亀岡市情報セキュリティ対策基準規程

Standards for Information Security Measures

平成 27 年(2015 年)　4 月

令和 4 年(2022 年)　11 月(改正)

作成：政策企画部　情報政策課

目　　次

第１章　総則

第１条　目的

この規程は、本市の情報セキュリティ対策を実施するために必要となる統一的な基準を定めることにより、情報資産を組織として適切に管理し、運用を図るために必要な事項を定めるものとする。

第２条　定義

この規程において使用する用語の意義は、亀岡市情報化の推進に関する規程（平成25年亀岡市訓令第4号。以下「情報化推進規程」という。）の例によるほか、次に掲げるところによる。

第１号

行政系ネットワーク　「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。

第２号

基幹業務システム　住民記録、税、国民健康保険、国民年金、福祉等の情報を一括的に処理するための情報システムをいう。

第３号

電算処理　基幹業務システムを使用して行われる情報の入力、蓄積、加工、編集、修正、更新、検索、消去、出力その他これらに類する処理をいう。

第４号

業務主管課　主に基幹業務システムに係る電算処理業務を主管する課等をいう。

第５号

記録媒体　USBメモリ、光ディスク、磁気ディスク、フラッシュメモリその他の電子情報を記録するための媒体をいう。

第６号

USBメモリ　記録媒体のうち、コンピュータのUSBコネクタ等に接続して使用する持ち歩きが可能な記録媒体をいう。

第 7 号

モバイル端末　小型若しくは薄型又は軽量で持ち歩きが可能であり、かつ、一定時間電源に接続することなく使用することができる情報通信機器をいう。

第 8 号

マイナンバー利用事務系(個人番号利用事務系)　個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

第 9 号

LGWAN 接続系　LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

第 10 号

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。

第 11 号

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のみを許可できるようにすることをいう。

第 12 号

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。

第３条　適用範囲

この規程が適用される範囲は、本市の情報資産に関する業務に携わる全ての職員等（臨時的任用職員及び非常勤職員を含む。以下「職員等」という。）とする。

第2項

この規程が適用される情報資産は、ネットワーク及び情報システムで取り扱う構成機器並びにネットワーク及び情報システムで取り扱う全ての情報資産（紙等の有体物に出力された情報を含む。以下同じ。）とする。

第３条の２　対象とする脅威

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

第１号

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

第2号

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、操作又は設定ミス、メンテナンス不備、内部又は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

第3号

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

第4号

大規模又は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

第5号

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

第４条　情報セキュリティ対策の管理体制

情報セキュリティ対策における、最高情報統括責任者、情報統括管理者、情報責任者、情報管理者、ネットワーク管理者及びシステム業務管理者の権限及び責任は、情報化推進規程に定めるもののほか、次に掲げるところによる。

第１号

最高情報統括責任者は、市におけるネットワーク、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。

第２号

情報統括管理者は、市におけるネットワーク、情報システム等の情報資産の管理及び情報

セキュリティ対策の実施について、必要な指示をする権限及び責任を有する。

第３号

情報責任者は、所管する部等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し、情報資産の管理及びこれに係る情報セキュリティを適正に実施する。

第４号

情報管理者は、所管する課等における情報資産を利用する職員等に対して、情報セキュリティ対策に関する指導及び監督を行う権限及び責任を有する。情報管理者は、情報責任者の命を受け、所管する課等における情報セキュリティ対策を実施する。

第５号

ネットワーク管理者は、本市のネットワークを使用して構築された情報システムについて、情報セキュリティ対策の具体的な手順等を明記した情報セキュリティ実施手順（以下、実施手順という。）を策定するものとする。

第６号

システム業務管理者は、情報責任者の命を受け、所管する情報システムの適正な管理及び情報セキュリティ対策を実施するとともに、情報システムごとに実施手順を策定するものとする。

第２章　情報資産の分類及び管理等

第１節　情報資産の分類及び管理

第５条　情報資産の分類

情報資産は、情報セキュリティの重要性に応じ、次に掲げる分類に区分する。

第１号

重要性分類Ⅰ　亀岡市情報公開条例（平成12年亀岡市条例第32号）第7条各号に規定する不開示情報を含む情報資産

第２号

重要性分類Ⅱ　公にすることを予定していない情報資産（個人情報を含む情報資産を除く。）及び情報セキュリティに対する侵害が市の事務又は事業の執行等に重大な影響を及ぼすおそれのあ

る情報資産

第３号

重要性分類Ⅲ　前2号に掲げる情報資産以外の情報資産

第2項

前項に掲げる情報資産の重要性分類の指定は、情報責任者が行う。

第６条　情報資産の管理

ネットワーク管理者、情報管理者及びシステム業務管理者（以下「情報資産管理責任者」という。）は、所管する情報資産を前条第1項の分類に従い責任をもって適正に管理しなければならない。

第2項

職員等は、情報システムで取り扱う情報を、前条第1項の分類に従い責任をもって適正に利用しなければならない。

第７条　情報資産の取扱い

職員等は、情報資産を取り扱う場合は、次に掲げる事項を遵守しなければならない。

第１号

業務上必要のない情報資産を作成し、又は入手しないこと。

第２号

情報資産を作成し、又は入手したときは、第5条の規定による重要性の分類を定めること。

第３号

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すること。（情報の作成途上で不要になった場合は、当該情報を消去すること。）

第４号

業務以外の目的に情報資産を利用しないこと。

第５号

情報資産を利用する者は、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、当該記録媒体を取り扱うこと。

第６号

重要性分類Ⅰ及びⅡの情報資産は、原則として支給以外の端末で作業をしないこと。

第７号

必要以上に複製及び配布をしないこと。

第８条　情報資産の外部提供及び公表

重要性分類Ⅰに該当する情報資産等は、法令又は条例の規定に基づく場合を除き、外部に提供してはならない。

第2項

重要性分類Ⅰ及びⅡの情報資産等を外部に提供する者は、情報資産管理責任者の承認を得た上で、必要に応じ鍵付きケースへの格納、パスワード等による暗号化等を行わなければならない。

