経済産業省

制定　平成18年3月31日
平成18･03･24シ第１号

改正　平成20年2月1日
平成20･02･01シ第２号

改正　平成20年12月10日
平成20･10･29シ第２号

改正　平成21年12月1日
平成21･11･18シ第２号

改正　平成23年4月1日
平成23･04･01シ第２号

改正　平成23年7月25日
平成23･07･08シ第２号

改正　平成24年7月25日
20120719シ第２号

改正　平成27年3月26日
20150324シ第２号

改正　平成29年3月30日
20170327シ第１号

改正　令和元年5月31日
20190529官第2号

改正　令和4年10月24日
20221007官第4号

最終改正　令和6年７月１日
20240624官第5号

本　　省
外　　局

経済産業省情報セキュリティ管理規程（平成１８・０３・２２シ第１号）第２１条の規定に基づき、経済産業省情報セキュリティ対策基準を次のように定める。

平成１８年３月３１日

最高情報セキュリティ責任者
大臣官房長　鈴木　隆史

経済産業省情報セキュリティ対策基準

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、経済産業省情報セキュリティ管理規程（平成１８・０３・２２シ第１号。以下「管理規程」という。）第２１条の規定に基づき、経済産業省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を定める。

（定義）

第２条　この基準における用語の定義は、経済産業省情報セキュリティ管理規程の定義によるほか、次のとおりとする。

（１）　「業務継続計画」とは、経済産業省において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。

（２）　「アプリケーション」とは、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。

（３）　「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。

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

（５）　「記録媒体」とは、情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面その他文字、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（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によって認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、CD-R、DVD、MO、USBメモリ、フラッシュメモリ等の外部電磁的記録媒体がある。

（６）　「サーバ装置」とは、情報システムの構成要素である機器のうち、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、経済産業省が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）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。

（７）　「可用性２情報」とは、経済産業省で取り扱う情報（電磁的記録に限る。）のうち、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行政事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。

（８）　「可用性１情報」とは、経済産業省で取り扱う情報（電磁的記録に限る。）のうち、可用性２情報以外の情報をいう。

（９）　「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

（１０）　「完全性２情報」とは、経済産業省で取り扱う情報（電磁的記録に限る。）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行政事務の遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

（１１）　「完全性１情報」とは、経済産業省で取り扱う情報（電磁的記録に限る。）のうち、完全性２情報以外の情報をいう。

（１２）　「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。

（１３）　「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ユーザID等のコード（符号）をいう。

（１４）　「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。

（１５）　「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群をいう。

（１６）　「主体」とは、情報システムにアクセスする者並びに複数の情報システム及び装置等が連携して動作する場合に情報システム及び装置等にアクセスを行う他の情報システム及び装置等をいう。

（１７）　「主体認証」とは、情報システムが主体から提示された識別コード及び主体認証情報を検証することにより、当該主体が当該識別コードを付与された者か否かを確認することをいう。

（１８）　「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パスワード等の情報をいう。

（１９）　「主体認証情報格納装置」とは、磁気ストライプカード及びICカード等の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。

（２０）　「省内通信回線」とは、経済産業省が管理する電子計算機（一体的に管理している場合、経済産業省が一部管理していないものを含む。）を接続する通信回線をいう。

（２１）　「省外通信回線」とは、経済産業省が管理していない電子計算機が接続する通信回線をいう。

（２２）　「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。

（２３）　「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（PDAを含む。）をいう。

（２４）　「多要素主体認証方式」とは、知識、所有及び生体情報等のうち、複数の方法の組合せにより主体認証を行う方法をいう。

（２５）　「不正プログラム」とは、コンピュータウイルス及び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。

（２６）　「付与」（主体認証に係る情報及びアクセス制御における許可情報等に関する場合に限る。）とは、発行、更新及び変更することをいう。

（２７）　「要安定情報」とは、可用性２情報をいう。

（２８）　「要管理対策区域外」とは、情報取扱区域におけるクラス０の区域をいう。

（２９）　「要機密情報」とは、機密性２情報及び機密性３情報をいう。

（３０）　「要保全情報」とは、完全性２情報をいう。

（３１）　「要保護情報」とは、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。

（３２）　「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。

（３３）　「特定用途機器」とは、テレビ会議システム、IP電話システム及び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機器をいう。

（３４）　「情報セキュリティインシデント」とは、電磁的記録に関する障害及び事故等であって、JIS　Q　27000：2019　における情報セキュリティインシデントに該当するものをいう。

（３５）　「CSIRT（Computer　Security　Incident　Response　Team）」とは、発生した情報セキュリティインシデントに対処するため、事態を正確に把握し、被害拡大防止、復旧、再発防止策等を迅速かつ的確に行うことを可能とするため経済産業省に設置された体制をいう。

