守口市門真市消防組合情報セキュリティ対策基準

本対策基準は、守口市門真市消防組合情報セキュリティ基本方針を実行に移すための、守口市門真市消防組合（以下「本消防組合」という。）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。

第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) 消防長をCISOとする。

(2) CISOは、本消防組合における全てのネットワーク、情報機器等及び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。

2　統括管理者

(1) 統括管理者は、総務課長をもって充てる。

(2) 統括管理者は、本消防組合における全てのネットワーク、情報機器等及び情報システム等の情報資産を統括的に管理運営する。

(3) 統括管理者は、適正な管理運営を図るため、必要な調査及び指導を行うとともに、管理運営に関する事務の改善に努めなければならない。

(4) 統括管理者は、CISOを補佐しなければならない。

(5) 統括管理者は、本消防組合における全てのネットワーク、情報機器等及び情報システム等の情報資産の情報セキュリティ対策に関する権限及び責任を有し、統括を行う。

(6) 統括管理者は、本消防組合における全てのネットワーク、情報機器等及び情報システム等の情報資産における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

(7) 統括管理者は、本消防組合における全てのネットワーク、情報機器等及び情報システム等の情報資産における開発、設定の変更、運用、見直し及び情報セキュリティ対策を推進し、情報機器等運営管理責任者に対し、指導及び助言を行う権限及び責任を有する。

(8) 統括管理者は、本消防組合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。

(9) 統括管理者は、本消防組合における共通的なネットワーク、情報機器等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実施手順の維持・管理を行う権限及び責任を有する。

(10)統括管理者は、緊急時等の円滑な情報共有を図るため、CISO、情報機器等管理運営責任者、情報機器等管理責任者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

(11)統括管理者は、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。

(12)統括管理者は、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。

3　情報機器等管理運営責任者

(1) 情報機器等管理運営責任者は、課長をもって充てる。要綱第4条において課長の職務が「管理運営」と規定されていることから、その職名を「情報機器等管理運営責任者」とする。

(2) 情報機器等管理運営責任者は、所属職員を指揮監督し、その課における情報機器等、情報システム等の情報資産を適正に管理運営しなければならない。

(3) 情報機器等管理運営責任者は、所管する課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。

(4) 情報機器等管理運営責任者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

(5) 情報機器等管理運営責任者は、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等に対する教育、訓練、助言及び指示を行う。

4　情報機器等管理責任者

(1) 課に情報機器等管理責任者を置く。

(2) 情報機器等管理責任者は、その課の管理職員のうちから情報機器等管理運営責任者が指定する。

(3) 情報機器等管理運営責任者は、情報機器等管理責任者を指定し、又は変更したときは、速やかに統括管理者に通知しなければならない。

(4) 情報機器等管理責任者は、情報機器等管理運営責任者の命を受けて、その課における情報機器等及び情報システムを良好な状態に保つとともに、業務に従事する職員を監督指導し、情報資産の保護に努めなければならない。

(5) 情報機器等管理責任者は、情報機器等及び情報システムの障害、情報セキュリティ事故等に備え、重要なデータを定期的にバックアップ処理しなければならない。

(6) 情報機器等管理責任者は、その所管する課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。

(7) 情報機器等管理責任者は、その所管する課において、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、情報機器等管理運営責任者へ速やかに報告を行い、指示を仰がなければならない。

(8) 情報機器等管理責任者は、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。

(9) 情報機器等管理責任者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

(10) 情報機器等管理責任者は、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。

5　情報システム担当者

情報機器等管理責任者の指示等に従い、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。

6　情報セキュリティ委員会

本消防組合の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を審議し、CISO に報告する。

第２　情報資産の分類と管理

1　情報資産の分類

本消防組合における情報資産が漏洩、利用不能、改ざん等のセキュリティ侵害を受けた際の影響の深刻度に応じ、下表のとおり重要性の分類を定める。業務で取り扱う情報資産は、作成、入手、利用、保管、廃棄等の各局面で、重要性分類を踏まえた管理体制、手順としなければならない。

	重要性分類
1	侵害により、重大な被害が想定される情報資産 （個人情報やその他法令で制限される情報、直ちに他のセキュリティ侵害につながる情報等）
2	侵害により、行政に対する信頼を著しく害するおそれや行政事務の執行等に重大な影響を及ぼすと想定される情報資産
3	侵害により、行政事務の執行等に軽微な影響を及ぼす情報資産
4	上記１、２、３以外

