

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 年度版）  
（案）

年 月 日

情報セキュリティ対策推進会議

## 目次

第 2.1 部 総則	1
2.1.1.1 本統一技術基準の位置付け	1
(1) 政府機関の情報セキュリティ対策の強化における本統一技術基準の位置付け	1
(2) 本統一技術基準の改訂	1
(3) 法令等の遵守	1
2.1.1.2 本統一技術基準の使い方	1
(1) 全体構成	1
(2) 対策項目の記載事項	1
(3) 「対策レベルの設定」に係る変更点	1
2.1.1.3 情報の格付の区分及び取扱制限の種類	1
(1) 格付及び取扱制限	1
(2) 格付の区分	1
(3) 取扱制限の種類	2
2.1.1.4 情報取扱区域における管理及び利用制限	2
(1) 情報取扱区域	2
(2) 情報取扱区域のクラスの決定	2
(3) 情報取扱区域のクラス別管理及び利用制限	2
(4) 情報取扱区域の個別管理及び個別利用制限	2
2.1.1.5 評価の方法	2
2.1.1.6 用語定義	2
第 2.2 部 情報セキュリティ要件の明確化に基づく対策	4
2.2.1 情報セキュリティについての機能	4
2.2.1.1 主体認証機能	4
遵守事項	4
(1) 主体認証機能の導入	4
2.2.1.2 アクセス制御機能	5
遵守事項	5
(1) アクセス制御機能の導入	5
(2) 適正なアクセス制御	6
2.2.1.3 権限管理機能	6
遵守事項	6
(1) 権限管理機能の導入	6
(2) 識別コードと主体認証情報の付与管理	6
2.2.1.4 証跡管理機能	7

遵守事項.....	7
(1) 証跡管理機能の導入.....	7
(2) 証跡の取得と保存.....	8
2.2.1.5 保証のための機能.....	8
遵守事項.....	8
(1) 保証のための機能の導入.....	8
2.2.1.6 暗号と電子署名（鍵管理を含む）.....	8
遵守事項.....	8
(1) 暗号化機能及び電子署名機能の導入.....	8
(2) 暗号化及び電子署名に係る管理.....	9
2.2.2 情報セキュリティについての脅威.....	10
2.2.2.1 セキュリティホール対策.....	10
遵守事項.....	10
(1) 情報システムの構築時.....	10
(2) 情報システムの運用時.....	10
2.2.2.2 不正プログラム対策.....	11
遵守事項.....	11
(1) 情報システムの構築時.....	11
(2) 情報システムの運用時.....	11
2.2.2.3 サービス不能攻撃対策.....	12
遵守事項.....	12
(1) 情報システムの構築時.....	12
(2) 情報システムの運用時.....	12
2.2.2.4 踏み台対策.....	13
遵守事項.....	13
(1) 情報システムの構築時.....	13
(2) 情報システムの運用時.....	13
2.2.2.5 標的型攻撃対策.....	13
遵守事項.....	13
(1) 情報システムの構築時.....	13
(2) 情報システムの運用時.....	13
第 2.3 部 情報システムの構成要素についての対策.....	14
2.3.1 施設と環境.....	14
2.3.1.1 情報取扱区域のクラス別管理及び利用制限.....	14
遵守事項.....	14
(1) 立ち入る者を制限するための管理対策.....	14

(2) 立ち入る者を許可する際の管理対策 .....	14
(3) 訪問者がある場合の管理対策 .....	14
(4) 設置する設備の管理対策 .....	15
(5) 作業がある場合の管理対策 .....	15
(6) 立ち入る者を制限するための利用制限対策 .....	15
(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 .....	16
(8) 荷物の受渡しについての利用制限対策 .....	16
(9) 災害及び障害への対策 .....	16
2.3.2 電子計算機 .....	17
2.3.2.1 電子計算機共通対策 .....	17
遵守事項 .....	17
(1) 電子計算機の設置時 .....	17
(2) 電子計算機の運用時 .....	17
(3) 電子計算機の運用終了時 .....	17
2.3.2.2 端末 .....	18
遵守事項 .....	18
(1) 端末の設置時 .....	18
(2) 端末の運用時 .....	18
2.3.2.3 サーバ装置 .....	18
遵守事項 .....	18
(1) サーバ装置の設置時 .....	18
(2) サーバ装置の運用時 .....	19
2.3.3 アプリケーションソフトウェア .....	20
2.3.3.1 電子メール .....	20
遵守事項 .....	20
(1) 電子メールの導入時 .....	20
(2) 電子メールの運用時 .....	20
2.3.3.2 ウェブ .....	20
遵守事項 .....	20
(1) ウェブサーバの導入時 .....	20
(2) ウェブアプリケーションの開発時 .....	21
(3) ウェブの運用時 .....	21
2.3.3.3 ドメインネームシステム (DNS) .....	21
遵守事項 .....	21
(1) DNS の導入時 .....	21
(2) DNS の運用時 .....	22

