藤枝市立総合病院

情報セキュリティポリシー

令和８年４月１日

初版

藤枝市立総合病院　医療情報分析室

－ 目 次 －

第 1 章 情報セキュリティ基本方針

第 2 章 情報セキュリティ対策基準

第1章 情報セキュリティ基本方針

1. 目的

本基本方針は、藤枝市立総合病院（以下「当院」という。）が保有し取り扱う医療情報系の情報資産について、その機密性、完全性及び可用性を維持するため、当院が実施する情報セキュリティ対策に関する基本的な事項を定めることを目的とする。

また、本基本方針は、診療業務の継続性の確保及び経営リスクの低減を図り、患者及び関係者の信頼並びに他の医療機関等との安全かつ適正な情報共有を確保することを目的とする。

2. 定義

本基本方針において使用する用語の定義は、次のとおりとする。

（1）ネットワーク

医療情報システム等において、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

電子カルテシステム、部門システムその他医療情報を取り扱うために、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る情報処理の仕組みをいう。

（3）情報セキュリティ

医療情報系の情報資産について、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

医療情報等について、正当な権限を有する者のみがアクセスできる状態を確保することをいう。

（6）完全性

医療情報等が破壊、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

医療情報等について、正当な権限を有する者が、必要なときに中断されることなく利用できる状態を確保することをいう。

（8）医療情報系

診療録、検査結果、画像データ等の診療情報、医事会計情報、及びこれらを取り扱う情報システム並びにネットワークをいう。

3. 対象とする脅威

医療情報系の情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリテ

ィ対策を実施する。

（1）不正アクセス、不正プログラム等によるウイルス攻撃、サービス不能攻撃等のサイバー攻撃、又は内部不正等の意図的要因による医療情報の漏えい、破壊、改ざん、消去及び診療業務の妨害

（2）医療情報の無断持ち出し、規程違反、設計又は設定の不備、操作ミス、保守・運用の不備、委託管理の不備、医療機器又は情報機器の故障等の非意図的要因による情報セキュリティ事故

（3）地震、火災、風水害等の災害による情報システムの停止又は診療業務の継続困難

（4）大規模又は広範囲にわたる感染症等による要員不足に伴う情報システム運用体制の機能不全

（5）電力、通信等の重要インフラの障害による情報システム及び診療業務への影響

4. 適用範囲

（1）組織の範囲

本基本方針は、当院の医療情報系の情報資産を取り扱う全部門に適用する。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、当院が保有し取り扱う次に掲げる医療情報系の情報資産とする。その他の情報資産については、設置者が定める情報セキュリティポリシーを適用するものとする。

①医療情報系の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医療情報系の情報システムで取り扱う医療情報及び関連情報（紙媒体を含む。）

③医療情報系の情報システムに関する仕様書、ネットワーク構成図等の関連文書

5. 職員等の遵守義務

当院の職員、非常勤職員（会計年度任用職員及び特別職非常勤職員等）、臨時職員及び委託事業者の従業員等（以下「職員等」という。）は、医療情報の重要性を十分に認識し、業務の遂行に当たっては、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、その他関連する内部規程等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の脅威から医療情報系の情報資産を保護するため、次に掲げる情報セキュリティ対策を講じる。

（1）組織体制

当院における医療情報系の情報資産について、情報セキュリティ対策を推進するための組織体制を確立する。

（2）情報資産の分類と管理

当院の保有する医療情報系の情報資産を、機密性、完全性及び可用性の観点から分類し、当該分類に応じた情報セキュリティ対策を実施する。また、医療情報系の情報資産のうち、サーバ、端末、ネットワーク機器等の情報機器については、適切な管理を行うため、台帳を整備し、当該台帳に基づき管理する。

（3）情報システム全体の安全性及び可用性の確保

医療情報系の情報システムについては、診療業務の継続性に十分配慮しつつ、不正アクセス対策、認証・アクセス制御、ネットワーク分離等の多層的な対策を講じる。

（4）物理的セキュリティ

サーバ室、診療情報管理室、医療情報を取り扱う端末、医療機器及びネットワーク機器について、十分な物理的セキュリティ対策を講じる。

（5）人的セキュリティ

職員等が遵守すべき事項を明確にするとともに、医療情報の取扱いに関する教育及び啓発を継続的に実施する。

（6）技術的セキュリティ

利用者認証、アクセス制御、ログ管理、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

医療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、業務委託時の安全管理措置等、運用面での対策を講じるとともに、医療情報に係る情報セキュリティ事故が発生した場合に迅速かつ適切に対応するための体制及び計画を整備する。

（8）業務委託及び外部サービス（クラウドサービス）の利用

医療情報の取扱いを伴う業務を委託する場合には、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、医療情報系の情報システム又はこれに接続される機器について、リモートメンテナンス（保守）の有無及び対象機器等の状況を把握する。

医療情報を取り扱う外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

（9）評価・見直し

情報セキュリティ対策の実施状況について、定期的又は必要に応じて評価を行い、継続的な改善を図る。

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並びに医療情報を取り巻く環境の変化を踏まえ、医療情報系の情報資産に係るリスクを分析した上で、必要に応じて情報セキュリティポリシーの見直しを行う。

9. 情報セキュリティ対策基準の策定

本章に定める情報セキュリティ対策を実施するため、具体的な遵守事項及び判断基準等を定めた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、医療情報系の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。

なお、情報セキュリティ実施手順は、公にすることにより当院の診療業務及び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。

第2章 情報セキュリティ対策基準

本対策基準は、藤枝市立総合病院（以下「当院」という。）において情報セキュリティ基本方針を実行に移すため、当院が保有し取り扱う医療情報系の情報資産に関する情報セキュリティ対策の基準を定めるものである。

1. 組織体制

（１）最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

①病院事業管理者を CISO とする。CISO は、当院における全てのネットワーク、情報システム、医療情報系の情報資産の管理並びに情報セキュリティ対策に関する最終的な決定権限及び責任を有する。

②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する者を助言者として置くことができる。

③CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、その役割を明確化する。

④CISO は、本対策基準に定められた自らの担務の一部を、本対策基準に定める責任者に担わせることができる。

（２）最高情報セキュリティ副責任者（以下、「副 CISO」という）

①院長を最高情報セキュリティ副責任者（副 CISO）とする。

②副 CISO は、CISO を補佐し、CISO 不在時にはその職務を代行する。

（３）統括情報セキュリティ責任者

①医療情報担当部長を、CISO 直属の統括情報セキュリティ責任者とする。

②統括情報セキュリティ責任者は、CISO 及び副 CISO を補佐し、当院全体の情報セキュリティ対策を統括する権限及び責任を有する。

③当院のネットワーク及び情報システムにおける開発、設定変更、運用、見直し等について統括的な権限及び責任を有する。

④情報セキュリティ責任者、統括情報セキュリティ管理者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対し、情報セキュリティに関する指導及び助言を行う。また、必要に応じて医療情報担当の副院長と情報共有を行う。

⑤情報セキュリティ侵害が発生又はそのおそれがある場合には、CISO 又は副 CISO の指示に従い、また両者不在時には自らの判断又は医療情報担当の副院長と相談の上、

必要な措置を実施する。

⑥情報セキュリティ実施手順の維持・管理を行う。

⑦緊急時の円滑な情報共有のため、関係者を網羅した緊急連絡体制を整備する。

⑧緊急時には速やかに CISO に報告し、回復のための対策を講じる。

⑨情報セキュリティ関係規程の運用状況を把握し、必要に応じて CISO に報告する。

（4）情報セキュリティ責任者

①各センター長及び各部長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、所管部門における情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、所管する情報システムにおける開発、設定の変更、維持・管理、及び見直し等に関する統括的な権限及び責任を有する。

④情報セキュリティ責任者は、所管部門における緊急時等の連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに当院の職員、非常勤職員（会計年度任用職員及び特別職非常勤職員等）、臨時職員及び委託事業者の従業員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

（5）統括情報セキュリティ管理者

①医療情報の管理等を担当する課（室）の長を統括情報セキュリティ管理者とする。

②統括情報セキュリティ管理者は、統括情報セキュリティ責任者を補佐する。

③統括情報セキュリティ管理者は、当院の共通的なネットワーク及び情報システムにおける運用・保守を行う権限及び責任を有する。

④統括情報セキュリティ管理者は、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ管理者は、情報セキュリティ対策の実施及び推進に関する事務を行う。

⑥統括情報セキュリティ管理者は、緊急時には速やかに統括情報セキュリティ責任者に報告するとともに、関係部門と連携し、その状況の確認及び評価を行い、被害の拡大防止及び回復のための必要な措置を講じなければならない。

