神戸市職員共済組合情報セキュリティ対策基準

令和６年４月１日

神戸市職員共済組合（以下「組合」という。）における情報セキュリティ対策基準は、情報セキュリティ基本方針を実行に移すために職員、非常勤職員、派遣職員、嘱託職員及び臨時職員（以下「職員等」という。）が遵守する基準である。

１　組織体制

１－１　対象範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③　情報システムの仕様書、ネットワーク図等のシステム関連文書

１－２　組織及び体制

（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　事務局長をＣＩＳＯとする。ＣＩＳＯは、組合における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　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及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

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

⑤　ＣＩＳＯは、副ＣＩＳＯその他の本対策基準に定める責任者に対し、本対策基準に定められた自らの担務を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 統括情報セキュリティ責任者は、事務局次長とする。
② 統括情報セキュリティ責任者は、ＣＩＳＯ及び副ＣＩＳＯを補佐し、組合の情報セキュリティポリシーの遵守に関する責任を有する。
③ 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及び情報システム管理者に対して、情報セキュリティポリシーの遵守に関する指導及び助言を行う権限を有する。
④ 統括情報セキュリティ責任者は、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（ＣＩＳＯの担務を担う者を含む。以下同じ。）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行う権限及び責任を有する。
⑤ 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理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。
⑥ 統括情報セキュリティ責任者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、回復のための対策を講じなければならない。
⑦ 統括情報セキュリティ責任者は、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にその内容を報告しなければならない。

（３） 情報セキュリティ責任者
① 情報セキュリティ責任者は、事務局次長とする。
② 情報セキュリティ責任者は、組合の情報セキュリティ対策に関する統括的な権限及び責任を有する。
③ 情報セキュリティ責任者は、組合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 情報セキュリティ責任者は、組合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及び職員等に対する教育、訓練、助言及び指示を行う。

（４） 情報セキュリティ管理者
① 情報セキュリティ管理者は、事務局次長とする。
② 情報セキュリティ管理者は、共済組合の情報セキュリティ対策に関す

る権限及び責任を有する。

③　情報セキュリティ管理者は、共済組合において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（５）　情報システム管理者

①　事務局次長を、各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の開発、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　情報システム管理者は、所管する情報システムの情報セキュリティに関する権限及び責任を有する。

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。

（６）　情報セキュリティ委員会

①　情報セキュリティ委員会（以下「委員会」という。）は、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及び情報システム管理者をもって構成する。

②　委員会は、ＣＩＳＯを長とし、情報セキュリティに関する事項を総括し、情報セキュリティ対策を統一的に実施するため、情報セキュリティポリシーの承認等重要事項の決定を行い、重要事項に関する関係部署との連絡及び調整を行う。

③　委員会は、毎年度、組合における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

④　委員会の庶務は、企画係において処理する。

（７）　兼務の禁止

①　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②　情報セキュリティ監査の実施において、監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（８）　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に所属する職員を選任し、その中からＣＳＩ

ＲＴ責任者を置くとともに、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員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が発生した場合、その状況を確認し、ＣＩＳＯへ報告が行われる体制を整備しなければならない。

④　ＣＳＩＲＴは、ＣＩＳＯによる情報セキュリティ対策の意思決定が行われた際には、その内容を関係課に提供しなければならない。

⑤　ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、都道府県知事（指定都市職員共済組合については、総務大臣）、全国市町村職員共済組合連合会（以下「市町村連合会」という。）等へ報告しなければならない。

⑥　ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦　ＣＳＩＲＴは、情報セキュリティに関して、関係機関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。

（９）　クラウドサービス利用における組織体制

①　統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、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ける情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

２　情報資産の管理方法等

（１）　情報資産の分類

組合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又は機密性２	個人情報（個人番号及び特定個人情報を含む。以下同じ。）、業務上必	・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

	要とする最小限の者のみが扱うべき情報及び業務上セキュリティ侵害が年金受給権者及び組合員等の生命及び財産等へ重大な影響を及ぼす情報資産	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	公開することを予定してない情報及びセキュリティ侵害が業務の執行等に重大な影響を及ぼす情報資産	
機密性１	上記以外の情報資産	－

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	組合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、年金受給権者若しくは組合員等の権利が侵害される又は組合事務の適確な遂行に支障（軽微なものを除く。）を及ぼすお	・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

