取扱注意

幸田町情報セキュリティポリシー

令和８年４月１日　６．０版

愛知県幸田町

改版履歴

版　数	作成日
初　版	平成１５年　７月１７日
第２版	平成１９年　４月　１日
第３版	平成２７年１２月　１日
第４版	令和　４年　４月　１日
第５版	令和　６年　５月　１日
第６版	令和　８年　４月　１日

《目　　次》

序　情報セキュリティポリシーの構成

「情報セキュリティポリシー」とは、幸田町が所掌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、幸田町が所掌する情報資産に関する業務に携わる職員（町のすべての職員をいう。以下同じ。）及び外部委託事業者に浸透、普及及び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は、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ものとする。

また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　　容
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をいう。
	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全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準をいう。
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毎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をいう。

第1章 情報セキュリティ基本方針

1 目的

情報セキュリティ基本方針（以下「基本方針」という。）は、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、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。

なお、本基本方針については、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

2 定義

次の各号に掲げる用語の意義は、それぞれ当該各号に定めるとおりとする。

⑴ **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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵ **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及び情報処理を行う仕組みをいう。

⑶ **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。

⑷ **情報セキュリティポリシー** 基本方針及び情報セキュリティ対策基準をいう。

⑸ **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。

⑹ **完全性** 情報が破壊し、改ざんし、又は消去されていない状態を確保することをいう。

⑺ **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。

⑻ **マイナンバー利用事務系（いわゆる「個人番号利用事務系」をいう。）** 個人番号利用事務（社会保障、地方税、防災、その他の個人番号を利用する事務に関する事務）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。

⑼ **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。）。

⑽ **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。

⑾ **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。

⑿ **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。

3 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

⑴ 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、改ざん又は消去、重要情報の詐取、内部不正等

⑵ 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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は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、破壊又は消去等

⑶ 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

⑷ 大規模又は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

⑸ 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

⑴ **行政機関の範囲** 基本方針が適用される行政機関は、町長部局、各行政委員会、幸田町農業委員会、議会事務局、議会、消防本部及び地方公営企業とし、各教育機関（事務室及び職員室を除く。）は対象外とする。この場合において、各教育機関における教育のために用いるネットワーク、システム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

⑵ **情報資産の範囲** 基本方針が対象とする情報資産は、次のとおりとする。

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

5 職員の遵守義務

職員は、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。

6 情報セキュリティ対策

３の各号に掲げる脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

⑴　**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。

⑵　**情報資産の分類と管理**　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行う。

⑶　**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３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。この場合において、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。この場合において、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。

⑷　**物理的セキュリティ**　サーバ、情報システム室、通信回線及び職員のパソコン等の管理について物理的な対策を講じる。

⑸　**人的セキュリティ**　情報セキュリティに関し、職員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。

⑹　**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。

⑺　**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。この場合において、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、必要に応じ、インシデント対応フローの見直しを行う。

⑻　**外部サービスの利用**　外部委託をする場合には、外部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、外部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。

⑼ **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、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

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。この場合において、情報セキュリティ実施手順は、公にすることにより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。