米原市情報セキュリティ対策基準

1　目的

米原市情報セキュリティ対策基準（以下「本対策基準」という。）は、米原市情報セキュリティ基本方針を実行に移すため、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。ただし、文部科学省の「教育情報セキュリティポリシーに関するガイドライン」により定めている情報資産の範囲については本対策基準の対象外とする。

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。）

① 副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理および情報セキュリティ対策に関する最終決定権限および責任を有する。

② CISO は、必要に応じ、情報セキュリティに関する専門的な知識および経験を有した専門家をアドバイザーとして置くものとする。

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

④ CISO は、本対策基準に定められた自らの担務を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 電算管理主管部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO を補佐しなければならない。

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

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および責任を有する。

④ 統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、ネットワーク管理者、情報システム管理者およ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および助言を行う権限を有する。

⑤ 統括情報セキュリティ責任者は、本市の情報資産に対する侵害が発生した場合または侵害のおそれがある場合は、CISO の指示に従い、CISO が不在の場合は自らの判断に基づき、必要かつ十分な措置を行う権限および責任を有する。

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

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

⑧ 統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、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 米原市部長会議規程(平成 25 年米原市訓令第 3 号)別表に掲げる職員およびこれに相当する職員ならびに会計管理者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および責任を有する。

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および責任を有する。

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ならびに職員、非常勤職員、会計年度任用職員等（以下「職員等」という。）に対する教育・訓練、助言および指示を行う。

（4）情報セキュリティ管理者

① 米原市事務分掌規則(平成 17 年米原市規則第 9 号)第 5 条第 1 項の規定により配置される課長またはこれに相当する職員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および責任を有する。

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、情報資産に対する侵害が発生した場合または侵害のおそれがある場合は、情報セキュリティ責任者、ネッ

トワーク管理者、統括情報セキュリティ責任者および 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）ネットワーク管理者

① 電算管理主管課長をネットワーク管理者とする。

② ネットワーク管理者は、米原市事務分掌規則(平成 17 年米原市規則第 9 号)第 4 条に規定する課、米原市教育委員会事務局組織規則(平成 22 年米原市教育委員会規則第 1 号)第 3 条に規定する課、議会事務局、監査委員事務局、農業委員会事務局、選挙管理委員会、公平委員会、固定資産評価審査委員会および会計室の事務または事業の用に供する施設の内部または相互間を接続するためのネットワーク（以下「行政情報ネットワーク」という。）ならびに個別に構築するネットワーク（以下「特定ネットワーク」という。）における情報セキュリティに関する統一的な対策を実施する権限および責任を有する。

③ ネットワーク管理者は、ネットワーク、情報システムの技術に関する専門的知識と高い公務員倫理を有し、統括情報セキュリティ責任者を補佐しなければならない。

④ ネットワーク管理者は、権限および責任を有するネットワークに対する重大な侵害または侵害のおそれのある場合は、統括情報セキュリティ責任者の指示に従い、統括情報セキュリティ責任者が不在の場合は自らの判断に基づき、必要かつ十分な全ての措置を行う権限および責任を有する。

（6）情報システム管理者

① 各情報システムの担当課室長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および責任を有する。

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および責任を有する。

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維持・管理を行う。

（7）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新

等の作業を行う者を情報システム担当者とする。

（8）米原新時代デジタルトランスフォーメーション推進本部

本市の情報セキュリティ対策を統一的に行うため、米原新時代デジタルトランスフォーメーション推進本部において、次に掲げる重要な事項を審議する。

① 情報セキュリティポリシーの策定および見直しに関する事項

② リスク分析の実施に関する事項

③ リスク分析の結果に基づく情報セキュリティ対策の実施に関する事項

④ 情報セキュリティの維持・向上のための啓発、研修・訓練に関する事項

⑤ 新しい情報システムまたは新しい情報サービスのための情報セキュリティ対策の評価およびその実施の調整に関する事項

⑥ 情報セキュリティインシデントの原因、対策等についての検討に関する事項

⑦ 情報セキュリティ監査の実施に関する事項

⑧ 緊急時対応計画の策定および見直しに関する事項

⑨ 情報セキュリティ対策を推進するための全体調整に関する事項

（9）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、承認または許可の申請を行う者とその承認者または許可者は、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。

（10）CSIRT の設置・役割

① CISO は、情報セキュリティインシデント発生時に、迅速かつ的確に対応するための体制として、CSIRT を設置する。

② CISO 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 内の業務統括およ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。

③ CISO 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。

④ 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は、CISO、総務省、滋賀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。

3　情報資産の分類と管理方法

（1）情報資産の分類

本市における情報資産は、機密性、完全性および可用性により、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	・支給以外のコンピュータでの作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製および配付禁止 ・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または機密性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、誤びゅうまたは破損により、住民の権利が侵害されるまた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、電子署名付与 ・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、紛失また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また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	・バックアップ、指定する時間以内の復旧 ・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 管理責任

