

半田常滑看護専門学校管理組合情報セキュリティ基本方針

(目的)

第1条 この方針は、当組合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、当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。

(用語の定義)

第2条 この方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) ネットワーク コンピュータ等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。
- (2) 情報システム コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。
- (3) 情報資産 記録媒体に関わらず、組合が保有する全ての情報のうち、管理すべき情報をいう。
- (4) 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。
- (5) 情報セキュリティポリシー この方針及び情報セキュリティ対策基準をいう。
- (6) 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。
- (7) 完全性 情報が破壊、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。
- (8) 可用性 情報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、情報にアクセスできる状態を確保することをいう。
- (9) マイナンバー利用事務系 個人番号利用事務に関わる情報システム及びデータをいう。
- (10) インターネット接続系 インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。
- (11) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(対象とする脅威)

第3条 情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施するものとする。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な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) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等
(適用範囲)

第4条 この方針の適用範囲は次のとおりとする。

- (1) この方針が適用される行政機関は半田常滑看護専門学校管理組合、半田常滑看護専門学校管理組合議会及び半田常滑看護専門学校管理組合監査とする。
- (2) この方針が対象とする情報資産は、次に掲げるものとする。
 - ア ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
 - イ 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。)
 - ウ 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
(職員の遵守義務)

第5条 当組合の業務に従事する全ての職員は、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。

(情報セキュリティ対策)

第6条 第3条の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

- (1) 当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全庁的な組織体制を確立するものとする。
- (2) 当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分類し、当該分類に基づき情報セキュリティ対策を実施するものとする。
- (3) 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じるものとする。
 - ア マイナンバー利用事務系においては、原則として、他の領域との通信をできないよ

うにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、情報の流出を防ぐものとする。

イ インターネット接続系においては、ファイアウォールによる通信制御や不正通信の監視等の情報セキュリティ対策を実施するものとする。

(4) サーバ室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じるものとする。

(5) 情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じるものとする。

(6) コンピュータ等の管理、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ものとする。

(7) 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、業務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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定するものとする。

(8) 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じること。

(9) 外部サービス(クラウドサービス)を利用する場合には、利用に係る規定を整備し対策を講じるものとする。

(10) ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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るものとする。

(情報セキュリティ監査及び自己点検の実施)

第7条 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監査及び自己点検を実施しなければならない。

(情報セキュリティポリシーの見直し)

第8条 情報セキュリティ監査及び自己点検の結果、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、保有する情報並びに利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直さなければならない。

(情報セキュリティ対策基準の策定)

第9条 前3条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ものとする。

2 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当組合の行政運営に重大な支障を及ぼすおそれがあることから公開してはならない。