糸島市情報セキュリティポリシー

令和６年１月４日　改正

目次

第１章　総則

（目的）

第１条　この情報セキュリティポリシーは、糸島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。

（定義）

第２条　この情報セキュリティポリシーにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

⑴　職員等　糸島市の情報資産を取扱う職員、会計年度任用職員、業務委託を行っている委託先事業者の社員、派遣労働者等をいう。

⑵　ＩＤ　コンピュータやネットワークの利用者を識別するための符号をいう。

⑶　コンピュータ　パソコン及びサーバ（いずれもソフトウェアを含む。以下同じ。）並びにその周辺機器で、機器内部に情報を記録可能なものをいう。

⑷　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。

⑸　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。

⑹　個別業務システム　情報システムのうち、個別業務の情報処理を行う仕組みをいう。

⑺　情報資産　情報システムを構成する機器及びそのシステムで取り扱うすべての電磁的記録（電磁的記録の印刷物及び電磁的記録の入力の基となった届出書等の紙媒体の文書を含む。）並びに情報システムの開発、運用に係る紙媒体の文書をいう。

⑻　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。

(9) 記録媒体　情報を記録するための媒体で、ハードディスク、USBメモリ、CD-R、DVD-R等をいう。

(10) 庁内 LAN　市役所本庁舎及び公共施設等を接続した、糸島市で最も主要なネットワークをいう。

(11) ASP等　糸島市でサーバ等を保有せず、ネットワークを介して必要なサービスを利用する情報システムの利用形態をいう。

(12) 個人情報　個人に関する情報であって、特定の個人が識別され、又は識別され得るもの（法人その他の団体に関して記録された情報に含まれる当該法人その他の団体の役員に関する情報を除く。）をいう。

(13) 特定個人情報　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。以下「番号法」という。）に規定する個人番号を含む個人情報をいう。

(14) 非公開情報　糸島市情報公開条例（平成22年糸島市条例第17号）第９条各号のいずれかに該当する情報をいう。

(15) 情報セキュリティインシデント　情報漏えい、不正アクセス、ウイルス感染、その他情報システムの欠陥及び誤動作、情報セキュリティポリシーの違反等のことをいう。

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

(17) 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。

(18) 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。）。

(19) 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。

(20) 認証カード　マイナンバー利用事務系のコンピュータの利用者認証を行うための IC カードのことをいう。

(21) 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。

(22) 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。

(23) 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。

(24) 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。

(25) 無害化通信　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。

（対象とする脅威）

第３条　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。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　この情報セキュリティポリシーが適用される機関は、市長、議会事務局、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び公営企業管理者の権限を行う市長及び消防長とする。

２　この情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

⑴　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

⑵　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。）

⑶　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

（職員等の遵守義務）

第５条　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴　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。

⑵　情報資産の分類と管理

本市の保有する情報資産を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実施する。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報

システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

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

③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。また、高度な情報セキュリティ対策として、福岡県自治体情報セキュリティクラウドを通じてインターネットに接続する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

① 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。

② 約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

③ 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する。

(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情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

第２章　組織体制

（最高情報セキュリティ責任者）

第９条　最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）は、副市長とする。

２　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に関する最終決定権限及び責任を有する。

３　CISO 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。

（統括情報セキュリティ責任者）

第 10 条　統括情報セキュリティ責任者は、経営戦略部長とする。

２　統括情報セキュリティ責任者は、CISO を補佐しなければならない。

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

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、情報セキュリティ管理者及び情報システム・セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

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おそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

６　統括情報セキュリティ責任者は、本市の庁内 LAN、情報システム及び情報資産に関する情報セキュリティポリシーの維持・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、情報システム・セキュリティ管理者、情報セキュリティ責任者、情報セキュリティ管理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。

（情報システム・セキュリティ管理者）

第 11 条　情報システム・セキュリティ管理者は、情報政策課長とする。

２　情報システム・セキュリティ管理者は、本市の全てのネットワークにおける開発、設定の変更、見直し等を行う権限及び責任を有する。

３　情報システム・セキュリティ管理者は、情報システム及び情報資産における情報セキュリティに関する権限及び責任を有する。

（情報セキュリティ責任者）

第 12 条　情報セキュリティ責任者は、各部等の長とする。

２　情報セキュリティ責任者は、所管する部等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

３　情報セキュリティ責任者は、所管する個別業務システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

４　情報セキュリティ責任者は、所管する個別業務システムについて、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並びに職員等に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）

