

政府機関の情報セキュリティ対策のための
統一基準(2005年項目限定版)
解説資料

内閣官房情報セキュリティセンター

目次

第1部 総則	1
1.1.1 本統一基準の位置付け	1
(1) 政府機関の情報セキュリティ対策の強化における本統一基準の位置付け ..	1
(2) 本統一基準の改訂	1
(3) 法令等の遵守	1
1.1.2 本統一基準の使い方	2
(1) 本統一基準と省庁対策基準との関係	2
(2) 適用対象範囲	2
(3) 全体構成	2
(4) 対策項目の記載事項	3
(5) 対策レベルの設定	3
(6) 評価の方法	3
1.1.3 用語定義	4
第2部 組織と体制の構築	11
2.1 導入	11
2.1.1 組織・体制の確立	11
趣旨（必要性）	11
遵守事項	11
(1) 最高情報セキュリティ責任者の設置	11
(2) 情報セキュリティ委員会の設置	12
(3) 情報セキュリティ監査責任者の設置	12
(4) 情報セキュリティ責任者の設置	13
(5) 情報システムセキュリティ責任者の設置	14
(6) 情報システムセキュリティ管理者の設置	14
(7) 課室情報セキュリティ責任者の設置	14
2.1.2 役割の分離	15
趣旨（必要性）	15
遵守事項	15
(1) 兼務を禁止する役割の規定	15
2.1.3 違反と例外措置	16
趣旨（必要性）	16
遵守事項	16
(1) 違反への対応	16
(2) 例外措置	17
2.2 運用	20
2.2.1 情報セキュリティ対策の教育	20
趣旨（必要性）	20

遵守事項.....	20
(1) 行政事務従事者に対する情報セキュリティ対策教育の実施.....	20
(2) 行政事務従事者による情報セキュリティ対策教育の受講義務.....	21
2.2.2 事故及び障害の対応.....	22
趣旨（必要性）.....	22
遵守事項.....	22
(1) 障害等の発生に備えた事前準備.....	22
(2) 障害等の発生時における報告と応急措置.....	23
(3) 障害等の原因調査と再発防止策.....	24
2.3 評価.....	25
2.3.1 情報セキュリティ対策の自己点検.....	25
趣旨（必要性）.....	25
遵守事項.....	25
(1) 自己点検に関する年度計画の策定.....	25
(2) 自己点検の実施に関する準備.....	25
(3) 自己点検の実施.....	26
(4) 自己点検結果の評価.....	26
(5) 自己点検に基づく改善.....	26
2.3.2 情報セキュリティ対策の監査.....	27
趣旨（必要性）.....	27
遵守事項.....	27
(1) 監査計画の整備.....	27
(2) 情報セキュリティ監査の実施に関する指示.....	28
(3) 個別の監査業務における監査実施計画の立案.....	28
(4) 情報セキュリティ監査を実施する者の要件.....	29
(5) 情報セキュリティ監査の実施.....	29
(6) 情報セキュリティ監査結果に対する対応.....	30
2.4 見直し.....	32
2.4.1 情報セキュリティ対策の見直し.....	32
趣旨（必要性）.....	32
遵守事項.....	32
(1) セキュリティ対策の見直し.....	32
第3部 情報についての対策.....	33
3.1 情報の格付け.....	33
3.1.1 情報の格付け.....	33
趣旨（必要性）.....	33
遵守事項.....	33
(1) 情報の格付け.....	33
3.2 情報の取扱い.....	34
3.2.1 情報の作成と入手.....	34

趣旨（必要性）	34
遵守事項	34
(1) 業務以外の情報の作成又は入手の禁止	34
(2) 情報の作成又は入手時における格付けの決定と取扱制限の検討	34
(3) 格付けと取扱制限の明示	35
(4) 格付けと取扱制限の継承	35
(5) 格付けと取扱制限の変更	35
3.2.2 情報の利用	36
趣旨（必要性）	36
遵守事項	36
(1) 業務以外の利用の禁止	36
(2) 格付け及び取扱制限に従った情報の取扱い	37
(3) 要保護情報の取扱い	37
3.2.3 情報の保存	38
趣旨（必要性）	38
遵守事項	38
(1) 格付けに応じた情報の保存	38
(2) 情報の保存期間	40
3.2.4 情報の移送	40
趣旨（必要性）	40
遵守事項	40
(1) 情報の移送に関する許可及び届出	40
(2) 情報の送信と運搬の選択	41
(3) 移送手段の選択	41
(4) 書面に記載された情報の保護対策	41
(5) 電磁的記録媒体に記録された情報の保護対策	41
3.2.5 情報の提供	42
趣旨（必要性）	42
遵守事項	42
(1) 情報の公表	42
(2) 他者への情報の提供	43
3.2.6 情報の消去	43
趣旨（必要性）	43
遵守事項	44
(1) 電磁的記録の消去方法	44
(2) 書面の廃棄方法	45
第4部 情報セキュリティ要件の明確化に基づく対策	46
4.1 情報セキュリティについての機能	46
4.1.1 主体認証	46
趣旨（必要性）	46

用語解説.....	46
遵守事項.....	46
(1) 主体認証機能の導入.....	46
(2) 行政事務従事者における識別コードの管理.....	51
(3) 行政事務従事者における主体認証情報の管理.....	52
4.1.2 アクセス制御.....	54
趣旨（必要性）.....	54
用語解説.....	54
遵守事項.....	54
(1) アクセス制御機能の導入.....	54
(2) 行政事務従事者による適正なアクセス制御.....	55
4.1.3 権限管理.....	56
趣旨（必要性）.....	56
用語解説.....	56
遵守事項.....	56
(1) 権限管理機能の導入.....	56
(2) 識別コードと主体認証情報の付与管理.....	57
(3) 識別コードと主体認証情報における代替措置の適用.....	59
4.1.4 証跡管理.....	60
趣旨（必要性）.....	60
遵守事項.....	61
(1) 証跡管理機能の導入.....	61
(2) 行政事務従事者による証跡の取得と保存.....	63
(3) 取得した証跡の点検、分析及び報告.....	64
(4) 証跡管理に関する利用者への周知.....	64
4.1.6 暗号と電子署名（鍵管理を含む）.....	65
趣旨（必要性）.....	65
遵守事項.....	65
(1) 暗号化機能及び電子署名の付与機能の導入.....	65
(2) 暗号化及び電子署名の付与に係る管理.....	67
(3) 暗号化機能及び電子署名を付与する機能の利用.....	68
4.2 情報セキュリティについての脅威.....	70
4.2.1 セキュリティホール対策.....	70
趣旨（必要性）.....	70
遵守事項.....	70
(1) 情報システムの構築時.....	70
(2) 情報システムの運用時.....	71
4.2.2 不正プログラム対策.....	73
趣旨（必要性）.....	73
遵守事項.....	73

(1) 情報システムの構築時.....	73
(2) 情報システムの運用時.....	74
4.2.3 サービス不能攻撃対策.....	76
趣旨（必要性）.....	76
遵守事項.....	77
(1) 電子計算機、通信回線装置及び通信回線がインターネットからのアクセスを受ける情報システムの構築時.....	77
(2) 電子計算機及び通信回線がインターネットからのアクセスを受ける情報システムの運用時.....	78
第5部 情報システムについての対策.....	80
5.1 施設と環境.....	80
5.1.1 電子計算機及び通信回線装置を設置する安全区域.....	80
趣旨（必要性）.....	80
遵守事項.....	80
(1) 立入り及び退出の管理.....	80
(2) 訪問者及び受渡業者の管理.....	81
(3) 電子計算機及び通信回線装置のセキュリティ確保.....	83
(4) 安全区域内のセキュリティ管理.....	84
(5) 災害及び障害への対策.....	85
5.2 電子計算機.....	86
5.2.1 電子計算機共通対策.....	86
趣旨（必要性）.....	86
遵守事項.....	86
(1) 電子計算機の設置時.....	86
(2) 電子計算機の運用時.....	88
(3) 電子計算機の運用終了時.....	90
5.2.2 端末.....	90
趣旨（必要性）.....	90
遵守事項.....	91
(1) 端末の設置時.....	91
(2) 端末の運用時.....	92
5.2.3 サーバ装置.....	93
趣旨（必要性）.....	93
遵守事項.....	93
(1) サーバ装置の設置時.....	93
(2) サーバ装置の運用時.....	93
5.3 アプリケーションソフトウェア.....	96
5.3.1 通信回線を介して提供するアプリケーション共通対策.....	96
趣旨（必要性）.....	96
遵守事項.....	96

(1) サービスの導入時	96
(2) サービスの運用時	96
5.3.2 電子メール	97
趣旨（必要性）	97
遵守事項	97
(1) 電子メールの導入時	97
(2) 電子メールの運用時	97
5.3.3 ウェブ	98
趣旨（必要性）	98
遵守事項	98
(1) ウェブの導入時	98
(2) ウェブの運用時	99
5.4 通信回線	100
5.4.1 通信回線共通対策	100
趣旨（必要性）	100
遵守事項	100
(1) 通信回線を構築する場合	100
(2) 通信回線を運用する場合	102
(3) 通信回線の運用停止時	104
5.4.2 府省庁内通信回線の管理	104
趣旨（必要性）	104
遵守事項	104
(1) 府省庁内通信回線を構築する場合	104
(2) 府省庁内通信回線を運用する場合	104
(3) 回線の対策	105
5.4.3 府省庁外通信回線との接続	106
趣旨（必要性）	106
遵守事項	106
(1) 府省庁内通信回線を府省庁外通信回線と接続する場合	106
(2) 府省庁外通信回線と接続している府省庁内通信回線を運用する場合	107
第6部 個別事項についての対策	109
6.1 個別事項	109
6.1.1 外部委託	109
趣旨（必要性）	109
遵守事項	109
(1) 府省庁内における情報セキュリティ確保の仕組みの整備	109
(2) 委託先に適用する情報セキュリティ対策の整備	110
(3) 外部委託の実施における手続きの遵守	110
6.1.2 府省庁外での情報処理の制限	112
趣旨（必要性）	112

遵守事項.....	113
(1) 安全管理措置の整備	113
(2) 許可及び届出の取得及び管理	113
(3) 安全管理措置の遵守	115
6.1.3 府省庁支給以外の情報システムによる情報処理の制限	116
趣旨（必要性）	116
遵守事項.....	116
(1) 安全管理措置の整備	116
(2) 許可及び届出の取得及び管理	116
(3) 安全管理措置の遵守	117
6.2 その他	119
6.2.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止.....	119
趣旨（必要性）	119
遵守事項.....	119
(1) 措置の徹底.....	119

第1部 総則

1.1.1 本統一基準の位置付け

(1) 政府機関の情報セキュリティ対策の強化における本統一基準の位置付け

各府省庁の情報セキュリティの確保については、各府省庁が自らの責任において対策を講じていくことが原則である。しかし、政府機関全体の情報セキュリティ対策を強化・拡充するためには、「政府機関の情報セキュリティ対策の強化に関する基本方針（平成17年9月15日付情報セキュリティ政策会議決定）」に基づき、政府機関が行うべき情報セキュリティ対策の統一的な枠組みを構築し、各府省庁の情報セキュリティ水準の斉一的な引き上げを図ることが必要である。そこで本統一基準は、この政府機関統一的な枠組みの中で、各府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

(2) 本統一基準の改訂

情報セキュリティの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捉え、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。本統一基準については、これを各府省庁においてそれぞれの府省庁の特性を踏まえた上で情報セキュリティ対策基準（以下「省庁対策基準」という。）及び実施手順の整備に活用し、また情報セキュリティ対策の評価に使用することにより、本統一基準の内容を追加・修正等すべきことが明らかになることが考えられる。また、情報技術の進歩に応じて、本統一基準に記載する情報セキュリティ対策を変更することも必要となり得る。

このため、本統一基準の見直しを定期的に行い、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、その適用性を将来にわたり維持するものとする。また、各府省庁においては、本統一基準が更新された場合、その内容を省庁対策基準に適切に反映させる必要がある。

(3) 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、法令及び規制等（以下「関連法令等」という。）においても規定されているため、情報セキュリティ対策を実施する際には、本統一基準のほか関連法令等を遵守しなければならない。なお、これらの関係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、情報セキュリティ対策に係る内容について定めた既存の政府決定等についても同様に遵守すること。

解説：既存の政府決定等については本書別添資料 A.1.3 を参照。

1.1.2 本統一基準の使い方

(1) 本統一基準と省庁対策基準との関係

本統一基準は、すべての府省庁が情報セキュリティの確保のために採るべき対策、及び、その水準を更に高めるための対策の基準を定めたものである。各府省庁においては、本統一基準で定められた以上の情報セキュリティ確保を目標として、現行の情報セキュリティ関係規程について必要な見直しを行うものとする。したがって、各府省庁において、本統一基準で定められている内容を合理的な理由なく省庁対策基準に反映させないということはあってはならない。各府省庁は、各府省庁の特性を踏まえつつ、情報セキュリティ関係規程に盛り込むべき内容を決定し、本統一基準を直接参照する、本統一基準をそのまま取り込む、又は構成や表現を変えて盛り込む等の方法により適切に反映させるものとする。

(2) 適用対象範囲

本統一基準が適用される対象範囲を以下のように定める。

- (a) 本統一基準は、「情報」を守ることを目的に作成されている。本統一基準において「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。したがって、作業途上の文書も適用対象であり、書面に記載された情報には、情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面及び情報システムに関する設計書が含まれる。
- (b) 本統一基準は、行政事務従事者のうち、情報及び情報システムを取り扱う者に適用される。なお、本統一基準中、特に断りがないものを除き、「行政事務従事者」とは、情報及び情報システムを取り扱う行政事務従事者をいう。
- (c) 本統一基準における「府省庁」とは、内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、防衛庁、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省及び環境省をいう。

(3) 全体構成

本統一基準は、部、節及び項の3つの階層によって構成される。

本統一基準は、情報セキュリティ対策を「組織と体制の構築」、「情報についての対策」、「セキュリティ要件の明確化に基づく対策」、「情報システムについての対策」、「個別事項についての対策」に部として分類し、さらに内容に応じて節として対策項目に分け、その下に項として対策基準を定めている。

- (a) 「組織と体制の構築」では、組織全体として情報セキュリティ対策を実施するに当たり、実施体制や評価手順、違反や例外措置などの組織として構築すべき課題を取り上げ、組織としての運用に係る各職員の権限と責務を明確にする。
- (b) 「情報についての対策」では、情報の作成、利用、保存、移送、提供及び消去等といった情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、

各職員が業務の中で常に実施する情報保護の対策を示す。

- (c) 「セキュリティ要件の明確化に基づく対策」では、情報システムにおいて、アクセス制御の観点など導入すべきセキュリティ機能を示すとともに、セキュリティホール、不正プログラム及びサービス不能攻撃等の脅威を防ぐために遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。
- (d) 「情報システムについての対策」では、電子計算機及び通信回線等の個別の情報システムの特性及びライフサイクルの観点から、それぞれ遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。
- (e) 「個別事項についての対策」では、業務の外部委託や政府部外での情報処理等の、特に情報セキュリティ上の配慮が求められる個別事象に着目し、それぞれ遵守すべき事項を定める。

(4) 対策項目の記載事項

本統一基準では、各府省庁が行うべき対策基準について対策項目ごとに、遵守事項を示す。

(5) 対策レベルの設定

情報セキュリティ対策においては、対象となる情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様ではない。また、該当する情報システム及び業務の特性に応じて、各対策項目で適切な強度の対策を実施すべきである。したがって、本統一基準においては、各対策項目で対策の強度に段階を設け、採るべき遵守事項を定めている。この段階を「対策レベル」と呼び、以下のように定義する。

- (a) 「基本遵守事項」は、保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項
- (b) 「強化遵守事項」は、特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項

以上より、各府省庁は、基本遵守事項以上の対策を実施することとなるが、当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない。

なお、対策項目によっては、強度にかかわらず実施されるべき対策もあるため、その場合には対策レベルは設けていない。

(6) 評価の方法

情報セキュリティ対策は、一過性のものとはせず、遅滞なく継続的に取組みを実施できるものであることが重要である。したがって、各府省庁においては本統一基準に基づき、定期的又は事案等の発生の状況に応じて情報セキュリティ監査を行い、以下のことを確認する必要がある。

- (a) 各府省庁の基準が統一基準に準拠した内容となっていること。(設計の遵守性確認)
- (b) 実際の運用が各府省庁の基準に準拠していること。(運用の遵守性確認)
- (c) 情報セキュリティ関係規程の内容がリスクに応じて適切であること、効率的な内容であること、あるいは実現困難な内容となっていないこと。(設計の妥当性確認)
- (d) 実際の運用がリスクに応じて有効で効率的であること。(運用の妥当性確認)

特に、各府省庁の情報セキュリティ監査においては、設計及び運用の遵守性確認をその第一の目的とする。ただし、監査の過程において、設計(整備)及び運用(実施)の妥当性に関連して改善すべきと思われる点が発見された場合には、それを要検討事項にすることが望ましい。なお、本統一基準においては、実施すべき者を具体的に示して遵守事項を定めているため、対策の実施状況については各自の役割に応じた自己点検を実施することとする。情報セキュリティ対策においては、各自がそれぞれの役割を十分に実行することが不可欠であり、自己点検を活用することによって、各自における対策の実効性を確保するためである。したがって、各府省庁が監査を行う際には、その自己点検の適正さを確認し、運用の実施状況の把握に用いるものとする。

また、情報セキュリティ対策の実施については、原則として、各府省庁の責任において運用することが大前提であるが、政府全体としての情報セキュリティ対策推進の観点から、各府省庁は対策の実施状況及び監査結果について内閣官房情報セキュリティセンターに報告を行うこととする。さらに、内閣官房情報セキュリティセンターは、本統一基準の評価指標に基づき、各府省庁の情報セキュリティ関係規程の整備状況及び対策実施状況について定期的又は必要に応じて検査し、評価することとする。なお、対象となる情報システムの範囲については内閣官房情報セキュリティセンターが各府省庁と協議して定めるものとする。

1.1.3 用語定義

【あ】

- 「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。
- 「アプリケーション」とは、オペレーティングシステム上で動作し、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、第三者に容易に解読されないよう、あらかじめ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ハードウェア、ソフトウェア、ファームウェア及びそれらの組合せをいう。
- 「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバールーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

- 「委託先」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を請け負った者をいう。
- 「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。
- 「ウェブサーバ」とは、HTTP サーバアプリケーション、当該サーバアプリケーションで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のようにウェブサーバと一体として動作するハードウェアをいう。
- 「受渡業者」とは、安全区域内で職務に従事する行政事務従事者との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。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。

【か】

- 「外部委託」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を政府部外の者に請け負わせることをいう。
- 「外部記録媒体」とは、情報機器から取り外しすることが可能な記録装置（磁気テープ、磁気ディスク、光ディスク、カセットテープ、MO、フロッピーディスク及び USB メモリ等）をいう。
- 「可用性」とは、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。
- 「可用性 1 情報」とは、可用性 2 情報以外の情報をいう。
- 「可用性 2 情報」とは、行政事務で取り扱う情報のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
- 「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- 「完全性 1 情報」とは、完全性 2 情報以外の情報をいう。
- 「完全性 2 情報」とは、行政事務で取り扱う情報のうち、その改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
- 「機密性」とは、情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保することをいう。
- 「機密性 1 情報」とは、機密性 2 情報又は機密性 3 情報以外の情報をいう。
- 「機密性 2 情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報をいう。
- 「機密性 3 情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。
- 「強制アクセス制御（MAC：Mandatory Access Control）」とは、主体が客体に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それを保護すべき対象ではない

ものとする事はできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。

- 「行政事務従事者」とは、政府職員、請負業者、外部委託先その他行政事務の遂行に係る者のうち、それぞれの府省庁の管理対象である情報及び情報システムを取り扱う者をいう。
- 「業務用電子メール」とは、各府省庁が運営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いう。
- 「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、1つの識別コードは1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、利用状況などを考慮して、1つの識別コードを複数の主体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。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
- 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造又は提供元等から公開されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公開されたセキュリティホール等が該当する。
- 「公開されていないセキュリティホール」とは、ソフトウェアの提供元等からセキュリティホール情報が公開されていないようなセキュリティホールのことであり、パッチなども提供されていないことが想定される。

【さ】

- 「サーバ装置」とは、通信回線等を經由して接続してきた電子計算機に対して、自らが保持しているサービスを提供する電子計算機をいう。
- 「サービス」とは、サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能群をいう。
- 「サービス不能攻撃」とは、セキュリティホールを悪用しサーバ装置若しく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、又はサーバ装置、通信回線装置若しくは通信回線の容量を上回る大量のアクセスを意図的に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。
- 「最小特権機能」とは、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。
- 「識別」とは、情報システムにアクセスする主体を特定することをいう。
- 「識別コード」とは、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や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。
- 「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。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本統一基準における「主体認証」については、公的又は第三者による証明に限るものではない。

- 「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、磁気テープカードやICカード等がある。
- 「情報システム」とは、情報処理及び通信に係るシステムをいう。
- 「情報セキュリティ関係規程」とは、省庁基準及び省庁基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。
- 「情報セキュリティ対策」とは、情報に関してその機密性、完全性及び可用性を維持することをいい、策定・導入、運用、評価、見直しの各サイクルで実施すべき情報セキュリティに関する取組みの全体をいう。
- 「情報の移送」とは、府省庁外に、電磁的に記録された情報を送信すること及び情報を記録した外部記録媒体やPC並びに書面に印刷された情報を運搬することをいう。
- 「政府職員」とは、人事発令を受けて行政事務に従事する者をいう。
- 「セキュリティホール」とは、オペレーティングシステム又はアプリケーション等に存在し、それら自身や処理する情報のセキュリティが侵害される原因となる可能性のある問題をいう。
- 「ソフトウェア」とは、電子計算機を動作させる手順及び命令を電子計算機が理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム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】

- 「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。
- 「耐タンパー性」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。
- 「端末」とは、端末を利用する行政事務従事者が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆるPCのほか、PDA等も該当する。
- 「通信回線」とは、これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、電子計算機間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的

な通信回線をいう。

- 「通信回線装置」とは、回線の接続のために設置され、電子計算機により通信回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。
- 「電子計算機」とは、コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。
- 「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、電子メールの利用者に対する電子メールの送受信のサービス及び電子メールの配送を行うアプリケーション並びにそのアプリケーションを動作させる電子計算機をいう。
- 「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、再配付禁止、暗号化必須、読後廃棄等をいう。

【は】

- 「パッチ」とは、発見された問題点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、パッチ、ホットフィクス、サービスパック等名称が異なる。
- 「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組み合わせにより主体認証を行う方法である。
- 「府省庁外」とは、政府職員の各々が所属する府省庁が管理する庁舎の外をいう。
- 「府省庁外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び府省庁管理又は他組織管理）及び通信回線装置を問わず、府省庁が管理していない電子計算機が接続され、当該電子計算機間の通信に利用する論理的な通信回線をいう。
- 「府省庁外での情報処理」とは、府省庁の管理部外で行政事務の遂行のための情報処理を行うことをいう。なお、オンラインで府省庁外から政府職員の各々が所属する府省庁の情報システムに接続して、情報処置を行う場合だけではなく、オフラインで行う場合も含むものとする。
- 「府省庁支給以外の情報システム」とは、政府職員の各々が所属する府省庁が支給する情報システム以外の情報システムをいう。いわゆる私物のPCその他、当該府省庁への出向者に対して出向元組織が提供する情報システムも含むものとする。
- 「府省庁支給以外の情報システムによる情報処理」とは、府省庁支給以外の情報システムを用いて行政事務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、たとえば、府省庁の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

