八幡市情報セキュリティポリシー

令和 6 年 9 月一部改定版

２００４（平成１６）年　１月１９日策定
２００７（平成１９）年　３月３０日全部改定
２００９（平成２１）年　６月３０日一部改定
２０１４（平成２６）年　９月３０日一部改定
２０１６（平成２８）年　９月２０日一部改定
２０２０（令和　２）年　８月２１日一部改定
２０２１（令和　３）年　８月１２日一部改定
２０２３（令和　５）年　８月２９日一部改定
２０２４（令和　６）年　９月　９日一部改定

八幡市ＩＴ推進本部

目次

はじめに 1
情報セキュリティポリシーの構成 1
第１章　情報セキュリティ基本方針 3
１．目的 3
２．定義 3
３．情報セキュリティポリシーの策定根拠 4
４．情報セキュリティポリシーの位置づけと職員等及び受託業者の遵守義務 4
５．対象とする脅威 4
６．適用範囲 5
７．情報セキュリティ対策 5
８．情報セキュリティ監査及び自己点検の実施 6
９．情報セキュリティポリシーの見直し 6
10．情報セキュリティ対策基準の策定 6
11．情報セキュリティ実施手順の策定 7
第２章　情報セキュリティ対策基準 8
１．組織・体制 8
２．情報資産の分類と管理 12
３．情報システム全体の強靭性の向上 14
４．物理的セキュリティ 16
４．１．サーバ等の管理 16
４．２．管理区域(情報システム室等)の管理 17
４．３．通信回線及び通信回線装置の管理 18
４．４．職員等の利用する端末や電磁的記録媒体等の管理 18
５．人的セキュリティ 19
５．１．職員等の遵守事項 19
５．２．研修・訓練 21
５．３．情報セキュリティインシデントの報告 22
５．４．ID 及びパスワード等の管理 23
６．技術的セキュリティ 24
６．１．コンピュータ及びネットワークの管理 24
６．２．アクセス制御 29
６．３．システム開発、導入、保守等 31
６．４．不正プログラム対策 33
６．５．不正アクセス対策 35
６．６．セキュリティ情報の収集 36

７．運用 37
７．１．情報システムの監視 37
７．２．情報セキュリティポリシーの遵守状況の確認 37
７．３．侵害時の対応等 38
７．４．例外措置 39
７．５．法令順守 39
７．６．情報セキュリティポリシー違反に対する対応 40
８．業務委託と外部サービス（クラウドサービス）の利用 40
８．１．業務委託 40
８．２．外部サービス（クラウドサービス）の利用（重要性分類Ⅱ以上の情報を取り扱う場合） 41
８．３．外部サービス（クラウドサービス）の利用（重要性分類Ⅱ以上の情報を取り扱わない場合） 45
９．評価・見直し 45
９．１．監査 45
９．２．自己点検 46
９．３．情報セキュリティポリシー及び関係規程等の見直し 47
【付録】用語解説 48

はじめに

セキュリティポリシーの目的

情報を収集し、保有し、又は利用しようとする者には、それぞれが目指すところ、目指す事柄に応じて自らの行動を律し、その実現に努めることが求められる。

この時に拠り所とした内容を総合し、又は集約したものを、制定形式に拘わらず行動規範と呼び、このうち、その者が管理すべき情報の価値を守り、又は当該情報のうち、秘匿すべきものの安全性を確保するために設定する方針、基準その他の措置を「情報セキュリティポリシー」と呼ぶ。

本市の情報管理施策の経過

- 平成　元年１２月「八幡市電子計算機の利用に係る個人情報の保護に関する条例」を施行
- 平成１１年１０月「八幡市情報公開条例」を施行
- 平成１３年　６月「八幡市個人情報保護条例」を施行
- 平成１５年　２月「八幡市コンピュータシステムの管理、運用及び情報保護に関する規則（以下「規則」という。）」をはじめとする１２の基準を施行
- 平成１６年　１月「八幡市情報セキュリティポリシー」を施行
- 平成１９年　３月「八幡市情報セキュリティポリシー」を全部改定
- 平成２１年　６月「八幡市情報セキュリティポリシー」を一部改定
- 平成２６年　９月「八幡市情報セキュリティポリシー」を一部改定
- 平成２８年　９月「八幡市情報セキュリティポリシー」を一部改定
- 令和　２年　８月「八幡市情報セキュリティポリシー」を一部改定
- 令和　３年　８月「八幡市情報セキュリティポリシー」を一部改定
- 令和　５年　８月「八幡市情報セキュリティポリシー」を一部改定

情報セキュリティポリシーの構成

八幡市情報セキュリティポリシーは、本市が組織的に管理する情報をどのような理念に基づき、どのように保護し、又は利用するのかについて、現行の法体系及び計画との関係を調整したうえで、総合的かつ体系的に取りまとめたものである。

規定する内容については、情報の資産的価値に着目してその保全を図るだけに留まらず、当該情報の主体（当事者）と密接に関係する様々な権利の保護の実現に資するものでなければならない。

さらに、この実行性を確保するためには、情報処理業務に携わる本市の職員等（規則第２条第１６号に規定する「職員等」をいう。）及び当該処理業務を受託した事業者（以下「受託業者」という。）に情報セキュリティポリシーを普及し、浸透し、及び定着させることが前提となるため、安定的な規範であることが望ましい。

他方、情報通信技術の急速な進歩・革新に伴う環境の変化、プライバシーを取り巻く社会情勢の変化へ柔軟に対応することも重要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と管理客

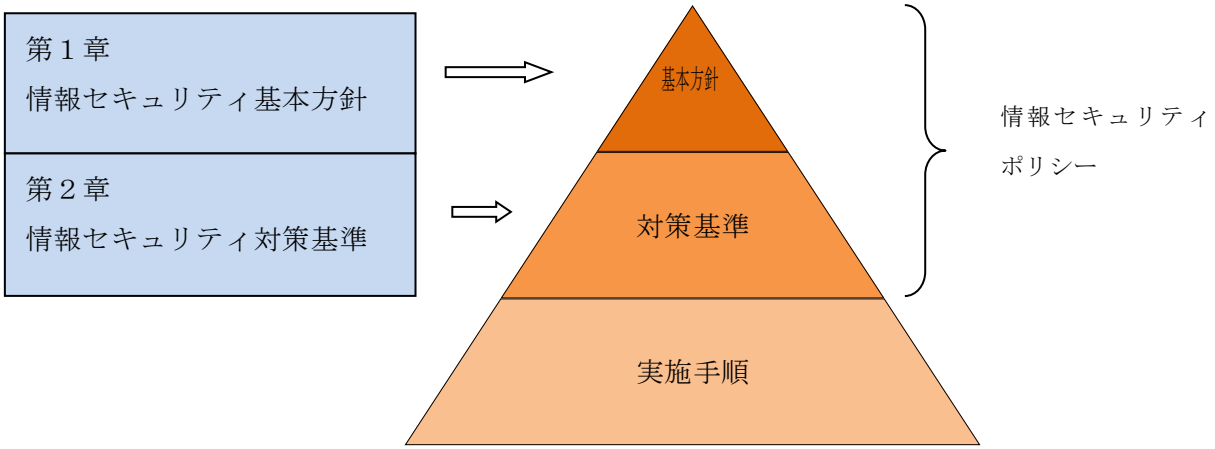
体を取り巻く状況の変化に即応する部分(対策基準)とに分けて策定することとした。

具体的には、情報セキュリティポリシーを「情報セキュリティ基本方針」及び「情報セキュリティ対策基準」２階層で構成することとし、これらに基づき、コンピュータシステムごとの具体的な情報セキュリティ対策の実施手順を示した「情報セキュリティ実施手順」を策定することとした(次頁参照)。

また、情報セキュリティポリシーに規定した義務、制限の実効性は、強制規範である法令等が、当該法令等の所掌する範囲内において担保すべき事柄であるとの考えから、コンピュータシステムの機能別の遵守事項を規則、規程、基準等として体系化することにより、情報管理施策を総合的に進めることとした。

情報セキュリティポリシーの階層的構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	「情報セキュリティポリシー」全体を統括する理念及び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
	情報セキュリティ対策基準	「情報セキュリティ基本方針」を実行に移すために本市が行政全般で利用するネットワーク、コンピュータシステム及びこれらを操作することにより作成され、又は保管される情報資産に関する情報セキュリティ対策の標準
情報セキュリティ実施手順		事案ごとにネットワーク、コンピュータシステム及び情報資産の保護対策を定める「情報セキュリティ対策基準」に基づく具体的な実施手順



