斜里町情報セキュリティポリシー

令和５年９月（改訂版）

斜　　里　　町

目次

序　斜里町情報セキュリティポリシーの構成

斜里町情報セキュリティポリシーとは、斜里町が保有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する。情報セキュリティポリシーは、斜里町が保有する情報資産に関する業務に携わる職員、非常勤及び臨時職員（以下、「職員等」という。）並びに外部委託者に浸透、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情報セキュリティ対策の最上位に位置づけ、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。

情報セキュリティポリシーの構成

文書名		内容
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。
	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。

第１章　情報セキュリティ基本方針

１．目的

斜里町では、町民の個人情報のみならず行政運営上重要な情報など多数取り扱っており、これらの情報資産を様々な脅威から防御することは、町民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。

さらに近年、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大しており、それにより電子政府や電子自治体の実現が期待されているところであるが、斜里町がこれらに積極的な対応をするためには、斜里町が管理しているすべての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となる。

よって、基本方針は、斜里町が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性を維持するため、斜里町が行う情報セキュリティ対策の統一的かつ基本的な考え方及び方策を定め、情報資産の管理を徹底することを目的とする。

２．定義

（１）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。

（２）情報資産

情報システムで取扱う全てのデータ及び行政情報のことで、斜里町が保有している以下の資産のこと。

①情報

１）住民情報

２）企業や団体情報

３）契約書、帳票類、運用手順書等の文書・記録

４）その他重要情報

②情報システム

１）ハードウェア

２）ソフトウェア

３）ネットワーク

４）電子記憶媒体

（３）職員

職員、非常勤職員、臨時職員（以下「職員等」という。）及び本町管理下で業務を行う要員のこと。

（４）情報システム

コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みをいう。

（５）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。

（６）電子記憶媒体

行政情報の記録、管理に使用される文書、図面、写真、ファイル及び電磁的記録（電子的方式、電磁的方式、その他の人の知覚によっては認識することができない方式で作られた記録をいう。）で磁気ディスク、磁気テープ、光ディスク等の媒体をいう。

（７）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。

（８）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。

（９）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。

(10) 可用性

情報にアクセスすることを認められた者が、必要な時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。

(11) セキュリティインシデント

システム障害、機密漏えい、被災等、人為的ミスを含む情報セキュリティ事件・事故のこと。

(12) 脅威

情報資産の機密性、完全性、可用性を失わせ、損失を発生させる直接の要因のこと。

(13) 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。

(14) 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。）。

(15) 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。

(16) 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。

(17) 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．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）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、外部委託管理の不備、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、水道供給途絶等の提供サービスの障害からの波及等

４．適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、斜里町部設置条例（昭和４６年条例１２号）第１条に掲げる部、会計、教育委員会、議会、農業委員会、選挙管理委員会、監査委員会、公平委員会、国民健康保険病院、斜里郡三町終末処理事業組合、消防署とする。

（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。

①ネットワーク、情報システム及び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

５．職員等の遵守義務

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。

６．情報セキュリティ対策

上記３の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じる。

（１）組織体制

斜里町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

斜里町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行う。

（３）物理的セキュリティ

サーバ等、コンピュータ室等、通信回線等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。

（４）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、十分な教育及び技術的対策を講じる。

（５）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。

（６）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、外部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、緊急時対応計画の策定に努める。

（７）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、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。

（８）業務委託と外部サービスの利用

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。

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、情報セキュリティポリシーを見直す。

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．情報セキュリティに関する違反への対応

本ポリシー、その他の関連規定等に違反した場合は、その重大性、発生した事案の状況に応じて条例や規定等に基づき、懲戒処分等の対象とする。

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町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２章　情報セキュリティ対策基準

斜里町行政全般における情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、斜里町行政全般の情報資産に関する情報セキュリティ対策の基準である。

１．対象範囲

（１）行政機関の範囲

本対策基準が適用される行政機関は、斜里町部設置条例（昭和４６年条例１２号）第１条に掲げる部、会計、教育委員会、議会、農業委員会、選挙管理委員会、監査委員会、公平委員会、国保病院、斜里郡三町終末処理事業組合、消防とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及び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

２．組織体制

（１）最高情報セキュリティ責任者（ＣＩＳＯ）

①副町長を、最高情報セキュリティ責任者とする。最高情報セキュリティ責任者は、斜里町における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②最高情報セキュリティ責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

③最高情報セキュリティ責任者は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team 以下「CSIRT」という。）を整備し、役割を明確化する。

④最高情報セキュリティ責任者は、最高情報セキュリティ責任者を助けて斜里町における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて斜里町の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置く。

⑤最高情報セキュリティ責任者は、本対策基準に定められた自らの担務を、最高情報セキュリティ副責任者その他の本対策基準に定める責任者に担わせることができる。

（２）統括情報セキュリティ責任者

①総務部長を、最高情報セキュリティ責任者直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐しなければならない。

②統括情報セキュリティ責任者は、斜里町の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③統括情報セキュリティ責任者は、斜里町の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④統括情報セキュリティ責任者は、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及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、斜里町の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥統括情報セキュリティ責任者は、斜里町の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、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、情報システム担当者を網羅する連絡体制を整備しなければならない。

⑧統括情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。

⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告しなければならない。

（３）情報セキュリティ責任者

①各部（局）の長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

（４）情報セキュリティ管理者

①各課等の長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課等の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、その所掌する課等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（５）情報セキュリティ担当者

①各課等の係長等を、情報セキュリティ担当者とする。

②情報セキュリティ担当者は、情報セキュリティ管理者の指示等に従い、情報セキュリティ管理者が所管する課等のセキュリティ対策を講じる。

（６）情報システム管理者

①各情報システムの担当の課等の長を、当該情報システムに関する情報システム管理者とする。

②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（７）情報システム担当者

①各課等の係長等を、情報システム担当者とする。

②情報システム担当者は、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。

（８）情報セキュリティ委員会

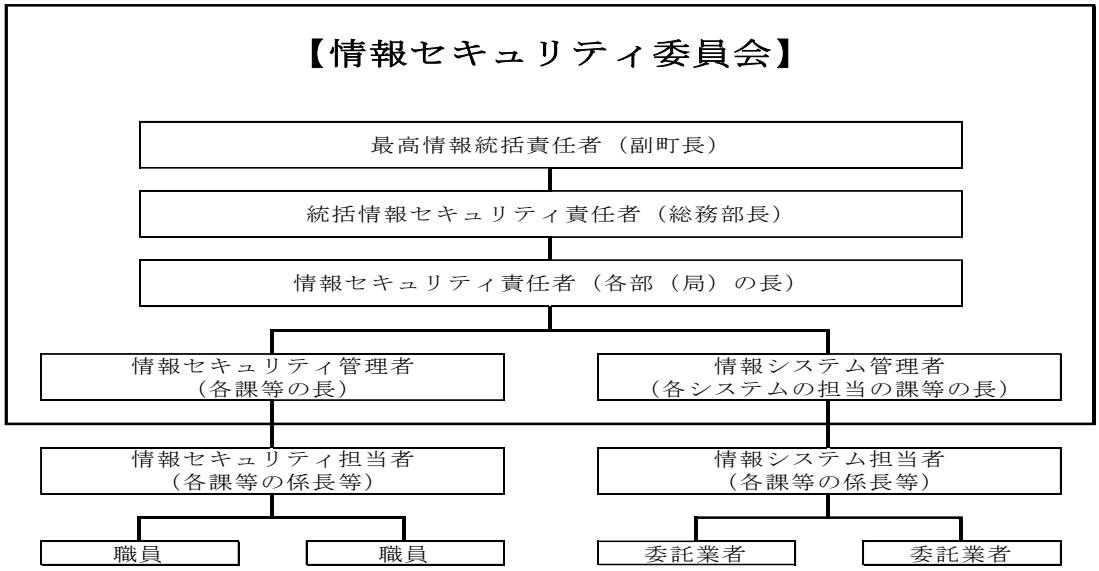
①斜里町の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

②情報セキュリティ委員会は、毎年度、斜里町における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

（9）兼務の禁止

①情報セキュリティ対策の実施においては、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。



(10) CSIRT の設置・役割

①最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化しなければならない。

②最高情報セキュリティ責任者は、CSIRT に所属する職員等を選任し、その中からCSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③最高情報セキュリティ責任者は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

