

政府機関の情報セキュリティ対策のための 統一管理基準 新旧対照表

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
1	表紙	政府機関の情報セキュリティ対策のための統一 <u>管理基準</u>	表紙	政府機関の情報セキュリティ対策のための統一基準(<u>第4版</u>)(<u>平成21年度修正</u>)	構成変更
2	1.1.1.1	1.1.1.1 本統一 <u>管理基準</u> 及び統一 <u>技術基準</u> の位置付け	1.1.1.1	1.1.1.1 本統一基準の位置付け	構成変更
3	1.1.1.1(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 <u>管理基準</u> 及び統一 <u>技術基準</u> の位置付け	1.1.1.1(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	構成変更
4	1.1.1.1(1)	府省庁の情報セキュリティの確保については、 <u>それぞれの</u> 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、「 <u>政府機関の情報セキュリティ対策のための統一規範(平成23年4月21日付情報セキュリティ政策会議決定)</u> 」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、 <u>それぞれの</u> 府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要である。そこで本統一 <u>管理基準</u> 及び「 <u>政府機関の情報セキュリティ対策のための統一技術基準</u> 」(以下「統一技術基準」という。)は、政府機関における統一的な枠	1.1.1.1(1)	<u>各</u> 府省庁の情報セキュリティの確保については、 <u>各</u> 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、「 <u>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)</u> 」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、 <u>各</u> 府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要である。そこで本統一基準は、 <u>この</u> 政府機関統一的な枠組みの中で、 <u>各</u> 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	構成変更、表現の適正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		組みの中で、 <u>それぞれの</u> 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。		準を定めたものである。	
5	1.1.1.1(2)	本統一 <u>管理基準及び統一技術基準</u> の改訂	1.1.1.1(2)	本統一基準の改訂	構成 変更
6	1.1.1.1(2)	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とらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。本統一 <u>管理基準及び統一技術基準</u> については、 <u>それぞれの府省庁がその特性を踏まえた</u> 上で省庁対策基準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 <u>管理基準及び統一技術基準</u> 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 <u>管理基準</u> 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 <u>管理基準</u> 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、府省庁においては、本統一 <u>管理基準及び統一技術基準</u> が更新された場合、その内容を <u>それ</u>	1.1.1.1(2)	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とらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。本統一基準については、 <u>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</u> 上で省庁対策基準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、 <u>各</u> 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。	構成 変更、 表現 の適 正化

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
		ぞれの 省庁対策基準に適切に反映させる必要がある。			
7	1.1.1.1(3)	情報及び情報システムの取扱いに関しては、法令及び規則等（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 管理基準 及び統一 技術基準 のほか関連法令等を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本統一 管理基準 及び統一 技術基準 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。	1.1.1.1(3)	情報及び情報システムの取扱いに関しては、法令及び規則等（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、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本統一基準では、あえて関連法令等の遵守について明記していない。また、情報セキュリティ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。	構成 変更
8	1.1.1.2	1.1.1.2 本統一 管理基準 及び統一技術基準の使い方	1.1.1.2	1.1.1.2 本統一基準及び統一技術基準の使い方	表現 の適 正化
9		（「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」へ移動）	1.1.1.2(1)	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、	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				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、省庁対策基準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。	
10		(1.1.1.5へ移動、併せて「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」にも記載)	1.1.1.2(2)(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、電磁的に記録されている情報を記載した書面（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。	構成 変更
11		(1.1.1.5へ移動)	1.1.1.2(2)(b)	本統一基準は、行政事務従事者に適用される。本統一基準において「行政事務従事者」とは、政府職員及びそれぞれの府省庁の指揮命令に服している者のうち、それぞれの府省庁の管理対象である情報	構成 変更

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
				及び情報システムを取り扱う者をいう。	
12		(「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」へ移動)	1.1.1.2(2)(c)	本統一基準において「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）、金融庁、消費者庁、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、環境省及び防衛省をいう。	構成変更
13	1.1.1.2(1)	<p>本統一<u>管理基準</u>及び<u>統一技術基準</u>は、部、節及び項の <u>3つ</u>の階層によって構成される。</p> <p>本統一<u>管理基準</u>は、組織全体で情報セキュリティ対策を推進する組織・体制の整備、情報のライフサイクルの各段階における情報セキュリティ対策、情報システムに関連のある規程類の整備等について遵守すべき事項を定めており、<u>統一技術基準</u>は技術的な内容であり改訂頻度が高いものとして情報システムに求められるセキュリティ要件等について遵守すべき事項を定めている。</p> <p><u>本統一管理基準</u>では、「総則」、「組織と体制の整備」、「情報についての対策」、「情報処理についての対策」、「情報システムについての基本的な対策」を、<u>統一技術基準</u>では、「情報セキュリティ要件の明確化に基づく対策」、「情報システム</p>	1.1.1.2(3)	<p>本統一基準は、<u>編</u>、部、節及び項の <u>4つ</u>の階層によって構成される。</p> <p>本統一基準は、<u>情報セキュリティ対策を「基本編」、「情報システム編」に編として分類しており、基本編では組織全体で情報セキュリティ対策を推進する組織・体制の整備、情報のライフサイクルの各段階における情報セキュリティ対策、情報システムに関連のある規程類の整備等について遵守すべき事項を定めており、情報システム編は技術的な内容であり改訂頻度が高いものとして情報システムに求められるセキュリティ要件等について遵守すべき事項を定めている。</u></p> <p><u>基本編</u>では、「総則」、「組織と体制の整備」、「情報についての対策」、「情報処理についての対策」、「情報システムについての基本的な対</p>	構成変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		の構成要素についての対策」、「個別事項についての対策」を <u>それぞれ</u> 部として分類している。 さらにそれぞれの部において、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。具体的には以下のとおり。		策」を、 <u>情報システム編</u> では、「情報セキュリティ要件の明確化に基づく対策」、「情報システムの構成要素についての対策」、「個別事項についての対策」を部として <u>それぞれ</u> 分類している。 さらにそれぞれの部において、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。具体的には以下のとおり。	
14	1.1.1.2(1)(a)	<u>第1.1部 総則</u>			構成 変更
15	1.1.1.2(1)(b)	<u>第1.2部 組織と体制の整備</u> 「組織と体制の整備」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 <u>等</u> 、組織としての運用に関する各 <u>行政事務従事者</u> の権限と責務を明確にするために整備すべき事項を <u>本統一管理基準において</u> 定めている。	1.1.1.2(3)(a)	「組織と体制の整備」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 <u>など</u> 、組織としての運用に関する各 <u>職員</u> の権限と責務を明確にするために整備すべき事項を定めている。	構成 変更
16	1.1.1.2(1)(c)	<u>第1.3部 情報についての対策</u> 「情報についての対策」では、情報の作成、利用、保存、移送、提供、 <u>消去等</u> といった情報のライフサイクルに着目し、各段階において各 <u>行政事務従事者</u> が情報を保護するために業務の中で常に実施すべき事項を <u>本統一管理基準において</u> 定めている。	1.1.1.2(3)(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 <u>及び</u> 消去等といった情報のライフサイクルに着目し、各段階において各 <u>職員</u> が情報を保護するために業務の中で常に実施すべき事項を定めている。	構成 変更
17	1.1.1.2(1)(d)	<u>第1.4部 情報処理についての対策</u> 「情報処理についての対策」では、	1.1.1.2(3)(c)	「情報処理についての対策」では、府省庁外での情報処理及び府省庁	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		情報システムの利用において実施すべき事項と、 府省庁外での情報処理及び府省庁支給以外の情報システムによる情報処理において制限すべき事項を 本統一管理基準において 定めている。		支給以外の情報システムによる情報処理において制限すべき事項を定めている。	
18	1.1.1.2(1)(e)	第1.5部 情報システムについての基本的な対策 「情報システムについての基本的な対策」では、 統一技術基準 で定められる遵守事項が適切に実施されるように、情報システムの計画、構築、運用、移行、 廃棄 及び見直しといった情報システムのライフサイクルの各段階において実施すべき事項と、情報システムに係る情報セキュリティを確保するために規定として整備すべき事項を 本統一管理基準において 定めている。	1.1.1.2(3)(d)	「情報システムについての基本的な対策」では、 情報システム編 で定められる遵守事項が適切に実施されるように、情報システムの計画、構築、 運用 、移行、 廃止 及び見直しといった情報システムのライフサイクルの各段階において実施すべき事項と、情報システムに係る情報セキュリティを確保するために規定として整備すべき事項を定めている。	構成 変更
19	1.1.1.2(1)(f)	第2.1部 総則			構成 変更
20	1.1.1.2(1)(g)	第2.2部 情報セキュリティ要件の明確化に基づく対策 「情報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等、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、情報システムにおいて実施すべき事項を 統一技術基準において	1.1.1.2(3)(e)	「情報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、情報システムにおいて実施すべき事項を定めている。	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		定めている。			
21	1.1.1.2(1)(h)	第2.3部 情報システムの構成要素 についての対策 「情報システムの構成要素について 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、情報システムにおいて実施 すべき事項を 統一技術基準におい て 定めている。	1.1.1.2(3)(f)	「情報システムの構成要素につい 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、情報システムにおいて実施 すべき事項を定めている。	構成 変更
22	1.1.1.2(1)(i)	第2.4部 個別事項についての対策 「個別事項についての対策」では、 新たな技術の導入等に関し特に情 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、遵守すべ き事項を 統一技術基準において 定 めている。	1.1.1.2(3)(g)	「個別事項についての対策」では、 新たな技術の導入等に関し特に情 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、遵守すべ き事項を定めている。	構成 変更
23	1.1.1.2(2)	対策項目の記載事項 本統一管理基準及び統一技術基準 では、府省庁が行うべき対策につ いて、対策項目ごとに遵守事項を 示す。	1.1.1.2(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。	構成 変更
24	1.1.1.2(3)	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 一管理基準及び統一技術基準にお いては、各対策項目で対策の強度	1.1.1.2(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	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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。		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。	
25	1.1.1.2(3)(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、府省庁が、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	1.1.1.2(5)(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、 <u>各府省庁において</u> 、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	表現 の適 正化
26	1.1.1.2(3)	以上により、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。	1.1.1.2(5)	以上より、 <u>各府省庁</u> 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。	表現 の適 正化
27		(1.1.1.4へ移動)	1.1.1.2(6)	評価の方法	構成 変更
28		(1.1.1.4へ移動)	1.1.1.2(6)	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。	構成 変更
29		(1.1.1.4へ移動)	1.1.1.2(6)(a)	省庁対策基準が統一基準に準拠した内容となっていること。(設計の準拠性確認)	構成 変更
30		(1.1.1.4へ移動)	1.1.1.2(6)(b)	実際の運用が省庁対策基準に準拠していること。(運用の準拠性確認)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				認)	
31		(1.1.1.4へ移動)	1.1.1.2(6)(c)	省庁対策基準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)	構成 変更
32		(1.1.1.4へ移動)	1.1.1.2(6)(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)	構成 変更
33		(1.1.1.4へ移動)	1.1.1.2(6)	特に、各府省庁の情報セキュリティ監査においては、設計及び運用の準拠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、設計及び運用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、各自における対策の実効性を確保するために、自己点検を活用するものである。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、運用の準拠性確認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	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				責任において運用することが大前提であるが、政府機関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、本統一基準に関する評価指標に基づき、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。	
34	1.1.1.3	情報の格付の区分及び取扱制限の種類	1.1.1.3	情報の格付けの区分及び取扱制限の種類	表現の適正化
35	1.1.1.3(1)	格付及び取扱制限	1.1.1.3(1)	格付け及び取扱制限	表現の適正化
36	1.1.1.3(1)	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様々であり、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、情報の格付の区分及び取扱制限の種類を定めるものとする。 情報の格付及び取扱制限は、その	1.1.1.3(1)	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様々であり、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、情報の格付けの区分及び取扱制限の種類を定めるものとする。 情報の格付け及び取扱制限は、そ	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュリティ対策を明確にするための手段であることから、適切に実施される必要がある。</p> <p>また、情報の格付及び取扱制限を実施することで、情報の利用者に対し、日々の情報セキュリティ対策の意識を向上させることができる。具体的には、情報を作成又は入手するたびに格付及び取扱制限の判断を行い、情報を取り扱うたびに格付及び取扱制限に従った対策を講ずることで、情報と情報セキュリティ対策が不可分であることについての認識を継続的に維持する効果も生ずるため、行政事務従事者にその内容を理解し遵守するように周知すること。</p>		<p>の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュリティ対策を明確にするための手段であることから、適切に実施される必要がある。</p> <p>また、情報の格付け及び取扱制限を実施することで、情報の利用者に対し、日々の情報セキュリティ対策の意識を向上させることができる。具体的には、情報を作成又は入手するたびに格付け及び取扱制限の判断を行い、情報を取り扱うたびに格付け及び取扱制限に従った対策を講ずることで、情報と情報セキュリティ対策が不可分であることについての認識を継続的に維持する効果も生ずるため、行政事務従事者にその内容を理解し遵守するように周知すること。</p>	
37	1.1.1.3(1) 解説	<p>解説：情報の格付及び取扱制限の実施方法については、「行政機関の保有する情報の公開に関する法律」（以下「情報公開法」という。）に<u>基づきそれぞれの府省庁において定めている</u>「処分に係る審査基準」や文書管理規程等を参考に決めるとよい。</p> <p>なお、情報の格付及び取扱制限については、府省庁における情報セキュリティ対策基準の施行日以後に作成又は入手した<u>全て</u>の情報に</p>	1.1.1.3(1) 解説	<p>解説：情報の格付け及び取扱制限の実施方法については、「行政機関の保有する情報の公開に関する法律」（以下「情報公開法」という。）に<u>基づく各府省庁における</u>「処分に係る審査基準」や文書管理規程などを参考に決めるとよい。</p> <p>なお、情報の格付け及び取扱制限については、<u>各府省庁における</u>情報セキュリティ対策基準の施行日以後に作成又は入手した<u>すべての</u>情報について適用するものであ</p>	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		ついて適用するものであり、施行 日前に作成又は入手した情報につ いて一括して処理することを求め <u>ているものではない</u> 。しかし、施 行日前に作成又は入手した情報に ついて、適宜その <u>決定</u> を行うこ とが望ましいことから、当該情報 を施行日以後取り扱う際に、 <u>格付</u> 及び取扱制限を行う必要がある。		り、施行日前に作成又は入手した 情報について一括して処理するこ とを <u>求めている</u> 。しかし、施行 日前に作成又は入手した情報につ いても、適宜その <u>指定</u> を行うこ とが望ましいことから、当該情報を 施行日以後取り扱う際に、 <u>格付け</u> 及び取扱制限を行う必要がある。	
38	1.1.1.3(2)	<u>格付</u> の区分	1.1.1.3(2)	<u>格付け</u> の区分	表現 の適 正化
39	1.1.1.3(2)	情報について、機密性、完全性 <u>及 び</u> 可用性の3つの観点を区別し、 それぞれにつき <u>格付</u> の区分の定義 を示す。 <u>格付</u> としては、以下に記載のもの を本統一 <u>管理</u> 基準の遵守事項で用 いるが、 <u>それぞれの</u> 府省庁におい て、適宜変更又は追加して構わな い。しかし、変更又は追加する場 合には、 <u>それぞれの</u> 府省庁の対策 基準における <u>格付</u> 区分と遵守事項 との関係が本統一 <u>管理</u> 基準 <u>及び統 一技術</u> 基準での関係と同等以上と なるように準拠しなければならない。 また、変更又は追加した場合 には、他の府省庁との情報の <u>やり 取り</u> をする際に、自身の <u>格付</u> 区分 が本統一 <u>管理</u> 基準 <u>及び統一技術</u> 基準で用いた <u>格付</u> 区分とどのよう に対応するかを伝達する方法につ いて定めなければならない。例えば、	1.1.1.3(2)	情報について、機密性、完全性、 <u>、</u> 可用性の3つの観点を区別し、そ れぞれにつき <u>格付け</u> の区分の定義 を示す。 <u>格付け</u> としては、以下に記載のも のを本統一基準の遵守事項で用い るが、 <u>各</u> 府省庁において、適宜変 更又は追加して構わな。しかし、 変更又は追加する場合には、 <u>各</u> 府 省庁の対策基準における <u>格付け</u> 区 分と遵守事項との関係が本統一基 準での関係と同等以上となるよう に準拠しなければならない。また、 変更又は追加した場合には、他の 府省庁との情報の <u>やりとり</u> をする 際に、自身の <u>格付け</u> 区分が本統一 基準で用いた <u>格付け</u> 区分とどのよ うに対応するかを伝達する方法に ついて定めなければならない。例 えば、他の府省庁に情報を提供す る際に、本統一基準で用いた <u>格付</u>	構成 変 更、 表現 の適 正化

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
		他の府省庁に情報を提供する際に、本統一管理基準及び統一技術基準で用いた格付区分を記載する方法が考えられる。		け区分を記載する方法が考えられる。	
40	1.1.1.3(2)(a) 機密性についての格付の定義	機密性についての格付の定義	1.1.1.3(2)(a) 機密性についての格付の定義	機密性についての格付けの定義	表現の適正化
41	1.1.1.3(2)(a) 機密性についての格付の定義表	格付の区分	1.1.1.3(2)(a) 機密性についての格付の定義表	格付けの区分	表現の適正化
42	1.1.1.3(2)(a)	情報の格付の区分は、機密性、完全性及び可用性について、それぞれ以下のとおりとする。	1.1.1.3(2)(a)	情報の格付けの区分は、機密性、完全性、可用性について、それぞれ以下のとおりとする。	表現の適正化
43	1.1.1.3(2)(a) 解説	解説：機密性の格付については、文書管理規程上の秘密文書に相当する機密性を要する情報であり、行政事務従事者のうち、特定の者だけがアクセスできる状態を厳密に確保されるべき情報は機密性3情報に、秘密文書には相当しないが、情報公開法に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報等、行政事務従事者以外がアクセスできない状態を最低限確保されるべき情報は機密性2情報に、それ以外の情報は、機密性1情報に決定することを基本とする。 例えば、従来「取扱注意」等と表示されてきたような資料は、機密性2情報に決定することが考えら	1.1.1.3(2)(a) 解説	解説：機密性の格付けについては、文書管理規程上の秘密文書に相当する機密性を要する情報であり、行政事務従事者のうち、特定の者だけがアクセスできる状態を厳密に確保されるべき情報は機密性3情報に、秘密文書には相当しないが、情報公開法に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報であり、行政事務従事者以外がアクセスできない状態を最低限確保されるべき情報は機密性2情報に、それ以外の情報は、機密性1情報に決定することを基本とする。 例えば、従来「取扱注意」などと表示されてきたような資料は、機密性2情報に決定することが考え	解説の修正

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
		れるが、その内容によっては、機密性1情報に決定した上で取扱制限を <u>決定すること</u> で十分な場合も考えられる。		られるが、その内容によっては、機密性1情報に決定した上で取扱制限を <u>決定するので</u> 十分な場合も考えられる。	
44	1.1.1.3(2)(a) 完全性についての格付の定義	完全性についての <u>格付</u> の定義	1.1.1.3(2)(a) 完全性についての格付の定義	完全性についての <u>格付け</u> の定義	表現の適正化
45	1.1.1.3(2)(a) 完全性についての格付の定義表	<u>格付</u> の区分	1.1.1.3(2)(a) 完全性についての格付の定義表	<u>格付け</u> の区分	表現の適正化
46	1.1.1.3(2)(a) 解説	解説：完全性の <u>格付</u> については、情報が改ざん、誤びゅう又は破損されていない状態を確保されるべき情報は完全性2情報に、それ以外の情報は、完全性1情報に決定することを基本とする。 例えば、原本に相当する情報を完全性2情報に、複製に相当する情報（例えば、電子メールに添付されるファイル <u>等</u> ）を完全性1情報に決定すること <u>等</u> が考えられる。	1.1.1.3(2)(a) 解説	解説：完全性の <u>格付け</u> については、情報が改ざん、誤びゅう又は破損されていない状態を確保されるべき情報は完全性2情報に、それ以外の情報は、完全性1情報に決定することを基本とする。 例えば、原本に相当する情報を完全性2情報に、複製に相当する情報（例えば、電子メールに添付されるファイル <u>など</u> ）を完全性1情報に決定すること <u>など</u> が考えられる。	解説の修正
47	1.1.1.3(2)(a) 可用性についての格付の定義	可用性についての <u>格付</u> の定義	1.1.1.3(2)(a) 完全性についての格付の定義	可用性についての <u>格付け</u> の定義	表現の適正化
48	1.1.1.3(2)(a) 可用性についての格付の定義表	<u>格付</u> の区分	1.1.1.3(2)(a) 可用性についての格付の定義表	<u>格付け</u> の区分	表現の適正化
49	1.1.1.3(2)(a)	行政事務で取り扱う情報（書面を	1.1.1.3(2)(a)	行政事務で取り扱う情報（書面を	表現

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
	可用性2情報	除く。)のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報	可用性2情報	除く。)のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報 <u>をいう。</u>	の適 正化
50	1.1.1.3(2)(a) 解説	解説：可用性の格付については、情報が滅失又は紛失されていない状態及び情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保されるべき情報は可用性2情報に、それ以外の情報は可用性1情報に決定することを基本とする。 なお、可用性2情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。	1.1.1.3(2)(a) 解説	解説：可用性の格付けについては、情報が滅失又は紛失されていない状態及び情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保されるべき情報は可用性2情報に、それ以外の情報は可用性1情報に決定することを基本とする。 なお、可用性2情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。	
51	1.1.1.3(3)	情報について、機密性、完全性及び可用性の3つの観点から区別し、それぞれにつき取扱制限の種類について基本的な定義を定める。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。	1.1.1.3(3)	情報について、機密性、完全性、 <u>可用性の3つの観点を</u> 区別し、それぞれにつき取扱制限の種類 <u>の基本的な定義を行う</u> 。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。	表現 の適 正化
52	1.1.1.3(3)(a)	情報の取扱制限の種類は、機密性、完全性及び可用性について、それぞれ定めるものとする。 <u>なお、取扱制限の種類については適宜定め</u>	1.1.1.3(3)(a)	情報の取扱制限の種類は、機密性、完全性、可用性について、それぞれ定めるものとする。 <u>ただし、これら以外の取扱制限の種類を適宜</u>	表現 の適 正化

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		ることができる。		<u>用</u> いることができる。	
53	1.1.1.4	1.1.1.4 評価の方法	1.1.1.2(6)	1.1.1.2(6) 評価の方法	構成 変更
54	1.1.1.4	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 <u>取組</u> を実施できるものであることが重要である。 <u>そのためには</u> 、府省庁においては本統一 <u>管理基準及び統一技術基準</u> 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。	1.1.1.2(6)	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 <u>取組み</u> を実施できるものであることが重要である。 <u>したがって</u> 、 <u>各</u> 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。	構成 変更
55	1.1.1.4(a)	省庁対策基準が統一 <u>管理基準及び統一技術基準</u> に準拠した内容となっていること。(設計の準拠性確認)	1.1.1.2(6)(a)	省庁対策基準が統一基準に準拠した内容となっていること。(設計の準拠性確認)	構成 変更
56	1.1.1.4(b)	実際の運用が省庁対策基準に準拠していること。(運用の準拠性確認)		(1.1.1.2(6)(b)から移動)	構成 変更
57	1.1.1.4(c)	省庁対策基準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)		(1.1.1.2(6)(c)から移動)	構成 変更
58	1.1.1.4(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)		(1.1.1.2(6)(d)から移動)	構成 変更
59	1.1.1.4	特に、府省庁の情報セキュリティ監査においては、設計及び運用の準拠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、設計及び運用の妥当性に関連して	1.1.1.2(6)	特に、 <u>各</u> 府省庁の情報セキュリティ監査においては、設計及び運用の準拠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、設計及び運用の妥当性に関連	構成 変 更、 解説 の追

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>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、本統一管理基準及び統一技術基準においては、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、各自における対策の実効性を確保するために、自己点検を活用するものである。したがって、各府省庁が監査を行う際には、その自己点検の適切さを確認し、運用の準拠性確認に用いるものとする。また、監査を通じて把握した対策の実施状況と自己点検の結果に相違点があれば、相違点が発生した原因の分析及び自己点検結果の修正を行い正確な実施状況を把握するものとする。</p> <p>情報セキュリティ対策の実施については、原則として、それぞれの府省庁の責任において運用することが大前提であるが、政府機関全体としての情報セキュリティ対策推進の観点から、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。また、それぞれの府省庁にて情報セキュ</p>		<p>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、各自における対策の実効性を確保するために、自己点検を活用するものである。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、運用の準拠性確認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、政府機関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、本統一基準に関する評価指標に基づき、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</p>	加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>リティ報告書を作成し、自組織の情報セキュリティ対策の取組状況を公表する。</u> さらに、内閣官房情報セキュリティセンターは、本統一管理基準及び統一技術基準に関する評価指標に基づき、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府省庁と協議して定めるものとする。		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。	
60	1.1.1.5	1.1.1.5 用語定義	1.1.1.4	1.1.1.4 用語定義	構成 変更
61	1.1.1.5 【あ】	● 「移送」→「情報の移送」を参照。			
62		(2.1.1.5へ移動)	1.1.1.4 【あ】	「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。	構成 変更
63	1.1.1.5 【か】	● 「行政事務従事者」とは、政府職員（府省庁において行政事務に従事している国家公務員）及びそれぞれの府省庁の指揮命令に服している者（個々の勤務条件にもよるが、例えば、派遣労働者等）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。	1.1.1.2(2)(b)	<u>本統一基準は、行政事務従事者に適用される。本統一基準において</u> 「行政事務従事者」とは、政府職員及びそれぞれの府省庁の指揮命令に服している者のうち、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。	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
64	1.1.1.5 【か】	● 「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、利用状況等を考慮して、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。	1.1.1.5 【か】	● 「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。	表現 の適 正化
65	1.1.1.5 【か】	● 「記録媒体」とは、情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面、書類その他文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、 <u>CD-R</u> 、 <u>DVD</u> 、 <u>MO</u> 、 <u>USB</u> メモリ、フラッシュメモリ等の外部電磁的記録媒体がある。		● 「記録媒体」とは、情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面、書類その他文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、 <u>CD-R</u> 、 <u>DVD</u> 、 <u>MO</u> 、 <u>USB</u> メモリ、フラッシュメモリ等の外部電磁的記録媒体がある。	表現 の適 正化
66		(2.1.1.5へ移動)	1.1.1.4	● 「公開されたセキュリティホ	構成

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
			【か】	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・提供元等から公表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表されたセキュリティホールが該当する。	変更
67	1.1.1.5 【さ】	● 「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、本統一管理基準及び統一技術基準における「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。	1.1.1.4 【さ】	● 「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。	構成 変更
68	1.1.1.5 【さ】	● 「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	1.1.1.4 【さ】	● 「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	表現 の適 正化

