令和元年8月23日

セキュリティ管理規定

（目的）

第一条 新松戸中央総合病院（以下当院）で利用される情報システム全般（医療情報システムおよび事務業務端末を指す）に関しての管理運営に関し必要な事項を定めるものとする。

（組織）

第二条 セキュリティ対策を総合的に実施するために、セキュリティ統括責任者を置きセキュリティ統括責任者は、病院長をもってこれにあてる。

2 電子カルテシステムの適切な管理を行うため、システム管理者を置きシステム管理者は、システム開発室室長をもって充てる。

3 情報システム利用する部署においてセキュリティ対策を実施するため、セキュリティ責任者を置きセキュリティ責任者は、各課所属長をもって充てる。

（会務）

第三条 セキュリティ統括責任者は、セキュリティ会議を招集するとともに、議長を務める。但し、セキュリティ統括責任者は必要な場合、セキュリティ統括責任書を別に指名することが出来る。又、セキュリティ会議は隔月で行い電子カルテ委員会をもってこれにあてる。

2 セキュリティ会議は、セキュリティ統括責任者のほか、次に掲げるものをもって組織する。

① システム管理者

② セキュリティ責任者

3 セキュリティ会議は、次に掲げる事項を審議する。

① 情報システムのセキュリティ対策の決定及び見直し

② 前号のセキュリティ対策の遵守状況の確認

③ 監査の実施

④ 教育・研修の実施

4 議長は、必要と認めるときは、関係職員の出席を求め、その意見又は説明を聴くことができる。

5 セキュリティ会議の庶務は、システム開発室において処理する。

（入退室管理）

第三条 次に掲げる情報システムの運用が行われる室においては、それぞれのセキュリティ区分に応じた、入退室管理を行うものとする。

セキュリティ区分	室
レベル 3	医療情報システムサーバ、ネットワークシステム機器設置室
レベル 2	医事課内保険請求端末
レベル 1	業務端末の設置室(各科・病棟)

2　それぞれのセキュリティ区分に応じた、入退室管理の方法は次のとおりである。

セキュリティ区分	入退室管理の方法
レベル 3	入退室を行う場合には、入退室管理者から事前に許可を得ている者のみが入退室を行い、その都度、鍵を用いて入退室を行い、入退室に関する記録を行う。
レベル 2	一般業務を行う場所であるために入室制限は行わないが最終退出者が必ず施錠を行うものとする。
レベル 1	部外者が立ち入らない場所であれば管理はしない。最終退出者が必ず施錠を行うものとする。

（入退室管理者）

第四条　入退室管理者は、サーバ、ネットワーク機器、電子カルテシステムのデータ、セキュリティ情報等の保管の設置室にあっては、システム開発室室長、業務端末の設置室にあっては、各科所属長をもって充てる。

2　入退室管理者は、前条第 1 項に掲げる室について、同条第 2 項に定める入退室の管理を行うほか、情報システムのセキュリティを確保するため、入退室の管理に関し、必要な措置をとらなければならない。

（鍵の管理）

第五条　鍵の管理は、入退出管理者が行う。

2　入退出管理者は、レベル 2・3 のセキュリティ区分に係る室については、許可を得ている者に限り鍵を貸与するものとする。

（管理簿の作成）

第六条　入退室管理者は、レベル 3 のセキュリティ区分に係る室については、入退室管理簿を作成し、これを保存するものとする。

（ネットワーク管理）

第七条　医療情報管理システムと外部接続（WAN）を可能とするネットワークを個別に管理するものとし同一ネットワーク上に混在させないものとする。

2　外部（インターネット）との通信を制御するためにファイアウォールを導入する。ファイアウォールは、ルータにある機能を使用するものとする。

3　院内の LAN ケーブルは、各階までの基幹線と、島から各机上までの枝線の２種類に分別するものとし、医療情報システムネットワークでは、障害を最小限にするために VLAN を組むものとする。また、医療情報システムは青色 UTP ケーブル、業務用端末は白色 UTP ケーブルを利用する。

4　病棟では無線 LAN を使用するが、無線にはステルス化を行い外部端末からの無線状況の確認が出来ない事を条件とする。(暗号化・PW 設定は無論必須である。)

4　IP アドレスの管理はシステム開発室にて行うものとし TCP/IP4 プロトコールを使用して接続を行うものとする。新規・変更・削除がある場合にはシステム開発室にて行うものとする。

5　ネットワーク利用者は、システム開発室の許可なくネットワークに PC・サーバー・ネットワーク機器を接続してはならない。

6　ネットワーク利用者は、ネットワーク管理者の許可なく、ネットワークケーブルを配線してはならない。
7　ネットワーク利用者は､ネットワーク管理者より与えられたIPアドレス以外のアドレスを使用してはならない。

（アクセス管理）
第八条 次に掲げる情報システムの構成機器について、アクセス管理を行う。
① サーバ
② ネットワーク機器
③ 各種医療情報システムソフトウエア
④ 業務端末
2　医療情報システムソフトへのアクセス権限に関しては別紙参照の事
3　業務端末に於いては必ずPW設定を行うものとし離席時にはログオフするものとする。
4　サーバー・ネットワーク機器に関してはシステム開発室スタッフ以外には、障害対応を行うメーカー担当者は可能とする。
5　障害発生時におこなわれるリモート操作に関しての規定は別途定める。

（アクセス管理責任者）
第九条 前条のアクセス管理を実施するため、アクセス管理責任者を置く。
2　アクセス管理責任者は、システム開発室室長をもって充てる。

（アクセスID/PW）
第十条 アクセス管理責任者は、操作者用パスワードの管理方法を定め、管理簿を作成する。

（利用者の責務）
第十一条　操作者は、操作者用パスワードの管理方法を遵守しなければならない。（運用管理規程に別途定める。）

（資産管理）
第十二条　情報システムの情報資産(電子カルテシステムに係る全ての情報並びにソフトウードウェア､ネットワーク及び磁気ディスクをいう。以下同じ。)について、管理責任者を置く。
2　管理責任者はシステム開発室室長をもってこれにあてる。

（委託管理）
第十三条　情報システムを管理し、又は利用する部署の長は、外部委託をしようとするときは、委託する事務の内容、理由及び情報の保護に関する事項等について、あらかじめ、セキュリティ会議の審議を経て、セキュリティ統括責任者の承認を得なければならない。
2　外部委託に係る契約書には、情報の保護に関し、次の各号に掲げる事項を明記しなければならない。
① 再委託に関する事項
② 情報が記録された資料の保管、返還又は廃棄に関する事項
③ 情報が記録された資料の目的外使用、複製・複写及び第三者への

提供の禁止に関する事項
④ 情報の秘密保持に関する事項
⑤ 事故等の報告に関する事項

（秘密保持）
第十四条　業務上知り得た患者等の秘密を他に漏らしてはならない。なお、職員でなくなった後においても同様とする。
２　個人情報などの秘密保持内容に関しては「個人情報保護規定」に準じて行うものとする。

（管理部署）
第十条　運用を含めた管理は電子カルテ委員会とし、実運用はシステム開発室が行うものとする。
２　取扱い・運用に関しては、医療情報システム監査項目とする。

（その他）
第十一条　この規程に定める事項が何らかの要素により変更になった場合には、電子カルテ委員会にて審議しこの規程を改定するものとし、関連スタッフへの周知させるものとする。

（付　則）
この規程は、平成 26 年 4 月 1 日から施行する。
・令和元年 8 月 23 日より、本改訂版を施行する。