

政府機関等のサイバーセキュリティ対策のための統一基準
(令和5年度版)

令和5年7月4日

サイバーセキュリティ戦略本部

目次

第1部	総則	1
1.1	本統一基準の目的・適用範囲	1
(1)	本統一基準の目的	1
(2)	本統一基準の適用対象	1
(3)	本統一基準の改定	1
(4)	法令等の遵守	2
(5)	機関等の対策基準	2
1.2	情報の格付の区分・取扱制限	3
(1)	情報の格付の区分	3
(2)	情報の取扱制限	4
1.3	用語定義	6
第2部	情報セキュリティ対策の基本的枠組み	10
2.1	導入・計画	10
2.1.1	組織・体制の整備	10
2.1.2	資産管理	12
2.1.3	情報セキュリティ関係規程の整備	12
2.2	運用	14
2.2.1	情報セキュリティ関係規程の運用	14
2.2.2	例外措置	14
2.2.3	教育	15
2.2.4	情報セキュリティインシデントへの対処	16
2.3	点検	19
2.3.1	情報セキュリティ対策の自己点検	19
2.3.2	情報セキュリティ監査	20
2.4	見直し	21
2.4.1	情報セキュリティ対策の見直し	21
2.5	独立行政法人及び指定法人	22
2.5.1	独立行政法人及び指定法人に係る情報セキュリティ対策	22
第3部	情報の取扱い	23
3.1	情報の取扱い	23
3.1.1	情報の取扱い	23
3.2	情報を取り扱う区域の管理	26
3.2.1	情報を取り扱う区域の管理	26
第4部	外部委託	27
4.1	業務委託	27
4.1.1	業務委託	27
4.1.2	情報システムに関する業務委託	29
4.2	クラウドサービス	31
4.2.1	クラウドサービスの選定（要機密情報を取り扱う場合）	31

4.2.2	クラウドサービスの利用（要機密情報を取り扱う場合）	32
4.2.3	クラウドサービスの選定・利用（要機密情報を取り扱わない場合）	34
4.3	機器等の調達	36
4.3.1	機器等の調達	36
第5部	情報システムのライフサイクル	37
5.1	情報システムの分類	37
5.1.1	情報システムの分類基準等の整備	37
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	39
5.2.1	情報システムの企画・要件定義	39
5.2.2	情報システムの調達・構築	40
5.2.3	情報システムの運用・保守	41
5.2.4	情報システムの更改・廃棄	42
5.2.5	情報システムについての対策の見直し	43
5.3	情報システムの運用継続計画	44
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	44
5.4	政府共通利用型システム	45
5.4.1	政府共通利用型システム管理機関における対策	45
5.4.2	政府共通利用型システム利用機関における対策	45
第6部	情報システムの構成要素	48
6.1	端末	48
6.1.1	端末	48
6.1.2	要管理対策区域外での端末利用時の対策	49
6.1.3	機関等支給以外の端末の導入及び利用時の対策	50
6.2	サーバ装置	52
6.2.1	サーバ装置	52
6.2.2	電子メール	53
6.2.3	ウェブ	54
6.2.4	ドメインネームシステム（DNS）	54
6.2.5	データベース	55
6.3	複合機・特定用途機器	57
6.3.1	複合機・特定用途機器	57
6.4	通信回線	58
6.4.1	通信回線	58
6.4.2	通信回線装置	59
6.4.3	無線 LAN	60
6.4.4	IPv6 通信回線	61
6.5	ソフトウェア	62
6.5.1	情報システムの基盤を管理又は制御するソフトウェア	62
6.6	アプリケーション・コンテンツ	64
6.6.1	アプリケーション・コンテンツの作成・運用時の対策	64

6.6.2	アプリケーション・コンテンツ提供時の対策	65
第 7 部	情報システムのセキュリティ要件	66
7.1	情報システムのセキュリティ機能	66
7.1.1	主体認証機能	66
7.1.2	アクセス制御機能	66
7.1.3	権限の管理	67
7.1.4	ログの取得・管理	68
7.1.5	暗号・電子署名	68
7.1.6	監視機能	69
7.2	情報セキュリティの脅威への対策	71
7.2.1	ソフトウェアに関する脆弱性対策	71
7.2.2	不正プログラム対策	71
7.2.3	サービス不能攻撃対策	72
7.2.4	標的型攻撃対策	73
7.3	ゼロトラストアーキテクチャ	74
7.3.1	動的なアクセス制御の実装時の対策	74
7.3.2	動的なアクセス制御の運用時の対策	75
第 8 部	情報システムの利用	76
8.1	情報システムの利用	76
8.1.1	情報システムの利用	76
8.1.2	ソーシャルメディアによる情報発信	79
8.1.3	テレワーク	80

第1部 総則

1.1 本統一基準の目的・適用範囲

(1) 本統一基準の目的

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

本統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策であり、政府機関等のサイバーセキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定）に基づく機関等における統一的な枠組みの中で、統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的とする。

(2) 本統一基準の適用対象

(a) 本統一基準において適用対象とする者は、全ての職員等とする。

(b) 本統一基準において適用対象とする情報は、以下の情報とする。

(ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）

(イ) その他のシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）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、又は開発したシステムの設計又は運用管理に関する情報

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

(3) 本統一基準の改定

情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、情報技術の進歩に応じて、本統一基準を定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。本統一基準の原案は、内閣官房内閣サイバーセキュリティセンターが策定し、サイバーセキュリティ対策推進会議（平成 27 年 2 月 10 日サイバーセキュリティ戦略本部長決定）を経てサイバーセキュリティ戦略本部において決定する。

なお、内閣官房内閣サイバーセキュリティセンターは、新たな脅威の発生や機関等における運用の状況を定期的に点検した結果を踏まえ、次の点に留意の上、原案の策定を行う。

- (a) 統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策を包含するものとし、責任体制、実施体制及び対策内容について、機関等が準拠できるよう、実状を踏まえるとともに、国際的な基準等との整合性に配慮の上、策定する。

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、本統一基準のほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本統一基準では、あえて関連法令等の遵守について明記していない。また、情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。

(5) 機関等の対策基準

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

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

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

1.2 情報の格付の区分・取扱制限

(1) 情報の格付の区分

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

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

機密性についての格付の定義

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

	<p>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</p> <p>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</p>
--	---

なお、機密性2情報及び機密性3情報を「要機密情報」という。

完全性についての格付の定義

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

なお、完全性2情報を「要保全情報」という。

可用性についての格付の定義

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

なお、可用性2情報を「要安定情報」という。

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

(2) 情報の取扱制限

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

職員等は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。機関等は、取り扱う情報につ

いて、機密性、完全性及び可用性の3つの観点から、取扱制限に関する基本的な定義を定める必要がある。

1.3 用語定義

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

【あ】

- 「アプリケーション・コンテンツ」とは、機関等が開発し提供する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。
- 「運用規程」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運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。

【か】

- 「機関等」とは、国の行政機関、独立行政法人及び指定法人をいう。
- 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。
- 「機関等内通信回線」とは、一つの機関等又は政府共通利用型システム管理機関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で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。
- 「業務委託」とは、機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において機関等の情報を取り扱わせる場合に限る。
- 「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二百十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。
- 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。

