東浦町情報セキュリティポリシー

平成24年４月１日制定
平成26年４月１日一部改正
平成28年１月１日一部改正
令和２年１月１日一部改正
令和３年４月１日一部改正
令和５年４月１日一部改正
令和６年２月１日一部改正
令和８年４月１日一部改正

目　次

第１章　情報セキュリティ基本方針

（目的）

第１条　東浦町情報セキュリティポリシー（以下「ポリシー」という。）は、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により、本町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する。

（定義）

第２条　ポリシーにおいて、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）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。

（５）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。

（６）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。

（７）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。

（８）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。）。

（９）インターネット接続系

インターネットメール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。

(10）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。

(11）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。

(12) 情報セキュリティインシデント

望ましくない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(13) 端末

情報システムの構成要素である機器のうち、情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボード、マウス等の周辺機器を含む。）をいう。

(14) パソコン

端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

(15) モバイル端末

端末のうち、業務上の必要に応じて、移動させて使用することを目的としたものをいい、端末の形態は問わない。

(16) 電磁的記録媒体

コンピュータによる情報処理に使用する、電子的又は電磁的な記録方式により作成された記録を保持するための媒体。ハードディスク、CD、DVD、USBメモリ、SDカード、コンパクトフラッシュ、フロッピーディスク、磁気テープ類等をいう。

(17) 情報システム室

重要な情報システム及びネットワークの基幹機器を設置し、当該機器等の管理並びに運用を行うための部屋をいう。

(18) 部等の長

東浦町部制条例（昭和56年東浦町条例第２号）、東浦町教育委員会事務局組織規則（昭和54年東浦町教育委員会規則第３号）で定める部の長、東浦町議会事務局処務規程（昭和61年東浦町議会規程第１号）に定める議会事務局の長をいう。

(19) 課等の長

東浦町事務分掌規則（昭和56年東浦町規則第４号）、東浦町教育委員会事務局組織規則、東浦町議会事務局処務規程、東浦町会計管理者の補助組織設置規則（昭和48年東浦町規則第１号）、東浦町監査委員事務局規程（平成17年東浦町監査委員告示第７号）に定める課等の長をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施するものとする。

(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、改ざん又は消去、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、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及び業務の停止等

（４）大規模又は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　ポリシーを適用する範囲は、次のとおりとする。

（１）行政機関の範囲を町長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、水道事業及び下水道事業の管理者の権限を行う町長とする。

（２）職員の範囲は、本町の保有する情報資産に関わる職員（地方公務員法(昭和25年法律第261号（以下「地方公務員法」という。）)第３条に規定する職員をいう。）とし、会計年度任用職員（地方公務員法第22条の２）及び臨時的任用職員（地方公務員法第22条の３）を含む。また、本町の保有する情報資産に関わることが必要と認められた者も含む（以下「職員等」という。）。

（３）情報資産の範囲を次のとおりとし、東浦町立学校設置条例（昭和46年東浦町条例第16号）で規定する各教育機関が保有する情報資産を除く。

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

（遵守義務）

第５条　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、業務の遂行に当たりポリシー、関係規定等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　第３条に規定する脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

（１）組織体制

本町の保有する情報資産について、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）情報資産の分類及び管理

本町の保有する情報資産を機密性、完全性及び可用性に応じて、分類及び管理を行い、当該分類及び管理に基づき情報セキュリティ対策を講じる。

（3）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。

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。

（4）物理的セキュリティ

サーバ及び通信機器、情報システム室、通信回線並びに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、職員等が遵守すべき事項を定めるとともに、十分な教育、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対策を講じる。

（7）運用

情報システムの監視、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、ポリシー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、緊急時対応計画を策定する。

（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

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。

ポリシーの見直しが必要な場合は、適宜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　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ものとする。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、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は、ポリシーを見直すものとする。

（情報セキュリティ実施手順の策定）

第９条　ポリシーに基づき、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　組織体制

（最高情報セキュリティ責任者及び最高情報統括責任者）

第10条 最高情報セキュリティ責任者（CISO：Chief Information Security Officer）及び最高情報統括責任者（CIO：Chief Information　Officer）は、副町長を充てる。

２　最高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。

３　最高情報統括責任者は、情報通信技術の活用による住民の利便性の向上、行政運営改善等に関する最終決定権限及び責任を有する。

４　最高情報セキュリティ責任者は、必要に応じて、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に意見を求めるものとする。