- 「府省庁内」とは、政府職員の各々が所属する府省庁が管理する庁舎の内をいう。
- 「府省庁内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び府省庁管理又は他組織管理）及び通信回線装置を問わず、府省庁が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。
- 「不正プログラム」とは、コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。
- 「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等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。
- 「付与」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。

【ま】

- 「無線 LAN」とは、無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a、802.11b、802.11g、Bluetooth 等が挙げられる。
- 「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。
- 「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。

【や】

- 「要安定情報」とは、可用性 2 情報をいう。
- 「要機密情報」とは、機密性 2 情報及び機密性 3 情報をいう。
- 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。
- 「要保全情報」とは、完全性 2 情報をいう。

【ら】

- 「例外措置」とは、行政事務従事者がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。
- 「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。
- 「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

【A～Z】

- 「VPN (Virtual Private Network)」とは、暗号技術等を利用し、インターネットなどの公衆回線を私設通信回線として広域化するための技術をいう。

第2部 組織と体制の構築

2.1 導入

2.1.1 組織・体制の確立

趣旨（必要性）

情報セキュリティ対策は、それに係るすべての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を確立する必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。

遵守事項

(1) 最高情報セキュリティ責任者の設置

【基本遵守事項】

(a) 最高情報セキュリティ責任者を1人置くこと。

解説：各府省庁における情報セキュリティ対策の最高責任者を定めた事項である。

情報セキュリティ対策の実現には、行政事務従事者一人一人の意識の向上や責務の遂行はもちろんのこと、組織的な取組みの推進や幹部の責任を持った関与が必須であり、各府省庁における最高責任者の設置とその役割の明確化が重要である。なお、本統一基準で規定する各役割についてはイメージ図（本書別添資料 A.1.1）を参考にされたい。

(b) 最高情報セキュリティ責任者は、自らが所属する府省庁における情報セキュリティ対策に関する事務を統括すること。

解説：最高情報セキュリティ責任者は、各府省庁内における情報セキュリティ対策の推進体制が十分機能するように管理するとともに、省庁基準の決定や評価結果による見直しに関する承認等を行う。

(c) 最高情報セキュリティ責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くこと。

解説：情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして設置することを定めた事項である。最高情報セキュリティ責任者が、情報システムに関する技術や事案の対処などの専門的な知識及び経験を高度な水準で有しているため、専門家の助言を必要としないといった特殊な場合を除き、設置を義務付けているものである。

各府省庁における情報セキュリティ対策については、情報システムに関

する技術や事案に対する対処など専門的な知識及び経験が必要となるため、省庁基準の策定・導入から運用、評価、見直しまで専門的な助言を行う専門家を活用することが重要である。なお、CIO(情報化統括責任者)補佐官は最高情報セキュリティアドバイザーを兼務することができる。

(2) 情報セキュリティ委員会の設置

【基本遵守事項】

- (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を設置し、委員長及び委員を任命すること。

解説：各府省庁の省庁基準の決定等を行う機能を持つ組織について定めた事項である。

情報セキュリティ対策の運用を円滑に進めるには、委員会を設置し組織全体で取り組むことが重要である。最高情報セキュリティ責任者は、委員長を兼務することが可能である。なお、実務を担当する下位委員会を設置し、又は既存の情報システム管理部門に情報セキュリティ対策の府省庁内での運用を統括する機能を付与するなどして、部門横断的な連携の仕組みを確立することが望まれる。

- (b) 情報セキュリティ委員会は、情報セキュリティに関する省庁基準を策定し、最高情報セキュリティ責任者に承認を得ること。

解説：府省庁全体として定めるべき省庁基準策定に関する情報セキュリティ委員会の役割を定めた事項である。

(3) 情報セキュリティ監査責任者の設置

【基本遵守事項】

- (a) 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を1人置くこと。

解説：各府省庁において決定した省庁基準に基づき監査を行う責任者を定めた事項である。

情報セキュリティ監査責任者は、情報セキュリティ責任者が所管する組織における情報セキュリティ監査を実施するため、情報セキュリティ責任者と兼務することはできない。

監査の実効性を確保するために、情報セキュリティ責任者より職務上の上席者を情報セキュリティ監査責任者に任命することが望ましい。

情報セキュリティ監査責任者は、府省庁内の情報セキュリティに関する情報を共有するために、情報セキュリティ委員会にオブザーバとして参加することが望まれる。

情報セキュリティ監査責任者の業務を補佐するために、府省庁の部内及び部外の担当者を設置することが必要となる場合もある。また、業務の実効性を担保するために外部組織の活用が必要となる場合も考えられる。

- (b) 情報セキュリティ監査責任者は、省庁基準に基づき監査を行うこと。

(4) 情報セキュリティ責任者の設置

【基本遵守事項】

- (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に係る管理を行う単位を定め、その単位ごとに情報セキュリティ責任者を置くこと。そのうち、情報セキュリティ責任者を統括する者として統括情報セキュリティ責任者を1人指名すること。

解説：情報セキュリティ対策の運用について管理を行う単位を定め、組織内で役割の明確化を行うべき事項に関して定めた事項である。

「管理を行う単位」は、部、局（外局、地方支分局等含む。）ごとや情報システムごと等が挙げられる。情報セキュリティ責任者は、府省庁の実施手順を策定するとともに、組織内での情報セキュリティ対策の運用実態を十分踏まえ、実務レベルでの管理の仕組みを確立し、すべての行政事務従事者への責務の周知や教育を行う等、個別対策を機能させる環境を整備することが重要である。

- (b) 情報セキュリティ責任者は、所管する部門における情報セキュリティ対策に関する事務を統括すること。
- (c) 統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定を策定し、最高情報セキュリティ責任者の承認を得ること。

解説：「雇用の開始、終了及び人事異動等に関する管理の規定」とは、現実の人事配置状況と、情報システム上のアクセス権の付与状況等の不整合や採用及び異動時等における適宜適切な教育の不十分さを原因とする情報セキュリティ侵害を回避することを目的とする規定のことである。具体的には、

- ・人事担当課又は各課室から、情報システム所管課に人事異動に関する情報が提供される連絡体制
- ・人事異動の情報に基づき、アクセス権の変更、職員の教育等の情報セキュリティ関係業務を適切に実施するための手順

等を整備することが求められる。これには、鍵やIDカード、通行証の発行から失効及び返却までの管理、古いアカウントの閉鎖等情報システムへのアクセス権の変更の管理も含まれる。

- (d) 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、終了及び人事異動等に関する管理の規定に従った運用がなされていることを定期的に確認すること。
- (e) 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を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を連絡すること。
- (f) 統括情報セキュリティ責任者は、すべての情報セキュリティ責任者に対する連絡網を整備すること。

(5) 情報システムセキュリティ責任者の設置

【基本遵守事項】

- (a) 情報セキュリティ責任者は、所管する部門における情報システムごとに情報システムセキュリティ責任者を置くこと。

解説：各情報システムにおける情報セキュリティ対策の責任者を定めた事項である。

庁内 LAN システムのような全省的なシステム、特定部門における個別業務システムその他府省庁のすべての情報システムを、情報システム単位の情報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。

- (b) 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対する情報セキュリティ対策の管理に関する事務を統括すること。
- (c) 情報セキュリティ責任者は、情報システムセキュリティ責任者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を報告すること。
- (d) 統括情報セキュリティ責任者は、すべての情報システムセキュリティ責任者に対する連絡網を整備すること。

(6) 情報システムセキュリティ管理者の設置

【基本遵守事項】

- (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：各情報システムにおいて、その管理業務ごとの情報セキュリティ対策の実施を管理する者を定めた事項である。

企画、開発、運用、保守等の情報システムのライフサイクルやサーバ、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設置する必要がある。

情報システムセキュリティ管理者は、情報セキュリティ責任者によって定められた手順や判断された事項に従い、対策を実施する。

- (b) 情報システムセキュリティ管理者は、所管する管理業務における情報セキュリティ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、情報システムセキュリティ管理者を置いた時及び変更した時は、統括情報セキュリティ責任者にその旨を報告すること。
- (d) 統括情報セキュリティ責任者は、すべての情報システムセキュリティ管理者に対する連絡網を整備すること。

(7) 課室情報セキュリティ責任者の設置

【基本遵守事項】

- (a) 各課室に、課室情報セキュリティ責任者を 1 人置くこと。

解説：課室単位での情報セキュリティ対策の事務を統括する者を定めた事項である。

課室情報セキュリティ責任者は、情報セキュリティ対策を効果的に把握、管理するために各課室に置くものであり、各課室が 1 人を定め、統括情報セキュリティ責任者に申告するものである。全省的な情報システムにおいては、パッチ等の対策用ファイルはネットワーク経由で適用されることが一般的であるが、課室等の物理的又は組織的な単位での情報セキュリティ対策の運用状況を把握・管理することが、対策の周知・徹底には重要であることから、課室情報セキュリティ責任者を置くものである。

- (b) 課室情報セキュリティ責任者は、課室における情報セキュリティ対策に関する事務を統括すること。
- (c) 課室情報セキュリティ責任者は、就任した時又は交代した時は、統括情報セキュリティ責任者にその旨を申告すること。
- (d) 統括情報セキュリティ責任者は、すべての課室情報セキュリティ責任者に対する連絡網を整備すること。

2.1.2 役割の分離

趣旨（必要性）

情報セキュリティ対策に係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、情報セキュリティが確保されていることが確認、証明されたことにはならない。情報セキュリティを確立するためには、兼務してはいけない役割が存在する。

これらのことを勘案し、本項では、情報セキュリティ対策に係る職務の分離に関する対策基準を定める。

遵守事項

(1) 兼務を禁止する役割の規定

【基本遵守事項】

- (a) 情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
 - (ア)承認又は許可事案の申請者とその承認者又は許可者
 - (イ)監査を受ける者とその監査を実施する者

解説：承認又は許可する役割の者自らが、申請をする場合には、その申請について自らが承認又は許可することはできない。その場合には、同じ承認又は許可をする役割を担う他者に申請し、承認又は許可を得る必要がある。

2.1.3 違反と例外措置

趣旨（必要性）

政府において情報セキュリティを継続的に維持するためには、万一違反があった場合に、定められた手続きに従って、適切に対応する必要がある。

また、情報セキュリティ関係規程の適用が行政事務の適正な遂行を著しく妨げる等、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採用し、又は規定を実施しないことを認めざるを得ない場合についても、あらかじめ定められた例外措置のための手続きにより、情報セキュリティを維持しつつ柔軟に対応できるものでなければ、当該規程の実効性を確保することが困難となる。

これらのことを勘案し、本項では、違反と例外措置に関する対策基準を定める。

遵守事項

(1) 違反への対応

【基本遵守事項】

- (a) 行政事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合には、各規定の実施に責任を持つ情報セキュリティ責任者にその旨を報告すること。

解説：府省庁における情報セキュリティを継続的に維持し、重大な違反を確実に捕捉するための事項である。府省庁においては、例規への違反を知った者に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おいては、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。

情報セキュリティ関係規程への重大な違反とは、当該違反により府省庁の業務に重大な支障を来すもの、又はその可能性のあるものをいう。

- (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採らせること。

解説：情報セキュリティ関係規程への重大な違反により機密性、完全性、可用性が損なわれる等した情報及び情報システムを回復するとともに、情報セキュリティ対策の適切な実施を再度徹底するための事項である。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ていれば、これを早急に解決し、問題の拡大を防止する必要がある。情報セキュリティ関係規程を知らずに違反を犯したのであれば、違反者にこれを知らせ、同者及び必要な者にこれらの措置を採らせる必要がある。

- (c) 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、違反者の任命権者及び統括情報セキュリティ責任者にその旨を報告すること。

解説：情報セキュリティ関係規程への違反があった場合に、懲罰を含む適切な措置がなされるための事項である。違反者に対する懲罰はその任命権者

が行うこととなるため、違反の事実を、その内容、結果、業務への影響、社会的評価等を含めて違反者の任命権者に報告する必要がある。

(2) 例外措置

【基本遵守事項】

- (a) 情報セキュリティ委員会は、例外措置の適用の申請を審査するための手続きを整備すること。

解説：例外措置の適用の申請を受けた際に審査を遅滞なく実施できるように、その手続きを事前に整備しておくための事項である。例外措置の内容に応じて、審査する者を事前に定めておく必要があるが、緊急を要して申請される場合、あらかじめ軽微な事案についての審査を適切な担当者に委任しておき、業務遂行に不要の遅滞を生じさせずに審査を速やかに実施する必要がある。そのため、審査を厳格に行う場合と審査を委任する場合の要件を事前に検討し、当該委任について定めておくことが重要である。

- (b) 行政事務従事者は、例外措置を適用する場合には、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情報システムセキュリティ管理者を通じて統括情報セキュリティ責任者に対して、例外措置の適用を申請し、許可を得ること。行政事務従事者は、申請の際に以下の事項を含む項目を明確にすること。

(ア)申請者の情報（氏名、所属、連絡先）

(イ)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適用箇所（規程名と条項等）

(ウ)例外措置の適用を申請する期間

(エ)例外措置の適用を申請する措置内容（講じる代替手段等）

(オ)例外措置の適用を終了したときの報告方法

(カ)例外措置の適用を申請する理由

解説：例外措置を当事者の独断で行わせないための事項である。

当事者は、許可を得てから、例外措置を講じる。ただし、行政事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とは異なる代替の方法を採用し、又は規定を実施しないことが不可避のときは、事後速やかに申請及び許可を得ること。

行政事務従事者は、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場合の被害の大きさと影響を検討、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、リスク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。

(c) 統括情報セキュリティ責任者、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及び情報システムセキュリティ管理者は、行政事務従事者による例外措置の適用の申請を、定められた手続きに従って審査し、許可の可否を決定すること。また、決定の際に、以下の項目を含む例外措置の適用審査記録を整備し、最高情報セキュリティ責任者に報告すること。

(ア)決定を審査した者の情報(氏名、役割名、所属、連絡先)

(イ)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(講じる代替手段等)
- 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

(ウ)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適用箇所(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：統括情報セキュリティ責任者、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及び情報システムセキュリティ管理者に、例外措置の適用の申請を適切に審査させるための事項である。

審査に当たっては、例外措置の適用を許可した場合のリスクと不許可とした場合の行政事務遂行等への影響を評価した上で、その判断を行う必要がある。例外措置の適用審査記録は、将来、許可をさかのぼって取り消す場合に、該当する申請をすべて把握し、一貫性をもって取り消すために必要となる。

(ア)の「役割名」には、統括情報セキュリティ責任者、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及び情報システムセキュリティ管理者のいずれかを記載する。

(d) 行政事務従事者は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了したときに、当該例外措置の許可を与えた者にその旨を報告すること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用の終了を確認するための事項である。

例外措置の適用期間が終了した場合及び期間終了前に適用を終了する場合には、許可を受けた行政事務従事者が、許可を与えた者に終了を報告

しなければならない。

- (e) 統括情報セキュリティ責任者、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及び情報システムセキュリティ管理者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用期間を、許可を受けた者に遵守させるための事項である。

必要な対応としては、許可を受けた者が報告を怠っているのであればそれを催促すること、許可を受けた者が例外措置の適用を継続している場合にはその延長について申請させそれについて審査すること、が挙げられる。

- (f) 最高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、例外措置の適用審査記録の参照について、情報セキュリティ監査を実施する者からの求めに応ずること。

解説：最高情報セキュリティ責任者に、例外措置の適用審査記録の台帳を維持・整備することを求める事項である。例外措置の適用を許可したとしても、それが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採用し、又は遵守事項を実施していないことに変わりはない。もしも、例外措置を適用していることにより重大な事故が発生した場合には、同様の例外措置を適用している者に対して、事故発生の予防について注意を喚起したり、例外措置適用の許可について見直しをしたりするなどの対応を検討する必要がある。そのためには、例外措置を適用している者や情報システムの現状について、最新の状態のものを集中して把握する必要がある。

2.2 運用

2.2.1 情報セキュリティ対策の教育

趣旨（必要性）

情報セキュリティ関係規程が適正に策定されたとしても、行政事務従事者にその内容が周知されず、行政事務従事者がこれを遵守しない場合には、情報セキュリティ対策の水準の向上を望むことはできない。このため、すべての行政事務従事者が、情報セキュリティ対策の教育を通じて、情報セキュリティ関係規程に関する理解を深め、情報セキュリティ対策を適切に実践できるようにすることが必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の教育に関する実施基準を定める。

遵守事項

(1) 行政事務従事者に対する情報セキュリティ対策教育の実施

【基本遵守事項】

- (a) 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、行政事務従事者（委託先の行政事務従事者を除く。以下この項において同じ。）に対し、その啓発をすること。

解説：統括情報セキュリティ責任者に情報セキュリティ対策の啓発の実施を求める事項である。

- (b) 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、行政事務従事者に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。

解説：統括情報セキュリティ責任者が情報セキュリティ対策の教育のための資料を整備することを求める事項である。

教育の内容については、府省庁の実情に合わせて幅広い角度から検討し、行政事務従事者が対策内容を十分に理解できるものとする必要がある。

- (c) 統括情報セキュリティ責任者は、行政事務従事者が毎年度最低1回、受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備すること。

解説：情報セキュリティ対策の教育の最低限の受講回数について定めた事項である。

なお、情報セキュリティ事案の発生など情報セキュリティ環境の変化に応じて、適宜、教育を行うことが重要である。

- (d) 統括情報セキュリティ責任者は、行政事務従事者の着任時、異動時に新しい職場等で3ヶ月以内に受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備すること。

解説：着任、異動した行政事務従事者に対して、早期に情報セキュリティ対策の教育を受講させることによって、当該行政事務従事者の情報セキュリティ対策の適正な実施を求める事項である。

なお、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、対象から除外され得る。

- (e) 統括情報セキュリティ責任者は、行政事務従事者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。

解説：情報セキュリティ対策の教育の受講状況について把握できる仕組みを整備し、行政事務従事者への教育を促すことを求める事項である。

- (f) 統括情報セキュリティ責任者は、行政事務従事者の受講状況について、課室情報セキュリティ責任者に通知すること。課室情報セキュリティ責任者は、行政事務従事者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。行政事務従事者が当該勧告に従わない場合には、統括情報セキュリティ責任者にその旨を報告すること。

解説：情報セキュリティ対策の教育を受講しない者への対策を定めた事項である。

なお、定められた教育を受講しない行政事務従事者は、その遵守違反について責任を問われることになる。

- (g) 統括情報セキュリティ責任者は、毎年度1回、最高情報セキュリティ責任者及び情報セキュリティ委員会に対して、行政事務従事者の情報セキュリティ対策の教育の受講状況について報告すること。

解説：最高情報セキュリティ責任者及び情報セキュリティ委員会に情報セキュリティ対策の教育の受講状況を報告することを求める事項である。

【強化遵守事項】

- (h) 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、行政事務従事者に対する情報セキュリティ対策の訓練の内容及び体制を整備すること。

解説：統括情報セキュリティ責任者が情報セキュリティ対策の訓練の内容及び体制を整備することを求める事項である。

訓練の内容については、府省庁の実情に合わせて幅広い角度から検討し、行政事務従事者が対策内容を十分に理解できるものとする必要がある。

(2) 行政事務従事者による情報セキュリティ対策教育の受講義務

【基本遵守事項】

- (a) 行政事務従事者は、毎年度最低1回、情報セキュリティ対策の教育に関する規定に従って、情報セキュリティ対策の教育を受講すること。

解説：行政事務従事者が、情報セキュリティ対策の教育に関する規定に従って、これを受講することを求める事項である。

- (b) 行政事務従事者は、着任時、異動時に新しい職場等で、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。

解説：着任、異動した行政事務従事者が、確実に情報セキュリティ対策の教育を受講するための事項である。

課室情報セキュリティ責任者への確認がなされない場合は、課室情報セキュリティ責任者において、受講日程を連絡することが望ましい。

- (c) 行政事務従事者は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、課室情報セキュリティ責任者を通じて、統括情報セキュリティ責任者に報告すること。

解説：情報セキュリティ対策の教育を受講できない理由についての報告をしないままで、定められた教育を受講しない場合には、行政事務従事者は、その遵守違反について責任を問われることになる。

【強化遵守事項】

- (d) 行政事務従事者は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って、情報セキュリティ対策の訓練に参加すること。

解説：行政事務従事者が、情報セキュリティ対策の訓練に関する規定に従って、これを受講することを求める事項である。

2.2.2 事故及び障害の対応

趣旨（必要性）

情報セキュリティに関する事故や障害が発生した場合には、早急にその状況を検出し、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、その際には、事故や障害の影響や範囲を定められた責任者へ報告し、事故・障害発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

これらのことを勘案し、本項では事故及び障害時の対応基準を定める。

遵守事項

- (1) 障害等の発生に備えた事前準備

【基本遵守事項】

- (a) 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事故及び障害等（以下「障害等」という。）が発生した場合、被害の拡大を防ぐとともに、障害等から復旧するための体制を整備すること。

解説：統一基準では、「災害」については各府省庁にて別に定めるところがあるものと考えため、それを含まないが、別の定めがない場合には、本項目と同様に規定する必要がある。

- (b) 統括情報セキュリティ責任者は、障害等について行政事務従事者から情報セキュリティ責任者への報告手順を整備し、当該報告手段をすべての行政事務従事者に周知すること。

解説：窓口についての周知は、情報セキュリティ教育の中で行うとともに、窓口の連絡先を執務室内に掲示するなどして、緊急時に行政事務従事者がすぐに参照できるようにすることが必要である。情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。

- (c) 統括情報セキュリティ責任者は、障害等が発生した際の対応手順を整備すること。

解説：対応手順として障害等の発生時における緊急を要する対応等の必要性に

備えて、通常とは異なる例外措置の承認手続きを設けることもあわせて検討する必要がある。対応する者に、ある程度の権限の委譲がされない、適切な措置に遅延等が発生することが予想される。そのようなことがないよう検討すること。

- (d) 統括情報セキュリティ責任者は、障害等に備え、要保護情報を取り扱う情報システムのうち行政事務の遂行のため特に重要と認めた情報システムについて、その情報システムセキュリティ責任者及び情報システムセキュリティ管理者の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

解説：統括情報セキュリティ責任者は、すべての情報システムセキュリティ責任者及び情報システムセキュリティ管理者の連絡網を整備しているものである（統一基準 2.1.1）が、これは「緊急」連絡網を加えて整備することを定める事項である。

【強化遵守事項】

- (e) 統括情報セキュリティ責任者は、障害等について府省庁の外部から報告を受けるための窓口を設置し、その窓口への連絡手段を府省庁外に公表すること。

解説：府省庁における情報セキュリティ対策の不備について外部の者が発見したり、府省庁において管理する電子計算機がサービス不能攻撃を外部に行った場合等、各府省庁を取り巻く外部に対して、関連業務に支障を生じさせたり、情報セキュリティ上の脅威を与えたりした際に、その連絡を外部から受ける体制についても整備し、連絡先を当該府省庁の外部に公表することを求める事項である。

(2) 障害等の発生時における報告と応急措置

【基本遵守事項】

- (a) 行政事務従事者は、障害等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、情報セキュリティ責任者にその旨を報告すること。

解説：障害等が発生した場合に、行政事務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害等への対応を開始することができるように求める事項である。

- (b) 行政事務従事者は、障害等が発生した際の対応手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

解説：行政事務従事者の判断による被害拡大防止策が常に適切なものであるとは限らないため、障害等への対応手順に従うことを求める事項である。なお、対応手順は、より具体的に整備するとともに、対応の体制を速やかに整え、組織的な対応を実施することが重要である。

