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１７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ものである。

（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　「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。

二　「クラス３」とは、クラス２より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域をいう。

三　「クラス２」とは、クラス１より強固な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域をいう。

四　「クラス１」とは、最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域をいう。

五　「クラス０」とは、クラス３、クラス２及びクラス１以外の区域をいう。六　「受渡業者」とは、要管理対策区域内で職務に従事する業務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

七　「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

八　「可用性１情報」とは、可用性２情報以外の情報（書面を除く。）をいう。

九　「可用性２情報」とは、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機構の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。

十　「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。

十一　「完全性１情報」とは、完全性２情報以外の情報（書面を除く。）をいう。

十二　「完全性２情報」とは、機構の業務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、国民の権利が侵害され又は機構の業務の的確

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。

十三　「機構外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び機構管理又は他組織管理）及び通信回線装置を問わず、機構が管理していない電子計算機が接続され、当該電子計算機間の通信に利用する論理的な通信回線をいう。

十四　「機構内」とは、機構が管理する組織又は建物の内をいう。

十五　「機構内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び機構管理又は他組織管理）及び通信回線装置を問わず、機構が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。

十六　「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。

十七　「機密性１情報」とは、独立行政法人等の保有する情報の公開に関する法律（平成１３年法律第１４０号）（以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報をいう。

十八　「機密性２情報」とは、機構の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む情報であって、「機密性３情報」以外の情報をいう。

十九　「機密性３情報」とは、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。）に定める秘密文書に準じた機密性を要する情報を含む情報をいう。

二十　「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況などを考慮して、１つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードという。

二十一　「権限管理」とは、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。

二十二　「公開された脆弱性」とは、誰もが知り得る状態に置かれている脆弱性のことであり、ソフトウェアやハードウェアの製造・提供元等から公表された脆弱性、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表された脆弱性が該当する。

二十三　「サービス」とは、サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能ｒｔ群をいう。

二十四　「最小特権機能」とは、管理者権限を実行できる範囲を管理作業に必要な最小の範囲に制限する機能をいう。

二十五　「識別」とは、情報システムにアクセスする主体を特定することをいう。

二十六　「識別コード」とは、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 が挙げられる。

二十七　「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、機構の業務の遂行に支障を及ぼすものをいう。

二十八　「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

二十九　「主体認証」とは、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。

　なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本基準における「主体認証」については、公的又は第三者による証明に限るものではない。

三十　「主体認証情報」とは、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。

三十一　「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、磁気ストライプカードや IC カード等がある。

三十二　「情報セキュリティ関係規程」とは、情報セキュリティ管理規程及び本基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。

三十三　「情報の移送」とは、機構外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。

三十四　「ソフトウェア」とは、電子計算機を動作させる手順及び命令を電子計算機が理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム上で動作するアプリケーションを含む広義の意味である。

三十五　「端末」とは、端末を利用する業務従事者が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆる PC のほか、PDA 等も該当する。

三十六　「通信回線」とは、これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、電子計算機間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線という。

三十七　「通信回線装置」とは、回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。

三十八　「電子計算機」とは、コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。

三十九　「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組合せにより主体認証を行う方法である。

四十　「不正プログラム」とは、コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。

四十一　「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。

四十二　「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。

四十三　「複合機」とは、プリンタ、ファクシミリ、イメージスキャナ及びコピー機等の機能を統合している機器をいう。

四十四　「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム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をいう。

四十五　「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。

四十六　「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

第２章　情報の分類と対策、情報のライフサイクルにわたる対策

第１節　情報の利用

（格付け及び取扱制限に従った情報の取扱い）

第３条　業務従事者は、利用する情報に明示等された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。

（要保護情報の取扱い）

第４条　業務従事者は、業務の遂行以外の目的で、要保護情報を機構外に持ち出さないこと。

２　業務従事者は、要保護情報を放置しないこと。

３　業務従事者は、要機密情報を必要以上に複製しないこと。

４　業務従事者は、要機密情報を必要以上に配布しないこと。

第２節　情報の保存

（格付けに応じた情報の保存）

第５条　業務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。

２　業務従事者は、情報の格付け及び取扱制限に応じて、情報が保存された電磁的記録媒体を適切に管理すること。

３　業務従事者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面のうち要機密情報である書面、又は重要な設計書を適切に管理すること。

４　業務従事者は、要機密情報を電磁的記録媒体に保存する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。

５　業務従事者は、要機密情報を電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

６　業務従事者は、要保全情報を電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

７　業務従事者は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。

８　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。

９　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、第１４条及び第１５条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

