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)(平成 21 年度修正)新旧対照表

No.	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	第 4 版遵守事項	第 4 版	変更点
1	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。	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、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。	適用対象範囲の修正
2	1.2.1.3(1)(b) 解説	情報セキュリティ関係規程への違反があった場合に、違反者及び当該規程の実施に責任を持つ者を含む必要な者に対して、情報セキュリティを維持するために必要な措置を講ずることを求める事項である。重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、問題の早期解決、拡大防止の必要がある。例えば、情報セキュリティ関係規程について再度周知する方法が考えられる。	1.2.1.3(1)(b) 解説	情報セキュリティ関係規程への重大な違反により機密性、完全性、可用性が損なわれる等した情報及び情報システムを回復するとともに、情報セキュリティ対策の適切な実施を再度徹底するために、違反者及び当該規定の実施に責任を持つ者を含む必要な者に情報セキュリティ維持のための措置を講ずることを求める事項である。違反により情報が漏えい、滅失、き損し又は情報システムの利用に支障を来していれば、これを早急に解決し、問題の拡大を防止する	解説の修正

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
				必要がある。情報セキュリティ関係規程を知らずに違反を犯したのであれば、違反者及び当該規定の実施に責任を持つ者を含む必要な者にこれを知らせ、情報セキュリティを維持するための措置を講じさせる必要がある。	
3	1.2.2.2(1)(a) 解説	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トと同意である。	1.2.2.2(1)(a) 解説	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。	解説の修正
4	1.2.4.1(1)(c) 解説	情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合に、その是非を検討し、必要な措置を講ずることを求める事項である。例えば、行政事務従事者からの相談が妥当であると思料する場合に情報セキュリティ関係規程の見直しを行ったり、逆に行政事務従事者の理解不足が原因であると思料する場合は、再教育の措置を講ずること等が考えられる。	1.2.4.1(1)(c) 解説	情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合に、その是非を検討し、必要な措置を講ずることを求める事項である。例えば、行政事務従事者からの相談が妥当であると思科する場合に情報セキュリティ関係規程の見直しを行ったり、逆に行政事務従事者の理解不足が原因であると思科する場合は、再教育の措置を講ずること等が考えられる。	解説の修正
5	1.2.5.1 適用範囲	本項は、府省庁による貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次に掲げる営業品目に該当するものに適用する。	1.2.5.1 適用範囲	本項は、会計法第 29 条に規定する貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次に掲げる営業品目に該当するものに適用する。	表現の適正化

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
6		(削除)	1.2.5.1(6)(a) 解説	「納品検査」とは、会計法第 29 条の 11 第 2 項に規定されている「その受ける給付の完了の確認をするため必要な検査」のことであり、本項の適用範囲であげた業務に係る外部委託すべてを対象とする。	削除
7	1.3.1.1(2)(a) 解説	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、格付け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、決定した格付け及び取扱制限に基づき、その指定を行うこと。	1.3.1.1(2)(a) 解説		解説の追加
8	1.3.1.1(2)(b) 解説	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。 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	1.3.1.1(2)(b) 解説	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。	解説の修正・追加

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
		利用（4）を参照のこと。			
9	1.3.1.1(3)(a) 解説	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。	1.3.1.1(3)(a) 解説		解説の追加
10	1.3.1.3(1)(g) 解説	バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。障害・事故等に備えて適切な頻度で復元の演習も行い、行政事務従事者に習熟させる。	1.3.1.3(1)(g) 解説	バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。障害等に備えて適切な頻度で復元の演習も行い、行政事務従事者に習熟させる。	解説の修正
11	1.3.1.5(2)(c) 解説	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。	1.3.1.5(2)(c) 解説		解説の追加
12	1.3.1.6(1)(a) 解説	抹消するための方法としては、次の方法が挙げられる。 ・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを個々に抹消する方法	1.3.1.6(1)(a) 解説	抹消するための方法としては、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や、ハードディスクを消磁装置に	解説の修正・追加

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
		・ハードディスクを消磁装置に入れてディスク内のすべてのデータを抹消する方法 ・媒体を物理的に破壊する方法 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		入れてディスク内のすべてのデータを抹消する方法、媒体を物理的に破壊する方法が挙げられる。	
13	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	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	趣旨の修正

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
		重要である。		ことが重要である。	
14	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。	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。	解説の修正
15	2.1.1.1(1)(n) 解説	なお、当該情報システムのオペレーティングシステムが Unix 系の場合には、一般利用者でログオンした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログオンを禁止する設定により、その手順を強制することができる。	2.1.1.1(1)(n) 解説	なお、当該情報システムのオペレーションシステムが Unix の場合には、一般利用者でログオンした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログオンを禁止する設定により、その手順を強制することができる。	解説の修正
16	2.1.1.1(2)(e) 解説	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 の設定変更などをしないときには、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	例えば、情報システムのオペレーションシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更などをしないときには、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
17	2.1.1.4(1)(a)	情報セキュリティは、様々な	2.1.1.4(1)(a)		解説の追加

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
	解説	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り、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。 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。 証跡には、以下のような管理	解説		(2.1.1.4(1)(b)解説からの移動)

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
		記録が考えられる。 ・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 なお、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。 ・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			
18	2.1.1.4(1)(b) 解説	解説：証跡を取得する機能を設ける必要があると認められた場合に、当該機能を情報システムに設けることを求める事項である。	2.1.1.4(1)(b) 解説	解説：利用者の行動等の事象を証跡として記録するための機能を情報システムに設けることを求める事項である。 情報セキュリティは、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	解説の修正 （2.1.1.4(1)(a)解説への移動）

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
				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り、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。 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。 証跡には、以下の記録を含めることが考えられる。 ・利用者による情報システムの操作記録 ・操作する者、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	

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
				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	
19	2.1.1.4(1)(e) 解説	また、証跡として利用記録や監視記録を含めた場合には、対象となる利用者のプライバシーを侵害しないことにも配慮して、アクセスできる者を制限するように注意しなければならない。	2.1.1.4(1)(e) 解説		解説の追加
20	2.1.1.6(1)(h) 解説	この場合、耐タンパー性を有するとは、例えば、JIS X 19790:2007 7.5 物理的セキュリティ（ISO/IEC 19790:2006）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。	2.1.1.6(1)(h) 解説	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。	解説の修正
21	2.2.4.2(3)(b) (ク)解説	参考：総務省「国民のための情報セキュリティサイト」の「情報管理担当者のための情報セキュリティ対策－実践編」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin00.htm）にある、「安全な無線 LAN の利用」のページの解説を適	2.2.4.2(3)(b) (ク)解説	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。	解説の修正

No.	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	第 4 版 遵守事項	第 4 版	変更点
		宜参照。			
22	A.1.4	「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。	A.1.4		解説の追加