公益財団法人地球環境戦略研究機関　情報セキュリティポリシー

2019年3月7日制定
2022年7月1日一部改定
2025年1月1日一部改定

1. 総則

1.1. 情報セキュリティの基本方針

(1) 情報セキュリティの基本方針

本機関は、公益財団法人地球環境戦略研究機関（以下「本機関」という。）の文書規程（IGES規程第4号）、個人情報保護規程（IGES規程第17号）及び政府機関による情報セキュリティポリシー等[1]に基づき、本機関の情報資産をあらゆる脅威から保護するために必要な情報セキュリティの確保に最大限取り組むこととする。

(2) ポリシーの適用対象

(a) ポリシーにおいて適用対象とする者は、本機関の役員、職員及び本機関との契約等に基づいて事業を行う事業者（以下「**業務従事者**」という。）業務とする。

(b) ポリシーにおいて適用対象とする情報は、以下の情報とする。

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

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

(iii) (i)及び(ii) のほか、本機関が調達し、又は開発した情報システムの設計又は運用管理に関する情報

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

(3) ポリシーの改定

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

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、ポリシーのほか法令、基準、本機関の規程等（以下「関連法令等」という。）を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、ポリシーでは、あえて関連法令等の遵守について明記していないが情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。また、ポリシーの実施計画や必要な手順等について整備すること。

1.2. 情報の格付の区分・取扱制限

(1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、ポリシーの遵守事項で用いる格付の区分の定義を示す。なお、本機関において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、ポリシーの遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。また、他機関等へ情報を提供する場合は、本機関のポリシーにおける格付区分と統一基準における格付区分の対応について、適切に伝達する必要がある。

[1] 環境省情報セキュリティポリシー（第１１版）令和５年1２月1８日環境省情報セキュリティ委員会発行

機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	業務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報を含む情報[2]
機密性２情報[3]	業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

機密性２情報及び機密性３情報を「要機密情報」と呼ぶ。

完全性についての格付の定義

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

完全性２情報を「要保全情報」と呼ぶ。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、他人の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

可用性２情報を「要安定情報」と呼ぶ。また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」と呼ぶ。

(2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを業務従事者に確実に行わせるための手段をいう。業務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある（別紙）。

2. 情報セキュリティ対策の基本的枠組み

2.1. 導入・計画

2.1.1. 組織・体制の整備

(1) 最高情報セキュリティ責任者の設置

本機関は、本機関における情報セキュリティに関する事務を統括する最高情報セキ

[2] 機密性３（「極秘」）に相当するものとしては、法律で安全管理が義務付けられている、守秘義務の対象として指定されている、限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている、営業秘密（秘密として管理されているもの）として指定されている、漏えいすると取引先や顧客に大きな影響がある等があるものと解される（独立行政法人情報処理推進機構（Information-technology Promotion Agency, Japan: IPA）発行「中小企業の情報セキュリティ対策ガイドライン 付録５」による）。

[3] 機密性２（「社外秘」）に相当するものとしては、一般に漏洩すると事業に大きな影響があるものと解される（同上）。

ュリティ責任者１人を置く。

(2) 情報セキュリティ委員会の設置

最高情報セキュリティ責任者は、ポリシーなどの検討や情報セキュリティ対策推進体制及びその他業務を実施するため、情報セキュリティ委員会を置き、委員を任命する。

(3) 情報セキュリティ監査責任者の設置

最高情報セキュリティ責任者は、その指示に基づき監査を実施する際に事務を統括する者として、情報セキュリティ監査責任者１人を任命する。

(4) 情報セキュリティ責任者等の設置

(a) 最高情報セキュリティ責任者は、本部戦略マネージメントオフィスに**情報セキュリティ責任者**及び**情報システムセキュリティ責任者**を置き、情報セキュリティ全般について集中管理的に対策を実施する。

(b) 最高情報セキュリティ責任者は、各サテライトオフィス等（東京サステナビリティフォーラム、関西リサーチセンター、北九州アーバンセンター、バンコク地域センター、IPCCインベントリータスクフォース技術支援ユニット、及びAPN 事務局に**サテライトオフィス情報セキュリティ責任者**を置き、情報セキュリティ責任者及び情報システムセキュリティ責任者の指示のもと、各サテライト等における情報セキュリティ対策を実施する。

(c) 最高情報セキュリティ責任者は、プロジェクトごとに**プロジェクト情報セキュリティ責任者**を置き、情報セキュリティ責任者及び情報システムセキュリティ責任者の指示のもと、各プロジェクトに必要な情報セキュリティ対策を実施する。また、必要に応じ**クラウドサービス管理者**を置く。

