資料２

標準医療情報に必要なセキュリティ対策と情報流通

一般社団法人日本ハッカー協会
合同会社エルプラス

杉浦　隆幸

標準医療情報に必要なセキュリティ要件

1. 大規模な情報漏洩を発生させない
2. 預かった個人情報が守られる
   利用者(全医療従事者)**250万人**を想定　→ 利用者にセキュリティ要件を求めてはいけない
3. 小規模・低予算でも安全に利用できる
4. 業務効率が向上し本来の業務により時間がさけるようになる
5. 習得コストが低い（→使ってみようと思えばすぐに利用できる）

要件を満たすには

1. 基本無料でオープンな実装が継続的に開発運用されている
2. セキュリティや運用方法を考えないで導入・運用を可能にする
3. 初期状態で十分なセキュリティが確保できる
4. 機器や通信費など維持コストが負担にならない金額
5. サポートや代行などの有償サービスで情報弱者をカバーする

電子カルテのセキュリティ

- クラウド電子カルテ、レセプトのクラウド化により、医療情報がインターネット接続されている。[閉域網ではない]
- 十分なセキュリティ対策がされている可能性は低い
- 患者の知らないところで情報利用や漏洩の可能性
- インターネット接続状態でのセキュリティ対策が必要
  - OSが最新の状態になっている
  - アプリケーションの継続的なセキュリティ対策がされている
  - IoT化された医療機器に対するセキュリティ対策が必要
  - 積極的に脆弱性が発見されている

プライバシーポリシーに関して

医療機関利用時のプライバシーポリシー

①医療機関の提供者の名称、連絡先等

医療法人●●病院

東京都千代田区●●町●－●－●

②医療機関が取得する情報の項目

患者の氏名・生年月日・住所・電話番号・保険機関名・保険番号・診療情報・検査結果・処方情報・レセプト（氏名・生年月日・保険機関名・保険番号・診療情報・処方情報）

③医療機関が取得する方法

診療、検査、保険証の提示

④利用目的の特定・明示

⑤第三者提供およびその目的

レセプトを保険適応のため：各医療保険機関・社会保険診療報酬支払基金・**国民健康保険団体連合会**

特定の診療情報を症例研究のため：A研究機関

レセプトを高齢者の医療の確保に関する法律に基づく提供のため：厚生労働省から国の機関や大学の研究者に提供

処方情報を薬の処方のため：利用された調剤薬局

第三者の名称と連絡先

⑥同意取得の方法及び利用者関与の方法

⑦問合せ窓口

医療機関の電話番号、メールアドレスなど

⑧プライバシーポリシーの変更を行う場合の手続

機械的に生成されたフォーマットであれば、将来的に情報提供者が情報を誰に提供したのか人が読まなくても明確になる。

スマートフォン プライバシー イニシアティブを参考にした　http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html

