加美町情報セキュリティポリシー

令和８年３月３１日　策定

宮城県加美町

目　次

改定履歴

日付	バージョン	概要
平成 16 年 7 月	第 1 版	初版制定
平成 29 年 3 月	第 2 版	CISO の設定、新たな攻撃への対応の追加等
令和 8 年 3 月	第 3 版	総務省ガイドライン改定等への対応

第１章 情報セキュリティ基本方針

１　目的

加美町は、まちづくりの基本理念「共生」、「協働」、「自治」に基づき「善意と資源とお金が循環する、人と自然に優しいまち」を目指しています。３町が合併して誕生した町であることから特定の地域に偏らない公平公正な地域づくりを心掛け、住民の皆様のために、生活環境の改善や産業・教育・福祉・医療・災害対策などのあらゆる生活の場面において、さまざまな行政サービスを展開しております。こうしたサービスはひと時も停止することは許されず、継続的且つ安定的に運営していく必要があります。

一方、近年のインターネットを中心とした情報通信技術の発展はめざましく、情報技術の活用によって行政サービスの利便性や効率性の向上等、多くのメリットが期待できる反面、情報の改ざんや漏えいを目的とした不正アクセスやコンピュータウイルスといった様々な脅威が存在し、行政サービスの提供が脅かされています。

加美町ではこうした脅威から情報資源を保護し、住民の皆様の信頼確保と安定した行政サービスの提供を目的に、全組織、全職員一人ひとりが扱う情報の保護において取り組む基準を定めると共に、その継続的な遵守の決意表明として、ここに「情報セキュリティポリシー」（以下「ポリシー」という）を定めることとしました。

第１章の情報セキュリティ基本方針では、情報セキュリティ対策に関する、統一的かつ基本的な方針を定めることとしました。第２章の情報セキュリティ対策基準では、情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準を定めることとしました。

また、情報セキュリティ対策を確実に実施するために、ポリシーに基づき、情報資産における取扱い手順等をとりまとめた、「情報セキュリティ実施手順書」を定めることとしました。

２　定義

ポリシーにおいて、次の各号に掲げる用語の意義は、それぞれの各号に定めるところによる。

（１）組織等に関する用語の定義

①　課等

「加美町課設置条例(平成15年 加美町条例第7号)」に規定する課、「加美町行政組織規則（平成15年 加美町規則第3号）」に規定する課等、「加美町教育委員会組織規則（平成15年 教育委員会規則第4号）」に規定する課等、「加美町議会事務局設置条例（平成15年 加美町条例第222号）」に規定する議会事務局及び「加美町農業委員会事務局設置及び処務規程（平成15年 加美町農業委員会訓令第3号）」に規定する農業委員会事務局をいう。

② 職員等

常勤職員、会計年度任用職員、臨時職員等の任用形態、職位を問わず、本町の全職員をいう。

（２）情報資産等に関する用語の定義

① 情報資産

行政情報及び情報システムをいう。

② 情報セキュリティ

情報資産の機密性（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。）、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。）及び可用性（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。）を確保し、維持することをいう。

③ 行政情報

職員等が職務上作成又は取得した情報で、その記録媒体の形態に関わらず本町が管理しているものをいう。

④ 個人情報

行政情報のうち、個人又は法人その他の団体に関する情報で、特定の個人又は法人その他の団体が識別され、又は識別され得るものをいう。

⑤ アクセス権限

情報資産を利用することのできる範囲をいう。

⑥ 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（３）情報システム等に関する用語の定義

① 情報システム

ハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体等で構成され、これら一部又は全体で業務処理を行う仕組みをいう。

② ハードウェア

電子的にデータを処理する機能を持ち、事務処理に使用する機器をいう。

③ ソフトウェア

ハードウェア上で稼働するプログラム等をいう。

④ ネットワーク

通信回線、通信機器等で構成された情報通信網をいう。

⑤ 電磁的記録媒体

行政情報の記録、管理に使用される磁気ディスク、磁気テープ、光ディスク等をいう。

⑥ サーバ

情報システムのうち、ネットワーク上においてファイル管理、印刷等の機能を提供するために設置される機器をいう。

⑦ クライアント

情報システムのうち、ネットワーク上においてデータの入力、更新、検索、出力等の操作を行うための機器をいう。

⑧ 庁内ネットワーク

情報システムのうち、本町の所管する施設内に敷設されたネットワークをいう。

⑨ 外部ネットワーク

情報システムのうち、電気通信事業者が提供する各種情報通信網等を通じ、複数のネットワークを接続する機能を持った機器を用いることにより、庁内ネットワークに接続することが可能なネットワークをいう。

⑩ ネットワーク機器情報システムのうち、

ネットワークを構成するケーブル及びネットワーク制御装置等の機器並びに附帯設備をいう。

⑪ 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。

⑫ 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。）。

⑬ 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。

⑭ 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。

⑮ 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。

⑯ 外部サービス

外部サービスとは、外部の事業者が提供するサービスの総称であり以下のも

のをいう。

(a) 委託による外部サービス

本町の業務を外部の事業者に委託することにより調達する外部サービスのことをいう。

(b) 約款による外部サービス

無料有料を問わず、以下の形態により調達する外部サービスのことをいう。

・約款への同意のみにより利用可能となる外部サービス

事業者が定める約款への同意によって利用可能となるサービスのことをいう。

・国が提供する外部サービス

国が運営し、提供するサービスのことをいう。

⑰ クラウドサービス

データやソフトウェアをネットワーク経由でサービスとして利用者に提供するものをいい，主に仮想化技術により実現されているものをいう。

なお、政府の情報システムについて、共通的な基盤・機能を提供する複数のクラウドサービスの利用環境である、ガバメントクラウドを含める。

3　対象範囲

(1)対象組織

ポリシーが対象とする組織は、町長事務部局、教育委員会、議会事務局、農業委員会、各行政委員会、各地方公営企業及び各教育機関とする。

また、本町の条例、規則その他の規定に基づき新たに設置される行政組織についても、本ポリシーの適用対象とする。

(2)対象情報資産

ポリシーが対象とする情報資産は、(1) に定める組織において行政事務を処理するために取扱う情報資産とする。

なお、対象とする情報資産には、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、これらで取り扱う情報（印刷文書を含む。）並びに仕様書、ネットワーク図等のシステム関連文書を含むものとする。

(3)対象者

ポリシーが対象とする者は、(2) に定める情報資産を取扱う全ての者とする。

4　職員等及び外部委託事業者の義務

職員等及び外部委託事業者は、情報セキュリティの重要度について共通の認識を持つとともに、業務の遂行に当たってポリシーを遵守する義務を負う。

5　情報セキュリティ対策

(1)情報セキュリティ管理体制

本町の情報資産に関する情報セキュリティ対策を、組織として統一された意思の下に、継続的に実施するため、幹部職員が率先して推進、管理する体制を確立する。

(2)情報資産の分類

本町の情報資産を、その内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

(3)情報資産への脅威

本町の情報資産の情報セキュリティを維持する上で、特に認識すべき脅威は次のとおりである。

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、重要情報の詐取等。

② 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等。

③ 地震、落雷、火災等の災害及び事故、故障等によるサービス及び業務の停止。

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)情報セキュリティ対策

本町の情報資産を(3)　で示した脅威から保護するため、次の情報セキュリティ対策を実施する。

① 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷、妨害等から保護するため、物理的な対策を実施する。

② 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者に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行われるよう必要な対策を実施する。

③ 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を実施する。

④ 運用におけるセキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、システム開発等の外部委託、ネットワークの監視、ポリシー遵守状況の確認等、運用面の対策を実施する。 また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を実施する。

⑤ 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。

(a) 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。

(b) 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。

(c) インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。⑥　業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

クラウドサービスを利用する場合には、利用に係る規定等との整合性を確認し、必要に応じて見直しを行ったうえで、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、実施手順により運用手順を定め、発信可能な情報の範囲を定めるとともにソーシャルメディアサービスごとの責任者を定める。

6　情報セキュリティに関する文書の整備

(1)情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づく情報セキュリティ対策を実施するために、本町において遵守すべき行為及び判断等の基準を統一的なレベルで定め、情報セキュリティ対策の基本的な要件を明記した情報セキュリティ対策基準を策定する。

(2)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を遵守して情報セキュリティ対策を実施するために、個々の情報資産に対する脅威及び重要度に対応する対策基準の基本的な要件に基づき、本町が所掌する情報資産における取扱い手順等をそれぞれとりまとめ、情報

