政府機関等の対策基準策定のためのガイドライン（案）
（平成 30 年度版）

平成 30 年　月　日

内閣官房 内閣サイバーセキュリティセンター

目次

第1部 総則

1.1 目的

政府機関等の対策基準策定のためのガイドライン（以下「本ガイドライン」という。）は、国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）が政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の規定を遵守するための対策事項について、対策基準を策定する際に参照するものであり、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、対策基準の策定及び実施に際しての考え方等を解説するものである。これにより、機関等が、統一基準を遵守するための対策事項として、本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対策基準を定められるようにすることを目的とする。

1.2 対策基準の策定手順

機関等は、基本方針に基づき、統一基準に定める遵守事項等の規定を満たすよう、具体的な対策事項を対策基準に規定する必要がある。

対策基準の構成としては、統一基準と本ガイドラインと同様に、遵守事項と対策事項を分けて記載する方法や、対策事項のみを記載する方法などが考えられるが、機関等の状況に応じてよりよい構成とすることが望ましい。

本ガイドラインに規定される基本対策事項は、必ず実施すべき事柄である遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要がある。

遵守事項に対して、本ガイドラインに対応する基本対策事項が規定されている場合は、個別具体的な対策事項を対策基準に規定することが求められる。ただし、機関等の規模、情報システムの構成、取り扱う情報の内容・用途等の特性によって、達成すべき情報セキュリティの水準やとるべき具体的な対策は異なり得ることから、基本対策事項に記載された対策とは別の対策により、基本対策事項と同等以上の情報セキュリティ水準が確保できると判断される場合は、当該対策事項を対策基準に定めてよい。

1.3 本ガイドラインの改定

情報セキュリティの水準を適切に維持・向上させていくためには、脅威の変化や技術の進展を的確にとらえ、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、本ガイドラインの規定内容については、環境の変化に応じて適宜内容の見直

しを行い、必要に応じて項目の追加やその内容の充実等を図ることによって、規定内容の適正性を将来にわたり維持することとする。

機関等においては、本ガイドラインが更新された場合には、その内容をそれぞれの対策基準に適切に反映させることが期待される。

1.4 統一基準、本ガイドライン及び実施手順の関係

政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）、政府機関等の情報セキュリティ対策の運用等に関する指針（サイバーセキュリティ戦略本部決定。以下「運用指針」という。）及び統一基準と本ガイドラインの関係は図 1.4-1 のとおりであり、これらを総称して、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（以下「統一基準群」という。）と呼ぶ。また、統一基準群と機関等の情報セキュリティポリシーの関係についても、併せて図 1.4-1 に示す。

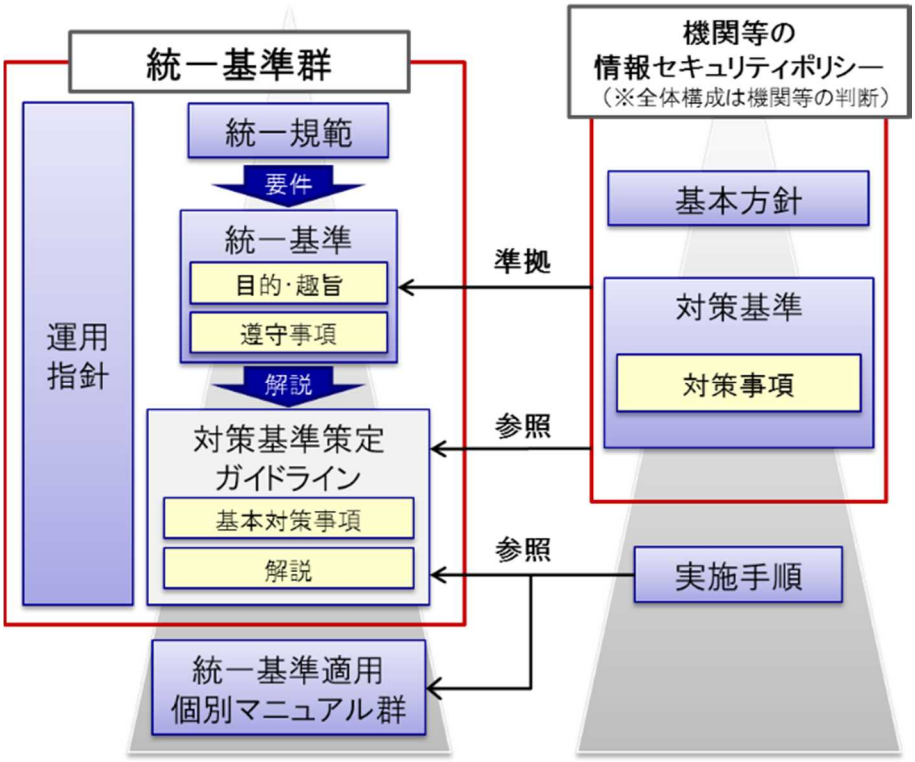


図 1.4-1 統一基準群と機関等の情報セキュリティポリシーの関係について

1.5　統一基準で定義されている用語

統一基準 1.2 において定義されている情報の格付の区分・取扱制限、1.3 において定義されている用語を以下に再度掲載する。

(1) 情報の格付の区分

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

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

機密性についての格付の定義

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

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

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

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

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

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

(2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを職員等に確実に行わせるための手段をいう。

職員等は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。機関等は、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定

める必要がある。

【参考】 取扱制限の例

取扱制限は、情報の機密性、完全性、可用性等の内容に応じた情報の取扱方法を具体的に指定するものであるから、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たすために適切に明示等する必要がある。以下の例のように、代表的な取扱制限を指定してもよい。例えば「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」等と記載しても目的を果たせると考えられる。

機密性についての取扱制限の定義の例

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配布について	配布禁止、配布要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

上記の指定方法の意味は以下のとおり。

- 「○○禁止」
  当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
- 「○○要許可」
  当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
- 「暗号化必須」
  当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。
- 「○○限り」
  当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「○○課内限り」「○○会議出席者限り」等、参照を許可する者が分かるように指定する。

・　「〇月〇日まで〇〇禁止」
　〇月〇日まで複製を禁止したい場合、「〇月〇日まで複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

例えば、上記の「〇〇要許可」は、「〇〇する行為を禁止するが、許可を得ることにより〇〇することができる」という意味を持たせている。取扱制限は、このように、職員等にとって簡便かつ分かりやすい表現を採用することが望ましい。

完全性についての取扱制限の定義の例

取扱制限の種類	指定方法
保存期間について	〇〇まで保存
保存場所について	〇〇において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

情報の保存期間の指定の方法は、以下のとおり。
・　保存の期日である「年月日」又は期日に「まで保存」を付して指定する。
例）平成〇〇年７月 31 日まで保存
例）平成〇〇年度末まで保存
・　完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。
例）年度内保存文書用共有ファイルサーバに保存
例）３か年保存文書用共有ファイルサーバに保存

可用性についての取扱制限の定義の例

取扱制限の種類	指定方法
復旧までに許容できる時間について	〇〇以内復旧
保存場所について	〇〇において保存

復旧許容時間の指定の方法は以下のとおり。
・　復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。
例）１時間以内復旧
例）３日以内復旧
・　可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用にお

いては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、端末のファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。

例）課室共有ファイルサーバ保存必須

例）各自 PC 保存可

(3) 統一基準 1.3「用語定義」において定義されている用語

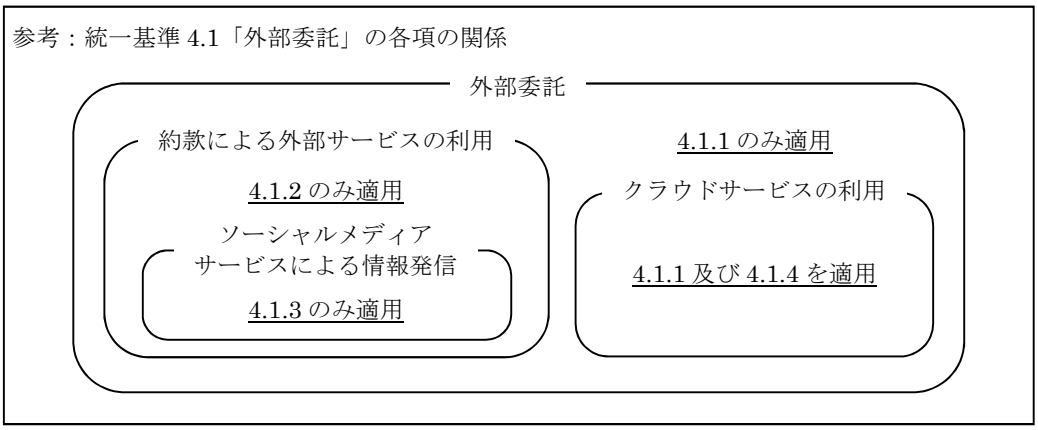
【あ】

● 「アプリケーション・コンテンツ」とは、アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

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

【か】

● 「外部委託」とは、機関等の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。



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

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

● 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部電磁的記録媒体等の総称をいう。（参考：図 1.5-1）

● 「基盤となる情報システム」とは、他の機関等と共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

● 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体

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

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

● 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

参考：JIS X 9401:2016（抄）

- クラウドサービス（cloud service）
  定義されたインタフェースを使って呼び出されるクラウドコンピューティング経由で提供される一つ以上の能力。
- クラウドコンピューティング（cloud computing）
  セルフサービスのプロビジョニング（provisioning）及びオンデマンド管理を備える，スケーラブルで伸縮自在な共有できる物理的又は仮想的なリソース共用へのネットワークアクセスを可能にするパラダイム。

注記：リソースの例には，サーバ，OS，ネットワーク，ソフトウェア，アプリケーション及びストレージが含まれる。

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

【さ】

● 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するものをいう。

● 「CYMAT（サイマット）」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。

● 「CSIRT（シーサート）」とは、機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。

● 「実施手順」とは、対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

● 「情報」とは、統一基準の「1.1(2) 本統一基準の適用対象」の(b)に定めるものをいう。（参考：図 1.5-2）

> 参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）
> (b) 本統一基準において適用対象とする情報は、以下の情報とする。
> (ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
> (イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報
> (ウ) (ア)及び(イ)のほか、機関等が調達し、又は開発した情報システムの設計又は運用管理に関する情報

● 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機関等が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。（参考：図 1.5-1）

> 参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）
> (c) 本統一基準において適用対象とする情報システムは、本統一基準の適用対象となる情報を取り扱う全ての情報システムとする。

● 「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。

> 参考：JIS Q 27000:2014（抄）
> ・ 情報セキュリティインシデント
> 望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
> ・ 情報セキュリティ事象
> 情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

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

● 「情報セキュリティ対策推進体制」とは、機関等の情報セキュリティ対策の推進に係る事務を遂行するため、当該機関等に設置された体制をいう。

● 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

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

【た】

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

● 「端末」とは、情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機関等が調達又は開発するもの以外を指す「機関等支給以外の端末」がある。また、機関等が調達又は開発した端末と機関等支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。

● 「通信回線」とは、複数の情報システム又は機器等（機関等が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機関等の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機関等が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

● 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

● 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は内蔵電磁的記録媒体を備えているものをいう。

【は】

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

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

● 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

● 「約款による外部サービス」とは、民間事業者等の外部の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

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

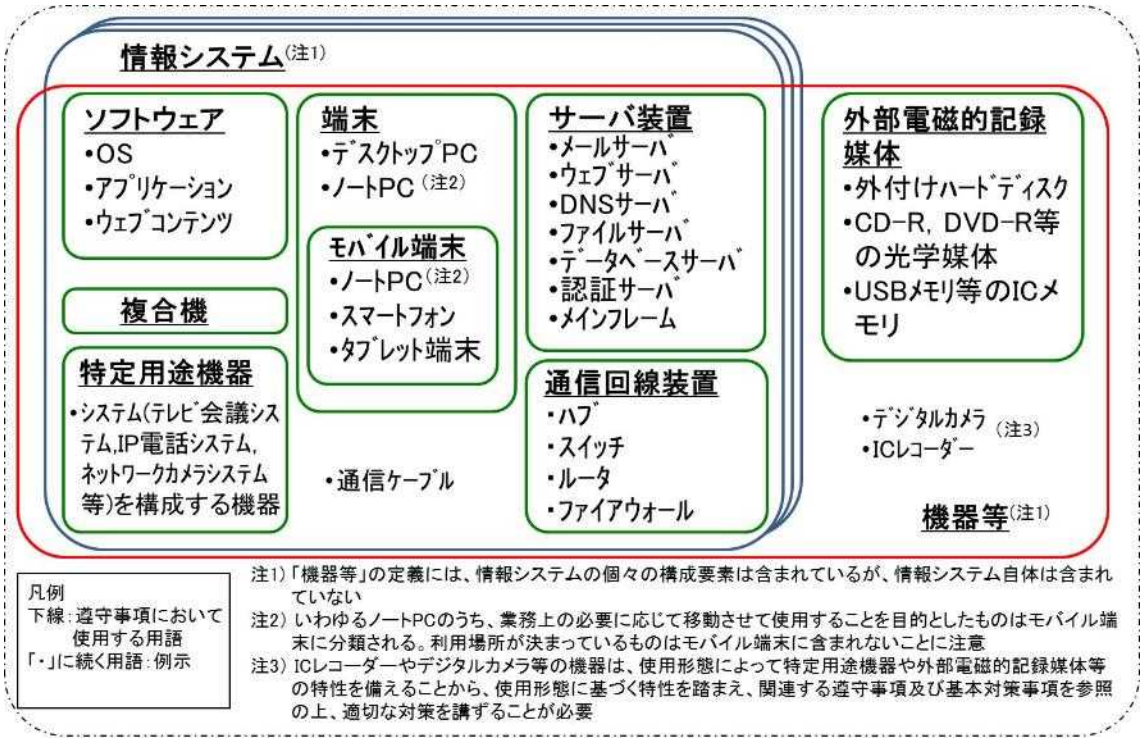


図 1.5-1　「情報システム」、「機器等」及びその関係

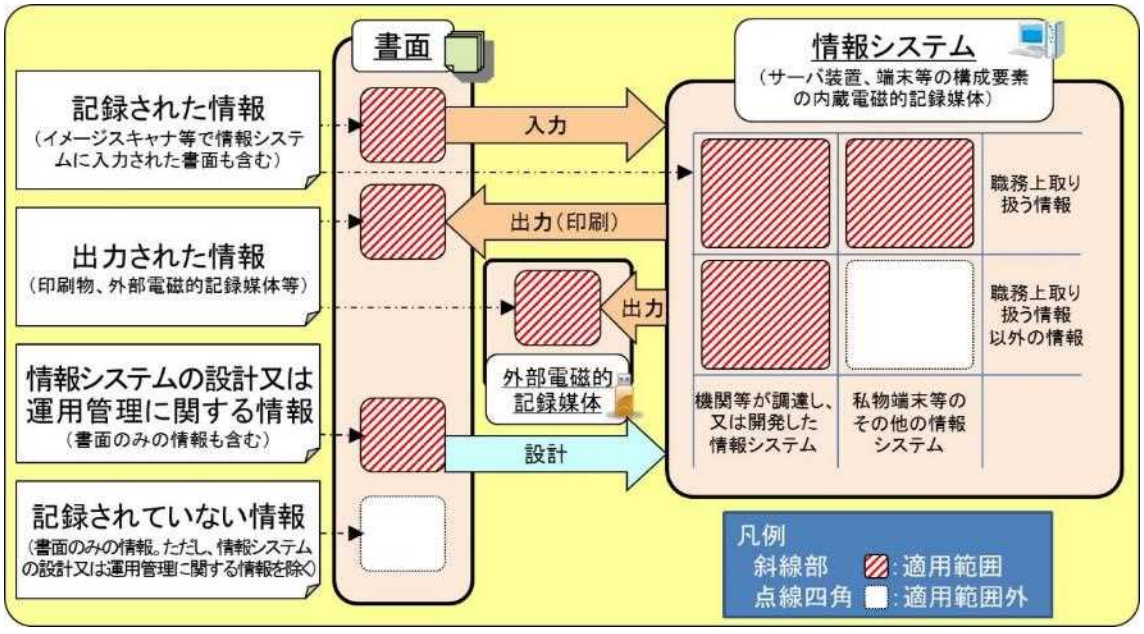


図 1.5-2　統一基準の適用を受ける「情報」の範囲

1.6　一般用語の解説

留意すべき一般用語を以下に解説する。

【あ】

● 「アクセス制御」とは、情報又は情報システムへのアクセスを許可する主体を制限することをいう。

● 「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

● 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。

● 「暗号化」とは、第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。

● 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。

● 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

【か】

● 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。

● 「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

● 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。

● 「業務継続計画」とは、機関等において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。

● 「共用識別コード」とは、複数の主体が共用するために付与された識別コードをいう。原則として、一つの識別コードは一つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。

● 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

● 「サービス不能攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサ

ーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。

● 「最小限の特権機能」とは、管理者権限を実行できる範囲を必要最小限に制限する機能をいう。

● 「識別」とは、情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

● 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

● 「主体」とは、情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。

● 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。

● 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

● 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

● 「セキュリティパッチ」とは、発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

● 「ソフトウェア」とは、サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

【た】

● 「耐タンパ性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。

● 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

● 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

● 「電子メールサーバ」とは、電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。

● 「ドメインネームシステム（DNS）」とは、クライアント等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について回答を行うシステムである。

● 「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.nisc.go.jp というウェブサイトの場合は、nisc.go.jp の部分がこれに該当する。

【な】

● 「名前解決」とは、ドメイン名やホスト名と IP アドレスを変換することをいう。

【は】

● 「複合機」とは、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機器をいう。

● 「不正プログラム定義ファイル」とは、不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。

● 「踏み台」とは、悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

【ま】

● 「無線 LAN」とは、IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad 等の規格により、無線通信で情報を送受信する通信回線をいう。

【ら】

● 「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。

● 「ルートヒントファイル」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC （Internet Network Information Center）のサイトから入手可能である。

【A～Z】

● 「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプ

ロジェクトである。

- 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の２種類に分けることができる。

- 「IPv6 移行機構」とは、物理的に一つのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、サーバ装置及び端末並びに通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。

- 「MAC アドレス（Media Access Control address）」とは、機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組合せによって表される。

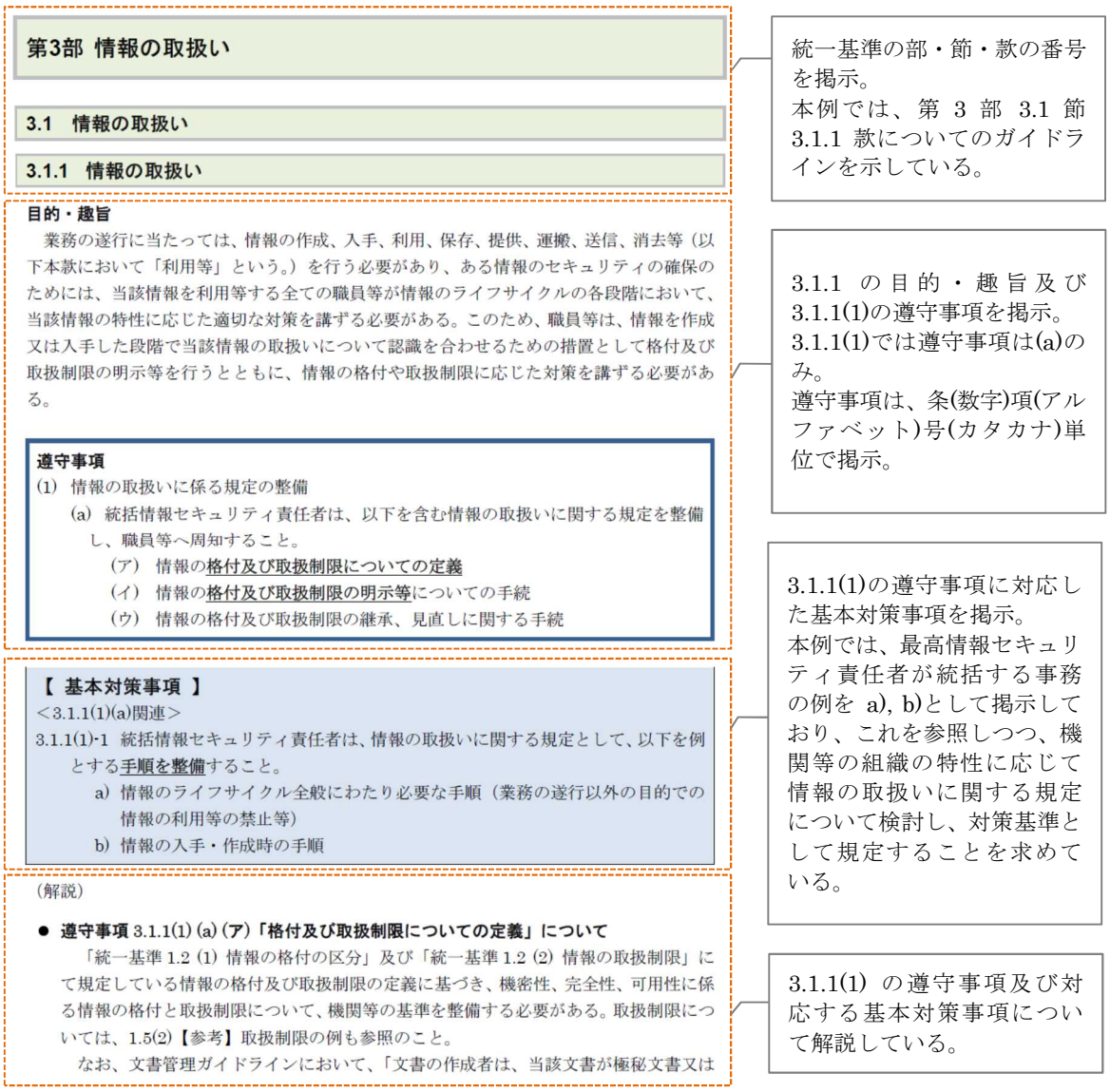
- 「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。

- 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。

1.7　基本対策事項及び解説の読み方

本ガイドラインの第２部以降に記述する遵守事項に対応した基本対策事項及び解説を参照するに当たり、留意すべき点を以下に示す。なお、以下の抜粋は、紙面の関係上、実際の記載内容から一部の文や規定を削除しているので、実際の記載内容は本文を確認すること。

◆第２部以降の基本的な記述構成



統一基準の部・節・款の番号を掲示。
本例では、第 3 部 3.1 節 3.1.1 款についてのガイドラインを示している。

3.1.1 の目的・趣旨及び 3.1.1(1)の遵守事項を掲示。
3.1.1(1)では遵守事項は(a)のみ。
遵守事項は、条(数字)項(アルファベット)号(カタカナ)単位で掲示。

3.1.1(1)の遵守事項に対応した基本対策事項を掲示。
本例では、最高情報セキュリティ責任者が統括する事務の例を a), b)として掲示しており、これを参照しつつ、機関等の組織の特性に応じて情報の取扱いに関する規定について検討し、対策基準として規定することを求めている。

3.1.1(1) の遵守事項及び対応する基本対策事項について解説している。

◆基本対策事項に個別対策事項が例示されている場合

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。

【 基本対策事項 】
＜6.1.2(1)(a)関連＞
6.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。
a) 利用時間や利用時間帯によるアクセス制御
b) 同一主体による複数アクセスの制限
c) IP アドレスによる端末の制限
d) ネットワークセグメントの分割によるアクセス制御
e) ファイルに記録された情報へのアクセスを制御するサーバにおいて認証されたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

複数の方法が考えられる基本対策事項については、具体例を示している。

◆基本対策事項の個別対策事項について、“～を含む”として例示されている場合

遵守事項
(2) IoT 機器を含む特定用途機器
(a) 情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

【 基本対策事項 】
＜7.1.3(2)(a)関連＞
7.1.3(2)-1 情報システムセキュリティ責任者は、特定用途機器の特性に応じて、以下を含む対策を講ずること。ただし、使用している特定用途機器の機能上の制約により講ずることができない対策を除く。
a) 特定用途機器について、主体認証情報を初期設定から変更した上で、適切に管理する。
b) 特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。
c) 特定用途機器が備える機能のうち利用しない機能を停止する。
d) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器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に接続しない。
e) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
f) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。
g) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。
h) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する。

基本対策事項が複数の事項から構成される場合は、主要な事項のみを含むべき事項として示している。

◆基本対策事項が規定されていない場合

2.1.2　対策基準・対策推進計画の策定

目的・趣旨

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

遵守事項

(1) 対策基準の策定

(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠した対策基準を定めること。また、対策基準は、機関等の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。

【 基本対策事項 】規定なし

遵守事項が具体的な対策事項となっている場合は、基本対策事項を定めていない。
この場合は、遵守事項の解説を参照し、対策基準を定めることになる。

（解説）

- **遵守事項 2.1.2(1)(a)「情報セキュリティ委員会における審議を経て、統一基準に準拠した対策基準を定める」について**

  対策基準の策定に当たっては、あらかじめ、情報セキュリティ委員会において審議を行うとともに、情報セキュリティの知見を持つ者に意見を求めるなどして、規定内容の網羅性や妥当性等について確認した上で決定することが望ましい。

第2部 情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1 組織・体制の整備

目的・趣旨

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

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

遵守事項

(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置

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

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

【 基本対策事項 】

＜2.1.1(1)(a)関連＞

2.1.1(1)-1 最高情報セキュリティ責任者は、次に掲げる事務を統括すること。

a) 情報セキュリティ対策推進のための組織・体制の整備
b) 対策基準の決定、見直し
c) 対策推進計画の決定、見直し
d) **情報セキュリティインシデント**に対処するために必要な指示その他の措置
e) 前各号に掲げるもののほか、情報セキュリティに関する重要事項

（解説）

- **遵守事項 2.1.1(1)(a)「最高情報セキュリティ責任者」について**

最高情報セキュリティ責任者は、機関等における情報セキュリティ対策の推進の責任者であり、機関等全体の情報セキュリティ対策を推進するため、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することが求められる。その

際には、国内外の情報セキュリティに関連する動向を注視するとともに、有益な最新の技術の活用を検討するなど、先手を打って必要な対策をとることが重要である。

最高情報セキュリティ責任者は、情報セキュリティに関する機関等全体の方向付けを行う事務について自ら直接関与すべきであることから、統一基準では、対策基準及び対策推進計画を決定するとともに、重大な情報セキュリティインシデントが発生した場合には、それに対処するための必要な指示その他の措置を行うこととしている。

なお、国の行政機関に置かれる最高情報セキュリティ責任者においては、所管する独立行政法人及び指定法人において情報セキュリティ対策が適切に推進されるようにすることについても、役割として求められる。

- **遵守事項 2.1.1(1)(b)「最高情報セキュリティ副責任者」について**

最高情報セキュリティ副責任者は、最高情報セキュリティ責任者からの委任（最高情報セキュリティ責任者が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、最高情報セキュリティ責任者に残る。）に基づき、最高情報セキュリティ責任者を助けて、機関等の情報セキュリティ対策に係る事務を総括整理する役割を担う。

このため、最高情報セキュリティ副責任者には、機関等において情報セキュリティ対策について一定程度の専門性を有するとともに、最高情報セキュリティ責任者を助け、組織全体として整合性の取れた方針等の策定、人的資源及び予算等の計画的で持続可能な投入等を実施していく役割が求められる。

なお、国の行政機関に置かれる最高情報セキュリティ副責任者においては、最高情報セキュリティ責任者を助けて、所管する独立行政法人及び指定法人において情報セキュリティ対策が適切に推進されるようにすることについても、役割として求められる。

- **基本対策事項 2.1.1(1)-1 d)「情報セキュリティインシデント」について**

情報セキュリティインシデントについては、統一基準 1.3「用語の定義」（本ガイドライン 1.5「統一基準で定義されている用語」）に示すとおりであるが、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものとして、実際に業務等への影響は顕在化していないものの、そのおそれがある場合を含むことに留意する必要がある。情報システムに関する情報セキュリティインシデントとしては、例えば、以下が考えられる。

  - 要機密情報が含まれる電子メールの外部への誤送信
  - 要機密情報が保存された USB メモリの紛失
  - 不正プログラムへの感染
  - 外部からのサーバ装置、端末への不正侵入
  - サービス不能攻撃等による情報システムの停止

遵守事項

(2) 情報セキュリティ委員会の設置

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

【 基本対策事項 】

＜2.1.1(2)(a)関連＞

2.1.1(2)-1 情報セキュリティ委員会の委員長及び委員は、最高情報セキュリティ責任者が情報セキュリティ対策推進体制及びその他の業務を実施する部局の代表者から指名すること。

2.1.1(2)-2 情報セキュリティ委員会は、次に掲げる事項を審議すること。

a) 対策基準

b) 対策推進計画

c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

（解説）

- **遵守事項 2.1.1(2)(a)「情報セキュリティ委員会」について**

最高情報セキュリティ責任者は、横断的な事項を審議するため、情報セキュリティを推進する情報セキュリティ対策推進体制及び各部局（部門）の代表者から構成される委員会を設置する。

委員長及び委員は、最高情報セキュリティ責任者の指名によるが、最高情報セキュリティ責任者自らが委員長を兼ねてもよい。

委員会は、各部門間の意見調整を図り情報セキュリティ対策と組織の方針を整合的なものとする機能を持つことから、組織全体としての方向付けを要する対策基準及び対策推進計画を審議事項とする必要がある。その他の審議事項については、機関等の実態に応じて柔軟に運用すればよいが、例えば、遵守事項 2.1.1(6)に規定する情報セキュリティ対策推進体制に担わせる具体的な役割や、その役割に基づく情報セキュリティ対策の推進状況の確認・評価に係る事項を審議することが考えられる。

また、委員会の配下に実務を担当する下位委員会を設置し、実務レベルの詳細な事項を調整することで、委員会の運営を効率化することも考えられる。

遵守事項

(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。

【 基本対策事項 】

＜2.1.1(3)(a)関連＞

2.1.1(3)-1 情報セキュリティ監査責任者は、命により次の事務を統括すること。

a) 監査実施計画の策定

b) 監査実施体制の整備

c) 監査の実施指示及び監査結果の最高情報セキュリティ責任者への報告

d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（解説）

- **遵守事項 2.1.1(3)(a)「情報セキュリティ監査責任者」について**

機関等における情報セキュリティ対策は、最高情報セキュリティ責任者の指揮の下で推進することとなるが、最高情報セキュリティ責任者は、自らが決定した情報セキュリティ対策が適切に実施されているか否かを正しく把握する必要がある。そのため、最高情報セキュリティ責任者は、情報セキュリティ監査責任者にその実施状況等の確認を行わせることにより、情報セキュリティ対策の実効性を確保しようとするものである。

なお、情報セキュリティ監査責任者は、組織のまとまりごとの情報セキュリティに関する事務を担う情報セキュリティ責任者よりも職務上の上位の者を置くことが望ましい。

情報セキュリティ監査責任者は、情報セキュリティ対策が適切に実施されているか否かを監査し、その結果について最高情報セキュリティ責任者に的確に報告しなければならない。

情報セキュリティ監査責任者は、これら監査事務を効率的に実施するため、担当者（監査実施者）を置き、必要に応じて外部組織を活用するなど、監査実施体制の整備を行う。

なお、機関等の実情に応じて、監査責任者を補佐する立場として監査副責任者を独自に設置してよい。

遵守事項

(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置

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

(b) 情報セキュリティ責任者は、遵守事項3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する**区域情報セキュリティ責任者** 1人を置くこと。

(c) 情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する**課室情報セキュリティ責任者**1人を置くこと。

(d) 情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、**情報システムセキュリティ責任者**を、当該情報システムの企画に着手するまでに選任すること。

【 基本対策事項 】

＜2.1.1(4)(a)関連＞

2.1.1(4)-1 統括情報セキュリティ責任者は、命を受け、次の事務を統括すること。

a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

b) 情報セキュリティ対策に関する実施手順の整備及び見直し並びに**実施手順**に関する事務の取りまとめ

c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

d) 例外措置の適用審査記録の台帳整備等

e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

2.1.1(4)-2 情報セキュリティ責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。

a) 定められた区域ごとの区域情報セキュリティ責任者の設置

b) 課室の課室情報セキュリティ責任者の設置

c) 情報システムごとの情報システムセキュリティ責任者の設置

d) 情報セキュリティインシデントの原因調査、再発防止策等の実施

e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備

f) 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

＜2.1.1(4)(b)関連＞

2.1.1(4)-3 区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び

環境に係る情報セキュリティ対策に関する事務を統括すること。
＜2.1.1(4)(c)関連＞
2.1.1(4)-4 課室情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括すること。
＜2.1.1(4)(d)関連＞
2.1.1(4)-5 情報システムセキュリティ責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。
2.1.1(4)-6 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管理業務において必要な単位ごとに**情報システムセキュリティ管理者**を置くこと。

（解説）

- **遵守事項 2.1.1(4)(a)「情報セキュリティ責任者」について**

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となる組織のまとまりごとに、その対策を委ねた方が効率的であることから、取りまとめの責任者として、情報セキュリティ責任者を設置する。情報セキュリティ対策の運用が可能なまとまりとしては、国の行政機関においては、部局（内局、外局、地方支分部局等、附属機関）ごとが想定される。独立行政法人及び指定法人においては、法人の組織構成によるが、例えば、役員を除く職員等の中で最も高位の職にある者が長となる組織のまとまりごととすることが想定される。

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の委任に基づき、所管する組織の情報セキュリティ対策を推進及び運用するため、組織内の体制整備及び事務を行う。

- **遵守事項 2.1.1(4)(a)「統括情報セキュリティ責任者」について**

最高情報セキュリティ責任者は、自らの事務及び最高情報セキュリティ副責任者の事務を補佐させるため、組織のまとまりごとに設置する情報セキュリティ責任者のうちから１人を統括情報セキュリティ責任者として選任する。

統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの委任（最高情報セキュリティ責任者が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、最高情報セキュリティ責任者に残る。）に基づき機関等の情報セキュリティ対策について総合調整する事務を担うとともに、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する役割を担う。例えば、対策基準や対策推進計画の案の作成を担うことが想定される。

- **遵守事項 2.1.1(4)(b)「区域情報セキュリティ責任者」について**

情報セキュリティ責任者は、所管する組織のまとまりの情報セキュリティ対策のうち施設及び環境に係る対策について、定められた区域ごとにその対策を推進する責任者として区域情報セキュリティ責任者を指名する。

区域情報セキュリティ責任者は、所管する区域について規定された対策の基準に従い、自ら対策を定めそれを実施する。また、区域情報セキュリティ責任者は、その役割

の性質上、施設の管理者が兼任することが想定される。定める単位としては、例えば以下が考えられる。

- 単一の課室が利用する執務室及び会議室を管理する場合は、課室情報セキュリティ責任者
- 情報システムが設置された部屋（サーバ室等）を管理する場合は、情報システムセキュリティ責任者
- ロビー、廊下等を管理する場合は、施設等の管理に関する部門の責任者

なお、基本対策事項 3.2.1(1)-1 で後述するクラス１は、施設管理の観点から行う措置が、情報セキュリティ上の対策と同等であれば、施設の管理者が指定されていることをもって、区域情報セキュリティ責任者を設置しているとみなしてよい。

- **遵守事項 2.1.1(4)(c)「課室情報セキュリティ責任者」について**

情報セキュリティ責任者は、課室又はこれと同等の組織単位内の情報の取扱い及び情報セキュリティ対策の責任者として、課室情報セキュリティ責任者を設置する。課室情報セキュリティ責任者は、情報の取扱い等に関して、その是非を判断する役割を担うため、課室長又はそれに相当する者であることが望ましい。

- **遵守事項 2.1.1(4)(d)「情報システムセキュリティ責任者」について**

情報セキュリティ責任者は、情報システムごとの情報セキュリティ対策及び運用の責任者として、情報システムセキュリティ責任者を指名する。

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ライフサイクル全般にわたって適切に情報セキュリティ対策を実施することが求められる。このため、情報セキュリティ責任者は、新規の情報システムについて企画に着手するまでに情報システムセキュリティ責任者を選任しなければならない。機関等 LAN システムのような機関等内で共通的に利用されるシステム、特定部門における個別業務システム等、機関等の全ての情報システムについて、情報システムごとにセキュリティ対策の運用の責任の所在を明確にすることが重要である。また、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にする必要がある。

情報システムセキュリティ責任者は、情報セキュリティ対策の技術的事項について補佐する者（基本対策事項 2.1.1(4)-6 で定める情報システムセキュリティ管理者）をデータベース、アプリケーション等の装置・機能ごとに、必要に応じて置き、技術的対策の実効性を確保することが望ましい。

- **基本対策事項 2.1.1(4)-1 b)「実施手順」について**

「（解説）遵守事項 2.2.1(1)(a)「実施手順を整備（本統一基準において整備すべき者を別に定める場合を除く。）」について」を参照のこと。

- **基本対策事項 2.1.1(4)-6「情報システムセキュリティ管理者」について**

情報システムセキュリティ管理者は、情報システムセキュリティ責任者が定めた手順や判断された事項に従い、所管する情報システムのセキュリティ対策を実施する。

遵守事項

(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。

【 基本対策事項 】

＜2.1.1(5)(a)関連＞

2.1.1(5)-1 最高情報セキュリティ責任者は、以下を例とする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。

a) 機関等全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者及び最高情報セキュリティ副責任者への助言
b) 情報セキュリティ関係規程の整備に係る助言
c) 対策推進計画の策定に係る助言
d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
e) 情報システムに係る技術的事項に係る助言
f) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
g) 職員等に対する日常的な相談対応
h) 情報セキュリティインシデントへの対処の支援
i) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（解説）

- **遵守事項 2.1.1(5)(a)「最高情報セキュリティアドバイザー」について**

最高情報セキュリティ責任者は、情報セキュリティに関する技術的事項等について自ら及び最高情報セキュリティ副責任者への助言等を含む機関等の情報セキュリティ対策への助言、支援等を行う者として最高情報セキュリティアドバイザーを置く。

最高情報セキュリティアドバイザーは、機関等における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち情報セキュリティに関する資格及び実務経験を有する者である必要がある。

なお、外部人材のみならず機関等内の職員等を充ててもよい。この場合、当該職員等が情報セキュリティ責任者やその他の責任者を兼務してもよい。

遵守事項

(6) 情報セキュリティ対策推進体制の整備

(a) 最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制を整備し、その役割を規定すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。

【 基本対策事項 】

＜2.1.1(6)(a)関連＞

2.1.1(6)-1 最高情報セキュリティ責任者は、以下を含む情報セキュリティ対策推進体制の役割を規定すること。

a) 情報セキュリティ関係規程及び対策推進計画の策定に係る事務
b) 情報セキュリティ関係規程の運用に係る事務
c) 例外措置に係る事務
d) 情報セキュリティ対策の教育の実施に係る事務
e) 情報セキュリティ対策の自己点検に係る事務
f) 情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

- **（解説）遵守事項 2.1.1(6)(a)「機関等の情報セキュリティ対策推進体制を整備」・基本対策事項 2.1.1(6)-1「情報セキュリティ対策推進体制の役割を規定する」について**

機関等の情報セキュリティ対策を推進するためには、組織横断的に施策を取りまとめて推進する情報セキュリティ対策推進体制が必要であり、本項では、そのような体制とその役割を組織として明確化することを求めている。

情報セキュリティ対策推進体制の基本的な役割は、本基本対策事項各号に定める事項を基本とし、組織の特性等に応じ、その他必要な事項を追加するなどして規定する必要がある。その他にも、例えば以下の事項を役割として担うことが考えられる。

- 情報セキュリティ委員会の運営に係る事務
- サイバーセキュリティ基本法第 25 条第 1 項第 2 号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（以下「本部監査」という。）への対応に係る事務
- 内閣官房内閣サイバーセキュリティセンターから発出される事務連絡や調査依頼事項等への対応に係る事務

また、「(解説) 遵守事項 2.1.1(4)(a)「統括情報セキュリティ責任者」について」に記載のとおり、統括情報セキュリティ責任者が機関等の情報セキュリティ対策について総合調整する事務を担っていることから、情報セキュリティ対策推進体制は、統一基準において統括情報セキュリティ責任者の役割として規定されている事項に係る実務を含む事務を担う体制として位置付けるとよい。

さらに、遵守事項 6.2.1(1)(c)において情報システムセキュリティ責任者に求めている脆弱性対策の状況の定期的な確認を支援するために、ソフトウェアに関する脆弱性情報の公開状況を確認し、情報システムセキュリティ責任者と情報共有を行うなど、情報

システムの情報セキュリティ対策を推進するための事務を担うことなども考えられる。

- **遵守事項 2.1.1(6)(b)「情報セキュリティ対策推進体制の責任者」について**

  「（解説）遵守事項 2.1.1(6)(a)「機関等の情報セキュリティ対策推進体制を整備」・基本対策事項 2.1.1(6)-1「情報セキュリティ対策推進体制の役割を規定する」について」において記述しているとおり、情報セキュリティ対策推進体制は、統括情報セキュリティ責任者が担う実務を中心とした事務を遂行するための体制として機能させることを想定している。そのため、本項で定める責任者として、統括情報セキュリティ責任者を充てることが考えられる。ただし、実際の組織構成等に応じて統括情報セキュリティ責任者以外の者を充てることを妨げるものではない。

遵守事項

(7) 情報セキュリティインシデントに備えた体制の整備

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

(b) 最高情報セキュリティ責任者は、職員等のうちから **CSIRT に属する職員等**として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、機関等における情報セキュリティインシデントに対処するための責任者として **CSIRT 責任者**を置くこと。また、**CSIRT 内の業務統括及び外部との連携等を行う職員等**を定めること。

(c) 最高情報セキュリティ責任者は、**情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制**を整備すること。

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

【 基本対策事項 】

＜2.1.1(7)(a)関連＞

2.1.1(7)-1 最高情報セキュリティ責任者は、以下を含む CSIRT の役割を規定すること。

a) 機関等に関わる情報セキュリティインシデント発生時の対処の一元管理

- **機関等全体における情報セキュリティインシデント対処の管理**
- 情報セキュリティインシデントの可能性の報告受付
- 機関等における情報セキュリティインシデントに関する情報の集約
- 所管する独立行政法人及び指定法人における情報セキュリティインシデントに関する情報の集約（当該法人を所管する国の行政機関に限る。）
- 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化

b) 情報セキュリティインシデントへの迅速かつ的確な対処

- 情報セキュリティインシデントであるかの評価
- 被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
- 内閣官房内閣サイバーセキュリティセンターへの連絡（国の行政機関に限る。）
- 法人を所管する国の行政機関への連絡（独立行政法人及び指定法人に限る。）
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- 他の機関等への情報セキュリティインシデントに係る情報の共有
- 情報セキュリティインシデントへの対処に係る**専門的知見の提供、対処作業の実施**

2.1.1(7)-2 最高情報セキュリティ責任者は、**実務担当者を含めた実効性のある CSIRT 体制**を構築すること。

2.1.1(7)-3 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

際に、情報セキュリティインシデント対処に関する知見を有する**外部の専門家等による必要な支援を速やかに得られる体制**を構築しておくこと。

2.1.1(7)-4 最高情報セキュリティ責任者は、機関等全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の**役割分担を規定**すること。

（解説）

- **遵守事項 2.1.1(7)(a)「CSIRT」について**

機関等の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、当該機関等が、最高情報セキュリティ責任者等の幹部の指揮の下、情報セキュリティインシデントへの対処を一元的に管理し、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備することが必要である。

一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRT は、時々刻々と明らかになる情報を基に、状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で最高情報セキュリティ責任者等の幹部に状況を報告する。

- **遵守事項 2.1.1(7)(b)「CSIRT に属する職員等」について**

CSIRT に属する職員等は、機関等における情報セキュリティインシデントを認知した際、最高情報セキュリティ責任者の指揮の下、これに対処する職員等であることから、最高情報セキュリティ責任者に対して適切に状況を報告し、最高情報セキュリティ責任者の指示を受け適切に対処できることが必要である。

CSIRT に属する職員等には、情報セキュリティ、情報システム等に関する知識及び技能を持つ者並びに機関等のネットワーク構成や個別システムの情報システムセキュリティ責任者及び管理者を把握している者を含めることが求められる。CSIRT が設置された部門において、求められる知識や技能等を有する者が不足している場合には、CSIRT が設置された部門以外の職員等を CSIRT に属する職員等として充てることも考えられる。

また、CSIRT に属する職員等には、上述した技術的な対処の外、発生した情報セキュリティインシデントの影響の大きさによっては、対外的な対応も必要となることから、広報を担当する職員等を CSIRT に含めておくことも考えられる。

なお、他の部門の職員等を CSIRT に属する職員等として充てる場合には、職務命令として CSIRT に係る職務を兼任させるなど、当該職員等が支障なく活動できるよう留意する必要がある。

- **遵守事項 2.1.1(7)(b)「CSIRT 責任者」について**

CSIRT 責任者とは、情報セキュリティインシデントの対処に係る責任者であり、情報セキュリティインシデントに関する全般的な対応が求められる。ただし、重大な情報セキュリティインシデントが生じ、最高情報セキュリティ責任者自らが、情報セキュリ

ティインシデントへ対処する必要があるときには、その指揮監督の下で必要な対応を行うこととなる。

- **遵守事項 2.1.1(7)(b)「CSIRT 内の業務統括及び外部との連携等を行う職員等」について**

CSIRT 内の業務統括及び外部との連携等を行う職員等は、CSIRT 責任者の指揮の下、CSIRT の業務や連絡を一元的に管理し統括する機能を担う。ここでいう職員等は、一人の職員等に制限するものではなく、いわゆる総括班のような位置付けで複数名置くことが望ましい。

- **遵守事項 2.1.1(7)(c)「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」について**

CSIRT 責任者が情報システムを所管している場合、当該情報システムの情報セキュリティインシデントを認知した際、２つの役職が利害相反関係にあることから、最高情報セキュリティ責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。

これを避けるため、例えば、CSIRT 責任者には情報セキュリティ責任者以外の者を充てる、最高情報セキュリティ責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途 CSIRT 責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保することが必要である。

- **遵守事項 2.1.1(7)(d)「CYMAT に属する職員」について**

CYMAT は、国の行政機関の情報セキュリティに関する知識及び技能を有する職員で構成する体制であり、サイバー攻撃等により支援対象機関で情報セキュリティインシデントを認知した場合であって、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インシデントを取り扱う。CYMAT の主な機能は以下のとおりである。

- 発生事象の正確な把握
- 被害拡大防止、復旧、再発防止のための技術的な支援及び助言
- 対処能力の向上に向けた平時の取組（研修、訓練等の実施）

CYMAT に属する職員には、CYMAT 要員及び CYMAT 研修員がある。CYMAT 要員になるために、セキュリティに関する特定の資格は求めていないものの、情報セキュリティ、情報システム等に関する基礎的な知識を有する者を充てることが望ましい。また、CYMAT 研修員については、将来 CYMAT 要員になる候補者として活動することが期待される職員で、情報セキュリティ、情報システム等といった分野に関心を持ち、内閣官房内閣サイバーセキュリティセンター等が提供する研修に参加し、研さんに励むことができる職員が望ましい。

CYMAT 要員に対しては、内閣官房の併任辞令を発令することで、内閣官房の予算を措置することにより内容の充実した訓練・演習の機会を提供している。また、CYMAT 研修員に対しても研修の機会を提供していることから、国の行政機関においては、組織内でのインシデントレスポンスに当たる職員の育成という観点からも、CYMAT 要員又は CYMAT 研修員として内閣官房内閣サイバーセキュリティセンターに登録することが望ましい。

- **基本対策事項 2.1.1(7)-1 a)「機関等全体における情報セキュリティインシデント対処の管理」について**

  情報セキュリティインシデントへの対処に当たっては、「検知／連絡受付」、「トリアージ（情報セキュリティインシデントであるか否かの評価、優先度付け等）」、「インシデントレスポンス（応急措置の実施、原因調査、復旧、再発防止等）」、「報告／情報公開（報道発表等の対外対応）」といったプロセスが必要となる。

  「機関等全体」とは、国の行政機関における CSIRT においては、外局、地方支分部局等を含み、独立行政法人及び指定法人における CSIRT においては、法人の組織構成によるが、例えば、支部、地方組織等を含む組織の全てを意味する。CSIRT には、上記のプロセス全体について、機関等内外の関係組織と連携・調整を図り、状況を把握し、適宜幹部等への報告を行うとともに、迅速かつ的確な対処が行われるように当事者部局への指示・勧告・助言を行うことが求められる。

- **基本対策事項 2.1.1(7)-1 b)「専門的知見の提供、対処作業の実施」について**

  機関等において、サイバーセキュリティや情報セキュリティインシデントへの対処に係る専門組織や専門知識を持った職員等を有する場合は、それらの組織・職員等の CSIRT への組み込み、又は情報セキュリティインシデント発生時に連携できる体制の構築を行うことが望ましい。

- **基本対策事項 2.1.1(7)-2「実務担当者を含めた実効性のある CSIRT 体制」について**

  CSIRT 体制には、情報セキュリティインシデント対処における最高情報セキュリティ責任者への早急な状況報告、被害拡大防止及び復旧のための対策の実施を果たし得るよう、実務担当の職員等（例えば、国の行政機関においては、課長補佐以下の者）を複数含むことが必要である。

  また、CSIRT は、最高情報セキュリティアドバイザー等から情報セキュリティインシデントへの対処の支援が円滑に受けられるような体制とすることが望ましい。

- **基本対策事項 2.1.1(7)-3「外部の専門家等による必要な支援を速やかに得られる体制」について**

  外部の専門家等による必要な支援を迅速に得られる体制の構築の例としては、情報セキュリティインシデント発生時にそうした事案への対処に精通した専門家を速やかに派遣してもらうための契約を事業者と結ぶこと等が挙げられる。

- **基本対策事項 2.1.1(7)-4「役割分担を規定」について**

  情報セキュリティインシデント発生時に、関係者が速やかに必要な対処を行えるように、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局（広報担当部局、調達担当部局、サイバーセキュリティ専門部局等）の役割分担をあらかじめ定めておくことが望ましい。ただし、役割分担は、情報セキュリティインシデントの種類や規模、影響度合い等によって変更されることも考えられるため、発生の頻度が比較的高いと考えられる情報セキュリティインシデントを想定した役割分担をあらかじめ定めておき、必要に応じて役割分担を再設定することも考えられる。

遵守事項

(8) 兼務を禁止する役割

(a) 職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

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

(イ) 監査を受ける者とその監査を実施する者

(b) 職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.1(8)(b)「承認権限者等の上司又は適切な者」について**

承認等の申請において、申請する者と承認する者が同一の場合又は申請する者が承認する者の上司である場合は、手続規定において定められた承認権限者等をもって承認等の可否の判断を行うことは適切とは言えない。

このような場合に対応するために、承認権限者等の上司等をもって承認するなどの手続をあらかじめ定めておく必要がある。

情報セキュリティ責任者等よりも高位の職員等が承認等を申請する場合においては、例えば、最高情報セキュリティ責任者が当該承認等の判断を行うことが想定される。他方、技術的な事項は、承認権限者等の上司よりも内容を理解している者が可否の判断を行う方が適切な場合もあり、この場合には、本来の承認権限者等が判断してよい。

また、最高情報セキュリティ責任者と同等以上の職位の者が、承認等を申請する場合も想定される。このような場合においても、最高情報セキュリティ責任者が、適切に判断することが考えられる。

【参考 2.1.1-1】 機関等の情報セキュリティ体制のイメージ例

機関等の情報セキュリティ体制のイメージを図 2.1.1-1 に示す。

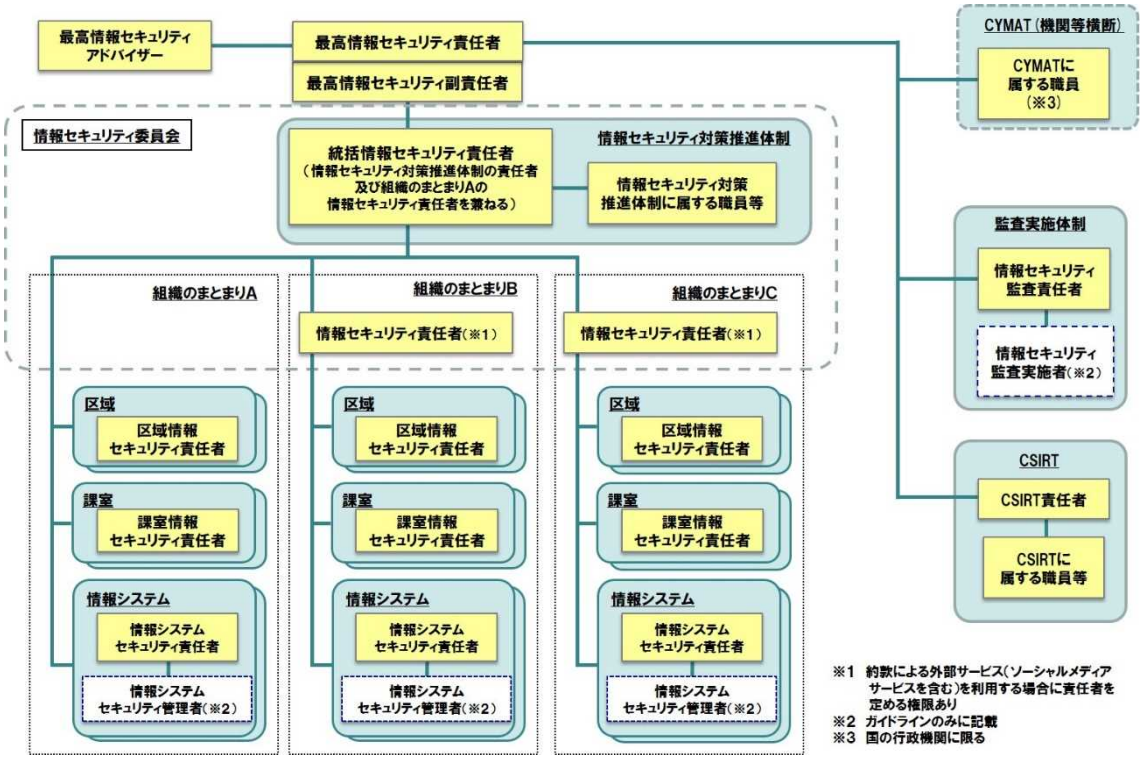


図 2.1.1-1　機関等の情報セキュリティ体制のイメージ

2.1.2 対策基準・対策推進計画の策定

目的・趣旨

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

遵守事項

(1) 対策基準の策定

(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠した対策基準を定めること。また、対策基準は、機関等の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.2(1)(a)「情報セキュリティ委員会における審議を経て、統一基準に準拠した対策基準を定める」について**

  対策基準の策定に当たっては、あらかじめ、情報セキュリティ委員会において審議を行うとともに、情報セキュリティの知見を持つ者に意見を求めるなどして、規定内容の網羅性や妥当性等について確認した上で決定することが望ましい。

  また、対策基準は、「統一基準 1.1(5)対策項目の記載事項」及び「運用指針２(2)」に記載されている内容に基づき、リスク評価の結果を踏まえ、定期的に見直しの必要性を確認するなど常に最新の状況に適合させることが重要である。

- **遵守事項 2.1.2(1)(a)「リスク評価の結果を踏まえた上で定める」について**

  対策基準の策定に当たっては、情報セキュリティを取り巻く様々な脅威や、機関等の業務、取り扱う情報及び保有する情報システムの特性等を踏まえた上で、リスク評価を行うことが重要である。リスク評価は、リスク分析の成果に基づき、如何なるリスクへの対応が必要か、講ずべき対策の優先順位はどうするかなどについて意思決定を支援することを目的に実施するものである（図 2.1.2-1 参照）。機関等の業務、取り扱う情報及び保有する情報システムの特性に応じてリスクは異なることから、機関等における情報セキュリティを確保するためには、リスク評価を実施し、対策基準に定めるべき対策事項等を決定することが重要である。

  リスク評価手法については、機関等の情報セキュリティに係るマネジメント能力の成熟度や機関等の置かれた環境に応じたふさわしい手法を選ぶとよい。リスク評価に係る規格には、ISO31000:2009, Risk management－Principles and guidelines（国内標準としては、JIS Q 31000:2010 リスクマネジメント－原則及び指針（以下「JIS Q

31000:2010」という。)）等がある。これらを活用するなどし、適切な評価を実施するとよい。また、重点的に守るべき業務及び情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 28 年 10 月 7 日情報セキュリティ対策推進会議）に従って、対策を講ずることが必要である。

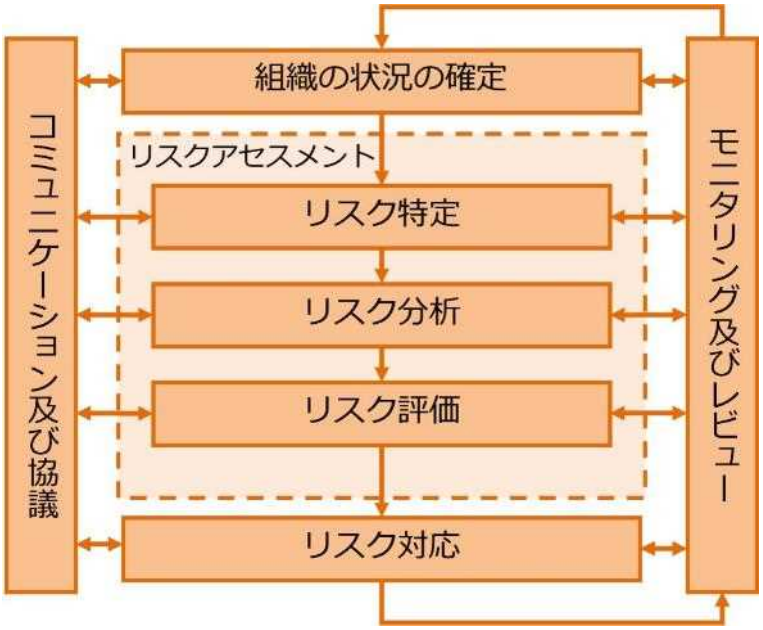


図 2.1.2-1　リスクマネジメントプロセスのイメージ図（JIS Q 31000:2010 による）

以下では、国際標準に基づいたリスク評価の手法を解説する。

リスク評価は、リスクの大きさが受容可能か否かを決定するために、リスク分析の結果をリスク基準と比較するプロセスのことを言う。これは、リスク対応に関する意思決定を手助けするものである。

