東串良町情報セキュリティポリシー

東串良町

第1章　情報セキュリティ基本方針

1　目的

本基本方針は、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　定義

(1)　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

(2)　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3)　情報資産

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、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。)並びに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をいう。

(4)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(5)　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(6)　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(7)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(8)　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(9)　情報セキュリティインシデント

望ま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。

(10)　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。

(11)　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。)。

(12)　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。

(13)　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。

(14)　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)　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

(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

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、東串良町課設置条例(昭和 23 年 8 月 14 日東串良町条例第 8 号)に掲げる課、東串良町教育委員会の行政組織等に関する規則(昭和 41 年東串良町教委規則第 1 号)第 25 条に掲げる課、各行政委員会、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

5　職員等の遵守義務

職員、会計年度任用職員、臨時的任用職員及び再任用職員(以下「職員等」という。)は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守することとする。

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

本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

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し、当該分類に基づき情報セキュリティ対策を行う。

(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。

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　原則、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、都道府県と市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

サーバ室等への不正な立入り、情報システム管理上や情報資産への損傷・妨害から保護するために物理的な対策を講じる。

(5)　人的セキュリティ

情報資産に接する職員等の情報セキュリティに関する権限や責任を定め、全ての職員に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じ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

情報資産を不正なアクセス等から適切に保護するため、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

情報セキュリティポリシーの実効性を確保し、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8)　外部サービス(クラウドサービス)の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。約款による外部サービス(クラウドサービス)を利用する場合には、利用にかかる規定を整備し対策を講じる。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。

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、必要に応じて自己点検及び、情報セキュリティ監査を実施する。

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。

11　共同利用等を実施する関係地方公共団体における対策等の協議・調整の実施

上記6、7、8、9及び10に規定する対策等を実施するにあたり、協定による情報システムの共同利用等を実施する関係地方公共団体において、当該対策等に関し、必要に応じて協議・調整を行うものとする。

第2章　情報セキュリティ対策基準

本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を実行に移すための本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を定めたものである。

1　組織・体制

本町の情報セキュリティ管理については、以下の組織・体制とする。

・最高情報セキュリティ責任者・・・・副町長
・統括情報セキュリティ責任者・・・・まちづくり推進課長
・情報セキュリティ管理責任者・・・・情報資産を取り扱う課局の長
・情報システム管理者・・・・・・・・各情報システムを所管する課局の長
・情報システム担当者・・・・・・・・各情報システムを所管する課局の職員等
・情報セキュリティ委員会・・・・・・副町長・総務課長・各課局の長
・情報セキュリティ緊急対策会議(CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。)・・・・・総務課長・情報システム管理者・関係課局の長

(1)　最高情報セキュリティ責任者(CISO：Chief Information Security Officer、以下「CISO」という。)

①　副町長をCISOとする。CISO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。

②　CISO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　CISOは、CSIRTを整備し、その内容について必要に応じて町長に報告する。

(2)　統括情報セキュリティ責任者

① まちづくり推進課長をCISO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CISOを補佐することとする。

② 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権限及び責任を有する。

③ CISOに事故あるとき、又はCISOが欠けたときは、統括情報セキュリティ責任者がその職務を代理する。

④ 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、CISO、統括情報セキュリティ責任者、情報セキュリティ管理責任者、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含めた緊急連絡網を整備することとする。

⑤ 統括情報セキュリティ責任者は、緊急時にはCISO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。

(3) 情報セキュリティ管理責任者

① 情報システムを利用する課局の長を情報セキュリティ管理責任者とする。

② 情報セキュリティ管理責任者は、その所管する課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 情報セキュリティ管理責任者は、その所管する課局において所有している情報資産を管理し、当該情報資産に係る情報セキュリティを確保する。

④ 情報セキュリティ管理責任者は、その所管する課局において、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には、統括情報セキュリティ管理責任者及び情報システム管理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 情報セキュリティ管理責任者は、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) 情報システム管理者

