資料４

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４－１　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正（案）について

資料４－２　政府機関等の情報セキュリティ対策のための統一規範（案）

資料４－３　政府機関等の情報セキュリティ対策のための統一基準（案）

資料４－４　政府機関等の情報セキュリティ対策の運用等に関する指針（案）

資料４－５　「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（案）」に対する意見募集の結果の概要

資料４－６　「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（案）」に対する意見募集の結果

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4－1

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

①情報システムの内部(端末等)での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止、②IT資産管理の自動化とそれによる脆弱性への迅速な対応、③データ保護による情報漏えい対策の導入を、今後政府機関等が目指すべき3本の柱とし、これらの対策の導入を推奨。

2. 政府機関等のサービスの利用者の側に立った対策

政府機関等は、自らの情報システムのサイバーセキュリティ対策に加え、国民が安心して安全にウェブサイト等を通じて行政サービスを利用できるよう、“利用者側に立った追加的な対策”を講じる。

3. 政府機関等の自律的な能力向上への誘導(PDCA※サイクルの効果的運用)

一巡した府省庁監査の結果から得られた知見を統一基準群にフィードバック。自らの対策状況を評価し、より効果的な改善に繋げるべく、政府機関等の自律的なPDCAサイクルの更なる循環を促す。

※ PDCA:[Plan(計画)、Do(実行)、Check(評価)、Act(改善)]

4. 業務形態に対応した規定の整備

多様な業務形態が存在する独立行政法人等に目を向け、これらを踏まえたサイバーセキュリティ対策を導入。

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構成

資料4－1

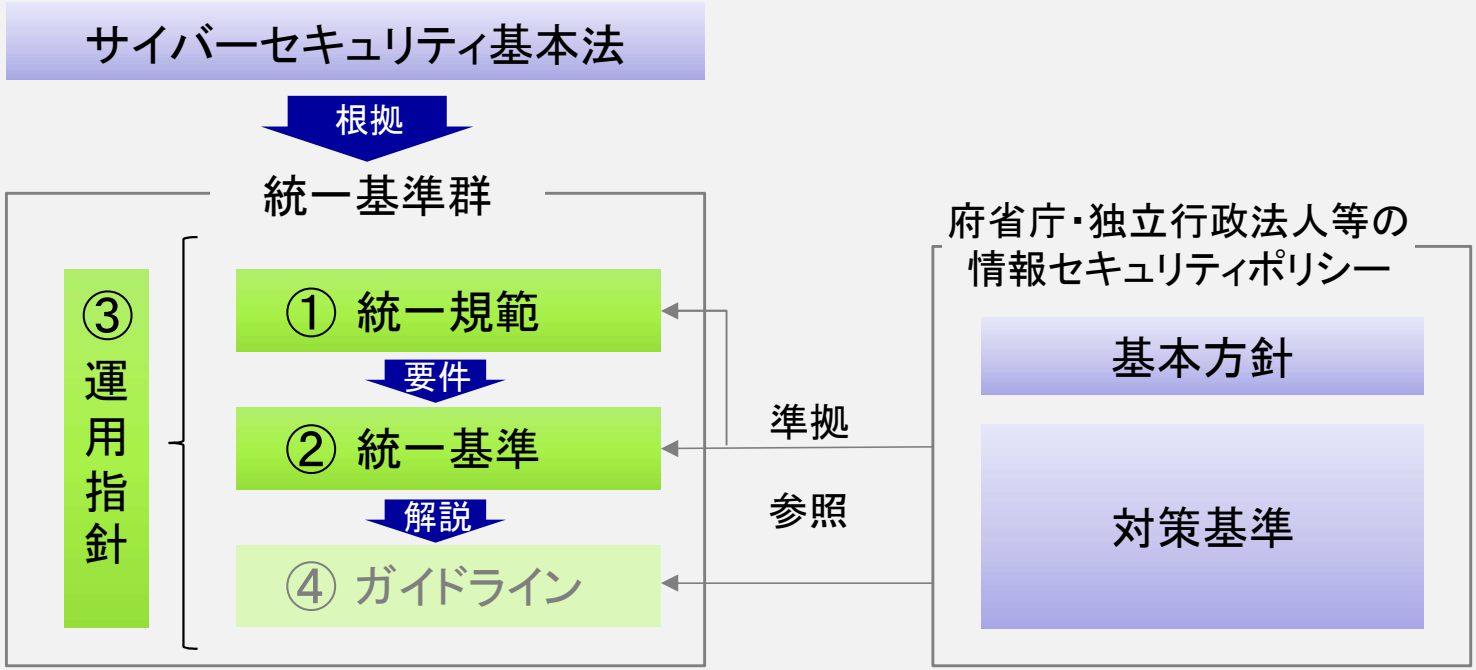
■ 統一基準群の対象

① 政府機関等の情報セキュリティ対策のための統一規範
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
③ 政府機関等の情報セキュリティ対策の運用等に関する指針
　　} サイバーセキュリティ戦略本部決定文書

④ 政府機関等の対策基準策定のためのガイドライン
　　} 内閣サイバーセキュリティセンター決定文書

※ ①～③と関連性が高いドキュメントのため、同時に改定する。

■ サイバーセキュリティ基本法、統一基準群、政府機関等の情報セキュリティポリシーの関係



3. 改定の概要1

資料4－1

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

≪主な内容≫

✓ 端末、サーバにおける『未知の不正プログラムの検知／実行の防止の機能の導入』
⇒未知の不正プログラム対策を「侵入後の検知」から「感染の未然防止」へ、「境界監視」に加え「プログラムが動作する内部」へ進化

✓ ソフトウェア等の情報を自動的に収集する『IT資産管理ソフトウェアの導入』
⇒脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応

✓ 情報へのアクセス制御機能として、『デジタル著作権管理による方式』を導入
⇒万が一ファイルが外部に流出しても、オンプレミス※／クラウドを問わず記録された内容の漏洩を防止し、ダメージを無効化

※ オンプレミス：[情報システムのハードウェアを自ら調達し主体的に管理する運用形態]

2. 政府機関等のサービスの利用者の側に立った対策

≪主な内容≫

✓ 『政府機関等の全ウェブサイトの常時暗号化』の義務化を新設
✓ 『電子メール通信の暗号化対応』の義務化を新設

利用者の通信相手（ウェブサイト、メールの送信元）が真に政府機関であることを保証するとともに、通信途中での盗聴／改ざん／なりすましの防止を可能とし、国民の安心感を醸成

4. 改定の概要2

資料4－1

3. 政府機関等の自律的な能力向上への誘導（PDCA サイクルの効果的運用）

≪主な内容≫

- ✓ 『情報セキュリティ対策の運用、自己点検、教育等』の取組において発生した課題をCISO※等責任者に報告させる規定を整備 **⇒責任者への報告を通じ、自らの課題の認識と、これに対する対応方針の検討を誘発し、自律的改善スパイラル（PDCAサイクル）を効果的に機能させる**
- ✓ CISOから、組織横断的及び部門特有の改善事項を、それぞれ適切な責任者に指示する規定を整備
  ⇒改善事項について、組織横断的取組及び部門特有の取組を、それぞれ効果的に推進させる
- ✓ 従来の責任者を中心に役割を規定していたことに加え、政府機関等の実情も踏まえ、情報セキュリティ対策の推進を担う部門を「情報セキュリティ対策推進体制」と位置付け、その役割を明確化
  ⇒マネジメントの更なる円滑な推進を促進

※CISO：[最高情報セキュリティ責任者 Chief Information Security Officer]

4. 業務形態に対応した規定の整備

≪主な内容≫

- ✓ モバイル端末の利用について、一定の安全対策を講じた場合には、組織内外のいずれにおいても端末をネットワーク接続して業務を行うことを可能とする規定を新設
  ⇒府省庁とは異なる独立行政法人等の柔軟な業務形態を支援すべく、統一基準群において、モバイル端末の柔軟な使用についての道を開拓
- ✓ 政府ドメイン名（go.jp）の使用に関する規定を見直し（『教育機関である法人における高等教育機関向けドメイン名（ac.jp）の使用に係る規定』を整備）
  ⇒独立行政法人において、業務の特性等に応じたドメイン名の選択を可能に

5. その他の見直し事項

≪主な内容≫

- ✓ IoT機器が統一基準群の規定の対象であることを明確化するとともに、安全対策に係る規定を追加
  ⇒一般の情報システムに加え、IoT機器にも防御の幅を広げる

資料４－２

政府機関等の情報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　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

（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。）第二十五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情報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 27000:2014 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（約款による外部サービスの利用を除く。）を実施する場合は、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、要機密情報を約款による外部サービスを利用して取り扱ってはならない。
４　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４－３

政府機関等の情報セキュリティ対策のための統一基準（案）
（平成 30 年度版）

平成 30 年　月　日

サイバーセキュリティ戦略本部

目次

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、政府機関等の情報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、機関等は統一基準適用個別マニュアル群を踏まえ、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。）に定める秘密文書に相当する機密性を要する情報を含む情報 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。

● 「委託先」とは、外部委託により機関等の情報処理業務の一部又は全部を実施する者をいう。

【か】

● 「外部委託」とは、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。「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。

● 「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。

● 「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。

● 「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。

【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 27000:2014 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、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。

【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。

● 「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】

● 「約款による外部サービス」とは、民間事業者等の外部の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする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除く。

● 「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、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。

(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。

(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。

(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　外部委託

4.1.1　外部委託

目的・趣旨

機関等外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、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。

外部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外部委託の契約時には、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、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、4.1.4「クラウドサービスの利用」についても本款に加えて遵守する必要がある。

＜外部委託の例＞

- 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）
- 情報システム、データセンター、通信回線等の賃貸借

遵守事項

(1) 外部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、外部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) 外部委託に係る契約

(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外部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、外部委託

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) 外部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) 外部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。

4.1.2 約款による外部サービスの利用

目的・趣旨

外部委託により業務を遂行する場合は、原則として 4.1.1「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、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は、民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3「用語定義」において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を機関等からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、4.1.1「外部委託」を適用するのではなく、本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) 約款による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、以下を含む約款による外部サービスの利用に関する規定を整備すること。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） 約款による外部サービスを利用してよい業務の範囲

（イ） 業務に利用できる約款による外部サービス

（ウ） 利用手続及び運用手順

(b) 情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。

(2) 約款による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約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

4.1.3 ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。機関等においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。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は、.go.jp で終わるドメイン名（以下「政府ドメイン名」という。）を使用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。

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の利用は、約款による外部サービスの利用に相当することから、4.1.2「約款による外部サービスの利用」の規定と同様に、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し、4.1.1「外部委託」及び 4.1.2「約款による外部サービスの利用」を適用するのではなく、本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