- (c) 行政事務従事者は、障害等が発生した場合であって、当該障害等について対応手順がないとき及びその有無を確認できないときは、その対応についての指示を受けるまで、障害等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

解説：対応手順が想定していない事故が発生した場合、行政事務従事者は対応の指示を受けるまでの間も障害等の拡大防止に努めることを求める事項である。

(3) 障害等の原因調査と再発防止策

【基本遵守事項】

- (a) 情報セキュリティ責任者は、障害等が発生した場合には、障害等の原因を調査し再発防止策を策定し、その結果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。

解説：情報セキュリティ責任者に対して、障害等の原因を究明し、それに基づき障害等の再発防止策を策定することを求める事項である。

- (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障害等についての報告を受けた場合には、その内容を審査し、再発防止策を実施するために必要な措置を講ずること。

解説：事故の再発防止策を講じることを、最高情報セキュリティ責任者に求める事項である。

2.3 評価

2.3.1 情報セキュリティ対策の自己点検

趣旨（必要性）

情報セキュリティ対策は、それに係るすべての行政事務従事者が、各自の役割を確実に行うことで実効性が担保されるものであることから、すべての行政事務従事者自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要である。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

これらのことを勘案し、本項では、自己点検に関する対策基準を定める。

遵守事項

(1) 自己点検に関する年度計画の策定

【基本遵守事項】

- (a) 最高情報セキュリティ責任者は、年度自己点検計画を整備すること。

解説：自己点検を実施するに当たり、その実施頻度、実施時期、自己点検すべき項目、実施項目の選択等に関する年度自己点検計画を整備することを求める事項である。

実施頻度については、自己点検は年に2度以上実施することが望ましいが、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等、様々な選択肢が考えられる。

実施時期については、例えば、当初は毎月10項目ずつ自己点検し、行政事務従事者の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。

自己点検すべき項目については、例えば、単純に実施したことを確認するほか、遵守率を確認する等、数値評価により客観性を持った評価とすることが望ましく、様々な選択肢が考えられる。

実施項目の選択については、例えば、当初はすべての行政事務従事者が容易に遵守できる項目のみを自己点検し、行政事務従事者の意識が高まった後、遵守率が低いと想定される項目を実施するように変更する等、様々な選択肢が考えられる。

(2) 自己点検の実施に関する準備

【基本遵守事項】

- (a) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を準備すること。

解説：各行政事務従事者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、行政事務従事者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を求める事項である。

(3) 自己点検の実施

【基本遵守事項】

- (a) 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が定める年度自己点検計画に基づき、行政事務従事者に対して、自己点検の実施を指示すること。

解説：年度自己点検計画に基づき、情報セキュリティ責任者自らも含めた行政事務従事者に対して、自己点検の実施に関し指示することを求める事項である。

- (b) 行政事務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施し、自らが実施すべき情報セキュリティに対する対策項目の実施の有無を確認すること。

解説：情報セキュリティに関わる行政事務従事者に対して、自己点検の実施を求める事項である。

(4) 自己点検結果の評価

【基本遵守事項】

- (a) 行政事務従事者は、実施した自己点検の結果について、各自、情報セキュリティ責任者による評価を受けること。

解説：行政事務従事者による自己点検の結果について、情報セキュリティ責任者が評価することを求める事項である。

なお、評価においては、自己点検が正しく行われていること、統一基準に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った値とすることが望ましい。例えば、自己点検実施率や、統一基準遵守率、要改善対策数/対策実施数などの準拠率の把握が挙げられる。

- (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による自己点検が行われていることを確認し、評価すること。

解説：情報セキュリティ責任者による自己点検が適切に行われていることを、最高情報セキュリティ責任者が評価することを求める事項である。

(5) 自己点検に基づく改善

【基本遵守事項】

- (a) 行政事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、情報セキュリティ責任者にその旨を報告すること。

解説：自己の権限の範囲で改善可能である問題点については、情報セキュリティに関わるすべての行政事務従事者自らが自己改善することを求める事項である。

- (b) 最高情報セキュリティ責任者は、自己点検の結果を評価し、情報セキュリティ責任者に改善を指示すること。

解説：自己点検の結果により明らかとなった問題点について、最高情報セキュリティ責任者は、情報セキュリティ責任者に対して改善することを求める事項である。

2.3.2 情報セキュリティ対策の監査

趣旨（必要性）

情報セキュリティの確保のためには、情報セキュリティ関係規程が本統一基準に準拠して適切に策定され、かつ、当該規程が適切に行われることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、行政事務従事者による自主点検によるだけでなく、独立性を有する者による情報セキュリティ監査を実施する必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策の監査に係る対策基準を定める。

遵守事項

(1) 監査計画の整備

【基本遵守事項】

- (a) 情報セキュリティ監査責任者は、最高情報セキュリティ責任者の承認を得た上で、年度情報セキュリティ監査計画を整備すること。

解説：監査の基本的な方針として、年度情報セキュリティ監査計画を立案し、承認を受けることを求める事項である。年度情報セキュリティ監査計画には、次の事項が含まれる。

- ・重点とする監査対象及び監査目標（漏えい防止、不正アクセス防止など）
- ・監査実施期間
- ・監査業務の管理体制
- ・外部委託による監査の必要性及び範囲
- ・監査予算

なお、以前実施した監査結果で明らかになった課題及び問題点の改善状況について、監査を実施する場合には、年度情報セキュリティ監査計画

に盛り込むこと。

(2) 情報セキュリティ監査の実施に関する指示

【基本遵守事項】

- (a) 最高情報セキュリティ責任者は、年度情報セキュリティ監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示すること。

解説：年度情報セキュリティ監査計画に従って監査を実施することを求める事項である。

- (b) 最高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て、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示すること。

解説：年度情報セキュリティ監査計画において実施する定期監査以外に、府省庁内、府省庁外における事案の発生の状況又は情報セキュリティ対策の実施についての重大な変化が生じた場合にも、必要に応じて臨機応変に監査を実施することを求める事項である。

なお、府省庁内において甚大な情報セキュリティ侵害が発生した場合であって、その侵害の規模や影響度をかんがみ、より客観性・独立性が求められるときは、内閣官房情報セキュリティセンターと協力の上、外部組織による監査を検討すること。

(3) 個別の監査業務における監査実施計画の立案

【基本遵守事項】

- (a) 情報セキュリティ監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を立案すること。

解説：監査の基本的な方針に基づいて、実施すべき監査についての詳細な計画を立案することを求める事項である。監査実施計画には、次の事項が含まれる。

- ・ 監査の実施時期
- ・ 監査の実施場所
- ・ 監査の実施担当者及び割当て
- ・ 準拠性監査（情報セキュリティ関係規程に準拠した手続きが実施されていることを確認する監査）のほか、必要に応じて妥当性監査（実施している手続きが有効なセキュリティ対策であることを確認する監査）を行うかについての方針
- ・ 実施すべき監査の概要（監査要点、実施すべき監査の種類及び試査の範囲を含む。）
- ・ 監査の進捗管理手段又は体制

(4) 情報セキュリティ監査を実施する者の要件

【基本遵守事項】

- (a) 情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼すること。

解説：情報セキュリティ監査を実施する者に監査人としての独立性及び客観性を有することを求める事項である。

情報システムを監査する場合には、当該情報システムの構築又は開発をした者は、その監査をしないこと。また、運用されている情報資産の監査を行う場合には、当該情報資産を運用している者はその監査をしないこと。

- (b) 情報セキュリティ監査責任者は、必要に応じて、府省庁外の者に監査の一部を請け負せること。

解説：情報セキュリティ監査を実施する者は、監査を実施するに当たり、必要に応じて監査対象システムの詳細情報を有する組織、府庁省内の情報システム部門又は外部専門家の支援を受けることを求める事項である。

組織内に監査を実施する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。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にするための情報セキュリティ監査調達基準を整備し、当該基準に基づき外部の情報セキュリティ監査実施組織に監査を請け負せることが重要である。情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与などを考慮することが望ましい。

(5) 情報セキュリティ監査の実施

【基本遵守事項】

- (a) 情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を適切に実施すること。

解説：情報セキュリティ監査を実施する者が適切に監査を実施することを求める事項である。

- (b) 情報セキュリティ監査を実施する者は、情報セキュリティ関係規程が統一基準に準拠しているか否かを確認すること。

解説：情報セキュリティ関係規程が統一基準に準拠しているか否かの確認を求める事項である。

- (c) 情報セキュリティ監査を実施する者は、被監査部門において実施されている自己点検が年度自己点検計画に基づき正しく行われているか否か、情報セキュリティ関係規程に基づき機器の設定が行われているか否かを確認すること。また、必要に応じて、自己点検記録の査閲、機器の設定状況の点検等により、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。

解説：監査人である情報セキュリティ監査を実施する者は、被監査部門において実施されている自己点検の仕組みを踏まえ、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か否かを確認することを求める事項である。

- (d) 情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存すること。

解説：監査意見表明の根拠となる監査調書を適切に作成することを求める事項である。

監査調書とは、情報セキュリティ監査を実施する者が行った監査業務の実施記録であって、監査意見表明の根拠となるべき監査証拠、その他関連資料等を綴り込んだものをいう。情報セキュリティ監査を実施する者自らが直接に入手した資料やテスト結果だけでなく、被監査部門側から提出された資料等を含み、場合によっては組織体外部の第三者から入手した資料等を含むことがある。

- (e) 情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、最高情報セキュリティ責任者へ提出すること。

解説：監査結果を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報告をすること求める事項である。

なお、本監査は、情報セキュリティ関係規程が統一基準に準拠しているか、確認作業が同規程等に準拠して行われているか等、準拠性監査を意図したものであるが、監査の過程において、遵守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ことが望ましい。

(6) 情報セキュリティ監査結果に対する対応

【基本遵守事項】

- (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、被監査部門の情報セキュリティ責任者に対して、指摘事案に対する対応の実施を指示すること。

解説：監査報告書において指摘された課題及び問題点に対する改善を図るため、最高情報セキュリティ責任者へ被監査部門の情報セキュリティ責任者に対する対応実施の指示を求める事項である。

- (b) 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、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の

部門の情報セキュリティ責任者に対しても、同種の課題及び問題点の有無を確認するように指示すること。

解説：監査報告書において指摘された課題及び問題点が、他の監査対象にも同種の課題及び問題点として存在する可能性が高い場合又は同種の課題及び問題点の存在を緊急に確認する必要性が高い場合には、想定される他の監査対象についても一様に調査を実施する必要がある。そのため、最高情報セキュリティ責任者から情報セキュリティ責任者に対する確認の指示を求める事項である。

- (c) 情報セキュリティ責任者は、監査報告書に基づいて最高情報セキュリティ責任者から改善を指示された事案について、対応計画を報告すること。

解説：監査報告書に基づいて最高情報セキュリティ責任者から改善を指示された事案について、対応計画の報告を求める事項である。監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成することが可能な対応目標を提示すること。また、その課題及び問題点が人為によるものである場合には、情報セキュリティ責任者は、提示された対応目標を情報セキュリティ対策の教育方法や教育施策に反映すること。

- (d) 最高情報セキュリティ責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。

解説：情報セキュリティ監査責任者から報告された監査報告書において、遵守内容の妥当性に関連した改善指摘を受けた場合には、既存の情報セキュリティ関係規程の更新を検討することを求める事項である。

検討の結果、情報セキュリティ関係規程の更新を行わない場合には、その理由について明確化すること。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

趣旨（必要性）

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、情報セキュリティレベルは維持できなくなる。このため、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、作成、導入、運用、評価の各段階において、適時見直しを行う必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策の見直しに関する基準について定める。

遵守事項

(1) セキュリティ対策の見直し

【基本遵守事項】

- (a) 情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。

解説：情報セキュリティ関係規程の内容を、必要に応じて見直すことを求める事項である。見直しを行う時期は、新たなセキュリティ脅威の出現、自己点検及び監査の評価結果等により、セキュリティ対策に支障が発生しないように情報セキュリティ関係規程を整備した者が判断する必要がある。

情報セキュリティ対策の課題及び問題点に対処するため情報セキュリティ関係規程を見直した者は、当該見直した者が所属する部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、その課題及び問題点に関連する部門の情報セキュリティ関係規程を整備した者に対しても、同種の課題及び問題点の有無を確認するように連絡することを推奨する。

- (b) 行政事務従事者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行うこと。

解説：情報セキュリティ関係規程としては整備されていない情報セキュリティ対策について、その見直しを行政事務従事者に求める事項である。

第3部 情報についての対策

3.1 情報の格付け

3.1.1 情報の格付け

趣旨（必要性）

行政事務で取り扱う情報については、その目的や用途により、取扱いに慎重を要する度合いはさまざまであり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、情報の格付けが必要となる。

これらのことを勘案し、本項では、情報の格付けに関する対策基準を定める。

遵守事項

(1) 情報の格付け

【基本遵守事項】

- (a) 情報セキュリティ委員会は、行政事務で取り扱う情報について、機密性、完全性及び可用性の観点による当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること。

解説：行政事務で取り扱う情報に対し、格付けを行うために必要となる基準等を定めることを求める事項である。なお、本統一基準における情報の格付けの一覧については、本書別添資料 A.1.2 を参照されたい。

3.2 情報の取扱い

3.2.1 情報の作成と入手

趣旨（必要性）

行政事務においては、その事務の遂行のために複数の者が共通の情報を利用する場合がある。この際、利用者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し又は入手した段階で、すべての利用者において認識を合わせるための措置が必要となる。

これらのことを勘案し、本項では、情報の作成及び入手に関する対策基準を定める。

遵守事項

(1) 業務以外の情報の作成又は入手の禁止

【基本遵守事項】

- (a) 行政事務従事者は、行政事務の遂行以外の目的で、情報システムに係る情報を作成し又は入手しないこと。

解説：行政事務の遂行以外の目的で、情報システムに係る情報については、作成し又は入手しないことを求める事項である。

(2) 情報の作成又は入手時における格付けの決定と取扱制限の検討

【基本遵守事項】

- (a) 行政事務従事者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：作成した情報について、以降、適切なセキュリティ管理が施されるように、機密性、完全性、可用性の格付け等を行うことを求める事項である。情報の格付けが適切に決定されていなかった、また、明示されていなかったことを一因として情報セキュリティに関する事故が発生した場合には、事故の直接の原因となった人物のほか、情報の格付け及び明示を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、行政事務従事者が、情報の格付けとその明示を確実にすることは重要である。なお、行政事務従事者は、情報の利用を円滑に行うため、格付けを必要以上に高くしないように配慮することも必要となる。あわせて、格付けに応じた情報の取扱いを確実にするための取扱制限の必要性の有無についても検討を行わなければならない。

- (b) 行政事務従事者は、府省庁外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：外部から入手した情報についても、格付けを行い、当該格付けに従った適正な管理を求める事項である。

(3) 格付けと取扱制限の明示

【基本遵守事項】

- (a) 行政事務従事者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。

解説：作成者又は入手者によって格付けが行われた情報に対して、以降、他者が当該情報を利用する際に必要とされるセキュリティ対策レベルを示すため、情報の格付けの明示を行うことを求める事項である。また、取扱制限が必要な場合は、あわせてその明示も行わなければならない。

格付けと取扱制限の明示は、当該情報が、電磁的ファイルとして取り扱われることが想定される場合にはファイル名自体又は情報内容の中に、可搬記録媒体に保存して取り扱うことが想定される場合には可搬記録媒体に、書面に印刷されることが想定される場合には書面のヘッダ部分等に、視認できる方法でそれぞれ行う必要がある。ただし、当該情報システムに保存されているすべての情報が同じ格付け、取扱制限であり、利用するすべての行政事務従事者にてその認識が周知徹底されている場合は、この限りでない。しかし、格付けや取扱制限を認識していない行政事務従事者に当該情報システムに保存されている情報を提供する必要が生じた場合は、当該情報に視認できるような明示を行った上で提供しなければならない。

また、既に書面として存在している情報に対して格付けや取扱制限を明示する場合には、手書きによる記入又はスタンプ等による押印が必要である。なお、原則として各書面それぞれに明示すべきであるが、取り扱う単位がフォルダ単位や冊子単位の時には、その単位ごとに明示することも可能である。

なお、格付け及び取扱制限の明示とあわせて、情報の作成者又は入手者の氏名、所属、連絡先等を記載することも有益である。

(4) 格付けと取扱制限の継承

【基本遵守事項】

- (a) 行政事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

解説：情報の作成者による情報の格付けと取扱制限を継承し、以降も同様のセキュリティ対策を維持することを求める事項である。

(5) 格付けと取扱制限の変更

【基本遵守事項】

- (a) 行政事務従事者は、情報の格付けを変更する必要があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

解説：情報を利用する行政事務従事者が、当該情報の格付けを変更する場合に、

当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。当初の格付けが作成者又は入手者によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を参照した者に対しても、当該情報の格付けを変更したことを周知させる必要がある。

なお、異動等の事由により、当該情報の作成者又は入手者と相談することが困難である場合においては、課室情報セキュリティ責任者が相談を受け、その是非を検討することになる。

- (b) 行政事務従事者は、情報の取扱制限を変更する必要があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

解説：情報を利用する行政事務従事者が、当該情報の取扱制限を変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。当初の取扱制限が作成者又は入手者によって不適正に設定されていれば、当該取扱制限を修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を利用した者に対しても、当該情報の取扱制限を変更したことを周知させる必要がある。

なお、異動等の事由により、当該情報の作成者又は入手者と相談することが困難である場合においては、課室情報セキュリティ責任者が相談を受け、その是非を検討することになる。

3.2.2 情報の利用

趣旨（必要性）

行政事務においては、その事務の遂行のために多くの情報を取り扱うが、情報システムの利用者の認識不足等による情報の不適切な利用や、情報システムの管理者によるセキュリティホール対策及び不正プログラム対策の不備等の問題により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。情報を不適切に利用すると、情報の漏えい、改ざん、不当な消去、不当な持出し等によって、情報セキュリティを損なうリスクが増大し、政府に何らかの損害を与えることが考えられる。それらのリスクに対応するため、情報を適切に利用しなければならない。

これらのことを勘案し、本項では、情報の利用時に関する対策基準を定める。

遵守事項

- (1) 業務以外の利用の禁止

【基本遵守事項】

- (a) 行政事務従事者は、行政事務の遂行以外の目的で、情報システムに係る情報を利用しないこと。

解説：行政業務の遂行以外の目的で、情報システムに係る情報については、利用しないことを求める事項である。

(2) 格付け及び取扱制限に従った情報の取扱い

【基本遵守事項】

- (a) 行政事務従事者は、利用する情報に明示された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。

解説：情報に明示された格付け及び取扱制限に従って、適切に取り扱うことを求める事項である。

(3) 要保護情報の取扱い

【基本遵守事項】

- (a) 行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を府省庁外に持ち出さないこと。

解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、行政事務従事者が行政事務の遂行以外の目的で要保護情報を府省庁外へ持ち出すことを禁止する事項である。

なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。

- (b) 行政事務従事者は、要保護情報を放置しないこと。

解説：第三者による不正な操作を防止することを求める事項である。

離席する際には、ロック付きスクリーンセーバーを起動するあるいはログオフして、画面に情報を表示しないこと、また、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などを徹底する必要がある。

- (c) 行政事務従事者は、機密性3情報を必要以上に複製しないこと。

解説：不必要な複製によって情報漏えいの危険性が高くなることを考慮し、必要以上に機密性3情報を複製しないことを求める事項である。

なお、「秘密文書等の取扱いについて」(昭和40.4.15事務次官等会議申合せ)第6項では、「「極秘」の文書の複製は、絶対に行なわないこと。「秘」の文書は、指定者の承認をうけて複製することができること。」と定めている。

なお、これを徹底させる手段として、「複製禁止」の取扱制限の明示等が挙げられる。

- (d) 行政事務従事者は、要機密情報を必要以上に再配付しないこと。

解説：情報漏えいを未然に防ぐため、要機密情報の再配付は最小限にとどめることを求める事項である。

なお、これを徹底させる手段として、「再配付禁止」の取扱制限の明示等が挙げられる。

【強化遵守事項】

- (e) 行政事務従事者は、機密性 3 情報には、機密性 3 情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる必要性があると思料される場合には、格付けの変更に必要な処理を行うこと。

解説：秘密としての管理を求められる期間を明記することにより、必要以上の秘密管理を防止するための事項である。

なお、「秘密文書等の取扱いについて」(昭和 40.4.15 事務次官等会議申合せ) 第 5 項 では、「秘密文書には、秘密にしておく期間を明記し、その期間が経過したときは、秘密の取扱いは、解除されたものとする。ただし、その期間中秘密にする必要がなくなったときは、その旨を通知して秘密の解除を行うものとする。」と定めている。

- (f) 行政事務従事者は、書面に印刷された機密性 3 情報には、一連番号を付し、その所在を明らかにしておくこと。

解説：書面に印刷された機密性 3 情報に一連番号を付与し、個別に所在管理を行うことを求める事項である。

配付時に一連番号を付与することによって、当該機密性 3 情報を受領した者に、一定の管理義務を要請する効果も期待できる。

なお、「秘密文書等の取扱いについて」(昭和 40.4.15 事務次官等会議申合せ) 第 4 項 では、「「極秘」の文書には、必ず一連番号を付し、その所在を明らかにしておくこと。」と定めている。

3.2.3 情報の保存

趣旨（必要性）

行政事務においては、その事務の継続性を確保するなどの必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。

これらのことを勘案し、本項では、情報の保存に関する対策基準を定める。

遵守事項

- (1) 格付けに応じた情報の保存

【基本遵守事項】

- (a) 情報セキュリティ責任者又は情報システムセキュリティ責任者は、電子計算機に保存された要保護情報について、適切なアクセス制御を行うこと。

解説：電子計算機に記録された情報に関して、機密性、完全性及び可用性の格付けに応じ、電子計算機の機能を活用して、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める

事項である。

電子計算機におけるアクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができる。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。

- (b) 行政事務従事者は、情報の格付けに応じて、情報が保存された外部記録媒体を適切に管理すること。

解説：外部記録媒体に記録された情報に関して、機密性、完全性及び可用性の格付けに応じて、外部記録媒体を適切に管理することを求める事項である。

例えば、機密性の格付けに応じて、外部記録媒体を施錠のできる書庫・保管庫に保存し、不正な持出しや盗難を防ぐことが考えられる。

外部記録媒体が主体認証情報（パスワード）によるロック機能を持つ場合は、アクセス制御が可能であるが、ロック機能を持たない外部記録媒体も多く、保存する情報に応じた外部記録媒体を選択する必要がある。

- (c) 行政事務従事者は、情報の格付けに応じて、情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面、及び情報システムの設計書等情報システムに係る書面を、適切に管理すること。

解説：情報を記載した書面を、機密性、完全性及び可用性の格付けに応じて管理することを求める事項である。

例えば、必要なく情報の参照等をさせないために、書面を施錠のできる書庫に保存するなどの措置が考えられる。

【強化遵守事項】

- (d) 行政事務従事者は、要機密情報を電子計算機又は外部記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めるときは、情報を暗号化すること。

解説：電子計算機又は外部記録媒体に保存された情報の機密性を確保するために、その暗号化を行うことを求める事項である。

これに加えて、情報の復号ができる者を限定することは、府省庁内において情報の機密性を高めるために有効である。また、万一 PC、ファイル又は外部記録媒体の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。