(5) 情報セキュリティ・サポートの設置

最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する情報セキュリティ・サポートを置く（本機関ITシステム運用委託者[4]）。

(6) 情報セキュリティインシデントへの対応

(a) 最高情報セキュリティ責任者は、情報セキュリティインシデントに対処する体制を整備する。

(b) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティ・サポートから技術的なサポートを受け情報セキュリティインシデントに対応し、最高情報セキュリティ責任者へ報告する。

(7) 兼務を禁止する役割

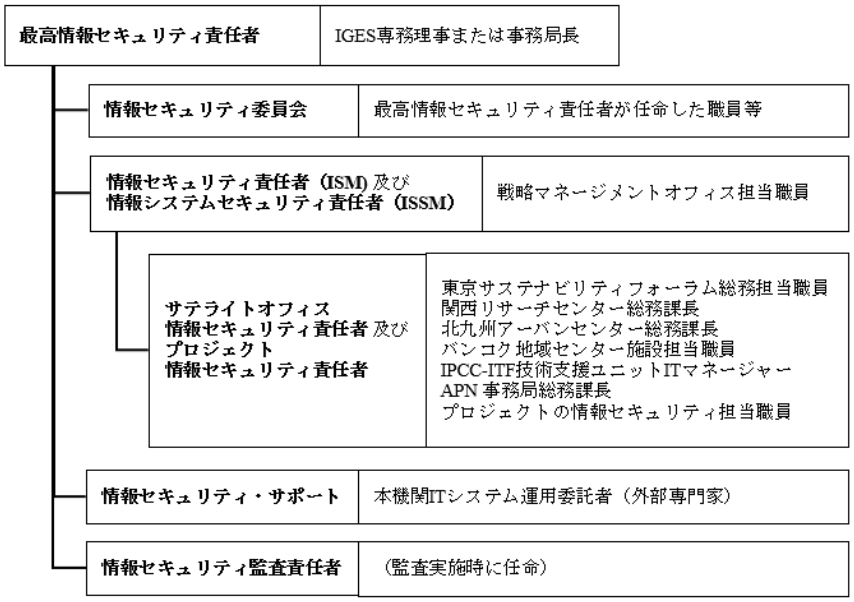
(a) 業務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア)承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う者（以下本条において「承認権限者等」という。）

(イ)監査を受ける者とその監査を実施する者

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

[4] ITヘルプデスクと呼ぶことがある。



本機関における情報セキュリティ体制図

2.1.2. ポリシー及び対策推進計画の策定

(1) ポリシー及び対策推進計画の策定

最高情報セキュリティ責任者は、本機関の業務、取り扱う情報及び保有する情報システムに関するリスクを踏まえ、情報セキュリティ委員会における検討を経てポリシーを定め、以下に掲げる対策を推進するための計画を策定すること。

(i) 情報セキュリティに関する教育

(ii) 情報セキュリティ対策の自己点検

(iii) 情報セキュリティ監査

(iv) 情報システムに関する技術的な対策を推進するための取組

(v) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.2. 運用

2.2.1. 情報セキュリティポリシーの運用

(1) 情報セキュリティ対策に関する実施手順の整備・運用

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、本機関における情報セキュリティ対策について、実施手順を整備して実施し、その状況を最高情報セキュリティ責任者に報告すること。

(b) 情報セキュリティ対策推進に携わる責任者は、最高情報セキュリティ責任者が定めた当該体制の役割に応じて必要な事務を遂行すること。

(c) サテライト情報セキュリティ責任者及びプロジェクト情報セキュリティ責任者は、業務従事者からポリシー等に係る課題及び問題点の報告を受けた場合は、情報セキュリティ責任者及び情報システムセキュリティ責任者に報告すること。

(2) 違反への対処

(a) 業務従事者は、ポリシー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及び情報システムセキュリティ責任者にその旨を報告すること。

(b) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、ポリシー等への重大な違反の報告を受けた場合及び 自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの 維持に必要な措置を講じさせるとともに、最高情報セキュリティ責任者に報告すること。

2.2.2. 例外措置

(1) 例外措置の申請と審査

最高情報セキュリティ責任者は、必要に応じ、情報セキュリティ委員会において、本ポリシーの例外措置適用の申請手続きの制定や審査を実施すること。業務従事者は、情報セキュリティ委員会に対し本ポリシーの例外措置の適用を申請すること。

2.2.3. 情報セキュリティインシデントへの対処

(1) 情報セキュリティインシデントに備えた事前準備

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の本機関内の報告手順を整備し、業務従事者に周知すること。