まず、リスク水準を把握する手法の例として、以下に 4 種類の手法を示す。

① ベースラインアプローチ
既存の基準をもとにセキュリティ対策のベースラインをリスク基準として作成し、実際の運用がベースラインの求める基準を満たしているかという観点で評価していく方法。簡単な方法であるが、選択する基準によっては、求める対策のレベルが高すぎたり低すぎたりする場合がある。

② 非形式的アプローチ
コンサルタント、組織又は担当者が、自身の知見や経験に基づき評価を行う方法。短時間に実施することが可能であるが、属人的な判断に偏るおそれがある。

③ 詳細リスク分析
システムについて情報資産ごとに「資産価値」、「脅威」、「脆弱性」及び「セキュリティ要件」を識別し、これらをリスク基準に照らして評価する方法。厳密なリ

スク評価が行える一方、多くの工数や費用がかかる。

④ 組合わせアプローチ
複数のアプローチの併用。よく用いられるのは、「① ベースラインアプローチ」と「③ 詳細リスク分析」の組合わせ。ベースラインアプローチと詳細リスク分析の両方のデメリットを相互に補完し、作業の効率化や分析制度の向上を図ることができる。

※枠内、情報処理推進機構、
https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html を基に作成
また、「ISMS ユーザーズガイド(JIP-ISMS111-3.0)」から文書を引用(④組合わせアプローチの説明に係る「相互に～向上を図ること」の記述

組織の情報セキュリティに係るマネジメント能力の成熟度が比較的十分でない組織においては、簡易な方法である「ベースラインアプローチ」を適用することが考えられる。

簡易なリスク評価の進め方として、例えば、前述した「ベースラインアプローチ」に着目し、機関等のポリシーをリスク基準として用いることが考えられる。

その際は、自己点検や情報セキュリティ監査をリスク評価プロセスの一部として活用すれば、リスク評価をより効率的に実施できる。

リスク評価に当たっては、特に、以下の５点に留意し検討すると、リスク評価が必要になることや、それを行う目的が分かるようになる。リスク評価においては、その目的意識を明確に持つことが重要である。

① 守るべき資産は何か。
② その資産にはどのようなリスクがあるか。
③ セキュリティ対策により、リスクはどれだけ低減するか。
④ 実施しようとしたセキュリティ対策の失敗により、どのようなリスクがもたらされるか。
⑤ 対策にはどれ程のコストとどのような二律背反の要素が付随するか。

また、リスク評価に際しては、リスクマネジメントプロセス全体に留意し、リスク対応を行った後、モニタリング及びレビューを行い、更なる改善を図ることが望ましい。

次に、リスク分析の結果をリスク基準と比較するプロセスについて解説する。

リスク基準決定の際は、JIS Q 31000 の支援規格でもある JIS Q31010:2012 リスクマネジメントーリスクアセスメント技法（IEC/ISO31010:2009,Risk management-Risk assessment techniques）において、リスクの発生確率、リスクレベル等を決定する旨が記載されている。これを踏まえ、脅威事象が発生する可能性を"非常に高い／高い／中間／低い／非常に低い"、脅威事象が負の影響をもたらす可能性を"非常に高い／高い／中間／低い／非常に低い"などと各々分類し、両者のマトリクスで結果を整理し

リスク基準を決定する方法等がある（表 2.1.2-1 参照）。

決定したリスク基準とリスク分析の結果を比較し、その結果、発生した脅威事象が組織の業務、資産又は個人に被害をもたらす総合的な可能性（以下「発生した脅威事象の総合的な可能性」という。）が「非常に高い」となった場合は、そのリスクを回避する（JIS Q 31000:2010,5 章 5.5.1 a 参照）ことが考えられる。

発生した脅威事象の総合的な可能性が「高い」、「中間」又は「低い」となった場合は、リスク源を除去する（JIS Q 31000:2010,5 章 5.5.1 c 参照）などリスクの低減、「非常に低い」となった場合は、リスクの保有（JIS Q 31000:2010,5 章 5.5.1 g 参照）による対応が考えられる。

ただし、例えば、脅威事象が発生する可能性が「非常に低い」、脅威事象が負の影響をもたらす可能性が「非常に高い」場合で、発生した脅威事象の総合的な可能性が「低い」となっていた場合は、低減でなく、他者とそのリスクを共有する（JIS Q 31000:2010,5 章 5.5.1 f 参照）リスク移転による対応を行うことが考えられる。

リスクに対し、どのような対応を行うかは、一意に決まるものではない。目的、リスク対応が新たに生み出すリスクの有無、費用対効果等を踏まえ、対応を決める時点において最善の対応を選択することが望ましい。

JIS Q 31010:2012 リスクマネジメントーアセスメント技法には、脅威事象が発生する可能性、脅威事象が負の影響をもたらす可能性を組み合わせ活用するための数値等は例示されていないが、National Institute of Standards and Technology（米国国立標準技術研究所）Special Publication 800-30 revision1（以下「NIST SP800-30 rev1」という。）に参考となる表（表 2.1.2-1 参照）、解説があるので記載する。

表 2.1.2-1　リスク基準例（発生した脅威事象が組織の業務、資産又は個人に被害をもたらす総合的な可能性:NIST SP800-30 rev1(情報処理推進機構訳)による）

脅威事象が負の影響をもたらす可能性 ＼ 脅威事象が発生する可能性	非常に低い	低い	中間	高い	非常に高い
非常に高い	低い	中間	高い	非常に高い	非常に高い
高い	低い	中間	中間	高い	非常に高い
中間	低い	低い	中間	中間	高い
低い	非常に低い	低い	低い	中間	中間
非常に低い	非常に低い	非常に低い	低い	低い	低い

※　発生した脅威事象が組織の業務、資産又は個人に被害をもたらす総合的な可能

性は、脅威事象が発生する可能性と脅威事象が負の影響をもたらす可能性の組み合わせによる。

- 脅威事象が発生する可能性について（NIST SP800-30 rev1(情報処理推進機構訳)による）

  - 脅威事象が発生する可能性　定性的な値：非常に高い、半定量的な値：96-100
    エラー、アクシデント又は天災が発生するのはほぼ確実である、あるいは 1 年間に 100 回以上発生する。

  - 脅威事象が発生する可能性　定性的な値：高い、半定量的な値：80-95
    エラー、アクシデント又は天災が発生する可能性は高い、あるいは 1 年間に 10 回ないし 100 回発生する。

  - 脅威事象が発生する可能性　定性的な値：中間、半定量的な値：21-79
    エラー、アクシデント又は天災が発生する可能性はある程度ある、あるいは 1 年間に 1 回ないし 10 回発生する。

  - 脅威事象が発生する可能性　定性的な値：低い、半定量的な値：5-20
    エラー、アクシデント又は天災が発生する可能性は低い、あるいは 1 年間に 1 回未満発生するが、10 年おきに 2 回以上発生する。

  - 脅威事象が発生する可能性　定性的な値：非常に低い、半定量的な値：0－4
    エラー、アクシデント又は天災が発生する可能性はほとんどない、あるいは 10 年おきに 1 回未満発生する。

- 脅威事象が負の影響をもたらす可能性について（NIST SP800-30 rev1(情報処理推進機構訳)による）

  - 脅威事象が負の影響をもたらす可能性　定性的な値：非常に高い、半定量的な値：96-100
    脅威事象が開始された／発生した場合、負の影響がもたらされるのはほぼ確実である。

  - 脅威事象が負の影響をもたらす可能性　定性的な値：高い、半定量的な値：80-95
    脅威事象が開始された／発生した場合、負の影響がもたらされる可能性は高い。

  - 脅威事象が負の影響をもたらす可能性　定性的な値：中間、半定量的な値：21-79
    脅威事象が開始された／発生した場合、負の影響がもたらされる可能性はある程度ある。

- 脅威事象が負の影響をもたらす可能性　定性的な値：低い、半定量的な値：5-20
  脅威事象が開始された／発生した場合、負の影響がもたらされる可能性は低い。

- 脅威事象が負の影響をもたらす可能性　定性的な値：非常に低い、半定量的な値：0－4
  脅威事象が開始された／発生した場合、負の影響がもたらされる可能性はほとんどない。

● リスク評価に係る用語

参考：JIS Q 31000:2010 リスクマネジメント－原則及び指針（抄）

- リスク基準（JIS Q 31000:2010, 2 章 2.22 のとおり）
  リスクの重大性を評価するための目安とする条件。

- コミュニケーション及び協議（JIS Q 31000:2010, 5 章 5.2 のとおり）
  リスクの運用管理において、情報の提供、共有、取得及び意思決定に影響を与えるなどの人々又は組織との対話を行うために、組織が継続的に及び繰り返し行うプロセス。

- リスクアセスメント（JIS Q 31000:2010, 5 章 5.4 のとおり）
  リスク特定、リスク分析及びリスク評価を網羅するプロセス全体を指す。

- モニタリング及びレビュー（JIS Q 31000:2010, 5 章 5.6 のとおり）
  リスクアセスメントを改善するため、更なる情報の入手や傾向等の分析を行うこと。

遵守事項

(2) 対策推進計画の策定

(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「**対策推進計画**」という。）を定めること。また、対策推進計画には、機関等の業務、取り扱う情報及び保有する情報システムに関する**リスク評価の結果を踏まえた全体方針**並びに以下に掲げる**取組の方針・重点**及びその実施時期を含めること。

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) **情報システムに関する技術的な対策を推進するための取組**

(オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.2(2)(a)「対策推進計画」について**

対策推進計画は、情報セキュリティ対策に関する一連の取組を対象とした全体計画であり、情報セキュリティ対策に関する取組の全体方針のほか、本条各号に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を設定するものである。

対策推進計画は、機関等が組織として、種々の情報セキュリティ対策を如何なる考え方や方向性に基づいて進めていくのかといった一連の取組全体の大枠について、最高情報セキュリティ責任者があらかじめ総合的に定めるものであり、個々の取組の実施に当たって詳細計画が必要となる場合は、対策推進計画に則して、それぞれの取組の責任者がその権限の下に詳細計画を策定する。

- **遵守事項 2.1.2(2)(a)「リスク評価の結果を踏まえた全体方針」について**

情報セキュリティ対策は、情報セキュリティを取り巻く様々な脅威、機関等の業務、取り扱う情報及び保有する情報システムの特性等を踏まえ、目的達成の成否等に影響を与える情報セキュリティに係るリスクの分析・評価を行った上で、対策の方針や優先度を判断し、計画的に推進することが重要である。また、情報セキュリティ対策については、限られた予算や人的資源を最大限に活用して、対策全体としての方向付けを行った上で対策基準に策定した個々の対策を実施していくことも重要である。

全体方針としては、例えば、優先的に対応すべき脅威や優先的に対策を講ずるべき対象を設定し、それらへの対応を重点として掲げることが考えられる。

また、自組織の目的等を踏まえ、情報セキュリティ対策の自己点検、情報セキュリティ監査、本部監査の結果等を考慮した上で、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ずることが求められる。

リスク評価の具体的な進め方については、「(解説) 遵守事項 2.1.2(1)(a)「リスク評価の結果を踏まえた上で定める」について」を参照のこと。

- **遵守事項 2.1.2(2)(a)「取組の方針・重点」について**

本条各号に掲げる情報セキュリティ対策に関する個々の取組の方針・重点は、全体方針を踏まえ、例えば、情報セキュリティ対策の教育において、特定の脅威（例：標的型攻撃、サプライチェーン・リスク）、特定の対象（例：業務の内容や役職に応じた者）、特定の内容（例：対策基準の改正点）を掲げることが考えられる。

- **遵守事項 2.1.2(2)(a)(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」について**

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としては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに基づく取組等、政府全体としての取組のほか、機関等において独自に推進している技術的な対策を含めることが望ましい。技術的対策には、情報システムを構成する機器等の更新等の投資による対策も含まれる。

2.2 運用

2.2.1 情報セキュリティ関係規程の運用

目的・趣旨

機関等は、対策基準に定められた対策を実施するため、具体的な実施手順を定める必要がある。

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

遵守事項

(1) 情報セキュリティ対策の運用

(a) 統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する実施手順を整備（本統一基準で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告すること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の規定を整備すること。

(c) 情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行すること。

(d) 情報セキュリティ責任者又は課室情報セキュリティ責任者は、職員等から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告すること。

(e) 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.1(1)(a)「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。）」について**

  統一基準で整備を求めている実施手順は、以下のとおり。

  （1）統括情報セキュリティ責任者

  - 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の管理に関する規定（遵守事項 2.2.1(1)(b)）
  - 情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機関等

関係者への報告手順（遵守事項 2.2.4(1)(a)）
- 情報セキュリティインシデントの可能性を認知した際の機関等外との情報共有を含む対処手順（遵守事項 2.2.4(1)(b)）
- 情報の取扱いに関する規定（遵守事項 3.1.1(1)(a)）
- 要管理対策区域の対策の基準（遵守事項 3.2.1(1)(b)）
- 外部委託に係る規定（遵守事項 4.1.1(1)(a)）
- 約款による外部サービスの利用に関する規定（遵守事項 4.1.2(1)(a)）
- ソーシャルメディアサービスによる情報発信時における情報セキュリティ対策に関する運用手順等（遵守事項 4.1.3(1)(a)）
- 機器等の調達に係る選定基準（遵守事項 5.1.2(1)(a)）
- 機器等の納入時の確認・検査手続（遵守事項 5.1.2(1)(b)）
- アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための規定（遵守事項 6.3.1(1)(a)）
- 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末についての安全管理措置に関する規定（遵守事項 7.1.1(4)(a)）
- 機関等の情報システムの利用のうち、情報セキュリティに関する規定（遵守事項 8.1.1(1)(a)）
- 機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合の利用手順及び許可手続（遵守事項 8.1.1(1)(b)）
- 要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する際の安全管理措置に関する規定及び許可手続（遵守事項 8.1.1(1)(c)）
- 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（遵守事項 8.1.1(1)(d)）
- 機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続（遵守事項 8.1.1(1)(e)）
- 機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続（遵守事項 8.2.1(2)(a)）

（２）その他の者が定めるもの
- 最高情報セキュリティ責任者
  - 例外措置の適用の申請を審査する者及び審査手続（遵守事項 2.2.2(1)(a)）
- 情報セキュリティ責任者
  - 職員等ごとの自己点検票及び自己点検の実施手順（遵守事項 2.3.1(1)(b)）
- 情報システムセキュリティ責任者
  - 情報セキュリティ対策を実施するために必要な文書（遵守事項 5.1.1(2)(a)）
  - 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（遵守事項 6.1.5(1)(b)）
  - 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（遵守事項 7.3.1(1)(i)）

- **遵守事項 2.2.1(1)(a)「実施手順に関する事務を統括」について**

  統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する実施手順について、監査結果を通じて、対策基準に従って整備されていないことを把握した場合には、整備すべき者に対して指導することが想定される。

  また、統括情報セキュリティ責任者は、情報セキュリティ関係規程について自己点検や監査の結果、例外措置の申請状況等を通じ、課題又は問題点について把握し得ることから、実施手順の整備主体が、特定の部門の情報セキュリティ責任者に係るものであったとしても、同種の課題又は問題点の有無を他の部局等に確認することも想定される。

- **遵守事項 2.2.1(1)(c)「最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行」について**

  情報セキュリティ対策推進体制の役割については、遵守事項 2.1.1(6)(a)及び基本対策事項 2.1.1(6)-1 において規定しているが、本項では、情報セキュリティ対策推進体制が規定された役割に従って事務を遂行すべきことを示している。

  当該事務の内容としては、例えば、情報セキュリティ関係規程の運用状況の適時の把握、情報セキュリティ関係規程に関する教育や訓練の実施、自己点検による情報セキュリティ関係規程の遵守状況の調査及び問題点の改善が考えられる。また、情報システムの脆弱性に係る情報や外部のインシデント情報等の情報セキュリティ対策に有用となる情報を入手するとともに、それらを関係機関と共有することも、対策の運用において重要な対応である。

遵守事項

(2) 違反への対処

(a) 職員等は、情報セキュリティ関係規程への重大な違反を知った場合は、**情報セキュリティ責任者にその旨を報告**すること。

(b) 情報セキュリティ責任者は、**情報セキュリティ関係規程への重大な違反**の報告を受けた場合及び自らが重大な違反を知った場合には、**違反者及び必要な者**に**情報セキュリティの維持に必要な措置**を講じさせるとともに、統括情報セキュリティ責任者を通じて、**最高情報セキュリティ責任者に報告**すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.1(2)(a)「情報セキュリティ責任者にその旨を報告」について**

機関等において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉するための事項である。一般的に、機関等においては、違反を知った者はこれを報告する義務が課されており、情報セキュリティ関係規程への違反については、各規定の実施に責任を持つ情報セキュリティ責任者に報告することとなる。本項は、職員等から情報セキュリティ責任者への直接の報告を必須とするものではなく、重大な違反等の有無を情報セキュリティ責任者が確実に認識できるようにすることを求めている。

なお、職員等は、自ら違反した場合に限らず、他の職員等が違反している場合においても、迅速な是正措置を促す理由から、当該職員等への助言に加えて情報セキュリティ責任者に報告するなど適切に対応することが求められる。また、情報セキュリティ関係規程に係る課題及び問題点を認識した場合についても、情報セキュリティ責任者に報告することが望ましい。

- **遵守事項 2.2.1(2)(b)「情報セキュリティ関係規程への重大な違反」について**

情報セキュリティ関係規程への重大な違反とは、当該違反により機関等の業務に重大な支障をきたすもの又はその可能性のあるものをいう。例えば、機密性の極めて高い情報を保存した端末を、許可無く要管理対策区域外に持ち出してしまった場合等が考えられる。

情報セキュリティ責任者は、機関等において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉し、被害の未然防止又は拡大防止のための措置を適切に講じさせるとともに、再発防止に関する取組を進めることが求められる。

- **遵守事項 2.2.1(2)(b)「違反者及び必要な者」について**

情報セキュリティ関係規程への重大な違反があった場合には、違反者自身が対策を講ずることは当然であるが、それ以外の「必要な者」として措置を義務付けられるのは、情報システムセキュリティ責任者、課室情報セキュリティ責任者及び区域情報セキュリティ責任者等の当該規程の実施に責任を有する者が挙げられる。情報システムの運用者や担当者、委託先等とも協力し、情報セキュリティを維持するために必要な措置を

講ずる必要がある。

- **遵守事項 2.2.1(2)(b)「情報セキュリティの維持に必要な措置」について**

  重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、早期解決、拡大防止等の対処を行う。拡大防止としては、情報セキュリティ関係規程について再周知の徹底が考えられる。

- **遵守事項 2.2.1(2)(b)「最高情報セキュリティ責任者に報告」について**

  報告を受けた最高情報セキュリティ責任者は、その内容、結果、業務への影響、社会的評価等を確認し、機関等全体として再発防止を徹底するなど、適切に対応する必要がある。

  また、統括情報セキュリティ責任者は、同様の違反が多発している可能性の有無を考慮し、違反の原因について分析し、必要に応じて情報セキュリティ関係規程の見直しを含めた対策を検討する必要がある。

2.2.2 例外措置

目的・趣旨

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

遵守事項

(1) 例外措置手続の整備

(a) 最高情報セキュリティ責任者は、**例外措置の適用の申請を審査する者**（以下本款において「許可権限者」という。）及び審査手続を定めること。

(b) 統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

【 基本対策事項 】

＜2.2.2(1)(a)関連＞

2.2.2(1)-1 最高情報セキュリティ責任者は、例外措置について以下を含む手順を定めること。

a) 例外措置の許可権限者

b) 事前申請の原則その他の申請方法

c) 審査項目その他の審査方法

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置により生じる情報セキュリティ上の影響と対処方法
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

＜2.2.2(1)(b)関連＞

2.2.2(1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、統括情報セキュリティ責任者へ定期的に報告すること。

a) 審査した者の情報（氏名、役割名、所属、連絡先）

b) 申請内容

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程

名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

c）審査結果の内容
- 許可又は不許可の別
- 許可又は不許可の理由
- 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を許可した期間
- 許可した措置内容（講ずるべき代替手段等）
- 例外措置を終了した旨の報告方法

（解説）

- **遵守事項 2.2.2(1)(a)「例外措置の適用の申請を審査する者」について**

例外措置の適用の申請を受けた際に適切な審査が実施できるように、許可権限者を定め、審査手続を整備しておく必要がある。情報セキュリティ関係規程の誤った解釈や恣意的な例外運用を防止するために、例えば、情報セキュリティ関係規程を策定した者を許可権限者に充てることが考えられる。申請の内容に応じて、適切な許可を与えられる者を許可権限者として定めておくことが重要である。

遵守事項

(2) 例外措置の運用

(a) 職員等は、定められた審査手続に従い、許可権限者に規定の**例外措置の適用を申請**すること。ただし、業務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。

(b) 許可権限者は、職員等による**例外措置の適用の申請**を、定められた審査手続に従って**審査**し、許可の可否を決定すること。

(c) 許可権限者は、例外措置の申請状況を台帳に記録し、**統括情報セキュリティ責任者に報告**すること。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.2(2)(a)「例外措置の適用を申請」について**

職員等は、定められた審査手続に従い例外措置の適用を申請し、許可を得てから例外措置を講ずることが原則であるが、業務の遂行に緊急を要するなどの場合であって、情報セキュリティ関係規程の規定内容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た対策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が必要である。

職員等は、例外措置の適用を希望する場合には、当該例外措置を適用したときの情報セキュリティ上の影響を検討、分析する必要がある。その上で、例外措置の適用が必要であると判断した場合は、その影響を低減させるための補完措置を提案し、適用の申請を行う必要がある。

- **遵守事項 2.2.2(2)(b)「例外措置の適用の申請」・「審査」について**

許可権限者は、例外措置の適用の申請を適切に審査しなければならない。審査に当たっては、申請内容の情報セキュリティ関係規程の該当箇所、期間、措置内容等が、申請する理由と照らして必要最小限の内容となっているか確認した上で、例外措置の適用を許可した場合の情報セキュリティ上の影響と、不許可とした場合の業務遂行等への影響を評価し、その判断を行う必要がある。

例外措置の適用期間が長期にわたる場合等においては、例外措置の実施によるリスクが変化する可能性を踏まえ、定期的に当該措置の適用状況等を許可権限者において把握することも重要である。

- **遵守事項 2.2.2(2)(c)「統括情報セキュリティ責任者に報告」について**

  統括情報セキュリティ責任者は、許可権限者から例外措置の適用状況の報告を受ける。これは、次項で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うためである。

- **遵守事項 2.2.2(2)(d)「情報セキュリティ関係規程の追加又は見直しの検討」について**

  例外措置の適用が多い状況は、例外とはみなせないと考えるべきである。その場合には、代替手段の導入を含め、情報セキュリティ関係規程の見直しを検討する必要がある。

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が職員等に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての職員等が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

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

遵守事項

(1) 教育体制の整備・教育実施計画の策定

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

(b) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すこと。

【 基本対策事項 】

＜2.2.3(1)(a)関連＞

2.2.3(1)-1 統括情報セキュリティ責任者は、職員等の役割に応じて**教育すべき内容を検討**し、教育のための資料を整備すること。

2.2.3(1)-2 統括情報セキュリティ責任者は、**職員等が毎年度最低１回は教育を受講**できるように、教育実施計画を立案するとともに、その実施体制を整備すること。

2.2.3(1)-3 統括情報セキュリティ責任者は、職員等の着任又は異動後に、**３か月以内に受講**できるように、その実施体制を整備すること。

（解説）

- **基本対策事項 2.2.3(1)-1「教育すべき内容を検討」について**

教育の内容については、最新の脅威動向、機関等の実状や情報セキュリティインシデントの発生状況等、情報セキュリティ環境の変化等を踏まえ、幅広い角度から検討し、受講者の役割、責任及び技能に適したものにする必要がある。

さらに、教育の内容は、職員等が対策内容を十分に理解できるものとする必要があり、そのためには、網羅的な資料ではなく、理解しておくべき事項に制限した資料を教育に用いるべきである。例えば、情報セキュリティ関係規程の教育資料の作成においては、遵守事項を遵守すべき者ごとに整理し、職員等が遵守する必要のない事項は、含まないように配慮すべきである。

また、違反の抑止効果を期待することを目的に、ウェブサイトの閲覧に係るログを取得していることや、必要に応じて当該ログを調査することがあること等の情報システ

ムの運用ルールを職員等の教育内容に含めることも考えられる。

このような教育内容の検討に加えて、教育実施後に簡単なテストを実施することにより受講者の理解度を把握したり、受講者にアンケートを記入してもらったりすることで、次回開催のテーマや現在の教育方法等についての改善を検討することも考えられる。

なお、情報セキュリティ対策推進体制を含む情報セキュリティ関係部署の者やCYMAT 及び CSIRT に属する職員等に対して、情報セキュリティに関する知識及び技能を向上させるため、研修及び実務を模擬した訓練を実施することも有効である。訓練内容や実施結果の評価等について、最高情報セキュリティアドバイザーの助言を受けることも有用である。より高度な技能の習得や将来的な脅威への対応等を求めた訓練を実施する場所等においては、外部の専門事業者に委託することにより訓練を実施してもよい。

- **基本対策事項 2.2.3(1)-2「職員等が毎年度最低１回は教育を受講」について**

機関等において情報セキュリティを維持するためには、職員等が常日頃から情報セキュリティの意識を持って業務を遂行する必要があり、そのためには職員等に対して継続的に教育を受講させることが重要である。本項では、全ての職員等に対して最低限の教育を受講させることを想定して「毎年度最低１回」と規定しているが、教育の対象が広範である、繰り返しの教育が必要であるなどの理由を考慮して、複数回の教育を計画することも考えられる。継続的な教育を実施するに当たっては、国の行政機関や民間企業が提供する研修プログラムや e-learning 等の活用も検討し、実施の効率性や受講のしやすさ等に配慮した上で、計画を策定するとよい。

情報セキュリティ対策推進体制を含む情報セキュリティ関係部局、CYMAT 及び CSIRT に属する職員等のセキュリティ人材に対する教育については、キャリアパスにも配慮し、十分な教育が受けられるよう、計画段階から実施内容や実施時期、手段を考慮する必要がある。

- **基本対策事項 2.2.3(1)-3「３か月以内に受講」について**

着任、異動した職員等に対しては、早期に情報セキュリティ対策の教育を受講させることも有益であり、着任後３か月以内には受講させるべきである。ただし、異動した後に使用する情報システムが、異動前と変わらないなど、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。

遵守事項

(2) 教育の実施

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

(b) 職員等は、教育実施計画に従って、**適切な時期に教育を受講**すること。

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

(d) 課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告すること。

(e) 統括情報セキュリティ責任者は、**教育の実施状況を分析、評価**し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.3(2)(a)「適切に受講」について**

  課室情報セキュリティ責任者は、職員等に情報セキュリティ対策の教育を受講させる責務があり、職員等に対して教育の実施を周知するとともに、教育を受講しない者に対して受講を勧告するほか、受講状況を把握するなどして、積極的に受講を促すこと等が求められる。また、受講時間を確保するなどの職員等が受講できるための環境を整備するなどの配慮も必要である。

- **遵守事項 2.2.3(2)(b)「適切な時期に教育を受講」について**

  職員等は、教育実施計画に従って、毎年度最低１回は教育を受講することが求められる。

  着任時又は異動時の場合には、新しい職場等で、情報セキュリティ対策の教育の受講方法について課室情報セキュリティ責任者に確認することも求められる。

- **遵守事項 2.2.3(2)(c)「情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講」・「CYMAT に属する職員にも教育を適切に受講」について**

  サイバー攻撃等の情報セキュリティに対する脅威が増大している状況を踏まえ、政府機関が一体となって対処することを目的に CYMAT が整備されているほか、情報セキュリティインシデントに迅速かつ適切に対処するための組織として機関等に CSIRT が整備されている。これらに属する職員等への教育も、その責務に照らすと極めて重要である。

- **遵守事項 2.2.3(2)(e)「教育の実施状況を分析、評価」について**

  より効果的な情報セキュリティに係る教育を実施するためには、終了した教育の実施状況を組織全体として分析、評価し、教育の実施内容や方法、対象者等を継続的に見直していくことが重要である。

  分析、評価の方法としては、例えば、受講者に演習問題を実施させることで理解度を定量的に把握する方法や、受講者のアンケート回答により改善点等の指摘を受ける方法が考えられる。受講者へアンケートを行う際は、改善すべき点等の有用な情報が得られるよう、具体的な質問をアンケート項目に加えるなどの工夫を考えるとよい。また、自組織において特定の実施手順が守られていないと考えられる場合は、当該実施手順に係る内容を教育に含め、教育実施前後での実施手順の遵守度合いを確認するといった手法で評価を行うことも考えられる。

2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

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

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

(a) 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機関等関係者への**報告手順**を整備し、**報告が必要な具体例**を含め、職員等に周知すること。

(b) 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の機関等外との情報共有を含む**対処手順**を整備すること。

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

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

(e) 統括情報セキュリティ責任者は、情報セキュリティインシデントについて**機関等外の者から報告を受けるための窓口を整備**し、その窓口への連絡手段を機関等外の者に明示すること。

(f) 統括情報セキュリティ責任者は、**対処手順が適切に機能することを訓練等により確認**すること。

【 基本対策事項 】

＜2.2.4(1)(a)関連＞

2.2.4(1)-1 国の行政機関の統括情報セキュリティ責任者は、所管する独立行政法人及び指定法人における情報セキュリティインシデント発生が報告された際にも、自組織における情報セキュリティインシデントの場合と同様に、最高情報セキュリティ責任者や内閣官房内閣サイバーセキュリティセンターに速やかに報告されるよう手順を定めること。

＜2.2.4(1)(b)関連＞

2.2.4(1)-2 統括情報セキュリティ責任者は、情報セキュリティインシデント発生時の対処手順のうち、**意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等**をあらかじめ定めておくこと。

＜2.2.4(1)(e)関連＞

2.2.4(1)-3　国の行政機関の統括情報セキュリティ責任者は、所管する独立行政法人及び指定法人において発生した情報セキュリティインシデントについて、当該法人から報告・連絡を受ける窓口について定めるとともに、各法人にその窓口の連絡先を周知すること。

（解説）

- **遵守事項 2.2.4(1)(a)「報告手順」について**

  報告手順として明記すべき事項としては、情報セキュリティインシデントの可能性が認知されてから最高情報セキュリティ責任者に報告するまでの具体的な手順等が考えられる。

  また、情報セキュリティインシデントの可能性の報告窓口については、報告手順の中で明らかにしておくほか、情報セキュリティ対策の教育の中で周知する、報告窓口の連絡先を執務室内に掲示するなどして、緊急時に職員等が速やかに報告できるようにする必要がある。

  報告窓口を CSIRT とは異なる部門に設ける場合は、当該部門から CSIRT への報告が速やかに実施される体制にすることが求められる。

- **遵守事項 2.2.4(1)(a)「報告が必要な具体例」について**

  「（解説）遵守事項 2.2.4(2)(a)「情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告」について」を参照のこと。

- **遵守事項 2.2.4(1)(b)「対処手順」について**

  対処手順として情報セキュリティインシデントの認知時において緊急を要する対処等の必要性に備えて、通常とは異なる例外的な承認手続を定めておくことも併せて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなことがないよう検討すること。

- **遵守事項 2.2.4(1)(c)「緊急連絡網」について**

  統括情報セキュリティ責任者は、通常時の全ての情報セキュリティ関連の責任者及び管理者の連絡網の整備に加えて、情報セキュリティインシデントを認知した場合に速やかに対処するための「緊急連絡網」を整備する必要がある。

  緊急連絡網には、該当する職員等に支給したスマートフォンや携帯電話の番号等を記載するほか、自宅や機関等支給以外のスマートフォンや携帯電話の番号等を含むことも考えられる。また、緊急連絡網には当該システムに係る責任者及び管理者のほか、重大な情報セキュリティインシデントに備えて最高情報セキュリティ責任者も含める必要がある。

- **遵守事項 2.2.4(1)(d)「訓練の内容及び体制を整備」について**

  実際に情報セキュリティインシデントへの対処を模擬的に行うことにより、対処能力を向上させるために実施する訓練の内容及び体制の整備を求める事項である。

対処能力を向上させるための訓練としては、業務の遂行のために特に重要と認めた情報システムでは、不正プログラム感染による情報漏えいやサービス不能攻撃によるシステム停止などへの対処を的確に実施できることが重要であると考えられることから、それらの情報セキュリティインシデントを想定した模擬的な対処を行う内容とすることが望ましい。

また、実効的な訓練を実施するためには、情報システム部門だけでなく、情報セキュリティインシデントに関する報告窓口となる部門、情報セキュリティ対策推進体制やCSIRTも参加することが望ましい。

- **遵守事項 2.2.4(1)(e)「機関等外の者から報告を受けるための窓口を整備」について**

例として、外部の者が機関等の情報セキュリティ対策の不備を発見した場合、機関等への攻撃のおそれ等を認知した場合、機関等外の者に情報セキュリティ上の脅威を与えていることを認知した場合（与えるおそれがある場合を含む。）等に、機関等外の者から連絡を受ける体制を整備することを求めている。

- **遵守事項 2.2.4(1)(f)「対処手順が適切に機能することを訓練等により確認」について**

情報セキュリティインシデントは定常的に発生するものではないが、実際に発生した場合には、機関等の業務に大きな影響をもたらすおそれがあるため、迅速かつ的確に対処を行うことが求められる。そのため、定めた対処手順が適切に機能することを訓練等によって確認しておくことが重要である。

訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を受けて判断等を行う「ロールプレイング」、状況設定の上で手順の検証を行う「シミュレーション」といった大掛かりなもののほか、より簡易な「ウォークスルー」や「机上チェック」といった手法も存在する。CSIRTの取組状況や職員等の習熟度等に応じて、必要な訓練等を検討し実施することが望まれる。

- **基本対策事項 2.2.4(1)-2 「意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等」について**

例えば、機関等LAN内での不正プログラム感染拡大やそれに伴う情報流出等が疑われる場合には、被害の拡大を阻止する措置を直ちに講ずることが重要である。そのような場合において、情報の重要度、情報が失われた場合のリスク、業務継続方法等を勘案した上で、調整等に時間をかけず直ちにネットワークを遮断するなどの措置を講ずるため、その手続や対象範囲等を事前に定めておくことが考えられる。これらの基準や手続は、機関等を取り巻くサイバー攻撃事例や情報セキュリティインシデント事例を基に、適時見直すことが求められる。

遵守事項

(2) 情報セキュリティインシデントへの対処

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

(b) CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

(c) CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、**最高情報セキュリティ責任者に速やかに報告**すること。

(d) CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための**応急措置の実施及び復旧に係る指示又は勧告**を行うこと。

(e) 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、機関等で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処すること。

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

(g) 国の行政機関における CSIRT は、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、**内閣官房内閣サイバーセキュリティセンターに連絡**すること。また、独立行政法人及び指定法人における CSIRT は、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関における CSIRT は、当該事象について速やかに、**内閣官房内閣サイバーセキュリティセンターに連絡**すること。

(h) CSIRT は、認知した情報セキュリティインシデントが**サイバー攻撃又はそのおそれのあるもの**である場合には、当該**情報セキュリティインシデントの内容に応じ、警察への通報・連絡等**を行うこと。

(i) 国の行政機関における CSIRT は、認知した情報セキュリティインシデント又は独立行政法人及び指定法人から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、**「大規模サイバー攻撃事態等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁）」に基づく報告連絡**を行うこと。

(j) CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて**対処全般に関する指示、勧告又は助言**を行うこと。

(k) CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。

(l) CSIRT は、情報セキュリティインシデントに関して、機関等を含む関係機関と

情報共有を行うこと。

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

【 基本対策事項 】

＜2.2.4(2)(b)関連＞

2.2.4(2)-1　CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、関係する者に情報共有を行うこと。

＜2.2.4(2)(d)関連＞

2.2.4(2)-2　CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局の役割分担を見直すこと。

（解説）

- **遵守事項 2.2.4(2)(a)「情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告」について**

職員等に、情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れ等につながるため、その可能性を認知した段階で報告を求める必要がある。報告窓口に報告する内容には、情報セキュリティインシデントの防止策を無効化したり、すり抜けられたりすることにより、被害に至らないまでも蓋然性が高まった状態も含まれる。例えば、不審な電子メールの添付ファイルを開いたり、URL リンクをクリックしたりしてしまった場合や、機密性の高い情報を保存したモバイル端末の所在が不明であるが、紛失したことや盗難されたことが確定的でない場合、平時の情報システムの利用において確認されないはずのエラーメッセージが端末に表示された場合等が想定される。

- **遵守事項 2.2.4(2)(c)「最高情報セキュリティ責任者に速やかに報告」について**

情報セキュリティインシデントの性質上、全ての状況が判然とするまでに時間がかかるものであるため、一度の報告で完了することはまれである。例えば、未確定情報を含んだ状態で第一報として報告し、その後に第二報、第三報と続けるような、適切な頻度で報告内容を更新する報告運用が望ましい。その場合、何が確定し、何が未確定であるのかを明らかにすることが望ましい。全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

- **遵守事項 2.2.4(2)(d)「応急措置の実施及び復旧に係る指示又は勧告」について**

応急措置や復旧に当たっては、情報セキュリティインシデントが発生した情報システムの停止、ネットワークの遮断等について、被害の拡大可能性、証拠保全、業務継続等を勘案し、CSIRT 責任者の判断で指示又は勧告をする。この場合には、情報セキュリティ対策推進体制が CSIRT 責任者の指示又は勧告を支援することが望ましい。

なお、応急措置や復旧に関して、事前に決められた手順がある場合はその手順に従うことが求められる（「(解説) 基本対策事項 2.2.4(1)-2 『意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等』について」を参照のこと。）。

- **遵守事項 2.2.4(2)(g)「内閣官房内閣サイバーセキュリティセンターに連絡」について**

内閣官房内閣サイバーセキュリティセンターへの連絡内容としては、以下が考えられる。

- 情報セキュリティインシデントが発生した部署
- 報道発表及び報道の有無
- 他部署への被害波及の可能性
- 業務への影響
- 発生日時とその内容
- 復旧状況及び復旧見込み

連絡方法については、「(解説) 遵守事項 2.2.4(2)(c) 『最高情報セキュリティ責任者に速やかに報告』について」と同様に、適切な頻度で連絡内容を更新することが望ましく、全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

- **遵守事項 2.2.4(2)(h)「サイバー攻撃又はそのおそれのあるもの」について**

サイバー攻撃の例としては、不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス攻撃、サービス不能攻撃等が挙げられる。また、「そのおそれのあるもの」とは、明らかなサイバー攻撃の痕跡が発見されていなくても、単なる機器の故障や操作上の誤りではなく、サイバー攻撃により発生した情報セキュリティインシデントであることが疑われる場合のことである。

- **遵守事項 2.2.4(2)(h)「情報セキュリティインシデントの内容に応じ」について**

サイバー攻撃又はそのおそれがある情報セキュリティインシデントを認知した場合で、当該情報セキュリティインシデントが犯罪に該当するときには、警察への通報・連絡等を求めるものである。明らかなサイバー攻撃に限らず、そのおそれがある場合についても、被害拡大の防止の観点から、可能な限り速やかな通報等を行うことが望ましい。

- **遵守事項 2.2.4(2)(h)「警察への通報・連絡等」について**

「通報・連絡等」の内容としては、相談、届出、告訴又は告発を想定している。

サイバー攻撃又はそのおそれがある情報セキュリティインシデントが発生した場合、当該サイバー攻撃等による被害の拡大を防止するとともに、攻撃者を追跡するため、警察が的確に初動措置を講ずる必要があることから、可能な限り速やかな通報・連絡等を求めている。

なお、その通報先は、各都道府県警察のサイバー攻撃対策部門であり、具体的には、警視庁では公安部の警視庁サイバー攻撃対策センター、道府県警察では警備部のサイバー攻撃対策担当課である。また、警察への通報に関する質問等については、警察庁警備局警備企画課において受け付けている。

- **遵守事項 2.2.4(2)(i)「「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」について

国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれがある緊急事態に際して政府一体となった初動対処体制をとる必要があることから、内閣官房副長官補（事態対処・危機管理担当）付等に関連情報等を迅速に報告連絡することとしている。

- **遵守事項 2.2.4⑵(j)「対処全般に関する指示、勧告又は助言」について**

機関等における情報セキュリティインシデント発生時の対処として、以下のプロセスが想定される。CSIRT には、これらの対処が迅速かつ的確に行われるように、対処状況を把握し、必要に応じて指示、勧告又は助言を行うことが求められる。

- 検知／連絡受付
  - 情報セキュリティインシデントの可能性の報告受付
- トリアージ
  - 報告された情報セキュリティインシデントの可能性に関する状況確認
  - 状況確認結果に基づく情報セキュリティインシデントであるか否かの評価
  - 対処する情報セキュリティインシデントの優先順位付け(事案が多発している場合等)
- インシデントレスポンス
  - 応急措置の実施
  - 証拠保全
  - 被害規模・範囲等の特定を含む状況分析
  - 関係部局、セキュリティベンダ等の外部組織、CYMAT 等への支援要請
  - 復旧対応の実施
  - 情報セキュリティインシデントの原因調査と原因が生じた理由の究明
  - 再発防止策の検討
- 報告／情報公開
  - 最高情報セキュリティ責任者への報告
  - 内閣官房内閣サイバーセキュリティセンター又は所管する国の行政機関への連絡
  - 警察等の関係組織への通報・連絡・報告等
  - 報道発表等の対外対応

- **遵守事項 2.2.4⑵(l)「情報共有を行う」について**

情報セキュリティインシデントに関して、被害拡大防止のため、関連する可能性のある関係機関と情報共有を行うことが重要である。例えば、自組織で発生した情報セキュリティインシデントについて調査した結果、他の関係機関においても同様の情報セキュリティインシデントの可能性がある場合には、それらの関係機関と情報を共有することが考えられる。

なお、国の行政機関については、情報共有に関し、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）において、「各府省庁は、その業務におい

て得たサイバー攻撃に係る情報を、可能な限り速やかに内閣官房情報セキュリティセンターに連絡する。また、内閣官房情報セキュリティセンターは、収集・集約された情報をサイバー攻撃に対する初動対処、被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う」と記載している。

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

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.4(3)(a)「再発防止策を検討」について**

一般に、再発防止策を定めるには、十分な原因調査を行い、どのような要素が絡んで情報セキュリティインシデントに至ったのか、因果関係を明らかにした上で、原因から情報セキュリティインシデントの発生段階の間で、因果関係の進行を断ち切るための防護策を複数検討し、講ずることが有効である。また、対策については、情報セキュリティインシデントが発生したシステム単独で講ずるよりも、他のシステムにも同様に展開することにより（水平展開）、類似事案の発生を組織全体にわたって食い止めることが可能となる。

なお、水平展開については、自らの組織の再発防止策に限らず、他組織の事案を参照することにより、事後対処よりも先んじた未然防止が可能となり、対応コストの低減も期待される。

さらに、再発防止策は、情報システムの利用手順で対策する方法及び情報システムへの情報セキュリティ機能の実装による対策を情報システムセキュリティ責任者へ求める方法の両面から検討し、必要な対策を定めて実施する必要がある。情報システムへの情報セキュリティ機能の実装には一定の時間を要することも考えられることから、利用手順による対策を暫定的に実施し、その後、機能追加により本格的な対策を行うなど段階的な実施も考慮する必要がある。

- **遵守事項 2.2.4(3)(b)「再発防止策を実施するために必要な措置」について**

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の再発防止策の報告を受けた場合は、その内容を確認する必要がある。

情報システムへの情報セキュリティ機能の実装等計画的に実施する必要がある再発防止策については、対策推進計画に反映させるなどして、適切に実施させるよう取組を

推進することが求められる。また、機関等全体として再発防止策を講ずることが有効と想定される場合は、機関等全体での取組を進めることも求められる。

- **遵守事項 2.2.4(3)(c)「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」について**

  CSIRT 責任者には、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対し、単に情報セキュリティインシデントの情報を共有するだけでなく、情報セキュリティインシデントの対処を踏まえ、統括情報セキュリティ責任者が定める対処手順等の改善や、個別の情報システムの情報セキュリティ水準の改善につなげられるような事項を含めて共有することが求められる。

2.3　点検

2.3.1　情報セキュリティ対策の自己点検

目的・趣旨

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

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

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

遵守事項

(1)　自己点検計画の策定・手順の準備

(a)　統括情報セキュリティ責任者は、対策推進計画に基づき**年度自己点検計画を策定**すること。

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

(c)　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(1)(a)「年度自己点検計画を策定」について**

  点検を実施するに当たり、対策推進計画に基づき適切に実施するため、実施頻度、実施時期、確認及び評価の方法や自己点検項目等を定めた年度自己点検計画を策定することが求められる。

  自己点検項目の選定に当たっては、情報セキュリティインシデントの発生状況に鑑みた項目や、前年度の自己点検実施率が低かった遵守事項等、様々な選択肢が考えられる。

- **遵守事項 2.3.1(1)(b)「職員等」について**

  本条における「職員等」には、情報セキュリティ責任者、課室情報セキュリティ責任者及び情報システムセキュリティ責任者等、情報セキュリティ対策の体制ごとの責任者を含む。具体的にどの責任者を対象に自己点検を実施するかについては、年度自己点検計画で策定する。

  情報セキュリティ責任者や課室情報セキュリティ責任者は、自組織の情報セキュリ

ティ対策について、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、区域情報セキュリティ責任者は、所管する区域における情報セキュリティ対策について実施するなど、役割に応じて異なることに留意が必要である。

なお、情報システムセキュリティ責任者の点検は、情報システムに係る各種セキュリティ対策の実施状況等を様々な観点で実施することが必要である。例えば、ソフトウェアの脆弱性への対処状況の点検であれば、セキュリティパッチや不正プログラム定義ファイルの更新状況を把握したり、実際の文書を確認したりするなど、代替の確認方法を含めた点検が考えられる。

- **遵守事項 2.3.1(1)(b)「自己点検票」について**

  職員等が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、情報セキュリティ責任者は、職員等ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することが重要である。

遵守事項

(2) 自己点検の実施

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

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(2)(a)「自己点検の実施」について**

  自己点検は、年に２度以上の頻度で実施することが望ましい。例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては、半年に一度の頻度で実施するなどが考えられる。

遵守事項

(3) 自己点検結果の評価・改善

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

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

(c) 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受けること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(3)(a)「自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価」について**

  情報セキュリティ責任者が自己点検の結果を分析、評価する際は、自らが担当する組織のまとまり、取り扱う情報等の特性に応じた課題や、改善すべき点があるか否かを確認する必要がある。例えば、職員等に求める安全管理措置のうち、特定の措置が実施できていないなどの課題の有無について、点検結果を分析して確認し、課題があることが判明した場合は、執務室の物理的条件、業務用システムの配備状況等の執務環境面も含めて原因分析を行う必要がある。原因分析の結果、速やかに改善すべきものがある場合は、自らの判断で措置が可能なものについては改善措置を講じた上で、その内容を含めて統括情報セキュリティ責任者へ報告することが望ましい。

  また、自己点検の実施内容が、自らが担当する組織のまとまりに対して適切であったか否かについて評価を行い、その結果を報告内容に含めることも重要である。例えば、情報の運搬に係る事務が多い職場において、重要な情報を紛失するなどのインシデントが発生しているにもかかわらず、情報の運搬に係る自己点検が項目に含まれていないなど、自己点検の実施内容について改善が必要と考えられる場合は、その旨を報告内容に含め、次回の自己点検において考慮されるようにすることが考えられる。

- **遵守事項 2.3.1(3)(b)「機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価」について**

  統括情報セキュリティ責任者が自己点検の結果を分析、評価する際は、機関等で共通的な課題や、改善すべき点があるか否かを確認する。例えば、複数の組織のまとまりにおいて同じ実施手順が守られていないことが判明した場合は、当該実施手順自体に問題がないか分析し、実施手順を見直す必要性を検討するなどして、その結果を最高情報セキュリティ責任者へ報告する。

また、自己点検の評価については、点検項目の選択の適切性や、組織のまとまりごとに適切な自己点検が実施されたか否かなどの観点で実施し、次回の年度自己点検計画の策定の際に参考にするとよい。

2.3.2 情報セキュリティ監査

目的・趣旨

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

また、監査の結果で明らかになった課題を踏まえ、最高情報セキュリティ責任者は、情報セキュリティ責任者に指示し、必要な対策を講じさせることが重要である。

遵守事項

(1) 監査実施計画の策定

(a) 情報セキュリティ監査責任者は、**対策推進計画に基づき監査実施計画を定める**こと。

(b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、**追加の監査実施計画を定める**こと。

【 基本対策事項 】

＜2.3.2(1)(a)関連＞

2.3.2(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

a) 監査の目的（例：情報セキュリティ対策の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等）

b) 監査の対象（例：監査の対象となる組織、情報システム、業務等）

c) 監査の方法（例：情報セキュリティ対策の運用状況を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、対策基準及び実施手順とする）

d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名）

e) 監査の実施時期（例：対象ごとの実施時期）

2.3.2(1)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足している場合等においては、**機関等外の者に監査の一部を請け負わせる**こと。

（解説）

- **遵守事項 2.3.2(1)(a)「対策推進計画に基づき監査実施計画を定める」について**

遵守事項 2.1.2(2)(a)に規定する対策推進計画には、監査の基本的な方針として、重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にする）・監査の実施時期・監査業務の管理体制等を簡潔に記載することを想定している。監査の基本的な方針の案は、情報セキュリティ監査責任者が作成することを想定している。また、情報セキュリティ監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。被監査部門に対しては、監査実施期間、監査実施者の

氏名、監査対象等を含む事項を、情報セキュリティ監査責任者より事前通知し、監査の内容や範囲をあらかじめ明確化しておくことが望ましい。

なお、内閣官房内閣サイバーセキュリティセンターが公表している「情報セキュリティ監査実施手順の策定手引書」は、監査実施計画の策定における考え方や計画に含めるべき内容等を具体的に示しており、これを参考に計画を策定するとよい。この他にも、経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」等にも詳細が説明されているので、併せて参考にするとよい。

参考 : 内閣官房内閣サイバーセキュリティセンター「情報セキュリティ監査実施手順の策定手引書」
（https://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf）

参考：経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」
（http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex05.pdf）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 2.3.2(1)(b)「追加の監査実施計画を定める」について**

機関等内外において注目すべき情報セキュリティインシデントが発生した場合は、機関等の実態を把握するため、追加的な監査を行い、必要な措置を講ずることが想定される。また、情報セキュリティ対策の実施内容に大きな変更が生じた場合は、その対策の実施状況を把握するために追加で監査を行うことも考えられる。このように、情報セキュリティ監査責任者は、対策推進計画に基づき策定した監査実施計画以外の事項についても、必要に応じて監査実施内容に含めることを考慮する必要がある。

- **基本対策事項 2.3.2(1)-2「機関等外の者に監査の一部を請け負わせる」について**

情報セキュリティ監査責任者は、監査を実施するに当たり、機関等内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮することが重要である。また、監査業務を外部事業者に請け負わせることは、外部委託に該当することから、関連する規定にも留意する必要がある。また、情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。加えて、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用するほか、経済産業省が定める「情報セキュリティ監査企業台帳に関する規則」に基づき作成される情報セキュリティ監査企業台帳を参照することも考えられる。

参考：経済産業省「情報セキュリティサービス基準」

（http://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf）

参考：独立行政法人情報処理推進機構（IPA）「情報セキュリティサービス基準適合サービスリスト」

（https://www.ipa.go.jp/security/it-service/service_list.html）

参考：経済産業省「情報セキュリティ監査企業台帳に関する規則」

（http://www.meti.go.jp/policy/netsecurity/is-kansa/audit_is_rule.pdf）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

遵守事項

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を**監査報告書**として最高情報セキュリティ責任者に報告すること。

(ア) 対策基準に**統一基準を満たすための適切な事項が定められていること**

(イ) 実施手順が対策基準に準拠していること

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

【 基本対策事項 】

＜2.3.2(2)(a)関連＞

2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、**被監査部門から独立した者**から選定し、情報セキュリティ監査実施者に指名すること。

（解説）

- **遵守事項 2.3.2(2)(a)「監査報告書」について**

監査報告書の作成に際しては、根拠となる監査調書を適切に作成することが必要である。監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等をつづり込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。

監査の結果は、監査報告書として文書化した上で、最高情報セキュリティ責任者へ確実に提出する必要がある。監査報告書には、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か、実際の運用状況が情報セキュリティ関係規程に準拠して行われているかなどの結果を記載する。さらに、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言・提案を監査報告書に含める。反対に組織として推奨すべき優れた取組等がある場合には、それらを組織全体に広めるなどの助言・提案があってもよい。

- **遵守事項 2.3.2(2)(a)(ア)「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」について**

運用指針 2(1)において、「統一基準には、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定する。」とされており、また、運用指針 2(2)において、「対策基準策定ガイドラインは、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、機関等による対策基準の策定及び実施に際しての考え方等を解説することを目的として策定する。基本対策事項は遵守事項に対応するものであるため、機関等は対策基準策

定ガイドラインを参照し、基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要があるものである。」とされている。これらの記述から、本項で定める「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」について監査する際は、基本対策事項及び解説の記載についても参照した上で監査を実施する必要がある。

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か否かを判断する際には、機関等における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性等を踏まえ、必要な事項が対策基準に盛り込まれているか否かを確認する必要がある。このため、対策基準の策定に当たり、対策基準に各事項を盛り込んだ理由や本ガイドラインの基本対策事項との関係等について記録を残しておくと、監査の際に有用である。

- **遵守事項 2.3.2(2)(a)(ウ)「実際の運用」について**

被監査部門の職員等に対する質問や記録文書の査閲、執務室等の観察、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することも求められる。例えば、監査対象によってはソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性の検査、情報システムに対する侵入検査といった方法によっても確認することができる。

なお、監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を行った場合には、その行為に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、情報セキュリティ対策の向上になり得る行為や、作業を効率的に行うことにつながる行為であるとしても、監査以外の行為を監査実施計画の中に取り込むべきではない。

- **基本対策事項 2.3.2(2)-1「被監査部門から独立した者」について**

情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。例えば、情報システムを監査する場合に、当該情報システムの構築をした者や運用を行っている者が監査をしてはならない。また、情報の取り扱われ方に関する監査を行う場合には、当該情報を取り扱う者はその監査をしないこととする。

遵守事項

(3) 監査結果に応じた対処

(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示すること。

(b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、**機関等内で横断的に改善が必要な事項**について、**必要な措置を行った上で改善計画を策定**し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。

(c) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、**自らが担当する組織のまとまりに特有な改善が必要な事項**について、**必要な措置を行った上で改善計画を策定**し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。

【 基本対策事項 】規定なし

(解説)

- **遵守事項 2.3.2(3)(b)「機関等内で横断的に改善が必要な事項」について**

監査報告書に記載される改善が必要な事項の内容によっては、監査を受けた部門以外の部門においても同種の課題や問題が存在している可能性がある。また、機関等内で共通的に使用している情報システムに対する改善が必要な事項については、監査を受けた部門のみで対処することが困難であると同時に、情報システムの利用部門全体に係る改善が必要な事項となる可能性がある。このような、組織全体として改善が必要な事項が確認された場合は、統括情報セキュリティ責任者がその対策に係る事務を統括することが求められる。

なお、改善を指示されていない事項であっても、監査によって得られた教訓等を被監査組織以外にも展開し、組織全体で監査の教訓を対策に生かすことを考慮することも、組織全体の情報セキュリティを強化するために重要な取組である。

- **遵守事項 2.3.2(3)(b)「必要な措置を行った上で改善計画を策定」・遵守事項 2.3.2(3)(c)「必要な措置を行った上で改善計画を策定」について**

改善が必要な事項の中には、緊急の措置が必要なものが存在する可能性があることから、そのような事項が確認された場合は、直ちに措置を行い、その結果を報告する必要がある。情報システムの機能改修を伴う措置等、即時の実施が困難と考えられるものについては、情報セキュリティに係るリスクを軽減させるための暫定的な措置を講ずるなどの対応を行うとともに、情報システムの改善計画を策定し、暫定的な措置の実施結果と併せて報告する必要がある。

- **遵守事項 2.3.2(3)(c)「自らが担当する組織のまとまりに特有な改善が必要な事項」につ**

いて

遵守事項 2.3.2(3)(a)により、最高情報セキュリティ責任者から指示を受けた改善すべき事項のうち、遵守事項 2.3.2(3)(b)における「機関等内で横断的に改善が必要な事項」を除いたものを指している。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

目的・趣旨

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

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

遵守事項

(1) 情報セキュリティ関係規程の見直し

(a) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策基準について必要な見直しを行うこと。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(1)(a)「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」について**

  機関等における情報セキュリティインシデントの発生状況、例外措置の申請状況、自己点検や情報セキュリティ監査の結果、職員等からの相談等を踏まえ、対策基準に課題及び問題点が認められるか否かなどの観点から総合的な評価を行い、対策基準について所要の見直しを行うことについて、最高情報セキュリティ責任者に求めている。

  また、本部監査において助言された事項に関し、対策基準を見直す必要があるか否かを確認し、必要とされる場合には対策基準の見直しを行う。

- **遵守事項 2.4.1(1)(b)「整備した者に対して規定の見直しを指示」について**

  機関等における情報セキュリティインシデントの発生状況、自己点検や情報セキュリティ監査の結果、本部監査の結果、職員等からの相談、最高情報セキュリティ責任者

からの指示等を踏まえ、情報セキュリティ対策に関する実施手順を見直すことの必要性を検討し、情報システムセキュリティ責任者等の実施手順を整備した者に、その見直しを指示することを統括情報セキュリティ責任者に求めている。

