

---

# 物理的・技術的セキュリティ管理基準

---

(第 2.6 版)

制定日：平成 23 年 3 月 16 日

改正日：令和 5 年 3 月 31 日

施行日：令和 5 年 4 月 1 日

神戸市

## 改訂履歴

改訂年月日	版番号	改訂理由・内容
平成 23 年 3 月 16 日	第 1.0 版	初版発行
平成 23 年 4 月 1 日	第 1.1 版	ポリシー改正に伴う一部改正（平成 23 年 3 月 30 日決裁）
平成 24 年 6 月 6 日	第 1.2 版	ポリシー改正に伴う一部改正（平成 24 年 6 月 6 日決裁）
平成 26 年 4 月 1 日	第 1.3 版	ポリシー改正に伴う一部改正（平成 26 年 3 月 17 日決裁）
平成 27 年 4 月 1 日	第 1.4 版	ポリシー改正に伴う一部改正（平成 27 年 3 月 25 日決裁）
平成 28 年 4 月 1 日	第 1.5 版	ポリシー改正に伴う一部改正（平成 28 年 3 月 25 日決裁）
平成 29 年 4 月 1 日	第 1.6 版	ポリシー改正に伴う一部改正（平成 29 年 3 月 9 日決裁）
平成 30 年 10 月 30 日	第 1.7 版	ポリシー改正に伴う一部改正（平成 30 年 10 月 18 日決裁）
平成 31 年 4 月 1 日	第 2.0 版	自治体強靱性向上事業にかかる管理基準の追加等（平成 31 年 3 月 25 日決裁）
令和元年 9 月 1 日	第 2.1 版	ポリシー改正に伴う一部改正（令和元年 8 月 16 日決裁）
令和 2 年 4 月 1 日	第 2.2 版	ポリシー改正に伴う一部改正（令和 2 年 3 月 6 日決裁）
令和 3 年 4 月 1 日	第 2.3 版	ポリシー改正に伴う一部改正（令和 3 年 4 月 1 日決裁）
令和 3 年 7 月 1 日	第 2.4 版	ポリシー改正に伴う一部改正（令和 3 年 6 月 28 日決裁）
令和 4 年 4 月 1 日	第 2.5 版	ポリシー改正に伴う一部改正（令和 4 年 3 月 28 日決裁）
令和 5 年 4 月 1 日	第 2.6 版	ポリシー改正に伴う一部改正（令和 5 年 3 月 31 日決裁）

## 目次

<b>1.</b>	<b>はじめに</b>	<b>1</b>
1.1	目的	1
1.2	適用範囲	1
1.3	改廃管理	1
1.4	本文書の位置付け	1
<b>2.</b>	<b>情報システム全体の強靱性の向上</b>	<b>1</b>
2.1	マイナンバー利用事務系	1
2.1.1	マイナンバー利用事務系と他の領域との分離【対策基準 5.1 ア】	1
2.1.2	特定通信【対策基準 5.1 ア】	2
2.2	情報のアクセス及び持ち出しにおける対策【対策基準 5.1 イ(2)】	3
2.3	マイナンバー利用事務系クラウドサービスでの情報システムの扱い【対策基準 5.1 ウ】	3
2.4	マイナンバー利用事務系クラウドサービス上での情報資産の取扱い【対策基準 5.1 エ】	4
2.5	LGWAN 接続系とインターネット接続系の分割【対策基準 5.2 ア】	4
2.6	メールやデータを LGWAN 接続系に取り込む場合の無害化处理【対策基準 5.2 イ】	4
2.7	LGWAN 接続系とインターネット接続系に接続する情報システム【対策基準 5.2 ア】	5
2.8	インターネット接続系のセキュリティ対策【対策基準 5.3 ア】	6
2.9	その他のセキュリティ対策	6
<b>3.</b>	<b>物理的セキュリティ管理</b>	<b>6</b>
3.1	サーバ等の管理【対策基準 6.1】	6
3.1.1	装置の取付け等【対策基準 6.1.1】	6
3.1.2	サーバの二重化等【対策基準 6.1.2】	7
3.1.3	電源【対策基準 6.1.3】	7
3.1.4	配線【対策基準 6.1.4】	7
3.1.5	機器等の定期保守及び修理【対策基準 6.1.5】	7
3.1.6	敷地外への機器の設置【対策基準 6.1.6】	7
3.1.7	機器の廃棄等【対策基準 6.1.7】	7
3.2	管理区域（情報システム室等）の管理【対策基準 6.2】	9
3.2.1	管理区域の構造等【対策基準 6.2.1】	9
3.2.2	入退室の管理【対策基準 6.2.2】	10
3.2.3	執務区域の入退室管理【対策基準 6.2.2】	10
3.2.4	機器等の搬出入【対策基準 6.2.3】	10
3.3	通信回線及び通信回線装置の管理【対策基準 6.3】	11
3.3.1	庁舎内の通信回線等の管理【対策基準 6.3.1】	11
3.3.2	機密を要する情報システムで使用する回線【対策基準 6.3.4】	11
3.3.3	ネットワークの可用性の確保【対策基準 6.3.5 イ】	11
3.4	端末や電磁的記録媒体等の管理【対策基準 6.4】	11
3.4.1	施錠保管庫【対策基準 6.4】	11
3.5	その他の管理策	12

3.5.1	端末の盗難防止策【対策基準 6.4.1】	12
3.5.2	ログイン認証【対策基準 6.4.2】	12
3.5.3	認証の併用【対策基準 6.4.2】	12
3.5.4	暗号化機能の利用【対策基準 6.4.3】	12
3.5.5	モバイル端末の利用【対策基準 6.4.4】	12
3.5.6	執務区域外における職員等の遵守事項【対策基準 7.1.1】	12
3.6	パスワードの管理【対策基準 7.4.3】	13
4.	技術的セキュリティ管理	13
4.1	コンピュータ及びネットワークの管理【対策基準 8.1】	13
4.1.1	データの保存【対策基準 8.1.1】	13
4.1.2	ファイルサーバの設定等【対策基準 8.1.2】	14
4.1.3	情報資産のバックアップ【対策基準 8.1.3】	14
4.1.4	他団体との情報システムに関する情報等の交換【対策基準 8.1.4】	14
4.1.5	仕様書等の保管【対策基準 8.1.6】	14
4.1.6	ログの取得等【対策基準 8.1.7】	14
4.1.7	ネットワークの接続制御、経路制御等【対策基準 8.1.9】	15
4.1.8	強制的な接続制御、経路制御【対策基準 8.1.9】	15
4.1.9	外部の者が利用するシステム【対策基準 8.1.10】	16
4.1.10	外部ネットワークとの接続【対策基準 8.1.11】	16
4.1.11	Web サイトでの情報公開時の注意事項【対策基準 8.1.12】	16
4.1.12	複合機のセキュリティ管理【対策基準 8.1.13】	17
4.1.13	IoT 機器を含む特定用途機器【対策基準 8.1.14】	17
4.1.14	無線 LAN 等の利用【対策基準 8.1.15】	17
4.1.15	電子メールのセキュリティ管理【対策基準 8.1.16】	18
4.1.16	利用可能なネットワークプロトコル【対策基準 8.1.22】	18
4.1.17	Web 会議サービスの利用時の対策【対策基準 8.1.24 ア】	18
4.1.18	Web 会議サービス主催時の対策【対策基準 8.1.24 イ】	19
4.1.19	ソーシャルメディアサービスによる情報発信【対策基準 8.1.25 ア(1)】	19
4.2	アクセス制御【対策基準 8.2】	20
4.2.1	利用者 ID の取扱い【対策基準 8.2.1】	20
4.2.2	特権 ID の管理等【対策基準 8.2.1 ウ】	20
4.2.3	職員等による外部からのアクセス【対策基準 8.2.2】	20
4.2.4	内部ネットワーク間の接続【対策基準 8.2.3】	21
4.2.5	ネットワーク機器の自動識別【対策基準 8.2.4】	21
4.2.6	ログイン試行回数の制限等【対策基準 8.2.5】	21
4.2.7	パスワードに関する情報の管理【対策基準 8.2.6】	21
4.3	システム開発、導入、保守等【対策基準 8.3】	22
4.3.1	情報システムの調達【対策基準 8.3.1】	22
4.3.2	情報システムの開発等【対策基準 8.3.2】	22

4.3.3	情報システムの導入【対策基準 8.3.3】	23
4.3.4	システム開発・保守に関連する資料等の整備・保管【対策基準 8.3.4】	24
4.3.5	情報システムの入出力データの正確性の確保【対策基準 8.3.5】	24
4.3.6	ソフトウェアの保守及び更新【対策基準 8.3.7】	24
4.4	不正プログラム対策【対策基準 8.4】	24
4.4.1	情報基盤管理者等の措置事項【対策基準 8.4.1】	24
4.4.2	職員等情報取扱者の遵守事項【対策基準 8.4.2】	25
4.4.3	専門家の支援体制【対策基準 8.4.3】	26
4.5	不正アクセス対策【対策基準 8.5】	26
4.5.1	使用されていないポートの閉鎖等【対策基準 8.5.1】	26
4.5.2	攻撃の予告等への措置【対策基準 8.5.2】	27
4.5.3	記録の保存【対策基準 8.5.3】	27
4.5.4	内部からの攻撃【対策基準 8.5.4】	27
4.5.5	職員等による不正アクセス時の措置【対策基準 8.5.5】	27
4.5.6	サービス不能攻撃【対策基準 8.5.6】	27
4.5.7	標的型攻撃【対策基準 8.5.7】	27
4.6	セキュリティ情報の収集【対策基準 8.6】	27
5.	情報システムの監視	28
5.1	事象の検知【対策基準 9.1 ア】	28
5.2	時刻同期【対策基準 9.1 イ】	28
5.3	常時監視【対策基準 9.1 ウ】	28
5.4	クラウドサービスの状況・設定の確認【対策基準 9.1 エ】	28
6.	業務委託等と外部サービスの利用	28
6.1	委託事業者等の選定基準【対策基準 10.1.1】	28
6.2	契約書の記載事項【対策基準 10.1.2】	28
6.2.1	委託先等の従事者の所属等に関する事項【対策基準 10.1.2 ア (11)】	28
6.2.2	委託先等の従事者等に対する研修の実施に関する事項【対策基準 10.1.2 ア (12)】	29
6.2.3	情報のライフサイクル全般での管理義務に関する事項【対策基準 10.1.2 ア (14)】	29
6.3	外部サービスの選定【外部サービス利用基準 3.2 カ】	29
6.4	外部サービスにおけるユーティリティプログラム【外部サービス利用基準 3.5.5】	29
6.5	外部サービス利用システムの運用・保守時の対策【外部サービス利用基準 3.6 ① ケ】	29
6.6	外部サービス利用システムの更改・廃棄時の対策【外部サービス利用基準 3.7 ③】	29