１０　業務従事者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。

１１　業務従事者は、情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずること。

１２　業務従事者は、機密性３情報を機器等に保存する場合には次の措置を講ずること。

一　機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器を使用すること。

二　当該情報に対し、暗号化による保護を行うこと。

三　当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための措置を講ずること。

（情報の保存期間）

第６条　業務従事者は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

第３節　情報の移送

（情報の移送に関する許可及び届出）

第７条　業務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する場合には、課室情報セキュリティ責任者の許可を得ること。

２　業務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面を移送する場合には、課室情報セキュリティ責任者に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

（情報の送信と運搬の選択）

第８条　業務従事者は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

（移送手段の決定）

第９条　業務従事者は、要保護情報又は重要な設計書を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

２　業務従事者が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課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こと。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

３　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の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。

４　業務従事者は、要保護情報である電磁的記録を送信する場合は、機構が管理する通信回線又は信頼できる通信回線を使用する等安全確保に留意して送信手段を決定すること。

（書面に記載された情報の保護対策）

第１０条　業務従事者は、要機密情報である書面又は重要な設計書を運搬する場合には、情報の格付け及び取扱制限などに応じて、別途定める手順書に従い安全確保のための適切な措置を講ずること。

（電磁的記録の保護対策）

第１１条　業務従事者は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。

２　業務従事者は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

３　業務従事者は、要保全情報である電磁的記録を移送する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

４　業務従事者は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めたときは、情報のバックアップを取得すること。

５　業務従事者は、要安定情報である電磁的記録を移送する場合には、移送中の滅失、

紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

第４節　情報の提供

（情報の公表）

第１２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情報に格付けされるものであることを確認すること。

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。

３　業務従事者は、電磁的記録を公表する場合には、当該情報の付加情報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。

４　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こと。

（他者への情報の提供）

第１３条　業務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を機構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こと。

２　業務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面を機構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に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた提供については、この限りでない。

３　業務従事者は、要保護情報又は重要な設計書を機構外の者に提供する場合には、提供先において、当該情報に付された情報の格付け及び取扱制限に応じて適切に取り扱われるための措置を講ずること。

４　業務従事者は、電磁的記録を提供する場合には、当該記録の付加情報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。

第５節　情報の消去

（電磁的記録の消去）

第１４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しなければならない。

２　業務従事者は、電磁的記録媒体を廃棄する場合には、すべての情報を復元が困難な状態にする（以下「抹消する」という。）こと。

３　業務従事者は、電磁的記録媒体を他の者へ提供する場合には、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

（書面の廃棄方法）

第１５条　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。

第３章　情報セキュリティ要件の明確化に基づく対策

第１節　情報セキュリティについての機能

（主体認証機能の導入）

第１６条　情報システムセキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。

２　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。

３　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こと。

４　情報システムセキュリティ管理者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないよう以下のとおり管理すること。

一　主体認証情報を保存する場合には、その内容の暗号化を行うこと。

二　主体認証情報を通信する場合には、その内容の暗号化を行うこと。

三　保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。

５　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。

一　利用者が定期的に変更しているか否かを確認する機能

二　利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

６　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。

７　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。

一　利用者が、自らの主体認証情報を設定する機能

二　利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

８　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項が適用可能かどうかを検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。

一　正当な主体以外の主体認証を受諾しないこと。（誤認の防止）

二　正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）

三　正当な主体が容易に他者に主体認証情報を付与（発行、更新及び変更を含む。以下本条において同じ。）及び貸与ができないこと。（代理の防止）

四　主体認証情報が容易に複製できないこと。（複製の防止）

五　情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）

六　必要時に中断することなく主体認証が可能であること。（可用性の確保）

七　新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）

八　主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

９　情報システムセキュリティ責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

（識別コードの管理）

第１７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こと。

２　業務従事者は、自己に付与された識別コードを他者に主体認証に用いる目的のため

に付与及び貸与しないこと。

３　業務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。

４　業務従事者は、業務のために識別コードを利用する必要がなくなった場合は、その旨を情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、情報システムセキュリティ責任者が定めている場合は、この限りでない。

５　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こと。

（主体認証情報の管理）

第１８条　業務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

２　情報システムセキュリティ責任者又は情報システムセキュリティ管理者は、主体認証情報が他者に使用され、又はその危険が発生したことの報告を受けた場合には、必要な措置を講ずること。

３　業務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

一　自己の主体認証情報を他者に知られないように管理すること。

二　自己の主体認証情報を他者に教えないこと。

三　主体認証情報を忘却しないように努めること。

四　主体認証情報を設定するに際しては、容易に推測されないものにすること。

五　情報システムセキュリティ管理者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。

六　他の情報システムで利用している主体認証情報を別の情報システムで設定しないこと。

４　業務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。

一　主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。

二　主体認証情報格納装置を他者に譲渡及び貸与しないこと。

三　主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

四　主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者又は情報システムセキュリティ管理者に返還すること。