セキュリティ実施手順を策定する。

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。

7　ポリシー違反時の対応

ポリシー違反に対しては、その重大性、発生した事件、事故等の状況等に応じて各関連法令の罰則の対象となり得る。

8　情報セキュリティ監査の実施

ポリシーが遵守され、情報セキュリティが維持されていることを検証するため、定期的に情報セキュリティ監査を実施する。

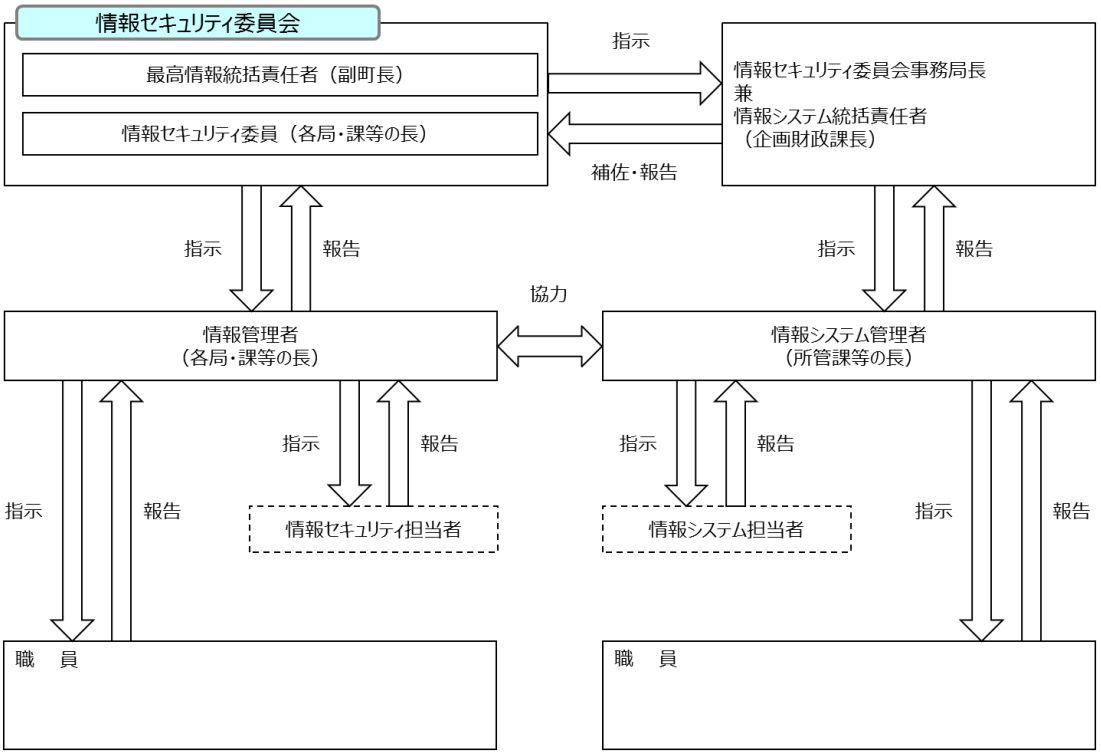
9　評価及び見直しの実施

情報セキュリティ監査の結果等により、ポリシーに定める事項及び情報セキュリティ対策の有効性等について評価するとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜ポリシーの見直しを実施する。

第２章 情報セキュリティ対策基準

１　組織、体制

本町の情報セキュリティ管理は、次の組織、体制で実施する。



（加美町情報セキュリティ組織図）

(１) 最高情報統括責任者

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を統括する最高情報セキュリティ責任者(CISO ： Chief Information Security Officer)を置く。最高情報セキュリティ責任者は加美町副町長とし、本町における情報活用に関する最高情報統括責任者(CIO ： Chief Information Officer)としての役割を兼務する。

(２) 情報セキュリティ委員会

①　情報セキュリティ委員会の設置

最高情報統括責任者を長とした情報セキュリティに関する最高機関として、情報セキュリティ委員会（以下、「委員会」という。）を置く。委員会は、最高情報統括責任者及び各情報システムを所管する所属長等をもって構成する。

②　役割、責任

(a) 本町の情報セキュリティの維持管理を、組織として統一された意思の下に継続的に実施するため、ポリシーや実施手順等の策定など、情報セキュリ

ティに関する重要な事項を協議し決定する。

(b) 組織内において情報セキュリティに関する役割、責任を明確にする。

(c) 職員等が情報セキュリティの重要度を認識し、ポリシーを理解し実践するために必要な教育、訓練等の計画を策定する。

(d) 緊急時対応計画の策定及び見直しを行い、緊急時対応計画に基づく訓練等の計画を策定し、実際に情報資産の漏洩等の事故が発生した場合に即応できるように体制を整える。

(e) 必要に応じて第三者から情報セキュリティに関する助言を求め、庁内全体を調整する。

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

(3) 情報セキュリティ委員会事務局

① 情報セキュリティ委員会事務局の設置

委員会を運営する機関として、情報セキュリティ委員会事務局（以下、「事務局」という。）を置く。事務局は企画財政課とし、企画財政課長を事務局長とする。

② 役割、責任

委員会の所掌事項の調査、検討及び庁内調整を実施する。

(4) 情報システム統括責任者

① 情報システム統括責任者の設置

本町全体の情報システムを統括する責任者として、情報システム統括責任者（以下、「統括責任者」という。）を置く。統括責任者は企画財政課長とする。

② 役割、責任

(a) 管理区域を設置、管理する。

(b) 委員会の策定した計画に基づき、教育、訓練等を実施する。

(c) 全ての情報システムに関する情報（情報システムの設置場所、利用目的及び行政情報の内容等）を統括する。

(d) 全ての情報システムにおける情報セキュリティ向上のための協力、助言を行う。

(e) 常に、情報セキュリティに関する最新情報を入手し、必要に応じて各関連部門に周知する。

(f) 緊急時には最高情報統括責任者に早急に報告を行うとともに、回復のための対策を講じる。

(5) 情報管理者

① 情報管理者の設置

各課の所管する情報資産の情報セキュリティを統括する責任者として、情報

管理者を置く。情報管理者は各課等の長とする。

② 役割、責任

(a) 所管する情報資産における情報セキュリティ対策を実施する。

(b) 所管する情報資産に関する実施手順を必要に応じて策定し、維持、管理を行う。

(c) 課等で任用する非常勤及び臨時職員に対し、ポリシーの遵守を徹底する。

③ その他

(a) 情報管理者は、業務において別の情報管理者の所管する情報資産を使用する場合は、双方協議の上、管理責任の範囲を明確にし、職員等に周知、徹底を図る。

(b) 情報管理者は、所管する情報資産の情報セキュリティに関する運用管理について補佐する者(情報セキュリティ担当者)を指定できる。

(6) 情報システム管理者

① 情報システム管理者の設置

各情報システムの情報セキュリティを統括する責任者として、情報システムを所管する課等に情報システム管理者を置く。情報システム管理者は情報システムを所管する課等の長とする。

② 役割、責任

(a) 所管する情報システムにおける開発、設定の変更、運用、更新等を行う。

(b) 所管する情報システムにおける情報セキュリティ対策を実施する。

(c) 所管する情報システムに関する実施手順を必要に応じて策定し、維持、管理を行う。

③ その他

(a) 情報システム管理者は、情報管理者が兼任することができる。

(b) 複数の課等において共同で使用する情報システムの情報システム管理者は、委員会が個別に指名する。

(c) 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の運用管理について補佐する者（情報システム担当者）を指定できる。

(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 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

(8) 情報セキュリティに関する統一的な窓口及び CSIRT

① 最高情報統括責任者は、情報セキュリティインシデントの統一的な窓口の機能（PoC：Point of Contact、ポック）を有する組織を整備し、当該インシデント

の初動対応、連絡調整、情報集約及び対応方針の整理を行う組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

② 最高情報統括責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、必要に応じて報道機関への通知・公表対応を行わなければならない。

④ 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、連絡調整及び連携を行う。

(9) クラウドサービス利用における組織体制

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

2　情報資産の分類と管理

(1) 情報資産の管理と利用に関する責任

① 情報資産の管理責任

情報資産は、その情報資産を作成した課等の情報管理者が管理責任を負う。

② 情報資産の利用責任

情報資産を利用する者は、情報資産の利用目的及び重要度分類に従って利用する責任を有する。

(2) 情報資産の分類

① 情報資産の分類

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

(a) 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、「行政文書の管理に関するガ イドライン」（平成 23 年４月１日 内閣総理大臣決定）に定める秘密 文書に相当する文書	・ 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付禁止 ・ 保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・ 情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・ 復元不可能な処理を施しての廃棄 ・ 信頼のできるネットワーク回線の選択
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、自治体機密性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、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	・ 外部で情報処理を行う際の安全管理措置の規定 ・ 電磁的記録媒体の施錠可能な場所への保管
機密性１	機密性２又は機密性３の情報資産以外の情報資産	－