(b) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の本機関外との情報共有を含む対処手順を整備すること。

(c) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先等を整備すること。

(d) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討すること。

(2) 情報セキュリティインシデントへの対処

(a) 業務従事者は、情報セキュリティインシデントやその可能性を認知した場合には、直ちに情報セキュリティ責任者、情報システムセキュリティ責任者、及び情報セキュリティ・サポートに報告し、指示に従うこと。

(b) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

(c) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告すること。

(d) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行うこと。

(e) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行い、また必要に応じ関係機関と情報共有を行うこと。

(f) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティインシデントに関する対処の内容を記録すること。

(g) 最高情報セキュリティ責任者は、情報セキュリティインシデント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とること。

2.2.4. 点検及び教育

(1) 業務従事者各個人の情報セキュリティの点検及び教育

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報セキュリティ・サポートの協力と共に、業務従事者各個人の情報セキュリティの状態を定期的に管理し、必要があれば、業務従事者に改善を指示し、情報セキュリティに係る研修等を受講させること。

2.2.5. 見直し

(1) 内部監査の実施

最高情報セキュリティ責任者は、情報セキュリティ・サポートの協力と共に、内部監査を実施し、本機関内において改善が必要な事項について対策を講じること。

(2) ポリシー及び対策推進計画の見直し

最高情報セキュリティ責任者は、情報セキュリティの運用を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会において、本ポリシーについて必要な見直しを行うこと。

3. 情報の取扱い

3.1. 情報の取扱い

(1) 情報の取扱いに係る規定の整備

情報セキュリティ責任者及び情報システムセキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、業務従事者へ周知すること。

(i) 情報の格付及び取扱制限についての定義

(ii) 情報の格付及び取扱制限の明示等についての手続

(iii) 情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報の目的外での利用等の禁止

業務従事者は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等すること。

(3) 情報の格付及び取扱制限の決定・明示等

(a) 業務従事者は、情報の作成時及び本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、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。

(b) 業務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

(c)業務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと

(4) 情報の利用・保存

(a) 業務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 業務従事者は、機密性３情報について要管理対策区域外で情報処理を行う場合は、情報セキュリティ責任者の許可を得ること。

(c) 業務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること

(d) 業務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及取扱制限に従って情報を適切に管理すること。

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

(5) 情報の提供・公表

(a) 業務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

(b) 業務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当

該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

(c)業務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

(6) 情報の運搬・送信

(a) 業務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

(b) 業務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合 には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

(7) 情報の消去

(a) 業務従事者は、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こと。

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

(c)業務従事者は、要機密情報である書面を廃棄する場合には復元が困難な状態にすること。

(8) 情報のバックアップ

(a) 業務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

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

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

3.2. 情報を取り扱う区域の管理

(1) 要管理対策区域における対策

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、要管理対策区域の範囲を定めること。

(b) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

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

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

(2) 要管理対策区域における対策の実施

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、該当するサテライト情報セキュリティ責任者又はプロジェクト情報セキュリティ責任者とともに管理する区域に対して必要な対策を講じること。

4. 外部委託

4.1. 業務委託

4.1.1. 業務委託[5]

(1) 外部委託に係る運用の整備

[5] （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

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、外部委託に係る以下の内容を含む運用を整備すること。

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

(ii) 委託先の選定基準

(2) 業務委託実施前の対策

(a) 情報システムセキュリティ責任者及びプロジェクト情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施すること。

(i) 委託する業務内容の特定

(ii) 委託先の選定条件を含む仕様の策定

(iii) 仕様に基づく委託先の選定

(iv) 契約の締結

(v) 委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

(b) 情報システムセキュリティ責任者及びプロジェクト情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求めること。

(i) 仕様に準拠した提案

(ii) 契約の締結

(iii) 委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

(3) 業務委託実施期間中の対策

(a) プロジェクト情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施すること。

(i) 委託判断基準に従った要保護情報の提供

(ii) 契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認

(iii) 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受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

(b) プロジェクト情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求めること。

(i) 情報の適正な取扱いのための情報セキュリティ対策

(ii) 契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告

(iii) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 業務委託終了時の対策

(a) プロジェクト情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施すること。

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

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

(b) プロジェクト情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求めること。

(i) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告

を含む検収の受検

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

(5) 業務を受託する時

(a) 情報システムセキュリティ責任者及びプロジェクト情報セキュリティ責任者は、契約を含め、業務の受託前、実施中、受託終了時において実施することが求められている事項について、契約前に確認すること。

4.1.2. 情報システムに関する業務委託[6]