第 13 条　情報セキュリティ管理者は、各課等の長とする。

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

３　情報セキュリティ管理者は、所管する課等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害の恐れがある場合には、情報セキュリティ責任者、情報システム・セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

（情報セキュリティ委員会）

第 14 条　情報セキュリティ委員会は、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、情報システム・セキュリティ管理者で構成する。

２　情報セキュリティ委員会は、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等、情報セキュリティに関する重要な事項を決定する。

３　情報セキュリティ委員会の会議は CISO が招集し、その議長となる。

４　情報セキュリティ委員会において必要と認めるときは、会議に構成員以外の者の出席を求め、その説明又は意見を聴くことができる。

５　情報セキュリティ委員会の庶務は、情報政策課において処理する。

（CSIRT の設置・役割）

第 15 条　CISO は、CSIRT を整備し、その役割を明確化しなければならない。

２　CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

３　CISO は、情報セキュリティに関する一括窓口を整備し、情報セキュリティインシデントについて部課等より報告を受けた場合には、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。

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

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

６　CSIRT は、情報セキュリティインシデントを認知した場合には、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　CSIRT は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

（クラウドサービス利用における組織体制）

第 16 条　情報セキュリティ責任者は、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。

第３章　情報資産の分類と管理

（情報資産の分類）

第 17 条　本市が保有する情報資産は、その重要度に応じ、次表に従って区分し、区分に応じた情報セキュリティ対策を行うものとする。

区分	重要性分類
Ⅰ	特定個人情報を含む情報資産（以下「重要性分類の区分Ⅰに該当する情報資産」という。）
Ⅱ	個人情報及び非公開情報を含む情報資産（以下「重要性分類の区分Ⅱに該当する情報資産」という。）
Ⅲ	個人情報及び非公開情報を含まないが、一般に広く公開されていない情報資産（以下「重要性分類の区分Ⅲに該当する情報資産」という。）
Ⅳ	ホームページ、出版物等に掲載し、一般に広く公開されている情報資産（以下「重要性分類の区分Ⅳに該当する情報資産」という。）

（情報資産の管理）

第 18 条　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。

２　情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も前条の分類に基づき管理しなければならない。

３　情報セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても、前条の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定めなければならない。

４　情報セキュリティ管理者は、クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

（情報の作成）

第 19 条　職員等は、業務上必要のない情報を作成してはならない。

２　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（情報資産の入手）

第 20 条　職員等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。

２　庁外の者が作成した情報資産を入手した者は、第 17 条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

３　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。

（情報資産の利用）

第 21 条　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。

２　情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

３　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第 22 条　情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

２　重要性分類の区分Ⅰに該当する情報資産のうち、電磁的記録については、情報セキュリティ管理者が決定したパスワードの設定を行った上で、管理区域に設置している機器のうちマイナンバー利用事務系のコンピュータで構成するネットワークに接続している機器に保存するものとし、当該機器以外には保存してはならない。また、重要性分類の区分Ⅰに該当する情報資産のうち、紙媒体の文書については、施錠可能な場所に保管しなければならない。

３　重要性分類の区分Ⅱに該当する情報資産は、施錠可能な場所に保存及び保管しなければならない。また、電磁的記録については、情報セキュリティ管理者が決定したパスワードの設定を行った上で保存しなければならない。

４　重要性分類の区分Ⅲに該当する情報資産は、可能な限り施錠可能な場所に保存及び保管しなければならない。

（情報の送信）

第 23 条　電子メール等により、インターネットを通じて重要性分類の区分Ⅱ以上に該当する情報資産を送信してはならない。ただし、他に合理的な手段が無く、パスワード等による暗号化を行った上で情報セキュリティ管理者がこれを認めた場合には、この限りでない。

（情報資産の運搬）

第 24 条　車両等により重要性分類の区分Ⅱ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、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