(b) 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	－

(c) 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 情報資産の分類の表示

情報管理者は、情報資産の取扱い方法を識別できるよう、重要度分類に基づき、情報資産を必要に応じて分類表示を実施する。ただし、分類表示の際には、部外者による不正使用等を防止するため、表示を記号化する等考慮する。

③ 情報資産の分類の効力

情報資産が複製された場合、複製についての重要度分類は、原本に準ずるものとする。

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についても、原本と同様に管理しなければならない。

(3) 情報資産の管理

① 情報資産の作成時における管理

(a) 情報管理者は、所管する情報資産の情報セキュリティを維持するために必要な情報を情報資産台帳にとりまとめ、常にこれを最新の状態に保たなければならない。

(b) 情報管理者は、所管する情報資産のアクセス権限を利用目的及び重要度分類に従って適切に設定し、管理する。

② 情報資産の運用時における管理

(a) 職員等は、情報資産を所定の場所から持ち出す場合、情報管理者の確認を得た上で持ち出す等適切に管理する。

(b) 職員等は、情報資産を庁外へ持ち出し又は送付する場合は、情報管理者の許可を得る。

(c) 情報管理者は、更新を必要としない情報資産を記録した電磁的記録媒体は、必要に応じて書込禁止処理を行った上で保管する。

(d) 情報管理者は、電磁的記録媒体に納められた情報資産を必要に応じて別の電磁的記録媒体に複製する。特に、機密性２以上、完全性２又は可用性２の情報資産の複製を納めた電磁的記録媒体は、災害等の被害を避けるため、原本と別の場所に保管する等の対策を実施する。

(e) 情報管理者は、情報資産を庁外へ送付する場合は、信頼できる事業者を選定し、複製の禁止、物理的保護規定及び違反した場合の罰則を契約に定める。

③ 情報資産の廃棄時における管理

(a) 職員等は、機密性２以上、完全性２又は可用性２の情報資産が不要となった場合、物理的に破壊する等記録を復元できないように処理を施した上で廃棄する。

(b) 職員等は、機密性２以上、完全性２又は可用性２の情報資産を廃棄する場合、情報管理者の許可を得るものとし、廃棄処理の実施日時、担当者及び処理内容を記録する。

(c) 情報管理者は、クラウドサービス上の情報資産を重要度分類に基づき適正に管理し、サービス更改・終了時の移行及び複製を含む削除が確実に行

われることを、文書等により確認しなければならない。

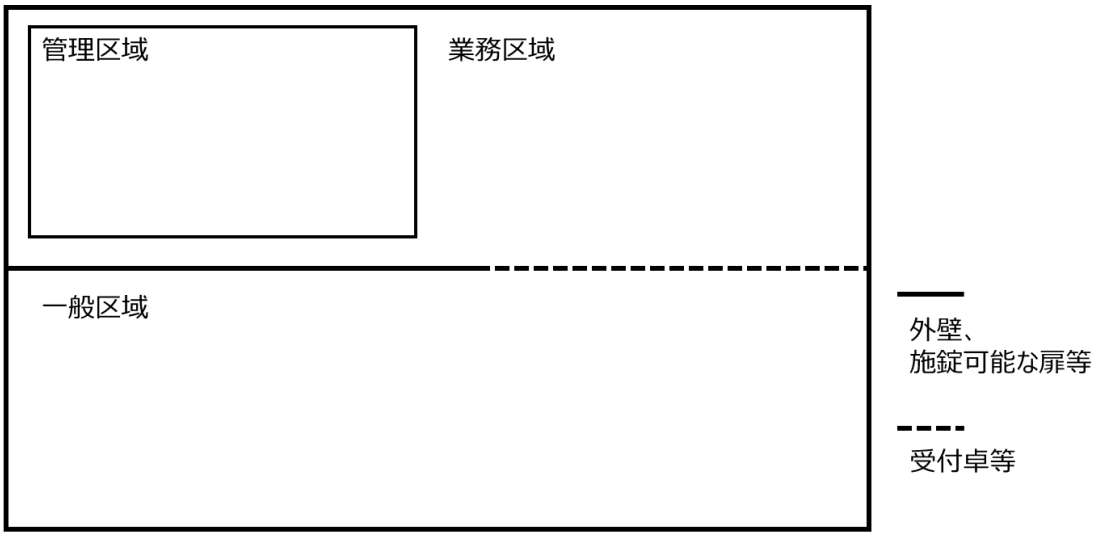
3　物理的セキュリティ

(1) 区画の管理

① 区画の分類

委員会は、情報資産の物理的セキュリティの維持と、効率的な業務環境の維持の両立を図るため、庁内の部屋を次のとおり分類し、それぞれ適切な対策を採る。

- 管理区域（サーバ室等、機密性２以上、完全性２又は可用性２の情報資産の管理及び運用を行うために設置する部屋をいう。）
- 業務区域（事務室等、職員等が各職責に応じて業務を行う部屋をいう。）
- 一般区域（待合室等、住民等が自由に出入りできる部屋をいう。）



【庁内の区画の概念図】

② 管理区域

(a) 管理区域の物理的セキュリティ対策は、統括責任者がこれを統括する。

(b) 統括責任者は、管理区域の設置に当たり、可能な限り次の条件を満たすことが可能な部屋を選定する。

- 外部からの侵入が容易にできないよう、外壁等で囲まれていること。
- 一般区域と隣接していないこと。
- 外部に通じる出入口が1ヶ所のみで、十分な強度の扉が設置してあること。
- 窓が設けられている場合、防火、防水、防犯対策及び窓ガラスの破損防止対策が実施できること。さらに、室内のサーバ等データ保管設備

が見えないようブラインド等で遮蔽できること。
- 火災による装置の被害を防止できるよう、消火設備が設置されていること。

(c) 統括責任者は、管理区域への入退室について、次の管理策を実施する。
- 管理区域へ入退室できる者をあらかじめ定めること。
- 入退室する者の行動を適切に把握、管理すること。
- 入退室に関する記録を取得し、適切に保管すること。
- 管理区域へ入退室できる者について、定期的に見直し及び更新すること。

(d) 統括責任者は、管理区域へ装置等を搬出入する場合は、次の管理策を実施する。
- あらかじめ搬出入する装置等の既存情報システムに及ぼす影響を考慮し、安全を確認すること。
- 装置等を搬出入する際、職員を同行させること。

(e) 統括責任者は、管理区域での作業について、次の管理策を実施する。
- 作業の内容をできるだけ部外者に知らせないようにすること。
- 部外者が作業する必要がある場合には、事前に作業者、作業内容について確認の上、職員等の立会いの下で実施すること。また、その際には取扱うことのできる情報資産を制限すること。

(f) 職員等及び外部委託事業者は、管理区域において作業を行う場合は、身分証明書等を携帯し、求めにより提示する。

③ 業務区域

(a) 業務区域の物理的セキュリティ対策は、その業務区域を主に業務に使用する課等の情報管理者がこれを統括する。

(b) 情報管理者は、業務区域への入退室について、次の管理策を実施する。
- 部外者が容易に入ることができないよう、適切な対策を実施すること。特に、一般区域との境界が受付卓等完全に遮断できないものである場合は、立札や監視等により部外者の立入りを抑制すること。
- 業務区域が無人になるときは扉、窓に施錠する等、部外者の侵入を防ぐこと。
- 必要に応じて、侵入者を検知し、警報する装置を導入すること。導入した警報装置は、業務区域が無人の場合、常に作動するようにすること。

(c) 情報管理者は、業務区域へ装置等を搬出入する場合は、次の管理策を実施する。
- あらかじめ搬出入する装置等や目的等必要事項を確認すること。

・ 装置等を搬出入する際、職員を同行させること。

(d) 職員等は、業務区域での作業について、次の管理策を実施する。

・ 作業の内容をできるだけ部外者に知らせないようにすること。

・ 部外者が作業する必要がある場合には、事前に作業者、作業内容について確認の上、職員等の立会いの下で実施すること。また、その際には取扱うことのできる情報資産を制限すること。

