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

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２０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（第１条－第２条）
第２章　情報の格付に応じた対策
　第１節　情報の作成及び入手（第３条－第７条）
　第２節　情報の利用（第８条－第１０条）
　第３節　情報の保存（第１１条－第１２条）
　第４節　情報の移送及び他者への提供（第１３条－第１５条）
　第５節　情報の消去（第１６条－第１７条）
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（第１８条－第３０条）
　第２節　情報セキュリティに関する脅威（第３１条－第３４条）
　第３節　標的型攻撃対策（第３５条）
　第４節　情報システムのライフサイクル（第３６条－第４２条）
第４章　情報システムの構成要素の対策
　第１節　施設と環境（第４３条）
　第２節　端末（第４４条－第４６条）
　第３節　サーバ装置（第４７条－第４９条）
　第４節　複合機（第５０条）
　第５節　特定用途機器（第５１条）
　第６節　電子メール（第５２条－第５３条）
　第７節　ウェブ（第５４条－第５６条）
　第８節　ドメインネームシステム（第５７条－第５８条）
　第９節　データベース（第５９条）
　第１０節　通信回線（第６０条－第６４条）
　第１１節　ＩＰｖ６通信（第６５条－第６６条）
第５章　調達及び開発に係る情報セキュリティ対策
　第１節　機器等の購入（第６７条－第６８条）
　第２節　外部委託（第６９条－第７２条）
　第３節　約款による外部サービス（第７３条）
　第４節　ソーシャルメディアサービスによる情報発信（第７４条）
　第５節　クラウドサービスの利用における対策（第７５条）
第６章　情報処理の制限
　第１節　要管理対策区域外における情報処理の制限（第７６条－第７８条）
　第２節　経済産業省支給の情報機器による情報処理の制限（第７９条－第８０条）
　第３節　経済産業省支給以外の情報機器による情報処理の制限（第８１条－第８３条）
　第４節　アプリケーション・コンテンツ提供時の対策（第８４条－第８７条）
第７章　情報セキュリティ対策に応じた教育、監査等
　第１節　教育（第８８条－第９０条）
　第２節　自己点検（第９１条－第９３条）

第３節　監査（第９４条－第９７条）
第４節　障害及び事故等（第９８条－第１００条）
第５節　業務継続計画（第１０１条）
第６節　情報セキュリティ対策推進体制（第１０２条）
第８章　雑則（第１０３条）

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「規程」という。）第２０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、次のとおりとする。

（１）　「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。

（２）　「委託先」とは、情報を取り扱う経済産業省の業務の一部又は全部を請け負った者をいう。

（３）　「受渡業者」とは、要管理対策区域内で職務に従事する職員等との宅配便の集配及び事務用品の納入等の物品の受渡しを目的として、やむを得ず要管理対策区域へ立ち入る者をいう。

（４）　「外部委託」とは、情報を取り扱う経済産業省の業務の一部又は全部を経済産業省外の者に請け負わせることをいう。

（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）　「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。

（７）　「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。

（８）　「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。

（９）　「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。

（１０）　「機器等」とは、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。

（１１）　「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。

（１２）　「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。

（１３）　「共用識別コード」とは、識別コードのうち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。

（１４）　「経済産業省支給以外の情報システム」とは、私物か、又は他組織が提供したものかを問わず経済産業省が支給する情報システム以外の情報システムをいう。

（１５）　「経済産業省支給以外の情報システムによる情報処理」とは、経済産業省支給以外の情報システムを用いて行政事務の遂行のための情報処理を行うこと（経済産業省支給以外の情報システムによって提供されているサービスを利用する場合も含む。）をいう。

（１６）　「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。

（１７）　「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。

（１８）　「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。

（１９）　「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。

（２０）　「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。

（２１）　「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。

（２２）　「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。

（２３）　「通信回線」とは、複数の電子計算機の間で、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。

（２４）　「通信回線装置」とは、通信回線の接続のために設置され、ハブ、スイッチ、ルータ及びファイアウォール等の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。

（２５）「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。

（２６）　「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。

（２７）　「情報の移送」とは、要管理対策区域外に、電磁的に記録された情報を送信すること、及び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。

（２８）　「ソフトウェア」とは、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。

（２９）　「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。

（３０）　「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。

（３１）　「複数要素（複合）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。

（３２）　「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。

（３３）　「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。

（３４）　「モバイル端末」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、移動して使用することを前提とする端末をいう。

（３５）　「要安定情報」とは、可用性２情報をいう。

（３６）　「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。

（３７）　「要機密情報」とは、機密性２情報及び機密性３情報をいう。

（３８）　「要保全情報」とは、完全性２情報をいう。

（３９）　「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。

（４０）　「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。

（４１）　「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。

（４２）　「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　２７０００：２０１４　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。

（４３）　「約款による外部サービス」とは、経済産業省外の者が約款に基づきインターネット上で提供する情報処理のサービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存及び送信等を行うもの（電気通信サービス、郵便及び運送サービス等を除く。）をいう。ただし、利用者が必要とする情報セキュリティ対策を締結しているものを除く。

