相模原市情報セキュリティポリシー

令和５年５月３１日（改正）

相　　模　　原　　市

相模原市情報セキュリティポリシー

◇序章

はじめに
市が保有する情報の安全管理対策
相模原市情報セキュリティポリシーの体系

◇第１章

情報セキュリティ基本方針

（相模原市情報セキュリティ対策に関する規程）

◇第２章

情報セキュリティ対策基準

序章

はじめに

地方公共団体は、他者に代替することができない行政サービスを提供する役割を担っており、市民の個人情報や行政事務執行上の様々な機密情報等を保有し、その多くを情報システムで管理しています。

情報システムが障害等により停止することで、事務執行を停滞させ市民生活に大きな影響を与える可能性があります。また、昨今の標的型攻撃に代表されるサイバー攻撃や不正アクセス等により、個人情報を含む機密情報の漏えい等の事案が発生する危険性を秘めています。

このため、市民の財産やプライバシー等を守るため、また、行政の円滑な事務執行を安定的かつ継続的に確保するために、情報セキュリティ対策を講じることは地方公共団体において極めて重要な責務となっています。

このことを踏まえ、本市においては、情報セキュリティ対策における取組みの基本的な考え方を示す基本方針（相模原市情報セキュリティ対策に関する規程）及び具体的な行動や判断の統一的な基準（対策基準）を取りまとめた情報セキュリティポリシーを策定し、職員に遵守を義務付けております。

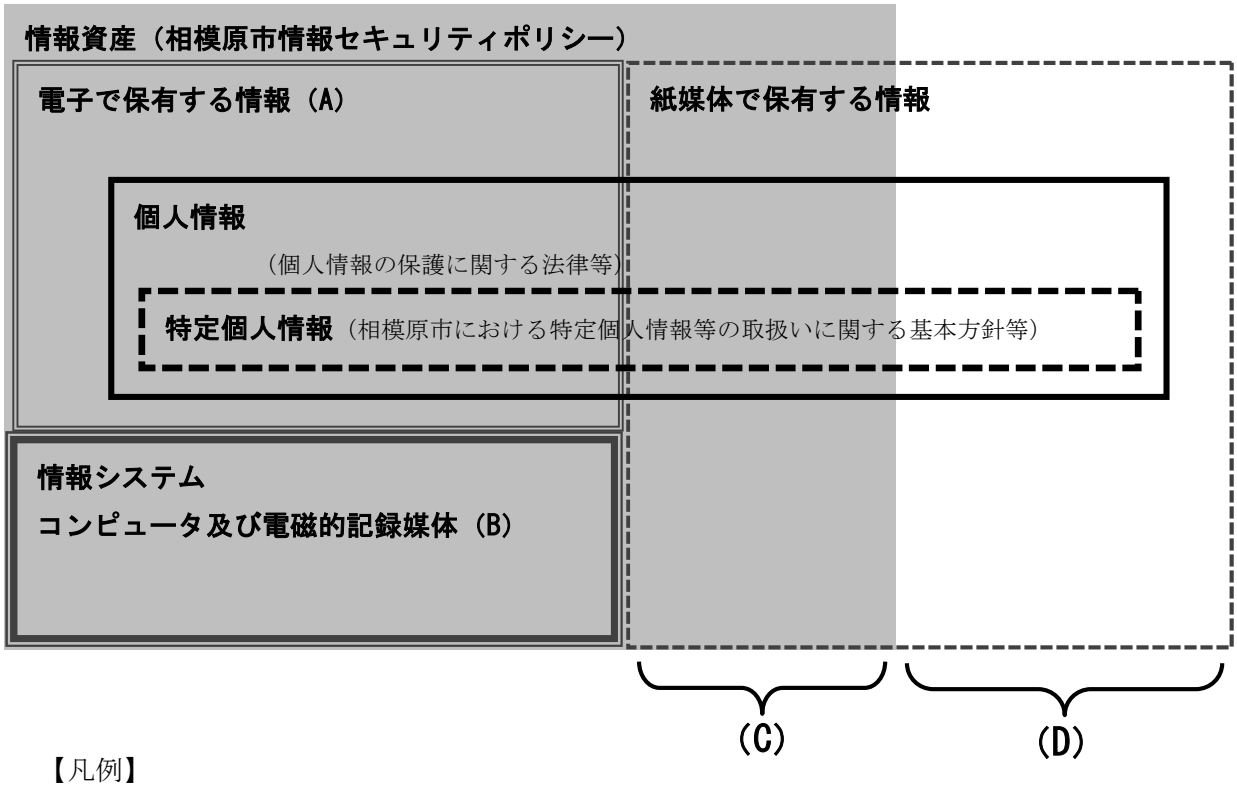
また、その内容は、情報通信技術や情報セキュリティに関する状況の変化等を踏まえ、継続的に見直しをしております。

今後につきましても、本市の情報セキュリティ水準を高め、市民の信頼の確保及び行政の円滑な事務執行に務めてまいります。

市が保有する情報の安全管理対策

市が保有する情報には、さまざまな種類があり、個人情報等機密性の高い情報が多く含まれています。それらの情報の安全管理対策として、次のとおり条例等を定めています。

【概念図】



【凡例】

情報資産

・情報システム（B）

・コンピュータ及び電磁的記録媒体
（それぞれ情報システムの構成要素となるものを除く。）（B）

・上記の機器等で取り扱う情報（これを印刷した文書を含む。）（A及びC）

・情報システムの仕様書、ネットワーク図等のシステム関連文書（A及びC）

紙媒体で保有する情報

・情報システム及びコンピュータ等で入出力した帳票等（C）

・情報システム及びコンピュータ等で入出力しない手書きの文書等（D）

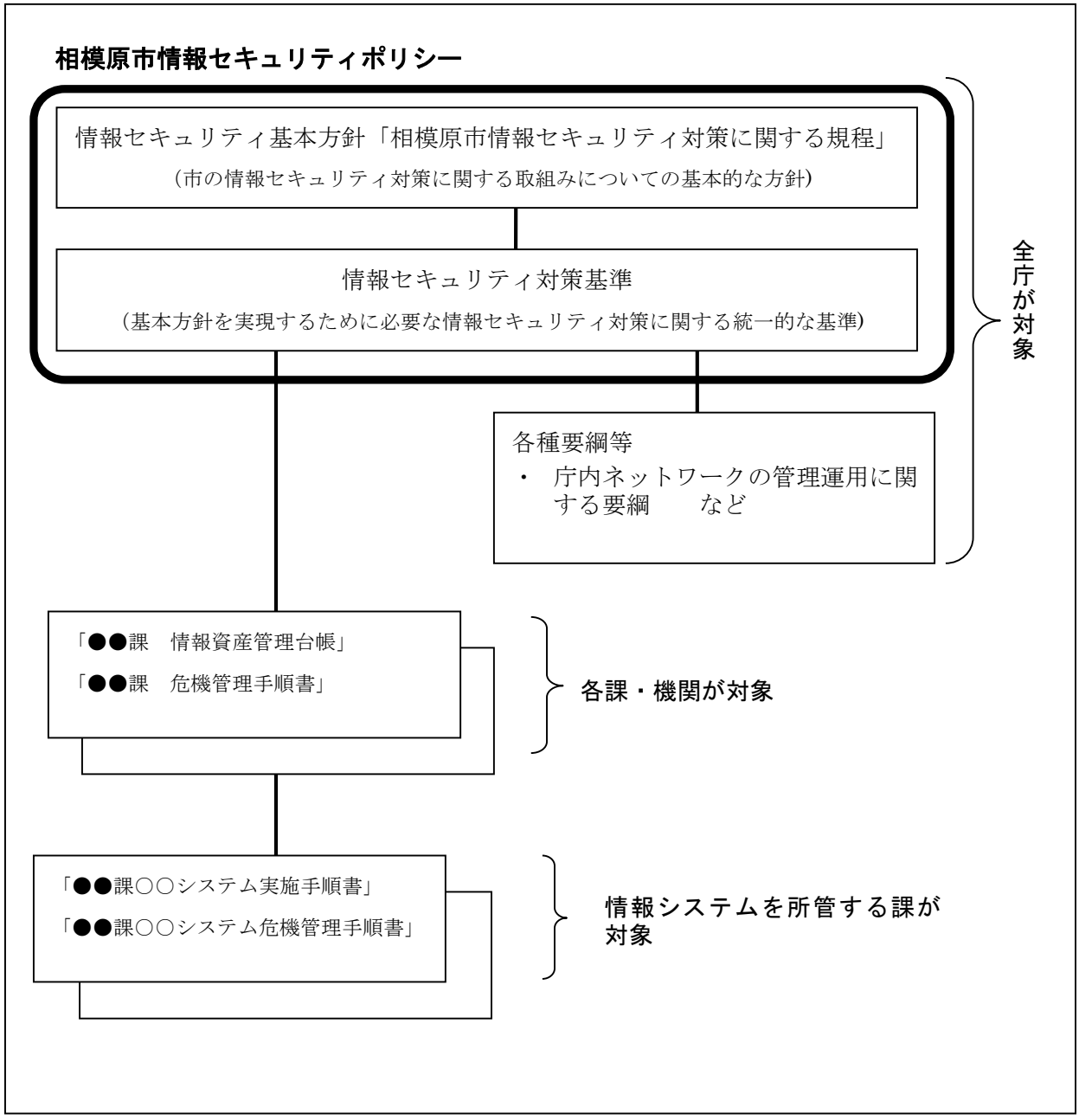
個人情報 …個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの

特定個人情報 …個人番号をその内容に含む個人情報

相模原市情報セキュリティポリシーの体系

情報セキュリティポリシーとは、「組織として一貫した情報セキュリティ対策を行うための方針と対策の基準を示したもの」です。すなわち、どのような情報資産を、どのような脅威及び脆弱性から、どのようにして守るのか、についての基本的な考え方や情報セキュリティを確保するための体制、組織及び運用を含めた規定をいいます。

