雫石町情報セキュリティポリシー
（改正案）

令和2年3月　策定
令和3年1月　第一次改定

雫　石　町

雫石町情報セキュリティポリシー

目　　次

第１章　情報セキュリティ基本方針

１　目的

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、本町が取り扱う住民の個人情報や行政運営上重要な情報など多数の情報も、電子自治体の構築の進展により、情報システムやネットワークに依存している状況である。

一方で、このような情報化の中で構築され運用されている情報資産は、常に個人情報の漏えい、不正アクセスや新たな攻撃手法による破壊・改ざん、操作ミスや、情報システムの事故･故障･地震･火災等の自然災害などを起因とするシステム運用の機能不全の脅威にさらされており、住民の権利、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、これらの情報資産を様々な脅威から防御することが必要不可欠である。

これらの状況を鑑み、本町における情報資産の機密性、完全性及び可用性を維持するため、本町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。

２　用語の定義

雫石町情報セキュリティポリシー（以下､｢ポリシー｣という）における用語の定義は、以下のとおりとする。

（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・確保することをいう。

（２）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。

（３）職員

雫石町職員及び本町管理下で業務を行う要員（非常勤職員、会計年度任用職員含む）をいう。

（４）情報資産

電磁的に記録された情報及び各種書類の総称であり、町行政の執行に係る情報をいう。

（５）課等

雫石町課設置条例（昭和35年条例第４号）に定める各課、教育委員会、出納課、選挙管理委員会、農業委員会及び議会をいう。

（６）情報システム

ハードウェア、ソフトウェア、ネットワーク及び情報記録媒体で構成されるものであり（構成、運用保守のための資料等を含む）、これら一部または全体で対象となる情報資産を取り扱う業務処理を行うもの。

（７）ネットワーク

コンピューター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。

（８）電子記憶媒体

端末に使用される磁気ディスク、磁気テープ、光ディスクその他これに類する記憶媒体。（例：ハードディスク、USBメモリ、SDカード、DVD-R、CD-R、フロッピーディスク、MO、テープ等）

（９）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。

（10）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。

（11）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。

（12）重要度

全ての情報資産を対象に、当該情報資産の機密性、完全性及び可用性を考慮して、重要性を分類したもの。

（13）端末

デスクトップ型パソコン、ノート型パソコン、タブレット等の職員が情報資産を取り扱うための機器をいう。

（14）サーバー

高い情報処理能力を有し、端末からの要求に従って各種処理を実行することを前提条件とした情報機器をいう。

(15) 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。

(16) 総合行政ネットワーク（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。）。

(17) 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。

(18) 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。

(19) 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。

(20) 情報セキュリティインシデント

コンピュータの利用や情報管理、情報システム運用に関して保安上の脅威となる事象であり、コンピュータウイルス感染、不正アクセス、アカウント乗っ取り、Web サイトの改竄、情報漏洩、迷惑メール送信、サービス不能攻撃、情報機器や記憶媒体の紛失や盗難などのほか、機器やシステムの破損や故障、意図しない停止をいう。

(21) ポート

ネットワークやサーバーにおける通信のための出入口をいう。

(22) サービス

情報システム上で動作するプログラム等により提供される各種機能をいう。

(23) サービス不能攻撃

情報システムに対して、その処理能力を超える膨大な通信を送り、情報システムの正常な動作を阻害する攻撃をいう。

(24) 標的型攻撃

攻撃対象として特定の法人等に狙いを定め、専用にあつらえたウイルス等のメール送付や、不正アクセスなどを執拗に長期間行い、最終的に内部に侵入して情報を盗み出すまで続けられる攻撃をいう。

３　セキュリティポリシーの位置付けと基本構成

町が保有する情報資産の情報セキュリティ対策について、総合的かつ体系的にとりまとめたものである。

情報セキュリティを確保するための組織、体制、対策及び運用を含めた規程であり、情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

（１）情報セキュリティ基本方針

町における、情報セキュリティ対策の根本的な考え方を表すもので、情報セキュリティに関するマネジメントの推進方法及び情報セキュリティ対策として行うべき項目を示すものである。