２　重要性分類の区分Ⅲ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に許可を得なければならない。

（情報資産の提供・公表）

第 25 条　重要性分類の区分Ⅱ以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

２　重要性分類の区分Ⅲ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。

３　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

（情報資産の廃棄等）

第 26 条　職員等は、保存している情報資産が糸島市文書規程（平成 22 年訓令第３号）に定める保存年限を経過した場合には、速やかに当該情報資産を廃棄しなければならない。

２　職員等は、情報資産を廃棄する場合は、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。

３　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の重要性分類の区分に応じ、情報を復元できないように処置しなければならない。

４　情報資産の廃棄やリース返却等を行う者は、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。

５　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

６　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

（情報資産の利用状況等の記録）

第 27 条　情報セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産のうち、情報システムに記録された以外の電磁的記録を新たに作成する場合には、電磁的記録の名称及び保存場所、特定個人情報を利用する組織の名称、作成した職員等の氏名、記録される項目及び本人として記録される個人の範囲、利用目的及び収集方法について記録しなければならない。

２　情報セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産の持ち出し又は送信（以下「送信等」という。）を認めた場合には、送信等を行った職員等の氏名、送信等の相手及び日時を記録しなければならない。

３　情報セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産を廃棄する場合には、廃棄を行った職員等の氏名、廃棄した日時及び廃棄方法を記録しなければならない。

４　情報システム・セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産のうち電磁的記録の利用状況等を確認するために、当該アクセス状況等を記録し、一定期間保存しなければならない。

（情報資産の取扱区域及び事務取扱担当者の指定）

第 28 条　情報セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産の漏えい等

を防止するために、当該情報資産を取り扱う事務を実施する取扱区域を指定しなければならない。また、情報の漏えい等がないよう物理的な措置を講じなければならない。

2　情報セキュリティ管理者は、重要性分類の区分Ⅰに該当する情報資産を取り扱う職員等を事務取扱担当者として指定しなければならない。また、当該事務取扱担当者が取り扱う特定個人情報の範囲についても、明確にしておかなければならない。

第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系）

第 29 条　情報システム・セキュリティ管理者は、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。

２　情報システム・セキュリティ管理者は、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

３　情報システム・セキュリティ管理者は、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）を用いなければならない。

４　情報システム・セキュリティ管理者は、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。

５　情報システム・セキュリティ管理者は、マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

６　情報システム・セキュリティ管理者は、マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施するものとし、その場合の暗号は十分な強度を持たなければならない。また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

（LGWAN 接続系）

第 30 条　情報システム・セキュリティ管理者は、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。

２　情報システム・セキュリティ管理者は、インターネット接続系からメールやデータを 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。

⑴　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 LGWAN 接続系に転送するメールテキスト化方式

⑵　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

⑶　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

３　情報システム・セキュリティ管理者は、LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

（インターネット接続系）

第 31 条　情報システム・セキュリティ管理者は、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　情報システム・セキュリティ管理者は、福岡県自治体情報セキュリティクラウドに参加するとともに、関係省庁や福岡県等と連携しながら、情報セキュリティ対策を推進しなければならない。

第５章　物理的セキュリティ対策

（サーバ等の管理）

第 32 条　情報システム・セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

２　情報システム・セキュリティ管理者は、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が安全に稼動できるよう、必要に応じてサーバの二重化等の措置を講じなければならない。

３　情報システム・セキュリティ管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、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。

４　情報システム・セキュリティ管理者は、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、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

５　情報システム・セキュリティ管理者は、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。

６　情報システム・セキュリティ管理者は、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に、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。また、通信ケーブル及び電源ケーブルの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。

７　情報システム・セキュリティ管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

８　情報システム・セキュリティ管理者は、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講じなければならない。

９　情報システム・セキュリティ管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

10　情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記録装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

11　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

（管理区域の管理）

第 33 条　情報システム・セキュリティ管理者は、施設管理部門と連携して、管理区域から外部へ通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

2　情報システム・セキュリティ管理者は、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。

3　情報システム・セキュリティ管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

4　情報システム・セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、IC カード及び入退室管理簿の記載による入退室管理を行わなければならない。

