川口市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　対象範囲

１　この対策基準が適用される行政機関は、川口市病院事業（医局は除く）（以下、「本事業」という。）とする。

２　この対策基準が対象とする資産（以下「対象資産）という。）は、次のとおりとする。

(1) 本事業に供するネットワーク（以下「ネットワーク」という。）及びこれに関する設備

(2) 本事業に供する情報システム（以下「情報システム」という。）及びこれに関する設備

(3) 本事業に供する情報資産（以下「情報資産」という。）

第３　組織体制

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

病院事業管理者を、最高情報セキュリティ責任者とする。最高情報セキュリティ責任者は、本事業における全ての対象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　統括情報セキュリティ責任者

(1) 事務局長を、最高情報セキュリティ責任者直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は最高情報セキュリティ責任者を補佐しなければならない。

(2) 統括情報セキュリティ責任者は、本事業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) 統括情報セキュリティ責任者は、本事業の全てのネットワーク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。

(4) 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) 統括情報セキュリティ責任者は、本事業の対象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) 統括情報セキュリティ責任者は、本事業の共通的な対象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) 統括情報セキュリティ責任者は、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、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) 統括情報セキュリティ責任者は、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) 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病院総務課長に処理させることができる。

3　情報セキュリティ責任者

(1) 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)、薬剤部の長、看護部の長及び診療所の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、当該部局等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。また、当該部局等の情報セキュリティ実施手順を作成しなければならない。なお、作成にあたっては、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ない。

(3) 情報セキュリティ責任者は、その所管する局、科(室)、部、センター、診療所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。

(4) 情報セキュリティ責任者は、その所管する局、科(室)、部、センター、診療所において所有している情報システムについて、緊急時等における連絡体制の整備、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職員、非常勤職員及び臨時職員（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。

4　情報セキュリティ管理者

(1) 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看護師長及び各診療所の長が指定する本事業の職員を、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その所管する事務局の課、診療局の科室、特殊診療局のセンター、薬剤部、看護部及び診療所（以下、「科課室等」という。）の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、情報セキュリティ責任者の指示に従い、所管する対象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。

(4) 情報セキュリティ管理者は、その所管する科課室等において、対象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) 情報セキュリティ管理者は、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。

(6) 情報セキュリティ管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

5　情報セキュリティ担当者

(1) 情報セキュリティ担当者は、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らなければならない。

(2) 情報セキュリティ担当者には、情報セキュリティ管理者が指定する本事業の職員をもって充てる。

6　川口市立医療センター情報セキュリティ委員会（経営会議）

本事業の情報セキュリティ対策を統一的に実施するため、川口市立医療センター情報セキュリティ委員会（以下「情報セキュリティ委員会」という。）において、本対策基準等、情報セキュリティに関する重要な事項を決定する。

7　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) 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

8 情報セキュリティに関する統一的な窓口の設置

(1) 最高情報セキュリティ責任者は、情報セキュリティの事件・事故等の情報セキュリティインシデント（以下「情報セキュリティインシデント」という。）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科課室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する。

(2) 情報セキュリティに関する統一的な窓口は、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、その内容を関係科課室等に提供する。

(3) 情報セキュリティに関する統一的な窓口は、情報セキュリティに関して、外部の事業者等との情報共有を行うこと。

第４　情報資産の分類と管理

１　情報資産の分類

本事業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。

(1) 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	・川口市情報公開条例第７条に規定する非公開情報のうち、特定の職員等又は組織等、業務上必要とする最小限の者のみが扱う情報 ・特定個人情報	機密性２に掲げる対策の他、以下に掲げる事項 ・暗号化又はパスワード設定 特定個人情報においては、上記に掲げる対策の他、以下に掲げる事項 ・法令で定める以外の事務での取扱いの禁止 ・インターネットに接続したコンピュータへの作成・保管・複製の禁止
機密性２	川口市情報公開条例第７条に規定する非公開情報のうち、上記以外の情報資産	・許可された者以外による閲覧の制限 ・適正なネットワーク回線の選択 ・必要以上の複製及び配付禁止 ・情報資産の送信・運搬・提供時における暗号化又はパスワード設定、鍵付きケースへの格納等 ・外部記録媒体の施錠可能な場所への保管 ・復元不可能な処理を施しての廃棄
機密性１	上記以外の情報資産	

(2) 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	改ざん、誤びゅう又は破損により、個人又は法人の権利が侵害される、又は病院事業事務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	・許可された者以外による編集の制限 ・バックアップの作成、保管 ・外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所への保管
完全性１	上記以外の情報資産	

