西尾市情報セキュリティポリシー

西尾市ＤＸ推進本部

西尾市情報セキュリティ基本方針

１ 目的

本市が所管する情報資産には最重要情報である個人情報をはじめ、行政運営において重要かつ必要不可欠な情報が数多く含まれる。この基本方針は、これらの情報を取り扱う上で発生する可能性がある様々な脅威から市民の財産、プライバシー等を守るとともに、継続的に、かつ、安定した行政運営に取り組むために、本市の情報セキュリティに関し基本的な方針を定めるものとする。

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

本基本方針及び情報セキュリティ対策基準をいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）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。

（９）LGWAN 接続系

財務会計システム等 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。

（１０）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１）通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保さ

れた通信だけを許可できるようにすることをいう。

（１２）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３ 対象とする脅威

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

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

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、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）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

４ 適用範囲

（１）情報資産の範囲

本基本方針では本市が所管するすべての情報資産のうち、以下のものを対象とする。

①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

（２）対象者

本市が所管する情報資産を取り扱う以下の者（ 以下「職員等」という。） を対象とする。

① 常勤の特別職及び教育長

② 西尾市職員定数条例（昭和 39 年 3 月 21 日条例第 27 号）第 2 条の別表に掲げる職員

③ 会計年度任用職員及び再任用短時間勤務職員

④ 県費負担職員

５ 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー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、以下の情報セキュリティ対策を講じる。

（１）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本市の保有する情報資産を機密性、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実施する。

（３）情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

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

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

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）物理的セキュリティ

サーバ等（サーバ、ファイアウォール等の情報システムの主要機器をいう。以下同じ。）、サーバ室、ネットワーク及び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ものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつに対応するため、緊急時対応計画を策定する。

（８）外部サービスの利用

外部委託する場合には、外部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、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

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を検証するため、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ため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

９ 情報セキュリティ対策基準の策定

６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

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。

１０ 情報セキュリティ実施手順の策定

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

附　則

この基本方針は、平成２６年　４月　１日から施行する。

附　則

この基本方針は、平成２８年　１月　１日から施行する。

附　則

この基本方針は、平成２８年　４月　１日から施行する。

附　則

この基本方針は、平成３１年　１月　１日から施行する。

附　則

この基本方針は、令和　２年　４月　１日から施行する。

附　則

この基本方針は、令和　２年１１月１８日から施行する。

西尾市情報セキュリティ対策基準

1. 目的

この西尾市情報セキュリティ対策基準は、西尾市情報セキュリティ基本方針に基づき、情報セキュリティ対策を講ずるにあたり遵守すべき行為及び判断等の基準を統一的に定めるため、必要な基本的要件を定めるものとする。

2. 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。）及び最高情報統括責任者（CIO：Chief Information Officer）

①副市長（総合政策部担当）をCISO兼CIOとする。ただし、副市長に事故があるときは、市長がその職務を代理する。

②CISOは、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

③CIO は、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関することを統括する。

④CISOは、情報セキュリティインシデントに対処するための体制（CSIRT：ComputerSecurity 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総合政策部長をCISO兼CIO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兼CIO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、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

③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必要かつ十分な措置を実施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、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

（３）情報セキュリティ責任者

①部局長（相当する職員含む。以下同じ）、会計管理者、教育長、消防長及び市民病院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、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見

の集約並びに職員及び会計年度任用職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

⑤情報セキュリティ責任者は、その所管する部局等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、CISO 及び統括情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（４）情報セキュリティ管理者

①課室長（相当する職員含む。以下同じ）、小中学校における校長及び市民病院における事務部以外の各部門長等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、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

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

④情報セキュリティ管理者は、その所管する課室等の職員等に、情報セキュリティポリシー及び実施手順について守るべき内容を理解させ、また実施及び遵守させなければならない。

（５）情報システム管理者

①各情報システムの担当課室長等を、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、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、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、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策定・管理を行う。

（６）西尾市ＤＸ推進本部

本市の情報セキュリティ対策を統一的に行うため、西尾市ＤＸ推進本部において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