5　職員等は、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。

6　情報システム・セキュリティ管理者は、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。

7　情報システム・セキュリティ管理者は、管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

8　情報システム・セキュリティ管理者は、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、あらかじめ職員等に確認を行わせなければならない。

9　情報システム・セキュリティ管理者は、管理区域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。

（通信回線及び通信回線装置の管理）

第 34 条　情報システム・セキュリティ管理者は、庁内 LAN に接続する通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

2　情報システム・セキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

3　情報システム・セキュリティ管理者は、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　情報セキュリティ責任者は、新たな個別業務システムを庁内 LAN に接続又は ASP 等により庁内 LAN から利用する場合は、事前に情報システム・セキュリティ管理者の許可を得なければならない。

5　情報システム・セキュリティ管理者は、新たな情報システムを庁内 LAN に接続又は ASP 等により庁内 LAN から利用する場合、既存の情報システムに与える影響等を調査した上で許可を行わなければならない。

6　情報システム・セキュリティ管理者は、重要性分類の区分Ⅱ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、必要な情報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。

7　情報システム・セキュリティ管理者は、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講じなければならない。

8　情報システム・セキュリティ管理者又は、情報セキュリティ管理者は、重要性分類の区分Ⅱ以上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。

（コンピュータ及び記録媒体の管理）

第 35 条　情報セキュリティ管理者は、所管しているコンピュータ及び記録媒体（CD-R、DVD-R 等の記録メディアを除く）について、管理台帳を作成し、添付品まで含め定期的に所在を確認しなければならない。

2　職員等は、前項において作成された管理台帳に記載されている以外のコンピュータや記録媒体（CD-R、DVD-R 等の記録メディアを除く）を使用してはならない。なお、管理台帳に記載されている記録媒体であっても、マイナンバー利用事務系のコンピュータ及び LGWAN 接続系のコンピュータでは使用してはならない。ただし、LGWAN 接続系のコンピュータでの使用については、情報システム・セキュリティ管理者の許可を得た場合はこの限りではない。

3　職員等は、LGWAN 接続系のコンピュータとインターネット接続系のコンピュータで記録媒体（CD-R、DVD-R 等の記録メディアを除く）を共用してはならない。

4　職員等は、コンピュータや記録媒体を庁舎外に持ち出してはならない。ただし、インターネット接続系のコンピュータ及びインターネット接続系のコンピュータで使用する記録媒体については、止むを得ない合理性があり、情報セキュリティ管理者の許可を得た場合はこの限りではない。

5　職員等は、市が管理するコンピュータで外部から持ち込まれた記録媒体を使用してはならない。ただし、インターネット接続系コンピュータでの使用については、止むを得ない合理性があり、情報セキュリティ管理者の許可を得た場合はこの限りではない。

6　情報セキュリティ管理者は、前２項において許可した内容の記録を作成し、保管しなければならない。

7　職員等は、退庁時にはコンピュータや記録媒体を可能な限り施錠可能な場所に保管しなければならない。施錠保管ができないコンピュータについては、ワイヤーによる固定等の盗難防止のための物理的措置を講じなければならない。

8　職員等は、使用しているコンピュータから一定時間以上離れる時は、ログアウトを行

う等、なりすまし及び画面の覗き見を防止する措置をとらなければならない。

第６章　人的セキュリティ対策

（職員等の遵守事項）

第 36 条　職員等は、情報セキュリティの重要性について認識するとともに、この情報セキュリティポリシーを遵守しなければならない。

２　職員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

３　職員等は、使用しているパソコンや記録媒体等について、第三者に使用されること又は許可なく情報を閲覧されることがないように、パソコンのロックや記録媒体の保管等、適切な措置を講じなければならない。

４　職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

５　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情報セキュリティ管理者が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める情報セキュリティポリシーに従い、情報システム・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。

６　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。

７　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。

８　職員等は、パソコン、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。

９　職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理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。

10　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情報セキュリティ管理者へ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。

11　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。

12　情報セキュリティ管理者は、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、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。

13　情報セキュリティ管理者は、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。

14　情報システム・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を閲覧できるよう掲示しなければならない。

15　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及び保守等を事業者に発注する場合、再委託事業者も含めて、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。