（３６）　「クラウドサービス」とは、事業者によって定義されたインターフェースを用いた、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（経済産業省外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するサービスであって、当該サービスにおいて経済産業省の情報が取り扱われるものに限る。）をいう。

（３７）　「クラウドサービス管理者」とは、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経済産業省の職員等をいう。

（３８）　「クラウドサービス提供者」とは、クラウドサービスを提供する事業者をいう。

（３９）　「ドメイン名」とは、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.meti.go.jpというウェブサイトの場合は、meti.go.jpの部分がこれに該当する。

（４０）　「名前解決」とは、ドメイン名やホスト名とIPアドレスを変換することをいう。

（４１）　「アプリケーション・コンテンツ」とは、経済産業省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。

（４２）　「CYMAT（Cyber Incident Mobile Assistance Team）」とは、サイバー攻撃等により国の行政機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。

（４３）　「ソーシャルメディア」とは、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。

（４４）　「Web会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像または音声を用いて会議参加者が対面せずに会議を行える外部サービス（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）を除く。）をいう。

（４５）　「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。

（４６）　「暗号化」とは、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。

（４７）　「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、暗号技術検討会及び関連委員会を指し、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である。

（４８）　「情報の抹消」とは、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、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。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。

（４９）　「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（WindowsのBitLocker等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

（５０）　「政府ドメイン名」とは、.go.jpで終わるドメイン名のことをいう。

（５１）　「テレワーク」とは、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。

（５２）　「電子署名」とは、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。

（５３）　「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。

（５４）　「ウェブクライアント」とは、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。

（５５）　「サービス不能攻撃」とは、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。

（５６）　「セキュリティパッチ」とは、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。

（５７）　「耐タンパ性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。

（５８）　「電子政府推奨暗号リスト」とは、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か今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストをいう。

（５９）　「電子メールサーバ」とは、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。

（６０）　「電子メールクライアント」とは、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。

（６１）　「ドメインネームシステム（DNS）」とは、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である。

（６２）　「無線LAN」とは、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。

（６３）　「NISC」とは、内閣官房内閣サイバーセキュリティセンターをいう。

第２章　情報セキュリティ対策の基本的枠組み

第１節　導入・計画

（情報セキュリティ対策推進体制の整備）

第３条　管理規程第１０条第１項に基づき、情報セキュリティ対策推進体制の役割は、次に掲げる事務を行うこととする。

（１）　情報セキュリティ関係規程及び対策推進計画の策定に係る事務

（２）　情報セキュリティ関係規程の運用に係る事務

（３）　例外措置に係る事務

（４）　情報セキュリティ対策の教育の実施に係る事務

（５）　情報セキュリティ対策の自己点検に係る事務

（６）　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

２　情報セキュリティ対策推進体制は、管理規程第１０条第２項で定める責任者の下、前項の役割に応じて必要な事務を遂行する。

（最高情報セキュリティ副責任者への委任）

第４条　最高情報セキュリティ責任者は、管理規程第３条第４項に基づいて、以下の権限を最高情報セキュリティ副責任者に委任する。ただし、本項の規定により委任された権限は、最高情報セキュリティ責任者が自ら行使することを妨げない。

（１）　管理規程第２１条第２項における運用規程等整備状況の報告受理

（２）　第６条第５項におけるインシデント報告体制の整備と報告受理

（３）　第１１条第３項における情報セキュリティインシデントの報告受理

（４）　第１３条第１項及び２項における情報セキュリティインシデント再発防止策の報告受理及び必要な措置の指示

（５）　第２０条第２項における関係規程に係る運用状況の報告受理

（例外措置の審査手続）

第５条　管理規程第２４条に基づき、職員等が情報セキュリティ関連規程における例外措置の適用を希望する場合に審査し、許可する許可権限者及び審査手続は次の各号のとおりとする。

（１）　例外措置の適用の申請を審査し、許可する許可権限者は、統括情報セキュリティ責任者をもって充てる。

（２）　例外措置の申請は、以下の審査項目を明記して、事前に行わなければならない。ただし、行政事務の遂行に緊急を要し、情報セキュリティ関係規程の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定を実施しないことが不可避のときは、事前申請が実施できなかった理由等を記載した経緯書とともに事後速やかに申請しなければならない。

（ア）　申請者の情報（氏名、所属、連絡先）

（イ）　例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）

（ウ）　例外措置の適用を申請する期間

（エ）　例外措置の適用を申請する措置内容（講ずる代替手段等）
（オ）　例外措置により生じる情報セキュリティ上の影響と対処方法
（カ）　例外措置の適用を終了した旨の報告方法
（キ）　例外措置の適用を申請する理由
（ク）　その他必要な事項

