川口市立医療センター情報セキュリティ対策基準

第１　趣旨

この対策基準は、川口市立医療センター（以下、「医療センター」という。）における川口市情報セキュリティ基本方針に規定する対策等の実施について、必要な事項を定めるものとする。

第２　定義

この対策基準における用語の意義は、川口市情報セキュリティ基本方針第２条に規定する用語の定義を準用する他、以下に定めるところによる。

- 医療情報システム
  電子カルテ及び各部門で使用する医療情報を扱う情報システムをいう。

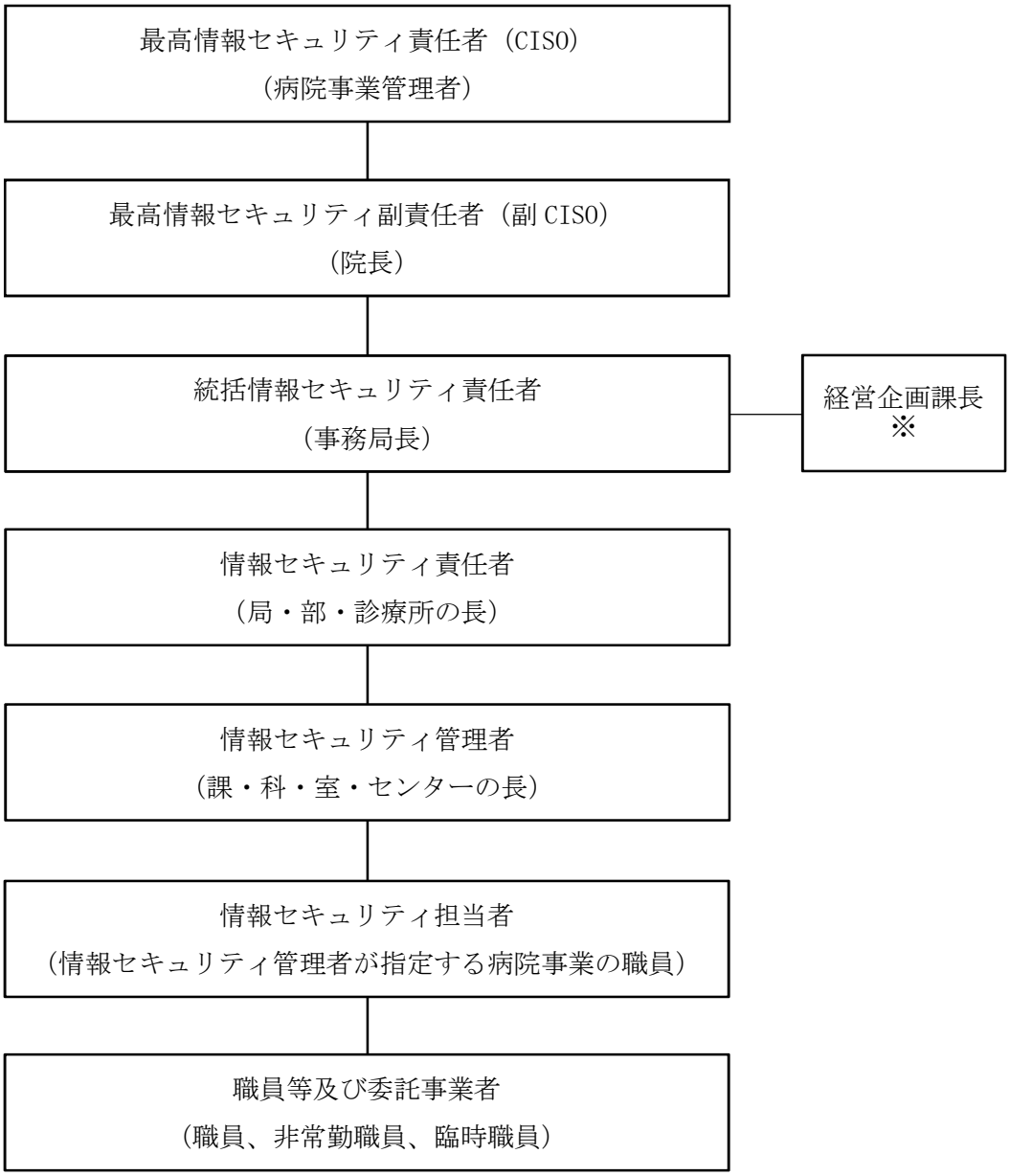
第３　情報資産の範囲

この対策基準が対象とする情報資産は、川口市情報セキュリティ基本方針第４条(2)に規定する情報資産の範囲のうち、川口市病院事業（以下、「病院事業」という。）に供するものとする。

第４　組織体制及び役割

１　組織体制

情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。



※　統括情報セキュリティ責任者は、自身の権限に属する事務を経営企画課長に処理させることができる。

（CISO: Chief Information Security Officer、最高情報セキュリティ責任者）

2　組織の構成員と役割

各組織の構成員及びその役割は以下のとおりとする。

なお、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）が定める「医療情報システム安全管理責任者」は、以下の「最高情報セキュリティ責任者（CISO)」が担うものとする。