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) 情報セキュリティ責任者は、機関等において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。

(c) 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。

4.1.4 クラウドサービスの利用

目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド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。

クラウドサービスを利用する際、機関等がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウド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、クラウドサービスでは、複数利用者が共通のクラウド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。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、機関等による委託先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考慮することが求められる。

遵守事項

(1) クラウドサービスの利用における対策

(a) 情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。

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

(c) 情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。

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

(e) 情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

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・保守を外部委託する場合については、4.1「外部委託」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（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。

(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外部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外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書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・保守を外部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・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用され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・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させること。

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、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。

(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。

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。

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）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・提供を外部委託する場合については、4.1.1「外部委託」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) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

(b) 職員等は、アプリケーション・コンテンツの開発・作成を外部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) 4.1.3 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外部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。

端末については、サーバ等の他の情報システムの構成要素と異なり、機関等の判断によっては機関等支給以外のものの利用があり得る。機関等における業務で端末を利用する以上は、機関等により支給されたものか、それ以外かにかかわらず、同等の情報セキュリティ水準が求められる。このため、本款及び 8.1.1「情報システムの利用」での端末に係る規定においては、両者を対象としている箇所がある。この際、両者を区別して「機関等が支給する端末」、「機関等支給以外の端末」と表現している。単に「端末」という場合は、1.3「用語定義」において定義されているとおり機関等が支給するものを指す。

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) 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）及び機関等支給以外の端末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、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）及び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) 機関等支給以外の端末において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

(b) 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。

(c) 次の各号に掲げる責任者は、職員等が当該各号に定める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(a)(ア)の安全管理措置を講ずること。

(ア) 情報システムセキュリティ責任者　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）

(イ) 端末管理責任者　機関等支給以外の端末

(d) 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(a)(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(a)(イ)に定める安全管理措置を職員等に講じさせること。

(e) 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(a)(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(a)(イ)に定める安全管理措置を講ずること。

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。仮に機関等が有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はない。

(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) リモートアクセス環境導入時の対策

(a) 情報システムセキュリティ責任者は、職員等の業務遂行を目的としたリモートアクセス環境を、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により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。

(5) 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、本款には 7.1.1「端末」と同様に、機関等が支給する端末と機関等支給以外の端末の両者を対象にしている箇所がある。また、両者を包含する場合は、「端末（支給外端末を含む）」と表現している。

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、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）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。

(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（支給外端末を含む）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) 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。

(e) 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。

8.2　機関等支給以外の端末の利用

8.2.1　機関等支給以外の端末の利用

目的・趣旨

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がある。この際、当該端末は機関等が支給したものではないという理由で、情報セキュリティ対策が講じられない場合、当該端末で取り扱われる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、その利用の可否を判断をした上で、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、機関等支給以外の端末の利用に係る情報セキュリティ対策については 7.1.1「端末」及び 8.1.1「情報システムの利用」を参照のこと。

遵守事項

(1) 機関等支給以外の端末の利用可否の判断

(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。

(2) 機関等支給以外の端末の利用規定の整備・管理

(a) 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。

(3) 機関等支給以外の端末の利用時の対策

(a) 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。

(b) 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。

資料４－４

政府機関等の情報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　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 25 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情報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。）及び政府機関等の情報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。

「政府機関等の情報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4－5

■ 実施方法：NISCのウェブページ及び電子政府の総合窓口(e-gov)に掲載して公募

■ 実施期間：2018年6月7日（木）～6月28日（木）

■ 意見総数：21者から66件【内訳：14企業・団体から延べ58件、7個人から延べ8件】

・統一規範に0件、統一基準に61件、運用指針に2件、全般に対して3件の意見提出

（1）修正意見：全63件

・表現の適正化を求めるものについて、統一基準を修正（1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（62件）

☆主な意見

・未知の不正プログラムに係る被害の未然防止／拡大防止や、IT資産管理の自動化に係る将来像を見据えた対策に関する意見（14件）

・ウェブサイトや電子メールの暗号化による利用者側に立った対策に関する意見（4件）

・PDCAサイクルの効果的運用のための体制等の整備に関する意見（8件）

（2）その他の意見：全3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15件の意見提出

解説の充実や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（8件）

（参考）提出者名：

株式会社 FFRI、CyberArk Software株式会社、スプランクサービスジャパン合同会社、株式会社テリロジー、トレンドマイクロ株式会社、日本マイクロソフト株式会社、マカフィー株式会社、一般社団法人　日本ネットワークインフォメーションセンター、特定非営利活動法人　日本セキュリティ監査協会、特定非営利活動法人　日本ネットワークセキュリティ協会、BSA｜ザ・ソフトウェア・アライアンス、迷惑メール対策推進協議会、国立研究開発法人　国立国際医療研究センター、大学共同利用機関法人　情報・システム研究機構国立情報学研究所、個人（7）

「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(案)」に対する意見募集の結果

資料4－6

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	大学共同利用機関法人 国立情報学研究所	統一基準	p.1	1.1	(2)以降は全て「適用範囲」を「適用対象」と変更しているので、本標題も変更すべきではないか。	御指摘の統一基準1.1表題の「適用範囲」の字句は、1.1(2)「本統一基準の適用対象」のみに対応している訳ではありません。 1.1(5)「対策項目の記載事項」に記載のとおり、基本対策事項が遵守事項に対応するものであることから、ガイドラインに記載の基本対策事項も本統一基準の範囲としていることを示すため、「適用範囲」と記載しております。
2	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.6	1.3	「機関等」について下記を用語定義に追加 ● 「機関等」とは、府省庁及び独立行政法人及び指定法人の総称であり、「政府機関等」ともいう。 理由: 現行は「府省庁」なのでわかりやすいが、「機関等」だと具体的にどのような組織が含まれるのかあいまいなため。	御指摘の点に関して、統一規範第2条第2項において「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。）」と記載しており、機関等にどの組織が含まれるかは明らかと考えられます。
3	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.7 p.57	1.3 7.3.2目的・趣旨	「ネットワーク」「通信ネットワーク」については、「通信回線」に変更 理由: 「ネットワーク」「通信ネットワーク」は「通信回線」と同義であり、統一すべき	御指摘については、本改定における改定箇所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、これらの用語については遵守事項では全て「通信回線」で統一しています。他の箇所では文脈上わかりやすい表現を用いています。このため、原案のとおりとします。
4	大学共同利用機関法人 国立情報学研究所	統一基準	p.8	1.3	統一規範(案) の第ニ条2で定義されている「職員等」よりも範囲が広がっている印象を受ける。すべての組織において「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」を対象とすることが不適切な場合も考えられるため、「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めることが適切な場合も考えられる」のような記述のほうが、統一規範との整合性が高まるのではないか。	御指摘では、「すべての組織において『職員等には（中略）研修生等も含まれている』を対象とすることが不適切な場合が考えられる」とのことですが、派遣労働者、研修生等の機関等の指揮命令に服している者を職員等に含めることが不適切な場合とは、これらの者が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わない場合に限られ、統一規範第2条第2項においては「次項に規定する情報を取り扱う者とする。」、統一基準1.3用語定義においては「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。」と定めているため、両文書の「職員等」の対象の範囲は一致していることから、原案のとおりとします。

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		
5	独立行政法人 情報処理推進機構	ガイドライン	p.16	1.6	CRYPTRECに関する記述について、暗号モジュール評価基準については、現在、CRYPTRECの検討の対象になっていないため、CRYPTRECのWebページの記載にならい次のように更新すべきと考えます。 現行:「CRYPTREC(Cryptography Research and Evaluation Committees)」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。 新 :「CRYPTREC(Cryptography Research and Evaluation Committees)」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。	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なく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
6	スプランク サービス ジャパン合同会社	統一基準		第2部 第6部	新規要件の追加:第2部に「システムの監視」を記載するとともに、第6部において「システムの監視と可視化」について要件化することを推奨します。 意見理由 第6部においては個々の対策については網羅されているが、それらを一元的に監視する可視化の仕組みを基準化することが必要と考えられます。個々の対策状況(認証、アクセス制御、不正プログラム対策等)を把握する具体的な手段を基準化しなければ、管理者によるセキュリティ上の問題の把握が難しく、政府ITシステム全体のセキュリティが確保されにくいと考えます。参考までに各国で謳われている検知や報告に関する統制状況を鑑みると(GDPR:72時間以内、CDM:72時間以内)、何らかの監視と可視化の義務化、報告までの目標期限が設定されています。我が国としても同等の基準が必要と考えています。	御指摘は、本改定における改定箇所ではないため、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重要と考えており、今回のガイドラインの改定にあたり、IT資産のシステムによる管理について記載を追加しております。頂いた御指摘については、今後の検討の参考とさせていただきます。
7	個人	統一基準	p.11	2.1.1(5)(a)	(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。 に関して、最高情報セキュリティアドバイザーの専門知識及び経験を担保するために情報処理安全確保支援士または同等以上の能力を有すると認められる者(CISSP等の国際資格)から最高情報セキュリティアドバイザーを専任することを要件とするべきと考えます。	御指摘については、本改定における改定箇所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、最高情報セキュリティアドバイザーの業務内容は基本対策事項2.1.1(5)-1の例示のとおり多岐にわたることから、その能力を一定程度証明する資格の一つとして、情報処理安全確保支援士も考えられますが、これに限るものではないと考えられ、原案のとおりとします。
8	個人	統一基準	p.11	2.1.1(7)	「統一基準」中の2.1.1 (7)「情報セキュリティインシデントに備えた体制の整備」については、「NISCにおける『CYMAT』および政府機関等における『CSIRT』においては『情報処理安全確保支援士』の資格を有する職員等を必ず配置する」など、「情報処理安全確保支援士」を積極的に活用することを明示してはどうか。	CSIRT/CYMATに属する職員には、情報セキュリティ等に関する知識及び技能を有する者を充てることとしているが、それぞれCSIRT/CYMATに特化した知識及び技能に係る教育を提供しているところ、これら要員には特定の資格を求めていないため、原案のとおりとします。

