情報漏洩・情報セキュリティ事故の対応フロー

情報事故

速やかに連絡する
※事故当日に行うこと

- 情報漏洩の事故の発生
- 漏洩の可能性が確認された場合
- 紛失・盗難・盗聴が確認された場合
- 情報漏洩の事故の発生

情報システム部門責任者
個人情報管理責任者

- 情報セキュリティ事故の原因究明
- アクセスログの収集・分析
- 問題のあるパソコンをネットワークから隔離
- システム障害がある場合の復帰

セキュリティ事故レベルの判定

- 深刻度：大
  事業の継続に大きな影響がある場合。
  患者や取引先等の病院外に対して病院が加害者となる場合。
- 深刻度：中
  通常の業務の遂行に影響がある場合。
  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。
  業務の一部に影響があったもの、且つ問題の発生原因・被害の範囲とも
  病院内に限定される場合。

個人情報管理委員会

- 深刻度：小の場合（修正・復帰）

- 緊急委員会を開催し、情報セキュリティ事故の対応を検討
- 病院長への連絡
- 影響を受ける可能性のある本人（患者等）への連絡
- 広報によるセキュリティ事故の公表
- 関係機関への報告（義務）
- 特別問い合わせ窓口の設置（セキュリティ事故問い合わせに対応）

報告・公表

セキュリティ事故報告

- 深刻度：大・中の場合は下記への報告義務あり
  該当する患者・取引先・警察
  東京都保健医療局医療政策部医療安全課　03-5320-4432
  個人情報保護委員会　03-6457-9685