	それがある情報資産	
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	組合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、年金受給権者若しくは組合員等の権利が侵害される又は組合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、所管する情報資産について管理責任を有する。

イ　情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製又は伝送された情報資産も（１）の分類に基づき管理しなければならない。

ウ　機密性３及び機密性２（以下「機密性２以上」という。）並びに完

全性２、可用性２の電子データ、紙等の情報資産については、施錠可能な場所に保管しなければならない。

エ　施錠に使用する鍵の管理については、保管元の課で厳重に管理しなければならない。

オ　情報セキュリティ管理者は、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、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）の取扱いを定めるとともに、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、サービス利用前に文書での提示を求め、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、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理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）の情報資産の分類に基づき、当該情報の分類を行わなければならない。

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。

エ　情報を作成する者は、情報の作成自体が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　組合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　組合外の者が作成した情報資産を入手した者は、（１）の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、適正な取扱いをしなければならない。

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

⑥　情報資産の保管

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

イ　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ　情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体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場所に保管しなければならない。

エ　情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２及び可用性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。

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　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場合は、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、年金受給権者、組合員等に提供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、情報セキュリティ管理者の許可を得るとともに、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　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管理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）　マイナンバー事務系

①　マイナンバー事務系と他の領域との分離

マイナンバー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

業務ごとに専用端末を設置するものとし、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。

イ　情報の持ち出し不可設定

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、情報を持ち出すことが必要と認められたときは、この限りでない。

（２）　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

④　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

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。

４　物理的セキュリティ

４－１　サーバ機器等の管理

（１）　機器の取付け

情報システム管理者は、サーバ機器等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必要な措置を講じなければならない。

（２）　サーバの冗長化

①　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及びその他の基幹サーバを可能な限り冗長化し、同一データを保持しなければならない。

②　情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動する等システムの運用停止時間を最小限

にしなければならない。

（３）　機器の電源

①　情報システム管理者は、統括情報セキュリティ責任者及び庁舎管理担当課と連携し、サーバ機器等の電源について、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　情報システム管理者は、統括情報セキュリティ責任者及び庁舎管理担当課と連携し、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及び情報システム管理者は、庁舎管理担当課と連携し、通信ケーブル及び電源ケーブルの損傷を防止するために、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及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、庁舎管理担当課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及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正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及び情報システム管理者は、自ら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又は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）　機器の定期保守及び修理

①　情報システム管理者は、情報システム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委託事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（６）　組合外への機器の設置

①　統括情報セキュリティ責任者及び情報システム管理者は、組合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。

②　統括情報セキュリティ責任者及び情報システム管理者は、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

①　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。

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）をする者は、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確認しなければならない。

なお、当該確認にあたっては、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、その監査報告書や認証等を利用できる。

４－２　管理区域の管理

（１）　管理区域

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、当該機器等の管理並びに運用を行うための部屋（壁又は間仕切り等による区画を含む。以下「情報システム室」という。）や電磁的記録媒体の保管庫及び保管室（壁又は間仕切り等による区画を含む。）をいう。

②　統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。

③　統括情報セキュリティ責任者及び情報システム管理者は、庁舎管理担当課と連携して、管理区域から外部に通ずるドアを必要最小限とし、鍵、監視機能又は警報装置等によって許可されていない者の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及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。

⑤　統括情報セキュリティ責任者及び情報システム管理者は、庁舎管理担当課と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

⑥　統括情報セキュリティ責任者及び情報システム管理者は、管理区域に

配置する消火薬剤や消防用設備等が、機器等及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）　管理区域の入退室管理

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、静脈認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

②　職員等及び委託事業者は、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には、必要に応じて立入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又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

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、あらかじめ職員又は委託事業者に確認を行わせなければならない。

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

４－３　取扱区域の管理

（１）　取扱区域

取扱区域とは、特定個人情報等（神戸市職員共済組合個人番号及び特定個人情報の適正な取扱いに関する規程（平成 27 年規程第 178 号）第１条に規定する特定個人情報等をいう。以下同じ。）の情報漏えい等を防止するために、特定個人情報等を取り扱う事務を実施する区域をいう。

（２）　取扱区域の管理

①　統括情報セキュリティ責任者は、取扱区域を明確にし、物理的な安全管理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及び情報セキュリティ管理者は、取扱区域を明確にするために、取扱区域に壁又は間仕切り等の設置及び座席配置の工夫等により物理的な安全管理に努めなければならない。