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
		して、 <u>IC</u> カード等がある。		して、 <u>磁気ストライプカードやIC</u> カード等がある。	
69	1.1.1.5 【さ】	● 「省庁対策基準」とは、 <u>政府機関統一管理基準及び政府機関統一技術基準に準拠した、それぞれの府省庁における全ての</u> 情報資産に適用する情報セキュリティ対策の基準をいう。	1.1.1.4 【さ】	● 「省庁対策基準」とは、 <u>各府省庁のすべての</u> 情報資産に適用する情報セキュリティ対策の基準をいう。	表現の適正化
70	1.1.1.5 【さ】	● 「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、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面 <u>又は</u> 情報システムから出力した情報を記載した書面 <u>をいう。</u> ）及び情報システムに関する設計書が含まれる。	1.1.1.2(2)(a)	<u>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、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、<u>情報システムから出力した情報を記載した書面</u>）及び情報システムに関する設計書が含まれる。</u>	構成変更
71	1.1.1.5 【さ】	● 「 <u>情報の抹消</u> 」とは、 <u>廃棄した情報が漏えいすることを防止するために、全ての情報を復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態ではない。</u>		1.2.5.1(1)(a)(イ)、1.3.1.6(1)(a)の説明を集約	解説の集約
72		(削除)	1.1.1.4 【さ】	● 「 <u>政府職員</u> 」とは、 <u>人事発令を受けて行政事務に従事する者を</u>	構成変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				<u>いう。</u>	
73	1.1.1.5 【た】	● 「端末」とは、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。	1.1.1.4 【た】	● 「端末」とは、 <u>端末を利用する</u> 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。	表現 の適 正化
74	1.1.1.5 【た】	● 「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 <u>であり、物理的なものと論理的なものがある。</u>	1.1.1.4 【た】	● 「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 <u>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という。</u>	表現 の適 正化
75		(2.1.1.5へ移動)	1.1.1.4 【は】	● 「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、複数の方法の組合せにより主体認証を行う方法である。	構成 変更
76	1.1.1.5 【は】	● 「府省庁外」とは、 <u>行政事務従事者</u> の各々が所属する府省庁が管理する組織又は庁舎の外をいう。	1.1.1.4 【は】	● 「府省庁外」とは、 <u>政府職員</u> の各々が所属する府省庁が管理する組織又は庁舎の外をいう。	表現 の適 正化
77	1.1.1.5 【は】	● 「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	1.1.1.5 【は】	● 「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	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		び通信回線装置を問わず、 <u>行政事務従事者の各々が所属する</u> 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。		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。	
78	1.1.1.5 【は】	● 「府省庁外での情報処理」とは、 <u>行政事務従事者の各々が所属する</u> 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 <u>行政事務従事者</u> の各々が所属する府省庁の情報システムに接続して、 <u>情報処理</u> を行う場合だけでなく、オフラインで行う場合も含むものとする。	1.1.1.4 【は】	● 「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 <u>政府職員</u> の各々が所属する府省庁の情報システムに接続して、 <u>情報処置</u> を行う場合だけでなく、オフラインで行う場合も含むものとする。	表現 の適 正化
79	1.1.1.5 【は】	● 「府省庁支給以外の情報システム」とは、 <u>行政事務従事者</u> 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のほか、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。	1.1.1.4 【は】	● 「府省庁支給以外の情報システム」とは、 <u>政府職員</u> 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のほか、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。	表現 の適 正化
80	1.1.1.5 【は】	● 「府省庁支給以外の情報システムによる情報処理」とは、 <u>行政事務従事者の各々が所属する</u> 府省庁が <u>支給する情報システム</u> 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なく、それら装置等によって提供されているサービ	1.1.1.4 【は】	● 「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 <u>支給</u> 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	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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、例えば、 行政事務従事者の各々が所属する 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。		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、例えば、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。	
81	1.1.1.5 【は】	● 「府省庁内」とは、 行政事務従事者 の各々が所属する府省庁が管理する組織又は庁舎の内をいう。	1.1.1.4 【は】	● 「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組織又は庁舎の内をいう。	表現 の適 正化
82	1.1.1.5 【は】	● 「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、 行政事務従事者の各々が所属する 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。	1.1.1.4 【は】	「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。	表現 の適 正化
83	1.1.1.5 【は】	● 「抹消」→「情報の抹消」を参照。			解説 の集 約
84	1.1.1.4 【ま】	「明示等」とは、情報を取り扱う 全て の者が当該情報の格付について共通の認識となるように措置することをいう。なお、情報ごとに格付を記載することにより明示することを原則とするが、その他に	1.1.1.4 【ま】	「明示等」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、情報ごとに格付けを記載することにより明示することを原則とするが、そ	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		も、当該情報の格付に係る認識が共通となる措置については、明示等を含むものとする。例えば、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を規定等に明記し、当該情報システムを利用する全ての者に当該規定を周知することができていれば明示等を含むものとする。		の他にも、当該情報の格付けに係る認識が共通となる措置については、明示等を含むものとする。例えば、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ができていれば明示等を含むものとする。	
85		(2.1.1.5へ移動)	1.1.1.4 【ま】	● 「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。	構成 変更
86	1.2.1.1 趣旨	情報セキュリティ対策は、それに係る全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。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。 <u>具体的には、</u> ・最高情報セキュリティ責任者の設置とその役割 ・情報セキュリティ委員会の設置とその役割 ・情報セキュリティ監査責任者の	1.2.1.1 趣旨	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・体制を整備する必要がある。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。	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>設置とその役割</u> <ul style="list-style-type: none"> ・<u>情報セキュリティ責任者の設置とその役割</u> ・<u>情報システムセキュリティ責任者の設置とその役割</u> ・<u>情報システムセキュリティ管理者の設置とその役割</u> ・<u>課室情報セキュリティ責任者の設置とその役割</u> ・<u>最高情報セキュリティアドバイザーの設置とその役割</u> <u>についての遵守事項を定めるものである。</u>			
87	1.2.1.1(1)(a) 解説	解説： <u>それぞれの</u> 府省庁における情報セキュリティ対策の最高責任者を置くこと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 <u>取組</u> の推進や幹部の責任を持った関与が必須であり、 <u>それぞれの</u> 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 <u>管理</u> 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。	1.2.1.1(1)(a) 解説	解説： <u>各</u> 府省庁における情報セキュリティ対策の最高責任者を置くこと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 <u>取組み</u> の推進や幹部の責任を持った関与が必須であり、 <u>各</u> 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。	解説 の修 正
88	1.2.1.1(1)(b) 解説	解説：最高情報セキュリティ責任者は、 <u>それぞれの</u> 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、省庁対策基準の決定や	1.2.1.1(1)(b) 解説	解説：最高情報セキュリティ責任者は、 <u>各</u> 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、省庁対策基準の決定や評価結	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		評価結果による見直しに関する承認等を行う。		果による見直しに関する承認等を行う。	
89	1.2.1.1(2)(a) 解説	解説： <u>それぞれの府省庁における</u> 省庁対策基準の策定等を行う機能を持つ組織の設置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運用を統括する機能を持たせる等して、部門横断的な連携の仕組みを確立することが望まれる。	1.2.1.1(2)(a) 解説	解説： <u>各府省庁の</u> 省庁対策基準の策定等を行う機能を持つ組織の設置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 <u>各府省庁内での</u> 運用を統括する機能を持たせる等して、部門横断的な連携の仕組みを確立することが望まれる。	解説 の修 正
90	1.2.1.1(2)(b)	情報セキュリティ委員会は、 <u>統一管理基準に準拠して、</u> 情報セキュリティに関する省庁対策基準を策定し、最高情報セキュリティ責任者の承認を得ること。	1.2.1.1(2)(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対策基準を策定し、最高情報セキュリティ責任者の承認を得ること。 <u>ただし、あらかじめ最高情報セキュリティ責任者が認めた場合は、一部の技術的な事項について、指定した者に委任することができる。</u>	遵守 事項 の修 正
91	1.2.1.1(2)(b) 解説	解説：全省的に定めるべき省庁対策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。	1.2.1.1(2)(b) 解説	解説：全省的に定めるべき省庁対策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。 <u>ただし、あらかじめ最高情報セキュリティ責任者が認めた場合は、一部の技術的な事項（本統一基準の第2編に相当する事項）</u>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				<u>について、統括情報セキュリティ責任者等に委任することができる。なお、統括情報セキュリティ責任者等が委任に基づき基準を策定する場合は、情報セキュリティ委員会及び最高情報セキュリティ責任者に報告することが望ましい。</u>	
92	1.2.1.1(3)(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。	1.2.1.1(3)(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。	遵守 事項 の修 正
93	1.2.1.1(3)(a) 解説	<p>解説：<u>それぞれの</u>府省庁において策定した省庁対策基準に基づき監査を行う責任者を置くことを定めた事項である。</p> <p>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。</p> <p>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として置くことが望ましい。</p> <p>情報セキュリティ監査責任者は、<u>それぞれの</u>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。</p>	1.2.1.1(3)(a) 解説	<p>解説：<u>各</u>府省庁において策定した省庁対策基準に基づき監査を行う責任者を置くことを定めた事項である。</p> <p>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。</p> <p>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として置くことが望ましい。</p> <p>情報セキュリティ監査責任者は、<u>各</u>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。</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>情報セキュリティ監査責任者の業務を補佐するために、府省庁の内部及び外部の担当者を置く必要性を検討することが望まれる。また、業務の実効性を担保するために外部組織の活用も考えられる。</p> <p><u>なお、府省庁において、監査責任者を補佐する立場として監査副責任者等を独自に設置することを妨げるものではない。</u></p>		<p>情報セキュリティ監査責任者の業務を補佐するために、府省庁の内部及び外部の担当者を置く必要性を検討することが望まれる。また、業務の実効性を担保するために外部組織の活用も考えられる。</p>	
94	1.2.1.1(4)(a) 解説	<p>解説：組織内での役割の明確化のため、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決めることを定めた事項である。</p> <p>「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、<u>全て</u>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。</p>	1.2.1.1(4)(a) 解説	<p>解説：組織内での役割の明確化のため、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決めることを定めた事項である。</p> <p>「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、<u>すべて</u>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。</p>	解説 の修 正
95	1.2.1.1(4)(b)	<p><u>統括情報セキュリティ責任者は、最高情報セキュリティ責任者の指示に基づき、統一技術基準に準拠して、情報セキュリティに関する省庁対策基準における技術的側面の基準を策定すること。なお、当該基準の策定については、最高情</u></p>			遵守 事項 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>報セキュリティ責任者が指定した者に委任することができる。</u>			
96	1.2.1.1(4)(b) 解説	<u>解説：全省的に定めるべき省庁対策基準における技術的側面の基準策定に関する統括情報セキュリティ責任者の役割を定めた事項である。また、当該基準の策定については、最高情報セキュリティ責任者が指定した者に委任することができる。なお、情報セキュリティ責任者等が委任に基づき技術基準を策定する場合は、最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告することが望ましい。</u>			解説 の追 加
97	1.2.1.1(4)(d) 解説	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切な教育の不十分さを原因とする情報セキュリティの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、 <u>行政事務従事者</u> 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。	1.2.1.1(4)(c) 解説	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切な教育の不十分さを原因とする情報セキュリティの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、 <u>職員</u> 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。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		これには、転出に伴うアカウントの失効、情報システムへのアクセス権の変更の管理等も含まれる。		これには、転出に伴うアカウントの失効、情報システムへのアクセス権の変更の管理等も含まれる。	
98	1.2.1.1(4)(g)	統括情報セキュリティ責任者は、 <u>全ての</u> 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。	1.2.1.1(4)(g)	統括情報セキュリティ責任者は、 <u>すべての</u> 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。	表現の適正化
99	1.2.1.1(5)(a) 解説	<p>解説：各情報システムにおいて、計画、構築、運用等のライフサイクル全般を通じて必要となるセキュリティ対策の責任者を置くことを定めた事項である。</p> <p>情報システムの<u>セキュリティ要件</u>は計画段階において決定されることから、情報システムセキュリティ責任者は新規の情報システムについては計画段階までに置かなければならない。</p> <p>府省庁内 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<u>全ての</u>情報システムを、情報システム単位にセキュリティ対策の運用の責任の所在を明確にすることが重要である。</p> <p><u>なお、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にすること。</u></p>	1.2.1.1(5)(a) 解説	<p>解説：各情報システムにおいて、計画、構築、運用等のライフサイクル全般を通じて必要となる<u>情報</u>セキュリティ対策の責任者を置くことを定めた事項である。</p> <p>情報システムの<u>情報セキュリティ要件</u>は計画段階において決定されることから、情報システムセキュリティ責任者は新規の情報システムについては計画段階までに置かなければならない。</p> <p>府省庁内 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<u>すべての</u>情報システムを、情報システム単位に<u>情報</u>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。</p>	解説の修正
100	1.2.1.1(5)(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セキュリティ対策に関する事務を統括すること。	1.2.1.1(5)(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 <u>情報</u> セキュリティ対策に関する事務を統括すること。	表現の適正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
101	1.2.1.1(5)(d)	統括情報セキュリティ責任者は、 <u>全て</u> 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。	1.2.1.1(5)(d)	統括情報セキュリティ責任者は、 <u>すべて</u> 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。	表現 の適 正化
102	1.2.1.1(6)(a) 解説	解説：各情報システムにおいて、 その管理業務ごとのセキュリティ 対策の実施を管理する者を置くこ とを定めた事項である。 計画、構築、運用等の情報システ 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。	1.2.1.1(6)(a) 解説	解説：各情報システムにおいて、 その管理業務ごとの <u>情報</u> セキュリ ティ対策の実施を管理する者を置 くことを定めた事項である。 計画、構築、運用等の情報システ 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。	解説 の修 正
103	1.2.1.1(6)(d)	統括情報セキュリティ責任者は、 <u>全て</u> 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。	1.2.1.1(6)(d)	統括情報セキュリティ責任者は、 <u>すべて</u> 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。	表現 の適 正化
104	1.2.1.1(7)(a) 解説	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置 くことを定めた事項である。 課室情報セキュリティ責任者は、 所管する事務や <u>行政事務従事者</u> における情報の取扱い等に関して、 その是非を判断し、情報の持ち出 しや公開等についての責任を有す る者であり、課室長若しくはそれ に相当する者であることが望まし い。情報セキュリティ責任者が各 課室で1人任命し、統括情報セキ	1.2.1.1(7)(a) 解説	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置 くことを定めた事項である。 課室情報セキュリティ責任者は、 所管する事務や <u>職員</u> における情報 の取扱い等に関して、その是非を 判断し、情報の持ち出しや公開等 についての責任を有する者であ り、課室長若しくはそれに相当す る者であることが望ましい。情報 セキュリティ責任者が各課室で1 人任命し、統括情報セキュリティ	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		セキュリティ責任者に報告するものである。		責任者に報告するものである。	
105	1.2.1.1(7)(d)	統括情報セキュリティ責任者は、 <u>全て</u> 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。	1.2.1.1(7)(d)	統括情報セキュリティ責任者は、 <u>すべて</u> 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。	表現 の適 正化
106	1.2.1.1(8)(a) 解説	<p>解説：情報セキュリティに関する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を定めた事項である。</p> <p>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等の専門的な知識及び経験が必要となるため、省庁対策基準の策定・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。</p> <p>最高情報セキュリティアドバイザーについては、高度な国家安全保障、治安に係る分野においては、内部人材を充てることもできる。</p> <p>またこの場合、最高情報セキュリティアドバイザーは情報セキュリティ責任者等の各責任者を兼務することができる。</p> <p>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。この場合、CIO 補佐官に情報セキュリティ担当を設けることが望ましい。</p>	1.2.1.1(8)(a) 解説	<p>解説：情報セキュリティに関する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を定めた事項である。</p> <p><u>各</u>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等の専門的な知識及び経験が必要となるため、省庁対策基準の策定・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。</p> <p>最高情報セキュリティアドバイザーについては、高度な国家安全保障、治安に係る分野においては、内部人材を充てることもできる。</p> <p>またこの場合、最高情報セキュリティアドバイザーは情報セキュリティ責任者等の各責任者を兼務することができる。</p> <p>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。この場合、CIO 補佐官に情報セキュリティ担当を設けることが望ましい。</p>	解説 の修 正
107	1.2.1.2	情報セキュリティ対策に係る組織	1.2.1.2	情報セキュリティ対策に係る組織	趣旨

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
	趣旨	<p>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。また、承認や許可事案においては、情報セキュリティ対策に係る組織体制に加えて、職務上の権限等から、当該組織体制上の承認等を行う者の上司が承認等をすべき場合がある。</p> <p>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役割の割当てに関する対策基準として、兼務を禁止する役割、上司による承認・許可についての遵守事項を定める。</p>	趣旨	<p>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。また、承認や許可事案においては、情報セキュリティ対策に係る組織体制に加えて、職務上の権限等から、当該組織体制上の承認等を行う者の上司が承認等をすべき場合がある。</p> <p>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役割の割当てに関する対策基準を定める。</p>	の修 正
108	1.2.1.2(2)(b) 解説	<p>解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。例えば、機密性3情報、完全性2情報又は可用性2情報について、府省庁外での情報処理や府省庁支給以外の情報システムによる情報処理を課室情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得すること等が求められる。</p>	1.2.1.2(2)(b) 解説	<p>解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。例えば、機密性3情報、完全性2情報又は可用性2情報について、府省庁外での情報処理や府省庁支給以外の情報システムによる情報処理を課室情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得することなどが求められる。</p>	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
109	1.2.1.3 趣旨	<p>府省庁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、定められた手続に従って、適切に対処する必要がある。</p> <p>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の理由により、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すること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、定められた例外措置のための手続により、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。</p> <p>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として、違反への対処方法及び例外措置の適用方法についての遵守事項を定める。</p>	1.2.1.3 趣旨	<p><u>各</u>府省庁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、定められた手続に従って、適切に対処する必要がある。</p> <p>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の理由により、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すること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、定められた例外措置のための手続により、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。</p> <p>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。</p>	趣旨 の修 正
110	1.2.1.3(2)(b)	<p>行政事務従事者は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に例外措置の適用を申請すること。</p> <p>ただし、行政事務の遂行に緊急を要する等の場合であって、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直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。</p>	1.2.1.3(2)(b)	<p>行政事務従事者は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に例外措置の適用を申請すること。</p> <p>ただし、行政事務の遂行に緊急を要する等の場合であって、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直ちに採用すること又は規定を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。行政事務従</p>	遵守 事項 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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。		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。	
111	1.2.1.3(2)(b) (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 <u>該当</u> 箇所(規程名と条項等)	1.2.1.3(2)(b) (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 <u>適用</u> 箇所(規程名と条項等)	遵守事項の修正
112	1.2.1.3(2)(b) (オ)	例外措置の適用を終了した <u>旨</u> の報告方法	1.2.1.3(2)(b) (オ)	例外措置の適用を終了した <u>とき</u> の報告方法	遵守事項の修正
113	1.2.1.3(2)(c) (ウ)・	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 <u>該当</u> 箇所(規程名と条項等)	1.2.1.3(2)(c) (ウ)・	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 <u>適用</u> 箇所(規程名と条項等)	遵守事項の修正
114	1.2.1.3(2)(c) (ウ)解説	<p>解説：許可権限者に、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。</p> <p>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の<u>報告を受け、最高情報セキュリティ責任者は適用審査記録の台帳を整備することとなるが、これは、</u>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<u>全て</u>把握し、一貫性をもって取り消すために必要となる。</p> <p>(ア)の「役割名」には、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュ</p>	1.2.1.3(2)(c) (ウ)解説	<p>解説：許可権限者に、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。</p> <p>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、<u>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</u>把握し、一貫性をもって取り消すために必要となる。</p> <p>(ア)の「役割名」には、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュ</p>	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		リティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者又は課室情報セキュリティ責任者のいずれかを記載する。		セキュリティ管理者又は課室情報セキュリティ責任者のいずれかを記載する。	
115	1.2.1.3(2)(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、それを終了した時に、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。	1.2.1.3(2)(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権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。	遵守 事項 の修 正
116	1.2.1.3(2)(f) 解説	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すること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情報セキュリティの侵害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、情報セキュリティの侵害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等の対処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	1.2.1.3(2)(f) 解説	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すること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情報セキュリティの侵害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、情報セキュリティの侵害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処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	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		を集中して把握する必要がある。		のを集中して把握する必要がある。	
117	1.2.2.1 趣旨	<p>情報セキュリティ関係規程が<u>適切に整備されている</u>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、<u>全ての</u>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。</p> <p>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対策基準として、<u>統括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による教育体制の整備に係る規程及び行政事務従事者による教育の受講についての遵守事項</u>を定める。</p>	1.2.2.1 趣旨	<p>情報セキュリティ関係規程が<u>適正に策定された</u>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、<u>すべての</u>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。</p> <p>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対策基準を定める。</p>	趣旨 の修 正
118	1.2.2.1(1)(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 <u>の役割に応じて</u> 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。	1.2.2.1(1)(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 <u>に</u> 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。	遵守 事項 の修 正
119	1.2.2.1(1)(c)	統括情報セキュリティ責任者は、行政事務従事者 <u>の役割に応じて</u> 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に係る計画を企画 <u>及び</u> 立案するとともに	1.2.2.1(1)(c)	統括情報セキュリティ責任者は、行政事務従事者 <u>が</u> 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に係る計画を企画、 <u>立案</u> するとともに、その実	遵守 事項 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		に、その実施体制を整備すること。		施体制を整備すること。	
120	1.2.2.1(1)(c) 解説	解説：情報セキュリティ対策の教育の最低限の受講回数等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等、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。計画の作成に際しては、関係する教育計画を参照し、効率性に注意するとともに人材育成にも留意すること。	1.2.2.1(1)(c)解 説	解説：情報セキュリティ対策の教育の最低限の受講回数等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。計画の作成に際しては、関係する教育計画を参照し、効率性に注意するとともに人材育成にも留意すること。	表現 の適 正化
121	1.2.2.1(1)(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又は異動時に、その役割に応じて新しい職場等で3か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及び立案するとともに、その実施体制を整備すること。	1.2.2.1(1)(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か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、立案するとともに、その実施体制を整備すること。	遵守 事項 の修 正、 表現 の適 正化
122	1.2.2.1(1)(d) 解説	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等、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。	1.2.2.1(1)(d) 解説	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。	解説 の修 正
123	1.2.2.1(1)(g)	<u>課室情報セキュリティ責任者は、行政事務従事者に情報セキュリティ対策の教育を受講させること。</u>			遵守 事項 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
124	1.2.2.1(1)(g) 解説	<u>解説：課室情報セキュリティ責任者が、行政事務従事者に情報セキュリティ対策の教育を受講させる責務について定めた事項である。</u> <u>なお、例えば、受講時間を確保する等の行政事務従事者が受講できるための環境を整備することも必要である。</u>			解説の追加
125	1.2.2.1(1)(j) 【強化】から 【基本】へ移動	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 <u>必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。</u>	1.2.2.1(1)(i)	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。	遵守事項の修正、強化遵守事項から基本遵守事項への修正
126	1.2.2.1(1)(j) 解説 【強化】から 【基本】へ移動	解説：実際に情報セキュリティ対策のための <u>模擬的に</u> 事務を行うことにより、 <u>情報セキュリティ関係規程に係る知識・技能等を習得するために実施する訓練の内容及び体制を整備することを求める事項</u> である。 <u>なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられ</u>	1.2.2.1(1)(i) 解説	解説： <u>模擬的な状況において</u> 実際に情報セキュリティ対策のための事務を行うことにより、 <u>その</u> 知識・技能等 <u>の</u> 習得するために実施する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。 <u>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。</u>	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>る。その際には、統括情報セキュリテイ責任者は、指定した者より適宜報告を受けることが望ましい。</u>			
127	1.2.2.1(2)(b)	行政事務従事者は、着任時 <u>又は</u> 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。	1.2.2.1(2)(b)	行政事務従事者は、着任時、 <u>異動</u> 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。	表現 の適 正化
128	1.2.2.1(2)(b) 解説	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。	1.2.2.1(2)(b) 解説	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。 <u>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。</u>	解説 の修 正
129	1.2.2.1(2)(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。	1.2.2.1(2)(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 <u>と思</u> <u>われる</u> 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。	遵守 事項 の修 正
130	1.2.2.1(2)(d) 【強化】から 【基本】へ移動	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。			強化 遵守 事項 から 基本 遵守 事項 への

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
					修正
131	1.2.2.2 趣旨	<p>情報セキュリティに関する障害・事故等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、障害・事故等の影響や範囲を定められた責任者へ報告し、障害・事故等の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。</p> <p>これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準として、障害・事故等の発生に備えた事前準備、発生時における報告と応急措置、原因調査と再発防止策についての遵守事項を定める。</p>	1.2.2.2 趣旨	<p>情報セキュリティに関する障害・事故等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、障害・事故等の影響や範囲を定められた責任者へ報告し、障害・事故等の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。</p> <p>これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準を定める。</p>	趣旨 の修 正
132	1.2.2.2(1)(a) 解説	<p>解説：最高情報セキュリティ責任者に障害・事故等に対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配慮することが求められる。</p> <p>なお、情報セキュリティに関する障害・事故等とは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。</p> <p>また、「インシデント」とは、JIS Q 27002:2006 (ISO/IEC 17799:2005) における情報セキュ</p>	1.2.2.2(1)(a) 解説	<p>解説：最高情報セキュリティ責任者に障害・事故等に対する体制の整備を求める事項である。本事項が効果的に機能するように他の規程との整合性に配慮することが求められる。</p> <p>なお、情報セキュリティに関する障害・事故等とは、機密性、完全性、可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。</p> <p>また、「インシデント」とは、JIS Q 27002:2006 (ISO/IEC 17799:2005) におけるインシデン</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		リティインシデント と同意である。		ト と同意である。	
133	1.2.2.2(1)(b)	統括情報セキュリティ責任者は、障害・事故等について報告手順を整備し、当該報告手段を 全て の行政事務従事者に周知すること。	1.2.2.2(1)(b)	統括情報セキュリティ責任者は、障害・事故等について 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。	遵守 事項 の修 正
134	1.2.2.2(1)(b) 解説	解説：窓口についての周知は、情報セキュリティ対策の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 等 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。	1.2.2.2(1)(b)解 説	解説：窓口についての周知は、情報セキュリティ対策の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。	解説 の修 正
135	1.2.2.2(1)(c) 解説	解説：対処手順として障害・事故等の発生時に おいて 緊急を要する対処等の必要性に備えて、通常とは異なる例外措置の承認手続を設けることもあわせて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想される ため 、そのようなことがないよう検討すること。 対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を行政事務従事者が記録すべきことを定	1.2.2.2(1)(c) 解説	解説：対処手順として障害・事故等の発生時に おける 緊急を要する対処等の必要性に備えて、通常とは異なる例外措置の承認手続を設けることもあわせて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想される。 。 そのようなことがないよう検討すること。 対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を行政事務従事者が記録すべきことを定	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		めることも考えられる。		めることも考えられる。	
136	1.2.2.2(1)(d)	統括情報セキュリティ責任者は、 障害・事故等に備え、行政事務の 遂行のため特に重要と認めた情報 システムについて、緊急連絡先、 連絡手段、連絡内容を含む緊急連 絡網を整備すること。	1.2.2.2(1)(d)	統括情報セキュリティ責任者は、 障害・事故等に備え、行政事務の 遂行のため特に重要と認めた情報 システムについて、 <u>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</u> 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。	遵守 事項 の修 正
137	1.2.2.2(1)(d) 解説	解説：統括情報セキュリティ責任 者は、 <u>全ての</u> 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 <u>管理</u> 基 準 1.2.1.1）が、 <u>障害・事故等が発 生した場合に速やかに対応するた め、「緊急」連絡網を加えて整備す ることを定める事項である。</u> <u>緊急連絡網には、1.2.1.1において 整備を求める連絡網とは異なり、 該当する行政事務従事者の自宅や 携帯電話の番号等の個人情報を含 まれることも想定され、この場合、 それぞれの連絡網の取扱いが異な ることに注意する必要がある。な お、緊急連絡網には当該システム に係る責任者及び管理者のほか、 大規模な障害・事故等に備えて最 高情報セキュリティ責任者も含め る必要がある。</u>	1.2.2.2(1)(d) 解説	解説：統括情報セキュリティ責任 者は、 <u>すべての</u> 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 1.2.1.1）が、 <u>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。</u>	解説 の修 正
138	1.2.2.2(1)(e)	<u>統括情報セキュリティ責任者は、 障害・事故等への対処の訓練の必 要性を検討し、必要と判断した場</u>			遵守 事項 の追