（研修・訓練）

第 37 条　統括情報セキュリティ責任者は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

２　統括情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

３　統括情報セキュリティ責任者は、全ての職員等を対象とする情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

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

５　統括情報セキュリティ責任者は、新規採用の職員等を対象とする情報セキュリティ研修を実施しなければならない。

６　情報セキュリティ管理者は、所管する課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。

７　情報システム・セキュリティ管理者は、研修の実施状況を分析、評価し、–統括情報セキュリティ責任者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。

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

９　統括情報セキュリティ責任者は、緊急時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。

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

11　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。

（情報セキュリティインシデントの報告）

第 38 条　職員等は、情報セキュリティインシデントを認知した場合は、情報セキュリティ緊急時対応計画（以下「緊急時対応計画」という。）に従い、速やかに一括窓口に報告しなければならない。

（認証カードの取り扱い）

第 39 条　職員等は、自己の管理する認証カードに関し、次の事項を遵守しなければならな

い。

(1)　認証カードを、職員等間で共有してはならない。

(2)　業務上必要のないときは、認証カード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。

(3)　認証カードを紛失した場合には、速やかに情報システム・セキュリティ管理者に通報し、指示に従わなければならない。

2　情報システム・セキュリティ管理者は、認証カードの紛失等の通報があり次第、当該認証カード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。

3　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、認証カードを廃棄する場合、切替え前の認証カード等を回収し、破砕するなど復元不可能な処理を行わなければならない。

（ID の取り扱い）

第 40 条　職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

(1)　自己が利用している ID 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。

（パスワードの取扱い）

第 41 条　職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(1)　パスワードは、他者に知られないように管理しなければならない。

(2)　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(3)　パスワードは、十分な長さとし、文字列は想像しにくいものにしなければならない。

(4)　パスワードが流出したおそれがある場合は、情報セキュリティ管理者及び情報システム・セキュリティ管理者へ速やかに報告し、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、統合ログイン等シングルサインオン以外のパスワードについて、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、共用 ID に対するパスワードは除く）。

第７章　技術的セキュリティ対策

（ファイルサーバの設定等）

第 42 条　情報システム・セキュリティ管理者は、職員等が使用できるファイル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。

２　情報システム・セキュリティ管理者は、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及びファイルを閲覧及び使用できないように、設定しなければならない。

３　情報システム・セキュリティ管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、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。

（バックアップの実施）

第 43 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、所管する業務システムのデータベースやファイルサーバ及び庁内 LAN に接続されている記録媒体等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

２　情報システム・セキュリティ管理者又は情報セキュリティ管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（他団体との情報システムに関する情報等の交換）

第 44 条　情報セキュリティ管理者は、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、情報システム・セキュリティ管理者の許可を得なければならない。

（システム管理記録及び作業の確認）

第 45 条　情報システム・セキュリティ管理者は、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・セキュリティ管理者は、所管する情報システムについて、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正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・セキュリティ管理者及び契約により操作を認められた委託事業者が重要な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。

（情報システム仕様書等の管理）

第 46 条　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（ログの取得等）

第 47 条　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

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

３　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者からの不正侵入、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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応についても、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

４　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（障害記録）

第 48 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第 49 条　情報システム・セキュリティ管理者は、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を設定しなければならない。

２　情報システム・セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適正な制御を施さなければならない。

（外部の者が利用できるシステムの分離等）

第 50 条　情報システム・セキュリティ管理者は、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。

（外部ネットワークとの接続制限等）

第 51 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、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・セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

３　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

４　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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・セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、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。

（複合機のセキュリティ管理）

第 52 条　情報セキュリティ管理者は、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　情報セキュリティ管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

３　情報セキュリティ管理者は、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。

（IoT 機器を含む特定用途機器のセキュリティ管理）

第 53 条　情報セキュリティ管理者は、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。

（無線 LAN 及びネットワークの盗聴対策）

第 54 条　統括情報セキュリティ責任者及び情報セキュリティ責任者は、所管するネットワークにおいて無線 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付けなければならない。

２　統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第 55 条　統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

２　統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合には、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。

（電子メールの利用制限）

第 56 条　職員等は、自動転送機能を用いて、市が管理しないアカウントに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は、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。