- 「クラウドサービス管理者」とは、クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う機関等の職員等をいう。
- 「クラウドサービス提供者」とは、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。
- 「クラウドサービス利用者」とは、クラウドサービスを利用する機関等の職員等又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。

【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（政府共通利用型システムが提供するものを含む。）をいう。また、物理的なハードウェアを有するサーバ装置を「物理的なサーバ装置」という。
- 「^{サイマット}CYMAT」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。
- 「^{シーサート}CSIRT」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。
- 「^{ジーソック}GSOC」とは、24 時間 365 日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、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。Government Security Operation Coordination Team（政府機関情報セキュリティ横断監視・即応調整チーム）の略。なお、GSOC には、政府機関を対象とした「第一 GSOC」と独立行政法人及び指定法人を対象とした「第二 GSOC」がある。
- 「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や手続をいう。
- 「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。
- 「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や政府共通利用型システムを含む。）をいう。

- 「情報セキュリティインシデント」とは、JIS Q 27000:2019 における情報セキュリティインシデントをいう。
- 「情報セキュリティ関係規程」とは、対策基準、運用規程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。
- 「職員等」とは、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の管理対象である情報及び情報システムを取り扱う者をいう。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。
- 「政府共通利用型システム」とは、他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム及び他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムをいう。なお、政府共通利用型システムを構築・運用する機関等を「政府共通利用型システム管理機関」といい、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する機関等及び政府共通利用型システムが提供する機器等を利用する機関等を「政府共通利用型システム利用機関」という。
- 「政府ドメイン名」とは、.go.jp で終わるドメイン名のことをいう。日本国の政府機関、独立行政法人、特殊法人（特殊会社を除く。）が登録（取得）することができる。

【た】

- 「対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
- 「対策推進計画」とは、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。
- 「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、特に断りが無い限り、機関等が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）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。さらに、物理的なハードウェアを有する端末を「物理的な端末」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。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。
- 「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、通信回線に接続する機能を備え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】

- 「本部監査」とは、サイバーセキュリティ基本法第 26 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をいう。

【ま】

- 「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。

【や】

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

第2部 情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1 組織・体制の整備

目的・趣旨

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

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

遵守事項

- (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置
 - (a) 機関等は、機関等における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者1人を置くこと。
 - (b) 機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者1人を必要に応じて置くこと。
- (2) 情報セキュリティ委員会の設置
 - (a) 最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。
- (3) 情報セキュリティ監査責任者の設置
 - (a) 最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者1人を置くこと。
- (4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置
 - (a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者1人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する者として、統括情報セキュリティ責任者1人を選任すること。

- (b) 情報セキュリティ責任者は、遵守事項 3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者 1 人を置くこと。
 - (c) 情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する課室情報セキュリティ責任者 1 人を置くこと。
 - (d) 情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任すること。
- (5) 最高情報セキュリティアドバイザーの設置
- (a) 最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。
- (6) 情報セキュリティ対策推進体制の整備
- (a) 最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制を整備し、その役割を規定すること。
 - (b) 最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。
- (7) 情報セキュリティインシデントに備えた体制の整備
- (a) 最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化すること。
 - (b) 最高情報セキュリティ責任者は、職員等のうちから CSIRT に属する職員等として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、機関等における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めること。
 - (c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。
 - (d) 最高情報セキュリティ責任者は、CYMAT に属する職員を指名すること。(国の行政機関に限る。)
- (8) 兼務を禁止する役割
- (a) 職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。
 - (ア) 承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う許可権限者
 - (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、自らが許可権限者であるときその他許可権限者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、当該許可権限者の上司又は適切な者に承認等を申請し、承認等を得ること。

2.1.2 資産管理

目的・趣旨

機関等において情報セキュリティ対策を検討する際に、自組織の資産の状況を把握することが重要である。資産の把握が不十分な状況では、把握できていない資産が存在することによる対策の漏れや、網羅的な対策がなされず情報システムに脅威が存在し続ける可能性がある。さらに、情報セキュリティインシデントが発生した際、資産が正しく管理されていないと情報セキュリティインシデントに対応するための情報収集に時間を要するなど、情報セキュリティインシデントへの対処が遅れる等の可能性がある。

このため機関等においては、自組織の資産の全容を把握するために必要な事項を整理し、職員等が資産を把握しやすいように、資産台帳として情報システム台帳を整備しておく必要がある。

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。

2.1.3 情報セキュリティ関係規程の整備

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。

また、対策基準に定められた対策を実施するためには具体的な運用規程や実施手順を定める必要があるが、それらが整備されていない、又は内容に漏れがあると、対策が適切に実施されないおそれがあることから、その場合には、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運用規程等の整備を指示し、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) リスク評価の実施

- (a) 最高情報セキュリティ責任者は、機関等の目的等を踏まえ、自己点検の結果、情報セキュリティ監査の結果、本部監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価すること。

(2) 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、これと同等以上の情報セキュリティ対策が可能となるように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、保有する情報システムに関するリスク評価の結果及び対策基準や対策推進計画の見直し結果を踏まえた上で定めること。

(3) 運用規程及び実施手順の策定

- (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運用規程（本統一基準で最高情報セキュリティ責任者が整備すべきとされている場合を除く。）及び実施手順（本統一基準で整備すべき者を別に定める場合を除く。）を整備し、運用規程及び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運用規程を整備すること。

(4) 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、対策推進計画を定めること。

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に定める具体的な運用規程及び実施手順を適切に運用する必要がある。

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

(2) 違反への対処

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

2.2.2 例外措置

目的・趣旨

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

遵守事項

(1) 例外措置手続の整備

- (a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査し、許可する者（以下本款において「許可権限者」という。）及び審査手続を定めること。
- (b) 統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

(2) 例外措置の運用

- (a) 職員等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。ただし、業務の遂行に緊急を要し、当該規定の趣旨を十分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。
- (b) 許可権限者は、職員等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。
- (c) 許可権限者は、例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者に報告すること。
- (d) 統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告すること。

2.2.3 教育

目的・趣旨

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

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

遵守事項

(1) 教育体制の整備・教育実施計画の策定

- (a) 統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。
- (b) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すこと。

(2) 教育の実施

- (a) 課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を適切に受講させること。
- (b) 職員等は、教育実施計画に従って、適切な時期に教育を受講すること。
- (c) 課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講させること。また、国の行政機関における課室情報セキュリティ責任者は、CYMAT に属する職員にも教育を適切に受講させること。
- (d) 課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告すること。
- (e) 統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

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

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

- (a) 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機関等関係者への報告手順を整備し、報告が必要な具体例を含め、職員等に周知すること。
- (b) 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の機関等外との情報共有を含む対処手順を整備すること。
- (c) 統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。
- (d) 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。
- (e) 統括情報セキュリティ責任者は、情報セキュリティインシデントについて機関等外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機関等外の者に明示すること。
- (f) 統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認すること。