（アクセス制御機能の導入）

第１９条　情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。

２　情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。

３　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。

（適正なアクセス制御）

第２０条　情報システムセキュリティ責任者は、業務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付け及び取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

（権限管理機能の導入）

第２１条　情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。

２　情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。

（識別コードと主体認証情報の付与管理）

第２２条　情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断するとともに、やむを得ず共用識別コードを付与する必要性がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いを定め、それに従って利用者に付与すること。

２　情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。

一　主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続

二　主体認証情報の初期配布方法及び変更管理手続

三　アクセス制御情報の設定方法及び変更管理手続

３　情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。

４　権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。
５　権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。
６　権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下本条において同じ。）すること。
７　権限管理を行う者は、業務従事者が情報システムを利用する必要がなくなった場合には、当該業務従事者の識別コード及び主体認証情報を無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コード及び主体認証情報の有無を点検すること。
８　権限管理を行う者は、業務従事者が情報システムを利用する必要がなくなった場合には、当該業務従事者に交付した主体認証情報格納装置を返還させること。
９　権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。
１０　権限管理を行う者は、単一の情報システムにおいては、１人の業務従事者に対して単一の識別コードのみを付与すること。
１１　権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。
１２　権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。

（識別コードと主体認証情報における代替手段等の適用）
第２３条　情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった業務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。
２　情報システムセキュリティ責任者及び情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を停止させること。

（証跡管理機能の導入）
第２４条　情報システムセキュリティ責任者は、すべての情報システムについて、証跡

管理を行う必要性の有無を検討すること。

２　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

３　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。

４　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。

５　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。

（証跡の取得と保存）

第２５条　情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ責任者が情報システムに設けた機能を利用して、証跡を記録すること。

２　情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

３　情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。

（取得した証跡の点検、分析及び報告）

第２６条　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ統括情報セキュリティ責任者若しくは情報セキュリティ責任者に報告すること。

２　情報システムセキュリティ責任者は、取得した証跡を効率的かつ確実に点検及び分析しその結果を報告するために、必要に応じて、当該作業を支援する機能を導入すること。

（証跡管理に関する利用者への周知）

第２７条　情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ管理者及び利用者等に対して、証

跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

（保証のための機能の導入）

第２８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情報システムについて、保証のための対策を行う必要性の有無を検討すること。

２　情報システムセキュリティ責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。

（暗号化機能及び電子署名の付与に係る方式の整備）

第２９条　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付与について、そのアルゴリズム及び方法は次に従うこと。これによりがたい場合は、あらかじめ統括情報セキュリティ責任者に協議し、その指示に従うこと。

一　電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。

二　情報システムの新規構築又は更新に伴い暗号化又は電子署名の付与を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名の付与を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。

２　統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下同じ。）の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等（以下「鍵の管理手順等」という。）を定めること。

３　情報システムセキュリティ責任者は、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、鍵の保存方法及び保存場所（以下「鍵の保存方法等」という。）を定めること。

４　情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。

（暗号化機能及び電子署名機能の導入）

第３０条　情報システムセキュリティ責任者は、要機密情報（書面を除く。以下同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

２　情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システ

ムには、暗号化を行う機能を設けること。
３　情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。
４　情報システムセキュリティ責任者は、電子署名の付与及び検証を行う必要があると認めた情報システムには、電子署名の付与及び検証を行う機能を設けること。

（暗号化及び電子署名に係る管理）
第３１条　情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、信頼できる機関による電子証明書の提供等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提供すること。
２　情報システムセキュリティ責任者は、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。

（暗号化機能及び電子署名機能の利用）
第３２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及び方法に従うこと。
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及び鍵の保存方法等に従い、これを適切に管理すること。

第２節　情報セキュリティについての脅威

（情報システムの構築時の脆弱性対策）
第３３条　情報システムセキュリティ責任者は、電子計算機及び通信回線装置の設置又は運用開始時に、脆弱性が混入されることを防ぐためのセキュリティ実装方針、セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合には修正が施されること、ソフトウェアのサポート期間又はサポート打ち切り計画に対する情報提供を仕様書に明記する等して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の対策を実施すること。
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、電子計算機及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。
３　情報システムセキュリティ責任者は、外部公開する電子計算機の設置又は運用開始時にセキュリティ診断（プラットフォーム診断及びアプリケーション診断）を実施し、情報システムセキュリティ責任者又は情報セキュリティ責任者は診断結果を統括情

報セキュリティ責任者に報告すること。また、発見された脆弱性に対する対策の実施状況を統括情報セキュリティ責任者に報告すること。

（情報システムの運用時の脆弱性対策）

第３４条　情報システムセキュリティ責任者は、電子計算機及び通信回線装置の運用時における脆弱性対策を実施すること。

２　情報システムセキュリティ管理者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開された脆弱性に関連する情報を適宜入手すること。