（電子署名・暗号化）

第 57 条　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

２　職員等は、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、CISO が定めた方法で暗号化を行うための鍵を管理しなければならない。

３　CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）

第 58 条　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、情報システム・セキュリティ管理者及び情報セキュリティ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は、ソフトウェアのライセンスを管理しなければならない。

３　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（機器構成の変更の制限）

第 59 条　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、情報システム・セキュリティ管理者及び情報セキュリティ管理者の許可を得なければならない。

（業務外ネットワークへの接続の禁止）

第 60 条　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム・セキュリティ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　情報システム・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する。

３　職員等は、情報システム・セキュリティ管理者の許可なくコンピュータやネットワーク機器を庁内 LAN に接続してはならない。

４　職員等は、持込みを許可された私物のパソコン、スマートフォン及びタブレット端末等を庁内ＬＡＮ以外のネットワークに接続（無線による接続を含む。）する場合は、当該ネットワークを所管する情報セキュリティ管理者の許可を得なければならない。

５　前項について、情報システム・セキュリティ管理者は、情報セキュリティ管理者に対し、許可及び接続状況の報告を求めることができる。

（業務以外の目的でのウェブ閲覧の禁止）

第 61 条　職員等は、業務以外の目的でウェブを閲覧してはならない。

２　情報システム・セキュリティ管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

（Web 会議サービスの利用時の対策）

第 62 条　職員等は、Web 会議の参加者や取り扱う情報の区分に応じ、以下の情報セキュリティ対策を実施しなければならない。

①　原則として、支給された端末を利用すること。

②　重要性分類の区分Ⅱ以上の情報を取り扱う場合は、可能な限りエンドツーエンドの暗号化を行うこと。

③　重要性分類の区分Ⅱ以上の情報を取り扱う場合は、議事録作成機能、自動翻訳機能及び録画機能等、エンドツーエンドの暗号化を利用できなくなる機能を可能な限り使用しないこと。

④　重要性分類の区分Ⅱ以上の情報については、資料共有、チャットへの書き込み等、保存が可能となる操作をしないこと。

⑤音声を取り扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

2　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、以下の対策を講じなければならない。

①　会議室にアクセスするためのパスワード等をかけること。

②　会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知すること。

③　原則として待機室を設け、参加者と確認できた者だけを会議室に入室させること。

④　なりすましや入れ替わりが疑われるなどの不審な参加者を、会議室から退室させること。

（ソーシャルメディアサービスの利用）

第 63 条　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。

⑴　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。

⑵　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

⑶　重要性分類の区分Ⅱ以上の情報はソーシャルメディアサービスで発信しないこと。

⑷　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ること。

2　重要性分類の区分Ⅲ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。

（アクセス制御等）

第 64 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないようにシステム上制限しなければならない。

2　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱いを適正に行わなければならない。

3　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、情報システム・セキュリティ管理者に通知しなければならない。

4　情報システム・セキュリティ管理者は、利用されていないＩＤ及び認証カードが放置

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。

（特権を付与されたIDの管理等）

第65条　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、管理者権限等の特権を付与されたID及び認証カードを利用する者を必要最小限にし、当該ID及び認証カードのパスワード漏えい等が発生しないよう、当該ID及び認証カードのパスワードを厳重に管理しなければならない。

2　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、特権を付与されたID及び認証カードのパスワードの変更について、委託事業者に行わせてはならない。

3　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、特権を付与されたID及び認証カードの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、入力回数の制限等のセキュリティ機能を強化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・セキュリティ管理者は、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。

（職員等による外部からのアクセス等の制限）

第66条　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、情報システム・セキュリティ管理者及び当該情報システムを管理する情報セキュリティ管理者の許可を得なければならない。

2　情報システム・セキュリティ管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

3　情報システム・セキュリティ管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

4　情報システム・セキュリティ管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

5　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

6　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、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　情報システム・セキュリティ管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、「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多要素認証に加えて通信内容の暗号化等、情報セキュリティ

確保のために必要な措置を講じなければならない。

（自動識別の設定）

第 67 条　情報システム・セキュリティ管理者は、庁内 LAN で使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（ログイン時の表示等）

