神戸市職員共済組合情報セキュリティ対策基準

平成 29 年 2 月 28 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、嘱託職員及び臨時的任用職員（以下「職員等」という。）が遵守する基準である。

１　対象範囲及び体制等

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及び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）　最高情報統括責任者（ＣＩＯ：Chief Information Officer、以下「ＣＩＯ」という。）

①　ＣＩＯは、事務局長とする。

②　ＣＩＯは、組合の情報資産を統括する最高責任者とする。

（２）　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、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、ＣＩＯと兼務とする。

（３）　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、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行う権限及び責任を有する。

④　統括情報セキュリティ責任者は、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。

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。

（４）　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。

（５）　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。

（６）　情報システム管理者

①　情報システムに関する情報システム管理者を事務局次長とする。

②　情報システム管理者は、所管する情報システムの開発、運用管理の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。

（７）　情報セキュリティ委員会（以下「委員会」という。）

①　委員会は、ＣＩＯ、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、庶務係において処理する。

（８）　兼務の禁止

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

②　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。

2　情報資産の管理方法等

（1）　情報資産の重要性分類

組合における情報資産は、次のとおり重要性に応じて分類した上で管理をしなければならない。

Ⅰ	個人情報（個人番号及び特定個人情報を含む。）、業務上必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
Ⅱ	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
Ⅲ	外部に公開する情報のうち、セキュリティ侵害が業務の執行等に軽微な影響を及ぼす情報資産
Ⅳ	上記以外の情報資産

（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重要性分類に基づき管理しなければならない。

ウ　重要性分類Ⅱ以上の電子データ又は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。

②　情報資産の重要性分類の表示

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）、格納する記録媒体のラベル、文書の隅等に、重要性分類を表示する等適切な管理を行わなければならない。

③　情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に重要性分類に基づき、当該情報の重要性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、重要性分類に基づき、当該情報の重要性分類を行わなければならない。

ウ　情報資産を入手した者は、入手した情報資産の重要性分類が不明な場合、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、情報資産の重要性分類に応じ、適切な取扱いをしなければならない。

ウ　情報資産を利用する者は、電磁的記録媒体に情報資産の重要性分類が異なる情報が複数記録されている場合、最高度の重要性分類に従って、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、情報資産の重要性分類に従って、情報資産を適切に保管しなければならない。

イ　情報セキュリティ管理者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、重要性分類Ⅱ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。

⑦　情報の送信

電子メール等により重要性分類Ⅱ以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧　情報資産の運搬

ア　重要性分類Ⅱ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、又は暗号化若しくはパスワードの設定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Ⅱ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　職員等は、情報セキュリティ管理者の許可が有る場合を除き、重要性分類Ⅱ以上の情報を外部へ送付し、又は持ち出してはならない。

イ　重要性分類Ⅱ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

ウ　重要性分類Ⅱ以上の情報資産を外部に提供する場合は、信頼できる者を選定し、送受の証拠が残るようにしなければならない。

エ　情報セキュリティ管理者は、外部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

ア　重要性分類Ⅱ以上の情報資産を廃棄する者は、電磁的記録媒体を初期化する等情報を復元できないように処置した上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、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。

3　物理的セキュリティ

3―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、重要な情報資産を管理する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、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②　情報システム管理者は、統括情報セキュリティ責任者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、サーバ機器等を保護

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切に管理しなければならない。

④　統括情報セキュリティ責任者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外部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、重要性分類Ⅱ以上の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外部の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。ただし、内容を消去することが組合の業務に多大な影響があると情報システム管理者が判断した場合は、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った上で、内容を消去せずに外部の事業者に修理をさせることができるものとする。

（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

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、すべ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。

３―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「共済組合システム室」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、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。

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、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、共済組合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等による入退室管理を行わなければならない。

②　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。

③　職員等及び外部委託事業者は、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。

④　情報システム管理者は、重要性分類Ⅱ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、あらかじめ職員等又は委託した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、管理区域からの機器等の搬入出について、職員等を立ち会わせなければならない。

３－３　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。

３―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、適切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、重要性分類Ⅱ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。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、重要性分類Ⅱ以上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。

３－５ 職員等のパソコン等の管理

① 情報システム管理者は、盗難防止のため、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及びモバイル端末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。

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、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用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。

