和歌山市情報セキュリティポリシー

目次

和歌山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

本基本方針及び情報セキュリティ対策基準において、使用する用語の意義は、個人情報の保護に関する法律（平成１５年法律第５７号）及び和歌山市情報公開条例（平成５年条例第３３号）で使用する用語の例によるほか、次の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）情報セキュリティインシデント

情報セキュリティ事故及び事故にいたる可能性も含めた情報セキュリティを脅かす事象をいう。

（９）個人番号利用等事務系

個人番号利用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。

（１０）ＬGWAN接続系

ＬGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（個人番号利用等事務系を除く。）。

（１１）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。

（１２）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。

（１３）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、部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊、消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

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

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

４　適用範囲

（1）行政機関の範囲

情報セキュリティポリシーが適用される行政機関は、本市の全ての実施機関とする。

（2）情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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。）

ウ　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

エ　紙書類やデータなどの状態、記録媒体に限らず、組織内にある全ての情報

５　職員の遵守義務

情報資産に接する全ての職員は、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

前記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）情報資産の分類及び管理

本市の保有する情報資産を「重要情報」及び「重要情報以外の情報」に分類し、当該分類

に基づき情報セキュリティ対策を実施する。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

ア　個人番号利用等事務系においては、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。

イ　ＬＧＷＡＮ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。

ウ　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、自治体情報セキュリティクラウドの導入等を実施する。

（4）物理的セキュリティ

サーバ、情報システム設置区画、通信回線、職員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、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。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正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

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。

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、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。

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改定する。

９　情報セキュリティ対策基準の策定

前記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

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。

附　則（平成１５年８月１日）

この基本方針は、平成１５年８月１日から施行する。

附　則（平成２９年２月２４日）

この基本方針は、平成２９年２月２４日から施行する。

附　則（平成３１年４月１日）

この基本方針は、平成３１年４月１日から施行する。

附　則（令和３年７月１日）

この基本方針は、令和３年７月１日から施行する。

附　則（令和５年４月１日）

この基本方針は、令和５年４月１日から施行する。

和歌山市情報セキュリティ対策基準

1　組織体制

別紙１に定める。以下に主たる役割を示す。

（1）情報セキュリティ統括責任者

ア　情報セキュリティ統括責任者は、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。

イ　情報セキュリティ統括責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

ウ　情報セキュリティ統括責任者は、情報セキュリティインシデントに対処するための体制を整備し、役割を明確化する。

エ　情報セキュリティ統括責任者は、情報セキュリティポリシーに定められた自らの担務を、情報セキュリティポリシーに定める責任者に担わせることができる。

（2）情報セキュリティ執行責任者

ア　情報セキュリティ執行責任者は、情報セキュリティ統括責任者を補佐しなければならない。

イ　情報セキュリティ執行責任者は、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。

ウ　情報セキュリティ執行責任者は、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。

エ　情報セキュリティ執行責任者は、情報セキュリティ責任者、情報セキュリティ管理者、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。

オ　情報セキュリティ執行責任者は、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、情報セキュリティ統括責任者の指示に従い、情報セキュリティ統括責任者及び副統括責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

カ　情報セキュリティ執行責任者は、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及び管理を行う権限並びに責任を有する。

キ　情報セキュリティ執行責任者は、緊急時等の円滑な情報共有を図るため、情報セキュリティ統括責任者、情報セキュリティ執行責任者、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。

ク　情報セキュリティ執行責任者は、緊急時には情報セキュリティ統括責任者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。

ケ　情報セキュリティ執行責任者は、情報セキュリティに関する規程等に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて情報セキュリティ統括責任者にその内容を報告しなければならない。

（3）情報セキュリティ責任者

ア　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。

イ　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。

ウ　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に対する教育、訓練、助言及び指示を行う。

（4）情報セキュリティ管理者

ア　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。

イ　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、情報セキュリティ執行責任者及び情報セキュリティ統括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。

（5）情報システム管理者

ア　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。

イ　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。

ウ　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維持及び管理を行う。

（6）情報システム担当者

情報システム管理者が指名し、その指示等に従い、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。

（7）情報セキュリティ委員会

ア　本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシーの改定等、情報セキュリティに関する重要な事項を決定する。

イ　情報セキュリティ委員会は、必要に応じ、本市における情報セキュリティ対策の改善計画を策定する。

（8）兼務の禁止

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

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

（9）情報セキュリティに関する統一的な窓口の設置

ア　情報セキュリティ統括責任者は、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組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

