独立行政法人国立高等専門学校機構サイバーセキュリティポリシー対策規則

独立行政法人国立高等専門学校機構規則第９８号
制定　平成２２年３月３１日
一部改正　平成２５年９月３０日
全部改正　平成３０年２月２２日
一部改正　令和２年１０月２０日
一部改正　令和４年　１月２８日

目次

第３節　テレワーク

別表

用語の定義（第８条関係）

１．一般的な用語

２．機構独自の用語

別紙

各節又は款の目的及び趣旨（第５条関係）

第１章　総則

第２章　情報セキュリティ対策の基本的枠組み

第３章　情報の取扱い

第４章　外部委託

第５章　情報システムのライフサイクル

第６章　情報システムのセキュリティ要件

第７章　情報システムの構成要素

第８章　情報システムの利用

第１章　総則

第１節　本対策規則の目的・適用対象

（目的）

第１条　この対策規則は,「政府機関等のサイバーセキュリティ対策のための統一規範」（サイバーセキュリティ戦略本部決定）に基づく機関等における統一的な枠組みの中で，統一規範の実施のための必要な要件として，情報セキュリティ対策の項目ごとに独立行政法人国立高等専門学校機構（以下「機構」という。）が遵守すべき事項（以下「遵守事項」という。）を規定することにより，機構の情報セキュリティ水準の斉一的な引き上げを図ることを目的とする。

（適用対象）

第２条　この対策規則において適用対象とする者は,機構における全ての業務従事者（以下「業務従事者」という。）とする。

２　この対策規則において適用対象とする情報は，以下の情報とする。

一　業務従事者が職務上使用することを目的として機構が調達し，又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

二　前号に定めるもの以外の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって，業務従事者が職務上取り扱うもの

三　前２号に定めるもののほか，機構が調達し，又は開発した情報システムの設計又は運用管理に関する情報

３　この対策規則において適用対象とする情報システムは，この対策規則の適用対象となる情報を取り扱う全ての情報システムとする。

（規則の改定）

第３条　機構は，情報セキュリティ水準を適切に維持していくためには，状況の変化を的確にとらえ，それに応じて情報セキュリティ対策の見直しを図ることが重要であることにかんがみ，情報技術の進歩に応じて，この対策規則を定期的に点検し，必要に応じ規定内容の追加・修正等の改定を行うものとする。

（法令の遵守）

第４条　業務従事者は，情報及び情報システムの取扱いに関しては，この対策規則のほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。また，情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守するものとする。

（記載事項）

第５条　この対策規則では，機構が行うべき対策について，目的別に章，節，款及び目の４階

層にて対策項目を分類することとし，規定の解釈に当たっては，別紙に定める節又は款の目的，趣旨に基づくものとする。

第２節　情報の格付の区分・取扱制限

（情報の格付の区分）

第６条　情報の格付けについては，独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係る情報格付規則（機構規則第９９号。以下「情報格付規則」という。）に定めるところによる。機密性，完全性及び可用性の３つの観点を区別するものとし，観点ごとの格付の区分の定義は次の各号に定めるところによるものとする。

一　機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	機構業務で取り扱う情報のうち，秘密の保護が高度に必要であって，当該秘密の漏洩が法人の利益に対し，重大な損害を与えるおそれのある情報
機密性２情報	機構業務で取り扱う情報のうち，独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって，「機密性３情報」以外の情報
機密性１情報	情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

なお，機密性２情報及び機密性３情報を「要機密情報」という。

二　完全性についての格付の定義

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

なお，完全性２情報を「要保全情報」という。

三　可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	機構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，国民又は機構関係者の権利が侵害され又は機構業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

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

２　機構において前項に定める格付の定義を変更又は追加する場合にあっては，機構の対策規則における格付区分と遵守事項との関係が政府機関等の情報セキュリティ対策のための統一基準との関係と同等以上となるように準拠しなければならない。
３　業務従事者は，他機関へ情報を提供する場合にあっては，自身の格付区分と政府機関等の情報セキュリティ対策のための統一基準における格付区分の対応について，適切に伝達するものとする。

（情報の取扱制限）
第７条　この対策規則において「取扱制限」とは，情報の取扱いに関する制限であって，複製禁止，持出禁止，配布禁止，暗号化必須，読後廃棄その他の情報の適正な取扱いを業務従事者に確実に行わせるための手段をいう。
２　業務従事者は，格付に応じた情報の取扱いを適切に行う必要があるが，その際に，格付に応じた具体的な取扱い方を示す方法として取扱制限を用いるものとする。
３　機構は，取り扱う情報について，機密性，完全性及び可用性の３つの観点から，取扱制限に関する基本的な定義を定めるものとする。

第３節　用語定義

（用語の定義）
第８条　この対策規則並びに機構において定められる規則等（以下「実施規則」という。）及び実施規程等における用語の定義は，それぞれの実施規則及び実施規程等において個別に定めるものを除き，別表又は当該各号に定めるところによる。

第４節　関連規則等

（関連規則等）
第９条　機構が扱う情報の格付及び取扱制限の指定並びに明示等の詳細については，情報格付規則に従うものとする。
２　機構が扱う情報の公開及び非公開については，独立行政法人国立高等専門学校機構情報公開取扱規則（機構規則第７０号）及び独立行政法人国立高等専門学校機構個人情報管理規則（機構規則第６５号）に従うものとする。
３　機構におけるソフトウェアの管理運用については，独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係るソフトウェア管理規則（機構規則第９４号）に従うものとする。

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

第１款　組織・体制の整備

（最高情報セキュリティ責任者の設置）

第１０条　機構は，機構における情報セキュリティに関する業務を統括する最高情報セキュリティ責任者１人を置き，最高情報責任者をもって充てる。

（情報セキュリティ委員会の設置）

第１１条　最高情報セキュリティ責任者は，対策規則等の審議を行う機能を持つ組織として，機構の情報セキュリティを推進する部局及び学校等の代表者によって構成される情報セキュリティ委員会を置くものとし，機構の企画委員会をもって充てる。

（最高情報セキュリティ監査責任者の設置）

第１２条　最高情報セキュリティ責任者は，その指示に基づき実施する監査に関する事務を統括する者として，最高情報セキュリティ監査責任者１人を置く。

（統括情報セキュリティ責任者・情報セキュリティ責任者等の設置）

第１３条　最高情報セキュリティ責任者は，情報セキュリティに責任を持つ者として，学校等にそれぞれ情報セキュリティ責任者を置き，機構本部においては事務局長をもって充て，学校においては校長をもって充てる。

２　最高情報セキュリティ責任者は，前項に定める者のうち，情報セキュリティ責任者を統括し，最高情報セキュリティ責任者を補佐する者として，統括情報セキュリティ責任者１人を置き，機構本部事務局長をもって充てる。

３　情報セキュリティ責任者は，第５５条で定める区域ごとに，当該区域における情報セキュリティ対策の業務を統括する区域情報セキュリティ責任者１人を置き，機構本部においては事務局次長をもって充て，学校においては校長をもって充てる。

４　情報セキュリティ責任者は，課室ごとに情報セキュリティ対策に関する業務を統括する情報セキュリティ管理者１人を置くものとする。

５　情報セキュリティ責任者は，所管する情報システムに対する情報セキュリティ対策に関する業務の責任者として，情報セキュリティ推進責任者を，当該情報システムの企画に着手するまでに選任するものとする。

（最高情報セキュリティアドバイザーの設置）

第１４条　最高情報セキュリティ責任者は，情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き，自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めるものとする。

（情報セキュリティ対策推進体制の整備）

第１４条の２　最高情報セキュリティ責任者は，機構の情報セキュリティ対策推進体制を整備し，その役割を規定するものとする。

２　最高情報セキュリティ責任者は，情報セキュリティ対策推進体制の責任者を定めるものと

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１５条　最高情報セキュリティ責任者は，情報セキュリティインシデントに備えるための体制として CSIRT を整備し，その役割を明確化するものとする。

２　最高情報セキュリティ責任者は，業務従事者のうちから CSIRT に属する教職員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ものとする。

３　最高情報セキュリティ責任者は，前項に基づき選任した者のうち，機構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 CSIRT 責任者を置き，併せて，CSIRT 内の業務統括及び外部との連携等を行う教職員を定めるものとする。

４　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ものとする。

（兼務を禁止する役割）

第１６条　業務従事者は，情報セキュリティ対策の運用において，以下の役割を兼務しないものとする。

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

二　監査を受ける者とその監査を実施する者

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

（最高情報セキュリティ副責任者の設置及び業務）

第１７条　機構に，最高情報セキュリティ副責任者を置き，最高情報セキュリティ責任者がこれを指名する。

２　最高情報セキュリティ副責任者は，最高情報セキュリティ責任者を補佐し，必要に応じてその業務を代行する。

（情報セキュリティ副責任者の設置及び業務）

第１８条　学校等にそれぞれ情報セキュリティ副責任者を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ副責任者は，情報セキュリティ責任者を補佐し業務を代行する。

（情報セキュリティ推進員の設置及び業務）

第１９条　学校等にそれぞれ情報セキュリティ推進員を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ推進員は，情報セキュリティ推進委員会の指示により，割り当てられた範囲の専門的及び技術的問題への対応を行うものとする。

（情報セキュリティ管理委員会の設置及び業務）

第２０条　学校等に，それぞれ情報セキュリティ管理委員会を置くものとする。

２　情報セキュリティ管理委員会は，学校等における次の各号に掲げる事項を審議する。ただし，専門的及び技術的問題の審議は情報セキュリティ推進委員会に委ねるものとする。

一　実施規程及び実施手順の制定並びに改廃

二　基本方針，実施規則，実施規程及び実施手順に関し，当該規則等の実施，周知徹底，遵守及び励行の推進，違反に対する措置，並びに遵守状況の調査

三　情報セキュリティ教育

四　リスク管理及び非常時行動計画の策定並びに実施

五　情報セキュリティインシデント防止策の策定及び実施

六　例外措置の許可権限者の選任

七　情報セキュリティの強化に関する調査及び検討

八　情報セキュリティに関する情報の調査及び周知

九　実施規程及び実施手順の実施状況の評価及び見直し

十　その他情報セキュリティに関する事項

（情報セキュリティ管理委員会の構成員）

第２１条　情報セキュリティ管理委員会は，情報セキュリティ責任者を委員長とし，次の各号に掲げる者を委員として組織する。

一　情報セキュリティ副責任者

二　情報セキュリティ管理者

三　情報セキュリティ推進責任者

２　前項の規定にかかわらず，情報セキュリティ責任者は，必要に応じて情報セキュリティ管理委員会の委員を別に定めることができる。

（情報セキュリティ推進委員会の設置及び業務）

第２２条　学校等に，それぞれ情報セキュリティ推進委員会を置くものとする。

２　情報セキュリティ推進委員会は次の各号に掲げる事項を行う。

一　情報セキュリティに関する専門的及び技術的問題の審議

二　情報システムに関わる情報セキュリティインシデントの発生時の対応

三　情報セキュリティ責任者，情報セキュリティ副責任者及び情報セキュリティ管理者への専門的及び技術的立場からの助言及び支援

（情報セキュリティ推進委員会の構成員）

第２３条　情報セキュリティ推進委員会は，情報セキュリティ推進責任者を委員長とし，次の各号に掲げる者を委員として組織する。

一　情報セキュリティ管理者

二　その他，情報セキュリティ責任者が必要と認める者

（管理運営部署の設置及び業務）

第２４条　学校等に情報セキュリティに関する管理運営部署を設置し，原則として，学校等の総務担当課をもって充てる。

２　管理運営部署は，情報セキュリティ責任者又は情報セキュリティ副責任者の指示により，次の各号に掲げる業務を行う。

一　情報セキュリティ管理委員会及び情報セキュリティ推進委員会の運営に関する業務

二　情報セキュリティ管理委員会及び情報セキュリティ推進委員会の審議に関連する事項の取りまとめ

三　情報セキュリティに関する連絡と通報

四　情報セキュリティに関する文書の保管

（情報セキュリティ監査者の設置及び業務）

第２５条　機構に，情報セキュリティ監査者を置き，最高情報セキュリティ監査責任者がこれを指名する。

２　情報セキュリティ監査者は，最高情報セキュリティ監査責任者の業務を補佐する。

第２款　対策規則・対策推進計画の策定

（対策規則の策定）

第２６条　最高情報セキュリティ責任者は，情報セキュリティ委員会における審議を経て，情報セキュリティ対策のための統一基準に準拠した対策規則を定めるものとする。また，対策規則は，機構の業務，取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めるものとする。