（４４）　「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。

（４５）　「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をいう。

（４６）　「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。

（４７）　「アプリケーション・コンテンツ」とは、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。

（４８）　「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。

第２章　情報の格付に応じた対策

第１節　情報の作成及び入手

（情報の業務目的以外での作成又は入手の禁止）

第３条　職員等は、行政事務の遂行以外の目的で情報を作成し、又は入手してはならない。

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。

（職員等による情報の作成又は入手時における格付及び取扱制限の決定）

第４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規程第２２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する。

２　課室情報セキュリティ責任者は、職員等が決定した機密性の格付及び取扱制限の妥当性を判断し、必要に応じ、修正を指示する。

（情報の格付及び取扱制限の明示等）

第５条　職員等は、前条第１項に基づく決定及び前条第２項に基づく修正の指示を受けた場合には明示等を行う。

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。

（情報の格付及び取扱制限の継承）

第６条　職員等は、情報を作成する際に、参照した情報又は入手した情報が既に格付又は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。

２　職員等は、情報を複製する場合には、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。

（情報の格付及び取扱制限の変更）

第７条　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、課室情報セキュリティ責任者に相談する。

２　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４条第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。

３　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４条第１項に基づき再決定する。

第２節　情報の利用

（情報の業務目的以外での利用の禁止）
第８条　職員等は、行政事務の遂行以外の目的で情報を利用してはならない。

（情報の格付及び取扱制限に従った情報の取扱い）
第９条　職員等は、利用する情報に明示等された格付に従って、当該情報を適切に取り扱う。格付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。

（情報の取扱い）
第１０条　職員等は、行政事務の遂行以外の目的で、要保護情報を要管理対策区域外に持ち出してはならない。
２　職員等は、要保護情報を放置してはならない。
３　職員等は、要機密情報を必要以上に配付してはならない。
４　職員等は、機密性３情報を必要以上に複製してはならない。複製に当たっては、課室情報セキュリティ責任者の承認を受けることとする。

第３節　情報の保存

（格付及び取扱制限に応じた情報の保存）
第１１条　職員等は、情報の格付及び取扱制限に応じて、情報を適切に保存する。
２　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。
３　統括情報セキュリティ責任者は、外部電磁的記録媒体を用いた情報の取扱に関する規程を整備する。
４　職員等は、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。
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、要保全情報又は要安定情報について、情報の格付に応じて、適切な方法でバックアップ又は複写の必要の有無を検討し、必要があると認めたときは、バックアップ又は複写を作成する。

（情報の保存期間）
第１２条　職員等は、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。

第４節　情報の移送及び他者への提供

（情報の移送又は他者への提供に関する許可、手段の決定）
第１３条　職員等は、要保護情報を移送する場合又は経済産業省外の者へ提供する場合には、課室

情報セキュリティ責任者の許可を得た上で、情報の格付及び取扱制限に応じて、課室情報セキュリティ責任者が指定する安全確保のための適切な措置を講ずる。ただし、課室情報セキュリティ責任者が許可を要しないと定めた機密性２情報の移送及び経済産業省外の者への提供については、この限りでない。

（電磁的記録を中心とした保護対策）

第１４条　職員等は、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。

２　職員等は、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。

３　職員等は、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。

４　職員等は、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。

５　職員等は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いる必要性の有無を検討し、必要と認めたときは、当該措置を講ずるものとする。

６　職員等は、要保護情報を経済産業省外の者に提供する場合には、提供先において、当該要保護情報が、経済産業省の付した情報の機密性の格付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。

７　職員等は、電磁的記録を経済産業省外の者に提供する場合には、当該記録の付加情報等からの情報漏えいを防止するための措置を講ずる。

（情報の公表）

第１５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、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。

第５節　情報の消去

（電磁的記録の消去方法）

第１６条　職員等は、電磁的記録媒体に保存された情報が不要になった場合は、速やかに消去すること。

２　職員等は、電磁的記録媒体を廃棄する場合には、全ての情報を復元が困難な状態にする。

（要機密情報が記録された書面の廃棄方法）

第１７条　職員等は、要機密情報が記録された書面を廃棄する場合には、破砕、溶解及び焼却等の方法により、復元が困難な状態にする。

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１８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、主体認証を行う必要の有無を検討する。

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（以下「主体認証対象情報システム」という。）において、主体の識別及び主体認証を行う機能を設ける。

３　情報システムセキュリティ管理者は、主体認証対象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に次の各号に掲げる管理を行う。

（１）　主体認証情報を保存する場合には、内容の暗号化を行うこと

（２）　主体認証情報を通信する場合には、内容の暗号化を行うこと

（３）　主体認証情報に対するアクセス制限を設けること

４　情報システムセキュリティ責任者は、主体認証対象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。

（１）　利用者が定期的に変更しているか否かを確認する機能

（２）　利用者が定期的に変更しなければ、主体認証対象情報システムの利用を継続させない機能

５　情報システムセキュリティ責任者は、主体認証対象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主体認証対象情報システムの利用を停止する機能を設ける。

６　情報システムセキュリティ責任者は、主体認証対象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。

（１）　利用者が自らの主体認証情報を設定する機能

（２）　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

７　情報システムセキュリティ責任者は、主体認証対象情報システムにおいて、情報セキュリティ水準と情報システムの利便性等を考慮し、次の各号に掲げる主体認証機能の運用に係る要件の実装要否を判断する。

