政府機関の情報セキュリティ対策のための統一基準(第４版)

新旧対照表

＊第３版から第４版で項番変更をしただけのものについては、以下に記載していません。それらについては、項番対応表及び遵守事項対応表を参照してください。

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
1	第１編	基本編			構成変更
2	1.1.1.2(3) 全体構成	本統一基準は、編、部、節及び項の４つの階層によって構成される。 本統一基準は、情報セキュリティ対策を「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。 基本編では、「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、情報システ	1.1.2(3) 全体構成	本統一基準は、部、節及び項の３つの階層によって構成される。 本統一基準は、情報セキュリティ対策を「組織と体制の構築」、「情報についての対策」、「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」に部として分類し、さらに内容に応じて節として対策項目に分け、その下に項として対策基準を定めている。	修正 構成変更

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		ム編では、「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」を部としてそれぞれ分類している。 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。			
3	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、違反や例外措置など、組織としての運用に関係する各職員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。	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、違反や例外措置などの組織として構築すべき課題を取り上げ、組織としての運用に関係する各職員の権限と責務を明確にする。	表現の適正化
4	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、提供及び消去等といった情報のライフサイクルに着目し、各段階において各職員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。	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、提供及び消去等といった情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、各職員が業務の中で常に実施する情報保護の対策を示す。	表現の適正化
5	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。			修正 構成変更
6	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			修正 構成変更

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。			
7	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。	1.1.2(3)(c)	「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遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。	表現の適正化
8	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。	1.1.2(3)(d)	「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、それぞれ遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。	表現の適正化
9	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際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。	1.1.2(3)(e)	「個別事項についての対策」では、調達・開発や府省庁外での情報処理等の、特に情報セキュリティ上の配慮が求められる個別事象に着目し、それぞれ遵守すべき事項を定める。	表現の適正化
10	1.1.1.3	情報の格付けの区分及び取扱制	3.1.1	情報の格付け	遵守事項の

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		限の種類			修正
11	1.1.1.3(1)	格付け及び取扱制限	3.1.1 趣旨	趣旨（必要性）	遵守事項の 修正
12	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。 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	3.1.1 趣旨 3.1.1(1) 3.1.1(1)(a)	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、情報の格付けが必要となる。これらのことを勘案し、本項では、情報の格付けに関する対策基準を定める。 遵守事項 情報の格付け 【基本遵守事項】 情報セキュリティ委員会は、行政事務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備すること。	遵守事項の 修正 削除 削除 削除 遵守事項の 修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。			
13	1.1.1.3(1) 解説	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。）に基づく各府省庁における「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。 なお、情報の格付け及び取扱制限については、各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すべての情報に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ていない。しかし、施行日前に作成又は入手した情報についても、適宜その指定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、格付け及び取扱制限を行う必要がある。	3.1.1(1)(a) 解説	解説：行政事務で取り扱う情報に対し、格付けを行うために必要となる規定を定めることを求める事項である。なお、本統一基準における情報の格付けの一覧については、本書別添資料 A.1.2 を参照されたい。 また、内閣官房情報セキュリティセンターでは、当該規定の作成の用に資するため、「情報の格付け及び取扱制限に関する規程策定手引書」を以下に DM3-01 として掲載している。 http://www.nisc.go.jp/active/general/kijun_man.html	解説の修正
14	1.1.1.3(2)	格付けの区分			遵守事項の修正
15	1.1.1.3(2)	情報について、機密性、完全性、可用性の３つの観点を区別し、それぞれにつき格付けの区分の定義を示す。 格付けとしては、以下に記載のものを本統一基準の遵守事項で用いるが、各府省庁において、適宜変更又は追加して構わな			遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		い。しかし、変更又は追加する場合には、各府省庁の対策基準における格付け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やりとりをする際に、自身の格付け区分が本統一基準で用いた格付け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格付け区分を記載する方法が考えられる。			
16	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。			遵守事項の修正
17	1.1.1.3(2)(a)	機密性についての格付けの定義			遵守事項の修正
18	1.1.1.3(2)(a)	格付けの区分 分類の基準 機密性３情報 行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報 機密性２情報 行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報	1.1.3【か】	「機密性３情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。 「機密性２情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報をいう。	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		機密性１情報 機密性２情報又は機密性３情報以外の情報 なお、機密性２情報及び機密性３情報を「要機密情報」という。	1.1.3【や】	「機密性１情報」とは、機密性２情報又は機密性３情報以外の情報をいう。 「要機密情報」とは、機密性２情報及び機密性３情報をいう。	
19	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、それ以外の情報には、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決定するので十分な場合も考えられる。	1.1.3【か】	「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。	解説の修正
20	1.1.1.3(2)(a)	完全性についての格付けの定義			遵守事項の修正
21	1.1.1.3(2)(a)	格付けの区分 分類の基準 完全性２情報 行政事務で取り扱う情報（書面	1.1.3【か】	「完全性２情報」とは、行政事務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、国民の権	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報 完全性１情報 完全性２情報以外の情報（書面を除く。） なお、完全性２情報を「要保全情報」という。	1.1.3【や】	利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。 「完全性１情報」とは、完全性２情報以外の情報（書面を除く。）をいう。 「要保全情報」とは、完全性２情報をいう。	
22	1.1.1.3(2)(a) 解説	解説：完全性の格付けについては、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など）を完全性１情報に決定することなどが考えられる。	1.1.3【か】	「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。	解説の修正
23	1.1.1.3(2)(a)	可用性についての格付けの定義			遵守事項の修正
24	1.1.1.3(2)(a)	格付けの区分 分類の基準 可用性２情報 行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的	1.1.3【か】	「可用性２情報」とは、行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をい	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。 可用性１情報 可用性２情報以外の情報（書面を除く。） なお、可用性２情報を「要安定情報」という。 また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。	1.1.3【や】	う。 「可用性１情報」とは、可用性２情報以外の情報（書面を除く。）をいう。 「要安定情報」とは、可用性２情報をいう。 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。	
25	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。	1.1.3【か】	「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。	解説の修正
26	1.1.1.3(3)	取扱制限の種類			遵守事項の修正
27	1.1.1.3(3)	情報について、機密性、完全性、可用性の３つの観点を区別し、それぞれにつき取扱制限の種類の基本的な定義を行う。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須	1.1.3【た】	「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄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。	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		、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。			
28	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。ただし、これら以外の取扱制限の種類を適宜用いることができる。			遵守事項の修正
29	1.1.1.3(3)(a) 解説	解説：付表を用いて定める場合の例については本書別添資料 A.1.2 取扱制限の種類に係る付表例を参照。			解説の修正
30		（削除）	1.1.3【か】	「可用性１情報」とは、可用性２情報以外の情報（書面を除く。）をいう。	1.1.1.3　明示による削除
31		（削除）	1.1.3【か】	「可用性２情報」とは、行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。	1.1.1.3　明示による削除
32		（削除）	1.1.3【か】	「完全性１情報」とは、完全性２情報以外の情報（書面を除く。）をいう。	1.1.1.3　明示による削除
33		（削除）	1.1.3【か】	「完全性２情報」とは、行政事務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを	1.1.1.3　明示による削除

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
				除く。）を及ぼすおそれがある情報をいう。	
34		（削除）	1.1.3【か】	「機密性１情報」とは、機密性２情報又は機密性３情報以外の情報をいう。	1.1.1.3　明示による削除
35		（削除）	1.1.3【か】	「機密性２情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報をいう。	1.1.1.3　明示による削除
36		（削除）	1.1.3【か】	「機密性３情報」とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。	1.1.1.3　明示による削除
37	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。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。	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。	遵守事項の修正
38	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。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）について、統括情報セキュリティ責任者等に委	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。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。			
39	1.2.1.1(5)(a)	情報セキュリティ責任者は、所管する単位における情報システムごとに情報システムセキュリティ責任者を、当該情報システムの計画段階までに置くこと。	2.1.1(5)(a)	情報セキュリティ責任者は、所管する単位における情報システムごとに情報システムセキュリティ責任者を置くこと。	遵守事項の修正
40	1.2.1.1(5)(a) 解説	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情報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。 情報システムの情報セキュリティ要件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。 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、その他府省庁のすべての情報システムを、情報システム単位に情報セキュリティ対策の運用の責任の所在を明確にすることが重要である。	2.1.1(5)(a) 解説	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情報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。 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、その他府省庁のすべての情報システムを、情報システム単位に情報セキュリティ対策の運用の責任の所在を明確にすることが重要である。	解説の修正
41	1.2.1.1(8)(a)	最高情報セキュリティアドバイザーの設置 【基本遵守事項】	2.1.1(1)(c)	最高情報セキュリティ責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		最高情報セキュリティ責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くこと。		経験を有した専門家を最高情報セキュリティアドバイザーとして置くこと。	
42	1.2.1.1(8)(a) 解説	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。 各府省庁における情報セキュリティ対策については、情報システムに関する技術や事案に対する対処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。 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。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。 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。	2.1.1(1)(c) 解説	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。 各府省庁における情報セキュリティ対策については、情報システムに関する技術や事案に対する対処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。 最高情報セキュリティ責任者が、情報システムに関する専門的な知識及び経験を高度な水準で有しているため、専門家の助言を必要としないといった特殊な場合を除き、置くことを義務付けているものである。 なお、CIO（情報化統括責任者）補佐官は最高情報セキュリティアドバイザーを兼務することができる。	解説の修正
43	1.2.1.1(8)(b)	最高情報セキュリティ責任者			遵守事項の

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		は、情報セキュリティ対策等の実施において最高情報セキュリティアドバイザーが行う業務の内容について定めること。			追加
44	1.2.1.1(8)(b) 解説	解説：最高情報セキュリティアドバイザーの業務を明確化するため、最高情報セキュリティ責任者に、最高情報セキュリティアドバイザーの業務の内容について定めることを求める事項である。 最高情報セキュリティアドバイザーの業務として、情報セキュリティ対策に係る様々な事務への助言等が想定されるが、その事務として例えば、 ・情報セキュリティ施策の全般的な計画策定 ・情報セキュリティ教育の計画立案、教材開発及び実施 ・各種規定の整備 ・情報システムに係る技術的事項 ・情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定 ・行政事務従事者に対する日常的な相談対応 ・緊急時対応 ・自己点検の計画立案と実施 ・情報セキュリティの監査の計画立案と実施 等が想定される。			解説の追加