（対策推進計画の策定）

第２７条　最高情報セキュリティ責任者は，情報セキュリティ委員会における審議を経て，情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。

２　前項に基づき定める対策推進計画には，機構の業務，取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めるものとする。

一　情報セキュリティに関する教育

二　情報セキュリティ対策の自己点検

三　情報セキュリティ監査

四　情報システムに関する技術的な対策を推進するための取組

五　前各号に掲げるもののほか，情報セキュリティ対策に関する重要な取組

第３款　実施規定及び実施手順の策定

（実施規程及び実施手順の作成）

第２８条　基本方針及び実施規則に基づき策定される実施規程，並びに実施規程に基づき策定

される実施手順は，学校等を単位として情報セキュリティ責任者が定めるものとする。
２　情報セキュリティ責任者は，必要に応じ，この対策規則に規定した以外の事項について追加規定することができる。

第４款　業務継続計画の策定

（業務継続計画の作成）
第２９条　最高情報セキュリティ責任者及び情報セキュリティ責任者は，地震等の大規模災害時における，情報の保護，最小限の情報システムの機能保全，業務継続計画等の対策を整備するものとする。
２　最高情報セキュリティ責任者及び情報セキュリティ責任者は，大規模災害が発生した場合は，業務継続計画に従った措置を実施するものとする。

第２節　運用

第１款　機構情報セキュリティ関連規程等の運用

（情報セキュリティ対策の運用）
第３０条　統括情報セキュリティ責任者は，機構における情報セキュリティ対策に関する実施手順を整備（この対策規則で整備すべき者を別に定める場合を除く。）し，実施手順に関する業務を統括し，整備状況について最高情報セキュリティ責任者に報告するものとする。
２　統括情報セキュリティ責任者は，情報セキュリティ対策における雇用の開始，終了及び人事異動時等に関する管理の規定を整備するものとする。
３　情報セキュリティ対策推進体制は，最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行するものとする。
４　情報セキュリティ責任者又は情報セキュリティ管理者は，業務従事者から機構情報セキュリティ関連規程等に係る課題及び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ものとする。
５　統括情報セキュリティ責任者は，機構情報セキュリティ関連規程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ものとする。

（違反への対処）
第３１条　業務従事者は，機構情報セキュリティ関連規程等への重大な違反を知った場合は，情報セキュリティ責任者にその旨を報告するものとする。
２　情報セキュリティ責任者は，機構情報セキュリティ関連規程等への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には，違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに，統括情報セキュリティ責任者を通じて，最高情報セキュリティ責任者に報告するものとする。

第２款　例外措置

（例外措置手続の整備）

第３２条　最高情報セキュリティ責任者は，例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び，審査手続を定めるものとする。

２　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，許可権限者に対して，定期的に申請状況の報告を求めるものとする。

（例外措置の運用）

第３３条　業務従事者は，定められた審査手続に従い，許可権限者に規定の例外措置の適用を申請するものとする。ただし，機構業務の遂行に緊急を要し，当該規定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，機構情報セキュリティ関連規程等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されている方法を実施しないことが不可避のときは，事後速やかに届け出るものとする。

２　許可権限者は，業務従事者による例外措置の適用の申請を，定められた審査手続に従って審査し，許可の可否を決定するものとする。

３　許可権限者は，例外措置の申請状況を台帳に記録し，統括情報セキュリティ責任者に報告するものとする。

４　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機構情報セキュリティ関連規程等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ものとする。

第３款　教育

（教育体制の整備・教育実施計画の策定）

第３４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（以下,「教育実施計画」）を策定し，その実施体制を整備するものとする。

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業務従事者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ものとする。

（教育の実施）

第３５条　情報セキュリティ管理者は，教育実施計画に基づき，業務従事者に対して，機構情報セキュリティ関連規程等に係る教育を適切に受講させるものとする。

２　業務従事者は，教育実施計画に従って，適切な時期に教育を受講するものとする。

３　情報セキュリティ管理者は，情報セキュリティ対策推進体制及び CSIRT に属する教職員に教育を適切に受講させるものとする。

４　情報セキュリティ管理者は，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ものとする。

５　統括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ものとする。

第４款　情報セキュリティインシデントへの対処

（情報セキュリティインシデントに備えた事前準備）

第３６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機構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，業務従事者に周知するものとする。

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文部科学省等との情報共有を含む対処手順を整備するものとする。

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，機構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ものとする。

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，機構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ものとする。

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機構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機構外の者に明示するものとする。

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ものとする。

（情報セキュリティインシデントへの対処）

第３７条　業務従事者は，情報セキュリティインシデントの可能性を認知した場合には，機構の報告窓口に報告し，指示に従うものとする。

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ものとする。

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ものとする。

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ものとする。

５　情報セキュリティ推進責任者は，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，機構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，適切に対処するものとする。

６　情報セキュリティ推進責任者は，認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり，当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には，当該運用管理規程等に従い，適切に対処するものとする。

７　CSIRT は，機構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，文部科学省等に連絡するものとする。

8　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，当該情報セキュリティインシデントの内容に応じ，警察への通報・連絡等を行うものとする。

9　CSIRT は，認知した情報セキュリティインシデントが，国民及び機構関係者の生命，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ものとする。

１０　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，必要に応じて対処全般に関する指示，勧告又は助言を行うものとする。

１１　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ものとする。

１２　CSIRT は，情報セキュリティインシデントに関して，機構を含む関係機関と情報共有を行うものとする。

（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３８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ものとする。

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ものとする。

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及び関係する情報セキュリティ責任者等に共有するものとする。

第３節　点検

第１款　情報セキュリティ対策の自己点検

（自己点検計画の策定・手順の準備）

第３９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ものとする。

2　情報セキュリティ責任者は，年度自己点検計画に基づき，業務従事者ごとの自己点検票及び自己点検の実施手順を整備するものとする。

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，業務従事者に対して新たに点検すべき事項が明らかになった場合には，年度自己点検計画を見直すものとする。

（自己点検の実施）

第４０条　情報セキュリティ責任者は，年度自己点検計画に基づき，業務従事者に自己点検の実施を指示するものとする。
２　業務従事者は，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ものとする。

（自己点検結果の評価・改善）
第４１条　情報セキュリティ責任者は，自己点検結果について，自らの所掌範囲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し，評価するものとする。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ものとする。
２　統括情報セキュリティ責任者は，機構に共通の課題を確認するなどの観点から自己点検結果を分析，評価すること。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ものとする。
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ものとする。

第２款　情報セキュリティ監査

（監査実施計画の策定）
第４２条　最高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定めるものとする。
２　最高情報セキュリティ監査責任者は，情報セキュリティの状況の変化に応じ，対策推進計画で計画された以外の監査の実施が必要な場合には，追加の監査実施計画を定めるものとする。

（監査の実施）
第４３条　最高情報セキュリティ監査責任者は，監査実施計画に基づき，以下の事項を含む監査の実施を情報セキュリティ監査者に指示し，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ものとする。
一　各校の規則及び規程が，対策規則を満たすための適切な事項を定められていること。
二　実施手順が機構規則に準拠していること。
三　被監査部門における実際の運用が機構情報セキュリティ関連規程等に準拠していること。

（監査結果に応じた対処）
第４４条　最高情報セキュリティ責任者は，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ものとする。
２　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からの改善の指示のうち，機構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ものとする。

３　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ものとする。

第４節　情報セキュリティ対策の見直し

（機構情報セキュリティ関連規程等の見直し）

第４５条　最高情報セキュリティ責任者は，情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに，情報セキュリティに係る重大な変化等を踏まえ，情報セキュリティ委員会の審議を経て，対策規則について必要な見直しを行うものとする。

２　統括情報セキュリティ責任者は，情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し，又は整備した者に対して規定の見直しを指示し，見直し結果について最高情報セキュリティ責任者に報告するものとする。

（対策推進計画の見直し）

第４６条　最高情報セキュリティ責任者は，情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに，情報セキュリティに係る重大な変化等を踏まえ，情報セキュリティ委員会の審議を経て，対策基準及び対策推進計画について定期的な見直しを行うものとする。

第３章　情報の取扱い

第１節　情報の取扱い

（情報の取扱いに係る規定の整備）

第４７条　統括情報セキュリティ責任者は，以下を含む情報の取扱いに関する規定を整備し，業務従事者へ周知するものとする。

一　情報の格付及び取扱制限についての定義

二　情報の格付及び取扱制限の明示等についての手続

三　情報の格付及び取扱制限の継承，見直しに関する手続

（情報の目的外での利用等の禁止）

第４８条　業務従事者は，自らが担当している機構業務の遂行のために必要な範囲に限って，情報を利用等するものとする。

（情報の格付及び取扱制限の決定・明示等）

第４９条　業務従事者は，情報の作成時及び機構外の者が作成した情報を入手したことに伴う

管理の開始時に，格付及び取扱制限の定義に基づき格付及び取扱制限を決定し，明示等するものとする。

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

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

（情報の利用・保存）

第５０条　業務従事者は，利用する情報に明示等された格付及び取扱制限に従い，当該情報を適切に取り扱うものとする。

2　業務従事者は，機密性３情報について学校等の管理区域外で情報処理を行う場合は，情報セキュリティ責任者の許可を得るものとする。

3　業務従事者は，要保護情報について学校等の管理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ものとする。

4　業務従事者は，保存する情報にアクセス制限を設定するなど，情報の格付及び取扱制限に従って情報を適切に管理するものとする。なお，機密性３情報を機器等に保存する際，以下の措置を講ずるものとする。

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，サーバー装置等の機器等を使用すること。

二　該当情報に対し，暗号化による保護を行うこと。

三　該当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対策を講ずること。

5　業務従事者は，USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際，定められた利用手順に従うものとする。

（情報の提供・公表）

第５１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（情報格付規則第５条に定めるものをいう。以下同じ。)に格付されるものであることを確認するものとする。

2　業務従事者は，閲覧制限の範囲外の者に情報を提供する必要が生じた場合は，当該格付及び取扱制限の決定者等に相談し，その決定に従うものとする。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ものとする。

3　業務従事者は，機密性３情報を閲覧制限の範囲外の者に提供する場合には，情報セキュリティ管理者の許可を得るものとする。

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

（情報の運搬・送信）

第５２条　業務従事者は，要保護情報が記録又は記載された記録媒体を学校等の管理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ものとする。業務従事者が，機密性３情報を管理区域外に持ち出す場合には，暗号化措置を施した上で，情報セキュリティ管理者が指定する方法により運搬するものとする。ただし，機構外の学校等の管理区域であって，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，当該区域を学校等の管理区域とみなすことができる。

２　業務従事者は，要保護情報である電磁的記録を電子メール等で送信する場合には，安全確保に留意して送信の手段を決定し，情報の格付及び取扱制限に応じて，安全確保のための適切な措置を講ずるものとする。業務従事者が，機密性３情報を機構外通信回線（インターネットを除く。）を使用して送信する場合には，暗号化措置を施した上で，情報セキュリティ管理者が指定する方法により送信するものとする。

（情報の消去）

第５３条　業務従事者は，電磁的記録媒体に保存された情報が職務上不要となった場合は，速やかに情報を消去するものとする。

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

３　業務従事者は，要機密情報（第５条に定めるものをいう。以下同じ。)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ものとする。

（情報のバックアップ）

第５４条　業務従事者は，情報の格付に応じて，適切な方法で情報のバックアップを実施するものとする。

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

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

第２節　情報を取り扱う区域の管理

（学校等の管理区域における対策の基準の決定）

第５５条　情報セキュリティ責任者は，学校等の管理区域の範囲を定めるものとする。

２　情報セキュリティ責任者は，学校等の管理区域の特性に応じて，以下の観点を含む対策の基準を定めるものとする。

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

二　許可されていない者の立入りを制限するため及び立入りを許可された者による立入り

時の不正な行為を防止するための入退管理対策

（区域ごとの対策の決定）

第５６条　情報セキュリティ責任者は，前条２項で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ものとする。

