〇三郡衛生組合情報セキュリティポリシー

1　目的

本基本方針は、三郡衛生組合(以下「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、組合が実施する情報セキュリティの基本方針及びこれを実行に移すための対策基準(以下「情報セキュリティポリシー」という。)を定めることを目的とする。

2　定義

(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。

(4)　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。

(5)　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。

(6)　可用性

情報にアクセスすることを認められた者が、必要な時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。

3　対象とする脅威

情報資産に対する脅威として、次のものを想定し、6 に規定する情報セキュリティ対策を実施する。

(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、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)　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

4　適用範囲

情報セキュリティポリシーが適用される範囲は、次の各号に掲げる区分に応じ、当該各号に定めるところによる。

(1)　組合の機関　事務局、公平委員会、監査委員及び議会

(2)　情報資産　次に掲げるもの

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

5　職員等の遵守義務

職員、非常勤職員、臨時職員等(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 10 に規定する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、次に掲げる情報セキュリティ対策を講じる。

(1)　組織体制

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。

(2)　情報資産の分類及び管理

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。

(3)　物理的セキュリティ

サーバ、サーバ室、通信回線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、十分な教育及び啓発を行う等の人的な対策を講じる。

(5)　技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策及び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及び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。

(8)　業務委託及び外部サービス(クラウドサービス)の利用

ア　業務委託を行う場合　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するとともに、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。

イ　外部サービス(クラウドサービス)を利用する場合　利用に係る規定を整備し対策を講じる。

ウ　ソーシャルメディアサービスを利用する場合　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する。

7　情報セキュリティ監査及び自己点検の実施

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監査及び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、保有する情報及び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、リスクを検討したうえで、情報セキュリティポリシーの見直しを行うものとする。

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、具体的な遵守事項及び判断基準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

上記 9 に規定する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、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。

11　その他

上記 9 及び 10 に規定する情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより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非公開とする。