TOKYO TECH
Pursuing Excellence

第5回社会情報流通基盤研究
センター・シンポジウム

HPKI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

国立大学法人 東京工業大学

東京工業大学

ソリューション研究機構

李中淳

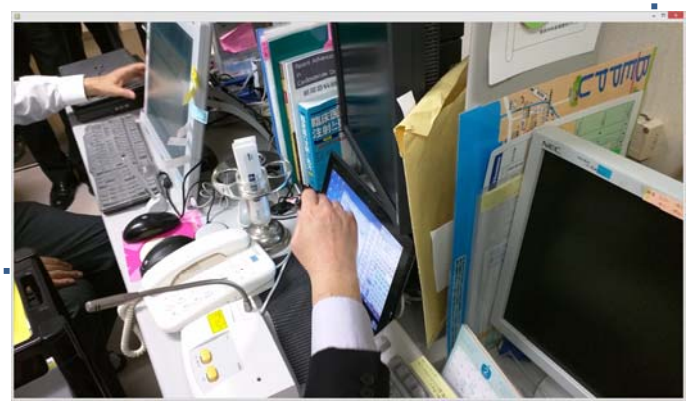
ASIST
Assist in improving the information quality

医療分野のネットワークの現状

- 様々な業務におけるネットワークの外部接続
  - ○　レセプト請求用（審査支払機関向け、実施）
  - ○　医療連携用（医療機関相互向け、一部実施）
  - ○　保険資格確認用（保険者など向け、未実施）
- 外部接続に専用の端末を使用
- 院内LANと論理的、物理的に分離
- 用途ごとに独立のネットワーク機器、回線を設置

- 使用上の不便さと費用の問題

診療中に電子カルテ端末から、外部の情報を参照することが出来ない。



医療情報システムの安全管理に関するガイドライン

- 医療機関が外部と接続する際に必要な**ネットワークの要件**
- 伝送途中での情報漏えいなどの**危険性**に対して適切に**対応**
- **責任分界点**の明確化