（２）情報セキュリティ対策基準

上記の基本方針において定められた情報セキュリティ対策を実現するために遵守すべき行為及び判断等の基準を示すものである。

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、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（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連する設備、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構成図等のシステム関連文書

５　職員の遵守義務

全ての職員は、本ポリシーの定める事項を理解し、遵守する責務を負う。

（１）管理職の責務

管理職の意志決定は本ポリシーに背反するものであってはならず、職員に対して本ポリシーに違反する行為を命じてはならない。また、課内で発生したセキュリティ事件・事故に対する復旧策や再発防止策を講じ、情報資産が適切に管理・保護されていることを確認する責務を負う。

（２）職員の責務

職員は本ポリシーに準拠した手順を実施する責務を負う。またセキュリティ事件・事故を発見した場合は、速やかに管理職に報告する責務を負う。

６　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）想定される脅威

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、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、水道供給の途絶等のインフラの障害からの波及等

７　情報セキュリティ対策

上記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）体制

雫石町情報セキュリティ管理・運用の維持改善を推進することを目的として統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム担当者を定め、情報セキュリティ管理・運用の運営体制を整備し、個々の役割と責任を明確にする。

（2）情報資産の分類と管理

本町の保有する情報資産を機密性、完全性及び可用性を踏まえ、その重要度に応じて分類し、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。

② 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。

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。また、高度な情報セキュリティ対策として、岩手県情報セキュリティクラウドにインターネット接続口を集約する。

（4）物理的セキュリティ

重要度の高い情報資産を取り扱う機器については、入退室管理などを厳重に施した区域に設置し、通信回線及び職員の端末機器等の管理について、物理的な対策を講じる。

（5）人的セキュリティ

職員及び委託業者が情報セキュリティの重要性を認識し、セキュリティポリシーを遵守するために守るべき事項が定められ、十分な教育及び啓発が図られるように必要な対策を講じる。

（6）技術的セキュリティ

不正なアクセス等から情報資産を適切に保護するため、情報システム及びネットワークの管理、情報資産に対するアクセス制御、ウィルス対策、不正アクセス対策及び情報システムの導入基準等の必要な対策を講ずる。

（７）外部サービスの利用

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じる。

約款によ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。

（８）運用

情報システムの監視、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、ポリシーの運用面の対策を講じるものとする。

８　情報セキュリティに係る評価及び自己点検の実施

ポリシーの遵守状況を検証するため、評価及び自己点検を実施し、セキュリティポリシー及び対策基準等が実情に即したものとなるよう見直しを行う。

９　情報セキュリティ対策基準の策定

情報セキュリティ対策及び見直し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

情報セキュリティ対策基準は、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実施するにあたって、準拠すべき行為及び判断等の基準を以下のとおり定めるものとする。

１　組織体制

情報セキュリティ管理体制と役割に関する基準は、本町が所有する情報資産に対する適切な情報セキュリティを確保するために、情報セキュリティ管理の責任者や管理者等を定め、その職務範囲と権限及び責務について定める。

（１）統括情報セキュリティ責任者

統括情報セキュリティ責任者は、本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。統括情報セキュリティ責任者は、副町長をもって充てる。

（２）情報セキュリティ責任者

① 情報セキュリティ責任者は、LGWAN を所管する課等の所属長をもって充てる。

② 情報セキュリティ責任者は、本町の全てのネットワークにおける開発、設定の変更、運用、見直し及び、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 情報セキュリティ責任者は、情報セキュリティ管理者、情報システム管理者に対して、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。

④ 情報セキュリティ責任者は、本町の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、統括情報セキュリティ責任者の指示に従い、統括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実施する権限及び責任を有する。

⑤ 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、統括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を網羅する連絡体制を含めた緊急連絡網を整備するとともに、緊急時には統括情報セキュリティ責任者に早急に報告を行い、回復のための対策を講じなければならない。

（３）情報セキュリティ管理者

① 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情報セキュリティ管理者は、各課等の長をもって充てる。

② 情報セキュリティ管理者は、その所管する課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とともに、緊急時等における連絡体制の整備、ポリシーの遵守に関する意見の集約並びに職員に対する教育、訓練、助言及び指示を行う。

