資料２

政府機関等の情報セキュリティ対策のための統一基準群の改定（案）

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

資料２－２　政府機関の情報セキュリティ対策のための統一規範（案）

資料２－３　政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）（案）

資料２－４　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２－５　「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（案）

資料２－６　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の改定（案）に対する意見募集の結果一覧

資料2－1

National center of
Incident readiness and
Strategy for
Cybersecurity

「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

平成28年8月

内閣官房

内閣サイバーセキュリティセンター

統一基準群（平成26年度版）策定後の主な経緯

26年8月　民間企業の大量個人情報流出事案を踏まえた対策強化の指示

☛ 機微度の高い情報を始めとする情報管理の徹底を推進

27年1月　サイバーセキュリティ基本法の完全施行

☛ 独法の対策強化、戦略本部による監査の実施、NISCの機能強化等を推進

27年5月　日本年金機構における不正アクセスによる情報流出事案の発生

☛ 事案対処体制の強化、標的型攻撃を前提とした対策強化等を政府機関全体で推進

27年9月　新たなサイバーセキュリティ戦略の決定

☛ 新たに直面した脅威・課題への対応、IT製品・サービスの普及に伴う対策強化を推進

28年3月　サイバーセキュリティ人材育成総合強化方針の決定

☛ 政府機関における専門人材の確保・育成や一般職員の素養向上への取組方針

28年4月　サイバーセキュリティ基本法の改正法案の成立

☛ 指定法人への適用範囲の拡大等（公布の日から6月以内に施行）

統一基準群の位置づけの見直し及び独立行政法人等への適用範囲の拡大

統一基準群を、基本法に基づく政府機関及び独立行政法人等におけるサイバーセキュリティに関する対策の基準と位置づける。
独立行政法人等において、所管府省庁の助言等の下、情報セキュリティ対策が適切に講じられるよう、対策基準等の策定、体制の構築、対策実施状況の評価等に関する規定を追加する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋※）　※平成28年4月成立の改正法施行後の条文
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

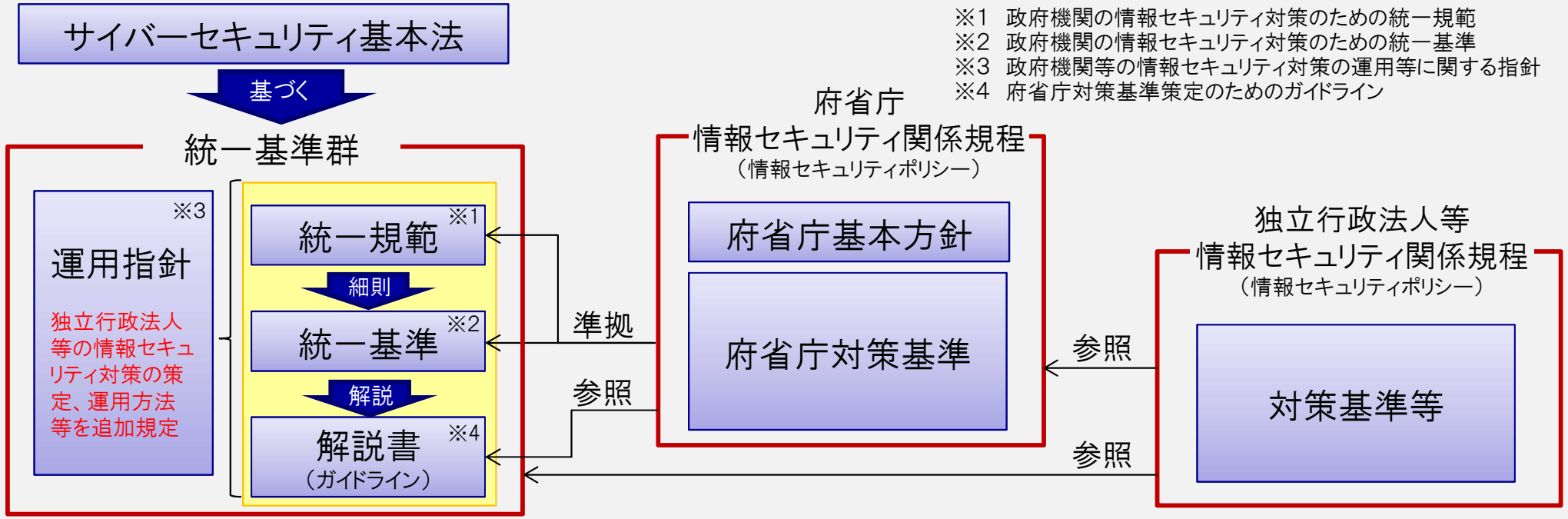
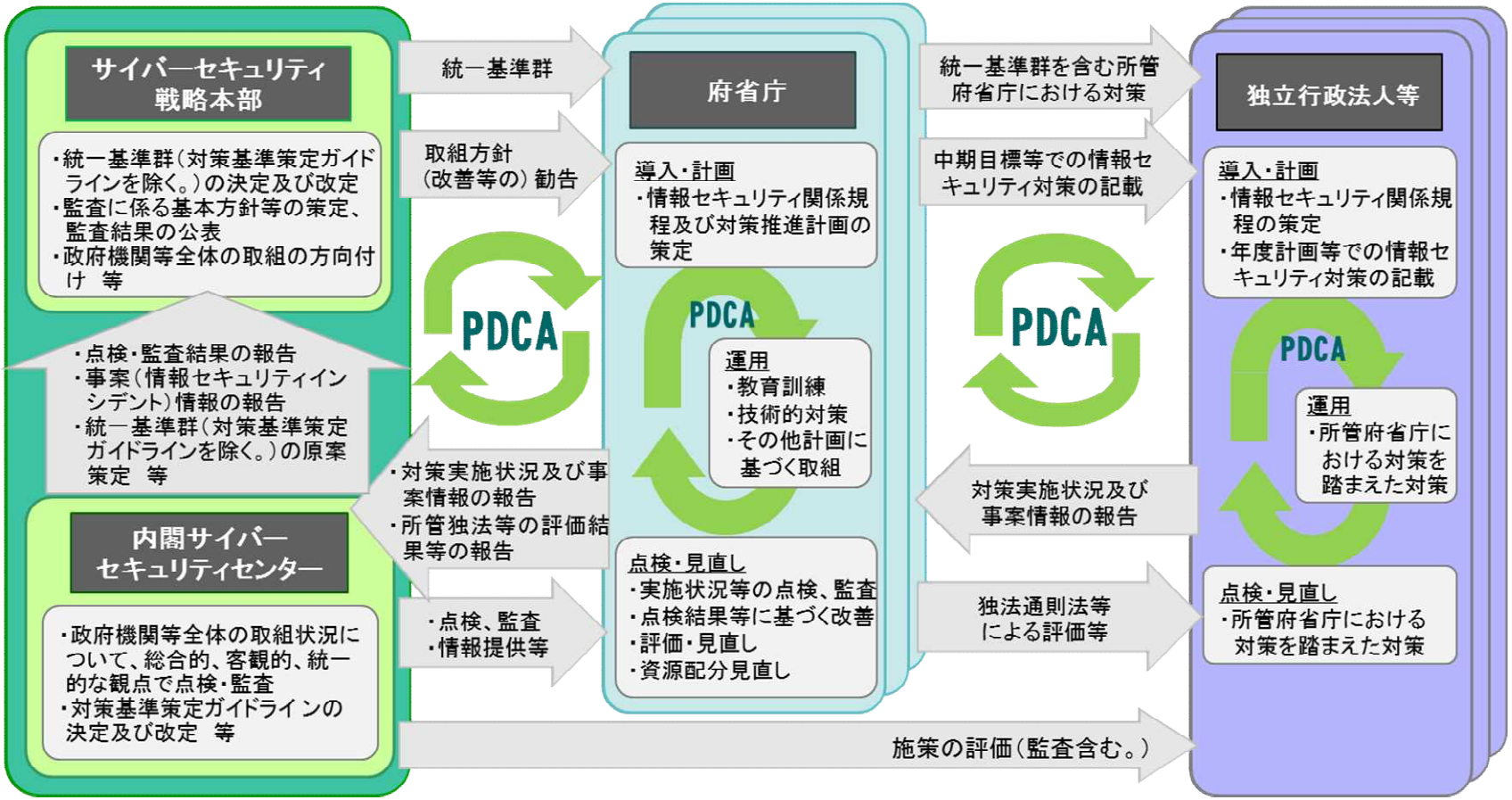


図　サイバーセキュリティ基本法と統一基準群及び情報セキュリティ関係規程の関係

監査に係る規定整備及び政府機関等の情報セキュリティ対策の強化

基本法第25条第1項第2号に基づく監査の実施に係る規定を整備し、以下のとおり独立行政法人等を含む政府機関等のセキュリティ強化に向けたPDCA※サイクルを明確化する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋：平成28年4月成立の改正法施行後の条文）
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。



※ PDCA：（Plan〔計画〕、Do〔実行〕、Check〔評価〕、Act〔改善〕）

日本年金機構事案等の外部動向を踏まえた規定の見直し・強化

日本年金機構における不正アクセスによる情報流出事案を始めとする事案（情報セキュリティインシデント）の発生状況やサイバー攻撃の動向、IT利活用環境の変化等を踏まえ、以下の規定の追加及び強化を図る。

事案発生に備えた対処体制（CSIRT※）、対処・連絡手順等の整備に係る規定の強化

- 事案対処に必要な知識・能力を有する**対処体制（CSIRT）の構築、外部専門家による支援**
- 発生した事案の対処に係る**意思決定手法や判断基準、対処方法等の事前準備**

※ CSIRT（Computer Security Incident Response Teamの略称）

標的型攻撃等による不正プログラム感染の発生を前提とする情報システムの防御策の強化

- **情報システムの重要な情報を扱う部分のインターネットからの分離**
- セキュリティ監視の集中・強化等を目的とした、**インターネット接続口の集約**
- **実行プログラム形式ファイルが添付された電子メール受信時のシステム措置**
- サイバー攻撃を受けた際の影響範囲の特定、原因究明等を適切に実施するための**通信記録の管理**

情報及び情報システムへの不正アクセスの防止等を目的とする対策の見直し・強化

- 個人情報や機微な情報を始めとした機密性・完全性の高い情報を大規模かつ体系的に管理する**データベースに対する対策**

新たなIT製品・サービスの普及等に伴う対策事項の明確化

- 情報の取扱いを外部事業者に委ねる際のリスク評価に基づく**クラウドサービス※利用可否の判断**
- 必要に応じて**委託事業の実施場所（クラウド構成機器の所在地等）、準拠法・裁判管轄の指定**
- **クラウドサービス及び提供事業者の信頼性の確認**

