第 6 版

彦根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）

彦根市

目　次

改訂履歴

当初制定日	平成 15 年(2003 年) 8 月 29 日
第 2 版	平成 18 年(2006 年) 6 月 15 日　改正
第 3 版	平成 28 年(2016 年) 2 月 10 日　改正
第 4 版	令和　5 年(2023 年)11 月 21 日　改正
第 5 版	令和　7 年(2025 年) 5 月 12 日　改正
第 6 版	令和　8 年(2026 年) 3 月 2 日　改正

第１章　総則

１．１　情報セキュリティポリシーの位置付けおよび構成

情報セキュリティポリシーは、本市が運用する情報システムおよび保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、情報セキュリティ基本方針および情報セキュリティ対策基準から構成される。

情報セキュリティ対策における基本的な考え方を定めるものが､｢基本方針｣である。この情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、地方公務員法に規定する一般職および特別職の職員（以下「職員」という。）が遵守すべき事項および判断基準をまとめたものが「情報セキュリティ対策基準」である。

本市では、情報資産の適正な管理・運用を行うための明確な枠組みとして、「彦根市情報セキュリティポリシー」を策定し、これを実践していくことにより、市民の利便性の向上と情報資産の保護を高次元で両立させ、高度情報化社会に対応した行政運営を進めることとする。

１．２　取組方針

本市の情報資産をどのような脅威からどのようにして守るかについての基本的な考え方や方向性などを｢彦根市情報セキュリティポリシー｣として示すこととし、これを全庁的に遵守すべき行為および判断等の基準としながら、さらに、定期的な見直しや改善を図り、情報資産の適正な管理・運用に努めることとする。

(1) 情報資産取扱者全員の関与

本市の職員および業務委託先会社社員など本市の情報資産を扱う者は、情報セキュリティポリシーを遵守し、情報資産の適正な管理・運用に努める。

(2)　法令遵守

地方公務員法、著作権法、不正アクセス禁止法、個人情報保護法等関連する法令等を遵守し、情報資産の適正な管理・運用に努める。

(3)　情報セキュリティ関連手順書等

情報資産の管理・運用において、関連する手順書やマニュアルを作成する場合は、情報セキュリティポリシーの内容を盛り込むこととする。

１．３　情報セキュリティの枠組み

情報セキュリティ管理は､情報に関する脅威から情報資産を守ることと位置づける。

その情報資産を守るにあたっては、情報が不当に他者に漏えいしない(機密性)、情報が改ざんされない(完全性)、障害発生時にも継続して提供できる(可用性)の３つの側面を定義する。

