政府機関の情報セキュリティ対策のための
統一技術基準
新旧対照表

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
1		(削除)	第 2 編	第 2 編　情報システム編	構成変更
2	第 2.1 部	第 2.1 部　総則			構成変更
3	2.1.1.1	2.1.1.1 本統一技術基準の位置付け			構成変更
4	2.1.1.1(1)	政府機関の情報セキュリティ対策の強化における本統一技術基準の位置付け			構成変更
5	2.1.1.1(1)	政府機関の情報セキュリティ対策のための統一管理基準（以下「統一管理基準」という。）に準じる。			構成変更
6	2.1.1.1(2)	本統一技術基準の改訂			構成変更
7	2.1.1.1(2)	統一管理基準に準じる。			構成変更
8	2.1.1.1(3)	法令等の遵守			構成変更
9	2.1.1.1(3)	統一管理基準に準じる。			構成変更
10	2.1.1.2	2.1.1.2 本統一技術基準の使い方			構成変更
11	2.1.1.2(1)	全体構成			構成変更
12	2.1.1.2(1)	統一管理基準に準じる。			構成変更
13	2.1.1.2(2)	対策項目の記載事項			構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
					変更
14	2.1.1.2(2)	統一管理基準に準じる。			構成変更
15	2.1.1.2(3)	対策レベルの設定			構成変更
16	2.1.1.2(3)	統一管理基準に準じる。			構成変更
17	2.1.1.3	2.1.1.3 情報の格付の区分及び取扱制限の種類			構成変更
18	2.1.1.3(1)	格付及び取扱制限			構成変更
19	2.1.1.3(1)	統一管理基準に準じる。			構成変更
20	2.1.1.3(2)	格付の区分			構成変更
21	2.1.1.3(2)	統一管理基準に準じる。			構成変更
22	2.1.1.3(3)	取扱制限の種類			構成変更
23	2.1.1.3(3)	統一管理基準に準じる。			構成変更
24	2.1.1.4	2.1.1.4 評価の方法			構成変更
25	2.1.1.4	統一管理基準に準じる。			構成変更
26	2.1.1.5	2.1.1.5 用語定義			構成変更
27	2.1.1.5	統一管理基準に準じる。 以下は、本統一技術基準で初出の用語。			構成変更
28	2.1.1.5 【あ】	● 「受渡業者」とは、行政事務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとし		(1.1.1.4 から移動)	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ては、宅配便の集配、事務用品の納入等が考えられる。			
29	2.1.1.5 【か】	● 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表されたセキュリティホールが該当する。		(1.1.1.4 から移動)	構成変更
30	2.1.1.5 【は】	● 「複数要素（複合）主体認証（multiple factors authentication）方式」とは、複数の方法の組合せにより主体認証を行う方法である。	1.1.1.4	「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組合せにより主体認証を行う方法である。	構成変更
31	2.1.1.5 【ま】	● 「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。		(1.1.1.4 から移動)	構成変更
32	第 2.2 部	第 2.2 部　情報セキュリティ要件の明確化に基づく対策	第 2.1 部	第 2.1 部　情報セキュリティ要件の明確化に基づく対策	構成変更
33	2.2.1	2.2.1　情報セキュリティについての機能	2.1.1	2.1.1　情報セキュリティについての機能	構成変更
34	2.2.1.1	2.2.1.1 主体認証機能	2.1.1.1	2.1.1.1 主体認証機能	構成変更
35	2.2.1.1 趣旨	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来	2.1.1.1 趣旨	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。 これらのことを勘案し、本項では、主体認証機能の導入に関する対策基準を定める。 また、政府機関が有する各情報システムの利用者は、行政事務従事者に限られるものではない。例えば、国民向けのサービスを提供する情報システムの利用者は、行政事務従事者以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、行政事務従事者以外の者は本統一管理基準の適用範囲ではないため、それらの者に対しては、これを保護するよう注意喚起することが望ましい。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。		アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。 これらのことを勘案し、本項では、主体認証に関する対策基準を定める。 なお、政府機関が有する各情報システムの利用者は、行政事務従事者のほか、それ以外の者がある。例えば、国民向けのサービスを提供する情報システムの利用者は、行政事務従事者以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、行政事務従事者以外の者は本統一基準の適用範囲ではない。しかし、それらの者に対し、これを保護するよう注意喚起することが望ましい。	
36	2.2.1.1(1)(a)	情報システムセキュリティ責任者	2.1.1.1(1)(b)	情報システムセキュリティ責任者	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。		は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。	変更
37	2.2.1.1(1)(a) 解説	解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。 主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。 生体情報による主体認証を用いる場合には、その導入を決定する前に、この方式特有の誤認率と誤否率の課題があることを考慮して情報システムを設計する必要がある。この方式では、正当な本人に	2.1.1.1(1)(b) 解説	解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。 （以下は、2.1.1.1(1)(a)解説から移動） 主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カードや磁気ストライプカード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。なお、本項における解説としてはそれら３つの方	解説の移動、修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の行政事務の遂行への影響について検討してから導入を決定すること。 機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせる等について考慮するとよい。 なお、具体的な主体認証機能の設計に当たっては、当該情報システムに対して決定したセキュリティ要件（1.5.1.1(1)(b)を参照）を満たす必要がある。		式について記述するが、その他、位置情報等による方式もある。 生体情報による主体認証を用いる場合には、その導入を決定する前に、この方式特有の誤認率と誤否率の課題があることを考慮して情報システムを設計する必要がある。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の行政事務の遂行への影響について検討してから導入を決定すること。 機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせるなどについて考慮するとよい。	
38		(1.5.2.8(1)(a)(ア)へ移動)	2.1.1.1(1)(a)	情報システムセキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。	構成変更
39		(1.5.2.8(1)(a)(ア)解説へ移動) 解説の後半は、2.2.1.1(1)(a)解説へ移動	2.1.1.1(1)(a) 解説	解説：主体認証を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセスする主体の主体認証を行う必要性の有無を検討することを求める事項である。要保護情報を取	解説の移動

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				り扱う情報システムにおいては、主体認証を行う必要があると判断すること。 主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カードや磁気ストライプカード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。なお、本項における解説としてはそれら３つの方式について記述するが、その他、位置情報等による方式もある。 生体情報による主体認証を用いる場合には、その導入を決定する前に、この方式特有の誤認率と誤否率の課題があることを考慮して情報システムを設計する必要がある。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の行政事務の遂行への影響について検討してから導入を決定すること。 機微な情報へのアクセスであれ	

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				ば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせるなどについて考慮するとよい。	
40	2.2.1.1(1)(b)(ウ)	保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更及び提供（入力）させる際に、暗号化が行われない旨を通知すること。	2.2.1.1(1)(b)(ウ)	保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。	表現の適正化
41	2.2.1.1(1)(b)(ウ)解説	解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。 保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、主体認証情報が漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定する等の回避	2.1.1.1(1)(c)(ウ)解説	解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。 保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、これが漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定するなどの回避策を	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		策をとる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。 したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」等の警告を表示するようにすることが必要である。		とる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。 したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」などの警告を表示するようにすることが必要である。	
42	2.2.1.1(1)(d) 解説	解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用等の対策を講ずること。	2.2.1.1(1)(e) 解説	解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用などの対策を講ずること。	解説の修正
43	2.2.1.1(1)(e) (ア)解説	解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の利点が期待できる。 ・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が容易に記憶できる。 ・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、	2.1.1.1(1)(f) (ア)解説	解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の利点が期待できる。 ・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が容易に記憶できる。 ・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		本人自身が設定することにより、そのおそれが少なくなる。 なお、例えば、運用上の理由等で他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知することが望ましい。		本人自身が設定することにより、そのおそれが少なくなる。 なお、例えば、運用上の理由など で他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知することが望ましい。	
44	2.2.1.1(1)(e) (イ)解説	解説：情報システムセキュリティ責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。情報システムセキュリティ責任者に悪意がなくとも、悪意のある第三者によってその管理者権限が奪取されてしまった場合には、全ての利用者の主体認証情報を知られてしまうおそれがあるため、不可逆の暗号化を用いる等により、情報システムセキュリティ責任者自らも、他者の主体認証情報を知ることができないような措置を講ずる必要がある。	2.1.1.1(1)(f) (イ)解説	解説：情報システムセキュリティ責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。情報システムセキュリティ責任者に悪意がなくとも、仮に悪意ある者によってそのシステム管理者権限を奪取されてしまった場合に、すべての利用者の主体認証情報を知られてしまうおそれがあるため、不可逆の暗号化を用いるなどにより、情報システムセキュリティ責任者自らも、他者の主体認証情報を知ることができないような措置を講ずる必要がある。	解説の修正
45	2.2.1.1(1)(f)	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項のうちその特性に応じて適用可能な要件を全て満たす主体認証方式	2.1.1.1(1)(g)	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項が適用可能かどうかを検証した上で、当該主体認証方式に適用する	構成変更、遵守事項の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		を導入すること。		ことが可能な要件をすべて満たすこと。	
46	2.2.1.1(1)(f)(ウ)	正当な主体が容易に他者に主体認証情報の付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）	2.1.1.1(1)(g)(ウ)	正当な主体が容易に他者に主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）	表現の適正化
47		(1.4.1.1(2)(e)へ移動)	2.1.1.1(1)(h)	情報システムセキュリティ責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。	構成変更
48		(1.4.1.1(2)(e)解説へ移動)	2.1.1.1(1)(h)解説	解説：利用者の指紋情報など、主体認証情報として生体情報を取り扱う場合に、個人のプライバシーに配慮し、個人情報として厳格な管理を求める事項である。	構成変更
49	2.2.1.1(1)(f)解説	解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性等も考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしも全て充足することを求めるものではない。例えば、主体認証情報（パスワード）等による「知識」方式の場合には、要件(ウ)や(エ)を技術的に充足する必要はない。また、上記の（ア）	2.1.1.1(1)(g)解説	解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性なども考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしもすべて充足することを求めるものではない。例えば、主体認証情報（パスワード）等による「知識」方式の場合には、要件(ウ)や(エ)を技術的に充足する必要はない。また、上	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		～（ク）以外に気づいた事項があれば、適宜追加することが望ましい。		記の（ア）～（ク）以外に気づいた事項があれば、適宜追加することが望ましい。	
50	2.2.1.1(1)(g) 解説	解説：複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証が可能となる。 これは、単一要素（単一）主体認証方式（「単一要素（単一）主体認証（single factor authentication / single authentication）方式」とは、知識、所有、生体情報等のうち、単一の方法により主体認証を行う方式である。）の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまうが、複数要素（複合）主体認証方式の場合には、仮に一方の主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログオンされる可能性は依然低いと考えられるからである。	2.1.1.1(1)(i) 解説	解説：複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証が可能となる。 これは、単一要素（単一）主体認証方式（「単一要素（単一）主体認証（single factor authentication / single authentication）方式」とは、知識、所有、生体情報などのうち、単一の方法により主体認証を行う方式である。）の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまうが、複数要素（複合）主体認証方式の場合には、仮に一方の主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログオンされる可能性は依然低いと考えられるからである。	解説の修正
51	2.2.1.1(1)(h) 解説	解説：識別コードによる前回のログオンに関する情報（日時や装置名等）を通知することで、本人の識別コードが他者によって不正に使われた場合に、本人が気付く機会を得られるようにすることを求める事項である。	2.1.1.1(1)(j) 解説	解説：識別コードによる前回のログオンに関する情報（日時や装置名等）を通知することで、本人の識別コードが他者によって不正に使われた場合に、本人が気付く機会を得られるようにする。	解説の修正
52	2.2.1.1(1)(i) 解説	解説：通知によって本人が知る機会を得ること、及び組織が状況を	2.1.1.1(1)(k) 解説	解説：例えば、識別コードによるログインにおいて、指定回数以上	解説の修

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		管理できるようにすること等が考えられる。例えば、識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を本人に通知する、あるいは、当該識別コードによる情報システムへの以後のログインを無効にする（アカウントをロックする）機能の付加が挙げられる。		の主体認証情報の誤入力が検知された場合に、その旨を通知する、あるいは、当該識別コードによる情報システムへの以後のログインを無効にする（アカウントをロックする）機能の付加が挙げられる。通知によって本人が知る機会を得ること及び組織が状況を管理できることの 2 点を達成できることが望ましい。	正
53	2.2.1.1(1)(k) 解説	解説：一度使用した主体認証情報（パスワード等）の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。	2.1.1.1(1)(m) 解説	解説：一度使用した主体認証情報（パスワードなど）の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。	解説の修正
54		(1.4.1.1(1)へ移動)	2.1.1.1(2)	識別コードの管理	構成変更
55		(1.4.1.1(1)(a)へ移動)	2.1.1.1(2)(a)	行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと。	構成変更
56		(1.4.1.1(1)(a)解説へ移動)	2.1.1.1(2)(a) 解説	解説：自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、なりすまし行為であることを認識する必要がある。仮に、悪意がない行為であっても、他者の識別コードを使って情報システムを利用することは、安易に許容されてはならない。	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				例えば、何らかの障害により自己の識別コードの利用が一時的に不可能になった場合には、まず、当該情報システムを使って行おうとしている業務について、他者へ代行処理依頼することを検討すべきであり、他者の許可を得て、当該者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを用いて、情報システムを利用するということは制限されなければならない。 また、業務の継続のために、他者の識別コードを用いることが不可避の場合には、本人の事前の了解に加えて、情報システムセキュリティ管理者の了解を得ることが最低限必要である。極めて緊急性が高い場合には、他者の識別コードを利用していた期間とアクセスの内容を、事後速やかに、情報システムセキュリティ管理者に報告しなければならない。情報システムセキュリティ管理者は、その理由と利用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えるのが望ましい。 いずれの場合も、用いる識別コードの本人からの事前の許可を得ずに、その者の識別コードを用いて、情報システムを利用することは禁	

