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（140202002）

Development of network controller application for medical information system cooperating with healthcare PKI

研究代表者
小尾高史　東京工業大学 像情報工学研究所
Takashi OBI　Tokyo Institute of Technology

研究分担者
李　中淳†　大山永昭††　鈴木裕之††
Joong-Sun LEE,　Nagaaki OHYAMA,　Hiroyuki SUZUKI
東京工業大学 †統合研究院　††像情報工学研究所
Tokyo Institute of Technology

研究期間　平成 25 年度～平成 26 年度

概要

本研究開発では、OpenFlowの持つ柔軟なフロー制御の仕組みと管理型VPNの持つ安全に任意多地点でのVPNを構成する仕組みを、保健医療福祉分野の公開鍵基盤（HPKI）と組み合わせて制御することで、1本の物理的ネットワーク回線上で統合的に医療用のネットワークを提供する技術を開発し、その有効性を示した。また、管理型VPNサービスを提供するネットワーク管理事業者と協力し、統合型医療ネットワーク実現に向けた検討を行った。

１．まえがき

厚生労働省から出されている「医療情報システムの安全管理に関するガイドライン」(以下、「厚労省ガイドライン」という）では、医療機関同士が接続する際に必要なネットワーク要件、外部から医療機関内部のネットワークに接続するための要件などが示されており、オンデマンド VPN（任意多地点間でオンデマンドに暗号通信路を構築する技術）は、このガイドラインに合致する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として、現在、民間企業 4 社がサービスを行っている。

しかしながら、医療分野で利用されているオンデマンド VPN などの管理型 VPN 技術は、医療機関等に設置された外部接続用ルータ間で安全な VPN を設定するための技術であり、暗号通信路上を通る様々なプロトコルの制御や院内ネットワークのルーティング制御などを想定したサービスではないため、複数の論理回線（ここでは、暗号通信路上で提供される特定のサービスのために使用される仮想的な通信回線をいう）を設定することができない。ここで、上記ガイドラインは、医療機関等における留意事項として、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を求めているが、一般的に管理型 VPN では、複数のネットワーク利用サービス、例えば、院内システムのリモートメンテナンスや医療機関間の情報連携などを同時に利用した際に生じる、ルータを介した通信の回り込みの危険性や意図しないサーバへの接続の可能性を想定していない。

このため、現在多くの医療機関は、レセプト申請や地域内医療連携などの異なる用途には複数のネットワークを使い分ける、又は、ある用途で使用する際には特定の端末のみを接続するなどの措置を講じている。さらに、病院内 LAN からのインターネット接続も原則禁止されており、例えば、診療室に設置された PC 等から医薬品関連の最新情報を入手することや症例データベースの参照などを行うことはできない。

このような状況は、利便性の低下や医療機関に対する割高な費用負担を強いているだけでなく、現在政府が進める質の高い医療実現のための全国レベルでの医療連携や、公的 EHR(Electrical Health Record)・PHR(Personal Health Record)の構築などに必要となる、医療機関が安心して利用できる医療用ネットワーク基盤が事実上存在しないことを示しており、早急に新たな仕組みの開発を進める必要がある。本開発では、上記の課題を解決し、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の開発を目的とする。

２．研究開発内容及び成果

本研究では、OpenFlow の持つ柔軟なフロー制御の仕組みに加え、従来の管理型 VPN の持つ安全に任意多地点での VPN を構成する仕組みを組み合わせることで、様々な設定情報を安全に管理し、物理的には 1 本のネットワーク回線上で統合的に医療用のネットワークを制御する技術を開発した。そのために、利用シーンを取り上げ、その際の想定シナリオと VPN との連動時に必要となるフロー制御の検討、それに対応するフローテーブルの制御条件の検討を行った。検討した利用シーンは、医療情報連携、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並びに、医薬安全情報の参照に加え、番号制度により交付される個人番号カード（公的個人認証サービスの電子利用者証明の機能）を利用した保険資格のオンライン確認、平成 28 年の導入が検討されている電子処方箋の運用である。

また、想定シナリオ共通の脅威の他に、各シナリオ特有の脅威を抽出した。例えば、平成 30 年からの導入が検討されている個人番号カードを利用した保険資格のオンライン確認では、セッションハイジャックにより PIN コードを利用しない場合に行われる個人番号カードに対する機関認証時に、別サーバとの間でカードコマンドがやり取りされることによる別サービスでの個人番号カード利用の危険性が想定される。これら脅威に対処するために、ネットワーク管理事業者が保持すべき事前設定情報の整理、フローエントリ書込み処理時の制御条件等を定めた。保険

資格確認では、専用の保険資格確認端末が利用され、接続先が審査支払機関の提供する保険資格確認サーバとなる。また、接続者が許可された事務員または医師であることが認証された場合には、保険資格確認端末から保険資格確認サーバ間の接続を許可するとともに、レセプト請求端末と院内の他の端末の通信はすべて遮断するフローエントリを OpenFlow スイッチに書き込む処理を実施し、医療機関と審査支払機関間の VPN 接続を実施する。他の通信機器類からのセッションハイジャック等については、VPN とフローを連動して制御することで、防止することが可能である。そしてこれら検討を踏まえ、提案手法の拡張性、機能の独立性、共通性を整理し、医療分野で今後導入が予定される様々なサービスや、医療サービスのクラウドサービスとしての提供を見据えたネットワーク機能のサービス提供の仕組みを明らかにするとともに、セキュリティ障害に対応するための責任分界のあり方を検討した。

