薩摩川内市情報セキュリティ基本方針

令和８年４月１日　初版

（目的）

第１条　この基本方針は、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、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、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。

（定義）

第２条　この基本方針において、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。

⑴　実施機関　市長（公営企業管理者の職務を行う実施機関を含む。）、消防局長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会をいう。

⑵　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並びにその構成機器であるハードウェア及びソフトウェアをいう。

⑶　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。

⑷　情報資産　次に掲げるものをいう。

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

⑸　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。

⑹　情報セキュリティポリシー　本基本方針及び第９条に規定する情報セキュリティ対策基準をいう。

⑺　機密性　情報にアクセスすることを認められた者に限り、情報にアクセスできる状態を確保することをいう。

⑻　完全性　情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

⑼　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。

⑽　マイナンバー利用事務系　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）又は戸籍事務等に係る情報システム及び当該情報システムで取り扱うデータをいう。

⑾　ＬＧＷＡＮ接続系　ＬＧＷＡＮに接続された情報システム及び当該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。）。

⑿　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係るインターネットに接続された情報システム及び当該情報システムで取り扱うデータをいう。

⑬　通信経路の分割　ＬＧＷＡＮ接続系及び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のみを許可できるようにすることをいう。

⑭　無害化通信　インターネットメール本文のテキスト化、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ない等の安全が確保された通信をいう。

⑮　外部サービス 自組織以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス、Ｗｅｂ会議サービス、ソーシャルネットワーキングサービス、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。

（対象とする脅威）

第３条　情報資産に対する脅威は、次に掲げる脅威を想定する。

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、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、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、操作又は設定の誤り、メンテナンス不備、内部又は外部監査機能の不備、外部委託による管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい、破壊、改ざん、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　大規模かつ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

（適用範囲）

第４条　この基本方針は、実施機関及び実施機関が所管する情報資産に適用する。

（職員等の遵守義務）

第５条　実施機関の職員、非常勤職員等（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。

（情報セキュリティ対策）

第６条　実施機関は、第３条に規定する脅威から情報資産を保護するため、次の各号に掲げる区分に応じ、当該各号に定める情報セキュリティ対策を講ずるものとする。

⑴　組織体制　次に掲げる対策を講ずる。

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ため、全庁的な組織体制を確立する。

⑵　情報資産の分類及び管理　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講ずる。

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、業務の効率性及び利便性の観点から、情報システム全体に対し、次に掲げる対策を講ずる。

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。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。

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。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、サーバ室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

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ずる。

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ずる。

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、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ずるものとする。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　外部サービスの利用　次のアからウまでに掲げる対策を講ずる。

ア　外部委託する場合には、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ずる。

イ　約款によ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ずる。

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。

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、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　実施機関は、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　実施機関は、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な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な場合には、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、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　実施機関は、第６条から前条までの規定を実施するために、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ものとする。

（情報セキュリティ実施手順の策定）

第１０条　実施機関は、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。

（非公開）

第１１条　情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより実施機関の運営に重大な支障を及ぼす恐れのある情報資産であることから、非公開とする。

附　則

（施行期日）

１　この基本方針は、令和８年４月１日から施行する。