4　人的セキュリティ

4―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の遵守

ア　職員等は、情報セキュリティポリシー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　パソコン等の端末の持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Ⅱ以上の情報資産を外部で処理する場合には、情報セキュリティ管理者に安全管理措置を定めさせなければならない。

イ　職員等は、組合のパソコン等の端末、記録媒体及びソフトウェア等の情報資産を外部に持出す場合には、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　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

ア　職員等は、業務上支給されたもの以外のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

イ　職員等は、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、安全管理措置を遵守しなければならない。

⑤　持出し及び持込みの記録

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

⑥　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の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システム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、パソコン等の端末、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端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等適切な措置を講じなければならない。

⑧　退職時等の遵守事項

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。

（２）　非常勤職員、派遣職員、嘱託職員及び臨時的任用職員（以下「非常勤職員等」という。）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、非常勤職員等に対し、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、実施させ、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及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員等にパソコン等の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、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を閲覧できるように掲示しなければならない。

（４）　外部委託事業者に対する説明

情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部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外部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。

４―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 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 研修計画において、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及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤ 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、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制及び範囲等を定め、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

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。

４―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、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に報告しなければならない。

③　統括情報セキュリティ責任者は、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、必要に応じて全国市町村職員共済組合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、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に報告しなければならない。

③　統括情報セキュリティ責任者は、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、必要に応じて全国市町村職員共済組合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連絡手段を公表しな

ければならない。

（３）　情報セキュリティインシデント原因の究明・記録、再発防止等

①　統括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした情報セキュリティ管理者及び情報システム管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。

②　統括情報セキュリティ責任者は、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。

③　ＣＩＳＯは、統括情報セキュリティ責任者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。

４―４　ＩＤ及びパスワードの管理

職員等は、自己の管理するＩＤ及びパスワードについて、次の事項を遵守しなければならない。

（１）　ＩＤの取扱い

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。

（２）　パスワードの取扱い

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、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤　パスワードは定期的又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

⑥　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。

⑦　仮のパスワードは、最初のログイン時点で変更しなければならない。

⑧　パソコン等の端末のパスワードの記憶機能を利用してはならない。

⑨　職員等間でパスワードを共有してはならない。

⑩　パスワードを記載したメモを作成してはならない。

5　技術的セキュリティ

5―1　ネットワーク、情報システム及び情報資産の管理

（1）　アクセス記録の取得

①　情報システム管理者は、重要性分類Ⅰの資産を扱う情報システムについて、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定期間保管しなければならない。

②　情報システム管理者は、定期的に当該記録を分析し、及び監視しなければならない。

（2）　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。

（3）　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切に管理しなければならない。

③　統括情報セキュリティ責任者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外部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。

（４）　システム関連情報の保管

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、情報システムの仕様書、システム構成図及びネットワーク構成図等を適切に保管し、業務上必要とする者のみが閲覧できるようにしなければならない。

（５）　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、適切に保存しなければならない。

（６）　バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、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。

（７）　電子メールの利用制限

①　職員等は、自動転送機能を用いて電子メールを転送してはならない。

②　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスが分からないようにしなければならない。

④　職員等は、重要性分類Ⅱ以上の内容の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。

⑤　職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（８）　外部ネットワークとの接続

①　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。

② 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。

③ 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。

（９） 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、文書サーバを係等の単位で構成し、職員等が他係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、情報セキュリティ管理者から個人情報、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る必要があるとの報告を受けた場合は、同一係等であっても、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。

（10） 電子署名・暗号化

① 職員等は、情報資産の重要性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、暗号化又はパスワード設定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。

(11)　無許可ソフトウェアの導入の禁止

①　職員等は、端末に対して当該端末を管理する情報システム管理者に許可されていないソフトウェアを導入してはならない。

②　職員等は、業務を円滑に遂行するために必要とするソフトウェアの利用について、個別に統括情報セキュリティ責任者及び当該端末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。

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。

(12)　機器構成の変更

職員等は、業務上支給された端末に対し、統括情報セキュリティ責任者及び情報システム管理者の許可なく改造等を行ってはならない。

(13)　接続できる端末

職員等が組合のネットワークに接続することができる端末は、組合から業務上支給された端末のみとする。

(14)　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、イメージスキャナ及び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、適切なセキュリティ要件を策定しなければならない。

