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(平成 24 年度改定)

新旧対照表

No.	統一管理基準(平成 24 年度改定版)		旧版	
1	1.1.1.2(1)(d)	第 1.4 部 情報処理についての対策 「情報処理についての対策」では、情報システムの利用において実施すべき事項と、要管理対策区域外での情報処理及び府省庁支給以外の情報システムによる情報処理において制限すべき事項を本統一管理基準において定めている。	1.1.1.2(1)(d)	第 1.4 部 情報処理についての対策 「情報処理についての対策」では、情報システムの利用において実施すべき事項と、府省庁外での情報処理及び府省庁支給以外の情報システムによる情報処理において制限すべき事項を本統一管理基準において定めている。
2	1.1.1.2(3)	「対策レベルの設定」に係る変更点	1.1.1.2(3)	対策レベルの設定
3	1.1.1.2(3)	「政府機関の情報セキュリティ対策における統一管理基準」(平成 23 年 4 月 21 日策定、NISD-K304-101)及び「政府機関の情報セキュリティ対策における統一技術基準」(平成 23 年 4 月 21 日策定、NISD-K305-101)までは、各対策項目で対策の強度に段階を設けていた。この段階を「対策レベル」と呼び、採るべき遵守事項を「基本遵守事項」又は「強化遵守事項」としていた。 そして、「基本遵守事項」を「保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項」、「強化遵守事項」を「特に重要な情報とこれを取り扱う情報システムにおいて、府省庁が、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対	1.1.1.2(3)	情報セキュリティ対策においては、対象となる情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様ではない。また、該当する情報システム及び業務の特性に応じて、各対策項目で適切な強度の対策を実施すべきである。したがって、本統一管理基準及び統一技術基準においては、各対策項目で対策の強度に段階を設け、採るべき遵守事項を定めている。この段階を「対策レベル」と呼び、以下のように定義する。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		策事項」と定義し、「強化遵守事項」については、各府省庁において省庁対策基準の策定時に、府省庁の情報システム及び業務の特性を踏まえ、省庁対策基準への採用を選択することとしていた。 今後は、従来の「基本遵守事項」及び「強化遵守事項」の区分を廃止して「遵守事項」とする。「遵守事項」は、省庁対策基準において、保護すべき情報とこれを扱うシステムにおいて、必須として実施すべき対策事項とする。なお、必要性の有無を検討し、必要があると判断した際に実施する対策事項については、実施の必要性の有無の検討を必須とし、対策の実施についてはそれぞれの府省庁の判断とする。		
4		(削除)	1.1.1.2(3)(a)	「基本遵守事項」は、保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項
5		(削除)	1.1.1.2(3)(b)	「強化遵守事項」は、特に重要な情報とこれを取り扱う情報システムにおいて、府省庁が、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項
6		(削除)	1.1.1.2(3)(b)	以上により、府省庁は、基本遵守事項以上の対策を実施することとなるが、当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない。
7	1.1.1.3(2)(a) 解説	解説：可用性の格付については、情報が滅失又は紛失されていない状態並びに情報及び関連資産へのアクセスを認められた者が、必要時に中断する	1.1.1.3(2)(a) 解説	解説：可用性の格付については、情報が滅失又は紛失されていない状態及び情報へのアクセスを認められた者が、必要時に中断することなく、情報

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ことなく、情報及び関連資産にアクセスできる状態を確保されるべき情報は可用性２情報に、それ以外の情報は可用性１情報に決定することを基本とする。 なお、可用性２情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。		及び関連資産にアクセスできる状態を確保されるべき情報は可用性２情報に、それ以外の情報は可用性１情報に決定することを基本とする。 なお、可用性２情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。
8	1.1.1.4	情報取扱区域における管理及び利用制限		(新規追加)
9	1.1.1.4 (1)	情報取扱区域		(新規追加)
10	1.1.1.4 (1)	情報セキュリティを確保するためには、適切な対策が講じられている区域で行政事務を行うことが必要不可欠である。そのため、執務室や会議室、サーバ室等の管理に当たっては、それらの区域でどのような行政事務が行われるのかを想定し、それに応じて必要となる管理対策を決定し、適切な措置を講ずる必要がある。 また、それらの区域の利用に当たっては、用途や施されている管理対策に応じて、必要な制限を利用者に求めることも情報セキュリティを確保する上で必要となる。 さらに、このような対策を有効なものとするためには、行政事務を行う者が、それらの区域に求められる管理対策及び利用の制限について正しく認識でき、取り扱う情報の重要性に応じて適切な区域を選択できるようにする必要がある。 これらのことから、それぞれの府省庁の内外において情報を取り扱う区域		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		を「情報取扱区域」とし、それらの区域のうち、求める対策の観点から「クラス」の区分を定めるものとする。		
11	1.1.1.4 (2)	情報取扱区域のクラスの決定		(新規追加)
12	1.1.1.4 (2)	情報取扱区域について、求める対策の基準ごとに「クラス」の区分を定める。		(新規追加)
13	1.1.1.4 (2)(a)	情報取扱区域におけるクラス及びクラスにおける区分の基準を、それぞれ以下のとおりとする。		(新規追加)
14	1.1.1.4 (2)(a)	クラス 区分の基準 クラス 3 クラス 2 より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域 クラス 2 クラス 1 より強固な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域 クラス 1 最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域 クラス 0 クラス３、クラス２及びクラス１以外の区域であり、情報セキュリティを確保するため、利用制限対策を実施する必要がある区域		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		なお、クラス 1 以上の区域を「要管理対策区域」という。		
15	1.1.1.4 (2)(a) 解説	解説：各クラスに該当する区域の例は、本書別添資料 A.1.5 情報取扱区域のクラスと区域例を参照。		(新規追加)
16	1.1.1.4 (3)	情報取扱区域のクラス別管理及び利用制限		(新規追加)
17	1.1.1.4 (3)	各府省庁は、定めた情報取扱区域について、クラス 0 からクラス 3 の区域においてクラス別に講ずる管理対策（以下「クラス別管理」という。）及び対策が講じられた区域におけるクラス別の利用制限対策(以下「クラス別利用制限」という。）を決定し、それらに基づいて適切に対策を講ずるものとする。 なお、統一管理基準及び統一技術基準において定めるクラス別管理及び利用制限は、最低限の管理対策及び利用制限対策であるため、それぞれの府省庁において、名称の変更、クラスの追加並びに実施する管理対策及び利用制限対策の変更又は追加を適宜実施して構わない。ただし、変更又は追加する場合には、それぞれの府省庁の対策基準で求める情報取扱区域における情報セキュリティ水準が、本統一管理基準及び統一技術基準において求める情報セキュリティ水準と同等以上となるように準拠しなければならない。		(新規追加)
18	1.1.1.4 (4)	情報取扱区域の個別管理及び個別利用制限		(新規追加)
19	1.1.1.4 (4)	情報取扱区域について、決定したクラスの区分において必要な対策が不足		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		している と認められる区域、又はクラスとは別の区分で対策を講ずる必要のある区域があるときは、求める情報セキュリティ水準を確保又は向上させるため、定められたクラス別管理及び利用制限にかかわらず、当該区域ごとに個別の管理対策(以下「個別管理」という。) 及び個別の利用制限対策(以下「個別利用制限」という。) を決定することができる。		
20	1.1.1.4 (4) 解説	解説 : 付表を用いて定める場合の例については本書別添資料 A.1.6 情報取扱区域の個別管理及び個別利用制限の付表例を参照。 なお、情報は、適切な対策が講じられた区域で取り扱うことが望ましいが、区域を利用する用途や講じられる対策により下位のクラスにせざるを得ない区域については、個別管理及び個別利用制限を講ずることで、求める情報セキュリティ水準の確保を図ることも可能である。		(新規追加)
21	1.1.1.5	1.1.1.5 評価の方法	1.1.1.4	1.1.1.4 評価の方法
22	1.1.1.6	1.1.1.6 用語定義	1.1.1.5	1.1.1.5 用語定義
23		(削除)	1.1.1.5	● 「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。
24	1.1.1.6	● 「可用性」とは、情報及び関連資産へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保	1.1.1.5	● 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをい

No.	統一管理基準(平成 24 年度改定版)		旧版	
		することをいう。		う。
25	1.1.1.6	● 「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、行政事務の遂行に支障を及ぼすものをいう。情報の格付では、要機密情報に相当する。	1.1.1.5	● 「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、行政事務の遂行に支障を及ぼすものをいう。
26	1.1.1.6	● 「情報の移送」とは、要管理対策区域外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。	1.1.1.5	● 「情報の移送」とは、府省庁外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。
27	1.1.1.6	(削除)	1.1.1.5	● 「府省庁外での情報処理」とは、行政事務従事者の各々が所属する府省庁の管理部外で行政事務の遂行のための情報処理を行うことをいう。なお、オンラインで府省庁外から行政事務従事者の各々が所属する府省庁の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。
28	1.1.1.6	● 「要管理対策区域」とは、施設及び環境に係る管理対策が講じられている区域であって、情報取扱区域におけるクラス 1 以上の区域をいう。 ● 「要管理対策区域外」とは、情報取扱区域におけるクラス 0 の区域をいう。 ● 「要管理対策区域外での情報処理」とは、行政事務従事者が情報取扱区域におけるクラス 0 の区域において行政事務の遂行のための情報処理を行うことをいう。なお、オンラインで府省庁外から行政事務従事者の		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		各々が所属する府省庁の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。		
29	1.2.1.1	情報セキュリティ対策は、それに係る全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。 これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。具体的には、 ・最高情報セキュリティ責任者の設置とその役割 ・情報セキュリティ委員会の設置とその役割 ・情報セキュリティ監査責任者の設置とその役割 ・情報セキュリティ責任者の設置とその役割 ・情報システムセキュリティ責任者の設置とその役割 ・情報システムセキュリティ管理者の設置とその役割 ・課室情報セキュリティ責任者の設置とその役割 ・区域情報セキュリティ責任者の設置とその役割 ・最高情報セキュリティアドバイザーの設置とその役割 についての遵守事項を定めるもので	1.2.1.1	情報セキュリティ対策は、それに係る全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。 これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。具体的には、 ・最高情報セキュリティ責任者の設置とその役割 ・情報セキュリティ委員会の設置とその役割 ・情報セキュリティ監査責任者の設置とその役割 ・情報セキュリティ責任者の設置とその役割 ・情報システムセキュリティ責任者の設置とその役割 ・情報システムセキュリティ管理者の設置とその役割 ・課室情報セキュリティ責任者の設置とその役割 ・最高情報セキュリティアドバイザーの設置とその役割 についての遵守事項を定めるものである。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ある。		
30	1.2.1.1(8)	区域情報セキュリティ責任者の設置		(新規追加)
31	1.2.1.1(8)(a)	統括情報セキュリティ責任者は、要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う区域の単位を定め、その単位ごとに区域情報セキュリティ責任者を置くこと。		(新規追加)
32	1.2.1.1(8)(a) 解説	解説：要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う単位を決め、区域ごとの情報セキュリティ対策を実施する者を置くことを定めた事項である。 要管理対策区域には、執務室やサーバ室だけでなく、ロビーや庁舎内の廊下といった区域も含まれる。そのため、府省庁において漏れなく情報セキュリティ対策を実施する観点から、それぞれの区域に区域情報セキュリティ責任者を置く必要がある。 「管理を行う区域の単位」は、当該区域の利用用途や設置環境等を勘案して、例えば、 ・部局又は課室単位で管理している執務室又は会議室ごと ・情報システムが設置された部屋(サーバ室等) ごと 等とすることが挙げられる。また、上記以外の要管理対策区域(ロビー、廊下等) を一つの区域とする場合も考えられる。 なお、区域情報セキュリティ責任者は、当該区域の利用用途や設置環境等を勘案して、情報セキュリティ責任者、課室情報セキュリティ責任者、情報システムセキュリティ責任者又は		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		庁舎等の管理に関する部門の責任者等の中から定めることが考えられる。 定める単位としては、例えば、 ・単一の課室が利用する執務室及び会議室を管理する場合は、課室情報セキュリティ責任者 ・複数の課室が利用する執務室及び会議室を管理する場合は、情報セキュリティ責任者 ・情報システムが設置された部屋(サーバ室等）を管理する場合は、情報システムセキュリティ責任者 ・異なる区域（クラスが異なる場合も含む）をまとめて管理する場合は、情報セキュリティ責任者 ・執務室又はサーバ室以外の要管理対策区域(ロビー、廊下等）を管理する場合は、庁舎等の管理に関する部門の責任者 等を区域情報セキュリティ責任者として定めることが考えられる。		
33	1.2.1.1(8)(b)	区域情報セキュリティ責任者は、所管する単位における区域ごとの情報セキュリティ対策に関する事務を統括すること。		(新規追加)
34	1.2.1.1(8)(c)	統括情報セキュリティ責任者は、全ての区域情報セキュリティ責任者に対する連絡網を整備すること。		(新規追加)
35	1.2.1.2(2)(b) 解説	解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。 例えば、機密性３情報、完全性２情報又は可用性２情報について、要管理対策区域外での情報処理や府省庁支給	1.2.1.2(2)(b) 解説	解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。 例えば、機密性３情報、完全性２情報又は可用性２情報について、府省庁外での情報処理や府省庁支給以外の情