（７）CSIRT の設置・役割

①情報政策課を CSIRT とし、統括情報セキュリティ責任者を CSIRT 責任者とする。

②CSIRT は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備すること。

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

④CSIRT は、情報セキュリティインシデントを認知した場合には、必要に応じて CISO、総務省、都道府県等へ報告すること。

⑤情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を当該部門及び広報部門と連携し行わなければならない。

⑥CSIRT は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行うこと。

⑦CSIRT は、「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施行令」第 23 条第 2 項の体制に該当し、特定個人情報の情報漏えい事案が発生した場合に、被害の拡大防止、原因究明、個人情報保護委員会への報告等の対応を行うこと。

3. 情報資産の分類と管理

（１）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性２	行政事務で取り扱う情報資産のうち、個人情報を含む情報資産及び秘密文書に相当する機密性を要する情報資産	・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性１	機密性２以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
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、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資産	・バックアップの義務付け ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産の	・バックアップの義務付け

	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、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資産	・電磁的記録媒体の施錠可能な場所への保管 ・業務継続が可能となる代替機材の設置などによる冗長化の義務付け
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、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。

③情報資産の利用

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

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

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

④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、情報資産を適正に保管しなければならない。

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

（ウ）情報セキュリティ管理者及び情報システム管理者は、機密性２の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に施錠して保管しなければならない。

⑤情報の送信

電子メール~~等~~により機密性２の情報を送信する者は、機密性２の情報を本文ではなく添付ファイルで行なわなければならない。この場合、添付ファイルは暗号化を行わなければならない。

⑥情報資産の運搬

（ア）車両等により機密性２の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、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）機密性２の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑦情報資産の提供・公表

（ア）機密性２の情報資産を外部に提供する者は、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）機密性２の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（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。

⑧情報資産の廃棄

（ア）情報資産を廃棄する者は、情報を復元できないように処置した上で廃棄しなければならない。

（イ）情報資産の廃棄を行う者は、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。

（ウ）情報資産の廃棄を行う者は、情報システム管理者の許可を得なければならない。

4. 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領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。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(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。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、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

（イ）情報の持ち出し不可設定

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

（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

（３）インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②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。

5. 物理的セキュリティ

5.1. 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正に固定する等、必要な措置を講じなければならない。

（２）機器の電源

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

②情報システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（３）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必要な措置を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、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。

（４）機器の定期保守及び修理

①情報システム管理者は、サーバ等の機器について外部事業者等と保守契約を締結しなければならない。

②情報システム管理者は、外部の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。

（５）市の施設以外への機器の設置

情報システム管理者は、市の施設以外に機密性２の情報を含むサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（６）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。

5.1.　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、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（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、施錠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情報システム管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

④情報システム管理者は、必要に応じて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。

（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、入退室管理簿の記載等による入退室管理を行わなければならない。

②職員等及び外部委託事業者は、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。

（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。

5.1　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、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。

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

③情報システム管理者は、機密性２の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

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、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。

5.4. 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等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②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、スマートカード、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、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

6. 人的セキュリティ

6.1. 職員等の遵守事項

（１）職員等の遵守事項

①情報セキュリティポリシー等の遵守

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

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③パソコンやモバイル端末、電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア）職員等は、本市のパソコン、モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。ただし、在宅勤務の許可を所属長から得ている場合は、この限りではない。

（イ）職員等は、機密性２の情報資産について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。ただし、在宅勤務の許可を所属長から得ている場合は、この限りではない。

（ウ）情報セキュリティ管理者は、パソコン、モバイル端末、電磁的記録媒体等の持ち出しについて、記録を作成し、保管しなければならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を市所有の情報機器等に接続し、業務に利用してはならない。ただし、画面転送方式など情報システム管理者が特に認めた方式で、支給以外のパソコンを利用する場合はこの限りではない。

（イ）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合に

は、情報システム管理者の許可を得なければならない。ただし、画面転送方式など情報システム管理者が特に認めた方式で、支給以外のパソコンを利用する場合はこの限りではない。