（ア）情報セキュリティ管理者は、作成および所管する情報資産ならびに複製、移送、送信等された情報資産の管理責任を有する。

（イ）職員等は、情報資産の分類に従い利用する責任を有する。

（ウ）職員等は、作成途中等、管理責任が明確でない情報資産は、当該職員等が適切に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（CD-R のラベル等)、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切な管理を行わなければならない。

③ 情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に情報資産の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなけ

ればならない。

④　情報資産の入手

（ア）庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

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

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

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、適切な取扱いをしなければならない。

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

⑥　情報資産の保管

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

（イ）情報セキュリティ管理者また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また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や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性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または情報システム管理者は、機密性２以上、完全性２または可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水および耐湿を講じた施錠可能な場所に保管しなければならない。

⑦　情報の送信

電子メール等により機密性２以上の情報を送信する者は、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）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。

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、情報セキュリティ管理者に許可を得なければならない。

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

⑩　情報資産の廃棄等

（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、その情報の機密性に応じ、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、行った処理について、日時、担当者および処理内容を記録しなければならない。

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

（エ）情報を記録している電磁的記録媒体が不要になった場合、記録されている情報の機密性に応じた電磁的記録媒体の廃棄方法は、次のとおりとする。

分類	機器の廃棄等の方法	確実な履行を担保する方法
（ｉ）マイナンバー利用事務系の領域において住民情報を保存する電磁的記憶媒体	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、あらかじめ仕様に明記の上、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述(ⅲ)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。

（ⅱ）機密性2以上に該当する情報を保存する記憶媒体（上記(ⅰ)に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置またはデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述(ⅲ)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（ⅲ）機密性1に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、(ⅱ)に記述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置またはデータ消去ソフトウェアにより上書き消去する方法がある。 OS および記憶装置の初期化（フォーマット等）による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない。	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。

※上記(ⅰ)は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む。）

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。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)およ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マイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

② 情報のアクセスおよ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、業務ごと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、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。ただし、電磁的記録媒体による端末からの情報持ち出しを行う場合は、次の手段により実施しなければならない。

（a）端末には利用許可された媒体のみ接続可能とし、データ暗号化機能を備えた媒体を使用すること。

（b）データは暗号化しパスワードを設定すること。

（c）利用媒体は、全て管理し利用履歴を残せること。

（d）データの受け渡しには、必ず情報セキュリティ管理者の承認と承認記録を残せること。

（2）LGWAN 接続系

① 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、電子メールやデータを 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、また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および 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 滋賀県および本市含む県内各市町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、関係省庁や滋賀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、ネットワーク基幹機器および情報システム（以下「システム機器」という。）の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（2）サーバの冗長化

情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバおよびその他の基幹サーバを冗長化し、同一データを保持するよう努めなければならない。

（3）機器の電源

① 情報システム管理者は、統括情報セキュリティ責任者および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、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

② 情報システム管理者は、統括情報セキュリティ責任者および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 統括情報セキュリティ責任者および情報システム管理者は、施設管理部門と連携し、通信ケーブルおよ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 統括情報セキュリティ責任者および情報システム管理者は、主要な箇所の通信ケーブルおよ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 統括情報セキュリティ責任者およ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切に管理しなければならない。

④ 統括情報セキュリティ責任者および情報システム管理者は、自らまたは情報システム担当者および契約により操作を認められた委託事業者以外の者が配線を変更、

追加できないように必要な措置を施さなければならない。

（5）機器の定期保守および修理

① 情報システム管理者は、可用性2のサーバ等の機器の定期保守を実施しなければならない。

② 情報システム管理者は、電磁的記録媒体を内蔵する機器を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当たり、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などを行わなければならない。

（6）庁舎外への機器の設置

統括情報セキュリティ責任者および情報システム管理者は、庁舎外に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。

（7）機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

5.2 管理区域（情報システム室等）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および重要な情報システムを設置し、当該機器等の管理ならびに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 統括情報セキュリティ責任者および情報システム管理者は、管理区域を地階または1階に設けてはならない。

③ 統括情報セキュリティ責任者およ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しなければならない。

④ 統括情報セキュリティ責任者および情報システム管理者は、情報システム室内の機器等に、転倒およ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。

⑤ 統括情報セキュリティ責任者および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、機器等およ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）管理区画およびその他の区画の定義