① 情報システムを所管する課局の長を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、情報システム及び情報資産を適切に管理し、情報システムにおける情報セキュリティを確保する。

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。

(5) 情報システム担当者

① 情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

(6) CSIRT

① 統括情報セキュリティ責任者は、情報システム及び情報資産に関する事件及び事故に適切かつ迅速に対応するため、必要に応じCSIRTを設置するものとする。

② 統括情報セキュリティ責任者は、必要に応じてCSIRTを開催し、その議長になる。

③　CSIRT は、統括情報セキュリティ責任者、情報システム管理者及び当該事案に関係する情報セキュリティ管理責任者で構成する。

④　CSIRT は、情報システム及び情報資産に関する事件又は事故発生時の対応及び事件、事故の防止対策について所掌する。

⑤　統括情報セキュリティ責任者は、CSIRT の内容について、必要に応じて CISO に報告するものとする

(7)　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　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。

2　情報資産の分類と管理方法

(1)　情報資産の分類

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、次のとおり分類し、必要に応じ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	・支給以外の端末での作業の原則禁止(機密性 3 の情報資産に対して) ・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磁的記録媒体等の持込禁止 ・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
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	

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 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体等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	

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、指定する時間以内の復旧 ・電磁的記録媒体等の施錠可能な場所への保管
可用性 1	可用性 2 の情報資産以外の情報資産	

(2) 情報資産の管理

① 管理責任

(ア) 情報セキュリティ管理責任者は、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責任者は、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することとする。

② 情報資産の分類の表示

職員等は、情報資産について、格納する電磁的記録媒体、文書の隅等に、必要に応じて取扱制限を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、作成時に(1)の分類に基づき、当該情報の分類と取扱い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することとする。また、情報の作成途上で不要になった場合は、当該情報を消去することとする。

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することとする。

(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責任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、適切な取扱いをすることとする。

(ウ) 情報資産を利用する者は、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は、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥ 情報資産の保管

（ア） 情報セキュリティ管理責任者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管することとする。

（イ） 情報セキュリティ管理責任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責任者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や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保管する場合は、自然災害を被る可能性が低い地域に保管することとする。

（エ） 情報セキュリティ管理責任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の情報を記録した外部電磁的記録媒体を保管する場合、施錠可能な場所に保管することとする。

⑦ 情報の送信

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、必要に応じて暗号化又はパスワード設定を行わなければならない。

⑧ 情報資産の運搬

（ア） 車両等により機密性２以上の情報を運搬する者は、必要に応じて鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、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。

（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責任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以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ） 機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理責任者の許可を得なければならない。

（ウ） 情報セキュリティ管理責任者は、住民に公開する情報資産について完全性を確保することとする。

⑩ 情報資産の廃棄等

（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電磁的記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄することとする。

（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することとする。

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

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することとする。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)を利用することとする。

(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することとする。

(2) LGWAN 接続系

① LGWAN 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することとする。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

(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 都道府県及び町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することとする。

4 物理的セキュリティ

4.1 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、必要な措置を施さなければならない。

(2) サーバの二重化

① 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、同一データを保持することとする。

(3) 機器の電源

① 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源供給する容量の予備電源を備えなければならない。

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

① 情報セキュリティ管理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、配線収容箱を使用する等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、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、連携して対応することとする。

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することとする。

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及び契約により操作を認められた外部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

① 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することとする。

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なければならない。内容を消去できない場合は、情報システム管理者は、外部業者に修理させるにあたり、修理を委託させる事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認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、CISO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することとする。

(7) 機器の廃棄等

情報システム管理者は、機器の廃棄、リース返却等をする場合、機器内部の記録装置から、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。

4．2 管理区域(サーバ室等)の管理

(1) 管理区域の構造等

① 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「サーバ室」という。)や電磁的記録媒体の保管庫をいう。

