医療病院社団慈恵会　新須磨病院
情報セキュリティポリシー・
対策手順

【第５版】

制定日：平成１７年４月１日
（最終改定日：令和5年４月１日）

目　次

第1章 情報セキュリティポリシー

1 基本的な考え方

情報セキュリティ基本方針は、医療病院社団慈恵会　新須磨病院（以下「当院」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、当院が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 適応の範囲

対象者

（1） 役職者、及び職員、契約職員及び派遣・嘱託職員、パート・アルバイト等の全ての従業員（以下、「職員」という）

（2） 当院の情報資産を使用し業務が行われている取引先、業務委託先及びその従業員。

対象範囲

職員が業務で使用するすべての情報資産を対象とし、事業・組織・物理的及びネットワーク範囲は、当院が保有するすべての情報資産に関連する範囲とする。

3 定義

この情報セキュリティポリシーにおいて、次に掲げる用語の意義は、当該各号に定めるところによる。

（1） 情報資産

当院にとって価値を持つ情報及びその情報を利用可能とする手段（ハードウエア、ソフトウェア、サービス等）

（2） ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（3） 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みのことで、当院の所有であるかを問わず、当院の所掌する業務に使用するものすべてをいう。

（4） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（5） 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

（6） 機密性　※1

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（7） 完全性　※2

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（8） 可用性　※3

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

4 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（4） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

5 職員の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6 情報セキュリティ対策

上記4の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1） 組織体制

当院の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（2） 情報資産の分類と管理

当院の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3） 人的セキュリティ対策

情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（4） 物理的セキュリティ対策

サーバ、情報システム室、通信回線及びパソコン等のハードウェアの管理について、可能な範囲で物理的な対策を講じる。

（5） 技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（6） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（7） 外部サービスの利用

外部委託や約款による外部サービス、ソーシャルメディアサービスを利用する場合は、外部事業者等において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

（8） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

上記5、6及び7に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を本書とは別に策定するものとする。

なお、情報セキュリティ実施手順は、公にすることに病院運営に重大な支障を及ぼすおそれがあることから非公開とする。

第2章 情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針を実行に移すための、当院における情報資産に関する情報セキュリティ対策の基準を定めたものである。
具体的な運用は実施手順として別に定めるものとし、対策基準と実施手順が重複する項目については実施手順が優先されるものとする。

1 組織体制

名称	対象者	役割
情報セキュリティ統括責任者	理事長	情報資産の管理及び情報セキュリティ対策の最終決定権限
情報セキュリティ副統括責任者	副院長	情報セキュリティ統括責任者の補助
情報セキュリティ管理者	所属長	副統括責任者の補助で各部署の情報セキュリティの管理者
情報セキュリティ担当者		情報セキュリティ管理者の補助
情報システム担当者/ネットワーク管理者	総務・システム担当者	情報システムのセキュリティ担当者
情報セキュリティ事務局	医療情報室	窓口等の役割
職員	職員	
監査チーム		情報セキュリティ運用上の承認・監査・審議を行う

（1）情報セキュリティ統括責任者

① 情報資産の情報セキュリティを統括する最高責任者として、情報セキュリティ統括責任者を置くこととする。尚、情報セキュリティ統括責任者は、理事長をもって充てることとする。

② 情報セキュリティ統括責任者は、当院で取扱われる情報資産を保護するための統括責任を持つとともに、その責任を果たすための全ての権限を有するものとする。

③ 情報セキュリティ統括責任者は、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」 という。）に対処するため、情報セキュリティ委員会を整備し、別に定める緊急時対応計画の中で役割を明確化しなければならない。

（2）情報セキュリティ副統括責任者

① 情報セキュリティ統括責任者を補佐するために、情報セキュリティ副統括責任者を置くこととする。尚、情報セキュリティ副統括責任者は副院長をもって充てることとする。

② 情報セキュリティ副統括責任者は、情報セキュリティ統括責任者の補佐及び、情報セキュリティ管理者を統括し、情報セキュリティ対策に関する連絡、調整を担当することとする。