組織・役職名	対象者・構成員	役割・権限等
川口市立医療センター情報セキュリティ委員会（以下、「セキュリティ委員会」という。）	「川口市立医療センター情報セキュリティ委員会設置及び運営要綱」に基づき選出	医療センターの情報セキュリティ対策を統一的に行うため、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
最高情報セキュリティ責任者（CISO)	病院事業管理者	1 医療センターにおける全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 2 最高情報セキュリティ責任者に事故があるとき、又は最高情報セキュリティ責任者が欠けたときは、最高情報セキュリティ副責任者がその職務を代理する。 3 最高情報セキュリティ責任者は、本対策基準に定められた自らの担務を、最高情報セキュリティ副責任者その他の本対策基準に定める責任者に担わせることができる。 4 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した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めることができる。
最高情報セキュリティ副責任者（副 CISO)	院長	1 最高情報セキュリティ責任者を補佐する。 2 最高情報セキュリティ責任者からの委任を受けて医療センターの情報セキュリティに関する事務を総括する。
統括情報セキュリティ責任者	事務局長	1 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する。 2 医療センターの全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 3 医療センターの全てのネットワークにおける情

組織・役職名	対象者・構成員	役割・権限等
		報セキュリティ対策に関する権限及び責任を有する。 4 情報セキュリティ責任者及び情報セキュリティ管理者に対して、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 医療センターの情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。 6 医療センターの共通的な情報資産に関する情報セキュリティ実施手順の策定及び維持・管理を行う権限及び責任を有する。 7 緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、最高情報セキュリティ副責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。 8 緊急時には最高情報セキュリティ責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。 9 情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告しなければならない。 10 自身の権限に属する事務を、経営企画課長に処理させることができる。
情報セキュリティ責任者	事務局の長、診療局の長、特殊診療局の長（最高情報セキュリティ責任者が指定するセンター長)、薬剤部	1 所管する局・部・診療所（以下、「部局等」という。）の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。 2 所管する部局等の情報セキュリティ実施手順を作成する。なお、作成に当たっては、統括情報セキュリティ責任者に意見を求めなければなら

組織・役職名	対象者・構成員	役割・権限等
	の長、看護部の長及び診療所の長	ない。 3 所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
情報セキュリティ管理者	事務局の課長、診療局の科室長、特殊診療局のセンター長、薬剤部の長が指定する副薬剤部長又は薬剤長、看護部の長が指定する副看護部長又は看護師長及び診療所の長が指定する病院事業の職員	1 所管する課・科・室・センター・部・診療所（以下、「科課室等」という。）及び情報システム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。 2 情報セキュリティ責任者の指示に従い、所管する情報資産に係る情報セキュリティ実施手順の策定及び更新を行う。 3 所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 4 所掌する科課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、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最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。 5 外部サービス（クラウドサービス、以下「クラウドサービス」という。）管理者として、許可された外部サービスの利用状況の管理とし、導入・構築・運用・保守・公開・廃棄といった利用のライフサイクルにおいて実施状況の確認や記録を行う。 ※複数の組織にまたがって利用する場合、主管する科課室等がクラウドサービス管理者となる。
情報セキュリティ担当者	情報セキュリティ管理者が指定する病院事業の職員	情報セキュリティ管理者の指示等に従い、その所属する科課室等及び施設等の情報セキュリティに関する対策の向上を図る。
職員等	職員、非常勤・臨時職員等	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する。

3　兼務の禁止

(1) 情報セキュリティ対策の実施において、や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、や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。

4　CSIRT の設置・役割

(1) 最高情報セキュリティ責任者は、CSIRT（シーサート：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、その役割を明確化しなければならない。

(2) 最高情報セキュリティ責任者は、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との連携等を行う職員等を定めなければならない。

(3) 最高情報セキュリティ責任者は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より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。

(4) 最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

(5) 情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者、厚生労働省、埼玉県等へ報告しなければならない。

(6) 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・公表対応を行わなければならない。

(7) 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

5　クラウドサービス利用における組織体制

情報セキュリティ責任者及び情報セキュリティ管理者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

第５　情報資産の分類と管理

1　情報資産の分類

医療センターにおける情報資産は、機密性、完全性及び可用性により、次のとおり分類し、当該分類に応じた取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
自治体 機密性３Ａ	行政事務及び病院事務（以下、「病院事務等」という。）で取り扱う情報資	・医療センターが管理する以外のパソコン等の端末での作業の原

	産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報資産	則禁止（自治体機密性３の情報資産に対して） ・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・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 ・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
自治体 機密性３Ｂ	病院事務等で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体 機密性３Ｃ	病院事務等で取り扱う情報資産のうち、自治体機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体 機密性２	病院事務等で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体 機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	－

完全性による情報資産の分類

分類	分類基準	取扱制限
自治体 完全性２	病院事務等で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害される又は病院事務等の適確な遂行に支障（軽微なものを除く。）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
自治体 完全性１	自治体完全性２の情報資産以外の情報資産	－

可用性による情報資産の分類

分類	分類基準	取扱制限
自治体	病院事務等で取り扱う情報資産のう	・バックアップ、指定する時間以

可用性２	ち、滅失、紛失又は当該情報資産が利用不可能であることにより、利用者の権利が侵害される又は病院事務等の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体 可用性１	自治体可用性２の情報資産以外の情報資産	－

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　情報セキュリティ管理者は、所管する情報システムに対して、当該情報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、複製等された情報資産も１の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、クラウドサービスの環境に保存される情報資産についても１の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

(2) 情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（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等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、当該情報の分類と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になった場合は、当該情報を消去しなければならない。

(4) 情報資産の入手

ア　病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扱いをしなければならない。

イ　病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、当該情報の分類

と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、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、業務以外の目的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、情報資産の分類に応じ、適正な取扱いをしなければならない。

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。

(6) 情報資産の保管

ア　情報セキュリティ管理者は、情報資産の分類に従って、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は、書込禁止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は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

エ　情報セキュリティ管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記録媒体を保管する場合、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自治体機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