（ウ）外部で情報処理作業を行う際には安全管理措置を遵守しなければならない。また、機密性２の情報資産については、支給以外のパソコンによる（画面転送方式など情報システム管理者が特に認めた方式は除く）情報処理を行ってはならない。

⑤パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報システム管理者の許可なく変更してはならない。

⑥机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑦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。

（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、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、会計年度任用職員の採用の際、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び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。

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

（４）外部委託事業者に対する説明

情報システム管理者は、情報システムの開発・保守等を外部委託事業者に発注する場合、外部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のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

6.2.　研修等

（１）研修の実施

①統括情報セキュリティ責任者は、幹部を含めすべての職員等に対する情報セキュリティに関する研修を定期的に実施しなければならない。

②統括情報セキュリティ責任者は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（２）緊急時対応訓練

情報システム管理者は、緊急時対応を想定した訓練を必要に応じて実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

（３）研修等への参加

幹部を含めた全ての職員等は、定められた研修等に参加しなければならない。

6.3. 情報セキュリティインシデントの報告

（１）庁内での情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び CSIRT 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、情報セキュリティ責任者、情報システム管理者に報告しなければならない。

③情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び統括情報セキュリティ責任者に報告しなければならない。

（２）住民等外部からの情報セキュリティインシデントの報告

①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ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、情報セキュリティ責任者、情報システム管理者及び CSIRT に報告しなければならない。

③情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び統括情報セキュリティ責任者に報告しなければならない。

（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

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

②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。

③CSIRT 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。

④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検

討し、CISO に報告しなければならない。

⑤CISO は、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。

6.4. ID 及びパスワード等の管理

（１）IC カード（IC チップを埋め込み、本人確認のための認証が可能なカード。以下同じ）の取扱い

①職員等は、管理する IC カードに関し、次の事項を遵守しなければならない。

（ア）業務上必要がないときは、IC カードをカードリーダ若しくはパソコン等のスロットから抜いておかなければならない。

（イ）IC カードを紛失した場合には、速やかに情報システム管理者に報告し、指示に従わなければならない。

②情報システム管理者は、IC カードの紛失等の通報があり次第、当該 IC カードを使用したアクセス等を速やかに停止しなければならない。

③情報システム管理者は、IC カードを切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

①自己が利用している ID は、他人に利用させてはならない。

②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

（３）パスワードの取扱い

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

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

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

⑤パソコン等にパスワードを記憶させてはならない。

7. 技術的セキュリティ

7.1. 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情報システム管理者は、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。

（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、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

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。

（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、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することや紛失等がないよう、適正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、必要に応じて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、取得したログを必要に応じて、悪意ある第三者からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（６）障害記録

情報システム管理者は、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（７）ネットワークの接続制御、経路制御等

①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、ルータ等の通信ソフトウェア等を設定しなければならない。

②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。

（８）外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、ネットワークを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、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者は、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。

③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、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。

④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）複合機のセキュリティ管理

①情報システム管理者は、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、適正なセキュリティ要件を策定しなければならない。

②情報システム管理者は、複合機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複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③情報システム管理者は、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又は再利用できないようにする対策を実施しなければならない。

（１１）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、IP 電話、ネットワークカメラ等の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実施しなければならない。

（１２）無線 LAN 及びネットワークの盗聴対策

①情報システム管理者は、ネットワークにおいて無線 LAN を使用する場合は、統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者は、無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

③情報システム管理者は、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。

（１３）電子メールのセキュリティ管理

①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しなければならない。

③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情報システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している外部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、外部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。

（１４）電子メール等の利用制限

①職員等は、自動転送機能を用いて、外部へ電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③職員等は、業務上必要のないサービスに電子メールを登録してはならない。

④職員等は、外部の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。

⑤職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑥職員等は、ウェブで利用できるフリーメールを使用してはならない。

⑦職員等は、ウェブで利用できるオンラインストレージサービスについて情報システム管理者の許可したもの以外、使用してはならない。

（１５）USB メモリ等の利用制限

①職員等は、情報システム管理者の許可なしに USB メモリ等の外部記憶媒体（以下「USB メモリ等」という。）を接続してはならない。

②情報漏えいを防ぐため、許可する USB メモリは暗号化等の機能を有したものでなければならない。

（１６）無許可ソフトウェアの導入等の禁止

①職員等は、パソコンやモバイル端末にソフトウェアを情報システム管理者の許可無く導入してはならない。許可を求められた情報システム管理者は導入するソフトウェアの保有又は使用できる権利等を確認しなければならない。