No.	統一管理基準(平成 24 年度改定版)		旧版	
		以外の情報システムによる情報処理を課室情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得すること等が求められる。		報システムによる情報処理を課室情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得すること等が求められる。
36	1.2.2.2	情報セキュリティに関する障害・事故等が発生又はそのおそれがある場合には、早急にその状況を検出又は確認し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、障害・事故等の影響や範囲に関する責任者への報告及び府省庁内外の関係部門との情報共有により、障害・事故等の発生現場の混乱や誤った指示の発生等を最小限に抑えるとともに、被害の拡大防止策や再発防止策を講ずることが重要である。 これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準として、障害・事故等の発生に備えた事前準備、発生時における報告と対処の流れ、原因調査と再発防止策についての遵守事項を定める。	1.2.2.2	情報セキュリティに関する障害・事故等が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、障害・事故等の影響や範囲を定められた責任者へ報告し、障害・事故等の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。 これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準として、障害・事故等の発生に備えた事前準備、発生時における報告と応急措置、原因調査と再発防止策についての遵守事項を定める。
37	1.2.2.2(1)(a)	最高情報セキュリティ責任者は、情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）の発生に対応するために以下の役割及び機能を有する体制を整備すること。	1.2.2.2(1)(a)	最高情報セキュリティ責任者は、情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生した場合、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備すること。
38	1.2.2.2(1)(a) (ア)	障害・事故等に対応する責任者の決定		(新規追加)
39	1.2.2.2(1)(a) (イ)	障害・事故等の発生の報告		(新規追加)
40	1.2.2.2(1)(a)	障害・事故等の発生報告の受付		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
	(ウ)			
41	1.2.2.2(1)(a) (エ)	関係する部門への障害・事故等の発生に関する速やかな連絡		(新規追加)
42	1.2.2.2(1)(a) (オ)	応急措置の実施(被害の拡大防止)		(1.2.2.2(1)(a)から移動)
43	1.2.2.2(1)(a) (カ)	障害・事故等からの復旧		(1.2.2.2(1)(a)から移動)
44	1.2.2.2(1)(a) (キ)	原因調査の実施		(新規追加)
45	1.2.2.2(1)(a) (ク)	再発防止策の策定及び実施		(新規追加)
46	1.2.2.2(1)(a) (ケ)	再発防止策の実施の確認		(新規追加)
47	1.2.2.2(1)(a) 解説	解説:最高情報セキュリティ責任者に障害・事故等に対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配意することも必要である。 障害・事故等に対する体制を整備するに当たっては、複数の部門で機能を分担することも考えられる。 「障害・事故等に対応する責任者」とは、障害・事故等が発生した場合の対応に係る責任者であり、その役割としては、障害・事故等に関する全般的な対応が求められる。また、最高情報セキュリティ責任者が自ら障害・事故等への対応に当たる場合は、その指揮監督の下で必要な対応を行うこととなる。 障害・事故等に対応する責任者は、情報セキュリティ対策に関する事務を総括する部門の責任者がその役割を担うことが考えられるが、統括情報セキュリティ責任者又は各部門の情報	1.2.2.2(1)(a) 解説	解説:最高情報セキュリティ責任者に障害・事故等に対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配意することが求められる。 なお、情報セキュリティに関する障害・事故等とは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。 また、「インシデント」とは、JIS Q 27002:2006(ISO/IEC 17799:2005)における情報セキュリティインシデントと同意である。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		セキュリティ責任者がその役割を担うことも考えられる。その場合は、障害・事故等に関係する部門及び情報セキュリティ対策に関する事務を総括する部門との間で速やかな連絡ができる体制にすることが望ましい。 「関係する部門への障害・事故等の発生に関する速やかな連絡」には、府省庁内だけでなく、府省庁外の関係部門への連絡も含まれる。なお、障害・事故等の発生時に、府省庁外の関係部門へ速やかに連絡するためには、府省庁外の関係部門と日常的な情報共有等の連携を図る必要がある。その場合、障害・事故等の発生時の連絡と日常的な連携を複数の部門で分担することも考えられる。ただし、機能を分担する場合は、互いの部門間で、障害・事故等に関する情報や日常的な連携で得られた情報を共有する必要がある。 なお、情報セキュリティに関する障害・事故等とは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。 また、「インシデント」とは、JIS Q 27002:2006(ISO/IEC 17799:2005）及び ISO/IEC 27035:2010 における情報セキュリティインシデントと同意である。		
48	1.2.2.2(1)(b) 解説	解説：報告手順として、障害・事故等の発生を知った行政事務従事者から報告を受け、障害・事故等に対応する責任者が、最高情報セキュリティ責任者に報告するまでの具体的な手順や	1.2.2.2(1)(b) 解説	解説：窓口についての周知は、情報セキュリティ対策の教育の中で行うとともに、窓口の連絡先を執務室内に掲示する等して、緊急時に行政事務従事者がすぐに参照できるようにするこ

No.	統一管理基準(平成 24 年度改定版)		旧版	
		決定された障害・事故等に対応する責任者に対し、確実に報告ができる連絡手段等について明記する必要がある。また、報告手順の中には、例えば、最高情報セキュリティ責任者に障害・事故等の報告を集約するための窓口を設けることが考えられる。窓口についての周知は、情報セキュリティ対策の教育の中で行うとともに、窓口の連絡先を執務室内に掲示する等して、緊急時に行政事務従事者がすぐに参照できるようにする必要がある。なお、情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。 窓口は、情報セキュリティ対策に関する事務を総括する部門に設置することが考えられるが、別の部門に窓口を設ける場合は、当該部門から障害・事故等に関係する部門への連絡や情報セキュリティ対策に関する事務を総括する部門への報告が速やかに実施される体制にすることが望ましい。		とが必要である。情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。
49	1.2.2.2(1)(c)	統括情報セキュリティ責任者は、障害・事故等が発生した際の府省庁内及び府省庁外との情報共有を含む対処手順を整備すること。	1.2.2.2(1)(c)	統括情報セキュリティ責任者は、障害・事故等が発生した際の対処手順を整備すること。
50	1.2.2.2(1)(c) 解説	解説：対処手順として障害・事故等の発生時において緊急を要する対処等の必要性に備えて、通常とは異なる例外措置の承認手続を設けることもあわせて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなこ	1.2.2.2(1)(c) 解説	解説：対処手順として障害・事故等の発生時において緊急を要する対処等の必要性に備えて、通常とは異なる例外措置の承認手続を設けることもあわせて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなこ

No.	統一管理基準(平成 24 年度改定版)		旧版	
		とがないよう検討すること。 対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を行政事務従事者が記録すべきこと並びに府省庁内外の関係部門への障害・事故等の情報共有を行うまでの目標時間を定めること等も考えられる。 情報共有の枠組みとしては、「政府におけるサイバー攻撃等への対処態勢の強化について」(平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ) 等で定めた連絡連携体制を利用すること。		とがないよう検討すること。 対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を行政事務従事者が記録すべきことを定めることも考えられる。
51	1.2.2.2(1)(e) 解説	解説：実際に障害・事故等への対処を模擬的に行うことにより、対応力を強化するために実施する訓練の内容及び体制の整備を求める事項である。 訓練には、情報システム部門だけでなく、障害・事故等の報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門も参加することが望ましい。この場合、障害・事故等の報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門では、障害・事故等への専門的な対処を行う必要があるため、必要となる知識もより高度になる。そのため、訓練の一部として、障害・事故等の対処に関する教育を受講したり、外部から情報セキュリティに関する情報を適宜収集したりする必要がある。	1.2.2.2(1)(e) 解説	解説：実際に障害・事故等への対処を模擬的に行うことにより、対応力を強化するために実施する訓練の内容及び体制を整備することを求める事項である。 なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		なお、あらかじめ統括情報セキュリティ責任者が認めた場合には、統括情報セキュリティ責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、統括情報セキュリティ責任者は、指定した者より適宜報告を受けることが望ましい。		
52	1.2.2.2(2)	障害・事故等の発生時における報告と対処の流れ	1.2.2.2(2)	障害・事故等の発生時における報告と応急措置
53	1.2.2.2(2)(a)	行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に報告することができない場合は、定められた報告手順に従って、最高情報セキュリティ責任者に報告すること。	1.2.2.2(2)(a)	行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、情報セキュリティ責任者にその旨を報告すること。
54	1.2.2.2(2)(a) 解説	解説：障害・事故等が発生した場合に、行政事務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害・事故等への対処を開始すること、及び障害・事故等が発生したことについて行政事務従事者から障害・事故等に対応する責任者に報告され、障害・事故等に対応する責任者が速やかに最高情報セキュリティ責任者に報告することにより、最高情報セキュリティ責任者が状況を把握し、適切に対処することができるようにすることを	1.2.2.2(2)(a) 解説	解説：障害・事故等が発生した場合に、行政事務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害・事故等への対処を開始することができるようにすることを求める事項である。 なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		求める事項である。 なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。 また、障害・事故等に対応する責任者に報告することができない場合は、他の手順により最高情報セキュリティ責任者に確実に報告される必要がある。		
55	1.2.2.2(2)(b)	障害・事故等に対応する責任者は、被害の拡大防止等を図るための応急措置の実施及び障害・事故等からの復旧に係る指示又は勧告を行うこと。		(新規追加)
56	1.2.2.2(2)(b) 解説	解説：障害・事故等に対応する責任者に対し、報告を受けた障害・事故等に係る必要な措置を講ずることを求める事項である。 応急措置や復旧に当たっては、障害・事故等が発生している情報システムの停止又は隔離について、障害・事故等に対応する責任者の判断で指示又は勧告ができるようにする必要がある。 なお、障害・事故等に対応する責任者の役割を情報セキュリティ対策に関する事務を総括する部門の責任者が担う場合は、当該部門の責任者が応急措置及び復旧に関する具体的な指示又は勧告を行うこととなるが、統括情報セキュリティ責任者又は各部門の情報セキュリティ責任者が担う場合についても情報セキュリティ対策に関する事務を総括する部門が、具体的な指示又は勧告の取りまとめを支援		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		する体制にすることが望ましい。		
57	1.2.2.2(2)(e)	最高情報セキュリティ責任者は、報告を受けた障害・事故等について、定められた対処手順に従って、府省庁内外の関係部門と情報共有を行うこと。		(新規追加)
58	1.2.2.2(2)(e) 解説	解説:障害・事故等が発生した場合に、府省庁内外の関係部門と情報を共有することで、被害の拡大防止策及び再発防止策が講じられるようにすることを求める事項である。 情報共有の枠組みとしては、「政府におけるサイバー攻撃等への対処態勢の強化について」(平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ)等で定めた連絡連携体制を利用すること。		(新規追加)
59	1.2.2.2(3)(a)	情報セキュリティ責任者は、障害・事故等が発生した場合には、障害・事故等に対応する責任者が実施した内容も踏まえ、障害・事故等の原因を調査するとともに再発防止策を策定し、その結果を報告書として最高情報セキュリティ責任者に報告すること。	1.2.2.2(3)(a)	情報セキュリティ責任者は、障害・事故等が発生した場合には、障害・事故等の原因を調査し再発防止策を策定し、その結果を報告書として最高情報セキュリティ責任者に報告すること。
60	1.2.2.2(3)(a) 解説	解説:情報セキュリティ責任者に対し、障害・事故等に対応する責任者が把握している障害・事故等の状況や実施した応急措置・復旧等の内容も踏まえて、障害・事故等の原因を究明し、それに基づき障害・事故等の再発防止策の策定を求める事項である。	1.2.2.2(3)(a) 解説	解説:情報セキュリティ責任者に対して、障害・事故等の原因を究明し、それに基づき障害・事故等の再発防止策を策定することを求める事項である。
61	1.2.2.2(4)	障害・事故等の発生するおそれがある場合の対処		(新規追加)
62	1.2.2.2(4)(a)	最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリ		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ティ責任者又は障害・事故等に対応する責任者は、障害・事故等の発生するおそれがある場合においては、本項の各遵守事項に準じて、必要な措置を講ずること。		
63	1.2.2.2(4)(a) 解説	解説：攻撃予告等により、インシデント等の発生するおそれがある場合については、それぞれの役割の者が、本項の各遵守事項に準じて必要な措置を講ずることを求める事項である。		(新規追加)
64	1.2.2.2(4)(b)	行政事務従事者は、障害・事故等の発生するおそれがある場合においては、前事項による報告手順や対処手順等に基づき、適切な措置を講ずること。		(新規追加)
65	1.2.2.2(4)(b) 解説	解説：攻撃予告等により、インシデント等の発生するおそれがある場合において、行政事務従事者は、前事項(1.2.2.2(4)(a))の規定に基づいて整備された報告手順や対処手順等に従い、適切な措置を講ずることを求める事項である。		(新規追加)
66	1.2.5.1(1)(b) 解説	解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。 統括情報セキュリティ責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、省庁対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。 選定基準としては、例えば、委託先が省庁対策基準の該当項目を遵守し得る者であること、省庁対策基準と同等の情報セキュリティ管理体制を整備	1.2.5.1(1)(b) 解説	解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。 統括情報セキュリティ責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、省庁対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。 選定基準としては、例えば、委託先が省庁対策基準の該当項目を遵守し得る者であること、省庁対策基準と同等の情報セキュリティ管理体制を整備