イ　情報セキュリティ統括責任者による情報セキュリティ戦略の意思決定が行われた際に

は、その内容を関係部局等に提供しなければならない。

ウ　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、影響範囲等を勘案し、情報セキュリティ統括責任者、総務省、個人情報保護委員会、和歌山県等適切な報告先へ報告しなければならない。

エ　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、影響範囲等を勘案し、報道機関への通知、公表対応を行わなければならない。

オ　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組織は、情報セキュリティに関して、関係機関、委託事業者等との情報共有を行わなければならない。

2　情報資産の分類及び管理方法

（1）情報資産の分類

本市における情報資産は、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、必要に応じ別紙２を参考に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資産
	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資産
	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資産
	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資産
重要情報以外の情報	①～④のいずれにも該当しない情報資産

（2）情報資産の管理

ア　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。

（ウ）情報セキュリティ管理者は、「重要情報」に分類される情報資産（以下「重要情報資産」という。）を取り扱う事務を実施する区域（以下「取扱区域」という。）においては、適正な管理を行わなければならない。

イ　情報資産の分類の表示

職員は、情報資産について、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、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

ウ　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、当該情報の分類及び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、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。

エ　情報資産の入手

（ア）職員は、業務上必要のない情報を入手してはならない。

（イ）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。

（ウ）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、当該情報の分類及び取扱制限を定めなければならない。

（エ）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がなければならない。

オ　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閲覧又は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、当該情報資産に「重要情報」及び「重要情報以外の情報」が混在して記録されている場合、「重要情報資産」として、当該情報資産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、「重要情報資産」を複製及び配布を行ってはならない。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複製及び配布することができる。

カ　情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）情報セキュリティ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、利用頻度が低い電磁的記録媒体及び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、必要に応じ、自然災害を被る可能性が低い地域に保管しなければならない。

（エ）情報セキュリティ管理者又は情報システム管理者は、「重要情報資産」を保管する場合、必要に応じ、耐火、耐熱、耐水、耐湿等を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

電子メール等により「重要情報」を外部へ送信してはならない。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送信することができる。送信時は、パスワード等による暗号化を行わなければならない。

ク　情報資産の運搬

（ア）車両等により「重要情報資産」を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）「重要情報資産」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。

ケ　情報資産の提供及び公表

（ア）「重要情報資産」を外部に提供する者は、必要に応じパスワード等による暗号化等の対策を行わなければならない。

（イ）「重要情報資産」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。

コ　情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、当該情報の情報資産分類に応じた方法により、電磁的記録媒体の情報を復元できないように処置しなければならない。

（イ）「重要情報資産」の廃棄を行う者は、情報セキュリティ管理者の許可を得た上で廃棄を行い、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。

3　情報システム全体の強靭性の向上

（1）個人番号利用等事務系

ア　個人番号利用等事務系と他の領域との分離

個人番号利用等事務系と他の領域を通信できないようにしなければならない。個人番号利用等事務系と外部との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、インターネット等と個人番号利用事務系との双方向通信でのデータ移送を可能とする。

イ　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

ア　ＬGWAN接続系とインターネット接続系の分割

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

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

（イ）インターネット接続系の端末から、ＬGWAN接続系の端末へ画面を転送する方式

（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

（3）インターネット接続系

ア　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。

イ　県内市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、関係省庁や和歌山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。

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正に固定する等、必要な措置を講じるように努めなければならない。

（2）サーバの冗長化

ア　情報システム管理者は、「重要情報」を格納しているサーバ等を冗長化し、同一データを保持しなければならない。

イ　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は、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

ア　情報システム管理者は、情報セキュリティ執行責任者及び施設管理部門と連携し、停止することで業務に多大な影響を与えるシステム等を扱う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。

イ　情報システム管理者は、情報セキュリティ執行責任者及び施設管理部門と連携し、落雷等による過電流に対して、停止することで業務に多大な影響を与えるシステム等を扱う機器を保護するため、必要な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　情報セキュリティ執行責任者及び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るよう努めなければならない。

イ　情報セキュリティ執行責任者及び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。

ウ　情報セキュリティ執行責任者及び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な管理に努めなければならない。

エ　情報セキュリティ執行責任者及び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、追加できないよう必要な措置を講じるよう努めなければならない。

（5）機器の定期保守及び修理

ア　情報システム管理者は、「重要情報」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。

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、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）庁外への機器の設置

情報システム管理者は、庁外にサーバ等の「重要情報」を扱う機器を設置する場合、情報セキュリティ執行責任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。

（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、当該機器の記憶装置に保存されている情報の情報資産分類に応じた方法により、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。また、機器の廃棄等を外部委託する際において、事業者にて情報を消去する旨を契約に明記し、消去したことの証明を書面で提出させなければならない。