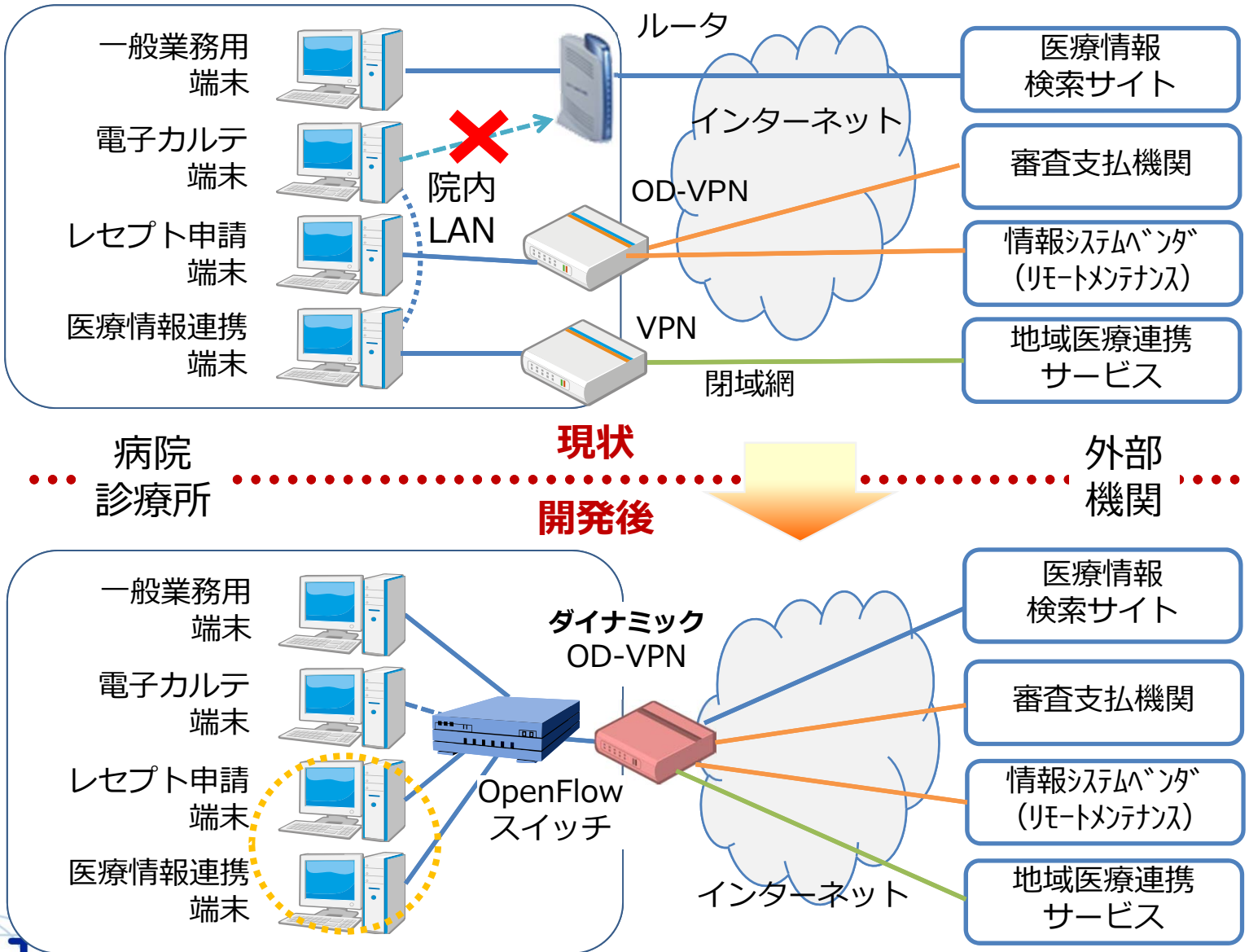
オンデマンドVPNサービス

ガイドラインに唯一合致した
インターネットを利用した医療分野のネットワークサービス

現状のオンデマンドVPN

- **任意の拠点間**をオンデマンドに **VPN 構築**
- **内部ネットワークのルーティング制御**や**様々なプロトコルの制御**には関与しない。その故、**複数の論理回線**の**設定**が困難。
- 内部ネットワークを介した**回り込み**の危険性を**回避**できない。

統合型医療用ネットワーク制御

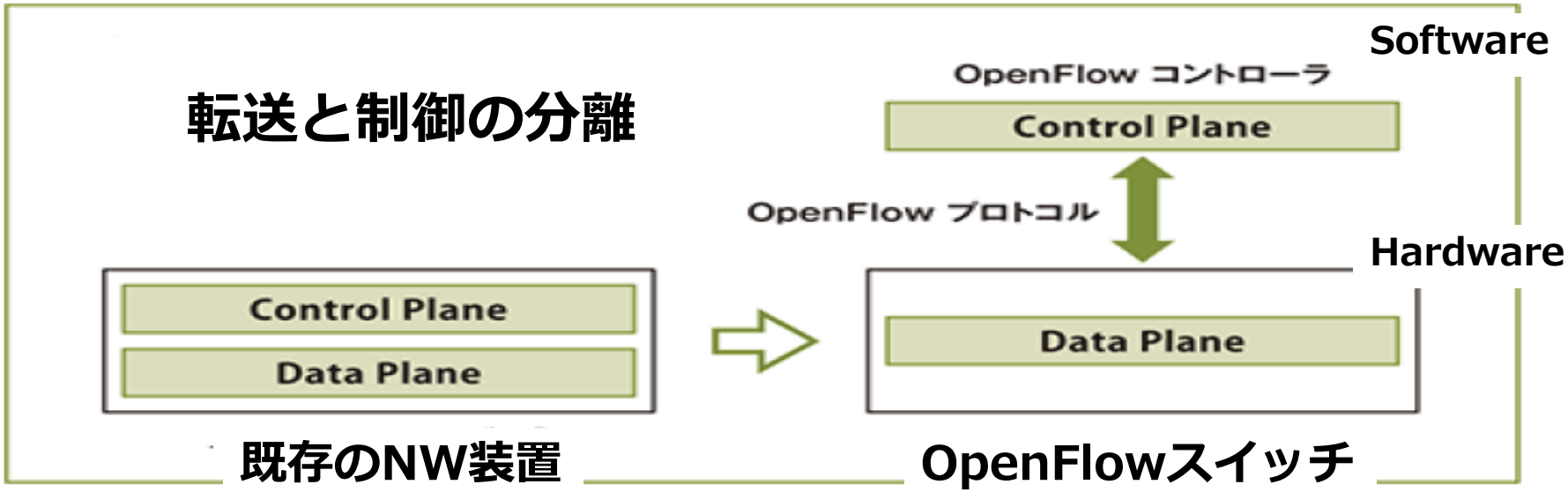


ネットワーク制御技術の検討