## 1. はじめに

### 1.1 目的

物理的・技術的セキュリティ管理基準（以下、「本文書」という。）は、神戸市（以下、「本市」という。）における情報資産に関する情報セキュリティ対策の基準を定めた「神戸市情報セキュリティ対策基準」（平成 15 年 1 月 27 日情報セキュリティ最高責任者決定）のうち、とくに物理的セキュリティ対策及び技術的セキュリティ対策についての具体的な考え方及び内容の理解を促すことを目的とする。

### 1.2 適用範囲

本文書は、神戸市情報セキュリティ対策基準の適用範囲とする。

### 1.3 改廃管理

本文書の承認者は、情報セキュリティ最高責任者（CISO）である。

### 1.4 本文書の位置付け

本文書は、以下の文書に準拠して記述している。

- ・神戸市情報セキュリティ基本方針
- ・神戸市情報セキュリティ対策基準

## 2. 情報システム全体の強靱性の向上

### 2.1 マイナンバー利用事務系

#### 2.1.1 マイナンバー利用事務系と他の領域との分離【対策基準 5.1 ア】

対策基準 5.1 アにおける「マイナンバー利用事務系と他の領域との分離」とは、住民情報の流失を防ぐ必要があることから、他の領域（LGWAN 接続系及びインターネット接続系）との通信をできないように論理的に分離することをいう。

ア 統合パッケージシステムを利用している場合であっても、マイナンバー利用事務系と LGWAN 接続系との端末は分けなければならない。

イ 総合窓口を実施している場合等、業務毎に専用端末を設置することが難しい場合には、端末からの情報持ち出し不可設定や端末への多要素認証の導入を図り、利用状況をチェックする運用体制などを整備した上で実施する。

ウ マイナンバー利用事務系と LGWAN 接続系のサーバが仮想化基盤上にあり、物理的なサーバに共存している場合は、各システムの通信について、分離を徹底することが重要であることから、通信が分離されていることの確認を行わなければならない。なお、地方公共団体が共同で利用するデータセンターに構築しているネットワークについても、庁内ネットワークとして同様の措置を行わなければならない。

エ マイナンバー利用事務系と外部との通信の必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。これらの限定を行った通信を特定通信という。特定通信を行う際は、

L2SW/L3SW による通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。

オ マイナンバー利用事務系にあるデータの他の領域への移動は原則として禁止する。ただし、十分なセキュリティ対策を実施し、業務システム管理者の承認を得た場合に限り、必要最小限の範囲において行うことができる。

#### 2.1.2 特定通信【対策基準 5.1 ア】

ア 対策基準 5.1 アにおける「通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定」を行った通信（以下「特定通信」という。）とは、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付や LGWAN・ASP サービスなど接続先が信頼される特定先との通信のことをいう。マイナンバー利用事務系は、LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。

イ 特定通信となる外部接続の例として、職員認証情報の連携、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用の LGWAN 接続、データバックアップセンターや共同利用／クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。なお、特定通信を行う外部接続先についても、インターネット等と接続されていない。

ウ 対策基準 5.1 アの「国等の公的機関が構築したシステム等」とは、eLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォーム等のほか、十分に安全性が確保された外部接続先として情報セキュリティ統括責任者が認めるものとする。これらの外部接続先と LGWAN を経由してマイナンバー利用事務系が双方向でデータを移送する場合、特定通信を行う際の留意点に加え、以下の対策を行う。

- ・外部接続先とは、連携サーバを設置して通信を行う。外部接続先からのデータやファイルは、連携サーバを介してマイナンバー利用事務系と通信する。また、ファイアウォールやプロキシサーバ等でマイナンバー利用事務系から外部接続先に直接通信する経路が許可されないよう設定する。

- ・ファイアウォールや連携サーバで外部接続先との通信を制限（FQDN 指定）することで通信先を限定する。

- ・許可されていないマイナンバー利用事務系の端末から外部接続先へ接続することがないように、ファイアウォールや連携サーバで通信を制限する。

- ・マイナンバー利用事務系のサーバ、端末については、ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OS 等の修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない。マイナンバー利用事務系においては、インターネットとの接続が出来ないため、シグネチャ（既知の不正な通信や攻撃パターンを識別するためのルール）の更新方法（自治体情報セキュリティ向上プラットフォームの活用や媒体による手動更新等）を十分に確認する。

- ・住民の情報を扱う場合は、外部接続先とは TLS プロトコルを利用し、認証、暗号化、改ざんの検知等の対策を実施する。これらの対策に加え、ファイアウォール及び連携サーバの通信の履歴等を取得する。

- ・USB メモリ等の電磁的記録媒体により不正プログラムに感染する場合があるため、マイナンバー利

用事務系の端末及び外部接続先との接続に利用する端末について、電磁的記録媒体の利用制御を実施しなければならない。

- ・ウェブアプリケーションを利用しているシステムの場合は、ウェブアプリケーションの実装面として脆弱性を作り込まない対策、定期的な診断などを行って脆弱性を検出・対処する対策を実施しなければならない。

## 2.2 情報のアクセス及び持ち出しにおける対策【対策基準 5.1 イ(2)】

ア 対策基準 5.1 イ(2)における「原則として」とは、納付書など大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供等の電磁的記録媒体の利用が止むを得ない場合があることをいう。その場合においては、管理者権限を持つ職員等によってその都度限定を解除する又は管理者権限を持つ職員等のみに許可する設定とすることを例外として取り扱わなければならない。

イ USB メモリ等の電磁的記録媒体による端末からの情報持ち出しを行う場合は、次の手段により実施しなければならない。

- (1) 端末には情報管理者に利用許可された媒体のみ接続可能とすること。
- (2) データは暗号化しパスワードを設定すること。
- (3) 利用媒体は、全て管理し利用履歴を残すこと。
- (4) データの受け渡しには、必ず情報管理者の承認と承認記録を残すこと。

## 2.3 マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い【対策基準 5.1 ウ】

ア 対策基準 5.1 ウにおける「分離」は、必ずしも物理的な分離ではなく、論理的な制御による分離（論理的に分離された仮想ネットワーク）を可とする。ただし、論理的な制御により分離を行う場合は、設定における正確性や安全性を確保しなければならない。

イ クラウドサービス上で構築するマイナンバー利用事務系の標準準拠システム等における脆弱性の対処を行うために、OS、ミドルウェア及びアプリケーション等の修正プログラム並びにウイルス対策ソフトのパターンファイルの更新並びに標準準拠システム等を動作する上で必要となるソフトウェアのアクティベーションを実施する場合は、以下の対策を行う。

- ・クラウドサービス上のマイナンバー利用事務系と異なる新たなネットワーク（DMZ）を構築する。
- ・上記 DMZ 内に連携サーバ（修正プログラム及びウイルス対策ソフト等の更新サーバ）を配置した上で、限定された通信の設定（FQDN のホワイトリスト設定やファイアウォール（FW）によるクラウドサービス上に構築したクライアント及びサーバ等からインターネットへのアウトバウンド通信の制御・インターネットからクラウドサービス上に構築したクライアント及びサーバ等へのインバウンド通信の禁止）を行う。
- ・不正なアクセスが無いか日常的な監視（例えば、通常時のネットワークトラフィックの状態を監視し、通常時と異なる場合は、異常と判断し詳細を確認する）を徹底する。

ウ クラウドサービスの管理コンソールに対して、例外的にインターネット経由でアクセスする場合は、次の対応を行う。



- ・多要素認証によりアクセスを行う。
- ・許可された端末からのアクセスに限定する必要があるため、端末認証(MAC アドレス、シリアル番号及び電子証明書等)又は接続する機器や拠点の IP アドレス等の認証情報を利用し端末を制限する。
- ・操作履歴などの監査ログを取得することやアクセス者に対して必要最小限の権限設定を行う。
- ・これらの対策が適切に実施され、外部からの攻撃や脅威に対するリスクが低減されているのか、運用前に事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行う。
- ・運用保守等により、これらのアクセスを業務委託等で行う場合は、委託先等の情報セキュリティ対策が確実に実施されるよう委託先等への要求事項を調達仕様書等に定め契約条件とするとともに、当該条件が遵守されているか、委託先等を定期的に確認し、遵守していない場合には、職員等が委託先等に適切に指導を行う。

エ 上記イ及びウの対応については、リスクアセスメント（リスクの特定、リスクの分析及びリスクの評価）を実施した上で、具体的なリスクに対する対応措置（情報セキュリティ対策）を行う。

オ 上記エの措置が適切に実施され、外部からの攻撃や脅威に対するリスクが低減されているのか、運用前に事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行う。

## 2.4 マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い【対策基準 5.1 エ】

ア クラウドサービス上で処理が実行されている状態では、原則として暗号化されない状態で情報を利用していることになるため、処理が終了した時にメモリ領域や記憶領域に残留データが残らないように利用した領域を開放しているか、クラウドサービスの利用前に仕様や動作を確認すること。

イ 対策基準 5.1 エにおける「十分な強度」を担保するために、クラウドサービスの仕組みに応じ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の「電子政府推奨暗号リスト」中で推奨された暗号利用モードで暗号化されるのか確認すること。

ウ 通信の暗号化には、IPsec、TLS や SSH を使った暗号化があり、OSI 参照モデルにおける暗号化を行うレイヤが異なるが、通信元と通信先それぞれでサポートしている暗号の違いにより、意図しない脆弱な暗号が使われる、通信が失敗するといったリスクがある。これを避けるために、クラウドサービス側だけでなく、その通信先（回線事業者や庁内の通信機器等）でも「電子政府推奨暗号リスト」中の暗号をサポートしているかを確認すること。可能であれば、実際の通信から、想定した暗号で暗号化されているかを確認することが望ましい。

## 2.5 LGWAN 接続系とインターネット接続系の分割【対策基準 5.2 ア】

対策基準 5.2 アにおける「分割」とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

## 2.6 メールやデータを LGWAN 接続系に取り込む場合の無害化処理【対策基準 5.2 イ】

ア 対策基準 5.2 イ(1)における方式とは、LGWAN 接続系へインターネットメールを転送する際には、インターネットメールの転送に必要な特定サーバ間以外の通信を遮断するとともに、LGWAN

環境とインターネット環境は SMTP 以外の Web 通信を始めとするプロトコルを遮断し、インターネットメールの添付ファイルの削除及び HTML メールテキスト化を行う方式のことをいう。

イ 対策基準 5.2 イ(2)における方式とは、インターネット接続系の端末を仮想デスクトップ化し、LGWAN 接続系の端末から添付ファイルも含むメールの閲覧を可能とする方式のことをいう。仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、インターネット接続系から LGWAN 接続系へマルウェア感染を防ぐ必要があるため、許可する通信は、画面転送用のプロトコル等、無害なものだけに限定すること。上記の他に、ファイルを一旦分解した上で、ウイルスが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し分解前と同様のファイル形式に復元する方法（サニタイズ処理）がある。

ウ 対策基準 5.2 イ(3)における方式とは、インターネット接続系から LGWAN 接続系にファイルを取り込む際は、以下のような手法により、危険因子をファイルから除去又は危険因子がファイルに含まれていないことの確認を行った上で、取り込む方式のことをいう。（いずれかの手法のみ又は複数の手法を組み合わせ採用することが考えられる。）危険因子が埋め込まれたファイルを LGWAN 接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行されるおそれがあるためである。