4．2　管理区域（情報システム設置区画等）の管理

（1）管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための区画（以下「情報システム設置区画」という。）並びにその他情報資産の保管庫をいう。

イ　情報セキュリティ執行責任者及び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するよう努めなければならない。

ウ　情報セキュリティ執行責任者及び情報システム管理者は、情報システム設置区画内の機

器等に、転倒、落下防止等の耐震対策、防火措置、防水措置等を講じるよう努めなければならない。

エ　情報セキュリティ執行責任者及び情報システム管理者は、管理区域に配置する消火薬剤、消防用設備等が、機器等、情報資産に影響を与えないようにしなければならない。

（2）管理区域の入退管理等

ア　情報システム管理者は、管理区域への入退を許可された者のみに制限し、入退を管理しなければならない。

イ　職員及び委託事業者は、管理区域に入る場合、本人確認書類等を携帯し、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、外部からの訪問者が管理区域に入る場合には、必要に応じ、立ち入り区域を制限した上で、管理区域への入退を許可された職員が確認し、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、「重要情報」を扱うシステムを設置している管理区域について、当該情報システムに関連しない、また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、電磁的記録媒体等の持込みの管理に努めなければならない。

（3）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事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、情報システム設置区画の機器等の搬入出について、職員を立ち会わせなければならない。

４．３　通信回線及び通信回線装置の管理

（1）情報セキュリティ執行責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

（2）情報セキュリティ執行責任者は、外部へのネットワーク接続を必要最低限に限定し、出来る限り接続ポイントを減らさなければならない。

（3）情報セキュリティ執行責任者は、「重要情報」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）情報セキュリティ執行責任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）情報セキュリティ執行責任者は、「重要情報」を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

４．４　職員の利用する端末、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、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理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、個人番号利用等事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

（4）情報システム管理者は、パソコン、モバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

（5）情報システム管理者は、モバイル端末の庁外での業務利用の際は、前記対策に加え、紛失・盗難時にデータを保護することができる措置を講じなければならない。

5　人的セキュリティ

5．1　職員の遵守事項

（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　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）情報セキュリティ統括責任者は、「重要情報資産」を外部で処理する場合における安全確保のための適切な措置を講じなければならない。また、その継続的改善に努めなければならない。

（イ）職員は、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。

エ　貸与以外のパソコン、モバイル端末、電磁的記録媒体等の業務利用

（ア）職員は、貸与以外のパソコン、モバイル端末、電磁的記録媒体等を原則業務に利用してはならない。ただし、重要情報資産を扱わない業務に限り、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）職員は、貸与以外のパソコン、モバイル端末、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、安全確保のための適切な取扱いを行わなければならない。

オ　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。

カ　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

職員は、パソコン及び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セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

職員は、パソコン、モバイル端末、電磁的記録媒体、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、離席時のパソコン及びモバイル端末のロック並びに電磁的記録媒体、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。

ク　退職時等の遵守事項

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

ケ　情報セキュリティポリシーの遵守状況の確認

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５．３（１）に則り報告しなければならない。

（2）非常勤及び臨時職員等への対応

ア　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、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等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。

イ　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、非常勤及び臨時職員等の採用の際、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同意書への署名を求めるものとする。

ウ　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、非常勤及び臨時職員等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、保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

５．２　研修及び訓練

（1）情報セキュリティに関する研修及び訓練

情報セキュリティ統括責任者は、定期的に情報セキュリティに関する研修及び訓練を実施

しなければならない。

（2）研修計画の策定及び実施

ア　情報セキュリティ統括責任者は、全ての職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を行わなければならない。

イ　研修計画において、情報セキュリティ研修を年に１回以上実施するようにしなければならない。

ウ　新規採用の職員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。

エ　研修は、情報セキュリティ執行責任者、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、情報システム担当者及びその他職員に対して、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。

オ　情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、情報セキュリティ執行責任者に対して、報告しなければならない。

カ　情報セキュリティ統括責任者は、職員の情報セキュリティ研修の実施状況について把握しなければならない。

キ　情報セキュリティ管理者は、所属する職員に対して、研修への参加の機会を確保できるよう配慮する等必要な措置を講じなければならない。

（3）緊急時対応訓練

情報セキュリティ統括責任者は、緊急時対応を想定した訓練を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）研修及び訓練への参加