- (e) 行政事務従事者は、要保全情報及び要安定情報について、バックアップを取得すること。

解説：情報の完全性及び可用性を確保するために、バックアップの取得を求める事項である。

バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。事故に備えて適切な頻度で復元の演習も行い、行政事務従事者に習熟させる。また、災害等を想定してバックアップを取得する場合には、媒体を遠隔地に保存する必要がある。

なお、バックアップ情報を記録した媒体の紛失・盗難により情報が漏え

いするおそれがあるため、必要に応じて、その情報を暗号化することが望ましい。

(2) 情報の保存期間

【基本遵守事項】

- (a) 行政事務従事者は、電子計算機又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

解説：情報の保存期間に従って管理することを求める事項である。

行政事務従事者は、必要な期間は確実に情報を保存するとともに、その期間を経過した場合には当該情報を速やかに消去してリスクの増大を回避する必要がある。

3.2.4 情報の移送

趣旨（必要性）

行政事務においては、その事務の遂行のために情報を移送する場合があります。インターネット上での電子メール等による送信、回線接続を通じての送信並びに情報を格納した外部記録媒体及び PC、紙面に印刷された情報の運搬等の方法が用いられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。

これらのことを勘案し、本項では、情報の移送に関する対策基準を定める。

遵守事項

(1) 情報の移送に関する許可及び届出

【基本遵守事項】

- (a) 行政事務従事者は、機密性 3 情報を移送する場合には、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の許可を得ること。

解説：機密性 3 情報を移送する際に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の許可を求める事項である。

機密性 3 情報の移送は、業務上必要であると認められる場合にのみ、定められた手続きに従って許可される。

- (b) 行政事務従事者は、機密性 2 情報を移送する場合には、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に届け出ること。

解説：機密性 2 情報を移送する際に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に届け出ることを求める事項である。

機密性 2 情報の移送は、業務上必要であると認められる場合にのみ、定められた手続きに従って許可される。

(2) 情報の送信と運搬の選択

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを決定し、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に届け出ること。

解説：要機密情報の安全確保に留意した移送を求める事項である。

(3) 移送手段の選択

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報を移送する場合には、安全確保に留意して、当該要機密情報の移送手段を決定し、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に届け出ること。

解説：多種多様な移送手段の中から要機密情報を安全に移送するための手段の選択を求める事項である。

「移送手段」とは、送信については外部を経由しないネットワーク、信頼できるプロバイダ、VPN及び暗号メール(S/MIME)等、運搬については信頼できる運送業者や、情報セキュリティ責任者があらかじめ指定する運送サービス及び職員自らによる携行等が挙げられる。なお、「S/MIME (Secure Multipurpose Internet Mail Extensions)」とは、電子メールの暗号化の方式の1つである。

(4) 書面に記載された情報の保護対策

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報が記載された書面を移送する場合には、情報の格付けに応じて、安全確保のための適切な措置を講ずること。

解説：要機密情報が記載された書面を移送する場合におけるセキュリティ対策を求める事項である。

行政事務従事者は、書面を運搬する場合には、外見ではその内容が要機密情報であると知られないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。

(5) 電磁的記録媒体に記録された情報の保護対策

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めるときは、情報にパスワードを設定すること。

解説：移送手段の種別を問わず、行政事務従事者以外の者が要機密情報を容易に参照できないようにするため、パスワードによって保護することを求

める事項である。

方法としては、文書作成アプリケーションによるパスワード保護オプション及び圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。

- (b) 行政事務従事者は、要機密情報を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。

なお、暗号化された通信路を用いて情報を送信する場合は、この限りでない。

- (c) 行政事務従事者は、電子ファイルを移送する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないかを確認すること。

解説：行政事務従事者が意図せず情報を漏えいすることを防止するための事項である。

移送するファイルの「プロパティ」に個人情報が残っていたり、作成履歴が残っていたりすることがないように確認する必要がある。要機密情報に限らず、電子ファイルを移送する場合には、事前の確認を要する。

【強化遵守事項】

- (d) 行政事務従事者は、要機密情報を移送する場合には、適切な強度の暗号化を行った上で、複数の情報に分割してそれぞれ異なる移送経路を用いること。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。

3.2.5 情報の提供

趣旨（必要性）

行政事務においては、その事務の遂行のために府省庁外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがある。

これらのことを勘案し、本項では、情報の提供に関する対策基準を定める。

遵守事項

(1) 情報の公表

【基本遵守事項】

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

解説：公表すべきでない情報の公表を防止することを求める事項である。

府省庁の業務においては、保有する行政情報をホームページ等により広

く国民に提供する場合がある。この場合には、公表しようとする情報に対する格付けの適正さを再度検討し、必要に応じて格付けの変更等を行った上で、当該情報が機密性 1 情報に格付けされるものであることを確認する必要がある。なお、当該情報が法律の規定等で公表が禁じられたものでないことも確認する必要がある。

(2) 他者への情報の提供

【基本遵守事項】

- (a) 行政事務従事者は、機密性 3 情報を府省庁外の者に提供する場合には、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の許可を得ること。

解説：機密性 3 情報を府省庁外の者に提供する際に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の許可を得ることを求める事項である。

機密性 3 情報の府省庁外の者への提供は、業務上必要であると認められる場合にのみ、定められた手続きに従って許可される。

- (b) 行政事務従事者は、機密性 2 情報を府省庁外の者に提供する場合には、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に届け出ること。

解説：機密性 2 情報を府省庁外の者に提供する際に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に届け出ること求める事項である。

- (c) 行政事務従事者は、要機密情報を府省庁外の者に提供する場合には、提供先において、当該要機密情報が、自らが所属する府省庁の付した情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。

解説：要機密情報を府省庁外の者に提供する場合において遵守すべきことを定める事項である。

要機密情報を府省庁外の者に提供する場合には、提供先において当該要機密情報が適切に取り扱われるように、情報の機密性の格付けを含む取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該要機密情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。外部委託の場合には、委託先に、情報漏えいの防止と外部委託目的の範囲内での取扱いを要求し、請負契約にその内容を含め、委託先に遵守させる必要がある。

3.2.6 情報の消去

趣旨（必要性）

行政事務において利用した情報システム又は外部記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報の消去を行っていたつもりでも、適切な措置が採られていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されない。

これらのことを勘案し、本項では、情報の消去に関する対策基準を定める。

遵守事項

(1) 電磁的記録の消去方法

【基本遵守事項】

- (a) 行政事務従事者は、電子計算機、通信回線装置及び外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にすること。

解説：電子計算機、通信回線装置及び外部記録媒体を廃棄する場合に、すべての情報を復元が困難な状態にすることを求める事項である。

「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消去されずに媒体に残留した状態となっているおそれがある。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該記録媒体に記録されているすべての情報を適切な方法で復元が困難な状態にする必要がある。

- (b) 行政事務従事者は、初期化されていない電子計算機、通信回線装置及び外部記録媒体を利用する場合には、これらに保存された情報を復元が困難な状態にする必要性の有無を検討し、必要があると認めるときは、データ消去ソフトウェア又はデータ消去装置を用いて、すべての情報を復元が困難な状態にすること。

解説：初期化されていない電子計算機、通信回線装置及び外部記録媒体に保存された情報を、必要に応じて、復元が困難な状態にすることを求める事項である。

長期にわたり利用された電子計算機、通信回線装置及び外部記録媒体には、要機密情報が断片的に残留した状態となっているおそれがある。そのため、担当者間による業務の引継ぎを伴わず、別の業務に当該機器等が利用されることが想定される場合には、データ消去ソフトウェア又はデータ消去装置を利用し、すべての情報を復元が困難な状態にすることが必要である。特に、外部記録媒体を用いて府省庁外の者に情報を提供する場合には、その実施が重要である。

【強化遵守事項】

- (c) 行政事務従事者は、電子計算機、通信回線装置及び外部記録媒体について、設置環境等から必要があると認められる場合は、データ消去ソフトウェアを用いて、当該電子計算機等の要機密情報を復元が困難な状態にし、当該電子計算機等に残留する要機密情報を最小限に保つこと。

解説：無人の執務室に設置されていたり、設置場所及び利用場所が確定していない電子計算機、通信回線装置及び外部記録媒体など、安全といえない環境で利用される電子計算機等に残留する要機密情報を最小限にすることを求める事項である。

(2) 書面の廃棄方法

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報が記録された書面を廃棄する場合には、復元できない方法を用いること。

解説：電磁的記録の消去と同様に、書面に印刷された情報が不要となった場合には、シュレッダーによる細断処理、焼却又は溶解などにより、復元できない方法で廃棄することを求める事項である。

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.1 主体認証

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、本項では、主体認証に関する対策基準を定める。

なお、政府の情報システムの利用者は、行政事務従事者のほか、それ以外の者がある。例えば、国民向けのサービスを提供する情報システムの利用者は、行政事務従事者以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、行政事務従事者以外の者は本統一基準の適用範囲ではない。しかし、それらの者に対し、これを保護するよう注意喚起することが望ましい。

用語解説

- 主体認証の方式として、知識、所有、生体情報の3つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、ICカードや磁気テープカード等、本人のみが所有する機器を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。なお、本項における解説としてはそれら3つの方式について記述するが、その他、位置情報等による方式もある。
- 生体情報による主体認証を用いる場合には、その導入を決定する前に、この方式特有の誤認率と誤否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。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の行政事務の遂行への影響について検討してから導入を決定すること。
機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせるなどについて考慮するとよい。

遵守事項

(1) 主体認証機能の導入

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、すべての情報システムについて、主体認証

を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要があると判断すること。

解説：主体認証を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセスする主体の主体認証を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、主体認証を行う必要があると判断すること。

- (b) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムには、識別及び主体認証を行う機能を設けること。

解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。

- (c) 情報システムセキュリティ管理者は、主体認証を行う必要があると認めた情報システムであって、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

(ア)主体認証情報を保存する場合には、その内容の暗号化を行うこと。

(イ)主体認証情報を通信する場合には、その内容の暗号化を行うこと。

(ウ)保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。

解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。

保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、これが漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定するなどの回避策をとる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。

したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」などの警告を表示するようにすることが必要である。

- (d) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、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、以下のいずれかの機能を情報システムに設けること。

(ア)利用者が定期的に変更しているか否かを確認する機能

(イ)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

解説：定期的な変更を遵守事項とする場合には、それが実施されているか否かを確認できる機能を用意しておく必要がある。

その機能を自動化することが望ましいが、技術的に困難な場合においては、運用によって対処する必要がある。

- (e) 情報システムセキュリティ責任者は、利用者から主体認証情報又は主体認証情報格納装置を他者に使用された又は使用される危険性がある旨の報告を受けた場合には、直ちに当該主体認証情報又は主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を情報システムに設けること。

解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用などの対策を講ずること。

- (f) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムであって、知識による主体認証方式を用いる場合には、以下の機能を情報システムに設けること。

(ア)利用者が、自らの主体認証情報を設定する機能

解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の事項が改善される。

・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が記憶が容易である。

・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、本人自身が設定することにより、そのおそれが少なくなる。

なお、例えば、運用上の理由などで他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知する必要がある。

- (イ)利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

解説：情報システムセキュリティ責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。情報システムセキュリティ責任者に悪意がなくとも、仮に悪意ある者によってそのシステム管理者権限を奪取されてしまった場合に、すべての利用者の主体認証情報を知られてしまうおそれがあるため、不可逆の暗号化を用いるなどにより、情報システムセキュリティ責任者自らも、他者の主体認証情報を知ること

ができないような措置を講ずる必要がある。

- (g) 情報システムセキュリティ責任者は、主体認証を行う必要があると認められた情報システムであって、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

解説：利用者の指紋情報など、主体認証情報として生体情報を取り扱う場合に、個人のプライバシーに配慮し、個人情報として厳格な管理を求める事項である。

- (h) 情報システムセキュリティ責任者は、主体認証を行う必要があると認められた情報システムであって、知識、所有、生体情報以外の主体認証方式を用いる場合には、以下の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。

(ア) 正当な主体以外の主体を誤って主体認証しないこと。(誤認の防止)

(イ) 正当な主体が本人の責任ではない理由で主体認証できなくなるしないこと。(誤否の防止)

(ウ) 正当な主体が容易に他者に主体認証情報を付与及び貸与ができないこと。(代理の防止)

(エ) 主体認証情報が容易に複製できないこと。(複製の防止)

(オ) 情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。(無効化の確保)

(カ) 主体認証について業務遂行に十分な可用性があること。(可用性の確保)

(キ) 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)

(ク) 主体に付与した主体認証情報を使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)

解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性なども考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしもすべて充足することを求めるものではない。例えば、主体認証情報(パスワード)等による「知識」方式の場合には、要件(ウ)や(エ)を技術的に充足する必要はない。

【強化遵守事項】

- (i) 情報システムセキュリティ責任者は、複数要素(複合)主体認証方式で主体認証を行う機能を情報システムに設けること。

解説：複数要素(複合)による主体認証方式を用いることにより、より強固な主体認証が可能となる。

これは、単一要素(単一)主体認証方式(「単一要素(単一)主体認証(single factor authentication / single authentication)方式」とは、知識、

所有、生体情報などのうち、単一の方法により主体認証を行う方式である。)の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまいが、複数要素(複合)主体認証方式の場合には、仮に一方の主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログオンされる可能性は依然低いと考えられるからである。

- (j) 情報システムセキュリティ責任者は、ログオンした利用者に対して、前回のログオンに関する情報を通知する機能を情報システムに設けること。

解説：仮に、本人の識別コードが他者によって不正に使われた場合には、その識別コードによる前回のログオンに関する情報(日時や装置名等)を通知することで、本人が不正な使用に気付く機会を得られるようにする。

- (k) 情報システムセキュリティ責任者は、不正にログオンしようとする行為を検知又は防止する機能を情報システムに設けること。

解説：例えば、識別コードによるログオンにおいて、指定回数以上の主体認証情報の誤入力検知された場合に、その旨を通知する、あるいは、当該識別コードによる情報システムへの以後のログオンを無効にする(アカウントをロックする)機能の付加が挙げられる。

報告によって、本人が知る機会を得ることと、組織が状況を管理できることの2点を達成できるよう、検知又は防止した旨を報告する仕組みを設ける必要がある。

- (l) 情報システムセキュリティ責任者は、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。

解説：通知メッセージの例としては、以下のようなものがある。

- ・利用者が政府の情報システムへアクセスしようとしていること
- ・情報システムの使用が監視、記録される場合があり、監査対象となること
- ・情報システムの不正使用は禁止されており、刑法の罰則対象となること

- (m) 情報システムセキュリティ責任者は、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、以前に設定した主体認証情報と同じものを再設定することを防止する機能を情報システムに設けること。

解説：一度使用した主体認証情報(パスワードなど)の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

- (n) 情報システムセキュリティ責任者は、管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を情報システムに設けること。

解説：管理者権限を有した識別コードを管理者グループで共用した場合には、そのログオン記録だけでは、共用している管理者のうち、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。そのため、管理者個人を特定することを目的として、非管理者権限の識別コードを本人に付与した上、その識別コードで最初にログオンした後に限り、管理者権限を有する共用識別コードに切り替えて管理者作業を実施することを可能とする必要がある。

なお、当該情報システムのオペレーションシステムが Unix の場合には、一般利用者がログオンした後に 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 によるログオ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。

(2) 行政事務従事者における識別コードの管理

【基本遵守事項】

- (a) 行政事務従事者は、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。

解説：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、なりすまし行為であることを認識する必要がある。

仮に、悪意がない行為であっても、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、安易に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利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使って行おうとしている業務について、他者へ代行処理依頼することを検討すべきであり、他者の許可を得て、当該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用いて、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。また、業務の継続のために、他者の識別コードを用いることが不可避の場合には、本人の事前の了解に加えて、情報システムセキュリティ管理者の了解を得ることが最低限必要である。極めて緊急性が高い場合には、他者の識別コードを利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管理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管理者は、その理由と利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なければならない。

いずれの場合も、用い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用いて、情報システムを利用することは禁止されるべきである。

- (b) 行政事務従事者は、自己に付与された識別コードを他者に付与及び貸与しないこと。

解説：共用する識別コードについても情報システムセキュリティ管理者から各本人に個別に付与されるものであり、付与された者がそれを他者に付与、貸与してはならない。また、情報システムセキュリティ管理者が明示的

に共用識別コードとしているもの以外の識別コードを、共用してはならない。

- (c) 行政事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。

解説：ほとんどの場合には、識別コード自体は必ずしも秘密ではないが、積極的に公開したり、公然となるような放置はしないようにすることを求める事項である。

本来、主体認証のためには、主体認証情報が用いられるが、識別コード自体も秘密にすることによって、不正に主体認証される可能性をより低くすることが可能となる。そのため、識別コードについても適切に管理することが求められる。

- (d) 行政事務従事者は、行政事務のために識別コードを利用する必要がなくなった場合は、情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、あらかじめ情報システムセキュリティ責任者が定めている場合は、この限りでない。

解説：識別コードを利用する必要がなくなった場合に、行政事務従事者自らが情報システムセキュリティ管理者へ届け出ることを求める事項である。ただし、人事異動など、大規模に識別コードの行政事務従事者が変更となる場合や、その変更を情報システムセキュリティ管理者が行政事務従事者自らからの届出によらずして把握できる場合には、行政事務従事者自らの届出は不要とすることができる。

【強化遵守事項】

- (e) 管理者権限を持つ識別コードを付与された者は、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。

解説：この遵守事項は、最小特権機能（least privilege 機能）と呼ばれている。

この遵守事項は、当然のことであるが、実際には繁雑な操作をしなければいけない場合がある。

例えば、情報システムのオペレーションシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更などをしていないときには、administrator 権限なしの識別コードを使用し、設定変更をするときにだけログインしなめすということを遵守しなければならない。

なお、最小特権機能が容易に操作できるような環境を整えば、これを遵守すべきであるが、当該の情報システムで取り扱う情報の重要性などを勘案し、必要に応じて遵守事項として本事項を選択されたい。

(3) 行政事務従事者における主体認証情報の管理

【基本遵守事項】

- (a) 行政事務従事者は、主体認証情報が他者に使用され又はその危険が発生した場合

には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

解説：主体認証情報自体の露呈や主体認証情報に関連する情報の露呈又はそれが露呈した可能性がある場合には、情報システムセキュリティ責任者又は情報システムセキュリティ管理者へ報告の上、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるログオン制限などの対策を講ずること。

(b) 知識による主体認証情報を用いる場合には、当該主体認証情報について以下の要件を満たすこと。

(ア)行政事務従事者は、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こと。

解説：行政事務従事者は、例えば自己の主体認証情報を内容が分かる状態で付箋に記入して貼付する様なことを行ってはならず、主体認証情報を入力する際に周囲からの盗み見に注意を払ったり、管理者を名乗って主体認証情報を聞き出す行為に注意したりする等、他者に知られないように管理すること。

(イ)行政事務従事者は、自己の主体認証情報を他者に教えないこと。

解説：行政事務従事者が他者に処理代行させるために自己の主体認証情報を教示しないことを求める事項である。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連があいまいとなる可能性があり、アクセス制御、権限管理、証跡管理等その他の情報セキュリティ対策の基礎が崩壊する可能性がある。また、教示された側にとっても、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、「教えない」、「聞かない」を徹底すべきである。

(ウ)行政事務従事者は、主体認証情報を忘却しないように努めること。

解説：他者が容易に見ることができないような措置（施錠して保存する等）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、メモを取ることそのものを禁ずるものではない。むしろ、忘れることのないようにしなければならない。

本人の忘却によって主体認証情報を初期化（リセット）する場合に備えて、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設計・運用すべきであり、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が望ましい。

(エ)行政事務従事者は、主体認証情報を設定するに際しては、容易に推測されないものにすること。

解説：辞書に載っている単語、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。

また、使用する文字種として、数字だけでなく、アルファベットの大文字及び小文字、更に特殊記号なども織り交ぜて主体認証情報を構成することが望ましい。

(オ)行政事務従事者は、情報システムセキュリティ管理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こと。

解説：定期的な変更の要求を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することでも差し支えない。

(c) 所有による主体認証を用いる場合には、主体認証情報格納装置について以下の要件を満たすこと。

(ア)行政事務従事者は、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こと。

(イ)行政事務従事者は、主体認証情報格納装置を他者に付与及び貸与しないこと。

(ウ)行政事務従事者は、主体認証情報格納装置を紛失しないように管理すること。
紛失した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

解説：所有による主体認証方式では、それを取得した者が正当な主体として主体認証されることになるため、他者に使用されることがないように、また、紛失などで、その可能性がある場合の報告を徹底する必要がある。

4.1.2 アクセス制御

趣旨（必要性）

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本項では、アクセス制御に関する対策基準を定める。

用語解説

- アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。

http://www.bits.go.jp/inquiry/pdf/secure_os_2004.pdf

遵守事項

(1) アクセス制御機能の導入

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。

解説：アクセス制御を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセス制御を行う必要性の有無を検討しなければならない。要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。

- (b) 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムには、アクセス制御を行う機能を設けること。

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式（任意アクセス制御：DAC）を利用すること。なお、「任意アクセス制御（DAC：Discretionary Access Control）」とは、主体が客体に設定したアクセス制御について、その設定がそれ以後継承されるかが任意である方式であり、この方式では、その客体にアクセス許可されている主体が別の客体を作成し複製等する際に、元のアクセス制御を新しい客体のアクセス制御として継承するかは当該主体の任意であり、変更が可能である。

【強化遵守事項】

- (c) 情報システムセキュリティ責任者は、利用者等の属性以外に基づくアクセス制御を行う必要があると認めた情報システムには、当該アクセス制御の機能を追加すること。

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式（任意アクセス制御：DAC）を利用するほか、情報システムの利用者やそのグループの属性以外に基づくアクセス制御を追加すること。

情報システムの利用者やそのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

- ・ 利用時間による制御
- ・ 利用時間帯による制御
- ・ 同時利用者数による制限
- ・ 同一IDによる複数アクセスの禁止
- ・ IPアドレスによる端末制限

- (d) 情報システムセキュリティ責任者は、強制アクセス制御を行う必要があると認めた情報システムには、当該機能を設けること。

解説：強制アクセス制御機能(MAC)の組み込みを導入すること。

強制アクセス制御機能を備えたものとして、トラステッドOSやセキュアOSがある。

- (2) 行政事務従事者による適正なアクセス制御

【基本遵守事項】

- (a) 行政事務従事者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

解説：要機密情報であれば、不適當な者から参照されないようなアクセス制御を設定し、完全性2情報であれば、不適當な者から変更されないようなアクセス制御を設定すること。

例えば、行政事務従事者自らが作成した要機密情報をファイルに保存する際にその行政事務従事者が読取制限の属性を付与することがこれに当たる。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。情報システムが備えていない機能については、行政事務従事者が取扱上注意することで、その指示を遵守することになる。

4.1.3 権限管理

趣旨（必要性）

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、権限管理に関する対策基準を定める。

用語解説

- アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与される許可のことをいい、権限管理とは、主体に対する許可を管理することである。主体に付与する権限は、識別コードと主体認証情報である。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。

遵守事項

(1) 権限管理機能の導入

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。

解説：権限管理を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。

- (b) 情報システムセキュリティ責任者は、権限管理を行う必要があると認められた情報システムには、権限管理を行う機能を設けること。

解説：権限管理を行う機能を設ける必要があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

【強化遵守事項】

- (c) 情報システムセキュリティ責任者は、最小特権機能を情報システムに設けること。

解説：管理者権限を持つ識別コードを付与された者が、管理作業をする時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最小特権機能を、情報システムに設けることを求める事項である。

