橿原市　情報セキュリティポリシー

令和２年　２月１４日　実施
令和２年　４月　１日　一部改正
令和３年　４月　１日　一部改正
令和６年　４月　１日　一部改正

第１章　橿原市情報セキュリティ基本方針

１．目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２．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

「橿原市情報セキュリティ基本方針」及び「橿原市情報セキュリティ対策基準」の総称をいう。

（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）マイナンバー利用事務系

個人番号利用事務（社会保障、地方税及び災害対策に関する事務）、住民情報等大量の個人情報を扱う事務、戸籍事務等に関わる情報システム並びにデータを取り扱うネットワークをいう。

（９）LGWAN 接続系

グループウェア、財務会計及び人事給与等LGWANに接続された情報システム並びにデータを取り扱うネットワークをいう。

（１０）インターネット接続系

ホームページ閲覧及び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並びにデータを取り扱うネットワークをいう。

（１１）通信経路の分割

LGWAN接続系、インターネット接続系等の異なるネットワーク間の通信環境を分離したうえで、安全が確保された通信のみ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、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．対象とする脅威

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

（１）標的型攻撃、ランサムウェア、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・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・外部監査結果の見直しの不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害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障害による波及等

４．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、教育委員会、行政委員会、議会事務局及び地方公営企業とする。

（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、情報システム及びこれらに関する設備並びに電磁的記録媒体

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、ネットワーク図等のシステム関連文書

５．職員等の遵守義務

職員及び会計年度任用職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６．情報セキュリティ対策

上記３の脅威から情報資産を保護するために、次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）情報資産の分類及び管理

本市の保有する情報資産を機密性、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行う。

（３）強靭性の向上

次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他のネットワークとの通信をできないようにしたうえで、端末からの情報持ち出し不可設定、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、無害化通信を行う。

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行う。

（４）物理的セキュリティ

サーバ等重要な情報システムの設置場所等、通信回線等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、外部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。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に橿原市危機管理指針に則り対応する。

（８）外部サービスの利用

外部サービスを利用する場合には、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、契約に基づき必要な措置を講じる。

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

７．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の把握及び評価を行うため、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。

８．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応することが必要となった場合には、情報セキュリティポリシーを見直す。

９．情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項、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。

１０．情報セキュリティ実施手順の策定

橿原市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　橿原市情報セキュリティ対策基準

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

１．組織体制

（１）最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

①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並びに責任を有する。

②CISOは、情報セキュリティインシデントに対処するための組織CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

（２）統括情報セキュリティ責任者

①企画戦略部長をCISO直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISOを補佐しなければならない。

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

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

④統括情報セキュリティ責任者は、情報セキュリティ責任者、ネットワーク管理者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い（CISOが不在の場合には自らの判断に基づき）、必要かつ十分な措置を行う権限及び責任を有する。

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

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、ネットワーク管理者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧統括情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、有事からの回復のための対策を講じなければならない。

（３）ネットワーク管理者

①情報システム課長をネットワーク管理者とする。

②ネットワーク管理者は、CISO及び統括情報セキュリティ責任者の補佐をしなければならない。

③ネットワーク管理者は、庁内ネットワーク（マイナンバー利用事務系、LGWAN接続系及びインターネット接続系のネットワークをいう。）及び該当ネットワークで利用する情報システムの統括的な管理を行う権限及び責任を有する。

④ネットワーク管理者は、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及び統括情報セキュリティ責任者の指示に従い、必要かつ十分な措置を行う権限及び責任を有する。

（４）情報セキュリティ責任者

①市長部局、行政委員会事務局及び地方公営企業の部局長を情報セキュリティ責任者とする。

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

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

（５）情報セキュリティ管理者

①市長部局、行政委員会事務局及び地方公営企業の所属長を情報セキュリティ管理者とする。

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

③情報セキュリティ管理者は、その所管する所属において、情報資産に対する重大なセキュリティインシデントが発生した場合又は重大なセキュリティインシデントのおそれがある場合には、必要に応じて、情報セキュリティ責任者、ネットワーク管理者、統括情報セキュリティ責任者及び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）情報システム管理者