４－４　通信回線及び通信回線装置の管理

①　統括情報セキュリティ責任者は、事務室内の通信回線及び通信回線装置を、庁舎管理担当課と連携し、適正に管理しなければならない。これらに関連する文書についても同様とする。

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、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。この場合において、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　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、改ざん又は消去等が生じないよう十分なセキュリティ対策を実施しなければならない。

⑤　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。この場合において、必要に応じ、回線を冗長化する等の措置を講じなければならない。

４－５　職員等の利用する端末や電磁的記録媒体等の管理

①　情報システム管理者は、盗難防止のため、事務室等で利用するパソコン（ノート）のワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②　情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③　情報システム管理者は、端末の電源起動時のパスワード（ＢＩＯＳパスワード、ハードディスクパスワード等）を併用しなければならない。

④　情報システム管理者は、マイナンバー事務系では、「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　情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならず、当該端末にセキュリティチップが搭載されている場合、その機能を有効に活用するよう努めなければならない。

⑥　情報システム管理者は、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用するよう努めなければならない。

⑦　情報システム管理者は、モバイル端末の組合外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

5　人的セキュリティ

5－1　職員等の遵守事項

（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、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

イ　職員等は、情報セキュリティ対策について不明な点及び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出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③　モバイル端末や電磁的記録媒体等の持出し及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、完全性２、可用性２いずれか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、業務上支給されたモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

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

④　業務上支給されたもの以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア　職員等は、業務上支給されたもの以外のパソコン、モバイル端末、電磁的記録媒体等を業務に利用してはならない。ただし、業務上支給されたもの以外の端末の業務利用の可否判断をＣＩＳＯが行った後に、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、業務上支給されたもの以外のパソコン、モバイル端末、電磁的記録媒体等を用い、情報セキュリティ管理者の許可を得た上で、組合の外部で情報処理作業を行う場合には、安全管理措置に関する規定を遵守しなければならない。

⑤　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない

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、情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないよう離席時のパソコン、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。

⑧　退職時等の遵守事項

ア　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。

イ　職員等は、異動、退職等により業務を離れた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）　非常勤職員等への対応

①　情報セキュリティポリシーの遵守

情報セキュリティ管理者は、非常勤職員、派遣職員、嘱託職員及び臨時職員（以下「非常勤職員等」という。）に対し、採用時に情報セキュリティポリシーのうち、非常勤職員等が守るべき内容を理解させ、その内容を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、非常勤職員等の採用の際、必要に応じ、情報セキュリティポリシー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、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、電子メールの使用等が不要の場合、当該情報システムを担当する情報システム管理者に報告し、当該情報システム管理者は、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の掲示

統括情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順を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

情報システム管理者は、ネットワーク、情報システムの開発・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含め情報セキュリティポリシー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 ＣＩＳＯは、職員等に対し情報セキュリティポリシーについて普及及び啓発しなければならない。

② ＣＩＳＯは、定期的に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、教育及び訓練を実施するとともに、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確認しなければならない。

③ 職員等は、定められた研修に参加の上、情報セキュリティポリシーを理解し、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。

（２） 研修計画の策定及び実施

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、委員会の承認を得なければならない。

② 研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

③ 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。

④ 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、情報セキュリティ管理者、情報システム管理者、その他の職員等に対して、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ものにしなければならない。

⑤ 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

⑥ 統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、ＣＩＳＯ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しなければならない。

⑦ ＣＩＳＯは、毎年度１回、委員会に対して、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

① 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。

② ＣＩＳＯは、ネットワーク、各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるよう計画しなければならない。

（４） 研修・訓練への参加

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。

５－３ 情報セキュリティインシデントの報告

（１） 内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、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

② 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 情報セキュリティ管理者は、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及び情報セキュリティ責任者に報告しなければならない。

④　情報セキュリティ責任者は、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の報告について連絡体制の対象者に報告しなければならない。

⑤　ＣＩＳＯ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、必要に応じて市町村連合会事務局長に報告しなければならない。

⑥　ＣＩＳＯ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、必要に応じて都道府県知事（指定都市職員共済組合については、総務大臣）に報告しなければならない。

（２）　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、組合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、外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

②　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてＣＩＳＯ及び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、報告のあった情報セキュリティインシデントについて、必要に応じて市町村連合会事務局長に報告しなければならない。