※ 外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

資料２－２

政府機関の情報セキュリティ対策のための統一規範（案）

平成　年　月　日
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、政府機関のとるべき対策の統一的な枠組みを定め、各政府機関に自らの責任において対策を図らしめることにより、もって政府機関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政府機関は、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（以下「府省庁」という。）とする。

２　本規範の適用対象とする者は、府省庁において行政事務に従事している国家公務員その他の府省庁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「行政事務従事者」という。）とする。

３　本規範の適用対象とする情報は、行政事務従事者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　府省庁は、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　府省庁は、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。

（府省庁情報セキュリティ文書）

第四条　府省庁は、自組織の特性を踏まえ、府省庁基本方針（府省庁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。）及び府省庁対策基準（府省庁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。 府省庁基本方針及び府省庁対策基準（以下「府省庁ポリシー」という。）の呼称は府省庁で独自に定めることができる。

２　府省庁基本方針は、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　府省庁対策基準は、別に定める政府機関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　府省庁は、前条第一項の評価結果を踏まえ、府省庁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　府省庁は、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　府省庁は、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、府省庁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府省庁における情報セキ

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等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　府省庁は、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　府省庁は､府省庁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　府省庁は、行政事務従事者が自覚をもって府省庁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　府省庁は、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、府省庁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　府省庁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　府省庁は、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　府省庁は、府省庁対策基準が本規範及び統一基準に準拠し、かつ実際の

運用が府省庁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　府省庁は、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　府省庁は、府省庁間での情報の提供、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　府省庁は、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　府省庁は、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　府省庁は、府省庁間での情報の提供、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　府省庁は、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　府省庁は、自組織が管理する庁舎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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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　府省庁は、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行政事務従事者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の手続その他その執行について必要な細則は、統一基準で定める。

附則

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

資料２－３

政府機関の情報セキュリティ対策のための統一基準
（平成 28 年度版）（案）

平成　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、府省庁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、それぞれの府省庁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。しかし、府省庁共通の IT 環境の利用、府省庁間の情報流通の現状を踏まえると、政府機関全体の統一的な枠組みを構築し、それぞれの府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要である。

本統一基準は、「政府機関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）に基づく政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

(2) 本統一基準の適用範囲

(a) 本統一基準において適用範囲とする者は、全ての行政事務従事者とする。

(b) 本統一基準において適用範囲とする情報は、以下の情報とする。

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

(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、行政事務従事者が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、府省庁が調達し、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範囲とする情報システムは、本統一基準の適用範囲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、府省庁が行うべき対策について、目的別に部、節及び項の３階層にて対策項目を分類し、各項に対して目的、趣旨及び遵守事項を示している。遵守事項は、府省庁対策基準において必ず実施すべき対策事項である。府省庁は、内閣官房内閣サイバーセキュリティセンターが別途整備する府省庁対策基準策定のためのガイドライン及び政府機関統一基準適用個別マニュアル群において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、府省庁対策基準を策定する必要がある。

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。

府省庁において格付の定義を変更又は追加する場合には、それぞれの府省庁の対策基準における格付区分と遵守事項との関係が本統一基準での関係と同等以上となるように準拠しなければならない。また、他府省庁へ情報を提供する場合は、自身の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	行政事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
機密性２情報	行政事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
機密性１情報	情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

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	行政事務で取り扱う情報（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行政事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	行政事務で取り扱う情報（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行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
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行政事務従事者に確実に行わせるための手段をいう。

行政事務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。府省庁は、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、外部委託により府省庁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、府省庁の情報処理業務の一部又は全部について、契約をもって府省庁外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、他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

● 「行政事務従事者」とは、府省庁において行政事務に従事している国家公務員その他の府省庁の指揮命令に服している者であって、府省庁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。行政事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。

● 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

● 「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、府省庁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政府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、府省庁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、当該府省庁に設置された体制をいう。Computer Security Incident Response Team の略。

● 「実施手順」とは、府省庁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) 本統一基準の適用範囲」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、府省庁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、府省庁対策基準及び実施手順を総称したものをいう。

● 「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。

【た】

● 「端末」とは、情報システムの構成要素である機器のうち、行政事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体とし

て扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、府省庁が調達又は開発するものをいう。端末には、モバイル端末も含まれる。

● 「通信回線」とは、複数の情報システム又は機器等（府省庁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、府省庁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、府省庁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】

● 「府省庁」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 11 年法律第 89 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 23 年法律第 120 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。「府省庁」と表記する場合は、単一の機関を指す。

● 「府省庁外通信回線」とは、通信回線のうち、府省庁内通信回線以外のものをいう。

● 「府省庁対策基準」とは、府省庁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。

● 「府省庁内通信回線」とは、一つの府省庁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、当該府省庁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。府省庁内通信回線には、専用線や VPN 等物理的な回線を府省庁が管理していないものも含まれる。

● 「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、民間事業者等の府省庁外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、府省庁が管理する庁舎等（外部の組織から借用している施設等を含む。）府省庁の管理下にある区域であって、取り扱う情報を保護するために、施設及び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、それに係る全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に最高情報セキュリティ責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、最高情報セキュリティ責任者は、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等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の設置

(a) 府省庁は、府省庁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。

(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、府省庁対策基準等の審議を行う機能を持つ組織として、府省庁の情報セキュリティを推進する部局及びその他行政事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、行政事務従事者のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁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。

(7) 兼務を禁止する役割

(a) 行政事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア) 承認又は許可（以下本項において「承認等」という。）の申請者と当該承認等を行う者（以下本項において「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) 行政事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

2.1.2 府省庁対策基準・対策推進計画の策定

目的・趣旨

府省庁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、府省庁として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

遵守事項

(1) 府省庁対策基準の策定

(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府省庁対策基準を定めること。

(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、府省庁の業務、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

府省庁は、府省庁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に関する実施手順の整備・運用

(a) 統括情報セキュリティ責任者は、府省庁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) 情報セキュリティ責任者又は課室情報セキュリティ責任者は、行政事務従事者より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。

(2) 違反への対処

(a) 行政事務従事者は、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行政事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「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) 行政事務従事者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。ただし、行政事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、行政事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。

(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、その内容が行政事務従事者に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての行政事務従事者が、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、政府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) 教育体制等の整備

(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。

(2) 教育の実施

(a) 課室情報セキュリティ責任者は、行政事務従事者に対して、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) 行政事務従事者は、教育実施計画に従って、適切な時期に教育を受講すること。

(c) 課室情報セキュリティ責任者は、CYMAT 及び CSIRT に属する職員に教育を適切に受講させること。

(d) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者に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府省庁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、行政事務従事者に周知すること。

(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府省庁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、行政事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

(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、行政事務の遂行のため特に重要と認めた情報システムについて、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府省庁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府省庁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) 行政事務従事者は、情報セキュリティインシデントの可能性を認知した場合には、

府省庁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、府省庁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) CSIRT は、府省庁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、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。さらに、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においては、「大規模サイバー攻撃事態等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁）」に基づく報告連絡も行うこと。

(h) 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。

(i) 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。

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

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

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

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、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

(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、行政事務従事者に自己点検の実施を指示すること。

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

(3) 自己点検結果の評価・改善

(a) 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は、行政事務従事者による自己点検結果を分析し、評価すること。統括情報セキュリティ責任者は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。

(b) 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の指示を、最高情報セキュリティ責任者から受けた場合には、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) 府省庁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) 実施手順が府省庁対策基準に準拠していること

(ウ) 自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること

(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情報セキュリティ責任者に指示すること。

(b) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、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、府省庁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、府省庁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

行政事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（以下本項において「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行政事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、行政事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

なお、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。

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、行政事務従事者へ周知すること。

（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) 行政事務従事者は、自らが担当している行政事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) 行政事務従事者は、情報の作成時及び府省庁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) 行政事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

(c) 行政事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を

引き継いだ者を含む。）又は決定者の上司（以下この項において「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) 行政事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 行政事務従事者は、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) 行政事務従事者は、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) 行政事務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。

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

(5) 情報の提供・公表

(a) 行政事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

(b) 行政事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。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) 行政事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

(6) 情報の運搬・送信

(a) 行政事務従事者は、要保護情報が記録又は記載された記録媒体を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。ただし、他府省庁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) 行政事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

(7) 情報の消去

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

(b) 行政事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が

残留した状態とならないよう、全ての情報を復元できないように抹消すること。

(c) 行政事務従事者は、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) 行政事務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

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

(c) 行政事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)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行政事務の内容、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。行政事務従事者が実施すべき対策については、行政事務従事者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) 行政事務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、行政事務従事者が府省庁外の者を立ち入らせる際には、当該府省庁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

府省庁外の者に、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、行政事務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において府省庁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 項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。

また、民間事業者が不特定多数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 節において「約款による外部サービス」として定義するものを利用し、行政事務を遂行する場合も外部委託の一つの形態であるが、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、その際は本項に代えて 4.1.2 項「約款による外部サービスの利用」を適用すること。

＜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

（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、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、委託先企業又はその従業員、再委託先、若しくはその他の者による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

(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

(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(a)(b)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府省庁に提供し、府省庁の承認を受けるよう、仕様内容に含めること。

(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行政事務従事者より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせること。

(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) 行政事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。

(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

外部委託により行政事務を遂行する場合は、原則として 4.1.1 項「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 節において「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、種々の情報を政府機関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、本項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) 行政事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で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。政府機関においても、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、政府機関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 項の規定と同様に、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、本項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、府省庁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) 府省庁のアカウントによる情報発信が実際の府省庁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、府省庁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) 行政事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを

用いる場合は、府省庁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、政府機関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、政府機関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、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。

(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

府省庁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、府省庁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、府省庁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、その管理を府省庁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 節「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、情報システムを統括する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府省庁が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

(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

（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、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づき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、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。

(e) 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。

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。

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、府省庁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府省庁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、府省庁において業務継続計画を策定し運用している。

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

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

(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、府省庁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、行政事務従事者と共有を図ること。

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

政府機関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政府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、政府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、政府機関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 項「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採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。

(d) 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及び独自に開発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し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

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、政府機関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。以下この項において同じ。）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

府省庁では、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。府省庁は、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 項「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府省庁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、府省庁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限り、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) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(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) 行政事務従事者は、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