(2) 情報セキュリティインシデントへの対処

- (a) 職員等は、情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口へ報告し、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。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システムセキュリティ責任者へ確認を指示すること。
- (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) 政府共通利用型システム利用機関の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政府共通利用型システムに関するものである場合には、当該政府共通利用型システムの情報セキュリティ対策に係る運用管理規程に従い、適切に対処すること。
- (g) 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、警察への通報・連絡等を行うこと。
- (h) CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、対処全般に関する指示、勧告又は助言を行うこと。
- (i) CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。
- (j) CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。

(3) 情報セキュリティインシデントに係る情報共有

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

一攻撃事態等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁）」に基づく報告連絡を行うこと。

(c) 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。

(d) 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告を行うこと。

(4) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告すること。

(b) 最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

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

2.3 点検

2.3.1 情報セキュリティ対策の自己点検

目的・趣旨

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

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

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

遵守事項

- (1) 自己点検計画の策定・手順の準備
 - (a) 統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定すること。
 - (b) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等ごとの自己点検票及び自己点検の実施手順を整備すること。
 - (c) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。
- (2) 自己点検の実施
 - (a) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示すること。
 - (b) 職員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。
- (3) 自己点検結果の評価・改善
 - (a) 情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を統括情報セキュリティ責任者に報告すること。
 - (b) 統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を最高情報セキュリティ責任者に報告すること。
 - (c) 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受けること。

2.3.2 情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。機関等において実施する情報セキュリティ監査は、業務や情報システムへの理解度が高く、効率的に監査の深掘りができ、組織の情報セキュリティ対策の改善に係る PDCA サイクルを円滑に機能させるためにも重要である。

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

遵守事項

(1) 監査実施計画の策定

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

(2) 監査の実施

- (a) 情報セキュリティ監査責任者は、監査実施計画に基づき、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。

(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。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示すること。
- (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。また、措置が完了していない改善計画は、定期的に進捗状況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。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

目的・趣旨

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

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

遵守事項

(1) 情報セキュリティ対策の見直し

- (a) 最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、対策基準や対策推進計画の必要な見直しを行うこと。

(2) 情報セキュリティ関係規程等の見直し

- (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、情報セキュリティ監査、本部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、情報セキュリティ監査、本部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運用規程及び実施手順を見直し、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。
- (c) 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、情報セキュリティ監査、本部監査等の結果等を踏まえて機関等内で横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、機関等内の職制及び職務に応じた措置の実施又は指示し、措置の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。

(3) 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自己点検、情報セキュリティ監査、本部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。

2.5 独立行政法人及び指定法人

2.5.1 独立行政法人及び指定法人に係る情報セキュリティ対策

目的・趣旨

独立行政法人や指定法人においても、国の行政機関の重要な情報に相当する情報が取り扱われている場合があるため、国の行政機関と同様に情報セキュリティ対策が適切に講じられる必要がある。そのためには、当該法人を所管する国の行政機関との連携による情報セキュリティマネジメントが適切に機能することが重要である。

遵守事項

- (1) 独立行政法人及び指定法人を所管する国の行政機関における体制の整備
 - (a) 独立行政法人及び指定法人を所管する国の行政機関に置かれる最高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の情報セキュリティ対策が適切に推進されるために必要な機関内の体制の整備を指示すること。
- (2) 独立行政法人及び指定法人における情報セキュリティ対策
 - (a) 独立行政法人及び指定法人の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適切に推進するため、所管省庁と密接な連携を要する事項や専門的知見を要する事項について、当該法人を所管する国の行政機関へ助言を求めること。

第3部 情報の取扱い

3.1 情報の取扱い

3.1.1 情報の取扱い

目的・趣旨

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

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

遵守事項

(1) 情報の取扱いに係る規定の整備

- (a) 統括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。
 - (ア) 情報の格付及び取扱制限についての定義
 - (イ) 情報の格付及び取扱制限の明示等についての手続
 - (ウ) 情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報の目的外での利用等の禁止

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

(3) 情報の格付及び取扱制限の決定・明示等

- (a) 職員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。
- (b) 職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

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

(4) 情報の利用・保存

- (a) 職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。
- (b) 職員等は、機密性 3 情報について要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ること。
- (c) 職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。
- (d) 職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、機密性 3 情報を機器等に保存する際、以下の措置を講ずること。ただし、独立行政法人及び指定法人において、機密性 3 情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。
 - (ア) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。
 - (イ) 当該情報に対し、暗号化による保護を行うこと。
 - (ウ) 当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。
- (e) 職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

(5) 情報の提供・公表

- (a) 職員等は、情報を公表する場合には、当該情報が機密性 1 情報に格付されるものであることを確認すること。
- (b) 職員等は、閲覧制限の範囲外の者に情報を提供する必要がある場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。
- (c) 独立行政法人及び指定法人における職員等は、機密性 3 情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。
- (d) 職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

(6) 情報の運搬・送信

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

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

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

(7) 情報の消去

- (a) 職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。
- (b) 職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。
- (c) 職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

(8) 情報のバックアップ

- (a) 職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。
- (b) 職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。
- (c) 職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

目的・趣旨

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

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることによって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、以下の観点を含み対策の基準を運用規程として定めること。
 - (ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。
 - (イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。
- (2) 区域ごとの対策の決定
 - (a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。
 - (b) 区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。
- (3) 要管理対策区域における対策の実施
 - (a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。職員等が実施すべき対策については、職員等が認識できる措置を講ずること。
 - (b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。
 - (c) 職員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、職員等が機関等外の者を立ち入らせる際には、当該機関等外の者にも当該区域で定められた対策に従って利用させること。

第4部 外部委託

4.1 業務委託

4.1.1 業務委託

目的・趣旨

機関等外の者に、調査・研究等の業務を委託、あるいは情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、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、委託先に提供する要保護情報等を適切に保護するための情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

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

なお、委託業務でクラウドサービスを利用する場合は、委託先においてもクラウドサービス特有のリスクがあることから、4.2「クラウドサービス」で規定する内容についても取り扱う情報の格付、委託する業務や利用するクラウドサービスの特性等に応じて委託先への要求事項に含める必要がある。また、情報システムに関する業務を委託する際は、情報システムに関する別のリスクがあることから、4.1.2「情報システムに関する業務委託」に規定する内容についても実施する必要がある。さらに、機器等を調達する場合には、調達する機器等におけるサプライチェーン上のリスクがあることから、4.3「機器等の調達」で規定する内容についても実施する必要がある。

<業務委託の例>

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

遵守事項

(1) 業務委託に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備すること。

(ア) 委託先への提供を認める情報及び委託する業務の範囲を判断する基準(以下

本款において「委託判断基準」という。)

(イ) 委託先の選定基準

(2) 業務委託実施前の対策

(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、業務委託の実施までに、以下を全て含む事項を実施すること。

(ア) 委託する業務内容の特定

(イ) 委託先の選定条件を含む仕様の策定

(ウ) 仕様に基づく委託先の選定

(エ) 契約の締結

(オ) 委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求めること。

(ア) 仕様に準拠した提案

(イ) 契約の締結

(ウ) 委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

(3) 業務委託実施期間中の対策

(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、業務委託の実施期間において以下を全て含む対策を実施すること。

(ア) 委託判断基準に従った要保護情報の提供

(イ) 契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認

(ウ) 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における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求めること。