2　情報資産の管理

(1) 管理責任

ア　情報機器等管理責任者は、その所管する情報資産について管理責任を有する。

イ　情報機器等管理責任者は、所管する情報システムに対して、当該システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

ウ　情報資産が複製又は伝送された場合には、複製等された情報資産も１の分類に基づき管理しなければならない。

(2) 情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、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。

(3) 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判断し難い場合は、情報機器等管理責任者に判断を仰がなければならない。

(4) 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。

(5) 情報資産の保管

ア　情報機器等管理責任者は、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　情報機器等管理責任者は、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　情報機器等管理責任者は、重要性分類３以上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、耐水及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。

(6) 情報の送信

電子メール等により重要性分類３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。

(7) 情報資産の運搬

ア　車両等により重要性分類３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　重要性分類３以上の情報資産を運搬する者は、情報機器等管理責任者に許可を得なければならない。

(8) 情報資産の提供・公表

ア　重要性分類３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　重要性分類３以上の情報資産を外部に提供する者は、情報機器等管理責任者に許可を得なければならない。

ウ　情報機器等管理責任者は、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。

(9) 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、全ての情報を消去の上、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情報資産廃棄等記録簿(別記様式)により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、情報機器等管理責任者の許可を得なければならない。

第３　情報システム全体の強靭性の向上

１　LGWAN 接続系

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。

(1) 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

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

(3) 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　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、構成両市等と連携しながら、情報セキュリティ対策を推進しなければならない。

(3) (β モデルを採用する場合)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業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

（β´モデルを採用する場合）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業務端末と入札情報や職員の情報等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、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

第４　物理的セキュリティ対策

１　サーバ等の管理

(1) 機器の取付け

情報機器等管理責任者は、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

ア　情報機器等管理責任者は、統括管理者及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、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　情報機器等管理責任者は、統括管理者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(3) 通信ケーブル等の配線

ア　統括管理者及び情報機器等管理責任者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ　統括管理者及び情報機器等管理責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

ウ　統括管理者及び情報機器等管理責任者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ　統括管理者及び情報機器等管理責任者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できない

よう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

ア　情報機器等管理責任者は、情報システムの安定性を確保するため、サーバ等の機器の定期保守を実施しなければならない。

イ　情報機器等管理責任者は、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、情報機器等管理責任者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、秘密保持契約（NDA）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

統括管理者及び情報機器等管理責任者は、庁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。

(6) 機器の廃棄等

情報機器等管理責任者は、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　管理区域（情報システム室等）の管理

(1) 管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（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。

イ　統括管理者及び情報機器等管理責任者は、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。

ウ　統括管理者及び情報機器等管理責任者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

エ　統括管理者及び情報機器等管理責任者は、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) 管理区域の入退室管理等

ア　情報機器等管理責任者は、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。

イ　職員等及び委託事業者は、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。

ウ　情報機器等管理責任者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報機器等管理責任者は、重要性分類３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。

(3) 機器等の搬入出

ア　情報機器等管理責任者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。

イ　情報機器等管理責任者は、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。

３　通信回線及び通信回線装置の管理

(1) 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) 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) 統括管理者は、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) 統括管理者は、重要性分類３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。

(6) 統括管理者は、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　職員等の利用する端末や電磁的記録媒体等の管理

(1) 情報機器等管理責任者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存

される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(2) 情報機器等管理責任者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

第５　人的セキュリティ対策

１　職員等の遵守事項

(1) 職員等の遵守事項

ア　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、速やかに情報機器等管理責任者に相談し、指示を仰がなければならない。

イ　業務以外の目的での使用の禁止

職員等は、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。

ウ　モバイル端末や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) CISO は、重要性分類３以上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、本消防組合のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報機器等管理責任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には、情報機器等管理責任者の許可を得なければならない。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用は必要最小限とすること。

オ　持ち出し及び持ち込みの記録

情報機器等管理責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ　パソコン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機器等管理責任者の許可なく変更してはならない。

キ　机上の端末等の管理

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

ク　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) 非常勤及び臨時職員等への対応

ア　情報セキュリティポリシー等の遵守

情報機器等管理責任者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

イ　情報セキュリティポリシー等の遵守に対する同意

情報機器等管理責任者は、非常勤及び臨時職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ　インターネット接続及び電子メール使用等の制限

