携帯型VPNルーターの開発

郡 隆之[1] 松井 英男[2] 浅尾 高行[3] 山口 雅浩[4] 菅野 好史[5] 嗣江 建栄[6]

[1]利根中央病院 外科 [2]川崎高津診療所
[3]群馬大学 がん治療臨床開発学講座 [4]東京工業大学学術国際情報センター
[5]NTTデータ・アイ [6]ViewSend ICT

Development of portable VPN rooter

Takayuki Kohri[1] Hideo Matsui[2] Takayuki Asao[3] Masahiro Yamaguchi[4]
Yoshihumi Kanno[5] Kenei Shie[6]

[1]Tone central hospital [2]Kawasaki Takatsu clinic [3]Gunma university
[4]Tokyo institute of technology [5]NTT DATA i corporation [6]Viewsend ICT

要旨

厚生労働省の「医療情報システムの安全管理に関するガイドライン 第4.2版」では、外部と個人情報を含む医療情報を交換する場合の安全管理に対してセキュアな通信路を確保することを求めている。医師が外出先の携帯端末から病院の端末にアクセスする際はソフトウェアレベルのセキュリティが用いられることが多い。今回我々はIPSec (Security Architecture for Internet Protocol) とIKE (Internet Key Exchange protocol) による拠点間接続が可能な携帯型VPNルーターと遠隔監視システムを開発した。WiFiおよび有線LANを利用した本機器によるVPN接続では通常接続の50-60%の通信速度が確保された。携帯型VPNルーターにより、携帯端末から場所を選ばず拠点間接続によるセキュリティの確立が可能となった。

キーワード：携帯型VPNルーター、IPsec、遠隔医療

1. はじめに

厚生労働省の「医療情報システムの安全管理に関するガイドライン 第4.2版」では、外部と個人情報を含む医療情報を交換する場合の安全管理に対して、1) 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること、2) セッション乗っ取り、IPアドレス詐称等のなりすましを防止する対策をとること、3) 上記を満たす対策として、例えばIPSec (Security Architecture for Internet Protocol) とIKE (Internet Key Exchange protocol) を利用することによりセキュアな通信路を確保することを求めている[1]。

そのため、遠隔画像診断を行うためには上記の条件を満たすセキュリティ環境の構築が必要である。保健収載されている遠隔画像診断加算では施設基準があるため、読影は施設内で行われており、施設間をIPsec + IKEによるVPN (Virtual Private Network) を設置型のVPNルーターで行うセキュリティ設定が一般的である。

近年、医師負担軽減や早期診断の目的で、医師が自宅や外出先の携帯端末からインターネット回線や3G回線などを用いたリモート接続で勤務施設の医療画像の閲覧が実運用されている[2]。これらのリモート接続では2点間で設置型のVPNルーターを用いてVPNを構築することは困難である。そのため、ソフトウェアレベルでのL2TP (Layer Two Tunneling Protocol) /IPsecを用いたVPNやSSL (secure sockets layer) による通信が利用されている。

L2TP/IpsecによるVPN構築ではホスト側のVPNルーターの機能によりIKEが利用不能なものがある。また、施設外からのリモートアクセスで利用する場合は端末の盗難による利用者の成りすましなどの対策も必要となる。

そこで、今回我々は厚生労働省のガイドラインを満たすIPsec + IKEを準拠したトンネルモードでVPN構築が可能な、設置型VPNルーターと同等のセキュリティ機能を有する外出先でのネットワーク環境に対応した携帯型VPNルーターと、携帯型VPNルーターの遠隔管理システムを開発したので報告する。