なお、策定済みの実施手順を見直すだけではなく、例えば、機関等内における共通のルールが存在しないため、各所属等において個別にルールを定めて運用しているなどの場合について、機関等内における共通のルールを整備するか否かを検討することも考えられる。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(2)(a)「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」について**

  機関等における情報セキュリティインシデントの発生状況、自己点検、情報セキュリティ監査の結果、職員等からの相談等を踏まえ、対策推進計画に加えるべき事項の有無、策定済みの計画の変更が必要であるか等の観点から、評価を行う。

  また、本部監査において助言された事項において、対策推進計画に盛り込むべき事項がある場合は、当該事項の実施優先順位を検討した上で、適切に計画に盛り込むこととする。

- **遵守事項 2.4.1(2)(a)「情報セキュリティに係る重大な変化等」について**

  サイバー攻撃の量的な拡大や攻撃手法の高度化等による質的な変化等、計画策定時に前提としていた条件から大きく異なり、情報セキュリティに係るリスクが高まった場合や、年度途中における種々の要因により、当初の対策推進計画では課題解決が図られていない場合等を想定している。

第3部 情報の取扱い

3.1 情報の取扱い

3.1.1 情報の取扱い

目的・趣旨

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

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

遵守事項

(1) 情報の取扱いに係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、職員等へ周知すること。

(ア) 情報の**格付及び取扱制限についての定義**

(イ) 情報の**格付及び取扱制限の明示等**についての手続

(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続

【 基本対策事項 】

＜3.1.1(1)(a)関連＞

3.1.1(1)-1 統括情報セキュリティ責任者は、情報の取扱いに関する規定として、以下を例とする**手順を整備**すること。

a) 情報のライフサイクル全般にわたり必要な手順（業務の遂行以外の目的での情報の利用等の禁止等）

b) 情報の入手・作成時の手順

c) 情報の利用・保存時の手順

d) 情報の提供・公表時の手順

e) 情報の運搬・送信時の手順

f) 情報の消去時の手順
g) 情報のバックアップ時の手順

＜3.1.1(1)(a)(イ)関連＞

3.1.1(1)-2 統括情報セキュリティ責任者は、情報の格付及び取扱制限の**明示の方法**について、以下を例に、規定を整備すること。

a) 電磁的記録として取り扱われる情報に明示する場合
- 電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
- 電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
- フォルダ単位等で取り扱う情報は、フォルダ名に記載
- 電子メールで取り扱う情報は、電子メール本文又は電子メール件名に記載

b) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合
- 保存する電磁的ファイル又は文書等の単位ごとに記載
- 外部電磁的記録媒体本体に記載

c) 書面に印刷されることが想定される場合
- 書面のヘッダ部分等に記載
- 冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載

d) 既に書面として存在している情報に対して格付や取扱制限を明示する場合
- 手書きによる記入
- スタンプ等による押印

3.1.1(1)-3 統括情報セキュリティ責任者は、情報の格付及び取扱制限の**明示を省略**する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。

＜3.1.1(1)(a)(ウ)関連＞

3.1.1(1)-4 統括情報セキュリティ責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。

a) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。
b) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。
c) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。
d) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。
e) 完全性及び可用性については、作成時又は**複製時に適切な格付を決定**する。
f) 他者が決定した情報の格付及び取扱制限を**見直す必要がある場合**には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本款において「決定者等」という。）に確認を求める。

（解説）

- **遵守事項 3.1.1(1)(a)(ア)「格付及び取扱制限についての定義」について**

「統一基準 1.2 (1) 情報の格付の区分」及び「統一基準 1.2 (2) 情報の取扱制限」にて規定している情報の格付及び取扱制限の定義に基づき、機密性、完全性、可用性に係る情報の格付と取扱制限について、機関等の基準を整備する必要がある。取扱制限については、1.5(2)【参考】取扱制限の例も参照のこと。

なお、文書管理ガイドラインにおいて、「文書の作成者は、当該文書が極秘文書又は秘文書に該当すると考えられる場合には、それぞれに準じた管理を開始する」とされており、指定前の秘密文書も、機密性３情報として管理することが求められる。また、独立行政法人及び指定法人における機密性３情報についても同様の管理が求められるが、法人において機密性３情報を取り扱わない場合は、統一基準群における機密性３情報に係る規定について、対策基準の策定においてその必要性も含め検討し、法人の実情に合わせて規定するとよい。

- **遵守事項 3.1.1(1)(a)(イ)「格付及び取扱制限の明示等」について**

秘密文書においては、文書管理ガイドラインにおける「秘密文書表示」を行った場合には、別途「機密性３情報」に係る明示等を行う必要はない。

- **基本対策事項 3.1.1(1)-1「手順を整備」について**

a)～g)は、遵守事項 3.1.1(2)～(8)における職員等を名宛人とした対策事項とそれぞれ対応している。本事項では、これらの内容を包含する形で手順を定めることを求めている。

- **基本対策事項 3.1.1(1)-2「明示の方法」について**

当該情報を参照する者が、情報の格付及び取扱制限を確実に視認することができるよう、当該情報に記載することによる明示を原則とする。また、情報の格付及び取扱制限の明示については、以下の事項についても留意すること。

  - 本文において格付を明示することに加え、ファイル名の先頭に格付を付す。（例：「【機２】○○整備計画」）
  - 格付及び取扱制限の明示と併せて、情報の作成者又は入手者の氏名、所属、連絡先等も記載する。
  - 文書の一部の情報に取扱制限を追加するときは、追加する取扱制限を当該情報に近接した場所に明記する。
  - 電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記する。
  - 文書の作成者名、組織名その他の記録に使用できる「プロパティ」に格付の区分を記載することは明示に当たらない。

- **基本対策事項 3.1.1(1)-3「明示を省略」について**

情報の格付及び取扱制限を確実に視認することができるよう、当該情報に明示しておくことが原則ではあるが、必要な場合には、以下を例に明示が省略可能な条件につい

て定めておくとよい。

- 情報システムに記録される情報の格付及び取扱制限を当該情報システムの手順書等により明記し、当該情報システムの利用者にあらかじめ周知している場合。
- 情報の格付及び取扱制限の省略時における当該情報の格付及び取扱制限の取扱について、取扱手順に規定し、職員等にあらかじめ周知している場合。

ただし、格付及び取扱制限の明示を省略した場合には、以下の事項に注意する必要がある。

- 格付及び取扱制限の省略を認識できない者への情報の提供

  格付の区分及び取扱制限が明示されていない要保護情報を、格付及び取扱制限の決定内容を認識できない職員等に提供する必要が生じた場合（例えば、他機関等に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限を明示した上で提供するなどしなければならない。
- 取扱制限の明示を省略した場合における取扱制限の追加・変更

  例えば、ある文書の取扱制限の明示を省略している場合であって、当該文書の一部に取扱制限を追加するときは、追加する取扱制限を明示すること。

- **基本対策事項 3.1.1(1)-4 e)「複製時に適切な格付を決定」について**

複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、完全性及び可用性については、適宜、複製の目的に応じて格付を決定する必要がある。

- **基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について**

利用する元の情報への修正、追加又は削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は当該決定者の上司に相談し、その是非を検討することになる。決定者等による見直しが無い限り、当該情報の利用者がこれらの者に無断で、格付又は取扱制限を変更することは許されない。

なお、見直しを行わなければならない場合については、以下を参考に規定すること。

- 作成時には要機密情報だった情報の機密性が失われた場合（時間の経過により変化した場合）
- 機密性３情報として格付されている資料等から機密性３情報に係る部分を全て削除した場合
- 取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
- 取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合
- 格付及び取扱制限を決定した際の判断が不適切であったと考えられる場合
- 行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等における情報の取扱いに変更がある場合

遵守事項

(2) 情報の目的外での利用等の禁止

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(2)(a)「情報を利用等」について**

情報は、業務の目的を達成するために利用等するのであって、業務の遂行以外の目的で情報を利用等すべきではない。国家公務員法 第100条 第1項においても、「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。」と定められている。

情報の目的外利用に当たる場合としては、例えば、業務上知り得た情報をソーシャルメディアサービスの個人アカウントの掲示板等に掲示する、私的にウェブ上の各種サービス（SNS 等）を利用する際に、業務に使用しているメールアドレスと主体認証情報を利用するなどの行為が考えられる。その他にも、情報の利用形態は様々であり、注意が必要である。

なお、本条で対象としている情報は、職員等が従事する業務において利用する機関等の情報システムから入手可能な業務に係る情報（業務上知り得る情報）や、情報システムにおいて利用される主体認証情報（パスワード等）であり、情報システムの仕様やデータ設定等に係る情報（メールアドレス等）も含んでいる。一方、業務時間外に自宅等の私物端末から機関等のウェブサイトにアクセスして、公表されている情報を入手するなどの行為については、本条の対象とはしていない。

遵守事項

(3) 情報の格付及び取扱制限の決定・明示等

(a) 職員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。

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

(c) 職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(3)(a)「格付及び取扱制限を決定」について**

格付及び取扱制限が不十分な場合、情報漏えい等のリスクが高まるが、一方で、情報の利用を円滑に行うためには、格付及び取扱制限を必要以上に高くしないことが必要である。そのため、格付及び取扱制限を決定する際には、機関等の基準に照らして、要件に過不足が生じないようにすること。例えば、機密性１情報に相当する公開しても差し支えない情報をむやみに要機密情報に決定すると、過度な保護対策を求めることになり、業務の効率的な運営に支障をきたすおそれがある。

また、他機関等との情報の受け渡しを行う際には、統一基準との格付定義の差分に関する情報を当該機関等から得るなどして、自機関等の基準との差分について考慮の上、格付及び取扱制限を決定する必要がある。

- **遵守事項 3.1.1(3)(b)「継承」について**

業務資料等を参考に新たに別の資料を作成する場合等において、元となった資料等に記載されていた情報の機密性に関する格付及び取扱制限について、新たに作成した資料等に適切に引き継ぐことを求めている。例えば機密性３情報を他の資料等に転用する場合においては、当該資料に記載されている転用部分については機密性３情報として取り扱われるべきである。また、要保全情報又は要安定情報を複製する場合については、複製された情報に対して過度な保護対策を求めないように、完全性１情報又は可用性１情報として格付を見直し再決定することが望ましい。ただし、バックアップを原本として情報を保管する目的で複写する場合は、要保全情報とすべきであるなど、状況に応じた適切な判断が求められる。

- **遵守事項 3.1.1(3)(c)「決定者等に確認し、その結果に基づき見直す」について**

「(解説)基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照のこと。

遵守事項

(4) 情報の利用・保存

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

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

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

(d) 職員等は、**保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること**。なお、独立行政法人及び指定法人における職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずること。

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

(ｲ) 当該情報に対し、暗号化による保護を行うこと。

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

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

【 基本対策事項 】

＜3.1.1(4)(a)(d)関連＞

3.1.1(4)-1 職員等は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。

a) 要保護情報を**放置しない**。

b) 要機密情報を**必要以上に複製しない**。

c) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

d) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

e) 情報の**保存方法を変更**する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。

3.1.1(4)-2 職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

（解説）

- **遵守事項 3.1.1(4)(c)「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」について

機関等外で開催される会議への出席等の際に、要機密情報を用いて情報処理を行う場合は、のぞき見の防止や不要となった情報の削除等の措置を講ずるなど、情報の格付や取扱制限に応じて適切な安全管理措置を講ずる必要がある。この際、技術的な対策については、遵守事項 7.1.1(4)(a)に基づき定められた安全管理措置を参考にするとよい。

- **遵守事項 3.1.1(4)(d)「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」について**

情報システムに、ファイルに対する書込権限者の制限や、ファイルのセキュリティ設定でパスワード設定等のアクセス制御機能が装備されている場合、当該情報の格付及び取扱制限に従って、必要なアクセス制御の設定を行うことが求められる。例えば、取扱制限として閲覧範囲の制限が指定されている場合は、第三者等から参照されないよう、読取制限の属性を付与することや、要保全情報であれば、第三者等から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

アクセス制御は、サーバ装置、端末、OS、アプリケーション、ファイル等を単位に行うことができるため、これらを選択し組み合わせて、適切なアクセス制御を実現するとよい。

なお、文書管理ガイドラインの秘密文書の管理に関するモデル要領において、「秘密文書については、インターネットに接続していない電子計算機又は媒体等に保存し、暗号化等による保護を行うとともに、当該秘密文書を記録する電子計算機、媒体等について、保存を金庫等で行うなどにより物理的な盗難防止措置を施すこと。秘文書については、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機でも保存することができる。」とされている。

- **遵守事項 3.1.1(4)(d)(ウ)「盗難及び不正な持ち出し等の物理的な脅威から保護するための対策」について**

端末についての対策例は基本対策事項 7.1.1(1)-2、サーバ装置についての対策例は基本対策事項 7.1.2(1)-2 を参照のこと。

- **遵守事項 3.1.1(4)(e)「外部電磁的記録媒体」について**

外部電磁的記録媒体には、USB メモリ等の、繰返し情報を書き換えできる媒体と、CD-R 等の書き換えできない媒体が存在する。特に前者の媒体を利用する場合は、不正プログラムに感染するおそれが大きいため、その取扱いには細心の注意を払う必要がある。（具体的な対策等については、【参考 8.1.1-1】を参照のこと。）

- **遵守事項 3.1.1(4)(e)「定められた利用手順」について**

遵守事項 8.1.1(1)(d)において定められた利用手順を指す。

- **基本対策事項 3.1.1(4)-1 a)「放置しない」について**

悪意ある第三者等による不正な操作や盗み見等を防止することを求める事項である。例えば、離席する際には、ロック付きスクリーンセーバを起動する又はログアウトして画面に情報を表示しない、机の上に書類を放置して長時間離席しない、印刷した書面を

速やかに回収し出力トレイに放置しないこと等を徹底する必要がある。

- **基本対策事項 3.1.1(4)-1 b)「必要以上に複製しない」について**

  電磁的記録は比較的容易に複製することができるという特性があり、可用性の観点から複製された情報が多数の端末に散在する傾向になることが想定されるため、機密性３情報に該当しない情報であっても、複製は必要最小限にとどめるよう留意する必要がある。

  なお、秘密文書に関しては、文書管理ガイドラインにおいて、「秘密文書の複製等は必要最小限にとどめること。」と定められていることに留意すること。

- **基本対策事項 3.1.1(4)-1 e)「保存方法を変更」について**

  当該情報が記載されている文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか､利用の制限についての意見を付すなどして移管する必要がある｡その際、パスワードを設定していた場合は解除するなどして、移管先がその内容を参照できるように配慮する必要がある。

遵守事項

(5) 情報の提供・公表

(a) 職員等は、情報を公表する場合には、当該情報が**機密性１情報に格付されるもの**であることを確認すること。

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

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

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

【 基本対策事項 】

＜3.1.1(5)(d)関連＞

3.1.1(5)-1 職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

（解説）

- **遵守事項 3.1.1(5)(a)「機密性１情報に格付されるもの」について**

保有する情報をウェブサイト等により広く国民に提供する場合、公表しようとする情報の格付の適正さを再度検討し、格付及び取扱制限の明示を削除するなどを考慮する必要がある。

なお、情報の公表ではないものの、電子調達システム等において調達情報を委託先候補事業者に閲覧を許可する場合が考えられる。情報システムの構成図等サイバー攻撃を企図する者が有利になるような情報については、開示対象者と機密保持契約を締結するなどして厳重な管理のもと閲覧を許可するなどして、細心の注意を払う必要がある。

- **遵守事項 3.1.1(5)(b)「決定者等に相談」について**

「（解説）基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照のこと。

- **遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について**

要保護情報を機関等外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の取扱い上の留意事項を提供先へ確実に伝達する必要がある。

伝達方法としては、他機関等や委託先等の情報の提供先に、対策基準や情報の取扱いに関する手順書、統一基準との格付定義の差分に関する説明等を提示し、格付や取扱制限に応じた取扱方法を示す方法が考えられる。この場合、格付の区分だけを示しても、

提供先においては当該格付区分がどのように取り扱われるべきものであるか認識できない可能性があるため、当該格付の区分の定義について提供先にあらかじめ周知しておく必要がある。また、提供する情報を適切に管理するために必要な措置が具体的に分かるようにする（例えば、「委員以外への再配布を禁止する」と明示する。）など、格付以外の方法で取扱方法を示すことも考慮する必要がある。

- **遵守事項 3.1.1(5)(d)「不用意な情報漏えい」について**

  情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。

  また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

遵守事項

(6) 情報の運搬・送信

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

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

【 基本対策事項 】

＜3.1.1(6)(a)関連＞

3.1.1(6)-1 職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、**セキュアな運送サービス**を提供する運送事業者により運搬すること。

＜3.1.1(6)(a)(b)関連＞

3.1.1(6)-2 職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は機関等外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。

a) **運搬又は送信する情報を暗号化する**。

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。

c) 主体認証機能や暗号化機能を備える**セキュアな外部電磁的記録媒体**が存在する場合、これに備わる機能を利用する。

＜3.1.1(6)(b)関連＞

3.1.1(6)-3 職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

a) 機関等管理の通信回線を用いて送信する。

b) **信頼できる通信回線**を使用して送信する。

c) VPN を用いて送信する。

d) S/MIME 等の暗号化された電子メールを使用して送信する。

e) 機関等独自で運用するなどセキュリティが十分確保されたウェブメールサー

ビス又はオンラインストレージ環境を利用する。

（解説）

- **基本対策事項 3.1.1(6)-1「セキュアな運送サービス」について**

  セキュアな運送サービスとしては、受領印が必要となる書留郵便や、専用車両による配達サービス、配達状況の追跡が可能なサービス等が存在する。

- **基本対策事項 3.1.1(6)-2 a)「運搬又は送信する情報を暗号化する」について**

  暗号化された情報の復号に用いる鍵は、十分な長さと複雑さを有することが求められる。また、暗号化された情報の復号に用いる鍵を、暗号化された情報と同じ経路で送信等したり、第三者が容易に知り得る方法で送信等したりしてしまうと、第三者によって情報が復号されるおそれが高くなると考えられることから、暗号化された情報の復号に用いる鍵は、暗号化された情報とは別の方法で送信するなどして秘匿性を確保することが考えられる。

- **基本対策事項 3.1.1(6)-2 b)「複数の情報に分割し」について**

  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、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。

- **基本対策事項 3.1.1(6)-2 c)「セキュアな外部電磁的記録媒体」について**

  セキュアな外部電磁的記録媒体が備える機能としては、主体認証機能、暗号化機能の他、不正プログラムの検閲・駆除機能、遠隔データ消去機能、接続管理機能等がある。USB メモリ等の外部電磁的記録媒体の運搬に当たっては、必要最小限の情報のみを保存するよう留意するとともに、盗難・紛失等による情報漏えいに備え、当該機能を適切に利用することが必要である。

- **基本対策事項 3.1.1(6)-3 b)「信頼できる通信回線」について**

  空港や商業施設等が提供する無線 LAN 等の通信回線は、十分なセキュリティ対策がとられていない場合もあるため、要保護情報を送信する場合にこれを用いるべきではない。

遵守事項

(7) 情報の消去

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

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

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(7)(a)「速やかに情報を消去」について**

情報セキュリティの観点からは、不正プログラム感染による情報窃取や操作ミスによる情報漏えい等を防ぐ観点から、職務上不要となった情報を速やかに消去する必要があるが、その際には、公文書管理法等で保存が求められる情報を誤って消去しないよう、注意を払う必要がある。

- **遵守事項 3.1.1(7)(b)「抹消する」について**

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。

- データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法
- ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
- 媒体を物理的に破壊する方法

また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。

- （フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法
- （CD-R/RW、DVD-R/RW 等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法
- （媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法

また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。

なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と

抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施してもよい。

- **遵守事項 3.1.1(7)(c)「復元が困難な状態にする」について**

  電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却、溶解等により、復元が困難な状態にする必要がある。

  なお、廃棄すべき書類が大量にあるなどの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。また、無人の執務室に設置されている又は設置場所及び利用場所が確定していないなどの環境で利用される情報システム、外部電磁的記録媒体等については、不要な情報を可能な限り抹消しておくことが望ましい。

遵守事項

(8) 情報のバックアップ

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

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

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

【 基本対策事項 】

＜3.1.1(8)(a)関連＞

3.1.1(8)-1 職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。

＜3.1.1(8)(b)関連＞

3.1.1(8)-2 職員等は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は**重要な設計書**のバックアップについて、**災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する**こと。

（解説）

- **遵守事項 3.1.1(8)(a)「適切な方法で情報のバックアップを実施する」について**
  - 災害や情報セキュリティインシデントが発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。以下の例を参考に、情報のバックアップ方法について考慮するとよい。想定する災害等の事象（地震、津波、火災、高出力電磁波等）
  - バックアップの対象（対象とするシステム、データ、ソフトウェアその他）
  - バックアップの範囲（フルバックアップ、差分バックアップ等）
  - バックアップを保存する電磁的記録媒体等の種類
  - バックアップの周期、世代管理の方法
  - 使用するバックアップツール
  - バックアップデータの秘匿性確保、改ざん防止の方法

- **遵守事項 3.1.1(8)(b)「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」について**

  バックアップデータに要機密情報が含まれる場合は、バックアップデータの盗難・紛失による情報漏えい等を回避するために、バックアップデータを要管理対策区域に保管することが望ましい。また、バックアップデータを保存する媒体の耐久性にも留意し、定期的に媒体を新しいものに入れ替えるなども考慮するとよい。

- **基本対策事項 3.1.1(8)-2「重要な設計書」について**

  情報システムの委託先から書面のみで提示された設計書類等、情報システムに記録されていない書面のみの情報であって、紛失、改ざん等により情報システムの運用に支障を及ぼす可能性のあるものを指している。バックアップが外部に流出することにより、攻撃者に有利になるものについては、保管の際に機密性を確保することにも留意する必要がある。

- **基本対策事項 3.1.1(8)-2「災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する」について**

  災害等を想定してバックアップを取得する場合は、完全性等の要求に応じ、想定する災害等の事象に耐性のある保管庫や施設、同時被災しない遠隔地に保管すること等が考えられる。また、遠隔地に保管するに当たっては、実際にバックアップを用いた復旧に要する時間が、情報システム運用継続計画における復旧目標時間内に納まるよう、緊急時のバックアップデータの配送手段、配送時間等を考慮し、保管場所を決定する必要がある。

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**。

【 基本対策事項 】

＜3.2.1(1)(b)(ア)(イ)関連＞

3.2.1(1)-1　統括情報セキュリティ責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。

a）下表のとおり、３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

3.2.1(1)-2　統括情報セキュリティ責任者は、クラス１の区域について、以下を含む施設の

整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

b) 不特定の者が容易に立ち入らないように、**立ち入る者の身元、訪問目的等の確認を行うための措置**を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

c) 要管理対策区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。

- 職員等は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。
- 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

3.2.1(1)-3 統括情報セキュリティ責任者は、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は職員等が窓口を常に目視できるような措置を講ずること。

b) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

c) **クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

3.2.1(1)-4 統括情報セキュリティ責任者は、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

b) **クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

c) クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合

は立会いや監視カメラ等により監視するための措置を講ずること。

3.2.1(1)-5 統括情報セキュリティ責任者は、以下を例とする、区域への**クラスの割当ての基準**を定めること。

a) クラスの割当ての基準を以下のように定める。

- サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。
- 一般的な執務室や執務室内の会議室には、職員等以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

（解説）

- **遵守事項 3.2.1(1)(a)「要管理対策区域の範囲を定める」について**

執務室やサーバ室のほか、複数の機関等で共用する会議室や職員等が書面やモバイル端末等を運搬するときの安全性を高めるために、執務室間や会議室に接続されている廊下等も要管理対策区域に含めることを考慮してもよい。

なお、要管理対策区域外で業務を行う必要がある場合には、施設及び環境に係る対策が講じられないことから情報の漏えい等の可能性が高くなる。情報の漏えい等の可能性を低減するためには、要管理対策区域外でのモバイル端末の利用に関する遵守事項（ 遵守事項 7.1.1(4)、遵守事項 8.1.1(1)(b)等）を参照し、適切な対策を行うことが必要である。

- **遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について**

本基本対策事項 3.2.1(1)-2～4 に示した対策の基準のほか、以下を対策の基準に含めてもよい。

- 共連れ（立入りを許可された者が立ち入る際に、立入りを許可されていない者を同時に立ち入らせるような行為）を防止する措置を講ずること。

  具体的な対策として、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。
- 立入りを許可されていない者の侵入等、区域の安全性が侵害された場合に追跡することができるように、立入り及び当該区域からの退出を記録及び監視する措置を講ずること。

  「記録及び監視する」具体的な対策として、警備員、監視カメラ等による記録及び監視のほか、要管理対策区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。継続的に立入りが許可されている者以外の者の立入りがあった場合には、立入りの記録として立ち入った者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日、立入り及び退出の時刻を記録することが挙げられる。

- 受渡業者と物品の受渡しを行う場所を制限すること。
  なお、「受渡業者」とは、職員等との物品の受渡しを行う者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

- **基本対策事項 3.2.1(1)-2 b)「立ち入る者の身元、訪問目的等の確認を行うための措置」について**

クラス１の区域に「立ち入る者」について、継続的に立入りを許可された者のほか、一時的に立ち入る者（訪問者）がある。継続的に立入りを許可された者として、職員等や一定期間立入りを認められ、認められたことを示す許可証（入館カード等）が貸与されている業者等を想定している。また、一時的に立ち入る者として、不定期に訪れる来客や受渡業者等を想定している。

「身元、訪問目的等の確認を行うための措置」の具体的な対策として、以下が挙げられる。

- セキュリティゲートの設置、警備員や受付係等の配置をして立ち入る者に身分証明書等の提示を求める。
- 一時的に立ち入る者の氏名及び所属、訪問目的等を記録する。

- **基本対策事項 3.2.1(1)-3 c)「クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。
  なお、IC カード等による主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずることが望ましい。
- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
- 立入りを監視する警備員、受付係等を配置している場合は、許可する者が警備員等にあらかじめ一時的に立ち入る者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日時等を伝えておき、一時的に立ち入る者が来訪した際に警備員、受付係等が照合する。

クラス２の区域への立入り時の「許可された者であることの確認」について、クラス１の区域への立入り時に「身元、訪問目的等の確認」ではなく「許可された者であることの確認」を行っている場合においては、それをもって代替してもよい。

- **基本対策事項 3.2.1(1)-4 b)「クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。
- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可

する者が自ら区域の境界まで迎えに行く。

- 継続的に立入りが許可されている者のみに、常時施錠される扉の鍵を貸与したり、解錠するための暗証番号を通知したりしておき、鍵の所持や入力した暗証番号の一致により、確認する。

- **基本対策事項 3.2.1(1)-5「クラスの割当ての基準」について**

各区域へのクラスの割当ての基準の策定に当たっては【参考 3.2.1-1】を参考にするとよい。本基本対策事項においては、例としてサーバ室や日常的に機密性が高い情報を取り扱う執務室にはクラス３、一般の執務室や執務室内の会議室にはクラス２を割り当てるという基準を示している。

統括情報セキュリティ責任者は、区域情報セキュリティ責任者に、管理する区域で取り扱う情報、設置される情報システムの特性から、外部からの侵入があった場合の被害の大きさを考慮してクラスを決定させる必要があることを踏まえ、本基本対策事項で示す基準を参考とし、クラスの割当ての基準を定める必要がある。

また、業務の単位でクラスの割当ての基準（例：○○、××に関係する業務を行う執務室はクラス３、これら以外の業務を行う執務室はクラス２）を定めておくことも考えられる。

【参考 3.2.1-1】 要管理対策区域へのクラスの割当ての例

要管理対策区域へのクラスの割当ての例を図 3.2.1-1～3 に示す。

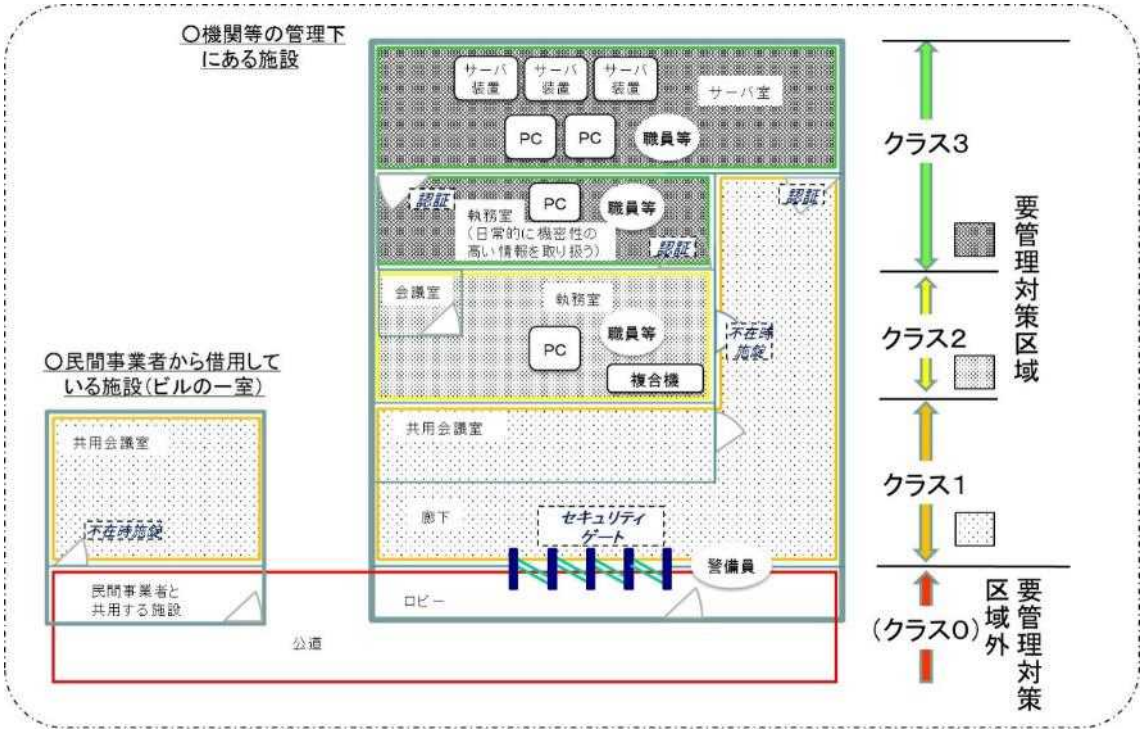


図 3.2.1-1 要管理対策区域へのクラスの割当ての例１（庁舎又は民間事業者から借用する施設）

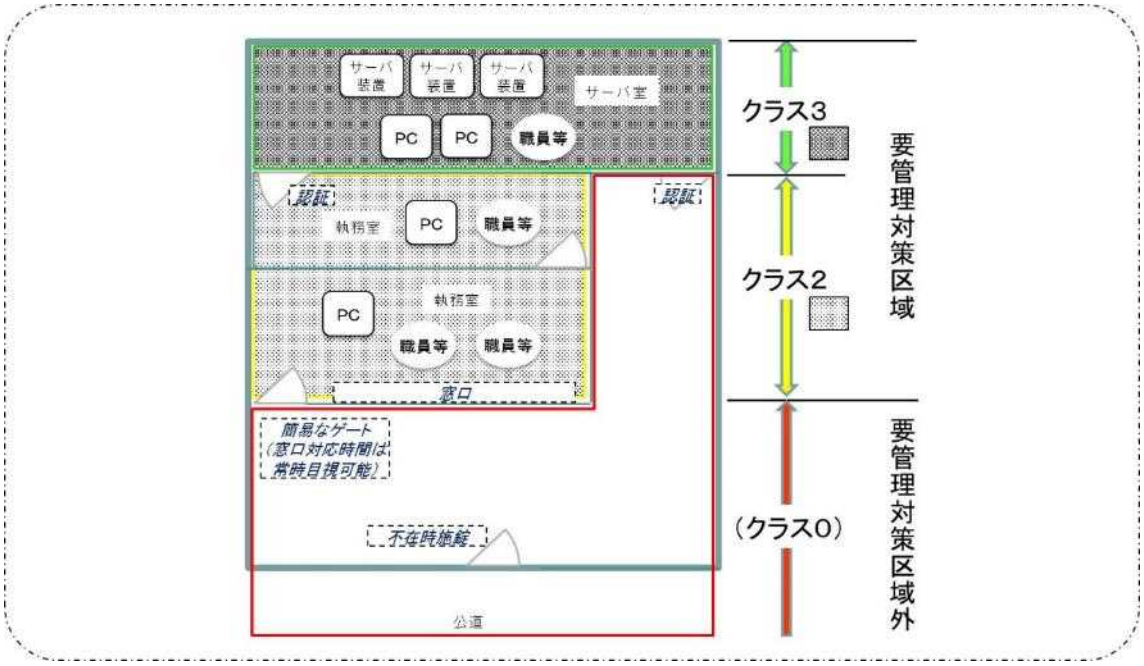


図 3.2.1-2 要管理対策区域へのクラスの割当ての例２（窓口のある執務室）

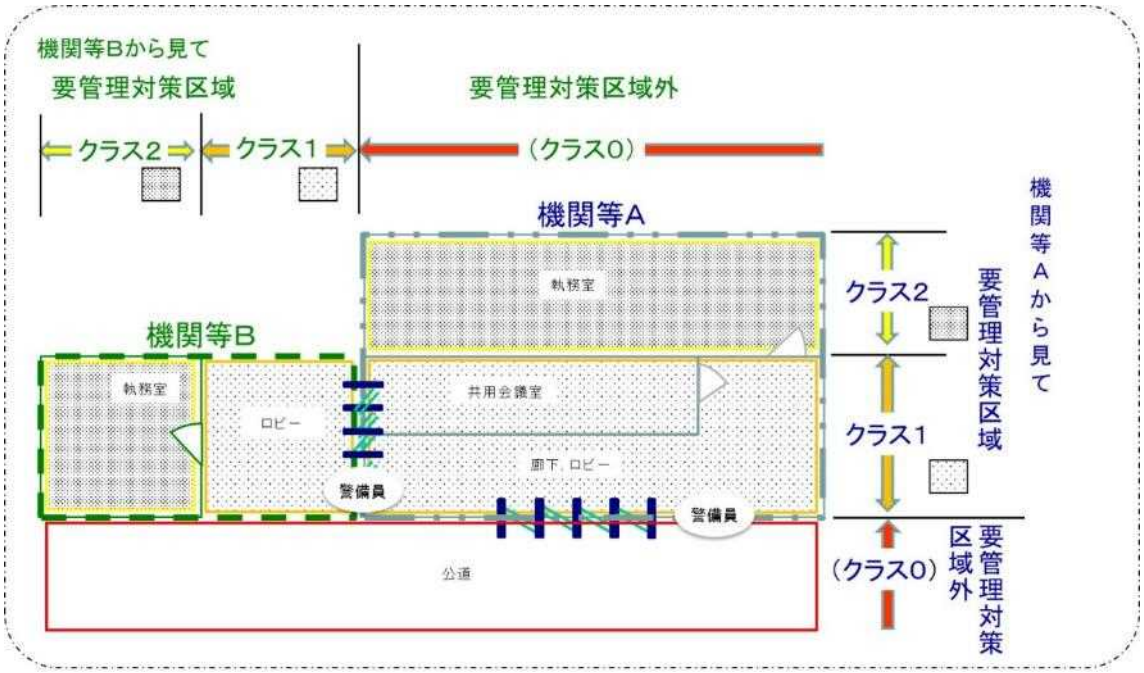


図 3.2.1-3 要管理対策区域へのクラスの割当ての例３
（複数の機関等で共用する施設）

遵守事項

(2) 区域ごとの対策の決定

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

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

【 基本対策事項 】

＜3.2.1(2)(b)関連＞

3.2.1(2)-1 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。

（解説）

- **遵守事項 3.2.1(2)(a)「施設及び執務環境に係る対策を行う単位ごとの区域を定める」について**

  複数の部局で共用する廊下等については、施設管理の観点での各部門の管理範囲を確認した上で「施設及び執務環境に係る対策を行う単位ごとの区域」を定めるとよい。共用する施設の区域情報セキュリティ責任者の定め方については、「(解説) 遵守事項 2.1.1(4)(b)「区域情報セキュリティ責任者」について」を参照のこと。

- **基本対策事項 3.2.1(2)-1「割り当てるクラスを決定する」について**

  クラス３、クラス２以外の要管理対策区域はクラス１となることにも留意して決定する必要がある。クラス１の区域は、不特定の者が容易に立ち入れない程度の安全性が確保された区域である。したがって、原則として、盗難や盗み見等への対策が講じられていない端末や書面が置かれる区域にクラス１を割り当ててはならない。やむをえずクラス１の区域に端末を置く必要がある場合（例：来訪者受付に職員等や来訪者の名簿を閲覧するための端末を置く場合）には、セキュリティワイヤ等で固定することや、常時目視により監視するなどの措置を講ずる必要がある。

- **基本対策事項 3.2.1(2)-1「当該区域において実施する対策を決定する」について**

  周辺の区域のクラスや管理状況も確認して具体的な対策を決定するとよい。例えば、クラス３の区域がクラス０の区域と接続している場合は、クラス３の区域の扉の施錠管理をより厳重にすることが考えられる。また、民間事業者が管理するビルの部屋を借りて業務を行っているような場合は、当該ビルの共用部分等では十分な対策が講じられないことが想定される。そのような場合には、借用している部屋の入退管理の強化や

共用施設での業務の禁止を徹底すること等により、安全性を高めることが重要である。

なお、必要な対策が施設管理等の別の仕組みにより実施されている場合については、その対策をもって代替しても構わない。

- **基本対策事項 3.2.1⑵-1「個別の対策」について**

個別の対策については、「(解説) 遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について」に示した例（対策の基準となっていない場合）のほか、以下に示す例を参考に決定するとよい。

- 機関等の施設内の案内板等において、サーバ室等の所在の表示を禁止する。
- 外部から室内が見えるような場所にある会議室において、要機密情報の取扱い時はブラインドを閉じる。
- 外部の者が周辺の会議室等へ出入りする時間帯には、執務室の扉を施錠する又は開放しない。
- 低階層の窓際等における無線 LAN の傍受対策を行う。
- ワイヤレスマイクの電波が室外にも到達するような会議室において、要機密情報の取扱い時はワイヤレスマイクの使用を禁止する。
- ディスプレイケーブル等から生ずる電磁波から情報が漏えいするおそれがある場合には電磁波軽減フィルタを取り付けるなどの対策(テンペスト対策)を行う。
- 飲食物をこぼした際に情報システムの運用上の障害が発生するような場所での飲食を禁止する。
- 情報システムに関係する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行う。
- クラス３の区域の中でもより厳重な管理が必要な区域において、機器の持込み、利用、持ち出しについて制限を設ける。
- 会議室において、重要な情報を取り扱う会議が開催される時間帯には機器の持込み、利用について制限を設ける。

機器の持込み、利用、持ち出しの制限について詳細を以下に示す。

- 「機器の持込み」とは、職員等が、執務室に業務に関係しない機器を持ち込むことや情報システムが設置される区域に当該情報システムに関係しない機器を持ち込むことを指す。「機器」には、モバイル端末、デジタルカメラ等の撮影機器、IC レコーダー等の録音機器、USB メモリ等の外部電磁的記録媒体等が含まれる。また、私物のスマートフォン等の機関等支給以外の機器も含まれる。以下に示すように、利用のみを禁止する対策もあるが、例えば、持ち込まれたスマートフォンが不正プログラムに感染していて、持ち込んだ者の意図に反して撮影や録音をされるという脅威も存在するため、持ち込ませないという対策も考えられる。
- 「機器の利用」とは、職員等が、持ち込んだ機器を利用することを指す。「利用」には、モバイル端末の起動や、デジタルカメラ等による撮影、IC レコーダー等による録音等が含まれる。管理する区域で取り扱う情報の機密性の高さに応じて、利用の制限を設けるか決めるとよい。スマートフォン等の通常電源をオンに

している機器であれば、立ち入る際に電源をオフにさせるという対策も有効である。

- 「機器の持ち出し」とは、情報システムが設置される区域から当該情報システムに関係する者が、当該情報システムに関係するサーバ装置、端末、外部電磁的記録媒体等を持ち出すことを指す。情報セキュリティインシデント発生時に追跡等できるように、機器の持ち出し時には、持ち出しの記録を取ることが考えられる。記録の内容としては、持ち出しを行う者の氏名及び所属、日時、機器名、事由等が挙げられる。

遵守事項

(3) 要管理対策区域における対策の実施

(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。職員等が実施すべき対策については、**職員等が認識できる措置を講ずる**こと。

(b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために**物理的な対策**を講ずること。

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

【 基本対策事項 】

＜3.2.1(3)(a)関連＞

3.2.1(3)-1 区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する職員等に周知すること。

a) 扉の施錠及び開閉に関する利用手順

b) 一時的に立ち入る者が許可された者であることを確認するための手順

c) 一時的に立ち入る者を監視するための手順

（解説）

- **遵守事項 3.2.1(3)(a)「職員等が認識できる措置を講ずる」について**

当該区域のクラスや当該クラスにおいて職員等が実施すべき対策を周知することが考えられる。扉の施錠や一時的に立ち入る者が許可された者であることの確認等の職員等に実施させる事項については、利用手順を定めて周知するとよい。

なお、関係者限りで利用する区域については、関係者のみに周知することでも構わない。

- **遵守事項 3.2.1(3)(b)「物理的な対策」について**

地震、火災、停電等の災害から情報システムを保護するための対策を指す。

具体的な対策として、例えば、サーバラックの利用のほか、以下の設備等の設置が挙げられる。

- ハロゲン化物消火設備
- 無停電電源装置
- 自家発電装置
- 空調設備
- 耐震又は免震設備

これらの対策については、必ずしも区域情報セキュリティ責任者単独で実施できるものではないが、例えば、情報システムに関係する対策であれば情報システムセキュリティ責任者、施設管理に関係する対策であれば施設管理を行う部門の関係者と調整す

ることが求められる。

また、情報システムへの対策として、作業する者が災害によりサーバ装置等に近づくことができない場合に、作業する者の安全性を確保した上で遠隔地からサーバ装置等の電源を遮断できるようにする機能を設けておくことも考えられる。

- **遵守事項 3.2.1(3)(c)「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」について**

  職員等は、自身が所属する機関等が管理する区域を利用する場合は、自機関等が定めた対策に従って利用することが求められる。一方、他の機関等が管理する区域を利用する場合には、他の機関等が定めた対策に従って利用する必要がある。

第4部 外部委託

4.1 外部委託

4.1.1 外部委託

目的・趣旨

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

外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

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

＜外部委託の例＞

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

遵守事項

(1) 外部委託に係る規定の整備

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

(ア) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本款において「**委託判断基準**」という。）

(イ) **委託先の選定基準**

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(1)(a)(ア)「委託判断基準」について**

委託先や第三者による許可されていない情報及び情報システムへのアクセス等が行われないように、委託先におけるそれらの取扱いに関する機関等の基準を規定することを求めている。規定すべき内容としては、例えば以下の事項が考えられる。

- 外部委託を許可（又は禁止）する業務又は情報システムの範囲
- 外部委託を許可（又は禁止）する業務又は情報システムの具体的例示（公開ウェブサーバは外部委託可等）
- 格付及び取扱制限その他取り扱う情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（機密性３情報は要管理対策区域外での取扱いを禁止するなど）

特に、委託業務において取り扱われる情報が海外のデータセンターに存在する場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスが行われる可能性があることに注意が必要である。機関等における「行政機関の保有する個人情報の保護に関する法律」（平成 15 年法律第 58 号）が規定する保有個人情報、「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号）が規定する保有個人情報及び「個人情報の保護に関する法律」（平成 15 年法律第 57 号）が規定する個人データについては、国内法令のみが適用される場所に制限する必要があると考えられるため、当該個人情報を取り扱う委託業務においては、保存された情報等に対して国内法令のみが適用されること等を外部委託の際の判断条件としておくべきである。

- **遵守事項 4.1.1(1)(a)(イ)「委託先の選定基準」について**

統括情報セキュリティ責任者は、委託先の選定基準の整備に当たって、当該委託先が、事業の継続性を有し存続する可能性が高く、機関等の対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。

選定基準としては、委託先が対策基準を遵守し得る者であること、対策基準と同等の情報セキュリティ管理体制を整備していること、対策基準と同等の情報セキュリティ対策の教育を委託先の事業従事者に対して実施していること等が挙げられる。

また、機関等の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を機関等内で統一的に整備することが重要である。

委託先の選定基準策定に当たって、委託先の情報セキュリティ水準の評価方法を整備する際、例えば、ISO/IEC 27001 等の国際規格とそれに基づく認証制度の活用、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用も考えられる。その場合、委託先の情報セキュリティ水準の認証に関わる認定・認証機関について、これら機関がマネジメントシステム認証の信頼性向上を目的とした取組である「MS 認証信頼性向上イニシアティブ」に参画し、不祥事への対応や透明性確保に係る取組を実施していることを確認することも考えられる。

なお、委託先の選定基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施時に反映することが必要である。

遵守事項

(2) 外部委託に係る契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って外部委託を実施すること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを**委託先の選定条件とし、仕様内容にも含める**こと。

(ア) **委託先に提供する情報の委託先における目的外利用の禁止**

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

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

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

(オ) **情報セキュリティインシデントへの対処方法**

(カ) **情報セキュリティ対策その他の契約の履行状況の確認方法**

(キ) **情報セキュリティ対策の履行が不十分な場合の対処方法**

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において**取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること**。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(b)(c)の措置の実施を委託先に担保させるとともに、**再委託先**の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、仕様内容に含めること。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。

【 基本対策事項 】

＜4.1.1(2)(b)関連＞

4.1.1(2)-1 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、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。

a) 当該委託業務に携わる者の特定

b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

4.1.1(2)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む**情報の取扱手順**について委託先と合意し、定められた手順により情報を取り扱うこと。

（解説）

- **遵守事項 4.1.1(2)(b)「委託先の選定条件とし、仕様内容にも含める」について**

一般競争入札の中でも総合評価落札方式で行う場合は、本項各号について、評価の際に入札者に対し提出を求めるなど、選定条件を満たしているかの確認をすること。また、事前に評価を行えない最低価格落札方式等で行う場合であっても、仕様書に対する履行能力証明書等を提出させるなどにより、 本項各号について契約時までに提出することを確約させること。

なお、委託事業の内容によっては、一部の条件が設定不可能な場合や意味をなさない場合も考えられるため、そのような場合には、除外することもやむを得ない。

また、国の安全に関する重要な情報を委託先に取り扱わせることを内容とする外部委託契約については、「調達における情報セキュリティ要件の記載について」（平成 24 年 1 月 24 日、内閣官房副長官から各省庁大臣官房長等あて）に基づく情報セキュリティ要件を当該契約に含めることも考えられる。

- **遵守事項 4.1.1(2)(b)(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」について**

委託先に提供する情報は、当該委託業務を遂行させるために提供するのであって、業務の遂行以外の目的で情報を利用させてはならない。

目的外利用に当たる場合としては、例えば、委託先が当該委託業務で提供を受けた機関等が利用するソフトウェアの情報を保有し、今後の営業活動で利用するなどが考えられる。

また、「情報セキュリティ対策に関する官民連携の在り方について」（平成 24 年 1 月 19 日 情報セキュリティ対策推進会議 官民連携の強化のための分科会）においては、「国の安全に関する重要な情報を国以外の者に扱わせることを内容とする契約を行う際には、契約方式にかかわらず、契約に係る業務の実施のために国が提供する国の安全に関する重要な情報その他当該業務の実施において知り得た国の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持させ、また当該業務の目的以外に利用させない」との旨が記載されている。

- **遵守事項 4.1.1(2)(b)(ウ)「機関等の意図せざる変更が加えられないための管理体制」について**

情報システムの開発等の外部委託において、「機関等の意図せざる変更が加えられないための管理体制」が確保されることを求めている。

具体的に仕様書等に記載する事項としては、例えば以下が考えられる。

  - 情報システムの開発工程において、機関等の意図しない変更が行われないこと

を保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

- 情報システムに機関等の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、機関等と委託先が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

- **遵守事項 4.1.1(2)(b)(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」について**

遵守事項 4.1.1(2)(b)(ウ)における管理体制等を確認する際の参照情報として用いるため、提供を求める規定である。

- **遵守事項 4.1.1(2)(b)(エ)「委託事業の実施場所」について**

データセンター等のスペースを借用して情報システムを設置する場合等では、要安定情報を取り扱う情報システムにおいて、自然災害その他による影響を考慮し、データセンターの立地条件をあらかじめ考慮しておく必要がある。

また、委託業務において使用する情報システムが民間事業者等の機関等外のデータセンターに設置される場合においては、「（解説）遵守事項 4.1.1(1)(b)(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」について」を参照のこと。

- **遵守事項 4.1.1(2)(b)(オ)「情報セキュリティインシデントへの対処方法」について**

委託先において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、契約時にあらかじめ委託先と合意しておくとよい。対処方法について合意していないと、インシデントが発生しているにもかかわらず委託先と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に合意しておくことが重要である。

対処方法には、例えば、復旧を優先する場合は委託業務を一時的に停止するための手順を規定し、業務継続を優先する場合は、委託事業を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る委託先と機関等間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

- **遵守事項 4.1.1(2)(b)(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」について**

委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであり、また、履行が不十分である場合には、速やかに適切な対処をすべきである。

情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。情報セキュリティ監査の内容には、請け負わせる業務のうち監査の対象とする範囲、実施者（機関等が指定する第三者、委託先が選定する第三者、機関等又は委託先において当該業務を行う部門とは独立した部門）、実施方法（情

報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先の情報セキュリティポリシーとの整合性等を委託先が判断するために必要と考えられる事項を含める。

情報セキュリティ監査により履行状況を確認する場合は、4.1.1(2)(c)に示す情報セキュリティ監査の受入れを仕様書に明記するとよい。

なお、契約内容の中で委託先における情報セキュリティ対策以外の内容についても、機関等の情報セキュリティに影響を及ぼす内容であると考えられる場合は、その履行状況についても確認することが求められる。情報セキュリティ対策以外の内容としては、例えば、委託先の資本関係、国籍に関する情報等についての契約後の変化などが考えられる。

- **遵守事項 4.1.1(2)(b)(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」について**

情報セキュリティ対策の履行が不十分である場合の対処方法としては、例えば、委託先と改善について協議を行い、合意した改善策を実施させること等が考えられる。また、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自身が契約を行わない場合には、本条に係る取決めについて、契約する者に対して依頼する必要がある。

- **遵守事項 4.1.1(2)(c)「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」について**

要保護情報を委託先にて取り扱う場合には、必要時に情報セキュリティ対策の履行状況の報告を求めるものである。また、委託先への立入検査又は情報セキュリティに関する監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む委託先と合意した事項について、契約に含めるなどにより明らかとしておくことが必要である。

また、要安定情報を取り扱う場合には、サービスレベルの保証について委託先と契約を取り交わすことを検討する必要がある。サービスレベルに関しては、セキュリティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、委託先に保証させることが重要である。

- **遵守事項 4.1.1(2)(d)「再委託先」について**

「再委託先」には、再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む。

- **基本対策事項 4.1.1(2)-2「情報の取扱手順」について**

格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、委託先においても機関等の対策基準に定める内容と同等の取扱いが行われるよう、あらかじめ委託先と合意しておくことが重要である。また、委託先に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、委託先における情報の取扱状況を適宜把握することも重要である。

なお、委託先において、約款による外部サービス、ソーシャルメディアサービス、クラウドサービス等を用いて委託業務を遂行することが考えられる場合は、統一基準

4.1.2「約款による外部サービスの利用」、4.1.3「ソーシャルメディアサービスによる情報発信」、4.1.4「クラウドサービスの利用」の規定を委託先においても遵守させるよう仕様書等に規定し、委託先とあらかじめ合意しておくことが望ましい。

遵守事項

(3) 外部委託における対策の実施

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における**情報セキュリティ対策の履行状況を確認する**こと。

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

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた**情報が確実に返却、又は抹消されたことを確認する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(3)(a)「情報セキュリティ対策の履行状況を確認する」について**

  委託先における情報セキュリティ対策の履行状況の確認に際し、情報セキュリティ監査を利用することとした場合には、契約に基づいた監査の範囲及び実施方法に従い、機関等自らが情報セキュリティ監査を行う以外に、第三者又は委託先に情報セキュリティ監査を行わせることが考えられる。

- **遵守事項 4.1.1(3)(c)「情報が確実に返却、又は抹消されたことを確認する」について**

  当該遵守事項を職員等に求めるに当たり、委託先ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。情報が完全に抹消されたことを確認することが困難な場合は、確認書を委託先に提出させるなどの方法も考慮する必要がある。

  情報の抹消については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」及び「（解説）遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について」を参照し、確認手段を定めるとよい。

遵守事項

(4) 外部委託における情報の取扱い

(a) 職員等は、委託先への情報の提供等において、以下の事項を遵守すること。

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

(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

(ウ) 委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(4)(a)「委託先への情報の提供」について**

  委託契約開始から終了に至るまでに行う委託先への情報の提供に伴う要機密情報の漏えい等を防止するためには、委託業務に係る職員等それぞれが委託先との情報の授受時に情報セキュリティを確保することが重要である。

  委託先への情報の提供に関する解説については、「（解説）遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について」を参照のこと。

4.1.2 約款による外部サービスの利用

目的・趣旨

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

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

遵守事項

(1) 約款による外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む**約款による外部サービス**の利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ア) **約款による外部サービスを利用してよい業務の範囲**

(イ) **業務に利用できる約款による外部サービス**

(ウ) 利用手続及び運用手順

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

【 基本対策事項 】

＜4.1.2(1)(a)(ウ)関連＞

4.1.2(1)-1 統括情報セキュリティ責任者は、機関等において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。

a) 利用申請の**許可権限者**

b) 利用申請時の申請内容

- 利用する組織名
- 利用するサービス
- 利用目的（業務内容）
- 利用期間
- **利用責任者（利用アカウントの責任者）**

c) サービス利用中の安全管理に係る運用手順

- サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
- 情報の滅失、破壊等に備えたバックアップの取得
- 利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有

無の確認等）
d）情報セキュリティインシデント発生時の連絡体制

（解説）

- **遵守事項 4.1.2(1)(a)「約款による外部サービス」について**

「約款による外部サービス」としては、民間事業者等がインターネット上で不特定多数の利用者（主に一般消費者）に対して提供する電子メール、ファイルストレージ、グループウェア等のサービスが代表的であり、有料、無料に関わらず、画一的な約款や利用規約等への同意、簡易なアカウントの登録（登録が不要な場合もある）等により利用可能なサービスは、約款による外部サービスとなる。その他にインターネットの検索サービスや辞書サービス等も約款による外部サービスに該当する。

また、職員等自身が取得した電子メールアカウント等を業務で利用する場合についても約款による外部サービスの利用に当たる。

このようなサービスは、利用の際の情報管理について保証がないことが一般的であり、不用意な利用によって機関等の情報が意図せず漏えいすることが懸念されることから、要機密情報が取り扱われないよう、適切に管理することが重要である。

なお、インターネット回線接続サービス、音声による電話サービス、郵便、運送サービス等は「約款による外部サービス」の適用範囲外である。

- **遵守事項 4.1.2(1)(a)(ア)「約款による外部サービスを利用してよい業務の範囲」について**

取り扱う情報の格付及び取扱制限に応じて、情報セキュリティの確保の観点から、約款による外部サービスを利用してよい業務の範囲を定めることを求めている。

約款による外部サービス利用に当たって考慮すべきリスクには、以下のようなものがある。統括情報セキュリティ責任者は、これらのリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

- サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
- 情報が意に反して公開されてしまった場合や、情報が改ざんされた場合でも、サービス提供者は一切の責任を負わない。
- サービス提供者が海外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。
- 突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。

- 保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
- 約款及び利用規約の内容が、サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。
- 情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
- 利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

なお、本款において、約款による外部サービスで要機密情報を取り扱うことを禁止しているが、例外として、国外等の機関から約款による外部サービスを用いて情報共有等を求められる場合等、やむを得ず要機密情報を約款による外部サービスにおいて取り扱う場合においても、上記リスクを踏まえ、適切な対策を講じた上で利用することが求められる。例えば、海外のデータセンター等に情報を保存し、現地の法令等が適用されることで情報の漏えいにつながるリスクについては、国内にサーバ装置が設置される事業者に委託し、国内法令のみが適用されることを事前に確認できれば当該リスクを低減することが可能と判断できる。このように、サービス提供者のサービス提供形態により低減又は回避可能なリスクもあることから、約款、利用規約等の詳細を確認するなどして例外措置の可否を判断することが重要である。

- **遵守事項 4.1.2(1)(a)(イ)「業務に利用できる約款による外部サービス」について**

約款による外部サービスのうち利用可能なサービスについて、以下を例にサービスを特定し、機関等の基準として定めることが考えられる。

なお、以下の例は要機密情報を取り扱わないことが前提であることに注意すること。

- サービスの約款や利用規約の内容
- サービス事業者の情報セキュリティポリシー及びプライバシーポリシー
- 提供サービスにおけるセキュリティ設定及びプライバシー設定の方法（初期設定を含む。）
- 情報セキュリティインシデント発生時における個別対応の可否（運用実績等を勘案するとよい。）

また、要機密情報を取り扱わない場合であっても、例えば検索サービスの利用においては、インターネット上に職員等の身分を明らかにして検索ワード等の情報を提供する行為に等しく、膨大な検索ワード等の情報から、機関等の関心事項等が分析されるおそれがあることに留意しなければならない。検索サービスを業務に利用する組織において特にそのようなリスクが懸念される場合は、上記のサービス提供条件の確認に加えて、インターネット上で利用端末や通信元を匿名化する対策を導入し、システム部門による適切な管理の下で利用すること等を考慮するとよい。