３　情報システムセキュリティ責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、脆弱性に関連する情報を入手した場合には、当該脆弱性が情報システムにもたらすリスクを分析した上で、以下の事項について判断し、脆弱性対策計画を策定すること。

一　対策の必要性

二　対策方法

三　対策方法が存在しない場合の一時的な回避方法

四　対策方法又は回避方法が情報システムに与える影響

五　対策の実施予定

六　対策試験の必要性

七　対策試験の方法

八　対策試験の実施予定

４　情報システムセキュリティ管理者は、脆弱性対策計画に基づき脆弱性対策を講ずること。

５　情報システムセキュリティ管理者は、脆弱性対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。

６　情報システムセキュリティ管理者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

７　情報システムセキュリティ管理者は、定期的に脆弱性対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

８　情報システムセキュリティ責任者は、入手した脆弱性に関連する情報　及び対策方法に関して、必要に応じ、他の情報システムセキュリティ責任者と共有すること。

９　情報システムセキュリティ責任者は、外部公開する電子計算機について年１回以上セキュリティ診断（プラットフォーム診断及びアプリケーション診断）を実施し、情

報システムセキュリティ責任者又は情報セキュリティ責任者は診断結果を統括情報セキュリティ責任者に報告すること。また、発見された脆弱性に対する対策の実施状況を統括情報セキュリティ責任者に報告すること。

（情報システムの構築時の不正プログラム対策）

第３５条　情報システムセキュリティ責任者は、情報システムの構築時における不正プログラム対策を実施する。

２　情報システムセキュリティ責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。）にアンチウイルスソフトウェア等を導入すること。

３　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すべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。

（情報システムの運用時の不正プログラム対策）

第３６条　情報システムセキュリティ管理者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、業務従事者にその対処の実施に関する指示を行うこと。

２　業務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

３　業務従事者は、アンチウイルスソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

４　業務従事者は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にすること。

５　業務従事者は、アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

６　業務従事者は、外部からデータやソフトウェアを電子計算機等（業務従事者が機構支給以外の情報システムを業務に使用する場合にはそれを含む）に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

７　業務従事者は、ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

８　業務従事者は、不正プログラムに感染した恐れのある場合には、感染した電子計算機（業務従事者が機構支給以外の情報システムを業務に使用する場合にはそれを含む）の通信回線への接続を速やかに切断し、必要な措置を講ずること。

９　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、その見直しを行うこと。

（情報システムの構築時のサービス不能攻撃対策）

第３７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電子計算機、通信回線装置又は通信回線を有する情報システムに限る。）については、サービス提供に必要な電子計算機及び通信回線装置を、障害及び過度のアクセス並びにサービス不能攻撃への対策として冗長化構成とすることなどにより可用性を確保すること。

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、障害、過度のアクセス及び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。

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、可用性を確保することを目的に、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。

（情報システムの構築時の踏み台対策）

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（インターネット等の機構外の通信回線に接続される電子計算機、通信回線装置又は通信回線を有する情報システムに限る。）が踏み台として使われることを防止するための措置を講ずること。

（情報システムの構築時の標的型攻撃対策）

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。

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）を講ずること。

第３節　情報システムのライフサイクル

（情報システムの計画時の情報セキュリティ対策検討）

第４０条　情報システムセキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ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。

２　情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムに係る規程等に応じた体制の確保を、

最高情報セキュリティ責任者に求めること。

３　最高情報セキュリティ責任者は、前二項で求められる体制の確保に関し、情報統括官の協力を得ることが必要な場合は、情報統括官に当該体制の全部又は一部の整備を求めること。

４　情報システムセキュリティ責任者は、情報システムに係る政府調達におけるセキュリティ要件策定マニュアルを活用するなどして、情報システムが提供する業務及び取り扱う情報、利用環境を考慮した上で、必要となる情報システムのセキュリティ要件を適切に決定すること。また、開発する情報システムが運用される際に想定される脅威を分析し、当該情報システムにおいて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適切に策定し、仕様書等に明記すること。

５　情報システムセキュリティ責任者は、「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、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において考慮すべき脅威を検討し、必要なセキュリティ要件を策定すること。

６　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、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について定めること。

７　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に重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

８　情報システムセキュリティ責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。

９　情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

１０　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段階へ移行す

るに当たって、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。

（情報システムの構築・運用の情報セキュリティ対策実施）

第４１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、運用に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うとともに、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。

２　情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する機関との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