第１章　情報セキュリティ基本方針

１．目的

本市が管理し、又は保有するコンピュータシステムが取り扱う情報には、市民等の個人情報、法人等の内部管理情報、行政運営上重要な情報等、外部へ漏えい、又は流出した場合には、極めて重大な事態を招くおそれのある情報が多数含まれている。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

このため、情報資産並びにそれを取り扱うコンピュータシステム及びネットワークを様々な脅威から防御することは、市民の生命、財産、プライバシー等を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠なものである。

さらに、ICT による行政の推進が積極的に進められる中、本市も ICT を活用し、業務効率化・高度化、住民サービスの向上等を行うためには、全てのネットワーク及びコンピュータシステムにおいて、高度な安全性を確保することは、最優先すべき課題である。

以上のことを踏まえて、本市の保有する情報の機密性、完全性及び可用性を維持するための対策を整備するために「八幡市情報セキュリティポリシー」（以下、「情報セキュリティポリシー」という）を定めるものである。

このうち、「情報セキュリティ基本方針」については、本市が情報セキュリティ対策を講ずるうえで根幹となり、また、展開される施策、実行される対策の是非を判定するための指針となるものであるため、一定の普遍性及び安定性を兼ね備えたものとし、かつ、ICT 関連の専門用語の使用を精査したうえで、情報セキュリティポリシーの位置づけ、対象範囲等について規定することとした。

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

本基本方針及び情報セキュリティ対策基準をいう。

（５）　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。

（６）　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。

（７）　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。

（８） 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（個人番号利用事務系を除く。）。

(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。

３．情報セキュリティポリシーの策定根拠

本市における情報セキュリティポリシーは、デジタル社会形成基本法第３３条に規定する「サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。第三十七条第二項第十四号において同じ。）の確保、情報通信技術を用いた犯罪の防止、情報通信技術を用いた本人確認の信頼性の確保、情報の改変の防止、高度情報通信ネットワークの災害対策、個人情報の保護その他の国民が安心して高度情報通信ネットワークの利用及び情報通信技術を用いた情報の活用を行うことができるようにするために必要な措置」及び個人情報の保護に関する法律第１２条に規定する「地方公共団体は、その機関が保有する個人情報の適正な取扱いが確保されるよう必要な措置」の一環として策定する。

４．情報セキュリティポリシーの位置づけと職員等及び受託業者の遵守義務

情報セキュリティポリシーは、個人情報保護条例、規則をはじめとする情報管理分野の法体系とともに、本市の情報セキュリティ対策における中核をなす非常に重要な規範である。

したがって、本市が保有する情報資産の管理業務又は処理業務に携わるすべての職員等（職員及び会計年度任用職員をいう。以下同じ。）及び受託業者は、情報セキュリティの重要性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は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

５．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、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、火災等の災害によるサービス及び業務の停止等

（4） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

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

6．適用範囲

（1） 行政機関の範囲

本基本方針が適用される行政機関は、市長部局、消防本部、教育委員会、選挙管理委員会、監査委員会、公平委員会、農業委員会、固定資産評価審査委員会、議会及び水道事業とする。

（2） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク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

7．情報セキュリティ対策

上記５の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1） 組織体制

本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。

（2） 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。

（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個人番号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、京都府及び京都府下市町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4） 物理的セキュリティ

サーバ、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。

（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。

クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。

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

（9） 評価・見直し

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。

８．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

９．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果等に基づき、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な場合には、情報セキュリティポリシーを見直す。

10．情報セキュリティ対策基準の策定

上記７、８及び９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。

11. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本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２章　情報セキュリティ対策基準

「情報セキュリティ対策基準」とは、本市が行政全般において利用するネットワーク、コンピュータシステム及びこれらを操作することにより作成され、又は保管される情報資産に関する情報セキュリティ対策の標準である。

この対策基準を的確に実行することが、前章において規定した「情報セキュリティ基本方針」を実現し、更には情報セキュリティポリシーの目的を達成することに繋がるものである。

１．組織・体制

本市の情報セキュリティ対策は、以下の組織・体制によって行うものとする。

この組織・体制は、情報セキュリティ対策の市全体への包括的、統一的かつ体系的な適用を実現するために、法令等の一義的な解釈に固執することなく柔軟な運用のもと、各執行機関の権限を市長の所轄のもとに一元化して表したものであるが、それぞれの執行機関が持つ独立性までも否定するものではない。

また、この組織・体制の確立によって、情報セキュリティ対策に関する意思決定の際の所属長、関係部課等への決裁、合議、供覧、報告等の個別の手続及び義務を妨げるものでもない。各執行機関の固有の権限と情報セキュリティポリシーの適用の間に疑義が生じた場合は、当面、市長の調整権により解決するものとする。

（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行政情報化担当課を担当する副市長を、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くものとする。

③CISO 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。

④CISO は、本ポリシーに定められた自らの担務を、副 CISO その他の本ポリシーに定める責任者に担わせることができる。

（２）　情報保護管理者（規則第５条に規定する「情報保護管理者」をいう。）

①行政情報化担当課長を、CISO 直属の情報保護管理者とする。情報保護管理者は CISO 及び副 CISO を補佐しなければならない。

②情報保護管理者は、本市の全てのネットワーク、及び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情報保護管理者は、本市の全てのネットワーク、及び所管する情報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情報保護管理者は、情報セキュリティ統括責任者、情報セキュリティ実行責任者、コンピュータシステム所管課長、システム管理者及びコンピュータシステム担当者に対して、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情報保護管理者は、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情報保護管理者は、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情報保護管理者は、緊急時等の円滑な情報共有を図るため、CISO、情報保護管理者、情報セキュリティ統括責任者、情報セキュリティ実行責任者、コンピュータシステム所管課長、システム管理者、コンピュータシステム担当者を網羅する連絡体制を整備しなければならない。

⑧情報保護管理者は、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情報保護管理者は、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） システム管理者

①本市の全てのネットワーク及び情報システムの管理運用並びに情報セキュリティに関する統一的な対策を実施するため、システム管理者を行政情報化担当課に置く。

②システム管理者は、ネットワーク、システム開発等の技術に関する専門的知識と公務員倫理を有し、CISO 及び情報保護管理者を補佐しなければならない。

③システム管理者は、管理する情報資産に対するセキュリティ侵害又はセキュリティ侵害の恐れのある場合には、CISO 及び情報保護管理者の指示に従い、CISO 及び情報保護管理者が不在の場合には自らの判断に基づき必要かつ十分な全ての措置を行う権限及び責任を有する。

④システム管理者は、次に掲げる事務を所掌する。

(ア)情報保護管理者の権限に属するネットワークの構築、運用、設定変更、更新等を実施し、管理し、審査する権限を有する。

(イ)情報保護管理者の権限に属するネットワークにおける情報システムの導入、運用、変更、更新等を管理し、審査する権限を有する。

(ウ)情報システムの本市の全てのネットワークへの接続に関すること。

(エ)本市の全てのネットワーク、情報システム及び端末装置の障害対応に関すること。

(オ)情報システムの外部との結合に関すること。

(カ)端末装置の設定並びに端末装置の本市の全てのネットワークへの接続に関すること。

(キ)本市の全てのネットワーク及び情報システムに係る委託契約の締結に関すること。

(ク)本市の全てのネットワーク及び情報システムに係る情報セキュリティ実施手順の策定、運用状況の点検、報告等に関すること。

（4） 情報セキュリティ統括責任者

①部長等の庁議構成員を情報セキュリティ統括責任者とする。

②情報セキュリティ統括責任者は、当該部局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統括的な権限及び責任を有する。

③情報セキュリティ統括責任者は、その所管する部局等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、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ統括責任者は、その所管する部局等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。

（5） 情報セキュリティ実行責任者

①課等の長及び施設等の長を情報セキュリティ実行責任者とする。

②情報セキュリティ実行責任者は、その所管する課室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情報セキュリティ実行責任者は、その所管する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ統括責任者、情報保護管理者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

（6） コンピュータシステム所管課長（規則第７条に規定する「コンピュータシステム所管課長」をいう。）

①各情報システムの担当課等の長及び施設等の長を、当該情報システムに関するコンピュータシステム所管課長とする。

②コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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。

（7） コンピュータシステム担当者

コンピュータシステム所管課長の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者をコンピュータシステム担当者とする。

