枚方市情報セキュリティポリシー

[　平成 15 年　9 月　1 日　施行　]
[　平成 20 年 10 月　1 日　改訂　]
[　平成 22 年　7 月 16 日　改訂　]
[　平成 24 年　4 月　1 日　改訂　]
[　平成 25 年　9 月　1 日　改訂　]
[　平成 27 年　2 月　1 日　改訂　]
[　平成 27 年 5 月 11 日　改訂　]
[　平成 27 年 12 月 25 日　改訂　]
[　平成 29 年　1 月 11 日　改訂　]
[　平成 29 年　9 月 13 日　改訂　]
[　平成 30 年　7 月　2 日　改訂　]
[　平成 31 年　1 月 24 日　改訂　]
[　令和　2 年　4 月　1 日　改訂　]
[　令和　3 年　3 月　31 日　改訂　]
[　令和　4 年　4 月　1 日　改訂　]
[　令和　5 年　4 月　1 日　改訂　]
[　令和　5 年　9 月　4 日　改訂　]

目　　次

情報セキュリティ基本方針

情報セキュリティ対策基準

情報セキュリティ基本方針

1　目的

本市では、保有する情報資産の保護や、情報システムの安全性を常に確保するための情報セキュリティ対策を実施するとともに、更なる市民サービスの向上や行政事務の効率化・高度化を図るための情報化施策に取り組んでいるところである。

近年の情報システムの高度化やスマート自治体の進展の反面、個人情報の漏えいや、システム障害による業務停止をはじめとした、情報セキュリティを侵害する様々な問題も発生し続けている。また、不正アクセスや、コンピュータウイルス等の脅威は多様化、高度化しており、これらに対する情報セキュリティ対策も一層の強化、拡充が求められる。

ついては、情報資産の保護や、情報システムの安全性、信頼性の確保のため、情報セキュリティ対策の基本的な事項を定めるものである。

2　情報セキュリティポリシーの構成と位置づけ

情報セキュリティポリシーは、市が保有する情報資産の情報セキュリティ対策について総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティに対する取組姿勢を示す「情報セキュリティ基本方針」と、この情報セキュリティ基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示す「情報セキュリティ対策基準」をもって構成する。

3　用語の定義

情報セキュリティポリシーにおける用語の定義は、次に定めるところによる。

（1）　情報セキュリティ
　情報資産の機密性、完全性及び可用性を維持することをいう。

（2）　機密性
　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（3）　完全性
　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（4）　可用性
　情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（5）　行政情報
　電磁的に記録された行政事務の執行に関わる情報をいう。

（6）　ネットワーク
　コンピュータ等を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）をいう。

（7）　サーバ等
　ネットワーク上で行政情報を処理し、端末機に提供するコンピュータ（ホストコンピュータを含む。）をいう。

（8）　端末機
　ネットワークを通じてサーバに接続されたパソコンをいう。

（9）　情報システム
　行政情報を処理するためのハードウエア及びソフトウエアをいう。

（10）　記録媒体
　情報システムでデータ等を記録するための媒体（メディア）をいう。
　ハードディスク、フロッピーディスク、USBメモリ等。

（11）　スマートデバイス
　情報処理端末（デバイス）のうち、スマートフォンやタブレット型端末など携行可能な多機能端末をいう。

（12） 情報資産
情報システム及びネットワーク並びにこれらで取扱われる行政情報（これらを印刷した文書も含む。）
（13） 無線 LAN
電波等を利用してデータの送受信を行う構内通信網システム
（14） 広域無線通信
電波等を利用してデータの送受信を行う、事業者が提供する広域向けの通信網システム
（15） ASP／クラウド
庁外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念。
（16） データセンター
耐震性に優れた建物にシステムを収容して高速な通信回線を引き込み、空調設備や入退室管理、カメラによる監視等のセキュリティ対策を施した施設
（17） 情報セキュリティインシデント
望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。
（18） ソーシャルメディアサービス
インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語。
（19） 標的型攻撃
明確な意思と目的を持ち、特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。
（20） テレワーク
自宅等の勤務庁舎外において勤務すること。
（21）Web（ウェブ）会議サービス
「Web（ウェブ）会議サービス」とは、専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

（22）外部サービス
「外部サービス」とは、事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

（23）「外部サービス提供者」
「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

（24）「外部サービス利用者」
「外部サービス利用者」とは、外部サービスを利用する自組織の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう

4 情報資産への脅威

情報資産に対して想定される脅威は、その発生度合や発生した場合の影響を考慮するものとし、次のとおりとする。

（1） 部外者による意図的な不正アクセス、又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等
（2） 職員等及び外部委託業者による非意図的な操作、又は意図的な不正アクセス又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏えい等
（3） 地震、落雷、火災、水害等の災害並びに事故、故障等による業務の停止

5 情報セキュリティ対策

情報資産を脅威から保護するため、次に定める情報セキュリティ対策を講ずるものとする。

（1） 管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

（2） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、行政系ネットワークの情報システム全体に対し、次の三段階の対策を講じる。

①個人番号利用事務等を取り扱うネットワークにおいては、原則として、他の領域との通信をできないようにした上で、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等により、住民情報の流出を防ぐ。

②人事給与、財務会計及び文書管理等の内部事務を取り扱うネットワークにおいては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネットに接続されたネットワークにおいては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（3） 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。

