周南市情報セキュリティ対策基準

目次

序章　はじめに

（１）目的

この対策基準は、周南市情報セキュリティ基本方針（以下「基本方針」という。）第９条の規定に基づき、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

（２）定義

この対策基準における用語は、基本方針第２条に規定するところによる。

（３）適用範囲

この対策基準が適用される行政機関は、基本方針第４条に規定するところによる。

第１章　組織体制

（１）最高情報セキュリティ責任者

①副市長を最高情報セキュリティ責任者（Chief Information Security Officer、以下「ＣＩＳＯ」という。）とする。ＣＩＳＯは、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②ＣＩＳＯ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。

③ＣＩＳＯ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（Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）を整備し、役割を明確化する。

④ＣＩＳＯは、ＣＩＳＯを助けて本市における情報セキュリティに関する事務を整理し、ＣＩＳＯの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）１人を必要に応じて置く。

⑤ＣＩＳＯは、本対策基準に定められた自らの担務を、副ＣＩＳＯその他の本対策基準に定める責任者に担わせることができる。

（２）統括情報セキュリティ責任者

①情報政策担当部長をＣＩＳＯ直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、ＣＩＳＯ及び副ＣＩＳＯを補佐しなければならない。

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

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

④統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、ＣＩＳＯの指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

⑤統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、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等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。

⑥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内部部局の長、行政委員会事務局の長、消防長及び地方公営企業の総務担当の長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、その所管する部局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、非常勤職員及び臨時職員等（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。

（４）情報セキュリティ管理者

①内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する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。

④情報セキュリティ管理者は、その所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

⑤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、情報システム管理者、統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（５）情報システム管理者

①情報政策担当課長を情報システム管理者とする。

②情報システム管理者は、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。

③情報システム管理者は、本市の共通のネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

④情報システム管理者は、情報セキュリティ関係規程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ＣＩＳＯにその内容を報告しなければならない。

（６）情報システム担当者

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

（７）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を設置し、情報セキュリティに関する重要な事項を決定する。

②情報セキュリティ委員会に関する必要な事項は、周南市情報セキュリティ委員会要領で別に定める。

（８）兼務の禁止

①情報セキュリティ対策の実施において、や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。

②情報セキュリティ監査の実施において、や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）ＣＳＩＲＴの設置・役割

①ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化しなければならない。

②ＣＩＳＯは、ＣＳＩＲＴに所属する職員等を選任し、その中からＣＳＩＲＴ責任者を置かなければならない。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③ＣＩＳＯ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しなければならない。

④ＣＩＳＯ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。

⑤情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、山口県等へ報告しなければならない。

⑥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・公表対応を行わなければならない。

⑦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、委託事業者等との情報共有を行わなければならない。

第２章　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３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	１　機密性３の情報資産に対する支給以外の端末での作業の原則禁止 ２　必要以上の複製及び配布の禁止 ３　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 ４　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 ５　復元不可能な処理を施しての廃棄 ６　信頼のできるネットワーク回線の選択 ７　外部で情報処理を行う際の安全管理措置の規定 ８　電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	－

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	１ バックアップ、電子署名付与 ２ 外部で情報処理を行う際の安全管理措置の規定 ３ 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の情報資産以外の情報資産	－

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	１ バックアップ、指定する時間以内の復旧 ２ 電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	－

（２）情報資産の管理

①情報資産の管理責任

（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）情報セキュリティ管理者は、情報資産を複製又は伝送した場合には、複製等された情報資産も前節の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、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、適正な管理に努めるものとする。

③情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、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、不要になった場合は、当該情報を速やかに消去しなければならない。

④情報資産の入手

庁内及び庁外の者が作成した情報資産を入手した者は、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。

⑤情報資産の利用

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

（イ）情報資産を利用する者は、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。

⑥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間保管する場合は、書込禁止の措置を講じなければならない。

⑦情報資産の送信

電子メール等により機密性２以上の情報資産を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧情報資産の運搬

（ア）機密性２以上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。

（イ）車両等により機密性２以上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、パスワード等による暗号化等の措置を講じるなど、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。

⑨情報資産の提供・公表

（ア）機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性２以上の情報資産を外部に提供する者は、必要に応じ、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、市民等に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄等