- ・ファイルからテキストのみを抽出
- ・ファイルを画像 PDF に変換
- ・サービス等を活用してサニタイズ処理（ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する）を行う。
- ・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、LGWAN 接続系において以下のようなセキュリティ対策を実施しなければならない。

- ・OS 等の修正プログラムの適時適用（自治体情報セキュリティ向上プラットフォームの利用等）
- ・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）
- ・業務に必要なファイルやメール等の定期的なバックアップの実施

また、上記の LGWAN 接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN 接続系端末にアプリケーションブラックリストを設定し、実行できるアプリケーションの制限等を行うこと。

## 2.7 J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムへの対応【対策基準 5.2 ア】

対策基準 5.2 アにおける「LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない」の例外として J-ALERT 等のように LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムがある場合は、ファイアウォールを設置し、さらに特定通信としなければならない。あるいはデータベースのみを共用し、情報システムは LGWAN 接続系とインターネット接続系の各系統で別に設置する方法で実現してもよい。

## 2.8 インターネット接続系のセキュリティ対策【対策基準 5.3 ア】

対策基準 5.3 アにおける「情報セキュリティ対策」の内容は具体的には以下のようなものがある。

### ア サーバ等の監視

Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバ、LGWAN 接続ファイアウォールのログの監視を行う。

### イ 情報セキュリティ機器の導入

通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審な URL へのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った、高度な情報セキュリティ機器を導入する。

### ウ 情報セキュリティ運用監視

情報セキュリティ専門人材による高水準なセキュリティ運用監視を行う。

## 2.9 その他のセキュリティ対策

### ア プリンタ・複合機の情報セキュリティ対策

プリンタ・複合機は、必要に応じてマイナンバー利用事務系、LGWAN 接続系、インターネット接続系のネットワーク毎に設置する。共有する場合においてもマイナンバー利用事務系又は LGWAN 接続系について、インターネット接続系と共有することは認められない。共有する場合には、1 台のプリンタ・複合機にネットワーク毎に専用の LAN ポートを設け、他の領域と分離された通信を保証する。それが困難である場合には、ネットワークの一方を LAN ポートに、もう一方は USB ポートにプリンタサーバを繋ぐなどの方法を検討する。

### イ インターネットメールによる障害通報

インターネット接続系についてはインターネットメールを利用してシステム障害通報を行ってもよい。マイナンバー利用事務系及び LGWAN 接続系については、特定サーバ間通信に限定した上で、LGWAN-ASP を活用する。

### ウ アクセス記録を外部に提供する場合、又は他団体からアクセス記録を受領する場合

アクセス記録に保有個人情報が含まれる場合、個人情報保護法等に従わなければならない。

### エ 修正プログラム及びパターンファイルの更新

マイナンバー利用事務系及び LGWAN 接続系では、OS・アプリケーションの修正プログラム及びウイルス対策ソフトのパターンファイルの更新等において、兵庫県セキュリティクラウドのサービスや、LGWAN-ASP 等を利用して修正プログラム等を取得し適用すること。マイナンバー利用事務系及び LGWAN 接続系の WSUS のファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、兵庫県セキュリティクラウドのサービスや、LGWAN-ASP 等を利用すること。

## 3. 物理的セキュリティ管理

### 3.1 サーバ等の管理【対策基準 6.1】

#### 3.1.1 装置の取付け等【対策基準 6.1.1】

対策基準 6.1.1 における「影響を可能な限り排除した場所」とは、情報システムの機器等に物理的に影響を与える脅威や人的な脅威への対策を実施している場所をいう。設置場所への対策としては、火災時に消火を行う設備、地震の時に機器等が落下しない固定設備、温度・湿度の変化による機器等の故障防止設備、盗難や破壊防止のための施錠設備等がある。

#### 3.1.2 サーバの二重化等【対策基準 6.1.2】

対策基準 6.1.2 における「二重化等」とは、システム停止等に伴うリスクを軽減するため、機器等の冗長構成もしくはスタンバイ構成、外部事業者によるデータ保管サービスの利用といった対策を行うことをいう。それに加えて、装置に悪影響を与えることがある環境条件（温度、湿度等）を監視する。対策を実施するにあたっては、情報資産の重要性とリスクを軽減するための対策に要する経費を考慮する。

#### 3.1.3 電源【対策基準 6.1.3】

ア 対策基準 6.1.3 アにおける「十分な電力」とは、何らかの原因でサーバ等の機器へ供給する電源が停止した場合に、機器を正常にシャットダウンさせるために必要な電力をいう。対策としては UPS（無停電電源装置）の設置、自家発電機の設置、電源供給元の冗長化等がある。

イ 対策基準 6.1.3 イにおける「過電流」とは、落雷等により機器等を故障させてしまうような大きな電流が流れることをいう。対策としては、コンセントからの過電流の除去機能を持った OA タップや放電するためのアースの設置等がある。

#### 3.1.4 配線【対策基準 6.1.4】

ア 対策基準 6.1.4 ウにおける「損傷等」の対策として、通信ケーブルと電源ケーブルを物理的に分離して設置することがある。また、損傷が起きた場合の対策手順書をあらかじめ用意しておく。

イ 対策基準 6.1.4 エにおける「容易に接続出来ない場所」とは、主に施錠が可能な設備のことをいう。ネットワーク接続口に他者が容易に接続できないようにするためのその他の対策としては、定期的な現地調査、検知用のソフトウェア等を用いて許可されていない装置がケーブルに取付けられていないかの調査等がある。

#### 3.1.5 機器等の定期保守及び修理【対策基準 6.1.5】

対策基準 6.1.5 アにおける「定期保守」とは、可用性 2 のサーバ機器等に予め決められた間隔（1 年、6 ヶ月等）ごとに実施する保守のことをいう。実施間隔を決定する際には、機器等の製造元が推奨する期間を考慮しなければならない。また、実施した保守及び点検の結果は、適切に保管しなければならない。

#### 3.1.6 敷地外への機器の設置【対策基準 6.1.6】

対策基準 6.1.6 における「庁舎の敷地外にサーバ等の機器を設置する場合」とは、データセンター等本市の庁舎敷地外に本市所有（リースによるものを含む）のサーバ等の機器を設置することをいう。設置するには対策基準に規定する内容に加え、以下の事項を検討しなければならない。

ア 敷地外に設置する機器について担当する職員等、事業者等を明確にする。

イ 必要に応じて、設置期限を設定し、返却時には機器を点検する。

#### 3.1.7 機器の廃棄等【対策基準 6.1.7】

対策基準 6.1.7 における「復元不可能な状態」とは、ハードディスク等の記憶装置からデータを単純に消去するだけでなく、データ復元ツールを使用しても復元ができないように公的機関が推奨する消去方式のデータ削除専用ソフトウェアで元の情報を残さず抹消した状態や、磁気データ消去装置や穴あけ装置などで物理的に記憶装置を破壊した状態のことをいう。

また、復元不可能な状態にする作業を業務委託等（再委託等を含む）する場合は、委託事業者等との間で守秘義務契約を締結するだけでなく、職員の立ち会い又は証拠書面の提出により履行確認を確実に行ったうえで、機器内部の記憶装置からすべての情報を消去し、復元不可能な状態にする措置を講じることが仕様書へ明記して確実に相手方に遵守させなければならない。

分類	機器の廃棄等の方法	確実な履行を担保する方法
<p>（１）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体</p> <p>※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ</p>	<p>当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。</p> <p>なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記する。</p>	<p>職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていること。なお、職員による左記措置の完了までの立ち会いについては、委託先事業者等の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。</p>
<p>（２）機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）</p>	<p>一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。</p> <p>具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択すること。</p>	<p>庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。</p>

分類	機器の廃棄等の方法	確実な履行を担保する方法
(3) 機密性 1 に該当する情報を保存する記憶媒体	<p>一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去すること。</p> <p>具体的には、(2) に記述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。</p> <p>OS 及び記憶装置の初期化（フォーマット等）による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない</p>	<p>庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。</p>
※上記（１）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

## 3.2 管理区域（情報システム室等）の管理【対策基準 6.2】

### 3.2.1 管理区域の構造等【対策基準 6.2.1】

#### ア 区域の定義

対策基準 6.2 における「管理区域」以外の区域を定義する。

##### (1) 執務区域

職員等が、通常執務を行う区域。執務室や会議室スペース等、庁舎内の区域を、執務区域と位置づける。  
(なお、対策基準ならびにこの管理基準においては、在宅勤務の場合の自宅は執務区域に含めない。)

##### (2) 準管理区域

執務区域内にルータ、スイッチ等のネットワークの基幹機器及び重要な情報システムを設置した区域。主にサーバラックや機器等が設置されている施錠可能な区画等が対象区域となる。

##### (3) 一般区域

主に一般市民等が立ち入ることができる区域。

#### イ 管理区域の管理

(1) 対策基準 6.2.1 イで「地階又は 1 階に設けてはならない」としている理由は、部外者の管理区域への侵入を容易にさせないため及び大雨等による水害時の浸水の影響を防ぐためである。

(2) 対策基準 6.2.1 ウにおける「外部に通ずるドアは必要最小限」とは、原則として、通常利用するドアを 1 つに制限することをいう。通常利用するドアが複数存在する場合は、不正侵入のリスクが増える事になるため、監視カメラの設置、担当者による本人確認等別途対策を行うことが必要になる。

#### ウ 消火薬剤及び消防用設備

対策基準 6.2.1 オにおける「影響を与えるもの」とは、主に機器及び電磁的記録媒体へ影響を与える水や発泡性薬剤による消火設備のことをいう。対策としては、水や発泡性薬剤による消火設備を極力避け、二酸化炭素やハロンガス等、気体による消火設備とする。

### 3.2.2 入退室の管理【対策基準 6.2.2】

ア 対策基準 6.2.2 アにおける「許可された者」とは、当該業務を担当している職員等の他、職員等との打ち合わせや機器等の設置作業等のために、事前に入室の許可を得ている者をいう。ID カード等による認証等入退室管理設備を設置している場合には、入退室管理者は入退室管理設備を利用する者に、入退室管理設備の使用方法及び ID カード等による識別に関する管理方法をあらかじめ説明しておかなければならない。

イ 対策基準 6.2.2 ウにおける「外見上職員等と区別できる措置」とは、入室許可証等を常時見える位置に着用する等の措置をいう。職員等以外の者が管理区域に入室する際は、所定の手続きを経て、入退室管理者が入室許可証(ビジターバッジ等)を一時的に貸与する。なお、入室を許可された者は、貸与された入室許可証を入室中常時着用し、退室時に入退室管理者に返却しなければならない。

ウ 対策基準 6.2.2 エにおける「当該システムに関連しない」とは、作業目的等で使用するパーソナルコンピュータ等以外の機器のことをいう。対策としては、入退室の際に、適切でない機器等を所持していないか確認を行うこと等がある。また、対策基準 6.2.2 エの「端末、モバイル端末、通信回線装置、電磁的記録媒体等」は、「当該情報システムに関連しない」もの、又は「個人所有である」ものに限られる。