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	個人	統一基準	p.11	2.1.1(5)(a) 2.1.1(7)(b)	「政府機関等の情報セキュリティ対策のための統一基準（案）」について意見を述べたい。 p10「組織・体制の整備」の項目内容において専門性を認定する具体的基準が欠けていると感じた。 特に、 ・p11.「(5) 最高情報セキュリティアドバイザーの設置」にて 『(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。』 と記載ある。また同様の表記として、 ・p11 「(7) 情報セキュリティインシデントに備えた体制の整備」にて 『(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。』 との表記がある。 双方とも「専門的な知識」を求めているが、これを認定する具体的基準が欠けているため下記内容の追加を提案する。 経済産業省の「情報セキュリティサービス基準」を参照し、このp11「４．セキュリティ監視・運用サービスに関する附則 」に例示される「情報処理安全確保支援士」などの資格を専門的知識の認定要件とすることを提案する。 この資格は政府IT入札要件、内閣官房情報通信技術(IT)総合戦略室と総務省行政管理局の定める「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第3編第6章 調達）」のP44、P91、P92にも要件として示されている。	御指摘については、本改定における改定箇所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、最高情報セキュリティアドバイザーの業務内容は基本対策事項2.1.1(5)-1の例示のとおり多岐にわたることから、その能力を一定程度証明する資格の一つとして、情報処理安全確保支援士も考えられますが、これに限るものではないと考えられ、原案のとおりとします。 また、CSIRTに属する職員には、情報セキュリティ等に関する知識及び技能を有する者を充てることとしているが、CSIRTに特化した知識及び技能に係る教育を提供しているところ、これら要員には特定の資格を求めていないため、原案のとおりとします。
10	東日本高速道路株式会社	ガイドライン	p.21 p.25	2.1.1(1)(b) 2.1.1(4)(a)	統一基準2.1.1(1)(b)最高情報セキュリティ副責任者と2.1.1(4)(a)統括情報セキュリティ責任者の違いについて。今回の改定で最高情報セキュリティ副責任者を必要に応じておくことができるように規定され、業務を見ると「最高情報セキュリティ責任者を助けて．．．」と記載されています。一方以前からある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を補佐する者．．．」と記載されています。助けると補佐は同義語なので、この両者の業務の違いがはっきりと理解できません。最高情報セキュリティ副責任者と統括情報セキュリティ責任者の違いをガイドラインで業務の具体例を明示しながら明記していただけないでしょうか。	最高情報セキュリティ責任者の役割は、遵守事項2.1.1(1)(a)において「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」ことと規定しており、ここで「事務を統括する」とは、ガイドラインの解説「遵守事項2.1.1(1)(a)『最高情報セキュリティ責任者』について」に記載のとおり、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することを意味しますが、これら最高情報セキュリティ責任者の所掌する事務を分掌することが、最高情報セキュリティ副責任者の役割となります。 一方、統括情報セキュリティ責任者の役割は、ガイドラインの解説「遵守事項2.1.1(4)(a)『統括情報セキュリティ責任者』について」に記載のとおり、「機関等の情報セキュリティ対策について総合調整する事務を担う」ことであり、ここで「総合調整する事務を担う」とは、機関等における具体的な情報セキュリティ対策を取りまとめることを意味します。 以上のことから、最高情報セキュリティ副責任者と統括情報セキュリティ責任者の役割は明確に異なることから、原案のとおりとします。

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		
11	独立行政法人 情報処理推進機構	ガイドライン	p.40 p.42	2.1.2(1)(a)解説	JIS の用語に基づいて、JISについて、X章としている部分は、箇条Xと改めるべきと考えます。 現行：JIS Q 31000:2010, 5章 新　：JIS Q 31000:2010, 箇条5	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、御指摘を踏まえ修正します。
12	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(1)(b)	最高情報セキュリティ副責任者は、最高情報セキュリティ責任者の命を受けてにしても、事務を「統括」すると定めるのは不適切ではないか。ガイドラインに示されている副責任者設置の趣旨を踏まえると、「統括を補佐する」「統括業務を分担する」程度の書き方が適切ではないか。また、最高情報セキュリティ副責任者の役割として、最高情報セキュリティ責任者に事故があった場合（緊急時にその役割を担うことが困難な場合を含む）に最高情報セキュリティ責任者の役割を代行することも定めるべきではないか。	最高情報セキュリティ副責任者の役割は、最高情報セキュリティ責任者の所掌する事務を分掌することであることから、最高情報セキュリティ責任者の規定（遵守事項2.1.1(1)(a)）と同様の「事務を統括する」という表現を用いております。 また、最高情報セキュリティ副責任者の役割は、各組織において、最高情報セキュリティ責任者が、最高情報セキュリティ副責任者へ命を与えることにより決まることから、統一基準に規定する必要はないと考えております。
13	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(2)(a)	情報セキュリティ対策推進体制は、対策基準等の(審議)策定とも密接な関係を持つと考えられるため、(2)の情報セキュリティ委員会の役割と統合する規定として、次のように修正してはどうか。 「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の整備ならびに対策基準等の審議を行う組織として、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。」	情報セキュリティ対策推進体制の役割は、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ことであり、一方、情報セキュリティ委員会の役割は、情報セキュリティに係る組織横断的な事項を審議することです。したがって、両者は役割が異なるため、原案のとおりとします。
14	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(4)(a)	機関の実態等を鑑みて、統括情報セキュリティ責任者は最高情報セキュリティ副責任者と兼務できる規定にしてはどうか。	最高情報セキュリティ副責任者の役割は最高情報セキュリティ責任者の所掌する事務を分掌することであり、一方、統括情報セキュリティ責任者の役割は機関等における具体的な情報セキュリティ対策を取りまとめることであることから、両者は役割が異なります。また、遵守事項2.1.1(1)(b)において最高情報セキュリティ副責任者は必要に応じて置くことと規定しており、機関等において必ず設置される役職ではありません。これらを踏まえると、最高情報セキュリティ副責任者と統括情報セキュリティ責任者の兼務についてあらかじめ規定しておくことは適切とは考えられないため、原案のとおりとします。
15	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.10	2.1.1(1)(b)	「最高情報セキュリティ副責任者１名を必要に応じて置くこと」とされているが、組織の事情によっては副責任者を2名以上置くのが適切な可能性もあると思われるので、「最高情報セキュリティ副責任者１名以上を必要に応じて置くこと」とすべきではないか。	御指摘の点につきましては、各行政機関におけるサイバーセキュリティ担当の幹部職員の配置状況の実態に鑑み、これを統一基準に反映したものであるため、原案のとおりとします。

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		
16	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.29	4.1.4	我々は特にクラウドサービスの利用に関する箇所（第 4 部「外部委託」 4.1.4「クラウドサービスの利用」）において、クラウドサービスを利用する場合にはセキュリティリスクが高くなると解釈されかねないことを懸念します。当該箇所の記述は、オンプレミスのITシステムと比較してクラウドコンピューティングのリスクが高くなるのではないかという印象を与え、誤解を招きかねません。また、プライベートクラウド、パブリッククラウド、ハイブリッドクラウドなど様々なクラウドサービスモデルを考慮に入れることも重要であり、オンプレミスシステム同様、具体的なリスクは、どのような状況で使用されるかに基づいて評価されなければなりません。	御指摘の箇所は、本改定における改定箇所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利用において、検討しなければならないことや契約に定める要件等を定めており、セキュリティリスクについてクラウドサービスをオンプレミスの情報システムと比較して論じているわけではありません。
17	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.29	4.1.4(1)(b)	4.1.4「 遵守事項(1)(b)」において、委託業務の実施場所に関する記述も修正した方が良いと考えます。クラウドサービスプロバイダーが、準拠法に従いデータを安全・適切に扱うことを保証することができれば足り、本基準群において委託事業の実施場所の指定を求める必要はないと考えます。日本政府はクラウドコンピューティング利用を促進しようとされていますが、その一方で、このような記載をすれば、クラウドコンピューティング技術やサービスの導入が阻まれてしまうことになります。	御指摘の箇所は、本改定における改定箇所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利用契約において準拠法が合意されている場合でも、サーバが国外にある場合に、国外法が適用されるケースが想定されるため、実施場所も併せて指定することは有効な規定であると考えており、原案のとおりとします。
18	マカフィー株式会社	統一基準	p.29	4.1.4(1)(a)	変更案: (a)情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すると共に委ねた情報に対して適切な取扱制限を実施すること。 理由: 重要な情報を委ねることの可否に加えて、委ねると判断した後にクラウドサービスへ保存される情報に対して適切な対策を実施していくことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所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、クラウドの利用におけるセキュリティ対策は、遵守事項4.1.4(1)(d)に規定し、具体的な対策は、基本対策事項4.1.4(1)-2に記載しているため、原案のとおりとします。
19	マカフィー株式会社	統一基準	p.29	4.1.4(1)(b)	変更案: (b) 情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定することが望ましい。 理由: 「委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること」という記載により、クラウドサービス事業者選定の幅が狭まるため、表現の緩和が必要と考えます。	御指摘の箇所は、本改定における改定箇所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、4.1.4「クラウドサービスの利用」は、クラウドサービスのセキュリティを確保するため、利用における対策を規定しているものであり、ご指摘の「クラウドサービス事業者選定の幅が狭まるため、表現の緩和」については、統一基準の本旨にそぐわないため、原案のとおりとします。
20	マカフィー株式会社	統一基準	p.29	4.1.4(1)(b)	変更案: (b) 情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定すること。 理由: 「委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること」という記載により、クラウドサービス事業者選定の幅が狭まることが想定されます。	御指摘の箇所は、本改定における改定箇所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利用に当たっては、その委託先で機関等の情報が適切に取り扱われることが重要であるため遵守事項4.1.4(1)(b)「クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。」が必要と考えており、原案のとおりとします。