情報は誰の所有物か

- 現状（データを保持している組織のもの）
  - 医療機関
  - クラウド電子カルテ会社
  - 保険機関・社会保険診療報酬支払基金

- 将来的
  - 患者本人および情報委託先（情報銀行など）
  - 医療機関
  - クラウド電子カルテ会社
  - 保険機関・社会保険診療報酬支払基金

クラウドストレージで
ファイルを本人のみ開示可能で公開

- カルテ（標準化が必要）
- レセプト
- 投薬情報
- 健康診断
- 診断書など

がん告知などは診療医の許可が必要

プロフィール情報
（都道府県・生年・性別）

公開鍵DBと通知サーバ

公開通知

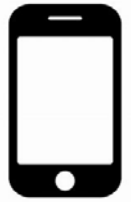
医療機関

マイナンバーカードや保険証・診察券の公開鍵で暗号化

ローカルストレージ

カード紛失時は、データのある医療機関で再アップロード可

PUSH
メールで通知



個人インデックスデータ

クエリー実行
：条件にあった場合は、来院や情報提供などができる。
解読にはカードが必要

救急医療時に、マイナンバーカードや保険証で承認し
全データの引き出しも可能

個人のスマートフォン等

情報銀行に委託可

クエリー発行：去年インフルエンザに罹患
実行：データ処理用プログラム送信

データ分析機関

情報提供に関しては、データ分析機関は料金を支払い、その何割かは、情報提供者のポイントにできる。

その他明確にしておく必要がある項目

- セキュア設計
  - 脆弱性を生まない設計、開発体制
  - 長寿命なIT医療機器に対応できるように、長期間システムを放置しても脆弱にならないように設計する必要
  - 頻繁なシステムの更新に耐えられる設計
  - 素人でも、セキュリティの心配をしなくてもよいようにする
- 使用できるOS
  - しっかりとメンテナンスされるOS(Windows, iOS, Ubuntu Linux ［AndroidはGoogleのデバイスのみ］)を対象とする
  - OSが最新の状態であればウイルス対策はすでに入っており後付けは不要
- 利用者のセキュリティルール
  - 標準的なセキュリティ：最新のOS最新の状態で利用し、業務以外に利用しないだけで安全に運用できる。
- 脆弱性管理
  - 脆弱性が見つかっていないシステムほど、脆弱性が多い。
- クラウドベースで構築
  - オフラインでも使用できるようにする。（災害時や故障時を考慮）
  - 電子カルテやレセプトがクラウド化しており、閉域網にインターネットが接続されており多数の利用者がいる閉域網はすでに閉域網ではなくなっている。
  - それ故、標準医療情報のシステムもクラウドベースでも設計したほうがメリットが大きい
- 各電子カルテの情報をどのように統合
  - 共通フォーマットの策定と閲覧機能（ビューワー）、コンバータの整備を行う必要がある。
  - 他システムでのビルドインが必要、Webでレンダリング可能にする方法がよい。

アクセス権

アクセス権者
医療機関
医者
医療従事者
患者
保険機関
支払基金
国民健康保険団体連合会
他の医療機関
他の医師

現在の認証
生体認証＋PKI PKI（ICカード） ID/パスワード

医療従事者すべての公開鍵基盤が必要

Web: ¥0~ 自動更新処理あり 数分
法務局: ¥7900/年 専用ソフトで窓口対応
日本医師会： ¥5000/年 郵送 1ヶ月以上
MEDIS:　¥50000/5年

失敗する認証基盤

普及していない or 強制力がない
発行に時間がかかる
費用負担があるもしくは、費用負担が現行のシステムに乗らない
パスワードや暗証番号を忘れると、復旧までに時間がかかる
仕様が公開されていない
不便

成功させるためには

関係者すべてに配布する
無料（無人で行えるもののみ）
オープン（仕様や作成方法など）
安全
大局で考え細かいことにとらわれない
とりあえず入れておくにしない

PKIの配布はICカードもしくは、
スマートフォンからのQRコードでもよい

外部データ連携のデータ暗号化

医療機関A

通信はTLSで暗号化

① 診療歴リクエスト

② 診療歴リスト

③ 診療情報リクエスト
Aの公開鍵付き

⑥ データストアの
位置(URL)を受信

⑦ 暗号化された医療
情報を受信

標準形式のビューワもしくは、変換して表示

データストア

個人向けデータ(PHR)

医療機関連携用データ
(EHR)