(e) 情報管理者は、業務区域における情報資産の取扱いについて、次の管理策を実施する。

・ 外部からの情報資産の盗み見等を防止するため、情報システムや印刷機の配置を工夫すること。

・ 機密性２以上、完全性２又は可用性２の情報資産について、可能な限り耐火、耐熱、耐水及び耐湿対策を行い、施錠して保管すること。

・ 機密性２以上、完全性２又は可用性２の情報資産を持ち出す必要がある場合は、持ち出し時及び返却時の記録を取得すること。

・ 職員等が事務室の情報資産を無許可で持ち出すことを抑制するため、周知及び啓発を行うこと。

(f) 職員等は、業務区域における情報資産の取扱いについて、次の管理策を実施する。

・ 机上には重要な情報資産を放置せず、許可されていない情報資産へのアクセスや消失及び損傷を防止すること。

・ 離席する場合は端末等の装置をログアウト状態にし、パスワード等によって保護すること。

・ 機密性２以上、完全性２又は可用性２の行政情報を印字した際は、印字装置から速やかに取り出すこと。

(g) 職員等及び外部委託事業者は、管理区域において作業を行う場合は、身分証明書等を携帯し、求めにより提示する。

④ 一般区域

(a) 一般区域の物理的セキュリティ対策は、委員会がこれを統括する。

(b) 職員等は、一般区域における情報資産の取扱いについて、次の対策を実施する。

・ 機密性２以上、完全性２又は可用性２の情報資産を一般区域に持ち込む場合は、必ずこれを携行し、許可されていない情報資産へのアクセスや消失及び損傷を防止すること。

・ 一般区域での作業は必要最小限にとどめ、その内容や利用する情報資産を部外者に知られないよう、会話等に配慮する。

(2) 装置等の管理

① 装置の設置場所

(a) 情報システム管理者は、サーバ及びネットワーク機器等の取り付けを行う場合、管理区域又は次の条件を可能な限り満たす業務区域に設置する。

【共通事項】

- 地震、火災、水害、爆発等の災害の影響を受ける恐れが少ない場所であること。
- 煙、埃、電波障害等の影響を受ける恐れが少ない場所であること。
- 侵入、破壊、窃盗等を防止するため外部から容易に入れない場所であること。
- 保守に必要な空間を確保できること。
- 装置等を設置した場所を非表示とすること。

【機密性２以上、完全性２又は可用性２】

- 配線等から放射される電磁波の傍受による情報漏洩への対策ができること。
- 温度、湿度の調整ができること。
- 出入口に入退管理設備及び防犯設備を設置できること。

(b) 情報システム管理者は、サーバ及びネットワーク機器等及び電磁的記録媒体等について、一般区域又は庁外に設置する必要がある場合は、次の管理策を実施する。

- 管理簿を設け、常にこれを最新の状態に保つこと。
- 管理方法及び使用方法を定めること。
- 必要に応じて保険を適用すること。

(c) 情報システム統括責任者及び情報システム管理者は、委託事業者のデータセンター等の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 しなければならない。

② 装置の取り付け

(a) 情報システム管理者は、サーバ及びネットワーク機器等の取り付けに当たり、必要に応じて次の管理策を実施する。

【共通事項】

- 取り外しや転倒を防ぐため、適切に固定すること。
- 許可を受けた以外の者が装置等の変更、追加を行うことができないよう必要な対策を実施すること。

【機密性２以上、完全性２又は可用性２】

- 施錠可能なラック等に収容すること。

(b) 情報システム管理者は、サーバ及びネットワーク機器等の適切な運転のため、次のような電源等管理を行う。

- 適切に停止又は連続運転を行うため、予備電源を備えること。
- 電源設備の容量を把握、予測し、電力の安定供給に努めること。
- 主電源の停電時用として非常時照明を備えること。
- 落雷による事故や障害から保護するため、落雷防護対策を実施すること。

(c) 情報システム管理者は、サーバ及びネットワーク機器等の適切な運転のため、次のような配線等管理を行う。

- 電源ケーブル及び通信ケーブルの配線について、傍受又は損傷等による影響を最小限にするよう必要な対策を実施すること。
- 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機関サーバを冗長化し、同一データを保持すること。

③ 装置の保守

(a) 情報システム管理者は、サーバ及び配線等の装置について、実施手順に従って定期的な点検を行う。

(b) 情報システム管理者は、保守の実施内容について記録し保管する。

(c) 情報システム管理者は、保守を実施する目的でサーバ等の装置を庁外に搬出する場合、必要な保護対策を実施する。

(3) 職員等の利用する端末や電磁的記憶媒体等の管理

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のワイヤーによる固定、モバイル端末の使用時以外の施錠保管等の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パスワードの入力を必要とするように設定しなければならない。

③ 情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。

④ 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指紋認証等の二要素認証を併用しなければならない。

⑤ 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しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、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しなければならない。

⑥ 情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、必要な対策措置を講じなければならない。

4　人的セキュリティ

(1) 職員等及び外部委託事業者の役割、責任

① 職員等

(a) 職員等は、ポリシーに定められている事項を遵守する。

(b) 職員等は、情報セキュリティに関して定められた役割及び責任を認識し遵守する。

(c) 職員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報管理者に相談し、指示等を受ける。

(d) 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管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、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。

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

- 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、情報管理者の許可を得なければならない。
- 職員等は、外部で情報処理業務を行う場合には、情報管理者の許可を得なければならない。

(f) 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の制限

- 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。
- 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を遵守しなければならない。

(g) 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管理者の許可なく変更してはならない。

(h) 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。

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

② 外部委託事業者等

(a) ネットワーク及び情報システムの開発、保守、運用に関わる業務を外部委託事業者に委託する場合は、その委託に関して責任を有する課等を明確にする。

(b) 外部委託に関して責任を有する課等は、信頼性を確保するために次のような要件を定め、外部委託事業者が条件に合致しているか確認する。

- 再委託先も含めた経営状況
- 検査要求事項等に関する契約
- 技術情報の開示

(c) 外部委託に関して責任を有する課等は、外部委託事業者から再委託を受ける事業者も含めて、次のような事項を明記した契約を締結する。

【共通事項】

- ポリシー及び実施手順の遵守
- 業務上知り得た行政情報の守秘義務
- 提供された情報資産の目的外利用及び受託者以外の者への提供の禁止
- 提供された情報資産の返還義務
- 本町に対する報告義務
- 本町による定期的な報告徴収、監査、検査の実施
- 従業員に対する教育の実施
- ポリシー遵守のための体制
- ポリシーが遵守されなかった場合の規定(損害賠償等)

【機密性３Ｃ以上】

- 庁外への搬送時における盗難防止策の厳重な実施
- 不正コピー等の防止策の厳重な実施
- 外部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

(d) 外部委託に関して責任を有する課等は、契約内容が遵守されていることを定期的に確認する。

(e) 外部委託に関して責任を有する課等は、外部委託事業者に対し、委託業務の遂行中の身分証明書の携帯を求め、契約で定められた資格を有するものが従事しているか必要に応じて確認する。

(2) 教育、訓練

① 委員会

(a) 委員会は、職員等及び外部委託事業者に対し、教育及び啓発を通じポリシーの周知徹底を図る。

(b) 委員会は、職員等がその役割、責任に応じて情報セキュリティに関する教育、訓練等を定期的に受けられるようにするための計画を策定する。

(c) 委員会は、情報セキュリティに関する教育、訓練の効果を点検し、必要に応じて内容等の見直しを行う。

② 統括責任者

統括責任者は、委員会の策定した計画に基づき、教育、訓練を実施する。

③ 情報管理者及び情報システム管理者

(a) 情報管理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役割、責任に応じて教育を受ける。

(b) 非常勤及び臨時職員への対応

- 情報管理者は、非常勤及び臨時職員に対し、採用時にポリシー等のうち、非常勤及び臨時職員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。
- 情報管理者は、非常勤及び臨時職員の採用の際、必要に応じ、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。
- 情報管理者は、非常勤及び臨時職員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。

④ 職員等

職員等は、情報セキュリティに関する役割、責任に応じた教育、訓練を受ける。

(3) 事故、欠陥に対する報告

① 職員等

(a) 職員等は、情報セキュリティインシデント、システム上の欠陥及び誤動作を発見した場合には、速やかに情報管理者及び情報システム管理者に報告する。

(b) 職員等は、住民から、本町が管理するネットワーク及び情報システムに関する事故、欠陥及び誤動作に関する報告、連絡を受けた場合には、速やかに情報管理者及び情報システム管理者に報告する。

(c) 職員等は、事故、欠陥等の原因調査時には、協力する。

② 情報システム管理者

(a) 情報管理者は、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。

(b) 情報管理者及び情報システム管理者は、情報セキュリティインシデント、システム上の欠陥及び誤動作を自ら発見又は報告を受けた場合には、速

やかに統括責任者に報告する。

(c) 情報管理者及び情報システム管理者は、統括責任者からの指示を受け、事故、欠陥発生時に必要な対策を実施する。

(d) 外部委託に関して責任を有する課等は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

③ 統括責任者

(a) 統括責任者 は、機密性２以上、完全性２又は可用性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。

