一般財団法人鹿児島県教職員互助組合
情報セキュリティポリシー

一般財団法人鹿児島県教職員互助組合情報セキュリティポリシー

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、一般財団法人鹿児島県教職員互助組合（以下「互助組合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、互助組合が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

(1)　情報資産

コンピュータ、ネットワーク、情報システム及びこれらの仕様書、関連文書並びに職員が業務上知り得た個人情報等をいう。

(2)　コンピュータ

電子計算機及びパーソナルコンピュータ（以下「パソコン」という。）をいう。

(3)　ネットワーク

コンピュータを相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(4)　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(5)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(6)　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(7)　機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

(8)　完全性

情報資産が破壊、改ざん又は消去されていない状態を確保することをいう。

(9)　可用性

情報資産にアクセスすることを認められた者が、必要なときに中断される

ことなく、情報資産にアクセスできる状態を確保することをいう。

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1)　サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

４　適用範囲

本基本方針が対象とする情報資産は、２定義(１)の情報資産の範囲内とする。

５　職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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。

６　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1)　組織体制

互助組合の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2)　セキュリティ対策基準の構成

互助組合の保有する情報資産を機密性、完全性及び可用性に応じて構成し、当該構成に基づき情報セキュリティ対策を行う。

(3)　物理的セキュリティ

サーバ等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4)　人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、

十分な啓発を行うなどの人的な対策を講じる。

(5)　技術的セキュリティ

コンピュータ及びネットワークの管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6)　運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合または発生するおそれがある場合に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7　情報セキュリティ自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ自己点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティ自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

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は、公にすることにより互助組合の事業運営に重大な支障を及ぼすおそれがあることから非開示とする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための互助組合の情報資産に関する情報セキュリティ対策の基準である。

