大仙市情報セキュリティポリシー

（第5版）

総務省

地方公共団体における情報セキュリティポリシーに関する

ガイドライン（令和7年 3 月版）対応

令和8年3月

秋田県大仙市

改訂履歴

版数	改訂年月日	改訂履歴
初版	平成17年12月発行 （新規策定）	地方公共団体における情報セキュリティポリシーに関するガイドライン（平成15年3月版）対応
第2版	平成26年 4月改訂 （全面改正）	地方公共団体における情報セキュリティポリシーに関するガイドライン（平成22年11月版）対応
第3版	平成28年 4月改訂	地方公共団体における情報セキュリティポリシーに関するガイドライン（平成27年3月版）対応
第4版	令和4年 12月改訂	地方公共団体における情報セキュリティポリシーに関するガイドライン（令和4年3月版）対応
第5版	令和8年 3月改訂	地方公共団体における情報セキュリティポリシーに関するガイドライン（令和7年3月版）対応

目　次

第1章　総則

本章は、大仙市（以下「本市」という。）の情報セキュリティポリシーを適切に運用、維持及び改善するための仕組みを示すものである。

1.1　情報セキュリティポリシーの目的

本情報セキュリティポリシーは、本市を取り巻く環境を勘案し、市民等の信頼を確保するとともに、地域の情報基盤の充実に貢献するために、本市の保有する情報資産の保護及び正確な行政サービスを提供するための安全対策を確実に実施する目的で策定するものである。

また、地方自治法第 244 条の 6 第 1 項の規定に基づき、本市の議会、長その他の執行機関が管理する情報システムの利用における「サイバーセキュリティを確保するための方針」として位置付け、以下の執行機関において共同で策定するものである。

・市長
・市議会
・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
・地方公営企業の管理者（上下水道事業）
・財産区

（本市を取り巻く環境）

（1）インターネットをはじめ情報技術の急速な普及・発展は、社会経済のあらゆる面に及んでいる。
（2）本市においても、電子自治体化が進み、多くの業務が情報システムやネットワークに依存している現状にある。
（3）官民問わず情報機器からの情報漏えい事件や情報システムの停止、ネットワーク障害等が発生している状況にある。
（4）市民等の大切な個人情報や行政運営上重要な情報を多数保有するとともに、正確な行政サービスを遅延なく提供する責務を担っている。
（5）災害から情報資産を守ることも大きな課題であり、これらの情報資産を様々な脅威から防御することは、極めて重要である。

1.2 情報セキュリティの基本的な考え方

1.2.1 情報セキュリティとサイバーセキュリティの定義

「情報セキュリティ」とは、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。「サイバーセキュリティ」とは、情報システム及び情報通信ネットワークの安全性及び信頼性を確保し、サイバー攻撃等の脅威から情報資産を保護することをいう。

本市は、情報システム及び情報通信ネットワークが市民生活の基盤であることを深く

認識し、サイバーセキュリティの確保を地方自治法上の法的義務として、組織を挙げて取り組まなければならない。

(1)情報セキュリティ対策に取り組むための全庁的な体制を確立する。
(2)情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。
(3)本市の保有する情報資産を適切に管理する。
(4)情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するため、職員等に対して必要な教育を実施する。
(5)情報セキュリティに関する事故が発生した場合又はその予兆があった場合において速やかに対応するため緊急時対応計画を定める。
(6)情報セキュリティ対策の実施状況検証のため、情報セキュリティ点検及びセルフチェック等を通して、定期的に対策の見直しを実施する。
(7)すべての職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を順守する。
(8)地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。
(9)法規の改正があった場合には、本ポリシーを適切に見直しする。

1.3 情報セキュリティポリシーの構成

情報セキュリティポリシーの体系は、図1に示す階層構造とする。

(1)基本方針:情報セキュリティ対策における基本的な考え方を定めたものである。
(2)対策基準:基本方針に基づき、庁内共通の情報セキュリティ対策の基準を定めたものである。
(3)実施手順:必要により対策基準に基づいた具体的な手順や手続を定めたものである。

なお、情報セキュリティポリシーは、すべての職員等及び委託事業者が、業務の遂行に当たって順守する義務を負うものである。

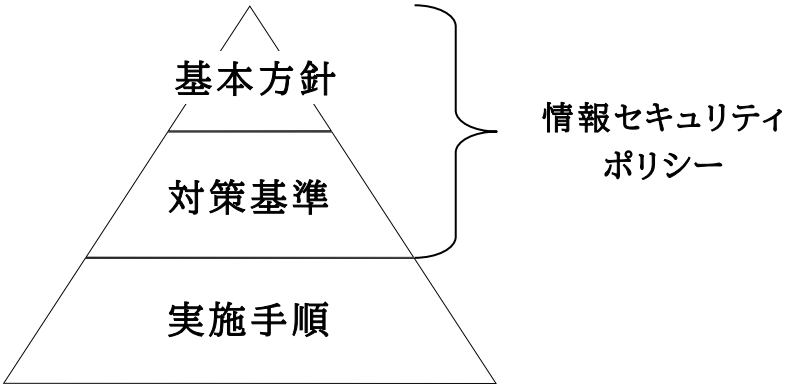


図1 情報セキュリティポリシーの体系

1.4 情報セキュリティの実施サイクル

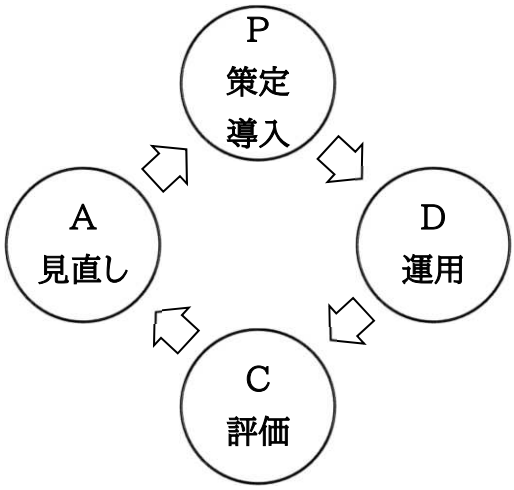


図2 実施(PDCA)サイクル

情報セキュリティを取り巻く環境は常に変化していることから、本サイクルを定期的に実行する。

P:Plan(策定・導入)

情報セキュリティポリシー・実施手順の策定、周知

D:Do(運用)

対策の実施、障害時の対応

C:Check(評価)

情報セキュリティ点検、セルフチェック

A:Action(見直し)

情報セキュリティポリシー・実施手順の見直し

1.5 策定と導入(P)