情報システム管理者および施設管理部門は、物理的なスペースを次に掲げる区画に区分し、区画に応じた管理を行うものとする。

レベル	区　分	区画の定義	区画の管理方針
0	一般区画	不特定の人が比較的自由に出入りする区画（ロビー、ローカ等、室のカウンター等の外側）	市民等の利用に係るものを除き、情報システムを設置しない。
1	事務室区画Ⅰ	在室者の許可を得て入退室し、監視する区画（在室者の相互監視が機能する事務室）	情報システムを利用するが、 機密性３の情報を蓄積しない。
2	事務室区画Ⅱ	退室時に施錠されるキャビネット・机・ロッカー等	管理区画で使用する電磁的記録媒体や鍵を管理
3	管理区画	常時施錠され、厳重な入退室管理、室内での作業管理を行う区画 （サーバ室等）	機密性３の情報を蓄積、処理する。

（3）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、IC カード、指紋認証等の生体認証や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 職員等および委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③ 情報システム管理者は、外部からの訪問者が管理区域に入る場合は、必要に応じて立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。

④ 情報システム管理者は、機密性２以上の情報資産を扱う情報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コンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（4）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、あらかじめ職員また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、職員を立ち会わせなければならない。

5.3 通信回線およ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、庁内の通信回線および通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線および通信回線装置に関連する文書を適切に保管しなければならない。

② 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 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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

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。

5.4 職員等の利用するパソコン等の管理

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、モバイル端末は、原則、セキュリティワイヤー等により固定しなければならない。

② 職員等は、セキュリティワイヤー固定されないモバイル端末および電磁的記録媒体の使用時以外は、ロッカー等に保管をする等の措置をとらなければならない。

③ 職員等は、機器を設置、移動または撤去するときは、情報セキュリティ管理者の許可を得なければならない。情報セキュリティ管理者は、機器を設置、撤去するとき、課室等を越えて移動するときは、情報システム管理者の許可を得るものとする。

④ 職員等は、電磁的記録媒体を使用するときは、情報セキュリティ管理者の許可を得

なければならない。

⑤ 電磁的記録媒体について、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。

⑥ 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、ある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。

⑦ 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。

⑧ 電磁的記録媒体については、原則、データ暗号化機能を備えた媒体を使用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

（ア）職員等は、職務上知り得た秘密を他に漏らしてはならない。異動、退職その他の事由により職務を離れた後においても同様とする。

（イ）職員等は、情報セキュリティポリシーおよ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およ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および外部における情報処理作業の制限

（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講じなければならない。

（イ）職員等は、本市のモバイル端末、電磁的記録媒体、情報資産およびソフトウェアを外部に持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

（ウ）職員等は、外部で情報処理業務を行う場合は、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）職員等は、外部で情報処理作業を行う際、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

④ 貸与以外のパソコン、モバイル端末および電磁的記録媒体等の業務利用

（ア）職員等は、貸与以外のパソコン、モバイル端末およ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、貸与以外のパソコンやモバイル端末の業務利用の可否判断を CISO が行った後で、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、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、貸与以外のパソコン、モバイル端末および電磁的記録媒体等を用いる場合は、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際

に安全管理措置を遵守しなければならない。

⑤　持ち出し時および持込み時の記録

情報セキュリティ管理者は、端末装置等の持ち出しおよび持込みについて、記録を作成し、保管しなければならない。

⑥　パソコン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　机上の端末装置等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体およ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、また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、適切な措置を講じなければならない。

⑧　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合は、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、会計年度任用職員等への対応

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、会計年度任用職員等に対し、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、会計年度任用職員等が守るべき内容を理解させ、また、実施およ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、会計年度任用職員等の採用の際、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誓約書への署名を求めるものとする。

③　インターネット接続およ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、会計年度任用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において、インターネットへの接続およ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および実施手順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説明

情報セキュリティ管理者は、ネットワークおよび情報システムの開発・運用・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およびその機密事項を説明しなければならない。

6.2 研修・訓練

（1）情報セキュリティに関する研修・訓練

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

（2）研修計画の策定および実施

① CISO は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、米原新時代デジタルトランスフォーメーション推進本部の承認を得なければならない。

② CISO 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、ネットワーク管理者、情報セキュリティ管理者、情報システム管理者およ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研修を実施しなければならない。

④ CISO は、毎年度 1 回、米原新時代デジタルトランスフォーメーション推進本部に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（3）緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワークおよび各情報システムの重要度、発生確率、影響範囲の大きさ等を考慮し、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。

（4）研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加し、情報セキュリティポリシーおよび実施手順ならびに緊急時対応について理解し、情報セキュリティ上の問題が生じないように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、情報セキュリティに関する事故、システム上の欠陥および誤動作等情報セキュリティインシデントを認知した場合、直ちに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、速やかに統括情報セキュリティ責任者および情報システム管理者ならびに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。

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、CISO および情報セキュリティ責任者に報告しなければならない。

