情報システムセキュリティ実施手順書  
（〇〇システム）

【手順書サンプル使用時の注意事項】

1. 実施手順書は、情報セキュリティポリシーをはじめとした一連のルールを、具体の事務ベースで実現していくためのものです。そのシステムを現在使っている人が、ふとしたときに立ち返ったり、新しく着任した人が事務を学ぶ際、最初に参照したりするときなどのために、ルールを具体化・可視化しておけば、セキュリティレベルを維持していくことができます。どんなに小さなシステムでも、手順書を作成する必要がありますので、必ず作成してください。
2. 実施手順書の内容は、「こうあるべき」という決まりはありません。ここにお示しした手順書は、あくまでサンプルです。個人情報など、重要なデータを取扱う場合や、そのシステムが基幹的な機能を担う場合などは、必要に応じて、内容を追加してください。もちろん、より簡素な手順書とすることも可能ですが、最低限、責任体制とインシデント発生時の対応については、定めておく必要があります。
3. 基本的には、このサンプルをベースにしていただければ、最低限必要な項目は盛り込めるようにしています。それでも、初めて作成するときや大規模な改正を行うときをはじめ、分からないことが出てくるときもあると思われます。そのときは、デジタル戦略部ICT総合戦略担当まで、お気軽にご相談ください。
4. とりわけ特定個人情報（マイナンバー）を取り扱う場合には、番号法やガイドラインなどに定められている取扱いに注意が必要です。「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」内にある「（別添）特定個人情報に関する安全管理措置」を、よくご参照ください。  
   （参照「個人情報保護委員会ホームページ」　https://www.ppc.go.jp/legal/policy/）

○○局〇〇課  
  
制定日：令和3年5月6日

改訂履歴

|  |  |  |
| --- | --- | --- |
| 改訂年月日 | 版 | 改訂理由・内容 |
| 令和 年 月 日 | 第1.0版 | 初版作成 |

目次

[1. はじめに 1](#_Toc44928689)

[1.1. 目的 1](#_Toc44928690)

[1.2. 適用範囲 1](#_Toc44928691)

[1.3. 改廃管理 1](#_Toc44928692)

[1.4. 本文書の位置付け 1](#_Toc44928693)

[2. システム概要 1](#_Toc44928694)

[2.1. 対象とするシステムの名称 1](#_Toc44928695)

[2.2. 対象とするシステムの概要及び使用所属 1](#_Toc44928696)

[2.3. 管理体制 1](#_Toc44928697)

[2.3.1. 業務システム責任者（〇〇局長） 1](#_Toc44928698)

[2.3.2. 業務システム副責任者（○○部長） 1](#_Toc44928699)

[2.3.3. 業務システム管理者（〇〇課長） 2](#_Toc44928700)

[2.3.4. 業務システム担当者 2](#_Toc44928701)

[2.3.5. 機器利用担当者（○○課担当者） 2](#_Toc44928702)

[3. 情報資産の分類及びデータの管理 2](#_Toc44928703)

[3.1. 情報資産台帳の作成及び管理 2](#_Toc44928704)

[3.2. 情報資産の分類の実施 3](#_Toc44928705)

[3.3. データ資産の管理 3](#_Toc44928706)

[3.4. ハードウェアの管理 3](#_Toc44928707)

[3.4.1. サーバ等機器の管理 3](#_Toc44928708)

[3.4.2. ネットワークの管理 3](#_Toc44928709)

[3.4.3. 業務端末 4](#_Toc44928710)

[4. 情報システムの運用 5](#_Toc44928711)

[4.1. アクセス制御 5](#_Toc44928712)

[4.1.1. ユーザーの管理 5](#_Toc44928713)

[4.1.2. 特権管理 5](#_Toc44928714)

[4.1.3. 情報システムへのアクセス制限 5](#_Toc44928715)

[4.1.4. 利用者ID及び特権IDの取り扱い 6](#_Toc44928716)

[4.1.5. IDの定期棚卸点検 6](#_Toc44928717)

[4.2. 情報システムの保守運用 6](#_Toc44928718)

[4.2.1. 操作手順書 6](#_Toc44928719)

