草津町情報セキュリティポリシー

草津町

令和８年２月

序章　草津町情報セキュリティポリシーの構成について

草津町情報セキュリティポリシー（以下：情報セキュリティポリシー）とは、草津町が所掌する情報資産に関する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を総称する。情報セキュリティポリシーは、草津町が所掌する情報資産に関する業務に携わる全職員（再任用職員・会計年度任用職員を含む。）（以下、「職員等」という。）及び外部委託事業者に普及、定着をさせるものであり、安定的な規範であることが要請される。しかしながら一方で、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも求められている。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

①情報セキュリティ基本方針

②情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。

なお、情報セキュリティポリシーに基づき、具体的な実施手順として「情報セキュリティ実施手順」を別に策定することとする。（下表参照）

※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は、公にすることにより草津町の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

情報セキュリティポリシーの構成

文書名		内容
草津町情報セキュリティポリシー	①情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	②情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すためのネットワーク及び情報システムに関する情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

１．目的

草津町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報等、外部への漏洩等が発生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いる。

これらの情報資産や情報資産を取り扱うネットワーク及び情報システム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、このことが草津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。

各種手続オンライン利用の本格化や情報システムの高度化等、自治体 DX の推進を図るに当たり、住民生活等に重大な支障が生じないよう、各種ネットワーク及び情報システムが確実な安全性を有することが不可欠な前提条件である。

本基本方針は、草津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、草津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とともに、総務省が策定した「地方公共団体におけるサイバーセキュリティを確保するための方針又は変更に関する指針」を踏まえて、草津町情報セキュリティを確保するための方針として定めるものである。

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）情報資産

ネットワーク及び情報システムの開発、運用及び管理等に係る全ての情報（アクセス記録、文書・図書等の電磁的記録及び紙等の有機体に出力された記録等)並びに構成機器をいう。

（４）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。

（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）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。

（１０）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。)。

（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、Ｗｅｂ会議システム、その他自治体ＤＸの推進に不可欠な事業に関わるインターネットに接続されたシステム及びそれら情報システムで取り扱うデータをいう。

（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。

（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添付ファイルのダウンロード及び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。

（１４）自治体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。

（１５）委託事業者

草津町よりネットワーク、情報システム及び情報資産に関する業務について委託される全ての事業者をいう。

（１６）外部

情報セキュリティポリシーの適用範囲以外のネットワーク、情報システム、又は職員以外の者をいう。

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、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、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、草津町情報公開条例（平成 18 年条例第 4 号）第 2 条第 1 項に規定する機関及び地方公営企業の管理者（草津町の情報システムを利用する部署に限る。）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

５．職員等の遵守義務

（１）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。

（２）職員等は、委託事業者に対し、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、契約等により遵守する義務を負わせなければならない。

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

草津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

草津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実施する。

（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、他の領域との通信ができない環境下で、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、両システム間でデータの共有を行う場合には、無害化されたデータのみとする。また、LGWAN 接続系の端末は職員用職責証明カード（※以下：IC カード）の利用と個人用パスワードの設定により、職員等以外が利用できない環境を講じる。

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、群馬県及び県内市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を利用する。

（４）物理的セキュリティ

サーバ、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

資産管理システムやウイルス対策ソフトの導入に加えて、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、承認デバイスの制御等の技術的対策を講じる。

（７）運用

ネットワーク及び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）業務委託とクラウドサービスの利用

情報ネットワークに関連する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することとし、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（共同調達を含む）には、利用に係るセキュリティ対策を講じる。ソーシャルネットワークサービスを利用する場合には、ソーシャルネットワークサービスの運用手順を定め、ソーシャルネットワーク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ネットワーク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

情報セキュリティの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は、保有する情報及び利用する情報システムに係る驚異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及び情報セキュリティ実施手順を見直す。

9．情報セキュリティ対策基準の策定

上記 6 から 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

ネットワーク及び情報システムを保有する者は、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し、必ず緊急時対応計画を明記するものとする。

また、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は、公にすることにより草津町の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。