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(平成 24 年度改定)

資料１－３

新旧対照表

No.	統一技術基準（平成 24 年度改定）		現行	
1	2.1.1.2(3)	「対策レベルの設定」に係る変更点	2.1.1.2(3)	対策レベルの設定
2	2.1.1.4	2.1.1.4 情報取扱区域における管理及び利用制限		(新規追加)
3	2.1.1.4(1)	情報取扱区域		(新規追加)
4	2.1.1.4(1)	統一管理基準に準じる。		(新規追加)
5	2.1.1.4(2)	情報取扱区域のクラスの決定		(新規追加)
6	2.1.1.4(2)	統一管理基準に準じる。		(新規追加)
7	2.1.1.4(3)	情報取扱区域のクラス別管理及び利用制限		(新規追加)
8	2.1.1.4(3)	統一管理基準に準じる。		(新規追加)
9	2.1.1.4(4)	情報取扱区域の個別管理及び個別利用制限		(新規追加)
10	2.1.1.4(4)	統一管理基準に準じる。		(新規追加)
11	2.1.1.5	2.1.1.5 評価の方法	2.1.1.4	2.1.1.4 評価の方法
12	2.1.1.6	2.1.1.6 用語定義	2.1.1.5	2.1.1.5 用語定義
13	2.1.1.6	●「モバイル端末」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端末は、モバイル端末に含まれない。	2.1.1.5	●「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。
14	2.2.1.1(1)(e)(ウ)	主体認証情報を設定する時は、セキュリティ上の強度が指定以上となるように要求する機能		(新規追加)
15	2.2.1.1(1)(e)(ウ)解説	解説：安易な主体認証情報（パスワード）を設定すると、悪意のある第三者によって解読されてしまうため、必要なセキュリティ上の強度を持つようにする必要がある。 セキュリティ上の強度の指定について		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		は、次の要素を考慮する必要がある。 ・パスワードに用いる文字の種類 ・パスワードの桁数 ・パスワードの有効期間 ・アカウントをロックする方法 ・アカウントのロックを解除する方法 ・当該情報システムを利用する人数 ・当該情報システムへログインする方法 ・当該情報システムに保存される情報の格付等 なお、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムにおいては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づいてセキュリティ要件を決定する必要があるが、パスワード等のセキュリティ上の強度に関する設定例について記載があるため、参考にされたい。		
16		(削除)	2.2.1.1(1)(f) (ク)	【強化遵守事項】
17	2.2.1.1(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、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。	2.2.1.1(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、複数要素（複合）主体認証方式で主体認証を行う機能を設けること。
18	2.2.1.1(1)(g) (ア)	複数要素（複合）主体認証方式で主体認証を行う機能	2.2.1.1(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、複数要素（複合）主体認証方式で主体認証を行う機能を設けること。
19	2.2.1.1(1)(g) (イ)	ログオンした利用者に対して、前回のログオンに関する情報を通知する機能	2.2.1.1(1)(h)	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、ログオンした利用者

No.	統一技術基準（平成 24 年度改定）		現行	
				に対して、前回のログオンに関する情報を通知する機能を設けること。
20	2.2.1.1(1)(g)(ウ)	不正にログオンしようとする行為を検知し、又は防止する機能	2.2.1.1(1)(i)	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、不正にログオンしようとする行為を検知し、又は防止する機能を設けること。
21	2.2.1.1(1)(g)(ウ)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管理でき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。 なお、OS といった一般的に主体認証機能を有する機器やソフトウェア等を調達する場合には、当該機能を有する機器やソフトウェア等を選択することが望ましい。	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管理でき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。
22	2.2.1.1(1)(g)(エ)	利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能	2.2.1.1(1)(j)	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、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。
23	2.2.1.1(1)(g)(オ)	利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能	2.2.1.1(1)(k)	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、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。

No.	統一技術基準（平成 24 年度改定）		現行	
24	2.2.1.1(1)(g) (カ)	管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能	2.2.1.1(1)(l)	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、管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を設けること。
25		(削除)	2.2.1.2(1)(a)	【強化遵守事項】
26	2.2.1.2(1)(b)	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。	2.2.1.2(1)(b)	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。
27	2.2.1.2(1)(b) (ア)	利用者及び所属するグループの属性以外に基づくアクセス制御機能の追加	2.2.1.2(1)(b)	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。
28	2.2.1.2(1)(b) (イ)	強制アクセス制御機能	2.2.1.2(1)(c)	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。
29	2.2.1.2(1)(b) (イ)解説	解説：強制アクセス制御機能(MAC)の組み込みを導入することを求める事項である。 強制アクセス制御機能を備えたものとして、トラステッドＯＳやセキュアＯＳ等で実装したものもある。 なお、強制アクセス制御機能の組み込みを導入した場合、任意アクセス制御機能の組み込みができなくなるが、強制アクセス制御機能の方がより強力な機能のため、2.2.1.2(1)(a)を遵守していると考えられる。	2.2.1.2(1)(c) 解説	解説：強制アクセス制御機能(MAC)の組み込みを導入すること。 強制アクセス制御機能を備えたものとして、トラステッドＯＳやセキュアＯＳ等で実装したものもある。

No.	統一技術基準（平成 24 年度改定）		現行	
30		(削除)	2.2.1.3(1)(a)	【強化遵守事項】
31	2.2.1.3(1)(b)	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。	2.2.1.3(1)(b)	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。
32	2.2.1.3(1)(b) (ア)	最少特権機能	2.2.1.3(1)(b)	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。
33	2.2.1.3(1)(b) (イ)	主体認証情報の再発行を自動で行う機能	2.2.1.3(1)(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、主体認証情報の再発行を自動で行う機能を設けること。
34	2.2.1.3(1)(b) (ウ)	デュアルロック機能	2.2.1.3(1)(d)	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、デュアルロック機能を設けること。
35	2.2.1.3(2)(c)	権限管理を行う者は、管理者権限を持つ識別コードを付与（発行、更新及び変更を含む。以下この項において同じ。）する場合は、以下の措置を講ずること。	2.2.1.3(2)(c)	権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下この項において同じ。）すること。
36	2.2.1.3(2)(c) (ア)	業務又は業務上の責務に則した場合に限定すること	2.2.1.3(2)(c)	権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下この項において同じ。）すること。
37	2.2.1.3(2)(c) (イ)	初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更すること		(新規追加)
38	2.2.1.3(2)(c) (ウ)	初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更すること		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
39	2.2.1.3(2)(c) (エ)	ネットワークからのログインを制限すること		(新規追加)
40	2.2.1.3(2)(c) (エ)解説	解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。また、管理者権限に係る識別コード及び主体認証情報の取扱いについては、2.2.1.1 の識別コード及び主体認証情報に係る遵守事項も踏まえること。 なお、管理者権限を持つ識別コードについては、初期設定の識別コードの使用を禁止し、又は必要時以外は無効化することが望ましい。 「ネットワークからのログインを制限する」こととしては、例えば、電子証明書による端末認証、IP アドレス、MAC アドレス等により制限することが考えられる。	2.2.1.3(2)(c) 解説	解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。
41		(削除)	2.2.1.3(2)(f)	【強化遵守事項】
42	2.2.1.3(2)(g)	権限管理を行う者は、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.2.1.3(2)(g)	権限管理を行う者は、単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみを付与すること。
43	2.2.1.3(2)(g) (ア)	単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみの付与	2.2.1.3(2)(g)	権限管理を行う者は、単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみを付与すること。
44	2.2.1.3(2)(g) (イ)	識別コードをどの主体に付与したかについての記録及び当該記録を消去する場合の情報セキュリティ責任者からの事前の許可	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

No.	統一技術基準（平成 24 年度改定）		現行	
				を得ること。
45	2.2.1.3(2)(g)(ウ)	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ことの禁止	2.2.1.3(2)(i)	権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。
46		(削除)	2.2.1.4(1)(c)	【強化遵守事項】
47	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、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を情報システムに設けること。	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。
48	2.2.1.4(1)(d)(ア)	証跡の点検、分析及び報告を支援するための自動化機能	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。
49	2.2.1.4(1)(d)(イ)	情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能	2.2.1.4(1)(e)	情報システムセキュリティ責任者は、取得した証跡の内容により、情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能を情報システムに設けること。
50	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：	2.2.1.5(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：