⑤情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者、総務省、都道府県等へ報告しなければならない。

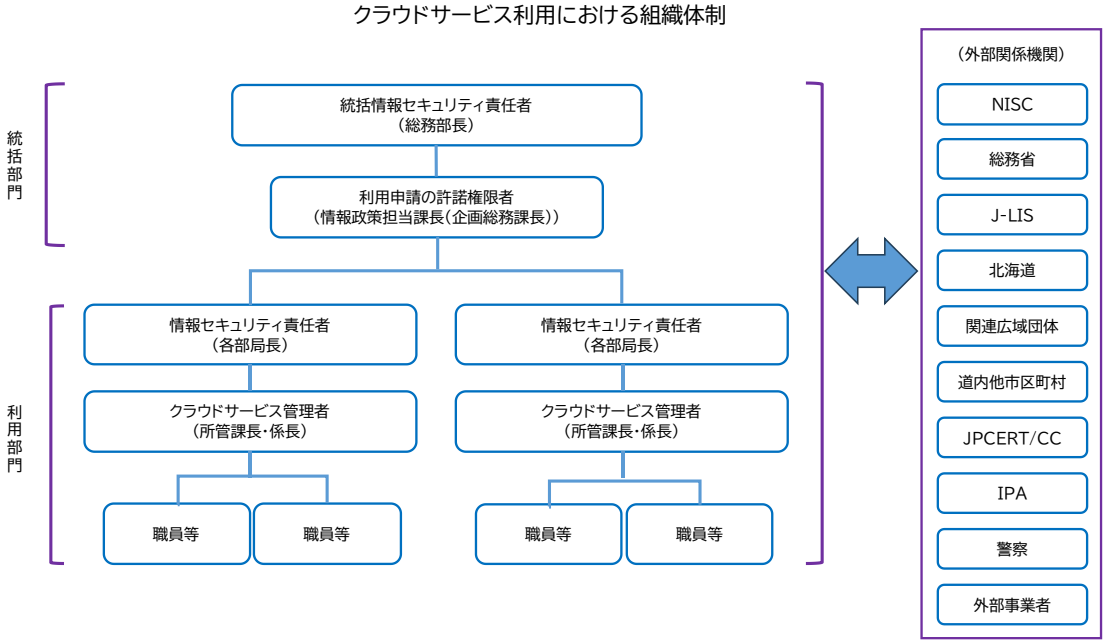
⑥情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

（11）クラウドサービス利用における組織体制

①統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

クラウドサービス利用における組織体制



※訳述
･NISC：内閣サイバーセキュリティーセンター
･J-LIS：地方公共団体情報システム機構
･JPCERT/CC：インターネットによる侵入や不正アクセスなど、
コンピューターセキュリティインシデントに対応する情報提供機関
･IPA　：独立行政法人情報処理推進機構

３．情報資産の分類と管理方法

（１）情報の分類

斜里町における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、取扱制限を行うものとする。

【機密性による情報資産の分類】

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・私物パソコンでの作業禁止 ・インターネット環境での作業禁止 ・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電子記憶媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・職場外で情報処理を行う際の安全管理措置の規定 ・電子記憶媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

※機密性：情報にアクセスすることが許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。

【安全性による情報資産の分類】

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・職場外で情報処理を行う際の安全管理措置の規定 ・電子記憶媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	―

※完全性：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。

【可用性による情報資産の分類】

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間内の復旧 ・電子記憶媒体の施錠可能な場所への保管
可用性１	可用性２情報資産以外の情報資産	―

※可用性：許可された利用者が必要な時に情報にアクセスできることを確実にすること。

（２）情報資産の管理

①管理責任

（ア） 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ） 情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

（ウ） 情報セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロバディ）、ヘッダー、フッター等）、格納する記録媒体（CD-R のラベル等）、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③情報の作成

（ア）　職員等は、業務上必要のない情報を作成してはならない。

（イ）　情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）　情報を作成する者は、作成途上の情報についても、紛失や流失等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④情報資産の入手

（ア）　庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）　庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用

（ア）　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

（ウ）　情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取扱わなければならない。

⑥情報資産の管理

（ア）　情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、保管期間を定め、情報資産を適切に保管しなければならない。但し、条例等で定められている場合は、その限りではない。

（イ）　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電子記憶媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）　情報セキュリティ管理者又は情報システム管理者は、情報資産や情報システムのバックアップデータを記録した電子記憶媒体を長期保管する場合は、災害等に十分配慮し、保管しなければならない。

（エ）　情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電子記憶媒体を保管する場合、耐火等を講じた施錠可能な場所に保管しなければならない。

⑦情報資産の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行われなければならない。

⑧情報資産の運搬

（ア） 車両等により機密性２以上の情報資産を運搬する者は、情報資産の不正利用を防止するための措置を講じなければならない。

（イ） 機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

（ア） 機密性２以上の情報資産を電子記憶媒体等により職場外に提供する者は、暗号化又はパスワード設定を行わなければならない。

（イ） 機密性２以上の情報資産を職場外に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（ウ） 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保し、不要になった情報の整理を行わなければならない。

（エ） 提供される情報の著作権等の権利は、それぞれの著作者に帰属しなければならない。

（オ） 既に著作権が別の者に帰属しているものを除き、斜里町が提供する情報全てについて斜里町は、著作権を主張するものとし、提供情報の中でそれを明示しなければならない。

⑩情報資産の廃棄

（ア） 機密性２以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化及び物理的な破壊等、情報を復元できないように処置した上で廃棄しなければならない。

（イ） 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ） 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

（エ） クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

４．情報システム全体の強靭性の向上

（１）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

②情報のアクセス及び持ち出しにおける対策

（ア） 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

（イ） 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

③マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本町の他の領域とはネットワークを分離しなければならない。

④マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

（２）LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア） インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

（イ） インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

（ウ） 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

②LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

（３）インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②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する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