[4.2.2. 作業の実施 6](#_Toc44928720)

[4.2.3. 作業の記録 6](#_Toc44928721)

[4.2.4. アクセス記録の取得等 7](#_Toc44928722)

[4.2.5. ソフトウェアの保守及び更新 7](#_Toc44928723)

[4.2.6. コンピュータウイルス等不正プログラム対策 7](#_Toc44928724)

[4.2.7. バックアップの実施 7](#_Toc44928725)

[5. 管理区域等の管理 7](#_Toc44928726)

[5.1. 区域の定義 7](#_Toc44928727)

[5.2. 区域の決定 8](#_Toc44928728)

[5.3. 執務区域の管理 8](#_Toc44928729)

[5.4. 準管理区域の管理 8](#_Toc44928730)

[5.4.1. 準管理区域の設備 8](#_Toc44928731)

[5.4.2. 入退管理策 8](#_Toc44928732)

[5.5. 管理区域 8](#_Toc44928733)

[6. 研修・訓練等の実施 8](#_Toc44928734)

[6.1. 研修の実施 9](#_Toc44928735)

[6.2. 緊急時対応訓練の実施 9](#_Toc44928736)

[7. 緊急時の対応 9](#_Toc44928737)

[7.1. 緊急連絡網の整備 9](#_Toc44928738)

[7.2. 情報セキュリティインシデントに対する緊急対応 9](#_Toc44928739)

[8. 自己点検・監査の実施 9](#_Toc44928740)

[8.1. 自己点検の実施 9](#_Toc44928741)

[8.2. 監査の実施 9](#_Toc44928742)

[8.3. 自己点検・監査結果の報告・活用 9](#_Toc44928743)

[9. その他 9](#_Toc44928744)

[9.1. 情報システムセキュリティ実施手順書の見直し 10](#_Toc44928745)

[9.2. 委託事業者への情報セキュリティ対策の実施状況の確認 10](#_Toc44928746)

# はじめに

## 目的

情報システムセキュリティ実施手順書（○○システム）（以下、「本文書」という）は、情報セキュリティポリシーに基づき、当該情報システムの管理者及び利用者が日常的に守るべき主な基準や手順等を定めることにより、情報セキュリティを確保することを目的とする。

## 適用範囲

本文書は、神戸市○○局○○部○○課が所管する以下の情報システム及びその利用に関わる職員等すべてを対象とする。

○○システム

## 改廃管理

本文書の承認者は、業務システム管理者である。

## 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
* その他、情報セキュリティに係る基準や通知文等

# システム概要

## 対象とするシステムの名称

○○システム

## 対象とするシステムの概要及び使用所属

#### システムの概要

本システムは、○○事務を実施するために、○○の情報をデータベース化し、事務処理を支援するシステムである。

なお、本システムにおいては、個人情報を取扱う。

#### 使用所属

○○局○○部○○課

## 管理体制

### 業務システム責任者（〇〇局長）

1. 情報セキュリティの最高責任者として業務システム責任者をおき、○○局長がその任にあたる。
2. 業務システム責任者は、情報セキュリティ対策に関する統括的な権限及び責任を有し、業務システム管理者を適宜監督するとともに、必要な指示を出す。

### 業務システム副責任者（○○部長）

1. 情報セキュリティに関する副責任者として業務システム副責任者をおき、〇〇部長がその任にあたる。
2. 業務システム副責任者は、業務システム責任者を補佐し、業務システム責任者が不在のときは、その職務を代行する。

### 業務システム管理者（〇〇課長）

1. システム環境及びネットワーク環境を適切に管理し、当該システムを適切に運用する役割を担う者として業務システム管理者をおき、○○局○○部○○課長がその任にあたる。
2. 業務システム管理者は、○○システムの開発、設定、運用及びこれらの見直しなど、当該システムの情報セキュリティ対策全般に関する権限及び責任を有する。
3. 業務システム管理者は、本文書の維持及び管理を行う。
4. 業務システム管理者は、○○システムの事務処理全般について管理、調整を行う。
5. 業務システム管理者は、○○システムにおいて情報セキュリティインシデントが発生した場合又は発生のおそれがある場合には、情報管理者、業務システム責任者、情報セキュリティ管理者へ速やかに報告を行い、指示を仰ぐ。