(8) 情報資産の運搬

ア　車両等により自治体機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産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。

イ　自治体機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。また、情報セキュリティ管理者は、記録を作成し、保管しなければならない。

(9) 情報資産の提供・公表

ア　自治体機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。なお、委託事業者に廃棄等を行わせる場合も同様とする。

イ　自治体機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

ウ　情報セキュリティ管理者は、自治体機密性２以上の情報資産の外部提供を許可する場

合は、当該情報資産の外部提供が個人情報の保護に関する法律及びその他関連する規定に抵触しないことを確認しなければならない。

エ　情報セキュリティ管理者は、利用者に公開する情報資産について、完全性を確保しなければならない。

(10) 情報資産の廃棄等

ア　情報資産の廃棄やリース返却等を行う者は、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、物理的又は磁気的破壊を実施する等、情報を復元できないように処置しなければならない。なお、委託事業者に廃棄等を行わせる場合も同様とする。

イ　情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

ウ　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

エ　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

第６　情報システム全体の強靭性の向上

統括情報セキュリティ責任者は、情報システム全体の強靭性の向上として、次の事項を措置しなければならない。

１　医療情報システム接続系

(1) 医療情報システム接続系と他の領域との分離

医療情報システム接続系と他の領域を通信できないようにしなければならない。医療情報システム接続系と外部との通信をする必要がある場合は、通信経路の限定(IP アドレス等)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、十分に安全性が確保された外部接続先については、この限りではない。

(2) 情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、２つ以上を併用する認証（多要素認証）を利用しなければならない。ただし、運用や機能上の制限等により利用が困難であり、別に十分な対策が取られている場合については、この限りではない。

イ　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

２　病院用インターネット接続系（病院業務用、自己研鑽用、利用者開放用）

(1) 病院用インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化等により、情報セキュリティインシデントの早期発見と対処等の情報セキュリティ対策を講じなければならない。

(2) 病院用インターネット接続系と他の領域との分離

病院用インターネット接続系と他の領域を通信できないようにしなければならない。病院用インターネット接続系の各用途間のネットワークにおいても同様とする。

(3) 情報のアクセス及び持ち出しにおける対策（病院業務用、自己研鑽用）

ア　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、２つ以上を併用する認証（多要素認証）を利用しなければならない。ただし、運用や機能上の制限等により利用が困難であり、別に十分な対策が取られている場合については、この限りではない。

イ　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

3　個人番号（マイナンバー）利用事務系、LGWAN 接続系及びインターネット接続系

個人番号（マイナンバー）利用事務系、LGWAN 接続系及びインターネット接続系については、川口市が定める規定に従うものとする。

第７　物理的セキュリティ

1　サーバ等の管理

(1) 機器の取付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、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正に固定する等、必要な措置を講じなければならない。

(2) サーバの冗長化

情報セキュリティ管理者は、所管するサーバに格納している情報の重要性、可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長化を施し、サービスや業務を停止させないよう努めなければならない。

(3) 機器の電源

ア　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及び施設管理部門と連携し、所管するサーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を可能な限り備え付けなければならない。

イ　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及び施設管理部門と連携し、落雷等による過電流に対して、所管するサーバ等の機器を保護するための措置を可能な限り講じなければならない。

(4) 通信ケーブル等の配線

ア　情報セキュリティ管理者は、施設管理部門と連携し、所管する通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ　情報セキュリティ管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

ウ　情報セキュリティ管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ　情報セキュリティ管理者は、自ら又は操作を認めた者以外の者が配線を変更、追加できないように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

ア　情報セキュリティ管理者は、所管する自治体可用性２のサーバ等の機器の定期保守を必要に応じて実施しなければならない。

イ　情報セキュリティ管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、秘密保持契約を締結するほか、秘密保持体制の確認等を行わなければならない。

(6) 病院外への機器の設置

情報セキュリティ管理者は、病院外に所管するサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(7) 機器の廃棄等

ア　情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

イ　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

２　管理区域の管理

(1) 管理区域の構造等

ア　管理区域とは、ネットワークの基幹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や電磁的記録媒体の保管庫をいう。

イ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、可能な限り管理区域を地階又は１階に設けてはならない。また、無窓の外壁にする等可能な限り外部からの侵入が容易にできないようにしなければならない。

ウ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

エ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、可能な限り管理区域内の機器等に転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

オ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、可能な限り管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

カ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携して、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

ア　情報セキュリティ管理者は、施設管理部門と連携して、管理区域への入退室を許可された者のみに制限し、磁気、IC カード及び指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

イ　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報セキュリティ管理者は、自治体機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(3) 機器等の搬入出

ア　情報セキュリティ管理者は、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。

イ　情報セキュリティ管理者は、管理区域の機器等の搬入出について、職員を立ち会わせなければならない。

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責任者は、基幹となる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) 情報セキュリティ管理者は、所管する情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

(3) 統括情報セキュリティ責任者は、医療センターの管轄外のネットワーク（以下「外部ネ

ットワーク」という。）との接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

(4) 統括情報セキュリティ責任者は、自治体機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

(5) 統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

(6) 統括情報セキュリティ責任者は、自治体可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

4　職員等の利用する端末や外部記録媒体等の管理

(1) 情報セキュリティ管理者は、盗難防止のため、執務室等で利用するパソコン等の端末のワイヤー等により固定し（病院内の会議室等に持ち出す場合や病院業務に支障が生じる場合等を除く）、保存されている情報資産の機密性に応じて外部記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。外部記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(2) 情報セキュリティ管理者は、パソコン等の端末及び情報システムへのログインに際し、IC カード、パスワード又はその他の認証情報の入力を必要とするように設定しなければならない。また、取り扱う機密性に応じて、「知識」、「所持」、「存在」を利用する認証手段のうち２つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

