第２章　情報セキュリティ基本方針

１　総則

市の情報システムが取り扱う情報には、市民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、市民の財産やプライバシー等を守るためにも、また継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため、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ことを目的として、留萌市情報セキュリティ基本方針（以下「基本方針」という。）を定める。

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）　情報資産

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、パンチカードその他の電磁的記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（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）　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。

（６）　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。

（７）　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。

（８）　可用性

情報にアクセスすることを認められた者だけが、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。

（９）　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。

(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（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。

(14)　職員等

留萌市に在職する正職員及び会計年度任用職員をいう。

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。

（１）　不正アクセス、ウイルス攻撃及び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

（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の流行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

４　適用範囲

（１）　組織の範囲

留萌市事務分掌条例（平成２４年条例第１号）第１条に規定する部、会計管理者の補助組織、行政委員会、議会事務局及び公営企業並びに消防本部とし、市立小中学校（事務室を除く）の教育のために用いるネットワーク及びシステム等は対象外とする。

（２）　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。

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

５　職員等の責務

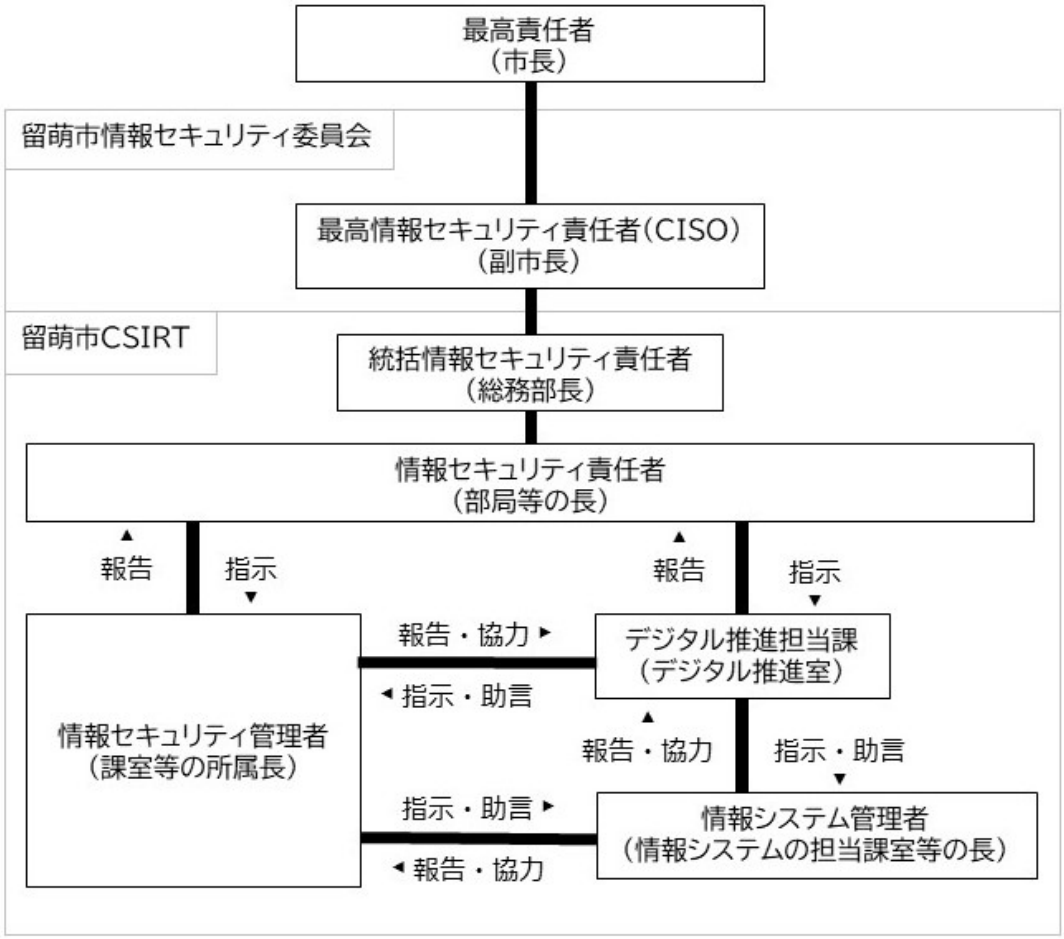
職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたっては情報セキュリティポリシーを遵守するものとする。

６　情報セキュリティ対策

脅威から情報資産を保護するため、次の情報セキュリティ対策を講じる。

（１）　組織体制

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。



留萌市情報セキュリティ組織図

（２）　情報資産の分類と管理

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

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る対策を実施する。

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、自治体情報セキュリティクラウドの導入等を実施する。

（４）　物理的セキュリティ

サーバ、サーバ等を設置する部屋、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。

（５）　人的セキュリティ

情報セキュリティに関し、職員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。

（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な対策を講じる。

（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、緊急時対応手順を策定する。

（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する等対策を講じる。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る等、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。

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。

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、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の見直しを行う。

９　情報セキュリティ対策基準の策定

上記６、７及び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。

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。情報セキュリティ実施手順は、公にすることにより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。

第３章　情報セキュリティ対策基準

１　総則

本対策基準は、留萌市情報セキュリティ基本方針を実行に移すための、市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

２　情報セキュリティ管理体制

（１）　組織体制

適切に情報セキュリティ対策を推進・管理するため、次の者を置く。

ア　最高情報セキュリティ責任者

（Chief Information Security Officer、以下「CISO」という）

副市長をCISOとする。

イ　統括情報セキュリティ責任者

総務部長を統括情報セキュリティ責任者とする。

ウ　情報セキュリティ責任者

各部局等の長を情報セキュリティ責任者とする。

エ　情報セキュリティ管理者

各課又は室等の長を情報セキュリティ管理者とする。

オ　情報システム管理者

各情報システムの担当課又は室等の長を、情報システム管理者とする。

カ　情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

キ　監査管理者

監査事務局長を、監査管理者とする。

ク　情報セキュリティ委員会

CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、デジタル推進担当課で構成され、情報セキュリティ対策に関する調整等を行うものとする。

（２）　権限と責任

留萌市情報セキュリティ基本方針及び前項で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

ア　CISO