①各情報システムを所管する所属長等を当該情報システムに関する情報システム管理者とする。

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

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

④情報システム管理者は、その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）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

（８）CISO 及び CSIRT の役割

①CISOは、情報セキュリティインシデントの統一的な窓口の機能を持たせたCSIRTを整備し、その役割を明確化すること。

②CISOは、CSIRTを構成する職員を選任し、その中からCSIRT責任者を置くこと。また、CSIRT内の業務統括及び外部との連携等を行う職員を定めること。

③CSIRTは、CISOによる情報セキュリティ対策の意思決定が行われた際には、その内容を関係部局に提供すること。

④CISOは、CSIRTから情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

⑤CSIRTは、情報セキュリティインシデントを認知した場合には、CISO、関係機関、総務省、奈良県等へ報告すること。

⑥CSIRTは、情報セキュリティに関して、関係機関、外部の事業者等との情報共有を行うこと。

⑦CSIRTは、報告された内容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どうかの判断を行わなければならない。

⑧CSIRTは、重大な情報セキュリティインシデントであると判断した場合、速やかにその旨をCISOに報告しなければならない。

⑨CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止策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。

⑩CSIRT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、CISOに報告しなければならない。

⑪CSIRTは、サーバ等に攻撃を受けた場合、又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、関係機関、総務省、奈良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。

⑫CSIRTは、サーバ等に攻撃を受け、当該攻撃が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）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。

２．情報の分類と情報資産の管理方法

（１）情報の分類

本市における情報は、次の表のとおり、「重要情報」及び「重要情報以外の情報」に分類し、取扱制限を行うものとする。

分類	本市における分類の定義
重要情報	① 特定個人情報､その他個人情報をはじめとする秘密文書に相当する機密性を要する情報
	② 秘密文書に相当する機密性は要しないが､時期や状況により取扱注意となる情報
	③ 誤り、改ざん、破損等により、完全性が損なわれることで、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
	④ 滅失、紛失、利用不可能等により、可用性が損なわれることで、住民の権利が侵害される又は行政事務の安定的な遂行に支障(軽微なものを除く。）を及ぼすおそれがある情報
重要情報以外の情報	①～④のいずれにも該当しない情報

（２）情報資産の管理

①管理責任

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

（イ）情報資産が複製又は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。

②情報資産の分類の表示

職員等は、情報資産について、必要に応じ電子データ、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、取扱制限についても明

示する等適切な管理を行わなければならない。

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扱いをしなければならない。

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

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰ぎ、決定する。

⑤情報資産の利用

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

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

（ウ）情報資産を利用する者は、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）情報セキュリティ管理者及び情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

（イ）情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を必要に応じて講じなければならない。

（ウ）情報セキュリティ管理者又は情報システム管理者は、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の低い地域及び遠隔地に保管しなければならない。

（エ）情報セキュリティ管理者又は情報システム管理者は、重要情報を記録した電磁的記録媒体を保管する場合、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

インターネットメールにより重要情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

（ア）車両等により重要情報と分類された情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）重要情報と分類された情報資産を運搬する者は、情報セキュリティ管理者に許可を得、記録を残さなければならない。

⑨情報資産の提供・公表

（ア）重要情報と分類された情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ）重要情報と分類された情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

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

⑩情報資産の廃棄

（ア）重要情報と分類された情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄処分等しなければならない。

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

３．情報システム全体の強靭性の向上

（１）マイナンバー利用事務系

①マイナンバー利用事務系と他のネットワークとの分離

マイナンバー利用事務系と他のネットワークを通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定及びアプリケーションプロトコルの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

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、２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。

（イ）情報の持ち出し不可設定

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

（２）LGWAN 接続系

①LGWAN接続系とインターネット接続系の分割

LGWAN接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

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

（イ）インターネット業務端末からLGWAN接続系の端末へ画面を転送する方式

（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行わなければならない。

②市区町村のインターネット接続口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、関係機関や他の地方公共団体等と連携しながら、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

