資料２

政府機関等の情報セキュリティ対策のための統一基準群の改定

（案）

資料２－１　政府機関等の情報セキュリティ対策のための統一基準群の改定（案）について

※資料２－２　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（案）

※資料２－３　政府機関等のサイバーセキュリティ対策のための統一基準（案）

※資料２－４　政府機関等のサイバーセキュリティ対策の運用等に関する指針（案）

資料２－５　「政府機関等のサイバーセキュリティ対策のための統一基準群（案）」に対する意見募集の結果の概要

※資料２－６　「政府機関等のサイバーセキュリティ対策のための統一基準群（案）」に対する意見募集の結果

※は、席上配布省略。

1. 政府機関等の情報セキュリティ対策のための統一基準群の改定（案）について

資料２－１

１．クラウドサービスの利用拡大を見据えた記載の充実

- 政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、クラウドサービス利用者側として実施すべき対策や考え方に係る記載を追加。
  ⇒外部サービスを安全に利用するために、業務内容や取り扱う情報の格付や取扱制限に応じた情報セキュリティ対策を自ら講じられることが重要。

２．情報セキュリティ対策の動向を踏まえた記載の充実

- 政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえた記載、また今後取り組むべき情報セキュリティ対策の将来像について記載。
  ⇒従来からの境界型防御を補完するものとして「常時アクセス判断・許可アーキテクチャ」にも目を向ける。また、情報システムの「常時システム診断・対処」を引き続き推進するなど、情報セキュリティ対策基盤を着実に進化させることが重要。

３．多様な働き方を前提とした情報セキュリティ対策の整理

- 新型コロナウイルス感染症対策として政府機関等においても急速に広まったテレワークや遠隔会議の経験も踏まえ、係る多様な働き方を前提とする場合に必要な情報セキュリティ対策について、参照すべき統一基準上の規定や解説を整理することで、政府機関等が実施すべき対策の水準を明確にする。
  ⇒危機管理や働き方改革への対応として、通常とは異なる環境下においても必要な情報セキュリティ水準を確保した上で業務の円滑な継続を図ることが重要。

2. 改定の概要1

１．クラウドサービスの利用拡大を見据えた記載の充実

«主な内容»

✓ 外部サービスの再定義と取り扱う情報に応じた適切なセキュリティ対策の実施
⇒境目が曖昧となっている「約款による外部サービス」と「クラウドサービス」を「外部サービス」として統合した上で、「外部サービス」上での要機密情報の取り扱いの有無により、求めるセキュリティ対策のレベルを整理。
⇒政府機関等が外部サービスを選択する際には、セキュリティ確保のために必要な事項を十分に考慮した上で、外部サービスが当該セキュリティ要件を満たす（※）ことを確認することが必要。

※民間事業者等が不特定多数の利用者に対して提供するSNS等の、画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない点は、従前より変更なし。

✓ ISMAP制度の活用
⇒要機密情報を取り扱う外部サービスのうちクラウドサービスを利用する場合に、その選定においてISMAP制度を活用。

✓ 外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加
⇒外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策のみならず、構築・運用・廃棄等のライフサイクルに渡ることから、要機密情報を取り扱う外部サービスの利用における導入・構築・運用・保守・更改・破棄の各フェーズのセキュリティ対策に係る規定を、ISO/IEC27017:2015を参考に追加。

✓ 外部サービスに係るシャドーIT対策
⇒組織の承認を得ずに職員等が外部サービスを利用するシャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。シャドーIT対策として、外部サービス利用時の組織内での承認・審査・申請の手続きを規定。

※従来の統一基準群では「約款による外部サービス」のみを承認等の対象としていたが、クラウドサービスを含む外部サービス全体を対象とした。

2. 改定の概要2

２．情報セキュリティ対策の動向を踏まえた記載の充実

«主な内容»

✓ 政府機関等に対する主要なサイバー攻撃や近年のサイバーセキュリティインシデント事例を踏まえた対策等の記載の追加
⇒以下の解説を追加し、より強固なサイバーセキュリティ対策を例示。

- EDR　端末の動作を監視し、異常時の管理者による迅速な対応を支援するための機能
- CDNサービス　Webコンテンツを複数のサーバに分配配置し、大量アクセスの負荷を軽減するサービス
- IT資産管理ソフトウェア　Windows Updateに代表されるセキュリティ更新ソフトウェアの適用状況を管理し、最適な状態を維持するソフトウェア
- 標的型メール攻撃　組織や個人の情報を入念に調査し情報を収集した上で、攻撃対象が疑念を抱かないよう、巧妙に偽装したメールにより仕掛けてくる攻撃
- 暗号化消去　暗号化された情報を復号するための「鍵」を抹消する論理的削除方法
- SSD等内蔵記録媒体を含む種々の電磁的記録媒体廃棄時の記録された情報の抹消
  フラッシュメモリタイプの電磁的記録媒体は、データ抹消ソフトウェアによる上書きを実施しても、実際には書き込みが行われず、消去すべき情報がそのまま残ってしまう領域が発生してしまうことへの注意

✓ 情報セキュリティ対策に係る最新の考え方等の反映
⇒アクセス制御機能の例として、常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ。「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という性悪説に基づいた考え方。）に関する記載を追加。
⇒メール添付による暗号化された電子ファイル受け渡し時の復号用パスワード受け渡し方法に関する記載を追加。また、暗号化する際に設定するパスワードやパスフレーズに求める十分な長さと複雑さについての解説を追加。

2. 改定の概要3

３．多様な働き方を前提とした情報セキュリティ対策の整理

«主な内容»

✓ テレワークに係る項目の新設
⇒テレワークを実施する際のサイバーセキュリティ対策に係る記述が複数の部に分散していたため項目を新設。テレワークに特有の情報セキュリティ対策について包括的に記載。

✓ Web会議サービス利用時の対策に係る項目の新設
⇒政府機関等において利用が急増したWeb会議サービスについて、利用時に行うべき情報セキュリティ対策について、項目を新設して記載。

✓ 機関等支給以外の端末に係る留意事項等の整理
⇒機関等支給以外の端末に係る記述が複数の部に分散していたため項目を新設して記載。
⇒機関等支給以外の端末においては、情報セキュリティ水準を一定以上に保ち続けることが困難であり、情報セキュリティインシデントの引き金となる可能性が高いことから、機関等が支給する端末の利用を原則としつつ、やむを得ず利用する場合の対策について整理。

資料２－２

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（案）

平成 28 年８月 31 日
平成 30 年７月 25 日改定
平成 31 年４月１日改定
令和３年　月　日改定
サイバーセキュリティ戦略本部決定

第一章　目的及び適用対象（第一条―第二条）
第二章　政府機関等の情報セキュリティ対策のための基本方針（第三条―第四条）
第三章　政府機関等の情報セキュリティ対策のための基本対策（第五条―第二十三条）
附則

第一章　目的及び適用対象

（目的）

第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。

一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人

三　指定法人　法第十三条に規定する指定法人

２　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職

員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。

３　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）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。）及び情報システムの設計又は運用管理に関する情報とする。

第二章　政府機関等の情報セキュリティ対策のための基本方針

（リスク評価と対策）

第三条　機関等は、自組織の目的等を踏まえ、第十条に定める自己点検の結果、第十一条に定める監査の結果、法に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、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、必要となる情報セキュリティ対策を講じなければならない。

２　機関等は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直さなければならない。

（情報セキュリティ文書）

第四条　機関等は、自組織の特性を踏まえ、基本方針（機関等における情報セキュリティ対策の基本的な方針をいう。以下同じ。）及び対策基準（機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。以下同じ。）を定めなければならない。基本方針及び対策基準（以下「ポリシー」という。）の呼称は機関等で独自に定めることができる。

２　基本方針は、情報セキュリティを確保するため、情報セキュリティ対策の目的、対象範囲等の情報セキュリティに対する基本的な考え方を定めなければならない。

３　対策基準は、別に定める政府機関等のサイバーセキュリティ対策のための統一基準（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。

４　国の行政機関は、必要に応じて、所管する独立行政法人及び指定法人に対して、自らのポリシーを当該法人がポリシーを定める際に参照するよう求めることとする。

５　独立行政法人及び指定法人は、前項の求めに応じることとする。

６　機関等は、前条第一項の評価結果を踏まえ、ポリシーの評価及び見直しを行わなければならない。

第三章　政府機関等の情報セキュリティ対策のための基本対策

（管理体制）

第五条　機関等は、情報セキュリティ対策を実施するための組織・体制を整備しなければならない。

２　機関等は、最高情報セキュリティ責任者１人を置かなければならない。

３　最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置かなければならない。

４　最高情報セキュリティ責任者は、本規範にて規定した機関等における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。

５　最高情報セキュリティ責任者は、統一基準に定められた自らの担務を、統一基準に定める責任者に担わせることができる。

（対策推進計画）

第六条　最高情報セキュリティ責任者は、第三条第一項の評価の結果を踏まえた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。）を定めなければならない。

２　機関等は、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。

３　最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行わなければならない。

（例外措置）

第七条　機関等は、ポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を定めなければならない。

（教育）

第八条　機関等は、職員等が自覚をもってポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行わなければならない。

（情報セキュリティインシデントへの対応）

第九条　機関等は、情報セキュリティインシデント（JIS Q 27000:2019 における情報

セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施しなければならない。

２　情報セキュリティインシデントの可能性を認知した者は、ポリシーに定める報告窓口に報告しなければならない。

３　ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じなければならない。

（自己点検）

第十条　機関等は、情報セキュリティ対策の自己点検を行わなければならない。

（監査）

第十一条　機関等は、対策基準が本規範及び統一基準に準拠し、かつ実際の運用が対策基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。

（情報の格付）

第十二条　機関等は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付さなければならない。

２　機関等は、機関等間での情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。

（情報の取扱制限）

第十三条　機関等は、情報の格付に応じた取扱制限を定めなければならない。

２　機関等は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。

３　機関等は、機関等間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。

（情報のライフサイクル管理）

第十四条　機関等は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施しなければならない。

（情報を取り扱う区域）

第十五条　機関等は、自組織が管理する又は自組織以外の組織から借用している施設等、自組織の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施しなければならない。

（外部委託）

第十六条　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。

２　機関等は、外部委託を実施する際に要機密情報を取り扱う場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。

３　機関等は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。

（情報システムに係る文書及び台帳整備）

第十七条　機関等は、所管する情報システムに係る文書及び台帳を整備しなければならない。

（情報システムのライフサイクル全般にわたる情報セキュリティの確保）

第十八条　機関等は、所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において、情報セキュリティを確保するための措置を定め、実施しなければならない。

（情報システムの運用継続計画）

第十九条　機関等は、所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案しなければならない。

２　機関等は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認しなければならない。

（暗号・電子署名）

第二十条　機関等は、自組織における暗号及び電子署名の利用について、必要な措置を定め、実施しなければならない。

（インターネット等を用いた行政サービスの提供）

第二十一条　機関等は、インターネット等を用いて行政サービスを提供する際には、利用者端末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に、必要な措置を定め、実施しなければならない。

（情報システムの利用）

第二十二条　機関等は、情報システムの利用に際して、情報セキュリティを確保するために職員等が行わなければならない必要な措置を定め、実施させなければならない。

（統一基準への委任）

第二十三条　本規範に定めるもののほか、本規範の実施のため必要な要件は、統一基準で定める。

附則

政府機関の情報セキュリティ対策のための統一規範（平成 23 年４月 21 日情報セキュリティ政策会議決定）は廃止する。

資料２－３

政府機関等のサイバーセキュリティ対策のための統一基準

(案)

(令和３年度版)

令和３年　月　日

サイバーセキュリティ戦略本部

資料２－３

目次

第１部　総則 1
1.1　本統一基準の目的・適用範囲 1
(1)　本統一基準の目的 1
(2)　本統一基準の適用対象 1
(3)　本統一基準の改定 1
(4)　法令等の遵守 1
(5)　対策項目の記載事項 2
1.2　情報の格付の区分・取扱制限 3
(1)　情報の格付の区分 3
(2)　情報の取扱制限 4
1.3　用語定義 6
第２部　情報セキュリティ対策の基本的枠組み 11
2.1　導入・計画 11
2.1.1　組織・体制の整備 11
(1)　最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置 11
(2)　情報セキュリティ委員会の設置 11
(3)　情報セキュリティ監査責任者の設置 11
(4)　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 11
(5)　最高情報セキュリティアドバイザーの設置 12
(6)　情報セキュリティ対策推進体制の整備 12
(7)　情報セキュリティインシデントに備えた体制の整備 12
(8)　兼務を禁止する役割 12
2.1.2　対策基準・対策推進計画の策定 13
(1)　対策基準の策定 13
(2)　対策推進計画の策定 13
2.2　運用 14
2.2.1　情報セキュリティ関係規程の運用 14
(1)　情報セキュリティ対策の運用 14
(2)　違反への対処 14
2.2.2　例外措置 15
(1)　例外措置手続の整備 15
(2)　例外措置の運用 15
2.2.3　教育 15
(1)　教育体制の整備・教育実施計画の策定 16
(2)　教育の実施 16
2.2.4　情報セキュリティインシデントへの対処 16
(1)　情報セキュリティインシデントに備えた事前準備 16
(2)　情報セキュリティインシデントへの対処 17
(3)　情報セキュリティインシデントの再発防止・教訓の共有 18