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>合には、その訓練の内容及び体制を整備すること。</u>			加
139	1.2.2.2(1)(e) 解説	<u>解説：実際に障害・事故等への対処を模擬的に行うことにより、対応力を強化するために実施する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。</u> <u>なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。</u>			解説 の追 加
140	1.2.2.2(1)(f)	<u>行政事務従事者は、障害・事故等への対処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、障害・事故等への対処の訓練に参加すること。</u>			遵守 事項 の追 加
141	1.2.2.2(1)(f) 解説	<u>解説：行政事務従事者が、障害・事故等への対処の訓練に関する規定に従って、これに参加することを求める事項である。</u>			解説 の追 加
142	1.2.2.2(1)(g) 解説	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、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	1.2.2.2(1)(e) 解説	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	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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、連絡先を府省庁の外部に公表することを求める事項である。		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、連絡先を各府省庁の外部に公表することを求める事項である。	
143	1.2.2.2(a) 解説	解説：障害・事故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・事故等への対処を開始することができるようにすることを求める事項である。 <u>なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。</u>	1.2.2.2(a) 解説	解説：障害・事故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・事故等への対処を開始することができるようにすることを求める事項である。	解説 の修 正
144	1.2.3.1 趣旨	情報セキュリティ対策は、それに係る <u>全て</u> の行政事務従事者が、各自の役割を確実にを行うことで実効性が担保されるものであることから、 <u>全て</u> 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として、 <u>自己点検に関する年度計画の策定とその実施に関する準備、自己点検の実施、結果の評価及び自己点検に基づく改善についての遵守事項</u> を定める。	1.2.3.1 趣旨	情報セキュリティ対策は、それに係る <u>すべて</u> の行政事務従事者が、各自の役割を確実にを行うことで実効性が担保されるものであることから、 <u>すべて</u> 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。	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
145	1.2.3.1(1)(a) 解説	<p>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、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である。</p> <p>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。</p> <p>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。</p> <p>確認及び評価の方法については、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。</p> <p>実施項目の選択については、例えば、当初は<u>全て</u>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。</p>	1.2.3.1(1)(a) 解説	<p>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、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である。</p> <p>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。</p> <p>実施時期については、例えば、当初は毎月<u>10</u>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。</p> <p>確認及び評価の方法については、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。</p> <p>実施項目の選択については、例えば、当初は<u>すべて</u>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。</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		なお、行政事務従事者自らが行う自己点検を原則とするが、システムの仕組を用いてパッチやパターンファイルの更新状況を把握したり、実際の文書を確認することによりその整備状況を把握する等、自己点検と同等以上の信頼性を有する方法が存在する場合には、代替方法としてそれを採用しても良い。		なお、行政事務従事者自らが行う自己点検を原則とするが、システムの仕組を用いてパッチやパターンファイルの更新状況を把握したり、実際の文書を確認することによりその整備状況を把握する等、自己点検と同等以上の信頼性を有する方法が存在する場合には、代替方法としてそれを採用しても良い。	
146	1.2.3.1(4)(a) 解説	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、省庁対策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、客観性を持った評価とすることが望ましい。例えば、自己点検実施率や、省庁対策基準遵守率、要改善対策数/対策実施数等の準拠率の把握が挙げられる。	1.2.3.1(4)(a) 解説	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、省庁対策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、客観性を持った評価とすることが望ましい。例えば、自己点検実施率や、省庁対策基準遵守率、要改善対策数/対策実施数 <u>など</u> の準拠率の把握が挙げられる。	解説 の修 正
147	1.2.3.1(4)(c) 解説	解説：統括情報セキュリティ責任者は、自己点検の結果を最高情報セキュリティ責任者へ <u>報告</u> することを求める事項である。	1.2.3.1(4)(c) 解説	解説：統括情報セキュリティ責任者は、自己点検の結果を <u>報告書として文書化した上で</u> 、最高情報セキュリティ責任者へ <u>提出</u> することを求める事項である。	解説 の修 正
148	1.2.3.1(5)(a) 解説	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	1.2.3.1(5)(a) 解説	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	解説 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		セキュリティに関わる <u>全て</u> 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。		セキュリティに関わる <u>すべて</u> 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。	正
149	1.2.3.2 趣旨	<p>情報セキュリティの確保のためには、本統一<u>管理基準及び統一技術基準</u>に準拠して省庁対策基準が適切に策定され、かつ、情報セキュリティ関係規程が適切に運用さ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、その準拠性と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、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。</p> <p>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関する対策基準として、<u>監査計画の策定とその実施に関する指示、個別の監査業務における監査実施計画の策定、監査の実施に係る準備、監査の実施及びその結果に対する対処についての遵守事項</u>を定める。</p>	1.2.3.2 趣旨	<p>情報セキュリティの確保のためには、本統一基準に準拠して省庁対策基準が適切に策定され、かつ、情報セキュリティ関係規程が適切に運用さ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、その準拠性と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、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。</p> <p>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関する対策基準を定める。</p>	趣旨 の修 正
150	1.2.3.2(1)(a)解 説	<p>解説：監査の基本的な方針として、年度監査計画を策定し、承認を受けることを求める事項である。年度監査計画には、次の事項が含まれる。</p> <ul style="list-style-type: none"> ・重点とする監査対象及び監査目標（情報漏えい防止、不正アクセ 	1.2.3.2(1)(a) 解説	<p>解説：監査の基本的な方針として、年度監査計画を策定し、承認を受けることを求める事項である。年度監査計画には、次の事項が含まれる。</p> <ul style="list-style-type: none"> ・重点とする監査対象及び監査目標（情報漏えい防止、不正アクセ 	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>ス防止等)</p> <ul style="list-style-type: none"> ・ 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 <p>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、年度監査計画に盛り込むこと。</p>		<p>ス防止など)</p> <ul style="list-style-type: none"> ・ 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 <p>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、年度監査計画に盛り込むこと。</p>	
151	1.2.3.2(2)(b) 解説	<p>解説：年度監査計画において実施する監査以外に、府省庁内外における注目すべき事案の発生又は情報セキュリティ対策の実施内容について重大な変更が生じた場合に、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。</p>	1.2.3.2(2)(b) 解説	<p>解説：年度監査計画において実施する監査以外に、府省庁内、<u>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</u>が生じた場合に、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。</p> <p><u>なお、府省庁内において甚大な情報セキュリティの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が求められる。</u></p>	解説 の修 正
152	1.2.3.2(3)(a) 解説	<p>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策定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。(経済産業省情報セキュリティ監査基準 実施</p>	1.2.3.2(3)(a) 解説	<p>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策定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。(経済産業省情報セキュリティ監査基準 実施</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>基準ガイドライン Ver1.0 等を参考)</p> <ul style="list-style-type: none"> ・ 監査の実施時期 ・ 監査の実施場所 ・ 監査実施者及び担当職務の割当て ・ 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（実施している手続が有効な情報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 <p>なお、被監査部門に対し監査の内容や範囲を明確化するために、監査実施期間、監査実施者の氏名、監査対象等を含む事項に関して、情報セキュリティ監査責任者より事前通知することが望ましい。</p> <p>また、本統一管理基準においては、監査業務に対して監査を別途実施することを必須とはしてない。しかし、監査実施者が監査過程で被監査者を監査すること以外のことを実施した場合には、その実施に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、監査実施計画を策定する際は、監査実施</p>		<p>基準ガイドライン Ver1.0 等を参考)</p> <ul style="list-style-type: none"> ・ 監査の実施時期 ・ 監査の実施場所 ・ 監査実施者及び担当職務の割当て ・ 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 <p>なお、被監査部門に対し監査の内容や範囲を明確化するために、監査実施期間、監査実施者の氏名、監査対象等を含む事項に関して、情報セキュリティ監査責任者より事前通知することが望ましい。</p> <p>また、本統一基準においては、監査業務に対して監査を別途実施することを必須とはしてない。しかし、監査実施者が監査過程で被監査者を監査すること以外のことを実施した場合には、その実施に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、監査実施計画を策定する際は、監査実施者</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		者が実施することが情報セキュリティ対策の向上になり得ることや、何らかの作業を効率的に行えるとしても、それを安易に監査実施計画の中に取り込むべきではない。		が実施することが情報セキュリティ対策の向上になり得ることや、何らかの作業を効率的に行えるとしても、それを安易に監査実施計画の中に取り込むべきではない。	
153	1.2.3.2(4)(a) 解説	解説：情報セキュリティ監査責任者に、 <u>それぞれの</u> 府省庁において監査業務を実施するに当たり、必要となる者を情報セキュリティ監査実施者に指名することを求める事項である。 情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。 例えば、情報システムを監査する場合には、当該情報システムの構築をした者は、その監査をしないこととする。また、情報資産の運用状況に関する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とする。	1.2.3.2(4)(a) 解説	解説：情報セキュリティ監査責任者に、 <u>各</u> 府省庁において監査業務を実施するに当たり、必要となる者を情報セキュリティ監査実施者に指名することを求める事項である。 情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。 例えば、情報システムを監査する場合には、当該情報システムの構築をした者は、その監査をしないこととする。また、情報資産の運用状況に関する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とする。	解説 の修 正
154	1.2.3.2(4)(b)	情報セキュリティ監査責任者は、 <u>府省庁外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、府省庁外の者に監査の一部を請け負わせること。</u>	1.2.3.2(4)(b)	情報セキュリティ監査責任者は、 <u>必要に応じて</u> 、府省庁外の者に監査の一部を請け負わせること。	遵守 事項 の修 正
155	1.2.3.2(4)(b) 解説	解説：情報セキュリティ監査責任者に、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、府省庁内	1.2.3.2(4)(b) 解説	解説：情報セキュリティ監査責任者に、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、府省庁内	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>の情報システム部門に加えて外部専門家の支援を受けることを求める事項である。</p> <p>組織内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮し、外部委託に関する対策基準に従うこと。また、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<u>等</u>を考慮することが望ましい。</p>		<p>の情報システム部門に加えて外部専門家の支援を受けることを求める事項である。</p> <p>組織内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮し、外部委託に関する対策基準に従うこと。また、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<u>など</u>を考慮することが望ましい。</p>	
156	1.2.3.2(5)(b)	情報セキュリティ監査実施者は、省庁対策基準が統一 <u>管理基準及び統一技術基準</u> に準拠していることを確認すること。	1.2.3.2(5)(b)	情報セキュリティ監査実施者は、省庁対策基準が統一基準に準拠していることを確認すること。	遵守事項の修正
157	1.2.3.2(5)(b) 解説	解説：省庁対策基準が統一 <u>管理基準及び統一技術基準</u> に準拠して設計されていることの確認を求める事項である。	1.2.3.2(5)(b) 解説	解説：省庁対策基準が統一基準に準拠して設計されていることの確認を求める事項である。	解説の修正
158	1.2.3.2(5)(c) 解説	解説： <u>それぞれの</u> 府省庁における実施手順が省庁対策基準に準拠して設計されていることの確認を求める事項である。	1.2.3.2(5)(c) 解説	解説： <u>各</u> 府省庁の <u>実施</u> 手順が省庁対策基準に準拠して設計されていることの確認を求める事項である。	解説の修正
159	1.2.3.2(5)(d) 解説	解説：被監査部門における実際の運用が、 <u>それぞれの</u> 府省庁の情報セキュリティ関係規程に準拠して	1.2.3.2(5)(d) 解説	解説：被監査部門における実際の運用が、 <u>各</u> 府省庁の情報セキュリティ関係規程に準拠して実施され	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>実施されていること（運用の準拠性）の確認を求める事項である。運用の準拠性の確認は、自己点検の適正性の確認によることが実効性の高い方法であると考えられる。</p> <p>監査に当たっては、自己点検結果に基づく担当者への質問、記録文書の査閲、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かの妥当性を確認することも求められる。<u>例えば、監査対象によっては脆弱性検査、侵入検査等のその他の方法によっても確認することができる。</u></p>		<p>ていること（運用の準拠性）の確認を求める事項である。運用の準拠性の確認は、自己点検の適正性の確認によることが実効性の高い方法であると考えられるが、<u>監査対象によってはシステム監査、脆弱性検査などのその他の方法によっても確認することができる。</u></p> <p>監査に当たっては、自己点検結果に基づく担当者への質問、記録文書の査閲、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かの妥当性を確認することも求められる。</p>	
160	1.2.3.2(5)(e) 解説	<p>解説：<u>監査報告書</u>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。</p> <p>監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、<u>監査報告書に記載する監査意見</u>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実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料<u>のほか</u>、場合によっては組織の外部の第三者から入手した資料等を含むことがある。</p>	1.2.3.2(5)(e) 解説	<p>解説：<u>監査意見表明</u>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。</p> <p>監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、<u>監査意見表明</u>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実施者自らが直接に入手した資料や試験の結果<u>だけでなく</u>、被監査部門側から提出された資料<u>等を含み</u>、場合によっては組織の外部の第三者から入手した資料等を含むことがある。</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
161	1.2.3.2(5)(f) 解説	<p>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提出をすること求める事項である。</p> <p>なお、本監査は、省庁対策基準が統一<u>管理基準及び統一技術基準</u>に準拠しているか、実際の運用状況が情報セキュリティ関係規程に準拠して行われているか等、準拠性の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。</p>	1.2.3.2(5)(f) 解説	<p>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提出をすること求める事項である。</p> <p>なお、本監査は、省庁対策基準が統一基準に準拠しているか、実際の運用状況が情報セキュリティ関係規程に準拠して行われているか等、準拠性の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。</p>	解説 の修 正
162	1.2.3.2(6)(d) 解説	<p>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、課題とその改善に対する助言意見<u>等の指摘</u>を受けた場合には、既存の情報セキュリティ関係規程の見直しを検討することを求める事項である。</p> <p>検討の結果、情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。</p>	1.2.3.2(6)(d) 解説	<p>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、課題とその改善に対する助言意見<u>など</u>を受けた場合には、既存の情報セキュリティ関係規程の見直しを検討することを求める事項である。</p> <p>検討の結果、情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。</p>	表現 の適 正化
163	1.2.4.1(1)(a) 解説	<p>解説：情報セキュリティ関係規程を<u>整備した者</u>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を踏まえつつ、<u>情報セキュリティ対策に支障が生じないように見直しを行う時期</u>を判</p>	1.2.4.1(1)(a) 解説	<p>解説：情報セキュリティ関係規程の<u>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</u>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を踏まえつつ、セキュ</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>断する必要がある。</p> <p>情報セキュリティ関係規程を見直した者は、他部門へも影響があると思われる場合、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。</p>		<p>リティ対策に支障が<u>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</u>判断する必要がある。</p> <p><u>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、当該規定を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の有無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</u>、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。</p>	
164	1.2.5.1 趣旨	<p>府省庁外の者に情報処理業務を委託する場合 (外部の設備を利用した役務提供も含む) には、府省庁が委託先を直接管理することができないため、府省庁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。</p> <p>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 それぞれの 府省庁の省庁対策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定める必要がある。</p> <p>これらのことを勘案し、本項では、</p>	1.2.5.1 趣旨	<p>府省庁外の者に情報処理業務を委託する場合には、府省庁が委託先を直接管理することができないため、府省庁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。</p> <p>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 府省庁の省庁対策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定める必要がある。</p> <p>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。</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>外部委託に関する対策基準を定める。<u>具体的には、</u></p> <ul style="list-style-type: none"> ・<u>情報セキュリティ確保のための府省庁内共通の仕組みの整備</u> ・<u>委託先に実施させる情報セキュリティ対策の明確化</u> ・<u>委託先の選定</u> ・<u>外部委託に係る契約</u> ・<u>外部委託の実施における手続</u> ・<u>外部委託終了時の手続</u> <p><u>についての遵守事項を定めるものである。</u></p>			
165	1.2.5.1(1)(a) 解説	<p>解説：外部委託の対象としてよい範囲としてはいけない範囲を判断する基準を府省庁として整備することを定めた事項である。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。</p> <p><u>また、データの所在については、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。例えば、「行政機関の保有する個人情報の保護に関する法律」で定義する個人情報については、国内法が適用される場所に制限する必要があると判断すること等が考えられる。</u></p>	1.2.5.1(1)(a) 解説	<p>解説：外部委託の対象としてよい範囲としてはいけない範囲を判断する基準を府省庁として整備することを定めた事項である。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。</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
166	1.2.5.1(1)(b) 解説	<p>解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。</p> <p>統括情報セキュリティ責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、省庁対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。</p> <p>選定基準としては、<u>例えば</u>、委託先が<u>省庁対策基準</u>の該当項目を遵守し得る者であること、省庁対策基準と同等の情報セキュリティ管理体制を整備すること、<u>省庁対策基準</u>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。</p> <p>また、府省庁の情報セキュリティ水準を一定以上に保つために、<u>委託先</u>に対して要求すべき情報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。</p> <p>なお、本基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施に反映することが必要である。</p>	1.2.5.1(1)(b) 解説	<p>解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。</p> <p>統括情報セキュリティ責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、省庁対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。</p> <p>選定基準としては、委託先が省庁対策基準の該当項目を遵守し得る者であること、<u>各府省庁の省庁対策基準</u>と同等の情報セキュリティ管理体制を整備すること、<u>各府省庁の省庁対策基準</u>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。</p> <p>また、府省庁の情報セキュリティ水準を一定以上に保つために、<u>委託先職員</u>に対して要求すべき情報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。</p> <p>なお、本基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施に反映することが必要である。</p>	解説 の修 正
167	1.2.5.1(1)(c) 解説	<p>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。</p> <p>評価方法の整備には、<u>例えば</u>、</p>	1.2.5.1(1)(c) 解説	<p>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。</p> <p>評価方法の整備には、ISO/IEC</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		ISO/IEC 27001 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自己評価によるツール等の応用が考えられる。		27001 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自己評価によるツール等の応用が考えられる。	
168	1.2.5.1(2)(b) 解説	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の侵害発生時の対処方法を府省庁として整備することを定めた事項である。情報セキュリティの侵害の業務に対する影響度の大きさや機密性、完全性及び可用性の要求度に応じて、対処の緊急性等を考慮することが重要である。	1.2.5.1(2)(b) 解説	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の侵害発生時の対処方法を府省庁として整備することを定めた事項である。情報セキュリティの侵害の業務に対する影響度の大きさや機密性、完全性、可用性の要求度に応じて、対処の緊急性等を考慮することが重要である。	解説 の修 正
169	1.2.5.1(2)(c) 解説	解説：委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであること、及び履行が不十分である場合に速やかに適切な対処をすべきであることにかんがみ、これらのための方法の整備を求める事項である。 情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。 周知する情報セキュリティ監査の内容には、請け負わせる業務のうちで監査の対象とする範囲、実施者（府省庁が指定する第三者、委	1.2.5.1(2)(c) 解説	解説：委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであること、及び履行が不十分である場合に速やかに適切な対処をすべきであることにかんがみ、これらのための方法の整備を求める事項である。 情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。 周知する情報セキュリティ監査の内容には、請け負わせる業務のうちで監査の対象とする範囲、実施者（府省庁が指定する第三者、委	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>託先が選定する第三者、府省庁又は委託先において当該業務を行う部門とは独立した部門)、実施方法（情報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先候補の情報セキュリティポリシーとの整合性等を委託先候補が判断するために必要と考えられる事項を含める。</p> <p>情報セキュリティ対策の履行が不十分である場合の対処方法としては、<u>例えば</u>、府省庁及び委託先が改善について協議を行い、合意した改善策を実施させること等が考えられる。</p> <p>また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。</p>		<p>託先が選定する第三者、府省庁又は委託先において当該業務を行う部門とは独立した部門)、実施方法（情報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先候補の情報セキュリティポリシーとの整合性等を委託先候補が判断するために必要と考えられる事項を含める。</p> <p>情報セキュリティ対策の履行が不十分である場合の対処方法としては、府省庁及び委託先が改善について協議を行い、合意した改善策を実施させること等が考えられる。</p> <p>また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。</p>	
170	1.2.5.1(4)(b) (イ)解説	<p>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等の<u>提出</u>に関し定めた事項である。</p> <p>必要に応じて、当該委託業務に携わる委託先の者の特定や、当該者が実施する取組内容を、委託先に確認することが重要になる。</p> <p>特に、情報システムの構築及びソフトウェア開発等の外部委託の場</p>	1.2.5.1(4)(b) (イ)解説	<p>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等の<u>入手</u>に関し定めた事項である。</p> <p>必要に応じて、当該委託業務に携わる委託先の者の特定や、当該者が実施する取組内容を、委託先に確認することが重要になる。</p> <p>特に、情報システムの構築及びソフトウェア開発等の外部委託の場</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		合には、成果物における情報セキュリティ対策の実施が、その作成プロセスと不可分であることが想定されるため、遂行される業務全体の責任者を報告させることが重要である。		合には、成果物における情報セキュリティ対策の実施が、その作成プロセスと不可分であることが想定されるため、遂行される業務全体の責任者を報告させることが重要である。	
171	1.2.5.1(4)(d)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の提供する <u>役務</u> （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、選定基準及び選定手続に基づき、その是非を審査すること。	1.2.5.1(4)(d)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の提供する <u>サービス</u> （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、選定基準及び選定手続に基づき、その是非を審査すること。	遵守 事項 の修 正
172	1.2.5.1(4)(e)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先が <u>その役務内容を一部再委託する場合は、再委託されること</u> により生ずる脅威に対して情報セキュリティが十分に確保される措置を委託先に担保させること。	1.2.5.1(4)(e)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先が <u>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、再請負させること</u> により生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されると判断する場合は、その限りでない。	遵守 事項 の修 正
173	1.2.5.1(4)(e) 解説	解説： <u>委託先がその委託内容を再委託することは、セキュリティレベルの低下を招くことが懸念されることから原則として避けるべきである。一方、委託先がその委託内容を再委託する場合には、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保される措置を委託先に担保さ</u>	1.2.5.1(4)(e) 解説	解説： <u>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事項である。</u> <u>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、再請負をするべきではない。ただし、委託先から申請を受け、再請負を行うことが合理的であると認められる</u>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>せることを定めた事項である。</u> 情報セキュリティを十分に確保するためには、委託先<u>自体が業務を実施する場合に求めるべき水準と同一水準の情報セキュリティ対策を再委託先においても確保させる必要がある。</u></p>		<p><u>場合には、再請負させることにより生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されることを条件に再請負を認めるものとする。</u>情報セキュリティを十分に確保するためには、委託先を<u>選定する場合と同一観点から再請負先が委託契約の内容を遵守できる者であることを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確認し、再請負先に行わせる内容に応じて、委託先自体が実施する場合に求めるべき水準と同一水準の情報セキュリティ対策を実施させることを契約等に盛り込むよう委託先に求めることが必要である。</u> <u>また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めに</u> <u>ついて、契約する者に対して依頼すること。</u></p>	
174	1.2.5.1(5)(a) (ア)	委託先に情報を提供する場合は、安全な <u>受渡し</u> 方法によりこれを実施し、提供した記録を取得すること。	1.2.5.1(5)(a) (ア)	委託先に情報を提供する場合は、安全な <u>受渡</u> 方法によりこれを実施し、提供した記録を取得すること。	表現 の適 正化
175	1.2.5.1(5)(a) (イ)	外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消 <u>(全ての情報を復元が困難な状態にすることをいう。以下同</u>	1.2.5.1(5)(a) (イ)	外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消させること。	遵守 事項 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>じ。</u> させること。			
176	1.2.5.1(5)(a) (イ)解説	<p>解説：委託契約開始から終了に至るまでに行う委託先への情報の提供を必要最小限に止め、また、提供に伴う要保護情報の漏えいや滅失等を防止するための措置の実施を求める事項である。</p> <p>委託先への情報の提供における遵守事項は、本統一管理基準の「1.3.1.4 情報の移送」及び「1.3.1.5 情報の提供」の定めに基づき、例えば機密性3情報を提供する場合には、当該外部委託について責任を負う情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること、また、機密性2情報を提供する場合には、これらの者のいずれかに届け出ることが必要となる。</p> <p>委託先の選定基準や情報セキュリティの侵害時の対処方法を整備した上で、当事者間の情報の授受において上記の措置に従うことにより情報セキュリティを確保することが重要である。</p>	1.2.5.1(5)(a) (イ)解説	<p>解説：委託契約開始から終了に至るまでに行う委託先への情報の提供を必要最小限に止め、また、提供に伴う要保護情報の漏えいや滅失等を防止するための措置の実施を求める事項である。</p> <p>委託先への情報の提供における遵守事項は、本統一基準の「1.3.1.4 情報の移送」及び「1.3.1.5 情報の提供」の定めに基づき、例えば機密性3情報を提供する場合には、当該外部委託について責任を負う情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること、また、機密性2情報を提供する場合には、これらの者のいずれかに届け出ることが必要となる。委託先の選定基準や情報セキュリティの侵害時の対処方法を整備した上で、当事者間の情報の授受において上記の措置に従うことにより情報セキュリティを確保することが重要である。</p>	解説 の修 正
177	1.2.5.1(5)(b)	<p>情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、<u>取り交わした契約</u>の対処方法に従い、委託先に必要な措置を講じさせること。</p>	1.2.5.1(5)(b)	<p>情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、<u>定められた</u>対処方法に従い、委託先に必要な措置を講じさせること。</p>	遵守 事項 の修 正
178	1.2.5.1(5)(c)	情報システムセキュリティ責任者	1.2.5.1(5)(c)	情報システムセキュリティ責任者	遵守