本市では平成１５年４月から情報セキュリティポリシーを運用しています。この情報セキュリティポリシーは下図のとおりの構成としており、「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」を指して、相模原市情報セキュリティポリシーとして位置付けています。



第１章

相模原市情報セキュリティ対策に関する規程

（平成１５年３月３１日訓令第４号）

庁中一般
行政機関一般
出先機関一般

（趣旨）

第１条　この訓令は、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、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ものとする。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　ネットワーク　コンピュータを相互に接続するための通信網並びにその構成機器であるハードウェア及びソフトウェアをいう。

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

（３）　情報資産　次に掲げるものをいう。

ア　情報システム

イ　コンピュータ及び電磁的記録媒体（それぞれ情報システムの構成要素となるものを除く。）

ウ　ア及びイで取り扱う情報（これを印刷した文書を含む。）

エ　情報システムの仕様書、ネットワーク図等のシステム関連文書

（４）　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。

（５）　完全性　情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

（６）　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。

（７）　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。

（８）　情報セキュリティインシデント　情報セキュリティを脅かす、又は脅かすおそれのある事象をいう。

（９）　課　相模原市行政組織及び事務分掌規則（平成１９年相模原市規則第６６号）第４０条第１項の課等、相模原市区役所組織及び事務分掌規則（平成２２年相模原市規則第１９号）第７条第１項の課等並びに相模原市消防局組織等規則（平成１９年相模原市規則第６７号）第２条第１項に規定する課及び相模原市消防署組織等規程（昭和３９年相模原市消防本部告示第５号）第２条第１項に規定する課をいう。

（脅威及びリスク）

第３条　この訓令に基づく情報セキュリティ対策は、次に掲げる脅威及びリスクを想定して行われなければならない。

（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、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、改ざん又は消去、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定のミス、メンテナンスの不備、監査の機能の不備、業務委託管理の不備、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）　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

（職員の義務）

第４条　職員は、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、業務の遂行において、情報セキュリティに関する法令等を遵守しなければならない。

２　職員は、契約により市の事務事業の委託を受けた事業者、派遣労働者（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和６０年法律第８８号）第２６条第１項に規定する労働者派遣契約に基づき市に派遣され、市の事務事業に従事する者をいう。）その他市の事務事業に従事する者に対して、事業執行に当たりこの訓令を遵守するよう周知し、及び徹底しなければならない。

（組織体制）

第５条　統一的な情報セキュリティを確保するため、次に掲げる責任者、管理者、委員会及びチームを置く。

（１）　最高情報セキュリティ責任者

（２）　統括情報セキュリティ管理者

（３）　情報セキュリティインシデント対応チーム

（４）　情報セキュリティ管理者

（５）　情報システム管理者

（６）　情報セキュリティ評価委員会

（７）　情報セキュリティ向上委員会

（８）　情報セキュリティ監査チーム

２　最高情報セキュリティ責任者は、情報セキュリティに関する全ての活動を総括し、並びに緊急時における情報セキュリティ対策を指揮する責任及び権限を有し、市長公室長をもって充てる。

３　統括情報セキュリティ管理者は、情報セキュリティ対策の実行を統括する責任及び権限を有し、ＤＸ推進課長をもって充てる。

４　情報セキュリティインシデント対応チームは、外部からの意図的な脅威に起因する情報セキュリティインシデントが発生した場合における情報セキュリティインシデントの評価、被害拡大防止及び復旧に関する責任及び権限を有する。

５　情報セキュリティ管理者は、所管する課に係る情報セキュリティ対策（情報システム管

理者が行うものを除く。）の実行に関する責任及び権限を有し、課の長をもって充てる。

6　情報システム管理者は、所管する情報システムに係る情報セキュリティ対策の実行に関する責任及び権限を有し、当該情報システムを所管する課の長をもって充てる。

7　情報セキュリティ評価委員会は、情報セキュリティ対策の仕組みの確立及び維持に関する責任及び権限を有する。

8　情報セキュリティ向上委員会は、情報セキュリティ評価委員会から指示された事項に関する責任及び権限を有する。

9　情報セキュリティ監査チームは、情報セキュリティ監査の計画及び実施に関する責任及び権限を有する。

（情報セキュリティ対策）

第6条　情報セキュリティ管理者及び情報システム管理者は、次に掲げる情報セキュリティ対策を行うものとする。

（1）　情報資産の管理における対策として、情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を講ずること。

（2）　物理的セキュリティ対策として、サーバ、管理区域、通信回線、職員のパソコン等の管理について、必要な対策を講ずること。

（3）　人的セキュリティ対策として、情報セキュリティに関し、職員が遵守すべき事項の周知及び徹底を図るとともに、十分な教育及び啓発を行う等の必要な対策を講ずること。

（4）　技術的セキュリティ対策として、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必要な対策を講ずること。

（5）　情報セキュリティ対策の運用における対策として、情報システムの監視、情報セキュリティ対策の遵守状況の確認等の対策を講ずるとともに、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の危機管理対策を講ずること。

（6）　外部サービスの利用における対策として、ア及びイに掲げる場合に応じ、それぞれア及びイに定める対策を講ずること。

ア　業務委託する場合　情報セキュリティ対策のうち委託事業者が守るべき事項を明記した契約書に基づき、委託事業者において必要な情報セキュリティ対策が確保されていることを確認するとともに、必要に応じ、契約に基づく措置等を行うこと。

イ　約款による外部サービスを利用する場合　利用にかかる規定を整備し、必要な対策を行うこと。

2　統括情報セキュリティ管理者は、情報セキュリティ対策の実行に関して、情報セキュリティ管理者及び情報システム管理者への指導、助言及び許可を行うものとする。

（情報セキュリティ監査の実施等）

第7条　情報セキュリティ監査チームは、毎年度情報セキュリティ監査計画を作成し、情報セキュリティ評価委員会の承認を得るものとする。

2　情報セキュリティ監査チームは、情報セキュリティ対策が遵守されていることを検証するため、前項の監査計画又は情報セキュリティ評価委員会の指示に基づき情報セキュリティ監査を実施し、当該監査の結果を情報セキュリティ評価委員会へ報告するものとする。

（評価等）

第８条　情報セキュリティ評価委員会は、情報セキュリティ監査の結果及び情報セキュリティを取り巻く状況の変化等を踏まえ、情報セキュリティ対策が有効に機能しているかについて随時に評価を実施し、評価結果を最高情報セキュリティ責任者へ報告するものとする。

２　情報セキュリティ向上委員会は、情報セキュリティ評価委員会から指示された事項に関する調査及び分析を行い、当該調査及び分析の結果を情報セキュリティ評価委員会へ報告するものとする。

（情報セキュリティ対策基準の策定）

第９条　最高情報セキュリティ責任者は、この訓令に基づく情報セキュリティ対策を実施するための統一的な遵守事項、判断基準等を明らかにするため、情報セキュリティ対策基準を策定するものとする。

（委任）

第10条　この訓令に定めるもののほか、情報セキュリティ対策の実施に関し必要な事項は、別に定める。

(一部改正〔平成３１年訓令３号〕)

附　則

この訓令は、平成１５年４月１日から施行する。

附　則(平成１９年３月３０日訓令第１３号)

この訓令は、平成１９年４月１日から施行する。

附　則(平成２２年３月３１日訓令第１４号)

この訓令は、平成２２年４月１日から施行する。

附　則(平成２４年３月３０日訓令第３号)

この訓令は、平成２４年４月１日から施行する。

附　則(平成２４年９月２８日訓令第１０号)

この訓令は、平成２４年１０月１日から施行する。

附　則(平成２５年３月１４日訓令第２号)

この訓令は、平成２５年３月１５日から施行する。

附　則(平成２５年３月２９日訓令第１０号)

この訓令は、平成２５年４月１日から施行する。

附　則(平成２６年３月３１日訓令第６号)

この訓令は、平成２６年４月１日から施行する。

附　則(平成２７年１２月２８日訓令第１３号)

この訓令は、公表の日から施行する。

附　則(平成２９年３月３１日訓令第７号)

この訓令は、平成２９年４月１日から施行する。

附　則(平成３１年３月２９日訓令第３号抄)

この訓令は、平成３１年４月１日から施行する。

附　則(令和２年３月３１日訓令第６号)

この訓令は、令和２年４月１日から施行する。

附　則(令和３年３月３１日訓令第８号)

この訓令は、令和３年４月１日から施行する。

附　則（令和５年３月３１日訓令第２号）

（施行期日）
この訓令は、令和５年４月１日から施行する。

第２章

情報セキュリティ対策基準

本対策基準は、相模原市情報セキュリティ対策に関する規程（以下「情報セキュリティ基本方針」という。）第９条に基づき、本市の情報資産を保護するための統一的な遵守事項及び判断基準等を定めたものである。

第１節　情報セキュリティポリシーの遵守等

１　情報セキュリティポリシーの遵守

最高情報セキュリティ責任者は、次のいずれかの手段により情報セキュリティポリシーに対する職員の理解及び自覚を促進し、遵守させなければならない。

（１）ホームページへの掲載

（２）相模原市職員ポータルの掲示板への掲載

（３）情報セキュリティ管理者への紙媒体での送付

２　職員の義務

職員は、情報セキュリティポリシーを理解し、遵守しなければならない。

３　その他の特記事項

（１）議会局、教育委員会事務局、市選挙管理委員会事務局、区選挙管理委員会事務局、監査委員事務局、人事委員会事務局及び農業委員会事務局に属する職員についても、本対策基準の対象とする。（ただし、相模原市立小中学校等が保有する情報資産は除く）

（２）本対策基準に定めるもののほか、具体的な情報セキュリティ対策について必要な事項は、別に定める。

第２節　定義

１　本対策基準で使用する用語は、情報セキュリティ基本方針で使用する用語の例による。

２　本対策基準において、次に掲げる用語の意義は、次に定めるところによる。

（１）情報セキュリティポリシー　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をいう。

（２）課長　情報セキュリティ基本方針に規定する課の長をいう。

（３）外部機関等　市の行政組織以外の組織をいう。

（４）基幹系（マイナンバー利用事務系）　個人番号（社会保障、地方税若しくは防災に関する事務）を取り扱う情報システム、共通基盤システムと連携する情報システム及び個人や法人の特定に利用する番号を有する情報システムが存在する領域をいう。