３　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すること。

（情報システムの移行・廃棄時の情報セキュリティ対策実施）

第４２条　情報システムセキュリティ責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。

（情報システムの見直し時の情報セキュリティ対策実施）

第４３条　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見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

（情報システムの台帳整備）

第４４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、当該情報システムの台帳の記載事項について統括情報セキュリティ責任者に報告すること。政府情報システム管理データベースの登録対象となるシステムについては、当該データベースに必要な情報を記録し、適時最新の情報に更新すること。

２　統括情報セキュリティ責任者は、すべての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。

一　情報システム名、管理課室及び管理責任者の氏名・連絡先

二　システム構成

三　接続する機構外通信回線の種別
四　取り扱う情報の格付け及び取扱制限に関する事項
五　当該情報システムの設計・開発、運用、保守に関する事項

３　前項に関し、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合には、以下の事項を含めた事項を記載した台帳を整備すること。
一　情報処理サービス名
二　契約事業者
三　契約期間
四　情報処理サービスの概要
五　ドメイン名

第４章　情報システム及び保管施設設備の構成要素についての対策

第１節　施設と環境

（要管理対策区域のクラス、管理及び利用制限）

第４４条の２　統括情報セキュリティ責任者は、要管理対策区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限の手順を定めること。
２ 区域情報セキュリティ責任者は、要管理対策区域については、当該区域を管理又は利用する業務従事者がクラスについて認識できる措置を講ずること。
３ 区域情報セキュリティ責任者は、要管理対策区域を管理する場合には、当該区域のクラスを確認し、第１項及び前項に定める管理対策及び利用制限を講ずること。
４ 区域情報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、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。
５ 業務従事者は、情報を取り扱う場合には、情報を取り扱う区域のクラスを確認し、第１項及び第３項に定める管理対策及び利用制限に従って利用すること。

（立入り及び退出の管理）

第４５条　区域情報セキュリティ責任者は、要管理対策区域に不審者を立ち入らせない措置を講ずること。
２　区域情報セキュリティ責任者は、要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。
３　区域情報セキュリティ責任者は、要管理対策区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。
４　情報システムセキュリティ責任者は、立入りを許可された者が、立入りを許可され

ていない者を要管理対策区域へ立ち入らせ、及び要管理対策区域から退出させない措置を講ずること。

５　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情報システムについては、下位クラスの区域と物理的に隔離し、立入り及び退出を管理するための措置を講ずること。

６　区域情報セキュリティ責任者は、クラス３の区域へ継続的に立ち入る者を承認する手続を整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載するための文書を整備すること。

７　区域情報セキュリティ責任者は、クラス３の区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前項の文書へ反映させること。また、当該変更の記録を保存すること。

８　情報システムセキュリティ責任者は、クラス３の区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。

（訪問者及び受渡業者の管理）

第４６条　情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。

２　区域情報セキュリティ責任者は、要管理対策区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。

３　区域情報セキュリティ責任者は、要管理対策区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。

４　区域情報セキュリティ責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。

５　区域情報セキュリティ責任者は、クラス３の区域への訪問者がある場合には、訪問相手の業務従事者が訪問者のクラス３の区域への立入りについて審査するための手続を整備すること。

６　区域情報セキュリティ責任者は、訪問者が不正な行為を行うことを防止するために、業務従事者が訪問者に立会うなどにより、その者を放置しないための措置を講ずること。訪問者が作業を行う場合には、業務従事者が立会うなど監視のための措置を講ずること。

７　区域情報セキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。

一　クラス３以外の区域で受渡しを行うこと。

二　業者がクラス３の区域へ立ち入る場合は、当該業者がクラス３の区域内の電子計

算機、通信回線装置、記録媒体に触れることができない場所に限定し、業務従事者が立ち会うこと。

（電子計算機及び通信回線装置のセキュリティ確保）

第４７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情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。

２　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情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。

３　情報システムセキュリティ責任者は、業務従事者が離席時に電子計算機及び通信回線装置を不正操作から保護するための措置を講ずること。

（クラス３の区域内のセキュリティ管理）

第４８条　業務従事者は、情報システムセキュリティ責任者の承認を得た上で、要保護情報を取り扱う情報システムに関連する物品のクラス３の区域への持込み及びクラス３の区域からの持出しを行うこと。

２　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情報システムに関連する物品のクラス３の区域への持込み及びクラス３の区域からの持出しに係る記録を取得すること。

３　情報システムセキュリティ責任者は、情報システムに関連する物品のクラス３の区域への持込み及びクラス３の区域からの持出しにおいて、入退室時の検査や作業中の監視等により不正プログラム対策や情報漏えいを防止するための措置を講ずること。

４　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については、情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）のクラス３の区域への持込みについて制限すること。

（災害及び障害への対策）

第４９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については、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。