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

（２）サーバの冗長化

①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、ネットワーク機器等を必要に応じて冗長化しなければならない。

②情報システム管理者は、停止することで業務に多大な影響を与えるシステム等のメインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

（３）機器の電源

①情報システム管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②情報システム管理者は、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情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等の措置を必要に応じて講じなければならない。

②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、損傷等の報告があった場合、施設管理部門と連携して対応しなければならない。

③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切な管理に努めなければならない。

④情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

（５）機器の定期保守及び修理

①情報システム管理者は、「重要情報」と分類された情報資産を扱うサーバ等の機器の定期保守を実施しなければならない。

②情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の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、情報システム管理者は、外部の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等、秘密保持体制の確認等を行わなければならない。

（６）庁外への機器の設置

情報システム管理者及びネットワーク管理者は、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、CISOの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７）機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、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。

４．２　管理区域（サーバ室等）の管理

（１）管理区域の構造等

①管理区域とは、重要なネットワーク機器及び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（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

②ネットワーク管理者又は情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、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。

③ネットワーク管理者又は情報システム管理者は、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。

（２）管理区域の入退室管理等

①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿等の記載による入退室管理を行わなければならない。

②職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が確認し、外見上職員等と区別できる措置を講じなければならない。

④情報システム管理者は、「重要情報」と分類された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、許可無くコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

②情報システム管理者は、サーバ室の機器等の搬入出について、職員を立ち会わせなければならない。

４．３　通信回線及び通信回線装置の管理

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

②ネットワーク管理者又は統括情報セキュリティ責任者は、「重要情報」と分類された情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

③ネットワーク管理者又は統括情報セキュリティ責任者は、「重要情報」と分類された情報資産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、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情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末の使用時以外の施錠保管等の物理的措置を講じなければならない。

②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。

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。

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等の情報資産の利用を行ってはならない。

③情報資産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、重要情報を含む情報資産を外部で利用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、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

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

④本市の情報資産以外のパソコン、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、原則として、本市の情報資産以外のパソコン、モバイル端

末及び電磁的記録媒体等を業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

（イ）職員等は、本市の情報資産以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

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

⑥パソコン及び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、パソコン及びモバイル端末のセキュリティに関する設定を、ネットワーク管理者又は情報セキュリティ管理者の許可なく変更してはならない。

⑦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管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロック、電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

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、業務を離れた後にあっても業務上知り得た情報を漏らしてはならない。

⑨電子メールの利用制限

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

(イ)職員等は、複数人に電子メールを一斉送信する場合、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BCCに宛先を設定しなければならない。

(ウ)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。

(エ)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。

(オ)職員等は、業務に必要のないフリーメール、ネットワークストレージ

サービス等を使用してはならない。

（２）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

情報セキュリティ管理者は、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、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誓約書等

情報セキュリティ管理者は、会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の誓約書等への署名を求めるものとする。

③インターネット接続、電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員にパソコン及び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、電子メールの使用等が不要の場合、これら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周知

情報セキュリティ管理者は、職員等に情報セキュリティポリシー及び実施手順を周知しなければならない。

（４）委託事業者に対する説明

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

５．２　研修・訓練

（１）情報セキュリティに関する研修・訓練

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

（２）研修計画の策定及び実施

①CISOは、全ての職員等に対する情報セキュリティに関する研修計画の策定を行う。

②CISOは、研修計画において、職員等は定期的に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情報セキュリティ管理者は、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初任者教育を実施しなければならない。

④研修は、統括情報セキュリティ責任者、ネットワーク管理者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者、その他職員等に対して、それぞれの役割に応じたものにしなければならな

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、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

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CSIRT、情報セキュリティ管理者及び情報システム管理者に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者及びネットワーク管理者に報告しなければならない。

③統括情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISOに報告しなければならない。

（２）職員等は市民等外部からの情報セキュリティインシデントの通報についても（１）①、②、③の流れにおいて報告を行う。なお、通報者への状況及び対応結果の報告については、CSIRT から行う。

５．４　ID、パスワード等の管理

（１）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。なお、IDとは情報システムを利用するために、許可された職員等に配布された番号及びコードのことをいう。