1.5.1 策定及び導入の概要

情報セキュリティポリシーの策定及び導入は、以下の手順により実施する。

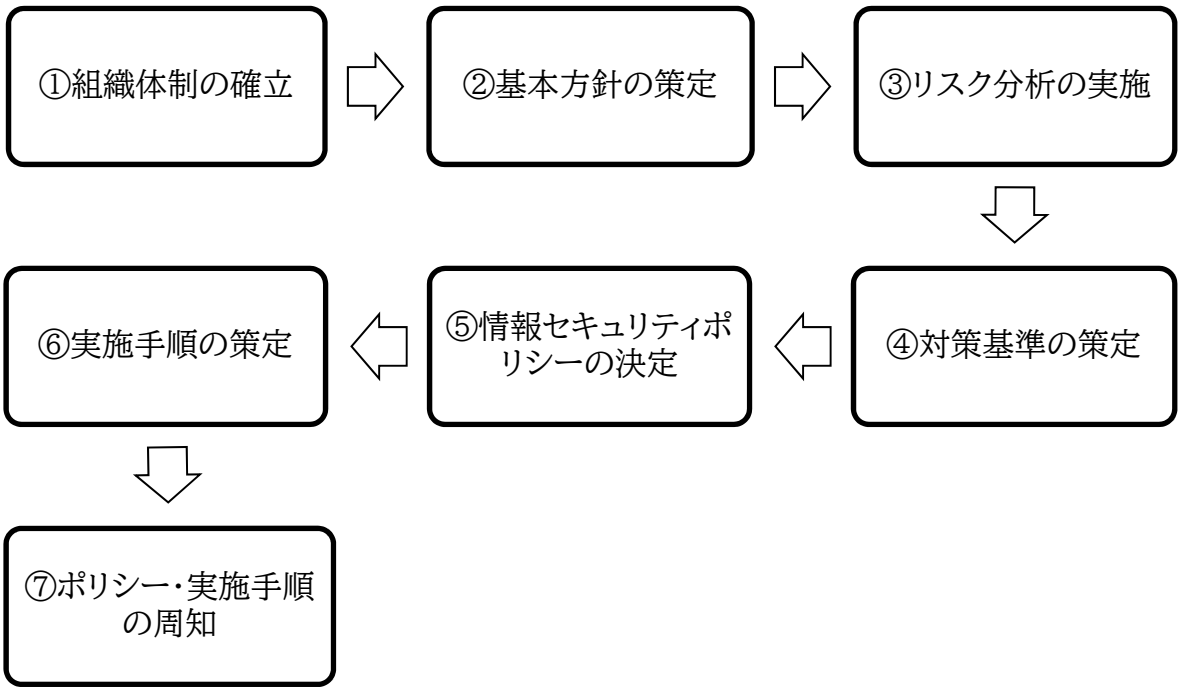


図3 策定及び導入の手順

1.5.2 組織体制の確立

本市は、情報セキュリティポリシーを運用するに当たり、組織内の様々な情報資産を取り扱うため、責任の所在を明確にし、すべての部局支所の長、情報システムを所管する課等の長及び情報セキュリティに関する専門的知識を有する者などで構成する組織体制を確立する。本市における組織体制を、「付録A 組織体制」に示す。

1.5.3 情報セキュリティ基本方針の策定

「第2章 情報セキュリティ基本方針」において、情報セキュリティ対策の目的、体系等、本市の情報セキュリティに対する基本的な考え方を示す。

1.5.4 リスク分析の実施

リスク分析とは、本市が保有する情報資産を明らかにし、それらに対するリスクを評価することである。

手順概略

（概略1）本市が保有する情報資産を調査の上、重要性（C：機密性、I：完全性、A：可用性）の分類を行い、その結果に基づき、要求されるセキュリティの水準を定める。

（概略2）本市の情報資産を取り巻く脅威の調査を行い、その発生の可能性及び発生した際の被害の大きさからリスクの大きさを求める。

（概略3）リスクに対応した対策基準を策定し、適切なリスク管理を行う。

なお、情報資産や情報資産に対するリスクに大きな変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果、情報セキュリティポリシーの見直しが必要と判断される場合には、その見直しを行う。また、定期的な情報セキュリティポリシーの評価及び見直しの際にもリスク分析から実施する。

リスク分析に関する資料は、情報セキュリティポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性に関する事項が記載されているため、厳重に管理するものとする。

1.5.5 情報セキュリティポリシーの対策基準の策定

リスク分析の結果得られる情報セキュリティ要求水準に対して、それを実現するための順守事項や判断基準等を、「第3章 情報セキュリティ対策基準」に定める。情報セキュリティ対策基準は、想定される情報リスクに十分に対処し、情報セキュリティ要求水準を満たすものとする。

1.5.6 情報セキュリティポリシーの決定

最高情報セキュリティ責任者（CISO: Chief Information Security Officer 、以下「CISO 」という。）の決裁により、本市における情報セキュリティポリシーとして正式に決定する。

1.5.7 実施手順の策定

実施手順は、職員等関係者が、それぞれ扱うネットワーク及び情報システムに携わる業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるものである。この実施手順には、主要な情報資産に対するセキュリティ対策実施手順も含まれる。

なお、実施手順は、個別の目的のために作成し、見直し等を柔軟に行っていくため、業務担当課において情報システムや情報資産を管理する者が必要に応じ策定する。

1.5.8 情報セキュリティポリシー及び実施手順の周知

情報セキュリティ対策を最終的に実施するのは職員等である。実効性を確保するため、情報セキュリティポリシー及び共通実施手順の配布や研修会などにより、職員等に十分に周知する。

また、個別目的のための実施手順については、業務担当課の責任者が当該手順を実行する者に周知する。

1.6 運用(D)

情報セキュリティポリシーを確実に運用していくため、情報システムの監視や情報セキュリティポリシーに従って対策が適切に順守されているか否かの確認を行い、情報資産に対する侵害や情報セキュリティポリシー違反に対し、適正に対応する。このため、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直し等を実施する。

1.7 評価・見直し(C, A)

情報セキュリティポリシーの実効性を確保するとともに、情報資産や情報システム等の変化、情報セキュリティに関する脅威や対策等の変化に対応していくため、情報セキュリティポリシーの評価・見直しを行い、前述のPDCAサイクル(1.4 図2参照)を繰り返し、情報セキュリティ対策を継続的に強化し続ける。

1.7.1 情報セキュリティ点検・セルフチェック(C)

情報セキュリティ対策の実効性を確保し、実施状況を検証し、情報セキュリティポリシーの見直しに反映させるため、独立かつ専門的知識を有する専門家(部内者であっても点検対象から独立した点検担当者等が行う場合を含む。)による情報セキュリティ点検や情報システム等を運用するもの自らによるセルフチェックを行う。

1.7.2 情報セキュリティポリシーの見直し(A)

情報セキュリティ点検の結果、セルフチェックの結果及び情報セキュリティに関する環境の変化を踏まえ、情報セキュリティポリシーの見直しの必要性を評価し、改正の要否、具体的な対応方法を定める。

その結果を基に、前述のPDCAサイクル(1.4 図2参照)の策定と導入(P)へ必要な情報を提供する。

第2章　情報セキュリティ基本方針

2.1 目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市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。

2.2 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）情報セキュリティポリシー

情報の目的外使用や外部からの侵入、情報漏えいなどを防止するための方針を定めたもので、本基本方針及び情報セキュリティ対策基準からなる。

（5）機密性

情報にアクセス（データの書き込み又は読み出し）することを正当に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。

（6）完全性

情報が破壊、改ざん又は消去されていない状態及び情報が正確なことを確保することをいう。

（7）可用性

情報にアクセスすることが正当に認められた者が、必要なとき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。

（8）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。

（9）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。）。

（10）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。

（11）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。

（12）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。

(13)外部サービス

民間事業者等の庁外の組織がインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うもののこと。クラウドサービス、Web 会議サービス等の全般を指す。

(14)サイバー攻撃

情報通信ネットワークを通じて行われる、情報の破壊、漏えい、改ざん、システムの機能停止等を目的とした攻撃をいう。

(15)サイバーセキュリティ

情報システム及び情報通信ネットワークの安全性及び信頼性を確保し、サイバー攻撃等の脅威から情報資産を保護することをいう。

その他の用語については、「付録B 用語集」を参照のこと。

2.3 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)有形・無形を問わず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・外部点検機能の不備、委託管理の不備、管理及び運用の欠陥、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提供サービスの障害からの波及等