No.	統一管理基準(平成 24 年度改定版)		旧版	
		すること、省庁対策基準と同等の情報セキュリティ対策の教育を実施すること等が挙げられる。 また、府省庁の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を府省庁内で統一的に整備することが重要である。 委託先の選定基準策定に当たって、委託先の情報セキュリティ水準の評価方法を整備する際、例えば、ISO/IEC 27001 等に基づく認証制度の活用や、国際規格を踏まえ、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用も考えられる。その場合、委託先の情報セキュリティ水準の認証に関わる認定・認証機関について、これら機関がマネジメントシステム認証の信頼性向上を目的とした取組である「MS 認証信頼性向上イニシアティブ (http://www.jisc.go.jp/mss/other.html)」に参画し、不祥事への対応や透明性確保に係る取組を実施していることを確認することが望ましい。 なお、本基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施に反映することが必要である。		すること、省庁対策基準と同等の情報セキュリティ対策の教育を実施すること等が挙げられる。 また、府省庁の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を府省庁内で統一的に整備することが重要である。 なお、本基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施に反映することが必要である。
67		(1.2.5.1(1)(b) 解説へ移動)	1.2.5.1(1)(c)	統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
68		(1.2.5.1(1)(b) 解説へ移動)	1.2.5.1(1)(c) 解説	解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。評価方法の整備には、例えば、ISO/IEC 27001 等に基づく認証制度の活用や、国際規格を踏まえ、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用が考えられる。
69		(1.2.5.1(1)(b) 解説へ移動)	1.2.5.1(3)(b)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法に従って、委託先の候補者の情報セキュリティ水準を確認し、委託先の選定における評価の一要素として利用すること。
70		(1.2.5.1(1)(b) 解説へ移動)	1.2.5.1(3)(b) 解説	解説：国際規格を踏まえた委託先の情報セキュリティ水準の評価方法に基づく評価結果を、委託先の選定における評価の一要素として利用することを求める事項である。
71	1.2.5.1(4)(a) 解説	解説：情報セキュリティの観点から、外部委託に係る契約に含めるべき事項を定めた事項である。 機密保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報を守るべきであることから、これを記載する必要がある。 情報セキュリティ監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む、委託先と合意した事項を契約に含める。 サービスレベルに関しては、セキュリ	1.2.5.1(4)(a) 解説	解説：情報セキュリティの観点から、外部委託に係る契約に含めるべき事項を定めた事項である。 機密保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報を守るべきであることから、これを記載する必要がある。 情報セキュリティ監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む、委託先と合意した事項を契約に含める。 サービスレベルに関しては、セキュリ

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、事故発生時の対処方法等を決定し、委託先に保証させることが重要である。 情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。 なお、国の安全に関する重要な情報を委託先に扱わせることを内容とする外部委託契約については、「調達における情報セキュリティ要件の記載について」(平成 24 年 1 月 24 日、内閣官房副長官から各省庁大臣官房長等あて)に基づく情報セキュリティ要件を当該契約に含めること。		ティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、事故発生時の対処方法等を決定し、委託先に保証させることが重要である。 情報システムセキュリティ責任者又は課室情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼すること。
72	1.2.5.1(5)(a)	行政事務従事者は、委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。	1.2.5.1(5)(a)	行政事務従事者は、委託先に要保護情報又は重要な設計書を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。
73	1.2.5.2	1.2.5.2 業務継続計画及び情報システム運用継続計画との整合的運用の確保	1.2.5.2	1.2.5.2 業務継続計画との整合的運用の確保
74	1.2.5.2	府省庁においては、「中央省庁業務継続ガイドライン 第 1 版」(平成 19 年 6 月、内閣府)に基づき、業務の継続に重大な支障を来し、あるいは国民の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。また、「中央省庁における情報システ	1.2.5.2	府省庁においては、「中央省庁業務継続ガイドライン 第 1 版」(平成 19 年 6 月、内閣府)に基づき、業務の継続に重大な支障を来し、あるいは国民の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。他方では、業務継続計画の対象とする事

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ム運用継続計画ガイドライン」(平成 23 年 3 月、内閣官房情報セキュリティセンター）を活用し、必要な情報システムについて、運用を継続するために必要な計画（以下「情報システム運用継続計画」という。）を策定することが求められる。他方、業務継続計画及び情報システム運用継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、それぞれの府省庁の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画及び情報システム運用継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。 これらのことを勘案し、本項では、業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保並びに情報セキュリティ関係規程との間の不整合の報告に関する対策基準を定める。		態は、多くの場合に情報セキュリティを損なうものともなり、それぞれの府省庁の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。 これらのことを勘案し、本項では、業務継続計画と情報セキュリティ対策の整合的運用の確保及び不整合の報告に関する対策基準を定める。
75		(削除)	1.2.5.2	適用範囲
76		(削除)	1.2.5.2	「中央省庁業務継続ガイドライン 第 1 版」(平成 19 年 6 月、内閣府）に基づき、業務継続計画を整備し、又は整備を予定している府省庁に適用する。
77	1.2.5.2(1)	業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保	1.2.5.2(1)	業務継続計画と情報セキュリティ対策の整合性の確保
78	1.2.5.2(1)(a)	情報セキュリティ委員会は、府省庁において業務継続計画、情報システム運用継続計画又は省庁対策基準を整備	1.2.5.2(1)(a)	情報セキュリティ委員会は、府省庁において業務継続計画又は省庁対策基準を整備する場合には、業務継続計画

No.	統一管理基準(平成 24 年度改定版)		旧版	
		する場合には、業務継続計画及び情報システム運用継続計画と省庁対策基準との間の整合性の確保のための検討を行うこと。		と省庁対策基準との整合性の確保のための検討を行うこと。
79	1.2.5.2(1)(a) 解説	解説：業務継続計画、情報システム運用継続計画及び省庁対策基準は、それぞれの目的を達成するために、特定の事態に対して異なる対応が定められることも考えられる。当該事態の例として、情報システムの稼動を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画、情報システム運用継続計画及び省庁対策基準のそれぞれで定める対策に矛盾があると、それぞれの遵守を求められる府省庁組織及び行政事務従事者は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画及び情報システム運用継続計画と省庁対策基準との間で整合性を確保するよう検討を行うことが必要である。 本統一管理基準の 1.2.1.1 項で情報セキュリティ委員会は省庁対策基準の策定を求められているが、その策定及び見直しの際に、府省庁が業務継続計画及び情報システム運用継続計画で定め、又は定めることが予定されている要求事項を情報セキュリティ委員会が把握した上で、業務継続計画及び情報システム運用継続計画の整備を担当する者と協議しそれぞれが定め	1.2.5.2(1)(a) 解説	解説：業務継続計画と省庁対策基準は、特定の事態に対して、それぞれの体系において定められることがあり得る。当該事態の例として、情報システムの稼動を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画及び省庁対策基準のそれぞれで定める対策に矛盾があると、双方の遵守を求められる府省庁組織及び行政事務従事者は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画と省庁対策基準の間で整合性を確保するよう検討を行うことが必要である。 本統一管理基準の 1.2.1.1 項で情報セキュリティ委員会は省庁対策基準の策定を求められているが、その策定及び見直しの際に、府省庁が業務継続計画で定め、又は定めることが予定されている要求事項を情報セキュリティ委員会が把握した上で、業務継続計画の整備計画を担当する者と協議し双方の定めを調整する必要がある。また、業務継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が省庁対策基準に影響するかどうかを確認し、必要があれば、省庁対策基準の改訂を行う等して、業

No.	統一管理基準(平成 24 年度改定版)		旧版	
		る内容を調整する必要がある。また、業務継続計画及び情報システム運用継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が省庁対策基準に影響するかどうかを確認し、必要があれば、省庁対策基準の改訂を行う等して、業務継続計画及び情報システム運用継続計画との整合性の確保に努めなければならない。		務継続計画との整合の確保に努めなければならない。
80	1.2.5.2(1)(b)	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画及び情報システム運用継続計画を整備する場合には、全ての情報システムについて、当該業務継続計画及び情報システム運用継続計画との関係の有無を検討すること。	1.2.5.2(1)(b)	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画の整備計画がある場合には、全ての情報システムについて、当該業務継続計画との関係の有無を検討すること。
81	1.2.5.2(1)(b) 解説	解説：業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の整合性を確保する前提として、府省庁の情報システムのうち、業務継続計画及び情報システム運用継続計画と関係のある情報システムを特定することを求める事項である。	1.2.5.2(1)(b) 解説	解説：業務継続計画と情報セキュリティ関係規程との整合性を確保する前提として、府省庁の情報システムのうち、業務継続計画と関係のある情報システムを特定することを求める事項である。
82	1.2.5.2(1)(c)	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画及び情報システム運用継続計画を整備する場合には、当該業務継続計画及び情報システム運用継続計画と関係があると認めた情報システ	1.2.5.2(1)(c)	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁において業務継続計画の整備計画がある場合には、当該業務継続計画と関係があると認めた情報システムについて、以下に従って、業務継続計画と省庁対策基準に

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ムについて、業務継続計画及び情報システム運用継続計画との整合性を考慮し、必要な措置を講ずること。		基づく共通の実施手順を整備すること。
83	1.2.5.2(1)(c) (ア)	通常時において業務継続計画及び情報システム運用継続計画と省庁対策基準との整合的運用が可能となるよう必要な措置を講ずること。	1.2.5.2(1)(c) (ア)	通常時において業務継続計画と省庁対策基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。
84	1.2.5.2(1)(c) (ア) 解説	解説：例えば、事態発生時には、業務の継続以外の対応として、府省庁の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障を来すおそれがある。このため、セキュリティ確保の面で配慮を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、施設全体の入館管理だけでなく、各執務室や各行政事務従事者の卓上の情報セキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。 また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ずる必要がある。	1.2.5.2(1)(c) (ア) 解説	解説：例えば、事態発生時には、業務の継続以外の対応として、府省庁の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障をきたすおそれがある。このため、セキュリティ確保の面で配慮を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、施設全体の入館管理だけでなく、各執務室や各行政事務従事者の卓上の情報セキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。 また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ずる必要がある。
85	1.2.5.2(1)(c) (イ)	事態発生時において業務継続計画、情報システム運用継続計画及び省庁対策基準との整合的運用が可能となるよう実施手順の整備等の必要な措置を講ずること。	1.2.5.2(1)(c) (イ)	事態発生時において業務継続計画と省庁対策基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定を整備すること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
86	1.2.5.2(1)(c) (イ) 解説	解説：事態発生への対応として、業務継続計画、情報システム運用継続計画及び省庁対策基準のそれぞれにおいて事態発生時における情報システムの稼動水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対応を実施手順において具体的に定めることとなるため、相互の整合性を確保するための実施手順の整備が必要となる。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。 また、事態発生時には、情報システムの主体認証情報（パスワード）を設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。しかしながら、個人が管理しているパスワードの共用(共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。このような事態発生時の手順については、業務継続計画及び情報システム運用継続計画で安易に定めるのではなく、事態発生時においても必要な情報セキュリティを確保するために、省庁対策基準において事態発生時の実施手順とし	1.2.5.2(1)(c) (イ) 解説	解説：統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に、業務継続計画と自らが担当する実施手順の整合性の確保を求める事項である。整合性を確保するための対応には、通常時の運用において実施するものと、事態発生時に実施するものがある。事態発生への対応として、業務継続計画及び省庁対策基準のそれぞれにおいて事態発生時における情報システムの稼動水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対策を実施手順において具体的に定める等が想定される。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。 これらの目標及び対策を業務継続計画及び情報セキュリティ関係規程の双方で定めることとなるため、相互の整合性を確保するための規定の整備が必要となる。 また、事態発生時には、情報システムの主体認証情報（パスワード）を設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。しかしながら、個人が管理しているパスワードの共用(共用識別

