地方独立行政法人宮城県立病院機構情報セキュリティ基本方針

1 目的

宮城県立病院機構が取り扱う医療情報及びこれに関連する情報（以下「医療情報」という。）には、地域住民の個人情報をはじめ病院運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。これらの守るべき情報や情報を取り扱う情報ネットワーク及び情報システム等を災害・事故・故意及び過失等の様々な脅威から防御することは、宮城県立病院機構に対する患者や地域住民の信頼の維持・向上に寄与するものである。

宮城県立病院機構情報セキュリティ基本方針は、宮城県立病院機構の情報セキュリティ対策の基本的な方針として、適用の対象や位置づけ等を定め、宮城県立病院機構が所掌する情報資産の機密性、完全性及び可用性を維持し、総合的・体系的且つ継続的に情報セキュリティ対策を図ることを目的とする。

2 用語の定義

(1) コンピュータ

パーソナルコンピュータ、サーバ、モバイル端末、ストレージ等の機器をいう。

(2) 情報ネットワーク

コンピュータを相互に接続するための通信網、接続機器のハードウエア及びソフトウエア並びに電磁的記録媒体で構成され、処理を行う仕組みを情報ネットワークという。

(3) 情報システム

ハードウエア及びソフトウエアで構成されるコンピュータ、情報ネットワーク並びに電磁的記録媒体で構成され、処理を行う仕組みを情報システムという。(サーバ、パソコン等)

(4) 情報資産

次の各号を情報資産という。

ア：情報ネットワークと情報システムの開発・運用に係る全ての情報及び情報ネットワークと情報システムで取り扱う全ての情報

イ：アの情報が記録された紙等の有体物及び電磁的記録媒体

ウ：情報ネットワーク及び情報システム

(5) 情報セキュリティ

情報資産の機密性、完全性、可用性を維持すること。

機密性：アクセスを許可された者だけが情報にアクセスできることを確実にすること。

完全性：情報及び処理方法が正確であること及び完全である状態を保護すること。

可用性：許可された利用者が必要な時に情報及び関連する資産にアクセスできることを確実にすること。

(6)業務系

電子カルテや部門システム等の患者情報を取り扱う医療情報システム（以下「医療情報システム」という。）及びデータをいう。医療機器等、直接医療情報システムと連携しないが、ネットワークを介して医療情報システムと接続する機器は業務系として取り扱う。

(7)情報系

業務系を除く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。当機構が業務で使用するために提供するインターネットに接続されたネットワーク及び同ネットワーク上で使用する機器全般のうち特定のもの。

(8)その他のネットワーク機器

その用途又はセキュリティの観点から情報系とは分離した情報ネットワーク及び同ネットワーク上で使用する機器全般をいう。

(9)通信経路の分割

業務系と情報系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

3 情報セキュリティ関係規定の位置づけと規定の体系

宮城県立病院機構情報セキュリティ関係規定は、宮城県立病院機構が所掌する情報資産に関する情報セキュリティ対策について総合的且つ体系的に取りまとめたものである。また、宮城県立病院機構情報セキュリティ基本方針と宮城県立病院機構情報セキュリティ対策基準を併せたものを「情報セキュリティポリシー」という。

宮城県立病院機構セキュリティ関係規定の構成

<table>
<tr><th>区分</th><th colspan="2">内容</th></tr>
<tr><td>宮城県立病院機構情報セキュリティ基本方針</td><td>宮城県立病院機構が所掌する情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものであり、情報セキュリティ対策の頂点に位置するものである。</td><td rowspan="2">宮城県立病院機構情報セキュリティポリシー（情報セキュリティ対策本部において決定する。）</td></tr>
<tr><td>宮城県立病院機構情報セキュリティ対策基準</td><td>宮城県立病院機構情報セキュリティ基本方針に基づき、情報セキュリティ対策を統一的に講ずるために、職員等 が遵守すべき行為及び判断等の基準を規定するものである。</td></tr>
<tr><td>情報セキュリティ実施手順</td><td colspan="2">宮城県立病院機構情報セキュリティポリシーに基づき、情報セキュリティ対策を具体的に実施するために、職員等が遵守すべき情報セキュリティ対策の実施手順を具</td></tr>
</table>

	体的に規定するものである。(各病院長が決定する。) 内容については、「宮城県立病院機構ネットワーク運用管理要領」、宮城県立精神医療センター並びに宮城県立がんセンターが定める医療情報システム運用管理規程に類似するため、これを情報セキュリティ実施手順とする。

4 適用範囲

宮城県立病院機構情報セキュリティポリシー（以下、「本ポリシー」という）の適用範囲は、以下の各号に示すものとする。

(1) 適用組織

宮城県立病院機構の本部事務局、宮城県立精神医療センター並びに宮城県立がんセンターとする。

(2) 適用情報資産

適用組織が所掌する情報資産とする。

(3) 適用対象

適用される情報資産に接する適用組織の職員（有期雇用職員等を含む。以下「職員等」という。）とする。

5 職員等の義務

(1) 遵守義務

職員等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共に、宮城県立病院機構が所掌する情報資産を取り扱う際には、「不正アクセス行為の禁止等に関する法律」等の情報セキュリティに関連する法令並びに本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。