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		又は課室情報セキュリティ責任者は、 取り交わした契約の対処方法 に従い、委託先における情報セキュリティ対策の履行状況を確認すること。		又は課室情報セキュリティ責任者は、 定められた方法 に従い、委託先における情報セキュリティ対策の履行状況を確認すること。	事項 の修 正
179	1.2.5.2 趣旨	府省庁においては、「中央省庁業務継続ガイドライン 第1版」(平成19年6月、内閣府)に基づき、業務の継続に重大な支障を来し、あるいは国民の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。他方では、業務継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、 それぞれの 府省庁の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。 これらのことを勘案し、本項では、業務継続計画と情報セキュリティ対策の整合的運用の確保 及び不整合の報告 に関する対策基準を定める。	1.2.5.2 趣旨	各 府省庁においては、「中央省庁業務継続ガイドライン 第1版」(平成19年6月、内閣府)に基づき、業務の継続に重大な支障を来し、あるいは国民の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。他方では、業務継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、 各 府省庁の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。 これらのことを勘案し、本項では、業務継続計画と情報セキュリティ対策の整合的運用の確保に関する対策基準を定める。	趣旨 の修 正
180	1.2.5.2(1)(a) 解説	解説：業務継続計画と省庁対策基準は、特定の事態に対して、それぞれの体系において定められることがあり得る。当該事態の例とし	1.2.5.2(1)(a) 解説	解説：業務継続計画と省庁対策基準は、特定の事態に対して、それぞれの体系において定められることがあり得る。当該事態の例とし	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>て、情報システムの稼働を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画及び省庁対策基準のそれぞれで定める対策に矛盾があると、双方の遵守を求められる府省庁組織及び行政事務従事者は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画と省庁対策基準の間で整合性を確保するよう検討を行うことが必要である。</p> <p>本統一管理基準の 1.2.1.1 項で情報セキュリティ委員会は省庁対策基準の策定を求められているが、その策定及び見直しの際に、府省庁が業務継続計画で定め、又は定めることが予定されている要求事項を情報セキュリティ委員会が把握した上で、業務継続計画の整備計画を担当する者と協議し双方の定めを調整する必要がある。また、業務継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が省庁対策基準に影響するかどうかを確認し、必要があれば、省庁対策基準の改訂を行う等して、業務継続計画との整合の確保に努めなければならない。</p>		<p>て、情報システムの稼働を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画及び省庁対策基準のそれぞれで定める対策に矛盾があると、双方の遵守を求められる府省庁組織及び職員は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画と省庁対策基準の間で整合性を確保するよう検討を行うことが必要である。</p> <p>本統一基準の 1.2.1.1 項で情報セキュリティ委員会は省庁対策基準の策定を求められているが、その策定及び見直しの際に、府省庁が業務継続計画で定め、又は定めることが予定されている要求事項を情報セキュリティ委員会が把握した上で、業務継続計画の整備計画を担当する者と協議し双方の定めを調整する必要がある。また、業務継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が省庁対策基準に影響するかどうかを確認し、必要があれば、省庁対策基準の改訂を行うなどして、業務継続計画との整合の確保に努めなければならない。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
181	1.2.5.2(1)(b)	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課室情報セキュリティ責任者は、府省庁において業務継続計画の整備計画がある場合には、 <u>全て</u> の情報システムについて、当該業務継続計画との関係の有無を検討すること。	1.2.5.2(1)(b)	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課室情報セキュリティ責任者は、府省庁において業務継続計画の整備計画がある場合には、 <u>すべて</u> の情報システムについて、当該業務継続計画との関係の有無を検討すること。	趣旨 の修 正
182	1.2.5.2(1)(c) (ア)解説	解説：例えば、事態発生時には、業務の継続以外の対応として、府省庁の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障をきたすおそれがある。このため、セキュリティ確保の面で配慮を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、施設全体の入館管理だけでなく、各執務室や各 <u>行政事務従事者</u> の卓上の <u>情報</u> セキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。 また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ず	1.2.5.2(1)(c) (ア)解説	解説：例えば、事態発生時には、業務の継続以外の対応として、府省庁の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障をきたすおそれがある。このため、セキュリティ確保の面で配慮を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、施設全体の入館管理だけでなく、各執務室や各 <u>職員</u> の卓上のセキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。 また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ず	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		る必要がある。			
183	1.2.5.2(1)(c) (イ)解説	<p>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課室情報セキュリティ責任者に、業務継続計画と自らが担当する実施手順の整合性の確保を求める事項である。整合性を確保するための対応には、通常時の運用において実施するものと、事態発生時に実施するものがある。事態発生への対応として、業務継続計画及び省庁対策基準のそれぞれにおいて事態発生時における情報システムの稼働水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対策を実施手順において具体的に定める等が想定される。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。</p> <p>これらの目標及び対策を業務継続計画及び情報セキュリティ関係規程の双方で定めることとなるため、相互の整合性を確保するための規定の整備が必要となる。</p> <p>また、事態発生時には、情報シス</p>	1.2.5.2(1)(c) (イ)解説	<p>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課室情報セキュリティ責任者に、業務継続計画と自らが担当する実施手順の整合性の確保を求める事項である。整合性を確保するための対応には、通常時の運用において実施するものと、事態発生時に実施するものがある。事態発生への対応として、業務継続計画及び省庁対策基準のそれぞれにおいて事態発生時における情報システムの稼働水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対策を実施手順において具体的に定める等が想定される。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。</p> <p>これらの目標及び対策を業務継続計画及び情報セキュリティ関係規程の双方で定めることとなるため、相互の整合性を確保するための規定の整備が必要となる。</p> <p>また、事態発生時には、情報シス</p>	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>システムの主体認証情報（パスワード）を設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。しかしながら、個人が管理しているパスワードの共用（共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。このため、個人が管理しているパスワードを聞き出したり、共用するために管理者において控えを管理する手順を業務継続計画で安易に認めるべきではなく、これに代わる手順を十分検討する必要がある。</p> <p>手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、ついで、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生時</p>		<p>システムの主体認証情報（パスワード）を設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。しかしながら、個人が管理しているパスワードの共用（共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認などが不十分となることも想定される。このため、個人が管理しているパスワードを聞き出したり、共用するために管理者において控えを管理する手順を業務継続計画で安易に認めるべきではなく、これに代わる手順を十分検討する必要がある。</p> <p>手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、ついで、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時に</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容を記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。		は、その紙面を参照し事態発生時のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容を記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。	
184	1.2.5.2(2)(a)	行政事務従事者は、府省庁において業務継続計画の整備計画がある場合であって、業務継続計画と情報セキュリティ関係規程が定める要求事項との違い <u>等</u> により、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。	1.2.5.2(2)(a)	行政事務従事者は、府省庁において業務継続計画の整備計画がある場合であって、業務継続計画と情報セキュリティ関係規程が定める要求事項との違い <u>など</u> により、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。	表現 の適 正化
185	1.3.1.1 趣旨	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	1.3.1.1 趣旨	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	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>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、<u>全ての</u>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。</p> <p>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として、<u>業務以外の情報の作成又は入手における格付と取扱制限の決定、格付と取扱制限の明示等、格付と取扱制限の加工時における継承についての遵守事項</u>を定める。</p>		<p>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、<u>すべての</u>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。</p> <p>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。</p>	
186	1.3.1.1(2)	情報の作成又は入手時における <u>格付</u> と取扱制限の決定	1.3.1.1(2)	情報の作成又は入手時における <u>格付け</u> と取扱制限の決定	表現の適正化
187	1.3.1.1(2)(a)	行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に <u>格付</u> 及び取扱制限の定義に基づき、 <u>格付</u> 及び取扱制限を決定すること。	1.3.1.1(2)(a)	行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に <u>格付け</u> 及び取扱制限の定義に基づき、 <u>格付け</u> 及び取扱制限を決定すること。	表現の適正化
188	1.3.1.1(2)(a) 解説	<p>解説：作成又は入手した情報について、以降、適切な<u>情報</u>セキュリティ<u>対策が実施される</u>ように、機密性、完全性、可用性の<u>格付</u>及び取扱制限を<u>決定する</u>ことを求める事項である。</p> <p>情報の<u>格付</u>が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障</p>	1.3.1.1(2)(a) 解説	<p>解説：作成又は入手した情報について、以降、適切なセキュリティ<u>管理が施される</u>ように、機密性、完全性、可用性の<u>格付け</u>及び取扱制限を<u>行う</u>ことを求める事項である。</p> <p>情報の<u>格付け</u>が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障</p>	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>害・事故等の直接の原因となった人物のほか、情報の格付及び明示等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、情報の格付及び取扱制限とその明示等を確実にすることは重要である。</p> <p>なお、格付及び取扱制限の決定をする際は、要件に過不足が生じないように十分注意しなければならない。格付及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなって事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを行政事務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。</p> <p>特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。</p> <p>例えば、本来要機密情報とする情報を要機密情報に格付けないことは不適切であるが、逆に、本来要機密情報ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けるこ</p>		<p>障害・事故等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等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、情報の格付け及び取扱制限とその明示等を確実にすることは重要である。</p> <p>なお、格付け及び取扱制限の決定をする際は、要件に過不足が生じないように十分注意しなければならない。格付け及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなって事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを行政事務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。</p> <p>特に、格付け及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。</p> <p>例えば、本来要機密情報とする情報を要機密情報に格付けないことは不適切であるが、逆に、本来要機密情報ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けるこ</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>とも不適切であることに注意すること。</p> <p>また、取扱制限については必要性の有無を検討し、その結果指定しないという<u>決定を行っても</u>差し支えない。</p> <p>電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、<u>格付</u>及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した<u>格付</u>及び取扱制限に基づき、その指定を行うこと。</p> <p><u>なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。</u></p>		<p>とも不適切であることに注意すること。</p> <p>また、取扱制限については必要性の有無を検討し、その結果指定しないという<u>決定でも</u>差し支えない。</p> <p>電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、<u>格付け</u>及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した<u>格付け</u>及び取扱制限に基づき、その指定を行うこと。</p>	
189	1.3.1.1(2)(b)	<p>行政事務従事者は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の<u>格付</u>及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。</p>	1.3.1.1(2)(b)	<p>行政事務従事者は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の<u>格付け</u>及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。</p>	表現 の適 正化
190	1.3.1.1(2)(b) 解説	<p>解説：元の情報の修正、追加、削除のいずれかにより、<u>格付</u>又は取扱制限を変更する必要性が生じた場合には、<u>格付</u>及び取扱制限の再決定を行う必要がある。</p> <p>例えば、以下のような場合が考えられる。</p> <ul style="list-style-type: none"> ・機密性の低い情報に機密性の高 	1.3.1.1(2)(b) 解説	<p>解説：元の情報の修正、追加、削除のいずれかにより、<u>格付け</u>又は取扱制限を変更する必要性が生じた場合には、<u>格付け</u>及び取扱制限の再決定を行う必要がある。</p> <p>例えば、以下のような場合が考えられる。</p> <ul style="list-style-type: none"> ・機密性の低い情報に機密性の高 	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>い情報を追加したことによって、情報の機密性が上がる場合</p> <ul style="list-style-type: none"> ・機密性の高い情報から機密に該当する部分を削除したことによって、情報の機密性が下がる場合 <p>なお、情報の格付及び取扱制限は、省庁対策基準に沿った対策を適正に実施するための基礎となる重要な事項であることについては、前記のとおりである。このため、これらを変更するに当たっても適正な手続により実施する必要がある。情報の格付及び取扱制限の変更には、大別して再決定と見直しがある。</p> <p>再決定した場合には、再決定後の新たな格付等の決定者は再決定した者となる。見直しについては、1.3.1.2 情報の利用 (4) を参照のこと。</p>		<p>い情報を追加したことによって、情報の機密性が上がる場合</p> <ul style="list-style-type: none"> ・機密性の高い情報から機密に該当する部分を削除したことによって、情報の機密性が下がる場合 <p>なお、情報の格付け及び取扱制限は、省庁対策基準に沿った対策を適正に実施するための基礎となる重要な事項であることについては、前記のとおりである。このため、これらを変更するに当たっても適正な手続により実施する必要がある。情報の格付け及び取扱制限の変更には、大別して再決定と見直しがある。</p> <p>再決定した場合には、再決定後の新たな格付け等の決定者は再決定した者となる。見直しについては、1.3.1.2 情報の利用 (4) を参照のこと。</p>	
191	1.3.1.1(3)	格付と取扱制限の明示等	1.3.1.1(3)	格付けと取扱制限の明示等	表現の適正化
192	1.3.1.1(3)(a)	行政事務従事者は、情報の格付及び取扱制限を決定（再決定を含む。以下同じ。）した際に、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等すること。	1.3.1.1(3)(a)	行政事務従事者は、情報の格付け及び取扱制限を決定（再決定を含む。以下同じ。）した際に、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等すること。	表現の適正化
193	1.3.1.1(3)(a) 解説	解説：作成者又は入手者によって格付及び取扱制限が決定された情報に対して、以降、他者が当該情報を利用する際に必要とされる情	1.3.1.1(3)(a) 解説	解説：作成者又は入手者によって格付け及び取扱制限が決定された情報に対して、以降、他者が当該情報を利用する際に必要とされる	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>報セキュリティ対策の内容を示すため、情報の格付及び取扱制限の明示等を行うことを求める事項である。「明示等」とは、情報を取り扱う<u>全て</u>の者が当該情報の格付及び取扱制限について共通の認識となるように措置することをいい、情報ごとの格付の区分及び取扱制限の種類を当該情報に記載することによる明示を原則とする。なお、格付の区分及び取扱制限の種類を記載していたとしても、当該ファイルを参照する者が、その内容を参照する際に格付の区分及び取扱制限の種類を特段の手順なく視認することができない状態（例えば、文書ファイルのプロパティ設定に格付の区分を記載することや、文章閲覧時に画面表示はされず印刷しかされないヘッダ部分に記載すること等）については、記載しても明示に当たらない。</p> <p>格付及び取扱制限の明示等は、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、外部電磁的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外部電磁的記録媒体に、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、それぞれ記載する必要がある。</p>		<p>セキュリティ対策の内容を示すため、情報の格付け及び取扱制限の明示等を行うことを求める事項である。「明示等」とは、情報を取り扱う<u>すべて</u>の者が当該情報の格付け及び取扱制限について共通の認識となるように措置することをいい、情報ごとの格付けの区分及び取扱制限の種類を当該情報に記載することによる明示を原則とする。なお、格付けの区分及び取扱制限の種類を記載していたとしても、当該ファイルを参照する者が、その内容を参照する際に格付けの区分及び取扱制限の種類を特段の手順なく視認することができない状態（例えば、文書ファイルのプロパティ設定に格付けの区分を記載することや、文章閲覧時に画面表示はされず印刷しかされないヘッダ部分に記載することなど）については、記載しても明示に当たらない。</p> <p>格付け及び取扱制限の明示等は、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、外部電磁的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外部電磁的記録媒体に、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、それぞれ記載する必要がある。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>既に書面として存在している情報に対して<u>格付</u>や取扱制限を明示等する場合には、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等すべきであるが、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等することも可能である。</p> <p>なお、<u>格付</u>及び取扱制限の明示等とあわせて、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。</p> <p>明示等を<u>行うに当たっては、格付</u>の区分及び取扱制限の種類を記載することによる明示が原則であるが、<u>以下のような場合に明示等を簡便化してもよい。</u></p> <p>① <u>格付</u>及び取扱制限の明示等を簡便化<u>できる場合</u></p> <p>特定の情報（例えば、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<u>格付</u>及び取扱制限を規定等により明記し、当該情報にアクセスする<u>全ての者に当該規定を周知している場合は、格付</u>の区分及び取扱制限の種類について記載することを省略することができる。<u>具体的な例としては、次のような場合が考えられる。</u></p>		<p>る。</p> <p>既に書面として存在している情報に対して<u>格付け</u>や取扱制限を明示等する場合には、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等すべきであるが、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等することも可能である。</p> <p>なお、<u>格付け</u>及び取扱制限の明示等とあわせて、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。</p> <p>明示等を<u>行なうには、格付け</u>の区分及び取扱制限の種類を記載することによる明示が原則であるが、<u>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その認識が周知徹底されている場合は、以下のよう記載以外の方法で簡便化してもよい。</u></p> <p>① <u>格付け</u>及び取扱制限の明示等の簡便化</p> <p>特定の情報（例えば、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<u>格付け</u>及び取扱制限を規定等により明記し、当該情報にアクセスするすべ</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>・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の区分及び取扱制限を規定等により明記し、当該情報システムの利用者にあらかじめ周知している場合。</p> <p>・取り扱う情報の格付が機密性1、完全性1、可用性1の場合には、記載による明示を簡便化できることを規定等により周知している場合。</p> <p>ただし、格付及び取扱制限の明示等を簡便化した場合には、以下の事項に注意する必要がある。</p> <p><u>格付及び取扱制限の明示等を簡便化した場合の注意事項</u></p> <p>① <u>格付及び取扱制限の決定を認識できない者への情報の提供</u> 格付の区分及び取扱制限の種類が記載されていない要保護情報を、格付及び取扱制限の決定内容を認識できない行政事務従事者に提供する必要がある場合（例えば、他府省庁に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限の種類を記載した上で提供しなければならない。</p> <p>② <u>取扱制限の明示等を簡便化した場合における取扱制限の追加・変更</u> 例えば、簡便化に係る規定等により、特定の文書ファイルについて、</p>		<p>ての者に当該規定を周知することによって、格付けの区分及び取扱制限の種類を記載することを省略することができる。</p> <p>② <u>格付け及び取扱制限の決定を認識できない者への提供</u> 格付けの区分及び取扱制限の種類が記載されていない情報に対する格付け及び取扱制限の決定内容を認識していない行政事務従事者に当該情報を提供する必要がある場合（例えば、他府省庁に情報を提供等する場合）は、当該情報に格付けの区分及び取扱制限の種類を記載した上で提供しなければならない。</p> <p>③ <u>取扱制限の明示等を簡便化した場合における取扱制限の追加・変更</u> 例えば、簡便化に係る規定等により、特定の文書ファイルについて、取扱制限の種類を記載することを省略している場合、当該ファイルのうち一部のファイルについて取扱制限を追加するときは、追加する取扱制限の種類のみを記載し、逆に取扱制限を解除するときは、当該解除する取扱制限を「送信可」「印刷可」などのように記載することが想定される。</p> <p>ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できな</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>取扱制限の種類の記事を省略している場合において、当該ファイルのうち一部のファイルについて取扱制限を追加するときは、追加する取扱制限の種類のみを記載すること。また、取扱制限を解除する場合は、当該解除する取扱制限を「送信可」「印刷可」等のように記載することが考えられる。</u></p> <p>ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記すること。</p>		<p>い場合には、文章の先頭ページに明記すること。</p>	
194	1.3.1.1(4)	格付と取扱制限の加工時における継承	1.3.1.1(4)	格付けと取扱制限の加工時における継承	表現の適正化
195	1.3.1.1(4)(a)	行政事務従事者は、情報を作成する際に、参照した情報又は入手した情報が既に格付又は取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。	1.3.1.1(4)(a)	行政事務従事者は、情報を作成する際に、参照した情報又は入手した情報が既に格付け又は取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付け及び取扱制限を継承すること。	表現の適正化
196	1.3.1.1(4)(a) 解説	解説：作成の際に参照した情報又は入手した情報が既に機密性に係る格付又は取扱制限の指定がされている場合には、元となる格付及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、引用した新たな情報において適切な格付及び取扱制限を決定すること。	1.3.1.1(4)(a) 解説	解説：作成の際に参照した情報又は入手した情報が既に機密性に係る格付け又は取扱制限の指定がされている場合には、元となる格付け及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、引用した新たな情報において適切な格付け及び取扱制限を決定すること。	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				と。	
197	1.3.1.2 趣旨	行政事務においては、その遂行のために多くの情報を利用するが、利用者の認識不足等により情報を不適切に取り扱くと、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。このリスクに対応するため、行政事務の遂行において、情報は、 <u>格付</u> 等に応じて定められた手続に従い、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、情報の利用に関する対策基準として、 <u>業務以外の利用の禁止、格付及び取扱制限に従った情報の取扱い、格付及び取扱制限の複製時における継承、格付及び取扱制限の見直し、要保護情報の取扱いについての遵守事項</u> を定める。	1.3.1.2 趣旨	行政事務においては、その遂行のために多くの情報を利用するが、利用者の認識不足等により情報を不適切に取り扱くと、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。このリスクに対応するため、行政事務の遂行において、情報は、 <u>格付け</u> 等に応じて定められた手続に従い、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、情報の利用に関する対策基準を定める。	趣旨 の修 正
198	1.3.1.2(2)	<u>格付</u> 及び取扱制限に従った情報の取扱い	1.3.1.2(2)	<u>格付け</u> 及び取扱制限に従った情報の取扱い	表現 の適 正化
199	1.3.1.2(2)(a)	行政事務従事者は、利用する情報に明示等された <u>格付</u> に従って、当該情報を適切に取り扱うこと。 <u>格付</u> に加えて取扱制限の明示等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。	1.3.1.2(2)(a)	行政事務従事者は、利用する情報に明示等された <u>格付け</u> に従って、当該情報を適切に取り扱うこと。 <u>格付け</u> に加えて取扱制限の明示等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。	表現 の適 正化
200	1.3.1.2(2)(a) 解説	解説：情報に明示等された <u>格付</u> 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。	1.3.1.2(2)(a) 解説	解説：情報に明示等された <u>格付け</u> 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。	解説 の修 正
201	1.3.1.2(3)	<u>格付</u> 及び取扱制限の複製時にお	1.3.1.2(3)	<u>格付け</u> 及び取扱制限の複製時にお	表現

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		る継承		ける継承	の適 正化
202	1.3.1.2(3)(a)	行政事務従事者は、情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。	1.3.1.2(3)(a)	行政事務従事者は、情報を複製する場合には、元となる情報の機密性に係る格付け及び取扱制限を継承すること。	表現 の適 正化
203	1.3.1.2(3)(a) 解説	解説：複製の際に元となる情報が既に機密性に係る格付又は取扱制限の明示等がされている場合には、元となる格付及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、複製した新たな情報において適切な格付及び取扱制限を決定すること。	1.3.1.2(3)(a) 解説	解説：複製の際に元となる情報が既に機密性に係る格付け又は取扱制限の明示等がされている場合には、元となる格付け及び取扱制限を継承し、同一情報について一貫した対策を維持することを求める事項である。なお、完全性及び可用性については、複製した新たな情報において適切な格付け及び取扱制限を決定すること。	解説 の修 正
204	1.3.1.2(4)	格付及び取扱制限の見直し	1.3.1.2(4)	格付け及び取扱制限の見直し	表現 の適 正化
205	1.3.1.2(4)(a)	行政事務従事者は、情報を利用する場合に、元の格付又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付又は取扱制限そのものを見直す必要があると思料する場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下この項において「決定者等」という。）に相談すること。	1.3.1.2(4)(a)	行政事務従事者は、情報を利用する場合に、元の格付け又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付け又は取扱制限そのものを見直す必要があると思料する場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下、この項において「決定者等」という。）に相談すること。	表現 の適 正化
206	1.3.1.2(4)(a) 解説	解説：利用する元の情報への修正、追加、削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適切と考える場合に	1.3.1.2(4)(a) 解説	解説：利用する元の情報への修正、追加、削除のいずれでもないが、元の格付け又は取扱制限そのものがその時点で不適切と考える場合に	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>は、<u>格付</u>又は取扱制限の見直しについてその決定者に確認を求める必要がある。</p> <p>また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は同人の上司に相談し、その是非を検討することになる。</p> <p>ただし、元の決定者等のいずれかによる再決定がない限り、当該情報の利用者がそれらの者に無断で、<u>格付</u>又は取扱制限を変更することは許されない。</p> <p>見直しにより元の決定者等に相談することが必要となる例として以下のような場合が考えられる。</p> <ul style="list-style-type: none"> ・作成時には非公開だった情報が正規の手続によって公開されることで機密性が失われた場合（時間の経過により変化した場合） ・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合 ・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合 ・<u>格付</u>及び取扱制限を決定した時の判断が不適切であったと考えられる場合 ・<u>行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等に</u> 		<p>には、<u>格付け</u>又は取扱制限の見直しについてその決定者に確認を求める必要がある。</p> <p>また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は同人の上司に相談し、その是非を検討することになる。</p> <p>ただし、元の決定者等のいずれかによる再決定がない限り、当該情報の利用者がそれらの者に無断で、<u>格付け</u>又は取扱制限を変更することは許されない。</p> <p>見直しにより元の決定者等に相談することが必要となる例として以下のような場合が考えられる。</p> <ul style="list-style-type: none"> ・作成時には非公開だった情報が正規の手続によって公開されることで機密性が失われた場合（時間の経過により変化した場合） ・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合 ・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合 ・<u>格付け</u>及び取扱制限を決定した<u>とき</u>の判断が不適切であったと考えられる場合 <p>相談を受けた決定者等は、次項(b)に基づいて所要の措置を講ずることになる。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		おける情報の取扱いに変更がある 場合 相談を受けた決定者等は、次項(b) に基づいて所要の措置を講ずること になる。			
207	1.3.1.2(4)(b)	行政事務従事者は、自らが 格付 及 び取扱制限の決定者等である情報 に対して、見直しの必要があると 認めた場合には、当該情報の 格付 又は取扱制限を再決定し、それを 明示等すること。また、それ以前 に当該情報を参照した者に対し て、その旨を可能な限り周知する こと。	1.3.1.2(4)(b)	行政事務従事者は、自らが 格付け 及び取扱制限の決定者等である情 報に対して、見直しの必要がある と認めた場合には、当該情報の 格 付け 又は取扱制限を再決定し、そ れを明示等すること。また、それ 以前に当該情報を参照した者に対 して、その旨を可能な限り周知す ること。	表現 の適 正化
208	1.3.1.2(4)(b) 解説	解説：いずれの理由であっても、 適切な 格付 又は取扱制限がなされ ていない場合は、情報セキュリ ティ対策が適正に実施されないお それが生ずるため、適切な 格付 又は 取扱制限に変更することを求める 事項である。 また、同一の情報が異なる 格付 又 は取扱制限とならないように、変 更以前に当該情報を参照した者 に対しても、 格付 又は取扱制限が 変更された旨を周知させることに 努める必要がある。 当該情報を直接提供した相手やそ れを参照したと思われる者を特定 することが困難な場合には、わか る範囲で構わない。	1.3.1.2(4)(b) 解説	解説：いずれの理由であっても、 適切な 格付け 又は取扱制限がなさ れていない場合は、情報セキュリ ティ対策が適正に実施されないお それが生ずるため、適切な 格付け 又は取扱制限に変更することを求 める事項である。 また、同一の情報が異なる 格付け 又は取扱制限とならないように、 変更以前に当該情報を参照した者 に対しても、 格付け 又は取扱制限 が変更された旨を周知させること に努める必要がある。 当該情報を直接提供した相手やそ れを参照したと思われる者を特定 することが困難な場合には、わか る範囲で構わない。	解説 の修 正
209	1.3.1.2(5)(b) 解説	解説：第三者による不正な操作や 盗み見等を防止することを求める	1.3.1.2(5)(b) 解説	解説：第三者による不正な操作や 盗み見等を防止することを求める	解説 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		事項である。例えば、離席する際には、ロック付きスクリーンセーバ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等を徹底する必要がある。		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。	正
210	1.3.1.2(5)(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、情報の格付を下げるとは取扱制限を緩和する必要があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。	1.3.1.2(5)(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とは取扱制限を緩和する必要があると思料される場合には、格付け及び取扱制限の見直しに必要な処理を行うこと。	表現 の適 正化
211	1.3.1.2(5)(e) 解説	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時は、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。	1.3.1.2(5)(e) 解説	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。	解説 の修 正
212	1.3.1.3	行政事務においては、その事務の	1.3.1.3	行政事務においては、その事務の	趣旨

