八尾市情報セキュリティ対策基準

令和６年３月１１日

情報セキュリティ対策基準

情報セキュリティ対策基準とは、八尾市情報セキュリティ規則（以下「規則」という。）を実行に移すための、八尾市の情報資産に関する情報セキュリティ対策の基準であり、対象範囲は規則第３条による。

１．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 CISO は副市長をもって充て、本市におけるネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最高責任者とする。

② 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：ComputerSecurity Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

③ CISO を補佐し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、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。）を必要に応じて置くことができる。

④ CIO 補佐官は「八尾市デジタル戦略推進本部設置要綱（以下「本部要綱」という。）に基づいた内容で CISO を補佐する。

⑤ 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等に担わせることができる。

（２）情報システム・セキュリティ統括責任者等

① 政策企画部長及び CIO 補佐官を置いている場合は CIO 補佐官を本部要綱に基づいた内容で、CISO 直下の情報システム・セキュリティ統括責任者（以下「システム等統括責任者」という。）とし、CISO を補佐及び副 CISO を置いている場合は副 CISO を補佐しなければならない。

② システム等統括責任者は、本市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 システム等統括責任者は、本市の ICT 関連施策の総合的な推進及び八尾市デジタル戦略推進本部で取り扱った案件も含めて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 システム等統括責任者は、本対策基準に定める責任者等に対して、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。

⑤ システム等統括責任者は、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。

⑥　システム等統括責任者は、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・管理を行う権限及び責任を有する。

⑦　システム等統括責任者は、緊急時等の円滑な情報共有を図るため、緊急連絡網を整備するものとする。

⑧　システム等統括責任者は、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。

⑨　システム等統括責任者は、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または八尾市デジタル戦略推進本部等にその内容を報告しなければならない。

⑩　システム等統括責任者の事務の一部を取り扱わせるため、情報システム・セキュリティ統括管理者（以下「システム等統括管理者」という。）を置き、政策企画部デジタル戦略課長をもって充てる。

（3）情報システム・セキュリティ責任者

①　外部サービスを含む情報システム又はその一部を使用する課等を所管する部局等に情報システム・セキュリティ責任者（以下「システム等責任者」という。）を置き、その部局等の長をもって充てる。

②　システム等責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

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

（4）情報システム・セキュリティ管理者等

①　外部サービスを含む情報システム又はその一部を使用する課等に情報システム・セキュリティ管理者（以下「システム等管理者」という。）を置き、使用する課等の長をもって充てる。

②　システム等管理者は、所管す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。

③　システム等管理者は、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。

④　システム等管理者は、所管する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、システム等責任者、システム等統括管理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　システム等管理者は、所管する課等の職員のうちから、情報システムを設置する部屋・施設等ごとに情報システム管理主任（以下「管理主任」という。）を指名する。

⑥　管理主任は、システム等管理者の指示を受け、情報システムの開発、設定の変更、運用、更新等の作業を行い、情報システムの管理及び情報システムの操作が適正に行われるよう努めなければならない。

（５）八尾市デジタル戦略推進本部等

① 情報資産の適正かつ効率的な管理運営を行うため、八尾市情報セキュリティ規則及び本対策基準（以下「情報セキュリティポリシー」という。）等、本市の情報セキュリティに係る重要な事項については、本部要綱に基づき、八尾市デジタル戦略推進本部及び八尾市デジタル戦略推進委員会（以下「本部等」という。）において取り扱う。

（６）兼務の禁止

① 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。

② 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。

（７）CSIRT の設置・役割

① CISO は、CSIRT を整備し、その役割を明確化しなければならない。

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。

③ 情報セキュリティインシデントに関する統一的な窓口については、デジタル戦略課がこれを担うものとする。部局等は、情報セキュリティインシデントが発生した場合には、デジタル戦略課に報告し、デジタル戦略課は、その状況を確認し CISO に報告する。