資料２－３

2.3　点検 19
2.3.1　情報セキュリティ対策の自己点検 19
(1)　自己点検計画の策定・手順の準備 19
(2)　自己点検の実施 19
(3)　自己点検結果の評価・改善 19
2.3.2　情報セキュリティ監査 20
(1)　監査実施計画の策定 20
(2)　監査の実施 20
(3)　監査結果に応じた対処 20
2.4　見直し 21
2.4.1　情報セキュリティ対策の見直し 21
(1)　情報セキュリティ関係規程の見直し 21
(2)　対策推進計画の見直し 21
第 3 部　情報の取扱い 22
3.1　情報の取扱い 22
3.1.1　情報の取扱い 22
(1)　情報の取扱いに係る規定の整備 22
(2)　情報の目的外での利用等の禁止 22
(3)　情報の格付及び取扱制限の決定・明示等 22
(4)　情報の利用・保存 23
(5)　情報の提供・公表 23
(6)　情報の運搬・送信 23
(7)　情報の消去 24
(8)　情報のバックアップ 24
3.2　情報を取り扱う区域の管理 25
3.2.1　情報を取り扱う区域の管理 25
(1)　要管理対策区域における対策の基準の決定 25
(2)　区域ごとの対策の決定 25
(3)　要管理対策区域における対策の実施 25
第 4 部　外部委託 26
4.1　業務委託 26
4.1.1　業務委託 26
(1)　業務委託に係る規定の整備 26
(2)　業務委託に係る契約 26
(3)　業務委託における対策の実施 27
(4)　業務委託における情報の取扱い 27
4.2　外部サービスの利用 29
4.2.1　要機密情報を取り扱う場合 29
(1)　外部サービスの利用に係る規定の整備 30
(2)　外部サービスの選定（クラウドサービスの場合） 30

(3)　外部サービスの選定（クラウドサービス以外の場合）……30
(4)　外部サービスの利用に係る調達・契約……31
(5)　外部サービスの利用承認……32
(6)　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……32
(7)　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……32
(8)　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……33
4.2.2　要機密情報を取り扱わない場合……33
(1)　外部サービスの利用に係る規定の整備……33
(2)　外部サービスの利用における対策の実施……33
第 5 部　情報システムのライフサイクル……35
5.1　情報システムに係る文書等の整備……35
5.1.1　情報システムに係る台帳等の整備……35
(1)　情報システム台帳の整備……35
(2)　情報システム関連文書の整備……35
5.1.2　機器等の調達に係る規定の整備……35
(1)　機器等の調達に係る規定の整備……36
5.2　情報システムのライフサイクルの各段階における対策……37
5.2.1　情報システムの企画・要件定義……37
(1)　実施体制の確保……37
(2)　情報システムのセキュリティ要件の策定……37
(3)　情報システムの構築を業務委託する場合の対策……38
(4)　情報システムの運用・保守を業務委託する場合の対策……38
5.2.2　情報システムの調達・構築……38
(1)　機器等の選定時の対策……39
(2)　情報システムの構築時の対策……39
(3)　納品検査時の対策……39
5.2.3　情報システムの運用・保守……39
(1)　情報システムの運用・保守時の対策……40
5.2.4　情報システムの更改・廃棄……40
(1)　情報システムの更改・廃棄時の対策……40
5.2.5　情報システムについての対策の見直し……40
(1)　情報システムについての対策の見直し……41
5.3　情報システムの運用継続計画……42
5.3.1　情報システムの運用継続計画の整備・整合的運用の確保……42
(1)　情報システムの運用継続計画の整備・整合的運用の確保……42
第 6 部　情報システムのセキュリティ要件……43
6.1　情報システムのセキュリティ機能……43
6.1.1　主体認証機能……43
(1)　主体認証機能の導入……43
(2)　識別コード及び主体認証情報の管理……43

6.1.2　アクセス制御機能 43
(1)　アクセス制御機能の導入 44
6.1.3　権限の管理 44
(1)　権限の管理 44
6.1.4　ログの取得・管理 44
(1)　ログの取得・管理 45
6.1.5　暗号・電子署名 45
(1)　暗号化機能・電子署名機能の導入 45
(2)　暗号化・電子署名に係る管理 46
6.2　情報セキュリティの脅威への対策 47
6.2.1　ソフトウェアに関する脆弱性対策 47
(1)　ソフトウェアに関する脆弱性対策の実施 47
6.2.2　不正プログラム対策 47
(1)　不正プログラム対策の実施 48
6.2.3　サービス不能攻撃対策 48
(1)　サービス不能攻撃対策の実施 48
6.2.4　標的型攻撃対策 49
(1)　標的型攻撃対策の実施 49
6.3　アプリケーション・コンテンツの作成・提供 50
6.3.1　アプリケーション・コンテンツの作成時の対策 50
(1)　アプリケーション・コンテンツの作成に係る規定の整備 50
(2)　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 50
6.3.2　アプリケーション・コンテンツ提供時の対策 51
(1)　政府ドメイン名の使用 51
(2)　不正なウェブサイトへの誘導防止 51
(3)　アプリケーション・コンテンツの告知 51
第 7 部　情報システムの構成要素 52
7.1　端末・サーバ装置等 52
7.1.1　端末 52
(1)　端末の導入時の対策 52
(2)　端末の運用時の対策 52
(3)　端末の運用終了時の対策 53
(4)　機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策 53
(5)　機関等支給以外の端末の導入及び利用時の対策 53
7.1.2　サーバ装置 54
(1)　サーバ装置の導入時の対策 55
(2)　サーバ装置の運用時の対策 55
(3)　サーバ装置の運用終了時の対策 55
7.1.3　複合機・特定用途機器 56

(1) 複合機 56
(2) IoT 機器を含む特定用途機器 56
7.2 電子メール・ウェブ等 57
7.2.1 電子メール 57
(1) 電子メールの導入時の対策 57
7.2.2 ウェブ 57
(1) ウェブサーバの導入・運用時の対策 57
(2) ウェブアプリケーションの開発時・運用時の対策 58
7.2.3 ドメインネームシステム（DNS） 58
(1) DNS の導入時の対策 59
(2) DNS の運用時の対策 59
7.2.4 データベース 59
(1) データベースの導入・運用時の対策 59
7.3 通信回線 61
7.3.1 通信回線 61
(1) 通信回線の導入時の対策 61
(2) 通信回線の運用時の対策 62
(3) 通信回線の運用終了時の対策 62
(4) 無線 LAN 環境導入時の対策 62
7.3.2 IPv6 通信回線 63
(1) IPv6 通信を行う情報システムに係る対策 63
(2) 意図しない IPv6 通信の抑止・監視 63
第 8 部 情報システムの利用 64
8.1 情報システムの利用 64
8.1.1 情報システムの利用 64
(1) 情報システムの利用に係る規定の整備 64
(2) 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 64
(3) 情報システムの利用時の基本的対策 65
(4) 電子メール・ウェブの利用時の対策 65
(5) 識別コード・主体認証情報の取扱い 66
(6) 暗号・電子署名の利用時の対策 66
(7) 不正プログラム感染防止 66
(8) Web 会議サービスの利用時の対策 66
8.1.2 ソーシャルメディアサービスによる情報発信 67
(1) ソーシャルメディアサービスによる情報発信時の対策 67
8.1.3 テレワーク 68
(1) 実施規定の整備 68
(2) 実施環境における対策 68
(3) 実施時における対策 68

第1部 総則

1.1 本統一基準の目的・適用範囲

(1) 本統一基準の目的

情報セキュリティの基本は、機関等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、それぞれの機関等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。

本統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策であり、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必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的とする。

(2) 本統一基準の適用対象

(a) 本統一基準において適用対象とする者は、全ての職員等とする。

(b) 本統一基準において適用対象とする情報は、以下の情報とする。

(ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供する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。）

(イ) その他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、職員等が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、機関等が調達し、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

(c) 本統一基準において適用対象とする情報システムは、本統一基準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。

(3) 本統一基準の改定

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。

このため、情報技術の進歩に応じて、本統一基準を定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、本統一基準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。なお、これらの関連法令等は情報

セキュリティ対策にかかわらず当然に遵守すべきものであるため、本統一基準では、あえて関連法令等の遵守について明記していない。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こと。

(5) 対策項目の記載事項

本統一基準では、機関等が行うべき対策について、目的別に部、節及び款の３階層にて対策項目を分類し、各款に対して目的及び趣旨並びに遵守事項を示している。

内閣官房内閣サイバーセキュリティセンターが別途策定する政府機関等の対策基準策定のためのガイドラインには、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）が例示されるとともに、対策基準の策定及び実施に際しての考え方等が解説されている。基本対策事項は遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要がある。

さらに、機関等は策定した対策基準で定める対策を実施するための、実施手順を整備する必要がある。

1.2　情報の格付の区分・取扱制限

(1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、本統一基準の遵守事項で用いる格付の区分の定義を示す。

なお、機関等において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本統一基準の遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。また、他機関等へ情報を提供する場合は、自組織の対策基準における格付区分と本統一基準における格付区分の対応について、適切に伝達する必要がある。

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	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性２情報	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 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 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う

	情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報

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。

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	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（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。

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

「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職員等に確実に行わせるための手段をいう。

職員等は、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。機関等は、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必要がある。

1.3 用語定義

統一基準において次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

- 「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」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。

- 「Web（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」とは、機関等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関等の情報が取り扱われる場合に限る。

- 「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」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関等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」とは、外部サービスを利用する機関等の職員等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。

- 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。

- 「機関等内通信回線」とは、一つの機関等が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該機関等の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。機関等内通信回線には、専用線や VPN 等物理的な回線を機関等が管理していないものも含まれる。

- 「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。

- 「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

つの機関等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」とは、機関等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関等の情報を取り扱わせる場合に限る。

● 「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。

● 「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。

● 「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、機関等が調達又は開発するものをいう。

● 「CYMAT（サイマット）」とは、サイバー攻撃等により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。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。

● 「CSIRT（シーサート）」とは、機関等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、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。

● 「実施手順」とは、対策基準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」とは、「1.1(2) 本統一基準の適用対象」の(b)に定めるものをいう。

● 「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、機関等が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

● 「情報セキュリティインシデント」とは、JIS Q 27000:2019 における情報セキュリティインシデントをいう。

● 「情報セキュリティ関係規程」とは、対策基準及び実施手順を総称したものをいう。

● 「情報セキュリティ対策推進体制」とは、機関等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、当該機関等に設置された体制をいう。

● 「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。

● 「職員等」とは、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の管理対象である情報及び情報システムを取り扱う者をいう。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

● 「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】

● 「対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。

● 「端末」とは、情報システムの構成要素である機器のうち、職員等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、機関等が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機関等が調達又は開発するもの以外を指す「機関等支給以外の端末」がある。また、機関等が調達又は開発した端末と機関等支給以外の端末の双方を合わせて「端末

（支給外端末を含む）」という。

● 「通信回線」とは、複数の情報システム又は機器等（機関等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、機関等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、機関等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。

● 「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、ルータ等のほか、ファイアウォール等も含まれる。

● 「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」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。

【は】

● 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「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」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。

【や】

● 「要管理対策区域」とは、機関等の管理下にある区域（機関等が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

第2部 情報セキュリティ対策の基本的枠組み

2.1　導入・計画

2.1.1　組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての職員等が、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、統一基準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統一基準に定める責任者に担わせることができる。

遵守事項

(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置

(a) 機関等は、機関等における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者１人を置くこと。

(b) 機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置くこと。

(2) 情報セキュリティ委員会の設置

(a) 最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。

(3) 情報セキュリティ監査責任者の設置

(a) 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、情報セキュリティ監査責任者１人を置くこと。

(4) 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

(a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこと。そのうち、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及び最高情報セキュリティ副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人を選任すること。

(b) 情報セキュリティ責任者は、遵守事項 3.2.1(2)(a)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事務を統括する区域情報セキュリティ責任者 1 人を置くこと。

(c) 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事務を統括する課室情報セキュリティ責任者 1 人を置くこと。

(d) 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事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任すること。