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				止されるべきである。 遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。	
57		(1.4.1.1(1)(b)へ移動)	2.1.1.1(2)(b)	行政事務従事者は、自己に付与された識別コードを他者に主体認証に用いる目的のために付与及び貸与しないこと。	構成変更
58		(1.4.1.1(1)(b)解説へ移動)	2.1.1.1(2)(b) 解説	解説：共用する識別コードについても情報システムセキュリティ管理者から各本人に個別に付与されるものであり、付与された者がそれを他者に付与、貸与してはならない。また、情報システムセキュリティ管理者が明示的に共用識別コードとしているもの以外の識別コードを、共用してはならない。 遵守事項に「主体認証に用いる目的のために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
59		(1.4.1.1(1)(c)へ移動)	2.1.1.1(2)(c)	行政事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。	構成変更
60		(1.4.1.1(1)(c)解説へ移動)	2.1.1.1(2)(c) 解説	解説：ほとんどの場合には、識別コード自体は必ずしも秘密ではないが、積極的に公開したり、公然となるような放置はしないようにすることを求める事項である。 本来、主体認証のためには、主体認証情報が用いられるが、識別コード自体も秘密にすることによって、不正に主体認証される可能性をより低くすることが可能となる。そのため、識別コードについても適切に管理することが求められる。	構成変更
61		(1.4.1.1(1)(d)へ移動)	2.1.1.1(2)(d)	行政事務従事者は、行政事務のために識別コードを利用する必要がなくなった場合は、その旨を情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、情報システムセキュリティ責任者が定めている場合は、この限りでない。	構成変更
62		(1.4.1.1(1)(d)解説へ移動)	2.1.1.1(2)(d) 解説	解説：識別コードを利用する必要がなくなった場合に、行政事務従事者自らが情報システムセキュリティ管理者へ届け出ることを求める事項である。ただし、人事異動など、大規模に識別コードの行政事務従事者が変更となる場合や、その変更を情報システムセキュリ	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				ティ管理者が行政事務従事者自らからの届出によらずして把握できる場合には、行政事務従事者自らの届出は不要とすることができる。	
63		(1.4.1.1(1)(e)へ移動)	2.1.1.1(2)(e)	行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。	構成変更
64		(1.4.1.1(1)(e)解説へ移動)	2.1.1.1(2)(e) 解説	解説：管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用することを求める事項である。 例えば、情報システムのオペレーティングシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更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。 なお、この遵守事項は、実際には繁雑な操作を必要とする場合があるため、最少特権機能が設けられている場合は、これを遵守するべきであるが、当該の情報システムで取り扱う情報の重要性などを勘案し、必要に応じて遵守事項として本事項を選択されたい。	構成変更
65		(1.4.1.1(2)へ移動)	2.1.1.1(3)	主体認証情報の管理	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
					変更
66		(1.4.1.1(2)(a)へ移動)	2.1.1.1(3)(a)	行政事務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。	構成変更
67		(1.4.1.1(2)(a)解説へ移動)	2.1.1.1(3)(a)解説	解説：行政事務従事者は、自らの主体認証情報自体の露呈や主体認証情報に関連する情報の露呈又はそれらが露呈した可能性がある場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者へ報告することを求める事項である。	構成変更
68		(1.4.1.1(2)(b)へ移動)	2.1.1.1(3)(b)	情報システムセキュリティ責任者又は情報システムセキュリティ管理者は、主体認証情報が他者に使用され、又はその危険が発生したことの報告を受けた場合には、必要な措置を講ずること。	構成変更
69		(1.4.1.1(2)(b)解説へ移動)	2.1.1.1(3)(b)解説	解説：報告を受けた者が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるログオン制限等がある。	構成変更
70		(1.4.1.1(2)(c)へ移動)	2.1.1.1(3)(c)	行政事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。	構成変更
71		(1.4.1.1(2)(c)(ア)へ移動)	2.1.1.1(3)(c)(ア)	自己の主体認証情報を他者に知られないように管理すること。	構成変更
72		(1.4.1.1(2)(c)(ア)解説へ移動)	2.1.1.1(3)(c)	解説：行政事務従事者は、例えば	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
			(ア)解説	自己の主体認証情報を内容が分かる状態で付箋に記入して貼付するようなことを行ってはならず、主体認証情報を入力する際に周囲からの盗み見に注意を払ったり、管理者を名乗って主体認証情報を聞き出す行為に注意したりする等、他者に知られないように管理すること。	変更
73		(1.4.1.1(2)(c)(イ)へ移動)	2.1.1.1(3)(c)(イ)	自己の主体認証情報を他者に教えないこと。	構成変更
74		(1.4.1.1(2)(c)(イ)解説へ移動)	2.1.1.1(3)(c)(イ)解説	解説：行政事務従事者が他者に処理代行させるために自己の主体認証情報を教示しないことを求める事項である。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関連があいまいとなる可能性があり、アクセス制御、権限管理、証跡管理その他の情報セキュリティ対策の基礎が崩壊する可能性がある。また、教示された側にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、「教えない」、「聞かない」を徹底すべきである。	構成変更
75		(1.4.1.1(2)(c)(ウ)へ移動)	2.1.1.1(3)(c)(ウ)	主体認証情報を忘却しないように努めること。	構成変更
76		(1.4.1.1(2)(c)(ウ)解説へ移動)	2.1.1.1(3)(c)(ウ)解説	解説：他者が容易に見ることができないような措置（施錠して保存する等）や、他者が見ても分から	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				ないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取ることそのものを禁ずるものではない。むしろ、忘れることのないようにもしなければならない。 本人の忘却によって主体認証情報を初期化（リセット）する場合に備えて、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用すべきである。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討することが望ましい。	
77		(1.4.1.1(2)(c)(エ)へ移動)	2.1.1.1(3)(c)(エ)	主体認証情報を設定するに際しては、容易に推測されないものにすること。	構成変更
78		(1.4.1.1(2)(c)(エ)解説へ移動)	2.1.1.1(3)(c)(エ)解説	解説：辞書に載っている単語、利用者の名前や利用者個人に関連する情報から簡単に派生させたもの等、容易に推測されるものを用いてはならない。また、使用する文字種として、数字だけでなく、アルファベットの大文字及び小文字、更に特殊記号なども織り交ぜて主体認証情報を構成することが望ましい。	構成変更
79		(1.4.1.1(2)(c)(オ)へ移動)	2.1.1.1(3)(c)	情報システムセキュリティ管理者	構成

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
			(オ)	から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。	変更
80		(1.4.1.1(2)(c)(オ)解説へ移動)	2.1.1.1(3)(c)(オ)解説	解説：定期的な変更の要求を自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達するなどの運用によって対処することでも差し支えない。	構成変更
81		(1.4.1.1(2)(d)へ移動)	2.1.1.1(3)(d)	行政事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。	構成変更
82		(1.4.1.1(2)(d)(ア)へ移動)	2.1.1.1(3)(d)(ア)	主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。	構成変更
83		(1.4.1.1(2)(d)(イ)へ移動)	2.1.1.1(3)(d)(イ)	主体認証情報格納装置を他者に付与及び貸与しないこと。	構成変更
84		(1.4.1.1(2)(d)(ウ)へ移動)	2.1.1.1(3)(d)(ウ)	主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。	構成変更
85		(1.4.1.1(2)(d)(エ)へ移動)	2.1.1.1(3)(d)(エ)	主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者又は情報システムセキュリティ管理者に返還すること。	構成変更
86		(1.4.1.1(2)(d)(エ)解説へ移動)	2.1.1.1(3)(d)(エ)解説	解説：所有による主体認証方式では、それを取得した者が正当な主体として主体認証されることにな	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				るため、他者に使用されることがないように、また、紛失などで、その可能性がある場合の報告を徹底する必要がある。異動等により主体認証情報格納装置を利用する必要がなくなった場合には、これを返却する必要がある。	
87	2.2.1.2	2.2.1.2 アクセス制御機能	2.1.1.2	2.1.1.2 アクセス制御機能	構成変更
88	2.2.1.2 趣旨	主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。 これらのことを勘案し、本項では、アクセス制御に関する対策基準として、アクセス制御機能の導入、適正なアクセス制御についての遵守事項を定める。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。	2.1.1.2 趣旨	主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。 これらのことを勘案し、本項では、アクセス制御に関する対策基準を定める。	趣旨の修正
89		(1.5.2.8(1)(a)(イ)へ移動)	2.1.1.2(1)(a)	情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。	
90		(1.5.2.8(1)(a)(イ)解説へ移動)	2.1.1.2(1)(a) 解説	解説：アクセス制御を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセス制御を行う必要性の有無を検討しなければならない。 要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。 なお、アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。 http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf	構成変更
91	2.2.1.2(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及び取扱制限に従って、アクセス制御を行うこと。	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。	表現の適正化
92	2.2.1.2(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	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		とができない場合、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)(b)の規程に基づき対策を行うこと。		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。	
93	2.2.1.3	2.2.1.3 権限管理機能	2.1.1.3	2.1.1.3 権限管理機能	構成変更
94	2.2.1.3 趣旨	主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。 これらのことを勘案し、本項では、権限管理に関する対策基準として、権限管理機能の導入、識別コードと主体認証情報の付与管理についての遵守事項を定める。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制	2.1.1.3 趣旨	主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。 これらのことを勘案し、本項では、権限管理に関する対策基準を定める。	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。			
95		(1.5.2.8(1)(a)(ウ)へ移動)	2.1.1.3(1)(a)	情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。	構成変更
96		(1.5.2.8(1)(a)(ウ)解説へ移動)	2.1.1.3(1)(a) 解説	解説：権限管理を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。 なお、アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与（発行、更新及び変更を含む。以下この項において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。	構成変更
97	2.2.1.3(1)(c)	解説：情報システムの利用を開始	2.1.1.3(1)(d)	解説：情報システムの利用を開始	解説

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
	解説	している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。 なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することは、管理者による不正な操作が発生する機会を減らし、安全性を強化することができる。	解説	している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。 なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することにより、安全性を強化することができる。	の修正
98		(1.4.1.1(3)(a)へ移動)	2.1.1.3(2)(a)	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。	構成変更
99		(1.4.1.1(3)(a)解説へ移動)	2.1.1.3(2)(a) 解説	解説：原則として、識別コードは、情報システムへアクセスする主体へ個別に付与することになる。しかしながら、情報システム上の制約や、利用状況などを考慮して、１つの識別コードを複数の主体で共用する必要がある場合には、当該情報システムごとに利用許可の判断をすることを求める事項である。	構成変更
100		(1.4.1.1(3)(b)へ移動)	2.1.1.3(2)(b)	情報システムセキュリティ責任者	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。	変更
101		(1.4.1.1(3)(b)(ア)へ移動)	2.1.1.3(2)(b)(ア)	主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続	構成変更
102		(1.4.1.1(3)(b)(イ)へ移動)	2.1.1.3(2)(b)(イ)	主体認証情報の初期配布方法及び変更管理手続	構成変更
103		(1.4.1.1(3)(b)(ウ)へ移動)	2.1.1.3(2)(b)(ウ)	アクセス制御情報の設定方法及び変更管理手続	構成変更
104		(1.4.1.1(3)(b)解説へ移動)	2.1.1.3(2)(b)(ウ)解説	解説：情報システムへアクセスする主体に対して、識別コード及び主体認証情報を付与する際の関連手続を明確に定めることを求める事項である。また、情報システムへアクセスする主体ごとに、確実にアクセス権限を設定するため、関連手続を明確に定めることを求める事項である。	構成変更
105		(1.4.1.1(3)(c)へ移動)	2.1.1.3(2)(c)	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。	構成変更
106		(1.4.1.1(3)(c)解説へ移動)	2.1.1.3(2)(c)解説	解説：アクセス権限の管理については、情報システムのセキュリティ保護上、非常に重要な役割を果たすため、権限管理を行う者を定め、厳格な運用を求める事項である。	構成変更
107	2.2.1.3(2)(a)解説	解説：情報システムにおける識別コード及び主体認証情報は、情報	2.1.1.3(2)(d)解説	解説：情報システムにおける識別コード及び主体認証情報は、情報	解説の修