④ デジタル戦略課は、CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

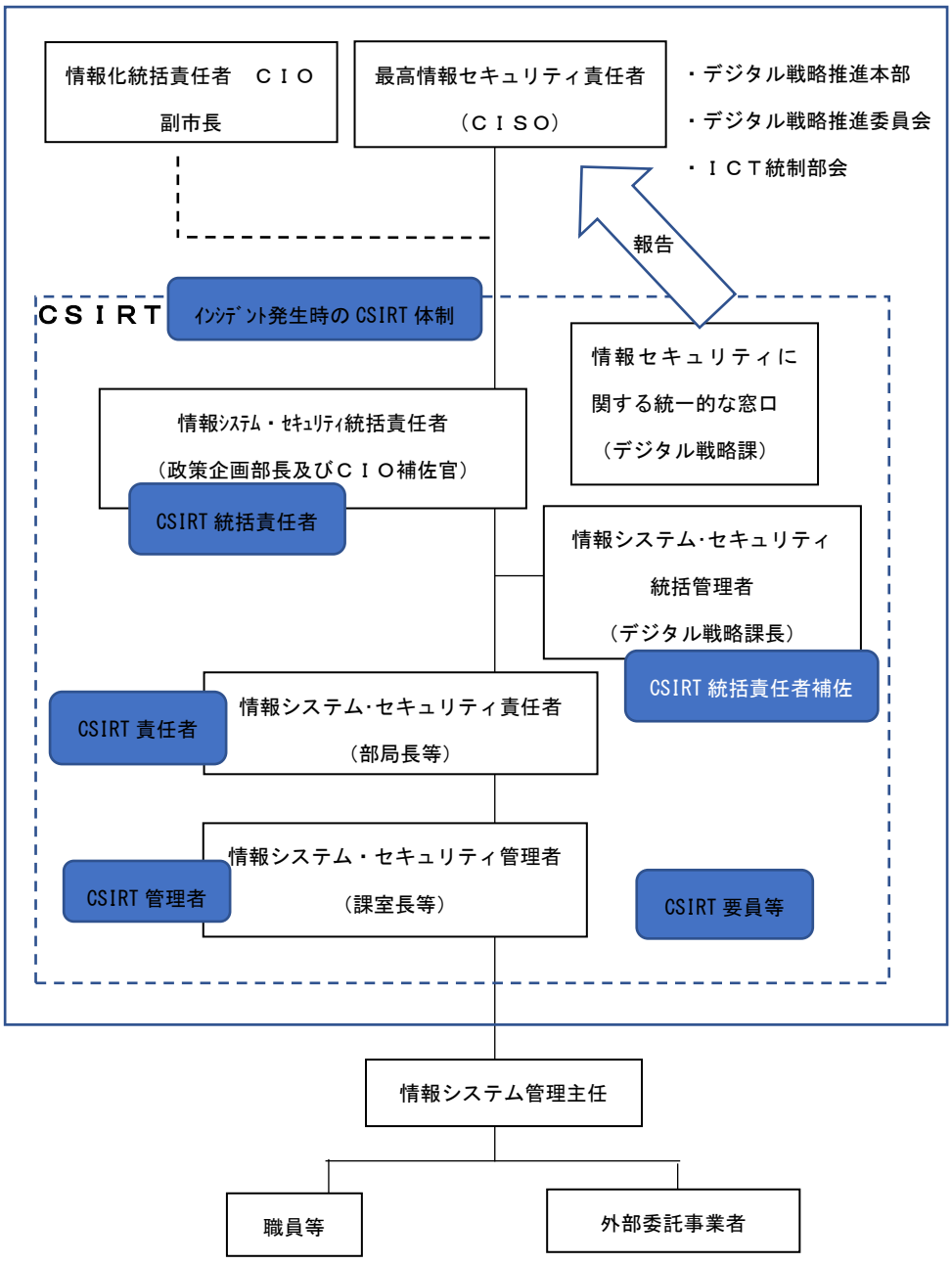
⑤ 情報セキュリティインシデントを認知した場合には、CISO、総務省、大阪府等へ報告しなければならない。

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、必要に応じて広報担当課と協議の上公表するものとする。

⑦ デジタル戦略課は、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

（８）クラウドサービス利用における組織体制

① システム等管理者は、クラウドサービスを利用する際には、当該事業者への問い合わせ等によって、クラウドサービスプロバイダやアプリケーションサービスプロバイダ等、複数の事業者の存在があるかを確認し、複数の事業者が存在する場合は、それぞれの責任の所在確認及び必要な連絡体制を構築しなければならない。また、クラウドサービス利用においては、「八尾市外部サービスの利用に関する基準」に準じて行うこととする。