No.	統一技術基準（平成 24 年度改定）		現行	
		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）の保護、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。 （省略）		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。 （省略）
51		(削除)	2.2.1.6(1)(d)	【強化遵守事項】
52	2.2.1.6(1)(e)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.2.1.6(1)(e)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。
53	2.2.1.6(1)(e) (ア)	暗号モジュールの交換可能なコンポーネント化による構成	2.2.1.6(1)(e)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。
54	2.2.1.6(1)(e) (イ)	複数のアルゴリズムを選択可能にする構成	2.2.1.6(1)(f)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。
55	2.2.1.6(1)(e) (ウ)	選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、	2.2.1.6(1)(g)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装

No.	統一技術基準（平成 24 年度改定）		現行	
		暗号モジュール試験及び認証制度に基づく認証を取得している製品の選択		され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。
56	2.2.1.6(1)(e)(エ)	暗号化された情報の復号又は電子署名の付与に用いる鍵の耐タンパー性を有する暗号モジュールへの格納	2.2.1.6(1)(h)	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。
57		(削除)	2.2.1.6(2)(a)	【強化遵守事項】
58	2.2.2.1(1)(a)	情報システムセキュリティ責任者は、電子計算機及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。	2.2.2.1(1)(a)	情報システムセキュリティ責任者は、電子計算機及び通信回線装置（公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。）の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。
59		(削除)	2.2.2.1(1)(a)	【強化遵守事項】
60	2.2.2.1(1)(b)	情報システムセキュリティ責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。	2.2.2.1(1)(b)	情報システムセキュリティ責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機及び通信回線装置上で採り得る対策を実施すること。
61		(削除)	2.2.2.2(1)(b)	【強化遵守事項】
62	2.2.2.2(1)(c)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせて導入する必要性の有無を検討し、必要と認めたと	2.2.2.2(1)(c)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせ、導入すること。

No.	統一技術基準（平成 24 年度改定）		現行	
		きは、当該措置を講ずること。		
63	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、拡散を防止する措置の必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	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。
64	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、及びアンチウイルスソフトウェアの自動検査機能の有効化等が挙げられる。	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。
65	2.2.2.2(2)(b) 解説	解説：1.5.2.8(1)(a)の規定による統括情報セキュリティ責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。	2.2.2.2(2)(b) 解説	解説：1.5.2.7(1)(a)の規定による統括情報セキュリティ責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。
66		(削除)	2.2.2.3(1)(d)	【強化遵守事項】
67	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	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

No.	統一技術基準（平成 24 年度改定）		現行	
		影響を排除し、又は低減する措置の必要性の有無を検討し、必要と認めたときは、対策措置を講ずること。		影響を排除し、又は低減する対策装置を導入すること。
68	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、サービス不能攻撃に係る通信の遮断等、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による対策又は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。 なお、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だけでは、サービス不能攻撃の影響を排除又は低減できない場合には、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による対策又は対策装置を導入する必要性があると判断すること。	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。
69	2.2.2.3(1)(f)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保することの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.2.2.3(1)(f)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。
70	2.2.2.3(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、サービス提供に必要な電子計算	2.2.2.3(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、サービス提供に必要な電子計算

No.	統一技術基準（平成 24 年度改定）		現行	
		機、通信回線装置又は通信回線を冗長構成にすることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。		機、通信回線装置又は通信回線を冗長構成にすること。
71		(削除)	2.2.2.4(1)(b)	【強化遵守事項】
72	2.2.2.4(1)(c)	情報システムセキュリティ責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定める必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.2.2.4(1)(c)	情報システムセキュリティ責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定めること。
73		(削除)	2.2.2.4(2)	【強化遵守事項】
74	2.2.2.4(2)(a)	情報システムセキュリティ管理者は、監視を行う情報システムについては、定められた監視方法に従って情報システムを監視し、その記録を保存すること。	2.2.2.4(2)(a)	情報システムセキュリティ管理者は、定められた監視方法に従って情報システムを監視し、その記録を保存すること。
75	2.2.2.5	標的型攻撃対策		(新規追加)
76	2.2.2.5 趣旨	標的型攻撃は、複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃である。この攻撃を完全に検知及び防御することは困難であり、かつ、端末やサーバ装置への侵入後、情報システム内に潜伏し、バックドアの設置等の攻撃を行うものもある。 府省庁で管理している情報システムの内部に不正侵入された場合、組織内部の情報が漏えいする等により、政府の社会的な信用が失われるおそれがある。また、攻撃のあった府省庁から窃取された情報が府省庁外への攻撃に利用される場合もある。 そのため、府省庁の外部と内部の境界で攻撃を検知及び防御する対策だけでなく、府省庁の情報システム内の通信及び		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		外部への通信の監視・制御等を行うことにより、情報システム内部からの攻撃の検知及び被害の拡大を防止するための対策も講ずる必要がある。 これらのことを勘案し、本項では、標的型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。		
77	2.2.2.5(1)	情報システムの構築時		(新規追加)
78	2.2.2.5(1)(a)	情報システムセキュリティ責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。		(新規追加)
79	2.2.2.5(1)(a) 解説	解説：電子計算機等に対し、情報システムの構築時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。標的型攻撃への対策は、個々のサーバ装置や端末だけではなく、情報システムのネットワーク全体の通信要件も対象となる。そして、当該通信要件に従って、アクセス制御及び経路制御を含むネットワークシステム全体の対策を講ずる必要がある。 対策としては、例えば、以下のものが挙げられる。 （ア）通信回線における対策 ・ファイアウォール等を利用した通信要件の制限 ・侵入検知システム等による不正な通信の検知・遮断 ・端末間、グループ化された電子計算機間の通信の制限 ・府省庁内通信回線上の端末から府省庁外通信回線への通信はプロキシを経由		(新規追加)

No.	統一技術基準（平成 24 年度改定）	現行
	させる等の経路制御等 （イ）端末及びサーバ装置共通の対策 ・管理者権限を持つ識別コードの個別の付与（管理者権限を持つ既定の識別コードの付与の禁止又は必要時以外の無効化） ・管理者権限を持つ識別コードの業務に必要な権限のみの付与 ・指定回数以上の主体認証情報の誤入力後の、一定期間の当該識別コードの無効化 ・主体認証情報を設定する時の、セキュリティ上の強度が指定以上となるように要求する機能の設置 ・アンチウイルスソフトウェア等の導入 ・不正プログラム定義ファイル利用型アンチウイルスソフトウェアとふるまい検知型アンチウイルスソフトウェアの併用 ・不正プログラムの自動検査機能の有効化 ・セキュリティホールの対処 ・不要なサービスの削除 ・不審なプログラムの実行禁止 ・許可していない外部電磁的記録媒体及び端末の接続制限 ・送信ドメイン認証等を利用した、受信した電子メールのなりすましの有無の確認 ・ファイルの暗号化等 （ウ）端末における対策 ・パーソナルファイアウォールの導入等 （エ）サーバ装置における対策 ・重要な情報を保存しているサーバ装置へのログイン可能な端末の制限	

No.	統一技術基準（平成 24 年度改定）		現行	
		・重要な情報を保存しているサーバ装置上のセキュリティ状態の監視 等 なお、不正プログラムの自動検査機能の有効化といった不正プログラム感染防止のための日常的実施事項については 1.5.2.8、セキュリティホールへの対処といったセキュリティホールについての対策については 2.2.2.1、アンチウイルスソフトウェア等の導入といった不正プログラム対策については 2.2.2.2、サーバ装置にログイン可能な端末の制限や不要なサービスの削除といったサーバ装置や端末に関する対策については 2.3.2.1～2.3.2.3、電子メールに関する対策については 2.3.3.1 及びファイアウォールや侵入検知システム等の導入といった通信回線に関する対策については 2.3.4.1～2.3.4.3 を参照すること。		
80	2.2.2.5(1)(b)	情報システムセキュリティ責任者は、インターネット等の府省庁外の通信回線に接続される情報システムについて標的型攻撃に利用されることを防止するための措置を講ずること。		（新規追加）
81	2.2.2.5(1)(b) 解説	解説：インターネット等の府省庁外の通信回線に接続される電子計算機等に対し、標的型攻撃に利用されることへの対処の実施を求める事項である。 対策としては、送信ドメイン認証を利用した送信する電子メールの送信元ドメイン名のなりすまし防止、政府ドメイン名の利用及び府省庁外に提供するソフトウェア等への電子証明書の付与、当該電子計算機が標的型攻撃に利用されているか否かの監視等が挙げられる。		（新規追加）