幹部を含めた全ての職員は、定められた研修及び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

ア　職員は、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に対する違反並びにその兆候（以下「情報セキュリティインシデント等」という。）を認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口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、当該情報セキュリティインシデント等の内容、重要度、影響範囲等に応じ、情報セキュリティ執行責任者、情報セキュリティ責任者及び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、情報セキュリティ統括責任者及び情報セキュリティ委員会より報告を求められた場合は、これに応じなければならない。

（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

ア　職員は、本市が管理するネットワーク、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等について、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及び情報セキュリティに関する統一的な窓口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、当該情報セキュリティインシデント等の内容、

重要度、影響範囲等に応じ、情報セキュリティ執行責任者、情報セキュリティ責任者及び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、情報セキュリティ統括責任者及び情報セキュリティ委員会より報告を求められた場合は、これに応じなければならない。

（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　情報セキュリティに関する統一的な窓口は、報告された情報セキュリティインシデント等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。

（ア）当該事案が情報セキュリティインシデントと評価された場合、緊急時対応計画に則り、原因の究明、記録、再発防止等の対応を行わなければならない。

（イ）当該事案が情報セキュリティインシデントではないと評価されたが、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には、速やかに、情報セキュリティ執行責任者は当該職員が所属する課室等の情報セキュリティ管理者に、適正な措置を求めなければならない。

イ　前項の状況を踏まえ、情報セキュリティ統括責任者は、職員のネットワーク若しくは情報システムを使用する権利を停止又は剥奪することができる。その後速やかに、情報セキュリティ統括責任者は、職員の権利を停止又は剥奪した旨を当該職員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。

ただし、情報セキュリティインシデントに該当しない職員の情報セキュリティポリシー違反の場合は、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に限り、情報セキュリティ執行責任者の決定において行うことができる。

５．４　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）個人認証に用いるＩＣカード等を、職員間で共有してはならない。

（イ）業務上必要のないときは、ＩＣカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

（ウ）ＩＣカード等を紛失した場合には、速やかに情報セキュリティ執行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。

イ　情報セキュリティ執行責任者及び情報システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

ウ　情報セキュリティ執行責任者及び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、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、パスワードの照会等には一切応じてはならない。

ウ　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。

エ　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。

オ　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。

カ　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。

キ　サーバ、ネットワーク機器及びパソコン等の端末において、他人が容易に参照できるような状況の場所にパスワードを記録させてはならない。

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

6　技術的セキュリティ

6．1　コンピュータ及びネットワークの管理

（1）文書サーバの設定等

ア　情報システム管理者は、職員が使用できる文書サーバの容量を設定し、職員に周知しなければならない。

イ　情報システム管理者は、文書サーバを課室等の単位で構成し、職員が必要のない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。

ウ　情報システム管理者は、住民の個人情報、人事記録等、特定の職員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が閲覧及び使用できないようにしなければならない。

（2）バックアップの実施

情報セキュリティ執行責任者及び情報システム管理者は、文書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、定期的にバックアップを実施しなければならない。

（3）他団体との情報システムに関する情報等の交換

情報システム担当者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、情報システム管理者の許可を得なければならない。

（4）システム管理記録及び作業の確認

ア　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、必要な作業記録を作成しなければならない。

イ　情報セキュリティ執行責任者及び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正に管理しなければならない。

ウ　情報セキュリティ執行責任者、情報システム管理者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がシステム変更等の作業を行う場合は、必要に応じ、２名以上で作業し、互いにその作業を確認しなければならない。

（5）情報システム仕様書等の管理

情報セキュリティ執行責任者及び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、紛失等がないよう、適正に管理しなければならない。

（6）ログの取得等

ア　情報セキュリティ執行責任者及び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。

イ　情報セキュリティ執行責任者及び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　情報セキュリティ執行責任者及び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、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

なお、個人番号利用事務に関わる情報システムにおいては、定期に及び必要に応じ随時に分析等を実施しなければならない。

（7）障害記録

情報セキュリティ執行責任者及び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、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。

（8）ネットワークの接続制御、経路制御等

ア　情報セキュリティ執行責任者は、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。

イ　情報セキュリティ執行責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（9）外部の者が利用できるシステムの分離等

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、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（１０）外部ネットワークとの接続制限等

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には、情報セキュリティ執行責任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資産の漏えい、破壊、改ざん、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。なお、国等が用意する情報システムなど契約によらず利用する場合においては、当該国等との責任分界点を明確にしておかなければならない。

エ　情報セキュリティ執行責任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、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。

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には、情報セキュリティ執行責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（１１）複合機のセキュリティ管理

ア　情報セキュリティ執行責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　情報セキュリティ執行責任者は、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。