通信はTLSで暗号化

医療機関B
PHR
EHR

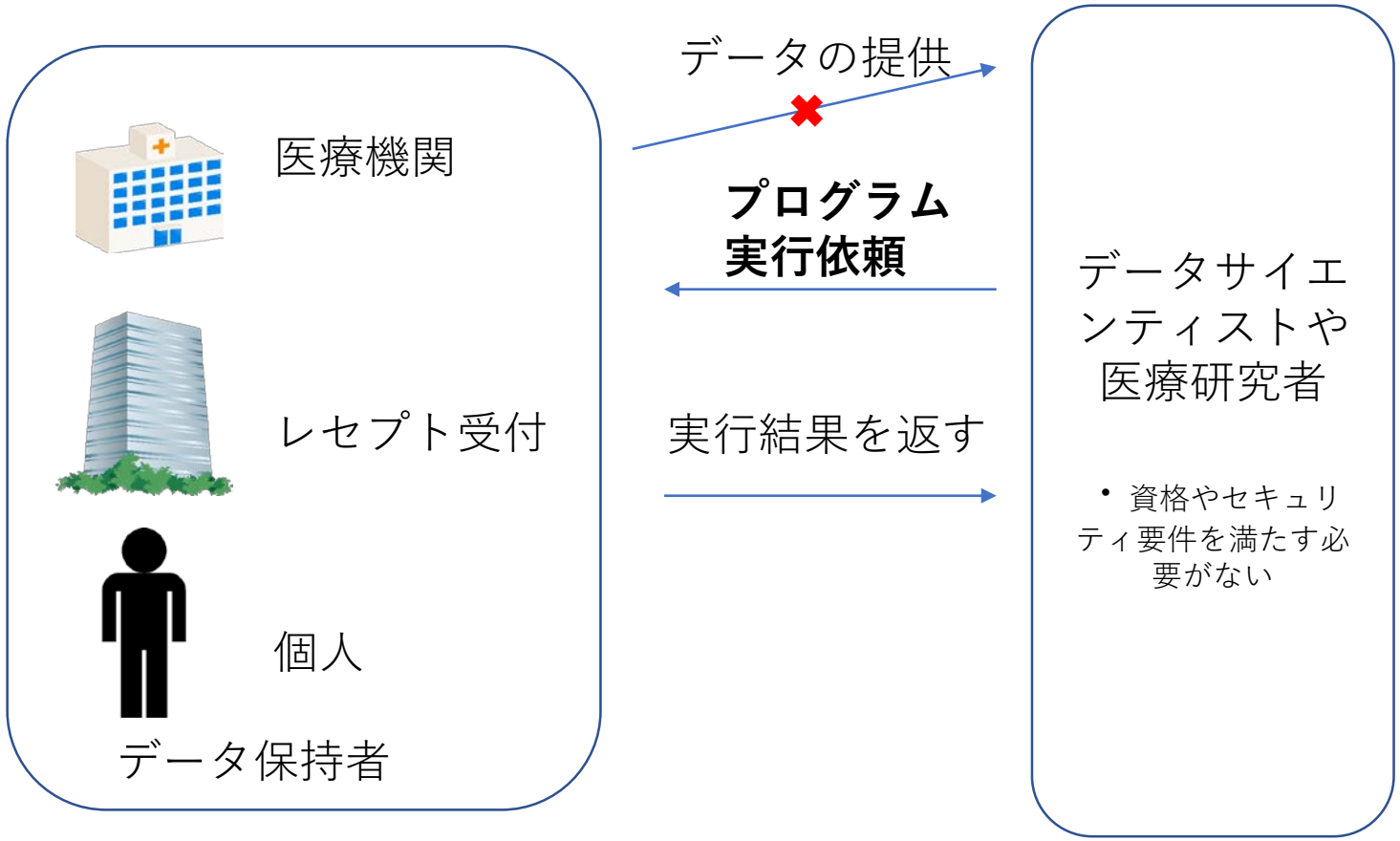
④診療情報要求

⑤ 医療機関Aの公開
鍵で暗号化して送信

データストアでは、
平文の情報を保管しない。

通信の暗号化と、コンテンツの暗号化の2種類で、サーバでの情報保存を安全にする。

情報流通を加速するには



・医療以外の専門家を参入させることができる。

動作検証用データセットや実行環境作成手順などが事前テストができる情報の提供が必要

データ保持者自身が統計処理をするのであれば問題は少ない
統計利用であればデータ所有者にプログラムを実行してもらう方法がよい
医療では広告のようなリアルタイム性(数十ms)は必要ない