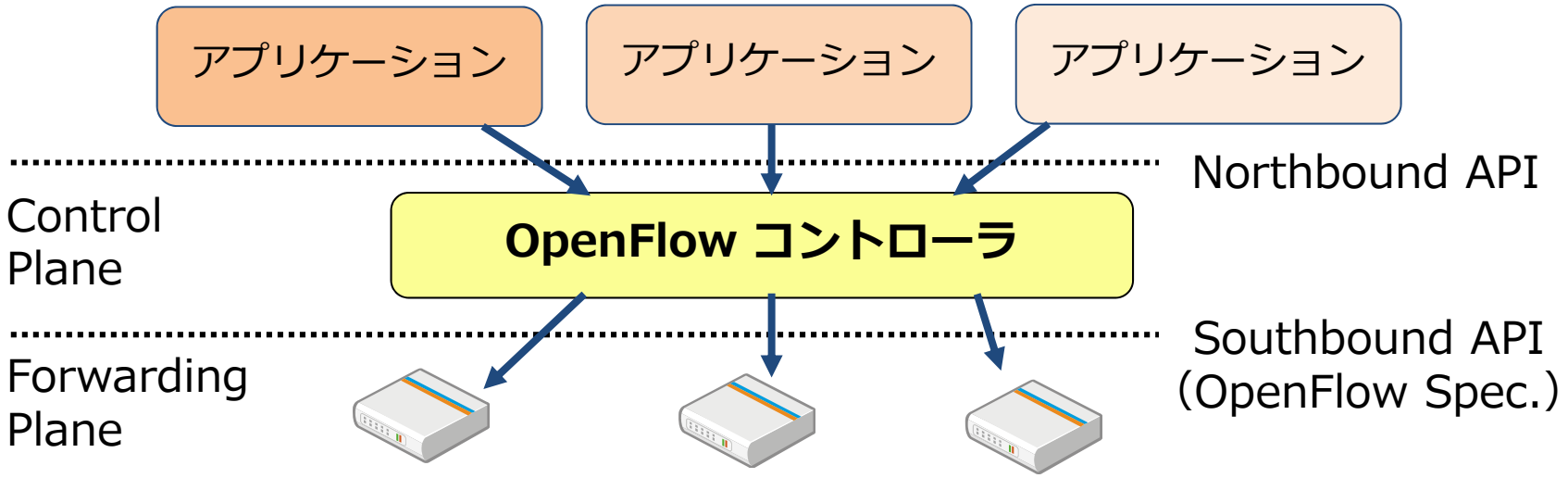
- 従来のネットワーク仮想化技術
  - VLAN
    - レイヤ２での仮想化
    - 個々のフレームにタグ（ VLAN ID）を挿入して識別
  - VRF：Virtual Routing Forwarding
    - レイヤ３での仮想化
    - 1台のルータの中に、仮想的に複数台のルータ（ルーティングテーブル）を作成
    - 個々のルーティングテーブルは、物理ポート又は論理ポート（VLAN）と関連付け
- 従来技術の課題
  - VLAN ID数の制限（MAX 4,096）
  - 制御手法が標準化されていないため、設定の自動化が困難
  - 柔軟なネットワーク構成をとることができない