その対策基準は以下に掲げる８項目に分け策定及び管理を行う。

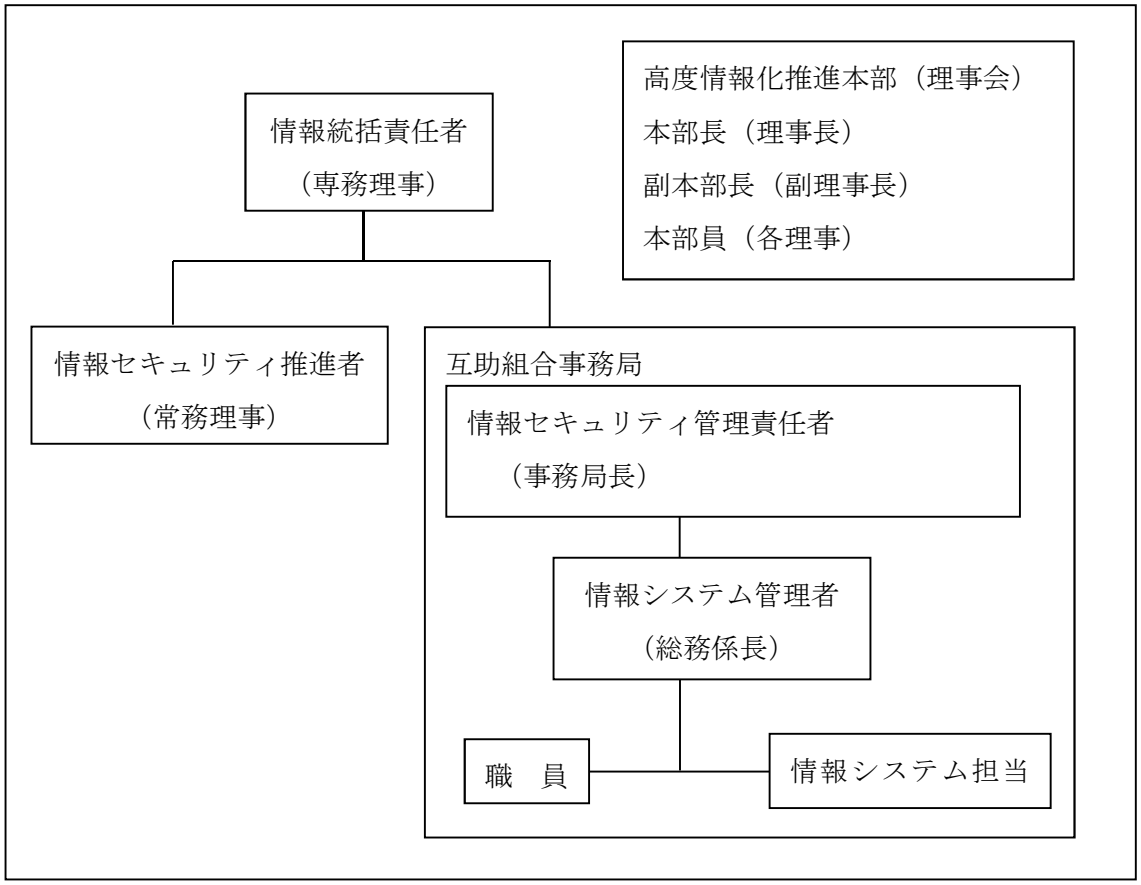
①　組織体制

②　セキュリティ対策基準の構成

③　物理的セキュリティ
④　人的セキュリティ
⑤　技術的セキュリティ
⑥　運用
⑦　情報セキュリティ自己点検の実施
⑧　情報セキュリティポリシーの見直し

1　組織体制

互助組合の情報セキュリティ管理については、以下の組織体制とする。



(1)　高度情報化推進本部

①　理事会を高度情報化推進本部とする。

②　互助組合の情報セキュリティ対策を統一的に行うため、理事会において、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決定する。

(2)　情報統括責任者

①　専務理事を、情報統括責任者とする。専務理事は、互助組合における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュ

リティ対策の実施に関する最終決定権限及び責任を有する。

② 専務理事は、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アドバイザーとして置くことができる。

(3) 情報セキュリティ推進者

① 常務理事を、情報セキュリティ推進者とする。常務理事は、専務理事を補佐する。

② 常務理事は、互助組合の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 常務理事は、互助組合の全てのネットワークにおける情報セキュリティ対策の実施に関する権限及び責任を有する。

④ 常務理事は、情報セキュリティ管理責任者、情報システム管理者及び情報システム担当者に対して、情報セキュリティ対策の実施に関する指導及び助言を行う権限を有する。

⑤ 常務理事は、互助組合の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、専務理事の指示に従い、専務理事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。

⑥ 常務理事は、互助組合の共通的なネットワーク、情報システムなど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。

⑦ 常務理事は、緊急時等の円滑な情報共有を図るため、情報統括責任者、情報セキュリティ管理責任者、情報システム管理者及び情報システム担当者を網羅する連絡体制を整備しなければならない。

(4) 情報セキュリティ管理責任者

① 事務局長を情報セキュリティ管理責任者とする。

② 事務局長は、互助組合事務局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③ 事務局長は、互助組合事務局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④ 事務局長は、互助組合事務局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び

指示を行う。

(5)　情報システム管理者

①　総務係長を、情報システム管理者とする。

②　総務係長は、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。

③　総務係長は、情報システムにおける情報セキュリティ対策の実施に関する権限及び責任を有する。

④　総務係長は、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)　情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、見直し等の作業を行う者を、情報システム担当者とする。

(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　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　セキュリティ対策基準の構成

情報資産の機密性、完全性及び可用性の確保及び管理を以下のとおり行うものとする。

(1)　機密性

データの暗号化・パスワード設定・鍵付きケース保管

(2)　完全性

①　保管場所の制限と外部記録媒体の持込禁止

②　外部での情報処理を行う際の安全管理

(3)　可用性

①　データのバックアップ

②　システム及びデータの復旧

３　物理的セキュリティ

(1)　サーバ等の管理

①　機器の取付け

総務係長は、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するとともに、故障等の障害に備えて２台設置することとし、容易に取り外せないよう適切に固定するなど、必要な措置を講じなければならない。

② 機器の電源

総務係長は、サーバ等の機器の電源について、停電（落雷）等による電供給の停止に備え、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、機器を保護するための措置を講じなければならない。

③ 機器の定期保守及び修理

ア 総務係長は、必要に応じて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 総務係長は、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。内容を消去できない場合、総務係長は、外部の業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認等を行わなければならない。

④ 機器の廃棄等

総務係長は、機器の廃棄、リース返却等をする場合、機器の記録装置等から、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。また、廃棄を業者に委託する場合、廃棄証明を発行してもらうなど、確実に廃棄されたかを確認しなければならない。

⑤ 機器等の搬入出

ア 総務係長は、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した業者に確認を行わせなければならない。