（５）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が存在する領域をいう。

（６）情報系（LGWAN 接続系）　基幹系及びインターネット接続系に属さない、LGWAN に接続可能な情報システム（共通ファイルサーバ等）が存在する領域をいう。

（７）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。

（８）特定用途機器　ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

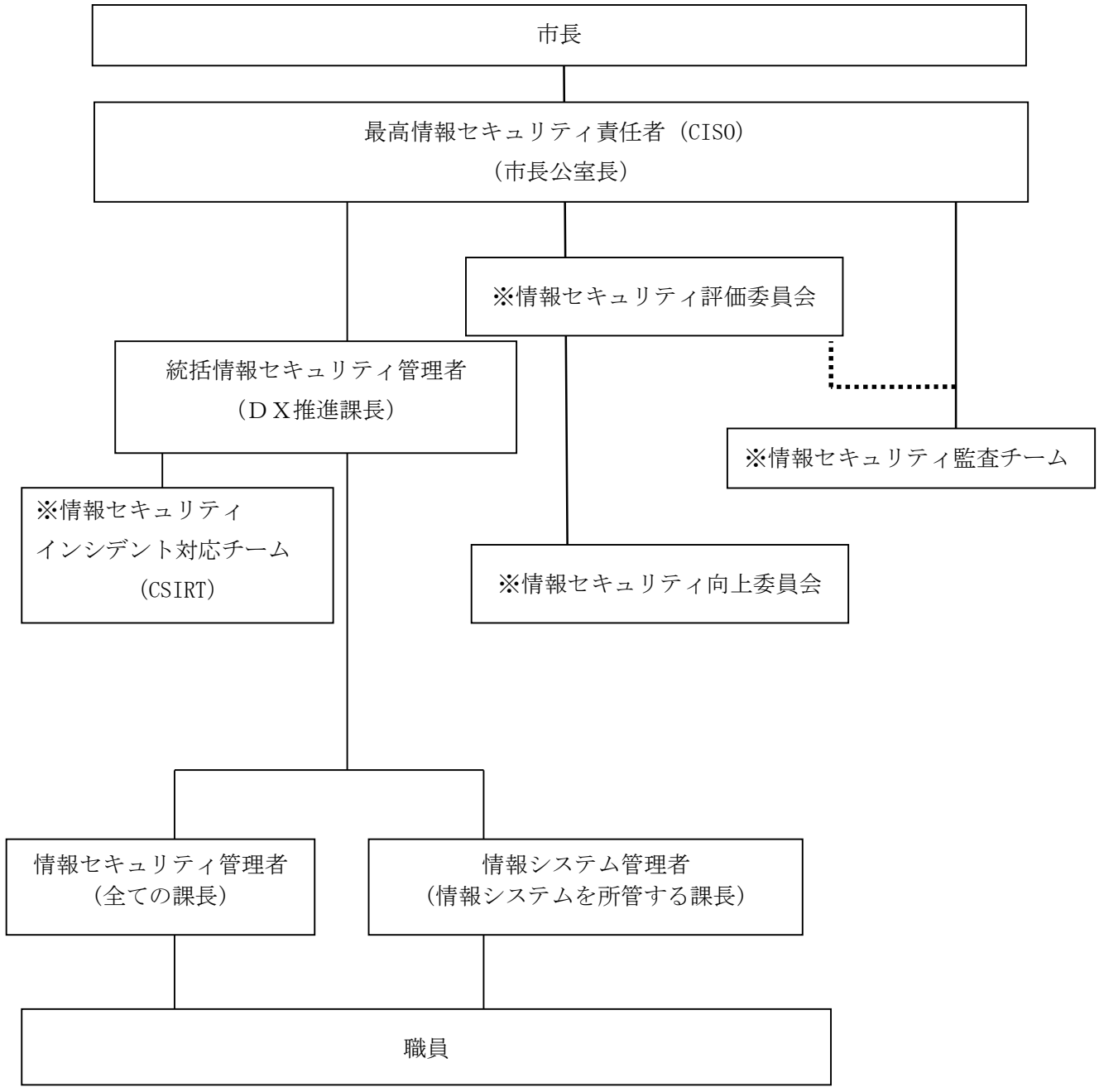
（９）クラウドサービス　事業者によって定義されたインタフェースを用いた、拡張性及び柔軟性を持つ、共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

（10）外部サービス　事業者等の庁外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。

第３節　組織体制

１　組織

次のとおり組織を整備する。



※詳細については、別途各運営要綱等に定める。

２　責任及び役割

（１）最高情報セキュリティ責任者(Chief　Information　Security　Officer,　以下「CISO（シー・アイ・エス・オー)」という。)

ア　市長公室長をCISOとする。

イ　CISOは次に掲げる責任及び権限を有する。

（ア）情報セキュリティポリシーに定められた全ての活動に関する総括

（イ）情報セキュリティ対策基準の制定及び改定

（ウ）職員に対する情報セキュリティポリシー遵守の徹底

（エ）緊急時における情報セキュリティ対策の指揮

（オ）情報セキュリティ評価委員会の設置

（カ）情報セキュリティ監査チームの設置

（キ）情報セキュリティインシデント対応チーム（Computer　Security　Incident　Response　Team,　以下「CSIRT（シーサート)」という。）の設置

（２）統括情報セキュリティ管理者

ア　ＤＸ推進課長を統括情報セキュリティ管理者とする。

イ　統括情報セキュリティ管理者は次に掲げる責任及び権限を有する。

（ア）CISOの指示に従い、情報セキュリティ対策の実行を統括する責任と権限

（イ）情報セキュリティ対策の実行に関する情報セキュリティ管理者及び情報システム管理者への指導、助言及び許可

（ウ）情報セキュリティに関する教育及び訓練の実施

（エ）情報セキュリティ関連情報の収集及び提供

（オ）CSIRTを指揮する責任と権限

（３）情報セキュリティ管理者

ア　全ての課長を情報セキュリティ管理者とする。

イ　情報セキュリティ管理者は次に掲げる責任及び権限を有する。

（ア）所管する課の情報セキュリティ対策に関する責任と権限

（イ）所管する情報資産の維持及び管理

（ウ）情報セキュリティ監査への協力及び指摘事項に関する是正

（４）情報システム管理者

ア　情報システムを所管する課長を情報システム管理者とする。

イ　情報システム管理者は次に掲げる責任及び権限を有する。

（ア）所管する情報システムの情報セキュリティ対策に関する責任と権限

（イ）所管する情報システムの運用、変更、見直しに関する責任と権限

（ウ）所管する情報システムの実施手順書の作成並びに実施手順の遵守及び管理

（エ）情報セキュリティ監査への協力及び指摘事項に関する是正

（５）情報セキュリティ評価委員会

情報セキュリティ評価委員会は次に掲げる責任及び権限を有する。

ア　情報セキュリティ対策の仕組みの確立及び維持

イ　情報セキュリティ対策の実施状況の評価

ウ　情報セキュリティ対策の実行に必要な教育訓練の計画

（６）情報セキュリティ向上委員会

情報セキュリティ向上委員会は、情報セキュリティ評価委員会から指示された事項に関する責任及び権限を有する。

（７）情報セキュリティ監査チーム

情報セキュリティ監査チームは次に掲げる責任及び権限を有する。

ア　情報セキュリティ監査の計画及び実施

イ　情報セキュリティ監査結果の情報セキュリティ評価委員会への報告

（８） CSIRT

CSIRT は次に掲げる責任及び権限を有する。

ア　情報セキュリティインシデントの把握、分析及び対応

イ　情報セキュリティインシデントに関する報告

ウ　情報セキュリティインシデントに関する外部との情報共有

（９）兼務の禁止

ア　情報セキュリティ対策の実施において、やむをえない場合を除き、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。

イ　監査を受けるものとその監査を実施する者は、やむをえない場合を除き、同じ者が兼務してはならない。

(10) 読み替え規定

情報システムに含まれない機器を所管している場合、「情報システム管理者」とあるのは「情報セキュリティ管理者」と読み替えるものとする。

第４節　情報資産の分類と管理

１　情報資産の分類

情報セキュリティ管理者及び情報システム管理者は、情報資産を機密性、完全性及び可用性により、次のとおり分類しなければならない。

（１）機密性による情報資産の分類

分類	分類基準
機密性３	行政事務で取り扱う情報資産のうち、個人情報（公知の情報は除く。）及び機密情報等、情報漏えいにより市民の権利が侵害される、又は業務の遂行に多大な影響を及ぼすおそれがある情報資産
機密性２	行政事務で取り扱う情報資産のうち、機密性３に相当する機密性は有しないが、直ちに一般に公表することを前提としていない重要な情報資産
機密性１	機密性２又は機密性３以外の情報資産

（２）完全性による情報資産の分類

分類	分類基準
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、市民の権利が侵害される、又は業務の遂行に多大な影響を及ぼすおそれがある情報資産
完全性１	完全性２以外の情報資産

（３）可用性による情報資産の分類

分類	分類基準
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、市民の権利が侵害される、又は業務の遂行に多大な影響を及ぼすおそれがある情報資産
可用性１	可用性２以外の情報資産

２　情報資産の管理

（１）管理責任

ア　情報セキュリティ管理者及び情報システム管理者は、その所管する情報資産について管理責任を有する。

イ　情報資産が複製及び伝送された場合、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。

（２）情報資産台帳の作成

ア　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について、電磁的記録媒体等の単位で情報資産管理台帳に登録しなければならない。

イ　職員は、情報を外部に持ち出す場合及び外部機関等に提供する場合、情報単位で分類し、分類結果に応じた対策を行わなければならない。

（３）情報の作成

ア　職員は、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、当該情報の分類を実施しなければならない。

ウ　情報を作成する者は、情報の作成途上についても、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、当該情報を消去しなければならない。