情報化統括責任者　ＣＩＯ
副市長
最高情報セキュリティ責任者
（ＣＩＳＯ）
・デジタル戦略推進本部
・デジタル戦略推進委員会
・ＩＣＴ統制部会
報告
ＣＳＩＲＴ
ｲﾝｼﾃﾞﾝﾄ発生時の CSIRT 体制
情報ｼｽﾃﾑ・ｾｷｭﾘﾃｨ統括責任者
（政策企画部長及びＣＩＯ補佐官）
CSIRT 統括責任者
情報セキュリティに
関する統一的な窓口
（デジタル戦略課）
情報システム･セキュリティ
統括管理者
（デジタル戦略課長）
CSIRT 統括責任者補佐
CSIRT 責任者
情報システム･セキュリティ責任者
（部局長等）
CSIRT 管理者
情報システム・セキュリティ管理者
（課室長等）
CSIRT 要員等
情報システム管理主任
職員等
外部委託事業者

２.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	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性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	・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	・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)システム等管理者は、その所管する情報資産について管理責任を有する。

（イ）システム等管理者は、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）システム等管理者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、特に住民情報等、機密性等の高い情報資産について、クラウドサービスとして新たに利用する場合は、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、特に住民情報等、重要な情報資産についてはサービス利用前に文書等での提示を求め、又は公開されている内容を確認しなければならない。

②　情報資産の分類の表示

職員等は、情報資産の分類を確認し、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。

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（１）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、（１）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、システム等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、情報資産の分類基準について判断が異なる可能性がある場合は、最高度の分類に従って取り扱わなければならない。

⑥　情報資産の保管

（ア）システム等管理者は、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)システム等管理者は、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)システム等管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、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、システム等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、システム等管理者に許可を得なければならない。

(ウ)システム等管理者は、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、担当者及び処理内容を記録しなければならない。

(ウ)情報資産の廃棄やリース返却等を行う者は、システム等管理者の許可を得なければならない。

(エ)クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう、クラウドサービス事業者に確認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）マイナンバー利用事務系

①　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。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。

③ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

④ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

（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、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

② LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

（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 府内市町村のインターネットとの通信を集約する大阪版自治体情報セキュリティクラウドに参加するとともに、関係省庁や大阪府と連携しながら、情報セキュリティ対策を推進しなければならない。

③ 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる入札情報や職員の情報といった重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、事前に八尾市デジタル戦略推進委員会専門部会であるＩＣＴ統制部会（以下「部会」という。）に諮り承認を得なければならない。また、配置後も定期的に外部監査を実施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

システム等管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（２）機器の電源

① システム等管理者は、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 システム等管理者は、サーバ等の機器を、落雷等による過電流に対して保護できる場所に原則設置すること。

（３）通信ケーブル等の配線

① システム等統括管理者は、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、可能な限り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 システム等統括管理者及びシステム等管理者は、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。

③　システム等統括管理者及びシステム等管理者は、可能な限り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しづらいよう、職員等の目の届く場所に設置する等適正に管理しなければならない。

④　システム等統括管理者及びシステム等管理者は、自ら又は情報システムを所管する職員等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。

（４）機器の定期保守及び修理

①　システム等管理者は、可用性２の情報資産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。

②　システム等管理者は、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、システム等管理者は、事業者に故障を修理させるにあたり、職員等の監視下で修理をさせるか、修理を委託する事業者との間で、修理の際に知り得た情報について守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（５）庁外への機器の設置

システム等管理者は、庁外にサーバ等の機器を設置する場合、事前に部会に諮り承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（６）機器の廃棄等

①　システム等管理者は、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。

②　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする場合は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、それらの提出を求めるなどの確認をしなければならない。

4.2 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（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

②　管理区域から外部に通ずるドアは必要最小限とし、施錠設備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。

また、施錠設備に関連する鍵、カード等（以下「カード等」という。）は適正に管理

しなければならない。

③　サーバ室内の機器等については、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

④　管理区域に配置する消火薬剤や消防用設備等は、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）管理区域の入退室管理等

①　管理区域への入退室は許可された者のみに制限し、カード等、静脈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　職員等及び外部委託事業者等は、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　システム等管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添い又は許可を得るものとし、ネームプレートの着用等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　システム等管理者は、機密性２以上の情報資産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、電磁的記録媒体等を持ち込ませないようにしなければならない。