④ 職員等は、情報セキュリティ事故の予兆、疑いまたは脆弱性を発見した場合、速やかにその内容に応じて、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、ネットワーク管理者および情報システム管理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、市が管理するネットワークおよ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、直ちに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、速やかに統括情報セキュリティ責任者およ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 および情報セキュリティ責任者に報告しなければならない。

④ CISO 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、住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するものとする。

（3）情報セキュリティインシデントの原因究明・記録、再発防止等

① 統括情報セキュリティ責任者は、事故等を引き起こした部門の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および情報セキュリティに関する統一的な窓口と連携し、これらの事故等の原因を究明し、記録を保存しなければならない。また、事故原因の究明結果から、再発防止策を検討し、CISO に報告しなければならない。

② CISO は、統括情報セキュリティ責任者から、事故等について報告を受けた場合は、

その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

6.4　ID およびパスワード等の管理

（1）IC カード等の取扱い

① 職員等は、認証に用いる IC カード等を、職員等間で共有してはならない。

② 職員等は、離席、終業等により業務上必要のないときは、IC カード等をカードリーダまた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。

③ 職員等は、IC カード等を紛失した場合は、速やかに統括責任者およびシステム管理者に通報し、指示に従わなければならない。

④ 統括情報セキュリティ責任者およ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。

⑤ 統括情報セキュリティ責任者およ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）ユーザ ID の取扱い

① 職員等は、自己が利用しているユーザ ID は、他人に利用させてはならない。

② 職員等は、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 統括情報セキュリティ責任者および情報システム管理者は、IC カード、ユーザ ID およびパスワードの取扱い違反または事故を発見したとき、ならびに違反または事故の報告を受けたときは、速やかに当該職員等の利用者権限を停止しなければならない。

（3）パスワードの取扱い

① 職員等は、パスワードを他者に知られないように管理しなければならない。

② 職員等は、自己のパスワードを守秘し、パスワードの照会等には一切応じてはならない。

③ 職員等は、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 職員等は、パスワードが流出したおそれがある場合は、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 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥ 仮のパスワードは、最初のログイン時点で変更しなければならない。

⑦ 職員等は、パソコン等の端末のパスワード記憶機能を利用してはならない。

⑧ 職員等は、許可された共用 ID を利用する場合を除き、職員等間でパスワードを共有してはならない。

7　技術的セキュリティ

7.1　コンピュータおよびネットワークの管理

（1）文書サーバの設定等

① 情報システム管理者は、職員等が使用できる文書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、文書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およびファイルを閲覧およ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、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧および使用できないようにしなければならない。

④ 職員等は、電子化された文書については、文書管理等に従った運用を行うものとする。

（ア）公文書としての取扱いおよび管理

（イ）作成途中の文書は適宜バックアップを実施し、安全に保存、保管するものとする。

（ウ）一日の業務終了時には、サーバ等の定められたフォルダに保存するものとする。

（エ）個人情報を含む電子ファイルは、サーバ等の定められたフォルダに保存し、端末装置に保存してはならない。

（2）バックアップの実施

統括情報セキュリティ責任者および情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、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等の交換

情報システム管理者は、他の団体と情報システムに関する情報およ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、統括情報セキュリティ責任者および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）システム管理記録および作業の確認

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

② 統括情報セキュリティ責任者および情報システム管理者は、所管するネットワークおよび情報システムにおいて、変更等の作業を行った場合は、作業内容について

記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③ 統括情報セキュリティ責任者、情報システム管理者、情報システム担当者およ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、2人以上で作業し、互いにその作業を確認しなければならない。

④ 情報システム管理者および情報システム担当者は、委託事業者が実施した作業については、作業報告書によりその作業内容を確認し、作業報告書は適切に保管しなければならない。

（5）情報システム仕様書等の管理

ネットワーク管理者およ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、情報システム運用操作説明書等について、電磁的記録媒体にかかわらず、業務上必要とする者以外の者による閲覧や、紛失等がないよう、適切に管理しなければならない。

（6）アクセス記録（ログ）の取得等

① 統括情報セキュリティ責任者および情報システム管理者は、各種アクセス記録およ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 統括情報セキュリティ責任者および情報システム管理者は、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じるように努めなければならない。

③ 統括情報セキュリティ責任者およ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、取扱方法およ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、適切にログを管理しなければならない。

④ 統括情報セキュリティ責任者および情報システム管理者は、取得したログを定期的に点検また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または分析を実施するように努めなければならない。

（7）障害記録

統括情報セキュリティ責任者および情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果または問題等を、障害記録として記録し、適切に保存しなければならない。

（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および情報システム管理者は、フィルタリングおよ

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

（9）外部の者が利用できるシステムの分離等

統括情報セキュリティ責任者および情報システム管理者は、市民公開端末、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およ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は、CISO およ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。なお、確認を行うに当たっては、必要に応じて統括情報セキュリティ責任者の協力を得ることができる。