（４）情報資産の入手

情報資産を入手した者は、１の分類に基づき、当該情報の分類を実施しなければならない。

（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、１の分類に基づき、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。

エ　情報資産を利用する者は、機密性２以上の情報を必要以上に複製及び配布を行ってはならない。

オ　情報資産を利用する者は、機密性３の情報が記載されている紙媒体は、裏紙利用してはならない。

（６）情報資産の保管

ア　職員は、次のとおり、情報を電磁的記録媒体に保管することができる。なお、取り扱う情報の分類により必要な措置を講じなければならない。

（ア）情報の保管場所

保管場所	機密性２以上、完全性２又は可用性２のいずれかにあたる情報	その他の情報
サーバ（ＮＡＳを含む）	○	○
パソコン	× ※作業用（２～３営業日以内に完了するもの）を除く。	○
可搬記憶媒体（電磁的記録媒体のうち、持ち運びができる記録媒体）	○	○

（イ）機密性２以上、完全性２又は可用性２のいずれかにあたる情報を保管する場合の措置内容

保管場所	機密性２以上、完全性２又は可用性２のいずれかにあたる情報
サーバ	・アクセス制御を設定すること
可搬記憶媒体	・受け渡し用途（委託事業者等への情報提供等）と一定期間保管用途（共通ファイルサーバからの退避等）の媒体を使い分け、媒体に表記すること ・一定期間保管用途で使用する際は、必ずバックアップを行うこと

イ　職員は、保管する必要がなくなった情報について、その時点で速やかに情報を消去しなければならない。

ウ　情報セキュリティ管理者及び情報システム管理者は、情報を記録した電磁的記録媒体を長期保管する場合、書込禁止の措置を講じなければならない。

エ　情報セキュリティ管理者及び情報システム管理者は、機密性２以上、完全性２又は可用性２のいずれかにあたる情報を記録した電磁的記録媒体及び紙媒体を必ず施錠可能な場所に保管し、必要に応じて耐火、耐熱、耐水及び耐湿の対策を講じなければならない。

（７）情報の送信

電子メール等により外部機関等へ機密性２以上の情報を送信する者は、必要に応じ、送信する情報に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　車両等により機密性２以上の情報資産を外部へ運搬する者は、情報資産の不正利用を防止するため、次のいずれかの措置を講じなければならない。

（ア）当該情報資産を鍵付きのケース等に格納する。

（イ）当該情報資産に記録されている情報にパスワード等による暗号化を行う。

イ　機密性２以上の情報資産を外部へ運搬する者は、情報セキュリティ管理者又は情報セキュリティ管理者が認めた者に許可を得なければならない。

（９）情報資産の提供・公表

ア　機密性２以上の情報資産を外部機関等に提供する者は、情報資産の不正利用を防止するため、次のいずれかの措置を講じなければならない。

（ア）当該情報資産を鍵付きのケース等に格納する。

（イ）当該情報資産に記録されている情報にパスワード等による暗号化を行う。

イ　機密性２以上の情報資産を外部機関等に提供する者は、情報セキュリティ管理者又は情報セキュリティ管理者が認めた者に許可を得なければならない。

ウ　情報セキュリティ管理者は、市民に公開する情報について、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、当該機器に内蔵されている電磁的記録媒体を統括情報セキュリティ管理者が指定する場所で物理的に破壊し、又はデータ消去し、復元不可能な状態にする措置を講じなければならない。

イ　機密性２以上の情報が記載された紙媒体を廃棄する者は、シュレッダー又は溶解等適切な措置を講じなければならない。

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

エ　情報資産の廃棄やリース返却等を行う者は、日時、担当者及び処理内容を記録しなければならない。

第５節　情報システム全体の強靭性の向上

１　基幹系

（１）基幹系と他の領域との分離

基幹系は、他の領域と通信できないようにしなければならない。ただし、基幹系と他の領域との通信をする必要がある場合、通信経路の限定（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）レベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。

（２）情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

「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。

イ　情報の持ち出し不可設定

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

２ 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、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を監視するため、通信パケットの監視又はふるまい検知等の不正通信の監視機能を強化しなければならない。

（２）自治体セキュリティクラウドが標準要件に基づいた機能を有すること及び運用がなされていることについて、定期的に外部監査を受けなければならない。

３　情報系

情報系は、インターネット接続系と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、インターネット接続系からメールや添付ファイルを情報系に取り込む場合は、無害化通信等を図らなければならない。

第６節　物理的セキュリティ

１　庁内にサーバ等を設置する際の対策

（１）機器の取付け

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

（２）サーバの冗長化

情報システム管理者は、緊急停止した際に即時に復旧しなければならない情報システムについて、業務を継続できるようにするため、サーバを冗長化しなければならない。

（３）機器の電源

ア　情報システム管理者は、施設管理者と連携し、可用性２の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ＵＰＳ（無停電電源装置）等の予備電源を備え付けなければならない。

イ　情報システム管理者は、施設管理者と連携し、可用性２のサーバ等の機器について、落雷等による過電流に備え、当該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

ア　情報システム管理者は、施設管理者と連携し、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。

イ　情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理者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。

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

エ　情報システム管理者は、第三者が配線を変更、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

ア　情報システム管理者は、可用性２のサーバ等の機器について定期保守を実施しなければならない。

イ　情報システム管理者は、電磁的記録媒体を内蔵する機器を委託事業者に修理させる場合、当該電磁的記録媒体から内容を退避した状態で行わせなければならない。内容を退避できない場合、委託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ほか、秘密保持体制の確認等を行わなければならない。

（6）機器の廃棄等

ア　情報セキュリティ管理者及び情報システム管理者は、機器の廃棄、リース返却等をする場合、当該機器に内蔵されている電磁的記録媒体内の情報を復元困難な状態にする措置を講じなければならない。

イ　情報セキュリティ管理者及び情報システム管理者は、次の管理策により適切に措置を行うものとする。

分類	廃　棄　方　法
マイナンバー利用事務系に該当するもの	機器に内蔵されている電磁的記録媒体を廃棄する場合は、庁舎内で、当該機器から電磁的記録媒体を取り外し、物理的な破壊を行うこと。なお、破壊後の電磁的記録媒体及び機器本体は、統括情報セキュリティ管理者が一括して廃棄すること。
上記以外の機密性３、機密性２、機密性１	㈠職員が庁舎内で、物理的な破壊を行うこと。なお、破壊後の電磁的記録媒体は、統括情報セキュリティ管理者が一括して廃棄すること。 ㈡職員による立ち会いにより、庁舎内で委託業者に物理破壊を実施させることができる。なお、破壊後の電磁的記録媒体は、統括情報セキュリティ管理者が一括して廃棄すること。 ㈢職員が庁舎内で、統括情報セキュリティ管理者が指定したデータ抹消を行うこと。※データ抹消後、賃貸借業者に引き渡す場合には破壊証明書等を提出させるものとする。 ㈠～㈢いずれかを選択すること。

（7）管理区域の構造等

ア　管理区域とは、機密性２以上、完全性２又は可用性２のいずれかにあたる情報システムを設置する区域、当該機器等の管理及び運用を行うための区域並びに電磁的記録媒体の保管庫をいう。

イ　情報システム管理者は、施設管理者と連携して、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。

ウ　情報システム管理者は、管理区域内の機器等に、転倒及び落下防止等の耐震対策を講じるとともに、必要に応じて防火措置、防水措置等を講じなければならない。

エ　情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（8）管理区域の入退室管理等

ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証又は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。

イ　職員及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めに

より提示しなければならない。

ウ　情報システム管理者は、外部機関等からの訪問者が管理区域に入る場合、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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

エ　情報システム管理者は、機密性２以上の情報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、又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。

（９）機器等の搬入出

ア　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

イ　情報システム管理者は、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。

２　庁外にサーバ等を設置する際の対策

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

（２）情報システム管理者は、庁外にサーバ等の機器を設置する場合、別途定める「データセンター利用基準」を遵守しなければならない。

３　通信回線及び通信回線装置の管理

（１）情報システム管理者は、施設管理者と連携し、所管する通信回線及び通信回線装置を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）情報システム管理者は、外部機関等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）情報システム管理者は、機密性２以上の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。

（４）情報システム管理者は、ネットワークに使用する回線について、必要に応じ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。

（５）情報システム管理者は、可用性２の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　職員の利用する端末や電磁的記録媒体等の管理

（１）情報セキュリティ管理者は、所管する課に設置されているパソコン等の機器について、次の管理策により適切に管理を行うものとする。

ア　パソコン等の管理

管理対象名	管理策
ノート型パソコン 及びモバイル端末等	次の管理のうち、適切な措置を講ずること。 ・施錠可能な場所での保管 ・鍵付チェーンで保護し、机上での管理

イ　可搬記憶媒体の管理

管理対象名	管理策
外付けハードディスク、 ＵＳＢメモリ、 デジタルカメラ等	・課において台帳管理すること。 ・３か月に１回以上は現物を確認し、確認結果を記録すること。 ・施錠可能な場所に保管すること。 ・個人管理ではなく、課において一括管理すること。 ・ＵＳＢメモリは、紛失防止策として、キーホルダー等の目印をつけること。 ・メモリカードを装置から取外して保管する場合、紛失防止のためケース等に収納すること。

情報セキュリティ管理者は、可搬記憶媒体の紛失の可能性を軽減させるため、所管するＵＳＢメモリ等の本数削減に取り組まなければならない。

ウ　プリンタの管理

管理	管理策
設置場所	印刷物の内容が第三者から容易に見られない場所に設置すること。
利用手順	・印刷物の長時間放置をしないこと。 ・ミスプリントは、その内容を確認し、機密性の情報が印刷されているものは、再利用せず適切な廃棄（シュレッダー又は溶解など）を行うこと。

（２）情報システム管理者は、情報システムへのログインに際し、パスワード、IC カード、或いは生体認証等複数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）情報システム管理者は、基幹系では「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。