ただし、当該情報システムの対応に関連する場合の当該機器等の持ち込みについては、事前にシステム等管理者の了解を得た場合はこの限りではない。

（3）機器等の搬入出

①　システム等管理者は、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外部委託事業者等に確認を行わせなければならない。

②　システム等管理者は、サーバ室の機器等の搬入出について、職員を立ち会わせなければならない。

4.3 通信回線及び通信回線装置の管理

①　システム等統括管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。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　システム等統括管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③　システム等統括管理者は、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。

④　システム等統括管理者は、ネットワークに使用する回線について、伝送途上に情報が

破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤　システム等統括管理者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

4.4 職員等の利用する端末や電磁的記録媒体等の管理

①　システム等管理者は、盗難防止のため、執務室等で利用する端末等機器のうち常設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　システム等管理者は、情報システムへのログインに際し、パスワード、特に住民情報等を取り扱う場合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　システム等管理者はシステム等統括管理者と連携して、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。

５．人的セキュリティ

5.1 職員等の遵守事項

（１）職員等の遵守事項

①　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかにシステム等管理者に相談し、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　端末機等及び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)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（以下「外部情報処理」という。）する場合は、部会に諮って承認を得なければならない。

(イ)職員等は、端末機等及び電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、システム等管理者の許可を得なければならない。

(ウ)職員等は、外部で情報処理を行う場合には、システム等管理者の許可を得なければならない。

④　支給以外の端末機等及び電磁的記録媒体等の業務利用

職員等は、支給または市が調達した以外の端末機等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、システム等管理者の許可を得て、システム等統括管理者の定める手順に従い利用することができる。

⑤　持ち出し及び持ち込みの記録

システム等管理者は、端末機等の持ち出し及び持ち込みについて、それに係る記録や申請書等を保管しなければならない。

⑥　端末機等におけるセキュリティ設定変更の禁止

職員等は、端末機等のソフトウェアに関するセキュリティ機能の設定をシステム等管理者の許可なく変更してはならない。

⑦　机上の端末等の管理

職員等は、端末機等、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又はシステム等管理者の許可なく情報を閲覧されることがないように、離席時の端末機等のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

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。

⑨　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

（2）会計年度任用職員及び臨時的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

システム等管理者は、会計年度任用職員及び臨時的任用職員等に対し、必要に応じて情報セキュリティポリシー等のうち、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

システム等管理者は、会計年度任用職員及び臨時的任用職員等に対して、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

システム等管理者は、会計年度任用職員及び臨時的任用職員等に端末機等による作業を行わせる場合において、業務上インターネットへの接続及び電子メールの使用等が必要な場合に限り、利用を認めるものとする。

（3）情報セキュリティポリシー等の掲示

システム等統括管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

（4）委託事業者に対する説明

システム等管理者は、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・訓練

（1）情報セキュリティに関する研修・訓練

① システム等統括管理者は人事研修担当と連携して、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 上記①にはクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練も含む。またシステム等管理者は委託先を含む関係者については委託先等で教育、訓練が行われていることを、報告等を求める等、確認しなければならない。

（2）研修計画の策定及び実施

① システム等統括管理者は、職員等に対する情報セキュリティに関する研修を、職員研修計画に基づいて実施し、必要に応じて本部等に実施計画について報告するものとする。

② 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、職員等に対して情報セキュリティに関する理解度を高めるためのものにしなければならない。

④ システム等統括管理者は、研修の実施状況を分析し、必要に応じて本部等に情報セキュリティ対策に関する研修の実施状況について報告するものとする。

（3）緊急時対応訓練

システム等管理者は、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。また、システム等統括管理者は訓練計画を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

職員等は研修・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

職員等は、情報セキュリティインシデント（クラウドサービス利用における情報セキュリティインシデント含む）を認知した場合、速やかに「７．３侵害時の対応等」で策定が定められている八尾市情報セキュリティ緊急時対応計画（以下、「緊急時対応計画」という。）に従い適正に対処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通報等

① 職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から通報等を受けた場合、速やかに緊急時対応計画に従い適正に対処しなければならない。

② システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

（3）情報セキュリティインシデントの対処

CSIRT は報告のあった事故等について、緊急時対応計画に従い、報告・公表・事後対応等を含めて適正に対処しなければならない。

5.4ID 及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、自己の管理するカード等に関し、次の事項を遵守しなければならない。