(1) 情報システムに関する業務委託における共通的対策

(a) 情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに本機関の意図しない変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。

(2) 情報システムの構築を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求めること。

(i) 情報システムのセキュリティ要件の適切な実装

(ii) 情報セキュリティの観点に基づく試験の実施

(iii) 情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求めること。

(b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めること。

(4) 情報システムの一部の機能を提供するサービスを利用する場合の対策

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

(b) 情報システムセキュリティ責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定すること。

(c) 情報システムセキュリティ責任者は、委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

4.2. クラウドサービス[7]

4.2.1. クラウドサービスの選定（要機密情報を取り扱う場合）

(1) クラウドサービスの選定に係る運用の整備

(a) 情報セキュリティ責任者及び情報システムセキュリティ責任者は、以下を含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用を整備すること。

---

[6] （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、機関等内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務の委託（ホスティング型プライベートクラウド）

[7] （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）、web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

(i) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 4.2 節において「クラウドサービス利用判断基準」という。）

(ii) クラウドサービスの選定基準

(iii) クラウドサービスの利用申請の許可権限者と利用手続

(iv) **クラウドサービス管理者**の指名とクラウドサービスの利用状況の管理

(v) その他最高情報セキュリティ責任者または情報セキュリティ委員会が必要と判断した条件等

(b) 本機関における許可権限者は情報システムセキュリティ責任者とし、プロジェクトが利用するクラウドのサービスの選定、調達及び利用について、プロジェクト情報セキュリティ管理者に代行させることができる。

(c) 情報セキュリティ責任者または情報システムセキュリティ責任者がクラウドサービスの選定、調達及び利用を行う場合は、高情報セキュリティ責任者の承認を得ること。

(2) クラウドサービスの選定

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討すること。

(b) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めること。

(i) クラウドサービスに求める情報セキュリティ対策

(ii) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(iii) クラウドサービスに求めるサービスレベル

(c) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、選定すること[8]。

(3) クラウドサービスの利用に係る調達

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

(b) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認すること。また、調達仕様の内容は、契約に含めること。

(4) クラウドサービスの利用承認

(a) プロジェクト情報セキュリティ責任者は、クラウドサービスを利用する場合には、情報システムセキュリティ責任者へクラウドサービスの利用申請を行うこと。

(b) 情報システムセキュリティ責任者は、前項におけるクラウドサービスの利用申請を審査し、利用の可否を決定すること。

(c) 情報システムセキュリティ責任者は、クラウドサービスの利用申請を承認した場合は、プロジェクト情報セキュリティ責任者をクラウドサービス管理者として指名

[8] **（参考）官公庁は、政府情報システムのためのセキュリティ評価制度**（Information system Security Management and Assessment Program (ISMAP)）**による選定。**

すること。

4.2.2. クラウドサービスの利用（要機密情報を取り扱う場合）

(1) クラウドサービスの利用に係る運用の整備

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備すること。

(i) クラウドサービスの利用終了時における対策

(ii) クラウドサービスで取り扱った情報の廃棄

(iii) クラウドサービスの利用のために作成したアカウントの廃棄

(2) クラウドサービスの利用に係るセキュリティ要件の策定

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)の基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認し、セキュリティ要件を策定すること。

(3) クラウドサービスを利用した情報システムの導入・構築時の対策

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、(1)の基本方針及び(2)(a)において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずること。また、導入・構築時に実施状況を確認すること。

(b) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスの情報セキュリティ対策を実施するための文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備すること。

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

(ii) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(iii) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

(4) クラウドサービスを利用した情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、(1)(b)で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録すること。

(b) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、情報システムセキュリティ責任者へ報告すること。

(c) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、最高情報セキュリティ責任者又は情報セキュリティ委員会の求めに応じクラウドサービスの運用に関するデータ、履歴、その他の情報を提出しなければならない。

(5) クラウドサービスを利用した情報システムの更改・廃棄時の対策

(a) 情報システムセキュリティ責任者又は代行するプロジェクト情報セキュリティ責任者は、(1)(a)で定めた運用を踏まえて、更改・廃棄時の必要な措置を講ずること。また、クラウドサービスの利用終了時に実施状況を確認・記録すること。

4.2.3. クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

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

(a) 情報システムセキュリティ責任者は、以下を含むクラウドサービス（要機密情報を取り扱わない場合）の利用に関する運用を整備すること

(i) クラウドサービスを利用可能な業務の範囲

(ii) クラウドサービスの利用申請の許可権限者と利用手続

(iii) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(iv) クラウドサービスの利用の運用

(b) 本機関における許可権限者は情報システムセキュリティ責任者とし、プロジェクトが利用するクラウドのサービスの選定、調達及び利用について、プロジェクト情報セキュリティ管理者に代行させることができる。