第3項

情報資産管理責任者は、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。

第９条　情報資産の送信

重要性分類Ⅰに該当する電子情報は、電子メール等により送信してはならない。ただし、他に合理的な方法がない場合には、情報資産管理責任者の承認を得た上で、総合行政ネットワーク（以下「LGWAN」という。）を利用し、暗号化及びパスワード設定を行わなければならない。

第2項

重要性分類Ⅱに該当する電子情報を電子メール等により送信する必要がある場合は、情報資産管理責任者の承認を得た上で、暗号化及びパスワード設定を行わなければならない。

第3項

前2項により暗号化及びパスワード設定を行う場合において、復号鍵又はパスワードは、当該電子メール等以外の確実な方法により送信先に伝達しなければならない。

第２節　基幹業務システムにおけるデータ等の管理

第１０条　データの使用又は閲覧

業務主管課が保有する、基幹業務システムに係るデータ(以下この節において「データ」という。)を、他の課等がデータを閲覧又は使用し電算処理を行う場合又は処理を外部に委託する場合は、データ使用・閲覧承諾申請により、業務主管課の承諾及びネットワーク管理者の同意を得なければならない。ただし、インターネットに公開されているデータについては、この限りでない。

第１１条　データの出力

業務主管課が保有するデータを、電算処理により帳票等に出力する場合は、あらかじめデータ出力承諾申請により、ネットワーク管理者の承諾を得なければならない。

第2項

業務主管課が保有するデータを、他の課等が電算処理により帳票等に出力する場合も前項と同様とする。この場合、あらかじめデータを保有する業務主管課の同意を得るものとする。

第3項

業務主管課が、電子計算機室で出力処理を終えた帳票等を電子計算機室から搬出する場合は、出力帳票等記録簿に必要事項を記入して電子計算機担当課職員の確認を受けなければならない。

第１２条　処理計画等の提出

業務主管課は、翌月の電算処理計画を電算処理計画書により当月の 20 日までにネットワーク管理者に提出しなければならない。

第３章　人的セキュリティ

第１節　職員等の責務

第１３条　職員等の役割及び責任

職員等は、情報セキュリティ対策の実施にあたり、次に掲げる事項を遵守しなければならない。

第１号

この規程及び実施手順に定められている事項を遵守すること。

第２号

この規程及び実施手順について不明な点及び遵守することが困難な点がある場合は、速やかに情報管理者に報告し、指示等を仰ぐこと。

第３号

業務以外の目的で情報システム又は電子メールの使用及びインターネットへのアクセス等をしないこと。

第４号

使用を許可された情報システムを、最大の注意義務をもって使用すること。

第５号

業務において利用するパソコン、モバイル端末（以下「パソコン等」という。）、記録媒体、情報システム、ソフトウェア等を外部に持ち出さないこと。ただし、外部で情報処理業務を行う等必要な場合で事前に情報管理者の許可を得たときは、この限りでない。

第６号

支給以外のパソコン等、記録媒体、情報システム、ソフトウェア等を業務で利用しないこと。ただし、業務上の必要がある場合は、別に CIO が定めるガイドラインに従い、事前に情報管理者の許可を得たものについては、利用することができる。

第７号

情報漏えい及び不正操作を防止するため、離席するときは、パスワード入力が必要な画面に戻す等、情報システムの業務内容及び機能に応じて適切な対策を講じること。

第８号

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すること。また、その後も業務上知り得た情報を漏らさないこと。

第１４条　臨時的任用職員等に対する指導

情報管理者は、臨時的任用職員、非常勤職員、外部委託事業者等に情報資産を取り扱わせる

場合は、この規程及び実施手順の内容を遵守させる等取扱いに関する適切な指導を行わなければならない。

第2項

ネットワーク管理者及び情報管理者は、臨時的任用職員又は非常勤職員の採用の際、必要に応じ、情報セキュリティ対策基準等を遵守する旨の同意書への署名を求めるものとする。

第3項

ネットワーク管理者は、臨時的任用職員又は非常勤職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

第１５条　パスワードの管理

職員等は、自己の保有するID及びパスワード（以下「パスワード」という。）の管理について、次に掲げる事項を遵守しなければならない。

第１号

パスワードを他者に知られないよう厳重に管理すること。

第２号

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ないこと。

第３号

職員等の間でパスワードを共有しないこと。

第４号

パソコン等にパスワードを記憶させないこと。

第５号

パスワードを他者に知られた場合又は知られた可能性がある場合は、直ちにネットワーク管理者及びシステム業務管理者に報告すること。

第６号

インターネット系ネットワークに接続するための初期パスワードは、最初のログイン時に

変更すること。

第１６条　ＩＣカードの管理

職員等は、自己の保有するICカードの管理について、次に掲げる事項を遵守しなければならない。

第１号

ICカードを貸与しないこと。

第２号

業務上必要のないときは、IC カード等をカードリーダから抜いておくこと。

第３号

ICカードを紛失又は毀損した場合若しくは盗難、詐取等にあった場合（以下「紛失等」という。）は、直ちにネットワーク管理者及び情報管理者に報告すること。

第2項

ネットワーク管理者及び情報管理者は、紛失等の報告を受けたときは、直ちに該当するICカードの利用を無効とする措置を講じなければならない。

第１７条　業務に利用するソフトウェア

職員等は、端末の誤動作、コンピュータウイルスの感染等を防止するため、パソコン等の端末に無断でソフトウェアを導入してはならない。

第2項

職員等は、情報管理者が業務上特に必要と認め、ネットワーク管理者がパソコン等の端末の動作に支障がないと認める場合は、定められたソフトウェア以外のソフトウェアを、パソコン等の端末に導入することができる。