③ 情報セキュリティ副統括責任者は、情報セキュリティ統括責任者が責務の遂行が困難な場合は、情報セキュリティ統括責任者の代理として、2（1）の権限を遂行することとする。

（3）情報セキュリティ管理者

① 情報セキュリティ副統括責任者を補佐するために、情報セキュリティ管理者を置くこととする。情報セキュリティ管理者は、原則として各部署の長をもって充てることとする。ただし、診療部に関しては、診療部の責任者をもって充てることとする。

② 情報セキュリティ管理者は、各部署内で取扱われる情報資産を保護するための統括責任を持つとともに、その責任を果たすための権限を有することとする。

③ 情報セキュリティ管理者は、各部署内において次の役割を担うこととする。

A) 情報セキュリティ対策の整備、運用及び管理等

B) 情報セキュリティポリシーの遵守に関し、職員に対する教育、訓練、助言及び指示

C) 情報セキュリティインシデント発生時の情報収集管理及び対応

④ 各部署の情報セキュリティ管理者の債務遂行が困難な場合は、情報セキュリティ担当者が代理者を選定し、情報セキュリティ副統括責任者へ連絡の上、部署の統括権限を委譲する。

（4）情報セキュリティ担当者

情報セキュリティ管理者の指示に従い、各部署内の情報セキュリティ対策の整備、運用及び管理等を行う担当者として、情報セキュリティ担当者を置くこととする。情報セキュリティ担当者は、各部門の情報セキュリティ管理者が指名した者をもって充てることとする。

（5）情報システム担当者/ネットワーク管理者（以下、システム担当者）

① 情報システム・ネットワークの企画、開発、導入、運用及び管理を行う者として、総務・システム部署にシステム担当者を置くこととする。

② システム担当者は、情報セキュリティ副統括責任者が指名した者をもって充てることとする。

③ システム担当者は主管する情報システム/ネットワークに関し、情報セキュリティを保護するための権限を有することとする。

④ システム担当者は、その所管する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恐れがある場合には、緊急時対応計画で定める業務改善委員会の窓口及び統括情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

（6）情報セキュリティ事務局

① 情報セキュリティ委員会の運営やその他申請の窓口として情報セキュリティ事務局を設置する。情報セキュリティ事務局は医療情報室に置くこととする。

② 情報セキュリティ事務局は情報セキュリティ副統括責任者の指示のもと会議・監査チームの招集、新入職員の教育等を行う。

（7）職員

職員は、情報セキュリティポリシー・対策基準及び情報セキュリティ実施手順のうち職員向けに定められている事項を遵守する。

（8）監査チーム

情報セキュリティ対策の実施における業務の承認、新たなシステムの導入、セキュリティレベルの変更等の作業が必要場合、監査チームにて内容の審議を行う。

チームメンバーは下記とするとする

・情報システム担当者

・情報セキュリティ事務局

・事務管理部長

※チームメンバーが監査を受ける場合は情報セキュリティ統括責任者が代替メンバーを任命する

（9）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、同じ者が兼務してならない。

（10） 情報セキュリティ委員会（以下、委員会とする）

情報セキュリティの確保、向上を統一的な視点で行うために、情報セキュリティポリシー・対策基準、情報セキュリティ実施手順等の策定及び監査など、情報セキュリティに関する重要な事項を審議する情報セキュリティ委員会を設置する。

2 情報資産の分類と管理

（1）情報資産の分類当院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、必要に応じ取扱制限を行うものとする。

区分	種別	分類基準	主な取り扱い制限
機密性 ※1	第Ⅰ種	・個人情報 ・秘密文書に相当する情報資産	・支給以外の端末での作業の禁止 ・保管場所の制限 ・保管場所への必要以上の電子的記録媒体の持ち込禁止
	第Ⅱ種	・不開示情報のうち個人情報を除くもの ・秘密文書に相当する機密性は要しないが、一般に公表することを前提としていない情報資産	
	第Ⅲ種	上記第Ⅰ種及び第Ⅱ種以外の情報資産	
完全性 ※2	第Ⅰ種	・個人情報 ・改竄又は破損により、患者等の権利（生命、財産、プライバシー）が侵害される又は業務遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	・情報資産のバックアップ ・外部で情報処理を行う際の安全管理措置の徹底 ・電磁的記録媒体の施錠可能な場所への保管
	第Ⅱ種	改竄又は破損により、業務遂行に支障を及ぼすおそれがある情報資産	
	第Ⅲ種	上記第Ⅰ種及び第Ⅱ種以外の情報資産	

