茨城県看護教育財団情報セキュリティポリシー対策基準

情報セキュリティポリシー対策基準とは、情報セキュリティポリシー基本方針を実行に移すための財団の情報資産に関する情報セキュリティポリシー対策の基準である。

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

財団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) 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、財団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、財団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、財団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。

(2) 情報システム管理者

① 事務局次長を、情報システム管理者とする。

② 事務局次長は、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 事務局次長は、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 事務局次長は、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。

(3) 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。

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

事務局次長は、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、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

事務局次長は、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　事務局次長は、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　事務局次長は、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、事務局次長は、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

事務局次長は、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　事務局次長は、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　事務局次長は、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　事務局次長は、 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　事務局次長は、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　事務局長及び事務局次長は、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　事務局次長は、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

事務局長または事務局次長は、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)　ＩＤ及びパスワード等の管理

①　ＩＤの取扱い

職員等は、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

事務局次長は、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。

②　障害記録

事務局次長は、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。

③　ネットワークの接続制御、経路制御等

ア　事務局次長は、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　事務局次長は、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。

④　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)　事務局次長は、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)　事務局次長は、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。

(ｳ)　事務局次長は、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。

⑤　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　事務局長又は事務局次長は、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

事務局次長は、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

事務局次長は、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) 不正プログラム対策

①　事務局長の措置事項

事務局次長は、不正プログラム対策として、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ほか、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、財団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。

② 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。

6 運用

(1) 情報システムの監視

事務局長及び事務局次長は、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

事務局長及び事務局次長は、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

事務局長が指名した者は、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、直ちに事務局長に報告を行わなければならない。

(3)　外部委託

①　外部委託事業者の選定基準

ア　事務局次長は、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　事務局次長は、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　財団による監査、検査

サ　財団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

事務局次長は、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。

(4)　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）

7　セキュリティポリシーの自己点検

(1)　実施方法

事務局長及び事務局次長は、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)　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　事務局は、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

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。