立科町情報セキュリティポリシー

「情報セキュリティ基本要綱」

平成 16 年 3 月 12 日
訓令第 4 号

（目的）

第１条　立科町が取り扱う情報資産には、町民の個人情報をはじめとし行政運営上重要な情報など、部外に漏えい又は滅失等した場合には、極めて重大な結果を招く恐れのある情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等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、また、継続的かつ安全並びに安定的な行政サービスの実施を確保するためにも必要不可欠であり、ひいては、立科町に対する町民からの信頼の維持向上に寄与するものである。

また、近年のいわゆる IT 革命の進展により、電子政府や電子自治体の実現が期待されている中で、ネットワーク及び情報システムが高度な安全性を有することが不可欠となる。

このため、この要綱は立科町の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の立科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ものとする。

（定義）

第２条　用語の定義

（１）電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体（磁気ディスク等）をいう。

（２）ソフトウェア

電子計算機で稼働するプログラム及びユーザーマニュアル等をいう。

（３）ネットワーク

立科町役場本庁、現地機関、行政委員会、議会事務局、及び福祉施設の事務室で使用される電子計算機及びそれらを相互に接続するための通信網で構成され、情報処理を行う仕組みをいう。

（４）公共端末

立科町の施設等に設置され、職員等及び業務委託者以外の者が操作する端末の総称をいう。

（５）情報システム

立科町の業務用に使用される電子計算機及び記録媒体で構成され、処理を行う仕組みをいう。

（６）情報資産

ネットワーク及び情報システムの開発と運用に係るすべてのデータ並びにネットワーク及び情報システムで取り扱うすべてのデータをいう。

（７）構成情報

電子計算機及びネットワークの設定や配置場所の情報をいう。

（８）行政情報

職員等が職務上収集し、利用及び保管している情報をいう。

（９）機密性

情報にアクセスすることが許可された者だけがアクセスできること。

(10) 完全性

情報及び処理の方法が正確かつ完全であること。

(11) 可用性

許可された利用者が必要なときに情報にアクセスできること。

(12) 情報セキュリティ

機密性、完全性及び可用性の維持並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。

(13) 職員

地方公務員法で規定された特別職、一般職の中で、立科町に勤務する者の総称をいう。

(14) 関係機関の職員等

各種委員会、福祉施設等に勤務し、立科町が管理する情報資産を職務で利用する者の総称をいう。

(15) 職員等

職員及び関係機関の職員等（それぞれ再任用職員、任期付職員、非常勤職員、会計年度任用職員、臨時職員を含む）の総称をいう。

(16) 業務委託者

契約に基づいて立科町の機関で作業する職務委託先社員及び業務委託事業者の総称をいう。

(17) 部外者

職員等及び業務委託者以外の立科町の情報資産に接することが認められていない者の総称をいう。

(18) 情報セキュリティポリシー

立科町情報セキュリティ基本要綱、情報セキュリティ対策基準及び情報セキュリティ実施手順を総称する。

(19) 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。

(20) 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。

(21) 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及びその情報システムで取り扱うデータをいう。

(22) 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。

(23) 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。

(24) 教育系

地方公共団体が設置する学校の管理運営に係る事務を担う執行機関もしくは学校が所掌するネットワーク、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。

(情報セキュリティポリシーの位置付け)

第３条　情報セキュリティポリシーは、立科町が掌握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り、情報セキュリティ対策の具体的考え方及び運用方法を示すものである。

(適用範囲)

第４条　本要綱の適用範囲は、次の各号に定めるものとする。

（１）情報資産の範囲

本要綱が対象とする情報資産は、次のとおり。

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図等のシステム関連文書

（２）行政機関の範囲

本要綱が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

(職員等の遵守義務)

第５条　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もつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

(情報セキュリティ組織体制)

第６条　立科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及び管理するための全庁的な組織体制を確立するものとする。

(情報資産の分類)

第７条　立科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、その分類に基づき情報セキュリティ対策を行うものとする。

(情報資産への脅威)

第８条　情報セキュリティポリシーを策定する上で、発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（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

（情報セキュリティ対策）

第９条　立科町の情報資産を前条に示した脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策

情報資産を扱う職員等の情報セキュリティに関する権限や責任等を定めるとともに、職員等及び業務委託者に情報セキュリティポリシーの内容を周知徹底し、教育、訓練及び啓発等を実施する。

（２）物理的セキュリティ対策

部外者等の情報システム設置場所への不正な立入りによる破壊若しくは盗難並びに地震等の災害から、情報システム及び情報資産を保護するために物理的な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理及びコンピュータウィルス対策等を実施する。

（４）情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

ア　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。

イ　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。

ウ　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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（５）運用

情報セキュリティポリシーの実効性を確保し、不正なアクセス等から適切に保護するため、システム開発等の業務委託、システムの管理、ネットワークの監視及び情報セキュリティポリシー遵守状況の確認等の運用面における必要な措置を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

（６）業務委託と外部サービスの利用

ア　業務委託する場合には、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。

イ　外部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。

ウ　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。

（情報セキュリティ対策基準の策定）

第 10 条　立科町の様々な情報資産について、前条の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき行為及び判断等の基準を統一的に定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。なお、情報セキュリティ対策基準は、公にすることにより立科町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

（情報セキュリティ実施手順の策定）

第 11 条　情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要があることから、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、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立科町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

（情報セキュリティ監査及び自己点検の実施）

第 12 条　情報セキュリティポリシーが遵守されていることを検証するため、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。

（評価及び見直しの実施）

第 13 条　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

附　　則

この要綱は、平成 15 年 11 月 1 日から施行する。

附　　則

（施行日）

この要綱は、令和 2 年 3 月 31 日から施行する。

附　　則

（施行日）

この要綱は、令和 6 年 2 月 1 日から施行する。

附　　則

（施行日）

この要綱は、令和８年３月 31 日から施行する。