可用性 ※3	第Ⅰ種	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、患者等の権利が侵害される又は当院業務の安定的な遂行に支障（軽微なものを除く。）を及ぼす情報資産	・情報資産のバックアップ ・電磁的記録媒体の施錠可能な場所への保管
	第Ⅱ種	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、当院業務の安定的な遂行に支障を及ぼす情報資産	
	第Ⅲ種	上記第Ⅰ種及び第Ⅱ種以外の情報資産	

（2）情報資産の管理

① 管理責任者及び管理方法

A) 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。

B) 情報セキュリティ管理者は、（1）の分類に基づき情報資産を管理しなければならない（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含む）。

C) 情報セキュリティ管理者は、保有する情報資産について情報資産管理台帳を作成し、当該情報資産を適切に管理しなければならない。

D) 情報は、原則として、病院配布の端末もしくは共有ファイルに保存するものとする。ただし、各業務の実態に合わせて、外部記録媒体に情報を保存することができるものとする。

E) 情報セキュリティ管理者は、分類に応じて、各々の情報にアクセスできる職員及びアクセス権限を定めるものとする。

F) 情報セキュリティ管理者は、情報システム等が取り扱う情報について、ファイル名、記録媒体の表示等から第三者が重要性の識別を容易に認識できないように、適切な管理を行うものとする。

② 情報の作成

A) 職員は、業務上必要のない情報を作成してはならない。

B) 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。

C) 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 情報資産の導入

情報セキュリティ管理者は、情報セキュリティに支障が生じる可能性のある情報資産を導入する場合は、あらかじめ情報セキュリティ統括責任者と協議しなければならない。

④ 情報資産の入手

A) 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

B) 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、当該情報分類と取扱制限を定めなければならない。

C) 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

A) 職員は、業務以外の目的に情報資産を利用してはならない。

B) 職員は、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。

C) 職員は、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

A) 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。

B) 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。

C) 情報セキュリティ管理者は、機密性の基準第Ⅰ種又は第Ⅱ種、完全性の基準第Ⅰ種又は第Ⅱ種、可用性の基準第Ⅰ種又は第Ⅱ種に該当する情報資産を保管する場合、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情報を送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑧ 情報資産の運搬

A) 車両等により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の設定を行う等、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。

B) 機密性の基準第Ⅰ種又は第Ⅱ種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。

⑨ 情報資産の提供・公表

A) 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。

B) 機密性の基準第Ⅰ種又は第Ⅱ種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。

C) 情報セキュリティ管理者は、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。

D) 情報セキュリティ管理者は、情報資産を外部に利用させる、又は提供するときは、別に定める手続によらなければならない。

⑩ 情報資産の廃棄

A) 情報資産を廃棄する者は、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、必要に応じて電磁的記録媒体の初期化等、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。

B) 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。

C) 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。

D) 情報セキュリティ管理者は、電磁的記録媒体の消去又は記録装置の破砕等を外部の者に依頼する場合は、記録の消去に係る確認書の提出を受けなければならない。

⑪ 情報資産に関する業務の委託等

情報セキュリティ管理者は、情報システムの導入もしくは保守その他情報資産に関する業務の委託又は電子計算機もしくは通信関係装置の借入れについての契約（以下「委託等契約」という。）を締結するときは、情報資産の適切な管理が行われるように委託等契約の相手方に対し必要な措置を講じなければならない。