### 業務システム担当者

1. ○○システムの開発、設定の変更、運用等についての作業を行う者を業務システム担当者とする。
2. 業務システム担当者は、○○局○○部○○課○○係の職員から業務システム管理者が指名した者をもってあてる。
3. 業務システム担当者は、業務システム管理者の指示等に従う。

### 機器利用担当者（○○課担当者）

1. ○○システムの業務端末を使用する者を機器利用担当者とする。
2. 機器利用担当者は、業務システム管理者や業務システム担当者の指示等に従って、○○システムを利用する。
3. 機器利用担当者は、業務目的以外に○○システムを使用しない。
4. 機器利用担当者は、業務システム管理者の許可を得た場合を除き、所属外へ情報資産を持ち出さない。
5. 機器利用担当者は、定められた執務区域外において、情報処理作業を行わない。ただし、業務システム管理者が許可する場合（在宅勤務等）を除く。許可された執務区域外作業をする際には、執務区域外における情報処理作業についての情報セキュリティポリシーの規定を遵守すること。

※マイナンバー利用事務系の業務に対して、執務区域外における情報処理作業を許可してはならない。

1. 機器利用担当者は、異動、退職時には、利用していた○○システムに係るすべての情報資産を返却する。
2. 機器利用担当者は、本文書に対する違反行為を発見したとき、○○システムの欠陥の発生等が起きたときは、直ちに業務システム管理者に報告する。

# 情報資産の分類及びデータの管理

## 情報資産台帳の作成及び管理

業務システム管理者は、○○システムに関する主要な情報資産※を管理するため、情報資産台帳を作成する。情報資産台帳は、年1回又は必要に応じて見直しを行う。

※情報資産の対象は以下のとおり。

* ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
* ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
* 情報システムの仕様書及びネットワーク図等のシステム関連文書
* ただし、全庁的に管理している情報資産（例：事務処理用ＰＣ、庁内ネットワーク）や、課等で管理している情報資産（例：ＵＳＢメモリ、サーバ室）は除く

## 情報資産の分類の実施

業務システム管理者は、前項で識別した主要な情報資産に対して、機密性、完全性、可用性の重要性分類を行う。情報資産の分類は、年1回又は必要に応じて見直しを行う。

## データ資産の管理

1. データの収集は、法令上の根拠があり、かつ、業務上、必要な範囲に限って行う。
2. データの保管は、権限ある者だけがアクセスできるように行う。個人情報が記載されたデータ資産は、保管庫や什器等に施錠して保管する。
3. データの廃棄は、保管の必要がなくなり次第、速やかに行う。特に個人情報が記載されたデータ資産は、容易に復元できない手段により廃棄処理を行うとともに、削除・廃棄記録も残し、５年間保管する。

## ハードウェアの管理

### サーバ等機器の管理

○○システムで使用するサーバ、サーバに内蔵された磁気ディスク及びそれに付随する機器については、以下のとおり管理する。

1. 市役所○号館○階△△課サーバルームのラック内に設置する。それ以外の機器は安全性を考慮した上で、△△課内に設置する。
2. 機器の利用状況を定期的に確認し、機器の適正な設置を図るとともに、計画的に機器を更新する。
3. 機器を廃棄、リース返却等する場合、機器内部の記憶装置について、復元不可能な状態にする措置（抹消措置）を実施しなければならない。。

* 復元不可能な状態にする措置は、次のいずれかによる。（ただし、マイナンバー利用事務系のシステムで住民情報を保存する記憶媒体は、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を行うこととする。）
* 物理的な破壊または磁気的な破壊を実施すること
* 公的機関が推奨する消去方式の専用ソフトによるデータ消去を行うこと（賃貸借契約の契約条件により機器の返却が必要な場合等）
* 当該措置を外部の業者に委託する場合は、委託事業者との間で守秘義務契約を締結する他、秘密保持体制及び消去証明書の確認等を行う。原則として職員が立ち会い、確実な履行を確認する。職員の立ち会いができない場合は、抹消措置の手順等を記したドキュメントとあわせて破壊済であることを示す写真又は消去ソフトが実行済であることを示すレポートやログデータ等の提出を、提出期限を定めて求めることで、抹消措置の確実な履行を確認する。