No.	統一管理基準(平成 24 年度改定版)	旧版
	て整備する必要がある。 手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生時用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容を記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。	コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。このため、個人が管理しているパスワードを聞き出したり、共用するために管理者において控えを管理する手順を業務継続計画で安易に認めるべきではなく、これに代わる手順を十分検討する必要がある。 手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、ついで、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生時用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容を記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無の確認が可能となる。なお、このよ

No.	統一管理基準(平成 24 年度改定版)		旧版	
				うな手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。
87	1.2.5.2(2)	業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の不整合の報告	1.2.5.2(2)	業務継続計画と情報セキュリティ関係規程の不整合の報告
88	1.2.5.2(2)(a)	行政事務従事者は、府省庁において業務継続計画及び情報システム運用継続計画と整備する場合であって、業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。	1.2.5.2(2)(a)	行政事務従事者は、府省庁において業務継続計画の整備計画がある場合であって、業務継続計画と情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害・事故等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。
89	1.2.5.2(2)(a) 解説	解説：本来、業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程が定める要求事項との間の整合性については、上記(1)の遵守事項を適正に実施することで担保されるものである。しかしながら、情報セキュリティ関係規程との間では、業務継続計画及び情報システム運用継続計画の対象となる状況においては、事前に想定していなかった様々な不整合が発生すると考えられる。業務継続計画の重要性を考慮すると、万が一、不整合について、情報セキュリティ委員会等が事前に想定できなかった場合にも、それを迅速に改善できるようにしておくべきである。	1.2.5.2(2)(a) 解説	解説：本来、業務継続計画と情報セキュリティ関係規程が定める要求事項との整合性については、上記(1)及び(2)の遵守事項を適正に実施することで担保されるものである。しかしながら、業務継続計画の対象となる状況においては、事前に想定していなかった様々な不整合が発生すると考えられる。業務継続計画の重要性を考慮すると、万が一、不整合について、情報セキュリティ委員会等が事前に想定できなかった場合にも、それを迅速に改善できるようにしておくべきである。
90	1.2.5.3	1.2.5.3 情報取扱区域		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
91	1.2.5.3	趣旨(必要性) 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。 これらのことを勘案し、本項では、情報取扱区域にクラスの区分を設け、クラスに応じた管理及び利用を行うための対策基準として、情報取扱区域のクラス、管理及び利用制限の決定、情報取扱区域の管理並びに情報取扱区域における利用制限についての遵守事項を定める。		(新規追加)
92	1.2.5.3(1)	情報取扱区域のクラス、管理及び利用制限の決定		(新規追加)
93	1.2.5.3(1)(a)	統括情報セキュリティ責任者は、情報取扱区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限対策を決定すること。なお、決定する内容は、統一技術基準 2.3.1.1（別表 1 及び別表 2 を含む。）に定める。		(新規追加)
94	1.2.5.3(1)(a) 解説	解説：情報取扱区域にクラスの区分を設け、各クラスの利用用途に応じたセキュリティの確保を求めるための事		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		項である。		
95	1.2.5.3(1)(b)	情報セキュリティ責任者は、要管理対策区域については、当該区域を管理又は利用する行政事務従事者がクラスについて認識できる措置を講ずること。		(新規追加)
96	1.2.5.3(1)(b) 解説	解説:決定された情報取扱区域のクラス区分について共通の認識となるように措置することで、クラスに応じた管理対策及び利用制限対策が講じられるようにするための事項である。 「認識できる措置」には、A.1.5 情報取扱区域のクラスと区域例の内容を参考に各府省庁で定めた内容を周知する、区域ごとにクラスを掲示する、若しくは当該区域で情報を取り扱う際に必要な利用制限対策を掲示又は周知する等が考えられる。 なお、関係者限りで管理及び利用する区域については、関係者のみにクラスを周知することでも構わない。		(新規追加)
97	1.2.5.3(1)(c)	区域情報セキュリティ責任者は、個別の管理対策及び利用制限対策を決定する必要性の有無を検討し、必要と認めた場合は、当該対策を決定し、統括情報セキュリティ責任者に報告すること。		(新規追加)
98	1.2.5.3(1)(c) 解説	解説:決定したクラスの区域において、必要な対策が不足していると認められる区域、又は定められたクラスとは別の区分で対策を講ずる必要がある区域があるときは、求める情報セキュリティ水準を確保又は向上させるために、定められたクラス別管理及び利用制限にかかわらず、当該区域ごと		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		に個別に管理対策及び利用制限対策を決定することを求める事項である。		
99	1.2.5.3(2)	情報取扱区域の管理		(新規追加)
100	1.2.5.3(2)(a)	区域情報セキュリティ責任者は、要管理対策区域を管理する場合には、統括情報セキュリティ責任者が定めた当該区域のクラスを確認し、統一技術基準 2.3.1.1（別表 1 を含む。）に定める管理対策を講ずること。また、個別の管理対策を決定している場合には、同様に対策を講ずること。		(新規追加)
101	1.2.5.3(2)(a) 解説	解説：区域情報セキュリティ責任者が要管理対策区域を管理する場合に、当該区域で求められる管理対策を講ずることを求める事項である。 個別の管理対策については、A.1.6 情報取扱区域の個別管理及び利用制限の付表例を参照。		(新規追加)
102	1.2.5.3(3)	情報取扱区域における利用制限		(新規追加)
103	1.2.5.3(3)(a)	区域情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた情報取扱区域のクラスを確認し、統一技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策を講ずること。なお、個別に利用制限対策を決定している場合には、同様に講ずること。		(新規追加)
104	1.2.5.3(3)(a) 解説	解説：区域情報セキュリティ責任者が当該区域で求められる利用制限対策を講ずることを求める事項である。		(新規追加)
105	1.2.5.3(3)(b)	行政事務従事者は、情報を取り扱う場合には、統括情報セキュリティ責任者が定めた情報取扱区域のクラスを確認し、統一技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策に従って利用すること。なお、個別の利用		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		制限対策を決定している場合には、同様に従うこと。		
106	1.2.5.3(3)(b) 解説	解説：行政事務従事者が要管理対策区域を利用する場合に、当該区域で求められる利用制限対策に従って利用することを求める事項である。 なお、行政事務従事者が府省庁外の者を立ち入らせる際に、当該区域で求められる利用制限対策に従って利用させることも含まれる。 個別の利用制限対策については、A.1.6 情報取扱区域の個別管理及び利用制限の付表例を参照。		(新規追加)
107	1.3.1.1(2)(a) 解説	解説：作成又は入手した情報について、以降、適切な情報セキュリティ対策が実施されるように、機密性、完全性及び可用性の格付及び取扱制限を決定することを求める事項である。 情報の格付が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障害・事故等の直接の原因となった人物のほか、情報の格付及び明示等を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、行政事務従事者が、情報の格付及び取扱制限とその明示等を確実に行うことは重要である。 なお、格付及び取扱制限の決定をする際は、要件に過不足が生じないように十分注意しなければならない。格付及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適	1.3.1.1(2)(a) 解説	解説：作成又は入手した情報について、以降、適切な情報セキュリティ対策が実施されるように、機密性、完全性及び可用性の格付及び取扱制限を決定することを求める事項である。 情報の格付が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障害・事故等の直接の原因となった人物のほか、情報の格付及び明示等を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、行政事務従事者が、情報の格付及び取扱制限とその明示等を確実に行うことは重要である。 なお、格付及び取扱制限の決定をする際は、要件に過不足が生じないように十分注意しなければならない。格付及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適

No.	統一管理基準(平成 24 年度改定版)		旧版	
		切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなって事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを行政事務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。 特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。 例えば、本来要機密情報とする情報を要機密情報に決定しないことは不適切であるが、逆に、本来要機密情報ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に決定することも不適切であることに注意すること。 また、取扱制限については必要性の有無を検討し、その結果指定しないという決定を行っても差し支えない。 電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から、格付及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定(取扱制限については必要性の有無を含む。）をし、決定した格付及び取扱制限に基づき、その指定を行うこと。 なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。		切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなって事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを行政事務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。 特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。 例えば、本来要機密情報とする情報を要機密情報に格付けないことは不適切であるが、逆に、本来要機密情報ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けることも不適切であることに注意すること。 また、取扱制限については必要性の有無を検討し、その結果指定しないという決定を行っても差し支えない。 電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から、格付及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定(取扱制限については必要性の有無を含む。）をし、決定した格付及び取扱制限に基づき、その指定を行うこと。 なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。
108	1.3.1.2(5)(a)	行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を要管理対策	1.3.1.2(5)(a)	行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を府省庁外に

No.	統一管理基準(平成 24 年度改定版)		旧版	
		区域外に持ち出さないこと。		持ち出さないこと。
109	1.3.1.2(5)(a) 解説	解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、行政事務従事者が行政事務の遂行以外の目的で要保護情報を要管理対策区域外へ持ち出すことを禁止する事項である。 なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。	1.3.1.2(5)(a) 解説	解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、行政事務従事者が行政事務の遂行以外の目的で要保護情報を府省庁外へ持ち出すことを禁止する事項である。 なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。
110	1.3.1.2(5)(e)	行政事務従事者は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。	1.3.1.2(5)(e)	行政事務従事者は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。
111	1.3.1.2(5)(f)	行政事務従事者は、情報を機密性３情報と決定した書面のうち、必要なものには、一連番号を付し、その所在を明らかにしておくこと。	1.3.1.2(5)(f)	行政事務従事者は、機密性３情報である書面には、一連番号を付し、その所在を明らかにしておくこと。
112	1.3.1.3(1)(a) 解説	解説：電磁的記録媒体に保存された情報、書面に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切に保存することを求める事項である。 例えば、行政事務従事者が書面を保存する場合は、要管理対策区域内の棚に保存したり、必要なく情報の参照等をさせないために、施錠のできる書庫・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報(パスワード）によるロック機能を利用して、当該媒体の利用を防止するこ	1.3.1.3(1)(a) 解説	解説：電磁的記録媒体に保存された情報、書面又は重要な設計書に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切に保存することを求める事項である。 例えば、行政事務従事者が書面又は重要な設計書を保存する場合は、安全区域内の棚に保存したり、必要なく情報の参照等をさせないために、施錠のできる書庫・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報(パスワード）によるロック機能を利用して、当該媒体の利用を防止

No.	統一管理基準(平成 24 年度改定版)		旧版	
		とが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。 一方、行政事務従事者が要保護情報に関する情報処理を行う場合は、例えば、要管理対策区域内に設置された情報システム上に保存すること等が考えられる。また、行政事務従事者が許可を得て、個人で利用する ASP・SaaS サービスの外部の情報システムを用いて、要保護情報に関する情報処理を行う場合は、省庁対策基準と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。		することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。 一方、行政事務従事者が要保護情報に関する情報処理を行う場合は、例えば、安全区域に設置された情報システム上に保存すること等が考えられる。また、行政事務従事者が許可を得て、個人で利用する ASP・SaaS サービスの外部の情報システムを用いて、要保護情報に関する情報処理を行う場合は、省庁対策基準と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。
113	1.3.1.4(1)(a)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を移送する場合には、課室情報セキュリティ責任者の許可を得ること。	1.3.1.4(1)(a)	行政事務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する場合には、課室情報セキュリティ責任者の許可を得ること。
114	1.3.1.4(1)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報を移送する際に課室情報セキュリティ責任者の許可を求める事項である。 なお、機密性３情報、完全性２情報又は可用性２情報を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望まし	1.3.1.4(1)(a) 解説	解説：機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する際に課室情報セキュリティ責任者の許可を求める事項である。 なお、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、

No.	統一管理基準(平成 24 年度改定版)		旧版	
		い。		情報の保護対策に関して、手続を定めておくことが望ましい。
115	1.3.1.4(3)(a)	行政事務従事者は、要保護情報を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。	1.3.1.4(3)(a)	行政事務従事者は、要保護情報又は重要な設計書を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。
116	1.3.1.4(3)(a) 解説	解説：多種多様な移送手段の中から要保護情報を安全に移送するための手段の選択を求める事項である。 「移送手段」とは、送信については府省庁内通信回線、信頼できるプロバイダ、VPN 及び暗号メール(S/MIME)等、運搬については信頼できる運送業者や、情報セキュリティ責任者が指定する運送役務及び行政事務従事者自らによる携行等が挙げられる。なお、「S/MIME(Secure Multipurpose Internet Mail Extensions)」とは、電子メールの暗号化の方式の１つである。 また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。	1.3.1.4(3)(a) 解説	解説：多種多様な移送手段の中から要保護情報又は重要な設計書を安全に移送するための手段の選択を求める事項である。 「移送手段」とは、送信については府省庁内通信回線、信頼できるプロバイダ、VPN 及び暗号メール(S/MIME)等、運搬については信頼できる運送業者や、情報セキュリティ責任者が指定する運送役務及び行政事務従事者自らによる携行等が挙げられる。なお、「S/MIME(Secure Multipurpose Internet Mail Extensions)」とは、電子メールの暗号化の方式の１つである。 また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。
117	1.3.1.4(4)(a) 解説	解説：要機密情報が記録又は記載された記録媒体を運搬する場合における情報セキュリティ対策を求める事項	1.3.1.4(4)(a) 解説	解説：要機密情報が記録又は記載された記録媒体を運搬する場合における情報セキュリティ対策を求める事項