（8） ＩＴ推進本部

①本市の情報セキュリティ対策を統一的に実施するため、ＩＴ推進本部において、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決定する。

②ＩＴ推進本部は、情報セキュリティポリシーに関する監査を行う。

（9） 兼務の禁止

①情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(10) 情報セキュリティに関する統一的な窓口（「庁内の CSIRT（Computer Security Incident Response Team)」以下、「庁内の CSIRT」という。）の設置・役割

①CISO は、庁内の CSIRT 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しなければならない。

②CISO 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。

③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、京都府等へ報告しなければならない。

④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。

⑤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。

(11) クラウドサービス利用における組織体制

①情報保護管理者は、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。

(12) クラウドサービス管理者

①各クラウドサービスの担当課等の長及び施設等の長を、当該クラウドサービスに関するクラウドサービス管理者とする。

②クラウドサービス管理者は、所管するクラウドサービスにおける選定、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クラウドサービス管理者は、所管するクラウドサービス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クラウドサービス管理者は、所管するクラウドサービスに係る情報セキュリティ実施手順の維持・管理を行う。

(13)　クラウドサービス許可権限者

①行政情報化担当課長を、クラウドサービス許可権限者とする。

②クラウドサービス許可権限者は、クラウドサービス利用における申請手続きについて、運用、見直し等を行う権限及び責任を有する。

③クラウドサービス許可権限者は、申請されたクラウドサービスの審査について、情報セキュリティに関する権限及び責任を有する。

④クラウドサービス許可権限者は、申請されたクラウドサービスの審査結果について、情報セキュリティ統括責任者へ報告を行わなければならない。

2．情報資産の分類と管理

（1）　情報資産の分類

本市における情報資産は、重要性により、次のとおり分類する。

重要性による情報資産の分類

分類	分類基準
Ⅰ	個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報資産。
Ⅱ	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報資産。
Ⅲ	重要性分類Ⅰ又はⅡの情報資産以外の情報資産

（2）　情報資産の管理

①情報資産の管理責任

（ア）　情報セキュリティ実行責任者は、その所管する情報資産について管理責任を有する。

（イ）　情報セキュリティ実行責任者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（1）の分類に基づき管理しなければならない。

（ウ）　情報セキュリティ実行責任者は、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（1）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）の取扱いを定める。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。

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、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正な管理を行わなければならない。

③情報の作成

（ア）　職員等は、業務上必要のない情報を作成してはならない。

（イ） 情報を作成する者は、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り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、情報セキュリティ実行責任者に判断を仰がなければならない。

⑤情報資産の利用

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

（イ） 情報資産を利用する者は、情報資産の分類に応じ、適正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、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。

⑥情報資産の保管

（ア） 情報セキュリティ実行責任者は、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。

（イ） 情報セキュリティ実行責任者は、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） 情報セキュリティ実行責任者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

（エ） 情報セキュリティ実行責任者は、重要性分類Ⅱ以上の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により重要性分類Ⅱ以上の情報を送信する者は、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。

⑧情報資産の運搬

（ア） 車両等により重要性分類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。

（イ） 重要性分類Ⅱ以上の情報資産を運搬する者は、情報セキュリティ実行責任者に許可を

得なければならない。

⑨情報資産の提供・公表

（ア） 重要性分類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。

（イ） 重要性分類Ⅱ以上の情報資産を外部に提供する者は、情報セキュリティ実行責任者に許可を得なければならない。

（ウ） 情報セキュリティ実行責任者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄等

（ア） 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。

（イ） 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。

（ウ） 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ実行責任者の許可を得なければならない。

（エ） 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。

3．情報システム全体の強靭性の向上

（1） 個人番号利用事務系

①個人番号利用事務系と他の領域との分離

個人番号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。個人番号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、外部接続先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個人番号利用事務系との双方向通信でのデータの移送を可能とする。

②情報のアクセス及び持ち出しにおける対策

（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。

③個人番号利用事務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

個人番号利用事務系の端末・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、個人番号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。

④個人番号利用事務系と接続されるクラウドサービス上での情報資産の取扱い

個人番号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。その場合、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。

（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

②LGWAN 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、個人番号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。

（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。

②京都府及び京都府下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、関係省庁や京都府等と連携しながら、情報セキュリティ対策を推進しなければならない。

４．物理的セキュリティ

４．１．サーバ等の管理

（１） 機器の取付け

コンピュータシステム所管課長は、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） サーバの冗長化

①コンピュータシステム所管課長は、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コンピュータシステム所管課長は、サーバに障害が発生した場合に備え、システムの運用停止時間を最小限に止める対策を取らなければならない。

（３） 機器の電源

①コンピュータシステム所管課長は、情報保護管理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、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②コンピュータシステム所管課長は、情報保護管理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コンピュータシステム所管課長は、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。

②コンピュータシステム所管課長は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③コンピュータシステム所管課長は、ネットワーク接続口（ハブの通信ポート等）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。

④コンピュータシステム所管課長は、自ら又はコンピュータ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。

（５） 機器の定期保守及び修理

①コンピュータシステム所管課長は、重要性分類Ⅱ以上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コンピュータシステム所管課長は、電磁的記憶媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、コンピュータシステム所管課長は、事業者に故障を修理させるにあたり、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他、秘密保持体制の確認等を行わなければならない。

③コンピュータシステム所管課長は、定期保守及び修理の作業記録を保存しなければならない。

（6） 庁外への機器の設置

コンピュータシステム所管課長は、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。

（7） 機器の廃棄等

①コンピュータシステム所管課長は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

②機器の廃棄、リース返却等の際に情報を消去又は復元不可能な状態にする措置を行う者は、行った措置について、日時、担当者及び処理内容を記録し、一定期間保存しなければならない。

③機器を廃棄、リース返却等を行う者は、コンピュータシステム所管課長の許可を得なければならない。

④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。

4．2．管理区域(情報システム室等)の管理

（1） 管理区域の構造等

①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋(以下「情報システム室」という。)や電磁的記録媒体の保管庫をいう。

②コンピュータシステム所管課長は、管理区域を地階又は 1 階に設けてはならない。

③コンピュータシステム所管課長は、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、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④コンピュータシステム所管課長は、情報システム室内の機器等に、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コンピュータシステム所管課長は、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全て塞がなければならない。

⑥コンピュータシステム所管課長は、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。

（2） 管理区域の入退室管理等

①コンピュータシステム所管課長は、管理区域への入退室を許可された者のみに制限し、可能な限り高次元の認証等監視機能、施錠、警報装置、入退室管理簿等により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､名札の着用及び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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、重要性分類Ⅱ以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、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コンピュータシステム所管課長は、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確認を行わせなければならない。

②コンピュータシステム所管課長は、情報システム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。

4．3．通信回線及び通信回線装置の管理

①情報保護管理者は、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情報保護管理者は、 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情報保護管理者は、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情報保護管理者は、重要性分類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。

⑤情報保護管理者は、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実施しなければならない。

⑥情報保護管理者は、重要性分類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。

4．4．職員等の利用する端末や電磁的記録媒体等の管理

①コンピュータシステム所管課長は、盗難防止のため、執務室等で利用するパソコン、モバイ

ル端末及び電磁的記録媒体のワイヤーによる固定、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コンピュータシステム所管課長は、情報システムへのログインに際し、パスワード、IC カード、或いは生体認証等の認証情報の入力を必要とするように設定しなければならない。

③コンピュータシステム所管課長は、情報資産を保存する場合は、サーバに保存する等、執務室等のパソコン、モバイル端末に保存しない等の措置を講じなければならない。また、情報システムの機能によりパソコン、モバイル端末に前記の情報資産を保存する必要がある場合は、ディスクデータの暗号化と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コンピュータシステム所管課長は、個人番号利用事務系では「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。

⑤コンピュータシステム所管課長は、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取り扱う情報の重要度に応じて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コンピュータシステム所管課長は、市が管理する施設以外の場所にパソコン及びモバイル端末を持ち出す場合は、管理簿等により管理しなければならない。

⑦コンピュータシステム所管課長は、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、遠隔消去機能を利用する等の措置を講じなければならない。

５．人的セキュリティ

５．１．職員等の遵守事項

（１） 職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び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実行責任者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報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パソコン等の端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア） CISO は、重要性分類Ⅱ以上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、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、情報セキュリティ実行責任者の許可を得なければならない。