③（βモデルを採用する場合）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

５．物理的セキュリティ

（１）サーバ等の管理

①機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

②サーバの冗長化

（ア） 情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、システムの運用停止時間を最小限にしなければならない。

（イ） 情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

③機器の電源

（ア） 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ） 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

④通信ケーブル等の配線

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じる。

（イ） 統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

（ウ） 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

（エ） 統括情報セキュリティ責任者、情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

⑤機器の定期保守及び修理

（ア） 情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

（イ） 情報システム管理者は、記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

⑥庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑦機器の廃棄等

（ア） 情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶媒体装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（イ） クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

（２）管理区域（電算室）の設置

①管理区域の構造等

（ア） 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。

（イ） 統括情報セキュリティ責任者及び情報システム管理者は、管理区域を独立した場所に設置し、一般事務室との共用は避け、外観は目立たないものにし、室名表示も最小限に抑えなければならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。

（ウ） 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵等によって許可されていない立入りを防止しなければならない。

（エ）　統括情報セキュリティ責任者及び情報システム管理者は、電算室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

（オ）　統括情報セキュリティ責任者及び情報システム管理者は、電算室内に、適切な温湿度条件を確保するために、専用空調を設置しなければならない。

（カ）　統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体に影響を与えないようにしなければならない。

（キ）　機器周辺では、飲食をしてはならない。

②管理区域の入退室管理等

（ア）　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード等による入退室管理を行う。

（イ）　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（ウ）　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

（エ）　情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

③機器等の搬入出

（ア）　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

（イ）　情報システム管理者は、電算室の機器等の搬入出について、職員を立ち会わせなければならない。

（３）通信回線及び通信回線装置の管理

①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関する文書を適切に保管しなければならない。

②統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最小限に限定し、できる限り接続ポイントを減らさなければならない。

③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（ＬGWAN）に集約するように努めなければならない。

④統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑤統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（４）職員等のパソコン等の管理

①情報システム管理者は、執務室等のパソコン等の端末について、盗難防止のための措置を講じなければならない。

②情報システム管理者は、パソコン等の端末を追加・変更・廃棄、及び庁内ネットワークに接続する場合は、情報システム主管課長と協議しなければならない。

③情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

６．人的セキュリティ

（１）職員等の遵守事項

①職員等の遵守事項

（ア）　情報セキュリティポリシーの遵守

職員等は、情報セキュリティポリシーを遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

（イ）　業務以外の目的での使用禁止

職員等は、業務以外の目的で情報資産の職場外への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（ウ）　パソコン等の端末の持ち出し及び職場外における情報処理作業の制限

（ａ）最高情報セキュリティ責任者は、機密性２以上、可用性２、完全性２の情報資産を職場外で処理する場合における安全管理措置を定めなければならない。

（ｂ）職員等は、斜里町のパソコン等の端末、記録媒体、情報資産及びソフトウェアを職場外に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

（ｃ）職員等は、職場外で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

（エ）　パソコン等の端末の持ち込み

職員等は、私物のパソコン及び記録媒体を職場内に持ち込んではならない。

（オ）　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は､パソコン等の端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

（カ）　机上の端末等の管理

職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三者に使用されること、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末のロック及びスクリーンセイバーを起動するとともに記録媒体等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

（キ）　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（ク）　コピー機等からの入出力書類の取扱い

職員等は、コピー機、ファクシミリ、プリンタ等において入出力した書類をその場に放置してはならない。

（ケ）　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（コ）　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

②非常勤及び臨時職員への対応

（ア）　情報セキュリティポリシーの遵守

情報セキュリティ管理者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシーのうち、非常勤及び臨時職員は守るべき内容を理解させ、また、実施及び遵守させなければならない。

（イ）　情報セキュリティ等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員の採用の際、必要に応じ、情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

（ウ）　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

③情報セキュリティポリシーの遵守

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシーを閲覧できるように掲示しなければならない。

④委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシーのうち、委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（２）研修・訓練

①情報セキュリティに関する研修・訓練

（ア） 最高情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（イ） 最高情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

②研修計画の立案及び実施

（ア） 最高情報セキュリティ責任者は、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的に立案し、情報セキュリティ委員会の承認を得なければならない。

（イ） 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

（ウ） 研修は、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、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（エ） 最高情報セキュリティ責任者は、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

③緊急時対応訓練

最高情報セキュリティ責任者は、緊急時対応を想定した訓練を必要に応じて実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

④研修・訓練への参加

幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

（３）事故、欠陥等の報告

①職場内からの事故等の報告

（ア）　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ管理者に報告の上、必要な指示を仰がなければならない。

（イ）　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

（ウ）　情報セキュリティ管理者は、報告のあった事故等について、必要に応じて最高情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

（エ）　情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

②住民等外部からの事故等の報告

（ア）　職員等は、斜里町が管理するネットワーク及び情報システム等の情報資産に関する事故欠陥について、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