2.3.4 通信回線 .....	23
2.3.4.1 通信回線共通対策 .....	23
遵守事項.....	23
(1) 通信回線の構築時.....	23
(2) 通信回線の運用時.....	24
(3) 通信回線の運用終了時 .....	24
2.3.4.2 府省庁内通信回線の管理 .....	24
遵守事項.....	24
(1) 府省庁内通信回線の構築時 .....	24
(2) 府省庁内通信回線の運用時 .....	25
(3) 回線の対策 .....	25
2.3.4.3 府省庁外通信回線との接続.....	26
遵守事項.....	26
(1) 府省庁内通信回線と府省庁外通信回線との接続時.....	26
(2) 府省庁外通信回線と接続している府省庁内通信回線の運用時.....	26
第 2.4 部 個別事項についての対策.....	27
2.4.1 その他.....	27
2.4.1.1 情報システムへの IPv6 技術の導入における対策 .....	27
遵守事項.....	27
(1) IPv6 通信がもたらす脆弱性対策 .....	27
(2) 意図しない IPv6 通信の抑止と監視 .....	27

別表

別表 1 情報取扱区域のクラス別管理

別表 2 情報取扱区域のクラス別利用制限

## 第 2.1 部 総則

### 2.1.1.1 本統一技術基準の位置付け

- (1) 政府機関の情報セキュリティ対策の強化における本統一技術基準の位置付け  
政府機関の情報セキュリティ対策のための統一管理基準（以下「統一管理基準」という。）に準じる。
- (2) 本統一技術基準の改訂  
統一管理基準に準じる。
- (3) 法令等の遵守  
統一管理基準に準じる。

### 2.1.1.2 本統一技術基準の使い方

- (1) 全体構成  
統一管理基準に準じる。
- (2) 対策項目の記載事項  
統一管理基準に準じる。
- (3) 「対策レベルの設定」に係る変更点  
統一管理基準に準じる。

### 2.1.1.3 情報の格付の区分及び取扱制限の種類

- (1) 格付及び取扱制限  
統一管理基準に準じる。
- (2) 格付の区分  
統一管理基準に準じる。

- (3) 取扱制限の種類  
統一管理基準に準じる。

#### 2.1.1.4 情報取扱区域における管理及び利用制限

- (1) 情報取扱区域  
統一管理基準に準じる。
- (2) 情報取扱区域のクラスの決定  
統一管理基準に準じる。
- (3) 情報取扱区域のクラス別管理及び利用制限  
統一管理基準に準じる。
- (4) 情報取扱区域の個別管理及び個別利用制限  
統一管理基準に準じる。

#### 2.1.1.5 評価の方法

統一管理基準に準じる。

#### 2.1.1.6 用語定義

統一管理基準に準じる。

以下は、本統一技術基準で初出の用語。

##### 【あ】

- 「受渡業者」とは、行政事務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

##### 【か】

- 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表されたセキュリティホールが該当する。

【は】

- 「複数要素（複合）主体認証（multiple factors authentication）方式」とは、複数の方法の組合せにより主体認証を行う方法である。

【ま】

- 「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。



## 第 2.2 部 情報セキュリティ要件の明確化に基づく対策

### 2.2.1 情報セキュリティについての機能

#### 2.2.1.1 主体認証機能

##### 遵守事項

##### (1) 主体認証機能の導入

- (a) 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、識別及び主体認証を行う機能を設けること。
- (b) 情報システムセキュリティ管理者は、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、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。
  - (ア) 主体認証情報を保存する場合には、その内容の暗号化を行うこと。
  - (イ) 主体認証情報を通信する場合には、その内容の暗号化を行うこと。
  - (ウ) 保存又は通信を行う際に暗号化を行うことができない場合には、利用者から自らの主体認証情報を設定、変更及び提供（入力）させる際に、暗号化が行われない旨を通知すること。
- (c) 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、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。
  - (ア) 利用者が定期的に変更しているか否かを確認する機能
  - (イ) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能
- (d) 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、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。
- (e) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。
  - (ア) 利用者が、自らの主体認証情報を設定する機能
  - (イ) 利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能
  - (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

- (f) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項のうちその特性に応じて適用可能な要件を全て満たす主体認証方式を導入すること。
- (ア) 正当な主体以外の主体認証を受諾しないこと。(誤認の防止)
  - (イ) 正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。(誤否認の防止)
  - (ウ) 正当な主体が容易に他者に主体認証情報の付与(発行、更新及び変更を含む。以下この項において同じ。)及び貸与ができないこと。(代理の防止)
  - (エ) 主体認証情報が容易に複製できないこと。(複製の防止)
  - (オ) 情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。(無効化の確保)
  - (カ) 必要時に中断することなく主体認証が可能であること。(可用性の確保)
  - (キ) 新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。(継続性の確保)
  - (ク) 主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。(再発行の確保)
- (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、必要と認めるときは、当該機能を設けること。
- (ア) 複数要素(複合)主体認証方式で主体認証を行う機能
  - (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
  - (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
  - (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
  - (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
  - (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