（ウ） 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ実行責任者の許可を得なければならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、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、情報保護管理者の定める実施手順に従い、情報セキュリティ実行責任者の許可を得て利用することができる。

（イ） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ実行責任者の許可を得た上で、次に挙げる安全管理措置を講じなければならない。

ⅰ支給以外のパソコン、モバイル端末に不正プログラム対策ソフトウェアが導入され、最新のパターンファイルが適用されていることを、情報セキュリティ実行責任者が確認する。

ⅱパスワード、IC カード、或いは生体認証等の認証情報による、端末ロック機能が備わっていることを、情報セキュリティ実行責任者が確認する。

（ウ） 職員等は、次の場合は、支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いてはならない。

ⅰ重要性分類Ⅱ以上の情報資産を取り扱うこと

ⅱ無許可で行政情報を記録、持ち出す行為を行うこと

（エ） 業務利用する必要がなくなった場合は、利用したパソコン、モバイル端末、及び電磁的記録媒体から、業務に関する情報を削除しなければならない。

⑤持ち出し及び持ち込みの記録

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

⑥パソコンやモバイル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保護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実行責任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、適正な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却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。

⑨クラウドサービス利用時等の遵守事項

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） 会計年度任用職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ実行責任者は、会計年度任用職員に対し、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

情報保護管理者は、会計年度任用職員に ID を交付する場合には、セキュリティ研修を受講させ、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

情報セキュリティ実行責任者は、会計年度任用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エジソンネット（本市における電子メール等グループウェアをいう。以下同じ。）等の使用が不要の場合、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

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

（４） 委託事業者に対する説明

情報セキュリティ実行責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、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。

５．２．研修・訓練

（１） 情報セキュリティに関する研修・訓練

①CISO 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。

②CISO 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。

（２） 研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、ＩＴ推進本部の承認を得なければならない。

②研修計画において、職員等は、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、情報保護管理者、情報セキュリティ統括責任者、情報セキュリティ実行責任者、コ

ンピュータシステム所管課長、システム管理者、コンピュータ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情報セキュリティ実行責任者は、所管する課等の研修の実施状況を記録し、情報保護管理者及び情報セキュリティ統括責任者に対して、報告しなければならない。

⑥情報保護管理者は、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、ＩＴ推進本部に対して、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。

（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

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

５．３．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実行責任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実行責任者は、速やかに情報保護管理者、コンピュータシステム所管課長及び庁内の CSIRT に報告しなければならない。

③情報セキュリティ実行責任者は、報告のあった情報セキュリティインシデントについて、CISO 及び情報セキュリティ統括責任者に報告しなければならない。

④情報セキュリティ統括責任者は、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。

（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、情報セキュリティ実行責任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実行責任者は、速やかに情報保護管理者及びコンピュータシステム所管課長に報告しなければならない。

③情報セキュリティ実行責任者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ統括責任者に報告しなければならない。

④情報保護管理者は、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。

（3） 情報セキュリティインシデント原因の究明・記録、再発防止等

①情報保護管理者は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

②情報保護管理者は、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。

③情報保護管理者は、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実行責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

④情報保護管理者は、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実行責任者と連携して、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。

⑤CISO は、情報保護管理者から、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。

5．4．ID 及びパスワード等の管理

（1） IC カード等の取扱い

①職員等は、自己の管理する IC カード等に関し、次の事項を遵守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、速やかにコンピュータシステム所管課長に通報し、指示に従わなければならない。

②コンピュータシステム所管課長は、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。

③コンピュータシステム所管課長は、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。

（3） パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）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、情報セキュリティ実行責任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）。

６．技術的セキュリティ

６．１．コンピュータ及びネットワークの管理

（１） 文書保存サーバの設定等

①コンピュータシステム所管課長は、職員等が使用できる文書保存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コンピュータシステム所管課長は、文書保存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。
③コンピュータシステム所管課長は、住民の個人情報、人事記録等のデータの情報漏えいを防止できる機能を有したフォルダを作成する等の措置を講じなければならない。

（２） バックアップの実施

①コンピュータシステム所管課長は、業務システムのデータベースや文書保存サーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
②コンピュータシステム所管課長は、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。

（３） 他団体との情報システムに関する情報等の交換

コンピュータシステム所管課長は、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、情報保護管理者及び情報セキュリティ統括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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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正に管理しなければならない。

③コンピュータシステム所管課長又はコンピュータ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、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

コンピュータシステム所管課長は、ネットワーク構成図、情報システム仕様書について、電磁的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。

（6） ログの取得等

①コンピュータシステム所管課長は、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、一定期間保存しなければならない。

②コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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。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、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コンピュータシステム所管課長は、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。

（7） 障害記録

コンピュータシステム所管課長は、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、一定期間保存しなければならない。

（8） ネットワークの接続制御(フィルタリング)、経路制御等(ルーティング)

①情報保護管理者は、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等を設定しなければならない。

②情報保護管理者は、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

コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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 及び情報保護管理者の許可を得なければならない。

②コンピュータシステム所管課長は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③コンピュータシステム所管課長は､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情報保護管理者及びコンピュータシステム所管課長は、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うえで接続しなければならない。

⑤コンピュータシステム所管課長は、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、情報保護管理者の判断に従い、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情報保護管理者は、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情報保護管理者は、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情報保護管理者は、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。

(12) IoT 機器を含む特定用途機器のセキュリティ管理

情報保護管理者は、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。

(13)　無線 LAN 及びネットワークの盗聴対策

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

(14)　電子メールのセキュリティ管理

①情報保護管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②情報保護管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

③情報保護管理者は、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情報保護管理者は、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なければならない。なお、上限を超えた場合は、職員等がエジソンネットのウェブメール機能で受信をし、メールボックス内の電子メールの総量が上限値未満になるまで、一時的にメールの送受信を停止しなければならない。

⑤情報保護管理者は、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情報保護管理者は、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、システム上措置を講じなければならない。

(15)　電子メール等の利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないように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、情報セキュリティ実行責任者に報告しなければならない。

⑤職員等は、ウェブで利用できる電子メール等を使用してはならない。

⑥職員等は、ネットワークストレージサービスを原則使用してはならない。ただし、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、情報保護管理者の定める実施手順に従い、情報保護管理者の許可を得て利用することができる。

(16)　電子署名・暗号化

①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完

全性を確保することが必要な場合には、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のための鍵を管理しなければならない。

③CISO 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。

(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、情報保護管理者及びコンピュータシステム所管課長の許可を得て、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、情報セキュリティ実行責任者は、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、情報保護管理者及びコンピュータシステム所管課長の許可を得なければならない。

(19) 業務外ネットワークへの接続の禁止

①職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するようコンピュータシステム所管課長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コンピュータシステム所管課長は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②情報保護管理者は、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、情報セキュリティ実行責任者に通知し適正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コンピュータシステム所管課長は、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、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22) ソーシャルメディアサービスの利用

①情報セキュリティ実行責任者は、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（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②重要性分類Ⅱ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重要性分類Ⅱ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。

6．2．アクセス制御

（1） アクセス制御等

①アクセス制御

コンピュータシステム所管課長は、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利用者 ID の取扱い

(ア) コンピュータシステム所管課長は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

(イ) 職員等は、ユーザーアカウント登録、エジソンネット利用、個人番号利用事務系のコンピュータシステムの利用について、関係する規程又は基準に従って手続を行うものとする。この場合において、当該手続には、コンピュータシステムの利用の前提として情報保護管理者が実施する「情報セキュリティ研修」を欠かさないこと。

(ウ) 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、情報保護管理者又はコンピュータシステム所管課長に通知しなければならない。

（エ） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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） コンピュータシステム所管課長の特権を代行する者は、情報保護管理者及びコンピュータシステム所管課長が指名し、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、速やかに情報保護管理者、情報セキュリティ統括責任者、情報セキュリティ実行責任者及びコンピュータシステム所管課長に通知しなければならない。

（エ） コンピュータシステム所管課長は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

（オ） コンピュータシステム所管課長は、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セキュリティ機能を強化しなければならない。

（カ） コンピュータシステム所管課長は、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） 職員等によるテレワーク等におけ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、情報保護管理者及び当該情報システムを管理するコンピュータシステム所管課長の許可を得なければならない。

②情報保護管理者は、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情報保護管理者は、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情報保護管理者は、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情報保護管理者は、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、情報保護管理者の許可を得るか、もしくは情報保護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情報保護管理者は、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、利用者の ID、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

