特定医療法人　慈恵会　新須磨病院
情報セキュリティポリシー
（基本方針）

平成１７年　１０月　１３日

序　文

IT の急速的な進展により、医療業務においても電子化が進み、特定医療法人　慈恵会　新須磨病院（以下「当院」といいます）でも電子カルテなどのシステムを導入し医療業務を遂行しています。
当院が保有している確実な安全管理が望まれる情報資産（紙・音声・フィルム・電子データ等あらゆる形式で保存されているものすべてを含みます）には患者様の個人情報、職員に関する情報、当院の機密情報等があります。また、これらの情報資産を取り扱う全てのネットワーク及びシステムにも高度な安全性を確保することも不可欠な前提条件となります。
これらの情報資産とネットワーク及びシステムを安全に運用することが望まれる中、
２００５年４月に施行された「個人情報保護法」によって、情報資産の取扱いについてより高い安全性が求められるようになりました。しかし内部漏洩による情報資産の流出事件が後を絶たないのが現状です。情報資産を内外問わずあらゆる脅威から防御することは安全で安心できる医療業務を継続するために必要不可欠と考えています。
しかし「個人情報保護法」に過剰に執着した運用は利便性を損なうだけでなく、最優先すべき患者様の利益を損なうことになりかねません。
当院では患者様の利益を最優先に考えた柔軟な対応と安全で安心できる医療業務を継続するために情報セキュリティポリシーを策定し、当院の情報資産および全ネットワークとシステムへの取扱いに対して全職員へ教育を行い、意識の向上を図ります。

情報セキュリティポリシーは、基本方針を定めた「基本方針」とセキュリティ対策の基準を定めた「対策基準」、当院の全職員が具体的に実行をする内容を定めた「実施手順」により構成されています。この情報セキュリティポリシーを全職員が遵守することにより、患者様へさらなる安全で安心していただける医療サービスの提供を実行していきます。

第１章　総則

１．目的

情報セキュリティ基本方針は、特定医療法人　慈恵会　新須磨病院の情報セキュリティに関し、包括的な対策を図ることにより、特定医療法人　慈恵会　新須磨病院が保有する情報資産を適切に保護することを目的とする。

２．定義

２．１　定義

（１）　対策基準において使用する用語及び定義は、それぞれ次のとおり定める。

１．　情報

紙、音声、電子データ等、あらゆる形式で保存されている事物、出来事などの内容、様子をいう。

２．　情報セキュリティ

当院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ことをいう。

３．　情報資産

４．　個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などにより特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）をいう。

映像･音声･血液･検体もこれに含まれる

患者情報に限らず、職員の情報もこれにあたる

５．　医療情報

医療業務の執行に係る情報（個人情報を含む）をいう。また、一時的に記録されたメモ等の情報も含む。

６．　脅威

自然災害や悪意のある行為等、情報資産に被害を与える要因をいう。

７．　脆弱性

情報資産が保有する情報セキュリティの弱い部分や､情報セキュリティを弱める環境等により、脅威を発生し易くさせる要因をいう。

８．　セキュリティエリア

病院（１、２、３号館)、地域医療相談センター、マーガレット会館をいう。

９．　セキュリティ境界

セキュリティエリア内において、職員及び当院が許可を与えた者のみ入る事が出来る領域をいう。

１０．部門

各診療科

１１．執務室

執務（窓口業務・医療事務及び医療行為）を行う場所のこと。例えば、医事課、各病棟の詰所 、各診療科等をいう。

１２．職員

職員とは、当院に在職する正職員、非常勤職員、臨時職員及び研修医、ボランティアなど、雇用関係の有無に関わらず当院の業務に従事する全ての者を示す。

１３．持出し

情報資産をセキュリティエリア内において、物理的及び電子的に移動させることをいう。また、情報を記録媒体に出力する行為、セキュリティエリア外への許可された移動も含む。

１４．廃棄

廃棄行為、リサイクル行為またはリース端末のリースアップ行為をいう。

１５．漏洩

情報が許可なくセキュリティエリア外へ持出されることをいう。

１６．記録媒体

情報を保存した電子媒体及び情報が記録された紙媒体、写真のフィルム等をいう。

１７．周辺機器

端末に接続する、情報を保存する外付けハードディスク、外付けMO、外付けフロッピーディスク等の機器をいう。

１８．アクセス権限

データ資産を利用する人が情報資産を扱える範囲のことをいう。

１９．外部ネットワーク

院内ネットワーク以外のネットワーク（本基準の適用範囲外のネットワークを含む）をいう。

２０．情報セキュリティインシデント

情報セキュリティに関連した事件、出来事、事象を示す。例えば、情報資産の不正持ち出し、情報資産の不正使用、情報資産の紛失、業務妨害行為、データの破壊、意図しない情報の開示や、それらに至るまでの行為（事象）等をいう。