（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、情報を復元できないように処置しなければならない。

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

第３章　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。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。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、インターネット等とＬＧＷＡＮを経由してマイナンバー利用事務系との双方向でのデータの移送を可能とする。

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）情報の持ち出し制限

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を行ってはならない。ただし、業務上必要な場合、情報セキュリティ管理者の許可を得て持ち出すことができる。

（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

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４章　物理的セキュリティ対策

第１節　サーバ等機器の管理

情報システムを所管する情報セキュリティ管理者は、所管する機器等及び情報システム管理者から配付された機器等について、必要に応じて、次のような対策を講じなければならない。

（１）機器の取付け

サーバ等の機器を取付ける場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（２）サーバの冗長化

重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

（３）機器の電源

①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。

（４）通信ケーブル等の配線

①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。

③ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④情報政策担当課職員及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（５）機器の定期保守及び修理

①可用性２のサーバ等の定期保守を実施する。

②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うこと。ただし、内容を消去できない場合、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

庁舎の敷地外へのサーバ等の機器の設置については、情報システム管理者の承認を得なければならない。また、設置後は、必要に応じて当該機器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

機器を廃棄、リース返却等する場合、機器内部の記録装置から全ての情報を消去の上、復元不可能な状態であることを確認しなければならない。

第２節　情報システム室の管理

（１）情報システム室の構造等

①全庁的な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部屋を「情報システム室」といい、情報システム管理者が管理する。

②情報システム管理者は、施設管理部門と連携して、情報システム室から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

③情報システム管理者は、情報システム室内に設置する機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（２）情報システム室の入退室管理等

①情報システム管理者は、情報システム室への入退室を許可した者のみに制限し、ＩＣカード認証や別に定める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。

②職員等及び委託事業者は、情報システム室に入室する場合、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、情報システム室への入室について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末（タブレット、スマートフォン等）、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。ただし、情報システム管理者が許可した場合はこの限りではない。

（３）機器等の搬入出

①情報システム管理者は、情報システム室に搬入する機器等が、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。

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

第３節　通信回線及び通信回線装置の管理

①統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（ＬＧＷＡＮ）に集約するように努めなければならない。

④統括情報セキュリティ責任者は、機密性２以上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。

⑤統括情報セキュリティ責任者は、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。

⑥統括情報セキュリティ責任者は、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。

第４節　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、必要に応じて、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るものとする。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情報セキュリティ管理者又は情報システム管理者は、情報システムへのログインに際し、パスワード、ＩＣカード、生体認証等複数の認証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）を行うよう設定しなければならない。

第５章　人的セキュリティ対策

第１節　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モバイル端末や電磁的記録媒体等の持ち出し等の制限

（ア）ＣＩＳＯは、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）職員等は、本市のパソコン、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。持ち出しする際の事前申請及び許可は、別に定める「情報資産持出等管理簿」によるものとする。ただし、情報システム管理者が所管するモバイル端末及び電磁的記録媒体などを外部に持ち出す場合は、別に定める「コンピュータ等貸出申請書」により、情報システム管理者の許可を得るものとする。

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

（エ）外部に持ち出したパソコン及びモバイル端末を本市が使用を認めるネットワーク以外には接続してはならない。ただし、業務上必要な場合、情報セキュリティ管理者及び情報システム管理者の許可を得て接続することができる。

（オ）外部から持ち込んだパソコン及びモバイル端末を本市のネットワークに接続してはならない。ただし、業務上必要な場合、情報セキュリティ管理者及び情報システム管理者の許可を得て持ち込むことができる。

（カ）外部から持ち込んだ電磁的記録媒体を本市のネットワークに接続してはならない。ただし、業務上必要な場合、情報セキュリティ管理者の許可を得て接続することができる。その場合、インターネット接続系端末に接続し、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。なお、不正プログラムの感染が疑われる場合は、本対策基準第６章第４節（３）⑦のとおり対応しなければならない。

④支給以外のパソコン、モバイル端末等の業務利用

（ア）職員等は、本市から支給した以外のパソコン、モバイル端末及び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、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

