情報セキュリティ対策基準

第１１版
令和７年１月３０日改正

独立行政法人 製品評価技術基盤機構

目　次

第１章　総則

第１節　目的及び定義

（目的）

第１条　この基準は、独立行政法人製品評価技術基盤機構（以下「機構」という。）の情報セキュリティ管理規程第１８条第１項の規定に基づき、機構における情報セキュリティ対策に関して遵守すべき事項の基準を定める。

（定義）

第２条　この基準における用語の定義は情報セキュリティ管理規程の定義によるほか、次の各号による。

一　機密性３情報　機構の業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報に準ずる情報をいう。

二　機密性２情報　機構の業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報をいう。

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

四　要機密情報　「機密性２情報」及び「機密性３情報」をいう。

五　完全性２情報　機構の業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され、又は業務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

六　完全性１情報　「完全性２情報」以外の情報（書面を除く。）をいう。

七　要保全情報　「完全性２情報」をいう。

八　可用性２情報　機構の業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

九　可用性１情報　「可用性２情報」以外の情報（書面を除く。）をいう。

十　要安定情報　「可用性２情報」をいう。

十一　要保護情報　「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情報をいう。

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

十三　端末　情報システムの構成要素である機器のうち、業務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機構が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機構が調達又は開発するもの以外を指す「機構支給以外の端末」がある。また、機構が調達又は開発した端末と機構支給以外の端末の双方を合わせて「端末（支給外端末を含む。）」という。さらに、物理的なハードウェアを有する端末を「物理的な端末」という。

十四　モバイル端末　端末のうち、端末の形態に関係なく、業務上の必要に応じて移動させて使用することを目的としたものをいう。

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

十六　暗号化　第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。

十七　記録媒体　情報が記録され、又は記載される有体物をいう。また、記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。

　なお、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

十八　機関等　国の行政機関、独立行政法人及び指定法人をいう。

十九　通信回線　複数の情報システム又は機器等（機構が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機構の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機構が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

二十　機構外通信回線　通信回線のうち、機構内通信回線以外のものをいう。

二十一　情報の抹消　電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。

なお、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。

二十二　業務委託　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。

二十三　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ものをいう。

なお、クラウドサービスの例としては、SaaS（Software as a Service)、PaaS（Platform as a Service)、IaaS（Infrastructure as a Service）等がある。

二十四　クラウドサービス管理者　クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う機構の職員等をいう。

二十五　クラウドサービス提供者　クラウドサービスを提供する事業者をいう。

なお一般にはクラウドサービスプロバイダを指す。

二十六　クラウドサービス利用者　クラウドサービスを利用する機構の業務従事者又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。

二十七　主体　情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。

二十八　主体認証　識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。

二十九　アクセス制御　情報又は情報システムへのアクセスを許可する主体を制限することをいう。

三十　権限管理　主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

三十一　不正プログラム　コンピュータウイルス、ワーム（他のプログラムに寄生せ

ず単体で自己増殖するプログラム)、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

三十二　通信回線装置　通信回線間又は通信回線と情報システムとの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。

三十三　ソフトウェア　サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む。

三十四　機構内　機構が管理する組織又は建物の内をいう。

三十五　機構内通信回線　機構が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、機構の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。機構内通信回線には、専用線や VPN 等物理的な回線を機構が管理していないものも含まれる。

三十六　電子メールサーバ　電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。

三十七　電子メールクライアント　電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

三十八　DNS（ドメインネームシステム）　クライアント等からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うシステムをいう。

三十九　名前解決　ドメイン名やホスト名と IP アドレスとを変換することをいう。

四十　複合機　プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。

四十一　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、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続する機能を備えている、又は内蔵電磁的記録媒体を備えているものをいう。

四十二　無線 LAN　IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad 等の規格により、無線通信で情報を送受信する通信回線をいう。

四十三　アプリケーション　OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

四十四　アプリケーション・コンテンツ　機構が開発し提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。

四十五　ドメイン名　国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.nite.go.jp というウェブサイトの場合は、nite.go.jp の部分がこれに該当する。

四十六　政府ドメイン名　.go.jp で終わるドメイン名のことをいう。日本国の政府機関、独立行政法人、特殊法人（特殊会社を除く。）が登録（取得）することができる。