(ア)認証に用いるカード等を、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、カード等をカードリーダ又は端末等の機器のスロット等から抜いておかなければならない。

(ウ)カード等を紛失した場合には、速やかにシステム等管理者及びカード等所管部署に報告し、指示に従わなければならない。

② システム等管理者及びカード等所管部署は、カード等の紛失等の報告を受け次第、当該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。

③ システム等管理者及びカード等所管部署は、カード等を切り替える場合、切替え前のカード等を回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2）ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

① 自己が利用している ID は、他人に利用させてはならない。

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

（3）パスワードの取扱い

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

① パスワードは、他者に知られないように管理しなければならない。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③ パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

④ パスワードが流出したおそれがある場合には、当該システム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（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。

⑦　サーバ、ネットワーク機器及び住民情報系等の端末にパスワードを記憶させてはならない。

⑧　職員等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

①　システム等管理者は、職員等が使用できる文書サーバの容量を適切に設定しなければならない。

②　システム等管理者は、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　システム等管理者は、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、システム上可能な限り別途 ID 管理や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努めなければならない。

（２）バックアップの実施

①　システム等管理者は、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。

②　システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合で、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者に必要なバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、技術的課題等を鑑み、可能な限り、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（３）他団体との情報システムに関する情報等の交換

システム等管理者は、他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ことが必要となった場合、必要に応じて部会に諮るものとする。

（４）システム管理記録及び作業の確認

①　システム等管理者は、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　システム等管理者は、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。

③　契約等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、作業ミスがないように努めなければならず、システム等管理者は不備、不正等が発生しないよう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

システム等管理者は、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したり、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

①　システム等管理者は、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。

②　システム等管理者は、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も踏まえた上で、適正にログを管理しなければならない。

③　システム等管理者は、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取得したログの点検又は分析を実施しなければならない。なお、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合は、クラウドサービス事業者が収集し、保存するログを含む記録に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、ログ等に関する保護が実施されているのか確認しなければならない。

④　システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合は、監査及びデータ調査分析技術に必要となる、クラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（7）障害記録

システム等管理者は、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　システム等管理者はシステム等統括管理者と連携して、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　システム等管理者はシステム等統括管理者と連携して、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

システム等管理者はシステム等統括管理者と連携して、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 システム等管理者は、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、必要に応じて部会に諮らなければならない。

② システム等管理者はシステム等統括管理者と連携して、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ システム等管理者は、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 システム等管理者はシステム等統括管理者と連携して、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する等、安全対策をしなければならない。

⑤ システム等管理者は、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、システム等統括管理者と連携して、速やかに当該外部ネットワークの遮断等の対応をしなければならない。

（１１）複合機のセキュリティ管理

① システム等管理者はシステム等統括管理者と連携して、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、適正な対策を講じなければならない。

② システム等管理者はシステム等統括管理者と連携して、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。

③ システム等管理者はシステム等統括管理者と連携して、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

システム等管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１３）無線 LAN 及びネットワークの盗聴対策

① システム等管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用等の措置を講じなければならない。

② システム等管理者はシステム等統括管理者と連携して、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

① システム等統括管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② システム等統括管理者は、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、必要に応じてメールサーバの運用停止等、速やかに対応しなければならない。

③ システム等統括管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ システム等統括管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤ システム等管理者は、システム開発や運用、保守等のため庁舎内に常駐している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を転送してはならない。ただし、危機管理に関する所管部署において全国瞬時警報システムといった、特に市民の安全を脅かすおそれがあり且つ緊急を要するものに限り、転送を行うことができる。その場合、所管のシステム等管理者からの依頼に基づき、システム等統括管理者が設定を行う。

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、BCC 機能を利用する等、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、速やかにシステム等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、情報資産の重要度により、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、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は暗号のための鍵を適正に管理しなければならない。

③ システム等管理者は、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、供用された端末等の機器に対して、システム等統括管理者の許可がないソフトウェアの導入を行ってはならない。

② 職員等は、業務上の必要があり、または業務を円滑に遂行するために必要なソフトウェアについては、合理的理由のある場合、かつシステム等統括管理者の事前の了解を得た場合に限り、利用することができる。なお、導入する際、必要に応じてシステム等管理者は、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