No.	統一技術基準（平成 24 年度改定）		現行	
		なお、府省庁外に提供するソフトウェア等への電子証明書の付与といった府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する対策については 1.5.2.6、ドメイン名の使用に関する対策については 1.5.2.7 当該電子計算機の監視といった踏み台対策については 2.2.2.4 及び電子メールに関する対策については 2.3.3.1 を参照すること。		
82	2.2.2.5(2)	情報システムの運用時		(新規追加)
83	2.2.2.5(2)(a)	情報システムセキュリティ責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。		(新規追加)
84	2.2.2.5(2)(a) 解説	解説：電子計算機等に対し、情報システムの運用時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。 対策としては、例えば、以下のものが挙げられる。 （ア）通信回線における対策 ・府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容の監視 ・府省庁内通信回線上の電子計算機同士で送受信される通信内容の監視 ・アンチウイルスソフトウェア等で検出されないボットの通信の監視等 （イ）端末及びサーバ装置共通の対策 ・アンチウイルスソフトウェア等における不正プログラム定義ファイルの最新の状態の維持 ・定期的な全ての電子ファイルに対する不正プログラムの有無の確認 ・セキュリティホールに関連する情報の収集及びリスク分析した上での対策実		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		施 ・ログの取得及び解析等 （ウ）その他 ・標的型攻撃に関する訓練の実施 ・送信ドメイン認証を利用した、送信する電子メールの送信元ドメイン名のなりすまし防止等 なお、不正プログラム定義ファイルの最新の状態の維持や定期的な全ての電子ファイルに対する不正プログラムの有無の確認といった不正プログラム感染防止のための日常的実施事項については 1.5.2.8、セキュリティホールに関する情報の収集といったセキュリティホールに関する対策については 2.2.2.1、電子メールに関する対策については 2.3.3.1 及び通信内容の監視といった通信回線に関する対策については 2.3.4.2 を参照のこと。		
85	2.3.1.1	情報取扱区域のクラス別管理及び利用制限	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
86	2.3.1.1 趣旨	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設置環境にある場合においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざん等が行われるおそれがある。また、その他にも、設置環境に関する脅威としては、自然災害の発生による情報システムの損傷や情報の紛失等が発生するおそれもある。 このように施設全体や区域ごとに様々な脅威が考えられるため、それぞれの区域に応じた管理と想定される利用形態に応じた情報の取扱いを行う必要がある。	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

No.	統一技術基準（平成 24 年度改定）		現行	
		これらのことを勘案し、本項では、情報取扱区域のクラス別管理及び利用制限の対策基準として、立ち入る者を制限するための管理対策、立ち入る者を許可する際の管理対策、訪問者がある場合の管理対策、設置する設備の管理対策、作業がある場合の管理対策、立ち入る者を制限するための利用制限対策、物品の持込み、持ち出し及び利用についての利用制限対策、荷物の受渡しについての利用制限対策並びに災害及び障害への対策に関する遵守事項を定める。		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。
87	2.3.1.1(1)	立ち入る者を制限するための管理対策	2.3.1.1(1)	立入り及び退出の管理
88	2.3.1.1(1)(a)	区域情報セキュリティ責任者は、立ち入る者を制限するための管理対策として、以下の事項について、別表 1 に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。		(新規追加)
89	2.3.1.1(1)(a) (ア)	不審者を立ち入らせない措置	2.3.1.1(1)(a)	情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。
90	2.3.1.1(1)(a) (ア)解説	解説：要管理対策区域への不審者の立入りを防止し、要管理対策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、要管理対策区域の所在の表示の制限等が挙げられる。	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。

No.	統一技術基準（平成 24 年度改定）		現行	
91		(削除)	2.3.1.1(1)(b)	【強化遵守事項】
92	2.3.1.1(1)(a) (イ)	要保護情報を取り扱う情報システムについては、物理的に隔離し、立入り及び退出を管理するための措置	2.3.1.1(1)(b)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、安全区域を物理的に隔離し、立入り及び退出を管理するための措置を講ずること。
93	2.3.1.1(1)(a) (イ)解説	解説：電子計算機及び通信回線装置が設置された区域を、物理的隔離及び立入り及び退出の管理により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、壁、施錠可能な扉、パーティション等で囲むことで区域を隔離し、当該区域が無人になる際には扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。なお、要管理対策区域では、扉を開放したまま無人の状態にしてはならない。	2.3.1.1(1)(b) 解説	解説：要保護情報を取り扱う情報システムを構成する電子計算機及び通信回線装置が設置された安全区域を、物理的隔離及び立入り及び退出の管理により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、壁、施錠可能な扉、パーティション等で囲むことで安全区域を隔離し、安全区域が無人になる際には扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。安全区域の扉を開放したまま無人の状態にしてはならない。
94	2.3.1.1(2)	立ち入る者を許可する際の管理対策		(新規追加)
95	2.3.1.1(2)(a)	区域情報セキュリティ責任者は、立ち入る者を許可する際の管理対策として、以下の事項について、別表 1 に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。		(新規追加)
96	2.3.1.1(2)(a) (ア)	要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置	2.3.1.1(1)(c)	情報システムセキュリティ責任者は、安全区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。
97	2.3.1.1(2)(a) (ア)解説	解説：要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。	2.3.1.1(1)(c) 解説	解説：安全区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。

No.	統一技術基準（平成 24 年度改定）		現行	
		なお、立入りを許可された者であるかの確認のために主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずること等が望ましい。		なお、立入りを許可された者であるかの確認のために主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずること等が望ましい。
98	2.3.1.1(2)(a)(イ)	要管理対策区域から退出する者が立入りを許可された者であるかの確認を行うための措置	2.3.1.1(1)(d)	情報システムセキュリティ責任者は、安全区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。
99	2.3.1.1(2)(a)(ウ)	立入りを許可された者が、立入りを許可されていない者を要管理対策区域へ立ち入らせ、及び当該区域から退出させない措置	2.3.1.1(1)(e)	情報システムセキュリティ責任者は、立入りを許可された者が、立入りを許可されていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。
100	2.3.1.1(2)(a)(ウ)解説	解説：要管理対策区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。 対策としては、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。	2.3.1.1(1)(e)解説	解説：安全区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。 対策としては、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。
101	2.3.1.1(2)(a)(エ)	継続的に立ち入る者を許可する手続の整備	2.3.1.1(1)(f)	情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を許可する手続を整備すること。また、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載するための文書を整備すること。
102	2.3.1.1(2)(a)(エ)解説	解説：文書を整備することで、要管理対策区域へ継続的に立ち入る者を把握するための事項である。立入期間については、例えば、月又は年単位といった期間が考えられる。 なお、文書には、その者の氏名、所属、立入許可日、立入期間及び許可事由を含	2.3.1.1(1)(f)解説	解説：文書を整備することで、安全区域へ継続的に立ち入る者を把握するための事項である。

No.	統一技術基準（平成 24 年度改定）		現行	
		む事項を記載すること。		
103	2.3.1.1(2)(a)(オ)	継続的に立入りを許可された者に変更がある場合の手続の整備	2.3.1.1(1)(g)	情報システムセキュリティ責任者は、安全区域へ立入りを許可された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。
104	2.3.1.1(2)(a)(オ)解説	解説：立入りを許可された者に変更がある場合に変更手続をとることで、継続的に立ち入る者を把握するための事項である。変更の手続きには、変更の内容を前事項の文書へ反映することが挙げられる。 また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。	2.3.1.1(1)(g)解説	解説：変更の内容を前事項の文書へ反映することで安全区域へ継続的に立ち入る者を把握するための事項である。 また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。
105	2.3.1.1(2)(a)(カ)	全ての者の要管理対策区域へ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	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。
106	2.3.1.1(2)(a)(カ)解説	解説：要管理対策区域への立入り及び当該区域からの退出の記録、監視を行い、区域のセキュリティが侵害された場合に追跡することができるようにするための事項である。 「記録し及び監視する」とは、警備員又は監視カメラ等による記録及び監視のほか、要管理対策区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。	2.3.1.1(1)(h)解説	解説：安全区域への立入り及び当該区域からの退出の記録、監視を行い、安全区域のセキュリティが侵害された場合に追跡することができるようにするための事項である。 「記録し及び監視する」とは、警備員又は監視カメラ等による記録及び監視のほか、安全区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。
107	2.3.1.1(3)	訪問者がある場合の管理対策	2.3.1.1(2)	訪問者及び受渡業者の管理
108		(削除)	2.3.1.1(2)	【強化遵守事項】
109	2.3.1.1(3)(a)	区域情報セキュリティ責任者は、訪問者がある場合の管理対策として、以下の事		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。		
110	2.3.1.1(3)(a)(ア)	訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置	2.3.1.1(2)(a)	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。
111	2.3.1.1(3)(a)(イ)	訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置	2.3.1.1(2)(b)	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。
112	2.3.1.1(3)(a)(ウ)	訪問相手の行政事務従事者が訪問者の要管理対策区域への立入りについて審査するための手続の整備	2.3.1.1(2)(c)	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の行政事務従事者が訪問者の安全区域への立入りについて審査するための手続を整備すること。
113	2.3.1.1(3)(a)(ウ)解説	解説：訪問者の要管理対策区域への立入りについて、訪問相手の行政事務従事者が審査するための手続を整備することを求める事項である。 手続としては、「警備員等が訪問相手の行政事務従事者に連絡し、訪問者の立入りについて審査する」、「訪問相手の行政事務従事者が、区域との境界線まで迎えに行き審査する」等の方法が挙げられる。なお、警備員等に対しては、必要に応じ、立入りの制限等について予め周知しておくこと等が考えられる。	2.3.1.1(2)(c)解説	解説：訪問者の安全区域への立入りについて、訪問相手の行政事務従事者が審査するための手続を整備することを求める事項である。 手続としては、「警備員等が訪問相手の行政事務従事者に連絡し、訪問者の立入りについて審査する」、「訪問相手の行政事務従事者が、安全区域との境界線まで迎えに行き審査する」等の方法が挙げられる。
114	2.3.1.1(3)(a)(エ)	訪問者の立ち入る区域を制限するための措置	2.3.1.1(2)(d)	情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。

