茨城県立中央病院情報セキュリティ対策基準を定める要項

第１章　総則

（目的）

第１条 この要項は，茨城県情報セキュリティ基本方針を定める規程（平成２５年茨城県訓令第３号，茨城県企業局訓令第２号，茨城県病院局訓令第５号，茨城県教育委員会教育長訓令第２号，茨城県監査委員訓令第１号，茨城県人事委員会訓令第１号，茨城県労働委員会訓令第１号，県議会訓令第１号。以下「基本方針」という。）第１１条の規定に基づき，県の保有する情報資産のうち茨城県立中央病院（以下「病院」という。）の保有する情報資産の情報セキュリティ対策を実施するにあたって，具体的な遵守事項及び判断基準を定めるものである。

（用語の定義）

第２条 この要項において，次に掲げる用語の定義は，当該各号に定めるところによる。

（１）情報セキュリティポリシー 基本方針及びこの要項のことをいう。

（２）職員 茨城県立中央病院に勤務している職員をいう。

（３）脅威 基本方針第４条第１項に定める脅威をいう。

（４）リスク 脅威が実際に発生する危険性をいう。

（５）事案 脅威が実際に発生したことをいう。

（６）端末 情報システムを利用するためのコンピュータをいう。

（７）電磁的記録媒体 電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって，情報システムによる情報処理の用に供されるものに係る記録媒体をいう。

（８）複合機 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をいう。

（９）特定用途機器 ネットワークカメラシステム，テレビ会議システム及びＩＰ電話システム等の特定の用途に使用される情報システム特有の構成要素であって，通信回線に接続されている，又は内蔵電磁的記録媒体を備えている機器をいう。

(10) サーバ等 情報システムにおけるサーバ，ネットワーク装置その他の重要な機器をいう。

(11) アクセス 情報資産の情報を，参照，変更，削除又は追加することをいう。

(12) ユーザＩＤ等 利用者の識別のために利用者に与えられた記号及びこれを記録した媒体（ＩＣカード等）をいう。

(13) パスワード ユーザＩＤ等を与えられた利用者が，当該ユーザＩＤ等を利用するために，利用者自身で管理する文字列をいう。

(14) 調達 情報システムの購入，開発（変更を含む。以下同じ。）又は運用に係る契約を伴う業務において，委託，請負，賃貸借等，業務の形態を問わず，事前準備から業務の相手方との契約が成立するまでの一連の手続きのことをいう。

(15) 整備 次に掲げる手続きをいう。

ア 情報システムの開発に係る契約を伴う業務において，委託，請負，賃貸借等，業務の形態

を問わず，契約の成立から当該情報システムの運用（情報システムの変更にあたっては，変更後の運用）を開始するまでの一連の手続き

イ 情報システムの開発に係る契約を伴わない業務において，事前準備から当該情報システムの運用（情報システムの変更にあたっては，変更後の運用）を開始するまでの一連の手続き

(16) 外部委託 情報システムの開発又は運用に係る業務において，委託，請負，賃貸借等，業務の形態を問わず，当該業務の全部又は一部を，外部の事業者（以下「外部委託事業者」という。）に実施させることをいう。

第２章　組織体制

（組織体制）

第３条 病院の情報セキュリティ管理は，次の各号の組織・体制により行う。

（１）医療情報セキュリティ管理責任者

（２）医療情報セキュリティ委員会

（３）医療情報セキュリティ管理事務局

２ 前項の体制の概要は，別表第１のとおりとする。

（医療情報セキュリティ管理責任者）

第４条 医療情報セキュリティ管理責任者は，病院の情報セキュリティの統括的な権限及び責任を有する。

２　医療情報セキュリティ管理責任者は，病院長をもって充てる。

（医療情報セキュリティ委員会）

第５条　情報セキュリティの維持管理を行うため，医療情報セキュリティ委員会を設置する。

２　医療情報セキュリティ委員会は，次の各号のメンバーで構成する。

（１）委員長

（２）委員

３　医療情報セキュリティ委員会委員長は，病院長が指名する者をもって充てる。

４　委員は，委員長が指名する者をもって充てる。

５　医療情報セキュリティ委員会は，次の各号の事項を行う。

（１）この要項の改善

（２）リスク分析の指示，結果確認

（３）研修の指示，結果確認

（４）監査の指示，結果確認

（５）その他情報セキュリティに関する重要事項への対応の審議，決定

（医療情報セキュリティ管理事務局）

第６条　医療情報セキュリティ管理事務局は，病院における情報資産に対する情報セキュリティ

を統括する。
２　医療情報セキュリティ管理事務局は，次の各号のメンバーで構成する。
（１）医療情報セキュリティ管理事務局長
（２）事務局員
３　医療情報セキュリティ管理事務局長は，事務局企画情報室長をもって充てる。
４　事務局員は，企画情報室の職員をもって充てる。
５　医療情報セキュリティ管理事務局は，情報セキュリティに関する次の各号の事項を行う。
（１）情報セキュリティポリシーに基づく情報セキュリティ対策の実施
（２）情報資産の管理
（３）管理区域の区分の決定
（４）事案対応の実施及び情報セキュリティ委員会への報告
（５）重大事案の病院局への報告

第３章　情報資産の管理と分類

（情報資産の分類と管理の基準）
第７条　医療情報セキュリティ管理事務局は，情報資産を，機密性，完全性及び可用性に基づき分類，管理及び利用するための基準を作成しなければならない。
２　職員は，情報資産の分類，管理及び利用にあたって，前項の基準を遵守しなければならない。
３　医療情報セキュリティ管理事務局は，第１項の基準を，定期的に，又は必要に応じて見直さなければならない。

（管理責任）
第８条 医療情報セキュリティ管理事務局は，情報資産の管理責任を有する。
２　情報セキュリティ管理事務局は，病院の情報資産が適切に取り扱われるよう，職員に対して必要かつ適切な監督を行わなければならない。
３ 医療情報セキュリティ管理事務局は，その所管する情報資産を現に利用しておらず，将来にわたって使う見込みのない場合は，法令その他規則で保存期間が定められている場合を除き，速やかに廃棄しなければならない。また，必要以上の情報資産を保有してはならない。

（利用責任）
第９条 職員は，業務以外の目的で情報資産を利用してはならない。
２ 職員は，第７条第１項の基準に基づく情報資産の分類に応じ情報資産を適切に取り扱わなければならない。
３ 職員は，業務上不要な情報の作成，収集，複製，加工，送付，提供及び保管をしてはならない。

第４章　管理区域

（管理区域の区分）

第１０条　病院を次の各号の管理区域に区分する。

（１）セキュリティ区域 サーバ等及び別に定める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並びに機密性の高い情報を記録した文書及び電磁的記録媒体を保管する保管庫等であり，特定の職員及び外部委託事業者のみが入室可能な区域

