医療法人誠心会　情報セキュリティポリシー　第３版

1. 目的

医療法人誠心会(以下「法人」という。)医療情報セキュリティポリシーは、法人の医療情報セキュリティ対策の基本的な方針として、適用の対象や位置づけ等を定め、法人が所掌する医療情報資産の機密性、完全性及び可用性を維持し、総合的・体系的かつ継続的に情報セキュリティ対策を目的とする。

2. 用語の定義

① 情報ネットワーク

コンピュータを相互に接続するための通信網、接続機器のハードウェア(無線ＬＡＮを含む)及びソフトウェア並びに電磁的記録媒体で構成され、処理を行う仕組みを情報ネットワークという。

② 情報システム

ハードウェア及びソフトウェアで構成されるコンピュータ、情報ネットワーク並びに電磁的記録媒体で構成され、処理を行う仕組みを情報システムという。

③ 情報資産

次の各号を情報資産という。

⑴ 情報ネットワークと情報システムの開発・運用に係る全ての情報及び情報ネットワークと情報システムで取り扱う全ての情報

⑵ （1）の情報が記録された紙等の有体物及び電磁的記録媒体

⑶ 情報ネットワーク及び情報システム

④ 情報セキュリティ

情報の真正性、見読性、保存性を維持すること。

⑴「真正性」

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、および混同が防止されていることである。また記名、押印が必要な文書については、電子署名、タイムスタンプなどを付すことが必要である。

⑵「見読性」

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること。

ただし、見読性とは本来「診療に用いるのに支障がないこと」と「監査等に差し支えないようにすること」であり、この両方を満たすことが、ガイドラインで求められる実質的な見読性の確保」である。冗長性やバックアップをとることなどのシステム全般の保護対策が必要。

⑶「保存性」

記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

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、法人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セキュリティ実施手順から構成される。

【医療法人誠心会情報セキュリティポリシー】

■情報セキュリティ基本方針

法人が所掌する医療情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものであり、情報セキュリティ対策の頂点に位置するものである。

■情報セキュリティ対策基準

法人医療情報セキュリティ基本方針に基づき、情報セキュリティ対策を統一的に講ずるために、職員等が遵守すべき行為及び判断等の基準を規定するものである。

■情報セキュリティ実施手順

法人医療情報セキュリティポリシーに基づき、情報セキュリティ対策を具体的に実施するために、職員等が遵守すべき情報セキュリティ対策の実施手順を具体的に規定するものである。

次ページより詳細に記述する。

３－１　情報セキュリティ基本方針

基本方針

法人が保有するまたは、管理する情報資産（電子情報システム・電子情報資産及び紙媒体の資産）を過失、事故、災害、犯罪、などの脅威から守り、患者さんの個人情報を保護するため、次により情報セキュリティ基本方針を定める。

1. 情報セキュリティポリシーに基づき、物理的、人的、技術的において、適切な情報セキュリティ対策をこうじて、情報資産に対する不正な侵入、漏洩、改ざん、紛失、破壊、妨害などが発生しないように充分な備えに勤めます。

2. 情報セキュリティに関し職員に必要な教育啓発活動を実施するほか、適切な管理・監査体制を確立し、患者さんの個人情報保護に努めます。

3. 情報セキュリティに関する法令その他の規範を遵守します。

4. 以上の内容を、継続的に見直し改善に努めます。

３－２情報セキュリティ対策基準

１．適用範囲

法人医療情報セキュリティポリシーの適用範囲は、以下の各号に示すものとする。

① 適用組織

当院の各部及び事務の各課とする。

② 適用情報資産

適用組織が所掌する医療情報資産とする。

③ 適用対象者

適用される情報資産に接する適用組織の職員（非常勤職員及び臨時職員等を含む。以下「職員等」という。）とする。

２．職員等の義務

① 厳守義務

職員等は情報セキュリティの重要性について共通の認識を持つと共に、法人が所掌する医療情報資産を取り扱う際には、不正アクセス行為の禁止等に関する法律や著作権法等の情報セキュリティに関連する法令並びに当院医療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。

② 処分等

本ポリシーに違反した職員等は、その重大性及び発生した事案の状況等に応じて処分対象となる場合がある。

３．情報セキュリティ管理体制

法人の所掌する医療情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立する。

４．情報資産の分類

法人の所掌する医療情報資産をその内容によって分類し、その重要度に応じた情報セキュリティ対策を講ずる。

５．情報資産への脅威

情報セキュリティ対策を講ずる上で、特に認識すべき脅威は以下のとおりである。

① 本ポリシーに規定する適用対象者以外の第 3 者による、故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗聴、改竄、消去並びに機器及び記録媒体の盗難等。

② 職員等及び業務を委託した者（以下「外部委託業者」という。）による、誤操作又は故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗聴、改竄、消去並びに機器及び記録媒体の盗難等。

③ 地震、落雷、火災、水害等の災害、事故及び故障等。
④ 廃棄時の漏洩。

６．情報セキュリティ対策

法人の所掌する医療情報資産を先に掲げた脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

① 物理的セキュリティ対策

最重要な情報システムを設置する施設（サーバー室）への不正な立ち入り、医療情報資産への損傷・妨害等を防ぐため、入退室や機器管理上の物理的な対策を講ずる。

② 人的セキュリティ対策

医療情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めると共に、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育及び啓発が行われるよう必要な対策を講ずる。