５　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。

６　最高情報セキュリティ責任者は、次に掲げる事務を行うため、各課等または施設にITリーダーを設置する。

（１）情報機器等の管理、障害対応

（２）ITリテラシーの普及及び向上並びにICT及び情報セキュリティに関する指導及び助言

（統括情報セキュリティ責任者）

第11条　統括情報セキュリティ責任者は、情報主管課の属する部長を充てる。

２　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を補佐しなければならない。

3　統括情報セキュリティ責任者は、本町の共用的なネットワークにおける開発、導入、保守等の調達、設定の変更、運用、見直し等を行う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、本町の共用的な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。
5　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、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。
6　統括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、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。
7　統括情報セキュリティ責任者は、本町の共用的なネットワーク、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及び管理を行う権限及び責任を有する。
8　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及び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しなければならない。
9　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。
10　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定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。

（情報セキュリティ責任者）

第12条　情報セキュリティ責任者は、各部等の長を充て、部に属さない課等の情報セキュリティ責任者は、在籍する部長相当職にある者を充て、部長相当職にある者が在籍していない場合には、総務部長を充てる。
2　情報セキュリティ責任者は、当該部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、所管する部等において保有している情報システムにおける開発、保守等の調達、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、所管する部等において保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、ポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）

第13条　情報セキュリティ管理者は、各課等の長を充てる。
2　情報セキュリティ管理者は、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、所管する課等において、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、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、指示を受けなければならない。

（情報システム管理者）

第14条　情報システム管理者は、各情報システムの担当課等の長を充てる。
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、保守等の調達、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。

（情報システム担当者）

第15条　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、導入、保守等の調達、設定の変更、運用、更新等の作業を行う者とする。

（情報セキュリティ委員会）

第16条　情報セキュリティ委員会は、行政経営会議が兼ねるものとする。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において、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。

（兼務の禁止）

第17条　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　情報セキュリティ監査の実施において、や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。

（CSIRTの設置・役割）

第18条　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課等より報告を受けた場合は、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、その内容を関係部課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は、その重要性、影響範囲等を勘案し、報道機関への通知及び公表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、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。

第３章　情報資産の分類と管理

（情報資産の分類）

第19条　本町における情報資産は、機密性、完全性及び可用性により、別表のとおり分類し、必要に応じて、取扱制限を行うものとする。

（情報資産の管理責任）

第20条　情報セキュリティ管理者は、所管する情報資産について管理責任を有するものとする。

２　情報資産が複製又は伝送された場合は、複製等された情報資産も前条の分類に基づき管理しなければならない。

（情報資産の分類の表示）

第21条　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（プロパティ）、ヘッダー及びフッター等）、格納する電磁的記録媒体のラベル、文書の隅等に必要に応じて、情報資産の分類を表示し、取扱制限についても明示するなど適正な管理を行わなければならない。

（情報資産の作成）

第22条　職員等は、業務上必要のない情報資産を作成してはならない。

２　職員等は、情報資産を作成する場合、第19条の別表に基づき、当該情報資産の分類と取扱制限を定めなければならない。

３　職員等は、情報資産を作成する場合、作成途中の情報資産についても、紛失、流出等を防止しなければならない。また、情報資産の作成途中で不要になった場合は、当該情報資産を消去しなければならない。

（情報資産の入手）

第23条　職員等は、他の職員等が作成した情報資産を入手した場合、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。

２　職員等は、職員等以外の者が作成した情報資産を入手した場合、第19条の別表に基づき、当該情報資産の分類と取扱制限を定めなければならない。

３　情報資産を入手した職員等は、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指示を受けなければならない。

（情報資産の利用）

第24条　情報資産を利用する職員等は、業務の目的以外に情報資産を利用してはならない。

２　情報資産を利用する職員等は、第19条の別表に基づく情報資産の分類に応じて、適正な取扱いをしなければならない。

３　情報資産を利用する職員等は、電磁的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、最も高い分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第25条　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。

２　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間保管する場合、書込禁止の措置を講じなければならない。

３　情報セキュリティ管理者又は情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期間保管する場合、情報システムの重要性に応じて、自然災害を被る可能性が低い地域に保管しなければならない。

４　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又は３、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、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。

（情報の送信）

第26条　電子メール等により機密性２又は３の情報を送信する職員等は、パスワード等による暗号化を行わなければならない。

（情報資産の運搬）

第27条　車両等により機密性２又は３の情報資産を運搬する場合は、必要に応じて、鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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。

２　機密性２又は３の情報資産を運搬する場合は、情報セキュリティ管理者の許可を得なければならない。

（情報資産の提供及び公表）

第28条　機密性２又は３の情報資産を外部に提供する場合は、パスワード等による暗号化を行わなければならない。

２　機密性２又は３の情報資産を外部に提供する場合は、情報セキュリティ責任者の許可を得なければならない。

３　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、完全性を確保しなければならない。

（情報資産の廃棄）

第29条　情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、記録されている情報の機密性に応じ、電磁的記録媒体の情報を復元できないように処置したうえで廃棄しなければならい。