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		システムを利用する許可を得た主体に対してのみ、本人確認の上で初期発行することが重要である。また、識別コード及び主体認証情報の安全な初期配布方法について求める事項である。		システムを利用する許可を得た主体に対してのみ発行することが重要である。そのため、初期発行に関する本人確認や、識別コード及び主体認証情報の初期配布方法について厳格な方法を採ることを求める事項である。	正
108	2.2.1.3(2)(f) 解説	解説：業務又は業務上の責務に即して、必要となる者に限り、当該者の業務遂行に必要となるアクセス権のみを付与することを求める事項である。	2.1.1.3(2)(i) 解説	解説：業務又は業務上の責務に即して、必要となる者に限り、当該者の業務遂行に必要となるアクセス権限のみを付与することを求める事項である。	解説の修正
109	2.2.1.3(2)(h)	権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の許可を得ること。	2.1.1.3(2)(k)	権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。	構成変更、遵守事項の修正
110	2.2.1.3(2)(h) 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、許可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。	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。	解説の修正
111	2.2.1.3(2)(i) 解説	解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。こ	2.1.1.3(2)(l) 解説	解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。こ	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		のため、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合等、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、例外措置を申請する必要がある。そして、当該申請を許可するときは、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理することが求められる。 なお、当該例外措置は、どの識別コードを誰が使用しているかを管理する ID マネジメントに係る重要事項であるため、情報セキュリティ責任者が許可・不許可を判断することが望ましい。		のため、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合など、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、例外措置を申請する必要がある。そして、当該申請を許可するときは、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理することが求められる。 なお、当該例外措置は、どの識別コードを誰が使用しているかを管理する ID マネジメントに係る重要事項であるため、情報セキュリティ責任者が許可・不許可を判断することが望ましい。	
112		(1.4.1.1(4)へ移動)	2.1.1.3(3)	識別コードと主体認証情報における代替手段等の適用	構成変更
113		(1.4.1.1(4)(a)へ移動)	2.1.1.3(3)(a)	情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった行政事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
114		(1.4.1.1(4)(a)解説へ移動)	2.1.1.3(3)(a) 解説	解説：情報システムを利用する行政事務従事者においては、何らかの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合が想定される。例えば、知識による主体認証方式であれば主体認証情報（パスワード）を忘れた場合、所有による主体認証方式であれば携帯するのを忘れた場合、指紋による主体認証方式であれば指を怪我した場合等が挙げられる。 それらの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合には、代替手段の使用に関する許可申請をすることができる。情報システムセキュリティ管理者は、その申請を受理した時には、その申請が正当な利用者からの許可申請であること及び許可申請の理由が妥当であること等を確認した上で、その必要性を判断し代替手段を提供することを求める事項である。なお、代替手段としては、例えば、当日限り有効とした暫定的な識別コード及び主体認証情報の提供や、当該情報システムから切り離された代替 PC の提供､情報システムを利用しない業務環境の提供などが想定されるが、情報システムセキュリティ管理者が情報セキュリティ保護の観点に加えて行	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				政事務従事者本人による業務執行の緊急性、効率性、利便性及び当該情報システムの可用性等も考慮して、適正な代替手段を準備しておくこと。 なお、代替手段の提供に当たっては、その申請理由と使用期間、使用者等を記録として残すことが望ましい。	
115		(1.4.1.1(4)(b)へ移動)	2.1.1.3(3)(b)	情報システムセキュリティ責任者及び情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を停止させること。	構成変更
116		(1.4.1.1(4)(a)解説へ移動)	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。	構成変更
117	2.2.1.4	2.2.1.4 証跡管理機能	2.1.1.4	2.1.1.4 証跡管理機能	構成変更

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
118	2.2.1.4 趣旨	情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。 これらのことを勘案し、本項では、証跡管理に関する対策基準として、証跡管理機能の導入、証跡の取得と保存についての遵守事項を定める。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。	2.1.1.4 趣旨	情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。 これらのことを勘案し、本項では証跡管理に関する対策基準を定める。	趣旨の修正
119	2.2.1.4(1)	証跡管理機能の導入	2.1.1.4(1)	証跡管理機能の導入	構成変更
120		(1.5.2.8(1)(a)(エ)へ移動)	2.1.1.4(1)(a)	情報システムセキュリティ責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。	構成変更
121		(1.5.2.8(1)(a)(エ)解説へ移動)	2.1.1.4(1)(a) 解説	解説：証跡管理を行う前提として、情報システムセキュリティ責任者	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				に、情報システムについて、証跡管理を行う必要性の有無を検討することを求める事項である。 情報セキュリティは、様々な原因で損なわれることがある。クラッカー等の部外者による不正アクセス、不正侵入、操作する者の誤操作又は不正操作、府省庁の内部及び外部の情報システム利用者の誤操作又は不正操作などがその原因となる。また、職務外の目的でウェブの閲覧や電子メールの送受信がなされるおそれもある。万一問題が発生した場合にはその実行者を特定する必要があり、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、以下のような管理記録	

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				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	
122	2.2.1.4(1)(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情報セキュリティ責任者が認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。	2.1.1.4(1)(b)	情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。	遵守事項の修正
123		(1.5.2.8(1)(a)(オ)へ移動)	2.1.1.4(1)(c)	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、証跡として取得する情報項目及び証跡の保存期間を定めること。	構成変更
124		(1.5.2.8(1)(a)(オ)解説へ移動)	2.1.1.4(1)(c) 解説	解説：証跡を取得する場合に、取得する情報項目及び証跡の保存期間を適切に定めることを求める事	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				項である。 以下に示す例は一般的に取得すべき基本的な情報項目であるが、限られた情報量で実効性のある証跡を取得するように設計することが重要である。 証跡に含める情報項目の例： ・事象の主体である者又は機器を示す識別コード等 ・事象の種類（ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等） ・事象の対象（アクセスした URL（ウェブアドレス）、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等） ・日付、時刻 ・成功、失敗の区別、事象の結果 ・電子メールのヘッダ情報、通信内容 ・通信パケットの内容 ・操作する者、監視する者及び保守する者等への通知の内容 また、保存期間は、１つの情報システムであっても取得する箇所や情報項目により異なることもあり得る。 情報セキュリティに関する問題を事後に追跡し、また事前に抑止するという証跡管理の目的に照らし	