⑤　ＣＩＳＯ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、必要に応じて都道府県知事（指定都市職員共済組合については、総務大臣）に報告しなければならない。

⑥　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、外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

⑦　統括情報セキュリティ責任者は、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原因の究明・記録、再発防止等

①　ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

②　ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、

ＣＩＳＯに速やかに報告しなければならない。

③　ＣＳＩＲＴは、情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

④　ＣＳＩＲＴは、情報セキュリティインシデント原因を究明し、記録を保存するとともに再発防止策を検討し、ＣＩＳＯに報告しなければならない。

⑤　ＣＩＳＯは、ＣＳＩＲＴから情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

５―４　ＩＤ及びパスワードの管理

（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ないこと。

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くこと。

ウ　ＩＣカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従うこと。

②　統括情報セキュリティ責任者及び情報システム管理者は、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。

③　統括情報セキュリティ責任者及び情報システム管理者は、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。

①　自己が利用しているＩＤは、他人に利用させないこと。

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ないこと。

（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すること。
② パスワードを秘密にし、パスワードの照会には一切応じないこと。
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）にすること。
④ パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更すること。
⑤ 複数の情報システムを扱う職員等の場合、同一のパスワードをシステム間で用いないこと。
⑥ 仮のパスワード（初期パスワードを含む。）を最初のログイン時点で変更すること。
⑦ サーバ、ネットワーク機器、パソコン等の端末のパスワードの記憶機能を利用しないこと。
⑧ 職員等間でパスワードを共有しないこと（ただし、共有ＩＤに対するパスワードを除く。）。

6　技術的セキュリティ

6－1　ネットワーク、情報システム及び情報資産の管理

（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。
③ 情報システム管理者は、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

① 統括情報セキュリティ責任者及び情報システム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、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。
② 統括情報セキュリティ責任者及び情報システム管理者は、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、その機能の仕様が組合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、自らバックアップ機能の導入に関する責任を負い、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

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、統括情報セキュリティ責任者及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）　システム管理記録及び作業の確認

①　情報システム管理者は、担当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及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③　統括情報セキュリティ責任者又は情報システム管理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

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、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

①　統括情報セキュリティ責任者及び情報システム管理者は、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　統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③　統括情報セキュリティ責任者及び情報システム管理者は、取得したロ

グを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）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、記録（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　統括情報セキュリティ責任者及び情報システム管理者は、監査及びデジタルフォレンジック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

統括情報セキュリティ責任者及び情報システム管理者は、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　統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（９）　外部の者が利用できるシステムの分離等

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

(10)　外部ネットワークとの接続制限等

①　情報システム管理者は、イントラネットのサーバ及び端末には、インターネットから直接アクセスできないアドレスを付与し、かつインターネットとイントラネットの間にはファイアウォール等でアクセスを制限しなければならない。

②　情報システム管理者は、外部ネットワークと接続する場合には、接続するネットワークの構成、セキュリティレベル等を詳細に検討し、組合の情報システム及び情報資産に影響が生じないように確認した上で、接

続しなければならない。

③　情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④　統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、組合内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤　情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11)　複合機のセキュリティ管理

①　統括情報セキュリティ責任者は、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能を一つにまとめた機器（以下「複合機」という。）を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の重要性分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

②　統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③　統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消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。

④　ファクシミリによる送信を行うときには、誤送信を防ぐために、受信相手の番号を十分に確認する又は番号登録による送信を行うこととする。

⑤　受信側が自動受信となっている場合を考慮し、送信後、送り先の担当者と連絡を取るなどの対応を行うものとする。

⑥　ファクシミリによる受信を行うときには、ＦＡＸサーバによる受信を行うなど、受信した書面が放置されないように配慮するものとする。

(12)　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（ＩＰ電話システム等特

定の用途に使用される情報システム特有の構成要素であって、通信回線に接続され、又は電磁的記録媒体を内蔵しているものをいう。）について、取り扱う情報、利用方法及び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　統括情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②　統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(14)　電子メールのセキュリティ管理

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、保守等のため組合内に常駐している委託事業者の作業員がいる場合、当該者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、機密性２以上の内容が含まれた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、２（１）の情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、ＣＩＳＯが定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

②　職員等は、暗号化を行う場合にＣＩＳＯが定める以外の方法を用いてはならない。また、ＣＩＳＯが定めた方法で暗号化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又は手段を署名検証者へ安全に提供しなければならない。