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		これらの事務を行う最高情報セキュリティ責任者、情報セキュリティ監査責任者、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、課室情報セキュリティ責任者等が定められた事項を遂行するために、最高情報セキュリティアドバイザーが専門的な知識及び経験に基づき行う助言等の内容を定める。			
45	1.2.1.2(1)(a)(ア)	承認又は許可事案の申請者とその承認又は許可を行う者（以下、本項において「承認権限者等」という。）	2.1.2(1)(a)(ア)	承認又は許可事案の申請者とその承認権限者又は許可権限者（以下「承認権限者等」という。）	表現の適正化
46	1.2.1.2(2)(b) 解説	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。	2.1.2(2)(b) 解説	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外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。	誤字訂正
47	1.2.1.3(2)(a)	情報セキュリティ委員会は、例外措置の適用の申請を審査する者（以下、本項において「許可権限者」という。）を定め、審査手続を整備すること。	2.1.3(2)(a)	情報セキュリティ委員会は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）を定め、審査手続を整備すること。	表現の適正化
48	1.2.2.2	障害・事故等の対処	2.2.2	障害等の対処	表現の適正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
					化
49	1.2.2.2 趣旨	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。 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。	2.2.2 趣旨	情報セキュリティに関する障害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、障害等の影響や範囲を定められた責任者へ報告し、障害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。 これらのことを勘案し、本項では、障害等の発生時に関する対策基準を定める。	表現の適正化
50	1.2.2.2(1)	障害・事故等の発生に備えた事前準備	2.2.2(1)	障害等の発生に備えた事前準備	表現の適正化
51	1.2.2.2(1)(a)	最高情報セキュリティ責任者は、情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生した場合、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備すること。	2.2.2(1)(a)	最高情報セキュリティ責任者は、情報セキュリティに関する障害等（インシデント及び故障を含む。以下「障害等」という。）が発生した場合、被害の拡大を防ぐとともに、障害等から復旧するための体制を整備すること。	表現の適正化
52	1.2.2.2(1)(a) 解説	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意することが求められる。 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	2.2.2(1)(a) 解説	解説：最高情報セキュリティ責任者に障害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意することが求められる。 なお、情報セキュリティに関する障害等とは、機密性、完全性、可用性が侵害されるものを対象	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 また、「インシデント」とは、ISO/IEC 27002 におけるインシデントと同意である。		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。 また、「インシデント」とは、ISO/IEC 17799 におけるインシデントと同意である。	
53	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。	2.2.2(1)(b)	統括情報セキュリティ責任者は、障害等について行政事務従事者から情報セキュリティ責任者への報告手順を整備し、当該報告手段をすべての行政事務従事者に周知すること。	表現の適正化
54	1.2.2.2(1)(c)	統括情報セキュリティ責任者は、障害・事故等が発生した際の対処手順を整備すること。	2.2.2(1)(c)	統括情報セキュリティ責任者は、障害等が発生した際の対処手順を整備すること。	表現の適正化
55	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めることも考えられる。	2.2.2(1)(c) 解説	解説：対処手順として障害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、障害等の発生日及び内容、障害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めることも考えられる。	表現の適正化

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
56	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、その情報システムセキュリティ責任者及び情報システムセキュリティ管理者の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。	2.2.2(1)(d)	統括情報セキュリティ責任者は、障害等に備え、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、その情報システムセキュリティ責任者及び情報システムセキュリティ管理者の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。	表現の適正化
57	1.2.2.2(1)(d) 解説	解説：統括情報セキュリティ責任者は、すべての情報システムセキュリティ責任者及び情報システムセキュリティ管理者の連絡網を整備しているものである（統一基準 1.2.1.1）が、これは「緊急」連絡網を加えて整備することを定める事項である。	2.2.2(1)(d) 解説	解説：統括情報セキュリティ責任者は、すべての情報システムセキュリティ責任者及び情報システムセキュリティ管理者の連絡網を整備しているものである（統一基準 2.1.1）が、これは「緊急」連絡網を加えて整備することを定める事項である。	構成変更
58	1.2.2.2(1)(e)	統括情報セキュリティ責任者は、障害・事故等について府省庁の外部から報告を受けるための窓口を設置し、その窓口への連絡手段を府省庁外に公表すること。	2.2.2(1)(e)	統括情報セキュリティ責任者は、障害等について府省庁の外部から報告を受けるための窓口を設置し、その窓口への連絡手段を府省庁外に公表すること。	表現の適正化
59	1.2.2.2(2)	障害・事故等の発生時における報告と応急措置	2.2.2(2)	障害等の発生時における報告と応急措置	表現の適正化
60	1.2.2.2(2)(a)	行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、情報セキュリティ責任者にその旨を報告すること。	2.2.2(2)(a)	行政事務従事者は、障害等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、情報セキュリティ責任者にその旨を報告すること。	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
61	1.2.2.2(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。	2.2.2(2)(a) 解説	解説：障害等が発生した場合に、行政事務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害等への対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。	表現の適正化
62	1.2.2.2(2)(b)	行政事務従事者は、障害・事故等が発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。	2.2.2(2)(b)	行政事務従事者は、障害等が発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。	表現の適正化
63	1.2.2.2(2)(b) 解説	解説：行政事務従事者の判断による被害拡大防止策が常に適切なものであるとは限らないため、障害・事故等への対処手順に従うことを求める事項である。	2.2.2(2)(b) 解説	解説：行政事務従事者の判断による被害拡大防止策が常に適切なものであるとは限らないため、障害等への対処手順に従うことを求める事項である。	表現の適正化
64	1.2.2.2(2)(c)	行政事務従事者は、障害・事故等が発生した場合であって、当該障害・事故等について対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、障害・事故等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。	2.2.2(2)(c)	行政事務従事者は、障害等が発生した場合であって、当該障害等について対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、障害等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。	表現の適正化
65	1.2.2.2(2)(c) 解説	解説：対処手順が想定していない障害・事故等が発生した場合、行政事務従事者は対処の指示を受けるまでの間も障害・事故等の拡大防止に努めることを求める事項である。	2.2.2(2)(c) 解説	解説：対処手順が想定していない障害等が発生した場合、行政事務従事者は対処の指示を受けるまでの間も障害等の拡大防止に努めることを求める事項である。	表現の適正化
66	1.2.2.2(3)	障害・事故等の原因調査と再発防止策	2.2.2(3)	障害等の原因調査と再発防止策	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
67	1.2.2.2(3)(a)	情報セキュリティ責任者は、障害・事故等が発生した場合には、障害・事故等の原因を調査し再発防止策を策定し、その結果を報告書として最高情報セキュリティ責任者に報告すること。	2.2.2(3)(a)	情報セキュリティ責任者は、障害等が発生した場合には、障害等の原因を調査し再発防止策を策定し、その結果を報告書として最高情報セキュリティ責任者に報告すること。	表現の適正化
68	1.2.2.2(3)(a) 解説	解説：情報セキュリティ責任者に対して、障害・事故等の原因を究明し、それに基づき障害・事故等の再発防止策を策定することを求める事項である。	2.2.2(3)(a) 解説	解説：情報セキュリティ責任者に対して、障害等の原因を究明し、それに基づき障害等の再発防止策を策定することを求める事項である。	表現の適正化
69	1.2.2.2(3)(b)	最高情報セキュリティ責任者は、情報セキュリティ責任者から障害・事故等についての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。	2.2.2(3)(b)	最高情報セキュリティ責任者は、情報セキュリティ責任者から障害等についての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。	表現の適正化
70	1.2.2.2(3)(b) 解説	解説：障害・事故等の再発防止策を講ずることを、最高情報セキュリティ責任者に求める事項である。	2.2.2(3)(b) 解説	解説：障害等の再発防止策を講ずることを、最高情報セキュリティ責任者に求める事項である。	表現の適正化
71	1.2.5	その他			構成変更
72	1.2.5.1(1)(c) 解説	解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。 評価方法の整備には、ISO/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。	6.1.2(1)(c) 解説	解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。 評価方法の整備には、ISO/IEC 27001:2005 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。	表現の適正化

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
73	1.2.5.1(5)(a)(イ) 解説	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。 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」の定めに準ずるが、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。	6.1.2(5)(a)(イ) 解説	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。 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「3.2.4 情報の移送」及び「3.2.5 情報の提供」の定めに準ずるが、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。	解説の修正
74		（削除）	6.3.2.(1)	府省庁における業務継続計画の整備計画の把握 【基本遵守事項】	削除
75		（削除）	6.3.2.(1)(a)	最高情報セキュリティ責任者は、府省庁における業務継続計画の整備計画について統括情報セキュリティ責任者を通じ情報	削除

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
				セキュリティ委員会が適時に知ることができる体制を整備すること。	
76		（削除）	6.3.2.(1)(a) 解説	最高情報セキュリティ責任者が、府省庁が整備する業務継続計画の内容や状況について、情報セキュリティ委員会が適時に情報を入手できるような体制を整備することを求める事項である。 業務継続計画に変更がある場合などにも、必要な情報が継続的に得られるようにしなければならない。 なお、一般に業務継続計画については事業継続計画又は BCP（Business Continuity Plan）ともいうが、「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）に従い、本統一基準においては業務継続計画という。	削除
77		（削除）	6.3.2.(1)(b)	統括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を把握した場合は、その内容を情報セキュリティ委員会並びに必要に応じて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連絡すること。	削除
78		（削除）	6.3.2.(1)(b) 解説	情報セキュリティ委員会並びに必要に応じて情報セキュリティ責任者、情報システムセキュリ	削除

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
				ティ責任者及び課室情報セキュリティ責任者が府省庁における業務継続計画の整備計画を知ることができるために、統括情報セキュリティ責任者に対して、把握した業務継続計画の整備計画の内容を連絡することを求める事項である。 業務継続計画に変更がある場合にも、当該連絡を行わなければならない。	
79	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。当該事態の例として、情報システムの稼動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。 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、	6.3.2(2)(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。当該事態の例として、情報システムの稼動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。 例えば、情報セキュリティ委員会は、「情報の格付け及び取扱制限の指定並びに明示等の規定」	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		の整備について、本統一基準の 3.1.1 項で求められている。その整備の際に、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、その変更が当該基準に影響するかどうかを確認し、必要があれば、当該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。	
80	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、各執務室や各職員の卓上のセキュリティ対策を含め、通常	6.3.2(2)(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、各執務室や各職員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	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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る必要がある。		想定した対策を講ずる必要がある。	
81	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などにより、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。	6.3.2(3)(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などにより、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
82	1.3.1.1(2)	情報の作成又は入手時における格付けと取扱制限の決定	3.2.1(2)	情報の作成又は入手時における格付けの決定と取扱制限の検討	表現の適正化
83	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格付け及び取扱制限の定義に基づき、格付け及び取扱制限を決定すること。	3.2.1(2)(a)	行政事務従事者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。	遵守事項の修正 表現の適正化
84	1.3.1.1(2)(a) 解説	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管理が施されるように、機密性、完全性、可用性の格付け及び取扱制限を行うことを求め	3.2.1(2)(a) 解説	解説：作成した情報について、以降、適切なセキュリティ管理が施されるように、機密性、完全性、可用性の格付け等を行うことを求める事項である。	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		る事項である。 情報の格付けが適切に決定されていなかった、また、明示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行うことは重要である。 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。 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		情報の格付け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等が発生した場合には、障害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、情報の格付けとその明示等を確実に行うことは重要である。 なお、行政事務従事者は、情報の利用を円滑に行うため、格付けを必要以上に高くしないように配慮することも必要となる。あわせて、格付けに応じた情報の取扱いを確実にするための取扱制限の必要性の有無についても検討を行わなければならない。	