1. サーバ等機器に、年1回の定期保守を実施する。（※④は、可用性２以上の情報を取り扱っているシステムのみ記載すること）

### ネットワークの管理

○○システムで使用するネットワークについては、以下のとおり管理する。

1. 無断でネットワークに機器を接続できないよう、ネットワークに接続している機器のネットワークアドレスを管理する。
2. 情報システムと外部ネットワークの接続箇所に、ファイアウォールを設置し、不正アクセスを遮断する。
3. ネットワークへ新たに機器を接続する場合には、必要性やセキュリティの状況について確認する。
4. 外部にデータを送信する場合は、通信経路の暗号化等、情報漏えいや改ざんを防止するための措置を講じる。

### 業務端末

#### 業務端末の管理

業務システム管理者は、機器利用担当者が使用する業務端末については、以下のとおり管理する。

1. 業務端末の利用者は、機器利用担当者に限定する。また、あらかじめ機器に制限をし、認められた機器以外の業務端末が接続できないようにする。
2. 業務端末の取扱いに関する手順書を作成する。
3. 業務端末には、あらかじめ定めたソフトウェアのみインストールし、その他のソフトウェアを無断で導入してはならない。
4. 業務端末の起動（以下、「ログオン」という。）、業務端末の終了（以下、「ログオフ」という。）の実績を記録し、必要に応じて状況を確認する。
5. 業務端末に障害が発生した場合には、速やかに機器利用担当者へ通知する。
6. 業務端末に個人情報を保存して使用するときは、ワイヤーロックなど、業務端末の盗難防止対策を講じる。

#### 業務端末の取り扱い

業務端末については、以下のとおり取扱う。

1. 機器利用担当者が○○システムの業務端末を利用するときは、所定の研修を受講した上で利用することとする。
2. ○○システムの稼動時間は、平日（開庁日）の8時30分～17時45分とする。ただし、業務の都合上必要があり、業務システム管理者の承認を得たときは、稼働時間を延長できる。
3. 業務上必要でない操作は行わない。
4. プリンタへの出力は必要最小限とし、出力した帳票類は情報漏えい防止のため、プリンタや机上に放置されたままにならないよう適切に管理する。また、定期的にプリンタに帳票類が放置されていないかのチェックを行い、放置された帳票類等は廃棄する。
5. 長時間席を離れる場合には、業務端末の画面に個人情報等を表示したままにしない。
6. 業務端末の画面が窓口に来庁している住民から見えないようにするなど、情報漏えい等を防止するために、業務端末及び付属機器を適切な場所に設置する。

#### 業務端末の設定

業務システム管理者は、業務端末については、以下のとおり設定を行う。

1. ＯＳ及び標準ソフトウェアのほか、業務に必要なソフトウェアのみを導入する。
2. コンピュータウイルス対策ソフトウェアを導入し、1日に1回、当該ソフトウェア及びウイルス定義ファイルの更新を行う。
3. 業務システム管理者の許可なく、業務端末に対するハードディスク等の増設又は改造、環境の設定変更等を行わない。
4. 機器利用担当者がログオンするためのユーザーＩＤ、パスワードを設定する。また、当該ユーザーに応じたアクセス権限を設定する。
5. 時刻の同期等を行い、正確な時刻を設定する。
6. 許可されていない他のネットワーク（インターネット等）に接続しない。

#### 電磁的記録媒体の管理

電磁的記録媒体は、業務に必要な最小限の数を保有し、使用状況については、使用者や業務システム管理者の許可の有無、使用目的、使用後のデータ削除などを台帳に記録して管理する。この管理台帳は、５年間保管する。