（6）情報セキュリティ管理者

①各課科室長及び各看護師長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、所管部署における情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、情報セキュリティインシデントが発生又はそのおそれがある場合には、速やかに情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

（7）情報システム管理者

①各情報システムを所管する課科室長を、当該情報システムの情報システム管理者とする。

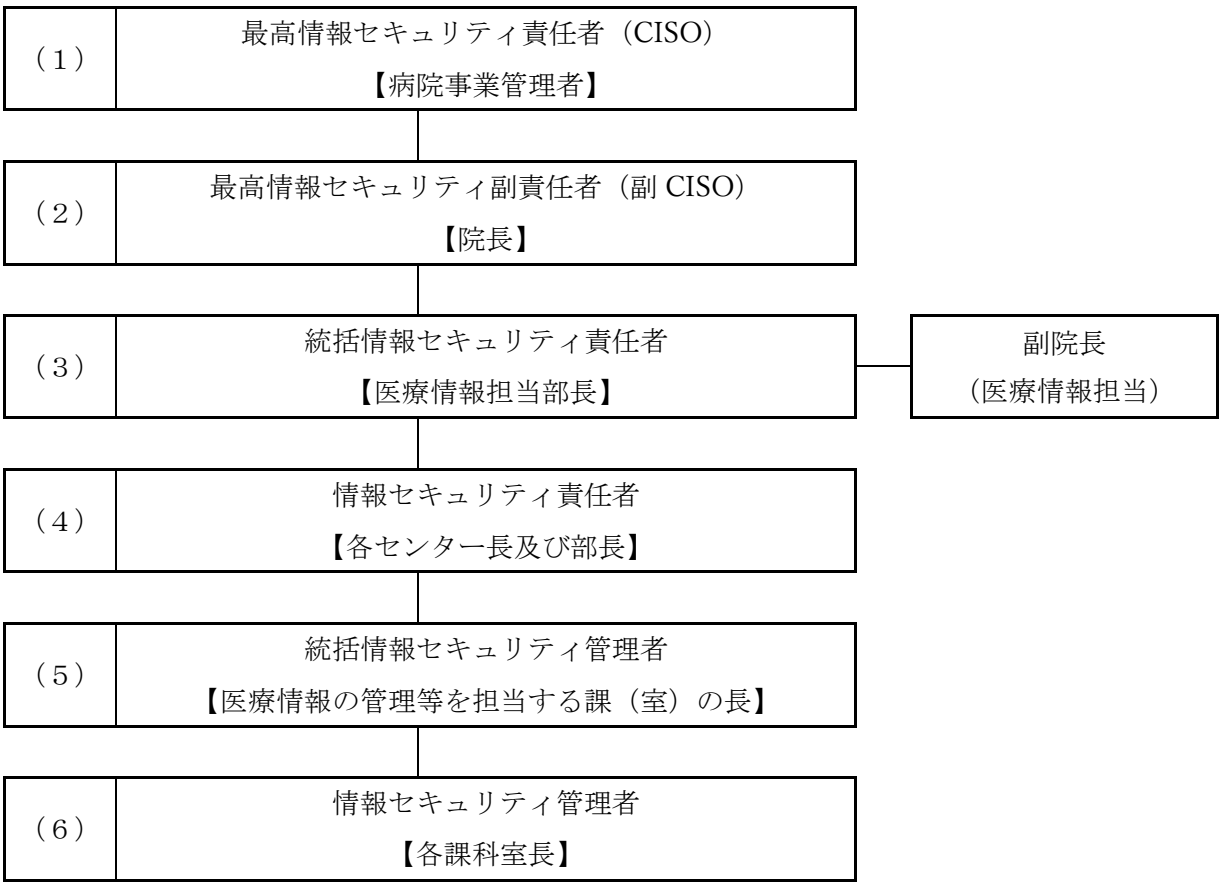
②情報システム管理者は、所管する情報システムの開発、設定変更、運用・保守、維持・管理、見直し等を行う権限及び責任を有する。

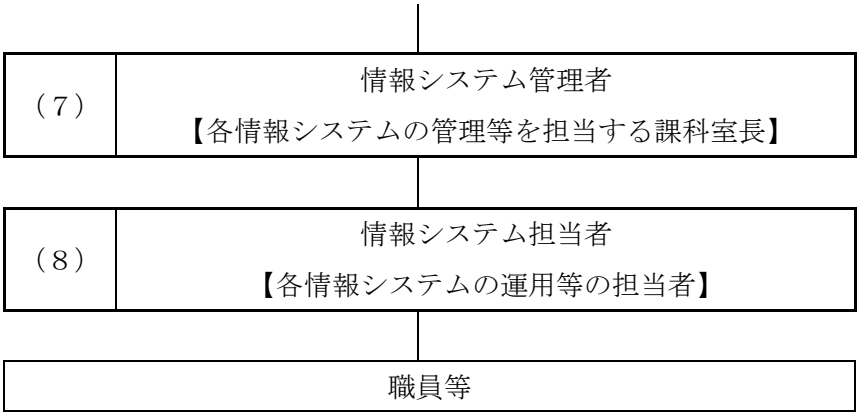
③情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（8）情報システム担当者

情報システム管理者の指示に従い、情報システムの開発、設定変更、運用、更新等の作業を行う者を情報システム担当者とする。

【組織体制図】





（9）兼務の禁止（職務分離）

①情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者と、その承認者又は許可者は同じ者が兼務してはならない。

②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者と、その監査を実施する者は、同じ者が兼務してはならない。

（１０）CSIRT の設置及び役割

①CISO は、情報セキュリティインシデントへの迅速かつ的確な対応を行うため、CSIRT を整備し、その役割を明確化しなければならない。

②CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部機関との連携を行う職員等を定めなければならない。

③CISO は、CSIRT に情報セキュリティに関する院内の統一的な窓口を整備し、各部門等から報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④CISO は、情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部門等に提供しなければならない。

⑤CSIRT は、情報セキュリティインシデントを認知した場合には、その内容及び影響の程度に応じて、CISO へ報告するとともに、法令、ガイドライン等に基づき必要な関係機関への報告を行わなければならない。

⑥CSIRT は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知又は公表対応を行わなければならない。

⑦CSIRT は、情報セキュリティに関して、関係機関（IPA、警察、関係行政機関等）、他の医療機関又は委託事業者等と必要な情報共有を行わなければならない。

2. 情報資産の分類と管理

（1）情報資産の分類

当院において取り扱う医療情報系の情報資産は、機密性、完全性及び可用性の観点から次のとおり分類し、必要に応じて取扱制限を行うものとする。

【機密性による分類】

分類	分類基準	取扱制限
病院機密性 3	診療情報、患者基本情報等の要配慮個人情報を含み、漏えいした場合に患者の権利利益に重大な影響を及ぼす情報資産	・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・電磁的記録媒体の施錠可能な場所への保管
病院機密性 2	医事会計情報等、漏えいした場合、一定の不利益や混乱が生じるが、直ちに公表を前提としない情報資産	
病院機密性 1	上記以外の情報資産	―

【完全性による分類】

分類	分類基準	取扱制限
病院完全性 2	診療情報、患者基本情報及び医事会計情報等、改ざん又は誤りにより診療の安全性又は業務の適正な遂行に重大な影響を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
病院完全性 1	上記以外の情報資産	―

【可用性による分類】

分類	分類基準	取扱制限
病院可用性２	診療情報、患者基本情報及び医事会計情報等、利用不能となった場合に診療の継続又は患者の生命・身体に影響を及ぼすおそれがある情報資産	・バックアップ、指定時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
病院可用性１	上記以外の情報資産	－

（２）情報資産の管理

①管理責任

（ア）情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ）情報システム管理者は、所管する情報システムについて、当該システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

（ウ）情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製された情報資産についても（１）に定める分類に基づき管理しなければならない。

（エ）情報セキュリティ管理者は、医療情報系の情報資産のうち、サーバ、端末、ネットワーク機器等の情報機器については、所在及び管理責任者等を明確にするため、台帳により管理しなければならない。

②情報資産の分類の表示

職員等は、病院機密性２以上の情報資産について、ファイル（ファイル名、ファイル属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の機密性分類を表示し、必要に応じて取扱制限についても明示するなど、適正な管理を行わなければならない。

③情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要となった情報については、速やかに消去しなければならない。

