

大崎市民病院における情報セキュリティ基本方針，医療情報システム（総合運営システム）に係る規程について

○ 情報セキュリティ基本方針（抜粋）

○ 大崎市情報セキュリティ基本方針（令和3年大崎市訓令第13号）（抜粋）

- 1 目的** 本基本方針は，本市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，本市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，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) 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。
 - (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，情報に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。
 - (8)～(9) 略
 - (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) 略
 - (12) 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。

3 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，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

4 適用範囲

- (1) 行政機関の範囲
本基本方針が適用される行政機関は，市長，**公営企業管理者**，教育委員会，選挙管理委員会，監査委員，農業委員会，固定資産評価審査委員会及び議会とする。
- (2) 情報資産の範囲
本基本方針が対象とする情報資産は，次のとおりとする。
 - ① 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
 - ② 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。）
 - ③ 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，会計年度任用職員等(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，以下の情報セキュリティ対策を講じる。

- (1) 組織体制 本市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) 情報資産の分類と管理 本市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) 情報システム全体の強靱性の向上 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。
 - ①～② 略
 - ③ インターネット接続系においては，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。高度な情報セキュリティ対策として，都道府県及び市区町村のインターネットとの通信を集約した上で，自治体情報セキュリティクラウドの導入等を実施する。
 - (4) 物理的セキュリティ サーバ，情報システム室，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。
 - (5) 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。
 - (6) 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，不正アクセス対策等の技術的対策を講じる。
 - (7) 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，外部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) 外部サービスの利用 外部委託する場合には，外部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，外部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。
約款による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。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定める。
 - (9) 評価・見直し 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，運用改善を行い，情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は，適宜情報セキュリティポリシーの見直しを行う。
- 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，情報セキュリティポリシーを見直す。
 - 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。
 - 10 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，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。