(c) 情報システムセキュリティ責任者がクラウドサービスの選定、調達及び利用を行う場合は、最高情報セキュリティ責任者の承認を得ること。

(2) 要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施

(a) 業務従事者は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、情報システムセキュリティ責任者へクラウドサービスの利用を申請すること。

(b) 情報システムセキュリティ責任者は、業務従事者による利用するクラウドサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることの確認結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定すること。

(c) 情報システムセキュリティ責任者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、プロジェクト情報セキュリティ責任者をクラウドサービス管理者として指名し、承認したクラウドサービスを記録すること。

(d) プロジェクト情報セキュリティ責任者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずること。

4.3. 機器等の調達

4.3.1. 機器等の調達

(1) 機器等の調達に係る運用の整備

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

(b) 情報システムセキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

5. 情報システムのライフサイクル

5.1. 情報システムの分類

5.1.1. 情報システムの分類基準等の整備

(1) 情報システムにおける分類のための運用の整備

(a) 情報システムセキュリティ責任者は、情報システムの情報セキュリティインシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である情報システムの分類基準を運用として整備すること。

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

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

(3) 情報システムの分類基準に基づいた分類の実施

(a) 情報システムセキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を実施し、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用の修正を行うこと。

(4) 情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用の見直し

(a) 情報システムセキュリティ責任者は、情報システムの分類基準と分類基準に応じた情報セキュリティ対策の具体的な対策事項の運用について定期的な確認による見直しをすること

5.2. 情報システムのライフサイクルの各段階における対策

5.2.1. 情報システムの要件定義

(1) 実施体制の確保

(a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めること。

(b) 最高情報セキュリティ責任者は、前項で求められる体制の確保に際し協力を得ることが必要な場合には、当該情報システムに係る業務の責任者に当該体制の全部又は一部の整備を求めること。

(2) 情報システムの分類基準に基づいた分類の実施

(a) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システムの分類基準に基づいて情報システムの分類を行い、情報セキュリティ責任者に報告すること。

(3) 情報システムのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等を勘案し構築する情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、以下の全ての事項を含む情報システムのセキュリティ要件を策定すること。

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

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

(iii) 情報システムに関連する脆弱性及び不正プログラムについての対策要件

(iv) 情報システムの可用性に関する対策要件

(v) 情報システムのネットワーク構成に関する要件

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

(5) 情報システムセキュリティ責任者は、機器等を調達する場合には. 入手可能な最新の情報や必要に応じ専門的なアドバイスを得ながら、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

5.2.2. 情報システムの調達・構築

(1) 情報システムの構築時の対策

(a) 情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

(b) 情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

(c) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について情報セキュリティ責任者に報告すること・

(d) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備すること

(i) 情報システムを構成するサーバ装置及び端末関連情報

(ii) 情報システムを構成する通信回線及び通信回線装置関連情報

(e) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備すること。

(i) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(ii) 情報セキュリティインシデントを認知した際の対処手順

(iii) 情報システムが停止した際の復旧手順

(2) 納品検査時の対策

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

(b) 情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。

5.2.3. 情報システムの運用・保守

(1) 情報システムの運用・保守時の対策

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

(b) 情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

(c) 情報システムセキュリティ責任者は、情報システムの運用・保守において、変更が生じた場合、情報システム台帳及び関連 文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、情報セキュリティ責任者へ報告すること。

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

(e) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をすること。

5.2.4. 情報システムの更改・廃棄

(1) 情報システムの更改・廃棄時の対策

(a) 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合

は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限 を考慮した上で、以下の措置を適切に講ずること。

(i) 情報システム更改時の情報の移行作業における情報セキュリティ対策

(ii) 情報システム廃棄時の不要な情報の抹消

5.3. 情報システムの運用継続計画

5.3.1. 情報システム運用継続計画の整備・整合的運用の確保

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 情報システムセキュリティ責任者は、本機関の非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用及び実施手順の整備を検討すること。

(b) 情報システムセキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用及び実施手順が運用可能であるかを定期的に確認すること。

(c) 情報システムセキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用及び実施手順を定期的に見直すこと。

6. 情報システムの構成要素

6.1. 端末

6.1.1. 端末

(1) 端末の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させないこと。

(c) 情報システムセキュリティ責任者は、端末に接続を認める機器等を定め、接続を認めた機器等以外は接続させないこと。

(d) 報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した内容に従い、端末に対して適切なセキュリティ対策を実施すること