(b) 統括責任者は、情報セキュリティインシデント、システム上の欠陥及び誤動作の報告を受けた場合には、事故、欠陥発生時に必要な対策を検討し、関連する情報管理者及び情報システム管理者に対しこれを指示する。

(c) 統括責任者は、情報セキュリティインシデントを引き起こした部門の情報管理者、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と連携し、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、委員会に報告しなければならない。

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

④ 委員会

(a) 委員会は、情報セキュリティインシデント、欠陥等の分析結果の報告を受け、再発防止に必要な対策を実施する。

(b) 委員会は、分析結果の報告書を、必要と認められる期間、記録として保管する。

5　技術的セキュリティ

(1) 情報システム及び情報資産の管理

① アクセス制御

(a) 情報システム管理者は、所管する情報システムについて、情報管理者により設定された個々の情報資産に対するアクセス権限に基づき、アクセス制限を設ける。

(b) 情報システム管理者は、所管する情報システムについて、住民又は第三者による利用を認める場合、他の情報システムに影響を与えないよう対策を実施する。

② 事象の記録

(a) 情報システム管理者は、所管する情報システムに対するアクセス及び実施手順で定められた事象について、次のような事項を記録する。

- 利用者ID
- ログイン及びログアウトの日時
- 端末又は所在が特定できるID
- アクセスに成功及び失敗した記録
- その他実施手順に定める事項

(b) 情報システム管理者は、将来の調査及びアクセス制御を補うために、取得した記録を実施手順で定められた期間、適切な方法で保存する。

(c) 統括責任者及び情報システム管理者又は委員会から承認を得た者は、記録を定期的に確認し、情報システムの使用状況を把握する。

(d) 統括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が取得する記録について、対策や保護がなされているのかを確認する。

③ 情報システムの復旧

(a) 情報システム管理者は、情報システムに障害が発生した場合、迅速な復旧を行えるような対策を実施する。

(b) 情報システム管理者は、情報システムが障害時に迅速な復旧を行えるかどうか確認するために、定期的に検査する。

④ 情報資産のバックアップ

(a) 情報システム管理者は、情報資産を記録した媒体のバックアップを作成する。

(b) 情報システム管理者は、情報資産の重要度分類に応じてバックアップの取得間隔、保存期間などを設定する。

⑤ 情報システムに関する文書の管理

情報システム管理者は、情報システムに関する文書等を、電磁的記録媒体の形態に関わらず適切に保管する。

・ 情報システム構成図
・ 情報システム仕様書
・ その他情報システム管理者が必要と認める文書

⑥ 情報システムの入出力情報

(a) 情報システム管理者は、情報システムに入力される行政情報に対し、それが正確で適切であることを確実にするためのチェックを実施できるよう対策を実施する。

(b) 情報システム管理者は、情報システム内において、エラー又は故意の行為により行政情報が改ざんされる恐れがある場合、これを検出できるよう対策を実施する。

(c) 情報システム管理者は、改ざんの有無を検出し、必要な場合は行政情報の修復を実施できるよう対策を実施する。

(d) 情報システム管理者は、情報システムから出力される行政情報に対し、保存された情報の処理が正しく反映され、出力されることを確実にするための確認を実施できるよう対策を実施する。

⑦ 情報資産の暗号化と電子署名

(a) 機密性３Ｃ以上、完全性２又は可用性２の情報資産を電子媒体に保管する場合は、必要に応じて実施手順で定められた方式による暗号化を実施する。

(b) 機密性３Ｃ以上、完全性２又は可用性２の情報資産を庁外へ送信又は電子媒体に格納して搬出する際には、必要に応じて実施手順で定められた方式による電子署名の付与及び暗号化を実施する。

⑧ 文書サーバの設定等

(a) 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、職員等に周知しなければならない。

(b) 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、設定しなければならない。

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

⑨ 複合機のセキュリティ管理

(a) 統括責任者は、複合機を調達する場合、当該複合機が備える機能、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、適切なセキュリティ要件を策定しなければならない。

(b) 統括責任者は、複合機が備える機能について適切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。

(c) 統括責任者は、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。

⑩ 特定用途機器のセキュリティ管理

統括責任者は、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実施しなければならない。

⑪ 電子メールのセキュリティ管理

(a) 統括責任者は、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。

(b) 統括責任者は、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。

(c) 統括責任者は、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。

(d) 統括責任者は、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。

(e) 統括責任者は、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、外部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。

⑫ 電子メールの利用制限

(a) 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。

(b) 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。

(c) 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。

(d) 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。

(e) 職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

(2) 情報システム及び情報資産の利用

① 情報システムの利用に関する原則

(a) 職員等は、業務目的のみに情報システム資源を利用する。

(b) 統括責任者は、職員等の情報システム利用について、明らかに業務に関係のない情報システム利用を発見した場合は、情報管理者に通知し適切な措置を求めなければならない。

(c) 職員等は、インターネット等を経由した機密性２以上、完全性２又は可用性２の送受信を行う場合、情報管理者の許可を得る。

② ソフトウェア及び機器構成の維持

(a) 職員等は、各自に供用された端末等のソフトウェア及び機器の構成を原則として維持し、無断で構成変更を行ってはならない。

(b) 職員等は、各自に供用された端末等に対し、未承認ソフトウェアの導入や機器構成の変更が業務上必要な場合は、事前に情報システム管理者の承認を得る。

(c) 職員等は、導入されたソフトウェアの設定等の変更が業務上必要な場合は、事前に情報システム管理者の承認を得る。なお、導入する際は、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。

(d) 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。

③ 情報システムの入出力情報

(a) 職員等は、情報システムに入力される行政情報に対し、それが正確で適切であることを確実にするための確認を行う。

(b) 職員等は、情報システムから出力される行政情報に対し、保存された情報の処理が正しく反映され、出力されることを確実にするための確認を行う。

(c) 情報管理者は、入出力時に行政情報が漏洩、破壊、改ざんされないよう対策を実施する。

④ 情報及びソフトウェアの交換

情報システム管理者は、組織間において、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際の取扱いについて実施手順を定める。

(3) アクセス制御

① 利用者登録

(a) 情報システム管理者は、職員等の採用、退職、異動、出向、職務変更等が発生した場合、情報管理者の指示に基づき、情報システムに対するアクセス権限の登録、変更、抹消等の処理を速やかに実施する。

(b) 情報システム管理者は、職員等の情報システムに対するアクセス権限を管理する。

(c) 情報システム管理者は、職員等の情報システムに対するアクセス権限が適切に付与されていることを確実にするため、次の事項を定期的に確認

する。

・ アクセス権限が付与されている職員等の人数が必要最小限であること。

・ それぞれの職員等に付与されているアクセス権限が、業務上必要な権限のみであること。

(d) 統括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。

② 管理者権限

(a) 情報システムの管理者権限は、委員会の承認を得た情報システム管理者に与えることができる。

(b) 情報システム管理者は、統括責任者が業務上やむを得ないと認めた場合、その管理者権限を代行して使用する者（情報システム担当者）を指名することができる。

(c) 情報システム管理者は、管理者権限の使用者の登録、変更、抹消等が発生した場合、速やかに統括責任者に報告する。

(d) 統括責任者は、管理者権限の使用者及びそれぞれの使用者に付与されている権限に関する管理簿を作成し、常に最新の状態に保つ。

(e) 統括責任者は、管理者権限が適切に付与されていることを確実にするため、次の事項を定期的に確認し、委員会に報告する。

・ 管理者権限の使用者の人数が必要最小限であること。

・ それぞれの使用者に付与されている管理者権限が、必要最小限の管理機能を使用するための権限のみであること。

(f) 情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

(g) 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。

③ ログイン手順

情報システム管理者は、職員等が情報システムにログインするための実施手順を定める。ログイン手順は、正当なアクセス権限を持つ職員等がログインすることを確保するために、次のような条件を満たす内容とする。

・ メッセージ及びログイン試行回数の制限

・ アクセスタイムアウトの設定

・ ログイン、ログアウト時刻の表示等

④ 認証情報（ID、パスワード等）の管理方法

(a) 職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

・ 自己が利用している ID は、他人に利用させてはならない。
・ 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。

(b) 職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
・ 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。
・ 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。
・ 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。
・ 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。
・ 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。
・ 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。
・ 仮のパスワードは、最初のログイン時点で変更しなければならない。
・ 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。
・ 職員等間でパスワードを共有してはならない。