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、管理区域を地下又は1階に設けてはならない。また、外部からの侵入が容易にできないようにすることとする。

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、施設管理部門と連携して、管理区域から外部に通じ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者の立ち入りを防止することとする。

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、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火対策、防水対策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、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等に影響を与えないようにすることとする。

(2) 管理区域の入退室管理等

① 情報システム管理者は、管理区域の入退室は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録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、求めにより提示することとする。

③ 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者のみ入室さえせることとし、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コンピュータ、モバイル端末、通信回線装置、外部電磁的記録媒体等を持ち込ませないようにすることとする。

(3) 機器等の搬入出

① 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、サーバ室の機器等の搬入出について、事前に管理区域に入室を許可された者のみが入室できるようにすることとする。

4．3 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、適切に管理することとする。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することとする。

② 統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施することとする。

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接続は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。

④ 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。

⑤　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、適切な回線を選択することとする。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。

⑥　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が実施することとする。

⑦　統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

⑧　統括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することとする。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。

4．4　職員等の利用する端末や電磁的記録媒体等の管理

①　情報システム管理者は、盗難防止のため、執務室等で利用するパソコン、モバイル端末及び電磁的記録媒体について、必要に応じて物理的措置を講じなければならない。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することとする。

②　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、パスワードの入力を必要とするように設定することとする。

③　情報システム管理者は、取り扱う情報の重要度に応じて、パスワード以外にICカード等や生体認証等の認証手段のうち二つ以上を併用する認証(多要素認証)を行うよう設定することとする。

④　情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用することとする。電磁的記録媒体についても、データ暗号化機能を備える媒体を使用するよう努めなければならない。

5　人的セキュリティ

5．1　職員等の遵守事項

(1)　職員等の遵守事項

①　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守することとする。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責任者に相談し、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

職員等は、業務以外の目的で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）　CISOは、機密性２以上、可用性2、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。

（イ） 職員等は、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責任者の許可を得なければならない。

（ウ） 職員等は、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責任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

（ア） 職員等は、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、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責任者の許可を得て利用することができる。

（イ） 職員等は、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用いる場合には、情報セキュリティ管理責任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を遵守することとする。

⑤ 持ち出し及び持ち込みの記録

情報セキュリティ管理責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管することとする。

⑥ 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責任者の許可なく変更してはならない。

⑦ ソフトウェアのインストールの禁止

職員等は、パソコン等の端末にソフトウェアをインストール又はアンインストールしてはならない。ただし、業務上必要がある場合は、情報セキュリティ管理責任者にその旨を報告し、許可を受けた上で、ソフトウェア管理を担当する部署に依頼してインストール及びアンインストールすることができる。

⑧ 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び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責任者の許可なく情報を閲覧されることのないようにないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等を容易に閲覧されない場所へ保管する等、適切な措置を講じなければならない。

⑨ 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することとする。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。

(2) 会計年度任用職員及び臨時的任用職員等への対応

① 情報セキュリティポリシー等の遵守

情報セキュリティ管理責任者は、会計年度任用職員及び臨時的任用職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員及び臨時的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 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理責任者は、非常勤及び会計年度任用職員及び臨時的任用職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③　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責任者は、会計年度任用職員及び臨時的任用職員等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することとする。

(3)　情報セキュリティポリシー等の掲示

情報セキュリティ管理責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示することとする。

(4)　委託事業者に対する説明

情報セキュリティ管理責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、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することとする。

5．2　研修・訓練

(1)　情報セキュリティに関する研修・訓練

統括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研修・訓練を実施することとする。

(2)　研修計画の策定及び実施

①　統括情報セキュリティ責任者は、全ての職員等に対する情報セキュリティに関する研修を実施する際は、研修計画の策定とその実施体制を構築することとする。

②　統括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することとする。

③　統括情報セキュリティ責任者は、研修の実施状況を記録し、適切に保管しなくてはならない。

(3)　緊急時対応訓練

CISOは、緊急時対応を想定した訓練を定期的に実施することとする。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、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにすることとする。