(e) 情報システムセキュリティ責任者は、端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。

(2) 端末の運用時の対策

(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて定期的な確認による見直しを行うこと。

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

(3) 端末の運用終了時の対策

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

6.1.2. 要管理対策区域外での端末利用時の対策

(1) 本機関が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用の整備

(a) 情報システムセキュリティ責任者は、本機関が支給する物理的な端末（要管理対

策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。

(b) 情報システムセキュリティ責任者は、要機密情報を取り扱う本機関が支給する端末（要管理対策区域外で使用する場合に限る）及び本機関支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する運用を整備すること。

(c) 情報システムセキュリティ責任者は、要管理対策区域外において、本機関外通信回線に接続した本機関が支給する物理的な端末を、本機関内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から本機関内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた技術的な措置に関する運用を定めること。

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

(a) 情報システムセキュリティ責任者は、端末について前条(b)または前条(c)の技術的な措置を講ずること。

6.1.3. 本機関支給以外の端末の導入及び利用時の対策

(1) 本機関支給以外の端末の利用可否の判断

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

(2) 本機関支給以外の端末の利用に関する運用等の整備

(a) 情報システムセキュリティ責任者は、業務従事者が本機関支給以外の端末を用いて本機関の業務に係る情報処理を行う場合の許可等の手続を実施手順として定めること。

(b) 情報システムセキュリティ責任者は、業務従事者が本機関支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。

(c) 情報システムセキュリティ責任者は、要機密情報を取り扱う本機関支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を含めた安全管理措置に関する運用を整備すること。

(d) 情報システムセキュリティ責任者は、要管理対策区域外において本機関外通信回線に接続した本機関支給以外の端末を本機関内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から本機関内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する運用及び許可手続に関する実施手順を定めること。

(3) 本機関支給以外の端末の利用に関する責任者

(a) は、本機関支給以外の端末を用いた本機関の業務に係る情報処理に関する安全管理措置の実施状況を管理するは情報セキュリティシステム責任者とする。

(4) 本機関支給以外の端末の利用時の対策

(a) 業務従事者は、本機関支給以外の端末を用いて本機関の業務に係る情報処理を行う場合には、情報システムセキュリティ責任者の許可を得ること。

(b) 業務従事者は、本機関支給以外の端末を用いて要保護情報を取り扱う場合は、(2)(b)で定める利用手順に従うこと。

(c) 情報システムセキュリティ責任者は、要機密情報 を取り扱う本機関支給以外の端

末について、(2)(c) に定める安全管理措置を講じる又は業務従事者に講じさせること。

(d) 業務従事者は、情報処理の目的を完了した場合は、要保護情報を本機関支給以外の端末から消去すること。

6.2. サーバ装置

6.2.1. サーバ装置

(1) サーバ装置の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

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

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

(d) 情報システムセキュリティ責任者は、サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させないこと。

(e) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施すること。

(f) 情報システムセキュリティ責任者は、サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。

(g) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得すること。

(2) サーバ装置の運用時の対策

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

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

(c) 情報システムセキュリティ責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するための措置を講ずること。

(d) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行える運用をすること。

(3) サーバ装置の運用終了時の対策

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

6.2.2. 電子メール

(1) 電子メールの導入時の対策

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

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

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

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

6.2.3. ウェブ

(1) ウェブサーバの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、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。

(b) 情報システムセキュリティ責任者は、ウェブサーバからの不用意な情報漏えいを防止するための措置を講ずること

(c) 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を担当する主体を限定すること。

(d) 情報システムセキュリティ責任者は、インターネットを介して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こと。

6.2.4. ドメインネームシステム（DNS）

(1) DNS の導入時の対策

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

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

(c) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、本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こと

(2) DNS の運用時の対策

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

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

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

6.2.5. データベース

(1) データベースの導入・運用時の対策

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

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

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

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

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

6.3. 複合機・特定用途機器

6.3.1. 複合機・特定用途機器

(1) 複合機

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

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

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

(2) IoT機器を含む特定用途機器

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

6.4. 通信回線

6.4.1. 通信回線

(1) 通信回線の導入時の対策

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

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

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

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

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

(2) 本機関外通信回線の接続時の対策

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

(b) 情報システムセキュリティ責任者は、本機関内通信回線と本機関外通信回線との間で送受信される通信内容を監視するための措置を講ずること。

(c) 情報システムセキュリティ責任者は、保守又は診断のために、本機関外通信外線から本機関内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保すること。

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

(3) 通信回線の運用時の対策

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

(b) 情報システムセキュリティ責任者は、本機関内通信回線と本機関外通信回線との間及び本機関内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをすること。

