情報システム・ネットワーク管理規定

1. 目的

当院の情報システム・ネットワークのセキュリティを確保する。

2. 責任

個人情報管理責任者及び情報システム部門は、情報システム、ネットワークのセキュリティを確保する責任を持つ。

3. システム体系

(1) 当院の情報システムとネットワークの全体は、別紙情報システム・ネットワーク図で管理する。
(2) Web など対外情報発信サーバーは、セキュリティ上信頼できるホスティング業者にアウトソーシングする。
(3) 特例の場合を除いて、院内 PC の接続は LAN で接続し、ルータ経由でインターネットに接続する。

4. セキュリティ対策

(1) インターネット等外部との接続点にはファイアーウォールを設置し、外部からの進入を防止する。
(2) 外部からのウイルスに感染したファイル等の監視のためにウイルス監視システムを稼動させる。
(3) PC の使用は、ID、パスワードでの利用者認証を行う。
(4) 院内 LAN でのサーバー接続、ダイヤルアップ接続などでは、ID、パスワードでの利用者認証を行う。
(5) パスワードは一定期間内に変更する。
(6) システムの特権 ID は、情報システムの管理者が管理する。
(7) Web などで、顧客と個人情報のやり取りする場合は、SSL 等で暗号化する。
(8) 個人情報管理責任者の承諾を得ないで、個人情報の目的外利用、第三者への提供・預託、通常の利用場所からの持ち出し、外部への送信等の個人情報の漏えい行為をしてはならない。

5. ユーザー管理

(1) 従業員に貸与するパソコンに必要なセキュリティの設定など初期化を行う。
(2) 個人情報管理責任者は、従業員に対して業務に応じて必要な ID、パスワード、アクセス権限を決定する。
(3) ユーザーID、初期パスワード、アクセス権限は、情報システム部門の管理者がシステム設定して、従業員に直接手渡す。
(4) ユーザーID、初期パスワードは、情報システム部門の管理者が台帳で管理する。この台帳

は個人情報管理責任者以外の一般従業員に開示してはならない。

(5) 従業員の ID、パスワードが不要になった場合、情報システム部門の管理者は即日 ID、パスワードをシステム設定から削除する。

6. システム管理

(1) 情報機器やネットワークの設置場所、接続を管理する。

(2) 情報機器やネットワーク、ソフトウエアの導入について、機能、性能、信頼性、品質の確認を行い、判定基準を決め、受け入れ検収を行う

(3) ソフトウエアのライセンス契約内容を確認し、ライセンス管理を行う。

(4) ソフトウエアのバージョン管理、インストール管理を行う。

(5) 情報機器やネットワーク、ソフトウエアについて、保守方法を計画し、必要な保守契約を結ぶ。

(6) システムの運用については、運用管理者が運用手順を決め、運用担当者はそれに沿って、運用操作を行う。運用について、実施内容と引継ぎ事項、その他気付き事項について記録して、管理者に報告する。

(7) システムの障害やセキュリティの問題・違反などのセキュリティ事故の発生を監視し、適切に対処、是正、予防の処置及び記録を行う。

(8) セキュリティ事故の原因調査、セキュリティ違反検出、セキュリティ事故防止のために、必要なログを常時採取するようシステムを設定する。また、ログは定期的に監視を行い、違反や不正なアクセスなどがないかチェックする。

(9) セキュリティの情報、技術動向、ソフトウエア修正情報をウォッチし、当院の対応の要否を検討する。

(10) 情報機器やネットワーク、システムの性能、効率を把握し、改善・更改の要否を検討する。

この規程は、平成 17 年 4 月 1 日より施行する。

改定履歴

平成 17 年 4 月 1 日　作成および施行

平成 22 年 4 月 1 日　一部改定

平成 24 年 4 月 1 日　一部改定

令和 6 年 4 月 1 日　一部改定