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，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機構業務の内容，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ものとする。

（学校等の管理区域における対策の実施）

第５７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ものとする。この場合において，業務従事者が実施すべき対策については，業務従事者が認識できる措置を講ずるものとする。

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ものとする。

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

第４章　外部委託

第１節　業務委託

第１款　業務委託

（業務委託に係る規定の整備）

第５８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含む規定を整備するものとする。

一　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（以下本款において「委託判断基準」という。）

二　委託先の選定基準

（業務委託に係る契約）

第５９条　情報セキュリティ推進責任者又は情報セキュリティ管理者は，委託判断基準に従って業務委託を実施すること。

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，業務委託を実施する際には，選定基準及び選定手続に従って委託先を選定するものとする。また，以下の内容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条件とし，仕様内容にも含めるものとする。

一　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
二　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
三　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，機構の意図せざる変更が加えられないための管理体制
四　委託先の資本関係・役員等の情報，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
五　情報セキュリティインシデントへの対処方法
六　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
七　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　情報セキュリティ推進責任者又は情報セキュリティ管理者は，委託する業務において取り扱う情報の格付等を勘案し，必要に応じて以下の内容を仕様に含めるものとする。
一　情報セキュリティ監査の受入れ
二　サービスレベルの保証

４　情報セキュリティ推進責任者又は情報セキュリティ管理者は，委託先がその役務内容を一部再委託する場合は，再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう，前２項及び３項の措置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機構に提供し，機構の承認を受けるよう，仕様内容に含めるものとする。また，委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断するものとする。

（業務委託における対策の実施）

第６０条　情報セキュリティ推進責任者又は情報セキュリティ管理者は，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ものとする。

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，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業務従事者より受けた場合は，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ものとする。

３　情報セキュリティ推進責任者又は情報セキュリティ管理者は，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，又は抹消されたことを確認するものとする。

（業務委託における情報の取扱い）

第６１条　業務従事者は，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ものとする。
一　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。
二　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抹消させること。
三　委託業務において，情報セキュリティインシデント，情報の目的外利用等を認知した場合は，速やかに情報セキュリティ推進責任者又は情報セキュリティ管理者に報告すること。

第２款　外部サービスの利用

第１目　要機密情報を取り扱う場合

（外部サービスの利用に係る規定の整備）

第６２条　統括情報セキュリティ責任者は，次の各号に掲げる内容を含む外部サービス（要機密情報を取り扱う場合に限る。以下この目において同じ。）の利用に関する規定を整備するものとする。

一　外部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，本節において「外部サービス利用判断基準」という。）

二　外部サービス提供者の選定基準

三　外部サービスの利用申請の許可権限者と利用手続

四　外部サービス管理者の指名と外部サービスの利用状況の管理

（クラウドサービスに係る外部サービスの選定）

第６３条　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービスに係る外部サービスの利用を検討するに当たっては，取り扱う情報の格付及び取扱制限を踏まえ，外部サービス利用判断基準に従って行うものとする。

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービスに係る外部サービス提供者の選定に当たっては，外部サービスで取り扱う情報の格付及び取扱制限を踏まえ，外部サービス提供者の選定基準に従って選定するものとする。また，業務に特有のリスクが存在する場合には，必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めるものとする。

３　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービスに係る外部サービスの選定に当たっては，取り扱う情報の格付及び取扱制限並びに外部サービス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セキュリティ要件を定めるものとする。

（クラウドサービス以外の外部サービスの選定）

第６３条の２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービスの利用を検討するに当たっては，取り扱う情報の格付及び取扱制限を踏まえ，外部サービス利用判断基準に従って行うものとする。

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部サービスで取り扱う情報の格付及び取扱制限を踏まえ，外部サービス提供者の選定基準に従って選定するものとする。また，次の各号に掲げる内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めるものとする。

一　外部サービスの利用を通じて機構が取り扱う情報の外部サービス提供者における目的外利用の禁止

二　外部サービス提供者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

三　外部サービスの提供に当たり，外部サービス提供者若しくはその従業員，再委託先又は

その他の者によって，機構の意図せざる変更が加えられないための管理体制

四　外部サービス提供者の資本関係・役員等の情報，外部サービスの提供が行われる施設等の場所，外部サービス提供に従事する者の所属・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

五　情報セキュリティインシデントへの対処方法

六　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

七　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　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部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，外部サービス提供者の選定条件に含めるものとする。

4　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部サービスの利用を通じて機構が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内容を外部サービス提供者の選定条件に含めるものとする。

一　情報セキュリティ監査の受入れ

二　サービスレベルの保証

5　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部サービスの利用を通じて機構が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し，必要に応じて機構の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めるものとする。

6　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部サービス提供者がその役務内容を一部再委託する場合は，再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう，外部サービス提供者の選定条件で求める内容を外部サービス提供者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機構に提供し，機構の承認を受けるよう，外部サービス提供者の選定条件に含めるものとする。また，外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断するものとする。

7　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，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定め，外部サービスを選定するものとする。また，外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めるものとする。

8　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外部サービス提供者の選定を検討するに当たっては，外部サービスの特性を考慮した上で，外部サービスが提供する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，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，セキュリティ要件を定めるものとする。

9　情報セキュリティ推進責任者又は情報セキュリティ管理者は，クラウドサービス以外の外

部サービス提供者の選定を検討するに当たっては，情報セキュリティ監査による報告書の内容，各種の認定・認証制度の適用状況等から，外部サービス提供者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ものとする。

（外部サービスの利用に係る調達・契約）

第６３条の３　情報セキュリティ推進責任者又は情報セキュリティ管理者は，外部サービスを調達する場合は，外部サービス提供者の選定基準及び選定条件並びに外部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ものとする。

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，外部サービスを調達する場合は，外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し，調達仕様の内容を契約に含めるものとする。

（外部サービスの利用申請）

第６３条の４　情報セキュリティ推進責任者又は情報セキュリティ管理者は，外部サービスを利用する場合には，利用申請の許可権限者へ外部サービスの利用申請を行うものとする。

２　利用申請の許可権限者は，業務従事者による外部サービスの利用申請を審査し，利用の可否を決定するものとする。

３　利用申請の許可権限者は，外部サービスの利用申請を承認した場合は，承認済み外部サービスとして記録し，外部サービス管理者を指名するものとする。

（外部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６３条の５　統括情報セキュリティ責任者は，外部サービスの特性や責任分界点に係る考え方等を踏まえ，次の各号に掲げる内容を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定するものとする。

一　不正なアクセスを防止するためのアクセス制御

二　取り扱う情報の機密性保護のための暗号化

三　開発時におけるセキュリティ対策

四　設計・設定時の誤りの防止

２　外部サービス管理者は，前項において定める規定に対し，構築時に実施状況を確認・記録するものとする。

（外部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６３条の６　統括情報セキュリティ責任者は，外部サービスの特性や責任分界点に係る考え方を踏まえ，次の各号に掲げる内容を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定するものとする。

一　外部サービス利用方針の規定

二　外部サービス利用に必要な教育

三　取り扱う資産の管理

四　不正アクセスを防止するためのアクセス制御

五　取り扱う情報の機密性保護のための暗号化

六　外部サービス内の通信の制御
七　設計・設定時の誤りの防止
八　外部サービスを利用した情報システムの事業継続

２　情報セキュリティ推進責任者又は情報セキュリティ管理者は，外部サービスの特性や責任分界点に係る考え方を踏まえ，外部サービスで発生したインシデントを認知した際の対処手順を整備するものとする。

３　外部サービス管理者は，前各項において定める規定に対し，運用・保守時に実施状況を定期的に確認・記録するものとする。

（外部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６３条の７　統括情報セキュリティ責任者は，外部サービスの特性や責任分界点に係る考え方を踏まえ，次の各号に掲げる内容を含む外部サービスの利用を終了する際のセキュリティ対策を規定するものとする。

一　外部サービスの利用終了時における対策
二　外部サービスで取り扱った情報の廃棄
三　外部サービスの利用のために作成したアカウントの廃棄

２　外部サービス管理者は，前項において定める規定に対し，外部サービスの利用終了時に実施状況を確認・記録するものとする。

第２目　要機密情報を取り扱わない場合

（外部サービスの利用に係る規定の整備）

第６４条　統括情報セキュリティ責任者は，次の各号に掲げる内容を含む外部サービス（要機密情報を取り扱わない場合に限る。以下この目において同じ。）の利用に関する規定を整備するものとする。

一　外部サービスを利用可能な業務の範囲
二　外部サービスの利用申請の許可権限者と利用手続
三　外部サービス管理者の指名と外部サービスの利用状況の管理
四　外部サービスの利用の運用手順

（外部サービスの利用における対策の実施）

第６５条　業務従事者は，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が許容できることを確認した上で要機密情報を取り扱わない場合の外部サービスの利用を申請するものとする。また，承認時に指名された外部サービス管理者は，当該外部サービスの利用において適切な措置を講ずるものとする。

２　利用申請の許可権限者は，業務従事者による外部サービスの利用申請を審査し，利用の可否を決定するものとする。また，承認した外部サービスを記録するものとする。

第５章　情報システムのライフサイクル

第１節　情報システムに係る文書等の整備

第１款　情報システムに係る台帳等の整備

（情報システム台帳の整備）

第６６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ものとする。

２　情報セキュリティ推進責任者は，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ものとする。

（情報システム関連文書の整備）

第６７条　情報セキュリティ推進責任者は，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，以下を網羅した情報システム関連文書を整備するものとする。

一　情報システムを構成するサーバー装置及び端末関連情報

二　情報システムを構成する通信回線及び通信回線装置関連情報

三　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

四　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

第２款　機器等の調達に係る規定の整備

（機器等の調達に係る規定の整備）

第６８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ものとする。この場合において，必要に応じて，選定基準の一つとして，機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ，その管理を機構が確認できることを加えるものとする。

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ものとする。

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

第１款　情報システムの企画・要件定義

（実施体制の確保）

第６９条　情報セキュリティ推進責任者は，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ものと

する。

２　情報セキュリティ推進責任者は，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を整備し運用管理する機構が定める運用管理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ものとする。

（情報システムのセキュリティ要件の策定）

第７０条　情報セキュリティ推進責任者は，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システムのセキュリティ要件を策定するものとする。

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

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

三　情報システムに関連する脆弱性についての対策要件

２　情報セキュリティ推進責任者は，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ものとする。

３　情報セキュリティ推進責任者は，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ものとする。

４　情報セキュリティ推進責任者は，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情報セキュリティ対策に関する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ものとする。

（情報システムの構築を業務委託する場合の対策）

第７１条　情報セキュリティ推進責任者は，情報システムの構築を業務委託する場合は，以下の事項を含む委託先に実施させる事項を，調達仕様書に記載するなどして，適切に実施させるものとする。

一　情報システムのセキュリティ要件の適切な実装

二　情報セキュリティの観点に基づく試験の実施

三　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７２条　情報セキュリティ推進責任者は，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，調達

仕様書に記載するなどして，適切に実施させるものとする。

２　情報セキュリティ推進責任者は，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，速やかに報告させるものとする。

第２款　情報システムの調達・構築

（機器等の選定時の対策）

第７３条　情報セキュリティ推進責任者は，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，その結果を機器等の選定における判断の一要素として活用するものとする。

（情報システムの構築時の対策）

第７４条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，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ものとする。

（納品検査時の対策）

第７５条　情報セキュリティ推進責任者は，機器等の納入時又は情報システムの受入れ時の確認・検査において，仕様書等定められた検査手続に従い，情報セキュリティ対策に係る要件が満たされていることを確認するものとする。

２　情報セキュリティ推進責任者は，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き継がれる項目に，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ものとする。