OpenFlowの利用

- ネットワーク機器の経路制御機能とパケット転送機能を分離
- 経路制御を行う OpenFlow Controller と、転送機能を担当する OpenFlow Switch が、標準化された制御プロトコル（OpenFlowプロトコル)で接続
- OSI参照モデル L1 ～ L4 の要素を利用してフローを制御
- ネットワークをサービス形態に合わせて自由にかつ一元的に管理可能
- OpenFlowの制御をアプリケーションから実現



OpenFlowネットワーク



OpenFlow 対応ネットワーク機器類

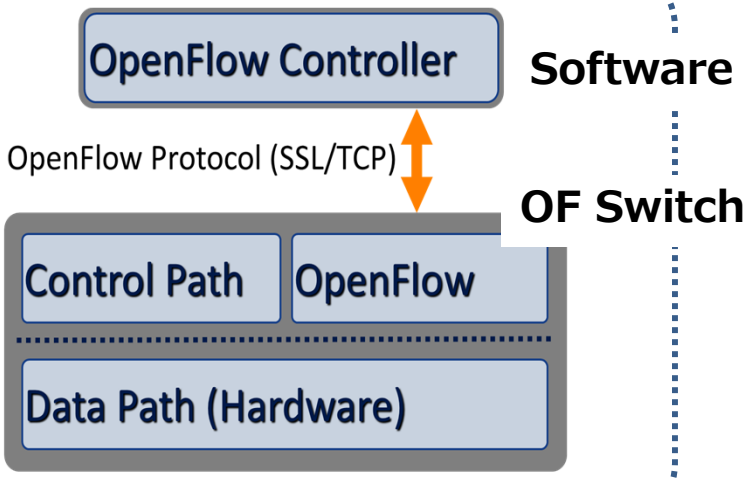
OpenFlow

Open Networking Foundation

- スタンフォード大学発祥、
- 現在 **ONF** による標準化
- 2009年　Ver. 1.0
- 2013年10月　Ver. 1.4

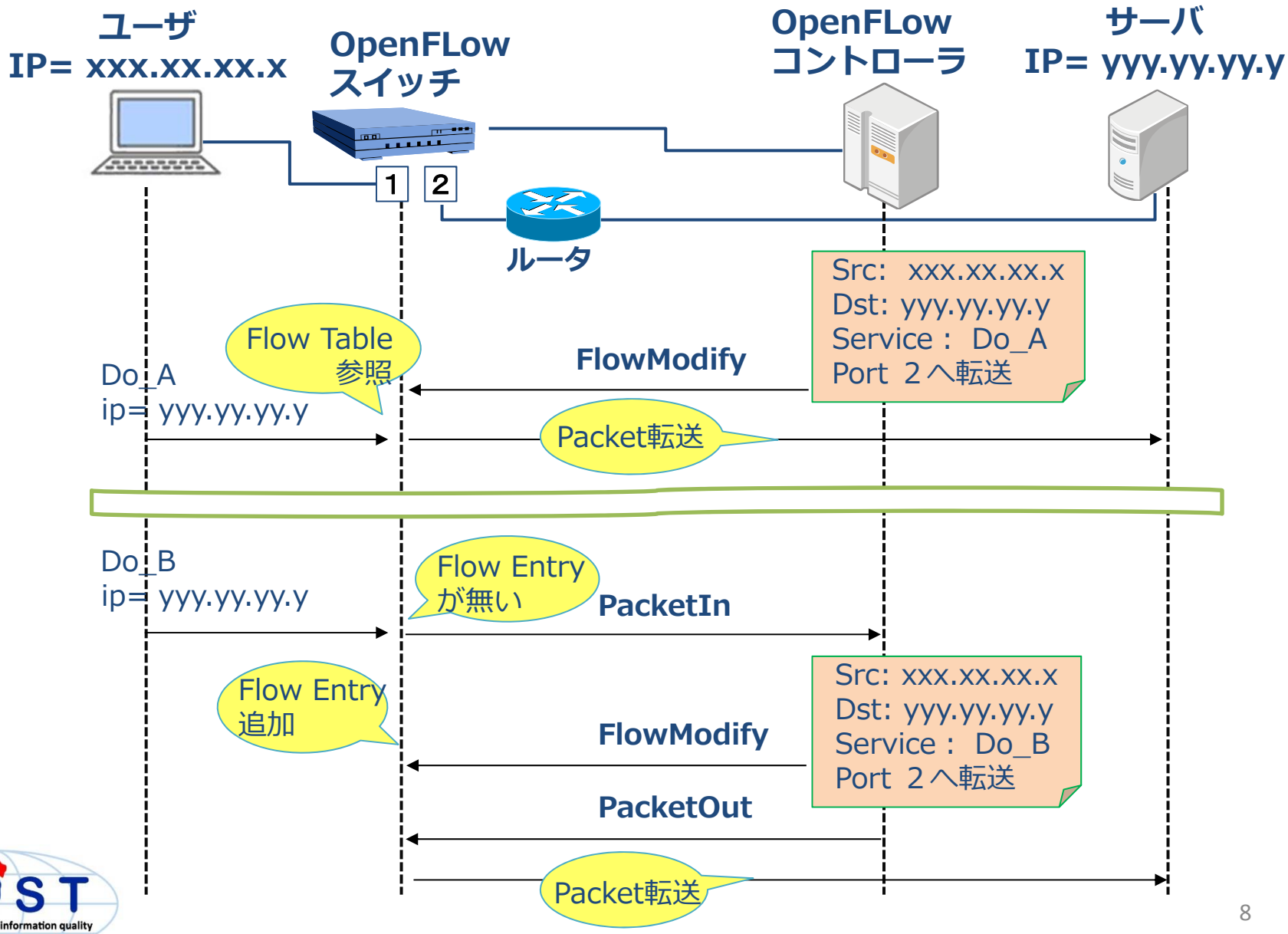
OpenFlow Framework

- **Trema**
- **POX**
- **NOX**
- **Floodlight**



ASIST
Assist in improving the information quality

OpenFlowネットワークの動作



フロー制御のマッチングルールに使われる項目

名前	説明	レイヤ	使用
Ingress Port	スイッチの物理ポート番号	L1	○
Ether src	送信元 MAC アドレス	L2	○
Ether dst	宛先 MAC アドレス	L2	○
Ether type	イーサネットの種別	L2	○
VLAN id	VLAN ID	L2	
VLAN priority	VLAN PCP の値 (CoS)	L2	
IP src	送信元 IP アドレス	L3	○
IP dst	宛先 IP アドレス	L3	○
IP proto	IP のプロトコル種別	L3	○
IP ToS bits	IP の ToS 情報	L3	
TCP/UDP src port	TCP/UDP の送信元ポート番号	L4	○
TCP/UDP dst port	TCP/UDP の宛先ポート番号	L4	○