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
	趣旨	継続性を確保する <u>等</u> の必要性から情報を保存する必要があるが、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として、 <u>格付に応じた情報の保存及び保存期間における取扱い又は保存期間満了後の取扱期間についての遵守事項</u> を定める。	趣旨	継続性を確保する <u>など</u> の必要性から情報を保存する必要があるが、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。	の修 正
213	1.3.1.3(1)	<u>格付</u> に応じた情報の保存	1.3.1.3(1)	<u>格付け</u> に応じた情報の保存	表現 の適 正化
214	1.3.1.3(1)(a)	<u>行政事務従事者は、情報の格付及び取扱制限に応じて、情報を適切に保存すること。</u>			遵守 事項 の追 加
215	1.3.1.3(1)(a) 解説	<u>解説：電磁的記録媒体に保存された情報、書面又は重要な設計書に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切な場所に保存することを求める事項である。</u> <u>例えば、行政事務従事者が書面又は重要な設計書を保存する場合は、安全区域内の棚に保存したり、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・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報（パスワード）によ</u>			解説 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>るロック機能を利用して、当該媒体の利用を防止することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。</u></p> <p><u>一方、行政事務従事者が要保護情報に関する情報処理を行う場合は、例えば、安全区域に設置された情報システム上に保存すること等が考えられる。また、行政事務従事者が許可を得て、個人で利用する ASP・SaaS サービスなどの外部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は、省庁対策基準と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。</u></p>			
216	1.3.1.3(1)(b) 解説	<p>解説：電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、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。</p> <p>電磁的記録媒体に保存された情報には電子計算機等を利用してアク</p>	1.3.1.3(1)(a) 解説	<p>解説：電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付け及び取扱制限に応じ、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。</p> <p>電磁的記録媒体に保存された情報には電子計算機等を利用してアク</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>セスすることになるため、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、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。</p> <p>情報システムに行政事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、行政事務従事者は、当該情報の格付及び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行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性2情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。<u>例えば、上書き禁止の属性を付与する方法としては、ファイルに対する書込権限者の制限、又はファイルのセキュリティ設定でパスワード設定した上での読取専用の設定等がある。</u></p> <p>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。その場合には、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</p>		<p>セスすることになるため、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、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。</p> <p>情報システムに行政事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、行政事務従事者は、当該情報の格付け及び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行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性2情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。</p> <p>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。その場合には、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。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		遵守することになる。			
217		(削除)	1.3.1.3(1)(c)	<u>行政事務従事者は、情報の格付け及び取扱制限に応じて、情報が保存された電磁的記録媒体を適切に管理すること。</u>	遵守 事項 の集 約
218		(削除)	1.3.1.3(1)(c) 解説	<u>解説：電磁的記録媒体に関して、機密性、完全性及び可用性の格付け及び取扱制限に応じて、適切に管理することを求める事項である。</u> <u>例えば、機密性の格付け及び取扱制限に応じて、外部電磁的記録媒体及び内蔵電磁的記録媒体を含む機器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。</u> <u>外部電磁的記録媒体については、主体認証情報（パスワード）によるロック機能を持つ場合には、当該媒体の利用を防止することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。</u>	解説 の集 約
219		(削除)	1.3.1.3(1)(d)	<u>行政事務従事者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面のうち要機密情報である書面、又は重要な設計書を適切に管理すること。</u>	遵守 事項 の集 約
220		(削除)	1.3.1.3(1)(d) 解説	<u>解説：書面の適切な管理を求める事項である。</u> <u>例えば、必要なく情報の参照等を</u>	解説 の集 約

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				<u>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。</u>	
221	1.3.1.3(1)(c) 解説	解説：電磁的記録媒体に保存された情報の機密性を確保するために、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、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。 <u>なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。</u>	1.3.1.3(1)(d) 解説	解説：電磁的記録媒体に保存された情報の機密性を確保するために、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、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。	解説 の修 正
222	1.3.1.3(1)(g) 解説	解説：バックアップ又は複写の適切な保管を求める事項である。 例えば、バックアップ又は複写を防火金庫に保管することや、同時被災に備えて遠隔地に保管すること <u>等</u> が考えられる。	1.3.1.3(1)(h) 解説	解説：バックアップ又は複写の適切な保管を求める事項である。 例えば、バックアップ又は複写を防火金庫に保管することや、同時被災に備えて遠隔地に保管すること <u>など</u> が考えられる。	
223	1.3.1.3(2)(a)	行政事務従事者は、電磁的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。	1.3.1.3(2)(a)	行政事務従事者は、電磁的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。	遵守 事項 の修 正
224	1.3.1.3(2)(a) 解説	解説： <u>電磁的記録媒体に保存された情報に関して、情報セキュリティ確保の観点から保存期間を定め</u>	1.3.1.3(2)(a) 解説	解説： <u>情報の</u> 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	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>ている場合に、当該</u>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。</p> <p>行政事務従事者は、<u>情報セキュリティ上</u>、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。<u>また、当該情報が記載されている行政文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか、利用の制限についての意見を付す等して移管するものとする。その際、本統一管理基準及び統一技術基準における遵守事項に従いつつ、例えば、行政事務従事者でパスワードを設定していた場合は、解除する等して移管先がその内容を参照できるように配慮すること。</u></p>		<p>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。</p>	
225	1.3.1.4 趣旨	<p>行政事務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部電磁的記録媒体及び PC の運搬、書面の運搬等の方法が挙げられるが、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。</p>	1.3.1.4 趣旨	<p>行政事務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部電磁的記録媒体及び PC の運搬、書面の運搬等の方法が挙げられるが、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。</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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として、 情報の移送に関する許可及び届出、情報の送信と運搬の選択、移送手段の決定、記録媒体及び電磁的記録の保護対策についての遵守事項 を定める。		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。	
226	1.3.1.4(3)(a) 解説	解説：多種多様な移送手段の中から要保護情報又は重要な設計書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、送信については府省庁内通信回線、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指定する運送 役務 及び 行政事務従事者 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。 また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを十分に検討する必要がある。	1.3.1.4(3)(a) 解説	解説：多種多様な移送手段の中から要保護情報又は重要な設計書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、送信については府省庁内通信回線、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。 また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを十分に検討する必要がある。	解説 の修 正
227	1.3.1.4(4)	記録媒体 の保護対策	1.3.1.4(4)	書面 の保護対策	遵守 事項 の修 正
228	1.3.1.4(4)(a)	行政事務従事者は、要機密情報 が 記録又は記載された記録媒体 を運	1.3.1.4(4)(a)	行政事務従事者は、要機密情報で ある書面又は重要な設計書 を運搬	遵守 事項

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		搬ずる場合には、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。		ずる場合には、情報の格付け及び取扱制限に応じて、安全確保のための適切な措置を講ずること。	の修 正
229	1.3.1.4(4)(a) 解説	解説：要機密情報が記録又は記載された記録媒体を運搬する場合における情報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、外部電磁的記録媒体、PC、書面又は重要な設計書等を運搬する場合には、例えば、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。	1.3.1.4(4)(a) 解説	解説：要機密情報である書面又は重要な設計書を運搬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。	解説 の修 正
230	1.3.1.4(5)(a) 解説	解説：移送手段の種別を問わず、受取手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。 なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。	1.3.1.4(5)(a) 解説	解説：移送手段の種別を問わず、受取手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。	解説 の修 正
231	1.3.1.4(5)(e)	行政事務従事者は、要安定情報である電磁的記録を移送する場合に	1.3.1.4(5)(e)	行政事務従事者は、要安定情報である電磁的記録を移送する場合に	遵守 事項

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		は、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送する等の措置を講ずる必要性の有無を検討し、必要があると認めるときは、所要の措置を講ずること。		は、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めるときは、所要の措置を講ずること。	の修 正
232	1.3.1.4(5)(f) 解説	<p>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。</p> <p>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。</p> <p>この考え方は、専門用語で秘密分散技術といわれ、例えば、1個の電子情報についてファイルを2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をCD-R、DVD、MO、USBメモリ、フラッシュメモリ等の外部電磁的記録媒体で郵送する方法が挙げられる。</p>	1.3.1.4(5)(f) 解説	<p>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。</p> <p>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。</p> <p>この考え方は、専門用語で秘密分散技術といわれ、例えば、1個の電子情報についてファイルを2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をCD-ROM等の外部電磁的記録媒体で郵送する方法が挙げられる。</p>	解説 の修 正
233	1.3.1.5 趣旨	<p>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。</p> <p>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とし</p>	1.3.1.5 趣旨	<p>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。</p> <p>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</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		て、情報の公表及び他者への情報の提供についての遵守事項 を定める。		める。	
234	1.3.1.5(1)(a)	行政事務従事者は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認すること。	1.3.1.5(1)(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。	表現 の適 正化
235	1.3.1.5(1)(a) 解説	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、保有する情報をウェブサイト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の適正さを再度検討し、必要に応じて格付の変更等を行った上で、当該情報が機密性1情報に格付されるものであることを確認する必要がある。 なお、情報セキュリティ関係規程の定めによらず、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は別途確認する必要がある。	1.3.1.5(1)(a) 解説	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、情報セキュリティ関係規程の定めによらず、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は別途確認する必要がある。	解説 の修 正
236	1.3.1.5(2)(c)	行政事務従事者は、要保護情報又は重要な設計書を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。	1.3.1.5(2)(c)	行政事務従事者は、要保護情報又は重要な設計書を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付け及び取扱制限に応じて適切に取り扱われるための措置を講ずること。	表現 の適 正化
237	1.3.1.5(2)(c) 解説	解説：要保護情報又は重要な設計書を府省庁外の者に提供する場合	1.3.1.5(2)(c) 解説	解説：要保護情報又は重要な設計書を府省庁外の者に提供する場合	解説 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>において遵守すべきことを定める事項である。</p> <p>要保護情報又は重要な設計書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情報が適切に取り扱われるように、情報の格付及び取扱制限の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。</p> <p>確実に伝達する方法として、提供先が統一管理基準及び統一技術基準に準じた組織の場合には、統一管理基準及び統一技術基準による情報の格付及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付の区分だけを示すのでは不十分である。なぜなら、提供先においては当該格付区分がどのように取り扱われるべきものであるかが認識できないからである。格付の区分（例えば、「機密性2」と記載する）で示すのであれば、当該格付の区分の定義について提供先にあらかじめ周知しておくか、格付の区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す（例えば、「委員以外への再配布を禁止する」と記載する）等をする</p>		<p>において遵守すべきことを定める事項である。</p> <p>要保護情報又は重要な設計書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情報が適切に取り扱われるように、情報の格付け及び取扱制限の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。</p> <p>確実に伝達する方法として、提供先が統一基準に準じた組織の場合には、統一基準による情報の格付け及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付けの区分だけを示すのでは不十分である。なぜなら、提供先においては当該格付け区分がどのように取り扱われるべきものであるかが認識できないからである。格付けの区分（例えば、「機密性2」と記載する）で示すのであれば、当該格付けの区分の定義について提供先に予め周知しておくか、格付けの区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す（例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。また、提供した情報</p>	正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>必要がある。また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要がある。</p> <p>行政事務従事者は、格付及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付及び取扱制限に従った取扱いを確保するため、提供する前に、明記が不要とされている情報の格付及び取扱制限を当該書面又は電磁的記録に明記すること。</p>		<p>が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要がある。</p> <p>行政事務従事者は、格付け及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付け及び取扱制限に従った取扱いを確保するため、提供する前に、明記が不要とされている情報の格付け及び取扱制限を当該書面又は電磁的記録に明記すること。</p>	
238	1.3.1.6 趣旨	<p>行政事務において利用した電子計算機、通信回線装置及び外部電磁的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、情報を消去する際に、適切な措置が講じられていなければ、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。</p> <p>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として、電磁的記録の消去方法及び書面の廃棄方法についての遵守事項</p>	1.3.1.6 趣旨	<p>行政事務において利用した電子計算機、通信回線装置及び外部電磁的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、情報を消去する際に、適切な措置が講じられていなければ、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。</p> <p>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。</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		を定める。			
239	1.3.1.6(1)(a)	行政事務従事者は、電磁的記録媒体を廃棄する場合には、 <u>全て</u> の情報を <u>抹消する</u> こと。	1.3.1.6(1)(a)	行政事務従事者は、電磁的記録媒体を廃棄する場合には、 <u>すべての</u> 情報を <u>復元が困難な状態にする</u> <u>(以下「抹消する」という。)</u> こと。	遵守 事項 の修 正
240	1.3.1.6(1)(a) 解説	<p>解説：電磁的記録媒体を廃棄する場合に、<u>全て</u>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。</p> <p>「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。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、内蔵電磁的記録媒体及び外部電磁的記録媒体に記録されている<u>全て</u>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。</p> <p>抹消するための方法としては、<u>例えば</u>、次の方法が挙げられる。</p> <ul style="list-style-type: none"> ・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを個々に抹消する方法 ・ハードディスクを消磁装置に入れてディスク内の<u>全て</u>のデータを抹消する方法 	1.3.1.6(1)(a) 解説	<p>解説：電磁的記録媒体を廃棄する場合に、<u>すべての</u>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。</p> <p>「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。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、内蔵電磁的記録媒体及び外部電磁的記録媒体に記録されている<u>すべての</u>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。</p> <p>抹消するための方法としては、次の方法が挙げられる。</p> <ul style="list-style-type: none"> ・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを個々に抹消する方法 ・ハードディスクを消磁装置に入れてディスク内の<u>すべての</u>データを抹消する方法 	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<ul style="list-style-type: none"> ・媒体を物理的に破壊する方法 なお、媒体を物理的に破壊する方法としては、<u>例えば</u>、次の方法が挙げられる。 ・FD等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等して情報を記録している内部の円盤を破壊する方法 ・CD-R/RW、DVD-R/RW等の光学媒体の場合には、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法 		<ul style="list-style-type: none"> ・媒体を物理的に破壊する方法 なお、媒体を物理的に破壊する方法としては、次の方法が挙げられる。 ・FD等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等して情報を記録している内部の円盤を破壊する方法 ・CD-R/RW、DVD-R/RW等の光学媒体の場合には、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法 	
241	1.3.1.6(1)(c) 解説	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電磁的記録媒体 <u>等</u> 、安全といえない環境で利用される電子計算機等に要機密情報を残留させないことを求める事項である。行政事務従事者は、要機密情報が保存された電子ファイル又は空き領域に残留する情報を抹消すること。	1.3.1.6(1)(c) 解説	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電磁的記録媒体 <u>など</u> 、安全といえない環境で利用される電子計算機等に要機密情報を残留させないことを求める事項である。行政事務従事者は、要機密情報が保存された電子ファイル又は空き領域に残留する情報を抹消すること。	解説 の修 正
242	1.3.1.6(2)(a)解 説	解説：電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却又は溶解 <u>等</u> により、復元が困難な状態にすることを求める事項である。なお、廃棄すべき書類が大量である <u>等</u> の理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処	1.3.1.6(2)(a) 解説	解説：電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却又は溶解 <u>など</u> により、復元が困難な状態にすることを求める事項である。なお、廃棄すべき書類が大量である <u>など</u> の理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。		棄処理証明書の取得などにより、書面が確実に廃棄されていることを確認するとよい。	
243	1.4.1.1	1.4.1.1 情報システムの利用			構成 変更
244	1.4.1.1 趣旨	<p>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、本来アクセス権のない者が、故意又は過失により、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。</p> <p>これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。</p> <p>なお、1.5.2.4において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、統一技術基準2.2.1.1~2.2.1.5においても各機能の導入等に関する対策基準を定めている。</p>	2.1.1.1 趣旨 より引用	<p>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、本来アクセス権のない者が、故意又は過失により、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。</p> <p>これらのことを勘案し、本項では、主体認証機能の導入に関する対策基準を定める。</p> <p><u>また、政府機関が有する各情報システムの利用者は、行政事務従事者に限られるものではない。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。</u></p>	趣旨 の追 加、 修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
245	1.4.1.1(1)	識別コードの管理			構成 変更
246	1.4.1.1(1)(a)	行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと。		(2.1.1.1(2)(a)から移動)	構成 変更
247	1.4.1.1(1)(a) 解説	<p>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。</p> <p>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、仮に他者の許可を得たとしても、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。</p> <p>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、例外措置の承認を行う際に本人の事前の了解に加えて、情報システムセ</p>	2.1.1.1(2)(a) 解説	<p>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。</p> <p>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</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>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るのが望ましい。</p> <p>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。</p> <p>遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。</p>		<p>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るのが望ましい。</p> <p>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。</p> <p>遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。</p>	
248	1.4.1.1(1)(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 が 主体認証に用いるために付与及び貸与しないこと。	2.1.1.1(2)(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 主体認証に用いる 目的 のために付与及び貸与しないこと。	構成 変 更、 遵守 事項

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
					の修 正
249	1.4.1.1(1)(b) 解説	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。 遵守事項に「主体認証に用いるために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。	2.1.1.1(2)(b) 解説	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。 遵守事項に「主体認証に用いる <u>目的</u> のために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。	解説 の修 正
250	1.4.1.1(1)(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：～		(2.1.1.1(2)(c)から移動)	構成 変更
251	1.4.1.1(1)(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、その旨を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、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。		(2.1.1.1(2)(d)から移動)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
252	1.4.1.1(1)(d) 解説	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をを求める事項である。ただし、 <u>例えば、人事異動等によって、行政事務従事者の識別コードが大規模に変更となる場合</u> 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の届出によらずして把握できる場合等、 <u>行政事務従事者自らの届出が不要となる条件を情報システムセキュリティ責任者が定めても良い。</u>	2.1.1.1(2)(d) 解説	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をを求める事項である。ただし、 <u>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</u> 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の届出によらずして把握できる場合には、 <u>行政事務従事者自らの届出は不要とすることができる。</u>	解説 の修 正
253	1.4.1.1(1)(e)	行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。		(2.1.1.1(2)(e)から移動)	構成 変更
254	1.4.1.1(1)(e) 解説	解説：管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用することを求める事項である。 例えば、情報システムのオペレーティングシステムが 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 <u>等</u> をしないときには、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 administrator 権限で再ログインすることを遵守しなければならない。	2.1.1.1(2)(e) 解説	解説：管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用することを求める事項である。 例えば、情報システムのオペレーティングシステムが 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 <u>など</u> をしないときには、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 administrator 権限で再ログインすることを遵守しなければならない。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		なお、 <u>本</u> 遵守事項は、実際には複雑な操作を必要とする場合があるため、最少特権機能が設けられている場合は、これを遵守すべきであるが、当該情報システムで取り扱う情報の重要性 <u>等</u> を勘案し、必要に応じて選択されたい。		なお、 <u>この</u> 遵守事項は、実際には複雑な操作を必要とする場合があるため、最少特権機能が設けられている場合は、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 <u>など</u> を勘案し、必要に応じて <u>遵守事項として本事項</u> を選択されたい。	
255	1.4.1.1(2)	<u>主体認証情報の管理</u>			構成 変更
256	1.4.1.1(2)(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：～		(2.1.1.1(3)(a)から移動)	構成 変更
257	1.4.1.1(2)(b)	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ことを知った場合には、必要な措置を講ずること。		(2.1.1.1(3)(b)から移動)	構成 変更
258	1.4.1.1(2)(b) 解説	解説： <u>自らが発見したり、報告を受けたりして、主体認証情報の他者使用又は危険発生を知った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</u> が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、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	2.1.1.1(3)(b) 解説	解説： <u>報告を受けた者</u> が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、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等がある。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		等がある。			
259	1.4.1.1(2)(c)	行政事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。 (ア)～(オ)		(2.1.1.1(3)(c)から移動)	構成 変更
260	1.4.1.1(2)(c) (イ)解説	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、証跡管理その他の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、 <u>自己の主体認証情報は他者に「教えない」ことを徹底すべきである。</u>	2.1.1.1(3)(c) (イ)解説	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、証跡管理その他の <u>情報</u> 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」、「 <u>聞かない</u> 」を徹底すべきである。	解説 の修 正
261	1.4.1.1(2)(c) (ウ)解説	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。 <u>なお</u> 、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	2.1.1.1(3)(c) (ウ)解説	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	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。		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構築・運用すべきである。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること が 望ましい。	
262	1.4.1.1(2)(c) (エ)解説	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、更に特殊記号等も織り交ぜて主体認証情報を構成することが望ましい。	2.1.1.1(3)(c) (エ)解説	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。	解説 の修 正
263	1.4.1.1(2)(c) (オ)解説	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等の運用によって対処することでも差し支えない。	2.1.1.1(3)(c) (オ)解説	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。	解説 の修 正
264	1.4.1.1(2)(d)	行政事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。 (ア)～(エ)		(2.1.1.1(3)(d)から移動)	構成 変更
265	1.4.1.1(2)(d) (エ)解説	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	2.1.1.1(3)(d) (エ)解説	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	解説 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		体として主体認証されることになるため、他者に使用されないように、また、紛失 <u>等</u> で、その可能性がある場合の報告を徹底する必要がある。異動等により主体認証情報格納装置を利用する必要がなくなった場合には、これを返却する必要がある。		体として主体認証されることになるため、他者に使用されないように、また、紛失 <u>など</u> で、その可能性がある場合の報告を徹底する必要がある。異動等により主体認証情報格納装置を利用する必要がなくなった場合には、これを返却する必要がある。	正
266	1.4.1.1(2)(e)	情報システムセキュリティ責任者は、 <u>主体認証のために取得した情報を</u> 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。	2.1.1.1(1)(h)	情報システムセキュリティ責任者は、 <u>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</u> 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。 <u>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。</u>	構成 変更、 遵守 事項 の修 正
267	1.4.1.1(2)(e) 解説	解説：利用者の指紋情報 <u>等</u> 、主体認証情報として生体情報を取り扱う場合には、 <u>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が求められる。管理方法としては、元の生体情報が再現できないように保存すること等が考えられる。</u>	2.1.1.1(1)(h) 解説	解説：利用者の指紋情報 <u>など</u> 、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 <u>を求める事項である。</u>	解説 の修 正
268	1.4.1.1(3)	<u>識別コードと主体認証情報の付与管理</u>			構成 変更
269	1.4.1.1(3)(a)	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た情報システムにおいて、共用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：～		(2.1.1.3 (2)(a)から移動)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
270	1.4.1.1(3)(a) 解説	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、利用状況等を考慮して、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。	2.1.1.3(2)(a) 解説	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。	解説 の修 正
271	1.4.1.1(3)(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おいて、権限管理について、以下の事項を含む手続を定めること。 (ア)～(ウ)		(2.1.1.3(2)(b)から移動)	構成 変更
272	1.4.1.1(3)(b) 解説	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。	2.1.1.3(2)(b) 解説	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。	解説 の修 正
273	1.4.1.1(3)(c)	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おいて、権限管理を行う者を定めること。		(2.1.1.3(2)(c)から移動)	構成 変更
274	1.4.1.1(3)(c) 解説	解説：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る事	2.1.1.3(2)(c) 解説	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	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		項である。		<u>め、厳格な運用を求める</u> 事項である。	
275	1.4.1.1(4)	識別コードと主体認証情報における代替手段等の適用			構成 変更
276	1.4.1.1(4)(a)	<p>情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、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、必要があると認めたときは、代替手段を提供すること。</p> <p>解説：～</p>		(2.1.1.3(3)(a)から移動。)	構成 変更
277	1.4.1.1(4)(a) 解説	<p>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。</p> <p>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</p>		(2.1.1.3(3)(a)解説から移動。)	構成 変更、 解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>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、その申請が正当な利用者からの許可申請であること及び許可申請の理由が妥当であること等を確認した上で、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等が想定されるが、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、適正な代替手段を準備しておくこと。</p> <p>なお、代替手段の提供に当たっては、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。</p>			
278	1.4.1.1(4)(b)	<p>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、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用を知った場合には、直ちに当該識別コードによる使用を停止させること。</p>	2.1.1.3(3)(b)	<p>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、権限管理を行う必要があると認めた情報システムにおいて、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。</p>	構成 変更、 遵守 事項 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
279	1.4.1.1(4)(b) 解説	解説： <u>自らが発見したり、報告を受けたりして、識別コードの不正使用を知った場合</u> には、他の項目で定められている障害・事故等の対処に係る遵守事項とともに、 <u>本遵守事項</u> の対処を実施する。 <u>なお、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、例えば、全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が望ましい。</u> 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 <u>再発行することが望ましい。</u>	2.1.1.3(3)(b) 解説	解説： <u>不正使用の報告を受けた場合</u> には、他の <u>基準</u> 項目で定められている障害・事故等の対処に係る遵守事項とともに、 <u>本事項</u> の対処を実施する。 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、 <u>すべての</u> 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 <u>取得すべきである。</u> 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 <u>再発行すべきである。</u>	解説 の修 正
280	1.4.2	<u>1.4.2</u> 情報処理の制限	1.4.1	<u>1.4.1</u> 情報処理の制限	構成 変更
281	1.4.2.1	<u>1.4.2.1</u> 府省庁外での情報処理の制限	1.4.1.1	<u>1.4.1.1</u> 府省庁外での情報処理の制限	構成 変更
282	1.4.2.1 趣旨	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ある場合がある。この際、府省庁外での実施では物理的な安全対策を講ず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として、 <u>安全管理措</u>	1.4.1.1 趣旨	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ある場合がある。この際、府省庁外での実施では物理的な安全対策を講ず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。	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項 を定める。			
283	1.4.2.1(1)(a) 解説	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。 ただし、情報処理の種類により個別の規定を設けても構わない。 府省庁外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通じた通信の形態、関与する府省庁内外の者等に応じた措置を示した規定を整備する必要がある。	1.4.1.1(1)(a) 解説	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。府省庁外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通じた通信の形態、関与する府省庁内外の者等に応じた措置を示した規定を整備する必要がある。	解説 の修 正
284	1.4.2.1(2)(a) 解説	解説：機密性3情報、完全性2情報又は可用性2情報に係る情報処理を府省庁外で行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。 なお、「情報処理に係る記録」には、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を含めること	1.4.1.1(2)(a) 解説	解説：機密性3情報、完全性2情報又は可用性2情報に係る情報処理を府省庁外で行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>が考えられる。</u>			
286	1.4.2.1(2)(g) 解説	解説：機密性3情報、完全性2情報又は可用性2情報を取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該 <u>持ち出し</u> の業務上の必要性については課室情報セキュリティ責任者の、当該 <u>持ち出し</u> の安全性については情報システムセキュリティ責任者の許可を得ることとなる。	1.4.2.1(2)(g) 解説	解説：機密性3情報、完全性2情報又は可用性2情報を取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該 <u>持出し</u> の業務上の必要性については課室情報セキュリティ責任者の、当該 <u>持出し</u> の安全性については情報システムセキュリティ責任者の許可を得ることとなる。	解説 の修 正
287	1.4.2.1(2)(h) 解説	解説：機密性2情報であって完全性1情報かつ可用性1情報である情報を取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出をを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない府省庁外への <u>持ち出し</u> を定める際には、届出をしないことにより発生するリスクを十分に検討する必要がある。	1.4.1.1(2)(h) 解説	解説：機密性2情報であって完全性1情報かつ可用性1情報である情報を取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出をを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない府省庁外への <u>持出し</u> を定める際には、届出をしないことにより発生するリスクを十分に検討する必要がある。	解説 の修 正
288	1.4.2.1(2)(i)	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情報システムの府省庁外への <u>持ち出し</u> に係る記録を取得すること。	1.4.1.1(2)(i)	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情報システムの府省庁外への <u>持出し</u> に係る記録を取得すること。	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
289	1.4.2.1(2)(i) 解説	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 <u>持ち出し</u> に係る記録を取得することを求める事項である。 「持ち出しに係る記録」には、 <u>持ち出し</u> 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を含めることが考えられる。	1.4.1.1(2)(i) 解説	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 <u>持出し</u> に係る記録を取得することを求める事項である。 「持出しに係る記録」には、 <u>持出し</u> 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を含めることが考えられる。	表現 の適 正化
290	1.4.2.1(2)(k) 解説	解説：届出期間が長期にわたる <u>場合等</u> 、必要に応じて、府省庁外への <u>持出し</u> 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。	1.4.1.1(2)(k) 解説	解説：届出期間が長期にわたる <u>など</u> 、必要に応じて、府省庁外への <u>持出し</u> 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。	解説 の修 正
291	1.4.1.1(2)(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、業務の遂行に必要な最小限の情報システムの <u>持ち出し</u> にとどめること。	1.4.1.1(2)(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、業務の遂行に必要な最小限の情報システムの <u>持出し</u> にとどめること。	表現 の適 正化
292	1.4.2.1(3)(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 <u>持ち出し</u> について定められた安全管理措置を講ずること。	1.4.1.1(3)(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 <u>持出し</u> について定められた安全管理措置を講ずること。	表現 の適 正化
293	1.4.2.1(3)(c) 解説	解説：行政事務従事者に対して、情報システムの府省庁外への <u>持ち出し</u> 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。 定められた安全管理措置の内容としては、例えば、盗難及び亡失の	1.4.1.1(3)(c) 解説	解説：行政事務従事者に対して、情報システムの府省庁外への <u>持出し</u> 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。 定められた安全管理措置の内容としては、例えば、盗難及び亡失の	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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 <u>フィルター</u> 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考えられる。		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 <u>ファイ</u> <u>ルター</u> 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考えられる。	
294	1.4.2.1(3)(d) 解説	解説：行政事務従事者に対して、府省庁外へ情報システムの <u>持ち出し</u> 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。	1.4.1.1(3)(d) 解説	解説：行政事務従事者に対して、府省庁外へ情報システムの <u>持出し</u> 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。	解説 の修 正
295	1.4.2.2	1.4.2.2 府省庁支給以外の情報システムによる情報処理の制限	1.4.1.2	1.4.1.2 府省庁支給以外の情報システムによる情報処理の制限	構成 変更
296	1.4.2.2 趣旨	行政事務においては、その遂行のため、府省庁支給以外の情報システムを利用する必要がある場合がある。この際、当該情報システムが、府省庁が支給したもので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として、 <u>安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項</u> を定める。	1.4.1.2 趣旨	行政事務においては、その遂行のため、府省庁支給以外の情報システムを利用する必要がある場合がある。この際、当該情報システムが、府省庁が支給したもので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。	趣旨 の修 正
297	1.4.2.2(1)(a) 解説	解説：行政事務従事者が所有する個人の <u>PC 等</u> を用いて要保護情報に関する情報処理を行う場合であ	1.4.1.2(1)(a) 解説	解説：行政事務従事者が所有する個人の <u>PC など、府省庁支給以外の情報システム</u> を用いて要保護情	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		っても、府省庁支給の情報システムと同程度の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。 <u>ただし、情報システムの種類により個別の規定を設けても構わない。</u>		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。	
298	1.4.2.2(2)(e) 解説	解説：届出期間が長期にわたる場合 <u>等</u> 、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。	1.4.2.2(2)(e) 解説	解説：届出期間が長期にわたる場合 <u>など</u> 、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。	解説 の修 正
299	1.4.2.2(3)(a) 解説	解説：行政事務従事者が所有する個人の PC 等 、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。	1.4.2.2(3)(a) 解説	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。	解説 の修 正
300	1.4.2.2(3)(b)	【強化遵守事項】			
301	1.4.2.2(3)(c)	<u>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府省庁支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に直接確認すること。</u>			遵守 事項 の追 加
302	1.4.2.2(3)(c) 解説	<u>解説：情報システムセキュリティ責任者に対して、許可又は届出を</u>			解説 の追