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		る。 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とも不適切であることに注意すること。 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決定でも差し支えない。			
85	1.3.1.1(2)(b)	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格付け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。	3.2.1(5)(a)	行政事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。	遵守事項の修正
86	1.3.1.1(2)(b) 解説	解説：元の情報の修正、追加、削除のいずれかにより、格付け又は取扱制限を変更する必要が生じた場合には、格付け及び取扱制限の再決定を行う必要がある。 例えば、以下のような場合が考えられる。 ・機密性の低い情報に機密性の高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 ・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	3.2.1(5)(a) 解説	解説：情報を利用する行政事務従事者が、当該情報の格付けを変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成し、又は入手した場合も含まれる。当初の格付けが作成者又は入手者によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまで	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		よって、情報の機密性が下がる場合 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、大別して再指定と見直しがある。		その情報を参照した者に対しても、当該情報の格付けを変更したことを周知させることが望ましい。 なお、異動等の事由により、当該情報の作成者又は入手者と相談することが困難である場合においては、引継ぎを受けた者又は課室情報セキュリティ責任者が相談を受け、その是非を検討することになる。 また、内閣官房情報セキュリティセンターでは、当該規定の作成の用に資するため、「情報の格付け及び取扱制限に関する規程策定手引書」を以下に DM3-01 として掲載している。 http://www.nisc.go.jp/active/general/kijun_man.html	
87	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。	3.2.1(3)(a)	行政事務従事者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示等し、必要に応じて取扱制限についても明示等すること。	表現の適正化
88	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、情報を取り扱うすべての	3.2.1(3)(a) 解説	解説：作成者又は入手者によって格付けが行われた情報に対して、以降、他者が当該情報を利用する際に必要とされるセキュリティ対策レベルを示すため、情報の格付けの明示等を行うことを求める事項である。また、取扱制限が必要な場合は、あわせてその明示等も行わなければ	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。 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。 既に書面として存在している情報に対して格付けや取扱制限を明示等する場合には、手書きに		ならない。 格付けと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、視認できる方法でそれぞれ行う必要がある。ただし、当該情報システムに保存されているすべての情報が同じ格付け、取扱制限であり、利用するすべての行政事務従事者にその認識が周知徹底されている場合は、この限りでない。しかし、格付けや取扱制限を認識していない行政事務従事者に当該情報システムに保存されている情報を提供する必要が生じた場合は、当該情報に視認できるような明示等を行った上で提供しなければならない。 また、既に書面として存在している情報に対して格付けや取扱制限を明示等する場合には、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	

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。 なお、格付け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。 明示等を行なうには、格付け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、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、以下のように記載以外の方法で簡便化してもよい。 ①　格付け及び取扱制限の明示等の簡便化 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）の格付け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		等することも可能である。 なお、格付け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。	

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		きる。 ② 格付け及び取扱制限の決定を認識できない者への提供 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生じた場合（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。 ③ 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 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。			
89	1.3.1.1(4)	格付けと取扱制限の加工時における継承	3.2.1(4)	格付けと取扱制限の継承	表現の適正化
90	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	3.2.1(4)(a)	行政事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承	表現の適正化 遵守事項の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		すること。	
91	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。	3.2.1(4)(a) 解説	解説：情報の作成者による情報の格付けと取扱制限を継承し、以降も同様のセキュリティ対策を維持することを求める事項である。	解説の修正
92	1.3.1.2(3)	格付け及び取扱制限の複製時における継承	3.2.1(4)	格付けと取扱制限の継承	遵守事項の修正
93	1.3.1.2(3)	【基本遵守事項】			遵守事項の修正
94	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。	3.2.1(4)(a)	行政事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。	遵守事項の修正
95	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。	3.2.1(4)(a) 解説	解説：情報の作成者による情報の格付けと取扱制限を継承し、以降も同様のセキュリティ対策を維持することを求める事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
96	1.3.1.2(4)	格付け及び取扱制限の見直し	3.2.1(5)	格付けと取扱制限の変更	遵守事項の修正
97	1.3.1.2(4)	【基本遵守事項】			遵守事項の修正
98	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。	3.2.1(5)(a)	行政事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。	遵守事項の修正
99	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当と考える場合には、格付け又は取扱制限の見直しについてその決定者に確認を求める必要がある。 また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は同人の上司に相談し、その是非を検討することになる。 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、格付け又は取扱制限を変更することは許されない。	3.2.1(5)(a) 解説	解説：情報を利用する行政事務従事者が、当該情報の格付けを変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成し、又は入手した場合も含まれる。当初の格付けが作成者又は入手者によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を参照した者に対しても、当該情報の格付けを変更したことを周知させることが望ましい。 なお、異動等の事由により、当該情報の作成者又は入手者と相	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 ・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 ・格付け及び取扱制限を決定したときの判断が不適切であったと考えられる場合 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。		談することが困難である場合においては、引継ぎを受けた者又は課室情報セキュリティ責任者が相談を受け、その是非を検討することになる。 また、内閣官房情報セキュリティセンターでは、当該規定の作成の用に資するため、「情報の格付け及び取扱制限に関する規程策定手引書」を以下に DM3-01 として掲載している。 http://www.nisc.go.jp/active/general/kijun_man.html	
100	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。	3.2.1(5)(a)	行政事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。	遵守事項の修正
101	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	3.2.1(5)(a) 解説	解説：情報を利用する行政事務従事者が、当該情報の格付けを変更する場合に、当該情報の作成者又は入手者に相談し、了承	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。		を得ることを求める事項である。なお、自らが作成し、又は入手した場合も含まれる。当初の格付けが作成者又は入手者によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を参照した者に対しても、当該情報の格付けを変更したことを周知させることが望ましい。 なお、異動等の事由により、当該情報の作成者又は入手者と相談することが困難である場合においては、引継ぎを受けた者又は課室情報セキュリティ責任者が相談を受け、その是非を検討することになる。 また、内閣官房情報セキュリティセンターでは、当該規定の作成の用に資するため、「情報の格付け及び取扱制限に関する規程策定手引書」を以下に DM3-01 として掲載している。 http://www.nisc.go.jp/active/general/kijun_man.html	
102	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又は取扱制限を緩和する必要性があると思	3.2.2(3)(e)	行政事務従事者は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる必要性があると思料される場合には、格付	遵守事項の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		けの変更に必要な処理を行うこと。	
103	1.3.1.3(1)(a) 解説	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。 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。 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	3.2.3(1)(a) 解説	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。 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。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		当たる。 ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。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。			
104	1.3.1.3(1)(b)	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。	3.2.3(1)(b)	行政事務従事者は、情報の格付けに応じて、情報が保存された電磁的記録媒体を適切に管理すること。	遵守事項の修正・
105	1.3.1.3(1)(b) 解説	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。 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。 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	3.2.3(1)(b) 解説	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に応じて、適切に管理することを求める事項である。 例えば、機密性の格付けに応じて、外部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。 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。	解説の修正・