(3) 情報セキュリティ管理者は、その所管するパソコン等の端末について、外部記録媒体への情報資産の書き込み禁止の措置を講じなければならない。ただし、統括情報セキュリティ責任者の許可を得た場合は、この限りではない。

(4) 情報セキュリティ管理者は、外部記録媒体の管理一覧表及び使用簿を作成し管理しなければならない。

第８　人的セキュリティ

1　職員等の遵守事項

(1) 職員等の遵守事項

ア　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及び実施手順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、遵守することが困難な点等がある場合は、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。

イ　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、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(ｱ) 統括情報セキュリティ責任者は、自治体機密性２以上、自治体可用性２、自治体完全性２の情報資産を外部で処理する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、情報資産を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。また、情報セキュリティ管理者は、その記録を作成し、保管しなければならない。

(ｳ) 職員等は、外部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なければならない。

エ　医療センターが管理する以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ｱ) 職員等は、医療センターが管理する以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合で、情報セキュリティ管理者の許可を得た場合はこの限りでない。

(ｲ) 情報セキュリティ管理者は、医療センターが管理する以外のパソコン、モバイル端末及び電磁的記録媒体等の使用について、適正に管理しなければならない。

(ｳ) 職員等は、外部で情報処理作業を行う際、医療センターが管理する以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、統括情報セキュリティ責任者が定めた実施手順を遵守しなければならない。

オ　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、病院外で業務をする場合、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ　情報システムにおけるセキュリティ設定変更の禁止

職員等は、情報システムに関するセキュリティ機能の設定を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。

キ　机上の端末等の管理

(ｱ) 職員等は、机上のパソコン等の端末を第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席する際にはICカードを取り外し、端末をロックすることにより、情報資産を保全しなければならない。

(ｲ) 職員等は、ICカードによる運用対象外の情報システムについては、離席する際には、アプリケーションの終了、パスワードによるロックをかけたスクリーンセーバー、ログオフ等の手段を複合的に用いることにより、情報資産を保全しなければならない。

(ｳ) 職員等は、机上の外部記録媒体や情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席する際には、外部記録媒体や文書等の容易に閲覧されない場所への保管等、

適正な措置を講じなければならない。

ク　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。

ケ　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用に当たっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(2) 非常勤及び臨時職員等への対応

ア　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、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

イ　情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意についての署名を求めるものとする。

ウ　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員等にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(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責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように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、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

2　研修・訓練

(1) 情報セキュリティに関する研修・訓練

ア　最高情報セキュリティ責任者は、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。

イ　最高情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

(2) 研修計画の立案及び実施

ア　経営企画課長は、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を定期的に立案し、統括情報セキュリティ責任者の承認を得なければならない。

イ　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければなら

ない。

ウ　研修は、情報セキュリティ責任者、情報セキュリティ管理者及びその他職員等に対して、それぞれの役割等に応じたものにしなければならない。

エ　経営企画課長は、統括情報セキュリティ責任者に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。また、必要に応じ、情報セキュリティ委員会に報告するものとする。

(3) 緊急時対応訓練

最高情報セキュリティ責任者は、定期的又は必要に応じて緊急時対応を想定した訓練を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

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。

3　情報セキュリティインシデントの報告

(1) 情報セキュリティインシデントの報告

ア　職員等は、情報セキュリティインシデント（事故、情報システムの欠陥及び誤動作等）を認知した場合や利用者等外部から報告を受けた場合は、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。

イ　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責任者に報告しなければならない。

ウ　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者並び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。

エ　情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

オ　情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

カ　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、所定の手順に従い関係機関等へ報告しなければならない。

(2) 情報セキュリティインシデント原因の究明・記録、再発防止等

ア　CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ　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、最高情報セキュリティ責任者に速やかに報告しなければならない。

ウ　CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければ

ならない。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生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セキュリティ管理者へ確認を指示しなければならない。

エ　CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

オ　最高情報セキュリティ責任者は、CSIRT から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

4　ID 及びパスワード等の管理

(1) IC カード等の取扱い

ア　情報セキュリティ管理者及び職員等は、IC カード等について関係実施手順に基づき適正に取扱わなければならない。

イ　統括情報セキュリティ責任者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

ウ　統括情報セキュリティ責任者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2) ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　自己が利用している ID は、他人に利用させてはならない。

イ　共用 ID を利用する場合は、共用 ID の利用を許可された者以外に利用させてはならない。

(3) パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字や小文字、数字、記号を織り交ぜる等）にしなければならない。

エ　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

カ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

キ　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

ク　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

は除く。

第９　技術的セキュリティ

１　情報システム及びネットワークの管理

(1) 情報システムの設定等

情報セキュリティ管理者は、情報システムを設置する場合、他科課室等の許可していない職員等が情報資産を閲覧及び使用できないように、アクセス制御の設定をしなければならない。

(2) ファイルサーバの設定等

ア 情報セキュリティ管理者は、職員等が使用できる所管するファイルサーバの容量を設定し、職員等に周知しなければならない。

イ 情報セキュリティ管理者は、所管するファイルサーバを科課室等の単位で構成し、原則として、職員等が他科課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ　情報セキュリティ管理者は、利用者の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一科課室内であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