２　電磁的記録媒体の廃棄を行う者は、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。

３　電磁的記録媒体の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系）

第30条　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、国等の公共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を、次のとおり実施しなければならない。

（１）情報アクセス対策

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。

（２）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。

（LGWAN接続系）

第31条　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LGWAN接続系に転送するメールテキスト化方式

（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する方式

（３）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

（インターネット接続系）

第32条　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。

第５章　物理的セキュリティ

第１節　サーバ等の管理

（機器の取付け）

第33条　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正に固定するなど、必要な措置を講じなければならない。

（サーバの冗長化）

第34条　情報システム管理者は、重要情報を格納しているサーバ、認証サーバ、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、同一データを保持しなければならない。

（機器の電源）

第35条　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者と連携し、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。

２　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者と連携し、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。

３　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者と連携し、重要情報を格納しているサーバ等（関連機器を含む。）の電源について、停電等による電源供給の停止に備え、十分な電力を供給する容量の自家発電装置を備え付けなければならない。

（通信ケーブル等の配線）

第36条　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、施設管理者と連携し、主要な箇所の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など必要な措置を講じなければならない。

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、通信ケーブル及び電源ケーブルについて、施設管理者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。

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、ネットワーク機器の接続口を職員等以外の者が容易に接続できない場所に設置するなど適正に管理しなければならない。

４　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、自ら又は情報システム担当者若しくは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又は追加できないように必要な措置を講じなければならない。

（機器の定期保守及び修理）

第37条　情報システム管理者は、可用性２のサーバ等の機器に対し、定期保守を実施しなければならない。

２　情報システム管理者は、電磁的記録媒体を内蔵する機器を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、事業者に故障を修理させるに当たり、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。

（施設外への機器の設置）

第38条　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、本町の施設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。

（機器の廃棄等）

第39条　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。

第２節　管理区域の管理

（管理区域の構造等）

第40条　管理区域とは、情報システム室をいう。

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、システムの重要性に応じて、浸水のおそれを考慮し、管理区域を設けなくてはならない。また、外部からの侵入が容易にできないよう、無窓の外壁と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、施設管理者と連携して、管理区域から外部に通ずるドアを必要最小限とし、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。

４　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、情報システム室内の機器等に、転倒、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。

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、施設管理者と連携して、管理区域を囲む外壁等の開口部を全て塞がなければならない。

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、施設管理者と連携して、管理区域に配置する消火薬剤、消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（管理区域の入退室管理等）

第41条　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、指紋認証等の生体認証又は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。

２　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。

３　情報システム管理者は、外部の者が管理区域に入る場合は、必要に応じて、立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。

４　情報システム管理者は、機密性２又は３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、許可なく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。

（機器等の設置及び撤去）

第42条　情報システム管理者は、設置及び撤去する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせなければならない。

２　情報システム管理者は、情報システム室の機器等の設置及び撤去について、職員等を立ち会わせなければならない。

第３節　通信回線及び通信回線装置の管理

（通信回線等の管理）

第43条　情報セキュリティ責任者は、施設内の通信回線及び通信回線装置を、施設管理者と連携し、適正に管理しなければならない。また、配線及び配置を記した図面並びに設定等を記録した文書を適正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　統括情報セキュリティ責任者は、外部へ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又は３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、適正な回線を選択しなければならない。また、必要に応じて、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、可用性２の情報を取り扱う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、必要に応じて、回線を冗長構成にするなどの措置を講じなければならない。

第４節　職員等の利用する端末、電磁的記録媒体等の管理

（職員等の利用する端末、電磁的記録媒体等の管理）

第44条　情報システム管理者は、盗難防止のため、事務室等で利用するパソコンを原則としてワイヤーにより固定しなければならない。ただし、一時的に会議室等へ持

ち込んで利用し、会議室等の施錠を適正に行う場合は、この限りでない。
2　情報システム管理者は、モバイル端末及び電磁的記録媒体について、使用時以外の施錠管理等の物理的措置を講じなければならない。
3　情報システム管理者は、電磁的記録媒体について、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。
4　情報システム管理者は、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　情報システム管理者は、第三者により端末の重要な設定を不正に変更されることを防ぐため、端末にBIOSパスワードを設定しなければならない。
6　情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用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）を行うよう設定しなければならない。
7　情報システム管理者は、パソコン及びモバイル端末に暗号化の機能を有する又はセキュリティチップが搭載されている場合、その機能を有効にしなければならない。
8　情報システム管理者は、USBメモリについて、データ暗号化機能を備える製品を使用しなければならない。
9　情報システム管理者は、モバイル端末の外部での利用の際は、前各項の対策に加え、遠隔消去機能を利用するなどの措置を講じなければならない。