（１）　正当な主体以外の主体を誤って主体認証しないこと（誤認の防止）

（２）　正当な主体が本人の責任ではない理由で主体認証できなくならないこと（誤否の防止）

（３）　正当な主体が容易に他者に主体認証情報を付与又は貸与ができないこと（代理の防止）

（４）　主体認証情報が容易に複製できないこと（複製の防止）

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

（６）　主体認証について業務遂行に十分な可用性があること（可用性の確保）

（７）　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、それらの供給が主体認証対象情報システムの使用期間の間、十分受けられること（継続性の確保）

（８）　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）

8　情報システムセキュリティ責任者は、主体認証対象情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けるものとする。

（1）　複数要素（複合）主体認証方式で主体認証を行う機能

（2）　ログインした利用者に対して、前回のログインに関する情報を通知する機能

（3）　不正にログインしようとする行為を検知し、又は防止する機能

（4）　利用者が情報システムにログインする前に、当該主体認証対象情報システムの利用に関する通知メッセージを表示する機能

（5）　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、以前に設定した主体認証情報と同じものを再設定することを防止する機能

（6）　管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログインすることが必要となる機能

9　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及び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。

（識別コードの管理）

第１９条　職員等は、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、主体認証対象情報システムを利用してはならない。

2　職員等は、自己に付与された識別コードを他者に付与及び貸与してはならない。

3　職員等は、自己に付与された識別コードを知る必要のない者に知られるような状態で放置してはならない。

4　職員等は、行政事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、情報システムセキュリティ管理者に届け出なければならない。ただし、個別の届出が必要ないと、あらかじめ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　情報システムセキュリティ責任者は、管理者権限を持つ識別コードを付与された職員等に、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させる必要性の有無を検討し、必要と認めたときは、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させるものとする。

6　職員等は、管理者権限を持つ識別コードを付与されたかつ情報システムセキュリティ責任者が求めた場合には、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。

（主体認証情報の管理）

第２０条　職員等は、知識による主体認証情報を用いる場合には、次の各号に掲げる管理を徹底する。

（1）　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

（2）　自己の主体認証情報を他者に教えないこと

（3）　主体認証情報を忘却しないように努めること

（4）　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

（5）　経済産業省支給以外の情報システムの識別コードを含め、異なる識別コードに対して、共通の主体認証情報を用いないこと

（6）　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、指示に従って定期的に変更すること

２　職員等は、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。
（１）　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措置を講じて管理すること
（２）　主体認証情報格納装置を他者に付与又は貸与しないこと
（３）　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報告すること
（４）　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２１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を行う機能を設ける。

（適正なアクセス制御）
第２２条　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、アクセス制御を行う。

（権限管理機能の導入）
第２３条　情報システムセキュリティ責任者は、所管する全ての情報システムについて、権限管理を行う必要の有無を検討する。
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（以下「権限管理対象情報システム」という。）において、権限管理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、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搾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。

（識別コードと主体認証情報の付与管理）
第２４条　情報システムセキュリティ責任者は、権限管理対象情報システムにおいて、共用識別コードを原則付与しないこと。ただし、行政事務の遂行のため、複数の主体で共用する識別コードを付与する必要がある場合には、適切に管理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、権限管理対象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明確にする。
（１）　主体からの申請に基づいて権限管理を行う場合の手続
（２）　主体認証情報の初期配布方法及び変更管理手続
（３）　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、権限管理対象情報システムにおいて、権限管理を行う者を定める。
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。
５　権限管理を行う者は、識別コードを発行する際に、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。ただし、共用識別コードは、情報システムセキュリティ責任者が、利用を認めた情報システムでのみ付与することができる。
６　権限管理を行う者は、管理者権限を持つ識別コードを付与（発行、更新及び変更を含む。以下

この項において同じ。）する場合は、以下の措置を講ずる。

（１）　業務又は業務上の責務に則した場合に限定すること

（２）　初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更すること

（３）　初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更すること

（４）　ネットワークからのログインを制限すること

７　権限管理を行う者は、職員等が情報システムを利用する必要がなくなった場合には、当該職員等の識別コードを無効にする。また、人事異動等により、識別コードを追加し、又は削除するときに、不要な識別コードの有無を点検する。

８　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アクセス制御に係る設定をする。また、人事異動等により、識別コードを追加し、又は削除するときに、不適切なアクセス制御設定の有無を点検する。

９　権限管理を行う者は、以下の措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずるものとする。

（１）　単一の情報システムにおいては、１人の職員等に対して単一の識別コードのみの付与

（２）　識別コードをどの主体に付与したかについての記録及び当該記録を消去する場合の情報セキュリティ責任者からの事前の承認

（３）　主体に付与した識別コードを別の主体に対して付与することの禁止

（証跡の取得等）

第２５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、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証跡を取得する。

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、その特性に応じて証跡を取得する目的を設定した上で、証跡を取得する対象の機器等、証跡として取得する情報項目、証跡の保存期間、要保護情報の観点での証跡情報の取扱方法、並びに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等を整備し、措置を講ずる。

３　情報システムセキュリティ責任者は、第１項で取得した証跡に対して不正な消去、改ざん又は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含む必要な機能を設ける。

（証跡の保存）

第２６条　情報システムセキュリティ責任者は、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がある場合は、延長することができる。