第3項

前項の場合において、情報管理者は、事前にパソコン環境変更に係る申請を行い、ネットワーク管理者の許可を得なければならない。

第4項

ネットワーク管理者及び情報管理者は、導入したソフトウェアのライセンスを管理しなければならない。

第5項

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。

第１８条　機器構成の変更

職員等は、端末の誤動作、保守の困難化等を防止するため、パソコン等の端末に対し無断で設定の変更、機器の改造及び増設・交換を行ってはならない。

第2項

職員等は、情報管理者が業務上特に必要と認め、ネットワーク管理者がパソコン等の端末の動作に支障がないと認める場合は、設定の変更、機器の改造及び増設・交換を行うことができる。

第3項

前項の場合において、情報管理者は、事前に前条第 3 項に規定する申請を行い、ネットワーク管理者の許可を得なければならない。

第4項

職員等は、ネットワーク機器の設定を変更してはならない。

第5項

職員等は、ネットワーク管理者の許可なくパソコン等の端末をネットワークに接続してはならない。

第１９条　Web 会議サービスの利用

ネットワーク管理者は、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。

第2項

職員等は、本市の定める利用手順に従い、セキュリティ対策を実施するものとする。

第２０条　職員等によるコンピュータウイルス対策

職員等は、情報システムへのコンピュータウイルス感染を防止するため、次に掲げる事項を遵守しなければならない。

第１号

記録媒体、電子メール等によりデータ又はソフトウェアを外部から取り入れる場合又は外部にデータを送付する場合は、必ずコンピュータウイルスチェックを行うこと。

第２号

ネットワーク管理者が提供するコンピュータウイルスに関する情報及び指導を常に確認し、その情報及び指導に従い必要な措置を講じること。

第３号

コンピュータウイルス対策ソフトウェアの設定を許可なく変更しないこと。

第４号

コンピュータウイルスが発見された場合は、直ちに情報システムの利用を中止し、情報管理者を通じてネットワーク管理者に報告するとともに、ネットワーク管理者の指示に従うこと。

第５号

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、速やかに削除すること。

第６号

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うこと。この場合において、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。

第２１条　セキュリティ事故等に対する報告

職員等は、情報セキュリティに対する事故、情報システム上の欠陥及び誤動作等を発見したとき、又は住民等からの連絡を受けたときは、速やかに情報管理者又はシステム業務管理者を通してネットワーク管理者に報告しなければならない。

第２項

ネットワーク管理者、システム業務管理者又は情報管理者は、報告のあった事故等について、セキュリティ事故報告書（別記第１号様式）により情報統括管理者に報告しなければな

らない。

第 3 項

情報統括管理者は、CSIRT に指示し、当該事故等について状況の確認及び評価をさせなければならない。また、当該事故等が外部に重大な影響を及ぼすおそれがある場合には、最高情報統括責任者に報告し必要な指示を仰がなければならない。

第 4 項

CSIRT は、情報統括管理者の指示を受け、当該事故等に係る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対応を行わなければならない。

第 5 項

CSIRT は、これらの事故等を分析し、再発防止のための情報として記録し、適切に保存しなければならない。また、事故原因の究明結果から、再発防止策を検討し、最高情報統括責任者に報告しなければならない。

第 6 項

最高情報統括責任者は、CSIRT から事故等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。

第２１条の２

職員等は、使用する電子計算機等に事故が発生した場合は、ネットワーク管理者及び情報管理者に報告しなければならない。

第 2 項

ネットワーク管理者、システム業務管理者又は情報管理者は、前項の報告のあった事故等について、電子計算機等事故発生報告書(別記第 2 号様式)により情報統括管理者に報告しなければならない。

第 3 項

情報統括管理者は、当該事故等の復旧に必要な措置について、ネットワーク管理者、システム業務管理者又は情報管理者に指示するとともに、当該事故等が外部に重大な影響を及ぼすおそれがある場合には、最高情報統括責任者に報告し必要な指示を仰がなければならない。

第４項

ネットワーク管理者、システム業務管理者又は情報管理者は、これらの事故等を分析し、再発防止のための情報として記録し、適切に保存しなければならない。また、事故原因の究明結果から、再発防止策を検討し、最高情報統括責任者に報告しなければならない。

第５項

最高情報統括責任者は、情報統括管理者から事故等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。

第２節　情報セキュリティに関する啓発及び周知

第２２条　情報セキュリティに関する啓発及び周知

最高情報統括責任者は、職員等に対し、情報セキュリティについての啓発を行わなければならない。

第2項

情報管理者は、所属する職員等に対して、情報セキュリティに関する周知を行い、その徹底を図らなければならない。

第２３条　情報セキュリティに関する教育及び訓練

最高情報統括責任者は、職員等に対し、その役割に応じた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。

第2項

職員等は、定められた研修に参加し、情報セキュリティ及び実施手順を理解し、情報セキュリティ上の問題を生じさせないようにしなければならない。

第４章　物理的セキュリティ

第１節　執務室等での管理

第２４条　執務室等での管理

執務等を行う場所（以下「執務室等」という。）の施設に関する警備、施錠等の物理的情報セキュリティ対策は、施設の管理責任者及び情報管理者が行わなければならない。

第2項

職員等は、執務室等に配置した端末について、盗難防止のため、ワイヤー等による固定又は施錠可能な保管庫に収納できるものは、業務が終了した時点で収納し厳重に保管しなければならない。