No.	統一管理基準(平成 24 年度改定版)		旧版	
		である。 行政事務従事者は、外部電磁的記録媒体、PC、書面等を運搬する場合には、例えば、外見ではその内容が要機密情報であると知られないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。		である。 行政事務従事者は、外部電磁的記録媒体、PC、書面又は重要な設計書等を運搬する場合には、例えば、外見ではその内容が要機密情報であると知られないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。
118	1.3.1.4(5)(f)	行政事務従事者は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用い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。	1.3.1.4(5)(f)	行政事務従事者は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること。
119	1.3.1.5(2)(a)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を府省庁外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	1.3.1.5(2)(a)	行政事務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を府省庁外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。
120	1.3.1.5(2)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報を府省庁外の者に提供する際に課室情報セキュリティ責任者の許可を得ることを求める事項である。	1.3.1.5(2)(a) 解説	解説：機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を府省庁外の者に提供する際に課室情報セキュリティ責任者の許可を得ることを求める事項である。
121	1.3.1.5(2)(c)	行政事務従事者は、要保護情報を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。	1.3.1.5(2)(c)	行政事務従事者は、要保護情報又は重要な設計書を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。
122	1.3.1.5(2)(c) 解説	解説：要保護情報を府省庁外の者に提供する場合において遵守すべきこと	1.3.1.5(2)(c) 解説	解説：要保護情報又は重要な設計書を府省庁外の者に提供する場合におい

No.	統一管理基準(平成 24 年度改定版)	旧版
	を定める事項である。 要保護情報を府省庁外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。 確実に伝達する方法として、提供先が統一管理基準及び統一技術基準に準じた組織の場合には、統一管理基準及び統一技術基準による情報の格付及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付の区分だけを示すのでは不十分である。なぜなら、提供先においては当該格付区分がどのように取り扱われるべきものであるかが認識できないからである。格付の区分（例えば、「機密性２」と記載する）で示すのであれば、当該格付の区分の定義について提供先にあらかじめ周知しておくか、格付の区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す(例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要	て遵守すべきことを定める事項である。 要保護情報又は重要な設計書を府省庁外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。 確実に伝達する方法として、提供先が統一管理基準及び統一技術基準に準じた組織の場合には、統一管理基準及び統一技術基準による情報の格付及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付の区分だけを示すのでは不十分である。なぜなら、提供先においては当該格付区分がどのように取り扱われるべきものであるかが認識できないからである。格付の区分（例えば、「機密性２」と記載する）で示すのであれば、当該格付の区分の定義について提供先にあらかじめ周知しておくか、格付の区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す(例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載

No.	統一管理基準(平成 24 年度改定版)		旧版	
		がある。 行政事務従事者は、格付及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付及び取扱制限に従った取扱いを確保するため、提供する前に、明記が不要とされている情報の格付及び取扱制限を当該書面又は電磁的記録に明記すること。		する等の方法によって伝達する必要がある。 行政事務従事者は、格付及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付及び取扱制限に従った取扱いを確保するため、提供する前に、明記が不要とされている情報の格付及び取扱制限を当該書面又は電磁的記録に明記すること。
123	1.3.1.6(1)(c)	行政事務従事者は、電磁的記録媒体について、設置環境等から要機密情報を抹消する必要性の有無を検討し、必要と認めたときは、当該電磁的記録媒体の要機密情報を抹消すること。	1.3.1.6(1)(c)	行政事務従事者は、電磁的記録媒体について、設置環境等から必要があると認められる場合は、当該電磁的記録媒体の要機密情報を抹消すること。
124	1.4.1.1	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。 なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する	1.4.1.1	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。 なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策

No.	統一管理基準(平成 24 年度改定版)		旧版	
		対策基準を定めている。		基準を定めている。
125	1.4.1.1(1)(e)	情報システムセキュリティ責任者は、管理者権限を持つ識別コードを付与された行政事務従事者に、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させる必要性の有無を検討し、必要と認めたときは、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させること。		(新規追加)
126	1.4.1.1(1)(e) 解説	解説：行政事務従事者に、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、利用させることを求める事項である。 なお、本遵守事項は、実際には行政事務従事者が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、当該情報システムで取り扱う情報の重要性等を勘案し、必要に応じて選択されたい。		(新規追加)
127	1.4.1.1(1)(f)	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、かつ情報システムセキュリティ責任者が求めた場合には、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。	1.4.1.1(1)(e)	行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。
128	1.4.1.1(1)(f) 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 の設定変更等をしないときには、administrator 権限なし	1.4.1.1(1)(e) 解説	解説：管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用することを求める事項である。 例えば、情報システムのオペレーティングシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更等をしないときには、administrator 権限なし

No.	統一管理基準(平成 24 年度改定版)		旧版	
		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。		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、本遵守事項は、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、当該情報システムで取り扱う情報の重要性等を勘案し、必要に応じて選択されたい。
129	1.4.1.1(2)(c) (ア) 解説	解説：行政事務従事者は、例えば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。 また、主体認証情報を、容易に他者に知られてしまう状態で、主体認証を行う情報システムとは異なる情報システムに記憶させないこと。	1.4.1.1(2)(c) (ア) 解説	解説：行政事務従事者は、例えば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。
130	1.4.1.1(2)(c) (オ)	異なる識別コードに対して、共通の主体認証情報を用いないこと。		(新規追加)
131	1.4.1.1(2)(c) (オ) 解説	解説：行政事務従事者が付与された複数の識別コードで共通の主体認証情報を用いていると、一つの識別コードに対応する主体認証情報が漏えいした場合に、他方の識別コードを用いた不正アクセスを受ける危険性が高くなるため、共通の主体認証情報を用いないことを求める事項である。複数の識別コードの権限レベルが異なって		(新規追加)

No.	統一管理基準(平成 24 年度改定版)		旧版	
		いたり、複数の識別コードを用いる情報システムのセキュリティレベルが異なっていたりする場合、低いレベルの主体認証情報の漏えいにより、高いレベルの権限や高いセキュリティレベルの情報システムが正規の主体認証方式を用いて容易に不正アクセスされないようにすることを求めている。対象となる識別コードには、府省庁支給の情報システムだけでなく、府省庁支給以外の情報システムで使用している識別コードも含める必要がある。 なお、シングルサインオンシステム等、一組の識別コード及び主体認証情報を用いて複数のシステムの利用を可能とするシステムは、当該複数システム間のそれぞれの主体認証情報が異なっていれば、本項目が想定する脅威は存在しないため、共通の主体認証情報を用いたことにはならない。		
132	1.4.1.1(2)(c) (カ) 解説	解説：定期的な変更の要求を自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達する等の運用によって対処することでも差し支えない。 なお、例えば、主体認証やその後の情報システムにおける処理を自動的に行うと、定期的な変更の際に、それらの処理をその都度修正する必要があることに注意すること。	1.4.1.1(2)(c) (オ) 解説	解説：定期的な変更の要求を自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達する等の運用によって対処することでも差し支えない。
133	1.4.2.1	1.4.2.1 要管理対策区域外での情報処理の制限	1.4.2.1	1.4.2.1 府省庁外での情報処理の制限
134	1.4.2.1	行政事務においては、その事務の遂行のため、要管理対策区域外において情	1.4.2.1	行政事務においては、その事務の遂行のため、府省庁外において情報処理を

No.	統一管理基準(平成 24 年度改定版)		旧版	
		報処理を実施する必要が生ずる場合がある。この際、要管理対策区域外での実施では物理的な安全対策を講ずることが比較的困難になることから、行政事務従事者は、要管理対策区域内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。 これらのことを勘案し、本項では、要管理対策区域外での情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。		実施する必要が生ずる場合がある。この際、府省庁外での実施では物理的な安全対策を講ずることが比較的困難になることから、行政事務従事者は、庁舎内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。 これらのことを勘案し、本項では、府省庁外での情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。
135	1.4.2.1(1)(a)	統括情報セキュリティ責任者は、要保護情報について要管理対策区域外での情報処理を行う場合の安全管理措置についての規定を整備すること。	1.4.2.1(1)(a)	統括情報セキュリティ責任者は、要保護情報について府省庁外での情報処理を行う場合の安全管理措置についての規定を整備すること。
136	1.4.2.1(1)(a) 解説	解説：統括情報セキュリティ責任者が、要管理対策区域外において情報処理を行う場合の安全管理措置についての規定を整備することを求める事項である。ただし、情報処理の種類により個別の規定を設けても構わない。要管理対策区域外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通した通信の形態、関与する府省庁内外の者等に応じた措置を示した規定を整備する必要がある。	1.4.2.1(1)(a) 解説	解説：統括情報セキュリティ責任者が、府省庁外において情報処理を行う場合の安全管理措置についての規定を整備することを求める事項である。ただし、情報処理の種類により個別の規定を設けても構わない。府省庁外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通した通信の形態、関与する府省庁内外の者等に応じた措置を示した規定を整備する必要がある。
137	1.4.2.1(1)(b)	統括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を要管理対策区域外に持ち出す場合の安全管理措置についての規定を整備すること。	1.4.2.1(1)(b)	統括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を府省庁外に持ち出す場合の安全管理措置についての規定を整備すること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
138	1.4.2.1(1)(b) 解説	解説：統括情報セキュリティ責任者が、要管理対策区域外に要保護情報を取り扱う情報システムを持ち出す場合の安全管理措置についての規定を整備することを求める事項である。持ち出す情報システム及び持ち出し先等を具体的に想定して規定を整備する必要がある。	1.4.2.1(1)(b) 解説	解説：統括情報セキュリティ責任者が、府省庁外に要保護情報を取り扱う情報システムを持ち出す場合の安全管理措置についての規定を整備することを求める事項である。持ち出す情報システム及び持ち出し先等を具体的に想定して規定を整備する必要がある。
139	1.4.2.1(2)(a)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	1.4.2.1(2)(a)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。
140	1.4.2.1(2)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報に係る情報処理を要管理対策区域外で行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。 なお、「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。	1.4.2.1(2)(a) 解説	解説：機密性３情報、完全性２情報又は可用性２情報に係る情報処理を府省庁外で行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については課室情報セキュリティ責任者の、当該情報処理の安全性については情報システムセキュリティ責任者の許可を得ることとなる。 なお、「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。
141	1.4.2.1(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室	1.4.2.1(2)(b)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外で情報処理を行う場合には、情報システムセキュリティ責任者及び課室情報セキ

No.	統一管理基準(平成 24 年度改定版)		旧版	
		情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。		ュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。
142	1.4.2.1(2)(b) 解説	解説：要管理対策区域外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。	1.4.2.1(2)(b) 解説	解説：府省庁外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない府省庁外での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。
143	1.4.2.1(2)(c)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、要管理対策区域外での要保護情報の情報処理に係る記録を取得すること。	1.4.2.1(2)(c)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁外での要保護情報の情報処理に係る記録を取得すること。
144	1.4.2.1(2)(c) 解説	解説：要管理対策区域外での要保護情報の情報処理に係る記録を取得することを求める事項である。 「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。	1.4.2.1(2)(c) 解説	解説：府省庁外での要保護情報の情報処理に係る記録を取得することを求める事項である。 「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。
145	1.4.2.1(2)(d)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者か	1.4.2.1(2)(d)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について府省庁外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了し