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>受理した要保護情報を取り扱う府省庁支給以外の情報システムについて、府省庁支給の情報システムと同程度のセキュリティ対策が施されていることの確認を求める事項である。</u></p> <p><u>確認する頻度は、情報処理の開始時や一定期間経過後等、それぞれの府省庁の特性に応じて設定することが望ましい。また、当該情報システムが固定されている等の理由で、情報システムの運搬が不可能な場合には、当該情報システムが設置されている現地に赴いて確認することが望ましい。</u></p> <p><u>なお、あらかじめ情報システムセキュリティ責任者が認めた場合には、情報システムセキュリティ責任者が指定した者に確認させることも考えられる。その際には、情報システムセキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。</u></p>			加
303	1.5.1.1 趣旨	<p>情報システムは、目的業務を円滑に遂行するため、その計画、構築、運用、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせてセキュリティ対策を実施する必要がある。</p>	1.5.1.1 趣旨	<p>情報システムは、目的業務を円滑に遂行するため、その計画、構築、運用、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせて情報セキュリティ対策を実施する必要がある。</p>	趣旨の追加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		これらのことを勘案し、本項では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。		これらのことを勘案し、本項では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。	
304	1.5.1.1(1)(b)	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。 この場合、国民・企業と政府との間で申請・届出等のオンライン手続を提供するシステムにおいては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づき決定すること。	1.5.1.1(1)(b)	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。	遵守 事項 の修 正
305	1.5.1.1(1)(b) 解説	解説：情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。 「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。なお、前者のセキュリティ要件については、構築環境や構築手法等 ^① のセキュリティに関する手順も含まれる。 具体的なセキュリティ要件につい	1.5.1.1(1)(b) 解説	解説：情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。 「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。なお、前者のセキュリティ要件については、構築環境や構築手法 ^② などのセキュリティに関する手順も含まれる。 具体的なセキュリティ要件につい	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>ては、省庁対策基準において<u>統一技術基準</u>に対応して定められた事項、本統一管理基準の「1.5.2 情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。</p> <p>決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。</p> <p><u>また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが発生しないようにすること。</u></p> <p><u>なお、物理的に分割されたシステムに限らず、論理的に分割されたシステムも同様に考慮すること。</u></p> <p><u>「論理的に分割されたシステム」とは、一つの情報システムのきょう体上に複数のシステムを共存させることを目的として、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。</u></p>		<p>ては、省庁対策基準において<u>本統一基準の「第2編 情報システム編」</u>に対応して定められた事項、本統一基準の「1.5.2 情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。</p> <p>決定されたセキュリティ要件は、システム要件定義書や仕様書<u>など</u>の形式で明確化した上で、実装していくことが望ましい。</p>	
306	1.5.1.1(1)(c) 解説	解説：情報システムのセキュリティ要件を満たすために必要な対策を定めることを求める事項であ	1.5.1.1(1)(c) 解説	解説： <u>本項は</u> 、情報システムのセキュリティ要件を満たすために必要な対策を定めることを求める事	解説 の修 正

No.	統一管理基準 遵守事項	統一管理基準	第4版(平成21年度修正) 遵守事項	第4版(平成21年度修正)	変更点
		る。 情報システムにおいて必要な対策としては、省庁対策基準において 統一技術基準 に対応して定められた事項、本統一管理基準の「1.5.2 情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件に基づく対策がある。		項である。 情報システムにおいて必要な対策としては、省庁対策基準において 本統一基準の「第2編 情報システム編」 に対応して定められた事項、本統一基準の「1.5.2 情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件に基づく対策がある。	
307	1.5.1.1(1)(d) 【強化】から 【基本】へ移動	情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、 ITセキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性の有無を検討し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。	1.5.1.1(1)(g)	情報システムセキュリティ責任者は、構築する情報システムの構成要素については、重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合であって、その中に当該セキュリティ機能に関してITセキュリティ評価及び認証制度に基づく認証を取得している製品がある場合には、当該製品を情報システムの構成要素として選択すること。	遵守事項の修正
308	1.5.1.1(1)(d) 解説 【強化】から	解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択	1.5.1.1(1)(g) 解説	解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択	解説の修正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
	【基本】へ移動	<p>肢がある場合、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得しているものを選択することを求める事項である。第三者による情報セキュリティ機能の客観的な評価によって、安全性の高い情報システムの構築が期待できる。</p> <p><u>製品分野として当該認証を取得する必要性の判断については、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ることが望ましい。なお、国際承認アレンジメント (CCRA) 参加国における ISO/IEC 15408 に基づく認証取得製品又は実質的に CC 認証取得製品とセキュリティ機能上同等であると確認されている製品 (上記のリストを参照) を活用することが考えられる。</u></p>		<p>肢がある場合、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得しているものを選択することを求める事項である。</p> <p>第三者による情報セキュリティ機能の客観的な評価によって、より信頼度の高い情報システムの構築が期待できる。</p>	
309		(1.5.1.1(1)(g)へ移動)	1.5.1.1(1)(d)	<p>情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書 (ST : Security Target) の ST 評価・ST 確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微で</p>	遵守 事項 の移 動

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				あると認めたときは、この限りでない。	
310		(1.5.1.1(1)(g)解説へ移動)	1.5.1.1(1)(d) 解説	<p>解説：重要なセキュリティ要件がある情報システムについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価・ST 確認を受けることを求める事項である。</p> <p>「ST 評価・ST 確認を受けること」とは、ST 評価・ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。情報システムの構築が終了するまでにセキュリティ設計仕様書について、ST 評価・ST 確認済みとなっている必要があるが、セキュリティ設計仕様書が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。</p> <p>なお、情報システムの構築を外部委託する場合には、契約時に条件として含め納品までに ST 評価・ST 確認を受けさせることになる。</p>	解説 の移 動
311	1.5.1.1(1)(e) 解説	解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。情報セキュリティの侵害とは、要保護情報につい	1.5.1.1(1)(e) 解説	解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。情報セキュリティの侵害とは、要保護情報につい	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>て機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。</p> <p>監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、府省庁の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の安全区域への立ち入り等があり得る。</p> <p>また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。</p> <p>(1) 設ける監視機能を定める。</p> <p>監視機能には、以下の例がある。</p> <ul style="list-style-type: none"> ・府省庁外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能（侵入検知システム等による） ・不正プログラム感染や踏み台に利用されること等による府省庁外への不正な通信を監視する機能 ・府省庁内通信回線へのPCの接続を監視する機能 ・PCへの外部記録媒体の挿入を監視する機能 ・サーバ装置等の機器の正常な動 		<p>て機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。</p> <p>監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、府省庁の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の安全区域への立ち入り等があり得る。</p> <p>また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。</p> <p>(1) 設ける監視機能を定める。</p> <p>監視機能には、以下の例がある。</p> <ul style="list-style-type: none"> ・府省庁外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能（侵入検知システム等による） ・ウイルス感染や踏み台に利用されること等による府省庁外への不正な通信を監視する機能 ・府省庁内通信回線へのPCの接続を監視する機能 ・PCへの外部記録媒体の挿入を監視する機能 ・サーバ装置等の機器の正常な動 	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>作を監視する機能</p> <ul style="list-style-type: none"> ・安全区域への人の出入を監視する機能 <p>(2) 監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。</p> <p>(3) 監視によりプライバシーを侵害する可能性がある場合は、当該行政事務従事者等への説明について定める。</p>		<p>作を監視する機能</p> <ul style="list-style-type: none"> ・安全区域への人の出入を監視する機能 <p>(2) 監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。</p> <p>(3) 監視により職員等のプライバシーを侵害する可能性がある場合は、当該職員等への説明について定める。</p>	
312	1.5.1.1(1)(g) 【基本】から 【強化】へ移動	<p>情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価及びST確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めるときは、この限りでない。</p>		(1.5.1.1(1)(d)から移動)	遵守事項の移動
313	1.5.1.1(1)(g) 解説 【基本】から 【強化】へ移動	<p>解説：重要なセキュリティ要件がある情報システムについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書のST評価及びST確認を受</p>		(1.5.1.1(1)(d)解説から移動)	解説の移動

No.	統一管理 基準 遵守事項	統一管理基準	第 4 版(平成 21年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変 更 点
		<p>けることを求める事項である。</p> <p>「ST 評価及びST 確認を受けること」とは、ST 評価及びST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。情報システムの構築が終了するまでにセキュリティ設計仕様書について、ST 評価及びST 確認済みとなっている必要があるが、セキュリティ設計仕様書が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。</p> <p>なお、情報システムの構築を外部委託する場合には、契約時に条件として含め納品までに ST 評価及びST 確認を受けさせることになる。</p>			
314		(1.5.1.1(1)(d)へ移動)	1.5.1.1(1)(g)	<p>情報システムセキュリティ責任者は、構築する情報システムの構成要素については、重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合であって、その中に当該セキュリティ機能に関して IT</p>	<p>強化 遵守 事項 から 基本 遵守 事項 への 修正</p>

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				セキュリティ評価及び認証制度に基づく認証を取得している製品がある場合には、当該製品を情報システムの構成要素として選択すること。	
315		(1.5.1.1(1)(d)解説へ移動)	1.5.1.1(1)(g) 解説	解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択肢がある場合、ISO/IEC 15408に基づくITセキュリティ評価及び認証制度による認証を取得しているものを選択することを求める事項である。 第三者による情報セキュリティ機能の客観的な評価によって、より信頼度の高い情報システムの構築が期待できる。	解説 の移 動
316	1.5.1.1(2)	情報システムの構築及び運用	1.5.1.1(2)	情報システムの構築・運用	表現 の適 正化
317	1.5.1.1(2)(a)	情報システムセキュリティ責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めたセキュリティ対策を行うこと。	1.5.1.1(2)(a)	情報システムセキュリティ責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。	遵守 事項 の修 正
318	1.5.1.1(3)	情報システムの移行及び廃棄	1.5.1.1(3)	情報システムの移行・廃棄	表現 の適 正化
319	1.5.1.1(4)(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対策について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	1.5.1.1(4)(a)	情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について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	遵守 事項 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		い、必要な措置を講ずること。		を行い、必要な措置を講ずること。	
320	1.5.1.1(4)(a) 解説	解説：情報システムの <u>セキュリティ対策</u> について、必要に応じて見直しとそれに必要な措置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、運用、監視等の状況により判断する必要がある。	1.5.1.1(4)(a) 解説	解説：情報システムの <u>情報セキュリティ対策</u> について、必要に応じて見直しとそれに必要な措置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、運用、監視等の状況により判断する必要がある。	解説 の修 正
321	1.5.2.1 趣旨	府省庁の情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うためには、情報システムの管理のために必要な情報を文書として整備する必要がある。また、府省庁全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するためには、府省庁が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備し、維持管理していく必要がある。これらのことを勘案し、本項では、府省庁における情報システムに係る文書整備及び台帳整備に関する情報セキュリティの対策基準を定める。	1.5.2.1 趣旨	府省庁の情報システムにおいて、適切な <u>情報</u> セキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うためには、情報システムの管理のために必要な情報を文書として整備する必要がある。また、府省庁全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するためには、府省庁が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備し、維持管理していく必要がある。これらのことを勘案し、本項では、府省庁における情報システムに係る文書整備及び台帳整備に関する情報セキュリティの対策基準を定める。	趣旨 の修 正
322	1.5.2.1(1)(a) (エ)解説	解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として	1.5.2.1(1)(a) (エ)解説	解説：所管する情報システムにおいて、適切な <u>情報</u> セキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書とし	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>整備することを定めた遵守事項である。文書の整備に<u>当たって</u>は、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。</p> <p>所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。</p> <p>電子計算機、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアにセキュリティホールが存在することにより使用上のリスクが高まった場合に、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。</p> <p>電子計算機の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システム構成要素の管理状況を確実に把握できるようにするとともに、障害・事故等を防止する責任の所在を明確化するために必要な事項である。</p> <p>通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、</p>		<p>て整備することを定めた遵守事項である。文書の整備に<u>あたって</u>は、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。</p> <p>所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。</p> <p>電子計算機、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアにセキュリティホールが存在することにより使用上のリスクが高まった場合に、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。</p> <p>電子計算機の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システム構成要素の管理状況を確実に把握できるようにするとともに、障害・事故等を防止する責任の所在を明確化するために必要な事項である。</p> <p>通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>及び通信回線の利用部署の記載は、通信回線の管理状況を把握するために必要な事項である。</p> <p>情報システムに係る仕様書又は設計書は、情報セキュリティ対策実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。</p> <p>情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。</p> <p>障害・事故等が発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。</p> <ul style="list-style-type: none"> ・業務継続計画で定める当該情報システムを利用する業務の重要性 ・情報システムの運用等の外部委託の内容 <p>また手順に記載される内容として、例えば以下が想定される。</p> <ul style="list-style-type: none"> ・障害・事故等の内容・影響度の大きさに応じた情報連絡先のリス 		<p>及び通信回線の利用部署の記載は、通信回線の管理状況を把握するために必要な事項である。</p> <p>情報システムに係る仕様書又は設計書は、情報セキュリティ対策実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。</p> <p>情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。</p> <p>障害・事故等が発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。</p> <ul style="list-style-type: none"> ・業務継続計画で定める当該情報システムを利用する業務の重要性 ・情報システムの運用等の外部委託の内容 <p>また手順に記載される内容として、例えば以下が想定される。</p> <ul style="list-style-type: none"> ・障害・事故等の内容・影響度の大きさに応じた情報連絡先のリス 	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>ト</p> <ul style="list-style-type: none"> ・情報システムを障害・事故等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準 ・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項 ・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場合等に支援を受けるための外部の専門家の連絡先 <p>なお、統括情報セキュリティ責任者が整備する対処手順(1.2.2.2(1)(c)を参照)により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。</p>		<p>ト</p> <ul style="list-style-type: none"> ・情報システムを障害・事故等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準 ・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項 ・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場合等に支援を受けるための外部の専門家の連絡先 <p>なお、統括情報セキュリティ責任者が整備する対処手順(1.2.2.2(1)(c)を参照)により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。</p>	
323	1.5.2.1(1)(b)	情報システムセキュリティ管理者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理においてセキュリティ対策を行うこと。	1.5.2.1(1)(b)	情報システムセキュリティ管理者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理において 情報 セキュリティ対策を行うこと。	遵守 事項 の修 正
324	1.5.2.1(1)(b) 解説	解説：所管する情報システムの運用管理において、適切なセキュリティ対策を行うことを求める遵守事項である。	1.5.2.1(1)(b) 解説	解説：所管する情報システムの運用管理において、適切な 情報 セキュリティ対策を行うことを求める遵守事項である。	解説 の修 正
325	1.5.2.1(2)(a)	統括情報セキュリティ責任者は、 全て の情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。	1.5.2.1(2)(a)	統括情報セキュリティ責任者は、 すべて の情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
326	1.5.2.1(2)(a) (ア)	情報システム名	1.5.2.1(2)(a)	情報システム名、 <u>管理課室及び管 理責任者の氏名・連絡先</u>	遵守 事項 の修 正
327	1.5.2.1(2)(a) (イ)	管理課室、 <u>当該情報システムセキ ュリティ</u> 責任者の氏名 <u>及び</u> 連絡先	1.5.2.1(2)(a)	<u>情報システム名、管理課室及び管 理責任者の氏名・連絡先</u>	遵守 事項 の修 正
328	1.5.2.1(2)(a) (オ)	取り扱う情報の <u>格付</u> 及び取扱制限 に関する事項	1.5.2.1(2)(a)	取り扱う情報の <u>格付け</u> 及び取扱制 限に関する事項	表現 の適 正化
329	1.5.2.1(2)(a)	<u>また、情報処理業務を外部に委託 する場合は、以下の事項を記載し た台帳を整備すること。</u>			遵守 事項 の追 加
330	1.5.2.1(2)(a) (キ)	<u>役務名</u>			遵守 事項 の追 加
331	1.5.2.1(2)(a) (ク)	<u>管理課室、当該情報システムセキ ュリティ</u> 責任者の氏名 <u>及び</u> 連絡先			遵守 事項 の追 加
332	1.5.2.1(2)(a) (ケ)	<u>契約事業者</u>			遵守 事項 の追 加
333	1.5.2.1(2)(a) (コ)	<u>契約期間</u>			遵守 事項 の追 加
334	1.5.2.1(2)(a) (サ)	<u>役務概要</u>			遵守 事項