（３）　申請者は、申請事項が他組織や他部署と関連のある場合は、事前に関連先に協議し、調整を行った上で例外措置の申請を行わなければならない。

（４）　統括情報セキュリティ責任者は、例外措置において必要な情報セキュリティ水準の確保が出来ないと判断する場合は、これを許可してはならない。

（５）　統括情報セキュリティ責任者は、例外措置の申請手続の助けとするため、必要に応じて申請手続に関する実施手順を整備することが出来る。

（６）　統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、申請状況を記録し、定期的に最高情報セキュリティ副責任者に報告する。

（７）　統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

（情報セキュリティインシデントに備えた体制の整備）

第６条　最高情報セキュリティ責任者は、CSIRTを整備し、その役割を明確化する。

２　最高情報セキュリティ責任者は、職員等のうちからCSIRTに属する職員等として専門的な知識又は適性を有すると認められる者を選任する。また、CSIRT内の業務統括及び外部との連携等を行う職員等を定める。

３　最高情報セキュリティ責任者は、経済産業省における情報セキュリティインシデントに対処するための責任者として、統括情報セキュリティ責任者をCSIRT責任者として充てる。

４　最高情報セキュリティ責任者は、CSIRTの役割、職員の体制及び情報セキュリティインシデントへの対処等に関して、統括情報セキュリティ責任者に実施手順を整備させる。

５　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が発生した際、直ちに自らへの報告が行われる体制を整備する。

６　最高情報セキュリティ責任者は、CYMATに属する職員を指名する。

（情報システム台帳の整備）

第７条　統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備する。

２　統括情報セキュリティ責任者は、以下の内容を全て含む台帳を整備する。

（１）　情報システム名
（２）　管理課室
（３）　当該情報システムセキュリティ責任者の氏名及び連絡先
（４）　システム構成
（５）　接続する省外通信回線の種別
（６）　取り扱う情報の格付及び取扱制限に関する事項
（７）　当該情報システムの設計・開発、運用、保守に関する事項
（８）　情報システムの利用目的
（９）　情報システムの分類基準に基づいて実施した情報システムの分類結果
（１０）　連携する情報システム及び連携内容

３　また、民間事業者等が提供するクラウドサービス等を利用して情報システムを構築する場合は、前項各号の事項に加え、以下を全て含む内容についても台帳として整備する。

（１）　クラウドサービス等の名称（クラウドサービスの場合、必要に応じて機能名までを含む）

（２）　クラウドサービス等の提供者の名称

（３）　利用期間

（４）　クラウドサービス等の概要

（５）　ドメイン名

（６）　クラウドサービス等で取り扱う情報の格付及び取扱制限に関する事項

（７）　情報の暗号化に用いる鍵の管理主体（経済産業省管理かクラウドサービス等の提供者管理か）

（８）　クラウドサービス等で取り扱う情報が保存される国・地域

（９）　サービスレベル

第２節　運用

（教育体制の整備・教育実施計画の策定）

第８条　統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

２　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直す。

３　統括情報セキュリティ責任者は、職員等の役割に応じて教育すべき内容を検討し、教育のための資料を整備する。

４　統括情報セキュリティ責任者は、職員等が毎年度１回以上は教育を受講できるように整備する。

５　統括情報セキュリティ責任者は、使用する情報システムに変更がある職員等に対し、着任時又は異動時に新しい職場等で、３か月以内に受講できるように整備する。

（情報セキュリティ教育の実施）

第９条　課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を適切に受講させる。

２　職員等は、教育実施計画に従って、適切な時期に教育を受講する。

３　課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及びCSIRTに属する職員等に教育を適切に受講させる。また、CYMATに属する職員にも教育を適切に受講させる。

４　課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告する。

５　課室情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告する。

（情報セキュリティインシデントに備えた事前準備）

第１０条　統括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の可能性を認知した際の報告窓口を含む経済産業省関係者への報告手順を整備し、報告が必要な具体例を含め、職員等に周知する。

２　統括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の可能性を認知した際の省外との情報共有を含む対処手順を整備する。
３　統括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備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。
４　統括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への対処の訓練の必要性を検討し、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、その訓練の内容及び体制を整備する。
５　統括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省外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を省外の者に明示する。
６　統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認する。