第3項

職員等は、第三者に情報を閲覧されることがないようにしなければならない。

第4項

職員等は、端末及び記録媒体について、第三者に使用されることがないよう管理しなければならない。

第２節　管理区域の管理

第２５条　管理区域の管理

ネットワーク管理者は、サーバ等、特に重要な情報システムの設置及び運用を行うための部屋（以下「管理区域」という。）について、火災その他の災害及び盗難等に備え次に掲げる措置を講じなければならない。

第１号

管理区域内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を行うこと。

第２号

管理区域内に設置する消火剤や消防用設備等が、機器及び記録媒体等に影響を与えるものでないこと。

第３号

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、監視装置、警報装置等によって許可されていない立入りを防止すること。

第４号

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ぎ、外部からの侵入が容易にできないようにすること。

第５号

管理区域内の情報システムに関連しない機器、通信回線装置、記録媒体等を持ち込ませないこと。

第２６条　管理区域の入退室管理

ネットワーク管理者は、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。

第2項

管理区域へ入室が認められた職員等は、入退室記録簿（別記第３号様式）に入退室時間、氏名及び用件を記入しなければならない。

第3項

ネットワーク管理者は、外部委託事業者等を、管理区域に入室させる場合、必要に応じ身分証明書等の提示を求めるものとする。

第4項

ネットワーク管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立入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。

第5項

ネットワーク管理者は、管理区域について、当該情報システムに関連しない、又は個人所有であるパソコン等、通信回線装置、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。ただし、やむを得ず持ち込む必要がある場合、情報政策課職員が立ち合いの上、持ち込みを許可することとする。

第２７条　管理区域の機器等の搬入出

ネットワーク管理者は、管理区域へ搬入する機器等が、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事業者に確認を行わせなければならない。

第2項

ネットワーク管理者は、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。

第３節　機器等に対する管理

第２８条　機器の取付け

新たにネットワーク機器及び情報システム機器等を設置又は更新する場合は、最高情報統括責任者とあらかじめ協議しなければならない。

第2項

情報資産管理責任者は、ネットワーク機器及び情報システム機器等の取付けを行う場合、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した施錠可能な区画内に設置し、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。

第3項

情報資産管理責任者は、システムの停止により、行政事務の執行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い、同一データを保持し、システムの運用が停止しないように努めなければならない。

第２９条　機器の電源

情報資産管理責任者は、施設管理部門と連携して、ネットワーク機器及び情報システム機器等の電源について、当該機器を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。

第2項

情報資産管理責任者は、施設管理部門と連携して、落雷等による過電流に対して、ネットワーク機器及び情報システム機器等を保護するための措置を講じなければならない。

第３０条　通信ケーブル等の配線

職員等は、通信ケーブル及び電源ケーブルを損傷しないよう適切に取り扱うとともに、ネットワーク管理者の許可なく通信ケーブルの配線を変更又は追加してはならない。

第2項

ネットワーク管理者及びシステム業務管理者は、施設管理部門と連携して、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。

第3項

ネットワーク管理者及びシステム業務管理者は、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。

第4項

ネットワーク管理者及びシステム業務管理者は、ネットワーク接続口を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

第３１条　機器等の定期保守及び修理

ネットワーク管理者及びシステム業務管理者は、重要性分類Ⅰ及びⅡの情報を記録したそれぞれが所管する情報システム機器について、定期保守を実施しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、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は、内容を消去し、又は内容を消去できない場合においては、事業者と守秘義務契約を締結する等、機密保持の措置を講じなければならない。

第３２条　市の施設以外への機器の設置

ネットワーク管理者及びシステム業務管理者は、市の施設以外の場所に情報システムを設置し、又は事業者等が設置する情報システムを利用しようとする場合は、必要な情報セキュリティ対策が十分に確保されていることを確認し、最高情報統括責任者の承認を受けなければならない。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。

第３３条　機器の廃棄等

ネットワーク管理者及びシステム業務管理者は、情報システム機器を廃棄、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。

第３４条　庁舎内の通信回線等の管理

情報統括管理者は、庁舎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。

第2項

情報統括管理者は、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。

第3項

情報統括管理者は、重要性分類Ⅰ及びⅡの情報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。

第4項

情報統括管理者は、重要性分類Ⅰ及びⅡ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。

第5項

ネットワークに使用する回線は、送信途上においてデータの破壊、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が実施されたものでなければならない。

第３５条　マイナンバー利用事務系のセキュリティ対策

マイナンバー利用事務系は、他の領域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、インターネット以外の回線を選択するとともに、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。

第2項

前項ただし書において、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、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータ移送を行うことができる。

第3項

ネットワーク管理者は、マイナンバー利用事務系の情報の持出しの対策として、原則 USB

メモリ等の記録媒体による端末からの情報の持出しができないように設定しなければならない。

第３５条の２　ＬＧＷＡＮ接続系のセキュリティ対策

LGWAN 接続系及び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、必要な通信のみを許可できるようにしなければならない。なお、メール又はデータを LGWAN 接続系に取り込む場合は、次の方式により、無害化通信を図らなければならない。

(1) 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

(2) 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

第３５条の３　インターネット接続系のセキュリティ対策

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及び対処並びに 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。

第2項

都道府県及び市区町村のインターネットとの通信を集約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、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

第3項

業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

第４節　記録媒体の取扱い及び管理

第３６条　記録媒体の管理

情報資産管理責任者は、情報資産の分類に従って、情報資産の盗用、漏えい、紛失及び破損等を防止するため、記録媒体について、次に掲げるとおり、適切な管理を行わなければならない。