- (d) 情報システムセキュリティ責任者は、主体認証情報の再発行を自動で行う機能を情報システムに設けること。

解説：情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。

なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することにより、安全性を強化することができる。

- (e) 情報システムセキュリティ責任者は、デュアルロック機能を情報システムに設けること。

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも 2 名の者が操作しなければその行為を完遂できない方式のことである。

(2) 識別コードと主体認証情報の付与管理

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、共有識別コードの利用許可については、情報システムごとにその必要性を判断すること。

解説：原則として、識別コードは、情報システムへアクセスする主体へ個別に付与することになる。しかしながら、情報システム上の制約や、利用状況などを考慮して、1つの識別コードを複数の主体で共用する必要がある場合には、当該情報システムごとに利用許可の判断をすることを求める事項である。

- (b) 情報システムセキュリティ責任者は、権限管理について、以下の事項を含む手続きを明確にすること。
- (ア)主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続き
 - (イ)主体認証情報の初期配布方法及び変更管理手続き
 - (ウ)アクセス制御情報の設定方法及び変更管理手続き
- 解説：情報システムへアクセスする主体に対して、識別コード及び主体認証情報を付与する際の関連手続を明確に定めることを求める事項である。また、情報システムへアクセスする主体ごとに、確実にアクセス権限を設定するため、関連手続を明確に定めることを求める事項である。
- (c) 情報システムセキュリティ責任者は、権限管理を行う者を定めること。
- 解説：アクセス権限の管理については、情報システムのセキュリティ保護上、非常に重要な役割を果たすため、権限管理を行う者を定め、厳格な運用を求める事項である。
- (d) 権限管理を行う者は、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発行すること。
- 解説：情報システムにおける識別コード及び主体認証情報は、情報システムを利用する許可を得た主体に対してのみ発行することが重要である。そのため、初期付与に関する本人確認や、識別コード及び主体認証情報の初期付与方法について厳格な方法を採用することを求める事項である。
- (e) 権限管理を行う者は、識別コードを発行する際に、それが共有識別コードか、共有ではない識別コードかの区別を利用者に通知すること。ただし、共有識別コードは、情報システムセキュリティ責任者が、その利用を認めた情報システムでのみ付与することができる。
- 解説：識別コードを利用者に発行する際に共有識別コードか共有ではない識別コードかの別について通知することにより、それらの区別を利用者が独自に判断するようなことを防ぐための事項である。
- (f) 権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に則した場合に限定して付与すること。
- 解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、最小権限付与の原則に従って、管理者権限を持つ識別コードは、業務又は業務上の責務に則して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。
- (g) 権限管理を行う者は、退職等により行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者の識別コードを無効にすること。また、人事異動等の必要時に、不要な識別コードの有無を点検すること。
- 解説：識別コードの付与を最小限に維持するため、不必要となった識別コードについては、これを無効にすることを求める事項である。これは、本人による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必要がある。

- (h) 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をすること。

解説：最小権限付与の原則に従って、業務又は業務上の責務に即して、必要となる者に限り、当該者の業務遂行に必要となるアクセス権限のみを付与することを求める事項である。

【強化遵守事項】

- (i) 権限管理を行う者は、単一の情報システムにおいては、1人の行政事務従事者に対して単一の識別コードのみを付与すること。

解説：デュアルロック機能を備えた情報システムでは、1人の行政事務従事者に複数の識別コードでの主体認証を許してしまうと、デュアルロック機能による強化が万全とならないことから、1人の行政事務従事者に対して単一の識別コードのみを付与することを求める事項である。

- (j) 権限管理を行う者は、付与した識別コードをどの主体に付与していたかの記録について、保存すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。

解説：識別コードは将来の事故原因調査に備えて長期保存を原則とし、削除しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、適切な承認を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体に付与したかを知るための記録を消去してはならない。

- (k) 権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。

解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。ただし、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合など、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、識別コードを再利用しても構わないが、その際、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理すること。なお、同一の主体に対する再利用を認めるか、認めないかについては、情報セキュリティ責任者による判断に従うものとする。

(3) 識別コードと主体認証情報における代替措置の適用

【基本遵守事項】

- (a) 情報システムセキュリティ管理者は、付与した識別コードが使用できなくなった行政事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、

必要があると認めるときは、代替手段を提供すること。

解説：情報システムを利用する行政事務従事者においては、何らかの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合が想定される。例えば、知識による主体認証方式であれば主体認証情報（パスワード）を忘れた場合、所有による主体認証方式であれば携帯するのを忘れた場合、指紋による主体認証方式であれば指を怪我した場合等が挙げられる。

それらの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合には、代替手段の使用に関する許可申請をすることができる。情報システムセキュリティ管理者は、その申請を受理した時には、その申請が本人からの事前許可申請であること、申請者が正当な行政事務従事者であること及び許可申請の理由が妥当であることを確認した上で、その必要性を判断し代替手段を提供することを求める事項である。なお、代替手段としては、例えば、当日限り有効とした暫定的な識別コード及び主体認証情報の提供や、当該情報システムから切り離された代替 PC の提供、情報システムを利用しない業務環境の提供などが想定されるが、情報システムセキュリティ管理者が情報セキュリティ保護の観点に加えて行政事務従事者本人による業務執行の緊急性、効率性、利便性及び当該情報システムの可用性等も考慮して、適正な代替手段をあらかじめ準備しておくこと。

なお、代替手段の実施に当たっては、その申請理由と使用期間、使用者等を記録として残すことが望ましい。

- (b) 情報システムセキュリティ責任者及び情報システムセキュリティ管理者は、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を停止させること。

解説：不正使用の報告を受けた場合には、他の基準項目で定められている事故対応の遵守事項とともに、本事項の対応を実施する。

不正使用による被害が甚大であると予想される場合には、すべての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得すること。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行すること。

4.1.4 証跡管理

趣旨（必要性）

情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティ侵害が発生した場合に適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、ま

た事後に追跡することが可能となる。

これらのことを勘案し、本項では証跡管理に関する対策基準を定める。

遵守事項

(1) 証跡管理機能の導入

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、証跡管理を行う必要があると判断すること。

解説：証跡管理を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、証跡管理を行う必要性の有無を検討しなければならない。要保護情報を取り扱う情報システムにおいては、証跡管理を行う必要があると判断すること。

- (b) 情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

解説：利用者の行動等の事象を証跡として記録するための機能を情報システムに設けることを求める事項である。

情報セキュリティの侵害は、様々な原因で発生する。クラッカー等の部外者による不正アクセス、不正侵入、操作員の誤操作又は不正操作、府省庁の部内及び部外の情報システム利用者の誤操作又は不正操作などがその原因となる。また、職務外の目的でウェブの閲覧や電子メールの送受信がなされるおそれもある。万一侵害等が発生した場合にはその実行者を特定する必要があり、そのために不正アクセス、不正侵入等の情報セキュリティ事象、操作員及び利用者の行動を含む事象を情報システムで証跡として取得し、保存する必要がある。

証跡として多くの情報を取得すれば、事後追跡及び事前抑止の効果は高まる。その反面、多くの証跡を取得する場合には、情報システムの処理能力及び記憶容量を多く消費することになる。情報システムセキュリティ責任者は、この両面に配慮し、また情報システムの重要度や取り扱う情報の機密性も考慮して、証跡として取得する情報と、証跡を取得する箇所を決定する必要がある。

記録事項には、以下の記録を含めることが考えられる。

- ・利用者による情報システムの操作記録
- ・操作員、監視要員及び保守要員等による情報システムの操作記録
- ・ファイアウォール、侵入検知システム（Intrusion Detection System）等通信回線装置の通信記録
- ・プログラムの動作記録

- (c) 情報システムセキュリティ責任者は、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。

解説：証跡を取得する場合に、取得する情報項目を適切に選択することを求め

る事項である。

以下に示す例は一般的に取得すべき基本的な情報項目であるが、限られた情報量で実効性のある証拠を取得するように設計することが重要である。

証拠に含める情報項目の例：

- ・ 事象の主体である人又は機器を示す識別コード
- ・ 事象の種類（ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等）
- ・ 事象の対象（アクセスした URL（ウェブアドレス）、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等）
- ・ 日付、時刻
- ・ 成功、失敗の区別、事象の結果
- ・ 電子メールのヘッダ情報、通信内容
- ・ 通信パケットの内容
- ・ 操作員、監視要員及び保守要員等への通知の内容

- (d) 情報システムセキュリティ責任者は、証拠が取得できない場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。

解説：証拠の取得ができない場合及び取得できなくなるおそれがある場合に対応する機能を情報システムに設けることを求める事項である。

設けるべき機能としては、用意したファイル容量を使い切った場合に証拠の取得を中止する機能、古い証拠に上書きをして取得を継続する機能、ファイル容量を使い切る前に操作員に通知して対処をさせる機能等が考えられる。

- (e) 情報システムセキュリティ責任者は、取得した証拠に対して不当な消去、改ざん及びアクセスがなされないように、サーバ装置に取得した証拠についてはアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証拠についてはこれを適正に管理すること。

解説：不正アクセス、不正操作若しくは職務外利用又は誤操作を行った者にとって、その証拠は自己に不利益をもたらすものであることも考慮し、証拠が不当に消去、改ざんされることのないように管理することを求める事項である。

証拠は、訴訟において証拠として利用されることがある。その適切な取扱いを組織として定め、かつこれを遵守していることが、証拠に証拠力が認められる前提となることにも留意する必要がある。

また、証拠には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。

これらの理由で、証拠は、情報システムセキュリティ管理者及び操作員

を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。

【強化遵守事項】

- (f) 情報システムセキュリティ責任者は、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。

解説：取得した証跡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、その作業を自動化する機能を設けることを求める事項である。証跡は、その量が膨大になるため、証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成するなどにより、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。

- (g) 情報システムセキュリティ責任者は、セキュリティ侵害の可能性を示す事象を検知した場合は、監視要員等にその旨を即時に通知する機能を情報システムに設けること。

解説：セキュリティ侵害の可能性を示す事象が発生した場合に、迅速な対応を可能とするために、監視要員等に即時に通知する機能を設けることを求める事項である。

府省庁外からの不正侵入の可能性、府省庁における持込み PC の情報システムへの接続など、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。

(2) 行政事務従事者による証跡の取得と保存

【基本遵守事項】

- (a) 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情報システムに設けた機能を利用して、証跡を記録すること。

解説：情報システムの運用中に、利用者の行動等の事象を証跡として記録することを求める事項である。

情報システムセキュリティ管理者は、証跡を取得するために、定められた操作を行う必要がある。

- (b) 情報システムセキュリティ管理者は、取得した証跡の保存期間を定め、当該保存期間が満了する日まで保存すること。

解説：取得した証跡を適正に保存することを求める事項である。

情報システムセキュリティ管理者は、事後追跡に必要であると考えられる保存期間をあらかじめ定め、その間証跡を保存する必要がある。証跡を保存する期間は、1つの情報システムの各所で取得する証跡により異なることもあり得る。

必要な期間にわたり証跡を保存するために、当該期間に取得する証跡をすべて保有できるファイル容量としたり、証跡を適宜外部媒体に退避したりする方法がある。

なお、法令の規定により保存期間が定められている場合には、これにも従うこと。

- (c) 行政事務従事者は、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行うこと。

解説：証跡の取得ができない場合又は取得できなくなるおそれがある場合の対応を定める事項である。

これらの場合には、操作員その他の行政事務従事者は、あらかじめ定められた操作を行うことが求められる。

(3) 取得した証跡の点検、分析及び報告

【強化遵守事項】

- (a) 情報セキュリティ責任者又は情報システムセキュリティ責任者は、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ統括情報セキュリティ責任者若しくは情報セキュリティ責任者に報告すること。

解説：取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずることにより、情報セキュリティを維持し、あるいはその侵害を早期に検知することを求める事項である。

取得した証跡は、そのすべてを定期的に精査することは一般には困難であり、その一部を重点あるいは指標として点検及び分析することが有効である。重点項目の内容と証跡の量を定期的に点検し、その範囲で通常とは異なる状況が見られた場合に更に詳細な点検及び分析を行うことも考えられる。

証跡の点検、分析及び報告を支援するための自動化機能が設けられていれば、これを利用することにより、作業を効率的かつ確実に行うことができる。

情報セキュリティの侵害が特定された場合は、復旧及び再発防止のために必要な対策を採らなければならない。

- (b) 監視要員等は、セキュリティ侵害の可能性を示す事象を検知した旨の通知を受けた場合には、あらかじめ定められた措置を採ること。

解説：セキュリティ侵害の可能性を示す事象を検知した場合にこれを監視要員等に即時に通知する機能を持つ情報システムにおいて、通知を受けた監視要員等に対して、あらかじめ定められた措置を採ることを求める事項である。あらかじめ定められた措置とは、操作手順の実行、特定の者への報告等が想定される。

(4) 証跡管理に関する利用者への周知

【基本遵守事項】

- (a) 情報セキュリティ責任者又は情報システムセキュリティ責任者は、情報システム

セキュリティ管理者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明をすること。

解説：証跡の取得等について、あらかじめ情報システムセキュリティ管理者及び利用者等に対して適切な説明を行うことを求める事項である。

取得、保存する証跡には、情報システムの管理者、操作員及び利用者等の行動に関する情報が記録される。そのため、証跡を取得、保存し、事後に参照、点検、分析する可能性があることを、利用者に説明する必要がある。

4.1.6 暗号と電子署名（鍵管理を含む）

趣旨（必要性）

情報システムの利用においては、当該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に、情報の暗号化及び電子署名の付与が有効とされている。

これらのことを勘案し、本項では、暗号化及び電子署名の付与に関する対策基準を定める。

遵守事項

(1) 暗号化機能及び電子署名の付与機能の導入

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱うすべての情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

解説：暗号化を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の機密性の程度から暗号化を行う機能を付加する必要性の有無を検討しなければならない。

- (b) 情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。

解説：情報の機密性の程度から暗号化を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

- (c) 情報システムセキュリティ責任者は、要保全情報（書面を除く。以下この項において同じ。）を取り扱うすべての情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。

解説：電子署名の付与を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の完全性の程度から電子署名の付与を行う機能を付加する必要性の有無を検討しなければならない。

- (d) 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた

情報システムには、電子署名の付与を行う機能を設けること。

解説：情報の完全性の程度から電子署名の付与を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

- (e) 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の付与に用いるアルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行うこと。この際、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。なお、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。

解説：暗号化又は電子署名の付与に用いるアルゴリズムを選択するに当たっては、その暗号強度、利用条件、効率性などについて多角的な検討を行うことを求める事項である。

【強化遵守事項】

- (f) 情報システムセキュリティ責任者は、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。

解説：選択したアルゴリズムが危殆化した場合を想定し、暗号モジュールを交換可能なコンポーネントとして構成するため、設計段階からの考慮を求める事項である。そのためには、暗号モジュールのアプリケーションインターフェイスを統一しておく等の配慮が必要である。

- (g) 情報システムセキュリティ責任者は、複数のアルゴリズムを選択可能とすること。

解説：アルゴリズムが危殆化した場合に、設定画面などによって、当該アルゴリズムを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を、情報システムに設けることを求める事項である。

- (h) 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の付与に使用されるアルゴリズムのうち、少なくとも一つは電子政府推奨暗号リストの中から選択すること。

解説：行政情報システム関係課長連絡会議では、「必要とされる安全性及び信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする」こととされており、これに基づく措置を求める事項である。

- (i) 情報システムセキュリティ責任者は、選択したアルゴリズムが、ソフトウェアやハードウェアへ適切に実装されているか否かを確認すること。

解説：アルゴリズムの実装状況について確認することを求める事項である。

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ず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ず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。

- (j) 情報システムセキュリティ責任者は、暗号化された情報（書面を除く。以下この

項において同じ。)の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。

解説：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、技術的な対策などに加え、物理的対策を講ずることを求める事項である。鍵を格納する媒体が盗難され、鍵が開封されるなどしても、鍵情報が外部へ漏えいしない仕組みが必要である。

(2) 暗号化及び電子署名の付与に係る管理

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の生成手順及び有効期限を定めること。

解説：鍵の生成手順及び有効期限を定めることによって、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適正な管理を求める事項である。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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、あらかじめ鍵の生成手順や有効期限が定められている時は、安全性を検討の上、これを準用することが可能である。

- (b) 情報システムセキュリティ責任者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存媒体及び保存場所を定めること。

解説：鍵の保存媒体及び保存場所を定めることによって、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適正な管理を求める事項である。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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、あらかじめ鍵の保存媒体や保存場所が定められている時は、安全性を検討の上、これを準用することが可能である。

- (c) 情報システムセキュリティ責任者は、電子署名を付与した場合には、そ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提供すること。

解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。

通常、電子署名の付与を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性を保証するためには、府省庁の窓口での直接提供、信頼できる機関による電子証明書

の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開などの方法がある。

【強化遵守事項】

- (d) 情報システムセキュリティ責任者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップの取得方法及び鍵の預託方法を定めること。

解説：暗号化された情報の復号に用いる鍵の紛失及び消去に備え、鍵のバックアップの取得方法及び鍵の預託方法を定めることを求める事項である。例えば、復号に用いる鍵を紛失又は消去した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得し、又は信頼できる第三者へ鍵情報を預託するなどの対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。

- (e) 情報システムセキュリティ責任者は、選択したアルゴリズムの危殆化に関する情報を常時収集すること。

解説：様々な機関から提供されているアルゴリズムの危殆化に関する脆弱性情報を常に入手しておくことを求める事項である。
また、CRYPTREC 暗号技術監視委員会による発表に関心を払うことが必要である。

(3) 暗号化機能及び電子署名を付与する機能の利用

【基本遵守事項】

- (a) 行政事務従事者は、要機密情報を移送する場合又は電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めるときは、情報を暗号化すること。

解説：要機密情報を移送する場合又は電磁的記録媒体に保存する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。

- (b) 行政事務従事者は、要保全情報を移送する場合又は電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めるときは、情報に電子署名を付与すること。

解説：要保全情報を移送する場合又は電磁的記録媒体に保存する場合、その改ざんに係るリスクを勘案し、必要に応じて電子署名を付与することを求める事項である。

- (c) 行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵を付与された場合には、これを他者に知られないように自己管理すること。

解説：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が露呈した場合、暗号化された情報の漏えいや電子署名の偽造などのおそれがある。そのため、行政事務従事者による鍵情報の保護を求める事項である。

- (d) 行政事務従事者は、暗号化された情報の復号に用いる鍵を付与された場合には、そのバックアップを取得すること。

解説：暗号化された情報の復号に用いる鍵について、行政事務従事者によるバックアップの取得を求める事項である。バックアップ用の鍵は、通常使用する鍵が保存されている電磁的記録媒体とは異なる電磁的記録媒体に保存し、安全に保管する必要がある。

4.2 情報セキュリティについての脅威

4.2.1 セキュリティホール対策

趣旨（必要性）

セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置に存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、ウイルス感染等の脅威の発生原因になるなど、情報システム全体のセキュリティの大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、政府の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対応は迅速かつ適切に行わなければならない。

これらのことを勘案し、本項では、セキュリティホールに関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の機種並びに当該電子計算機及び通信回線装置が利用しているオペレーティングシステム、ソフトウェア又はファームウェア等の種類及びバージョンに関する書面を整備すること。

解説：公開されたセキュリティホール情報との対応付けをするため、電子計算機及び通信回線装置等を特定しておくことを求める事項である。

- (b) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の構築又は運用開始時に公開されたセキュリティホールの対策を実施すること。

解説：電子計算機及び通信回線装置の構築又は運用開始時に、その時点でのセキュリティホール対策が完了していることを求める事項である。

【強化遵守事項】

- (c) 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は、要安定情報を取り扱う情報システムについては、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。

解説：セキュリティホール対策を実施する際に電子計算機及び通信回線装置を停止する場合に、サービス提供を中断させないための措置を求める事項である。

サービス提供を中断できない情報システムでは、電子計算機及び通信回線装置を冗長構成にすることで、セキュリティ対策を実施する際の可用性を高めることが必要である。

- (d) 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は、セキュリティホールが公開されていない段階においても電子計算機及び通信回線装置上で

その対策を実施すること。

解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。

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が挙げられる。

(2) 情報システムの運用時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機及び通信回線装置の機種並びに当該電子計算機及び通信回線装置が利用しているオペレーティングシステム、ソフトウェア又はファームウェア等の種類及びバージョンに変更があった場合には、関連する書面を更新すること。

解説：公開されたセキュリティホール情報との対応付けをするため、電子計算機及び通信回線装置等を特定した情報の最新化を求める事項である。

- (b) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、管理対象となる電子計算機及び通信回線装置等に関連する公開されたセキュリティホールの情報を適宜入手すること。

解説：セキュリティホール情報の収集を求める事項である。

自動アップデート機能を持つオペレーティングシステム又はソフトウェアの場合には、当該機能を利用して、定期的にセキュリティホール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、当該機能がない場合は、適時調査を行う必要がある。

- (c) 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は、入手したセキュリティホール情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。

(ア)対策の必要性

(イ)対策方法

(ウ)対策方法が存在しない場合の一時的な回避方法

(エ)対策方法又は回避方法が情報システムに与える影響

(オ)対策の実施予定

(カ)対策テストの必要性

(キ)対策テストの方法

(ク)対策テストの実施予定

解説：セキュリティホールが情報システムにもたらすリスクを分析し、対策計画の作成を求める事項である。

「対策テスト」とは、セキュリティホール対策の実施による情報システムへの影響の有無について、他の情報システムを用いて試験することをいう。

- (d) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

解説：セキュリティホール対策計画に基づいて対策が実施されることを求める事項である。

- (e) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者等を記録すること。

解説：セキュリティホール対策の実施記録の様式は問わないが、実施日、実施内容及び実施者は必ず記録しなければならない必須事項である。これらの事項のほかに必要事項があれば、適宜追加する。

- (f) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、信頼できる方法で対策用ファイルを手に入れること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮し、対策用ファイルを信頼できる方法で入手することを求める事項である。

対策としては、ソフトウェアの開発元等が公開するウェブサイトからのダウンロード又は郵送された媒体を利用して入手する方法が挙げられる。また、改ざんなどについて検証することができる手段があれば、これを実行する必要がある。

【強化遵守事項】

- (g) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

解説：電子計算機及び通信回線装置上のセキュリティホール対策及びソフトウェア構成の状況を確認し、対策を担保するための事項である。

「セキュリティホール対策及びソフトウェア構成」とは、導入及び利用されているソフトウェアの種類、当該ソフトウェアの設定のことである。調査の間隔については、短いほど効果が高いため、可能な範囲で短くすることが望ましい。「不適切な状態」とは、パッチが適用されていない等、セキュリティホール対策が講じられていない状態のことである。

- (h) 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は、入手したセキュリティホール情報及び対策方法に関して、他の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と共有すること。

解説：公開されたセキュリティホール情報の入手及びセキュリティホール対策を効果的に実施するために、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間の連携を求める事項である。

4.2.2 不正プログラム対策

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報（パスワード）等の秘密情報や業務上の機密情報を漏えいさせることから機密性に対する脅威ともなる。

さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、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危険性など他者に対するセキュリティ脅威の原因となり得る。

これらのことを勘案し、本項では、不正プログラムに関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

- (a) 情報セキュリティ責任者は、不正プログラム感染の回避を目的とした行政事務従事者に対する留意事項を含む日常的实施事項を定めること。

解説：日常的に不正プログラム対策のために実施する事項の明文化を求める事項である。

「行政事務従事者に対する留意事項」とは、アンチウイルスソフトウェア等が現存する不正プログラムをすべて検知できるとは限らないため、行政事務従事者に対して注意喚起を行う事項であり、例えば、差出人が不明な電子メールに添付された不審なファイルを実行しないこと、ウェブクライアントのセキュリティ設定を不必要に低下させないこと、不審なホームページを閲覧しないこと等である。