エ 対策基準 6.2.2 オにおける「情報管理者」を入退室の管理責任者（以下、「入退室管理者」という。）とする。ただし、複数の所属等の共通の情報資産が存在する区域の場合は、協議等により入退室管理者を定めなければならない。

オ 対策基準 6.2 に従うほか、管理区域の存在は、それを知る必要がある職員等や委託業者等だけに知らせ、公表はしない。管理区域を無人にする場合は、施錠を行う。また、無人の管理区域を設置した場合は、定期的に確認を行う。

### 3.2.3 執務区域の入退室管理【対策基準 6.2.2】

対策基準 6.2.2 では、管理区域の入退室管理が中心のため、執務区域の入退室管理について、以下に示す。

#### ア 入退室管理策

職員等以外の者が執務区域へ入室する場合は、入退室管理者もしくは面会する職員等から許可された者のみ入室可能とする。また、必要に応じて本人かどうかの確認と入退室管理簿の記載による管理を行うとともに、管理区域への入室と同様に入室許可証を貸与することも検討する。

#### イ 許可証を使用する場合の取扱い

職員等以外の者が執務区域に入室する際には、入退室管理者が定めた手続きを経て入室許可証(ビジターバッジ等)を一時的に貸与する。なお、入室を許可された者は、貸与された入室許可証を入室中常時着用し、退室時に返却しなければならない。

### 3.2.4 機器等の搬出入【対策基準 6.2.3】

対策基準 6.2.3 アにおける「既存の情報システムに与える影響」がないようにするため、搬入出の際に

十分な人員及び作業スペースが確保されているか等の確認を実施する。また、外部の者が搬入出のため、管理区域に立ち入る場合は、職員等が同行し搬入出作業に立ち会わなければならない。

### 3.3 通信回線及び通信回線装置の管理【対策基準 6.3】

#### 3.3.1 庁舎内の通信回線等の管理【対策基準 6.3.1】

対策基準 6.3.1 における「通信回線及び通信回線装置に関連する文書」とは、例えば「通信回線敷設図」、「結線図」、「ネットワーク構成図」、「通信回線の契約書」等の文書をいう。

#### 3.3.2 機密を要する情報システムで使用する回線【対策基準 6.3.4】

ア 対策基準 6.3.4 における「適正な回線」とは、閉域イーサネット、専用線、IP-VPN 等の閉域網をいう。

イ 次の条件にあてはまるときは、情報セキュリティ管理者が許可した場合に限り、機密性 2 以上の情報を取り扱うことができるものとする。

(1) インターネット VPN を利用してシステムまたは外部サービスを利用する場合

(2) ファイアウォール、WAF、IP アドレス制限等の付加的なセキュリティ対策を施したシステムまたは外部サービスとの通信にインターネット回線（TLS 通信）を利用する場合

ウ インターネット回線の利用は、TLS 通信を用いることを条件として、次の場合に限り利用可能とする。

(1) Web 会議や監視カメラ等の映像通信サービスを利用する場合

(2) 対策基準 8.1.14 の特定用途機器により通信する場合

#### 3.3.3 ネットワークの可用性の確保【対策基準 6.3.5 イ】

情報基盤管理者及び業務システム管理者は、対策基準 6.3.1 通信回線及び通信回線装置の管理 に従うほか、管理するネットワークの可用性の確保についても考慮しなければならない。可用性を確保するために考慮すべき内容は、以下の通りとする。

ア ネットワークで使用する通信回線が、性能低下や異常によるサービス停止が発生しにくいものかどうか。

イ ピーク時においてもネットワークで使用する通信回線の容量及び機器の処理能力が十分に確保されるか。

ウ 可用性を確保するために通信回線や機器の冗長化を行う必要があるか。冗長化を行う場合、障害時に円滑に切り替えができるようになっているか。

エ 特定箇所での障害の影響がネットワーク全体に及ぶネットワーク構成になっていないか。

オ ネットワークで使用する回線や機器の監視を行い、障害からの復旧時間を短縮する必要があるか。

### 3.4 端末や電磁的記録媒体等の管理【対策基準 6.4】

#### 3.4.1 施錠保管庫【対策基準 6.4】

対策基準 6. 物理的セキュリティ に従う以外に、各所属の情報管理者は、機密性の高い情報資産等を保管する施錠保管庫、金庫、施錠キャビネット等について、以下の管理を実施する。

ア 施錠鍵及び保管物の管理者



情報管理者は、施錠鍵及び保管物の管理者を定める。保管物の管理者は、適切に保管物を管理する。

イ 施錠鍵及び保管物の管理状況の確認

情報管理者は、施錠鍵及び保管物が適切に管理されているか、定期的に確認を行う。

### 3.5 その他の管理策

#### 3.5.1 端末の盗難防止策【対策基準 6.4.1】

ア 対策基準 6.4.1 における「執務区域等の端末等」とは、マイナンバー利用事務系の端末、各種システムの専用端末のほか、デスクトップの事務処理用 PC、NAS、ネットワーク機器等をいう。

イ 盗難防止の措置には、ワイヤーロック、施錠管理等がある。

#### 3.5.2 ログイン認証【対策基準 6.4.2】

対策基準 6.4.2 アにおける「必要に応じて電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない」とは、情報システムのパスワード機能だけでなく、セキュリティ強化のため、他のパスワードとの併用を推奨していることをいう。なお、例示しているもの以外には、OS パスワードがある。

#### 3.5.3 認証の併用【対策基準 6.4.2】

対策基準 6.4.2 イにおける「知識」にはパスワード・パスフレーズ・暗証番号・ピクチャーパスワード等、「所持」には IC カード・USB トークン・SIM カード等、「存在」にはバイオメトリックス認証（指紋、声紋、静脈等）・リスクベース認証（行動パターン、キーボードを使う時の癖など）等がある。

#### 3.5.4 暗号化機能の利用【対策基準 6.4.3】

対策基準 6.4.3 における「端末等におけるデータの暗号化等の機能」には、セキュリティチップによるハードウェア自体の暗号化、の機能や OS 専用ソフトウェアによる暗号化等がある。

#### 3.5.5 モバイル端末の利用【対策基準 6.4.4】

ア 対策基準 6.4.4 ウにおける「覗き見防止の措置」には、端末の画面にプライバシーフィルタを装着する等がある。

イ 対策基準 6.4.4 エにおける「管理システム（MDM）」には次の機能を必須とする。

- (1)デバイス管理機能
- (2)ユーザー管理機能
- (3)チーム管理機能
- (4)アプリ管理機能
- (5)不正利用防止機能（リモートワイプ等）

#### 3.5.6 執務区域外における職員等の遵守事項【対策基準 7.1.1】

ア 対策基準 7.1.1 オにおける「モバイル端末」には、タブレット端末等のほか在宅勤務等により事務処理用 PC を執務区域外で使用する場合も含まれる。

イ 対策基準 7.1.1 オ(2)における「大量または機微な保有個人情報」の取扱いを禁止する趣旨は、執務区域外において大量又は機微な保有個人情報を取り扱う危険性を回避するものとする。また、ここでいう機微な保有個人情報とは、個人情報保護法第 2 条 3 項並びに神戸市会の個人情報の保護に関する条例第 2 条第 3 項の要配慮個人情報をいい、「公共の場所」とは道路、公園、広場、駅、空

港、劇場、レストラン等、有償・無償を問わず、不特定多数の者が、自由に出入りし利用することができる場所をいい、「公共の乗り物」とは電車、バス、飛行機等をいう。

ウ 対策基準 7.1.1 オ(3)における「細心の注意」とは、電車の網棚や自動車内・会議室・タクシー等に端末を放置せず常に身近に携帯し、歩道を通る際に端末の入ったかばんを車道側の手で持たない、自転車で運搬する場合は前かごに端末が入ったかばんを入れてカバーをかける、端末を保持したまま酒席に参加しない等、盗難・紛失防止に最大限の注意を払うことをいう。

エ 対策基準 7.1.1 オ(5)における「必要な対策」とは、端末を使用しない時間中は画面をロックし、認証に必要な職員証を端末のカードリーダーから取り外すこと等をいう。端末を使用しない場合は、施錠できる場所に LTE 接続端子を保管することを条件とする。

オ 対策基準 7.1.1 オ(6)における「指定されたファイルサーバの領域」とは、情報基盤管理者が指定したサーバのことである。(機密性 2 以上のデータについては必ずパスワードを設定すること。)

カ 対策基準 7.1.1 オ(6)における「端末内にデータを保存してはならない」の例外として、機密性 3 の情報資産を事務処理用 PC 以外のモバイル端末で執務区域外に持ち出す場合は、事前に情報セキュリティ統括責任者の許可を得なければならない。

キ 対策基準 7.1.1 オ(7)における「定期的」とは月に 1 回以上である。ただし、共用の端末の場合は、使用のたびに確認を受けるものとする。

情報管理者は端末実機の PC 管理番号等を確認するほか、端末内に業務データが保存されていないことを確認する。

ク 対策基準 7.1.1 オ(8)の例外として、業務上必要な範囲でモバイル端末をプリンタに接続して機密性 2 以上の情報資産の出力等を行う場合は、事前に業務内容の単位で情報セキュリティ統括責任者の許可を得なければならない。

ケ 対策基準 7.1.1 カ(1)における「業務に利用してはならない」の例外として、テレワークにおけるグループウェアの機能、又は通話やメール・アプリ等の連絡手段として個人の所有する端末又はモバイル端末を業務に利用するものや、事前に業務内容の単位で情報セキュリティ統括責任者の許可を得たものはこの限りではない。ただし、メール機能を業務利用する際は、付与された公用メールアドレスを用いなければならない。

### 3.6 パスワードの管理【対策基準 7.4.3】

ア 対策基準 7.4.3 カにおける「同一のパスワードをシステム間で用いてはならない」については、情報基盤管理者及び業務システム管理者があらかじめ同一パスワードをシステム間で用いるよう設定している場合を除く。

イ 対策基準 7.4.3 クにおける「パスワードを記憶させてはならない」については、情報基盤管理者及び業務システム管理者があらかじめ記憶させている場合を除く。

## 4. 技術的セキュリティ管理

### 4.1 コンピュータ及びネットワークの管理【対策基準 8.1】

#### 4.1.1 データの保存【対策基準 8.1.1】

対策基準 8.1.1 における「定める方法」とは、情報基盤管理者等権限のある者がデータの重要性を考慮

し、記録媒体、保存方法等を定めなければならない。また、その際にはデータの保存期間も併せて決定する。

#### 4.1.2 ファイルサーバの設定等【対策基準 8.1.2】

対策基準 8.1.2 における「ファイルサーバ」は、全市的に共用するファイルサーバを対象としているが、所属単位で設置する場合にもこれに準じた対策を行うことが推奨される。

ア 対策基準 8.1.2(1)における「周知」とは、職員等が使用できるファイルサーバの容量等の基本的事項だけでなく、障害が発生した場合の対応方法等について、周知することを含む。