府省庁では、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府省庁のものであると確認できることが重要である。また、政府機関になりすましたウェブサイトを放置しておくと、政府機関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、府省庁外向けに提供するウェブサイト等が実際の府省庁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よう仕様に含めること。ただし、4.1.3 項に掲げる場合を除く。

(b) 行政事務従事者は、府省庁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、前号と同様、政府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府省庁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) 行政事務従事者は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

(b) 行政事務従事者は、府省庁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、行政事務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「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、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するため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、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。

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。仮に政府機関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、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、6.2.3 項「サービス不能攻撃対策」、7.3.2 項「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、本項での共通的な対策に加え、それぞれ 7.2 節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

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

府省庁においては、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、府省庁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、府省庁においては、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、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や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) 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行政事務従事者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本項の遵守事項のほか、7.1.2 項「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。

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、本項の遵守事項のほか、7.1.2 項「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) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

(b) 情報システムセキュリティ責任者は、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、府省庁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、本項の遵守事項のほか、7.1.2 項「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、府省庁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

本項における「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行政事務従事者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

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

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「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、行政事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

(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、府省庁内通信回線にインターネット回線、公衆通信回線等の府省庁外通信回線を接続する場合には、府省庁内通信回線及び当該府省庁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、府省庁内通信回線と府省庁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、行政事務従事者の業務遂行を目的としたリモートアクセス環境を、府省庁外通信回線を経由して府省庁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 技術を利用して府省庁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、府省庁においても、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

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

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

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、府省庁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、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を想定し、要管理対策区域外に持ち出した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安全管理措置に関する規定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、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。

(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、行政事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

(3) 情報システムの利用時の基本的対策

(a) 行政事務従事者は、行政事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) 行政事務従事者は、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府省庁の情報システムを接続しないこと。

(c) 行政事務従事者は、府省庁内通信回線に、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) 行政事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。

(e) 行政事務従事者は、接続が許可されていない機器等を情報システムに接続しない

こと。

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

(g) 行政事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。

(h) 行政事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。

(4) 電子メール・ウェブの利用時の対策

(a) 行政事務従事者は、要機密情報を含む電子メールを送受信する場合には、それぞれの府省庁が運営し、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) 行政事務従事者は、府省庁外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合は除く。

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

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

(e) 行政事務従事者は、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) 行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

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

(b) 行政事務従事者は、自己に付与された識別コードを適切に管理すること。

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

(d) 行政事務従事者は、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) 行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

(b) 行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。
(c) 行政事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

(7) 不正プログラム感染防止
(a) 行政事務従事者は、不正プログラム感染防止に関する措置に努めること。
(b) 行政事務従事者は、情報システム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　府省庁支給以外の端末の利用

8.2.1　府省庁支給以外の端末の利用

目的・趣旨

行政事務の遂行においては、府省庁から支給された端末を用いて行政事務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず府省庁支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は府省庁が支給したものではないという理由で、行政事務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、府省庁対策基準を満たさないおそれがある。

したがって、そのような可能性がある場合は、府省庁支給以外の端末を行政事務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、府省庁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。

また、府省庁支給以外の端末であっても、府省庁から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1 項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、行政事務従事者に安全管理措置を講じさせる必要がある。

遵守事項

(1) 府省庁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、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

(b) 統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

(c) 情報セキュリティ責任者は、府省庁支給以外の端末による行政事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を定めること。

(d) 前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。

(2) 府省庁支給以外の端末の利用時の対策

(a) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項 8.2.1(1)(c)で定める責任者の許可を得ること。

(b) 行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(c) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。

(d) 行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。

資料２－４

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　年　月　日
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、政府機関について、政府機関の情報セキュリティ対策のための統一規範（平成〇年〇月〇日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。）及び政府機関の情報セキュリティ対策のための統一基準（平成〇年〇月〇日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。）に基づく府省庁対策基準の策定及びその運用等のために必要な事項、並びに独立行政法人等（独立行政法人及び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 13 条に定める指定法人。以下同じ。）における情報セキュリティマネジメント等に関して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、本指針及び府省庁対策基準策定のためのガイドライン（平成〇年〇月〇日内閣官房内閣サイバーセキュリティセンター。以下「対策基準策定ガイドライン」という。）の総称をいい、統一規範、統一基準及び本指針の原案は、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。）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（以下「戦略本部」という。）において決定する。また、対策基準策定ガイドラインは、府省庁と協議の上、NISC において決定する。

なお、NISC は、新たな脅威の発生や府省庁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、全ての府省庁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、府省庁が準拠できるよう、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。

(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採るべき基本的な対策事項の例示、考え方等を解説することを目的として策定する。

３　府省庁における情報セキュリティマネジメント

(1)　導入・計画

①　府省庁基本方針の策定

府省庁は、情報セキュリティ対策の目的、対象範囲等、情報セキュリティに

対する基本的な考え方を示した府省庁基本方針を定める。

府省庁基本方針の策定に当たっては、対象となる情報、情報システム、組織（者）、場所・区域の範囲及びその境界について、外部委託の観点も含めて明確にするとともに、対象範囲外においては、他の主体により情報セキュリティ対策が講じられていることを確認するなどにより、その境界が妥当であることを確認することが重要である。

なお、府省庁基本方針は、情報セキュリティに対する基本的な方向性を決定付けるものであることから、頻繁に更新される性質のものではないことに留意する必要がある。

② 府省庁対策基準の策定

府省庁は、府省庁基本方針に基づき、統一規範及び統一基準に準拠して府省庁対策基準を定める。府省庁対策基準には、統一基準の規定を遵守するための対策事項について、対策基準策定ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて定めることとする。また、脅威の変化等に迅速に対応するために政府機関共通の情報セキュリティ対策が個別に決定されている場合にはそれを反映する。

③ 対策推進計画の策定

府省庁は、最高情報セキュリティ責任者の指揮の下、情報セキュリティに係るリスク評価の結果を踏まえ、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。）を策定する。対策推進計画は、教育訓練、情報システムに対する技術的な対策を含め、府省庁における情報セキュリティに関する一連の取組をふ瞰できるものとする。

(2) 運用

府省庁は、対策推進計画に基づき、行政事務従事者に対する教育訓練を実施し、府省庁基本方針及び府省庁対策基準（以下「府省庁ポリシー」という。）の浸透を図るとともに、情報システムに対する技術的な対策を強化するなど、情報セキュリティに関する取組を実施する。

(3) 点検・見直し

府省庁は、対策推進計画に基づく取組について、年度ごとに実施状況を把握し点検するとともに、必要に応じて見直しや改善を行う。

府省庁は、情報セキュリティ対策について、その適正性を確保するため、情報セキュリティ対策の実施状況、効果及び対策実施の結果としての情報セキュリティの状態を点検することが必要である。

なお、点検は客観的な視点から行なわれていると認められることが重要であり、このため点検対象の部門や者から独立した組織又は部門による監査を含めることが必要である。

点検の結果、求める情報セキュリティ水準が達成されていないと判断された場合又は情報セキュリティ対策の実施状況や効果が不十分であると判断された場合は、それについて、再発防止を考慮した改善を実施しなければならない。改善においては、府省庁対策基準等の改正、教育による府省庁対策基準等の周知徹底、情報システムや機器の更新、情報セキュリティの重要性に係る啓発等の措置を講ずることとなる。改善措置の結果については、意図した目的が達成されていることを確認する必要がある。

最高情報セキュリティ責任者は、対策推進計画に照らして自府省庁の情報セキュリティマネジメントの状況を総合的に評価し、情報セキュリティに係る取組をより一層推進するため、今後の情報セキュリティマネジメントの方向性、資源配分の見直しを行う。

また、府省庁は、本部監査（法第 25 条第１項第２号に基づく監査をいう。以下同じ。）において助言された事項についても、優先順位を検討した上で、必要に応じて上記(1)から(3)のプロセスに則り情報セキュリティ対策の見直しや改善を行う。

４　独立行政法人等における情報セキュリティマネジメント

(1)　導入・計画

法第 25 条第１項第２号に基づき作成する独立行政法人等におけるサイバーセキュリティに関する対策の基準は統一基準群を指すものとする。独立行政法人等は、３(1)に掲げる府省庁における情報セキュリティマネジメントの導入及び計画を踏まえ、対策基準等（以下「独法等ポリシー」という。）を策定する。

また、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、対策基準等に基づき、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。指定法人においては、個別の根拠法に基づき、所管府省庁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)　運用

独立行政法人等は、３(2)に掲げる府省庁における情報セキュリティマネジメントの運用を踏まえ、独法等ポリシーの浸透を図るとともに、情報セキュリティに関する取組を実施する。

また、独立行政法人等は、被害の拡大防止等の観点から、情報セキュリティインシデントに関する情報を迅速かつ有効に活用するため、所管府省庁との間の情報連絡体制を構築する。情報セキュリティインシデント対処の際には経営判断が求められる場合もあることから、この情報連絡体制は、実務者クラスと並行して、所管府省庁管理職及び当該法人役員クラスにも情報セキュリティインシデントに関する情報及び対処状況が周知される体制とする。所管府省庁は、情報共有体

制を通じて、情報セキュリティインシデント発生時の NISC への情報提供、NISC からの注意喚起等、双方向の円滑な情報連絡を図る。

(3)　点検・見直し

独立行政法人等は、３(3)に掲げる府省庁における情報セキュリティマネジメントの点検及び見直しを踏まえ、年度ごとに実施状況を把握し点検するとともに、必要に応じて見直しや改善を行う。

また、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。府省庁は、所管の指定法人に対しても、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。係る評価結果に関しては、NISC においても確認し、必要に応じて所管府省庁に対して助言等を行う。

また、独立行政法人等は、本部監査において助言された事項についても、優先順位を検討した上で、必要に応じて上記(1)から(3)のプロセスに則り情報セキュリティ対策の見直しや改善を行う。

５　情報セキュリティ対策の改善の在り方

(1)　府省庁への情報セキュリティ対策の点検

情報セキュリティ対策は、一過性のものではなく、継続的な取組が必要であることから、客観的に比較検証することが可能な判断基準による点検を実施することが重要である。

情報セキュリティ対策の実施状況の点検は、府省庁の責任において行われることが原則であるが、政府機関全体として、これを更に効果的かつ効率的に実施するため、戦略本部及び NISC は、統一基準群に基づき府省庁が定める情報セキュリティ関係規程等の整備状況及び対策の実施状況並びに府省庁の情報セキュリティマネジメントの状況について、総合的、客観的及び統一的な視点で、定期的に、又は必要に応じて点検及び本部監査を実施する。