③ 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し、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、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へ速やかに報告を行い、指示を仰がなければならない。

④ 情報セキュリティ管理者は、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。

（4）情報システム担当者

情報セキュリティ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。

（5）情報セキュリティ委員会

本町の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会（以下、委員会という。）を設置する。情報セキュリティ委員会は、ポリシー等の情報セキュリティに関する重要な事項の決定を行うこととし、事務局をLGWANを所管する課等に置く。

（6）兼務の禁止

① 情報セキュリティ対策の実施において、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 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（7）CSIRT（シーサート）（Computer Security Incident Response Team）の設置・役割

① 統括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ついて課等より報告を受けた場合に、情報セキュリティに関する統一的な窓口となり、その状況が自らに報告される体制として、CSIRTを整備し、その役割を明確化すること。

② CSIRT 責任者は、情報セキュリティ責任者をもって充てる。

③ CSIRT は、情報セキュリティインシデントを認知した場合には、必要に応じて関係機関や外部の事業者と連携して対応するとともに、統括情報セキュリティ責任者、総務省、岩手県へ報告し、その重要度や影響範囲等に応じて報道機関への通知・公表対応を行う。

④ CSIRT は、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、外部の事業者等との情報共有を行う。

２　情報資産の分類と管理

（１）情報資産の管理と利用に関する責任

① 情報資産の管理責任

情報資産は、その情報資産を作成あるいは構築した課等の情報セキュリティ管理者が管理責任を負う。

② 情報資産の利用責任

情報資産を利用する職員及び外部委託事業者等は、情報資産の利用目的及び重要度分類に従って利用する責任を有する。

（２）情報資産の分類

① 分類

情報セキュリティ管理者は、所管する情報資産を、その情報資産に求められる機密性、完全性及び可用性を踏まえ、次の重要度分類に従って分類する。

情報資産の重要度分類

分類	情報種類	情報の内容
Ⅰ	個人情報	個人に関する情報であって、特定の個人を識別し得る情報
Ⅱ	行政情報（重要）	セキュリティ侵害が行政事務の執行に大きな影響を及ぼす情報 ・重要度Ⅲを除く行政情報
Ⅲ	行政情報（軽易）	セキュリティ侵害が行政事務の執行に軽微な支障を及ぼす情報 ・誰でも利用可能な情報であり、既に公開済みの情報

② 取扱制限

情報資産については重要度分類に応じ、以下の取扱制限を行うものとする。

情報資産の取扱制限

分類	制限内容
Ⅰ	・ インターネットを経由するメール及びインターネット上の汎用的な外部サービスを使用した情報の送信の禁止 ・ セキュリティケースの使用やデータの暗号化等、情報の運搬・提供時における安全対策の徹底 ・ 必要以上の複製の禁止 ・ 保管場所の制限の実施 ・ 統括情報セキュリティ責任者及び管理部門の許可を得ない外部サービス上での保存・運用の禁止 ・ 使用できる職員を限定する措置の実施 ・ 重要度分類Ⅱに対する制限内容
Ⅱ	・ 情報の送信・提供時における暗号化や電子署名付与の実施 ・ 情報セキュリティ管理者の許可のない外部への送信及び持ち出しの禁止 ・ 物理的な破壊等、復元不可能な処理を施しての廃棄の実施 ・ 内容の改ざんや盗難、消失等を防ぐ措置の実施 ・ 副本・バックアップ等の作成・管理 ・ 重要度分類Ⅲに対する制限内容
Ⅲ	・ 業務以外の目的での利用の禁止

③ 分類表示

職員は、情報資産の取扱い方法を識別できるよう、重要度分類Ⅱ以上の情報資産について必要に応じて分類表示を実施する。ただし、分類表示の際には、部外者による不正使用等を防止するため、表示を記号化する等考慮する。

（3）情報資産の管理

① 情報の作成

（ア） 職員は、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（２）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、紛失や流出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。

②　情報資産の入手及び利用

（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、（２）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。

③　情報資産の保管

（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、情報資産を適正に保管しなければならない。

（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磁的記録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は、重要度分類Ⅱ以上の情報を記録した電磁的記録媒体を保管する場合、できるだけ耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑤　情報資産の廃棄

