保健医療福祉分野PKIと連携する医療用ネットワーク制御アプリケーションの開発

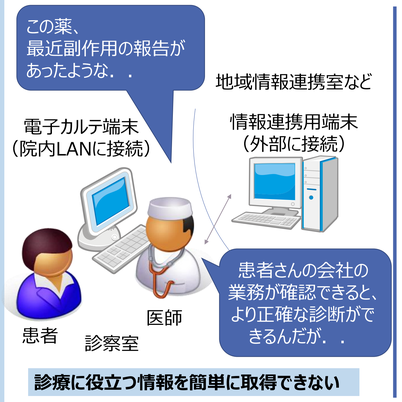
小尾高史、 李中淳、 鈴木裕之、 秋山大輔
東京工業大学 ソリューション研究機構　統合型医療情報ネットワーク基盤構築プロジェクト、 社会情報流通基盤研究センター

背景

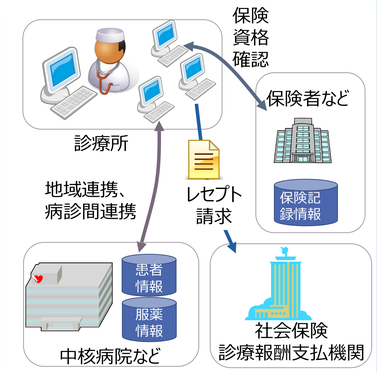
- 医用分野での様々な業務でネットワークが利用されている
  - レセプト請求用（審査支払機関向けネットワーク、多くの施設で利用）
  - 医療連携用（医療機関相互のネットワーク、一部地域で利用）
  - 保険資格確認用（保険者向けネットワーク、今後実施予定）
- 医療情報システムの安全管理に関するガイドラインでは
  - 医療機関等に対して、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ることや、ネットワーク機材の不適切な設定により意図しない情報漏えいや誤送信が起こるなどの危険性に対して適切に対応することが求められている
- これら業務には専用の端末が使用され、院内LANとも接続されていない
  - 医療機関内における各ネットワークの終端は、論理的にも物理的にも分離

➡ **一般的には、用途ごとに個別のネットワーク、機器を設置**

医療機関での現状



診療に役立つ情報を簡単に取得できない



専用端末と複数のネットワーク利用が必要

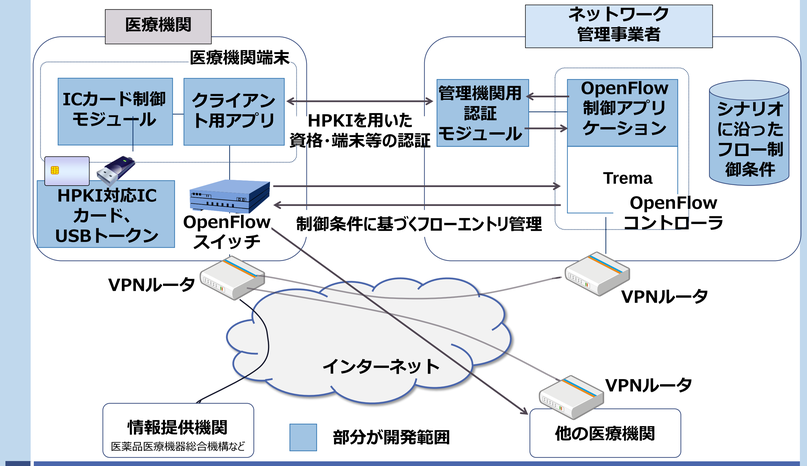
目的

- OpenFlow技術を利用
  - OpenFlowの柔軟なフロー制御により、様々なユースケースに対応可能
  - OpenFlowコントローラを利用した制御モデルが、医療分野で利用されている管理型VPNの管理モデルと類似
- 医療分野での適用には、
  - 医療機関における利用シーンを設定し、フロー制御の有効性を提示
  - OpenFlowコントローラによるフローテーブルの制御と利用者の認証情報などを連携させる仕組みの開発 ➡ **保健医療福祉分野PKI（HPKI）利用**
  - 管理機関と利用者である医療機関間の明確な責任分界点の検討