②　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機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、受信相手を確認後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。

(15)　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電話システム等通信回線に接続している機器をいう。）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

５―２　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）　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、変更及び抹消の情報管理並びに職員等の異動、出向及び退職に伴う利用者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）　職責に応じた権限の設定

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、外部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よりも定期的変更又は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担当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、外部からのアクセスに使用し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の有無、パッチの適用状況等を確認しなければならない。

⑦　統括情報セキュリティ責任者は、公衆通信回線（公衆無線ＬＡＮ等）の組合外通信回線を内部のネットワークに接続してはならない。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及び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）　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。

（８）　パスワードに関する情報の管理

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、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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、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。

５―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恐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、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

ウ　情報システム管理者は、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、個人情報及び重要性Ⅱ以上の情報をマスキングせずテストデータとして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切に整備・保管しなければならない。

②　情報システム管理者は、テスト結果を一定期間保管しなければならない。

③　情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（５）　情報システムにおける入出力データの正確性の確保

①　情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②　情報システム管理者は、故意又は過失により情報が改ざんされ、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。

５―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の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。

（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ること。

②　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。

③　不正プログラム対策ソフトウェアのパターンファイル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。

（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（ノート）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、メールを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。

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、ＬＡＮケーブルの即時取り外しを行い、所管する情報システム管理者に報告すること。

５―５　不正アクセス対策

（１）　情報システム管理者の措置

①　情報システム管理者は、ファイヤウォールの設定で、使用終了又は使用される予定のないポートを長時間空けたままにしないようにし、セキ

ュリティホールの発見に努め、メーカーなどからパッチの提供があり次第速やかにパッチをあてなければならない。

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 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、設定しなければならない。

④ 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査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ることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、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、職員等及び外部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情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（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、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、職員等への教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部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

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。

（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。

（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。

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、適切かつ速やかに対処しなければならない。

③　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（2）　パソコン、モバイル端末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

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切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

委員会は、情報セキュリティに関する事故、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切に実施するために、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切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

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。

７－４　外部委託

（１）　外部委託による運用契約

情報システム管理者は、運用を外部委託する場合、委託業者に対してセキュリティに関する要件を記載した契約書を締結しなければならない。

（２）　情報システム管理者は、セキュリティに関する要件として、契約書に以下の項目を必要に応じて明記しなければならない。

①　受託者の守秘義務及び守秘義務違反の場合の措置及び罰則

②　データの保管、管理及び廃棄方法

③　再委託に関する制限事項の遵守

④　システムの運用管理状況及び障害状況の報告

⑤　事故報告などの緊急時の連絡体制及び緊急時の措置

⑥　委託内容の検査・監査に応じる義務

⑦　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

⑧　外部委託事業者の責任者、委託内容、作業者及び作業場所の特定

⑨　提供される通信の速度、安定性及びシステムの信頼性の確保等の品質レベルの保証

⑩　外部委託事業者にアクセスを許可する情報の種類と範囲及びアクセス方法

⑪　外部委託事業者の従業員に対する教育の実施

⑫　提供された情報の目的外利用及び受託者以外の者への提供の禁止

（３）　外部委託事業者の選定基準

①　情報システム管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②　情報システム管理者は、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、事業者を選定しなければならない。

③　情報システム管理者は、クラウドサービスを利用する場合は、情報の重要性に応じたセキュリティレベルが確保されているサービスを利用

しなければならない。

（４）　確認・措置等

①　情報システム管理者は、外部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、（１）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、当該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。

８　情報セキュリティ実施手順の策定

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順については、組合の事業運営に重大な支障を及ぼすおそれがあるため非公開とする。

９　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、ＣＩＳＯの許可を得ないで例外措置を取ることができる。この場合において、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切に保管し、定期的に申請状況を確認しなければならない。

10　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、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

（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）

11　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情報セキュリティ管理者に通知し、適切な措置を求める。

（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情報セキュリティ管理者に通知し、適切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ができる。

（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しなければならない。

（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とする。

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

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）　外部委託事業者に対する監査

外部委託事業者に委託している場合､情報セキュリティ監査統括責任者(外部委託事業者から下請けとして受託している事業者を含む｡)は､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、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切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。

（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

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、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、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。

12－３　情報セキュリティポリシー及び関係規程等の見直し

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。