No.	統一技術基準（平成 24 年度改定）		現行	
115	2.3.1.1(3)(a) (エ)解説	解説：訪問者が許可されていない要管理対策区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。	2.3.1.1(2)(d) 解説	解説：訪問者が許可されていない区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。
116	2.3.1.1(3)(a) (オ)	訪問相手の行政事務従事者による訪問者に付き添う措置	2.3.1.1(2)(e)	情報システムセキュリティ責任者は、安全区域内において訪問相手の行政事務従事者が訪問者に付き添うための措置を講ずること。
117	2.3.1.1(3)(a) (オ)解説	解説：訪問者が許可されていない要管理対策区域へ立ち入らないように行政事務従事者が監視することを求める事項である。	2.3.1.1(2)(e) 解説	解説：訪問者が許可されていない区域へ立ち入らないように行政事務従事者が監視することを求める事項である。
118	2.3.1.1(3)(a) (カ)	訪問者と継続的に立入りを許可された者とを外見上判断できる措置	2.3.1.1(2)(f)	情報システムセキュリティ責任者は、訪問者と継続的に立入りを許可された者とを外見上判断できる措置を講ずること。
119	2.3.1.1(3)(a) (カ)解説	解説：継続的に立入りを許可された者と訪問者を区別するための事項である。 これにより、許可されていない要管理対策区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。	2.3.1.1(2)(f) 解説	解説：継続的に立入りを許可された者と訪問者を区別するための事項である。 これにより、許可されていない区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。
120	2.3.1.1(4)	設置する設備の管理対策		(新規追加)
121		(削除)	2.3.1.1(3)	電子計算機及び通信回線装置のセキュリティ確保
122		(削除)	2.3.1.1(3)(a)	【強化遵守事項】
123	2.3.1.1(4)(a)	区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、別表１に従って、クラスの区分に応じて、設置及び利用場所が確定している	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

No.	統一技術基準（平成 24 年度改定）		現行	
		電子計算機及び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。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。		の不正な持ち出しを防止するための措置を講ずること。
124	2.3.1.1(4)(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る。 通信回線装置に係る対策としては、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又は施錠できる場所への機器設置等が挙げられる。なお、府省庁外通信回線と府省庁内通信回線を結ぶルータを回線事業者が所有している場合は、契約等において不正な持ち出しを防止するための措置を講ずるよう	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る。

No.	統一技術基準（平成 24 年度改定）		現行	
		求めることなどが考えられる。		
125	2.3.1.1(4)(b)	区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置の設置に係る管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。		(新規追加)
126	2.3.1.1(4)(b) (ア)	電子計算機及び通信回線装置を設置する情報取扱区域を物理的に隔離するための措置	2.3.1.1(3)(b)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。
127	2.3.1.1(4)(b) (ア)解説	解説：電子計算機及び通信回線装置を設置する情報取扱区域が隣接する低いクラスと隔離されないことにより、安全性が確保できないことを防ぐための措置を求める事項である。	2.3.1.1(3)(b) 解説	解説：他の情報システムと共用の安全区域に設置していることにより安全性が確保できない場合に、安全区域を共用せずに物理的に隔離することを求める事項である。
128		(2.3.1.1(4)(a)へ統合)	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。
129		(2.3.1.1(4)(a)解説へ統合)	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。

No.	統一技術基準（平成 24 年度改定）		現行	
130	2.3.1.1(4)(b)(イ)	電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置	2.3.1.1(3)(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、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。
131	2.3.1.1(4)(b)(ウ)	情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置	2.3.1.1(3)(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情報システムについては、情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。
132	2.3.1.1(4)(b)(エ)	情報システムから放射される電磁波による情報漏えい対策の措置	2.3.1.1(3)(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、電磁波による情報漏えい対策の措置を講ずること。
133	2.3.1.1(5)	作業がある場合の管理対策		(新規追加)
134	2.3.1.1(5)(a)	区域情報セキュリティ責任者は、別表 1 に従って、クラスの区分に応じて、要管理対策区域内での作業を監視するための措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。	2.3.1.1(4)(e)	情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。
135	2.3.1.1(5)(a)解説	解説：要管理対策区域内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。	2.3.1.1(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。
136	2.3.1.1(6)	立ち入る者を制限するための利用制限対策	2.3.1.1(4)	安全区域内のセキュリティ管理
137		(削除)	2.3.1.1(4)(a)	【強化遵守事項】
138	2.3.1.1(6)(a)	行政事務従事者は、要管理対策区域内において、行政事務従事者であることを常時視認することが可能な状態にすること。	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。
139	2.3.1.1(6)(a)解説	解説：要管理対策区域に立ち入っている者が行政事務従事者であることを外見	2.3.1.1(4)(a)解説	解説：安全区域への立入りを許可されていることを外見上判断できるようにす

No.	統一技術基準（平成 24 年度改定）		現行	
		上判断できるようにするために、身分証明書を着衣上に掲示すること等により常時視認できる状態にすることを求める事項である。		るための事項である。
140	2.3.1.1(7)	物品の持込み、持ち出し及び利用についての利用制限対策		(新規追加)
141	2.3.1.1(7)(a)	区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムに関連する物品の持込み及び持ち出しに係る利用制限対策として、以下の事項について、別表 2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。		(新規追加)
142	2.3.1.1(7)(a) (ア)	情報システムに関連する物品の持込み及び持ち出しを行う措置	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。
143	2.3.1.1(7)(a) (ア)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、要管理対策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。	2.3.1.1(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。
144	2.3.1.1(7)(a) (イ)	情報システムに関連する物品の持込み及び持ち出しに係る記録の保存	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。
145	2.3.1.1(7)(a) (ウ)	情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録	2.3.1.1(4)(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

No.	統一技術基準（平成 24 年度改定）		現行	
		装置（音声、映像及び画像を記録するものを含む。）の要管理対策区域への持込みについての制限		いては、情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。
146	2.3.1.1(7)(b)	行政事務従事者は、撮影又は録音する場合は、別表 2 に従って、クラスの区分に応じて、区域情報セキュリティ責任者に撮影又は録音の許可を得、又は届け出ること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。		(新規追加)
147	2.3.1.1(7)(b) 解説	解説：動画及び写真の撮影並びに音声の録音に係る許可を得、又は届け出ることを求める事項である。 許可又は届出先となる主体は、当該区域を管理する区域情報セキュリティ責任者となるが、許可又は届出の窓口は担当の行政事務従事者が行うことが考えられる。		(新規追加)
148	2.3.1.1(8)	荷物の受渡しについての利用制限対策		(新規追加)
149	2.3.1.1(8)(a)	区域情報セキュリティ責任者は、受渡業者と物品の受渡しを行う際の対策として、別表 2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。	2.3.1.1(2)(g)	情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。 (ア)安全区域外で受渡しを行うこと。 (イ)業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、記録媒体に触れることができない場所に限定し、行政事務従事者が立ち会うこと。
150	2.3.1.1(8)(a) 解説	解説：物品の受渡しを行う業者が要管理対策区域内に立ち入ることを制限するための事項である。 制限する措置としては、受渡しが認めら	2.3.1.1(2)(g) 解説	解説：安全区域内の行政事務従事者と物品の受渡しを行う業者の立入りを制限するための事項である。「記録媒体」には電磁的記録媒体及び情報システムか