③ 情報システム管理者は、接続した外部ネットワークの不適合によりデータの漏えい、破壊、改ざんまた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およ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。

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) 複合機等のセキュリティ管理

① 統括情報セキュリティ責任者は、施設管理部門等が複合機、印刷機等（以下「複合機等」という。）を調達する場合、当該複合機等が備える機能、設置環境ならびに

取り扱う情報資産の分類および管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

② 統括情報セキュリティ責任者は、複合機等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等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 統括情報セキュリティ責任者は、複合機等の運用を終了する場合、複合機等の持つ電磁的記録媒体の全ての情報を抹消また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

統括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実施しなければならない。

(13) 無線 LAN およびネットワークの盗聴対策

① 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および認証技術の使用を義務付けなければならない。

② 統括情報セキュリティ責任者は、機密性の高い情報を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るよう努めなければならない。

(14) 電子メールのセキュリティ管理

① 統括情報セキュリティ責任者は、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。

② 統括情報セキュリティ責任者は、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。

③ 統括情報セキュリティ責任者は、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。

④ 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤ 統括情報セキュリティ責任者は、システム開発や運用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。

⑥ 統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように、添付ファイルの監視等により

システム上の措置を講じなければならない。

（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、情報セキュリティ管理者に報告しなければならない。

（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または完全性を確保することが必要な場合は、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統括情報セキュリティ責任者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。

③ CISO は、電子署名の正当性を検証するための情報または手段を、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またはバージョンアップしてはならない。

② 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者および情報セキュリティ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および情報システム管理者は、ネットワーク、情報システムおよび端末装置への影響ならびにソフトウェアのライセンス（ソフトウェアの使用権をいう。）の許諾状況等を調査の上、その可否を決定するものとする。

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

① 職員等は、パソコンやモバイル端末に対し機器の改造および増設・交換を行ってはならない。

② 職員等は、業務上、パソコンやモバイル端末に対し機器の改造および増設・交換を

行う必要がある場合は、統括情報セキュリティ責任者および情報セキュリティ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

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

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 統括情報セキュリティ責任者は、ウェブアクセスのフィルタリングを行い、不正・不適切なサイトへのアクセスを防止し、アクセス状況を管理するよう努めなければならない。

③ 職員等は、業務上必要なウェブサイトへアクセスできない場合は、統括情報セキュリティ責任者および情報セキュリティ管理者にアクセスの許可を得なければならない。

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切な措置を求めなければならない。

(21) ウェブ会議サービスの利用時の対策

① 統括情報セキュリティ責任者は、ウェブ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、ウェブ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、ウェブ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、外部からウェブ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 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およ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。

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 ウェブサイトに当該情報を掲載して参照可能とすること。

7.2 アクセス制御

（１）アクセス制御等

① アクセス制御

統括情報セキュリティ責任者または情報システム管理者は、所管するネットワークまた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）統括情報セキュリティ責任者およ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、職員等の異動、出向、退職者に伴う IC カードおよびユーザ 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、統括情報セキュリティ責任者および情報システム管理者に通知しなければならない。

（ウ）統括情報セキュリティ責任者および情報システム管理者は、利用されていない IC カードおよびユーザ 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）統括情報セキュリティ責任者および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 を利用する者は 2 人以上の必要最小人数とし、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 およびパスワードを厳重に管理しなければならない。

（イ）統括情報セキュリティ責任者および情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者および情報システム管理者が指名し、CISO が認めた者でなければならない。

（ウ）CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者および情報システム管理者に通知しなければならない。

（エ）統括情報セキュリティ責任者および情報システム管理者は、特権を付与された ID およ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）統括情報セキュリティ責任者および情報システム管理者は、特権を付与された ID およ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を強化しなければならない。

（カ）統括情報セキュリティ責任者およ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 職員等が外部から内部のネットワークまたは情報システムへアクセスする場合は、厳格なセキュリティ対策項目を明確にした上で、統括情報セキュリティ責任者および情報システム管理者の承認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、内部のネットワークまた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。

③ 統括情報セキュリティ責任者は、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。

④ 統括情報セキュリティ責任者は、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。

⑤ 統括情報セキュリティ責任者およ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パソコン等の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 職員等は、持ち込んだまたは外部から持ち帰ったパソコン等の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か、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければなら

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また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、利用者の ID、パスワードおよび生体認証に係る情報等の認証情報ならびにこれを記録した媒体（IC カード等）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。

（3）情報システム処理の制限

端末の操作その他の情報システム処理に従事させる者は、非常勤職員および会計年度任用職員を除く職員とする。ただし、それ以外の者に従事させる必要がある場合は、情報システム管理者は情報セキュリティ責任者の許可を得て、統括情報セキュリティ責任者および情報システム管理者にアクセス権限の設定を依頼するものとする。