(3) バックアップの実施

ア　統括情報セキュリティ責任者及び情報セキュリティ管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

イ　情報セキュリティ管理者は、所管する重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

ウ　情報セキュリティ管理者は、所管する重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

エ　情報セキュリティ責任者及び情報セキュリティ管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が医療センターの求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、必要に応じて、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(4) 他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、必要に応じてその取扱いに関する事項をあらかじめ定め、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の許可を得なければならない。

(5) システム管理記録及び作業の確認

ア　情報セキュリティ管理者は、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。

イ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管する情報システムにおいて、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、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。

ウ　情報セキュリティ管理者は、所管する情報システムにおいて、自ら又は操作を認めた者がシステム変更等の作業を行う場合は、必要に応じて２名以上で作業させ、互いにその作業を確認させなければならない。

(6) 情報システム仕様書等の管理

情報セキュリティ管理者は、所管する情報システムのネットワーク構成図、仕様書等の情報資産について、記録媒体に関わらず、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。

(7) ログの取得等

ア　情報セキュリティ管理者は、所管する情報システムの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、一定の期間保存しなければならない。

イ　情報セキュリティ管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

ウ　情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

エ　情報セキュリティ責任者及び情報セキュリティ管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

(8) 障害記録

情報セキュリティ管理者は、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。

(9) ネットワークの接続制御、経路制御等

ア　統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定

しなければならない。

イ　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

ウ　情報セキュリティ管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直さなければならない。

(10) 外部の者が利用できるシステムの分離等

情報セキュリティ管理者は、所管する情報システムにおいて、外部の者が利用できる場合、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

(11) 外部ネットワークとの接続制限等

ア　情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者並びに統括情報セキュリティ責任者の許可を得なければならない。

イ　情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、病院内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

ウ　情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、病院内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

オ　情報セキュリティ管理者は、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しなければならない。

(12) 複合機のセキュリティ管理

ア　統括情報セキュリティ責任者は、プリンタ・ファクシミリ・イメージスキャナ・コピー等の機能が一つにまとめられている機器（以下「複合機」という。）を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　複合機を調達した情報セキュリティ管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　複合機を調達した情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講

じなければならない。

(13) IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、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。

(14) 無線 LAN のセキュリティ対策及びネットワークの盗聴対策

ア　情報セキュリティ管理者は、無線 LAN を利用するときは、統括情報セキュリティ責任者の許可を得なければならない。

イ　統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

ウ　統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、必要に応じて暗号化等の措置を講じなければならない。

(15) 電子メールのセキュリティ管理

ア　統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ　統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

オ　統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

(16) 電子メールの利用制限

ア　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

イ　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

ウ　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(17) 電子署名・暗号化

ア　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、最高情報セキュリティ責任者が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

イ　職員等は、暗号化を行う場合に最高情報セキュリティ責任者が定める以外の方法を用いてはならない。また、最高情報セキュリティ責任者が定めた方法で暗号のための鍵を

管理しなければならない。

ウ　最高情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(18) 無許可ソフトウェアの導入等の禁止

ア　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。

イ　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責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

ウ　職員等は、不正にコピー、改ざん等されたソフトウェアを利用してはならない。

(19) 機器構成の変更の制限

ア　職員等は、パソコン等の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。

イ　職員等は、業務上、パソコン等の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、機器を所管する情報セキュリティ管理者の許可を得なければならない。

(20) 無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なく情報システムをネットワークに接続してはならない。

(21) 業務外ネットワークへの接続の禁止

ア　職員等は、パソコン等の端末を、有線・無線を問わず、その端末を接続して利用するよう情報セキュリティ管理者によって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。

イ　統括情報セキュリティ責任者は、パソコン等の端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(22) 業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、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。

(23) ウェブ会議サービスの利用時の対策

ア　統括情報セキュリティ責任者は、ウェブ会議を適切に利用するための利用手順を定めなければならない。

イ　職員等は、医療センターの定める利用手順に従い、ウェブ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

ウ　職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

エ　職員等は、外部からウェブ会議に招待される場合は、医療センターの定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(24) ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、医療センターが管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ｱ) 医療センターのアカウントによる情報発信が、実際の医療センターのものであることを明らかにするために、医療センターの自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

イ　自治体機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

ウ　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なければならない。

エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

オ　自治体可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、医療センターの自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

２　アクセス制御

(1) アクセス制御等

ア　アクセス制御

統括情報セキュリティ責任者又は情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者 ID の取扱い

(ｱ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

(ｲ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、当該情報システムを所管する情報セキュリティ管理者に報告しなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管する情報システムについて、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(ｴ) 情報セキュリティ管理者は、職員等に対する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。

ウ　特権を付与された ID の管理等

(ｱ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管する情報システムに係る管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該

IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを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責任者又は情報セキュリティ管理者の特権を付与されたIDを利用する者は、統括情報セキュリティ責任者又は情報セキュリティ管理者が認めた者でなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、特権を付与されたID及びパスワードの変更について、委託事業者に行わせてはならない。

(ｴ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、特権を付与されたID及びパスワードについて、職員等の端末等のパスワードよりもセキュリティ機能を強化しなければならない。

(ｵ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

ア　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得なければならない。

イ　統括情報セキュリティ責任者は、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。

ウ　統括情報セキュリティ責任者は、外部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。

エ　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

オ　統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者は、外部からのアクセスに利用するパソコン等の端末に、セキュリティ確保のために必要な措置を講じなければならない。

カ　職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を病院内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

キ　統括情報セキュリティ責任者は、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、やむを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 自動識別の設定

統括情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別される設定となるよう努めるものとする。

(4) ログイン時の表示等

情報セキュリティ管理者は、所管する情報システムについて、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情報システムを設定しなければならない。