（情報セキュリティインシデントへの対処）
第１１条　職員等は、情報セキュリティインシデントの可能性を認知した場合には、前条第１項に基づく手順に従い報告窓口に報告し、指示に従う。
２　CSIRT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。
３　CSIRT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。
４　CSIRT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又は勧告を行う。また、CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システムセキュリティ責任者へ確認を指示する。
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について情報セキュリティインシデントを認知した場合には、経済産業省で定められた対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処する。
６　政府共通利用型システム利用機関の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政府共通利用型システムに関するものである場合には、当該政府共通利用型システムの情報セキュリティ対策に係る運用管理規程に従い、適切に対処する。
７　CSIRT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、警察への通報・連絡等を行う。
８　CSIRTは、情報セキュリティインシデントに関する対処状況を把握し、対処全般に関する指示、勧告又は助言を行う。
９　CSIRT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。
１０　CSIRTは、CYMATの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行う。

（情報セキュリティインシデントに係る情報共有）
第１２条　CSIRTは、経済産業省の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、NISCに連絡する。また、経済産業省が所管する独立行政法人のCSIRTから情報セキュリティインシデントの連絡を受けた場合には、当該事象について速やかに、NISCに連絡する。
２　CSIRTは、認知した情報セキュリティインシデント又は独立行政法人から連絡を受けた情報セ

キュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「大規模サイバー攻撃事態等への初動対処について（平成22年３月19日内閣危機管理監決裁）」に基づく報告連絡を行う。

３　CSIRTは、情報セキュリティインシデントに関して、経済産業省を含む関係機関と情報共有を行う。

４　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告を行う。

（情報セキュリティインシデントの再発防止・教訓の共有）

第１３条　情報セキュリティ責任者は、CSIRTから応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告する。

２　最高情報セキュリティ責任者は、情報セキュリティ責任者から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指示する。

３　CSIRT責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有する。

第３節　点検

（自己点検計画の策定・手順の準備）

第１４条　統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定する。

２　統括情報セキュリティ責任者は、年度自己点検計画に基づき、職員等ごとの自己点検票及び自己点検の実施手順を整備する。

３　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直す。

（自己点検の実施）

第１５条　情報セキュリティ責任者は、前条第１項に基づく年度自己点検計画に基づき、職員等に対して、自己点検の実施を指示する。

２　職員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。

（自己点検結果の評価及び改善）

第１６条　情報セキュリティ責任者は、自己点検結果について、自らが担当する部局庁等の組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を統括情報セキュリティ責任者に報告する。

２　統括情報セキュリティ責任者は、経済産業省に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を最高情報セキュリティ責任者に報告する。

３　最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受ける。

（監査実施計画の策定）

第１７条　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を策定しなければならない。

２　情報セキュリティ監査責任者は、管理規程第２８条第２項の指示を受けた場合には、追加の監査実施計画を策定しなければならない。

（情報セキュリティ監査の実施）

第１８条　情報セキュリティ監査責任者は、監査実施計画に基づき、監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告する。

２　情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名することができる。

３　情報セキュリティ監査責任者は、以下の事項を全て含む監査の実施を監査実施者に指示する。

（１）　対策基準に統一基準を満たすための適切な事項が定められていること

（２）　運用規程及び実施手順が整備されている場合、運用規程及び実施手順が管理規程及び対策基準に準拠していること

（３）　被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること

４　情報セキュリティ監査責任者は、経済産業省外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、経済産業省外の者に監査の一部を請け負わせることができる。

（監査結果に応じた対処）

第１９条　最高情報セキュリティ責任者は、前条第１項の監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示する。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示する。

２　統括情報セキュリティ責任者は、前項の指示に基づき、経済産業省内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

３　情報セキュリティ責任者は、第１項の指示に基づき、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

４　最高情報セキュリティ責任者は、本条で定める必要な措置の実施結果、改善計画及び改善計画に基づく改善の実施について、不十分と認める場合には、情報セキュリティ責任者に追加の指示をすることができる。

（情報セキュリティ関連規程に係る問題点の報告）

第２０条　情報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、職員等から情報セキュリティに係る問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告する。

２　統括情報セキュリティ責任者は、情報セキュリティに係る課題及び問題点を含む運用状況を適

時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告する。

第４節　独立行政法人

（独立行政法人を所管するための体制の整備）

第２１条　統括情報セキュリティ責任者は、管理規程第３１条の指示を受けた場合には、所管する独立行政法人の情報セキュリティ対策が適切に推進されるために必要な体制として、当該法人所管部署等の関係部署及び所管する法人等に必要な助言等を行うための窓口を、当該法人所管部署等の関係部署と連携して整備する。