④情報資産の入手

（ア）院内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取り扱いをしなければならない。

（イ）院外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報

資産の分類及び取扱制限を定めなければならない。

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用

（ア）情報資産を利用する者は、業務目的以外に情報資産を利用してはならない。

（イ）情報資産を利用する者は、当該情報資産の分類に応じ、適正な方法で取り扱わなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（エ）情報資産を外部機関と共有し、又は外部機関との情報連携に利用する場合においても、当該情報資産の分類に応じた適切安全管理措置を講じなければならない。

⑥情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に応じて、情報資産を適正に保管しなければならない。

（イ）情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合には、書込み禁止等の措置を講じなければならない。

（ウ）情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体又はバックアップデータを記録した媒体を長期保管する場合には、より自然災害の影響を受けにくい又は安全性が確保された場所に保管するよう努めなければならない。

（エ）病院機密性 2 以上、病院完全性 2 又は病院可用性 2 の情報を記録した電磁的記録媒体は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により病院機密性 2 以上の情報を送信する者は、暗号化、パスワード通知の分離等の措置を講じなければならない。

⑧情報資産の運搬

車両等により病院機密性 2 以上の情報資産を運搬する場合には、必要に応じて鍵付きのケース等に収納する、暗号化を行う等、情報資産の不正利用又は紛失を防止するための措置を講じなければならない。

⑨情報資産の提供・公表

（ア）病院機密性 2 以上の情報資産を外部に提供する場合には、必要に応じて暗号化等の措置を講じなければならない。

（イ）病院機密性 2 以上の情報資産を外部に提供する場合には、あらかじめ情報セキ

ュリティ管理者の承認を得なければならない。

（ウ）患者又は一般に公開する情報資産については、その完全性が確保されるよう、改ざん防止等の措置を講じなければならない。

⑩情報資産の廃棄等

（ア）情報資産の廃棄又は機器のリース返却等を行う場合には、情報を記録している電磁的記録媒体について、その情報の機密性に応じて、復元不可能な方法により情報を消去又は破壊しなければならない。

（イ）情報資産の廃棄又は返却に際して実施した処理については、日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄又はリース返却等を行う場合には、あらかじめ情報セキュリティ管理者の承認を得なければならない。

3. 情報システム全体の強靭性の向上

（１）情報システムの分離とアクセス制御

電子カルテシステム等の中核的な医療情報系の情報システムについては、インターネット接続系等の他の領域と適切に分離し、多要素認証、端末制御等により不正アクセス及び情報の持ち出しの防止に努めなければならない。

（２）ネットワークの分離と安全な通信

医療情報系のネットワークとその他のネットワークとの間は、通信制御及び無害化等の措置を講じ、必要最小限の通信のみを許可するものとする。

（３）診療継続性の確保

医療情報系の情報システムの停止が診療に重大な影響を及ぼすことを踏まえ、監視機能の強化、バックアップ、冗長化、災害対策等を講じ、情報セキュリティインシデントの早期発見と必要な時間内に復旧可能な体制を確保しなければならない。

4. 物理的セキュリティ

4.1. サーバ等の管理

（１）機器の取付け

情報システム管理者は、サーバ等の機器を設置する場合、火災、水害、埃、振動、温度及び湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（２）サーバの冗長化

①情報システム管理者は、診療業務等における重要な情報を格納するサーバについて、必要に応じ冗長化を行い、可用性の確保に努めなければならない。

②情報システム管理者は、主系サーバに障害が発生した場合に、速やかに副系サーバへ

切り替えられるよう、運用手順を定めなければならない。

（３）機器の電源

①情報システム管理者は、統括情報セキュリティ管理者及び施設管理部門と連携し、停電等に備え、サーバ等の機器が安全に停止又は継続稼働できるよう、必要な容量の予備電源を確保しなければならない。

②情報システム管理者は、統括情報セキュリティ管理者及び施設管理部門と連携し、落雷等による過電流から機器を保護するための措置を講じなければならない。

（４）通信ケーブル等の配線

①統括情報セキュリティ管理者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷防止のため、必要な配線管理措置を講じなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、主要な通信ケーブル等に異常が認められた場合は、速やかに施設管理部門およびネットワーク保守事業者と連携して対応しなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク接続口は、第三者が容易に接続できないよう適切に管理しなければならない。

④統括情報セキュリティ管理者及び情報システム管理者は、配線の変更又は追加は、許可された者以外が行えないよう必要な措置を講じなければならない。

（５）機器の定期保守及び修理

①情報システム管理者は、重要なサーバ等の機器について定期保守を実施しなければならない。

②情報システム管理者は、電磁的記憶媒体を内蔵する機器を事業者に修理させる場合は、可能な限り内容を消去した上で行わせ、消去できない場合は守秘義務の確保等必要な措置を講じなければならない。

（６）院外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、院外（委託事業者のデータセンター等）にサーバ等の機器を設置する場合は、CISO の承認を得た上で、定期的に情報セキュリティ対策状況を確認しなければならない。

（７）機器の廃棄等

情報システム管理者は、機器を廃棄又はリース返却等する場合は、機器の内部記憶装置から全ての情報を消去し、復元不可能な状態にする措置を講じなければならない。

4.2. 管理区域（情報システム室等）の管理

（１）管理区域の構造等

①管理区域とは、基幹ネットワーク機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。」や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ管理者及び情報システム管理者は、管理区域への出入口は必要最小限とし、施錠、監視等の措置により無許可の立入りを防止するよう努めなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、情報システム室内の機器に対して、耐震、防火、防水等の対策を講じなければならない。

④統括情報セキュリティ管理者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

①統括情報セキュリティ管理者及び情報システム管理者は、管理区域への入退室を許可された者に限定し、適切な入退室管理を行わなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、必要に応じて入室者に身分証明書等の提示を求め、その身分を確認するものとする。

③統括情報セキュリティ管理者及び情報システム管理者は、入室者の所属・氏名・入退室時刻、目的等の情報を台帳等で管理し、保管しなければならない。

④統括情報セキュリティ管理者及び情報システム管理者は、外部事業者等が入室する場合は、職員による許可を得るものとし、名札を着用するなど、外見上職員と区別できるよう措置を講じなければならない。

（３）機器等の搬入出

①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせなければならない。

②情報システム管理者は、機器の搬入出について職員を立ち会わせなければならない。

4.3. 通信回線及び通信回線装置の管理

①統括情報セキュリティ管理者は、院内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

②統括情報セキュリティ管理者は、院内の通信回線及び通信回線装置について、ネット

ワーク構成要件に基づき適切なセキュリティ対策を講じなければならない。

③統括情報セキュリティ管理者は、外部へのネットワーク接続を必要最小限とするよう努めなければならない。

④統括情報セキュリティ管理者は、情報システムに通信回線を接続する場合、必要に応じて暗号化、監視、冗長化等の措置を講じなければならない。

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

①情報セキュリティ管理者は、盗難又は紛失による情報漏えいを防止するため、業務で利用する端末について、固定又は施錠可能な保管場所での管理等、業務実態に応じた物理的措置を講じるよう努めなければならない。また、電磁的記録媒体に保存された情報については、保存の必要がなくなった時点で、速やかに消去又は復元不可能な方法により廃棄しなければならない。

②情報セキュリティ管理者は、情報システムへのログインに際して、ID 及びパスワードによる認証を適切に設定しなければならない。なお、電子カルテシステム等の機密性が高い情報資産を取り扱う情報システムについては、可能な限り IC カード、生体認証等を組み合わせた多要素認証の導入に努めなければならない。

③情報セキュリティ管理者は、端末の不正利用防止の観点から、必要に応じて端末起動時のパスワード（BIOS パスワード、ストレージのパスワード等）を設定することに努めなければならない。

④情報セキュリティ管理者は、パソコン、モバイル端末等に保存される情報について、端末の暗号化機能を有効に利用しなければならない。端末にセキュリティチップ等が搭載されている場合は、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用するよう努めなければならない。

5. 人的セキュリティ

5.1. 職員等の遵守事項

（1）職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー、関連する規程及び実施手順等を遵守しなければならない。また、情報セキュリティ対策について不明な点や、遵守することが困難な事項がある場合には、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセスを行ってはならない。

③モバイル端末及び電磁的記録媒体等の持ち出し並びに院外における情報処理作業の制限

（ア）CISO は、病院機密性 2 以上の情報資産を院外で取り扱う場合における安全管理措置を定めなければならない。

（イ）職員等は、当院が管理するモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを院外へ持ち出す場合には、事前に情報セキュリティ管理者の許可を得なければならない。

（ウ）職員等は、院外で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得るとともに、定められた安全管理措置を遵守しなければならない。