（取得した証跡の点検及び分析等）

第２７条　情報システムセキュリティ責任者は、取得した証跡を定期的に又は必要に応じて点検及び分析し、適切な措置を講ずる。

（暗号化機能又は電子署名付与機能の導入）

第２８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を防ぐため、以下の措置を講ずる。

（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（以下「暗号化機能

」という。）の必要性の有無を検討し、必要があると認めたときは、暗号化機能を設けること。

（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（以下「電子署名付与機能」という。）の必要性の有無を検討し、必要があると認めたときは、電子署名付与機能を設けること。

２　情報システムセキュリティ責任者は、暗号化機能又は電子署名付与機能を選択するに当たっては、以下の事項を定める。

（１）　情報システムの新規構築又は更新に伴い、暗号化機能又は電子署名付与機能を導入する場合には、やむを得ない場合を除き、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」に記載されたアルゴリズム並びにそれを利用した安全なプロトコルを採用すること。

（２）　暗号化機能又は電子署名付与機能に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

（３）　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、鍵の生成、有効期限、廃棄、更新、保存、バックアップ及び鍵が露呈した場合の管理手順（以下「鍵の管理手順」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、情報システムで電子証明書を用いて暗号化機能又は電子署名付与機能を設けるに当たり、適用可能な場合は、政府認証基盤（ＧＰＫＩ）が発行している電子証明書を使用する。

４　情報システムセキュリティ責任者は、第１項第１号に基づく情報システム（以下「暗号化対象情報システム」という。）又は同項第２号に基づく情報システム（以下「電子署名対象情報システム」という。）において、以下の措置を講ずること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。

（１）　暗号モジュールの交換可能なコンポーネント化による構成

（２）　複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択可能にする構成

（３）　選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、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及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品の選択

（４）　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の耐タンパ性を有する暗号モジュールへの格納

５　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又は更新する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

（暗号化又は電子署名付与に係る管理）

第２９条　情報システムセキュリティ責任者は、暗号化対象情報システム又は電子署名対象情報システムにおいて、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、職員等との共有等の措置を講ずる。

２　情報システムセキュリティ責任者は、電子署名対象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提供する。

（暗号化機能又は電子署名付与機能の利用）

第３０条　職員等は、暗号化又は電子署名に使用するアルゴリズムについて、やむを得ない場合を除き、電子政府推奨暗号リストに記載されたアルゴリズムを利用する。
２　職員等は、暗号化又は電子署名に使用するアルゴリズムが危殆化した場合には、緊急対応手順に従い、適切に管理する。
３　職員等は、暗号化又は電子署名に使用する鍵について、鍵の管理手順に従い、適切に管理する。
４　職員等は、暗号化又は電子署名に使用する鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

第２節　情報セキュリティに関する脅威

（情報システムの脆弱性対策）
第３１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時及び運用開始時に、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、公開された脆弱性に関連する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、入手した脆弱性に関連する情報から、情報システムにもたらす影響を考慮した上で、以下の事項について脆弱性対策計画を作成し、対策を講ずる。
（１）　対策の必要性
（２）　対策方法
（３）　対策方法が存在しない場合の一時的な回避方法
（４）　対策方法又は回避方法が情報システムに与える影響
（５）　対策の実施予定
（６）　対策試験の必要性
（７）　対策試験の方法
（８）　対策試験の実施予定
４　情報システムセキュリティ責任者は、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。
５　情報システムセキュリティ責任者は、信頼できる方法で対策用ファイルを入手する。
６　情報システムセキュリティ責任者は、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及び分析し、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には、必要な措置を講ずる。

（情報システムの不正プログラム対策の整備）
第３２条　情報システムセキュリティ責任者は、電子計算機に不正プログラム対策ソフトウェア等を導入する。ただし、当該電子計算機で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。
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侵入経路のすべ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実施する。
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、必要な対処を講ずる。

（情報システムの不正プログラム対策の実施）

第３３条　職員等は、不正プログラム感染防止に関する措置を講ずる。

２　職員等は、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。

（サービス不能攻撃対策）

第３４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。以下「要安定情報対象情報システム」という。）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が装備している機能又は経済産業省外の者が提供する手段を用いてサービス不能攻撃対策を実施する。

２　情報システムセキュリティ責任者は、要安定情報対象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に影響が最小となるように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、要安定情報対象情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視し、監視記録を保存する。

第３節　標的型攻撃対策

（標的型攻撃対策）

第３５条　情報システムセキュリティ責任者は、情報システムにおいて、以下の対策事項を含む標的型攻撃対策を講ずる。

（１）　組織内部への侵入を低減する対策（入口対策）

（２）　組織内部に侵入した攻撃を早期検知、侵入範囲の拡大の困難化及び外部との不正通信を検知並びにそれらに対処する対策（内部対策）

第４節　情報システムのライフサイクル

（情報システムの情報セキュリティの実施体制）

第３６条　情報システムセキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティの確保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　情報システムセキュリティ責任者は、複数の省庁で共通に使用する情報システム（以下「省庁共通情報システム」という。）を利用して情報システムを構築する場合は、省庁共通情報システムを整備し、運用管理する府省庁が定める手順等に応じた体制を整備する。

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システムの体制の確保に際し、情報システムを統括する責任者の協力を得ることが必要な場合は、その者に体制の全部又は一部の整備を求めることができる。

（情報システム設計時等の情報セキュリティ対策）

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に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報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、証跡管理、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合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についての対策要件