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		
21	マカフィー株式会社	統一基準	p.29	4.1.4(1)(c)	変更案: (c) 情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、利用するサービスを選定する際の要件とすること。 理由: クラウドサービスの活用を考えていく上で、「委託」という考えが適合し難いと考えます。	御指摘の箇所は、本改定における改定箇所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、利用するサービスを含めた委託先を選定する際の要件として記載しているため、原案のとおりとします。
22	マカフィー株式会社	統一基準	p.29	4.1.4(1)(d)	変更案: (d) 情報システムセキュリティ責任者は、クラウドサービスの特性である「共同責任モデル（責任共有モデル）」を理解し、4.1.4(1)(a)基づく情報の格付けに応じて、利用者側が実施できるセキュリティ対策について検討し要件を定めること。また、自機関が認可したクラウドサービス以外が利用されていないかを監視する仕組みもその要件に含むこと。 理由: クラウドという環境において、情報の流通経路全般を見渡しセキュリティ設計を行うことは、クラウドサービス利用者においてはほぼ不可能に近いと考えます。4.1.4の目的・趣旨の8行目以降の記載にある「また、クラウドサービスでは、～困難である」と本項目は乖離があるように思われます。クラウドサービス利用の特性を理解する上では、一般的には「共同責任モデル（責任共有モデル）」という考え方を述べた方が適切と考えます。	御指摘の箇所は、本改定における改定箇所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、クラウドサービスとオンプレミスでは異なる特性があることから、情報の流通経路全般を俯瞰してセキュリティ対策を講ずる必要があり、4.1.4(1)(d)にこれを記載しております。また、「自機関が認可したクラウドサービス以外が利用されていないかを監視する仕組み」については、遵守事項7.3.1(1)(h)において、「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。」と定めており、さらに基本対策事項8.1.1(2)(a)においてウェブサイトフィルタリング機能を例とした「職員等が閲覧できる範囲を制限する機能を情報システムに導入すること」を求めているため、原案のとおりとします。
23	マカフィー株式会社	統一基準	p.29	4.1.4(1)(e)	変更案: (e) 情報システムセキュリティ責任者は、クラウドサービス利用検討時の及び、利用後において各クラウドサービスに関する安全性の格付け情報を収集すること。利用するサービスの信頼性が十分であるかを第三者機関の評価に基づき定期的にスクリーニングし利用の検討や、利用の継続を判断すること。 理由: クラウドサービスにおいては、個々の利用者が個別にクラウド事業者の安全性を確保するために監査等を行よりも、信頼できる第三者機関の評価を定期的に入手し確認することが重要と考えます。CSA（Cloud Security Alliance）などが求めるセキュリティ基準を満たしているかなど標準化された指標での評価を入手できることが必要と考えます。	御指摘の箇所は、本改定における改定箇所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、ご指摘の第三者機関の評価については、ガイドラインの解説4.1.4(1)(e)「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること」について」において、既に第三者による監査／認証等を活用することとしており、原案のとおりとします。
24	マカフィー株式会社	統一基準	p.29	4.1.4(1)(f)	追加案: (f) 情報システムセキュリティ責任者は、クラウドサービス利用する場合は、自機関の利用者に起因して起きるセキュリティインシデントにも留意しセキュリティ対策を講じること。 理由: 4.1.1には、事業者がセキュリティインシデントを起こした場合、もしくはその危険性については備えるように言及しているが、自機関における利用者に起因した事案（アカウント情報の漏洩）への言及がされていません。クラウドサービス利用においては、この点に備えるように言及すべきであると考えます。	御指摘の箇所は、本改定における改定箇所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、御指摘の利用者に起因するセキュリティインシデント（アカウント情報の漏えい）の対策として、遵守事項8.1.1(5)にて識別コード・主体認証情報の取扱いに係る対策を記載しているため、原案のとおりとします。

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		
25	マカフィー株式会社	統一基準	p.29	4.1.4(1)(f)	追加案: (f)情報システムセキュリティ責任者は、自身が認知・許可していないクラウドサービスが使用されていないことを定期的に確認し、使用されている場合には適切な対策を実施すること。 理由: 情報システム担当が許可しているクラウドサービスでは無いもの(シャドーIT)が使用されていることが大きな課題になっており、遵守事項として明記する必要があると考えます。	御指摘の箇所は、本改定における改定箇所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7.3.1(1)(h)において、「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。」と定めており、さらに基本対策事項8.1.1(2)-1においてウェブサイトフィルタリング機能を例とした「職員等が閲覧できる範囲を制限する機能を情報システムに導入すること」を求めているため、原案のとおりとします。
26	日本マイクロソフト株式会社	統一基準	p.25	4.1.1(2)(b)	クラウドサービスの提供において、左記に関する規格や認証の取得の証明により、上記にかかる情報提供は不要として頂きたい。 理由: 専門機関による第三者の監査結果によって、クラウドサービス提供上、十分なセキュリティ対策が講じられているか確認しうると考えるため。	御指摘の箇所は、本改定における改定箇所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4.1.1(2)(b)において定めている事項は、情報セキュリティ責任者が情報システムの運用等を外部委託する際に、情報システムの特性も踏まえ実施すべき情報セキュリティ対策について規定しているものであり、クラウドサービス事業者が自ら取得する第三者の認証により確認される事項とは必ずしも合致するものではないため、原案のとおりとします。
27	日本マイクロソフト株式会社	統一基準	p.26	4.1.1(2)(c)(ア)	クラウドサービスの利用においては、信頼に足る第3者監査機関によるクラウドサービスに対する監査結果をもって、代替できることとして頂きたい。 理由: 専門機関による第三者の監査結果によって、クラウドサービス提供上、十分なセキュリティ対策が講じられているか確認しうると考えるため。	御指摘の箇所は、本改定における改定箇所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4.1.1(2)(c)(ア)の規定は、外部委託において、平常時だけではなくインシデント発生時などの必要性が生じた時に機関等自らが監査する場合も含まれることから、必ずしも第三者監査機関による監査結果によって代替できるものではないため、原案のとおりとします。
28	国立研究開発法人 国立国際医療研究センター	統一基準	p.26	4.1.1(2)(c)	情報セキュリティ監査の受け入れについて 独立行政法人の業態は多岐にわたるため、各独立行政法人に対して、外部委託している業者全てに対して情報セキュリティ監査を行うことは技術的にも人的にも困難である。また受け入れる業者側も、多くの顧客から監査を受け、内部の情報や体制を晒すこととなり、却って業者自身のセキュリティを下げることや、監査対応で著しく業務効率を下げることが予想される。 情報セキュリティ監査を受けた実績の報告で代替する等の対応を検討いただき、業態によっては(特に病院等の業務が多岐にわたり多数の外部委託を実施している法人など)この方法で許可する旨の文言を追加いただきたい。	御指摘の箇所は、本改定における改定箇所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4.1.1(2)(c)(ア)の規定は、「必要に応じた」ものであり、全ての外部委託先の情報セキュリティ監査を必ず実施しなければならないとするものではないため、原案のとおりとします。

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	個人	統一基準	p.29	4.1.4	クラウドシステム等の提供場所（提供ホスト所在国）についても注意するよう周知を行っていただきたい。（金融庁、財務省、国税庁等の各種ホストが香港やシンガポールにあるものによって提供されているのであるが、国民による個人情報や他機密ともすべき様な内容を含む意見提出や通報等をこれらに提出させるのか、という話である（フィンテック？聞いて呆れる。）。政府として止められたい。） また、名前解決のエリアスにより、*.go.jpとなっているホスト名を海外のサーバによって提供しないようにしていただきたい。	御指摘の箇所は、本改定における改定箇所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利用に当たっては、その委託先で政府機関の情報が適切に取り扱われることが重要であり、遵守事項4.1.4(1)(b)「クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。」と定めております。
30	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.30	5.1.1(1)	「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。」は文として不自然である。下記に修正すべき。 「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をとりまとめた情報システム台帳を整備すること。」	御指摘の箇所は、本改定における改定箇所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、当該情報システムのセキュリティ要件に係る事項を情報システム台帳として整備する趣旨としており、誤解が生じるものではないと認識していることから、原案のとおりとします。
31	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.32	5.2.1(2)(a)	5.2.1 の「情報システムの企画・要件定義」における「遵守事項(2)(a)」において、セキュリティ対策として「インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離」することが提案されていることに懸念があります。インターネットから分離すれば、リアルタイムでセキュリティ・アップデイトを受けられるという利点が阻まれ、却ってリスクが増大しかねません。	御指摘の箇所は、本改定における改定箇所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、ガイドラインの解説「遵守事項5.2.1(2)(a)『インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する』について」に記載のとおり、特に重要な情報を取り扱う情報システムについてインターネットからの分離が求められる旨の考え方を示したものであり、情報システム全般について一律に分離を求めるものではなく、分離によるメリット、デメリットを総合的に判断した上で、分離の要否を判断することを求めています。したがって、御懸念の点も判断の要素に含まれております。

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		
32	一般社団法人 日本ネットワークインフォメーションセンター	統一基準	新規	5.2	ドメイン名の活用におけるライフサイクルの考慮について 情報システムのライフサイクルを考慮する際、ドメイン名のライフサイクルについても考慮が必要です。既存システムについても、日本の政府機関や各省庁所管の研究所、特殊法人、独立行政法人のみが登録可能なgo.jpドメイン名への移行により、ドロップキャッチを防止することができます。加えてこれまで利用した過去のgo.jpドメイン名以外のドメイン名の利用停止の際には、そのドメイン名を直ちに登録解除するのではなく、問題のなくなる期間までドメイン名を保持することで、ドロップキャッチを防止できます。 第5部 情報システムのライフサイクル、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、において、次の通り提案します。 イ.「go.jpドメイン名ではないドメイン名を使用する政府機関等のシステムはgo.jpドメイン名への移行を推奨すること。go.jpドメイン名への移行後の旧ドメイン名については一定期間登録を維持するなど第三者による再登録への対策を採ること。」を追記する。 ロ.「go.jpドメイン名の使用ができず他のドメイン名を使用する場合は、使用後も一定期間登録を維持するなど第三者による再登録への対策を採ること。」を追記する。	御指摘については、本改定における改定箇所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は、政府部内においては、「Webサイト等の整備及び廃止に係るドメイン管理ガイドライン（2018年3月30日 各府省情報化統括責任者（CIO）連絡会議決定）」に規定されております。また、統一基準においても、遵守事項 6.3.2(1)(a) にて、政府ドメイン名の使用に関する規定を設けており、さらに、ガイドラインの解説「遵守事項6.3.2(1)(a)『政府ドメイン名を情報システムにおいて使用する』について」において、「仮に政府ドメイン名以外を使用した場合には、そのサイトの使用を終了した後も、当該ドメイン名を不正に利用されないように登録管理を一定期間維持しなければならない」ことを示しています。
33	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.33	5.2.1(2)(a)(イ)	「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」とされているが、暗号化されている情報を監視環境において復号することが困難な場合も多いので、「監視するデータが暗号化されている場合は、可能な範囲で必要に応じて復号すること」としてはどうか。	復号の必要性を判断するに当たっては、暗号化されたデータを復号できるか否かについても踏まえることを想定しており、原案のとおりとします。
34	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.33	5.2.1(4)(b)	「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」との記述内容がやや理解しにくいので、「当該対策による情報システムの変更内容について、変更が発生次第速やかに報告させること」としてはどうか。	御指摘の記載については、変更が発生した場合は、遅滞なく報告させるものとして記載しているものであり、誤解が生じるものではないと認識していることから、原案のとおりとします。
35	スプランクサービスジャパン合同会社	統一基準	p.40	6.1.4(1)(a)	6.1.4(1) (a)に「サーバ、ネットワーク及びクライアントに関する必要なログを取得すること」と明記の検討を推奨します。 意見理由 ガイドラインにはサーバー・ネットワーク等のログ取得の記載はあるが、クライアントについての記載は見受けられません。また、どのログを取得すべきかはガイドラインではなく、統一基準として明確に定めることを推奨します。特にクライアントログは重要であると考えており、今日のセキュリティ・インシデントの発生源は、70%以上がクライアントからというデータも存在します。	御指摘の箇所は、本改定における改定箇所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、端末のログを取得することも重要と考えており、6.1.4(1) (a)の情報システムには端末も含まれているため、原案のとおりとします。