第３款　情報システムの運用・保守

（情報システムの運用・保守時の対策）

第７６条　情報セキュリティ推進責任者は，情報システムの運用・保守において，情報システムに実装されたセキュリティ機能を適切に運用するものとする。

２　情報セキュリティ推進責任者は，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構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ものとする。

３　情報セキュリティ推進責任者は，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ものとする。

第４款　情報システムの更改・廃棄

（情報システムの更改・廃棄時の対策）

第７７条　情報セキュリティ推進責任者は，情報システムの更改又は廃棄を行う場合は，当該情報システムに保存されている情報について，当該情報の格付及び取扱制限を考慮した上で，以下の措置を適切に講ずるものとする。

一　情報システム更改時の情報の移行作業における情報セキュリティ対策

二　情報システム廃棄時の不要な情報の抹消

第５款　情報システムについての対策の見直し

（情報システムについての対策の見直し）

第７８条　情報セキュリティ推進責任者は，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ものとする。

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７９条　統括情報セキュリティ責任者は，機構において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は，非常時における情報セキュリティに係る対策事項を検討するものとする。

２　統括情報セキュリティ責任者は，情報システムの運用継続計画の教育訓練や維持改善を行う際等に，非常時における情報セキュリティに係る対策事項が運用可能であるかを確認するものとする。

第６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

第１款　主体認証機能

（主体認証機能の導入）

第８０条　情報セキュリティ推進責任者は，情報システムや情報へのアクセス主体を特定し，それが正当な主体であることを検証する必要がある場合，主体の識別及び主体認証を行う機能を設けるものとする。

２　情報セキュリティ推進責任者は，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ものとする。
３　情報セキュリティ推進責任者は，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ものとする。

（識別コード及び主体認証情報の管理）
第８１条　情報セキュリティ推進責任者は，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ものとする。
２　情報セキュリティ推進責任者は，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ものとする。

第２款　アクセス制御機能

（アクセス制御機能の導入）
第８２条　情報セキュリティ推進責任者は，情報システムの特性，情報システムが取り扱う情報の格付及び取扱制限等に従い，権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けるものとする。
２　情報セキュリティ推進責任者は，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ものとする。

第３款　権限の管理

（権限の管理）
第８３条　情報セキュリティ推進責任者は，主体から対象に対するアクセスの権限を適切に設定するよう，措置を講ずるものとする。
２　情報セキュリティ推進責任者は，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ものとする。

第４款　ログの取得・管理

（ログの取得・管理）
第８４条　情報セキュリティ推進責任者は，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ものとする。
２　情報セキュリティ推進責任者は，情報システムにおいて，その特性に応じてログを取得する目的を設定した上で，ログを取得する対象の機器等，ログとして取得する情報項目，ログの保存期間，要保護情報の観点でのログ情報の取扱方法，及びログが取得できなくなった場合の対処方法等について定め，適切にログを管理するものとする。

３　情報セキュリティ推進責任者は，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ものとする。

第５款　暗号・電子署名

（暗号化機能・電子署名機能の導入）

第８５条　情報セキュリティ推進責任者は，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，以下の措置を講ずるものとする。

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

二　要保全情報（情報格付規則第５条に定めるものをいう。以下同じ。)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　情報セキュリティ推進責任者は，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」を参照した上で，情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について，以下の事項を含めて定めるものとする。

一　業務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて，「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には，それを使用させること。

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を導入する場合には，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及びそれを利用した安全なプロトコルを採用すること。

三　暗号化及び電子署名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。

四　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，管理手順を定めること。

３　情報セキュリティ推進責任者は，機構における暗号化及び電子署名のアルゴリズム及び運用方法に，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ものとする。

（暗号化・電子署名に係る管理）

第８６条　情報セキュリティ推進責任者は，暗号及び電子署名を適切な状況で利用するため，以下の措置を講ずるものとする。

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

二　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて，暗号化又は電子署名のために選択されたアルゴリズム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。

第２節　情報セキュリティの脅威への対策

第１款　ソフトウェアに関する脆弱性対策

（ソフトウェアに関する脆弱性対策の実施）

第８７条　情報セキュリティ推進責任者は，サーバー装置，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ものとする。

２　情報セキュリティ推進責任者は，公開された脆弱性の情報がない段階において，サーバー装置，端末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ものとする。

３　情報セキュリティ推進責任者は，サーバー装置，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に確認するものとする。

４　情報セキュリティ推進責任者は，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ー装置，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，措置を講ずるものとする。

第２款　不正プログラム対策

（不正プログラム対策の実施）

第８８条　情報セキュリティ推進責任者は，サーバー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ものとする。ただし，当該サーバー装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

２　情報セキュリティ推進責任者は，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ものとする。

３　情報セキュリティ推進責任者は，不正プログラム対策の状況を適宜把握し，必要な対処を行うものとする。

第３款　サービス不能攻撃対策

（サービス不能攻撃対策の実施）

第８９条　情報セキュリティ推進責任者は，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ー装置，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ものとする。

２　情報セキュリティ推進責任者は，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ものと

する。
３　情報セキュリティ推進責任者は，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ー装置，端末，通信回線装置又は通信回線から監視対象を特定し，監視するものとする。

第４款　標的型攻撃対策

（標的型攻撃対策の実施）
第９０条　情報セキュリティ推進責任者は，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）を講ずるものとする。
２　情報セキュリティ推進責任者は，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）を講ずるものとする。

第３節　アプリケーション・コンテンツの作成・提供

第１款　アプリケーション・コンテンツの作成時の対策

（アプリケーション・コンテンツの作成に係る規定の整備）
第９１条　統括情報セキュリティ責任者は，アプリケーション・コンテンツの提供時に機構外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備するものとする。

（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９２条　情報セキュリティ推進責任者は，機構外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう，アプリケーション・コンテンツについて以下の内容を仕様に含めるものとする。
一　提供するアプリケーション・コンテンツが不正プログラムを含まないこと。
二　提供するアプリケーションが脆弱性を含まないこと。
三　実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き，実行プログラムの形式でコンテンツを提供しないこと。
四　電子証明書を用いた署名等，提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には，それをアプリケーション・コンテンツの提供先に与えること。
五　提供するアプリケーション・コンテンツの利用時に，脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を，OS やソフトウェア等の利用者に要求することがないよう，アプリケーション・コンテンツの提供方式を定めて開発すること。
六　サービス利用に当たって必須ではない，サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

２　業務従事者は，アプリケーション・コンテンツの開発・作成を業務委託する場合において，前号に掲げる内容を調達仕様に含めるものとする。

第２款　アプリケーション・コンテンツ提供時の対策

（政府ドメイン名の使用）

第９３条　情報セキュリティ推進責任者は，機構外向けに提供するウェブサイト等が実際の機構提供のものであることを利用者が確認できるように，政府ドメイン名及び機構ドメイン名を情報システムにおいて使用するものとする。ただし，次に掲げる場合を除く。

一　機構が，高等教育機関向けのドメイン名を使用する場合。この場合において，機構は，あらかじめ，情報セキュリティの確保の観点から，政府ドメイン名と高等教育機関向けのドメイン名のどちらかを使用すべきかを比較考慮の上，判断するものとする。

二　第１２４条に掲げ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。

２　業務従事者は，機構外向けに提供するウェブサイト等の作成を業務委託する場合においては，前項各号列記以外の部分，同項一及び二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ものとする。

（不正なウェブサイトへの誘導防止）

第９４条　情報セキュリティ推進責任者は，利用者が検索サイト等を経由して機構のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずるものとする。

（アプリケーション・コンテンツの告知）

第９５条　業務従事者は，アプリケーション・コンテンツを告知する場合は，告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう，必要な措置を講ずるものとする。

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

第７章　情報システムの構成要素

第１節　端末・サーバー装置等

第１款　端末

（端末の導入時の対策）

第９６条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，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ものとする。

（端末の運用時の対策）

第９７条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，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，改善を図るものとする。

（端末の運用終了時の対策及び機構が支給する端末（要管理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９８条　情報セキュリティ推進責任者は，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ものとする。

２　統括情報セキュリティ責任者は，業務従事者が，機構が支給する端末（要管理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等のリスクを踏まえた利用手順及び許可手続を定めるものとする。

３　統括情報セキュリティ責任者は，要機密情報を取り扱う機構が支給する端末（要管理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規定を整備するものとする。

４　統括情報セキュリティ責任者は，要管理区域外において機構外通信回線に接続した機構が支給する端末を機構内通信回線に接続することについての可否を判断した上で，可と判断する場合は，当該端末から機構内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めるものとする。

５　情報セキュリティ推進責任者は，業務従事者が，機構が支給する端末（要管理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，当該端末について本条(b)の技術的な措置を講ずるものとする。

（機構支給以外の端末の導入及び利用時の対策）

第９８条の２　最高情報セキュリティ責任者は，機構支給以外の端末の利用について，取り扱うこととなる情報の格付及び取扱制限，機構が講じる安全管理措置，当該端末の管理は機構ではなくその所有者が行うこと等を踏まえ，求められる情報セキュリティの水準の達成の見込みを勘案し，機構における機構支給以外の端末の利用の可否を判断するものとする。

２　統括情報セキュリティ責任者は，業務従事者が機構支給以外の端末を用いて機構の業務に係る情報処理を行う場合の許可等の手続を定めるものとする。

３　統括情報セキュリティ責任者は，業務従事者が機構支給以外の端末を用いて要保護情報を取り扱う場合について，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定めるものとする。

４　統括情報セキュリティ責任者は，要機密情報を取り扱う機構支給以外の端末について，以下の安全管理措置に関する規定を整備するものとする。

一　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

二　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利用時の措置

５　統括情報セキュリティ責任者は，要管理区域外において機構外通信回線に接続した機構支給以外の端末を機構内通信回線に接続することについての可否を判断した上で，可と判断する場合は，当該端末から機構内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めるものとする。

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

７　端末管理責任者は，業務従事者が機構支給以外の端末を用いて要機密情報を取り扱う場合は，当該端末について本条第４項第一号の安全管理措置を講ずるものとする。

８　端末管理責任者は，要機密情報を取り扱う機構支給以外の端末について，前項の規定にかかわらず本条第４項第一号に定める安全管理措置のうち自ら講ずることができないもの，及び本条第４項第二号に定める安全管理措置を業務従事者に講じさせるものとする。

９　業務従事者は，要機密情報を取り扱う機構支給以外の端末について，前項において本条第４項第一号に定める安全管理措置のうち端末管理責任者が講ずることができないもの，及び本条第４項第二号に定める安全管理措置を講ずるものとする。

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

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

第２款　サーバー装置

（サーバー装置の導入時の対策）

第９９条　情報セキュリティ推進責任者は，要保護情報を取り扱うサーバー装置について，サーバー装置の盗難，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ものとする。

２　情報セキュリティ推進責任者は，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ー装置を冗長構成にするなどにより可用性を確保するものとする。

３　情報セキュリティ推進責任者は，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，サーバー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ものとする。

４　情報セキュリティ推進責任者は，通信回線を経由してサーバー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ものとする。

（サーバー装置の運用時の対策）

第１００条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，所管する範囲のサーバー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ー装置を検出等した場合には改善を図るものとする。

３　情報セキュリティ推進責任者は，サーバー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，当該サーバー装置を監視するための措置を講ずるものとする。ただし，サーバー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はない。

４　情報セキュリティ推進責任者は，要安定情報を取り扱うサーバー装置について，サーバー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となるよう，必要な措置を講ずるものとする。

（サーバー装置の運用終了時の対策）

第１０１条　情報セキュリティ推進責任者は，サーバー装置の運用を終了する際に，サーバー装置の電磁的記録媒体の全ての情報を抹消するものとする。

第３款　複合機・特定用途機器

（複合機）

第１０２条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，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ものとする。

３　情報セキュリティ推進責任者は，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ものとする。

（IoT 機器を含む特定用途機器）

第１０３条　情報セキュリティ推進責任者は，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ものとする。

第２節　電子メール・ウェブ等

第１款　電子メール

（電子メールの導入時の対策）

第１０４条　情報セキュリティ推進責任者は，電子メールサーバーが電子メールの不正な中継

を行わないように設定するものとする。
２　情報セキュリティ推進責任者は，電子メールクライアントから電子メールサーバー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ものとする。
３　情報セキュリティ推進責任者は，電子メールのなりすましの防止策を講ずるものとする。
４　情報セキュリティ推進責任者は，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防止のため，電子メールのサーバー間通信の暗号化の対策を講ずるものとする。