第6章　人的セキュリティ

第1節　職員等の遵守事項

（職員等の遵守事項）
第45条　職員等は、ポリシー及び実施手順を遵守しなければならない。
2　職員等は、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、指示を受けなければならない。
3　職員等は、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。
4　情報資産の持出し及び外部における情報処理作業の制限を、次のとおり実施するものとする。
（1）最高情報セキュリティ責任者は、機密性２若しくは3、可用性２又は完全性２の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。
（2）職員等は、モバイル端末、電磁的記録媒体等の情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ責任者の許可を得なければならない。
（3）職員等は、外部で情報処理業務を行う場合は、情報セキュリティ責任者の許可を得なければならない。

5　支給以外のパソコン、モバイル端末、電磁的記録媒体等の業務利用については次のとおりとする。

（1）職員等は、支給以外のパソコン、モバイル端末、電磁的記録媒体等を原則として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最高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、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

（2）職員等は、支給以外のパソコン、モバイル端末、電磁的記録媒体等を用いる場合、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

6　情報セキュリティ管理者は、パソコン、モバイル端末、電磁的記録媒体等の持出し及び持込みについて、記録を作成し、及び保管しなければならない。

7　職員等は、パソコン及び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管理者の許可なく変更してはならない。

8　職員等は、パソコン、モバイル端末、電磁的記録媒体、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を閲覧されることがないように、離席時のパソコン及びモバイル端末のロック、電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

9　職員等は、異動、退職等の場合には、利用していた情報資産を、情報システム管理者へ返却しなければならない。

10　職員等は、異動、退職等の後も業務上知り得た情報を漏らしてはならない。

（会計年度任用職員等への対応）

第46条　情報セキュリティ管理者は、会計年度任用職員、臨時的任用職員、本町の保有する情報資産に関わることが必要と認められた者（以下「会計年度任用職員等」という。）に対し、採用の際、ポリシーのうち会計年度任用職員等が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。

2　情報セキュリティ管理者は、会計年度任用職員等の採用の際、必要に応じて、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。

3　情報セキュリティ管理者は、会計年度任用職員等にパソコンやモバイル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外部への電子メールを利用できないようにしなければならない。ただし、業務においてインターネットへの接続が必要な場合、定められた手続きを行った上で利用させることができる。

（情報セキュリティポリシー等の掲示）

第47条　情報セキュリティ管理者は、職員等が常にポリシー、関係規定等を閲覧できるように掲示しなければならない。

（委託事業者に対する説明）

第48条　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、再委託事業者も含めて、ポリシー等のうち委託事業

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。

第２節　研修及び訓練

（情報セキュリティに関する研修及び訓練）

第49条　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及び訓練を実施しなければならない。

（研修計画の策定及び実施）

第50条　最高情報セキュリティ責任者は、町長を始め全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の策定とその実施体制の構築を定期的に行わなければならない。

２　最高情報セキュリティ責任者は、研修計画において、職員等が毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

３　最高情報セキュリティ責任者は、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。

４　研修は、ポリシー上の組織体制におけるそれぞれの役割、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。

５　最高情報セキュリティ責任者は、毎年度１回、職員等の情報セキュリティ研修の実施状況について、情報セキュリティ委員会に報告しなければならない。

（緊急時対応訓練）

第51条　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定期的に実施しなければならない。

２　前項の訓練は、効果的に実施できるよう、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定めなければならない。

（研修及び訓練への参加）

第52条　町長を始め全ての職員等は、定められた研修及び訓練に参加しなければならない。

第３節　情報セキュリティインシデントの報告

（庁内での情報セキュリティインシデントの報告）

第53条　職員等は、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管理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。

２　前項の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。

３　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、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。

（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）

第54条　職員等は、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、速やかに情報セキュリティ管理者に報告しなければならない。
２　前項の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。
３　情報セキュリティ管理者は、当該情報セキュリティインシデントについて、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。
４　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。

（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）

第55条　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。
２　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。
３　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。
４　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、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　最高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講じなければならない。

第４節　ID及びパスワード等の管理

（ICカード等の取扱い）

第56条　職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。
（１）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。
（２）業務上必要のないときは、ICカード等をカードリーダ又はパソコンのスロット等から抜いておかなければならない。
（３）ICカード等を紛失した場合は、直ち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、指示に従わなければならない。
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、ICカード等の紛失等の報告があった場合、当該ICカード等を使用したアクセス等を直ちに停止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、ICカード等を廃棄する場合、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。