２１．　情報サービス

患者様への医療サービスと内部業務を行うために必要な情報の提供、情報システム処理の提供をいう。

２２．　サービスレベル

情報サービスに関する信頼、安全及び効率面での品質をいう。

２３．　許容停止時間

医療業務に大きな支障を及ぼさない範囲で、情報サービスの停止を許容できる時間をいう。システムの部門等が、復旧計画を策定する場合の目標回復時間になる。

２４．　代替率

情報サービスが停止している場合に、代替手段（手作業など）によって、通常のサービスレベルを代替できる割合をいう。

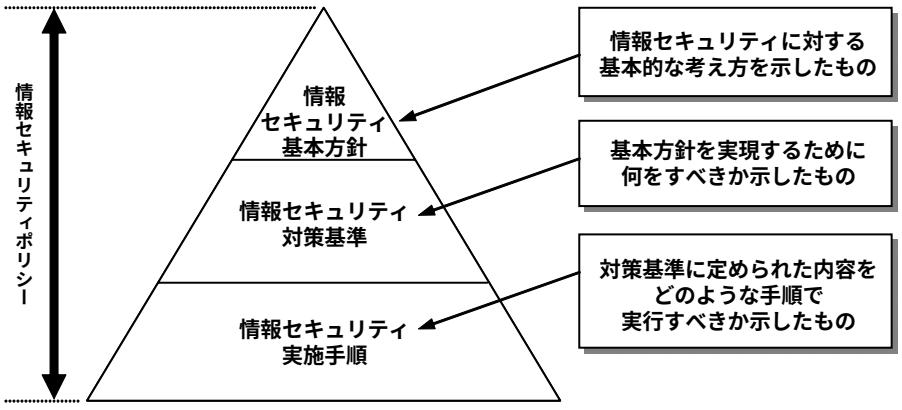
２５．　セキュリティホール

ソフトウェアの設計ミスなどによって生じた、システムの情報セキュリティ上の弱点をいう。

３．情報セキュリティポリシーの構成

情報セキュリティポリシーとは、特定医療法人　慈恵会　新須磨病院の情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティに関する文書は、以下の３つの階層に分けて策定、管理するものとし、情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順から構成される。



３．１　情報セキュリティ基本方針

情報セキュリティ基本方針は、特定医療法人　慈恵会　新須磨病院情報セキュリティポリシーの最上位に位置する文書である。

この文書は、情報セキュリティの対策に関する基本的な方針を記述した文書である。

３．２　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に基づき、全情報システム及び業務で遵守すべき対策の基準を記述した文書である。

３．３　情報セキュリティ実施手順

情報セキュリティ実施手順は、情報セキュリティ対策基準に基づき、各情報システム又は業務における具体的な実施手順を記述した文書である。

４．情報セキュリティポリシーの公開

情報セキュリティポリシーには、特定医療法人　慈恵会　新須磨病院のセキュリティ上の脆弱性に関する内容が含まれており、情報セキュリティ確保の観点から、基本方針は公開とするが、他の文書については公開してはならない。

５．情報セキュリティポリシーの適用範囲

適用範囲は、次に掲げる範囲とする。

① 特定医療法人　慈恵会　新須磨病院が管理する情報資産及び情報資産を取扱う者（職員及び委託先事業者の従事者）全てに適用する。

② 前項に係る業務を外部委託する場合は、この対策基準に準拠した契約を締結し、委託先事業者に対してもこの基準を適用する。

第２章　基本方針

１．情報セキュリティ組織運営基準

情報セキュリティの推進と向上のための組織体制及び教育等に関して、必要な事項を定めるものとする。

２．個人情報管理基準

医療業務を行うために必要な情報の取得、利用、及び第三者への提供に関して、必要な事項を定めるものとする。

３．医療情報管理基準

医療情報として取扱う電子情報及び可視的に記録された情報を適切に作成、取得、保存、利用及び提供するための取扱いに関して、必要な事項を定めるものとする。

４．情報セキュリティ行動基準

情報セキュリティの確保を図るために、職員が遵守すべき事項を定めるものとする。

５．環境・機器・設備管理基準

コンピュータの設置環境、情報を取扱う機器及び設備に関して、情報セキュリティの確保を図るために必要な事項を定めるものとする。

６．情報システム管理基準

医療業務を行う上で必要な情報システムの運用に関して、情報セキュリティの確保を図るために必要な事項を定めるものとする。

７．ネットワーク管理基準

情報システムで利用するネットワークに関して、情報セキュリティの確保を図るために必要な事項を定めるものとする。

８．情報システム開発基準

情報システムの企画、設計、開発及び導入に関して、情報セキュリティを確保するために必要な事項を定めるものとする。

９．外部委託基準

情報サービスを外部委託する場合及び指定管理者を選任する場合において、情報セキュリティを確保するために必要な事項を定めるものとする。

１０．情報セキュリティインシデント対応基準

情報セキュリティインシデントが発生した場合に、迅速かつ正確な対応を行うための情報セキュリティ関連の情報収集、緊急時対応計画に関して必要な事項を定めるものとする。

１１．医療業務継続基準

医療業務を行うために必要な情報サービスの可用性や代替手段を確保し、それによって医療業務の継続性を高めることを目的とし、必要な事項を定めるのものとする。

１２．情報セキュリティの評価・見直し

情報システムのリスク管理体制が適切かつ効果的であるかを評価するために、監査及び点検に関して、必要な事項を定めるものとする。

１３．法令等の遵守

情報セキュリティに関する法令違反の発生を防止するために、関連する法律、条令等に関して周知徹底することを目的と、必要な事項を定めるものとする。

１４．違反への対応

情報セキュリティポリシーの遵守状況を確認するために、定期的な確認事項及び対策基準への遵守違反を発見した場合の報告義務に関して、必要な事項を定めるものとする。