イ 総務係長は、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。

(2) 通信回線及び通信回線装置の管理

① 総務係長は、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。

② 総務係長は、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。

(3)　クライアント（パソコン）等の管理

①　事務局長及び総務係長は、事務局内のパソコン等の機器及び記録媒体について、盗難防止のための必要な措置を講じなければならない。

②　総務係長は、情報システムにログインするためにパスワードを設定しなければならない。

4　人的セキュリティ

(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を遵守する。

イ　業務以外の目的での情報資産の使用を禁止する。

ウ　パソコン等の端末の持ち出し及び外部における情報処理作業を制限する。

エ　パソコン等の持込を原則禁止する。

オ　持ち出しの記録

事務局長は、パソコン等の機器及び記録媒体の持ち出しについて、記録を作成し、保管しなければならない。

カ　パソコン等の端末におけるセキュリティ設定変更を禁止する。

キ　ファイル交換（共有）ソフトウェアの導入等を禁止する。

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　情報セキュリティポリシー等の掲示

事務局長または総務係長は、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。

③　外部委託事業者に対する説明

事務局長は、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て、情報セキュリティポリシー等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。

(2)　事故、欠陥等の報告

①　事務局からの事故等の報告

ア　職員等は、情報セキュリティに関する事故、情報システム上の欠陥及び

誤動作を発見した場合、速やかに各部長に報告しなければならない。

イ　報告を受けた各部長は、速やかに専務理事、常務理事、事務局長及び総務係長に報告しなければならない。

②　組合員等外部からの事故等の報告

ア　職員等は、互助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事故、欠陥について、組合員等外部から報告を受けた場合、各部長に報告しなければならない。

イ　報告を受けた各部長は、速やかに専務理事、常務理事及び事務局長に報告しなければならない。

ウ　専務理事は、情報システム等の情報資産に関する事故、欠陥について、組合員等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

③　事故等の分析・記録等

常務理事は、事故等を引き起こした部門の部長及び総務係長と連携し、これらの事故等を分析し、記録を保存しなければならない。

(3)　ＩＤ及びパスワード等の管理

①　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。

②　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、事務局長に速やかに報告し、パスワードを速やかに変更しなければならない。

オ　パスワードは定期的に、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。

５　技術的セキュリティ

(1)　コンピュータ及びネットワークの管理

①　バックアップの実施

総務係長は、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。また、バックアップデータを分散するため、データセンター等に預けるなど、事務局以外にも保管を行わなければならない。

②　他団体との情報システムに関する情報等の交換

総務係長は、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、常務理事及び事務局長の許可を得なければならない。

③　障害記録

総務係長は、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。

④　ネットワークの接続制御、経路制御等

ア　総務係長は、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　総務係長は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑤　無線 LAN及びネットワークの盗聴対策

常務理事は、無線 LANの利用を認めるに当たっては、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

⑥　電子メールのセキュリティ管理等

ア　電子メールのセキュリティ管理

(ｱ)　総務係長は、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)　総務係長は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

(ｳ)　総務係長は、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)　総務係長は、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。

イ　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、事務局長に報告しなければならない。

(ｵ)　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。

⑦　Ｗｅｂファイル共有システムのセキュリティ管理等

ア　Ｗｅｂファイル共有システムのセキュリティ管理

(ｱ)　総務係長は、外部から外部へのファイル共有が行われることを不可能とするよう、Ｗｅｂファイル共有システムのサーバの設定を行わなければならない。

(ｲ)　総務係長は、共有フォルダの容量の上限を設定し、上限を超えるファイルの共有を不可能にしなければならない。

(ｳ)　総務係長は、共有フォルダの容量の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。

(ｴ)　総務係長は、システム開発や運用、保守等のためＷｅｂファイル共有システムを利用する委託先との間で利用方法を取り決めなければならない。

⑧　ソフトウェアのライセンス管理

ア　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。また、ライセンスを超えたインストールを行ってはならない。

イ　常務理事、事務局長又は総務係長は、その調達に係るソフトウェアのライセンスを適正に管理しなければならない。

(2)　アクセス制御

①　アクセス制御

総務係長は、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、必要に応じてシステム上制限しなければならない。

② パスワードに関する情報の管理

総務係長は、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。

(3) 情報システム開発、導入、保守等

① 情報システムの調達

ア 総務係長は、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。

イ 総務係長は、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

ア 総務係長は、情報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。

イ 情報システム開発における責任者、作業者のＩＤの管理

(ｱ) 総務係長は、情報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) 総務係長は、情報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らない。

ウ 情報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) 総務係長は、情報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) 総務係長は、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情報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

ア 開発環境と運用環境の分離及び移行手順の明確化

(ｱ) 総務係長は、情報システム開発、保守及びテスト環境と情報シス

テム運用環境を分離しなければならない。

(ｲ)　総務係長は、情報システム開発・保守及びテスト環境から情報システム運用環境への移行について、情報システム開発・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)　総務係長は、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。