（IDの取扱い）

第57条　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。

（１）自己が利用しているIDを、他人に利用させてはならない。

（２）共用ID（複数人が利用することを前提としたIDをいう。）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。

（パスワードの取扱い）

第58条　職員等は、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。

（１）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。

（２）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。

（３）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。

（４）パスワードが流出したおそれがある場合は、情報システム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。

（５）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はならない。

（６）仮パスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

（７）サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

（８）職員等間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く）。

第７章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

（ファイルサーバの設定等）

第59条　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を設置した場合は、容量を設定し、職員等に周知しなければならない。

２　情報システム管理者は、ファイルサーバのフォルダ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。

３　情報システム管理者は、人事記録等、特定の職員等しか取り扱えないデータについて、別途フォルダを作成するなどの措置を講じ、同一課等であっても、担当職員等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。

（バックアップの実施）

第60条　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、サーバ等に記録さ

れた情報について、サーバの冗長化対策に関わらず、必要に応じて、定期的にバックアップを実施しなければならない。

（システム管理記録及び作業の確認）

第61条　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。

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、所管するシステムにおいて、システム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、適正に管理しなければならない。

３　情報システム管理者又は情報システム担当者若しくは、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。

（情報システム仕様書等の管理）

第62条　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の閲覧、紛失等がないよう、適正に管理しなければならない。

（ログの取得等）

第63条　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、各種ログ及び情報セキュリティの確保に必要な情報を取得し、一定の期間保存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、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　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。

（障害記録）

第64条　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、適正に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第65条　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、ルータ等の通信ソフトウェア等を設定しなければならない。

２　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、ネットワークに適正なアクセス制御を施さなければならない。

（外部の者が利用できるシステムの分離等）

第66条　情報システム管理者は、自己管理ウェブサイト、図書館システム等、外部の者が利用できるシステムについて、必要に応じて、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などの措置を講じなければならない。

（外部ネットワークとの接続制限等）

第67条　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、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。

２　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。

４　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、サーバ等を外部からアクセスできる状態にする場合、庁内の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上で接続しなければならない。

５　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、統括情報セキュリティ責任者の判断に従い、直ち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。

（複合機のセキュリティ管理）

第68条　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て、適正なセキュリティ要件を策定しなければならない。

２　統括情報セキュリティ責任者は、前項で定めたセキュリティ要件に基づき、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。

３　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、複合機に内蔵された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。

（IoT機器を含む特定用途機器のセキュリティ管理）

第69条　統括情報セキュリティ責任者は、ネットワークカメラ等、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。

（無線LANのセキュリティ対策及びネットワークの盗聴対策）

第70条　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機能の使用を義務付けなければならない。

２　統括情報セキュリティ責任者は、機密性の高い情報を取り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。

（電子メールのセキュリティ管理）

第71条　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。

２　統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

３　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。

４　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の保存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。

５　統括情報セキュリティ責任者は、委託事業者の作業員に本町の管理する電子メールアドレスを利用させてはならない。

６　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外部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するよう努めなければならない。

（電子メールの利用制限）

第72条　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。

２　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

３　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。

４　職員等は、電子メールを外部に送信する場合、原則として、課等の長又は課等の長が指示する者へカーボンコピーの機能を用いて送信しなければならない。

５　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速やかに報告しなければならない。

６　職員等は、ウェブで利用できる電子メールを原則使用してはならない。

７　職員等は、統括情報セキュリティ責任者が許可する場合を除き、ネットワークストレージサービス等を使用してはならない。

（電子署名及び暗号化）

第73条　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、最高情報セキュリティ責任者が定めた電子署名又はパスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

２　職員等は、前項による暗号化を行う場合、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パスワード等を管理しなければならない。

３　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。

（無許可ソフトウェアの導入等の禁止）

第74条　職員等は、サーバ、パソコン及び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。
２　職員等は、業務上の必要がある場合は、関係する全ての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を管理しなければならない。
３　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。
（機器構成の変更の制限）
第75条　職員等は、サーバ、パソコン及びモバイル端末の改造、増設及び交換を原則として行ってはならない。
２　職員等は、業務上、サーバ、パソコン及びモバイル端末に対し機器の改造、増設又は交換を行う必要がある場合には、情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。
（業務外ネットワークへの接続の禁止）
第76条　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。
２　情報セキュリティ管理者は、支給した端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に対策を講じなければならない。
（業務以外の目的でのウェブ閲覧の禁止）
第77条　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。
２　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正な措置を求めなければならない。
（Web会議サービスの利用時の対策）
第78条　統括情報セキュリティ責任者は、Web会議サービスを適切に利用するためのガイドラインを定めなければならない。
２　職員等は、本町の定めるガイドラインに従い、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しなければならない。
３　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じなければならない。