四十七　主体認証情報　主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

四十八　識別　情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

四十九　識別コード　主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID がある。

五十　電子署名　情報の正当性を保証するための電子的な署名情報をいう。

五十一　CRYPTREC（Cryptography Research and Evaluation Committees）　電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトをいう。

五十二　電子政府推奨暗号リスト　CRYPTREC 暗号リストにおいて、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分である、又は今後の普及が見込まれると判断され、当該暗号技術の利用を推奨するもののリストをいう。

五十三　アルゴリズム　ある特定の目的を達成するための演算手順をいう。

五十四　セキュリティパッチ　発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

五十五　サービス不能攻撃　悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。

五十六　ウェブクライアント　ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

五十七　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、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。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。

五十八　ソーシャルメディア　インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成してい

くものをいう。

五十九　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、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。

第２章　情報取扱い

第１節　情報の取扱い

（情報の目的外での利用等の禁止）

第３条　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。

（情報の格付及び取扱制限の決定・明示等）

第４条　業務従事者は、情報の作成時及び機構外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等する。

２　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。

３　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を決定した業務従事者（決定を引き継いだ者を含む。）又は決定した業務従事者の上司（以下この節において「決定者等」という。）に確認し、その結果に基づき見直す。

（情報の利用・保存）

第５条　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。

２　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、課室情報セキュリティ責任者の許可を得る。

３　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。

４　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、情報の格付及び取扱制限に従って情報を適切に管理する。

５　業務従事者は、機密性３情報を機器等に保存する際、次の各号に掲げる措置を講ずる。ただし、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

一　インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等の使用

二　その保存する情報に対し、暗号化による保護

三　その保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策

６　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。

（情報の提供・公表）

第６条　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。

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

３　業務従事者は、機密性３情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得る。

４　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。

（情報の運搬・送信）

第７条　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。

２　業務従事者は、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬する。

３　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。

４　業務従事者は、機密性３情報を機構外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信する。ただし、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えるこ

とができる。

（情報の消去・抹消）

第８条　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。

２　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、全ての情報を抹消する。

３　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。

（情報のバックアップ）

第９条　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。

２　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。

３　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、前条の規定に従い、適切な方法で消去、抹消又は廃棄する。

第３章　情報を取り扱う区域の管理

第１節　情報を取り扱う区域の管理

（要管理対策区域における対策の基準の決定）

第１０条　統括情報セキュリティ責任者は、要管理対策区域の範囲を定める。

２　統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、次の各号に掲げる全ての対策における観点を含む対策の基準を運用規程として定める。

一　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

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

（区域ごとの対策の決定）

第１１条　情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定める。

２　区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等

とを勘案し、当該区域において実施する対策を決定する。

（要管理対策区域における対策の実施）

第１２条　区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施する。業務従事者が実施すべき対策については、業務従事者が認識できる措置を講ずる。

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

３　業務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する。また、機構外の者を立ち入らせる際には、当該機構外の者にも当該区域で定められた対策に従って利用させる。

第４章　外部委託

第１節　業務委託

（業務委託に係る運用規程の整備）

第１３条　統括情報セキュリティ責任者は、業務委託（機構の情報を取り扱わせる場合に限る。以下この節において同じ。）に係る次の各号に掲げる全ての基準を含む運用規程を整備する。

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

二　委託先の選定基準

（業務委託実施前の対策）

第１４条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、次の各号に掲げる全ての事項を実施する。

一　委託する業務内容の特定

二　委託先の選定条件を含む仕様の策定

三　仕様に基づく委託先の選定

四　契約の締結

五　委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

２　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、次の各号に掲げる事項の全ての実施を委託先に求める。

一　仕様に準拠した提案

二　契約の締結

三　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

（業務委託実施期間中の対策）

第１５条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において次の各号に掲げる全ての事項を含む対策を実施する。

一　委託判断基準に従った要保護情報の提供

二　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

三　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業務従事者より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

２　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において次の各号に掲げる全ての事項を含む対策の実施を委託先に求める。

一　情報の適正な取扱いのための情報セキュリティ対策

二　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

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

（業務委託終了時の対策）

第１６条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の終了に際して次の各号に掲げる全ての事項を含む対策を実施する。

一　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

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

２　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して次の各号に掲げる全ての事項を含む対策の実施を委託先に求める。