3 人的セキュリティ対策

（1）職員の遵守事項

① 職員の順守事項

A) 情報セキュリティポリシー等の尊守

職員は、情報セキュリティポリシー・対策基準、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。

B) 業務以外の目的での使用禁止

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を行ってはならない。

職員は、業務時間中に業務以外の目的でパソコンおよびモバイル端末等からインターネットへのアクセスを行ってはならない。

C) パソコン、モバイル端末及び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

イ) 情報資産を外部で処理する場合は病院内における対策基準に加え、安全管理のための必要な措置を確認したうえで、実施手順を定めなければならない。

ロ) 職員は、病院のパソコン、モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを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。

ハ) 職員は、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

D) 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

イ) 職員は、支給以外のパソコン、モバイル端末を原則業務に利用してはならない。

ロ) 職員は、支給以外のパソコン、モバイル端末などを院内で利用する場合は情報セキュリティ統括責任者が別に定める手続きによらなければならない。

ハ) 職員は、支給以外のパソコン、モバイル端末を業務に利用する場合は情報セキュリティ統括責任者が別に定める手続きによらなければならない。

ニ) 職員は、支給以外の電磁的記録媒体を原則業務に利用してはならない。また、利用するUSBメモリは、原則、パスワード認証等の暗号化機能付きのものとしなければならない。

E) 持ち出しの記録

情報セキュリティ管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

F) パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、パソコンやモバイル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システム担当者の許可なく変更してはならない。

G) 机上の端末等の管理

職員は、パソコン、モバイル端末、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、モバイル端末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。

H) 退職時等の遵守

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

② 情報セキュリティポリシーなどの掲示

情報セキュリティ統括責任者は、職員が常に情報セキュリティポリシー・対策基準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。

③ 外部委託事業に対する説明

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・保守並びにその他情報資産に関する業務等を外部委託事業者に発注する場合、外部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外部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

① 情報セキュリティに関する研修

委員会もしくは情報セキュリティ事務局は定期的に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。

② 研修への参加

職員は、定められた研修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

委員会は情報セキュリティインシデント発生時の報告手順を定め、情報セキュリティ管理者及び情報システム担当者は、情報セキュリティインシデントが発生した場合、報告手順に従って委員会に報告を行わなければならない。

（4）ID及びパスワード等の管理

① IDの管理

職員は、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。

A) 自己が利用しているIDは、他人に利用させてはならない。

B) 共用利用する場合は、共用IDの利用者以外に利用させてはならない。

② パスワードの管理

職員は、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。

A) 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。

B) パスワードを秘密にし、第三者からのパスワードの照会等には一切応じてはならない。

C) パスワードは英数字・記号を混在させた 8 文字以上の推定困難な英数字・記号を定期的に変更しなければならない
パスワードの利用は最長 2 ヶ月以内とする。

D) 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。

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

F) 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。

G) 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。

H) 職員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）。

I) 緊急時用のID及びパスワードの利用に関しては使用者の勤務期間中のみ有効とする。

4 物理的セキュリティ対策

（1）サーバ等の管理

① 機器の取り付け

システム担当は、施設管理部門と連携し、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、可能な限り必要な措置を講じなければならない。また、パソコン等の機器を設置する場合、第三者から閲覧可能な場所にあるものはディスプレイに表示される情報が他者から覗き見されないような措置を講じなければならない。

② 機器の電源

A) システム担当者は、施設管理部門と連携し、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備え付けなければならない。

B) システム担当者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

③ 通信ケーブル等の配線

A) システム担当者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷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。

B) システム担当者は、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。

C) システム担当者は、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可能な限り対応しなければならない。

D) システム担当者は、自ら又は情報セキュリティ管理者及び契約により操作を認められた外部委託事業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。

④ 機器の定期保守及び修理

A) システム担当者は、サーバ等の機器の定期保守を実施しなければならない。

B) システム担当者は、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、情報の取り扱いに留意しなければならない。

⑤ 病院の敷地外へ機器の設定

システム担当者は、病院の施設外に業務システムのサーバ等の機器を設置する場合、委員会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。

⑥ 機器の廃棄等

システム担当者は、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（サーバ室等）の管理

① 管理区域の構造等

A) 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（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

B) システム担当者は、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、施錠管理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。

C) システム担当者は、施設管理部門と連携して、サーバ室内の機器等に、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。

D) システム担当者は、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可能な限り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