(5) 最高情報セキュリティアドバイザーの設置

(a) 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こと。

(6) 情報セキュリティ対策推進体制の整備

(a) 最高情報セキュリティ責任者は、機関等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こと。

(b) 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こと。

(7) 情報セキュリティインシデントに備えた体制の整備

(a) 最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化すること。

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

(c) 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こと。

(d) 最高情報セキュリティ責任者は、CYMAT に属する職員を指名すること。（国の行政機関に限る。）

(8) 兼務を禁止する役割

(a) 職員等は、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こと。

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

(イ) 監査を受ける者とその監査を実施する者

(b) 職員等は、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、承認等を得ること。

2.1.2 対策基準・対策推進計画の策定

目的・趣旨

機関等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、機関等として遵守すべき対策の基準を、情報セキュリティに係るリスク評価の結果等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。

遵守事項

(1) 対策基準の策定

(a) 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、統一基準に準拠した対策基準を定めること。また、対策基準は、機関等の業務、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こと。

(2) 対策推進計画の策定

(a) 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。）を定めること。また、対策推進計画には、機関等の業務、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こと。

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) 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

(オ) 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

2.2　運用

2.2.1　情報セキュリティ関係規程の運用

目的・趣旨

機関等は、対策基準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。

遵守事項

(1) 情報セキュリティ対策の運用

(a) 統括情報セキュリティ責任者は、機関等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（本統一基準で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、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こと。

(b) 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こと。

(c) 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こと。

(d) 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関係規程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こと。

(e) 統括情報セキュリティ責任者は、情報セキュリティ関係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こと。

(2) 違反への対処

(a) 職員等は、情報セキュリティ関係規程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こと。

(b) 情報セキュリティ責任者は、情報セキュリティ関係規程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こと。

2.2.2 例外措置

目的・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、情報セキュリティ関係規程の適用が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。

遵守事項

(1) 例外措置手続の整備

(a) 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（以下本款において「許可権限者」という。）及び審査手続を定めること。

(b) 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こと。

(2) 例外措置の運用

(a) 職員等は、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こと。ただし、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、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定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こと。

(b) 許可権限者は、職員等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こと。

(c) 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こと。

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

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が職員等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、全ての職員等が、情報セキュリティ関係規程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、機関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。

遵守事項

(1) 教育体制の整備・教育実施計画の策定

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

(b) 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こと。

(2) 教育の実施

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

(b) 職員等は、教育実施計画に従って、適切な時期に教育を受講すること。

(c) 課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講させること。また、国の行政機関における課室情報セキュリティ責任者は、CYMAT に属する職員にも教育を適切に受講させること。

(d) 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こと。

(e) 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こと。

2.2.4 情報セキュリティインシデントへの対処

目的・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。

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

(a) 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関等関係者への報告手順を整備し、報告が必要な具体例を含め、職員等に周知すること。

(b) 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機関等外との情報共有を含む対処手順を整備すること。

(c) 統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

(d) 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。

(e) 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関等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関等外の者に明示すること。

(f) 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こと。

(2) 情報セキュリティインシデントへの対処

(a) 職員等は、情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告し、指示に従うこと。

(b) 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こと。

(c) 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こと。

(d) 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こと。

(e) 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、機関等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、適切に対処すること。

(f) 情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが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、適切に対処すること。

(g) 国の行政機関における CSIRT は、当該機関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、内閣官房内閣サイバーセキュリティセンターに連絡すること。また、独立行政法人及び指定法人における CSIRT は、当該法人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、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関における CSIRT は、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。

(h) 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・連絡等を行うこと。

(i) 国の行政機関における CSIRT は、認知した情報セキュリティインシデント又は独立行政法人及び指定法人から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「大規模サイバ

一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こと。

(j) 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こと。

(k) 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こと。

(l) CSIRT は、情報セキュリティインシデントに関して、機関等を含む関係機関と情報共有を行うこと。

(m) CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。

(3) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 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こと。

(b) 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こと。

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

2.3　点検

2.3.1　情報セキュリティ対策の自己点検

目的・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、情報セキュリティ関係規程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、職員等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。

遵守事項

(1) 自己点検計画の策定・手順の準備

(a) 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こと。

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

(c) 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こと。

(2) 自己点検の実施

(a) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示すること。

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

(3) 自己点検結果の評価・改善

(a) 情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。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こと。

(b) 統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。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こと。

(c) 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こと。

2.3.2 情報セキュリティ監査

目的・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。

遵守事項

(1) 監査実施計画の策定

(a) 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こと。

(b) 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こと。

(2) 監査の実施

(a) 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監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告すること。

(ア) 対策基準に統一基準を満たすための適切な事項が定められていること

(イ) 実施手順が対策基準に準拠していること

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

(3) 監査結果に応じた対処

(a) 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こと。

(b) 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、機関等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こと。

(c) 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こと。

2.4　見直し

2.4.1　情報セキュリティ対策の見直し

目的・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、機関等の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、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基準及び対策推進計画に反映することも重要である。

遵守事項

(1) 情報セキュリティ関係規程の見直し

(a) 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、対策基準について必要な見直しを行うこと。

(b) 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こと。

(2) 対策推進計画の見直し

(a) 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、対策推進計画について定期的な見直しを行うこと。

第3部 情報の取扱い

3.1　情報の取扱い

3.1.1　情報の取扱い

目的・趣旨

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職員等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、職員等は、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。

なお、国の行政機関における秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本統一基準の規定に基づき、適切に情報が取り扱われるよう留意すること。また、独立行政法人及び指定法人における機密性３情報の管理に関しては、本統一基準の規定に基づき対策を講ずること。

遵守事項

(1) 情報の取扱いに係る規定の整備

(a) 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、職員等へ周知すること。

（ア） 情報の格付及び取扱制限についての定義

（イ） 情報の格付及び取扱制限の明示等についての手続

（ウ） 情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報の目的外での利用等の禁止

(a) 職員等は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等すること。

(3) 情報の格付及び取扱制限の決定・明示等

(a) 職員等は、情報の作成時及び機関等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、明示等すること。

(b) 職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

(c) 職員等は、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（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと。

(4) 情報の利用・保存

(a) 職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ること。

(c) 職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。

(d) 職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、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こと。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

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

(イ) 当該情報に対し、暗号化による保護を行うこと。

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

(e) 職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

(5) 情報の提供・公表

(a) 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こと。

(b) 職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

(c) 独立行政法人及び指定法人における職員等は、機密性３情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。

(d) 職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

(6) 情報の運搬・送信

(a) 職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち

出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

(b) 職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

(7) 情報の消去

(a) 職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

(b) 職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

(c) 職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

(8) 情報のバックアップ

(a) 職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

(b) 職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。

(c) 職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

3.2　情報を取り扱う区域の管理

3.2.1　情報を取り扱う区域の管理

目的・趣旨

サーバ装置、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。

遵守事項

(1) 要管理対策区域における対策の基準の決定

(a) 統括情報セキュリティ責任者は、要管理対策区域の範囲を定めること。

(b) 統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

(ア) 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。

(イ) 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。

(2) 区域ごとの対策の決定

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

(b) 区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

(3) 要管理対策区域における対策の実施

(a) 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こと。職員等が実施すべき対策については、職員等が認識できる措置を講ずること。

(b) 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こと。

(c) 職員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、職員等が機関等外の者を立ち入らせる際には、当該機関等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こと。

第4部 外部委託

4.1　業務委託

4.1.1　業務委託

目的・趣旨

機関等外の者に、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、職員等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）

遵守事項

(1) 業務委託に係る規定の整備

(a) 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こと。

(ア) 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。）

(イ) 委託先の選定基準

(2) 業務委託に係る契約

(a) 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業務委託を実施すること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託

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こと。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こと。

（ア） 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

（イ） 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

（ウ） 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、機関等の意図せざる変更が加えられないための管理体制

（エ） 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

（オ） 情報セキュリティインシデントへの対処方法

（カ） 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

（キ） 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

(c) 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、必要に応じて以下の内容を仕様に含めること。

（ア） 情報セキュリティ監査の受入れ

（イ） サービスレベルの保証

(d) 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、上記(b)(c)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関等に提供し、機関等の承認を受けるよう、仕様内容に含めること。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こと。

(3) 業務委託における対策の実施

(a) 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こと。

(b) 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こと。

(c) 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、又は抹消されたことを確認すること。

(4) 業務委託における情報の取扱い

(a) 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こと。

（ア） 委託先に要保護情報を提供する場合は、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。

(イ) 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。

(ウ) 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。

4.2　外部サービスの利用

4.2.1　要機密情報を取り扱う場合

目的・趣旨

政府機関において今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

機関等が外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用する可能性があり、自身を含む他の利用者にも関係する情報の開示を受けることが困難になる場合もある。機関等が外部サービスを利用して要機密情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、機関等による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、機関等と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に早いサイクルで変化しており、利用開始時に行ったセキュリティ対策が途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。

＜外部サービスの例＞

- クラウドサービス
- Ｗｅｂ会議サービス
- ＳＮＳ（ソーシャルネットワーキングサービス）
- 検索サービス、翻訳サービス、地図サービス
- ホスティングサービス
- インターネット回線接続サービス

なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない。

遵守事項

(1) 外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む外部サービス（要機密情報を取り扱う場合）の利用に関する規定を整備すること。

(ア) 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 4.2 節において「外部サービス利用判断基準」という。）

(イ) 外部サービス提供者の選定基準

(ウ) 外部サービスの利用申請の許可権限者と利用手続

(エ) 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

(2) 外部サービスの選定（クラウドサービスの場合）

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

(b) 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外部サービス提供者を選定すること。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こと。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びに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、外部サービスを選定すること。

(3) 外部サービスの選定（クラウドサービス以外の場合）

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

(b) 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外部サービス提供者を選定すること。また、以下の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こと。

(ア) 外部サービスの利用を通じて機関等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

(イ) 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

(ウ) 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、機関等の意図せざる変更が加えられないための管理体制

(エ) 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

（オ） 情報セキュリティインシデントへの対処方法

（カ） 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

（キ） 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

(c) 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こと。

(d) 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、外部サービスの利用を通じて機関等が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外部サービス提供者の選定条件に含めること。

（ア） 情報セキュリティ監査の受入れ

（イ） サービスレベルの保証

(e) 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、外部サービスの利用を通じて機関等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、必要に応じて機関等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こと。

(f) 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関等に提供し、機関等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こと。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こと。

(g) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限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こと。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こと。

(h) 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こと。

(i) 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、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こと。

(4) 外部サービスの利用に係る調達・契約

(a) 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こと。

(b) 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こと。

(5) 外部サービスの利用承認

(a) 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こと。

(b) 利用申請の許可権限者は、職員等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こと。

(c) 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こと。

(6) 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

(a) 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、以下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こと。

(ア) 不正なアクセスを防止するためのアクセス制御

(イ) 取り扱う情報の機密性保護のための暗号化

(ウ) 開発時におけるセキュリティ対策

(エ) 設計・設定時の誤りの防止

(b) 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・記録すること。

(7) 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

(a) 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、以下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こと。

(ア) 外部サービス利用方針の規定

(イ) 外部サービス利用に必要な教育

(ウ) 取り扱う資産の管理

(エ) 不正アクセスを防止するためのアクセス制御

(オ) 取り扱う情報の機密性保護のための暗号化

(カ) 外部サービス内の通信の制御

(キ) 設計・設定時の誤りの防止

(ク) 外部サービスを利用した情報システムの事業継続

(b) 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こと。

(c) 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・記録すること。

(8) 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

(a) 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、以下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こと。

(ア) 外部サービスの利用終了時における対策

(イ) 外部サービスで取り扱った情報の廃棄

(ウ) 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

(b) 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・記録すること。

4.2.2 要機密情報を取り扱わない場合

目的・趣旨

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ない場合においても、種々の情報を機関等から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て利用することが求められる。一方、要機密情報を取り扱う場合と同等のセキュリティ対策を求めることは外部サービスの利用推進を妨げるものであるため、要機密情報を取り扱わない前提で外部サービスを利用する場合は、本款で定めた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。

遵守事項

(1) 外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備すること。

(ア) 外部サービスを利用可能な業務の範囲

(イ) 外部サービスの利用申請の許可権限者と利用手続

(ウ) 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

(エ) 外部サービスの利用の運用手順

(2) 外部サービスの利用における対策の実施

(a) 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こと。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こと。

(b) 利用申請の許可権限者は、職員等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こと。また、承認した外部サービスを記録すること。

第5部 情報システムのライフサイクル

5.1 情報システムに係る文書等の整備

5.1.1 情報システムに係る台帳等の整備

目的・趣旨

機関等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、機関等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。

遵守事項

(1) 情報システム台帳の整備

(a) 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こと。

(b) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム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こと。

(2) 情報システム関連文書の整備

(a) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

(イ) 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

(ウ) 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

(エ) 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

5.1.2 機器等の調達に係る規定の整備

目的・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、対策基準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。

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 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こと。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、その管理を機関等が確認できることを加えること。