① 職員等は、端末等の機器に対し機器の改造及び増設・交換を行ってはならない。

② 職員等は、業務上、端末等の機器に対し改造及び増設・交換を行う必要がある場合には、必要に応じて部会に諮り許可を得るか、またはシステム等統括責任者及びシステム等統括管理者の事前の了解を得た場合に限り、それらを行うことができる。

（１９）業務外ネットワークへの接続の禁止

① 職員等は、供用された機器等端末を、有線・無線を問わず、部会で得た許可等、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 システム等統括管理者は、支給した端末等機器について、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 システム等統括管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、システム等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 （非公開）

② 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。

（２２）ソーシャルメディアサービスの利用

① システム等管理者は、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（ハードディスク、電磁的記録媒体、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、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。

6.2 アクセス制御

（１）アクセス制御等

① アクセス制御

システム等統括管理者又はシステム等管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

利用者 ID の取扱い

(ア)システム等統括管理者又はシステム等管理者は、所管する情報システム利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID を厳重に取扱わなければならない。

(イ)職員等は、人事異動等以外で業務上情報システム利用の必要がなくなった場合は、利用者登録を抹消するよう、当該情報システムを所管するシステム等管理者等に通知しなければならない。

(ウ)システム等統括管理者又はシステム等管理者は、利用されていない ID が放置されないよう、定期人事異動時等の人事情報を基に、適時点検しなければならない。

② 特権を付与された ID の管理等

(ア)システム等統括管理者又はシステム等管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(イ)システム等統括管理者又はシステム等管理者の特権を代行する者は、それぞれが指名した者でなければならない。

(ウ)システム等統括管理者又はシステム等管理者の特権を代行する者は、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。

(エ)システム等統括管理者及びシステム等管理者は、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)システム等統括管理者及びシステム等管理者は、特権を付与された ID 及びパスワー

ドについて、必要に応じてパスワードの定期変更を増やすなど、セキュリティ上の管理を強化しなければならない。

(カ)システム等統括管理者及びシステム等管理者は、特権を付与されたIDを速やかに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 職員等が外部から本市のメールを参照するためにアクセスする場合は、システム等統括管理者の許可を得なければならない。

② （非公開）

（3）ログイン時の表示等

システム等統括管理者又はシステム等管理者は、所管するシステムにおい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及びログイン・ログアウト時刻の表示等、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に努めなければならない。

（4）認証情報の管理

① システム等統括管理者又はシステム等管理者は、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 システム等統括管理者又はシステム等管理者は、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、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。

③ システム等統括管理者又はシステム等管理者は、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

システム等統括管理者又はシステム等管理者は、所管するシステムにおいて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となるよう努めなければならない。

6.3 システム開発、導入、保守等

（1）情報システムの調達

① システム等管理者は、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 システム等管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（2）情報システムの開発

① システム開発における責任者及び作業者の特定

システム等管理者は、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、全体スケジュールや進捗管理方法をはじめ、システム開発のための各種事項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)システム等管理者は、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)システム等管理者は、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させる等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)システム等管理者は、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)システム等管理者は、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 移行手順の明確化

(ア)システム等管理者は、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・保守計画の策定時や適時、手順を確認する等しなければならない。

(イ)システム等管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(ウ)システム等管理者は、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)システム等管理者は、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)システム等管理者は、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)システム等管理者は、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)システム等管理者は、開発したシステムについて受け入れテストを行う場合、開発ベンダ等と導入する担当部署が、それぞれ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 システム等管理者は、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 システム等管理者は、テスト結果を一定期間保管しなければならない。

③　システム等管理者は、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　システム等管理者は、情報システムに入力されるデータについて、技術的課題等を鑑み、可能な限り、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　システム等管理者は、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、技術的課題等を鑑み、可能な限り、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　システム等管理者は、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するかさせなければならない。

（６）情報システムの変更管理

システム等管理者は、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させる等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

システム等管理者は、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

システム等管理者は、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）システム等統括管理者又はシステム等管理者の措置事項

システム等統括管理者又はシステム等管理者は、不正プログラム対策として、次の事項を措置しなければならない。

①　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④　所掌するサーバ及びパソコン等の端末に、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、技術的課題等を鑑み、可能な限り、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するソフトウェアについては更新や運用方法、切り替え等を検討する必要がある。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。