コンピュータシステム所管課長は、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

コンピュータシステム所管課長は、ログイン時におけ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情報保護管理者又はコンピュータシステム所管課長は、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情報保護管理者又はコンピュータシステム所管課長は、職員等に対してパスワードを発行する場合に仮のパスワードを発行した場合は、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情報保護管理者又はコンピュータシステム所管課長は、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

コンピュータシステム所管課長は、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。

6．3．システム開発、導入、保守等

（1） 情報システムの調達

①コンピュータシステム所管課長は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②コンピュータシステム所管課長は、機器及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し､情報セキュリティ上問題のないことを確認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

コンピュータシステム所管課長は、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。

②システム開発における責任者、作業者の ID の管理

（ア） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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。

（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） コンピュータシステム所管課長は、システム開発、保守及びテスト環境とシステム運用環境について、必要に応じて分離しなければならない。

（イ） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ） コンピュータシステム所管課長は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ） コンピュータシステム所管課長は、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） コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、テスト結果を一定期間保管しなければならない。

③コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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

コンピュータシステム所管課長は、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

（7） 開発・保守用のソフトウェアの更新等

コンピュータシステム所管課長は、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

コンピュータシステム所管課長は、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。

6．4．不正プログラム対策

（1） 情報保護管理者の措置事項

情報保護管理者は、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、必要に応じ職員等に対して注意喚起しなければならない。

④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。

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） コンピュータシステム所管課長の措置事項

コンピュータシステム所管課長は、不正プログラム対策に関し、次の事項を措置しなければならない。

①所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。また、当該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。

②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

③不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、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、情報保護管理者が許可した職員を除く職員等に当該権限を付与してはならない。

（3） 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守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情報保護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。

⑤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、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た上で、速やかに情報セキュリティ実行責任者に報告しなければならない。報告を受けた情報セキュリティ実行責任者は、速やかに情報保護管理者、コンピュータシステム所管課長及び庁内のCSIRTに報告しなければならない。

（4） 専門家の支援体制

情報保護管理者は、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、必要に応じて外部の専門家の支援を受けられるようにしておかなければならない。

6．5．不正アクセス対策

（1） 情報保護管理者の措置事項

情報保護管理者は、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番号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、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情報保護管理者は、庁内のCSIRT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。

⑤本市が定めたクラウドサービスの利用に関するポリシー（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。

⑥クラウドサービスを利用する際に、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。

⑦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、本市が定めたクラウドサービスの利用に関するポリシー（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。

（2） 攻撃への対処

CISO及び情報保護管理者は、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、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、京都府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及び情報保護管理者は、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

コンピュータシステム所管課長は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5） 職員等による不正アクセス

コンピュータシステム所管課長は、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室等の情報セキュリティ実行責任者に通知し、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

コンピュータシステム所管課長は、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

コンピュータシステム所管課長は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6．6．セキュリティ情報の収集

（1） セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

①コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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。

（2） 不正プログラム等のセキュリティ情報の収集・周知

情報保護管理者は、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。

（3） 情報セキュリティに関する情報の収集及び共有

コンピュータシステム所管課長は、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。

7．運用

7．1．情報システムの監視

①コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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。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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、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コンピュータシステム所管課長は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑥コンピュータシステム所管課長は、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

7．2．情報セキュリティポリシーの遵守状況の確認

（1） 遵守状況の確認及び対処

①情報セキュリティ統括責任者及び情報セキュリティ実行責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにCISO及び情報保護管理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、適正かつ速やかに対処しなければならない。

③コンピュータシステム所管課長は、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録媒体等の利用状況調査

①CISO 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。

②CISO は、指名された者が前項の調査を適切に実施するために、作業記録等の必要な措置を講じさせなければならない。

（3） 職員等の報告義務

①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報保護管理者及び情報セキュリティ実行責任者に報告を行わなければならない。

②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報保護管理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正に対処しなければならない。

7．3．侵害時の対応等

（1） 緊急時対応計画の策定

①CISO 又はＩＴ推進本部は、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。

②CISO 又はＩＴ推進本部は、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。

（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） 業務継続計画と整合性確保

①本市が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、ＩＴ推進本部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。

②職員等は、業務継続計画の実施時、当該計画と情報セキュリティポリシーの整合性を確保できない場合は、情報保護管理者に判断を仰がなければならない。

（4） 緊急時対応計画の見直し

CISO 又はＩＴ推進本部は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

7．4．例外措置

（1） 例外措置の許可

情報セキュリティ実行責任者は、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、例外措置を講じることができる。

（2） 緊急時の例外措置

情報セキュリティ実行責任者は、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正に保管し、定期的に申請状況を確認しなければならない。

7．5．法令順守

①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等及び規定等を遵守し、これに従わなければならない。

（ア） 地方公務員法(昭和 25 年法律第 261 号)

（イ） 著作権法（昭和 45 年法律第 48 号）

（ウ） 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）

（エ） 個人情報の保護に関する法律（平成 15 年法律第 57 号）

（オ） 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)

（カ） サイバーセキュリティ基本法（平成 26 年法律第 104 号）

（キ） 八幡市個人情報の保護に関する法律施行条例（令和 5 年条例第 2 号）

（ク） 地方自治法（昭和 22 年法律第 67 号）

（ケ） 地方税法（昭和 25 年法律第 226 号）

（コ） 住民基本台帳法（昭和 42 年法律第 81 号）

（サ） 八幡市コンピュータシステムの管理、運用及び情報保護に関する規則（平成 15 年八幡市規則第 5 号）

（シ） 八幡市エジソンネットの管理及び運用に関する規程（平成 15 年八幡市規程第 1 号）

（ス） 八幡市電算処理の管理､運営及び情報保護に関する規程(平成 13 年八幡市規程第 7 号)

（セ） 八幡市特定個人情報の取扱いに関する規程（平成 27 年八幡市規程第 4 号）

②コンピュータシステム所管課長は、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。

７．６．情報セキュリティポリシー違反に対する対応

（1） 指導等

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、情報セキュリティ統括責任者又は情報セキュリティ実行責任者を通じた指導の対象となる。

（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情報保護管理者が違反を確認した場合は、情報保護管理者は当該職員等が所属する情報セキュリティ実行責任者に通知し、適正な措置を求めなければならない。

②コンピュータシステム所管課長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情報保護管理者及び当該職員等が所属する情報セキュリティ実行責任者に通知し、適正な措置を求めなければならない。

③情報セキュリティ統括責任者又は情報セキュリティ実行責任者の指導によっても改善されない場合、情報保護管理者は、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、情報保護管理者は、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情報セキュリティ実行責任者に通知しなければならない。

８．業務委託と外部サービス（クラウドサービス）の利用

８．１．業務委託

（1） 委託事業者の選定基準

①情報セキュリティ実行責任者は、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情報セキュリティ実行責任者は、委託内容の重要度に応じて、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委託事業者を選定しなければならない。

（2） 契約項目

重要な情報資産を取り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。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（3） 確認・措置等

情報セキュリティ実行責任者は、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を実施しなければならない。また、その内容を情報保護管理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。

8．2．外部サービス（クラウドサービス）の利用（重要性分類Ⅱ以上の情報を取り扱う場合）

（1） クラウドサービスの利用に係る規定の整備

情報保護管理者は、以下を含むクラウドサービス(重要性分類Ⅱ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クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 8.2 節において「クラウドサービス利用判断基準」という。）
②クラウドサービス提供者の選定基準
③クラウドサービスの利用申請のクラウドサービス許可権限者と利用手続
④クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

卐

（2） クラウドサービスの選定

①情報セキュリティ統括責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従ってクラウドサービスの利用を検討すること。
②情報セキュリティ統括責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏

まえ､クラウドサービス提供者の選定基準に従ってクラウド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クラウドサービス提供者の選定条件に含めること。

③情報セキュリティ統括責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用するクラウドサービスが、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。

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

（イ） クラウド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） クラウドサービスの提供に当たり、クラウド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） クラウドサービス提供者の資本関係・役員等の情報、クラウド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並びに調達仕様書による施設の場所やリージョンの指定

（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

④情報セキュリティ統括責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めること。

⑤情報セキュリティ統括責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

⑥情報セキュリティ統括責任者は、クラウド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クラウドサービス提供者の選定条件に含めること。

（注） クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断すること。

（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

⑦情報セキュリティ統括責任者は、クラウドサービスの利用を通じて本市が取り扱う情報に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クラウドサービス供者を選定し、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。

