土　庄　町
情報セキュリティポリシー

［ 平成 15 年 8 月 1 日 策定 ］
［ 平成 17 年 4 月 1 日 改定 ］
［ 平成 19 年 4 月 1 日 改定 ］
［ 平成 30 年 10 月 29 日 改定 ］
［ 令和　8 年 3 月 31 日 改定 ］

土庄町情報セキュリティ基本方針

目次

1　目的

土庄町（以下「町」という。）では、保有する情報資産の保護や、情報システムの安全性を常に確保するための情報セキュリティ対策を実施するとともに、住民サービスの向上や行政事務の効率化・高度化を図るための情報化施策に取り組んでいる。

近年の情報システムの高度化や電子自治体の進展の反面、個人情報の漏えいや、システム障害による業務停止をはじめとした、情報セキュリティを侵害する様々な問題も発生し続けている。また、不正アクセスや、コンピュータウイルス等の脅威は多様化、高度化しており、これらに対する情報セキュリティ対策も一層の強化、拡充が急務である。

ついては、情報資産の保護や、情報システムの安全性、信頼性の確保のため、情報セキュリティ対策の基本的な事項を定めるものである。

2　情報セキュリティポリシーの構成と位置づけ

情報セキュリティポリシーは、町が保有する情報資産の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、情報セキュリティに対する取組姿勢を示す「情報セキュリティ基本方針」と、この情報セキュリティ基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示す「情報セキュリティ対策基準」をもって構成する。

3　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

情報システム及びネットワークで取り扱われる全ての情報（電磁的に記録されている情報及び出力した媒体を含む。）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

土庄町情報セキュリティ基本方針及び土庄町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） サーバ等

ネットワーク上で行政情報を処理し、端末機に提供するコンピュータ（ホストコンピュータを含む。）をいう。

（１０） 端末機

ネットワークを通じてサーバに接続されたパソコンをいう。

（１１） 記録媒体

情報システムでデータ等を記録するためのハードディスク、フロッピーディスク、ＵＳＢメモリ等の媒体（メディア）をいう。

（１２） 無線ＬＡＮ

電波等を利用して無線でデータの送受信を行う構内情報通信網をいう。

（１３） 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。

（１４） 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。）

（１５） インターネット接続系

インターネットメール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。

（１６） 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。

（１７） 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。

４ 情報資産への脅威

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、火災及び水害等の災害並びに事故、故障等によるサービス及び業務の停止等

（４） 電力供給の途絶、通信の途絶等のインフラの障害からの波及等

（５） 大規模かつ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 適用範囲

（１） 行政機関の適用範囲

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、消防本部及び地方公営企業とする。

（２） 情報資産の適用範囲

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、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情報システム関連文書

６ 職員等の遵守義務

職員、嘱託職員及び会計年度任用職員等（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関連法令及び情報セキュリティポリシーを遵守しなければならない。

７ 情報セキュリティ対策

上記４の脅威から情報資産及び情報システムを保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

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を導入する。
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、県と市町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。

（３） 物理的セキュリティ

情報システムを設置する施設への立入り、通信回線等及び職員等のパソコン等の管理について、施設整備等の物理的な対策を講じる。

（4） 人的セキュリティ

情報セキュリティに関する権限及び責任や職員等が遵守すべき事項を定めるとともに、職員等に十分な教育及び啓発を行う等の人的な対策を講じる。

（5） 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な対策を講じる。

（6） 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情報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。

（7） 情報資産の分類及び管理

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。

（8） 業務委託と外部サービス（クラウドサービス等）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。

（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。

8　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。

9　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、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。

１０　情報セキュリティ対策基準の策定

上記７、８及び９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。

１１　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。