⑧　所掌するサーバ及び端末等機器、コンピュータウイルス等の不正プログラム対策を実施しなければならない。

⑨　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。

⑩　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、限られた職員のみが行うこと。

⑪　仮想サーバ等を設定する際には不正プログラムへの対策を実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか必要に応じてクラウドサービス事業者に報告を求めなければならない。

（２）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　端末等機器において、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やデータの無害化を行わなければならない。

③　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、速やかにデジタル戦略課に連絡する。

④　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。

⑤　コンピュータウイルス等の不正プログラムに感染した場合若しくは感染が疑われる場合又は検知した場合は、該当の端末等機器において LAN ケーブルの即時取り外しを行う等、通信を行わない措置を行い、速やかにシステム等管理者及びデジタル戦略課に報告しなければならない。

（４）外部組織等の支援体制

システム等統括管理者又はシステム等管理者は、所管するシステムにおいて不測の事態に備え、必要に応じて委託業者及び外部組織等の支援を受けられるように準備しなければならない。

6.5 不正アクセス対策

（１）システム等統括管理者の措置事項

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

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ システム等管理者に対し、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、パターンファイルを検出するような不正アクセス対策等を講じさせなければならない。

（２）システム等管理者の措置事項

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

① 本市情報セキュリティポリシーにおけるアクセス制御に関する事項が、クラウドサービス又はクラウドサービス事業者の提供機能等により実現できるのか、クラウドサービス事業者に確認しなければならない。

② 特に住民情報等、重要な資産について、クラウドサービスを新たに利用する場合で、委託事業者等に管理権限を与える場合、可能な限り多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

③ パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等について、本市情報セキュリティポリシーを遵守させなければならない。

（３）攻撃への対処

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、大阪府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。

（４）記録の保存

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。

（５）内部からの攻撃

システム等統括管理者は、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。

（６）職員等による不正アクセス

職員等は、不正アクセスを発見した場合は、所管するシステム等管理者に通知し、適正な処置を求めなければならない。

（７）サービス不能攻撃

システム等統括管理者は、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。

（８）標的型攻撃

システム等統括管理者は、標的型攻撃による内部への侵入を防止するために、研修実施等、人的対策を講じなければならない。また、技術的課題等を鑑み、可能な限り、標的型攻撃による様々な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

① システム等統括管理者及びシステム等管理者は、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た対策を実施しなければならない。

② システム等管理者は、特に住民情報等、重要な資産について新たに利用する場合の、クラウドサービスに影響し得る技術的脆弱性の管理内容については、クラウドサービス事業者に対して情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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

システム等統括管理者は、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、メール等によって庁内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

システム等統括管理者及びシステム等管理者は、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。

７．運用

7.1 情報システムの監視

① システム等管理者は、セキュリティに関する事案を検知するため、常に情報システムを監視しなければならない。

② システム等管理者は、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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならな

い。

③　システム等管理者は、外部と常時接続するシステムについては、ネットワーク侵入監視装置の設置等で常時監視しなければならない。

④　システム等管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑤　システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合は、イベントログ取得機能の提供があるかを確認し、クラウドサービス事業者からログ取得機能が提供されない場合は、その代替手段を検討しなければならない。当該機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑥　システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合で、重大なインシデントに繋がるおそれのある以下の重要な操作に関して、クラウドサービス事業者に対して手順等を確認しなければならない。

(ア)サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

(イ)クラウドサービス利用の終了手順

(ウ)バックアップ及び復旧

7.2 情報セキュリティポリシーの遵守状況の確認

（1）遵守状況の確認及び対処

①　システム等管理者は、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、速やかにシステム等統括責任者及びシステム等統括管理者に報告しなければならない。

②　システム等統括責任者は、発生した問題に係るセキュリティポリシーの遵守や改正について、適正かつ速やかに対処しなければならない。

③　システム等統括管理者及びシステム等管理者は、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）端末等機器及び電磁的記録媒体等の利用状況調査

システム等統括責任者又はシステム等統括管理者が指名した者は、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端末等機器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、直ちにシステム等統括管理者及びシステム等管理者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システム等統括責任者又はシステム等統括管理者が判断した場合は、適正かつ速やかに対処しなければならない。

7.3 侵害時の対応等

（1）緊急時対応計画の策定

① CISO 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 システム等管理者は、特に住民情報等、重要な資産について、クラウドサービスとして新たに利用する場合は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスのセキュリティ侵害時に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。