（２）業務区域 職員が日常の業務を実施する区域であり，職員以外の第三者（県民・企業等）の入室を制限する区域

（３）共用区域 前２号以外で職員以外の第三者（県民・企業等）が入室可能な区域

（管理区域区分の決定）

第１１条 医療情報セキュリティ管理事務局は，病院における前条の管理区域の区分を決定しなければならない。

（管理区域のセキュリティ）

第１２条 医療情報セキュリティ管理事務局は，前条に基づき決定した管理区域の区分ごとに，それぞれの区分に応じた情報セキュリティ対策を実施しなければならない。

２ 医療情報セキュリティ管理事務局が管理区域ごとに遵守すべき事項は，別に定める。

第５章 情報セキュリティ管理者の遵守事項（人的セキュリティ）

（情報資産の持ち出し・持込み等の記録）

第１３条　医療情報セキュリティ管理事務局は，職員が端末等の機器（電磁的記録媒体を除く。）を，執務室外に持ち出す場合又は執務室に持ち込む場合には，その都度，目的，情報資産の内容等を確認のうえ，記録を作成し，保管しなければならない。

２　医療情報セキュリティ管理事務局は，職員が電磁的記録媒体を利用する場合には，その都度，目的，格納する情報の内容等を確認のうえ，医療情報セキュリティ管理事務局が管理する電磁的記録媒体を貸し出さなければならない。また，利用の目的が達せられたときは，職員に対して，速やかに当該電磁的記録媒体を返却させなければならない。

３　前項に規定する場合において，医療情報セキュリティ管理事務局は貸し出し及び返却の都度，その記録を作成し，保管しなければならない。

４　医療情報セキュリティ管理事務局は，第１項及び前項の記録と，所管している機器の状況が一致しているかどうか，定期的に確認しなければならない。

５　医療情報セキュリティ管理事務局は，職員が機密性の高い情報を持ち出し，又は運搬するときは，情報の暗号化等の必要な措置を講じるよう指示しなければならない。

６　医療情報セキュリティ管理事務局は，執務室の端末及び電磁的記録媒体その他機器について，ワイヤーによる固定，使用時以外の施錠保管等，盗難防止のための物理的措置を講じなければならない。

７　第１項から前項までの規程にかかわらず，医療情報セキュリティ管理事務局は，各部署に配布した電磁的記録媒体の管理について，各部署の長に委任することができる。この場合において，各部署の長は本条第２項から前項までの規程に準じて電磁的記録媒体を管理しなければな

らない。

（情報セキュリティポリシーの参照）

第１４条　医療情報セキュリティ管理事務局は，職員が常に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係規程を参照できるよう，執務室に備え置く等の措置を講じなければならない。

（非常勤職員等の遵守義務）

第１５条　医療情報セキュリティ管理事務局は，臨時職員，嘱託職員等が新たに勤務するときは，機密保持に係る事項，情報セキュリティポリシーに係る事項及び当該職員が使用する情報システムの情報セキュリティ実施手順に係る事項を説明しなければならない。

第６章 職員の遵守事項①（人的セキュリティ）

（端末等の盗難防止対策）

第１６条　職員は，執務室等に職員が不在となる場合は，執務室等の施錠等，情報資産の盗難防止のための措置を講じなければならない。

（情報セキュリティ対策の遵守義務）

第１７条 職員は，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に定められている事項を遵守しなければならない。

２ 職員は，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については，速やかに医療情報セキュリティ管理事務局に相談し，指示等を仰がなければならない。

３ 職員は，異動の場合には，利用していた情報資産を速やかに返却し，医療情報セキュリティ管理事務局の許可なく持ち出してはならない。また，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速やかに返却し，持ち出してはならない。

４ 職員は，職務上知り得た情報を漏らしてはならない。

（業務目的以外の使用の禁止）

第１８条　職員は，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。

（情報資産の持ち出し・持込み）

第１９条 職員は，病院の情報資産を執務室外に持ち出す場合は，医療情報セキュリティ管理事務局の許可を得るとともに，持ち出した情報資産を適切に管理しなければならない。

２ 職員は，情報資産を執務室に持ち込む場合（持ち出した情報資産を執務室に持ち帰る場合を含む。）は，医療情報セキュリティ管理事務局の許可を得なければならない。この場合において，職員は，持ち込んだ情報資産（文書を除く。）を情報システムへ接続するにあたって，コンピューターウイルスの感染の状況等を確認しなければならない。

３ 職員は，外部で県の情報資産を用いて情報処理業務を行う場合は，医療情報セキュリティ管理事務局の許可を得るとともに，適切な安全管理措置を実施しなければならない。
４ 職員は，前３項に係る情報資産が不要になった場合は，適切に処分しなければならない。

（私物のパソコン等を使用する場合の特例）
第２０条　職員は，病院内で業務上の情報を取り扱うために私物のパソコンを使用しようとする場合には，その機器ごとに医療情報セキュリティ管理事務局に申請し，その使用の許可を受けなければならない。
２　職員は，前項の許可を受けたパソコンについて，原則として（患者等の）個人情報を扱ってはならない。
３　第１項の許可を受けた職員は，次に掲げる事項を遵守しなければならない。
（1）パソコン（第１項の許可に係るパソコンに限る。以下同じ。）については，パスワードによるセキュリティ対策を講じること。また，パスワードは，文字数を 8 文字以上とし，他人に推測されやすい符号を避け，定期的に変更すること。
（2）パソコンには，病院が提供するウイルス対策ソフトをインストールし，定期的にパターンファイルの更新を行うこと。
４　前項の規程を順守せず，病院システム等に損害を生じさせた場合は，懲戒処分の対象となりうる。
５　院内で使用するＵＳＢメモリについては，原則として（患者等の）個人情報を扱ってはならないこと。

（私物のパソコン等で（患者等の）個人情報を取り扱う場合の特例）
第２１条 職員は，前条１項の許可を受けたパソコンについて，業務上特に個人情報を扱うことが必要な場合，医療情報セキュリティ管理事務局の許可を受けなければならない。
２　第１項の許可を受けた職員は，次に掲げる事項を遵守しなければならない。
（1）パソコン（第１項の許可に係るパソコンに限る。以下同じ。）については，病院外に持ち出してはならないこと。
（2）パソコンを使用する部屋については，職員不在時に関係者以外が立ち入りできないように必ず施錠すること。また，長時間離席する場合には，パソコンが第三者に操作されないよう画面ロックによるセキュリティ対策を講じること。
（3）パソコンについては，原則としてインターネットに接続してはならないこと。
３　前項の規程を順守せず，個人情報を紛失・漏洩した場合，懲戒処分の対象となりうる。
４　院内で使用するＵＳＢメモリについては，やむを得ず（患者等の）個人情報を取り扱う場合は，必ずパスワードロック付きのセキュリティＵＳＢメモリとすること。
５　職員は，離職時に私物パソコン等を病院外に持ち出す場合，個人情報は全て削除しなければならない。この規程を遵守せず，個人情報を紛失・漏洩した場合，当事者がその責任を負う。

（端末のセキュリティ設定変更の禁止）
第２２条　職員は，端末及びそのソフトウェアに関するセキュリティ機能の設定を医療情報セキ

ュリティ管理事務局の許可なく変更してはならない。

（机上の端末等の管理）

第２３条 職員は，使用する端末や電磁的記録媒体，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，又は許可なく情報を閲覧されることがないように，離席時の端末ロックや，容易に閲覧されない場所に配置し，又は保管する等，適切な措置を講じなければならない。