職員は、重要度分類Ⅱ以上の情報資産を廃棄する場合、情報セキュリティ管理者の許可を得るものとし、廃棄処理の実施日時、担当者及び処理内容を記録するものとする。

３　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。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、通信プロトコル（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、インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込みを可能とする。

② 情報のアクセスにおける対策

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。

（２）LGWAN 接続系

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。

① 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テキスト形式で LGWAN 接続系に転送する方式

② 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

（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 岩手県内市町村のインターネット接続口を集約する岩手県セキュリティクラウドに参加するとともに、関係省庁や岩手県と連携しながら、情報セキュリティ対策を推進しなければならない。

４ 物理的セキュリティ

（1）サーバー等の管理

① 機器の取付け

情報セキュリティ管理者は、サーバー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正に固定する等、必要な措置を講じなければならない。

② 機器の電源

（ア） 情報セキュリティ管理者は、情報セキュリティ責任者及び施設管理部門と連携し、サーバー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、当該機器が適正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） 情報セキュリティ管理者は、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、サーバー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。

③ 機器の定期保守及び修理

（ア） 情報セキュリティ管理者は、サーバー等の機器の定期保守を実施しなければならない。

（イ） 情報セキュリティ管理者は、電磁的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等を行わなければならない。

④ 庁外への機器の設置

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、庁外にサーバー等の機器を設置する場合、統括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。

⑤ 機器の廃棄等

情報セキュリティ管理者は、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。

（２）管理区域（情報システム室等）の管理

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「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

（イ）　情報セキュリティ責任者は、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、監視機能、警報装置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。

（ウ）　情報セキュリティ責任者は、情報システム室内の機器等に、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。

（エ）　情報セキュリティ責任者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

②　管理区域の入退室管理等

（ア）　情報セキュリティ責任者は、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、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

（イ）　職員及び外部委託事業者は、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）　情報セキュリティ責任者は、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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

（エ）　情報セキュリティ責任者は、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）　情報セキュリティ責任者は、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）　情報セキュリティ管理者は、情報システム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 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、適正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連する文書を適正に保管しなければならない。

② 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低限に限定し、できる限り接続ポイントを減らさなければならない。

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

④ 情報セキュリティ責任者は、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、適正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 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。

⑥ 情報セキュリティ責任者は、情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（4）職員の利用する端末や電磁的記録媒体等の管理

① 情報セキュリティ管理者は、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 情報セキュリティ管理者は、情報システムへのログインに際し、パスワード、IC カード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

５　人的セキュリティ

（1）職員の遵守事項

① ポリシー等の遵守

職員は、ポリシー及び実施手順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。

② 業務以外の目的での使用の禁止

職員は、業務以外の目的で情報資産の外部への持ち出し、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。

③ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア） 統括情報セキュリティ責任者は、情報資産を外部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。

（イ） 職員は、本町のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部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。

（ウ） 職員は、外部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。

④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を統括情報セキュリティ責任者が行った後に、業務上必要な場合は、情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ責任者の許可を得て利用することができる。

⑤ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、パソコンやモバイル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責任者の許可なく変更してはならない。

⑥ 無許可ソフトウェアの導入等の禁止

（ア） 職員は、パソコンやモバイル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。

⑦ 机上の情報資産の管理

職員は、情報システムを使用するにあたり、外部に情報が漏れることのないよう必要な対策を講じなければならない。

（２）外部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・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、ポリシー等のうち外部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。

（３）研修・訓練

① 統括情報セキュリティ責任者は、職員に対し、権限と責任に応じた次の事項についてポリシーに関する研修を実施する。

（ア） ポリシーの周知徹底

（イ） 関連法令等の理解

（ウ） 関連する実施手順の理解（関連する部門対象者への教育）

（エ） 情報セキュリティ事故対策の教育訓練

② 職員は、定められた研修に参加し、ポリシー及び実施手順を理解し、情報セキュリティ上の問題を生じさせないようにしなければならない。

（４）ID及びパスワード等の管理

① IDの取扱い

職員は、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。

② パスワードの取扱い

職員は、自己の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） パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

（ウ） パスワードは十分な長さとし、文字列は想像しにくいもの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は、同一のパスワードをシステム間で用いてはならない。