第２款　ウェブ

（ウェブサーバーの導入・運用時の対策）

第１０５条　情報セキュリティ推進責任者は，ウェブサーバー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ものとする。
一　ウェブサーバー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　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　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，すべ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ずるものとする。
２　情報セキュリティ推進責任者は，ウェブサーバー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ーに保存されないことを確認するものとする。

（ウェブアプリケーションの開発時・運用時の対策）

第１０６条　情報セキュリティ推進責任者は，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ものとする。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ものとする。

第３款　ドメインネームシステム（DNS）

（DNS の導入時の対策）

第１０７条　情報セキュリティ推進責任者は，要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバーにおいて，名前解決を停止させないための措置を講ずるものとする。
２　情報セキュリティ推進責任者は，キャッシュサーバーにおいて，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ものとする。
３　情報セキュリティ推進責任者は，コンテンツサーバーにおいて，機構のみで使用する名前の解決を提供する場合，当該コンテンツサーバー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ものとする。

（DNS の運用時の対策）

第１０８条　情報セキュリティ推進責任者は，コンテンツサーバー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ー間で整合性を維持するものとする。

２　情報セキュリティ推進責任者は，コンテンツサーバー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ものとする。

３　情報セキュリティ推進責任者は，キャッシュサーバーにおいて，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ものとする。

第４款　データベース

（データベースの導入・運用時の対策）

第１０９条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，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，措置を講ずるものとする。

３　情報セキュリティ推進責任者は，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，対策を講ずるものとする。

４　情報セキュリティ推進責任者は，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ものとする。

５　情報セキュリティ推進責任者は，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ものとする。

第３節　通信回線

第１款　通信回線

（通信回線の導入時の対策）

第１１０条　情報セキュリティ推進責任者は，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ものとする。

２　情報セキュリティ推進責任者は，通信回線において，サーバー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ものとする。

３　情報セキュリティ推進責任者は，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ものとする。

４　情報セキュリティ推進責任者は，業務従事者が通信回線へ情報システムを接続する際に，当該情報システムが接続を許可されたものであることを確認するための措置を講ずるものとする。機構内通信回線へ機構支給以外の端末を接続する際も同様とする。

５　情報セキュリティ推進責任者は，通信回線装置を学校等の管理区域に設置すること。ただし，学校等の管理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などして，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ものとする。
６　情報セキュリティ推進責任者は，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ものとする。
７　情報セキュリティ推進責任者は，機構内通信回線にインターネット回線，公衆通信回線等の機構外通信回線を接続する場合には，機構内通信回線及び当該機構内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずるものとする。
８　情報セキュリティ推進責任者は，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ものとする。
９　情報セキュリティ推進責任者は，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ものとする。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　情報セキュリティ推進責任者は，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ものとする。
１１　情報セキュリティ推進責任者は，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ものとする。

（通信回線の運用時の対策）
第１１１条　情報セキュリティ推進責任者は，情報セキュリティインシデント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ものとする。
２　情報セキュリティ推進責任者は，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ものとする。
３　情報セキュリティ推進責任者は，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など，不適切な状態にある通信回線装置を認識した場合には，改善を図るものとする。
４　情報セキュリティ推進責任者は，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ものとする。

（通信回線の運用終了時の対策）
第１１２条　情報セキュリティ推進責任者は，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ものとする。

（リモートアクセス環境導入時の対策）

第１１３条　情報セキュリティ推進責任者は，業務従事者の業務遂行を目的としたリモートアクセス環境を，機構外通信回線を経由して機構の情報システムへリモートアクセスする形態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ものとする。

（無線 LAN 環境導入時の対策）

第１１４条　情報セキュリティ推進責任者は，無線 LAN 技術を利用して機構内通信回線を構築する場合は，通信回線の構築時共通の対策に加えて，通信内容の秘匿性を確保するために通信路の暗号化を行った上で，その他の情報セキュリティ確保のために必要な措置を講ずるものとする。

第２款　IPv6 通信回線

（IPv6 通信を行う情報システムに係る対策）

第１１５条　情報セキュリティ推進責任者は，IPv6 技術を利用する通信を行う情報システムを構築する場合は，製品として調達する機器等について，IPv6 Ready Logo Program に基づく Phase-2 準拠製品を，可能な場合には選択するものとする。

２　情報セキュリティ推進責任者は，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ものとする。

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・監視）

第１１６条　情報セキュリティ推進責任者は，サーバー装置，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ものとする。

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定の整備）

第１１７条　統括情報セキュリティ責任者は，機構の情報システムの利用のうち，情報セキュ

リティに関する規定を整備するものとする。

2　統括情報セキュリティ責任者は，業務従事者が機構が支給する端末（学校等の管理区域外で使用する場合に限る。）及び機構支給以外の端末を用いて要保護情報を取り扱う場合について，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定めるものとする。

3　統括情報セキュリティ責任者は，学校等の管理区域外において機構外通信回線に接続した端末（支給外端末を含む。以下この項において同じ。）を学校等の管理区域外で機構内通信回線に接続することについての可否を判断した上で，可と判断する場合は，当該端末から機構内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

4　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利用手順を定めるものとする。当該手順には，以下の事項を含めるものとする。

一　業務従事者は，機構が支給する外部電磁的記録媒体，又は本条に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機構との間で取り決めた機構外の組織から受け取った外部電磁的記録媒体を使用すること。

二　自組織以外の組織から受け取った外部電磁的記録媒体は，自組織と当該組織との間で情報を運搬する目的に限って使用することとし，当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずるものとする。

5　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学校等の管理区域外に持ち出す際の許可手続を定めるものとする。

（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１１８条　情報セキュリティ推進責任者は，業務従事者による規定の遵守を支援する機能について情報セキュリティリスク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ものとする。

（情報システムの利用時の基本的対策）

第１１９条　業務従事者は，機構業務の遂行以外の目的で情報システムを利用しないものとする。

2　業務従事者は，情報セキュリティ推進責任者が接続許可を与えた通信回線以外に機構の情報システムを接続しないものとする。

3　業務従事者は，機構内通信回線に，情報セキュリティ推進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ものとする。

4　業務従事者は，情報システムで利用を禁止するソフトウェアを利用しないこと。また，情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は，情報セキュリティ推進責任者の承認を得るものとする。

5　業務従事者は，接続が許可されていない機器等を情報システムに接続しないものとする。

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

７　業務従事者は，機構が支給する端末（学校等の管理区域外で使用する場合に限る。）及び機構支給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ものとする。

８　業務従事者は，次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は，情報セキュリティ責任者の許可を得るものとする。

一　機構が支給する端末（学校等の管理区域外で使用する場合に限る）　機密性３情報，要保全情報又は要安定情報

二　機構支給以外の端末　要保護情報

９　業務従事者は，管理区域外において機構外通信回線に接続した端末（支給外端末を含む）を学校等の管理区域外で機構内通信回線に接続する場合には，情報セキュリティ管理者の許可を得た上で，定められた安全管理措置を講ずるものとする。

１０　業務従事者は，機密性３情報，要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を学校等の管理区域外に持ち出す場合には，情報セキュリティ管理者の許可を得るものとする。

（電子メール・ウェブの利用時の対策）

第１２０条　業務従事者は，要機密情報を含む電子メールを送受信する場合には，それぞれの機構が運営し，又は業務委託した電子メールサーバーにより提供される電子メールサービスを利用するものとする。

２　業務従事者は，機構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ドメイン名及び機構ドメイン名を使用するものとする。ただし，次に掲げる場合は除く。

一　機構が，高等教育機関向けのドメイン名を使用すると判断する場合。

二　電子メールを受信する機構外の者が，業務従事者から送信された電子メールであることを認知できる場合（政府ドメイン名又は前号に基づき取得したドメイン名が使用できない場合に限る）。

３　業務従事者は，不審な電子メールを受信した場合には，あらかじめ定められた手順に従い，対処するものとする。

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

５　業務従事者は，ウェブクライアントが動作するサーバー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ものとする。

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

一　送信内容が暗号化されること。

二　当該ウェブサイトが送信先として想定している組織のものであること。

（識別コード・主体認証情報の取扱い）

第１２１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ものとする。
２　業務従事者は，自己に付与された識別コードを適切に管理するものとする。
３　業務従事者は，管理者権限を持つ識別コードを付与された場合には，管理者としての業務遂行時に限定して，当該識別コードを利用するものとする。
４　業務従事者は，自己の主体認証情報の管理を徹底するものとする。

（暗号・電子署名の利用時の対策）
第１２２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ものとする。
２　業務従事者は，暗号化された情報の復号又は電子署名の付与に用いる鍵について，定められた鍵の管理手順等に従い，これを適切に管理するものとする。
３　業務従事者は，暗号化された情報の復号に用いる鍵について，鍵のバックアップ手順に従い，そのバックアップを行うものとする。

（不正プログラム感染防止）
第１２３条　業務従事者は，不正プログラム感染防止に関する措置に努めるものとする。
２　業務従事者は，情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は，感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断し，各情報インシデント窓口に連絡するなど，必要な措置を講ずるものとする。

（ウェブ会議サービスの利用時の対策）
第１２３条の２　業務従事者は，機構の定める利用手順に従い，ウェブ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ものとする。

２　業務従事者は，ウェブ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ものとする。
３　業務従事者は，ウェブ会議の運用時には以下の事項に留意するものとする。
(ア)事前にウェブ会議の操作方法を確認し，自分の発言時以外は常にマイクをミュートにすること。
(イ)会議音声が外部へ漏れないよう，適宜ヘッドセット等のツールを用いること。
(ウ)機密性の高い情報をウェブ会議で取り扱う場合は周りに人がいない環境で行うこと。
(エ)ウェブ会議の主催者は，事前にウェブ会議の操作方法を確認し，発言者以外でマイクがオンになっているのを発見した場合は適宜ミュートにすること。
(オ)カメラを使用する場合は，事前に背景をぼかす，別の画像にする等の対応を行い，背景に機密性の高い情報が映らないよう注意を払うこと。
(カ)画面共有時には，ウィンドウ単位での共有等を行う等，機密性の高い情報が画面共有で映らないよう注意を払うこと。
(キ)原則として，複数の会議に同時に参加しないこと。
(ク)その他，ウェブ会議を運用する場合は，意図せぬところで情報が漏れることがないよ

う注意を払うこと

第２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時の対策）

第１２４条　統括情報セキュリティ責任者は，機構が管理するアカウントでソーシャルメディアサービスを利用することを前提として，以下を含む情報セキュリティ対策に関する運用手順等を定めるものとする。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ものとする。

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

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

２　業務従事者は，要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は，機構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ものとする。

第３節　テレワーク

（実施規定の整備）

第１２５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規定を整備すること。なお，原則としてテレワークは機構が支給する端末で行うよう定めるものとする。

（実施環境における対策）

第１２６条　情報セキュリティ推進責任者は，テレワークの実施により機構外通信回線を経由して機構の情報システムへリモートアクセスする形態となる情報システムを構築する場合は，通信経路及びリモートアクセス特有の攻撃に対するセキュリティを確保するものとする。

２　情報セキュリティ推進責任者は，リモートアクセスに対し多要素主体認証を行うものとする。

３　情報セキュリティ推進責任者は，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ものとする。

４　情報セキュリティ推進責任者は，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ものとする。

（実施時における対策）

第１２７条　情報セキュリティ推進責任者は，テレワーク実施前及び実施後に業務従事者がチェックするべき項目を定め，業務従事者に当該チェックを実施させるものとする。

２　業務従事者は，画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定するものとする。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も