# 情報システムの運用

## アクセス制御

### ユーザーの管理

業務システム管理者は、ユーザーＩＤ及びパスワードについては、以下のとおり管理する。

1. 不要なユーザーＩＤは設定しない。異動・退職等でユーザーＩＤが不要になった場合には速やかに削除する。
2. パスワードは、関係職員以外に知られないように管理する。
3. パスワードを発行する場合は、強制的に発行する。
4. パスワードは8桁以上とし、数字、英字（大文字・小文字区別有）及び記号を含む文字列となるよう制限する。
5. 機器利用担当者のアクセス権は、年1回以上見直しを行う。
6. 機器利用担当者の利用するパスワードの漏えいを確認した者は、直ちに業務システム管理者へ報告する。報告を受けた業務システム管理者は、パスワードを変更する。

### 特権管理

業務システム管理者は、特権ＩＤについては、以下の管理を行う。

1. 特権をもつユーザーＩＤと、一般のユーザーＩＤとは別に設定する。
2. 特権ＩＤの利用は、必要最小限の人員に対してのみ承認する。
3. 特権ＩＤについては、パスワードは8桁以上とし、数字、英字（大文字・小文字区別有）及び記号を含む文字列となるよう制限する。また、少なくとも６か月に１度、あるいは特権ＩＤを利用する職員等が異動した都度で、パスワードを変更し、その際は古いパスワードを再利用しない。
4. 委託業務従事者等の特権ＩＤの利用について、業務システム管理者から認可しているか、またこのＩＤの利用者の担当業務が変更になっていないか等を毎月確認する。

### 情報システムへのアクセス制限

業務システム管理者は、○○システムへのアクセスを必要最小限の範囲に制限するために、以下の事項を実施する。

1. ○○システムのログイン手順が記載された文書等は、関係職員以外が閲覧できないようにする。
2. 機器利用担当者のアクセス権限（閲覧、追加、削除、更新、印刷、プログラムの実行等）を職務等に応じて制御する。
3. ○○システムからは、許可を得た者等、権限ある者以外がデータを取り出せないようにする。

### 利用者ID及び特権IDの取り扱い

業務システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職等に伴う利用者ＩＤおよび特権ＩＤの取扱いを適切に行わなければならない。

①　業務システム管理者は、職務分掌を考慮した適切な責任と権限に合わせてアクセス権限を設定する。

②　利用者ＩＤおよび特権ＩＤの発行およびアクセス権の付与、変更、削除は、「〇〇システム　ＩＤ申請書」で申請を行い、適切な責任者によって承認を行い、その記録を残す。

③　複数の利用者でＩＤを共有せざるを得ない場合、その理由と利用者を明確にし、業務システム管理者の承認を得て、補完的統制を整備した上で共有のＩＤを設定できることとする。

### IDの定期棚卸点検

業務システム管理者は、利用されていないＩＤが放置されないよう、また、ＩＤに必要以上のアクセス権限が付与されないようにするために、以下の事項を実施する。

1. 〇〇システムのユーザーＩＤおよび特権ＩＤのＩＤ管理簿を作成し、職員等の異動、出向、退職等に伴い、都度更新する。

②　年１回、〇〇システムから出力したＩＤ一覧（帳票や画面）と、上記①のＩＤ管理簿を照合し、利用されていないＩＤが放置されていないか、ＩＤに必要以上のアクセス権限が付与されていないか等のチェックを行う。

③　業務システム管理者は、上記②の照合結果を確認し、その記録を残す。照合の結果、検出した不要なＩＤやアクセス権限等については上記4.1.4に準じ、ＩＤの改廃を行う。

## 情報システムの保守運用

### 操作手順書

業務システム管理者は、○○システムの運用に関して、以下の手順書を作成し、年に1回見直しを行い、最新の状態に維持する。

1. データの処理及び運用に関する手順
2. ○○システムの構成変更等、各種作業に関する計画及び手続き
3. ○○システムの障害発生時の対応手順又は復旧手順

### 作業の実施

業務システム管理者は、○○システムに係る作業を行う場合、以下のとおり管理を行う。

1. 作業指示者と作業実施者を可能な限り分離する。
2. 実施した作業内容は、「作業管理記録」等へ記録する。
3. 委託事業者が庁内で作業を行う場合は、作業前に身分証明書の提示を求め、契約で定められた資格を有する者が作業に従事しているかを確認する。
4. 委託事業者が庁内のシステム変更作業を実施する場合、業務システム担当者が立会いを行い、作業の実施状況を監督する。
5. 委託事業者が重要な変更等の作業を行う場合は、設定ミス等のリスクを減らすため、複数名（最低2名）で作業を行い、互いにその作業を確認しなければならない。