⑧情報セキュリティ統括責任者は、クラウド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、クラウドサービス提供者の選定条件で求める内容をクラウド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、クラウドサービス提供者の選定条件に含めること。また、クラウドサービス利用判断基準及びクラウド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。

⑨情報セキュリティ統括責任者は、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、クラウドサービスを選定すること。また、クラウド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。

⑩情報セキュリティ統括責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス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。

⑪情報保護管理者は、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、クラウド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） クラウドサービスの利用に係る調達・契約

①情報セキュリティ統括責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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情報セキュリティ統括責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウド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） クラウドサービスの利用承認

①情報セキュリティ統括責任者は、クラウドサービスを利用する場合には、利用申請のクラウドサービス許可権限者へクラウドサービスの利用申請を行うこと。

②利用申請のクラウドサービス許可権限者は、職員等によるクラウド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利用申請のクラウドサービス許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名すること。（クラウドサービスを利用する場合も同様の措置を行う。）

（5） クラウド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情報保護管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウド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

（オ） クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

②クラウドサービス管理者は、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。

③クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

（6） クラウド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情報保護管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウド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） クラウドサービス利用方針の規定

（イ） クラウド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） クラウドサービス内の通信の制御

（キ） 設計・設定時の誤りの防止

（ク） クラウドサービスを利用した情報システムの事業継続

（ケ） 設計・設定変更時の情報や変更履歴の管理

②情報セキュリティ実行責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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クラウドサービス管理者は、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。

④クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

（7） クラウド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情報保護管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウド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） クラウドサービスの利用終了時における対策

（イ） クラウドサービスで取り扱った情報の廃棄

（ウ） クラウドサービスの利用のために作成したアカウントの廃棄

②クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録すること。

③クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存

する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

8．3．外部サービス（クラウドサービス）の利用（重要性分類Ⅱ以上の情報を取り扱わない場合）

（1） クラウドサービスの利用に係る規定の整備

情報保護管理者は、以下を含むクラウドサービス（重要性分類Ⅱ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） クラウドサービスを利用可能な業務の範囲

（イ） クラウドサービスの利用申請のクラウドサービス許可権限者と利用手続

（ウ） クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

（エ） クラウドサービスの利用の運用手順

（2） クラウドサービスの利用における対策の実施

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重要性分類Ⅱ以上の情報を取り扱わない場合のクラウド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クラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講ずること。

②情報セキュリティ実行責任者は、職員等によるクラウド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、承認したクラウドサービスを記録すること。

9．評価・見直し

9．1．監査

（1） 実施方法

CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は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

①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。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（3） 監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、CISOに報告し、承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（4） 委託事業者に対する監査

①事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者含む。）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。

②クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

（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、CISO 及びＩＴ推進本部に報告する。

（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正に保管しなければならない。

（7） 監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管するコンピュータシステム所管課長及び情報セキュリティ実行責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していないコンピュータシステム所管課長及び情報セキュリティ実行責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、情報保護管理者に対し、当該事項への対処を指示しなければならない。

（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

ＩＴ推進本部は、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。

9．2．自己点検

（1） 実施方法

①コンピュータシステム所管課長は、所管するネットワーク及び情報システムについて、定期的に又は必要に応じ自己点検を実施しなければならない。

②情報セキュリティ統括責任者は、情報セキュリティ実行責任者と連携して、所管する部局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、必要に応じ自己点検を行わなければならない。

（2） 報告

コンピュータシステム所管課長及び情報セキュリティ統括責任者は、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、ＩＴ推進本部に報告しなければならない。

（3） 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②ＩＴ推進本部は、この点検結果を情報セキュリティポリシー及び関連規定等の見直し、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。

9．3．情報セキュリティポリシー及び関係規程等の見直し

①ＩＴ推進本部は、情報セキュリティポリシー及び関係規定等について、情報セキュリティ監査及び自己点検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、定期的に及び重大な変化が発生した場合に評価を行い、必要であると認めた場合、改善を行うものとする。

②ＩＴ推進本部は、個人情報保護に関する重要事項を見直す場合、必要に応じ、八幡市情報公開・個人情報保護審議会の意見を求めることができる。

【付録】用語解説

索引	用語	解説	備考
ア	アクセス権(限)	コンピュータシステム上で、プログラムの実行や、データの参照、追加、変更、削除などをできる資格のこと。企業や組織などでは、データの内容に応じて、利用者やグループごとに異なるアクセス権限を設定できる。たとえば、機密情報を含むファイルについては、アクセス権限を必要な利用者のみに適切に設定すれば、安全性を高めることができる。	※1
	アカウント	コンピュータやソフトウェア、ネットワークなどを使用するための権利や資格のこと。また、それらのシステムにログインするために必要な ID とパスワードの組み合わせをアカウントと呼ぶこともある。	※1
	アクセス制御	大事な情報を他人には知られないようにするため、データを見てもその内容がわからないように、定められた処理手順でデータを変えてしまうこと。暗号化されたデータは、復号という処理によって元のデータに戻すことができる。	
	暗号化	大事な情報を他人には知られないようにするため、データを見てもその内容がわからないように、定められた処理手順でデータを変えてしまうこと。暗号化されたデータは、復号という処理によって元のデータに戻すことができる。	※1
	ウイルス対策ソフト	コンピュータをウイルスから防御するためのソフトウェアのこと。「アンチウイルスソフト」とも呼ばれている。コンピュータに侵入したウイルスを駆除したり、電子メールなどで送信するファイルにウイルスが含まれていないかどうかをチェックしたりすることができる。他のコンピュータとの通信状況を監視してウイルスの侵入を予防するファイアウォールの機能を備えているものもある。	※1
	Web（ウェブ）会議サービス	専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。	
	SLA	サービス提供者と利用者との間でサービス内容に関し明示的になされた合意であり、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、サービス提供者に保証させることをいう。	
	遠隔消去機能	携帯電話などに記録してあるデータを、当該端末から操作す	

		るのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。	
	オペレーティングシステム	OS（Operating System の略）ともいう。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。 たとえば、メモリやディスクなどのハードウェアの制御、キーボードやマウスといったユーザインタフェースの処理、画面への表示とウィンドウの制御など、コンピュータが動作するための数多くの基本処理を行っている。さらに、コンピュータシステムを管理するための数多くのツールが用意されている。代表的な OS には Windows、Mac OS 等がある。	※1
カ	外部委託（情報システ ムの外部委託）	情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を庁外の者に請け負わせること。	
	外部からのアクセス	インターネット、電話回線等を通じて庁外のパソコン、ネットワークから庁内のネットワークに接続すること。	
	外部サービス	事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。	
	外部ネットワーク	インターネット等の庁外のネットワークのこと。	
	可用性	認可された利用者が、必要なときに情報にアクセスできることを確実にすること。国際標準化機構（ISO）が定める標準に定義されるもので、Availability（アベイラビリィティ）の訳語。	※1
	監査	（「情報セキュリティ監査」を参照）	
	監視（情報システムの監視）	情報システムへの攻撃等を防ぐため、情報システムの稼働状況を常に監視すること。	
	完全性	情報および処理方法の正確さおよび完全である状態を安全防護すること。国際標準化機構（ISO）が定める標準に定義されるもので、Integrity（インテグリティ）の訳語。	※1
	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（情報システム室）や電磁的記録媒体の保管庫のこと。	
	技術的セキュリティ	コンピュータの管理やアクセス制御等の技術的なセキュリティのこと。	
	機密性	情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。国際標準化機構（ISO）が定める標準に定義されるもので、Confidentiality（コンフィデ	※1