イ 対策基準 8.1.2(2)における「所属等の単位で構成」とは、原則として所属毎にフォルダを作成し、他所属等からアクセス出来ないようにアクセス制御を実施することをいう。

ウ 対策基準 8.1.2(3)における「権限のない者が閲覧及び使用できないよう」とは、特定の職員しか取扱えない保有個人情報、人事記録等のデータを保護する対策のことをいう。管理者がサーバ上に専用ディレクトリを作成してアクセス制御を実施するか、職員等が当該データやファイル自体にパスワードを付けることによりアクセス制御を実施する等の方法がある。

#### 4.1.3 情報資産のバックアップ【対策基準 8.1.3】

ア 対策基準 8.1.3 アにおける「情報資産のバックアップ」とは、データの重要性、可用性等を検討した定期的なバックアップのことをいう。必要に応じて、確実に処理が行われたか、バックアップの処理が正常終了したかを確認し、その記録を行う。

イ 対策基準 8.1.3 イにおける「バックアップに関する本市が求める要求事項」には、RTO（目標復旧時間）と RPO（目標復旧時点）を考慮した対象データ、システム、バックアップ方式、実施手順、実施頻度、保存期間、保存場所及び復旧手順が挙げられる。

#### 4.1.4 他団体との情報システムに関する情報等の交換【対策基準 8.1.4】

対策基準 8.1.4 における「他団体」とは、国や他の地方公共団体等のことをいう。他団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関して以下の事項を予め定める。

ア 紛失した場合の責任

イ 不正アクセスからの保護義務

ウ 目的外の使用禁止

エ 内容改変の禁止

オ 外部漏えいへの対応及び損害賠償

カ 暗号機能の採用の有無

#### 4.1.5 仕様書等の保管【対策基準 8.1.6】

対策基準 8.1.6 における「適正に管理」とは、業務上必要とする者以外の者が閲覧、複製、改ざん、削除等が出来ないような対策が取られた保管のことをいう。保管されている場所から業務目的等で持ち出す場合は、持ち出し記録を作成する。

#### 4.1.6 ログの取得等【対策基準 8.1.7】

ア 対策基準 8.1.7 アにおける「情報セキュリティの確保に必要な記録」とは、アクセスログ、システム稼動ログ、障害時のシステム出力ログ及び障害対応記録等のログであり、第三者等による不正侵入や不正操作等の情報セキュリティインシデントを検知するための重要な材料となる。また、情

報システムに係る情報セキュリティの上の問題が発生した場合には、当該ログ等は、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログ等が取得され、改ざんや消失等が起こらないよう、ログ等が適切適正に保全保存されなければならない。目的や取得する機器の明確化のほか、取得後において定期的又は必要に応じて確認をしなければならない。またログは1年以上保存する。

イ アクセス記録等を厳密に管理する必要がある情報システムのサーバについては、時刻同期が正しく行われているかどうか定期的に確認しなければならない。

ウ アクセス記録等は保管期間を設定し、期限が切れた場合は、これらの記録を確実に消去する等、適正な処置を施さなければならない。

エ 対策基準 8.1.7 ウにおける「保護」について、クラウドサービス事業者が管理主体の部分の記録については、収集される記録の内容、収集される期間及び保存される期間といった記録の保護機能に関する対応状況も入手できない可能性がある。不正アクセスの記録の調査及び証拠保全のためには記録が取られることが必要であるため、利用するクラウドサービスにおいて記録の収集が行われるか、行われる場合は収集される記録の内容、収集される期間及び保存される期間について確認しておく必要がある。

一方、クラウドサービス利用者が管理主体の部分の記録については、サービスとして記録の保護機能が提供されている場合がある。ただし、これらは、クラウドサービスモデルやクラウドサービス事業者の方針により、入手不可の場合がある。よって、クラウドサービス利用開始前の段階で、こうした機能に関する情報が入手できるサービスモデルやクラウドサービス事業者を選択する必要がある。なお、サービスとして記録の保護機能が提供されない場合は、クラウドサービスで発生する記録をクラウドサービス利用者のオンプレミス環境等にコピーして保存及び保護する方法も考えられる。

オ 対策基準 8.1.7 エにおける「外部記録媒体」とは、DVD-RAM 等耐久性に優れている電磁的記録媒体のことをいう。それらは、磁気や温度変化等の媒体劣化の要因が少ない場所で保管しなければならない。

カ 対策基準 8.1.7 オにおける「デジタルフォレンジック」とは、電子データを調査分析することで事実解明及び証拠保存を行うための技術のことをいい、アプリケーション、システム及び通信のログ、システムのディスク並びにメモリのイメージが含まれる。ただし、これらは、クラウドサービスモデルやクラウドサービス事業者の方針により入手不可の場合がある。よって、クラウドサービス利用開始前の段階で、監査項目の確認等により必要なデジタル証拠を事前に定義し、そうした情報が入手できるサービスモデルやクラウドサービス事業者を選択する必要がある。

#### 4.1.7 ネットワークの接続制御、経路制御等【対策基準 8.1.9】

対策基準 8.1.9 アにおける「アクセスできる者」とは、情報基盤管理者及び業務システム管理者から承認を受けた者のことをいう。ネットワークの使用制限に関しては、ルータ等ネットワーク間の適切なインターフェースの設置、利用者の認証機構、利用者のアクセス制限等を考慮する。

#### 4.1.8 強制的な接続制御、経路制御【対策基準 8.1.9】

ア 対策基準 8.1.9 イにおける「フィルタリング及びルーティング」によって、電子メール、ファイル転送、対話型アクセス、業務用ソフトウェアによるアクセス等を決められた経路のみを通過する

よう制御する。対策として、ファイアウォールやルータ等のセキュリティゲートウェイ機能を使った制御を行う。

イ 対策基準 8.1.9 イにおける「設定の不整合」とは、ファイアウォール、ルータ等の誤設定により、接続対象先のサーバ等にアクセス出来ない状態になってしまうことをいう。

#### 4.1.9 外部の者が利用するシステム【対策基準 8.1.10】

ア 対策基準 8.1.10 アにおける「外部の者が利用できるシステム」とは、市民等がアクセス可能なインターネット等により公開されているシステムのことをいう。不正アクセス等の脅威が増大するため、他の情報システムと物理的な分離、データベースへの不正アクセス防止、システムファイルの置換防止、厳格な認証機能等、情報セキュリティ対策について、特に強固に対策をとらなければならない。

イ 対策基準 8.1.10 ウにおける「多段階認証」とは、情報システムが正規の利用者かどうかを判断する認証手段のうち、単体又は複数の要素を用いて 2 回以上の認証を要求するものをいう。

#### 4.1.10 外部ネットワークとの接続【対策基準 8.1.11】

ア 対策基準 8.1.11 アにおける「情報資産に影響が生じないことを確認」する方法としては、事前に十分な技術的調査を実施し、障害時に物理的に遮断が可能なこと等を契約書等に記載する。

イ 対策基準 8.1.11 イにおける「契約上担保」とは、本市の情報資産が漏えい、破壊、改ざんされたために業務への影響が出た場合、損害賠償請求権があることを契約書等に記載しておくことをいう。

#### 4.1.11 Web サイトでの情報公開時の注意事項【対策基準 8.1.12】

ア 対策基準 8.1.12 アにおける「防止」について、攻撃手法は日進月歩なので限定しづらいが、「安全なウェブサイトの作り方」(IPA)掲載のセキュリティ実装チェックリストが参考になるので、仕様書等で引用するなどして備えておく。対策としては、IDS による検知、IPS による不正侵入防御、ファイアウォール機能や負荷分散装置の設置等による Dos 攻撃対策、ファイル書換えの検知及び防止システム、WAF の導入等がある。

なお、公的な Web サイトを開設する際は、ドメイン管理にも相応の注意を払う。利用者が公的な Web サイトを閲覧するときは、より高い信頼感をもっていることが予想されるため、悪質ななりすましサイトが現れたときの被害も大きくなることが予想されるからである。したがって、可能な限り「lg.jp」ドメインを利用しなければならない。独自ドメインを利用するときも、利用者に正規のサイトであることが分かりやすいドメインにしたり、サーバ証明書の活用を検討したりするなどの対策が求められる。さらに、旧ドメインを取得した第三者が悪用するのを防ぐため、ドメインを変更・廃棄するときは、旧ドメインを 1 年程度保有しておく。

イ 対策基準 8.1.12 ウにおける、「全てのページの TLS 通信の必要性」とは、公衆 Wi-Fi ネットワーク利用端末と Web サーバとの通信を盗聴されたり、正規の利用者に成りすまして Web サービスにアクセスされたりする危険の他、情報を盗まれるだけでなく、悪意のあるプログラムが埋め込まれるように通信情報が改ざんされる可能性があるためである。

また、一般的に使われるブラウザで、TLS 通信を行っていない Web ページを閲覧した場合、URL 欄などに、通信が保護されていない旨の警告が表示されるようになり、閲覧者に不安を与えてしまわないよう、全てのページで TLS 通信を行う必要もある。

TLS 通信を行っている Web ページでは URL が https://から始まるため、http://から始まる URL の Web ページがすでに公開されている場合、早急に対策することが求められる。

#### 4.1.12 複合機のセキュリティ管理【対策基準 8.1.13】

対策基準 8.1.13 における「複合機」とは、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。複合機は、庁内ネットワークや公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定されることに注意が必要である。

#### 4.1.13 IoT 機器を含む特定用途機器【対策基準 8.1.14】

ア 対策基準 8.1.14 における「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途だけに使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。

例えば、テレビ会議システム、IP 電話システム等は組織等 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。これらの IoT 機器等の脆弱性がサイバー攻撃の標的となることが懸念される。また、内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。そのため、特定用途機器の特性に応じて、以下の対策を講じるものとする。

- ・ 特定用途機器について、認証情報を初期設定から変更した上で、適切に管理する。
- ・ 特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。
- ・ 特定用途機器が備える機能のうち利用しない機能を停止する。
- ・ インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接点を有する情報システムに接続しない。
- ・ 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
- ・ 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

イ 対策基準 8.1.14 における「機器の特性に応じた対策」とは、定期的なファームウェアの更新、適切なパスワードの設定、適切なルータ経由でのインターネットへの接続等のことをいう。また、原則としてこれらの対策については、メーカーによるサポートが提供されているものを利用しなければならない。

#### 4.1.14 無線 LAN 等の利用【対策基準 8.1.15】

ア 対策基準 8.1.15 における「無線 LAN」の脅威として、無線電波の漏えいによる通信の盗聴、無線 LAN のアクセスポイントを通じたネットワーク内のサーバやパーソナルコンピュータへの不正侵入、同一周波数帯の機器を使用することによるネットワークの利用妨害等がある。有線 LAN での接続に比べ、情報漏えい等が発生しやすいため、職員等は、庁内のネットワークにおいて、無線 LAN を利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。特に、