2. システム開発

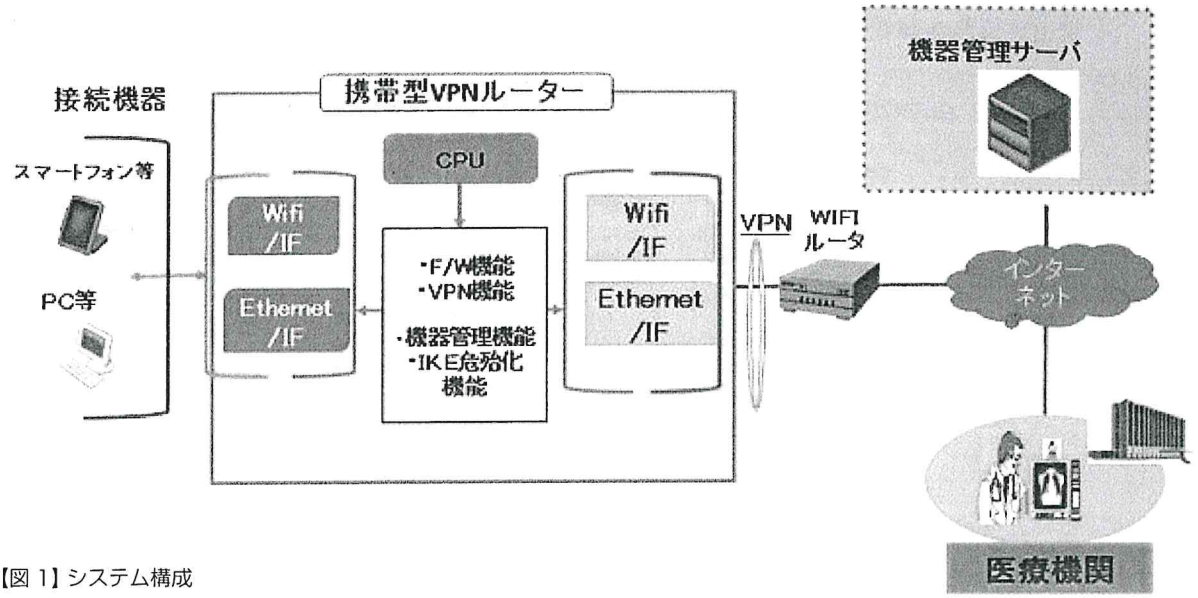
本システム開発は平成24年度から継続実施している経済産業省 課題解決型医療機器等開発事業「病院と医師間をリアルタイムで繋ぐセキュアな遠隔医療用画像診断支援システムの開発・改良」の一環で行われた。

携帯型VPNルーターは外出先でアクセスできるための以下の仕様を満たすものとした。

1) 医師が自宅および外出先でアクセスできるために有線LAN (Local Area Network)、無線LANおよび携帯端末のテザリング接続が可能
2) IPsec + IKEを用いた設置型VPNルーターと同等のセキュリティ機能を有したハードウェアによるトンネリングモードのVPN構築
3) USB端末からの電源確保
4) 携帯可能なサイズおよび重量

また、VPNルーターを介して接続する機器管理をする遠隔管理システムは以下の機能を満たすものとした。

1) サーバモジュール機能
   接続可否、死活確認、鍵更新、バージョン確認、VPN接続先検索



【図 1】システム構成

【表 1】携帯型 VPN ルーター仕様

VPN サポート 最大 10 回線の IPSec VPN トンネリング 最大 5 回線の PPTP VPN トンネリング IPSec VPN IKE：Pre-Shared keys IPSec Encryption DES/3DES/AES128/AES192/AES256 IPSec Authentication MD5/SHA1 NAT Traversal Wireless SSID Fire wall 機能

【表 2】遠隔管理システム　ソフトウェア構成

管理サーバー OS：Linux DB：My SQL5.5 Web サーバ：Apache 2 PHP5.3 アプリケーション 対象ブラウザ：WebKit 系 サーバ VPN ルーター YAMAHA RTX 1200 監視アプリケーションモジュール 1 Windows. NET Framework 3.5 C# アプリケーション 対象 OS：Windows7, Windows8 監視アプリケーションモジュール 2 Objective-C アプリケーション 対象 OS：iOS 7

2）監視アプリモジュール機能
　VPN 接続制御、VPN 接続状況モニタリング、アクセスルール制御、死活確認
3）サーバ管理画面機能

全体のシステム構成を【図 1】に示す。

3. 結果

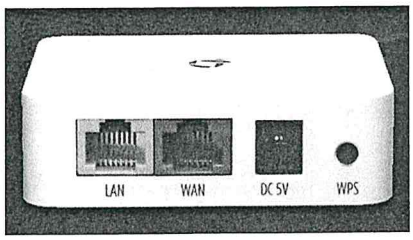
現在試作品を開発終了した。携帯型 VPN ルーターを【図 2】に仕様を【表 1】に示す。また、遠隔管理システムのソフトウェア構成を【表 2】に示す。

WiFi および有線 LAN に携帯型 VPN ルーターを接続し、IPsec ＋ IKE による VPN 接続における通信速度を複数地点で計測した【図 3】。上り速度下り速度とも非 VPN 接続時の 50-60%の通信速度が確保された【表 3】。