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
					の追 加
335	1.5.2.1(2)(a) (シ)	ドメイン名（インターネット上で提供されるサービス等を利用する場合）			遵守 事項 の追 加
336	1.5.2.1(2)(a) (ス)	取り扱う情報の格付及び取扱制限に関する事項			遵守 事項 の追 加
337	1.5.2.1(2)(a) (ス)解説	<p>解説：府省庁全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するため、自府省庁が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備することを求める事項である。</p> <p>情報システム名、管理課室及び当該情報システムセキュリティ責任者の氏名・連絡先の記載は、府省庁が所管する全ての情報システムを把握し、当該情報システムに係る管理責任を把握するために必要な事項である。</p> <p>システム構成の記載は、情報システムを構成する電子計算機、通信回線及び通信回線装置に関する事項である。当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、府省庁としての情報セキュリティ対策を行うために一元的に</p>	1.5.2.1(2)(a) (オ)解説	<p>解説：府省庁全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するため、自府省庁が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備することを求める事項である。</p> <p>情報システム名、管理課室及び管理責任者の氏名・連絡先の記載は、府省庁が所管する全ての情報システムを把握し、当該情報システムに係る管理責任を把握するために必要な事項である。</p> <p>システム構成の記載は、情報システムを構成する電子計算機、通信回線及び通信回線装置に関する事項である。当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、府省庁としての情報セキュリティ対策を行うために一元的に把握する必要があると判断する事</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>把握する必要があると判断する事項を含める必要がある。</p> <p>接続する府省庁外通信回線の種別、取り扱う情報の格付及び取扱制限に関する事項の記載は、当該情報システムを設置し、また運用管理することによるセキュリティ上のリスクを府省庁として把握するために必要な事項である。なお、取り扱う情報の格付及び取扱制限に関する事項については、情報システムを構成する電子計算機等について機器別又は機器の形態・目的別に記載することが望ましい。</p> <p>当該情報システムの設計・開発、運用、保守に関する事項の記載は、実施責任者若しくは実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。</p> <p><u>また、情報処理業務を外部委託する場合は、役務名、管理課室及び当該情報システムセキュリティ責任者の氏名・連絡先、契約事業者、契約期間、役務概要、ドメイン名（インターネット上で提供される役務等を利用する場合）、取り扱う情報の格付及び取扱制限に関する</u></p>		<p>項を含める必要がある。</p> <p>接続する府省庁外通信回線の種別、取り扱う情報の格付け及び取扱制限に関する事項の記載は、当該情報システムを設置し、また運用管理することによるセキュリティ上のリスクを府省庁として把握するために必要な事項である。なお、取り扱う情報の格付け及び取扱制限に関する事項については、情報システムを構成する電子計算機等について機器別又は機器の形態・目的別に記載することが望ましい。</p> <p>当該情報システムの設計・開発、運用、保守に関する事項の記載は、実施責任者若しくは実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>事項を記載した決裁に係る書類を集約し、容易に参照できるようにすることで、台帳の代替とすることも可能である。</u></p> <p><u>なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該台帳を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。</u></p>			
338	1.5.2.2 趣旨	<p>機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要なセキュリティ機能が装備されていない場合及び購入後にセキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等で取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。</p> <p>この課題に対応するため、機器等を購入する際は、<u>それぞれの</u>府省庁の省庁対策基準に準拠した機器等の購入を行うべく、購入先への要求事項を定める必要がある。</p> <p>これらのことを勘案し、本項では、機器等の購入に関する対策基準として、<u>統括情報セキュリティ責任者による機器等の購入に係る規定の整備、情報システムセキュリティ責任者による当該規定の遵守についての遵守事項</u>を定める。</p>	1.5.2.2 趣旨	<p>機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要な<u>情報</u>セキュリティ機能が装備されていない場合及び購入後に<u>情報</u>セキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等で取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。</p> <p>この課題に対応するため、機器等を購入する際は、<u>各</u>府省庁の省庁対策基準に準拠した機器等の購入を行うべく、購入先への要求事項を定める必要がある。</p> <p>これらのことを勘案し、本項では、機器等の購入に関する対策基準を定める。</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
339	1.5.2.2(1)(b) 解説	<p>解説：<u>機器等の購入において、セキュリティ機能の要求仕様があり</u>、総合評価落札方式により購入を行う際に、当該機能を有する製品の中でも ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得している製品の優遇を選定基準の一つとすることを求める事項である。</p> <p>第三者による情報セキュリティ機能の客観的な評価のある製品を選定することによって、より信頼度の高い情報システムが構築できる。</p>	1.5.2.2(1)(b) 解説	<p>解説：<u>情報セキュリティ機能が重要である機器等の購入において</u>、総合評価落札方式により購入を行う際に、当該機能を有する製品の中でも ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得している製品の優遇を選定基準の一つとすることを求める事項である。</p> <p>第三者による情報セキュリティ機能の客観的な評価のある製品を選定することによって、より信頼度の高い情報システムが構築できる。</p>	解説 の修 正
340	1.5.2.3 趣旨	<p>ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、アクセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。</p> <p>加えて、開発するソフトウェアの処理に対するセキュリティホール の混入（設計及び作成時のミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発者により意図的に埋め込まれること等）についての防止対策も必要となる。</p>	1.5.2.3 趣旨	<p>ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、アクセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。</p> <p>加えて、開発するソフトウェアの処理に対するセキュリティホール の混入（設計及び作成時のミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発者により意図的に埋め込まれること等）についての防止対策も必要となる。</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		これらのことを勘案し、本項では、ソフトウェアを開発する際の対策基準として、 <u>統括情報セキュリティ責任者によるソフトウェア開発に係る規定の整備、情報システムセキュリティ責任者による当該規定の遵守についての遵守事項</u> を定める。		これらのことを勘案し、本項では、ソフトウェアを開発する際の対策基準を定める。	
341	1.5.2.3(1)(a) 解説	解説：本遵守事項では、統括情報セキュリティ責任者が情報システムセキュリティ責任者に求める規定を整備することとしているが、別途規定を <u>整備することとはせず</u> に、省庁対策基準内において情報システムセキュリティ責任者に対する遵守事項として（ア）～（セ）の事項を <u>直接</u> 定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく情報システムセキュリティ責任者となることに留意すること。	1.5.2.3(1)(a) 解説	解説：本事項では、統括情報セキュリティ責任者が情報システムセキュリティ責任者に求める規定を整備することとしているが、別途規定を <u>整備することとせず</u> に、省庁対策基準内において <u>直接</u> に情報システムセキュリティ責任者に対する遵守事項として（ア）～（セ）の事項を定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく情報システムセキュリティ責任者となることに留意すること。	解説 の修 正
342	1.5.2.3(1)(a) （ア）	情報システムセキュリティ責任者は、セキュリティに係る対策事項（本項(1)(a)(ウ)から(セ)の遵守事項をいう。）を満たすことが可能な開発体制を確保すること。	1.5.2.3(1)(a) （ア）	情報システムセキュリティ責任者は、セキュリティに係る対策事項（本項(ウ)から(セ)の遵守事項）を満たすことが可能な開発体制を確保すること。	遵守 事項 の修 正
343	1.5.2.3(1)(a) （ア）解説	解説：ソフトウェア開発を実施する体制が、セキュリティ維持の側面からも実施可能な開発体制（人員、機器、予算等）を確保することを求める事項である。 なお、開発体制の確保に <u>当たって</u>	1.5.2.3(1)(a) （ア）解説	解説：ソフトウェア開発を実施する体制が、セキュリティ維持の側面からも実施可能な開発体制（人員、機器、予算等）を確保することを求める事項である。 なお、開発体制の確保に <u>あたって</u>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		は、情報システムを統括する責任者に要求することとなる。ここで、情報システムを統括する責任者とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を指す。		は、情報システムを統括する責任者に要求することとなる。ここで、情報システムを統括する責任者とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を指す。	
344	1.5.2.3(1)(a) (イ)	情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項(本項(1)(a)(ウ)から(セ)の遵守事項をいう。)の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。	1.5.2.3(1)(a) (イ)	情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項(本項(ウ)から(セ)の遵守事項)の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。	遵守 事項 の修 正
345	1.5.2.3(1)(a) (ウ)解説	解説：ソフトウェア開発に係る情報資産を保護するための手順及び環境を定めることを求める事項である。「手順」とは、例えば、仕様書及びソースコード等の成果物に対してソフトウェアのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツールを指し、「環境」とは、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用する電子計算機の設置場所及びアクセス制御の方法等を指す。 なお、ソフトウェア開発を外部委託する場合は、委託先に対するセ	1.5.2.3(1)(a) (ウ)解説	解説：ソフトウェア開発に係る情報資産を保護するための手順及び環境を定めることを求める事項である。「手順」とは、例えば、仕様書、ソースコード等の成果物に対してソフトウェアのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツールを指し、「環境」とは、例えば、ドキュメント、ソースコードに対するアクセス権、開発に利用する電子計算機の設置場所、アクセス制御の方法等を指す。 なお、ソフトウェア開発を外部委託する場合は、委託先に対するセ	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		セキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。		セキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。	
346	1.5.2.3(1)(a) (オ)	情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。	1.5.2.3(1)(a) (オ)	情報システムセキュリティ責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付け及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。	表現 の適 正化
347	1.5.2.3(1)(a) (オ)解説	解説：開発するソフトウェアに必要となるセキュリティ機能について、その設計を適切に行うとともに、設計書に明確に記録することを求める事項である。 なお、汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、 <u>全て</u> を独自開発する場合であっても、外部から察知される脅威（例えば、SQLインジェクション、バッファオーバーフロー等）は存在するため、開発するソフトウェアの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。	1.5.2.3(1)(a) (オ)解説	解説：開発するソフトウェアに必要となるセキュリティ機能について、その設計を適切に行うとともに、設計書に明確に記録することを求める事項である。 なお、汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、 <u>すべて</u> を独自開発する場合であっても、外部から察知される脅威（例えば、SQLインジェクション、バッファオーバーフロー等）は存在するため、開発するソフトウェアの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。	解説 の修 正
348	1.5.2.3(1)(a) (ク)解説	解説：ソフトウェアの内部及び入出力するデータについて、処理の誤りや意図的な改ざん等を検出す	1.5.2.3(1)(a) (ク)解説	解説：ソフトウェアの内部及び入出力するデータについて、処理の誤りや意図的な改ざん等を検出す	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>るための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等を組み込むことを求める事項である。</p> <p>「データの妥当性」とは、例えば、HTML タグや JavaScript、SQL 文等として機能する不正な文字列や通信過程において生じたデータ誤り等、適切なデータ処理の障害になる情報がデータ内に含まれない状態であることを意味している。データの妥当性を確認する方法として、不正な文字列を変換し、又は削除する機能（いわゆるサニタイジング）の付加、チェックデジット（検査数字）による処理の正当性を確認する機能の付加等がある。</p>		<p>るための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等を組み込むことを求める事項である。</p> <p>「データの妥当性」とは、例えば、HTML タグや JavaScript、SQL 文などとして機能する不正な文字列や通信過程において生じたデータ誤りなど、適切なデータ処理の障害になる情報がデータ内に含まれない状態であることを意味している。データの妥当性を確認する方法として、不正な文字列を変換し、又は削除する機能（いわゆるサニタイジング）の付加、チェックデジット（検査数字）による処理の正当性を確認する機能の付加等がある。</p>	
349	1.5.2.3(1)(a) (ケ)	<p>情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST : Security Target）の ST 評価及び ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価及び ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設</p>	1.5.2.3(1)(a) (ケ)	<p>情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST : Security Target）の ST 評価・ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価・ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様</p>	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		計仕様書において重要なセキュリティ要件の変更が軽微であると認めるときは、この限りでない。		書において重要なセキュリティ要件の変更が軽微であると認めるときは、この限りでない。	
350	1.5.2.3(1)(a) (ケ)解説	<p>解説：重要なセキュリティ要件があるソフトウェアについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を行うことを求める事項である。</p> <p>「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。ソフトウェアの開発が終了するまでにセキュリティ設計仕様書について、ST 評価及び ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。</p> <p>なお、ソフトウェア開発を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。</p>	1.5.2.3(1)(a) (ケ)解説	<p>解説：重要なセキュリティ要件があるソフトウェアについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価・ST 確認を行うことを求める事項である。</p> <p>「ST 評価・ST 確認を受けること」とは、ST 評価・ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。ソフトウェアの開発が終了するまでにセキュリティ設計仕様書について、ST 評価・ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。</p> <p>なお、ソフトウェア開発を外部委託する場合には、契約時に条件として含め納品までに ST 評価・ST 確認を受けさせることになる。</p>	解説 の修 正
351	1.5.2.3(1)(a) (シ)解説	<p>解説：ソースコードレビューの範囲及び方法について定めることを求める事項である。例えば、脆弱性の原因となるソースコードにつ</p>	1.5.2.3(1)(a) (シ)解説	<p>解説：ソースコードレビューの範囲及び方法について定めることを求める事項である。例えば、脆弱性の原因となるソースコードにつ</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>いては、開発言語ごとに典型的なパターンが知られていることから、これらについては静的解析ツール、又はソースコードレビュー等による検証が挙げられる。なお、ソースコードレビューについては、開発するソフトウェアだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。</p>		<p>いては、開発言語ごとに典型的なパターンが知られていることから、これらについては静的解析ツール、又はソースコードレビュー等による検証が挙げられる。なお、ソースコードレビューについては、開発するソフトウェアだけを対象として想定しており、市販製品を組み込む場合など、ソースコードの入手が困難な場合に実施することは想定していない。</p>	
352	1.5.2.3(1)(a) (ス)解説	<p>解説：セキュリティの観点から必要な試験がある場合にその試験の項目及び試験方法を定めることを求める事項である。攻撃が行われた際にソフトウェアがどのような動作をするかを試験する項目として想定しており、具体的には、バッファオーバーフローが発生しないか、想定外のデータの入力を拒否できるか、DoS 攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、といった項目が挙げられる。</p> <p>なお、セキュリティ機能の試験だけにとどまらず、ソフトウェアの試験計画全般について、セキュリティホールの有無、必要なチェック機能の欠如等について、単体試験、結合試験、統合試験等の複数の試験を通じて、必要な試験が網羅されるよう留意することが望ま</p>	1.5.2.3(1)(a) (ス)解説	<p>解説：セキュリティの観点から必要な試験がある場合にその試験の項目及び試験方法を定めることを求める事項である。攻撃が行われた際にソフトウェアがどのような動作をするかを試験する項目として想定しており、具体的には、バッファオーバーフローが発生しないか、想定外のデータの入力を拒否できるか、DoS 攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、といった項目が挙げられる。</p> <p>なお、セキュリティ機能の試験だけにとどまらず、ソフトウェアの試験計画全般について、セキュリティホールの有無、必要なチェック機能の欠如等について、単体試験、結合試験、統合試験など複数の試験を通じて、必要な試験が網羅されるよう留意することが望ま</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		しい。		しい。	
353	1.5.2.4	1.5.2.4 主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順			構成 変更
354	1.5.2.4 趣旨	<p>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、本来アクセス権のない者が、故意又は過失により、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。</p> <p>一方、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かを情報ごとにアクセス制御する必要がある。また、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。</p> <p>これらのことを勘案し、本項では、主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準として、統括情報セキュリティ責任者による</p>			趣旨 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p><u>主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備、情報セキュリティ責任者及び情報システムセキュリティ責任者による当該規定の遵守、情報システムセキュリティ責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。</u></p> <p><u>なお、1.4.1.1において識別コードと主体認証情報の管理等に関する判断基準を、統一技術基準2.2.1.1~2.2.1.5においても主体認証・アクセス制御・権限管理・証跡管理・保障等の導入等に関する対策基準を定めている。</u></p>			
355	1.5.2.4(1)	<u>主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備</u>			構成 変更
356	1.5.2.4(1)(a)	<u>統括情報セキュリティ責任者は、府省庁における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を、以下の事項を含めて定めること。</u>			遵守 事項 の追 加
357	1.5.2.4(1)(a) 解説	<u>解説：本遵守事項では、統括情報セキュリティ責任者が情報セキュリティ責任者及び情報システムセキュリティ責任者に求める規定を整備することとしているが、別途規定を整備することはせずに、省庁対策基準内において情報セキュリティ責任者及び情報システムセ</u>			解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>セキュリティ責任者に対する遵守事項として(ア)～(カ)の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく情報セキュリティ責任者及び情報システムセキュリティ責任者となることに留意すること。</u>			
358	1.5.2.4(1)(a) (ア)	情報システムセキュリティ責任者は、 <u>全ての</u> 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 <u>必要</u> があると判断すること。	2.1.1.1(1)(a)	情報システムセキュリティ責任者は、 <u>すべての</u> 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 <u>必要性</u> があると判断すること。	構成 変更
359	1.5.2.4(1)(a) (ア)解説	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 <u>に</u> 、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。 (後段の解説は、2.2.1.1(1)(a)解説へ移動)	2.1.1.1(1)(a) 解説	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 <u>は</u> 、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。 <u>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カードや磁気ストライプカード等、本人の</u>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				<p><u>みが所有する機器等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。</u></p> <p><u>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。</u></p> <p><u>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。</u></p>	
360	1.5.2.4(1)(a) (イ)	情報システムセキュリティ責任者は、 <u>全ての</u> 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		(2.1.1.2(1)(a)から移動)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>要があると判断すること。</p> <p>解説：～</p>			
361	1.5.2.4(1)(a) (ウ)	<p>情報システムセキュリティ責任者は、<u>全て</u>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。</p>		(2.1.1.3(1)(a)から移動)	構成 変更
362	1.5.2.4(1)(a) (ウ)解説	<p>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<u>に</u>、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。</p> <p>なお、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（発行、更新及び変更を含む。以下この項において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。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。</p>	2.1.1.3(1)(a) 解説	<p>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<u>は</u>、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。</p> <p>なお、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（発行、更新及び変更を含む。以下この項において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。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。</p>	解説 の修 正
363	1.5.2.4(1)(a) (エ)	<p><u>情報セキュリティ責任者</u>は、<u>全て</u>の情報システムについて、証跡管</p>	2.1.1.4(1)(a)	<p><u>情報システムセキュリティ責任者</u>は、<u>すべて</u>の情報システムについ</p>	主語 の変

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		理を行う必要性の有無を検討すること。		て、証跡管理を行う必要性の有無を検討すること。	更
364	1.5.2.4(1)(a) (エ)解説	<p>解説：証跡管理を行う前提として、情報セキュリティ責任者に、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を求める事項である。</p> <p>情報セキュリティは、府省庁の内部及び外部からの不正アクセス、不正侵入、誤操作又は不正操作等の様々な原因により損なわれることがある。また、行政事務の遂行以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。万一問題が発生した場合にはその実行者を特定する必要があるため、一連の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。</p> <p>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証跡管理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。</p> <p>証跡には、以下のような管理記録が考えられる。</p>	2.1.1.4(1)(a) 解説	<p>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に、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を求める事項である。</p> <p>情報セキュリティは、様々な原因で損なわれることがある。クラッカー等の部外者による不正アクセス、不正侵入、操作する者の誤操作又は不正操作、府省庁の内部及び外部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。万一問題が発生した場合にはその実行者を特定する必要があるため、そのために不正アクセス、不正侵入等の事象、操作する者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。</p> <p>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証跡管理情報の</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<ul style="list-style-type: none"> ・識別コードの発行等の管理履歴 ・各識別コードへのアクセス権設定の管理履歴 ・それらの権限管理者の許認可そのものの管理履歴 <p><u>また</u>、証跡として、上記の他に以下のような利用記録や監視記録等を含めることも考えられる。</p> <ul style="list-style-type: none"> ・利用者による情報システムの操作記録 ・操作する者、監視する者及び保守する者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 <p><u>なお、証跡管理を行う必要性の有無の判断に当たっては、情報システムの側面だけではなく、組織的な側面からの検討も必要であるため、情報セキュリティ責任者によるものとしている。</u></p>		<p>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。</p> <p>証跡には、以下のような管理記録が考えられる。</p> <ul style="list-style-type: none"> ・識別コードの発行等の管理履歴 ・各識別コードへのアクセス権設定の管理履歴 ・それらの権限管理者の許認可そのものの管理履歴 <p><u>なお</u>、証跡として、上記の他に以下のような利用記録や監視記録等を含めることも考えられる。</p> <ul style="list-style-type: none"> ・利用者による情報システムの操作記録 ・操作する者、監視する者及び保守する者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 	
365	1.5.2.4(1)(a) (オ)	<p>情報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おいては、証跡として取得する情報項目及び証跡の保存期間を定めること。</p> <p>解説：～</p>		(2.1.1.4(1)(c)から移動)	構成 変更
366	1.5.2.4(1)(a) (カ)	<p>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られた情報システムにおいて</p>		(2.1.1.4(4)(a)から移動)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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すること。 解説：～			
367	1.5.2.4(1)(a) (キ)	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、保証のための対策を行う必要性の有無を検討すること。 解説：～		(2.1.1.5(1)(a)から移動)	構成 変更
368	1.5.2.4(2)	主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の遵守			構成 変更
369	1.5.2.4(2)(a)	情報セキュリティ責任者及び情報システムセキュリティ責任者は、府省庁における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定に基づいて、情報システムの導入を行うこと。			遵守 事項 の追 加
370	1.5.2.4(2)(a) 解説	解説：情報セキュリティ責任者及び情報システムセキュリティ責任者が、府省庁で主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を遵守して、情報システムの導入を行うことを定めた事項である。			解説 の追 加
371	1.5.2.4(3)	取得した証跡の点検、分析及び報告			構成 変更
372	1.5.2.4(3)(a)	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		(2.1.1.4(3)(a)から移動)	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		認められた情報システムにおいては、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、又は情報セキュリティ責任者に報告すること。			
373	1.5.2.4(3)(a)	<p>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。</p> <p>取得した証跡は、その<u>全て</u>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。</p> <p>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。</p> <p>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。</p>	2.1.1.4(3)(a) 解説	<p>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。</p> <p>取得した証跡は、その<u>すべて</u>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。</p> <p>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。</p> <p>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。</p>	解説 の修 正
374	1.5.2.5	1.5.2.5 暗号と電子署名の標準手	1.5.2.4	1.5.2.4 暗号と電子署名の標準手	構成

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		順		順	変更
375	1.5.2.5 趣旨	<p>情報システムの利用において、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は、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、行政事務従事者による個別判断で選択されることのないよう、府省庁で標準となる手順を定めることが重要である。</p> <p>これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、統括情報セキュリティ責任者による暗号と電子署名に係る規定の整備、行政事務従事者による当該規定の遵守についての遵守事項を定める。</p> <p>なお、1.5.2.4において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、統一技術基準2.2.1.1~2.2.1.5においても各機能の導入等に関する対策基準を定めている。</p>	1.5.2.4 趣旨	<p>情報システムの利用において、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は、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、行政事務従事者による個別判断で選択されることのないよう、府省庁で標準となる手順を定めることが重要である。</p> <p>これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準を定める。</p>	趣旨 の修 正
376	1.5.2.5(1)(a)	統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び 運用方法	1.5.2.4(1)(a)	統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び 方法 を、以	遵守 事項 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		を、以下の事項を含めて定めること。		下の事項を含めて定めること。	正
377	1.5.2.5(1)(a) (イ)	情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。	1.5.2.5(1)(a) (イ)	情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。	証言 の適 正化
378	1.5.2.5(1)(a) (イ)解説	解説：府省庁内の情報システムにおける暗号化及び電子署名について、使用を認めるアルゴリズム及び方法を統括情報セキュリティ責任者が定めることを求める事項である。アルゴリズム及び方法は、暗号及び電子署名の使用場面等に応じて整備することも可能である。例えば、電子メールの暗号化に関してアルゴリズムを定めるとともにその方法を S/MIME とし、ウェブサーバとブラウザの通信の暗号化に関してアルゴリズムを定めるとともに方法を SSL とする。他に、データベースのデータ暗号化や、電子申請における電子署名等についても、アルゴリズム及び方法を定めることが考えられる。行政事務従事者は、文書の作成、	1.5.2.4(1)(a) (イ)解説	解説：府省庁内の情報システムにおける暗号化及び電子署名について、使用を認めるアルゴリズム及び方法を統括情報セキュリティ責任者が定めることを求める事項である。アルゴリズム及び方法は、暗号及び電子署名の使用場面等に応じて整備することも可能である。例えば、電子メールの暗号化に関してアルゴリズムを定めるとともにその方法を S/MIME とし、ウェブサーバとブラウザの通信の暗号化に関してアルゴリズムを定めるとともに方法を SSL とする。他に、データベースのデータ暗号化や、電子申請における電子署名等についても、アルゴリズム及び方法を定めることが考えられる。行政事務従事者は、文書の作成、	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>電子メールの送受信等に汎用のソフトウェアを日常的に使用しているが、これらのソフトウェアでは、暗号化及び電子署名について、複数のアルゴリズムを用意し、設定画面等で利用者が選択できるようにしている場合がある。そのような場合には、行政事務従事者は、</p> <p>(ア) にもとづき電子政府推奨暗号リストに記載されたアルゴリズムを選択して使用することになる。</p> <p>情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、情報システムセキュリティ責任者は、本遵守事項に基づき統括情報セキュリティ責任者が定めたアルゴリズム及び方法を使用する。</p> <p>暗号化又は電子署名を行う特定の箇所について見ると、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、複数のアルゴリズムを実装し、使用可能とする場合がある。この場合には、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、電子政府推奨暗号リストに記載されたアルゴリズムを少なくとも一つ含めることを求める。</p>		<p>電子メールの送受信等に汎用のソフトウェアを日常的に使用しているが、これらのソフトウェアでは、暗号化及び電子署名について、複数のアルゴリズムを用意し、設定画面等で利用者が選択できるようにしている場合がある。そのような場合には、行政事務従事者は、</p> <p>(ア) にもとづき電子政府推奨暗号リストに記載されたアルゴリズムを選択して使用することになる。</p> <p>情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、情報システムセキュリティ責任者は、本事項に基づき統括情報セキュリティ責任者が定めたアルゴリズム及び方法を使用する。</p> <p>暗号化又は電子署名を行う特定の箇所について見ると、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、複数のアルゴリズムを実装し、使用可能とする場合がある。この場合には、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、電子政府推奨暗号リストに記載されたアルゴリズムを少なくとも一つ含めることを求める。</p>	
379	1.5.2.5(1)(a) (ウ)	<p>アルゴリズムが危殆化した場合の緊急対応計画の必要性の有無を検討し、必要と認めたときは、緊急</p>			遵守 事項 の追