（4） 人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、全ての職員等に情報セキュリティポリシーを周知徹底するための教育を実施する等、必要な対策を講ずる。

（5） 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策ソフト導入等の技術面における対策を講ずる。

（6） 運用

① 情報システムの監視、情報セキュリティポリシーの遵守状況の確認等、情報セキュリティポリシーの運用面の対策を講ずる。

② 情報セキュリティが侵害される事態が発生した場合に被害の拡大防止、復旧等を迅速かつ的確に実施するため、緊急時対応計画を整備する。また、侵害に備えた対応訓練の定期的な実施等の対策を講ずるよう努める。

（7） 外部委託

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

６ 情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、市の情報資産を有する全ての行政機関とする。

７ 情報セキュリティ委員会

情報セキュリティポリシーの遵守を促進するとともに、情報セキュリティに関する事項について調査検討を行うため、枚方市情報セキュリティ委員会（以下、「委員会」という。）を設置する。

委員会の構成及び運営に関し必要な事項は、別にこれを定める。

８ 職員等の責務

（1） 正職員、再任用職員、任期付職員、非常勤職員、会計年度任用職員、臨時職員（以下、「職員等」という。）は、情報資産の利用にあたっては、関連法令を遵守しなければならない。

（2） 職員等は、情報セキュリティの重要性を認識し、情報セキュリティポリシーを遵守しなければならない。

９ 監査及び自己点検

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査を受ける。また、定期的に自己点検を実施する。

１０ 情報セキュリティポリシーの評価・見直し

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び、情報セキュリティ対策の評価を実施するとともに、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じて情報セキュリティポリシーの見直しを実施する。

情報セキュリティ対策基準

1　趣旨

（1）趣旨

情報セキュリティ対策基準は、情報セキュリティ基本方針に沿って個々の対策を具体化したものであり、情報セキュリティ対策の基準とする。

（2）適用範囲

本対策基準の適用範囲は、市の情報資産を有する全ての行政機関とする。

（3）情報資産の分類と管理

① 情報資産が漏洩、利用不能、改ざん等のセキュリティ侵害を受けた際の影響の深刻度に応じ、下表のとおり重要性の分類を定める。

	重要性分類
Ⅰ	侵害により、重大な被害が想定される情報資産 （個人情報やその他法令で制限される情報、直ちに他のセキュリティ侵害につながる情報等）
Ⅱ	侵害により、行政に対する信頼を著しく害するおそれや行政事務の執行等に重大な影響を及ぼすと想定される情報資産
Ⅲ	侵害により、行政事務の執行等に軽微な影響を及ぼす情報資産
Ⅳ	上記Ⅰ、Ⅱ、Ⅲ以外

② 業務で取扱う情報資産は、作成、入手、利用、保管、廃棄等の各局面で、①の重要性分類を踏まえた管理体制、手順としなければならない。

2　管理体制

情報セキュリティの管理体制は、次に掲げるとおりとする。

（1） 最高情報統括責任者

市長を最高情報統括責任者とする。

最高情報統括責任者は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する統括を行うとともに、最高の権限及び責任を有する。

（2） 情報統括責任者

副市長、教育長、上下水道事業管理者、病院事業管理者を情報統括責任者とする。

情報統括責任者は、最高情報統括責任者を補佐するとともに、所管部署に係る情報システム等の情報資産の管理及び情報セキュリティ対策に関する統括を行う。

最高情報統括責任者が不在の場合は、自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

（3） 情報セキュリティ責任者（CISO）

（CISO ： Chief Information Security Officer、以下「CISO」という）

総合政策部長を情報セキュリティ責任者（CISO）とする。

情報セキュリティ責任者（CISO）は、本市の全ての情報資産、ネットワークにおける開発、設定の変更、運用、見直し及び情報セキュリティ対策の実施に関する権限及び責任を有する。

情報セキュリティ責任者（CISO）は、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、必要かつ十分な措置を行う権限及び責任を有する。

情報セキュリティ責任者（CISO）は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要かつ十分な措置を行う権限及び責任を有する。

（4） 情報セキュリティ管理者

各部長、会計管理者、上下水道局部長、市民病院事務局長、教育委員会部長、市議会事務局長、監査委員事務局長、選挙管理委員会事務局長、農業委員会事務局長を情報セキュリティ管理者とする。

情報セキュリティ管理者は所管する部局の情報資産において、統括的な管理及び情報セキュリティ対策に関する権限及び責任を有する。

（5） 副情報セキュリティ責任者（副 CISO）

総合政策部次長を副情報セキュリティ責任者とする。副情報セキュリティ責任者は、情報セキュリティ責任者を補佐すると共に、情報セキュリティに係る研修・訓練を行う。

（6） システム統括管理者

DX推進課長をシステム統括管理者とする。

システム統括管理者は、本市の全ての情報資産、ネットワークにおける開発、設定の変更、運用、見直し、及び情報セキュリティ対策を推進し、システム管理者、データ管理責任者に対し、指導、助言を行う権限及び責任を有する。また、外部サービスの許可権限者とする。

（7） システム管理者

システム所管課の長をシステム管理者とする。

システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し及び情報セキュリティ対策を行う権限及び責任を有する。