- **遵守事項 4.1.2(1)(b)「責任者」・基本対策事項 4.1.2(1)-1 a)「許可権限者」について**

本条(b)に定める「責任者」と本基本対策事項 a)に定める「許可権限者」は同一であり、約款による外部サービスを利用する場合において、利用可否を判断する責任者とな

る。当該責任者は、利用可能なサービスごとに設置され、利用部門からの申請を受け付けて、申請内容に従い利用を許可することになる。一人の責任者が複数のサービスを所管してもよい。また、当該責任者は、所管する約款による外部サービスについて、約款及び利用規約の変更の有無等について定期的に状況把握することが求められる。

また、当該責任者には、所管する約款による外部サービスに関する技術的な知見を有し、約款による外部サービスを利用する際に考慮すべきリスクを十分理解し、個々の利用申請に対して適切に判断することが可能な者を充てることが必要である。

- **基本対策事項 4.1.2(1)-1 b)「利用責任者（利用アカウントの責任者）」について**

本条(b)及び本基本対策事項 a)において定めている責任者（許可権限者）とは別に、約款による外部サービスを利用する際に利用アカウントごとの責任者を利用責任者として定めることを求めている。利用部門において利用責任者を定めることになるが、課室情報セキュリティ責任者、情報システムセキュリティ責任者、又は約款による外部サービスの許可権限者が利用責任者を兼ねるなど、組織の規模や特性に応じて柔軟に定めてよい。

【参考 4.1.2-1】約款による外部サービスの利用申請フローの例

約款による外部サービスの申請手続及び申請許可権限者、運用管理者等の配置例を図 4.1.2-1 に示す。

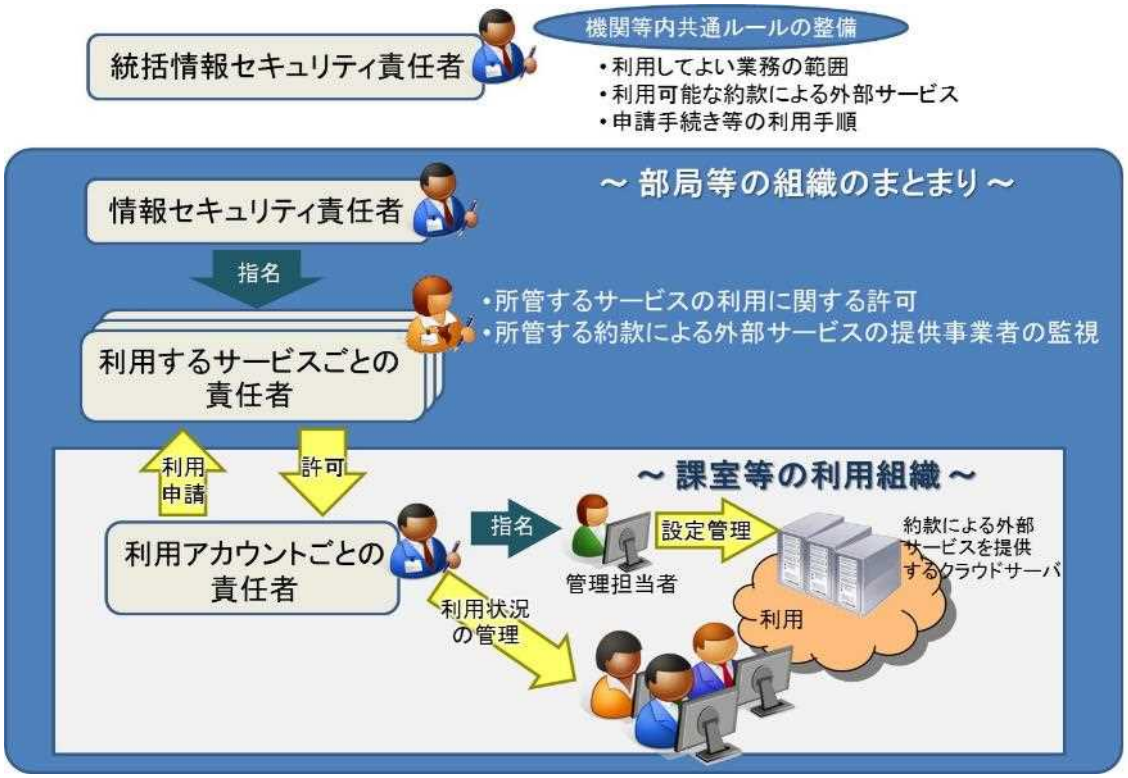


図 4.1.2-1　約款による外部サービスの申請手続及び責任者の役割例

遵守事項

(2) 約款による外部サービスの利用における対策の実施

(a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.2(2)(a)「利用に当たってのリスク」について**

個々の業務の遂行において、約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、以下のリスクや課題への対策を明確化した上で、適切に利用の必要性を判断することが必要である。

なお、以下に掲げるリスクの例は、要機密情報を約款による外部サービスにて取り扱わないことを前提としたものであることに注意すること。

- サーバ装置の故障やサービス提供事業者の運用手順誤り等により、サーバ装置上の情報が滅失して復元不可能となるおそれがある。
- サーバ装置上の要保全情報が第三者等により改ざんされ、復元が困難となるおそれがある。
- サービスが突然停止されるおそれがある。
- 約款や利用規約等が予告なく一方的に変更され、セキュリティ設定が変更されるおそれがある。
- 情報の取扱いが保証されず、一旦記録された情報を確実に消去することができないおそれがある。

4.1.3 ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。機関等においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、民間事業者等により提供されているソーシャルメディアサービスは、.go.jp で終わるドメイン名（以下「政府ドメイン名」という。）を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、機関等のアカウントを乗っ取られた場合や、利用しているソーシャルメディアサービスが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民等に提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

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

なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、 4.1.2「約款による外部サービスの利用」の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、4.1.1「外部委託」及び 4.1.2「約款による外部サービスの利用」を適用するのではなく、本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) ソーシャルメディアサービスによる情報発信時の対策

(a) 統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する**運用手順等を定める**こと。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ｱ) 機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

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

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

(c) 職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる

場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

【 基本対策事項 】

＜4.1.3(1)(a)関連＞

4.1.3(1)-1 統括情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている機関等の当該ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

b) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

4.1.3(1)-2 統括情報セキュリティ責任者は、機関等のアカウントによる情報発信が実際の機関等のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

a) 機関等からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、機関等が運用していることを利用者に明示すること。

b) 機関等からの情報発信であることを明らかにするために、機関等が政府ドメイン名を用いて管理している当該ウェブサイト内（政府ドメイン名を登録する資格を持たない機関等においては、機関等の当該ウェブサイト内）において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている機関等の当該ウェブサイト上のページの URL を記載すること。

d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

4.1.3(1)-3 統括情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

a) パスワードを適切に管理すること。具体的には、ログインパスワードには十分

な長さと複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

c) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

4.1.3(1)-4 統括情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT に報告すること。報告を受けた CSIRT は遵守事項 2.2.4(2)に従い、内閣官房内閣サイバーセキュリティセンターへの連絡（独立行政法人及び指定法人においては所管する国の行政機関を経由）を含む適切な対処を行うこと。

（解説）

- **遵守事項 4.1.3(1)(a)「運用手順等を定める」について**

運用手順等を定めるに当たっては、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準を低下させることがないよう留意する必要がある。機関等のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するウェブサイト等へのリンクを掲載することは、当該の投稿やウェブサイト等の内容を信頼性のあるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やウェブサイト等の内容が変更される可能性があることを考慮した上で、慎重に行う必要がある。

- **遵守事項 4.1.3(1)(b)「情報発信」について**

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまうため、完全に削除することは不可能となる。このため、当該情報が公開可能な情報であるか否かについて、情報発信する前に十分に確認する必要がある。

- **遵守事項 4.1.3(1)(b)「責任者」について**

  遵守事項 4.1.2(1)(b)にて定めている責任者と同等であり、ソーシャルメディアサービスの利用申請を受け付けて、利用を許可する許可権限者となる。申請手順や利用責任者の設置等の運用方法については、4.1.2「約款による外部サービスの利用」を参照すること。

- **基本対策事項 4.1.3(1)-3 a)「パスワードを適切に管理する」について**

  パスワードの管理については、遵守事項 8.1.1(5)(d)も参照のこと。

- **基本対策事項 4.1.3(1)-3 a)「パスワードを知る担当者を限定」について**

  ソーシャルメディアのアカウントは、複数の担当者で利用することが一般的であり、また、担当者の異動に伴いアカウントの利用者が交代することが想定される。したがって、ログインパスワードの管理に当たっては、担当者の交代があった時点で直ちにパスワードを変更し、権限のない者がパスワードを知る状態が生じないようにすることが求められる。

4.1.4 クラウドサービスの利用

目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

クラウドサービスを利用する際、機関等がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、機関等による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

遵守事項

(1) クラウドサービスの利用における対策

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

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

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

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

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

【 基本対策事項 】

＜4.1.4(1)(c)関連＞

4.1.4(1)-1 情報システムセキュリティ責任者は、クラウドサービスを利用するに当たり、

サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含めること。

a) 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件
b) 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

＜4.1.4(1)(d)関連＞

4.1.4(1)-2 情報システムセキュリティ責任者は、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こと。また、対策を実現するために、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認すること。

a) クラウドサービスに係るアクセスログ等の証跡の保存及び提供
b) インターネット回線とクラウド基盤の接続点の通信の監視
c) クラウドサービスの委託先による情報の管理・保管の実施内容の確認
d) クラウドサービス上の脆弱性対策の実施内容の確認
e) クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標
f) クラウドサービス上で取り扱う情報の暗号化
g) 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄
h) 利用者が求める情報開示請求に対する開示項目や範囲の明記

（解説）

- **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**

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、その情報の適正な取扱いの確認が容易ではなくなる。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。

- クラウドサービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、クラウドサービス事業者の運用詳細は公開されないために利用者にブラックボックスとなっている部分があり、利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。
- オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス事業者との間の責任分界点やサービスレベルの合意が容易ではない。
- クラウドサービス事業者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、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。

- クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。
- サーバ装置等機器の整備環境がクラウドサービス事業者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

なお、情報セキュリティ確保のためにクラウド利用者自らが行うべきことと、クラウドサービス事業者に対して求めるべきこと等をまとめたガイドラインについては、以下の取組を参考にするとよい。

参考：総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」（平成 26 年 4 月）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html）

参考：経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」、「クラウドセキュリティガイドライン活用ガイドブック」（平成 26 年 3 月 14 日）
（http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html）

参考：公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」（平成 26 年 11 月 14 日）
（https://www.fisc.or.jp/isolate/?id=759&c=topics&sid=190）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 4.1.4(1)(b)「国内法以外の法令が適用されるリスク」について**

国内法以外の法令が適用されるリスクとして、データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取り決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が機関等のデータを含んだまま没収されるなどが考えられる。

- **遵守事項 4.1.4(1)(b)「委託事業の実施場所」について**

バックアップデータ、サーバ装置内のデータ等、機関等の情報が存在し得る場所全てを委託事業の実施場所として考慮することが必要である。

- **遵守事項 4.1.4(1)(d)「クラウドサービスの特性」について**

クラウドサービスを利用した情報システムは、従来のオンプレミスによる情報システムと比べ、主に以下の特性がある。

- クラウドサービス事業者の用意するコンピューティング資源を多くのクラウド利用者で共有し、その上に各クラウド利用者が利用する情報システムが構築される。そのため、機関等が情報システムを構築する際のセキュリティ対策のみで

なく、クラウドサービス事業者やコンピューティング資源を共有している他のクラウド利用者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が発生し、その影響を受ける可能性がある。

- クラウド利用者は処理能力やストレージ等のコンピューティング資源を、利用者の操作で追加又は削減することができる。しかし、クラウドサービス事業者の用意する資源の不足等が発生した場合に即座に資源の追加ができず、可用性を損なう可能性がある。
- クラウドサービス事業者はコンピューティング資源を分散して配置することが可能であり、海外に配置されている可能性がある。

- **遵守事項 4.1.4(1)(e)「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、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」について**

クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。その場合、監査や認証等によって保証される対象範囲がクラウドサービス事業者の全部又は一部の場合があるので、機関等が委託するクラウドサービスが当該対象範囲に含まれていることを確認する必要がある。また、監査の場合には、監査項目の網羅性に留意して、重要な監査項目が除かれていないか、監査意見に除外事項（内部統制の不備）が含まれていないかなどを確認する必要がある。さらに、その監査や認証等によっては、クラウドサービス事業者の経営の安定性やサプライチェーン・リスク等は上記の評価に含まれていないことが考えられるため、これらのリスクについては機関等において評価する必要がある。

なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証の国際規格があり、そこでは「クラウドサービス事業者が選択する監査は、一般的には、十分な透明性をもった当該事業者の運用をレビューしたいとする利用者の関心を満たすに足りる手段とする」ことが要求されており、これらの国際規格をクラウドサービス事業者選定の際の要件として活用することも考えられる。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やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）を活用することも考えられる。特に、SOC2・SOC3 は、米国公認会計士協会が開発した「Trust サービス原則と基準」で定義された「セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシー」の５つの原則を適用したものであるため、クラウドサービス事業者及びサービスに対する評価の際の参考となり得る。

また、SOC2・SOC3 については、日本公認会計士協会の IT 委員会の実務指針により国内でも同様の保証報告書が制度化されている。ただし、SOC2・SOC3 及び実務指針第 7 号においては、この５つの原則の一部のみを選択して実施することができるため、当該監査で選択した原則に「セキュリティ」が含まれていることを保証報告書により確かめる必要がある。

参考：国際規格
「ISO/IEC 27017（安全なクラウドサービス利用のための分野別 ISMS 規格）」

参考：日本セキュリティ監査協会
「クラウド情報セキュリティ管理基準」
（http://jcispa.jasa.jp/documents/）
「クラウド情報セキュリティ監査制度規程」
（http://jcispa.jasa.jp/cloud_security/jcispa_regulation/）

参考：日本公認会計士協会「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書（日本公認会計士協会 IT 委員会実務指針第 7 号）」
（https://jicpa.or.jp/specialized_field/45_8.html）

参考：米国公認会計士協会「Service Organization Control (SOC) Reports」
（https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 4.1.4(1)-1「サービスの中断や終了時に際し、円滑に業務を移行するための対策」について**

クラウドサービス事業者が何らかの理由で、クラウドサービスの継続的な提供ができなくなった場合に、他のクラウドサービス事業者に対し、情報の移行を円滑に実施することにより、利用者側での業務を継続できるようにすることが求められる。

そのため、移植性又は相互運用性を確保する観点から、可能な限り、標準化されたデータ形式やインタフェースを使用することが望ましい。

- **基本対策事項 4.1.4(1)-2 a)「アクセスログ等の証跡の保存」について**

クラウドサービス上におけるアクセスログ等の証跡に係る保存期間については、オンプレミスと同様に情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する（「（解説）遵守事項 6.1.4(1)(b)「保存期間」について」を参照のこと。）。

- **基本対策事項 4.1.4(1)-2 c)「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**

  情報管理上の問題として、仮に情報がクラウド上にあったとしても、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ため、利用者はクラウドサービス事業者による情報の管理・保管方法について事前に把握する必要がある。

  また、クラウドサービス事業者が外部委託先に情報の管理・保管を委託した場合、当該情報が利用者の意図しない場面で二次利用されることも懸念されるため、外部委託先における情報セキュリティ水準や情報の取扱方法に関してクラウドサービス事業者に確認の上、合意しておく必要がある。

- **基本対策事項 4.1.4(1)-2 d)「脆弱性対策」について**

  例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドに対するリスクであり、対策を講ずる必要がある。このような脆弱性を発見する方法として、脆弱性検査ツールを用いた手法やペネトレーションテスト等が挙げられる。

- **基本対策事項 4.1.4(1)-2 h)「情報開示請求に対する開示項目や範囲」について**

  クラウドサービスに関し、クラウドサービス事業者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に機関等とクラウドサービス事業者が協議の上、クラウドサービス事業者が提供する内容の項目や範囲を契約において明記することが必要である。また対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得することが求められる。

第5部 情報システムのライフサイクル

5.1 情報システムに係る文書等の整備

5.1.1 情報システムに係る台帳等の整備

目的・趣旨

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

遵守事項

(1) 情報システム台帳の整備

(a) 統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

(b) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告すること。

【 基本対策事項 】

＜5.1.1(1)(a)関連＞

5.1.1(1)-1 統括情報セキュリティ責任者は、以下の内容を含む台帳を整備すること。

a) 情報システム名
b) 管理課室
c) 当該情報システムセキュリティ責任者の氏名及び連絡先
d) システム構成
e) 接続する機関等外通信回線の種別
f) 取り扱う情報の格付及び取扱制限に関する事項
g) 当該情報システムの設計・開発、運用・保守に関する事項

また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。

a) 情報処理サービス名
b) 契約事業者
c) 契約期間
d) 情報処理サービスの概要
e) ドメイン名

f) 取り扱う情報の格付及び取扱制限に関する事項

＜5.1.1(1)(b)関連＞

5.1.1(1)-2 情報システムセキュリティ責任者は、政府情報システム管理データベースの登録対象となるシステムについては、当該データベースに必要な情報を記録し、適時最新の情報に更新すること。

（解説）

- **遵守事項 5.1.1(1)(a)「情報システム台帳に整備する」について**

  統括情報セキュリティ責任者は、情報システム台帳の整備状況について報告を受け、把握しておくことが重要である。

- **遵守事項 5.1.1(1)(b)「情報システムを新規に構築し、又は更改する際には」について**

  台帳の整備内容の網羅性維持のため、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た際又は更改した際には、速やかに台帳に記載の事項を報告する必要がある。

  なお、台帳を最新に保つため、台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、台帳を更新する必要があるが、その報告の方法や時期については、機関等ごとに定めることが望ましい。

- **基本対策事項 5.1.1(1)-1 d)「システム構成」について**

  当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、機関等としての情報セキュリティ対策を行うために一元的に把握する必要があると判断する事項を含める必要がある。

- **基本対策事項 5.1.1(1)-1 g)「設計・開発、運用・保守に関する事項」について**

  当該情報システムの設計・開発、運用・保守に関する事項の記載は、実施責任者又は実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。

- **基本対策事項 5.1.1(1)-1「民間事業者等が提供する情報処理サービスにより情報システムを構築する場合」について**

  機関等として独自の情報システムを構築せずに、クラウドサービス等の情報処理サービスを利用して情報システムを構築し運用する場合や電気通信事業者が提供する電気通信サービスを利用して情報処理業務を行う場合は、利用する情報処理サービス名や契約事業者等の事項を記載したサービス契約に係る書類を適切に管理しておくことが重要である。これらの書類を集約し、容易に参照できるようにすることをもって台帳整備に代えることができる。

  なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の台帳を整備することも考えられる。

- **基本対策事項 5.1.1(1)-2「政府情報システム管理データベースの登録対象となるシステム」について**

  国の行政機関においては、情報システム台帳の整備に当たって、政府機関の情報システムを統一的に管理する政府情報システム管理データベースにおいて管理することが求められる。当該データベースの管理対象となるシステムについては、データベースにおいて管理することをもって台帳整備に代えることができる。

遵守事項

(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**

【 基本対策事項 】

＜5.1.1(2)(a)(ア)関連＞

5.1.1(2)-1 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を構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。

a) サーバ装置及び端末を**管理する職員等**及び利用者を特定する情報

b) サーバ装置及び端末の**機種並びに利用しているソフトウェアの種類及びバージョン**

c) サーバ装置及び端末で利用する**ソフトウェアを動作させるために用いられる他のソフトウェア**であって、以下を含むものの種類及びバージョン

- 動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの
- フレームワーク等、ソフトウェアを実行するための実行環境となるもの
- プラグイン等、ソフトウェアの機能を拡張するもの
- 静的リンクライブラリ等、機関等がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの
- インストーラー作成ソフトウェア等、機関等がソフトウェアを開発する際に開発を支援するために使用するもの

d) サーバ装置及び端末の**仕様書又は設計書**

5.1.1(2)-2 情報システムセキュリティ責任者は、前項 b)及び c)の情報を収集するため、**自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェア**を導入するなどにより、これら情報を効率的に収集する手法を決定すること。

＜5.1.1(2)(a)(イ)関連＞

5.1.1(2)-3 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を構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。

a) 通信回線及び通信回線装置を**管理する職員等**を特定する情報

b) 通信回線装置の**機種並びに利用しているソフトウェアの種類及びバージョン**

c) 通信回線及び通信回線装置の**仕様書又は設計書**

d) 通信回線の構成

e) 通信回線装置におけるアクセス制御の設定
f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応
g) 通信回線の利用部門

＜5.1.1(2)(a)(ウ)関連＞

5.1.1(2)-4 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、情報システム構成要素ごとの<u>セキュリティ維持に関する以下を含む手順</u>を定めること。
a) サーバ装置及び端末のセキュリティの維持に関する手順
b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順
c) 通信回線及び通信回線装置のセキュリティの維持に関する手順

（解説）

- **遵守事項 5.1.1(2)(a)「情報システム関連文書を整備する」について**

当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、機関等としての情報セキュリティ対策を行うために一元的に把握する必要があると判断するものを含める必要がある。

文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は電磁的記録として整備してもよい。

また、所管する情報システムに変更があった場合、また、想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になるため、文書の見直しを定期的に行うことをあらかじめ定めておくとよい。

なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の情報システム関連文書を整備することも考えられる。

- **遵守事項 5.1.1(2)(a)(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」について**

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は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。

- 業務継続計画で定める当該情報システムを利用する業務の重要性
- 情報システムの運用等の外部委託の内容

また、手順に記載される内容として、例えば以下が想定される。

- 情報セキュリティインシデントの内容・影響度の大きさに応じた情報連絡先のリスト
- 情報システムを障害等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準
- 情報セキュリティインシデントに対する情報システムの構成要素ごとの対処に関する事項
- 不正プログラム対策ソフトウェアでは検知されない新種の不正プログラムに感

染した場合等に支援を受けるための外部の専門家の連絡先

なお、統括情報セキュリティ責任者が整備する対処手順(「(解説)遵守事項 2.2.4(1)(b)「対処手順」について」を参照のこと。)が、情報システムの事情に応じた内容で整備されているならば、情報システム別に整備しなくても構わない。

- **基本対策事項 5.1.1(2)-1 a)・基本対策事項 5.1.1(2)-3 a)「管理する職員等」について**

サーバ装置及び端末の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システムの構成要素の管理状況を確実に把握できるようにするとともに、障害等を防止する責任の所在を明確化するために必要な事項である。

- **基本対策事項 5.1.1(2)-1 b)・基本対策事項 5.1.1(2)-3 b)「機種並びに利用しているソフトウェアの種類及びバージョン」について**

サーバ装置及び端末、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアに脆弱性が存在することにより使用上のリスクが高まった場合に、速やかに脆弱性対策を行うなど、適切に対処するために必要な事項である。

- **基本対策事項 5.1.1(2)-1 c)「ソフトウェアを動作させるために用いられる他のソフトウェア」について**

一般に外部から入手するソフトウェアは、ソフトウェア開発元が脆弱性情報を提供する。一方、機関等が開発するソフトウェアについては、機関等自身が開発元として当該ソフトウェアの脆弱性情報を提供する立場となる。機関等は、当該ソフトウェアを国民等に提供する場合のみでなく、機関等自身が利用する場合においても情報セキュリティ対策を実施する必要があることから、いずれの場合においても当該ソフトウェアに組み込まれて使用されるライブラリ等のソフトウェアについても脆弱性情報を把握することが求められる。そのため、組み込まれているライブラリ等についても種類及びバージョンを機関等自身が把握する必要がある。なお、機関等がソフトウェアの開発を委託する場合においては、委託事業者から当該情報を漏れなく入手することが必要である。

また、システムで使用するソフトウェアには、プラグイン等の機能拡張用のソフトウェアにより機能を追加できるものがある。ただし、機能拡張用のソフトウェアは、元となるソフトウェアと開発元が異なる場合があり、機能拡張用のソフトウェアの脆弱性情報が、元となるソフトウェアの開発元から提供されない可能性がある。そのため、機能拡張用のソフトウェアについても個別に種類及びバージョンを把握しておく必要がある。

- **基本対策事項 5.1.1(2)-1 d)・基本対策事項 5.1.1(2)-3 c)「仕様書又は設計書」について**

情報システムに係る仕様書又は設計書は、情報セキュリティ対策の実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。

- **基本対策事項 5.1.1(2)-2「自動でソフトウェアの種類やバージョン等を管理する機能を**

有する IT 資産管理ソフトウェア」について

近年の IT の利活用拡大により、システムで使用しているソフトウェア等の種類も増加していることから、IT 資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有する IT 資産管理ソフトウェアを導入することが有用である。

- **基本対策事項 5.1.1⑵-4「セキュリティ維持に関する以下を含む手順」について**

情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理及びログ管理の設定・変更等の手順が挙げられる。

5.1.2 機器等の調達に係る規定の整備

目的・趣旨

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

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

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更**が加えられない管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜5.1.2(1)(a)関連＞

5.1.2(1)-1 統括情報セキュリティ責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。

a) 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、機関等と調達先が連携して**原因を調査・排除できる体制**を整備していること。

5.1.2(1)-2 統括情報セキュリティ責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、**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。

＜5.1.2(1)(b)関連＞

5.1.2(1)-3 統括情報セキュリティ責任者は、機器等の納入時の確認・検査手続には**以下を含む事項を確認できる手続**を定めること。

a) 調達時に指定したセキュリティ要件の実装状況

b) 機器等に不正プログラムが混入していないこと

（解説）

- **遵守事項 5.1.2(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的

に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 5.1.2(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、当該事項の適用要否を判断した上で整備することを求めている。

- **遵守事項 5.1.2(1)(a)「不正な変更」について**

ここでいう「不正な変更」とは、機器等の製造工程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことを意味している。

不正な変更が行われない管理がなされていることとは、例えば、機器等の製造工程における不正行為の有無について、定期的な監査を行っていること、機器等の製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われていること等が考えられる。その他、特に高い信頼性が求められる製品を調達する場合は、各製造工程の履歴が記録されているなどの厳格な管理されていることが考えられる。

- **基本対策事項 5.1.2(1)-1 a)「原因を調査・排除できる体制」について**

OEM（Original Equipment Manufacturer）によって提供される機器等についても、OEM 製品の製造者においても不正な変更が加えられないよう、OEM 製品の販売者が機器等のサプライチェーン全体について適切に管理していることも含めて、要件を定めることが考えられる。

- **基本対策事項 5.1.2(1)-2「ISO/IEC 15408 に基づく認証」について**

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。

ISO/IEC 15408 に基づく認証では、第三者によって、対抗する脅威に必要な機能が設計書に反映されていること、その機能が設計どおり実装されていること、開発現場や製造過程においてセキュリティが侵害される可能性が無いこと、利用マニュアル・ガイダンス等にセキュリティを保つための必要事項が明確に示されていること等が客観的に評価され、評価結果及び既知の情報から懸念される脆弱性についての評定及びテストが実施される。ただし、第三者によって評価・保証される範囲は、適合する Protection Profile（国際標準に基づくセキュリティ要件）や、評価保証レベル（EAL : Evaluation Assurance Level）によって異なるため、どの程度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。

- **基本対策事項 5.1.2(1)-3「以下を含む事項を確認できる手続」について**

  機器等の納入時の確認・検査手続の具体例として、以下の内容が考えられる。

  - 調達時に指定したセキュリティ要件（機器等に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェア等が最新の脆弱性に対応しているか否か等にも留意）に関する試験実施手順及び試験結果を納品時に報告させて確認
  - セキュリティ要件として調達時に指定した機能が正しく動作することを受入れテストにより確認
  - 内部監査等により不正な変更が加えられていないことを確認した結果を納品時に報告させて確認

5.2　情報システムのライフサイクルの各段階における対策

5.2.1　情報システムの企画・要件定義

目的・趣旨

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

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

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

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

また、情報システムの構築、運用・保守を外部委託する場合については、 4.1「外部委託」についても併せて遵守する必要がある。

遵守事項

(1)　実施体制の確保

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

(b)　情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機関等が定める運用管理規程等に応じた体制の確保を、最高情報セキュリティ責任者に求めること。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.1(1)(a)「最高情報セキュリティ責任者に求める」について**

  最高情報セキュリティ責任者に、セキュリティの維持が実施可能な体制（人員、機器、

予算等）の確保を求める事項である。

遵守事項

(2) 情報システムのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムを**インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する**ことの要否を判断した上で、以下の事項を含む**情報システムのセキュリティ要件**を策定すること。

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

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

(ウ) 情報システムに関連する脆弱性についての対策要件

(b) 情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、**接続するインターネット回線を定めた上で**、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

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

(d) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

【 基本対策事項 】

＜5.2.1(2)(a)関連＞

5.2.1(2)-1 情報システムセキュリティ責任者は、「**情報システムに係る政府調達におけるセキュリティ要件策定マニュアル**」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。

5.2.1(2)-2 情報システムセキュリティ責任者は、**開発する情報システムが運用される際に想定される脅威**の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。

＜5.2.1(2)(a)(ア)関連＞

5.2.1(2)-3 情報システムセキュリティ責任者は、開発する情報システムが対抗すべき脅

威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、**ST 確認**を受けること。

＜5.2.1(2)(a)(イ)関連＞

5.2.1(2)-4 情報システムセキュリティ責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。

a) 情報システム運用時に情報セキュリティ確保のために必要となる**管理機能**を仕様書等に明記すること。

b) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、**監視のために必要な機能**について、以下を例とする機能を仕様書等に明記すること。

- 機関等外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
- 不正プログラム感染や踏み台に利用されること等による機関等外への不正な通信を監視する機能
- 端末等の組織内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能
- 機関等内通信回線への端末の接続を監視する機能
- 端末への外部電磁的記録媒体の挿入を監視する機能
- サーバ装置等の機器の動作を監視する機能

c) 暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を仕様書等に明記すること。

＜5.2.1(2)(a)(ウ)関連＞

5.2.1(2)-5 情報システムセキュリティ責任者は、開発する情報システムに関連する**脆弱性への対策**が実施されるよう、以下を含む対策を仕様書等に明記すること。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

b) 開発時に情報システムに**脆弱性が混入されることを防ぐためのセキュリティ実装方針**。

c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する機関等への情報提供。

＜5.2.1(2)(c)関連＞

5.2.1(2)-6 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち、製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施す

ること。

a) 「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、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する**機器等の利用環境において対抗すべき脅威**を分析し、必要なセキュリティ要件を策定すること。

（解説）

- **遵守事項 5.2.1(2)(a)「インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する」について**

標的型攻撃による不正プログラム感染の脅威は避けられないものになっており、外部のネットワークと接続する情報システムは、不正プログラムの感染を前提とした対策を講ずることの重要度が、年々増加している。

外部ネットワークとの接続形態を含む情報システムの全体構成は、情報システムにおいて取り扱われる情報の格付や取扱制限、情報システムを利用する業務の形態等によって決定する必要があるが、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。また、分離した情報システムの USB ポート等の外部ネットワーク・システムとの接点についても適切に運用することが望ましい。

- **遵守事項 5.2.1(2)(a)「情報システムのセキュリティ要件」・基本対策事項 5.2.1(2)-1「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」について**

「情報システムのセキュリティ要件」には、ハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。

なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。

セキュリティ要件の策定には、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用するか又はそれと同等以上のセキュリティ水準となるよう検討を行い、その結果をシステム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。

情報システムのセキュリティ要件を検討する際には、仮想化技術の活用の有無を確認し、物理的に分割されたシステムに限らず、論理的に分割されたシステムであるかを考慮したセキュリティ要件を検討することも重要である。「論理的に分割されたシステ

ム」とは、一つの情報システムの筐体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。

また、外部の情報システムを利用する場合は、 4.1.1「外部委託」も参照の上、委託先との管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが生じないようにすることも重要である。

このように、情報システムの構築形態及び調達形態に応じてセキュリティ要件を定めることが求められる。

参考：内閣官房内閣サイバーセキュリティセンター「「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について」（平成 27 年 5 月 22 日）
（https://www.nisc.go.jp/active/general/sbd_sakutei.html）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 5.2.1(2)(a)(イ)「監視するデータが暗号化されている場合は、必要に応じて復号」について**

ウェブの常時暗号化（TLS（SSL）化）や電子メールサーバ間通信の暗号化（TLS（SSL）化）等といった通信の暗号化が社会的に進められ、その利用割合が上昇する中で、不正なプログラム等の脅威が暗号化された通信の中に含まれていると、当該通信の監視による脅威の検知が困難になる。また、機関等自身においても上記の暗号化を進めていけば、その傾向は更に大きくなる。このため、監視に際しては、監視対象のデータが暗号されているかどうかを把握し、対象とする脅威の監視可否に与える影響を考慮した上で復号の要否を判断し、必要と判断した場合にはその対策を講じなければならない。

- **遵守事項 5.2.1(2)(b)「接続するインターネット回線を定めた上で」について**

構築する情報システムごとに、個々にインターネット回線を構築すると、当該インターネット回線の監視等に係る体制や運用コストが分散し、効率的かつ集中的なセキュリティ監視が行われず、セキュリティ水準が低下するおそれがある。このような観点から、機関等として（又は国の行政機関にあってはこれら機関全体で）インターネット接続口を統合・集約し、集中的なセキュリティ監視を行うなどの取組を行っている場合は、当該取組の範疇とするか否か検討した上で、構築する情報システムに接続するインターネット回線を仕様書等において明確化しておくことを求めている。

なお、既設のインターネット回線を利用せずに、独立したインターネット回線を調達してセキュリティ監視等の運用を個別に行う場合も想定される。情報システムが取り扱う情報の格付や取扱制限等の特性に従って、既設のインターネット回線の利用可否を判断することが望ましい。

- **遵守事項 5.2.1(2)(c)「IT 製品の調達におけるセキュリティ要件リスト」について**

「IT 製品の調達におけるセキュリティ要件リスト」には、デジタル複合機、OS、ファイアウォール等の製品分野ごとに一般的に想定されるセキュリティ上の脅威が記載

されており、それらが自身の運用環境において該当する場合には、当該脅威に対抗する必要がある。

対抗手段の一つとして、「IT 製品の調達におけるセキュリティ要件リスト」には、IT セキュリティに関わる「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、製品の利用環境や製品に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

参考：経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
（http://www.meti.go.jp/policy/netsecurity/cclistmetisec.pdf）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 5.2.1⑵-2「開発する情報システムが運用される際に想定される脅威」について**

汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、全てを独自開発する場合であっても、外部から脆弱性をつかれる可能性があるため、開発する情報システムの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。

また、情報システムを構成する端末、サーバ装置、それらに搭載されているソフトウェア等に関して想定される脅威に対しては、第 7 部で規定された対策が適切に実施されるようにセキュリティ要件を策定することが必要となる。策定に当たっては、運用開始後に適切に対策が講じられるようにシステムの企画段階から留意する必要がある。例えば、サーバ装置の運用時に必要になる不正アクセス等の監視機能を実装すること、端末やサーバ装置等に利用を認めるソフトウェア以外のソフトウェアが意図せず混入されないこと等について留意が必要となる。

- **基本対策事項 5.2.1⑵-3「ST 確認」について**

セキュリティ要件の策定に当たっては、脅威に対抗するために妥当なセキュリティ要件となっていることの確認を求める事項である。

セキュリティ要件の妥当性確認には、機関等内でのレビューの実施等の他に、対象とする情報システムが扱う業務及び情報の重要度によっては、セキュリティ要件の策定に関っていない客観的な立場の者による検証を実施することが望ましい。

「ST 確認」とは、情報システムが対抗すべき脅威について適切なセキュリティ要件が策定されていることを確認するために、セキュリティ設計仕様書（ST:Security Target）を IT セキュリティ評価基準（ISO/IEC 15408）に基づき、第三者である評価

機関が評価し、その評価結果が妥当であることを認証機関（独立行政法人情報処理推進機構）が検証し、確認することをいう。

- **基本対策事項 5.2.1⑵-4 a)「管理機能」について**

「管理機能」とは、真正確認、権限管理等のセキュリティ機能を管理するための機能のほか、情報セキュリティインシデントの発生時に行う対処及び復旧に係る機能、証跡保全の機能等を指し、これらの必要性を情報システムの設計時から検討することにより、必要がある場合には情報システムに組み込む必要がある。

- **基本対策事項 5.2.1⑵-4 b)「監視のために必要な機能」について**

情報システム及び取り扱う情報の格付や取扱制限等を考慮して、情報システムの各所において様々なイベントを監視する必要性を見極める必要がある。監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。

監視に係る運用管理機能要件の策定の際には、イベント情報を効率的に活用できるようにするため、当該情報を収集する際のデータ形式については、その標準化の動向を踏まえ、一般的に用いられる見込みのある形式をとることが望ましい。

なお、監視によりプライバシーを侵害する可能性がある場合は、関係者への説明について定めること。

- **基本対策事項 5.2.1⑵-5「脆弱性への対策」について**

脆弱性対策を怠った場合には、セキュリティ侵害の機会を増大することにつながるため、情報システムの企画段階から対策を講じておく必要がある。

脆弱性が存在することが公表されているソフトウェア等については対策が施されているバージョンのものを利用することや、開発後の情報システムに脆弱性が存在することが発覚した場合に備えて、調達時の仕様書に対策のための要件を明記しておくことが重要となる。

- **基本対策事項 5.2.1⑵-5 b)「脆弱性が混入されることを防ぐためのセキュリティ実装方針」について**

「脆弱性が混入されることを防ぐためのセキュリティ実装方針」とは、情報システム開発者が情報システムに脆弱性を混入することを防ぐために、開発時における脆弱性への具体的な対策方法を定めたものである。脆弱性は種類ごとに対策が異なり、懸念される脆弱性の種類ごとに方針を定める必要がある。具体的に定めるものとして、例えば以下の内容が考えられる。

  - バッファオーバーフローによる不正なプログラムの挿入及び実行を防ぐために、データを転記する場面においてメモリ領域長とデータ長を検査する処理を付加する。
  - SQL インジェクションによるデータベース内の情報の漏えい・改ざんを防ぐために、プレースホルダにより SQL 文を組み立てる。
  - OS コマンドインジェクションによる不正なシステム操作を防ぐために、シェル

を起動できる言語機能を利用しない。

6.2.1「ソフトウェアに関する脆弱性対策」及び 7.2.2「ウェブ」の規定内容も参考にして、懸念される全ての脆弱性の種類に対して、実装方針を定め、仕様書に明記する必要がある。

- **基本対策事項 5.2.1(2)-6 b)「機器等の利用環境において対抗すべき脅威」について**

機器等に対するセキュリティ上の脅威は利用環境によって変わるため、調達時にどのような環境で運用するのかを把握し、その環境において存在する脅威及びその脅威に対する脆弱性を分析した上で、必要となるセキュリティ要件を策定する必要がある。

例えば、ネットワークに接続し、通信データとして要機密情報を送受信する場合に盗聴による情報漏えいが想定される場合には、通信データの保護に係るセキュリティ要件が必要となるが、スタンドアロンで利用する場合で、盗聴による情報漏えいが想定されない場合には、通信データの保護に係るセキュリティ要件は不必要なセキュリティ要件となる可能性がある。

また、特定の人物しか物理的にアクセスできないように隔離された場所へ機器等を設置すること等で、誰もが物理的にアクセスできる環境で想定される脅威を軽減することも考えられる。

調達する機器ごとの利用環境において想定される脅威を漏れなく分析した上で、脅威に対抗するために必要十分なセキュリティ要件を策定することが重要である。

遵守事項

(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

【 基本対策事項 】

＜5.2.1(3)(a)(イ)関連＞

5.2.1(3)-1 情報システムセキュリティ責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。

a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から**運用中の情報システムに悪影響**が及ばないように、運用中の情報システムと分離すること。

b) **情報セキュリティの観点から必要な試験**がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

c) 情報セキュリティの観点から実施した試験の**実施記録**を保存すること。

＜5.2.1(3)(a)(ウ)関連＞

5.2.1(3)-2 情報システムセキュリティ責任者は、**開発工程における情報セキュリティ対策**として、以下を含む事項を実施させること。

a) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

- ソースコードの変更管理
- ソースコードの閲覧制限のためのアクセス制御
- ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、**設計レビュー**及び**ソースコードレビュー**の範囲及び方法を定め、これに基づいてレビューを実施すること。

（解説）

- **基本対策事項 5.2.1(3)-1 a)「運用中の情報システムに悪影響」について**

運用中の情報システムを利用してソフトウェアの作成及び試験を行う場合は、運用中の情報システムに悪影響が及ぶことを回避することが大前提となる。

また、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにする必要がある。

- **基本対策事項 5.2.1(3)-1 b)「情報セキュリティの観点から必要な試験」について**

攻撃が行われた際に情報システムがどのような動作をするかを試験する項目として想定しており、具体的には、想定の範囲外のデータの入力を拒否できるか、サービス不能攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、レースコンディションが発生しないか（「(解説) 基本対策事項 7.2.2(2)-1 l) 「レースコンディション脆弱性」について」を参照のこと。）といった項目が挙げられる。

なお、セキュリティ機能の試験だけにとどまらず、情報システムの脆弱性の有無、必要なチェック機能の欠如等について、必要な試験が網羅されるよう留意することが望ましい。

- **基本対策事項 5.2.1(3)-1 c)「実施記録」について**

「実施記録」とは、試験の項目、実施結果、実施時に判明した不具合及び当該不具合の修正の記録等を指し、これらを保存することにより、脆弱性を発見した場合の対処に利用できるようにすることが求められる。

- **基本対策事項 5.2.1(3)-2「開発工程における情報セキュリティ対策」について**

情報システム開発に係る情報資産についてセキュリティを維持するための手順及び環境を定めることを求めている。

具体的な手順としては、例えば、仕様書、ソースコード等の成果物に対して情報システムのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツール等が考えられる。

開発環境については、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用するサーバ装置及び端末の設置場所及びアクセス制御の方法等がある。

なお、情報システム開発を外部委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。

- **基本対策事項 5.2.1(3)-2 c)「設計レビュー」について**

情報システムの設計について、脆弱性の原因となる設計の不具合をなくすために、設計レビューの実施が求められる。

一般に設計レビューには、①レビュー対象内にあるエラーの発見を第一目的とし、開発責任者等が実施する確認手法（インスペクション）、②開発担当者自身が開発関係者を集め、レビュー対象プログラムを実行の流れに従って追跡し確認する手法（ウォークスルー）等があり、これらを、いつ、誰が、何に対して実施するのか、といったことを定める必要がある。

- **基本対策事項 5.2.1(3)-2 c)「ソースコードレビュー」について**

ソースコードに脆弱性が混入しないように、ソースコードレビューの範囲及び方法について、あらかじめ定めておくことが求められる。例えば、脆弱性の原因となるソースコードについては、開発言語ごとに典型的なパターンが知られていることから、ソースコードレビューによる検証が有効な場合がある。ソースコードレビューについては、開発する情報システムだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。

遵守事項

(4) 情報システムの運用・保守を外部委託する場合の対策

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

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

【 基本対策事項 】

＜5.2.1(4)(a)関連＞

5.2.1(4)-1 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に、以下を含む要件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。

a) 情報システムの**運用環境に課せられるべき条件**の整備

b) 情報システムのセキュリティ監視を行う場合の**監視手順**や連絡方法

c) 情報システムの**保守における情報セキュリティ対策**

d) 運用中の情報システムに**脆弱性が存在することが判明**した場合の情報セキュリティ対策

（解説）

- **遵守事項 5.2.1(4)(b)「当該対策による情報システムの変更内容」について**

情報セキュリティ対策を実施することにより、ソフトウェアのバージョン等、遵守事項 5.1.1(2)で整備することとされている情報システム関連文書の内容に変更が生じる可能性がある。情報セキュリティ対策を実施するためには情報システムの状態を正確に把握する必要があることから、情報セキュリティ関連文書の内容を最新に保つために、当該文書で管理している項目について報告を求めることが重要である。

- **基本対策事項 5.2.1(4)-1 a)「運用環境に課せられるべき条件」について**

情報システムの運用環境に課せられるべき条件としては、物理的、接続的（ネットワーク環境）及び人的側面が考えられる。どのような条件を設定するかによって想定される脅威が異なってくるため、脅威を想定する上で必要となる条件は全て調達仕様書、契約書等に記載する必要がある。

物理的側面とは、サーバ装置を設置する場所の特定、耐震･防火に関する基準、電源供給に関する基準等に関する条件を示すものである。

接続的（ネットワーク環境）側面とは、情報システムが接続される通信回線の種類や外部サービスをネットワーク経由で利用する場合の条件等を示すものである。

人的側面とは、対象とするシステムの管理者や業務担当職員等の信頼性に関する条

件、当該システムに関わる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものである。

- **基本対策事項 5.2.1(4)-1 b)「監視手順」について**

  情報システムのセキュリティ監視を行う体制を特別に設けずに、情報システムの運用を行う体制にてセキュリティ監視を行うことも考えられる。

  監視によりプライバシーを侵害する可能性がある場合は、対象となる関係者への説明等の手順についても機関等として定めておくこと。

- **基本対策事項 5.2.1(4)-1 c)「保守における情報セキュリティ対策」について**

  情報システムの保守においては、保守担当者が作業中に権限外の情報にアクセスできないよう、アクセス制御や権限管理を考慮する必要がある。また、保守担当者へのなりすましが脅威として想定される場合には、保守担当者に対する主体認証が実装された情報システムのセキュリティ要件を考慮する必要がある。

- **基本対策事項 5.2.1(4)-1 d)「脆弱性が存在することが判明」について**

  ソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性は日々新たなものが報告されており、調達時に策定した脆弱性についての対策要件だけでは十分に対処できない可能性もあり得る。

  また、運用・保守を行う委託先が、情報システムの構築を行った委託先と異なる場合、情報システム運用開始後に発見された脆弱性に対して、情報システムの構築を行った委託先のみでは対処することが困難な場合もあり得る。そのため、運用・保守を行う委託先に対して、運用開始後に発見された脆弱性への対処を求めることも、契約又は仕様書において考慮する必要がある。

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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.2(1)(a)「選定基準に対する機器等の適合性を確認」について**

  遵守事項 5.1.2(1)(a)において整備された機器等の選定基準に従って、機器等の開発等のライフサイクルにおいて不正な変更が加えられない管理体制が確認できることや、第三者による情報セキュリティ機能の客観的な評価が行われていることを確認すること等を求めている。

  なお、ISO/IEC 15408 に基づく認証を取得していることを選定基準として活用する場合には、認証を取得していることを証明するための認定書等を調達先に提示させることも考えられる。

遵守事項

(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。

【 基本対策事項 】

＜5.2.2(2)(a)関連＞

5.2.2(2)-1 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以下を含む**情報セキュリティ対策**を行うこと。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。

c) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。

d) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。

e) 脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

5.2.2(2)-2 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段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。

a) 情報セキュリティに関わる運用保守体制の整備

b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

c) 情報セキュリティインシデントを認知した際の対処方法の確立

（解説）

- **遵守事項 5.2.2(2)(b)「移行手順及び移行環境」について**

情報システムの開発環境、テスト環境から本番運用の環境への移行時において、情報システムに保存されている情報の取扱手順の整備、人為的な操作ミスを防止するための手順・環境の整備、移行の際に関連システム停止が伴う場合には可用性確保のための環境整備等が必要となる。

- **基本対策事項 5.2.2(2)-1「情報セキュリティ対策」について**

情報システムの構築を外部委託する場合には、遵守事項 5.2.1(3)の内容を委託先に適切に実施させることが求められる。また、情報システムの構築を外部委託せず、機関等自らが構築する場合であっても、同項の内容を参照し、必要な対策を実施することが求められる。

遵守事項

(3) 納品検査時の対策

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

(b) 情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、**情報セキュリティ対策に必要な内容が含まれている**ことを確認すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.2(3)(a)「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」について**

  情報セキュリティ対策の視点を加味して整備された納入時の確認・検査手続に従い、納入された情報システム及び機器等が要求仕様どおりに正しく動作することの検査を行うことが求められる。

  機関等における受入れテストの実施、納入元が実施したテストに関する資料の提出要求及びその検査内容の確認、第三者への受入れテストの委託、ISO/IEC 15408 に基づく第三者認証取得の確認等、検査対象の情報システム及び機器等の特性に応じて適切な検査を実施する必要がある。

- **遵守事項 5.2.2(3)(b)「情報セキュリティ対策に必要な内容が含まれている」について**

  情報セキュリティ対策に必要な内容とは、遵守事項 5.1.1(2)(a)(ア)、(イ)及び(ウ)に記載の情報を意味する。

  なお、情報システムの運用保守事業者が交代する場合には、現在の事業者から次期事業者への引継事項の確認も同様に行うことが必要である。

5.2.3 情報システムの運用・保守

目的・趣旨

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

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

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

遵守事項

(1) 情報システムの運用・保守時の対策

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

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

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

【 基本対策事項 】

＜5.2.3(1)(a)関連＞

5.2.3(1)-1 情報システムセキュリティ責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。

a) 監視するイベントの種類
b) 監視体制
c) 監視状況の報告手順
d) 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の報告手順
e) 監視運用における情報の取扱い（機密性の確保）

5.2.3(1)-2 情報システムセキュリティ責任者は、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ていること**を確認すること。

5.2.3(1)-3 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り扱う情報に

ついて、当該情報の格付及び取扱制限が適切に守られていることを確認すること。

5.2.3(1)-4 情報システムセキュリティ責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

（解説）

- **基本対策事項 5.2.3(1)-2「セキュリティ機能が適切に運用されていること」について**

  運用する情報システムについて、外部環境が大きく変化した場合等には、セキュリティ機能が適切に運用されるために、機器等のパラメータ設定、物理的な設置環境、ネットワーク環境、人的な運用体制等について問題が無いことを適宜確認する必要がある。

- **基本対策事項 5.2.3(1)-3「当該情報の格付及び取扱制限が適切に守られていること」について**

  情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更される必要がある。

- **基本対策事項 5.2.3(1)-4「脆弱性の存在が明らかになった場合」について**

  機関等が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。

  また、情報セキュリティ対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずる必要もある。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.4(1)(a)(ア)「情報の移行」について**

情報システムを更改する際は、更改元の情報システムから更改先の情報システムに情報（本番データ）を移行する作業が発生する場合が多いが、移行作業の過程で情報が外部に漏えいすることのないよう、移行用の本番データを適切に管理することが必要である。移行用の本番データの管理手順や外部電磁的記録媒体を使用する場合の安全管理措置等をあらかじめ定めておくとよい。移行作業を外部委託する場合においては、委託先とあらかじめ手順について合意し、仕様書に明記しておく必要がある。

- **遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について**

情報システムの廃棄を行う場合には、情報システムを構成する機器等並びに内部に保存されている情報の格付及び取扱制限を考慮して、適切に抹消する必要がある。要機密情報を保存している情報システムにおいては、情報の抹消が求められる。廃棄の際に本条を考慮すべき機器等としては、サーバ装置や端末以外にも、複合機等の内蔵電磁的記録媒体を備えた機器については同様に考慮する必要がある。第 7 部において機器ごとの廃棄時の対応を規定しているので、併せて考慮されたい。

なお、情報システムの廃棄を外部委託する際は、委託先において情報の抹消が適切に実施されるよう、遵守事項 3.1.1(7)の規定も参考に、抹消方法等についてあらかじめ合意し仕様書等に明記しておく必要がある。委託先の抹消作業に関する作業完了届（廃棄したことが証明されるもの）等を書面で受け取るなどするとよい。

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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.5(1)(a)「見直し」について**

情報システムの情報セキュリティ対策について、新たな情報セキュリティ上の脅威、情報セキュリティインシデント発生事案例及び情報セキュリティインシデント発生時の影響等を検討した上で、情報システムの情報セキュリティ対策について定期的に見直しを行い、セキュリティ要件の追加、修正等の必要な措置を求める事項である。

所管する情報システムに変更があった場合、情報システムの外部環境に変化が生じた場合等の際には、定期的な情報セキュリティ対策の見直しに加えて、適時見直すことも必要となる。

5.3 情報システムの運用継続計画

5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、国の行政機関においては、府省業務継続計画と情報システム運用継続計画を策定し運用している。独立行政法人及び指定法人においても、業務の特性に応じて、中期目標による指示等により、法人の業務継続計画と情報システムの運用継続計画を策定し運用している。

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

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

遵守事項

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 統括情報セキュリティ責任者は、機関等において**非常時優先業務**を支える**情報システムの運用継続計画を整備**する必要がある場合は、**非常時における情報セキュリティに係る対策事項**を検討すること。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.3.1(1)(a)「非常時優先業務」について**

政府業務継続計画では、首都直下地震発生時に優先的に実施する業務を「非常時優先業務」とし、非常時優先業務を遂行するために必要な組織管理、庁舎管理等の事務を「管理事務」としている。非常時優先業務及び管理事務に位置付ける業務については、中央省庁業務継続ガイドライン 第２版（首都直下地震対策）等を参考にするとよい。

また、本款では、首都直下地震以外の災害等の発生時に優先的に実施する業務を行う必要がある場合には、当該業務も非常時優先業務として取り扱うことが求められる。

独立行政法人及び指定法人においても、法人の特性に応じて、災害等の発生時に優先的に実施する業務を非常時優先業務としておくことが必要である。

参考：内閣府（防災担当）「国の業務継続計画」

（http://www.bousai.go.jp/taisaku/chuogyoumukeizoku/）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 5.3.1(1)(a)「情報システムの運用継続計画を整備」について**

国の行政機関における情報システム運用継続計画は、内閣官房情報セキュリティセンターが取りまとめた「中央省庁における情報システム運用継続ガイドライン」に基づき作成することとされている。

独立行政法人及び指定法人においても、情報システムの運用継続計画を「中央省庁における情報システム運用継続ガイドライン」に基づき作成するとよい。

参考：内閣官房情報セキュリティセンター「「中央省庁における情報システム運用継続計画ガイドライン」及び関連資料」（平成 25 年 6 月）
（https://www.nisc.go.jp/active/general/itbcp-guideline.html）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 5.3.1(1)(a)「非常時における情報セキュリティに係る対策事項」について**

情報システムの運用継続を脅かす危機的事象の例として、地震、風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、不正アクセス等の運用妨害、機器等の故障等が想定される。これらの非常時に対して、業務継続計画、情報システムの運用継続計画及び情報セキュリティ関係規程のそれぞれで定める対策に矛盾があると、非常時に職員等は一貫性のある行動をとることができない。このため、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際は、業務継続計画及び情報システムの運用継続計画と情報セキュリティ関係規程との間で整合性を確保するよう検討することが必要である。

例えば、非常時に、情報システムの主体認証情報として設定したパスワードを設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。このような場合の実施手順について、業務継続計画及び情報システムの運用継続計画で安易に定めるのではなく、情報セキュリティ関係規程において、非常時でも情報セキュリティ水準を確保した実施手順を整備する必要がある。手順の一例としては、通常時に利用する識別コードとパスワードとは別に、非常時用の識別コードとパスワードをあらかじめ設定しておく方法が考えられる。この場合、非常時用のパスワードは人が記憶困難な文字列で設定し、そのパスワードを記載した紙面を施錠された安全な保管場所に保管することで、通常時のパスワードを非常時に聞き出したり、通常時にパスワードを共用したりすることなく、非常時においても情報システムの利用が可能となる。また、パスワードを記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無を確認できる。

また、非常時には、機関等の施設の一部に帰宅困難者等を受け入れる場合等、通常時

の情報セキュリティ水準の確保に支障をきたす状況が考えられる。このような場合を想定し、あらかじめ情報セキュリティ水準の確保を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、通常時及び非常時の対応を定める必要がある。例えば、各執務室や各職員等の卓上の情報セキュリティ対策を含め、通常時から不特定の者の出入りを想定した対策を講ずること等が考えられる。

なお、停電や交通機関の麻痺等の社会インフラの不全等により、通常時に利用している情報システムが利用できなくなる場合や、通常時に利用している場所で情報システムを利用することができない場合等、情報システムを利用する環境が制限される状況が考えられる。このような場合を想定し、約款による外部サービス、機関等支給以外の端末等の利用が非常時優先業務の継続に有効であると判断される場合には、それらを利用して業務を継続することについても、そのリスクや情報セキュリティ水準の確保等を十分に検討した上で、あらかじめ定めておく必要がある。

- **遵守事項 5.3.1(1)(b)「運用可能であるかを確認」について**

情報システムの運用継続を脅かす非常時においては、非常時の情報セキュリティに係る対策事項を整備した際には想定していなかった様々な不整合が発生し、整備した対策事項が有効に機能しないことも考えられる。このため、非常時の対策事項を定期的に見直し、課題を発見した場合は改善することが重要である。

なお、情報システムの運用継続計画の教育訓練を行う際は、非常時の対策事項の理解と対応能力の向上の他、対策事項の有効性の確認も目的とすることが望ましい。

第6部 情報システムのセキュリティ要件

6.1 情報システムのセキュリティ機能

6.1.1 主体認証機能

目的・趣旨

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

また、機関等の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(1) 主体認証機能の導入

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

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

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

【 基本対策事項 】

＜6.1.1(1)(a)関連＞

6.1.1(1)-1 情報システムセキュリティ責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入すること。この際、認証の強度として２つ以上の方式を組み合わせる主体認証方式（**多要素主体認証方式**）が求められる場合には、これを用いること。

a) **知識**（パスワード等、利用者本人のみが知り得る情報）による認証

b) **所有**（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

c) **生体**（指紋や静脈等、本人の生体的な特徴）による認証

6.1.1(1)-2 情報システムセキュリティ責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によ

るパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設けること。

＜6.1.1(1)(c)関連＞

6.1.1(1)-3 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、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下を例とする機能を設けること。

a) 利用者が定期的に変更しているか否かを確認する機能
b) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能
c) 利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能