（研修の受講）

第２４条 職員は，それぞれの職務に応じ定められた研修に参加し，情報セキュリティを理解するよう努めなければならない。

（ユーザＩＤ等の管理）

第２５条 職員は，自己の管理するユーザＩＤ等に関し，次の事項を遵守しなければならない。

（１）自己が利用しているユーザＩＤ等は，他人に利用させてはならない。

（２）共用のユーザＩＤ等を利用する場合は，共用のユーザＩＤ等の利用者以外に利用させてはならない。

（パスワードの管理）

第２６条 職員は，自己の管理するパスワードについて，秘密にし，照会には一切応じないなど，適正に管理しなければならない。

２ 職員は，パスワードの管理にあたり，次の事項を遵守しなければならない。

（１）パスワードは，定期的に変更すること。また，古いパスワードの再利用は行わないこと。

（２）パスワードは，十分な長さを有し，かつ英数字及び記号を無作為に組み合わせるなどした推測され難いものとすること。

（３）パスワードのメモを情報システムの周辺に配置しないこと。また，パスワードを端末に記録しないこと。

（４）パスワードが漏えいしたおそれがある場合は，パスワードを速やかに変更するとともに，医療情報セキュリティ管理事務局に報告すること。

第７章 職員の遵守事項②（技術的セキュリティ）

（電子メールの利用制限）

第２７条 職員は，電子メールの自動転送機能を用いて，職場の電子メールを外部ネットワークに転送してはならない。

２ 職員は，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。

３ 職員は，電子メールの利用にあたって，情報資産に対する脅威を誘発する恐れのある行為をしてはならない。

（電子署名・暗号化等）

第２８条 職員は，送信する情報の完全性又は機密性を確保する必要がある場合には，医療情報セキュリティ管理事務局が別に定める電子署名方法，暗号化方法等を使用して送信しなければならない。

２ 職員は，保存する情報の機密性を確保する必要がある場合には，医療情報セキュリティ管理事務局が別に定める暗号化方法等を使用して保存しなければならない。

３ 職員は，暗号化した情報を復号化するための鍵を，医療情報セキュリティ管理事務局が別に定める方法で管理しなければならない。

（情報の著作権管理及び取扱い）

第２９条 職員は，ソフトウェアライセンスを遵守し，不正にソフトウェアのコピーを行ない，若しくは不正にコピーされたソフトウェアを使用してはならない。また，著作権を有する者の許可なく文書及び画像等の複製，加工又は転載等をしてはならない。

（無許可ソフトウェアの導入等の禁止）

第３０条 職員は，医療情報セキュリティ管理事務局に無断で，端末にソフトウェアを導入してはならない。

２ 職員は，業務上の必要により，医療情報セキュリティ管理事務局が認めるもの以外のソフトウェアを，端末へ導入しようとするときは，医療情報セキュリティ管理事務局の許可を得なければならない。

３ 医療情報セキュリティ管理事務局は，前項により導入されたソフトウェアのライセンスを適切に管理しなければならない。

（機器構成の変更の制限）

第３１条 職員は，使用する情報システムの機器の改造及び増設・交換を行ってはならない。

２ 前項の規定にかかわらず，職員は，業務を遂行するために，使用する情報システムの機器の改造及び増設・交換を行う必要がある場合は，医療情報セキュリティ管理事務局の許可を得なければならない。

３ 職員は，使用する情報システムの機器の故障等を発見した場合は，医療情報セキュリティ管理事務局に報告しなければならない。

（端末等の無許可接続の禁止）

第３２条 職員は，端末その他の機器を情報システムに接続する場合，医療情報セキュリティ管理事務局の許可を得なければならない。

（不正プログラム対策）

第３３条 職員は，医療情報セキュリティ管理事務局の指示に基づき，コンピュータウイルス等の不正プログラム対策を実施しなければならない。

２ 職員は，端末に保存されている全てのファイルに対して，定期的にコンピュータウイルス等の

不正プログラムの有無を確認しなければならない。

３ 職員は，情報及びソフトウェアを，外部から端末又はサーバ等に取り入れる場合は，コンピュータウイルス等の不正プログラムの有無を確認しなければならない。

４ 職員は，パッチやバージョンアップ等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。

第８章 情報システム管理者の遵守事項①（物理的セキュリティ）

（機器の設置等）

第３４条 医療情報セキュリティ管理事務局は，サーバ等の設置等を行う場合，転落，転倒，盗難及び無許可の移動を防ぐための対策を実施するとともに，火災，水害，埃，振動，温度，湿度等の影響をできる限り排除した場所に設置し，情報システムの安全な運用のため適切に管理しなければならない。

（電源）

第３５条 医療情報セキュリティ管理事務局は，サーバ等の電源について，停電等による電源供給の停止に備え，当該機器を適切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必要に応じて備え付けなければならない。

２ 医療情報セキュリティ管理事務局は，落雷その他電源異常等によるサーバ等の故障を防ぐために必要な対策を講じなければならない。

（配線）

第３６条 医療情報セキュリティ管理事務局は，サーバ等の電源，通信用配線及びネットワーク接続口が，第三者により無許可で追加，変更，傍受又は損傷等を受けることのないよう，必要な措置を施すとともに，配線の状況を把握し，常に適切な管理に努めなければならない。

（機器の保守，修理，廃棄及び返却）

第３７条 医療情報セキュリティ管理事務局は，サーバ等及び端末の保守，修理，廃棄及び返却に関し，次の各号の事項を遵守しなければならない。

（１）第 13 条第１項の基準に基づくサーバ等の分類に応じて定期的にサーバ等の保守を実施すること。

（２）電磁的記録媒体が含まれる機器を外部委託事業者に修理させる場合は，職員の管理のもとで実施させるか，機密性の高い情報を消去し，又は容易に読み取れない状態にして行わせること。

（３）前号の場合において，情報を消去し，又は容易に読み取れない状態にすることが難しい場合は，修理を行う外部委託事業者との間で，守秘義務に係る契約を締結すること。

（４）電磁的記録媒体が含まれる機器を交換，廃棄又は返却する場合は，全ての情報を消去し，復元不可能な状態にすること。

（複合機等のセキュリティ管理）

第３８条 医療情報セキュリティ管理事務局は，複合機及び特定用途機器（以下「複合機等」という。）を設置する場合は，当該複合機等が備える機能について適切な設定等を行わなければならない。

２ 医療情報セキュリティ管理事務局は，複合機等を外部ネットワークに接続する場合は，コンピュータウイルス等の感染，マルウェアによる不正操作又は情報漏えいの対象となるリスクを勘案して，必要な対策を講じなければならない。

３ 医療情報セキュリティ管理事務局は，複合機等を外部ネットワークに接続する場合は，前項の対策を講じるとともに，通信を行う相手先を業務の目的に必要な相手先のみに限定し，及び相手先に送信される情報が必要最少限となるようにしなければならない。

４ 医療情報セキュリティ管理事務局は，複合機等を廃棄又は返却する場合は，複合機等に保存されている全ての情報（ネットワークの設定に関する情報を含む。）を抹消し，又は再利用できない状態にしなければならない。

（サーバ等の管理）

第３９条 医療情報セキュリティ管理事務局は，サーバ等を病院以外に設置する場合（医療情報セキュリティ管理事務局が別に定める場合を除く。）は，医療情報セキュリティ委員会の承認を受けなければならない。

２ 医療情報セキュリティ管理事務局は，定期的にサーバ等の情報セキュリティ対策の状況について確認しなければならない。

（外部ネットワークとの接続）

第４０条 医療情報セキュリティ管理事務局は，所管するネットワークと外部ネットワークとの接続は必要最低限のものに限定し，できる限り接続ポイントを減らさなければならない。

