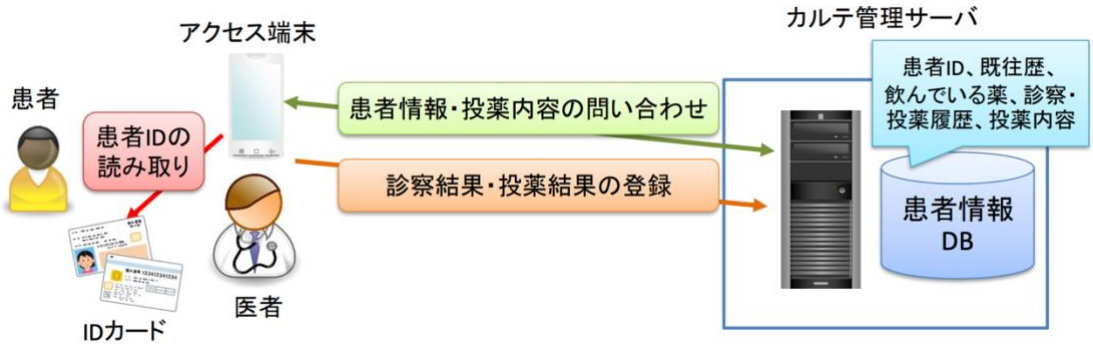
情報セキュリティー応用レポート 1

◆ 医療システム

- (訪問)診察
  (1)アクセス端末を用いて、患者のIDカードを読み取って患者IDを取得
  (2)患者IDを用いて、アクセス端末から患者情報(既往歴、飲んでいる薬、診察・投薬履歴など)をサーバに問合せ
  (3)患者を診察して、診察結果をアクセス端末に入力して、サーバへ送信・DBへ登録
- 投薬
  (1)アクセス端末を用いて、患者のIDカードを読み取って患者IDを取得
  (2)患者IDを用いて、アクセス端末から患者への投薬内容をサーバに問合せ
  (3)投薬内容にしたがって、投薬を実施
  (4)投薬結果を、アクセス端末に入力して、サーバへ送信・DBへ登録



(1)(情報)資産を列挙せよ。

1.物理的資産:
患者の ID カード
アクセス端末
カルテ管理サーバ
2.データ資産:
患者 ID、既往歴、

飲んでいる薬、診察・

投薬履歴、投薬内容
3.ソフトウエア資産:
医療システムソフトウェア
患者データベース管理ソフトウェア
4.人資産:
医者、カルテ管理サーバ管理者、システム保守運用者

(2)対策の優先度が高い脅威を 3 つ挙げよ。また、それぞれの理由を答えよ。
1. データセキュリティの脅威; その理由は、ID 認証システムが完全ではなく、システム境界にアクセスするときに ID を認証できないためです。
2. 外部ネットワークからのブルート フォース クラッキング、ウイルス侵入などのネットワークセキュリティの脅威により、ネットワークシステムが麻痺する。
3.応用セキュリティの脅威: システムの緊急サポートがなければ、システムがクラッシュしたときに情報が失われる可能性がある。

(3)上記で挙げた脅威に対する対策をそれぞれ述べよ。

データセキュリティ対策
1. アプリケーション システムの識別とアクセス制御
パスワードの複雑さの検証機能を追加し、動的パスワード、CA 証明書、指紋などの別の識別技術を追加する。
2. データの機密性
データリソースの機密性に従って分類され、公開、内部、秘密、機密の 4 つのレベルに分けられる。
3. データのバックアップと復元
病院のデータ使用要件に従って、データの可用性、有効性、および整合性を確保するために、データをオンライン、ニアライン、およびオフラインで保存できます。本番データとバックアップ コピー データを同じ物理デバイスに保存することは避ける。

ネットワークセキュリティ対策
ネットワーク侵入防止検出、防御およびセキュリティ監査
ネットワークベースの侵入防止システムを展開し、アラーム機能を有効にして侵入を防ぎ、ネットワークファイアウォールの背後に展開して、ネットワーク上のトラフィックを検出して防御する。

応用のセキュリティ対策
クラウドコンピューティング サービスをインポートして、偶発的なシステムクラッシュが発生した場合のデータ損失を回避する。