④管理対象外端末等の業務利用

（ア）職員等は、当院の管理対象外のパソコン、モバイル端末及び電磁的記録媒体等を、原則として業務に利用してはならない。ただし、業務上の必要性を踏まえ、統括情報セキュリティ責任者の許可を得た場合に限り、利用することができる。

（イ）職員等は、当院の管理対象外の端末等を用いて業務を行う際には安全管理措置に関する規程を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の院外への持ち出し及び院内への持ち込みについて、必要に応じて記録を作成し、適切に保管しなければならない。

⑥端末におけるセキュリティ設定変更の禁止

職員等は、業務用のパソコン及びモバイル端末等におけるセキュリティ機能に関する設定を、統括情報セキュリティ管理者又は情報セキュリティ管理者の許可なく変更してはならない。

⑦机上等における端末及び情報の管理

職員等は、業務用のパソコン、モバイル端末、電磁的記録媒体並びに情報が印刷された文書等について、第三者に不正に使用又は閲覧されることのないよう、離席時の端末のロック、文書等の適切な保管等、適正な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も、業務上知り得た情報を漏らしてはならない。

（2）非常勤職員及び臨時職員等への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤職員及び臨時職員等に対し、採用時に当該職員が遵守すべき情報セキュリティポリシー等の内容を理解させ、遵守させなければならない。

②遵守に関する同意

情報セキュリティ管理者は、必要に応じて、非常勤職員及び臨時職員等に対し、情報セキュリティポリシー等を遵守する旨の書類への署名を求めるものとする。

（3）情報セキュリティポリシー等の掲示

統括情報セキュリティ管理者は、職員等が情報セキュリティポリシー及び実施手順を常時確認できるよう、院内グループウェア等により掲示しなければならない。

（4）委託事業者に対する説明

情報セキュリティ管理者は、情報システムの開発、保守、運用等を委託する場合には、再委託事業者を含め、委託事業者が遵守すべき情報セキュリティポリシー等の内容及び機密保持に関する事項について説明しなければならない。

5.2. 研修・訓練

（1）情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（2）研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行う。

②研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

③統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

（3）緊急時対応訓練

CSIRT は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（4）研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

5.3. 情報セキュリティインシデントの報告

（1）院内での情報セキュリティインシデントの報告

①職員等による報告義務

職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②情報セキュリティ管理者による報告

報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ管理者、情報セキュリティ責任者に報告しなければならない。

③統括情報セキュリティ管理者による報告

報告を受けた統括情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に報告しなければならない。

④CISO への報告

統括情報セキュリティ責任者及び情報セキュリティ責任者は、当該情報セキュリティインシデントの内容に応じて、CISO に報告しなければならない。

（2）患者・外部からの情報セキュリティインシデントの報告

①外部からの通報の取扱い

職員等は、当院が管理する情報システム及びネットワーク等の情報資産に関する情報セキュリティインシデントについて、患者等外部から通報を受けた場合には、速やかに情報セキュリティ管理者に報告しなければならない。

②情報セキュリティ管理者による内部共有

情報セキュリティ管理者は、外部からの通報内容を確認の上、速やかに統括情報セキュリティ管理者、情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

③統括情報セキュリティ管理者による報告

報告を受けた統括情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に報告しなければならない。

④CISO 等への報告

統括情報セキュリティ管理者及び情報セキュリティ責任者は、当該情報セキュリティインシデントの内容に応じて、CISO に報告しなければならない。

（3）情報セキュリティインシデント原因の究明、記録及び再発防止

①初動対応及び評価

CSIRT（又はこれに相当する体制）は、報告された事案について、速やかに事実関係を確認し、情報セキュリティインシデントに該当するか否かの評価を行わなければならない。

②CISO への報告

CSIRT は、情報セキュリティインシデントであると評価した場合には、速やかに CISO に報告しなければならない。

③被害拡大防止及び復旧対応

CSIRT は、関係する情報セキュリティ責任者及び情報システム管理者に対し、被害拡大防止のための応急措置の実施及び情報システムの復旧に関する指示を行わなければならない。また、同様のインシデントが他の情報システムに影響を及ぼしている可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

④原因究明及び記録の保存

CSIRT は、当該情報セキュリティインシデントの原因を究明し、対応経過及び結果を記録として保存しなければならない。

⑤再発防止策の検討及び報告

CSIRT は、原因究明の結果を踏まえ、再発防止策を検討し、CISO に報告しなければならない。

⑥再発防止策の実施

CISO は、CSIRT からの報告内容を確認し、必要な再発防止策の実施を指示しなければならない。

5.4. ID 及びパスワード等の管理

（1）IC カード等の取扱い

①職員等の遵守事項

職員等は、自己に貸与された IC カード、職員証、トークン等（以下「IC カード等」という。）について、次の事項を遵守しなければならない。

（ア）認証に用いる IC カード等を、他の職員等と共有してはならない。

（イ）業務上必要のないときは、IC カード等をカードリーダ又は端末のスロット等から抜いておかなければならない。

（ウ）IC カード等を紛失又は破損した場合には、速やかに統括情報セキュリティ管理者及び情報システム管理者に報告し、指示に従わなければならない。

②利用停止等の措置

統括情報セキュリティ管理者及び情報システム管理者は、IC カード等の紛失、盗難等の報告を受けた場合には、当該 IC カード等による情報システムへのアクセスを速やかに停止しなければならない。

③IC カード等の回収・廃棄

統括情報セキュリティ管理者及び情報システム管理者は、IC カード等を更新又は廃止する場合には、旧カード等を回収し、破砕その他復元不可能な方法により廃棄し

なければならない。

（２）ID の取扱い

①個人 ID の取扱い

職員等は、原則として個人に付与された ID を使用しなければならず、自己の ID を他者に利用させてはならない。

②共用 ID の取扱い

職員等は、統括情報セキュリティ管理者又は情報セキュリティ管理者に許可された業務および利用者に限定して共用 ID を使用するものとし、許可範囲を超えての利用をしてはならない。

（３）パスワードの取扱い

①秘密保持

職員等は、自己の管理するパスワードを他者に知られないよう適切に管理し、パスワードの照会等には一切応じてはならない。

②パスワードの強度

パスワードは、十分な長さを有し、推測されにくい文字列（英大文字・小文字、数字等を組み合わせる）とし、適切に管理しなければならない。

③流出時の対応

パスワードが漏えいした又はそのおそれがある場合には、速やかに情報セキュリティ管理者に報告し、指示に従って変更しなければならない。

④使い回しの禁止

複数の情報システムを利用する職員等は、原則として同一のパスワードを複数のシステム間で使用してはならない。

⑤初期パスワードの変更

仮のパスワード（初期パスワードを含む。）は、最初のログイン時に変更しなければならない。

⑥記憶設定の禁止

サーバ、ネットワーク機器及び端末において、パスワード入力を省略する設定又は自動保存機能は、原則として利用してはならない。

⑦パスワードの共有禁止

職員等間でパスワードを共有してはならない。ただし、共用 ID に対するパスワードについてはこの限りではない。

6. 技術的セキュリティ

6.1 コンピュータ及びネットワークの管理

（1）バックアップの実施

①統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムの診療情報等や、運用状態を復元させるために必要なシステム設定情報及びマスタ情報等について、適切な方法でバックアップを取得しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、バックアップデータからの復旧が可能であることを、定期的に確認しなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、情報システムが停止した場合に備え、紙媒体による代替運用等の診療業務の継続計画及び手順を別途定めるものとする。

（2）システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。また、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

③統括情報セキュリティ管理者、情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、誤操作や不正を防止するため、慎重に作業を行い、必要に応じて相互に確認しなければならない。

（3）情報システム仕様書等の管理

統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（4）ログの取得等

①統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムについて、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間保管しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければ

ならない。

（５）障害記録

統括情報セキュリティ管理者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（６）医療機器等のセキュリティ管理

統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムに接続する医療機器等について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（７）システムの脆弱性対策

①統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システム又はこれに接続される機器（医療機器を含む。）について、製造業者又はサービス事業者から提供される最新のファームウェア又は更新プログラムを、診療業務への影響及び安全性に十分配慮した上で、適切に適用しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムについて、業務上必要のないソフトウェア及びサービスがバックグラウンドで動作しないよう管理するとともに、システムの安全性及び安定性を確保するための適切な措置を講じなければならない。

（８）無許可ソフトウェアの導入等の禁止

①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②職員等は、業務上の必要がある場合は、統括情報セキュリティ管理者及び情報システム管理者の許可を得なければならない。

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

（９）機器構成の変更の制限

①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ管理者及び情報システム管理者の許可を得なければならない。