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		た外部電磁的記録媒体を選択する必要がある。			
106	1.3.1.3(1)(d)	行政事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。			遵守事項の追加
107	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。			解説の追加
108	1.3.1.3(1)(e) 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、その暗号化を行うことを求める事項である。 暗号化を行うと情報の復号ができる者を限定することとなり、府省庁内において情報の機密性を高めるために有効である。また、万一 PC、光ディスク、USB メモリ等の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。 情報を暗号化する際は、1.5.2.4	3.2.3(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、その暗号化を行うことを求める事項である。 暗号化を行うと情報の復号ができる者を限定することとなり、府省庁内において情報の機密性を高めるために有効である。また、万一 PC、光ディスク、USB メモリ等の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		暗号と電子署名の標準手順の定めに従うこと。			
109	1.3.1.3(1)(f) 解説	解説：要保全情報を電磁的記録媒体に保存する場合、その改ざんのおそれを勘案し、必要に応じて電子署名を付与することを求める事項である。 情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。	3.2.3(1)(e) 解説	解説：要保全情報を電磁的記録媒体に保存する場合、その改ざんのおそれを勘案し、必要に応じて電子署名を付与することを求める事項である。	解説の修正
110	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する場合には、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。	3.2.4(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する場合には、情報の格付けなどに応じて、安全確保のための適切な措置を講ずること。	表現の適正化
111	1.3.1.4(5)(b) 解説	解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。情報を暗号化する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。	3.2.4(5)(b) 解説	解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。	解説の修正
112	1.3.1.4(5)(c) 解説	解説：要保全情報を移送する場合、必要に応じて電子署名の付与を行うことを求める事項である。情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。	3.2.4(5)(c) 解説	解説：要保全情報を移送する場合、必要に応じて電子署名の付与を行うことを求める事項である。	解説の修正
113	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	3.2.5(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に応じて適切に取	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		じて適切に取り扱われるための措置を講ずること。		り扱われるための措置を講ずること。	
114	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において遵守すべきことを定める事項である。 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。 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	3.2.5(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において遵守すべきことを定める事項である。 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、情報の格付けなど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。	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。			
115	第 1.4 部	情報処理についての対策			構成変更
116	1.4.1	情報処理の制限			構成変更
117	1.4.1.1(2)(a)	行政事務従事者は、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情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	6.2.1(2)(a)	行政事務従事者は、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情報処理を行う場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。	表現の適正化
118	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。	6.2.1(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又は課室情報セキュリティ責任者の許可を得ることを求める事項である。情報システムに係る事項は情報システムセキュリティ責任者の、情報に係る事項は課室情報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.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
119	1.4.1.1(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、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届出を要しないとした場合は、この限りでない。	6.2.1(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外で情報処理を行う場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。	表現の適正化 遵守事項の修正
120	1.4.1.1(2)(b) 解説	解説：府省庁外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、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に届け出ること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での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。	6.2.1(2)(b) 解説	解説：府省庁外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者又は課室情報セキュリティ責任者に届け出ることを求める事項である。	解説の修正
121	1.4.1.1(2)(g)	行政事務従事者は、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場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	6.2.1(2)(g)	行政事務従事者は、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場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。	遵守事項の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
122	1.4.1.1(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。当該持出し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、当該持出し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。	6.2.1(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又は課室情報セキュリティ責任者の許可を得ることを求める事項である。情報システムに係る事項は情報システムセキュリティ責任者の、情報に係る事項は課室情報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
123	1.4.1.1(2)(h)	行政事務従事者は、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場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、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届出を要しないとした場合は、この限りでない。	6.2.1(2)(h)	行政事務従事者は、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場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。	表現の適正化 遵守事項の修正
124	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ることを求める事項である。また、情報システムセキュリティ	6.2.1(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又は課室情報セキュリティ責任者に届け出ることを求める事項である。	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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持出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。			
125	1.4.1.2(2)(a)	行政事務従事者は、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支給以外の情報システムにより情報処理を行う必要がある場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	6.2.2(2)(a)	行政事務従事者は、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支給以外の情報システムにより情報処理を行う必要がある場合には、情報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。	表現の適正化
126	1.4.1.2(2)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合に、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。 府省庁支給以外の情報システムによる機密性３情報、完全性２情報又は可用性２情報の情報処理を許可する場合は、その期間については、最長で１年間にす	6.2.2(2)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合に、許可を得ることを求める事項である。情報システムに係る事項は情報システムセキュリティ責任者の、情報に係る事項は課室情報セキュリティ責任者の許可を得ることとなる。 府省庁支給以外の情報システムによる機密性３情報、完全性２情報又は可用性２情報の情報処理を許可する場合は、その期間については、最長で１年間にすることが望ましい。ただし、期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		ることが望ましい。ただし、期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。			
127	1.4.1.2(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、情報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届け出ること。ただし、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届出を要しないとした場合は、この限りでない。	6.2.2(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者に届け出ること。	表現の適正化 遵守事項の修正
128	1.4.1.2(2)(b) 解説	解説：府省庁支給以外の情報システムによる機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、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に届け出ること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支給以外の情報システムによる情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。	6.2.2(2)(b) 解説	解説：府省庁支給以外の情報システムによる機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者又は課室情報セキュリティ責任者に届け出ることを求める事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
129	第 1.5 部	情報システムについての基本的な対策			構成変更
130	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を考慮して決める必要がある。 決定されたセキュリティ要件	4.3.1(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、その中で重要とみなされる要求事項について対策を実施する対象を確定し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などのセキュリティに関する手順も含まれる。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などの形式で明確化した上で、実装していくことが望ましい。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		は、システム要件定義書や仕様書などの形式で明確化した上で、実装していくことが望ましい。			
131	1.5.1.1(1)(c) 解説	解説：本項は、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。	4.3.1(1)(c) 解説	解説：本項は、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る。省庁対策基準から当該情報システムのセキュリティ対策として実施する遵守事項を選択した上でセキュリティ要件を満たしているかを検討し、満たしていないセキュリティ要件がある場合には、その対策も定めることが必要である。	解説の修正
132	1.5.1.1(1)(d) 解説	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。 「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	4.3.1(1)(d) 解説	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 確認を行うことを求める事項である。 「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	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 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。		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。 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。	
133	1.5.2	情報システムに係る規定の整備と遵守			構成変更
134	1.5.2.1	情報システムに係る文書及び台帳整備	4.3.1(5)	情報システムの台帳整備	表現の適正化
135	1.5.2.1 趣旨	府省庁の情報システムにおいて、適切な情報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	4.3.1 趣旨	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	趣旨の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		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。	
136	1.5.2.1(1)	情報システムの文書整備			遵守事項の集約
137	1.5.2.1(1)	【基本遵守事項】			遵守事項の集約
138	1.5.2.1(1)(a)	情報システムセキュリティ責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。	5.2.1(1)(b)	情報システムセキュリティ責任者は、すべての電子計算機に対して、電子計算機を管理する行政事務従事者及び利用者を特定するための文書を整備すること。	遵守事項の集約
139	1.5.2.1(1)(a)(ア)	当該情報システムを構成する電子計算機関連事項 電子計算機を管理する行政事務従事者及び利用者を特定する情報 電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン 電子計算機の仕様書又は設計書	5.2.1(1)(b)	情報システムセキュリティ責任者は、すべての電子計算機に対して、電子計算機を管理する行政事務従事者及び利用者を特定するための文書を整備すること。	遵守事項の集約
140	1.5.2.1(1)(a)(イ)	当該情報システムを構成する通信回線及び通信回線装置関連事項 通信回線及び通信回線装置を管理する行政事務従事者を特定す	5.4.1(1)(e)	情報システムセキュリティ責任者は、すべての通信回線及び通信回線装置に対して、これを管理する者を特定するための文書を整備すること。	遵守事項の集約

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		る情報 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン 通信回線及び通信回線装置の仕様書又は設計書 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 通信回線の利用部署			
141	1.5.2.1(1)(a)(ウ)	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 電子計算機のセキュリティ維持に関する手順 通信回線を介して提供するサービスのセキュリティ維持に関する手順 通信回線及び通信回線装置のセキュリティ維持に関する手順	5.2.1(1)(a)	情報システムセキュリティ責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。	遵守事項の集約
142	1.5.2.1(1)(a)(エ)	障害・事故等が発生した際の対処手順			遵守事項の統合・追加
143	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、適切な情報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、文書として整備することを定めた遵守事項である。文書の整備にあたっては、維持管理が	4.2.2(2)(i) 解説	解説：アンチウイルスソフトウェア等では検知されない新種の不正プログラムに感染した等、新種の不正プログラム等に対応した不正プログラム定義ファイルがアンチウイルスソフトウェア等の製造業者から提供されるより前に、不正プログラムに感染した場合等において、外部か	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 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。 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。 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。 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、及び通信回線の利用		ら支援を受けられるように準備しておくことを求める事項である。	

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 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。 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るべき手順であり、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。 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。 ・業務継続計画で定める当該情報システムを利用する業務の重要性 ・情報システムの運用等の外部委託の内容 また手順に記載される内容として、例えば以下が想定される。 ・障害・事故等の内容・影響度			

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		の大きさに応じた情報連絡先のリスト ・情報システムを障害・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 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。			
144	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。	5.2.1(2)(a)	情報システムセキュリティ管理者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。	遵守事項の追加
145	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。	5.2.1(2)(a) 解説	解説：整備された規定に従った運用管理を行い、担当者による個別の判断で運用管理を行わないことを求める事項である。 運用管理は専用のアプリケーションを利用しても差し支えない。	解説の追加
146	1.5.2.1(2)(a)	統括情報セキュリティ責任者	4.3.1(5)(b)	統括情報セキュリティ責任者	遵守事項の

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。		は、すべての情報システムに対して、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を記載した台帳を整備すること。	修正
147	1.5.2.1(2)(a)(ア)	情報システム名、管理課室及び管理責任者の氏名・連絡先			遵守事項の修正
148	1.5.2.1(2)(a)(イ)	システム構成			遵守事項の修正
149	1.5.2.1(2)(a)(ウ)	接続する府省庁外通信回線の種別			遵守事項の修正
150	1.5.2.1(2)(a)(エ)	取り扱う情報の格付け及び取扱制限に関する事項	4.3.1(5)(b)	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、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を記載した台帳を整備すること。	遵守事項の修正
151	1.5.2.1(2)(a)(オ)	当該情報システムの設計・開発、運用、保守に関する事項			遵守事項の集約
152	1.5.2.1(2)(a) 解説	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。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。	4.3.1(5)(b) 解説	解説：自府省庁でどのような情報システムを保有し、当該情報システムで取り扱う情報やその格付けを把握して一元管理することは、日常的な運用管理や障害等発生時における対処を適正に実施する上での前提となる。情報システムの台帳に記載する項目としては、当該情報システムが取り扱うことを許可する情報の格付けのほか、利用目的、利用者数、外部ネットワークとの接続の有無等が考えられる。既に情報システムの台帳が整備されており統括情報セキュリテ	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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項を含める必要がある。 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。 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		ィ責任者が利用可能な場合には、当該台帳に情報システムが取り扱うことを許可する情報の格付け等を追記しても良い。 なお、情報システムは、業務内容や運用形態等により、端末１台で１つの情報システムを構成する場合もあれば、複数の端末、サーバ装置、通信回線等で１つの情報システムを構成する場合もある。情報システムの台帳には、そのような構成単位ごとに取り扱う情報とその格付けを記載することになる。その際、情報システムで取り扱う情報のうち、同様に取り扱われる情報については、類型化した上で格付けを記載すると効率的である。	

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		するために必要な事項である。			
153	1.5.2.1(2)(b)	情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項について統括情報セキュリティ責任者に報告すること。	4.3.1(5)(a)	情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を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
154	1.5.2.1(2)(b) 解説	解説：府省庁の各情報システムを所管する情報システムセキュリティ責任者が、情報システムに係る台帳に記載の事項について統括情報セキュリティ責任者に報告することを求める事項である。 台帳における網羅性の維持のため、情報システムセキュリティ責任者は、情報システムを新規に構築した際、又は更改した際には、速やかに台帳に記載の事項を報告する必要がある。なお、台帳の最新性の維持のため、台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、台帳を更新する必要があるが、その報告の方法やタイミングについては、府省庁ごとに定めることが望ましい。	4.3.1(5)(a) 解説	解説：情報システムのセキュリティ要件の決定に際し、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を、統括情報セキュリティ責任者に報告することを求める事項である。	解説の修正
155	1.5.2.2(1)	機器等の購入に係る規定の整備	6.1.1(1)	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	表現の適正化
156	1.5.2.2(1)(b)	統括情報セキュリティ責任者は、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、総合評価落札方式により購	6.1.1(2)(d)	情報システムセキュリティ責任者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセ	主語の変更等 遵守事項の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		入を行う際には、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かどうかを評価項目として活用することを選定基準として定めること。		キュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行うときは、これについて、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かどうかを評価項目として活用すること。	
157	1.5.2.2(1)(b) 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、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。 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。	6.1.1(2)(d) 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、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ものを優遇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が構築できる。	解説の修正
158	1.5.2.2(1)(c) 解説	解説：機器等の納入時の確認・検査に関する手続を定めるものである。 特に、確認・検査手続では、納入された機器等が定められた選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加える手続を組み込む必要がある。 具体的な確認・検査の方法として、必要なセキュリティ機能の実装状況（機器等に最新のパッ	6.1.1(1)(b) 解説	解説：機器等の納入時の確認・検査に関する手続を定めるものである。 確認・検査手続としては、必要なセキュリティ機能の実装の確認（機器等に最新のパッチが適用されているかどうか、アンチウイルスソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）を、購入先からの報告で確認すること等が挙げられる。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		チが適用されているかどうか、アンチウイルスソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）及び機器等に不正プログラムが混入していないことを、購入先からの報告で確認すること等が挙げられる。			
159	1.5.2.2(2)	機器等の購入に係る規定の遵守	6.1.1(2)	機器等の購入の実施における手続	表現の適正化
160	1.5.2.2(2)(b)	情報システムセキュリティ責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。	6.1.1(2)(b)	情報システムセキュリティ責任者は、機器等の納入時において、納入された機器等が選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加えること。	表現の適正化
161	1.5.2.2(2)(b) 解説	解説：情報セキュリティ対策の視点を加味して定められた納入時の確認・検査手続に準拠して、納入された機器等の納品検査を行うことを求める事項である。	6.1.1(2)(b) 解説	解説：納入された機器等が選定基準を満たすことを確認・検査することを求める事項である。	解説の修正
162	1.5.2.3(1)	ソフトウェア開発に係る規定の整備	6.1.3(1)	ソフトウェア開発体制の確立時	遵守事項の集約
163	1.5.2.3(1)(a)	統括情報セキュリティ責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を情報システムセキュリティ責任者に求めるための規定を整備すること。			遵守事項の集約