		ンシャリティ）の訳語。	
	業務継続計画	BCP(Business Continuity Plan（ビジネス コンティニュイティ プラン)）ともいう。自然災害等の問題発生シナリオに基づいて具体的な作業手順を定め、業務等が停止する時間を可能な限り少なくする目的で作られる管理策や計画のこと。	
	緊急時対応訓練	実際に情報の漏えい等の事故が発生した場合に即応できる態勢を構築しておくための緊急時を想定した訓練のこと。	
	緊急時対応計画	情報資産への侵害が発生した場合等に備えて、あらかじめ実施すべき具体的な措置を定めた計画のこと。	
	クラウドサービス	クラウドコンピューティングの形態で提供されるサービスのこと。従来は、利用者側がコンピュータのハードウェア、ソフトウェア、データなどを、自身で保有・管理し利用したが、クラウドサービスでは、利用者側が最低限の環境（パーソナルコンピュータや携帯情報端末などのクライアント、その上で動く Web ブラウザ、インターネット接続環境など）を用意することで、さまざまなサービスを利用できるようになる。クラウドサービスは、主に SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）の 3 つの形態で提供されている。	※1
	クラウドサービス管理者	クラウドサービスの利用における利用申請のクラウドサービス許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う者をいう。	
	クラウドサービス提供者	クラウドサービスを提供する事業者をいう。クラウドサービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。	
	経路制御(ルーティング)	ネットワーク上に送り出されたデータの宛て先の情報を調べて、それが正しい相手に送られるように、適切な通信経路を設定すること。	
	公衆無線 LAN	駅や街中など、公共の場所で利用できるように設定された無線 LAN の施設やサービスのこと。	※1
	個人情報保護法	個人の権利と履歴を保護するために、2005 年 4 月から施行された法律。個人情報保護法では、個人情報を所有する事業者に対する義務や対応を定めている。	
	（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、意図的に何らかの被害を及ぼすように作られたプログラムのこと。ディスクに保存されているファイルを破壊したり、個人情報などを盗むこともある。また感染経路として、ウイルスは、インターネッ	※1

		トからダウンロードしたファイルや、他人から借りた CD メディアや、USB メモリ、電子メールの添付ファイル、ホームページの閲覧など媒介して感染する。ウイルスにはウイルス対策ソフトでは検出・駆除できないものもあり、ウイルスに感染したことに気づかずにコンピュータを使用し続けるとウイルス自身が自分を複製する仕組みを持っていた場合には、他のコンピュータにウイルスを感染させてしまう危険性もある。	
	コンピュータシステム所管課長	所管する個々の情報システムの開発、設定の変更、運用、見直し等及び当該情報システムに対する情報セキュリティ対策に関する権限及び責任を負う者のこと。	
	コンピュータシステム担当者	コンピュータシステム所管課長の指示に従い、情報システムの開発、設定の変更、運用、見直し等の作業を行う者のこと。	
サ	サーバ証明書	SSL(TLS)を用いて、利用者がアクセスしているサーバが「本物」であることを保証する電子的な証明書のこと。例えば、インターネットバンキングや、ショッピングサイトなど、利用者がアクセスする Web サーバなどの真正性が重要となる場面で使用され、そのサーバと暗号化通信を行うためにも使用される。サーバ証明書は、認証局と呼ばれる第三者機関によって発行される。	※1
	サーバの冗長化	サーバに故障が発生しても、機器の二重化等により、業務を継続できるようにすること。	
	サービス不能攻撃	DoS（Denial of Service）攻撃や DDoS（Distributed Denial of Service）とも呼ばれ、対象の Web サイトへトラフィックを大量に送り負荷をかけてサービスが提供できない状態にする攻撃のこと。	
	時刻同期	サーバ間で時刻設定を自動的に合わせること。	
	自己点検	情報セキュリティポリシーの履行状況等について情報システム等を運用する職員等が自ら点検、評価すること。	
	システム管理記録	情報システムの状況を正確に把握するため、情報システムに対して行った作業を記録しておくこと。	
	システム管理者	行政情報ネットワーク、個別ネットワークの管理運用、情報セキュリティに関する統一的な対策に関する権限と責任を有する者のこと。	
	システム関連文書	システム設計書やプログラム仕様書等保有する情報システムに関わる文書のこと。	
	実施手順	（「情報セキュリティ実施手順」を参照）	
	自治体情報セキュリ	自治体における不正通信の監視機能の強化等への取組に際	

	ティクラウド	し、より高い水準のセキュリティ対策を講じるために、インターネット接続系において、都道府県と市区町村が協力して接続口の集約化をし、高度なセキュリティ対策を講じる仕組み。	
	守秘義務契約	外部委託先等に対し、業務上知りえた情報を漏らさないことを義務づける契約のこと。	
	障害記録	システム障害の内容や発生期日等を記録したもの。システム障害への対応時に過去に起きた類似障害を参考とするため、適切に保存すること。	
	最高情報セキュリティ責任者（CISO）	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や情報セキュリティに関する権限及び責任を有する者のこと。行政情報化担当の副市長。CISO は Chief Information Security Officer （チーフ・インフォメーション・セキュリティ・オフィサー）の略。	
	情報資産	企業や組織などで保有している情報全般のこと。顧客情報や販売情報などの情報自体に加えて、ファイルやデータベースといったデータ、CD-ROM や USB メモリなどのメディア、そして紙の資料も情報資産に含まれる。	※1
	情報資産の分類	重要性に基づき情報資産の分類を行うこと。	
	情報システム	コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行うシステムのこと。	
	情報システム仕様書	情報システムの仕様（スペック）を記載した文書のこと。	
	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。	
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。	
	情報セキュリティ監査	ネットワーク、情報システム等における情報セキュリティ対策の実施状況について、客観的に専門的見地から評価し、関係者に改善事項等の助言、勧告を行うこと。	
	情報セキュリティ基本方針	情報セキュリティ対策の目的、体系等、各地方公共団体の情報セキュリティに対する基本的な考え方を定めた文書のこと。	
	情報セキュリティ実行責任者	所管課及び施設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者のこと。課長及び施設長。	
	情報セキュリティ実施手順	情報セキュリティ対策基準に基づき、職員等関係者が、各々の扱うネットワーク及び情報システムや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について定めたマニュアルのこと。	
	情報セキュリティ対策	情報セキュリティを確保する対策のこと。	
	情報セキュリティ対策基準	情報セキュリティ基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策を規定する文書のこと。	
	情報セキュリティ統括責任者	担当部署等の情報セキュリティに関する統括的な権限及び責任を有する者のこと。部長等の庁議構成者	
	情報セキュリティに関する統一的な窓口（庁内の CSIRT）	CISO が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整備する、インシデントの状況を確認し、CISO へ報告する体制。CSIRT については、「CSIRT」を参照。	
	情報セキュリティポリシー	情報の機密性や完全性、可用性を維持していくために規定する組織の方針や行動指針をまとめたもの。	※1
	情報保護管理者	情報管理統括監を補佐する。本市の全てのネットワークにおける開発、設定変更、運用、見直し等や情報セキュリティ等に関する権限及び責任を有する者のこと。行政情報化担当課長。	
	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こと。	
	スパムメール	迷惑メールのこと。利用者が送信を要求していないのにも関わらず、勝手に送りつけてくる商品広告などの電子メールのこと。電子メールを受信する通信料を利用者側が負担しなければならないということもあり、大きな社会問題になっている。	※1
	生体認証	ひとりひとりが異なる人間の身体的特徴を利用する認証技術全般のこと。指紋や声紋、虹彩（眼球の模様）を登録しておくことで、本人以外の人間がコンピュータやシステムを利用したり、施錠された空間に入ったりすることができないようにするために利用される。	※1
	セキュリティホール	OS やソフトウェアにおいて、情報セキュリティ上の欠陥となる不具合のこと。脆弱性とも呼ばれる。	※1
	接続制御（フィルタリング）	一般的な意味では「ろ過」することであるが、コンピュータや Web などインターネットの世界では「情報ろ過」を指す。情報ろ過としては、未成年者に対する成人サイトや有害情報サイトなどからの保護などが代表的な例である。その他に、コンピュータウイルスや不正アクセスからの保護を主な目的とするファイアウォールも、フィルタリングの一種と言え	※1

		る。こうしたそれぞれの目的によって、Web サイトの内容に応じて閲覧の制御を行うコンテンツフィルタリングや、ネットワークを行き交うパケットをポリシーに応じて制御するパケットフィルタリングなどの手法がある。	
	総合行政ネットワーク	地方公共団体間を相互に接続する行政専用ネットワークのことで、LGWAN（エルジーワン）と呼ばれる。LGWAN は Local Government Wide Area Network の略。	
	ソースコード	プログラミング言語を用いて記述したプログラムのこと。	
	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。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持った Web サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。	
タ	対策基準	（「情報セキュリティ対策基準」を参照）	
	多要素認証	システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。	
	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（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、本市が調達又は開発するものをいう。	
	庁内ネットワーク	本市の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを委託しているデータセンターに設置している情報システムをいう。	
	通信回線	情報を伝送する回線・ネットワークのこと。	
	通信回線装置	通信回線に接続して、通信を行うための装置。ルータ等。	
	電子署名	電子署名は、一般に暗号技術の一つである公開鍵暗号方式を利用して作成される。電子署名は、メッセージの作成者が自分の鍵ペアのうちの秘密鍵（プライベート鍵とも呼ばれる）を使って作成する。メッセージを受信した人は、作成者の鍵ペアのうちの公開鍵（パブリック鍵）を使用して、受信した	※1