(5) 認証情報の管理

ア　統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

イ　統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

ウ　統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、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責任者又は情報システムを所管する情報セキュリティ管理者は、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。

3　システム開発、導入、保守等

(1) 情報システムの調達

ア　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、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のないことを確認しなければならない。

(2) 情報システムの開発

ア　システム開発における責任者及び作業者の特定

情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。

イ　システム開発における責任者、作業者の ID の管理

(ｱ) 情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

ウ　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) 情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、必要に応じて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。

(3) 情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

(ｱ) 情報システムを所管する情報セキュリティ管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、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。

イ　テスト

(ｱ) 情報システムを所管する情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ｳ) 開発したシステムについて受け入れテストを行う場合、情報システムを所管する部署及び経営企画課がそれぞれ独立したテストを行わなければならない。

ウ　機器等の納入時又は情報システムの受入れ時

情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

(4) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

ア　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

イ　情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(5) システム開発・保守に関連する資料等の整備・保管

ア　情報システムを所管する情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

(ｱ) 情報システムを所管する情報セキュリティ管理者は、情報システムを新規に構築

し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

・情報セキュリティインシデントを認知した際の対処手順

・情報システムが停止した際の復旧手順

イ　情報システムを所管する情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

ウ　情報システムを所管する情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(6) 情報システムにおける入出力データの正確性の確保

ア　情報システムを所管する情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

イ　情報システムを所管する情報セキュリティ管理者は、所管するウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ｱ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、 脆弱性が発覚した際は必要な措置を講じなければならない。

(ｲ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　情報システムを所管する情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(7) 情報システムの変更管理

情報システムを所管する情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(8) 開発・保守用のソフトウェアの更新等

情報システムを所管する情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(9) システム更新又は統合時の検証等

情報システムを所管する情報セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

4　不正プログラム対策

(1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、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。

ア　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

イ　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

エ　所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の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。

オ　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

カ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

キ　業務で利用するソフトウェアは、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したソフトウェアを利用してはならない。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。

ク　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

(2) 情報セキュリティ管理者の措置事項

情報システムを所管する情報セキュリティ管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

ア　所管する情報システムに、コンピュータウイルス等の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。

イ　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

ウ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

エ　インターネットに接続していない情報システムにおいて、外部記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市又は医療センターが管理し許可されている媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵

入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報セキュリティ管理者が許可した職員を除く職員等に当該権限を付与してはならない。

(3) 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。

ア　パソコン等の端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

エ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN接続系に取り込む場合は無害化しなければならない。

オ　他の情報システムで作成又は入手したファイルは、原則、医療情報システム接続系には取り込まない。ただし、業務の都合上、必要であると判断された場合は必要最小限とし、ファイルは無害化又は不正プログラム対策ソフトウェアでチェックを行い、安全が確認されたものを取り込むことができるものとする。

カ　統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

キ　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、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。

(4) 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるように努めるものとする。

5　不正アクセス対策

(1) 統括情報セキュリティ責任者の措置事項

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

ア　使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて、機能を削除又は停止しなければならない。

ウ　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出するよう設定しなければならない。

エ　重要な情報システムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ　統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

カ　医療センターが定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

キ　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

ク　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、医療センターが定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

(2) 攻撃への対処

最高情報セキュリティ責任者及び最高情報セキュリティ副責任者並びに統括情報セキュリティ責任者は、情報システムに攻撃を受けた場合又は攻撃を受けるリスクがあることが明確になった場合、情報システムの停止を含む必要な措置を講じなければならない。また、関係機関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

最高情報セキュリティ責任者及び最高情報セキュリティ副責任者並びに統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及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

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの病院内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者及び情報セキュリティ管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する科課室等の情報セキュリティ管理者に通知し、適正に処置を講じなければならない。

(6) サービス不能攻撃

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、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

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6　セキュリティ情報の収集

(1) 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

ア　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

イ　情報セキュリティ責任者及び情報セキュリティ管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、医療センターの業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等の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) 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、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や技術環境等の変化によって新たな脅威を認識した場合は、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講じなければならない。

第１０　　運用

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

ア　統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

イ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により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。

ウ　統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

(2) 情報システムの監視機能

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

イ　情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

(3) 情報システムの監視

ア　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、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監視しなければならない。

イ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、重要なログ等を取得する情報システムの正確な時刻設定及び情報システム間の時刻同期ができる措置を講じなければならない。

ウ　統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、利用するクラウドサービスで使用する時刻の同期について適切になされているのか確認しなければならない。

エ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

オ　統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

カ　統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

キ　統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

(ｱ) サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

(ｲ) クラウドサービス利用の終了手順

(ｳ) バックアップ及び復旧

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

ア　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシー

の遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者及び最高情報セキュリティ副責任者並び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。

イ　最高情報セキュリティ責任者は、発生した問題について、適正かつ速やかに対処しなければならない。

ウ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

(2) パソコン等の端末及び電磁的記録媒体等の利用状況調査

最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 職員等の報告義務

ア　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

イ　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責任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。

3　侵害時の対応等

(1) 緊急時対応計画の策定

ア　最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

イ　統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時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、以下の内容を定めなければならない。

ア　発生した事案に応じた報告先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

(3) 業務継続計画との整合性確保

医療センターが自然災害等に備えて業務継続計画を策定した場合、最高情報セキュリティ責任者又は情報セキュリティ委員会は当該計画と情報セキュリティポリシー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