A) システム担当者は、管理区域への入退室を許可された者のみに制限し、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。

B) 職員及び外部委託事業者は、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。

C) システム担当者は、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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

D) システム担当者は、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可能な限り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

A) システム担当者は、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、あらかじめ職員又は委託した業者に確認を行わせなければならない。

B) 管理区域へ機器等の搬入出する際はシステム担当者もしくはシステム担当者が許可した職員が立ち会なければならない。

（3） 通信回線及び通信回線装置の管理

① システム担当者及び情報セキュリティ担当者は、病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 システム担当者は、外部へのネットワーク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 システム担当者は、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 システム担当者は、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。

⑤ システム担当者は、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） 職員の利用する端末や電磁的記録媒体等の管理

情報セキュリティ管理者およびシステム担当者は、盗難防止のため、執務室等で利用するパソコン、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等、可能な限り物理的措置を講じなければならない。また電磁的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。

（5） 取扱区域（執務室等）の管理

① 情報セキュリティ管理者は、取扱区域における情報資産の盗難又は紛失等を防止しなければならない。

② 情報セキュリティ管理者は、外部からの訪問者が取扱区域に入る場合には、必要に応じて職員が付き添うなど、担当者以外の者が容易に閲覧等できないようにしなければならない。

5 技術的セキュリティ対策

（1） 情報システム全体の強靭性の向上

複雑・巧妙化しているサイバー攻撃の脅威により、病院の業務に重大な影響をあたえるリスクが想定されるため、機密性、可用性、完全性の確保に十分配慮した攻撃に強い情報システムにしなければならない。

（2） コンピュータ及びネットワークの管理

① システム管理記録及び作業の確認

A) 情報セキュリティ管理者およびシステム担当者は、所管する情報システムの運用において実施した作業に関する記録を作成しなければならない。

B) 情報セキュリティ管理者およびシステム担当者は、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なければならない。

② 情報システム仕様書等の管理

システム担当者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者の閲覧や、紛失等がないよう、適正に管理しなければならない。

③ バックアップの実施

システム担当者は、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。

④ ログの取得等

A) システム担当者は、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。

B) システム担当者は、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。

C) システム担当者は、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を可能な限り実施しなければならない。

⑤ 障害記録

システム担当者は、職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

⑥ ネットワークの接続制御、経路制御等

システム担当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。

システム担当者は、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。

⑦ 外部の者が利用できるシステムの分離等

システム担当者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑧ 外部ネットワークとの接続制限等

A) システム担当者は、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、情報セキュリティ統括責任者の許可を得なければならない。

B) システム担当者は、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。

C) 情報システム担当者及びシステム担当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、契約時に損害賠償責任を契約上担保することが望ましい。

D) システム担当者は、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。

E) システム担当者は、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、情報セキュリティ統括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。

⑨ 複合機のセキュリティ管理

A) 職員は、複合機を調達する場合、当該複合機が備える機能、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対策を講じなければならない。

B) 職員は、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。

C) 職員は、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。

⑩ 特定用途機器のセキュリティ管理

システム担当者は、特定用途機器（ネットワークカメラシステム等の通信又は電磁的記録媒体を内蔵する機器）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。

⑪ 無線LANの盗聴対策

A) 情報セキュリティ統括責任者は、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。

B) システム担当者は、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、暗号化等の措置を講じなければならない。

⑫ 電子メールのセキュリティ管理

A) セキュリティ担当者は、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。

B) セキュリティ担当者は大量のスパムメール等の受信又は送信を検知した場合は、情報セキュリティ統括責任の指示のもとメールサーバの運用を停止しなければならない。

C) セキュリティ担当者は、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。

D) セキュリティ担当者は、職員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に周知しなければならない。

⑬ 電子メールの利用制限

A) 職員は、自動転送機能を用いて、電子メールを転送してはならない。

B) 職員は、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。

C) 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。

D) 職員は、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。

E) 職員は、病院が提供するネットワークサービス以外のサービス等を原則使用してはならない。

⑭ 無許可ソフトウェアの導入等の禁止

職員は、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。

職員は、業務上の必要がある場合は、情報資産を管理している情報システム担当者の許可を得て、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又はシステム担当者は、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。