②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。

（１７）機器構成の変更の制限

職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を情報システム管理者の許可無く導入してはならない。

（１８）無許可でのネットワーク接続の禁止

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

（１９）クラウドサービス利用におけるアクセス回線の制限

情報システム管理者は、クラウドサービスを利用する場合は、そのアクセス回線について通信途上の盗聴を防御するための暗号化等の措置を講じなければならない。

（２０）業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

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

7.2. アクセス制御

（１）アクセス制御等

①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）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、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

（イ）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、点検しなければならない。

③特権を付与された ID の管理等

（ア）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等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

（イ）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、外部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 及びパスワードについて、その他の ID のパスワードよりも複雑なものにしなければならない。

（エ）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情報システム管理者は、職員等がインターネット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ことを許可してはならない。

②情報システム管理者は、インターネットから内部のネットワークへのアクセスを遮断するための措置を講じなければならない。

③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、システム上利用者の本人確認を行う機能を確保しなければならない。

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

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

⑥情報システム管理者は、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を禁止しなければならない。

（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システムの機能がある場合は設定しなければならない。

（４）認証情報の管理

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。

（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。

7.3. システム開発、導入、保守等

（１）情報システムの調達

①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。

（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。

②システム開発における責任者、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 を管理しなければならない。

（イ）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のアクセス権限を設定しなければならない。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）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。

（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、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

②テスト

（ア）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、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（４）システム開発・保守に関連する資料等の整備・保管

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

②情報システム管理者は、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、情報システムに係るソースコードを適正な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①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。

②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正し

く反映され、出力されるように情報システムを設計しなければならない。

（６）情報システムの変更管理

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。

（７）開発・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・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（８）システム更新又は統合時の検証等

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。

7.4. 不正プログラム対策

（１）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。

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に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

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

⑥不正プログラム対策のソフトウェアは、業務に支障が無い限り常に最新の状態に保たなければならない。

⑦インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

⑧業務で利用するソフトウェアは、業務に支障が出る場合を除きパッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（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。

②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、速やかに情報システム管理者に報告しなければならない。

③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。

④情報システム管理者が提供するウイルス情報を、常に確認しなければならない。

⑤コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、LANケーブルの即時取り外しを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わなければならない。

（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わなければならない。

（３）専門家の支援体制

情報システム管理者は、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。

7.5. 不正アクセス対策

（１）情報システム管理者の措置事項

情報システム管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報システム管理者へ通報するよう、設定しなければならない。

④情報システム管理者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（２）攻撃への対処

統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、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

統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（４）内部からの攻撃

情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）職員等による不正アクセス

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、当該職員等が所属する課室等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、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。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

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

（２）不正プログラム等のセキュリティ情報の収集・周知

情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（３）情報セキュリティに関する情報の収集及び共有

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や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

8. 運用

8.1. 情報システムの監視

①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しなければならない。

②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措置を講じなければならない。

③情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

8.2. 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適宜確認を行い、問題を認めた場合には、速やかに情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は必要に応じて CISO 及び統括情報セキュリティ責任者に報告し

なければならない。

②統括情報セキュリティ責任者は、発生した問題について、適正かつ速やかに対処しなければならない。

③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、定期的または必要に応じて確認を行い、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

CISO、統括情報セキュリティ責任者又は統括情報セキュリティ責任者が指名した者は、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、インターネットアクセス履歴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。報告を受けた情報セキュリティ管理者は必要に応じて情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は必要に応じて統括情報セキュリティ責任者に報告しなければならない。

②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

8.3. 侵害時の対応等

（１）緊急時対応計画の策定

統括情報セキュリティ責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、情報システム管理者に緊急時対応計画を定めさせなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（３）業務継続計画との整合性確保

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

（４）緊急時対応計画の見直し

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に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