一　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

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

第２節　クラウドサービスの選定（要機密情報を取り扱う場合）

（クラウドサービスの利用に係る規程の整備）

第１７条　統括情報セキュリティ責任者は、クラウドサービスの利用において要機密情報を取り扱う場合は、次の各号に掲げる全ての事項を含む当該利用に関する規程を整備する。

一　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（以下この節において「クラウドサービス利用判断基準」という。）

二　クラウドサービス提供者の選定基準

三　クラウドサービスに係る利用申請の許可権限者及び利用手続

四　クラウドサービス管理者の指名及びクラウドサービスの利用状況の管理

（クラウドサービスの選定）

第１８条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討する。

２　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びに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、次の各号に掲げる全ての事項を含むセキュリティ要件を定める。

一　クラウドサービスに求める情報セキュリティ対策

二　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

三　クラウドサービスに求めるサービスレベル

３　情報システムセキュリティ責任者又は課室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、原則としてISMAP 等クラウドサービスリストからクラウドサービスを選定する。

（クラウドサービスの利用に係る調達）

第１９条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含める。

２　情報システムセキュリティ責任者又は課室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し、利用承認を得る。また、当該契約に調達仕様の内容を含める。

（クラウドサービスの利用承認）

第２０条　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行う。
２　利用申請の許可権限者は、前項におけるクラウドサービスの利用申請を審査し、利用の可否を決定する。
３　利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名する。

第３節　クラウドサービスの利用（要機密情報を取り扱う場合）

（クラウドサービスの利用に係る運用規程の整備）
第２１条　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備する。
２　統括情報セキュリティ責任者は、サービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備する。
３　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、次の各号に掲げる全ての事項を含むクラウドサービスの利用を終了する際における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。
一　クラウドサービスの利用終了時における対策
二　クラウドサービスで取り扱った情報の廃棄
三　クラウドサービスの利用のために作成したアカウントの廃棄

（クラウドサービスの利用に係るセキュリティ要件の策定）
第２２条 クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認する。
２　クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定する。

（クラウドサービスを利用した情報システムの導入・構築時の対策）
第２３条　クラウドサービス管理者は、第２２条第１項で定めた運用規程を踏まえて、

前条第２項において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずる。また、導入・構築時に実施状況を確認・記録する。

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

３　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに次の各号に掲げる全ての手順を実施手順として整備する。

一　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

二　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

三　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

（クラウドサービスを利用した情報システムの運用・保守時の対策）

第２４条　クラウドサービス管理者は、第２１条第２項で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施する。また、運用・保守時に実施状況を定期的に確認・記録する。

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

３　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。

（クラウドサービスを利用した情報システムの更改・廃棄時の対策）

第２５条　クラウドサービス管理者は、第２１条第３項で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずる。また、クラウドサービスの利用終了時に実施状況を確認・記録する。

第４節　クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

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

第２６条　統括情報セキュリティ責任者は、クラウドサービスの利用において要機密情報を取り扱わない場合は、次の各号に掲げる全ての事項を含む当該利用に関する運用

規程を整備する。
一　クラウドサービスを利用可能な業務の範囲
二　クラウドサービスの利用申請の許可権限者及び利用手続
三　クラウドサービス管理者の指名及びクラウドサービスの利用状況の管理
四　クラウドサービスの利用の運用手順規程

（要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施）
第２７条　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利用申請の許可権限者へ要機密情報を取り扱わない場合の外部サービスの利用を申請する。
２　利用申請の許可権限者は、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。
３　利用申請の許可権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録する。
４　クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずる。

第５節　機器等の調達

（機器等の調達に係る運用規程の整備）
第２８条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備する。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機構が確認できることを当該運用規程に加える。
２　統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備する。

第５章　情報システムのライフサイクル

第１節　情報システムの分類

（情報システムにおける分類のための運用規程の整備）
第２９条　統括情報セキュリティ責任者は、情報システムの情報セキュリティインシデ

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

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

第３０条　統括情報セキュリティ責任者は、情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を運用規程として整備する。

（情報システムの分類基準に基づいた分類の実施）

第３１条　統括情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ、実施した結果を報告させる。情報システムセキュリティ責任者から報告を受けた情報システムの分類結果については、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行う。

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

第３２条　統括情報セキュリティ責任者は、情報システムの分類基準及び分類基準に応じた情報セキュリティ対策の具体的な対策事項の運用規程について定期的な確認による見直しをする。