2.4 適用範囲

(1)適用の範囲

本基本方針の適用範囲は、次のいずれかの条件を満たす職員等とする。

① 本市が管理するネットワークを利用する場合
（マイナンバー利用事務系、LGWAN 接続系、インターネット接続系）
② 機密性2以上の市の情報資産を取り扱う場合

(2)情報資産の範囲

本基本方針が対象とする情報資産は、以下のとおりとする。

①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
②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
③情報システムの仕様書及びネットワーク図等のシステム関連文書

2.5 職員等の遵守義務

職員、会計年度職員等（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、業務の遂行に当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しなければならない。

2.6 情報セキュリティ対策

2.3 の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

（1）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。また、サイバーセキュリティを確保するため、サイバー攻撃等のインシデントに即応する体制を整備する。（付録A 組織体制 参照）

（2）情報資産の分類と管理

本市が保有する情報資産を機密性、完全性、可用性及び重要性に応じて分類し、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。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、秋田県及び県内市町村のインターネット接続口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、情報センター、通信回線及び職員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、職員等が順守すべき事項を定めるとともに、十分な教育及び啓発を行う等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、アクセス制限、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、情報セキュリティポリシーの順守状況の確認、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。特に、地方自治法に基づき、サイバーセキュリティ確保のために必要な措置を継続的に講じなければならない。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応する

ため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。特に再委託（再々委託以降を含む。）が行われる場合には、本市による事前の承認を必須とし、委託事業者を通じて、再委託先においても本市と同等のセキュリティ対策が講じられていることを確認し、責任の所在を明確にしなければならない。

外部サービス（クラウドサービス）を利用する場合には、ISMAP（政府情報システムのためのセキュリティ評価制度）登録サービス等の客観的な安全評価基準を活用して安全性を確認した上で、対策を講じる。また、サービス提供事業者と本市との間における責任分界点（データ保護、障害対応等の責任範囲）を明確にしなければならない。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて外部専門家による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。CISO は、地方自治法に基づくサイバーセキュリティ確保の状況を適宜評価し、情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

2.7 情報セキュリティ点検及びセルフチェック

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ点検及びセルフチェックを実施する。

2.8 情報セキュリティポリシーの見直し

情報セキュリティ点検及びセルフチェックの結果、情報セキュリティポリシーの見直しが必要と判断され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。

2.9 情報セキュリティ対策基準の策定

2.6、2.7 及び 2.8 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。

2.10 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手順を定める必要がある場合、具体的に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市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第3章　情報セキュリティ対策基準

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

3.1 適用範囲

（1）適用の範囲

本対策基準が適用される範囲は、2.4 適用範囲 (1)適用の範囲に示す。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、2.4 適用範囲 (2)情報資産の範囲に示す。

3.2　組織体制

（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市長が指名する副市長を最高情報セキュリティ責任者（CISO）とする。CISOは、本市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・サイバーセキュリティ確保に関する最終決定権限及び責任を有する。

②CISO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。

③CISO 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。

④CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISOの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）1人を必要に応じて置く。

⑤CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

⑥CISOは、最高情報統括責任者（CIO）と兼務することができる。

（2）統括情報セキュリティ責任者

①情報政策担当部長を 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 及び副 CISO を補佐しなければならない。

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

③統括情報セキュリティ責任者は、本市の全てのネットワークシステムにおける情報セキュリティ対策に関する権限及び責任を有する。

④統括情報セキュリティ責任者は、情報セキュリティ責任者（部局支所の長）、情報セキュリ

ティ管理者（課等の長）、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指示を行う権限を有する。

⑤統括情報セキュリティ責任者は、本市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恐れがある場合には、CISO の指示に従い、又は CISO が不在のときには自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

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

⑦ 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、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。

⑧ 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。

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

（3）情報セキュリティ責任者

①内部部局、各支所、各行政委員会事務局及び各公営企業局の長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、所管する部局支所の情報セキュリティ対策に対する総括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局支所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、見直し等を行う総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、所管する部局において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

（4）情報セキュリティ管理者

①内部部局、内部部局の出先機関及び各支所、各行政委員会事務局及び各地方公営企業の課等の長を、情報セキュリティ管理者とする。但し、情報セキュリティ管理者に相当する者がいない場合には、情報セキュリティ責任者がその職を兼ねる。

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

③情報セキュリティ管理者は、その所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恐れがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO に対し速やかに報告を行い、指示を仰がなければならない。

（5）情報システム管理者

①情報システム担当課長を、情報システムに関する情報システム管理者とする。なお、各課等独自で導入し、所管しているシステムがある場合、当該システムに限り、当該課等の情報セキュリティ管理者が情報システム管理者となり、情報システム担当者相当の要員を当該課内で任命し、維持管理しなければならない。

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

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

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

（6）情報システム担当者

情報システム管理者の指示等に従い、ネットワーク及び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。

（7）情報セキュリティポリシー推進事務局

①情報システム担当課を情報セキュリティポリシー推進事務局とする。

②本市の情報セキュリティ対策を統一的に行うため、情報セキュリティポリシー推進事務局において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を統括情報セキュリティ責任者と協議し、CISO の承認により決定する。

③情報セキュリティポリシー推進事務局は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

（8）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情報セキュリティ点検の実施において、やむを得ない場合を除き、情報セキュリティ点検を受ける者とその情報セキュリティ点検を実施する者は、同じ者が兼務してはならない。

（9）CSIRT の設置・役割

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

②CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置くこと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ることなければならない。

③CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティ事故について部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

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

⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、秋田県等へ報告しなければならない。

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

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

3.3 情報資産の分類と管理方法

(1) 情報資産の分類

本市における情報資産は、機密性、完全性、可用性及び重要性の度合により、以下のとおり分類し、必要に応じ取扱制限を行うものとする。

①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3A	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有する文書	・ 情報システム担当課にて支給する端末以外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ち込み禁止 ・ 情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や安全対策の実施 ・ 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対策の実施 ・ 電磁的記録媒体の施錠可能な場所への保管
機密性3B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
機密性3C	行政事務で取り扱う情報資産のうち、機密性3B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
機密性2	行政事務で取り扱う情報資産のうち、機密性3に相当する機密性は有しないが、直ちに一般に公表することを前提としていない情報資産	
機密性1	機密性2又は機密性3の情報資産	―

分類	分類基準	取扱制限
	以外の情報資産	

②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、又は行政事務の適正な遂行に支障（軽微なものを除く。）を及ぼす恐れがある情報資産	・バックアップの実施 ・電子署名付与の実施（例：電子公印） ・外部で情報処理を行う際の安全対策 ・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の情報資産以外の情報資産	―

③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。）を及ぼす恐れがある情報資産	・バックアップ及び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）情報資産が複製又は送信された場合には、複製等された情報資産も（1）の分類に基づき管理しなければならない。複製等を提供する側は、提供先に対し、取扱い上の要求を明確にし、指示しなければならない。

②情報資産の分類の表示

職員等は、特に機密性3に該当する情報資産について、ファイル（ファイル名、ファイルの属性、ヘッダー・フッター等）、格納する記憶媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。但し、第三者が重要性の識別を容易に認識できないよう留意しなければならない。

特に文書を取り扱う際、「大仙市文書取扱規程」を確実に遵守しなければならない。

③情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

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

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流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、当該情報を確実に消去しなければならない。

④情報資産の入手

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

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

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

⑤情報資産の利用

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

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

（ウ）情報資産を利用する者は、記憶媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記憶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又は情報システム管理者は、機密性２以上、完全性２及び可用性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、耐水又は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。

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以上の情報資産を運搬する者は、必要に応じ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者の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。必要により守秘義務に関する文書を交わさなければならない。

（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者に許可を得なければならない。

（ウ）情報セキュリティ管理者は、「大仙市情報公開条例」及び関連例規を遵守し、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。