（５）情報セキュリティインシデントの報告

①　庁内での情報セキュリティインシデントの報告

（ア）　職員は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口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責任者は、速やかに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。

②　住民等外部からの情報セキュリティインシデントの報告

（ア）　職員は、本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情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ責任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責任者は、速やかに統括情報セキュリティ責任者及に報告しなければならない。

③　情報セキュリティインシデント原因の究明・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、統括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、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。

（オ）　統括情報セキュリティ責任者は、CSIRTから、情報セキュリティインシデント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。

６　技術的セキュリティ

（１）他団体との情報システムに関する情報等の交換

情報システム担当者は、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、情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

（２）ログの取得等

①　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、各種ログ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。

②　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、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③　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、取得したログ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。

（３）ネットワークの接続制御、経路制御等

①　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、ルータ等の通信ソフトウェア等を設定しなければならない。

②　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、ネットワークに適正なアクセス制御を施さなければならない。

（４）外部ネットワークとの接続制限等

①　情報セキュリティ管理者は、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、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。

② 情報セキュリティ管理者は、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、庁内の全てのネットワーク、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。

③ 情報セキュリティ管理者は、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。

④ 情報セキュリティ管理者は、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、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。

（5）機器構成の変更の制限

① 職員は、パソコンやモバイル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。

② 職員は、業務上、パソコンやモバイル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、情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

（6）無許可でのネットワーク接続の禁止

職員は、情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（7）アクセス制御等

① アクセス制御

情報セキュリティ責任者又は情報セキュリティ管理者は、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。

② 利用者 ID の取扱い

（ア） 職員は、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、情報セキュリティ責任者又は情報セキュリティ管理者に通知しなければならない。

（イ）　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、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

③　特権を付与されたIDの管理等

（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、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。

（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、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（８）職員による外部からのアクセス等の制限

①　職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、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セキュリティ管理者の許可を得なければならない。

②　情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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。

③　情報セキュリティ責任者は、外部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。

④　情報セキュリティ責任者は、外部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。

⑤　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、外部からのアクセスに利用するモバイル端末を職員に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥　職員は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内の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、情報セキュリティ管理者の許可を得てから接続しなければならない。

⑦　情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（９）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。

(10) 不正プログラム対策

①　不正プログラム対策の原則

コンピュータウィルスをはじめとする不正プログラムの脅威に備えるため、情報セキュリティ責任者は、ネットワークへの接続の有無によらず、パソコン等の端末をはじめとする各種機器には全て対策を講じることで、不正プログラムの侵入及び拡散の防止を図ること。

②　不正プログラム対策の実施

情報セキュリティ責任者は、不正プログラム対策として、次の事項を実施すること。

（ア）　所管するネットワーク上の境界点、サーバー及び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を常駐させること。

（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及びプログラムを常に最新の状態に保つこと。

（ウ）　不正プログラムに関する情報を常に収集し、必要に応じて職員に注意喚起すること。

（エ）　電磁的記録媒体を使用する必要がある場合、町が管理または許可している媒体以外を職員に利用させないこと。

（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、職員等に当該権限を付与しないこと。

③　職員が遵守すべき対策

職員は、不正プログラム対策について、次の事項を遵守すること。

（ア）　不正プログラム対策ソフトウェアの設定を変更しないこと。

（イ）　庁外から情報又はプログラム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実施すること。

（ウ）　不正プログラム対策ソフトウェアによるチェックは、処理を途中で中断せず最後まで実施すること。

（エ）　添付ファイルのある電子メールを受信した場合、差出人が不明又は不審なメールや、内容に不自然な部分のあるメールの添付ファイルは開くことなく速やかに削除すること。

（オ）　情報セキュリティ責任者が提供する不正プログラムに関する情報を常に確認すること。

（カ）　不正プログラムに感染した場合又は感染が疑われる場合は、直ちに端末の利用を中止し、LAN ケーブルの取り外し等により通信が行えない状態とした上で、情報セキュリティ管理者及び情報セキュリティ責任者へ直ちに報告すること。