(2)　独立行政法人等の情報セキュリティ対策の監査

独立行政法人等は、本部監査を受けるとともに、監査結果を所管府省庁に報告する。

(3)　監査結果の検証及び公表

戦略本部は、(1)及び(2)の監査結果により情報セキュリティ対策の実施等に係る課題を把握し、それを踏まえた府省庁及び独立行政法人等（以下「政府機関等」という。）の全体の取組の方向性を取りまとめ、その概要を公表するものとする。

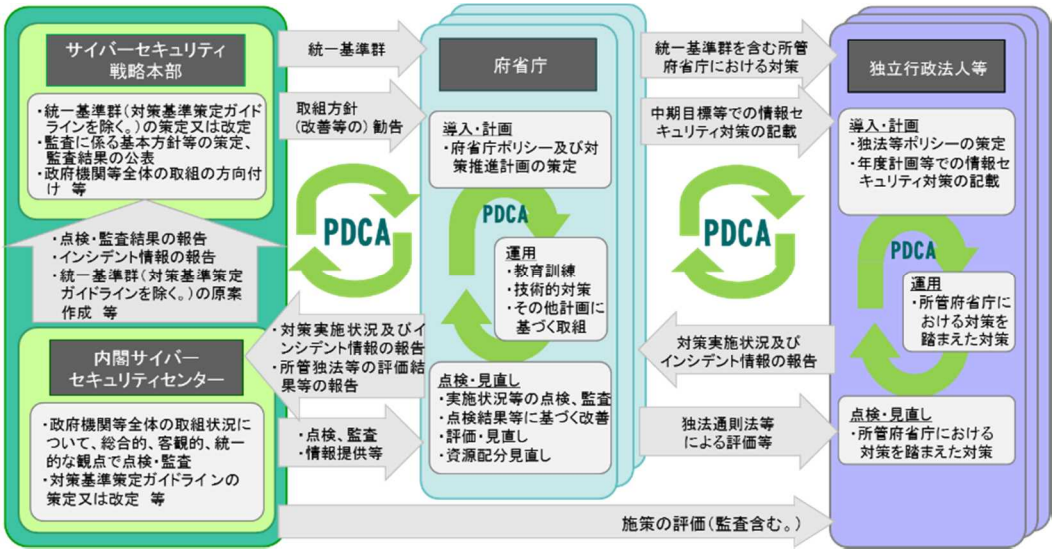


図　政府機関等における情報セキュリティマネジメントの全体像

６　情報セキュリティ対策の進め方

(1)　基本原則及び最高情報セキュリティ責任者の指揮と推進体制の確立

政府機関等の各機関における情報セキュリティの確保については、国民、企業等からの情報セキュリティ確保に関する要求や期待を踏まえた上で、自らが取り扱う情報の管理に責任を持ち、それぞれの業務や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則である。

そのためには、最高情報セキュリティ責任者は各機関における情報セキュリティ対策の推進を指揮し、その方向性を明確化するとともに、情報セキュリティ対策に必要な人員・予算等の資源配分の方針を決定する。

また、情報セキュリティ対策を効率的かつ実用的に推進するためには、取り扱う情報や業務、組織等の特性を踏まえる必要があることから、各機関において部門横断的に取り組むため、情報セキュリティ対策の推進のための組織・体制を確立する。

府省庁は、所掌の業務において機微な個人情報を含む多くの重要情報を扱っており、その適切な管理を国民から期待されていることを行政事務従事者に認識させるとともに、このような認識を日頃から所管の独立行政法人等とも共有しつつ、監督等を行っていくことが重要である。

(2)　情報セキュリティ対策の実施

政府機関等は、策定した府省庁ポリシー又は独法等ポリシーの適切な運用を通じて、一定のセキュリティ水準を確保する。また、重要な業務、情報等に対しては詳細にリスクを把握した上で情報セキュリティ対策を講ずる。

その際は、過度のセキュリティ対策の実施によってルールを潜脱する行為を招かないよう、業務要件や業務フローを考慮した上で、業務の効率・効果を高める

形で情報セキュリティ対策が講じられるようにすることが重要である。

また、政府機関等は、リスクを把握し、情報セキュリティ対策を実施する手法について、政府機関等において適用されているガイドライン等が存在する場合は、それらに沿って実施することが求められる

(3)　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

他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）については、これを使用する各機関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を整備・運用管理を行う機関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（以下「整備・運用管理機関」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、それぞれの府省庁ポリシー又は独法等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、各機関が定めるそれぞれの府省庁ポリシー又は独法等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。

(4)　情報セキュリティインシデントの情報共有

情報セキュリティインシデントに対し、政府機関等全体として迅速かつ的確に対処するためには、情報セキュリティインシデントに関する情報が組織内外の関係部門と適時・適切に共有されることが重要である。

そのため、府省庁は、当該府省庁又は所管する独立行政法人等における情報セキュリティインシデントの認知時には、当該情報セキュリティインシデントに係る情報を速やかに NISC に連絡するとともに、平時においても、収集した情報セキュリティインシデントに関する情報を NISC に連絡する。

独立行政法人等は、情報セキュリティインシデントについて、所管府省庁との間で緊密な情報共有を行う。

NISC は、平時から府省庁や外部の関係機関との情報共有の結節点となり、収集・集約された情報を情報セキュリティインシデントによる被害の未然防止又は拡大防止、応急措置・復旧のための措置及び再発防止に活用するため、情報元の同意を得た上で、府省庁に対して積極的な情報提供を行う。

(5)　情報セキュリティインシデントへの対処

府省庁は、情報セキュリティインシデントの認知時には、自らが設置した CSIRT（Computer Security Incident Response Team）を中心として、早急にその状況を確認し、被害の拡大防止及び応急措置・復旧のための措置を講ずる。

独立行政法人等も、情報セキュリティインシデントの認知時には府省庁と同様に、情報セキュリティインシデントへの対処を行う。

NISC は、情報セキュリティインシデントへの政府一体となった対応の中核となる機関として、府省庁間の連携・調整を行う。また、CSIRT の能力向上の支援等、府省庁へ技術的な支援及び助言を行い、府省庁の求めに応じて情報セキュリティ緊急支援チーム（Cyber Incident Mobile Assistance Team（CYMAT））による支援を行う。

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（案）

資料 2－5

- 実施方法：NISCのホーム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：2016年６月13日（月）～７月４日（月）
- 意見総数：13者から29件【内訳：８企業・団体から延べ20件、５個人から延べ９件】
  - ・統一規範に３件、運用指針に１件、統一基準に24件、全般に対して１件の意見提出。

（１）修正意見：全29件

- ・表現の明確化や適正化等を求めるものについては、必要に応じて趣旨を踏まえて、統一基準の解説書であるガイドラインを修正（4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（25件）

（２）主な意見

- ・クラウドサービス※の利用等の外部委託に対する意見（12件）
- ・標的型攻撃対策等の情報セキュリティの脅威への対策に対する意見（６件）
- ・情報セキュリティ対策の自己点検・監査に対する意見（３件）

※　外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

意見募集の対象外である「府省庁対策基準策定のためのガイドライン」に対しても延べ17件の意見提出。表現の明確化に関する意見について、趣旨を踏まえ修正（１件）

- （参考）提出者名：

特定非営利活動法人ＩＴプロ技術者機構、KPMGコンサルティング株式会社、（株）セールスフォース・ドットコム、日本オラクル株式会社、日本マイクロソフト株式会社、BSA｜ザ・ソフトウェア・アライアンス、秘密分散法コンソーシアム、ブルーコートシステムズ合同会社、個人（５）