情報機器等管理責任者は、非常勤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において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 情報セキュリティポリシー等の掲示

情報機器等管理責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

(4) 委託事業者に対する説明

情報機器等管理責任者は、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。

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・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・訓練に参加しなければならない。

3　情報セキュリティインシデントの報告

庁内での情報セキュリティインシデントの報告

(1) 職員等及び情報システム担当者は、情報セキュリティインシデントを認知した場合、速やかに情報機器等管理責任者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

(2) 報告を受けた情報機器等管理責任者は、速やかに情報機器等管理運営責任者に報告しなければならない。

(3) 情報機器等管理運営責任者は、速やかに統括管理者に報告しなければならない。ただし、重大な情報セキュリティインシデントについては、情報機器等管理責任者又は情報機器等管理運営責任者は、統括管理者を経ずに直接 CISO に報告することができる。

(4) 統括管理者は、報告のあった情報セキュリティインシデントについて、速やかに CISO に報告しなければならない。

(5) CISO は、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。

4　ID 及びパスワード等の管理

(1) IC カード等の取扱い

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

(ｱ) 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。

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

(ｳ) IC カード等を紛失した場合には、速やかに統括管理者及び情報機器等管理責任者に通報し、指示に従わなければならない。

イ　統括管理者及び情報機器等管理責任者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

ウ　統括管理者及び情報機器等管理責任者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2) ID の取扱い

職員等は、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。

ア　自己が利用している ID は、他人に利用させてはならない。

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

(3) パスワードの取扱い

職員等は、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。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

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

エ　パスワードが流出したおそれがある場合には、情報機器等管理責任者に直ちに報告し、パスワードを直ちに変更しなければならない。

オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

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

キ　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

ク　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）。

第６　技術的セキュリティ対策

１　コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

ア　情報機器等管理責任者は、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。

イ　情報機器等管理責任者は、文書サーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ　情報機器等管理責任者は、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

ア　統括管理者及び情報機器等管理責任者は、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。

イ　統括管理者及び情報機器等管理責任者は、重要な情報を取り扱うサーバ装置

については、適切な方法でサーバ装置のバックアップを取得しなければならない。

ウ　統括管理者及び情報機器等管理責任者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し、保管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

情報機器等管理責任者は、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、統括管理者及び情報機器等管理運営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

ア　情報機器等管理責任者は、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。

イ　統括管理者及び情報機器等管理責任者は、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、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

ウ　統括管理者、情報機器等管理責任者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

(5) 情報システム仕様書等の管理

統括管理者及び情報機器等管理責任者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、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

ア　統括管理者及び情報機器等管理責任者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

イ　統括管理者及び情報機器等管理責任者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

ウ　統括管理者及び情報機器等管理責任者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

統括管理者及び情報機器等管理責任者は、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

ア　統括管理者は、フィルタリング及びルーティングについ　て、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ　統括管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

ウ　統括管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直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

情報機器等管理責任者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10)外部ネットワークとの接続制限等

ア　情報機器等管理責任者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括管理者の許可を得なければならない。

イ　情報機器等管理責任者は、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、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

ウ　情報機器等管理責任者は、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。

エ　統括管理者及び情報機器等管理責任者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

(ｱ) 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。

(ｲ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

(ｳ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

(ｴ) 情報機器等管理責任者は、ウェブコンテンツの編集作業を行う主体を限定

しなければならない。

オ　情報機器等管理責任者は、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、統括管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11)複合機のセキュリティ管理

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

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

ウ　統括管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消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

統括管理者は、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

ア　統括管理者は、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を義務付けなければならない。

イ　統括管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(14)電子メールのセキュリティ管理

ア　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。

イ　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、メールサーバの運用を停止しなければならない。

ウ　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。

エ　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。

オ　統括管理者は、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

ア　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。

イ　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。

ウ　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。

エ　職員等は、重要な電子メールを誤送信した場合、情報機器等管理責任者に報告しなければならない。

(16)電子署名・暗号化

ア　職員等は、外部に送る重要性分類３以上の情報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。

イ　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。

ウ　CISO 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

ア　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。

イ　職員等は、業務上の必要がある場合は、統括管理者及び情報機器等管理責任者の許可を得て、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、情報機器等管理責任者は、ソフトウェアのライセンスを管理しなければならない。