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。

（２）ID カード等の取扱い

①職員等は、自己の管理するID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ID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、IDカード等をカードリーダ、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）IDカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、IDカード等の紛失等の通報があり次第、当該ID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統括情報セキュリティ責任者及び情報システム管理者は、IDカード等を切り替える場合、切替え前のカードを改修し、破砕する等復元不可能な処理を行ったうえで廃棄しなければならない。

（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、文字列は推測されにくいものにしなければならない。

④パスワードが流出したおそれがある場合には、パスワードを速やかに変更し、情報セキュリティ管理者に報告しなければならない。

⑤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。

⑥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。

⑦職員等間でパスワードを共有してはならない。

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）ファイルサーバの設定等

①ネットワーク管理者又は情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

②ネットワーク管理者は、ファイルサーバを所属等の単位で構成し、職員等が他所属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。

（２）バックアップの実施

情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、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。

（３）システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③情報システム管理者、情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、軽微なものを除き、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。

（４）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、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、適切に管理しなければならない。

（５）ログの取得等

①情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②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、ログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて不正アクセス、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。

（６）障害記録

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

（７）ネットワークの接続制御、経路制御等

①ネットワーク管理者又は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、ファイアウォール、ルータ等の通信ソフトウェア等を適切に設定しなければならない。

②ネットワーク管理者又は情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（８）外部の者が利用できるシステムの分離等

ネットワーク管理者及び情報システム管理者は、電子申請、電子入札等、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。

（９）外部ネットワークとの接続制限等

①情報システム管理者は、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。

②ネットワーク管理者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

③情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、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。

（１０）複合機等のセキュリティ管理

①情報セキュリティ責任者は、複合機等を調達する場合、当該機器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、適切なセキュリティ要件を策定しなければならない。

②情報セキュリティ責任者は、機器が備える機能について適切な設定等を行うことにより運用中の機器に対する情報セキュリティインシデントへの対策を講じなければならない。

③情報セキュリティ責任者は、機器の運用を終了する場合、機器の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１１）無線 LAN 及びネットワークの盗聴対策

①ネットワーク管理者又は情報システム管理者は、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。

②ネットワーク管理者又は情報システム管理者は、重要情報を含む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

①ネットワーク管理者及び情報システム管理者は、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ネットワーク管理者及び情報システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する等の必要な対策を講じなければならない。

③ネットワーク管理者及び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ネットワーク管理者及び情報システム管理者は、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、上限を超えた場合の対応を職員等に周知しなければならない。

⑤統括情報セキュリティ責任者は、システム開発、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本市ドメインの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ネットワーク管理者及び情報システム管理者は、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添付ファイルの監視等によりシステム上の措置を講じるよう努めなければならない。

（１３）電子署名・暗号化

職員等は、重要な情報資産を外部に送信する場合は、電子署名、暗号化、パスワード設定等、セキュリティを考慮して送信しなければならない。

（１４）無許可ソフトウェアの導入・利用等の禁止

①職員等は、パソコン及びモバイル端末等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、ネットワーク管理者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③職員等は、不正にコピーしたソフトウェアを導入・利用してはならない。

（１５）機器構成の変更の制限

①職員等は、パソコン、モバイル端末等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、パソコン及びモバイル端末等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、ネットワーク管理者及び情報システム管理者の許可を得なければならない。

（１６）無許可でのネットワーク接続の禁止

職員等はネットワーク管理者及び情報システム管理者の許可なくパソコン、モバイル端末等をネットワークに接続してはならない。

（１７）業務以外の目的でのウェブ閲覧の禁止

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。

６．２　アクセス制御

（１）アクセス制御等

①アクセス制御

ネットワーク管理者又は情報システム管理者は、所管するネットワーク又は情報システムごとに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）ネットワーク管理者又は情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、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）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、ネットワーク管理者又は情報システム管理者に通知しなければならない。

（ウ）ネットワーク管理者又は情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、確認しなければならない。