のとする。

３　業務従事者は，原則として情報セキュリティ対策の状況が定かではない又は不十分な機構外通信回線を利用してテレワークを行わないものとする。

附　則（平成２２年３月３１日制定）

この規則は，平成２２年４月１日から施行する。ただし，第２章 情報セキュリティの管理体制は平成２０年４月１日から適用する。

附　則（平成２５年９月３０日一部改正）

この規則は，平成２５年１０月１日から施行する。

附　則（平成３０年２月２２日全部改正）

この規則は，平成３０年２月２２日から施行する。

附　則（令和２年１０月２０日一部改正）

この規則は，令和２年１０月２０日から施行する。

附　則（令和４年１月２８日一部改正）

この規則は，令和４年１月２８日から施行する。

別表

用語の定義（第８条関係）

１．一般的な用語

用語		解説
【あ】	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」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。
	暗号化消去	●「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。
	ウェブ会議サービス	●「ウェブ会議サービス」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をいう。なお，特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。
【か】	外部サービス	●「外部サービス」とは，機構外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ものをいう。ただし，当該機能において機構の情報が取り扱われる場合に限る。
	外部サービス管理者	●「外部サービス管理者」とは，外部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外部サービスに係る管理を行う者をいう。
	外部サービス提供者	●「外部サービス提供者」とは，外部サービスを提供する事業者をいう。外部サービスを利用して機構に向けて独自のサービスを提供する事業者は含まれない。
	外部サービス利用者	●「外部サービス利用者」とは，外部サービスを利用する業務従事者又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。
	機器等	●「機器等」とは，情報システムの構成要素（サーバー装置，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。
	機構外通信回線	●「機構外通信回線」とは，通信回線のうち，機構内通信回線以外のものをいう。

用語		解説
	機構内通信回線	●「機構内通信回線」とは，一つの機構が管理するサーバー装置又は端末の間の通信の用に供する通信回線であって，当該機構の管理下にないサーバー装置又は端末が論理的に接続されていないものをいう。機構内通信回線には，専用線や VPN 等物理的な回線を機構が管理していないものも含まれる。
	基盤となる情報システム	●「基盤となる情報システム」とは，他の機関等と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。
	業務委託	●「業務委託」とは，機構の業務の一部又は全部について，契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず，全て含むものとする。ただし，当該業務において機構の情報を取り扱わせる場合に限る。
	記録媒体	●「記録媒体」とは，情報が記録され，又は記載される有体物をいう。記録媒体には，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は認識することができない方式で作られる記録であって，情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（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，サーバー装置，端末，通信回線装置等に内蔵される内蔵電磁的記録媒体と，USB メモリ，外付けハードディスクドライブ，DVD-R 等の外部電磁的記録媒体がある。
	クラウドサービス	●「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。
【さ】	サーバー装置	●「サーバー装置」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，機構が調達又は開発するものをいう。

用語		解説
	CSIRT	●「CSIRT」（シーサート）とは，機構において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，当該機構に設置された体制をいう。Computer Security Incident Response Team の略。
	実施手順	●「実施手順」とは，対策規則に定められた対策内容を個別の情報システムや業務において実施するため，あらかじめ定める必要のある具体的な手順をいう。
	情報	●「情報」とは，第２条第２項に定めるものをいう。
	情報システム	●「情報システム」とは，ハードウェア及びソフトウェアから成るシステムであって，情報処理又は通信の用に供するものをいい，特に断りのない限り，機構が調達又は開発するもの（管理を業務委託しているシステムを含む。）をいう。
	情報の抹消	●「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，暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や，情報を記録している記録媒体を物理的に破壊すること等も含まれる。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。
	政府ドメイン名	●「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。日本国の政府機関，独立行政法人，特殊法人（特殊会社を除く。）が登録（取得）することができる。
【た】	端末	●「端末」とは，情報システムの構成要素である機器のうち，業務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい，特に断りがない限り，機構が調達又は開発するものをいう。端末には，モバイル端末も含まれる。
	通信回線	●「通信回線」とは，複数の情報システム又は機器等（機構が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい，特に断りのない限り，機構の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には，機構が直接管理していないものも含まれ，その種類（有線又は無線，物理回線又は仮想回線等）は問わない。

用語		解説
	通信回線装置	●「通信回線装置」とは，通信回線間又は通信回線と情報システムの接続のために設置され，回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には，いわゆるハブやスイッチ，ルーター等のほか，ファイアウォール等も含まれる。
	テレワーク	●「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。
	特定用途機器	●「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，入退管理システム，施設管理システム，環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって，通信回線に接続されている，又は内蔵電磁的記録媒体を備えているものをいう。
	不正プログラム	●「不正プログラム」とは，コンピューターウイルス，ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム），スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の，情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。
【ま】	抹消	●「抹消」→「情報の抹消」を参照。
	明示等	●「明示等」とは，情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には，情報ごとに格付を記載することによる明示のほか，当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては，特定の情報システムに記録される情報について，その格付を情報システムの規程等に明記するとともに，当該情報システムを利用する全ての者に周知すること等が挙げられる。
	モバイル端末	●「モバイル端末」とは，端末のうち，業務上の必要に応じて移動させて使用することを目的としたものをいい，端末の形態は問わない。

２．機構独自の用語

用語		解説
【機構組織に関する用語】		
	機構	独立行政法人国立高等専門学校機構をいう。
	機構本部	独立行政法人国立高等専門学校機構本部をいう。
	学校	独立行政法人国立高等専門学校機構が設置する高等専門学校をいう。
	学校等	「機構本部」及び「学校」をいう。
	役員	独立行政法人国立高等専門学校機構法に定める役員をいう。
	最高情報責任者	独立行政法人国立高等専門学校機構最高情報責任者（CIO）等に関する規則（機構規則第８５号）に定められた者をいう。
	機構の教職員	「役員」及び「学校等の教職員」の全体をいう。
	学校等の教職員	「学校等」に勤務する常勤又は非常勤の教職員をいう。各学校等の教職員の範囲については，当該「学校等」の情報セキュリティ管理規程別表２に定める。
	学校の学生	「学校」に在籍する本科生，専攻科生，科目等履修生，研究生，及び研修生をいう。各学校の学生の範囲については，当該学校の情報セキュリティ管理規程別表３で定める。
	利用者	「経常的利用者」，「臨時利用者」，その他「機構」のアクセス制限された「情報資産」を利用するすべての者をいう。
	経常的利用者	「学校等の教職員」，「学校の学生」，及び「学校等」の「実施規程」に基づき「情報資産」を「機構」の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者をいう。
	臨時利用者	「学校等」の「実施規程」に基づき「情報資産」を臨時に利用する許可を得て利用する者をいう。
	業務従事者	「学校等の教職員」，及び「学校等」の「実施規程」に基づき「情報資産」を機構の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者をいう。
	文部科学省等	具体的に「文部科学省サイバーセキュリティ・情報化推進室，文部科学省高等教育局専門教育課高等専門学校係，情報処理推進機構セキュリティセンター（IPA），外部 CSIRT（シーサート）」等を示す。
	機構の管理区域	「学校等の管理区域」の全体をいう。

用語		解説
	学校等の管理区域	「学校等」が保有又は管理する土地，建物，建物附属設備，構築物及び船舶等における物理的環境内の情報資産を管理する区域をいう。各学校等の管理区域の範囲については，当該学校の情報セキュリティ管理規程別図１及び別表４で定める。
	安全区域	要保護情報又はそれを処理する「情報システム」を設置する区域であって，許可された者以外の侵入や災害の発生等を原因とする情報セキュリティの侵害に対して，施設及び環境面から対策が講じられている区域をいう。
	情報セキュリティ対策推進体制	機構の情報セキュリティ対策の推進に係る事務を遂行するため，設置された体制をいう。
【機構のセキュリティに関する用語】		
	情報セキュリティインシデント	「物理的インシデント」，「システムインシデント」及び「コンテンツインシデント」をいう。
	物理的インシデント	「情報セキュリティ」の確保を困難とする物理的原因の発生及び発生の恐れをいう。物理的原因には，地震・暴風雨・浸水・落雷・火災・建物の倒壊・爆破・盗難等，「情報システム」の機能不全や障害等を引き起こすすべての災害・事故・過失・妨害等及び情報の盗難，紛失等を含む。

用語		解説
	システムインシデント	「情報セキュリティ」の確保を困難とする「情報システム」に係わる行為又は事象の発生並びにそれらの恐れをいう。そのような行為には，「情報システム」の稼動を妨害する行為，データの改ざん・消失・漏洩・暴露等を起こす行為，及びネットワークの帯域や「コンピューターシステム」の CPU・メモリ等の資源を浪費する行為すべてを含み，その行為が意図的に実施されたものであるか否かを問わない。システムインシデントを誘起する行為又は事象として下記の例がある。 ・大量のスパムメールの送信 ・コンピューターウイルスの頒布や蔓延 ・不正アクセス禁止法に定められた特定電子計算機のアクセス機能を免れる行為 ・サービス不能攻撃 ・当該「情報システム」の管理権限を持つ者の要請に基づかずに，管理権限のない「情報システム」のセキュリティ上の脆弱性を検知する行為 ・実施規程により禁止されている形態での P2P ソフトウェアの利用 ・許可された方法によらない「情報システム」の接続 ・機構の「情報システム」への侵入を許すような「アカウント」を格納した「情報システム」の盗難・紛失 ・操作ミス又は故意による機密情報の漏洩又は暴露
	コンテンツインシデント	法令又は公序良俗に違反する内容の情報取得又は発信行為及びその恐れをいう。コンテンツインシデントを誘起する行為の例として次のものがある。 ・通信の秘密を侵害する行為 ・他人の著作物の違法コピーのアップロード等，他人の著作権等の知的財産権を侵害する情報の発信 ・児童ポルノ，わいせつ画像等の公開 ・差別，侮辱，ハラスメント等にあたる情報の発信又は公開 ・機構の情報システムを用いた営業ないし商業を目的とした内容の発信又は公開
【規則に関する用語】		
	基本方針	独立行政法人国立高等専門学校機構サイバーセキュリティポリシー基本方針をいう。

用語		解説
	実施規則	独立行政法人国立高等専門学校機構サイバーセキュリティポリシー対策規則（機構規則第９８号）並びに独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係る情報格付規則（機構規則第９９号）及び独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係る監査規則（機構規則第１０１号）及び独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係るソフトウェア管理規則（機構規則第９４号）をいう。
	実施規程	「基本方針」，「実施規則」に基づき，「学校等」において策定される規程，基準及び計画をいう。
	実施手順	「実施規程」に基づき，「学校等」において策定される具体的な手順やマニュアル，ガイドラインをいう。
	機構情報セキュリティ関連規程等	「基本方針」，「実施規則」，「実施規程」，「実施手順」を総称したものをいう。
【機構の情報及び情報システムに関する用語】		
	学校等の情報システム	次に掲げる「情報システム」をいう。 ①「学校等」により保有又は管理されている「情報システム」 ②「学校等」との契約又は他の協定に従って提供される「情報システム」各学校等の情報システムの範囲については，当該「学校等」の情報セキュリティ管理規程別表１で定める。
	情報資産	「情報」及び「情報システム」をいう。
	コンピューターシステム	メインフレーム計算機，ワークステーション，サーバー，パーソナルコンピューターなど計算機全般を指し，オペレーティングシステム，接続される周辺機器，「情報ネットワーク機器」及び端末装置等を含む。
	情報ネットワーク機器	情報ネットワークの接続のために設置され，情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール，ルーター，ハブ，情報コンセント及び無線ネットワークアクセスポイントを含む。）をいう。

用語		解説
	アカウント	「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」又は他の「情報システム」に付与された正当な権限をいう。また，狭義には，「利用者」又は他の「情報システム」に付与された「識別符号」及び「主体認証情報」の組み合わせ，又はそれらのいずれかを指してアカウントという。なお，アカウントには統一認証に対応した「情報システム」のアカウントも含む。
	証跡	証跡はログの中でも高い証拠性を求められるものをいう。

別紙

各節又は款の目的及び趣旨（第５条関係）

第１章　総則

「第１節　本対策規則の目的・適用範囲」の目的及び趣旨

情報セキュリティの基本は，機構で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり，機構が自らの責任において情報セキュリティ対策を講じていくことが原則である。