LGWAN 接続系で無線 LAN を利用する場合は、盗聴及びなりすましアクセスポイント（AP）などによる情報漏えいや不正アクセスに対して、認証サーバを利用した WPA2/WPA3 エンタープライズによる認証（IEEE802.1X 認証）を採用する等、セキュリティ対策を実施しなければならない。なお、マイナンバー利用事務系においては、無線 LAN は利用しないこととしなければならない。

イ インターネット回線を用いた無線 LAN 構築は、他の方法では構築することが困難である等合理的な理由があり、情報セキュリティ統括責任者が情報セキュリティを確保するために別途定める要件（通信の暗号化、端末認証及びユーザー認証等の対策が行われていること）を満たす場合に限り、情報セキュリティ管理者の許可を得て、無線 LAN を利用した接続等を行うことができる。その場合、アクセスポイントの管理者パスワードを適切に設定（強固な ID・パスワードの設定、アクセスポイント単位での管理など）を行うとともに、無線端末間の通信が行われないよう適切な設定を行わなければならない。

ウ 対策基準 8.1.15 アにより「端末等の無線機能を利用した端末間通信を行ってはならない」が、以下の場合を例外とする。

(1)ワイヤレス映像転送機器を利用する場合

(2)Bluetooth 通信（目の届く範囲での利用に限る）により接続するマウス、キーボード、プリンタ等の PC 周辺機器（データ保存機能のあるものを除く）を利用する場合

(3)支給端末間で印刷または表示の用途に限って Wi-Fi ダイレクトを利用する場合

#### 4.1.15 電子メールのセキュリティ管理【対策基準 8.1.16】

対策基準 8.1.16 に従うほか、外部への電子メール送信においてなりすまされる事を防ぐため、送信するメールは SPF などによる送信ドメイン認証された@office.city.kobe.lg.jp をはじめとするドメインを利用しなければならない。

#### 4.1.16 利用可能なネットワークプロトコル【対策基準 8.1.22】

対策基準 8.1.22 における「業務上必要最低限」とは、主に Web サイトの閲覧やメール送受信で使用するプロトコル等、職員等が業務上利用するアプリケーションで使用するプロトコルのみに絞込みを行なうことをいう。

#### 4.1.17 Web 会議サービスの利用時の対策【対策基準 8.1.24 ア】

対策基準 8.1.24 アにおける Web 会議サービス利用時の情報セキュリティ対策として、下記の対策を実施する必要がある。

- ・原則として、公用アカウントを利用すること。
- ・外部から招待された場合を除き、外部サービス利用基準に従って許可された Web 会議サービスを利用すること。
- ・利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認すること。
- ・機密性 2 以上の情報を取り扱う場合は、外部サービス利用基準に基づいて機密性 2 以上の情報の取り扱いを認められているサービスを利用すること。
- ・機密性 2 以上の情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を使用しないこと。
- ・音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

#### 4.1.18 Web 会議サービス主催時の対策【対策基準 8.1.24 イ】

対策基準 8.1.24 イにおける会議に無関係の者が参加できないようにするための対策として、以下の情報セキュリティ対策を講ずる。

- ・会議室にアクセスするためのパスワード等をかける。
- ・会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。
- ・待機室を設けて参加者と確認できた者だけを会議室に入室させる。
- ・なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

#### 4.1.19 ソーシャルメディアサービスによる情報発信【対策基準 8.1.25 ア(1)】

ア 対策基準 8.1.25 ア(1)のなりすまし対策として、情報管理者は以下の対策を行うこと。

- (1)本市からの情報発信であることを明らかにするために、本市のドメイン名を用いて管理している Web サイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設ける。
- (2)本市からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、自組織が運用していることを利用者に明示する。
- (3)運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている自組織の Web サイト上のページの URL を記載する。
- (4)ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得する。
- (5)URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

イ 情報管理者は、対策基準 8.1.25 エの第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下のとおり対策を行うこと。

- (1)パスワードを適切に管理すること。具体的には、ログインパスワードには十分な長さで複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしない。
- (2)多段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する。
- (3)ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難にあった場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行う。
- (4)ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施する。

また、なりすましや不正アクセスを確認した場合の対処として、以下のとおり対策を行うこと。



- (1)本市 Web サイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行う。
- (2)アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、本市 Web サイト等で周知を行うとともに、本市自組織のエスカレーションルールに従い報告する。

## 4.2 アクセス制御【対策基準 8.2】

### 4.2.1 利用者 ID の取扱い【対策基準 8.2.1】

ア 対策基準 8.2.1 イ(2)における「利用者 ID の取扱い等」とは、利用者の所属部署、役職、在籍の有無等の状態と ID の権限が連動した取扱いのことをいう。情報基盤管理者及び業務システム管理者が担当業務に応じたアクセス範囲とアクセスレベルを定める。情報基盤管理者及び業務システム管理者は、許可しているアクセスのレベルが業務の目的に適合しているか、補職等に応じた権限となっているかを定期的に検査する。また、情報基盤管理者及び業務システム管理者は、情報システムごとユーザーID・権限の登録・変更・削除が申請され上長により承認される手続きについて、記録し保管する。

イ 対策基準 8.2.1 イ(2)に従うほか、職員認証基盤システムと連携する場合や所属等ごとにユーザーID が配布されている場合を除き、原則として、一つの情報システムにつき一人が一つのユーザーID を使用し、複数の人が一つのユーザーID を使いまわしてはならない。また、情報基盤管理者及び業務システム管理者はアクセス範囲やアクセスレベルが容易に推測できるようなユーザーID 体系にしてはならない。

ウ 対策基準 8.2.1 イ(3)における「利用されていない ID」とは、主に退職者や異動等により業務から離れた者が利用していた ID のことをいう。情報基盤管理者及び業務システム管理者は、利用されていない ID が利用できる状態のまま放置されないよう、定期的に点検し、その結果を記録し保管しなければならない。

### 4.2.2 特権 ID の管理等【対策基準 8.2.1 ウ】

ア 対策基準 8.2.1 ウ(1)における「厳重に管理」とは、特権 ID を利用する者を最小限に絞込み、暗号化ファイルによる利用者への通知、定期的な変更等、一般ユーザーの ID より厳しいルールで管理することをいう。

イ 対策基準 8.2.1 ウ(2)における「委託事業者等に行なわせてはならない」の例外として、サービス提供型の委託事業者等に関しては、契約内容でセキュリティが担保されている事が確認出来れば、特権 ID 及びパスワードの変更を認める。

ウ 対策基準 8.2.1 ウ(3)における「それ以上のセキュリティ強化」とは、職員等の端末用のパスワードのルールより、最低パスワード長、文字列に含まれる文字の種類、変更間隔等を厳しく設定することをいう。

### 4.2.3 職員等による外部からのアクセス【対策基準 8.2.2】

ア 対策基準 8.2.2 アにおける「外部からのアクセスを許可する場合」のうち、職員等がテレワークにより市内ネットワークや情報システムに接続を認める場合には、外部からの不正な通信、マルウェアによる情報漏えいを防ぐために、接続に際してアクセス制御等の技術的対策を行う。また、な

りすまし、情報漏えい及び盗難・紛失といったリスク等を踏まえ、接続するネットワークで扱う情報の重要度を勘案しつつ、適切なセキュリティ対策を講じる。なお、マイナンバー利用事務系は、住民情報等の特に重要な情報資産が大量に配置されており、情報漏えいリスクが高いこと等を踏まえ、テレワークの対象外としなければならない。

LGWAN 接続系の情報資産には、職員の個人情報等重要な情報資産が配置されている。テレワークにおいては、情報資産の重要性を踏まえ、取り扱う情報資産を明確にする。なお、大量又は機微な住民情報を扱う業務がある場合、庁舎と同等の物理的な対策がなされたサテライトオフィスでの場合を除き、テレワークの対象外とする。

イ 対策基準 8.2.2 イにおける「利用者の本人確認を行う機能」を確保するための対策として、必要に応じて、ワンタイムパスワードや生体認証の使用等の措置を講じなければならない。

ウ 対策基準 8.2.2 ウにおける「通信途上の盗聴を防御するため暗号化等の措置」とは、具体的には、以下のモデルを採用し、各モデルを導入する際は、「新型コロナウイルスへの対応等を踏まえた LGWAN 接続系のテレワークセキュリティ要件について」（令和 2 年 8 月 18 日 総務省自治行政局地域情報政策室長通知）にある技術要件を遵守しなければならない。

（インターネット回線を使用しないモデル）：

- ・閉域 SIM による接続サービスを利用するモデル

（インターネット回線を使用するモデル）：

- ・LGWAN-ASP サービスを利用して庁内にある LGWAN 接続系の端末に接続するモデル
- ・インターネット接続系を経由して LGWAN 接続系の端末に接続するモデル

エ 対策基準 8.2.2 エにおける「セキュリティ確保のために必要な措置」とは、貸与前や、持ち帰ったモバイル端末を庁内ネットワークに接続する前に、最新の定義ファイルでスキャンを行ったり、OS 等をアップデートしたりするなどして、ウイルス等に感染していない状態を確保することをいう。

#### 4.2.4 内部ネットワーク間の接続【対策基準 8.2.3】

対策基準 8.2.3 アにおける「情報資産に影響が生じない」対策として、アクセス制御を職員毎もしくは所属単位で実施するか、追加のルーティングで適切に制御すること等がある。

#### 4.2.5 ネットワーク機器の自動識別【対策基準 8.2.4】

対策基準 8.2.4 における「自動識別の設定」の目的は、ネットワークに不正な機器の接続を防止するためであり、電子証明書による端末認証や、接続する機器の IP アドレス、MAC アドレス等の認証情報を利用し制限する。

#### 4.2.6 ログイン試行回数の制限等【対策基準 8.2.5】

対策基準 8.2.5 に従うほかに、以下の対策についても考慮しなければならない。

ア 情報システムの識別する情報は正常なログインが終了するまで表示しない。

イ ログイン時に誤り条件があっても、どの部分が間違っているか指摘はしない。

ウ ログイン手順中に利用者への手助けになるようなメッセージを表示しない。

エ 前回のログイン又はログアウト時刻を表示する。

#### 4.2.7 パスワードに関する情報の管理【対策基準 8.2.6】

ア 対策基準 8.2.6 アにおける「セキュリティ強化機能」とは、パスワードの文字数や文字の種類以外にも同一文字の使用数制限等、より厳密なパスワード設定を行う事が可能な機能をいう。

イ 対策基準 8.2.6 イにおける「仮のパスワード」とは、職員等のパスワードを発行するにあたり、一時的に短時間有効なパスワードを職員等に付与することをいう。

ウ 対策基準 8.2.6 ウに従うほか、職員等への周知としては、以下のようなことがある。

- (1) パーソナルコンピュータ等の端末のパスワードの記憶機能を利用してはならない。(情報基盤管理者及び業務システム管理者があらかじめ記憶させている場合を除く。)
- (2) 職員等の間でパスワードを共有してはならない。
- (3) パスワードの照会等には一切応じてはならない。