システム管理者は、所管する情報システムにおける情報セキュリティ実施手順を策定し、その運用及び所属職員等に対する周知、指導を行う。

（8） データ管理責任者

各所属課の長をデータ管理責任者とする。

データ管理責任者は、所管する事務における情報セキュリティ対策を行う権限及び責任を有し、所属する職員等の情報セキュリティ対策の実施について管理、指導を行う。

（9） 情報システム担当者

情報システムを所管する課における、情報システムの管理、運用に携わる担当者を情報システム担当者とする。

（10） CSIRT の設置・役割

① サイバー攻撃等の情報セキュリティインシデント発生時に、迅速かつ的確に対応するための体制として、CSIRT を設置する。

② システム統括管理者を CSIRT 責任者とし、CSIRT の役割を担う職員等の選任、業務統括等を行う。

③ 個人情報漏洩に係る危機管理基本マニュアルにより設置されたセキュリティ事案連絡・相談窓口を CSIRT における情報セキュリティの統一的な窓口として、個人情報の漏洩やサイバー攻撃等による情報セキュリティの侵害、もしくはそれらのおそれが発生した際の報告を受ける体制として位置付ける。

④ CSIRT は、セキュリティ事案連絡・相談窓口を通じて報告を受けた事象について、正確に把握・分析し、被害拡大防止・復旧・再発防止等を行う。

⑤ 情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。
⑥ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
⑦ 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行わなければならない。
⑧ 職員等に対して情報セキュリティインシデントの予防や啓発のための活動等を行う。

3 情報システム全体の強靭性の向上

※ 本対策基準については、原則として、地方公共団体に共通の内容となることから、ネットワーク系統の名称に関して、総務省の地方公共団体における情報セキュリティポリシーに関するガイドラインの表記をそのまま引用している。

枚方市の行政系事務で利用しているネットワーク系統との対応は下表のとおり(4 物理的セキュリティ対策 以降については、枚方市表記に基づく)。

総務省ガイドライン表記	枚方市表記
マイナンバー利用事務系	住基系
LGWAN 接続系	内部系
インターネット接続系	インターネット系

(1) マイナンバー利用事務系

① マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)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わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする

② 情報のアクセス及び持ち出しにおける対策

(ア)情報のアクセス対策

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、二つ以上を併用する認証(多要素認証)を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

(イ)情報の持ち出し不可設定

原則として、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ができないように設定しなければならない。

(2) LGWAN 接続系

① LGWAN 接続系とインターネット接続系の分割

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。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ア)インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(イ)インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ウ)危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3) インターネット接続系

① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びLGWANへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

② 都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

4 物理的セキュリティ対策

4．1 サーバ等の管理

(1) 機器の取り付け

① サーバ等の機器の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

② サーバ等の機器については、ラベル等の貼り付けにより、用途、種類等が明確に認識できるような措置を講じなければならない。

(2) サーバ等の冗長化

① 重要情報を格納しているサーバ等は冗長化し、ミラーリング等により同一データを保持する等の措置を講じなければならない。

② メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動する等、システムの運用停止時間を最小限にしなければならない。

(3) 機器の電源

① サーバ等の機器の電源については、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に、十分な電力を供給する容量の予備電源を備え付けなければならない。

② 落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

① 通信ケーブル及び電源ケーブルについては、損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② ネットワーク接続口（ハブのポート等）については、他者が容易に接続できない場所に設置する等適正に管理しなければならない。

(5) 機器の定期保守及び修理

① 情報システムの安定性を保つため、サーバ等については、機器の定期保守を実施する等の措置を講じるよう努めなければならない。

② 記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合は、修理を委託する事業者との間で、守秘義務契約を締結する等、秘密保持体制の確認等を行わなければならない。

(6) 機器の廃棄等

機器の廃棄等の場合は、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

４．２ 管理区域（サーバ室等）の管理

（1） 管理区域の構造等

① 管理区域とは、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、当該機器等の管理及び運用を行うための部屋（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

② サーバ室から外部に通ずるドアは必要最小限にし、施錠設備等によって許可されていない立ち入りを防止しなければならない。
また、施錠設備に関連する鍵、ICカード等は適正に管理しなければならない。

③ サーバ室内に設置する機器等については、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

④ サーバ室内に設置する消火薬剤その他の消防用設備等については、室内の機器及び記録媒体等に影響を与えないものを設置しなければならない。

⑤ サーバ室内には温度及び湿度を適正に保つための空気調節設備を設置しなければならない。

（2） 管理区域の入退室管理等

① 管理区域への入退室は許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿への記載による入退室管理を行わなければならない。

② 職員等及び外部委託事業者等、管理区域への入室を行う者は、身分証明書等を携帯し、求めにより提示しなければならない。また、管理区域では、名札その他の身分証明書等を着用しなければならない。

③ システム管理者は、管理区域への入室について、当該情報システムに関連しない端末機、スマートデバイス、記録媒体等を持ち込ませないようにしなければならない。

④ システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

（3） 機器等の搬入出

① システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は当該システムの開発・運用・保守等を委託業者に確認を行わせなければならない。

② システム管理者は、管理区域への機器等の搬入出について、職員等を立ち会わせなければならない。

４．３ 通信回線及び通信回線装置の管理

（1） システム統括管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

（2） システム統括管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

（3） システム統括管理者及びシステム管理者は、情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、重要性分類Ⅲ以上の情報について、盗聴等の脅威が想定される回線を利用する場合は、送受信される情報の暗号化を行わなければならない。

（4） システム統括管理者及びシステム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分な対策を実施しなければならない。