第２節　電子計算機

（電子計算機の設置時の情報セキュリティ対策）

第５０条　情報システムセキュリティ責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。これにあたっては、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定すること。

一　当該情報システムを構成する電子計算機関連事項

イ　電子計算機を管理する業務従事者及び利用者を特定する情報

ロ　電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン

ハ　電子計算機の仕様書又は設計書

二　当該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事項

イ　通信回線及び通信回線装置を管理する業務従事者を特定する情報

ロ　通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

ハ　通信回線及び通信回線装置の仕様書又は設計書

ニ　通信回線の構成

ホ　通信回線装置におけるアクセス制御の設定

ヘ　通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応

ト　通信回線の利用部署

三　情報システムの構成要素のセキュリティ維持に関する手順

イ　電子計算機のセキュリティ維持に関する手順

ロ　通信回線を介して提供するサービスのセキュリティ維持に関する手順

ハ　通信回線及び通信回線装置のセキュリティ維持に関する手順

四　障害・事故等が発生した際の対処手順

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電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

３　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情報システムについては、サーバ装置をクラス３の区域に設置すること。ただし、モバイル PC については別に定める。

（電子計算機の運用時の情報セキュリティ対策）

第５１条　情報システムセキュリティ管理者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理において情報セキュリティ対策を行うこと。

２　業務従事者は、業務の遂行以外の目的で電子計算機を利用しないこと。

３　情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されている

すべ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電子計算機を検出した場合には、当該不適切な状態の改善を図ること。

４　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。

（電子計算機の運用終了時の情報セキュリティ対策）

第５２条　情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体のすべての情報を抹消すること。

（端末の設置時の情報セキュリティ対策）

第５３条　情報システムセキュリティ責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙し、又は両者を併用することができる。

（端末の運用時の情報セキュリティ対策）

第５４条　業務従事者は、端末で利用可能と定められたソフトウェアを除いて、ソフトウェアを利用しないこと。

２　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。

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

４　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端末を接続しないこと。

５　情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、端末の時刻を同期すること。

（サーバ装置の設置時の情報セキュリティ対策）

第５５条　情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化するための機能を設けること。

２　情報システムセキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。

３　情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼働している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーショ

ンであっても、利用しない機能を無効化して稼働すること。
４　情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないソフトウェアをサーバ装置から削除すること。

（サーバ装置の運用時の情報セキュリティ対策）
第５６条　情報システムセキュリティ責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。
２　情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。
３　情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。
４　情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。
５　情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。
６　情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。

（複合機の情報セキュリティ対策）
第５７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、当該複合機に対して想定される脅威を分析等した上で、適切なセキュリティ要件を策定すること。
２　情報システムセキュリティ責任者は、利用者認証が成功した者のみ印刷が許可される機能を活用する等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。
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、契約で対策を講ずるなどにより、複合機の電磁的記録媒体の全ての情報を抹消すること。

（特定用途機器の情報セキュリティ対策）
第５８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、特定用途機器のソフトウェアに関する脆弱性への対応など当該機器の特性に応じた対策を講ずること。

第３節　アプリケーションソフトウェア

（電子メール導入時の情報セキュリティ対策）

第５９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こと。

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 SMTP 認証等による業務従事者の主体認証を行う機能を備えること。

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こと。

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、相手の電子メールサーバが対応している場合には、電子メールのサーバ間通信の暗号化を行うこと。

（電子メール運用時の情報セキュリティ対策）

第６０条　業務従事者は、業務遂行に係る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こと。ただし、機構支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

２　業務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。

３　情報システムセキュリティ責任者は、受信メールに対するフィルタリング機能や電子メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能等、職員が不審な電子メールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。また当該機能に係る設定や条件は定期的に見直すこと。

（ウェブサーバ導入時の情報セキュリティ対策）

第６１条　情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。

一　ディレクトリインデックスの表示を禁止する等ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

二　作成や更新に必要な者以外に更新権を与えない等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。

三　公開を想定していないファイルをウェブ公開用ディレクトリに置かない等公開してはならない又は無意味なウェブコンテンツが公開されないように管理するこ

と。

四　ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

五　サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること

２　情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

（ウェブ開発時及び運用時の情報セキュリティ対策）

第６２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、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。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

２　情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。

３　情報システムセキュリティ責任者は、ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。

（ウェブ利用時の情報セキュリティ対策）

第６３条　業務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。

２　業務従事者は、ウェブクライアントが動作する電子計算機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。

３　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。

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。

４　情報システムセキュリティ責任者は、業務従事者が閲覧することが可能な機構外のウェブサイトを制限し、定期的にその見直しを行うこと。

（DNS 導入時の情報セキュリティ対策）

第６４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 DNS の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。