（１０）業務外ネットワークへの接続の禁止

職員等は、業務用の端末を、有線・無線を問わず、その端末を接続して利用するよう定められたネットワークと異なるネットワークに接続してはならない。

（１１）ネットワーク及び通信の管理

統括情報セキュリティ管理者及び情報システム管理者は、医療情報系のネットワークについて、次に掲げる措置を講じなければならない。

①インターネット接続系等の他のネットワークから、論理的又は物理的に分離すること。

②業務上外部ネットワークとの接続が必要と認められる場合には、ファイアウォール、ルータ等の設定により、必要最小限の通信に制限すること。

③不正アクセス又は不正通信を防止するため、接続元制限等の通信経路の制御及び監視を行うこと。

④ベンダの遠隔保守等、院外からの接続については、事前に許可した接続手段に限定すること。

⑤無線 LAN を使用する場合は、解読困難な暗号化及び認証技術を適用すること。

⑥接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断すること。

⑦外部機関等とのネットワーク接続又は情報連携を行う場合は、必要な安全対策及びリスク評価を実施しなければならない。

6.2. アクセス制御

（１）アクセス制御等

①アクセス制御

統括情報セキュリティ管理者及び情報システム管理者は、所管するネットワーク、又は情報システムごとに、職種、役割及び業務内容に応じて、必要最小限のアクセス権限を付与しなければならない。

②利用者 ID の取扱い

（ア）統括情報セキュリティ管理者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、退職等に伴う利用者 ID の廃止等の取扱い等の方法を定め、適正に措置しなければならない。

（イ）職員等は、業務上 ID の必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ管理者又は情報システム管理者に通知しなければならない。

（ウ）統括情報セキュリティ管理者及び情報システム管理者は、利用されていない ID

が放置されないよう、定期的に点検しなければならない。

（エ）統括情報セキュリティ管理者及び情報システム管理者は、利用者 ID に対し不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③特権 ID 及び共用 ID の管理

（ア）統括情報セキュリティ管理者及び情報システム管理者は、管理者権限等の特権 ID を利用する者を必要最小限に限定して付与するものとし、当該 ID 及びパスワードの漏えいが発生しないよう厳重に管理しなければならない。

（イ）統括情報セキュリティ管理者及び情報システム管理者は、共用 ID の利用を診療現場において、迅速な対応が求められる等の業務上の理由により利用範囲及び利用者を必要最小限に限定して付与するものとし、範囲を超えた利用がされていないことを定期的に確認しなければならない。

（２）職員等による院外からのアクセス等の制限

①職員等が院外から医療情報系の情報システムへ接続する場合には、統括情報セキュリティ管理者又は情報システム管理者の許可に基づき、承認された方法に限定するものとする。

②統括情報セキュリティ管理者又は情報システム管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③統括情報セキュリティ管理者又は情報システム管理者は、院外からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ管理者又は情報システム管理者は、院外からのアクセスを認める場合、通信途上の情報漏えいを防ぐために暗号化等のセキュリティ対策の措置を講じなければならない。

⑤統括情報セキュリティ管理者又は情報システム管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、多要素による認証に加えて通信内容の暗号化等のセキュリティ対策の措置を講じなければならない。

（３）ログイン時の表示等

統括情報セキュリティ管理者及び情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（４）アクセス状況の確認

統括情報セキュリティ管理者及び情報システム管理者は、必要に応じてアクセスログ等をもとに不適切な利用がないか確認し、不審なアクセスを認知した場合には、速やかに必要な対応を行うものとする。

（５）認証情報の管理

①統括情報セキュリティ管理者又は情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。また、オペレーティングシステム又はアプリケーションが提供する認証情報保護機能（パスワードポリシー設定、アカウントロック、二要素認証等）が利用可能な場合は、これを有効に活用しなければならない。

②統括情報セキュリティ管理者又は情報システム管理者は、職員等に対してパスワードを発行する場合には、初期パスワード又は仮パスワードを発行し、初回ログイン後直ちに変更させなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、管理者権限等の特権 ID について、複数のシステム間で同一のパスワードを設定してはならない。また、システム出荷時の初期パスワードをそのまま使用してはならない。

④統括情報セキュリティ管理者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（６）特権による接続時間の制限

統括情報セキュリティ管理者又は情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

6.3. システム開発、導入及び保守

（１）機器等の調達に係る運用規程の整備

①統括情報セキュリティ管理者は、当院において使用する情報機器、医療情報系の情報システム及び関連ソフトウェア（以下「機器等」という。）の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルにおいて、不正な変更が加えられないような対策を講じなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、情報セキュリティの観点を踏まえ、機器等の納入時又は情報システムの受入時における確認・検査手続を整備しなければならない。

（２）機器等及び情報システムの調達

①統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システ

ムの開発、導入又は保守に係る調達に当たっては、調達仕様書に必要とする技術的な情報セキュリティ機能を明記しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、機器等の調達に当たり、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題がないことを確認しなければならない。

（3）情報システムの開発

①システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を明確にし、必要に応じて役割分担を整理しなければならない。

②システム開発における ID の管理

（ア）情報システム管理者は、システム開発に使用する ID を管理し、開発又は作業完了後は不要となった ID を速やかに削除又は無効化しなければならない。

（イ）情報システム管理者は、システム開発に関与する者のアクセス権限を業務上必要な範囲に限定しなければならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム開発に使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。

（イ）情報システム管理者は、承認されていないソフトウェアが確認された場合には、当該ソフトウェアをシステムから削除しなければならない。

④アプリケーション・コンテンツ開発時の対策

情報システム管理者は、ウェブアプリケーション等の開発において、既知の脆弱性への対策を考慮し、必要な情報セキュリティ対策を講じるよう努めなければならない。

（4）情報システムの導入

①開発環境と運用環境の分離及び移行手順

（ア）情報システム管理者は、可能な範囲で開発・テスト環境と運用環境を分離するよう努めるものとする。

（イ）情報システム管理者は、開発・テスト環境から運用環境への移行に当たっては、移行手順を事前に明確にしなければならない。

（ウ）情報システム管理者は、移行に際しては、医療情報の保存を確実に行い、診療業務への影響が最小限となるよう配慮しなければならない。

（エ）情報システム管理者は、導入するシステムやサービスの可用性が確保されてい

ることを確認した上で導入しなければならない。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既存システムと接続する前に十分な試験を実施しなければならない。

（イ）情報システム管理者は、運用テストにおいては、可能な限り擬似環境又は検証環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、個人情報又は機密性の高い実データを、テストデータに使用してはならない。

（エ）情報システム管理者は、開発したシステムの受入テストを行う場合には、開発した組織と導入した組織の双方で独立したテストを行わなければならない。

（オ）情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないようテスト計画を策定し、確実に検証が実施されるよう、委託事業者の監督を行わなければならない。

③受入時の確認

（ア）情報システム管理者は、機器等の納入時又は情報システムの受入時に、調達仕様書等で定めた要件が満たされていることを確認しなければならない。

（イ）情報システム管理者は、情報システムが開発事業者から運用保守事業者へ引き継がれる際には、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（５）基盤管理ソフトウェア導入時の対策

①情報システム管理者は、サーバ、ネットワーク機器等の基盤を管理又は制御するソフトウェアを導入する場合、必要に応じて保護措置を講じるよう努めるものとする。

②情報システム管理者は、当該ソフトウェアの特性を踏まえ、情報セキュリティ水準の維持及びインシデント発生時の対応に関する手順を整備するものとする。

（６）基盤管理ソフトウェア運用時の対策

①情報システム管理者は、基盤管理ソフトウェアの運用・保守に当たり、セキュリティの維持及びセキュリティインシデントの迅速な検知及び対応に配慮するよう努めるものとする。

②情報システム管理者は、利用を認めているソフトウェアについて、必要に応じて見直しを行わなければならない。

（７）資料等の整備・保管

①情報システム管理者は、システム開発・保守に関する資料及び関連文書を適正に整

備・保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適切な方法で管理しなければならない。

（８）入出力データの正確性の確保

①情報システム管理者は、入力データの妥当性を確保するためのチェック機能を組み込むよう情報システムを設計しなければならない。

②情報システム管理者は、ウェブアプリケーション等については、脆弱性への対応及び改ざん防止に配慮しなければならない。

③情報システム管理者は、出力データについては、処理結果が正確に反映されるよう配慮しなければならない。

（９）情報システムの変更管理

情報システム管理者は、情報システムの変更を行った場合、変更内容及び履歴を記録しなければならない。

（１０）開発・保守用ソフトウェアの更新

情報システム管理者は、開発・保守用ソフトウェアの更新又はパッチ適用に当たり、他情報システムへの影響を確認しなければならない。

（１１）システム更新又は統合時の検証

情報システム管理者は、システム更新又は統合時には、移行に伴うリスク及び業務への影響を考慮し、必要な検証を行わなければならない。

（１２）対策の見直し

情報システム管理者は、運用状況等を踏まえ、情報システムの情報セキュリティ対策を適切に見直し、その結果を統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