２ 医療情報セキュリティ管理事務局は，所管するネットワークを外部ネットワークと接続する場合は，接続しようとする外部ネットワークのセキュリティ対策の状況を調査し，当該ネットワークを使用する全ての情報システムに影響が生じないようにしなければならない。また，各情報システムで取り扱う情報資産に係る管理の基準に応じて，必要なセキュリティ対策を講じなければならない。

３ 医療情報セキュリティ管理事務局は，外部ネットワークと接続するにあたっては，事前に医療情報セキュリティ委員会の許可を得なければならない。ただし，医療情報セキュリティ委員会が別に定める場合はこの限りでない。

４ 医療情報セキュリティ管理事務局は，接続している外部ネットワークのセキュリティに問題が認められ，情報資産に脅威が発生した場合又は発生するおそれがある場合には，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。

第９章 情報システム管理者の遵守事項②（技術的セキュリティ）

（バックアップ）

第４１条 医療情報セキュリティ管理事務局は，サーバ等に記録された情報について，冗長化措置の有無に関わらず，必要に応じて，期間を設定し定期的にバックアップをとらなければならない。

（システム運用における作業と記録）

第４２条 医療情報セキュリティ管理事務局は，所管する情報システムの運用において作業を実施する場合（外部委託事業者が作業を実施する場合を含む。）は，次の各号の事項を遵守しなければならない。

（１）作業計画書を作成のうえ，作業を実施すること。

（２）情報システムの変更等の作業を行う場合は，２名以上で作業させ，互いにその作業を確認させること。

（３）情報システムの変更等の作業を行った場合は，作業記録を作成し，適切に管理すること。

（情報システム仕様書等の管理）

第４３条 医療情報セキュリティ管理事務局は，情報システムの仕様書及びネットワーク構成図等のシステム関連文書については，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，又は紛失すること等がないよう，適切に管理しなければならない。

（アクセス記録の取得等）

第４４条 医療情報セキュリティ管理事務局は，所管する情報システムのアクセス記録その他情報セキュリティの確保に必要な記録（以下この条において「アクセス記録等」という。）について，次の各号の事項を遵守しなければならない。

（１）各種アクセス記録等を取得し，一定の期間（ただし，法令等で期間が定められている場合はその期間）保存し，必要に応じて分析すること。

（２）アクセス記録等の正確性を確保するため，正確な時刻の設定を行うこと。

（３）アクセス記録等が詐取，改ざん，消去等されないように必要な措置を講じること。

（障害記録）

第４５条 医療情報セキュリティ管理事務局は，職員からのシステム障害の報告及びその処理結果並びに問題等を，障害記録として記録し，適切に保存しなければならない。

（ネットワークの接続制御，経路制御）

第４６条 医療情報セキュリティ管理事務局は情報資産に対する不正アクセス等の脅威を防止するため，適切なアクセス制御を講じなければならない。

２ 医療情報セキュリティ管理事務局は，ネットワークにおけるアクセス制御を確実に実施するために，ファイアウォール等を設置し，適切な設定を行うなど必要な措置を講じなければならない。

（職員以外の者が利用できる情報システム）

第４７条 医療情報セキュリティ管理事務局は，職員以外の者（県民・企業等）が利用する情報システムと，職員が利用する情報システムを分離しなければならない。

（無線ＬＡＮの使用許可）

第４８条 医療情報セキュリティ管理事務局は，所管する情報システムのネットワークに無線ＬＡＮを使用する場合は，解読が困難な暗号化方法及び認証技術を使用しなければならない。

２ 医療情報セキュリティ管理事務局は，無線ＬＡＮを使用するにあたっては，事前に医療情報セキュリティ委員会の許可を得なければならない。ただし，医療情報セキュリティ委員会が別に定める場合はこの限りでない。

（ネットワークの盗聴等対策）

第４９条 医療情報セキュリティ管理事務局は，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，改ざん，なりすまし等を防ぐため，送受信する情報の暗号化，電子署名等の措置を講じなければならない。

（ネットワークの可用性対策）

第５０条 医療情報セキュリティ管理事務局は，可用性の高い情報を扱うネットワークにおいては，継続的な運用が可能な構成としなければならない。また，必要に応じて，ネットワークを冗長化する等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第５１条 医療情報セキュリティ管理事務局は，所管する情報システムの電子メールサーバ等について，情報システムの外部ネットワークから外部ネットワークへのメール転送（メールの不正中継処理）を不可能とする等，セキュリティ対策のための設定を講じなければならない。

（使用可能なソフトウェア）

第５２条 医療情報セキュリティ管理事務局は，所管する情報システムの端末に導入を認めるソフトウェアを定め，職員へ周知しなければならない。

（アクセス制御）

第５３条 医療情報セキュリティ管理事務局は，所管する情報システムに，アクセスする権限のない職員がアクセスできないよう必要な制限をしなければならない。

（利用者情報及びユーザＩＤ等の管理）

第５４条 医療情報セキュリティ管理事務局は，情報システムの利用者の登録，変更，抹消等にあたって，利用者の登録情報及びユーザＩＤ等の取扱い方法を定め，適切に管理しなければならない。

２ 医療情報セキュリティ管理事務局は，情報システムの利用者の異動及び退職等にあたって，不要になったユーザＩＤ等の抹消等の取扱い方法を定め，当該ユーザＩＤ等が放置されることが

ないよう適切に管理しなければならない。

（管理者権限）

第５５条 医療情報セキュリティ管理事務局は，情報システムの管理者権限を必要最小限の者に与え，厳重に管理しなければならない。また，管理者権限を付与された者以外が使用できないようにするために必要な措置を講じなければならない。

２ 医療情報セキュリティ管理事務局は，管理者権限を有するパスワードを初期設定のパスワード以外に変更しなければならない。

３ 医療情報セキュリティ管理事務局は，管理者権限を有するパスワードについて，パスワードの強度，変更せずに利用できる期間，入力時の試行回数の制限等のセキュリティ対策を講じなければならない。

４ 医療情報セキュリティ管理事務局は，管理者権限での情報システムへの接続時間が必要最小限となるよう設定しなければならない。

５ 医療情報セキュリティ管理事務局は，管理者権限を有するユーザＩＤ等を複数の者が共用する場合は，利用記録簿又は利用管理ができるソフトウェア等により，操作記録を作成し，保管しなければならない。

（外部からのアクセスの制限）

第５６条 医療情報セキュリティ管理事務局は，所管する情報システムに対する外部からのアクセス（以下，この条において「外部アクセス」という。）を認める場合，医療情報セキュリティ委員会の許可を得なければならない。ただし，医療情報セキュリティ委員会が別に定める場合はこの限りでない。

２ 医療情報セキュリティ管理事務局は，外部アクセスが可能な者を，外部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らい。

３ 医療情報セキュリティ管理事務局は，外部アクセスを認める場合，外部アクセスを行う利用者の本人確認を行う機能を情報システム上に確保しなければならない。

４ 医療情報セキュリティ管理事務局は，外部アクセスを認める場合，通信途上の盗聴又は不正アクセス，盗難等による情報漏えい等を防止するために，情報の暗号化，端末内で情報を保存しない仕組み等の措置を講じなければらい。