第３章　情報の取扱い

第１節　情報の取扱い

（情報の目的外での利用禁止）

第２２条　職員等は、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。

２　職員等による機密性３情報の作成又は取得は、必要最小限にとどめなければならない。

（情報の格付及び取扱制限の決定・明示等）

第２３条　職員等は、情報の作成時又は経済産業省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管理規程第２３条に基づく当該情報の格付及び取扱制限の基準並びに格付の取扱制限を明示する手順に基づき、当該情報の格付及び取扱制限を決定し、明示等する。

２　職員等は、機密性３情報以外の情報について、機密性３情報としての表示又はこれに類似の表示を付してはならない。

３　職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付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。

４　職員等は、情報を利用する場合に、元の格付又は取扱制限が現時点において不適切と考えるため、他者が決定した情報の格付又は取扱制限を見直す必要があると思料する場合には、当該情報の格付及び取扱制限を決定した職員等（当該決定を引き継いだ職員等を含む。）又は決定した職員等の上司に確認する。

５　職員等は、自らが格付及び取扱制限の決定者である情報に対して、見直しの必要があると認めた場合には、当該情報の格付又は取扱制限を第１項に基づく再決定に従い、明示等するとともに、当該情報に関係する者に周知する。

６　職員等は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の格付及び取扱制限を変更する必要があると思料する場合には、第１項に基づき再決定する。

（情報の利用・保存）

第２４条　職員等は、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　職員等は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講

ずる。

（１）　要保護情報を放置しない。

（２）　要機密情報を必要以上に複製しない。

（３）　電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

（４）　電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

（５）　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。

３　職員等は、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。

４　課室情報セキュリティ責任者は、機密性３情報について、所在が明らかになるように管理しなければならない。この場合において、当該情報へのアクセスを認める者の範囲を定めなければならない。

５　職員等は、機密性３情報について、金庫等施錠できる書庫その他これと同等の秘密情報の漏えいを防止することができるものとして、課室情報セキュリティ責任者が指定する場所において、適切に保存しなければならない。

６　職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理する。

７　職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

８　職員等は、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。

９　職員等は、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。

（情報の提供・公表）

第２５条　職員等は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認する。

２　職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、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　職員等は、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。

４　職員等は、電磁的記録媒体を他の者へ提供する場合は、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。

（情報の運搬・送信）

第２６条　職員等は、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。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。
2　職員等は、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。
3　職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬する場合には、情報漏えいを防止するための対策を講ずる。
4　職員等は、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。
5　職員等は、要機密情報である電磁的記録を省外通信回線を使用して送信する場合には、情報漏えいを防止するための対策を講ずる。
6　職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、当該情報の送信の手段を決定する。

（情報の消去）
第２７条　職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去する。
2　職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消する。
3　職員等は、端末やサーバ装置等をリース契約で調達する場合は、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、対策を行う。
4　職員等は、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２８条　職員等は、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　職員等は、要保全情報又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、バックアップを取得する。
3　職員等は、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。
4　職員等は、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バックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定する。要保全情報又は要安定情報である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、情報システムや情報とバックアップが同時に破壊されない保管場所を選定する。
5　職員等は、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２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２９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、以下の観点を全て含む対策

の基準を運用規程として定める。

（１）　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。

（２）　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３０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、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。

３　区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定する。

（要管理対策区域における対策の実施）

第３１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。職員等が実施すべき対策については、職員等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　職員等は、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、職員等が省外の者を立ち入らせる際には、当該省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３２条　統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備する。

（１）　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。）

（２）　委託先の選定基準及び選定手続き

（業務委託実施前の対策）

第３３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、以下を全て含む事項を実施する。

（１）　委託する業務内容の特定

（２）　委託先の選定条件を含む仕様の策定
（３）　仕様に基づく委託先の選定
（４）　契約の締結
（５）　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、以下を全て含む事項の実施を委託先に求める。
（１）　仕様に準拠した提案
（２）　契約の締結
（３）　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３４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以下を全て含む対策を実施する。
（１）　委託判断基準に従った要保護情報の提供
（２）　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
（３）　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、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以下を全て含む対策の実施を委託先に求める。
（１）　情報の適正な取扱いのための情報セキュリティ対策
（２）　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
（３）　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３５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以下を全て含む対策を実施する。
（１）　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
（２）　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以下を全て含む対策の実施を委託先に求める。
（１）　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
（２）　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

（情報システムに関する業務委託における共通的対策）

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経済産業省の意図せざる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。

（情報システムの構築を業務委託する場合の対策）

第３７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を業務委託する場合は、契約に基づき、以下を全て含む情報セキュリティ対策の実施を委託先に求める。

