小野町情報セキュリティポリシー

改訂履歴

施行年月日	版番号	備　考
平成１５年１２月　１日	第１版	初版（小野町情報化推進本部決定）
平成２４年　７月　９日	第２版	対策基準一部改正（小野町情報化推進本部決定）
令和　８年　３月１７日	第３版	一部改正（小野町 DX 推進本部決定）

目次

第１章小野町情報セキュリティ基本方針

１.目的

行政が取り扱う情報資産には、住民の個人情報のみならず、運営上重要な情報など外部に漏えい等した場合には極めて重大な結果を招く情報が多数含まれており、これらの情報資産を様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、継続的かつ安全・安定的な行政運営のためにも必要不可欠である。

また、住民サービスの向上、業務効率化や合理化の要請に対応するために、行政における情報システムによる業務量及び利用範囲は拡大の一途をたどっており、行政運営基盤として欠かせないものとなっている。そのため、円滑に業務を進めるためには、管理している全ての情報システムが高度な安全性を有することが不可欠である。

このことから、小野町（以下「本町」という。）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「小野町情報セキュリティポリシー」を定めるものとする。このうち、情報セキュリティ基本方針は、本町の情報セキュリティ対策の基本的な方針を定めたものである。

２.定義

（１）職員等

本町の職員（会計年度任用職員等を含む。）、外部委託事業者、その他本町の業務に携わる者のうち本町の情報資産を取り扱う者をいう。

（２）情報資産

本町が保有する情報やデータ及びそれに関連する資源をいう。

（３）データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（４）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。

（５）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。

（６）サーバ室

ネットワークの基幹機器及び情報システム、電磁的記録媒体等の保管庫を設置し、当該機器等の管理及び運用を行うための部屋をいう。

（７）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。

（８）情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

（９）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。

（１０）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。

（１１）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。

（１２）マイナンバー利用事務系（個人番号利用事務系）

マイナンバー利用事務（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。

（１３）LGWAN 接続系

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（マイナンバー利用事務系を除く）。

（１４）インターネット接続系

インターネットメール、ウェブサイト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その情報システムで取り扱うデータをいう。

（１５）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。

（１６）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.対象とする脅威

情報資産に関する脅威として、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、業務委託等の管理の不備、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

情報セキュリティ基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、地方公営企業及びその他本町が保有する情報資産を扱う組織等（以下「実施機関」という。）とする。

（２）情報資産の範囲

情報セキュリティ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、日々の業務において情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたって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、以下の情報セキュリティ対策を講じる。

（１）組織体制

本町の情報資産について、適切に情報セキュリティ対策を推進・管理するため、全庁的な組織体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

（２）情報資産の分類と管理

本町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。

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

情報システム設置場所への入退室、サーバ等の管理、通信回線及び端末等へ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し、職員等が遵守すべき事項を定めるとともに、十分な研修・訓練及び啓発を実施するなど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、コンピュータウイルス等の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、業務委託等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切に対応するため、情報セキュリティインシデント発生時対応手順書を策定する。

（８）業務委託等及び外部サービス（クラウドサービス）の利用

業務委託等をする場合には、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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。

クラウドサービスを利用する場合には、外部サービス（クラウドサービス）利用ガイドラインを整備し対策を講じる。

（９）ソーシャルメディアサービスの利用

ソーシャルメディアサービスを利用する場合は、運営者情報のほか利用目的、発信内容、運用方法（運用時間、対応方法）、利用規約（注意事項、著作権、免責事項）、炎上・トラブル時の対応策、アカウントの管理方法など、運用に必要な事項を含めたソーシャルメディアサービス運用方針や運用ルールを定めなければならない。

７.情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施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施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町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。

第２章小野町情報セキュリティ対策基準

　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を実行に移すため、本町における情報資産に関する情報セキュリティ対策の基準を定めたものである。

非公開

　情報セキュリティ対策基準の一部は、公にすることにより本町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。