みどり市情報セキュリティポリシー

みどり市情報セキュリティ基本方針

（第 4.0 版）

みどり市

◇策定・改定履歴

版数	策定・改定年月日	内容
第 1.0 版	平成 19 年 4 月 1 日	策定（最高情報統括責任者承認）
第 2.0 版	平成 23 年 1 月 17 日	全部改定
第 3.0 版	令和 5 年 2 月 15 日	一部改定
第 4.0 版	令和 8 年 3 月 26 日	一部改定

目　次

1　目的

みどり市が取り扱う情報には、市民の個人情報をはじめ行政運営上重要な情報など、外部に漏えい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。

これらの本市が所管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の基本的な方針を定めることを目的とする。

2　用語の定義

(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

次の各号を情報資産という。

①ネットワーク、情報システム、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

(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) 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）

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。

(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（マイナンバー利用事務系を除く。）。

(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。

（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　みどり市情報セキュリティポリシーの構成

みどり市情報セキュリティポリシーは、本市が所管する情報資産に関する情報セキュリティ対策を総合的かつ体系的に取りまとめたものであり、みどり市情報セキュリティ基本方針及びみどり市情報セキュリティ対策基準により構成する。

また、みどり市情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策の実施手順を示す情報セキュリティ実施手順を策定するものとする。

みどり市情報セキュリティポリシーの構成

文　書　名		内　　容
みどり市情報セキュリティポリシー	みどり市情報セキュリティ基本方針	みどり市が所管する情報資産に関する情報セキュリティ対策の統一的かつ基本的な方針。
	みどり市情報セキュリティ対策基準	みどり市情報セキュリティ基本方針に基づき、情報セキュリティ対策を統一的に実施するために本市の職員が遵守すべき行為及び判断等の基準。
情報セキュリティ実施手順		みどり市情報セキュリティポリシーに基づき、本市の職員が遵守すべき情報セキュリティ対策の実施手順を具体的に規定するもの。全庁的に共通する情報資産の取り扱いを定める実施手順と情報システムごとに取り扱いを定める実施手順を策定する。

4　対象とする脅威

本市は情報資産に対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サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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提供サービスの障害からの波及等

5　適用範囲

みどり市情報セキュリティポリシーの適用範囲を以下の各号に示す。

（1）適用組織

市長部局、議会、教育委員会、選挙管理委員会、公平委員会、監査委員及び監査委員事務局、農業委員会及び固定資産評価審査委員会とする。

（2）適用情報資産

本市が所管する情報資産とする。ただし、市立小・中学校における教育情報は除く。

（3）適用対象者

適用情報資産に接する本市の職員（非常勤職員及び会計年度任用職員等を含む。以下「職員等」という。）及び議員並びに委員とする。

（4）情報資産の範囲

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（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

6　職員等及び議員並びに委員の遵守義務

①職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たり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。

②職員等は、委託業者に対し、契約等によりみどり市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する義務を負わせなければならない。

③議会を構成する議員及び各委員会の委員は、情報セキュリティの重要性について共通の認識を持ち、議会及び各委員会の管理する情報システムの利用に際しては、情報システムを管理する職員等の指示に従わなければならない。

7　情報セキュリティ対策

上記４の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

（1）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。

（2）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実施する。

(3) 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、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。

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、県及び市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を利用する。

(4) 物理的セキュリティ

情報システムの設置場所、情報資産の保管場所等への不正な立入り、情報資産の損傷及び利用の妨害等から保護するための物理的な対策を講じる。

(5) 人的セキュリティ

職員等の情報セキュリティに関する権限や責任等を定めるとともに、職員等が遵守すべき事項を周知徹底するため、教育及び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、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、情報資産への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（クラウドサービス）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（クラウドサービス）を利用する場合には、利用にかか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に新たな対策が必要になった場合は、情報セキュリティポリシーの見直しを実施する。

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、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。

なお、情報セキュリティ対策基準は、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。

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。