### 2.2.1.2 アクセス制御機能

#### 遵守事項

- (1) アクセス制御機能の導入

- (a) 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、アクセス制御を行う機能を設けること。
- (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。
  - (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
  - (イ) 強制アクセス制御機能

(2) 適正なアクセス制御

- (a) 情報システムセキュリティ責任者は、行政事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従って、アクセス制御を行うこと。

### 2.2.1.3 権限管理機能

#### 遵守事項

(1) 権限管理機能の導入

- (a) 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。
- (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。
  - (ア) 最少特権機能
  - (イ) 主体認証情報の再発行を自動で行う機能
  - (ウ) デュアルロック機能

(2) 識別コードと主体認証情報の付与管理

- (a) 権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。
- (b) 権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。
- (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。
  - (ア) 業務又は業務上の責務に則した場合に限定すること
  - (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

(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

(エ) ネットワークからのログインを制限すること

(d) 権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。

(e) 権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者に交付した主体認証情報格納装置を返還させること。

(f) 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限り許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

(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、必要と認めるときは、当該措置を講ずること。

(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

(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

(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

#### 2.2.1.4 証跡管理機能

##### 遵守事項

(1) 証跡管理機能の導入

(a) 情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

(b) 情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。

(c) 情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリテ

- ィ責任者が認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。
- (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。
- (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
  - (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) 証跡の取得と保存

- (a) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、情報システムに設けられた機能を利用して、証跡を取得すること。
- (b) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。
- (c) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。

### 2.2.1.5 保証のための機能

#### 遵守事項

- (1) 保証のための機能の導入
- (a) 情報システムセキュリティ責任者は、保証のための対策を行う必要があると認められた情報システムにおいて、保証のための機能を設けること。

### 2.2.1.6 暗号と電子署名(鍵管理を含む)

#### 遵守事項

- (1) 暗号化機能及び電子署名機能の導入
- (a) 情報システムセキュリティ責任者は、要機密情報(書面を除く。以下この項において同じ。)を取り扱う情報システムについて、暗号化を行う機能を付加する必要性

の有無を検討すること。

- (b) 情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。
- (c) 情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。
- (d) 情報システムセキュリティ責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。
- (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。
  - (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
  - (イ) 複数のアルゴリズムを選択可能にする構成
  - (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、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
  - (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) 暗号化及び電子署名に係る管理

- (a) 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供すること。
- (b) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。

## 2.2.2 情報セキュリティについての脅威

### 2.2.2.1 セキュリティホール対策

#### 遵守事項

- (1) 情報システムの構築時
  - (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。
  - (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う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) 情報システムの運用時
  - (a) 情報システムセキュリティ管理者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。
  - (b) 情報システムセキュリティ責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。
    - (ア) 対策の必要性
    - (イ) 対策方法
    - (ウ) 対策方法が存在しない場合の一時的な回避方法
    - (エ) 対策方法又は回避方法が情報システムに与える影響
    - (オ) 対策の実施予定
    - (カ) 対策試験の必要性
    - (キ) 対策試験の方法
    - (ク) 対策試験の実施予定
  - (c) 情報システムセキュリティ管理者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。
  - (d) 情報システムセキュリティ管理者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。
  - (e) 情報システムセキュリティ管理者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイル(以下「対策用ファイル」という。)を入手すること。また、当該対策用ファイルの完全性

検証方法が用意されている場合は、検証を行うこと。

- (f) 情報システムセキュリティ管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。
- (g) 情報システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の情報システムセキュリティ責任者と共有すること。

## 2.2.2.2 不正プログラム対策

### 遵守事項

- (1) 情報システムの構築時
  - (a) 情報システムセキュリティ責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）にアンチウイルスソフトウェア等を導入すること。
  - (b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。
  - (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、必要と認めたときは、当該措置を講ずること。
  - (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) 情報システムの運用時
  - (a) 情報システムセキュリティ管理者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、行政事務従事者にその対処の実施に関する指示を行うこと。
  - (b) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。



### 2.2.2.3 サービス不能攻撃対策

#### 遵守事項

- (1) 情報システムの構築時
  - (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（インターネットからアクセスを受ける電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）については、サービス提供に必要な電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。
  - (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、サービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。
  - (c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。
  - (d) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。
  - (e) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する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。
  - (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。
  - (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。
- (2) 情報システムの運用時
  - (a) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法が定められている場合は、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