（5）　システム統括管理者及びシステム管理者は、情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

４．４ 外部記録媒体の管理

（1）　USB メモリ等の外部記録媒体は、サーバ室又は施錠可能な保管庫に保管するなどの盗難防止対策を講じなければならない。

（2）重要性分類Ⅲ以上の情報を記録し、保管及び委託事業者や外部機関への受渡しを行う外部記録媒体は、暗号化を実施するとともに、安全な輸送体制を確保しなければならない。

（3）外部記録媒体を委託事業者や外部機関と交換する場合は、適正な盗難防止策を講じるとともに、その履歴を残さなければならない。

（4）記録する情報の重要度にかかわらず、外部記録媒体の利用時には利用記録を作成しなければならない。また、外部記録媒体の盗難・紛失等時には、速やかにシステム統括管理者への報告を行わなければならない。

（5）外部記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

４．５ 端末機及びその他の機器の管理

（1）　端末機は盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。

（2）　スマートデバイスは盗難防止のため、施錠可能な保管庫に保管するなどの物理的措置を講じなければならない。

（3）　システム管理者及びシステム統括管理者は、端末機及びスマートデバイスには盗難や不正アクセス等に備え、利用者認証を必要とするように設定しなければならない。

（4）　システム管理者及びシステム統括管理者は、庁内ネットワークへ接続する端末機等については、原則として、「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

（5）　システム管理者及びシステム統括管理者は、庁内ネットワークへ接続する端末機等で USB メモリ等の外部記録媒体による情報持ち出しを行う場合、原則として、予めシステム統括管理者が許可した外部記録媒体のみに限定のうえ、データ管理責任者等のみが利用可能なよう設定しなければならない。

（6）システム管理者及びシステム統括管理者は、ネットワーク機器及びその他の機器については、不可抗力による損傷、破損、または意図的な情報の傍受等を防止するため、必要な措置を講じるよう努めなければならない。

５ 人的セキュリティ対策

５．１ 職員等の遵守事項

（1） 職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティの重要性を認識し、情報セキュリティポリシー並びにシステム管理者の定める情報セキュリティ実施手順に従い、情報資産を適正に扱わなければならない。

また、システム管理者及びデータ管理責任者は、採用時に情報セキュリティポリシーまたは情報セキュリティ実施手順、その他の関連法令等のうち、職員等が守るべき内容を理解させ、また実施及び遵守させなけなければならない。

② 業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

また、データ管理責任者は、所属する職員等に対し業務以外の目的でのインターネットへのアクセスを行わないよう常に周知、徹底し、適正に利用させなければならない。

③ 情報資産の持ち出しの制限

職員等は端末機等及び外部記録媒体等を外部に持ち出す場合は、システム統括管理者の許可を得なければならない。

④ 持ち出し及び持ち帰りの記録

データ管理責任者は、テレワークの実施に係る端末等の外部への持ち出し及び持ち帰りについて、記録を作成し、保管しなければならない。

⑤ 支給以外の端末機等の利用

（ア）職員等は、情報セキュリティ責任者（CISO）が認めた場合を除き支給以外のパソコン、モバイル端末を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

（ウ） 職員等は、支給以外の端末機、スマートデバイス及び外部記録媒体等を、原則業務で利用する公用の端末機等やネットワークに接続してはならない。

（エ） 職員等は、支給以外の端末機、スマートデバイス及び外部記録媒体等に、原則重要性分類Ⅲ以上の情報を記録してはならない。

⑥ 端末機やスマートデバイスにおけるセキュリティ設定変更の禁止

職員等は、端末機やスマートデバイスのソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦ 机上の端末機等の管理

職員等は、端末機、スマートデバイス、外部記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末機、スマートデバイスのロックや外部記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

職員等は、異動、退職等により業務に従事しなくなった後、利用していた情報資産を利用してはならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑨ インターネット接続及び電子メール使用等の制限

システム統括管理者は、職員等に端末機による作業を行わせる場合においては、業務上、インターネットへの接続及び電子メールの使用等が必要な場合に限り、利用を認めるものとする。

（2） 情報セキュリティポリシー等の掲示

システム統括管理者は、職員等が容易に情報セキュリティポリシー等を閲覧できるようにしなければ

ならない。

（3） 外部委託事業者に対する説明

システム管理者及びデータ管理責任者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

５．２ 研修・訓練

（1） 副情報セキュリティ責任者は、職員等に対し、情報セキュリティの重要性について啓発に努めるとともに、情報セキュリティポリシーに関する研修及び訓練を定期的に実施しなければならない。

（2） システム管理者は、管理する情報システムの情報セキュリティの維持・向上のため、所属する担当職員に対し、研修及び訓練を定期的に実施しなければならない。

（3） データ管理責任者は、利用する情報資産に関する情報セキュリティの理解を高めるため、所属する職員等に対し、研修及び訓練を定期的に実施しなければならない。また、研修の実施状況を記録し、情報セキュリティ責任者に対して報告しなければならない。

（4） 情報セキュリティ責任者は、研修の実施状況をセキュリティ委員会に報告しなければならない。

（5） 緊急時対応訓練

システム統括管理者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

５．３ 情報セキュリティインシデントの報告

（1） 情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントを発見した場合、個人情報漏洩に係る危機管理基本マニュアルに基づき、速やかにデータ管理責任者、システム管理者、危機管理調整担当及びセキュリティ事案連絡・相談窓口に報告しなければならない。