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
164	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、別途規定を整備することとせずに、省庁対策基準内において直接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
165	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。	6.1.3(1)(a)	情報システムセキュリティ責任者は、ソフトウェア開発について、セキュリティにかかわる対策事項（本項(2)から(5)の遵守事項）を満たすことが可能な開発体制の確保を、情報システムを統括する責任者に求めること。	遵守事項の集約
166	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、開発体制の確保にあたっては、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	6.1.3(1)(a) 解説	解説：情報システムを統括する責任者が確立した体制が、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）となるように求める事項である。 なお、「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	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		の資源を確保する者を想定している。	
167	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。	6.1.3(1)(b)	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、委託先が実施すべき対策事項（本項(2)から(5)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。	遵守事項の集約
168	1.5.2.3(1)(a)(イ) 解説	解説：ソフトウェア開発を委託先に行わせる場合には、ソフトウェア開発を実施する者に実施の責任を負わせるセキュリティに係る要件を選択し、それを委託先に保証させることを求める事項である。「委託先に実施について保証させる」手段は、契約（付随する確認書等を含む。）によることとなる。	6.1.3(1)(b) 解説	解説：ソフトウェア開発を委託先に行わせる場合には、ソフトウェア開発を実施する者に実施の責任を負わせるセキュリティにかかわる要件を選択し、それを委託先に保証させることを求める事項である。「委託先に実施について保証させる」手段は、契約（付随する確認書等を含む。）によることとなる。	解説の修正
169	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	6.1.3(2)(a) 解説	解説：ソフトウェア開発にかかわ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	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		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。	
170	1.5.2.3(1)(a)(エ) 解説	解説：運用中の情報システムを利用してソフトウェアの作成及び試験を行うことにより、運用中の情報システムに悪影響が及ぶことを回避することを求める事項である。これは運用中の情報システム全体ではなく一部だけの場合も同様である。例えば、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにすること等も含まれる。	6.1.3(2)(b) 解説	解説：運用中の情報システムを利用してソフトウェアの作成及び試験を行うことにより、運用中の情報システムに悪影響が及ぶことを回避することを求める事項である。	解説の修正
171	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	6.1.3(3)(a)	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、及び当該ソフトウェアにおいて取り扱う情報の格付けに応じて、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	遵守事項の集約

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		適切に設計し、設計書に明確に記述すること。		し、設計書に明確に記述すること。	
172	1.5.2.3(1)(a)(カ) 解説	解説：「管理機能」とは、真正確認及び権限管理等のセキュリティ機能を管理するための機能のほか、故障、事故及び障害等の発生時に行う対処及び復旧に係る機能、事故発生時の証跡保全の機能等を指し、これらの必要性をソフトウェアの設計時から検討することにより、必要がある場合にはソフトウェアに組み込むことを求める事項である。	6.1.3(3)(b) 解説	解説：「管理機能」とは、真正確認及び権限管理等のセキュリティ機能を管理するための機能のほか、故障、事故及び障害等の発生時に行う対処及び復旧にかかわる機能、事故発生時の証跡保全の機能等を指し、これらの必要性をソフトウェアの設計時から検討することにより、必要がある場合にはソフトウェアに組み込むことを求める事項である。	解説の修正
173	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。 「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	6.1.3(3)(d) 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。 「データの妥当性」とは、例えば、HTML タグやスクリプト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	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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。		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。	
174		（削除）	6.1.3(4)(c)	【強化遵守事項】	強化遵守事項から基本遵守事項に修正
175	1.5.2.3(1)(a)(シ)	情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。	6.1.3(4)(c)	情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。	遵守事項の集約 強化遵守事項から基本遵守事項に修正
176	1.5.2.3(2)	ソフトウェア開発に係る規定の遵守			遵守事項の集約
177	1.5.2.3(2)	【基本遵守事項】			遵守事項の集約
178	1.5.2.3(2)(a)	情報システムセキュリティ責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。			遵守事項の集約
179	1.5.2.3(2)(a) 解説	解説：ソフトウェア開発を行う情報システムセキュリティ責任者が、府省庁で整備したソフトウェア開発に係る規定を遵守して、ソフトウェアの開発を行うことを定めた事項である。			集約による移動
180	1.5.2.4	暗号と電子署名の標準手順	4.1.6	暗号と電子署名（鍵管理を含む）	修正
181	1.5.2.4 趣旨	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	4.1.6 趣旨	情報システムの利用においては、当該情報システムで取り扱	趣旨の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		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の付与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。 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。		う情報の漏えいや改ざん等を防ぐために、情報の暗号化及び電子署名の付与が有効とされている。なお、暗号化及び電子署名の付与のアルゴリズム、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方式を定めることが重要である。 これらのことを勘案し、本項では、暗号化及び電子署名の付与に関する対策基準を定める。	
182	1.5.2.4(1)	暗号と電子署名に係る規定の整備	4.1.6(1)	暗号化機能及び電子署名の付与に係る方式の整備	表現の適正化
183	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、以下の事項を含めて定めること。	4.1.6(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付与のアルゴリズム及び方法を、以下の事項を含めて定めること。	表現の適正化
184	1.5.2.4(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	4.1.6(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の付与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の付与を実装する	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		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。	
185	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、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、（ア）にもと	4.1.6(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の付与について、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の付与等についても、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、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の付与について、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、（ア）	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。 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。 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。		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。 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の付与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。 暗号化又は電子署名の付与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。	
186	1.5.2.4(1)(b)	統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）及び（イ）の手順（以下「鍵の管理手順等」という。）を定めること。	4.1.6(1)(b)	統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等（以下「鍵の管理手順等」という。）を定めること。	遵守事項の集約
187	1.5.2.4(1)(b)(ア)	鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した	4.1.6(1)(b)	統括情報セキュリティ責任者は、暗号化された情報（書面を	表現の適正化