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

「第１款　組織・体制の整備」の目的及び趣旨

情報セキュリティ対策は，それに係る全ての業務従事者が，職制及び職務に応じて与えられている権限と責務を理解した上で，負うべき責務を全うすることで実現される。そのため，それらの権限と責務を明確にし，必要となる組織・体制を整備する必要がある。特に最高情報セキュリティ責任者は，情報セキュリティ対策を着実に進めるために，自らが組織内を統括し，組織全体として計画的に対策が実施されるよう推進しなければならない。

なお，最高情報セキュリティ責任者は，対策規則に定められた自らの担務を，最高情報セキュリティ副責任者その他の対策規則に定める責任者等に担わせることができる。

「第２款　対策規則・対策推進計画の策定」の目的及び趣旨

機構の情報セキュリティ水準を適切に維持し，情報セキュリティリスクを総合的に低減させるためには，機構として遵守すべき対策の基準を定めるとともに，情報セキュリティに係るリスク評価の結果を踏まえた上で定めるとともに，計画的に対策を実施することが重要である。

「第３款　実施規定及び実施手順の策定」の目的及び趣旨

機構においては，学校等の単位で実施規則等を定める事項である。

「第４款　業務継続計画の策定」の目的及び趣旨

業務継続計画について定める事項である。

第２節　運用

「第１款　機構情報セキュリティ関連規程等の運用」の目的及び趣旨

機構は，対策規則に定められた対策を実施するため，具体的な実施手順を定める必要がある。

実施手順が整備されていない，又はそれらの内容に漏れがあると，対策が実施されないおそれがあることから，最高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に実施手順の整備を指示し，その結果について定期的に報告を受け，状況を適確に把握することが重要である。

「第２款　例外措置」の目的及び趣旨

例外措置はあくまで例外であって，濫用があってはならない。しかしながら，機構情報セキュリティ関連規程等の適用が機構業務の適正な遂行を著しく妨げるなどの理由により，規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために，例外措置の手続を定めておく必要がある。

「第３款　教育」の目的及び趣旨

機構情報セキュリティ関連規程等が適切に整備されているとしても，その内容が業務従事者に認知されていなければ，当該規定が遵守されないことになり，情報セキュリティ水準の向上を望むことはできない。このため，全ての業務従事者が，機構情報セキュリティ関連規程等への理解を深められるよう，適切に教育を実施することが必要である。

また，機構等における近年の情報セキュリティインシデントの増加等に鑑み，情報セキュリティの専門性を有する人材を育成することも求められる。

「第４款　情報セキュリティインシデントへの対処」の目的及び趣旨

情報セキュリティインシデントを認知した場合には，最高情報セキュリティ責任者に早急にその状況を報告するとともに，被害の拡大を防ぎ，回復のための対策を講ずる必要がある。また，情報セキュリティインシデントの対処が完了した段階においては，原因について調査するなどにより，情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し，再発防止や対処手順，体制等の見直しにつなげることが重要である。

第３節　点検

「第１款　情報セキュリティ対策の自己点検」の目的及び趣旨

情報セキュリティ対策の実効性を担保するためには，機構情報セキュリティ関連規程等の遵守状況等を点検し，その結果を把握・分析することが必要である。

自己点検は，業務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく，組織全体の情報セキュリティ水準を確認する目的もあることから，適切に実施することが重要である。

また，自己点検の結果を踏まえ，各当事者は，それぞれの役割の責任範囲において，必要となる改善策を実施する必要がある。

「第２款　情報セキュリティ監査」の目的及び趣旨

情報セキュリティ対策の実効性を担保するためには，情報セキュリティ対策を実施する者による自己点検だけでなく，独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

また，監査の結果で明らかになった課題を踏まえ，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に指示し，必要な対策を講じさせることが重要である。

「第４節　情報セキュリティ対策の見直し」の目的及び趣旨

情報セキュリティを取り巻く環境は常時変化しており，こうした変化に的確に対応しないと，情報セキュリティ水準を維持できなくなる。このため，機構の情報セキュリティ対策の根幹をなす機構情報セキュリティ関連規程等は，実際の運用において生じた課題，自己点検・監査等の結果や情報セキュリティに係る重大な変化等を踏まえ，保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し，リスクを評価し，適時見直しを行う必要がある。

また，情報セキュリティに係る取組をより一層推進するためには，上記のリスク評価の結果を対策規則及び対策推進計画に反映することも重要である。

第３章　情報の取扱い

「第１節　情報の取扱い」の目的及び趣旨

機構業務の遂行に当たっては，情報の作成，入手，利用，保存，提供，運搬，送信，消去等（以下本款において「利用等」という。）を行う必要があり，ある情報のセキュリティの確保のためには，当該情報を利用等する全ての業務従事者が情報のライフサイクルの各段階において，当該情報の特性に応じた適切な対策を講ずる必要がある。このため，業務従事者は，情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに，情報の格付や取扱制限に応じた対策を講ずる必要がある。

「第２節　情報を取り扱う区域の管理」の目的及び趣旨

サーバー装置，端末等が，不特定多数の者により物理的に接触できる設置環境にある場合においては，悪意ある者によるなりすまし，物理的な装置の破壊のほか，サーバー装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他，設置環境に関する脅威として，災害の発生による情報システムの損傷等もある。

したがって，執務室，会議室，サーバー室等の情報を取り扱う区域に対して，物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し，当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

第４章　外部委託

第１節　業務委託

「第１款　業務委託」の目的及び趣旨

機構外の者に，情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に，業務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は，委託先において対策規則に適合した情報セキュリティ対策が確実に実施されるよう，委託先への要求事項を調達仕様書等に定め，委託の際の契約条件とする必要がある。

業務委託には以下の例のように様々な種類があり，また，契約形態も，請負契約や委任，準委任，約款への同意等様々であるが，いずれの場合においても，前述のように委託先において対策基準に適合した情報セキュリティ対策が確実に実施される必要のある業務委託の契約時には，委託する業務の範囲や委託先の責任範囲等を明確化し，契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお，委託先で外部サービスを利用する場合は，委託先においても外部サービス特有のリスクがあることから，4.2「外部サービスの利用」で規定する内容についても委託先への要求事項に含める必要がある。

＜業務委託の例＞

- 情報システムの開発及び構築業務
- アプリケーション・コンテンツの開発業務
- 情報システムの運用業務
- 業務運用支援業務（統計，集計，データ入力，媒体変換等）
- プロジェクト管理支援業務
- 調査・研究業務（調査，研究，検査等）

「第２款　外部サービスの利用」の目的及び趣旨

業務委託により機構業務を遂行する場合は，原則として第４章第１節第１款「業務委託」にて規定する事項について，外部サービス提供先と特約を締結するなどし，情報セキュリティ対策を適切に講ずる必要がある。しかしながら，要機密情報を取り扱わない場合であって，外部サービス提供先における高いレベルの情報管理を要求する必要が無い場合には，民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等，別表「用語の定義」において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には，種々の情報を機構からサービス提供事業者等に送信していることを十分認識し，リスクを十分踏まえた上で利用の可否を判断し，第４章第１節第１款「業務委託」を適用するのではなく，本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

第５章　情報システムのライフサイクル

第１節　情報システムに係る文書等の整備

「第１款　情報システムに係る台帳等の整備」の目的及び趣旨

機構が所管する情報システムの情報セキュリティ水準を維持するとともに，情報セキュリティインシデントに適切かつ迅速に対処するためには，機構が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに，情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように，日頃から文書として整備しておき，その所在を把握しておくことが重要である。

「第２款　機器等の調達に係る規定の整備」の目的及び趣旨

調達する機器等において，必要なセキュリティ機能が装備されていない，当該機器等の製造過程で不正な変更が加えられている，調達後に情報セキュリティ対策が継続的に行えないといった場合は，情報システムで取り扱う情報の機密性，完全性及び可用性が損なわれるおそれがある。

これらの課題に対応するため，対策規則に基づいた機器等の調達を行うべく，機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

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

「第１款　情報システムの企画・要件定義」の目的及び趣旨

情報システムのライフサイクル全般を通じて，情報セキュリティを適切に維持するためには，情報システムの企画段階において，適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は，過剰な情報セキュリティ対策に伴うコスト増加のおそれ，要件解釈のばらつきによる提案内容の差異からの不公平な競争入札，設計・開発工程での手戻り，運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため，情報システムが対象とする業務，業務において取り扱う情報，情報を取り扱う者，情報を処理するために用いる環境・手段等を考慮した上で，当該情報システムにおいて想定される脅威への対策を検討し，必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて，構築する情報システムへの脆弱性の混入を防止するための対策も，構築前の企画段階で考慮することが重要となる。

また，情報システムの構築，運用・保守を業務委託する場合については，第４章第１節「業務委託」についても併せて遵守する必要がある。

「第２款　情報システムの調達・構築」の目的及び趣旨

情報システムを調達・構築する際には，策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために，選定基準に適合した機器等の調達や，情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また，機器等の納入時又は情報システムの受入れ時には，整備された検査手続に従い，当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が，適切に情報システムに組み込まれていることを検査することが必要となる。

「第３款　情報システムの運用・保守」の目的及び趣旨

情報システムの運用段階に移るに当たり，企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように，人的な運用体制を整備し，機器等のパラメータが正しく設定されていることの定期的な確認，運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから，適宜情報システムの情報セキュリティ対策の実効性を確認するために，情報システムの運用状況を監視することも重要である。

また，情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても，対策規則に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

「第４款　情報システムの更改・廃棄」の目的及び趣旨

情報システムの更改・廃棄において，情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や，格付や取扱制限を完全に把握

できていない場合等においては，記録されている情報の完全な抹消等の措置を講ずることが必要となる。

「第５款　情報システムについての対策の見直し」の目的及び趣旨

情報セキュリティを取り巻く環境は常時変化しており，新たに発生した脅威等に的確に対応しない場合には，情報セキュリティ水準を維持できなくなる。このため，情報システムの情報セキュリティ対策を定期的に見直し，さらに外部環境の急激な変化等が発生した場合は，適時見直しを行うことが必要となる。

「第３節　情報システムの運用継続計画」の目的及び趣旨

業務の停止が国民及び機構関係者の安全や利益に重大な脅威をもたらす可能性のある業務は，非常時でも継続させる必要があり，機構においては，中期目標による指示等により，業務継続計画と情報システム運用継続計画を策定し運用している。

一方，非常時に情報システムの運用を継続させる場合には，非常時における情報セキュリティに係る対策事項を検討し，定めることが重要となる。

なお，こうした業務継続計画や情報システムの運用継続計画が定める要求事項と，機構情報セキュリティ関連規程等が定める要求事項とで矛盾がないよう，それぞれの間で整合性を確保する必要がある。

第６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

「第１款　主体認証機能」の目的及び趣旨

情報又は情報システムへアクセス可能な主体を制限するためには，主体認証機能の導入が必要である。その際，アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また，機構の情報システムにおいて，国民及び機構関係者向けのサービスを提供する場合は，国民及び機構関係者が情報システムへのアクセスの主体となることにも留意して，主体認証情報を適切に保護しなければならない。

「第２款　アクセス制御機能」の目的及び趣旨

アクセス制御とは，情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合，当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって，情報漏えい等のリスクを軽

減することができると考えられる。

「第３款　権限の管理」の目的及び趣旨

重要システムのアクセス制御機能を適切に運用するためには，主体から対象に対するアクセスの権限を適切に設定することが必要である。権限の管理が不適切になると，情報又は情報システムへ不正アクセスされるおそれが生じる。

また，情報システムの管理機能として，一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合，主体認証情報等の漏えい，改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから，限られた主体のみに管理者権限が付与されることが重要である。

「第４款　ログの取得・管理」の目的及び趣旨

情報システムにおけるログとは，システムの動作履歴，利用者のアクセス履歴，通信履歴その他運用管理等に必要な情報が記録されたものであり，悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また，情報システムに係る情報セキュリティ上の問題が発生した場合には，当該ログは，事後の調査の過程で，問題を解明するための重要な材料となる。したがって，情報システムにおいては，仕様どおりにログが取得され，また，改ざんや消失等が起こらないよう，ログが適切に保全されなければならない。