附 則 この訓令は，令和3年4月1日から施行する。

○ 医療情報システム（総合運営システム）の管理規程（抜粋）

○ 大崎市病院事業総合運営システム運用管理規程（平成23年大崎市病院管理規程第8号）（抜粋）

- (目的)
- 第1条** この規程は，大崎市病院事業(以下「病院事業」という。)における総合運営システムの安全かつ合理的な運用を図り，併せて法令に基づき保存が義務付けられた診療録及び診療諸記録(以下「保存義務のある情報」という。)の電子媒体による運用の適正な管理を図るため，必要な事項を定めるものとする。
- (定義)
- 第2条** 総合運営システムとは，次のシステムをいう。
 - (1) 電子カルテシステム
 - (2) 電子カルテシステムと接続する各部門のシステム(以下「各部門システム」という。)
 - (3) 電子カルテシステム及び各部門システムに接続する各部署の機器(以下「接続機器」という。)
 - (4) 医事システム
 - (5) 事務部門システム(総合運営システムの管理体制)
 - 第3条** 総合運営システムを管理するため，次に掲げる責任者を置く。
 - (1) システム管理責任者
 - (2) 運用責任者
 - (3) 監視責任者
 - (4) 接続機器管理責任者(システム管理責任者)
 - 第4条** システム管理責任者は，院長又は院長が指名した者をもって充て，次に掲げる職務を行う。
 - (1) 総合運営システムの管理及び運営を統括すること。
 - (2) 保存義務のある情報の安全性を確保し，常に閲覧可能な状況に保存管理すること。
 - (3) この規程の周知徹底を図ること。
 - (4) ソフトウェアの導入(大崎市病院事業 IT推進委員会(以下「委員会」という。)の認定したものに限る。)を許可すること。
 - (5) 総合運営システムと外部システムとのデータ連携に関すること。(運用責任者)
 - 第5条** 運用責任者は，システム管理責任者が指名する者をもって充て，次に掲げる職務を行う。
 - (1) 総合運営システムの安全かつ合理的な運用に関すること。
 - (2) 総合運営システムの利用マニュアル，仕様書等の整備及び各部門への周知に関すること。
 - (3) 接続機器の配置及び利用について決定すること。
 - (4) 総合運営システムを利用する者(以下「利用者」という。)に対し，安全な運用に関する研修を実施すること。(監視責任者)
 - 第6条** 監視責任者は，各部門の長をもって充て，次に掲げる職務を行う。
 - (1) 各部門システムの内容の変更に関し，運用責任者の承認を得ること。
 - (2) 各部門システムに問題が生じた場合，運用責任者に報告すること。
 - (3) 各部門システムへのコンピュータウイルス及び不正アクセスの対策を講じること。(接続機器管理責任者)
 - 第7条** 接続機器管理責任者は，システム管理責任者の指名する者をもって充て，次に掲げる職務を行う。
 - (1) 接続機器の内容の変更に関し，運用責任者の承認を得ること。
 - (2) 接続機器に問題が生じた場合，運用責任者に報告すること。
 - (3) 接続機器へのコンピュータウイルス及び不正アクセスの対策を講じること。(総合運営システムの監査)
 - 第8条** 総合運営システムの運用，管理等の状況についての監査を実施するため，監査責任者を置き，システム管理責任者が指名する者をもって充てる。
 - 2 監査責任者は，システム管理責任者の承認を得て，監査担当者を選任する。
 - 3 監査責任者は，監査実施前に監査計画を立案し，システム管理責任者の承認を得るものとする。
 - 4 監査責任者及び監査担当者は，監査の結果に問題がある場合は，その改善策を提案するように努めるものとする。
 - 5 監査は，年1回定期的を実施する。ただし，システム管理責任者が必要と認めた場合は，随時の監査を実施することができる。(利用停止)
 - 第9条** システム管理責任者は，前条第5項の監査の結果，総合運営システムの運用，管理等に問題がある場合又はこの規程に違反する事実がある場合，総合運営システムを利用停止とする。
 - 2 利用停止の期間等は，委員会の審議を経て，システム管理責任者が決定する。(利用者)
 - 第10条** 利用者は，次に掲げる者のうち，システム管理責任者が利用を許可した者とする。
 - (1) 病院事業の職員で医療業務に従事する者
 - (2) 研修登録医
 - (3) 診療従事者の許可を得た者
 - (4) 研究員及び研究生
 - (5) 前各号に掲げる者のほか，システム管理責任者が特に必要と認めた者(利用制限)
 - 第11条** システム管理責任者は，利用者の職種により，総合運営システムの利用範囲に制限を課すことができる。(利用申請等)
 - 第12条** 利用者は，利用者認証に関する ID 及びパスワード(以下「ID 等」という。)を取得するために，大崎市病院事業総合運営システム利用申請書(別記様式)により利用申請を行わなければならない。
 - 2 システム管理責任者は，前項の申請について許可したときは，ID 等を交付するものとする。
 - 3 利用者は，交付された ID 等を厳重な注意をもって管理しなければならない。
 - 4 利用者が ID 等の適切な管理を行わないために生じた事故や障害については，当該利用者が責任を負う。
 - 5 利用者が総合運営システムの利用資格を失った場合又は利用の必要がなくなった場合若しくは利用状況に変更があった場合には，運用責任者及び監視責任者に速やかに報告しなければならない。(利用者の責務)
 - 第13条** 利用者は，総合運営システムの動作の異常及び安全性の問題点を発見したときは，直ちに運用責任者に報告しなければならない。
 - 2 利用者は，運用責任者が実施する安全な運用に関する研修を受けなければならない。
 - 3 利用者は，大崎市病院事業個人情報保護条例施行規程(平成18年大崎市病院管理規程第8号)を遵守し，患者の個人情報保護しなければならない。(電子媒体による保存)
 - 第14条** 保存義務のある情報の電子媒体による保存については，当該保存義務のある情報の真正性，見読性及び保存性を確保しなければならない。(雑則)
 - 第15条** この規程に定めるもののほか，総合運営システムの運用管理に必要な事項は，委員会の審議を経て，システム管理責任者が定める。
- 附 則 (抜粋)
- (施行期日) この管理規程は，令和4年4月1日から施行する。

○ 電子カルテシステム等，医療情報システムに関する問い合わせ窓口

臨床支援センター臨床支援室システム担当 **TEL0229-23-3311(代)**（電話交換手に「臨床支援室システム担当へ」とお伝えください）

医療情報システム安全管理責任者（システム管理責任者） 大崎市民病院院長 今泉 秀樹