第１号

最終的に確定したデータを記録した記録媒体は、書込禁止措置を行ったうえで保管すること。

第 2 号

重要性分類Ⅰ及びⅡの情報を記録した記録媒体を保管する場合、施錠可能な場所に保管すること。

第 3 号

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への保管を考慮すること。

第 4 号

重要性分類Ⅰ及びⅡの情報を記録した記録媒体の搬送にあたっては、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ること。

第 5 号

重要性分類Ⅰ及びⅡの情報を記録した記録媒体を運搬する者は、情報資産管理責任者に許可を得ること。

第３７条　記録媒体の廃棄

重要性分類Ⅰ及びⅡの情報を記録した記録媒体が不要となった場合は、当該記録媒体の初期化等、データを復元できないように処置した上で廃棄しなければならない。

第2項

記録媒体の廃棄を行う者は、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。

第3項

記録媒体の廃棄を行う者は、情報資産管理責任者に許可を得なければならない。

第３８条　ＵＳＢメモリの取扱い

情報管理者は、USB メモリを使用しようとするときは、ネットワーク管理者に USB メモリ等使用申請を行い、その承認を受けなければならない。この場合において、承認する期間は、当該年度内とする。

第2項

前項の規定により使用するUSBメモリは、ハードウェア暗号化及びパスワードによる認証をすることができるものでなければならない。

第3項

職員等は、情報資産の盗用、漏えい、紛失及び破損等を防止するため、USBメモリを外部に持ち出してはならない。ただし、次の各号のいずれかに該当する場合は、情報管理者は、その持出しを職員又は守秘義務を明記した契約等を締結した外部事業者に行わせるとともに、USBメモリの物理的な保護措置の指示を出し、USBメモリ等管理台帳（別記第4号様式）に記載し、許可を与えることができる。

第１号

所属する課等以外に情報を持ち出す必要がある場合

第２号

国、地方公共団体及び外部委託事業者等との情報の交換が必要な場合

第３号

その他特に必要と認められる場合

第4項

前項各号の理由により外部に持ち出したUSBメモリは、その使用後は速やかに記録した情報の削除を行い、情報管理者に報告しなければならない。

第5項

情報管理者は、USBメモリを使用しないときは、施錠した場所に保管し、かつ、類推されにくいパスワードを設定するなど、紛失又は盗難を防止する措置を講じなければならない。

第6項

情報管理者は、USBメモリを紛失し、又は盗難にあった場合は、直ちにその状況を調査し、必要な措置を講じるとともに、その旨をネットワーク管理者に報告しなければならない。

第５章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

第３９条　ファイルサーバの設定等

ネットワーク管理者は、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。

第2項

ネットワーク管理者は、ファイル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。

第3項

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

第４０条　アクセス記録の取得等

ネットワーク管理者及びシステム業務管理者は、アクセス記録及び情報セキュリティの確保に必要な記録（以下「アクセス記録等」という。）を取得し、窃取、改ざん、誤消去等を防止する措置を講じた上で一定期間保存しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、取得したアクセス記録等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。

第４１条　情報システム仕様書等の管理

ネットワーク管理者及びシステム業務管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体の形態に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすることがないよう、適切な管理をしなければならない。

第４２条　情報資産のバックアップ

ネットワーク管理者及びシステム業務管理者は、ファイルサーバ等に記録された情報資産につい

て、サーバの二重化対策実施の有無に関わらず、必要に応じて定期的に情報資産のバックアップを実施しなければならない。

第４３条　ログの取得等

情報統括管理者及びネットワーク管理者は、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。

第2項

情報統括管理者及びネットワーク管理者は、取得したログを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。

第４４条　ネットワークのアクセス制御

ネットワーク管理者は、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、ファイアウォール、ルータ等の通信機器、通信ソフトウェア等を設定しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、不正アクセスを防止するため、ネットワークのアクセス制御について、適切な措置を講じなければならない。

第４５条　外部の者が利用できるシステムの分離

ネットワーク管理者及びシステム業務管理者は、インターネット等により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。

第４６条　外部ネットワークとの接続制限

ネットワーク管理者及びシステム業務管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、最高情報統括責任者及び情報統括管理者の許可を得なければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、適用範囲における情

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。

第3項

ネットワーク管理者及びシステム業務管理者は、当該外部ネットワークのかしにより本市のデータの漏えい、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応するため、必要に応じて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するよう努めなければならない。

第4項

情報統括管理者及びネットワーク管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

第5項

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、適用範囲における情報資産に脅威が生じることが想定される場合には、ネットワーク管理者及びシステム業務管理者は当該外部ネットワークとの接続を物理的に遮断しなければならない。

第４７条　複合機のセキュリティ管理

情報管理者は、複合機を調達する場合、当該複合機が備える機能、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。

第2項

情報管理者は、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。

第3項

情報管理者は、複合機の運用を終了する場合、複合機の持つ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。

第４８条　IoT 機器を含む特定用途機器のセキュリティ管理

情報統括管理者は、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。

第４９条　無線 LAN 及びネットワークの盗聴対策

情報統括管理者は、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。

第2項

情報統括管理者は、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。

第3項

ネットワーク管理者及びシステム業務管理者が許可した端末以外は、庁内無線 LAN に接続してはならない。

第4項

マイナンバー利用事務系においては、無線 LAN に接続して通信を行ってはならない。

第２節　電子メールの取扱い及び管理

第５０条　電子メールのセキュリティ対策

ネットワーク管理者は、電子メールの不正な第三者中継を不可能とするよう、電子メールサーバの設置を行わなければならない。

第2項

ネットワーク管理者は、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。

第3項

ネットワーク管理者は、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。

第4項

ネットワーク管理者は、セキュリティ上問題があると思われる添付ファイルについて、送受信を制限できるようにしなければならない。

第５１条　電子メールの利用制限

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。

第2項

職員等は、複数の宛先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わからないようにしなければならない。