ウ　職員等は、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

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

イ　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及び増設・交換を行う必要がある場合には、統括管理者及び情報機器等管理責任者の許可を得なければならない。

(19)業務外ネットワークへの接続の禁止

ア　職員等は、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機器等管理責任者によって定められたネットワークと異なるネットワークに接続してはならない。

イ　情報機器等管理責任者は、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利用の禁止

ア　職員等は、業務以外の目的でウェブサイトを閲覧してはならない。

イ　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ウェブサイトを閲覧していることを発見した場合は、情報機器等管理責任者に通知し、適正な措置を求めなければならない。

(21)Web 会議サービスの利用時の対策

ア　統括管理者は、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。

イ　職員等は、本消防組合の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

ウ　職員等は、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

ア　情報機器等管理責任者は、本消防組合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等を定めなければならない。

(ｱ) 本消防組合のアカウントによる情報発信が、実際の本消防組合のものであることを明らかにするために、本消防組合の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

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

イ　重要性分類３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。

ウ　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。

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

オ　住民に対し可用性を確保すべき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、本消防組合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。

２　アクセス制御

(1) アクセス制御等

ア　アクセス制御

統括管理者又は情報機器等管理責任者は、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必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者 ID の取扱い

(ｱ) 統括管理者及び情報機器等管理責任者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

(ｲ) 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、統括管理者又は情報機器等管理責任者に通知しなければならない。

(ｳ) 統括管理者及び情報機器等管理責任者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(ｴ) 統括管理者及び情報機器等管理責任者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

ウ　特権を付与された ID の管理等

(ｱ) 統括管理者及び情報機器等管理責任者は、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) 統括管理者及び情報機器等管理責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置を講じなければならない。

(ｳ) 統括管理者及び情報機器等管理責任者の特権を代行する者は、統括管理者及び情報機器等管理責任者が指名し、CISO が認めた者でなければならない。

(ｴ) CISO は、代行者を認めた場合、速やかに統括管理者、情報機器等管理運営責任者、情報機器等管理責任者に通知しなければならない。

(ｵ) 統括管理者及び情報機器等管理責任者は、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。

(ｶ) 統括管理者及び情報機器等管理責任者は、特権を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、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。

(ｷ) 統括管理者及び情報機器等管理責任者は、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

ア　職員等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、統括管理者及び当該情報システムを管理する情報機器等管理責任者の許可を得なければならない。

イ　統括管理者は、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、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ　統括管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

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

オ　統括管理者及び情報機器等管理責任者は、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。

カ　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報機器等管理責任者の許可を得るか、もしくは情報機器等管理責任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。

キ　統括管理者は、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、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並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) ログイン時の表示等

情報機器等管理責任者は、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及びログイン・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。

(4) 認証情報の管理

ア　統括管理者又は情報機器等管理責任者は、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。

イ　統括管理者又は情報機器等管理責任者は、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。

ウ　統括管理者又は情報機器等管理責任者は、認証情報の不正利用を防止するための措置を講じなければならない。

(5) 特権による接続時間の制限

情報機器等管理責任者は、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。

3　システム開発、導入、保守等

(1) 機器等の調達に係る運用規程の整備

ア　統括管理者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

イ　統括管理者及び情報機器等管理責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

(2) 機器等及び情報システムの調達

ア　統括管理者及び情報機器等管理責任者は、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。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

イ　統括管理者及び情報機器等管理責任者は、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。

(3) 情報システムの開発

ア　システム開発における責任者及び作業者の特定

情報機器等管理責任者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

イ　システム開発における責任者、作業者の ID の管理

(ｱ) 情報機器等管理責任者は、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) 情報機器等管理責任者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

ウ　システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) 情報機器等管理責任者は、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、それ以外のものを利用させてはならない。

(ｲ) 情報機器等管理責任者は、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。

エ　アプリケーション・コンテンツの開発時の対策

情報機器等管理責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(4) 情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

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

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

(ｳ) 情報機器等管理責任者は、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。

イ　テスト

(ｱ) 情報機器等管理責任者は、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) 情報機器等管理責任者は、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) 情報機器等管理責任者は、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) 情報機器等管理責任者は、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。

(ｵ) 情報機器等管理責任者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

ウ　機器等の納入時又は情報システムの受入れ時

(ｱ) 情報機器等管理責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

(ｲ) 情報機器等管理責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

(5) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなけれ

ばならない。

ア　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

イ　情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(6) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