第７節　人的セキュリティ

１　職員の遵守事項

（１）　職員の遵守事項

ア　情報セキュリティポリシー等の遵守

職員は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ　業務以外の目的での使用の禁止

職員は、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。

ウ　パソコンやモバイル端末等の持ち出し及び庁外における情報処理作業の制限

（ア）職員は、本市のパソコン、モバイル端末及び可搬記憶媒体等を外部に持ち出す場合、情報セキュリティ管理者又は情報セキュリティ管理者が認めた者の許可を得なければならない。

（イ）情報セキュリティ管理者は、職員のパソコン、モバイル端末及び可搬記憶媒体等の持ち出し状況について、記録を作成し保管しなければならない。

（ウ）職員は、庁外で情報処理業務を行う場合、情報セキュリティ管理者の許可を得なければならない。

エ　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システム管理者の許可なく変更してはならない。

オ　机上の端末等の管理

職員は、机上のパソコン、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及び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、次の対策を講じなければならない。

（ア）離席時のパソコン及びモバイル端末のスクリーンロック

（イ）電磁的記録媒体及び文書等の容易に閲覧されない場所への保管

カ　退職時等の遵守事項

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

（２）私有の機器の取り扱い制限

ア　私有の機器の使用禁止

（ア）職員は、私有のパソコン、モバイル端末及び可搬記憶媒体等を使用し、機密性２以上の情報を取り扱ってはならない。

（イ）機密性１の情報を取り扱う場合については、情報セキュリティ管理者が業務にあたって必要と認めた場合に限り、私有の機器を使用することができる。

イ　私有の機器の接続禁止

（ア）職員は、私有のパソコン、モバイル端末及び可搬記憶媒体等を本市の機器及び庁内のネットワークに接続してはならない。

（イ）マウス、キーボード、ディスプレイ及びイヤホンについては、有線かつ記憶領域がないものに限り、情報セキュリティ管理者の許可を得て接続することができる。ただし、統括情報セキュリティ管理者が安全性を認めた場合は無線接続可能とする。なお、本来付属していた機器については、紛失がないよう適切に管理すること。

（3）情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員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）委託事業者等に対する説明

情報セキュリティ管理者は、委託事業者及び指定管理者等に業務を委託する場合、再委託先の事業者も含めて、情報セキュリティポリシー等のうち委託事業者及び指定管理者等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。

2　研修・訓練

（1）情報セキュリティに関する研修・訓練

ア　次の表に定める実施責任者は、分類に応じて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。

分類	受講対象者	教育の概要	実施責任者
新規採用職員研修	新規採用職員	情報セキュリティポリシーを理解し、確実に実行することを目的とした研修	統括情報セキュリティ管理者
情報セキュリティ啓発研修	職員	情報セキュリティの重要性及び対策の意義等、情報セキュリティの意識向上を目的とした研修	統括情報セキュリティ管理者
情報セキュリティ内部監査員養成研修	新規セキュリティ内部監査員	内部監査実施のために必要な知識を取得することを目的とした研修	情報セキュリティ監査チームリーダー（ＤＸ推進課長）
所属セキュリティ研修	全ての職員	各所属において、１年に１回以上実施する研修	情報セキュリティ管理者

イ　実施責任者は、効果的な研修を実施するために次の内容により教育の計画を立案し、実施する。

（ア）研修実施予定日

（イ）研修実施者

（ウ）受講対象者

（エ）実施内容及び使用するテキスト

（オ）研修の効果測定方法

（カ）上記以外で研修実施責任者が必要と判断した内容

（2）緊急時対応訓練

統括情報セキュリティ管理者は、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。また、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。

（3）研修・訓練への参加

全ての職員は、定められた研修・訓練に参加しなければならない。

3　情報セキュリティインシデントの報告

（1）情報セキュリティインシデントの報告

ア　職員は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び緊急度が高い場合はCSIRTに報告しなければならない。

イ　報告を受けた情報セキュリティ管理者は、情報セキュリティインシデントが情報システムに関連する場合、速やかに情報システム管理者に報告しなければならない。

ウ　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、重要度に応じて統括情報セキュリティ管理者に報告しなければならない。

エ　CSIRTは、報告を受けた情報セキュリティインシデントについて、統括情報セキュリティ管理者に報告しなければならない。

オ　統括情報セキュリティ管理者は、報告を受けた情報セキュリティインシデントについて、重要度に応じ、CISOに報告しなければならない。

（2）情報セキュリティインシデントの記録

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティインシデントの対応結果を記録し、保管しなければならない。

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

ア　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の可能性について報告を受けた場合、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うよう、CSIRTに指示しなければならない。

イ　CSIRTは、情報セキュリティインシデントであると評価した場合、統括情報セキュリティ管理者に速やかに報告しなければならない。

ウ　CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ管理者及び情報システム管理者に対し、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。

エ　CSIRTは、情報セキュリティインシデントの原因を究明し、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、統括情報セキュリティ管理者を通じてCISOに報告しなければならない。

オ　CISOは、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、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。

4　ID 及びパスワード等の管理

（1）IC カード等の取扱い

ア　職員は、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、職員間で共有してはならない。

（イ）認証完了後は、IC カード等をカードリーダ若しくはパソコン等の端末のスロット等から抜かなければならない。

（ウ）IC カード等を紛失した場合、速やかに情報システム管理者に通報し、指示に従わなければならない。

イ　情報システム管理者は、IC カード等の紛失の通報があり次第、当該 IC カード等を使用したアクセスを速やかに停止しなければならない。

ウ　情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、当該カードが使えないよう、処理を行わなければならない。

（2）ID の取扱い

職員は、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。

ア　自己が利用している ID は、他人に利用させてはならない。

イ　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。

ア　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。

イ　パスワードを秘密にし、パスワードの照会には一切応じてはならない。

ウ　パスワードが流出したおそれがある場合、速やかにパスワードを変更するとともに、情報セキュリティ管理者に報告しなければならない。

エ　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。

オ　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。

カ　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。（ただし、シングルサインオンは除く。）

キ　職員の間でパスワードを共有してはならない。（ただし、共有 ID に対するパスワードは除く。）

ク　サーバ及びパソコン等のパスワードは、次のとおり管理する。

（ア）サーバ OS 及びシステムの管理者権限のパスワード管理

区分	サーバ OS	システムの管理者権限
文字	・英数混在（大文字小文字識別有） ・記号使用【推奨事項】	・英数混在（大文字小文字識別有） ・記号使用【推奨事項】
桁数	9 桁以上	9 桁以上
変更周期		システム担当者が変わった際

（イ）パソコン 0S 及びシステムのユーザー権限のパスワード管理

区分	パソコン 0S	システムのユーザー権限
文字	・英数混在（大文字小文字識別有） ・記号使用【推奨事項】	・英数混在（大文字小文字識別有） ・記号使用【推奨事項】
桁数	８桁以上	８桁以上

第８節　技術的セキュリティ

１　コンピュータ及びネットワークの管理

（１）バックアップの実施

ア　情報システム管理者は、サーバにおけるデータのバックアップについて、情報システムの運用サイクル及び障害発生時における目標復旧時点を鑑みた上で、バックアップ周期を定め、計画的に実施しなければならない。

イ　情報システム管理者は、システムのバックアップについて、情報システム導入時及び情報システム修正時に実施しなければならない。

ウ　情報システム管理者は、バックアップに使用した媒体を施錠可能な場所に保管しなければならない。

エ　情報システム管理者は、正常にバックアップが行われているか確認しなければならない。

（２）システム管理記録及び作業の確認

ア　情報システム管理者は、所管する情報システムにおいて、システム変更等の作業を行った場合、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。

イ　情報システム管理者は、情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合、2 名以上で作業内容及び作業結果を確認させなければならない。

（３）情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、業務上必要とする者以外の者による閲覧や紛失等がないよう、施錠可能な場所に保管しなければならない。

（４）ログの取得等

ア　情報システム管理者は、アクセスログ及びその他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。

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

ウ　情報システム管理者は、機密性３、完全性２又は可用性２の情報システムにおいて、取得したアクセスログ等を基に、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、定期的に点検しなければならない。その他の情報システムにおいても、必要に応じて点検を実施しなければならない。

（５）障害記録

情報システム管理者は、職員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及び問題等を、障害記録として記録し、適正に保存しなければならない。

（６）ネットワークの接続制御、経路制御等

ア　情報システム管理者は、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、ルータ等の通信機器を設定しなければならない。

イ　情報システム管理者は、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。

（7）職員以外の者が利用できるシステムの分離

情報システム管理者は、職員以外の者が利用できる情報システムについて、庁内の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。

（8）外部ネットワークとの接続制限等

ア　情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合、統括情報セキュリティ管理者の許可を得なければならない。

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

ウ　情報システム管理者は、接続した外部ネットワークの瑕疵により情報の漏えい、破壊、改ざん及び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。

エ　情報システム管理者は、インターネット接続系にウェブサーバ等を設置する場合、庁内の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インターネットとの境界に設置した上で接続しなければならない。

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

（9）ネットワークに接続した複合機のセキュリティ管理

ア　情報システム管理者は、ネットワークに接続する複合機（複写機、プリンタ、ファクシミリ等の複数の機能を有する機器）を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　情報システム管理者は、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、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。

ウ　情報システム管理者は、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及び再利用できないようにする対策を講じなければならない。

（１０）特定用途機器のセキュリティ管理

情報システム管理者は、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、当該機器の特性に応じた対策を講じなければならない。

（１１）無線 LAN 及びネットワークの盗聴対策

ア　情報システム管理者は、無線 LAN の利用を行う場合、事前に統括情報セキュリティ管理者の許可を得なければならない。

イ　統括情報セキュリティ管理者は、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付けなければならない。

ウ　情報システム管理者は、機密性２以上の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。

（１２）電子メールのセキュリティ管理

ア　情報システム管理者は、権限のない利用者により、外部機関等から外部機関等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。