(b) 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こと。

5.2　情報システムのライフサイクルの各段階における対策

5.2.1　情報システムの企画・要件定義

目的・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、4.1「業務委託」についても併せて遵守する必要がある。

遵守事項

(1) 実施体制の確保

(a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めること。

(b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機関等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こと。

(c) 最高情報セキュリティ責任者は、前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。

(2) 情報システムのセキュリティ要件の策定

(a) 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（外部サービスを含む。）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こと。

(ア) 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
(イ) 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)
(ウ) 情報システムに関連する脆弱性についての対策要件

(b) 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こと。

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

(d) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの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こと。

(3) 情報システムの構築を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、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、適切に実施させること。
(ア) 情報システムのセキュリティ要件の適切な実装
(イ) 情報セキュリティの観点に基づく試験の実施
(ウ) 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

(4) 情報システムの運用・保守を業務委託する場合の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。

(b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させること。

5.2.2 情報システムの調達・構築

目的・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。

遵守事項

(1) 機器等の選定時の対策

(a) 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、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こと。

(2) 情報システムの構築時の対策

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

(b) 情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

(3) 納品検査時の対策

(a) 情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、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こと。

(b) 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こと。

5.2.3 情報システムの運用・保守

目的・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、対策基準に基づ

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。

遵守事項

(1) 情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

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

(c) 情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

5.2.4 情報システムの更改・廃棄

目的・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。

遵守事項

(1) 情報システムの更改・廃棄時の対策

(a) 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。

（ア） 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

（イ） 情報システム廃棄時の不要な情報の抹消

5.2.5 情報システムについての対策の見直し

目的・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。

遵守事項

(1) 情報システムについての対策の見直し

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

5.3　情報システムの運用継続計画

5.3.1　情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民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、国の行政機関においては、府省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。独立行政法人及び指定法人においても、業務の特性に応じて、中期目標による指示等により、法人の業務継続計画と情報システムの運用継続計画を策定し運用している。

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、情報セキュリティ関係規程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。

遵守事項

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 統括情報セキュリティ責任者は、機関等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こと。

(b) 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こと。

第6部 情報システムのセキュリティ要件

6.1　情報システムのセキュリティ機能

6.1.1　主体認証機能

目的・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、機関等の情報システムにおいて、国民向けのサービスを提供する場合は、国民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。

遵守事項

(1) 主体認証機能の導入

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

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

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

(2) 識別コード及び主体認証情報の管理

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

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

6.1.2　アクセス制御機能

目的・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。

遵守事項

(1) アクセス制御機能の導入

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

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

6.1.3 権限の管理

目的・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。

遵守事項

(1) 権限の管理

(a) 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

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

6.1.4 ログの取得・管理

目的・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。

遵守事項

(1) ログの取得・管理

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

(b) 情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、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こと。

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

6.1.5 暗号・電子署名

目的・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。

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

(ア) 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。

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

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」

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こと。

(ア) 職員等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。

(イ) 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。

(ウ) 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。

(エ) 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。

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

(2) 暗号化・電子署名に係る管理

(a) 情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。

(ア) 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。

(イ) 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、職員等と共有を図ること。

6.2　情報セキュリティの脅威への対策

6.2.1　ソフトウェアに関する脆弱性対策

目的・趣旨

機関等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関等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関等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、機関等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、5.2.2「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。

遵守事項

(1)　ソフトウェアに関する脆弱性対策の実施

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

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

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

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

6.2.2　不正プログラム対策

目的・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。

遵守事項

(1) 不正プログラム対策の実施

(a) 情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ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。

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

(c) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

6.2.3 サービス不能攻撃対策

目的・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、機関等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。近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている。

遵守事項

(1) サービス不能攻撃対策の実施

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

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

(c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から

監視対象を特定し、監視すること。

6.2.4 標的型攻撃対策

目的・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。

近年は攻撃対象の組織に対する直接的な攻撃だけでなく、委託先等の関連組織への間接的な攻撃も確認されており、より幅広い対策の検討が求められる。

遵守事項

(1) 標的型攻撃対策の実施

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

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

6.3　アプリケーション・コンテンツの作成・提供

6.3.1　アプリケーション・コンテンツの作成時の対策

目的・趣旨

機関等では、情報の提供、行政手続、意見募集等の行政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。機関等は、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、4.1.1「業務委託」についても併せて遵守する必要がある。

遵守事項

(1) アプリケーション・コンテンツの作成に係る規定の整備

(a) 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関等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こと。

(2) 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

(a) 情報システムセキュリティ責任者は、機関等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こと。

(ア) 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。

(イ) 提供するアプリケーションが脆弱性を含まないこと。

(ウ) 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。

(エ) 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をアプリケーション・コンテンツの提供先に与えること。

(オ) 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。

(カ) 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、サービス利用に当たって必須ではない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。

(b) 職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項各号に掲げる内容を調達仕様に含めること。

6.3.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

機関等では、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を用意し、国民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、国民等にとっては、そのサービスが実際の機関等のものであると確認できることが重要である。また、機関等になりすましたウェブサイトを放置しておくと、機関等の信用を損なうだけでなく、国民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。

遵守事項

(1) 政府ドメイン名の使用

(a) 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。ただし、次に掲げる場合を除く。

(ア) 指定法人が政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。

(イ) 独立行政法人及び指定法人のうち教育機関である法人が、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、当該法人は、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を使用するべきかを比較考慮の上、判断すること。

(ウ) 8.1.2(1)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

(b) 職員等は、機関等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(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。

(2) 不正なウェブサイトへの誘導防止

(a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機関等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こと。

(3) アプリケーション・コンテンツの告知

(a) 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こと。

(b) 職員等は、機関等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 等の有効性を保つこと。

第7部 情報システムの構成要素

7.1　端末・サーバ装置等

7.1.1　端末

目的・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、職員等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。端末のモバイル利用に当たっては、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。

また、機関等の業務の遂行においては、機関等から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず機関等支給以外の端末を利用して情報処理を行う場合も考えられるが、この際、当該端末の情報セキュリティ水準が対策基準を満たさないおそれがある。このため、機関等支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で、職員等に対して機関等における厳格な管理の下で利用させることが必要である。

なお、本款の遵守事項のほか、6.1「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、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「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。

遵守事項

(1) 端末の導入時の対策

(a) 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こと。

(b) 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こと。

(2) 端末の運用時の対策

(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

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

合には、改善を図ること。

(3) 端末の運用終了時の対策

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

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

(a) 統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）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こと。

(b) 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関等が支給する端末（要管理対策区域外で使用する場合に限る）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こと。

(c) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する端末を機関等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、当該端末から機関等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。

(d) 情報システムセキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）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こと。

(5) 機関等支給以外の端末の導入及び利用時の対策

(a) 最高情報セキュリティ責任者は、機関等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、機関等が講じる安全管理措置、当該端末の管理は機関等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、機関等における機関等支給以外の端末の利用の可否を判断すること。

(b) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等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こと。

(c) 統括情報セキュリティ責任者は、職員等が機関等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こと。

(d) 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関等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こと。

(ア) 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

（イ） 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

(e) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を機関等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、当該端末から機関等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。

(f) 情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等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。）を定めること。

(g) 端末管理責任者は、職員等が機関等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(d)(ア)の安全管理措置を講ずること。

(h) 端末管理責任者は、要機密情報を取り扱う機関等支給以外の端末について、前項の規定にかかわらず本条(d)(ア)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(d)(イ)に定める安全管理措置を職員等に講じさせること。

(i) 職員等は、要機密情報を取り扱う機関等支給以外の端末について、前項において本条(d)(ア)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(d)(イ)に定める安全管理措置を講ずること。

(j)職員等は、機関等支給以外の端末を用いて機関等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こと。

(k) 職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。

7.1.2 サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、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。仮に機関等が利用するサーバ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、国民からの信頼を大きく損なう。加えて、サーバ装置は、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、本款の遵守事項のほか、6.1「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、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、6.2.3「サービス不能攻撃対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうちサーバ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、ウェブサーバ、DNS サーバ及びデータ

ベースについては、本款での共通的な対策に加え、それぞれ 7.2「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。

遵守事項

(1) サーバ装置の導入時の対策

(a) 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こと。

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

(c) 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こと。

(d) 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こと。

(2) サーバ装置の運用時の対策

(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

(b) 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こと。

(c) 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。

(d) 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となるよう、必要な措置を講ずること。

(3) サーバ装置の運用終了時の対策

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

7.1.3 複合機・特定用途機器

目的・趣旨

機関等においては、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、機関等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、機関等においては、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。

遵守事項

(1) 複合機

(a) 情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。

(b) 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こと。

(c) 情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

(2) IoT 機器を含む特定用途機器

(a) 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こと。

7.2　電子メール・ウェブ等

7.2.1　電子メール

目的・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職員等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の管理が必要である。

なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ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。

遵守事項

(1) 電子メールの導入時の対策

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

(b) 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こと。

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

(d) 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こと。

7.2.2　ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、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、7.1.2「サーバ装置」において定めるサーバ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。

遵守事項

(1) ウェブサーバの導入・運用時の対策

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

(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。
(イ) 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。
(ウ) 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。
(エ) 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。
(オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。

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

(2) ウェブアプリケーションの開発時・運用時の対策

(a) 情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

7.2.3 ドメインネームシステム（DNS）

目的・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、機関等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に対して問合せを行うキャッシュサーバが存在する。キャッシュサーバ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 サーバの適切な管理が必要である。

なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ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。

遵守事項

(1) DNS の導入時の対策

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

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

(c) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等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こと。

(2) DNS の運用時の対策

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

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

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

7.2.4 データベース

目的・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職員等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、6.1「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、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「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。

遵守事項

(1) データベースの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、データベースに対する内部不正を防止する

ため、管理者アカウントの適正な権限管理を行うこと。

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

(c) 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、対策を講ずること。

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

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

7.3　通信回線

7.3.1　通信回線

目的・趣旨

サーバ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。

遵守事項

(1) 通信回線の導入時の対策

(a) 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こと。

(b) 情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

(c) 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こと。

(d) 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こと。機関等内通信回線へ機関等支給以外の端末を接続する際も同様とする。

(e) 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こと。

(f) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

(g) 情報システムセキュリティ責任者は、機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するた

めの措置を講ずること。

(h) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずること。

(i) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

(j) 情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。

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

(2) 通信回線の運用時の対策

(a) 情報システム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こと。

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

(c) 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、改善を図ること。

(d) 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こと。

(3) 通信回線の運用終了時の対策

(a) 情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。

(4) 無線 LAN 環境導入時の対策

(a) 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等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こと。

7.3.2 IPv6 通信回線

目的・趣旨

政府機関において、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、機関等においても、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。

遵守事項

(1) IPv6 通信を行う情報システムに係る対策

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

(b) 情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

(ア) 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

(イ) 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

(ウ) 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

(エ) 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

(2) 意図しない IPv6 通信の抑止・監視

(a) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

目的・趣旨

職員等は、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、職員等は規定に従って利用することが求められる。

なお、機関等が支給する端末（要管理対策区域外で使用する場合に限る）に係る規定の整備については遵守事項 7.1.1(4)、機関等支給以外の端末に係る規定の整備については遵守事項 7.1.1(5)をそれぞれ参照すること。

遵守事項

(1) 情報システムの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、機関等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こと。

(b) 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こと。当該手順には、以下の事項を含めること。

（ア） 職員等は、国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体、又は本項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関等との間で取り決めた機関等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。

（イ） 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こと。

(c) 統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めること。

(2) 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

(a) 情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

(3) 情報システムの利用時の基本的対策

(a) 職員等は、業務の遂行以外の目的で情報システムを利用しないこと。

(b) 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機関等の情報システムを接続しないこと。

(c) 職員等は、機関等内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。

(d) 職員等は、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、情報システムセキュリティ責任者の承認を得ること。

(e) 職員等は、接続が許可されていない機器等を情報システムに接続しないこと。

(f) 職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

(g) 職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

(h) 職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

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

(イ) 機関等支給以外の端末 要保護情報

(i) 職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、定められた安全管理措置を講ずること。

(j) 職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、課室情報セキュリティ責任者の許可を得ること。

(k) 職員等は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、課室情報セキュリティ責任者の許可を得ること。

(4) 電子メール・ウェブの利用時の対策

(a) 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、それぞれの機関等が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。

(b) 職員等は、機関等外の者と電子メールにより情報を送受信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、次に掲げる場合は除く。

(ア) 指定法人が、政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。

(イ) 独立行政法人及び指定法人のうち教育機関である法人が、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。

（ウ） 電子メールを受信する機関等外の者が、職員等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二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。）。