OpenFlowの持つ柔軟なフロー制御を、HPKIを利用した人・モノ・資格の認証に基づき実施することで、高度な個人情報である医療情報の流通へ対応可能な統合型医療用ネットワーク制御技術を構築

研究方法

- OpenFlowの持つ柔軟なフロー制御を、厚生労働省で策定された認証用途の保健医療福祉分野公開鍵基盤（Healthcare PKI、HPKI）を利用した人・モノ・資格の認証に基づいて実施することで、単一の回線上で高度な個人情報である医療情報の流通を可能とする新たな医療用ネットワーク制御アプリケーションを開発
- 本開発では、利用シーンとして病診連携を想定した医療情報連携での利用、現在多くの診療所、調剤薬局で利用されているレセプト申請及びレセプト申請用端末のリモートメンテナンス、さらに、医療機関内の端末からの医薬安全情報の参照を設定
- これら利用シーン毎に、診療所などの小規模な医療機関における利用シナリオを定め想定される脅威の分析を実施
- フローテーブルの制御条件を検討し、事前に設定するべき情報、フロー制御を行うためのルールの定義、ルール照合に基づき書き込むフローエントリの内容を決定
- 医師等が利用する端末上で動作するPKI認証モジュール及びOpenFlowコントローラ（Trema）と連携して動作するOpenFlow制御アプリケーションを開発
- 開発アプリケーションを使用して，資格や端末の認証と連携したフロー制御の検証、評価を実施



結果

実験システムの全体構成

HPKI相当の証明書を格納したICカード

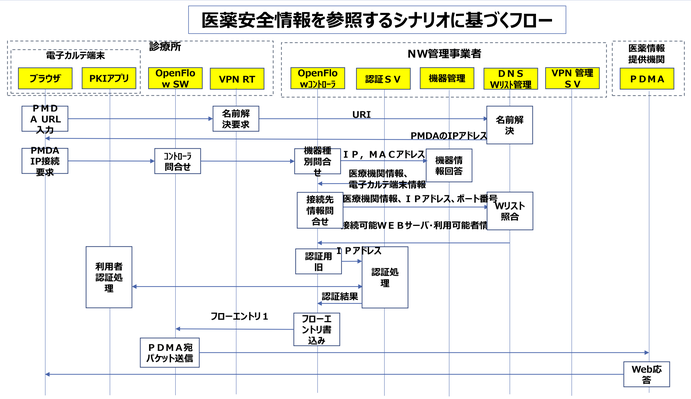
ネットワーク管理事業者

医療機関

- 開発システムを用いて、本ポスターで示した医薬安全情報の参照シナリオ及びそれ以外のシナリオについて、ユースケースに基づき決定したフローを正しく実現できていることを確認した
- 医師のHPKIを用いることで、許可された人のみが、認められたサービスを、自らの意思で利用できることを確認した
- 外部からの接続においては、機器等の認証を利用して、正しい機器に確実に接続することを保証可能であることを示した

結果

医薬安全情報を参照するシナリオに基づくフロー



まとめ

- 本研究の成果により、医療機関内及び医療機関と外部を接続する際のネットワーク制御を実施することが可能となり，保健医療福祉分野PKIによる認証と組み合わせることで、医療機関・医療従事者とネットワーク事業者間においてネットワークの安全性に関わる責任分界点を定めることができ、医療情報の安全性担保に対する責任の所在を明らかにできる
- 本研究の成果は、ネットワーク管理者を置くことが難しい小規模の医療機関、薬局などへの導入が期待でき、全国の医療機関等をネットワーク化するための重要な基盤となる
- 今後、個人番号カードのインフラを利用する在宅医療の展開などを想定し、Network Function Virtualization(NFV)技術と組み合わせて、タブレットなどの携帯端末を含めた医療用ネットワーク技術の構築を目指す