(4)　研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加することとする。

5．3　情報セキュリティインシデントの報告

(1)　庁内からの情報セキュリティインシデントの報告

①　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責任者及び情報セキュリティを担当する部署に報告することとする。

②　報告を受けた情報セキュリティ管理責任者は、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することとする。

③　情報セキュリティ管理責任者は、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CISOに報告することとする。

④　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告することとする。

(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

①　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、情報セキュリティ管理責任者に報告することとする。

②　報告を受けた情報セキュリティ管理責任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することとする。

③　情報セキュリティ管理責任者は、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CISOに報告することとする。

(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

①　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、CISOに速やかに報告することとする。

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管理責任者に対し、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。また、CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示することとする。

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、記録を保存することとする。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に報告することとする。

⑤　CISO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することとする。

5．4　ID及びパスワード等の管理

(1)　ICカード等の取扱い

①　職員等は、自己の管理するICカード等に関し、次の事項を遵守することとする。

（ア）　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。

（イ）　業務上必要のないときは、ICカード等をカードリーダから抜いておかなければならない。

（ウ）　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。

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することとする。

③　ICカード等を切り替える場合、管理担当部署の情報セキュリティ管理責任者は、切替え前のカードを回収し、当該のICカード等を初期化することとする。

(2)　IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守することとする。

① 自己が利用しているIDは、他人に利用させてはならない。

② 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、自己の管理するパスワードに関し、次の事項を遵守することとする。

① パスワードは、他者に知られないように管理することとする。

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することとする。

④ 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責任者に速やかに報告し、パスワードを速やかに変更することとする。

⑤ パスワードは定期的に、又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。

⑥ 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。

⑦ 仮のパスワード(初期パスワードを含む。)は、最初のログイン時点で変更することとする。

⑧ 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。

⑨ 職員等間でパスワードを共有してはならない。ただし、共用IDに対するパスワードは除く。

6 技術的セキュリティ

6.1 コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

① 情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知することとする。

② 情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室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、設定することとする。

③ 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り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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにすることとする。

(2) バックアップの実施

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、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、必要に応じて定期的にバックアップを実施することとする。

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、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得することとする。

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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管することとする。

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、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、その仕様を確認することとする。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

認することとする。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管理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

①　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、作業記録を作成することとする。

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、窃取、改ざん等をされないように適切に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

③　統括情報セキュリティ責任者、情報システム管理者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外部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することとする。

(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、適切に管理することとする。

(6)　ログの取得等

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、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、一定の期間保存することとする。

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、取扱方法を定め、適切にログを管理することとする。

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することとする。

(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、適切に保存することとする。

(8)　ネットワークの接続制御、経路制御等

①　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することとする。

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、ネットワークに適切なアクセス制御を施さなければならない。

③　統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保することとする。また、情報セキュリティ対策について、定期的な確認により見直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等

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等

①　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、CISO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することとする。

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することとする。

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、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施することとする。

（ア）　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上で接続することとする。

（イ）　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用することとする。

（ウ）　ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

（エ）　情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定することとする。

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することとする。

(11)　複合機のセキュリティ管理

①　情報セキュリティ管理責任者は、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することとする。

②　情報セキュリティ管理責任者は、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。

③　情報セキュリティ管理責任者は、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。

(12)　IoT 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

①　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は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。

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。

(14)　電子メールのセキュリティ管理

①　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、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することとする。

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することとする。

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することとする。

⑤　統括情報セキュリティ責任者は、システム開発や運用等のため庁舎内に常駐している外部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。

(15)　電子メールの利用制限

①　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することとする。

④　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責任者に報告することとする。

(16)　電子署名・暗号化

①　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、統括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等、セキュリティを考慮して、送信することとする。

②　職員等は、暗号化を行う場合に統括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、統括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することとする。