		メッセージを検証する。つまり、作成者本人しか持ち得ない秘密鍵を使ってメッセージが作成されたことを検証することで、作成元の確認ができることになる。電子署名を利用することにより、なりすましやメッセージの改ざんが行われていないことの検証と、否認防止が可能になる。	
	電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体のこと。	
	特権	情報システムにおいて一般の利用者が利用できない機能を利用することが認められた権限のこと。管理者権限等。	
ナ	ネットワーク	複数のコンピュータを接続して、データを共有化したり、他のコンピュータの機能を利用したり、共有のプリンタを使用したりできるようにする通信網のこと。もっとも小さな単位のネットワークは、家庭や会社において、何台かのコンピュータを接続したものであるが、それらのネットワークが世界的に接続されて、インターネットが構成されている。	※1
	ネットワークストレージサービス	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	ハードディスクパスワード	パソコンを紛失、盗難にあってもハードディスクのデータが閲覧、コピー等されないようにするため、ハードディスクに設定するパスワードのこと。	
	パケット	ネットワークを通して送信されるデータを分割する際に使われる単位のこと。たとえば、ファイルを他のコンピュータに送信する際には、ファイルのデータをいくつかのパケットに分割して、各パケットにヘッダ情報を付加する。ヘッダには、IP アドレスなどの相手のコンピュータを識別する情報、受信した相手がパケットに分割されたデータを組み立て直すためのそれぞれのパケットの順番情報と、データのエラー補正のための情報などが含まれている。送信データをパケットに分割することにより、データの送信途中にエラーが発生してデータの再送信が必要になっても、データ全体を再送信するのではなく、パケット単位で再送信を行うだけで済むため、データの転送効率を向上させることができる。	※1
	パスワード	本人であることを確認するために、ユーザ名とともに入力する文字列。銀行のキャッシュカードの暗証番号も、一種のパスワードである。	※1
	パソコン	端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないもの	

		をいい、端末の形態は問わない。	
	パターンファイル	ウイルス対策ソフトがウイルスを発見するための参考にするファイルのこと。コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録している。	
	バックアップ	データを磁気テープなどの別の記憶媒体に保存して、大事なデータの複製を作っておくこと。バックアップを取っておくことで、データが壊れてしまったときに、バックアップ時の状態に復元することができる。	※1
	パッチ	完成したプログラムに対して、脆弱性（ぜいじゃくせい）などをなくすために後から配布される修正プログラムのこと。メーカーのホームページなどで提供される。	※1
	標的型攻撃	特定の組織を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取しようとする攻撃のこと。この攻撃では、標的の組織がよくやり取りをする形式のメールを送りつけ、そこについている添付ファイルやリンクをクリックさせ実行させ、そこからマルウェア配布サイトに誘導するなどの手口がよく使われている。	※1
	ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。ファイアウォールには“防火壁”の意味がある。火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。また、ウイルス対策ソフトに機能が統合された、個人向けのパーソナルファイアウォールソフトもある。	※1
	複合機	コピー機能、プリンタ機能、イメージスキャナ、ファクシミリなどの機能がまとめられた事務機器のこと。	
	不正アクセス	利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。日本国内においても、インターネットに接続されたコンピュータに対する不正アクセスによる被害が急増したため、これらの行為を処罰する不正アクセス禁止法が施行された。	※1
	不正プログラム	コンピュータウイルス、スパイウエア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称。ウイルス、スパイウエアなど。	
	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こと。	

	ふるまい検知	従来の方法と異なり、正常なプログラムには見られない、ウイルス特有の動作をすることを手掛かりに、ウイルスを検知する方法。	
	プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順などの国際標準規則のこと。通信プロトコルとも呼ばれる。文化や言語が異なる国と国との外交様式の決めごとというのが元々の意味。コンピュータや通信機器も、メーカーや機種ごとに通信形式が異なると相互に通信が行えないため、ITU-Tなどの国際機関で標準が決められている。標準に準拠した形で開発されるため、コンピュータや通信機器は、メーカーが異なっても相互に通信を行うことができる。	※1
	ポート番号	インターネットで情報のやり取りを行うために、使用される番号のこと。ポート番号またはサービス番号とも呼ばれている。IP アドレスとともに指定される補助用のアドレスで、通常、プロトコルに応じてポートが割り当てられている。たとえば、FTP は TCP の 21 番ポート（制御用）と 20 番ポート（データ用）、HTTP は TCP の 80 番ポート、HTTPS は TCP の 443 番ポートを使用する。	※1
マ	無線 LAN	ケーブル線の代わりに電波を使った LAN のこと。ADSL や光回線などの敷設が困難な地域への接続手段として伝送距離が 2～10km で、最大伝送速度は最大 74.81Mbps、2.5GHz 帯や 3.5GHz 帯、5.8GHz 帯を使用する WiMAX という規格もある。最近では携帯電話などの通信帯域がひっ迫しないようにするオフロード対策のひとつとしても注目されている。	
	モバイル端末	端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。	
ヤ	約款によるクラウドサービス	民間事業者等の庁外の組織が約款に基づき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、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。	
	予備電源	何らかの要因で電力供給が途絶し、機器が緊急停止した場合には、情報システムの機能が損なわれるおそれがあるため、機器が適正に停止するまでの間、電力を供給するために設けた予備の電源のこと。	
ラ	ログ	コンピュータが保有するユーザの接続時刻や処理内容などを記録したファイル。通常は、ログを参照することで、コン	※1

		ピュータが正常に動作しているかどうかを管理することができる。たとえば、Web サーバの場合には、管理している Web サイトに訪問してきたユーザの情報が格納される。	
英	BIOS（バイオス）	Basic Input Output System の略。コンピュータの電源を入れたときに最初に起動するプログラムであり、キーボードやマウス、ハードディスクなどの外部とのインターフェースを制御するプログラムが含まれている。Windows や Mac OS などの OS は、基本的に BIOS を介してこれらの機器とやり取りをしている。	※1
	CSIRT（シーサート）	Computer Security Incident Response Team の略。コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称。	
	IC カード（アイシーカード）	キャッシュカードやクレジットカードのようなプラスチック製のカードに、IC チップを埋め込んだもの。IC チップには、さまざまな情報が書き込まれており、専用の IC カードリーダを使用することで、その内容を読み出すことができる。IC カードに書き込まれた値によって、ユーザ認証に利用したり、電子マネーの残高を管理したりすることができる。	※1
	ICT（アイシーティー）	Information and Communication Technology（インフォメーション・アンド・コミュニケーション・テクノロジー）の略。情報通信技術のこと。従来から使われていた IT(Information Technology:インフォメーション・テクノロジー）に替わって、通信ネットワークによって情報が流通することの重要性を意識して使用される言葉。	※1
	ID（アイディー）	identification（アイデンティフィケーション）の略。個人を識別・把握する情報の総称のこと。ユーザ名、ユーザ ID とも呼ばれる。	※1
	IP アドレス（アイピー アドレス）	コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。現在主に使用されているこれらの 4 つの数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電等で大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が検	※1

		討されている。なお、IPv6 では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている。	
	ＩＴ推進本部	本市の情報化を総合的・計画的に推進するため庁議メンバーで構成される組織。本部長は、市長がつとめる。	
	MAC アドレス(マックアドレス)	Media Access Control（メディア・アクセス・コントロール）アドレスの略。LAN カードの中で、イーサネットを使って通信を行うカードに割り振られた一意の番号のこと。インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、まったく同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。	※1
	USB メモリ(ユーエスビー メモリ)	コンピュータの USB 端子に接続して利用できる小さなメモリデバイスのこと。USB 端子に接続するだけで、外部ドライブとして簡単に読み書きができる。消しゴム程度のサイズであるため、手軽に利用できるという利点はあるが、その分だけ盗難や紛失の危険性が高く、情報セキュリティ上のリスクが高いという欠点がある。また、最近は USB メモリをターゲットにした USB 媒介ウイルスが発生している。USB 媒介ウイルスは、コンピュータに USB メモリを差し込んだだけでウイルスに感染してしまうものである。	※1

(※1)出典：総務省『国民のための情報セキュリティサイト』
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）
を加工して作成