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

（１２）ＩｏＴ機器を含む特定用途機器のセキュリティ管理

情報セキュリティ執行責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１３）無線ＬＡＮ及びネットワークの盗聴対策

ア　情報セキュリティ執行責任者は、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。

イ　情報セキュリティ執行責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（１４）電子メールのセキュリティ管理

ア　情報セキュリティ執行責任者は、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。

イ　情報セキュリティ執行責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　情報セキュリティ執行責任者は、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。

エ　情報セキュリティ執行責任者は、職員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に周知しなければならない。

オ　情報セキュリティ執行責任者は、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。

カ　情報セキュリティ執行責任者は、職員の電子メールの送信等による情報資産の外部への持ち出しを監視しなければならない。

（１５）電子メールの利用制限

ア　職員は、自動転送機能を用いて、本市が管理する電子メールアドレス以外に電子メールを転送してはならない。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転送することができる。

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、ＢＣＣ機能を利用するなど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、情報漏えいにつながる電子メールの誤送信が発生した場合、本対策基準５．３に則り速やかに報告しなければならない。

オ　職員は、私用メールアドレス（本市が管理する電子メールアドレスではなく、個人が取得しているメールアドレス）を業務に利用してはならない。ただし、重要情報資産を扱わない業務に限り、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。

（１６）電子署名、暗号化

職員は、「重要情報」を送信する場合には、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。情報セキュリティ執行責任者は、暗号化及び電子署名について、安全性を確保できる措置を講じなければならない。

（１７）無許可ソフトウェアの導入等の禁止

ア　職員は、パソコン及びモバイル端末に無断でソフトウェアを導入してはならない。

イ　職員は、業務上の必要がある場合は、情報セキュリティ執行責任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。

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。

（１８）機器構成の変更の制限

ア　職員は、貸与されたパソコン及びモバイル端末に対し機器の改造、増設及び交換を行ってはならない。

イ　職員は、業務上、パソコン及びモバイル端末に対し機器の改造、増設及び交換を行う必要がある場合には、情報セキュリティ執行責任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。

（１９）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・無線を問わず、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。

（２０）業務以外の目的でのウェブ閲覧の禁止

ア　職員は、業務以外の目的でウェブを閲覧してはならない。

イ　情報セキュリティ執行責任者は、職員のウェブ利用について、明らかに業務に関係のな

いサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

（２１）Ｗｅｂ会議サービスの利用時の対策

ア　情報セキュリティ執行責任者は、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、本市の定める利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

ウ　職員は、Ｗｅｂ会議を主催する場合、会議に無関係のものが参加できないよう対策を講ずること。

（２２）ソーシャルメディアサービスの利用

ア　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、認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、ＵＳＢメモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

イ　情報セキュリティ管理者は、利用するソーシャルメディアサービスごとに担当者を指名すること。

ウ　「重要情報」はソーシャルメディアサービスで発信してはならない。

エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

６．２　アクセス制御

（1）アクセス制御等

ア　アクセス制御

情報セキュリティ執行責任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アクセスする権限のない職員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。

イ　利用者ＩＤの取扱い

（ア）情報セキュリティ執行責任者及び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、職員の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（イ）職員は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ執行責任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）情報セキュリティ執行責任者及び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にしなければならない。

ウ　特権を付与されたＩＤの管理等

（ア）情報セキュリティ執行責任者及び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、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）情報セキュリティ執行責任者及び情報システム管理者の特権を代行する者は、情報セキュリティ執行責任者及び情報システム管理者が指名し、情報セキュリティ統括責任者が認めた者でなければならない。

（ウ）情報セキュリティ統括責任者は、代行者を認めた場合、速やかに情報セキュリティ執行責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ）情報セキュリティ執行責任者及び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、委託事業者に行わせてはならない。

（オ）情報セキュリティ執行責任者及び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、職員の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（カ）情報セキュリティ執行責任者及び情報システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

（2）職員による外部からのアクセス等の制限

ア　職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報セキュリティ執行責任者及び当該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。

イ　情報セキュリティ執行責任者は、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。

ウ　情報セキュリティ執行責任者は、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。

エ　情報セキュリティ執行責任者は、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。

オ　情報セキュリティ執行責任者及び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。

カ　職員は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得る、又は情報セキュリティ管理者によって事前に定められた手順に従って接続しなければならない。

キ　情報セキュリティ執行責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。

（3）ログイン時の表示等

情報システム管理者は、システムの特性に応じて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。

（4）認証情報の管理

ア　情報セキュリティ執行責任者又は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　情報セキュリティ執行責任者又は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は、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　情報セキュリティ執行責任者又は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、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