(c) 情報システム管理者は、職員等が認証情報を変更もしくは再発行を要求した場合、職員等の本人確認を確実に実施する。

(d) 情報システム管理者は、第三者への漏洩防止のために、認証情報を暗号化する等の取扱い方法を実施手順に定める。

⑤ IC カード等の取扱い

(a) 職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。
・ 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。
・ 業務上必要のないときは、IC カード等をカードリーダ若しく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。
・ IC カード等を紛失した場合には、速やかに統括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。

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

(c) 統括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。

⑥ 接続時間の制限

情報システム管理者は、情報システムへの接続について、必要最小限の接続となるように接続時間の制限を設ける。

⑦ 庁内ネットワークのアクセス制御

(a) 情報システム管理者は、職員等によってアクセスされるネットワークが、業務上必要最小限となるように構成する。

(b) 情報システム管理者は、アクセス権限を有しない職員等によるネットワークへのアクセスを制限する。

(c) 情報システム管理者は、許可されていない端末等からのアクセスを防止するため、次のような施策によってネットワーク経路上の制限を設ける。

- 相互にアクセスする必要がないネットワーク及びネットワークサービス間を分離すること。
- 業務上、使用する必要のない通信プロトコルを遮断すること。

(d) 情報システム管理者は、端末等をネットワークに接続する際に、端末等の固有情報によってネットワークへのアクセス可否を自動的に判別できるようにネットワーク機器等を設定する。

⑧ 無線LANの管理

(a) 機密性２以上、完全性２又は可用性２の行政情報を送信する場合、情報漏洩防止策として、伝送系路上の暗号化等を行うこと。

(b) 無線LANを導入する場合、接続の目的、技術要件に関して情報システム管理者、統括責任者、及び最高情報統括責任者に事前に申請し、承認を得ること。

(c) 庁内で無線LANを使用している場合、職員等や委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続してはならない。（一般町民等不特定多数による利用を想定したパブリックなネットワークの場合を除く 。）

⑨ 庁外からのアクセス

(a) 情報システム管理者は、庁外からのアクセスが必要な場合は、その利用目的等について委員会に報告し、承認を得る。

(b) 情報システム管理者は、庁外からの不正なアクセスを防止するため、次のような対策を実施する。

- 利用者及びアクセス可能な情報資産を必要最小限に限定すること。
- アクセス方法及び利用方法等を、利用者の本人確認が確実に実施できる内容とすること。
- その他情報システム管理者が必要と認める事項。

(c) 委員会は、庁外からのアクセスについて、その利用目的等が適切で、必要な対策が実施されると認められるものについて、必要最小限の範囲でこれを承認する。

(d) 統括責任者は、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。

(e) 統括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。

(f) 職員等は、町が貸与し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なければならない。

(g) 統括責任者は、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。

⑩ 外部ネットワークとの接続

(a) 情報システム管理者は、ネットワーク又は情報システムを外部ネットワークと接続する必要がある場合は、統括責任者と協議し、庁内全てのネットワーク、情報システム及び情報資産に影響が生じないと明確に確認した上で、接続の目的等について委員会に報告し、承認を得る。なお、確認に当たっては、その外部ネットワークについてあらかじめ次の事項を調査し、その根拠とする。

- ネットワーク構成。
- 機器構成。
- セキュリティレベル。
- その他情報システム管理者が必要と認める事項。

(b) 情報システム管理者は、外部ネットワークとの接続に際しては、伝送経路上における破壊、盗聴、改ざん、消去等に対して十分留意したネットワーク構成を採用し、適切に管理する。

(c) 情報システム管理者は、外部ネットワークの瑕疵により行政情報の漏洩、破壊、改ざん又はシステムダウン等による業務への影響に対処するため、外部ネットワークの管理責任者による損害賠償責任を約款サービスの上限とすることを契約上担保する。

(d) 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。

(e) 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

括責任者の判断に従い、速やかに外部ネットワークを物理的に遮断する。

(f) 委員会は、庁内から外部ネットワークへの接続について、その利用目的等が適切で、必要な対策が実施されると認められるものについて、必要最小限の範囲でこれを承認する。

(g) 統括責任者は、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。

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

(i) 統括責任者は、機密性２以上、完全性２又は可用性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、回線を冗長構成にする等の措置を講じなければならない。

(４) 情報システムの調達、開発、導入、保守等

① 情報システムの調達、開発、導入、保守時に定める事項

情報システム管理者は、情報システムの調達、開発、導入、保守時の作業における事故、不正行為対策のため、次のような事項を定める。

- 作業の責任者及び監督者
- 作業担当者及び業務範囲
- 作業記録の提出義務
- 作業において一時的に使用する情報システムと本町の運営する情報システムとの分離
- 作業者のアクセス制限
- 作業者のアクセス権限等の不要となった時点での速やかな抹消
- 作業の際の許可されていないソフトウェアの使用禁止
- 作業に伴う機器搬出入の際の情報システム管理者の許可及び確認
- 守秘義務
- 再委託管理
- その他情報システム管理者が必要と認める事項

② 情報システムの調達

(a) 統括責任者は、情報システムの調達に当たり、計画書を作成し、委員会の承認を得る。

(b) 統括責任者は、情報システムの調達に当たっては、一般に公開する調達仕様書が計画書に基づくようにする。

(c) 統括責任者は、機器及びソフトウェアを購入等する場合は、その製品の仕様が計画書に基づいているか確認する。

(d) 統括責任者は、情報システムの調達が完了するまでに、その運用に関する実施手順書を作成する。

③ 情報システムの開発

(a) 情報システム管理者は、システム開発の責任者及び作業者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。

(b) 情報システム管理者は、システム開発の責任者及び作業者が使用する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。

(c) 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。

(d) 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。

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

④ 情報システムの導入、移行

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

(b) 情報システム管理者は、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。

(c) 情報システム管理者は、新たに情報システムを導入する際には、事前に十分な試験を行い、既存の情報システムに影響が発生しないことを確認する。

(d) 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、試験データに使用してはならない。

(e) 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試験を行う場合、開発した組織と導入する組織が、それぞれ独立した試験を行わなければならない。

(f) 情報システム管理者は、試験に使用した行政情報及びその結果を委員会へ提出するとともに試験結果を一定期間厳重に保管する。

(g) 情報システム管理者は、情報システムを移行する場合、移行の内容、必要性、計画等を文書にて委員会に提出し、承認を得る。

(h) 情報システム管理者は、情報システムを移行する場合、事前に移行後と同等の擬似環境にて情報システムが動作することを確認する。

(i) 情報システム管理者は、情報システムを移行する際に、情報システムに記録されている情報資産の保存が確実に行われていることを確認し、復帰が即座に可能な状態にする。

(j) 情報システムの移行作業は、原則として執務時間外に行う。また、作業を行う際には、複数の職員等が相互に作業内容を確認しながら実施し、作業進捗状況を記録する。

⑤ 情報システムの保守、更新

(a) 情報システム管理者は、ソフトウェア等の更新、又は修正プログラムの導入を計画的に実施する。

(b) 情報システム管理者は、ソフトウェア等を更新、又は修正プログラムを導入する場合、事前に不具合及び他の既存情報システムに対する影響を調査し、問題がないことを確認した上で、統括責任者に報告する。

(c) 情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかに対応する。

(d) 情報システム管理者は、記憶媒体を含む機器を、外部の事業者に修理又は廃棄委託する場合、事前にその内容が消去された状態であることを確認する。

(e) 情報システム管理者は、事前に情報資産を消去することが難しい場合、修理を委託する事業者に対し秘密保持に関する契約を締結する。

⑥ システム開発・保守に関連する資料等の整備・保管

(a) 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に整備・保管しなければならない。

(b) 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。

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

⑦ 情報システムの変更管理

統括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。

⑧ 情報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。

(5) コンピュータウイルス等の不正プログラム対策

① 不正プログラム対策の原則

(a) ネットワークを利用して情報又はプログラムを送受信する際には、ネッ

トワークとの境界、サーバ、クライアント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実施し、不正プログラムの侵入及び拡散の防止を図る。

(b) 電磁的記録媒体を利用して庁外と情報又はプログラムをやり取りする場合には適宜コンピュータウイルス等不正プログラムのチェックを実施し、不正プログラムの侵入及び拡散の防止を図る。

② 不正プログラム対策

(a) 情報システム管理者は、コンピュータウイルス対策として、次の事項を実施する。

- 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ること。
- 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つこと。
- 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つこと。
- 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ないこと
- 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。
- 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、町が許可している媒体以外を職員等に利用させないこと。