#### 2.2.2.4 踏み台対策

##### 遵守事項

- (1) 情報システムの構築時
  - (a) 情報システムセキュリティ責任者は、情報システム（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、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）が踏み台として使われることを防止するための措置を講ずること。
  - (b) 情報システムセキュリティ責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。
  - (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) 情報システムの運用時
  - (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。

#### 2.2.2.5 標的型攻撃対策

##### 遵守事項

- (1) 情報システムの構築時
  - (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。
  - (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。
  
- (2) 情報システムの運用時
  - (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。

## 第 2.3 部 情報システムの構成要素についての対策

### 2.3.1 施設と環境

#### 2.3.1.1 情報取扱区域のクラス別管理及び利用制限

##### 遵守事項

- (1) 立ち入る者を制限するための管理対策
  - (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。
    - (ア) 不審者を立ち入らせない措置
    - (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) 立ち入る者を許可する際の管理対策
  - (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。
    - (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
    - (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
    - (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
    - (エ) 継続的に立ち入る者を許可する手続の整備
    - (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
    - (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
- (3) 訪問者がある場合の管理対策
  - (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。
    - (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

- (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
- (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
- (エ) 訪問者の立ち入る区域を制限するための措置
- (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
- (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

(4) 設置する設備の管理対策

- (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。
- (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。
  - (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
  - (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
  - (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
  - (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

(5) 作業がある場合の管理対策

- (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。

(6) 立ち入る者を制限するための利用制限対策

- (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。

- (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
- (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。
- (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
  - (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
  - (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
- (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。
- (8) 荷物の受渡しについての利用制限対策
- (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。
- (9) 災害及び障害への対策
- (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。
- (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。

## 2.3.2 電子計算機

### 2.3.2.1 電子計算機共通対策

#### 遵守事項

- (1) 電子計算機の設置時
  - (a) 情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。
  - (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。
  - (c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にする必要性を検討し、必要と判断した場合には、その電子計算機を冗長構成にすること。
  - (d) 情報システムセキュリティ責任者は、行政事務従事者の離席時に、電子計算機を不正操作から保護するための措置を講ずること。
  - (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。
- (2) 電子計算機の運用時
  - (a) 行政事務従事者は、行政事務の遂行以外の目的で電子計算機を利用しないこと。
  - (b) 行政事務従事者は、離席時に電子計算機を不正操作から保護するための措置を講ずること。
  - (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。
  - (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、必要と認めるときは、当該措置を講ずること。
- (3) 電子計算機の運用終了時
  - (a) 情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体の全ての情報を抹消すること。

### 2.3.2.2 端末

#### 遵守事項

- (1) 端末の設置時
  - (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。
  - (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。
  - (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。
  - (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。
  - (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) 端末の運用時
  - (a) 行政事務従事者は、要保護情報を取り扱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。
  - (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。
  - (c) 行政事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に端末を接続しないこと。
  - (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。

### 2.3.2.3 サーバ装置

#### 遵守事項

- (1) サーバ装置の設置時
  - (a) 情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業

を行う場合は、通信を秘匿する必要性の有無を検討し、必要があると認めるときは、送受信される情報を秘匿するための機能を設けること。この場合、府省庁外通信回線を経由する保守作業については、通信を秘匿する必要があると判断すること。

- (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、必要と認めるときは、当該措置を講ずること。

(2) サーバ装置の運用時

- (a) 情報システムセキュリティ責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。
- (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については、サーバ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。
- (c) 情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。
- (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、サーバ装置の時刻を同期すること。
- (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、必要と認めるときは、当該措置を講ずること。
- (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、必要と認めるときは、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。



## 2.3.3 アプリケーションソフトウェア

### 2.3.3.1 電子メール

#### 遵守事項

- (1) 電子メールの導入時
  - (a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。
  - (b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に行政事務従事者の主体認証を行う機能を備えること。
  - (c) 情報システムセキュリティ責任者は、電子メールの送信元について、なりすましの防止策を講ずること。
- (2) 電子メールの運用時
  - (a) 行政事務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、それぞれの府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。ただし、府省庁支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。
  - (b) 行政事務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。

### 2.3.3.2 ウェブ

#### 遵守事項

- (1) ウェブサーバの導入時
  - (a) 情報システムセキュリティ責任者は、情報セキュリティが確保されるよう適切にウェブサーバのセキュリティ設定をすること。適切なセキュリティ設定として、以下に挙げる事項を含む措置を講ずること。
    - (ア) ウェブサーバの機能を適切に制限すること。
    - (イ) ウェブサーバに保存された情報へのアクセス制限を適切に設定すること。
    - (ウ) 識別コードを適切に管理すること。
    - (エ) 通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能を設けること。
  - (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) ウェブアプリケーションの開発時