「第５款　暗号・電子署名」の目的及び趣旨

情報システムで取り扱う情報の漏えい，改ざん等を防ぐための手段として，暗号と電子署名は有効であり，情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は，使用する暗号アルゴリズムに加え，それを用いた暗号プロトコルが適切であること，運用時に当該アルゴリズムが危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

第２節　情報セキュリティの脅威への対策

「第１款　ソフトウェアに関する脆弱性対策」の目的及び趣旨

機構の情報システムに対する脅威としては，第三者が情報システムに侵入し機構の重要な情報を窃取・破壊する，第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に，国民及び機構関係者向けに提供するサービスが第三者に侵入され，個人情報等の重要な情報の漏えい等が発生した場合，国民生活に多大な影響を及ぼ

すとともに機構に対する社会的な信用が失われる。

一般的に，このような攻撃では，情報システムを構成するサーバー装置，端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって，機構の情報システムにおいては，ソフトウェアに関する脆弱性について，迅速かつ適切に対処することが求められる。

なお，情報システムを構成するハードウェアに関しても，同様に脆弱性が存在する場合があるので，第５章第２節第２款「情報システムの調達・構築」の規定も参照し，必要な対策を講ずる必要がある。

「第２款　不正プログラム対策」の目的及び趣旨

情報システムが不正プログラムに感染した場合，情報システムが破壊される脅威や，当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには，不正プログラムに感染した情報システムは，他の情報システムに感染を拡大させる，迷惑メールの送信やサービス不能攻撃等の踏み台として利用される，標的型攻撃における拠点として利用されるなどが考えられ，当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため，不正プログラムへの対策を適切に実施することが必要である。

「第３款　サービス不能攻撃対策」の目的及び趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては，第三者からサービス不能攻撃を受け，利用者がサービスを利用できなくなることが想定される。このため，機構の情報システムのうち，インターネットからアクセスを受けるものについては，サービス不能攻撃を想定し，システムの可用性を維持するための対策を実施する必要がある。

「第４款　標的型攻撃対策」の目的及び趣旨

標的型攻撃とは，特定の組織に狙いを絞り，その組織の業務習慣等内部情報について事前に入念な調査を行った上で，様々な攻撃手法を組み合わせ，その組織に最適化した方法を用いて，執拗に行われる攻撃である。典型的なものとしては，組織内部に潜入し，侵入範囲を拡大し，重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は，未知の手段も用いて実行されるため，完全に検知及び防御することは困難である。

したがって，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），並びに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）からなる，多重防御の情報セキュリティ対策体系によって，標的型攻撃に備える必要がある。

第３節　アプリケーション・コンテンツの作成・提供

「第１款　アプリケーション・コンテンツの作成時の対策」の目的及び趣旨

機構では，情報の提供，手続，意見募集等のサービスのためにアプリケーション・コンテンツを用意し，広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に，利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。機構は，アプリケーション・コンテンツの提供に際しても，情報セキュリティ対策を講じておく必要がある。

また，アプリケーション・コンテンツの開発・提供を業務委託する場合については，第４章第１節第１款「業務委託」についても併せて遵守する必要がある。

「第２款　アプリケーション・コンテンツ提供時の対策」の目的及び趣旨

機構では，情報の提供，手続及び意見募集等のサービスのためにウェブサイト等を用意し，国民及び機構関係者等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため，国民及び機構関係者等にとっては，そのサービスが実際の機構のものであると確認できることが重要である。また，機構になりすましたウェブサイトを放置しておくと，機構の信用を損なうだけでなく，国民及び機構関係者等が不正サイトに誘導され，不正プログラムに感染するおそれがあるため，このような事態への対策を講ずる必要がある。

第７章　情報システムの構成要素

第１節　端末・サーバー装置等

「第１款　端末」の目的及び趣旨

端末の利用に当たっては，不正プログラム感染や不正侵入を受けるなどの外的要因により，保存されている情報の漏えい等のおそれがある。また，業務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては，盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して，対策を講ずる必要がある。

端末については，サーバー等の他の情報システムの構成要素と異なり，機構の判断によっては機構支給以外のものの利用があり得る。機構における業務で端末を利用する以上は，機構により支給されたものか，それ以外かにかかわらず，同等の情報セキュリティ水準が求められる。このため，本款及び第８章第１節「情報システムの利用」での端末に係る規定においては，両者を対象としている箇所がある。この際，両者を区別して「機構が支給する端末」，「機構支給以外の端末」と表現している。単に「端末」という場合は，「用語定義」において定義されているとおり機構が支給するものを指す。

なお，本款の遵守事項のほか，第６章第１節「情報システムのセキュリティ機能」におい

て定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策，第６章第２節第１款「ソフトウェアに関する脆弱性対策」，第６章第２節第２款「不正プログラム対策」及び第７章第３節第２款「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

「第２款　サーバー装置」の目的及び趣旨

電子メールサーバーやウェブサーバー，ファイルサーバー等の各種サーバー装置には，大量の情報が保存されている場合が多く，当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また，サーバー装置は，通信回線等を介してその機能が利用される場合が多く，不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に機構が有するサーバー装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば，国民及び機構関係者からの信頼を大きく損なう。加えて，サーバー装置は，同時に多くの者が利用するため，その機能が停止した場合に与える影響が大きい。これらのことを考慮して，対策を講ずる必要がある。

なお，本項の遵守事項のほか，第６章第１節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策，第６章第２節第１款「ソフトウェアに関する脆弱性対策」，第６章第２節第２款「不正プログラム対策」，第６章第２節第３款「サービス不能攻撃対策」及び第７章第３節第２款「IPv6 通信回線」において定める遵守事項のうちサーバー装置に関係するものについても遵守する必要がある。また，特に電子メールサーバー，ウェブサーバー，DNS サーバー及びデータベースについては，本項での共通的な対策に加え，それぞれ第７章第２節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

「第３款　複合機・特定用途機器」の目的及び趣旨

機構においては，プリンタ，ファクシミリ，イメージスキャナ，コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は，機構内通信回線や公衆電話網等の通信回線に接続して利用されることが多く，その場合には，ウェブによる管理画面を始め，ファイル転送，ファイル共有，リモートメンテナンス等多くのサービスが動作するため，様々な脅威が想定される。

また，機構においては，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，入退管理システム，施設管理システム，環境モニタリングシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては，汎用的な機器のほか，システム特有の目的を達成するために必要な機能を有した特定用途機器が利用されている。さらに，特定用途機器の中には，インターネットに接続されるいわゆる IoT 機器があるが，近年 IoT 機器の脆弱性をついた攻撃が数多く発生しており，IoT 機器が踏み台となって他の情報システムへの攻撃に利用されるなど，社会的問題となってきている。このため，これらの機器に対する情報セキュリティ対策が必要となる。

したがって，複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と

捉え，責任者を明確にして適切に対策を講ずることが重要である。

第２節　電子メール・ウェブ等

「第１款　電子メール」の目的及び趣旨

電子メールの送受信とは情報のやり取りにほかならないため，不適切な利用により情報が漏えいするなどの機密性に対するリスクの他，悪意ある第三者等によるなりすまし等，電子メールが悪用される不正な行為の被害に電子メールを利用する業務従事者が巻き込まれるリスクもある。これらの問題を回避するためには，適切な電子メールサーバーの管理が必要である。

なお，本款の遵守事項のほか，第７章第１節第２款「サーバー装置」において定めるサーバー装置に係る遵守事項についても併せて遵守する必要がある。

「第２款　ウェブ」の目的及び趣旨

インターネット上に公開するウェブサーバーは，常に攻撃を受けるリスクを抱えている。様々な攻撃により，ウェブコンテンツ（ウェブページとして公開している情報）の改ざん，ウェブサーバーの利用停止，偽サイトへの誘導等の被害が想定されるため，適切な対策を組み合わせて実施することが求められる。

なお，本款の遵守事項のほか，第７章第１節第２款「サーバー装置」において定めるサーバー装置に係る遵守事項についても併せて遵守する必要がある。

「第３款　ドメインネームシステム（DNS)」の目的及び趣旨

ドメインネームシステム（DNS：Domain Name System）は，インターネットを使った階層的な分散型システムで，主としてインターネット上のホスト名や電子メールに使われるドメイン名と，IP アドレスとの対応づけ（正引き，逆引き）を管理するために使用されている。DNS では，端末等のクライアント（DNS クライアント）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等について回答を行う。DNS には，機構が管理するドメインに関する問合せについて回答を行うコンテンツサーバーと，DNS クライアントからの要求に応じてコンテンツサーバーに対して問合せを行うキャッシュサーバーが存在する。キャッシュサーバーの可用性が損なわれた場合は，ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また，コンテンツサーバーが提供する情報の完全性が損なわれ，誤った情報を提供した場合は，端末等の DNS クライアントが悪意あるサーバーに接続させられるなどの被害に遭う可能性がある。さらに，電子メールのなりすまし対策の一部は DNS で行うため，これに不備があった場合には，なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには，DNS サーバーの適切な管理が必要である。

なお，本款の遵守事項のほか，第７章第１節第２款「サーバー装置」において定めるサーバー装置に係る遵守事項についても併せて遵守する必要がある。

「第４款　データベース」の目的及び趣旨

本款における「データベース」とは，データベース管理システムとそれによりアクセスされるデータファイルから構成され，体系的に構成されたデータを管理し，容易に検索・抽出等が可能な機能を持つものであって，要保護情報を保管するサーバー装置とする。

要保護情報を保管するデータベースでは，不正プログラム感染や不正アクセス等の外的要因によるリスク及び業務従事者の不適切な利用や過失等の内的要因によるリスクに対して，管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合，そのデータが漏えい等した際の影響が大きく，また，そのようなデータは攻撃者の標的となりやすい。

なお，本款の遵守事項のほか，第６章第１節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策，第６章第２節第１款「ソフトウェアに関する脆弱性対策」，第６章第２節第２款「不正プログラム対策」及び第７章第３節第２款「IPv6 通信回線」において定める遵守事項のうち，データベースに関係するものについても併せて遵守する必要がある。

第３節　通信回線

「第１款　通信回線」の目的及び趣旨

サーバー装置や端末への不正アクセスやサービス不能攻撃等は，当該サーバー装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから，通信回線及び通信回線装置に対する情報セキュリティ対策については，情報システムの構築時からリスクを十分検討し，必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し，対策を講ずる必要がある。

また，情報システムの運用開始時と一定期間運用された後とでは，通信回線の構成や接続される情報システムの条件等が異なる場合があり，攻撃手法の変化も想定されることから，情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため，通信回線の運用時においても，継続的な対策を実施することが重要である。

「第２款　IPv6 通信回線」の目的及び趣旨

機構において，インターネットの規格である IPv6 通信プロトコルに対応するための取組が進められているが，IPv6 通信プロトコルを採用するに当たっては，グローバル IP アドレスによるパケットの直接到達性や IPv4 通信プロトコルから IPv6 通信プロトコルへの移行過程における共存状態等，考慮すべき事項が多数ある。

近年では，サーバー装置，端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷され，運用者が意図しな

い IPv6 通信が通信ネットワーク上で動作している可能性があり，結果として，不正アクセスの手口として悪用されるおそれもあることから，必要な対策を講じていく必要がある。

なお，IPv6 技術は今後も技術動向の変化が予想されるが，一方で，IPv6 技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから，機構においても，IPv6 の情報セキュリティ対策に関する技術動向を十分に注視し，適切に対応していくことが重要である。

第８章　情報システムの利用

「第１節　情報システムの利用」の目的及び趣旨

業務従事者は，業務の遂行のため，端末での事務処理のほか電子メール，ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合，情報セキュリティインシデントを引き起こすおそれがある。

このため，情報システムの利用に関する規定を整備し，業務従事者は規定に従って利用することが求められる。

なお，本款には第７章第１節第１款「端末」と同様に，機構が支給する端末と機構支給以外の端末の両者を対象にしている箇所がある。また，両者を包含する場合は，「端末（支給外端末を含む)」と表現している。