(c) 職員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

(d) 職員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

(e) 職員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

(f) 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、以下の事項を確認すること。

（ア） 送信内容が暗号化されること

（イ） 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

(5) 識別コード・主体認証情報の取扱い

(a) 職員等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

(b) 職員等は、自己に付与された識別コードを適切に管理すること。

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

(d) 職員等は、自己の主体認証情報の管理を徹底すること。

(6) 暗号・電子署名の利用時の対策

(a) 職員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

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

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

(7) 不正プログラム感染防止

(a) 職員等は、不正プログラム感染防止に関する措置に努めること。

(b) 職員等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

(8) Web 会議サービスの利用時の対策

(a) 職員等は、機関等の定める利用手順に従い、Web 会議の参加者や取り扱う情報に

応じた情報セキュリティ対策を実施すること。

(b) 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

8.1.2 ソーシャルメディアサービスによる情報発信

目的・趣旨

機関等においても、積極的な広報活動等を目的としたソーシャルメディアサービスの利用が一般的になっている。しかし、民間事業者等により提供されているソーシャルメディアサービスでは政府ドメイン名を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、機関等のアカウントを乗っ取られた場合や、利用しているソーシャルメディアサービスが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民等に提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

また、このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアサービスは、定型的な約款や利用規約等への同意のみで利用可能となる一方、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことは困難であることが一般的である。このことから、ソーシャルメディアサービスの利用は、要機密情報を取り扱わず、委託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限るものとする。

遵守事項

(1) ソーシャルメディアサービスによる情報発信時の対策

(a) 統括情報セキュリティ責任者は、機関等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こと。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こと。

(ア) 機関等のアカウントによる情報発信が実際の機関等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。

(イ) 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。

(b) 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、機関等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こと。

8.1.3 テレワーク

目的・趣旨

働き方改革実行計画（平成 29 年 3 月 28 日　働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、職員等が業務を遂行する上で、必ずしも勤務官署に出勤する必要はなく、自宅やサテライトオフィス等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模感染症の感染予防対策として、勤務官署への出勤が抑制されるような状況下では、大半の職員等が勤務官署以外から業務を遂行できるようにテレワーク環境の整備が必要となる。

本款では、テレワークの実施に特に必要な対策についてのみ規定しているため、本款以外に、3.1.1「情報の取扱い」、7.3.1「通信回線」及び 8.1.1「情報システムの利用」の各款、遵守事項 7.1.1(4)「機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策」及び遵守事項 7.1.1(5)「機関等支給以外の端末の導入及び利用時の対策」も参照すること。

遵守事項

(1) 実施規定の整備

(a) 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関等が支給する端末で行うよう定めること。

(2) 実施環境における対策

(a) 情報システムセキュリティ責任者は、テレワークの実施により機関等外通信回線を経由して機関等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こと。

(b) 情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行うこと。

(c) 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じること。

(d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。

(3) 実施時における対策

(a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等がチェックするべき項目を定め、職員等に当該チェックを実施させること。

(b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。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こと。

(c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な

機関等外通信回線を利用してテレワークを行わないこと。

資料２－４

政府機関等のサイバーセキュリティ対策の運用等に関する指針（案）

平成 28 年８月 31 日
平成 30 年７月 25 日改定
平成 31 年４月１日改定
令和３年　月　日改定
サイバーセキュリティ戦略本部決定

１　本指針の目的

本指針は、サイバーセキュリティ基本法（平成 26 年法律第 104 号。以下「法」という。）第 26 条第１項第２号に定める国の行政機関、独立行政法人（独立行政法人通則法（平成 11 年法律第 103 号）第２条第１項に規定する法人をいう。以下同じ。）及び指定法人（法第 13 条に規定する指定法人をいう。以下同じ。）（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準の運用に関して、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）における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。以下「統一規範」という。）及び政府機関等のサイバーセキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の案の策定、政府機関等の対策基準策定のためのガイドライン（NISC 決定。以下「対策基準策定ガイドライン」という。）の策定、独立行政法人及び指定法人における情報セキュリティ対策の運用並びに複数の機関等で共通的に使用する情報システム（一つの機関等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。以下「基盤となる情報システム」という。）に関する情報セキュリティ対策の運用のために必要な事項を定めるものである。

２　統一基準群の策定

統一基準群は、統一規範、統一基準、本指針及び対策基準策定ガイドラインの総称をいい、統一規範、統一基準及び本指針の原案は、NISC が策定し、サイバーセキュリティ対策推進会議（平成 27 年２月 10 日サイバーセキュリティ戦略本部長決定）を経てサイバーセキュリティ戦略本部において決定する。また、対策基準策定ガイドラインは、国の行政機関と協議の上、NISC において決定する。

なお、NISC は、新たな脅威の発生や機関等における運用の状況を定期的に点検した結果を踏まえ、次の点に留意の上、原案の策定を行う。

(1)　統一規範及び統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策を包含するものとし、責任体制、実施体制及び対策内容について、機関等が準拠できるよう、実状を踏まえるとともに、国際的な基

準等との整合性に配慮の上、策定する。統一基準には、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定する。

(2)　対策基準策定ガイドラインは、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、機関等による対策基準の策定及び実施に際しての考え方等を解説することを目的として策定する。基本対策事項は遵守事項に対応するものであるため、機関等は対策基準策定ガイドラインを参照し、基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要があるものである。

３　独立行政法人及び指定法人の情報セキュリティ対策に係る主務大臣等の責務

(1)　導入・計画

独立行政法人を所管する主務大臣は、独立行政法人通則法（平成 11 年法律第 103 号）第 29 条第１項の規定により指示した同項の中期目標、第 35 条の４第１項の規定により指示した同項の中長期目標又は第 35 条の９第１項の規定により指示した同項の年度目標に、統一基準群に基づいて定めたポリシーに従って情報セキュリティ対策を講ずる旨を盛り込むこととする。指定法人に対しては、個別の根拠法に基づき、当該指定法人を所管する国の行政機関が必要な情報セキュリティ対策についての指導等を実施する。

(2)　評価

独立行政法人を所管する主務大臣は、独立行政法人通則法に基づく業務の実績等に関する評価の際に、情報セキュリティ対策の実施状況に関しても評価を行い、評価結果を公表する。指定法人を所管する国の行政機関は、当該指定法人に対して、個別の根拠法に基づき、情報セキュリティ対策の実施状況に関して評価を行う。

独立行政法人及び指定法人の情報セキュリティ対策に係る評価の結果に関しては、NISC においても確認し、必要に応じてこれら法人を所管する国の行政機関に対して助言等を行う。

４　共通的に使用する情報システムにおける情報セキュリティ対策

基盤となる情報システムについては、これを使用する各機関等の情報システムと連携して運用管理を行うものであることから、各機関等の間での情報セキュリティ対策の遺漏防止を図る必要がある。また、基盤となる情報システムと連携する一部の情報システムにおける情報セキュリティインシデントが他の情報システムに影響を及ぼす可能性等も踏まえ、情報セキュリティマネジメントを適切に実行し、情報システム全体としての情報セキュリティ水準を適切に確保しなければならない。

このため、基盤となる情報システムの整備・運用管理を行う機関等及び基盤となる情報システムと連携する情報システムを管理する機関等（以下「整備・運用管理

機関等」という。）は、基盤となる情報システムの運用管理を行う体制を整備するに当たっては、各機関等の責任と役割分担を明確化するとともに、情報セキュリティ対策を確実かつ迅速に調整・実施できる体制にする必要がある。

また、整備・運用管理機関等は、基盤となる情報システムの情報セキュリティを確保するための方策等について包括的に定めた文書を整備するに当たっては、それぞれのポリシーとの関係について検討し、適切な運用管理が行われるよう、以下の事項等を整理するものとする。

・各機関等の間の責任分界
・平常時及び非常時の協力・連携体制
・非常時の具体的対応策　等

以上の検討・実施に当たっては、各機関等の間での十分な合意形成を図るとともに、情報セキュリティ対策の円滑かつ迅速な実施に支障を来さないように留意する必要がある。

なお、基盤となる情報システムの情報セキュリティ対策を共通的に行うため、基盤となる情報システムを整備し、運用管理を行う機関等は、当該基盤となる情報システムと連携する情報システムを管理する機関等と協議の上、基盤となる情報システムの情報セキュリティについて、各機関等が定めるそれぞれのポリシーの定めにかかわらず、共通的な規程を定めることができるものとする。

附則　政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（平成 17 年 9 月 15 日情報セキュリティ政策会議決定）は廃止する。

「政府機関等のサイバーセキュリティ対策のための統一基準群(案)」に対する意見募集の結果の概要

■ 実施方法：ＮＩＳＣのウェブページ及びe-Govに掲載して公募

■ 実施期間：2021年４月26日（月）～５月13日（木）

■ 意見総数：18者から59件【内訳：6企業・団体から延べ41件、12個人から延べ18件】

・統一規範に1件、統一基準に51件、運用指針に0件、全般に対して３件の意見提出

（１）修正意見：全55件

・表現の適正化を求めるものについて、統一基準を修正（９件）

・他の箇所で規定しているなどの理由で原案どおりとする意見については、理由を付して回答（46件）

☆主な意見

・ISMAP制度の活用と外部サービスの将来像を見据えた対策に関する意見（８件）

・ゼロトラストアーキテクチャや暗号アルゴリズム、電子署名等といった最新のセキュリティ対策に関する意見（16件）

・Web会議利用時の対策やテレワークで利用されるクラウドサービスへのセキュリティ対策に関する意見（３件）

（２）その他の意見：全４件

※意見募集の対象外である「政府機関等の対策基準策定のためのガイドライン」に対しても延べ４件の意見提出

表現の適正化を求めるものについては、趣旨を踏まえてガイドラインを修正（１件）

（参考）提出者名：

日本マイクロソフト株式会社、 BSA | ザ・ソフトウェア・アライアンス、KPMGコンサルティング株式会社、TIS株式会社、パロアルトネットワークス株式会社、日本プルーフポイント株式会社、個人（12）