２　統括情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認する。

第２節　情報システムのライフサイクルの各段階における対策

（実施体制の確保）

第３３条　情報システムセキュリティ責任者は、最高情報セキュリティ責任者に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求める。

２　最高情報セキュリティ責任者は、前項で求められる体制の確保に関し、情報システムを統括する責任者（組織規程第７条に規定するデジタル監（組織）の長）の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求める。

（情報システムの分類基準に基づいた分類の実施）

第３４条　情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告する。

（情報システムのセキュリティ要件の策定）

第３５条　情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等を勘案し情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、次の各号に掲げる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。

一　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

二　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を含む。）

三　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

四　情報システムの可用性に関する対策要件

五　情報システムのネットワーク構成に関する要件

２　情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットから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。

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

４　情報システムセキュリティ責任者は、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要求する情報システムについては、情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等へ助言を求め、業務の特性や情報システムの特性を踏まえて、上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いかを確認する。

（情報システムの構築時の対策）

第３６条　情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずる。

２　情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。
３　情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告する。
４　情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の各号に掲げる全ての情報を含む情報システム関連文書を整備する。
一　情報システムを構成するサーバ装置及び端末関連情報
二　情報システムを構成する通信回線及び通信回線装置関連情報
５　情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の各号に掲げる全ての手順を含む実施手順を整備する。

一　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
二　障害・事故等を認知した際の対処手順
三　情報システムが停止した際の復旧手順

（納品検査時の対策）
第３７条　情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達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。
２　情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認する。

（情報システムの運用・保守時の対策）
第３８条　情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用する。
２　情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直す。
３　情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システム台帳及び関連文書の内容に変更が生じた場合、情報システム台帳及び関連文書

を更新又は修正する。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告する。

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

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

（情報システムの更改・廃棄時の対策）

第３９条　情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、次の各号に掲げる全ての事項を含む措置を適切に講ずる。

一　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

二　情報システム廃棄時の不要な情報の抹消

（情報システムについての対策の見直し）

第４０条　情報システムセキュリティ責任者は、対策推進計画に基づき情報システムの情報セキュリティ対策を適切に見直す。

２　情報システムセキュリティ責任者は、機構内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直す。また、措置の結果については、統括情報セキュリティ責任者へ報告する。

第３節　情報システムの運用継続計画

（情報システムの運用継続計画の整備・整合的運用の確保）

第４１条　統括情報セキュリティ責任者は、機構において非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討する。

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

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

第６章　情報システムの構成要素

第１節　端末

（端末の導入時の対策）

第４２条　情報システムセキュリティ責任者は、要保護情報を取り扱う物理的な端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。

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

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

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

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

（端末の運用時の対策）

第４３条　情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認及びその見直しを行う。

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

（端末の運用終了時の対策）

第４４条　情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消する。

（機構が支給する端末（要管理対策区域外で使用する場合に限る。）の導入及び利用に係る運用規程の整備）

第４５条　統括情報セキュリティ責任者は、業務従事者が機構で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、これらの端末及び利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定める。

２　統括情報セキュリティ責任者は、要機密情報を取り扱う機構が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）について、盗難、紛失、不正プログ

ラムの感染等により情報が窃取されることを防止するための技術的な措置に関する運用規程を整備する。

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

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

第４６条　情報システムセキュリティ責任者は、業務従事者が機構で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）を用いて要機密情報を取り扱う場合は、当該端末について前条第２項の技術的な措置を講ずる。

２　情報システムセキュリティ責任者は、要管理対策区域外において機構外通信回線に接続した機構が支給する物理的な端末を機構内通信回線に接続させる際、当該端末について前条第３項の技術的な措置を講ずる。

（機構支給以外の端末の利用可否の判断）

第４７条　最高情報セキュリティ責任者は、機構支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機構が講じる安全管理措置、当該端末の管理は機構ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機構における機構支給以外の端末の利用の可否を判断する。

（機構支給以外の端末の利用に関する運用規程等の整備）

第４８条　統括情報セキュリティ責任者は、業務従事者が機構支給以外の端末を用いて機構の業務に係る情報処理を行う場合の許可等の手続を実施手順として定める。

２　統括情報セキュリティ責任者は、業務従事者が機構支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報が窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定める。

３　統括情報セキュリティ責任者は、要機密情報を取り扱う機構支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置を含めた安全管理措置に関する運用規程を整備する。