医療分野での適用

ネットワークのフロー制御

OpenFlowとオンデマンドVPNの連動

管理機関と医療機関間の明確な責任分解点の検討

HPKIによるユーザ認証

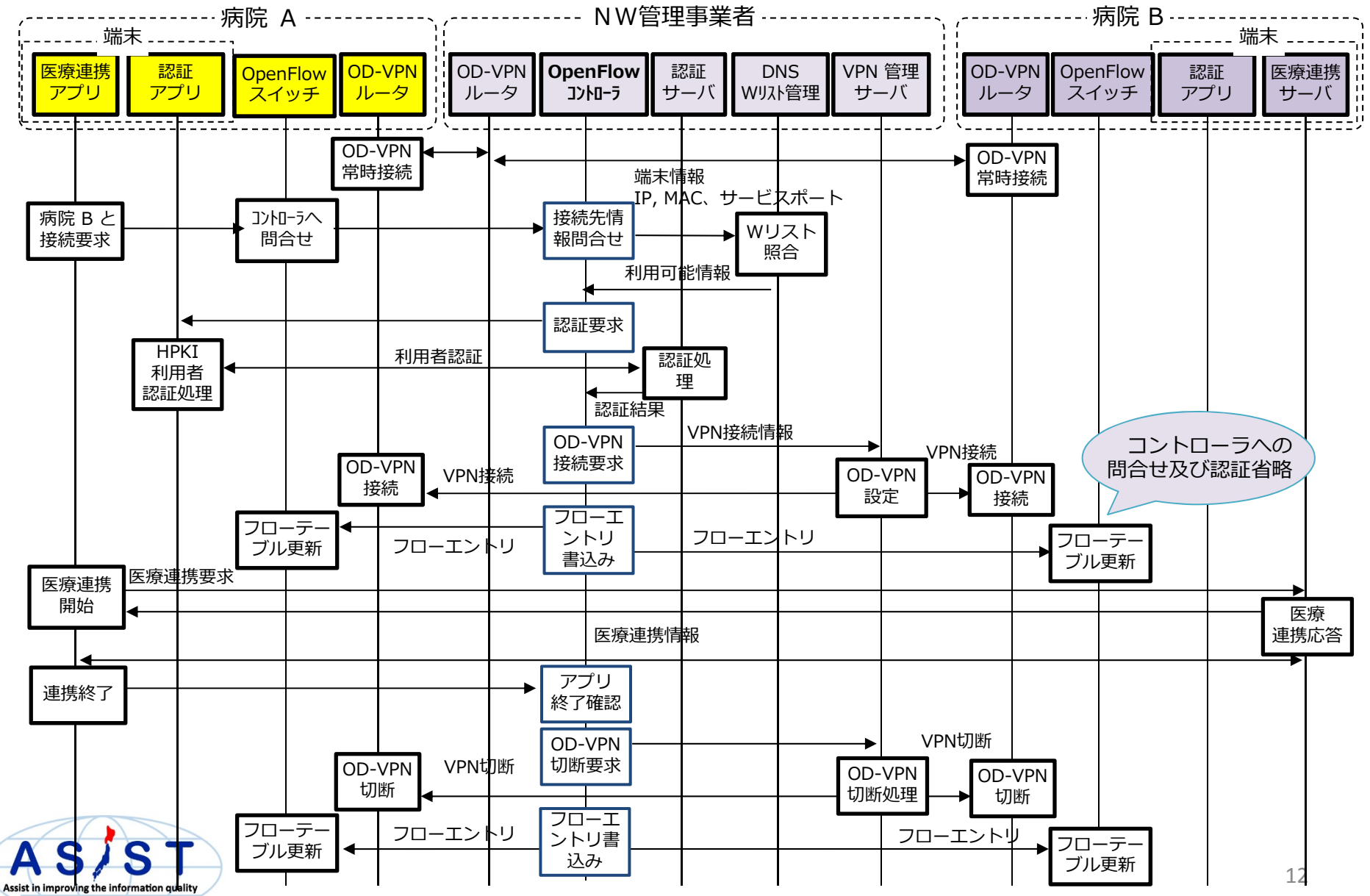
医療機関と外部機関を接続する利用シーンを設定し，
医師などの資格や医療機器の端末認証などに基づいて，
オンデマンドVPNと連動してOpenFlowスイッチ上のフローテーブルを制御するOpenFlowコントローラ上のアプリケーションを開発

OpenFlowの持つ柔軟なフロー制御を
HPKIを利用した人・モノ・資格の認証に基づいて実施し，
オンデマンドVPN技術を組み合わせることで，
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

研究開発内容

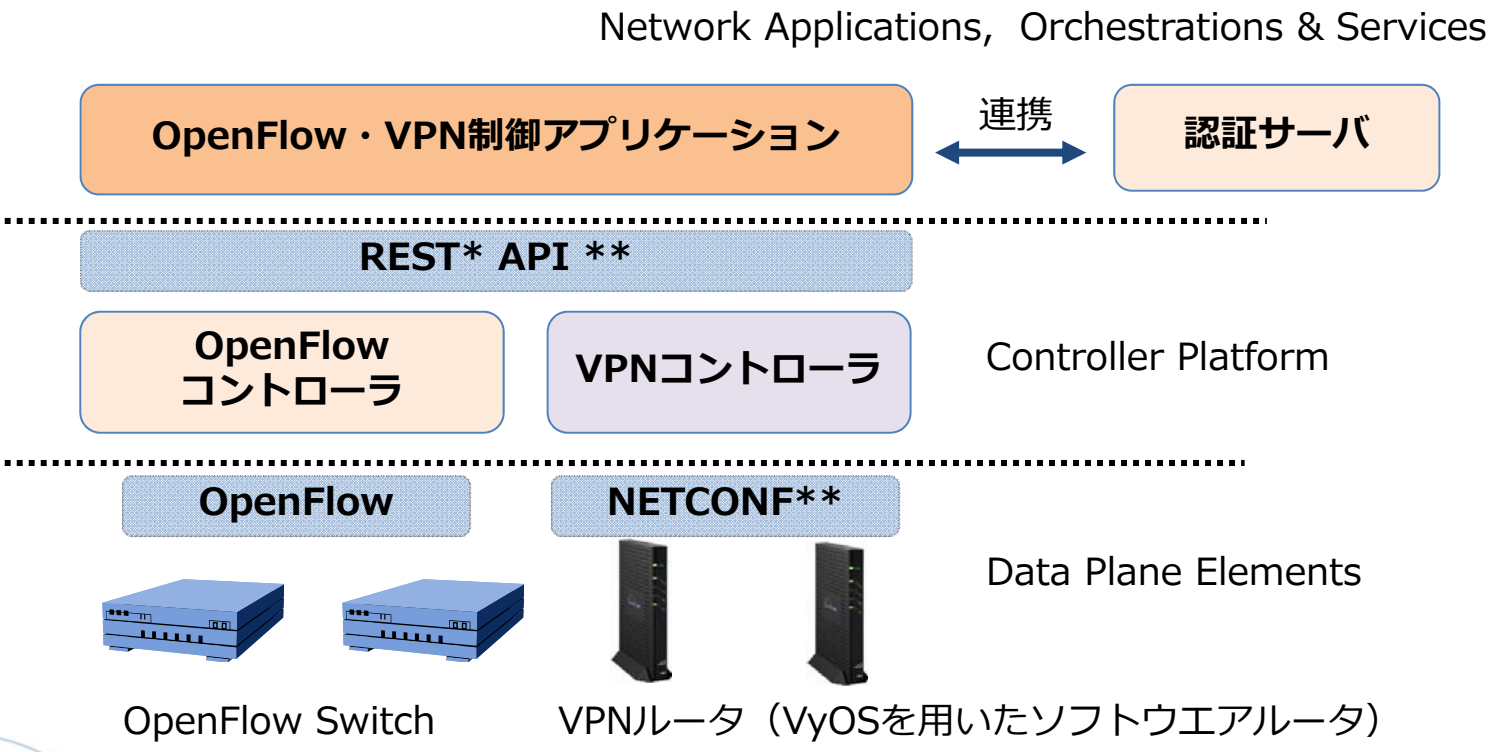
1. 想定されるユースケース
   （平成25年度：医療情報連携、レセプトのオンライン請求、レセプト端末のリモートメンテナンス、医薬安全情報の参照、平成26年度：保険資格のオンライン確認、電子処方箋の運用について，VPNとの連動時に必要となるフロー制御を検討）
2. HPKI認証・VPN制御連携OpenFlowコントローラ用アプリケーションの開発と評価
3. 医療機関等における開発成果の適用可能性に関する調査・分析