(c) 情報システムセキュリティ責任者は、保守又は診断のために、本機関外通信回線から本機関内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認による見直しをすること。

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

6.4.2. 通信回線装置

(1) 通信回線装置の導入時の対策

(a) 情報システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないようにすること。

(b) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めること。

(c) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。

(d) 情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。

(2) 通信回線装置の運用時の対策

(a) 情報システムセキュリティ責任者は、通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

(c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講ずること。

(3) 通信回線の運用終了時の対策

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

6.4.3. 無線LAN

(1) 無線LAN 環境導入時の対策

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

6.4.4. IPv6 通信回線

(1) IPv6 通信を行う情報システムに係る対策

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

(b) 情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、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こと。

(2) 意図しないIPv6 通信の抑止・監視

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

6.5. ソフトウェア

6.5.1. 情報システムの基盤を管理又は制御するソフトウェア

(1) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

(a) 情報システムセキュリティ責任者は、情報セキュリティの観点から、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際は、端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講ずること。

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

(i) 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

(ii) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(2) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

(a) 情報システムセキュリティ責任者は、情報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こと。

(i) 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

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

6.6. アプリケーション・コンテンツ

6.6.1. アプリケーション・コンテンツの作成・運用時の対策

(1) アプリケーション・コンテンツの作成に係る運用の整備

(a) 情報システムセキュリティ責任者は、アプリケーション・コンテンツの提供時に本機関外の情報セキュリティ水準の低下を招く行為を防止するための運用を整備すること。

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、本機関外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、セキュリティ要件を仕様に含めること。

(b) 業務従事者は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に掲げる内容を調達仕様に含めること。

(3) アプリケーション・コンテンツの開発時の対策

(a) 情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、

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こと。

(4) アプリケーション・コンテンツの運用時の対策

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

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

(c) 情報システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずること。

6.6.2. アプリケーション・コンテンツ提供時の対策

(1) 本機関ドメイン名の使用

(a) 情報システムセキュリティ責任者は、本機関外向けに提供するウェブサイト等が実際の本機関提供のものであることを利用者が確認できるように、本機関のドメイン名を取得できない場合を除きドメイン名を情報システムにおいて使用すること。

(b) 業務従事者は、本機関外向けに提供するウェブサイト等の作成を外部委託する場合においては、本機関に適するドメイン名を使用するよう調達仕様に含めること。

(2) 不正なウェブサイトへの誘導防止

(a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して本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こと。

(3) アプリケーション・コンテンツの告知

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

(b) 業務従事者は、本機関外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

7. 情報システムのセキュリティ機能

7.1. 情報システムのセキュリティ機能

7.1.1. 主体認証機能

(1) 主体認証機能の導入

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

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

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

(2) 識別コード及び主体認証情報の管理

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

こと。

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

7.1.2. アクセス制御機能

(1) アクセス制御機能の導入

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

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

7.1.3. 権限の管理

(1) 権限の管理

(a) 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

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

(c) 情報システムセキュリティ責任者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認すること。

7.1.4. ログの取得・管理

(1) ログの取得・管理

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

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

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

7.1.5. 暗号・電子署名

(1) 暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

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

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

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

実施手順を定めること。

(c) 情報システムセキュリティ責任者は、本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、電子署名の目的に合致し、かつ適用可能な公的な鍵基盤が存在する場合は、それを使用すること。

(2) 暗号化・電子署名に係る管理

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

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

(ii) 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や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、業務従事者と共有を図ること。

7.1.6. 監視機能

(1) 監視機能の導入・運用

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

(b) 情報システムセキュリティ責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用すること。

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

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) ソフトウェアに関する脆弱性対策の実施

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

(b) 情報システムセキュリティ責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

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

(d) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的及び適時に確認すること。

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

7.2.2. 不正プログラム対策

(1) 不正プログラム対策の実施

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

(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全て

において、不正プログラム対策ソフトウェア等により対策を講ずること。

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

7.2.3. サービス不能攻撃対策

(1) サービス不能攻撃対策の実施

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

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

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

7.2.4. 標的型攻撃対策

(1) 標的型攻撃対策の実施

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

(b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。

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) 動的なアクセス制御の導入方針の検討

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

(2) 動的なアクセス制御の実装時の対策

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

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

7.3.2. 動的なアクセス制御の運用時の対策

(1) 動的なアクセス制御の実装方針の見直し

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

(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

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

8. 情報システムの利用

8.1. 情報システムの利用

8.1.1. 情報システムの利用

(1) 情報システムの利用に係る規定の整備

(a) 情報システムセキュリティ責任者は、本機関の情報システムの利用のうち、情報セキュリティに関する運用を整備すること。

(b) 情報システムセキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。

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

(2) 情報システム利用者の運用遵守のための対策

(a) 情報システムセキュリティ責任者は、業務従事者による運用遵守を促進する機能について情報セキュリティリスクと業務効率化の観点から検討して情報システムを構築すること。