情報機器等管理責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(7) システム開発・保守に関連する資料等の整備・保管

ア　情報機器等管理責任者は、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。

(ｱ) 情報機器等管理責任者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括管理者に報告しなければならない。

(ｲ) 情報機器等管理責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
・情報セキュリティインシデントを認知した際の対処手順
・情報システムが停止した際の復旧手順

イ　情報機器等管理責任者は、テスト結果を一定期間保管しなければならない。

(8) 情報システムにおける入出力データの正確性の確保

ア　情報機器等管理責任者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

イ　情報機器等管理責任者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ｱ) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直さなければならない。

(ｲ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(ｳ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　情報機器等管理責任者は、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。

(9) 情報システムの変更管理

情報機器等管理責任者は、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。

(10)開発・保守用のソフトウェアの更新等

情報機器等管理責任者は、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。

(11)システム更新又は統合時の検証等

情報機器等管理責任者は、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。

(12)情報システムについての対策の見直し

情報機器等管理責任者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本消防組合内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括管理者へ報告しなければならない。

4　不正プログラム対策

(1) 統括管理者の措置事項

統括管理者は、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。

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

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

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

エ　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。

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

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

キ　業務で利用するソフトウェアは、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) 情報機器等管理責任者の措置事項

情報機器等管理責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

ア　情報機器等管理責任者は、その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システムに常駐させなければならない。

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

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

エ　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本消防組合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。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報機器等管理責任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。

ア　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。

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

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

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

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

カ　統括管理者が提供するウイルス情報を、常に確認しなければならない。

キ　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、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

統括管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

5　不正アクセス対策

(1) 統括管理者の措置事項

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。

ア　使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて、機能を削除又は停止しなければならない。

ウ　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括管理者及び情報機器等管理責任者へ通報するよう、設定しなければならない。

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

(2) 攻撃への対処

CISO 及び統括管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県、構成両市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

CISO 及び統括管理者は、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

統括管理者及び情報機器等管理責任者は、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。

(5) 職員等による不正アクセス

統括管理者及び情報機器等管理責任者は、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等の情報機器等管理責任者に通知し、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

統括管理者及び情報機器等管理責任者は、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

統括管理者及び情報機器等管理責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6　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管理者及び情報機器等管理責任者は、サーバ装置、端末及び通信回線装置等における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

統括管理者及び情報機器等管理責任者は、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　運用

1　情報システムの監視

(1) 情報システムの運用・保守時の対策

ア　統括管理者及び情報機器等管理責任者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

イ　統括管理者及び情報機器等管理責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

ウ　統括管理者及び情報機器等管理責任者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

(2) 情報システムの監視機能

ア　統括管理者及び情報機器等管理責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

イ　統括管理者及び情報機器等管理責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

ウ　統括管理者及び情報機器等管理責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

エ　統括管理者及び情報機器等管理責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

(3) 情報システムの監視

ア　統括管理者及び情報機器等管理責任者は、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　統括管理者及び情報機器等管理責任者は、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。

ウ　統括管理者及び情報機器等管理責任者は、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。

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

ア　情報機器等管理運営責任者及び情報機器等管理責任者は、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CISO及び統括管理者に報告しなければならない。

イ　CISO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。

ウ　統括管理者及び情報機器等管理責任者は、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

CISO 及び 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、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

ア　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、直ちに統括管理者及び情報機器等管理責任者に報告を行わなければならない。

イ　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管理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。

3　侵害時の対応等

(1) 緊急時対応計画の策定

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

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

(3) 業務継続計画との整合性確保

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

(4) 緊急時対応計画の見直し

CISO 又は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の規程を見直さなければならない。

4　例外措置

(1) 例外措置の許可

情報機器等管理責任者は、情報セキュリティ関係規程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

する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

情報機器等管理責任者は、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。

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) 守口市門真市消防組合個人情報保護法施行条例(令和５年守口市門真市消防組合条例第２号)

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、直ちに次の措置を講じなければならない。

ア　統括管理者が違反を確認した場合は、統括管理者は当該職員等が所属する課等の情報機器等管理責任者に通知し、適正な措置を求めなければならない。

イ　情報機器等管理責任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管理者及び当該職員等が所属する課等の情報機器等管理責任者に通知し、適正な措置を求めなければならない。