(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。

- (ア) 利用者による URL の確認を妨げないこと。
- (イ) 主体認証と情報へのアクセス制御を適切に行うこと。
- (ウ) ウェブアプリケーションが使用するファイルのパス名を限定すること。
- (エ) 不正な入力データを排除すること。
- (オ) 不正な出力データを排除すること。
- (カ) 安全なセッション管理を行うこと。

(3) ウェブの運用時

(a) 行政事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。

(b) 行政事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

(c) 行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

- (ア) 送信内容が暗号化されること。
- (イ) 当該ウェブサイトが送信先として想定している組織のものであること。

(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。

### 2.3.3.3 ドメインネームシステム(DNS)

#### 遵守事項

(1) DNS の導入時

(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の名前解決を提供する DNS のコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

- (b) 情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続を定めること。
- (c) 情報システムセキュリティ責任者は、DNS のキャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。
- (d) 情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて、府省庁内のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。
- (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。

(2) DNS の運用時

- (a) 情報システムセキュリティ管理者は、DNS のコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。
- (b) 情報システムセキュリティ管理者は、DNS のコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。

## 2.3.4 通信回線

### 2.3.4.1 通信回線共通対策

#### 遵守事項

- (1) 通信回線の構築時
  - (a) 情報システムセキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。
  - (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、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。
  - (c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定めること。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。
  - (d) 情報システムセキュリティ責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。
  - (e) 情報システムセキュリティ責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用し、アクセス制御及び経路制御を行うこと。
  - (f) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、通信を秘匿するための機能を設けること。
  - (g) 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、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。
  - (h) 情報システムセキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。
  - (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。
  - (j) 情報システムセキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。
  - (k) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にする必要性を検討し、必要と判断した場合には、その通信回線又は通信回線装置を冗長構成にすること。

- (1) 情報システムセキュリティ責任者は、通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。
- (2) 通信回線の運用時
  - (a) 情報システムセキュリティ管理者は、通信回線装置のソフトウェアを変更する場合には、情報システムセキュリティ責任者の許可を得ること。
  - (b) 情報システムセキュリティ管理者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。
  - (c) 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の確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。
  - (d) 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受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。
  - (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、通信回線装置の時刻を同期すること。
  - (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。
  - (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。
  - (h) 情報システムセキュリティ管理者は、通信回線装置を不正操作から保護するための措置を講ずること。
- (3) 通信回線の運用終了時
  - (a) 情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体の全ての情報を抹消すること。

#### 2.3.4.2 府省庁内通信回線の管理

##### 遵守事項

- (1) 府省庁内通信回線の構築時
  - (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。

(2) 府省庁内通信回線の運用時

- (a) 情報システムセキュリティ責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。
- (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。
- (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。

(3) 回線の対策

- (a) 情報システムセキュリティ責任者は、VPN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。
  - (ア) 利用開始及び利用停止時の申請手続の整備
  - (イ) 通信内容の暗号化
  - (ウ) 通信を行う電子計算機の識別又は利用者の主体認証
  - (エ) 主体認証記録の取得及び管理
  - (オ) VPN 経由でアクセスすることが可能な通信回線の範囲の制限
  - (カ) VPN 接続方法の機密性の確保
  - (キ) VPN を利用する電子計算機の管理
- (b) 情報システムセキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要があると判断すること。
  - (ア) 利用開始及び利用停止時の申請手続の整備
  - (イ) 通信内容の暗号化
  - (ウ) 通信を行う電子計算機の識別又は利用者の主体認証
  - (エ) 主体認証記録の取得及び管理
  - (オ) 無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
  - (カ) 無線 LAN に接続中に他の通信回線との接続の禁止
  - (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
- (c) 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境

を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

- (ア) 利用開始及び利用停止時の申請手続の整備
- (イ) 通信を行う者又は発信者番号による識別及び主体認証
- (ウ) 主体認証記録の取得及び管理
- (エ) リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
- (オ) リモートアクセス中に他の通信回線との接続の禁止
- (カ) リモートアクセス方法の機密性の確保
- (キ) リモートアクセスする電子計算機の管理

### 2.3.4.3 府省庁外通信回線との接続

#### 遵守事項

- (1) 府省庁内通信回線と府省庁外通信回線との接続時
  - (a) 情報システムセキュリティ責任者は、情報セキュリティ責任者の許可を得た上で、府省庁内通信回線を府省庁外通信回線と接続すること。
  - (b) 情報システムセキュリティ責任者は、府省庁内通信回線を府省庁外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線として府省庁内通信回線を構築すること。
- (2) 府省庁外通信回線と接続している府省庁内通信回線の運用時
  - (a) 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の確保が困難な事由が発生した場合には、他の情報システムと共有している府省庁内通信回線又は府省庁外通信回線から独立した通信回線に構成を変更すること。
  - (b) 情報システムセキュリティ責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。
  - (c) 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。
  - (d) 情報システムセキュリティ管理者は、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を監視すること。