（１）　情報システムのセキュリティ要件の適切な実装

（２）　情報セキュリティの観点に基づく試験の実施

（３）　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

（情報システムの運用・保守を業務委託する場合の対策）

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。

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・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。

（機関等向けに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）

第３９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、省外の一般の者が経済産業省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。

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。

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、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。

４　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サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行う。

５　統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定する。

６　統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名する。

第２節　クラウドサービス

（クラウドサービスの選定に係る運用規程の整備）

第４０条　統括情報セキュリティ責任者は、以下を全て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規程を整備する。

（１）　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。）

（２）　クラウドサービスの選定基準

（３）　クラウドサービスの利用申請の許可権限者と利用手続
（４）　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

（クラウドサービスの選定）
第４１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、以下を全て含むセキュリティ要件を定める。
（１）　クラウドサービスに求める情報セキュリティ対策
（２）　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
（３）　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４２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、調達仕様の内容は、契約に含める。

（クラウドサービスの利用承認）
第４３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。

（クラウドサービスの利用に係る運用規程の整備）
第４４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、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、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、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。

（１）　クラウドサービスの利用終了時における対策
（２）　クラウドサービスで取り扱った情報の廃棄
（３）　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４５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４６条　クラウドサービス管理者は、第４４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。なお、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以下の全ての実施手順を整備する。
（１）　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
（２）　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
（３）　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４７条　クラウドサービス管理者は、第４４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。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。
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４８条　クラウドサービス管理者は、第４４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。

（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４９条　統括情報セキュリティ責任者は、以下を全て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規程を整備する。

（１）　クラウドサービスを利用可能な業務の範囲

（２）　クラウドサービスの利用申請の許可権限者と利用手続

（３）　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

（４）　クラウドサービスの利用の運用規程

（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５０条　職員等は、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クラウドサービスの利用を申請する。

２　利用申請の許可権限者は、職員等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３節　機器等の調達

（機器等の調達に係る運用規程の整備）

第５１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、その管理を経済産業省が確認できることを加える。

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５２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５３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５４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５５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５６条　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。

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際し、情報システムを統括する責任者（デジタル統括責任者（CIO））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５７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５８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、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。

（１）　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

（２）　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）

（３）　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

（４）　情報システムの可用性に関する対策要件

（５）　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５９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、以下を全て含む情報システム関連文書を整備する。
（１）　情報システムを構成するサーバ装置及び端末関連情報
（２）　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、以下を全て含む実施手順を整備する。
（１）　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
（２）　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
（３）　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６０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６１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・廃止時の対策）

第６２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、以下を全て含む措置を適切に講ずる。

（１）　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

（２）　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６３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、省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６４条　統括情報セキュリティ責任者は、経済産業省における業務継続計画（以下「業務継続計画」という。）や経済産業省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（以下「運用継続計画」という。）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。

（１）　通常時において業務継続計画、運用継続計画、管理規程及びこの基準との整合的運用が可能となるよう必要な措置を講ずること。

（２）　事態発生時において業務継続計画、運用継続計画、管理規程及びこの基準との整合的運用が可能となるよう実施手順の整備等の必要な措置を講ずること。

2　統括情報セキュリティ責任者は、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、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４節　政府共通利用型システム

（情報セキュリティ対策に関する運用管理規程の整備）

第６５条　情報システムセキュリティ責任者は、政府共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用管理規程を整備し、政府共通利用型シス

テム利用機関と十分な合意形成を行う。

（１）　政府共通利用型システム管理機関と政府共通利用型システム利用機関との間の責任分界

（２）　平常時及び非常時の協力・連携体制

（３）　非常時の具体的対応策

（情報システム台帳及び情報システム関連文書の整備）

第６６条　政府共通利用型システム管理機関の統括情報セキュリティ責任者は、第７条第２項で整備する情報システム台帳について、政府共通利用型システム利用機関に関係するセキュリティ要件に係る事項を含めて整備する。

２　政府共通利用型システム管理機関の情報システムセキュリティ責任者は、第５９条第４項で整備する情報システム関連文書について、政府共通利用型システム利用機関に関係する情報を含めて整備する。

（政府共通利用型システム利用機関における体制の整備）

第６７条　情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程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。

２　統括情報セキュリティ責任者は、政府共通利用型システムが提供する機器等の提供を受けこれを経済産業省の職員等が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに政府共通利用型システム利用管理者を指名する。

３　政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程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。

（政府共通利用型システム利用機関における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、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システム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、適切にセキュリティ要件を策定し、運用する。

２　情報システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

（政府共通利用型システム利用機関における機器等の管理）

第６９条　政府共通利用型システム利用管理者は、政府共通利用型システムが提供する機器等の提供を受けてこれを経済産業省の職員等が利用する場合は、当該政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程及び実施手順を整備する。