6．3　システム開発、導入、保守等

（1）情報システムの調達

ア　情報セキュリティ執行責任者及び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。

イ　情報セキュリティ執行責任者及び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、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

ア　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規則を確立しなければならない。

イ　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、開発完了後、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、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

ウ　システム開発に用いるハードウェア及びソフトウェアの管理

（ア）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導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（3）情報システムの導入

ア　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とシステム運用環境を分離するよう努めなければならない。

（イ）情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ）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。

（エ）情報システム管理者は、導入するシステム及び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。

イ　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、個人情報及び機密性の高い情報資産を、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

ア　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関連文書を適正に整備・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。

（5）情報システムにおける入出力データの正確性の確保

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。

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。

６．４　不正プログラム対策

（1）情報セキュリティ執行責任者の措置事項

情報セキュリティ執行責任者は、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等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。

イ　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等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。

ウ　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、必要に応じ職員に対して注意喚起しなければならない。

エ　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。

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、常に最新の状態に保たなければならない。

カ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

キ　業務で利用するソフトウェアは、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等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。なお、原則、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）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に関し、次の事項を措置しなければならない。

ア　情報システム管理者は、その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システムに常駐させなければならない。

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は、常に最新の状態に保たなければならない。

ウ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

エ　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に原則利用させてはならない。また、電磁的記録媒体を使用する端末においては、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。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員以外に当該権限を付与してはならない。

（3）職員の遵守事項

職員は、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。

ア　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。

イ　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。

ウ　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。

エ　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。

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

カ　情報セキュリティ執行責任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。

キ　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、当該端末にＬＡＮケーブルが接続されている場合はＬＡＮケーブルを取り外し、ＬＡＮケーブル以外で通信を行っている場合は、通信を行わない設定への変更等を実施しなければならない。

（4）専門家の支援体制

情報セキュリティ執行責任者は、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）情報セキュリティ執行責任者の措置事項

情報セキュリティ執行責任者は、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。

ア　使用されていないポートを閉鎖しなければならない。

イ　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　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できるように努めなければならない。

エ　情報セキュリティ執行責任者は、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、適正な対応等を実施できる体制及び連絡網を構築しなければならない。

（2）攻撃への対処

情報セキュリティ統括責任者及び情報セキュリティ執行責任者は、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、和歌山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

情報セキュリティ統括責任者及び情報セキュリティ執行責任者は、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

情報セキュリティ執行責任者及び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。

（5）職員による不正アクセス

情報セキュリティ執行責任者及び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は、当該職員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

情報セキュリティ執行責任者及び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

情報セキュリティ執行責任者及び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低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6．6　セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集、共有及びソフトウェアの更新等

情報セキュリティ執行責任者及び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及び周知

情報セキュリティ執行責任者は、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

情報セキュリティ執行責任者及び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）情報セキュリティ執行責任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、情報システムを監視するよう努めなければならない。

（2）情報セキュリティ執行責任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措置を講じなければならない。

（3）情報セキュリティ執行責任者及び情報システム管理者は、外部と常時接続するシステムを監視するよう努めなければならない。

7．2　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

情報セキュリティ統括責任者及び情報セキュリティ統括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。

7．3　侵害時の対応等

（1）緊急時対応計画の策定

情報セキュリティ統括責任者又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（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。

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）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、情報セキュリティ委員会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。

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の採用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、情報セキュリティ統括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、事後速やかに情報セキュリティ統括責任者に報告しなければならない。

（3）例外措置の申請書の管理

情報セキュリティ統括責任者は、例外措置の申請書及び審査結果を適正に保管し、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２６年法律第１０４号）
（７）和歌山市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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成２７年条例第５１号）

８　業務委託と外部サービスの利用

８．１　業務委託

（１）委託事業者の選定基準等

ア　情報セキュリティ管理者は、委託事業者の選定に当たり、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、情報セキュリティ監査の実施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。

ウ　情報セキュリティ管理者は、再委託の禁止の例外として、業務委託の再委託を認める場合は、再委託先、再委託する業務内容及び次項に定める委託事業者と同様の規定の遵守について明確にし、再委託先における情報セキュリティ対策が確保されることを確認した上で、再委託の諾否を判断しなければならない。また、申請と承諾については、書面にて取り交わすものとする。

（２）契約項目

「重要情報資産」を取り扱う事務を業務委託する場合には、委託事業者との間で次の情報セキュリティ要件を明記した上で契約を締結しなければならない。

ア　明記が必要な要件

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・本市による監査、検査
・本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）

イ　情報システムの運用、保守等を外部委託する場合に、必要に応じて明記する要件
・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