「日常的实施事項」とは、不正プログラムに関する情報の収集やアンチウイルスソフトウェア等による不正プログラムの検出等が挙げられる。これらの事項については、不正プログラム対策の実施単位ごとに定めることが原則であるが、複数の不正プログラム対策の実施単位において共通して運用できる場合には、複数の実施単位で内容を整備する等状況に応じていずれかの方法を選択することが可能である。

- (b) 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は、電子計算機にアンチウイルスソフトウェア等を導入すること。

解説：不正プログラム感染の経路となる可能性が高い電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。

なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない端末については、不正プログラムが送り込まれることは実質的にないため、本事項は適用されない。

- (c) 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は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。

解説：電子計算機以外に感染経路となり得るものにおいても、不正プログラム対策の適切な実施を求める事項である。

不正プログラムの感染経路には、電子メール、ウェブ装置等のネットワークのほか、不正プログラムに感染した電子記録媒体も考えられ、複数の感染経路を想定した適切な対策が必要である。

【強化遵守事項】

- (d) 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は、想定される不正プログラムの感染経路において、異なる業者のアンチウイルスソフトウェア等を組み合わせ、導入すること。

解説：複数の業者のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。

アンチウイルスソフトウェア等は、製品ごとに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、これらは現存するすべての不正プログラムを検知及び除去できるとは限らず、アンチウイルスソフトウェア等の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が発生する可能性を低減させるため、感染経路において複数の製品や技術を組み合わせ、どれか1つの不具合で、その環境のすべ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必要がある。

- (e) 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は、不正プログラムが通信により拡散することを防止するための対策を実施すること。

解説：不正プログラムが短時間かつ大規模に感染を拡大する場合には通信を利用することが多いため、その防止策の導入を求める事項である。

不正プログラム定義ファイル又はパッチ適用等が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情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。

(2) 情報システムの運用時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、行政事務従事者にその対処の実施に関する指示を行うこと。

解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。

「特段の対処が必要な場合」とは、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アンチウイルスソフトウェア等に用いる定義ファイルが配布されないなど、日常から行われている不正プログラム対策では対応が困難と判断される場合が挙げられる。

- (b) 行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

解説：不正プログラムに感染したソフトウェアを実行した場合には、他の情報システムへ感染を拡大させることがなくても、復旧に労力を要するため、不正プログラムとして検知される実行ファイル等の実行を禁止する事項である。

- (c) 行政事務従事者は、アンチウイルスソフトウェア等にかかわ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こと。

解説：アンチウイルス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最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。

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。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。

また、最新の状態に維持する方法としては、端末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、情報セキュリティ責任者が適切な方法を選択すること。同様に(e)～(h)の事項は、情報セキュリティ責任者が適切な方法を選択すること。

- (d) 行政事務従事者は、アンチウイルス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こと。

解説：人為による対策の漏れや遅れを回避するために、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を求める事項である。

ファイルの作成、参照等のたびに検査を自動的に行う機能をオンに設定し、その機能をオフにしないことが必要である。

- (e) 行政事務従事者は、アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

解説：定期的に不正プログラムの有無を確認することを求める事項である。

前事項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定義ファイル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、定期的にすべての電子ファイルを検査する必要がある。

- (f) 行政事務従事者は、外部からデータやソフトウェアを電子計算機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、必ず不正プログラム感染の有無を確認すること。

解説：外部とやり取りするデータやソフトウェアには、ウェブの閲覧やメールの送受信等のネットワークを経由したもののほか、USB メモリや CD-ROM 等の外部記録媒体によるものも含む。

不正プログラムの自動検査による確認ができていればそれで差し支えない。

- (g) 行政事務従事者は、ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

解説：例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの感染を防ぐ、といった個別のアプリケーションごとに設定することが可能な不正プログラム感染の予防に役立つ措置の実施を求める事項である。オペレーティングシステムに不正プログラムに対応する機能がある場合には、当該機能を利用しても差し支えない。

- (h) 情報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、その見直しを行うこと。

解説：定期的に不正プログラム対策状況を把握し、問題点が発見された場合は改善することを求める事項である。

【強化遵守事項】

- (i) 情報セキュリティ責任者は、アンチウイルスソフトウェア等では検知されない新種の不正プログラムに感染した等、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくこと。

解説：新種の不正プログラム等に対応した不正プログラム定義ファイルがアンチウイルスソフトウェア等の製造業者からこれらが提供されるより前に、不正プログラムに感染した場合等において、外部から支援を受けられるように準備しておくことを求める事項である。

4.2.3 サービス不能攻撃対策

趣旨（必要性）

インターネットを経由して外部に提供しているサービスを実現するサーバ装置等は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。また、インターネットに接続しているサーバ装置及び端末は、ウイルス感染又は不正侵入等により、管理者が意図しないにもかかわらず他者へサービス不能攻撃を行ってしまうおそれがある。

このため、インターネットに接続しているサーバ装置等については、高い可用性を維持

するための対策が必要となる。

これらのことを勘案し、サービス不能攻撃に関する対策基準を定める。

遵守事項

(1) 電子計算機、通信回線装置及び通信回線がインターネットからのアクセスを受ける情報システムの構築時

【基本遵守事項】

(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については、サービス提供に必要とするサーバ装置及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

解説：サーバ装置や通信回路装置が設けている機能を有効にすることを求める事項である。

対策としては、サーバ装置における SYN Cookie、通信回線装置における SYN Flood 対策機能等を有効にすること等が挙げられる。

【強化遵守事項】

(b) 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、通信回線装置や通信回線を共用している他サービスや内部からインターネットへのアクセスにも影響を及ぼすことを考慮して通信回線装置及び通信回線の構築を行うこと。

解説：管理する情報システムと通信回線装置や通信回線を共有している他の情報システムとの関係も考慮した上で、サービス不能攻撃の影響を分析し、通信回線装置、通信回線の構築を行うことを求める事項である。

(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電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法を定めること。

解説：サービス不能攻撃に関する監視対象の特定と監視方法の整備を求める事項である。

インターネットからアクセスされるサーバ装置、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サーバ装置、通信回線装置及び通信回線を優先的に監視する必要がある。また、不正プログラムの感染又は不正侵入等を受けることにより、管理する電子計算機から他者にサービス不能攻撃を行ってしまうおそれがあるため、当該電子計算機等を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、負荷の定量的な把握があり、サービス不能攻撃を行わされることに関する監視には、電子計算機からインターネットへの通信の監視のほか、電子計算機にサービス不能攻撃を行わせる命令の有無の監視がある。監視方法は多種多様であるため、適切な方法を選択する必要がある。

(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情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響

を排除又は低減する対策装置を導入すること。

解説：電子計算機及び通信回線装置における対策については、ソフトウェアの脆弱性を悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除又は低減するために必要な装置の導入を求める事項である。

- (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については、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。

解説：大量のアクセスによる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における対処を効果的に実施するための事項である。

例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、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に設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意することなどが挙げられる。

- (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については、サービス提供に必要な電子計算機、通信回線装置及び通信回線を冗長構成にすること。

解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置及び代替回線に切り替えることにより、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を求める事項である。

サービス不能攻撃の検知及び代替計算機等への切り替えは短時間にできるようにすることが必要である。

- (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情報システムについては、サービスを提供しているサーバ装置や通信回線装置だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を定めておくこと。

解説：情報システムセキュリティ責任者が、サービス不能攻撃の対策を実施しても、政府部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、政府部外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備すること。

- (2) 電子計算機及び通信回線がインターネットからのアクセスを受ける情報システムの運

用時

【強化遵守事項】

- (a) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

解説：電子計算機、通信回線装置及び通信回線の通常時の状態を記録し把握することを求める事項である。

電子計算機、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、季節変動を検討した上で記録を一定期間保存する。

- (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、前事項の記録をサービス不能攻撃の検知精度向上等に反映すること。

解説：前事項で把握した情報をサービス不能攻撃による異常発生の検知精度向上及び検知時間の短縮等に活用することを求める事項である。

- (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、定期的にサービス不能攻撃の対策の見直しを行うこと。

解説：サービス不能攻撃の動向や電子計算機等への対策を運用した結果に応じて、定期的に対策を見直すことを求める事項である。

第5部 情報システムについての対策

5.1 施設と環境

5.1.1 電子計算機及び通信回線装置を設置する安全区域

趣旨（必要性）

電子計算機及び通信回線装置の設置環境について、悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる状況においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざんが行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等おそれもある。

これらのことを勘案し、本項では、安全区域に関する対策基準を定める。

遵守事項

(1) 立入り及び退出の管理

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。

解説：安全区域への不審者の立入りを防止し、安全区域のセキュリティを確保するための事項である。

措置としては、身分を確認できる物の提示の義務化、安全区域の所在の表示の制限等が挙げられる。

【強化遵守事項】

- (b) 情報システムセキュリティ責任者は、安全区域をセキュリティレベルが異なる区域から物理的に隔離し、立入り及び退出が可能な場所を制限する措置を講ずること。

解説：安全区域を壁及び施錠することが可能な扉等によりセキュリティレベルが異なる区域から隔離し、安全区域へ立ち入る者の主体認証を行うことが可能な管理された箇所からのみ立入り及び退出できるようにするための事項である。

- (c) 情報システムセキュリティ責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。

解説：安全区域へ立ち入る者の主体認証を実施することで、許可されていない者の立入りを排除するための事項である。

なお、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等が望ましい。

- (d) 情報システムセキュリティ責任者は、安全区域から退出する者の主体認証を行うための措置を講ずること。

解説：立ち上がった者の退出を把握するための事項である。

- (e) 情報システムセキュリティ責任者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。

解説：安全区域の立入り及び退出時における主体認証を確実に実施するための事項である。

対策としては、1人ずつでない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。

- (f) 情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を承認する手続きを整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載した書面を整備すること。

解説：書面を整備することで、安全区域へ継続的に立ち入る者を把握するための事項である。

- (g) 情報システムセキュリティ責任者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の書面へ反映させること。また、当該変更の記録を保存すること。

解説：変更の内容を前事項の書面へ反映することで安全区域へ継続的に立ち入る者を把握するための事項である。

また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。

- (h) 情報システムセキュリティ責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。

解説：安全区域への立入り及び当該区域からの退出の記録、監視を行い、安全区域のセキュリティが侵害された際に追跡することができるようにするための事項である。

「記録し及び監視する」とは、警備員又は監視カメラ等による記録及び監視のほか、安全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。

(2) 訪問者及び受渡業者の管理

【強化遵守事項】

- (a) 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。

解説：訪問者の身元を確認するための事項である。

確認方法としては、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。

- (b) 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問

者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。

解説：訪問記録の作成を求める事項である。

- (c) 情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の行政事務従事者が訪問者の安全区域への立入りについて承認するための措置を講ずること。

解説：訪問者の安全区域への立入りについて、訪問相手の行政事務従事者の承認を得る仕組みを整備することを求める事項である。

承認を得る方法としては、「警備員等が訪問相手の行政事務従事者に連絡し、訪問者の立入りについて承認を得る」、「訪問相手の行政事務従事者が、安全区域との境界線まで迎えに行き承認する」等の方法が挙げられる。

- (d) 情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。

解説：訪問者が許可されていない区域へ立ち入らないようにすることを求める事項である。訪問者に主体認証情報格納装置は貸与しない及び貸与する場合には最小限の権限を持った装置とする方法等が挙げられる。

- (e) 情報システムセキュリティ責任者は、安全区域内において訪問相手の行政事務従事者が訪問者に付き添うための措置を講ずること。

解説：訪問者が許可されていない区域へ立ち入らないように行政事務従事者が監視することを求める事項である。

- (f) 情報システムセキュリティ責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。

解説：継続的に立入りが許可された者と訪問者を区別するための事項である。

これにより、許可されていない区域への訪問者の立入りが検知できる。

対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。

- (g) 情報システムセキュリティ責任者は、訪問者の立入りを監視するための措置を講ずること。

解説：訪問者の立入りの監視を行うことで、安全区域のセキュリティが侵害された際に追跡することができるようにするための事項である。

対策としては、警備員又は監視カメラ等による記録及び監視すること等が挙げられる。

- (h) 情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。
- (ア)安全区域外で受渡しを行うこと。
 - (イ)業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、電子記録媒体、書面に触れることができない場所に限定し、行政事務従事者が立ち会うこと。
- 解説：安全区域内の行政事務従事者と物品の受渡しを行う業者の立入りを制限するための事項である。

(3) 電子計算機及び通信回線装置のセキュリティ確保

【強化遵守事項】

- (a) 情報システムセキュリティ責任者は、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。
- 解説：他の情報システムと共用の安全区域に設置した場合であって、セキュリティが確保できないときに、物理的に隔離することを求める事項である。
- (b) 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情報システムについては、設置及び利用場所が確定している電子計算機及び通信回線装置を所定の設置場所から移動できない措置を講ずること。
- 解説：設置場所が固定された電子計算機及び通信回線装置に関して、盗難及び行政事務従事者による不当な持出しを防止するための事項である。
- 「設置及び利用場所が確定している」とは、サーバ装置及び据え置き型PCのように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。
- 対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠等が挙げられる。
- (c) 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情報システムについては、安全区域内で利用するモバイルPCの盗難を防止するための措置を講ずること。
- 解説：モバイルPCは容易に持ち運びできるため、安全区域内で利用する場合、盗難を防止するための措置を求める事項である。
- 対策としては、セキュリティワイヤーによる固定又は利用しない場合には施錠することが可能な保管庫への保存等が挙げられる。
- (d) 情報システムセキュリティ責任者は、行政事務従事者が離席時に電子計算機及び通信回線装置を不正操作及び盗み見から保護するための措置を講ずること。
- 解説：行政事務従事者の離席時に、第三者に電子計算機及び通信回線装置を不正操作や盗み見から保護するための事項である。
- 対策としては、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証

情報格納装置を事務室の主体認証にも利用する方法等が挙げられる。

- (e) 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については、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。

解説：電子計算機に接続されたディスプレイ、通信回線装置のメッセージ表示用ディスプレイ等を許可のない第三者に見られないように対策を実施することを求める事項である。

対策としては、偏光フィルタの利用等が挙げられる。

- (f) 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情報システムについては、情報システムで利用する電源ケーブル又は通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。

解説：電源ケーブルの損傷又は通信ケーブルからの通信の盗聴等の脅威から、情報システムを保護するための事項である。

対策としては、ケーブルの床下への埋設、ケーブルのナンバリング等が挙げられる。

- (g) 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については、電磁波による情報漏えい対策の措置を講ずること。

解説：ディスプレイケーブル等から生じる電磁波による情報漏えい等のリスクについて対策を講ずるための事項である。

具体的には、電磁波軽減フィルタの利用等が挙げられる。

(4) 安全区域内のセキュリティ管理

【基本遵守事項】

- (a) 行政事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。

解説：安全区域への立入りを許可されていることを外見上判断できるようにするための事項である。

【強化遵守事項】

- (b) 行政事務従事者は、情報システムセキュリティ責任者の承認を得た上で、情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。

解説：情報システムに関連する物品の持込み及び持出しによって生ずるリスクに対応するための事項である。

「情報システムに関連する物品」とは、安全区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電子記録媒体及び情報システムから出力された書面等が含まれる。

- (c) 情報システムセキュリティ責任者は、安全区域への持込み及び安全区域からの持出しについて、持込み及び持出しをした者、日時、物品及び事由を含む事項について記録すること。

解説：情報システムに関連する物品の持込み及び持出しを記録し、追跡性を確

保するための事項である。

- (d) 情報システムセキュリティ責任者は、情報システムに関連しない電子計算機、通信回線装置、電子記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。

解説：情報漏えいの原因となる可能性のある電子計算機、通信回線装置、電子記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の持込みを制限するための事項である。

- (e) 行政事務従事者は、要保護情報を含む電子記録媒体及び書類については、机上に放置したままで、離席しないこと。

解説：机上に放置した電子記録媒体及び書類の盗難及び紛失を防止するための事項である。

電子計算機等は、固定又は施錠して管理することとされているので、その内蔵記録媒体には本事項は適用されない。

- (f) 情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。

解説：安全区域での作業を監視するための事項である。

第三者による立会いや、監視カメラの導入などが挙げられる。

(5) 災害及び障害への対策

【強化遵守事項】

- (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については、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。

解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。

対策としては、サーバラックの利用のほか、ハロゲン化物消火設備、無停電電源装置等の設備、空調設備、耐震又は免震設備、非常口及び非常灯等の設置又は確保が挙げられる。

- (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、安全区域内において災害及び障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

解説：作業する者が災害等により安全区域内に設置された電子計算機及び通信回線装置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電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。

5.2 電子計算機

5.2.1 電子計算機共通対策

趣旨（必要性）

電子計算機の利用については、ウイルス感染や不正侵入等を受けるなどの外部的要因により、保存されている情報の漏えい若しくは改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、職員の不適切な利用などの内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを含む。

これらのことを勘案し、本項では、電子計算機に関する対策基準を定める。

遵守事項

(1) 電子計算機の設置時

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。

解説：電子計算機に関する対策について定めることを求める事項である。

「電子計算機のセキュリティ維持に関する規定」とは、主体認証、アクセス制限及び情報システムの保守に関する目的、対象とする機器の範囲、管理する行政事務従事者及び利用者の役割及び責任のほか、端末の利用許可、モバイルPCの持出許可、利用者の識別コードの管理方法及び主体認証情報の管理方法並びに接続可能通信回線及びセキュリティ設定等の手順を整備する規定である。情報システムセキュリティ責任者の所管する単位ごとに規定を整備することが原則であるが、当該規定の内容を変更する必要がない場合には複数の実施単位で共通に整備する等状況に応じていずれかの方法を選択することが可能である。

- (b) 情報システムセキュリティ責任者は、すべての電子計算機に対して、電子計算機を管理する行政事務従事者及び利用者の特定制の文書を整備すること。

解説：電子計算機の管理状況の確認等を容易にするとともに、盗難又は紛失等を防止する責任の所在を明確にすることにより、適切な管理に対する行政事務従事者の意識向上を図ることを目的とした事項である。

- (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電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見直しを含め検討し、確保すること。

解説：通常の運用において十分な能力を確保することを求める事項である。

例えば、電子計算機の負荷に関して事前に見積もり、テスト等を実施し、必要となる処理能力及び容量を想定し、それを備える。また、将来にわたっても十分な性能を確保できるように、余裕を持たせておく必要がある。

- (d) 情報システムセキュリティ責任者は、利用者が電子計算機にログオンする場合には主体認証を行うように電子計算機を構成すること。ただし、識別コードを複数の利用者と共有することにつき合理的な理由がある場合であって、情報システムセキュリティ責任者の承認を得たとき、及び主体認証機能を付加できない端末の場合であって、利用者が電子計算機を専有するときは、この限りでない。

解説：電子計算機を利用した者を特定するために行う事項である。

サーバ装置及び複数者で利用する共有PC等の端末の場合でも利用者に識別コードを個別に割り当て、各識別コードに対応する主体認証情報（パスワード）を用いた主体認証等、本人性を確認することが可能な主体認証技術を用いる必要がある。

- (e) 情報システムセキュリティ責任者は、ログオンした利用者の識別コードに対して、権限管理を行うこと。

解説：識別コードごとに必要となる権限のみを付与することを求める事項である。管理者権限は、最小限の識別コードに与える必要がある。

- (f) 情報システムセキュリティ責任者は、電子計算機上で動作するオペレーティングシステム及びアプリケーションに存在する公開されたセキュリティホールから電子計算機を保護するための対策を講ずること。

解説：セキュリティホール対策を行うことで、電子計算機のセキュリティが確保された状態にするための事項である。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、公開されたセキュリティホールがまれにしか報告されないものもあるが、これらについても、公開されている通信プロトコルに関してセキュリティホールが報告された場合等においては、これと関連するソフトウェアに関して措置を講ずる必要がある。

当該オペレーティングシステム及びアプリケーションを搭載していない端末については、セキュリティホールが報告されることはないため、本事項は適用されない。

- (g) 情報システムセキュリティ責任者は、攻撃者により送り込まれる公開された不正プログラムから電子計算機を保護するための対策を講ずること。

解説：ウイルス及びワーム等の不正プログラムから電子計算機を保護するための事項である。

セキュリティホール対策だけでなく、アンチウイルスソフトウェア等の導入等を実施する必要がある。

多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない端末については、不正プログラムが送り込まれることは実質的にないため、本事項は適用されない。

- (h) 情報システムセキュリティ管理者は、電子計算機関連文書を整備すること。

解説：電子計算機と関連文書の整合性を確保するための事項である。

「電子計算機関連文書」とは、電子計算機的设计書、仕様書及び操作マ

ニユアル等である。書面ではなく電子記録媒体で整備していても差し支えない。

- (i) 情報システムセキュリティ責任者は、電子計算機を安全区域に設置すること。ただし、情報セキュリティ責任者の承認を得た場合は、この限りでない。

解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。

人為的な脅威としては建物内への侵入、利用者による誤操作、失火による火災又は停電等があり、環境的脅威としては地震、落雷又は風害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。

- (j) 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、サービス提供に必要な電子計算機を冗長構成にすること。

解説：障害等によりサービスを提供できない状態が発生した場合、サービスを提供する電子計算機を代替電子計算機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を求める事項である。

(2) 電子計算機の運用時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。

解説：整備された規定に従った運用管理を行い独断で運用管理を実施しないことを求める事項である。

運用管理は専用のアプリケーションを利用しても差し支えない。

- (b) 情報システムセキュリティ責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。

解説：電子計算機のセキュリティ対策を適宜見直すことを求める事項である。

セキュリティ対策は、想定するリスクに対して実施するため、時間の経過によりリスクが変化すれば、その見直しが必要になる。

- (c) 行政事務従事者は、行政事務の遂行以外の目的で電子計算機を利用しないこと。

解説：電子計算機を業務目的以外に利用することを禁止する事項である。

政府機関が所管する電子計算機への不正アクセスを禁止する意味を含んでいる。

- (d) 情報システムセキュリティ責任者は、電子計算機を管理する行政事務従事者及び利用者を変更した場合には、当該変更の内容を、電子計算機を管理する行政事務従事者及び利用者を特定するための文書へ反映すること。また、当該変更の記録を保存すること。

解説：電子計算機を管理する行政事務従事者及び利用者を変更した場合に、現

状を反映するように管理することを求める事項である。

また、変更に関して記録を残し、後で参照できるようにしておく必要がある。

- (e) 情報システムセキュリティ責任者は、電子計算機のセキュリティレベルを維持するため、公開されたセキュリティホールから電子計算機を保護するための対策を講ずること。

解説：電子計算機の運用中に公開されたセキュリティホールに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。

例えば、対策としては、公開されたセキュリティホールに対処するための対策計画の検討及び実施を意味し、対策計画を検討する初期の段階では、「直接解決する対策方法がないため代替案を実施する」、「リスクが大きくないので対策しない」といった計画で差し支えない。その判断は各実施単位に委ねられる。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、公開されたセキュリティホールがまれにしか報告されないものもあるが、これらについても、公開されている通信プロトコルに関してセキュリティホールが報告された場合等においては、これと関連するソフトウェアに関して対処する必要がある。

オペレーティングシステム及びアプリケーションを搭載していない端末については、セキュリティホールが報告されることはないため、本事項は適用されない。

- (f) 情報システムセキュリティ責任者は、電子計算機のセキュリティレベルを維持するため、攻撃者により送り込まれる公開された不正プログラムから電子計算機を保護するための対策を講ずること。