③ 技術的セキュリティ対策

医療情報資産を不正なアクセス等から適切に保護するため、医療情報資産へのアクセス制御、コンピュータウィルス対策等の技術的な対策を講ずる。またリモートアクセスの状態を管理する。

④ 運用セキュリティ対策

情報セキュリティポリシーの実効性を確保するため、情報システム等の稼動状況の監視や情報セキュリティポリシーの遵守状況の確認のため、運用面における必要な対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするため、危機管理対策を講ずる。

７．情報セキュリティ対策に関する規定の公開・非公開

法人医療情報セキュリティ基本方針は公開するが、法人医療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の公開は、犯罪の予防その他の公共の安全及び秩序の維持に支障を及ぼす恐れがあるため、これらは公開しない。

８．情報セキュリティ対策実施状況の検証

法人医療情報セキュリティポリシーが適切に遵守されていることを確認するために、定期的に情報セキュリティ対策の実施状況について検証を行う。

９．情報セキュリティ対策の評価・見直し

情報セキュリティ対策の実施状況の検証結果、情報システムの変更、新たな脅威等情報セキュリティを取り巻く情報の変化に対応し、法人医療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評価と見直しを適宜行う。

３－３　情報セキュリティ実施手順

＊ローカルパソコン等へ、個人情報の安易なコピーはしない
＊情報の院外、職場外の持ち出し
・取り扱いに注意を要する→原則禁止、必要があれば承認ルールの明確化
・自動車内に、記録媒体および情報機器の放置禁止
＊情報の破棄
・機密性の高い情報が記載された紙媒体はシュレッダー処理（裏紙等の使いまわしはしない）
・パソコン、ＨＤＤ等のデータ保存媒体は、復元不能な方法で消去するか破砕処理
＊個別に外部接続（インターネットプロバイダーへの接続等）への制限
・原則禁止、必要があれば承認ルールの明確化
＊ＩＤ/パスワードの管理
・ユーザーＩＤの共同利用はしない
・離職者、退職者のユーザーＩＤは直ちに削除等の利用不可の状態にする
・パスワードは守秘（人に教えない→電話等で聞かれても教えない）
・2 種類以上の文字種を含む 6 文字以上のパスワード設定
（生年月日や家族名、ありふれた文字の連続など、推測容易な内容としない）
・パスワードを定期的に変更する期間については別途検討する
・パスワードの自動入力などの設定を行わない（ＩＥ等の web ブラウザなどに対して）
・パスワード入力時に、他人に見られないよう留意する
＊使用情報機器の管理→使用台数、設置場所等、数の把握管理
＊離席、退社時等の機密性確保
・退社時や機器を使用しない場合は機器の電源を落とす
・在籍時も他者から情報がのぞきこまれない等、表示機器の向き、設置場所等にも配慮する
＊モバイル機器の持ち出し
・必要性を考慮した承認ルールの明確化
・ＨＤＤパスワードを設定する
・ローカルＩＤ「Administrator」にもパスワードを付ける
・セキュリティパッチを常に最新に保つ
・アンチウイルスソフトも設定する
・パスワード付きスクリーンセイバーを設定する（5 分以内）
・不必要なファイルは常に削除する
・常に「ごみ箱」の内容も削除する
＊私有機器の持ち込み
・原則禁止、必要があれば承認ルールの明確化（最低限上長もしくは職場ＰＣ管理者の許可を得る）
＊情報機器のネットワークからの切り離しおよび盗難防止
・長時間使用しない機器は、ネットワークから切り離す

・外部から持ち込んだ機器は、ネットワークに接続しない。もしくは徹底したセキュリティ対策を施す。

＊着脱可能なメディアの管理

・外部メモリ、ディスク、カード等着脱可能な外部記憶メディアの取り扱い管理ルールを設定

・USB メモリの使用制限　情報セキュリティ委員会**によりセキュリティロックを掛け配布された** USB メモリを使用する。**今後バックアップ先はファイルサーバーに統合される予定であるが、現段階において可能な原則的方法とする。**

・USB 接続等のモバイル HDD 使用の場合、情報セキュリティ委員会に報告の上、本体へのパスワードロックをかけること。ロックソフトについては情報セキュリティ委員会に相談すること。大量の個人情報、企業情報である場合、その紛失、破損については USB メモリ以上に多大なリスクを伴うので、使用に関する責任は重大であることを自覚すること。私物の USB 接続等のモバイル HDD は使用禁止とする。

＊机上の整理

＊ネットワークセキュリティの確保（サーバー保全も含め）

＊ネチケットの遵守

＊無線 LAN の接続

・接続、使用ルールの明確化

＊コンピューターウイルス対策

・サーバー及び各パソコンでの、定期的かつリアルタイムのウイルスチェックの実施

・ウイルス感染時は直ちにネットワークから切り離す（ネットワークケーブルを抜く）

附則

1.　この医療法人誠心会情報セキュリティ基本方針は、平成 24 年 7 月 1 日から施行する。

2. 内容全般について改訂した第 2 版は、平成 26 年 2 月 1 日から施行する。

３、内容全般について改訂した第３版は、平成 27 年９月 1 日から施行する。