⑩情報資産の廃棄

（ア）情報資産の廃棄を行う者は、情報を記録している記憶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、電磁的記憶媒体の情報を復元できないように処置した上で廃棄しなければならない。

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

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

3.4　情報システム全体の強靭性の向上

（1）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先と接続する場合や、画面転送技術等により信頼される特定先と接続する場合はこの限りではない。

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

また、業務毎に専用端末を設置することが望ましい。

（イ）情報の持ち出し不可設定

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

（2）LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要

な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

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

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

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

②(α´モデルを採用する場合)LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の業務端末から、主に外部のクラウドサービス(SaaS 等)の利用を目的として、接続先に直接接続(ローカルブレイクアウト)する構成(α´モデル)を採用する場合は、次の措置を講じなければならない。

(ア)利用可能なサービスの制限

原則として、ISMAP(政府情報システムのためのセキュリティ評価制度)管理基準を満たし、クラウドサービスリストに登録されているサービスでなければならない。

(イ)通信の制御と制限

許可したサービス以外への通信を確実に遮断するため、接続先制限(URL フィルタリング等)やテナントアクセス制御等の技術的対策

(ウ)データの保護

通信経路の暗号化

(エ)DDoS 攻撃への対策

サービス不能攻撃(DDoS 攻撃)による被害を最小化するため、対策機器の導入等の対策実施

(オ)外部監査

システムの導入前及び導入後に、必要なセキュリティ対策が適切に講じられているかについて専門家による外部監査

(カ)α'モデルにおいて利用するクラウドサービスへのアクセス状況やアプリケーション利用状況のログを常に取得・保存し、異常がないかの状態監視

(キ)クラウドサービスを利用しインターネットメールを受信する場合は、受信メールの本文テキスト化や、添付ファイルのサニタイズ(無害化)

(ク)クラウドサービスにおいてインターネットメール以外の Web 会議システムやファイル管理システムを通じて外部とファイルの共有・受け取りを行わない場合、クラウドサービス上から業務端末へのファイルダウンロードを制限する対策

(ケ)クラウドサービスにおいてインターネットメール以外の Web 会議システムやファイル管理システムを通じて外部とファイルの共有・受け取りを行う場合は、LGWAN 接続系端末にファイルを取り込む前にファイル無害化処理

(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秋田県及び県内市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、関係省庁や秋田県と連携しながら、情報セキュリティ対策を推進しなければならない。

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

3.5 物理的セキュリティ

3.5.1 サーバ等の管理

(1)機器の取付け

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

(2)サーバの冗長化

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、同一データを保持しなければならない。

②情報システム管理者は、メインサーバに障害が発生した場合、可能な限りシステムの運用停止時間を最小限にしなければならない。

(3)機器の電源

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統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するため、配線収納管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には、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、ネットワーク接続口（HUBのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

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しなければならない。

②情報システム管理者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合、原則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。

（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には、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しなければならない。

（7）機器の廃棄等

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には、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。

3.5.2 管理区域の管理

（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、当該機器等の管理及びに運用を行うための部屋や電磁的記憶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、管理区域を外部からの侵入が容易にできないような区域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、生体認証や施錠等による入退室管理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、管理区域内の機器等に、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。

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、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を可能な限り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、管理区域に配置する消火薬剤や消防用設備等が、機器及び記憶媒体等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

①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、生体認証等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、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

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、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

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事業者による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、職員を立ち会わせなければならない。

3.5.3 通信回線及び通信回線装置の管理

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

②統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定

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、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④統括情報セキュリティ責任者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適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。

①統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑥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しなければならない。また、必要に応じ、回線を冗長化する等の措置を講じなければならない。

3.5.4 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のパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を可能な限り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しなければならない。

②情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカードあるいは生体認証等複数の認証情報の入力を必要となる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、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。

3.6 人的セキュリティ

3.6.1 職員等の遵守事項

（1）職員等の順守事項

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禁止

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。

③パソコン等の端末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及び完全性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、本市のパソコン等の端末、電磁的記憶媒体、情報資産及びソフトウェアを市が管理する庁舎・施設での使用以外を目的として持ち出す場合には、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）職員等は、市が管理する庁舎・施設以外で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

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、支給以外の端末の業務利用の可否判断をCISO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。

（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。

⑤持ち出し及び持ち込みの記録

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

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管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記憶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者の許可なく情報を閲覧されることがないように、端末の配置、離席時のパソコン、モバイル端末のロックや電磁的記憶媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑧管理区域外での情報機器の管理

職員等は、管理区域外に携行する情報機器（パソコン、業務連絡やカメラ機能等を使用する公用の携帯電話やスマートフォンホン、タブレット端末及びデジカメやボイスレコーダー）に対し、紛失・盗難・漏えい等による被害を受けないように適切な措置を講じなければならない。

⑨退職時等の順守事項

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

ない。

(2)会計年度任用職員等への対応

①情報セキュリティポリシー等の順守

情報セキュリティ管理者は、非常勤及び臨時職員等に対し、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者は、会計年度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電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3)情報セキュリティポリシー等の掲示

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

(4)委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー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。

3.6.2 研修・訓練

(1)情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(2)研修計画の立案及び実施

①CISO 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計画の策定とその実施体制の構築を定期的に行い、情報セキュリティポリシー推進事務局に実施させなければならない。

②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、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、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に対して、報告しなければならない。

⑥統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

⑦CISO は、毎年度1回、情報セキュリティポリシー推進事務局に対して、職員等の情報セキュリティ研修の実施状況について確認しなければならない。

(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させなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4)研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

3.6.3 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

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、情報システム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。

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、CISO 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。

(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、本市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者に報告しなければならない。

②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 CISO 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 CISO 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。

(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

①CSIRT 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。

②CSIRT 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 に速やかに報告しなければならない。

③CSIRT 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。

④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

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しなければならない。

3.6.4 ID及びパスワード等の管理

(1)ICカード等の取り扱い

①職員等は、自己管理するICカード等に関し、以下の事項を遵守しなければならない。

(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又はパソコン等の端末のスロット等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カードを速やかに使用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カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2)IDの取扱い

職員等は、自己管理する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、自己管理するパスワードに関し、以下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。

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）。

⑨職員等は、パスワードによる認証に加え、生体認証や所持品認証等の多要素認証を組み合わせるよう努めなければならない。なお、システムの仕様により多要素認証が困難な場合は、パスワードの複雑性を高める等の代替措置を講じるものとする。

3.7 技術的セキュリティ

3.7.1 コンピュータ及びネットワークの管理

（1）共有ファイルサーバの設定等

①情報システム管理者は、職員等が使用できる共有ファイルサーバの容量を設定し、周知しなければならない。

②情報システム管理者は、共有ファイルサーバを課等の単位で構成し、職員等が他課等のフォルダや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、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、別途フォルダを作成する等の措置を講じ、同一課等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（2）バックアップの実施

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、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

(3)他団体との情報システムに関する情報等の交換

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

(4)システム管理記録及び作業の確認

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に適切に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、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委託事業者がシステム変更等の作業を行う場合は、原則2名以上で作業し、互いにその作業を確認しなければならない。

(5)情報システム仕様書等の管理

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

(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。

(7)障害記録

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

(8)ネットワークの接続制御、経路制御等

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。

（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、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

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原則として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、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した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には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（11）複合機のセキュリティ管理

①統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティ事故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

①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、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、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