No.	統一技術基準（平成 24 年度改定）		現行	
		れる区域の決定並びに受渡しが認められない区域で、受渡しが必要な場合は、当該業者が該当区域内の電子計算機、通信回線装置及び記録媒体に触れることができない場所に限定し、行政事務従事者が立ち会うようにすることが考えられる。「記録媒体」には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の非電磁的な媒体が含まれる。		ら出力された書面等の非電磁的な媒体が含まれる。
151		(削除)	2.3.1.1(5)	【強化遵守事項】
152	2.3.1.1(9)(a)	区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。	2.3.1.1(5)(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。
153	2.3.1.1(9)(a) 解説	解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。 対策としては、例えばサーバラックの利用のほか、 ・ハロゲン化物消火設備 ・無停電電源装置 ・自家発電装置 ・空調設備 ・耐震又は免震設備 ・非常口及び非常灯 等の設置又は確保が挙げられる。	2.3.1.1(5)(a) 解説	解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。 対策としては、サーバラックの利用のほか、ハロゲン化物消火設備、無停電電源装置等の設備、空調設備、耐震又は免震設備、非常口及び非常灯等の設置又は確保が挙げられる。
154	2.3.1.1(9)(b)	区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、要管理対策区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。	2.3.1.1(5)(b)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、安全区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

No.	統一技術基準（平成 24 年度改定）		現行	
155	2.3.1.1(9)(b) 解説	解説：作業する者が災害等により要管理対策区域内に設置された電子計算機及び通信回線装置に近づくことができない場合に、作業する者の安全性を確保した上で電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。	2.3.1.1(5)(b) 解説	解説：作業する者が災害等により安全区域内に設置された電子計算機及び通信回線装置に近づくことができない場合に、作業する者の安全性を確保した上で電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。
156	2.3.2.1(1)(b)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機を要管理対策区域内に設置すること。ただし、モバイル端末について情報セキュリティ責任者の承認を得た場合は、この限りでない。	2.3.2.1(1)(b)	情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置すること。ただし、モバイル PC について情報セキュリティ責任者の承認を得た場合は、この限りでない。
157	2.3.2.1(1)(e)	情報システムセキュリティ責任者は、電子計算機で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。		(新規追加)
158	2.3.2.1(1)(e) 解説	解説：多様なソフトウェアを利用することによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、電子計算機で利用するソフトウェアを制限することを求める事項である。		(新規追加)
159		(削除)	2.3.2.1(2)(b)	【強化遵守事項】
160	2.3.2.1(2)(c)	行政事務従事者は、電子計算機で利用を禁止するソフトウェアに定められたものを利用しないこと。また、電子計算機で利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。		(新規追加)
161	2.3.2.1(2)(c) 解説	解説：多様なソフトウェアを実行することによりセキュリティホール等の脅威が増大することから、利用を認めるソフトウェアに定められたもの以外のソフ		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		トウェアの利用を制限する事項である。利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、承認を得る必要がある。情報システムセキュリティ責任者は、利用承認の申請を受け付けたソフトウェアについて、引き続き利用を認める場合には、利用を認めるソフトウェアのリストに追加し、引き続き利用を禁止する場合には、利用を禁止するソフトウェアのリストに追加することで、一つのソフトウェアにつき最低１回の手続きで済ませることができる。		
162	2.3.2.1(2)(d)	情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されている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電子計算機を検出等した場合には、当該不適切な状態の改善を図る必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.3.2.1(2)(c)	情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されている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電子計算機を検出した場合には、当該不適切な状態の改善を図ること。
163	2.3.2.1(2)(d) 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。ただし、サーバ装置において利用を認めるソフトウェアに定められたもの以外のソフトウェアが稼働している場合には、当該ソフトウェアを停止し、又は削除する必要がある。また、サーバ装置において利用を認めるソフトウェアに定められたものであっても、利用しない機能については無効化する必要がある。 「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	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。

No.	統一技術基準（平成 24 年度改定）		現行	
		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。		
164		(2.3.2.1(1)(e)へ移動)	2.3.2.2(1)(a)	情報システムセキュリティ責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙し、又は両者を併用することができる。
165		(2.3.2.1(1)(e)解説へ移動)	2.3.2.2(1)(a) 解説	解説：多様なソフトウェアを利用することによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、端末で利用するソフトウェアを制限することを求める事項である。
166	2.3.2.2(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モバイル端末については、要管理対策区域外で使われる際にも、要管理対策区域で利用される端末と同等の保護手段が有効に機能するように構成すること。	2.3.2.2(1)(b)	情報システムセキュリティ責任者は、要保護情報を取り扱うモバイル PC については、府省庁外で使われる際にも、府省庁内で利用される端末と同等の保護手段が有効に機能するように構成すること。
167	2.3.2.2(1)(a) 解説	解説：要管理対策区域外で利用されるモバイル端末は、要管理対策区域で利用される端末と異なる条件下に置かれるため、要管理対策区域外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。 例えば、モバイル端末が通常接続される通信回線で実施されているアクセス制御及び監視等は、他の通信回線では同等	2.3.2.2(1)(b) 解説	解説：府省庁外で利用されるモバイル PC は、府省庁内で利用される端末と異なる条件下に置かれるため、府省庁外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。 例えば、モバイル PC が通常接続される通信回線で実施されているアクセス制御及び監視等は、他の通信回線では同等に実施されているとは限らないため、モ

No.	統一技術基準（平成 24 年度改定）		現行	
		に実施されているとは限らないため、モバイル端末において実施する必要がある。		バイル PC において実施する必要がある。
168	2.3.2.2(1)(b)	行政事務従事者は、モバイル端末を利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。	2.3.2.2(1)(c)	行政事務従事者は、モバイル PC を利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。
169	2.3.2.2(1)(b) 解説	解説：モバイル端末には様々なセキュリティ上のリスクが考えられるため、不必要にリスクを増大させないために、業務上必要なモバイル端末の利用にとどめるための事項である。	2.3.2.2(1)(c) 解説	解説：モバイル PC には様々なセキュリティ上のリスクが考えられるため、不必要にリスクを増大させないために、業務上必要なモバイル PC の利用にとどめるための事項である。
170	2.3.2.2(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モバイル端末については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。	2.3.2.2(1)(d)	情報システムセキュリティ責任者は、要機密情報を取り扱うモバイル PC については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。
171	2.3.2.2(1)(c) 解説	解説：モバイル端末が物理的に外部の者の手に渡った場合には、モバイル端末から取り外された内蔵電磁的記録媒体、及びモバイル端末で利用していた外部電磁的記録媒体を他の電子計算機を利用して解読する等の攻撃によって要機密情報が読み取られる危険性がある。このような情報漏えいの対策として、端末に暗号化機能を装備することを求める事項である（ただし、当該モバイル端末で電磁的記録媒体に保存される情報の暗号化を行う機能が存在しない場合を除く。）。 なお、機密性 3 情報を取り扱う場合には、端末に暗号化機能を装備することが必要である。	2.3.2.2(1)(d) 解説	解説：モバイル PC が物理的に外部の者の手に渡った場合には、モバイル PC から取り外された内蔵電磁的記録媒体、及びモバイル PC で利用していた外部電磁的記録媒体を他の電子計算機を利用して解読する等の攻撃によって要機密情報が読み取られる危険性がある。このような情報漏えいの対策として、端末に暗号化機能を装備することを求める事項である。
172	2.3.2.2(1)(d)	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端末については、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。	2.3.2.2(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。

No.	統一技術基準（平成 24 年度改定）		現行	
173	2.3.2.2(1)(d) 解説	解説：モバイル端末は容易に搬出することが可能なため盗難又は紛失に遭う可能性が高いことから、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、要管理対策区域においては、モバイル端末を入退出が管理される区域内に設置している場合においても端末の形状に応じて、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、常時所持又は携帯すること等が挙げられる。モバイル端末を要管理対策区域外に持ち出す場合は、常時所持又は携帯することや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。	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。
174		（削除）	2.3.2.2(1)(e)	【強化遵守事項】
175	2.3.2.2(1)(e)	情報システムセキュリティ責任者は、行政事務従事者が情報を保存できない端末を用いて情報システムを構築する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.3.2.2(1)(f)	情報システムセキュリティ責任者は、行政事務従事者が情報を保存できない端末を用いて情報システムを構築すること。
176		(2.3.2.1(2)(c)へ移動)	2.3.2.2(2)(a)	行政事務従事者は、端末で利用可能と定められたソフトウェアを除いて、ソフトウェアを利用しないこと。
177		(2.3.2.1(2)(c)解説へ移動)	2.3.2.2(2)(a) 解説	解説：多様なソフトウェアを実行することによりセキュリティホール等の脅威が増大することから、定められたソフトウェア以外の利用を禁止する事項である。
178	2.3.2.2(2)(a)	行政事務従事者は、要保護情報を取り扱	2.3.2.2(2)(b)	行政事務従事者は、要保護情報を取り扱