(ア) 情報の適正な取扱いのための情報セキュリティ対策

(イ) 契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告

(ウ) 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又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 業務委託終了時の対策

(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、業務委託

の終了に際して以下を全て含む対策を実施すること。

- (ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
 - (イ) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
- (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、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求めること。
- (ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
 - (イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

4.1.2 情報システムに関する業務委託

目的・趣旨

機関等外の者に、情報システムやアプリケーションプログラムの開発・運用・保守等の情報システムに関する業務を委託する際は、4.1.1「業務委託」で規定する内容に加え、委託先によって情報システムに機関等の意図せざる変更が加えられないための対策や、情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策等の情報システムに関する業務委託に特有の対策を講ずる必要があるこれらについても、委託先への要求事項として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。

＜情報システムに関する業務委託の例＞

- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- 機関等内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務の委託（ホスティング型プライベートクラウド）

遵守事項

- (1) 情報システムに関する業務委託における共通的対策
 - (a) 情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに機関等の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。
- (2) 情報システムの構築を業務委託する場合の対策
 - (a) 情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求めること。
 - (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

(3) 情報システムの運用・保守を業務委託する場合の対策

- (a) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求めること。
- (b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めること。

(4) 機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

- (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、機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加えること。
- (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定すること。
- (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。
- (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業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行うこと。
- (e) 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定すること。
- (f) 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名すること。

4.2 クラウドサービス

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

目的・趣旨

機関等が委託先に取扱いを委ねる情報は、当該委託先によって適正に取り扱われなければならないが、クラウドサービスにおけるセキュリティ対策の詳細を直接確認することは一般に容易ではない。このため機関等がクラウドサービスを利用して要機密情報を取り扱う場合は、クラウドサービスの特性を理解し、機関等によるクラウドサービス提供者へのガバナンスの有効性や、利用の際のセキュリティ確保のために必要な事項を十分に考慮し、機関等とクラウドサービス提供者の役割や責任分担を明確にした上で、クラウドサービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

＜クラウドサービスの例＞

- 仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
- データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
- Web会議サービス
- ソーシャルメディア
- 検索サービス、翻訳サービス、地図サービス

なお、民間事業者等が不特定多数の利用者に対して提供する、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできないため、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の規定を遵守する必要がある。

遵守事項

(1) クラウドサービスの選定に係る運用規程の整備

- (a) 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程を整備すること。
 - (ア) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 4.2 節において「クラウドサービス利用判断基準」という。）
 - (イ) クラウドサービスの選定基準
 - (ウ) クラウドサービスの利用申請の許可権限者と利用手続
 - (エ) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(2) クラウドサービスの選定

- (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討すること。

- (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めること。

- (ア) クラウドサービスに求める情報セキュリティ対策

- (イ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

- (ウ) クラウドサービスに求めるサービスレベル

- (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、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則として ISMAP 等クラウドサービスリストからクラウドサービスを選定すること。

(3) クラウドサービスの利用に係る調達

- (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、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

- (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得ること。また、調達仕様の内容は、契約に含めること。

(4) クラウドサービスの利用承認

- (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行うこと。

- (b) 利用申請の許可権限者は、前項におけるクラウドサービスの利用申請を審査し、利用の可否を決定すること。

- (c) 利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名すること。

4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）

目的・趣旨

クラウドサービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後のクラウドサービスを利用した情報システムの導入・構築、運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。

クラウドサービスのサービス内容は非常に早いサイクルで変化しており、新たに追加される機能を活用することで業務の効率化や情報セキュリティの向上を図ることができる。一方で、構築時には想定していなかった脅威や脆弱性が発生する可能性もある。したがって、クラウドサービスの利用においては、情報セキュリティ対策の定期的な確認による見直し

をすることで、セキュリティ要件の追加及び修正を漏れなく実施することが求められる。さらに、クラウドサービスへのアクセス権限については、機関等の業務やクラウドサービスの利用環境等の変化に応じて、定期的な確認による見直しをすることが重要である。

なお、本款ではクラウドサービスを利用する場合のライフサイクルの各段階において、特に必要となる情報セキュリティ対策を示しており、情報システム全体のライフサイクルの各段階で必要な情報セキュリティ対策については、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」で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) クラウドサービスの利用に係る運用規程の整備

- (a) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備すること。
- (b) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備すること。
- (c) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備すること。
 - (ア) クラウドサービスの利用終了時における対策
 - (イ) クラウドサービスで取り扱った情報の廃棄
 - (ウ) クラウドサービスの利用のために作成したアカウントの廃棄

(2) クラウドサービスの利用に係るセキュリティ要件の策定

- (a) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認すること。
- (b) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定すること。

(3) クラウドサービスを利用した情報システムの導入・構築時の対策

- (a) クラウドサービス管理者は、(1)(a)で定めた運用規程を踏まえて、(2)(b)において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずること。また、導入・構築時に実施状況を確認・記録すること。
- (b) クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載すること。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告すること。

- (c) クラウドサービス管理者は、クラウドサービス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、クラウドサービスの運用開始前までに以下の全ての実施手順を整備すること。
 - (ア) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
 - (イ) クラウドサービスを利用した情報システムの運用・監視中における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
 - (ウ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順
- (4) クラウドサービスを利用した情報システムの運用・保守時の対策
 - (a) クラウドサービス管理者は、(1)(b)で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録すること。
 - (b) クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告すること。
 - (c) クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。
- (5) クラウドサービスを利用した情報システムの更改・廃棄時の対策
 - (a) クラウドサービス管理者は、(1)(c)で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずること。また、クラウドサービスの利用終了時に実施状況を確認・記録すること。

4.2.3 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

目的・趣旨

要機密情報を取り扱わない場合であって、クラウドサービス提供者における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を機関等から送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、要機密情報を取り扱う場合と同等のセキュリティ対策を求めることはクラウドサービスの利用推進を妨げるものであるため、要機密情報を取り扱わない前提でクラウドサービスを利用する場合は、本款で定めた遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

- (1) 要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備

- (a) 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱わない場合）の利用に関する運用規程を整備すること。
 - (ア) クラウドサービスを利用可能な業務の範囲
 - (イ) クラウドサービスの利用申請の許可権限者と利用手続
 - (ウ) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理
 - (エ) クラウドサービスの利用の運用規程
- (2) 要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施
 - (a) 職員等は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、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利用申請の許可権限者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請すること。
 - (b) 利用申請の許可権限者は、職員等による利用するクラウドサービスの定型約款、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の確認結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定すること。
 - (c) 利用申請の許可権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録すること。
 - (d) クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずること。

4.3 機器等の調達

4.3.1 機器等の調達

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。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

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運用規程の整備

- (a) 統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備すること。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。

第5部 情報システムのライフサイクル

5.1 情報システムの分類

5.1.1 情報システムの分類基準等の整備

目的・趣旨

機関等が所管する情報システムが多様化するなか、自組織で所管する情報システムの情報セキュリティインシデントの発生リスクを低減させるためには、多様な情報セキュリティ対策からその情報システムに求められる対策を過不足無く適切に選択する必要がある。