④　不正プログラム被害に関する履歴の記録

情報セキュリティ責任者は、職員からの不正プログラム被害に関する報告、及び不正プログラムによって引き起こされた情報システムの障害に対する対処履歴等を記録し、常に活用できるよう分類、保存すること。

(11) 不正アクセス対策

①　不正アクセス対策での実施事項

情報セキュリティ責任者は、不正アクセス対策として、次の事項を実施すること。

（ア）　情報システムのセキュリティ上の問題の発見に努め、メーカー等から修正プログラムの提供があり次第、安全を確認した上で、計画的かつ速やかに修正プログラムを反映すること。

（イ）　重要な情報システムの設定に係るファイル等について、定期的に改ざんの有無を検査すること。

（ウ）　不要又は使用されていないポート及びサービスは、速やかに使用できないような制限を施すこと。

（エ）　不正アクセスによるウェブページ等の改ざん防止を確実にするために、ウェブページ等の不正な書き換えを検出し、情報システム担当者へ通報する仕組みを導入するよう設定すること。

② 不正アクセスへの対処

情報セキュリティ責任者は、サーバー等に攻撃を受けた場合または攻撃を受けるリスクがある場合は、システムの停止を含む必要な対策を実施すること。また、総務省、岩手県等との連絡を密にして情報の収集に努めること。

③ 犯罪行為に対する対応

情報セキュリティ責任者は、不正アクセス禁止法違反等犯罪の可能性がある攻撃を受けた場合、記録の保存に努めるとともに、統括情報セキュリティ責任者及び委員会に対し報告すること。

統括情報セキュリティ責任者及び委員会は、情報セキュリティ責任者から報告を受けた攻撃に関し、警察及び関係機関との緊密な連携に努めること。

④ 内部からの攻撃の監視

情報セキュリティ責任者は、庁内で職員及び外部委託事業者等が使用しているパソコン等の端末から、庁内のサーバー等に対する攻撃や外部のサイトに対する攻撃が行われていないか、監視すること。

⑤ 職員による不正アクセス行為

情報セキュリティ責任者は、庁内、庁外を問わず、職員による不正アクセスがあった場合、統括情報セキュリティ責任者及び委員会に通知し、適切な処置を求めること。

⑥ サービス不能攻撃

情報セキュリティ管理者び情報システム担当者は、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ること。

⑦ 標的型攻撃

情報セキュリティ管理者及び情報システム担当者は、情報システムにおいて標的型攻撃による内部への侵入を防止するために、不正プログラムの振る舞い検知や端末における自動再生機能の無効化等の入口対策を講じること。また、内部に侵

入した攻撃を早期検知して対処するために、不審な通信のチェック及び自動遮断等の内部対策を講じること。

(12) 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

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。

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セキュリティ責任者は、情報セキュリティ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、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。