6.1.1(1)-4 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、主体認証情報が第三者に対して明らかにならないよう、以下を含む方法を用いて適切に管理すること。

a) 主体認証情報を送信又は保存する場合には、その内容を暗号化する。
b) 主体認証情報に対するアクセス制限を設ける。

6.1.1(1)-5 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、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。

a) 当該主体認証情報及び対応する識別コードの利用を停止する機能
b) 主体認証情報の再設定を利用者に要求する機能

（解説）

- **遵守事項 6.1.1(1)(a)「識別」について**

識別のための機能が実装されていない情報システムにおいて主体認証を行う場合（例えば、識別コード自体が存在せず、主体認証情報の検証のみで主体認証を行う場合）は、例外措置として判断し、主体を識別しないことによる影響を勘案の上、必要に応じて代替又は追加の措置を講ずる必要がある。

- **遵守事項 6.1.1(1)(a)「主体認証」について**

情報セキュリティ水準と情報システムの利便性等を考慮し、主体認証機能の運用に係る以下の要件の実装要否を情報システムの導入時に考慮するとよい。

- 正当な主体以外の主体認証を受諾しないこと。（誤認の防止）
- 正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）
- 正当な主体が容易に他の主体に主体認証情報の付与（発行、更新及び変更を含む。以下本款において同じ。）及び貸与ができないこと。（代理の防止）
- 主体認証情報が容易に複製できないこと。（複製の防止）
- 情報システムセキュリティ責任者の判断により、ログインを個々に無効化できる手段があること。（無効化の確保）
- 必要時に中断することなく主体認証が可能であること。（可用性の確保）

- 新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）
- 主体に付与した主体認証情報を利用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

- **遵守事項 6.1.1(1)(b)「オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること」について**

本項は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する際に、利用者本人であることを確認するための認証機能を適切に実装することを求めるものである。

オンライン手続におけるリスク評価に当たっては、サイバー攻撃等の脅威から生じ得る正当な認証の失敗や不正な認証の成功等による影響についてリスクの評価を行い、オンライン手続に必要な認証方式を適切に選択することが重要である。リスク評価を行う際は、以下の認証プロセスに係る６つの評価軸に対応する脅威を踏まえるとよい。

① 認証情報の登録（身元証明等、登録申請の正当性の確認）
② 認証情報の発行や失効等の処理
③ 認証情報の失効時の処理等の運営管理ルール
④ 発行元における認証情報の技術的な管理手法
⑤ 利用者における認証情報の管理
⑥ 認証情報を使用した認証機能の実行

次に、上記に示す認証プロセス①～⑥ごとに、リスクを生じさせる脅威を特定し、リスクの影響度とそれが生じる可能性の高さを判定した上で、必要な認証方式を決定するとよい。オンライン手続において想定されるリスクとしては、主に以下の６種類に分類することができる。

① オンライン手続サービスの利用において国民等の利用者に不便、苦痛を与える、又はオンライン手続サービスを所管する機関等が信頼を失う
② 国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える
③ 機関等の活動計画や公共の利益に対して影響を与える
④ 国民等の利用者の個人情報等の機微な情報が漏えいする
⑤ 国民等の利用者の身の安全に影響を与える
⑥ 法律に違反する

なお、認証方式の選択に当たっては、上記①～⑥のリスクを検討し、適切なセキュリティ確保と普及を妨げない利便性とを両立させることが重要である。その際は、特定のリスクのみに着目せず、様々な観点でリスクを評価した上で認証方式を決定する必要がある。

- **遵守事項 6.1.1(1)(c)「不正な主体認証の試行に対抗するための措置」について**

主体認証機能に対する不正を防止するための機能として、以下を例とする機能を設けることを検討することが重要である。

- 前回のログインに関する情報を通知する機能

  主体ごとに割り当てられた識別コードに対して、前回のログインに関する情報（日時や装置名等）を、次回のログイン時等のタイミングで主体に通知する機能を指す。正当な主体以外の者が主体に割り当てられた識別コードを使用して不正にログインした場合に、正当な主体がそれを検知することができるようになると考えられる。
- 不正にログインしようとする行為を検知又は防止する機能

  特定の識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を正当な主体や情報システムの運用担当者等に通知し、一定期間当該端末（又は識別コード）からのログイン操作受付を停止する機能を指す。当該識別コードによる情報システムへの以後のログインを無効にすることも考えられる。この機能により、不正なログインの試行の有無等について、正当な主体や情報システムの運用担当者等がその状況を確認するとともに、一定程度不正ログイン等を防止することができる。
- 情報システムへのログイン時にメッセージを表示する機能

  情報システムへのログインの際に、軽率に不正アクセスに及ぶ行為を抑止する効果が期待されるメッセージを画面に表示する機能を指す。

  通知メッセージとして、以下の例が考えられる。
  - アクセス履歴が管理者に通知されること
  - 利用状況を監視、記録しており、監査対象となること
  - 情報の目的外利用は禁止されていること
  - 情報システムへの不正アクセス行為は禁止されており、不正アクセス禁止法の罰則対象となること
- 管理者権限によるログインの際に個別の識別コードによりログインすることを併せて求める機能

  管理者権限を有する共用識別コードの利用において、実際の作業者となる個別の識別コードによるログインを併せて行うことを求める機能を指す。

  管理者権限を有する共用識別コードのログイン記録だけでは、実際に作業をした管理者を個人単位で特定することが困難となるため、作業者個別の識別コードによるログインを行った後に管理者権限を有する共用識別コードによるログインを許可するものである。

  例えば、当該情報システムの OS が Unix 系の場合には、一般利用者でログインした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログインを禁止する設定により、その手順を強制することができる。

- **基本対策事項 6.1.1(1)-1「多要素主体認証方式」について**

主体認証を行う情報システムにおいて、1 つの主体認証方式のみで行う認証の強度におけるリスクが許容できない場合には、2 つ以上の主体認証方式を用いて認証を行う多要素主体認証方式を導入することが望ましい。

主体認証方式は、一般に、異なる認証方式を組み合わせた方が、強度が高くなる。異なる認証方式を組み合わせた多要素主体認証方式であれば、例えば仮にパスワード（知識）が露呈してしまっても、IC カード（所有）もしくは指紋（生体）等の残りの主体認証情報が他者の手に渡らない限り、不正なログインを防ぐことができる。

通常の運用時は単一の主体認証を実施するケースであっても、認証の要求時に、アクセス元の IP アドレス、アクセスする時間帯、位置情報等が通常のアクセスとは異なる特徴が確認された場合は、不正ログインのリスクが高まったと判断して多要素主体認証を行う方法も考えられる。

- **基本対策事項 6.1.1(1)-1 a)「知識」について**

端末によっては、例えばパスワード以外にも、自分のみが知る「パターン」を主体認証情報として扱うケースがあるが、これも「知識」に分類される。

- **基本対策事項 6.1.1(1)-1 b)「所有」について**

「所有」による認証の例として、国の行政機関が個別に保有するアカウント情報のマスターデータベース機能を提供する「統合ディレクトリ」とのデータ連携を行う「職員等利用者共通認証基盤（GIMA：Government Identity Management for Authentication）」を介し、政府認証基盤（GPKI）における電子証明書を用いた認証、国家公務員 IC カードを用いた認証等が挙げられる。

- **基本対策事項 6.1.1(1)-1 c)「生体」について**

生体情報による主体認証を用いる場合には、その導入前に、この方式特有の他人受入率（本人を他人と誤って認証してしまう確率）と本人拒否率（本人の認証が受け入れられない確率）の課題があることを考慮して情報システムを設計する必要がある。

- **基本対策事項 6.1.1(1)-3「利用者に主体認証情報の定期的な変更を求める場合」について**

定期的な変更を促すことについて、「利用者に主体認証情報の定期的な変更を求める場合には」と改めて適用する場面を限定しているのは、生体情報のように利用者本人でも変更が不可能なものも主体認証情報に含まれていることが理由の一つであるが、これに限られず、主体認証情報がパスワードである場合に、その変更を強制することが利用者の利便性を低下させ、利用者が強度の低い安易なパスワードを設定しやすくなるなど、結果的に主体認証機能の安全性を低下させる懸念が想定されることを踏まえて、定期的な変更が真に必要である場合に限り適用すべき基本対策事項であることを示す趣旨である。

パスワードを定期的に変更することの情報セキュリティ上の効果は、情報システムの運用方法や認証技術の方式により異なるものであり、必ずしも明らかでない。

利用者にパスワードの定期的な変更を求めるか否かは、その効果と逆効果を勘案して判断する必要がある。

パスワードを変更する目的は、パスワードを他の主体に不正に利用されることを未然に防止することにあるが、どの程度の頻度で定期的に変更すればこれを防止するだけの意義を果たすと言えるのかは一概に言うことはできない。

例えば、利用者がパスワードを入力する様子を背後から盗み見られる事態を想定して、その不正利用を確実に防止するためにパスワードの定期的な変更を求めるのであれば、変更は毎日必要となり、現実的でない。一定の不正利用はやむを得ないとしつつ、長期間にわたって不正利用され続けることを防止することを目的とするのであれば、例えば、半年に 1 度の定期的な変更を求めている場合は、平均して 3 か月間の不正利用を許すことになる。許容できる不正利用の平均継続期間を 1 週間と想定した場合には、2 週間に 1 度の変更が必要となり、これも現実的でない場合が多いと考えられる。このような目的では他の対策を講じることの方が効果的である場合があり、そのような場合にはその対策の採用を検討するべきである。

また、技術的な誤解に基づく判断の下で定期的な変更を求めることは避けられるべきである。技術的な誤解の例としては、以下が考えられる（後掲の「参考」を参照）。

① パスワードは当てられる前に変更すれば当てられるのを避けられるとの誤解

② 共通鍵暗号の鍵を定期的に変更する必要があることと混同した誤解

③ 使用によりパスワードが劣化する通信プロトコルを用いているとの誤解

これらの点を踏まえ、パスワードの定期的な変更が必要であるとすれば、次の場合などが考えられる。

- 旧式の認証プロトコルが用いられている場合

  LAN 内で用いられている認証プロトコルには、TLS が用いられていない場合があり、認証プロトコルによってはオフライン攻撃が可能なものもあり得る。LAN 内での盗聴を脅威として想定する必要があって、かつ、そのような旧式の認証プロトコルが用いられている場合には、パスワードの定期的な変更にも意義があると言えなくもない。この場合、パスワード変更の頻度は、オフライン攻撃が完了しないうちに変更するようにする必要があることから、設定されているパスワードの複雑さに応じて高頻度で変更する必要がある。

  なお、十分に長いパスワードを設定可能であれば、オフライン攻撃による総当りを現実的に不可能にすることができる（過去に脆弱性が指摘された実装を利用している場合を除く。）。例えば、13 文字のランダムな英数字（62 文字種）の場合、300 万回/秒で試行した場合、総当たりに 21 億年を要し、100 年以内に当てられる確率を十分に小さくできる。そのような強度のパスワードを設定させる運用が可能ならば、この目的での定期的変更は必要でない。

- 短いパスワードしか設定できない情報システムを用いている場合

  上記のようなオフライン攻撃を許す旧式の認証プロトコルが用いられている場合であって、13 文字といった十分に長いパスワードを設定できない旧式の情報システムを用いている場合には、パスワードの定期的な変更は必要である。この場合には、オフライン攻撃によってパスワードを復元されるまでにかかる時間を踏まえて、必要な周期での定期的な変更を求める必要がある。

- 複数の者で 1 つのパスワードを共用する場合

  同一の部署に属する複数の主体に利用を認める場合など、主体認証情報を複数の主体で共用する必要がある場合（本来はこのような利用は避けるべきであるが、利用せざるを得ない場合（複合機などの機器やソーシャルメディア（「(解

説）基本対策事項 4.1.3(1)-3 a)「パスワードを知る担当者を限定」を参照）のアカウント等が想定される。)）においては、人事異動等によりグループを出入りする者がいる場合、一定の期間が経過すると、権限のない者がパスワードを知っている状態が生ずる。そこで、定期的にパスワードを変更することにより、権限のなくなった者が知るパスワードを無効化し、不正利用を防止することができる。しかし、本来ならばグループから出る者が生じる都度すぐにパスワードを変更することがより適切な運用であって、定期的に変更する運用は結果的に防止する効果はあるものの迂遠的な対策にすぎない。そもそもパスワードを共用すること自体が適切でない面もある。とはいえ、その程度のリスクは許容できるとする場合に限ってグループパスワードを使っている場合には、一年や半年程度の期間で定期的にパスワードを変更することは、有意義であるとも言える。

- 何十年にも渡り全くパスワードを見直さないのはよろしくないとの趣旨から

  昨今、パスワードをどう運用するべきかが改めて論点となっているように、1990 年代と今日とでは、パスワードに関するリスクも異なり、また、情報システムで利用可能なパスワードの最大長も変化してきている。かつては、8 文字までといった制限がしばしば見られたが、今日では、64 文字まで設定可能とした情報システムも増えてきている。したがって、十数年前に設定した 8 文字のパスワードをこの際見直して、20 文字ほどの覚えやすいパスワードに変更したり、ランダムなパスワードに変更することには意義がある。パスワードの定期的な変更を義務付けていれば、結果的にこうした見直しを促すことにはなるが、その目的であれば、一度見直せばよいのであって、短期間に定期的に見直す必要性はない。

参考：パスワードの定期的な変更の必要性に関する技術的な誤解の例

① パスワードは当てられる前に変更すれば当てられるのを避けられるとの誤解

パスワードの長さが短い場合に、「一つひとつ試していけばいずれ当てられてしまうのだから、当てられる前に変更すればそれを避けられる。」という素朴な感覚による誤解である。

しかし、どのパスワードが攻撃者によって既に試行済みであるかは、利用者には分からないので、利用者が変更した後のパスワードが攻撃者の残りの施行対象から外れることになるとは限らない。

結局のところ、パスワードは当てられない程度に十分に長くするほかないのであり、その尺度には、例えば、「100 年以内に 1 回以上当てられる確率が 0.0001%以下」といった基準が考えられ、これを満たす長さのパスワードを設定していれば、定期的に変更してもしなくても、当てられる確率はこれ以下に抑えられる。

② 共通鍵暗号の鍵を定期的に変更する必要があることと混同した誤解

共通鍵暗号において鍵の定期的な変更が求められていることから、パスワードについても同様の変更が必要であると考えてしまう誤解である。

共通鍵暗号では、一般に、同じ鍵を繰り返し用いていると、その鍵で暗号化された暗号文を大量に得ることができれば、それを用いて鍵を推定できる確率が高まっていく性質があることから、鍵の定期的な変更が求められている。このことからの類推で、パスワードについても使用回数が増えるとパスワードの秘匿性が劣化すると考えてしまうとすれば、それは誤解である。

なぜなら、もしパスワードそのものを暗号鍵として暗号化した暗号文をそのまま通信する認証プロトコルが存在するならば、たしかに、共通鍵暗号で定期的鍵変更が求められるのと同様に定期的パスワード変更が必要となるが、そのようなプロトコルは使われていないので、共通鍵と同じ理由で変更が必要になるわけではない。

③ 使用によりパスワードが劣化する通信プロトコルを用いているとの誤解

旧式の通信プロトコルが用いられていた時代に必要とされていた対策を今現在も必要とされていると考えてしまう誤解である。

1990 年代に設計された通信プロトコルには、パスワードの送信に当たって一方向性関数（暗号論的ハッシュ関数）を用いるチャレンジ・レスポンス方式を用いたものが多い。例として、電子メールの受信に用いられる「APOP」、電子メールの送信に用いられる「CRAM-MD5」などがある。これらの方式では、盗聴者は、「チャレンジ」と「レスポンス」（レスポンスは、チャレンジにパスワードを連結させた文字列にハッシュ関数を通したもの）を傍受し、これをもとに「総当たり攻撃」することにより、パスワードを復元できる可能性がある。このような攻撃は「オフライン攻撃」と呼ばれる。

ハッシュ関数は高速に計算することができるため、1 秒に数百万回といった高速な試行が可能であり、例えば、8 文字のランダムな英数字（62 文字種）の場合、300 万回/秒で試行した場合、2 年 4 か月で全部を総当りすることができる計算になる。したがって、この期間より十分に早く定期的にパスワードを変更することで、不正利用を防止できる。この意味においてはパスワードの定期的な変更は有効と言える。

しかし、TLS(SSL)が普及した今日では、チャレンジ・レスポンス方式は使われなくなった（POP over TLS や、SMTP over TLS に取って代わられた）か、または、使われているとしてもその外側で TLS(SSL)による暗号化が行われていて（APOP over TLS など）、チャレンジとレスポンスを傍受できなくなっている。TLS(SSL)による暗号化通信では、公開鍵暗号方式を用いた鍵交換により共通鍵暗号の鍵が接続ごとに毎回変更されており、同じパスワードを繰り返し送信しても、パスワードの手がかりになる情報は 1 ビットも漏れない。このため、TLS(SSL)が普及した今日では、このような意味でのパスワードの定期的変更の必要性は消滅し、過去のものとなっている。

- **基本対策事項 6.1.1(1)-3「利用者に対して定期的な変更を促す機能」について**

定期的な変更の要求を行う場合は、システムで自動化できることが望ましいが、技術

的に困難な場合には、定期的に変更依頼を通達するなどの運用によって対処してもよい。

遵守事項

(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。

【 基本対策事項 】

＜6.1.1(2)(a)関連＞

6.1.1(2)-1 情報システムセキュリティ責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下本項において同じ。）すること。

6.1.1(2)-2 情報システムセキュリティ責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずること。

a) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

b) 主体への識別コードの付与に関する記録を消去する場合の情報セキュリティ責任者からの事前の許可

6.1.1(2)-3 情報システムセキュリティ責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ**安全な方法で主体認証情報を配布する**よう、措置を講ずること。

6.1.1(2)-4 情報システムセキュリティ責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。

6.1.1(2)-5 情報システムセキュリティ責任者は、知識による主体認証方式を用いる場合には、**他の情報システムで利用している主体認証情報を設定しない**よう主体に注意を促すこと。

6.1.1(2)-6 情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず**共用識別コードを付与する必要がある場合**には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。

＜6.1.1(2)(b)関連＞

6.1.1(2)-7 情報システムセキュリティ責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずること。

a) 当該主体の**識別コードを無効にする**。

b) 当該主体に交付した主体認証情報格納装置を返還させる。
c) 無効化した識別コードを他の主体に新たに発行することを禁止する。

（解説）

- **遵守事項 6.1.1(2)(a)「主体認証情報を適切に付与」について**

情報システムにおいて認証機能を統合している場合、各機器等の管理者権限を持つローカルアカウントは通常の運用では未使用となるが、その場合においてもデフォルトパスワードのままにせず、設定するパスワードについても同一の値にしないといった措置を講ずる必要がある。

なお、主体認証が必要となる場面が多岐にわたるような情報システムの場合、認証連携を適切に用いることにより、業務の効率化を図ることも考えられる。

- **基本対策事項 6.1.1(2)-3「安全な方法で主体認証情報を配布する」について**

利用者以外の者（情報システムの管理者等）が主体認証情報を設定する場合には、以下を例とする方法で、当該主体認証情報を安全な方法で利用者に配布する必要がある。

- 本人の電子メールアドレスに対し、必要に応じて、暗号化を施すことにより、主体認証情報を送付する。この際、暗号化された主体認証情報が添付された電子メールに復号するための鍵を同時に付すのは情報セキュリティ上、好ましくない。
- 本人の電子メールアドレスに対して主体認証情報を入手するためのウェブサイト及びパスワードを送付し、当該パスワードによる認証の上で当該ウェブサイトから主体認証情報をダウンロードする。
- 本人の住所に対して主体認証情報を運搬する。

- **基本対策事項 6.1.1(2)-5「他の情報システムで利用している主体認証情報を設定しない」について**

複数の情報システムにおいて共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に利用されるというリスクが発生する。機関等の管理下にない情報システムからの漏えいを防止することは不可能であるため、このような情報システムから主体認証情報が漏えいした場合の機関等の情報システムへの影響について考慮しておく必要がある。対策の例としては、他の情報システムで利用している主体認証情報を機関等の情報システムに設定しないよう注意喚起を表示する、識別コードを情報システム側で割り当てることで識別コードの共通利用を防止する、といった方法が考えられる。

- **基本対策事項 6.1.1(2)-6「共用識別コードを付与する必要がある場合」について**

共用識別コードは、その利用履歴だけでは利用者を特定できないため、情報セキュリティインシデントが発生した場合に、真相究明の支障となる可能性がある。この点を踏まえ、やむを得ず、共用識別コードを利用する場合には、利用者を特定するための以下を例とする仕組みを講ずる必要がある。

- 当該情報システムにおける別途の認証手段を併用する
- 入退室管理装置等の物理的認証手段を併用する

- **基本対策事項 6.1.1⑵-7 a)「識別コードを無効にする」について**

  識別コードの付与を最小限に維持するため、退職等により不必要となった識別コードについては、これを無効にする必要がある。また、本人からの届出による場合のほか、人事異動等の時期を考慮の上、定期的及び必要に応じて不要な識別コードが存在しないことを確認することにより、無効化漏れを防止することが期待できる。

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。

【 基本対策事項 】

＜6.1.2(1)(a)関連＞

6.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。

a) 利用時間や利用時間帯によるアクセス制御

b) 同一主体による複数アクセスの制限

c) IP アドレスによる端末の制限

d) ネットワークセグメントの分割によるアクセス制御

e) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

（解説）

- **基本対策事項 6.1.2(1)-1「主体の属性、アクセス対象の属性に基づくアクセス制御」について**

具体的な手法としては､端末や共有フォルダ上のファイルやフォルダ(ディレクトリ)に対する許可属性のリストであるアクセス制御リスト（ACL： Access Control List）が挙げられる。ACL では例えば、アクセス対象の所有者／所有者の属するグループ／全利用者といったアクセス主体に対して、読み取り／書き込み／実行の権限を設定する。

ただし､一般的な情報システムでは､利用者が適切なアクセス制御の設定を行っても、システムの管理者は全てのファイルやフォルダへアクセス可能である。実際に、運用保

守の担当者が、管理者権限相当のアクセス権限を行使して、機密性の高い情報を不正に閲覧するといった事案も確認されている。そのため、アクセス対象が要機密情報等の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等されないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。

- **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**

  業務や取り扱う情報の性質・量に応じて、重要な情報に攻撃が到達しないよう、情報システムの重要な情報を取り扱う部分を他の情報システムやインターネットから分離するといった対策をとる必要がある。特に、情報システムの管理を行う部分を独立したセグメントとし、これをインターネットから切り離しておくことは、攻撃の拡大阻止の観点から有効である。同時に、セグメント分割の意義を損なうことのないよう、各システムで取り扱うことができる情報についてルール化し、職員等に徹底することも重要である。

  なお、遵守事項 5.2.1(2)(a)において、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について判断を求めているが、本基本対策事項は、その際に併せて検討し、情報システムのネットワーク構成の要件を決定するとよい。

- **基本対策事項 6.1.2(1)-1 e)「ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御」について**

  ファイル自体にセキュリティ機能を組み込むことで、ファイルに対する閲覧、編集、印刷等の操作を制御する技術（DRM(Digital Rights Management)やIRM(Information Rights Management)として知られるデジタル著作権管理技術）を利用することも考えられる。この技術を利用したファイルは暗号化されるため、ファイルを利用するには、ファイルに記録された情報へのアクセスを制御するサーバで主体認証を受け、正当な主体として認識されること及びファイルへのアクセス権限が付与されていることが必要となる。そのため、第三者がファイルを閲覧しようとしても、主体認証を受け、正当な主体として認識されない限り当該ファイルの内容を参照することはできず、ファイルに記録された情報の漏えいを防止することができる。

  また、ファイル利用時には、利用者はファイルの暗号化・復号を意識することなく、付与されたアクセス権限に従った閲覧、編集、印刷等の操作を行えるため、利便性が損なわれることはない。

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。

【 基本対策事項 】

＜6.1.3(1)(b)関連＞

6.1.3(1)-1 情報システムセキュリティ責任者は、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、以下を例とする措置を講ずること。

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

（解説）

- **遵守事項 6.1.3(1)(b)「内部からの不正操作や誤操作を防止するための措置」について**

  権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、複数名による主体認証操作がなければ、その処理自体を完遂できない「デュアルロック機能」を導入することが考えられる。

  その他の情報システムについては、操作ログを取得したり、確認画面を表示したりするなどの措置が考えられる。

- **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**

  管理者権限等の特権は、システム全体へのアクセス権を持ち、あらゆる操作が可能であることが多く、仮に不正な目的を有する悪意ある第三者等が当該権限を入手すれば、当該システムに対して不正な操作が可能となってしまう。必要最小限の権限のみ付与とは、権限が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な権限を付与することにより、当該権限を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。

  例えば、管理作業をするときに限定してその識別コードを利用することを可能とする方式（例 Unix 系システムにおける sudo 等）や、あらかじめ実行できるプログラムやアクセス可能な領域を限定し、権限を付与する方式がある。

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。

【 基本対策事項 】

＜6.1.4(1)(a)関連＞

6.1.4(1)-1 情報システムセキュリティ責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の**時刻を同期**させ、ログに時刻情報も記録されるよう、設定すること。

＜6.1.4(1)(b)関連＞

6.1.4(1)-2 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特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

a) 事象の主体（人物又は機器等）を示す識別コード
b) 識別コードの発行等の管理記録
c) 情報システムの操作記録
d) **事象の種類**

e) **事象の対象**
f) 正確な日付及び時刻
g) 試みられたアクセスに関わる情報
h) 電子メールのヘッダ情報及び送信内容
i) 通信パケットの内容
j) 操作する者、監視する者、保守する者等への通知の内容

6.1.4(1)-3 情報システムセキュリティ責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、**ログ情報の保全方法**を定めること。

6.1.4(1)-4 情報システムセキュリティ責任者は、ログが取得できなくなった場合の対処方法を定めること。

＜6.1.4(1)(c)関連＞

6.1.4(1)-5 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。

a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の**自動化**

（解説）

- **遵守事項 6.1.4(1)(b)「ログを取得する目的」について**

情報システムにおいて出力できる様々なログは、その全てを無期限に保存し、定期的にその点検や分析を行うことができれば理想的であるが、そのためには莫大なストレージ容量が必要になり、解析にかかる時間も長くなるなど、現実的ではない。

そのため、情報システムの特性（取り扱われる情報、接続されるネットワーク、設置環境、利用者等）に応じ、当該情報システムでどのような事象を検知すべきかを目的として設定した上で、取得すべきログ情報やその保存期間等を検討することが望ましい。

例えば、標的型攻撃の早期発見・初期調査を目的とした場合には、以下のようなログを取得することが考えられる。

- 電子メールサーバ： 電子メールクライアントで表示される表記名*、送信者アドレス*、実際の電子メール送信者アドレス*、添付ファイル名*
- ファイアウォール： ファイアウォールポリシーのアクション、送信先のゾーン設定*、送信元アドレス、送信元ポート、送信先アドレス、送信先ポート
- Web プロキシサーバ： リクエスト受信時刻、URL、リモートホスト、メソッド、UserAgent*、プロキシ認証のユーザ ID*、通信データサイズ（送信、受信）、ステータスコード
- DNS キャッシュサーバ： 名前解決を行おうとしている PC 等の IP アドレス*、要求及び応答したホストや IP アドレスの情報*
- 認証サーバ（Active Directory）： 資格認証の確認の監査*、Kerberos 認証サービスの監査*、ログオンの監査*、その他ログオン／ログオフイベントの監査*、

特殊なログオンの監査*

- DHCP サーバ：　IP アドレス割り当て・リリースログ

その他、Web サイトからの情報窃取や改ざんの早期発見・初期調査を目的とした場合には、以下のようなログを取得することが考えられる。

- Web サーバ：　アクセスログ（リモートホスト、リモートポート*、リクエスト受信時刻。TLS（SSL）アクセスログを含む。）
- アプリケーションサーバ：　既製の CMS 等のソフトウェア及び独自開発アプリケーション等のログ（アクセスログ*、認証ログ*、操作ログ*）
- データベースサーバ：　データベースソフトウェアのログ（アクセスログ*、クエリログ*)
- 各サーバ共通（OS レベル）：　認証ログ（成功*、失敗）、Windows の場合はイベントログ、プロセスログ*、Linux の場合はセキュリティログ
- ロードバランサー、リバースプロキシ：　IP アドレスを含む接続元ログ
- ファイアウォール：　DMZ からのアウトバウンド通信に関するログ*

なお、上記のログの例において、項目名の終わりに*を付与しているログ項目は各機器の標準設定では出力されない場合があるため、注意が必要である。

- **遵守事項 6.1.4(1)(b)「保存期間」について**

保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、ログの長期保存にはコストがかかるため、費用を抑える観点から、直近のログはすぐに調査可能なハードディスク等のオンラインの電磁的記録媒体に保存し、それ以降はテープや光ディスク等の長期保存に適した外部電磁的記録媒体に保存する方法も考えられる。オンラインの電磁的記録媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

- **遵守事項 6.1.4(1)(b)「ログが取得できなくなった場合の対処方法」について**

以下を例とする対処方法が考えられる。

- 古いログに上書きする設定を施し、ログの取得を継続する。
- ログが取得できなくなった際に出力されているメッセージ、エラーコード等を確認し、障害の原因を特定すると同時に当該障害の原因の対処を実施する。
  なお、情報システムにおいて、事前に収集したログのバックアップ設定を行っている場合は、復旧手順に従い、速やかにログを復旧させる。このとき、復旧するバックアップの古さの目標値を示す RPO（Recovery Point Objective）は情報システムの特性及び取り扱う情報によって、適切に設定する必要がある。
- あらかじめ用意したファイル容量を使い切った場合、情報システムに対する挙動がログに保存されないため、一旦情報システムを停止し、ファイル容量を新たに用意するなどした後に、ログの取得を再開する。

- **遵守事項 6.1.4(1)(c)「点検又は分析」について**

  情報システムの特性等に応じて、点検・分析の頻度や分析の精度を高める必要がある場合には、専任の分析担当者の設置や監視事業者への委託を検討することが考えられる。

- **基本対策事項 6.1.4(1)-1「時刻を同期」について**

  具体的な実装例としては、ログを取得する機器のシステム時刻を、タイムサーバを用いて同期する方法がある。タイムサーバは、NTP（Network Time Protocol）や SNTP（Simple Network Time Protocol）等の方式により、ネットワーク上のクライアント機器に対して、時刻を提供する。例えば、公開 NTP サービスを用いる方式や組織内にタイムサーバを設置し、サーバ装置・端末・通信回線装置をタイムサーバに時刻同期するよう設定する方式が挙げられる。後者については、タイムサーバを複数利用することにより、時刻の精度や冗長性を高めることができる。

  また、機器によっては明示的に設定を行わないとログに出力する時刻が現地時間とならない場合があるため注意が必要である。

- **基本対策事項 6.1.4(1)-2 d)「事象の種類」について**

  事象の種類の例を以下に示す。

  - ウェブサイトへのアクセス
  - ログイン及びログアウト
  - サーバ、ファイルへのアクセス
  - 要保護情報の書き出し
  - アプリケーションの起動及び終了
  - 特定の操作指令

- **基本対策事項 6.1.4(1)-2 e)「事象の対象」について**

  事象の対象の例を以下に示す。

  - アクセスした URL
  - ログインしたアプリケーション名
  - アクセスしたファイル名及びファイル操作内容
  - 起動及び終了したアプリケーション名及びパス
  - 特定の操作指令の対象

- **基本対策事項 6.1.4(1)-3「ログ情報の保全方法」について**

  取得したログ情報に対する不正な消去、改ざん及びアクセスを防止するためのログ情報の保全方法として、以下の例が考えられる。

  - ログ収集サーバにログを転送し保存する。ログ収集サーバの管理者を他のサーバ等の管理者と異なる者とし、他の管理者によるログ情報の消去や改ざんが行われないようにする。
  - ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保管する。
  - ログを書き換え不能な外部電磁的記録媒体（DVD-R 等）に書き出して保管する。

- **基本対策事項 6.1.4(1)-5 a)「自動化」について**

  ログとして取得する項目数、利用者数等が多くなるにつれて、ログの量は膨大になり、システム担当者等がログを目視することによって問題(又はその予兆)を検出するのは、困難を極める。システム自体に実装される機能や各種運用管理ツールを組み合わせ、ログの点検・分析・通知が自動的に実行されるなど、ログ管理作業を支援する仕組みを構築することが望ましい。

6.1.5 暗号・電子署名

目的・趣旨

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

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

遵守事項

(1) 暗号化機能・電子署名機能の導入

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

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

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

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

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

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、**やむを得ない場合**を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

(ウ) 暗号化及び電子署名に使用する**アルゴリズムが危殆化**した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、**管理手順を定めること**。

(c) 情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な**電子証明書を政府認証基盤（GPKI）が発行している**場合は、それ

を使用するように定めること。

【 基本対策事項 】

＜6.1.5(1)(a)関連＞

6.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、**暗号モジュールを交換**することが可能な構成とする。

b) **複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択**することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、**「暗号モジュール試験及び認証制度」に基づく認証**を取得している製品を選択する。

d) 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は、**耐タンパ性**を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、**安全性に実績のあるプロトコル**を選択し、**長期的な秘匿性**を保証する観点を考慮する。

（解説）

- **遵守事項 6.1.5(1)(b)(イ)「やむを得ない場合」について**

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おいては、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則であるが、連携する他の情報システム側で対応していないなどの場合も想定される。このような場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用することもやむを得ないと考えられるが、「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、安全性が高いアルゴリズムを採用することが必要である。

- **遵守事項 6.1.5(1)(b)(ウ)「アルゴリズムが危殆化」について**

暗号化や電子署名に用いられる暗号アルゴリズムは、年月が経つにつれ、情報システムの処理能力の向上や新たな暗号解読技法の考案等によって、アルゴリズム設計当初の強度を失い、結果として、安全性を保てなくなる。このことを一般に「アルゴリズムが危殆化する」という。

暗号アルゴリズムの強度には理論上の強度及び実装上の強度が存在する。理論上の強度の低下は情報システムの処理能力の向上や暗号解読法の考案によるところが大きく、実装上の強度の低下はサイドチャネル攻撃等の攻撃技術によるところが大きい。サイドチャネル攻撃の例として、実装時に暗号アルゴリズムの動作に伴う消費電力や暗

号モジュールから漏えいする電磁波等の付加的な情報を悪意ある第三者等が知り得る場合には、実装上の強度は極端に低下する可能性がある。

- **遵守事項 6.1.5(1)(b)(エ)「管理手順を定めること」について**

  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（以降本条において「鍵」という。）の管理手順として、以下の視点を含む鍵のライフサイクルを考慮した管理手順を策定するとよい。また、暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、適切に管理する必要がある。

  - 鍵の生成
    適切な暗号モジュールの内部において、その値を推定することが困難である乱数又は擬似乱数に係る処理を通じて生成し、かつ利用者以外の者が入手できないことを保証する仕組みが必要である。
  - 鍵の配送
    鍵の受取先と事前に対面等で確認し合うなどにより、受取先の正当性に係る十分な確証が得られない限り、オンライン上での鍵の配送を行うべきではない。鍵を配送する際は、受取先のなりすまし対策等、配送先が確実であることを保証するとともに当該鍵に係る情報が適切に保護される仕組みが必要である。
  - 鍵の保管
    鍵は、例えば HSM 等の保存装置又は記録媒体等に適切に保護された環境で保管され、第三者等による窃取の防止に加え、改ざんからの保護、検知及び回復を実現する仕組みを備えることが必要である。
  - 鍵の利用
    鍵はその運用期限が有効な限り、当該鍵へのアクセスが取扱いの許可されたものだけに限定されるよう可用性が確保され、かつ適切に実装された上で利用することが必要である。
  - 鍵の期限切れ
    有効期限を過ぎた鍵は使用を停止し、適切な手段で取り除かれることが必要である。
  - 鍵の更新
    鍵の有効期限が終了した後も運用を継続する場合、鍵としての継続性を維持するため、基本的に有効期限の終了前に古い鍵のパラメータを基に、新たな鍵を生成することが望ましい。
    なお、古い鍵は適切に廃棄されることが必要である。
  - 鍵の失効
    鍵の漏えいによる危殆化や、鍵を利用していた職員等が組織から離れることに伴う鍵の登録抹消等により、そのコピーやバックアップが存在する場合も含め、有効期限前の鍵の利用を適切に停止することが必要である。
  - 鍵の廃棄
    特別な理由を除き、不要となった鍵の情報はそのコピーやバックアップが存在

する場合も含め、有効期限後に適切な物理的又は電磁気学的な消去方法を用いて確実に消去される仕組みが必要である。

- **遵守事項 6.1.5(1)(c)「電子証明書を政府認証基盤（GPKI）が発行している」について**

  GPKI 以外が発行するサーバ証明書、コード署名証明書等の電子証明書が有効期限内であって GPKI を適用可能な場合、次期更新時には、GPKI で発行している電子証明書を利用することが求められる。一方で、保健医療福祉分野の公開鍵基盤（HPKI）のように特定の分野における公的な PKI が存在し、その使用が求められる場合には、当該 PKI を使用しても差し支えない。

- **基本対策事項 6.1.5(1)-1 a)「暗号モジュールを交換」について**

  暗号モジュールは、暗号化、電子署名、ハッシュ関数等の暗号に関連した機能を提供するソフトウェアの集合体又はハードウェアとして定義される。選択した暗号化アルゴリズムが将来危殆化することを想定し、暗号モジュールの交換が可能な構成とすることを、情報システムの設計段階から考慮する必要がある。

  また、あらかじめ暗号モジュールのアプリケーションインタフェースを統一しておくなどを考慮する必要がある。

- **基本対策事項 6.1.5(1)-1 b)「複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択」について**

  選択したアルゴリズムが将来危殆化することを想定し、危殆化していない他のアルゴリズムへ直ちに変更できる機能と併せて、暗号利用モード等との組合せ等により脆弱性の顕在化が認められない安全なプロトコルを選択できる機能も、あらかじめ情報システムに設けておく必要がある。

- **基本対策事項 6.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について**

  アルゴリズム自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する疑似乱数に偏りが生じるなどの理由で疑似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生じるなどの理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがあることから、これらを確認するには、ISO/IEC 19790 に基づく「暗号モジュール試験及び認証制度」が利用可能である。

- **基本対策事項 6.1.5(1)-1 d)「耐タンパ性」について**

  JIS X 19790 (ISO/IEC 19790)の規定によると、耐タンパ性は以下の３つの機能から構成される。

  - タンパ検出
    暗号モジュールのセキュリティを危殆化する試みがなされたことの、暗号モジュールによる自動的な判定
  - タンパ証跡
    暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、外観

上の表示

- タンパ応答

  暗号モジュールがタンパを検出したときにとる自動的な動作

また、暗号モジュールを利用する環境等に応じ、セキュリティレベルが１から４まで設定されている。セキュリティレベル１は、最小限の物理的保護を要求している。セキュリティレベル２では、タンパ証跡メカニズムの追加を要求している。セキュリティレベル３では、除去可能なカバー及びドアに対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。セキュリティレベル４では、囲い全体に対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。

なお、タンパ検出及びタンパ応答は、タンパ証跡の代わりにはならない。

暗号モジュールの耐タンパ性に関わるセキュリティレベルは、情報システムが取り扱う以下の特性を踏まえて選択することが望ましい。

- 暗号化又は復号する情報の特性
- 電子署名が付与される情報の特性

- **基本対策事項 6.1.5(1)-1 e)「安全性に実績のあるプロトコル」について**

情報システムで暗号を用いるとき、暗号アルゴリズムの適切な選択に加え、暗号プロトコル（暗号アルゴリズムをどのように用いるかの手順）が適切なものとなっている必要がある。一般に、情報システムを新規に構築するときに、独自の暗号プロトコルを設計することは、その安全性について十分に検証されないときは、期待される安全性が確保されていない可能性がある。安全な暗号プロトコルの設計は高度な専門性を有する者以外には容易なことではないため、可能な限り、独自の設計を避け、既に広く利用実績のある著名な暗号プロトコルを用いることが求められる。

なお、必要とする機能を実現する暗号プロトコルとして既存のものが存在しない場合はこの限りでないが、独自に暗号プロトコルを設計するときは、その安全性に関して十分に検証する必要がある。

- **基本対策事項 6.1.5(1)-1 e)「長期的な秘匿性」について**

情報システム上で機微な情報のやり取りを行う場合、情報を暗号化して通信しても、その暗号文が悪意ある第三者等に傍受され、将来の解読に備えて長期間にわたり保管されるという脅威が想定される。この場合に、「前方秘匿性（Forward Secrecy）」を有しない暗号プロトコルを用いた結果、公開鍵暗号の鍵が将来破られることになれば、過去に遡って全ての暗号文が解読されてしまうことになる。そのため、長期の機密性を確保する必要のある機微な情報のやりとりを行う情報システムを構築するときは、「前方秘匿性」を実現する暗号プロトコルの採用を検討し、必要かつ可能であれば、採用することが求められる。

遵守事項

(2) 暗号化・電子署名に係る管理

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

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

(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図ること。

【 基本対策事項 】

＜6.1.5(2)(a)(ア)関連＞

6.1.5(2)-1 情報システムセキュリティ責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。

a) 信頼できる機関による電子証明書の提供

b) 機関等の窓口での電子証明書の提供

（解説）

- **基本対策事項 6.1.5(2)-1 a)「信頼できる機関による電子証明書の提供」について**

  例えば、信頼できる機関のサイトから、利用者が電子署名を検証するための電子証明書をダウンロードできるように環境を整備する方法である。利用者はダウンロードした電子証明書を端末に取り込み、それを基に署名検証を行う。

- **基本対策事項 6.1.5(2)-1 b)「機関等の窓口での電子証明書の提供」について**

  機関等において、利用者に電子署名を検証するための電子証明書を電磁的記録媒体で配布する方法である。利用者は電磁的記録媒体経由で電子証明書を端末に取り込み、それを基に署名検証を行う。

6.2 情報セキュリティの脅威への対策

6.2.1 ソフトウェアに関する脆弱性対策

目的・趣旨

機関等の情報システムに対する脅威としては、第三者が情報システムに侵入し機関等の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、国民向けに提供するサービスが第三者に侵入され、個人情報等の重要な情報の漏えい等が発生した場合、国民生活に多大な影響を及ぼすとともに機関等に対する社会的な信用が失われる。

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

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

(1) ソフトウェアに関する脆弱性対策の実施

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

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

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

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

【 基本対策事項 】

＜6.2.1(1)(a)(c)関連＞

6.2.1(1)-1 情報システムセキュリティ責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む**情報を適宜入手**すること。

a) 脆弱性の原因
b) 影響範囲
c) 対策方法
d) **脆弱性を悪用する不正プログラムの流通状況**

6.2.1(1)-2 情報システムセキュリティ責任者は、利用するソフトウェアは**サポート期間を考慮**して選定し、**サポートが受けられないソフトウェア**は利用しないこと。

6.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする手段で脆弱性対策の状況を確認すること。

a) 構成要素ごとに**ソフトウェアのバージョン等を把握**し、当該ソフトウェアの脆弱性の有無を確認する。
b) **脆弱性診断**を実施する。

＜6.2.1(1)(c)関連＞

6.2.1(1)-4 情報システムセキュリティ責任者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くすること。

＜6.2.1(1)(d)関連＞

6.2.1(1)-5 情報システムセキュリティ責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。

a) 対策の必要性
b) 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法を予め決定すること
c) 対策方法が存在しない**ゼロデイ**と呼ばれる状態の場合又は対策が完了するまでの期間に対する**一時的な回避方法**
d) 対策方法又は回避方法が情報システムに与える影響
e) 対策の実施予定時期
f) **対策試験**の必要性
g) 対策試験の方法
h) 対策試験の実施予定時期

6.2.1(1)-6 情報システムセキュリティ責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認すること。

6.2.1(1)-7 情報システムセキュリティ責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

a) 実施日
b) 実施内容
c) 実施者

6.2.1(1)-8 情報システムセキュリティ責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「**対策用ファイル**」という。）は、信頼できる方法で入手すること。

（解説）

- **遵守事項 6.2.1(1)(b)「公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策」について**

  脆弱性が明らかになっていない段階においても、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施する。対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施すること等が挙げられる。

- **遵守事項 6.2.1(1)(c)「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」について**

  情報システムの構築時に、ソフトウェアを効率的に開発するためにソフトウェアフレームワーク開発用のフレームワークとして情報システムに組み込まれたまま納入されるソフトウェア等、情報システムの運用中に動作しないものについても考慮する必要がある。また、ソフトウェアには外部から入手するもののみでなく、機関等が自ら開発するもの及び委託により開発するものについても含まれる。当該ソフトウェアの脆弱性による影響についても考慮し、脆弱性対策の対象とするソフトウェアを定めておくことが望ましい。

- **基本対策事項 6.2.1(1)-1「情報を適宜入手」について**

  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上で利用するソフトウェアの脆弱性に関する情報は、製品ベンダや脆弱性情報提供サイト等を通じて適時調査を行う必要がある。自動アップデート機能を持つソフトウェアの場合には、当該機能を利用して、定期的に脆弱性に関連する情報が報告されているかを確認する方法で差し支えないが、自動アップデート機能の対象範囲を把握し、対象範囲外のソフトウェアについては適時調査を行う必要がある。例えば、ウェブアプリケーション等のソフトウェアを効率的に開発するためにソフトウェアフレームワークを利用する場合があるが、ソフトウェアフレームワークを利用して開発したアプリケーションは自動アップデートが行えないため、脆弱性の有無については適宜調査を行う必要がある。

  入手した脆弱性に関連する情報及び対策方法に関しては、脆弱性対策を効果的に実施するために、他の情報システムセキュリティ責任者と共有することが望ましい。

- **基本対策事項 6.2.1(1)-1 d)「脆弱性を悪用する不正プログラムの流通状況」について**

  脆弱性が既知になると、インターネット上の情報交換コミュニティ等を通じて、その脆弱性を悪用する方法が考案され、その悪用方法を機械的に実行するための不正プログラム（exploit コードとも呼ばれる）が作られ、次第に広まっていく。この「脆弱性を悪用する不正プログラム」が流通している段階に入ると、脆弱性が攻撃されるリスクが格段に高まると考えられる。脆弱性を悪用する不正プログラムが世の中に流通していることが確認された場合には、速やかに当該の脆弱性について対処することが望ましい。

- **基本対策事項 6.2.1(1)-2「サポート期間を考慮」について**

  利用するソフトウェアのサポート期間が過ぎた場合、それ以降はセキュリティ関連

の脆弱性を修正するためのセキュリティパッチは、原則としてソフトウェアベンダから提供されなくなる。したがって、情報システムのライフサイクルを考慮し、少なくとも情報システムの次期改修までは対策用ファイルの提供が継続されるソフトウェアを選定する必要がある。

また、情報システムは特定のソフトウェアバージョンに依存しないよう設計することが望ましいが、情報システムの中には、特定のソフトウェアバージョンに強く依存する場合がある。この場合には、ソフトウェアをバージョンアップすることが困難となるが、新しいバージョンのソフトウェアでしか対処できない脆弱性が発生したときに、情報システムの停止という最悪の事態も想定される。したがって、情報システムが特定のソフトウェアバージョンに依存せざるを得ない場合には、当該ソフトウェアのサポート期間を考慮して情報システムの更改について検討しておく必要がある。

- **基本対策事項 6.2.1(1)-2「サポートが受けられないソフトウェア」について**

ソフトウェアベンダによるサポートや他の事業者によるサポートサービスが一切受けられないものを対象としている。ソフトウェアベンダの製品ロードマップの見直し等により、サポートの打ち切りが突然予告されることもあり得るため、利用するソフトウェアのサポート期間に関する情報を適時入手し、ソフトウェア更改やサポート事業者の切替え等の対策が適切に講じられるよう考慮することが望ましい。

- **基本対策事項 6.2.1(1)-3 a)「ソフトウェアのバージョン等を把握」について**

ソフトウェアのバージョン等の把握については、「(解説) 基本対策事項 5.1.1(2)-1 b)・基本対策事項 5.1.1(2)-3 b)「機種並びに利用しているソフトウェアの種類及びバージョン」について」及び「(解説) 基本対策事項 5.1.1(2)-1 c)「ソフトウェアを動作させるために用いられる他のソフトウェア」について」を参照のこと。

例えば、外部から入手した脆弱性情報が世の中で大きな被害をもたらしているような緊急性の高い場合には、情報システムにおける該当する脆弱性の有無の確認を運用保守業者に作業を委託するのみでなく、情報システムセキュリティ責任者自らも情報セキュリティ関連文書を参照し確認することが望まれる。

- **基本対策事項 6.2.1(1)-3 b)「脆弱性診断」について**

OS や各種サーバ、ファイアウォール等の通信回線装置等における脆弱性対策の状況を効率的に確認する方法として、専用ツールを用いて機関等自らが脆弱性診断を行ったり、事業者が提供するサービス等を利用して脆弱性診断を行うことが挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。

ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。

プラットフォーム診断では、OS や各種サーバ、ファイアウォール等を対象に、テス

ト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に１回診断を実施するなど、定期的に実施することが望ましい。

ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信するなどの方法によって、SQL インジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ましい。

- **基本対策事項 6.2.1(1)-5 c)「ゼロデイ」について**

発見されたソフトウェアの脆弱性を解消する手段が公開されておらず、脅威にさらされている状態を「ゼロデイ」という。

- **基本対策事項 6.2.1(1)-5 c)「一時的な回避方法」について**

ソフトウェアにおいて脆弱性が顕在化した際に、ソフトウェアベンダが対応するまでの間は、当該ソフトウェアの利用を禁止する、脆弱性が関係する機能を無効化する、ファイアウォール、WAF（Web Application Firewall）等により当該ソフトウェアへの通信を制限するなどの対応が必要となる。

しかし、これらの対応によって業務に著しく悪影響を与えることが想定される場合は、事前に必要な措置を講じておくことが求められる。例えば、ブラウザは業務上利用せざるを得ないケースが多いが、異なるソフトウェアベンダが提供する複数のブラウザを、端末にあらかじめ導入しておくことで、業務継続性を維持しつつ、脆弱性を悪用した攻撃を受けるリスクを低減することができる。複数のブラウザを導入することは、情報システムのコスト増加を招く可能性があるが、一方のブラウザを常時利用するとともに、他方を緊急時のインターネットへのアクセス手段として利用するなど、用途を分ける方法も考えられる。また、ログ出力の設定を確認し、対応が完了するまでの期間、出力されたログの監視を強化するなどの対応も考えられる。

- **基本対策事項 6.2.1(1)-5 f)「対策試験」について**

「対策試験」とは、脆弱性対策の実施による情報システムへの影響の有無を確認するために、事前に試験用の情報システムを用いて試験することが想定される。

- **基本対策事項 6.2.1(1)-8「対策用ファイル」について**

入手した対策用ファイルに悪意のあるコードが含まれている可能性を考慮し、対策用ファイルは信頼できる方法で入手する必要がある。

信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからダウンロードする方法、又は郵送により対策用ファイルが記録された外部電磁的記録媒体を入手する方法が挙げられる。また、対策用ファイルが改ざんされていないこと等の完全性を検証できる手段があれば、併せてこれを実行する必要がある。

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。

【 基本対策事項 】

＜6.2.2(1)(a)関連＞

6.2.2(1)-1 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ソフトウェア等の導入に当たり、**既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する**ソフトウェアを導入すること。

6.2.2(1)-2 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ソフトウェア等が常に最新の状態となるように構成すること。

6.2.2(1)-3 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態なるように構成すること。

6.2.2(1)-4 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ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

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ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

＜6.2.2(1)(b)関連＞

6.2.2(1)-6 情報システムセキュリティ責任者は、想定される全ての**感染経路を特定**し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機

能の無効化等による感染拡大の防止等の必要な対策を行うこと。

＜6.2.2(1)(c)関連＞

6.2.2(1)-7 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

（解説）

- **遵守事項 6.2.2(1)(a)「動作可能な不正プログラム対策ソフトウェア等」について**

不正プログラム対策ソフトウェアの例としては、コンピュータウイルスを検知対処する「ウイルス対策ソフトウェア」や、キーロガーやアドウェア等のいわゆるスパイウェアを検知対処する「スパイウェア対策ソフトウェア」等がある。

多くのメインフレームシステム並びに OS 及びアプリケーションを搭載していないサーバ装置及び端末については、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ため、本条の対象外である。ただし、新たに動作可能な不正プログラム対策ソフトウェア等が出現した場合には、速やかな導入が求められることから、情報システムセキュリティ責任者は、該当するサーバ装置及び端末の把握を行っておくとともに、不正プログラム対策ソフトウェア等に関してベンダが提供するサポート情報に常に注意を払っておくことが望ましい。

また、新たな不正プログラムの存在が明らかになった後でも、利用中の不正プログラム対策ソフトウェア等に用いる定義ファイルがベンダから配布されないなど、日常から行われている不正プログラム対策では対処が困難と判断される場合、情報システムセキュリティ責任者は職員等に回避策の実施を指示する必要がある。

なお、回避策は一律ではなく、個々の状況によって様々な内容があり得る。例えば、インターネット上の一部のウェブサイトを閲覧すると不正プログラムに感染することが判明している場合に、不正プログラム対策ソフトの定義ファイルが対応するまでの間、一時的にインターネット閲覧を制限する、という回避策が想定される。

- **基本対策事項 6.2.2(1)-1「既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する」について**

既知の不正プログラムについては、不正プログラム対策ソフトベンダにより、その不正プログラムに関するシグネチャが対策ソフトの定義ファイルに反映されることにより感染を防止することができる。一方で、標的型攻撃等の攻撃手法においては、不正プログラムのソースコードを部分的に改変する亜種や、ソフトウェアの新たな脆弱性を突く不正プログラムなど、不正プログラム対策ソフトウェア等の検知を回避しようとする攻撃が多く見られる。

このような未知の不正プログラムの検知及び感染防止への対応として、ソフトウェアの脆弱性への適切な対策に加えて、シグネチャにより検知する方式以外の手法を用いる製品やサービスを導入することの重要性も高まっている。例えば、シグネチャに依

存せずに OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、攻撃にスクリプト等を使用するファイルレスマルウェアの対策としても効果が期待できる。その他にも、サンドボックス、ふるまい検知等の技術があり、必要に応じこれら複数の検知方式の組み合わせにより、不正プログラムの検知精度を向上させることで、端末及びサーバ装置に対する不正プログラム感染リスクの低減を図ることも可能となる。

なお、不正プログラム対策ソフトウェア等の選定に当たっては、ソフトウェアの稼働によって端末及びサーバ装置への負荷が増加し、業務に影響を与えるおそれがあること等も勘案した上で判断する必要がある。

- **基本対策事項 6.2.2(1)-6「感染経路を特定」について**

不正プログラムの感染経路には、電子メール、ウェブ等のネットワーク経由のほか、不正プログラムに感染したモバイル端末の機関等支給回線への直接接続や外部電磁的記録媒体の経由も考えられる。

不正プログラム対策ソフトウェア等は、製品ごとに検知方式や不正プログラム定義ファイルの提供時期及び種類が異なる。また、不正プログラム対策ソフトウェア等は現存する全ての不正プログラムを検知及び除去できるとは限らないほか、不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害を低減させるため、感染経路において、異なる定義ファイルを用いる不正プログラム対策製品を組み合わせる、又は定義ファイルパターンマッチングやふるまい検知等の異なる技術を用いる製品を組み合わせることにより、どれか一つの不具合で、その環境の全てが不正プログラムの被害を受けることのないようにすることが望ましい。例えば、電子メールサーバに導入する不正プログラム対策と端末に導入する不正プログラム対策について、それぞれ異なる検知技術を用いる製品を導入すること等が考えられる。

- **基本対策事項 6.2.2(1)-6「感染拡大の防止」について**

ネットワークを経由した感染拡大の防止策としては、例えば以下が挙げられる。

- OS やアプリケーションに関するセキュリティパッチ及び不正プログラム定義ファイルについて最新化されていない端末をネットワークに接続させない仕組みの導入
- 通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断する仕組みの導入

6.2.3 サービス不能攻撃対策

目的・趣旨

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

遵守事項

(1) サービス不能攻撃対策の実施

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

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

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

【 基本対策事項 】

＜6.2.3(1)(a)関連＞

6.2.3(1)-1 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について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

a) パケットフィルタリング機能
b) 3-way handshake 時のタイムアウトの短縮
c) 各種 Flood 攻撃への防御
d) アプリケーションゲートウェイ機能

＜6.2.3(1)(b)関連＞

6.2.3(1)-2 情報システムセキュリティ責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。

6.2.3(1)-3 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に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。

a) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策
b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入
c) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

6.2.3(1)-4 情報システムセキュリティ責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。

＜6.2.3(1)(c)関連＞

6.2.3(1)-5 情報システムセキュリティ責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めること。

6.2.3(1)-6 情報システムセキュリティ責任者は、監視対象の監視記録を保存すること。

（解説）

- **遵守事項 6.2.3(1)(a)「サービス不能攻撃」について**

サービス不能攻撃は、DoS (Denial of Service)攻撃とも呼ばれる。また、この DoS 攻撃を複数の拠点から一か所に対して行う攻撃は、DDoS (Distributed Denial of Service) 攻撃と呼ばれ、攻撃元が複数に分散しているために防御側の対処が困難な攻撃として知られている。

- **基本対策事項 6.2.3(1)-3 a)「インターネットに接続している通信回線」について**

情報システムに対してサーバ装置、端末及び通信回線装置に係るサービス不能攻撃の対策を実施しても、機関等外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、インターネットに接続している通信回線の提供元となる事業者に確認した上で、サービス不能攻撃発生時の対処手順や連絡体制を整備する必要がある。

- **基本対策事項 6.2.3(1)-3 c)「冗長化」について**

冗長化の例としては、サービス不能攻撃が発生した場合に備え、サービスを提供するサーバ装置、端末、通信回線装置又は通信回線について、負荷を分散させる、又はそれぞれ代替のものに切り替えるなどにより、サービスを継続することができるように情報システムを構成することが考えられる。

なお、代替のものへの切替えについては、サービス不能攻撃の検知及び代替サーバ装置等への切替えが許容される時間内に行えるようにする必要がある。

- **基本対策事項 6.2.3(1)-4「攻撃への対処を効率的に実施できる手段」について**

対処例としては、サービス提供に利用している通信回線がサービス不能攻撃により過負荷状態に陥った場合においても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保することが挙げられる。具体的には、管理者が当該装置を操作するためのサーバ装置、端末及び通信回線を、サービス提供に利用しているものとは別に用意することが挙げられる。