第 68 条　情報システム・セキュリティ管理者は、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。

（認証情報の管理）

第 69 条　情報システム・セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。

２　情報システム・セキュリティ管理者は、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、初回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・セキュリティ管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（特権による接続時間の制限）

第 70 条　情報システム・セキュリティ管理者は、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。

（情報システムの調達）

第 71 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第 72 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

３　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、システム開発の

責任者及び作業者のアクセス権限を設定しなければならならない。

4　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

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

（情報システムの導入）

第 73 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

2　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

3　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

4　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

5　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

6　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

7　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

（システム開発・保守に関連する資料等の整備・保管）

第 74 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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・セキュリティ管理者及び情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

（情報システムの変更管理）

第 75 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発・保守用のソフトウェアの更新等）

第 76 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

（システム更新又は統合時の検証等）

第 77 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

（不正プログラム対策）

第 78 条　情報システム・セキュリティ管理者は、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、必要に応じて職員等に対して注意喚起しなければならない。

(4)　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、所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

(5)　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(6)　不正プログラム対策ソフトウェアは、常に最新の状態を保たなければならない。

(7)　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、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。

(8)　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・セキュリティ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。

(9)　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

２　職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　情報システム・セキュリティ管理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。

⑺　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、緊急時対応計画の手順に従って対応を行わなければならない。

（専門家の支援体制）

第 79 条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（不正アクセス対策）

第 80 条　統括情報セキュリティ責任者は、不正アクセス対策として、次の事項を遵守しなければならない。

⑴　使用されていないポートを閉鎖しなければならない。

⑵　不要なサービスについて、機能を削除または停止しなければならない。

⑶　不正アクセスによるウェブページの改ざんを防止するためにデータの書換えを検出し、情報セキュリティ管理者へ通報するよう、設定しなければならない。

⑷ 情報セキュリティに関する一括窓口と連携し、監視、通知、外部連絡窓口及び適正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。

⑸　本市が定めた情報セキュリティポリシーにおけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑹　クラウドサービスで利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑺　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、そ

の管理手順等が、情報セキュリティポリシーを満たすことを確認しなければならない。

（攻撃への対処）

第 81 条　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、福岡県等と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第 82 条　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。

（内部からの攻撃）

第 83 条　統括情報セキュリティ責任者は、職員等が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃が生じた場合に速やかに対応しなければならない。

（職員等による不正アクセス）

第 84 条　統括情報セキュリティ責任者は、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へ通知し、適正な処置を求めなければならない。

（サービス不能攻撃）

第 85 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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することができなくなることを防止するために、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第 86 条　統括情報セキュリティ責任者は、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。

（セキュリティホールに関する情報の収集）

第 87 条　情報システム・セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

２　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業

者に確認しなければならない。

（不正プログラム等のセキュリティ情報の収集・周知）

第 88 条　情報システム・セキュリティ管理者は、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。

（情報セキュリティに関する情報の収集及び共有）

第 89 条　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、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、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第８章　運用

（情報システムの監視）

第 90 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

３　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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　情報システム・セキュリティ管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

５　情報システム・セキュリティ管理者及び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は、イベントログを取得しなければならない。また、クラウドサービス事業者から提供されるログ取得機能が適切かどうかを確認しなければならない。

６　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）　サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）　クラウドサービス利用の終了手順

（ウ）　バックアップ及び復旧

（情報セキュリティポリシーの遵守状況の確認）

第 91 条　情報セキュリティ責任者及び情報セキュリティ管理者は、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。

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

３　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における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。

４　CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

5　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ管理者を通じて情報システム・セキュリティ管理者に報告を行わなければならない。

6　前項の違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合においては、職員等は、緊急時対応計画に従って適切に対処しなければならない。

7　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、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。

（侵害時の対応等）

第 92 条　統括情報セキュリティ責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

2　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。

⑴　関係者の連絡先

⑵　発生した事案に係る報告すべき事項

⑶　発生した事案への対応措置

⑷　再発防止措置の策定

3　統括情報セキュリティ責任者は、自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

4　統括情報セキュリティ責任者は、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。

（例外措置）

第 93 条　情報システム・セキュリティ管理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、例外措置を講じることができる。

