

## Ⅶ 技術的セキュリティ対策

### 1 アクセス記録の取得等

重要な電子情報を扱う業務システムについては、システム管理者は各種アクセス記録を取得し、一定期間保存するものとする。

### 2 アクセス制御

#### (1) システムのアクセス制御

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスのシステム的不正な変更防止

##### ②業務システム及びサーバの管理策

電子情報の重要性の分類に応じ、次のうち適切な管理を行う。

- ・セグメント分離
- ・ルータ等の装置によるアクセス制御
- ・暗号化
- ・パスワード設定
- ・アプリケーション、ドライブの利用制限

##### ③パソコンの管理策

電子情報の重要性の分類に応じ、次のうち適切な管理を行う。

- ・認証キー
- ・ICカード
- ・ファイルの暗号化
- ・パスワード設定

④各管理対象別のアクセス制御管理策の詳細は、電子情報資産管理台帳に定める。

#### (2) インターネットのアクセス制御

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスのシステムの改ざん防止
- ・サービス停止による市民サービスの低下の防止

##### ②管理策

ファイアウォール	a 不要なポートは制御するなど、適切な設定を行う。 b 不正アクセスの監視等の防御策を施す。 c 設定権限を適正に管理する。 d 定期的にログを監視及び保存する。 e セキュリティパッチは遅滞なく適用する。
ルータ	a 必要のないプロトコルやサービス等を制御する。 b 設定権限を適正に管理する。 c セキュリティパッチは遅滞なく適用する。

③インターネットのアクセス制御管理策の詳細については、インターネットアクセス制御管理台帳に定める。

#### (3) モデム接続及びモバイルコンピューティングのアクセス制御

モデム接続及びモバイルコンピューティングの利用は、原則として禁止する。

### 3 パスワード管理

#### (1) 目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤用（意図されない利用・参照）防止

#### (2) サーバのパスワード管理

次の事項を遵守し、適切な管理を行う。

- a 設定又は変更する場合は、推測可能なものを使用しないこと。
- b 変更する場合は、過去に使用したパスワードを使用しないこと。
- c パスワードを口外したり、記録したメモなどを放置したりしないこと。

サーバのパスワードに関する管理策の詳細は、電子情報資産管理台帳に定める。

#### (3) クライアントのパスワード管理

次の事項を遵守し、適切な管理を行う。

- a 設定又は変更する場合は、推測可能なものを使用しないこと。
- b 変更する場合は、過去に使用したパスワードを使用しないこと。
- c パスワードを記録したメモなどを放置しないこと。

### 4 コンピュータウイルス対策

#### (1) 目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスからの情報の改ざんの防止
- ・ウイルス感染によるネットワーク、パソコン等のシステム停止の防止

#### (2) 対策

##### ①各システム管理者の遵守事項

システム導入時	<ul style="list-style-type: none"><li>a サーバ及びクライアントには必ずウイルス対策ソフトを導入しなければならない。</li><li>b 必要に応じてゲートウェイサーバ等の対策を行う。</li></ul>
システム導入後	<ul style="list-style-type: none"><li>a ウィルス定義ファイルは常に最新版に更新しなければならない。</li><li>b 内部セキュリティ監査の結果に基づき、必要に応じて情報政策課は、各システムのウイルス対策について指導する。</li></ul>

##### ②利用者の遵守事項

- a 送信元不明等、不審な電子メールの添付ファイルに対しては、これに操作を加えてはならない。
- b 電子メールやフロッピーディスク等で外部へ提供するファイルは、必ずウイルス検査を行うこと。
- c ウィルスの感染やウイルスと思われる症状を発見した場合は、各システム管理者へ速やかに報告を行う。

## 5 障害対策

### (1) 目的

- ・システムの障害による情報利用停止の防止
- ・システムの障害による情報破損・紛失の防止

### (2) 電源バックアップ管理

#### ①遵守事項

- a 電子情報資産管理台帳に登録されたサーバは十分な電源を確保し、必ずUPS（無停電電源装置）の設置を行うこと。
- b UPSでのバックアップ対象は、必要最低限の装置とすること。（プリンタ及びモニタ画面などの出力装置は極力接続しないこと）
- c UPSは、バックアップ対象の電源規定量を確認の上選定を行うこと。
- d 製造元の取扱説明書に基づき、定期的にUPSの電池を交換すること。なお、使用状況等を考慮し、必要に応じて性能確認を行うこと。

### (3) データバックアップ管理

#### ①遵守事項

- a サーバのデータは必ずバックアップを行うこと。
- b バックアップ装置は、バックアップ対象の規定量（ディスクサイズ）を確認の上選定すること。
- c バックアップは計画された手順（手法及び頻度）に基づき、定期的に行うこと。
- d バックアップの手順（手法及び頻度）は定期的に見直すこと。
- e バックアップに使用した媒体は適切に保管すること。
- f 内部システム監査等により、定期的に各システムのバックアップ管理の状況を確認する。

②各管理対象別の電子情報バックアップ管理に関する管理策の詳細は、電子情報資産管理台帳に定める。