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、情報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、省庁共通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、省庁共通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、情報セキュリティ要件を策定する。

５　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、運用及び監視に際しては、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。

６　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、移行手段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。

７　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。

８　情報システムセキュリティ責任者は、情報システムの受入れ時の確認・検査において、仕様書等に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。

９　情報システムセキュリティ責任者は、省庁共通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、省庁共通情報システムを整備し運用管理する機関等との責任分界に応じた運用管理体制の下、省庁共通情報システムの運用管理規程等に従い、省庁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。

１０　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。

１１　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外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書への記載等により適切に実施させる。

（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

１２　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・保守を外部委託する場合は、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ための要件について、調達仕様書への記載等により適切に実施させる。

１３　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・保守を外部委託する場合は、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、速やかに報告させる。

（情報システムの利用時の基本的対策）

第３８条　職員等は、行政事務の遂行以外の目的で情報システムを利用してはならない。

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外の情報システムを接続してはならない。

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てはならない。

４　職員等は、情報システムで利用を認められたソフトウェア以外を利用してはならない。ただし、情報システムセキュリティ責任者の許可を得た場合はこの限りでは無い。

５　職員等は、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機器等を情報システムに接続してはならない。

６　職員等は、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、要保護情報を取り扱う端末にて情報処理を行う場合は、定められた安全管理措置を講ずる。

８　職員等は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得る。

９　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、当該省内通信回線を管理する情報システムセキュリティ責任者の許可を得た上で、以下を含む安全管理措置を講ずることとする。

（１）　アンチウイルス対策の実施

（２）　セキュリティパッチの適用

（情報システムの更改又は廃棄時の情報セキュリティ対策）

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必要性を検討し、以下の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における情報セキュリティ対策

（２）　情報システム廃棄時におけるすべての情報の抹消

（情報システムの見直し）

第４０条　情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について見直しを行う必要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。

（情報システム台帳）

第４１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、当該情報システムに係る以下の事項を記載した台帳を整備する。ただし、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、政府情報システム管理データベースにおいて管理することをもって台帳整備に代えることができる。

（１）　情報システム名

（２）　管理課室、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

（３）　システム構成

（４）　接続する省外通信回線の種別
（５）　取り扱う情報の格付及び取扱制限に関する事項
（６）　当該情報システムの設計・開発、運用、保守に関する事項
２　情報システムセキュリティ責任者は、情報処理業務を外部委託する場合は、前項各号の事項に加え、以下の事項を記載した台帳を整備する。ただし、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、政府情報システム管理データベースにおいて管理することをもって台帳整備に代えることができる。
（１）　役務名
（２）　契約事業者
（３）　契約期間
（４）　役務概要
（５）　ドメイン名（インターネット上で提供されるサービス等を利用する場合）
（６）　取り扱う情報の格付及び取扱制限に関する事項
３　情報システムセキュリティ責任者は、前二項の台帳を新規に作成し、又は更改する際には、台帳を統括情報セキュリティ責任者に報告する。

（情報システム関連文書の整備）
第４２条　情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策を実施するために必要となる以下の文書を整備する。
（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
（３）　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
（４）　情報セキュリティインシデントを察知した際の対処手順

第４章　情報システムの構成要素の対策

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４３条　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。
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職員等がクラスについて認識できる措置を講ずる。
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。
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。
５　職員等は、情報を取り扱う場合には、情報取扱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。

第２節　端末

（端末の導入時の対策）

第４４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及び利用を禁止するソフトウェアを定める。

（端末の運用時の対策）

第４５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。

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４６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復元が困難な状態にする。

第３節　サーバ装置

（サーバ装置の導入時の対策）

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等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及び利用を禁止するソフトウェアを定める。

４　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際に送受信される情報が漏えいすることを防止するための対策を講ずる。

（サーバ装置の運用時の対策）

第４８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。

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、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りでない。

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、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずる。

（サーバ装置の運用終了時の対策）

第４９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復元が困難な状態にする。

第４節　複合機

（複合機）

第５０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た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復元が困難な状態にする。

第５節　特定用途機器

（１ｏＴ機器を含む特定用途機器）

第５１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６節　電子メール

（電子メールの導入時の対策）

第５２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。

（電子メールの利用時の対策）

第５３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しなければならない。

２　職員等は、経済産業省外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府機関のドメイン名であることが保証される「．ｇｏ．ｊｐ」で終わるドメイン名（以下「政府ドメイン名」という。）を使用しなければならない。ただし、経済産業省外の者にとって、当該職員等が既知の場合には、この限りでない。

３　職員等は、不審な電子メールを受信した場合には、定められた手順に従い、対処する。

第７節　ウェブ

（ウェブサーバの導入時の対策）

第５４条　情報システムセキュリティ責任者は、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。

（１）　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。

（２）　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。

（３）　公開するウェブコンテンツを必要最小限にする。

（４）　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。

（５）　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防止のため全ての情報に対する暗号化の機能及び電子証明書による認証の対策を講じる。

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。

（ウェブアプリケーションの開発時及び運用時の対策）

第５５条　情報システムセキュリティ責任者は、ウェブアプリケーションの開発時及び運用時おいて、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。

（ウェブの利用時の対策）

第５６条　情報システムセキュリティ責任者は、職員等が閲覧することが可能な経済産業省外のウェブサイトを制限する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、定期的にその見直しを行うものとする。