（4）利用者の識別と認証

① 情報システム管理者は、個人を識別できる IC カードおよびユーザ ID を使用させるものとする。

② 情報システム管理者は、IC カードおよびユーザ ID の共用が止むを得ないときは、統合情報セキュリティ責任者の許可を得なければならない。

（5）利用者パスワードの付与および変更

① 情報システム管理者は、利用者にパスワードを付与するときは、本人確認を確実に行うものとする。

② 情報システム管理者は、利用者に付与したパスワードは、適宜または定期的に変更することを求めるものとする。

（6）職員等の遵守事項

職員等は、アクセス制御に関して、次の事項を遵守しなければならない。

① 職員等は、許可された権限を越えたアクセスを行ってはならない。

② 職員等は、他人の IC カードおよびユーザ ID を使用してはならない。

③ 職員等は、他人の所有するデータへ無許可でアクセスしてはならない。

（7）自動識別の設定

統括情報セキュリティ責任者および情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末装置とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（8）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、ログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（9）認証情報（パスワード、生体認証情報等）に関する情報の管理

① 統括情報セキュリティ責任者または情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。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。

② 統括情報セキュリティ責任者または情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

③ 統括情報セキュリティ責任者また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。

(10) 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およ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 統括情報セキュリティ責任者およ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。

② 統括情報セキュリティ責任者および情報システム管理者は、機器およ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および作業者の特定

情報システム管理者は、システム開発の責任者およ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、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およ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および作業者のアクセス権限を設定しなければならない。

③ システム開発に用いるハードウェアおよ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および作業者が使用するハードウェアおよ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

① 開発環境と運用環境の分離およ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・保守およ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）情報システム管理者は、システム開発・保守およ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、個人情報およ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）情報システム管理者は、開発したシステムについて受入れテストを行う場合、別々の組織でそれぞれ独立したテストを行わなければならない。

（オ）情報システム管理者は、セキュリティ要求事項が設計され、実装され、試験され

たことを確認しなくてはならない。

（4）システム開発・保守に関連する資料等の保管

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およびシステム関連文書を適切に整備・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切な方法で保管しなければならない。

（5）情報システムにおける入出力データの正確性の確保

① 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能およ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、故意または過失により情報が改ざんされるまた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、また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）システム更新または統合時の検証等

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、移行基準の明確化および更新・統合後の業務運営体制の検証を行わなければならない。

（9）ネットワークおよび情報システムの移行・更新等

① 情報システム管理者は、ネットワークを移行・更新等するときは、復帰が即座に可能な状態にし、その内容に応じたテストを行わなければならない。移行・更新等の作業は、統括情報セキュリティ責任者の承認を得て行い、作業内容は記録・保管しなければならない。

② 情報システム管理者は、情報システムを移行・更新等するときは、復帰が即座に可

能な状態にし、その内容に応じたテストを行わなければならない。移行・更新等の作業は、情報システム管理者双方が確認の下に行い、作業内容は記録・保管しなければならない。

③ 情報システム管理者は、ネットワークおよび情報システムの障害対応手順をまとめ、情報システム担当者に周知しなければならない。

7.4 不正プログラム対策

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

⑤ 不正プログラム対策ソフトウェアのパターンファイルは、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。

① 情報システム管理者は、その所掌するサーバ、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。

② 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。

③ 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。

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に、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、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およびパターンファイルの更新を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、情報システム管理者が許可した職員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 外部からデータまたはソフトウェアを取り入れる場合は、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 差出人が不明また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また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 統括情報セキュリティ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。

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また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 ケーブルの即時取

り外しまたは機器の電源遮断等通信が行えないように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）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、機能を削除また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、統括情報セキュリティ責任者および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 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統一的な窓口と連携し、監視、通知、外部連絡窓口および適切な対応などを実施できる体制なら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 およ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または受けるリスクがある場合、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、滋賀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および情報システム管理者は、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は、攻撃の記録を保存するとともに、警察およ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

統括情報セキュリティ責任者および情報システム管理者は、職員等およ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、適切な処置を求めなければなら

ない。

（6）サービス不能攻撃

統括情報セキュリティ責任者および情報システム管理者は、庁外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

統括情報セキュリティ責任者およ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（内部対策および出口対策）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、ソフトウェアの更新等

統括情報セキュリティ責任者およ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および共有

統括情報セキュリティ責任者およ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 統括情報セキュリティ責任者および情報システム管理者は、ネットワークおよび情報システムを安全かつ安定的に運用し、セキュリティに関する事案を検知するため、監視の範囲および手順を定めるものとする。

② 情報システムの監視およびアクセスログの保管

（ア）統括情報セキュリティ責任者および情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

（イ）統括情報セキュリティ責任者および情報システム管理者は、アクセスログの証拠としての記録の正確性を確保するために、情報システム機器等の正確な時刻設定および時刻同期措置を講じなければならない。