（イ）　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

（ウ）　情報セキュリティ管理者は、当該事故等について、必要に応じて最高情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

（エ）　最高情報セキュリティ責任者は、情報システム等の情報資産に関する事故、欠陥について、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（オ）　統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

③事故等の原因の究明・記録、再発防止等

（ア） CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

（イ） CSIRT は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告しなければならない。

（ウ） CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

（エ） CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

（オ） 最高情報セキュリティ責任者は、CSIRT から、事故等について報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（４）ＩＤ及びパスワード等の管理

①ＩＣカード等の取扱い

（ア） 職員等は、自己の管理するＩＣカード等に関し、次の事項を順守しなければならない。

・認証に用いるＩＣカード等を、職員等間で共有してはならない。

・ＩＣカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

（イ） 統括情報セキュリティ責任者及び情報システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

（ウ） 統括情報セキュリティ責任者及び情報システム管理者は、ＩＣカード等を切り替える場合、切り替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

②ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

（ア） 自己が利用しているＩＤは、他人に利用させてはならない。

（イ） 共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

③パスワードの取扱い

職員等は、自己が管理するパスワードに関し、次の事項を遵守しなければならない。

（ア） パスワードは、他者に知られないように管理しなければならない。

（イ） パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

（ウ） パスワードは定められたルールに従って設定し、文字列は想像しにくいもの（アルファベットの大文字 及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

（エ） パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

（オ） パスワードは定期的に、またはアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

（カ） 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてならない。

（キ） 仮のパスワードは、最初のログイン時点で変更しなければならない。

（ク） パソコン等の端末、他人が容易に閲覧できる場所にパスワードを記録、保管させてはならない。

（ケ） 職員等間でパスワードを共有してはならない。

７．技術的セキュリティ

（１）コンピュータ及びネットワークの管理

①ファイルサーバの設定等

（ア）　情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

（イ）　情報システム管理者は、ファイルサーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

（ウ）　情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

②パックアップの実施

（ア）　統括情報セキュリティ責任者及び情報システム管理者は、業務システムのデータベースやファイルサーバ等の業務上重要なサーバに記録されたデータ及び履歴について、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。なお、バックアップ作業は、業務に影響が及ばないように作業時間については十分に配慮しなければならない。

（イ）　統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本町の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

③他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

④システム管理記録及び作業の確認

（ア） 情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

（イ） 統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システムの変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

（ウ） 統括情報セキュリティ責任者、情報システム管理者または情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2 名以上で作業し、互いにその作業を確認しなければならない。

⑤情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

⑥アクセス記録の取得等

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

（イ） 統括情報セキュリティ責任者及び情報システム管理者は、アクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じなければならない。

（ウ） 統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、電子記憶媒体にバックアップしなければならない。

（エ） 統括情報セキュリティ責任者及び情報システム管理者は、取得したアクセス記録を定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（アクセス記録等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（アクセス記録等）に関する保護が実施されているのか確認しなければならない。

（オ） 統括情報セキュリティ責任者及び情報システム管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるアクセス記録等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるアクセス記録等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

⑦障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

⑧ネットワークの接続制御、経路制御

（ア） 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルーター等の通信ソフトウェア等を設定しなければならない。

（イ） 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑨外部の者が利用できるシステムの分離

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑩外部ネットワークとの接続制限

（ア） 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、最高情報セキュリティ責任者及び統括情報セキュリティ責任者の許可を得なければならない。

（イ） 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

（ウ） 情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

（エ） 統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

（オ） 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑪複合機のセキュリティ管理

（ア） 統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

（イ） 統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

（ウ） 統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

⑫IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

⑬無線ＬＡＮ及びネットワークの盗聴対策

（ア） 統括情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

（イ） 統括情報セキュリティ責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑭電子メールのセキュリティ管理

（ア） 職員等は、電子メールの送受信にあたっては、情報システム管理者が指定した電子メールソフトウェアを利用しなければならない。

（イ） 職員等は、情報システム管理者の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

（ウ） 統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

（エ） 統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

（オ） 統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

（カ） 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

（キ）　統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

（ク）　職員等は、重要情報（パスワード、個人情報等）は、原則として電子メールを用いて送信してはならない。

（ケ）　統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で職場外に持ち出すことが不可能となるように、添付ファイルの監視等によりシステム上措置しなければならない。

⑮電子メールの利用制限

（ア）　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

（イ）　職員等は、業務上必要のない送信先に電子メールを送信・転送してはならない。

（ウ）　職員等は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上、送信しなければならない。

（エ）　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

（オ）　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

（カ）　職員等は、必要がある場合を除き、ウェブで利用できるフリーメール、ネットワークストレージ等を使用してはならない。

⑯電子署名・暗号化

（ア）　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、最高情報セキュリティ責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