５ 医療情報セキュリティ管理事務局は，外部アクセスをした者から，外部アクセスをした旨の報告を求めるともに，外部アクセスの状況を確認し，記録しなければならない。また定期的に，又は必要に応じて，外部アクセスの状況を確認しなければならない。

（自動識別）

第５７条 医療情報セキュリティ管理事務局は，情報システムで使用されるネットワーク機器について，必要に応じて，機器固有情報によってアクセスの可否を自動的に識別する設定をしなければならない。

（ログイン手順）

第５８条 医療情報セキュリティ管理事務局は，ログイン手順中におけるメッセージ及びログイン試行回数の制限，アクセスタイムアウトの設定，ログイン・ログアウト時刻の表示等，正当なアクセス権限を持つ利用者がログインしたことを確認することができる機能を，必要に応じて導入しなければならない。

（パスワードの管理）

第５９条 医療情報セキュリティ管理事務局は，所管する情報システムに利用者がログインする場合，パスワードの入力が必要となるよう情報システムを設定しなければならない。

２ 医療情報セキュリティ管理事務局は，所管する情報システムの利用者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。

３ 医療情報セキュリティ管理事務局は，所管する情報システムの利用に必要なパスワードを発行する場合には，利用者に仮のパスワードを発行し，この仮のパスワードによる最初のログイン後直ちに，利用者がパスワードを変更しなければ，継続して利用ができないよう情報システムを設定しなければならない。

４ 医療情報セキュリティ管理事務局は，利用者がパスワードを定期的に変更しなければ，継続して利用ができないよう情報システムを設定しなければならない。

（不正アクセス対策）

第６０条 医療情報セキュリティ管理事務局は，不正アクセス対策に関し，次の各号の事項を実施しなければならない。

（１）不正アクセスを防止するために適切な措置を講ずること。

（２）情報システムが攻撃を受ける恐れがある場合には，関係機関と連絡を密にして情報の収集に努めるとともに，情報システムの停止を含む必要な措置を講ずること。

（３）情報システムが攻撃を受け，又は攻撃を受けたおそれがあり，それらの攻撃が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）に規定する不正アクセス行為に該当する可能性がある場合には，攻撃の記録を保存するとともに，医療情報セキュリティ委員会，警察及び関係機関と緊密な連携に努めること。

（情報システムの監視）

第６１条 医療情報セキュリティ管理事務局は，情報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。

第１０章 情報システムの調達，整備，運用等

（情報システムの調達及び整備）

第６２条 医療情報セキュリティ管理事務局は，情報システムの調達及び整備にあたっては，必要とする技術的なセキュリティ機能（以下「セキュリティ要件」という。）を仕様書に明記しなければならない。

２ 医療情報セキュリティ管理事務局は，機器を調達する場合は，当該機器が備えるべき機能，設

置する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，適切なセキュリティ要件を策定しなければならない。

３ 医療情報セキュリティ管理事務局は，機器及びソフトウェア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。

４ 医療情報セキュリティ管理事務局は，パッチやバージョンアップ等の開発元のサポートが終了した機器及びソフトウェアを利用してはならない。また，運用期間中に開発元のサポートが終了すると見込まれる機器及びソフトウェアを調達してはならない。ただし，開発元のサポートが終了した後の代替措置を用意可能な場合は，この限りでない。

（リスク分析）

第６３条 医療情報セキュリティ管理事務局は，情報システムの整備及び変更にあたっては，当該情報システムに対する脅威と当該情報システムの脆弱性を識別したうえで，保有する情報資産のリスクを分析及び評価し，リスクを軽減するよう情報システムを設計し，及び必要な機能を実装しなければならない。

２ 医療情報セキュリティ管理事務局は，前項における情報資産のリスクの分析及び評価に基づき，情報セキュリティ実施手順の作成及び見直しを行わなければならない。

３ 医療情報セキュリティ管理事務局は，情報セキュリティ実施手順を当該情報システムを利用する職員に提供し，その内容を周知しなければならない。

（情報システムに係る情報セキュリティの品質確保）

第６４条 医療情報セキュリティ管理事務局は，情報システムの調達及び整備にあたっては，情報システムの用途やネットワークの構成に応じて，企画，設計等の各段階における情報セキュリティに関するリスクを軽減し，品質を確保しなければならない。

（情報システムの試験）

第６５条 医療情報セキュリティ管理事務局は，情報システムの整備にあたり試験を行う場合には，試験環境とシステム運用環境の分離に努めなければならない。

２ 医療情報セキュリティ管理事務局は，情報システムの整備にあたり試験を行う場合には，既に稼働している情報システムに障害等を与えないように検討し，作業手順を明確にした上で行わなければならない。

３ 医療情報セキュリティ管理事務局は，個人情報等の機密性の高いデータを，試験データに使用してはならない。

（情報システムに関連する資料等の保管）

第６６条 医療情報セキュリティ管理事務局は，情報システムの調達，整備及び運用に関連する資料及び文書を適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性及び安全性の確保）

第６７条 医療情報セキュリティ管理事務局は，情報システムにおける入力処理，内部処理及び出

力処理の際に，データの正確性が確保されるよう，情報システムを設計しなければならない。
２ 医療情報セキュリティ管理事務局は，情報システムにおける入力処理，内部処理及び出力処理の際に，データの安全性が確保され，故意又は過失による情報の漏えい又は改ざん（いわゆるクロスサイトスクリプティング，ＳＱＬインジェクション等の脆弱性）が生じないよう情報システムを設計し，必要な機能を組み入れなければならない。

（情報システムの履歴管理）
第６８条 医療情報セキュリティ管理事務局は，情報システムを追加，変更，廃棄等した場合，追加，変更，廃棄等の履歴を記録し，保管しなければならない。

（ソフトウェアの保守及び更新）
第６９条 医療情報セキュリティ管理事務局は，ソフトウェアの保守及び更新に関し，次の各号の事項を遵守しなければならない。
（１）ソフトウェアを更新する場合は，他の情報システムとの整合性の確認を行い，計画的に実施しなければならない。
（２）情報セキュリティに重大な影響を及ぼすソフトウェアの脆弱性に対する修正プログラムについては，速やかに適用することとし，その他のソフトウェアの更新等については，計画的に実施しなければならない。

（情報システムの不正プログラム対策）
第７０条 医療情報セキュリティ管理事務局は，所管する情報システムのサーバ等及び端末に，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。また，不正プログラム対策ソフトウェアを常に最新の状態にしておかねばならない。
２ 医療情報セキュリティ管理事務局は，サーバ等及び端末に保存されている全てのファイルに対して，定期的に不正プログラムの有無を確認しなければならない。
３ 医療情報セキュリティ管理事務局は，情報システムの利用者に対し，不正プログラムに関する情報を提供しなければならない。

（システム更新又は統合時の検証等）
第７１条 医療情報セキュリティ管理事務局は，情報システムの更新及び統合を実施する場合には，更新及び統合に伴うリスクに対する管理体制の構築，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事前に行わなければならない。

第１１章 外部委託

（情報システムの調達時の措置）
第７２条　医療情報セキュリティ管理事務局は，所管する情報システムに係る調達をしようとする場合，調達先の事業者に対して，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に関する事項のうち，当該事業者が遵守すべき事項を書面にて説明し，その記録を残さなけれ