No.	統一技術基準（平成 24 年度改定）		現行	
		うモバイル端末を利用する場合には、盗難防止措置を行うこと。		うモバイル PC を利用する場合には、盗難防止措置を行うこと。
179	2.3.2.2(2)(a) 解説	解説：モバイル端末を利用する行政事務従事者に対して、モバイル端末の盗難防止措置について、情報システムセキュリティ責任者が定めた手順に従い、措置を実施することを求める事項である。	2.3.2.2(2)(b) 解説	解説：モバイル PC を利用する行政事務従事者に対して、モバイル PC の盗難防止措置について、情報システムセキュリティ責任者が定めた手順に従い、措置を実施することを求める事項である。
180	2.3.2.2(2)(b)	行政事務従事者は、要機密情報を取り扱うモバイル端末については、モバイル端末を要管理対策区域外に持ち出す場合に、当該モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。	2.3.2.2(2)(c)	行政事務従事者は、要機密情報を取り扱うモバイル PC については、モバイル PC を府省庁外に持ち出す場合に、当該モバイル PC で利用する電磁的記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
181	2.3.2.2(2)(b) 解説	解説：モバイル端末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。	2.3.2.2(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。
182	2.3.2.2(2)(c) 解説	解説：適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の脅威にさらされることを回避するための事項である。 政府内通信回線でも許可を得た通信回線以外に接続してはならない。モバイル端末を持ち出した際に接続する通信回線についても接続許可を得る必要がある。	2.3.2.2(2)(d) 解説	解説：適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の脅威にさらされることを回避するための事項である。 政府内通信回線でも許可を得た通信回線以外に接続してはならない。モバイル PC を府省庁外に持ち出した際に接続する通信回線についても接続許可を得る必要がある。

No.	統一技術基準（平成 24 年度改定）		現行	
183		（削除）	2.3.2.2(2)(d)	【強化遵守事項】
184	2.3.2.2(2)(d)	情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、端末の時刻を同期する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.3.2.2(2)(e)	情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、端末の時刻を同期すること。
185		(2.3.2.1(1)(e)へ移動)	2.3.2.3(1)(b)	情報システムセキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。
186		(2.3.2.1(1)(e)解説へ移動)	2.3.2.3(1)(b) 解説	解説：サーバ装置において、サービスの提供及びサーバ装置の運用管理に必要となるソフトウェアを定めるための事項である。必要なソフトウェアを定める方法としては、サーバ装置の仕様書において定める、独立の文書として定める等が挙げられる。
187		(2.3.2.1(2)(c)移動)	2.3.2.3(1)(c)	情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。
188		(2.3.2.1(2)(c)解説へ移動)	2.3.2.3(1)(c) 解説	解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。なお、ソフトウェアの設定は初期状態が安全であるとは限らないことについても留意して確認すること。
189		（削除）	2.3.2.3(1)(c)	【強化遵守事項】
190		(2.3.2.1(2)(c)へ移動)	2.3.2.3(1)(d)	情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当し

No.	統一技術基準（平成 24 年度改定）		現行	
				ないソフトウェアをサーバ装置から削除すること。
191		(2.3.2.1(2)(c)解説へ移動)	2.3.2.3(1)(d) 解説	解説：利用が定められたソフトウェアに該当しないものが導入されている場合、利用を禁止していても不正侵入した攻撃者等に悪用される可能性があるため、当該ソフトウェアをサーバ装置から削除することを求める事項である。
192	2.3.2.3(1)(b)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とする必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.3.2.3(1)(e)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とすること。
193	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。 ・サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。 ・バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。 また、取得した情報を記録した電磁的記	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。

No.	統一技術基準（平成 24 年度改定）		現行	
		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。 なお、災害等を想定してバックアップを取得する場合には、記録媒体を耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地にある施設に保存することが考えられる。その際には、情報を遠隔地に送信や移送する際のセキュリティ及び取得した情報の保管時のセキュリティを確保する必要がある。セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。		「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。
194		（削除）	2.3.2.3(2)(d)	【強化遵守事項】
195	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必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	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。
196	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。 なお、アクセスログを確認する際は、運用管理作業の記録若しくは管理者権限	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。

No.	統一技術基準（平成 24 年度改定）		現行	
		を持つ識別コードを付与された者の出退勤記録又は入退室記録等と相関分析を行うことが考えられる。		
197	2.3.2.3(2)(f)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、当該サーバ装置に関する障害等の発生を検知すること。	2.3.2.3(2)(f)	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。
198	2.3.3.1(1)(c) 解説	解説：電子メールの送信時及び受信時において、なりすましを防止することを求める事項である。 「なりすましの防止策」には、平時から行う防止策、電子メールの送信時に行う防止策及び電子メールの受信時に行う防止策等がある。これらの防止策は、第３レベルのドメインだけでなく、第４レベル以上のドメインについても、考慮する必要がある。 （ア）平時から行うなりすましの防止策として、SenderPolicyFramework（以下「SPF」という。）、SenderID 及び DomainKeysIdentifiedMail（以下「DKIM」という。）を利用した送信側における送信ドメイン認証等が挙げられる。（なお、「SenderID」及び「DKIM」は、それぞれ送信ドメイン認証の１つである。）これらは、電子メールで使用するドメインを管理する DNS サーバに、電子メールサーバの情報や署名で使用する公開鍵の登録・公開を行う。なお、SPF や SenderID における DNS サーバへの電子メールサーバ情報の登録では、次の事項に留意する必要がある。	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。

No.	統一技術基準（平成 24 年度改定）	現行
	・電子メールを利用していないドメインは、その情報を登録する必要があること。 ・なりすましの防止策のため、ウェブによるサービス等も含め全く利用していない、若しくは将来にわたって利用の予定のないドメインについては、なりすましの防止策を講ずるか、又はドメイン名の登録を廃止すること。 ・SPF レコードについては、チェックツール等で、文法的に記述間違いのないことを確認すること。（なお、「SPF レコード」とは、SPF や SenderID において、DNS サーバの TXT レコードに記述される送信サーバ等の情報をいう。） ・SPF レコードの末尾は、”~all”ではなく”-all”を記述すること。 ・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と。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りした場合を除き、外部委託先のグローバル IP アドレスを SPF レコードに登録することは認められない。 （イ）電子メールの送信時に行うなりすましの防止策として、S/MIME や DKIM を利用した送信メール（メールマガジンを含む）への電子署名の添付等が挙げ	

No.	統一技術基準（平成 24 年度改定）		現行	
		られる。 （ウ）電子メールの受信時に行うなりすましの防止策として、電子署名の検証及び受信側における SPF の検証（具体的には、受信時に通信を行った送信側の電子メールのサーバと、受信した電子メールに記載されている送信側ドメインを管理する DNS サーバに登録されている電子メールサーバの情報との比較によるなりすましの判定）等が挙げられる。		
199		(削除)	2.3.3.2(1)(a) (エ)	【強化遵守事項】
200	2.3.3.2(1)(b)	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、当該サーバに特定した情報以外の要機密情報が含まれないことを確認すること。	2.3.3.2(1)(b)	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。
201	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。利用が想定されていないデータ等を、ウェブサーバに保存しないことが必要である。	2.3.3.2(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。
202	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ずること。	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。
203	2.3.3.2(2)(a) (カ)解説	解説：（省略） （オ）は、ウェブアプリケーションが出	2.3.3.2(2)(a) (カ)解説	解説：（省略） （オ）は、ウェブアプリケーションが出

No.	統一技術基準（平成 24 年度改定）		現行	
		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ず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。		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。
204		(削除)	2.3.3.2(2)(a) (カ)	【強化遵守事項】
205		(削除)	2.3.3.2(2)(b)	情報システムセキュリティ責任者は、ウ