（イ）　職員等は、暗号化を行う場合に最高情報セキュリティ責任者が定める以外の方法を用いてはならない。また、最高情報セキュリティ責任者が定めた方法で暗号のための鍵を管理しなければならない。

（ウ）　最高情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

⑰無許可ソフトウェアの導入等の禁止

（ア）　職員等は、パソコン等の端末に無断でソフトウェアを導入してはならない。

（イ）　職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスの管理、セキュリティ上の問題点が解決済みであるかの確認、供給者の連絡先及び更新情報が明確であるかの確認を行わなければならない。

（ウ）　職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑱機器構成の変更の制限

（ア）　職員等は、パソコン等の端末に対し機器の改造及び増設・交換を行ってはならない。

（イ）　職員等は、業務上、パソコン等の端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

⑲無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコン等の端末をネットワークに接続してはならない。

⑳業務以外の目的でのウェブ閲覧の禁止

（ア）　職員等は、ウェブブラウザの利用にあたって、情報システム管理者が指定したウェブブラウザの設定を施さなければならない。

（イ）　職員等は、業務以外の目的でウェブを閲覧してはならない。

（ウ）　職員等は、業務上不必要なバナー広告はクリックしてはならない。

（エ）　職員等は、業務上不必要なファイルやソフトウェア、不審なファイル等をダウンロードしてはならない。

（オ）　統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

㉑Web 会議サービスの利用時の対策

（ア） 統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

（イ） 職員等は、斜里町の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

（ウ） 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

（エ） 職員等は、外部から Web 会議に招待される場合は、斜里町の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

㉒ソーシャルメディアサービスの利用

（ア） 情報セキュリティ管理者は、本町が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ａ）本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

（ｂ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

（イ） 機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

（ウ） 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なければならない。

（エ） アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

（オ） 可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、斜里町の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

（２）アクセス制御

①アクセス制御等

（ア） アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

（イ）　利用者ＩＤ・パスワードの取扱い

（ａ）統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤ・パスワードの取扱い等の方法を定め、ＩＤ・パスワードが登録されている職員等の情報を記録し、維持しなければならない。

（ｂ）職員等は、業務で使用する端末は、ユーザＩＤとパスワードで保護しなければならない。

（ｃ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（ｄ）統括情報セキュリティ責任者及び情報システム管理者は、利用されていないＩＤ・パスワードが放置されないよう、定期的に点検しなければならない。

（ｅ）統括情報セキュリティ責任者及び情報システム管理者は、異動等により、庁内システムや端末を使用しなくなった職員等、又は退職した職員等のユーザＩＤとパスワードは直ちに削除しなければならない。

（ウ）　特権を付与されたＩＤの管理等

（ａ）統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

（ｂ）統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、最高情報セキュリティ責任者が認めた者でなければならない。

（ｃ）最高情報セキュリティ責任者は、代行者を認めた場合、速やかに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及び情報システム管理者に通知しなければならない。

（ｄ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせてはならない。

（ｅ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（ｆ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

②職員等による職場外からのアクセス等の制限

（ア） 職員等が職場外から庁内ネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

（イ） 統括情報セキュリティ責任者は、庁内ネットワーク又は情報システムに対する職場外からのアクセスを認める場合、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

（ウ） 統括情報セキュリティ責任者は、職場外からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

（エ） 統括情報セキュリティ責任者は、職場外からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

（オ） 職員等は、職場外から持ち帰ったパソコン等の端末を庁内ネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

③自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

④ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

⑤パスワードに関する情報の管理

（ア） 統括情報セキュリティ責任者又は情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

（イ） 統括情報セキュリティ責任者又は情報システム管理者は、本人であることを確認の上、職員等に対してパスワードを発行する。

⑥特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

（３）システム開発、導入、保守等

①情報システムの調達

（ア）　統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならい。

（イ）　統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

②情報システムの開発

（ア）　基本方針を遵守したソフトウェア開発・維持・管理

職員等または委託業者によって行われるソフトウェア開発及びソフトウェア維持管理作業は、斜里町の定める情報セキュリティ基本方針、対策基準を遵守しなければならない。

（イ）　システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。

（ウ）　システム開発における責任者、作業者のＩＤの管理

（ａ）情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（ｂ）情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

（エ）　システム開発に用いるハードウェア及びソフトウェアの管理

情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

③情報システムの導入

（ア）　開発環境と運用環境の分離及び以降手順の明確化

（ａ）情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

（ｂ）情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ｃ）情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止時の影響が最小限になるよう配慮しなければならない。

（ｅ）情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

（イ）　テスト

（ａ）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（ｂ）情報システム管理者は、運用テストを行う場合、あらかじめ疑似環境による操作確認を行わなければならない。

（ｃ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（ｄ）情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