(2) 懲戒処分等

本ポリシーに違反した職員等は、その重大性及び発生した事案の状況等に応じて職員就業規則等による懲戒処分の対象となる場合がある。

6 情報セキュリティ管理体制

宮城県立病院機構の所掌する情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立する。

7 情報資産の分類

宮城県立病院機構の所掌する情報資産をその内容によって分類し、その重要度に応じた情報セキュリティ対策を講ずる。

８ 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) 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

９ 情報セキュリティ対策

宮城県立病院機構の所掌する情報資産を先に掲げた脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1) 情報システム全体の強靭性の向上

ア　情報技術の発展に伴うセキュリティ対策について、最新の技術に対する情報収集を行うなど危殆化を防ぐ努力を行う。

イ　インターネット等外部へのネットワーク接続においては、必要に応じて不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

(2) 物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入り、情報資産への損傷・妨害等を防ぐため、入退室や機器管理上の物理的な対策を講ずる。

(3) 人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めると共に、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育及び啓発が行われるよう必要な対策を講ずる。

(4) 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策等の技術的な対策を講ずる。

(5) 運用セキュリティ対策

情報セキュリティポリシーの実効性を確保するため、情報システム等の稼動状況の監視や情報セキュリティポリシーの遵守状況の確認のため、運用面における必要な対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするため、危機管理対策を講ずる。

(6) 業務委託と外部サービスの利用

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。また、外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

10 情報セキュリティ対策に関する規定の公開・非公開

宮城県立病院機構情報セキュリティ基本方針は公開するが、宮城県立病院機構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の公開は、犯罪の予防その他の公共の安全及び秩序の維持に支障を及ぼす恐れがあるため、これらは公開しない。

11 情報セキュリティ対策実施状況の検証

宮城県立病院機構情報セキュリティポリシーが適切に遵守されていることを確認するために、定期的に情報セキュリティ対策の実施状況について検証を行う。

12 情報セキュリティ対策の評価・見直し

情報セキュリティ対策の実施状況の検証結果、情報システムの変更、新たな脅威等情報セキュリティを取り巻く情報の変化に対応し、宮城県立病院機構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評価と見直しを適宜行う。

13 情報セキュリティ監査の実施

本部長は、情報セキュリティ監査統括責任者を指名し、別に定める情報セキュリティ監査実施手順に基づき、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わなければならない。

附則

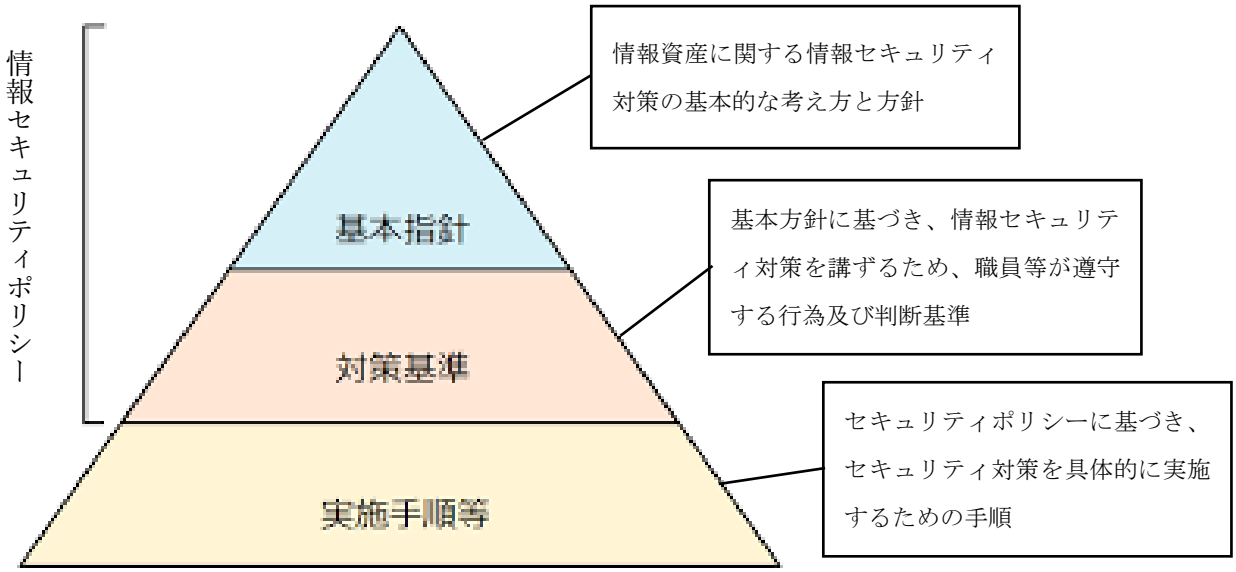
１　この基本方針の施行に伴い、次に掲げる要領は廃止する。

地方独立行政法人宮城県立病院機構情報セキュリティに関する要領（平成 24 年２月１日施行）

２　この宮城県立病院機構情報セキュリティ基本方針は、令和３年４月１日から施行する。

附則（令和８年３月２６日・一部改正）

この方針は、令和８年４月１日から施行する。


情報セキュリティポリシー
基本指針
対策基準
実施手順等
情報資産に関する情報セキュリティ対策の基本的な考え方と方針
基本方針に基づき、情報セキュリティ対策を講ずるため、職員等が遵守する行為及び判断基準
セキュリティポリシーに基づき、セキュリティ対策を具体的に実施するための手順