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				て、保存期間を定めることになる。	
125	2.2.1.4(1)(b)	情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。	2.1.1.4(1)(d)	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、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。	遵守事項の修正
126	2.2.1.4(1)(c)	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情報セキュリティ責任者が認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。	2.1.1.4(1)(e)	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、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。	遵守事項の修正
127	2.2.1.4(1)(c) 解説	解説：不正アクセス、不正操作若しくは職務外利用又は誤操作を行った者にとって、その証跡は自己に不利益をもたらすものであることも考慮し、証跡が不当に消去、改ざんされることのないように、適切な格付を与えてこれを管理することを求める事項である。証跡の格付は、多くの場合に、機密性２情報又は機密性３情報で、要保全情報となるものと考えられる。 証跡は、訴訟において証拠として利用されることがある。その適切な取扱いを組織として定め、かつこれを遵守していることが、証跡	2.1.1.4(1)(e) 解説	解説：不正アクセス、不正操作若しくは職務外利用又は誤操作を行った者にとって、その証跡は自己に不利益をもたらすものであることも考慮し、証跡が不当に消去、改ざんされることのないように、適切な格付けを与えてこれを管理することを求める事項である。証跡の格付けは、多くの場合に、機密性２情報又は機密性３情報で、要保全情報となるものと考えられる。 証跡は、訴訟において証拠として利用されることがある。その適切な取扱いを組織として定め、かつ	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		に証拠力が認められる前提となることにも留意する必要がある。 また、証跡には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。 これらの理由で、証跡は、情報システムセキュリティ管理者を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。 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する必要があるため、アクセスできる者を制限することが重要になる。		これを遵守していることが、証跡に証拠力が認められる前提となることにも留意する必要がある。 また、証跡には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。 これらの理由で、証跡は、情報システムセキュリティ管理者を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。 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。	
128	2.2.1.4(1)(d)	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情報セキュリティ責任者が認めた情報システムにおいては、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。	2.1.1.4(1)(f)	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、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。	遵守事項の修正
129	2.2.1.4(1)(d) 解説	解説：取得した証跡を効率的かつ確実に点検及び分析し、その結果を報告するために、その作業を自動化する機能を設けることを求める事項である。 証跡は、その量が膨大になるため、	2.1.1.4(1)(f) 解説	解説：取得した証跡を効率的かつ確実に点検及び分析し、その結果を報告するために、その作業を自動化する機能を設けることを求める事項である。 証跡は、その量が膨大になるため、	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成する等により、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。		証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成するなどにより、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。	
130	2.2.1.4(1)(e) 解説	解説：情報セキュリティの侵害の可能性を示す事象が発生した場合に、迅速な対処を可能とするために、監視する者等に即時に通知する機能を設けることを求める事項である。 府省庁外からの不正侵入の可能性、府省庁における持込み PC の情報システムへの接続等、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。必要に応じ、情報システムの利用者に即時に注意を促す仕組みを設けることも考えられる。	2.1.1.4(1)(e) 解説	解説：情報セキュリティの侵害の可能性を示す事象が発生した場合に、迅速な対処を可能とするために、監視する者等に即時に通知する機能を設けることを求める事項である。 府省庁外からの不正侵入の可能性、府省庁における持込み PC の情報システムへの接続など、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。必要に応じ、情報システムの利用者に即時に注意を促す仕組みを設けることも考えられる。	解説の修正
131	2.2.1.4(2)(a)	情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、情報システムに設けられた機能を利用して、証跡を取得すること。	2.1.1.4(2)(a)	情報システムセキュリティ管理者は、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責任者が情報システムに設けた機能を利用して、証跡を記録すること。	遵守事項の修正
132	2.2.1.4(2)(a) 解説	解説：情報システムの運用中に、利用者の行動等の事象を証跡として取得することを求める事項であ	2.1.1.4(2)(a) 解説	解説：情報システムの運用中に、利用者の行動等の事象を証跡として記録することを求める事項であ	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		る。 情報システムセキュリティ管理者は、証跡を取得するために、必要な操作を行う必要がある。		る。 情報システムセキュリティ管理者は、証跡を取得するために、必要な操作を行う必要がある。	
133	2.2.1.4(2)(b)	情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。	2.1.1.4(2)(b)	情報システムセキュリティ管理者は、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、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。	遵守事項の修正
134	2.2.1.4(2)(b) 解説	解説：取得した証跡を適正に保存し、又は消去することを求める事項である。 情報システムセキュリティ管理者は、証跡の保存期間が満了するまで当該証跡を保存する必要がある。 必要な期間にわたり証跡を保存するために、当該期間に取得する証跡を全て保有できるファイル容量としたり、証跡を適宜外部電磁的記録媒体に退避したりする方法がある。 なお、法令の規定により保存期間が定められている場合には、これにも従うこと。	2.1.1.4(2)(b) 解説	解説：取得した証跡を適正に保存し、又は消去することを求める事項である。 情報システムセキュリティ管理者は、証跡の保存期間が満了するまで当該証跡を保存する必要がある。 必要な期間にわたり証跡を保存するために、当該期間に取得する証跡をすべて保有できるファイル容量としたり、証跡を適宜外部電磁的記録媒体に退避したりする方法がある。 なお、法令の規定により保存期間が定められている場合には、これにも従うこと。	解説の修正
135	2.2.1.4(2)(c)	情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できない場合又は取得できな	2.1.1.4(2)(c)	情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合	遵守事項の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		くなるおそれがある場合は、定められた対処方法に基づいて対処すること。		は、定められた対処方法に基づいて対処すること。	
136		(1.5.2.8(3)へ移動)	2.1.1.4(3)	取得した証跡の点検、分析及び報告	構成変更
137		(1.5.2.8(3)へ移動)	2.1.1.4(3)	【強化遵守事項】	構成変更
138		(1.5.2.8(3)へ移動)	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。	構成変更
139		(1.5.2.8(3)(a)へ移動)	2.1.1.4(3)(a)解説	解説：取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずることにより、情報セキュリティを維持し、あるいはその侵害を早期に検知することを求める事項である。 取得した証跡は、そのすべてを定期的に精査することは一般には困難であり、その一部を重点あるいは指標として点検及び分析することが有効である。重点項目の内容と証跡の量を定期的に点検し、その範囲で通常とは異なる状況が見られた場合に更に詳細な点検及び分析を行うことも考えられる。 証跡の点検、分析及び報告を支援	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				するための自動化機能が設けられていれば、これを利用することにより、作業を効率的かつ確実に行うことができる。 情報セキュリティの侵害が特定された場合は、復旧及び再発防止のために必要な対策を採らなければならない。	
140		(1.5.2.8(1)(a)(カ)へ移動)	2.1.1.4(4)	証跡管理に関する利用者への周知	構成変更
141		(1.5.2.8(1)(a)(カ)へ移動)	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。	構成変更
142		(1.5.2.8(1)(a)(カ)解説へ移動)	2.1.1.4(4)(a) 解説	解説：証跡の取得等について、あらかじめ情報システムセキュリティ管理者及び利用者等に対して説明を行うことを求める事項である。 取得、保存する証跡には、情報システムの管理者、操作員及び利用者等の行動に関する情報が記録される。そのため、証跡を取得、保存し、事後に参照、点検、分析する可能性があることを、利用者に説明する必要がある。なお、証跡を証拠として活用する際の正当性を高めるためにも周知することが望ましい。	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
143	2.2.1.5	2.2.1.5 保証のための機能	2.1.1.5	2.1.1.5 保証のための機能	構成変更
144	2.2.1.5 趣旨	統一管理基準及び本統一技術基準では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能によるセキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることになると考えるが、基本的な対策ではないからといって最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。 これらのことを勘案し、本項では、保証のための機能に関する対策基準を定める。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。	2.1.1.5 趣旨	本統一基準では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能による情報セキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることになると考えるが、基本的な対策ではないからといって最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。 これらのことを勘案し、本項では、保証のための機能に関する対策基準を定める。	趣旨の修正
145		(1.5.2.4(1)(a)(キ)へ移動)	2.1.1.5(1)(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについて、保証のための対	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				策を行う必要性の有無を検討すること。	
146		(1.5.2.4(1)(a)(キ)解説へ移動)	2.1.1.5(1)(a) 解説	解説：要保護情報を取り扱う情報システムについて、情報が適切な状態であることを保証するための対策の必要性の有無を検討することを求める事項である。	構成変更
147	2.2.1.5(1)(a) 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、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、2.2.1.1～2.2.1.4 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）2.2.1.1～2.2.1.4 の機能とは異なる観点での保護を高めるための機能： 2.2.1.1～2.2.1.4 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）、否認防止（Non-Repudiation）の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。 真正性の保護及び否認防止のため	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、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。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		の機能としては、例えば、電子署名及びタイムスタンプが挙げられる。 （イ）2.2.1.1～2.2.1.4 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：2.2.1.1～2.2.1.4 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。 （イ）の機能としては、例えば、侵入検知システムやネットワーク監視等が挙げられる。 また、保証のための機能は、主体認証機能等のように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遵守事項を達成することができる。		（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。	
148	2.2.1.6	2.2.1.6 暗号と電子署名（鍵管理を	2.1.1.6	2.1.1.6 暗号と電子署名（鍵管理を	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		含む)		含む)	変更
149	2.2.1.6 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、あらかじ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として、暗号化機能及び電子署名機能の導入、暗号化及び電子署名に係る管理についての遵守事項を定める。 なお、統一管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。	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。	趣旨の修正
150	2.2.1.6(2)(a) 解説	解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。 通常、付与された電子署名を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性	2.1.1.6(2)(a) 解説	解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。 通常、付与された電子署名を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		を保証するためには、府省庁の窓口での直接提供、信頼できる機関による電子証明書の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開等の方法がある。 なお、電子署名の正当性を検証するための情報又は手段については、当該電子署名が付与された情報が真正なものであることを証明する必要がある間、提供することとなる。例えば、電子署名の有効期限内にアルゴリズムの危殆化が発生し、又は有効期限を超えるため、別の電子署名を付与する場合にあっては、これら全ての電子署名の正当性を検証するための情報又は手段を提供する必要がある。		を保証するためには、府省庁の窓口での直接提供、信頼できる機関による電子証明書の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開等の方法がある。 なお、電子署名の正当性を検証するための情報又は手段については、当該電子署名が付与された情報が真正なものであることを証明する必要がある間、提供することとなる。例えば、電子署名の有効期限内にアルゴリズムの危殆化が発生し、又は有効期限を超えるため、別の電子署名を付与する場合にあっては、これらすべての電子署名の正当性を検証するための情報又は手段を提供する必要がある。	
151	2.2.1.6(2)(b) 解説	解説：様々な機関から提供されているアルゴリズムの危殆化に関する情報を適宜入手しておくことを求める事項である。 例えば、CRYPTREC を始めとする暗号技術の有識者による発表に関心を払うことが必要である。	2.1.1.6(2)(b) 解説	解説：様々な機関から提供されているアルゴリズムの危殆化に関する情報を適宜入手しておくことを求める事項である。 また、CRYPTREC による発表に関心を払うことが必要である。	解説の修正
152	2.2.2	2.2.2 情報セキュリティについての脅威	2.1.2	2.1.2 情報セキュリティについての脅威	構成変更
153	2.2.2.1	2.2.2.1 セキュリティホール対策	2.1.2.1	2.1.2.1 セキュリティホール対策	構成変更
154	2.2.2.1 趣旨	セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフ	2.1.2.1 趣旨	セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフ	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		トウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、不正プログラム感染の原因になる等、情報システム全体のセキュリティを維持する上で大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、政府の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対処は迅速かつ適切に行わなければならない。 これらのことを勘案し、本項では、セキュリティホールに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。		トウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、ウイルス感染等の原因になるなど、情報システム全体のセキュリティを維持する上で大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、政府の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対処は迅速かつ適切に行わなければならない。 これらのことを勘案し、本項では、セキュリティホールに関する対策基準を定める。	
155		(2.3.2.1(1)(c)、2.3.4.1(1)(k)に集約のため削除)	2.1.2.1(1)(b)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。	遵守事項の修正
156		(2.3.2.1(1)(c)、2.3.4.1(1)(k)に集約のため削除)	2.1.2.1(1)(b) 解説	解説：セキュリティホール対策を実施する際に電子計算機及び通信回線装置を停止する場合に、サービス提供を中断させないための措置を求める事項である。 サービス提供を中断できない情報	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				システムでは、電子計算機及び通信回線装置を冗長構成にすることで、セキュリティ対策を実施する際の可用性を高めることが必要である。	
157	2.2.2.1(1)(b) 解説	解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。 対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施すること等が挙げられる。	2.1.2.1(1)(c) 解説	解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。 対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施することなどが挙げられる。	解説の修正
158	2.2.2.1(2)(e) 解説	解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮し、対策用ファイルを信頼できる方法で入手することを求める事項である。 信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからのダウンロード又は郵送された外部電磁的記録媒体を利用して入手する方法が挙げられる。また、改ざん等について検証することができる手段があれば、これを実行する必要がある。	2.1.2.1(2)(e) 解説	解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮し、対策用ファイルを信頼できる方法で入手することを求める事項である。 信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからのダウンロード又は郵送された外部電磁的記録媒体を利用して入手する方法が挙げられる。また、改ざんなどについて検証することができる手段があれば、これを実行する必要がある。	解説の修正
159	2.2.2.2	2.2.2.2 不正プログラム対策	2.1.2.2	2.1.2.2 不正プログラム対策	構成変更
160	2.2.2.2 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	2.1.2.2 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	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		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等他者に対するセキュリティ脅威の原因となり得る。 これらのことを勘案し、本項では、不正プログラムに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。		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。	
161	2.2.2.2(1)(a) 解説	解説：動作可能なアンチウイルスソフトウェア等が存在する電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。 なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない電子計算機については、動作可能なアンチウイルスソフトウェアが存在しないため、本遵守事項は適用されない。ただし、アンチウイルスソフトウェア等が新たにサポートを開始する場合には、速やかな導入が求められることから、情報システムセキュリテ	2.1.2.2(1)(a) 解説	解説：動作可能なアンチウイルスソフトウェア等が存在する電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。 なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない電子計算機については、動作可能なアンチウイルスソフトウェアが存在しないため、本事項は適用されない。ただし、アンチウイルスソフトウェア等が新たにサポートを開始する場合には、速やかな導入が求められることから、情報システムセキュリテ	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ィ責任者は、該当する電子計算機の把握を行っておくとともに、アンチウイルスソフトウェア等に関するサポート情報に常に注意を払っておくことが望ましい。 なお、アンチウイルスソフトウェア等には、他社製品・技術だけでなく、同一社の製品でもアンチウイルスソフトウェアの他、パーソナルファイアウォールやスパイウェア対策ソフト等も含む。		ィ責任者は、該当する電子計算機の把握を行っておくとともに、アンチウイルスソフトウェア等に関するサポート情報に常に注意を払っておくことが望ましい。	
162	2.2.2.2(1)(b)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。	2.2.2.2(1)(b)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。	表現の適正化
163	2.2.2.2(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、これらは現存する全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	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	解説の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
		製品や技術を組み合わせ、どれか１つの不具合で、その環境の全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。例えば、メールサーバに導入するアンチウイルスソフトウェアと端末に導入するアンチウイルスソフトウェアを異なるパターンファイルを用いた製品にすること等が考えられる。		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。	
164	2.2.2.2(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、拡散することを防止するための対策を実施すること。	2.1.2.2(1)(d)	情報システムセキュリティ責任者は、不正プログラムが通信により拡散することを防止するための対策を実施すること。	遵守事項の修正
165	2.2.2.2(1)(d) 解説	解説：ネットワーク及び外部電磁的記録媒体を経由した感染拡大を防止することを求める事項である。ネットワークを経由した感染拡大の防止策としては、例えば、不正プログラム定義ファイル又はパッチ適用等が最新化されていない端末をネットワークに接続させない情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。また、外部電磁的記録媒体を経由した感染拡大の防止策としては、例えば、自動再生機能の無効化、外部電磁的記録媒体の電子計算機接続時の手動検索、及びア	2.1.2.2(1)(d) 解説	解説：不正プログラムが短時間かつ大規模に感染を拡大する場合には通信を利用することが多いため、その防止策の導入を求める事項である。 不正プログラム定義ファイル又はパッチ適用等が最新化されていない端末をネットワークに接続させない情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ンチウイルスソフトウェアのリアルタイム検索機能の有効化等が挙げられる。			
166	2.2.2.2(2)(a) 解説	解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。 「特段の対処が必要な場合」とは、新たな不正プログラムの存在が明らかになった後でも利用中のアンチウイルスソフトウェア等に用いる定義ファイルが配布されない等、日常から行われている不正プログラム対策では対処が困難と判断される場合が挙げられる。	2.1.2.2(2)(a) 解説	解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。 「特段の対処が必要な場合」とは、新たな不正プログラムの存在が明らかになった後でも利用中のアンチウイルスソフトウェア等に用いる定義ファイルが配布されないなど、日常から行われている不正プログラム対策では対処が困難と判断される場合が挙げられる。	解説の修正
167	2.2.2.3	2.2.2.3 サービス不能攻撃対策	2.1.2.3	2.1.2.3 サービス不能攻撃対策	構成変更
168	2.2.2.3 趣旨	インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。 このため、インターネットに接続しているサーバ装置、並びにそのアクセスに利用される通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。この対策については、ソフトウェアのセキュリティホー	2.1.2.3 趣旨	インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。また、インターネットに接続しているサーバ装置及び端末は、不正プログラム感染又は不正侵入等により、管理者が意図しないにもかかわらず他者へサービス不能攻撃を行ってしまうおそれがある。 このため、インターネットに接続	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ルを悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。 これらのことを勘案し、本項では、サービス不能攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。		しているサーバ装置、並びにそのアクセスに利用される通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。 これらのことを勘案し、サービス不能攻撃に関する対策基準を定める。	
169	2.2.2.3(1)(a) 解説	解説：電子計算機や通信回線装置が設けている機能を有効にすることを求める事項である。 対策としては、例えば、3-way handshake 時のタイムアウトの短縮、各種 Flood 攻撃への防御機能、アプリケーションゲートウェイ機能、パケットフィルタリング機能を利用すること等が挙げられる。	2.1.2.3(1)(a) 解説	解説：電子計算機や通信回線装置が設けている機能を有効にすることを求める事項である。 対策としては、サーバ装置における SYN Cookie、通信回線装置における SYN Flood 対策機能等を有効にすること等が挙げられる。	解説の修正
170	2.2.2.3(1)(b) 【強化】から【基本】へ移動	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。	2.2.2.3(1)(b)	情報システムセキュリティ責任者は、情報システムがサービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。	強化遵守事項から基本遵守事項に修正
171	2.2.2.3(1)(b) 解説 【強化】から【基本】へ移動	解説：要安定情報を取り扱う情報システムがサービス不能攻撃を受けた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害	2.1.2.3(1)(b) 解説	解説：管理する情報システムがサービス不能攻撃を受けた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバー	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		や、サーバの処理能力低下等が考えられる。このため、例えば、サービス不能攻撃を受けたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、通信回線の通信量に制限をかける等といった手段を有する情報システムを構築する必要がある。		の処理能力低下等が考えられる。このため、サービス不能攻撃を受けたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、通信回線の通信量に制限をかける等といった手段を有する情報システムを構築する必要がある。	
172	2.2.2.3(1)(c) 【強化】から【基本】へ移動	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。		（2.1.2.3(1)(c)から移動）	強化遵守事項から基本遵守事項に修正
173	2.2.2.3(1)(c) 解説 【強化】から【基本】へ移動	解説：サービス不能攻撃に関する監視対象の特定と監視方法及び監視記録の保存期間を定めることを求める事項である。 インターネットからアクセスされるサーバ装置、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるサーバ装置、通信回線装置及び通信回線を優先的に監視する必要がある。「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握、負荷の定量的な把握がある。監視方法は多種多様	2.1.2.3(1)(c) 解説	解説：サービス不能攻撃に関する監視対象の特定と監視方法及び監視記録の保存期間を定めることを求める事項である。 インターネットからアクセスされるサーバ装置、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるサーバ装置、通信回線装置及び通信回線を優先的に監視する必要がある。また、不正プログラムの感染又は不正侵入等を受けることにより、管理する電子計算機から他者にサービス不能攻撃を行ってしまうおそれがあるため、	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		であるため、適切な方法を選択する必要がある。 「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。		当該電子計算機等を監視する必要がある。 「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握、負荷の定量的な把握があり、サービス不能攻撃に利用されることに関する監視には、電子計算機からインターネットへの通信の監視のほか、電子計算機にサービス不能攻撃を行わせる命令の有無の監視がある。監視方法は多種多様であるため、適切な方法を選択する必要がある。 「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。	
174	2.2.2.3(1)(d) 【強化】から【基本】へ移動	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。		（2.1.2.3(1)(g)から移動）	強化遵守事項から基本遵守事項に修正
175	2.2.2.3(1)(d) 解説	解説：情報システムセキュリティ責任者が、電子計算機や通信回線装置に係るサービス不能攻撃の対策を実施しても、府省庁外へ接続		（2.1.2.3(1)(g)解説から移動）	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、府省庁外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備することを求める事項である。			
176	2.2.2.3(1)(e)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する対策装置を導入すること。		（2.1.2.3(1)(d)から移動）	構成変更
177	2.2.2.3(1)(e) 解説	解説：通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除し、又は低減するために必要な装置の導入を求める事項である。例えば、巧みに偽装したパケットや正規の送信元アドレスを使用した巧妙な DDoS 攻撃を抑制するには、電子計算機及び通信回線装置が持つ既存のセキュリティ対策機能に加え、サービス不能攻撃の影響を排除し、又は低減することのできる専用の対策装置の導入が挙げられる。	2.1.2.3(1)(d) 解説	解説：電子計算機及び通信回線装置における対策については、ソフトウェアのセキュリティホールを悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除し、又は低減するために必要な装置の導入を求める事項である。	解説の修正
178	2.2.2.3(1)(f) 解説	解説：大量のアクセスによるサービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合における対処を効果的に実施するた	2.1.2.3(1)(e) 解説	解説：大量のアクセスによるサービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合における対処を効果的に実施するた	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		めの事項である。 例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するために設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意すること等が挙げられる。		めの事項である。 例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するために設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意することなどが挙げられる。	
179		（2.2.2.3(1)(d)へ移動）	2.1.2.3(1)(g)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。	構成変更
180		（2.2.2.3(1)(d)解説へ移動）	2.1.2.3(1)(g) 解説	解説：情報システムセキュリティ責任者が、電子計算機や通信回線装置に係るサービス不能攻撃の対策を実施しても、府省庁外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、	構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				府省庁外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備することを求める事項である。	
181	2.2.2.3(1)(g) 解説	解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置又は代替通信回線に切り替えることにより、サービスが中断しないように、情報システムを構成することを求める事項である。 サービス不能攻撃の検知及び代替計算機等への切替えは短時間にできるようにすることが必要である。	2.1.2.3(1)(f) 解説	解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置又は代替回線に切り替えることにより、サービスが中断しないように、情報システムを構成することを求める事項である。 サービス不能攻撃の検知及び代替計算機等への切替えは短時間にできるようにすることが必要である。	解説の修正
182	2.2.2.3(2)(a) 【強化】から【基本】へ移動	情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法が定められている場合は、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。	2.1.2.3(2)(a)	情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。	強化遵守事項から基本遵守事項に修正、遵守事項の修正
183	2.2.2.4	2.2.2.4 踏み台対策	2.1.2.4	2.1.2.4 踏み台対策	構成変更
184	2.2.2.4 趣旨	インターネット等の府省庁外の通信回線に接続された情報システム	2.1.2.4 趣旨	インターネット等の府省庁外の通信回線に接続された情報システム	趣旨の修

