制定：平成１５年　７月２２日
改定：令和　６年　８月　１日
版数：第１．４版

取 扱 注 意

情報セキュリティポリシー

【基本方針】

瀬 戸 市

＜　改定履歴　＞

版　数	発行(改定)年月日	改定内容
第1.0版	H15/7/22	初版
第1.1版	H28/4/1	第2版
第1.2版	R03/8/1	第3版
第1.3版	R05/8/4	第4版
第1.4版	R06/8/1	第5版

※版数は新規制定を第1.0版とし、改定が発生した場合は第1.1版とする。
※改定があった場合は、必ず改定内容を記載すること。

目　次

序章　瀬戸市情報セキュリティポリシーの構成

瀬戸市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、本市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、本市が所掌する情報資産に関する業務に携わる全職員、非常勤職員（以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、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）で構成した。

（構成）

情報 セキュリティ ポリシー	第１章 情報セキュリティ 基本方針	情報セキュリティに関する統一的かつ基本的な方針
	第２章 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

第１章　情報セキュリティ基本方針

1.1　目的

本基本方針は、本市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、本市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。

1.2　定義

情報セキュリティ基本方針における用語については、次のとおり定義する。

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、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され、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

本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、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。

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（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。

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。

⒀ ソーシャルメディアサービス

インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

⒁ デジタルフォレンジック

電子データを調査分析することで事実解明及び証拠保存を行うための技術をいう。

⒂ IoT機器

「Internet of Things」の略で、あらゆるモノがインターネットを介してつながり情報をやりとりし相互に制御を行う機器のことをいう。

⒃ Web会議

インターネット環境とパソコンやスマートフォンといったデバイスを利用して遠隔地の拠点とつなぎ、両者がリアルタイムで会議や打ち合わせなどを行える仕組みをいう。

⒄ 仮想マシン

ソフトウェアにより疑似的に再現されたコンピュータをいう。

⒅ SaaS

「Software as a Service」の略称で、提供者であるサーバ側で稼働するソフトウェアをインターネットなどを経由させることで、利用者であるクライアント側で必要な機能や分量のみを選択して利用できるサービスをいう。

⒆ IaaS

「Infrastructure as a Service」の略称で、情報システムの構築に必要なサーバや各種機材、ネットワークなどのインフラ環境をインターネット上で提供するサービスをいう。

1.3 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。

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・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・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、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・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・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

1.4 適用範囲

⑴ 行政機関の範囲

本基本方針が適用される行政機関は、次のとおりとする。

①瀬戸市行政組織規則（平成１７年瀬戸市規則第３９号）の規定に基づき設置される組織

②瀬戸市事務分掌条例施行規則（平成１８年瀬戸市規則第８号）の規定に基づき設置されるプロジェクトチーム

③瀬戸市会計管理者の補助組織設置規則（昭和４９年瀬戸市規則第１０号）の規定に基づき設置される組織

④瀬戸市教育委員会事務局組織規則（平成１７年瀬戸市教育委員会規則第６号）の規定に基づき設置される組織

⑤瀬戸市立図書館条例（昭和４５年瀬戸市条例第１９号）の規定に基づき設置される組織

⑥瀬戸市水道事業の組織及び処務に関する規程（平成１８年瀬戸市水道事業管理規程第１号）の規定に基づき設置される組織

⑦瀬戸市消防本部組織規則（平成１８年瀬戸市規則第３号）の規定に基づき設置される組織

⑧瀬戸市消防署組織規程（昭和６１年瀬戸市消防本部告示第１号）の規定に基づき設置される組織

⑨瀬戸市議会事務局条例（昭和５４年瀬戸市条例第１６号）の規定に基づき設置される組織

⑩瀬戸市監査委員事務局運営規程（昭和６０年瀬戸市監査委員告示第１号）の規定に基づき設置される組織

⑪その他前各号の規定に基づき設置される組織に準ずる組織のうち市長が認める組織

⑵ 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（全ての文書を含む。）

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

1.5 職員等の遵守義務

職員及び非常勤職員（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。

1.6 情報セキュリティ対策

上記1.3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。

⑴ 組織体制

本市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

本市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、住民情報の流出を防ぐため、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等を実施する。

②LGWAN 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、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。

⑷ 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等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。

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、情報セキュリティポリシーの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正に対応するため、緊急時対応計画を策定する。

⑻ 外部委託と外部サービス（クラウドサービス）の利用

外部委託を行う場合には、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（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。

1.7 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。

1.8 情報セキュリティポリシーの見直し

情報セキュリティポリシーは、情報セキュリティ監査及び自己点検の結果により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、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、見直しを行う。

1.9 情報セキュリティ対策基準の策定

上記1.6、1.7及び1.8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。

1.10 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。

なお、情報セキュリティ対策基準及び実施手順は、公にすることにより本市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。

以上