③統括情報セキュリティ責任者は、LGWAN 接続系において無線 LAN を利用する場合は、次の対策を講じなければならない。

（ア）WPA2 又は WPA3 による高度な暗号化規格を採用すること。

（イ）認証サーバを利用した WPA2/WPA3 エンタープライズ方式を採用し、ID・パスワードによらないクライアント証明書による機器認証を行うこと。

（ウ）アクセスポイントにおける無線端末同士の通信を禁止する設定を行うこと。

④統括情報セキュリティ責任者は、マイナンバー接続系において無線 LAN を利用する場合は、次の対策を講じなければならない。

（ア）WPA2 又は WPA3 による高度な暗号化規格を採用すること。

（イ）認証サーバを利用した WPA2/WPA3 エンタープライズ方式を採用し、ID・パスワードによらないクライアント証明書による機器認証を行うこと。

（ウ）アクセスポイントにおける無線端末同士の通信を禁止する設定を行うこと。

（エ）特定個人情報の安全管理措置として無線 LAN 利用を許可する職員をリスト化し、厳格に管理すること。

（オ）特定個人情報の安全管理措置としてアクセスポイントや認証システムを、第三者が容易に触れられない高所や施錠管理された場所に設置すること。

（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、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ボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

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適正な措置を講じなければならない。

(15)電子メールの使用制限

①職員等は、原則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、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(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、CISO 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、送信しなければならない。

②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、最高情報セキュリティ責任者が定めた方法で暗号のための鍵を管理しなければならない。

(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。

②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンス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。

(18)機器構成の変更の制限

①職員等は、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)業務外での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、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制限しなければならない。

（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、本市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、Web 会議サービスを利用する際、機密性2以上の情報資産を取り扱ってはならない。

⑤情報システム管理者は、Web 会議サービスを適正に実施するために Web 会議用パソコン等、ネットワーク環境を整備すること。

（22）テレワーク実施時の対策

①統括情報セキュリティ責任者は、テレワークを適正に実施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、本市の定める利用手順に従い、テレワーク実施時の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情報システム管理者は、テレワークを適正に実施するためにテレワーク用パソコン等の整備、不要な接続を制限するようネットワーク環境を整備すること。

（23）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者は、本市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）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理 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（ICカード等）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、本市の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

3.7.2 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、システムの上制限をしなければならない。

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しなければならない。

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

(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し、CISO が認めた者でなければならない。

(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、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

(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について、委託事業者に原則行わせてはならな

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可能な限り強化しなければならない。

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

（2）職員等による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パソコンやモバイル端末を職員等に貸与する場合には、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パソコンや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や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、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、パスワード及び生体認証に係る情報等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。

（3）自動識別の設定

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

（4）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、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しなければならない。

(5)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しなければならない。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。

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、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

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、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。

(6)特権による接続時間の制限

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

3.7.3 システム開発、導入、保守等

(1)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。

(2)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しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者のID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を管理し、開発完了後、開発用IDを削除しなければならない。

(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なければならない。

（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には、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。

（3）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とシステム運用環境を原則として分離しなければならない。

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

（ウ）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しなければならない。

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

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は、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には、あらかじめ擬似環境による操作確認を原則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に使用してはならない。

（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。

（4）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正に整備・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。

（5）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に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

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。

(6)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は、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。

(7)開発・保守のソフトウェアの更新等

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

(8)システム更新又は統合時の検証等

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

3.7.4 不正プログラム対策

(1)統括情報セキュリティ責任者の措置事項

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

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、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

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しなければならない。

④所管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元のサポートが終了する予定がないことを確認しなければならない。

(2)情報システム管理者の措置事項

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

① 情報システム管理者は、その所管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及び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、電磁的記憶媒体を使う場合、コンピュータウイルス等の感染を防止するため、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

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、以下の事項を遵守しなければならない。

① パソコンやモバイル端末において、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、速やかに削除しなければならない。

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しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。

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、該当の端末において 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。

(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。

3.7.5 不正アクセス対策

(1)統括情報セキュリティ責任者の措置事項

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

①使用されていないポートを閉鎖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、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう設定しなければならない。

④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

(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、秋田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庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5)職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正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。

3.7.6 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、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、職員等に周知しなければならない。

(3)情報セキュリティに関する技術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、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

3.8 運用

3.8.1 情報システムの監視

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

②統括情報セキュリティ責任者及び情報システム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

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

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

3.8.2 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情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 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。

②CISO は、発生した問題について、適切かつ速やかに対処しなければならない。

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、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。

(2)パソコン、モバイル端末及び電磁的記憶媒体などの利用状況調査

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等の端末、記憶媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

(3)職員等の報告義務

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には、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しなければならない。

3.8.3　侵害時の対応

(1)緊急時対応計画の策定

CISO 又は情報セキュリティポリシー推進事務局は、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への侵害が発生した場合又は発生する恐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正に対処しなければならない。

(2)緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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)業務継続計画との整合性確保

本市が自然災害、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、情報セキュリティポリシー推進事務局は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4)緊急時対応計画の見直し

CISO 又は情報セキュリティポリシー推進事務局は、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。

3.8.4　例外措置

(1)例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用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、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 に報告しなければならない。

(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しなければならない。

3.8.5 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、以下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大仙市個人情報保護条例(平成17年条例第20号)等の本市条例・規則
⑥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)
⑦サイバーセキュリティ基本法(平成26年法律第104号)

3.8.6 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」及び「大仙市職員の懲戒処分等の審査に関する規程」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等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
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は、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。

3.9 業務委託と外部サービスの利用

3.9.1 業務委託

(1)委託先の選定基準

①情報セキュリティ管理者は、委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

(2)契約項目

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しなければならない。

①情報セキュリティポリシー及び実施手順の遵守
②委託先の責任者、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市による情報セキュリティ点検、検査
⑫市による情報セキュリティインシデント発生時等の公表
⑬情報セキュリティポリシーが遵守されなかった場合の損害賠償等の規定

(3)確認・措置等

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

3.9.2 外部サービスの利用(機密性2以上の情報を取り扱う場合)

(1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス(機密性2以上の情報

を取り扱う場合）の利用に関する規定を整備すること。

①外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）

②外部サービス提供者の選定基準

③外部サービスの利用申請の許可権限者と利用手続

④外部サービス管理者の指名と外部サービスの利用状況の管理

（2）外部サービスの選定

①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

②情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

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

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

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

（エ）外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に 関する情報提供

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

④情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

⑥情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分

に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提 供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

⑧情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

⑨統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

（3）外部サービスの利用に係る調達・契約

①情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

（4）外部サービスの利用承認

① 情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

（5）外部サービスを利用した情報システムの導入・構築時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

(ア)不正なアクセスを防止するためのアクセス制御

(イ)取り扱う情報の機密性保護のための暗号化

(ウ)開発時におけるセキュリティ対策

(エ)設計・設定時の誤りの防止

②外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確

認・記録すること。

（6）外部サービスを利用した情報システムの運用・保守時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

(ア)外部サービス利用方針の規定

(イ)外部サービス利用に必要な教育

(ウ)取り扱う資産の管理

(エ)不正アクセスを防止するためのアクセス制御

(オ)取り扱う情報の機密性保護のための暗号化

(カ)外部サービス内の通信の制御

(キ)設計・設定時の誤りの防止

(ク)外部サービスを利用した情報システムの事業継続

②情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

③外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

（7）外部サービスを利用した情報システムの更改・廃棄時の対策

① 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

(ア)外部サービスの利用終了時における対策

(イ)外部サービスで取り扱った情報の廃棄

(ウ)外部サービスの利用のために作成したアカウントの廃棄

②外部サービス管理者は、前項において定める規定に対し、外部サービスの提供の停止や終了、又は契約解除時において、市が保有するデータを確実かつ速やかに回収・消去する方法をあらかじめ定義し、業務継続性に支障をきたさないよう代替手段の検討やバックアップの取得を行わなければならない