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		は、第三者によって不正アクセスや迷惑メール配信の中継地点として、意図しない用途に使われてしまうこと、いわゆる、踏み台とされてしまうおそれがある。踏み台とされた情報システムは、府省庁外に迷惑をかけるだけにとどまらず、例えば、当該情報システムが提供していたサービスを利用者が利用できないという可用性に対する水準の低下や、府省庁内の他の情報システムに対するセキュリティ脅威の原因ともなり得る。これらを防ぐためには、府省庁が意図しない目的で府省庁の情報システムが使われないようにすることが必要である。 これらのことを勘案し、踏み台防止に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。		は、第三者によって不正アクセスや迷惑メール配信の中継地点として、意図しない用途に使われてしまうこと、いわゆる、踏み台とされてしまうおそれがある。踏み台とされた情報システムは、府省庁外に迷惑をかけるだけにとどまらず、例えば、当該情報システムが提供していたサービスを利用者が利用できないという可用性に対する水準の低下や、府省庁内の他の情報システムに対するセキュリティ脅威の原因ともなり得る。これらを防ぐためには、府省庁が意図しない目的で府省庁の情報システムが使われないようにすることが必要である。 これらのことを勘案し、踏み台防止に関する対策基準を定める。	正
185	第 2.3 部	第 2.3 部　情報システムの構成要素についての対策	第 2.2 部	第 2.2 部　情報システムの構成要素についての対策	構成変更
186	2.3.1	2.3.1　施設と環境	2.2.1	2.2.1　施設と環境	構成変更
187	2.3.1.1	2.3.1.1 電子計算機及び通信回線装置を設置する安全区域	2.2.1.1	2.2.1.1 電子計算機及び通信回線装置を設置する安全区域	構成変更
188	2.3.1.1 趣旨	電子計算機及び通信回線装置の設置環境について、悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる状況においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改	2.2.1.1 趣旨	電子計算機及び通信回線装置の設置環境について、悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる状況においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ざんが行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等のおそれもある。 これらのことを勘案し、本項では、安全区域に関する対策基準として、安全区域への立入り及び退出、訪問者及び受渡業者、電子計算機及び通信回線装置のセキュリティ確保、安全区域内のセキュリティ管理並びに災害及び障害についての遵守事項を定める。		ざんが行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等のおそれもある。 これらのことを勘案し、本項では、安全区域に関する対策基準を定める。	
189	2.3.1.1(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、本項の全ての遵守事項のうち、庁舎等の施設全体で対策が実施されている遵守事項については、当該対策を更に居室等ごと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。	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。	解説の修正
190	2.3.1.1(1)(h)	情報システムセキュリティ責任者は、安全区域への全ての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。	2.2.1.1(1)(h)	情報システムセキュリティ責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。	表現の適正化
191	2.3.1.1(2)(a)	解説：訪問者の身元を確認するた	2.2.1.1(2)(a)	解説：訪問者の身元を確認するた	解説

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
	解説	めの事項である。 確認方法としては、例えば、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。	解説	めの事項である。 確認方法としては、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。	の修正
192	2.3.1.1(3)(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。	2.2.1.1(3)(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。	表現の適正化
193	2.3.1.1(3)(a) 解説	解説：設置場所が固定された電子計算機に関して、盗難及び不正な持ち出しを防止するための事項である。 「設置及び利用場所が確定している」とは、サーバ装置及び据置き型 PC のように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。 対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠、施設からの退出時における持ち物検査等が挙げられる。 なお、重要システムを設置している場合やサーバ室に設置している複数のサーバラックの運用主体が異なる場合、サーバラックの鍵を適切に管理すること等が考えられ	2.2.1.1(3)(a) 解説	解説：設置場所が固定された電子計算機に関して、盗難及び不正な持出しを防止するための事項である。 「設置及び利用場所が確定している」とは、サーバ装置及び据置き型 PC のように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。 対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠、施設からの退出時における持ち物検査等が挙げられる。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		る。			
194	2.3.1.1(3)(c)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。	2.2.1.1(3)(c)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。	表現の適正化
195	2.3.1.1(3)(c) 解説	解説：設置場所が固定された通信回線装置に関して、盗難及び不正な持ち出しを防止するための事項である。 対策としては、基幹の通信回線装置（ファイアウォール、ルータ、レイヤ３スイッチ、レイヤ２スイッチ等）であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置（レイヤ２スイッチ等）であれば床下への埋設等が挙げられる。	2.2.1.1(3)(c) 解説	解説：設置場所が固定された通信回線装置に関して、盗難及び不正な持出しを防止するための事項である。 対策としては、基幹の通信回線装置（ファイアウォール、ルータ、レイヤ３スイッチ、レイヤ２スイッチ等）であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置（レイヤ２スイッチ等）であれば床下への埋設等が挙げられる。	解説の修正
196		(2.3.2.1(1)(d)、(2)(b)、2.3.4.1(1)(k)へ分割移動)	2.2.1.1(3)(d)	情報システムセキュリティ責任者は、行政事務従事者が離席時に電子計算機及び通信回線装置を不正操作から保護するための措置を講ずること。	遵守事項の修正
197		(2.3.2.1(1)(d)解説、(2)(b)解説、2.3.4.1(1)(k)解説へ分割移動)	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				ないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報格納装置を事務室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。	
198	2.3.1.1(4)(a)	行政事務従事者は、安全区域内において、身分証明書を他の行政事務従事者から常時視認することが可能な状態にすること。	2.2.1.1(4)(a)	行政事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。	遵守事項の修正
199	2.3.1.1(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ち出しを行うこと。	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。	表現の適正化
200	2.3.1.1(4)(b) 解説	解説：情報システムに関連する物品の持込み及び持ち出しによって生ずるリスクに対処するための事項である。 「情報システムに関連する物品」とは、安全区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電磁的記録媒体及び情報システムから出力された書面等が含まれる。	2.2.1.1(4)(b) 解説	解説：情報システムに関連する物品の持込み及び持出しによって生ずるリスクに対処するための事項である。 「情報システムに関連する物品」とは、安全区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電磁的記録媒体及び情報システムから出力された書面等が含まれる。	解説の修正
201	2.3.1.1(4)(c)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムに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ち出しに係る記録を保存すること。	2.2.1.1(4)(c)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムに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に係る記録を取得すること。	遵守事項の修正
202	2.3.1.1(4)(c)	解説：情報システムに関連する物	2.2.1.1(4)(c)	解説：情報システムに関連する物	

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
	解説	品の持込み及び持ち出しを記録し、追跡性を確保するための事項である。記録を取得する項目としては、持込み及び持ち出しを行う者の名前及び所属、日時、物品又は事由等が挙げられる。	解説	品の持込み及び持出しを記録し、追跡性を確保するための事項である。記録を取得する項目としては、持込み及び持出しを行う者の名前及び所属、日時、物品又は事由等が挙げられる。	
203	2.3.1.1(4)(e) 解説	解説：安全区域での作業を監視するための事項である。 第三者による立会いや、監視カメラの導入等が挙げられる。	2.2.1.1(4)(e) 解説	解説：安全区域での作業を監視するための事項である。 第三者による立会いや、監視カメラの導入などが挙げられる。	解説の修正
204	2.3.2	2.3.2　電子計算機	2.2.2	2.2.2　電子計算機	構成変更
205	2.3.2.1	2.3.2.1 電子計算機共通対策	2.2.2.1	2.2.2.1 電子計算機共通対策	構成変更
206	2.3.2.1 趣旨	電子計算機の利用については、不正プログラム感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい、改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、行政事務従事者の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、電子計算機に関する対策基準として、電子計算機に関する設置時、運用時及び運用終了時についての遵守事項を定める。	2.2.2.1 趣旨	電子計算機の利用については、ウイルス感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい若しくは改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、職員の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、電子計算機に関する対策基準を定める。	趣旨の修正
207	2.3.2.1(1)(c)	情報システムセキュリティ責任者	2.2.2.1(1)(c)	情報システムセキュリティ責任者	強化

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
	【強化】から【基本】へ移動	は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にする必要性を検討し、必要と判断した場合には、そのサービス提供に必要な電子計算機を冗長構成にすること。		は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にすること。	遵守事項から基本遵守事項に修正、遵守事項の修正
208	2.3.2.1(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。可用性を高めるためには、電子計算機本体だけでなく、ハードディスク等のコンポーネント単位で冗長構成にすることも考えられる。 なお、災害等を想定して冗長構成にする場合には、代替の電子計算機を遠隔地に設置することが望ましい。	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。	解説の修正
209	2.3.2.1(1)(d)	情報システムセキュリティ責任者は、行政事務従事者の離席時に、電子計算機を不正操作から保護するための措置を講ずること。		2.2.1.1(3)(d)から分離して移動	遵守事項の追加
210	2.3.2.1(1)(d) 解説	解説：行政事務従事者の離席時に、電子計算機を第三者による不正操作から保護するための事項であ		2.2.1.1(3)(d)から分離して移動	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		る。 対策としては、例えば、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報格納装置を事務室への立入りの許可の確認にも利用する方法等が考えられる。また、スクリーンのロックを設定できない電子計算機については、施錠管理可能な棚又はラック等に収納したり、キーボード、マウス及びUSBポート等を使用できないようにロックしたりする方法等が考えられる。			
211	2.3.2.1(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、不正プログラムに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。	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。	解説の修正
212	2.3.2.1(2)(b)	行政事務従事者は、離席時に電子計算機を不正操作から保護するための措置を講ずること。		2.2.1.1(3)(d)から分離して移動	遵守事項の追加
213	2.3.2.1(2)(b) 解説	解説：行政事務従事者が、離席時に電子計算機を第三者による不正操作から保護するために、スクリーンのロック、ログオフ又は施錠		2.2.1.1(3)(d)から分離して移動	解説の追加

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		管理等の実施を求める事項である。			
214	2.3.2.1(2)(c) 解説	解説：電子計算機で利用されているソフトウェアの状態を定期的に調査し、不適切な状態にある場合にその改善を図ることを求める事項である。「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。 また、「不適切な状態」とは、利用を許可されていないソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていない等の状態のことをいう。	2.2.2.1(2)(b) 解説	解説：電子計算機で利用されているソフトウェアの状態を定期的に調査し、不適切な状態にある場合にその改善を図ることを求める事項である。「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。 また、「不適切な状態」とは、利用を許可されていないソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない等の状態のことをいう。	解説の修正
215	2.3.2.1(3)(a)	情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体の全ての情報を抹消すること。	2.2.2.1(3)(a)	情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体のすべての情報を抹消すること。	表現の適正化
216	2.3.2.1(3)(a) 解説	解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電磁的記録媒体から、全ての情報を抹消することを求める事項である。 「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれが	2.2.2.1(3)(a) 解説	解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電磁的記録媒体から、すべての情報を抹消することを求める事項である。 「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれが	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ある。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電磁的記録媒体に保存されている全ての情報を適切な方法で抹消する必要がある。		ある。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電磁的記録媒体に保存されているすべての情報を適切な方法で抹消する必要がある。	
217	2.3.2.2	2.3.2.2 端末	2.2.2.2	2.2.2.2 端末	構成変更
218	2.3.2.2 趣旨	端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失による不正プログラム感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。 このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、端末に関する対策基準として、端末の設置時及び運用時についての遵守事項を定める。	2.2.2.2 趣旨	端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失によるウイルス感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。 このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、端末に関する対策基準を定める。	趣旨の修正
219	2.3.2.2(1)(e)	情報システムセキュリティ責任者は、要保護情報を取り扱うモバイル PC については、盗難防止及び盗難後の被害を軽減するための措置を定めること。	2.2.2.2(1)(e)	情報システムセキュリティ責任者は、要保護情報を取り扱うモバイル PC については、盗難を防止するための措置を定めること。	遵守事項の修正
220	2.3.2.2(1)(e) 解説	解説:モバイル PC は容易に搬出することが可能なため盗難又は紛失	2.2.2.2(1)(e) 解説	解説:モバイル PC は容易に搬出することが可能なため盗難又は紛失	誤字訂正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		に遭う可能性が高いことから、情報システムセキュリティ責任者にその対策を定めることを求める事項である。 対策としては、府省庁内においては、モバイル PC を安全区域内に設置している場合においても固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤーでつなぐことや、帰宅時に施錠できるキャビネットに保存すること、府省庁外においては、常に身近に置き目を離さないこと等が挙げられる。盗難後の被害を軽減するための具体的な措置としては、例えば、遠隔データ消去機能等が挙げられる。		に遭う可能性が高いことから、情報システムセキュリティ責任者にその対策を定めること求める事項である。 対策としては、府省庁内においては、モバイル PC を安全区域内に設置している場合においても固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤーでつなぐことや、帰宅時に施錠できるキャビネットに保存すること、府省庁外においては、常に身近に置き目を離さないこと等が挙げられる。	
221	2.3.2.2(2)(c) 解説	解説： モバイル PC で利用する電磁的記録媒体の紛失又は盗難により保存されている情報が漏えいすることを防ぐため、必要に応じて、ハードディスク、USB メモリ等に記録されている情報に対してファイル又は電磁的記録媒体全体を暗号化することを求める事項である。暗号化する方法としては、ハードディスク全体やファイルを暗号化するソフトウェアの導入や OS に標準装備されている暗号化機能の使用が挙げられる。	2.2.2.2(2)(c) 解説	解説： モバイル PC で利用する電磁的記録媒体の盗難により保存されている情報が漏えいすることを防ぐため、ハードディスク、USB メモリ等に記録されている情報に対してファイル又は電磁的記録媒体全体を暗号化する必要性を検討すること。府省庁外に持ち出す場合、紛失又は盗難等のリスクが高まるため、可能な限り暗号化する必要がある。暗号化に準ずる方法としては、秘密分散等の情報保護措置の実施が挙げられる。	解説の修正
222	2.3.2.3	2.3.2.3 サーバ装置	2.2.2.3	2.2.2.3 サーバ装置	構成変更
223	2.3.2.3	サーバ装置については、当該サー	2.2.2.3	サーバ装置については、当該サー	趣旨