6.4. 不正プログラム対策

（１）統括情報セキュリティ管理者及び情報システム管理者の措置事項

統括情報セキュリティ管理者及び情報システム管理者は、コンピュータウイルス等の不正プログラム対策として、次の事項を措置しなければならない。

①院外から受信または提供を受けたファイル等については、当院のネットワーク境界等において、不正プログラムの検査を行い、不正プログラムの院内システムへの侵入

防止に努めなければならない。

②院外へ送信または提供するファイル等についても、必要に応じて不正プログラムの検査を行い、不正プログラムの外部への拡散防止に努めなければならない。

③不正プログラムに関する脅威情報、注意喚起情報等を収集し、必要に応じて職員等へ周知しなければならない。

④当院が管理する医療情報系の情報システムのサーバ及びパソコン等の端末に対し、不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェア自体及びパターンファイルは、常に最新の状態を維持するよう努めなければならない。

⑥業務で利用するソフトウェアについては、原則として開発元によるセキュリティサポートが終了したものを使用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

⑦当院が管理する医療情報系の情報システムのパソコン等の端末については、職員等が USB メモリ等の外部記録媒体を自由に利用し、又は不要なプログラムのインストール若しくはシステム設定の変更等を行うことができないよう、システム的な制限を実施するなど、適切な措置を講じなければならない。

⑧不正プログラム対策ソフトウェア等の設定変更権限は適切に管理し、情報システム管理者が許可した者以外に付与してはならない。

（2）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①当院が導入した不正プログラム対策ソフトウェアの設定を、許可なく変更してはならない。

②診療情報提供書に添付された記録媒体等、外部から取得したファイルを業務に使用する場合は、事前に不正プログラムの検査を行わなければならない。

③医療情報系の情報システムに対してファイル等の入出力を行う場合には、当院が指定する USB メモリ及び入出力専用の端末を利用しなければならない。また、その内容を管理台帳に記録しなければならない。

④コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、定められた初動対応手順に従い、該当端末の LAN ケーブルの抜去等、速やかに対応しなければならない。

⑤その他、診療情報の取扱いに関する運用については、関連する院内規程を遵守しなければならない。

（3）専門家の支援体制

統括情報セキュリティ管理者は、院内の対応のみでは不十分な事態に備え、情報システム保守事業者及びネットワーク保守事業者等、専門家の支援を受けられる体制の確保に努めなければならない。

6.5. 不正アクセス対策

（1）統括情報セキュリティ管理者の措置事項

統括情報セキュリティ管理者は、不正アクセス対策として、次の事項を措置しなければならない。

①サーバ、ネットワーク機器等について、使用されていない通信ポートや不要な通信経路の閉鎖。

②不要なサービスについて、機能の削除又は停止。

③不正アクセス発生時の連絡体制、対応窓口及び外部連絡先等の明確化、並びに適正な対応などを実施できる体制の整備。

（2）攻撃への対処

CISO 及び統括情報セキュリティ責任者は、不正アクセスを受けた場合又はそのおそれがある場合には、診療への影響を考慮しつつ、必要に応じてシステム停止等の措置を講じなければならない。また、関連するシステム保守事業者、厚生労働省および都道府県の担当部門と連絡を密にして情報の収集に努めなければならない。

（3）記録の保存

CISO 及び統括情報セキュリティ責任者は、不正アクセスが犯罪に該当する可能性がある場合には、通信ログ等の記録を適切に保存し、警察および関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃への対策

統括情報セキュリティ管理者及び情報システム管理者は、職員等又は委託事業者による不正な通信や操作について、必要に応じてログ等による監視・確認を行わなければならない。

（5）職員等による不正アクセスへの対応

統括情報セキュリティ管理者及び情報システム管理者は、職員等による不正アクセスが確認された場合には、当該職員等が所属する情報セキュリティ管理者と連携し、適正な対応を行わなければならない。

（6）サービス不能攻撃（DoS／DDoS）対策

統括情報セキュリティ管理者及び情報システム管理者は、外部からアクセスできる情報システムを運用している場合、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7）標的型攻撃対策

統括情報セキュリティ管理者及び情報システム管理者は、標的型攻撃による侵入を防止するため、職員への教育・注意喚起等の人的対策を講じるとともに、侵入の検知及び被害拡大防止のための技術的対策を講じなければならない。

6.6. セキュリティ情報の収集

（1）脆弱性（セキュリティホール）に関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムおよび関連機器等に関する脆弱性（セキュリティホール）の情報を継続的に収集し、必要に応じ、関係者間で共有しなければならない。また、診療業務への影響を考慮しつつ、当該セキュリティホールの緊急度に応じて、ソフトウェアの更新等の対策を講じなければならない。

（2）不正プログラム等に関するセキュリティ情報の収集・周知

統括情報セキュリティ管理者は、不正プログラム等に関するセキュリティ情報を収集し、必要に応じ対応方法について職員等に周知しなければならない。

（3）情報セキュリティ全般に関する情報の収集及び共有

統括情報セキュリティ管理者及び情報システム管理者は、情報セキュリティに関する法令・ガイドラインの改正、医療機関における事故・インシデント事例、技術動向等の情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境又は技術環境の変化により、新たな脅威が想定される場合には、セキュリティ侵害を未然に防止するための対策を速やかに検討し講じなければならない。

7. 運用

7.1. 情報システムの監視

（1）情報システムの運用・保守時の対策

①統括情報セキュリティ管理者及び情報システム管理者は、医療情報系の情報システムの運用・保守において、監視機能を含む情報セキュリティ機能を適切に運用しなけ

ればならない。

②統括情報セキュリティ管理者及び情報システム管理者は、新たな脅威の出現、運用状況、インシデント発生状況等を踏まえ、情報セキュリティ対策の見直しを適時検討し、必要な措置を講じなければならない。

③重要な医療情報（病院機密性 2 以上）を取り扱う情報システムについては、障害や侵害発生時に診療への影響を最小限とできるよう、危機的事象を想定した運用を行わなければならない。

（2）情報システムの監視機能

①統括情報セキュリティ管理者及び情報システム管理者は、情報システムの監視に関する運用管理機能要件を定め、可能な範囲で監視機能を実装するよう努めなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、情報システムの運用において、実装された監視機能を適切に運用しなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、新たな脅威や運用状況の変化を踏まえ、監視対象及び監視手法について定期的に見直さなければならない。

④統括情報セキュリティ管理者及び情報システム管理者は、サーバ装置等における情報セキュリティインシデントを検知するため、当該装置を監視するための措置を講じるよう努めなければならない。

（3）情報システムの監視

①統括情報セキュリティ管理者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時又は定期的に監視しなければならない。

②統括情報セキュリティ管理者及び情報システム管理者は、重要なログを取得するサーバについては、正確な時刻設定及びサーバ間の時刻同期が確保される措置を講じなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、クラウドサービス等、外部と常時接続するシステムについては、通信状況及び利用状況を適切に把握しなければならない。

7.2. 情報セキュリティポリシーの遵守状況の確認

（1）遵守状況の確認及び対処

①統括情報セキュリティ管理者及び情報システム管理者は、情報セキュリティポリシーの遵守状況を確認し、問題を認めた場合には速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。

②CISO 及び統括情報セキュリティ責任者は、報告された問題について、適正かつ速や

かに対処しなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク及びサーバ等の設定について、定期的にポリシー遵守状況を確認し、適正かつ速やかに対処しなければならない。

（２）端末・媒体等の利用状況調査

CISO 又は CISO が指名した者は、不正アクセス、不正プログラム等の調査を目的として、職員等が使用するパソコン等端末及び電磁的記録媒体等のログ等により、利用状況を調査することができる。

（３）職員等の報告義務

①職員等は、情報セキュリティポリシーに対する違反又はそのおそれを発見した場合、速やかに情報セキュリティ管理者又は統括情報セキュリティ管理者に報告しなければならない。

②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ管理者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

7.3. 侵害時の対応等

（１）緊急時対応計画の策定

CISO は、情報セキュリティインシデント等が発生した場合又は発生のおそれがある場合に備え、連絡、証拠保全、被害拡大防止、復旧、再発防止等を定めた緊急時対応計画を策定し、有事の際には当該計画に従って適正に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の事項を含めなければならない。