最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

4　例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、病院事務等の適正な遂行を継続するため、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合理的な理由がある場合には、最高情報セキュリティ責任者の許可を得て、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は、病院事務等の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに最高情報セキュリティ責任者に報告しなければならない。

(3) 例外措置の申請書の管理

最高情報セキュリティ責任者は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

5　法令遵守

(1) 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を遵守し、これに従わなければならない。

ア　地方公務員法(昭和 25 年　法律第 261 号)

イ　著作権法（昭和 45 年　法律第 48 号)

ウ　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)

エ　個人情報の保護に関する法律（平成 15 年　法律第 57 号)

オ　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)

カ　サイバーセキュリティ基本法（平成 26 年　法律第 104 号)

キ　川口市個人情報の保護に関する条例（令和 4 年　条例第 45 号)

(2) 統括情報セキュリティ責任者、情報セキュリティ責任者及び情報セキュリティ管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引

き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

6　違反に対する対応

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。

ア　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する科課室等の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。

イ　情報システムを所管する情報セキュリティ管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する科課室等の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。

ウ　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者及び当該職員等が所属する科課室等の情報セキュリティ管理者に通知しなければならない。

第１１　業務委託とクラウドサービスの利用

1　業務委託

(1) 委託事業者の選定基準

ア　情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

イ　情報セキュリティ管理者は、個人番号利用事務等の全部又は一部を委託する場合には、外部委託事業者（委託の要素を含む賃貸借・修繕等についても同じ）において、番号法に基づく安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。

ウ　情報セキュリティ管理者は、自治体機密性２以上の情報資産を取り扱う業務を委託する場合には、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定するよう努めるものとする。

(2) 業務委託実施前の対策

ア　情報セキュリティ管理者は、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（契約項目）

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・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遵守
・委託事業者の責任者、委託内容、作業者、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
・委託事業者にアクセスを許可する情報の種類と範囲、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
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・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還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市又は医療センターによる監査、検査（委託内容に応じた情報セキュリティ対策確保のための実地調査を含む。）
・市又は医療センター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規定(損害賠償等)
・特定個人情報の持ち出しの原則禁止

(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）の締結等

イ　情報セキュリティ管理者は、業務委託の実施までに、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) 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結等

(3) 業務委託実施期間中の対策

ア　情報セキュリティ管理者は、委託事業者において十分なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、契約に基づき改善要求等の措置を実施しなければならない。

イ　情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に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) 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な報告

(ｳ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 再委託の承認

情報セキュリティ管理者は、個人番号利用事務等の全部又は一部の業務を委託した委託事業者が再委託等をする場合、業務で取り扱う個人情報等が適切に取り扱われることを確

認した上で、再委託の諾否を判断しなければならない。

(5) 業務委託終了時の対策

ア　情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

(ｱ) 業務委託の実施期間を通じて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) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

イ　情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

(ｱ) 業務委託の実施期間を通じて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) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

2　情報システムの構築を業務委託する場合の対策

情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に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) 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、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ための要件について、契約に基づき、委託事業者に実施を求めなければならない。

(2) 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

4　医療センター向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

(1) 情報セキュリティ管理者は、外部の一般の者が医療センター向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

(2) 情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

(3) 情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

5　クラウドサービスの利用（自治体機密性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定の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービスの選定に関する規定を整備すること。

ア　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「クラウドサービス利用判断基準」という。）

イ　クラウドサービス提供者の選定基準

ウ　ネットワーク利用申請の許可権限者とクラウドサービスの利用手続

エ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(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、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

ア　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や責任分界点に係る考え方等を踏まえ、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を運用規程として整備しなければならない。

イ　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や責任分界点に係る考え方を踏まえ、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を運用規程として整備しなければならない。

ウ　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や責任分界点に係る考え方を踏まえ、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を運用規程として整備しなければならない。

(ｱ) クラウドサービスの利用終了時における対策

(ｲ) クラウドサービスで取り扱った情報の廃棄

(ｳ) クラウドサービスの利用のために作成したアカウントの廃棄

(3) クラウドサービスの選定

ア　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従ってクラウドサービスの利用を検討すること。

イ　情報セキュリティ責任者は、クラウドサービスの利用を検討している場合は、統括情報セキュリティ責任者に助言を求めること。

ウ　情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、次項の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めること。

エ　情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の

提供を求め、その内容を確認し、利用するクラウドサービスが、医療センターが定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。

(ｱ) クラウドサービスの利用を通じて医療センターが取り扱う情報のクラウドサービス提供者におけ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実施内容及び管理体制

(ｳ) クラウドサービスの提供にあたり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、医療センターの意図しない変更が加えられないための管理体制

(ｴ) クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

(ｵ) 情報セキュリティインシデントへの対処方法

(ｶ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(ｷ) 情報セキュリティ対策の履行が不十分な場合の対処方法

オ　情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めること。

カ　情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

キ　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医療センターが取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めること。

※クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が医療センターにおいて受容可能か判断すること。

(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

ク　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医療センター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、必要に応じて医療センター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ること。

ケ　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は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を医療センターに提供し、医療センターの承認を受けるよう、クラウドサ

ービス提供者の選定条件に含めること。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の可否を判断すること。

コ　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セキュリティ要件を定め、クラウドサービスを選定すること。なお、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めることが望ましい。

サ　情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、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般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

(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が保存される国・地域及び廃棄の方法

(ｳ) クラウドサービスに求めるサービスレベル

シ　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の内容、各種の認定・認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

(4) クラウドサービスの利用に係る調達・契約

ア　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は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

イ　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は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