資料2－6

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の改定（案）に関する意見募集の結果一覧

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	秘密分散法コンソーシアム	統一規範	P.2	第四条	政府機関の情報セキュリティ対策のための統一規範（案）の、P2、（府省庁情報セキュリティ文書）第4条3の、府省庁対策基準は、別に定める政府機関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。の記載末尾に、 尚、上記の、府省庁対策基準は、別に定める政府機関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を可能とする際には、既公開のNISC主要公表資料や公的組織の調査報告書、公的実証事業等の成果報告書等や調達可能な信頼できる民間等の最新セキュリティ技術標準化動向等の、公開資料等を参考とできる。 と、文章を追加すべきと考える。	統一規範では、府省庁が情報セキュリティ対策について行うべき基本的事項を規定しています。これを行うために参照するものとして、統一基準第1部総則1.1(5)において、府省庁対策基準の策定について定めており、御指摘の事項を含めて統一基準内で既に規定されています。
2	個人	統一規範	P.3	第十条	修文：「第十条　府省庁は、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。」 →「第十条　府省庁は、情報セキュリティ対策の動的な情報セキュリティリスク管理に基づく自己点検を行わなければならない。」 （理由） APT攻撃のような高度サイバー攻撃に実効性のある対応をするためには、脅威および脆弱性を常時監視しリスクを可視化するための動的な情報セキュリティリスク管理が必要である。このような情報セキュリティリスク管理は、ISO/IEC 27005およびNIST SP 800-137で標準化されている。我が国においても、このような標準に基づく動的な情報セキュリティリスク管理に基づく自己点検の仕組みを導入すべきである。	統一規範第三条において、リスク評価の実施及びその結果に基づく情報セキュリティ対策を講ずる旨を規定しています。第十条の自己点検は、その対策の実施状況を点検する位置づけとして規定したものになります。以上より、御指摘の内容については統一規範全体において規定済みと考えます。御指摘いただいた点につきましては、今後の検討の参考とさせていただきます。
3	個人	統一規範	P.3 P.4	第十一条	（意見内容） 修文：「第十一条　府省庁は、府省庁対策基準が本規範及び統一基準に準拠し、かつ実際の運用が府省庁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。」 →「第十一条　府省庁は、APT攻撃のような高度サイバー攻撃に実効性のある対応をするために、府省庁対策基準が本規範及び統一基準に準拠し、かつ実際の運用が府省庁対策基準に準拠していることを確認するため、監査周期を短縮化した情報セキュリティ監査を行わなければならない。」 （理由） APT攻撃のような高度サイバー攻撃に実効性のある対応をするためには、動的な情報セキュリティリスク管理を行うためのセキュリティ常時監視を導入するとともに、情報セキュリティ監査の監査周期の短縮化が必要である。	統一規範は、政府機関のとるべき枠組みを定めており、情報セキュリティ監査を府省庁自らが行わなければならないことを明確化することが本項を規定する意図であり、原案どおりとさせていただきます。なお、監査の実施時期については、ガイドライン基本対策事項の2.3.2(1)e)に記載しております。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
4	秘密分散法コンソーシアム	運用指針	P.5	5	意見内容: 「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)についての、P4、監査に係る規定整備及び政府機関等の情報セキュリティ対策の強化下段の図中(運用指針に同内容の図あり)、NISCからサイバーセキュリティ戦略本部への上向き矢印中の文言で、 ・統一基準群(対策基準策定ガイドラインを除く。)の原案策定　等と記載されているが、 ・統一基準群(対策基準策定ガイドラインを含む。)の原案策定及び決定　等 と修正すべきと考える。 理由: 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)の、P1、2　統一基準群の策定において、～対策基準策定ガイドラインは、府省庁と協議の上、NISCにおいて決定する。と記載されており、パブコメ案の、対策基準策定ガイドラインを除く。では整合性が取れない為。	統一基準群のうち、統一規範、運用指針及び統一基準はNISCにおいて原案を作成し、サイバーセキュリティ戦略本部において決定するもので、対策基準策定ガイドラインはNISCにおいて決定するものであることから、このような記述としており、整合はとれています。
5	個人	統一基準	―	全般	マイナンバーの取り扱いについて記載がないのに違和感がある。個人情報保護委員会のガイドラインはポリシーのみを記載されているものと考えられることから、政府におけるマイナンバーの取扱基準は統一基準として記載されるべきものと考える。 政府としてマイナンバーを一つも漏らさないような対策、万が一漏れてしまった場合における個人情報保護委員会との連携した対応などについてNISCが主体となって対応できるよう、本改正において必要かつ適切な事項を盛り込まなければならないと考える。 政府としてマイナンバーを取り扱うのであるから、そのセキュリティ基準は他でもないNISCが示すべきであって、他府省庁における対策に委ねることは許されない。 また、時期についても、本来であればマイナンバーの取り扱いが始まる前までに整備されるべきであり、既に手遅れと考えられることから、本改定に盛り込むべきと考えられる。	国が運営するマイナンバー関連の情報システムについても、統一基準群の対象範囲に含まれます。 ただし、統一基準群は、府省庁等の各組織がそれぞれ情報セキュリティポリシーを策定する際の情報セキュリティ対策のベースラインを定めているものであって、個別のシステムのセキュリティ要件を定める性質のものではございません。
6	日本オラクル株式会社	統一基準	P.6	1.3	【意見内容】 「クラウドサービス事業者」を「クラウドサービスを提供する事業者」と「クラウドサービスを用いて事業システムを開発・運用する事業者」に分けて定義する。 また(参考)「府省庁対策基準策定のためのガイドライン(案)」に該当箇所があるので、用語を再定義した上で記述内容を整理する。 【 理由 】 クラウドコンピューティングの参照アーキテクチャ国際規格(ISO/IEC 17789:2014)では、「クラウドサービスを提供する」ロール(Cloud Service Provider)と「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」ロール(Cloud Service Developer)を完全に分け、責任分界点を明確にしています。しかし、該当文書ではそれらを分離せずに用語を定義しているため、責任分界点が不明になる恐れがあります。ちなみに、クラウドサービスのISMS国際規格(ISO/IEC 27017:2015)もISO/IEC 17789の責任分界点を前提に記述されています。	「4.1.1 外部委託」の「目的・趣旨」において、「…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。」と明記しており、これはクラウドサービス事業者が「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事業システムを開発・運用する事業者」のいずれであろうと、それぞれの業務や責任の範囲を明らかにすることを意味しているため、特にクラウドサービス事業者の定義を変更する必要はないと考えます。

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		
7	個人	統一基準	P.14	2.2.4(1)	情報セキュリティインシデントへの対処 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に関して、 インシデントの予知・分析の対策も準備に含める。	御指摘の「インシデントの予知・分析の対策」が具体的にどのような対策を指すのか定かではありませんが、政府全体としては、政府横断的な監視によりサイバー攻撃やその準備動作等の脅威を検知するなどして情報収集を行い、関係機関に情報提供を行っています。 なお、御指摘を踏まえ、ガイドラインの解説を補足します。
8	個人	統一基準	P.15	2.2.4(3)	情報セキュリティインシデントへの対処 遵守事項 (3) 情報セキュリティインシデントの再発防止・教訓の共有に関して、 インシデント情報に関して、国内だけでなく、海外のトレンド・情報も含めた防止策・訓練・対応措置を検討していくことを追加。	統一基準群では、再発防止策等の検討に当たり情報収集を行う範囲について、国内、海外を限定しない記載としておりますが、御指摘を踏まえ、ガイドラインの解説を補足します。
9	KPMGコンサルティング株式会社	統一基準	P.18	2.3.2(2)	2.3.2(2) 監査の実施: 実施事項に、前年度の監査における指摘事項のうち未改善の事項を含むことが望ましいと考えます。	情報セキュリティ監査は、2.3.2(1)の監査実施計画及びその監査実施計画の基となる2.1.2(2)の対策推進計画に基づき実施するものです。対策推進計画は、府省庁の業務、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に基づき策定されるもので、これを受ける監査実施計画、即ち御指摘対象の「何を監査実施対象とするか」についても、当該リスク評価に基づき策定されるものとなり、「前回監査結果の未改善事項」については、この当該年度リスク評価において引き続きリスク有りと評価された場合、対象に含まれることになります。 以上のとおり、御指摘の点については既に統一基準に記載のある当該プロセスに含まれており、それのみ特出しすることで、前述の正しいプロセスやリスク評価を経ずに当該項目のみ特別扱いするかのようなミスリードのおそれもありますので、原案どおりとさせていただきます。

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		
10	KPMGコンサルティング株式会社	統一基準	P.23	3.2.1(1)(b)	3.2.1(1)(b) 要管理対策区域における対策の基準の決定: 要管理対策区域ごとに立ち入りを許可する/許可しない者を判断するための基準を追加することが望ましいと考えます。	組織や区域の特性は、府省庁又は部局等ごとに異なると考えられます。したがって、各府省庁が組織や区域の特性に応じて対策の基準をポリシーに規定できるよう、統一基準及びガイドラインでは、各府省庁に共通した基準を定めています。
11	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.24 P.28	4.1.1 4.1.4	4.1.1では、「クラウドサービスの利用に係る外部委託については、クラウド特有のリスクがあることを理解した上で、4.1.4項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。」と記述されています。クラウドが「特有の」リスクを有することは事実かもしれませんが、そのリスクが他の選択肢であるオンプレミスの情報システムなどのものよりも高いといった正しくない印象を与えることがない記載とすべきです。	御指摘の部分ですが、統一基準については、政府機関における判断材料とクラウドサービスへの要求事項を記しており、政府機関が求めるクラウドサービスの選定条件として意思表示することにより適合したクラウドサービスを市場から検索するという調達手続の方法について述べているものであって、クラウド特有のリスクが他の選択肢であるオンプレミスの情報システムなどのものよりも高いことを意図しているわけではありません。
12	(株)セールスフォース・ドットコム	統一基準	P.25	4.1.1(2)(c)	【原文】 委託先がその役務内容を一部再委託する場合には・・・ 【意見】 再委託先の管理については、再委託先のリスク管理のみならず、再委託先の選定に際し、委託元がリスク管理体制を鑑みた上で可否を申し出る権利、途中で再委託の中止の申し出の権限、適切な監査権限について、その代替案も含め記述されるべきと考えます。	御指摘の内容は、調達時の契約事項として取り扱われるものであり、統一基準においては、再委託の実施について、委託元の承認を受けることや再委託先のセキュリティ確保を委託先に担保させることなどを規定しています。
13	KPMGコンサルティング株式会社	統一基準	P.25	4.1.1(2)(c)	4.1.1(2)(c) 外部委託に係る契約: 当該規定は再委託に限定されているように見受けられますが、金融庁の監督指針を初め、世間の動向としては再委託先が更に業務を委託する(これを前述の指針では「二段階以上の委託」と表現)際にも、情報セキュリティの水準を十分に確保することが求められています。政府機関においては、その性質上大規模な情報システムも多数有することから、二段階以上の委託が発生する蓋然性が高いと思料します。このため、政府統一基準においても、再委託だけではなく二段階以上の委託先に対しても統制を可能と事項を含むことが望ましいと考えます。	契約における再々委託等の段階的な委託は様々な契約が想定されることから、統一基準においてそれらの詳細な規定はしていませんが、本規定における再委託の概念には、再々委託等の段階的な委託が含まれます。 なお、御指摘を踏まえ、誤解がないようガイドラインにて補足いたします。