２　情報システムセキュリティ責任者は、DNS の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を運用管理するための手続を定めること。

３　情報システムセキュリティ責任者は、DNS のキャッシュサーバにおいて、機構外からの名前解決の要求には応じず、機構内からの名前解決の要求のみに回答を行うための措置を講ずること。

４　情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて、機構内のみで使用する名前解決を提供する場合、当該情報が機構外に漏えいしないための措置を講ずること。

（DNS 運用時の情報セキュリティ対策）

第６５条　情報システムセキュリティ管理者は、DNS の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。

２　情報システムセキュリティ管理者は、DNS の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を運用管理するための手続に基づいて、当該情報が正確であることを定期的に確認すること。

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こと。

（データベースの導入・運用時の対策）

第６６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こと。

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、措置を講ずること。

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、通常の業務によるデータベースの操作から逸脱した証跡を記録する等対策を講ずること。

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こと。

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こと。データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等に対しても暗号化を実施すること。

第４節　通信回線

（通信回線の構築時の情報セキュリティ対策）

第６７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、必要に応じてセグメントを分けるなど、通信回線に対して必要な対策を講ずること。

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こと。

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、TLS（Transport Layer Security）等により通信内容の秘匿性を確保するための措置を講ずること。

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、情報システムの機器番号による識別等によって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措置を講ずること。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、通信回線装置をクラス３又はクラス２の区域に設置すること。ただし、クラス３又はクラス２の区域への設置が困難な場合は、物理的な保護措置を講ずる等して、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。

６　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。

７　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や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こと。

８　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。

９　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を定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

１０　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、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。

１１　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。

（通信回線運用時の情報セキュリティ対策）

第６８条　情報システムセキュリティ責任者は、通信回線運用時の情報セキュリティ対策を実施すること。

２　情報システムセキュリティ管理者は、通信回線装置のソフトウェアを変更する場合には、情報システムセキュリティ責任者の許可を得ること。

３　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。

４　情報システムセキュリティ管理者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。

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の確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。

６　業務従事者は、情報システムセキュリティ責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。

７　情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。

８　情報システムセキュリティ責任者は、所管する範囲の通信回線装置が動作するために必要なすべ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通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。

（通信回線の運用終了時の情報セキュリティ対策）

第６９条　情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体のすべての情報を抹消すること。

（機構外通信回線との接続時の情報セキュリティ対策）

第７０条　情報システムセキュリティ責任者は、情報セキュリティ責任者の承認を得た上で、機構内通信回線を機構外通信回線と接続すること。

２　情報システムセキュリティ責任者は、機構内通信回線を機構外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している機構内通信回線又は機構外通信回線から独立した通信回線として機構内通信回線を構築すること。

（機構外通信回線と接続している機構内通信回線の運用時の情報セキュリティ対策）

第７１条　情報システムセキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している機構内通信回線又は機構外通信回線から独立した通信回線に構成を変更すること。

２　情報システムセキュリティ責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

３　情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。

４　情報システムセキュリティ管理者は、機構内通信回線と機構外通信回線との間で送受信される通信内容を監視すること。

（その他の通信回線の情報セキュリティ対策）

第７２条　情報システムセキュリティ責任者は、VPN（暗号化などの技術を用いて、インターネットのような安全ではない通信網において、仮想的に専用線のような安全な通信回線で遠隔地のネットワーク同士を接続する技術）環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信内容の暗号化
三　通信を行う電子計算機の識別又は利用者の主体認証
四　主体認証記録の取得及び管理
五　VPN 経由でアクセスすることが可能な通信回線の範囲の制限
六　VPN 接続方法の機密性の確保
七　VPN を利用する電子計算機の管理

２　情報システムセキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要性があると判断すること。

一　利用開始及び利用停止時の申請手続の整備
二　通信内容の暗号化
三　通信を行う電子計算機の識別又は利用者の主体認証
四　主体認証記録の取得及び管理
五　無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
六　無線 LAN に接続中に他の通信回線との接続の禁止
七　無線 LAN 接続方法の機密性の確保
八　無線 LAN に接続する電子計算機の管理

３　情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備

二　通信を行う者又は発信者番号による識別及び主体認証

三　主体認証記録の取得及び管理

四　リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限

五　リモートアクセス中に他の通信回線との接続の禁止

六　リモートアクセス方法の機密性の確保

七　リモートアクセスする電子計算機の管理

第５章　ソフトウェア開発に係る情報セキュリティ対策

（ソフトウェア開発体制の確立）

第７３条　情報システムセキュリティ責任者は、ソフトウェア開発について、セキュリティにかかわる対策事項（第７４条～７７条の遵守事項）を満たすことが可能な開発体制の確保を、情報システムを統括する責任者に求めること。