No.	統一管理基準(平成 24 年度改定版)		旧版	
		ら終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。		た旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。
146	1.4.2.1(2)(d) 解説	解説：要管理対策区域外での情報処理を行うことを許可した期間が終了した時に報告の有無を確認し、措置を講ずること等を求める事項である。 状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。	1.4.2.1(2)(d) 解説	解説：府省庁外での情報処理を行うことを許可した期間が終了した時に報告の有無を確認し、措置を講ずること等を求める事項である。 状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。
147	1.4.2.1(2)(e)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。	1.4.2.1(2)(e)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。
148	1.4.2.1(2)(e) 解説	解説：機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば行政事務従事者に改めて届出をさせる等の措置を講ずることを求める事項である。	1.4.2.1(2)(e) 解説	解説：機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば行政事務従事者に改めて届出をさせる等の措置を講ずることを求める事項である。
149	1.4.2.1(2)(f)	行政事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。	1.4.2.1(2)(f)	行政事務従事者は、要保護情報について府省庁外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
150	1.4.2.1(2)(f) 解説	解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を要管理対策区域外で情報処理することを最小限にとどめることを求める事項である。	1.4.2.1(2)(f) 解説	解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を府省庁外で情報処理することを最小限にとどめることを求める事項である。
151	1.4.2.1(2)(g)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	1.4.2.1(2)(g)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。
152	1.4.2.1(2)(g) 解説	解説：機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該持ち出しの業務上の必要性については課室情報セキュリティ責任者の、当該持ち出しの安全性については情報システムセキュリティ責任者の許可を得ることとなる。	1.4.2.1(2)(g) 解説	解説：機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該持ち出しの業務上の必要性については課室情報セキュリティ責任者の、当該持ち出しの安全性については情報システムセキュリティ責任者の許可を得ることとなる。
153	1.4.2.1(2)(h)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。	1.4.2.1(2)(h)	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを府省庁外に持ち出す場合には、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に届け出ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。
154	1.4.2.1(2)(h) 解説	解説：機密性２情報であって完全性１情報かつ可用性１情報である情報を	1.4.2.1(2)(h) 解説	解説：機密性２情報であって完全性１情報かつ可用性１情報である情報を

No.	統一管理基準(平成 24 年度改定版)		旧版	
		取り扱う情報システムを要管理対策区域外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外への持ち出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。		取り扱う情報システムを府省庁外に持ち出す行政事務従事者に、情報システムセキュリティ責任者と課室情報セキュリティ責任者の両方に届け出ることを求める事項である。また、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない府省庁外への持ち出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。
155	1.4.2.1(2)(i)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得すること。	1.4.2.1(2)(i)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、要保護情報を取り扱う情報システムの府省庁外への持ち出しに係る記録を取得すること。
156	1.4.2.1(2)(i) 解説	解説：要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得することを求める事項である。 「持ち出しに係る記録」には、持ち出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。	1.4.2.1(2)(i) 解説	解説：要保護情報を取り扱う情報システムの府省庁外への持ち出しに係る記録を取得することを求める事項である。 「持ち出しに係る記録」には、持ち出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。
157	1.4.2.1(2)(j)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この	1.4.2.1(2)(j)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでな

No.	統一管理基準(平成 24 年度改定版)		旧版	
		限りでない。		い。
158	1.4.2.1(2)(j) 解説	解説：情報システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に報告の有無を確認すること等を求める事項である。 状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。	1.4.2.1(2)(j) 解説	解説：情報システムを府省庁外に持ち出すことを許可した期間が終了した時に報告の有無を確認すること等を求める事項である。 状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、行政事務従事者に改めて許可を得るようにさせること。
159	1.4.2.1(2)(k)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを要管理対策区域外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。	1.4.2.1(2)(k)	情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを府省庁外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。
160	1.4.2.1(2)(k) 解説	解説：届出期間が長期にわたる場合等、必要に応じて、要管理対策区域外への持ち出しの状況を確認することを求める事項である。 状況を確認した際に、期間の延長が必要な状況であれば、行政事務従事者に改めて届出をさせること。	1.4.2.1(2)(k) 解説	解説：届出期間が長期にわたる場合等、必要に応じて、府省庁外への持ち出しの状況を確認することを求める事項である。 状況を確認した際に、期間の延長が必要な状況であれば、行政事務従事者に改めて届出をさせること。
161	1.4.2.1(2)(l)	行政事務従事者は、要保護情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持ち出しにとどめること。	1.4.2.1(2)(l)	行政事務従事者は、要保護情報を取り扱う情報システムを府省庁外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持ち出しにとどめること。
162	1.4.2.1(2)(l) 解説	解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を取り扱うシステムを要管理対策区域外に持ち出すことを最小限にとどめることを求める事項である。	1.4.2.1(2)(l) 解説	解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を取り扱うシステムを府省庁外に持ち出すことを最小限にとどめることを求める事項である。

No.	統一管理基準(平成 24 年度改定版)		旧版	
163	1.4.2.1(3)(a)	行政事務従事者は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずること。	1.4.2.1(3)(a)	行政事務従事者は、要保護情報について府省庁外での情報処理について定められた安全管理措置を講ずること。
164	1.4.2.1(3)(a) 解説	解説：行政事務従事者に対して、要管理対策区域外での情報処理について定められた安全管理措置を講ずることを求める事項である。	1.4.2.1(3)(a) 解説	解説：行政事務従事者に対して、府省庁外での情報処理について定められた安全管理措置を講ずることを求める事項である。
165	1.4.2.1(3)(b)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。	1.4.2.1(3)(b)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。
166	1.4.2.1(3)(b) 解説	解説：行政事務従事者に対して、要管理対策区域外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。	1.4.2.1(3)(b) 解説	解説：行政事務従事者に対して、府省庁外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。
167	1.4.2.1(3)(c)	行政事務従事者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずること。	1.4.2.1(3)(c)	行政事務従事者は、要保護情報を取り扱う情報システムの府省庁外への持ち出しについて定められた安全管理措置を講ずること。
168	1.4.2.1(3)(c) 解説	解説：行政事務従事者に対して、情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずることを求める事項である。 定められた安全管理措置の内容としては、例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、	1.4.2.1(3)(c) 解説	解説：行政事務従事者に対して、情報システムの府省庁外への持ち出しについて定められた安全管理措置を講ずることを求める事項である。 定められた安全管理措置の内容としては、例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、操作を実施できなくすること等が考

No.	統一管理基準(平成 24 年度改定版)		旧版	
		操作を実施できなくすること等が考えられる。		えられる。
169	1.4.2.1(3)(d)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを要管理対策区域外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。	1.4.2.1(3)(d)	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。
170	1.4.2.1(3)(d) 解説	解説：行政事務従事者に対して、要管理対策区域外へ情報システムの持ち出しが終了したことを、その許可を与えた者に報告することを求める事項である。	1.4.2.1(3)(d) 解説	解説：行政事務従事者に対して、府省庁外へ情報システムの持ち出しが終了したことを、その許可を与えた者に報告することを求める事項である。
171	1.4.2.2(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府省庁支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に確認すること。	1.4.2.2(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府省庁支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に直接確認すること。
172	1.5.1.1(1)(b)	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。この場合、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の活用又はそれと同等以上の検討を行った上で決定すること。また、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」に基づき決定すること。	1.5.1.1(1)(b)	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。この場合、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」に基づき決定すること。
173	1.5.1.1(1)(b) 解説	解説：情報システムに求められる要求事項のうち、セキュリティに関わる要	1.5.1.1(1)(b) 解説	解説：情報システムに求められる要求事項のうち、セキュリティに関わる要

No.	統一管理基準(平成 24 年度改定版)	旧版
	求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。 「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。 具体的なセキュリティ要件については、省庁対策基準において統一技術基準に対応して定められた事項、本統一管理基準の「1.5.2　情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。この実施においては、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の活用又はそれと同等以上の検討結果を最低限のセキュリティ対策水準であると考え、これを踏まえてセキュリティ要件を決定すること。 決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。	求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。 「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。 具体的なセキュリティ要件については、省庁対策基準において統一技術基準に対応して定められた事項、本統一管理基準の「1.5.2　情報システムに係る規定の整備と遵守」に対応するものも含めた府省庁の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。 決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。 また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが発生しないようにすること。 なお、物理的に分割されたシステムに

No.	統一管理基準(平成 24 年度改定版)		旧版	
		また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが発生しないようにすること。 なお、物理的に分割されたシステムに限らず、論理的に分割されたシステムも同様に考慮すること。「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筐体上に複数のシステムを共存させることを目的として、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。		限らず、論理的に分割されたシステムも同様に考慮すること。「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筐体上に複数のシステムを共存させることを目的として、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。
174	1.5.1.1(1)(d)	情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。	1.5.1.1(1)(d)	情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性の有無を検討し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。
175	1.5.1.1(1)(e) 解説	解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。情報セキュリティの侵害とは、	1.5.1.1(1)(e) 解説	解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。情報セキュリティの侵害とは、

No.	統一管理基準(平成 24 年度改定版)	旧版
	要保護情報について機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。 監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、府省庁の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の要管理対策区域への立入り等があり得る。 また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。 （1）設ける監視機能を定める。監視機能には、以下の例がある。 ・府省庁外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能(侵入検知システム等による) ・不正プログラム感染や踏み台に利用されること等による府省庁外への不正な通信を監視する機能 ・府省庁内通信回線への PC の接続を監視する機能 ・PC への外部記録媒体の挿入を監視する機能 ・サーバ装置等の機器の正常な動作を監視する機能 ・要管理対策区域への入退出を監視す	要保護情報について機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。 監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、府省庁の外部から通信回線を通してなされる不正アクセス、不正侵入、情報システムの管理者・運用者又は利用者の誤操作又は不正操作、サーバ装置等機器の動作、及び、許可されていない者の安全区域への立ち入り等があり得る。 また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。 （1）設ける監視機能を定める。監視機能には、以下の例がある。 ・府省庁外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能(侵入検知システム等による) ・不正プログラム感染や踏み台に利用されること等による府省庁外への不正な通信を監視する機能 ・府省庁内通信回線への PC の接続を監視する機能 ・PC への外部記録媒体の挿入を監視する機能 ・サーバ装置等の機器の正常な動作を監視する機能 ・安全区域への人の出入を監視する機

No.	統一管理基準(平成 24 年度改定版)		旧版	
		る機能 (2) 監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。 (3) 監視によりプライバシーを侵害する可能性がある場合は、当該行政事務従事者等への説明について定める。		能 (2) 監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。 (3) 監視によりプライバシーを侵害する可能性がある場合は、当該行政事務従事者等への説明について定める。
176		(削除)	1.5.1.1(1)(g)	情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価及び ST 確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。
177		(削除)	1.5.1.1(1)(g) 解説	解説：重要なセキュリティ要件がある情報システムについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を受けることを求める事項である。 「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。情報システムの構築が終了するまでにセキュリティ設計仕様書について、ST 評価及び ST

No.	統一管理基準(平成 24 年度改定版)		旧版	
				確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。 なお、情報システムの構築を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。
178	1.5.2.1(1)(a) (イ) ・	通信回線の利用部門	1.5.2.1(1)(a) (イ) ・	通信回線の利用部署
179	1.5.2.1(1)(a) (エ) 解説	解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として整備することを定めた遵守事項である。文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。 所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。 電子計算機、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアにセキュリティホールが存在することにより使用上のリスクが高まった場合に、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。	1.5.2.1(1)(a) (エ) 解説	解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として整備することを定めた遵守事項である。文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。 所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。 電子計算機、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアにセキュリティホールが存在することにより使用上のリスクが高まった場合に、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。

No.	統一管理基準(平成 24 年度改定版)	旧版
	電子計算機の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システム構成要素の管理状況を確実に把握できるようにするとともに、障害・事故等を防止する責任の所在を明確化するために必要な事項である。 通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、及び通信回線の利用部門の記載は、通信回線の管理状況を把握するために必要な事項である。 情報システムに係る仕様書又は設計書は、情報セキュリティ対策実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。 情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施するべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。 障害・事故等が発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。 ・業務継続計画で定める当該情報システムを利用する業務の重要性	電子計算機の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システム構成要素の管理状況を確実に把握できるようにするとともに、障害・事故等を防止する責任の所在を明確化するために必要な事項である。 通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、及び通信回線の利用部署の記載は、通信回線の管理状況を把握するために必要な事項である。 情報システムに係る仕様書又は設計書は、情報セキュリティ対策実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。 情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施するべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。 障害・事故等が発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。 ・業務継続計画で定める当該情報システムを利用する業務の重要性

No.	統一管理基準(平成 24 年度改定版)		旧版	
		・情報システムの運用等の外部委託の内容 また手順に記載される内容として、例えば以下が想定される。 ・障害・事故等の内容・影響度の大きさに応じた情報連絡先のリスト ・情報システムを障害・事故等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準 ・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項 ・アンチウイルスソフトウェア等では検知されない新種の不正プログラムに感染した場合等に支援を受けるための外部の専門家の連絡先 なお、統括情報セキュリティ責任者が整備する対処手順(1.2.2.2(1)(c)を参照）により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。		・情報システムの運用等の外部委託の内容 また手順に記載される内容として、例えば以下が想定される。 ・障害・事故等の内容・影響度の大きさに応じた情報連絡先のリスト ・情報システムを障害・事故等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準 ・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項 ・アンチウイルスソフトウェア等では検知されない新種の不正プログラムに感染した場合等に支援を受けるための外部の専門家の連絡先 なお、統括情報セキュリティ責任者が整備する対処手順(1.2.2.2(1)(c)を参照）により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。
180	1.5.2.4	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。 一方、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がど	1.5.2.4	情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。 一方、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がど