3.9.3 外部サービスの利用（機密性2以上の情報を取り扱わない場合）

(1)外部サービスの利用に係る規定の整備

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

(ア)外部サービスを利用可能な業務の範囲

(イ)外部サービスの利用申請の許可権限者と利用手続

(ウ)外部サービス管理者の指名と外部サービスの利用状況の管理

(エ)外部サービスの利用の運用手順

(2)外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性2以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

②情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

3.10 評価・見直し

3.10.1 情報セキュリティ点検

情報セキュリティ点検は、以下の目的により実施するものである。

①情報セキュリティポリシーが、適切に運用されている確証を得るため

②情報セキュリティポリシーが、実際の環境に適切なものであるかを確認するため

(1)実施方法

CISO は、情報セキュリティ点検責任者を指名し、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、毎年度及び必要に応じて情報セキュリティ点検を行わせなければならない。

(2)情報セキュリティ点検を行う者の要件

①情報セキュリティ点検責任者は、情報セキュリティ点検を実施する場合には、被点検部門から独立した者に対して、情報セキュリティ点検の実施を依頼しなければならない。

②情報セキュリティ点検を行う者は、情報セキュリティ点検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。

(3)情報セキュリティ点検実施計画の立案及び実施への協力

①情報セキュリティ点検責任者は、情報セキュリティ点検を行うに当たって、情報セキュリティ点検実施計画を立案し、CISO の承認を得なければならない。

②被点検部門は、情報セキュリティ点検の実施に協力しなければならない。

(4)委託事業者に対する情報セキュリティ点検

委託事業者に委託している場合、情報セキュリティ点検責任者は委託事業者から下請け(もしくは再委託)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情報セキュリティ点検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

情報セキュリティ点検責任者は、情報セキュリティ点検結果を取りまとめ、CISOに報告するものとする。

(6)保管

情報セキュリティ点検責任者は、情報セキュリティ点検の実施を通して収集した点検証拠、点検報告書の作成のための点検調書を、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。

(7)情報セキュリティ点検結果への対応

CISO は、点検結果を踏まえ、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しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、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。

(8)情報セキュリティポリシーの見直し等への活用

情報セキュリティポリシー推進事務局は、点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3.10.2 セルフチェック

(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、毎年度及び必要に応じてセルフチェック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、所管する部局支所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、毎年度及び必要に応じてセルフチェックを行わなければならない。

(2)報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、セルフチェック結果とセルフチェック結果に基づく改善策を取りまとめ、情報セキュリティポリシー推進事務局に報告しなければならない。

(3)セルフチェック結果の活用

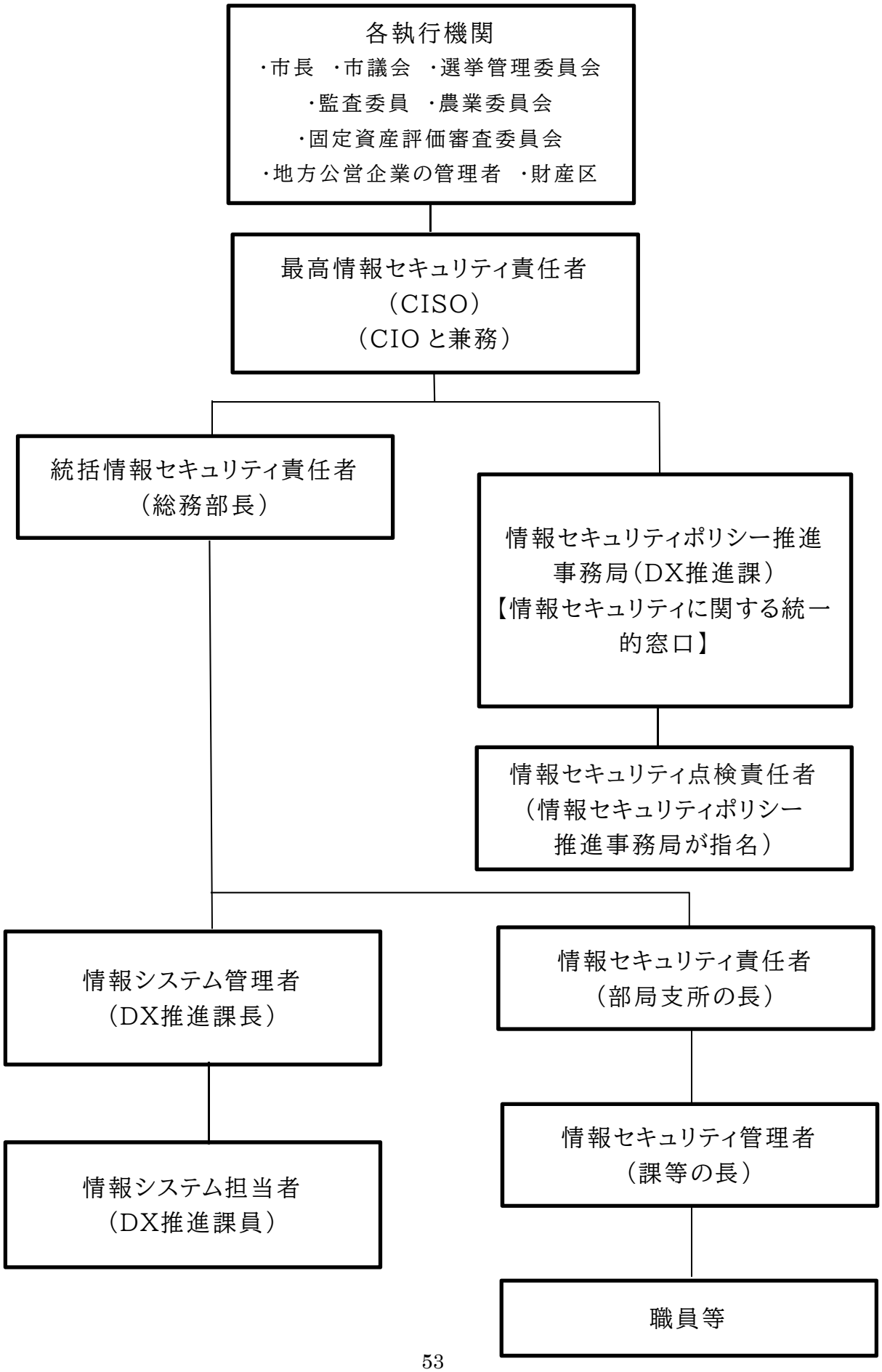
①職員等は、セルフチェックの結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②情報セキュリティポリシー推進事務局は、このセルフチェック結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3.10.3 情報セキュリティポリシーの見直し

情報セキュリティポリシー推進事務局は、情報セキュリティポリシーについて情報セキュリティ点検及びセルフチェック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、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合評価を行い、必要があると認めた場合改善を行うものとする。

付録A 組織体制


各執行機関
・市長 ・市議会 ・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
・地方公営企業の管理者 ・財産区
最高情報セキュリティ責任者
（CISO）
（CIO と兼務）
統括情報セキュリティ責任者
（総務部長）
情報セキュリティポリシー推進
事務局（DX推進課）
【情報セキュリティに関する統一
的窓口】
情報セキュリティ点検責任者
（情報セキュリティポリシー
推進事務局が指名）
情報システム管理者
（DX推進課長）
情報セキュリティ責任者
（部局支所の長）
情報システム担当者
（DX推進課員）
情報セキュリティ管理者
（課等の長）
職員等