④システム開発・保守に関する資料等の保管

（ア）　情報システム管理者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

（イ）　情報システム管理者は、テスト結果を一定期間保管しなければならない。

（ウ）　情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

⑤情報システムにおける入出力データの正確性の確保

（ア）　情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

（イ）　情報システム管理者は、故意または過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

（ウ）　情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑥情報システムの変更管理

（ア）　ソフトウェア更新の計画的実施

情報システム管理者は、情報システムのソフトウェアの更新については、計画的に実施しなければならない。

（イ）　システム変更・廃棄等の履歴保存と復旧措置

情報システム管理者は、重要なシステムを追加、変更、廃棄等した場合は、プログラム仕様書等の変更履歴を作成し、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

⑦開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

⑧システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（4）不正プログラム対策

①統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

（ア） 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

（イ） 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

（ウ） コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

（エ） 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

（オ） 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（カ） 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（キ） 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

（ク） 仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

②情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

（ア） 情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

（イ） 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（ウ） 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（エ） インターネットに接続していないシステムにおいて、記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、町が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（オ） 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

③職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

（ア） パソコン等の端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

（イ） 外部からのデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

（ウ） 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（エ） 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

（オ） 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。

（カ） 統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

（キ）　情報システム管理者の指示に従い、当該ソフトウェアのバージョンアップ及びセキュリティパッチの適用を行わなければならない。

（ク）　コンピュータウイルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの即時取り外しを行い、完全に駆除が終了するまでＬＡＮケーブルの再接続と該当する端末での作業を行ってはならない。

④専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、専門家等の支援体制を講じるものとする。

（５）不正アクセス対策

①統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

（ア）　使用されていないポートを閉鎖しなければならない。

（イ）　情報システムへアクセス可能な機器は、必要最小限にし、不必要な機器は接続してはならない。

（ウ）　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

（エ）　セキュリティホールを最小限に抑えるため、情報システムに、使用しないソフトウェアを搭載してはならない。

（オ）　不正アクセスを発見した場合、不正アクセスの被害の拡大及び再発防止のため、原因を分析し、再発防止対策を講じなければならない。

（カ）　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

（キ）　統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（ク）　本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

（ケ）　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

（コ）　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

②攻撃の予告

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

③記録の保存

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

④内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

⑤職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

⑥サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

⑦標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

（６）セキュリティ情報の収集

①セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

（ア）　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（イ）　統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本町の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

②不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

③情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を国及び関係団体、民間事業者等から適宜収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

８．運用

（１）情報システムの監視

①統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

④暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑥統括情報セキュリティ責任者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑦統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）　サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）　クラウドサービス利用の終了手順

（ウ）　バックアップ及び復旧

（２）情報セキュリティポリシーの遵守状況の確認

①遵守状況の確認及び対処

（ア）　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。

（イ）　最高情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

（ウ）　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

②端末及び記録媒体等の利用状況調査

最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

③職員等の報告義務

（ア）　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

（イ）　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（３）侵害時の対応

①緊急対応計画の策定

（ア）　最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切に対処しなければならない。

（イ）　最高情報セキュリティ責任者又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

②緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

（ア）　関係者の連絡先

（イ）　発生した事案に係る報告すべき事項

（ウ）　発生した事案への対応措置

（エ）　再発防止措置の策定

③業務継続計画との整合性確保

斜里町が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

④緊急時対応計画の見直し

最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（４）外部委託

①委託先の選定基準

（ア）　情報セキュリティ管理者は、委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（イ）　全庁的に影響するようなシステム等を委託する場合は、最高情報セキュリティ責任者の承認を得なければならない。

（ウ）　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

②契約項目

情報システムの運用、保守等を委託する場合には、委託事業者（外郭団体含む）との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシーの遵守
・委託先の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・斜里町による監査、検査
・斜里町による事故時等の公表
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

③確認・措置等

情報セキュリティ管理者は、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定期的に確認し、必要に応じ、②の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて最高情報セキュリティ責任者に報告しなければならない。

（５）例外措置

①例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、最高情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

②緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに最高情報セキュリティ責任者に報告しなければならない。

③例外措置の申請書の管理

最高情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

（６）法令遵守

①職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

（ア）　地方公務員法（昭和 25 年　法律第 261 号）

（イ）　著作権法（昭和 45 年　法律第 48 号）

（ウ）　不正アクセス行為の禁止等に関する法律（平成 11 年　法律第 128 号）

（エ）　個人情報の保護に関する法律（平成 15 年　法律第 57 号）

（オ）　斜里町個人情報保護条例（令和 5 年　条例第 2 号）

（カ）　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成 25 年　法律第 27 号）

（キ）　サイバーセキュリティ基本法（平成 26 年法律第 104 号）

②統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

（７）懲戒処分等

①懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

②違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

（ア） 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

（イ） 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

（ウ） 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知しなければならない。

９．業務委託と外部サービスの利用

（１）業務委託

①委託事業者の選定基準

（ア）　情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（イ）　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