（イ）職員等は、支給以外のパソコン等について、盗み見、盗難、紛失、不正プログラムの感染等により情報窃取されないよう、次の対策を講じなければならない。

□ パスワード等による端末ロックの常時設定

□ ＯＳやアプリケーションの最新化

□ 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施

□ 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）

□ 第三者に盗み見されないための措置

□ 端末内へ情報資産を複写しない

□ 安全性が確認できないソフトウェアのインストール及び利用をしない

□ 利用が禁止されているソフトウェアのインストール及び利用をしない

□ 許可されない通信回線サービスを利用しない

⑤持ち出し及び持ち込みの確認

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確認しなければならない。

⑥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、支給しているパソコンやモバイル端末等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又は情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の情報資産の管理

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が第三者に容易に使用又は閲覧されることがないように、離席時のパソコン、モバイル端末の画面ロック機能の活用や、退庁時等には記録媒体や文書等が容易に閲覧されない場所に保管するなど、適正な措置を講じなければならない。

⑧退職時等の遵守事項

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

（２）非常勤職員及び臨時職員等への対応

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、非常勤職員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、非常勤職員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。

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、非常勤職員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。

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、非常勤職員及び臨時職員等にパソコンやモバイル端末による作業を行わせる場合は、業務上必要最小限の範囲とするほか、インターネット接続及び電子メール使用等が不要の場合、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を閲覧できるように掲示しなければならない。

（４）委託事業者に対する指導

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、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について必要な指導をしなければならない。

第２節　研修・訓練

（１）情報セキュリティに関する研修

①統括情報セキュリティ責任者は、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。

②情報セキュリティ管理者は、その所管する情報システムの利用者に対して、情報システム利用に関わる研修を実施しなければならない。

③統括情報セキュリティ責任者は、情報セキュリティに関する情報を閲覧できる環境を整備し、職員等に対する情報セキュリティの啓発に努めなければならない。

（２）緊急時対応訓練の実施

ＣＩＳＯ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。訓練にあたっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また効果的に実施できるようにしなければならない。

（３）研修への参加

全ての職員等は、定められた研修に参加しなければならない。

第３節　情報セキュリティインシデントの報告

（１）庁内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、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周南市ＣＳＩＲＴ設置要領に示す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。

②報告を受けた情報セキュリティ管理者は、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情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

（２）市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、市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、速やかに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。

③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。

④ＣＩＳＯは、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、市民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（３）情報セキュリティインシデントの原因の究明・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。また必要に応じて、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。

第４節　ＩＤ及びパスワード等の管理

（１）ＩＣカードの取扱い

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

（ア）認証に用いる　ＩＣカードを、職員等間で共有してはならない。

（イ）業務上必要のないときは、ＩＣカード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カードを紛失した場合には、速やかに総務担当課長、情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

②総務担当課長及び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総務担当課長は、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付与されたＩＤを適正に管理し、他人に利用させてはならない。

②共有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パスワードを記載したメモを作成して他人が容易に見える場所に貼ってはならない。

③パスワードには、本人の氏名、生年月日など他人に容易に推測される文字列を用いてはならない。

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仮のパスワード（初期パスワード含む。）は、最初のログイン時点で変更しなければならない。

⑥サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑦職員等間でパスワードを共有してはならない（ただし、共有ＩＤに対するパスワードは除く。）。

第６章　技術的セキュリティ対策

第１節　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、職員等が他所属等のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。

③情報システム管理者は、市民の個人情報、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、必要に応じ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。

（２）バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（３）他団体との情報システムに関する情報交換等

情報セキュリティ管理者は、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、その取扱いに関する事項をあらかじめ定め、情報セキュリティ責任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

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

②情報セキュリティ管理者は、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。

（５）情報システム仕様書等の管理

情報セキュリティ管理者は、所管する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の閲覧や紛失等が発生しないよう、適正に管理しなければならない。

（６）ログの取得等

①情報セキュリティ管理者及び情報システム管理者は、所管する情報システムの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情報セキュリティ管理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。

③統括情報セキュリティ責任者及び情報システム管理者は、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の措置を講じなければならない。

（７）障害記録

情報セキュリティ管理者及び情報システム管理者は、職員等からの情報システムの障害報告、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。