「政府機関等のサイバーセキュリティ対策のための統一基準群（案）」に対する意見募集の結果一覧

資料２－６

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
1	日本マイクロソフト株式会社	統一基準	P.3	1.2	[該当箇所（原文コピー）] 機密性３情報 国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 [意見内容] 個人情報が含まれるという条件だけで機密性3情報に区分するのではなく、機密性2情報に相当する場合もあるとの注記があると、クラウドサービスの活用促進につながるのではと考えます。情報の共有が広く行われることが想定される中、情報主体の判断を容易にするためにも、情報の3分類の中の具体的な文書名などの例示があると良いかと考えます。 [理由]： 機密性3に区分されるとインターネット接続に制限が生じるところ、その範囲をより明確となるように改定いただいた点について、クラウドサービスを含めた外部サービスの活用促進につながるものと考えます。 ただ、政府機関において個人情報等が含まれる場合にはすべて機密性3に該当するとの誤解があるとお聞きすることもあり、その点について説明があると理解の助けになるのではと考えます。	文書管理ガイドラインにおいて「秘密文書」の定義が明確に規定されていることから、原案のとおりとします。
2	日本マイクロソフト株式会社	統一基準	P.6	1.3	[該当箇所（原文コピー）] 「外部サービス」とは、機関等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、当該機能を利用して機関等の情報を取り扱う場合に限る。 [意見内容] 但書にいう「情報を「取り扱う」場合」とありますが、この意味を明確にすることで、より外部サービス事業者の責任区分がわかるようになるのではないかと考えます。具体的な取り扱いに関する作業を明確にし、それに応じた共同責任を全うできるようにするためにも、情報を直接的に取り扱うサービスと間接的に取り扱う（内容に関与しない）サービスを明確にできるとさらに良いと考えます。 直接な取り扱いとは、機関等外のものがデータの閲覧、編集などを行うことを指し、間接的な取り扱いとは、機関等外のものが内容を閲覧しない状態での統計処理、保管やバックアップなどを行うことを指します。 [理由]： 個人情報保護委員会による、ガイドライン（「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ）によれば、クラウドサービスの利用に関して、「契約条項によって外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」については、当該クラウドサービスの利用についてクラウドサービス提供事業者は個人データを「取り扱わない」とされるもの説明されています。（Q5-33）本統一基準についても、上記のような要件をクラウドサービスが満たす場合、「機関等の情報を取り扱う場合」には該当しない、と考えてよろしいでしょうか。	御指摘の箇所につきましては、当該機能で情報が取り扱われる場合全てを想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。
3	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.6	1.3	クラウドサービスが「外部サービス」に該当することが明確にされたが、当該サービスの定義における「当該機能を利用して機関等の情報を取り扱う場合に限る」に関し、どのような場合が外部サービスの「情報を取り扱う」に該当するのかを明確にすることを希望する。	御指摘の箇所につきましては、外部サービスにおいて機関等の情報が取り扱われる場合を想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
4	TIS株式会社	統一基準	P.6	1.3	意見内容：外部サービスで取り扱う「機関等の情報」の定義を以下のように明確化してはどうか。 「機関等が職務上作成し、又は取得した情報及び機関等が組織的に用いる情報」 意見理由： 　職員の個人情報は、「機関等の情報」ではあるが、職員個人が出張の予約に際し特急券や宿泊施設の予約に外部サービスを利用したとして、外部サービスとしての管理が必要かとの観点から具体化したほうがよいのではと考えたため。	御指摘の箇所につきましては、外部サービスにおいて機関等の情報が取り扱われる場合を想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。
5	日本マイクロソフト株式会社	統一基準	P.6	1.3	[該当箇所（原文コピー）] 「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 [意見内容] 「外部サービス管理者」とは、外部サービスを利用する機関等において、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 [理由]： 外部サービス管理者が、外部サービス提供者側に存在するのか、利用する機関等に存在するのかが分かりにくいため、明確にしたほうが良いと考えます	御指摘の内容につきましては、ガイドラインの解説「遵守事項4.2.1(1)(a)(エ)「外部サービス管理者」について」において、利用する機関等の職員を対象にすることを記載しております。
6	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.6	1.3	「外部サービス管理者」の定義においても、政府機関等の職員を指すのか、事業者を指すのかを明確化することを求める。	御指摘の内容につきましては、ガイドラインの解説「遵守事項4.2.1(1)(a)(エ)「外部サービス管理者」について」において、利用する機関等の職員を対象にすることを記載しております。
7	個人	統一基準	P.6	1.3	「外部委託」が削られているが、依然として記載を行っておくべきと考える。（「業務委託」と若干の意味の違いがあるのではないかと思われるが、「外部委託」は「外部委託」で記しておく方が良いと思われる。）	御指摘の「外部委託」につきましては、本改定において一般用語として外部の者に委託することを指すこととしたので、原案のとおりといたします。
8	個人	統一基準	P.6	1.3	「業務委託」の末文の「ただし、機関等の情報を取り扱う場合に限る。」というのが少々分かりにくい。 その場合に限り「業務委託」という用語を使うのであれば、「（機関等の情報を取り扱う場合に限りこの用語を用いる。）」という形に変更した方が良いのではないかと思われた。	御指摘の箇所につきましては、委託する業務において情報を取り扱わせる場合を想定しておりましたので、御指摘を踏まえて、業務委託の用語定義等を修正いたします。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
9	KPMGコンサルティング株式会社	統一基準	P.7	1.3	「クラウドサービス」の定義から、「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」を削除してはいかがでしょうか。 理由としては、「約款による外部サービス」が削除されたこと、及びISMAPとの整合性確保が挙げられます。 元々、統一基準においては「約款による外部サービス」が規定されていて、その後に「クラウドサービス」が追加された経緯から、両概念の整合を図るために「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」との条件があったと理解しています。今回「約款による外部サービス」を削除するので、上記条件を設定する必要はないと考えます。 また、ISMAPは利用者からの「条件設定の余地」の有無にかかわらず、幅広く一般的な概念としてのクラウドサービスを対象としていると認識しております。しかし、「十分な条件設定の余地がない」サービスの場合には上記定義に照らすとクラウドサービスに該当しないため、改定案「4.2.1(3) 外部サービスの選定（クラウドサービス以外の場合）」が適用されることになります。 上記のように、「クラウドサービス」の定義を変更しないことにより不整合が発生するため、修正が必要と考えます。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、クラウドサービスの用語定義については、ISMAP基本規程にて定義されているクラウドサービスと同様となっており、不整合が発生するものではありません。
10	個人	統一基準	P.23	3.1.1(6)(b)	電磁的記録を電子メールで送信する場合には、S/MIME等を利用した電子署名と暗号化を必須とすること。特に、電子署名は、メールの送信者を明確にし、結果外部からの標的型攻撃対策にもつながるため、要保護情報以外の電磁的記録を送信する場合にも必須とすべきである。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の普及状況等を踏まえて検討してまいります。
11	個人	統一基準	P.23	3.1.1(6)(b)	独立行政法人及び指定法人（以下「独立行政法人等」）の職員等がインターネット回線を使用して機密性３情報を送信することはできないと考えられます。一方、国の行政機関においては、「行政文書の管理に関するガイドライン」における「秘密文書の管理に関するモデル要領」の第８の２（２）により、秘密文書（機密性３情報に該当）のうち、極秘文書についてはインターネット回線を使用した送信はできないと考えられますが、秘文書については暗号化等の措置を講じれば可能と考えられ、国の行政機関における取扱いと独立行政法人等における取扱いは同等ではないと考えられます。 今回の改定案で、情報の保存に関しては、２２ページ（４）（ｄ）において但し書きが追加されたことにより、独立行政法人等においても国の行政機関と同等の措置とすることが認められるようになりました。しかしながら、この但し書きは、２３ページ（６）（ｂ）には適用されないと考えられます。これは、外部への送信については、国の行政機関と同等の取扱いを認めないということでしょうか。 もし同等の取扱いを認めるということであれば、２３ページ（６）（ｂ）においても、２２ページ（４）（ｄ）に追加されたものと同	御意見ありがとうございます。 御指摘のとおり修正いたします。
12	個人	統一基準	P.25	4.1.1	外部委託に関する事項であるが、近年、(委託に限らず)業務上利用する外部サービスや外部開発のソフトウェア(Windows等のOSや、ウイルス対策ソフト等も含まれる)に対する「サプライチェーン攻撃」という攻撃が多くなってきている。そのため、当該サービスやソフトウェアの開発者の情報セキュリティ対策も評価すべきである。	サプライチェーンリスクについては重要と考えており、クラウドサービスの選定時においては、ISMAP管理基準において機関等の意図せざる変更が加えられないための管理体制を確認し、クラウドサービス以外においては、遵守事項4.2.1(3)(b)(ウ)において確認を求めております。また、外部開発のソフトウェア等を調達する場合においては、遵守事項5.1.2(1)(a)にて機器等の選定基準を整備することを求めております。