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
	趣旨	バ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。 また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。政府機関が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。 このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、サーバ装置に関する対策基準として、サーバ装置の設置時及び運用時についての遵守事項を定める。	趣旨	バ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。 また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、ウイルス感染や不正侵入等を受けるリスクが高い。政府機関が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。 このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、サーバ装置に関する対策基準を定める。	の修正
224	2.3.2.3(1)(a)	情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、通信を秘匿する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、送受信される情報を秘匿するための機能を設けること。	2.2.2.3(1)(a)	情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、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、送受信される情報を暗号化するための機能を設けること。	遵守事項の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		この場合、府省庁外通信回線を経由する保守作業については、通信を秘匿するための機能を設ける必要があると判断すること。			
225	2.3.2.3(1)(a) 解説	解説：通信回線を経由してサーバ装置の保守作業を行う際のセキュリティ強化を求める事項である。 情報システムセキュリティ責任者から保守作業を許可されている者がサーバ装置へログオンして作業する場合を想定し、例えばインターネットを介してサーバ装置の保守作業を行う場合等、通信の秘匿する必要がある必要な場合には、設置時に暗号化するための機能を設け、運用時に実際の情報の暗号化を実施できるようにしておくこと等が考えられる。	2.2.2.3(1)(a) 解説	解説：通信回線を経由してサーバ装置の保守作業を行う際のセキュリティ強化を求める事項である。 情報システムセキュリティ責任者から保守作業を許可されている者がサーバ装置へログオンして作業する場合を想定し、通信の暗号化が必要な場合には、設置時に暗号化するための機能を設け、運用時に実際の情報の暗号化を実施できるようにしておく必要がある。	解説の修正
226	2.3.2.3(2)(b) 解説	解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。 サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。 ・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。 ・前回内容からの変更部分の定期的なバックアップを実施する。 なお、取得した情報を記録した電	2.2.2.3(2)(b) 解説	解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。 サーバ装置の運用状態を復元するための必要な措置には、以下のようなものがある。 ・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。 ・前回内容からの変更部分の定期的なバックアップを実施する。 なお、取得した情報を記録した電	解説の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
		磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにする。また、災害等を想定してバックアップを取得する場合には、記録媒体を遠隔地に保存することが考えられる。「定期的」とは、1 日又は 1 週ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。		磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにする。また、災害等を想定してバックアップを取得する場合には、記録媒体を遠隔地に保存することが考えられる。「定期的」とは、1 日又は 1 週ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。	
227	2.3.2.3(2)(c) 解説	解説：運用管理作業の記録を文書として残すための事項である。 それぞれの府省庁において、ある程度統一的な様式を作成する必要がある。	2.2.2.3(2)(c) 解説	解説：運用管理作業の記録を文書として残すための事項である。 各府省庁において、ある程度統一的な様式を作成する必要がある。	解説の修正
228	2.3.2.3(2)(e)	情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視すること。	2.2.2.3(2)(e)	情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。	遵守事項の修正
229	2.3.2.3(2)(e) 解説	解説：サーバ装置のセキュリティ状態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無許可のアクセス等の意図しない事象の発生を監視することである。監視の方法の例としては、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	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		チウイルスソフトウェア又はファイル完全性チェックツール等の利用が挙げられる		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。	
230	2.3.3	2.3.3　アプリケーションソフトウェア	2.2.3	2.2.3　アプリケーションソフトウェア	構成変更
231	2.3.3.1	2.3.3.1 電子メール	2.2.3.1	2.2.3.1 電子メール	構成変更
232	2.3.3.1 趣旨	電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等に電子メールを利用する行政事務従事者が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。 これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する対策基準として、電子メールの導入時及び運用時についての遵守事項を定める。	2.2.3.1 趣旨	電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等に電子メールを利用する行政事務従事者が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。 これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する対策基準を定める。	趣旨の修正
233	2.3.3.1(1)(c)	情報システムセキュリティ責任者は、電子メールの送信元について、なりすましの防止策を講ずること。			遵守事項の追加

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
234	2.3.3.1(1)(c) 解説	解説：「なりすましの防止策」には、送信ドメイン認証(SPF)（具体的には、DNS サーバへの SPF レコードの記録）、及びメールマガジンへの電子署名の添付等が挙げられる。 なお、SPF レコードを登録する際、電子メールサーバを外部委託先において運用している場合には、外部委託先のグローバル IP アドレスを自府省庁のものとして SPF レコードに登録することは、同じ IP アドレスを民間業者も共用し、なりすましのおそれがある。このため、外部委託先には、同じサーバの他の利用者によるなりすまし防止策を講じたり、政府ドメイン名を使用する機関向けに民間業者と共用しない専用の IP アドレスを割り振られた場合を除き、認められない。			解説の追加
235	2.3.3.1(2)(a)	行政事務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、それぞれの府省庁が運営し、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を利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。	2.2.3.1(2)(a)	行政事務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、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を利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。	遵守事項の修正
236	2.3.3.1(2)(a) 解説	解説：それぞれの府省庁が運営し、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	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		（以下「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、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、許可を受けている場合であっても、当該電子メールに含まれる情報の格付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違反しないようにも留意する必要がある。		「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。	
237	2.3.3.1(2)(b) 解説	解説：例えば HTML メールの表示により、偽のウェブサイト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	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		て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、本遵守事項は、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、本遵守事項は、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。		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。	
238	2.3.3.2	2.3.3.2 ウェブ	2.2.3.2	2.2.3.2 ウェブ	構成変更
239	2.3.3.2 趣旨	ウェブを利用するに当たっては、サーバにおいて、OS 等既成のソフトウェアや開発したウェブアプリケーション等の複数の要素で構成されていること、一方で、クライアントにおいてもサーバと同様に情報処理が行われていることから、様々な脅威が考えられる。	2.2.3.2 趣旨	ウェブにおいては、様々なアプリケーション、データを組み合わせた情報を送受信すること、また IP ネットワークにおいて標準的に利用されるシステムとして一般的に普及していること等の理由により、セキュリティ脅威全般に係るリスクが考えられる。これらのリ	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を組み合わせて実施することが必要である。 これらのことを勘案し、本項では、ウェブに関する対策基準として、ウェブサーバの導入、ウェブアプリケーションの開発、ウェブの運用についての遵守事項を定める。 なお、ウェブサーバの導入及び運用については、本項に加えて、2.3.2.3 にて定めたサーバ装置に係る対策基準を、また、サービス不能攻撃等のウェブにおける脅威への対策としては、2.2.2.3 にて定めた情報セキュリティについての脅威に係る対策基準を参照する必要がある。		スクを回避するためには、システムのライフサイクル全般に対して適切な対策を施すことが必要である。 これらのことを勘案し、本項では、ウェブに関する対策基準を定める。	
240	2.3.3.2(1)	ウェブサーバの導入時	2.2.3.2(1)	ウェブの導入時	構成変更
241	2.3.3.2(1)(a)	情報システムセキュリティ責任者は、情報セキュリティが確保されるよう適切にウェブサーバのセキュリティ設定をすること。適切なセキュリティ設定として、以下に挙げる事項を含む措置を講ずること。			遵守事項の集約・修正
242	2.3.3.2(1)(a)(ア)	ウェブサーバの機能を適切に制限すること。			遵守事項の集約・修正
243	2.3.3.2(1)(a)	ウェブサーバに保存された情報へ			遵守

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
	(イ)	のアクセス制限を適切に設定すること。			事項の集約・修正
244	2.3.3.2(1)(a)(ウ)	識別コードを適切に管理すること。			遵守事項の集約・修正
245	2.3.3.2(1)(a)(エ)	通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能を設けること。			遵守事項の集約・修正
246	2.3.3.2(1)(a)解説	解説：ウェブサーバの導入時の設定に関して以下の項目を適切に行うことにより、セキュリティを確保することを求める事項である。 （ア）は、ウェブサーバで提供する機能の内、不要な機能を停止又は制限することを求めている。例えば、スクリプトやファイル実行の制限や保存場所の限定、インデックス表示の禁止、ホームページ作成ツールやコンテンツマネジメントシステム(CMS)等における不要な機能の制限等が挙げられる。 （イ）は、情報の漏えいやウェブページの改ざんを防ぐために、情報へのアクセス権限を適切に設定することを求めている。例えば、ウェブコンテンツファイルへのアクセス権限は、コンテンツの作成			解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		や更新に必要な者以外に更新権を与えない、公開を想定していないファイルをウェブ公開用ディレクトリに置かない等が挙げられる。 （ウ）は、OS やアプリケーションのインストール時に、標準で作成される識別コードやテスト用に作成した識別コード等の適切な管理を求めている。これらの識別コードはブルートフォース(総当たり)攻撃の標的になるリスクがあるため、その必要性を確認して、不要なものは削除することが重要である。また、初期状態で用意されるサンプルのページ、プログラム等も削除するといった注意が必要である。 （エ）は、通信時の盗聴による第三者への情報漏えいの防止及びウェブサーバの詐称を利用者が検知できるようにするための事項である。第三者への漏えいを防止する必要のある情報には、例えば、サービスの利用者の個人情報等が挙げられる。ウェブサーバにおいてこれらを解決するための機能としては、例えば、SSL 及び TLS が挙げられる。この機能を設けることにより、通信内容の暗号化が可能になるとともに、ウェブサーバの利用者は、ウェブサーバの電子証明書を参照することでその正当性を確認することができる。			

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		なお、政府機関のウェブサーバに電子署名を付与する必要があると認めたときのSSL及びTLSに用いる電子証明書は、政府認証基盤（GPKI）で発行したものを使用することが望ましい。			
247		(削除)	2.2.3.2(1)(a)	情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。	遵守事項の集約・修正
248		(削除)	2.2.3.2(1)(a) 解説	解説：特殊文字を無害化することを求める事項である。 特殊文字は不正侵入等の攻撃に用いられるため、すべての入力されるデータに対して特殊文字列が含まれていないかを確認する必要がある。	解説の修正
249		(削除)	2.2.3.2(1)(b)	情報システムセキュリティ責任者は、ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。	遵守事項の集約・修正
250		(削除)	2.2.3.2(1)(b) 解説	解説：ウェブアプリケーション又はデータベース等から発信されるエラーメッセージ、稼動している製品名及びそのバージョン、登録されているユーザ ID 等は、攻撃を試みる者に攻撃の糸口になり得る情報を与えてしまう危険性がある。これらのことを回避するため、不必要な情報を送信しないことを求める事項である。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
251		(削除)	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。	遵守事項の集約・修正
252		(削除)	2.2.3.2(1)(c) 解説	解説：通信時に盗聴により第三者へ漏えいすることを防止するための事項である。 「通信の盗聴から保護すべき情報」とは、例えば、ウェブで提供するサービスの運営に関わる要機密情報を指し、サービスの利用者から受け取る個人情報等も含む。	解説の修正
253		(2.3.3.2(1)(b)へ移動)	2.2.3.2(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情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。	遵守事項の集約・修正
254	2.3.3.2(1)(b) 解説	解説：万が一、不正侵入等が発生した場合であっても、当該サーバから要機密情報が漏えいしないよう、被害範囲の限定を図るための事項である。 全ての利用者が利用することが想定されているデータを除き、特定の利用者のみが利用するデータ等を、ウェブサーバに保存しないことが必要である。	2.2.3.2(1)(d) 解説	解説：万が一、不正侵入等が発生した場合であっても、当該サーバから要機密情報が漏えいしないよう、被害範囲の限定を図るための事項である。 すべての利用者が利用することが想定されているデータを除き、特定の利用者のみが利用するデータ等を、ウェブサーバに保存しないことが必要である。	解説の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
255		(削除)	2.2.3.2(1)(e)	情報システムセキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。	遵守事項の集約・修正
256		(削除)	2.2.3.2(1)(e) 解説	解説：電子証明書による検証により、利用者がウェブサーバの正当性を確認できるようにウェブサーバを構築することを求める事項である。	解説の修正
257	2.3.3.2(2)	ウェブアプリケーションの開発時	2.2.3.2(2)	ウェブの運用時	構成変更
258	2.3.3.2(2)(a)	情報システムセキュリティ責任者は、情報セキュリティが適切に確保されるようにウェブアプリケーションの開発においてセキュリティ対策機能を組み込むこと。適切なセキュリティ機能として、以下に挙げる事項を含む措置を講じること。			遵守事項の集約・修正
259	2.3.3.2(2)(a) (ア)	利用者による URL の確認を妨げないこと。			遵守事項の集約・修正
260	2.3.3.2(2)(a) (イ)	主体認証と情報へのアクセス制御を適切に行うこと。			遵守事項の集約・修正
261	2.3.3.2(2)(a) (ウ)	ウェブアプリケーションが使用するファイルのパス名を限定すること。			遵守事項の集