(17)　無許可ソフトウェアの導入等の禁止

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

②　職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。この場合において、情報セキュリティ管理者又は情報システム管理者は、当該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、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。

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及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

(19)　業務外ネットワークへの接続の禁止

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、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、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(21)　Ｗｅｂ会議サービス利用時の対策

①　統括情報セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

②　職員等は、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しなければならない。

③　職員等は、Ｗｅｂ会議を主催する場合、会議に無関係な者が参加できないよう対策を講じなければならない。

④　職員等は、外部からＷｅｂ会議に招待される場合は、組合の定める利用手順に従い、必要に応じて情報セキュリティ管理者に利用申請を行い、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、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を定めなければならない。

ア　組合のアカウントによる情報発信が、実際の組合のものであることを明らかにするために、組合の自己管理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、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。

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、組合の自己管理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　アクセス制御等

（１）　アクセス制御等

①　利用者登録

職員等の利用者登録、変更及び抹消の申請は書面で行い、統括情報セキュリティ責任者及び当該情報システムを担当する情報システム管理者が承認することとする。

②　アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員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

①　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理並びに職員等の異動、出向及び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。

②　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又は当該情報システムを担当する情報システム管理者に申請しなければならない。

③　統括情報セキュリティ責任者及び情報システム管理者は、利用されていないＩＤが放置されないよう、セキュリティ担当課と連携し、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

①　統括情報セキュリティ責任者及び情報システム管理者は、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。

②　統括情報セキュリティ責任者及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及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。

③　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及び情報システム管理者に通知しなければならない。

④　統括情報セキュリティ責任者及び情報システム管理者は、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。

⑤　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワード設定以上に定期変更、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。

⑥　統括情報セキュリティ責任者及び情報システム管理者は、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。

（４）　リモートアクセス

情報システム管理者は、リモートアクセスを必要最小限にするとともに、リモートアクセスのログを取得し、定期的に調査しなければならない。

（５）　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又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する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及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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、持ち込んだ又は外部から持ち帰ったモバイル端末を内部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及び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て接続又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、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報、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たときは、この限りでない。

（６）　ログインの制限

①　職員等は、自席を離れるときには端末のスクリーンロックを行い、他の者が使用できないようにしなければならない。

②　各端末において、10 分以上アクセスがなかったときにはスクリーンを自動的にロックするように設定しなければならない。

（７）　自動識別の設定

統括情報セキュリティ責任者及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）　認証情報の管理

①　統括情報セキュリティ責任者又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又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、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　統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

(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及び情報システムへの接続時間を必要最小限に制限しなければならない。

６－３　システム開発、導入、保守など

（１）　情報システムの調達

①　統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、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及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、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

情報システム管理者は、情報システムの開発及び保守の事故・不正行為防止対策のために次の事項を定めなければならない。

①　責任者及び監督者

②　作業者及び作業範囲

③　システム開発及び保守などの事故、不正行為に係るリスク分析

④　開発・保守の情報システムと運用システムとの分離

⑤　開発・保守に関するソースコードの提出

⑥　開発・保守の際のセキュリティ上問題となりうるおそれのあるオペレーティングシステム、ミドルウェア及びアプリケーションの使用禁止

⑦　開発・保守の際のアクセス制限

⑧　機器の搬出入の際の当該機器を管理する情報システム管理者の許可及び確認

⑨　開発・保守記録の提出義務

⑩　マニュアルなどの定められた場所への保管

⑪　開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発、保守終了後に不要となった時点での速やかな抹消

⑫　守秘義務

⑬　再委託管理

⑭　システム開発に用いるハードウェア及びソフトウェアの管理

ア　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

イ　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（３）　情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

ア 情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

イ 情報システム管理者は、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、個人情報及び機密性２以上の情報を、テストデータに使用してはならない。

エ 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（４） システム開発・保守に関連する資料等の整備・保管

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及びシステム関連文書を適正に整備・保管しなければならない。

② 情報システム管理者は、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正な方法で保管しなければならない。

（５） 情報システムにおける入出力データの正確性の確保

① 情報システム管理者は、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、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。