第3項

職員等は、重要な電子メールを誤送信した場合、情報管理者に報告しなければならない。

第4項

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。

第5項

職員等は、インターネットで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。ただし、業務上必要な場合は、ネットワーク管理者及び情報管理者の許可を得て利用することができる。

第５２条　電子署名・暗号化

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、最高情報統括責任者が定める電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

第2項

職員等は、暗号化を行う場合に最高情報統括責任者が定める以外の方法を用いてはならない。また、最高情報統括責任者が定める方法で暗号のための鍵を管理しなければならない。

第３節　アクセス制御

第５３条　利用者の識別及び認証

ネットワーク管理者及びシステム業務管理者は、所管するネットワーク又は情報システムに権限がない職員等がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。

第2項

ネットワーク管理者は、マイナンバー利用事務系では、パスワード、IC カード、生体認証等の認証手段のうち 2 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５４条　利用者ＩＤ等の管理

ネットワーク管理者及びシステム業務管理者は、所管する情報システムの利用者IDを適切に管理し、サーバ等へのログインに関して、不正なログインを防止するため、利用者IDの設定及びパスワードの設定等の対策を講じなければならない。

第５５条　管理者権限

情報統括管理者及びネットワーク管理者は、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。

第2項

情報統括管理者及びネットワーク管理者は、管理者権限等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。

第５６条　職員等による外部からのアクセス等の制限

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、ネットワーク管理者及び当該情報システムを管理する情報管理者の許可を得なければならない。

第2項

情報統括管理者は、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。

第3項

情報統括管理者は、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。

第4項

情報統括管理者は、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。

第5項

情報統括管理者及びネットワーク管理者は、外部からのアクセスに利用するパソコン等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。

第５７条　パスワードに関する情報の管理

ネットワーク管理者及びシステム業務管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、パスワード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パスワード設定のセキュリティ強化機能がある場合は、これを活用しなければならない。

第６章　情報システムの適正な運用

第１節　情報システムの開発、導入及び保守等

第５８条　情報システムの調達

ネットワーク管理者及びシステム業務管理者は、情報システムの調達にあたっては、調達に関する仕様書類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。

第2項

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。

第５９条　情報システムの開発等

ネットワーク管理者及びシステム業務管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、次の事項を定めるものとする。

第１号

責任者及び監督者

第 2 号

作業者及び作業範囲

第 3 号

開発するシステムと運用中のシステムとの分離

第 4 号

開発、保守に関する設計仕様等の成果物の提出

第 5 号

セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止

第 6 号

アクセス制限

第 7 号

機器の搬入出の際の許可及び確認

第 8 号

記録の提出義務

第 9 号

仕様書・マニュアル等の定められた場所への保管

第 10 号

情報システムに係るソースコードの適切な方法での保管

第 11 号

開発、保守を行った者の利用者ID、パスワード等の当該開発、保守終了後に不要となった時点での速やかな抹消

第 12 号

情報システムセキュリティ実施手順書等の整備

第2項

ネットワーク管理者及びシステム業務管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、不正にコピーしたソフトウェア及び個人所有のソフトウェアの導入又は使用等、問題のある行為が発生しないようにしなければならない。

第６０条　情報システムの移行

ネットワーク管理者及びシステム業務管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。また、移行の際、情報システムに記録されているデータ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。

第2項

ネットワーク管理者及びシステム業務管理者は、新たに情報システムを導入する際には、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。また、既存の情報システムを更新する際には、既に稼働している情報システムとの連携において、十分な試験を行わなければならない。

第3項

ネットワーク管理者及びシステム業務管理者は、テスト環境による動作確認後に情報システムの移行を行わなければならない。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

第4項

ネットワーク管理者及びシステム業務管理者は、原則として個人情報及び機密性の高いデータを試験データに使用してはならない。ただし、合理的な理由がある場合で、情報統括管理者及び情報責任者が許可した場合は、この限りでない。

第5項

ネットワーク管理者及びシステム業務管理者は、試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

第６１条　情報システムの入出力データ

ネットワーク管理者及びシステム業務管理者は、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必要に応じて組み込むよ

うに情報システムを設計しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、情報システムから出力されるデータは、保存された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。

第６２条　ソフトウェアの保守及び更新

ネットワーク管理者及びシステム業務管理者は、ソフトウェア等を更新、又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し、又は導入しなければならない。

第2項

ネットワーク管理者及びシステム業務管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかに対応を行わなければならない。

第６３条　情報システムの変更管理

ネットワーク管理者及びシステム業務管理者は、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。また、窃取、改ざん等をされないように適切に管理を行わなければならない。

第２節　外部サービスの利用

第６４条　外部委託に関する管理

ネットワーク管理者及びシステム業務管理者は、情報システムに関する企画、開発、保守、運用等及び電子計算機処理の一部又は全部を市以外の者に請け負わせる場合には、委託に係る契約書等に次に掲げる事項を必要に応じて明記しなければならない。

第１号

業務上知り得た情報の守秘義務に関する事項

第２号

再委託の禁止又は制限に関する事項

第３号

情報及び関連資料の第三者への提供の禁止並びに目的外の使用の禁止に関する事項

第 4 号

情報及び関連資料の取扱者の限定並びに複写及び複製の禁止に関する事項

第 5 号

記録媒体及び端末の取扱いに関する事項

第 6 号

事故発生時の報告義務及び立入調査に応ずる義務

第 7 号

契約に違反した場合における契約の解除及び損害賠償に関する事項

第 8 号

委託業務終了時の情報及び関連資料の返還、廃棄等に関する事項

第2項

前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

第 1 号

提供されるサービスレベルの保証に関する事項

第 2 号

外部委託事業者の従業員に対する研修の実施に関する事項

第 3 号

外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

第 4 号

委託業務の定期報告及び緊急時報告義務に関する事項

第 5 号

外部施設等への搬送時における盗聴、不正コピー等の防止に関する事項

第3項

ネットワーク管理者及びシステム業務管理者は、外部委託事業者のセキュリティ確保への取組状況、情報セキュリティマネジメントシステムに係る認証取得の状況、個人情報保護に関する取組状況の調査を行うとともに、契約締結後においても、定期的に又は随時、調査を行い、安全の確保に努めなければならない。