そのためには、情報セキュリティを取り巻く様々な脅威動向や情報システムにインシデントが発生した際の業務影響度、社会的影響、取り扱う情報、機関等の組織特性等を踏まえて、高度な情報セキュリティ対策が求められる情報システムを判別するための分類基準を定め、分類基準に応じた情報セキュリティ対策を規定することで、自組織が所管する情報システムの分類に応じた適切な対策が講じられるようにすることが重要である。

遵守事項

- (1) 情報システムにおける分類のための運用規程の整備
 - (a) 統括情報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インシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である情報システムの分類基準を運用規程として整備すること。
- (2) 情報システムの分類基準に基づいた情報セキュリティ対策に係る運用規程の整備
 - (a) 統括情報セキュリティ責任者は、情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を運用規程として整備すること。
- (3) 情報システムの分類基準に基づいた分類の実施
 - (a) 統括情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ、実施した結果を報告させること。情報システムセキュリティ責任者から報告を受けた情報システムの分類結果については、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行うこと。
- (4) 情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用規程の見直し
 - (a) 統括情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた情

報セキュリティ対策の具体的な対策事項の運用規程について定期的な確認による見直しをすること。

- (b) 統括情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認すること。

5.2 情報システムのライフサイクルの各段階における対策

5.2.1 情報システムの企画・要件定義

目的・趣旨

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

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

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

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

また、情報システムの構築、運用・保守を業務委託する場合については 4.1「業務委託」、クラウドサービスを利用して情報システムを構築する場合は 4.2「クラウドサービス」、情報システムで利用する機器等を調達する場合は 4.3「機器等の調達」、政府共通利用型システムを利用して情報システムを構築する場合は 5.4「政府共通利用型システム」を参照すること。

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) 最高情報セキュリティ責任者は、前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（デジタル統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。

(2) 情報システムの分類基準に基づいた分類の実施

- (a) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告すること。

(3) 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を勘案し情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、以下の全て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及び不正プログラムについての対策要件
 - (エ) 情報システムの可用性に関する対策要件
 - (オ) 情報システムのネットワーク構成に関する要件
- (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、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要求する情報システムについては、情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等へ助言を求め、業務の特性や情報システムの特性を踏まえて、上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いかを確認すること。

5.2.2 情報システムの調達・構築

目的・趣旨

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

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

なお、情報システムの構築を委託する場合は 4.1「業務委託」、クラウドサービスを利用して構築する場合は 4.2「クラウドサービス」、情報システムで使用する機器等を調達する場合は 4.3「機器等の調達」を参照し遵守する必要がある。

遵守事項

(1) 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。
- (c) 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、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。
- (d) 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、以下を全て含む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
- (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、以下を全て含む実施手順を整備すること。
 - (ア) 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
 - (イ) 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
 - (ウ) 情報システムが停止した際の復旧手順

(2) 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、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。
- (b) 情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。

5.2.3 情報システムの運用・保守

目的・趣旨

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

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するた

めに、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、対策基準に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。なお、情報システムの運用・保守を業務委託する場合は、4.1「業務委託」を参照のこと。

さらに、クラウドサービスを利用して構築された情報システムの運用・保守をする場合は、4.2「クラウドサービス」、政府共通利用型システムを利用して構築された情報システムを運用・保守する場合は、5.4「政府共通利用型システム」を参照すること。

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監視を含む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、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し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。
- (c) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システム台帳及び関連文書の内容に変更が生じた場合、情報システム台帳及び関連文書を更新又は修正すること。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告すること。
- (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。
- (e) 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、危機的事象発生時に適切な対処が行えるよう運用をすること。

5.2.4 情報システムの更改・廃棄

目的・趣旨

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

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

(1) 情報システムの更改・廃棄時の対策

- (a) 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、

当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下を全て含む措置を適切に講ずること。

- (ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策
- (イ) 情報システム廃棄時の不要な情報の抹消

5.2.5 情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策の定期的な確認による見直しや、外部環境の急激な変化等が発生した場合の適時確認を行うことによる見直しが必要となる。また、運用時における定期的な情報セキュリティ対策の確認による見直しの他、対策推進計画に基づく情報セキュリティ対策の見直しや自己点検・監査、本部監査等の結果等を踏まえた機関等内で横断的に改善が必要となる情報セキュリティ対策についての見直しも併せて実施する必要がある。

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、対策推進計画に基づき情報システムの情報セキュリティ対策を適切に見直すこと。
 - (b) 情報システムセキュリティ責任者は、機関等内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直すこと。また、措置の結果については、統括情報セキュリティ責任者へ報告すること。

5.3 情報システムの運用継続計画

5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、地震、火災、感染症、情報セキュリティインシデント等の危機的事象発生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。

危機的事象発生時に情報システムの運用を継続させるためには、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を検討し、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場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討すること。
- (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に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であることを定期的に確認すること。
- (c) 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に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直すこと。

5.4 政府共通利用型システム

5.4.1 政府共通利用型システム管理機関における対策

目的・趣旨

政府共通利用型システムは、政府共通利用型システムの管理機関と利用機関が連携して運用するものであることから、機関等の間で情報セキュリティ対策の漏れが生じないようにその防止を図る必要がある。また、政府共通利用型システムを利用する一部の情報システムで情報セキュリティインシデントが生じた場合に同システムを利用する他の情報システムにも影響が及ぶ可能性等も踏まえ、政府共通利用型システムの管理機関は、政府共通利用型システム全体としての情報セキュリティマネジメントを適切に実行し、情報セキュリティ水準を適切に確保する必要がある。

このため、両機関の責任と役割分担を明確化し、情報セキュリティインシデントを認知時にこれに係る対処を連携して迅速・確実に実施できる体制にする必要がある。

遵守事項

- (1) 情報セキュリティ対策に関する運用管理規程の整備
 - (a) 情報システムセキュリティ責任者は、政府共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用管理規程を整備し、政府共通利用型システム利用機関と十分な合意形成を行うこと。
 - (ア) 政府共通利用型システム管理機関と政府共通利用型システム利用機関との間の責任分界
 - (イ) 平常時及び非常時の協力・連携体制
 - (ウ) 非常時の具体的対応策
- (2) 情報システム台帳及び情報システム関連文書の整備
 - (a) 政府共通利用型システム管理機関の統括情報セキュリティ責任者は、遵守事項 2.1.2(1)(a)で整備する政府共通利用型システムに関する情報システム台帳について、政府共通利用型システム利用機関に関係するセキュリティ要件に係る事項を含めて整備すること。
 - (b) 政府共通利用型システム管理機関の情報システムセキュリティ責任者は、遵守事項 5.2.2(1)(d)で整備する政府共通利用型システムに関する情報システム関連文書について、政府共通利用型システム利用機関に関係する情報を含めて整備すること。

5.4.2 政府共通利用型システム利用機関における対策

目的・趣旨

政府共通利用型システム利用機関は、政府共通利用型システム管理機関が定める運用管理規程に基づき必要な体制を確保すると共に、責任と役割分担を踏まえ、適切に利用する必

要がある。また、情報セキュリティインシデントを認知した際の対処においては両機関の協力が必要となることから、管理機関が定める運用管理規程に基づき情報セキュリティインシデントを認知した際の両機関の責任と役割分担を明確にしておき、対処に必要な情報は両機関で共有されている状態にしておくことが重要である。