また、サービス不能攻撃に伴い、機関等の自己管理ウェブサイトの閲覧障害が発生し

た場合においても、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力回避すべきである。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼし得るような重要情報については、広報担当とも協力するなどして、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなどの必要な措置を考慮するとよい。

- **基本対策事項 6.2.3(1)-5「監視方法及び監視記録の保存期間」について**

インターネットからアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する必要がある。

「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握や、システムの構成要素に対する負荷の定量的な把握(CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等)がある。監視方法は多種多様であるため、当該情報システムの構成等の特性に応じて適切な方法を選択する必要がある。

「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。

- **基本対策事項 6.2.3(1)-6「監視記録を保存」について**

サーバ装置、端末、通信回線装置及び通信回線を監視している場合、監視対象の状態は一定ではなく変動することが一般的である。時間変動、曜日変動、週変動、月変動、季節変動等を検討した上で記録を一定期間保存する。

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。

【 基本対策事項 】

＜6.2.4(1)(a)関連＞

6.2.4(1)-1 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ついて、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 不要なサービスについて機能を削除又は停止する。

b) 不審なプログラムが実行されないよう設定する。

c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

6.2.4(1)-2 情報システム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利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。

b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

c) サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。

d) サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

e) サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

f) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

＜6.2.4(1)(b)関連＞

6.2.4(1)-3 情報システムセキュリティ責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。

a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。

b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

6.2.4(1)-4 情報システムセキュリティ責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。

a) 不要な管理者権限アカウントを削除する。

b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

6.2.4(1)-5 情報システムセキュリティ責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。

（解説）

- **遵守事項 6.2.4(1)(a)「標的型攻撃」について**

以下の各款における規定内容は、標的型攻撃への対策としても有効であるため、それぞれに示される対策を行う必要がある。

- 6.1.1「主体認証機能」
- 6.1.2「アクセス制御機能」
- 6.1.3「権限の管理」
- 6.1.4「ログの取得・管理」
- 6.1.5「暗号・電子署名」
- 6.2.1「ソフトウェアに関する脆弱性対策」
- 6.2.2「不正プログラム対策」
- 7.1.1「端末」
- 7.1.2「サーバ装置」
- 7.2.1「電子メール」
- 7.3.1「通信回線」
- 8.1.1「情報システムの利用」

- **基本対策事項 6.2.4(1)-1 b)「不審なプログラムが実行されないよう設定する」について**

具体的な設定手段としては、あらかじめ利用するアプリケーションを登録してそれ以外のアプリケーションの実行を拒否するよう設定する、通常のアプリケーションでは利用しないメモリ空間を利用しようとしたアプリケーションを不審と判定して実行

を拒否するソフトウェアを利用する、情報システムにおいて不正プログラムの起動又は動作を拒否する手法を導入するなどが挙げられる。

なお、これらを導入する場合には、業務で利用するアプリケーションに影響が及ぶ可能性があるため、事前に検証する必要がある。

- **基本対策事項 6.2.4(1)-2 c)「自動再生（オートラン）機能を無効化」について**

  自動再生（オートラン）機能とは、OS がその機能を備えている場合において、サーバ装置や端末に USB メモリ等の外部電磁的記録媒体を接続した際に、その媒体に格納されている特定のプログラムを自動的に実行する機能を指す。

  標的型攻撃に用いられる手段として、この機能を悪用するものがあり、例えば、不正プログラムを格納した USB メモリを端末に接続させることにより、不正プログラムを実行させるという手法が想定される。

  自動再生（オートラン）機能を無効化しておくことにより、この機能を悪用する手段による被害に遭うリスクを低減することができる。

- **基本対策事項 6.2.4(1)-2 d)「外部電磁的記録媒体内にあるプログラムを一律に実行拒否」について**

  OS によっては、あらかじめ設定することにより、USB メモリ等の外部電磁的記録媒体を端末に接続した場合において、その媒体にあるプログラムを、その媒体にある状態のまま実行することを一律に拒否することができる。プログラムを実行したい場合には、端末の内蔵電磁的記録媒体（PC 内蔵 HDD 等）にいったんコピーしてから実行する運用となる。この設定により、接続した途端に外部電磁的記録媒体上の不正プログラムが実行されるリスクを低減することができる。

- **基本対策事項 6.2.4(1)-2 e)「USB ポートを無効化」について**

  物理的に又はシステム的に USB ポートを利用できない状態にすることで、USB メモリ等の外部電磁的記録媒体を接続することによって生じる情報セキュリティインシデントの発生を抑止できる。

- **基本対策事項 6.2.4(1)-2 f)「組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービス」について**

  外部電磁的記録媒体のポートへの接続や利用を制御及び管理するため、以下のような機能を持つ製品やサービスが市場に提供されている。

  - 端末の USB ポートのインタフェースを無効化し、外部電磁的記録媒体を含む全ての機器を利用不可とする。
  - USB ポートに接続された機器のうち、全ての外部電磁的記録媒体を利用不可とする。
  - 利用を認める外部電磁的記録媒体を一元管理するサーバに事前に登録しておき、登録されていない外部電磁的記録媒体の利用不可とする。
  - 利用を認める外部電磁的記録媒体の個体識別情報（製品番号等）と利用者の組合せを一元管理するサーバに事前に登録しておき、組合せ以外での利用を不可とする。

- 外部電磁的記録媒体の接続の際における、利用者、出力日時、出力ファイル名等のログを自動的に取得する。

- **基本対策事項 6.2.4(1)-3「情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバ」について**

  悪意ある第三者等は、入口対策を突破して内部への侵入に成功すると、外部から遠隔指令を出して内部侵入の範囲を拡大しつつ、目的の達成を目指すと想定される。その目的としては、重要情報の窃取や破壊が想定され、したがって、識別コード及びアクセス権限を集中管理する認証サーバ、又は、情報が集中的に保存されるファイルサーバは、攻撃対象となる蓋然性が高いと考えられる。これら重要サーバには、特に注意を払って情報セキュリティ対策を講ずる必要がある。

- **基本対策事項 6.2.4(1)-3 b)「管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策」について**

  管理者権限を狙う攻撃としては、機械的にパスワードを変えながら連続してログイン試行する攻撃が考えられる。このような攻撃を受けることを想定した対策としては、以下に挙げるものが考えられる。

  - 連続でのログイン失敗回数に上限値を設け、この上限値を超えた場合は、次回ログイン試行までに一定の期間（例：15 分）ログイン試行を受け付けないようにシステム等で設定する。
  - ログイン失敗ログを取得し、その取得内容を継続的に監視することにより、大量のログイン失敗を検知する仕組みを導入する。

  なお、辞書攻撃とは、パスワードに単語の組合せや人名を用いている場合に有効なパスワード解析方法をいう。英語の辞書に限らず各国語の単語を用いる場合もあるため、日本語の単語、日本人の人名も安全ではない。また、単語と数桁の数字のような単純な組合せも解析の対象となる。また、ブルートフォース攻撃とは、無意味な英数記号の組合せも含めた、総当たりでのパスワード解析方法をいう。辞書攻撃より効率は劣るが、原理的には必ず正しいパスワードに到達する。

6.3　アプリケーション・コンテンツの作成・提供

6.3.1　アプリケーション・コンテンツの作成時の対策

目的・趣旨

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

また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1「外部委託」についても併せて遵守する必要がある。

遵守事項

(1)　アプリケーション・コンテンツの作成に係る規定の整備

(a)　統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.3.1(1)(a)「アプリケーション・コンテンツ」について**

  行政サービスは、アプリケーションプログラムやウェブコンテンツ等を用いて国民等に提供されている。特にウェブコンテンツでは、機関等以外が提供するコンテンツ（以下「外部コンテンツ」という。）を組み込むことによって、容易に様々な機能を提供することが可能となるが、機関等において外部コンテンツの信頼性を担保することは不可能であることから、このような利用方法には注意を要する。例えば、外部コンテンツが事前に通知されることなく変更されてしまい、行政サービスの利用者の意図に反して利用者の個人に関する情報が取得される可能性がある。また、外部コンテンツに不正プログラムが組み込まれ、行政サービスの利用者がそれに感染する被害が生じることも考えられる。そのため、ウェブコンテンツでは外部コンテンツを利用しないことが望ましいが、必要があって利用する場合には、これらの脅威に対して適切なセキュリティ対策を実施することが求められる。

- **遵守事項 6.3.1(1)(a)「機関等外の情報セキュリティ水準の低下を招く行為を防止する」について**

  国民等が機関等によって提供される行政サービスを利用する場合、行政サービスの利用によって、利用者の端末が不正プログラムに感染しやすい状況を強制したり、利用者個人の情報が利用者の意図に反して第三者に提供させられるといった状況を作り出

したりすることは避けなければならない。機関等は、機関等外の情報システム利用者の情報セキュリティ水準を低下させないように留意して、行政サービスのためのアプリケーション・コンテンツを提供する必要がある。

- **遵守事項 6.3.1(1)(a)「規定を整備」について**

  統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供に関する規定の整備に当たり、遵守事項 6.3.1(2)において規定した事項を含める必要がある。

遵守事項

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。

(ｱ) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

(ｲ) 提供するアプリケーションが脆弱性を含まないこと。

(ｳ) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと。

(ｴ) 電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。

(ｵ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

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

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

【 基本対策事項 】

＜6.3.1(2)(a)(ア)関連＞

6.3.1(2)-1 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

b) 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

＜6.3.1(2)(a)(ア)(カ)関連＞

6.3.1(2)-2 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツにおいて、機関等外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該機関等外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

6.3.1(2)-3 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない**機関等外へのアクセスを自動的に発生させる機能**を含めないこと。

＜6.3.1(2)(a)(エ)関連＞

6.3.1(2)-4 情報システムセキュリティ責任者は、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として電子証明書を用いた署名を提供する際に、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

（解説）

- **遵守事項 6.3.1(2)(a)(ア)「不正プログラムを含まない」について**

不正プログラムとは、一般的なコンピュータウイルスの他、ワームやスパイウェア等が該当する。不正プログラムを含まないようにすべきものは、機関等外の利用者の端末にインストールさせるプログラムの他、利用者に閲覧させるウェブサイトのウェブページも含む。

- **遵守事項 6.3.1(2)(a)(イ)「脆弱性を含まない」について**

脆弱性は、アプリケーションプログラムが動作する OS や利用する開発言語によって様々な種類のものが存在する。例えば、C 言語によって開発されたアプリケーションプログラムにバッファオーバーフローの脆弱性が存在した場合は、利用者の端末上で任意のプログラムを実行される可能性がある。したがって、OS や開発言語の特性に応じて適切な脆弱性対策を実施する必要がある。

- **遵守事項 6.3.1(2)(a)(ウ)「実行プログラムの形式でコンテンツを提供しない」について**

実行プログラムの形式とは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。本号に違反する例としては、会議資料等のプログラムではない文書を提供する際に、自己展開式圧縮ファイル作成ソフトウェアを用いて拡張子が「.exe」の圧縮ファイルを作成してこれを配布する行為が典型例として挙げられる。多数に及ぶ会議資料等のファイルを 1 個のファイルとして提供する必要がある場合には、拡張子「.zip」等の形式の圧縮ファイルを作成して配布すればよい。

なお、電子メールの添付により文書等を配布する場合については、「(解説) 基本対策事項 8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について」を参照のこと。

実行プログラムの形式は、不正プログラムがその感染手段として悪用することが多いため、基本的に開かないようにしなければならない。それにもかかわらず、機関等が日頃から実行プログラムの形式でのコンテンツ提供を行う場合、機関等の職員等だけでなく、一般の行政サービスの利用者に対しても、実行プログラムの形式のファイルを開くことに慣れさせてしまうことになり、利用者の情報セキュリティ水準を低下させてしまうことになる。そのため、本号は、実行プログラムの形式でのコンテンツ提供を

しないよう求めている。

なお、機関等が行政サービスのためにアプリケーションプログラムを提供する必要がある場合等、「実行プログラムの形式以外にコンテンツを提供する手段がない」場合は、実行プログラムの形式で提供してもよいが、本項(エ)に従った措置を行う必要がある。

- **遵守事項 6.3.1(2)(a)(エ)「改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与える」について**

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としては、電子証明書を用いた電子署名が有効である。

利用者に提供するものがアプリケーションプログラムである場合は、「コードサイニング証明書」等と呼ばれる電子証明書を用いてアプリケーションプログラムに署名を施すことがこれに該当する。利用者はアプリケーションプログラムに施された署名を確認することで、改ざんがないことを確認でき、さらに、そのアプリケーションプログラムの提供者が機関等であることを確認できる。利用者に提供するものが文書ファイルである場合は、文書ファイルに対応するアプリケーションが備える電子署名機能を利用することができる。文書ファイルの形式によっては、電子署名を施すアプリケーションが提供されていない場合があるが、こうした場合は TLS（SSL）により通信路を保護したウェブページから当該電子ファイルをダウンロードする等の対応が求められる。

提供するコンテンツがウェブサイト上にある場合には、TLS（SSL）を用いた「https://」で始まる URL のウェブページとすることができる。これにより、利用者は現在閲覧しているウェブページが「https://」で始まる URL のウェブページであることを目視確認の上で、そこからリンクをクリックするなどしてファイルをダウンロードする手順を踏むことにより、当該ファイルは、暗号化された通信によって改ざんなくダウンロードされることになる。TLS（SSL）を用いる際に、機関等のサーバ証明書を用いれば、当該サイトが機関等のものであることを確認できる。

コンテンツを電子メールで提供する場合には、S/MIME 等の電子署名の技術を用いることで、電子メールが配送途中で改ざんされていないこと及び発信者が機関等であることを確認できる。

- **遵守事項 6.3.1(2)(a)(オ)「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」について**

行政サービスを提供する情報システムの提供において、当該情報システムを利用するために、機関等外の事業者等が作成した汎用のソフトウェアやミドルウェアのインストールが利用者の端末で必要となる場合がある。この場合、利用者は機関等から指示されたソフトウェアを自身の端末にインストールせざるを得ないが、指定されるソフトウェア（又はソフトウェアバージョン）のサポート期間が過ぎているなどの理由により脆弱性が存在するものであると、利用者の情報セキュリティ水準を機関等が低下させることになる。したがって、脆弱性が存在するバージョンの OS の利用やソフトウェアのインストールを機関等が暗黙又は明示的に要求することにならないよう、利用者に使用を求めるソフトウェアのサポート状況を考慮した上で、アプリケーション・コンテンツの提供方式を定めて開発しなければならない。

具体的には、当該行政サービスを提供するシステムが準備された時点では脆弱性が発見されていなくても、運用開始後に発見されることがある。そのとき、利用者が迅速に当該脆弱性を回避できるようになっている必要がある。例えば、当該行政サービスを利用するために、第三者が提供している汎用のソフトウェアのインストールを必要としていたとする。このとき、当該ソフトウェアに脆弱性が発見され、それを修正した新バージョンのソフトウェアが公開された場合に、当該新バージョンのソフトウェアをインストールすることで当該行政サービスに不具合等が生じて利用が不可能になるような事態が発生すると、利用者は、当該ソフトウェアを新バージョンに更新することができなくなる。結果として、機関等の行政サービスが利用者の脆弱性回避を妨げることになってしまう。こうしたことが起きないよう、行政サービスを提供するシステムは、第三者の汎用ソフトウェアの併用を前提とする場合は、当該汎用ソフトウェアが新バージョンに置き換わっても、正常に動作するように設計する必要がある。予期せず不具合が発生する事態が発生した場合にも、行政サービスを提供するシステムを修正することができるよう、迅速に新バージョンのソフトウェアに対応することを保守契約に盛り込んでおくことが望ましい。

また、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても、他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にする必要がある。そのためには、例えば、２種類以上のウェブブラウザ又は同一製品の異なるバージョンが動作するように、情報システムの構築時に配慮し、その動作確認を行うことが考えられる。

なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、ソフトウェアの配布前に情報が公開された状態又は試用版ソフトウェアが配布され動作検証可能な状態にあれば、前もって利用可能か否かを検証するなど、その後に公開が想定されるバージョンにも対応できるよう、構築時に配慮することが望ましい。

- **遵守事項 6.3.1(2)(a)(オ)「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」について**

行政サービスを提供する情報システムを利用するために、利用者の端末にインストールされているソフトウェア（機関等が直接提供していないソフトウェア（例えば、端末の OS やウェブブラウザ等））の設定変更を必要とするとき、その設定変更が情報セキュリティ水準の低下を招くものである場合、そのような設定変更を要求してはならない。必要があって利用者に設定変更を求めるときは、その OS やブラウザの標準設定（初期設定）に変更することのみを求めるものとすることである。

- **遵守事項 6.3.1(2)(a)(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」について**

これに該当する典型的な例は、機関等のウェブサイトを構成する各 HTML ファイルの中に、機関等外のサイト（例として広告事業者の広告提供サーバ）のコンテンツを見えない形又は見える形で組み込むことで、機関等のウェブサイトの閲覧者のアクセス履歴を当該広告サーバへ自動的に送信する、いわゆる「トラッキング処理」を行う機能

である。このとき、当該広告提供サーバが HTTP の cookie 機能を用いて閲覧する利用者に識別番号を付番している場合は、アクセス履歴等の、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当該広告提供サーバを運営する第三者に提供されることになるので、本号はこのような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にすることを求めている。

また、トラッキング処理ではなくとも、例えば、利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能も、「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」に該当し得る。

なお、対象はウェブサイトの HTML ファイルに限られず、アプリケーションプログラムを提供する場合に、そのプログラムに含まれ得る機能についても同様である。

- **遵守事項 6.3.1(2)(b)「調達仕様に含める」について**

例えば、機関等が何らかのキャンペーンとして啓発コンテンツを提供する際に、その作成を広告会社等に外部委託する場合は、情報システム部門以外の職員等がその外部委託の調達仕様を定めることになると考えられる。このような場合でも、機関等外の情報セキュリティ水準を低下させないよう、前項各号に掲げるセキュリティ要件を調達仕様に含めることが求められる。

- **基本対策事項 6.3.1(2)-2「必要があって当該機能を含める場合」について**

機関等外へのアクセスを自動的に発生させる機能を含める必要がある場合の例としては、ソーシャルメディアサービスとの連携機能を提供するためのボタン（ボタン画像の他、ボタン押下の機能等を提供するプログラムを含む。）等を機関等のウェブページ上に設置する場合が挙げられる。万が一、機関等外のウェブサイトが提供するプログラムに不正なコードが含まれていると、当該プログラムを使用した機関等のウェブサイトが利用者に危険をもたらすことになるため、その安全性が確認できているボタン等のみを使用することが求められる。これはウェブページ等のコンテンツに限らず、機関等が提供するアプリケーションプログラムにおいても同様である。

- **基本対策事項 6.3.1(2)-3「機関等外へのアクセスを自動的に発生させる機能」について**

機関等外へのアクセスを自動的に発生させる機能とは、例えば、機関等が提供するウェブページの HTML ファイルに、<script src”http://機関等外のサイト/foo.js”>等の記述があり、機関等外のウェブサイトからプログラムを読み込んで実行する機能が該当する。もし、機関等外のウェブサイトが提供するプログラムに不正なコードが含まれる場合、当該プログラムを使用した機関等のウェブサイトが利用者に危険をもたらすことになるため、そのような機能をウェブページに含めることは可能な限り避けるべきである。具体的には、当該ファイルを当該機関等ウェブサイトのサーバ上に置いて提供することで解決できる。これはウェブページ等のコンテンツに限らず、機関等が提供するアプリケーションプログラムにおいても同様である。

6.3.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

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

遵守事項

(1) 政府ドメイン名の使用

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

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

(イ) 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用する場合。この場合において、当該法人は、あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断すること。

(ウ) 4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合

(b) 職員等は、機関等外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.3.2(1)(a)「政府ドメイン名を情報システムにおいて使用する」について**

機関等が政府ドメイン名以外のドメイン名を使用している場合、機関等からの情報を装ったなりすましの脅威が想定される。政府ドメイン名は、株式会社日本レジストリサービスが定める「属性型（組織種別型）・地域型 JP ドメイン名登録等に関する規則」に基づき、その登録資格は日本国の政府機関、各省庁所轄研究所、独立行政法人、特殊法人（特殊会社を除く）に限られる」とされていることから、日頃から機関等が政府ドメイン名を用いることを徹底しておくことにより、なりすましが発生しても、機関等外の者がウェブサイト等の真偽を見分けることが容易なものとすることができる。

また、仮に政府ドメイン名以外を使用した場合には、そのサイトの使用を終了した後も、当該ドメイン名を不正に利用されないように登録管理を一定期間維持しなければならないが、そのような管理の必要がないことも、政府ドメイン名を用いることの利点の一つである。

政府ドメイン名を用いるべき場合の例を以下に示す。

- 機関等の地方出先機関や在外公館等が組織の紹介サイトを提供する場合

  「.go.jp」で終わるドメイン名は、運営主体が日本国政府及び政府に関係する機関であることを示すものとして、閲覧者に理解される。サーバを外国に設置している場合であっても、当該サーバのホスト名として「.go.jp」で終わるドメイン名を設定することは可能である。
- 機関等が主催する講演会等に係るウェブサイトの提供において、参加者の登録をオンラインで行うために、ウェブサイト上で閲覧者に個人情報を入力させる場合

  閲覧する者にとって、当該ウェブサイトが機関等によって運営されているものであることの確認は、個人情報の入力を要する場合には特に重要となる。
- 機関等が広報活動として期間限定でキャンペーンサイトを広告会社に制作させ提供する場合

  一時的に提供するウェブサイトを構築する場合や、広告会社に制作からサーバ管理までを委託する場合であっても、機関等の公式な告知であると閲覧者が認識すべき内容である限りは、政府ドメイン名を用いるべきである。サーバが広告会社管理のもので、サーバに割り当てられた IP アドレスが機関等外のものであっても、そのホスト名として政府ドメイン名を用いることはできる。

- **遵守事項 6.3.2(1)(a)(イ)「高等教育機関向けのドメイン名を使用する場合」について**

高等教育教育機関向けのドメイン名とは、高等教育機関及び学校法人等が登録できるドメイン名（ac.jp）を指す。高等教育機関向けのドメイン名を取得するための要件は、政府ドメイン名の要件とは異なるものの、取得可能な機関が高等教育機関に限られていることから、高等教育機関向けのドメイン名を使用することは、なりすまし等の特定の脅威に対する対策として一定の効果があると考えられる。

- **遵守事項 6.3.2(1)(a)(イ)「あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断」について**

機関等の中には、「○○大学校」のように行政事務ではなく、教育や訓練を主たる事務とする機関又は部門（教育機関）が存在する。国の行政機関に属する教育機関は、一般に国の行政機関の職員の養成や研修を主たる事務として行うのに対して、独立行政法人や指定法人である教育機関は、これら法人の職員ではなく一般の国民に対して特定分野に係る教育を提供しており、機関等における教育機関の性格は一律ではない。

国の行政機関に属する教育機関については、従前より統一基準において政府ドメイン名の使用を求めてきているが、その性格が「職員の養成や研修」という点において国の行政機関の行政事務の一環としてとらえることができ、政府ドメイン名を用いるこ

とが適当である。

一方、独立行政法人や指定法人である教育機関については、これら教育機関で勉学を行う国民の目から見れば、国の行政関係機関というよりも教育の場としての性格が強いと考えられ、使用するドメイン名については、情報セキュリティ確保の観点と、ウェブサイトの利用者側の視点の両面から考慮する必要がある。また、例えば、教育機関に所属する学生が政府ドメイン名のメールアドレスを使用するとした場合、メールを受信した者にとっては、メールの送信者が機関等の職員であると誤解する可能性もあり、このような点も考慮する必要がある。

そのため、独立行政法人や指定法人である教育機関においては、これら自組織の特性及び情報セキュリティ確保の観点を踏まえた上で、どちらのドメイン名を使用するべきか比較考慮し、判断することが必要である。

- **遵守事項 6.3.2(1)(b)「前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含める」について**

機関等外向けのウェブサイトを構築する場合に、情報システム部門以外の職員等がウェブサイトの構築業務を外部委託することが考えられる。このような場合でも、情報セキュリティ水準の低下を招かないよう、例えば、国の行政機関であれば政府ドメイン名の使用を調達仕様に含めることが求められる。

遵守事項

(2) 不正なウェブサイトへの誘導防止

(a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して**機関等のウェブサイトになりすました不正なウェブサイト**へ誘導されないよう対策を講ずること。

【 基本対策事項 】

＜6.3.2(2)(a)関連＞

6.3.2(2)-1 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイトに対して、以下を例とする**検索エンジン最適化措置（SEO 対策）**を講ずること。

a) **クローラからのアクセスを排除しない**。

b) **cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする**。

c) **適切なタイトルを設定する**。

d) **不適切な誘導を行わない**。

6.3.2(2)-2 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、**不審なサイトへのアクセスを防止するための対策**を講ずること。

（解説）

- **遵守事項 6.3.2(2)(a)「機関等のウェブサイトになりすました不正なウェブサイト」について**

機関等外の者が、機関等の名前をタイトルに掲げるなどして、機関等のウェブサイトと誤認されかねないウェブサイトを作成することがあり、これを完全に防ぐことはできない。本来ならば、利用者は当該サイトの URL 中のドメイン名が政府ドメイン名であるかを確認することで、機関等のウェブサイトかを確認できるところであるが、検索サイト等を利用して機関等名で検索して訪れる利用者も多いことから、検索サイトで検索したときに、正規の機関等サイトが検索結果の上位に現れるようになっていることが望ましい。通常は、特別な対策をすることなく、そのような結果になることがほとんどであるが、正規の機関等サイトの側で、不適切な設定になっていたり、コンテンツが適切に構成されていない場合に、検索サイトで、正規の機関等サイトが最上位に現れなかったり、適切な表示がなされないことがある。本条はそのような事態を防止するための措置を講ずることを求めている。

- **基本対策事項 6.3.2(2)-1「検索エンジン最適化措置（SEO 対策）」について**

正規のウェブサイトが検索サイトで上位に現れるように正規のウェブサイト側で工夫を施すことを、一般に「検索エンジン最適化」又は「SEO 対策」と呼ぶ。本基本対策事項は、機関等サイトにおいても一般的な検索エンジン最適化の措置を講ずることを求めている。

- **基本対策事項 6.3.2(2)-1 a)「クローラからのアクセスを排除しない」について**

一般に、検索サイトは、ウェブクローラと呼ばれる自動的にウェブサイトのリンクをたどって全てのページを巡回するプログラムを、自ら稼働させることによって収集した HTML データを用いて検索機能を実現している。そのため、検索サイトのクローラからのアクセスを拒否する設定をしている場合、当該サイトは検索サイトの検索結果に現れなくなることがある。そのような設定は、ウェブサイトの「/robots.txt」のファイルの記述で簡単にできるものであるため、誤ってクローラからのアクセスを拒否する設定にしてしまう状況が想定される。通常、このファイルを設定する必要はないため、何ら記述しないでおくことが望ましい。

- **基本対策事項 6.3.2(2)-1 b)「cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする」について**

一般に、検索サイトが自ら稼働させるウェブクローラは、HTTP の cookie 機能に対応していない。そのため、cookie 機能を無効に設定したブラウザで閲覧したときに、正常に表示されないウェブページは、検索サイトの検索結果に正常に表示されない事態が起きる。通常のウェブサイトの構成では、cookie 機能を無効にしても正常に表示されるものであるが、一部の CMS（Content Management System）には、cookie を無効にして閲覧すると「cookie を有効にしてください」とだけ記述したエラー画面を表示するものがあり、そのような CMS を用いてウェブサイトを構成すると、前述の事態が生じる。実際に、過去に一部の機関等サイトでそのような事態が発生したことがあるため、ウェブサイトの構築を外部委託する場合を含め、注意する必要がある。

- **基本対策事項 6.3.2(2)-1 c)「適切なタイトルを設定する」について**

一般に、検索サイトの検索結果には、当該ページのタイトル（HTML 中の TITLE 要素で設定される文字列）が見出しとして表示され、利用者はこれを頼りにサイトを訪れることから、機関等サイトにおいても、ページのタイトルに機関等の名称を含めるなど、適切なタイトルを設定することが重要である。

その他の対策として、HTML 中の H1 要素や H2 要素を適切に記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。機関等サイトにおいても、H1 要素や H2 要素を適切に記述することで、検索結果の上位に現れやすくすることができる。また、HTML 中のメタタグ（「description」や「keywords」等）に概要やキーワード等を記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。機関等サイトにおいても、メタタグを適切に記述することで、検索結果の上位に現れやすくすることができる。

- **基本対策事項 6.3.2(2)-1 d)「不適切な誘導を行わない」について**

一般に、HTML 中に見えない文字等でページ内容に関係のないキーワードを過剰に記述するなどして、当該ページへのアクセスを無用に誘う行為（「SEO スパム」等と呼ばれる。）は、不適切な行為として検索サイトからペナルティを科され、検索結果の上位に表示されなくなることがある。機関等のウェブサイトにおいて、故意にそのような

行為が行われることは考えにくいが、コンテンツの作成を外部委託した場合に、委託先が独自判断で行うことも想定されるため、そのようなコンテンツを作成しないよう注意が必要である。

- **基本対策事項 6.3.2(2)-2「不審なサイトへのアクセスを防止するための対策」について**

  不審なサイトを確認した場合は、機関等のウェブサイト等において注意喚起を行うなどの対応を図るとともに、必要に応じて自組織や内閣官房内閣サイバーセキュリティセンター等の関係部門に状況を報告する。特に悪質な場合は、誤って当該サイトにアクセスすることを防止するため、検索サイト業者に対して検索結果に表示されないよう依頼する、機関等 LAN からアクセスできないよう当該サイトに対してフィルタを設定する、といった対策が考えられる。

遵守事項

(3) アプリケーション・コンテンツの告知

(a) 職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

(b) 職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

【 基本対策事項 】

＜6.3.2(3)(a)関連＞

6.3.2(3)-1 職員等は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示すること。また、短縮 URL を用いないこと。

6.3.2(3)-2 職員等は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

＜6.3.2(3)(b)関連＞

6.3.2(3)-3 職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の措置を講ずること。

a) 告知するアプリケーション・コンテンツを管理する組織名を明記する。

b) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

（解説）

- **遵守事項 6.3.2(3)(b)「機関等外の者が提供するアプリケーション・コンテンツを告知する」について**

機関等外の者が提供するアプリケーション・コンテンツを告知する場合、告知を開始した時点では、当該アプリケーション・コンテンツが、告知した URL 等の誘導先に確かに存在していても、将来にわたりその誘導先に意図したアプリケーション・コンテンツが存在し続けるとは限らない。誘導先のドメイン名等が放棄された場合には、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、機関等外の者が提供するアプリケーション・コンテンツを機関等が告知する場合には、誘導先の有効性を保つことが求められる。

- **基本対策事項 6.3.2(3)-1「URL 等を用いて直接誘導」について**

URL を用いた直接誘導に該当する例としては、ウェブサイトにハイパーリンクを設

ける場合のほか、電子メールに URL を記載して告知する場合、印刷物に URL を表示して誘導する場合等が挙げられる。URL「等」としているのは、例えば、ホスト名（FQDN 形式での表記）もこれに該当するものとする趣旨である。

- **基本対策事項 6.3.2(3)-1「検索サイトで指定の検索語を用いて検索することを促す方法」について**

  印刷物やテレビ CM により告知する際に、URL 等の文字列が長すぎると、利用者にその全部を入力させることが困難であることから、検索サイトで検索するよう検索語を指定して促す方法が広く普及している。

  しかし、この誘導方法では、偽サイトや別のサイトに誘導されてしまうリスクを否定できない。検索結果の上位に目的の誘導先が現れない可能性があるだけでなく、検索サイトの広告部分に悪意あるサイトを出現させる攻撃手法も想定され、利用者が検索サイトの広告部分を誘導先として解釈してしまうおそれがある。

  また、アプリケーション・コンテンツの告知を広告代理店に委託している場合、広告代理店が検索サイトの広告枠を購入し、広告部分を用いて目的の誘導先に誘導する方法が用いられることがある。この誘導方法が広告代理店によって頻繁に用いられると、広告部分を正規の誘導先として利用者が解釈するようになると考えられ、広告部分に攻撃者による偽サイトが現れることのリスクを無視することはできなくなる。したがって、機関等がアプリケーション・コンテンツを告知する場合には、検索サイトの広告枠を購入して誘導する方法は用いないようにすることが望ましい。

- **基本対策事項 6.3.2(3)-1「間接的な誘導方法を用いる場合」について**

  間接的な誘導方法を用いて機関等の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、当該誘導方法による誘導の状況を適時確認するなどして、不正な又は不適切なウェブサイトへ誘導されてしまう可能性が高い状況になっているか否かを確かめることが望ましい。

- **基本対策事項 6.3.2(3)-1「URL 等と一体的に表示する」について**

  アプリケーション・コンテンツの告知は URL 等を用いて直接誘導することを原則とするが、間接的な誘導方法を用いたい場合があることも想定されることから、その場合に実施すべき措置として、間接的な誘導方法と一体的に URL 等を表示することを求めている。

- **基本対策事項 6.3.2(3)-1「短縮 URL を用いない」について**

  短縮 URL を提供する民間事業者のサービスは、将来にわたり永続的に運営が保証されるものではなく、いずれサービスが消滅し、ドメイン名が放棄されれば、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、やむを得ない場合を除き、短縮 URL を用いるべきでない。やむを得ない場合の例としては、ソーシャルメディアサービスにおいて URL を告知する場合に、当該ソーシャルメディアサービスが強制的に所定の短縮 URL を用いてしまう場合が挙げられる。

- **基本対策事項 6.3.2(3)-2「アプリケーション・コンテンツの内容に係る記述を当該バーコードと一体的に表示」について**

  印刷物等でアプリケーション・コンテンツを告知する際に、URL 等の表示に代わるもの又は URL 等と一体的に表示するものとして、二次元コード等を用いて誘導する方法がある。この方法は、特にスマートフォンや携帯電話の利用者にとって利便性が高く、機関等においても用いられるようになってきている。

  しかしながら、二次元コード等のみを単体で表示した場合、それがどこへ誘導するものであるかが、利用者にとって必ずしも明確でない場合がある。そこで、本項では、当該二次元コード等がどこへ誘導するものであるかを、当該二次元コード等と一体的に表示することにより利用者に明示することを求めている。

  「アプリケーション・コンテンツの内容に係る記述」の例としては、誘導先の URL 等や、誘導先のアプリケーション・コンテンツの内容を示す記述が考えられる。

- **基本対策事項 6.3.2(3)-3「告知する URL 等の有効性を保つために以下の措置を講ずる」について**

  この措置を講ずるための対策事項 a)及び b)について、具体的な記載例を以下に示す。

  - このウェブサイトは○○協会が運営しており、○○省が運営しているものではありません。
  - このウェブサイトのアドレスについては、○○年○○月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、御自身で御確認ください。

第7部 情報システムの構成要素

7.1 端末・サーバ装置等

7.1.1 端末

目的・趣旨

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

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

なお、本款の遵守事項のほか、6.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(1) 端末の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

【 基本対策事項 】

＜7.1.1(1)(a)関連＞

7.1.1(1)-1 情報システムセキュリティ責任者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置すること。

7.1.1(1)-2 情報システムセキュリティ責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。
b) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。

7.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。
a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。
b) 要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

＜7.1.1(1)(b)関連＞

7.1.1(1)-4 情報システムセキュリティ責任者は、以下を考慮した上で、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バージョンも含め定めること。
a) ソフトウェアベンダ等のサポート状況
b) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容
c) インストール時に同時にインストールされる他のソフトウェア
d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

（解説）

- **遵守事項 7.1.1(1)(b)「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」について**

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それぞれのリストに登録する単位について、ソフトウェアの個別の製品名やバージョン単位で列挙すると分かりやすいが、利用を禁止する全てのソフトウェアについて製品名等を個別に列挙するのが難しい場合は、例えば、個別に把握できるソフトウェアの製品名に加えてカテゴリ単位で登録することも考えられる。カテゴリ単位で登録する例としては、いわゆるピアツーピアで通信を行うソフトウェア、ファイル交換ソフトウェア、端末内の情報又は端末に入力した情報が自動で機関等外のサーバ装置等に送信されるソフトウェア、というような単位で定めておき、利用者に周知しておくと不要な手続が減らせるほか、利用者の意識向上にも寄与すると考えられる。また、情報セキュリティリスクを低減する観点からは、利用を認めるソフトウェアを極力限定することが望ましい。

利用者が端末にソフトウェアをインストールすることができるような環境においては、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、利用者に周知徹底を図ることが重要である。

- **基本対策事項 7.1.1(1)-1「原則としてクラス２以上の要管理対策区域に設置する」について**

要保護情報を取り扱う端末はクラス２以上の区域に設置することが望ましい。クラス２より低位の区域に設置する必要がある場合は、利用者が常時目視できる場所への設置を義務付けるなど、クラス２の区域に設置する場合と同程度の安全性を確保するための代替の対策を講ずること。

- **基本対策事項 7.1.1(1)-3「第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずる」について**

  第三者による不正操作等の防止のための対策事項であるが、その他、端末の操作のロックの解除に IC カード等の主体認証情報格納装置を使用し、主体認証情報格納装置が無い状態で又は操作の無い状態が一定時間続くことで端末の操作がロックされるようにし、かつ、当該主体認証情報格納装置を執務室への立入りの確認にも利用するという方法が考えられる（これにより、利用者が執務室外にいる際には端末の操作が確実にロックできる）。

  また、正規の利用者による不正操作や誤操作の防止策として、端末が備える機能のうち、利用しない機能を停止することが考えられる。停止する機能の例としては、無線 LAN 等の通信用のインタフェース、USB ポート等の外部電磁的記録媒体を接続するためのインタフェース、マイク、ウェブカメラ等が考えられる。

- **基本対策事項 7.1.1(1)-4「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バージョンも含め定める」について**

  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際には、以下を行うことが考えられる。

  - ソフトウェアベンダによるセキュリティパッチ等のサポートが提供されていることや、セキュリティベンダ等の第三者が提供するソフトウェアの脆弱性等に関する情報を確認する。
  - 外部と通信を行う機能を有することが明確なもの又は外部との通信の有無について利用規約により確認できるものについては、当該機能による通信内容を事前に確認する。
  - インストール時に、他のソフトウェアのインストールの同意を求めるものについては、当該ソフトウェアの利用の可否についても併せて定める。
  - ブラウザ等のソフトウェアで利用される機能拡張用のソフトウェア（いわゆる、プラグインやアドオン）の利用の可否についても併せて定める。

  また、一度利用を認めたソフトウェアであっても、バージョンが上がった際に、旧バージョンと比べ、機能が変わったり、同時にインストールされる他のソフトウェアが追加されたりする場合があるので、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際には、バージョンも含めて定めることが重要である。

  なお、ソフトウェアによっては、バージョンによらず一律で利用を禁止するソフトウェアに指定できる場合もある。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.1.1(2)(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、また、利用者の要求に柔軟に対応するため、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の見直しを行うことが必要である。

「定期的」以外の見直しの契機として、端末の利用者から利用を認めるソフトウェア以外のソフトウェアの利用承認の申請（8.1.1「情報システムの利用」を参照のこと。）を受け付けたときが考えられる。申請のあったソフトウェアについて、引き続き利用を認める場合には、利用を認めるソフトウェアのリストに追加し、引き続き利用を禁止する場合には、利用を禁止するソフトウェアのリストに追加することで、一つのソフトウェアにつき１回の手続で済ませることができる。

- **遵守事項 7.1.1(2)(b)「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」について**

「不適切な状態」とは、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。

利用を認めるソフトウェア以外のソフトウェアが稼働している場合には、当該ソフトウェアを停止する、又は削除する必要がある。セキュリティパッチについては、6.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.1.1(3)(a)「端末の運用を終了する際」について**

  端末を廃棄処分する場合やリース契約が終了し端末を返却する場合が考えられる。

- **遵守事項 7.1.1(3)(a)「抹消する」について**

  抹消の方法については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」を参照のこと。

  なお、運用を外部委託しているなど、調達元の機関等において抹消できない場合においては、保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずることが必要である。

遵守事項

(4) 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末の導入及び利用時の対策

(a) 統括情報セキュリティ責任者は、**要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末**について、以下の安全管理措置に関する規定を整備すること。

(ｱ) 盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置

(ｲ) 機関等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置

(b) 情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等の業務に係る情報処理に関する**安全管理措置の実施状況を管理**する**責任者**（以下「端末管理責任者」という。）を定めること。

(c) 次の各号に掲げる責任者は、職員等が当該各号に定める端末を用いて要機密情報を取り扱う場合は、当該端末について(a)(ア)の安全管理措置を講ずること。

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

(ｲ) 端末管理責任者　機関等支給以外の端末

(d) 端末管理責任者は、要機密情報を取り扱う機関等支給以外の端末について、前項の規定にかかわらず(a)(ア)に定める安全管理措置のうち**自ら講ずることができないもの**、及び(a)(イ)に定める安全管理措置を職員等に講じさせること。

(e) 職員等は、要機密情報を取り扱う機関等支給以外の端末について、前項において(a)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び(a)(イ)に定める**安全管理措置を講ずる**こと。

【 基本対策事項 】

＜7.1.1(4)(a)(ア)関連＞

7.1.1(4)-1 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を**暗号化**するための機能を設けること。

a) **シンクライアント等**の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

b) **セキュアブラウザ等**を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。

c) **ファイル暗号化等のセキュリティ機能を持つアプリケーション**を導入する。

d) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。
e) 上記の各号のいずれの機能も使用できない場合は、端末に**ファイルを暗号化する機能を設ける**。
f) ハードディスク等の電磁的記録媒体に保存されている情報を**遠隔からの命令等により消去する機能**を設ける。ただし、この場合は本項 c)～e)を例とする暗号化の**機能を組み合わせること**。

＜7.1.1(4)(a)(イ))関連＞

7.1.1(4)-2　統括情報セキュリティ責任者は、要機密情報を取り扱う機関等支給以外の端末について、以下を例に、職員等が講ずるべき利用時の実施手順に係る安全管理措置を設けること。

a) パスワード等による端末ロックの常時設定
b) OS やアプリケーションの最新化
c) **不正プログラム対策ソフトウェアの導入**及び定期的な不正プログラム検査の実施（機関等として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
d) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
e) 機関等提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）
f) 以下を例とする禁止事項の遵守
- **端末、OS、アプリケーション等の改造行為**
- **安全性が確認できないアプリケーション**のインストール及び利用
- **利用が禁止されているソフトウェア**のインストール及び利用
- **許可されない通信回線サービスの利用**（利用する回線を限定する場合）
- **第三者への端末の貸与**

（解説）

- **遵守事項 7.1.1(4)(a)「要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末」について**

要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末とは、モバイル端末（機関等が支給するもの及び機関等支給以外のものの双方）と職員等の自宅で業務を行う際に用いる機関等支給以外の据え置き型端末が該当する。

- **遵守事項 7.1.1(4)(b)「安全管理措置の実施状況を管理」について**

機関等支給以外の端末を職員等が利用するに当たって、申請時に安全管理措置の実施状況について端末を目視確認する方法や、定期的な実施状況の確認を管理者にて行うことをあらかじめ定めておく方法等が考えられる。管理工数の増加が懸念される場

合は、サンプリングによる確認や定期的な注意喚起を利用者に行うなどの方法で管理作業の効率化を図ることも考えられる。

- **遵守事項 7.1.1(4)(b)「責任者」について**

機関等支給以外の端末の安全管理措置の実施状況を管理する責任者であり、PC やスマートフォン等に対して一定以上の知見を有している者がその任に当たることが望ましい。例えば、機関等 LAN システムの情報セキュリティ責任者等が考えられる。ただし、職員等の安全管理措置の実施状況について適時状況を把握することが求められるため、課室情報セキュリティ責任者が兼ねることも考えられる。

- **遵守事項 7.1.1(4)(d)「自ら講ずることができないもの」について**

基本的対策事項 7.1.1(4)-1 の安全管理措置のうち、職員等が講ずることが適当な項目としては、例えば OS の機能を利用する 7.1.1(4)-1 d)の「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」や 7.1.1(4)-1 e)の「ファイルを暗号化する機能」が考えられる。

- **遵守事項 7.1.1(4)(e)「安全管理措置を講ずる」について**

職員等は、機関等支給以外の端末の利用に係る機関等全体のポリシーをよく理解し、安全管理措置を徹底し、情報セキュリティインシデントの回避に努めなければならない。特にスマートフォン等の利用については、その特性に応じたリスクを利用者である職員等自身もよく理解した上で利用することが求められる。

- **基本対策事項 7.1.1(4)-1「暗号化」について**

機関等支給以外の端末に要機密情報を保存して業務を行う場合は、端末に保存する情報を暗号化して、盗難・紛失時の情報漏えいのリスクを低減する必要がある。情報へのアクセス権を管理する方法もあるが、モバイル端末が第三者の者の手に渡った場合には、モバイル端末から取り外された内蔵電磁的記録媒体や、モバイル端末で利用していた外部電磁的記録媒体に保存されている情報を他の端末を利用して解読するなどの手段によってアクセス権管理機構を回避され要機密情報が窃取される危険性がある。このような情報の窃取への対策として、端末に暗号化機能を搭載することが有効である。

暗号化する方法としては、ファイル暗号化等のセキュリティ機能を持つアプリケーションを用いる方法、ハードディスク全体又はファイル単体を暗号化するソフトウェアの導入や OS が備えている暗号化機能を使用することが挙げられる。遠隔データ消去機能を補助的な機能として組み合わせると効果的である。ハードディスク全体を暗号化している場合であっても、端末の起動中等の復号可能な状態で盗難等に遭った場合には情報窃取されるおそれがあるため、遠隔データ消去機能と組み合わせて用いると情報窃取される可能性をより低減できる。

また、安全性を確保するためには暗号化に用いる鍵の管理が重要になる。端末紛失時に端末内に鍵や、鍵を生成するために必要な全ての情報を保持していると暗号化したデータを復号されるリスクがある。

したがって、業務利用していないときはこれらを保持しないなど、鍵の漏えいリスク

が低減されるような管理の仕組みを持つ以下を例とする方式を導入するとよい。

＜例＞

- 端末内の耐タンパ性を備えた TPM（Trusted Platform Module）を利用する方法
- 鍵を USB セキュリティトークンに格納して、利用時以外は端末とは別に管理する方法
- 暗号化する範囲を業務領域に限定しパスワードを入力するタイミングを業務システムへのログイン時、パスワードを基に生成した鍵を消去するタイミングをログアウト時（又はタイムアウト時）とする方法

- **基本対策事項 7.1.1(4)-1 a)「シンクライアント等」について**

端末に情報を保存させない仕組みとして、シンクライアントやリモートデスクトップと呼ばれる技術の活用が有効である。既に市場において提供されているが、外部の情報処理サービスを組み合わせてシンクライアントやリモートデスクトップ関連の製品やソリューションサービスを利用する場合には、4.1.1「外部委託」、4.1.2「約款による外部サービスの利用」及び 4.1.4「クラウドサービスの利用」についても参照する必要がある。

＜シンクライアントの主な機能及び特徴＞

- 業務ネットワーク内の仮想デスクトップ画面を転送
- ユーザデータを端末に残さない
- ウェブキャッシュ、接続情報、作業履歴等全てサーバ装置内に保管
- 外部情報出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

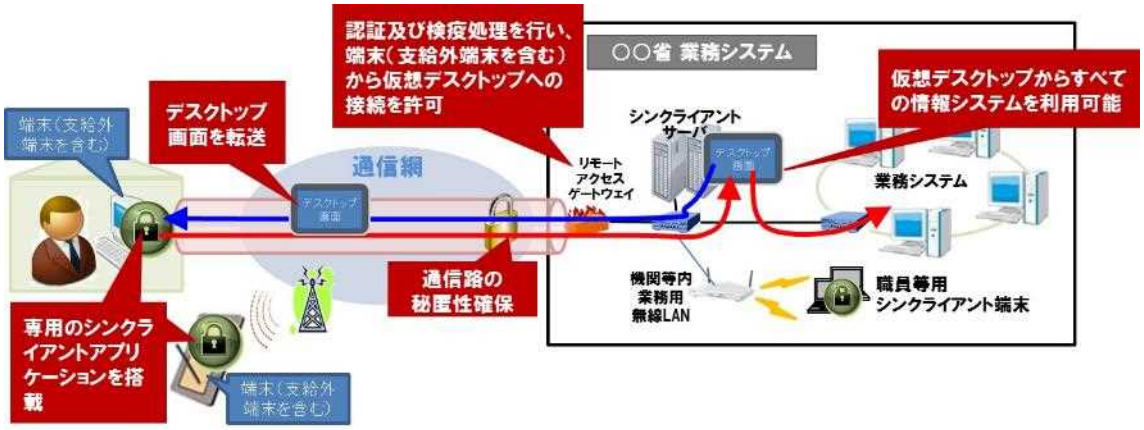


図 7.1.1-1　シンクライアントのシステム構成例

また、シンクライアントの発展形として、仮想デスクトップ環境の利用機能（ネットワーク接続や画面描画・ディスプレイ出力、キーボード・マウス入力等）のみに機能が絞り込まれたゼロクライアントやシンクライアント専用端末の利用も有効である。特にゼロクライアントは、汎用 OS や汎用ブラウザ等を搭載していないことから、不正プ

ログラム対策やソフトウェア更新等のセキュリティ管理の負荷が軽減でき、万一端末が故障しても、端末を交換するだけですぐに利用可能になるなど、セキュリティ管理面の負荷の軽減も期待される。処理能力やコスト負担等の課題も考えられるので、それらも勘案した上で利用を検討するとよい。

- **基本対策事項 7.1.1(4)-1 b)「セキュアブラウザ等」について**

  モバイル端末に情報を保存させない別の仕組みとして、セキュアブラウザを選択することも有効である。セキュアブラウザ製品についても、各種クラウドサービスと組み合わせたソリューションとして提供される場合があることから、外部の情報処理サービスを組み合わせて利用する場合は、4.1.1「外部委託」、4.1.2「約款による外部サービスの利用」及び 4.1.4「クラウドサービスの利用」についても参照する必要がある。

  ＜セキュアブラウザの主な機能及び特徴＞

  - 端末に電子メール、ファイル閲覧等を画面転送等で行い、端末内のブラウザ等で閲覧することなどが可能。閲覧終了時に当該データを端末に残さない
  - ブラウザ終了時に閲覧に関連する情報（ウェブキャッシュ、URL、cookie 等）を消去可能
  - 外部出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

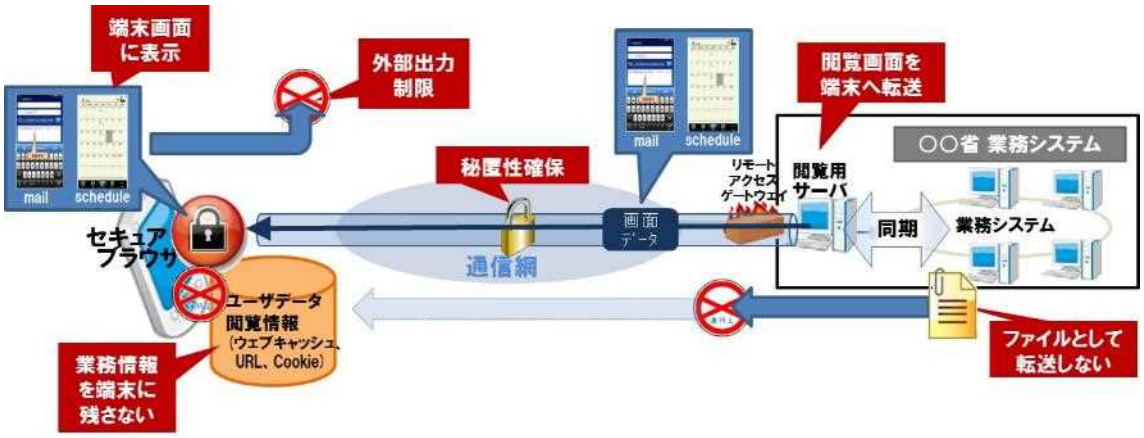


図 7.1.1-2　セキュアブラウザ活用型ソリューションのシステム構成例

- **基本対策事項 7.1.1(4)-1 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について**

  通信回線との接続環境が無い場所で業務を行うなど、やむを得ず情報を端末に保存させる必要がある場合は、セキュアブラウザやシンクライアントは利用できないことから、他の方法で安全な利用環境の提供を考える必要がある。この場合は、モバイル端末にファイル暗号化等のセキュリティ機能を持つ業務専用のアプリケーションを搭載し、アプリケーション単位で情報を暗号化するなどの方法が考えられる。当該機能を有するセキュリティソリューションが製品として民間事業者より提供されていることから、それらの活用を検討するとよい。

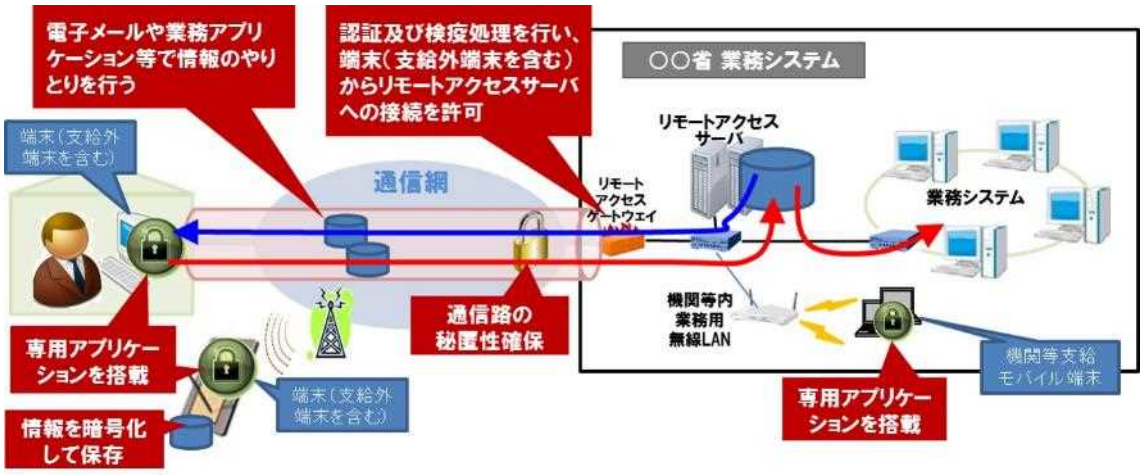


図 7.1.1-3　ファイル暗号化等セキュリティ機能を持つ
アプリケーションを活用したシステム構成例

- **基本対策事項 7.1.1(4)-1 e)「ファイルを暗号化する機能を設ける」について**

  機関等支給以外の端末のセキュリティ対策については、職員等の人的作業負担とならないようにすべきであり、職員等が講じた安全管理措置が不十分であることも考えられるため、基本対策事項 7.1.1(4)-1 a)～d)に示すシステム面で対応が取られることが望ましい。要管理対策区域外で要機密情報を取り扱う際の対策として、個々のファイルを手作業により暗号化する場合は、職員等に確実にこれを実施させることが必要となる。

- **基本対策事項 7.1.1(4)-1 f)「遠隔からの命令等により消去する機能」について**

  端末の通信機能を利用して、遠隔から端末内のデータを消去する機能であるが、通信が確立できないために遠隔からデータ消去できない場合に備え、主体認証の失敗した回数をカウントして一定数を超えた際に消去するなど特定の条件で自律的に消去する機能についても考慮するとよい。また、データ消去ではなく、端末の操作をロックするという対策も考えられる。

- **基本対策事項 7.1.1(4)-1 f)　「機能を組み合わせること」について**

  第三者により情報窃取されることを防止する対策として、遠隔からの命令等により情報を消去する機能のみを導入した場合、データ消去の処理が実行される前に端末のハードディスクの内容を直接解読されるおそれがある。したがって、当該機能を導入する際は、ハードディスク暗号化機能等と組み合わせることが必要がある。

- **基本対策事項 7.1.1(4)-2 c)「不正プログラム対策ソフトウェアの導入」について**

  OS の構造等により、不正プログラム対策ソフトウェアが提供されていない、又は部分的にしか対策機能が有効でないスマートフォンや携帯電話等の利用については、通信事業者によって事前に安全性が確認されたアプリケーションのみ当該端末へダウンロード可能とされているなどの別の方法で安全性を確保する必要がある。

- **基本対策事項 7.1.1(4)-2 f)「端末、OS、アプリケーション等の改造行為」について**

  iOS における Jailbreak や Android における root 化のように、ソフトウェア等の改造が行われた端末は外部からの攻撃の的となりやすく、不正パケットの受信によって不正プログラムに感染したり、端末が乗っ取られたりする危険性が高くなる。

  このような改造された端末が業務に使用されると、端末に保存された情報が漏えいするなどの情報セキュリティインシデントが発生する可能性があるため、機関等支給以外の端末を利用する際は、事前に端末、OS、アプリケーション等の改造行為を行わないことについて、職員等と同意しておくことが重要である。

  モバイル端末を業務利用することを目的とした、MDM（Mobile Device Management）ツール等を機関等のリモートアクセス環境と組み合わせ、改造された端末を検知するなどして、システム的に改造端末の使用を回避する方法も考えられる。

- **基本対策事項 7.1.1(4)-2 f)「安全性が確認できないアプリケーション」について**

  スマートフォンにおいては、専用のアプリケーション提供サイト等からオンデマンドでアプリケーションをダウンロードする利用形態が一般的であるが、不正プログラム等が混在する提供サイトの存在が懸念されるため、業務に利用する機関等支給以外のスマートフォン等においては安全性が不明なアプリケーションがインストールされた状態で利用されることがないように、例えば OS 提供事業者や通信事業者等がアプリケーションの安全性の審査を行っている信頼性の高いアプリケーション提供サイトにて提供されるアプリケーションのみに利用を限定すること等を対策にするとよい。ただし、大手の事業者であっても安全なアプリケーションを提供しているとは限らないので、提供サイトを運営する事業者のセキュリティ対策水準を十分見極めた上で判断することが求められる。

