舞鶴市情報セキュリティポリシー
情報セキュリティ基本方針

令和8年3月

1. 目的
本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2. 定義
(１)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（ハードウェア及びソフトウェア）をいう。
(２)情報システム
　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。
(３)情報資産
　本市の保有する情報及び情報システムをいう。
(４)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。
(５)情報セキュリティポリシー
　本基本方針及び情報セキュリティ対策基準をいう。
(６)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（情報の非開示性）をいう。
(７)完全性
　情報が破壊、改ざん又は消去されていない正確かつ最新の状態を確保すること（情報の真正性及び非改ざん性）をいう。
(８)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、情報にアクセスし、利用できる状態を確保することをいう。
(９)職員等
　本市の職員（地方公務員法に基づき任用される常勤職員、会計年度任用職員を含む。）、その他本市の情報資産の取扱いに従事する全ての者をいう。
(１０)マイナンバー利用事務系（個人番号利用事務系）
　個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータ（当該情報システムで取り扱う情報を含む。以下同じ。）をいう。
(１１)LGWAN接続系
　地方公共団体情報システム機構が運営する総合行政ネットワーク（LGWAN）に接続された情報システム及びデータ（マイナンバー利用事務系に係るものを除く。）をいう。
(１２)インターネット接続系
　インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びデータ（LGWAN経由でインターネットに接続するシステムを含む。）をいう。
(１３)通信経路の分割
　LGWAN接続系とインターネット接続系の両環境間の通信環境を論理的又は物理的に分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
(１４)無害化通信
　インターネットメール本文のテキスト化や端末への画面転送、ファイルの危険因子除去等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(１５)画面転送
　画面情報を、セキュリティが確保された通信路を介して、別の端末（インターネット接続系端末等）に表示する技術又は当該技術を用いた操作をいう。表示された情報に対する操作は許可された範囲に限定され、原則として元データは転送先端末に保存されない。
(１６)クラウドサービス
　クラウドコンピューティング（利用者の需要に応じて、動的に情報通信技術リソース（サーバ、ストレージ、アプリケーション、ネットワーク等）が割り当てられ、インターネット等のネットワーク経由で広範に利用可能な仕組み）を用いて提供されるサービスをいう。
(１７)ガバメントクラウド
　デジタル社会形成基本法に基づき、国が地方公共団体の情報システムの共同利用及び標準化を推進するために整備する、セキュリティが確保されたクラウドサービス利用環境をいう。
(１８)生成AI
　大量のデータから学習し、文章、画像、音声、プログラムコード等の新たなコンテンツを生成する能力を持つ人工知能（AI）の総称をいう。本ポリシーにおいては、特に大規模言語モデル（LLM）を構成要素とするテキスト生成AIを指す場合がある。
(１９)Web会議サービス
　インターネット等のネットワークを介して、遠隔地の相手と映像、音声、資料等を共有しながら会議を行うことを可能とするサービスをいう。
(２０)IoT機器（Internet of Things機器）
　センサー、アクチュエーター、通信機能等を備え、インターネット等のネットワークに接続され、情報の収集、交換、制御等を行う機器をいう（庁舎内の監視カメラ、環境センサー、スマートメーター等を含む。）。
(２１)ソーシャルメディアサービス
　利用者間の情報発信やコミュニケーションを主たる目的として、インターネット上で提供されるサービスをいう（SNS、ブログ、動画共有サイト等を含む。）。
(２２)CSIRT (Computer Security Incident Response Team)
　情報セキュリティインシデントの発生時に、その対応（検知、分析、対処、報告、再発防止等）を専門的に行う組織又はチームをいう。
(２３)EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
　無線LAN等において、電子証明書を用いて端末と認証サーバ間で相互認証を行うための認証プロトコルをいう。
(２４)WPA3-Enterprise
　Wi-Fi Allianceによって策定された、企業向けの無線LANセキュリティプロトコルであり、より強力な認証及び暗号化機能を提供するものをいう。

3. 対象とする脅威
　情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。
(１)不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
(２)情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去、業務停止等。

(３)地震、落雷、火災、風水害等の自然災害によるサービス及び業務の停止等。
(４)大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等。
(５)電力供給の途絶、通信の途絶、水道供給の途絶等の社会インフラの障害からの波及等。

4. 適用範囲
(１) 行政機関の範囲
　本基本方針が適用される行政機関は、市長部局、行政委員会（選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会）、教育委員会（ただし対策基準以下については別途定めるものとする）、議会事務局、消防本部及び地方公営企業とする。

(２)情報資産の範囲
　本基本方針が対象とする情報資産は、次のとおりとする。
①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
②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。）
③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

5. 職員等の遵守義務
　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及びこれに基づき策定される情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策
　上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(１)組織体制
　本市の情報資産について、情報セキュリティ対策を推進し、統括する全庁的な組織体制を確立する。

(２)情報資産の分類と管理
　本市の保有する情報資産を、機密性、完全性、可用性に応じて分類し、当該分類に基づき適切な情報セキュリティ対策を実施する。

(３)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、情報システム全体に対し、次の三段階の対策を講じる。
①マイナンバー利用事務系においては、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。
②LGWAN接続系においては、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インターネット接続系においては、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。

(４)物理的セキュリティ
　　サーバ等の情報システム機器、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(５)人的セキュリティ
　　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(６)技術的セキュリティ
　　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(７)運用
　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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(８)業務委託と外部サービス（クラウドサービス）の利用
　業務委託を行う場合には、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、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。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、運用手順を定め、発信できる情報を規定し、責任者を定める。

(９)評価・見直し
　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施
　情報セキュリティポリシーの遵守状況を検証し、その実効性を確保するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し
　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合、及び情報セキュリティに関する技術動向、脅威の状況、法令等の変化した場合は、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで必要に応じて情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定
　上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定
　情報セキュリティ対策基準に基づき、情報セキュリティ対策を具体的に実施するための手順、手続き等を定めた情報セキュリティ実施手順を、必要に応じて策定するものとする。な

お、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがある情報を含むため、原則として非公開とする。