医療情報連携シーケンスの例



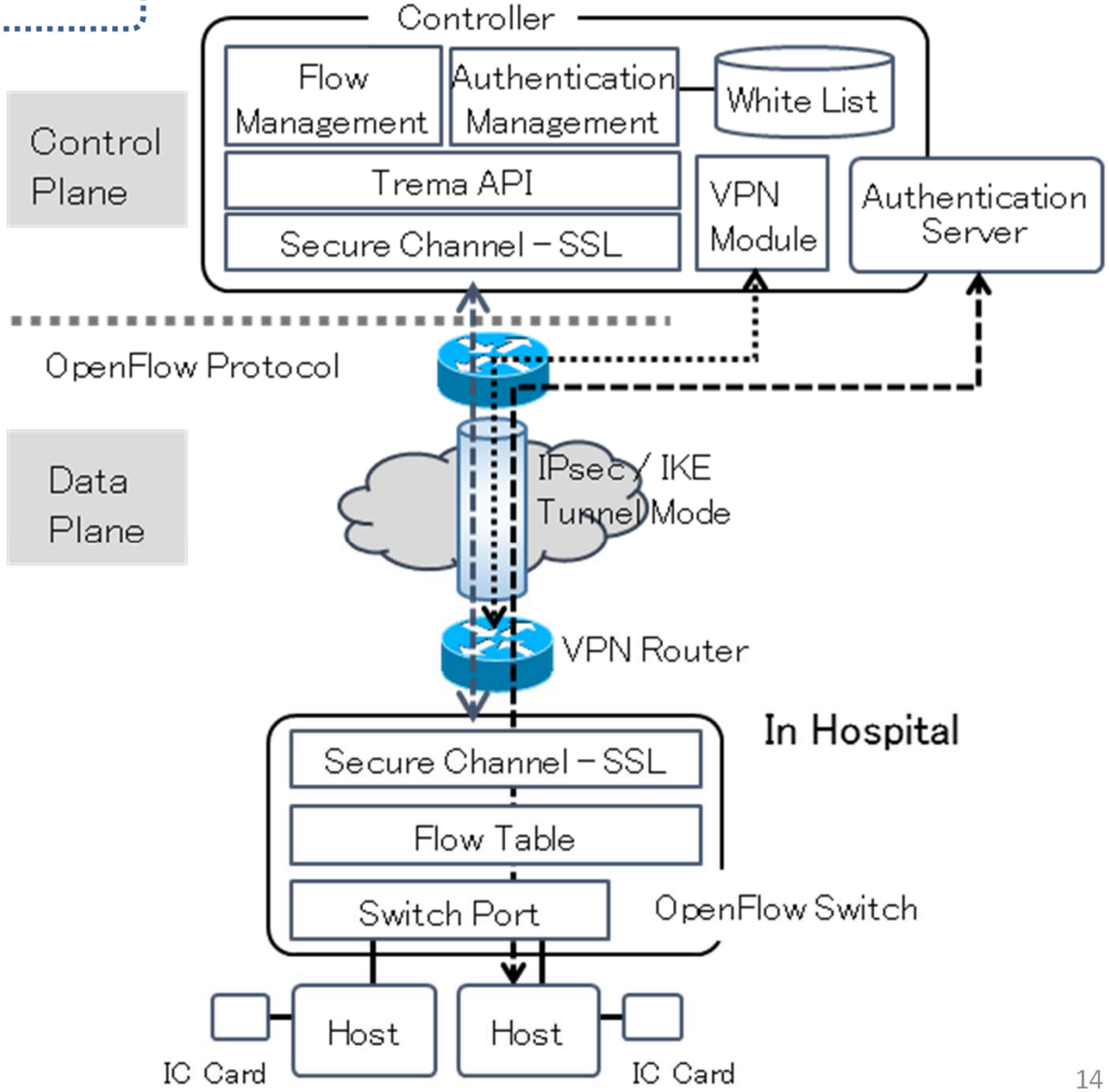
OpenFlow・VPNルータの同時制御

- OpenFlow、管理型VPNともに経路制御(VPN制御）機能とパケット転送機能が分離
- 経路制御をコントローラが、転送機能をSwitch、ルータが担当
- OpenFlowコントローラを利用した制御モデルが、OD-VPNの管理モデルと類似