(b) 職員等は、コンピュータウイルス対策として、次の事項を実施する。

- 庁外から情報又はプログラムを取り入れる場合には、必ずコンピュータウイルス等不正プログラムのチェックを実施すること。
- コンピュータウイルス等不正プログラムのチェックは、処理を途中で中断せず最後まで実施すること。
- 差出人が不明又は不自然に添付されたファイルは実行せずに速やかに削除すること。
- 情報システム管理者が提供するコンピュータウイルス等の不正プログラムに関する情報を常に確認すること。
- 添付ファイルのある電子メールを送受信する場合は、コンピュータウイルス等不正プログラムのチェックを実施すること。
- 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ないこと。
- パソコン等の端末に対して、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。

・ パソコン等の端末が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、LAN ケーブルの即時取り外しを行い、速やかに情報システム管理者へ報告を行うこと。
・ クラウドサービスを利用する場合は、利用形態及び責任分界に応じて、不正プログラムへの対策、必要最小限の通信設定、マルウェア対策並びにログの取得及び監視等を適切に実施すること。
・ クラウドサービス事業者が実施する対策については、サービス利用前にその内容を確認するとともに、利用期間中も定期的に報告を求めるなどにより、適切に実施されていることを確認する。
・

③ コンピュータウイルス被害に関する履歴の記録

情報システム管理者は、職員等からのコンピュータウイルス被害に関する報告、及びコンピュータウイルスによって引き起こされた情報システムの障害に対する対処履歴等を記録し、常に活用できるよう分類、保存する。

(6) 不正アクセス対策

① 不正アクセス対策

(a) 統括責任者は、不正アクセス対策として、次の事項を実施する。

・ 統括責任者は、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。
・ クラウドサービスを利用する場合は、本町の情報セキュリティポリシーに定めるアクセス制御、認証及び権限管理に関する要件を満たすことを、利用前に確認しなければならない。
・ クラウドサービスの利用に当たっては、利用者及び委託事業者等のアクセス権限を適切に管理し、特に管理権限を有するアカウントについては、多要素認証その他必要な安全管理措置を講じなければならない。
・ 認証情報、利用者ID又はアクセス権限の管理をクラウドサービス事業者の機能又は運用に依拠する場合は、その安全性及び管理方法が本町の情報セキュリティポリシーに適合することを、利用前及び利用期間中に確認しなければならない。

(b) 情報システム管理者は、不正アクセス対策として、次の事項を実施する。

・ 情報システムのセキュリティホールの発見に努め、メーカー等から修正プログラムの提供があり次第、安全を確認した上で、計画的かつ速やかに修正プログラムを反映すること。
・ 重要な情報システムの設定に係るファイル等について、定期的に改ざ

んの有無を検査する。

- 使用終了後、又は使用される予定のないネットワークの物理的、論理的ポートは、速やかに使用できないような制限を施す。
- 不正アクセスによるウェブページ等の改ざん防止を確実にするために、ウェブページ等の不正な書き換えを検出し、情報システム管理者へ通報する仕組みを導入するよう設定すること。
- 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。

② 既知の不正アクセスに対する未然の防止

(a) 情報システム管理者は、攻撃を受けることが明確な場合、システムの停止を含む必要な対策を実施する。

(b) 情報システム管理者は、関係機関との連絡を密にして既知の不正アクセスに関する情報の収集に努める。

③ 犯罪行為に対する対応

(a) 情報システム管理者は、不正アクセス禁止法違反等犯罪の可能性がある攻撃を受けた場合、記録の保存に努めるとともに、委員会に対し報告する。

(b) 委員会は、情報システム管理者から報告を受けた攻撃に関し、警察、関係機関との緊密な連携に努める。

④ 職員等による過失

職員等の怠惰が原因で行政情報の漏洩、破壊、改ざん又は情報システムの障害等が発生し、行政業務に深刻な影響をもたらした場合、当該職員等を地方公務員法等による処分の対象とする。

⑤ 職員等による不正アクセス行為

(a) 情報システム管理者は、職員等による不正アクセスがあった場合、委員会に通知し、適切な処置を求める。

(b) 職員等による不正アクセスの結果、行政情報の漏洩、破壊、改ざん又は情報システムの障害等が発生し、行政業務に深刻な影響をもたらした場合、その職員等を地方公務員法等による処分の対象とし、悪質な場合には刑事告発の対象とする。

⑥ サービス不能攻撃

統括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

統括責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や

入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

(7) セキュリティ情報の収集

- 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、所管する情報システムについて、必要な対策を実施する。
- 統括責任者は、これらの情報を定期的にとりまとめ、関係部局等に通知する。
- 情報システム管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は、緊急時対応計画に定める情報連絡先に連絡する。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。

6　運用

(1) 緊急時対応計画

① 緊急時対応計画の策定

(a) 委員会は、情報資産に影響を及ぼす情報セキュリティインシデントが発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な対策を迅速かつ円滑に実施し、再発防止の対策を実施するため、緊急時対応計画を定める。

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

(c) 委員会は、緊急対応計画について定期的に見直す。

(d) 統括責任者 は、緊急時対応を想定した訓練を定期的に実施しなければならない。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。

② 連絡先

委員会は、次の連絡先を把握し、緊急時対応計画に掲載する。

- 町長
- 最高情報統括責任者
- 委員会
- 統括責任者
- 情報管理者
- 情報システム管理者
- 情報システムに係る外部委託事業者
- 宮城県庁
- 宮城県警察
- 関係機関
- 影響が考えられる個人及び法人

③ 事案（情報セキュリティインシデント）の分類

委員会は、情報セキュリティインシデントが情報資産に及ぼす影響を考慮し、情報セキュリティインシデントの分類を定め、緊急時対応計画に掲載する。

④ 事案(情報セキュリティインシデント)の報告、連絡

(a) 委員会は、情報セキュリティインシデントが発生した、あるいはその疑いが発見された場合の報告手順を定め、緊急時対応計画に掲載する。報告事

項には、次のような項目を含む。

- 情報セキュリティインシデントの症状の分類
- 情報セキュリティインシデントが発生した原因として想定される行為又は事象
- 情報セキュリティインシデントによる被害、影響範囲
- 情報セキュリティインシデント発見時の現状記録等

(b) 委員会は、次のような情報セキュリティインシデントが発生した場合の連絡先を定め、緊急時対応計画に掲載する。

- ネットワークを通じた大規模な攻撃等により、住民に重大な被害が生じる恐れがあるとき。
- 不正アクセス等の犯罪行為により、被害が生じる恐れがあるとき。
- 踏み台攻撃に利用され、他者に被害を与える恐れがあるとき
- その他情報システムに関する被害が生じる恐れがあるとき。
- その他情報資産に関する被害が生じる恐れがあるとき。

⑤ 事案(情報セキュリティインシデント)に対する対処

(a) 委員会は、情報セキュリティインシデントが発生した場合の対処手順を定め、緊急時対応計画に掲載する。対処手順には、次のような事項を含む。

(b) 情報システム管理者は、次のような情報セキュリティインシデントが発生し、情報資産を保護するためにネットワークからの切断がやむを得ないと判断した場合は、統括責任者の了承の上、ネットワークから切断することができる。

- 異常なアクセスが継続して発生しているとき。
- 情報システムの運用に著しい支障をきたす攻撃が継続して発生しているとき。
- 不正アクセスと判断されるアクセスがあるとき。
- コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき。
- その他情報資産に係る重大な影響が懸念されるとき。

(c) 情報システム管理者は、次のような情報セキュリティインシデントが発生し、情報資産を保護するために情報システムの停止がやむを得ないと判断した場合は、統括責任者の了承の上、情報システムを停止することができる。

- コンピュータウイルス等不正プログラムが情報資産に深刻な影響を及ぼしているとき。
- 災害等により電源を供給することが危険又は困難なとき。
- その他情報資産に係る重大な影響が懸念されるとき

(d) 情報システム管理者は、ネットワークの切断及び情報システムの停止に当たっては、統括責任者の了承の上で実施することを原則とするが、情報資産の被害の拡大を速やかに停止させる必要がある場合には、事後報告とすることができる。

(e) 情報システム管理者は、必要と認められる暫定対策を実施した後、情報セキュリティインシデントからの復旧方法を検討し、実施する。復旧を行うに当たっては、次のような記録の取得等に努める。

- 情報セキュリティインシデントに係るシステムのアクセス記録及び現状の保存
- 情報セキュリティインシデントに対処した経過の記録
- 情報セキュリティインシデントに係る証拠の保全