通し No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
13	KPMGコンサルティング株式会社	統一基準	P.25	4.1.1	改定案では、これまでの「外部委託」よりも広範な「業務委託」が定義されていると認識しております。 （従来）　外部委託：機関等の情報処理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。 （改定案）業務委託：機関等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。（中略）ただし、機関等の情報を取り扱う場合に限る。 業務委託の「目的・趣旨」について、今回改定案での定義変更により「情報処理業務」以外についても適用範囲が拡大したことを明記してはいかがでしょうか。 現状の記載では、「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」となっており、このような場合に限定されると誤解される可能性があると思われます。 特に「機関等の情報を取り扱う場合」となっているものの、現実的には電子メールの授受や端末により作成した文書を提供するなど、ほぼすべての委託が該当するものと思われ、そのことを明記するべきと考えます。	御指摘の箇所につきましては、委託する業務において情報を取り扱わせる場合を想定しておりましたので、御指摘を踏まえて、業務委託の用語定義等を修正いたします。
14	個人	統一基準	P.25	4.1.1(2)	いくら契約でしっかり禁止事項等で合意しても、悪意をもってやられたらどうしようもないんで、外資を排除するのは当然としても、内資でも実質的に外国資本に支配されている場合もあるので、きちんとチェックが必要です。 そもそも秘密事項を外部に委託すること自体、安全保障上リスクが高すぎます。外部に委託することなく、すべて政府内でやるべきではないでしょうか？	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の点について、遵守事項4.1.1(2)(b)において委託先への情報セキュリティ対策を講ずることを求め、遵守事項4.1.1(2)(c)においては委託先に対して情報セキュリティ監査等を求めることにより、情報セキュリティが十分に確保できるように定めております。御意見も踏まえ、業務委託に係るセキュリティ確保について、より強固となる方策を検討してまいります。
15	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.2	政府目標の「クラウド・バイ・デフォルト原則」を達成する上でも、革新的なクラウドコンピューティング・ソリューションの採用がセキュリティ要件によって阻まれないように、本原則を統一基準に反映させることを奨励する。	本改定においては、「クラウド・バイ・デフォルト原則」を踏まえて改定をしており、クラウドサービスを選定する際はISMAP制度を活用すること等を記載しております。なお、クラウドサービスにおけるセキュリティ対策については、引き続き検討してまいります。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
16	日本マイクロソフト株式会社	統一基準	P.28	4.2	「4.2 外部サービスの利用」という項目が新設されたことによって、業務委託との違いが明確になり、クラウドバイデフォルトにおけるセキュリティ対策がわかりやすくなったと感じます。また、外部サービスの選定において、クラウドに対する要件がクラウドサービス以外の時と比較して簡素になっている点についても、クラウドサービスが単に機能だけを提供しているものではないということに対するご理解の表れだと感じています。 一方で、セキュリティ対策が攻撃ベースになっており、後付けのセキュリティ対策が中心的に考えられているように見受けられます。政府の調達の状況などを勘案するとIT基盤にセキュリティ機能を含むような形で、長期での運用に耐える形での要件提案ができると良いのではないかと考えます。そのために、追加のセキュリティ投資が必要のないサービス利用の一つとして、外部サービスベンダーから提供されるセキュリティベストプラクティスに沿ったアーキテクチャ設計を促すなど、クラウドサービスの活用などの提案ができるのではないかと考えます。	本改定においてクラウドバイデフォルトの原則を踏まえ、クラウドサービスの利用拡大を見据えて外部サービス利用者が行うべきセキュリティ対策について追加しております。なお、クラウドサービスにおけるセキュリティ対策については、引き続き検討してまいります。
17	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.2	セキュリティの責任共有モデルが反映されたことを歓迎する。このセキュリティモデルが政府機関全体で理解されることをNISCにて確実にすることを奨める。	今後NISCにおいて改定内容の周知や監査等の実施により機関等へフォローをしてまいります。
18	日本マイクロソフト株式会社	統一基準	P.28	4.2.1	[該当箇所（原文コピー）] また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。 [意見内容] また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用するサービスも存在することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。 [理由]： クラウドサービスの特徴としてマルチテナントが挙げられることがありますが、古い構成でのASPのようなものでない限り、同一アプリケーション（ライセンス）でのマルチテナント利用は少なくなっていると考えます。テナントごとに適切なログをオンデマンドセルフサービスで取得することができるかなどを明確にしていただくことで、利用可能なサービスの判断に役立つと考えます。	御意見ありがとうございます。 御指摘を踏まえて、当該目的・趣旨を修正いたします。
19	KPMGコンサルティング株式会社	統一基準	P.28	4.2.1	「目的・趣旨」において、外部サービスの例として「ＳＮＳ（ソーシャルネットワーキングサービス）」が記載されていますが、「ソーシャルメディアサービス」に修正してはいかがでしょうか。 統一基準の他の箇所では、ソーシャルメディアサービスの用語となっています。（例：ガイドライン P13「図1.5-1 「情報システム」、「機器等」及びその関係」では、図中で外部サービスの枠内には「ソーシャルメディアサービス」が記載。）	御指摘の箇所につきましては、ソーシャルメディアサービスのうち、ＳＮＳ（ソーシャルネットワーキングサービス）を想定し例示としてあげていますので、原案のとおりといたします。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
20	個人	統一基準	P.28 P.29	4.2.1(1) 4.2.1(2)	本改定案では、政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、クラウドサービス利用者側として実施すべき対策や考え方に係る記載が追加されています。 これに関して、クラウドサービス利用者側に対しては、係る新たな管理基準を自身のみで踏まえた上でクラウドサービス提供者及びクラウドサービスに対する評価及び対策等を一から講じさせるような、新たに重い負荷のみを強いているかのように思われました。これでは、クラウドサービス利用者側へISMAP制度のメリットが生かされないように思われました。 クラウドサービス利用者側が、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）を利用することにより、クラウドサービス提供者及びクラウドサービスに対する公開情報を参照し、クラウドサービス選定及び選定したクラウドサービスへの対策等の検討に係る負荷を軽減できるよう、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）の利用方法に踏み込んだ記載についても、統一基準群に追加すべきだと思われます。 また、ISMAPは、米国FedRAMP等と異なり、クラウドサービス提供者及びクラウドサービスへお墨付きを与える評価制度では無いことも踏まえ、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）の利用における留意点を含めて、統一基準群へ追加し、クラウドサービス利用者側へ係る注意喚起及び係る負荷の軽減を図るべきだと思われます。	ISMAPの成果物の利用方法や留意点については、今後も政府機関等への周知を図ってまいります。
21	KPMGコンサルティング株式会社	統一基準	P.29	4.2.1(2)	4.2.1(3)(e) 準拠法・裁判管轄の選定条件については、4.2.1(2)においても規定するべきではないでしょうか。 理由としては、ISMAPでは準拠法・裁判管轄は情報提供にとどまり、リスク評価は発注者側が実施する必要があるためです。	御指摘の内容につきましては、遵守事項4.2.1(2)(b)における外部サービス提供者の選定基準に含まれている想定です。
22	パロアルトネットワークス株式会社	統一基準	P.30	4.2.1(3)(d) （ア）	意見：クラウドサービス以外の場合にのみ情報セキュリティ監査の受入れが条件に含まれるようにもお見受け致しますが、クラウドサービス上で開発されるシステムにおいても同様に情報セキュリティ監査の受入れは必要と考えます。 理由：クラウドサービス上で開発されるシステムにおいても同様に情報セキュリティ監査の受入れは必要と考える為。	御指摘の箇所につきましては、外部サービス（クラウドサービス以外）を選定する際に、外部サービス提供者への情報セキュリティ監査の受入れを求めており、クラウドサービスにおいてはISMAP管理基準において外部サービス提供者への監査を求めております。なお、外部サービスを利用して構築された情報システムにおける情報セキュリティ監査については2.3.2款にて定めております。
23	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(6)(a) （ア）	[該当箇所（原文コピー）] （ア）不正なアクセスを防止するためのアクセス制御 [意見内容] （ア）情報やサービスに対する不正なアクセスを防止するためのアクセス制御 [理由]： クラウドサービスにおいては、データベースやストレージサービスのようにデータを預かる機能だけではなく、それを操作したり、状況を判断するためのダッシュボードなどの機能があります。これらのサービスに対する不正アクセスによって、管理者機能などを不正取得する可能性もあります。明示的に「情報やサービス」としていただくことでより分かりやすくなるかと思います。	御指摘の箇所につきましては、ガイドラインの基本対策事項4.2.1(6)-1において具体的なアクセス制御を示しているため、原案のとおりといたします。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
24	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(6)(a)（イ）	[該当箇所（原文コピー）] （イ）取り扱う情報の機密性保護のための暗号化 [意見内容] （イ）取り扱う情報の機密性及び完全性確保のための暗号化 [理由]： 暗号化はアクセス制御の一つの手段ですので、（ア）のみで十分だと考えます。突起する必要があるのならば、ランサムウェアなどによる攻撃を踏まえた完全性確保についても記載するのが良いと考えます。これによって、秘匿のための単純な暗号化ではなく、情報単位での管理を明示できるのではないかと考えます	御指摘の箇所につきましては、国内法以外の法令及び規制が適用されるリスク等も踏まえて、暗号化を求める趣旨であるため、原案のとおりといたします。
25	パロアルトネットワークス株式会社	統一基準	P.31	4.2.1(6)(a)（ウ）	該当文書：(ウ) 開発時におけるセキュリティ対策 意見：下記への文書の変更を意見として提出致します。 (ウ) 開発各フェーズにおけるセキュリティ対策 理由：開発にはいくつかのフェーズがあり、その各フェーズそれぞれでセキュリティ対策を施すことで、手戻りによる開発期間延長防止や、後の脆弱性予防として必要であると考える為。	今般の改定では開発全体を対象とした規定としておりますが、開発における各フェーズに求めるべきセキュリティ対策については今後の検討の参考とさせていただきます。
26	パロアルトネットワークス株式会社	統一基準	P.31	4.2.1(7)(a)	意見：(ケ)の追加を意見として提出致します。 (ケ) コンプライアンス準拠への継続的な監査 理由：外部サービスを利用する際には、人為的なミスに起因するインシデントをできる限り抑制するため、組織内で定められたコンプライアンスに対する継続的な監査が必要不可欠であると考える為。	御指摘の箇所につきましては、外部サービス特有の運用に関する規定を定めており、組織における情報セキュリティ監査については2.3.2款にて定めております。
27	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(7)(a)（キ）	[該当箇所（原文コピー）] （キ）設計・設定時の誤りの防止 [意見内容] （キ）設計・設定時に想定した構成の監視と修正 [理由]： クラウドサービスにおいては、構成をリアルタイムで精査できる機能が付与されているものが増えてきました。これはSaaSにおいてもPaaS/IaaSにおいても導入されています。これらの機能がないものは後付けでCloud Security Posture Management（CSPM）ツールを導入することで状態の把握と修正を行うことができます。いわゆるmis-configuration（構成ミス）への対策として具体的に記載することが良いと考えます	御指摘の箇所につきましては、ガイドラインの解説「基本対策事項4.2.1(7)-7 a)「設定の誤りを防止するための対策」について」において外部サービス提供者が提供するセキュリティ設定・監視ツールの利用についても言及しているため、原案のとおりといたします。
28	日本マイクロソフト株式会社	統一基準	P.32	4.2.2(2)(a)	[該当箇所（原文コピー）] (a) 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こと。 [意見内容] (a) 職員等は、利用するサービスの約款、その他の提供条件等、サービスに関連する情報を添えて、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こと。 [理由]： リスクは申請者が判断するのではなく、責任者が判断するのではないかと考える。本項だけではなく、職員が判断するとしているところはできる限り責任者が判断することにし、判断の均一化を図ることがガバナンスにおいて重要なことではないかと考えます。	御指摘の内容につきまして、最終的な判断は利用申請の許可権限者が行うにしても、外部サービス利用者自身においてもリスクの評価は必要であると考えていることから、原案のとおりといたします。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
29	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.35	5.2.1(2)(a)	統一基準の5.2.1 (2) (a) 及び「政府機関等の対策基準策定のためのガイドライン （令和３年度版）」（173ページ）において「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 （外部サービスを含む。）から分離する」という記述を削除することを求める。インターネット分離は、システムに保有されている情報へのアクセスや利用が大幅に減少するだけでなく、大手クラウドコンピューティング・サービス・プロバイダーによる最先端のセキュリティ・ソリューションの恩恵を政府機関が受けることも制限する。暗号化や厳格なアクセス管理システム等、最高水準の安全なソリューション利用を政策において確実にすることが不可欠であると考える	御指摘の箇所につきましては、通信経路を物理的又は論理的に分離することの要否を判断することを求めており、一切のインターネットアクセスを禁止する意図ではありません。
30	パロアルトネットワークス株式会社	統一基準	P.36	5.2.1(2)(a)(ア)	該当文書： (ア) 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 意見：下記への文書の変更を意見として提出致します。 (ア) 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、通信の可視化、暗号化機能等のセキュリティ機能要件 理由：通信の可視化がサイバー攻撃の挙動発見、次の対策への現状把握に重要な要素となるため。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の検討の参考とさせていただきます。
31	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.8 P.42	1.3 6.1	「常時アクセス判断・許可アーキテクチャ」や「常時システム診断・対処」などのキーワードを「1.3　用語定義」や、第6章6.1.「情報システムのセキュリティ機能」に追加し、「統一基準」に明確に反映させることを奨める。	「常時アクセス判断・許可アーキテクチャ」については、ガイドラインの基本対策事項6.1.2(1)-1 f)に記載を追加しておりますが、今後の普及状況等を踏まえ、用語定義への追加や遵守事項として規定することを検討してまいります。
32	日本マイクロソフト株式会社	統一基準	P.42	6.1.2	主体を制限することという記載はあるものの、管理者アカウントなどを含む共有IDなどを制限に関する記載は見られないため、アカウントの共有（root/ Administratorに代表されるもの）の利用を原則として禁じる項目も記載していただきたいと考えています。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、遵守事項6.1.1(2)(a)において識別コードを適切に付与すること、更に、当該遵守事項の基本対策事項において情報システムを利用する主体ごとに識別コードを個別に付与することを求めており、また、管理者権限の特権を持つ主体の識別コードの管理については遵守事項6.1.3(1)(b)に規定しているところです。御指摘も踏まえ、アカウント管理に係るセキュリティ対策については、引き続き検討してまいります。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
33	個人	統一基準	P.43	6.1.5(1)(a)（イ）	電子署名は、その情報の作成者を明確にし、結果外部からの標的型攻撃対策にもつながるため、要保全情報以外の電磁的記録にも必須とすべきである。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の普及状況を踏まえて検討してまいります。
34	日本マイクロソフト株式会社	統一基準	P.44	6.1.5(1)(b)	[該当箇所（原文コピー）] 追加 [意見内容] （オ）政府推奨暗号リストに記載された暗号アルゴリズムが利用できない環境においては、検証済みの暗号アルゴリズムの利用を検討することができるようにすること [理由]： 量子コンピュータの活用により、これまでの暗号アルゴリズムについても十分ではないと言う議論もされるようになりました。これらを踏まえ、検証済みの暗号アルゴリズムについて柔軟に利用できるようなガイダンスも必要だと考えます。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容につきましては、遵守事項6.1.5(1)(b)(イ)において、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及びそれを利用した安全なプロトコルを採用することを求めており、ガイドラインの解説「遵守事項6.1.5(1)(b)(イ)「やむを得ない場合」について」において、政府推奨暗号リストに記載された暗号アルゴリズムが対応していないなどの場合について記載しているため、原案のとおりといたします。
35	日本マイクロソフト株式会社	統一基準	P.46	6.2.3	[該当箇所（原文コピー）] 近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている [意見内容] 特に、接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている [理由]： 本書は報告書ではなく、時間に関係なく活用される文書だと認識しています。その中で「近年」とあった場合、文書の内容の正しさについて確保が難しくなると考えます。特記事項であれば「特に」とすることで良いかと考えます。以下に「近年」というキーワードが含まれています。 2.2.3 教育 6.2.3 サービス不能攻撃対策（本コメント） 6.2.4 標的型攻撃対策 7.1.3 複合機・特定用途機器 7.3.2 IPv6 通信回線 6.2.3、6.2.4以外は変更履歴にないことから、近年がすでに近年でないのではないかと判断します。	御意見ありがとうございます。 御指摘の箇所における内容につきましては、現時点では問題があるとは考えておりませんが、今後の課題と捉え、記載内容の検討をしてまいります。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
36	パロアルトネットワークス株式会社	統一基準	P.47	6.2.4	該当文書： 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。 意見：下記への文書の変更を意見として提出致します。 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、ネットワークや利用者の振る舞いから異常を発見する、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。 理由：巧妙化し続ける標的型攻撃により、攻撃を検知できず意図せず内部の利用者から外部へ情報が漏洩する事例も出ており、より高度な情報セキュリティ対策が必要と考えられる為。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の検討の参考とさせていただきます。
37	パロアルトネットワークス株式会社	統一基準	P.47	6.2.4(1)(b)	該当文書：(b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。 意見：(b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、証跡情報により影響範囲を把握する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。 理由：万が一、インシデント等の有事があった際には、速やかにその影響範囲を特定できるよう証跡情報を管理しておく必要があると考える為。	今般の改定にて、ガイドラインの基本対策事項6.2.2(1)-6の解説にEDRに係る記載を追加したところですが、御指摘の内容については今後の検討の参考とさせていただきます。
38	パロアルトネットワークス株式会社	統一基準	P.50	7.1.1	該当文書：業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で 意見：下記への文書の変更を意見として提出致します。 業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策及び有事の際の証跡管理対策を施した上で、 理由：制限や追加のセキュリティ対策を施した上で、万が一インシデント等の有事があった際に、その証跡を管理しておく必要があると考える為。	ログの取得・管理については遵守事項6.1.4にて規定しているところですが、御指摘の内容については今後の検討の参考とさせていただきます。
39	日本マイクロソフト株式会社	統一基準	P.51	7.1.1(4)(b)	[該当箇所（原文コピー）] (a)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関等が支給する端末（要管理対策区域外で使用する場合に限る）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こと [意見内容] (a)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関等が支給する端末（要管理対策区域外で使用する場合に限る）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および改ざん、悪用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こと [理由]： 本項目に限らず、情報窃取についての記述が多いのですが、改ざんや悪用に関するトラブルも多くなっており、全般的に考慮いただく必要があると考えます。特に端末の項目においては、端末そのものを悪用することにより、なりすましが容易になる場合があることを記載しておく必要もあるかと考えます。同様の記述が(5)(d)などにも見られます	端末に対する改ざん及び悪用されることを防止するための技術的な措置に関しては、引き続き検討してまいります。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
40	日本マイクロソフト株式会社	統一基準	P.52	7.1.2	[該当箇所（原文コピー）] 仮に機関等が利用するサーバ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、国民からの信頼を大きく損なう。 [意見内容] 改訂前が「機関等が有するサーバ装置が」ということになっており、外部サービスを想定して「機関等が利用するサーバ装置が」と変更されたと推察します。そのことは適切だと思いますが、その場合は遵守事項が外部サービスに適切であるかどうかについても検討していただきたく思います。 外部サービスを想定していないと言うことであれば、その旨を記載していただけると分かりやすいかと思います。	御意見ありがとうございます。 御意見を踏まえ、ガイドラインに解説を追加いたします。
41	日本プルーフポイント株式会社	統一基準	P.55	7.2.1(1)(c)	「情報システムセキュリティ責任者は、電子メールなりすましの防止策を講ずること」 意見　：　上記文言につきまして、下記の通り修正することを提案いたします。 「情報システムセキュリティ責任者は、電子メールなりすましの対策として、送信ドメイン認証技術による受信側および送信側の対策を講ずること」 理由　：　近年、なりすましメールによる被害は増大しております。一般的に信頼度が高いと認知されている政府機関の名を騙るメールについては、被害者が騙される可能性が高いと考えられるため、なりすましメール対策はより強化されるべきとかんがえております。参考資料として提示されております「政府機関等の対策基準策定のためのガイドライン（令和3年度版）（案）」の290ページを拝見しますと、SPF, DKIM, DMARCといった技術が例示されておりますが、DMARCはSPF, DKIMを補強する技術として登場したものであり、諸外国でも米国をはじめとする諸外国でも政府機関についてはDMARCを必須としております。SPFをはじめとする送信ドメイン認証技術の対策は当然のこととして、送信側が責任を負うなりすましメール対策をより強化するためにDMARC導入を促進すべきと考えます。そのような背景を統一基準そのものに表現するために、上記の文言修正を提案するものです。ご検討の程、よろしくお願い申し上	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、送信ドメイン認証技術による送信側の対策の例については、ガイドラインイ7.2.1(1)-2 a)に示しており、今後の普及状況等を踏まえて遵守化も検討してまいります。
42	個人	統一基準	P.56	7.2.2 (1)(a)(オ)	HTTP Strict Transport Securityを利用したHTTPS必須化を基準に追加すべき。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の普及状況を踏まえて検討してまいります。
43	パロアルトネットワークス株式会社	統一基準	P.56	7.2.3	該当文書：これらの問題を回避するためには、DNSサーバの適切な管理が必要である。 意見：下記への文書の変更を意見として提出致します。 これらの問題を回避するためには、DNSサーバの適切な管理と、端末等クライアントからのDNSクエリに対するセキュリティ対策が必要である。 理由：DNSサーバの管理と併せ、クライアントからのクエリに対するセキュリティ対策も同様に必要な為。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の検討の参考とさせていただきます。
44	パロアルトネットワークス株式会社	統一基準	P.57	7.2.3(2)(b)	該当文書：(b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。 意見：下記への文書の変更を意見として提出致します。 (b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、脅威インテリジェンスサービス等を通じ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こと。 理由：情報の持ち出しに使用される悪意のあるDNSドメインは、近年は標的型攻撃等においても多用される傾向があり、DNSサーバの管理と併せてクライアントからのクエリに対するセキュリティ対策も必要となる為。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の検討の参考とさせていただきます。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
45	日本プルーフポイント株式会社	統一基準	P.62	8.1.1(2)(a)	「情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること」 意見　：　上記文言につきまして、下記の通り修正することを提案いたします。 「情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から、外部攻撃者による誘導および他の手段による内部不正を防ぐための機能を持つ情報システムを構築すること」 理由　：　情報処理推進機構(IPA)様が発表されている10大脅威の中でも、近年、上位にランクインしている通り、セキュリティインシデントのなかで内部脅威の占める割合は高く、その対策の重要度は増していると考えております。参考資料として提示されております「政府機関等の対策基準策定のためのガイドライン（令和3年度版）（案）」の332ページを拝見しますと、職員による規定の遵守を支援する機能として、不審なWebアクセスへの防御や不審な電子メールへの対処といった部分が強調されておりまして、他の行為（例：機密情報のコピー、外部への送信等）に関する観点が薄いように感じられます。そのため、内部脅威対策防止も重要であるという考えを統一基準そのものに評点するために、上記の文言修正を提案するものです。ご検討の程、よろしくお願い申し上げます。	改定箇所への御指摘ではないためパブリックコメントの対象ではありませんが、御指摘の内容については今後の検討の参考とさせていただきます。
46	日本マイクロソフト株式会社	統一基準	P.65	8.1.1(8)	[該当箇所（原文コピー）] 追加 [意見内容] (c) 職員等は Web 会議への参加者の権限について適切な管理ができるようにすること [理由]： Web会議においては、プレゼンテーションや発言、会議の記録などの機能があり、参加者に必要のない機能をオンにしていることで妨害行為などが可能になります。それを防止するための措置についても言及できればと考えます。	遵守事項8.1.1(8)(b)において、会議に無関係の者が参加できないように措置することを求めていることから、参加者による妨害行為は想定していないため、原案のとおりといたします。
47	KPMGコンサルティング株式会社	統一基準	P.65	8.1.1(8)(b)	記載ぶりとして、名宛人の後に読点をいれること、語尾を他の規定と合わせてはいかがでしょうか。 「(b) 職員等はWeb会議を主催する場合、会議に無関係の者が参加できないよう措置すること。」 ↓ 「(b) 職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。	御意見ありがとうございます。 御指摘のとおり修正いたします。
48	日本マイクロソフト株式会社	統一基準	P.65	8.1.2	[該当箇所（原文コピー）] 全般 [意見内容] テレワークにおいてはクラウドサービスの利用が今後見込まれると考えていますが、具体的な対策がリモートアクセスについて中心的に記載されているように感じます。クラウドサービスへのアクセスはリモートアクセスとは異なる内容になりますので、その点が明確になっていると良いと考えます。 現在の遵守事項は端末内にデータが多く存在することが前提となっており、端末そのもの、またはその内部のデータへの攻撃が想定されているように思いますが、クラウドサービスの利用が進む中で端末内のデータが少なくなり、リスクも変化するのではないかと考えています。	テレワークにおけるクラウドサービスの利用に係るセキュリティ対策については、今後の利用状況を踏まえて検討してまいります。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
49	個人	統一基準	P.65	8.1.2(1)(a) 8.1.2(1)(b)	テレワークの実施に係る規定のすべての項目を、情報システムセキュリティ責任者が定めるのは責任の範疇を超えていると考えます。 テレワークの実施に係る規定に盛り込む内容は、必ずしも情報システムに係るものだけではない認識のためです。ガイドラインの基本対策事項8.1.2(1)-1において、規定に盛り込むべき項目が例示されていますが、例えば「c)要管理対策区域外での要機密情報の取扱手続」は統括情報セキュリティ責任者が定めるべきものと考えます。現に、遵守事項7.1.1(4)(a)において、「機関等が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順及び許可手続」は、統括情報セキュリティ責任者が定める実施手順として規定されています。 そのため、各役職における責任の範疇の規定を整備するよう、遵守事項を修正すべきと考えます。仮に、修正不要と判断されるのであれば、そう判断する根拠となる考え方を、ガイドラインに解説として記載することをご検討ください。	御意見を踏まえ、総括情報セキュリティ責任者が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といたします。
50	パロアルトネットワークス株式会社	統一基準	P.66	8.1.2(2)(d)	該当文書：(d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。 意見：下記への文書の変更を意見として提出致します。 (d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定する、もしくは、リモートアクセス経路上で包括的なセキュリティ対策を実施すること。 理由：リモートアクセスにおけるセキュリティ対策は、端末における対策のみではなく、SIG(Secure Internet Gateway)やSASE(Secure Access Service Edge)等の包括的なセキュリティ対策によっても実現可能である為。	御意見ありがとうございます。 御提案のテレワークやリモートアクセスでのクラウドサービスを利用したセキュリティ対策については、今後の利用状況を踏まえて検討してまいります。
51	個人	統一基準	ー	ー	平常時から暗号を使っている場合、鍵が盗まれない為の運用方法は、どこを参照すればよいか明記いただけると有意義だと感じます。	暗号化に用いる鍵の管理については、遵守事項6.1.5(1)(b)(エ)において手順を定めることとしており、管理手順の策定に係る留意事項に関してはガイドラインにおいて解説を記載しております。
52	個人	統一規範	P.5	16条	改正内容に賛成ではない。 機密情報については依然として外部サービスを利用して取り扱ってはならない形とすべきと考える。	改定案では、外部サービスを利用して要機密情報を取り扱う場合の遵守事項を4.2.1項で定めており、現行の統一基準群における「約款による外部サービス」は当該遵守事項を満たすことが一般的に困難であるため、実質的に「約款による外部サービス」では原則として要機密情報を取り扱えないことは変わりませんが、御指摘を踏まえ、統一基準の4.2.1款の目的・趣旨において補足します。
53	個人	ガイドライン	P.13	1.5	遵守事項2.1.1(4)(d) において、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事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任することとされています。 当該遵守事項では、情報システムの構成要素が外部サービスのみであった場合も、情報システムセキュリティ責任者の選任を求めているのでしょうか。 仮に求めていないのであれば、誤解を与えるため、今回の意見募集の対象外となりますが、ガイドラインの図1.5-1を修正いただくか、注記を追加することをご検討ください。	情報システムの構成要素が外部サービスのみであったとしても、当該情報システムのセキュリティ対策の運用の責任の所在を明確にすることが重要であることを踏まえ、情報システムセキュリティ責任者を選任することが求められます。