第２節　アクセス制御

（アクセス制御等）
第79条　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。
２　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管理者

は、IDの取扱いについて、次の各号に定める措置を講じなければならない。

（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、利用者の登録、変更、抹消等の情報管理、職員等の異動に伴う利用者IDの取扱い等の方法を定めなければならない。

（２）情報セキュリティ管理者は、利用者の登録、変更、抹消等の必要が生じた場合は、関係する情報システム管理者へ通知しなければならない。

（３）人事管理部門の管理者は、職員等の異動等が生じた場合、当該異動の情報を情報システム管理者に通知しなければならない。

（４）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が放置されないよう、人事管理部門の管理者と連携し、点検しなければならない。

３　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及びパスワードの管理について、次の各号に定める措置を講じなければならない。

（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、管理者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。

（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。

（３）最高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及び情報システム管理者の特権を代行する者を認めた場合、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その旨を通知しなければならない。

（４）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。

（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、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的な変更、パスワード入力回数制限等のセキュリティ機能を強固にしなければならない。

（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、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。

（外部からのアクセス等の制限）

第80条　職員等及び外部委託事業者が、外部から庁内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、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。

２　統括情報セキュリティ責任者は、庁内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　統括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　統括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、通信経路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　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、外部からのアクセスに利用するモバイル端末について、セキュリティ確保のための必要な措置を講じなければならない。

6　職員等は、外部で利用したモバイル端末を庁内のネットワークに接続する場合、コンピュータウイルスに感染していないこと、ソフトウェアの修正プログラム（以下「パッチ」という。）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るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

7　統括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インターネットを介した外部からのアクセスを原則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、パスワード及びワンタイムパスワード等の複数の認証情報並びに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。

（自動識別の設定）

第81条　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。

（ログイン時の表示等）

第82条　情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及び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職員等が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。

（認証情報の管理）

第83条　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、職員等の認証情報を厳重に管理しなければならない。

2　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、認証情報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認証情報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。

3　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、職員等に対してパスワードを発行する場合は、仮パスワードを発行し、初回ログイン後速やかに仮パスワードを変更させなければならない。

4　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、認証情報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。

（特権による接続時間の制限）

第84条　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。

第３節　情報システムに関する調達等

（情報システムの調達）

第85条　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、情報システムの開発、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、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。

（情報システムの開発）

第86条　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。また、システム開発のための方針及び手順を確立しなければならない。

２　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。

３　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らない。

４　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。

５　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（情報システムの導入）

第87条　情報システム管理者は、システム運用環境をシステム開発、保守及びテスト環境と分離しなければならない。

２　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の手順を、計画の策定時等にあらかじめ明確にしなければならない。

３　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等の影響が最小限になるよう配慮しなければならない。

４　情報システム管理者は、システム及び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情報システムを導入しなければならない。

５　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テストを行わなければならない。

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

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

８　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。

（情報システム開発及び保守に関連する資料等の整備及び保管）

第88条　情報システム管理者は、システム開発及び保守に関連する資料並びに文書を適正に整備及び保管しなければならない。

２　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。

３　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正な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第89条　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。

２　情報システム管理者は、故意又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、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。

３　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。

（情報システムの変更管理）

第90条　情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発及び保守用のソフトウェアの更新等）

第91条　情報システム管理者は、開発及び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。

（システム更新又は統合時の検証等）

第92条　情報システム管理者は、システム更新及び統合時に伴うリスク管理体制の構築、移行基準の明確化並びに更新及び統合後の業務運営体制の検証を行わなければならない。

第４節　不正プログラム対策

（統括情報セキュリティ責任者の措置事項）

第93条　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。

（１）外部ネットワークから受信したファイルは、インターネットと接続する中継点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。

（２）外部ネットワークに送信するファイルは、インターネットと接続する中継点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、不正プログラムの外部への拡散を防止しなければならない。

（３）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、必要に応じて、職員等に対して注意喚起しなければならない。
（４）所管するサーバ、パソコン及びモバイル端末に、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。
（５）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。
（６）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。
（７）業務で利用するソフトウェアは、パッチ、バージョンアップ等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中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。

（情報システム管理者の措置事項）

第94条　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。
（１）所管するサーバ及びパソコンに、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。
（２）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。
（３）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。
（４）インターネットに接続していないシステムにおいて、電磁的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、本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。
（５）インターネットに接続していないシステムにおいて、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。
（６）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、情報セキュリティ管理者が許可した職員等を除く職員等に当該権限を付与してはならない。

（職員等の遵守事項）

第95条　職員等は、パソコン及びモバイル端末の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。
（１）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。
（２）外部からデータ又はソフトウェアを取り入れる場合及び電磁的記録媒体を利用する場合は、事前に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。