本市では３つのセキュリティの側面において、本市の情報資産を守るための基盤として情報セキュリティポリシーおよび実施手順を定め､これらを遵守するものとする。

ただし、公文書の公開および個人情報の保護については、それぞれ彦根市情報公開条例および個人情報の保護に関する法律を優先する。

１．４　情報セキュリティポリシーの管理

１．４．１　情報セキュリティポリシーの周知徹底

情報セキュリティポリシーは、職員に対し電子データにて配布し、周知徹底する。

また、所属長は情報セキュリティポリシーを所属の職員に周知徹底しなければならない。

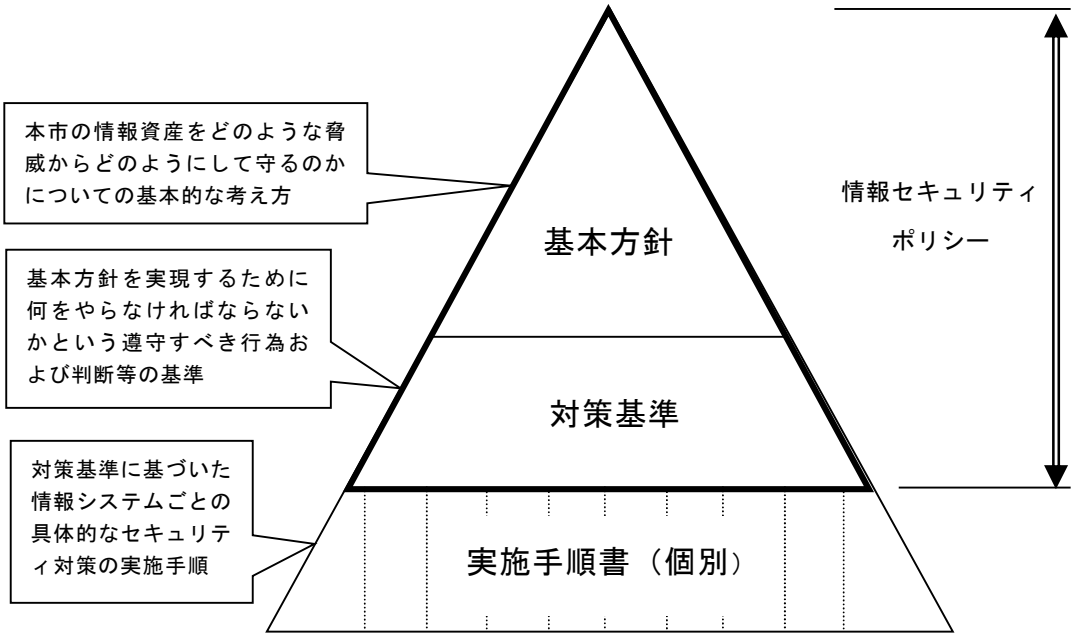
１．４．２　情報セキュリティポリシーの改訂

情報セキュリティポリシーは情報セキュリティ分科会により定期的に見直し、情報化戦略本部長の承認を得て改訂する。

⑴改訂後に所属長は、改訂内容を所属の職員に周知徹底する。

１．４．３　各組織における基準、手順

情報セキュリティポリシーに基づき、各組織に合った実行可能な基準、手順を定めることができる。



情報セキュリティポリシーに関する体系図

第２章　情報セキュリティ基本方針

２．１　目的

本基本方針は、本市が保有する情報資産の機密性、完全性およ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。

２．２　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(ハードウェアおよびソフトウェア)をいう。

(2)　情報システム

コンピュータ、ネットワークおよ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)　情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

(4)　情報セキュリティポリシー

本基本方針および情報セキュリティ対策基準をいう。

(5)　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。

(6)　完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

(7)　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。

(8)　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）または戸籍事務等に関わる情報システムおよびデータをいう。

(9)　LGWAN 接続系

LGWAN に接続された情報システムおよびその情報システムで取り扱うデータをいう(マイナンバー利用事務系を除く。)。

(10)　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およびその情報システムで取り扱うデータをいう。

(11)　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。

(12)　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など、安全が確保された通信をいう。

２．３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　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

⑵　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・消去等

⑶　地震、落雷、火災等の災害によるサービスおよび業務の停止等

⑷　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

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

２．４　適用範囲

⑴　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、議会事務局、消防本部および地方公営企業とする。

⑵　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ネットワークおよび情報システム並びにこれらに関する設備および電磁的記録媒体

②ネットワークおよ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およびネットワーク図等のシステム関連文書

２．５　職員の遵守義務

職員は、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および情報セキュリティ実施手順を遵守しなければならない。

２．６　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、完全性および可用性に応じて分類し、当該分類に基づき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、都道府県およ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、情報システム室、通信回線および職員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、職員が遵守すべき事項を定めるとともに、十分な教育およ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、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。

(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、定期的または必要に応じて情報セキュリティ監査およ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。

２．７　情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査および自己点検を実施する。

２．８　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および自己点検の結果、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および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になった場合には、保有する情報および利用する情報システムに係る脅威の発生の可能性および発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

２．９　情報セキュリティ対策基準の策定

上記６、７および８に規定する対策等を実施するために、具体的な遵守事項およ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。

２．１０　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実施するための具体的な手順を定めた情報セキュリティ実施手順を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ことから非公開とする