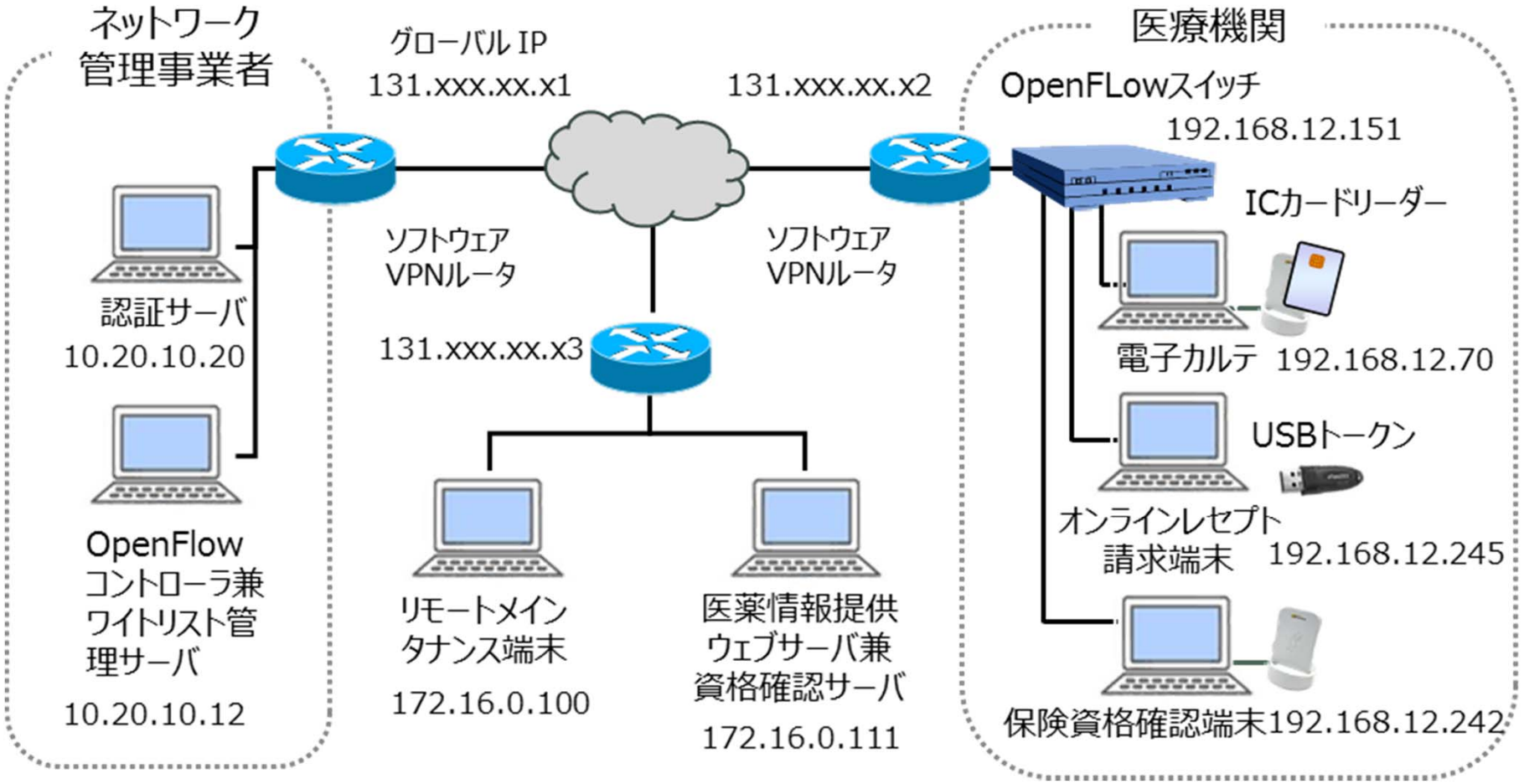


* *REST:Representational State Transfer*　　** 本年度の実装では、代替インターフェースを利用

アーキテクチャー


Controller
Flow Management
Authentication Management
White List
Trema API
Secure Channel – SSL
VPN Module
Authentication Server
Control Plane
OpenFlow Protocol
Data Plane
IPsec / IKE Tunnel Mode
VPN Router
In Hospital
Secure Channel – SSL
Flow Table
Switch Port
OpenFlow Switch
Host
Host
IC Card
IC Card