② 連絡を受けたシステム管理者及びシステム統括管理者は、当該事故等による情報セキュリティの侵害の程度に応じて、速やかに情報セキュリティ管理者、情報セキュリティ責任者（CISO）に報告しなければならない。

（2） 住民等外部からの情報セキュリティインシデントの報告

① 職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、個人情報漏洩に係る危機管理基本マニュアルに基づき、速やかにデータ管理責任者、システム管理者、危機管理調整担当及びセキュリティ事案連絡・相談窓口に報告しなければならない。

② 連絡を受けたシステム管理者及びシステム統括管理者は、当該事故等による情報セキュリティの侵害の程度に応じて、速やかに情報セキュリティ管理者、情報セキュリティ責任者（CISO）に報告しなければならない。

（3） 情報セキュリティインシデントの原因調査・記録、再発防止等

① CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

② CSIRT は、情報セキュリティインシデントであると評価した場合、情報セキュリティ責任者(CISO)に速やかに報告しなければならない。
③ CSIRT は、情報セキュリティインシデントに関係するシステム管理者及びデータ管理責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。
④ CSIRT は、関係するシステム管理者及びデータ管理責任者と連携し、これらの情報セキュリティインシデントの原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、情報セキュリティ責任者(CISO)に報告しなければならない。

5．4 ID 及びパスワード等の管理

(1) 個人認証カードの取扱い

① 職員等は、自己の管理する個人認証カードに関し、次の事項を遵守しなければならない。
(ア) 個人認証カードを職員等間で共有してはならない。
(イ) 退席時等で端末機を使用しない場合は、端末機の操作ロックを行い、個人認証カードを放置してはならない。
(ウ) 個人認証カードを紛失した場合には、速やかにシステム統括管理者に報告し、指示に従わなければならない。
② システム統括管理者は、個人認証カードの紛失等の報告があった場合は、当該個人認証カードを使用したアクセス等を速やかに停止しなければならない。

(2) ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。
① 自己が利用している ID は、他人に利用させてはならない。
② 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(3) パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
① パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
② パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
③ パスワードが流出したおそれがある場合には、パスワードを速やかに変更しなければならない。
④ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑤ サーバ、ネットワーク機器及び端末機のパスワードの記憶機能を利用してはならない。

6 技術的セキュリティ対策

6．1 サーバ等及びネットワークの管理

(1) 共有ファイルサーバの設定

① システム管理者は、職員等が使用できる共有ファイルサーバの容量を設定し、職員等に周知しなければならない。
② システム管理者は、共有ファイルサーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
③ 職員等は、所属する課室等の共有ファイルサーバの容量の増設を依頼する場合は、保存された既存のファイル等を整理してもなお増設が必要な場合に限り、増設の依頼をしなければならない。

(2) バックアップの実施

システム管理者は、所管するサーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

(3) 他団体との情報システムに関する情報等の交換

システム管理者は、他の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、その取扱いに関する事項をあらかじめ定め、システム統括管理者の許可を得なければならない。

(4) システム管理記録及び作業の確認

① システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、 改ざん等をされないように適正に管理しなければならない。

② システム管理者は、情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、作業内容を確認しなければならない。

(5) 情報システム仕様書等の管理

システム統括管理者及びシステム管理者は、所管する情報システムのネットワーク構成図、情報システム仕様書等について、記録 媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(6) アクセス記録等の各種ログの取得等

① システム統括管理者及びシステム管理者は、所管する情報システムのアクセス記録等の各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② システム統括管理者及びシステム管理者は、ログとして取得する項目、 保存期間、取扱方法及び取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③ システム統括管理者及びシステム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

システム管理者は、職員等からのシステム障害の連絡、システム障害に対する処理結果又は再発防止策等を、障害記録として記録し、適正に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

① システム統括管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないようにファイアーウォール、ルータ等の通信ソフトウエア等を設定しなければならない。

② システム統括管理者及びシステム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムへの対策

システム統括管理者及びシステム管理者は、電子申請システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと分離する等、強固なセキュリティ対策を講じなければならない。

(10) 外部ネットワークとの接続制限等

① システム管理者は、所管する情報システムを外部ネットワークと接続しようとする場合には、システム統括管理者と事前に協議し、許可を受けなければならない。

② システム統括管理者は、外部ネットワークとの接続に対して協議があった場合は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ システム統括管理者及びシステム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアーウォール等を外部ネットワークとの境界に設置したうえで、接続しなければならない。

④ システム統括管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（11） 複合機のセキュリティ管理

① システム管理者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ対策をしなければならない。

② システム管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ システム管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

（12） IoT 機器を含む特定用途機器のセキュリティ管理

システム統括管理者及びシステム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（13） 電子メールのセキュリティ管理

① システム統括管理者は、のスパムメール等が内部から送信されている検知をした場合は、メールサーバの運用を停止しなければならない。

② システム統括管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

③ システム統括管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

（14） 電子メールの利用制限

① 職員等は、自動転送機能を用いて、電子メールを転送してはならない。

② 職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③ 職員等は、複数人に電子メールを送信する場合、必要があるときを除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④ 職員等は、電子メールの送信等により情報資産を無断で外部に持ち出してはならない。

⑤ 職員等は、電子メールで送るデータの機密性を確保することが必要な場合には、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