（３）差出人が不明又は不自然に添付されたファイルを収受した場合は、速やかに情報セキュリティ管理者に報告し、指示を受けなければならない。

（４）不正プログラム対策ソフトウェアによる全ファイルチェック（以下「完全スキャン」という。）を定期的に実施しなければならない。

（５）ファイルが添付され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接続系に取込む場合は、原則として、無害化しなければならない。

（６）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。

（７）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又は、感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、当該端末においてLANケーブルの取り外しや通信を行わない設定への変更などを実施しなければならない。

（専門家の支援体制）

第96条　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、外部の専門家の支援を受けられるようにしておかなければならない。

第５節　不正アクセス対策

（統括情報セキュリティ責任者の措置事項）

第97条　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、次の事項を措置しなければならない。

（１）使用されていないポート番号を無効にしなければならない。

（２）不要なサービスについて、機能を削除又は停止しなければならない。

（３）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、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。

（４）重要なシステムの設定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するよう努めなければならない。

（５）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、外部窓口及び適正な対応等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。

（攻撃への対処）

第98条　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た場合又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措置を講じなければならない。この場合において、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第99条　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行為の禁止等に関する法律（平成11年法律第128号）等に抵触する可能性がある場合、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。

（内部からの攻撃）

第100条　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からのサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

（職員等による不正アクセス）

第101条　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、適正な処置を求めなければならない。

（サービス不能攻撃）

第102条　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。

（標的型攻撃）

第103条　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。

第６節　セキュリティ情報の収集

（セキュリティに関する情報の収集及び共有並びにソフトウェアの更新等）

第104条　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、必要に応じて、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。

（不正プログラム等のセキュリティ情報の収集及び周知）

第105条　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、必要に応じた対応方法について、職員等に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第106条　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収集し、必要に応じて、関係者間で共有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、情報セキュリティに関する社会環境、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。

第８章　運用

第１節　情報システムの監視

（情報システムの監視）

第107条　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する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。

第２節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第108条　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。

２　最高情報セキュリティ責任者は、前項の問題について、適正かつ速やかに対処しなければならない。

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、ネットワーク、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、適正かつ速やかに対処しなければならない。

（サーバ、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）

第109条　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サーバ、パソコン、モバイル端末、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。

（職員等の報告義務）

第110条　職員等は、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しなければならない。

２　前項の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は、職員等は、緊急時対応計

画に従って適正に対処しなければならない。

第３節　セキュリティ侵害時の対応等

（緊急時対応計画の策定）

第111条　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、情報セキュリティインシデント、ポリシー違反等により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正に実施するために、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。

（緊急時対応計画に盛り込むべき内容）

第112条　緊急時対応計画には、次の内容を定めなければならない。

（１）関係者の連絡先

（２）発生した事案に係る報告すべき事項

（３）発生した事案への対応措置

（４）再発防止措置の策定

（業務継続計画との整合性確保）

第113条　自然災害、大規模及び広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画とポリシーとの整合性を確保しなければならない。

（緊急時対応計画の見直し）

第114条　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、組織体制の変動等に応じて、緊急時対応計画の規定を見直さなければならない。

第４節　例外措置

（例外措置の許可）

第115条　情報セキュリティ管理者及び情報システム管理者は、ポリシー及び関係規定等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する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、例外措置を講じることができる。

（緊急時の例外措置）

第116条　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などの場合であって、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。

（例外措置の申請書の管理）

第117条　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正に

保管し、例外措置の必要性を定期的に確認しなければならない。

第５節　法令遵守

（法令遵守）

第118条　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。

（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26年法律第104号）

第６節　懲戒処分等

（懲戒処分）

第119条　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、地方公務員法第29条第１項による懲戒処分の対象とする。

２　職員等のポリシーに違反する行動を確認した場合、速やかに次の措置を講じなければならない。

（１）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。

（２）情報システム管理者又は情報セキュリティ管理者が違反を確認した場合は、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。

（３）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。

第９章　業務委託

第１節　外部サービスの利用

（委託事業者の選定基準）

第120条　情報セキュリティ管理者及び情報システム管理者は、委託事業者の選定に

当たり、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。

２　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。

（契約項目）

第121条　情報セキュリティ管理者及び情報システム管理者は、情報システムの開発、導入、運用及び保守を業務委託する場合、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。

（１）ポリシー及び情報セキュリティ実施手順等の遵守
（２）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
（３）提供されるサービスレベルの保証
（４）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
（５）委託事業者の従業員に対する教育の実施
（６）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
（７）業務上知り得た情報の守秘義務
（８）再委託に関する制限事項の遵守
（９）委託業務終了時の情報資産の返還、廃棄等
（10）委託業務の定期報告及び緊急時報告義務
（11）町による監査、検査
（12）町による情報セキュリティインシデント発生時の公表
（13）ポリシーが遵守されなかった場合の損害賠償等の規定