遵守事項

- (1) 政府共通利用型システム利用機関における体制の整備
 - (a) 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程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。
 - (b) 統括情報セキュリティ責任者は、政府共通利用型システムが提供する機器等の提供を受けこれを自機関等の職員等が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに政府共通利用型システム利用管理者を指名すること。
 - (c) 政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程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。
- (2) 政府共通利用型システム利用機関における情報セキュリティ対策
 - (a) 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システム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、適切にセキュリティ要件を策定し、運用すること。
 - (b) 情報システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。
- (3) 政府共通利用型システム利用機関における機器等の管理
 - (a) 政府共通利用型システム利用管理者は、政府共通利用型システムが提供する機器等の提供を受けてこれを自機関等の職員等が利用する場合は、当該政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程及び実施手順を整備すること。
 - (b) 政府共通利用型システム利用管理者は、提供を受けた政府共通利用型システムの機器等を把握するために必要な文書を整備すること。
 - (c) 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、政府共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知すること。

- (d) 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。

第6部 情報システムの構成要素

6.1 端末

6.1.1 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に注意する必要がある。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。これらのリスクを考慮し職員等が利用する端末については適切なセキュリティ対策を講ずるとともに、利用を認めるソフトウェアや接続を認める機器等を定めておくことが重要である。また、物理的な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。

なお、本款の遵守事項のほか、7.1「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、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、6.4.4「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物理的な端末について、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を定め、それ以外のソフトウェアは利用させないこと。
- (c) 情報システムセキュリティ責任者は、端末に接続を認める機器等を定め、接続を認めた機器等以外は接続させないこと。
- (d) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した内容に従い、端末に対して適切なセキュリティ対策を実施すること。
- (e) 情報システムセキュリティ責任者は、端末において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対策を実施すること。

(2) 端末の運用時の対策

- (a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。
- (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

合には、改善を図ること。

(3) 端末の運用終了時の対策

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

6.1.2 要管理対策区域外での端末利用時の対策

目的・趣旨

テレワークの実施等により、職員等が機関等外で業務を行うことが増え、機関等が支給する物理的な端末を利用して要管理対策区域外で業務を行う場合は、盗み見や盗難・紛失などのリスクが増える。そのようなリスクに対抗するため、要管理対策区域外で機関等が支給する物理的な端末を使用する場合は、利用手順や利用の許可手続等を定め、職員等に守らせる必要がある。また、端末においても盗難、紛失、不正プログラムの感染等による情報窃取を防止するため技術的な措置を講ずる必要がある。

さらに、職員等が機関等外通信回線を用いて情報システムにリモートアクセスをする場合は、リモートアクセス特有の攻撃等に対抗するためのセキュリティ対策を実施する必要がある。リモートアクセスについては、遵守事項 8.1.3(2)を参照のこと。

なお、機関等外通信回線を用いて情報システムにリモートアクセス環境を構築する場合は、情報システムへのアクセスについて初回のアクセス要求時のみ制御を行うのではなく、アクセスの都度信用できるアクセスであるかを検証し、信用できない場合には追加の措置を講ずるなど、アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御を実施することも有効である。動的なアクセス制御については、7.3「ゼロトラストアーキテクチャ」を参照のこと。

遵守事項

- (1) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用規程の整備
- (a) 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。
- (b) 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する運用規程を整備すること。
- (c) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等が支給する物理的な端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経

由して情報システムが不正プログラムに感染するリスクを踏まえた技術的な措置に関する運用規程を定めること。

- (2) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策
 - (a) 情報システムセキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、当該端末について前条(b)の技術的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、要管理対策区域外において機関等外通信回線に接続した機関等が支給する物理的な端末を機関等内通信回線に接続させる際、当該端末について前条(c)の技術的な措置を講ずること。

6.1.3 機関等支給以外の端末の導入及び利用時の対策

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

また、機関等支給以外の端末については、端末の管理を端末の所有者が行うこととなり、機関等において管理ができないことへのリスクを勘案し、その利用の可否を判断する必要がある。利用を認めたとしても、利用の許可手続を定めるとともに、情報の取扱いについての規定や手順を整備し遵守させる必要がある。

遵守事項

- (1) 機関等支給以外の端末の利用可否の判断
 - (a) 最高情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。
- (2) 機関等支給以外の端末の利用に関する運用規程等の整備
 - (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実施手順として定めること。

- (b) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。
 - (c) 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、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を含めた安全管理措置に関する運用規程を整備すること。
 - (d) 統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した機関等支給以外の端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する運用規程及び許可手続に関する実施手順を定めること。
- (3) 機関等支給以外の端末の利用に関する責任者の策定
- (a) 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。
- (4) 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、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、(2)(b)で定める利用手順に従うこと。
 - (c) 端末管理責任者等は、要機密情報を取り扱う機関等支給以外の端末について、(2)(c)に定める安全管理措置を講じる又は職員等に講じさせること。
 - (d) 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。

6.2 サーバ装置

6.2.1 サーバ装置

目的・趣旨

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

なお、本款の遵守事項のほか、7.1「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・監視機能等の機能面での対策、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、7.2.3「サービス不能攻撃対策」、6.4.4「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。さらに、機関等外通信回線を経由してサーバ装置の保守作業を行う場合は、6.4.1「通信回線」のリモートメンテナンスについての対策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、それぞれ本節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物理的な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を定め、それ以外のソフトウェアは利用させないこと。
- (d) 情報システムセキュリティ責任者は、サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させないこと。
- (e) 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要件として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施すること。
- (f) 情報システムセキュリティ責任者は、サーバ装置において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対策を実施すること。

- (g) 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、適切な方法でサーバ装置のバックアップを取得すること。

(2) サーバ装置の運用時の対策

- (a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。
- (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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視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、要安定情報を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行えるよう運用をすること。

(3) サーバ装置の運用終了時の対策

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

6.2.2 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、6.2.1「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

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。

6.2.3 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ることで実施することが求められる。

なお、本款の遵守事項のほか、6.2.1「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。さらに、ウェブサーバにおけるウェブアプリケーションについては、6.6「アプリケーション・コンテンツ」を参照のこと。

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、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、ウェブサーバが備える機能のうち、必要な機能のみを利用すること。
- (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。
- (c) 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行う主体を限定すること。
- (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ずること。

6.2.4 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、6.2.1「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（SaaS 系のクラウドサービスを利用する場合を除く）。

遵守事項

(1) DNS の導入時の対策

- (a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。
- (b) 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。
- (c) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

(2) DNS の運用時の対策

- (a) 情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。
- (b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。
- (c) 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

6.2.5 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、7.1「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、6.4.4「IPv6 通信回線」、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」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。

6.3 複合機・特定用途機器

6.3.1 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。これらの特定用途機器がインターネットに接続する機能を備える、いわゆる IoT 機器となっている場合が多くある。例えばネットワークカメラシステムの構成要素である機器のうちインターネットに接続する機能を備えるカメラや、環境モニタリングシステムの構成要素である機器のうちインターネットに接続する機能を備えるセンサーが挙げられる。近年、IoT 機器の脆弱性をついた攻撃が数多く発生しており、IoT 機器が踏み台となって他の情報システムへの攻撃に利用されるなど、社会的問題となってきている。このため、これらの機器に対する情報セキュリティ対策が必要となる。