（８）ネットワークの接続制御、経路制御等

①統括情報セキュリティ責任者は、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。

②統括情報セキュリティ責任者は、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

①情報セキュリティ管理者は、所管するネットワークを外部ネットワークと新たに接続しようとする場合には、情報セキュリティ責任者及び情報システム管理者に事前協議し、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統括情報セキュリティ責任者は、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、庁内のすべてのネットワーク、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情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、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。

④統括情報セキュリティ責任者は、サーバ等を外部ネットワークに接続する場合、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。

⑤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、統括情報セキュリティ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

①情報セキュリティ管理者又は情報システム管理者は、複合機を調達する場合、当該機器が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

②情報セキュリティ管理者又は情報システム管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の機器に対する情報セキュリティインシデントへの対策を講じなければならない。

③情報セキュリティ管理者又は情報システム管理者は、その所管する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の盗聴対策

統括情報セキュリティ責任者は、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。なお、マイナンバー利用事務系においては、無線ＬＡＮは利用してはならない。

(14)電子メールのセキュリティ管理

情報システム管理者は、電子メールの利用に関するセキュリティ対策として、次の事項を措置しなければならない

①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、措置しなければならない。

②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。

③電子メールの送受信容量の上限を設定し、上限を超える送受信を制限しなければならない。

④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。

(15)電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メール本文及び添付ファイ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、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。

④職員等は、重要な電子メールを誤送信した場合、速やかに情報セキュリティ管理者に報告しなければならない。

⑤職員等は、インターネットで利用できるフリーメール等を利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者及び情報システム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

①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、ＣＩＳＯが定めた電子署名、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。

②職員等は、暗号化を行う場合にＣＩＳＯが定める以外の方法を用いてはならない。また、ＣＩＳＯが定めた方法で暗号のための鍵を管理しなければならない。

③ＣＩＳＯは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17)無許可ソフトウェアの導入等の禁止

①職員等は、パソコンやモバイル端末に、無断でソフトウェアを導入してはならない。

②職員等は、業務上の必要がある場合は、情報セキュリティ管理者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18)機器構成の変更の制限

パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。業務上、機器の改造及び増設・交換を行う必要がある場合は、情報システム管理者の許可を得なければならない。なお、電磁的記録媒体を含まないキーボード、マウス及びディスプレイの増設・交換は、原状復帰を条件とした一時的なものに限り、情報セキュリティ管理者の許可を得て行うことができる。

(19)業務外ネットワークへの接続の禁止

①職員等は、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。

②情報システム管理者は、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できる。

(20)業務以外の目的でのウェブ閲覧の禁止

①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、職員等のインターネット又は電子メールの利用について、明らかに業務以外の目的に利用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

①情報システム管理者は、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。

②職員等は、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。

③職員等は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

④職員等は、外部からＷｅｂ会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22)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Ｗｅｂ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、ハードディスク、ＵＳＢメモリー、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

②機密性２以上の情報は、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。

④アカウント乗っ取りを確認した場合には、ログインパスワードの変更やアカウントの停止を実施する等、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。

⑤可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管

理Ｗｅｂサイトに当該情報を掲載して参照可能とすること。

第２節　アクセス制御

(１)アクセス制御等

①アクセス制御

情報セキュリティ管理者は、所管するネットワーク又は情報システムごとに、権限のない職員等がアクセスできないように、システム上制限しなければならない。

②利用者ＩＤの取扱い

（ア）情報セキュリティ管理者は、所管する情報システムの利用者の登録、変更、抹消等の情報管理、職員等の人事異動、出向、退職者に伴うＩＤの取扱い等の方法を定めなければならない。

（イ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ管理者に通知しなければならない。

（ウ）情報セキュリティ管理者は、所管する情報システムで利用されていない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）情報セキュリティ管理者は、所管する情報システムにおいて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）特権を付与されたＩＤを利用する者は、所管する情報システムの情報セキュリティ管理者が指名し、情報システム管理者又は情報セキュリティ管理者が認めた者でなければならない。

（ウ）情報セキュリティ管理者は、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。

（エ）情報セキュリティ管理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、職員等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の強化に努めるものとする。

（オ）情報セキュリティ管理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)職員等による外部からのアクセス等の制限