職員は、不正にコピーしたソフトウェアを利用してはならない。

⑮ 機器構成の変更の制限

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

B） 職員は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、システム担当者の許可を得なければならない。

⑯ 無許可でのネットワーク接続の禁止

職員は、システム担当者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。（病院支給も含む）

⑰ 業務以外の目的でのウェブ閲覧の禁止

A） 職員は、業務以外の目的でウェブを閲覧してはならない

B） 職員は、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報告し適切な措置を求めなければならない。

（3）アクセス制限

① アクセス制限

A） アクセス制限

システム担当者は、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。

B） 利用者IDの取り扱い

イ） システム担当者は、利用者の登録、変更、抹消等の情報管理、職員の異動、退職者に伴う利用者IDの取扱い等の方法を定めなければならない。

ロ） 職員は、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、システム担当者に通知しなければならない。

ハ） システム担当者は、利用されていないIDが放置されないよう、点検しなければならない。

C） 特権を付与されたIDの管理等

イ） システム担当者は、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

ロ） システム担当者の特権を代行する者は、システム担当者が認めた者でなければならない。

ハ） システム担当者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

ニ） システム担当者は、特権を付与されたID及びパスワードについて、職員の端末等のパスワードよりも定期変更等のセキュリティ機能を強化しなければならない。

ホ） システム担当者は、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 認証情報の管理

A） システム担当者は、職員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。

B） システム担当者は、職員に対して個別に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るよう可能な限り働きかけなければならない。

C) システム担当者は、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。

(4) システム開発、導入、保守等

① 情報システムの調達

A) システム担当者は、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。

B) システム担当者及び情報セキュリティ担当は、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可能な限り確認しなければならない。

② 情報システムの開発

A) 外部業者によるシステム開発の場合

イ) システム開発における責任者及び作業者の特定

職員は、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。また、システム開発のための方針手順等を決定し、開発に適用しなければならない。

ロ) システム開発における責任者、作業者のIDの管理

情報セキュリティ担当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、システム担当者へ開発用IDを削除するよう連絡しなければならない。

B) 院内での開発の場合システム開発

イ) システム作成制限

院内で開発するシステムは、業務サポートに特化したものとし、保管義務があるデータを入力するシステム作成は原則禁止とする

ロ) 作成依頼

職員は「システム作成申請書」を記載しシステム担当者へ作成依頼をしなければならない。

ハ) 開発

システム担当者は「システム作成申請書」が提出されたのち、要求仕様に従いシステムを開発する。その際、システムの仕様書を作成しなければならない。

③ 情報システムの導入

A) 外部業者によるシステム導入の場合

イ) システム担当者もしくは情報セキュリティ担当者は、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。

ロ) システム担当者はもしくは情報セキュリティ担当者は、移行導入の際情報システムに記録されている情報資産の保存、または職員に保存を指示しなければならない。また、移行時に伴う情報システムの停止などの影響が最小限になるように配慮しなければならない。

ハ) システム担当者もしくは情報セキュリティ担当者は、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。

ニ) システム担当者もしくは情報セキュリティ担当者は、個人情報及び機密性の高い生データを、テストデータに原則使用してはならない。

B) 院内開発システムの導入の場合

イ) システム担当者は、新たに情報システムを導入する場合、現在の環境下で稼働することを確認した上で導入しなければならない。

ロ) システム担当者は職員が緊急的に作成依頼をしたシステムに関しては、最低限の確認にて運用を行う事が可能とするが、現行情報システムに影響が出ない用配慮する。

④ システム開発・保守に関連する資料等の整備・保管

A) システム担当者もしくは情報セキュリティ担当者は、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。

B) システム担当者はもしくは情報セキュリティ担当者は、テスト結果を一定期間保管しなければならない。

C) システム担当者はもしくは情報セキュリティ担当者は、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

⑤ 情報システムにおける入出力データの正確性の確保

A) 外部業者によるシステム開発の場合

イ) システム担当者もしくは情報システム担当者は、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するように指導することが望ましい。