解説：電子計算機の運用中に公開された不正プログラムに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。

対策とは、不正プログラム対策の責任体制の整備、アンチウイルスソフトウェア等を利用した対策等を意味する。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、公開された不正プログラムがまれにしか報告されないものもあるが、報告された場合等においては、これと関連するソフトウェアに関して対処する必要がある。

- (g) 情報システムセキュリティ管理者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

解説：情報システムセキュリティ管理者が行った変更の内容を適宜関連文書に反映することで、電子計算機と関連文書の整合性を確保するための事項である。

【強化遵守事項】

- (h) 情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されているすべ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電子計算機を検出した場合には、当該不適切な状態の改善を図ること。

解説：電子計算機で利用されているソフトウェアのセキュリティホールの対処状況及び不正なソフトウェアの存在確認等を定期的に調べ、対処がなされていない場合にその改善を図ることを求める事項である。「定期的」とは、1ヶ月から6ヶ月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。

- (i) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、情報システムにおいて基準となる時刻に、すべての電子計算機の時刻を同期すること。

解説：情報システム内で同期されている基準となる時刻に、すべての電子計算機の時刻を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

(3) 電子計算機の運用終了時

【基本遵守事項】

- (a) 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電子計算機については、電子計算機の運用を終了する場合に、データ消去ソフトウェア又はデータ消去装置の利用、若しくは物理的な破壊又は磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にすること。

解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電子記録媒体から、すべての情報を復元が困難な状態にすることを求める事項である。

「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消去されずに媒体に残留した状態となっておりおそれがある。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電子記録媒体に保存されているすべての情報を適切な方法で復元が困難な状態にする必要がある。

5.2.2 端末

趣旨（必要性）

端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失によるウイルス感染等のリスクが高い。また、可搬性の高いものについては、紛失又は盗難のリスクも高くなる。

このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報

セキュリティが損なわれるリスクを含有する。

これらのことを勘案し、本項では、端末に関する対策基準を定める。

遵守事項

(1) 端末の設置時

【基本遵守事項】

- (a) 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は、端末にインストールしてはならないソフトウェアを定めること。

解説：ソフトウェアをインストールすることによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、端末で利用するソフトウェアを制限することを求める事項である。

インストールしてはならないソフトウェアを定める方法には、インストールしてはならないソフトウェアを列挙する方法、インストールしてよいソフトウェアを列挙する方法及びその両者を列挙する方法等があり、状況に応じた適切な方法を選択することが可能である。

- (b) 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は、要保護情報を取り扱うモバイル PC については、府省庁外で使われる際にも、府省庁内で利用される端末と同等の保護手段が有効に機能するように構成すること。

解説：府省庁外で利用されるモバイル PC は、府省庁内で利用される端末と異なる条件下に置かれるため、府省庁外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。

例えば、モバイル PC を管理する組織が運用する通信回線で実施されているアクセス制御及び監視等は、保護手段の異なる通信回線では同等に実施されているとは限らないため、モバイル PC ごとに実施する必要がある。

- (c) 行政事務従事者は、モバイル PC を利用する必要がある場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の承認を得ること。

解説：モバイル PC には様々なセキュリティ上のリスクが考えられるため、不必要なモバイル PC を増やさないための事項である。

- (d) 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は、要機密情報を取り扱うモバイル PC については、内蔵記録媒体に保存される情報の暗号化を行う機能を付加すること。

解説：モバイル PC が物理的に外部の者の手に渡った場合には、モバイル PC から取り外された内蔵記録媒体が他の電子計算機に取り付けられることによって情報が読み取られる危険性がある。このような情報漏えいの対策の手段について、モバイル PC を利用する行政事務従事者が使えるように、端末に装備することを求める事項である。

【強化遵守事項】

- (e) 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は、行政事務従事者が情報を保存できない端末を用いて情報システムを構築すること。

解説：端末から情報が漏えいすることを防ぐために、内蔵記録媒体又は外部記録媒体を装備しない端末を利用することを求める事項である。

端末に情報が保存できないことから、通信回線を経由して他の記録媒体に保存することになるため、その際に経由する通信回線、通信回線装置及び当該記録媒体に対してセキュリティ対策が必要となる。

(2) 端末の運用時

【基本遵守事項】

- (a) モバイル PC を利用する行政事務従事者は、要保護情報を取り扱う情報モバイル PC については、盗難防止措置を行うこと。

解説：モバイル PC は容易に搬出することが可能なため盗難又は紛失に遭う可能性が高いことから、その対策についてモバイル PC を利用する行政事務従事者に求める事項である。

対策としては、府省庁内においては、モバイル PC を安全区域内に設置している場合においても固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤー等をつなぐことや、帰宅時に施錠できるキャビネットに保存すること等、府省庁外においては、常に身近に置き目を離さないこと等が挙げられる。

- (b) 行政事務従事者は、要機密情報を取り扱うモバイル PC については、モバイル PC を府省庁外に持ち出す場合に、当該モバイル PC の内蔵記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めるときは、情報を暗号化すること。

解説：モバイル PC の盗難により保存されている情報が漏えいすることを防ぐため、ハードディスク内の情報に対してファイル又はハードディスク全体を暗号化する必要性を検討すること。府省庁外に持ち出す場合、紛失又は盗難等のリスクが高まるため、可能な限り暗号化する必要がある。暗号化以外の方法としては、秘密分散等の情報保護措置の実施が挙げられる。

- (c) 行政事務従事者は、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が接続許可を与えた通信回線以外に端末を接続しないこと。

解説：不適切な管理がなされている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事項である。

政府内通信回線でも許可を得た通信回線以外に接続してはならない。モバイル PC を府省庁外に持ち出した際に接続する通信回線についても接続許可を得る必要がある。

5.2.3 サーバ装置

趣旨（必要性）

サーバ装置については、当該サーバ装置の内蔵記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も比較的大きなものとなる。

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、ウイルス感染や不正侵入等を受けるリスクが高い。政府のサーバ装置が不正アクセスや迷惑メール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ことにもなる。

さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。

このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるリスクを含有する。

これらのことを勘案し、本項では、サーバ装置に関する対策基準を定める。

遵守事項

(1) サーバ装置の設置時

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、サーバ装置へのリモートログインについて、通信回線で送受信される情報の機密性を確保すること。

解説：サーバ装置へリモートログインする際のセキュリティ強化を求める事項である。

情報システムセキュリティ責任者から保守作業等のためにリモートログインを許可されている者がサーバ装置へログインする場合を想定し、通信の暗号化等の対策が必要である。

- (b) 情報システムセキュリティ責任者は、主たるサービスの提供に必要なサービスを提供し、また、必要なサービスであっても、利用しない機能を無効化して提供すること。

解説：不要なサービス又は機能の停止又は無効化により、サーバ装置から潜在的な脅威を排除するための事項である。なお、設定ができない場合は、それによって生ずるリスクを認識した上で設置する。

(2) サーバ装置の運用時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者は、サーバ装置の構成の変更を監視すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定すること。

解説：サーバ装置の構成が不正に変更されないように監視し、また、変更によるセキュリティレベルの低下が発生しないか検討することを求める事項である。

- (b) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

解説：バックアップを取得することにより情報の保護を目的とした事項である。バックアップの対象は、サーバ装置に保存されている情報から適宜選択すること。「安全に管理」とは、記録した媒体を施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにすることである。「定期的」とは、1日又は1週ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。

- (c) 情報システムセキュリティ管理者は、サーバ装置の運用管理について、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。

解説：運用管理作業の記録を書面として残すための事項である。各府省庁において、ある程度統一的な様式を作成する必要がある。

- (d) 情報システムセキュリティ管理者は、サーバ装置の障害について、障害発生日、障害を受けたサーバ装置、障害の内容、対策及び復旧作業内容並びに作業者を含む事項を記録すること。

概説：障害対応作業の記録を書面として残すための事項である。各府省庁において、ある程度統一的な様式を作成する必要がある。

【強化遵守事項】

- (e) 情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。

解説：サーバ装置上での不正行為及び不正利用を監視するための事項である。「セキュリティ状態を監視」とは、サーバ装置上での不正な行為及び要機密情報へのアクセス等の不正利用の発生を監視することである。監視の方法としては、侵入検知システム、アンチウイルスソフト又はファイル完全性チェックツール等が利用できる。

- (f) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム性能を監視し、当該サーバ装置に関するトラブルの発生を検知すること。

解説：日常的なサーバ装置のシステム性能について監視を行うことで、トラブルを未然に防止するための事項である。「システム性能を監視」とは、サーバ装置のCPU、メモリ、ディスク入出力等のパフォーマンスを監視することである。監視方法は、状況に応じて、ツールの利用、手動から、適切な方法を選択することが可能である。

- (g) 情報システムセキュリティ責任者は、サーバ装置上で記録されるログについて、記録対象、記録項目、保存期間及び保存方法を含む事項を定め、当該ログの記録と保管を情報システムセキュリティ管理者に実施させること。

解説：具体的な記録項目や保存期間等に関しては、サーバ装置が取り扱う情報

の重要性等に応じて異なるので、各組織において検討するものとする。
また、定期的なログの検査に備えて、求められるログを取得し保存する必要がある。

- (h) 情報システムセキュリティ管理者は、記録されたログの内容を定期的に確認、分析し、情報セキュリティ事象の発生を推測し又は検知すること。

解説：記録されたログを定期的に調査して、情報セキュリティ事象の発生を推測、検知するための事項である。

「定期的」とは、1ヶ月から3ヶ月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。なお、調査用のツールを利用すると効果的であるが、手動で調査を行うことも可能である。

5.3 アプリケーションソフトウェア

5.3.1 通信回線を介して提供するアプリケーション共通対策

趣旨（必要性）

IP ネットワークの技術は一般的に普及していること等の理由により、通信回線を介して提供するサービスには、セキュリティ脅威全般に係るリスクが考えられる。これらのリスクを回避するためには、情報システムのライフサイクル全般に対して適切な対策を施すことが必要である。

これらのことを勘案し、本項では、通信回線を介して提供するアプリケーションに関する対策基準を定める。

遵守事項

(1) サービスの導入時

【基本遵守事項】

- (a) 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は、通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備すること。

解説：通信回線を介して提供するサービスに関するセキュリティ維持のための対策について定めることを求める事項である。

「通信回線を介して提供するサービスのセキュリティ維持に関する規定」とは、例えば、サービスを利用する者及び電子計算機の主体認証、アクセス制御、権限管理及び証跡管理の手順等である。

(2) サービスの運用時

【基本遵守事項】

- (a) 情報システムセキュリティ管理者及び課室情報セキュリティ責任者は、サービスのセキュリティ維持に関して整備した規定に基づいて、日常的及び定期的に運用管理を実施すること。

解説：整備された規定に従った運用管理を行い、独断で運用管理を実施しないことを求める事項である。

- (b) 行政事務従事者は、通信回線を介して提供されるサービスを私的な目的のために利用しないこと。

解説：行政事務従事者に対して私的な目的でのサービス利用を禁止する事項である。

5.3.2 電子メール

趣旨（必要性）

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がある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれるなどの可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等に電子メールを利用する行政事務従事者が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。

これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する基準を定める。

遵守事項

(1) 電子メールの導入時

【基本遵守事項】

- (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。

解説：電子メールを不正に中継しないように電子メールサーバを設定することを求める事項である。

【強化遵守事項】

- (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送受信時における行政事務従事者の主体認証を行う機能を備えること。

解説：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主体認証を行うことを定めた事項である。

(2) 電子メールの運用時

【基本遵守事項】

- (a) 行政事務従事者は、業務遂行にかかわる情報を含む電子メールを送受信する場合には、業務用電子メールを利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

解説：第三者が提供する電子メールサービスを、業務遂行にかかわる情報を含む電子メールの送受信に利用することを禁ずる事項である。

- (b) 行政事務従事者は、受信したメールを電子メールクライアントにおいてテキストとして表示すること。

解説：HTMLメールの表示により、偽のホームページに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること及び不正なスクリプトが実行されること等を防ぐことを定めた事項である。

「テキスト」には、リッチテキストが含まれる。

5.3.3 ウェブ

趣旨（必要性）

ウェブにおいては、様々なアプリケーション、データを組み合わせた情報を送受信すること、また IP ネットワークにおいて標準的に利用されるシステムとして一般的に普及していること等の理由により、セキュリティ脅威全般に係るリスクが考えられる。これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を施すことが必要である。

これらのことを勘案し、本項では、ウェブに関する対策基準を定める。

遵守事項

(1) ウェブの導入時

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。

解説：特殊文字を無害化することを求める事項である。

特殊文字は不正侵入等の攻撃に用いられるため、すべての入力されるデータに対して特殊文字列が含まれていないかを確認する必要がある。

- (b) 情報システムセキュリティ責任者は、ウェブサーバからウェブクライアントに必要な情報を送信しないように情報システムを構築すること。

解説：ウェブアプリケーション又はデータベース等から発信するエラーメッセージ等が攻撃を試みる者に攻撃の糸口になり得る情報を与えること及びウェブサーバが保持する情報をウェブクライアントに送信することにより、情報が改ざんの危険にさらされること等を回避するための事項である。

- (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については、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

解説：通信時に盗聴により第三者へ漏えいすることを防止するための事項である。

「通信の盗聴から保護すべき情報」とは、例えば、ウェブで提供するサービスの運営に関わる要機密情報を指し、サービスの利用者から受け取る個人情報等も含む。

【強化遵守事項】

- (d) 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については、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。

解説：不正侵入等の事故発生時における被害範囲の限定を図るための事項である。

あらかじめすべての利用者が利用等することが想定されているデータを除き、特定の利用者のみが利用等するデータ等を、ウェブサーバに保存しないことが必要である。

- (e) 情報システムセキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。

解説：電子証明書による検証により、利用者がウェブサーバの正当性を確認できるようにウェブサーバを構築することを求める事項である。

(2) ウェブの運用時

【基本遵守事項】

- (a) 行政事務従事者は、ウェブクライアントが動作する電子計算機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。

解説：電子署名により配布元が確認できるソフトウェアについては、電子計算機にインストールすることが可能なソフトウェアとして許可されていればダウンロードすることができる。

【強化遵守事項】

- (b) 情報システムセキュリティ責任者は、行政事務従事者が閲覧することが可能なホームページを制限し、定期的にその見直しを行うこと。

解説：ウェブで閲覧したホームページからの不適切なソフトウェアのダウンロードや私的なホームページの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。

制限を実施する方法は、ウェブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。

5.4 通信回線

5.4.1 通信回線共通対策

趣旨（必要性）

通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを含んでいる。

これらのことを勘案し、本項では、通信回線に関する対策基準を定める。

遵守事項

(1) 通信回線を構築する場合

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。

解説：情報システムセキュリティ責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。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して構築する必要がある。

- (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、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保するための事項である。通信回線の負荷に関して事前にテスト等を実施し、必要となる容量及び能力を想定し、それを備える。また、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。

- (c) 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関連文書を整備すること。

解説：通信回線及び通信回線装置と関連文書の整合性を確保するための事項である。「通信回線及び通信回線装置関連文書」とは、通信回線の設計書又は仕様書及び通信回線の構成、電子計算機の識別コード又は通信回線装置の設定等が記載された文書が挙げられる。書面ではなく電子記録媒体で整備していても差し支えない。

- (d) 情報システムセキュリティ責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、電子計算機をグループ化し通信回線上で分離することを求め

る事項である。府省庁外通信回線の場合は、府省庁外通信回線に接続される電子計算機はグループ化し、府省庁内通信回線に接続される電子計算機と分離する必要がある。なお、府省庁外通信回線に接続される電子計算機は、物理的にグループ化することはできないが、論理的にグループ化しておきアクセス制御の対象とする。通信回線上のセキュリティを確保する方法の1つとして、電子計算機の利用目的、提供するサービス及び求められるセキュリティ機能等に照らし合わせて、必要と認められる通信以外は禁止する方法がある。

- (e) 情報システムセキュリティ責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。

解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。情報システムセキュリティ責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信をすべて確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。

- (f) 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については、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めるときは、情報を暗号化すること。

解説：通信回線を用いて送受信される要機密情報を保護するための事項である。情報システムセキュリティ責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の暗号化の必要性を検討する必要がある。

- (g) 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情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、選択すること。

解説：通信回線に利用する物理的な回線によってセキュリティレベルが異なることから、適切な回線を選択することを求める事項である。回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。

- (h) 情報システムセキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

解説：遠隔地からの通信回線装置の保守や診断に利用するサービスのセキュリティを確保するための事項である。セキュリティ確保の方法として、識別コード及び主体認証情報（パスワード）による主体認証、接続する電子計算機の識別コードによるアクセス制御、通信の暗号化等の機密性の確保だけでなく、通信回線が利用できない状況での代替接続手段の確保等の可用性の確保も挙げられる。

- (i) 情報システムセキュリティ責任者は、通信回線装置に存在する公開されたセキュ

リティホールから通信回線装置を保護するための対策を講ずること。

解説：セキュリティホール対策を行うことで、通信回線装置をセキュリティが確保された最新の状態にするための事項である。対策には、パッチ適用等だけでなく、設定等での回避も含まれる。

- (j) 情報システムセキュリティ責任者は、通信回線装置を安全区域に設置すること。また、損傷及び盗聴を含む脅威から通信ケーブルを保護するための対策を講ずること。

解説：通信回線装置及び通信ケーブルが設置される物理的環境における脅威への対策を求める事項である。

- (k) 情報システムセキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

解説：府省庁内通信回線同士を専用線で接続する場合に、当該専用線のサービスレベルを確保するための事項である。

情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約をする者に対して依頼すること。

【強化遵守事項】

- (l) 情報システムセキュリティ責任者は、通信を行う電子計算機の主体認証を行うこと。

解説：通信を行う電子計算機の主体認証を行うことで、通信相手の電子計算機が正しい相手であることを確認するための事項である。

- (m) 情報システムセキュリティ責任者は、通信回線を用いて送受信される情報を記録すること。

解説：通信回線を送受信される情報を記録することで、不正アクセス又は情報漏えい等の事象が発生した場合に、原因又は被害範囲等の特定を容易にするための事項である。

- (n) 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、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること。

解説：障害等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替回線又は代替通信回線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を求める事項である。

(2) 通信回線を運用する場合

【基本遵守事項】

- (a) 情報システムセキュリティ管理者は、通信回線を利用する電子計算機の識別コード及び電子計算機を利用する者と当該利用者の識別コードの対応並びに通信回線の利用部局を含む事項の管理を行うこと。

解説：通信回線の運用管理を行うことを求める事項である。情報システムセキ

セキュリティ管理者は、通信回線を利用する電子計算機の識別コード及び電子計算機を利用する者と当該利用者の識別コードの対応並びに通信回線の利用部局を含む事項の管理を行う必要がある。

- (b) 情報システムセキュリティ管理者は、通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項を変更した場合には、当該変更の内容を通信回線及び通信回線装置関連文書へ反映すること。また、当該変更の記録を保存すること。

解説：情報システムセキュリティ管理者が行った変更を適宜関連文書に反映することで、通信回線及び通信回線装置と関連文書の整合性を確保するための事項である。

- (c) 情報システムセキュリティ責任者は、通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項の他者による変更を監視すること。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定すること。

解説：通信回線の構成の不正な変更を監視し、変更によるセキュリティレベルの低下が発生しないか検討することを求める事項である。

- (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の確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生したときに、他の情報システムを保護するための事項である。

- (e) 行政事務従事者は、情報システムセキュリティ責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。

解説：通信回線に無断で電子計算機及び通信回線装置を接続された場合に生ずるリスクを防止するための事項である。

- (f) 情報システムセキュリティ責任者は、通信回線装置のセキュリティレベル維持のため、公開されたセキュリティホールから通信回線装置を保護するための対策を講ずること。

解説：通信回線及び通信回線装置の運用中に公開されたセキュリティホールに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。対策を検討する初期の段階では、「直接解決する対策方法がないため代替案を実施する」、「リスクが大きくないので対策しない」といった計画で差し支えない。その判断は各組織に委ねられる。

- (g) 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基準となる時刻に、すべての通信回線装置の時刻を同期するための措置を講ずること。

解説：情報システム内で同期されている共通の時刻に構築した通信回線装置の時刻を同期させることを求める事項である。

有事の際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えないものとする。

(3) 通信回線の運用停止時

【基本遵守事項】

- (a) 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については、通信回線装置の利用を停止する場合には、通信回線装置の内蔵記録媒体の情報を復元が困難な状態にすること。

解説：運用を停止した通信回線装置が再利用又は廃棄された後、停止前に保存していた情報が漏えいすることを防ぐために、情報の消去を求める事項である。

消去の方法としては、乱数データの書き込み、内蔵記録媒体の物理的な破壊等の方法がある。

5.4.2 府省庁内通信回線の管理

趣旨（必要性）

府省庁内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを含んでいる。また、利用する回線により想定される脅威及びリスクが異なる。

これらのことを勘案し、本項では、府省庁内通信回線に関する対策基準を定める。

遵守事項

(1) 府省庁内通信回線を構築する場合

【強化遵守事項】

- (a) 情報システムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続すること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。

解説：通信回線に接続する電子計算機の確認を行うことを求める事項である。

当該措置を実施するための技術としては、電子計算機固有の情報による主体認証、IEEE 802.1x 等が挙げられる。

(2) 府省庁内通信回線を運用する場合

【強化遵守事項】

- (a) 情報システムセキュリティ責任者は、通信要件の変更に際し又は定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定も見直す必要がある。「定期的」とは、

6ヶ月から12ヶ月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、情報システムセキュリティ責任者は定期的にアクセス制御の設定の見直しを行う。

- (b) 情報システムセキュリティ責任者は、定期的に、通信回線及び通信回線装置のセキュリティホールを検査すること。

解説：定期的なセキュリティホール検査の実施を求める事項である。「定期的」とは、1ヶ月から3ヶ月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。これによって、セキュリティレベルの低下、対策漏れ、アクセス制御の設定ミスがないかを確認する必要がある。

- (c) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況を確認、分析し、情報セキュリティ事象の発生を推測又は検知すること。

解説：確保している性能では適正な運用が困難な状態になることにより、情報の可用性を侵害する事態を回避するため、通信回線の監視を求める事項である。問題の発生を推測又は検知できた場合には、事前に対策を行うことが求められる。

- (d) 情報システムセキュリティ管理者は、府省庁内通信回線上を送受信される通信内容を監視すること。

解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。

(3) 回線の対策

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、VPNを利用する場合には、以下に挙げる事項を含む措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) VPN経由でアクセスすることが可能な通信回線の範囲の制限

(カ) VPN接続方法の機密性の確保

(キ) VPNを利用する電子計算機の管理

解説：VPNを利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネットVPN、IP-VPN、SSL-VPN、SoftEther等が挙げられる。

- (b) 情報システムセキュリティ責任者は、無線LANを利用する場合には、以下に挙

げる事項を含む措置を講ずること。

- (ア)利用開始及び利用停止時の申請手続の整備
- (イ)通信内容の暗号化
- (ウ)通信を行う電子計算機の識別又は利用者の主体認証
- (エ)主体認証記録の取得及び管理
- (オ)無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
- (カ)無線 LAN に接続中に他の通信回線との接続の禁止
- (キ)無線 LAN 接続方法の機密性の確保
- (ク)無線 LAN に接続する電子計算機の管理

解説：無線 LAN を利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。

- (c) 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセスを利用する場合には、以下に挙げる事項を含む措置を講ずること。