２　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ってはならない。

３　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しなければならない。

４　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、以下の事項を確認しなければならない。

（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

第８節　ドメインネームシステム

（ドメインネームシステムの導入時の対策）

第５７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ドメインネームシステム（以下「ＤＮＳ」という。）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。

（ドメインネームシステムの運用時の対策）

第５８条　情報システムセキュリティ責任者は、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。

第９節　データベース

（データベースの導入・運用時の対策）

第５９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１０節　通信回線

（通信回線の導入時の対策）

第６０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、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策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。

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。

７　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や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。
８　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。
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る。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。
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。

（通信回線の運用時の対策）
第６１条　情報システムセキュリティ責任者は、障害及び事故等による影響を防止するために、通信回線装置の運用時に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、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。
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を定期的に調査し、許可されていないソフトウェアがインストールされている等、不適切な状態にある通信回線装置を認識した場合には、改善を図る。
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。

（通信回線の運用終了時の対策）
第６２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、当該の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復元が困難な状態にする等適切な措置を講ずる。

（リモートアクセス環境導入時の対策）
第６３条　情報システムセキュリティ責任者は、職員等の業務遂行を目的としたモートアクセス環境を、省外通信回線を経由して経済産業省内の情報システムへリモートアクセスする形態により構築する場合は、ＶＰＮ回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保する。

（無線ＬＡＮ環境導入時の対策）
第６４条　情報システムセキュリティ責任者は、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うえで、情報セキュリティ確保のために必要な措置を講ずる。

第１１節　ＩＰｖ６通信

（ＩＰｖ６通信を行う情報システムに係る対策）

第６５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、ＩＰｖ６　Ｒｅａｄｙ　Ｌｏｇｏ　Ｐｒｏｇｒａｍに基づくＰｈａｓｅ－２準拠製品又はこれと同等以上の情報セキュリティを確保できる製品を調達する。

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、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。

（１）　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

（２）　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

（３）　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

（４）　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通信の遮断及び監視）

第６６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に対して情報セキュリティ確保するため、ＩＰｖ６通信を遮断する等の措置を講ずる。

第５章　調達及び開発に係る情報セキュリティ対策

第１節　機器等の購入

（機器等の購入時の情報セキュリティ要件の整備）

第６７条　統括情報セキュリティ責任者は、機器等の選定基準を整備する。

２　統括情報セキュリティ責任者は、情報セキュリティの確保を考慮した機器等の納入時の確認及び検査手続に係る規程を整備する。

（機器等の購入時の留意事項）

第６８条　情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、機器等の候補の選定における判断の一要素として活用する。

２　情報システムセキュリティ責任者は、機器等の納入後の情報セキュリティ対策に関する保守及び点検等の必要の有無を検討し、必要と認めた場合には、実施条件を明確にした契約を締結する。

３　情報システムセキュリティ責任者は、機器等の納入時において、納入された機器等が選定基準を満たすことを納品検査において確認する。

第２節　外部委託

（外部委託に係る規程の整備）

第６９条　統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備する。

（１）　委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本節において「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

（委託先の選定）

第７０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、委託判断基準に従って外部委託を実施し、その際は、委託先の選定基準及び選定手続きに従って委託先を選定する。

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、外部委託を実施する際には、次の各号に掲げる事項を含む情報セキュリティ対策を実施することを委託先の選定要件とし、仕様内容にも含めることとする。

（１）　委託先に提供する情報の委託先における目的外利用の禁止

（２）　委託先における情報セキュリティ対策の実施内容及び管理体制

（３）　委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、経済産業省の意図せざる変更が加えられないための管理体制

（４）　委託先の資本関係・役員等の報酬、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（５）　情報セキュリティインシデントへの対処方法

（６）　情報セキュリティ対策その他の契約の履行状況の確認方法

（７）　情報セキュリティ対策の履行が不十分な場合の対処方法

３　情報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、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて次の各号に掲げる事項を仕様に含める。

（１）　経済産業省が行う情報セキュリティ監査を受け入れること

（２）　委託先が請け負った業務のサービスレベルを保証すること

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、委託先が外部委託に係る業務の内容を一部再委託する場合は、第２項及び前項の情報セキュリティ対策の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を経済産業省に提供し、承認を受けるよう、仕様に含める。

（外部委託契約時における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又は課室情報セキュリティ責任者は、外部委託を実施する際に、前条第２項から第４項に掲げる事項を含む契約を締結する。

（外部委託における対策の実施）

第７２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、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認する。

２　職員等は、委託先への情報の提供等において、以下の事項を遵守する。

（１）　委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

（２）　提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は消去

させること。

（３）　委託業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合は、速やかに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に報告すること。

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、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせる。

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、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却又は消去されたことを確認する。

第３節　約款による外部サービス

（約款による外部サービスの利用）

第７３条　統括情報セキュリティ責任者は、次に掲げる事項を含む約款による外部サービスの利用に関する規程を整備する。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）　約款による外部サービスを利用してよい業務の範囲

（２）　業務に利用できる約款による外部サービス

（３）　利用手続及び運用手順

２　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、約款による外部サービスを利用する場合は、利用するサービス毎の責任者を定めること。

３　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクを認識した上で、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に約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