⑥ 再発防止

(a) 情報システム管理者は、情報セキュリティインシデントからの復旧後、必要と認められる期間、再発監視を行う。

(b) 統括責任者は、発生した情報セキュリティインシデントに係る原因を調査及び分析し、その結果を元にポリシー及び実施手順の改善に係る再発防止計画案を策定し、委員会に報告する。

(c) 委員会は、ポリシー及び実施手順の改善に係る再発防止計画案が有効であるか否か検討し、有効であると認められる場合は、これを承認する。

(d) 統括責任者は、承認された再発防止計画について、発生した情報セキュリティインシデントの概要と併せ職員等に周知徹底を図る。

⑦ 業務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、委員会は当該計画とポリシーの整合性を確保しなければならない。

(2) 運用管理

① 情報セキュリティ実施手順の策定

(a) 情報管理者及び情報システム管理者は、所管する情報資産に関する実施手順を必要に応じて策定し、維持、管理を行う。

(b) 情報管理者及び情報システム管理者は、職員等が常にポリシー及び必要な実施手順を参照できるよう配慮する。

② 情報システムの監視

(a) 情報システム管理者は、実施手順に定められたアクセス制御に違反している事象の検知及び情報セキュリティインシデントが生じた場合の証拠となるような事象を記録するため、常に情報システムを監視する。

(b) 情報システム管理者は、外部ネットワークと接続するシステムについて

は、ネットワークに対する侵入の確認が行える装置を設置し、アクセス履歴の監視等により、不正アクセス及び異常な操作等の監視を実施する機能を設ける。

(c) 情報システム管理者は、庁内のシステムについては、アクセス履歴の監視等により、不正アクセス及び異常な操作等の監視を実施する機能を設ける。

(d) 情報システム管理者及び統括責任者は、監視により得られた結果を元に、監視対象の情報資産に対する盗難、改ざん、消去等から保護するための対策を実施する。

(e) 情報システム管理者及び統括責任者は、情報セキュリティに関連した事象の記録を監査記録とし、その正確性を保証するため、サーバ内の時計の同期を取る等、正確な記録を取得するよう設定する。

(f) 情報システム管理者及び統括責任者は、監査記録を安全な場所に保管する。

(g) 情報システム管理者及び統括責任者は、クラウドサービス事業者の選定において、必要となるリソースの容量・能力が確保できること、サービスの使用において必要な監視機能が備わっていることを確認すること。

③ ポリシーの遵守状況の確認

(a) 職員等は、ポリシー違反の疑いを発見した場合には、速やかに情報管理者に報告する。

(b) 情報管理者は、所管する業務においてポリシーが遵守されているかどうか又は問題が発生していないかについて定期的に実態を調査する。

(c) 情報システム管理者は、構成情報等運用しているシステムの状況がポリシーに遵守している状態か、また他の情報セキュリティ上の問題が発生していないか定期的に確認する。

(d) 情報管理者及び情報システム管理者は、情報セキュリティ上の問題が発生していると判断した場合には、速やかに統括責任者に報告する。

(e) 統括責任者は、報告を受けた問題に対して速やかに調査を行い、適切に対処する。

(f) 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責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

④ 運用管理における留意事項

(a) 統括責任者は、次のような運用管理に必要な情報資産へのアクセス権限について定期的に見直す。

・ 情報資産へのアクセス記録

・ 電子メール記録
・ 個人のプライバシーに抵触する可能性のある情報資産

(b) 個人情報の保護に関する法律（平成15年5月30日 法律第57号）に関係する情報資産へのアクセス権限については、法令に定められた手続きに従う。

(3) 例外措置

① 例外措置の許可

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

② 緊急時の例外措置

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

③ 例外措置の申請書の管理

最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

7　外部サービスの利用（クラウドサービスを含む）

(1) 約款による外部サービスの利用

① 約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要度分類Ⅱ以上の情報が取扱われないように規定しなければならない。

- 約款によるサービスを利用してよい範囲
- 業務により利用する約款による外部サービス
- 利用手続及び運用手順

② 約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

(2) クラウドサービスの利用

① 情報セキュリティ管理者は、クラウドサービスを利用する場合には、取り扱う情報の重要度分類及び取扱制限を踏まえ、利用の可否を判断しなければならない。

② 情報セキュリティ管理者は、クラウドサービス事業者の選定に当たり、保存先の国・地域、再委託の有無、ログの取得、障害時の連絡体制、利用終了時の情報の返却及び削除の方法その他責任分界点に関する事項を確認しなければならない。

③ 統括責任者は、クラウドサービスの特性や責任分界点を踏まえ、導入・構築、運用・監視、障害対応及び利用終了時の移行・削除に関する実施手順を整備しなければならない。

④ クラウドサービス上で機密性の高い情報を保存する場合は、暗号化その他必要な措置により機密性を確保し、利用終了時には復元困難な状態で削除されることを確認しなければならない。

(3) ソーシャルメディアサービスの利用

① ソーシャルメディアサービスを利用する際は、情報セキュリティ管理者の許可を得てサービス申請を行うこと。

② 情報セキュリティ管理者は、本町が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(a) 本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自己記述欄等にアカウントの運用

組織を明示する等の方法でなりすまし対策を行うこと。

(b) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

③ 機密性２以上、完全性２又は可用性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。

④ 利用するソーシャルメディアサービスのアカウントごとの責任者を定めなければならない。

８　法令遵守

(１) 職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従う。

- 地方公務員法（昭和25年法律第261号）
- 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)
- 著作権法(昭和45年法律第48号)
- 個人情報の保護に関する法律(平成15年5月30日 法律第57号)
- 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）
- 加美町情報公開条例（平成15年4月1日 条例第10号）
- 加美町電子計算機処理に係る個人情報の保護に関する条例（平成15年4月1日 条例第11号）

(２) 情報システム管理者及び統括責任者は、情報システムにおいて利用するソフトウェア、サービス、ライブラリその他の情報資産等について、利用形態にかかわらず、ライセンス条項、利用規約その他の利用条件を確認し、これに従う。

9　情報セキュリティに関しての違反に対する対応

(1) 違反に対する対応

- 情報システム管理者は、情報セキュリティに関する違反を確認した場合は、速やかに統括責任者に連絡する。
- 統括責任者は、情報システム管理者から情報セキュリティ違反の報告を受けた場合、違反した職員等が所属する課等の情報管理者に通知し、適切な対応を求める。ただし、情報システム管理者が情報管理者と兼務の場合は、統括責任者が適切な対応を実施する。
- 情報システム管理者は、情報管理者又は統括責任者の指導によっても違反が改善されない場合、その職員等のネットワーク又は情報システムの使用に関する権利を、必要と認められる期間停止あるいは剥奪することができる。
- 情報システム管理者は、違反した職員等の権利を停止あるいは剥奪した場合、その旨を統括責任者及びその職員等が所属する課等の情報管理者に通知する。
- 情報システム管理者は、違反が解消されたことを委員会及び違反した職員等が所属する課等の情報管理者が確認した場合、その職員等のネットワーク又は情報システムの使用に関する権利を従前の状態に復旧させることができる。

(2) 違反に対する処分

情報セキュリティに関する違反を行った職員等及びその監督責任者に対しては、その重大性、発生した情報セキュリティインシデントの状況等に応じて地方公務員法等による処分の対象とする。

１０　評価、見直し

(1) 監査

① 実施方法

最高情報統括責任者は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度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

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

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

③ 監査実施計画の立案及び実施への協力実施方法

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

(b) 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に委託している場合、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、情報セキュリティ委員会に報告する。

⑥ 保管

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

⑦ 監査結果への対応

最高情報統括責任者 は、監査結果を踏まえ、指摘事項を所管する情報管理者に対し、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。

⑧ 情報セキュリティポリシー及び関係規程等の見直し等への活用

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

(2) 点検

① 情報管理者は、情報セキュリティ対策がポリシーを遵守して実施されているか定期的に点検する。

② 情報管理者は、①の点検結果をとりまとめ、委員会に報告する。

③ 職員等は、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。

④ 委員会は、この点検結果を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しなければならない。

(3) ポリシーの更新

- 委員会は、監査及び点検の結果を踏まえ、定期的にポリシーの遵守性、有効性等を評価する。
- 委員会は、評価の結果、改善の必要を確認した場合、速やかに改善案をとりまとめる。
- 委員会は、改善の一環としてポリシーを更新した場合、更新後のポリシーの周知徹底を図る。

附 則

このポリシーは、平成１６年８月１日より施行する。

附 則

このポリシーは、平成２９年４月１日より施行する。

附則

このポリシーは、令和８年３月３１日より施行する。