黒石市国民健康保険黒石病院
情報セキュリティポリシー

令和８年３月３０日　策定

黒石市国民健康保険黒石病院情報セキュリティポリシーの構成

黒石市国民健康保険黒石病院セキュリティポリシー（以下「セキュリティポリシー」という。）とは、黒石市国民健康保険黒石病院（以下「黒石病院」という。）が保有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、体系的かつ具体的に取りまとめたものである。

セキュリティポリシーは、黒石病院が所掌する情報資産を取り扱う職員（会計年度任用職員を含む。）及び委託事業者（従事者及び派遣労働者を含む。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、セキュリティポリシーを、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層に分け、それぞれを策定することとする。また、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」を策定することとする。

（下表参照）

セキュリティポリシーの構成

文書名		内容
セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づく情報セキュリティ対策を実施するための具体的な手順

黒石市国民健康保険黒石病院情報セキュリティ基本方針

1　目的

この情報セキュリティ基本方針は、黒石病院が保有する情報資産を様々な脅威から防御し、その機密性、完全性及び可用性（※注）を確保するため、組織的かつ計画的に取り組むための統一的な方針であり、情報セキュリティを実践するにあたっての基本的な考え方及び方策を定め、患者の財産、プライバシー等を守り、また業務を継続的に安全に行うことで信頼の維持向上に寄与することを目的とする。

（※注）：国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

機密性（confidentiality）	情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性（integrity）	情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性（availability）	許可された利用者が必要なときに情報にアクセスできできることを確実にすること。

2　国のガイドライン等との関係

情報セキュリティポリシー及び実施手順の運用にあたっては、以下に掲げる国のガイドライン等の最新情報と齟齬がないように注意する必要があり、ガイドライン等にならい適宜見直しを行うこととする。

・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）
・医療情報システムの安全管理に関するガイドライン（厚生労働省）
・医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（経済産業省・総務省）
・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（個人情報保護委員会／厚生労働省）
・黒石市情報セキュリティ基本方針（黒石市）

3　個人情報保護との関係

個人情報については、情報セキュリティポリシーに定めるもののほか、個人情報の保護に関する法律（平成１５年法律第５７号）、黒石市個人情報の保護に関する法律施行条例（令和５年条例第１号）、黒石市国民健康保険黒石病院個人情報取扱い規則に定められた内容にも留意して取扱う。

4　用語の定義

この情報セキュリティポリシーにおいて、次に掲げる用語の意義は、当該各号に定めるところによる。

⑴　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。

⑵　情報システム

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。

⑶　情報資産

情報システム及び情報システムの開発と運用に係る全ての情報並びに情報システムにより取り扱われる全ての情報をいう。

⑷　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。

⑸　業務系ネットワーク（統合情報システム接続系）

電子カルテや部門システム等の患者情報を取扱う情報システム及びデータをいう。

⑹　部門系ネットワーク（部門システム接続系）

部門独自に構築されたネットワークに接続された情報システム及びその情報システムで取扱うデータをいう。

⑺　情報系ネットワーク（インターネット接続系）

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。

⑻　通信経路の分割

業務系ネットワーク及び部門系ネットワーク並びに情報系ネットワークの環境間の通信環境を分離したうえで、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。

⑼　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。

5　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

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

6 職員の義務

黒石病院が所掌する情報資産に関する業務に携わる職員（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もつとともに、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

7 情報セキュリティ対策

上記の対象とする脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴ 組織体制

院内の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

⑵ 情報資産の分類と管理

院内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。

⑶ 情報システム全体の強靭性の向上

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、次の三段階の対策を講じる。

① 業務系ネットワーク（統合情報システム接続系）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等により、患者情報の流出を防ぐ。

② 部門系ネットワーク（部門システム接続系）においては、部門系ネットワーク（部門システム接続系）と接続する業務用システムと、業務系ネットワーク（統合情報システム接続系）の情報システムとの通信経路を分割する。なお、両ネットワーク間で通信する場合には、ファイアウォールや中間サーバを設置する等の情報セキュリティ対策を実施する。

③ 情報系ネットワーク（インターネット接続系）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高度な情報セキュリティ対策を実施する。

⑷　人的セキュリティ

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、職員に対する周知徹底を図るため、教育及び啓発を行う。

⑸　物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産への損傷及び利用の妨害等から保護するために物理的な対策を講じる。

⑹　技術的セキュリティ

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理・暗号化処理等の技術的な対策を講じる。

⑺　運用

情報システムの監視、情報セキュリティ対策の遵守状況の確認等の対策を実施する。また、緊急事態において迅速な対応を可能とするための対策を講じる。

⑻　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。外部サービス（クラウドサービス）を利用する場合には、利用にかかる規程を整備し対策を講じる。

8　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。

9　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、情報セキュリティポリシーを見直す。

10　情報セキュリティ対策基準の策定

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実施するに当たって必要となる基本的な要件を明記した情報セキュリティ対策基準を定める。

11　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、主要な情報システム等について情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順を定める。