  スマートフォンを安全に利用するための留意事項として、OS の最新化及び不正プログラム対策とともに注意喚起されているので、参考にすること。

  参考：総務省「スマートフォン情報セキュリティ３カ条」（スマートフォン・クラウドセキュリティ研究会最終報告）（平成 24 年 6 月 29 日公表）
  （http://www.soumu.go.jp/main_content/000166095.pdf）

  上記のウェブサイトのアドレスは、平成 30 年 X 月 X 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.1.1(4)-2 f)「利用が禁止されているソフトウェア」について**

  遵守事項 7.1.1(1)(b)の対策として、機関等支給の端末において規定される利用を禁止するソフトウェアと同等であることが考えられるが、例えば私的な利用の範囲を必要以上に制限しないよう考慮する必要がある。

- **基本対策事項 7.1.1(4)-2f)「許可されない通信回線サービスの利用」について**

  公衆無線 LAN サービスのうち無線経路の秘匿性や安全性が不明なものや接続経路の管理状況が不明な無料のインターネット接続サービス等は、通信内容の盗聴やなりすましによる情報の窃取等のおそれがあり、このような情報セキュリティ水準が不明な通信回線は業務に利用すべきではない。ただし、海外等で、情報セキュリティ水準が不明な通信回線サービスを利用せざるを得ない場合が想定されることから、例えば、情報システムへのリモートアクセス経路において VPN 回線を設定し end-end の秘匿性を確保するなどの方法を用いるとよい。

  なお、無線 LAN の利用に関する対策については、7.3.1(5)「無線 LAN 環境導入時の対策」の内容を併せて考慮する必要がある。

- **基本対策事項 7.1.1(4)-2 f)「第三者への端末の貸与」について**

  家族や知人に私物の端末等を貸与することがあるが、その際に意図的に機密性の高い情報を閲覧したり又は誤操作により機密性の高い情報を外部に転送してしまったりすることが懸念される。

  私物端末であっても業務に利用するのであれば、第三者への貸与は禁止すべきであり、それに同意できない職員等には私物端末を利用させるべきではない。

7.1.2 サーバ装置

目的・趣旨

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

なお、本款の遵守事項のほか、6.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、6.2.3「サービス不能攻撃対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本款での共通的な対策に加え、それぞれ 7.2「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

遵守事項

(1) サーバ装置の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

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

(c) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で**利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める**こと。

(d) 情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の**保守作業を行う際に送受信される情報が漏えいすることを防止するための対策**を講ずること。

【 基本対策事項 】

＜7.1.2(1)(a)関連＞

7.1.2(1)-1 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は、**クラス２以上の要管理対策区域に設置する**こと。

7.1.2(1)-2 情報システムセキュリティ責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) 施錠可能なサーバラックに設置して施錠する。

b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

7.1.2(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

＜7.1.2(1)(b)関連＞

7.1.2(1)-4 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は、将来の見通しも考慮し、以下を例とする対策を講ずること。

a) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

b) 同一システムを２系統で構成することによる冗長化

＜7.1.2(1)(c)関連＞

7.1.2(1)-5 情報システムセキュリティ責任者は、以下を考慮した上で、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バージョンも含め定めること。

a) ソフトウェアベンダ等のサポート状況

b) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容

c) インストール時に同時にインストールされる他のソフトウェア

d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

（解説）

- **遵守事項 7.1.2(1)(c)「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」について**

  「（解説）遵守事項 7.1.1(1)(b)「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」について」を参照のこと。

- **遵守事項 7.1.2(1)(d)「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」について**

  情報システムセキュリティ責任者から保守作業を許可されている者がサーバ装置へログインして作業する場合を想定し、例えばインターネットを介してサーバ装置の保守作業を行う場合等、通信内容を秘匿する必要がある場合には、サーバ装置の設置時に暗号化するための機能を設け、運用時に情報の暗号化を実施できるようにしておくこと等が考えられる。

- **基本対策事項 7.1.2(1)-1「クラス２以上の要管理対策区域に設置する」について**

  サーバ装置に関しては、取り扱う情報の重要性に応じてクラス３の区域に設置することも考慮するとよい。また、クラス２の区域（執務室等）に設置する場合においても常時施錠されたサーバラックに置くことも考慮するとよい。

- **基本対策事項 7.1.2(1)-4 b)「冗長化」について**

  「冗長化」とは、障害や過度のアクセスが発生した場合を想定し、サービスを提供するサーバ装置を代替サーバ装置に切り替えること等により、サービスが中断しないように、情報システムを構成することである。可用性を高めるためには、サーバ装置本体だけでなく、ハードディスク等のコンポーネント単位で冗長化することも考えられる。

  なお、災害等を想定して冗長化する場合には、代替のサーバ装置を遠隔地に設置することが望ましい。

- **基本対策事項 7.1.2(1)-5「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バージョンも含め定める」について**

  「(解説) 基本対策事項 7.1.1(1)-4「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バージョンも含め定める」について」を参照のこと。

遵守事項

(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。

【 基本対策事項 】

＜7.1.2(2)(b)関連＞

7.1.2(2)-1 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する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

＜7.1.2(2)(c)関連＞

7.1.2(2)-2 情報システムセキュリティ責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずること。

a) **アクセスログ等を定期的に確認する**。
b) IDS/IPS、WAF 等を設置する。
c) 不正プログラム対策ソフトウェアを利用する。
d) ファイル完全性チェックツールを利用する。
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

＜7.1.2(2)(d)関連＞

7.1.2(2)-3 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は、運用状態を復元するために以下を例とする対策を講ずること。

a) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。
b) 定期的な**バックアップ**を実施する。
c) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。
d) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

（解説）

- **遵守事項 7.1.2⑵(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、定期的に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の見直しを行うことが必要である。

- **遵守事項 7.1.2⑵(b)「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」について**

「不適切な状態」とは、サーバ装置のハードウェアの構成が不正に変更されている、又はセキュリティ水準の低下を招くような変更がされている、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。

利用を認めるソフトウェア以外のソフトウェアがインストールされているか否かについては、構成管理ツールを使用するほか、プロセスやその他挙動等を監視する方法もある。また、利用を認めるソフトウェアであっても、利用しない機能については無効化するなどの措置が考えられる。セキュリティパッチについては、6.2.1「ソフトウェアに関する脆弱性対策」を参照のこと。

- **基本対策事項 7.1.2⑵-2 a)「アクセスログ等を定期的に確認する」について**

不正アクセスを検知するために、サーバ装置へのアクセスに関するログのほか、サーバ装置が異常等を検出した際に出力するログ（エラーログ）を確認することも有効である。

アクセスログを確認する際は、運用管理作業の記録、管理者権限を持つ識別コードを付与された者の出退勤記録又は入退室記録等との相関分析を併せて行うことにより、不正なアクセスが行われた可能性を確認することも考えられる。

- **基本対策事項 7.1.2⑵-3 b)「バックアップ」について**

バックアップには、サービスの提供に当たって必要なデータやサービスの利用者が入力したデータのバックアップのほか、運用に必要となるシステム設定のバックアップも含まれる。バックアップの取得方法として、前回内容からの変更部分のみバックアップを実施する方法でもよい。

なお、バックアップの手段や保管場所については、「（解説）基本対策事項 3.1.1(8)-2「災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する」について」も参照のこと。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.1.2(3)(a)「サーバ装置の運用を終了する際」について**

  サーバ装置を廃棄処分する場合やリース契約が終了し返却する場合のほか、当該サーバ装置のサービス又は機能の提供を終了する場合も考えられる。

- **遵守事項 7.1.2(3)(a)「抹消する」について**

  「（解説）遵守事項 7.1.1(3)(a)「抹消する」について」を参照のこと。

7.1.3 複合機・特定用途機器

目的・趣旨

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

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

したがって、複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講ずることが重要である。

遵守事項

(1) 複合機

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

(b) 情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。

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

【 基本対策事項 】

＜7.1.3(1)(a)関連＞

7.1.3(1)-1 情報システムセキュリティ責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、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、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。

＜7.1.3(1)(b)関連＞

7.1.3(1)-2 情報システムセキュリティ責任者は、以下を例とする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。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。
b) 複合機が備える機能のうち利用しない機能を停止する。
c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。
d) 機関等内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。
e) 複合機をインターネットに直接接続しない。
f) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
g) 利用者ごとに許可される操作を適切に設定する。

＜7.1.3(1)(c)関連＞

7.1.3(1)-3 情報システムセキュリティ責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

（解説）

- **基本対策事項 7.1.3(1)-1「「IT 製品の調達におけるセキュリティ要件リスト」を参照」について**

遵守事項 5.2.1(2)(c)及び基本対策事項 5.2.1(2)-6 に規定されている「IT 製品の調達におけるセキュリティ要件リスト」には、複合機について一般的に想定される「セキュリティ上の脅威」が記載されているため、それらが自身の運用環境において該当する場合には対抗する必要がある。当該リストには、「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

なお、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、利用環境や複合機に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

- **基本対策事項 7.1.3(1)-2 a)「適切なセキュリティ設定」について**

自身の利用環境における脅威に対抗するために、運用前に複合機のセキュリティ機能の設定値が適切な値となっていることを確認する必要がある。例えば、管理者パスワードが初期設定のままでないか、イメージスキャナで複合機内部に保存したデータへのアクセス制御設定が適切であるかなどを確認する必要がある。

- **基本対策事項 7.1.3(1)-2 b)「利用しない機能を停止」について**

  運用において必要としていない機能が利用者の意図に反して動作していた場合、セキュリティ対策が不十分になっていることが考えられる。対策が不十分である場合は、情報セキュリティインシデントが発生するおそれがあるため、運用上不必要な機能については、運用前に停止した状態にする必要がある。

- **基本対策事項 7.1.3(1)-2 c)「操作パネルで利用者認証が成功した者のみ印刷が許可される機能」について**

  複合機の設置環境によっては、印刷された文書が第三者に閲覧される可能性がある。そのような場合には、印刷の際に複合機内部に一旦データを保存し、複合機本体の操作パネルで主体認証に成功した者だけが印刷できるように設定しておくなどの対策を講ずる必要がある。

- **基本対策事項 7.1.3(1)-2 d)「複合機の内部において接続されないようにする」について**

  複合機にモデム機能が搭載されている場合、公衆通信回線から複合機に接続された後に、複合機を経由して機関等 LAN にアクセスされる可能性がある。そのため、モデム機能の無効化等の対策が必要となる。

- **基本対策事項 7.1.3(1)-2 f)「ファイアウォール等の利用により適切に通信制御を行う」について**

  トナー残量の通知や遠隔地からの状態監視等の遠隔保守サービス等を利用する場合には、インターネットを介して外部と通信する必要が生じる。その際には必要最小限の通信のみを許可するようにする必要がある。また、ファイアウォール等の通信制御を行うための機器に例外的な設定を行う場合には、その設定によって脆弱性が生じないようにする必要がある。

- **基本対策事項 7.1.3(1)-2 g)「利用者ごとに許可される操作を適切に設定する」について**

  様々な機能を備えている複合機では、利用者ごとに許可される操作権限の管理が重要となる。例えば、ファクシミリで受信したデータを複合機内部に保存する場合のデータの読み出し権限等を適切に設定していない場合には、情報の漏えいにつながる可能性がある。

- **基本対策事項 7.1.3(1)-3「別の手段で対策を講ずる」について**

  内蔵電磁的記録媒体の全領域完全消去機能を備えていない複合機については、調達元の機関等において内蔵電磁的記録媒体の全ての情報を抹消することが困難であるため、外部委託先と情報の抹消サービスを契約するなどの情報の漏えいへの対策を講ずることが必要となる。

遵守事項

(2) IoT 機器を含む特定用途機器

(a) 情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、**当該機器の特性に応じた対策を講ずる**こと。

【 基本対策事項 】

＜7.1.3(2)(a)関連＞

7.1.3(2)-1 情報システムセキュリティ責任者は、特定用途機器の特性に応じて、以下を含む対策を講ずること。ただし、使用している特定用途機器の機能上の制約により講ずることができない対策を除く。

a) 特定用途機器について、**主体認証情報を初期設定から変更**した上で、適切に管理する。

b) 特定用途機器にアクセスする**主体に応じて必要な権限を割り当て、管理**する。

c) 特定用途機器が備える機能のうち**利用しない機能を停止**する。

d) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器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に接続しない。

e) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により**適切に通信制御を行う**。

f) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、**バージョンアップやセキュリティパッチの適用**、アクセス制御等の対策を講ずる。

g) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

h) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する。

（解説）

- **遵守事項 7.1.3(2)(a)「当該機器の特性に応じた対策を講ずる」について**

例えば、テレビ会議システム、IP 電話システム等は機関等 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。近年、あらゆるものがインターネットにつながる IoT が注目されてきているが、これらの IoT 機器等の脆弱性がサイバー攻撃の標的となることが懸念される。また、これら情報システムを構成する機器が内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。このような脅威に対抗するために、情報システムや端末、サーバ装置に対して定められた遵守事項や基本対策事項を参考にして、IoT 機器を含む特定用途機器の対策を講じる必要がある。

特定用途機器の導入時に注意すべき点として、特定用途機器の導入後にサポートが

適切に行われるかどうかという点や、特定用途機器の設定を適切に変更できるかどうかという点が挙げられる。

サポートが適切に行われなかったり、設定を適切に変更できなかったりする場合、必要なセキュリティ対策を講ずることが困難になる可能性がある。そのため、導入時にサポートの提供や設定変更が可能な範囲について仕様に盛り込むなどして、必要なセキュリティ対策を講ずることができる特定用途機器を調達することが必要がある。

なお、IoT 機器等については、セキュリティ対策に係るガイドラインや手引書が公表されていることから、必要に応じて参考にするとよい。

参考：IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン」（平成 28 年 7 月公表）
（http://www.iotac.jp/wg/security）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000108.html）
（http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html）

参考：IPA「IoT 開発におけるセキュリティ設計の手引き」（平成 28 年 12 月公表）
（https://www.ipa.go.jp/security/iot/iotguide.html）

参考：IPA「ネットワークカメラシステムにおける情報セキュリティ対策要件に関するチェックリスト　第２版」（平成 30 年３月公表）
（https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html）

上記のウェブサイトのアドレスは、平成 30 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.1.3(2)-1 a)「主体認証情報を初期設定から変更」について**

特定用途機器の一部の機種は、遠隔保守や外部ネットワークからの機能利用を目的として、インターネット回線等の通信回線を経由して、特定用途機器へログインする機能を有しているものがあるが、この機能を悪用したサイバー攻撃の手法が存在する。具体的には、工場出荷時に設定される初期のパスワードを変更せずに運用している特定用途機器を標的とし、一般によく使われる初期の識別コードとパスワードの組合せを用いて辞書攻撃を行い、不正なログインを試行するものである。特定用途機器の運用保守等のために、インターネット回線等の通信回線を介してログインを行う必要がある場合は、このような攻撃を受けることを想定して、特定用途機器の運用開始前に初期設定されているパスワード等の主体認証情報を変更することが重要である。

- **基本対策事項 7.1.3(2)-1 b)「主体に応じて必要な権限を割り当て、管理」について**

特定用途機器の運用においては、設定変更などを行う管理者権限と、状態の確認や閲覧等を行うだけの一般権限のアカウントを別にして使い分けることで、内部不正や誤操作の防止につながる。さらに管理者権限の利用を許可するアクセス元を制限するといった他の対策と複合的に組み合わせることによって、悪意のある第三者によって設定変更されたり攻撃に利用されたりする可能性を低減することが可能である。

- **基本対策事項 7.1.3(2)-1 c)「利用しない機能を停止」について**

「(解説) 基本対策事項 7.1.3(2)-1 a)「主体認証情報を初期設定から変更」について」にも示すとおり、インターネット回線等の通信回線を経由して特定用途機器へ不正なログインを試行する攻撃手法においては、Telnet のような汎用のプロトコルを利用したサービスが標的とされることがある。インターネット上には、グローバルアドレスに対してポートスキャンを行いレスポンスを返すサービスや、特定用途機器の情報を公表しているサイトが存在しており、そのようなサイトにセキュリティの弱いサービスや特定用途機器が登録されてしまうと、サイバー攻撃を企図する者の標的となる恐れがある。

このような攻撃手法への対抗策として、Telnet サービスや FTP サービス等のうち利用していないものは全て停止し、不正なログイン試行を無効化することが重要である。

なお、特定用途機器の中にはサービスの停止などの設定を変更することができないものも存在するため、導入に当たっては、係る設定を変更できることを仕様に盛り込むといったことを検討するとよい。一方で、代替の特定用途機器がなかったり、既に導入済みで更改まで使用を継続しなければならない場合も考えられる。そういった場合には適切に通信制御を行う等の対策を講ずることが重要である。

- **基本対策事項 7.1.3(2)-1 e)「適切に通信制御を行う」について**

特定用途機器への不正アクセスが生じると、不正プログラムへの感染、不正操作、情報窃取等の不正行為が行われるおそれがある。そのため、特定用途機器への通信制御を適切に実施し、不正アクセスを防止するとともに、不正行為が行われた場合の被害範囲を限定するなどの対策を行うことが重要である。

特定用途機器への通信制御は、例えば以下の方法により実施することが考えられる。

- 特定用途機器に実装されている通信制御機能を有効にする。
- 接続しているファイアウォール等で通信制御を行う。
- ルータ等を利用して、特定用途機器に直接グローバル IP アドレスを割り当てない。

- **基本対策事項 7.1.3(2)-1 f)「バージョンアップやセキュリティパッチの適用」について**

特定用途機器のソフトウェアの脆弱性を放置すると、脆弱性を悪用されるおそれがあることから、脆弱性が公表された場合は、ソフトウェアのバージョンアップやセキュリティパッチの適用により脆弱性対策を速やかに講ずることが重要である。特定用途機器の機種によっては、脆弱性対策が困難なものがあることに留意する必要がある。そのような特定用途機器がサイバー攻撃の踏み台にされるなどし、意図せず攻撃に加担してしまう可能性も考えられる。このような問題を回避するためには、特定用途機器の導入に当たって、脆弱性対策を実施することを仕様に盛り込むことを検討するとよい。具体的には、ベンダがセキュリティパッチを提供していること、ベンダが外部から報告を受けた脆弱性に対応するだけでなく開発時に利用したライブラリ等の脆弱性についても対応可能な体制となっていること等を確認することが考えられる。

また、運用保守の委託先に対して、運用している特定用途機器の脆弱性に対応する必要があることを認識させることも重要である。さらに、委託先に対して、特定用途機器

のバージョンアップやセキュリティパッチの適用手順、実施に当たってのサービスへの影響を把握させることも重要である。

調達元の機関等で対処できないような機器の場合には、特定用途機器の調達に当たって保守契約締結の必要性等について検討することも重要である。

7.2 電子メール・ウェブ等

7.2.1 電子メール

目的・趣旨

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

なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 電子メールの導入時の対策

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

(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

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

(d) 情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。

【 基本対策事項 】

＜7.2.1(1)(b)関連＞

7.2.1(1)-1 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、以下を例とする職員等の主体認証を行う機能を備えること。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

＜7.2.1(1)(c)関連＞

7.2.1(1)-2 情報システムセキュリティ責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。

a) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC （ Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策を行う。

b) SPF、DKIM、 DMARC 等の送信ドメイン認証技術による受信側の対策を行

う。

c) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。

＜7.2.1(1)(d)関連＞

7.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。

a) SMTP によるサーバ間通信を TLS（SSL）により保護する。

b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。

（解説）

- **遵守事項 7.2.1(1)(a)「不正な中継」について**

不正な中継が行われると、迷惑メールの送信等に悪用される問題がある。これにより、電子メールサーバや通信回線のリソースが消費されて運用に支障をきたす、不正な中継を行う電子メールサーバとして他の電子メールサーバ等から接続や電子メールの転送を拒否される、又は迷惑メールの受信者からの苦情や問合せへの対応が必要になるなどの問題が生じるおそれがある。これらを回避するため、電子メールの不正な中継を行わないように電子メールサーバを設定することが必要である。

- **遵守事項 7.2.1(1)(d)「サーバ間通信の暗号化」について**

相手先サーバが暗号化に対応していない状況も考慮しなければならない。自らが送信側となる際には、相手先が暗号化に対応可能であることを確認し、確認が取れた場合には以降の通信を暗号化することが求められる。また、自らが受信側となる際には、相手先から暗号化の要求に応じることが求められる。

暗号化された通信の監視については、「（解説）遵守事項 5.2.1(2)(a)(イ)「監視するデータが暗号化されている場合は、必要に応じて復号」について」を参照のこと。

- **遵守事項 7.2.1(1)(d)「対策を講ずること」について**

技術的な事情等により対策に時間を要する場合は、「インターネット通信のセキュリティ強化と利用者に対する配慮について」（平成 29 年 7 月 10 日　内閣官房内閣サイバーセキュリティセンター事務連絡）に基づいて、計画的に対策を推進することが求められる。

- **基本対策事項 7.2.1(1)-2 a)「送信ドメイン認証技術」について**

送信ドメイン認証技術には、SPF、DKIM 等が挙げられる。これらは、送信する電子メールのドメインを管理する DNS サーバに登録・公開された送信側の電子メールサーバの情報や電子署名で使用する公開鍵を利用することで実現する。

また、送信ドメイン認証技術によって電子メールのなりすましを防止するためには、送信した電子メールの正当性を受信者が確認できるようにするための送信側の対策と、受信した電子メールの正当性を判定して、なりすまされた電子メールから受信者を保護するための受信側の対策があり、両方の実施が求められる。

DMARC は、送信元ドメインに対し、効果的な認証基準が得られるよう、認証技術を

自身のインフラに実装するに当たっての、より統合的な手法を定義するとともに、電子メールの受信者が SPF、DKIM 等に係る送信ドメイン認証の詳細な結果を電子メールの送信者にフィードバックするフレームワークを実現するための仕様である。

これら送信ドメイン認証技術の導入に当たっては、技術的な解説や導入の手順などを詳細に解説した、迷惑メール対策推進協議会による「送信ドメイン認証技術導入マニュアル」を参考にするとよい。

参考：迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル　第２版」
（https://www.dekyo.or.jp/soudan/contents/anti_spam/report.html#dam）

上記のウェブサイトのアドレスは、平成 30 年 X 月 X 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.2.1(1)-2 a)「送信側の対策」について**

送信ドメイン認証技術による送信側の対策として、電子メールで使用するドメインを管理する DNS サーバに、受信者が電子メールの正当性を確認するための情報を登録し公開する必要がある。例えば、SPF の場合は送信側の電子メールサーバの情報を DNS サーバに登録する。また、DKIM の場合は電子メールに付与する電子署名の検証に使用する公開鍵を DNS サーバに登録する。DMARC については、DNS サーバに、受信側でなりすましと判定した電子メールの取扱いについてのポリシーを記載する。

なお、SPF については、以下の事項に留意すること。

- 電子メールを利用していないドメインについても、その情報を SPF レコードに登録する。（「SPF レコード」とは、SPF において、DNS サーバの TXT レコードに記述される送信側の電子メールサーバ等の情報をいう。）
- SPF レコードの末尾は、”~all”ではなく”-all”を記述する。
- SPF レコードは、チェックツール等で、文法的に記述間違いのないことを確認する。
- なりすましの防止策のため、ウェブによるサービス等も含め全く利用していない、又は将来にわたって利用の予定の無いドメインについては、なりすましの防止策を講ずるか、ドメイン名の登録を廃止する。
- 民間事業者等において提供されている、他の利用者と共用する電子メールサービスを利用する場合は、機関等をなりすました電子メールが、当該電子メールサービスを利用する他の利用者から送信されないような仕組みを備えていることを確認する。他の利用者と共用しない専用の IP アドレスを割り振ることが可能なサービスが提供されている場合は、当該サービスの利用を検討する。

- **基本対策事項 7.2.1(1)-2 b)「受信側の対策」について**

送信ドメイン認証技術による受信側の対策としては、受信した電子メールに対し送信ドメイン認証に基づくなりすまし判定（例えば SPF の場合、受信時に通信を行った送信側の電子メールサーバと、受信した電子メールに記載されている送信側ドメインを管理する DNS サーバに登録されている送信側の電子メールサーバの情報との比較

による判定）を行い、なりすましと判定した場合には、以下に例示するような電子メールの受信者への注意喚起等を行うことが挙げられる。

- 電子メールの件名（Subject）や本文への注意喚起文の挿入
- 電子メールクライアントの機能によるラベリングやメッセージの表示
- 電子メールクライアント又は電子メールサーバにおける電子メールの隔離や削除等のフィルタリング

また、送信者が DMARC に対応している場合は、送信者のポリシーに従って隔離や受信自体の拒否を行うことが可能となる。

- **基本対策事項 7.2.1(1)-2 c)「S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名」について**

外部に一斉送信する電子メールに、組織の電子証明書で電子署名をすることは、電子メールのなりすまし防止の観点から効果的である。

また、通常のメールについては、職員等に電子証明書を配布し、電子署名を付与することにより、電子メールクライアントによっては、同時に電子メールを自動的に暗号化することが可能となるというメリットもある。

- **基本対策事項 7.2.1(1)-3 a)「SMTP によるサーバ間通信を TLS（SSL）により保護」について**

メールサーバ間通信である SMTP によるサーバ間通信には、データを保護する仕掛けがないことから、これを TLS（SSL）により保護することが、インターネット上でのデータの盗聴及び改ざんの防止に有効である。

ただし、相手先サーバが TLS（SSL）に対応していない場合は、通常の SMTP で送受信することになる。相手先が TLS（SSL）に対応しているかを確認した後に TLS（SSL）接続を確立する標準的な手法は、STARTTLS(RFC3207)で規定されている。

なお、SMTP による電子メール転送は複数のサーバを経由することがあり、最終的な受信先のサーバまでの通信が全て保護されることは必ずしも保障されない点に留意しなければならない。確実に保護するべきデータは、電子メールの送信者が予め暗号化等の対策を行った上で送信する必要がある。

- **基本対策事項 7.2.1(1)-3 b)「S/MIME 等の電子メールにおける暗号化及び電子署名」について**

電子メールを、S/MIME で保護することは、電子メールの盗聴及び改ざんを防止する観点から効果的である。

S/MIME は電子メール自体に暗号化等を行うものであり、電子メールクライアント側で処理されるセキュリティ機能である。このため、送受信する相手側の電子メールクライアント側も S/MIME に対応している必要がある。

7.2.2 ウェブ

目的・趣旨

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

なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) ウェブサーバの導入・運用時の対策

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

(ｱ) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

(ｲ) ウェブコンテンツの編集作業を担当する主体を限定すること。

(ｳ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

(ｴ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

(ｵ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。

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

【 基本対策事項 】

＜7.2.2(1)(a)(ア)関連＞

7.2.2(1)-1 情報システムセキュリティ責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。

a) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

b) ディレクトリインデックスの表示を禁止する。

c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

＜7.2.2(1)(a)(イ)関連＞

7.2.2(1)-2 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例とするウェブサーバの管理や設定を行うこと。

a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。

b) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

＜7.2.2(1)(a)(ウ)関連＞

7.2.2(1)-3 情報システムセキュリティ責任者は、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管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。

a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。

b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

＜7.2.2(1)(a)(エ)関連＞

7.2.2(1)-4 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。

a) ウェブコンテンツの更新の際は、**専用の端末**を使用して行う。

b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、**情報セキュリティを確保した管理**を行う。

＜7.2.2(1)(a)(オ)関連＞

7.2.2(1)-5 情報システムセキュリティ責任者は、通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を含むウェブサーバの実装を行うこと。

a) **TLS（SSL）機能を適切に用いる**。

b) TLS（SSL）機能のために必要となるサーバ証明書には、**利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局**（証明書発行機関）により発行された電子証明書を用いる。

c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された**「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。

（解説）

- **遵守事項 7.2.2(1)(a)(オ)「対策を講じること」について**

技術的な事情等により対策に時間を要する場合は、「インターネット通信のセキュリティ強化と利用者に対する配慮について」（平成 29 年 7 月 10 日内閣官房内閣サイバーセキュリティセンター事務連絡）に基づいて、計画的に対策を推進することが求められる。

- **基本対策事項 7.2.2(1)-1 a)「CGI 機能」について**

CGI（Common Gateway Interface）とは、ウェブブラウザから送信された文字列を、スクリプト等のプログラムへの入力パラメータとして受け取り、当該スクリプト等をウェブサーバ上で実行するための仕組みである。外部からの文字列に基づいて実行されるスクリプト等は脆弱性の原因となり易い部分であり、細心の注意を払って脆弱性の無いスクリプト等のみを設置しなければならない。そのため、本基本対策事項は、サーバに設置するスクリプト等は必要最低限のものに限定することを求めている。

- **基本対策事項 7.2.2(1)-1 b)「ディレクトリインデックスの表示を禁止する」について**

ウェブサーバの機能であるディレクトリインデックスの表示機能とは、ウェブサイトの公開対象となるディレクトリが、ファイル名を指定しない形式の URL（すなわち、例えば「http://exmaple.go.jp/directory_name/」の形式）又は「index.html」等の所定のファイル名を指定した形式の URL によってアクセスされたときに、当該ディレクトリに存在するファイル名の一覧を自動的に生成して表示する機能である。万が一、公開するつもりのないファイルがディレクトリに混入していた場合、ディレクトリインデックス機能が有効であると、外部から容易にそのファイル名を見つけられてしまい、アクセスされてしまう。本来、公開対象のディレクトリには、非公開にすべきファイルが混入していてはならないところであるが、念のため、本基本対策事項は、ディレクトリインデックスの表示機能を無効にすることを求めている。

- **基本対策事項 7.2.2(1)-1 c)「不要な機能を制限する」について**

不要な機能の典型的な例としては、管理者画面の機能が挙げられる。ウェブコンテンツ作成ツールや CMS には、コンテンツを編集する管理者向けのログイン画面を有するものがある。このログイン画面がインターネットから閲覧可能であると、管理者のパスワードを破って不正にログインされ、ウェブサイトのコンテンツを改ざんされるリスクを生じさせる。管理者画面は、機関等内からのアクセスのみを許可し、インターネットからの利用を制限することを求めている。その他の不要な機能として制限すべき例として、アクセス解析の機能がインターネットから閲覧できるようになっている場合等が挙げられる。

- **基本対策事項 7.2.2(1)-4 a)「専用の端末」について**

ウェブコンテンツを管理する端末では、ウェブコンテンツの管理に関係する作業のみを行い、その作業に関係の無いウェブサイトを閲覧しない、セキュリティ対策が不十分な USB メモリを利用しないなど、情報セキュリティを確保した運用が必要である。また、ウェブサーバのみでなく、ウェブコンテンツを管理する専用の端末においても、不正プログラム対策やソフトウェアに関する脆弱性対策を行うことが重要である。

- **基本対策事項 7.2.2(1)-4 c)「情報セキュリティを確保した管理」について**

ウェブコンテンツを更新する際の主体認証情報について、パスワードを設定する場合は十分な長さと複雑さを持ったものとする、多要素主体認証方式で主体認証を行う機能を設けるなどにより、情報セキュリティを確保することが求められる。また、ウェブコンテンツの更新に利用する識別コードや主体認証情報は、他の情報システムの認

証で使用しているものを使い回さない、ウェブコンテンツを更新する者以外に知らせない、複数の更新を実施する者で共有しないなどの情報セキュリティを確保した管理が求められる。

- **基本対策事項 7.2.2(1)-5 a)「TLS（SSL）機能を適切に用いる」について**

ウェブサーバに TLS（SSL）機能を搭載することにより、利用者が当該ウェブサーバのサイトを「https://」で始まる URL でアクセスできるようになる。「https://」で始まる URL のページ（以下「セキュアページ」という。）へのアクセスは、ブラウザからウェブサーバへの入力及びウェブサーバからブラウザへの出力が自動的に暗号化されて送受信される。

盗聴による情報の漏えいを防止するには、盗聴を防ぐべき情報を出力するウェブページがセキュアページとなっていることが必要である。また、盗聴を防ぐべき情報を利用者に入力させるウェブページを設ける場合には、入力された情報の送信先となる URL がセキュアページとなっていることが必要であり、かつ、利用者に情報を入力させるウェブページ（入力欄が設置されている画面）自体もセキュアページとなっていることが必要である。

ウェブサーバに TLS（SSL）機能を搭載することは、当該ウェブサーバが正当なサーバである(偽のサーバでない)ことを確認できる手段を利用者に提供することにもなる。利用者は、当該サイトを「https://」で始まる URL でアクセスし、エラーなく正常に表示されたことで、当該サーバが当該ドメイン名の正当なサイトのものであると確認することができる。

なお、TLS（SSL）で配信されるページにおいて、TLS（SSL）を使わないコンテンツが含まれていると、警告が表示されたりブロックされたりすることがあるので留意が必要である。また、TLS（SSL）機能を用いるに当たっては、使用するバージョンの脆弱性に関する最新の情報も踏まえ、適切に使用することが必要である。

従来、サービス利用者の個人に関する情報を保護することが特に求められていたが、さらに今日では、全ての情報について、インターネット上の通信経路において第三者による盗聴や改ざんから守り、国民や外部組織が不利益を被らず安心して利用できるようにすることが求められている。このための対策として、ウェブサイト全体に対する TLS（SSL）適用が有効であり、本対策は、海外の政府機関や民間企業のウェブサイトにおいても取組が進められている。

利用者が「http://」から始まる URL を入力した場合であっても常に TLS（SSL）でアクセスさせるためには、次の対策が存在する。

- ブラウザからの TLS（SSL）を使わないアクセス要求に対しては、TLS（SSL）によるサービスへ自動的にリダイレクトする。
- HSTS(HTTP Strict Transport Security：RFC6797)を用いて、上記以降の要求は全て TLS（SSL）にすることをブラウザに伝達する。

携帯電話の一部機種等では TLS（SSL）を使ったサイトを表示できない可能性がある（SHA-2 サーバ証明書に対応していないなどの理由による）。このようなサービス提供を継続する場合は、ウェブサイト全体に TLS（SSL）を適用するサイトとは独立し

て、TLS（SSL）非対応の携帯電話向け専用サイトとすることが考えられる。

- **基本対策事項 7.2.2(1)-5 b)「利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局」について**

TLS（SSL）機能を用いるには、ウェブサーバ側に「サーバ証明書」と呼ばれる電子証明書の設置が必要であり、サーバ証明書はそれを発行する「認証局」から取得する必要がある。サーバ証明書の取得は、政府認証基盤（GPKI）の「アプリケーション認証局」から取得することもできるほか、民間事業者から取得することもできる。

本基本対策事項は、サーバ証明書をどの認証局から取得するかの選択において、「利用者が事前のルート証明書のインストールを必要とすることなくその正当性を検証できる認証局」を選択することを求めている。それ以外の認証局を選択した場合、利用者のウェブブラウザには、サーバ証明書の正当性検証ができないことを示す警告やエラー画面が表示されることになる。この警告やエラー画面は、事前に当該認証局の自己署名証明書をブラウザにルート証明書としてインストールすることによって解消することができる。しかし、一般に、利用者によるルート証明書のインストールは安全に行うことが容易でないものであり、利用者に危険を伴うルート証明書のインストールを強いるのはそもそも避けるべきことである。そのため、本基本対策事項は、利用者にルート証明書のインストールを求めなくても、警告やエラー画面が現れることなく、正常にTLS（SSL）通信ができるよう、適切に認証局を選択してサーバ証明書を取得することを求めている。

なお、ウェブサーバの利用が機関等内の管理された端末からのアクセスに限定されている場合には、対象となる全ての端末に対して事前に安全な方法でルート証明書をインストールすることも可能であるから、そのような管理がなされている場合には、当該ウェブサーバで使用するサーバ証明書として、機関等で独自に用意した認証局から発行されたものを用いることができる。

- **基本対策事項 7.2.2(1)-5 c)「「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」について**

CRYPTREC が発行している「SSL/TLS 暗号設定ガイドライン」は、TLS（SSL）通信での安全性と可用性（相互接続性）のバランスを踏まえた TLS（SSL）サーバの設定方法のガイドラインを示すものである。

このガイドラインでは、「高セキュリティ型」、「推奨セキュリティ型」、「セキュリティ例外型」の 3 段階の設定基準に分けて、各々の要求設定が示されており、どの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みてサーバ管理者が選択するものとされている。

「高セキュリティ型」は、利用例として「政府内利用（G2G 型）のなかでも、高い安全性が要求される通信を行う場合」が示されているように、一般の利用者がウェブブラウザ等で接続することのないサーバの場合を対象とし、専用システム内又は専用システム間で閉じたネットワークを構成して暗号化通信に TLS（SSL）を用いる際に選択すべき設定基準である。

他方、「推奨セキュリティ型」は、利用例に「電子申請等、企業・国民と役所等の電

子行政サービスを提供する場合」とあるように、一般の利用者がウェブブラウザで接続することを前提としたサーバを構成する場合に選択する設定基準であり、普及しているPC、スマートフォン等で問題なく相互接続性を確保できる要求設定が示されたものである。

ガイドラインは、巻末に付録として「チェックリスト」を提供しており、ここに、設定基準ごとに満たすべき要求設定として「プロトコルバージョン設定」、「サーバ証明書設定」、「暗号スイート設定」の具体的な基準が示されているので、これに従うことで、容易に適切なTLS（SSL）設定を行うことができる。

情報システムセキュリティ責任者は、TLS（SSL）を導入するシステムの特性に応じて、どの設定基準が相応しいかを決定し、その設定基準に対応する要求設定に従ったサーバ設定を、「チェックリスト」を活用して確認するなどして、適切に行うことが求められる。

また、ガイドラインは、「サーバ証明書の作成・管理について注意すべきこと」として、鍵ペアの適切な生成方法や鍵の適切な管理方法を示し、また、「さらに安全性を高めるために」として、HTTP Strict Transport Security (HSTS) の設定有効化その他を推奨している。これらについても併せて検討することが望ましい。

参考：CRYPTREC「SSL/TLS暗号設定ガイドライン」（第2.0版）（平成30年5月8日）
（http://www.cryptrec.go.jp/report/cryptrec-gl-3001-2.0.pdf）

上記のウェブサイトのアドレスは、平成30年X月X日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

遵守事項

(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。

【 基本対策事項 】

＜7.2.2(2)(a)関連＞

7.2.2(2)-1 情報システムセキュリティ責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。

a) **SQL インジェクション脆弱性**
b) **OS コマンドインジェクション脆弱性**
c) **ディレクトリトラバーサル脆弱性**
d) **セッション管理の脆弱性**
e) **アクセス制御欠如と認可処理欠如の脆弱性**
f) **クロスサイトスクリプティング脆弱性**
g) **クロスサイトリクエストフォージェリ脆弱性**
h) **クリックジャッキング脆弱性**
i) **メールヘッダインジェクション脆弱性**
j) **HTTP ヘッダインジェクション脆弱性**
k) **eval インジェクション脆弱性**
l) **レースコンディション脆弱性**
m) **バッファオーバーフロー及び整数オーバーフロー脆弱性**

（解説）

- **遵守事項 7.2.2(2)(a)「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」について**

ウェブアプリケーションの開発時には、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が求められる。脆弱性を排除したウェブアプリケーションを実装する方法の詳細については、独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」を参照することも考えられる。

参考：独立行政法人情報処理推進機構「安全なウェブサイトの作り方 改訂第 7 版」
（https://www.ipa.go.jp/security/vuln/websecurity.html）

これらのウェブサイトのアドレスについては、平成 30 年 X 月 X 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.2.2(2)-1 a)「SQL インジェクション脆弱性」について**

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 b)「OS コマンドインジェクション脆弱性」について**

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 c)「ディレクトリトラバーサル脆弱性」について**

ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 d)「セッション管理の脆弱性」について**

ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS（SSL）を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器（CSPRNG）で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

- **基本対策事項 7.2.2⑵-1 e)「アクセス制御欠如と認可処理欠如の脆弱性」について**

ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりすまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2⑵-1 f)「クロスサイトスクリプティング脆弱性」について**

ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる

  - HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
  - URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
  - SCRIPT 要素の内容を動的に生成しないようにする。
  - スタイルシートを任意のサイトから取り込める仕様を排除する。
  - 全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

- **基本対策事項 7.2.2⑵-1 g)「クロスサイトリクエストフォージェリ脆弱性」について**

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに前記 e)の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害（具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害）が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden

パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

- **基本対策事項 7.2.2⑵-1 h)「クリックジャッキング脆弱性」について**

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

- **基本対策事項 7.2.2⑵-1 i)「メールヘッダインジェクション脆弱性」について**

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

- **基本対策事項 7.2.2⑵-1 j)「HTTP ヘッダインジェクション脆弱性」について**

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

- **基本対策事項 7.2.2⑵-1 k)「eval インジェクション脆弱性」について**

ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用し

ていると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 l)「レースコンディション脆弱性」について**

  ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

- **基本対策事項 7.2.2(2)-1 m)「バッファオーバーフロー及び整数オーバーフロー脆弱性」について**

  ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

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で使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、機関等が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバの適切な管理が必要である。

なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) DNS の導入時の対策

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

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

(c) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

【 基本対策事項 】

＜7.2.3(1)(a)関連＞

7.2.3(1)-1 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、以下を例とする名前解決を停止させないための措置を講ずること。

a) コンテンツサーバを冗長化する。

b) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

＜7.2.3(1)(b)関連＞

7.2.3(1)-2 情報システムセキュリティ責任者は、**機関等外からの名前解決の要求に応じる必要性**があるかについて検討し、必要性がないと判断される場合は必要であれば機関等内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずること。

a) キャッシュサーバの設定でアクセス制御を行う。

b) ファイアウォール等でアクセス制御を行う 。

7.2.3(1)-3 情報システムセキュリティ責任者は、**DNS キャッシュポイズニング攻撃**から保護するため、以下を例とする措置を講ずること。

a) **ソースポートランダマイゼーション**機能を導入する。

b) **DNSSEC** を利用する。

＜7.2.3(1)(c)関連＞

7.2.3(1)-4 情報システムセキュリティ責任者は、機関等内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする**当該コンテンツサーバで管理する情報の漏えいを防止するための措置**を講ずること。

a) 外部向けのコンテンツサーバと別々に設置する。

b) ファイアウォール等でアクセス制御を行う。

（解説）

- **基本対策事項 7.2.3(1)-1 a)「冗長化」について**

コンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておくなど、情報と情報システムに要求される可用性の確保に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用等も、遠隔地への設置による冗長化の措置の例である。

また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。

- **基本対策事項 7.2.3(1)-2「機関等外からの名前解決の要求に応じる必要性」について**

不特定の DNS クライアントからの名前解決の要求に応じるキャッシュサーバはオープンリゾルバと呼ばれる。オープンリゾルバは、存在しないホスト名の名前解決の問合せを大量に送信することで上位の DNS サーバの過負荷を狙う DNS 水責め攻撃や、DNS リフレクター攻撃といったサービス不能攻撃等の踏み台として悪用される危険性がある。そのため機関等で利用するキャッシュサーバが機関等外からの名前解決の要求に応じる必要性があるか検討することが必要である。

- **基本対策事項 7.2.3(1)-3「DNS キャッシュポイズニング攻撃」について**

DNS キャッシュポイズニング攻撃とは、DNS のキャッシュサーバにキャッシュされている情報を偽の情報に書き換える攻撃である。この攻撃により、例えば、利用者は

正しい URL のウェブサイトに接続しているつもりでも、書き換えられた偽の情報により不正なウェブサイトに誘導されるといった被害を受ける可能性がある。

- **基本対策事項 7.2.3(1)-3 a)「ソースポートランダマイゼーション」について**

  ソースポートランダマイゼーションとは、キャッシュサーバからコンテンツサーバへの問合せに使用される UDP ポート番号をランダム化する技術である。UDP ポート番号をランダム化することにより、攻撃者がキャッシュポイズニング攻撃を行う際に UDP ポート番号の推測を困難にすることができ、攻撃の成功確率を低下させることが可能となる。

- **基本対策事項 7.2.3(1)-3 b)「DNSSEC」について**

  DNSSEC では、コンテンツサーバによって応答に電子署名が行われ、キャッシュサーバがその署名を検証することで、応答が改ざん等されているか確認することができる。DNSSEC は、公開鍵暗号技術を用いるため、その導入には情報の提供側であるコンテンツサーバと情報の問合せ側であるキャッシュサーバの双方に対応が必要となる。国民等への信頼できるサービスの提供と、機関等の情報セキュリティ向上の観点から、政府ドメイン名を管理するコンテンツサーバ及び機関等のキャッシュサーバに対する円滑な DNSSEC の導入が望ましい。

- **基本対策事項 7.2.3(1)-4「当該コンテンツサーバで管理する情報の漏えいを防止するための措置」について**

  コンテンツサーバにおいて、機関等内のみで使用する名前の解決を提供する場合、内部のみで使用している名前情報を機関等外の者が取得できないようにすることを求めている。

遵守事項

(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。

【 基本対策事項 】

＜7.2.3(2)(c)関連＞

7.2.3(2)-1 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、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（3か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持すること。

（解説）

- **遵守事項 7.2.3(2)(a)「サーバ間で整合性を維持」について**

複数台のコンテンツサーバでドメインに関する情報を保有し管理する場合に、各コンテンツサーバ間でドメインに関する情報の整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバで管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバが管理するドメインに関する情報も更新するといった方法が考えられる。

なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG（Transaction Signature）の利用等が考えられる。

- **遵守事項 7.2.3(2)(b)「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」について**

国内で使用されているドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加される“ドメイン名ハイジャック”と呼ばれる攻撃がある。このような攻撃への対策として、コンテンツサーバで管理するドメインに関する情報について、設定誤りや不正な改ざん等が発生していないかを定期的に確認することで、情報の正確性を維持することを求めている。管理するドメインに関する情報の具体例として、以下に挙げる登録内容等を確認することが考えられる。

- ホストの IP アドレス情報を登録する A（AAAA）レコード
- ドメインの電子メールサーバ名を登録する MX レコード
- なりすましメールを防ぐための SPF レコード等を登録する TXT レコード

なりすまし防止の観点からは、管理するドメインについての SPF レコードが正確であるか否かを確認したり、ドメインを廃止する場合には、ドメインの廃止申請を行い、当該ドメインが確実に廃止されていることを確認したりすることが重要である。

7.2.4 データベース

目的・趣旨

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

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

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

なお、本款の遵守事項のほか、6.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

(1) データベースの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

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

(c) 情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

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

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

【 基本対策事項 】

＜7.2.4(1)(a)関連＞

7.2.4(1)-1 情報システムセキュリティ責任者は、必要に応じて**情報システムの管理者とデータベースの管理者を別に**すること。

7.2.4(1)-2 情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

7.2.4(1)-3 情報システムセキュリティ責任者は、データベースの管理に関する**権限の不適切な付与**を検知できるよう、措置を講ずること。

＜7.2.4(1)(c)関連＞

7.2.4(1)-4 情報システムセキュリティ責任者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。

a) 一定数以上のデータの取得に関するログを記録し、警告を発する。

b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

＜7.2.4(1)(d)関連＞

7.2.4(1)-5 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。

7.2.4(1)-6 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。

a) ウェブアプリケーションファイアウォールの導入

b) データベースファイアウォールの導入

＜7.2.4(1)(e)関連＞

7.2.4(1)-7 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して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

（解説）

- **遵守事項 7.2.4(1)(b)「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」について**

一般的に、データベースの使用形態は図 7.2.4(1)-1 のように、データベースから見たアクセス主体が「人間の利用者」となる場合と、「中間アプリケーションサーバ」となる場合の２つのモデルに分けられる。中間アプリケーションサーバを利用するモデルでは、中間アプリケーションサーバ用にデータベースアクセス用のアカウントを作成して運用する構成となるのが通常である。この構成では、データベースのログにはアクセス主体が中間アプリケーションサーバとして記録されることになるため、不正な操作が行われた場合に実際には誰が操作をしたものかをデータベースのログのみからでは特定できない可能性がある。そのため中間アプリケーションサーバにおいて、データベースの利用者とデータベースへの操作要求とを紐づけてログを取得し、利用者を特定できるようにしておく必要がある。

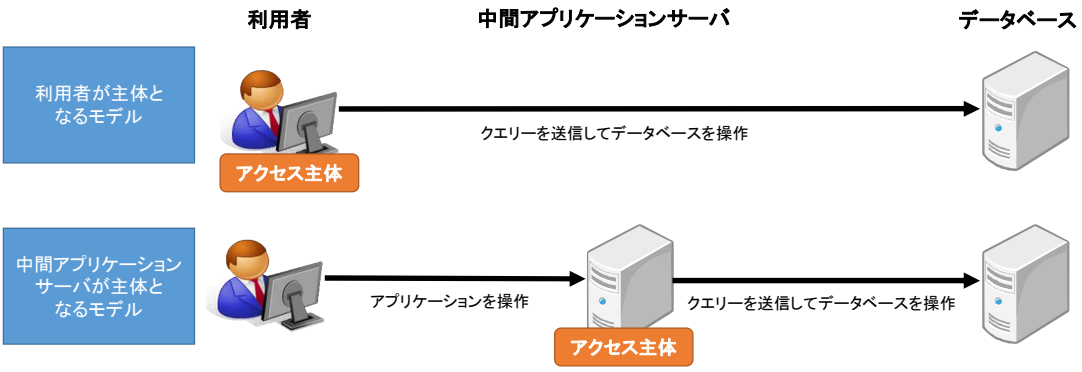


図 7.2.4(1)-1　データベース利用形態モデル

- **遵守事項 7.2.4(1)(e)「適切に暗号化」について**

  データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット･デメリットがあるため､適切な方式を選択することが望ましい。

- **基本対策事項 7.2.4(1)-1「情報システムの管理者とデータベースの管理者を別に」について**

  データベースの管理者は、データベースに格納されるデータの管理、アカウント・権限の管理、ネットワーク環境の構成等の管理を行う。多数の管理者特権を保持するアカウントを奪取された場合、甚大な被害を受けるおそれがあるため、重要な情報を管理するデータベースの管理者の特権を他の管理者と分掌することが望ましい。

- **基本対策事項 7.2.4(1)-3「権限の不適切な付与」について**

  業務の遂行、データベースの運用・管理等をするに当たって不必要なデータに対するアクセス権の付与のほか、他のアカウントに対して権限を付与する権限の付与等がある。

7.3 通信回線

7.3.1 通信回線

目的・趣旨

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

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

遵守事項

(1) 通信回線の導入時の対策

(a) 情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた**適切な回線種別を選択**し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。

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

(c) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

(d) 情報システムセキュリティ責任者は、職員等が**通信回線へ情報システムを接続する際に**、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。**機関等内通信回線へ機関等支給以外の端末を接続する際**も同様とする。

(e) 情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。

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

(g) 情報システムセキュリティ責任者は、機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び

当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

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

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

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

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

【 基本対策事項 】

＜7.3.1(1)(a)(b)関連＞

7.3.1(1)-1 情報システムセキュリティ責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、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て、以下を例とする通信経路の分離を行うこと。

a) 外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。

b) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う。

c) 他の情報システムから独立した専用の通信回線を構築する。

＜7.3.1(1)(c)関連＞

7.3.1(1)-2 情報システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、TLS（SSL）、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

＜7.3.1(1)(d)関連＞

7.3.1(1)-3 情報システムセキュリティ責任者は、機関等内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。

a) 情報システムの機器番号等により接続機器を識別する。

b) クライアント証明書により接続機器の認証を行う。

＜7.3.1(1)(e)関連＞

7.3.1(1)-4 情報システムセキュリティ責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。

a) 通信回線装置を施錠可能なラック等に設置する。

b) 機関等の施設内に敷設した通信ケーブルを物理的に保護する。

c) 通信回線装置の操作ログを取得する。

＜7.3.1(1)(f)関連＞

7.3.1(1)-5 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を構築する場合は、以下を例とする対策を講ずること。

a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。

b) 通信回線及び通信回線装置を冗長構成にする。

＜7.3.1(1)(g)関連＞

7.3.1(1)-6 情報システムセキュリティ責任者は、機関等内通信回線に、インターネット回線や公衆通信回線等の機関等外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。

a) ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。

b) 通信回線装置による特定の通信プロトコルの利用を制限する。

c) IDS/IPS により不正アクセスを検知及び遮断する。

＜7.3.1(1)(j)関連＞

7.3.1(1)-7 情報システムセキュリティ責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。

a) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。

b) 主体認証によりアクセス制御する。

c) 通信内容の暗号化により秘匿性を確保する。

d) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

（解説）

- **遵守事項 7.3.1(1)(a)「適切な回線種別を選択」について**

通信回線に利用する物理的な回線（通信事業者の回線・公衆無線 LAN 回線 等）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ対策が異なることから、適切な回線を選択することが求められる。

例えば、要安定情報を取り扱う情報システムにおいて、通信経路の破壊等による可用性への影響を回避することを目的として仮想的な通信回線を複数の通信経路により構築する場合、物理的にも分離された通信経路上にそれぞれ仮想的な通信回線を構築しなければ、本来求められる可用性の維持に関する要件を満たすことにはならない。

- **遵守事項 7.3.1(1)(d)「通信回線へ情報システムを接続する際に」・「機関等内通信回線へ機関等支給以外の端末を接続する際」について**

  要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続することについては、本項に加えて、遵守事項 8.1.1(1)(c)にて、接続することの可否の判断、可と判断する場合における安全管理措置に関する規定及び許可手続を求めている。

- **遵守事項 7.3.1(1)(j)「ソフトウェアを定め」について**

  通信回線装置としての機能や動作の明確化を行うとともに、ソフトウェアの脆弱性に関する対策を確実なものとするために、通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。通信回線装置の更新ソフトウェアの提供を受けた際に、それを無条件に適用せずに、更新内容等をあらかじめ確認し、適用する必要性を判断することが重要である。

- **遵守事項 7.3.1(1)(k)「契約時に取り決めておく」について**

  公衆通信回線サービスを使用する場合においては、回線の利用規約等に記載されているセキュリティレベルやサービスレベルを合意した上で当該回線を選択する必要がある。役務提供契約で通信回線を利用するなど、機関等において直接回線を調達しない場合については、通信回線に求めるセキュリティレベル及びサービスレベルについて、役務提供事業者と合意形成する必要がある。

- **基本対策事項 7.3.1(1)-1 c)「専用の通信回線を構築」について**

  リスクを検討した結果、他の情報システムと共通的な通信回線を利用すると情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするなどの構成を採用することが考えられるが、過剰なセキュリティ要件とならないように、閉鎖的な通信回線とする必要性を見極めることが重要である。例えば、通信回線を VLAN 等で論理的に分割し、分割された論理的な通信回線ごとに情報セキュリティを確保することで十分要件を満たすのであれば、費用や維持管理の面でメリットがある。このように情報セキュリティ以外の観点とのバランスをとって要件を定めることが重要である。

- **基本対策事項 7.3.1(1)-5 b)「通信回線及び通信回線装置を冗長構成にする」について**

  高い可用性が求められる情報システムを構築する場合は、大規模災害の発生を想定し、通信回線を冗長構成にしておくことが望ましい。また、機関等の施設から外部に敷設する通信回線の管路についても、例えば、異なる通信事業者による複数の経路で構築しておくことで、災害を受けた際に復旧にかかる時間が短縮されるなどの効果が期待される。

遵守事項

(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。

【 基本対策事項 】

＜7.3.1(2)(a)関連＞

7.3.1(2)-1 情報システムセキュリティ責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

7.3.1(2)-2 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を構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

（解説）

- **遵守事項 7.3.1(2)(b)「アクセス制御の設定の見直しを行う」について**

  アクセス制御の設定の見直しにより、設定条件を変更したり又は設定の不備を修正したりする場合は、当該通信回線に接続されている情報システムの情報システムセキュリティ責任者にも事前の連絡及び結果の通知が必要である。

- **遵守事項 7.3.1(2)(c)「ソフトウェアの状態を定期的に調査」について**

  通信回線の重要性、想定される脅威及び機器の特性等から調査の必要性及び調査の間隔を検討する必要がある。例えば、基幹回線等の重要な通信回線を構成する機器、ファイアウォールのようにインターネット等と直接接続されている機器、頻繁にソフトウェアがアップデートされるような機器等は調査の必要性が高く、より短期間に繰り返し調査を実施することが考えられる。また、必要性が低いと判断された機器についても、ソフトウェア等に脆弱性が報告されたり、通信回線の構成変更が発生したりする場合に随時調査することが望ましい。

- **遵守事項 7.3.1⑵(c)「不適切な状態」について**

  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場合や、定められたソフトウェアが動作するための設定が適切でないなどの状態のことを指す。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.1(3)(a)「情報を抹消するなど適切な措置」について**

運用を終了した通信回線装置が再利用されたとき又は廃棄された後に、保存されていた情報が漏えいすることを防ぐための抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。通信回線装置内にも、設定情報や通信ログ等の情報が保存されていることから、サーバ装置及び端末と同様に運用終了時に留意しておくことが必要である。

通信回線装置は通信事業者からリース提供されることがあり、その場合は通信回線の運用終了に伴い通信事業者に装置を返却することになるため、通信回線装置の初期化の手順等本項を遵守するための方法について、通信事業者に確認する必要がある。

遵守事項

(4) リモートアクセス環境導入時の対策

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

【 基本対策事項 】

＜7.3.1(4)(a)関連＞

7.3.1(4)-1 情報システムセキュリティ責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 通信を行う端末の識別又は認証
c) 利用者の認証
d) 通信内容の暗号化
e) 主体認証ログの取得及び管理
f) リモートアクセスにおいて利用可能な公衆通信網の制限
g) アクセス可能な情報システムの制限
h) リモートアクセス中の他の通信回線との接続禁止