（ウ）統括情報セキュリティ責任者およ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常時監視しなければならない。

（エ）統括情報セキュリティ責任者および情報システム管理者は、夜間および休日のアクセス等、不審なアクセスログを発見したとき、セキュリティ侵害の可能性があるときは、適宜アクセスログの解析を行わなければならない。

（オ）統括情報セキュリティ責任者および情報システム管理者は、ネットワークおよび情報システムの処理能力の妥当性ならびに記憶容量を定期的に検査しなければならない。

（カ）統括情報セキュリティ責任者および情報システム管理者は、アクセスログを盗難、改ざん、消去等から保護するために、必要な措置を講じ、安全な場所に保管しなければならない。

（キ）統括情報セキュリティ責任者およびシステム管理者は、セキュリティ侵害に備え、あらかじめ定めた期間アクセスログを保管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）遵守状況の確認および対処

① 情報セキュリティ責任者およ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、問題を認めた場合は、速やかに CISO およ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 CISO は、発生した問題について、適切かつ速やかに対処しなければならない。

③ 統括情報セキュリティ責任者および情報システム管理者は、ネットワークおよ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は適切かつ速やかに対処しなけ

ればならない。

（2）パソコン、モバイル端末電磁的記録媒体等の利用状況調査

CISO および CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、電磁的記録媒体のアクセス記録、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、直ちに統括情報セキュリティ責任者および情報セキュリティ管理者に報告を行わなければならない。

② 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は、職員等は、緊急時対応計画に従って適切に対処しなければならない。

8.3 セキュリティ侵害時の対応等

（1）対応手順および対応計画の策定

CISO または米原新時代デジタルトランスフォーメーション推進本部は、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への侵害が発生した場合また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、あらかじめ緊急時対応計画を定め、侵害時には当該手順および計画に従って適切に対処しなければならない。

（2） 緊急時対応計画に含める事項

① リスクの識別と対応に関する事項

② 緊急時の対応体制および役割分担に関する事項

③ 緊急時の対応手順（代替処置、復旧処置）に関する事項

④ 発生した事案に係る報告すべき事項

⑤ 再発防止措置の策定

⑥ 緊急時連絡網の整備に関する事項

⑦ 緊急時に使用する情報資産の確保、保管に関する事項

⑧ 緊急時対応訓練の実施に関する事項

（3）事業継続計画との整合性確保

CISO および米原新時代デジタルトランスフォーメーション推進本部は、本市が自然災害等に備えて事業継続計画を策定する場合、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

CISO および米原新時代デジタルトランスフォーメーション推進本部は、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およ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、また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は、CISO の許可を得て、例外措置を取ることができる。

（2）緊急時の例外措置

情報セキュリティ管理者およ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）例外措置の申請書の管理

CISO は、例外措置の申請書および審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

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 米原市個人情報の保護に関する法律施行条例(令和 5 年米原市条例第 2 号)

⑧ 米原市情報公開条例(平成 17 年米原市条例第 4 号)

⑨ 米原市個人番号の利用に関する条例(平成 27 年米原市条例第 41 号)

8.6 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およびその監督責任者に対して、その重大性、発生した事案の状況に応じて地方公務員法、米原市個人情報の保護に関する法律施行条例等の服務規程に基づく罰則を適用する。

（2） 違反時の対応

① 統括情報セキュリティ責任者は、違反の報告を受けたときは、情報システム管理者および情報セキュリティ管理者に事実関係の調査および対応を指示しなければならない。

② 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、適切な措置を求めなければならない。

③ 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およ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、適切な措置を求めなければならない。

④ 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、違反者のネットワークまたは情報システムの使用に関する権利を停止または剥奪できるものとする。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 およ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　業務委託と外部サービスの利用

9.1　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。

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、委託事業者を選定しなければならない。

（2）委託事業者に対して義務付ける事項

情報セキュリティ管理者および情報システム管理者は、委託契約書、覚書、セキュリティ特記仕様書等により、個人情報保護およびセキュリティ確保のための必要な措置を規定し、契約しなければならない。

・情報セキュリティポリシーおよ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、作業者の所属および作業場所の特定

・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およびアクセス方法

・委託事業者の従業員に対する教育の実施

・提供された情報の目的外利用およ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および緊急時報告義務

・市による検査、市または第三者による監査

・市による情報セキュリティインシデント発生時事の公表

・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）委託業務実施状況の管理、監督

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、委託契約書、覚書、セキュリティ特記仕様書等に基づき、措置を講じなければならない。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。

9.2　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、以下の事項を含む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。