ウ　情報機器等管理責任者の指導によっても改善されない場合、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、統括管理者は、職員等の権利を停止

あるいは剥奪した旨を CISO 及び当該職員等が所属する課等の情報機器等管理責任者に通知しなければならない。

第８　業務委託と外部サービス（クラウドサービス）の利用

１　業務委託

(1) 業務委託に係る運用規程の整備

統括管理者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

ア　委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

イ　委託事業者の選定基準

(2) 業務委託実施前の対策

ア　情報機器等管理責任者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

(ｱ) 委託する業務内容の特定

(ｲ) 委託事業者の選定条件を含む仕様の策定

(ｳ) 仕様に基づく委託事業者の選定

(ｴ) 情報セキュリティ要件を明記した契約の締結（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等に係る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
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・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
・本消防組合による監査、検査
・本消防組合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程(損害賠償等)

(ｵ) 委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

イ　情報機器等管理責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

(ｱ) 仕様に準拠した提案

(ｲ) 契約の締結

(ｳ) 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

(3) 業務委託実施期間中の対策

ア　情報機器等管理責任者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

(ｱ) 委託判断基準に従った重要情報の提供

(ｲ) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

(ｳ) 統括管理者へ措置内容の報告（重要度に応じてCISOに報告）

(ｴ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

イ　情報機器等管理責任者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

(ｱ) 情報の適正な取扱いのための情報セキュリティ対策

(ｲ) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

(ｳ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 業務委託終了時の対策

ア　情報機器等管理責任者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

(ｱ) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(ｲ) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

イ　情報機器等管理責任者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

(ｱ) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたこと

の報告を含む検収の受検

(ｲ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

2　情報システムに関する業務委託

(1) 情報システムに関する業務委託における共通的対策

情報機器等管理責任者は、情報システムに関する業務委託の実施までに、情報システムに本消防組合の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

(2) 情報システムの構築を業務委託する場合の対策

情報機器等管理責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

ア　情報システムのセキュリティ要件の適切な実装

イ　情報セキュリティの観点に基づく試験の実施

ウ　情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

ア　情報機器等管理責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

イ　情報機器等管理責任者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

(4) 本消防組合向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

ア　情報機器等管理責任者は、外部の一般の者が本消防組合向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

イ　情報機器等管理責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

ウ　情報機器等管理責任者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し、判断しなければならない。

エ　情報機器等管理責任者は業務委託サービスを利用する場合には、統括管理者又は情報機器等管理運営責任者へ当該サービスの利用申請を行わなければならない。

オ　統括管理者又は情報機器等管理運営責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

カ　統括管理者又は情報機器等管理運営責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

3　外部サービス（クラウドサービス）の利用（重要性分類３以上の情報を取り扱う場合）

(1) クラウドサービスの選定に係る運用規程の整備

統括管理者は、重要性分類３以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規程を整備しなければならない。

ア　クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下３において「クラウドサービス利用判断基準」という。）

イ　クラウドサービス提供者の選定基準

ウ　クラウドサービスの利用申請の許可権限者と利用手続

エ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(2) クラウドサービスの利用に係る運用規程の整備

統括管理者は、重要性分類３以上の情報を取り扱う場合、以下を含むクラウドサービス（重要性分類３以上の情報を取り扱う場合）の利用に関する規程を整備しなければならない。

ア　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

イ　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

ウ　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

(ｱ) クラウドサービスの利用終了時における対策

(ｲ) クラウドサービスで取り扱った情報の廃棄

(ｳ) クラウドサービスの利用のために作成したアカウントの廃棄

(3) クラウドサービスの選定

ア　情報機器等管理運営責任者は、取り扱う情報の格付及び取扱制限を踏まえ、

クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上で、クラウドサービスの利用を検討しなければならない。

イ　情報機器等管理運営責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定しなければならない。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

(ｱ) クラウドサービスの利用を通じて本消防組合が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

(ｲ) クラウド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) クラウドサービスの提供に当たり、クラウド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、本消防組合の意図しない変更が加えられないための管理体制

(ｴ) クラウドサービス提供者の資本関係・役員等の情報、クラウド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)・実績及び国籍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

ウ　情報機器等管理運営責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。

エ　情報機器等管理運営責任者は、クラウドサービスの利用を通じて本消防組合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クラウドサービス提供者の選定条件に含めなければならない。