また、これら検討結果に基づき、管理型 VPN における鍵の配送から VPN ルータ間の接続・切断までの一連のプロセスを含めたフローの検討を踏まえ、VPN ルータと連動する HPKI 認証連携 OpenFlow コントローラ用アプリケーション、サーバ用 HPKI 認証モジュール及びクライアント用 HPKI 認証アプリケーション、ソフトウェア VPN ルータを開発した。

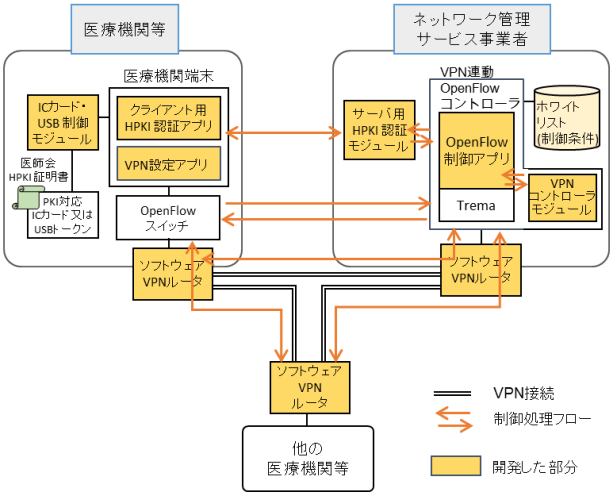

図１　開発したソフトウェアの関連図

OpenFlow コントローラ用アプリケーションは、ユーザが業務端末から外部接続を行う際に発生するデータパケットの制御のために、医療機関のセキュリティポリシーを基に作成されたホワイトリストに従って接続の有効性を判断し、OpenFlow スイッチのフローテーブルに当該のフローエントリを書き込むことでデータパケットの専用経路を確保する。HPKI 認証モジュールでは、この制御に関わるユーザ認証、資格認証に日本医師会が発行する実験用 HPKI 証明書を用いており、認証の際、日本医師会発行の証明書失効リスト（CRL: Certificate Revocation List）を参照して証明書の有効性確認を行っている。また、現在医療分野で利用されている管理型 VPN では、ルータ、コントローラ間のプロトコルが定められていないため、今後の拡張性等を考慮し、SDN の考え方に基づいて開発が進められている VyOS を用いるソフトウェア VPN ルータを採用し、IPsec に必要な暗号化アルゴリズムの決定と暗号鍵の交換を行っている。

そして、実験システムを構築し、実験的にユーザ資格や端末の認証と連携したフロー制御、VPN 制御の動作検証を行うことで、外部接続回線を含めたフロー制御が実現可能であることを確認した。

さらに、これら開発と並行して、医療向けネットワーク提供関連企業及び医療関連団体により構成される「保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム」（HEASNET）と定例会議を実施、また、HEASNET 情報交換会や、別途交付を受けている厚生労働科学研究費補助金による医療分野の共同研究者との会合において開発成果等を報告し、開発した技術の評価の実施、及び、本研究で実現を目指す統合型医療ネットワークのあり方の検討を行うとともに、今後の成果展開のためのロードマップを明確化した。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

本開発の成果展開については、平成 30 年以降の保険資格のオンライン確認の導入が検討されており、保険資格確認端末の普及のために、利用するネットワーク回線としては、既存のレセプト申請用有線回線を併用する方法や、新たに無線回線を導入する方法などが考えられている。このため、前者を実現するための具体的手法として、保険資格確認とレセプト申請の 2 つのサービスに利用を限定した本開発技術の実用化の検討や、後者を導入する際に必要となる保険資格確認端末と院内 LAN との接続への本開発技術の導入を優先的に進め、順次地域医療連携や電子処方箋など、他のサービスへの適用を図ることが適当であるとの結論を得た。

また、この場合には、厚生労働省ガイドラインの改定が必要かどうかも含めて、再度の影響調査が必要となることから、平成 27 年度は当初の予定通り、開発成果の厚生労働省ガイドラインへの影響調査を行い、平成 28 年から平成 29 年にかけて仕様の確定と一部検証実験の実施、そして、平成 29 年後半に保険資格確認とレセプト申請の 2 つのサービスを同一回線上で行うために必要となる技術評価基準を HISPRO などと協力して定め、平成 30 年度の商用サービスに備える計画である。

４．むすび

本研究では、単一の物理的ネットワーク回線上で統合的に医療用のネットワークを提供する技術を開発し、その有効性を示した。本研究の成果により、新たな医療情報ネットワーク基盤が構築可能となれば、確実な情報に基づく適切な医療を行うための基盤が整うこととなると期待する。

【誌上発表リスト】

[1] 李 中淳、 小尾高史、 鈴木裕之、 藤田和重、 谷内田益義、 大山永昭、“保健医療福祉分野 PKI と OpenFlow を連携した医療用ネットワークの提案”、情報通信マネジメント研究会 (ICM), 信学技報, ICM2014-17, pp. 7-11（2014 年 11 月 13 日）

[2] 李 中淳、 小尾高史、 鈴木裕之、 藤田和重、 谷内田益義、 大山永昭、“PKI ユーザ認証と OpenFlow 制御を用いたダイナミック VPN 構築手法の提案”, 情報ネットワーク研究会 (IN), 信学技報 114(373), IN2014-12-18, pp.35-39（2014 年 12 月 19 日）

[3] Joongsun Lee, Takashi Obi, Hiroyuki Suzuki, Kazushige Fujita, Masuyoshi Yachida, Nagaaki Ohyama, “A new method for constructing Dynamic VPN cooperating with OpenFlow control Technology and Healthcare PKI”, Asia-Pacific Network Operations and Management Symposium (APNOMS) 2015, Busan, Korea, 19 Aug. 2015