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		場合の対処手順等		除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等（以下「鍵の管理手順等」という。）を定めること。	
188	1.5.2.4(1)(b)(イ)	鍵の保存手順	4.1.6(1)(c)	統括情報セキュリティ責任者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存方法及び保存場所（以下「鍵の保存方法等」という。）を定めること。	表現の適正化
189	1.5.2.4(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って、暗号化された情報の復号又は電子署名の付与に用いる鍵の適正な管理を求める事項である。 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など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	4.1.6(1)(c) 解説	解説：鍵の保存方法及び保存場所を定めることによって、暗号化された情報の復号又は電子署名の付与に用いる鍵の適正な管理を求める事項である。 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など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	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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。		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ある。 情報システム共通として鍵の保存方法等を定める場合には、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方法等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。	
190	1.5.2.4(1)(c)	統括情報セキュリティ責任者は、暗号化された情報の復号に用いる鍵のバックアップの取得手順又は鍵の預託手順（以下「鍵のバックアップ手順等」という。）を定めること。	4.1.6(1)(d)	統括情報セキュリティ責任者は、暗号化された情報の復号に用いる鍵のバックアップの取得方法又は鍵の預託方法（以下「鍵のバックアップ方法等」という。）を定めること。	表現の適正化
191	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、鍵のバックアップ取得手順又は鍵の預託手順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	4.1.6(1)(d) 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、鍵のバックアップの取得方法又は鍵の預託方法を定めることを求める事項である。 例えば、復号に用いる鍵を紛失し、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	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
191	1.5.2.4(1)(c) 解説	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、本事項における鍵のバックアップ手順及び鍵の預託手順は、前事項の鍵の管理手順等に含めて整備することも可能である。	4.1.6(1)(d) 解説	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。	解説の修正
192	1.5.2.4(2)	暗号と電子署名に係る規定の遵守	4.1.6(4)	暗号化機能及び電子署名の付与機能の利用	表現の適正化
193	1.5.2.4(2)(a)	行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。	4.1.6(4)(a)	行政事務従事者は、要機密情報を移送する場合又は電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、定められたアルゴリズム及び方法に従い、情報を暗号化すること。	表現の適正化
194	1.5.2.4(2)(a) 解説	解説：情報を暗号化する場合及び情報に電子署名を付与する場合に、府省庁で定めたアルゴリズム及び方法を遵守することを求める事項である。	4.1.6(4)(a) 解説	解説：要機密情報を移送する場合又は電磁的記録媒体に保存する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。	解説の修正
195	1.5.2.4(2)(b)	行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順に従い、これを適切に管理すること。	4.1.6(4)(c)	行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等及び鍵の保存方法等に従い、これを適切に管理すること。	遵守事項の集約
196	1.5.2.4(2)(c)	行政事務従事者は、暗号化された情報の復号に用いる鍵につい	4.1.6(4)(d)	行政事務従事者は、暗号化された情報の復号に用いる鍵につい	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		て、定められた鍵のバックアップ手順等に従い、そのバックアップを取得すること。		て、定められた鍵のバックアップ方法等に従い、そのバックアップを取得すること。	
197	1.5.2.5(2)	規定の遵守	6.3.1(2)	措置の遵守	遵守事項の集約の適正化
198	1.5.2.5(2)(a)	行政事務従事者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。	6.3.1(2)(a)	行政事務従事者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずること。	表現の適正化
199	1.5.2.6(1)	ドメイン名の使用についての規定の整備	6.3.3(1)	ドメイン名の使用	表現の適正化
200	1.5.2.6(1)(a)(ア)	行政事務従事者は、府省庁外の者（国外在住の者を除く。以下、本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。 ･go.jp で終わるドメイン名 ･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 ただし、電子メール送信又は政府ドメイン名のウェブページでの掲載に限り以下の条件を満たす場合には、政府ドメイン名以外のドメイン名を府省庁以外のものとして告知してもよい。 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。	6.3.3(1)(a)(ア)	行政事務従事者が府省庁外の者（国外在住の者を除く。以下、本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。 ･go.jp で終わるドメイン名 ･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 ただし、電子メール送信又は政府ドメイン名のウェブページでの掲載に限り以下の条件をすべて満たす場合には、政府ドメイン名以外のドメイン名を府省庁以外のものとして告知してもよい。 ・電子メール送信の場合、告知内容についての問い合わせ先と	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		・告知内容についての問い合わせ先として政府ドメイン名による電子メールアドレスを明記しているか、又は政府ドメイン名による電子署名をしていること。 ・告知するドメイン名を管理する組織名を明記すること。 ・告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。 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る。 ・告知するドメイン名を管理する組織名を明記すること。 ・告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。		して政府ドメイン名による電子メールアドレスを明記しているか、又は政府ドメイン名による電子署名をしていること。 ・告知するドメイン名を管理する組織名を明記すること。 ・告知するドメイン名の有効性を確認した時期又は有効性を保証する期間について明記していること。	
201	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、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、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。	6.3.3(1)(a)(イ)	行政事務従事者が府省庁外の者に対して、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、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。	表現の適正化
202	1.5.2.6(1)(a)(ウ)	行政事務従事者は、府省庁外の者に対して、アクセスさせることを目的として情報を保存する	6.3.3(1)(a)(ウ)	行政事務従事者が府省庁外の者に対して、アクセスさせることを目的として情報を保存するた	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		ためにサーバを使用する場合には、政府ドメイン名のサーバだけを使用すること。		めにサーバを使用する場合には、政府ドメイン名のサーバだけを使用すること。	
203	1.5.2.6(2)	ドメイン名の使用についての規定の遵守			遵守事項の追加
204	1.5.2.6(2)	【基本遵守事項】			遵守事項の追加
205	1.5.2.6(2)(a)	行政事務従事者は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。			遵守事項の追加
206	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。			遵守事項の集約
207	1.5.2.7	不正プログラム感染防止のための日常的実施事項	4.2.2	不正プログラム対策	遵守事項の修正
208	1.5.2.7 趣旨	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	4.2.2 趣旨	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。 さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性など他者に対するセキュリティ脅威	趣旨の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		取り込み等において十分な注意を払う必要がある。 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とした対策基準を定める。		の原因となり得る。 これらのことを勘案し、本項では、不正プログラムに関する対策基準を定める。	
209	1.5.2.7(1)	不正プログラム対策に係る規定の整備	4.2.2(1)	情報システムの構築時	遵守事項の集約
210	1.5.2.7(1)(a)	統括情報セキュリティ責任者は、不正プログラム感染の回避を目的として、以下の措置を行政事務従事者に求める規定を整備すること。	4.2.2(1)(a)	情報セキュリティ責任者は、不正プログラム感染の回避を目的とした行政事務従事者に対する留意事項を含む日常的実施事項を定めること。	遵守事項の集約
211	1.5.2.7(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）～（キ）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。	4.2.2(1)(a) 解説	解説：日常的に不正プログラム対策のために実施する事項の明文化を求める事項である。 「行政事務従事者に対する留意事項」とは、アンチウイルスソフトウェア等が現存する不正プログラムをすべて検知できるとは限らないため、行政事務従事者に対して注意喚起を行う事項であり、例えば、差出人が不明な電子メールに添付された不審なファイルを実行しないこと、ウェブクライアントのセキュリティ設定を不必要に低下させないこと、不審なホームページを閲覧しないこと等である。 「日常的実施事項」とは、不正プログラムに関する情報の収集やアンチウイルスソフトウェア等による不正プログラムの検出等が挙げられる。これらの事項	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
				については、不正プログラム対策の実施単位ごとに定めることが原則であるが、複数の不正プログラム対策の実施単位において共通して運用できる場合には、複数の実施単位で内容を整備する等状況に応じていずれかの方法を選択することが可能である。	
212	1.5.2.7(1)(a)(ア)	行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。	4.2.2(2)(b)	行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。	表現の適正化
213	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る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	4.2.2(2)(b) 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る実行ファイル等の実行を禁止する事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		ームページを閲覧しないこと等である。			
214	1.5.2.7(1)(a)(イ) 解説	解説：アンチウイルスソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。 自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。 また、最新の状態に維持する方法としては、端末ごとに利用者が自動化の設定をする方法のほか、情報システムセキュリティ責任者等が管理する端末を一括して自動化する方法もあるため、情報セキュリティ責任者が適切な方法を選択すること。同様に(ウ)～(オ)の事項は、情報セキュリティ責任者が適切な方法を選択すること。	4.2.2(2)(c) 解説	解説：アンチウイルスソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。 自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。 また、最新の状態に維持する方法としては、端末ごとに利用者が自動化の設定をする方法のほか、情報システムセキュリティ責任者等が管理する端末を一括して自動化する方法もあるため、情報セキュリティ責任者が適切な方法を選択すること。同様に(d)～(f)の事項は、情報セキュリティ責任者が適切な方法を選択すること。	解説の修正
215	1.5.2.7(1)(a)(カ)	行政事務従事者は、不正プログ	4.2.2(2)(g)	行政事務従事者は、ソフトウェ	遵守事項の

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		ラム感染の予防に努めること。		アのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。	修正
216	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すべて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などがある。	4.2.2(2)(g) 解説	解説：例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの感染を防ぐ、といった個別のアプリケーションごとに設定することが可能な不正プログラム感染の予防に役立つ措置の実施を求める事項である。オペレーティングシステムに不正プログラムに対処する機能がある場合には、当該機能を利用しても差し支えない。	解説の修正
217	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恐れのある場合には、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。			遵守事項の追加
218	1.5.2.7(1)(a)(キ) 解説	解説：不正プログラムに感染した恐れがある電子計算機については、他の電子計算機への感染など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			解説の追加

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		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することがあげられる。			
219	1.5.2.7(2)	不正プログラム対策に係る規定の遵守			遵守事項の集約
220	1.5.2.7(2)	【基本遵守事項】			遵守事項の集約
221	1.5.2.7(2)(a)	行政事務従事者は、定められた不正プログラム対策に係る規定に基づいて、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。			遵守事項の集約
222	1.5.2.7(2)(a) 解説	解説：すべて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。			集約による移動
223	第 2 編	情報システム編			構成変更
224	2.1.1.2(2)(a)	情報システムセキュリティ責任者は、行政事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付け及び取扱制限に従って、アクセス制御を行うこと。	4.1.2(2)(a)	行政事務従事者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。	主語の変更 遵守事項の統合
225	2.1.1.2(2)(a) 解説	解説：共有ファイルサーバのアクセス制御のように、情報システムを行政事務従事者が利用する際に、自らがアクセス制御を行うことができない場合、情報システムの導入時及び運用時にアクセス制御を行うことを求め	4.1.2(2)(a) 解説	解説：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、当該情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定を行うことを求め	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		た事項である。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、読み取り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。 また、行政事務従事者自らがアクセス制御を行うことが出来る場合、1.3.1.3(1)(a)の規程に基づき対策を行うこと。		る事項である。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。 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。	
226	2.1.1.3(2)(k) 解説	解説：識別コードの付与に係る記録は将来の障害・事故等の原因調査に備えて、不用意に消去しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、適切な承認を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体に付与したかを知るための記録を消去してはならない。	4.1.3(2)(k) 解説	解説：識別コードの付与に係る記録は将来の障害等の原因調査に備えて、不用意に消去しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、適切な承認を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体に付与したかを知るための記録を消去してはならない。	表現の適正化
227	2.1.1.3(3)(b) 解説	解説：不正使用の報告を受けた場合には、他の基準項目で定められている障害・事故等の対処	4.1.3(3)(b) 解説	解説：不正使用の報告を受けた場合には、他の基準項目で定められている障害等の対処に係る	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		に係る遵守事項とともに、本事項の対処を実施する。 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、すべての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得すべきである。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行すべきである。		遵守事項とともに、本事項の対処を実施する。 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、すべての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得すべきである。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行すべきである。	
228	2.1.1.4(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認め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。	4.1.4(3)(a)	情報セキュリティ責任者又は情報システムセキュリティ責任者は、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、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ統括情報セキュリティ責任者若しくは情報セキュリティ責任者に報告すること。	主語の変更 遵守事項の修正
229	2.1.1.4(4)(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認めた情報システムにおいては、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。	4.1.4(4)(a)	情報セキュリティ責任者又は情報システムセキュリティ責任者は、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、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。	主語の変更 遵守事項の修正
230	2.1.1.5(1)(b) 解説	解説：保証のための対策を行う必要性があると認めた場合に、	4.1.5(1)(b) 解説	解説：保証のための対策を行う必要性があると認めた場合に、	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		保証のための機能を情報システムに設けることを求める事項である。 保証のための機能とは、2.1.1.1～2.1.1.4で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能のことをいう。これには大きく分けて以下の２つのものがある。 （ア）2.1.1.1～2.1.1.4の機能とは異なる観点での保護を高めるための機能： 2.1.1.1～2.1.1.4の機能は、主として情報及び情報システムの機密性、完全性及び可用性を保護することを目的とした機能である。これに加えて、情報及び情報システムの真正性（Authenticity）、否認不能性（Non-Repudiation）を保護するための機能等を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。 （イ）2.1.1.1～2.1.1.4 の機能及び上の（ア）の機能の動作が適正であることを確認するための機能： 2.1.1.1～2.1.1.4 の機能及び上の（ア）の機能は情報及び情報システムを保護するための機能		保証のための機能を情報システムに設けることを求める事項である。 保証のための機能とは、4.1.1～4.1.4で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能のことをいう。これには大きく分けて以下の２つのものがある。 （ア）4.1.1～4.1.4の機能とは異なる観点での保護を高めるための機能： 4.1.1～4.1.4の機能は、主として情報及び情報システムの機密性、完全性及び可用性を保護することを目的とした機能である。これに加えて、情報及び情報システムの真正性（Authenticity）、否認不能性（Non-Repudiation）を保護するための機能等を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。 （イ）4.1.1～4.1.4 の機能及び上の（ア）の機能の動作が適正であることを確認するための機能： 4.1.1～4.1.4 の機能及び上の（ア）の機能は情報及び情報システムを保護するための機能と	