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
					約・修正
262	2.3.3.2(2)(a)(エ)	不正な入力データを排除すること。			遵守事項の集約・修正
263	2.3.3.2(2)(a)(オ)	不正な出力データを排除すること。			遵守事項の集約・修正
264	2.3.3.2(2)(a)(カ)	安全なセッション管理を行うこと。			遵守事項の集約・修正
265	2.3.3.2(2)(a)解説	解説：ウェブアプリケーションの開発を行う場合に、以下のセキュリティ機能を実装することにより、セキュリティを確保することを求める事項である。 なお、セキュリティ機能の実装方法の詳細については、独立行政法人情報処理推進機構(IPA)による「セキュアプログラミング講座」（http://www.ipa.go.jp/security/awareness/vendor/programming/index.html）の「Web アプリケーション編」または、「安全なウェブサイトの作り方」（http://www.ipa.go.jp/security/vuln/websecurity.html）を適宜参照			解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		することが望ましい。 （ア）は、利用者が URL（ウェブアドレス）を確認できない場合、攻撃者が用意した危険なサイト（フィッシングサイト等）に誘導される可能性があることから、それを避けることを求めるものである。この対策としては、例えば、アドレスバーを隠さない、右クリックを無効にしない等が挙げられる。 （イ）は、主体認証を行うウェブアプリケーションにおいて、パスワード等の漏えいによる利用者のなりすまし防止や主体認証後の利用者のファイルへのアクセスについて適切に制御することを求めるものである。ユーザ ID とパスワードによって主体認証を行う場合、例えば、パスワードの設定時にその文字列に適切な条件を課す、利用者本人がパスワードを変更できるようにする、入力されたパスワードは隠し文字にして表示しない等の対策が挙げられる。また、利用者が設定したパスワードはハッシュ関数を用いて復元できない形にすることも重要である。ファイルへのアクセス制御については、ウェブサイトでどの主体がどの情報にアクセスする必要があるのかについて検討し、それに基づきアクセス制御を設計・実装すること			

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		が重要である。特に、主体認証後にのみ参照可能なファイルが主体認証前に参照できてしまうことがないよう、適切にアクセス制御を行うことが求められる。 （ウ）は、ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっていると、公開を想定しないファイルが参照されるリスクがあり、これを防止することを求めるものである。この対策としては、外部のパラメータからパス名を指定する仕様を排除するのが安全だが、これができない場合は、例えば、ファイルにアクセスする前に入力されたパラメータの検査を行う、ファイルのディレクトリと識別子を固定の文字列にしてアクセスする等の方法が挙げられる。 （エ）、ウェブサーバを用いて提供するサービスにおいて、利用者から文字列等の入力を受ける場合には、不当な入力データを排除することによって、バッファオーバフロー攻撃や SQL インジェクション等の攻撃を防ぐことを求めるものである。対策としては、例えば、ウェブアプリケーションへの入力を正しく定義し、不正なデータが渡されないよう、入力されたパラメータの長さや内容を検査し、無			

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		害化する機能を設ける等が挙げられる。 （オ）は、ウェブアプリケーションが出力する画面や OS の関数、SQL コマンド等の呼び出しといった出力情報に不正なデータの混入を排除することにより、クロスサイトスクリプティングや SQL インジェクション等の攻撃を防止することを求めるものである。対策としては、例えば、HTML に埋め込むデータを全て検査してエスケープ処理する、外部プログラムを呼び出す際のプログラム名、オプション、パラメータ等はできる限り固定の文字列にする等が挙げられる。また、ウェブアプリケーション又はデータベース等から発信されるエラーメッセージ、稼動している製品名及びそのバージョン、登録されているユーザ ID 等は、攻撃を試みる者に対し攻撃の糸口となり得る情報を与えてしまう危険性がある。これらのことを回避するため、不必要な情報は出力しない措置を講じることが求められる。 （カ）は、セッション管理の不備により利用者になりすましてアクセスされることを防止するため、適切なセション管理を求めるものである。対策としては、例えば、セション ID の有効期間を主体認証			

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
		直後のレスポンスからログアウトまでに限定する、推測困難なセッション ID を設定する、セッション ID を URL パラメータに格納しない、Cookie に入れる情報はセッション ID 以外に必要最小限とする、SSL を使用する Cookie は secure 属性にする等が挙げられる。			
266		(2.3.3.2(3)(a)へ移動)	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。	遵守事項の集約・修正
267		(2.3.3.2(3)(a)解説へ移動)	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 そのため、情報システムの管理者	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				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。	
268	2.3.3.2(2)(b)	情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが特定のウェブブラウザに依存しないように情報システムを構築すること。			遵守事項の集約・修正
269	2.3.3.2(2)(b) 解説	解説：万一、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても、他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にすることを求める事項である。そのためには、例えば、2 種類以上のウェブブラウザ又は同一製品の異なるバージョンで動作するように、情報システムの構築時に配慮し、その動作確認をおこなうことが考えられる。なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、正式リリース前に情報が公開されたり、プレビュー版での動作検証可能な状態にあれば、前もって利用可能かどうかを検証する等、その後に公開が想定されるバージョンにも対応できるよう、構築時に配			解説の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
		慮することが望ましい。			
270	2.3.3.2(3)(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、閲覧するウェブサイト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 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。	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 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。	解説の修正
271		(2.3.3.2(3)(b)へ移動)	2.2.3.2(2)(b)	行政事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。	遵守事項の集約・修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
272	2.3.3.2(3)(b) 解説	解説：ソフトウェアをダウンロードする場合は、電子署名により配布元の正当性を確認することを求める事項である。	2.2.3.2(2)(b) 解説	解説：ダウンロードするソフトウェアを電子署名により配布元を確認したソフトウェアに限定することを求める事項である。	解説の修正
273		(2.3.3.2(3)(c)へ移動)	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。	遵守事項の集約・修正
274		(2.3.3.2(3) (c)(ア)へ移動)	2.2.3.2(2)(c) (ア)	送信内容が暗号化されること。	遵守事項の集約・修正
275	2.3.3.2(3)(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、情報漏えいを防止するため、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。	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	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
				確認する必要がある。	
276		(2.3.3.2(3)(c)(イ)へ移動)	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。	遵守事項の集約・修正
277	2.3.3.2(3)(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、ウェブサーバの電子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ウェブサーバの電子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。	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。	解説の修正
278	2.3.3.2(3)(d)	情報システムセキュリティ責任者は、行政事務従事者が閲覧することが可能な府省庁外のウェブサイトを制限し、定期的にその見直しを行うこと。	2.2.3.2(2)(d)	情報システムセキュリティ責任者は、行政事務従事者が閲覧することが可能な府省庁外のホームページを制限し、定期的にその見直しを行うこと。	遵守事項の集約・修正
279	2.3.3.2(3)(d)解説	解説：ウェブサイトからの不適切なソフトウェアのダウンロードや私的なウェブサイトの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。 情報システムセキュリティ責任者は、制限を実施する方法として、	2.2.3.2(2)(d)解説	解説：ウェブで閲覧したホームページからの不適切なソフトウェアのダウンロードや私的なホームページの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。 情報システムセキュリティ責任者	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		ウェブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。		は、制限を実施する方法として、ウェブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。	
280	2.3.3.3	2.3.3.3 ドメインネームシステム（DNS）	2.2.3.3	2.2.3.3 ドメインネームシステム（DNS）	構成変更
281	2.3.3.3 趣旨	ドメインネームシステム（DNS：Domain Name System）は、クライアント等からの問い合わせを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うインターネットの基盤をなすサービスである。DNS の可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また DNS が提供する情報の完全性が損なわれ、誤った情報を提供した場合は、クライアント等が悪意あるサーバに接続させられる等の被害にあう可能性がある。このようなリスクを回避するためには、DNS サーバの適切な管理が必要である。 これらのことを勘案し、本項では、DNS に関する対策基準として、DNS の導入時及び運用時についての遵守事項を定める。	2.2.3.3 趣旨	ドメインネームシステム（DNS：Domain Name System）は、クライアント等からの問い合わせを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うインターネットの基盤をなすサービスである。DNS の可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また DNS が提供する情報の完全性が損なわれ、誤った情報を提供した場合は、クライアント等が悪意あるサーバに接続させられるなどの被害にあう可能性がある。 このようなリスクを回避するためには、DNS サーバの適切な管理が必要である。 これらのことを勘案し、本項では、DNS に関する対策基準を定める。	趣旨の修正
282	2.3.3.3(1)(a) 解説	解説：要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、名前解決を停止させないため	2.1.2.3(1)(a) 解説	解説：要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、名前解決を停止させないため	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		に、求められる可用性の度合いに応じた措置を求める事項である。 DNS のコンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々の DNS のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておく等、情報と情報システムに要求される可用性に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用も、冗長化による措置の例である。あるいは、悪意ある者からのサービス不能攻撃に備え、ソフトウェアや通信回線装置で適切なアクセス制御を実施しておくことも重要である。 また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。		に、求められる可用性の度合いに応じた措置を求める事項である。 DNS のコンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々の DNS のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておくなど、情報と情報システムに要求される可用性に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用も、冗長化による措置の例である。あるいは、悪意ある者からの大量アクセス等によるサービス不能攻撃に備え、ソフトウェアや通信回線装置で適切な アクセス制御を実施しておくことも重要である。 また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。	
283	2.3.3.3(1)(c)	情報システムセキュリティ責任者は、DNS のキャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。	2.2.3.3(1)(c)	情報システムセキュリティ責任者は、DNS のキャッシュサーバにおいて、府省庁外からの名前解決の要求には応じず、府省庁内からの名前解決の要求のみに回答を行うための措置を講ずること。	遵守事項の修正
284	2.3.3.3(1)(c) 解説	解説：DNS のキャッシュサーバの第三者による不正利用やキャッシュ情報の汚染等を防ぐための措置	2.2.3.3(1)(c) 解説	解説：DNS のキャッシュサーバの第三者による不正利用やキャッシュ情報の汚染等を防ぐための措置	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		を講ずることを求める事項である。キャッシュサーバにおいては、府省庁外からの名前解決の要求には応じず、府省庁内からの名前解決の要求のみに回答を行うように措置を講ずる必要がある。キャッシュサーバを動作させる場合は、サーバの設定やファイアウォール等でアクセス制御を行うことが重要である。 また、適正な名前解決の代行を維持するために、ルートヒントファイルの更新の有無を定期的に確認し、最新のものに維持する必要がある。「定期的」とは、3 ヶ月に一度程度実施することを想定している。		を講ずることを求める事項である。キャッシュサーバを動作させる場合は、サーバの設定やファイアウォール等でアクセス制御を行うことが重要である。	
285	2.3.3.3(1)(e)	情報システムセキュリティ責任者は、重要な情報システムに対し名前解決を提供する DNS サーバにおいて、コンテンツサーバによるドメイン名の情報提供時には電子署名を付与し、キャッシュサーバによる名前解決時には電子署名を検証すること。	2.3.3.3(1)(e)	情報システムセキュリティ責任者は、重要な情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、管理するドメインに関する情報に電子署名を付与すること。	遵守事項の修正
286	2.3.3.3(1)(e) 解説	解説：電子署名によって DNS のコンテンツサーバのなりすましや同サーバからの提供情報の改ざんを DNS のキャッシュサーバで検出できるようにすることを求める事項である。その対策としては、DNSSEC の利用等が挙げられる。DNSSEC は、公開鍵暗号技術を用	2.2.3.3(1)(e) 解説	解説：電子署名によって DNS サーバのなりすましや管理するドメインに関する情報の改ざんを検出することを求める事項である。対策としては、TSIG や DNSSEC の利用等が挙げられる。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		いて改ざん等を防止するため、その導入には情報の提供側である DNS のコンテンツサーバと情報の問い合わせ側である DNS のキャッシュサーバの双方に対応が必要となる。 国民等への信頼できるサービスの提供と、政府機関内の情報セキュリティ向上の観点から、政府系ドメインを管理する DNS のコンテンツサーバ、及び政府機関の DNS のキャッシュサーバに対する円滑な DNSSEC の導入が望ましい。			
287	2.3.3.3(2)(a) 解説	解説 : 複数台の DNS のコンテンツサーバが保有し管理するドメインに関する情報について、整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバの管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバの管理するドメインに関する情報も更新するといった方法が考えられる。 なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG の利用等が考えられる。	2.2.3.3(2)(a) 解説	解説 : 複数台の DNS のコンテンツサーバが保有する管理するドメインに関する情報について、整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバの管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバの管理するドメインに関する情報も更新するといった方法が考えられる。	解説の修正
288	2.3.4	2.3.4　通信回線	2.2.4	2.2.4　通信回線	構成変更