①関係者の連絡体制

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（３）業務継続計画との整合性

統括情報セキュリティ管理者は、自然災害、感染症流行等の事案を想定し事象発生時においても診療及び重要業務を継続又は早期復旧することを目的として業務継続計画と、情報セキュリティ対策との整合性を確保しなければならない。

（４）緊急時対応計画の見直し

統括情報セキュリティ管理者は、緊急時対応計画は、状況の変化等を踏まえ、必要に応じて見直しを行わなければならない。

7.4. 例外措置

（１）例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、診療業務の継続等のため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて、CISO の許可を得て例外措置を講じることができる。

（２）緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、診療業務の遂行に緊急を要する場合であって、例外措置の実施が不可避のときは、事後速やかに CISO に報告しなければならない。

（３）例外措置の管理

CISO は、例外措置の申請及び承認状況を適切に管理し、定期的に確認しなければならない。

7.5. 法令等の遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令及び内部規程を遵守し、これに従わなければならない。

①医療法（昭和 23 年法律第 205 号）
②地方公務員法(昭和 25 年法律第 261 号)
③著作権法（昭和 45 年法律第 48 号）
④不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
⑤個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑥行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
⑦サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑧藤枝市個人情報保護法施行条例（令和 4 年条例第 30 号）

7.6. 懲戒処分等

（１）懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督者は、その内容及び影響に応じて、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①統括情報セキュリティ管理者が違反を確認した場合は、当該職員等が所属する情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

②情報セキュリティ管理者の指導によっても改善が認められない場合は、統括情報セキュリティ管理者は、当該職員等の情報システム利用を制限又は停止することができる。その措置内容については、その後速やかに CISO 及び関係者へ報告しなければならない。

8. 業務委託と外部サービス（クラウドサービス）の利用

8.1. 業務委託

（１）業務委託に係る運用規程の整備

統括情報セキュリティ責任者は、当院における業務委託に関し、以下の内容を全て含む運用規程を整備しなければならない。

①委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

②委託事業者の選定基準

（２）業務委託実施前の対策

①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結

重要な情報資産を取り扱う業務を委託する場合には、必要に応じて以下の事項を契約に明記しなければならない。

・情報セキュリティポリシー及び関連手順の遵守

・個人情報及び診療情報の漏えい防止のための技術的・組織的安全管理措置

・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

・提供されるサービスレベルの保証

・アクセスを許可する情報の種類・範囲、アクセス方法の明確化など、情報のラ

イフサイクル全般での管理方法
・委託事業者従業員に対する情報セキュリティ教育の実施
・提供情報の目的外利用及び第三者提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返却、廃棄等
・委託業務の定期報告及び緊急時報告義務
・病院による監査又は報告要求
・病院による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の措置（損害賠償等）

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

②情報セキュリティ管理者又は情報システム管理者は、業務委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案

（イ）契約の締結

（ウ）重要情報を取り扱う場合の秘密保持契約（NDA）の締結

（３）業務委託実施期間中の対策

①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間中、以下を全て含む対策を実施しなければならない。

（ア）委託判断基準に従った重要情報の提供

（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的確認及び処置の実施

（ウ）情報セキュリティ管理者又は情報システム管理者への措置内容の報告（重要度に応じて統括情報セキュリティ責任者及び CISO へ報告）

（エ）情報セキュリティインシデント又は情報の目的外利用等を認知した場合における、委託業務の一時中断等を含む、契約に基づく対応要求

②情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間中、委託事業者に対し、以下を全て含む対策の実施を求めなければならない。

（ア）情報の適正な取扱いのための情報セキュリティ対策

（イ）情報セキュリティ対策の履行状況に関する定期的な報告

（ウ）情報セキュリティインシデント又は情報の目的外利用等を認知した場合における、委託業務の一時中断等を含む、契約に基づく対応

（４）業務委託終了時の対策

①情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際し、以下を

全て含む対策を実施しなければならない。

（ア）委託期間を通じた情報セキュリティ対策が適切に実施されたことの確認を含む検収

（イ）委託事業者において取り扱われた情報の返却、廃棄又は抹消の確認

②情報セキュリティ管理者又は情報システム管理者は、委託事業者に対し、以下を全て含む対応を求めなければならない。

（ア）委託期間を通じた情報セキュリティ対策が適切に実施されたことの報告を含む検収の受検

（イ）委託事業者において取り扱われた情報の返却、廃棄又は抹消

8.2. 情報システムに関する業務委託

（１）共通的対策

①情報システム管理者は、情報システムに関する業務委託に際し、当院の意図しない変更又は不正操作が加えられないための対策を、委託事業者の選定条件及び仕様に含めなければならない。

②情報システム管理者は、医療情報系の情報システム又はこれに接続される機器に関する業務を委託する場合には、委託事業者から、「製造業者又はサービス事業者が作成した医療情報セキュリティ開示書（MDS／SDS)」の提出を受け、当該情報の内容を確認しなければならない。

（２）情報システムの構築を業務委託する場合の対策

情報システム管理者は、契約に基づき、委託事業者に以下を全て含む対策の実施を求めなければならない。

①情報システムのセキュリティ要件の適切な実装

②情報セキュリティの観点に基づく試験の実施

③情報システムの開発環境及び開発工程における情報セキュリティ対策

（３）情報システムの運用・保守を業務委託する場合の対策

①情報システム管理者は、情報システムに実装されたセキュリティ機能が適切に運用されるよう、必要な要件を契約に基づき委託事業者に求めなければならない。

②情報システム管理者は、情報セキュリティ対策に伴うシステム変更について、委託事業者に速やかな報告を求めなければならない。

③情報システム管理者は、医療情報系の情報システム又はこれに接続される機器について、委託事業者によるリモートメンテナンス（保守）の有無及び対象機器を把握するため、当該事業者に対して確認を行わなければならない。

8.3. 外部サービス（クラウドサービス）の利用（病院機密性 2 以上の情報を取り扱う場合）

（1）クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、病院機密性 2 以上の情報を取り扱う場合、以下を含む外部サービス（以下「クラウドサービス」という。）の選定に関する運用規程を整備しなければならない。

①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下、本節において「クラウドサービス利用判断基準」という。）

②クラウドサービス提供者の選定基準

③クラウドサービスの利用申請に係る許可権限者及び利用手続

④クラウドサービス管理者の指名及びクラウドサービスの利用状況の管理方法

（2）クラウドサービスの利用に係る運用規程の整備

統括情報セキュリティ責任者は、病院機密性 2 以上の情報を取り扱う場合におけるクラウドサービスの利用について、以下を含む運用規程を整備しなければならない。

①クラウドサービスの特性及び責任分界点の考え方を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針

②クラウドサービスの特性及び責任分界点の考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針

③クラウドサービスの特性及び責任分界点の考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針

（ア）クラウドサービス利用終了時の対応

（イ）クラウドサービスで取り扱った情報の消去又は廃棄

（ウ）クラウドサービス利用のために作成したアカウントの無効化又は廃止

（3）クラウドサービスの選定

①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に基づき、診療業務への影響度等を考慮した上で、クラウドサービスの利用を検討しなければならない。

②情報セキュリティ責任者は、クラウドサービス提供者の選定にあたり、以下の事項を含む情報セキュリティ対策を選定条件に含めなければならない。

（ア）クラウドサービスの利用を通じて当院が取り扱う情報のクラウドサービス提供者による目的外利用の禁止

（イ）クラウドサービス提供者における情報セキュリティ対策の内容及び管理体制

（ウ）クラウドサービス提供者、その従業員又は再委託先等による当院の意図しない

情報の変更を防止する管理体制

（エ）クラウドサービス提供者の組織体制、実績、クラウドサービス提供に従事する者の専門性等に関する情報提供並びに調達仕様書による施設の場所（国・リージョン）の指定

（オ）情報セキュリティインシデント発生時の対処方法

（カ）情報セキュリティ対策及び契約履行状況の確認方法

（キ）情報セキュリティ対策が不十分な場合の是正措置

③情報セキュリティ責任者は、クラウドサービスの中断又は終了時においても診療業務が継続できるよう、業務移行や代替手段に関する対策を検討し、選定条件に含めなければならない。

④情報セキュリティ責任者は、クラウドサービスを通じて取り扱う情報の格付を踏まえ、以下の事項をクラウドサービス提供者の選定条件に含めなければならない。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤情報セキュリティ責任者は、クラウドサービスの利用を通じて当院が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて、当院の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