(3) 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 2	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、個人又は法人の権利が侵害される、又は病院事業事務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	・サーバやネットワーク等の冗長化 ・バックアップの作成、保管及び相当時間以内の復旧 ・外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所への保管
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。

(2) 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、当該情報を分類しなければならない。

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。

(3) 情報資産の入手

ア　川口市立医療センター（以下、「医療センター」という。）及び診療所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　医療センター及び診療所外の者が作成した情報資産を入手した者は、1 の分類に基づいた取扱いをしなければならない。

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。

(4) 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。

(5) 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、機密性 2 以上、完全性 2 又は可用性 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。

(6) 情報資産の運搬

ア　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。

イ　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、暗号化又はパスワードを設定する等、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。

(7) 情報資産の提供又は公表

ア　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。

イ　機密性 2 以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

(8) 情報資産の廃棄

ア　機密性 2 以上の情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、原則として物理的又は磁気的破壊を実施することにより、情報を復元できないように処置した上で廃棄しなければならない。

イ　機密性 2 以上の情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

ウ　機密性 2 以上の情報資産の廃棄を行う者は、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。

第５ 物理的セキュリティ

１　サーバ等の管理

(1) 機器の取付け

情報システムを所管する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、ネットワークの接続口（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施さなければならない。

(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外部の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、外部の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他、秘密保持体制の確認等を行わなければならない。

(6) 敷地外への機器の設置

情報セキュリティ管理者は、医療センター及び診療所の敷地外に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

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。

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、当該機器等の管理並びに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すべ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、機器等及び電磁的記録媒体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、ＩＣカード、指紋認証等の生体認証又は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、入室許可証及び身分証明書等を見やすい位置に着用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。

(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、情報システム室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、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責任者は、本事業及び本市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。

(3) 統括情報セキュリティ責任者は、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。

(4) 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。

4　職員等のパソコン等の管理

(1) 情報セキュリティ管理者は、執務室等のパソコン等の端末について、盗難防止のため、執務室の施錠等による措置を講じなければならない。

(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パスワードの入力を必要とするように設定しなければならない。

第６　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、情報セキュリティに関する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報告し、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、原則として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　パソコン等の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) 職員等は、本事業のパソコン等の端末、電磁的記録媒体、情報資産及びソフトウェア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。

(ｲ) 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。

(ｳ) 職員等は、外部で情報処理作業を行う際、支給以外のパソコン等の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、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。

エ　支給以外のパソコン等の端末及び電磁的記録媒体等の業務利用

職員等は、支給以外のパソコン等の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、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

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、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　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の端末のソフトウェア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

職員等は、パソコン等の端末、電磁的記録媒体及び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、離席時のパソコン等のロックや電磁的記録媒体、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、利用していた対象資産を、情報セキュリティ管理者に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) 非常勤及び臨時職員への対応

情報セキュリティ管理者は、非常勤及び臨時職員に対し、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。

(3) 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・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、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

最高情報セキュリティ責任者は、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) 研修計画の立案及び実施

ア　病院総務課長は、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、情報セキュリティに関する理解度等に応じたものにしなければならない。

エ　病院総務課長は、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、必要に応じて情報セキュリティ委員会に報告しなければならない。

(3) 緊急時対応訓練

最高情報セキュリティ責任者は、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、ネットワーク及び情報システムの規模等を考慮し、訓練実施の範囲等を定め、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及び対処

(1) 情報セキュリティインシデントの報告

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) 情報セキュリティインシデントの対処

情報セキュリティ管理者は、報告のあった事故等について、川口市医療センター情報セキュリティ緊急時対応計画（以下、「緊急時対応計画」という。）に従い適正に対処しなければならない。

4　ＩＤ及びパスワード等の管理

(1) ＩＤの取扱い

職員等は、自己が管理又は利用しているＩＤを、他人に利用させてはならない。また、共用ＩＤを管理又は利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

(2) 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間で、同一のパスワードを用いてはならない。
カ　仮のパスワードは、最初のログイン時点で変更しなければならない。
キ　パソコン等の端末のパスワードの記憶機能を利用してはならない。
ク　職員等間でパスワードを共有してはならない。ただし共有ＩＤに対するパスワードは除く。

第7　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

ア 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。

イ 情報セキュリティ管理者は、科課室等内の特定の職員等しか取扱えない情報資産がある場合は、別領域を作成しアクセス制御の措置を講じ、同一科課室等内であっても、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。

(2) バックアップの実施

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、必要に応じて情報資産のバックアップを実施しなければならない。

(3) 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及び情報資産を交換する場合、その取扱いに関する事項をあらかじめ定め、最高情報セキュリティ責任者の許可を得なければならない。

(4) 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　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、窃取、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。

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、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。