## 第 2.4 部 個別事項についての対策

### 2.4.1 その他

#### 2.4.1.1 情報システムへの IPv6 技術の導入における対策

##### 遵守事項

##### (1) IPv6 通信がもたらす脆弱性対策

- (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 IPv6 Ready Logo 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。
- (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。
- (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。
- (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。
- (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。

##### (2) 意図しない IPv6 通信の抑止と監視

- (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。
- (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。



## 別表

別表1 情報取扱区域のクラス別管理

別表2 情報取扱区域のクラス別利用制限

別表1 情報取扱区域のクラス別管理

行番号	遵守事項	対策例	備考	クラス0	クラス1	クラス2	クラス3	(クラス4以上(統一基準外)) 〔府省庁で独自定義する場合の例〕	
1	〔凡例〕クラス0～クラス3までの列に記載している内容は、それぞれのクラスにおいて、各欄の左側に記載された措置・対策・実施に対して、以下のとおり。 要：必要、不要：不要、可：使用可能又は設定可能、禁：禁止(許可(届出)申請が必要)、対象外：対象外、府省庁の判断：各府省庁で管理対策の方針を決定								
2	<b>(1) 立ち入る者を制限するための管理対策</b>								
3	(ア) 不審者を立ち入らせない措置 2.3.1.1(1)(a)(ア)	所在の表示 (案内板の表示等)	クラス0の表示	対象外	可			可 (なお、他のクラスにて、 クラス4の所在の表示は 「禁」とすることが望ましい)	
4			クラス1の表示	・例)省、局の名称	可				
5			クラス2の表示	・例)課室名、会議室名	可				
6			クラス3の表示	(※1) サーバ室は非表示	可(※1)				
7	(イ) 要保護情報を取り扱う情報システムについては、区域間を物理的に 隔離し、立入り及び退出を管理するための措置 2.3.1.1(1)(a)(イ)	入退出可能な 下位区域との 接続	クラス0との接続	対象外	可	＜府省庁の判断＞			禁
8			クラス1との接続	対象外		可			
9			クラス2との接続	対象外		可			
10			クラス3との接続	対象外					
11		下位の区域との 分離方法	天井を突き抜ける壁	対象外	可			可	
12			天井と接する固定式 パーティション、壁	対象外	可			禁	
13			天井と接しない固定式 パーティション	対象外	可	＜府省庁の判断＞			
14			可動式パーティション	対象外	可	禁			
15		管理方法	立入り及び退出の管理 方法	対象外	・セキュリティゲート ・警備員等による立ち番 り等。ただし、ドアガラス 等で見えても良 い	・施設可能な扉、間仕切 り等。ただし、ドアガラス 等で見えても良 い	・施設可能な扉等。中が 見えないこと。	・施設可能な扉。 ・入退出をモニターで監 視。	
16			全員不在時に制限	〔制限方法例〕 ・扉等を施設 ・出入口に警備員等を配置し、入 退出する者を確認	要			要	
17			常に制限	対象外			要		
18	<b>(2) 立ち入る者を許可する際の管理対策</b>								
19	(ア) 立ち入る者の確認 2.3.1.1(2)(a)(ア)		「立ち入る」とは、「下位のクラスの 区域から上位のクラスの区域への 立入り」を指す。	対象外	＜府省庁の判断＞			＜府省庁で独自定義＞	
20	(イ) 退出する者の確認 2.3.1.1(2)(a)(イ)		「退出」とは、「上位のクラスの区域 から下位のクラスの区域への退 出」を指す。	対象外	＜府省庁の判断＞				
21	(ウ) 許可されていない者の立入り及び退出を制限する措置 2.3.1.1(2)(a)(ウ)			対象外	＜府省庁の判断＞				
22	(エ) 継続的に立ち入る者を許可する手続 2.3.1.1(2)(a)(エ)			対象外	＜府省庁の判断＞				
23	(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 2.3.1.1(2)(a)(オ)			対象外	＜府省庁の判断＞				