＜特記事項＞

(1)DX推進課は、本情報セキュリティポリシー推進事務局としての活動を併せて担うものとする。

(2)総務課は、本情報セキュリティポリシーに記載の人事管理部門としての活動を担うものとする。

(3)管財担当課及び各支所・各施設の管財担当は、本情報セキュリティポリシーに記載の施設管理部門としての活動を担うものとする。

付録B 用語集

	用語	説明
C	CIO	Chief of Information Officer の略。情報システム及び情報戦略の最高責任者である最高情報統括責任者を指す。
	CISO	Chief of Information Security Officer の略。情報セキュリティポリシーを運用する組織体制における最高情報セキュリティ責任者を指す。
H	HUB	複数台のパソコンを接続し、ネットワークを構成する機器のこと。
I	ICカード	キャッシュカード大のプラスチック製カードに極めて薄い半導体集積回路（ICチップ）を埋め込み、情報を記録できるようにしたカードのこと。
	ID	システムの利用者を識別するために用いられる符号のこと。ネットワーク上においては、LAN上のデータに接続する際などに、ユーザー認証を行うために使用される。
L	LAN	ケーブルや無線などを使って、同じ建物の中にあるコンピュータや通信機器、プリンタなどを接続し、データをやり取りするネットワークのこと。
	LANケーブル	構内ネットワーク（LAN）を構成する機器間をつなぐ通信ケーブルのこと。
	LGWAN	地方自治体のコンピュータネットワークを相互接続した広域ネットワークのこと。 正式名称：「総合行政ネットワーク」
ア	アカウント	ユーザーが特定の機器（ネットワークやコンピュータなど）にログインするための権利のこと。また、ユーザーとは、コンピュータシステムの利用者を意味する。ユーザーに割り当てられたアカウントをユーザーアカウントとも呼ぶ。
	アクセス	情報システムや情報記憶媒体に対して接続し、データの書き込み又は読み出し等をすること。
	アクセス制限	定められた条件を基に、情報資産に対してアクセスできないように制限すること。
	アクセス制御	情報資産に対して，だれがどのような権限でアクセスするのかをコントロールすること。

ア	アクセスログ	コンピュータやネットワークシステム、特にサーバへのアクセスに関する情報を記録したもののこと。アクセス日時やアクセス者情報、アクセスした情報が、テキストファイルに記録される。
	暗号化	第三者に知られたくない機密情報、個人情報などを通信する際、盗聴や傍受によって内容を漏えい、改ざんされることを防ぐための技術のこと。ハードディスクやUSBメモリなどに含まれる重要なデータは、メールやインターネットでのやり取りに限らず、情報流出を防ぐため、暗号化して保護するのが望ましい。
イ	インターネット	世界中にある複数のネットワークを相互に接続することで構築された、巨大なネットワークのこと。一般的には、インターネット上で提供されるWebサービスを指してインターネットと呼ぶ場合もある。
ウ	ウェブ （Web）	インターネット上で文字・画像などを配置して見せ、簡単にアクセスできるようにするための仕組みのこと。
	ウェブページ	ウェブ上にある個々の文書のこと。
	運用テスト	情報システム開発やソフトウェア開発の最終段階で、実際の業務に即した利用の仕方をしてみて問題なく動作するかを試すテストのこと。
オ	オペレーティング システム （OS）	キーボード入力や画面出力といった入出力機能やディスクやメモリの管理など、多くのアプリケーションソフトから共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェアのこと。 （例：Windows、Mac OS、iOS、Android など）
カ	カードリーダ	メモリーカードの読み取り装置のこと。コンピュータに直接内蔵されているものや、USB接続する外付けタイプなどがある。
	外部サービス	民間事業者等の庁外の組織がインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うもののこと。クラウドサービス、Web 会議サービス等の全般を指す。 ＜外部サービスの例＞ ・クラウドサービス　・Web 会議サービス ・テレワーク用接続サービス ・SNS（ソーシャルネットワーキングサービス） ・検索サービス、翻訳サービス、地図サービス ・ホスティングサービス
	外部ネットワーク	構内ネットワーク（LAN）に対し、外部のネットワークのこと。（例：インターネット）
	瑕疵（かし）	通常、一般的には備わっているにもかかわらず本来あるべき機能・品質・性能・状態が備わっていないこと。

	管理者権限	対象のシステムやコンピュータに新しいハードウェアを追加したり、システムの構成を変更したりする権限のこと。
キ	共有ファイルサーバ	ネットワーク上で、ファイルを共有するために設置されるサーバのことで、記憶装置をネットワーク上の他のコンピュータと共有し、他から利用できるようにしたものである。
ケ	ゲートウェイ	ネットワーク間の接続を中継する機器又はソフトウェアのこと。本来は、異なるネットワーク間の違いを吸収するためという役割だったが、ネットワークの主流がインターネットになってからは、外部のネットワークの出入り口で、何らかの処理（ウイルスチェックなど）を行うコンピュータとしての意味合いが強まっている。
コ	コンピュータウイルス	他のコンピュータに勝手に入り込んで悪さをするプログラムのこと。画面表示をでたらめにしたり、無意味な単語を表示したり、ディスクに保存されているファイルを破壊したり、操作されたりする。ウイルスはインターネットからダウンロードしたファイルやメール、他から借りたUSBメモリなどを介して感染する。
	コンピュータウイルス攻撃	他のコンピュータに勝手に悪さをするプログラムを入れ、ディスクに保存されているファイルを破壊したり、勝手にファイルを読み出したり、動作不能にしたりすること。
サ	サーバ	ネットワークを介して他のコンピュータに対し、自身の持っている機能やサービス、データなどを提供するコンピュータのこと。また、そのような機能を持ったソフトウェアのこと。
	サービス不能攻撃	ネットワークを通じた攻撃の一つで、相手のコンピュータやルータなどに不正なデータを送信して使用不能やトラフィック（データの情報量）を増大させて相手のネットワークを麻痺させる攻撃のこと。
	サービスレベル	IT企業が情報システムや通信サービスなどを提供する際、どのくらいの品質のサービスを提供できるか、利用者に対して事前に提示し、合意したレベルのこと。
	サイト	インターネットで情報が保管されているサーバや、LANなどネットワークの単位を指して用いられる。Webサイトは、複数のWebページのまとまりのこと。
	サイバー攻撃	コンピュータシステムやインターネットなどを利用して、標的のコンピュータやネットワークに対し、不正に侵入してデータの詐取や破壊、改ざんなどを行い、標的のシステムを機能不全に陥らせること。
シ	時刻同期	ネットワークに接続するサーバや端末パソコンの時刻を正しい時刻に合わせておくこと。時刻同期する最大の理由は、複数サーバでのログ出力時間の信憑性を持たせるためである。
	システム障害	情報システムが何らかの不具合によってその機能に支障を来たし、本来の機能が利用できない状態のこと。

	社会インフラ	社会生活を支えるために整備された公共的な仕組み、基盤を指す。 例：道路、上水道、下水道、電気、ガス、電話等
	住基ネット	各地方自治体が持つ住民基本台帳のコンピュータネットワーク化を図り、全国共通で本人確認できるシステムのこと。
	冗長化	最低限必要な量よりリスクを想定した設備を用意しておき、一部の設備が故障してもサービスを継続して提供できるようにシステムを構築すること。
	情報資産	個人情報、組織運営のための情報、ノウハウ等の機密情報などを言い、外に漏れると組織運営上に重大な問題を引き起こす可能性がある情報のこと。また、情報は、コンピュータ（サーバ、パソコンなど）、外部記憶媒体、紙、又は人の記憶や知識など、様々な形態で蓄積されており、それらを保護するための設備、施設も含まれる。
	情報セキュリティマネジメントシステム	情報に関する個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスク分析により必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。（ISO27001）
	情報システム	コンピュータ、サーバ、ネットワークおよび情報記憶媒体で構成され、情報処理を行う仕組みをいう。
ス	スパムメール	受信者の意向を無視して、無差別かつ大量に一括して送信される、電子メールを主としたメッセージのこと。 電子メールを対象としたものについては、迷惑メールと呼ばれる場合が多い。
セ	生体認証	バイオメトリクス認証とも呼ばれ、人間の身体的特徴（生体器官）や行動的特徴（癖）の情報を用いて行う個人認証技術である。
	セキュリティサーバ	ウイルス対策・スパイウェア対策に加え、脆弱性を狙うネットワーク攻撃への対応、情報漏えい対策、ネットワーク検疫などを担うサーバのこと。
	セキュリティホール	コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。
	セルフチェック	自己点検のこと。自分の行動や状況・状態を自分自身で評価すること。
ソ	ソーシャルメディアサービス	インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのこと。
	ソースコード	コンピュータを動作させる実行形式のプログラムの元となる、プログラミング言語の記述仕様に従って記述された文書のこと。
	ソフトウェア	コンピュータシステム上で何らかの処理を行うプログラムや手続き、およびそれらに関する文書のこと。
タ	第三者	当事者以外の人やその事柄に直接関係のない者のこと。