⑥情報セキュリティ責任者は、クラウドサービス提供者がその役務内容を一部再委託する場合においても、当院と同等の情報セキュリティ水準が確保されるよう、再委託の条件及び承認手続を選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認可否を判断しなければならない。

⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じて必要なセキュリティ要件を定め、クラウドサービスを選定しなければならない。

⑧情報セキュリティ責任者は、クラウドサービスが提供する部分を含む情報の流通経路全体を考慮したセキュリティ設計を行い、以下を含むセキュリティ要件を定めなければならない。

（ア）クラウドサービスに求める情報セキュリティ対策

（イ）クラウドサービスで取り扱う情報の保存場所（国、地域）及び廃棄方法

（ウ）クラウドサービスに求めるサービスレベル

⑨統括情報セキュリティ責任者は、情報セキュリティ監査による報告書、各種認証制度の取得状況等を踏まえ、クラウドサービス提供者の信頼性を総合的・客観的に評価しなければならない。

（4）クラウドサービスの利用に係る調達・契約

①情報セキュリティ責任者は、クラウドサービスを調達する場合、クラウドサービス提供者の選定基準、選定条件及び定めたセキュリティ要件を調達仕様に含めなければならない。

②情報セキュリティ責任者は、クラウドサービス提供者およびクラウドサービスが調達仕様を満たすことを契約締結までに確認し、必要な承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

（5）クラウドサービスの利用承認

①情報セキュリティ責任者は、クラウドサービスの利用開始又は調達に際し、所定の手続により利用申請の許可権限者へ利用申請を行わなければならない。

②利用申請の許可権限者は、申請内容を審査し、利用の可否を決定しなければならない。

③利用申請の許可権限者は、承認したクラウドサービスは、承認済みクラウドサービスとして記録しなければならない。

（6）クラウドサービスを利用した情報システムの導入・構築時の対策

①統括情報セキュリティ責任者は、クラウドサービスの特性及び責任分界点の考え方を踏まえ、以下を含むクラウドサービスを利用した情報システムを構築する際のセキュリティ対策を規定しなければならない。

（ア）情報のアクセス制御

（イ）情報の暗号化

（ウ）開発時のセキュリティ対策

（エ）設計・設定ミス防止対策

②情報システム管理者は、クラウドサービスを利用する際には、情報システム台帳及び関連文書等に記録するとともに、統括情報セキュリティ責任者へ報告しなければならない。

③情報システム管理者は、クラウドサービスの運用開始前までに、情報セキュリティの維持に関する手順、インシデントへの対応手順及びサービス停止時の復旧手順等を整備しなければならない。

④情報システム管理者は、前項において定める規程に対し、構築時に実施状況を確認・記録しなければならない。

（7）クラウドサービスを利用した情報システムの運用・保守時の対策

①統括情報セキュリティ責任者は、クラウドサービスの特性及び責任分界点の考え方を踏まえ、以下を含むクラウドサービスの運用・保守時のセキュリティ対策を規定し

なければならない。

（ア）クラウドサービス利用方針

（イ）職員等への教育

（ウ）取り扱う資産の管理

（エ）アクセス制御

（オ）暗号化

（カ）通信制御

（キ）設計・設定時の誤り防止

（ク）事業継続対策

②情報システム管理者は、クラウドサービスの運用・保守時の情報セキュリティ対策の項目等で修正又は変更等があった場合、台帳及び関連文書を更新するとともに、統括情報セキュリティ責任者へ報告しなければならない。

③情報システム管理者は、新たな脅威の出現等を踏まえ、セキュリティ対策の見直しを適時行わなければならない。

④情報システム管理者は、クラウドサービスの特性及び責任分界点の考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対応手順を整備しなければならない。

⑤情報システム管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

（８）クラウドサービスを利用した情報システムの更改・廃棄時の対策

①統括情報セキュリティ責任者及び情報システム管理者は、クラウドサービスの特性及び責任分界点の考え方を踏まえ、以下を含むクラウドサービス利用終了時のセキュリティ対策を規定しなければならない。

（ア）利用終了時の対応

（イ）取り扱った情報の消去又は廃棄

（ウ）アカウントの廃止

②情報システム管理者は、前各項において定める規定に対し、クラウドサービス利用終了時に実施状況を定期的に確認・記録しなければならない。

8.4. 外部サービス（クラウドサービス）の利用（病院機密性 2 以上の情報を取り扱わない場合）

（１）クラウドサービスの利用に係る規程の整備

統括情報セキュリティ責任者は、病院機密性 2 以上の情報を取り扱わない場合におけるクラウドサービスの利用について、以下を含む運用規程を整備しなければならない。

①利用可能な業務の範囲
②利用申請に係る許可権限者及び利用手続
③利用状況の管理
④利用の運用手順

（2）クラウドサービスの利用における対策の実施
①情報セキュリティ管理者は、利用を予定するクラウドサービスについて、約款、利用規約その他の提供条件等を確認し、当該サービスの利用に伴う情報セキュリティ上のリスクが、当院として許容可能であることを確認した上で、利用申請の許可権限者へ利用申請を行わなければならない。また、情報セキュリティ管理者は、当該クラウドサービスの利用に際し、必要に応じて適切な情報セキュリティ対策を講じなければならない。
②利用申請の許可権限者は、情報セキュリティ管理者からのクラウドサービス利用申請について内容を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスは、承認済みクラウドサービスとして記録しなければならない。

9. 評価・見直し

9.1. 監査

（1）実施方法
CISO は、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、毎年度及び必要に応じて、監査を実施させなければならない。

（2）監査を行う者の要件
①統括情報セキュリティ管理者は、監査を実施する場合には、被監査部門から独立した立場の者に対して監査の実施を依頼しなければならない。
②監査を行う者は、情報セキュリティ及び監査に関する専門知識を有する者でなければならない。

（3）監査実施計画の立案及び実施への協力
①統括情報セキュリティ管理者は、監査を実施するに当たって監査実施計画を立案し、CISO の承認を得なければならない。
②被監査部門は、監査の実施に協力しなければならない。

（4）委託事業者に対する監査
事業者に業務委託を行っている場合、統括情報セキュリティ管理者は、委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査又

は確認を定期的又は必要に応じて行わなければならない。

（５）監査結果の報告

統括情報セキュリティ管理者は、監査結果を取りまとめ、CISO に報告しなければならない。

（６）監査記録の保管

CISO は、監査の実施により収集した監査証拠、監査報告書の作成のための監査調書について、紛失等が生じないよう適切に保管しなければならない。

（７）監査結果への対応

①CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者又は情報システム管理者に対し、必要な是正措置又は改善計画の策定及び実施を指示しなければならない。また、改善計画が未完了の場合は、定期的に進捗状況の報告を求めなければならない。

②CISO は、指摘事項を所管していない部門の情報セキュリティ管理者に対しても、同様の課題がある可能性が高いと判断した場合には、当該事項の内容を確認させなければならない。また、院内で横断的な改善が必要な事項については、統括情報セキュリティ管理者に対し、当該事項への対処（改善計画の策定等）を指示するとともに、改善計画が未完了の場合は、定期的に進捗状況の報告を求めなければならない。

（８）情報セキュリティポリシー等の見直しへの活用

CISO は、監査結果を、情報セキュリティポリシー及び関連規程等の見直し、並びにその他情報セキュリティ対策の改善に活用しなければならない。

9.2. 自己点検

（１）実施方法

①統括情報セキュリティ責任者、統括情報セキュリティ管理者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携し、所管する部門における情報セキュリティ対策の実施状況について、毎年度又は必要に応じて情報セキュリティポリシーに基づく自己点検を実施しなければならない。

（２）自己点検結果等の報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果及び当該結果に基づく改善策を取りまとめ、CISO に報告しなければなら

ない。

（3）自己点検結果の活用

①職員等は、自己点検の結果を踏まえ、自己の権限及び職務の範囲内において、情報セキュリティ対策の改善に努めなければならない。

②CISO は、自己点検結果を、情報セキュリティポリシー及び関連規程の見直し、その他情報セキュリティ対策の改善に活用しなければならない。

9.3. 情報セキュリティポリシー及び関係規程等の見直し

CISO は、情報セキュリティ監査及び自己点検の結果、並びに法令、ガイドライン、医療情報を取り巻く脅威動向等の変化を踏まえ、毎年度及び重大な変化が生じた場合にリスク評価を行い、必要があると認めた場合には、情報セキュリティポリシー及び関係規程等の見直しを行うものとする。また、院内全体で横断的な改善が必要と判断される情報セキュリティ対策については、職制及び職務に応じた措置の実施又は指示をしなければならない。