①職員等又は委託事業者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、事前に、当該情報システムを管理する情報セキュリティ管理者及び情報システム管理者の許可を得なければならない。ただし、テレワークにより外部から内

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、「周南市職員在宅等勤務実施要領」の規定によるものとする。

②情報システム管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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。

③当該情報システムを管理する情報セキュリティ管理者及び情報システム管理者は、職員等又は外部委託業者に外部からのアクセスを認める場合、システム上で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統括情報セキュリティ責任者は、職員等又は外部委託業者に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職員等又は委託業者は、持ち込んだ又は外部から持ち帰ったパソコンや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の感染やパッチの適用状況等を確認しなければならない。

⑦統括情報セキュリティ責任者は、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。ただし、やむを得ず接続を許可する場合は、多要素による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

⑧職員等又は委託事業者は、外部から内部のネットワーク又は情報システムへの接続を許可された場合は、許可されたアクセス方法以外でアクセスしてはならない。

（３）認証情報の管理

①情報セキュリティ管理者は、所管する情報システムにおける職員等の認証情報を厳重に管理しなければならない。

②情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、職員等により正規のパスワードを取得させなければならない。

③情報セキュリティ管理者は、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。

（４）特権による接続時間の制限

情報セキュリティ管理者は、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。

第３節　情報システムの開発、導入、保守等

（１）情報システムの調達

①情報セキュリティ管理者は、情報システム開発、導入、保守等の調達にあたっては、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情報セキュリティ管理者は、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。

（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

情報セキュリティ管理者は、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。

②システム開発における責任者及び作業者のＩＤの管理

（ア）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報セキュリティ管理者は、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しなければならない。

（イ）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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）情報セキュリティ管理者は、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）情報セキュリティ管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）情報セキュリティ管理者は、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情報セキュリティ管理者は、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。

②情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

③情報セキュリティ管理者は、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情報セキュリティ管理者は、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情報セキュリティ管理者は、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、これをチェック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。

③情報セキュリティ管理者は、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

情報セキュリティ管理者は、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

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新し、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

情報セキュリティ管理者は、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。

第４節　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不正プログラムのチェックを行い、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所管するサーバ及びパソコン等の端末に、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、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチ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。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

（２）情報システムを所管する情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、その所管する情報システムにおける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。

①所管するサーバ及びパソコン等に、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。

②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。

③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。

④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、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、不正プログラム対策ソフトウェアを導入し、不正プログラム対策ソフトウェアのパターンファイルの更新を定期的に実施しなければならない。

⑤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、情報セキュリティ管理者が許可した職員等を除く職員等に当該権限を付与してはならない。

（３）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

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

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

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

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

⑥情報システム管理者が提供するコンピュータウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

（４）専門家の支援体制

統括情報セキュリティ責任者は、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、外部の専門家との支援を受けられるように努めなければならない。

第５節　不正アクセス対策

（１）統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、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。

①使用し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

ＣＩＳＯ及び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、関係機関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

ＣＩＳＯ及び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

情報セキュリティ管理者は、職員等及び委託事業者が使用しているパソコン等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

情報セキュリティ管理者は、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情報セキュリティ責任者及び情報システム管理者に通知し、適正な処置を求めなければならない。また、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情報セキュリティ責任者に通知し、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

情報セキュリティ管理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、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。

第６節　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

統括情報セキュリティ責任者及び情報システム管理者は、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

統括情報セキュリティ責任者及び情報システム管理者は、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

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第７章　運　用

第１節　情報システムの監視

①情報セキュリティ管理者及び情報システム管理者は、セキュリティに関する事案を検知するため、所管する情報システムを常時監視しなければならない。

②情報セキュリティ管理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、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情報セキュリティ管理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、外部と常時接続する場合は、常時監視しなければならない。

第２節　情報セキュリティポリシーの遵守状況の確認

（１）遵守状況の確認及び対処

①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに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。また、問題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、ＣＩＳＯに報告しなければならない。

②ＣＩＳＯ及び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情報セキュリティ管理者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

統括情報セキュリティ責任者及び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、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）職員等の報告義務

