綾町情報セキュリティポリシー

第 2.1 版

綾町

令和８年３月１９日策定

序章　綾町情報セキュリティポリシーの構成

綾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、本町が管理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を総称する。情報セキュリティポリシーは、本町が管理する情報資産に関する業務に携わる全ての職員・非常勤職員・臨時職員（以下、「職員等」）および外部委託事業者や公の施設の指定管理者（以下、「委託事業者等」）に浸透・普及・定着させるものであり、安定的な規範である必要がある。

しかしながら一方では、技術の進歩などに伴う情報セキュリティを取り巻く状況の急速な変化に柔軟に対応することも必要である。

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する。

具体的には、セキュリティポリシーを以下の２階層に分け、それぞれを策定する。

・情報セキュリティ基本方針

・情報セキュリティ対策基準

また、情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順を、情報セキュリティ実施手順として別途策定することとする。

表．綾町情報セキュリティポリシーの構成

文書名		内容
綾町情報セキュリティポリシー	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。
	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すべてのネットワークと情報システムに共通の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		情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順。

第１章　情報セキュリティ基本方針

１　目的

本町の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など、外部への漏洩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。

したがって、情報資産とその情報資産を取り扱うネットワークや情報システムをさまざまな脅威から防御することは、町民の財産やプライバシーを守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、本町の行政に対する町民からの信頼の維持向上に寄与することとなる。

また、今後更なる電子自治体の構築を推進していくためには、全てのネットワークと情報システムが高度な安全性を有することが必要不可欠な前提条件となる。

そのため本町では情報資産の機密性、安全性、可用性（※）を維持するための対策（情報セキュリティ対策）を整備するために、情報セキュリティポリシーを定める。このうち、情報セキュリティ基本方針においては、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として、情報セキュリティポリシーの対象や位置付けを定める。

※：国際標準化機構（ISO）が定めるもの

機密性（confidentiality）	：認可された者だけが情報にアクセスできることを確実にすること
完全性（integrity）	：情報とその処理方法が正確かつ完全である状態を安全防護すること
可用性（availability）	：許可された利用者が必要な時に情報にアクセスできることを確実にすること

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通信網、その構成機器（ハードウェア・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

ネットワークや情報システムの開発・運用に係るすべての情報、ネットワークや情報システムで取り扱うすべての情報をいう。なお、情報資産には紙などの有体物に出力された情報も含まれる。

（４）情報セキュリティ

情報資産の機密を保持し、正確性と完全性を維持するとともに、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。

（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（個人番号利用事務系、基幹系）

個人番号利用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

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。

（１０）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。

（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感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マクロの除去、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進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範違反、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、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、町長部局、行政委員会、議会事務局、教育委員会及び地方公営企業とする。

（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

5　職員等の遵守義務

セキュリティポリシーは、本町が管理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頂点に位置するものである。

したがって、本町長をはじめとする本町の情報資産に関する業務に携わる職員等および委託事業者等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たってセキュリティポリシーを遵守する義務を負う。

6　情報セキュリティ対策

上記3で示した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実施する。

（3）情報システム全体の強靱性の向上

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。
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。高度なセキュリティ対策として、都道府県及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。

（4）物理的セキュリティ

電算室、サーバ・通信回線等及び職員等の汎用パソコンの管理について、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、十分な教育と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、業務委託を行う際のセキュリティ確保等、運用面の対策を講じる。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）業務委託と外部サービスの利用

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。

外部サービスを利用する場合には、利用にかかる規程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程し、利用するソーシャルメディアサービス毎の責任者を定める。

（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。

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が遵守されていることを検証するため、必要の都度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となった場合には、情報セキュリティポリシーの見直しを行う。

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。

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に、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。