第６５条　外部サービス利用に関する管理

ネットワーク管理者及びシステム業務管理者は、ネットワークを使用した外部サービスを利用する場合には、次に掲げる事項に留意し、外部サービス提供者の選定を行い、契約を締結しなければならない。

第１号

外部サービスで取り扱う情報の分類及び取扱制限を踏まえ、外部サービス提供者を選定すること。また、以下の内容を外部サービス提供者の選定条件に含めること。

(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

(ウ)外部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とれること

(エ)サービス利用時に取り扱う情報に対する国内法以外の法令及び規制の適用リスクの評価

(オ)サービス利用時に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及び裁判管轄

(カ)一部再委託する場合、再委託先に対する契約に定める情報セキュリティ要件の実施担保並びに本市への実施状況の提供及び承認

第２号

外部サービスの特性を考慮した上で、外部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、情報セキュリティに関する役割及び責任の範囲を踏まえ、次の内容を含むセキュリティ要件を定め、契約事項に含むこと。

(ア)外部サービス利用に必要な教育

(イ)取り扱う資産の管理

(ウ)不正アクセスを防止するためのアクセス制御

(エ)取り扱う情報の機密性保護のための暗号化

(オ)外部サービス内の通信の制御
(カ)設計又は設定時の誤りの防止
(キ)外部サービスを利用した情報システムの事業継続
(ク)サービス利用契約終了時の情報資産の返還、廃棄等
(ケ)外部サービス提供業務の定期報告及び緊急時報告義務
(コ)損害賠償請求に関する事項

第2項

ネットワーク管理者及びシステム業務管理者は、外部サービス提供事業者のセキュリティ確保への取組状況、情報セキュリティマネジメントシステムに係る認証取得の状況及び個人情報保護に関する取組状況の調査を行うとともに、契約締結後においても、定期的に又は随時に調査を行い、安全の確保に努めなければならない。

第６６条　ソーシャルメディアサービスの利用

情報管理者は、業務のために市の公式アカウントを取得し、ソーシャルメディア（以下「SMS」という。）を運用しようとする場合は、あらかじめ運用手順等を定め、最高情報統括責任者の承認を得なければならない。

第2項

情報管理者は、本市のアカウントによる発信が、実際の本市のものであることを明らかにするために、アカウントの運用組織を明示する等の方法でなりすまし対策を行わなければならない。

第3項

情報管理者は、重要性分類Ⅰ及びⅡの情報をSMSで発信してはならない。

第4項

情報管理者は、アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じるとともに、第 21 条の規定によるセキュリティ事故に対する報告を行わなければならない。

第３節　不正プログラム及び不正アクセス対策

第６７条　コンピュータウイルス等の不正プログラム対策

ネットワーク管理者及びシステム業務管理者は、不正プログラム対策として、次の事項を実施しな

ければならない。

第１号

外部ネットワーク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、不正プログラムによるシステムへの侵入を防止すること。

第２号

所管するサーバ及び端末において、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、常に最新の状態を保つこと。

第３号

ネットワークに接続していないシステムにおいても、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定義ファイルの更新を実施すること。

第４号

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を行うこと。

第５号

開発元のサポートが終了したソフトウェアを利用しないこと。

第６８条　専門家の支援体制

情報統括管理者は、実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え、コンピュータウイルス等対策ソフトのサポート契約を締結する等、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。

第６９条　不正アクセス対策

情報統括管理者は、不正なアクセスによる影響を防止するため、次の事項を実施しなければならない。

第１号

使用されていないポートを閉鎖すること。

第２号

不要なサービスについて、機能を削除又は停止すること。

第 3 号

ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用すること。

第2項

最高情報統括責任者及び情報統括管理者は、攻撃の予告などサーバ等に不正アクセスを受けることが明白な場合には、システムの停止、他のネットワークとの切断等の必要な措置を講じなければならない。また、警察・関係機関との連絡を密にして情報の収集に努めなければならない。

第3項

最高情報統括責任者及び情報統括管理者は、不正アクセス行為の禁止等に関する法律違反など、犯罪の可能性がある不正アクセスを受けた場合、不正アクセスの記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

第4項

ネットワーク管理者及びシステム業務管理者は、職員等及び外部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不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

第5項

ネットワーク管理者及びシステム業務管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報管理者に通知し、適切な処置を求めなければならない。

第6項

ネットワーク管理者及びシステム業務管理者は、情報システムにおいて、標的型攻撃による庁内への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。

第７０条　セキュリティ情報の収集

情報統括管理者は、セキュリティホール等の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、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。

第７１条　情報システムの監視

情報統括管理者及びネットワーク管理者は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

第2項

情報統括管理者及びネットワーク管理者は、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又はサーバ間の時刻同期ができる措置を施さなければならない。

第3項

情報統括管理者及びネットワーク管理者は、外部と接続するシステムを稼働中、常時監視しなければならない。

第４節　情報セキュリティの遵守状況の確認及び対処

第７２条　情報セキュリティの遵守状況の確認及び対処

情報統括管理者及びネットワーク管理者は、情報セキュリティ対策基準の遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報統括責任者及び情報管理者に報告しなければならない。