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
289	2.3.4.1	2.3.4.1 通信回線共通対策	2.2.4.1	2.2.4.1 通信回線共通対策	構成変更
290	2.3.4.1 趣旨	通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、通信回線に関する対策基準として、通信回線の構築時、運用時及び運用終了時についての遵守事項を定める。	2.2.4.1 趣旨	通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、通信回線に関する対策基準を定める。	趣旨の修正
291	2.3.4.1(1)(a) 解説	解説：情報システムセキュリティ責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。府省庁外通信回線と接続する場合のリスク軽減措置としては、例えば、ファイアウォールやウェブアプリケーションファイアウォール(WAF)等を利用する方法が考えられる。リスクを検討した結果、情報システムセキュリティ責任者は、情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするか、通信回線を構築しない等の判断を行うことが望ましい。なお、物理的に	2.2.4.1(1)(a) 解説	解説：情報システムセキュリティ責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。例えば、情報システムセキュリティ責任者は、リスクを検討した結果、情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするか、通信回線を構築しない等の判断を行うことが望ましい。	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		分割されたシステムに限らず、論理的に分割されたシステム間の通信も同様に考慮すること。(「論理的に分割されたシステム」とは、一つの情報システムのきょう体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。例えば、仮想化ソフトウェアを利用することが考えられる。なお、仮想化ソフトウェアとは、１つのハードウェアで複数のオペレーティングシステムを同時に実行する機能を有するソフトウェアをいう。以下同様。)			
292	2.3.4.1(1)(b) 解説	解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保するための事項である。例えば、通信回線の負荷に関して事前に試験等を実施し、必要となる容量及び能力を想定する等の対策が考えられる。 なお、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。	2.2.4.1(1)(b) 解説	解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保するための事項である。通信回線の負荷に関して事前に試験等を実施し、必要となる容量及び能力を想定し、それを備える。また、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。	解説の修正
293	2.3.4.1(1)(c) 解説	解説：通信回線装置としての機能や動作の明確化を行うとともに、セキュリティホール等の脅威への対処を確実なものとするために、通信回線装置が必要とするソフトウェアを定めておくことを求める事項である。	2.2.4.1(1)(c) 解説	解説：通信回線装置としての機能や動作の明確化を行うと共に、セキュリティホール等の脅威への対処を確実なものとするために、通信回線装置が必要とするソフトウェアを定めておくことを求める事項である。	解説の修正
294	2.3.4.1(1)(e)	情報システムセキュリティ責任者	2.2.4.1(1)(e)	情報システムセキュリティ責任者	遵守

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用し、アクセス制御及び経路制御を行うこと。		は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。	事項の修正
295	2.3.4.1(1)(e) 解説	解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。情報システムセキュリティ責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信を全て確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。	2.2.4.1(1)(e) 解説	解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。情報システムセキュリティ責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信をすべて確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。	解説の修正
296	2.3.4.1(1)(f)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、通信を秘匿するための機能を設けること。	2.3.4.1(1)(f)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化するための機能を設けること。	遵守事項の修正
297	2.3.4.1(1)(f) 解説	解説：通信における要機密情報を保護するための事項である。情報システムセキュリティ責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の秘匿化の必要性を検討して、運用時の暗号化に備えて構築時にそのための機能を設けておく必要がある。	2.2.4.1(1)(f) 解説	解説：通信回線を用いて送受信される要機密情報を保護するための事項である。情報システムセキュリティ責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の暗号化の必要性を検討して、運用時の暗号化に備えて構築時にそのための機能を設け	解説の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		また、通信路の秘匿化は、機密性だけでなく完全性を保護する上でも有用である。 なお、通信路の秘匿化のために、例えば、IPsec、SSL 及び TLS 等を使用することも考えられる。		ておく必要がある。	
298	2.3.4.1(1)(g) 解説	解説：通信回線に利用する物理的な回線（例えば、有線 LAN における LAN ケーブル、無線 LAN における伝搬路等の通信路）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ措置が異なることから、適切な回線を選択することを求める事項である。 回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。また、通信回線を仮想的に構築する場合には、物理的に同一の通信回線となる場合があることに注意する必要がある。	2.2.4.1(1)(g) 解説	解説：通信回線に利用する物理的な回線（例えば、有線 LAN における LAN ケーブル、無線 LAN における伝搬路等の通信路）の種別よって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ措置が異なることから、適切な回線を選択することを求める事項である。 回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。	解説の修正
299	2.3.4.1(1)(k) 【強化】から【基本】へ移動	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること必要性を検討し、必要と判断した場合には、その通信回線又は通信回線装置を冗長構成にする。	2.2.4.1(1)(l)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること。	遵守事項の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
300	2.3.4.1(1)(k) 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通信回線又は代替通信回線装置に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。	2.2.4.1(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。	解説の修正
301	2.3.4.1(2)(b) 解説	解説：運用管理作業の記録を文書として残すための事項である。 それぞれの府省庁において、ある程度統一的な様式を作成することが望ましい。	2.2.4.1(2)(b) 解説	解説：運用管理作業の記録を文書として残すための事項である。 各府省庁において、ある程度統一的な様式を作成する必要がある。	解説の修正
302	2.3.4.1(2)(c) 解説	解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。	2.2.4.1(2)(c) 解説	解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生したときに、他の情報システムを保護するための事項である。	解説の修正
303	2.3.4.1(2)(f)	情報システムセキュリティ責任者は、所管する範囲の通信回線装置が動作するために必要な全てのソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	2.2.4.1(2)(f)	情報システムセキュリティ責任者は、所管する範囲の通信回線装置が動作するために必要なすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	表現の適正化

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
304	2.3.4.1(2)(g)	情報システムセキュリティ管理者は、通信回線装置を不正操作から保護するための措置を講ずること。		（2.2.1.1(3)(d)から分離して移動）	遵守事項の修正
305	2.3.4.1(2)(g) 解説	解説：情報システムセキュリティ管理者が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、コンソールターミナル等での作業終了後の確実なログアウト、施錠可能なラック内への設置等が挙げられる。		（2.2.1.1(3)(d)から分離して移動	解説の修正
306	2.3.4.1(3)(a)	情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体の全ての情報を抹消すること。	2.3.4.1(3)(a)	情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体のすべての情報を抹消すること。	表現の適正化
307	2.3.4.2	2.3.4.2 府省庁内通信回線の管理	2.2.4.2	2.2.4.2 府省庁内通信回線の管理	構成変更
308	2.3.4.2 趣旨	府省庁内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。 これらのことを勘案し、本項では、府省庁内通信回線に関する対策基	2.2.4.2 趣旨	府省庁内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。 これらのことを勘案し、本項では、府省庁内通信回線に関する対策基	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		準として、府省庁内通信回線の構築時及び運用時、回線の対策についての遵守事項を定める。		準を定める。	
309	2.3.4.2(2)(c)解説	解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正な行為及び無許可のアクセス等の意図しない事象の発生がないかを監視することが挙げられる。	2.2.4.2(2)(c)解説	解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。	解説の修正
310	2.3.4.2(3)(a)(キ)解説	解説：VPN を利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネット VPN、IP-VPN、SSL-VPN 等が挙げられる。	2.2.4.2(3)(a)(キ)解説	解説：VPN を利用して論理的な府省庁内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネット VPN、IP-VPN、SSL-VPN、SoftEther 等が挙げられる。	解説の修正
311	2.3.4.2(3)(b)(ク)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）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信の妨害を発生させることが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	2.2.4.2(3)(b)(ク)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	解説の修正

No.	統一技術基準 遵守事項	統一技術基準	第 4 版(平成 21 年度修正) 遵守事項	第 4 版(平成 21 年度修正)	変更点
		情報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」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宜参照。		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」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宜参照。	
312	2.3.4.3	2.3.4.3 府省庁外通信回線との接続	2.2.4.3	2.2.4.3 府省庁外通信回線との接続	構成変更
313	2.3.4.3 趣旨	府省庁内通信回線と府省庁外通信回線との接続については、府省庁外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、府省庁外通信回線に送受信される情報の漏えい、改ざん又は破壊等、府省庁外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、府省庁外通信回線と接続する場合の府省庁内通信回線に関する対策基準として、府省庁内通信回線と府省庁外通信回線との接続時及び運用時についての遵守事項を定める。	2.2.4.3 趣旨	府省庁内通信回線と府省庁外通信回線との接続については、府省庁外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、府省庁外通信回線に送受信される情報の漏えい、改ざん又は破壊等、府省庁外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。 これらのことを勘案し、本項では、府省庁外通信回線と接続する場合の府省庁内通信回線に関する対策基準を定める。	趣旨の修正

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
314	2.3.4.3(1)(a)	情報システムセキュリティ責任者は、情報セキュリティ責任者の許可を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。	2.2.4.3(1)(a)	情報システムセキュリティ責任者は、情報セキュリティ責任者の承認を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。	遵守事項の修正
315	2.3.4.3(1)(a) 解説	解説：府省庁内通信回線を府省庁外通信回線と接続するとリスクの増大を招くので、情報セキュリティ責任者の判断を得ることを求める事項である。情報セキュリティ責任者は、様々なリスクを検討した上で許可の可否を判断する必要がある。	2.2.4.3(1)(a) 解説	解説：府省庁内通信回線を府省庁外通信回線と接続するとリスクの増大を招くので、情報セキュリティ責任者の判断を得ることを求める事項である。情報セキュリティ責任者は、様々なリスクを検討した上で承認の可否を判断する必要がある。	解説の修正
316	2.3.4.3(1)(b) 解説	解説：府省庁内通信回線に接続している情報システムを、府省庁外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している府省庁内通信回線から独立した通信回線として構成するか、府省庁外通信回線から切断した通信回線として構築することになる。独立した通信回線の場合でも、遵守すべき対策基準は実施する必要がある。	2.2.4.3(1)(b) 解説	解説：府省庁内通信回線に接続している情報システムを、府省庁外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している府省庁内通信回線から独立した通信回線として構成するか、府省庁外通信回線から切断した通信回線として構築することになる。独立な通信回線の場合でも、遵守すべき対策規準は実施する必要がある。	解説の修正
317	2.3.4.3(2)(a) 解説	解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。	2.2.4.3(2)(a) 解説	解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生したときに、他の情報システムを保護するための事項である。	解説の修正
318	第 2.4 部	第 2.4 部　個別事項についての対	第 2.3 部	第 2.3 部　個別事項についての対	構成

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		策		策	変更
319	2.4.1	2.4.1　その他	2.3.1	2.3.1　その他	構成変更
320	2.4.1.1	2.4.1.1 情報システムへの IPv6 技術の導入における対策	2.3.1.1	2.3.1.1 情報システムへの IPv6 技術の導入における対策	構成変更
321	2.4.1.1 趣旨	政府機関ではインターネットの規格である IPv6 通信プロトコルに対応するための取組みが進められているが、現在広く使用されている IPv4 通信プロトコルからの移行過程においては、新旧の規格が共存することから、十分に検討し、適切な措置を講じないと、情報システムのセキュリティを損なうおそれがある。また、昨今、電子計算機及び通信回線装置には IPv6 技術を利用する通信機能が標準で備わっているものが増えていることから、意図せず IPv6 技術を利用する通信機能が動作している可能性がある。このため、情報システムの IPv6 対応化計画の有無にかかわらず、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する環境を前提として、対策を講ずる必要がある。 これらのことを勘案し、本項では、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する情報システムのセキュリティ確保に関する対策基準を定める。	2.3.1.1 趣旨	政府機関ではインターネットの規格である IPv6 通信プロトコルに対応するための取組みが進められているが、現在広く使用されている IPv4 通信プロトコルからの移行過程においては、新旧の規格が共存することから、十分に検討し、適切な措置を講じないと、情報システムのセキュリティを損なうおそれがある。また、昨今、電子計算機及び通信回線装置には IPv6 技術を利用する通信機能が標準で備わっているものが増えていることから、意図せず IPv6 技術を利用する通信機能が動作している可能性がある。このため、情報システムの IPv6 対応化計画の有無にかかわらず、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する環境を前提として、対策を講ずる必要がある。 これらのことを勘案し、本項では、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する情報システムの情報セキュリティ確保に関する対策基準を定める。	趣旨の修正
322	2.4.1.1(2)(a)	情報システムセキュリティ責任者は、IPv6 通信を想定していない通	2.3.1.1(2)(a)	情報システムセキュリティ責任者は、IPv6 通信を想定していない通	表現の適

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		信回線に接続される全ての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。		信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。	正化
323	A.1.1	統一管理基準に準じる。			構成変更
324	A.1.2	統一管理基準に準じる。			構成変更
325	A.1.3	統一管理基準に準じる。			構成変更
326	A.1.4	統一管理基準に準じる。 以下は、統一技術基準で初出の用語。 【あ】 ● 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したハードウェア、ソフトウェア、ファームウェア及びそれらの組合せをいう。 【か】 ● 「強制アクセス制御 (MAC：Mandatory Access Control)」とは、主体が客体(情報、ファイル等)に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それ			構成変更

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		を保護すべき対象ではないものとすることはできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。 【た】 ● 「耐タンパー性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。 ● 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。 【な】 ● 「名前解決」とは、ドメイン名やホスト名と IP アドレスを変換することをいう。			
327	A.1.4	【ま】 ● 「無線 LAN」とは、無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a 、 802.11 b 、 802.11g 、802.11n 等が挙げられる。	A.1.4	【ま】 ● 「無線 LAN」とは、無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a 、 802.11b 、 802.11g 、Bluetooth 等が挙げられる。	解説の修正
328	A.1.4	【ら】 ● 「ルートヒントファイル」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下、「ルート DNS」という。）の情報をいう。ルートヒントファイルに			構成変更、用語解説の追

No.	統一技術基準遵守事項	統一技術基準	第 4 版(平成 21 年度修正)遵守事項	第 4 版(平成 21 年度修正)	変更点
		は、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC （Internet Network Information Center）のサイトから入手可能である。 【A～Z】 ● 「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。 「IPv6 移行機構」とは、物理的にひとつのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、電子計算機や通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性のない２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。			加