③特権を付与されたIDの管理等

（ア）ネットワーク管理者又は情報システム管理者は、管理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、パスワードを厳重に管理しなければならない。

（イ）ネットワーク管理者又は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）職員等による外部からのアクセス等の制限

①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仕組みを構築する場合、CISOの許可を得なければならない。

②ネットワーク管理者又は情報システム管理者は、原則として、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続することは禁止しなければならない。

③職員等は、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、ネットワーク管理者又は当該の情報システムを管理する情報システム管理者の許可を得なければならない。

④ネットワーク管理者又は情報システム管理者は、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。

⑤ネットワーク管理者又は情報システム管理者は、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の措置を講じなければならない。

⑥ネットワーク管理者又は情報システム管理者は、外部からアクセスするモバイル端末を職員等が利用する場合、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。

（3）自動識別の設定

ネットワーク管理者又は情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるよう、必要に応じて、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

①情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

②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、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ネットワーク管理者又は情報システム管理者は、職員等の認証情報を厳重に管理し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。

②ネットワーク管理者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（6）接続時間の制限

情報システム管理者は、特権によるアクセスも含めた全てのアクセスについて操作がなければ強制ログアウトする等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する措置を講じなければならない。

6．3　システム開発、導入、保守等

（1）情報システムの調達

①ネットワーク管理者又は情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②ネットワーク管理者又は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、必要に応じて情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

①システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための手順を確立しなければならない。

②システム開発における責任者及び作業者のIDの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後不要となった、開発用IDを削除しなければならない。

（イ）情報システム管理者は、必要に応じて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

情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを把握しなければならない。

（３）情報システムの導入

①開発環境及び運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システム開発、保守及びテスト環境を設ける必要がある場合は、システム運用環境を分離しなければならない。

（イ）情報システム管理者は、テスト環境を利用して本番運用を行う場合は、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、システム開発及び保守計画の策定時に手順を明確にしなければならない。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテスト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、あらかじめテスト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、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

（エ）情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織及び導入する組織が、それぞれ独立したテストを行わなければならない。

（４）システム開発及び保守に関連する資料等の整備及び保管

①情報システム管理者は、システム開発及び保守に関連する資料及びシステム関連文書を適切に整備及び保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、ソースコードの提供がある場合は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

（６）開発及び保守用のソフトウェアの更新等

情報システム管理者は、開発及び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。

（７）システム更新又は統合時の検証等

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

６．４　不正プログラム対策

（１）ネットワーク管理者及び情報システム管理者の措置事項

ネットワーク管理者及び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。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

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

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

⑥不正プログラム対策のソフトウェアは、可能な限り最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチ、バージョンアップ等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。やむを得ず利用する場合は、十分なリスク対策を講じなければならない。

⑧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及び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。

（２）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パソコン及びモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

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

⑥ネットワーク管理者が提供する情報セキュリティに関する情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、次に掲げる対応をそれぞれ行わなければならない。

（ア）パソコン等の端末の場合　LANケーブルの即時取り外しを行う。

（イ）モバイル端末の場合　直ちに利用を中止し、通信を行わない設定への変更を行う。

（３）専門家の支援体制

ネットワーク管理者は、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、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）ネットワーク管理者の措置事項

ネットワーク管理者は、不正アクセス対策として、次の事項を措置しなければならない。

①使用されていないポートを閉鎖すること。

②不要なサービスについて、機能を削除又は停止すること。

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、情報システム管理者へ通報するよう、設定すること。

（2）内部からの攻撃

ネットワーク管理者又は情報システム管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

（3）職員等による不正アクセス

ネットワーク管理者又は情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等の所属の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（4）サービス不能攻撃

ネットワーク管理者又は情報システム管理者は、外部からアクセスできる情報システムに対して、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。

（5）標的型攻撃

ネットワーク管理者又は情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育、自動再生無効化等の人的対策及び入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

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

（2）不正プログラム等のセキュリティ情報の収集・周知

ネットワーク管理者は、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・共有

ネットワーク管理者又は情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境、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。

７．運用

７．１　情報システムの監視

①ネットワーク管理者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視できる措置を講じなければならない。