通しNo.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
54	個人	ガイドライン	P.320	7.3.1(4)-1	現行では、「SSIDの隠ぺい」が記載されていましたが、今回記載が削除されました。これは、今やセキュリティ対策として意味をなさなくなった、との認識でよいでしょうか。他に意図がございましたら、今後のセキュリティ対策の参考としたく、教えてください。	ガイドラインについては、パブリックコメントの対象ではありませんが、本対策においては、より強固なセキュリティ対策を求めることとしました。
55	個人	ガイドライン	P.348	8.1.1(8)-1 d)	これは、令和2年10月12日、外務省において公表された「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」と明確に矛盾していると認識しました。 https://www.mofa.go.jp/mofaj/la_c/sa/co/page22_003432.html 本基準がそのまま施行され、これに準拠したサービスを各政府機関が導入した場合、当該政府機関が「要機密情報」と判断したWeb会議に関する記録について、各捜査機関がサービス提供者側から追えないことになり、政府機関等が絡む諸犯罪の立件を難しくするものと思料します。当該項目は本当に追加して問題無いのでしょうか。当方は削除すべきと考えます。	ガイドラインについては、パブリックコメントの対象ではありませんが、統一基準群の案は同ステートメントに矛盾しているとは考えておりません。
56	個人	ガイドライン	P.96	3.1.1(6)-2 b)	”秘密分散技術自体が暗号技術の一種であるので、これにより分割されたデータをさらに暗号化する必要はなく、暗号鍵も必要ない。”と表現されています。 仮に秘密分散技術が暗号技術一種であり政府が利用するものならば　「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」にあるものだと想定されます。ところが秘密分散技術を見つけることができませんでした。 対応の仕方として例えば次の2通りがあるかと考えます。 １）この統一基準公開までに”CRYPTREC暗号リスト”に秘密分散技術を具体的に明示する。 ２）問題の文章を含む現状の表現を変更する。 例えば、”基本対策事項3.1.1(6)-2 b)「複数の情報に分割し」について”の内容を次のように表現してみてはいかがでしょうか。 　１個の電子情報について、分割された一部のデータからは情報が復元できない方法で複数に分割し、電子メール、DVD、USB メモリ等の外部電磁的記録媒体で郵送するなど異なる経路で運搬・送信することで、情報漏えいを防止することができる。 　秘匿すべき情報を秘密分散技術を用いて、複数のデータに分割すると、そのうちの一部を窃取されても元の情報を復元することができない。 秘密分散技術を用いると分割されたデータは暗号化されたデータと同様に復元も類推もされないので　さらに暗号化する必要はない。 さらに秘密分散技術では暗号鍵も必要としていない。	ガイドラインについては、パブリックコメントの対象ではありませんが、統一基準では暗号化機能及び電子署名機能を導入する際にCRYPTREC電子政府推奨暗号リストの参照を求めているところ、秘密分散技術は暗号技術の一つではありますが、暗号化を行うわけではないため、原案のとおりといたします。

通し No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
57	個人	全般	ー	ー	・情報処理技術者試験に関する意見	御意見ありがとうございます。 統一基準群の改定に関するものではないため、お答えは困難です。
58	個人	全般	ー	ー	・サイバーセキュリティー対策 ・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人高度人材での導入で社会水準の向上による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準での基準による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案	御意見ありがとうございます。 統一基準群の改定に関するものではないため、お答えは困難です。
59	日本マイクロソフト株式会社	全般	ー	ー	文書群の名称を「サイバーセキュリティの」と変更されましたが、本文中には情報セキュリティという記載も多くあり、サイバーセキュリティと情報セキュリティの適用範囲についてわかりにくく苦なっているように感じました。改めて、サイバーセキュリティと情報セキュリティを明確に定義していただく必要があるのではないかと考えます。	サイバーセキュリティ戦略本部及びNISCの公表する資料名称を統一する観点から、文書名について「サイバーセキュリティ」を用いることといたしますが、内容面での変更はありません。「情報セキュリティ」と「サイバーセキュリティ」の明確な定義については引き続き検討してまいります。