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		
14	(株)セールスフォース・ドットコム	統一基準	P.26	4.1.2	【原文】　約款による外部サービスの利用 目的・趣旨 【意見】 省庁内での業務遂行において今後この約款による外部サービスは不可避のものとなると考えられます。この場合にこれらの検討を「やむを得ず」、「例外的に」と言った表現を使うことでその普及を根本から阻害する印象を与えかねません。積極的にこれらの検討も適正なリスク管理の元行っていくことを示し、選択肢の一つとすることを望みます。	本項では、政府機関において取り扱う情報の特性に鑑み、リスクを考慮の上、約款による外部サービスを利用してよい範囲等を定めて利用することを規定しており、約款による外部サービスの普及を阻害することは考えておりません。
15	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.26 P.28	4.1.2、4.1.4	①「約款による外部サービス」による取扱いを禁止される情報の範囲が過度に広くならないよう、該当する「要機密情報」の適用範囲を最も機微な情報に限定するよう狭めることを提言します。 ②本基準群中の記載により、クラウドサービスが「約款による外部サービス」ではないことを明示することを求めます。例えば、本ガイドラインの7頁に記載されている参考図を用いて、異なる外部委託サービスの関係についての説明を本基準群に含めることを提言します。 ③「約款による外部サービス」により「要機密情報」の取り扱いが禁止されるのは、当該サービスの約款の内容が要機密情報を扱う要件を満たしていない場合に限られる旨を明確にすべく、本基準群の記載を修正するよう提案します。 ④外部委託業者（特にクラウドサービスプロバイダー）が適切なセキュリティ対策を有するか否かを確認するために、政府機関は、利用可能な様々なセキュリティ対策に関する情報（例えば、第三者によるクラウドサービスプロバイダーの監査レポート、情報セキュリティに関する国際規格への準拠状況を活用すべきことを明確にしていただけるようお願いします。クラウドサービスプロバイダーが政府担当者による直接の現地調査を受け入れることを要件とすべきではありません。そのような要件は現実的でも効果的でもなく、間接的にデータやハードウェアを国内に置かせることを要求する結果を招くからです。	①要機密情報は、1.2節「情報の格付の区分」に規定するとおり、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り、要機密情報を範囲とすることについては過度に広くないと判断しています。 ②「クラウドサービス」は「約款による外部サービス」とは異なるものであることを、1.3節「用語の定義」において、条件設定の余地の有無により規定しています。 ③上記①のとおりです。 ④統一基準において、具体的な認定・認証制度等は規定すべき性質のものではないことからその旨記述はしていませんが、ガイドラインの解説部分では、参考となる認証や報告書等について例示しております。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
16	日本マイクロソフト株式会社	統一基準	P.28	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の目的・趣旨の小項目において、「クラウドサービスの委託先」との表現があるが、概念の受け止め方の違いによって理解に混乱が生じるおそれがある。 というのも、同遵守事項の小項目において、(1) クラウドサービスの利用における対策の(a) を見ると、「クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり」という表現が出てくる。そうすると、同(b)(c)(e)で出てくる「クラウドサービス」の「委託先」という表現は、両者（前者であれば民間事業者が提供する場合のさらに委託先として下請け業者を指すこととなり、後者であれば政府が自ら提供する場合の委託先としてクラウドサービス提供事業者自身を指すことになろうか）を含む概念になってしまい分かりにくい。 そもそも、4.1.4は全体的に、政府機関がクラウドサービスの利用者であって、政府機関内部向けであろうと住民サービスであろうと一定の業務について、その一部をクラウドサービス提供事業者に委託するというシナリオを前提にしているように読める。そうであれば、「委託先」という表現は避けて「クラウドサービス提供事業者」とするなど、混乱が生じないように分かりやすく表現してほしい。	「4.1.1 外部委託」の「目的・趣旨」において「…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。」と記述しており、混乱や誤解が生じることはないものと理解しています。
17	日本マイクロソフト株式会社	統一基準	P.28	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の遵守事項の小項目において、(1) クラウドサービスの利用における対策の(e) を見ると、「各種の認定・認証制度の運用状況等から」との表記がある。これに対して、具体的な例示は、府省庁対策基準策定のためのガイドライン（案）P118で3つの例（ISO/IEC 27017、クラウド情報セキュリティ監査、SOC報告書）が出てくるが、その重要性からしても読み手の理解の容易性からしても、ガイドラインではなく統一基準の中で例示すべきである。また、その際には、ISO/IEC 27017をベースとしたクラウド情報セキュリティ監査に基づく我が国固有のクラウドセキュリティマーク制度がせっかく新設されて運用が開始されているのだから、それについてまず記載するべきである。次にそのベースとなったISO/IEC 27017について記載し、そのあとでSOC報告書について記載するのが妥当である。なおISO/IEC 27017について記載する際には、単に国際規格というだけでなく、認定機関による認証がなされていることを含め正確な記載をしていただきたい。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。

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		
18	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.1.4	4.1.4遵守事項(1)(b)は、「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」を挙げています。BSAは準拠法、裁判管轄、適用される法令・規則を確認することの重要性について同意します。しかし、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、データの保存場所を指定する必要はないはずです。クラウドサービスがもたらす優位性の多くは、国境を越えたデータ移動が可能であることによりもたらされます。よって、そのような移動を制限し、データが「特定の場所」にあることの説明を求めることは、データのセキュリティを何ら増すことがないのに、クラウドサービスやプロバイダーを制限することになってしまいます。データのセキュリティは物理的な保管場所に依存するのではなく、データを保護するための品質の高い機能、効果的な手段、制御の行き届いた管理によってもたらされます。	4.1.4(1)(b)の規定は、「必要に応じた」ものであり、委託事業の実施場所を常に指定するものではありません。また、クラウドサービス利用契約において準拠法が合意されている場合でも、例えば次のような国内法以外の法令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います。 委託事業者の法人としての国籍が外国籍であって、サーバが国外にある場合に、実態的に国内法以外の法令が適用されるようなケース
19	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.1.4	委託先のクラウドサービスプロバイダーを選定する上で評価・判断するための要件として、関連する国際規格への準拠や認証を活用する旨、本ガイドラインにとどまらず、本基準群において明示するよう求めます。 また、米国政府が採用している、セキュリティ評価と認証における標準的手法の提供を目指すFederal Risk and Authorization Management Program（FedRAMP）のような、政府機関向けクラウドサービス認証制度の採用を推奨します。 これらを併せて用いることにより、情報システムセキュリティ責任者は、クラウドサービスプロバイダーを包括的に評価することができ、目的に対して、最も費用対効果が高く、安全で、機能に優れたクラウドサービスを選定する確率を高めることができます。また、結果として、公共部門にとどまらず、安全で効果的なクラウドサービスの導入の更なる普及を推進することになります。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインへ記載することとしています。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
20	ブルーコートシステムズ合同会社	統一基準	P.28	4.1.4	修正案） 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を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・裁判管轄の指定、又はトークン化・暗号化等のデータ保護の方法を定めること。 d）情報システムセキュリティ責任者は、個別の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サービス側、オンプレミス側共にセキュリティ要件を定めること。 f）情報システムセキュリティ責任者は、管理外の端末やクラウドのリスクを考慮してクラウドサービスの制御について検討し、クラウドの可視化やその監査、脅威やデータ漏洩からの保護について要件として対策を検討すること。 理由） b）既に国内法以外の法令が適用されるクラウドサービスに対し、国内法によるデータ保護が可能なソリューションが実用化されているため。 d）個別のクラウドサービス及び接続する方法によってセキュリティリスクは異なるため、共通のセキュリティ要件で網羅することは難しいため。 f）クラウドサービスのセキュリティとしてオンプレミス側で認められている技術であり、考慮が必要と考えられるため。	b）遵守事項(1)(b)において、国内法以外の法令が適用されるリスクを評価した上で、国内法以外の法令が適用されるクラウドサービスを選択した場合、遵守事項(1)(d)における「クラウドサービスの特性」に関する基本対策事項にて記される「f)クラウドサービス上で取り扱う情報の暗号化」をクラウドサービスに求め、契約内容に含められる旨が謳われているため、あえて遵守事項(1)(b)での「トークン化・暗号化等のデータ保護の方法を定めること」は内容的に重複となることから、現状のままといたします。 d）ご指摘のとおり、個別のクラウドサービス及び接続する方法によってセキュリティリスクは異なるため、ガイドラインの基本対策事項4.1.4(1)-2において、セキュリティ要件を例示しつつ、取捨選択等することにより、各々のリスクに対応できるよう自由度を持たせる構成にしてあるため、現状のままといたします。 f）については、どのような対策を指しているのか定かではありませんが、ガイドラインの基本対策事項4.1.4(1)-2において、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対策を構築するに当たっての要件を例示しており、オンプレミス側で認められている技術も包含しているとの認識であるため、現状のままといたします。
21	（株）セールスフォース・ドットコム	統一基準	P.28	4.1.4	【原文】クラウドサービスの利用 【意見】 日本政府として行政機関におけるクラウドサービス活用推進は世界最先端 IT 国家創造宣言や日本再興戦略においてもうたわれているところであり、今後積極的な利用を推進されることと推察いたします。しかし、ガイドラインも含め本章の表現にはその普及を根本から阻害するような危険性を煽る印象を与える可能性がある記述が散見されます。通常の情報システムサービスでも同様のこと、またはそれ以上の危険性が伴う場合もあります。このためクラウドサービスによるメリットがいかにあったとしても、それを採用することに躊躇する可能性があります。危険性を記述するのであれば、通常の情報システムについても同様に記述が必要と考えます。利用促進を後押しできる表現を再考いただくことを望みます。 また、米国のFedRampをはじめとして諸外国では行政機関がクラウドサービスの利用促進ができるように認証制度を作っています。現にこの認証制度によりクラウド利用が進んでいます。日本でも同様の制度を作ることをご提案いたします。	御指摘の部分ですが、統一基準については、政府機関における判断材料とクラウドサービスへの要求事項を記しており、政府機関が求めるクラウドサービスの選定条件として意思表示することにより適合したクラウドサービスを市場から検索するという調達手続の方法について述べているものであって、普及を根本から阻害するような趣旨ではないと考えます。

