情報セキュリティ基本方針

第3．2版

長　井　市

改正履歴

施行年月	版番号	内容
平成17年4月	第1．0版	策　　定
平成19年4月	第1．1版	一部改正
平成21年4月	第1．2版	一部改正
平成24年4月	第2．0版	全部改正 （平成24年4月1日決裁）
平成28年3月	第3．0版	全部改正 （平成28年3月7日決裁）
令和元年11月	第3．1版	一部改正（令和元年11月1日決裁）
令和8年3月	第3．2版	一部改正（令和8年3月31日決裁）

情報セキュリティポリシーの構成

情報セキュリティポリシーとは、長井市（以下、「市」という。）が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、体系的かつ具体的に取りまとめたものである。

市の情報システムが取扱う情報には、市民の個人情報や行政運営上重要な情報が多数含まれている。これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、安定的かつ継続的な行政サービスの運営のためにも必要不可欠である。

情報セキュリティポリシーは情報セキュリティ基本方針と情報セキュリティ対策基準の2階層に分け、それぞれを策定する。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として、必要に応じて情報セキュリティ実施手順を策定することとする（下表参照）。

【情報セキュリティポリシー】

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すためのすべての情報システムに共通する情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

目次

1　目的

本基本方針は、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、市が実施する情報セキュリティ対策について情報セキュリティポリシーの対象、位置付け等の基本的な事項を定めることを目的とする。

2　用語の定義

本基本方針における用語の定義は、次のとおりとする。

(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及びその構成機器（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。

(4)　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。

(5)　機密性

アクセスを認可さ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、改ざん又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

アクセスを許可された者が、必要なときに中断されることなく、情報及び関連する資産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）又は戸籍事務等に関わる情報システム及びデータをいう。

(9)　LGWAN 接続系

人事給与、財務会計及び文書管理等 LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

(10)　インターネット接続系

インターネットメール、ファイル交換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等、安全が確保された通信をいう。

3 対象範囲

本基本方針が適用される範囲は、長井市情報公開条例(平成 10 年 3 月 24 日条例第 1 号)第 2 条に規定する市長、議会、教育委員会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会、並びに長井市立学校設置条例(昭和46年条例第9号)により設置する小中学校の事務室及び職員室の一部とする。

また、本基本方針の対象となる職員等及び市の保有する情報資産、脅威は次のとおりとする。

(1) 職員等

① 市長、副市長等の特別職の職員
② 一般職の職員(技能労務職員を含む。)
③ 非常勤職員
④ 契約等に基づき、市の保有する情報資産に関する業務に携わる外部委託者(以下「外部委託者等」という。)

(2) 情報資産

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扱う情報(電子データ及び印刷文書を含む。)
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

(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。

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、外部委託管理の不備、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

③ 地震、落雷、火災等の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提供サービスの障害からの波及等

4 職員等の義務

市が保有する情報資産に関する業務に携わる全ての職員及び外部委託者等（以下「職員等」という。）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、情報資産の取扱に当たって、情報セキュリティポリシー、情報セキュリティ実施手順及び関連する諸規程を遵守しなければならない。

5 情報セキュリティ対策

市が保有する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

市が保有する情報資産について、適切に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

市の保有する情報資産を機密性、完全性及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行う。

(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

コンピュータ機器、ネットワーク機器等の設置場所等について、重要性レベルの高い機器は、施錠管理、入退室管理などを厳重に施した区域に設置する等の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する権限及び職員等が遵守すべき事項を定めるとともに、職員等が情報セキュリティポリシーを理解し、遵守するための、十分な教育・訓練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

不正なアクセス等から情報資産を適切に保護するため、情報システム及びネットワークの管理、情報資産へのアクセス制御、情報システムの開発・導入の基準、コンピュータウイルス対策等の技術的な対策を講じる。

(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、外部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。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切に対応するため、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。

(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。

6 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。

7 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情報セキュリティポリシーを見直す。

8　情報セキュリティ対策基準の策定

上記5、6及び7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。

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。

9　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。