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

①　情報システム管理者は、ソフトウェアを更新する場合は、その手続きを定めなければならない。

②　情報システム管理者は、ソフトウェアの更新又は修正プログラムの導入をする場合は、不具合の修正の確認及び他のシステムとの相性の確認を十分に行わなければならない。

③　情報システム管理者は、障害などで暫定的に修正したプログラムを導入する場合には、暫定期間を定め、本格的な対応プログラムに速やかに移行しなければならない。

（８）　システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

６―４　不正プログラム対策

（１）　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すること。

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すること。

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すること。

④　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常駐させること。

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つこと。

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つこと。

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ないこと。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すること。

⑧　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に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定期的にクラウドサービス事業者に報告を求めるなどにより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　所管するサーバ、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ること。

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を常に最新の状態に保つこと。

③　不正プログラム対策のソフトウェアを常に最新の状態に保つこと。

④　業務で利用するソフトウェアに、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したソフトウェアを利用しないこと。

⑤　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、組合が管理している媒体以外を職員等に利用させないこと。

⑥　不正プログラムの感染及び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すること。

⑦　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として、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、当該ソフトウェアの設定を変更しないこと。

②　外部からデータ又はソフトウェアを取り入れる場合、不正プログラム対策ソフトウェアによるチェックを行うこと。

③　差出人が不明又は不自然に添付されたファイルを伴ったメールを受信した場合、当該メールは開かず速やかに削除すること。

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すること。

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うこと。なお、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、無害化すること。

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、常に確認すること。

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

（４）　専門家の支援体制

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

６－５　不正アクセス対策

（１）　統括情報セキュリティ責任者の措置

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すること。

②　不要なサービスについて、機能を削除又は停止すること。

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及び情報システム管理者へ通報するよう、設定すること。

④　重要なファイルについて、定期的に当該ファイルの改ざんの有無を検査すること。

⑤　統括情報セキュリティ責任者は、情報システムについて、システムの販売供給元等の連絡先を含む緊急連絡網を整備し、不正アクセスが発生した際の対応手順を整備しなくてはならない。

⑥　組合が定めたクラウドサービスの利用に関するポリシー（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、クラウドサービスにおいて実現できるのか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、利用前にクラウドサービス事業者に確認しなければならない。

⑦　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、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。

⑧　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、その管理手順等が、組合が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

（２）　ＣＩＳＯ及び統括情報セキュリティ責任者の措置

①　ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

②　ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）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。

（３）　内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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組合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。

（４）　職員等による不正アクセス

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

（５）　サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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。

（６）　標的型攻撃

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

６－６　セキュリティ情報の収集

（１）　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

①　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。

②　統括情報セキュリティ責任者及び情報システム管理者は、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。

③　統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービス事業者に対して、利用する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情報を求め、組合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

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及び共有

①　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。

②　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する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　運用におけるセキュリティ対策

７－１　情報システムの監視

（１）　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティ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。

（２）　統括情報セキュリティ責任者及び情報システム管理者は、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）　統括情報セキュリティ責任者及び情報システム管理者は、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。

（４）　統括情報セキュリティ責任者及び情報システム管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

（５）　統括情報セキュリティ責任者及び情報システム管理者は、必要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監視により、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。

（６）　統括情報セキュリティ責任者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、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。

（７）　統括情報セキュリティ責任者及び情報システム管理者は、クラウドサー

ビス利用における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、手順化し、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　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにＣＩＳＯ及び統括情報セキュリティ責任者に報告しなければならない。

②　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。

③　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク、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、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、直ちに統括情報セキュリティ責任者及び情報セキュリティ責任者に報告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、７－３（１）に定める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。

７－３　侵害時の対応等

（１）　緊急時対応計画の策定等

①　ＣＩＳＯ又は委員会は、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への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、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 ＣＩＳＯ又は委員会は、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障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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） 事業継続計画との整合性確保

委員会は、組合が策定した事業継続計画（自然災害又は大規模・広範囲にわたる疾病等に備えた事業継続計画とする。）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定を見直さなければならない。

８ 例外措置

（１） 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、ＣＩＳＯの許可を得て、例外措置を取ることができる。

（２） 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、業務を遂行する上で、例外措置を実施することが不可避であり、かつ、緊急を要する事案により、やむを得ずＣＩＳＯの許可を得ないで例外措置を行った場合は、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。

９　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、以下の法令のほか関係法令を遵守しなければならない。

①　個人情報の保護に関する法律（平成 15 年法律第 57 号）

②　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）

③　著作権法（昭和 45 年法律第 48 号）

④　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）

（２）　統括情報セキュリティ責任者及び情報システム管理者は、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。