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		
22	特定非営利活動法人 ITプロ技術者機構	統一基準	P.31	5.2.1	「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」の原則が、要否の判断の条件「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」と一体にして示されているため、訴求性が弱くなり明確になっていない。 これでは、インターネットに接点を有する情報システムから分離すること」の原則が、その組織の情報システムセキュリティ責任者の判断に明確に反映されず、実施が不十分となることが危惧され、政府機関の統一基準として不適切ではないかと考えられる。 つまり、だれにでもわかりやすく統一された判断基準の提示が必要と思われるので、例えば、(a)項を下記に変更する。 「(a)情報システムセキュリティ責任者は、重要な情報を扱う情報システム（情報の格付等に基づき判断する）については、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（クラウドサービスを含む。）から分離することとし、分離する情報システムについても、分離しない情報システムについても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。」	「情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等」を、「分離すること」の要否の判断条件として規定しており、遵守事項は明確であると考えます。さらに、ガイドラインにおいて、特に重要な情報を取り扱うシステムは分離すべき旨を解説として記述しています。このようなことから、実施が不十分になるといった御懸念には及ばないものと考えます。
23	個人	統一基準	P.36	6.1.1	遵守事項(1)(a)で「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」ことが求められ、6.1.3 権限の管理　遵守事項(1)(a)で、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。」が求められている。 この統一基準（案）に対応する府省庁対策基準策定のためのガイドライン（28 年度版）（案）の基本対策事項6.1.3(1)-1では、一般的な情報システムの特性を考慮に入れ「主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、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として、 a) 業務上必要な場合に限定する b) 必要最小限の権限のみ付与する c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする の3点が例示されている。 しかし、最近の脅威の動向および主体に対する認証技術の動向を考慮して、また、2010年8月に各府省情報化統括責任者（CIO）連絡会議で決定された「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を参考に「複数要素認証」の導入を図り、アクセス制御技術の強化を図るべきではないかと考える。少なくとも、複数要素認証の導入を検討すべきだと考える。 特に、マイナンバーカードの導入に伴い、全ての担当者に対して身分証明書としての「マイナンバーカード」が発行される状況となったので、「知識」の認証要素としての「パスワード」と「所有」の認証要素として「マイナンバーカード」を用いた「二要素認証」を実現する素地は整ってきたと考える。	主体認証方式は、情報の格付等に応じて適当な方式が決定されることが求められるため、今般の改定においては一律に複数要素認証を遵守事項として位置づけておりません。 主体認証を行う情報システムにおいて、情報セキュリティ強度の更なる向上を図るために導入を検討するべき具体例として、多要素認証をガイドラインに掲載しておりますが、御指摘を踏まえ、ガイドラインの解説を補足します。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
24	KPMGコンサルティング株式会社	統一基準	P.40	6.2.1(1)(c)	6.2.1(1)(c) ソフトウェアに関する脆弱性対策の実施: ソフトウェアに関連する脆弱性情報を定期的に入手し、脆弱性対策計画を策定し、措置を講じることが望ましいと考えます。政府統一基準(案)では、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」と限定されているため、意図的に入手しない場合に必要な対策が講じられない可能性があります。	脆弱性対策の状況を定期的に確認することは6.2.1(1)(d)で規定しており、御指摘の「意図的に入手しない」行為は統一基準に反する行為であり、当然入手する努力は求められます。
25	KPMGコンサルティング株式会社	統一基準	P.41	6.2.2(1)(b)	6.2.2(1)(b) 不正プログラム対策の実施: 想定される不正プログラムの感染経路を特定することを明確化することが望ましいと考えます。	具体的な対策は統一基準に規定すべき性格のものではなく、ガイドラインに記載することとしています。なお、御指摘の点については、ガイドラインの基本対策事項において規定しています。
26	個人	統一基準	P.42	6.2.4	(意見内容) 修文:目的・趣旨 「――――、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。」 →「――――、多重防御の情報セキュリティ対策体系並びにセキュリティ常時監視によって、標的型攻撃に備える必要がある。」 (理由) 実効性のある標的型攻撃(APT攻撃)対策は、検知された脅威に対する対策だけでは不十分であり、すり抜けた脅威に対しては、自己の動的な情報セキュリティリスク管理のためのセキュリティ常時監視対策を追加する必要がある。	御指摘の標的型攻撃対策の目的・趣旨に対する御意見については、本項の遵守事項6.2.4(1)(b)において、外部との不正通信を検知して対処する対策(内部対策)として規定しております。
27	個人	統一基準	P.42	6.2.4	標的型攻撃対策 遵守事項に関して、 標的型攻撃により、情報漏えいが起きた場合でも、その漏えい情報が制御可能な手段を多重防衛の対策の1つとして検討していくこと。	具体的な手段の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。 なお、御指摘いただきました漏えい情報の制御可能な手段については、その有効性を見極めつつ、今後の取組の参考とさせていただきます。

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		
28	KPMGコンサルティング株式会社	統一基準	P.42	6.2.4(1)	6.2.4(1) 標的型攻撃対策の実施： 当該対策は、入口対策・内部対策・出口対策として整理することが望ましいと考えます。政府統一基準（案）では、内部対策にいわゆる出口対策の概念が入っているように見受けられますが、入口対策に対して内部対策という表現のみ用いた場合、表現が対になっておらず、出口対策の概念の理解が困難となり、本来政府統一基準が意図する対策が十分に施されないおそれがあると考えます。	内部対策には出口対策も含まれております。入口と出口を対にさせるよりも、外部からの侵入に対する入口対策だけではなく、侵入されることを前提に内部対策を講ずることが重要であることを強調するために現在の構成となっています。
29	個人	全般	P.228	7.2.2	行政機関全てのサイトにおいてhttpsアクセスの有効化とTLSv1.2の実装とPFS対応の暗号スイート利用の設定を行っていただきたい。 go.jpへのアクセスは全ての場合において狙われやすい事を各省庁に周知すべきであり、その前提で上記の措置を早急に行っていただきたい。	ガイドライン7.2.2(1)-5において、ウェブサーバの実装として、 1）TLS（SSL）機能を適切に用いる。 2)「SSL/TLS暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。 旨が記述されており、特に「SSL/TLS暗号設定ガイドライン」では暗号スイートとして、DHE、ECDHE方式の設定も含まれ、これらはPFSの特性を有しています。なお「行政機関全てのサイトにおいてhttpsアクセスの有効化」については、今後の検討の参考とさせていただきます。

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		
30	秘密分散法コンソーシアム	ガイドライン	P.80	3.1.1(6)(a)(b)	府省庁対策基準策定のためのガイドライン（案）のうち、データ送受信や移送が発生する箇所と、そうしたデータ送受信や移送に必要な機器、回線やメディア、関係する業者等に関しては、電子情報の移送（モバイルPCやUSBメモリー等も含む）に関しては、これまでのNISC公表の、統一管理基準やその解説書、府省庁対策基準策定のためのガイドライン等を参考とし、 遵守事項(6) 情報の運搬・送信 ＜3.1.1(6)(a)(b)関連＞3.1.1(6)-2 b) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。 （解説） 例えば、1個の電子情報について、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるように、秘密分散技術を適切に用いて分割して移送を行うこと。 なお、暗号と併用する場合には、分割前であっても分割後の複数生成ファイルに行っても良いが、分割前に暗号化を行うことで、管理すべき暗号鍵の管理数を抑制することができる。 分割後に暗号化する手法としては、要機密情報を秘密分散技術を用いて2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。 と修正し、各該当箇所に 遵守事項(6) 情報の運搬・送信 ＜3.1.1(6)(a)(b)関連＞3.1.1(6)-2 b) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。 を参照するよう追記する。 また、電子情報の保管（BCPも含め）に関しては、これまでのNISC公表の、統一記述基準解説書の記載事項を参考として、各該当箇所に、セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。 と、下記理由記載の、既公表主要文書の、政府機関の情報セキュリティ対策のための 統一技術基準（平成 24 年度版）解説書の記載事項を参考とし、暗号と併記するなどして、例示すると良いと考える。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 秘密分散技術以外にもデータを分割してセキュアに送信等行う方法が存在する可能性があることから、特定の技術を指定しないよう記載を見直しています。 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。
31	秘密分散法コンソーシアム	ガイドライン	P.80 P.81	3.1.1(6)-2 b)	該当箇所記載部分の、例えば、1個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを2個に分割し、～ の部分は、これまで継続して主要公開資料等で同一部分の記載内容を参考とし、 例えば、1個の電子情報について、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるように、秘密分散技術を適切に用いて分割して移送を行うこと。 なお、暗号と併用する場合には、分割前であっても分割後の複数生成ファイルに行っても良いが、分割前に暗号化を行うことで、管理すべき暗号鍵の管理数を抑制することができる。 分割後に暗号化する手法としては、要機密情報を秘密分散技術を用いて2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。 とすべきと考える。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 秘密分散技術以外にもデータを分割してセキュアに送信等行う方法が存在する可能性があることから、特定の技術を指定しないよう記載を見直しています。 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。

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	秘密分散法コンソーシアム	ガイドライン	P.82	3.1.1(7)(b)	これまでNISC主要公表資料の中で記載されてきている、「秘密分散技術」を適切に用いることで実現できる為、府省庁対策基準策定のためのガイドライン（案）の、P82～83、 （解説） 遵守事項3.1.1(7)(b)「抹消する」についての、最後尾（P83上部）には、 更に、要機密情報である書面を電磁的記録媒体に記録する際に、当初から「秘密分散技術」を適切に用いて、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるような処理を行ったものだけを記録する方法もある。 と追加し、P83中段の、遵守事項3.1.1(7)(c)「復元が困難な状態にする」については、その最後尾に、更に、秘密分散技術を適切に用いて、電子情報として事実上の廃棄処理を行い、生成された複数の割符ファイルを個別に適切に管理することにより、「復元が困難な状態にする」手法があり、こうした情報運用管理を日常的に行っていれば、不正アクセス等によって、組織内から完全な情報が一度に漏えいすることは発生しにくくなるメリットが期待できる。 と記載すると良いと考えられる。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の内容については、今後の技術の進展を見つつ、検討の参考とさせていただきます。
33	日本マイクロソフト株式会社	ガイドライン	P.115	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の目的・趣旨の小項目において、「クラウドサービスの委託先」との表現があるが、概念の受け止め方の違いによって理解に混乱が生じるおそれがある。 というのも、同遵守事項の小項目において、(1) クラウドサービスの利用における対策の(a) を見ると、「クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり」という表現が出てくる。そうすると、同(b)(c)(e)で出てくる「クラウドサービス」の「委託先」という表現は、両者（前者であれば民間事業者が提供する場合のさらに委託先として下請け業者を指すこととなり、後者であれば政府が自ら提供する場合の委託先としてクラウドサービス提供事業者自身を指すことになろうか）を含む概念になってしまい分かりにくい。 そもそも、4.1.4は全体的に、政府機関がクラウドサービスの利用者であって、政府機関内部向けであろうと住民サービスであろうと一定の業務について、その一部をクラウドサービス提供事業者に委託するというシナリオを前提にしているように読める。そうであれば、「委託先」という表現は避けて「クラウドサービス提供事業者」とするなど、混乱が生じないように分かりやすく表現してほしい。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 「4.1.1 外部委託」の「目的・趣旨」において「…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。」と記述しており、混乱や誤解が生じることはないものと理解しています。

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		
34	日本マイクロソフト株式会社	ガイドライン	P.118	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 P118で3つの例（ISO/IEC 27017、クラウド情報セキュリティ監査、SOC報告書）が出てくるが、その重要性からしても読み手の理解の容易性からしても、ガイドラインではなく統一基準の中で例示すべきである。また、その際には、ISO/IEC 27017をベースとしたクラウド情報セキュリティ監査に基づく我が国固有のクラウドセキュリティマーク制度がせっかく新設されて運用が開始されているのだから、それについてまず記載するべきである。次にそのベースとなったISO/IEC 27017について記載し、そのあとでSOC報告書について記載するのが妥当である。 なおISO/IEC 27017について記載する際には、単に国際規格というだけでなく、認定機関による認証がなされていることを含め正確な記載をしていただきたい。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。 JASAのCSマーク制度の記載提案について、ガイドラインの解説において「その他、日本セキュリティ監査協会のクラウド情報セキュリティ監査…を活用することも考えられる。」として紹介しております。
35	日本マイクロソフト株式会社	ガイドライン	P.116 P.120	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 遵守事項4.1.4(1)(a)「情報の取扱いを委ねることの可否」について、の解説で、「クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため・・・」との表記がある。 しかし、当該情報の中身に関与しないクラウドサービスにおいては、当該情報の管理責任はあくまで利用者の側に留保される。 例えば、4.1.4(1)-2c)「クラウドサービスの委託先による情報の管理・保管」について、の解説で、「当該情報の責任は利用者である情報オーナーが負うことになる」と言っているのはそのような趣旨であろう。情報オーナー（Data Subject）、情報管理者（Data Controller）、情報処理者（Data Processor）という違いを意識すべきであり、クラウドサービス事業者が常に情報管理主体となることを前提とするように読める冒頭のような記述は削除すべきであり、責任分界点はクラウドサービス内容によって異なることが分かるように記載いただきたい。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 御指摘の遵守事項4.1.4(1)(a)及びその解説において、クラウドサービスの委託先による情報の管理や処理をもって当該情報の管理責任がクラウドサービス事業者側にあるとは規定していません。ガイドラインの基本対策事項4.1.4(1)-2c)の解説に、「当該情報の責任は利用者である情報オーナーが負う」と明確に記載することで誤解は生じないものと考えます。