４　統括情報セキュリティ責任者は、要管理対策区域外において機構外通信回線に接続した機構支給以外の端末を機構内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機構内通信回線を経由して情報システム

が不正プログラムに感染するリスクを踏まえた安全管理措置に関する運用規程及び許可手続に関する実施手順を定める。

（機構支給以外の端末の利用に関する責任者）

第４９条　情報セキュリティ責任者は、機構支給以外の端末を用いた機構の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定める。

（機構支給以外の端末の利用時の対策）

第５０条　業務従事者は、機構支給以外の端末を用いて機構の業務に係る情報処理を行う場合には、端末管理責任者の許可を得る。

２　業務従事者は、機構支給以外の端末を用いて要保護情報を取り扱う場合は、第４８条第２項で定める実施手順に従う。

３　端末管理責任者等は、要機密情報を取り扱う機構支給以外の端末について、第４８条第３項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。

４　業務従事者は、情報処理の目的を完了した場合は、要保護情報を機構支給以外の端末から消去する。

第２節　サーバ装置

（サーバ装置の導入時の対策）

第５１条　情報システムセキュリティ責任者は、要保護情報を取り扱う物理的な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。

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

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

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

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

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

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

（サーバ装置の運用時の対策）

第５２条　情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認及び見直しを行う。

２　情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成及び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、その改善を図る。

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

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

（サーバ装置の運用終了時の対策）

第５３条　情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消する。

（電子メールの導入時の対策）

第５４条　情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定する。

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

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

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

（ウェブサーバの導入・運用時の対策）

第５５条　情報システムセキュリティ責任者は、ぜい弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用する。

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

３　情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を行う主体を限定する。

４　情報システムセキュリティ責任者は、インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の

対策を講じる。

（DNS の導入時の対策）

第５６条　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずる。

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

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

（DNS の運用時の対策）

第５７条　情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持する。

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

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

（データベースの導入・運用時の対策）

第５８条　情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。

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

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

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

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

第３節　複合機・特定用途機器

（複合機）

第５９条　情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定する。
２　情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずる。
３　情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消する。

（IoT 機器を含む特定用途機器）
第６０条　情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずる。

第４節　通信回線

（通信回線の導入時の対策）
第６１条　情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。
２　情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。
３　情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずる。
４　情報システムセキュリティ責任者は、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。機構内通信回線へ機構支給以外の端末を接続する際も同様とする。
５　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずる。

（機構外通信回線の接続時の対策）
第６２条　情報システムセキュリティ責任者は、機構内通信回線にインターネット回線、公衆通信回線等の機構外通信回線を接続する場合には、機構内通信回線及び当該機構

内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。

２　情報システムセキュリティ責任者は、機構内通信回線と機構外通信回線との間及び機構内通信回線内の不正な通信の有無を監視するための措置を講ずる。

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

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

（通信回線の運用時の対策）

第６３条　情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の確認及び見直しを行う。

２　情報システムセキュリティ責任者は、機構内通信回線と機構外通信回線との間及び機構内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認及び見直しをする。

３　情報システムセキュリティ責任者は、保守又は診断のために、機構外通信回線から機構内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認及び見直しをする。

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

（通信回線装置の導入時の対策）

第６４条　情報システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないよう措置を講ずる。

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

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

４　情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェア

に関連する公開されたぜい弱性について対策を実施する。

（通信回線装置の運用時の対策）

第６５条　情報システムセキュリティ責任者は、通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し、保管する。

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

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

（通信回線装置の運用終了時の対策）

第６６条　情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用されたとき、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。

（無線 LAN 環境導入時の対策）

第６７条　情報システムセキュリティ責任者は、無線 LAN 技術を利用して機構内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる。

（IPv6 通信を行う情報システムに係る対策）

第６８条　情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、可能な場合には IPv6 Ready Logo Program に基づく Phase-2 準拠製品を選択する。

２　情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、IPv6 通信による情報セキュリティ上の脅威又はぜい弱性に対する検討を行い、必要な措置を講ずる。