No.	統一技術基準（平成 24 年度改定）		現行	
				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。
206		(削除)	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、構築時に配慮することが望ましい。
207		(削除)	2.3.3.2(3)(c) (イ)	【強化遵守事項】
208	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する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、定期的にその見直しを行うこと。	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。
209		(削除)	2.3.3.3(1)(d)	【強化遵守事項】
210	2.3.3.3(1)(e)	情報システムセキュリティ責任者は、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	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

No.	統一技術基準（平成 24 年度改定）		現行	
		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必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。		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。
211	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。	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。
212	2.3.3.3(2)(b) 解説	解説：管理するドメインに関する情報が正確であるかどうかを確認することを求める事項である。管理するドメインに関する情報の設定ミスや不正な改ざん等が発生していないかを確認する必要がある。管理するドメインに関する情報の具体例として、ホストの IP アドレス情報を登録する A（AAAA）レコード、ドメインの電子メールサーバ名を登録する MX レコード、なりすましメールを防ぐための SPF レコード等を登録する TXT レコード等がある。なりすまし防止	2.3.3.3(2)(b) 解説	解説：管理するドメインに関する情報が正確であるかどうかを確認することを求める事項である。管理するドメインに関する情報の設定ミスや不正な改ざん等が発生していないかを確認する必要がある。

No.	統一技術基準（平成 24 年度改定）		現行	
		の観点からは、管理するドメインについての SPF レコードが正確であるかどうかを確認したり、ドメインを廃止する場合には、ドメインの廃止申請を行い、当該ドメインが確実に廃止されていることを確認したりすることが重要である。		
213	2.3.4.1(1)(d) 解説	解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、まず電子計算機をグループ化し通信回線上で分離することを求める事項である。府省庁外通信回線と接続する府省庁内通信回線の場合は、府省庁外通信回線上の電子計算機は、府省庁内通信回線に接続される電子計算機とは別のグループとし、分離する必要がある。なお、「グループ化」とは、対象機器をその利用目的、求められるセキュリティレベル、管理部門等から分類することをいう。	2.3.4.1(1)(d) 解説	解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、まず電子計算機をグループ化し通信回線上で分離することを求める事項である。府省庁外通信回線と接続する府省庁内通信回線の場合は、府省庁外通信回線上の電子計算機は、府省庁内通信回線に接続される電子計算機とは別のグループとし、分離する必要がある。なお、「グループ化」とは、対象機器をその利用目的、求められるセキュリティレベル、管理部署等から分類することをいう。
214	2.3.4.1(1)(i)	情報システムセキュリティ責任者は、通信回線装置を要管理対策区域内に設置すること。	2.3.4.1(1)(i)	情報システムセキュリティ責任者は、通信回線装置を安全区域に設置すること。
215	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。また、災害等を想定して冗長構成にする場合には、その通信回線及び代替通信回線がそれぞれ別の経路となることが望ましい。	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。
216		(削除)	2.3.4.1(1)(k)	【強化遵守事項】
217	2.3.4.1(1)(l)	情報システムセキュリティ責任者は、通	2.3.4.1(1)(l)	情報システムセキュリティ責任者は、通

No.	統一技術基準（平成 24 年度改定）		現行	
		信を行う電子計算機の主体認証を行う必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。		信を行う電子計算機の主体認証を行うこと。
218		(削除)	2.3.4.1(2)(e)	【強化遵守事項】
219	2.3.4.1(2)(f)	情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、通信回線装置の運用状態を復元するために必要な措置を講ずること。		(新規追加)
220	2.3.4.1(2)(f) 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に、サービスの可用性を担保することを目的とした事項である。対策としては、通信回線装置の設定情報を作成又は変更した際に、設定情報のバックアップを実施することが挙げられる。 なお、災害等を想定してバックアップを取得する場合には、取得した情報を記録した電磁的記録媒体を耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地にある施設に保存することが考えられる。		(新規追加)
221	2.3.4.1(2)(g)	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する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、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。	2.3.4.1(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。
222	2.3.4.1(2)(g) 解説	解説：通信回線装置における不正なソフトウェアの存在確認等を定期的に行い、対処がなされていない場合にその改善を図ることを求める事項である。「定期	2.3.4.1(2)(f) 解説	解説：通信回線装置における不正なソフトウェアの存在確認等を定期的に行い、対処がなされていない場合にその改善を図ることを求める事項である。「定期

No.	統一技術基準（平成 24 年度改定）		現行	
		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、調査する必要性については、一般的には、通信回線の重要性、想定される脅威及び機器の特性等から検討することが考えられる。例えば、基幹回線等の重要な通信回線を構成する機器、ファイアウォールのようにインターネット等と直接接続されている機器、頻繁にソフトウェアがアップデートされるような機器等は必要性が高い機器として考えられる。ただし、必要性が低いと判断された機器についても、ソフトウェア等にぜい弱性が報告されたり、通信回線の構成変更が発生したりする場合に随時調査することが望ましい。 なお、「不適切な状態」とは、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、定められた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。		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。 なお、「不適切な状態」とは、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、定められた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。
223	2.3.4.1(2)(h) 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、主体認証を行う通信回線装置については、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。	2.3.4.1(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。
224		(削除)	2.3.4.2(1)	【強化遵守事項】
225	2.3.4.2(1)(a)	情報システムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続す	2.3.4.2(1)(a)	情報システムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続す

No.	統一技術基準（平成 24 年度改定）		現行	
		ることを許可されたものであることを確認する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。		ることを許可されたものであることを確認するための措置を講ずること。
226		(削除)	2.3.4.2(2)	【強化遵守事項】
227	2.3.4.2(2)(b)	情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、通信回線の性能低下及び異常を推測し、又は検知すること。	2.3.4.2(2)(b)	情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。
228	2.3.4.2(2)(c)	情報システムセキュリティ管理者は、府省庁内通信回線上を送受信される通信内容を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。	2.3.4.2(2)(c)	情報システムセキュリティ管理者は、府省庁内通信回線上を送受信される通信内容を監視すること。
229		(削除)	2.3.4.2(3)(b)(キ)	無線 LAN 接続方法の機密性の確保
230	2.3.4.2(3)(b)(キ)	無線 LAN に接続する電子計算機及び通信回線装置の管理	2.3.4.2(3)(b)(ク)	無線 LAN に接続する電子計算機の管理
231	2.3.4.2(3)(b)(キ)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。無線 LAN を利用する場合は、構築する環境に応じて措置を講ずることが望ましい。 （イ）については、例えば、WPA2Enterprise（Wi-FiProtectedAccess2Enterprise）方式を選択することが考えられる。 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（WiredEquivalentPrivacy）、TKIP（TemporalKeyIntegrityProtocol）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	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（WiredEquivalentPrivacy）、TKIP（TemporalKeyIntegrityProtocol）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

No.	統一技術基準（平成 24 年度改定）		現行	
		きたりするという脆弱性が報告されており、また同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択すること。この場合、暗号化については、暗号と電子署名の標準手順に従わなければならない。 （ウ）については、例えば、通信回線上における主体認証の方式である IEEE802.1x（クライアント認証及びサーバ認証）を導入し、適切に設定することが考えられる。 （オ）については、例えば、行政事務従事者が利用する府省庁内通信回線と府省庁外の者向けに提供する府省庁内通信回線を分離することが考えられる。 （カ）については、例えば、無線 LAN に接続中に同時に有線 LAN と接続することを禁止することが考えられる。 （キ）については、例えば、無線 LAN に接続する電子計算機及び通信回線装置（無線 LAN アクセスポイント等）の機能で、以下のような管理を行うことが考えられる。 ・出力・チャンネル管理等による電波監理 ・IEEE802.1x 等による管理外の無線 LAN アクセスポイント及び電子計算機の検出及び除去 ・IPS（IntrusionPreventionSystem）機能等によるサービス不能攻撃の防御 ・MAC アドレス等による接続管理等 これらは、通信回線装置を要管理対策区域内に設置しても、第三者が区域外から不正に接続してくる可能性があることに注意して、設定する必要がある。	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。

No.	統一技術基準（平成 24 年度改定）		現行	
		なお、府省庁外の者向けに通信回線を提供する場合は、例えば、事前共有鍵等を利用した暗号化及び認証を行うことやVPN を利用することが考えられる。 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、及び各府省情報化統括責任者（CIO）補佐官等連絡会議の「無線 LAN セキュリティ要件の検討」（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）を適宜参照。		
232	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が進められているが、IPv6 通信プロトコルは IPv4 通信プロトコル環境下と同様にセキュリティ上のリスクがあるとともに、グローバル IP アドレスによる直接通信の利用等に際し考慮すべきリスクも考えられる。また IPv4 通信プロトコルから IPv6 通信プロトコルへの移行過程においても、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。さらに、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、それぞれの環境を前提と	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、IPv