今年度本システムによるセキュリティーを用いて病院救急医療画像を施設外の医師が閲覧する実証実験を行う予定である。

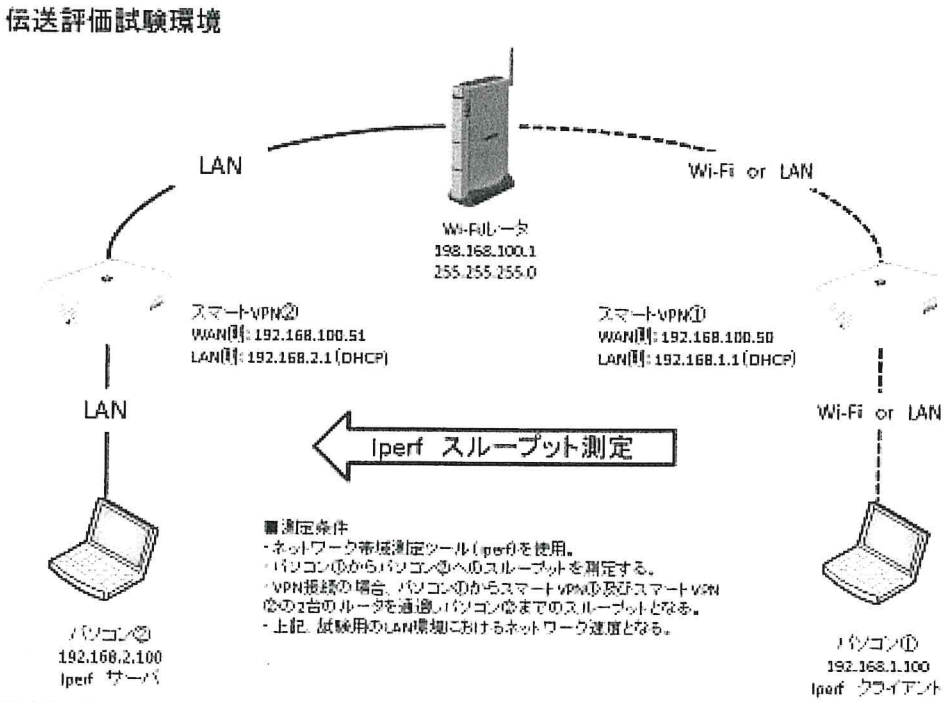
4. 考察

今回、設置型 VPN ルーターと同等のセキュリティ機能と外出先でのネットワーク環境に対応した携帯型 VPN ルーターと、携帯型 VPN ルーターの遠隔管理システムを開発した。設置型 VPN ルータを携帯可能なサイズにすることで、電源を確保できない外出先でも高度なセキュリティを構築することが可能になる。



【図 2】携帯型 VP ルーター

現在、据置型ではあるが 400g 前後の IPSec 対応有線 / モバイルルーターが複数種類存在しており、自宅・ホテル・空港ラウンジ等電源が確保可能な「出先」の環境下では利用可能である。しかし、据え置き型のルーターでは常に携帯するのには重量的負担があることと、電源が確保不能な場所では使用ができない問題点を有している。本システムは電源の確保が不要であるため、携帯電話を用いたテ



【図3】伝送評価試験方法

【表3】伝送評価試験結果

No	評価項目	試験日	スマートVPN①（iperf クライアント）		スマートVPN②（iperf サーバ）		伝送量（MB）	時間(MM:SS) TCP	
			LAN	WAN	WAN	LAN		VPN時	VPN無し
1	伝送評価	2014/6/6	ケーブル	ケーブル	ケーブル	ケーブル	10	11.1Mbps	94.6Mbps
2		2014/6/6					50	11.1Mbps	94.6Mbps
3		2014/6/6					100	11.1Mbps	94.4Mbps
4		2014/6/6					300	11.1Mbps	94.5Mbps
5		2014/6/6					500	11.1Mbps	94.6Mbps
6		2014/6/6	Wi-Fi（PC-スマートVPN間約1M）	ケーブル			10	9.79Mbps	22.7Mbps
7		2014/6/6					50	9.89Mbps	20.4Mbps
8		2014/6/6					100	10.3Mbps	22.7Mbps
9		2014/6/6					300	9.83Mbps	20.4Mbps
10		2014/6/6					500	9.99Mbps	19.1Mbps
11		2014/6/17	Wi-Fi（PC-スマートVPN間約5M）	Wi-Fi（スマートVPN-Wi-Fiルータ間約5M）			10	2.99Mbps	11.1Mbps
12		2014/6/17					50	2.51Mbps	14.1Mbps
13		2014/6/17					100	4.63Mbps	16.0Mbps
14		2014/6/17					300	8.03Mbps	14.5Mbps
15		2014/6/17					500	8.50Mbps	13.0Mbps
16		2014/6/17	ケーブル	Wi-Fi（スマートVPN-Wi-Fiルータ間約5M）			10	10.7Mbps	30.4Mbps
17		2014/6/17					50	10.8Mbps	36.9Mbps
18		2014/6/17					100	10.7Mbps	30.4Mbps
19		2014/6/17					300	10.4Mbps	35.4Mbps
20		2014/6/17					500	10.5Mbps	38.7Mbps