8.4.　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 及び統括情報セキュリティ責任者の許可を得て、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等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。

（３）例外措置の申請書の管理

CISO 及び統括情報セキュリティ責任者は、例外措置の申請書及び審査結果を適正に保管しなければならない。

8.5.　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、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 12 月 13 日法律第 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 5 月 30 日法律第 57 号）

⑤西尾市個人情報の保護に関する法律施行条例（令和４年 12 月 26 日規則第 58 号）

⑥西尾市職員服務規程（昭和 36 年 5 月 1 日規程第 7 号）

⑦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 5 月 31 日法律 27 号)

⑧サイバーセキュリティ基本法（平成 28 年法律第 31 号）

8.6.　違反時の対応

（１）違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪す

ることができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

9. 外部サービスの利用

9.1. 外部委託

（１）外部委託事業者の選定基準

委託契約等を行う情報システム管理者又は情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（２）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、外部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
・外部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
・外部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守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（３）確認・措置等

情報システム管理者又は情報セキュリティ管理者は、外部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必要に応じて確認しなければならない。

9.2 約款による外部サービスの利用

（１）約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

9.3 ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするため

に、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

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

②機密性２の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

9.4　クラウドサービス利用

①情報セキュリティ管理者は、クラウドサービス（民間事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、機密性２以上の情報を取り扱うサービスを利用する場合は、不正なアクセスを防止するためのアクセス制御（２要素認証による認証、IP アドレス制限等）や通信の暗号化により情報を保護しなければならない。

②情報セキュリティ管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

③情報セキュリティ管理者は、クラウドサービス利用が終了した際には、外部サービスで取り扱った情報が適切に廃棄されたことをクラウドサービス提供者に確認しなければならない。

10.　評価・見直し

10.1.　監査

（１）実施方法

統括情報セキュリティ責任者は、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なければならない。

（２）監査実施計画の立案及び実施への協力

①統括情報セキュリティ責任者は、監査を行うに当たって、監査実施計画を作成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。

（３）外部委託事業者に対する監査

外部委託事業者に委託している場合、委託契約等を行う情報システム管理者又は情報セキュリティ管理者は外部事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

（４）報告

統括情報セキュリティ責任者は、監査結果を取りまとめ、必要に応じて西尾市ＤＸ推進本部に報告しなければならない。

（５）保管

統括情報セキュリティ責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、一定の期間適正に保管しなければならない。

（６）監査結果への対応

統括情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報システム管理者または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システム管理者または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。

（７）情報セキュリティポリシー及び関係規定等の見直し等への活用

西尾市ＤＸ推進本部は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

10.2.　自己点検

（１）実施方法

①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、必要に応じて自己点検を行わなければならない。

②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、必要に応じて自己点検を実施しなければならない。

（２）報告

情報セキュリティ責任者及び情報システム管理者は、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統括情報セキュリティ責任者に報告しなければならない。統括情報セキュリティ責任者は、必要に応じて西尾市ＤＸ推進本部に報告しなければならない。

（３）自己点検結果の活用

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

②西尾市ＤＸ推進本部は、この点検結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

10.3.　情報セキュリティポリシー及び関係規定等の見直し

西尾市ＤＸ推進本部は、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ふまえ、情報セキュリティポリシー及び関係規定等について毎年度または必要に応じて評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

この対策基準は、平成２６年　４月　１日から施行する。

附　則

この対策基準は、平成２８年　１月　１日から施行する。

附　則

この対策基準は、平成２９年　１月　１日から施行する。

附　則

この対策基準は、平成２９年　１０月　１日から施行する。

附　則

この対策基準は、平成３１年　１月　１日から施行する。

附　則

この対策基準は、平成３１年　４月　１日から施行する。

附　則

この対策基準は、令和　２年　４月　１日から施行する。

附　則

この対策基準は、令和　２年１１月１８日から施行する。

附　則

この対策基準は、令和　３年　２月１５日から施行する。

附　則

この対策基準は、令和　４年　４月　１日から施行する。

附　則

この対策基準は、令和　５年　４月　１日から施行する。