ基本法施行令（平成 26 年政令第 400 号）
   - 高度情報通信ネットワーク社会形成基本法（平成 12 年法律第 144 号）
   - 政府機関等のサイバーセキュリティ対策のための統一規範
   - 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
   - 政府機関等のサイバーセキュリティ対策の運用等に関する指針
   - 政府機関等の対策基準策定のためのガイドライン

2. セキュリティ関係法令
   - 個人情報の保護に関する法律（平成 15 年法律第 57 号）
   - 不正競争防止法（平成 5 年法律第 47 号）
   - 著作権法（昭和 45 年法律第 48 号）
   - 電気通信事業法（昭和 59 年法律第 86 号）
   - 電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
   - 情報処理の促進に関する法律（昭和 45 年法律第 90 号）
   - 国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号）
   - 刑法（明治 40 年法律第 45 号）
   - 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

3. 無線 LAN の運用における総務省が定めるガイドライン等（6.1.(13)）
   - 総務省 無線 LAN ビジネスガイドライン（初版 平成 25 年 6 月 25 日，第 2 版 平成 28 年 9 月 23 日）
   - 総務省 企業等が安心して無線ＬＡＮを導入・運用するために（平成 25 年 1 月 30 日）
   - IPA 公衆無線 LAN 利用に係る脅威と対策

4. ログの保存期間について

   機関 CISO は，6.1(6)（エ）に基づきログの保存期間を定めようとする場合は下記の点等を配慮してバランス良く適切に設定するように留意すること。
   - 刑事訴訟法（昭和二十三年法律第百三十一号）第百九十七条第３項及び第４項

【参考】刑事訴訟法第百九十七条第３項及び第４項

３　検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。

４　前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。

5. 暗号化ガイドライン関係

・ 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)
・ CRYPTREC 暗号技術ガイドライン
・ 暗号鍵管理システム設計指針
・ TLS 暗号設定ガイドライン

6. サービス基準

・ 政府情報システムのためのセキュリティ評価制度（ISMAP）クラウドサービスリスト (https://www.ismap.go.jp/csm)
・ 経済産業省「情報セキュリティサービス基準」 (https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf)
・ IPA「情報セキュリティサービス基準適合サービスリスト」 (https://www.ipa.go.jp/security/it-service/service_list.html)
    - 情報セキュリティ監査サービス
    - 脆弱性診断サービス
    - デジタルフォレンジックサービス
    - セキュリティ監視・運用サービス

別紙５

用語索引