(5) クラウドサービスのネットワーク利用承認

ア　情報セキュリティ責任者は、医療センターのネットワークを利用してクラウドサービスを利用する場合には、統括情報セキュリティ責任者へネットワーク利用申請を行うこと。また、独自で調達したネットワークでクラウドサービスを利用する場合には、統括情報セキュリティ責任者に報告すること。

イ　統括情報セキュリティ責任者は、ネットワーク利用申請を審査し、利用の可否を決定すること。

ウ　統括情報セキュリティ責任者は、ネットワーク利用申請を承認した場合は、利用するクラウドサービス及びクラウドサービス管理者を記録すること。(クラウドサービスを利用する場合も同様の措置を行う。)

(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

ア　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や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

(ｱ) 不正なアクセスを防止するためのアクセス制御

(ｲ) 取り扱う情報の機密性保護のための暗号化

(ｳ) 開発時におけるセキュリティ対策

(ｴ) 設計・設定時の誤りの防止

(ｵ) クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

イ　クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

ウ　クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

エ　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、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。

オ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

(ｱ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(ｲ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

カ　クラウドサービス管理者は、前各項において定める規定に対し、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

ア　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や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

(ｱ) クラウドサービス利用方針の規定

(ｲ) クラウドサービス利用に必要な教育

(ｳ) 取り扱う資産の管理

(ｴ) 不正アクセスを防止するためのアクセス制御

(ｵ) 取り扱う情報の機密性保護のための暗号化

(ｶ) クラウドサービス内の通信の制御

(ｷ) 設計・設定時の誤りの防止

(ｸ) クラウドサービスを利用した情報システムの事業継続

(ｹ) 設計・設定変更時の情報や変更履歴の管理

イ　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、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。

ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新た

な脅威の出現、運用、監視等の状況により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。

エ　情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、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処手順を整備すること。

オ　クラウドサービス管理者は、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・記録すること。

カ　クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

(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

ア　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や責任分界点に係る考え方を踏まえ、以下を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を規定すること。

(ｱ) クラウドサービスの利用終了時における対策

(ｲ) クラウドサービスで取り扱った情報の廃棄

(ｳ) クラウドサービスの利用のために作成したアカウントの廃棄

イ　クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録すること。

ウ　クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（利用者情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

エ　情報セキュリティ責任者は、クラウドサービスを更改・廃棄する場合は、統括情報セキュリティ責任者に報告すること。

オ　統括情報セキュリティ責任者は、報告された内容を記録すること。

6　クラウドサービスの利用（自治体機密性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定の整備

統括情報セキュリティ責任者は、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

ア　クラウドサービスを利用可能な業務の範囲

イ　クラウドサービスの利用申請の許可権限者と利用手続

ウ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

エ　クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

ア　情報セキュリティ責任者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、統括情報セキュリティ責任者

に自治体機密性２以上の情報を取り扱わない場合のネットワーク利用申請を行うこと。また、承認時に指名されたクラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講ずること。

イ　統括情報セキュリティ責任者は、情報セキュリティ責任者によるクラウドサービスのネットワーク利用申請を審査し、利用の可否を決定すること。また、ネットワーク利用申請を承認したクラウドサービス及びクラウドサービス管理者を記録すること。

第１２　評価・見直し

１　監査

(1) 実施方法

最高情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、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せなければならない。

(2) 監査を行う者の要件

ア　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ　監査を行う者は、監査及び情報セキュリティ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

ア　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、最高情報セキュリティ責任者の承認を得なければならない。

イ　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

ア　事業者に業務委託を行っている場合、情報セキュリティ管理者は委託事業者（再委託事業者等を含む。）に対して、必要なセキュリティ対策及び情報セキュリティポリシーの遵守について、定期的に又は必要に応じて監査を実施しなければならない。

イ　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(5) 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、最高情報セキュリティ責任者に報告する。また、必要に応じて情報セキュリティ委員会に報告する。

(6) 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(7) 監査結果への対応

最高情報セキュリティ責任者は、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に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、病院内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

最高情報セキュリティ責任者又は情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

2　自己点検

(1) 実施方法

ア　統括情報セキュリティ責任者及び情報セキュリティ管理者は、所管するネットワーク及び情報システム資産に係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自己点検を実施しなければならない。

イ　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て、所管する部局における情報セキュリティポリシーに沿った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自己点検を行わなければならない。

(2) 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、自己点検結果と自己点検結果に基づく改善策を取りまとめ、最高情報セキュリティ責任者に報告する。また、必要に応じて情報セキュリティ委員会に報告する。

(3) 自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　最高情報セキュリティ責任者又は情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3　情報セキュリティポリシー及び関係規程等の見直し

(1) 最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について定期的及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、その改定を行うものとする。ただし、緊急を要する場合又は軽微な改定については、最高情報セキュリティ責任者の判断で改定を行い、事後速やかに情報セキュリティ委員会委員に報告するものとする。

(2) 情報セキュリティポリシー及び関係規程等の見直しにあたっては、以下に掲げるガイド

ライン等に基づき行うものとする。

・川口市情報セキュリティ基本方針及び川口市情報セキュリティ対策基準
・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）

附　則

川口市立医療センター情報セキュリティ対策基準は、平成 23 年 4 月 1 日から施行する。

附　則

川口市立医療センター情報セキュリティ対策基準は、令和 2 年 6 月 1 日から施行する。

附　則

川口市立医療センター情報セキュリティ対策基準は、令和 4 年 4 月 1 日から施行する。

附　則

川口市立医療センター情報セキュリティ対策基準は、令和 8 年 4 月 1 日から施行する。