(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

オ　情報機器等管理運営責任者は、クラウドサービスの利用を通じて本消防組合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クラウドサービス提供者を選定し、必要に応じて本消防組合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なければならない。

カ　情報機器等管理運営責任者は、クラウド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、クラウドサービス提供者の選定条件で求める

内容をクラウド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消防組合に提供し、本消防組合の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウド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しなければならない。

キ　情報機器等管理運営責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス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及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

(ｱ) クラウドサービスに求める情報セキュリティ対策

(ｲ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(ｳ) クラウドサービスに求めるサービスレベル

ク　統括管理者は、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、クラウド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、判断しなければならない。

(4) クラウドサービスの利用に係る調達・契約

ア　情報機器等管理運営責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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なければならない。

イ　情報機器等管理運営責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウド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なければならない。

(5) クラウドサービスの利用承認

ア　情報機器等管理運営責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

イ　利用申請の許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。

ウ　利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

(6) クラウドサービスを利用した情報システムの導入・構築時の対策

ア　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウド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しなければならない。

(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

イ　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括管理者へ報告しなければならない。

ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

(ｱ) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
(ｲ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順
(ｳ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

エ　クラウドサービス管理者は、ウにおいて定める規程に対し、構築時に実施状況を確認・記録しなければならない。

(7) クラウドサービスを利用した情報システムの運用・保守時の対策

ア　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウド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しなければならない。

(ｱ) クラウドサービス利用方針の規定
(ｲ) クラウド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) クラウドサービス内の通信の制御
(ｷ) 設計・設定時の誤りの防止
(ｸ) クラウドサービスを利用した情報システムの事業継続

イ　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括管理者へ報告しなければならない。

ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要

な措置を講じなければならない。

エ　情報機器等管理運営責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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しなければならない。

オ　クラウドサービス管理者は、アからエまでにおいて定める規程に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

(8) クラウドサービスを利用した情報システムの更改・廃棄時の対策

ア　統括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウド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しなければならない。

(ｱ) クラウドサービスの利用終了時における対策

(ｲ) クラウドサービスで取り扱った情報の廃棄

(ｳ) クラウドサービスの利用のために作成したアカウントの廃棄

イ　クラウドサービス管理者は、アにおいて定める規程に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。

4　外部サービス（クラウドサービス）の利用（重要性分類３以上の情報を取り扱わない場合）

(1) クラウドサービスの利用に係る規程の整備

統括管理者は、以下を含むクラウドサービスの利用に関する規程を整備しなければならない。

ア　クラウドサービスを利用可能な業務の範囲

イ　クラウドサービスの利用申請の許可権限者と利用手続

ウ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

エ　クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

ア　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重要性分類３以上の情報を取り扱わない場合のクラウド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クラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

イ　情報機器等管理運営責任者は、職員等によるクラウド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、承認したクラウドサービスを記録しなければならない。

第９　評価・見直し

1　監査

(1) 実施方法

CISO は、情報セキュリティ監査統括責任者に対して、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、毎年度及び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

ア　情報セキュリティ監査統括責任者は、次長をもって充てる。

イ　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

ウ　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

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

イ　被監査部門は、監査の実施に協力しなければならない。

(4) 委託事業者に対する監査

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又は必要に応じて行わなければならない。

(5) 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

(6) 保管

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

(7) 監査結果への対応

ア　CISO は、監査結果を踏まえ、指摘事項を所管する情報機器等管理責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

イ　CISO は、指摘事項を所管していない情報機器等管理責任者に対しても、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。また、庁内で横断的に改善が必要な事項については、統括管理者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告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及び関係規程等の見直し等への活用

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。

2　自己点検

(1) 実施方法

ア　統括管理者及び情報機器等管理責任者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

イ　情報機器等管理運営責任者は、情報機器等管理責任者と連携して、所管する課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、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

統括管理者、情報機器等管理責任者及び情報機器等管理運営責任者は、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

ア　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。

イ　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。

3　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踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示をし、措置の結果についてCISO に報告しなければならない。

附　則

この対策基準は、令和８年10月１日から施行する。

別記様式(第２．２．(9)関係)

情報資産廃棄等記録簿

廃棄日時	情報資産の名称	処理内容	理由	担当者	承認者