2　情報セキュリティ管理者及び情報システム・セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

3　CISO 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。

（法令遵守）

第 94 条　職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これらに従わなければならない。

(1)　地方公務員法（昭和 25 年法律第 261 号）

(2)　著作権法（昭和 45 年法律第 48 号）

(3)　不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

(4)　個人情報の保護に関する法律（平成 15 年法律第 57 号）

(5)　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

(6)　サイバーセキュリティ基本法(平成 26 年法律第 104 号）

(7)　糸島市個人情報保護法施行条例（令和 5 年条例第 1 号）

２　統括情報セキュリティ責任者及び情報システム・セキュリティ管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする(IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

（懲戒処分等）

第 95 条　情報セキュリティポリシーに違反した職員等及びその監督責任者は､その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

２　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・セキュリティ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)　職員等が違反を確認した場合は、速やかに自己が所属する課等の情報セキュリティ管理者に報告し、報告を受けた情報セキュリティ管理者は、情報システム・セキュリティ管理者およ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。

(4)　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を 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。

第９章　業務委託と外部サービスの利用

（委託事業者の選定基準）

第 96 条　情報システム・セキュリティ管理者及び情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　情報システム・セキュリティ管理者及び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。

（契約項目）

第 97 条　重要性分類の区分Ⅱ以上の情報資産を取扱う業務を委託する場合には、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。

⑴　糸島市個人情報保護法施行細則第６条各号に定める事項
⑵　情報セキュリティポリシーの遵守
⑶　委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
⑷　提供されるサービスレベルの保証
⑸　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
⑹　委託事業者の従業員に対する教育の実施
⑺　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
⑻　業務上知り得た情報の守秘義務
⑼　再委託に関する制限事項の遵守
⑽　委託業務終了時の情報資産の返還、廃棄等
⑾　委託業務の定期報告及び緊急時報告義務
⑿　市による監査、検査
⒀　市による情報セキュリティインシデント発生時の公表
⒁　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（確認・措置等）

第 98 条　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、前条の契約に基づき措置を実施しなければならない。また、その内容を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。

（外部サービスの利用基準(重要性分類の区分Ⅱ以上の情報を取り扱う場合)）

第 99 条　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（重要性分類の区分Ⅱ以上の情報を取り扱う場合）の利用に関する基準を定めなければならない。

⑴　外部サービスの選定条件

(2) 外部サービスの利用に係る調達・契約
(3) 再委託
(4) 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
(5) 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
(6) 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
(7) 外部サービスの利用手続き
(8) 外部サービス利用中の取扱い
(9) 外部サービス利用終了時の取扱い

（外部サービスの利用基準(重要性分類の区分Ⅱ以上の情報を取り扱わない場合））

第 100 条　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(重要性分類の区分Ⅱ以上の情報を取り扱わない場合）の利用に関する基準を定めなければならない。

(1) 外部サービスの選定条件
(2) 外部サービスの利用に係る調達・契約
(3) 再委託
(4) 外部サービスの利用手続き
(5) 外部サービス利用中の取扱い
(6) 外部サービス利用終了時の取扱い

第 10 章　評価・見直し

（監査）

第 101 条　CISO は、情報セキュリティ監査責任者を指名し、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の対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

2　情報セキュリティ監査責任者は、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。

3　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。

4　情報セキュリティ監査責任者は、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に報告しなければならない。

5　被監査部門は、監査の実施に協力しなければならない。

6　事業者に業務委託を行っている場合、所管する情報セキュリティ管理者は、委託事業者（再委託事業者含む）に対して、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。

7　情報セキュリティ監査責任者は、監査結果を取りまとめ、CISO に報告する。

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

9　CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、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。

10　情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程の見直し、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。

（自己点検）

第 102 条　統括情報セキュリティ責任者及び情報システム・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、毎年度及び必要に応じて自己点検を実施しなければならない。

2　統括情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

3　職員等は、前項の自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

4　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（情報セキュリティポリシー及び関係規程等の見直し）

第 103 条　統括情報セキュリティ責任者は、情報セキュリティ監査及び自己点検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に評価を行い、必要があると認めた場合、改善を行うものとする。

（委任）

第 104 条　この情報セキュリティポリシーに定めるもののほか必要な事項は、CISO が定める。