（意図しない IPv6 通信の抑止・監視）

第６９条　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で

想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずる。

第５節　ソフトウェア

（情報システムの基盤を管理又は制御するソフトウェア導入時の対策）

第７０条　情報システムセキュリティ責任者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講ずる。

２　情報システムセキュリティ責任者は、利用するソフトウェアの特性を踏まえ、次の各号に掲げる全ての手順を実施手順として整備する。

一　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

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

（情報システムの基盤を管理又は制御するソフトウェア運用時の対策）

第７１条　情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、次の各号に掲げる全ての対策を実施する。

一　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

二　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

第６節　アプリケーション・コンテンツ

（アプリケーション・コンテンツの作成に係る運用規程の整備）

第７２条　統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機構外の情報セキュリティ水準の低下を招く行為を防止するための運用規程を整備する。

（アプリケーション・コンテンツのセキュリティ要件の策定）

第７３条　情報システムセキュリティ責任者は、機構外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについてのセキュリティ要件を定め、仕様に含める。

２　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、前項各号に掲げる内容を調達仕様に含める。

（アプリケーション・コンテンツの開発時の対策）

第７４条　情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずる。

（アプリケーション・コンテンツの運用時の対策）

第７５条　情報システムセキュリティ責任者は、利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直す。

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

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

（政府ドメイン名の使用）

第７６条　情報システムセキュリティ責任者は、機構外向けに提供するウェブサイト等が実際の機構提供のものであることを利用者が確認できるように、政府ドメイン名を取得できない場合を除き政府ドメイン名を情報システムにおいて使用する。

２　業務従事者は、機構外向けに提供するウェブサイト等の作成を業務委託する場合においては、機構に適するドメイン名を使用するよう調達仕様に含める。

（不正なウェブサイトへの誘導防止）

第７７条　情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機構のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずる。

（アプリケーション・コンテンツの告知）

第７８条　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。

２　業務従事者は、機構外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つ。

第７章　情報システムのセキュリティ要件

第１節　情報システムのセキュリティ機能

（主体認証機能の導入）

第７９条　情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。

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

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

（識別コード及び主体認証情報の管理）

第８０条　情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずる。

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

（アクセス制御機能の導入）

第８１条　情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設ける。

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

（権限の管理）

第８２条　情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずる。

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

３　情報システムセキュリティ責任者は、主体から対象に対する不要なアクセス権限が

付与されていないか定期的に確認する。

（ログの取得・管理）

第８３条　情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

２　情報システム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等について定め、適切にログを管理する。

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

（暗号化機能・電子署名機能の導入）

第８４条　情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、次の各号に掲げる全ての措置を講ずる。

一　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。

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

２　情報システムセキュリティ責任者は、電子政府推奨暗号リストに基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定める。また、その運用方法について実施手順を定める。

３　情報システムセキュリティ責任者は、機構における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定める。

（暗号化・電子署名に係る管理）

第８５条　情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、次の各号に掲げる全ての措置を講ずる。

一　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。

二　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システ

ムにおいて、暗号化又は電子署名のために選択されたアルゴリズム又は鍵長の危殆化及びプロトコルのぜい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。

（監視機能の導入・運用）

第８６条　情報システムセキュリティ責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装する。

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

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

第２節　情報セキュリティの脅威への対策

（ソフトウェアに関するぜい弱性対策の実施）

第８７条　情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたぜい弱性についての対策を実施する。

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

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

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

（不正プログラム対策の実施）

第８８条　情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。

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

３　情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必

要な対処を行う。

（サービス不能攻撃対策の実施）

第８９条　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。

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

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

（標的型攻撃対策の実施）

第９０条　情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずる。

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

第３節　ゼロトラストアーキテクチャ

（動的なアクセス制御における責任者の設置）

第９１条　統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任する。

（動的なアクセス制御の導入方針の検討）

第９２条　情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定める。

（動的なアクセス制御の実装時の対策）

第９３条　情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、

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

（動的なアクセス制御の実装方針の見直し）
第９４条　情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しを必要に応じて実施する。

（リソースの信用情報に基づく動的なアクセス制御の運用時の対策）
第９５条　情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を随時行う。

第８章　情報システムの利用

第１節　情報システムの利用

（情報システムの利用に係る規程の整備）
第９６条　統括情報セキュリティ責任者は、機構の情報システムの利用のうち、情報セキュリティに関する実施手順を整備する。
２　統括情報セキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順を定める。
３　統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定める。

（情報システム利用者の規定の遵守を支援するための対策）
第９７条　情報システムセキュリティ責任者は、業務従事者による規定の遵守を支援する機能について情報セキュリティリスク及び業務効率化の観点から支援する範囲を検討し、当該機能をもつ情報システムを構築する。