7 情報システムの開発及び運用・保守

情報セキュリティ管理者及情報システム担当者は、情報システムの開発及び運用・保守を行う場合、次の事項を実施しなければならない。

（1）システム開発

① 情報セキュリティが確保されていることと、すでに稼動している情報システムへの影響の有無の確認。

② 業務用ソフトの選定や評価における、セキュリティ対策項目の設定。

③ 許可を受けた者以外のプログラムやシステムファイルの作成、更新及び削除の禁止。

④ ベンダー又は外部委託事業者等が支援のために情報システムにアクセスするときの、承認と監視。

⑤ 異常データの入出力を防止する機能の装備。

⑥　パソコンで稼動する情報システムの機能設定。

（ア）　利用者の権限に応じたアクセス制御の実施。

（イ）　ベンダーによって維持、サポートされている基本ソフトやアプリケーションソフトの使用。

（2）システム運用

①　情報セキュリティ管理者は、システム構築にあたり作成したドキュメント類を適正に管理し保管すること。

②　情報システム担当者は、情報処理設備のセキュリティを保った運用を確実にするため、実施手順に基づいた操作手順書を作成すること。

③　情報システム担当者は、情報処理の完全性及び可用性を維持するため、データ及びソフトウェアのバックアップを定期的に取得し検査すること。

④　情報システム担当者は、自分の作業の記録をとること。

⑤　情報システム担当者は、情報セキュリティインシデント発生時は情報セキュリティ管理者に報告を行い、実施手順に従い適正な処置をとること。

⑥　情報セキュリティ管理者は、セキュリティの維持に必要な情報（アクセスログ等）を適正に管理し、定期的に分析すること。

⑦　情報セキュリティ管理者は、設備の管理に関する責任及び手順を確立すること。

⑧　情報セキュリティ管理者は、情報セキュリティインシデント発生時において住民サービスへの影響を最小限にするよう対策をとること。

⑨　情報セキュリティ管理者は、情報システムの稼動やジョブの実行、パラメータの設定、データのバックアップやログの取得は可能な限り自動化し、人手による介入を削減すること。

（3）システム変更

①　情報セキュリティ管理者は、情報処理設備及び情報システムの変更について、その記録を適正に管理すること。また、情報セキュリティに影響を及ぼすシステム変更については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すること。

②　情報セキュリティ管理者は、情報システムの変更に際し、外部委託を行うときは契約書等においてポリシーを遵守する義務を課すこと。

８　外部サービスの利用

（１）外部委託

①　外部委託事業者の選定基準

情報セキュリティ管理者は、外部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よう確認に努めること。情報セキュリティの状況や信頼性確保のための条件としては、一般に以下の条件が考えられるので、選定条件決定の参考とすること。

（ア）　経営状況

（イ）　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

（ウ）　情報セキュリティ監査の実施状況

②　契約項目

情報セキュリティ管理者は、外部委託事業者との間で、必要な情報セキュリティ要件を明記した契約を締結すること。情報セキュリティ要件としては、以下の条件を基本とし、必要に応じて加除、修正を行うこと。

（ア）　業務委託範囲に応じたポリシーの遵守及びそのための体制整備

（イ）　業務上知り得た行政情報の守秘義務

（ウ）　提供された情報資産の目的外利用及び受託者以外の者への提供の禁止

（エ）　委託業務終了時の情報資産の返還義務、廃棄等

（オ）　町に対する定期報告及び緊急時報告の義務

（カ）　町による監査、検査の実施

（キ）　外部委託事業者の従業員に対する教育の実施

（ク）　情報資産の授受時及び搬送時における盗難防止措置の実施

（ケ）　町の許可のない情報資産の複写、複製の禁止

（コ）　情報資産の不正複写等の防止措置の実施

（サ）　再委託を行う場合の再委託業者への情報セキュリティ要件の徹底

（シ）　町による情報セキュリティ事案発生時の公表

（ス）　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、外部委託事業者において必要な情報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、必要に応じて前項の契約に基づく措置を実施すること。措置を実施した場合はその内容について、情報セキュリティ責任者に報告すること。

（２）約款による外部サービスの利用

①　規定の整備

情報セキュリティ管理者は、業務において約款による外部サービスを利用する場合は、利用前に管理部門と協議して了解を得た上で、当該サービスの利用に係る規定等を整備すること。規定等においては当該サービス上では重要度分類Ⅱ以上の情報資産を取り扱わないよう定めるほか、以下の項目について定めること。

（ア）　外部サービスを利用できる業務範囲の指定

（イ）　利用する外部サービスの特定

（ウ）　外部サービスの利用手続及び運用手順

②　対策の実施

職員は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

（３）ソーシャルメディアサービスの利用

①　運用手順の整備

情報セキュリティ責任者は、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。

（ア）　情報発信が町のものであることを明らかにするために、町の公式ホームページにアカウント情報を掲載するとともに、アカウントの自己紹介欄等に運用部署等を明示する等の方法でなりすまし対策を実施すること。

（イ）　町のアカウントの ID 及びパスワード等を適切に管理し、定期的にパスワードを変更する等の不正アクセス対策を行うこと。

②　利用体制の整備

情報セキュリティ責任者は、利用するソーシャルメディアに係る情報発信及びアカウント管理の責任者として、町のアカウントを使用した情報発信のための意

思決定手続きについて定め、実際に発信を行う職員及び端末を特定した利用体制を整備すること。

③　取扱い情報の制限・運用

重要度分類Ⅱ以上の情報資産については、ソーシャルメディアサービス上で発信しないこと。

また、情報セキュリティ責任者は、ソーシャルメディアサービス上で不適切な情報発信がなされないよう、発信の内容について職員に適切な指示を行うこと。

④　不正アクセス発生時の対策

情報セキュリティ責任者は、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。

（4）クラウドサービスの利用

①サービス利用の可否

情報セキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、町が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