エ 対策基準 8.2.6 ウの規定は、パスワードに一定のセキュリティ強度を確保するためのものである。

オ 対策基準 8.2.6 ウにおける「想像しにくいもの」とは、パスワードの文字列として、誕生日等の本人関連情報、「apple」等の辞書に含まれる単語、同じ文字・英字・数字で連続したもの、「qwerty」等のキーボードの連続した並び等、容易に推測出来るものを使用しないことをいう。

カ 対策基準 8.2.6 エにおける「古いパスワードの再利用は行なわない」の対策として、パスワード変更の際にチェックを行い、現在使っているパスワードを入力した時にエラー表示及び再入力の指示を出す機能をシステム上に実装すること等がある。

キ 対策基準 8.2.6 オにおける「認証情報の不正利用を防止」とは、ID・パスワードの厳重な管理の他に、ID カード等の管理がある。万が一 ID カード等を紛失した時は直ちにそのカードを無効化する等の処置を講じる。

### 4.3 システム開発、導入、保守等【対策基準 8.3】

#### 4.3.1 情報システムの調達【対策基準 8.3.1】

ア 対策基準 8.3.1 アにおける「調達仕様書」を作成するにあたり、「神戸市情報システム調達ガイドライン」を参照した上で、運用及び利用面で必要となるセキュリティ機能を洗い出し、一般に公開する調達仕様書にアクセス制御、パスワード設定等の技術面で必要となるセキュリティ機能を明記する。オンラインでの申請及び届出等の手続を提供するシステムについては、住民が情報システムのアクセス主体になることにも留意し、オンライン手続におけるリスクを評価した上で、認証に係る要件を策定する。

イ 対策基準 8.3.1 イにおける「ソフトウェアの調達」にあたり、システムにおいて必要とするセキュリティ機能に一番近い製品を調達するため、複数のソフトウェア等を評価し、決定する。

ウ 対策基準 8.3.1 ウに規定する「情報システム台帳」は、市全体の情報システムにおける情報セキュリティ対策の基礎資料として非常に重要である。台帳記載事項に変更があったときは、業務システム管理者は、照会に応じて、その旨を報告しなければならない。

#### 4.3.2 情報システムの開発等【対策基準 8.3.2】

ア 対策基準 8.3.2 アに従うほか、以下の事を考慮する。

- (1) 容量・能力等の計画作成

情報基盤管理者及び業務システム管理者は、情報システムが将来にわたって十分な処理能力及び記憶

容量を維持し、障害・停止が起こらないよう考慮したシステム導入計画書を作成し、管理策を策定する。

- ・プロセッサの性能
- ・メモリの容量
- ・ディスク容量
- ・通信システム（トラフィック、通信速度等）
- ・関連するアプリケーションや外部ネットワークとの関係（相性、互換性）
- ・耐障害性（フォールトトレランスの機能等）

## (2)変更開発の管理

情報基盤管理者及び業務システム管理者は、既存情報システムを変更する場合は、事前に変更の必要性和影響度合いを十分に検討し、変更の実施を職員等の利用者へ適切に通知の上、既存業務に影響を与えないよう適切な時期に行う。また、あわせて仕様書や操作手引きなど関連文書を更新する。システム変更の際は、システム変更管理記録を作成し、適切に管理する。

## (3) 試験計画

情報基盤管理者及び業務システム管理者は、予め決められた計画、内容に従って試験を行い、原則、本番データを試験環境で利用してはならない。ただし、合理的な理由があり、情報セキュリティ統括責任者が許可した場合はこの限りでない。試験には、機能試験、性能試験、運用確認試験を盛り込む。

## (4) 試験結果

業務システム管理者は、以下の項目を確認して、本番適用を判断する。

- ・試験計画書の試験項目が通常時と例外時を網羅している。
- ・試験計画書の全試験項目が終了している。
- ・試験段階で確認されたバグが修正されている。
- ・バッチ処理等、職員等の利用者が直接係わらない処理についても試験が終了している。
- ・性能試験結果に本番環境と試験環境の違いを加味して本番環境での性能パフォーマンスを予測し、その結果が要求基準を満たしている。
- ・職員等の利用者による運用確認試験を完了している。

## (5) 本番運用準備

業務システム管理者は、以下の項目を確認して、本番運用準備を行なう。

- ・運用を委託等した際のデータセンター運用等の受入れ手続きが終了している。
- ・本番適用後の障害発生時の対応体制が整っている。
- ・仕様書、運用マニュアル、プログラムソース等の納品物が揃っている。
- ・本番データの移行が完了している。
- ・開発した担当者のユーザーID、パスワード等が不要になった時点で、速やかに抹消されている。

イ 対策基準 8.3.2 イにおける「不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用等、問題のある行為が発生しないように」には、システム等の納品時に、開発時に使用した委託先等所有のソフトウェアが端末にインストールされたままの状態での納品されていないかを確認することも含む。

### 4.3.3 情報システムの導入【対策基準 8.3.3】

ア 対策基準 8.3.3 ア(1)における「移行手順を明確に」するため、移行についての事前準備、要求分析、外部設計、内部設計、詳細設計、試験、導入等の移行計画を作成しなければならない。必要に応じてデータ、プログラム等を移行するのに有益な、移行ツールの開発もしくは調達を行う。また、業務システム管理者は、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

イ 対策基準 8.3.3 イ(1)における「十分な試験」とは、予め作成された試験計画に従い、正常な動作を保証する網羅的な試験のことをいう。必要に応じて、新旧情報システムの並行運用を行う。

ウ 対策基準 8.3.3 イ(2)における「擬似環境」は、業務に精通している利用部門の協力のもと構築する。また、作業について、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

エ 対策基準 8.3.3 イ(3)における「生データ」とは、本番環境で使用しているデータのことをいう。

オ 対策基準 8.3.3 イ(5)における「一定期間厳重に管理」とは、試験に使用するデータは改ざん等があってはならないため、本市が定めた期間はアクセス制御された措置の下で管理することをいう。また、当該データが不要になった時点で速やかに削除しなければならない。

#### 4.3.4 システム開発・保守に関連する資料等の整備・保管【対策基準 8.3.4】

対策基準 8.3.4 イにおける「システム変更等の作業」は、十分な試験を行い、変更作業によって稼動が保証される状態で実施されなければならない。また、作業に誤りがなかったかを確認するため、作業管理記録を残さなければならない。作成した作業記録は、上長による承認を受けたうえで、窃取、改ざん等が行なわれないように、アクセス制御、施錠管理等を行い、本市が定める期間保管する。

#### 4.3.5 情報システムの入出力データの正確性の確保【対策基準 8.3.5】

ア 対策基準 8.3.5 アにおける「チェック機能」とは、情報システムにデータを入力する時点でデータが適切なものかどうか判断し、ユーザーに通知する機能等のことをいう。

イ 対策基準 8.3.5 イにおける「検出するチェック機能を組み込む」とは、データの改ざん又は漏えいを防止するための機能を情報システムの内部処理に組み込むことをいう。

ウ 対策基準 8.3.5 ウにおける「正しく反映され、出力される」とは、入力したデータが適切な内部処理、出力処理を経て、出力されることをいう。情報システムの処理した結果の正確性が確保されるよう、適切な設計を行なう。

エ 対策基準 8.3.5 ウに従うほかに、情報システムから出力した帳票等を払出し先に渡す場合、いつ誰に引き渡したかの記録を残すため出力帳票等受払簿に記録しなければならない。

#### 4.3.6 ソフトウェアの保守及び更新【対策基準 8.3.7】

対策基準 8.3.7 における「不具合及び他のシステムとの相性の確認」の対策として、不完全な処理が行われた場合のリスクの把握と不具合が起きた時の管理策を決めておく。それらを担保するため、ソフトウェアの提供元に本市の環境下でソフトウェアが稼動することを確認し、将来的なソフトウェア保守についての契約を締結する。

## 4.4 不正プログラム対策【対策基準 8.4】

### 4.4.1 情報基盤管理者等の措置事項【対策基準 8.4.1】

ア 対策基準 8.4.1 アにおいて、データ及びソフトウェアをインターネット経由で送受信するシステムの場合は、ゲートウェイにも別種類のウイルス対策ソフトウェアを導入することによりウイルスチェックを二重に実施する。また、対策基準 8.4.1 アにおける「常駐」とは、端末等の電源を入れた状態から自動的に起動し、動作し続けるウイルス対策ソフトウェアのことをいう。

イ 不正プログラムの検出、予防及び不正プログラムによる障害からの回復のため、以下の管理策を実施することが望ましい。

- (1) 異なる業者及び技術による不正プログラム対策ソフトウェア製品を複数利用することによって、マルウェアからの保護の有効性を高める。
- (2) 緊急時手順においては、不正プログラムに対する通常管理策を回避する場合があるため、不正プログラムの侵入防止に向けた注意を払う。
- (3) マルウェアの検出及び修復ソフトウェアだけを利用するのでは不十分であるため、不正プログラムの侵入を防止するための運用手順を併用する。

ウ 対策基準 8.4.1 カにおいて、適切な、不正プログラム対策とは以下の対策をいう。

- (1) ネットワークの分離や分割が正しく設定できている。
- (2) 導入している各機器や OS 等の資産管理を行い、脆弱性に関する最新の情報を漏れなく収集する。収集した情報に基づき修正を速やかに実施する仕組みとなっている。特に、インターネット接続系に配置したものについては、必要となる脆弱性の修正を速やかに実施する。
- (3) パスワードを第三者に推測されないようなものに設定し、システム・機器ごとに異なるものを設定する。また、デフォルト値での設定をしない。
- (4) ランサムウェアによる犯罪の手口とその対策に関する注意喚起と啓発を行う。
- (5) 利用しているネットワーク機器やリモートデスクトップのソフトウェアの脆弱性を速やかに修正する。
- (6) 必要の無い通信や不要サービスの設定がされていることはないか、各種設定の情報を確認する。
- (7) メールやファイル無害化の設定が正しく実施されているか定期的に確認するとともに、無害化を行う機器やソフトウェアの脆弱性を速やかに修正する。
- (8) 端末におけるウイルス対策ソフトの導入と定義ファイルの更新、OS 等の修正プログラム等の更新がされているか確認する。定義ファイルや修正プログラム等は速やかに更新を実施する。
- (9) OS 等の権限において、最小権限の設定がされているか確認する。

#### 4.4.2 職員等情報取扱者の遵守事項【対策基準 8.4.2】

ア 対策基準 8.4.2 クにおいて、ウイルス感染時等の対応としては、まずは情報管理者等への報告を第一としている。趣旨は、標的型攻撃の場合、気づいた時点では既に不正侵入済であることが多く、証拠保全の方が重要となるためである。ただし、標的型攻撃に気づくことは難しいため、不審に思い、判断に迷ったときは、被害拡大防止を最優先に、LAN ケーブルを抜く、又は無線 LAN の接続を切断する対応も次善の策としてとりえるものとする。

イ 対策基準 8.4.2 ケにおいて、必要なソフトウェアのみをインストールすることとしている。趣旨は、多数のソフトウェアのアップデート等をその都度行って最新の状態に保つこと自体が困難であるため、業務上必要となるケースは限定的と考えられるので、必要度が低ければインストールしない方が安全であることを規定したものである。