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、情報システム管理者に、情報システム管理者は統括情報セキュリティ責任者に直ちに報告を行わなければならない。

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。

第３節　侵害時の対応等

（１）緊急時対応計画の策定

情報セキュリティ委員会は、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）緊急時対応計画の内容

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、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。

（４）緊急時対応計画の見直し

情報セキュリティ委員会は、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４節　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に報告しなければならない。

（３）例外措置の管理

ＣＩＳＯは、例外措置の申請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。

第５節　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周南市個人情報保護法施行条例（令和４年第４１号）

第６節　懲戒処分等

（１）懲戒処分

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

（２）違反時の対応

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情報セキュリティ管理者又は情報システム管理者が違反行為を確認した場合は、速やかに当該職員等が所属する情報セキュリティ責任者及び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情報セキュリティ管理者に通知しなければならない。

第８章　業務委託と外部サービスの利用

第１節　業務委託

（１）委託事業者の選定基準

①情報セキュリティ管理者は、委託事業者の選定にあたり、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、委託事業者を選定するように努めるものとする。

（２）契約項目

情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び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
・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

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

第２節　外部サービスの利用（機密性２以上の情報を取り扱う場合）

（１）外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備すること。

（２）外部サービスの選定

①情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

②情報セキュリティ管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。ま

た、可能な範囲で以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

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

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

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

（エ）外部サービス提供者に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ管理者は、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検討し、必要に応じて外部サービス提供者の選定条件に含めること。

④情報セキュリティ管理者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて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

⑤情報セキュリティ管理者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて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・裁判管轄を選定条件に含めること。

⑥情報セキュリティ管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、可能な範囲で外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、可能な範囲で外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同程度の水準を求めること。

⑧情報セキュリティ管理者は、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て、セキュリティ要件を定めること。

⑨統括情報セキュリティ管理者は、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

（３）外部サービスの利用に係る調達・契約

①情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認すること。

（４）外部サービスの利用承認

①情報セキュリティ管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、情報システム管理者と協議のうえ、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

（５）外部サービスを利用した情報システムの導入・構築時の対策

統括情報セキュリティ管理者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

（６）外部サービスを利用した情報システムの運用・保守時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

②情報セキュリティ管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

（７）外部サービスを利用した情報システムの更改・廃棄時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスの利用を終了する際のセキュリティ対策を規定すること。

②情報セキュリティ管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

第３節　外部サービスの利用（機密性２以上の情報を取り扱わない場合）

（１）外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

（２）外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。

②情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

第９章　評価・見直し

第１節　監査

（１）実施方法

情報セキュリティ責任者は、情報セキュリティ管理者に対して、定期的又は必要に応じて、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、監査を実施しなければならない。

（２）監査を行う者の要件及び実施への協力

① 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。

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）委託事業者に対する監査

情報システムの保守又は管理運用等を事業者に業務委託している場合、情報セキュリティ責任者は委託事業者（再委託事業者を含む。）に対して、定期的に又は必要に応じて、情報セキュリティポリシーの遵守状況について監査を定期的又は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、情報セキュリティ責任者からの監査結果を取りまとめ、情報セキュリティ委員会に報告する。

（５）保管

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、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。

（６）監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者に対し、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責任者に対しても、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。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

（７）情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、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。

（８）外部監査

情報セキュリティ監査を外部の者に委託しようとする場合は、情報セキュリティ委員会の承認を必要とし、外部委託業者の管理については情報セキュリティポリシー等の徹底を図らなければならない。

第２節　自己点検

（１）実施方法

①統括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、すべての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）報告

統括情報セキュリティ責任者、情報セキュリティ責任者及び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、情報セキュリティ委員会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情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、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。

第３節　情報セキュリティポリシー及び関係規程等の見直し

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ふまえ、必要があると認めた場合、情報セキュリティポリシー及び関係規程等について見直しを行うものとする。

附　則

１　この対策基準は、平成２０年６月３０日から施行する。

２　周南市情報セキュリティポリシー（平成１６年１月１日施行）は、廃止する。

附　則

この対策基準は、平成２７年１０月１日から施行する。

附　則

この対策基準は、令和３年２月１９日から施行する。

附　則

この対策基準は、令和５年７月１日から施行する。