実験システム構成図



- 拠点間はトンネルIP使用 （グロバルIP）
- 機関内部のプライベート IP 使用可能

実験システム写真

実験装置

- OpenFlowコントローラ及び管理サーバ
  Linux (Ubuntu 12.04　64ビット) PC
- NW管理機関のサーバ
  Windows 7, 8 PC数台
- 認証デバイス
  ・ICカード：医師会発行 HPKI 証明書搭載非接触カード（ISO/IEC 14443）

pica8 p-3290

OpenFlow スイッチ

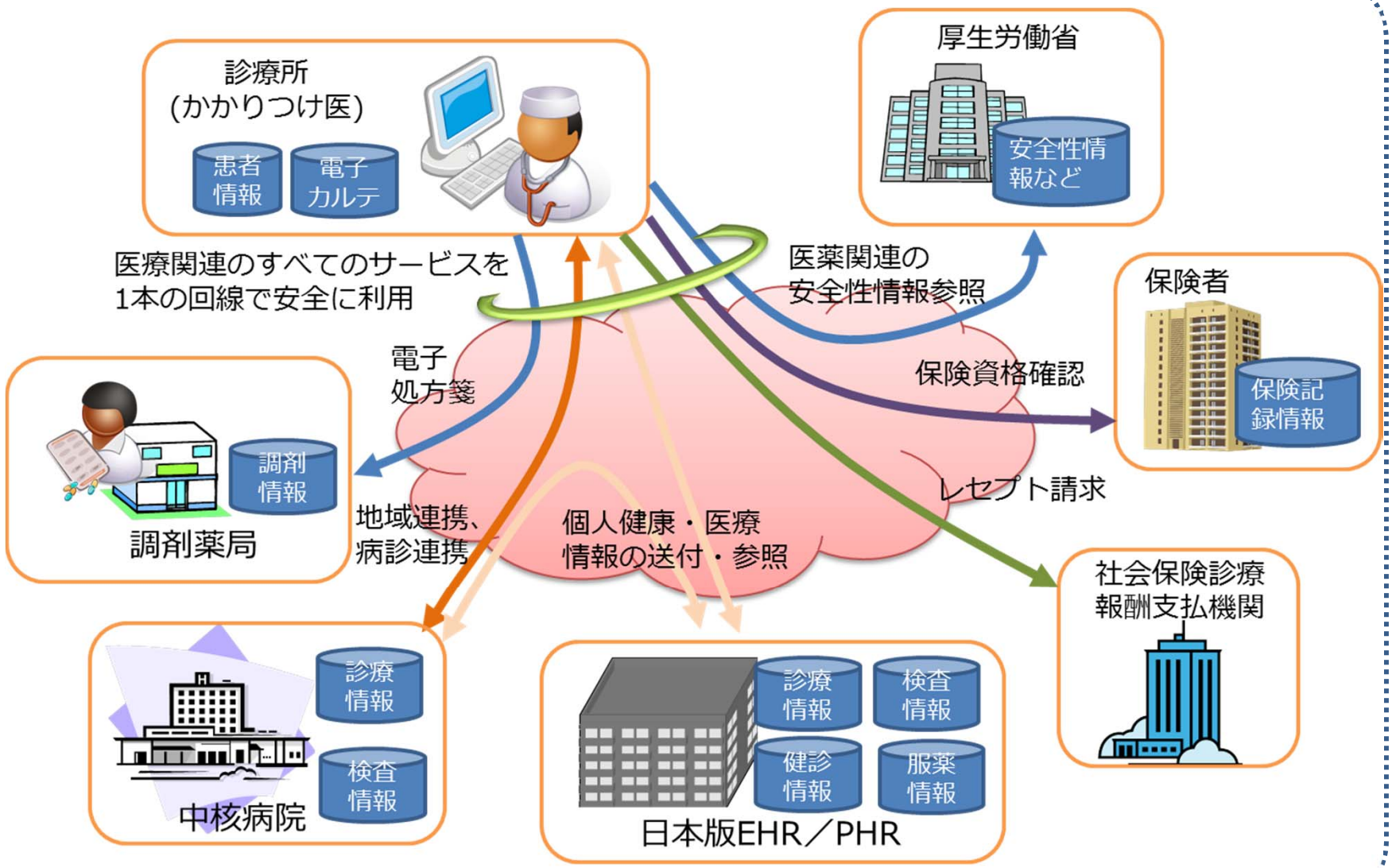
- 48ポート 10/100/1000BASE-T インタフェース
- 4ポート 10GbE （SFP+）インタフェース

実験装置

ソフトウェア・VPN ルータ

- **VyOS 1.1.0**
  Vyattaから派生したオープンソースのネットワークOS
- EPSON Endeavor ST170E
- PLANEX UE-1000T-U3
  （USB-LAN アダプタ）

本研究開発による医療情報NW基盤の整備



安全安心な医療情報の連携・流通を可能とするネットワーク基盤の実現

期待される効果

- 医療機関内部及び医療機関と外部を接続する際ネットワーク制御を実施可能
- HPKIなど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医療情報の安全性担保に対する責任の所在を明確化可能
- 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、医療機関等をネットワーク化するための重要な基盤技術となる可能性

医療分野における様々なネットワークサービスの創出を期待

今後に向けて

- 様々な医療向けサービスの新規導入時期と合わせて、新たな医療向けネットワークサービスとして展開することを想定した協力体制の構築
- 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、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
- 実証実験等を通して技術的評価，安全性評価を行い，ガイドラインなどへの反映・標準化等の実施

謝 辞

本研究は、総務省先進的通信アプリケーション開発推進事業の支援を受けて行ったものです。

関係各位に感謝いたします。