### 作業の記録

1. 業務システム担当者は、○○システムにおいて行った運用及び変更等の作業はすべて「作業管理記録」に記録し、上長（課長または係長）の承認を得る。作成した作業記録は、窃取、改ざん等をされないように施錠可能な保管庫等に当該年度終了後1年間（変更作業記録の場合は、3年間）保管する。
2. 業務システム管理者は、○○システムの運用に係る事項を検討した際の議事録等を当該年度終了後5年間保管する。

### アクセス記録の取得等

1. 業務システム管理者は、機器利用担当者によるアクセスの記録、端末操作ログ、システム動作ログ、障害時のエラーログ等の記録を取得し、窃取、改ざん、誤消去等を防止する措置を講じた上で、当該年度終了後１年間保管する。
2. 業務システム管理者は、システムから自動出力したアクセス記録等について、定められた保管期間中、破損の影響が少ない外部記録媒体にバックアップし適正に管理する。
3. アクセス記録や動作ログなどについては、１ヶ月に１回、監視・分析を行う。

### ソフトウェアの保守及び更新

業務システム管理者は、○○システムに係るソフトウェア等を更新、又は修正プログラムを適用する場合、不具合及びシステムとの相性の確認を行い、計画的に更新又は導入する。また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムを適用する必要がある場合には、速やかに対応を行う。

### コンピュータウイルス等不正プログラム対策

業務システム管理者は、○○システムで使用するネットワーク機器及びシステム機器に対して、以下の不正プログラム対策を行う。

1. コンピュータウイルス等対策ソフトウェアを常駐させる。
2. ○○システムにおいてUSBメモリ等の電磁的記録媒体を使用する場合（電磁的記録媒体からデータ又はソフトウェアを取り入れる場合、あるいは電磁的記録媒体へデータ又はソフトウェアを書き込む場合）、当該媒体の使用にあたり、ウイルスチェックを行う。
3. コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ必要があるため、1日に1回、当該ソフトウェア及び定義ファイルの更新を行う。
4. 使用されていないポート番号のポートを閉鎖する。
5. ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用する。
6. 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。
7. 本システム関連のファイルにはアクセスできないよう管理する。

### バックアップの実施

業務システム管理者は、日次で、〇〇システムの情報資産のバックアップを実施する。バックアップの処理が正常終了していることを定期的に確認し、バックアップファイルを１年以上保存する。

なお、バックアップファイルからのデータ復元テストを年１回以上行うこと。

# 管理区域等の管理

## 区域の定義

○○システムにおける管理区域等について、以下のとおり定義する。

1. 執務区域  
   機器利用担当者等が通常執務を行う区域であり、○○区役所○階の○○課執務スペースを指す。
2. 準管理区域  
   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ている区域であり、市役所○号館○階のサーバルームを指す。
3. 管理区域  
   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ている区域であり、市役所○号館○階の○○を指す。

## 区域の決定

○○システムに係る管理区域等は、別図のとおりとする。

## 執務区域の管理

業務システム管理者は、執務区域を以下のとおり管理する。

1. 執務区域への来庁者等部外者の入室は必要最小限度とし、入室に際しては、職員等が目的等を確認のうえ入室を許可する。また、執務区域へ入室した来庁者等部外者が、業務終了後確実に退室したことも職員等が確認する。
2. 執務区域に職員等が不在の時には、施錠等により来庁者等部外者が入室できないようにする。施設の構造上、執務区域を施錠できない場合は、職員等が不在となる際、所管業務に係る来庁者等部外者がいないことを確認する。
3. 執務区域に来庁者等部外者が許可なしで入室できないことが分かるよう、立入禁止の掲示等の措置を講じる。