２　政府共通利用型システム利用管理者は、提供を受けた政府共通利用型システムの機器等を把握するために必要な文書を整備する。

３　政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、政府共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知する。

４　政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

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７０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。

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脆弱性について対策を実施する。

（端末の運用時の対策）

第７１条　情報システムセキュリティ責任者は、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。

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、改善を図る。

（端末の運用終了時の対策）

第７２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。

（経済産業省が支給する端末（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７３条　統括情報セキュリティ責任者は、職員等が経済産業省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。

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経済産業省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省外通信回線に接続した経済産業

省が支給する物理的な端末を省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、当該端末から省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。

（経済産業省が支給する端末（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７４条　情報システムセキュリティ責任者は、職員等が経済産業省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省外通信回線に接続した経済産業省が支給する物理的な端末を省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。

（経済産業省支給以外の端末の利用可否の判断）

第７５条　最高情報セキュリティ責任者は、経済産業省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、経済産業省が講じる安全管理措置、当該端末の管理は経済産業省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、経済産業省における経済産業省支給以外の端末の利用の可否を判断する。

（経済産業省支給以外の端末の利用に関する運用規程等の整備）

第７６条　統括情報セキュリティ責任者は、職員等が経済産業省支給以外の端末を用いて経済産業省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、職員等が経済産業省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。

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経済産業省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省外通信回線に接続した経済産業省支給以外の端末を省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、当該端末から省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。

（経済産業省支給以外の端末の利用に関する責任者の策定）

第７７条　情報セキュリティ責任者は、経済産業省支給以外の端末を用いた経済産業省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。

（経済産業省支給以外の端末の利用時の対策）

第７８条　職員等は、経済産業省支給以外の端末を用いて経済産業省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　職員等は、経済産業省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７６条第２項

で定める利用手順に従う。
3　端末管理責任者等は、要機密情報を取り扱う経済産業省支給以外の端末について、第７６条第３項に定める安全管理措置を講じる又は職員等に講じさせる。
4　職員等は、情報処理の目的を完了した場合は、要保護情報を経済産業省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７９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、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。
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脆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８０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、定期的な確認による見直しを行う。
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。
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をする。

（サーバ装置の運用終了時の対策）
第８１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８２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、所管する情報システムに、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８３条　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。
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８４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。
2　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、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、DNSのコンテンツサーバにおいて、経済産業省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８５条　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、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、DNSの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８６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８７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８８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８９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、職員等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。省内通信回線へ経済産業省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。

（機関等外通信回線の接続時の対策）

第９０条　情報システムセキュリティ責任者は、省内通信回線にインターネット回線、公衆通信回線等の省外通信回線を接続する場合には、省内通信回線及び当該省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、省内通信回線と省外通信回線との間及び省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、省外通信回線から省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ておく。

（通信回線の運用時の対策）
第９１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、省内通信回線と省外通信回線との間及び省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。
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、省外通信回線から省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。
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９２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にする。
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脆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９３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９４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。

（無線LAN環境導入時の対策）

第９５条　情報システムセキュリティ責任者は、無線LAN技術を利用して省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９６条　情報システムセキュリティ責任者は、IPv6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準拠製品を選択する。ただし、IPv6 Ready Logo Programに基づくPhase-2準拠製品を選択する事が出来ない場合は、この限りではない。

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脆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９７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９８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、以下の全ての実施手順を整備する。

（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の情報セキュリティ水準の維持に関する手順

（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９９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、以下の全てのセキュリティ対策を実施する。

（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のセキュリティを維持するための対策

（２）　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１００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省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１０１条　情報システムセキュリティ責任者は、省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、所管する情報システムの開発等の仕様に含める。

２　職員等は、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。

（アプリケーション・コンテンツの開発時の対策）

第１０２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１０３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１０４条　情報システムセキュリティ責任者は、省外向けに提供するウェブサイト等が実際の経済産業省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　職員等は、省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、経済産業省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１０５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経済産業省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１０６条　職員等は、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　職員等は、省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１０７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、所管する情報システムに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・企業と経済産業省との間の申請、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１０８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１０９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、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１１０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。

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１１１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１１２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、以下の全ての措置を講ずる。

（１）　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。

（２）　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。

2　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会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定める。また、その運用方法について実施手順を定める。

3　情報システムセキュリティ責任者は、経済産業省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１１３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、以下の全ての措置を講ずる。

（１）　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。

（２）　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズム又は鍵長の危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図ること。

（監視機能の導入・運用）

第１１４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脆弱性対策の実施）

第１１５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脆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とり得る対策がある場合は、当該対策を実施する。

