瀬戸内市情報セキュリティポリシー

＜　目　次　＞

序　瀬戸内市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、瀬戸内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し、情報資産に関する業務に携わる全職員、非常勤及び臨時職員（以下、「職員等」という。）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）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及び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。又、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	備考
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	公開
	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情報システムに共通の情報セキュリティ対策の基準	非公開
情報セキュリティ実施手順		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	非公開

瀬戸内市情報セキュリティ基本方針

１　目的

瀬戸内市の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、部外に漏洩等した場合にはきわ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、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、又、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが瀬戸内市に対する住民からの信頼の維持向上に寄与するものである。

又、近年のいわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の実現が期待されているところである。瀬戸内市がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、瀬戸内市の情報資産の機密性、完全性及び可用性（注）を維持するための対策（情報セキュリティ対策）を整備するために瀬戸内市情報セキュリティポリシーを定めることとし、この内、情報セキュリティ基本方針については、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ＩＳＯ）が定めるもの（ＩＳＯ7498-2：1989）

機密性 (confidentiality)	情報にアクセスすることが認可された者だけがアクセスできることを確実にすること
完全性 (integrity)	情報及び処理の方法の正確さ及び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ときに情報にアクセスできることを確実にすること

２　用語の定義

（１）ネットワーク

瀬戸内市における内部部局、各行政委員会、議会事務局及び各教育機関（事務室及び職員室のみ）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）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）情報資産

市の業務に用いるデータ、データを記録する媒体、表示する媒体、ソフトウェア、及びハードウェアをいう。

（３）情報システム

情報資産を利用するための仕組みを総称していう。

（４）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並び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。

３　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、瀬戸内市が所掌する情報資産に関する業務について、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、瀬戸内市長をはじめとして瀬戸内市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、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あたって情報セキュリティポリシーを遵守する義務を負うものとする。

４　情報セキュリティ管理体制

瀬戸内市の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

６　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産の脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等

（２）職員等及び外部委託事業者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

（３）地震、落雷、火災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

７　情報セキュリティ対策

上記６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ずるものとする。

（１）物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（２）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

（４）運用

システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。又、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

８　情報セキュリティ対策基準の策定

瀬戸内市の様々な情報資産について、上記７の情報セキュリティ対策を講ずるにあたっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行ううえで必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９　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を遵守し、情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。

そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、内部部局の長などが所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシー及び情報セキュリティ実施手順は、公にするこ

とにより瀬戸内市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

10　情報セキュリティ監査の実施

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、定期的に監査を実施する。

11　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。