## 準管理区域の管理

### 準管理区域の設備

業務システム管理者は、準管理区域の設備について、以下のとおり管理する。

1. 燃えやすい材料や文書等は、原則として準管理区域内には保管しない。
2. 準管理区域へのアクセスは必要最小限とし、施錠等を行う。
3. 消火薬剤を準管理区域の近くに設置する。
4. 準管理区域が無人になった場合は、施錠等により、不正アクセスを防止する。

### 入退管理策

1. 準管理区域に設置しているラックの開閉は、許可された者のみに限定し、ラックの鍵は、○○係長が管理する。貸出が必要な場合は、業務システム管理者の承認を受けたうえで「サーバラック鍵貸出簿」に記載する。
2. 「サーバラック鍵貸出簿」は、施錠のできる保管庫等に当該年度終了後１年間保管する。

## 管理区域

管理区域である市役所1号館10階の機械室の利用に際しては、入退室時の記録簿への記入や、名札・入室許可証の着用等、デジタル戦略部が定めた管理ルールに従う。

# 研修・訓練等の実施

## 研修の実施

1. 業務システム管理者は、機器利用担当者に対して、○○システムの利用及び情報セキュリティ対策等に係る研修を、年１回実施する。ただし、既に利用研修を受けている場合や、特段の変更がない場合、情報セキュリティに関する問題が発生していない場合については、適宜、研修を省略したり、他の方法で替えたりすることができる。
2. 業務システム管理者は、新たな業務の追加及びシステムの変更があった場合は、随時、必要な研修を機器利用担当者に対して実施する。

## 緊急時対応訓練の実施

業務システム管理者は、機器利用担当者を対象として、システム障害時の対応等に係る訓練を年1回実施する。

# 緊急時の対応

## 緊急連絡網の整備

業務システム管理者は、○○システムに関わる情報セキュリティインシデントが発生したとき、非常災害時等の復旧に向けた安否確認が必要なときなどに、関係者間で迅速かつ正確な情報共有が行えるよう、あらかじめ「緊急連絡網」を作成する。

## 情報セキュリティインシデントに対する緊急対応

○○システムにおける情報セキュリティインシデントに対する緊急対応手順は、以下のとおりとする。

1. 情報セキュリティインシデントの発生を把握した職員等は、情報管理者に状況を報告する。
2. 報告を受けた情報管理者は、業務システム管理者と連携して情報セキュリティインシデントに係る状況を調査し、影響の拡大防止や被害の回復を図るなど、暫定対応をとる。
3. 情報管理者は、②の対応をとりながら、業務システム責任者や情報セキュリティ管理者に報告するとともに、関係機関にも連絡を行う。
4. ②の対応の結果が永続的な対応と見込まれる場合は、それを恒久対応とする。しかし、同様の原因で再発するおそれが見込まれる場合は再発防止策を策定し、速やかに実施する。
5. 業務システム管理者は、情報セキュリティインシデントの内容、実施した再発防止策等の内容を「障害対応報告」に記録し、5年間保管する。

# 自己点検・監査の実施

## 自己点検の実施

1. 業務システム管理者は、本文書に基づく運用に関する自己点検を定期的に行い、必要な改善を行う。
2. 自己点検は、年1回又は必要に応じて行う。

## 監査の実施

業務システム管理者は本文書に基づく適切な運用を確保するため、必要な監査を受ける。

## 自己点検・監査結果の報告・活用

自己点検や監査を行ったときは、業務システム管理者は、結果に基づく改善策をまとめ、適宜、業務システム責任者に報告する。

# その他

## 情報システムセキュリティ実施手順書の見直し

業務システム管理者は、年1回、又は以下の場合においては適宜、本文書を見直す。

1. 自己点検や監査の結果、本文書の見直しが必要となった場合
2. 情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合
3. システムに変更が生じた場合
4. その他、業務システム責任者が必要と判断した場合

## 委託事業者への情報セキュリティ対策の実施状況の確認

業務システム管理者は、委託契約締結後においても、当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について、年1回もしくは随時、確認を行う。