ロ) システム担当者もしくは情報システム担当者は、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、これを防止することができるように情報システムの設計を指導しなければならない。

ハ) システム担当者もしくは情報システム担当者は、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するように指導しなければならない。

⑥ 情報システムの変更管理

A) 外部業者によるシステム開発の場合

システム担当者もしくは情報セキュリティ担当者は、情報システムを変更した場合、作成業者へプログラム仕様書等の変更履歴を記載する要指示しなければならない。

B) 院内開発システムの導入の場合

職員は院内開発システムに対して変更を依頼する場合、E3 メールもしくは「システム作成申請書」にて変更を依頼する必要がある。

⑦ 開発・保守用のソフトウェアの更新等

システム担当者もしくは情報セキュリティ担当者は、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

システム担当者もしくは情報セキュリティ担当者は、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。

(5) 不正プログラム対策

① システム管理部門の措置事項

システム担当者は、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。

A) 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、必要に応じ職員に対して注意喚起しなければならない。

B) サーバを除く所掌する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。

C) 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、可能な限り最新の状態に保たなければならない。

D) 不正プログラム対策のソフトウェアは、可能な限り最新の状態に保たなければならない。

E) 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原則利用してはならない。

② 情報セキュリティ管理の措置事項

情報セキュリティ管理は、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。

A) 情報セキュリティ管理者は、その所掌する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システムに常駐させなければならない。

B) 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、可能な限り最新の状態に保たなければならない。

C) 不正プログラム対策のソフトウェアは可能な限り最新の状態に保たなければならない。

D) インターネットに接続していないシステムにおいて、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、病院が配布している媒体以外を職員に利用させてはならない。

③ 職員の遵守事項

職員は、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。

A) パソコンやモバイル端末において、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。

B) 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、必ず医療情報室にて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。

C) 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。

D) 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することが望ましい。

E) システム担当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。

F) 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、以下の対応を行わなければならない。

イ) パソコン等の端末の場合

ログを保存したうえで、LAN ケーブルの即時取り外し及び無線 LAN の停止を行わなければならない。

ロ) モバイル端末の場合

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。

④ 専門家の支援体制

システム担当者は、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しておかなければならない。

（6）不正アクセス対策

① 情報セキュリティ統括責任者の措置事項

情報セキュリティ統括責任者は、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

A) 情報セキュリティ統括責任者は、不要なサービスについて、機能を削除又は停止するようシステム担当者へ指示しなければならない。

B) 情報セキュリティ統括責任者は、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の対策システムの導入を可能な限り行っていかなければならない。

C) 情報セキュリティ統括責任者は、情報セキュリティインシデントに対処するための体制と連携し、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。

② 攻撃への対処

情報セキュリティ統括責任者及びシステム担当者は、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、総務省、都道府県等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

情報セキュリティ統括責任者及びシステム担当者は、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

情報セキュリティ統括責任者及びシステム担当者は、職員及び外部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 職員による不正アクセス

情報セキュリティ統括責任者及びシステム担当者は、職員による不正アクセスを発見した場合は、当該職員の情報セキュリティ管理者へ通知し、適正な処置を求めなければならない。

⑥ サービス不能攻撃

情報セキュリティ統括責任者及びシステム担当者は、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

情報セキュリティ統括責任者及びシステム担当者は、情報システムにおいて、標的型攻撃（特定のターゲットを狙った攻撃）による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（7）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

情報セキュリティ統括責任者及びシステム担当者は、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。

情報セキュリティ統括責任者及びシステム担当者は、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

情報セキュリティ統括責任者及びシステム担当者は、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。

6 運用

(1) 情報システムの監視

情報セキュリティ統括責任者及びシステム担当者は、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) 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

A) 情報セキュリティ統括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、速やかに関係各所に報告しなければならない。

B) 委員会は、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。

C) 情報セキュリティ統括責任者及びシステム担当者は、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、モバイル端末及び電磁的記録媒体等の利用状況調査

システム担当者及び委員会が指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、モバイル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 職員の報告義務