(3) 情報システムの利用時の基本的対策

(a) 業務従事者は、業務の遂行以外の目的で情報システムを利用しないこと。

(b) 業務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に本機関の情報システムを接続しないこと。

(c) 業務従事者は、本機関内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。

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

(e) 業務従事者は、接続が許可されていない機器等を情報システムに接続しないこと。

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

(g) 業務従事者は、機密性３情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者の許可を得ること。

(h) 業務従事者は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しないこと。

(4) 端末（支給外端末を含む）の利用時の対策

(a) 業務従事者は、本機関が支給する端末（要管理対策区域外で使用する場合に限る）及び本機関支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

(b) 業務従事者は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、情報システムセキュリティ責任者の許可を得ること。

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

(ii) 本機関支給以外の端末:要保護情報

(c) 業務従事者は、要管理対策区域外において本機関外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で本機関等内通信回線に接続する場合には、定められた措置を講ずること。

(5) 電子メール・ウェブの利用時の対策

(a) 業務従事者は、要機密情報を含む電子メールを送受信する場合には、本機関が運営し、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こと。

(b) 業務従事者は、本機関外の者と電子メールにより情報を送受信する場合は、本機関ドメイン名を取得できない場合を除き、当該電子メールのドメイン名に本機関のドメイン名を使用すること。

(c) 業務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

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

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

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

(i) 送信内容が暗号化されること

(ii) 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

(6) 識別コード・主体認証情報の取扱い

(a) 業務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

(b) 業務従事者は、自己に付与された識別コードを適切に管理すること。

(c) 業務従事者は、自己の主体認証情報の管理を徹底すること。

(7) 暗号・電子署名の利用時の対策

(a) 業務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

(b) 業務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

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

(8) 不正プログラム感染防止

(a) 業務従事者は、不正プログラム感染防止に関する措置に努めること。

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

(9) Web 会議サービスの利用時の対策

(a) 業務従事者は、定められた利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

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

(10) クラウドサービスを利用した本機関外の者との情報の共有時の対策

(a) 業務従事者は、本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要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずること。

(b) 業務従事者は、本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要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除すること。

8.1.2. ソーシャルメディアサービスによる情報発信

(1) ソーシャルメディアサービスによる情報発信時の対策

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

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

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

(2) 業務従事者は、要安定情報の公開にソーシャルメディアサービスを用いる場合は、本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こと。

8.1.3. テレワーク及びリモートワーク

(1) 運用の整備

(a) 情報システムセキュリティ責任者は、テレワーク及びリモートワーク実施時の情報セキュリティ対策に係る運用規程を整備すること。なお、原則としてテレワーク及びリモートワークは本機関が支給する端末で行うよう定めること。

(2) 実施環境における対策

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

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

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

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

(3) 実施時における対策

(a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に業務従事者が確認するべき項目を定め、業務従事者に当該項目を確認させること。

(b) 業務従事者は、画面ののぞき見や盗聴を防止できるようリモートワークの実施場所を選定すること。

(c) 業務従事者は、原則として情報セキュリティ対策の状況が定かではない又は不十分な通信回線を利用してテレワークやリモートを行わないこと。

8.1.4. 生成AIの利用

(1) 方針の策定及び利用に対する対策

情報セキュリティ責任者は、本機関の業務における生成AIの利用について、別途方針を策定し、必要な対策を講じること。

9. その他

9.1. 委任

このポリシーの施行に関し必要な事項は、別に理事長が定める。

附則

このポリシーは、平成 2025 年 1 月 1 日から施行する。

***

（別紙）情報取扱制限の例

機密性についての取扱制限の定義の例

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

上記の指定方法の意味は以下のとおり。

- 「○○禁止」：当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
- 「○○要許可」：当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
- 「暗号化必須」：当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。
- 「○○限り」：当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「○○課内限り」「○○会議出席者限り」等、参照を許可する者が分かるように指定する。
- 「○月○日まで○○禁止」：月○日まで複製を禁止したい場合、「○月○日まで複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

完全性についての取扱制限の定義の例

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

情報の保存期間の指定の方法は、以下のとおり。

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

可用性についての取扱制限の定義の例

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

復旧許容時間の指定の方法は以下のとおり。

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