イ　テスト

(ｱ)　総務係長は、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)　総務係長は、運用テストを行う場合、充分な操作確認を行わなければならない。

(ｳ)　総務係長は、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。

④　情報システム開発・保守に関連する資料等の保管

ア　総務係長は、情報システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

イ　総務係長は、テスト結果を一定期間保管しなければならない。

ウ　総務係長は、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

ア　総務係長は、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　総務係長は、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。

ウ　総務係長は、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

総務係長は、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

総務係長は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

⑧　システム更新又は統合時の検証等

総務係長は、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。

(4)　不正プログラム対策

①　常務理事の措置事項

常務理事は、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　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。

②　総務係長の措置事項

総務係長は、不正プログラム対策として、次の事項を措置及び監視しなければならない。

ア　所管するサーバ、パソコン等に、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。

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　ネットワークに接続していない情報システムにおいて、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、互助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物理的に排除されている場合を除き、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。

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。

ア　パソコン等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　パソコン等について、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。

カ　常務理事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が検出された場合は、各部長に報告しなければならない。この場合、各部長は直ちに専務理事、常務理事、事務局長及び総務係長に報告するとともに、その指示に従わなければならない。

④　専門家の支援体制

常務理事は、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　総務係長の措置事項

総務係長は、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するよう設定しなければならない。

②　攻撃の予告

専務理事及び常務理事は、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。

③　記録の保存

専務理事及び常務理事は、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

常務理事及び総務係長は、職員等及び外部委託事業者が使用しているパソ

コン等からの事務局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

常務理事及び総務係長は、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部長に通知し、適切な処置を求めなければならない。

６　運用

(1)　情報システムの監視

常務理事及び総務係長は、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)　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　事務局長及び部長は、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、速やかに専務理事及び常務理事に報告しなければならない。

イ　専務理事は、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。

ウ　常務理事及び総務係長は、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、記録媒体等の利用状況調査

専務理事が指名した者は、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、記録媒体等のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

③　職員等の報告義務

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、直ちに常務理事及び部長に報告を行わなければならない。

イ　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常務理事が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(3)　緊急時の対応

①　緊急時対応計画の策定

理事会は、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。

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 緊急時対応計画の見直し

理事会は、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。

(4) 外部委託

① 外部委託事業者の選定基準

ア 各部長は、外部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。

イ 各部長は、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、外部委託事業者を選定しなければならない。

② 契約項目

情報システムの運用、保守等を外部委託する場合には、外部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。

ア 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

イ 外部委託事業者の責任者、委託内容、作業者、作業場所の特定

ウ 提供されるサービスレベルの保証

エ 従業員に対する教育の実施

オ 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

カ 業務上知り得た情報の守秘義務

キ 再委託に関する制限事項の遵守

ク 委託業務終了時の情報資産の返還、廃棄等

ケ　委託業務の定期報告及び緊急時報告義務

コ　互助組合による監査、検査

サ　互助組合による事故時等の公表

シ　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

部長は、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、②の契約に基づき措置しなければならない。また、その内容を専務理事及び常務理事に報告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　就業規則

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　一般財団法人鹿児島県教職員互助組合個人情報保護規程

(6)　懲戒処分等

①　違反者に対する処分等

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、法令違反、就業規則による懲戒処分等の対象とする。

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、速やかに次の措置を講じなければならない。

ア　常務理事が違反を確認した場合は、常務理事は当該職員等が所属する部長に通知し、適切な措置を求めなければならない。

イ　総務係長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常務理事及び当該職員等が所属する部長に通知し、適切な措置を求めなければならない。

ウ　部長の指導によっても改善されない場合、常務理事は、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、常務理事は、職員等の権利を停止あるいは剥奪した旨を専務理事及び当該職員等が所属する部長に通知しなければならない。

７　セキュリティポリシーの自己点検

(1)　実施方法

①　常務理事及び総務係長は、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　事務局長は、部長と連携して、所管する部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

常務理事、事務局長及び総務係長は、自己点検結果と自己点検結果に基づく改善を取りまとめ、理事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　理事会は、この点検結果を情報セキュリティポリシーの見直し、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。

８　情報セキュリティポリシーの見直し

理事会は、情報セキュリティポリシーについて情報セキュリティ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ふまえ、毎年度評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

この情報セキュリティポリシーは、令和８年４月１日から施行する。