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		
36	独立行政法人 情報処理推進機構	ガイドライン	p.191	6.1.5(1)(b)(エ)解説	遵守事項6.1.5(1)(b)(エ)「管理手順を定めること」について 情報システムとしての鍵の管理手順を1から全て情報システムセキュリティ管理者が作成することは、非常に負荷が高く複雑な作業です。現実には、鍵管理を担う製品や、鍵管理を半自動化・支援する製品が存在し、そういった製品を組み合わせて現実的で実行可能な鍵の管理手順を実施するべきと考えます。 そのため、「暗号化された情報の復号又は電子署名の～適切に管理する必要がある。」の後に、次のような記述を追加すべきと考えます。 情報システムとしての鍵の管理手順の一部であって、製品が提供する暗号鍵管理機能によって実現可能な管理手順については、これによって代替しても良い。「暗号モジュール試験及び認証制度」に基づく認証を取得している製品については、(「公開セキュリティポリシ」(non-proprietary security policy)と呼ばれる、)製品が実現する鍵の管理方針が公開されており、情報システムとしての鍵の管理手順の作成にあたってそれを参照してもよい。	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なく、また、本改定における改定箇所ではありませんが、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択することについては、基本対策事項6.1.5(1)-1c)に記載があり、また、御指摘いただいた解説については、鍵の管理手順を策定するに考慮する視点を記載しているため、原案のとおりとします。
37	独立行政法人 情報処理推進機構	ガイドライン	p.191	6.1.5(1)(b)(エ)解説	「鍵の廃棄」部分について 「廃棄」という単語によって、単に捨てるといったニュアンスが強くなってしまいますが、鍵のライフサイクルの中で求められていることは、暗号鍵が復元できないように「消去」「破壊」することです。 そのため、用語としては「鍵の消去」又は「鍵の破壊」が適切な表現と考えます。 (なお、JIS X 19790では「鍵のゼロ化」という表現を用いています。) その上で、説明として「確実に消去される仕組みが必要である」と述べていますが、仕組みがあるだけで実行されなければ問題です。 鍵を消去する状況では、何らかの情報機器に格納された状態で鍵の消去を行うわけですが、そこで想定される情報機器としてはUSBメモリ、SSD、HDD、HSMなどが考えられます。 例えば、SSD、USBメモリなどのウェアレベリングを用いたフラッシュメモリにおいては、HDDと同様の方法で情報を消去しようとしても、確実に消去されたかについては、ほとんど確認できないのが現実です。 また、HDDやSSDの媒体の不良のリスクだけでなく、コントローラが故障して、最終的に消去できなくなるリスクも考慮に入れるべきと考えます。PCをリース、レンタルしている場合、コントローラが故障して代替手段として磁気的に消去しようとしても、契約によって禁止されている場合もあります。 以上から、説明文に次のような記述を追加すべきと考えます。 鍵を格納する機器を廃棄又は返却する場合に備えて、鍵を確実に消去する機能が備わっている機器を選定・調達し、その機能を実行する運用が必要である。「暗号モジュール試験及び認証制度」に基づく認証を取得している製品は、鍵を確実に消去する機能が備わっている。 鍵を確実に消去する機能が備わっていない機器に鍵を格納している場合には、代替となる消去方法を検討し実行する必要がある。	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なく、また、本改定における改定箇所ではありませんが、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択することについては、基本対策事項6.1.5(1)-1c)に記載があり、また、御指摘いただいた解説については、鍵の管理手順を策定するに考慮する視点を記載しているため、原案のとおりとします。
38	独立行政法人 情報処理推進機構	ガイドライン	p.192	6.1.5(1)-1c)解説	基本対策事項6.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について P.191で、既に「擬似乱数」という用語を用いているため、整合性をとるために、次のように修正すべきものと考えます。 現行:疑似乱数 新　:擬似乱数	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なく、また、本改定における改定箇所ではありませんが、御指摘を踏まえ、ガイドラインを修正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		
39	独立行政法人 情報処理推進機構	ガイドライン	p.192	6.1.5(1)-1d)解説	JIS X 19790が改正されたことを受けて、JIS X 19790の用語定義と整合するよう次のように修正すべきと考えます。 現行:タンパ検出 新　:タンパー検出 現行:タンパ証跡 新　:タンパー証跡 現行:暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、外観上の表示 新　:暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、観察可能な表示 現行:タンパ応答 新　:タンパー応答 現行:暗号モジュールがタンパを検出したときにとる自動的な動作 新　:暗号モジュールがタンパーを検出したときに取る自動的な動作	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なく、また、本改定における改定箇所ではありませんが、御指摘を踏まえ、「外観上の」を「観察可能な」に修正させていただきます。 また、御指摘の部分は、JIS X 19790 の文脈に係る部分ですが、「タンパ」の用語については、ほかの箇所でも使用しており、また、統一基準全体の用語については、 JIS X 19790 の記載のみに依拠している訳ではありません。ついては、「タンパ」の用語は、統一基準上の用語の平仄の観点などから、原案のとおりとします。
40	マカフィー株式会社	統一基準	p.40	6.1.4(c)	変更案: (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、様々な機器から取得したログを相関的かつ継続的に分析する機能を設けること。また、不正侵入や不正操作等が判明した場合には、原因調査のための分析を実施すること。 理由: 「政府機関等の情報セキュリティ対策のための統一基準(平成30年度版)(案)」において、CSIRTは、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や情報セキュリティインシデントに関する関係機関との情報共有を行うことを求められています。 しかしながら、現実にこれらを可能とするためには、情報セキュリティインシデントの原因調査を迅速かつ正確に行える仕組みが必要となり、サイバー攻撃が高度化・巧妙化を鑑みると、ログ分析の重要性は年々増していると考えております。 また、「サイバーセキュリティ戦略(案)」において、情報システムのセキュリティ対策の高度化・可視化に向けた具体策として、様々な機器で発生する事象やアカウント管理情報を組み合わせた脅威分析検知と、その分析作業の自動化の有効性がうたわれているところです。 つきましては、統一基準におきましても、6.1.4(1)(c)に記載されていた「定期的に点検又は分析する機能」に加えて、インシデント発生時の原因調査を迅速に実施するために様々な機器から発生するログを相関的に分析する機能を備えるべきと考えますので、遵守事項に左記を追加することを提言いたします。 さらに、ガイドラインにおいては、機関の規模、情報システムから送出されるログ量、対象となる行政事務の機密性等に応じて、「自動化」を基本対策事項に加えていただくことについても、合わせてご検討ください。	御指摘の箇所は、本改定における改定箇所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、今後、3年間のサイバーセキュリティに関する施策の基本的方針である「サイバーセキュリティ戦略(案)」を引用していただいているように、御指摘の内容は今後の課題であると認識しています。御意見については、今後の検討の参考とさせていただきます。
41	国立研究開発法人 国立国際医療研究センター	統一基準	p.41	6.1.5(1)(c)	電子証明書の使用について 規程自体が証明書をGPKIに限定しているわけではないのは承知しているが、技術的な制限を記載するべきと考える。 例えば自己証明書を使用しない、企業認証型SSL以上の強度とする、電子政府の暗号リストから漏れた技術を使用しない、などが考えられる。	御指摘の箇所は、本改定における改定箇所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、御指摘の電子証明書に関わる必要技術面の事項については、遵守事項6.1.5(1)(b)及びガイドラインに記載していますので、原案のとおりとします。