No.	統一管理基準(平成 24 年度改定版)		旧版	
		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。また、主体認証情報の機密性と完全性、及びアクセス制御情報の完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。これらのことを勘案し、本項では、主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準として、統括情報セキュリティ責任者による主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備、情報セキュリティ責任者及び情報システムセキュリティ責任者による当該規定の遵守、情報システムセキュリティ責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。 なお、1.4.1.1 において識別コードと主体認証情報の管理等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても主体認証・アクセス制御・権限管理・証跡管理・保証等の導入等に関する対策基準を定めている。		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。また、主体認証情報の機密性と完全性、及びアクセス制御情報の完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。これらのことを勘案し、本項では、主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準として、統括情報セキュリティ責任者による主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備、情報セキュリティ責任者及び情報システムセキュリティ責任者による当該規定の遵守、情報システムセキュリティ責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。 なお、1.4.1.1 において識別コードと主体認証情報の管理等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても主体認証・アクセス制御・権限管理・証跡管理・保障等の導入等に関する対策基準を定めている。
181	1.5.2.4(3)(a)	情報システムセキュリティ責任者は、証跡を取得する必要があると認められた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析することの必要性の有無を検討し、必要と認めたときは、当該措置を講じ、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。	1.5.2.4(3)(a)	情報システムセキュリティ責任者は、証跡を取得する必要があると認められた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又は情報セキュリティ責任者に報告すること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
182	1.5.2.5	情報システムの利用において、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐためには、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、行政事務従事者による個別判断で選択されることのないよう、府省庁で標準となる手順を定めることが重要である。 これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、統括情報セキュリティ責任者による暗号と電子署名に係る規定の整備、行政事務従事者による当該規定の遵守についての遵守事項を定める。 なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。	1.5.2.5	情報システムの利用において、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐためには、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、行政事務従事者による個別判断で選択されることのないよう、府省庁で標準となる手順を定めることが重要である。 これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、統括情報セキュリティ責任者による暗号と電子署名に係る規定の整備、行政事務従事者による当該規定の遵守についての遵守事項を定める。 なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保障等の必要性判断等に関する判断基準を、統一技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。
183	1.5.2.5(1)(b)	統括情報セキュリティ責任者は、暗号化された情報(書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）から（ウ）の手順(以下「鍵の管理手順等」という。）を定めること。		統括情報セキュリティ責任者は、暗号化された情報(書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）及び（イ）の手順(以下「鍵の管理手順等」という。）を定めること。
184	1.5.2.5(1)(c) (ウ)	鍵のバックアップ手順	1.5.2.5(1)(c)	統括情報セキュリティ責任者は、暗号化された情報の復号に用いる鍵のバックアップの取得手順又は鍵の預託

No.	統一管理基準(平成 24 年度改定版)		旧版	
				手順（以下「鍵のバックアップ手順等」という。）を定めること。
185	1.5.2.5(1)(c) (ウ) 解説	解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、鍵のバックアップ手順等を定めることを求める事項である。 鍵のバックアップ手順については、バックアップが必要な鍵とバックアップしてはならない鍵の区別を明確にし、バックアップが必要な鍵については、バックアップの取得又は預託手順等を定める。 例えば、復号に用いる鍵を紛失し、又は消失した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得したり、信頼できる第三者へ鍵情報を預託したりする等の鍵のバックアップ対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。 なお、本遵守事項における鍵のバックアップ手順は、前事項の鍵の管理手順等に含めて整備することも可能である。 なお、バックアップしてはならない鍵のタイプについては、例えば、乱数を生成するために用いられる鍵や暗号化に用いる鍵の共有を目的として一度だけ使用される鍵等が考えられる。また、米国国立標準技術研究所（NIST）が発行している文書「SP800-57」を参考とすることも考えられる。	1.5.2.5(1)(c) 解説	解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、鍵のバックアップ手順等を定めることを求める事項である。 例えば、復号に用いる鍵を紛失し、又は消失した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得し、又は信頼できる第三者へ鍵情報を預託する等の対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。 なお、本遵守事項における鍵のバックアップ手順等は、前事項の鍵の管理手順等に含めて整備することも可能である。

No.	統一管理基準(平成 24 年度改定版)		旧版	
186	1.5.2.5(1)(c) 解説	解説：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書を GPKI が発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。 なお、GPKI 以外で使用している電子証明書が有効期限内の場合、次期更新時には、GPKI で発行している電子証明書を使用するように求めることも考えられる。	1.5.2.5(1)(c) 解説	解説：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書を GPKI が発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。
187	1.5.2.5(2)(c)	行政事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。	1.5.2.5(2)(c)	行政事務従事者は、暗号化された情報の復号に用いる鍵について、定められた鍵のバックアップ手順等に従い、そのバックアップを取得すること。
188	1.5.2.6(1)(a) 解説	解説：府省庁外の情報セキュリティ水準の低下を招く行為の防止に関して、統括情報セキュリティ責任者が、規定を整備することを求める事項である。府省庁外の情報セキュリティ水準の低下を招く可能性のある行為としては、例えば、以下のものが挙げられる。 （ア）不適切なソフトウェア及びサービスの使用要求：電子行政サービス(例えば、府省庁のウェブによるコンテンツの提示等を言う。以下同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービ	1.5.2.6(1)(a) 解説	解説：府省庁外の情報セキュリティ水準の低下を招く行為の防止に関して、統括情報セキュリティ責任者が、規定を整備することを求める事項である。府省庁外の情報セキュリティ水準の低下を招く可能性のある行為としては、例えば、以下のものが挙げられる。 （ア）不適切なソフトウェア及びサービスの使用要求：電子行政サービス(例えば、府省庁のウェブによるコンテンツの提示等を言う。以下同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービ

No.	統一管理基準(平成 24 年度改定版)	旧版
	スへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。 （イ）ソフトウェアの不適切な設定要求：電子行政サービスを利用するために、利用者の環境にインストールされているソフトウェア(府省庁が直接提供していないソフトウェア(例えば、クライアント PC の OS やウェブブラウザ等）以下同じ。）について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。 （ウ）ソフトウェア等の不適切な削除要求：府省庁のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。 「明示的に要求する行為」とは、「『このような設定を変更してください。』等のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけではなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。 以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。 ・ソフトウェアを実行させる場合：電子行政サービスのためのソフトウェ	スへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。 （イ）ソフトウェアの不適切な設定要求：電子行政サービスを利用するために、利用者の環境にインストールされているソフトウェア(府省庁が直接提供していないソフトウェア(例えば、クライアント PC の OS やウェブブラウザ等）以下同じ。）について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。 （ウ）ソフトウェア等の不適切な削除要求：府省庁のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。 「明示的に要求する行為」とは、「『このような設定を変更してください。』等のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけではなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。 以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。 ・ソフトウェアを実行させる場合：電子行政サービスのためのソフトウェ

No.	統一管理基準(平成 24 年度改定版)	旧版
	アを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windows の「.exe」ファイル等)、ランタイム環境実行型(例えば、Java アプレットや Windows の ActiveX ファイル等)、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの全てを含む。 ・HTML メール等を送信する場合：府省庁から HTML メール等(利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。 これらの場合については、結果的に利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある。実行させるソフトウェアの提供については、オンラインによる提供(ウェブへの掲載、メールの添付等)について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については電子署名を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。	アを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windows の「.exe」ファイル等)、ランタイム環境実行型(例えば、Java アプレットや Windows の ActiveX ファイル等)、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの全てを含む。 ・HTML メール等を送信する場合：府省庁から HTML メール等(利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。 これらの場合については、結果的に利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある。実行させるソフトウェアの提供については、オンラインによる提供(ウェブへの掲載、メールの添付等)について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については電子署名を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。

No.	統一管理基準(平成 24 年度改定版)	旧版
	やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。 また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。 ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。 また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名(コード署名）が必要な場合には、政府認証基盤(GPKI）で発行したコード署名証明書を利用することが望ましい。 なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。 （ア)(イ）については、当該電子行政サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該電子行政サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加	やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。 また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。 ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。 また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名(コード署名）が必要な場合には、政府認証基盤(GPKI）で発行したコード署名証明書を利用することが望ましい。 なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。 （ア)(イ）については、当該電子行政サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該電子行政サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加

No.	統一管理基準(平成 24 年度改定版)	旧版
	の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める等の方法を考えることができる。 例えば、電子行政用ウェブのアプリケーションを利用するために、利用者のPC 上にあらかじめ標準的にインストールされているソフトウェアがバージョンＡであったとする。その後、そのソフトウェアの最新バージョンがＢに更新され、また、バージョンＡについて脆弱性が公開された場合には、バージョンＢで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョンＡだけで動作するような設計では、利用者に脆弱性のあるバージョンＡを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンＢでも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。 また、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必要がある。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	の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める等の方法を考えることができる。 例えば、電子行政用ウェブのアプリケーションを利用するために、利用者のPC 上にあらかじめ標準的にインストールされているソフトウェアがバージョンＡであったとする。その後、そのソフトウェアの最新バージョンがＢに更新され、また、バージョンＡについて脆弱性が公開された場合には、バージョンＢで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョンＡだけで動作するような設計では、利用者に脆弱性のあるバージョンＡを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンＢでも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		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、ソフトウェアの配布前に情報が公開された状態又は試用版ソフトウェアが配布され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。		
189	1.5.2.6(2)	措置についての規定の遵守	1.5.2.6(2)	規定の遵守
190	1.5.2.7(1)(a) (ア) 解説	解説：「.go.jp で終わるドメイン名」は、株式会社日本レジストリサービスが定める「属性型(組織種別型)・地域型 JP ドメイン名登録等に関する規則」に基づき登録等を行うこととなっている。また、登録資格は、日本国の政府機関、各省庁所管研究所、独立行政法人、特殊法人(特殊会社を除く）とされている。 アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.nisc.go.jp/）や FTP サーバ（例えば、ftp://ftp.nisc.go.jp/）等へのアクセスを促すことをいう。上記には、ウェブページの閲覧に必要なソフトウェア(プラグインを含む）を入手できる政府ドメイン名以外のウェブサイトを告知する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先	1.5.2.7(1)(a) (ア) 解説	解説：アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.nisc.go.jp/）や FTP サーバ（例えば、ftp://ftp.nisc.go.jp/）等へのアクセスを促すことをいう。上記には、ウェブページの閲覧に必要なソフトウェア(プラグインを含む）を入手できる政府ドメイン名以外のウェブサイトを告知する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先(例えば、null@nisc.go.jp）への送信等を促すことをいう。 本遵守事項における告知にあたる場合とは、情報提供のきっかけが府省庁側にある場合で、告知にあたらない場合とは、情報提供のきっかけが府省庁側にない場合である。例えば、府省庁外の者からの問い合わせに回答する場合は、問い合わせがきっかけである

No.	統一管理基準(平成 24 年度改定版)	旧版
	(例えば、null@nisc.go.jp）への送信等を促すことをいう。 本遵守事項における告知にあたる場合とは、情報提供のきっかけが府省庁側にある場合で、告知にあたらない場合とは、情報提供のきっかけが府省庁側にない場合である。例えば、府省庁外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらず、本遵守事項の対象とはならない。なお、いずれの場合についても媒体の種類(郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。 「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。なお、在外公館のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。 政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなものが考えられる。 （例） ・この告知についてのお問い合わせは、null@nisc.go.jp までご連絡ください。 ・この告知で案内しているウェブサイトは○○○協会が運営しており、内閣	ので、告知にはあたらず、本遵守事項の対象とはならない。なお、いずれの場合についても媒体の種類(郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。 「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。なお、在外公館のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。 政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなものが考えられる。 （例） ・この告知についてのお問い合わせは、null@nisc.go.jp までご連絡ください。 ・この告知で案内しているウェブサイトは○○○協会が運営しており、内閣官房が運営しているものではありません。 ・この告知で案内しているウェブサイトのアドレスについては、2007 年 12 月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		官房が運営しているものではありません。 ・この告知で案内しているウェブサイトのアドレスについては、2007 年 12 月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。		
191	1.5.2.8(1)(a) (キ)	行政事務従事者は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講ずること。	1.5.2.8(1)(a) (キ)	行政事務従事者は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。
192	1.5.2.8(1)(a) (キ) 解説	解説：不正プログラムに感染したおそれがある電子計算機については、他の電子計算機への感染等の被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講ずることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等をすることが挙げられる。	1.5.2.8(1)(a) (キ) 解説	解説：不正プログラムに感染したおそれがある電子計算機については、他の電子計算機への感染等の被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講じることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等をすることが挙げられる。
193	A.1.1	組織・体制イメージ図に区域情報セキュリティ責任者を追加 （詳細は、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 A.1.1 組織・体制イメージ図を参照）		
194	A.1.2	機密性についての取扱制限の定義 機密性についての取扱制限の定義について、表 A.1.2-1 に示す。	A.1.2	機密性についての取扱制限の定義 取扱制限の種類 指定方法