３　情報システム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１１６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１１７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１１８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１１９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１２０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１２１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１２２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１２３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１２４条　統括情報セキュリティ責任者は、経済産業省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。

（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１２５条　情報システムセキュリティ責任者は、職員等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と業務効率化の観点から支援する範囲を検討し、当該機能を持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１２６条　職員等は、業務の遂行以外の目的で情報システムを利用しない。

２　職員等は、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経済産業省の情報システムを接続しない。
３　職員等は、省内通信回線に、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　職員等は、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こと。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　職員等は、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　職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずる。
７　職員等は、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、課室情報セキュリティ責任者の許可を得る。
８　職員等は、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１２７条　職員等は、経済産業省が支給する端末（要管理対策区域外で使用する場合に限る）及び経済産業省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　職員等は、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。
（１）　経済産業省が支給する端末（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
（２）　経済産業省支給以外の端末　要保護情報
３　職員等は、要管理対策区域外において省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省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。

（電子メール・ウェブの利用時の対策）
第１２８条　職員等は、要機密情報を含む電子メールを送受信する場合には、経済産業省が運営し、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　職員等は、省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　職員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する。
４　職員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わない。
５　職員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認する。
６　職員等は、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、以下の全ての事項を確認する。
（１）　送信内容が暗号化されること
（２）　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１２９条　職員等は、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　職員等は、自己に付与された識別コードを適切に管理する。

３　職員等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用する。

４　職員等は、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１３０条　職員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム、鍵長及び方法に従う。

２　職員等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理する。

３　職員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

（不正プログラム感染防止）

第１３１条　職員等は、不正プログラム感染防止に関する措置に努める。

２　職員等は、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１３２条　職員等は、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。

２　職員等は、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関等外の者との情報の共有時の対策）

第１３３条　職員等は、省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　職員等は、省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。

（ソーシャルメディアによる情報発信時の対策）

第１３４条　統括情報セキュリティ責任者は、経済産業省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、以下を全て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。

（１）　経済産業省のアカウントによる情報発信が実際の経済産業省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。

（２）　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　職員等は、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、経済産業省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。

（テレワークに係る運用規程の整備）

第１３５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。なお、原則としてテレワークは経済産業省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１３６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省外通信回線を経由して経済産業省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。

（テレワーク実施時における対策）

第１３７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職員等が確認するべき項目を定め、職員等に当該項目を確認させる。

2　職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定する。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意する。

3　職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な省外通信回線を利用してテレワークを行わない。

第９章　雑則

（細則の策定）

第１３８条　最高情報セキュリティ責任者又は統括情報セキュリティ責任者は、この基準に定めるもののほか、必要な細則を定めることができる。

2　情報セキュリティ責任者は、自らの統括する部局又は所管するシステムについて、この基準に定めるほか、必要と認める事項について細則を定めることができる。

3　情報セキュリティ責任者は、前項の細則を制定、改正又は廃止したときは、最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。

附　則（平成１８・０３・２４シ第１号）

この基準は、平成１８年３月３１日から施行する。

附　則（平成２０・０２・０１シ第２号）

この基準は、平成２０年２月１日から施行する。

附　則（平成２０・１０・２９シ第２号）

この基準は、平成２０年１２月１０日から施行する。

附　則（平成２１・１１・１８シ第２号）

この基準は、平成２１年１２月１日から施行する。

附　則（平成２３・０４・０１シ第２号）

１．この基準は、平成２３年４月１日から施行する。

２．この基準の最終改正の施行の際に、従前の経済産業省行政文書管理規程（平成１３・０１・０６広第３号）に基づき、秘密文書としての表示が付されているものについては、「極秘」を機密性４情報に、「秘」を機密性３情報に読み替えて、「経済産業省情報セキュリティ対策基準」の規定を適用するものとする。

附　則（平成２３・０７・０８シ第２号）

この基準は、平成２３年７月２５日から施行する。

附　則（２０１２０７１９シ第２号）

この基準は、平成２４年７月２５日から施行する。

附　則

１．この基準は、経済産業省情報セキュリティ管理規程の一部を改正する訓令（２０１５０３２４シ第１号）の公布の日から施行する。

２.この基準の施行前にした廃止前の特許庁情報セキュリティポリシーに基づく行為については、なお従前の例による。

附　則（２０１９０５２９官第２号）

この基準は、令和元年５月３１日から施行する。

附　則（２０２２１００７官第４号）

この基準は、令和４年１０月２４日から施行する。

附　則（２０２４０６２４官第５号）

この基準は、令和６年７月１日から施行する。