（15） 電子署名・暗号化

①職員等は、外部に送る重要性分類Ⅲ以上の情報の機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

②職員等は、暗号化を行う場合にシステム統括管理者が定める以外の方法を用いてはならない。また、必要な場合には暗号化のための鍵を管理しなければならない。

③システム統括管理者及びシステム管理者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（16） 無許可ソフトウエアの導入等の禁止

① 職員等は、端末機に無断でソフトウエアを導入してはならない。

② 職員等は、業務上の必要がある場合は、システム統括管理者の許可を得た場合に限り、ソフトウエアを導入することができる。

③ 職員等は、不正にコピーしたソフトウエアを利用してはならない。

（17） 機器構成の変更の制限

① 職員等は、端末機やスマートデバイスに対し機器の改造及び増設・交換を行ってはならない。

② 職員等は、業務上、端末機やスマートデバイスに対し機器の改造及び増設・交換を行う必要がある場合には、システム統括管理者及びシステム管理者の許可を得なければならない。

（18） 無許可でのネットワーク接続の禁止

①職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

②情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

（19） 業務以外の目的でのインターネット閲覧の禁止

① 職員等は、業務以外の目的でインターネットを閲覧してはならない。

② 出所が不明なファイルや、内容に確証の得られていないファイル等は、実行してはならない。

③ データ管理責任者は、職員等が業務以外の目的でインターネットを閲覧していることが疑わしい又は判明した場合、当該職員への注意、指導を行わなければならない。

④ 情報セキュリティ責任者（CISO）及びシステム統括管理者は、職員等のインターネット利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、速やかにインターネット利用の停止等必要な措置を講じなければならない。

（20） 無線 LAN 及び庁外環境での端末機等の利用（広域無線通信含む）の制限

① 職員等は、災害時または、情報セキュリティ責任者（CISO）が認めた場合を除き、無線 LAN 及び庁外環境で端末機等の利用（広域無線通信含む）をしてはならない。

② 情報セキュリティ責任者（CISO）は、前項に基づき利用を認める場合、解読が困難な暗号化等の必要な措置を義務付けなければならない。

（21）個人情報等の保存制限

職員等は、インターネットに接続できる端末には、重要性分類Ⅲ以上の情報を保存してはならない。

（22）スマートデバイスに係るセキュリティ管理

① システム統括管理者及びシステム管理者は、スマートデバイスが備える機能や使用環境、取り扱う情報、その他業務の特性等に応じ、適正なセキュリティ要件を定め、必要な対策を実施しなければならない。

② 職員等は、スマートデバイスを使用するにあたり、システム統括管理者等が実施したセキュリティ対策及び、使用手順に従い、適正にスマートデバイスを使用しなければならない。

(23) Web 会議サービスの利用時の対策

①情報セキュリティ管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。

②職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

③職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

(24) ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ア)本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすし対策を実施すること。

(イ)パスワードや認証のためのコード等の認証情報及びこれを記録した媒体(ハードディスク、USB メモリ、紙等)等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②重要性分類Ⅲの情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

④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の措置を講じなければならない。

⑤情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

6.2 アクセス制御

(1) アクセス制御

① アクセス制御

システム統括管理者及びシステム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

② 利用者 ID の取扱い

(ア) システム統括管理者及びシステム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

(イ) システム統括管理者及びシステム管理者は、利用されていない ID が放置されないよう、人事管理部門等と連携し、点検しなければならない。

③ 特権を付与された ID の管理等

(ア) システム統括管理者及びシステム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(イ) システム統括管理者及びシステム管理者は、特権を付与された ID にて外部委託事業者が作業を行う場合は、職員等の立会いにより、作業内容の確認を行わなければならない。

(ウ) システム統括管理者及びシステム管理者は、特権を付与された ID 及びパスワードについては、定期的な変更または入力回数制限等により、特にセキュリティ機能を強化しなければならない。

(2) 職員等による外部からのアクセス等の制限

① システム統括管理者は、職員等が外部から内部のネットワーク又は情報システムにアクセスする経路を整備する場合、情報セキュリティ責任者(CISO)の許可を得なければならない。

② システム統括管理者は、外部からのアクセスを認める場合、端末認証や利用者認証を行う機能を確保しなければならない。

③ システム統括管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

④ システム統括管理者は、外部からのアクセスに利用する端末機等を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。また、その貸与記録を作成しなければならない。

⑤ システム統括管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスは情報セキュリティ責任者(CISO)が認めた場合を除き原則として禁止しなければならない。

(3) 自動識別の設定

システム統括管理者は、ネットワークに不正な機器の接続を防止するために、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よう努めなければならない。

(4) パスワード等の認証情報の管理

① システム統括管理者及びシステム管理者は、職員等のパスワード等の認証情報を厳重に管理しなければならない。各情報システムにおいて、認証情報を保護するためのセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② システム統括管理者及びシステム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③ システム統括管理者及びシステム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

(5) 特権による接続及び利用の制限

システム統括管理者及びシステム管理者は、管理者権限等の特権によるネットワークへの接続及び情報システムの利用を必要最小限にしなければならない。

6.3 システム開発、導入、保守等

(1) 情報システムの調達

① システム管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② システム管理者は、機器及びソフトウエアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