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		といえる。それに対して（イ）は、それらの機能を監視して、異常やその兆候を検知し、検知された問題を解決する対処をすることによって、それらの機能の回復に備えるための機能等である。これらの機能を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。 また、保証のための機能は、主体認証機能等の各項のような個別のものではなく、複数の機能であったり、それら複数のものを組み合わせた機能であったりする場合もある。情報セキュリティをより高めるために必要となる機能を設けることで本項の遵守事項を達成することができる。		いえる。それに対して（イ）は、それらの機能を監視して、異常やその兆候を検知し、検知された問題を解決する対処をすることによって、それらの機能の回復に備えるための機能等である。これらの機能を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。 また、保証のための機能は、主体認証機能等の各項のような個別のものではなく、複数の機能であったり、それら複数のものを組み合わせた機能であったりする場合もある。情報セキュリティをより高めるために必要となる機能を設けることで本項の遵守事項を達成することができる。	
231	2.1.1.6 趣旨	情報システムの利用においては、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐために、情報の暗号化及び電子署名が有効とされている。この際、予め定めた暗号アルゴリズム及び方法に基づき、暗号及び電子署名を適切な状況で利用する必要がある。 これらのことを勘案し、本項では、暗号化及び電子署名に関する対策基準を定める。	4.1.6 趣旨	情報システムの利用においては、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐために、情報の暗号化及び電子署名の付与が有効とされている。なお、暗号化及び電子署名の付与のアルゴリズム、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	趣旨の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
				で標準となる方式を定めることが重要である。 これらのことを勘案し、本項では、暗号化及び電子署名の付与に関する対策基準を定める。	
232	2.1.1.6(1)	暗号化機能及び電子署名機能の導入	4.1.6(2)	暗号化機能及び電子署名の付与機能の導入	遵守事項の修正
233	2.1.1.6(1)(c)	情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。	4.1.6(2)(c)	情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。	遵守事項の修正
234	2.1.1.6(1)(c) 解説	解説：電子署名の付与及び検証を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与及び検証を行う機能を付加する必要性の有無を検討しなければならない。	4.1.6(2)(c) 解説	解説：電子署名の付与を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の完全性の程度から電子署名の付与を行う機能を付加する必要性の有無を検討しなければならない。	解説の修正
235	2.1.1.6(1)(d)	情報システムセキュリティ責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。	4.1.6(2)(ｄ)	情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。	遵守事項の修正
236	2.1.1.6(1)(d) 解説	解説：情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与又は検証を行う機能を付加する必要性が認められる場合に、当該機能を情報シス	4.1.6(2)(d) 解説	解説：情報の完全性の程度から電子署名の付与を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項であ	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		テムに設けることを求める事項である。		る。	
237	2.1.1.6(1)(e)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。	4.1.6(2)(e)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。	遵守事項の修正
238	2.1.1.6(1)(f)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。	4.1.6(2)(f)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。	遵守事項の修正
239	2.1.1.6(1)(g)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。	4.1.6(2)(g)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。	遵守事項の修正
240	2.1.1.6(1)(h) 解説	解説：暗号化された情報の復号又は電子署名の付与に用いる鍵について、技術的な対策等に加え、物理的対策を講ずることを求める事項である。鍵を格納する電磁的記録媒体が盗難され、	4.1.6(2)(h) 解説	解説：暗号化された情報の復号又は電子署名の付与に用いる鍵について、技術的な対策等に加え、物理的対策を講ずることを求める事項である。鍵を格納する電磁的記録媒体が盗難され、	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		鍵が開封される等しても、鍵情報が外部へ漏えいしない仕組みが必要である。 この場合、耐タンパー性を有するとは、例えば、ISO/IEC 19790 第５章の規定に照らし合わせると、他のセキュリティ対策との組み合わせによりレベル２以上を選択することが可能であるが、他の組み合わせがない場合、レベル３以上が相当する。		鍵が開封される等しても、鍵情報が外部へ漏えいしない仕組みが必要である。	
241	2.1.1.6(2)	暗号化及び電子署名に係る管理	4.1.6(3)	暗号化及び電子署名の付与に係る管理	遵守事項の修正
242	2.1.1.6(2)(b)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。	4.1.6(3)(b)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。	遵守事項の修正
243	2.1.2.1(1)(a)	情報システムセキュリティ責任者は、電子計算機及び通信回線装置（公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。）の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。	4.2.1(1)(b)	情報システムセキュリティ責任者は、電子計算機及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。	遵守事項の統合
244	2.1.2.2(1)(c)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウ	4.2.2(1)(d)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、異なる業者のアンチウイルスソフトウ	表現の適正化

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		ェア等を組み合わせ、導入すること。		ェア等を組み合わせ、導入すること。	
245	2.1.2.2(1)(c) 解説	解説：複数の種類のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。 アンチウイルスソフトウェア等は、製品ごとに不正プログラム定義ファイルの提供時期及び種類が異なる。また、これらは現存するすべての不正プログラムを検知及び除去できるとは限らず、アンチウイルスソフトウェア等の不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害が発生する可能性を低減させるため、感染経路において異なる製品や技術を組み合わせ、どれか１つの不具合で、その環境のすべてが不正プログラムの被害を受けることのないようにする必要がある。	4.2.2(1)(d) 解説	解説：複数の業者のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。 アンチウイルスソフトウェア等は、製品ごとに不正プログラム定義ファイルの提供時期及び種類が異なる。また、これらは現存するすべての不正プログラムを検知及び除去できるとは限らず、アンチウイルスソフトウェア等の不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害が発生する可能性を低減させるため、感染経路において複数の製品や技術を組み合わせ、どれか１つの不具合で、その環境のすべてが不正プログラムの被害を受けることのないようにする必要がある。	解説の修正
246	2.1.2.2(2)(b)	情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。	4.2.2(2)(h)	情報セキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。	主語の変更 遵守事項の統合
247	2.1.2.2(2)(b) 解説	解説：1.5.2.7(1)(a)の規定による統括情報セキュリティ責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された	4.2.2(2)(h) 解説	解説：不正プログラム対策状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		場合は改善することを求める事項である。			
248	2.2.1.1(1)(a) 解説	解説：安全区域への不審者の立入りを防止し、安全区域のセキュリティを確保するための事項である。 措置としては、身分を確認できる物の提示の義務化、安全区域の所在の表示の制限等が挙げられる。 なお、本項のすべての遵守事項において、庁舎等の施設全体で対策が実施されている遵守事項がある場合には、当該対策を更に居室等毎に実施することまでは求めておらず、施設における対策により代替可能である。	5.1.1(1)(a) 解説	解説：安全区域への不審者の立入りを防止し、安全区域のセキュリティを確保するための事項である。 措置としては、身分を確認できる物の提示の義務化、安全区域の所在の表示の制限等が挙げられる。	解説の修正
249	2.2.1.1(1)(c)	情報システムセキュリティ責任者は、安全区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。	5.1.1(1)(c)	情報システムセキュリティ責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。	表現の適正化
250	2.2.1.1(1)(c) 解説	解説：安全区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。 なお、立入りを許可された者であるかの確認のために主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずること等が望ましい。	5.1.1(1)(c) 解説	解説：安全区域へ立ち入る者の主体認証を実施することで、許可されていない者の立入りを排除するための事項である。 なお、主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずること等が望ましい。	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
251	2.2.1.1(1)(d)	情報システムセキュリティ責任者は、安全区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。	5.1.1(1)(d)	情報システムセキュリティ責任者は、安全区域から退出する者の主体認証を行うための措置を講ずること。	表現の適正化
252	2.2.1.1(1)(e)	情報システムセキュリティ責任者は、立入りを許可された者が、立入りを許可されていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。	5.1.1(1)(e)	情報システムセキュリティ責任者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。	表現の適正化
253	2.2.1.1(1)(e) 解説	解説：安全区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。 対策としては、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。	5.1.1(1)(e) 解説	解説：安全区域の立入り及び退出時における主体認証を確実に実施するための事項である。 対策としては、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。	表現の適正化
254	2.2.1.1(1)(f)	情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を許可する手続を整備すること。また、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載するための文書を整備すること。	5.1.1(1)(f)	情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を承認する手続を整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載するための文書を整備すること。	表現の適正化
255	2.2.1.1(1)(g)	情報システムセキュリティ責任者は、安全区域へ立入りを許可された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。	5.1.1(1)(g)	情報システムセキュリティ責任者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
256	2.2.1.1(2)(d) 解説	解説：訪問者が許可されていない区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。	5.1.1(2)(d) 解説	解説：訪問者が許可されていない区域へ立ち入らないようにすることを求める事項である。訪問者に主体認証情報格納装置は貸与しない又は貸与する場合には最小限の権限を持った装置とする方法等が挙げられる。	解説の修正
257	2.2.1.1(2)(f)	情報システムセキュリティ責任者は、訪問者と継続的に立入りを許可された者とを外見上判断できる措置を講ずること。	5.1.1(2)(f)	情報システムセキュリティ責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。	表現の適正化
258	2.2.1.1(2)(f) 解説	解説：継続的に立入りを許可された者と訪問者を区別するための事項である。 これにより、許可されていない区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。	5.1.1(2)(f) 解説	解説：継続的に立入りが許可された者と訪問者を区別するための事項である。 これにより、許可されていない区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。	表現の適正化
259	2.2.1.1(3)(d) 解説	解説：行政事務従事者の離席時に、電子計算機及び通信回線装置を第三者による不正操作から保護するための事項である。 対策としては、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報	5.1.1(3)(d) 解説	解説：行政事務従事者の離席時に、電子計算機及び通信回線装置を第三者による不正操作から保護するための事項である。 対策としては、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		格納装置を事務室への立入りの許可の確認にも利用する方法等が挙げられる。		格納装置を事務室の主体認証にも利用する方法等が挙げられる。	
260	2.2.1.1(4)(b)	行政事務従事者は、情報システムセキュリティ責任者の許可を得た上で、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。	5.1.1(4)(b)	行政事務従事者は、情報システムセキュリティ責任者の承認を得た上で、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。	表現の適正化
261	2.2.2.1(1)(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。	5.2.1(1)(c)	情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。	表現の適正化
262	2.2.2.1(1)(a) 解説	解説：通常の運用において十分な性能を確保することを求める事項である。 例えば、電子計算機の負荷に関して事前に見積もり、試験等を実施し、必要となる処理能力及び容量を想定し、それを備える必要がある。また、将来にわたっても十分な性能を確保できるように、拡張性や余裕を持たせておく必要がある。	5.2.1(1)(c) 解説	解説：通常の運用において十分な能力を確保することを求める事項である。 例えば、電子計算機の負荷に関して事前に見積もり、試験等を実施し、必要となる処理能力及び容量を想定し、それを備える必要がある。また、将来にわたっても十分な性能を確保できるように、拡張性や余裕を持たせておく必要がある。	表現の適正化
263	2.2.2.1(1)(b) 解説	解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。 人為的な脅威としては建物内への侵入、部外者による操作、失火による火災又は停電等があり、環境的脅威としては地震、	5.2.1(1)(i) 解説	解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。 人為的な脅威としては建物内への侵入、利用者による誤操作、失火による火災又は停電等があり、環境的脅威としては地震、	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		落雷又は風水害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。		落雷又は風水害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。	
264	2.2.2.1(1)(c) 解説	解説：障害・事故等が発生した場合、サービスを提供する電子計算機を代替電子計算機に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。災害等を想定して冗長構成にする場合には、電子計算機を遠隔地に設置することが望ましい。	5.2.1(1)(j) 解説	解説：障害等が発生した場合、サービスを提供する電子計算機を代替電子計算機に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。災害等を想定して冗長構成にする場合には、電子計算機を遠隔地に設置することが望ましい。	表現の適正化
265	2.2.2.1(2)(a) 解説	解説：電子計算機を業務目的以外に利用することを禁止する事項である。例えば、悪意のあるウェブサイトを閲覧することによって、不正プログラムを感染させられてしまうことから回避するため、業務目的外でのウェブサイトの閲覧を禁止すること等が求められる。	5.2.1(2)(c) 解説	解説：電子計算機を業務目的以外に利用することを禁止する事項である。	解説の修正
266	2.2.2.2(1)(d)	情報システムセキュリティ責任者は、要機密情報を取り扱うモバイル PC については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。	5.2.2(1)(d)	情報システムセキュリティ責任者は、要機密情報を取り扱うモバイル PC については、電磁的記録媒体に保存される情報の暗号化を行う機能を付加すること。	表現の適正化
267	2.2.2.3(1)(c) 解説	解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。なお、ソフトウェ	5.2.3(1)(c) 解説	解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		アの設定は初期状態が安全であるとは限らないことについても留意して確認すること。			
268	2.2.2.3(1)(e)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とすること。	5.2.3(2)(h)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、サービス提供に必要なサーバ装置の負荷を複数のサーバ装置に分散すること。	遵守事項の修正
269	2.2.2.3(1)(e) 解説	解説：障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNSによる負荷分散又は冗長構成等の実施を求める事項である。	5.2.3(2)(h) 解説	解説：障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNSによる負荷分散等の実施を求める事項である。	解説の修正
270	2.2.2.3(2)(e) 解説	解説：サーバ装置上での不正行為及び不正利用を監視するための事項である。 「セキュリティ状態を監視」するとは、サーバ装置上での不正な行為及び要機密情報への不正なアクセス等の発生を監視することである。監視の方法としては、アクセスログを定期的に確認することや、侵入検知システム、アンチウイルスソフト又はファイル完全性チェックツール等を利用することができる。	5.2.3(2)(f) 解説	解説：サーバ装置上での不正行為及び不正利用を監視するための事項である。 「セキュリティ状態を監視」するとは、サーバ装置上での不正な行為及び要機密情報への不正なアクセス等の発生を監視することである。監視の方法としては、侵入検知システム、アンチウイルスソフト又はファイル完全性チェックツール等が利用できる。	解説の修正
271	2.2.3.1(1)(b)	（削除）	5.3.2(1)(b)	【強化遵守事項】	強化遵守事項から基本遵守事項に