イ　情報システム管理者は、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、メールサーバの運用を停止しなければならない。

ウ　情報システム管理者は、電子メールの送受信容量の上限を定めなければならない。

エ　情報システム管理者は、職員が使用できる電子メールボックスの容量上限を設定し、上限を超えた場合の対応を職員に周知しなければならない。

オ　情報システム管理者は、情報システムの開発や運用、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。

（１３）電子メール等の利用制限

ア　職員は、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。

イ　職員は、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。

ウ　職員は、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。

エ　職員は、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。

オ　職員は、インターネット上で提供されているフリーメール及び無料のネットワークストレージサービスを使用して情報を送信してはならない。

カ　職員は、原則として、電子メールで機密性３の情報を送信してはならない。ただし、事務事業の達成のための必要最低限の範囲であって、個人の権利利益を侵害するおそれがないと情報セキュリティ管理者が認めた場合は、パスワード等による暗号化を設定した上で送信することができる。

（１４）電子署名・暗号化

職員は、情報資産の分類により定めた取扱制限に従い、外部機関等に送る情報の機密性又は完全性を確保することが必要な場合には、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。

（１５）無許可ソフトウェアの導入等の禁止

ア　職員は、パソコンやモバイル端末に対して、当該機器を所管する情報システム管理者に無断でソフトウェアをインストール及びアンインストールしてはならない。

イ　職員は、業務上、ソフトウェアをインストール及びアンインストールする必要がある場合、当該機器を所管する情報システム管理者の許可を得なければならない。なお、当該ソフトウェアを所管する情報セキュリティ管理者及び情報システム管理者は、ソ

フトウェアのライセンスを管理しなければならない。

ウ　職員は、不正にコピーしたソフトウェアを利用してはならない。

（１６）無許可での機器構成変更の禁止

ア　職員は、パソコンやモバイル端末に対し、当該機器を所管する情報システム管理者の許可なく機器の改造、増設及び交換を行ってはならない。

イ　職員は、業務上、機器の改造、増設及び交換を行う必要がある場合、当該機器を所管する情報システム管理者の許可を得なければならない。

（１７）業務外ネットワークへの接続の禁止

ア　職員は、支給された端末を、有線・無線問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

イ　情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

（１８）業務以外の目的でのインターネット利用の禁止

ア　職員は、業務以外の目的でインターネットを利用してはならない。

イ　統括情報セキュリティ管理者は、職員のインターネット利用について、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、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。

（１９）Web 会議サービスの利用時の対策

ア　統括情報セキュリティ管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。

イ　職員は、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しなければならない。

ウ　職員は、Web 会議を開催する場合、会議に無関係の者が参加できないよう対策を実施しなければならない。

２　アクセス制御

（1）アクセス制御等

ア　アクセス制御

情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員がアクセスできないよう、システム上制限しなければならない。

イ　利用者 ID の取扱い

（ア）情報システム管理者は、利用者の登録、変更、抹消等の情報管理及び職員の異動、出向、退職等に伴う利用者 ID の取扱いの方法を定めなければならない。

（イ）情報システム管理者は、利用されていない ID が放置されないよう、点検しなければならない。

ウ　特権を付与された ID の管理等

（ア）情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必

要最小限にし、当該 ID のパスワードの漏えいが発生しないよう、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）情報システム管理者は、特権を付与された ID 及びパスワードの変更について、自身の許可なく委託事業者に行わせてはならない。

（ウ）情報システム管理者は、特権を付与された ID のパスワードを初期設定以外のものに変更しなければならない。

（２）職員による庁外からのアクセス等の制限

ア　情報システム管理者は、職員に庁外から庁内の情報システムにアクセスさせる場合、統括情報セキュリティ管理者の許可を得なければならない。

イ　情報システム管理者は、庁内の情報システムに対する庁外からのアクセスを、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。

ウ　統括情報セキュリティ管理者は、庁外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。

エ　統括情報セキュリティ管理者は、庁外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義務づけなければならない。

オ　情報システム管理者は、庁外からのアクセスに利用するパソコンやモバイル端末を職員に貸与する場合、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。

カ　職員は、庁外から持ち帰ったモバイル端末等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等を確認しなければならない。

キ　職員は、庁内のネットワークに接続するパソコンやモバイル端末を公衆通信回線（公衆無線 LAN 等）に接続してはならない。また、庁内のネットワークに接続しないパソコンやモバイル端末であっても、公衆通信回線に接続する場合は、機密性２以上の情報を扱ってはならない。

（３）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定又はログイン・ログアウト時刻の表示等により、不正にパソコン等の端末が利用されないよう、設定しなければならない。

（４）認証情報の管理

ア　情報システム管理者は、職員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。

イ　情報システム管理者は、職員に対してパスワードを発行する場合、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。

ウ　情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（５）特権による接続時間の制限

情報システム管理者は、特権による情報システムへの接続時間を必要最小限に制限しなければならない。

3　情報システムの開発、運用及び保守等

（1）情報システムの調達

ア　セキュリティ機能の明記及び調査

（ア）情報システム管理者は、情報システムの開発、運用及び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。

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

イ　責任者及び作業者の特定

情報システム管理者は、情報システムの開発、運用及び保守等の責任者及び作業者を特定しなければならない。

ウ　責任者、作業者の ID の管理

（ア）情報システム管理者は、情報システムの開発、運用及び等に関する責任者及び作業者が使用するＩＤを管理しなければならない。

（イ）情報システム管理者は、情報システムの開発、運用及び保守等に関する責任者及び作業者が使用するＩＤは、職員が使用するＩＤとは別に用意しなければならない。

（ウ）情報システム管理者は、情報システムの開発、運用及び保守等の責任者及び作業者が使用する ID のアクセス権限を設定しなければならならない。

エ　ハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、情報システムの開発、運用及び保守等の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアがインストールされている場合、当該ソフトウェアを情報システムから削除しなければならない。

オ　移行手順の明確化等

（ア）情報システム管理者は、情報システムの開発、保守及びテスト環境から運用環境への移行について、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。

（イ）情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（ウ）情報システム管理者は、導入する情報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。

カ　テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している他の情報システムに接続する前に十分な試験を行わなければならない。

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

（ウ）情報システム管理者は、原則として、機密性３の情報をテストデータに使用して

はならない。

（エ）情報システム管理者は、開発した情報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。

（２）資料等の整備及び保管

ア　情報システム管理者は、情報システムの開発、運用及び保守等に関連する資料及び関連文書を適正に整備し、保管しなければならない。

イ　情報システム管理者は、テスト結果を一定期間保管しなければならない。

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

（３）入出力情報の正確性の確保

ア　情報システム管理者は、情報システムに入力される情報について、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。

イ　情報システム管理者は、故意若しく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。

ウ　情報システム管理者は、情報システムから出力される情報について、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。

（４）変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（５）ソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等の更新及び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。

（６）更新及び統合時の検証等

情報システム管理者は、情報システムの更新・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。

４　不正プログラム対策

（１）統括情報セキュリティ管理者の措置事項

統括情報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。

ア　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、必要に応じ情報システム管理者に対して注意喚起しなければならない。

イ　不正プログラム対策ソフトウェアのパターンファイルの定期的な配信について、自動配信もしくは、媒体による配布を行わなければならない。

（２）情報システム管理者の措置事項

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

ア　外部機関等から受信したファイルは、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、不正プログラムの情報システムへの侵入を防止しなければならない。

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

ウ　不正プログラム対策ソフトウェアは、最新の状態に保たなければならない。ただし、業務への影響が重大で、かつ必要なセキュリティ対策が施されており、統括情報セキュリティ管理者が認めた場合はその限りではない。

エ　インターネットに接続していない情報システムにおいて、統括情報セキュリティ管理者が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と判断した場合を除き、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。

オ　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、最新の状態に保たなければならない。

カ　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。

キ　統括情報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、必要な措置を講じなければならない。

ク　所管するサーバ等がコンピュータウイルス等の不正プログラムに感染した場合及び感染が疑われる場合は、ネットワークからの即時遮断を行わなければならない。

（3）職員の遵守事項

職員は、不正プログラム対策として、次の事項を遵守しなければならない。

ア　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、当該ソフトウェアの設定を変更してはならない。

イ　外部機関等から情報及びソフトウェアを取り入れる場合、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。

ウ　差出人が不明又は不自然な電子メールに添付されたファイルを受信した場合、速やかに削除しなければならない。

エ　使用するパソコンやモバイル端末に対して、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３か月に１回以上、実施しなければならない。

オ　ファイルが添付された電子メールを送受信する場合、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メールの添付ファイル及びインターネット接続系から入手したファイルを情報系に取込む場合は、無害化しなければならない。

カ　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及び感染が疑われる場合、次の対応を行わなければならない。

（ア）有線 LAN の場合

直ちに利用を中止し、LAN ケーブルの取り外しを行わなければならない。

（イ）無線 LAN の場合

直ちに利用を中止し、通信を行わない設定への変更等を行わなければならない。

（４）専門家の支援体制

統括情報セキュリティ管理者は、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、CSIRT と連携し、外部機関等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。

５　不正アクセス対策

（１）不正アクセス対策

ア　情報システム管理者は、使用されているポートのみを開放しなければならない。

イ　情報システム管理者は、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。

ウ　統括情報セキュリティ管理者は、CSIRT と連携し、監視、通知、外部連絡窓口及び適正な対応等を実施できる体制並びに連絡網を構築しなければならない。

（２）攻撃への対処

情報システム管理者は、サーバ等に攻撃を受けた場合及び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、CSIRT と連携し、総務省や都道府県等と連絡を密にして情報の収集に努めなければならない。

（３）記録の保存

情報システム管理者は、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、攻撃の記録を保存するとともに、CSIRT と連携し、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

情報システム管理者は、職員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）職員による不正アクセス

情報システム管理者は、職員による不正アクセスを発見した場合、当該職員が所属する課の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（６）サービス不能攻撃

情報システム管理者は、外部機関等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

情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を防止する対策（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　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