③　統括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することとする。

(17)　無許可ソフトウェアの導入等の禁止

①　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。

②　職員等は、パソコン等の端末にソフトウェアをインストール又はアンインストールしてはならない。ただし、業務上必要がある場合は、情報セキュリティ管理責任者にその旨を報告し、許可を受けた上で、ソフトウェア管理を担当する部署に依頼してインストール及びアンインストールすることができる。なお、ソフトウェア導入後は、情報セキュリティ管理責任者又は情報システム管理者は、年に1回は、ソフトウェアのライセンス、バージョン及び利用状況を管理することとする。

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。

(18)　機器構成の変更の制限

①　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。

②　職員等は、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、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)　業務外ネットワークへの接続の禁止

①　職員等は、支給された端末を、優先・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責任者は、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制限することが望ましい。

(20)　業務以外の目的でのウェブ閲覧の禁止

①　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責任者に通知し適切な措置を求めなければならない。

(21)　Web会議サービスの利用時の対策

①　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。

②　職員等は、本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。

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ずること。

④　職員等は、外部からWeb会議に招待される場合は、本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

①　情報セキュリティ管理責任者は、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。

(ア) 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。

(イ) 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。

② 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。

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。

6.2 アクセス制御

(1) アクセス制御等

① 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、システム上制限することとする。

② 利用者 ID の取扱い

(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、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 の取扱い等の方法を定めなければならない。

(イ) 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することとする。

(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、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、点検することとする。

(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、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認することとする。

③ 特権を付与された ID の管理等

(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、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することとする。

(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することとする。

(ウ) CISO 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、情報セキュリティ管理責任者及び情報システム管理者に通知することとする。

(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、特権を付与されたID及びパスワードの変更が外部委託事業者によって行われる際は、その内容を把握し、適切な変更内容となっているか確認しなくてはならない。

(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、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することが望ましい。

(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、特権を付与されたIDを初期設定以外のものに変更することとする。

(2)　職員等による外部からのアクセス等の制限

①　職員等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、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。

②　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することとする。

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することとする。

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　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を職員等に貸与する場合、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　職員等は、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接続することとする。

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として禁止することとする。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。

(3)　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、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・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することとする。

(4)　認証情報の管理

①　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することとする。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、これを有効に活用することとする。

② 職員等は、自らパスワード変更が可能なシステムにおいては、初回利用時に発行されたパスワードを変更することとする。

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、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。

(5) 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することとする。

6．3 システム開発、導入、保守等

(1) 機器等の調達に係る運用規程の整備

① 統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備することとする。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策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、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備するよう努めなければならない。

(2) 機器等及び情報システムの調達

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、情報システム開発、導入、保守等の調達にあたっては、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することとする。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載することとする。

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あたっては、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することとする。

(3) 情報システムの開発

① 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することとする。また、システム開発のための規則を確立することとする。

② システム開発における責任者、作業者の ID の管理

(ア) 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 を適切に管理することとする。

(イ) 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。

③ 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

(ア) 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、それ以外のものを利用させてはならない。

(イ) 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することとする。

(4) 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

（ア） 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することとする。

（イ） 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等の影響が最小限になるよう配慮することとする。

（ウ） 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することとする。

② テスト

（ア） 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。

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

（ウ） 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、テストデータとして使用する場合、テスト終了後にテストデータを確実に廃棄しなくてはならない。

（エ） 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。

（オ） 情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

③ 機器等の納入時又は情報システムの受入れ時

（ア） 情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認することとする。

（イ） 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認することとする。

(5) システム開発・保守に関連する資料等の保管

① 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システム関連文書を適切な方法で保管することとする。

（ア） 情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告することとする。

（イ） 情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備することとする。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

（ウ） 情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備することとする。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
・情報セキュリティインシデントを認知した際の対処手順