- (ア)利用開始及び利用停止時の申請手続の整備
- (イ)通信を行う者又は発信者番号による識別及び主体認証
- (ウ)主体認証記録の取得及び管理
- (エ)リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
- (オ)リモートアクセス中に他の通信回線との接続の禁止
- (カ)リモートアクセス方法の機密性の確保
- (キ)リモートアクセスする電子計算機の管理

解説：公衆電話網を経由してリモートアクセスを利用する場合に、セキュリティを確保することを求める事項である。

5.4.3 府省庁外通信回線との接続

趣旨（必要性）

府省庁内通信回線と府省庁外通信回線との接続については、府省庁外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、府省庁外通信回線に送受信される情報の漏えい、改ざん又は破壊等、府省庁外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを含んでいる。

これらのことを勘案し、本項では、府省庁外通信回線と接続する場合の府省庁内通信回線に関する対策基準を定める。

遵守事項

- (1) 府省庁内通信回線を府省庁外通信回線と接続する場合

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、情報セキュリティ責任者の承認を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。

解説：府省庁内通信回線を府省庁外通信回線と接続するとリスクの増大を招く

ので、情報セキュリティ責任者の判断を得ることを求める事項である。
情報セキュリティ責任者は、様々なリスクを検討した上で承認の可否を判断する必要がある。

- (b) 情報セキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより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、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。

解説：府省庁内通信回線に接続している情報システムを、府省庁外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している府省庁内通信回線から独立した通信回線として構成するか、府省庁外通信回線から切断した通信回線として構築することになるが、必要なセキュリティ対策は実施すること。

(2) 府省庁外通信回線と接続している府省庁内通信回線を運用する場合

【基本遵守事項】

- (a) 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の確保が困難な事由が発生した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生したときに、他の情報システムを保護するための事項である。

- (b) 情報システムセキュリティ責任者は、通信回線の変更に際し又は定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定を見直す必要がある。「定期的」とは、3ヶ月から6ヶ月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されとは限らないので、情報システムセキュリティ責任者は定期的にアクセス制御の設定の見直しを行う。

- (c) 情報システムセキュリティ責任者は、定期的に、府省庁外通信回線から通信することが可能な府省庁内通信回線及び通信回線装置のセキュリティホールを検査すること。

解説：定期的なセキュリティホール検査の実施を求める事項である。これによって、セキュリティレベルの低下、対策漏れ、アクセス制御の設定ミスがないかを確認する必要がある。

- (d) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況を確認、分析し、情報セキュリティ事象の発生を推測又は検知すること。

解説：確保している性能では適正な運用が困難な状態になることにより、情報の可用性を侵害する事態を回避するため、通信回線の監視を求める事項である。問題の発生を推測又は検知できた場合には、事前に対策を行うことが求められる。

- (e) 情報システムセキュリティ管理者は、府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容を監視すること。

解説：府省庁外通信回線と送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。

第6部 個別事項についての対策

6.1 個別事項

6.1.1 外部委託

趣旨（必要性）

政府部外の者に情報処理業務を委託する場合には、政府が委託先を直接統制することができないため、政府部内で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報処理業務を外部委託する際は、委託先においても各府省庁の省庁基準と同等の対策を実施させるべく、委託先への要求事項を明確にする必要がある。

これらのことを勘案し、本項では、外部委託に関する対策基準を定める。

遵守事項

(1) 府省庁内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

- (a) 統括情報セキュリティ責任者は、外部委託の対象とする情報システム及び委託先による部門内の情報資産へアクセスすることが可能な範囲を明確化すること。

解説：外部委託の対象可能な範囲と対象としてはいけない範囲を府省庁として明確化することに関する遵守事項を定めたものである。府省庁内の情報システム及び関連する業務に関し、網羅性を確保しつつ統一的な基準で当該範囲を設定することが重要である。

- (b) 統括情報セキュリティ責任者は、委託先の選定手続、選定基準及び委託先が具備すべき要件（委託先職員に対する情報セキュリティ対策の実施を含む。）を整備すること。

解説：委託先の選定において整備すべき基準や要件に関する事項を定めたものである。

統括情報セキュリティ責任者は、外部委託の選定基準や要件の整備に当たっては、当該委託先が、事業継続性を有し存続可能であり、省庁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、委託先が省庁基準の該当項目を遵守し得る者であること、各府省庁の省庁基準と同等の情報セキュリティ管理体制を確立すること、各府省庁の省庁基準と同等の情報セキュリティ対策の教育を実施すること等が挙げられる。

また、府省庁のセキュリティレベルを一定水準以上に保つために、委託先職員に対して要求すべきセキュリティ要件を府省庁内で統一的に整備

することが重要である。

なお、本基準や要件は、法制度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、外部委託の実施に反映することが必要である。

【強化遵守事項】

- (c) 統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。

評価方法の整備には、ISO / IEC17799 等に基づく認証制度の活用や、国際規格を踏まえ、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セルフチェックベースのツール等の応用が考えられる。

- (d) 統括情報セキュリティ責任者は、前事項の評価方法に従って、求める情報セキュリティ要件に対する委託先の候補者の情報セキュリティ水準を確認し、委託先の選定基準の一要素として利用すること。

解説：前事項の評価方法に従って委託先候補者のセキュリティ水準を確認し、これを委託先の選定基準の一要素として利用することを求める事項である。

(2) 委託先に適用する情報セキュリティ対策の整備

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処手順を整備すること。

解説：委託先に請け負わせる業務における情報セキュリティ侵害発生時の対処手順を府省庁として整備することに関する遵守事項を定めたものである。請負内容における情報セキュリティ侵害の影響度の大きさや可用性に対する要求度に応じて、対処の緊急性等を考慮することが重要である。

- (b) 情報システムセキュリティ責任者は、委託先の情報セキュリティ対策への履行状況を確認するための評価基準を策定し、遵守すべき情報セキュリティ対策の履行が不十分である場合の措置に関して委託先に事前に通知すること。

解説：委託先における情報セキュリティ対策の履行が不十分である場合に対する措置に関し、対象となる情報システムや業務に応じて決定、事前通知すべき事項を定めたものである。

また、情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約する者に対して依頼すること。

(3) 外部委託の実施における手続きの遵守

【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、外部委託を実施する際に、情報セキュリテ

イ関係規程に基づく情報セキュリティ対策の遵守、機密の保持（情報の目的外利用の禁止等を含む。）委託先に請け負わせる業務における情報セキュリティ侵害発生時の対処手順の遵守及び情報セキュリティ対策の履行が不十分である場合の措置の遵守を含む外部委託に伴う契約書等を取り交わすこと。また、必要に応じて、以下の事項を含めること。

(ア)情報セキュリティ監査を受け入れること。

(イ)提供されるサービスレベルに関して委託先に保証させること。

解説：外部委託を実施する際の手続きの遵守に関して定めた事項である。

機密の保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報等を守る必要があることから、これを記載する必要がある。

委託先への監査の実施に際しては、提出させる各種ログの監査レベルや提出範囲等を決定し、事前に合意しておくことが重要である。また、当該業務の重要度により、立入監査の実施、重点項目のみ立入監査、委託先による内部監査報告の監査等を適切に選択することが必要である。

委託先から提供を受け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手順、並びに事故発生時の対応手順等を決定し、委託先に保証させることが重要である。

情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約する者に対して依頼すること。

(b) 情報システムセキュリティ責任者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書を提出させること。また、必要に応じて、以下の事項を当該確認書に含めること。

(ア)遵守すべき情報セキュリティ対策を実現するために、委託先における所属職員が実施する具体的な取組内容

(イ)外部委託した業務の作業に携わる者の特定とそれ以外の者による作業の禁止

解説：外部委託に係る契約者双方の責任の明確化と合意形成に基づく委託先からの確認書の入手に関する事項を定めたものである。

特に、開発委託の終了後の運用におけるセキュリティパッチの適用等、情報セキュリティの維持に関する責任の所在に関しては、外部委託の実施時に明確化しておく必要がある。

(c) 情報システムセキュリティ責任者は、外部委託契約の継続に関しては、選定手続、選定基準及び委託先が具備すべき要件に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。

解説：外部委託契約の継続、特に随意契約に関し、都度審査することの重要性を定めたものである。

また、情報システムセキュリティ責任者自身が契約を行わない場合には、

セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約する者に対して依頼すること。

- (d) 情報システムセキュリティ責任者は、委託先の提供するサービス（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定手続、選定基準及び委託先が具備すべき要件に基づき、その是非を審査すること。

解説：委託契約の実施中及び変更時における委託先のサービス変更の管理に関して定めた事項である。変更がある場合にはその是非を審査し、必要に応じて、契約変更をする等の対応が必要である。

また、情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約する者に対して依頼すること。

- (e) 情報システムセキュリティ責任者は、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負する合理的理由が認められる場合は、その限りではない。

解説：請負内容に関する第三者への再請負の原則禁止を定めたものである。一般的に、委託先が多階層化されるとセキュリティレベルが下がることが懸念されるため、合理的理由がない場合、再請負を禁止する。また、請負内容の全部を再請負させることは、合理的理由が成り立たないため、禁止する。

情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取り決めについて、契約する者に対して依頼すること。

- (f) 行政事務従事者は、委託先が要機密情報を取り扱う場合、以下の実施手順に従うこと。

(ア) 委託先に情報を移送する場合は、不要部分のマスキングや暗号化等安全な受け渡し方法により実施し、移送した記録を保存すること。

(イ) 外部委託の業務終了等により情報が不要になった場合には、確実に返却又は廃棄させること。

解説：委託契約開始から終了に至るまでの当事者間での情報の授受に関する実施手順遵守の徹底に関して定めたものである。委託先の選定基準や情報セキュリティ侵害時の対処手順等の仕組みを整備した上で、当事者間の情報の授受において実施手順に従うことによりセキュリティレベルを確保することが重要である。

6.1.2 府省庁外での情報処理の制限

趣旨（必要性）

行政事務においては、その事務の遂行のため、府省庁外において情報処理を実施する必

要が生じる場合がある。この際、府省庁外での実施では物理的な安全対策を講じることが比較的困難になることから、行政事務従事者は、庁舎内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

これらのことを勘案し、本項では、府省庁外での情報処理の制限に関する対策基準を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

- (a) 統括情報セキュリティ責任者は、要保護情報について府省庁外での情報処理を行う場合の安全管理措置についての規定を整備すること。

解説：統括情報セキュリティ責任者が、府省庁外において情報処理を行う場合の安全管理措置についての規定を整備することを求める事項である。

- (b) 統括情報セキュリティ責任者は、要保護情報を取り扱う情報システムを府省庁外に持ち出す場合の安全管理措置についての規定を整備すること。

解説：統括情報セキュリティ責任者が、府省庁外に情報処理システムを持ち出す場合の安全管理措置についての規定を整備することを求める事項である。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

- (a) 行政事務従事者は、要保護情報（機密性2情報を除く。）について府省庁外で情報処理を行う場合には、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の許可を得ること。

解説：本事項は、要保護情報（機密性2情報を除く。）に係る情報処理に限定して、府省庁外で行う情報処理について、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の許可を求める事項である。

- (b) 行政事務従事者は、機密性2情報について府省庁外で情報処理を行う場合には、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に届け出ること。

解説：本事項は、府省庁外で機密性2情報の情報処理を行う場合に、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に届け出ることを求める事項である。

- (c) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、府省庁外での要保護情報の情報処理に係る記録を取得すること。

解説：府省庁外での要保護情報の情報処理に係る記録を取得し、保存することを求める事項である。

「情報処理に係る記録」とは、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等が挙げられる。

- (d) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報（機密性2情報を除く。）について府省庁外での情報処理を行うことを許可した期間が終

了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。

- (e) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、機密性2情報について府省庁外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

解説：届出期間が長期にわたるなど、必要に応じて、府省庁外での情報処理の状況を確認することを求める事項である。

状況を確認した際に、期間の延長が必要な状況であれば、行政事務従事者に改めて届出をさせること。

- (f) 行政事務従事者は、要保護情報について府省庁外で情報処理を行う場合には、業務の遂行に必要な最小限の情報処理にとどめること。

解説：要保護情報を府省庁外で情報処理することを最小限にとどめることを求める事項である。

- (g) 行政事務従事者は、要保護情報（機密性2情報を除く。）を取り扱う情報システムを府省庁外に持ち出す場合には、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の許可を得ること。

解説：要保護情報（機密性2情報を除く。）を府省庁外に持ち出す行政事務従事者に、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から許可を得ることを求める事項である。

- (h) 行政事務従事者は、機密性2情報を取り扱う情報システムを府省庁外に持ち出す場合には、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に届け出ること。

解説：機密性2情報を府省庁外に持ち出す行政事務従事者に、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に届け出ることを求める事項である。

- (i) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報を取り扱う情報システムの府省庁外への持出しに係る記録を取得すること。

解説：要保護情報を取り扱う情報システムの府省庁外への持出しに係る記録を取得し、保存することを求める事項である。

「持出しに係る記録」とは、持出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等が挙げられる。

- (j) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報（機密性2情報を除く。）を取り扱う情報システムを府省庁外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。

- (k) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、機密性2情報を取り扱う情報システムを府省庁外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

解説：届出期間が長期にわたるなど、必要に応じて、府省庁外への持出しの状況を確認することを求める事項である。

状況を確認した際に、期間の延長が必要な状況であれば、行政事務従事者に改めて届出をさせること。

- (l) 行政事務従事者は、要保護情報を取り扱う情報システムを府省庁外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持出しにとどめること。

解説：要保護情報を取り扱うシステムを府省庁外に持ち出すことを最小限にとどめることを求める事項である。

(3) 安全管理措置の遵守

【基本遵守事項】

- (a) 行政事務従事者は、要保護情報（機密性2情報を除く。）について府省庁外での情報処理について定められた安全管理措置を講ずること。

解説：行政事務従事者に対して、府省庁外での情報処理について定められた安全管理措置を講ずることを求める事項である。

- (b) 行政事務従事者は、要保護情報（機密性2情報を除く。）について府省庁外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

解説：行政事務従事者に対して、府省庁外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。

- (c) 行政事務従事者は、要保護情報を取り扱う情報システムの府省庁外への持出しについて定められた安全管理措置を講ずること。

解説：適切な安全管理措置とは、本統一基準に定めた事項等である。

例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、操作を実施できなくすること等が挙げられる。

- (d) 行政事務従事者は、要保護情報（機密性2情報を除く。）を取り扱う情報システム

を府省庁外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

解説：行政事務従事者に対して、府省庁外へ情報処理システムの持出しが終了したことを、その許可を与えた者に報告することを求める事項である。

6.1.3 府省庁支給以外の情報システムによる情報処理の制限

趣旨（必要性）

行政事務においては、その事務の遂行のため、府省庁支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが府省庁が支給していないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できない。

これらのことを勘案し、本項では、府省庁支給以外の情報システムによる情報処理の制限に関する対策基準を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

- (a) 統括情報セキュリティ責任者は、要保護情報について府省庁支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

解説：行政事務従事者が所有する個人のPCなど、府省庁支給以外の情報システムを用いて要保護情報に関する情報処理を行う場合であっても、府省庁支給の情報システムと同程度の情報セキュリティ対策を施す必要があるため、その安全管理措置についての規定を整備することを求める事項である。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

- (a) 行政事務従事者は、要保護情報（機密性2情報を除く。）について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、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の許可を得ること。

解説：府省庁支給以外の情報システムによる要保護情報（機密性2情報を除く。）の情報処理を許可する場合は、その期間については、最長で1年間にすることが望ましい。ただし、期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。

- (b) 行政事務従事者は、機密性2情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、情報セキュリティ責任者又は課室情報セキ

セキュリティ責任者に届け出ること。

解説：府省庁支給以外の情報システムによる機密性2情報の情報処理を行う場合に、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に届け出をを求める事項である。

- (c) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、府省庁支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。

解説：府省庁支給以外の情報システムによる要保護情報の情報処理に係る記録を取得し、保存することを求める事項である。

「府省庁支給以外の情報システムによる情報処理に係る記録」とは、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等が挙げられる。

- (d) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報（機密性2情報を除く。）について府省庁支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。

- (e) 情報セキュリティ責任者及び課室情報セキュリティ責任者は、機密性2情報について府省庁支給以外の情報システムによる情報処理を行うことを届けた期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

解説：届出期間が長期にわたる場合など、必要に応じて、府省庁支給以外の情報システムによる情報処理の状況を確認することを求める事項である。状況を確認した際に、期間の延長が必要な状況であれば、行政事務従事者に改めて届出をさせること。

(3) 安全管理措置の遵守

【基本遵守事項】

- (a) 行政事務従事者は、要保護情報について府省庁支給以外の情報システムによる情報処理を行う場合には、原則として、当該情報システムについて定められた安全管理措置を講ずること。

解説：行政事務従事者が所有する個人のPCなど、府省庁支給以外の情報システムを用いて要保護情報に関する情報処理を行う場合であっても、府省庁支給の情報システムと同程度の情報セキュリティ対策を施す必要があるため、行政事務従事者に安全管理措置を講ずることを求める事項である。

- (b) 行政事務従事者は、要保護情報（機密性2情報を除く。）について府省庁支給以外の情報システムによる情報処理を終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場

合は、この限りでない。

解説：行政事務従事者が要保護情報（機密性 2 情報を除く。）について府省庁支給以外の情報システムによる情報処理を終了した時に、その報告を求める事項である。府省庁支給以外の情報システムの利用許可を与えた者は、その終了報告を受け、府省庁支給以外の情報システムによる情報処理の状況を把握することが可能となる。その結果、府省庁支給以外の情報システムを、本来必要とされる期間を超えて利用している場合には、これを検知し、利用実態を是正することが可能となる。

6.2 その他

6.2.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止

趣旨（必要性）

各府省庁が、府省庁外の情報セキュリティ水準の低下を招くような行為をすることは、府省庁外に対して適切な行為でないことは当然であって、その行為が他者の情報セキュリティ水準を低下させることによって、当該府省庁を取り巻く情報セキュリティ環境を悪化させるため、各府省庁にとっても好ましくない。

これらのことを勘案し、本項では、府省庁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対策基準を定める。

遵守事項

(1) 措置の徹底

【基本遵守事項】

- (a) 統括情報セキュリティ責任者は、府省庁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措置についての規定を整備すること。

解説：府省庁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して、統括情報セキュリティ責任者が、規定を整備することを求める事項である。府省庁外の情報セキュリティ水準の低下を招く行為としては、例えば、以下のものが挙げられる。

- ・府省庁のウェブのコンテンツを利用するために、ブラウザのセキュリティ設定の下方修正を明示的に要求する行為
- ・府省庁のウェブにより実行形式のファイル（Windows の場合、「.exe」ファイル）を提供（メールに添付する場合も同様）する行為
- ・府省庁のウェブにより署名していない実行モジュール（Java アプレットや Windows の ActiveX ファイル）を提供する行為
- ・府省庁から html メールを送信する行為

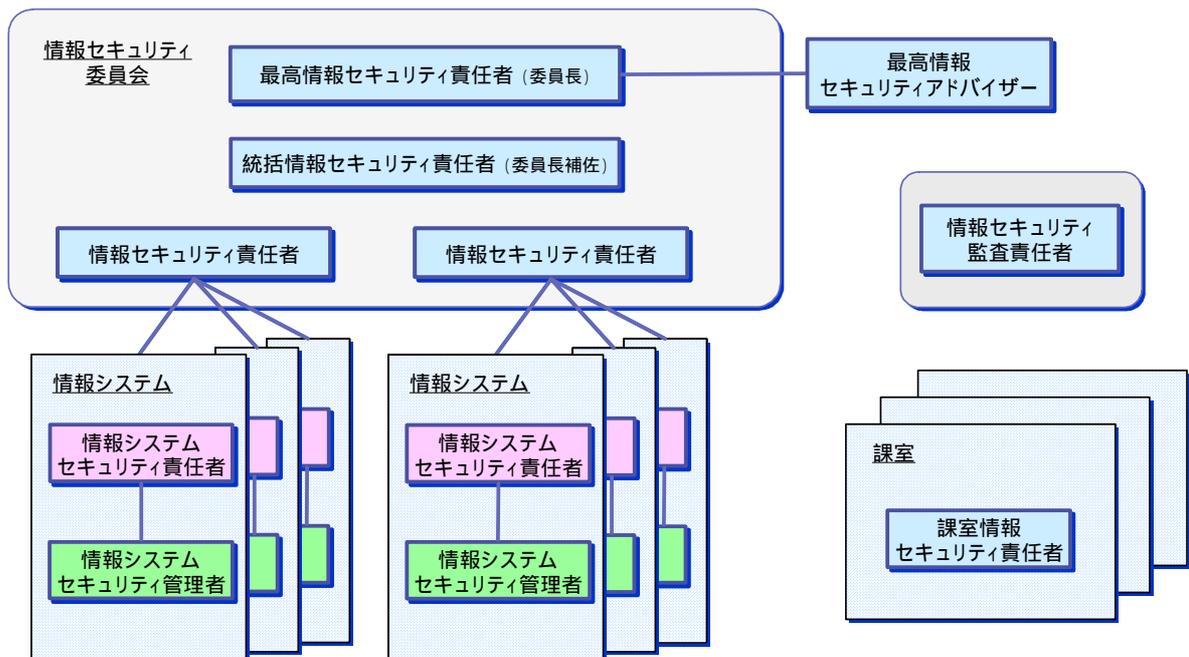
なお、後者の3つについては、利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある行為である。

- (b) 行政事務従事者は、原則として、府省庁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措置を講ずること。

解説：府省庁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各府省庁の役割を定めた事項である。統括情報セキュリティ責任者及び行政事務従事者は、各々組織及び個人として措置を講ずることが重要である。

A.1 本書別添資料

A.1.1 組織・体制イメージ図



A.1.2 本統一基準における情報の格付け一覧

機密性による情報の格付け

格付け	分類基準	取扱制限
機密性 3 情報	秘密文書に相当する機密性を要する情報	例) 複製禁止 再配付禁止 暗号化必須
機密性 2 情報	秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報	
機密性 1 情報	機密性 2 情報又は機密性 3 情報以外の情報	

完全性による情報の格付け

格付け	分類基準	取扱制限
完全性 2 情報	改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	例) 年 月 日まで 保存
完全性 1 情報	完全性 2 情報以外の情報	

可用性による情報の格付け

格付け	分類基準	取扱制限
可用性 2 情報	滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	例) 1 時間以内復旧
可用性 1 情報	可用性 2 情報以外の情報	

A.1.3 情報セキュリティ対策に関する政府決定等

- ・国の行政機関における情報システム関係業務の外注の推進について（平成 12 年 3 月 31 日行政情報システム各省庁連絡会議了承）
- ・各省庁の調達におけるセキュリティ水準の高い製品等の利用方針（平成 13 年 3 月 29 日行政情報化推進各省庁連絡会議了承）
- ・各府省の情報システム調達における暗号の利用方針（平成 15 年 2 月 28 日 行政情報システム関係課長連絡会議了承）
- ・電子政府構築計画（平成 16 年 6 月 14 日一部改訂 各府省情報化統括責任者（CIO）連絡会議決定）
- ・行政情報の電子的提供に関する基本的考え方（指針）（平成 16 年 11 月 12 日 各府省情報化統括責任者（CIO）連絡会議決定）
- ・国家公務員身分証明書の IC カード化（平成 16 年 2 月 6 日 e-Japan 戦略 II 加速化パッケージ）
- ・行政情報の電子的提供業務及び電子申請等受付業務の業務・システム最適化計画（平成 17 年 8 月 24 日 各府省情報化統括責任者（CIO）連絡会議決定）

注）詳細については、原文を参照すること。