情報システム管理者は、所管する情報システムに関するセキュリティホールの情報を収集し、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、ソフトウェア更新やパッチの適用等の対策を実施しなければならない。

（2）情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ管理者は、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９節　運用

１　情報システムの監視

ア　情報システム管理者は、情報セキュリティに関する事案を検知するため、情報システムを監視しなければならない。

イ　情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ・パソコン間の時刻同期ができる措置を講じなければならない。

ウ　情報システム管理者は、外部と常時接続する情報システムを常時監視しなければならない。

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

ア　情報セキュリティ管理者は、所管する課における情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ管理者を通じてCISOに報告しなければならない。

イ　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。

ウ　情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には、適正かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

統括情報セキュリティ管理者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）職員の報告義務

ア　職員は、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、統括情報セキュリティ管理者に報告を行わなければならない。

イ　職員は、当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ管理者が判断した場合において、危機管理手順書に従って適正に対処しなければならない。

３　侵害時の対応等

（１）危機管理手順書の策定

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティインシデント及び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及び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、復旧及び再発防止等の措置を迅速かつ適正に実施するために、危機管理手順書を定め、セキュリティ侵害時には、当該手順書に従って適正に対処しなければならない。

（２）危機管理手順書に盛り込むべき内容

危機管理手順書には、次の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

（３）危機管理手順書の見直し

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等を踏まえ、必要に応じて危機管理手順書を見直さなければならない。

（４）業務継続計画との整合性確保

ア　統括情報セキュリティ管理者は、地震や風水害等の大規模災害時において、応急・復旧業務や、平常時に行う業務のうち、災害時にも継続することが必要となる重要業務を早期に開始・継続させるために、非常時優先業務を支える情報システムに関して、今後実施すべき事前対策や災害時の体制・行動手順を定めた情報システム業務継続計画（ＩＣＴ－ＢＣＰ）を策定しなければならない。

イ　情報セキュリティ評価委員会は、情報システム業務継続計画（ＩＣＴ－ＢＣＰ）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　例外措置

（１）例外措置の許可

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

（２）緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する場合であって、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

統括情報セキュリティ管理者は、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。

５　法令遵守

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

（１）地方公務員法（昭和 25 年法律第 261 号）

（２）著作権法（昭和 45 年法律第 48 号）

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

（４）個人情報の保護に関する法律（平成 15 年法律第 57 号）
（５）行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
（６）サイバーセキュリティ基本法（平成 28 年法律第 31 号）
（７）個人情報の保護に関する条例
（８）相模原市庁内ネットワークの管理運用に関する要綱
（９）インターネット等に関する個人情報保護管理要綱
（10）相模原市庁内パーソナルコンピュータ管理運用要領
（11）相模原市個人情報取扱事務委託基準

6　違反時の対応

職員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、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管理者は、違反を確認した場合、当該職員が所属する課の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
（２）情報システム管理者は、違反を確認した場合、速やかに統括情報セキュリティ管理者に報告し、当該職員が所属する課の情報セキュリティ管理者に通知した上で、適正な措置を求めなければならない。
（３）情報セキュリティ管理者は、違反を確認した場合、速やかに統括情報セキュリティ管理者に報告した上で、当該職員に対して改善指導を行わなければならない。
（４）職員は、他の職員による違反を確認した場合、速やかに当該職員が所属する課の情報セキュリティ管理者に報告しなければならない。
（５）統括情報セキュリティ管理者は、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、当該職員の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管理者は、職員の権利を停止あるいは剥奪した旨を CISO 及び当該職員が所属する課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１０節　業務委託と外部サービスの利用

１　業務委託

（１）委託事業者の選定基準

ア　情報システム管理者は、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。

イ　情報システム管理者は、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、事業者を選定しなければならない。

（２）契約項目

ア　情報システム管理者は、情報システムの開発、運用及び保守等を委託する場合、情報セキュリティポリシーのうち委託事業者が守るべき事項の遵守を明記した契約を締結しなければならない。

イ　情報システム管理者は、情報システムの開発、運用及び保守等を業務委託する場合、委託事業者との間で、原則として、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。

（ア）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

（イ）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

（ウ）提供されるサービスレベルの保証

（エ）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

（オ）外部委託事業者の従業員に対する教育の実施

（カ）提供された情報の目的外利用及び委託事業受託者以外の者への提供の禁止

（キ）業務上知り得た情報の守秘義務

（ク）再委託に関する制限事項の遵守

（ケ）委託業務終了時の情報資産の返還、廃棄等

（コ）委託業務の定期報告及び緊急時報告義務

（サ）市による監査、検査

（シ）市による情報セキュリティインシデント発生時の公表

（ス）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

情報システム管理者は、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、契約内容に基づいた措置を実施しなければならない。また、契約内容に基づいた措置を実施した場合は、その内容を統括情報セキュリティ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。

２ 外部サービスの利用（機密性２以上の情報を取り扱う場合）

（１）外部サービス利用におけるガバナンスの確保

ア 統括情報セキュリティ管理者は、関係する外部サービス提供者及び利用者の存在を

把握し、必要な連絡体制を構築する。

イ 外部サービスを利用する情報システム管理者は、統括情報セキュリティ管理者に利用申請を行い許可を得なければならない。

（2）規定の整備

ア 外部サービスを利用可能な業務及び情報システムの範囲

本市における基幹系、及び個人番号を取り扱う情報システムを除く情報システムを対象範囲とする。

イ 情報の取扱いを許可する場所

外部サービス提供者のデータセンターの存在地は、日本の法令の範囲内で運用できる必要がある。

（3） 外部サービスの選定

ア 情報システム管理者は、外部サービスを利用する（機密性２以上の情報を取り扱う）場合、原則として、次の選定条件を明記した契約を締結しなければならない。

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

（イ） 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

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

（エ） 外部サービス提供者の資本関係・役員等の情報、外部サービス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

（ク） 外部サービスの中断時の復旧要件や、終了時の事前告知の方法・期限及びデータ移行方法等の円滑な業務移行対策

（ケ） 情報セキュリティ監査の受入れ

（コ） サービスレベルの保証

（サ） 作業場所の特定

（シ） 再委託に関する制限事項の遵守

イ 情報システム管理者は、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、外部サービス提供者を選定しなければならない。

ウ 情報システム管理者は、システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、情報の流通経路全般にわたるセキュリティ対策を調達仕様書に具体的に盛り込まなければならない。

（4）外部サービスの利用に係る調達・契約

情報システム管理者は、外部サービスを調達する場合、選定条件並びに選定時に定め

たセキュリティ要件を調達仕様に含めるとともに、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

（5）外部サービスの利用承認

ア 情報システム管理者は、外部サービスを利用する場合は、外部サービスの利用申請を行い、統括情報セキュリティ管理者の許可を得なければならない。

イ 統括情報セキュリティ管理者は、外部サービス提供者の信頼性が十分であることを総合的・客観的・一元的に情報収集し、評価して、利用の可否を決定する。

（6）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

ア 構築時におけるアクセス制御

（ア）情報システム管理者は、外部サービスを利用する際に外部サービス提供者が付与又は登録する識別コードについて、その作成から廃棄に至るライフサイクルにおいて管理しなければならない。

（イ）情報システム管理者は。外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御を設定しなければならない。

（ウ）情報システム管理者は、外部サービスの管理者特権を保有する利用者に対する強固な認証技術の利用を行わなければならない。

（エ）情報システム管理者は、外部サービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことを確認しなければならない。

（オ）情報システム管理者は、外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることを確認しなければならない。

（カ）情報システム管理者は、外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制を行わなければならない。

（キ）情報システム管理者は、外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施を確認しなければならない。

イ 構築時における暗号化

（ア）情報システム管理者は、外部サービス内及び通信経路全般における暗号化の確認を行わなければならない。

（イ）情報システム管理者は、利用する情報システムに係る法令や規則に対する暗号化方式の遵守について確認しなければならない。

ウ 構築時における開発に係る規定

情報システム管理者は、外部サービスを利用する情報システムの構築において、外部サービス提供者に対し、次の要件を明らかにするよう規定しなければならない。

（ア）セキュリティを保つための開発手順等

（イ）外部サービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス

（ウ）外部サービス提供者による設計、構築における知見

（エ）情報システムを構築する際の設定の誤りを見いだすための対策

（オ）ネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監

視

（カ）情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

（キ）可用性２の情報を取り扱う場合の可用性を考慮した設計

（ク）外部サービス内における時刻同期の方法の確認

（７）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

情報システム管理者は、外部サービスを利用した情報システムの運用・保守において、次の内容を含む規定を整備しなければならない。

ア 外部サービス利用方針の規定

（ア）責任分界点を意識した外部サービスの利用

（イ）利用承認を受けていない外部サービスの利用禁止

（ウ）外部サービス提供者に対する定期的なサービスの提供状態の確認

（エ）利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制

イ 外部サービス利用に必要な教育の実施

（ア）外部サービス利用のための規定及び手順

（イ）外部サービス利用に係る情報セキュリティリスクと対応

（ウ）外部サービス利用に関する適用法令や関連する規制等

ウ 取扱う資産の管理

（ア）外部サービス上で利用する IT 資産の適切な管理

（イ）外部サービス上に保存する情報に対する適切な格付・取扱制限の明示

（ウ）外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施

エ 不正アクセスを防止するためのアクセス制御

（ア）管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

（イ）外部サービス利用者に割り当てたアクセス権限に対する定期的な見直し

（ウ）外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

（エ）利用する外部サービスの不正利用の監視

オ 取り扱う情報の機密性保護のための暗号化

（ア）暗号化に用いる鍵の管理者と鍵の保管場所

（イ）鍵管理機能を外部サービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

（ウ）鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

カ 外部サービス内の通信の制御

（ア）利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

キ 設計・設定時の誤りの防止

（ア）外部サービスの設定を変更する場合の設定の誤りを防止するための対策

（イ）外部サービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

ク 外部サービスを利用した情報システムの事業継続

（ア）不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施（外部サービス提供者が提供する機能を利用する場合は、その実施の確認）