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		
42	CyberArk Software 株式会社	統一基準	p.39	6.1.3(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し、それらが適切に利用されていることを常時監視し対応するための措置を講ずること。 理由： 組織全体で膨大な数に及ぶ管理者権限（の認証情報）を適切に管理するには、初期段階でアクセス権限を適切に設定するだけなく、その設定が当初のルールに則った形で適正に利用されていることを常時確認することが必要です。適正な利用を人手で常時確認することは膨大な工数がかかりますが、最新の管理者権限ソリューションなどのツールを利用することで、24時間365日適正な利用を監視することが可能です。また、不正が疑われる利用あった場合は予め設定した対処を自動で実施することができます。実際、米国の国土安全保障省が主導するCDM(https://www.dhs.gov/cdm)Phase2では、政府機関全体の管理者権限を一元管理できる統合基盤を導入し、管理者権限の適切な設定と、その後適正な利用を常時監視する仕組みを実現しています。シンガポール政府も、同様の目的で特権アカウント統合管理基盤の導入を急ピッチで進めています。日本におきましても、国の機密情報や国民の個人情報を取り扱う機関においては、同様の取り組みを実施すべきと考えます。	御指摘の箇所は、本改定における改定箇所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、情報システムの状態のリアルタイムでの把握は重要と考えており、御意見については、今後の検討の参考とさせていただきます。御指摘の点については原案のとおりとします。
43	CyberArk Software 株式会社	統一基準	p.40	6.1.4	(c)情報システム責任者は、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。国の機密情報や国民の個人情報を取り扱う機関においては、重大セキュリティ事故に直結する可能性が極めて高い管理者権限を持つアカウントのアクセスログ、操作ログについて、その影響の大きさから鑑み、リアルタイムに点検または分析を実施し、悪意ある第三者等からの不正侵入・不正操作への対策を講じること。 理由： 米調査会社のForrester社が実施した調査によると、サイバー攻撃の80%において管理者権限を有するアカウント情報が窃取・悪用されています。攻撃者は、高権限を持つ管理者アカウントを搾取した上で、情報の搾取、改ざん、システム停止などの目的を遂行することが常套手段となっており、管理者権限を有するアカウントのログインログや操作履歴などは、他のログに比べ不正侵入や不正操作の発見に対し大きく寄与するものと考えます。また、サイバー攻撃による被害の防止・最小化の観点より、いかに早くその兆候・事実を検知し、対策を行うことが非常に重要です。そのため、管理者権限に関わるログの点検・分析の頻度を、定期的ではなくリアルタイムで実施可能な仕組みを構築することが望ましいと考えます。	御指摘の内容は、本改定における改定箇所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、ログの点検及び分析の作業の自動化についてガイドライン 基本対策事項 6.1.4.(1)-5に記載されています。よって原案のとおりとします。
44	CyberArk Software 株式会社	ガイドライン	p.185	6.1.4(1)-5	加筆 b)ログ情報をソフトウェア等により集計し、下記を例とする不正侵入や不正操作、誤操作等の情報セキュリティインデント及びその予兆の検知と通知の自動化 ・リアルタイムに事前に定義された手順以外での管理者権限利用(ログイン)を検知し通知する ・リアルタイムに未知の特権アカウントからのアクセス(ログイン)を検知し通知する ・リアルタイムにブラックリストコマンドの実行を検知し、ブロックする ・リアルタイムに、通常と大きく異なる時間帯・IPからの管理者権限利用(ログイン)を検知し通知する 理由： 悪意のある第三者等による不正侵入や不正操作、誤操作等の被害を最小化するためには、怪しい挙動をリアルタイムに検知した上で、迅速に対応策を講ずることが重要です。 最新の技術動向を踏まえると、事前に想定された操作手順やアクセス形態、または通常の振舞いと異なる形で管理者権限が利用されていると思われる操作などを、リアルタイムに捕捉することは十分可能です。国の機密情報や国民の個人情報など重要性の高いデータを取り扱う機関では、管理者権限の不正利用をリアルタイムに検知できる仕組みの導入が必要と考えます。	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なく、また、本改定における改定箇所ではありませんが、御指摘の内容は基本対策事項へ記載する内容としては詳細すぎることから、原案のとおりとします。御意見については、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	株式会社テリロジー	統一基準	p.42	6.2.1	1)脆弱性対策については定期的な確認のみを定めているが深刻な脆弱性（CVSSスコア9以上など）が周知された場合、脆弱性を持つ資産の特定、および外部回線を通じての攻撃の可能性の解析を速やかに実施し、脆弱性対策を実施すべき。	1) 御指摘の内容は、本改定における改定箇所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、脆弱性を持つ資産に対する速やかな対応は重要と考えており、今回の改定にあたり、ガイドラインにてIT資産管理ソフトウェアの導入による効率的な情報収集や脆弱性対策の実施を記載してます。よって原案のとおりとします。
46	株式会社テリロジー	統一基準	p.42	6.2.1	2)ソフトウェアだけではなく、OS、ミドルウェアなどプラットフォームの脆弱性についても対策を講じるよう、記述を追加すべき。	2)脆弱性対策を行う対象となるソフトウェアについては、 1.6 一般用語の解説に記載しているとおり、ソフトウェアだけでなく、OSやOS上で動作するアプリケーションを含む広義の意味としています。
47	株式会社テリロジー	統一基準	p.42	6.2.1	3)守るべき資産を特定し、対応の優先順位づけを行い、やるべきことを明確にするといった一連の流れをネットワーク脆弱性監査製品やプラットフォーム脆弱性診断製品との連携・連動により、システマイズすべきではないか。	3) 御指摘の内容は、本改定における改定箇所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、各政府機関等がリスク評価により判断するものであると考えております。リスク評価については、遵守事項2.1.2(1)(a)、2.1.2(2)(a)に記載しております。 よって原案のとおりとします。
48	株式会社テリロジー	統一基準	p.42	6.2.1	4)通信回線装置の製造時や流通経路で不正なソフトウェアを混入した偽装デバイスが海外では発見されている（Router Firmware Tampering）。 このようなケースでは、一般的なセキュリティ対策製品では検知する方法がなく、DC、AC、EMI（電磁妨害）、音響などサイドチャネルのデータをセンサーで収集し、異常値検知を行うことにより不正機器の検知を可能にする。 このような不正なソフトウェアを混入した偽装デバイスへの言及が必要だと考える。	4)御指摘の内容は、本改定における改定箇所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、サプライチェーン・リスクへの対応については遵守事項5.1.2に記載しております。 御指摘の内容は具体的な対応方策についてですが、統一基準の遵守事項には、遵守すべき基本原則について記載することとしているため、原案のとおりとします。
49	株式会社テリロジー	統一基準	p.42 p.44	6.2.2 6.2.4	1)不正プログラムや攻撃が検知された場合には可及的速やかに当該端末を通常の通信経路から隔離する処置を講ずるべき。 2)万が一、セキュリティインシデントが発生してしまった場合の事後対策についての記述をすべき。 パケットキャプチャ装置などによるネットワーク・フォレンジック、PCなどの端末に関してはコンピュータ・フォレンジック（EDR等）をシステムを導入し、追跡査証の仕組みを備えるべき。	1)御指摘の箇所は、本改定における改定箇所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、標的型攻撃時の端末の隔離に係る対策は、ガイドラインの基本対策事項7.3.1(5)-1 g)「不正プログラム感染を認知した場合の対処手順」に記載しております。 また、2)セキュリティインシデントの対処としては、統一基準　2.2.4「情報セキュリティインシデントへの対処」として記載しています。頂いた御指摘については、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		
50	トレンドマイクロ株式会社	統一基準	p.43	6.2.2(1)(c)	意見内容：記述の追加を行うべきと考えます。 (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、新たな対策の導入に際しては運用上の負荷に配慮しながら、必要な対処を行う事 理由： 政府機関等の対策基準策定のためのガイドライン（案）を見る限り、未知の不正プログラム対策の強化に強い方向性を含んでいるにも拘らず、遵守事項に何らの変更も加えられておらず、統一基準としての意図が十分に伝わらない可能性が有るものと思われます。 　未知・既知という分類自体が曖昧な定義で有る為、その記述を追記する事に意味は無いと思いますが、継続的に新しい攻撃手法が編み出される標的型攻撃との関連性が強い不正プログラムに対しても、新たな対策を継続的に検討し続ける必要性を意識してもらう必要が有るように思います。 　また、今回ログの監視の重要性を強く押し出している事は、セキュリティが製品を入れるだけではなく、既存対策も含め製品を適切に運用する事の重要性を示唆していると考えます。さらにガイドラインにおいても端末やサーバへの負荷により業務に影響を与える可能性について言及している為、製品の導入と運用上の負荷をバランスさせる事を意識してもらう必要も有るように思います。 高度化する標的型攻撃の入り口となる不正プログラムは巧妙化し、より積極的に検知しなければならない現状と、それに伴う過検知により業務に影響を与えるリスクを高いレベルでバランスする賢い対策が今後も必要とされていくと思われます。	御指摘の箇所は、本改定における改定箇所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、不正プログラム対策ソフトと運用上の負荷のバランスについては、今回の改定においてガイドラインの解説「基本対策事項 6.2.2.(1)-1『既知及び未知の不正プログラムの検知及びその実行の防止を有する』について」に記載されています。また、未知の不正プログラム対策については、基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨及び遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。
51	株式会社FFRI	統一基準	p.43	6.2.2	－該当箇所 目的・趣旨に記載の「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」部分および、その遵守事項 －意見内容 参考資料の「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見直し（案）について」1ページ目によると、「情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止」とあるのが今回の改訂の概要となっており、実際に参考資料のガイドライン案もその趣旨に沿った修正案となっている。 しかし、統一基準ではこの趣旨が説明されていないため、目的・趣旨の最後の文を今回の趣旨に沿って具体的に記載する必要がある。このままの記載であるとH28版当時の古い対策と同様の対策でも問題ないという誤解を与える可能性があるため危険である。そこで、例えば「情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止および拡大防止を行うことが必要である」といった形で記載をより具体化することで、趣旨を変えることなく目的を明確化し、さらに他の文書との整合性を取ることもできると考える。 なお、遵守事項にも同様の趣旨の更新が必要であると考える。	御指摘の箇所は、本改定における改定箇所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、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨及び遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。

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		
52	マカフィー株式会社	統一基準	p.42	6.2.1(1)(b)	変更案: 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、当該対策を実施し、脆弱性の悪用を遮断(遮断が困難な場合は検知)する措置を講ずること。 理由: 多重防御においては、「検知」と「遮断」という異なる技術が存在し、「遮断」においては攻撃を遮断することができるが業務システムに影響を与えやすいリスクがあり、「検知」においては業務システムへの影響は与えにくい傾向があるものの攻撃を可視化するのみで攻撃を遮断することができないという特徴があります。 効果的かつ各システムの運用に即した多重防御を実現するにあたっては、これらの特徴を踏まえ、各々の業務システムの特性と重要性を鑑み、バランスを考慮して各技術を採用することが必要であると考えます。 戦略的な多重防御を検討する際の前提となる「検知」「遮断」という考え方を明記することで、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。 尚、「検知」においてはシステムでも実現することができるが、検知後の対処に遅れが出る可能性や、対処の遅れにより侵入範囲が拡大に繋がる可能性があるため、可能な限り「遮断」できる技術を採用することが望ましいと考えます。	御指摘の箇所は、本改定における改定箇所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、基本対策事項 6.2.1(1)-5 c)に脆弱性が関係する機能の無効化等を記載しております。よって原案のとおりとします。
53	マカフィー株式会社	統一基準	p.42	6.2.2	目的趣旨・変更案: 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にあたり、既知の不正プログラム対策だけでは被害を未然に防止が出来ないことが考えられるため、既知の不正プログラムへの対策とともに、未知の不正プログラムへの対策も適切に実施することが必要である。 理由: 昨今の未知の手段を用いた攻撃活動の増加を踏まえ、「政府機関等の対策基準策定のためのガイドライン(案)(平成30年度版)」に明記のある未知の脅威対策の必要性について、政府機関等へ浸透させるため、「政府機関等の情報セキュリティ対策のための統一基準(案)(平成30年度版)」においても未知の脅威対策について、明確に記載するべきと考えます。	御指摘の箇所は、本改定における改定箇所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、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。
54	マカフィー株式会社	統一基準	p.43	6.2.2(1)(a)	遵守事項・変更案: 情報システムセキュリティ責任者は、サーバ端末及び端末に不正プログラム対策ソフトウェア等を導入し、既知及び未知の不正プログラムの検知及びその実行を防止する対策を実施すること。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。 理由: 昨今の未知の手段を用いた攻撃活動の増加を踏まえ、「政府機関等の対策基準策定のためのガイドライン(案)(平成30年度版)」に明記のある未知の脅威対策の必要性について、政府機関等へ浸透させるため、「政府機関等の情報セキュリティ対策のための統一基準(案)(平成30年度版)」においても未知の脅威対策について、明確に記載するべきと考えます。	御指摘の箇所は、本改定における改定箇所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、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。