第2項

最高情報統括責任者は、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。

第７３条　端末及び記録媒体等の利用状況調査

最高情報統括責任者及び最高情報統括責任者が指名した者は、情報漏えい、不正アクセス、コンピュータウイルス等の調査のために、パソコン等の端末、記録媒体、アクセス記録及びメール等の利用状況を調査することができる。

第７４条　職員等の報告義務

職員等は、情報セキュリティ対策基準に対する違反行為を発見した場合、直ちに情報管理者又はシステム業務管理者を通して情報統括管理者及びネットワーク管理者に報告を行わなければならない。

第2項

情報統括管理者は、前項の違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性が

あると判断した場合は、最高情報統括責任者に報告するとともに、次条に規定する緊急時対応計画に従って適切に対処しなければならない。

第７章　情報セキュリティの脅威に対する緊急時の対応

第１節　緊急時対応計画の策定

第７５条　緊急時対応計画の策定

ネットワーク管理者及びシステム業務管理者は、情報資産への重大な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、緊急時対応計画を策定しなければならない。

第７６条　緊急時対応計画に盛り込むべき内容

前条に規定する緊急時対応計画には、次の内容を定めなければならない。

第１号

関係者の連絡先

第２号

発生した事案に係る報告すべき事項

第３号

発生した事案への対応措置

第４号

再発防止措置の策定

第７７条　緊急時対応計画の見直し

ネットワーク管理者及びシステム業務管理者は、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に応じ、必要に応じて緊急時対応計画を見直さなければならない。

第７８条　例外措置の許可

ネットワーク管理者及びシステム業務管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守

事項を実施しないことについて合理的な理由がある場合には、最高情報統括責任者の許可を得て、例外措置を取ることができる。なお、ネットワーク管理者及びシステム業務管理者が、軽微な例外措置と判断したものについては、情報統括管理者の許可をもって、例外措置を取ることができる。

第2項

ネットワーク管理者及びシステム業務管理者は、前項に該当する場合であって、行政事務の遂行に緊急を要し、前項に定める許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかに最高情報統括責任者及び情報統括管理者に報告しなければならない。

第3項

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

第２節　違反に対する対応

第７９条　法令の遵守

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、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。

第１号

地方公務員法（昭和25年法律第261号）

第２号

著作権法（昭和45年法律第48号）

第３号

不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

第４号

個人情報の保護に関する法律（平成15年法律第57号）

第５号

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

27号）

第 6 号

サイバーセキュリティ基本法（平成 28 年法律第 31 号）

第 7 号

亀岡市個人情報保護条例（平成12年亀岡市条例第37号）

第８０条　違反時の対応

職員等に情報セキュリティ対策基準に違反する行為がみられた場合には、ネットワーク管理者及び情報管理者は、速やかに次の措置を講じなければならない。

第 1 号

情報統括管理者に報告するとともに、当該職員等に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

第 2 号

指導等によっても改善されない場合、情報統括管理者は、当該職員等の情報資産の使用権を停止又は剥奪することができる。

第 3 号

情報統括管理者は、職員等の情報資産の使用権を停止又は剥奪した旨を速やかに最高情報統括責任者及び当該職員等が所属する課室等の情報管理者に通知しなければならない。

第８章　情報セキュリティ対策の評価及び見直し

第１節　監査

第８１条　監査の実施

最高情報統括責任者は、情報統括管理者に命じ、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、必要に応じて監査を行わせなければならない。

第８２条　監査を行う者の要件

情報統括管理者は、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。

第2項

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。

第８３条　監査実施計画の策定及び実施への協力

情報統括管理者は、監査を行うにあたっては、監査実施計画を策定し、情報化推進委員会に報告しなければならない。

第2項

被監査部門は、監査の実施に協力しなければならない。

第８４条　外部委託事業者に対する監査

情報統括管理者は、外部委託事業者に対して、委託先事業者からの再委託の事業者も含めて、情報セキュリティ対策基準の遵守について、必要に応じて監査を行わなければならない。

第８５条　監査結果の報告及び監査書類の保管

情報統括管理者は、監査結果を取りまとめ、情報化推進委員会に報告する。

第2項

情報統括管理者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

第８６条　指摘事項への対処

最高情報統括責任者は、監査結果を踏まえ、指摘事項に関係する情報責任者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報責任者等に対しても、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。

第2項

最高情報統括責任者は、情報セキュリティ対策基準の見直しその他情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

第２節　自己点検

第８７条　自己点検の実施

ネットワーク管理者及びシステム業務管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、必要に応じて自己点検を実施しなければならない。

第2項

情報責任者は、所管する部等の情報セキュリティ対策状況について、必要に応じて自己点検を行わなければならない。

第８８条　自己点検結果等の報告

ネットワーク管理者、システム業務管理者及び情報責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報統括管理者に報告しなければならない。

第2項

情報統括管理者は、報告を受けた点検結果及び改善策を最高情報統括責任者に報告したうえで、情報化推進委員会に報告しなければならない。

第８９条　自己点検結果の活用

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。

第2項

最高情報統括責任者は、情報セキュリティ対策基準の見直しその他情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

第３節　改善及び見直し

第９０条　改善の措置

ネットワーク管理者、システム業務管理者及び情報責任者は、業務上発見された問題、住民からの指摘による問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を講じなければならない。

第2項

ネットワーク管理者、システム業務管理者及び情報責任者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティ事件・事故、監査及び自己点検において指摘されうる問題

等の発生を未然に防止するため、その原因を除去するための措置を講じなければならない。

第９１条　情報セキュリティ対策基準の見直し

最高情報統括責任者は、情報セキュリティ対策基準について、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、必要があると認めた場合、改善を行うものとする。

第９章　雑則

第９２条　委任

この規程に定めるもののほか、この規程の施行に関し必要な事項は、最高情報統括責任者が別に定める。