10　情報セキュリティポリシーに違反した場合の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

（１）　統括情報セキュリティ責任者が違反を確認した場合、当該職員等が所属する課の情報セキュリティ管理者に通知し、適正な措置を求めること。

（２）　情報システム管理者が違反を確認した場合、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課の情報セキュリティ管理者に通知し、適正な措置を求めること。

（３）　情報セキュリティ管理者の指導により改善されない場合は、統括情報セキュリティ責任者は、当該職員等のネットワーク若しくは情報システムを使用する権利を停止又は剥奪すること。

（４）　統括情報セキュリティ責任者は、職員等の権利を停止又は剥奪した旨を速やかにＣＩＳＯ及び当該職員等が所属する課の情報セキュリティ管理者に通知すること。

（５）　情報セキュリティポリシーに違反した職員等については、その重大性、発生した事案の状況等に応じ、必要な措置を講ずること。

11　業務委託と外部サービスの利用

11－１　業務委託

（１）　委託事業者の選定基準

①　情報システム管理者は、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　情報システム管理者は、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）　契約項目

情報システム管理者は、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。

①　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

②　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

③　提供されるサービスレベルの保証

④　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

⑤　委託事業者の従業員に対する教育の実施

⑥　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

⑦　業務上知り得た情報の守秘義務

⑧　再委託に関する制限事項の遵守

⑨　委託業務終了時の情報資産の返還、廃棄等

⑩　委託業務の定期報告及び緊急時報告義務

⑪　組合による監査、検査

⑫　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

⑬　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

①　情報システム管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置しなければならない。

②　情報システム管理者は、①において確認した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。

11－２　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、以下を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

①　外部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 11－２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指名と外部サービスの利用状況の管理

⑤　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）　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及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討しなければならない。

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及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定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外部サービス提供者の選定条件に含めなければならない。

③　情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、組合が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。

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

イ　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

ウ　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、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　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

④　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なければならない。

⑤　情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

⑥　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外部サービス提供者の選定条件に含めなければならない。

（注）　クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が組合によって受容可能か判断すること。

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

⑦　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外部サービス提供者を選定し、必要に応じて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。

⑧　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組合に提供し、組合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なければならない。また、外部サービス利用判断基準及び外部サー

ビス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

⑨　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定しなければならない。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。

⑩　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及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。

⑪　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しなければならない。

（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及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

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及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

（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には、利用申請の許可権限者へ外部サービスの利用申請を行わなければならない。

②　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定しなければならない。

③　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。（クラウドサービスを利用する場合も同様の措置を行う。）

（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
オ　クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

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・記録しなければならない。

③ クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

（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しなければならない。

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
ケ　設計・設定変更時の情報や変更履歴の管理

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しなければならない。

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・記録しなければならない。

④ クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

（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しなければならない。

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・記録しなければならない。

③ クラウドサービス管理者は、クラウドサービス上で機密性の高い情報を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

11－３　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しなければならない。

① 外部サービスを利用可能な業務の範囲

② 外部サービスの利用申請の許可権限者と利用手続

③ 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

④ 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しなければならない。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じなければならない。

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、利用の可否を決定しなければならない。また、承認した外部サービスを記録しなければならない。

12　評価・見直し

12－１　監査

（１）　実施方法

ＣＩＳＯは、情報セキュリティ監査統括責任者を指名し、ネットワーク、情報システム等の情報資産における情報セキュリティ対策状況について、

毎年度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

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。

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　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、委員会の承認を得なければならない。

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、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。

②　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を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

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、委員会に報告しなければならない。

（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及び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

①　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。

②　ＣＩＳＯは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

③　ＣＩＳＯは、組合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、関係規程等の見直し等への活用

委員会は、監査結果を情報セキュリティポリシー、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。

12－２　自己点検

（１）　実施方法

①　統括情報セキュリティ責任者及び情報システム管理者は、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。

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、所管する課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

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、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、委員会に報告しなければならない。

（３）　自己点検結果の活用

①　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②　委員会は、当該点検、結果を情報セキュリティポリシー、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。

12－３　情報セキュリティポリシー、関係規程等の見直し

委員会は、情報セキュリティ監査、自己点検結果、情報セキュリティに関する状況変化等を踏まえ、情報セキュリティポリシー等関係規程について毎年度及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。