② 情報システム管理者は、テスト結果を一定期間保管することとする。

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切な方法で保管することとする。

(6) 情報システムにおける入出力データの正確性の確保

① 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することとする。

② 情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施することとする。

(ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直しすることとする。

(イ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(ウ) ウェブアプリケーションやウェブコンテンツにおいて、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することとする。

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することとする。

(7) 情報システムの変更管理

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することとする。

(8) 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することとする。

(9) 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。

(10) 情報システムについての対策の見直し

情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本町内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告することとする。

6．4 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、次の事項を措置することとする。

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することとする。

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することとする。

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、必要に応じ職員等に対して注意喚起することとする。

④ 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。

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もとのサポートが終了する予定がないことを確認することとする。

(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、次の事項を措置することとする。

① 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。

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、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、外部記録媒体等で、データを取り込む際は、事前に当該の外部記録媒体に対しウイルスチェックを行わなくてはならない。

⑤ 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、次の事項を遵守することとする。

① 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。

② 外部から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。

③ 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、速やかに削除することとする。

④　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することとする。

⑤　添付ファイルが付いた電子メールを受信する場合は、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することとする。

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、常に確認することとする。

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、該当の端末においてLANケーブルの即時取り外しや、通信を行わない設定への変更などを実施することとする。

(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、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。

6．5　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、以下の事項を措置することとする。

①　使用されていないポートを閉鎖することとする。

②　不要なサービスについて、機能を削除又は停止することとする。

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、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、設定することとする。

④　統括情報セキュリティ責任者は、情報セキュリティインシデントを予防、感知するため、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築することとする。

(2)　攻撃への対処

CISO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。また、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。

(3)　記録の保存

CISO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することとする。

(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責任者に通知し、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。

6．6　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

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、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有することとする。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することとする。

(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、職員等に周知することとする。

(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収集し、必要に応じ、関係者間で共有することとする。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　運用

7．1　情報システムの監視

(1)　情報システムの運用・保守時の対策

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、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用することとする。

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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な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、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をすることとする。

(2)　情報システムの監視機能

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、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装することとする。

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、情報システムの運用において、情報システムに実装された監視機能を適切に運用することとする。

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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を必要に応じて見直さなければならない。

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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視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することとする。

②　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することとする。

7．2　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

①　情報セキュリティ管理責任者は、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CISO及び統括情報セキュリティ責任者に報告することとする。

②　CISOは、発生した問題について、適切かつ速やかに対処することとする。

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、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することとする。

(2)　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

CISO及びCISO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、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。

(3)　職員等の報告義務

①　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責任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、職員等は、緊急時対応計画に従って適切に対処することとする。

7．3　侵害時の対応

(1)　緊急時対応計画の策定

CISOは、情報セキュリティインシデント、情報セキュリティポリシーの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切に実施するために、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切に対処することとする。

(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。

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

(3)　事業継続計画との整合性確保

自然災害、大規模・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情報セキュリティポリシーの整合性を確保することとする。

(4)　緊急時対応計画の見直し

CISO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。

7．4　例外措置

(1)　例外措置の許可

情報セキュリティ管理責任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、CISO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責任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CISOに報告することとする。

(3)　例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適切に保管すること。

7．5　法令遵守

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)

⑦　東串良町個人情報の保護に関する法律施行条例(令和5年東串良町条例第3号)

7．6　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。

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室等の情報セキュリティ管理責任者に通知し、適切な措置を求めなければならない。

②　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室等の情報セキュリティ管理責任者に通知し、適切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責任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CISO及び当該職員等が所属する課室等の情報セキュリティ管理責任者に通知することとする。

8　業務委託と外部サービスの利用

8．1　業務委託

(1)　業務委託実施前の対策

①　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施することとする。

(ア)　委託する業務内容の特定

(イ)　委託事業者の選定条件を含む仕様の策定

(ウ)　仕様に基づく委託事業者の選定

(エ)　情報セキュリティ要件を明記した契約の締結(契約項目)

情報システムの運用、保守等を業務委託する場合には、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することとする。