A) 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、直ちに情報セキュリティ統括責任者もしくは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。

B) 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情報セキュリティ統括責任者が判断した場合において、職員は、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 緊急対応計画の策定

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切に実施するために、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切に対処しなければならない

② 緊急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。

A) 関係者の連絡先

B) 発生した事案に係る報告すべき事項

C) 発生した事案への対応措置

D) 再発防止措置の策定

③ 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、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

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

病院は、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、病院業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、委員会の許可を得て、例外措置を講じることができる。

② 緊急時の例外措置

病院は、業務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、事後速やかに委員会に報告しなければならない

（5）法令遵守

① 法令順守

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、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。

A) 個人情報の保護に関する法律

B) 不正アクセス行為の禁止等に関する法律

C) 刑法

D) 著作権法

E) 不正アクセス行為の禁止等に関する法律

F) 個人情報の保護に関する法律

G) サイバーセキュリティ基本法

H) 新須磨病院就業規則内　服務規程

I) 神戸市公開条例

J) 神戸市個人情保護条例

② マイナンバーガイドライン

マイナンバーを扱う個人番号利用事務及び個人番号関係事務は、個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン」を遵守しなければならない。

7 外部サービスの利用

（1）外部委託

① 外部委託事業者の選定基準

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。

② 契約項目

情報システムの運用、保守等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。

A) 情報セキュリティポリシー等の遵守
B) 外部委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
C) 提供されるサービスレベルの保証
D) 外部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
E) 外部委託事業者の従業員に対する教育の実施
F) 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
G) 業務上知り得た情報の守秘義務
H) 再委託に関する制限事項の遵守
I) 外部委託事業者のデータの保管に関する事項
J) データの複写及び複製の禁止に関する事項
K) データの授受及び搬送に関する事項
L) 委託業務終了時の情報資産の返還、廃棄等
M) 委託業務の定期報告及び緊急時報告義務
N) 病院による監査、検査
O) 病院による情報セキュリティインシデント発生時の公表
P) 特定個人情報を取り扱う従事者の明確化に関する事項
Q) 漏えい事案等が発生した場合の委託先の責任に関する事項
R) その他データの保護に関し必要な事項
S) 前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項

③ 確認・措置等

情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置を実施しなければならない。

（2） 約款による外部サービスの利用

① 約款による外部サービスの利用に係る情報の取扱い

情報セキュリティ管理者は、約款による外部サービス（民間事業者等の病院外の組織が約款に基づきインターネット上で提供する情報処理サービス）の利用において、機密性の基準第Ⅰ種に相当する情報（個人情報、秘密文書）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おける対策の実施

職員は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

（3） ソーシャルメディアサービスの利用

① インターネット上におけるブログ、ソーシャルネットワーキンサービス、動画共有サイト等のソーシャルメディアサービスを病院が管理するアカウントで利用する場合、情報セキュリティ対策に関する次の事項を含めた運用手順を定めなければならない。

A) 病院のアカウントによる情報発信が、実際の病院のものであることを明らかにするために、病院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。

B) 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。

② 機密性の高い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。

③ 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。

④ 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。

8 評価・見直し（監査・自己点検）

（1）監査

① 実施方法

委員会は、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、必要に応じて監査を行わなければならない

② 監査を行う者の要件

A) 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。

B) 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

A) 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、委員会の承認を得なければならない。

B) 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない

⑤ 監査の委託

情報セキュリティに関する監査は、外部の専門家を監査人として実施することができる。この場合において、客観的で公平な手続きに従って調達を行い、かつ、当該監査委託先は、監査対象と直接利害関係がないこととする。

⑥ 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、情報セキュリティ統括責任者及び委員会に報告する。

⑦ 監査結果への対応

委員会は、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、情報セキュリティ統括責任者に対し、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

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

A) システム担当者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

B) 情報セキュリティ管理者は、所管する部署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、毎年度及び必要に応じて自己点検を行わなければならない。

② 自己点検結果の活用

A) 職員は、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。

B) 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

委員会は、情報セキュリティポリシー及び関係規程等について毎年度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、改善を行うものとする。