① 外部サービスを利用可能な業務および情報システムの範囲ならびに情報の取扱いを許可する場所を判断する基準（以下本節において「外部サービス利用判断基準」という。）

② 外部サービス提供者の選定基準

③ 外部サービスの利用申請の許可権限者と利用手続

④ 外部サービス管理者の氏名と外部サービスの利用状況の管理

（２）外部サービスの選定

① 情報セキュリティ責任者は、取り扱う情報の格付およ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 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付およ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、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および管理体制

（ウ）外部サービスの提供に当たり、外部サービス提供者もしくはその従業員、再委託先また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の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績および国籍に関する情報提供なら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 情報セキュリティ責任者は、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、外部サービス提供者の選定条件に含めること。

④ 情報セキュリティ責任者は、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 情報セキュリティ責任者は、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およ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およ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 情報セキュリティ責任者は、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、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、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およ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 情報セキュリティ責任者は、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、情報セキュリティに関する役割およ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。

⑧ 統括情報セキュリティ責任者は、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、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 情報セキュリティ責任者は、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および選定条件なら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 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者およ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し、調達仕様の内容を契約に含めること。

（4）外部サービスの利用承認

① 情報セキュリティ責任者は、外部サービスを利用する場合は、統括情報セキュリテ

ィ責任者へ外部サービスの利用申請を行うこと。

② 統括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。

③ 統括情報セキュリティ責任者は、外部サービスの利用申請を承認した場合は、承認済外部サービスとして記録し、外部サービス管理者を指名すること。

（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

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等を踏まえ、以下を含む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。

（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止

② 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

（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、以下を含む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。

（ア）外部サービス利用方針の規定
（イ）外部サービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）外部サービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）外部サービスを利用した情報システムの事業継続

② 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。

③ 外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状

況を定期的に確認・記録すること。

（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、以下を含む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。

（ア）外部サービスの利用終了時における対策

（イ）外部サービスで取り扱った情報の廃棄

（ウ）外部サービスの利用のために作成したアカウントの廃棄

② 外部サービス管理者は、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。

9.3 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、以下を含む外部サービス（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。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

（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。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

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。また、承認した外部サービスを記録すること。

10　評価・見直し

10.1　監査

（1）実施方法

米原新時代デジタルトランスフォーメーション推進本部は、情報セキュリティ監査統括責任者を指名し、ネットワークおよ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、定期的にまたは必要に応じて監査を行わせなければならない。

（2）監査を行う者の要件

① 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は、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

② 監査を行う者は、監査および情報セキュリティに関する専門知識を有する者でなければならない。

（3）監査実施計画の立案および実施への協力

① 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、米原新時代デジタルトランスフォーメーション推進本部の承認を得なければならない。

② 監査人は、被監査部門に対して、必要な資料の提出や情報の閲覧を求めることができるものとする。

③ 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監査を定期的にまたは必要に応じて行わなければならない。

（5）監査結果の報告

情報セキュリティ監査総括責任者は、監査結果を取りまとめ、米原新時代デジタルトランスフォーメーション推進本部に報告するものとする。

（6）監査調書等の保管

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切に保管しなければならない。

（7）監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、

当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題および問題点がある可能性が高い場合は、当該課題およ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。

（8）情報セキュリティポリシーおよび関係規程等の見直し等への活用

米原新時代デジタルトランスフォーメーション推進本部は、監査結果を情報セキュリティポリシーおよ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 統括情報セキュリティ責任者および情報システム管理者は、所管するネットワークおよび情報システムについて、定期的にまたは必要に応じ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、毎年度または必要に応じ点検を行わなければならない。

（2）点検結果の報告

統括情報セキュリティ責任者、情報システム管理者および情報セキュリティ責任者は、点検結果と点検結果に基づく改善策を取りまとめ、米原新時代デジタルトランスフォーメーション推進本部に報告しなければならない。

（3）点検結果の活用

① 職員等は、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 米原新時代デジタルトランスフォーメーション推進本部は、この点検結果を情報セキュリティポリシーおよ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。

10.3　情報セキュリティポリシーの見直し

統括情報セキュリティ責任者は、情報セキュリティ監査および点検の結果なら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および関係規程等について毎年度および重大な変化が発生した場合に評価を行い、必要があ

ると認めた場合、改善を行うものとする。

施行日

（1） 本対策基準は、平成 20 年 2 月 1 日から施行する。

（平成 20 年 2 月 1 日ＩＣＴ推進会議承認）

（2） 平成 29 年 7 月 1 日改定

（平成 29 年 6 月 16 日ＩＣＴ推進会議承認）

（3） 平成 30 年 4 月 1 日改定

（平成 30 年 4 月の人事異動に伴う統括情報セキュリティ責任者やネットワーク責任者等の変更および軽微な修正）

（4） 令和 4 年 10 月 3 日改定

（令和 4 年 10 月 3 日米原新時代デジタルトランスフォーメーション推進本部承認）