（解説）

- **遵守事項 7.3.1(4)(a)「VPN 回線を整備するなど」について**

VPN 回線には、IP-VPN 等の閉域網をベースとした回線とインターネット VPN 等の公衆回線網をベースとした回線があるが、どちらを整備する場合であっても通信内容の暗号化及びリモートアクセス端末（又は利用者）の認証は、必ず講じておくべき措置となる。さらに、特に機密性の高い情報を取り扱う場合においては二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行う）などを考慮してもよい。

- **基本対策事項 7.3.1(4)-1 e)「主体認証ログ」について**

例えば MS-CHAPv2 のような、認証情報を第三者に窃取されるなどの脆弱性が認められる認証プロトコル（リモートアクセスによる利用者認証の際に汎用的に用いられるプロトコル）については、暗号化されている通信路上で認証処理を行い、認証ログを厳重に管理するなどの対策を講ずる必要がある。運用中のサーバ装置や通信回線装置の認証ログを定期的に確認するなどして、不正アクセスが行われていないことに留意することも重要である。

- **基本対策事項 7.3.1(4)-1 f)「利用可能な公衆通信網の制限」について**

リモートアクセスの際に足回りの回線として使用する通信回線については、安全な通信回線サービスに限定することが望ましいが、海外で利用する場合等においては、利

用可能な通信回線サービスが限られており、通信回線サービスを制限できない。このような場合は、「通信回線サービスを限定しない」という前提条件の下、通信回線サービスの安全性や信頼性に関わらず、取り扱われる情報のセキュリティが確保されるよう、VPN 接続時の認証処理及び通信内容の暗号化等の対策を考慮する必要がある。

遵守事項

(5) 無線 LAN 環境導入時の対策

(a) 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

＜7.3.1(5)(a)関連＞

7.3.1(5)-1 情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、以下を例とする対策を講ずること。

a) SSID の隠ぺい
b) 無線 LAN 通信の暗号化
c) MAC アドレスフィルタリングによる端末の識別
d) 802.1X による無線 LAN へのアクセス主体の認証
e) 無線 LAN 回線利用申請手続の整備
f) 無線 LAN 機器の管理手順の整備
g) 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

（解説）

- **基本対策事項 7.3.1(5)-1 b)「無線 LAN 通信の暗号化」について**

暗号化方式として、例えば WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式を選択することが考えられる。WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信を妨害できたりするという脆弱性が報告されており、利用すべきではない。他の暗号化方式においても同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択することが求められる。

- **基本対策事項 7.3.1(5)-1 f)「無線 LAN 機器の管理」について**

無線 LAN 機器の管理については、例えば、以下が考えられる。

- 無線 LAN 機器の電波出力・周波数チャンネル等の管理
- 管理外の無線 LAN アクセスポイント、端末の検出及び除去

なお、無線 LAN 回線を構築する場合は、政府機関から公表している以下の研究会報告書等を参考にするとよい。

参考：総務省「国民のための情報セキュリティサイト」の「情報管理担当者のための情報セキュリティ対策」

（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html）にある、「安全な無線 LAN 利用の管理」のページの解説

参考 : 各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告「無線 LAN セキュリティ要件の検討」（平成 23 年 3 月）
（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）

参考：総務省「無線 LAN ビジネス研究会」報告書（平成 24 年 7 月 20 日）
（http://www.soumu.go.jp/menu_news/s-news/02kiban04_03000093.html）

参考：総務省「無線 LAN ビジネスガイドライン　第 2 版」（平成 28 年 9 月 23 日）
（http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000112.html）

上記のウェブサイトのアドレスは、平成 30 年 X 月 X 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.3.1(5)-1 g)「不正プログラム感染を認知した場合の対処手順」について**

機関等 LAN 端末が不正プログラムに感染した場合は、通常は通信ケーブルを抜去するといった手順が設けられていることが多いが、無線 LAN 回線を使用している場合においては、不正プログラムに感染した端末が無線 LAN 回線を介して他の端末に感染を拡大しないように、無線 LAN 通信を遮断するための手順をあらかじめ定め、職員等へ周知しておく必要がある。例えば、以下の手順が考えられる。

- 感染を認知した際に電磁波を遮断するシールドボックスに感染端末を隔離する。
- 無線 LAN の通信圏外へ端末を移動し、保管する。
- 端末の無線 LAN 通信機能を停止する。

7.3.2 IPv6 通信回線

目的・趣旨

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

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

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

遵守事項

(1) IPv6 通信を行う情報システムに係る対策

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

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

(ｱ) グローバル IP アドレスによる直接の到達性における脅威

(ｲ) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

(ｳ) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(ｴ) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.2(1)(b)(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」について**

  IPv6 通信を想定して構築する情報システムにおいて、グローバル IP アドレスによる通信パケットの直接到達性における脅威に対抗するために、以下を例に対策を講ずることが考えられる。

- 不正な機器からの経路調査コマンド（traceroute 等）への応答の禁止
- ICMP エコー要求への応答の禁止
- 許可した宛先からのみアクセス可能とするなどの経路制御の設定
- サービス不能攻撃の検知及びフィルタ

- **遵守事項 7.3.2(1)(b)(イ)「不正アクセスの脅威」について**

IPv6 の特徴として、アドレスが長いこと、アドレスの省略形が複数パターン存在して一意に定まらない可能性があること、端末が複数の IP アドレスを持つこと等が挙げられる。このため、複雑なアクセス制御の設定が必要になり、設定不備等による不正アクセスにつながるリスクが想定される。

対策としては、外部ネットワークとの通信において、OSI 基本参照モデルのネットワーク層（第３層）及びトランスポート層（第４層）を中心にフィルタリングを行う機能及び断片化された通信の再構築を行う機能を適切に設定すること等、通信機器を流れる通信そのものを制御することが挙げられる。

なお、IPv6 通信を想定して構築する情報システムにおいて、IPv6 のログを取得し、分析する場合は、IPv6 アドレスでは桁数が大幅に増えること等から、IPv6 対応のログの解析ツールを利用することで、IPv6 アドレスの読み間違い等の運用上の作業ミスを軽減するための対策を検討することが望ましい。

- **遵守事項 7.3.2(1)(b)(ウ)「共存させる際の処理考慮漏れに起因する脆弱性」について**

IPv6 通信プロトコルに対応している端末やサーバ装置には、多様な IPv6 移行機構（デュアルスタック機構、IPv6-IPv4 トンネル機構等）が実装されている。それらの IPv6 移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用に当たっては、セキュリティホールの原因をつくらないよう十分な検討と措置が必要である。

例えば、デュアルスタック機構を運用する場合には、IPv4 のプライベートアドレスを利用したイントラネットの情報システムであっても外部ネットワークとの IPv6 通信が可能となるため、デュアルスタック機構を導入したサーバ装置及び端末を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4 トンネル機構を運用する場合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間の IPv6 通信が既設の IPv4 ネットワークを使って可能となるため、機関等のネットワークが外部から攻撃される危険性がある。管理されたサーバ装置及び端末以外のトンネル通信を当該 IPv4 ネットワークに設置されたファイアウォールにて遮断するなど、不適切な IPv6 通信を制御する対策が必要である。

- **遵守事項 7.3.2(1)(b)(エ)「IPv6 アドレスの取扱い考慮漏れに起因する脆弱性」について**

IPv4 のみに対応する機器及びソフトウェアが IPv6 ネットワーク上で動作する際、システム内部での IP アドレスの取扱いが IPv4 に依存している場合、IPv6 アドレスが取り扱えない、若しくはバッファオーバーラン等を引き起こす可能性があるというリスクを認識し、これが無いことを確認するなどが挙げられる。統合認証システムや、シ

ステム間連動を行うようなアプリケーションでは、IPv4/IPv6 が混在した状況でも適切なシステム連携を行う必要がある。

また、「IPv4 対応システムが IPv6 アドレスに対応するため、IPv6／IPv4 コンバータ等が使用される場合がある。このような場合、内部からは個別の IPv6 アドレスを特定できないため、通信ログの取得やパケットフィルタリング等の機能を実装し運用する際等において留意する必要がある。

遵守事項

(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。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.2(2)(a)「IPv6 通信を抑止するなどの措置」について**

複数の機関等の間及び機関等内のみで利用する情報システムについて、通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する必要がある。

IPv6 通信を想定していない通信回線においては、ファイアウォールや IDS/IPS 等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能なサーバ装置及び端末においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該サーバ装置及び端末への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、サーバ装置及び端末と外部のネットワークとの間に情報システムの利用者や情報システムの運用管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないようサーバ装置及び端末を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。

なお、「政府情報システムに係る IPv6 対応の取組について」（2011 年 11 月 2 日各府省情報化統括責任者（CIO）連絡会議決定）において IPv6 対応の取組を進めることが確認されているが、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を抑止又は遮断するための措置を講ずることが必要である。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

目的・趣旨

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

このため、情報システムの利用に関する規定を整備し、職員等は規定に従って利用することが求められる。

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

遵守事項

(1) 情報システムの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。

(b) 統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。

(c) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で**機関等内通信回線に接続することについての可否を判断**した上で、可と判断する場合は、当該端末（支給外端末を含む）から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた**安全管理措置に関する規定**及び許可手続を定めること。

(d) 統括情報セキュリティ責任者は、**USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順**を定めること。当該手順には、以下の事項を含めること。

(ｱ) 職員等は、**国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体**、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を**契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体**を使用すること。

(ｲ) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組

織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。

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

【 基本対策事項 】

＜8.1.1(1)(a)関連＞

8.1.1(1)-1 統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する規定として、**以下を例とする実施手順を定める**こと。

a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順
b) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順
c) 識別コードと主体認証情報の取扱手順
d) 暗号と電子署名の利用に関する手順
e) 不正プログラム感染防止の手順
f) アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為の防止に関する手順
g) ドメイン名の使用に関する手順

＜8.1.1(1)(b)関連＞

8.1.1(1)-2 統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合の利用手順を、以下を例として定めること。

a) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化
b) 盗み見に対する対策（のぞき見防止フィルタの利用等）
c) **盗難・紛失に対する対策**（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
d) 利用する場所や時間の限定
e) 端末の盗難・紛失が発生した際の緊急対応手順

8.1.1(1)-3 統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合について、以下を含む許可手続を定めること。

a) 利用時の許可申請手続
b) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）
c) **利用期間満了時の手続**
d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

＜8.1.1(1)(c)関連＞

8.1.1(1)-4 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続することの許可手続として、以下を含む手続を規定し、職員等に遵守させること。

a）利用時の許可申請手続

b）手続内容（利用者、目的、利用する情報、端末等）

c）利用期間満了時の手続

d）許可権限者（課室情報セキュリティ責任者）による手続内容の記録

＜8.1.1(1)(d)関連＞

8.1.1(1)-5 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として以下の事項を含めて定めること。

a）主体認証機能や暗号化機能を備える**セキュアな外部電磁的記録媒体**が存在する場合、これに備わる機能を利用する。

b）要機密情報は保存される必要がなくなった時点で速やかに削除する。

c）外部電磁的記録媒体を使用する際には、事前に**不正プログラム対策ソフトウェアによる検疫・駆除**を行う。

d）外部電磁的記録媒体の利用者が利用内容を**貸出簿等に記録する**。

＜8.1.1(1)(e)関連＞

8.1.1(1)-6 統括情報セキュリティ責任者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続として、以下を含む手続を規定し、職員等に遵守させること。

a）利用時の許可申請手続

b）**手続内容**（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）

c）利用期間満了時の手続

d）許可権限者（課室情報セキュリティ責任者）による手続内容の記録

（解説）

- **遵守事項 8.1.1(1)(c)「機関等内通信回線に接続することについての可否を判断」について**

要管理対策区域外においてインターネットに接続した端末（支給外端末を含む）を要管理対策区域において機関等 LAN に直接接続する場合、境界監視やファイアウォール等の多重防御を回避して不正プログラムが直接に機関等 LAN 内に持ち込まれることにより、情報窃取、情報の破壊、サービス不能攻撃の踏み台になること等のリスクが高まる。このため、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）の接続は好ましくない。現時点における業務の都合上、やむを得ずこのような端末（支給外端末を含む）の接続の必要性がある場合には、取り得る情報セキュリティ対策、接続先となる情報システムにおいて取り扱う情報、情報セキュリティインシデント発生時の影響等を適切に評価した上で、総合的な見地から可否の判断を行う必要がある。例えば、要管理対策区域外での端末（支給外端末を含む）の利用時に、機関等外通信回線を通じて機関等の情報システムのみにアクセスできる設定とし、シンク

ライアントや VPN とセキュアブラウザの組み合わせを用いて当該情報システムへリモートアクセスさせるような場合は、上記のリスクを懸念する必要性は低下する。このように取り得る情報セキュリティ対策等を考慮して上記の判断を行うことが求められる。

- **遵守事項 8.1.1(1)(c)「安全管理措置に関する規定」について**

  やむを得ずこのような端末（支給外端末を含む）の接続を行う場合には、利用可能な情報セキュリティ対策技術等を総合的に勘案の上、適切に対策を講じることが必要である。

- **遵守事項 8.1.1(1)(d)「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」について**

  USB メモリ等の外部電磁的記録媒体に関する対策は、情報システムの構成等によって様々であると考えられるが、基本対策事項 8.1.1(1)-5 及び「【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について」を参照しつつ、①端末等の不正プログラム感染、②盗難・紛失等による情報漏えい、③バックドアの埋め込み等のサプライチェーン・リスク、といった脅威に対抗するための利用手順を定める必要がある。また、職員等は当該手順に従う必要がある（遵守事項 3.1.1(4)(e)を参照のこと。）。

  なお、USB メモリ等の外部電磁的記録媒体の管理に際しては、利用手順の整備のほか、組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスの導入も有効である（基本対策事項 6.2.4(1)-2 f)を参照のこと。）。

- **遵守事項 8.1.1(1)(d)「国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体」・「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」について**

  USB デバイスの設計上の脆弱性を悪用するなどして、USB デバイスのファームウェアを不正に書き換えることによる攻撃手法が確認されている。例えば、悪意のある者が、端末を不正プログラムに感染させることを目的に USB メモリのファームウェアを書き換え、当該 USB メモリを攻撃対象者や不特定多数の者等に配ることが考えられる。当該 USB メモリは、USB ポートに挿入されると不正プログラムを自動的に実行し、端末が不正プログラムに感染してしまう。このようなファームウェアを書き換えられた USB デバイスは、不正プログラム対策ソフトウェア等では検出できない場合もあることから、出所が明らかでありかつ適切な取扱いがなされている外部電磁的記録媒体以外のものの使用については禁止する必要があり、本項で規定する利用手順に基づく管理がなされた外部電磁的記録媒体を使用すべきである。

  機関等で使用される外部電磁的記録媒体について、機関等が自組織以外の組織（以下、本解説において「他組織」という。）と、当該他組織が支給する外部電磁的記録媒体を用いて情報の受け渡しをする必要がある場合は、本項に規定する利用手順に定めることとしている対策が、当該他組織において講じられることを担保する必要がある。他組織が機関等である場合は、統一基準群の適用対象であり、上記は担保されるが、他組織

が機関等外の組織の場合は、これを契約により遵守させることが必要である。「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」の例としては、委託事業の成果物を外部電磁的記録媒体に記録した形で受け取るケースが想定される。

なお、業務の都合上、やむを得ず本号で定める媒体以外の外部電磁的記録媒体から情報を受け取らざるを得ない場合は、例外措置として判断し、不正プログラム感染のリスク等を勘案の上、安全確保のために必要な措置を講ずる必要がある。

- **基本対策事項 8.1.1(1)-1「以下を例とする実施手順を定める」について**

a)～e)は、それぞれ遵守事項 8.1.1(3)～(7)において、職員等を名宛人とした対策事項が規定されている。同様に、f)は遵守事項 6.3.1(1)において、また、g)は遵守事項 6.3.2(1)において対策事項が規定されている。本項では、これら規定内容を包含する形で、機関等の実施手順等を定めることを求めている。

なお、統一基準及び本ガイドラインの規定内容を、対策基準に含めて定めることで代替しても差し支えない。

- **基本対策事項 8.1.1(1)-2 c)「盗難・紛失に対する対策」について**

一般的に、以下に例を挙げる状況では、盗難・紛失が発生しやすいため、要機密情報を含むモバイル端末を携行する場合には十分注意させること。

  - 電車等での移動中に、モバイル端末の入ったかばん等を網棚に置き、そのまま下車する。
  - 飲酒が想定されるいわゆる宴会等でモバイル端末の入ったかばん等を置いたまま帰宅する。

- **基本対策事項 8.1.1(1)-3 c)「利用期間満了時の手続」について**

利用期間満了時は、職員等に報告を求めるよう手続に定める必要がある。特に機密性３情報等の取扱いに注意すべき情報を要管理対策区域外に持ち出す場合においては、以下を例とする管理手順を設けるとよい。

  - 利用期間満了時の連絡が無い場合は、当該利用者に確認する。
  - 利用期間の延長が必要であれば、再手続を要請する。
  - 利用期間満了前に利用が終了した際には、利用終了時に報告を求める。

- **基本対策事項 8.1.1(1)-5 a)「セキュアな外部電磁的記録媒体」について**

「（解説）基本対策事項 3.1.1(6)-2 c)「セキュアな外部電磁的記録媒体」について」を参照のこと。

また、外部電磁的記録媒体に要機密情報を記録する際には、盗難・紛失時の情報漏えいのリスクを低減するために、情報を暗号化することが求められる（基本対策事項 3.1.1(6)-2 a)を参照のこと。）。

- **基本対策事項 8.1.1(1)-5 c)「不正プログラム対策ソフトウェアによる検疫・駆除」について**

外部電磁的記録媒体に対する不正プログラム対策としては、端末等に導入した不正

プログラム対策ソフトウェア等を利用し、USB メモリ等に対して直接スキャンを実施することが考えられる。機関等内通信回線への感染のリスクを低減させるための更なる対策として、いわゆるサンドボックスとなる緩衝環境や機器等を導入し、端末等に接続する前に検疫・駆除を行うといった方法も考えられる。

- **基本対策事項 8.1.1(1)-5 d)「貸出簿等に記録する」について**

外部電磁的記録媒体の盗難・紛失が発生した場合に原因を追跡するために、保管場所から外部電磁的記録媒体を取り出す際や保管場所に返却する等の際に貸出簿等に利用状況を記載することが重要である。また、盗難・紛失が発生したことを速やかに把握するために、適宜貸出簿等の内容を確認するとよい。

貸出簿等の記載事項としては、利用者及び所属、利用開始日時、利用終了日時、機器名、利用する場所、利用目的といったものが考えられる。

- **基本対策事項 8.1.1(1)-6 b)「手続内容」について**

USB メモリ等の外部電磁的記録媒体を利用する際、利用手順に従い貸出簿等に記録することが求められており（基本対策事項 8.1.1(1)-5 d)を参照のこと。）、また利用時に許可が必要な場合は、許可手続に従い手続内容の記載が求められている（基本対策事項 8.1.1(1)-6 b)を参照のこと。）。手続内容が貸出簿等に記録する内容と重複する場合は、業務の効率化の観点から、例えば、貸出簿に一意に識別できる貸出番号の項目を追加し、参照することで手続内容の記載を省略するといった運用が考えられる。

【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について

USB メモリ等の外部電磁的記録媒体に関連する脅威（①②③）及び脆弱性（箇条書き）としては、以下が想定される。

① 端末等の不正プログラム感染
- 利用者、用法等が不明な物が使用されている。
- 外部電磁的記録媒体を接続した際に自動的にプログラムが実行される。
- 不正プログラム対策ソフトウェアによる検疫・駆除を行っていない。

② 盗難・紛失等による情報漏えい
- 利用者、用法等が不明な物が使用されている。
- 運搬の際等に暗号化等の安全管理措置がなされていない。
- 不要な要機密情報が保存されている。

③ バックドアの埋め込み等のサプライチェーン・リスク
- 製造元、製造過程が不明な物が使われる。

上記の脅威及び脆弱性に対しては、表 8.1.1-1 に掲げる対策が想定される。

表 8.1.1-1　USB メモリ等の外部電磁的記録媒体に関する対策の例

脅威	対策	対策の種類	関連する 基本対策事項
①不正プログラム感染	主体認証機能や暗号化機能を備える外部電磁的記録媒体を導入する	調達時の対策	5.2.1(2)関連
	不正プログラムの検疫・駆除機能を備える外部電磁的記録媒体を導入する	調達時の対策	5.2.1(2)関連
	情報を暗号化するための機能を備えたソフトウェアを導入する	調達時の対策	5.2.1(2)関連 6.1.5 関連
	外部電磁的記録媒体の検疫・駆除機能を備える不正プログラム対策ソフトウェアを導入する	調達時の対策	6.2.2(1)関連
	サーバ装置及び端末の自動再生（オートラン）機能を無効にする	技術的な設定	6.2.4(1)-2 c)
	サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする	技術的な設定	6.2.4(1)-2 d)
	サーバ装置及び端末において使用を想定しない USB ポート等を無効にする	技術的な設定	6.2.4(1)-2 e)
	外部電磁的記録媒体の使用前に、不正プログラム対策ソフトウェアや外部電磁的記録媒体に備わる機能による不正プログラムの検疫・駆除を行う	利用時の対策	8.1.1(1)-5 c) 8.1.1(7)関連

②情報漏えい	運搬の際等に主体認証機能や暗号化機能の利用等の安全管理措置を講ずる	利用時の対策	3.1.1(6)-2 c) 8.1.1(1)-5 a)
	要機密情報は保存される必要がなくなった時点で速やかに削除する	利用時の対策	8.1.1(1)-5 b)
③サプライチェーン・リスク	安全と考えられる製造元、製造過程の製品を調達する	調達時の対策	5.1.2 関連
①②③共通	使用可能な媒体の制限や利用方法等に関する手順を定める	管理対策	8.1.1(1)-5
	組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する	管理対策 調達時の対策	6.2.4(1)-2 f)

遵守事項

(2) 情報システム利用者の規定の遵守を支援するための対策

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

【 基本対策事項 】

＜8.1.1(2)(a)関連＞

8.1.1(2)-1 情報システムセキュリティ責任者は、機関等外のウェブサイトについて、職員等が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) ウェブサイトフィルタリング機能

b) 事業者が提供するウェブサイトフィルタリングサービスの利用

8.1.1(2)-2 情報システムセキュリティ責任者は、職員等が不審な電子メールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) 受信メールに対するフィルタリング機能

b) 受信メールを**テキスト形式で表示する機能**

c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアントの導入

d) 受信メールに添付されている**実行プログラム形式のファイルを削除等する**ことで実行させない機能

（解説）

- **遵守事項 8.1.1(2)(a)「職員等による規定の遵守を支援する機能」について**

職員等が対策基準に定めた規定を守ることを前提としつつ、情報システムの仕組みとして、情報セキュリティインシデントが発生しにくい利用環境を職員等に提供することにより、組織全体のセキュリティ水準を確保することを求める事項である。例えば、基本対策事項に示したとおり、閲覧するとウイルス感染被害に遭うことが判明しているサイトや受信した電子メールをフィルタリングして閲覧不可にすることで被害を回避するなどが考えられる。

これ以外にも、例えば、職員等が意図しない相手に電子メールを送信することをシステム的に抑止する対策として以下のような機能を情報システムに導入すること等も考えられる。

- 送信者の電子メールアドレスのドメイン名以外のドメインのアドレスが宛先アドレスに含まれる場合に警告を表示するなど、入力された宛先アドレスをチェックして警告する機能

- To、Cc、Bcc に入力された宛先アドレスの数が設定数以上になっているときに警告する機能
- 添付ファイルがある場合に警告する機能
- 送信メールの件名、本文、添付ファイルにあらかじめ設定した文字列が含まれる場合に警告する機能
- 送信者が送信指示を行った後、あらかじめ設定された時間だけ送信を保留することにより、送信者が誤送信に気が付いた場合に、送信を取り消すことができる機能

- **基本対策事項 8.1.1⑵-2 b)「テキスト形式で表示する機能」について**

いわゆるフィッシング等の脅威が想定される外部からの電子メールを受信する情報システムを対象とした規定である。HTML 形式の電子メールは、その形式の特徴が悪用され、本文中の URL を偽装した電子メールを送ることにより、フィッシング行為や不正プログラムを埋め込んだウェブサイトへの誘引行為に利用されている。フィッシング等の被害に遭うリスクが想定される場合には、テキスト形式や RTF(Rich Text Format)形式等の URL 偽装のリスクの無い形式で表示することが望ましい。

- **基本対策事項 8.1.1⑵-2 d)「実行プログラム形式のファイルを削除等する」について**

実行プログラム形式のファイルとは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。実行プログラム形式のファイルは、不正プログラムを感染させる手段として標的型攻撃等に悪用されることが多いことから、特に電子メールに添付された実行プログラム形式のファイルについては、職員等がこれを開くことができないよう、システム的に抑止する機能を導入することを基本対策事項としている。ファイルを削除等する機能の例としては、電子メールの中継サーバにおいて、中継する電子メールの全てを検査して、実行プログラム形式のファイルが添付ファイルとして含まれている場合にはその添付ファイルを削除する機能が挙げられるほか、中継サーバでの削除に代えて、電子メールを受信した端末側で該当する添付ファイルを開けないようにする機能等が想定される。

また、実行プログラム形式のファイルは、「.zip」、「.lzh」等の圧縮形式のファイルの内部に含められることがあり、職員等が圧縮形式のファイルを展開し、展開後に現れる実行プログラム形式のファイルを開いてしまうことにより、不正プログラムに感染する事態も想定されることから、圧縮形式のファイルの内部に含められた実行プログラム形式のファイルも削除等の対象とする必要がある。

なお、パスワードを用いて暗号化された圧縮形式のファイルについては、当該ファイル中に実行プログラム形式のファイルが含まれるか否かを技術的に検査できないことから、そのような場合は、暗号化された圧縮形式のファイル自体を添付ファイルから削除等する機能の導入を考慮する必要がある。圧縮形式のファイル中のファイルの検査をする機能を導入する代わりに、暗号化の有無にかかわらず圧縮形式のファイルのすべてを削除等する措置を用いてもよい。

これらファイル削除等の機能の導入は、職員等に一定の不便をもたらすことになり得るが、これを実施せず、開いてよいファイルか否かを職員等に添付ファイルの拡張子を個々に確認させる方法を代用策とした状態では、標的型攻撃等を企図した電子メールの添付ファイルを誤って開いてしまう危険性を十分に抑制することは困難であることから、これをシステム的に抑止する機能の導入が推奨される。

遵守事項

(3) 情報システムの利用時の基本的対策

(a) 職員等は、**業務の遂行以外の目的で情報システムを利用しない**こと。

(b) 職員等は、情報システムセキュリティ責任者が**接続許可を与えた通信回線以外**に機関等の情報システムを接続しないこと。

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

(d) 職員等は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、**情報システムセキュリティ責任者の承認を得る**こと。

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

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

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

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

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

(ｲ) 機関等支給以外の端末 要保護情報

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

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

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

【 基本対策事項 】

＜8.1.1(3)(f)関連＞

8.1.1(3)-1 職員等は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。

a) スクリーンロックの設定

b) 利用後のログアウト徹底

c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

（解説）

- **遵守事項 8.1.1(3)(a)「業務の遂行以外の目的で情報システムを利用しない」について**

業務の遂行以外の目的で情報システムを利用した場合の脅威を回避するための規定である。脅威の例としては、意図せず悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染することが想定される。

- **遵守事項 8.1.1(3)(b)「接続許可を与えた通信回線以外」について**

適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の脅威にさらされることを回避するための規定である。

機関等内通信回線であっても機関等外通信回線であっても、許可を得ていない通信回線に接続してはならない。モバイル端末を持ち出した際に接続する通信回線については、機関等内通信回線以外の利用となり、盗聴等の脅威が増大することから、許可されていない通信回線への接続は回避すべきである。ただし、出張先等で利用する通信回線が未定の場合は、事前の許可が難しいことから、回線の種別（通信事業者の回線・公衆無線 LAN 回線等）で管理すること等も考えられる。

なお、機関等支給以外の端末についても、本項と同等の対策を講じることが望ましい。

- **遵守事項 8.1.1(3)(c)「接続許可を受けていない情報システム」について**

機関等内通信回線を保護するための対策である。利用を許可されていないサーバ装置、端末（支給外端末を含む）等を機関等内通信回線に接続することを禁止している。

特に、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を機関等内通信回線に直接接続することについては、それぞれの情報システムについての接続許可を決定する前に、そもそもこのような接続を業務上認める必要があるのかどうかについて、その是非を判断することを遵守事項 8.1.1(1)(c)で求めている。

- **遵守事項 8.1.1(3)(d)「情報システムセキュリティ責任者の承認を得る」について**

職員等が、利用を認めるソフトウェア以外のソフトウェアを利用する必要がある場合に、情報システムセキュリティ責任者に利用を申請し承認を得ることを求める規定である。

なお、承認を得る際には、製品名、バージョン、入手方法（ソフトウェアの入手元となる URL、事業者名等）、入手可能な場合には利用規約等を添付して、情報システムセキュリティ責任者に申請することが望ましい。

- **遵守事項 8.1.1(3)(e)「接続が許可されていない機器等」について**

出所不明の USB デバイスやセキュリティ管理が不十分な私物のスマートフォン等が情報システムに接続されることが許容されていると、不正プログラム感染等のリスクが高まることから、情報システムへ接続可能な機器等（又は接続を禁止する機器等）をあらかじめ定めておくとよい。

「（解説）遵守事項 8.1.1(1)(d)「国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体」・「契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体」について」も参照のこと。

- **遵守事項 8.1.1(3)(g)「定められた利用手順」について**

  職員等に対して、遵守事項 8.1.1(1)(b)において統括情報セキュリティ責任者が定めた利用手順の遵守を求めている。取り扱う情報の格付や取扱制限に応じて、適切に情報処理を行うことが求められる。

- **遵守事項 8.1.1(3)(h)「許可を得る」について**

  職員等に対して、遵守事項 8.1.1(1)(b)において統括情報セキュリティ責任者が定めた許可手続の実施を求めている。利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、これらについても定められた手順に従うことが必要である。

- **遵守事項 8.1.1(3)(k)「許可を得る」について**

  遵守事項 8.1.1(1)(e)において、USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合についての統括情報セキュリティ責任者が定めた許可手続の実施を求めている。外部電磁的記録媒体の利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、定められた手順に従って、適切に措置する必要がある。

遵守事項

(4) 電子メール・ウェブの利用時の対策

(a) 職員等は、要機密情報を含む電子メールを送受信する場合には、それぞれの機関等が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。

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

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

(イ) 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用すると判断する場合。

(ウ) 電子メールを受信する機関等外の者が、職員等から送信された電子メールであることを認知できる場合（政府ドメイン名又は前二号に基づき取得したドメイン名が使用できない場合に限る。）。

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

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

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

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

(ア) 送信内容が暗号化されること

(イ) 当該ウェブサイトが送信先として想定している組織のものであること

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(4)(a)「送受信」について**

「送受信」には電子メールの「転送」が含まれる。したがって、機関等支給以外の電子メールサービスの電子メールアドレスに要機密情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に、自動転送については、許可を受けている場合であっても、当該電子メールに含まれる情報の格付及び取扱制限にかかわらず行われるため、遵守事項 3.1.1(6)に規定されている要機密情報の送信についての遵守事項に違反しないように留意する必要がある。

- **遵守事項 8.1.1(4)(b)(イ)「高等教育機関向けのドメイン名を使用すると判断する場合」について**

  「(解説) 遵守事項 6.3.2(1)(a)(イ)「高等教育機関向けのドメイン名を使用する場合」について」及び「(解説) 遵守事項 6.3.2(1)(a)(イ)「あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらかを使用するべきかを比較考慮の上、判断」について」を参照のこと。

- **遵守事項 8.1.1(4)(c)「不審な電子メール」について**

  「不審な電子メール」とは、受信する覚えのない電子メールであって、電子メール本文中に URL が記載されているもの、実行形式や文書形式のファイルが添付されているもの等が該当する。こういった電子メールについて、むやみに URL のリンク先や添付ファイルを開かないことも重要であるが、開かなかった場合でも他の者が同種の電子メールを受信することも考えられるため、情報提供を行うことも重要である。定められた連絡先としては、CSIRT や当該電子メールを扱う情報システムの情報システムセキュリティ責任者等が考えられる。

- **遵守事項 8.1.1(4)(d)「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」について**

  例えば、以下のようなブラウザのセキュリティ設定項目について、変更すると悪意のあるソフトウェアが端末において実行されること等により、情報の漏えいや、他のサーバ装置及び端末を攻撃することを引き起こすことも考えられるため、変更が可能であったとしても勝手に変更しないようにする必要がある。

  ＜ブラウザのセキュリティ設定項目の例＞

  - ActiveX コントロールの実行
  - Java の実行

- **遵守事項 8.1.1(4)(f)(ア)「送信内容が暗号化されること」について**

  主体認証情報等を入力して送信する場合には、ブラウザの鍵アイコンの表示を確認するなどにより、TLS（SSL）等の暗号化通信が使用され、要機密情報が適切に保護されることを確認することを求める事項である。

  なお、「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」とは、例えばウェブメール本文の入力欄に要機密情報を入力すること等を指す。

- **遵守事項 8.1.1(4)(f)(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」について**

  ブラウザで主体認証情報等を入力して送信する場合には、ウェブサーバの電子証明書の内容から当該ウェブサイトが想定している組織のものであることを確認するなどの方法により、適切でない送信先に当該情報を誤って送信することを回避する必要がある。

  なお、ウェブサイトの閲覧時にウェブサーバの電子証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可

能性があるため、利用を中止する必要がある。

近年において被害が広がっている「フィッシング(Phishing)」と呼ばれる悪質な行為に対しても十分警戒する必要がある。フィッシングは、悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メールを送りつけ、受け取った者にその電子メールに記載された URL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為である。このようなフィッシングの被害を避けるためにも、本項で示す対策を実施することが重要である。

遵守事項

(5) 識別コード・主体認証情報の取扱い

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

(b) 職員等は、自己に付与された識別コードを適切に管理すること。

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

(d) 職員等は、自己の主体認証情報の管理を徹底すること。

【 基本対策事項 】

＜8.1.1(5)(b)関連＞

8.1.1(5)-1 職員等は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。

a) 知る必要のない者に知られるような状態で放置しない。

b) 他者が主体認証に用いるために付与及び貸与しない。

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

＜8.1.1(5)(d)関連＞

8.1.1(5)-2 職員等は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 自己の主体認証情報を他者に知られないように管理する。

b) 自己の主体認証情報を他者に教えない。

c) 主体認証情報を忘却しないように努める。

d) 主体認証情報を設定するに際しては、推測されないものにする。

e) 異なる識別コードに対して、共通の主体認証情報を用いない。

f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。（シングルサインオンの場合を除く。）

g) 情報システムセキュリティ責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

8.1.1(5)-3 職員等は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

b) 主体認証情報格納装置を他者に付与及び貸与しない。

c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。

d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者に返還する。

（解説）

- **遵守事項 8.1.1(5)(a)「自己に付与された識別コード以外の識別コード」について**

自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、合理的な理由が無い限り「なりすまし行為」である。仮に、悪意がなくても、他者の識別コードを使って情報システムを利用することは、許容されてはならない。例えば、何らかの障害により自己の識別コードの使用が一時的に不可能になった場合には、まず、当該情報システムを利用して行おうとしている業務について、他者へ代行処理を依頼することを検討すべきであり、仮に他者の許可を得たとしても、他者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを使って、情報システムを利用するということは制限されなければならない。

業務の継続のために、他者の識別コードを使うことが不可避の場合には、例外措置の手続を行う際に本人の事前の了解に加えて、情報システムセキュリティ責任者の承認を得ることが最低限必要である。また、他者の識別コードを使用していた期間とアクセスの内容を、事後速やかに、情報システムセキュリティ責任者に報告しなければならない。情報システムセキュリティ責任者は、その理由と使用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えることが望ましい。

いずれの場合も、使用する識別コードの本人からの事前の許可を得ずに、その者の識別コードを使って、情報システムを利用することは禁止されるべきである。

- **遵守事項 8.1.1(5)(c)「管理者としての業務遂行時に限定して」について**

例えば、情報システムの OS が Windows であれば、管理者権限なしの識別コードと管理者権限ありの識別コードの両方を付与された場合において、端末の設定変更等の管理者権限が必要な操作をしないときには、管理者権限なしの識別コードを使用し、その一方、管理者権限が必要な操作をするときに限って管理者権限を使用するなどの運用が考えられる。

- **基本対策事項 8.1.1(5)-1 a)「知る必要のない者に知られるような状態で放置しない」について**

多くの場合、識別コード単体は必ずしも秘密ではないが、必要以上の範囲に開示する、又は公然となるような状態で放置しないように求めている。

主体認証には、識別コードと主体認証情報の組合せが用いられる。識別コードの開示範囲を必要最小限に止めることによって、第三者が不正に主体認証を行う可能性をより低くすることができる。そのため、識別コードを適切に管理することが必要である。

- **基本対策事項 8.1.1(5)-1 b)「他者が主体認証に用いるために付与及び貸与しない」について**

情報システムセキュリティ責任者が明示的に共用識別コードとしているもの以外の識別コードを、他の主体と共用してはならない。

- **基本対策事項 8.1.1(5)-1 c)「定められた手続に従い、識別コードの利用を停止する」について**

  識別コードを使用する必要がなくなった場合に、職員等自らが情報システムセキュリティ責任者へ届け出ること等、定められた手続に従い、識別コードを使用できない状態に変更することを求めている。ただし、例えば、人事異動等によって、職員等の識別コードが大規模に変更となる場合や、その変更を情報システムセキュリティ責任者が職員等自らからの届出によらず把握できる場合等、職員等自らの届出が不要となる条件を情報システムセキュリティ責任者が定めてもよい。

- **基本対策事項 8.1.1(5)-2 a)「自己の主体認証情報を他者に知られないように管理する」について**

  例えば、以下に挙げる他者からのパスワード窃取行為に注意する必要がある。

  - パスワードを入力する際に他者が周囲から盗み見する。
  - 他者が管理者を名乗ってパスワードを聞き出す。

  また、以下に挙げる行為は行うべきではない。

  - 自己のパスワードを、内容が分かる状態で付箋等に記入してモニタ、端末本体、及びその周辺に貼付する。
  - 自己のパスワードを、特段の保護をせずに平文のままテキスト形式で保存する。

  など、容易に他者に知られてしまう状態で、情報システム上に記録する。

- **基本対策事項 8.1.1(5)-2 b)「自己の主体認証情報を他者に教えない」について**

  たとえ、他者に処理を代行させる目的であっても、職員等は自己の主体認証情報を他者に教示してはならない。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関係が曖昧になり、アクセス制御、権限管理、ログ管理その他のセキュリティ対策が効果を失う可能性がある。また、教示された者にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己の主体認証情報は他者に「教えない」ことを徹底すべきである。

- **基本対策事項 8.1.1(5)-2 c)「主体認証情報を忘却しないように努める」について**

  他者が容易に見ることができないような措置（施錠して保存するなど）や、他者が見ても分からないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取る行為を禁ずるものではない。むしろ、忘れることのないように努めなければならない。

  なお、本人の忘却によって主体認証情報を初期化（リセット）する場合には、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。

- **基本対策事項 8.1.1(5)-2 d)「推測されないもの」について**

  主体認証情報がパスワードである場合、パスワードに利用者の名前や利用者個人に

関連する情報から簡単に派生させたもの等、容易に推測されるものを用いてはならない。

パスワードとして設定できる文字列の長さにシステム上の上限があるなどの理由により、8 文字程度の短い文字列しか使用できない場合には、辞書に載っているような単語をそのまま用いてはならず、使用する文字種として、アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜるなどして、可能な限りランダム生成に近い文字列（※）を選び、推測されないパスワードを設定することが望ましい。

一方、設定できる文字列の長さに上限がなく、十分に長い文字列をパスワードとして設定する場合には、辞書に載っている単語を用いてよい場合もある。例えば、5 万語の辞書から 3 つの語をランダムに選び(日常の使用頻度が低めの語を選ぶ方が望ましい。)それらを繋げた文字列（その長さは、30 文字を超えることになろう。）をパスワードとするならば、上記※の文字列と同程度に「推測されないもの」となるので、この場合は辞書に載っている単語をそのまま用いてよい。また、この場合、数字や記号を織り交ぜることも必要でない。

何文字以上の文字列ならば数字や記号を織り交ぜる必要がなくなるのかは、選択した文字列のランダム性との関係で決まるので一律の基準はないが、数字や記号を織り交ぜたくないならば長めの文字列を選び、長い文字列を選びたくないならば数字や記号を織り交ぜることになる。

- **基本対策事項 8.1.1(5)-2 e)「共通の主体認証情報を用いない」について**

複数の識別コードを付与されている場合に、それら識別コードに対して共通の主体認証情報を用いると、一つの識別コードに対応する主体認証情報が漏えいした場合に、他方の識別コードを用いた不正アクセスを受ける危険性が高くなる。したがって、共通の主体認証情報を用いてはならない。

- **基本対策事項 8.1.1(5)-2 f)「識別コード及び主体認証情報についての共通の組合せ」について**

複数の情報システムにおいて、共通の識別コードを使用し、かつ、共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に使用されるという情報セキュリティインシデントが発生することが考えられる。したがって、複数の情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを使用しないようにしなければならない。特に、機関等支給の情報システムと機関等支給以外の情報システムとの間では、共通の識別コード及び主体認証情報を使用しないよう注意する必要がある。

- **基本対策事項 8.1.1(5)-3 a)「主体認証情報格納装置を本人が意図せずに使われることのないように」について**

主体認証情報格納装置の例としては、建物への入退や端末ログインに必要となる IC カード等が挙げられる。所有による主体認証方式では、本人でなくとも主体認証情報格納装置を保持する者が正当な主体として主体認証されるため、他者に当該装置を使用されることがないように適切に管理する必要がある。

遵守事項

(6) 暗号・電子署名の利用時の対策

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

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

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(6)(a)「定められたアルゴリズム及び方法に従う」について**

  情報システムにおいて、認められていないアルゴリズムを利用することを禁止しているものである。暗号アルゴリズムは、ファイル単体の暗号化やハードディスク全体の暗号化、ブラウザを使う通信の暗号化等、様々な場面で利用されていることから、利用する場面ごとに適切なアルゴリズムを適切な方法で利用する必要がある。

  情報システムセキュリティ責任者は、職員等の暗号機能の利用において、認められていないアルゴリズムが利用されないよう、あらかじめ情報システムにおいて対処しておくことが望ましい。

- **遵守事項 8.1.1(6)(b)「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」について**

  暗号化された情報の復号又は電子署名の付与に用いる鍵の管理手順として、情報システム共通として鍵の保存手順を定めている場合と、情報システムごとに鍵の保存手順を個別に定めている場合があるので、各情報システムに対応した手順に従うことが求められる。

- **遵守事項 8.1.1(6)(c)「鍵のバックアップ手順に従い、そのバックアップを行う」について**

  暗号化された情報の復号に用いる鍵の滅失により、情報の可用性が損なわれるおそれがあることから、適切に鍵をバックアップすることを求めている。

  バックアップが必要な鍵については、バックアップの取得又は第三者への鍵情報の預託に関する手順等の規定に従う必要がある。

  また、バックアップしてはならない鍵や、鍵情報の複製が、その漏えいに係るリスクを高める可能性があるなどについても留意し、バックアップは必要最小限にとどめることも大切である。

遵守事項

(7) 不正プログラム感染防止

(a) 職員等は、不正プログラム感染防止に関する措置に努めること。

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

【 基本対策事項 】

＜8.1.1(7)(a)関連＞

8.1.1(7)-1 職員等は、不正プログラム対策ソフトウェア等を活用し、不正プログラム感染を回避するための以下措置に努めること。

a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。

b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。

c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。

d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。

8.1.1(7)-2 職員等は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

8.1.1(7)-3 職員等は、不正プログラムに感染するリスクを低減する情報システム（支給外端末を含む）の利用方法として、以下のうち実施可能な措置を講ずること。

a) 不審なウェブサイトを閲覧しない。

b) アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

c) プログラム及びスクリプトの実行機能を無効にする。

d) 安全性が確実でないプログラムをダウンロードしたり実行したりしない。

（解説）

- **遵守事項 8.1.1(7)(a)「不正プログラム感染防止に関する措置に努める」について**

  情報システムの利用に当たっては、職員等自らが不正プログラム感染の予防に努めなければならない。また、不正プログラム対策ソフトウェア等が全ての不正プログラムを検知できるとは限らないことを念頭に入れ、不正プログラムに感染するリスクを低減するために、可能な措置の実施に努める必要がある。

- **遵守事項 8.1.1(7)(b)「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」について

不正プログラムに感染したおそれがある情報システム（支給外端末を含む）については、他の情報システムへの感染等の被害の拡大を防ぐ必要がある。当該情報システムを構成するサーバ装置又は端末（支給外端末を含む）が通信回線に接続している場合には、それを切断するなど感染拡大を防止する措置を行い、2.2.4「情報セキュリティインシデントへの対処」に定められた報告や連絡等の対処を行うことが求められる。

不正プログラムに感染したおそれのある場合の対処について、手順が規定されている場合、その内容に従う必要がある。

- **基本対策事項 8.1.1(7)-1 a)「実行プログラム形式のファイルを実行しない」について**

不正プログラムとして検知された実行プログラム形式のファイルを実行した場合には、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に相当な労力を要することとなるため、このような実行プログラム形式のファイルを実行しないよう努めなければならない。

- **基本対策事項 8.1.1(7)-1 b)「最新の状態に維持する」について**

一般的に不正プログラムはほぼ毎日のように新種や亜種が出現しているため、不正プログラム対策ソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を更新機能や更新プログラムにより最新の状態に維持することで、不正プログラム等に感染することを回避する必要がある。自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。

また、最新の状態に維持する方法としては、端末（支給外端末を含む）ごとに利用者が自動化の設定をする方法のほか、情報システムセキュリティ責任者等が管理する端末を一括して自動化する方法もあるため、情報システムごとに定められた方法に従うこと。

- **基本対策事項 8.1.1(7)-1 c)「自動検査機能を有効にする」について**

手動による対策実施は、実施漏れや遅れが発生する可能性があるため、不正プログラム対策の中で自動化が可能なところは自動化することが望ましい。

自動検査機能の例としては、ファイルの作成や参照のたびに検査を自動的に行う機能等がある。

- **基本対策事項 8.1.1(7)-1 d)「不正プログラムの検査を実施する」について**

本項 c)の自動検査機能が有効になっていたとしても、検査した時点における不正プログラム対策ソフトウェア等では検知されない不正プログラムに感染している危険性が残る。このような危険性への対策として、最新の状態にした不正プログラム対策ソフトウェア等で定期的に全てのファイルについて検査する必要がある。

- **基本対策事項 8.1.1(7)-2「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合」について**

「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合」には、ウェブの閲覧や電子メールの送受信等のネットワークを経由する場合だけでなく、USB メモリや CD-ROM 等の外部電磁的記録媒体を経由する場合も含む。

8.2　機関等支給以外の端末の利用

8.2.1　機関等支給以外の端末の利用

目的・趣旨

機関等の業務の遂行においては、機関等から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず機関等支給以外の端末を利用して情報処理を行う場合がある。この際、当該端末は機関等が支給したものではないという理由で、情報セキュリティ対策が講じられない場合、当該端末で取り扱われる情報セキュリティ水準が、対策基準を満たさないおそれがある。このため、機関等支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、その利用の可否を判断をした上で、職員等に対して機関等における厳格な管理の下で利用させることが必要である。

なお、機関等支給以外の端末の利用に係る情報セキュリティ対策については 7.1.1「端末」及び 8.1.1「情報システムの利用」を参照のこと。

遵守事項

(1)　機関等支給以外の端末の利用可否の判断

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.2.1(1)(a)「求められる情報セキュリティの水準の達成の見込み」について**

  機関等支給以外の端末の導入に当たっては、以下のようなリスクが想定される。

  - 不正プログラムに感染し、要機密情報が外部に漏えいする。
  - 端末の盗難・紛失等により、要機密情報が外部に漏えいする。
  - 利用者の知識不足により、利用者の意図に反して要機密情報が海外のサーバ装置等に保存され、第三者に閲覧される。
  - 家族や知人の端末操作により端末内の要機密情報が外部に漏えいする。

- **遵守事項 8.2.1(1)(a)「可否を判断すること」について**

  個別判断により機関等支給以外の端末の利用を認めてしまうと、「(解説) 遵守事項 8.2.1(1)(a)「求められる情報セキュリティの水準の達成の見込み」について」に記載したリスクが顕在化する可能性が高いことから、機関等支給以外の端末を利用するのであれば、最高情報セキュリティ責任者が予め統一的に判断することを求めている。機関

等支給以外の端末の利用に当たっては、厳格な管理を行うことが不可欠であるため、機関等支給以外の端末の利用を許可するに当たり、機関等としての利用方針を定めて、その利用方針の下、厳格な管理を行うことが求められる。

機関等支給以外の端末の利用方針として、例えば以下の事項の明確化が考えられる。

- 利用を許可する部局・課室等の組織の単位
- 利用を許可する職員等の条件
- 利用を許可する端末の種類（スマートフォン、携帯電話、PC 等）
- 利用する機能（電子メール及びウェブ閲覧に限定 等）

また、機関等支給以外の端末の利用に際して、利用する通信回線やサーバ装置等、情報システム全体として情報セキュリティを確保することが重要であることから、リモートアクセス環境や端末の安全管理措置について、システム機能として提供することも考慮すべきである。

併せて、最高情報セキュリティ責任者による機関等支給以外の端末の利用可否及びその利用方針について、当該事項を対策基準に記載するとともに、職員等へ周知することで機関等支給以外の端末の適切な利用が行われるようにすることも重要である。

遵守事項

(2) 機関等支給以外の端末の利用規定の整備・管理

(a) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の**許可等の手続**を定めること。

【 基本対策事項 】

＜8.2.1(2)(a)関連＞

8.2.1(2)-1 統括情報セキュリティ責任者は、機関等支給以外の端末を利用する際に、以下を含む許可等の手続を整備し、職員等に周知すること。

a) 以下を含む機関等支給以外の端末利用時の申請内容

- 申請者の氏名、所属、連絡先
- **利用する端末の契約者の名義**（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の機種名
- 利用目的、取り扱う情報の概要、要機密情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- **利用する期間**

b) **利用許諾条件**

c) 申請手順

d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順

e) 利用期間満了時の利用終了又は利用期間更新の手続方法

f) **許可権限者**（端末管理責任者）

（解説）

- **遵守事項 8.2.1(2)(a)「許可等の手続」について**

許可等の手続きを定める際には、以下を参考にするとよい。

参考：各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告
「私物端末の業務利用におけるセキュリティ要件の考え方」（平成 25 年３月）
（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/index.html）

参考：総務省スマートフォン・クラウドセキュリティ研究会最終報告
「スマートフォンを安心して利用するために実施されるべき方策」
（平成 24 年６月 26 日）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html）

上記のウェブサイトのアドレスは、平成 30 年６月１日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 8.2.1⑵-1 a)「利用する端末の契約者の名義」について**

  契約者の名義の提示を求めるのは、業務に使用する端末の名義人と使用人の一致を確認するためである。端末の名義人が端末の利用に係る契約者であり、業務への使用や通信費用に係る訴訟リスクを回避するためには、利用申請時に使用人と名義人が一致していることの確認が必要である。

  なお、名義人と使用人である申請者が同一であることを利用条件とする場合は、名義人の確認を求める必要はない。

- **基本対策事項 8.2.1⑵-1 a)「利用する期間」について**

  機関等支給以外の端末を利用する際に、利用の都度申請手続を行うと事務処理が煩雑化する可能性があるため、例えば１年間の利用期間を定め、包括的な許可を与えるなどして事務処理を効率化する方法も考えられる。この場合は、安全管理措置の実施状況について定期的なチェックを行うなどの対応が求められる。

- **基本対策事項 8.2.1⑵-1 b)「利用許諾条件」について**

  職員等に機関等支給以外の端末の利用を許可するに当たり、以下の内容を例とした利用許諾条件を示し、許諾書にサインするなどして利用者の同意を証拠として残しておく必要がある。

  - 情報の格付及び取扱制限に応じた取扱いの遵守
  - 定められた安全管理措置の遵守
  - 組織による利用状況の情報収集の承諾
  - 組織による利用端末の制御及び端末の設定変更の承諾
  - 盗難・紛失時に私的な情報を含めた遠隔データ消去を行うことの承諾（職務上取り扱う情報のみ遠隔消去可能なツールを導入する場合は不要）
  - 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迅速な届出
  - 機種変更や端末交換の際の再届出の遵守
  - その他、情報システムセキュリティ責任者等の管理責任者の指示の遵守

- **基本対策事項 8.2.1⑵-1 f)「許可権限者」について**

  機関等支給以外の端末の利用の許可申請においては、許可権限者である端末管理責任者の許可を得ることになるが、必要に応じて取り扱う情報の管理責任を持つ課室情報セキュリティ責任者の許可（遵守事項 8.1.1(3)(h)で規定。）を同時に得る手続を定めるとよい。

遵守事項

(3) 機関等支給以外の端末の利用時の対策

(a) 職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。

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

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.2.1(3)(b)「要保護情報を機関等支給以外の端末から消去する」について**

  要保護情報を消去することは必須であるが、不必要な情報及び業務用のアプリケーション等についても併せて消去しておくことが望ましい。

付録

1. 情報セキュリティ対策に関連する政府決定等

- サイバーセキュリティ戦略（平成 30 年　月　日　閣議決定）
- 未来投資戦略 2018（平成 30 年　月　日　閣議決定）
- 世界最先端 IT 国家創造宣言・官民データ活用推進基本計画（平成 29 年 5 月 30 日　閣議決定）
- サイバーセキュリティ人材育成総合強化方針（平成 28 年 3 月 31 日　サイバーセキュリティ戦略本部）
- サイバーセキュリティを強化するための監査に係る基本方針（平成 27 年 5 月 25 日　サイバーセキュリティ戦略本部決定）
- 高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 28 年 10 月 7 日　サイバーセキュリティ対策推進会議）
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2015 年 5 月 21 日　内閣サイバーセキュリティセンター）
- 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（2016 年 10 月 25 日　内閣サイバーセキュリティセンター）
- スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書（2016 年 10 月 25 日　内閣サイバーセキュリティセンター）
- 情報セキュリティ監査実施手順の策定手引書（平成 29 年 4 月　内閣官房内閣サイバーセキュリティセンター）
- 政府業務継続計画（首都直下地震対策）（平成 26 年 3 月 28 日　閣議決定）
- 中央省庁業務継続ガイドライン 第 2 版（首都直下地震対策）（平成 28 年 4 月　内閣府（防災担当））
- 中央省庁における情報システム運用継続計画ガイドライン及び関連資料（平成 25 年 6 月 内閣官房情報セキュリティセンター）
- 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）
- 政府におけるサイバー攻撃等への対処態勢の強化について（平成 22 年 12 月 27 日　情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）
- 調達における情報セキュリティ要件の記載について（平成 24 年 1 月 24 日　内閣官房副

長官）

- 情報セキュリティ対策に関する官民連携の在り方について（平成 24 年 1 月 19 日　情報セキュリティ対策推進会議 官民連携の強化のための分科会）
- 情報セキュリティ管理基準（平成 28 年改正版）（平成 28 年経済産業省告示 37 号）
- クラウドサービス提供における情報セキュリティ対策ガイドライン（平成 26 年 4 月　総務省）
- クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013 年度版　経済産業省）
- クラウドセキュリティガイドライン活用ガイドブック（平成 26 年 3 月 14 日　経済産業省）
- 金融機関におけるクラウド利用に関する有識者検討会報告書（平成 26 年 11 月 14 日　公益財団法人 金融情報システムセンター）
- テレワークセキュリティガイドライン（第 3 版）（平成 25 年　総務省）
- 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）　平成 25 年 3 月 1 日　総務省、経済産業省）
- SSL/TLS 暗号設定ガイドライン（平成 30 年 5 月 8 日　CRYPTREC）
- IT 製品の調達におけるセキュリティ要件リスト（平成 26 年 5 月 19 日　経済産業省）
- IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック（2014 年 5 月　独立行政法人情報処理推進機構）
- 安全なウェブサイトの作り方 改訂第 7 版（2015 年 3 月　独立行政法人情報処理推進機構セキュリティセンター）
- 「高度標的型攻撃」対策に向けたシステム設計ガイド（2014 年 9 月　独立行政法人情報処理推進機構セキュリティセンター）
- 無線 LAN セキュリティ要件の検討（平成 23 年 3 月　各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告）
- 「無線 LAN ビジネス研究会」報告書（平成 24 年 7 月 20 日　総務省）
- 無線 LAN ビジネスガイドライン　第 2 版（平成 28 年 9 月 23 日　総務省）
- 私物端末の業務利用におけるセキュリティ要件の考え方（平成 25 年 3 月　各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告）
- スマートフォンを安心して利用するために実施されるべき方策（平成 24 年 6 月 26 日　総務省スマートフォン・クラウドセキュリティ研究会最終報告）
- 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）

- 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成 26 年 12 月 18 日　個人情報保護委員会）
- 行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）（平成 16 年 9 月 14 日付総管情第 84 号　総務省行政管理局長）
- 独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（通知）（平成 16 年 9 月 14 日付総管情第 85 号　総務省行政管理局長）
- デジタル・ガバメント推進標準ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定）
- IoT セキュリティガイドライン（平成 28 年 7 月　IoT 推進コンソーシアム、総務省、経済産業省）
- IoT 開発におけるセキュリティ設計の手引き（2016 年 12 月　独立行政法人情報処理推進機構）
- ネットワークカメラシステムにおける情報セキュリティ対策要件に関するチェックリスト　第２版（平成 30 年３月　独立行政法人情報処理推進機構）

2.　情報セキュリティ対策に関連する法律

〔法律〕

- サイバーセキュリティ基本法（平成 26 年法律第 104 号）

- 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）

- 独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号）

- 行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）

- 独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）

- 公文書等の管理に関する法律（平成 21 年法律第 66 号）

注）詳細については、原文を参照すること。