・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
・委託先事業者の責任者、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
・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)

(オ) 委託事業者に重要情報を提供する場合は、契約書内に秘密保持に関する条項を入れなければならない。

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を含む事項の実施を必要に応じて、委託事業者に求めなければならない。

(ア) 仕様に準拠した提案

(イ) 契約の締結

(ウ) 委託事業者において重要情報を取り扱う場合は、秘密保持契約(NDA)の締結

(2) 業務委託実施期間中の対策

① 情報セキュリティ管理責任者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施することとする。

(ア) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

(イ) 統括情報セキュリティ責任者へ措置内容の報告(重要度に応じてCISOに報告)

(ウ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

(ア) 情報の適正な取扱いのための情報セキュリティ対策

(イ) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

(ウ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(3) 業務委託終了時の対策

情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことを確認することとする。

8. 2 情報システムに関する業務委託

(1) 情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本町の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定することとする。

(2) 情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

① 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

② 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

(4) 本町向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

① 情報システム管理者又は情報セキュリティ管理責任者は、外部の一般の者が本町向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス(クラウドサービスを除く。)(以下「業務委託サービス」という。)を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

② 情報システム管理者又は情報セキュリティ管理責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定することとする。

③ 情報システム管理者又は情報セキュリティ管理責任者は、委託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することとする。

④ 情報システム管理者又は情報セキュリティ管理責任者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ管理責任者へ当該サービスの利用申請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又は情報セキュリティ管理責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定することとする。

⑥ 統括情報セキュリティ責任者又は情報セキュリティ管理責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名することとする。

8．3 外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱う場合)

(1) クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、機密性2以上の情報を取り扱う場合、以下を含む外部サービス(以下「クラウドサービス」という。)の選定に関する規定を整備しなくてはならない。

① クラウド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基準

② クラウドサービス提供者の選定基準

③ クラウドサービスの利用申請の許可権限者と利用手続

④　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)　クラウドサービスの利用に係る運用規程の整備

クラウドサービスの利用(機密性2以上の情報を取り扱う場合)に係る運用規程は、実施手順：外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱う場合)編に定める。

8．4　外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱わない場合)

(1)　クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、機密性2以上の情報を取り扱わない場合、以下を含むクラウドサービスの利用に関する規定を整備しなくてはならない。

①　クラウドサービスを利用可能な業務の範囲

②　クラウドサービスの利用申請の許可権限者と利用手続

③　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

④　クラウドサービスの利用の運用手順

(2)　クラウドサービスの利用に係る運用規程の整備

クラウドサービスの利用(機密性2以上の情報を取り扱わない場合)に係る運用規程は、実施手順：外部サービス(クラウドサービス)の利用(機密性2以上の情報を取り扱わない場合)編に定める。

9　評価・見直し

9．1　監査

(1)　実施方法

CISO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

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、監査の実施を依頼することとする。

(3)　監査実施計画の立案及び実施への協力

①　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することとする。

②　被監査部門は、監査の実施に協力することとする。

(4)　外部委託事業者に対する監査

外部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、外部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。

(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なければならない。

(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とする。

(7)　監査結果への対応

① CISO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責任者に対し、当該事項への対処(改善計画の策定等)を指示することとする。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示することとする。

② CISOは、指摘事項を所管していない情報セキュリティ管理責任者に対しても、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。また、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(改善計画の策定等)を指示することとする。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示することとする。

(8) 情報セキュリティポリシーの見直し等への活用

統括情報セキュリティ責任者は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用することとする。

9.2 自己点検

(1) 実施方法

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、所管するネットワーク及び情報システムについて、毎年度又は必要に応じ自己点検を実施することとする。

② 情報セキュリティ管理責任者は、所管する課等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、毎年度又は必要に応じ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管理責任者は、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なければならない。

(3) 自己点検結果の活用

① 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 統括情報セキュリティ責任者は、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することとする。