No.	統一管理基準(平成 24 年度改定版)	旧版
	表 A.1.2-1 機密性についての取扱制限の定義 取扱制限の種類 指定方法 複製について 複製禁止、複製要許可 配付について 配付禁止、配付要許可 暗号化について 暗号化必須、保存時暗号化必須、通信時暗号化必須 印刷について 印刷禁止、印刷要許可 転送について 転送禁止、転送要許可 転記について 転記禁止、転記要許可 再利用について 再利用禁止、再利用要許可 送信について 送信禁止、送信要許可 参照者の制限について ○○限り 期限について ○月○日迄○○禁止 上記の指定方法の意味は以下のとおり。 ・「○○禁止」 当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。 ・「○○要許可」	複製について 複製禁止、複製要許可 配付について 配付禁止、配付要許可 暗号化について 暗号化必須、保存時暗号化必須、通信時暗号化必須 印刷について 印刷禁止、印刷要許可 転送について 転送禁止、転送要許可 転記について 転記禁止、転記要許可 再利用について 再利用禁止、再利用要許可 送信について 送信禁止、送信要許可 参照者の制限について ○○限り 期限について ○月○日迄○○禁止 上記の指定方法の意味は以下のとおり。 ・「○○禁止」 当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。 ・「○○要許可」 当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 ・「暗号化必須」 当該情報について、暗号化を必須とする必要がある場合に指定する。また、

No.	統一管理基準(平成 24 年度改定版)		旧版	
		当該情報について、〇〇で指定した行為をするに際して、許可を得る必要がある場合に指定する。 ・「暗号化必須」 当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。 ・「〇〇限り」 当該情報について、参照先を〇〇に記載した者のみに制限する必要がある場合に指定する。例えば、「セキュリティセンター限り」「政策会議委員会出席者限り」等、参照を許可する者が分かるように指定する。 ・「〇月〇日迄〇〇禁止」 例えば、〇月〇日迄複製を禁止したい場合、「〇月〇日迄複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。		保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。 ・「〇〇限り」 当該情報について、参照先を〇〇に記載した者のみに制限する必要がある場合に指定する。例えば、「セキュリティセンター限り」「政策会議委員会出席者限り」等、参照を許可する者が分かるように指定する。 ・「〇月〇日迄〇〇禁止」 例えば、〇月〇日迄複製を禁止したい場合、「〇月〇日迄複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。
195	A.1.2	完全性についての取扱制限の定義 完全性についての取扱制限の定義について、表 A.1.2-2 に示す。 表 A.1.2-2 完全性についての取扱制限の定義 取扱制限の種類 指定方法 保存期間について 〇〇まで保存	A.1.2	完全性についての取扱制限の定義 取扱制限の種類 指定方法 保存期間について 〇〇まで保存 保存場所について 〇〇において保存 書換えについて 書換禁止、書換要許可 削除について 削除禁止、削除要許可

No.	統一管理基準(平成 24 年度改定版)		旧版	
		保存場所について ○○において保存 書換えについて 書換禁止、書換要許可 削除について 削除禁止、削除要許可 保存期間満了後の措置について 保存期間満了後要廃棄 情報の保存期間の指定の方法は、以下のとおり。 保存を要する期日である「年月日」又は期日を特定できる用語に「まで保存」を付して指定する。 例）平成○○年７月３１日まで保存 例）平成○○年度末まで保存 完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。 例）年度内保存文書用共有ファイルサーバに保管 例）３カ年保存文書用共有ファイルサーバに保管		保存期間満了後の措置について 保存期間満了後要廃棄 情報の保存期間の指定の方法は、以下のとおり。 保存を要する期日である「年月日」又は期日を特定できる用語に「まで保存」を付して指定する。 例）平成○○年７月３１日まで保存 例）平成○○年度末まで保存 完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。 例）年度内保存文書用共有ファイルサーバに保管 例）３カ年保存文書用共有ファイルサーバに保管
196	A.1.2	可用性についての取扱制限の定義 可用性についての取扱制限の定義について、表 A.1.2-3 に示す。 表 A.1.2-3 可用性についての取扱制限の定義 取扱制限の種類	A.1.2	可用性についての取扱制限の定義 取扱制限の種類 指定方法 復旧までに許容できる時間について ○○以内復旧 保存場所について ○○において保存

No.	統一管理基準(平成 24 年度改定版)		旧版	
		指定方法 復旧までに許容できる時間について ○○以内復旧 保存場所について ○○において保存 復旧許容時間の指定の方法は以下のとおり。 復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。 例） 1 時間以内復旧 例） 3 日以内復旧 可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、各自ＰＣのファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。 例）課室共有ファイル保存必須 例）各自ＰＣ保存可		復旧許容時間の指定の方法は以下のとおり。 復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。 例） 1 時間以内復旧 例） 3 日以内復旧 可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、各自ＰＣのファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。 例）課室共有ファイル保存必須 例）各自ＰＣ保存可
197	A.1.3	〔政府決定〕 ・国の行政機関における情報システム関係業務の外注の推進について(平成 12 年 3 月 31 日行政情報システム各省庁連絡会議了承) ・各省庁の調達におけるセキュリティ水準の高い製品等の利用方針（平成 13 年 3 月 29 日　行政情報化推進各省	A.1.3	〔政府決定〕 ・行政文書の管理方策に関するガイドライン（平成 12 年 2 月 25 日、各省庁事務連絡会議申し合わせ） ・国の行政機関における情報システム関係業務の外注の推進について(平成 12 年 3 月 31 日行政情報システム各省庁連絡会議了承)

No.	統一管理基準(平成 24 年度改定版)	旧版
	庁連絡会議了承） ・各府省の情報システム調達における暗号の利用方針（平成 15 年２月 28 日　行政情報システム関係課長連絡会議了承） ・国家公務員身分証明書の IC カード化(平成 16 年２月６日　e-Japan 戦略 II 加速化パッケージ) ・行政情報の電子的提供に関する基本的考え方(指針)(平成 16 年 11 月 12 日各府省情報化統括責任者（CIO）連絡会議決定） ・業務・システム最適化指針（ガイドライン)(平成 18 年３月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・電子政府推進計画(平成 18 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・情報システムに係る政府調達の基本指針(平成 19 年３月１日　各府省情報化統括責任者（CIO）連絡会議決定） ・中央省庁業務継続ガイドライン 第１版（平成 19 年６月　内閣府） ・行政文書の管理の徹底について(平成 19 年 12 月 14 日　関係省庁連絡会議申合せ）	・各省庁の調達におけるセキュリティ水準の高い製品等の利用方針（平成 13 年３月 29 日　行政情報化推進各省庁連絡会議了承） ・各府省の情報システム調達における暗号の利用方針（平成 15 年２月 28 日　行政情報システム関係課長連絡会議了承） ・電子政府推進計画(平成 18 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・行政情報の電子的提供に関する基本的考え方(指針)(平成 16 年 11 月 12 日各府省情報化統括責任者（CIO）連絡会議決定） ・業務・システム最適化指針（ガイドライン)(平成 18 年３月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・情報システムに係る政府調達の基本指針(平成 19 年３月１日　各府省情報化統括責任者（CIO）連絡会議決定） ・国家公務員身分証明書のＩＣカード化(平成 16 年２月６日　e-Japan 戦略 II 加速化パッケージ） ・中央省庁業務継続ガイドライン 第１版（平成 19 年６月　内閣府）

No.	統一管理基準(平成 24 年度改定版)	旧版
	・今後の行政文書の管理に関する取組について(平成 20 年 11 月 25 日　行政文書・公文書等の管理・保存に関する関係省庁連絡会議申合せ) ・オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（平成 22 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・政府におけるサイバー攻撃等への対処態勢の強化について(平成 22 年 12 月 27 日　情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ） ・中央省庁における情報システム運用継続計画ガイドライン（平成 23 年３月　内閣官房情報セキュリティセンター） ・情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（平成 23 年３月 30 日　内閣官房情報セキュリティセンター） ・調達における情報セキュリティ要件の記載について（平成 24 年１月 24 日　内閣官房副長官から各省庁大臣官房長等あて） ・IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト(平成 23 年４月 21 日　経済産業省）	・行政文書の管理の徹底について(平成 19 年 12 月 14 日　関係省庁連絡会議申合せ） ・今後の行政文書の管理に関する取組について(平成 20 年 11 月 25 日　行政文書・公文書等の管理・保存に関する関係省庁連絡会議申合せ） ・オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（平成 22 年８月 31 日　各府省情報化統括責任者（CIO）連絡会議決定） ・IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト(平成 23 年４月 21 日　経済産業省） 〔法律〕 ・行政機関の保有する情報の公開に関する法律(平成十一年五月十四日法律第四十二号) ・行政機関の保有する個人情報の保護に関する法律(平成十五年五月三十日法律第五十八号) ・公文書等の管理に関する法律（平成二十一年七月一日法律第六十六号） 注）詳細については、原文を参照すること。

No.	統一管理基準(平成 24 年度改定版)		旧版	
		〔法律〕 ・行政機関の保有する情報の公開に関する法律(平成十一年五月十四日法律第四十二号) ・行政機関の保有する個人情報の保護に関する法律(平成十五年五月三十日法律第五十八号) ・公文書等の管理に関する法律（平成二十一年七月一日法律第六十六号) 注）詳細については、原文を参照すること。		
198	A.1.4	●　「ウェブサーバ」とは、HTTP サービスを提供するソフトウェア、当該ソフトウェアで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のようにウェブサーバと一体として動作するハードウェアをいう。	A.1.4	●　「ウェブサーバ」とは、HTTP サーバアプリケーション、当該サーバアプリケーションで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のようにウェブサーバと一体として動作するハードウェアをいう。
199	A.1.4	●　「S/MIME(Secure Multipurpose Internet Mail Extensions)」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。		(新規追加)
200	A.1.5	A.1.5 情報取扱区域のクラスと区域例		(新規追加)
201	A.1.5	情報取扱区域のクラスと区域例 情報取扱区域のクラスと区域例について、表 A.1.5-1 に示す。 表 A.1.5-1 情報取扱区域のクラスと		(新規追加)

No.	統一管理基準(平成 24 年度改定版)	旧版
	区域例 クラス 区域例 クラス 3 ・他の部屋との境界において、施錠又は警備員等による立ち番で関係者以外の入退出を常に制限している執務室 ・サーバ室 クラス 2 ・行政事務従事者の不在時は、施錠管理している執務室又は会議室・窓口のある執務室(カウンター等の仕切りより内側の区域) クラス 1 ・セキュリティゲート又は警備員等の立ち番より内側のロビー(エントランス）又は敷地 ・共用会議室 ・庁舎内の廊下 ・窓口のある部屋（カウンター等の仕切りより外側の区域又は仕切られない区域) クラス 0 ・公道 ・敷地外 ・公道までの敷地内 ・駐車場 ・守衛所 ・セキュリティゲート又は警備員等の	

No.	統一管理基準(平成 24 年度改定版)		旧版	
		立ち番より外側のロビー(エントランス）又は敷地		
202	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)
203	A.1.6	解説：以下の表に記載のものを想定したが、それぞれの府省庁において、このうちから必要な項目を採用し、また、不足している場合は適宜追加して構わない。 個別管理及び個別利用制限は必要に応じて決定するものであるから、規程では例示するだけとして、「情報取扱区域を管理又は利用する者が、当該区域でどのような措置を講ずればよいかを認知させる」という目的を果たせるのであれば、決定する表現方法を一律に定めないという運用方法でも構わない。		(新規追加)
204	A.1.6	情報取扱区域の個別管理及び個別利用制限 情報取扱区域の個別管理例について、表 A.1.6-1、個別利用制限について、表 A.1.6-2 に示す。 表 A.1.6-1 情報取扱区域の個別管理例 個別管理の内容 決定方法 入退出の監視 ・セキュリティゲートを設置している区域は、監視 ・サーバを設置している区域は、監視 ・クラス 3 以上は、監視		(新規追加)

No.	統一管理基準(平成 24 年度改定版)	旧版
	無線 LAN の傍受対策(テンペスト対策) ・窓際側は対策を実施 所在の表示の禁止 ・サーバ室は、非表示 表 A.1.6-2 情報取扱区域の個別利用制限例 個別利用制限の内容 決定方法 要保護情報の一時保管の禁止 ・人の目の行き届かない会議室 飲食禁止 ・飲食物をこぼした際に、情報システムの運用上の障害が発生するような場所 ブラインド閉じ ・外部から室内が見えるような場所にある会議室で、要機密情報取扱い時はブラインド閉じ ワイヤレスマイク使用禁止 ・ワイヤレスマイクの電波が室外にも到達するような会議室で、要機密情報取扱い時、ワイヤレスマイク使用禁止	