第４節　ソーシャルメディアサービスによる情報発信

（ソーシャルメディアサービスによる情報発信）

第７４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サービスを利用する場合、以下を含む情報セキュリティ対策に関する運用手順等を定める。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　情報セキュリティ責任者は、経済産業省において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定める。

３　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サービスを用いる場合は、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。

第５節　クラウドサービスによる情報発信

（クラウドサービスの利用における対策）

第７５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（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する。

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、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定する。

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、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする。

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、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める。

５　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特性を考慮した上で、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証精度の適用状況等から、クラウドサービス及び当該サービスの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。

第６章　情報処理の制限

第１節　要管理対策区域外における情報処理の制限

（要管理対策区域外における安全管理措置に係る規程の整備）

第７６条　統括情報セキュリティ責任者は、要保護情報について要管理対策区域外での情報処理を行う場合の安全管理措置についての規程を整備する。

２　統括情報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を要管理対策区域外に持ち出す場合の安全管理措置についての規程を整備する。

（要管理対策区域外での情報処理に係る許可の取得及び管理）

第７７条　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には、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の許可を得る。ただし、機密性２情報であって、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が許可を要しないとした場合は、この限りでない。

２　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又は課室情報セキュリティ責任者は、許可をした要保護情報の要管理対策区域外での情報処理に係る記録を取得する。

３　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又は課室情報セキュリティ責任者は、要保護情報について要管理対策区域外での情報処理を行うことを許可した期間が終了したときに、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、必要な措置を講ずる。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

４　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には、業務の遂行に

必要最小限の情報処理にとどめる。
5　職員等は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得る。ただし、専ら、機密性２以下の情報を取り扱う情報システムである場合であって、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が許可を要しないとした場合は、この限りでない。
6　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又は課室情報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の要管理対策区域外への持ち出しに係る記録を取得する。
7　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又は課室情報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を要管理対策区域外に持ち出すことを許可した期間が終了したときに、許可を受けた者から終了した旨の報告がない場合には、状況を確認し、必要な措置を講ずる。ただし、機密性２情報であって、許可を与えた者が報告を要しないとした場合は、この限りでない。
8　職員等は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持ち出しにとどめる。

（要管理対策区域外における安全管理措置に係る規程の遵守）
第７８条　職員等は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずる。
2　職員等は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずる。

第２節　経済産業省支給の情報機器による情報処理の制限

（経済産業省支給の情報機器による安全管理措置に係る規程の整備）
第７９条　要保護情報について経済産業省支給の情報機器を使用して要管理対策区域外で情報処理を行う場合に講ずるべき安全管理措置についての規程を整備する。

（経済産業省支給の情報機器による安全管理措置に係る規程の遵守）
第８０条　職員等は、要保護情報について、経済産業省支給の情報機器を使用して要管理対策区域外での情報処理について定められた安全管理措置を講ずる。

第３節　経済産業省支給以外の情報機器による情報処理の制限

（経済産業省支給以外の情報機器による安全管理措置に係る規程の整備）
第８１条　要保護情報について経済産業省支給以外の情報機器を使用して情報処理を行う場合に講ずるべき安全管理措置についての規程を整備する。

（経済産業省支給以外の情報機器による情報処理の許可の取得及び管理）

第８２条　職員等は、要保護情報について経済産業省支給以外の情報機器により情報処理を行う必要がある場合には、課室情報セキュリティ責任者の許可を得る。ただし、課室情報セキュリティ責任者の許可を要しないとした場合は、この限りでない。

２　職員等は、経済産業省支給以外の情報機器により情報処理を行う場合には、前条に基づく規程を遵守しなければならない。

（経済産業省支給以外の情報機器による安全管理措置に係る規程の遵守）

第８３条　職員等は、要保護情報について経済産業省支給以外の情報システムによる情報処理を行う場合には、当該情報機器について定められた安全管理措置を講ずる。

第４節　アプリケーション・コンテンツ提供時の対策

（アプリケーション・コンテンツに係る規程の整備）

第８４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経済産業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措置に係る規程を整備する。

（ドメイン名の使用についての対策）

第８５条　情報システムセキュリティ責任者は、経済産業省外の者に提供するウェブサイト等が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、政府ドメイン名を使用すること。ただし、第７４条各項に基づき、ソーシャルメディアサービスによる情報発信をする場合はこの限りではない。

２　職員等は、経済産業省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、政府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８６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８７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、経済産業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　情報セキュリティ対策に応じた教育、監査等

第１節　教育

（情報セキュリティ教育）

第８８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情報セキュリティ教育実施計画を策定する。

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。

（情報セキュリティ教育の整備）

第８９条　統括情報セキュリティ責任者は、情報セキュリティ教育について、職員等に教育すべき内容を検討し、教育のための資料を整備する。
２　統括情報セキュリティ責任者は、情報セキュリティ教育について、職員等が毎年度１回以上、受講できるように整備する。
３　統括情報セキュリティ責任者は、情報セキュリティ教育について、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９０条　課室情報セキュリティ責任者は、職員等に情報セキュリティ対策の教育を受講させる。
２　職員等は、情報セキュリティ教育について、適切な時期に受講する。
３　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。
４　統括情報セキュリティ責任者は、最高情報セキュリティ責任者に対して、職員等の情報セキュリティ対策教育の受講状況について報告する。
５　課室情報セキュリティ責任者は、ＣＳＩＲＴ及びＣＹＭＡＴに属する職員等に教育を適切に受講させる。