#### 4.4.3 専門家の支援体制【対策基準 8.4.3】

対策基準 8.4.3 の「専門家」とは、本市の各管理者等では原因追及出来ないウイルスの感染が発生した場合に、協力を仰ぐことの出来る者をいう。必要に応じて、それらの専門家もしくは外部事業者から定期的なサービスを受けられるようにしておく。

### 4.5 不正アクセス対策【対策基準 8.5】

#### 4.5.1 使用されていないポートの閉鎖等【対策基準 8.5.1】

ア 対策基準 8.5.1 アにおける「使用されていないポートを閉鎖」とは、サーバにおいて、端末からの要求に対応するために必要なもの以外の通信の出入り口であるポートを閉じておくことをいう。サーバではなく、ルータ等の機器により制御することもある。

イ 対策基準 8.5.1 イにおける「不要なサービスを停止」とは、サーバにおいて不要な機能（Web 公開サーバであれば、メールや DNS といったサービス）を無効にすることもしくは削除することをいう。不要なサービスを起動しておく、そのサービスを使用する想定になっていないため脆弱性が発生した場合の対応が遅れ、脆弱性を利用した不正アクセスを受けるおそれがある。

ウ 対策基準 8.5.1 における「以下の事項の措置」に従うほか、以下のことを考慮しなければならない。

- (1) ネットワークの負荷を監視する。
- (2) 重要な情報の場合は、アクセスを許可する相手先を限定する。
- (3) システム関連のファイルはアクセスできないよう管理する。
- (4) 特権 ID 及びパスワードは厳重に管理し、特権 ID は定期的に変更する。
- (5) 重要な情報は、削除、改ざん、漏えい等が発生した場合の被害を少なくするため、一つのサーバやデータベース等に集約しないよう分散化に努める。

エ 対策基準 8.5.1 に従うほか、DNS の導入時には以下の対策を講じなければならない。

- (1) 庁外からの名前解決の要求に応じる必要があるかについて検討し、必要性がないと判断される場合は庁内からの名前解決の要求のみに応答をするよう措置を講じる。
- (2) DNS キャッシュポイズニング攻撃から保護するための措置を講じる。
- (3) ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新が明示的にアナウンスされた場合にはキャッシュサーバの更新を実施する等、最新の DNS ルートサーバの情報を維持する対策を講じること。

オ 対策基準 8.5.1 カにおける「アクセス制御」には、利用者の ID、パスワードによる制御だけでなく、電子証明書による端末認証や接続する機器の IP アドレス、MAC アドレス等の認証情報を利用し端末を制限する機能のほか、CASB 製品・サービスの導入がある。CASB とは、Cloud Access Security Broker の略で、クラウドサービス利用が進む中で、組織内のクラウドサービス利用をコントロールするためのサービスの総称である。

カ 対策基準 8.5.1 キにおける「多要素認証」とは、ID、パスワードといった知識認証だけでなく、所持認証（セキュリティカード等）、生体認証（指紋等）の2つ以上を組み合わせた認証方法をいう。

キ 対策基準 8.5.1 クにおける「ユーティリティプログラム」とは、設定の自動化ツール等、実行が容易ではあるがその影響がシステム全体に影響するようなものを指す。

#### 4.5.2 攻撃の予告等への措置【対策基準 8.5.2】

対策基準 8.5.2 における「必要な措置」としては、ログの確保等の情報収集、被害を受けた場合の復旧手順における庁内関係者の役割等の再確認等がある。

#### 4.5.3 記録の保存【対策基準 8.5.3】

対策基準 8.5.3 における「記録の保存」とは、不正アクセス時の機器及びネットワーク機器のアクセスログ、実施した対応策及び結果の作業記録等を残すことをいう。それらの記録は事実確認、原因追及、予防対策、防止対策に利用するため、適切に保管する。

#### 4.5.4 内部からの攻撃【対策基準 8.5.4】

対策基準 8.5.4 における「攻撃を監視」とは、ファイアウォールのアクセスログの監視、IDS による監視、IPS による防御等のことをいう。

#### 4.5.5 職員等による不正アクセス時の措置【対策基準 8.5.5】

ア 対策基準 8.5.5 における「通知」とは、職員及びその他従事者による不正アクセスを情報基盤管理者及び業務システム管理者が知り得た場合に、当該職員等が所属する局室区等の情報管理者へ連絡することをいう。連絡する内容としては、不正アクセスの被害を受けた日時、システム、発見した方法、不正アクセスの方法、被害の状況、一時的にとった措置等とする。

イ 対策基準 8.5.5 における「適正な処置」とは、当該職員等情報取扱者のアクセスの停止や指導等を行うことをいう。

#### 4.5.6 サービス不能攻撃【対策基準 8.5.6】

対策基準 8.5.6 における「サービス不能攻撃」については、事前にプロトコル毎に帯域を確保するなどの対策がある。ただし、一般的に、根本的な対策が困難であるので、攻撃発生時の対処手順や連絡体制の整備などにより、多層的に備えておく。

#### 4.5.7 標的型攻撃【対策基準 8.5.7】

対策基準 8.5.7 における「標的型攻撃」対策としては、サンドボックスの利用などが考えられるが、効果が限定的なので、心当たりのないメールを安易に開封しないなどの人的対策と併用するのはもちろん、ネットワーク機器のログ監視強化なども行い、多層的に備えておく。

### 4.6 セキュリティ情報の収集【対策基準 8.6】

対策基準 8.6.1 における「セキュリティホールに関する情報」とは、以下の技術的脆弱性情報をいう。これらの情報を収集することにより今後の予防策を検討しなければならない。また、情報を適切に入手するために、情報の入手先、連絡先等を最新の状態に維持・管理しなければならない。

ア 各ベンダーの Web サイト、サポートページ及び IPA の Web サイト等から定期的に収集する情報  
システムに導入されているハードウェア及びソフトウェアに関連する技術的脆弱性情報

イ 脆弱性関連のメーリングリスト、セミナー等から収集する技術的脆弱性情報



また、セキュリティホールへの対策状況の定期的な確認により、セキュリティホールへの対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連するセキュリティホールの情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するセキュリティホールへの措置を講ずる。

クラウドサービス事業者の責任範囲の機器やアプリケーション等については、当該事業者が適切に対応完了したことをサービス利用者が確認できる仕組みがあることが望ましい。

## **5. 情報システムの監視**

### **5.1 事象の検知【対策基準 9.1 ア】**

対策基準 9.1 アにおける「情報システムを常時監視」とは、主にネットワーク機器のログの監視、情報システム及び機器等の稼働状況の監視、IDS による不正アクセス監視等のことをいう。情報基盤管理者及び業務システム管理者は各情報システムの重要度、特性を考慮し、監視対象を決定する。

### **5.2 時刻同期【対策基準 9.1 イ】**

対策基準 9.1 イにおける対策は、本文書の 4.1.6 イの項と同様の対策とする。

### **5.3 常時監視【対策基準 9.1 ウ】**

対策基準 9.1 ウにおける「常時監視」とは、前述 5.1 による監視を常時実施することをいう。インターネット等の外部ネットワークと接続している情報システムは、全て監視対象に含まれる。

### **5.4 クラウドサービスの状況・設定の確認【対策基準 9.1 エ】**

クラウドサービス事業者によっては、設定した閾値以上のリソース利用を検知してアラートを発信する機能を提供しているため、必要に応じてこうした機能を利用することが望ましい。

クラウドサービスの稼働状況やアプリケーションの状況、設定値などが利用者側から確認できるツールや仕組みが用意されていることをクラウドサービス事業者やサービスの選定に合わせ、情報提供を求めて確認しておくこと。

## **6. 業務委託等と外部サービスの利用**

### **6.1 委託事業者等の選定基準【対策基準 10.1.1】**

対策基準 10.1.1 における「委託先等の選定」に当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する。具体的に、事業者の情報セキュリティ水準を評価する方法としては、情報セキュリティマネジメントシステムの国際規格の認証取得状況や情報セキュリティ監査の実施状況等がある。

### **6.2 契約書の記載事項【対策基準 10.1.2】**

#### **6.2.1 委託先等の責任者、委託等の内容、従事者の所属、作業場所の特定に関する事項【対策基準 10.1.2 ア (11)】**

ア 管理区域内に入室する際は、入室者に対して身分証の提示を求め、従事者名簿と突合することや職員の随行、監視カメラ等によって入室者を確認すること。

イ 従事者の変更があった際は、委託事業者等に対し、最新版の名簿の提出を求めるとともに、従事者名簿の提出時に身分証明書の確認や面談により本人確認を行うこと。

ウ 委託事業者等から名簿の提出がない場合であっても定期的（年 1 回程度）に従事者が変更されていないか確認すること。

#### **6.2.2 委託先等の責任者及び従事者に対する研修の実施に関する事項【対策基準 10.1.2 ア (12)】**

委託事業者等において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。なお、委託事業者等が重要な情報資産を取り扱う場合は、委託事業者等の従業員に、本市の情報セキュリティポリシーや各規定を理解させるため、本市が主催する情報セキュリティに関する教育・研修・訓練等に参加させることや、研修を合同で行うことも有効である。

#### **6.2.3 情報のライフサイクル全般での管理義務に関する事項【対策基準 10.1.2 ア (14)】**

ア 対策基準 10.1.2 ア (14)における「情報のライフサイクル全般での管理」とは、対策基準 4.2 ウ「情報の作成」から、ケ「情報資産の廃棄等」記載の内容をいう。

イ 委託事業者等が重要な情報資産を取り扱う場合は、情報セキュリティの原則である「最小限の権限」、「複数人による確認」等を徹底させること。

### **6.3 外部サービスの選定【外部サービス利用基準 3.2 カ】**

外部サービス利用者の責任範囲は、サービスモデルに依存して変化するが、データに対する管理責任は、どのモデルにおいてもサービス利用者である本市にあることに注意すること。

### **6.4 外部サービスにおけるユーティリティプログラムに対するセキュリティ対策【外部サービス利用基準 3.5.5】**

外部サービス利用基準 3.5.5 における「ユーティリティプログラム」とは、設定の自動化ツール等、実行が容易ではあるがその影響がシステム全体に影響するようなものを指す。

### **6.5 外部サービスを利用した情報システムの運用・保守時の対策【外部サービス利用基準 3.6 ① ケ】**

ア 外部サービスの利用開始時には問題なく利用できていた設定が、外部サービスの仕様変更や機能追加をきっかけに、不適切な設定に変わったり、隠れていた設定上の問題が顕在化したりするおそれがあるため、定期的に設定の確認や見直しを行うこと。

イ 外部サービス事業者が発表するリリース情報を把握し、仕様変更や機能追加が発表された（適用された）場合には、その都度、設定の見直しを行うこと。

### **6.6 外部サービスを利用した情報システムの更改・廃棄時の対策【外部サービス利用基準 3.7 ③】**

外部サービス事業者にて実施しているデータ消去方法は、当該事業者の公開情報や当該事業者への問合せで事前に確認すること。