②サービス利用リスクの評価

情報セキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

③サービス障害発生時の業務継続

情報キュリティ責任者は、クラウド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、委託先を選定する際の要件としなければならない。

④セキュリティの確保

情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス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セキュリティ要件を定めなければならない。

⑤サービス提供事業者の評価

情報セキュリティ責任者は、クラウドサービスに対する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、クラウドサービス及び当該サービス提供事業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しなければならない。

９　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セキュリティ責任者は、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セキュリティ責任者は、重要な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。

③　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。

（２）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、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）　統括情報セキュリティ責任者は、発生した問題について、適正かつ速やかに対処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セキュリティ管理者は、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正かつ速やかに対処しなければならない。

（３）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

統括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、職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、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。

（４）職員の報告義務

① 職員は、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。

② 当該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において、職員は、適正に対処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、統括情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

② 緊急時の例外措置

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、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。

③ 例外措置の申請書の管理

統括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正に保管し、定期的に申請状況を確認しなければならない。

（６）法令遵守

職員は、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。

① 地方公務員法(昭和 25 年法律第 261 号)

② 著作権法（昭和 45 年法律第 48 号)

③ 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)

④ 個人情報の保護に関する法律（平成 15 年法律第 57 号)

⑤ 行政手続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)

⑥ サイバーセキュリティ基本法（平成 28 年法律第 31 号)

⑦　雫石町個人情報保護条例（平成 12 年条例第２号）

（７）懲戒処分等

①　懲戒処分

ポリシーに違反した職員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なり得る。

②　違反時の対応

職員の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）　違反を確認した職員は、情報セキュリティ責任者及び違反を行った職員が所属する課等の情報セキュリティ管理者へ連絡すること。

（イ）　情報セキュリティ責任者は、統括情報セキュリティ責任者に報告の上、違反した職員が所属する課等の情報セキュリティ管理者に適切な対応を求めること。

（ウ）　統括情報セキュリティ責任者は、情報セキュリティ管理者の指導によっても違反が改善されない場合、その職員のネットワーク又は情報システムの使用に関する権利を、必要と認められる期間停止あるいは剥奪するよう、情報セキュリティ責任者に指示すること。その後速やかに、情報セキュリティ責任者は、職員の権利を停止あるいは剥奪した旨を、統括情報セキュリティ責任者及び当該職員が所属する課等の情報セキュリティ管理者に報告・通知すること。

10　評価、見直し

（１）自己点検

①　実施方法

情報セキュリティ責任者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施すること。

また、情報セキュリティ管理者は、情報セキュリティ責任者と連携して、所管する部署におけるポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を実施すること。

②　報告

情報セキュリティ責任者、情報セキュリティ管理者は、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、委員会に報告すること。

（2）監査

① 実施方法

統括情報セキュリティ責任者は、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、必要に応じて情報セキュリティ監査を行わせること。

② 監査を行う者の要件

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であり、監査及び情報セキュリティに関する専門知識を有する者に対して、監査の実施を依頼すること。

③ 監査実施計画の立案及び実施への協力

情報セキュリティ監査統括責任者は、監査を行うに当たって、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ること。

被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に業務の一部等を委託している場合、情報セキュリティ監査統括責任者は、外部委託事業者から再委託を受けている事業者を含めて、ポリシーの遵守についての監査を必要に応じて実施すること。

⑤ 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、委員会に報告すること。

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すること。

⑦ 監査結果への対応

統括情報セキュリティ責任者は、監査結果を踏まえ、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すること。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すること。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示するものとする。

（3）ポリシー及び関係規程等の見直し

委員会は、自己点検及び情報セキュリティ監査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踏まえ、定期的及び重大な事象等の発生時において、ポリシー及び関係規程等が十分かつ適切な内容であるかを確認・判断し、その必要があると認めた場合、ポリシー及び関係規程等の改善を行うこと。