① システム開発における責任者及び作業者の特定

システム管理者は、システム開発の責任者及び作業者を特定しなければならない。

② システム開発における責任者、作業者のIDの管理

(ア) システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発 用IDを削除しなければならない。

(イ) システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③ システム開発に用いるハードウエア及びソフトウエアの管理

(ア) システム管理者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

(イ) システム管理者は、利用を認めたソフトウエア以外のソフトウエアが導入されている場合、当該ソフトウエアをシステムから削除しなければならない。

(3) 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

(ア) システム管理者は、システム開発及びテスト環境とシステム運用環境を分離する等の措置を講じるよう努めなければならない。

（イ） システム管理者は、システム開発及びテスト環境からシステム運用環境への移行について、システム開発計画の策定時に手順を明確にしなければならない。

② テスト

（ア） システム管理者は、新たに情報システムを導入する場合、既に稼動している情報システムに接続する前に、十分な動作試験等を行わなければならない。

（イ） システム管理者は、個人情報及び機密性の高いデータを、厳密なセキュリティ対策を施さない環境において、テストデータに使用してはならない。

（4） システム開発・保守に関連する資料等の保管

① システム管理者は、システム開発・保守に関連する資料及び文書を適正な方法で保管しなければならない。

② システム管理者は、テスト結果を一定期間保管しなければならない。

③ システム管理者は、情報システムに係るプログラム等を適正な方法で保管しなければならない。

（5） 情報システムにおける入出力データの正確性の確保

① システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6） 情報システムの変更管理

システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成、保管しなければならない。

（7） 開発・保守用のソフトウェアの更新等

システム管理者は、開発・保守用のソフトウェア等に更新を適用する場合、他の情報システムとの整合性を確認しなければならない。

（8） システム更新時の検証等

システム管理者は、システム更新時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6．4 不正プログラム対策

（1） 不正プログラム対策

① システム統括管理者は、外部ネットワークからの不正プログラムによるコンピュータウイルス感染等を防止 するため、内部ネットワークと外部ネットワークの境界に、不正プログラム対策ソフトウエアの導入等の措置を講じなければならない。

また、内部ネットワークから外部ネットワークへの接続時は、同様のチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

② システム統括管理者は、コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

③ システム管理者は、所管するサーバ等及び端末機等に、コンピュータウイルス等の不正プログラム対策ソフトウエアを常駐させなければならない。

④ システム管理者は、不正プログラム対策ソフトウエアのパターンファイルを常に最新の状態に保たなければならない。

⑤ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑥ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、システム統括管理者が許可した職員を除く職員等に当該権限を付与してはならない。

⑦ 業務で利用するソフトウェアは、。パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

(2) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

① 端末機等において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

② 外部からデータ又はソフトウエアを取り入れる場合には、必ず不正プログラム対策ソフトウエアによるチェックやデータの無害化を行わなければならない。

③ 差出人が不明、又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行わなければならない。

⑤ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合、及び検知した場合は、LAN ケーブルの即時取り外しを行う等、通信を行わない措置を行い、速やかにシステム統括管理者及びデータ管理責任者に報告しなければならない。

(3)外部組織の支援体制

情報セキュリティ責任者(CISO)は、不測の事態に備え、必要に応じて委託業者及び外部組織の支援を受けられるように準備しなければならない。

6.5 不正アクセス対策

(1) 不正アクセス対策

① システム統括管理者及びシステム管理者は、外部ネットワークからの不正アクセスによる侵入等を防止するため、内部ネットワークと外部ネットワークの境界に、不正アクセス対策ソフトウエアの導入等の措置を講じなければならない

② システム統括管理者及びシステム管理者は、不要な通信ポートの閉鎖及びサービスを削除又は停止ししなければならない。

③ システム統括管理者及びシステム管理者は、パターンファイルによる脅威検出を行う不正アクセス対策ソフトウエアについて、正常なアクセスへの影響を考慮のうえ、パターンファイルを更新しなければならない。

④ システム統括管理者及びシステム管理者は、内部ネットワーク等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(2) 記録の保存

システム統括管理者及びシステム管理者は、内部ネットワーク等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(3) 内部からの攻撃

システム統括管理者は、職員等及び外部委託事業者が使用している端末機等からの内部ネットワーク

等に対する攻撃や外部に対する攻撃を監視しなければならない。

（4）職員等による不正アクセス

システム統括管理者は、職員等による不正アクセスを発見した場合、当該職員等が所属する部署等のシステム管理者及びデータ管理責任者に通知し、適正な処置を求めなければならない。

（5）サービス不能攻撃

システム統括管理者及びシステム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムが必要な時に中断されることなく情報にアクセスできる状態を確保する対策を講じなければならない。

（6）標的型攻撃

システム統括管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

６．６　セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

システム統括管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

システム統括管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、 職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集及び共有

システム統括管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係部署で共有しなければならない。また、情報セキュリティに関する技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7　運用

7．1　情報システムの監視

（1）システム統括管理者及びシステム管理者は、不正プログラム、不正アクセス等による情報システムへの攻撃、侵入等を防止するため、ネットワーク監視等により情報システムの稼働状況について監視を行う等の措置を講じるよう努めなければならない。

（2）システム統括管理者及びシステム管理者は、不正プログラム、不正アクセス等のアクセスログ等を取得するサーバ等については、アクセスログの正確性を担保するため、正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

7．2　侵害（事故、欠陥等を含む）時の対応

（1）緊急時対応計画の策定

情報セキュリティ責任者（CISO）は、情報セキュリティに関する事故や障害、または情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証

拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って、適正に対処するものとする。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

① 関係者の連絡先
② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

(3) 業継続計画との整合性確保

情報セキュリティ責任者(CISO)は事業継続計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

情報セキュリティ責任者(CISO)は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の内容を見直さなければならない。

7.3 例外措置

(1) 例外措置の許可

職員等は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ責任者(CISO) 及びシステム統括管理者の許可を得て、例外措置を講じることができる。

(2) 緊急時の例外措置

職員等は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに情報セキュリティ責任者(CISO) 及びシステム統括管理者に報告しなければならない。

(3) 例外措置の管理

情報セキュリティ責任者(CISO) 及びシステム統括管理者は、例外措置の申請書及び審査結果等を適正に保管しなければならない。

7.4 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令の他、関係法令を遵守し、これに従わなければならない。

(1) 地方公務員法
(2) 著作権法
(3) 不正アクセス行為の禁止等に関する法律
(4) 個人情報の保護に関する法律
(5) 行政手続における特定の個人を識別するための番号の利用等に関する法律
(6) サイバーセキュリティ基本法
(7) 枚方市保有個人情報安全管理規程

８ 外部委託

８．１ 外部委託

（1） 外部委託先の選定基準

システム統括管理者及びシステム管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（2） 委託契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で次の情報セキュリティ要件を規定した契約を締結しなければならない（なお、個人情報を取扱う作業を委託する場合は、個人情報の保護に関する法律、枚方市保有個人情報安全管理規程、その他関連法令の規定に基づき、個人情報の保護に関して遵守しなければならない事項について、特記仕様書等として、契約内容に規定しなければならない）。

① 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
② 委託先の責任者、委託内容、作業者の所属、作業場所の特定
③ 通信速度及び安定性、システムの信頼性等の品質保証
④ 従業員に対するセキュリティ教育の実施
⑤ 提供された情報の目的外利用及び受託者以外の者への提供の禁止
⑥ 業務上知りえた情報の守秘義務
⑦ 再委託に関する制限事項の遵守
⑧ 委託業務終了時の情報資産の返還、廃棄等
⑨ 委託業務の定期報告及び緊急時報告義務
⑩ 市による検査
⑪ 市による監査
⑫ 市による事故時等の公表
⑬ 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)
⑭ 委託業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

（3） 委託事業者に対する対応

システム統括管理者、システム管理者及びデータ管理責任者は、情報セキュリティポリシーまたは情報セキュリティ実施手順、その他の関連法令等のうち、委託事業者が守るべき内容について説明し、遵守させなければならない。また、必要に応じ、必要なセキュリティ対策が確保されていることを定期的に確認し、問題が認められる場合には、契約内容に基づき改善要求等の措置を実施しなければならない。

８．２ 外部サービスの利用（重要性分類Ⅲ以上の情報を取り扱う場合）

(1) 外部サービスの利用に係る規定の整備

情報セキュリティ責任者は、外部サービスの利用に関する規定を整備すること。

(2) 外部サービスの選定

① システム管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

② システム管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。

(3) 外部サービスの利用に係る調達・契約

① システム管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

② システム管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

(4) 外部サービスの利用承認

①システム管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

８．３ 外部サービスの利用（重要性分類Ⅲ以上の情報を取り扱わない場合）

(1) 外部サービスの利用に係る規定の整備

情報セキュリティ責任者は、外部サービス（重要性分類Ⅲ以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

(2) 外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で重要性分類Ⅲ以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

９ 評価・見直し

９．１ 監査

（1） 監査の実施

情報セキュリティ委員会は、情報セキュリティポリシー及び情報セキュリティ実施手順が遵守されているか、または情報セキュリティ対策の実施状況について、定期的に又は必要に応じて、別に定める規定に基づき、監査を行うものとする。

（2） 情報セキュリティポリシーの見直しへの活用

監査の結果、及びセキュリティ事案連絡・窓口に連絡のあった情報セキュリティインシデント等の内容を踏まえ、情報セキュリティポリシー、その他情報セキュリティ対策の見直しが必要な場合は、速やかに見直しを行うものとする。

（3） 庁内横断的な対処

情報セキュリティ責任者は、監査の結果、庁内で横断的に改善が必要な事項については、セキュリティ委員会に報告の上、システム管理者及びデータ管理責任者に当該事項への対処を指示しなければならない。

９．２ 自己点検

（1） システム統括管理者及びシステム管理者、データ管理責任者は、情報セキュリティポリシー及び情報セキュリティ実施手順が遵守されているか、または情報セキュリティ対策の実施状況について、定期的に又は必要に応じて、自己点検を実施しなければならない。

（2） 報告

自己点検を行った場合は、自己点検結果と自己点検結果に基づく改善策を情報セキュリティ責任者（CISO）に対して報告しなければならない。

（3） 自己点検結果の活用

① 職員等は、自己点検の結果に基づき、自己の業務の範囲内で改善を図らなければならない。

② 自己点検結果の報告等により、情報セキュリティポリシー、その他情報セキュリティ対策の見直しが必要な場合は、速やかに見直しを行うものとする。

９．３ 情報セキュリティポリシーの見直し

情報セキュリティ委員会は、社会情勢の変化や新たな脅威の発生に対し迅速かつ適正に対応するため、必要に応じて、情報セキュリティポリシーの見直しを行う。