雲仙市情報セキュリティ基本方針

平成２７年１２月２８日制定
令和２年４月１日改正
令和５年４月１日改正
令和８年３月３０日改正

（目的）

第１条　この訓令は、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、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。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（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。

（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。

（４）　情報セキュリティポリシー　この訓令及び雲仙市情報セキュリティ対策基準（平成２７年雲仙市訓令第１７号）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、改ざん又は消去を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　地方公共団体の組織内ネットワークを相互に接続し、情報の高度利用等を行うためのネットワークをいう。

（１０）　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。ただし、マイナンバー利用事務系を除く。

（１１）　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。

（１２）　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。

（１３）　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。

（対象とする脅威）

第３条　市は、情報資産に対する脅威として、次に掲げる事項を想定し、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、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、改ざん若しくは消去又は重要情報の詐取、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、設計及び開発の不備、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、破壊又は消去等

（３）　地震、落雷、火災等の災害によるサービス又は業務の停止等

（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

（適用範囲）

第４条　この訓令の適用を受ける実施機関は、市長、議会、教育委員会、農業委員会、選挙管理委員会、監査委員、固定資産評価審査委員会及び地方公営企業（以下「市の機関」という。）とする。

２　この訓令の適用を受ける情報資産の範囲は、次に掲げるとおりとする。

（１）　ネットワーク、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（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

（職員等の遵守義務）

第５条　市の機関に属する職員、会計年度任用職員及び非常勤職員等市の情報資産を取り扱う者（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を遵守しなければならない。

（情報セキュリティ対策）

第６条　市の機関は、第３条各号に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じる。

（１）　市の機関が取り扱う情報資産について、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こと。

（２）　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こと。

（３）　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する次の３段階の対策を講じること。

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止すること。

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の分割。この場合において、両システム間で通信

する場合には、無害化通信を用いて実施するものとする。

ウ　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の分割。この場合において、両システム間で通信する場合には、無害化通信を用いて実施するものとする。

（４）　サーバ等、情報システム室等、通信回線等及び職員等の情報機器の管理について物理的な対策を講じること。

（５）　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こと。

（６）　情報機器の管理、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こと。

（７）　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の情報セキュリティポリシーの運用面の対策を講じること。

（８）　次に掲げるサービスの形態に応じた措置を行う。

ア　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こと。

イ　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こと。

ウ　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こと。

（９）　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り、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。

（情報セキュリティ監査及び自己点検の実施）

第７条　市の機関は、情報セキュリティポリシーの遵守状況を検証するため、定期的に、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。

（情報セキュリティポリシーの見直し）

第８条　市の機関は、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ものとする。

（情報セキュリティ対策基準の策定）

第９条　市の機関は、情報セキュリティに関する対策を実施するため、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。

（情報セキュリティ実施手順の策定）

第１０条　市の機関は、前条の規定により策定した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。