②契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・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の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

③確認・措置等

情報セキュリティ管理者は、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定期的に確認し、必要に応じ、②の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて最高情報セキュリティ責任者に報告しなければならない。

（２）外部サービスの利用（機密性２以上の情報を取り扱う場合）

①外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備すること。

（ア） 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下９-（２）節において「外部サービス利用判断基準」という。）

（イ） 外部サービス提供者の選定基準

（ウ） 外部サービスの利用申請の許可権限者と利用手続

（エ） 外部サービス管理者の指名と外部サービスの利用状況の管理

（オ） クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

②外部サービスの選定

（ア） 情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

（イ） 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

（ウ） 情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。

（ａ）外部サービスの利用を通じて本町が取り扱う情報の外部サービス提供者における目的外利用の禁止

（ｂ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ｃ）外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本町の意図しない変更が加えられないための管理体制

（ｄ）外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（ｅ）情報セキュリティインシデントへの対処方法

（ｆ）情報セキュリティ対策その他の契約の履行状況の確認方法

（ｇ）情報セキュリティ対策の履行が不十分な場合の対処方法

（エ）　情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

（オ）　情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

（カ）　情報セキュリティ責任者は、外部サービスの利用を通じて本町が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（注）クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本町によって受容可能か判断すること。

（ａ）情報セキュリティ監査の受入れ

（ｂ）サービスレベルの保証

（キ）　情報セキュリティ責任者は、外部サービスの利用を通じて斜里町が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本町の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

（ク）　情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を斜里町に提供し、斜里町の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

（ケ）　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

（コ）　情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

（サ）　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

③外部サービスの利用に係る調達・契約

（ア）　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

（イ）　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

④外部サービスの利用承認

（ア）　情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

（イ）　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

（ウ）　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。（クラウドサービスを利用する場合も同様の措置を行う。）

⑤外部サービスを利用した情報システムの導入・構築時の対策

（ア）　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

（ａ）不正なアクセスを防止するためのアクセス制御

（ｂ）取り扱う情報の機密性保護のための暗号化

（ｃ）開発時におけるセキュリティ対策

（ｄ）設計・設定時の誤りの防止

（ｅ）クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

（イ）　外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

（ウ）　クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

⑥外部サービスを利用した情報システムの運用・保守時の対策

（ア） 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

（ａ）外部サービス利用方針の規定

（ｂ）外部サービス利用に必要な教育

（ｃ）取り扱う資産の管理

（ｄ）不正アクセスを防止するためのアクセス制御

（ｅ）取り扱う情報の機密性保護のための暗号化

（ｆ）外部サービス内の通信の制御

（ｇ）設計・設定時の誤りの防止

（ｈ）外部サービスを利用した情報システムの事業継続

（ｉ）設計・設定変更時の情報や変更履歴の管理

（イ） 情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

（ウ） 外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

（エ） クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

⑦外部サービスを利用した情報システムの更改・廃棄時の対策

（ア） 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

（ａ）外部サービスの利用終了時における対策

（ｂ）外部サービスで取り扱った情報の廃棄

（ｃ）外部サービスの利用のために作成したアカウントの廃棄

（イ） 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

（ウ） クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

（３）外部サービスの利用（機密性２以上の情報を取り扱わない場合）

①外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

（ア）　外部サービスを利用可能な業務の範囲

（イ）　外部サービスの利用申請の許可権限者と利用手続

（ウ）　外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）　外部サービスの利用の運用手順

②外部サービスの利用における対策の実施

（ア）　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

（イ）　情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

１０．評価・見直し

（１）監査

①実施方法

情報セキュリティ委員会は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

②監査を行う者の要件

（ア） 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ） 監査を行う者は、監査及び情報セキュリティに関する専門知識を有するものでなければならない。

③監査実施計画の立案及び実施への協力

（ア） 情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

（イ） 被監査部門は、監査の実施に協力しなければならない。

④委託事業者に対する監査

（ア） 委託事業者に委託している場合、情報セキュリティ監査統括責任者は委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（イ） クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

⑤報告

情報セキュリティ監査統括責任者は、監査報告書を作成し、情報セキュリティ委員会に報告する。

⑥保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

⑦監査結果への対応

最高情報セキュリティ責任者は、監査結果により発見された問題点について、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、指摘事項の対処は、各課等で直ちに実行されなければならない。

⑧情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（2）自己点検

①実施方法

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施しなければならない。

（イ） 情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じて自己点検を行わなければならない。

②報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

③自己点検結果の活用

（ア） 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（イ） 情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（3）情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要があると認めた場合、改善を行うものとする。