長野市情報セキュリティポリシー

更　新　履　歴

１　平成 15 年９月１日　施行する。

２　平成 21 年４月１日　全面改正し、施行する。

３　平成 27 年 11 月１日　一部改正し、施行する。

４　平成 30 年 11 月 21 日　一部改正し、施行する。

５　令和３年９月８日　一部改正し、施行する。

６　令和４年４月１日　一部改正し、施行する。

７　令和６年１月１日　一部改正し、施行する。

８　令和６年４月１日　一部改正し、施行する。

９　令和７年６月４日　一部改正し、施行する。

10　令和７年 12 月１日　一部改正し、施行する。

基本方針

長野市情報セキュリティ基本方針

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) 情報セキュリティインシデント

ネットワーク又は情報システムがウイルス感染や不正アクセス等を受けること若しくは人為的ミスによって、情報資産が停滞、流出又は紛失し、業務の遂行が困難になる又は情報セキュリティを脅かす事象のことをいう。具体的には、「３　対象とする脅威」を想定する。

(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状態を確保することをいう。

(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、情報にアクセスできる状態を確保することをいう。

(9) 特定個人情報

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（以下「番号法」という。）第２条第９項に規定する、個人番号をその内容に含む個人情報ファイルをいう。

(10) 個人番号利用事務

番号法第２条第 11 項に規定する個人番号を利用して処理する事務をいう。

(11) 個人番号関係事務

番号法第２条第 12 項に規定する個人番号利用事務に関して行われる他人の個人番号を利用して行う事務をいう。

(12) 基幹系ネットワーク

住民基本台帳法（昭和 42 年法律第 81 号）による住民基本台帳に記載された情報を利用して市民に行政サービスを提供する事務に係る情報システムにより構成される情報通信ネットワークをいう。

(13)情報系ネットワーク

部局及び執行機関において共通して処理する事務に係る情報システムであって、インターネットに接続されないもののみにより構成される情報通信ネットワークをいう。

(14)インターネット接続系ネットワーク

ホームページの更新及びウェブサイトの閲覧、その他主としてインターネットを利用して行う事務に係る情報システムのみにより構成される情報通信ネットワークをいう。

(15)個別ネットワーク

前３項目に掲げる情報通信ネットワーク以外の情報通信ネットワークをいう。

(16)通信経路の分割

情報系ネットワークとインターネット接続系ネットワーク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。

(17)無害化通信

インターネットメールの無害化やファイルの無害化により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

(18)業務委託

本市の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。なお、当該契約形態は、「委託」「準委任」「請負」といったものを問わず、全てを含むものとする。ただし、当該業務において本市の情報を取り扱わせる場合に限る。

(19)外部サービス（クラウドサービス）

一般の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サービスをいう。

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、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意図的な要因又は人為的ミスによる情報資産の漏えい・破壊・改ざん・消去・紛失、重要情報の詐取、内部不正等

(2) 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

(3) 地震、落雷、火災等の災害、事故、故障等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インフラの障害からの波及等

4　適用範囲

(1) 対象組織の範囲

本基本方針が適用される対象組織は、次のとおりとする。

市長部局、議会の事務局、選挙管理委員会及びその事務局、監査委員及びその事務局、公平委員会及びその事務局、農業委員会及びその事務局、固定資産評価審査委員会、教育委員会及びその事務局、教育機関、上下水道局並びに消防局

(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。

ア　ネットワーク及び情報システムに関する次の情報資産（表１に分類する。）

(ｱ) 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

(ｲ) 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。）

(ｳ) 情報システムの仕様書及びネットワーク構成図等のシステム関連文書

イ　行政情報（長野市情報公開条例第２条第２号　参照）

※個人的資料及びメモ類は情報資産の範囲外とするが、作成から廃棄まで個人が確実に管理する。

表１　情報資産の種類と例示

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	情報システム室、コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	サーバ装置、パソコン、通信回線装置等に内蔵される内蔵電磁的記録媒体、外付けハードディスク、FD、CD、DVD、BD、USB メモリ、デジタルカメラ、IC レコーダー、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書や帳票類を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

5　職員等の遵守義務

職員（非常勤職員を含む。）及び労働者派遣事業により本市の業務に携わる者（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、業務の遂行に当たって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書群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する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侵害された場合に想定される影響の大きさに応じて分類し、当該分類に基づき情報セキュリティ対策を講じる。

(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。ただし、個別ネットワークについては、当該個別ネットワークを構成する情報システムにより処理をする事務を所掌する課（課に相当する室、局、所、館及びセンターを含む。）の長が必要に応じて別に対策を講じる。

ア　基幹系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。

イ　情報系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ネットワーク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。

ウ　インターネット接続系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、長野県自治体情報セキュリティクラウドを利用する。

(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、利用にかか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。なお、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。

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。