ばならない。また，医療情報セキュリティ管理事務局は，業務上の必要があって機密性の高い情報を調達先の事業者に，開示する場合は，あらかじめ，当該情報に関する守秘義務及び業務上の目的以外での当該情報の使用禁止を含む書面を相手側と取り交わさなければならない。

（業務責任者等の提出）

第７３条　医療情報セキュリティ管理事務局は，所管する情報システムの外部委託をする場合には，外部委託事業者に，当該業務の責任者及び従事者を記載した書面をあらかじめ提出させなければならない。

２　医療情報セキュリティ管理事務局は，所管する情報システムの外部委託事業者に対し，情報システムのユーザＩＤ等を交付する必要がある場合には，必要最小限のアクセス権限を付与した専用のユーザＩＤ等を交付し，管理しなければならない。また，委託業務が終了するなどし，ユーザＩＤ等が不要になった場合には，速やかに該当するユーザＩＤ等を抹消しなければならない。

（情報システムの整備等に用いるソフトウェア等の管理）

第７４条　医療情報セキュリティ管理事務局は，所管する情報システムの外部委託にあたり，外部委託事業者が使用する機器及びソフトウェアを記載した書面をあらかじめ提出させ，その必要性を確認しなければならない。

２　医療情報セキュリティ管理事務局は，外部委託事業者が使用する機器に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ことを確認した場合は，直ちに削除させなければならない。

（調達先の情報セキュリティ対策）

第７５条　医療情報セキュリティ管理事務局は，情報システムに係る調達をしようとする場合，調達の相手先となる事業者の選定にあたり，調達内容に応じた情報セキュリティ対策を実施していることを，当該事業者における情報セキュリティマネジメントシステム及び個人情報保護マネジメントシステム等の認証の取得の状況並びに開発環境，設備，技術水準，従業員に対する監督・教育，経営の状況等により確認しなければならない。

（契約の締結）

第７６条　医療情報セキュリティ管理事務局は，所管する情報システムに関する業務を外部委託する場合には，外部委託事業者との間で，必要に応じて次の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。

（１）情報セキュリティポリシー，情報セキュリティ実施手順その他関係法令等の遵守

（２）外部委託事業者における責任者，委託内容，作業者，作業場所の特定

（３）外部委託事業者が提供するサービスレベルの保証

（４）従業員に対する監督・教育の実施

（５）外部委託事業者に提供する情報の種類及び範囲並びに提供された情報の複製・複写の制限及び適切な管理

（６）外部委託事業者に提供された情報の目的外利用及び認められた者以外の者への提供の禁止並びに漏洩の防止措置の実施
（７）定められた場所以外での情報の取扱いの禁止
（８）業務上知り得た情報の守秘義務
（９）再委託の原則禁止及び再委託を承認する場合の条件等（再委託先の情報セキュリティの水準が外部委託事業者と同等以上であることの確認義務及び再委託先が業務に関して外部委託事業者と同様の義務及び責任を負うこと等））
(10) 業務終了時の情報資産の返還，廃棄等
(11) 業務の定期報告，緊急時報告及び情報セキュリティ対策の実施状況報告の義務
(12) 県による監査，検査
(13) 県による事案発生時等の公表
(14) 情報セキュリティ対策が遵守されなかった場合の損害賠償等に係る規定

（委託先管理）
第７７条　医療情報セキュリティ管理事務局は，外部委託事業者における必要な情報セキュリティ対策の実施状況について，定期的に確認しなければならない。

（外部委託事業者の電磁的記録媒体等の利用）
第７８条　医療情報セキュリティ管理事務局は，運用，保守等のため病院内に常駐している外部委託事業者と電磁的記録媒体，電子メール等の利用方法を取り決めなければならない。

（クラウドサービスの利用）
第７９条　医療情報セキュリティ管理事務局は，情報システムの調達にあたり，クラウドサービス（インターネット等のネットワークを経由して，データセンターに蓄積された情報資産をサービスとして，利用者（第三者）に提供するものをいう。以下この条及び次条において同じ。）を利用する場合は，情報の機密性に応じた情報セキュリティの水準が確保及び維持されているクラウドサービスを選択しなければならない。
２ 前項の場合において，医療情報セキュリティ管理事務局は，クラウドサービス及びクラウドサービスのデータセンターで取り扱われる情報が国内法の適用を受け，かつそのデータセンターが国内に設置されているクラウドサービス（以下この項において「国内クラウドサービス」という。）を選択するよう努めなければならない。ただし，当該クラウドサービスにおいて，機密性の高い情報を取り扱う場合には，国内クラウドサービスを選択しなければならない。

（約款による外部サービスの利用）
第８０条 医療情報セキュリティ管理事務局は，約款による外部サービス（民間事業者等が約款に基づき提供するクラウドサービスのうち，利用者が必要とする情報セキュリティに関する十分な条件設定の余地がないものをいう。以下この条において同じ。）において，　機密性の高い情報を取り扱ってはならない。
２ 約款による外部サービスの利用に関して必要な事項は，医療情報セキュリティ管理事務局が別

に定める。

第１２章 研修・啓発

（研修の計画，実施）

第８１条　医療情報セキュリティ管理事務局は，職員に対し情報セキュリティについて啓発するための研修を次により実施しなければならない。

（１）全ての職員に対する定期的な研修を実施するための研修計画を策定すること。

（２）医療情報セキュリティ管理事務局及び職員に対して，それぞれの職務及び情報セキュリティの理解度に応じた研修を実施すること。

２ 医療情報セキュリティ管理事務局は，所管する所属の職員に対し情報セキュリティに関する教育を行わなければならない。

３ 医療情報セキュリティ管理事務局は，所管する所属の職員に係る研修の参加状況について記録を作成し，保管しなければならない。

（情報セキュリティに関する情報の収集及び提供）

第８２条　医療情報セキュリティ管理事務局は，脆弱性，不正プログラム，関係法令等，情報セキュリティに関する情報を収集し，必要に応じ，その対応方法とともに関係者へ通知し，当該情報を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，セキュリティ侵害等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。

２ 医療情報セキュリティ管理事務局は，収集した情報セキュリティに関する情報について，速やかに職員へ周知するとともに，情報セキュリティ対策を実施しなければならない。

第１３章 事案対応マニュアル

（事案対応マニュアル）

第８３条　医療情報セキュリティ管理事務局は，事案が発生した場合及び発生するおそれがある場合における連絡，証拠保全，被害拡大の防止及び復旧等の必要な措置を迅速かつ適切に実施し，再発防止の措置を講じるために，事案対応マニュアルを策定しなければならない。

（マニュアルの内容）

第８４条　前条に定める事案対応マニュアル（以下「事案対応マニュアル」という。）には，次の各号に掲げる項目を定めなければならない。

（１）事案の分類

（２）管理体制

（３）連絡体制

（４）初動体制

（５）事案の対処の流れ

（６）再発防止策の策定方法

（事案対応の体制整備）

第８５条　医療情報セキュリティ管理事務局は，事案発生に備えて，所管する情報システムの関係者の連絡体制並びに開発事業者及び保守事業者等の支援が受けられる体制をあらかじめ整備しておかなければならない。

２　医療情報セキュリティ管理事務局は，事案が発生し，又は発生するおそれがある場合における職員の対応手順及び必要となる資料（機器構成表，ネットワーク構成表，バックアップ・リカバリ手順，保守体制連絡表等）をあらかじめ整備し，情報セキュリティ実施手順に規定しておかなければならない。