したがって、複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講ずることが重要である。

遵守事項

(1) 複合機

- (a) 情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。
- (b) 情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。
- (c) 情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

(2) IoT 機器を含む特定用途機器

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

6.4 通信回線

6.4.1 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、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。

(2) 機関等外通信回線の接続時の対策

- (a) 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。

- (b) 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及び機関等内通信回線内の不正な通信の有無を監視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、保守又は診断のために、機関等外通信回線から機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保すること。
- (d) 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。

(3) 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、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確認及び見直しを行うこと。
- (b) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをすること。
- (c) 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、機関等外通信回線から機関等内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認による見直しをすること。
- (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。

6.4.2 通信回線装置

目的・趣旨

インターネット等の外部ネットワークからアクセス可能な通信回線装置においては、ソフトウェアの脆弱性を悪用された不正アクセスの被害を受ける可能性がある。そのため、通信回線装置におけるソフトウェアの脆弱性対策は、迅速かつ適切に対処することが求められる。また、通信回線装置は端末やサーバ装置などの経路制御やアクセス制御に用いるため、情報システムの構築時からリスクを十分検討し、必要なセキュリティ対策を実施しておく必要がある。さらに運用時においても、脅威動向の変化等に応じた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、物理的な通信回線装置を設置する場合、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。

- (b) 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に関する事項を含む実施手順を定めること。
- (c) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。
- (d) 情報システムセキュリティ責任者は、通信回線装置において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対策を実施すること。

(2) 通信回線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、通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、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。
- (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。
- (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等を調査し、認識した脆弱性等について対策を講ずること。

(3) 通信回線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、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。

6.4.3 無線 LAN

目的・趣旨

無線 LAN は、有線の通信回線及び通信回線装置において想定される脅威に加え、電波を利用するために有線と比較して通信の傍受等が容易であることに起因する脅威への対策が必要である。

なお、本款の遵守事項の他、6.4.1「通信回線」及び6.4.2「通信回線装置」において定める導入時の対策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) 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。

6.4.4 IPv6 通信回線

目的・趣旨

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ている。IPv6 通信プロトコルでは、グローバル IP アドレスによるパケットの直接到達性などを考慮する必要がある、設定不備によっては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、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。このため、必要な対策を講じていく必要がある。

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、IPv6 通信による情報セキュリティ上の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。

(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。

6.5 ソフトウェア

6.5.1 情報システムの基盤を管理又は制御するソフトウェア

目的・趣旨

情報システムの基盤を管理又は制御するソフトウェアは、情報システムを制御する上でセキュリティ上の重要な機能を有している。そのようなソフトウェアは悪用や不正アクセスされた場合、被害が広範囲に及ぶ可能性がある。したがって、情報システムの基盤を管理又は制御するソフトウェアを利用する端末やサーバ装置、通信回線装置等及びソフトウェア自体において、必要なセキュリティ対策を実施する必要がある。

本款では、情報システムの基盤を管理又は制御するソフトウェアを利用する場合に求めるセキュリティ対策として、7.1「情報システムのセキュリティ機能」で求めている対策から特に必要と考えられるものを示しており、本款以外に7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理、7.1.4「ログの取得・管理」で定めるログの取得に係る遵守事項についても併せて遵守する必要があるが、情報システムの基盤を管理又は制御するソフトウェアの機能や仕様等を踏まえて、適切な対策を講ずることが重要となる。

また、当該ソフトウェアを利用する際の操作ミスや設定不備などを防ぐためには、当該ソフトウェアの利用者や管理者が利用するソフトウェアを利用するための手順を整備することも重要である。さらに、情報システムの基盤を管理又は制御するソフトウェアを悪用した攻撃を防ぐにはソフトウェアの脆弱性対策が特に重要となる。当該ソフトウェアに関する脆弱性に関する情報を製品ベンダや脆弱性情報提供サイト等からの通知を受け取るようにするとともに、公開された脆弱性についての影響度と緊急度に応じてセキュリティパッチ等を適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。脆弱性対策については、7.2.1「ソフトウェアに関する脆弱性対策」を参照し確実な対策を実施することが重要である。

遵守事項

(1) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

- (a) 情報システムセキュリティ責任者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護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、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備すること。
 - (ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順
 - (イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した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

(2) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

- (a) 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施すること。
 - (ア) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
 - (イ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

6.6 アプリケーション・コンテンツ

6.6.1 アプリケーション・コンテンツの作成・運用時の対策

目的・趣旨

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

また、アプリケーション・コンテンツの開発・提供を業務委託する場合については、4.1「業務委託」についても併せて遵守する必要がある。

遵守事項

- (1) アプリケーション・コンテンツの作成に係る運用規程の整備
 - (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運用規程を整備すること。
- (2) アプリケーション・コンテンツのセキュリティ要件の策定
 - (a) 情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについてのセキュリティ要件を定め、仕様に含めること。
 - (b) 職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に掲げる内容を調達仕様に含めること。
- (3) アプリケーション・コンテンツの開発時の対策
 - (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、セキュリティ要件として定めた仕様に加えて、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。
- (4) アプリケーション・コンテンツの運用時の対策
 - (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、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。
 - (b) 情報システムセキュリティ責任者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずること。
 - (c) 情報システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずること。

6.6.2 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。これらの国民等に提供するサービス（クラウドサービスを含む）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、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、政府ドメイン名を取得できない場合を除き政府ドメイン名を情報システムにおいて使用すること。
- (b) 職員等は、機関等外向けに提供するウェブサイト等の作成を業務委託する場合においては、機関等に適するドメイン名を使用するよう調達仕様に含めること。

(2) 不正なウェブサイトへの誘導防止

- (a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機関等のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

(3) アプリケーション・コンテンツの告知

- (a) 職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。
- (b) 職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

第7部 情報システムのセキュリティ要件

7.1 情報システムのセキュリティ機能

7.1.1 主体認証機能

目的・趣旨

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

また、機関等の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(1) 主体認証機能の導入

- (a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。
- (b) 情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。
- (c) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

(2) 識別コード及び主体認証情報の管理

- (a) 情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。
- (b) 情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。

7.1.2 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、情報システムの特長、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。

7.1.3 権限の管理

目的・趣旨

情報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。その際、アクセス権限は最小権限の付与とするため、全てにアクセスできないことを前提に、アクセスの必要がある主体に対してのみ権限を付与し、アクセスの必要のない主体に対しては権限を与えないことを原則とすることが重要である。また、情報に対して権限を付与する場合も同様に、知る必要のある主体に対してのみ権限を付与し、知る必要のない主体に対しては権限を与えないことを原則とすることが重要である。なお、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、主体認証情報のみならず特権アクセスが可能な情報等の漏えい、改ざん、さらには情報システムや情報を破壊することを目的とした不正プログラムによって業務継続への影響もあり得る。また、これらの不正アクセスや不正プログラム等を検知又は防止するための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必要最小限の範囲で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。
- (c) 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不要なアクセス権限