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	日本マイクロソフト株式会社	ガイドライン	P.116	4.1.4(1)(a)	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 遵守事項4.1.4(1)(a)「情報の取扱いを委ねることの可否」について、の解説で、リスクとして挙げられている項目の「不特定多数の利用者の情報やプログラムを一つのクラウド基盤で共用することとなるため、情報が漏えいするリスクが存在する」との表記がある。 しかし、共用すること自体から情報が漏えいするリスクが導かれるような表現は誤解を生じる。 例えば、一戸建てなら安全だがマンションは建物を共用しているので盗難にあうリスクがある、というと論理飛躍で違和感があるのと同様である。この部分は削除とするか、「・・・共用することとなるため、個々のユーザーごとの環境の分離が適切に行われていることの確認を行うこと」といった方向での内容にすべきである（ISO/IEC 27017の13.1.3 Segregation in Networkを参照する等）。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 この解説の目的は、2～4行目で「そこで、適切なクラウドサービス事業者を選定することにより以下のようなリスクを低減することが考えられる。」のとおり、『適切なサービス事業者の存在を強調すること』です。よって、御指摘の表現は、政府機関側の読者にとっては留意すべきリスクとして理解しやすい例示であり、上記の適切なサービス事業者を強調するとの事項と併せ、バランスを取った表現としたものです。

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		
37	日本オラクル株式会社	ガイドライン	P.127 P.128	5.1.2(1)(a)	以下の「ISO/IEC 15408に基づく認証」に関する記述を「参考事項」に変更する。 ・基本対策事項　＜5.1.2(1)(a)関連＞ [現案] 5.1.2(1)-2・・・ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準と して定めること。 [提案] 5.1.2(1)-2・・・ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の参考事項として機器等の選定基準に加えるこ と。 ・（解説）基本対策事項5.1.2(1)-2「ISO/IEC 15408に基づく認証」について [現案] 機器等の調達においては、ISO/IEC 15408に基づく認証を取得している製品の優遇を選定基準の一つとすることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。 [提案] 機器等の調達においては、ISO/IEC 15408に基づく認証を取得している製品を参考事項に加えることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。但し、どの時点の保証を得ている認証製品であるかを調達時に確認することが必要となることと、認証の取得には一定期間が必要なため、選定対象を認証製品に限定すると最新の製品や技術の恩恵を受けられない制約になることを理解する必要がある。 【理由】 ISO/IEC15408に基づく認証は国際的な極めて重要な枠組みと考えます。しかしその認証取得には長期の審査と多大な経費が必要となります。実際問題として、新製品のリリースから認証取得まで長い期間を必要とするため、当該認証取得を評価項目に加えると、古い製品又はセキュリティ対策能力の低い製品が選定され、結果として情報システム全体のセキュリティ強度が低下するなど、セキュリティ対策が後手に回ります。 現在、セキュリティ対策はリスクマネジメントフレームワークを活用したリスクベースの対策へ軸足を移しつつあると認識していますので、典型的なチェックベースのポリシーであるISO/IEC15408認証取得を参考事項として位置付けることが良いと考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 ガイドライン基本対策事項5.1.2(1)-2では、ISO/IEC15408に基づく認証の取得を調達時の評価項目とすることを定めていますが、第三者による客観的な評価を必要と判断する場合に限るものであり、一律の基準ではないため、御指摘の御懸念には及ばないと考えます。

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		
38	BSA｜ザ・ソフトウェア・アライアンス	ガイドライン	P.133	5.2.1(2)(a)	5.2.1の遵守事項(2)(a)及び府省庁対策基準策定のためのガイドライン（28年度版）（以下「本ガイドライン」）（133頁）における「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」に関する記述を削除することを求めます。これにより、本基準群が政府職員に対して情報システムのセキュリティを確保するための最も効果的な方法がインターネットからの分離であるとの誤解を生じさせてしまうことを防ぐことができます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 インターネットに接点を有する情報システムにおいては、メール等の標的型攻撃による不正プログラム感染は避けられないものになっており、既に政府機関において様々な取組を進めているところ、本規定は、その一つを情報システムを構築する際の重要な要件として規定したものです。「インターネットに接点を有する情報システムから分離すれば他の対策は不要」といった趣旨ではなく、あくまで対策事項の一つとして位置づけられるものです。
39	（株）セールスフォース・ドットコム	ガイドライン	P.133	5.2.1(2)(a)	【原文】情報システムのセキュリティ要件の策定 【意見】 本項のガイドラインの解説には、「特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、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。）から分離することが求められる」とありますが、昨今の標的型攻撃による情報漏えい事件はインターネットに繋がった情報システムから漏洩する事案だけでなく、インターネットからはアクセス出来ない情報システムからの漏洩も多く存在しております。インターネットに繋がっているから危険なのではなく、利用する者のリテラシーおよびネットワーク構成、インターネットに繋がっていない情報システムのあり方にも依存するので、限定的に「インターネットに接点を有する情報システムからを分離することを求める」事が対策にはならないのではと考えます。記載について再考いただくことを望みます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 インターネットに接点を有する情報システムにおいては、メール等の標的型攻撃による不正プログラム感染は避けられないものになっており、既に政府機関において様々な取組を進めているところ、本規定は、その一つを情報システムを構築する際の重要な要件として規定したものです。「インターネットに接点を有する情報システムから分離すれば他の対策は不要」といった趣旨ではなく、あくまで対策事項の一つとして位置づけられるものです。
40	（株）セールスフォース・ドットコム	ガイドライン	P.133	5.2.1(2)(a)	【原文】情報システムのセキュリティ要件の策定 【質問】 本項のガイドラインの解説には、「特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、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。）から分離することが求められる」とありますが、この「特に重要な情報」とは機密性3の情報という理解でよろしいでしょうか？	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 政府機関が特に重要な情報と考える情報であり、機密性3情報と規定していません。

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		
41	KPMGコンサルティング株式会社	ガイドライン	P.163	6.1.2(1)-1 d)	解説　基本対策事項6.1.2(1)-1 d)「ネットワークセグメントの分割によるアクセス制御」について セグメンテーションの分割による分離を実施した場合、そのセグメンテーションが有効であることを定期的に検証する観点を取り入れることが望ましいと考えます。当該有効性の確認手段の例として、ペネトレーションテスト等が考えられます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 御指摘の内容については、遵守事項5.2.3(1)(a)及び基本対策事項5.2.3(1)-2において、セキュリティ機能の適切な運用を求める規定に含まれております。
42	KPMGコンサルティング株式会社	ガイドライン	P.165	6.1.3(1)-1 b)	解説　基本対策事項6.1.3(1)-1 b)「必要最小限の権限のみ付与」について 標準で組み込まれた識別コード（例　WindowsにおけるAdministrator等）を無効化する観点も取り入れることが望ましいと考えます。この観点は基本対策事項として定義することも考えられます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 不要な管理者権限アカウントの削除については、ガイドラインの基本対策事項6.2.4(1)-4a)において規定しています。
43	KPMGコンサルティング株式会社	ガイドライン	P.168	6.1.4(1)(b)	解説　遵守事項6.1.4(1)(b)「保存期間」について 世間の動向に鑑みると、不正アクセス発生等から1年以上経過したのちに情報漏えい等が検知される事例も多数あるため、ログの推奨保存期間が1年で十分か否かを、再度検討することが望ましいと考えます。（当然に設備投資の費用対効果の観点もあるため、それらを踏まえた検討が必要と思料します）	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 御指摘の点については承知しており、解説において「過去の事例を踏まえ、ログは1年以上保存することが望ましい」としております。

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		
44	KPMGコンサルティング株式会社	ガイドライン	P.181	6.2.2(1)(c)	基本対策事項 ＜6.2.2(1)(c)関連＞について 6.2.2(1)-5 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実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。 a) 不正プログラム対策ソフトウェア等の導入状況 b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況 上記例示として、電子メールに添付されている実行形式ファイルの不用意な実行防止や最近のランサムウェアによる被害の増加を勘案し、 c) 外部から入手した実行形式ファイルの実行を不可能となるように設定 d) 添付ファイルとして実行形式ファイルを付した電子メールの送受信遮断 e) 不正プログラム対策に係る適時のデータバックアップの徹底 を追記することが望ましいと考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 御指摘の実行プログラム形式ファイルの取扱いについては、基本対策事項8.1.1(2)-2、データバックアップについては、遵守事項3.1.1(8)(a)において規定を設けています。
45	KPMGコンサルティング株式会社	ガイドライン	P.188	6.2.4(1)(a)	解説　遵守事項6.2.4(1)(a)「標的型攻撃」について 標的型攻撃への対策として、以下の事項も有効であると考えます。 ・6.1.1項　主体認証機能 ・6.1.2項　アクセス制御機能 ・6.1.3項　権限管理機能 ・6.1.4項　ログの取得・管理 ・6.1.5項　暗号・電子署名	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘を踏まえ、解説を補足します。
46	KPMGコンサルティング株式会社	ガイドライン	P.187	6.2.4(1)-2 e)	基本対策事項　6.2.4(1)-2 e) USBポートの無効化のみならず、CD/DVDドライブの原則無効化も例示することが望ましいと考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方をお示しします。 最も危険性が高いUSBメモリの対策について例示していますが、本項の規定で、「USBメモリ等の外部電磁的記録媒体」が対象であることを明記しており、御指摘のCD/DVDドライブについても含まれるため、原案どおりとさせていただきます。