セキュリティ事故の検出と是正・予防処置規定

1. 目的

個人情報保護マネジメントシステムに基づいて、セキュリティ事故の検出に対する職員の義務を規定すると共に、セキュリティ事故発生時の対処をすみやかに実施し、業務の迅速な復旧と事業の継続を図る。また、適切な予防を図る。

セキュリティ事故とは、下記のことやその疑いをいう。

① ウイルス感染、不正アクセス、従業員による情報漏洩など人的行為の事故
② ソフトウェア障害、ネットワーク障害、ハードウェア障害などの偶発事故
③ 情報機器、機密書籍などの紛失及び盗難事故

2. 責任

個人情報管理責任者は、役員や従業員の義務の認識を図り、セキュリティ事故の早期発見による、適切な対処と業務の迅速な復旧を図らなければならない。

3. セキュリティ事故の監視

(1) 全ての従業員は、セキュリティ事故等を早期に検出するために、セキュリティの問題やその技術・運用上の必要性を認識し、適度なリスク意識を持ち、適当な監視を心がける。
(2) 情報システム部門はウイルス対策ソフトや最新の定義を配布する仕掛けを構築し、従業員は業務上利用するコンピューターについて、適切にウイルス検査を実行する。
(3) 情報システム部門は、将来起こりうる調査やアクセス制御の監視に役立てるために適切にログを取得し、定期的また必要時に点検を行う。

4. セキュリティ事故への対処

(1) 従業員は、セキュリティ事故を検出した場合は、情報システム部門および個人情報管理委員会に速やかに報告する。(フロー参照)
(2) セキュリティ事故発生時の対策は、情報システム部門が中心になって、その影響範囲の極小化と業務の回復を重視し、以下の活動を行う。

① 関連部署に報告して、各部門の協力を得て対応する。
② 影響を食い止めるための処置をとる。
③ 業務の影響と事業継続のための処置をとる。
④ 問題の除去を行う。
⑤ システムの回復を行う。

(3) セキュリティ事故発生時の対応レベルを、被害の深刻度に応じて、レベル分けする。従業員、情報システム部門、個人情報管理委員会はレベルに応じた報告先に対し、速や
(4) かに報告し、指示を仰ぐ。

(1) 深刻度：大
事業そのもの継続に大きな影響がある場合。または、顧客や取引先等の病院外に対して病院が加害者となる場合。
●報告先：情報システム部門、個人情報管理委員会、該当する顧客や取引先、警察関係、コンピュータ緊急対応センター(JPCERT)、情報処理推進機構(IPA)、
東京都保健医療局医療政策部医療安全課　電話 03－5320－4432（直通）
日本情報処理開発協会（JIPDEC）

(2) 深刻度：中
通常の業務の遂行に影響がある場合。または、病院外の第三者からのセキュリティ侵害により、病院が加害者となる場合。
●報告先：情報システム部門、個人情報管理委員会、該当する顧客や取引先、警察関係、**東京都保健医療局医療政策部医療安全課　電話 03－5320－4432（直通）**
●任意報告先：コンピュータ緊急対応センター(JPCERT)、情報処理推進機構(IPA)

(3) 深刻度：小
業務の一部に影響があったもの。かつ、問題の発生原因・被害の範囲とも病院内に限定される場合。
●報告先：情報システム部門、個人情報管理委員会

(4) セキュリティ事故については、発見者及び関連者が「セキュリティ事故報告書」に記載して記録する。

5. セキュリティ事故の再発防止

(1) 個人情報管理委員会および情報システム部門は、セキュリティ事故の被害状況等をもとに再発防止計画を作成し、適切に実施するために関係者、従業員に周知させる。
(2) 個人情報管理委員会は、発生したセキュリティ事故の内容・状況及び再発防止計画の記録を保管・管理する。

6. セキュリティ事故の予防

(1) 従業員は、ノート PC や機密資料等の情報資産を紛失しないように、適切な管理を行う。
(2) 情報システム従業員は、日常的にセキュリティ情報を収集し、病院内で使用しているソフトウェアに対しての対応を判断し、必要なパッチの実施、バージョンアップ作業を行う。
(3) 情報システム部門は、万一の場合の復旧作業に役立てるために、適切にバックアップを取得する。バックアップは災害などを考慮して別の場所に保管する。また、バックアップからの復旧訓練を定期的に行う。
(4) 情報システム部門は、不正アクセスを検知するために、侵入防止・侵入検知システムおよびネットワークの監視のための対策を検討し、実施運用を行う。
(5) 情報システム部門は、重要なシステムに対して冗長化構成、電源対策などを講じる。
(6) 個人情報管理委員会は、定期的にセキュリティ教育と対応訓練を計画し、実施する。また、訓練結果の報告、改善策の審議を行う。
(7) セキュリティ事故は、定期的に個人情報管理委員会に報告し、是正処置、予防処置の必要性について検討する。是正処置、予防処置が必要な場合には、具体的な内容と責任者を決めて、「セキュリティ事故報告書」に記録するとともに、事故からの学習として従業員に教育を行う。

7. セキュリティ事故防止に対する従業員の義務と違反時の処置

(1) 従業員は業務上適切な管理義務を果たすことによって、セキュリティ事故の防止と事故発生時の影響の低減に務めなければならない。また、セキュリティ事故を招くような行為及び、それと疑わしい行為をしてはならない。
(2) 本規定の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については就業規則の賞罰の規定に従う。

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 17 年 7 月 1 日　一部改定
平成 22 年 4 月 1 日　一部改定
平成 24 年 4 月 1 日　一部改定
平成 28 年 4 月 1 日　一部改定
平成 30 年 4 月 1 日　一部改定

部門責任者→情報システム部門→個人情報管理委員会

セキュリティ事故報告書

作成　　年　　月　　日

発生場所	発生システム	発生日時	発見部署　　氏名
事故現象			報告書番号

業務影響度	業務停止時間	処置
☐ 重大 ☐ 大 ☐ 中 ☐ 軽 ☐ 微･無	☐ 無 ☐ 有 （　　時間　　分）	☐ 無操作 ☐ 続行 ☐ 再実行 ☐ 停止し保留

☐ システムダウン　☐ サービス停止　☐ スローダウン　☐ ファイル・出力不正　☐ ウイルス検出
☐ 異常・エラー　☐ ネットワーク障害　☐ 機器故障　☐ 電子機器・媒体紛失　☐ 不審者　☐ システムダウン
☐ その他のセキュリティ問題

事故の詳細報告

事故が発生する前にあった事象（オペレーション・環境変更・状況変化・特異現象など）

保存・採取資料
☐ 業務ログ　☐ 業務パッケージログ　☐ OSシステムログ　☐ ネットワークログ　☐ 運用監視ログ　☐ 状態表示
☐ 画面ハードコピー　☐ メッセージ　☐ 入力データ　☐ 出力データ　☐ 印刷結果
☐ その他（　　）

事故に対する応急処置と結果	担当	承認

事故発生原因

事故発生結果に対する処置・完了予定日・実施責任者

事故原因の再発防止策（是正処置）・完了予定日・実施責任者

是正処置結果確認・確認日	担当	承認

予防処置 ☐ 不要 ☐ 必要（右記）	予防処置・完了予定日・実施責任者

予防処置結果確認・確認日	担当	承認