（2）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

① 関係者の連絡先

② 発生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

（3）業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えた別途業務継続計画と、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 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。

7.4 例外措置

（1）例外措置の許可

システム等管理者は、情報セキュリティポリシー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、システム等統括責任者又はシステム等統括管理者と協議の上、適切な措置を講じなくてはならない。

緊急の対応が必要でない場合は、事前に部会に諮ったうえで適切な措置を講じなくてはならない。

（2）緊急時の例外措置

システム等管理者は、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、速やかにシステム等統括責任者又はシステム等統括管理者に報告しなければならない。

（３）例外措置の管理

システム等統括責任者又はシステム等統括管理者は、例外措置の内容について、必要な措置を含めて適時状況を確認しなければならない。

7.5 法令遵守

（１）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 八尾市個人情報の保護に関する法律施行条例施行規則（令和 5 年 3 月 28 日規則第 8 号）
⑧ その他業務上制約を受ける条例

（２）システム等管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

7.6 違反時の対応等

（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なる場合がある。

（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 システム等統括責任者又はシステム等統括管理者が違反を確認した場合は、当該職員等が所属するシステム等管理者に通知し、適正な措置を求めなければならない。
② システム等管理者等が違反を確認した場合は、速やかにシステム等統括責任者又はシステム等統括管理者に通知し、適正な措置を求めなければならない。
③ システム等管理者の指導によっても改善されない場合、システム等統括責任者又はシステム等統括管理者は、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、職員等の権利を停止あ

るいは剥奪した旨を当該職員等が所属する課室等のシステム等管理者及び必要に応じてCISOに通知しなければならない。

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

システム等管理者は、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）契約項目

重要な情報資産を取扱う業務を委託する場合には、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
- 通信速度及び安定性等、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、調査等
- 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

システム等管理者は、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確認し、必要に応じて(２)の契約に基づいた措置を実施しなければならない。また、必要に応じてその内容をシステム等統括責任者又はシステム等統括管理者に報告しなければならない。報告を受けたシステム等統括責任者又はシステム等統括管理者は、その重要度に応じて本部等又は部会に報告しなければならない。

8.2 外部サービスの利用

事業者等の本市の外部の組織が、情報システムの一部又は全部の機能を提供するサービスの利用については、「八尾市外部サービスの利用に関する基準」に基づいて行うこととする。

なお、クラウドサービス利用についても本基準に準ずるものとする。

９．評価・見直し

9.1 監査

（１）実施方法

CISO は、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

① 監査を行う者は、1 組織体制(6)兼務の禁止②を踏まえたうえで、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 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。

（３）監査実施計画の立案及び実施への協力

① 監査を行うに当たって、監査実施計画を立案しなければならない。

② 被監査部門は、監査の実施に協力しなければならない。

（４）委託事業者に対する監査

① 事業者に業務委託を行っている場合、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必要に応じて行わなければならない。

② 特に住民情報等、重要な資産について、クラウドサービスとして利用している場合は、クラウドサービス事業者が定める情報セキュリティポリシーの遵守について、監査を必要に応じて行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する第三者認証等の証明書や監査報告書等をこの証拠とすることもできる。

（５）報告

監査実施後は結果を取りまとめ、本部等に報告する。

（６）保管

CISO は、システム等統括責任者又はシステム等統括管理者に対して、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させなければならない。

（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システム等管理者に対し、当該事項への対処をさせなければならない。また、指摘事項を所管していないシステム等管理者に対しても、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。なお、庁内で横断的に改善が必要な事項については、システム等統括責任者に対し、当該事項への対処をさせなければならない。

（８）情報セキュリティポリシー及び関係規程等の見直し等への活用

監査結果については、情報セキュリティポリシー等の見直し、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。

9.2 自己点検

（1）実施方法

① システム等管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施し、システム等統括管理者に報告しなければならない。

② システム等管理者は、所管する課・室等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い、システム等統括管理者に報告しなければならない。

（2）報告

システム等統括責任者又はシステム等統括管理者は、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、本部等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 この点検結果を情報セキュリティポリシー等の見直し、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。

9.3 情報セキュリティポリシー及び関係規程等の見直し

システム等統括責任者又はシステム等統括管理者は、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等に新たに必要な対策が発生した場合には改善を行い、情報セキュリティポリシー等の維持及び運用に努めなければならない。