(5) 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、業務上必要とする者以外の閲覧若しくは紛失等がないよう、適正に管理しなければならない。

(6) 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、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

(7) 障害記録

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。

(8) 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。

(9) 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。

(10) 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、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、ウェブサーバ等の情報システムをインターネットに公開する場合、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うえ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、対象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。

(11) 無線 LAN 及びネットワークの盗聴対策

ア　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づけなければならない。

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

(12) 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、暗号化又はパスワード設定等、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。

(13) 無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコン等の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。

ウ　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。

(14) 機器構成の変更の制限

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。ただし、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の許可を得て、これを行うことができる。

(15) 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パソコン等の端末をネットワークに接続してはならない。

2　アクセス制御

(1) アクセス制御

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、システム上制限しなければならない。

イ　利用者ＩＤ等の取扱い

(ｱ) 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等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又は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等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。

ウ　特権を付与されたＩＤ等の管理等

(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等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管理者権限等の特権を付与されたＩＤ等を利用する者は、統括情報セキュリティ責任者若しく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、管理者権限等の特権を付与された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、管理者権限等の特権を付与されたＩＤ等について、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。

(2) 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、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。

(3) パスワードに関する情報の管理

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、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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。

(4) 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、情報システムの開発、導入、保守等の調達にあたっては、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、情報システムの調達にあたっては、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　情報システムの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、情報システムの開発の責任者及び作業者を特定しなければならない。

イ　情報システムの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、情報システムの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、情報システムの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　情報システムの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、情報システムの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、当該ソフトウェアを情報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、情報システムの開発・保守及びテスト環境から情報システムの運用環境への移行について、情報システムの開発・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。

(4) システム開発・保守に関連する資料等の保管

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。

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。

(5) 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、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。

(6) 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。

(7) 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。

(8) システム更新又は統合時の検証等

情報セキュリティ管理者は、所管する情報システムの更新・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　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。

イ　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。

ウ　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。

エ　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。

(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。

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、電磁的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、医療センターが管理し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。

(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　パソコン等の端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

エ　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。

オ　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、LAN ケーブルの即時取り外しを行う、又は直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

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。

ウ　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等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。

(2) 攻撃への対処

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、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、適正な処置を求めなければならない。

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

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。

(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。

第８　運用

１　情報システムの監視

(1) 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。

(2) 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サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

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情報システムの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、電磁的記録媒体等のログ、院内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切に対処しなければならない。

3　侵害時の対応

(1) 緊急時対応計画の策定

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対象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。

(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　関係者の連絡先

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) 事業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事業継続計画を策定する場合、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　外部委託

(1) 外部委託事業者の選定基準

ア　情報セキュリティ管理者は、外部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、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

(2) 契約項目

情報セキュリティ管理者は、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。

ア　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

イ　委託先の責任者、委託内容、作業者、作業場所の特定

ウ　提供されるサービスレベルの保証

エ　従業員に対する教育の実施

オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止

カ　業務上知り得た情報の守秘義務
キ　再委託に関する制限事項の遵守
ク　委託業務終了時の情報資産の返還、廃棄等
ケ　委託業務の定期報告及び緊急時報告義務
コ　医療センターによる監査、検査
サ　医療センターによる事故時等の公表
シ　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)

(3) 確認・措置等

情報セキュリティ管理者は、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定期的に確認し、必要に応じ、契約に基づき措置しなければならない。

5　例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、情報セキュリティポリシーを遵守することが困難な状況で、行政事務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し、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、例外措置を取ることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者は、行政事務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。

(1) 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。

(2) 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。

(3) 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９　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、情報セキュリティ対策状況について、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、情報セキュリティ委員会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

情報セキュリティ管理者は、情報セキュリティ対策を要する業務を外部委託する場合は、委託事業者及び再委託を認める場合の再委託先事業者において、必要な情報セキュリティ対策が確保されていることを確認するために、必要に応じて監査を実施しなければならない。

(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、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。

(8) 情報セキュリティ対策基準の見直し等への活用

情報セキュリティ委員会は、監査結果を本対策基準及び関係規定等の見直し、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、所管する対象資産に係る情報セキュリティ対策状況について、必要に応じ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、必要に応じ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、情報セキュリティ委員会に報告しなければならない。

(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　情報セキュリティ委員会は、この点検結果を本対策基準の見直し、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　見直し

情報セキュリティ委員会は、本対策基準について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ふまえ、必要があると認めた場合、その見直しを行うものとする。

附則（平成 23 年 3 月 31 日 川口市医療センター情報化推進会議 決定）

川口市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（令和 2 年 5 月 26 日 川口市医療センター情報化推進会議 決定）

川口市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。