千代田町情報セキュリティポリシー

令和 7 年度

情報セキュリティ基本方針

１．目的

千代田町（以下「本町」という。）のネットワーク、情報システム、コンピュータ等が取り扱う情報には、町民の個人情報のみならず、外部に漏えい、消失した場合には生活に重大な影響を及ぼす行政運営上重要な情報等が多数含まれている。これらの情報並びに情報を取り扱うネットワーク、情報システム、コンピュータ等を様々な脅威から防御することは、町民の財産、プライバシー等を守るためにも、安定的な行政運営のためにも必要不可欠である。ひいては、このことが本町に対する町民からの信頼の維持・向上に寄与する。

本基本方針は、本町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

（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

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

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）

マイナンバー法に定められている個人番号利用事務（社会保障、地方税又は防災に関する特定の事務）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

マイナンバー利用事務系を除いた、ＬＧＷＡＮに接続された情報システム及び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

ＬＧＷＡＮ接続系を除いた、電子メール、Ｗｅｂサイト管理システム、内部事務を取り扱う情報システム等の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ない等、安全が確保された通信 をいう。

（１３）自治体情報セキュリティクラウド

インターネットとの通信の常時監視及びログの分析・解析を始め高度なセキュリティ対策を実施するものをいう。

（１４）クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。この構成要素として、SaaS（Software as a Service）1、PaaS（Platform as a Service）2、IaaS（Infrastructure as a Service）3が存在する。

（１５）ソーシャルメディアサービス

インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった

社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

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

本基本方針が適用される行政機関は、町長、教育委員会、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及び議会並びにこれらに置かれる機関とする。

（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、情報システム及びこれらに関する設備、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

（３） 適用除外

本基本方針は次の範囲を適用しない。

（ア）学校の範囲

小学校、中学校及び適用指導教室（以下、学校）は、コンピュータを活用した学習活動の実施など、教職員はもとより、児童生徒が日常的に情報システムにアクセスする機会があるなど、上記（1）の行政機関と異なるため、千代田町教育委員会事務局は千代田町教育情報セキュリティポリシーを策定すること。

５．職員等の遵守義務

正職員、再任用職員、臨時任用職員、特別職非常勤職員、会計年度任用職員、町長、副町長、教育長、群馬県教育委員会に属する職員等（本基本方針が対象とする行政機関の情報資産を利用する職員、事務職員及び学校栄養職員）、派遣労働者、外部人材（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を遵守しなければならない。

（１）　正職員

任期の定めのない常勤職員

（２）　任期付職員

任期付職員及び任期付時短職員

（３）　再任用職員

定年退職者を再任用する制度による再任用職員及び再任用短時間職員

（４）　臨時的任用職員

地方公務員法第 22 条の３に基づく常勤職員に欠員を生じた場合の臨時的任用臨時的任用職員

（５）　特別職非常勤職員

地方公務員法第 3 条の第 3 項に基づく、専門的な知識経験等に基づき、助言調査を行なう者特別職非常勤職員

（６）　会計年度任用職員

地方公務員法第 17 条及び第 22 条の 2 に基づく、会計年度任用職員（フルタイム）及び会計年度任用職員（パートタイム）

（７）　町長

千代田町長

（８）　副町長

千代田町副町長

（９）　教育町長

千代田町教育長

（１０）群馬県教育委員会に属する職員等

（ア）教職員

群馬県教育委員会に属する職員のうち行政機関の情報資産を利用する教職員

（イ）事務職員

群馬県教育委員会に属する職員のうち行政機関の情報資産を利用する事務職員

（ウ）学校栄養職員

群馬県教育委員会に属する職員のうち行政機関の情報資産を利用する学校栄養職員

（１１）派遣労働者

千代田町役場が契約する人材派遣会社から派遣される使用人のうち行政機関の情報資産を利用する派遣労働者

（１２）外部人材

内閣官房・内閣府が地方創生人材支援制度を通じて、千代田町に対して国家公務員、大学研究者、民間専門人材を派遣する外部人材

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

本町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、県及び市町村等のイン 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を利用する。

（４）物理的セキュリティ

サーバ等、情報システム室等、通信回線等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、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、緊急時対応計画を策定する。

（８）業務委託と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。 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。

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、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。

また、情報セキュリティ対策基準は、公にすることにより本県の情報セキュリティ対策 に支障を及ぼすおそれ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。