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
					修正
272	2.2.3.1(2)(a) 解説	解説：各府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービス以外の電子メールサービス（以下「各府省庁以外の電子メールサービス」という。）を、業務遂行に係る情報を含む電子メールの送受信に利用することを禁ずる事項である。なお、上記の「送受信」には電子メールの「転送」が含まれている。したがって、各府省庁以外の電子メールサービスの電子メールアドレスに業務遂行に係る情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に自動転送については当該電子メールに含まれる情報の格付け及び取扱制限にかかわらず行われるため、要機密情報の移送についての遵守事項に背反しないようにも留意する必要がある。	5.3.2(2)(a) 解説	解説：各府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービス以外の電子メールサービスを、業務遂行に係る情報を含む電子メールの送受信に利用することを禁ずる事項である。なお、上記の「送受信」には電子メールの「転送」が含まれている。したがって、私的に契約した電子メールサービスの電子メールアドレスに業務遂行に係る情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に自動転送については当該電子メールに含まれる情報の格付けにかかわらず行われるため、要機密情報の移送についての遵守事項に背反しないようにも留意する必要がある。	解説の修正
273	2.2.3.1(2)(b)	行政事務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。	5.3.2(2)(b)	行政事務従事者は、受信した電子メールを電子メールクライアントにおいてテキストとして表示すること。	遵守事項の修正
274	2.2.3.1(2)(b) 解説	解説：例えば HTML メールの表示により、偽のホームページに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること等の	5.3.2(2)(b) 解説	解説：HTML メールの表示により、偽のホームページに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること及び不正	解説の修正

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		不正なスクリプトが実行されることを防ぐことを定めた事項である。 「スクリプト」とは、ここではJavaScript 等の電子計算機にて簡易的に実行することができるプログラムをいう。 「スクリプトが電子計算機で実行されないように表示させる」とは、表示をテキスト形式のみに設定して表示することや端末でスクリプトの実行を禁止された情報システムを用いて表示することが挙げられる。 そのため、情報システムの管理者により、行政事務従事者が使用する電子メールクライアントの設定が上述のとおり適切に行われ、かつ、行政事務従事者が電子メールクライアントの設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。 なお、本項は、スクリプトが電子計算機で実行されないのであれば、電子メールの文字装飾や画像の表示を禁止するものではない。 また、本項は、端末等にインストールされる電子メールクライアントを対象としているため、ウェブブラウザにより読み書きする電子メール（いわゆるウェブメール）は対象外となる。		なスクリプトが実行されること等を防ぐことを定めた事項である。 なお、「テキスト」には、リッチテキストが含まれる。また、本項は、端末等にインストールされる電子メールクライアントを対象としているため、ウェブブラウザにより読み書きする電子メール（いわゆるウェブメール）は対象外となる。しかしながら、ウェブメールにおいても、同様の脅威が想定されることから、テキスト表示の設定が不可能なウェブメールは利用しないことが望ましい。	

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
275	2.2.3.2(1)(c)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化する機能を設けること。	5.3.3(1)(c)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。	表現の適正化
276	2.2.3.2(2)(a)	行政事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。			遵守事項の追加
277	2.2.3.2(2)(a) 解説	解説：行政事務従事者が意図しない悪意のあるソフトウェアが電子計算機において実行されること等により、情報が漏えいしてしまうことや他の電子計算機を攻撃してしまうこと等を防止するため、ウェブクライアントのセキュリティ設定を適切に行うことを求める事項である。 具体的には、閲覧するホームページの信頼性やウェブクライアントが動作する電子計算機にて扱う情報の機密性等に応じて、以下のようなセキュリティ設定項目について適切な値を選択すること。 ・ActiveX コントロールの実行 ・JavaScript の実行 ・Java の実行 ・Cookie の保存　等			解説の追加

No.	第4版 遵守事項	第4版	第3版 遵守事項	第3版	変更点
		そのため、情報システムの管理者がウェブクライアントのセキュリティ設定を上述のとおり行い、かつ、行政事務従事者が当該設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。			
278	2.2.3.2(2)(c)	行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。			遵守事項の追加
279	2.2.3.2(2)(c)(ア)	送信内容が暗号化されること。			遵守事項の追加
280	2.2.3.2(2)(c)(ア) 解説	解説：主体認証情報等を入力して送信する場合には、情報漏洩を防止するため、ブラウザの鍵アイコンの表示を確認する等により、SSL や TLS 等の暗号通信が使用されていること等の手段を限定することを求める事項である。なお、「閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合」とは、例えばウェブメールを使用する際に主体認証情報等を入力すること等を指す。なお、府省庁内の通信回線のみを使用しているウェブサイトの場合、2.2.3.2(1)(c)にて情報システムセキュリティ責任者が暗号化を行う必要があると認めた情報システムを利用する際には、当該事項を確認する必要があ			解説の追加

No.	第４版 遵守事項	第４版	第３版 遵守事項	第３版	変更点
		る。			
281	2.2.3.2(2)(c)(イ)	当該ウェブサイトが送信先として想定している組織のものであること。			遵守事項の追加
282	2.2.3.2(2)(c)(イ) 解説	解説：主体認証情報等を入力して送信する場合には、サイト証明書の内容から当該ウェブサイトが想定している組織のものであるかを確認することにより、当該情報の送信先を限定することを求める事項である。なお、ウェブサイトの閲覧時にサイト証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性がないかを確認することが必要である。			解説の追加
283	2.2.3.3(1)(d)	情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて、府省庁内のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。	5.3.4(1)(d)	情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて、内部のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。	表現の適正化
284	2.2.4.1(1)(l) 解説	解説：障害・事故等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替回線又は代替通信回線装置に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。災害等を想定して冗長構成にする場合には、被	5.4.1(1)(q)	解説：障害等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替回線又は代替通信回線装置に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。災害等を想定して冗長構成にする場合には、被災時に	表現の適正化

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		災時にも冗長構成のうち少なくとも一系統が存続可能な構成にすることが望ましい。		も冗長構成のうち少なくとも一系統が存続可能な構成にすることが望ましい。	
285	2.2.4.2(3)(b)	情報システムセキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要性があると判断すること。	5.4.2(3)(b)	情報システムセキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。	遵守事項の修正
286	2.2.4.2(3)(b) 解説	解説：無線 LAN を利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。 なお、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を求めているが、WEP（Wired Equivalent Privacy）等は、比較的容易に解読できるという脆弱性が報告されており、また同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択すること。この場合、暗号化については、暗号と電子署名の標準手順に従わなければならない。 参考：総務省「国民のための情報セキュリティサイト」（http://www.soumu.go.jp/joho_tsusin/security/index.htm）に	5.4.2(3)(b) 解説	解説：無線 LAN を利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。	解説の修正

No.	第 4 版 遵守事項	第 4 版	第 3 版 遵守事項	第 3 版	変更点
		て、 「企業・組織の情報管理担当者の実践」のページにある、「安全な無線 LAN の利用」のページの解説を適宜参照。			
287	2.2.4.3(1)(b)	情報システムセキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。	5.4.3(1)(b)	情報セキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。	主語の変更
288	2.3.1	その他			構成変更