が付与されていないか定期的に確認すること。

7.1.4 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。

7.1.5 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及び鍵長に加え、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又は鍵長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、以下の全て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」に基づき、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及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。
- (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、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定めること。

(2) 暗号化・電子署名に係る管理

- (a) 情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の全て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又は鍵長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。

7.1.6 監視機能

目的・趣旨

情報システムにおける情報セキュリティインシデントや不正利用等の速やかな認知や、情報セキュリティ対策の実効性を確認するためには、適切に監視機能を実装し、運用することが重要である。また、監視機能の実装に当たっては、情報システムの特性や当該情報システムで取り扱う情報の格付等を踏まえて、監視対象や監視内容を定める必要がある。

遵守事項

(1) 監視機能の導入・運用

- (a) 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監視に係る運用管理機能要件を策定し、監視機能を実装すること。

- (b) 情報システムセキュリティ責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用すること。
- (c) 情報システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直すこと。

7.2 情報セキュリティの脅威への対策

7.2.1 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、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。

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多く見受けられる。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りますので、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及び適時に確認すること。
- (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。

7.2.2 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。
- (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。

7.2.3 サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、機関等の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている。

遵守事項

(1) サービス不能攻撃対策の実施

- (a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。
- (b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。
- (c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

7.2.4 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、組織の情報システム内に何らかの手法で不正侵入・潜入し、権限の奪取等を通じて侵入範囲を拡大、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こともあり、完全に検知及び防御することは困難との前提に立った対策が必要である。

標的型攻撃への対策としては、情報システム内部への侵入を低減する対策（入口対策）に加え、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（内部対策）、及び外部との不正通信を検知して対処する対策（出口対策）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。

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

遵守事項

(1) 標的型攻撃対策の実施

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

7.3 ゼロトラストアーキテクチャ

7.3.1 動的なアクセス制御の実装時の対策

目的・趣旨

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の機関等外通信回線と組織内ネットワークである機関等内通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な政府情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。

ゼロトラストアーキテクチャに基づく情報資産の保護策の1つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装する場合に特に必要な対策について記載する。

動的なアクセス制御の機能を実装する場合は、本款以外に 7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理に係る遵守事項についても併せて遵守する必要があるが、既存の情報システムの構成に動的なアクセス制御を実装する場合は、既存の情報システムの構成やアクセス制御に用いるソフトウェアなどを見直していくことが重要となる。

遵守事項

(1) 動的なアクセス制御における責任者の設置

- (a) 統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用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選任すること。

(2) 動的なアクセス制御の導入方針の検討

- (a) 情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。

(3) 動的なアクセス制御の実装時の対策

- (a) 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成すること。
- (b) 情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

7.3.2 動的なアクセス制御の運用時の対策

目的・趣旨

テレワークの拡大やクラウド・バイ・デフォルト原則によって、リソースの利用形態は日々変化していることを踏まえ、動的なアクセス制御の運用時には、実装時に検討した対策内容が正しく機能しているかどうか確認し、必要に応じてアクセス制御ポリシーを見直すことが重要である。また、動的なアクセス制御の前提となるリソースの信用情報を収集する中でリスクが検出された場合は、当該リスクを低減するための措置が必要となる。

本款では、機関等が動的なアクセス制御を運用する場合に特に必要な対策についてのみ規定するため、本款以外に 7.1.1「主体認証機能」で定める識別コード・主体認証情報の管理、7.1.2「アクセス制御機能」で定めるアクセス制御の適切な運用、7.1.3「権限の管理」で定める権限の管理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) 動的なアクセス制御の実装方針の見直し

- (a) 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しをすること。

(2) リソースの信用情報に基づく動的なアクセス制御の運用時の対策

- (a) 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を行うこと。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

目的・趣旨

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

このため、情報システムの利用に関する規定を整備し、職員等は規定に従って利用することが求められる。

なお、機関等が支給する端末（要管理対策区域外で使用する場合に限る）に係る規定の整備については遵守事項 6.1.2(1)、機関等支給以外の端末に係る規定の整備については遵守事項 6.1.3(2)をそれぞれ参照すること。

遵守事項

- (1) 情報システムの利用に係る規定の整備
 - (a) 統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する実施手順を整備すること。
 - (b) 統括情報セキュリティ責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順を定めること。
 - (c) 統括情報セキュリティ責任者は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めること。
- (2) 情報システム利用者の規定の遵守を支援するための対策
 - (a) 情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。
- (3) 情報システムの利用時の基本的対策
 - (a) 職員等は、業務の遂行以外の目的で情報システムを利用しないこと。
 - (b) 職員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機関等の情報システムを接続しないこと。
 - (c) 職員等は、機関等内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。
 - (d) 職員等は、業務の遂行において、利用が認められていないソフトウェアを利用しないこと。また、当該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。
- (h) 職員等は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しないこと。

(4) 端末（支給外端末を含む）の利用時の対策

- (a) 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り）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。
- (b) 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り） 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
- (c) 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、定められた措置を講ずること。

(5) 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バを利用すること。
- (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、政府ドメイン名を取得できない場合を除き、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。
- (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、以下の全て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

(6) 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。

(7) 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、鍵長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。

(8) 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。

(9) Web 会議サービスの利用時の対策

- (a) 職員等は、定められた利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。
- (b) 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

(10) クラウドサービスを利用した機関等外の者との情報の共有時の対策

- (a) 職員等は、機関等外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずること。
- (b) 職員等は、機関等外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除すること。

8.1.2 ソーシャルメディアによる情報発信

目的・趣旨

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

また、このようなソーシャルメディア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は、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスであることが考えられ、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことは困難であることが一般的である。このことから、ソーシャルメディアの利用は、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要がある場合に限るものとする。ソーシャルメディアを利用の際は 4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の対策を参照すること。

遵守事項

(1) ソーシャルメディア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を利用することを前提として、以下を全て含む情報セキュリティ対策に関する運用規程を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。
 - (ア) 機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。
 - (イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。
- (b) 職員等は、要安定情報の国民への提供にソーシャルメディアを用いる場合は、機関等の自己管理ウェブサイト当該情報を掲載して参照可能とすること。

8.1.3 テレワーク

目的・趣旨

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

本款では、テレワークの実施に特に必要な対策についてのみ規定しているため、本款以外に、3.1.1「情報の取扱い」、6.1.2「要管理対策区域外での端末利用時の対策」、6.1.3「機関等支給以外の端末の導入及び利用時の対策」、6.4.1「通信回線」、6.4.2「通信回線装置」、6.4.3「無線 LAN」、7.1.6「監視機能」及び 8.1.1「情報システムの利用」の各款を参照すること。

遵守事項

(1) 運用規程の整備

- (a) 統括情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策に係る運用規程を整備すること。なお、原則としてテレワークは機関等が支給する端末で行うよう定めること。

(2) 実施環境における対策

- (a) 情報システムセキュリティ責任者は、テレワークの実施により機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保すること。
- (b) 情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行うこと。
- (c) 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じること。
- (d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。

(3) 実施時における対策

- (a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等が確認すべき項目を定め、職員等に当該項目を確認させること。
- (b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。
- (c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。