No.	統一技術基準（平成 24 年度改定）		現行	
		して、対策を講ずる必要がある。 なお、IPv6 に関する最新の動向については、引き続き状況の変化が予想されるため、各府省庁においても、IPv6 のセキュリティ対策に関する動向を十分に注視し、適切に対応していく必要がある。これらのことを勘案し、本項では、IPv6 技術を利用する情報システム、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。		4 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。
233	2.4.1.1(1)	IPv6 通信がもたらす脆弱性対策	2.4.1.1(1)	IPv6 移行機構がもたらす脆弱性対策
234	2.4.1.1(1)(a)	情報システムセキュリティ責任者は、IPv6 技術を利用する通信（以下「IPv6 通信」という。）を想定して構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に IPv6ReadyLogo Program に基づく Phase-2 準拠製品がある場合には、当該製品を情報システムの構成要素として選択すること。		(新規追加)
235	2.4.1.1(1)(a) 解説	解説：IPv6 に対応する機器等の購入において、一定水準以上のセキュリティ機能を有する製品を選択することを求める事項である。国際的な IPv6 に関する標準プログラムである IPv6ReadyLogo Program による客観的な基準に準拠する製品を選択することにより、安全性の高い情報システムの構築が期待できる。		(新規追加)
236	2.4.1.1(1)(b)	情報システムセキュリティ責任者は、IPv6 通信を想定して構築する情報システムにおいて、グローバル IP アドレスに		(新規追加)

No.	統一技術基準（平成 24 年度改定）		現行	
		よる直接の到達性における脅威を防止するための措置を講ずること。		
237	2.4.1.1(1)(b) 解説	解説：IPv6 で新たに導入された通信制御機構や、IPv6 の特徴である外部ネットワークとの直接接続の容易さに起因する各種攻撃への対策を求める事項である。 対策としては、不正な機器からの経路調査コマンド（traceroute 等）及び ICMP エコー要求等に応答しない、サービス不能攻撃への対策、並びに認可した宛先からのみアクセスを可能にする等が挙げられる。		（新規追加）
238	2.4.1.1(1)(c)	情報システムセキュリティ責任者は、IPv6 通信を想定して構築する情報システムにおいて、不正な通信を制限するフィルタリングを適切に行うこと。		（新規追加）
239	2.4.1.1(1)(c) 解説	解説：IPv6 の特徴として、アドレスが長い、アドレスの省略形が複数パターン存在し一意に定まらない、端末が複数の IP アドレスを持つ等が挙げられる。このような複雑なアクセス制御が設定の不備等を招き不正アクセス等に繋がるリスクが高まるため、フィルタリングを適切に実施することを求める事項である。 対策としては、外部ネットワークとの通信において、OSI 基本参照モデルのネットワーク層（第３層）及びトランスポート層（第４層）を中心にフィルタリングを行う機能及び断片化された通信の再構築を行う機能を適切に設定すること等、通信機器を流れる通信そのものを制御することが挙げられる。 なお、IPv6 通信を想定して構築する情報システムにおいて、IPv6 のログを取		（新規追加）

No.	統一技術基準（平成 24 年度改定）		現行	
		得し、分析する場合は、IPv6 アドレスでは桁数が大幅に増えること等から、IPv6 対応のログの解析ツールを利用することで、IPv6 アドレスの読み間違い等の運用上の作業ミスを軽減するための対策を検討することが望ましい。		
240	2.4.1.1(1)(d)	情報システムセキュリティ責任者は、情報システムに IPv6 通信の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。	2.4.1.1(1)(a)	情報システムセキュリティ責任者は、情報システムに IPv6 技術を利用する通信（以下「IPv6 通信」という。）の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。
241	2.4.1.1(1)(e)	情報システムセキュリティ責任者は、IPv6 通信を想定して構築する情報システムにおいて、IPv6 に対応していない機器及びソフトウェアの利用によるセキュリティの問題がないように措置を講ずること。		(新規追加)
242	2.4.1.1(1)(e) 解説	解説：IPv4 のみに対応する機器及びソフトウェアが IPv6 ネットワーク上で動作する際のセキュリティ上のリスクに対する対策を求める事項である。システム内部での IP アドレスの取扱いが IPv4 に依存している場合、IPv6 アドレスが取り扱えない、若しくはバッファオーバーラン等を引き起こす可能性があるというリスクを認識し、これが無いことを確認する等が挙げられる。統合認証システムや、システム間連動を行うようなアプリケーションでは、IPv4/IPv6 が混在した状況でも適切なシステム連携を行う必要がある。		(新規追加)
243	2.4.1.1(2)(a)	情報システムセキュリティ責任者は、府省庁間及び府省庁内部のみで利用する	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信回線に

No.	統一技術基準（平成 24 年度改定）		現行	
		情報システムについて、IPv6 通信を想定していない通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。		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。
244	2.4.1.1(2)(a) 解説	解説：府省庁間及び府省庁内部のみで利用する情報システムについて、通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する措置を求める事項である。 IPv6 通信を想定していない通信回線においては、ファイアウォールや侵入検知システム等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能な電子計算機においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該電子計算機への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、電子計算機と外部のネットワークとの間に利用者や管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないよう電子計算機を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。 なお、「政府情報システムに係る IPv6 対応の取組について」（2011 年 11 月 2 日	2.4.1.1(2)(a) 解説	解説：通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する措置を求める事項である。 IPv6 通信を想定していない通信回線においては、ファイアウォールや侵入検知システム等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能な電子計算機においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該電子計算機への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、電子計算機と外部のネットワークとの間に利用者や管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないよう電子計算機を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。

No.	統一技術基準（平成 24 年度改定）		現行	
		各府省情報化統括責任者（CIO）連絡会議決定）において IPv6 対応の取組を進めることが確認されているが、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を抑止するための措置を講ずることが必要である。		
245		(削除)	2.4.1.1(2)(a)	【強化遵守事項】
246	2.4.1.1(2)(b)	情報システムセキュリティ責任者は、府省庁間及び府省庁内部のみで利用する情報システムについて、IPv6 通信を想定していない通信回線を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。	2.4.1.1(2)(b)	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信回線を監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。
247	2.4.1.1(2)(b) 解説	解説：意図しない IPv6 通信が情報システムに与える脅威から情報システムを守るための事項である。 IPv6 技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが府省庁内通信回線を流れている場合には、管理者や利用者が気付かないうちに IPv6 技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6 通信を想定していない府省庁内通信回線において、IPv6-IPv4 トンネル機構で使用する通信パケットが検知された場合は、IPv6 技術を使った悪意のある通信がなされているおそ	2.4.1.1(2)(b) 解説	解説：意図しない IPv6 通信が情報システムに与える脅威から情報システムを守るための事項である。 IPv6 技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが府省庁内通信回線を流れている場合には、管理者や利用者が気付かないうちに IPv6 技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6 通信を想定していない府省庁内通信回線において、IPv6-IPv4 トンネル機構で使用する通信パケットが検知された場合は、IPv6 技術を使った悪意のある通信がなされているおそ

No.	統一技術基準（平成 24 年度改定）		現行	
		れがある。府省庁内通信回線を管理する者は、このような通信の有無を監視して、IPv6 通信が検知された場合は、当該通信の遮断等の措置を講ずる必要がある。 なお、「政府情報システムに係る IPv6 対応の取組について」（2011 年 11 月 2 日各府省情報化統括責任者（CIO）連絡会議決定）において IPv6 対応の取組を進めることが確認されているが、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を遮断するための措置を講ずることが必要である。		れがある。府省庁内通信回線を管理する者は、このような通信の有無を監視して、IPv6 通信が検知された場合は、当該通信の遮断等の措置を講ずる必要がある。
248	2.4.1.1(2)(b)	別表		(新規追加)
249	別表 1	別表 1 情報取扱区域のクラス別管理		(新規追加)
250	別表 2	別表 2 情報取扱区域のクラス別利用制限		(新規追加)
251	A.1.4	●「MAC アドレス（MediaAccessControladdress）」とは、電子計算機のネットワーク機器を識別するための固有の一意な値をいう。		(新規追加)
252	A.1.5	A.1.5 情報取扱区域のクラスと区域例		(新規追加)
253	A.1.5	統一管理基準に準じる。		(新規追加)
254	A.1.6	A.1.6 情報取扱区域の個別管理及び個別利用制限の付表例		(新規追加)
255	A.1.6	統一管理基準に準じる。		(新規追加)