（イ）可用性２の情報を外部サービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施

（ウ）外部サービス提供者からの変更通知の内容確認と復旧手順の確認

（エ）外部サービスで利用しているデータ容量、性能等の監視

ケ 運用・保守時におけるインシデント対応

（ア）外部サービス上での情報セキュリティインシデント、情報の目的外利用等を認知した場合の外部サービス管理者への報告

（イ）外部サービス管理者がインシデント報告を受けた場合の対応

（８） 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

情報システム管理者は、外部サービスを利用した情報システムの更改・廃棄時について、次の内容を含む規定を整備しなければならない。

ア 外部サービス利用終了時における対策

（ア）外部サービスの利用を終了する場合の移行計画書又は終了計画書の作成

（イ）移行計画書又は終了計画書の外部サービス利用者への事前通知

イ 外部サービスで取り扱った情報の廃棄

（ア）情報の廃棄方法

（イ）基盤となる物理機器の廃棄

ウ 外部サービスの利用のために作成したアカウントの廃棄

（ア）作成された外部サービス利用者アカウントの削除

（イ）利用した外部サービス管理者アカウントの削除・返却と再利用の確認

（ウ）外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

３ 外部サービスの利用（機密性２以上の情報を取り扱わない場合）

（１）規定の整備

情報セキュリティ管理者は、外部サービス（機密性２以上の情報を取り扱わない場合）を利用する場合、次の内容を含む規定を整備しなければならない。

ア 外部サービスを利用可能な業務の範囲

イ 外部サービスの利用許可手続と利用状況の管理

ウ 外部サービスの利用の運用手順

（２）対策の実施

職員は、利用するサービスの約款及びその他の提供条件から、利用に当たってのリスクが許容できることを確認した上で、機密性２以上情報を取り扱わない場合の外部サービス利用について情報セキュリティ管理者に許可を得て、利用しなければならない。

3　ソーシャルメディアサービスの利用

職員は、職務としてソーシャルメディアサービスを利用する場合、「相模原市ソーシャルメディア活用ガイドライン」を遵守しなければならない。

第１１節　評価・見直し

１　監査

（１）実施方法

情報セキュリティ監査チームは、本市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、定期的に監査を行わなければならない。

（２）監査を行う者の要件

ア　監査を行う者は、被監査部門から独立した者でなければならない。

イ　監査を行う者は、監査及び情報セキュリティに関する教育を受けた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

ア　情報セキュリティ監査チームは、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ評価委員会の承認を得なければならない。

イ　情報セキュリティ監査チームは、監査実施計画書に基づき、監査を実施しなければならない。ただし、監査の全部又は一部を外部の専門家に委託することができる。

ウ　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

情報セキュリティ監査チームは、情報システム管理者が委託事業者に情報システムの開発、運用及び保守等を委託している場合、当該委託事業者の情報セキュリティポリシーの遵守について、必要に応じて監査を行うことができる。

（５）監査結果への対応

情報セキュリティ監査チームは、監査結果を踏まえ、被監査部門の情報セキュリティ管理者及び情報システム管理者に対し、指摘事項への対処を指示しなければならない。

（６）報告

情報セキュリティ監査チームは、監査結果を取りまとめ、情報セキュリティ評価委員会に報告しなければならない。

（７）保管

情報セキュリティ監査チームは、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。

２　フォローアップ

（１）フォローアップの実施

情報セキュリティ監査チームは、監査結果に基づく指摘事項や改善提案事項について、被監査部門の改善及び是正措置に関して、その後の状況を継続的に調査・確認しなければならない。

（２）報告

情報セキュリティ監査チームは、フォローアップの結果を取りまとめ、情報セキュリティ評価委員会に報告しなければならない。

3　自己点検

（1）実施方法

ア　所属職員の自己点検

情報セキュリティ管理者は、所属する職員に対し、職員が遵守すべき情報セキュリティ対策について、１年に１回以上、自己点検を行わせなければならない。

イ　情報システムの自己点検

情報システム管理者は、所管する情報システムの情報セキュリティ対策について、１年に１回以上、自己点検を実施しなければならない。

（2）自己点検結果の活用

ア　所属職員の自己点検

情報セキュリティ管理者は、職員が実施した自己点検の結果を取りまとめ、その結果に基づき、職員に対し、改善を図るよう指示しなければならない。

イ　情報システムの自己点検

情報システム管理者は、自己点検の結果に基づき、改善を図らなければならない。

4　情報セキュリティ対策基準の見直し

最高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の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティ対策基準について、必要に応じて見直しを行わなければならない。

以　上

対策基準　改訂履歴

Ｖｅｒ.	制定／改訂 承認年月日	改訂項目	改訂内容	改訂理由
初版	H15.3.31	―	初版制定	―
第２版	H19.3.30	Ⅲ管理体制 1　組織 2　責任及び権限 （6）	構成員の変更 項目の変更	組織改変に伴う組織体制及び構成員を各要綱に委任するもの。 項目について修正するもの。
第３版	H22.3.31	Ⅴ　人的セキュリティ対策 1　職員の責任及び権限 2　教育及び訓練 3　セキュリティ事故への対応 Ⅶ　技術的セキュリティ対策 4　コンピュータウィルス対策 Ⅷ　運用管理 5　セキュリティ情報の収集 Ⅸ　監視・検証、監査及び評価・見直し 1　監視及び検証	組織名の変更	組織改変に伴い、組織名を変更するもの。
第４版	H24.3.30	Ⅰ　情報セキュリティ基本方針の取扱い Ⅱ　情報セキュリティ対策基準の取扱い Ⅲ　管理体制 Ⅳ　電子情報の管理 Ⅴ　人的セキュリティ対策 Ⅵ　物理的セキュリティ対策 Ⅶ　技術的セキュリティ対策 Ⅷ　運用管理 Ⅸ　監査及び評価・見直し Ⅹ　情報セキュリティポリシーに関する文書及び記録の管理	遵守項目の全面見直し	情報通信技術の進展や多様化、及び本市の現状を踏まえ、情報セキュリティ水準のさらなる向上を図るため全面的に改訂するもの。
第５版	H27.12.28	第１節　情報セキュリティ基本方針の取扱い 第２節　情報セキュリティ対策基準の取扱い 第３節　管理体制 第４節　電子情報の管理 第５節　人的セキュリティ対策 第６節　物理的セキュリティ対策 第７節　技術的セキュリティ対策	遵守項目の全面見直し	新たな脅威の増大や情報機器の多様化及び本市の現状を踏まえ、情報セキュリティ水準の向上を図るため全面的に改訂するもの。

		第８節　運用管理 第９節　危機管理対策 第１０節　監査及び評価･見直し 第１１節　情報セキュリティポリシーに関する文書及び記録の管理		
第６版	H31.4.1	第１節　情報セキュリティポリシーの遵守等 第２節　定義 第３節　組織体制 第４節　情報資産の分類と管理 第５節　情報システム全体の強靭性の向上 第６節　物理的セキュリティ 第７節　人的セキュリティ 第８節　技術的セキュリティ 第９節　運用 第１０節　外部サービスの利用 第１１節　評価・見直し	遵守項目の全面見直し	総務省が策定するガイドラインの改正及び本市の現状を踏まえ、情報セキュリティ水準の向上を図るため全面的に改訂するもの。
第７版	R2.3.13	第１節　情報セキュリティポリシーの遵守等 第２節　定義 第３節　組織体制 第４節　情報資産の分類と管理 第５節　情報システム全体の強靭性の向上 第６節　物理的セキュリティ 第７節　人的セキュリティ 第８節　技術的セキュリティ 第９節　運用 第１０節　外部サービスの利用 第１１節　評価・見直し	遵守項目の一部見直し	情報資産が保存された情報機器の処分について、より安全かつ確実な作業を担保するため一部規定を改訂するもの。
第８版	R2.4.1	第１節　情報セキュリティポリシーの遵守等 第２節　定義 第３節　組織体制 第４節　情報資産の分類と管理 第５節　情報システム全体の強靭性の向上 第６節　物理的セキュリティ 第７節　人的セキュリティ 第８節　技術的セキュリティ 第９節　運用 第１０節　外部サービスの利用 第１１節　評価・見直し		組織改変に伴い、最高情報セキュリティ責任者（CISO）の職名を変更するもの。

第9版	R3.4.1	第１節　情報セキュリティポリシーの遵守等 第２節　定義 第３節　組織体制 第４節　情報資産の分類と管理 第５節　情報システム全体の強靭性の向上 第６節　物理的セキュリティ 第７節　人的セキュリティ 第８節　技術的セキュリティ 第９節　運用 第１０節　外部サービスの利用 第１１節　評価・見直し	遵守項目の一部見直し	組織改変に伴い、最高情報セキュリティ責任者（CISO）の職名を変更するもの。 組織改変に伴い、統括情報セキュリティ管理者の職名、課名を変更するもの。 情報資産が保存された情報機器の処分について、一部規定を改訂するもの。
第10版	R4.6.1	第４節　情報資産の分類と管理 ２　情報資産の管理	遵守項目の一部見直し	メールの運用変更に際し、一部規定を改定するもの。
第11版	R5.4.1	第１節　情報セキュリティポリシーの遵守等 第２節　定義 第３節　組織体制 第４節　情報資産の分類と管理 第５節　情報システム全体の強靭性の向上 第６節　物理的セキュリティ 第７節　人的セキュリティ 第８節　技術的セキュリティ 第９節　運用 第１０節　外部サービスの利用 第１１節　評価・見直し	遵守項目の一部見直し	総務省が策定するガイドラインの改正及び本市の現状を踏まえ、情報セキュリティ水準の向上を図るため改訂するもの。
第12版	R5.5.31	第６節　物理的セキュリティ １　庁内にサーバ等を設置する際の対策（６）機器の廃棄等	遵守項目の一部見直し	機器の廃棄等に関し、一部規定を改定するもの。