広島市立病院機構情報セキュリティ基本方針

1　目的

本基本方針は、本機構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、本機構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)　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及びその構成機器（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

情報システムで取り扱うすべてのデータ（開発に係るデータを含む。）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)　機密性

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

(6)　完全性

情報及びその処理方法の正確さ並びに情報が破壊、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。

(7)　可用性

情報にアクセスすることを認められた者が、必要なときにアクセスできる状態を確保することをいう。

(8)　部門

本部事務局の各課、病院の各診療科、部、センター及び室をいう。

(9)　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。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、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)　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

4　適用範囲

(1)　対象とする機関の範囲

本基本方針は、本部事務局、広島市民病院、北部医療センター安佐市民病院、舟入市民病院及びリハビリテーション病院を適用範囲とする。

(2)　情報セキュリティ対策を実施する範囲

情報セキュリティ対策を実施する範囲は、次のとおりとする。

ア　情報資産及びこれを印刷した文書

イ　情報システム及びこれに関する設備、電磁的記録媒体

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

本機構に勤務する職員（嘱託職員、臨時職員、パート職員及び契約職員等を含む。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たり、情報セキュリティポリシー及び情報セキュリティ対策について具体的な実施手順を定めた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

対象とする脅威から情報資産を保護するため、次の情報セキュリティ対策を実施する。

(1)　管理体制

本機構が保有する情報資産について、情報セキュリティ対策を推進し、管理するための全機構的な体制を確立する。

(2)　情報資産セキュリティ

本機構の保有する情報資産を重要性に応じて分類し、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

サーバ等を設置する部屋、可搬記録媒体や情報システム機器の管理などの物理的な対策を実施する。

(4)　人的セキュリティ

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などの人的な対策を実施する。

(5)　技術的セキュリティ

コンピュータやネットワーク等の管理、不正アクセス対策などの技術的な対策を実施する。

(6)　調達・運用におけるセキュリティ

情報システムの機能設計・開発などの調達及び情報システム機器の保守・ユーザＩＤの利用者管理・情報セキュリティ事故等への対応などの運用における対策を実施する。

(7)　業務委託と外部サービスの利用におけるセキュリティ

①　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実施する。

②　外部サービスを利用する場合には、選定及び利用時に必要なセキュリティ対策を実施する。

③　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。

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、定期的に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驚異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実施する。

9　情報セキュリティ対策基準及び実施手順の策定

(1)　本基本方針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。

(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る情報セキュリティ実施手順を策定する。