日野町情報セキュリティポリシー

平成16年2月27日　策定
令和８年３月18日　改訂

日野町

改訂履歴

施工年月日	版番号	改訂内容・内容
平成 16 年 2 月 27 日	第 1.0 版	初版発行
平成 29 年 6 月 30 日	第 2.0 版	番号制度導入および総務省ガイドライン改正に伴う改訂
令和 8 年 3 月 18 日	第 3.0 版	総務省ガイドライン改正に伴う改訂

目次

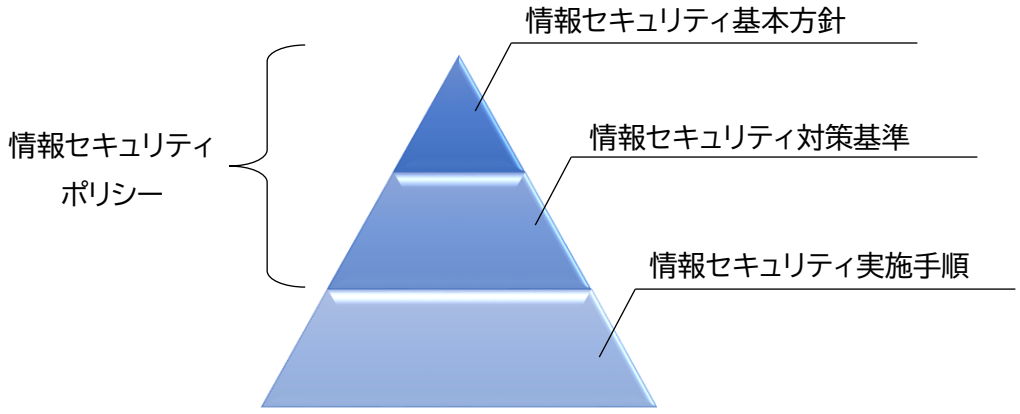
情報セキュリティ対策基準および情報セキュリティ実施手順については公にすることによりサイバー攻撃を受けるリスクがあることから、非公開とする。

序　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、本町が所掌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基準は、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、職員、再任用職員、任期付職員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により本町業務に従事する者（以下「職員等」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である。本町では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

情報セキュリティポリシーの構成



日野町情報セキュリティ基本方針

1. 目的

本町が取り扱う情報には、町民の個人情報や行政運営上の情報など、改ざんや漏えいがあった場合には極めて重大な結果を招くと懸念される情報が多く含まれている。

よって、本町の取り扱う情報ならびにネットワークおよび情報システムを様々な脅威から守ることは、町民の財産やプライバシーを保護し、行政サービスの安定的な運営を図るために必要不可欠であり、ひいては、本町の行政運営に対する町民の信頼の維持向上に結びつけるものである。

また、情報化の進展により重要性がます情報資産を、故意または過失による事故および災害の脅威から守り、情報セキュリティの水準を総合的、体系的かつ具体的に確保していくためには、本町が保有するすべての情報ネットワークおよび情報システムが高度な安全性を有していることが前提となる。

このため、本基本方針は、本町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、本町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

2.1 ネットワーク

本町における内部部局、各行政委員会、各出先機関等の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。

2.2 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。

2.3 情報資産

ネットワークおよび情報システムの開発と運用にかかるすべての情報ならびにネットワークおよび情報システムで取り扱うすべての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含むものとする。

2.4 情報セキュリティ

情報資産の機密性の保持および正確性、完全性の維持ならびに定められた範囲での利用可能な状態を維持することをいう。

2.5 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。

2.6 機密性(confidentiality)

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。

2.7 完全性(integrity)

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。

2.8 可用性(availability)

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。

2.9 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、地方税も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。

2.10 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。）。

2.11 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。

2.12 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。

2.13 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、不正操作、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機器または情報資産の破壊、盗難、持ち出し、盗聴、改ざん、消去、重要情報の詐取、内部不正等

(2) 職員等または委託事業者による情報資産または機器の無断持ち出し、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、パスワード等認証情報の不適切管理、搬送中の事故等による情報資産または機器等の紛失、盗難、規定外のネットワーク接続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、故障等による行政サービスおよび業務の停止等

(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

4.1 組織の範囲

本基本方針が適用される組織は、町長、教育委員会事務局、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、議会事務局、議会および地方公営企業とする。

4.2 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) ネットワークおよび情報システムなら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

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。

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。

6.1 組織体制

本町の情報資産を守るため、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。

6.2 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。

6.3 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、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。
(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。
(2) LGWAN 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。

6.4 物理的セキュリティ

情報システムを設置する施設（データセンターおよび庁舎サーバ室）への不正な立入り、情報資産への損傷、妨害等から保護するために入退室、通信回線およ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。

6.5 人的セキュリティ

情報セキュリティに関し、職員等が順守すべき事項を定めるとともに、情報セキュリティポリシーの内容を周知徹底する等、十分な教育および啓発に必要な人的な対策を講じる。

6.6 技術的セキュリティ

情報資産を外部からの不正なアクセス等から適切に保護するため、コンピュータ等の管理、情報資産へのアクセス制御、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。

6.7 運用面におけるセキュリティ対策

情報システムの監視、職員等および委託事業者の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等の緊急事態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。

6.8 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。

6.9 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。

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対策の実施状況の監査およ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

情報セキュリティ対策の実施状況の監査および自己点検の結果、情報セキュリティポリシー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。

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。

なお、情報セキュリティ対策基準は、公にすることによりサイバー攻撃を受けるリスクがあることから、非公開とする。

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。