３ 職員は，事案が発生した場合には，事案対応マニュアル，情報セキュリティ実施手順等に定められた初動対応を実施した上で，医療情報セキュリティ委員会，医療情報セキュリティ管理責任者の指示に基づき，対処しなければならない。

（事案対応マニュアルの訓練）

第８６条　医療情報セキュリティ管理事務局は，事案対応マニュアルの円滑な実施のために，定期的に事案対応訓練を実施しなければならない。

２　医療情報セキュリティ管理事務局は，管理する情報システムの規模に応じて，定期的に事案対応訓練を実施しなければならない。

（事案に対する報告）

第８７条 職員等は，情報セキュリティに関する事案を発見した場合には，速やかに事案対応マニュアルに基づき，医療情報セキュリティ管理事務局等所定の報告先へ報告しなければならない。

２ 前項の報告を受けた医療情報セキュリティ管理事務局は，事案対応マニュアルに基づき，所定の報告先へ報告するとともに，連携して，当該事案等の分析，事案発生原因の究明，証拠保全のための記録の保存を行うほか，再発防止に向けた策を講じなければならない。

（県民等外部からの事案通報）

第８８条 職員は，本県の情報資産に関する事案について，県民等から通報を受けた場合には，事案対応マニュアルに基づき，速やかに医療情報セキュリティ管理事務局に報告するとともに，医療情報セキュリティ委員会等に報告しなければならない。

（関係法令等との整合性確保）

第８９条 事案対応マニュアルは，茨城県災害対策本部条例（昭和 38 年茨城県条例第６号）等の関係法令等との整合性を確保しなければならない。

（事案対応マニュアルの見直し）

第９０条 医療情報セキュリティ管理事務局は，事案対応マニュアルの訓練結果や，情報セキュリティを取り巻く状況の変化等をふまえ，必要に応じ，事案対応マニュアルを見直さなければな

らない。

第１４章 評価・見直し

（監査計画の策定）

第９１条　医療情報セキュリティ管理事務局は，監査を行うにあたって，監査計画を策定し，医療情報セキュリティ委員会の承認を得なければならない。

（監査の実施）

第９２条　医療情報セキュリティ管理事務局は，前条の監査計画に基づき，監査を実施しなければならない。

２　前項のほか，医療情報セキュリティ管理事務局は，必要に応じて監査を実施することができる。

３　医療情報セキュリティ管理事務局は，監査結果をとりまとめ，医療情報セキュリティ委員会に報告しなければならない。

４　医療情報セキュリティ管理事務局は，自らが行う監査のほか，医療情報セキュリティ管理事務局の承認を受けた場合に，外部の事業者による外部監査を実施することができる。

（外部委託事業者に対する監査）

第９３条 医療情報セキュリティ管理事務局は，情報システムの調達又は整備等県の情報資産に係る業務について外部委託を行っている場合は，定期的に，又は必要に応じて，外部委託事業者（再委託が行われている場合はその事業者を含む。）に対する監査を行わなければならない。

（監査への協力）

第９４条 被監査所属の職員は，監査の実施に協力しなければならない。

（監査結果への対応）

第９５条 医療情報セキュリティ委員会は，監査結果を踏まえ，指摘事項の改善を，医療情報セキュリティ管理事務局に対し指示しなければならない。

２ 医療情報セキュリティ委員会は，前項の指示に基づく指摘事項の改善状況を，医療情報セキュリティ管理事務局に確認しなければならない。

（自己点検の実施方法）

第９６条 医療情報セキュリティ管理事務局は，所管する情報システムについて，毎年度及び必要に応じ自己点検を実施しなければならない。

２ 医療情報セキュリティ管理事務局は，所管する所属における情報セキュリティポリシーに基づく情報セキュリティ対策の実施状況について，毎年度及び必要に応じ自己点検を行わなければならない。

（自己点検の報告）

第９７条 医療情報セキュリティ管理事務局は，前条の自己点検の結果及び当該結果に基づく改善策を取りまとめ，医療情報セキュリティ委員会に報告しなければならない。

（自己点検結果の活用）

第９８条 医療情報セキュリティ管理事務局は，第９６条の自己点検の結果に基づき，自己の権限の範囲内で職員への指示等を行い，改善を図らなければならない。

２ 職員は，前項の指示に従い，情報セキュリティ対策を実施しなければならない。

（情報セキュリティ対策基準の見直し）

第９９条 医療情報セキュリティ管理事務局は，監査結果，自己点検結果及び情報セキュリティに関する状況の変化等を踏まえ，毎年度及び必要に応じて情報セキュリティポリシーの実効性を評価し，必要に応じて情報セキュリティポリシー及び関係規定等を見直すとともに情報セキュリティ対策に反映させなければならない。

２ 医療情報セキュリティ管理事務局は，この要項の見直しにあたって，医療情報セキュリティ委員会の承認を得なければならない。

（情報セキュリティ実施手順の見直し）

第１００条 医療情報セキュリティ管理事務局は，所管する情報システムについて，監査結果や情報セキュリティに関する状況の変化等を踏まえ，毎年度及び必要に応じて情報セキュリティ実施手順の実効性を評価し，必要に応じて情報セキュリティ実施手順を見直すとともに，情報セキュリティ対策に反映させなければならない。

第１５章 運用

（情報セキュリティ運用計画の策定）

第１０１条　医療情報セキュリティ管理事務局は，毎年度情報セキュリティ運用計画を策定し，医療情報セキュリティ委員会の承認を得なければならない。

（ポリシーの遵守状況の確認及び対処）

第１０２条 医療情報セキュリティ管理事務局は，所管する所属又は情報システムについて，情報セキュリティポリシーの遵守状況を定期的に確認し，問題が認められた場合は，適切かつ速やかに対処するとともに，医療情報セキュリティ委員会に報告しなければならない。

（職員の報告義務）

第１０３条 職員は，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は，事案対応マニュアルに基づき，直ちに医療情報セキュリティ管理事務局等の所定の報告先に報告しなければならない。

２ 前項の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医療情報セ

キュリティ管理事務局が判断した場合は，事案対応マニュアルに従って適切に対処しなければならない。

（利用状況調査）

第１０４条 医療情報セキュリティ管理事務局は，不正アクセス，不正プログラム等の事案及び情報セキュリティポリシーの違反に関する調査のため，必要があるときは，職員が使用している端末，電磁的記録媒体等の操作記録，インターネットへのアクセス状況，電子メールの利用状況等を調査することができる。

（法令等の遵守）

第１０５条 職員は，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，別表第２に掲げる法令のほか関係法令等を遵守しなければならない。

（ポリシー違反時の処分）

第１０６条 職員は，情報セキュリティポリシーに違反した場合，適切な改善措置及び法令に定める処分の対象となる。

（情報システムの不適切な利用に対する処置）

第１０７条 医療情報セキュリティ管理事務局は，職員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，当該職員に対する指導等の適切な措置を行わなければならない。

２ 医療情報セキュリティ管理事務局は，所管する情報システムについて，情報セキュリティポリシーに違反する行動を行った職員が，前項に基づく指導等の措置にも関わらず改善を行わない場合は，医療情報セキュリティ委員会と協議のうえ，当該職員に対する情報システムの使用制限等の処置を行うことができる。