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		
55	マカフィー株式会社	統一基準	p.44	6.2.4	変更案: 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及び防御して対処する、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及び防御して対処する対策（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: 本項目の「目的と趣旨」において、「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。」と記載のあることから、後に続く文中における「検知して対処」と記載のある箇所においても「検知及び防御して対処」と変更し一貫して記載することを提言します。 また、多重防御を検討する際の前提となる「検知」と「防御」という考え方を明記することで、「検知」による攻撃の可視化のみではなく、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所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、標的型攻撃を完全に防ぐことについては「検知及び防御することは困難」と記載しており、標的型攻撃によって内部に侵入された後については「検知して対処」と記載をし使い分けており、全てにおいて「検知及び防御して対処」と変更することは不適切であるため、原案のとおりとします。
56	マカフィー株式会社	統一基準	p.44	6.2.4(1)(b)	変更案: (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及び防御して対処する、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及び防御して対処する対策（内部対策）を講ずること。 理由: 本項目の「目的と趣旨」において、「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。」と記載のあることから、後に続く文中における「検知して対処」と記載のある箇所においても「検知及び防御して対処」と変更し一貫して記載することを提言します。 また、多重防御を検討する際の前提となる「検知」と「防御」という考え方を明記することで、「検知」による攻撃の可視化のみではなく、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所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、標的型攻撃を完全に防ぐことについては「検知及び防御することは困難」と記載しており、標的型攻撃によって内部に侵入された後については「検知して対処」と記載をし使い分けており、全てにおいて「検知及び防御して対処」と変更することは不適切であるため、原案のとおりとします。
57	個人	統一基準	p.46	6.3.2(1)	クラウドサービスを使用した、機関等が運用・管理しない外部のサーバを使用することが拡大していると思われますが、その場合でも政府ドメイン名等を使用し、委託業者のドメインを使用することを禁止するのかどうかを明確にした方が良いと思います。	御指摘の点については、統一基準6.3.2(1)において、政府ドメイン名以外のドメイン名を使用している場合、府省庁からの情報を装ったなりすましの脅威が想定される等、セキュリティが確保されない恐れがあり、クラウドサービスの利用等をシステムの利用形態を問わず、政府ドメイン名を用いることとしています。

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		
58	CyberArk Software 株式会社	統一基準	p.45	6.3.1	遵守事項(2)(a)への加筆 (キ) 提供するアプリケーション・コンテンツが他のシステムと連携を行う場合、他のシステムのIDとパスワードをアプリケーション・コンテンツに埋め込まないこと。 理由: 連携する他のシステムのIDとパスワードをアプリケーションに埋め込むケースが多くみられます。それらの連携用認証情報は、データベースの更新アクセス権などの管理者権限を持つ場合が多く、悪意ある第3者に搾取された場合、非常に大きな被害を出す可能性があります。一方、それらの認証情報は、アプリケーションを改修するまで変更されず、組織の脆弱性を残したまま放置されているケースが多いです。 上記の理由から、アプリケーション・コンテンツ内に第三者が直接識別可能な形でシステム連携用の認証情報を埋め込むことを禁止し、連携を必要とする場合は、外部システムから都度新たな認証情報を呼び出す仕組みを導入することが望ましいと考えます。	御指摘の箇所は、本改定における改定箇所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、6.3.1(2)(a)(イ)に記載されている「提供されるアプリケーションが脆弱性を含まないこと」に含まれる内容となります。
59	CyberArk Software 株式会社	ガイドライン	p.213	6.3.1(2)(a)(エ)関連	加筆 6.3.1(2)-5 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツに連携する他システムの認証情報を第三者識別できる平文で埋め込まず、連携時に認証情報を外部から呼び出す仕組みを導入する。 理由: アプリケーション・コンテンツに第三者が識別可能な形で認証情報が埋め込まれている場合、その認証情報を窃取される危険性があります。また、アプリケーション・コンテンツの改修を行わない限りその認証情報は変更できません。そのため、組織のセキュリティ基準に反して長期間同一の認証情報が使用されているケースが多くあります また、アプリケーション・コンテンツ間の連携に使用されるIDはデータベースの更新アクセス権などの管理者権限を持つ場合が多く、窃取された場合に非常に大きな影響を与える可能性があります。従って、アプリケーション・コンテンツ内に認証情報を平文で埋め込むのではなく、利用時に外部から新たな認証情報を呼び出すなどの手法を取る事が望ましいと考えます。	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なく、また、本改定における改定箇所ではありませんが、6.3.1(2)(a)(イ)に記載されている「提供されるアプリケーションが脆弱性を含まないこと」に含まれる内容となります。
60	株式会社テリロジー	統一基準	p.47	7部	電力、ガス、水道、交通などの社会インフラの制御システムや工場における産業制御システム向けの機器を構成要素に追加すべきと考える。 また、OT（Operation Technology）向けのセキュリティ対策についての記述を追加すべきではないか。	御指摘の箇所は、本改定による改定箇所ではないため、パブリックコメントの対象ではありませんが、本基準は国の行政機関、独立行政法人及び指定法人を対象としており、社会インフラにおける制御システムや工場における産業システムを対象としたものではありませんので、原案のとおりとします。

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		
61	株式会社テリロジー	統一基準	p.48	7.1.2	1)サーバ装置に対する不正な通信を防ぐため、回線経路上で当該サーバ装置への通信が適切に制御されているかどうかを定期的に監視する必要があるのではないか。 2)機密情報を含む重要情報資産を保持するサーバ装置に関しては、Host Identity Protocol (RFC5201)に対応した通信回線装置を導入するなどの対策を講じ、当該のサーバ装置へのアクセスを制限すべき。 HIP対応装置を導入することによりポート・スキャンなどの偵察行為を封じ込めることが可能になる。	1) 御指摘の箇所は、本改定による改定箇所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、情報システムの監視全般については、遵守事項5.2.1(2)において、情報システムの構築時に監視等の運用管理機能要件を含むセキュリティ要件を策定することを記載しています。さらに、遵守事項6.1.4(1)(c)において、ログを用いた定期的な点検又は分析に関する規定を記載していますので、原案のとおりとします。 2) 御指摘の点は、本改定による改定箇所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、サーバ装置等へのアクセス制御については、遵守事項6.1.2(1)アクセス制御機能の導入に記載しており、それに対応するガイドラインには実現方式としてネットワークセグメントの分割等を例示しています。この実装方法は各種考えられますが、統一基準の遵守事項においては個別には指定していませんので、原案のとおりとします。
62	国立研究開発法人 国立国際医療研究センター	統一基準	p.48 p.63	7.1.1 8.2.1	端末管理責任者と各課室情報セキュリティ責任者の責任分界点について 8.1.1にて、要管理対策区域外にてインターネット接続した端末を再接続する場合、許可を行えるのが統括情報セキュリティ責任者なのか、課室情報セキュリティ責任者なのか明確でないため、明確に記載いただきたい。また安全管理措置について、支給外の端末の安全管理措置、業務利用について、端末管理責任者と課室情報セキュリティ責任者の責任分界点がどのようになるか明確でないため、明確に記載いただきたい。	御指摘の要管理対策区域外にてインターネット接続した端末を再接続する場合の許可を行う責任者については、遵守事項8.1.1(3)(g)において、課室情報セキュリティ責任者と規定されています。 支給外端末の安全管理措置を講ずる責任者は、遵守事項7.1.1(4)(c)(イ)に、端末管理責任者と規定されいます。また、支給外端末の業務利用を許可する適任者は、遵守事項8.2.1(3)(a)に端末管理責任者と規定されています。 以上のように、御指摘の点については端末管理責任者と課室情報セキュリティ責任者の責任分界は明確となっています。

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		
63	迷惑メール対策推進協議会	統一基準	p.52	7.2.3	下記の通り修正することが望ましいと考える。 (原文) 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。 (修正案) さらに、電子メールのなりすまし対策の一部は DNS の設定が必要なため、これらが不十分である場合には、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 サーバに対する適切な設定および管理が必要である。 ■理由 なりすまし対策として利用できる送信ドメイン認証技術は、SPF や DKIM、DMARC など、それぞれ DNS に対する SPF レコードや DKIM レコード、DMARC レコードなどの設定や管理が、メール配送のための設定とは別に必要となる。 そのため、単に「不備」や「適切な管理」といった表現ではなく、別途設定が必要、という意味を含めて表現が必要と考えた。	御指摘の箇所は、本改定による改定箇所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7.2.1(1)(c)の電子メールのなりすまし対策並びに基本対策事項7.2.1(1)-2及び解説において、SPF, DKIM, DMARCについて詳しく記載していますので、原案のとおりとします。
64	迷惑メール対策推進協議会	ガイドライン	p.253	7.2.1(1)-3	下記のとおりDKIMに係る記述を追記することが望ましいと考える。 (原文) 7.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。 a) SMTP によるサーバ間通信を TLS(SSL)により保護する。 b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。 (修正案) 7.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。 a) SMTP によるサーバ間通信を TLS(SSL)により保護する。 b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。 c) DKIM による電子署名の技術を利用する。 ■理由 送信ドメイン認証技術 DKIM では、メールヘッダおよびメール本文から作成される電子署名をメールヘッダ上に追加することにより送信ドメイン認証を行う。この場合、署名対象となるメールヘッダやメール内容がメール配送中に改ざんされた場合、メール受信側で DKIM 認証が失敗するため改ざんを検知することができる。このため DKIM を、電子メールの改ざん防止技術としても利用すべきである。	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、本基本対策事項は「盗聴及び改ざんの防止」を目的とするものであり、一方で電子署名は改ざんの検知はできるものの、盗聴及び改ざんの防止対策とはならないことから不適と考えられますので、原案のとおりとします。

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		
65	迷惑メール対策推進協議会	ガイドライン	p.253	7.2.1(1)-2 a)解説	下記のとおりDMARCに係る記述を変更することが望ましいと考える。 (原文) DMARC は、送信元ドメインに対し、効果的な認証基準が得られるよう、認証技術を自身のインフラに実装するに当たっての、より統合的な手法を定義するとともに、電子メールの受信者が SPF、DKIM 等に係る送信ドメイン認証の詳細な結果を電子メールの送信者にフィードバックするフレームワークを実現するための仕様である。 (修正案) DMARCは、電子メールの送信者が自身のドメインをなりすまされたメールを受信者に届けなくするための仕組みで、電子メールの受信者が SPF、DKIM等に係る送信ドメイン認証の検証結果を電子メールの送信者にフィードバックする機能を備え、送信者が受信時の制御要求を段階的に引き上げることができる。 ■理由 DMARCの特徴の一つである、送信ドメイン側がメール受信者に対して、なりすましメール検知時の受信処理方法を示すポリシーの設定やその目的、そのポリシーに段階があることや引き上げられる部分についての言及が必要と考えた。	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なく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
66	迷惑メール対策推進協議会	ガイドライン	p.254	7.2.1(1)-2 a)解説	SPFに係る留意事項に続けて、DMARCに係る留意事項として下記内容を追記することが望ましいと考える。 (追加案) なお、DMARCについては、以下の事項に留意すること。 ・電子メールを利用していないドメインについても、DMARC のポリシーを″p=reject″ と設定することで、なりすましメールが受信者に届かない設定にする。 ・DMARC の設定を広く適用させるために、組織ドメインに対する DMARC レコードの設定を検討する。 ・DMARC レコードにはポリシーの設定が必須であるため、導入当初は″p=none″ と設定し、DMARC レポートを受け取り参照することで、メールの認証状況の把握につとめ、適切な SPF および DKIM の設定を行うことで，段階的に DMARC ポリシーの強化を実施する。 ■理由 既に DMARC のポリシーに基づいた処理を実施しているメール事業者もあるため、適切な DMARC レコード（ポリシー）の設定方法および強化方法について示す必要がある。 また、メールに利用しない実在するドメイン名を悪用したなりすましメールの被害を無くすために、 DMARC の強いポリシー ″p=reject″ を利用したなりすまし対策についても説明を追加すべき。	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なく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
67	迷惑メール対策推進協議会	ガイドライン	p.255	7.2.1(1)-3 c)解説	【 基本対策事項 】<7.2.1(1)(d)関連> への 7.2.1(1)-3 (c) への追加に関連した解説の追加。 ■理由 DKIMによりメール本文およびメールヘッダからなる電子署名を付与することは、電子メールの改ざんを防止する観点から効果的である。また、DKIMの署名付与及び検証はメールサーバ間で行われるため、送受信する電子メールクライアントに依存しない検証が可能である。	7.2.1(1)-3への追加の御意見への回答と同様に、原案のとおりとします。
68	日本マイクロソフト株式会社	統一基準	p.51	7.2.1(1)(d)	電子メールのサーバー間通信について従来の方式と合わせて、暗号化の対策も必要という記述が適切と考える。例えば「暗号化された要求に対しては暗号化に対応した方式で対応する」など。 理由： 電子メールのサーバー間通信は一組織の取り組みだけでは完結せず、広く多団体での対応が必要となるため。	相手先サーバが対応していない状況を考慮して、自らが送信側の場合には相手先が暗号化に対応可能かを確認し、自らが受信側の場合には相手側からの暗号化の要求に応じるものとしており、本内容はガイドラインの解説「遵守事項7.2.1(1)(d) 『サーバ間通信の暗号化』について」に記載しています。