（確認及び措置等）

第122条　情報セキュリティ管理者及び情報システム管理者は、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、前条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、その重要性に応じて、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。

第２節　約款による外部サービスの利用

（約款による外部サービスの利用）

第123条　情報セキュリティ管理者は、約款による外部サービスの利用を開始するに当たっては、利用するサービスの約款、その他の提供条件から、リスクが許容できることを確認した上で、統括情報セキュリティ責任者に利用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、約款による外部サービスは、適正な措置を講じた上で利用しなければならない。

３　情報セキュリティ管理者は利用手続き及び運用手順を整備しなければならない。

第３節　ソーシャルメディアサービスの利用

（ソーシャルメディアサービスの利用）

第124条　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。

（１）本町のアカウントによる情報発信が公式アカウントによるものであることを明らかにするために、本町の自己管理ウェブ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己記述欄等にアカウントの運用組織を明示するなどの方法で、なりすまし対策を実施すること。

（２）パスワード、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。

２　機密性２又は３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。

３　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。

４　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

５　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、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こと。

第４節　クラウドサービスの利用

（クラウドサービスの利用）

第125条　情報セキュリティ管理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、本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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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。

第10章　評価及び見直し

第1節　監査

（実施方法）

第126条　情報セキュリティ監査統括責任者は、情報主管課の属する部長を充てる。

２　最高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に情報システム及びネットワーク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、毎年度及び必要に応じて、監査を行うよう指示しなければならない。

（監査を行う者の要件）

第127条　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、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。

２　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者でなければならない。

（監査実施計画の立案及び実施への協力）

第128条　情報セキュリティ監査統括責任者は、監査の実施に当たっては、監査実施計画を立案し、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。

２　被監査部門は、監査の実施に協力しなければならない。

（委託事業者に対する監査）

第129条　委託事業者に業務委託している場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して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。

（報告）

第130条　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、情報セキュリティ委員会に報告する。

（保管）

第131条　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正に保管しなければならない。

（監査結果への対応）

第132条　最高情報セキュリティ責任者は、監査結果を踏まえ、指摘事項がある場合、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。

２　最高情報セキュリティ責任者は、前項と同種の課題及び問題点がある可能性が高い場合、関係する全ての情報セキュリティ管理者に対し、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、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しなければならない。

（情報セキュリティポリシー等の見直し等への活用）

第133条　情報セキュリティ委員会は、監査結果をポリシー及び関係規定等の見直し、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。

第２節　自己点検

（実施方法）

第134条　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、定期的及び必要に応じて、自己点検を実施しなければならない。

２　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、所管する部等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、定期的及び必要に応じて、自己点検を行わなければならない。

（報告）

第135条　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。

（自己点検結果の活用）

第136条　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。

２　情報セキュリティ委員会は、この点検結果をポリシー、関係規定等の見直し、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。

第３節　情報セキュリティポリシー等の見直し

（見直し）

第137条　情報セキュリティ委員会は、情報セキュリティ監査、自己点検の結果、情報セキュリティに関する状況の変化等を踏まえ、ポリシー及び関係規定等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

このポリシーは、平成24年４月１日から施行する。
このポリシーは、平成26年４月１日から施行する。
このポリシーは、平成28年１月１日から施行する。
このポリシーは、令和２年１月１日から施行する。
このポリシーは、令和３年４月１日から施行する。
このポリシーは、令和５年４月１日から施行する。
このポリシーは、令和６年２月１日から施行する。
このポリシーは、令和８年４月１日から施行する。

別表（第19条関係）

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、個人情報の保護に関する法律（平成15年法律第57号）第２条第１項で規定する個人情報に相当する機密性を要する情報資産	・機密性３の情報資産について支給以外の端末での作業を原則として禁止 ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬及び提供時における暗号化及びパスワード設定又は情報資産の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 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録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、東浦町情報公開条例（平成20年東浦町条例第39号）第７条で規定する不開示情報を含む情報資産のうち、機密性３の情報資産を除いたもの。	
機密性１	機密性２又は機密性３以外の情報資産	

※　機密性の高さは順に３、２、１とする。

完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、住民の権利がセキュリティ侵害される又は行政事務の適確な遂行に重大な支障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 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管

完全性１	完全性２以外の情報資産	

※　完全性の高さは順に２、１とする。

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、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利がセキュリティ侵害される又は行政事務の安定的な遂行に重大な支障を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２以外の情報資産	

※　可用性の高さは順に２、１とする。