②ネットワーク管理者及び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間の時刻同期ができるよう努めなければならない。

③ネットワーク管理者及び情報システム管理者は、外部と接続するシステムを常時監視できる措置を講じなければならない。

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情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにネットワーク管理者に報告しなければならない。

②ネットワーク管理者は、発生した問題について、適切かつ速やかに対処しなければならない。

③ネットワーク管理者及び情報システム管理者は、ネットワーク、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切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、電磁的記録媒体等の利用状況調査

CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末、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、直ちにネットワーク管理者及び情報セキュリティ管理者に報告を行わなければならない。

②情報セキュリティ管理者は、職員等から報告を受けた事項についてセキュリティ責任者に報告を行わなければならない。情報セキュリティ責任者は、報告を受けた事項が橿原市危機事案対策調整会議設置規定第２条に規定する危機事案に該当すると判断する場合は、直ちに危機管理監に報告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

CISO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切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２）業務継続計画との整合性確保

CISOは、情報セキュリティポリシーと業務継続計画（橿原市BCP）の整合性を確認しなければならない。

７．４　例外措置

（１）例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティポリシー及び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こと、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り、ネットワーク管理者が認めた場合には、CISOの許可を得て、例外措置を取ることができる。

（２）例外措置の申請書の管理

情報セキュリティ管理者及び情報システム管理者は、例外措置が必要な状況が終了した場合には、直ちに、ネットワーク管理者に報告しなければならない。CISOは、定期的に申請状況を確認しなければならない。

７．５　法令遵守

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

７．６　懲戒処分等

（１）懲戒処分の対象

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

（２）違反時の対応

次に掲げる者は、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、速やかにそれぞれ次に掲げる事項を行わなければならない。

①統括情報セキュリティ責任者は、当該職員等の所属の情報セキュリティ管理者に通知し、適切な措置を求める。

②ネットワーク管理者、情報システム管理者等は、速やかに統括情報セキュリティ責任者及び当該職員等の所属の情報セキュリティ管理者に通知し、適切な措置を求める。

③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又は剥奪するかどうかを判断し、停止又は剥奪した場合は、速やかにその旨をCISO及び当該職員等の所属の情報セキュリティ管理者に通知する。

８．外部サービスの利用

８．１　外部委託

（１）委託事業者の選定基準

①情報セキュリティ管理者は、委託事業者の選定にあたっては、必要に応じて委託内容に応じた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情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況等を参考にして、委託事業者を選定しなければならない。

③情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（２）契約項目

情報システムの運用、保守等を外部委託する場合には、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、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、範囲及びアクセス方法
・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受託者以外の者への提供の禁止
・業務上知り得た情報の目的外利用及び受託者以外の者への提供の禁止
・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
・市による監査及び検査
・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

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置しなければならない。

８．２　ソーシャルメディアサービスの利用

職員等は、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、別に定めるソーシャルメディアの利用に関するガイドラインに基づき利用する。

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、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

①CISO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

①CISOは、監査を行うに当たって、監査実施計画を立案しなければならない。

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

委託事業者に委託している場合、CISOは再委託事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（５）報告

監査を実施する者は、監査結果を取りまとめ、CISO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及び監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（７）監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合に

は、当該課題及び問題点の有無を確認させなければならない。

（８）情報セキュリティポリシー、関係規程等の見直し等への活用

CISOは、監査結果を情報セキュリティポリシー、関係規程等及びその他情報セキュリティ対策の見直し時に活用するよう努めなければならない。

９．２　自己点検

（１）実施方法

①ネットワーク管理者及び情報システム管理者は、所管するネットワーク及び情報システムについて、定期的及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局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、定期的及び必要に応じて自己点検を行わなければならない。

（２）報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、改善策を含めた自己点検結果をCISO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。

②CISOは、自己点検の結果を情報セキュリティポリシー、関係規程等及びその他情報セキュリティ対策の見直し時に活用するよう努めなければならない。

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

CISO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、情報セキュリティポリシー及び関係規程等について定期的又は重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。