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		
69	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.1 目的・趣旨	組織によっては電子メールサーバにクラウドサービスを利用する場合も想定されることから、「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。」に続いて「電子メールサーバにクラウドサービスを利用する場合は、4.1.4「クラウドサービスの利用」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。」と追記してはどうか。	御指摘の箇所は、本改定による改定箇所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、クラウドサービスを利用する場合は、「4.1.4 クラウドサービスの利用」が遵守事項となることは明らかと考えますので、原案のとおりとします。
70	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.2 目的・趣旨	組織によってはウェブサーバにクラウドサービスを利用する場合も想定されることから、「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。」に続いて「ウェブサーバにクラウドサービスを利用する場合は、4.1.4「クラウドサービスの利用」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。」と追記してはどうか。	御指摘の箇所は、本改定による改定箇所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、クラウドサービスを利用する場合は、「4.1.4 クラウドサービスの利用」が遵守事項となることは明らかと考えますので、原案のとおりとします。
71	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.1(1)(d)	「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。」とされているが、現状におけるインターネット経由の電子メールの配信方式においては、サーバ間の通信の暗号化が可能かどうかは送信先電子メールアドレスを管理する電子メールサーバにおける暗号化機能への対応状況に依存するため、つねに暗号化が可能とは限らない。従って、遵守不可能な事態が生ずることを避けるために「可能な範囲で電子メールのサーバ間通信を暗号化により保護する対策を講じること」としてはどうか。	相手先サーバが対応していない状況を考慮して、自らが送信側の場合には相手先が暗号化に対応可能かを確認し、自らが受信側の場合には相手側からの暗号化の要求に応じるものとしており、本内容はガイドラインの解説「遵守事項7.2.1(1)(d) 『サーバ間通信の暗号化』」に記述しています。
72	株式会社テリロジー	統一基準	p.55	7.3.1	通信回線装置の設定は日々のメンテナンスにより変更されるため、運用開始からセキュリティ・リスクは増大し続ける。通信回線装置の設定の見直し、セキュリティ面の担保は手作業では難しく、ネットワークセキュリティ監査製品による定期的かつ自動的な確認手段を装備すべき。	御指摘の箇所は、本改定による改定箇所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、御指摘いただいたセキュリティの運用に係わる自動化は重要と考えています。今回の改定においては、政府機関等が保有する膨大なIT機器の資産管理と脆弱性管理を優先して対応したところです。 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。
73	一般社団法人 日本ネットワークインフォメーションセンター	統一基準	p.55 p.56 p.57	7.3.1(1) 7.3.1(2) 7.3.1(3) 7.3.2	意見(1) Internet Routing Registryについて インターネットにおける経路制御では、経路制御上のセキュリティ対策の一つとして、Internet Routing Registry(IRR)への登録と常に正しい情報へ更新しつづけることが大切です。IRRは、いわゆるインターネット上の経路の乗っ取りや経路制御上の問題発生時に参照されるデータベースです。 イ. 7.3 通信回線 遵守事項 (1) 通信回線の導入時の対策 (g)について、「インターネット回線を接続する場合には、特に適切なIRRへの登録を行うこと。」を追記する。 ロ. 7.3 通信回線 遵守事項 (2) 通信回線の運用時の対策 (b)について、「インターネット回線を接続している場合には、特に適切なIRRへの登録情報を定期的に確認し見直すこと。」を追記する。 ハ. 7.3 通信回線 遵守事項 (3) 通信回線の運用終了時の対策 (a)について、「インターネット回線を接続していた場合には、特に適切なIRRへの登録情報を削除など適切に対応すること。」を追記する。 ニ. 7.3.2 IPv6 通信回線について、「IPv6においても適切なIRRへの登録と定期的な見直しを行うこと。」を追記する。	御指摘の箇所は、本改定による改定箇所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、統一基準は全ての政府機関等に向けたベースラインであるという位置付けに鑑み、原案のとおりとします。

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		
74	個人	統一基準	p.59	8.1.1	以下の記述の意味がよくわかりません。 文法的に正しいでしょうか。 『p.59 8.1.1 情報システムの利用 遵守事項 (1) 情報システムの利用に係る規定の整備 (d)(ア) 職員等は、国の行政機関、独立行政法人又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。』	御指摘を踏まえ、該当の規定を以下のとおり修正いたします。 『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。』
75	独立行政法人 情報処理推進機構	ガイドライン	p.319	付録	「IT 製品の調達におけるセキュリティ要件リスト」が更新されましたので、最新化をお願いいたします。 現行:IT 製品の調達におけるセキュリティ要件リスト(平成26 年5月19 日 経済産業省) 新 :IT 製品の調達におけるセキュリティ要件リスト(平成30年2月28日 経済産業省)	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、御指摘を踏まえ、ガイドラインを修正させていただきます。
76	独立行政法人 情報処理推進機構	ガイドライン	p.319	付録	「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」が更新されましたので、最新化をお願いいたします。 現行:IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック(2014 年5月 独立行政法人情報処理推進機構) 新 :IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック(2018 年2月 独立行政法人情報処理推進機構)	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、御指摘を踏まえ、ガイドラインを修正させていただきます。
77	スプランクサービスジャパン合同会社	運用指針	p.2	第3部(2)	指針第3部(2)「主務大臣が情報セキュリティ対策の実施状況に関して評価を行い、評価結果を公表する」に対応する具体的要領が統一基準に明記されていないので記載することを推奨します。 意見理由 独立行政法人及び指定法人のセキュリティを政府全体として一定の水準で確保するため、評価の方法については内容、期限、公開方法等、統一基準にて見解を示すことが必要と考えられるためです。	御指摘については、本改定における改定箇所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。また、御指摘については、独立行政法人通則法に基づき実施されるものであるため、その要領を統一基準に明記することは、考えておりません。
78	スプランクサービスジャパン合同会社	運用指針	p.2	第3部(2)	指針第3部(2)には独立行政法人及び指定法人の評価及び公表について義務化されていますが、同様に府省庁についても評価及び評価結果の公表を推奨します。 意見理由 評価と評価結果の公表の必要性については独立行政法人と同様に考えられるためです。	御指摘については、本改定における改定箇所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、各府省庁におけるサイバーセキュリティ対策に関する取組の総合評価結果等を内閣官房がサイバーセキュリティ政策に係る年次報告として取りまとめ、公表しております。また、監査の結果につきましても、同年次報告にて公表しております。

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		
79	個人	全般			・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。
80	国立研究開発法人 国立国際医療研究センター	全般			地方自治体にも同じ基準を求められないのか（文書全体について） 国の行政機関、独立行政法人、指定法人が対象となっているが、業態によっては、地方自治体の指導を受ける立場にある独立行政法人もある（例えば病院など）。 地方自治体から独立行政法人に対して求められている情報共有の仕組みの中には、統一基準の内容から逸脱するもの（セキュリティが低い方式が要求されているもの）が一部にあるため、地方自治体の意識を高めるためにも、地方自治体においても、統一基準群を準用するなどの努力義務を付記いただきたい。	御指摘については、本改定における改定箇所に関する事項ではないため、パブリックコメントの対象ではありませんが、統一基準群の適用対象については、サイバーセキュリティ基本法を根拠としております。 現状、地方自治体は、サイバーセキュリティ基本法において本統一基準群の適用対象となっていないため、努力義務を付記することは適切ではないと考えられます。
81	個人	全般			まずお願いしたいのであるが、意見募集の期限は、17時までとせずに24時までとしていただけるだろうか。 どうせ当日中に応募された意見を見終わるものでもないのであるし、意見募集の通例として（また行政や司法への提出物一般の通例として）、意見募集の期限は24時までとするのが妥当なはずであろう。（要するに、search.e-gov.go.jpを見て仕事から帰って当日終了分の意見提出を行おうとする様な者に対する嫌がらせであろう？NISC（や他一部の内閣官房・内閣府の部署）による意見公募は。改められたい。意地悪を公務員がしていいわけがない（あるいは国民からの「逃げ隠れ」かもしれないが。）。） であるので、次からは意見募集の期限は17時までではなく、24時までとされたい。それが妥当適切なはずである。（そして、受付を行うのは政府のサーバという機械なのであるから、その様な時刻まで誰にも特段の問題無く受付が行えるはずである。（なお、行政機関や司法機関への書類提出は、郵便や直接手渡しの場合、当日24時まで当日分として受付が行えるものである事を注意しておく。）） （それとであるが、各所での全角文字の故意的な使用は止めてはどうか？NISCの姿勢が現れているようで微笑ましいのであるが、「所詮文系」的な精神が溢れるようであるのは、当然好ましくないものである。それは躁的な性質をも伴うものであると断じて良いものであるが、当然、公共機関としてその様な病的な性質を露にして国民・社会・世界に接しようとするのは誤りであるので、今後態度を改められたい。）	御指摘いただいた内容は、統一基準群の改定に直接関わるものではありませんが、参考として承ります。