24	(カ) 立入り及び退出の記録及び監視 2.3.1.1(2)(a)(カ)		・例)警備員又は防犯カメラ等の導 入	対象外	＜府省庁の判断＞				
25	<b>(3) 訪問者がある場合の管理対策</b>								
26	(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(3)(a)(ア)	登録申請(訪問 者の身元確認)	事前貸与者(※2)	・合同庁舎や民間管理ビル等、自 府省庁で管理対策を講ずることが 出来ない場合は、当該管理府省庁 や民間管理ビルに対策状況を確 認するなどして、管理対策を決定 する。	不要	要	要(※3)	＜府省庁で独自定義＞	
27			訪問者(※2)		不要	要	要(※3)		
28	(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(3)(a)(イ)	訪問記録	事前貸与者(※2)		不要	＜府省庁の判断＞			
29			訪問者(※2)	(※2) ・「事前貸与者」とは、事前に識別 カードを貸与されている者を指す。 (府省庁外の者で、継続的に立入 りを許可された者)	不要	＜府省庁の判断＞			
30	(ウ) 訪問相手の行政事務従事者が訪問者の情報取扱区域への立入り について審査するための手続の整備 2.3.1.1(3)(a)(ウ)	登録申請(訪問 者の立入り時 の審査)	事前貸与者(※2)	・「訪問者」とは、事前に識別カード を貸与されていない者を指す。	不要	要	要(※3)		
31			訪問者(※2)		不要	要	要(※3)		
32	(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(3)(a)(エ)		事前貸与者(※2)	・「事前に識別カードを貸与されて いる」とは、民間事業者等に、継続 的な立入りのために自府省庁のセ キュリティゲートを通過可能な識別 カードを貸与している場合を指す。	不要	＜府省庁の判断＞			
33			訪問者(※2)		不要	＜府省庁の判断＞			
34	(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(3)(a)(オ)	行政事務従事 者の帯同、エ スコート	事前貸与者(※2)	(※3) ・クラス0からクラス1へ進入する際 の確認・審査で代替することも可 能	不要	＜府省庁の判断＞			
35			訪問者(※2)		不要	＜府省庁の判断＞			
36	(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(3)(a)(カ)	訪問者と継続的に立入りを許可された 者との外見上の区別			不要	要			
37	<b>(4) 設置する設備の管理対策</b>								
38	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 2.3.1.1(4)(a)	端末	・セキュリティファイヤーによる固定	(※4) 当該クラスへの立入りの際に立ち 入る者の確認を行う等の措置をと り、入退出者を制限できる場合は、 部屋全体の施設管理にて対策を 講ずることも考えられる。	対象外	要	要(※4)	＜府省庁で独自定義＞	
39		サーバ装置	・機器扉付きラック等で施設管理 ・セキュリティファイヤーによる固定		対象外	要	要(※4)		
40		通信回線装置(装置への主体認 証が必要なもの)	・機器扉付きラック等で施設管理		対象外	要	要(※4)		
41		通信回線装置(装置への主体認 証が不要なもの)			対象外	要	要(※4)		
42	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 の設置に係る対策 2.3.1.1(4)(b)	(ア) 他の区域との物理的な隔離			対象外	＜府省庁の判断＞			
43		(イ) 表示用デバイスの盗み見防止			対象外	＜府省庁の判断＞			
44		(ウ) 電源ケーブル及び通信ケーブル の損傷及び盗聴防止	・ケーブルの床下への埋設 ・ケーブルのナンバリング		対象外	＜府省庁の判断＞			
45		(エ) 電磁波による情報漏えい対策	・電磁波軽減フィルタの利用		対象外	＜府省庁の判断＞			
46	<b>(5) 作業がある場合の管理対策</b>								
47	当該区域内での作業を監視するための措置 2.3.1.1(5)(a)	行政事務従事 者の作業の立 会、監視	・当該作業に関係する他 の行政事務従事者による 同行、立会	対象外	＜府省庁の判断＞			＜府省庁で独自定義＞	
48			・監視カメラ等による監 視	対象外	＜府省庁の判断＞				
49		業者の作業の 立会、監視	・担当の行政事務従事 者による同行、立会	対象外	＜府省庁の判断＞		要		
50			・監視カメラ等による監 視	対象外	＜府省庁の判断＞				