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>対応計画を定めること。</u>			加
380	1.5.2.5(1)(a) (ウ)解説	<u>解説：アルゴリズムが危殆化した場合に備えて、情報システムの停止等の緊急避難的な対応計画を策定することを求める事項である。対象となるアルゴリズムは、用途に応じて変わること</u> <u>に留意すること。</u>			解説 の修 正
381	1.5.2.5(1)(b) (イ)解説	解説：鍵の保存手順を保存方法及び保存場所を含めて定めることによつて、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。 鍵の保存方法としては、電磁的記録媒体に保存することが考えられるが、それをどのように保存するかの方法や、保存する際に電磁的記録媒体以外の記録媒体と併用することの是非 <u>等</u> についても定める必要がある。 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、鍵を保存する電磁的記録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	1.5.2.5(1)(b) (イ)解説	解説：鍵の保存手順を保存方法及び保存場所を含めて定めることによつて、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。 鍵の保存方法としては、電磁的記録媒体に保存することが考えられるが、それをどのように保存するかの方法や、保存する際に電磁的記録媒体以外の記録媒体と併用することの是非 <u>など</u> についても定める必要がある。 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、鍵を保存する電磁的記録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	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		ある。 情報システム共通として鍵の保存手順を定める場合には、統括情報セキュリティ責任者が直接それを定めることが考えられる。あるいは、情報システムごとに鍵の保存手順を個別に定めるのであれば、各情報システムセキュリティ責任者にそれを定めさせることについて、定めるという方法でもよい。		ある。 情報システム共通として鍵の保存手順を定める場合には、統括情報セキュリティ責任者が直接それを定めることが考えられる。あるいは、情報システムごとに鍵の保存手順を個別に定めるのであれば、各情報システムセキュリティ責任者にそれを定めさせることについて、定めるという方法でもよい。	
382	1.5.2.5(1)(c) 解説	解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、 <u>鍵のバックアップ手順等</u> 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し、又は消失した場合には、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等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。 なお、 <u>本遵守事項</u> における鍵の <u>バックアップ手順等</u> は、前事項の鍵の管理手順等を含めて整備することも可能である。	1.5.2.4(1)(c) 解説	解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、 <u>鍵のバックアップ取得手順又は鍵の預託手順</u> 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し、又は消失した場合には、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等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。 なお、 <u>本事項</u> における鍵の <u>バックアップ手順及び鍵の預託手順</u> は、前事項の鍵の管理手順等を含めて整備することも可能である。	解説 の修 正
383	1.5.2.5(1)(d)	<u>統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電</u>			遵守 事項 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤(GPKI)が発行している場合には、それを使用するように定めること。</u>			
384	1.5.2.5(1)(d) 解説	<u>解説：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書をGPKIが発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。</u>			解説 の追 加
385	1.5.2.6	1.5.2.6 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	1.5.2.5	1.5.2.5 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	構成 変更
386	1.5.2.6 趣旨	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、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、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として、 <u>統括情報セキュリティ責任者による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の整備、行政事務従事者による当該規</u>	1.5.2.5 趣旨	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、 各 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。	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		定の遵守についての遵守事項 を定める。			
387	1.5.2.6(1)(a) 解説	<p>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。</p> <p>府省庁外の情報セキュリティ水準の低下を招く可能性のある行為としては、例えば、以下のものが挙げられる。</p> <p>(ア) 不適切なソフトウェア及びサービスの使用要求：電子行政サービス（例えば、府省庁のウェブによるコンテンツの提示等を言う。以下、同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービスへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。</p> <p>(イ) ソフトウェアの不適切な設定要求：電子行政サービスを利用するために、利用者の環境にインストールされているソフトウェア（府省庁が直接提供していないソフトウェア（例えば、クライアント</p>	1.5.2.5(1)(a) 解説	<p>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。</p> <p>府省庁外の情報セキュリティ水準の低下を招く可能性のある行為としては、例えば、以下のものが挙げられる。</p> <p>(ア) 不適切なソフトウェアの使用要求：電子行政サービス（例えば、府省庁のウェブによるコンテンツの提示等を言う。以下、同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェアの使用（脆弱性の問題が指摘されているソフトウェアのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェアへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。</p> <p>(イ) ソフトウェアの不適切な設定要求：電子行政サービスを利用するために、利用者の環境にインストールされているソフトウェア（府省庁が直接提供していないソフトウェア（例えば、クライアント</p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>トPCのOSやウェブブラウザ等)以下、同じ。)について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。</p> <p>(ウ) ソフトウェア等の不適切な削除要求：府省庁のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。</p> <p>「明示的に要求する行為」とは、「『このような設定を変更してください。』<u>等</u>のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけでなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。</p> <p>以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。</p> <ul style="list-style-type: none"> ・ソフトウェアを実行させる場合：電子行政サービスのためのソフトウェアを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windowsの「.exe」ファイル等）、 		<p>以下、同じ。)について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。</p> <p>(ウ) ソフトウェア等の不適切な削除要求：府省庁のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。</p> <p>「明示的に要求する行為」とは、「『このような設定を変更してください。』<u>など</u>のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけでなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。</p> <p>以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。</p> <ul style="list-style-type: none"> ・ソフトウェアを実行させる場合：電子行政サービスのためのソフトウェアを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windowsの「.exe」ファイル等）、ランタイム環境実行型（例えば、 	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>ランタイム環境実行型（例えば、Java アプレットや Windows の ActiveX ファイル等）、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの<u>全て</u>を含む。</p> <p>・HTML メール等を送信する場合：府省庁から HTML メール等（利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。</p> <p>これらの場合については、結果的に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。実行させるソフトウェアの提供については、オンラインによる提供（ウェブへの掲載、メールの添付等）について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については<u>電子署名</u>を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみ</p>		<p>Java アプレットや Windows の ActiveX ファイル等）、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの<u>すべて</u>を含む。</p> <p>・HTML メール等を送信する場合：府省庁から HTML メール等（利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。</p> <p>これらの場合については、結果的に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。実行させるソフトウェアの提供については、オンラインによる提供（ウェブへの掲載、メールの添付等）について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については<u>署名</u>を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>の送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。</p> <p><u>やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。</u></p> <p><u>また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。</u></p> <p><u>ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。</u></p> <p><u>また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名（コード署名）が必要な場合には、政府認証基盤（GPKI）で発行したコード署名証明書を利用することが望ましい。</u></p> <p><u>なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。</u></p> <p>（ア）（イ）については、当該電子行政サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘され</p>		<p>提供の義務付け<u>など</u>が考えられる。</p> <p>（ア）（イ）については、当該電子行政サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該電子行政サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める<u>など</u>の方法を考えることができる。</p> <p>例えば、電子行政用ウェブのアプリケーションを利用するために、利用者のPC上に<u>予め</u>標準的にインストールされているソフトウェアがバージョンAであったとする。その後、そのソフトウェアの最新バージョンがBに更新され、また、バージョンAについて脆弱性が公開された場合には、バージョンBで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケー</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>る場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該電子行政サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める<u>等</u>の方法を考慮することができる。</p> <p>例えば、電子行政用ウェブのアプリケーションを利用するために、利用者のPC上にあらかじめ標準的にインストールされているソフトウェアがバージョンAであったとする。その後、そのソフトウェアの最新バージョンがBに更新され、また、バージョンAについて脆弱性が公開された場合には、バージョンBで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョンAだけで動作するような設計では、利用者に脆弱性のあるバージョンAを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンBでも当該アプリケ</p>		<p>ションがそのソフトウェアのバージョンAだけで動作するような設計では、利用者に脆弱性のあるバージョンAを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンBでも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		ーションを利用できるようにする等) を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。			
388	1.5.2.6(2)(a) 解説	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府省庁の役割を定めた事項である。行政事務従事者は、組織及び個人として措置を講ずることが重要である。	1.5.2.5(2)(a) 解説	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。行政事務従事者は、組織及び個人として措置を講ずることが重要である。	解説 の修 正
389	1.5.2.7	1.5.2.7 ドメイン名の使用についての対策	1.5.2.6	1.5.2.6 ドメイン名の使用についての対策	構成 変更
390	1.5.2.7 趣旨	府省庁では、行政に係る情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサーバ、電子メール等を用意し、国民等の利用に供している。これらのサービスはインターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の府省庁のものであると信頼できることが重要である。一方、インターネット上のサービスの特定はドメイン名（例えば、nisc.go.jp のこと。）が重要な役割を果たしており、府省庁において一貫したドメイン名を使用することにより、万一府省庁以外の者による悪用や詐称がなされた場合にも国民が気付くための条件を整備する必要がある。これらのことを勘案し、本項では、	1.5.2.6 趣旨	府省庁では、行政に係る情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサーバ、電子メール等を用意し、国民等の利用に供している。これらのサービスはインターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の府省庁のものであると信頼できることが重要である。一方、インターネット上のサービスの特定はドメイン名（例えば、nisc.go.jp のこと。）が重要な役割を果たしており、府省庁において一貫したドメイン名を使用することにより、万一府省庁以外の者による悪用や詐称がなされた場合にも国民が気付くための条件を整備する必要がある。これらのことを勘案し、本項では、	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		府省庁におけるドメイン名の使用に関する対策基準として、 統括情報セキュリティ責任者によるドメイン名の使用についての規定の整備 、 行政事務従事者による当該規定の遵守についての遵守事項 を定める。		府省庁におけるドメイン名の使用に関する対策基準を定める。	
391	1.5.2.7(1)(a) 解説	解説： 本遵守事項 では、統括情報セキュリティ責任者が行政事務従事者に求める規定を 整備することとしているが、別途規定を整備することとはせずに 、省庁対策基準内において行政事務従事者に対する遵守事項として（ア）～（ウ）の事項を 直接 定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく行政事務従事者となることに留意すること。	1.5.2.6(1)(a) 解説	解説： 本事項 では、統括情報セキュリティ責任者が行政事務従事者に求める規定を整備することとしているが、 別途規定を整備することとせずに 、省庁対策基準内において 直接 に行政事務従事者に対する遵守事項として（ア）～（ウ）の事項を定める方法も可能である。ただし、後者の方法では、自己点検の対象が統括情報セキュリティ責任者ではなく行政事務従事者となることに留意すること。	解説 の修 正
392	1.5.2.7(1)(a) （ア）・	.go.jp で終わるドメイン名	1.5.2.6(1)(a) （ア）・	go.jp で終わるドメイン名	遵守 事項 の修 正
393		(削除)	1.5.2.6(1)(a) （ア）・	日本語ドメイン名の中で行政等に関するものとして予約されたドメイン名	遵守 事項 の修 正
394	1.5.2.7(1)(a) （ア）・	具体的には、電子メールの送信においては以下の条件を 全て 満たすことが必要である。	1.5.2.6(1)(a) （ア）・	具体的には、電子メールの送信においては以下の条件を すべて 満たすことが必要である。	表現 の適 正化
395	1.5.2.7(1)(a) （ア）・	また、政府ドメイン名のウェブページでの掲載においては以下の条件を 全て 満たすことが必要であ	1.5.2.6(1)(a) （ア）・	また、政府ドメイン名のウェブページでの掲載においては以下の条件を すべて 満たすことが必要であ	表現 の適 正化

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		る。		る。	
396	1.5.2.7(1)(a) (ア)解説	<p>解説：アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.nisc.go.jp/）やFTPサーバ（例えば、ftp://ftp.nisc.go.jp/）等へのアクセスを促すことをいう。<u>上記には、ウェブページの閲覧に必要なソフトウェア（プラグインを含む）を入手できる政府ドメイン名以外のウェブサイトを知覚する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先（例えば、null@nisc.go.jp）への送信等を促すことをいう。</u></p> <p><u>本遵守事項</u>における告知にあたる場合とは、情報提供のきっかけが府省庁側にある場合で、告知にあたらぬ場合とは、情報提供のきっかけが府省庁側にない場合である。例えば、府省庁外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらぬ、<u>本遵守事項</u>の対象とはならない。なお、いずれの場合についても媒体の種類（郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。</p> <p>「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時</p>	1.5.2.6(1)(a) (ア)解説	<p>解説：アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.nisc.go.jp/）やFTPサーバ（例えば、ftp://ftp.nisc.go.jp/）等へのアクセスを促すことをいう。送信させることを目的にドメイン名を告知するとは、電子メールの宛先（例えば、null@nisc.go.jp）への送信等を促すことをいう。</p> <p><u>本項</u>における告知にあたる場合とは、情報提供のきっかけが府省庁側にある場合で、告知にあたらぬ場合とは、情報提供のきっかけが府省庁側にない場合である。例えば、府省庁外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらぬ、<u>本項</u>の対象とはならない。なお、いずれの場合についても媒体の種類（郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。</p> <p>「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。</p> <p><u>「日本語ドメイン名の中で行政等に関するものとして予約されたドメイン名」とは、「JPドメイン名」</u></p>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>点で」実施しなければならない遵守事項である。</p> <p>なお、在外公館のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。</p> <p>政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなのが考えられる。</p> <p>(例)</p> <ul style="list-style-type: none"> ・この告知についてのお問い合わせは、null@nisc.go.jp までご連絡ください。 ・この告知で案内しているウェブサイトは〇〇〇協会が運営しており、内閣官房が運営しているものではありません。 ・この告知で案内しているウェブサイトのアドレスについては、2007年12月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。 		<p><u>の登録管理事業者によって行政等に関するものとして予約されている文字列に .jp を付加した形で終わるドメイン名をいう（以下、本項において同じ）。例えば、「内閣府.jp」等。</u></p> <p>なお、在外公館のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。</p> <p>政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなのが考えられる。</p> <p>(例)</p> <ul style="list-style-type: none"> ・この告知についてのお問い合わせは、null@nisc.go.jp までご連絡ください。 ・この告知で案内しているウェブサイトは〇〇〇協会が運営しており、内閣官房が運営しているものではありません。 ・この告知で案内しているウェブサイトのアドレスについては、2007年12月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。 	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
397	1.5.2.7(1)(a) (イ)	行政事務従事者は、府省庁外の者に対して、 <u>送信に使用する電子メールのドメイン名は</u> 、政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合を除く。	1.5.2.6(1)(a) (イ)	行政事務従事者は、府省庁外の者に対して、 <u>電子メールの送信元としてドメイン名を使用する場合には</u> 、政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合を除く。	遵守 事項 の修 正
398	1.5.2.7(1)(a) (イ)解説	解説： <u>送信に使用する電子メールのドメイン名として政府ドメインの使用を求める</u> 遵守事項である。 <u>また</u> 、電子メールの送信元として政府ドメイン名を使用するに当たっては、その送信に用いる電子メールサーバは、当該政府ドメイン名にかかる DNS サーバの MX レコードで指定している IP アドレスのサーバで <u>ある必要がある。</u> <u>なお、送信元として使われる電子メールアドレスを外部に告知する場合には、適切なドメイン名で告知するように、事前に準備する必要がある。</u>	1.5.2.6(1)(a) (イ)解説	解説： <u>「使用する場合」としているが、実際には「送信に使用する電子メールのドメイン名を決める時点で」実施しなければならない</u> 遵守事項である。 <u>なお</u> 、電子メールの送信元として政府ドメイン名を使用するに当たっては、その送信に用いる電子メールサーバは、当該政府ドメイン名にかかる DNS サーバの MX レコードで指定している IP アドレスのサーバで <u>なければならない。</u>	解説 の修 正
399	1.5.2.7(1)(a) (ウ)解説	解説：府省庁外の者にアクセスさせることを目的として情報を保存するサーバとは、主としてウェブサーバのことをいう。 (ア)により政府ドメイン名以外のドメイン名を告知することを禁止しているが、告知していなくとも、政府機関としての情報を政府ドメイン名以外のドメイン名のウェブサーバに保存していると、インターネット上の検索サービス <u>等</u>	1.5.2.6(1)(a) (ウ)解説	解説：府省庁外の者にアクセスさせることを目的として情報を保存するサーバとは、主としてウェブサーバのことをいう。 (ア)により政府ドメイン名以外のドメイン名を告知することを禁止しているが、告知していなくとも、政府機関としての情報を政府ドメイン名以外のドメイン名のウェブサーバに保存していると、インターネット上の検索サービス <u>な</u>	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>により表示される場合がある。そのような場合には、なりすましをしようとする者が、政府機関からの情報を装った内容を保存したウェブを作成して、検索されるのを待ち伏せするという方法によるなりすましが考えられる。普段から政府ドメイン名のウェブサーバだけを使うことで、検索結果が政府ドメイン名以外である場合に、そこに保存されている情報の真偽について府省庁以外の者が注意を心がけやすくなる。</p> <p>なお、既存のウェブサーバ等においてこれら以外のドメイン名のサーバの使用が避けられない場合には、本遵守事項に対する例外措置を必要な期間に限り適用し、かつ、政府ドメイン名のサイトから当該ドメイン名を案内することにより、新規に告知するドメイン名について（ア）を遵守すること。</p> <p>また、政府ドメイン名以外のウェブサーバの使用を停止した後も、当該ドメイン名を不正に利用されないように管理することに注意しなければならない。具体的には、そのような用途に使用した当該ドメイン名については、使用後も登録管理を一定期間維持することを求める規定を設ける必要がある。</p>		<p><u>ど</u>により表示される場合がある。そのような場合には、なりすましをしようとする者が、政府機関からの情報を装った内容を保存したウェブを作成して、検索されるのを待ち伏せするという方法によるなりすましが考えられる。普段から政府ドメイン名のウェブサーバだけを使うことで、検索結果が政府ドメイン名以外である場合に、そこに保存されている情報の真偽について府省庁以外の者が注意を心がけやすくなる。</p> <p>なお、既存のウェブサーバ等においてこれら以外のドメイン名のサーバの使用が避けられない場合には、本号に対する例外措置を必要な期間に限り適用し、かつ、政府ドメイン名のサイトから当該ドメイン名を案内することにより、新規に告知するドメイン名について（ア）を遵守すること。</p> <p>また、政府ドメイン名以外のウェブサーバの使用を停止した後も、当該ドメイン名を不正に利用されないように管理することに注意しなければならない。具体的には、そのような用途に使用した当該ドメイン名については、使用後も登録管理を一定期間維持することを求める規定を設ける必要がある。</p>	
400	1.5.2.7(2)(a) 解説	解説： 全て の行政事務従事者が、インターネットを経由した行政サ	1.5.2.6(2)(a) 解説	解説： すべて の行政事務従事者が、インターネットを経由した行政サ	解説 の修

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>ービスの提供に当たり、府省庁で整備したドメイン名の使用についての規定を遵守して、政府ドメイン名等のドメイン名を適切に使用することを定めた事項である。</p> <p><u>なお、ウェブサイトの構築・管理等の「ドメイン名の使用」を伴う業務を外部委託する場合は、行政事務従事者が委託先への要求事項に含める必要がある。</u></p> <p><u>そのような業務の外部委託は、情報システム部門以外の者が担当となる場合があるため、それらの者にも本遵守事項を周知すること。</u></p>		<p>ービスの提供にあたり、府省庁で整備したドメイン名の使用についての規定を遵守して、政府ドメイン名等のドメイン名を適切に使用することを定めた事項である。</p>	正
401	1.5.2.8	1.5.2.8 不正プログラム感染防止のための日常的实施事項	1.5.2.7	1.5.2.7 不正プログラム感染防止のための日常的实施事項	構成 変更
402	1.5.2.8 趣旨	<p>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、主体認証情報等の要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。不正プログラムへの感染を防止するためには、情報システムを利用する全ての行政事務従事者が、アンチウイルスソフトウェア等を活用して不正プログラムの検知・除去に努めるほか、ファイルの閲覧や実行、外部ファイルの取り込み等において十分な注意を払う必要がある。</p> <p>これらのことを勘案し、本項では、不正プログラム感染の回避を目的</p>	1.5.2.7 趣旨	<p>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、主体認証情報等の要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。不正プログラムへの感染を防止するためには、情報システムを利用する全ての行政事務従事者が、アンチウイルスソフトウェア等を活用して不正プログラムの検知・除去に努める他、ファイルの閲覧や実行、外部ファイルの取り込み等において十分な注意を払う必要がある。</p> <p>これらのことを勘案し、本項では、不正プログラム感染の回避を目的</p>	趣旨 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		とした対策基準として、 統括情報セキュリティ責任者による不正プログラム対策に係る規定の整備、 行政事務従事者による当該規定の遵守について遵守事項 を定める。		とした対策基準を定める。	
403	1.5.2.8(1)(a) (ア)解説	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、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に労力を要するため、不正プログラムとして検知された実行ファイル等の実行を禁止する事項である。 なお、アンチウイルスソフトウェア等が 全て の現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行うことが望ましい。予防措置とは、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 ウェブサイト を閲覧しないこと等である。	1.5.2.7(1)(a) (ア)解説	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、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に労力を要するため、不正プログラムとして検知された実行ファイル等の実行を禁止する事項である。 なお、アンチウイルスソフトウェア等が すべて の現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行うことが望ましい。予防措置とは、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。	解説 の修 正
404	1.5.2.8(1)(a) (エ)	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 全て 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。	1.5.2.7(1)(a) (エ)	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。	表現 の適 正化
405	1.5.2.8(1)(a) (エ)解説	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。	1.5.2.7(1)(a) (エ)解説	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。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		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 <u>全て</u> の電子ファイルを検査する必要がある。		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 <u>すべて</u> の電子ファイルを検査する必要がある。	
406	1.5.2.8(1)(a) (カ)解説	解説：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。アンチウイルスソフトウェア等が <u>全て</u> の不正プログラムを検知できるとは限らないことに注意して、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実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないこと <u>等</u> がある。	1.5.2.7(1)(a) (カ)解説	解説：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。アンチウイルスソフトウェア等が <u>すべて</u> の不正プログラムを検知できるとは限らないことに注意して、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実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないこと <u>など</u> がある。	解説 の修 正
407	1.5.2.8(1)(a) (キ)	行政事務従事者は、不正プログラムに感染した <u>おそれ</u> のある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。	1.5.2.7(1)(a) (キ)	行政事務従事者は、不正プログラムに感染した <u>恐れ</u> のある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。	遵守 事項 の修 正
408	1.5.2.8(1)(a) (キ)解説	解説：不正プログラムに感染した <u>おそれ</u> がある電子計算機については、他の電子計算機への感染 <u>等</u> の被害の拡大を防ぐために、当該電子計算機が通信回線に接続してい	1.5.2.7(1)(a) (キ)解説	解説：不正プログラムに感染した <u>恐れ</u> がある電子計算機については、他の電子計算機への感染 <u>など</u> の被害の拡大を防ぐために、当該電子計算機が通信回線に接続して	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		る場合には、それを切断して、必要な措置を講じることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等を行うことが <u>挙げられる</u> 。		いる場合には、それを切断して、必要な措置を講じることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等を行うことが <u>あげられる</u> 。	
409	1.5.2.8(2)(a) 解説	解説： <u>全て</u> の行政事務従事者が、不正プログラム対策に係る規定に基づき、不正プログラムの感染を防止するための対策を行うことを定めた事項である。	1.5.2.7(2)(a) 解説	解説： <u>すべて</u> の行政事務従事者が、不正プログラム対策に係る規定に基づき、不正プログラムの感染を防止するための対策を行うことを定めた事項である。	解説 の修 正
410	A.1.2 解説	解説：取扱制限の例として以下の表に記載のものを想定したが、 <u>それぞれの</u> 府省庁において、このうちから必要な取扱制限の種類を採用し、また、不足している場合は適宜追加して構わない。 取扱制限は必要に応じて指定するものであるから、規程では例示するだけとして、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たせるのであれば、記載する表現方法を一律に定めないという運用方法でも構わない。例えば、「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」 <u>等</u> と記載しても目的を果たせると考えられる。	A.1.2 解説	解説：取扱制限の例として以下の表に記載のものを想定したが、 <u>各</u> 府省庁において、このうちから必要な取扱制限の種類を採用し、また、不足している場合は適宜追加して構わない。 取扱制限は必要に応じて指定するものであるから、規程では例示するだけとして、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たせるのであれば、記載する表現方法を一律に定めないという運用方法でも構わない。例えば、「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」 <u>など</u> と記載しても目的を果たせると考えられる。	解説 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
411	A.1.2	当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」 <u>等</u> 、情報を取り扱う者が分かるように指定する。	A.1.2	当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」 <u>など</u> 、情報を取り扱う者が分かるように指定する。	付録 の修 正
412	A.1.2 解説	解説：上記の「〇〇要許可」の補足説明では「〇〇する行為を禁止」とは明言をせずに、「許可を得る必要がある」とすることで、暗黙に「許可を得なければ禁止」という文章例を示した。そうではなく、はっきりと「〇〇する行為を禁止するが、許可を得ることにより〇〇することができる」と <u>いった表現等</u> も考えられる。分かりやすく、簡便な表現であることが望ましい。 「複製禁止」の指定は、機密性の確保を目的とする以外に、知的財産権保護として指定することにも使用することができる。同様に、「暗号化必須」の指定も機密性だけではなく、完全性のために指定することに役立つ。その旨を補足することで、行政事務従事者による運用の適切性を増すことができる。	A.1.2 解説	解説：上記の「〇〇要許可」の補足説明では「〇〇する行為を禁止」とは明言をせずに、「許可を得る必要がある」とすることで、暗黙に「許可を得なければ禁止」という文章例を示した。そうではなく、はっきりと「〇〇する行為を禁止するが、許可を得ることにより〇〇することができる」と <u>などの表現など</u> も考えられる。分かりやすく、簡便な表現であることが望ましい。 「複製禁止」の指定は、機密性の確保を目的とする以外に、知的財産権保護として指定することにも使用することができる。同様に、「暗号化必須」の指定も機密性だけではなく、完全性のために指定することに役立つ。その旨を補足することで、行政事務従事者による運用の適切性を増すことができる。	
413	A.1.2 完全性についての取扱 制限の定義	<u>情報の</u> 保存期間の指定の方法は、以下のとおり。 保存を要する期日である「年月日」又は期日を特定できる用語に「ま	A.1.2 完全性についての取扱 制限の定義	保存期間の指定の方法は、以下のとおり。 保存を要する期日である「年月日」又は期日を特定できる用語に「ま	付録 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>で保存」を付して指定する。</p> <p>例) 平成〇〇年7月31日まで保存</p> <p>例) 平成〇〇年度末まで保存</p> <p>完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確保にすることができる。例えば、以下のように指定する。</p> <p>例) 年度内保存文書用共有ファイルサーバに保管</p> <p>例) 3カ年保存文書用共有ファイルサーバに保管</p>		<p>で保存」を付して指定する。</p> <p>例) 平成18年7月31日まで保存</p> <p>例) 平成18年度末まで保存</p> <p>完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確保にすることができる。例えば、以下のように指定する。</p> <p>例) 年度内保存文書用共有ファイルサーバに保管</p> <p>例) 3カ年保存文書用共有ファイルサーバに保管</p>	
414	A.1.3	<p><u>[政府決定]</u></p> <ul style="list-style-type: none"> ・行政文書の管理方策に関するガイドライン(平成12年2月25日、各省庁事務連絡会議申し合わせ) ・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 	A.1.3	<ul style="list-style-type: none"> ・行政文書の管理方策に関するガイドライン(平成12年2月25日、各省庁事務連絡会議申し合わせ) ・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 	付録 の修 正

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>月 28 日 行政情報システム関係課長連絡会議了承)</p> <ul style="list-style-type: none"> ・電子政府推進計画（平成 18 年 8 月 31 日 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） ・業務・システム最適化指針（ガイドライン）（平成 18 年 3 月 31 日 各府省情報化統括責任者（CIO）連絡会議決定） ・情報システムに係る政府調達の基本指針（平成 19 年 3 月 1 日 各府省情報化統括責任者（CIO）連絡会議決定） ・ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト（平成 23 年 4 月 21 日 経済産業省） ・国家公務員身分証明書の I C 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） ・中央省庁業務継続ガイドライン 		<p>課長連絡会議了承)</p> <ul style="list-style-type: none"> ・電子政府推進計画（平成 18 年 8 月 31 日 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 I C 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） ・中央省庁業務継続ガイドライン第 1 版（平成 19 年 6 月 内閣府） <p>注）詳細については、原文を参照すること。</p>	

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<p>第1版（平成19年6月 内閣府）</p> <p>・行政文書の管理の徹底について （平成19年12月14日 関係省 庁連絡会議申合せ）</p> <p>・今後の行政文書の管理に関する 取組について（平成20年11月25 日 行政文書・公文書等の管理・ 保存に関する関係省庁連絡会議申 合せ）</p> <p>・オンライン手続におけるリスク 評価及び電子署名・認証ガイドラ イン（平成22年8月31日 各府 省情報化統括責任者（CIO）連絡 会議決定）</p> <p>〔法律〕</p> <p>・行政機関の保有する情報の公開 に関する法律（平成十一年五月十 四日法律第四十二号）</p> <p>・行政機関の保有する個人情報の 保護に関する法律（平成十五年五 月三十日法律第五十八号）</p> <p>・公文書等の管理に関する法律（平 成二十一年七月一日法律第六十六 号）</p> <p>注）詳細については、原文を参照 すること。</p>			

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
415		(統一技術基準の A.1.4 に移動)	A.1.4	【あ】 ● 「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。	構成 変更
416		(統一技術基準の A.1.4 に移動)	A.1.4	【か】 ● 「強制アクセス制御 (MAC : Mandatory Access Control)」とは、主体が客体(情報、ファイル等)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とはできない。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。	構成 変更
417		(統一技術基準の A.1.4 に移動)	A.1.4	【た】 ● 「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。	構成 変更
418		(統一技術基準の A.1.4 に移動)	A.1.4	【た】 ● 「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	構成 変更

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
				<u>アプリケーションをいう。</u>	
419	A.1.4	【た】 ● 「ドメイン名」とは、サーバ装置や通信回線装置に付与したIPアドレスを、扱いやすいように英数字 <u>及び</u> 一部の記号を用いて表したものをいう。 <u>例えば、nisc.go.jp</u> のこと。	A.1.4	【た】 ● 「ドメイン名」とは、サーバ装置や通信回線装置に付与したIPアドレスを、扱いやすいように英数字 <u>および</u> 一部の記号を用いて表したものをいう。 <u>たとえば、nisc.go.jp</u> のこと。	表現 の適 正化
420		(統一技術基準の A.1.4 に移動)	A.1.4	<u>【な】</u> ● <u>「名前解決」とは、ドメイン名やホスト名と IP アドレスを交換することをいう。</u>	構成 変更
421		(統一技術基準の A.1.4 に移動)	A.1.4	<u>【ま】</u> ● <u>「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。</u>	構成 変更
422	A.1.4	<u>【ら】</u> ● <u>「リスク」とは、不確かさによって結果が目的からかい離することでもたらされる影響をいう。起こり得る事象（周辺状況の変化を含む。）の結果とその起こりやすさとの組み合わせで表される。</u>			用語 解説 の追 加
423	A.1.4	<u>【A～Z】</u> ● <u>「ASP・SaaS サービス」とは、「Application Service Provider (ASP)」及び「Software as a Service (SaaS)」の略で、インターネットを經由して、アプリケーション機能を利用するサービスをいう。例えば、レンタルウェブサ</u>			用語 解説 の追 加

No.	統一管理 基準 遵守事項	統一管理基準	第4版(平成 21年度修正) 遵守事項	第4版(平成21年度修正)	変更 点
		<u>ーバの利用、インターネットを經由したウェブアプリケーションの利用等が挙げられる。</u>			
424		(統一技術基準の A.1.4 に移動)	A.1.4	【A～Z】 ● <u>「CRYPTREC (Cryptography Research and Evaluation Committees)」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。</u>	構成 変更
425		(統一技術基準の A.1.4 に移動)	A.1.4	【A～Z】 ● <u>「IPv6 移行機構」とは、物理的にひとつのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、電子計算機や通信回線装置が2つの通信プロトコルを併用するデュアルスタック機構や、相互接続性のない2つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。</u>	構成 変更