第２節　自己点検

（自己点検）
第９１条　統括情報セキュリティ責任者は、対策推進計画に基づく自己点検年度計画を定める。
２　統括情報セキュリティ責任者は、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９２条　情報セキュリティ責任者は、前条第１項に基づく自己点検年度計画に基づき、職員等に対して、自己点検の実施を指示する。
２　職員等は、自己点検票及び自己点検の実施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９３条　情報セキュリティ責任者は、自己点検結果について、担当する部局庁等の組織の課題を確認する等の観点から自己点検結果を分析、評価し、必要に応じてその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、前項の結果について、経済産業省全体の課題等についての分析、評価を行う。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、前項を受けて、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。

第３節　監査

（監査計画に関する年度計画の策定）

第９４条　情報セキュリティ監査責任者は、対策推進計画に基づく情報セキュリティ監査年度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、規程第２７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９５条　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。

２　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。

３　情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施する。

４　情報セキュリティ監査実施者は、規程及びこの基準において整備することが定められている実施手順が規程及びこの基準に準拠しているか否かを確認する。

５　情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、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か否かを確認する。

６　情報セキュリティ監査責任者は、監査報告書を作成し、最高情報セキュリティ責任者へ提出する。

（情報セキュリティ監査結果に対する措置）

第９６条　最高情報セキュリティ責任者は、前条第６項の監査報告書の内容を踏まえ、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摘事項に対する改善を指示する。

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、必要な措置を実施するとともに改善計画を策定し、これら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、担当する部局庁等の改善が必要な事項について、必要な措置を実施するとともに改善計画を策定し、これらを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９７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　障害及び事故等

（障害及び事故等の発生に備えた事前準備）

第９８条　最高情報セキュリティ責任者は、ＣＳＩＲＴを整備し、職員等からＣＳＩＲＴに属する職員を置き、そのうちＣＳＩＲＴ責任者を置く。

２　ＣＳＩＲＴ責任者は、統括情報セキュリティ責任者をもって充てる。

３　統括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手順を整備する。

４　統括情報セキュリティ責任者は、障害及び事故等が発生した場合（発生したおそれがある場合を含む。以下同じ。）の報告手順及び報告手段を整備し、具体例を含め周知する。

５　統括情報セキュリティ責任者は、障害及び事故等が発生した場合における際の経済産業省内外との情報共有を含む対処手順を整備する。

６　統括情報セキュリティ責任者は、障害及び事故等に備え、行政事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。

７　統括情報セキュリティ責任者は、必要に応じ、障害及び事故等について経済産業省外から報告を受けるための窓口を設置することができる。その場合はその窓口への連絡手段を経済産業省内外に明示する。

８　統括情報セキュリティ責任者は、障害及び事故等への対処の訓練の必要性を検討し、必要と判断した場合には、訓練の内容及び体制を整備し、周知する。

９　統括情報セキュリティ責任者は、第３項及び第５項に掲げる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。

１０　ＣＹＭＡＴに属する職員等を置くこととし、その職員等は統括情報セキュリティ責任者が指名する。

（障害及び事故等の発生時における報告と応急措置）

第９９条　職員等は、障害及び事故等の発生した場合には、前条第４項に基づく手順に従い報告を行う。

２　統括情報セキュリティ責任者は、障害及び事故等が発生した場合には、情報システムセキュリティ責任者等に対し、被害の拡大防止等を図るための応急措置の実施及び障害及び事故等からの復旧に係る指示又は勧告を行う。

３　職員等は、障害及び事故等が発生した場合には、適用可能な対応手順がある場合には、当該手順に従い対応する。

４　職員等は、障害及び事故等が発生した場合であって、当該障害及び事故等について適用可能な対応手順がないときは、対応についての指示を受けるまで、障害及び事故等による被害の拡大防止に努める。

５　統括情報セキュリティ責任者は、報告を受けた障害及び事故等について、速やかに、経済産業省内外の関係部門と情報共有を行い、評価を行う。

６　情報システムセキュリティ責任者は、省庁共通情報システムにおいて障害及び事故等が発生した場合には、当該省庁共通情報システムに係る運用管理等、適用可能な対応手順がある場合には、当該手順に従い対応する。

（障害及び事故等の原因調査と再発防止策）

第１００条　情報セキュリティ責任者は、障害及び事故等が発生した場合には、障害及び事故等に対応する責任者が実施した内容も踏まえ、障害及び事故等の原因を調査するとともに再発防止策を策定し、結果を報告書として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、情報セキュリティ責任者から障害及び事故等についての報告を受けた場合には、内容を検討し、再発防止策を実施するために必要な措置を講ずるとともに、必要に応じ、最高情報セキュリティ責任者に報告する。

第５節　業務継続計画

（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１０１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。）と関係があると認めた情報システムについて、業務継続計画との整合性を考慮し、必要な措置を講ずる。

（１）　通常時において業務継続計画並びに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。

（２）　事態発生時において業務継続計画並びに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。

第６節　情報セキュリティ対策推進体制

（情報セキュリティ対策推進体制の役割）

第１０２条　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を以下の通り定める。

（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

第８章　雑則

（規程及び細則の策定）

第１０３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。