（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を講じなければならない。また、その内容を情報セキュリティ執行責任者に報告するとともに、その重要度に応じて情報セキュリティ統括責任者に報告しなければならない。

８．２　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係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、「重要情報」が取り扱われないように規定しなければならない。

ア　約款によるサービスを利用して良い範囲
イ　業務により利用する約款による外部サービス
ウ　利用手続及び運用手順

（2）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。

８．３　クラウドサービスの利用

（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、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断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、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。

（4）情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。

（5）情報セキュリティ管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

9　評価及び見直し

9．1　監査

（1）実施方法

情報セキュリティ監査統括責任者を別紙１のとおり定め、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、毎年度に及び必要に応じて随時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　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ　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又はこれらの支援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統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

イ　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

委託事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について、必要に応じ、監査を行わなければならない。

（5）報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ執行責任者に報告する。

（6）保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

（7）監査結果への対応

情報セキュリティ執行責任者は、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。

指摘事項への対処を指示された情報セキュリティ管理者は、当該指示の内容を踏まえ対策の改善を行い、その結果を情報セキュリティ執行責任者に報告しなければならない。

（8）情報セキュリティ委員会への報告

情報セキュリティ執行責任者は、指摘事項に対する改善状況も含めた監査の最終結果について、情報セキュリティ委員会に報告しなければならない。

9．2　自己点検

（1）実施方法

ア　情報セキュリティ責任者は、情報システム管理者と連携して、所管するネットワーク及

び情報システムについて、毎年度に及び必要に応じて随時に、自己点検を実施しなければならない。

イ　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、毎年度に及び必要に応じて随時に、自己点検を行わなければならない。

ウ　職員は、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）報告

情報セキュリティ責任者は、自己点検の結果を取りまとめ、情報セキュリティ執行責任者に報告する。

（3）情報セキュリティ委員会への報告

情報セキュリティ執行責任者は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

９．３　情報セキュリティポリシー、関係規程及びその他情報セキュリティ対策等の見直し

情報セキュリティ委員会は、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、関係規程及びその他情報セキュリティ対策等について毎年度及び必要に応じて随時に評価を行い、必要があると認めた場合、改善を行うものとする。

附　則　抄

１　この対策基準は、平成１５年８月１日から施行する。

附　則（平成１７年１１月１日）

この対策基準は、平成１７年１１月１日から施行する。

附　則（平成１８年６月３０日）

この対策基準は、平成１８年７月１日から施行する。

附　則（平成１８年９月３０日）

この対策基準は、平成１８年１０月１日から施行する。

附　則（平成１９年４月１日）

この対策基準は、平成１９年４月１日から施行する。

附　則（平成１９年６月１日）

この対策基準は、平成１９年６月１日から施行する。

附　則（平成２４年４月１日）

この対策基準は、平成２４年４月１日から施行する。

附　則（平成２６年８月１日）

この対策基準は、平成２６年８月１日から施行する。

附　則（平成２７年１月１日）

この対策基準は、平成２７年１月１日から施行する。

附　則（平成２７年４月１日）

この対策基準は、平成２７年４月１日から施行する。

附　則（平成２７年１０月５日）

この対策基準は、平成２７年１０月５日から施行する。

附　則（平成２９年２月２４日）抄

この対策基準は、平成２９年２月２４日から施行する。

附　則（平成３０年４月１日）

この対策基準は、平成３０年４月１日から施行する。

附　則（平成３１年４月１日）

この対策基準は、平成３１年４月１日から施行する。

附　則（令和３年４月１日）

この対策基準は、令和３年４月１日から施行する。

附　則（令和３年７月１日）

この対策基準は、令和３年７月１日から施行する。

附　則（令和５年４月１日）

この対策基準は、令和５年４月１日から施行する。

別紙１

組織体制

役職名	担当	位置づけ
情報セキュリティ統括責任者	総務局担当副市長	本市情報セキュリティの体制整備、改善計画、指示、実行状況の把握の総責任者
情報セキュリティ副統括責任者	総務局担当副市長以外の副市長 公営企業管理者及び教育長	
情報セキュリティ執行責任者	総務局長	本市の情報セキュリティ対策の実行者及び責任者
情報セキュリティ副執行責任者	総務部長	
情報セキュリティ監査統括責任者	総務部長	情報セキュリティ統括責任者の指名に基づく、本市の情報セキュリティ監査の総責任者
情報セキュリティ責任者	各局※１の長※２	局の情報セキュリティ対策の実行者及び責任者
情報セキュリティ副責任者	各部の長※３	
情報セキュリティ管理者	課等の長	課等の情報セキュリティ対策の実行者及び責任者
情報システム管理者	情報システムの管理及び運用を行う当該課等の長	情報システム単位での管理責任者
情報システム担当者	情報システム管理者が指名する者	情報システム管理者の指示に従い、情報システムの管理業務を補佐する