（情報システムの利用時の基本的対策）
第９８条　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。
２　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機構の情報システムを接続しない。
３　業務従事者は、機構内通信回線に、情報システムセキュリティ責任者の接続許可を

受けていない情報システムを接続しない。

４　業務従事者は、業務の遂行において、利用が認められていないソフトウェアを利用しない。また、当該ソフトウェアを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。

５　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。

６　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。

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

８　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。

（端末（支給外端末を含む）の利用時の対策）

第９９条　業務従事者は、機構が支給する端末（要管理対策区域外で使用する場合に限る。）及び機構支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従う。

２　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、課室情報セキュリティ責任者の許可を得る。

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

二　機構支給以外の端末　要保護情報

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

（電子メール・ウェブの利用時の対策）

第１００条　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、機構が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用する。

２　業務従事者は、機構外の者と電子メールにより情報を送受信する場合は、政府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政府ドメイン名を使用する。

３　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。

４　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。
５　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。
６　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、次の各号に掲げる全ての事項を確認する。
一　送信内容が暗号化されること
二　当該ウェブサイトが送信先として想定している組織のものであること

（識別コード・主体認証情報の取扱い）
第１０１条　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。
２　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。
３　業務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用する。
４　業務従事者は、自己の主体認証情報の管理を徹底する。

（暗号・電子署名の利用時の対策）
第１０２条　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、鍵長及び方法に従う。
２　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。
３　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。

（不正プログラム感染防止）
第１０３条　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。
２　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。

（Web 会議サービスの利用時の対策）
第１０４条　業務従事者は、定められた利用手順に従い、Web 会議の参加者及びその取り扱う情報に応じた情報セキュリティ対策を実施する。
２　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。

（クラウドサービスを利用した機構外の者との情報の共有時の対策）

第１０５条　業務従事者は、機構外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずる。

２　業務従事者は、機構外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除する。

第２節　ソーシャルメディアによる情報発信

（ソーシャルメディアによる情報発信時の対策）

第１０６条　統括情報セキュリティ責任者は、機構が管理するアカウントでソーシャルメディアを利用することを前提として、次の各号に掲げる全ての措置を含む情報セキュリティ対策に関する運用規程を定める。また、当該サービスの利用において要機密情報が取り扱われないよう規定する。

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

二　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、要安定情報の国民への提供にソーシャルメディアを用いる場合は、機構の自己管理ウェブサイトに当該要安定情報を掲載して参照可能とする。

第３節　テレワーク

（テレワークに係る運用規程の整備）

第１０７条　統括情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策に係る運用規程を整備する。また、原則としてテレワークは機構が支給する端末で行うよう定める。

（テレワークの実施環境における対策）

第１０８条　情報システムセキュリティ責任者は、テレワークの実施により機構外通信回線を経由して機構の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保する。

２　情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行う。
３　情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じる。
４　情報システムセキュリティ責任者は、リモートアクセスする端末を最新のぜい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。

（テレワーク実施時における対策）
第１０９条　情報システムセキュリティ責任者は、テレワーク実施前及び実施後に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。
２　業務従事者は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定する。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意する。
３　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、又は不十分な機構外通信回線を利用してテレワークを行わない。

第１０章　雑則

（本基準の管理部署）
第１１０条　この基準を管理する担当課等はリスクマネジメント推進室とする。

附則
（施行期日）
第１条　この基準は、平成２３年１月１日から施行する。

附則
（施行期日）
第１条　この基準は、平成２３年４月１日から施行する。

附則
（施行期日）
第１条　この基準は、平成２５年１月１８日から施行する。

附則
（施行期日）
第１条　この基準は、平成２７年４月１日から施行する。

附則
（施行期日）
第１条　この基準は、平成３０年４月１日から施行する。

附則
（施行期日）
第１条　この基準は、平成３１年１月７日から施行する。

附則
（施行期日）
第１条　この基準は、令和元年１０月１５日から施行する。

附則
（施行期日）
第１条　この基準は、令和２年３月２６日から施行する。

附則
（施行期日）
第１条　この基準は、令和４年１０月２１日から施行する。

附則
（施行期日）
第１条　この基準は、令和５年４月１日から施行する。

附則
（施行期日）
第１条　この基準は、令和７年１月３０日から施行する。