ザリングが使用可能な場所であればどこでも利用することができる。そのため、外出先で緊急の画像読影依頼があった場合などでは迅速な対応が可能となり有効であると思われる。

IPsecは、暗号技術によりIPパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。暗号化をサポートしていないトランスポート層やアプリケーションを用いても、通信経路で通信内容の傍受や改竄を防止できる。

IPsecは、AH（Authentication Header）による認証機構とデータの完全性保証、ESP（Encapsulated Security Payload）によるデータ暗号化等のセキュリティ

プロトコル、IKEなどによる鍵交換から構成されている[3]。

IPsecによるVPNは従来ではVPNゲートウェイなどのハードウェアで構築されていたが、現在ではL2TP/IPsecが携帯端末でも標準装備されており携帯端末から直接VPNを構築することが可能となった。

IPsecにはトランスポートモードとトンネルモードの2つの動作モードがある。トランスポートモードはルーターなどを介さないポイント・ツー・ポイントの通信で利用されており、L2TP/IPsecで使用されている。一方トンネルモードは拠点間接続で利用され、接続両地点にVPNゲートウェイの設置が必要である。

医師が自宅および外出先の携帯端末から病院の端末にソフトウェアによるIPsecによるVPNでアクセスするためにはL2TP/IPsecを用いることとなるため、トランスポートモードでの接続となる。携帯型VPNルーターを使用することで、トンネルモードが使用可能となり、リモート接続と拠点間接続を意識せずにシステム構築することが可能となる。

また、今回リモート接続時の端末の遠隔管理システムも同時に構築した。L2TP/IPsecではソフトウェアレベルでのVPN構築のため、設定情報が漏洩すると第3者の所有する携帯端末で同じ環境設定することが可能なためVPNを構築される危険性がある。L2TP/IPsecではリモート接続している端末がなりすましでないか遠隔管理システムで把握ができないため、常に第3者による接続の危険性を有している。

一方、携帯型VPNルーターには固有情報が付与されているため遠隔管理システムによる識別が可能である。ハードウェアレベルでのVPN構築のため、携帯型VPNルーターが盗難されない限り第3者によるアクセスは物理的に起きることがない。

また、携帯型VPNルーターが盗難された場合も遠隔管理システムで盗難された携帯型VPNルーターの使用を制限することが可能であるため、システム全体への影響を最小限にとどめることができる。

しかし一方で、専用端末を携帯することで、操作手順が増えて煩雑化する、重量的負担、使用機器が増えることで紛失のリスクが増大する可能性が上げられる。これらの問題に対しては将来的に携帯通信端末へ本機能を内蔵化して軽量化・一体化することで利便性も高まり解決できるものと思われる。現段階でも本システムは医療以外にも一般的に利用が可能であり、他分野で活用されることを期待したい。

またIPSecでは、1）IKE鍵管理が適切で無ければなりすましがなされる、2）IKEアグレッシブモード＋共有鍵運用では鍵を盗まれなりすまし・盗聴がなされやすい、3）ハードウェア実装であるため脆弱性が発見された場合更新がしにくいといった問題があげられる。本システムではIKEメインモードを使用して成りすまし対策を行っている。

本システムの利用により、携帯端末からのリモート接続のセキュリティを拠点間接続と同レベルに高めることが可能となった。リモート接続という概念自体がなくなる可能性のあるシステム開発であり、今後携帯端末へ内蔵化を検討していきたい。

5. まとめ

厚生労働省のガイドラインを満たすIPsec＋IKEを準拠したトンネルモードでVPN構築が可能な携帯型VPNルーターと、携帯型VPNルーターの遠隔管理システムを開発した。

本システムの利用により、リモート接続でもトンネルモードによるVPNが構築可能になる。

参考文献

1) 厚生労働省．医療情報システムの安全管理に関するガイドライン 第4.1版．2010年．
2) 郡隆之．医師負担軽減策としての遠隔画像診断システムの活用．日本遠隔医療学会雑誌　2012；8(2)：139–141．
3) IETF. REC2401: Security Architecture for the Internet Protocol. 1998.

Keywords：portable VPN rooter, IPsec, telemedicine