別表2 情報取扱区域のクラス別利用制限

行番号	遵守事項	対策例	備考	クラス0	クラス1	クラス2	クラス3	(クラス4以上(統一基準外)) 〔府省庁で独自定義する場合の例〕	
1	<p>〔凡例〕  <b>許可</b>：(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からの)許可が必要、  <b>届出</b>：(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への)届出が必要(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不要と判断した場合は、不要)、  <b>禁止</b>：原則禁止(許可を求める場合は、例外措置の適用の申請が必要(省庁対策基準に定める許可権限者の承認が必要))、  <b>要</b>：必要、<b>不要</b>：許可又は届出が不要、<b>可</b>：設置可能、<b>府省庁の判断</b>：各府省庁で利用制限対策の方針を決定、<b>対象外</b>：対象外</p>								
2	<b>(1) 立ち入る者を制限するための利用制限対策</b>								
3	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(6)(a)	識別カードの着用、明示(府省庁外の者も含む)		不要		要		<府省庁で独自定義>	
4	<b>(2) 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</b>								
5	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対策 2.3.1.1(7)(a)	(ア) 持込み及び持ち出しを行う措置		対象外		<府省庁の判断>		<府省庁で独自定義>	
6		(イ) 記録の保存		対象外		<府省庁の判断>		<府省庁で独自定義>	
7		(ウ) 情報システムに関連しない電子計算機等の持込みの制限	荷物検査	対象外		<府省庁の判断>		<府省庁で独自定義>	
8	行政事務従事者の所持する府省庁支給以外の情報システム(モバイル端末及び記録装置)の持込みの制限等 2.3.1.1(7)(a)	(ウ) 情報システムに関連しない電子計算機等の持込みの制限		対象外		不要	<府省庁の判断>		
9			起動・利用(府省庁内LAN未接続、要保護情報は取り扱わない場合)	対象外		不要			
10		モバイル端末の起動・利用 1.4.2.2(2)(a) (機密性3情報、完全性2情報又は可用性2情報を取り扱う場合)		(※1) 府省庁内通信回線への接続を認める場合は、府省庁内のすべての情報にアクセスできる可能性があるリスクを考慮すること。			許可(※1)		<府省庁で独自定義>
11		モバイル端末の起動・利用 1.4.2.2(2)(b) (機密性2情報であって完全性1情報かつ可用性1情報を取り扱う場合)				届出(※1)			
12	府省庁外の者の所持するモバイル端末及び記録装置の持込みの制限等 2.3.1.1(7)(a)、1.2.5.3(3)(b)	(ウ) 情報システムに関連しない電子計算機等の持込みの制限		対象外		不要	<府省庁の判断>		
13			起動・利用(府省庁内LAN未接続)	対象外		<府省庁の判断>		<府省庁で独自定義>	
14	行政事務従事者による写真撮影、録音 2.3.1.1(7)(b)		(※2) 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。	対象外		<府省庁の判断>(※2)			
15	府省庁外の者による写真撮影、録音 2.3.1.1(7)(b)、1.2.5.3(3)(b)			対象外		<府省庁の判断>(※2)			
16	<b>(3) 荷物の受渡しについての利用制限対策</b>								
17	受渡し管理 2.3.1.1(8)(a)	宅配便、荷物		不要		<府省庁の判断>		<府省庁で独自定義>	
18		要保護情報又は機密性1情報		<府省庁の判断>				<府省庁で独自定義>	
19	<b>(4) 情報処理の制限</b>								
20	要管理対策区域外での情報処理の制限 1.4.2.1(2)(a)(b)	機密性2情報について情報処理を行う場合		届出		対象外		不要	
21		機密性1情報並びに完全性2情報又は可用性2情報について情報処理を行う場合		許可		対象外		不要	
22		機密性3情報について情報処理を行う場合		許可		対象外		不要	
23	<b>(5) 設備の設置</b>								
24	端末の設置 2.3.2.1(1)(b)		・追加で設置する場合 ・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。	禁	<府省庁の判断>		可	可	
25	通信回線装置の設置 2.3.4.1(1)(i)			禁	<府省庁の判断>		可	可	
26	サーバ装置の設置 2.3.2.1(1)(b)			禁	<府省庁の判断>		可	可	
27	<b>(6) ネットワークの接続</b>								
28	通信回線構築によるリスクを検討し、通信回線を構築すること 2.3.4.1(1)(a)	府省庁内LAN	クラス0のLANとの接続	・追加で設置する場合	対象外	(府省庁外通信回線との接続に準じる)			<府省庁で独自定義>
29			クラス1のLANとの接続			可	<府省庁の判断>		
30			クラス2のLANとの接続		(府省庁外通信回線との接続に準じる)	<府省庁の判断>	可		
31			クラス3のLANとの接続			<府省庁の判断>	可		
32	無線LAN環境を構築する場合に、必要に応じて措置を講ずること 2.3.4.2(3)(b)	無線LAN	クラス0の無線LANとの接続	・追加で設置する場合	対象外	(府省庁外通信回線との接続に準じる)			<府省庁で独自定義>
33			クラス1の無線LANとの接続	・他の区域との接続制限の例：MACアドレス、IEEE802.1x等による接続制限		可	<府省庁の判断>		
34			クラス2の無線LANとの接続		(府省庁外通信回線との接続に準じる)	<府省庁の判断>	可	<府省庁の判断>	
35			クラス3の無線LANとの接続			<府省庁の判断>		可	
36		府省庁内から府省庁管理外のネットワーク経由でのインターネット直接接続		・府省庁内通信回線(府省庁内LAN)へは、接続禁止が前提 ・「府省庁管理外のネットワーク」又は、Wi-Fiルータ(府省庁外通信回線へ直接接続可能な通信回線装置)等の利用によるインターネットへの直接接続を想定	対象外	<府省庁の判断>			<府省庁で独自定義>