	多要素認証	本人確認を行う際、知識（パスワード等）、所持（ICカード、スマートフォン、ワンタイムパスワードトークン等）、生体（指紋、顔、静脈等）の3つの要素のうち、2つ以上の異なる要素を組み合わせて認証すること。単一の要素（例：パスワードのみ）に比べ、なりすましによる不正アクセスの防止に大きな効果がある。
	端末	情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもののこと。
	端末のロック	端末を使用不可能な状態にすること。
チ	チェック機能	調べて、不都合なものが入り込むのを阻止する機能のこと。
ツ	通信回線	コンピュータと端末、あるいはコンピュータ同士を接続して、情報をやり取りするために用いられる通信線のこと。電気事業者が提供する広域通信回線や、LANなどの構内通信回線などを広く指す。
	通信回線機器	コンピュータと端末、あるいはコンピュータ同士を接続して、情報をやり取りするために用いられる通信に使用する機器のこと。
	通信ケーブル	有線で情報を送るために使われるケーブルのこと。 （例：LANケーブル、電話ケーブル等）
テ	テストデータ	システムが正常に稼動するかどうかをテストするためのデータのこと。
	電子署名	電磁的記録（電子文書）に付与する、電子的な証拠であり、紙文書における印やサイン（署名）に相当する役割をはたすもののこと。主に本人確認、偽造・改ざんの防止のために用いられる。
	電子申請	これまで、窓口などで行われていた申請や届出を、本人もしくは代理人がネットワーク経由で実行できるようにしたもののこと。
	電磁的記憶媒体	コンピュータでの情報処理に使用する情報記憶媒体のこと。（例：ハードディスクやCD、DVD、USBメモリ、SDカード，MO，FD等）
	電子ファイル	文書や画像などを電子データとして記録・保管したもののこと。
ト	特定用途機器	テレビ会議システム、ネットワークカメラシステム等の特定の用途に使用される機器のこと。
	トラフィック	ネットワーク上を移動する音声や文書、画像などのデジタルデータのこと。ネットワーク上を移動するこれらのデータの情報量のことをさすこともある。
ナ	生データ	個人情報や機密性の高い情報が、未加工で直接確認できる状態のデータのこと。
ネ	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（ハードウェアおよびソフトウェア）をいう。
	ネットワークシステム	基幹業務システム、行政情報ネットワークシステム（庁内LAN）および両システムのいずれかと接続するすべての情報システムのこと。
	ネットワークストレージサービス	インターネットなどのネットワーク上でファイル保管用のディスクスペースにデータを保存することができるサービスのこと。

ハ	パスワード	特定の機能を使用する際に認証を得るため入力する文字及び数字の羅列のこと。
	パスワードファイル	ユーザー認証の際に参照されるファイルのこと。
	パターンファイル	ウイルス定義ファイルとは、世の中に存在する様々なコンピュータウイルスの特長を記録したファイルで、ウイルス対策ソフトがコンピュータウイルスを検出するために使用するファイルのこと。
	バックアップ	データの写しを取って保存すること。コンピュータに保存されたデータやプログラムを、破損やコンピュータウイルス感染などの事態に備え、別の情報記憶媒体に保存すること。
	ハードウェア	コンピュータを構成している電子回路や周辺機器などの物理的実体のこと。
	パッチ	コンピュータにおいてプログラムの一部分を更新して修正や機能変更を行なうためのデータのこと。
ヒ	標的型攻撃	明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種のこと。
フ	ファイアウォール	組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム又はそのようなシステムが組み込まれたコンピュータのこと。
	ファイル	ハードディスクやUSBメモリ、CD-ROMなどの情報記憶媒体に記録されたデータのまとまりのこと。
	ファイルの属性	ファイルごとに記録される、作成アプリケーションの種類や内容、作成日時、更新日時、サイズなどの情報のこと。
	フィルタリング	一定の条件に基づいてデータなどを選別・排除する仕組みのこと。
	フォルダ	ハードディスクやUSBメモリ、CD-ROMなどの記憶装置で、ファイルを分類・整理するための保管場所のこと。フォルダには識別のために固有の名称（フォルダ名）をつけることができ、関連する複数のファイルをまとめて一つのフォルダに入れることにより、効率的に記憶装置を管理することができる。フォルダの中にさらにフォルダを作成することもでき、階層構造によって細かい分類を表現することもできる。
	不正アクセス	あるコンピュータへの正規のアクセス権を持たない人が、ソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピュータを利用する、あるいは試みること。
	不正プログラム	コンピュータに害をおよぼすプログラムのこと。
	フッター	ワープロ文書等で用いられるもので、紙に印刷する文書の場合ページの下端に設けられた、定型的な情報を記すための領域のこと。（例：ページ番号等）
	プログラム	コンピュータが行うべき処理を順序立てて記述したもののこと。

	プログラミング	プログラムを作成することにより、人間の意図した処理を行うようにコンピュータに指示を与えること。
へ	ヘッダー	ワープロ文書等で用いられるもので、紙に印刷する文書の場合ページの上端に設けられた、定型的な情報を記すための領域のこと。(例:文書名称等)
ホ	ポート	外部とデータを入出力するための、ソフトウェアやハードウェアの末端部分(インターフェース)のこと。 (例:HUBのLANケーブル接続口等)
マ	マイナンバー	社会保障と税に関わる番号制度に基づいて住民全員に割り当てられる一意の個人番号のこと。
ム	無線LAN	無線でデータの送受信を行なうLANのこと。「アクセスポイント」と呼ばれる中継機器を中心に、無線通信機能を持ったコンピュータなどが相互に接続され、ネットワークを形成する。
モ	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のこと。
リ	リスク	一般的には、ある行動に伴って(あるいは行動しないことによって)、危険に遭う可能性のこと。
	リスク分析	現実に発生すれば損失をもたらすリスクが、情報システムのどこに、どのように潜在しているかを識別し、その影響の大きさを測定すること。
ル	ルータ	コンピュータネットワークにおいて、データを2つ以上の異なるネットワーク間に中継する通信機器のこと。ネットワークで、どのルートを通して転送すべきかを判断するルート選択機能を持っている。
	ルーティング	情報を送信する際、ネットワーク上で最適な経路を選択して送信すること。
レ	例外措置	通例の法則や規則、規定から外れたものを事態に応じて必要な対応をすること。
ロ	ログイン	コンピュータやネットワーク上の様々なサービスを利用する際に、予め登録しておいたアカウントを用いて各種のデータにアクセスする認証行為のこと。
ユ	ユーザー	コンピュータやシステムを利用する人のこと。