２　情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、委託先が実施すべき対策事項（第７４条～７７条の遵守事項）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

（ソフトウェア開発の開始時の情報セキュリティ対策）

第７４条　情報システムセキュリティ責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。

２　情報システムセキュリティ責任者は、ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。

（ソフトウェアの設計時の情報セキュリティ対策）

第７５条　情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付け及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。

２　情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に利用

されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。

３　情報システムセキュリティ責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

４　情報システムセキュリティ責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。

５　情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価・ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

（ソフトウェアの作成時の情報セキュリティ対策）

第７６条　情報システムセキュリティ責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。

２　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コーディングに関する規定を整備すること。

３　情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

（ソフトウェアの試験時の情報セキュリティ対策）

第７７条　情報システムセキュリティ責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する試験項目及び試験方法を定め、これに基づいて試験を実施すること。

２　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実施した試験の実施記録を保存すること。

第６章　個別事項に係る対策

第１節　情報システムへの IPv6 技術の導入における対策

（IPv6 移行機構がもたらす脆弱性対策）

第７８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（以下「IPv6 通信」という。）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。

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、以下の事項を含む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。

一　グローバル IP アドレスによる直接の到達性における脅威

二　IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

三　IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

四　アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

（意図しない IPv6 通信の抑止と監視）

第７９条　情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。

第２節　機構外の情報セキュリティ水準の低下を招く行為の防止

（措置についての要求）

第８０条　統括情報セキュリティ責任者は、機構外の情報セキュリティ水準の低下を招く行為の防止に関する措置を求めること。

（措置の遵守）

第８１条　業務従事者は、機構外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずること。

第３節　アプリケーション・コンテンツ提供時の対策

（ドメイン名の使用）

第８２条　統括情報セキュリティ責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」という。）の使用について、以下の事項を業務従事者に求めること。

２　業務従事者が機構外の者（国外在住の者を除く。以下、本条において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。ただし、情報セキュリティ実施要領第１５条の３に定めるソーシャルメディアサービスによる情報発信を行う場合及び国際約束に基づくものなどやむを得ない場合を除く。

一　go. jp で終わるドメイン名

二　日本語ドメイン名の中で行政等に関するものとして予約されたドメイン名

３　業務従事者が機構外の者に対して、電子メールの送信元としてドメイン名を使用する場合には、政府ドメイン名を使用すること。ただし、当該機構外の者にとって、当該業務従事者が既知の者である場合を除く。

４　業務従事者が機構外の者に対して、アクセスさせることを目的として情報を保存するためにサーバを使用する場合には、政府ドメイン名のサーバだけを使用すること。

５　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外部委託する場合においては、前各項の規定に則り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こと。

（不正なウェブサイトへの誘導防止）

第８３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、クローラ（ロボット型検索エンジンによる自動巡回プログラム）からのアクセスを排除しないなどの対策を講ずること。

２　情報システムセキュリティ責任者は、機構の業務等に関連するキーワードによる検索結果で不審サイトが存在した場合には、不審なサイト検索サイトへのアクセスを防止するための対策を講ずること。

（アプリケーション・コンテンツの告知）

第８４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、URL 等を用いて直接誘導するなど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。

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、告知するアプリケーション・コンテンツを管理する組織を明記する等告知する URL 等の有効性を保つこと。

第７章　業務継続計画との整合的運用の確保

（業務継続計画と情報セキュリティ対策の整合性の確保）

第８５条　情報セキュリティ委員会は、機構において業務継続計画又は情報セキュリティ管理規程及び本基準を整備する場合には、業務継続計画と情報セキュリティ管理規程及び本基準の整合性の確保のための検討を行うこと。

２　統括情報セキュリティ責任者、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課室情報セキュリティ責任者は、機構において業務継続計画の整備計画がある場合には、すべての情報システムについて、当該業務継続計画との関係の有無を検討すること。

３　統括情報セキュリティ責任者、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課室情報セキュリティ責任者は、機構において業務継続計画の整備計画がある場合には、当該業務継続計画と関係があると認めた情報システムについて、以下に従って、業務継続計画、情報セキュリティ管理規程及び本基準に基づく共通の実施手順を整備すること。

４　通常時において業務継続計画と情報セキュリティ管理規程及び本基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。

５　事態発生時において業務継続計画と情報セキュリティ管理規程及び本基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定を整備すること。

（業務継続計画と情報セキュリティ関係規程の不整合の報告）

第８６条　業務従事者は、機構において業務継続計画の整備計画がある場合であって、業務継続計画と情報セキュリティ関係規程が定める要求事項との違いなどにより、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。

第８章　雑則

（本基準の管理部署）

第８７条　この基準を管理する担当課等は情報統括官室とする。

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。