体制の役職名において「副」にあたる者は、その主たる役職の補佐を行うとともに、主たる役職が不在の際に代行を行う。

情報セキュリティ委員会

１　本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会（以下「委員会」という。）を置く。
２　委員会は、情報セキュリティ統括責任者、情報セキュリティ副統括責任者、情報セキュリティ執行責任者及び情報セキュリティ副執行責任者で構成し、情報セキュリティ統括責任者を委員長とする。
３　委員会の所掌事務は次のとおりとする。
（１）情報セキュリティポリシーの改定、評価、見直しに関すること。
（２）情報セキュリティ自己点検及び監査の報告に関すること。
（３）実害が生じるおそれがあるなど重要度の高い情報セキュリティインシデントを認知した場合、対応に係る意思決定に関すること。
（４）情報セキュリティ対策の改善計画の策定に関すること。
（５）その他、情報セキュリティに係る重要事項に関すること。
４　委員会の会議は、委員長が招集し、会務を総理する。
５　委員会は、必要に応じて、関係部局の情報セキュリティ責任者、情報セキュリティ副責任者、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の出席を求めて、意見又は説明を聴くことが出来る。
６　委員会の庶務は、情報セキュリティに関する統一的な窓口において処理する。委員会の庶務に関し必要な事項は、事務局が別に定めるものとする。

情報セキュリティに関する統一的な窓口

本市の情報セキュリティ対策を統一的に行うため、デジタル推進課を情報セキュリティに関する統一的な窓口とする。統一的な窓口は、情報セキュリティインシデントに対処するため、庁内及び関係機関や外部の事業者等との情報連携を行わなければならない。

※１　和歌山市事務分掌条例（昭和５１年条例第１号）第１条に規定する内部組織、出納室、消防局、教育委員会事務局、議会事務局、監査事務局、選挙管理委員会事務局、人事委員会事務局、農業委員会事務局、固定資産評価審査委員会事務局及び企業局
※２　出納室にあっては会計管理者、教育委員会事務局にあっては教育局長、企業局にあっては企業局長
※３　出納室にあっては出納室長、消防局にあっては消防局副局長、議会事務局にあっては議会事務局副局長

別紙２

取扱制限の考え方

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、その他の情報の適正な取扱いを職員に確実に行わせるための手段をいう。職員は、取扱制限に応じた情報の取扱いを適切に行う必要がある。以下に取扱制限の観点と指定方法を例示する。対象の情報に対し、必要な観点を用いて指定する。（全ての観点の指定を求めるものではない。）

分類	取扱制限の観点	指定方法	説明
完全性	保存期間	yyyy年mm月dd日まで保存	当該情報について、保存期限を指定する必要がある場合に指定する。
	保存場所	○○において保存	当該情報について、保存場所を指定する必要がある場合に指定する。
	保存期間満了後	保存期間満了後要廃棄	当該情報について、保存期間満了後の取り扱いを指定する必要がある場合に指定する。
	更新	更新禁止、要更新許可	「○○禁止」は当該情報について、指定した行為を禁止する必要がある場合に指定する。 「要○○許可」は当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。許可者は情報セキュリティ対策基準に則り指定する（特に指定がない場合は情報セキュリティ担当者を許可者とする）。
	削除	削除禁止、要削除許可	
機密性	複製	複製禁止、要複製許可	
	配布	配布禁止、要配布許可	
	印刷	印刷禁止、要印刷許可	
	転送	転送禁止、要転送許可	
	転記	転記禁止、要転記許可	
	再利用	再利用禁止、要再利用許可	
	送信	送信禁止、要送信許可	
	暗号化	暗号化必須、保存時暗号化必須、通信時暗号化必須	当該情報について、暗号化を必須とする必要がある場合に指定する。
	参照者	○○限り	当該情報について、参照してもよい者を○○に記載した者のみに制限する必要がある場合に指定する。 ○○には組織名や、役職名、会議体名等、参照を可とされる者が具体的に分かるように記載する。
	取扱制限期限	yyyy年mm月dd日まで○○禁止／要○○許可	当該情報について、特定の日まで指定した行為ををを制限したい場合に指定する。指定日以降に取扱制限を更新する必要がなくなる。
可用性	許容復旧時間	○○以内に復旧	復旧までに要する許容時間を指定する必要がある場合に指定する。