第１６章 例外措置

（例外措置の許可）

第１０８条 医療情報セキュリティ管理事務局は，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と認められる場合には，医療情報セキュリティ委員会の許可を得て，例外措置をとることができる。この場合において，医療情報セキュリティ委員会は例外措置を許可する期間を定めるものとする。

（緊急時の例外措置）

第１０９条 医療情報セキュリティ管理事務局は，業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，事後速やかに医療情報セキュリティ委員会に報告しなければならない。

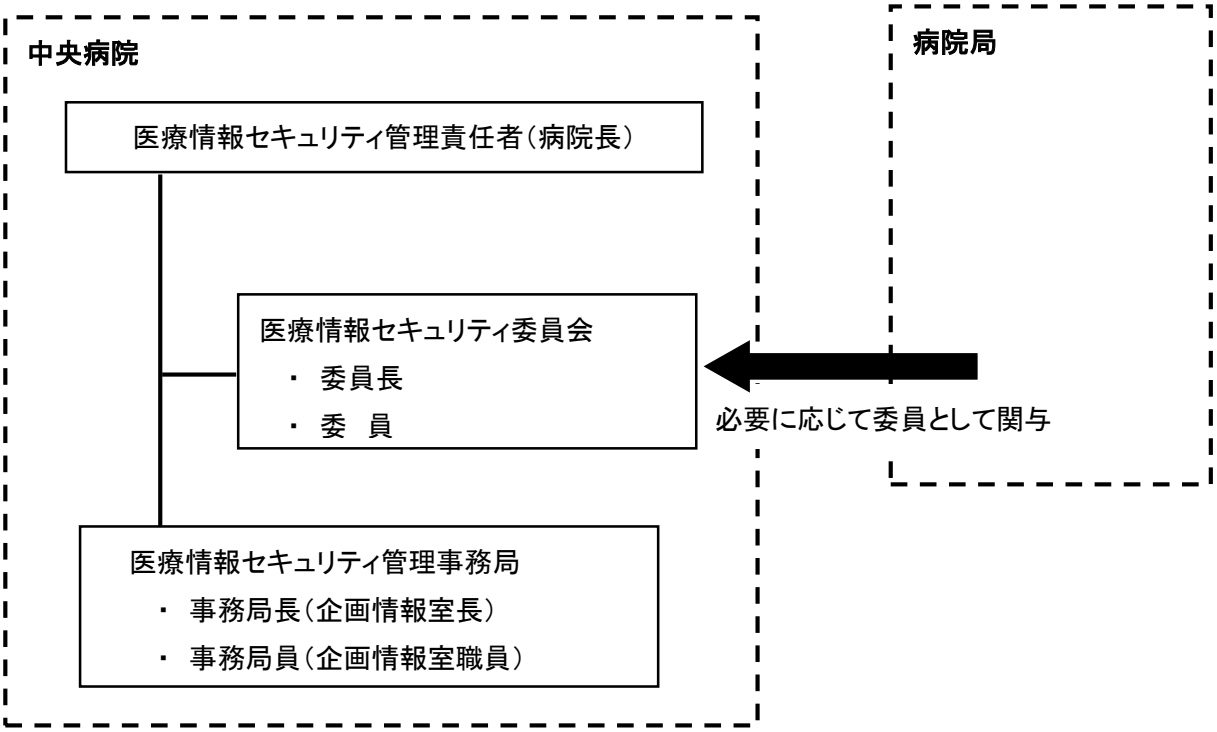
（例外措置の申請書の管理）

第１１０条 医療情報セキュリティ委員会は，例外措置の申請書及び審査結果を適切に保管しなければならない。

付則

１　この要項は，平成３０年　４月　１日から施行する。

別表第1（第 3 条関係）



別表第2（第 105 条関係）

【関連法令等一覧】

1	刑法（明治 40 年法第 45 号）
2	地方自治法（昭和 22 年法律第 67 号）
3	地方公務員法（昭和 25 年法律第 261 号）
4	著作権法（昭和 45 年法律第 48 号）
5	不正競争防止法（平成 5 年法律第 47 号）
6	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）
7	電子署名及び認証業務に関する法律(平成 12 年法律第 102 号）
8	特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号）
9	特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）
10	個人情報の保護に関する法律（平成 15 年法律第 57 号）
11	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）
12	サイバーセキュリティ基本法（平成 26 年法律第 104 号）
13	茨城県情報公開条例（平成 12 年茨城県条例第 5 号）
14	茨城県個人情報の保護に関する条例（平成 17 年茨城県条例第 1 号）
15	茨城県庁舎等管理規則（昭和 36 年茨城県規則第 74 号）
16	茨城県文書等整理保存規程（昭和 59 年茨城県訓令第 19 号）

○ 情報資産の分類，管理及び利用するための基準（第 7 条関係）

分　類	分類基準	取扱制限
最重要	個人情報及び事案が発生した場合，患者，職員，病院の運営その他社会に重大な影響を及ぼす情報で，特に厳格な取扱いが必要な情報	・原則として私物のパソコン，USB メモリでの取扱いの禁止 ・私物のパソコンで，業務上特に個人情報を扱うことが必要な場合，その機器ごとに医療情報セキュリティ管理事務局の許可を受けなければならない。 ・USB メモリで，業務上特に個人情報を扱うことが必要な場合，必ずパスワードロック付きのセキュリティUSBメモリとすること。
重　要	外部に公開することを予定していない情報及び事案が発生した場合，患者，職員，病院の運営その他社会に影響を及ぼす情報で慎重な取扱いが必要な情報	・情報資産を院外に持ち出す場合は，医療情報セキュリティ管理事務局の許可を得るとともに，持ち出した情報資産を適切に管理しなければならない。
その他	最重要又は重要の情報資産以外の情報資産	

○ 管理区域の区分とセキュリティ（第 10 条関係）

1．管理区域の区分

区　分	区　域
セキュリティ区域	サーバ室，コンピュータ室
業務区域	外来診察室，処置室，リハビリテーションセンター，透析センター，化学療法センター，人間ドック室，手術室，臨床治験管理部，薬剤局（調剤室等含む），各病棟（ナースステーション，カンファレンス室含む），内視鏡センター，医局（院長室等幹部医師室を含む），レジデントルーム，看護局，看護教育支援室，医療安全管理対策室，感染制御室，健康管理室，臨床検査科（各種検査室含む），栄養管理科，臨床工学技術科，病理検査室，放射線検査（各検査室および執務室），事務局，施設課，システム管理室
共通区域	セキュリティ区域，業務区域以外の区域

2．管理区域のセキュリティ

区　分	セキュリティ
セキュリティ区域	1）セキュリティ区域の入り口を施錠可能とすること。 2）セキュリティ区域内に耐震対策及び防火措置等災害対策を施すこと。 3）セキュリティ区域内を温度，湿度，塵芥等の影響から可能な限り排除すること。 4）セキュリティ区域への設備等の搬入搬出には職員が立ち会う等の必要な措置を施すこと。
業務区域	1）業務区域の入り口を施錠可能とすること。 2）来訪者の受付を行う受付場所を明示すること。 3）来訪者が入退室する場合に，来訪目的以外の情報資産にアクセスできないよう配慮すること。
共通区域	職員等は，職員等以外に利用を許可していない情報システムを構成する設備を共用区域に放置してはならない。