様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年５月３０日現在

機関番号：12608
研究種目：挑戦的萌芽研究
研究期間：2011～2012
課題番号：23656258
研究課題名（和文）　医療機関間の安全な接続可能とする医療用ネットワーク基盤技術の研究
研究課題名（英文）　Research of the network infrastructure for medical treatments

研究代表者
小尾　高史　　（Obi　Takashi）
東京工業大学・像情報工学研究所・准教授
研究者番号：40280995

研究成果の概要（和文）：
本研究では、現在のレセプト請求に代表される医療用ネットワークサービスで利用されている各社の OD-VPN の技術的仕様を調査し、相互接続に必要となる要件である、（１）相互接続に必要な情報を共有できること可能であること、（２）ネットワークドメイン同士で直接 VPN を構築できること、（３）プライベート IP アドレスに関する課題の解決のそれぞれについて具体的検討をおこなった。
また、医療、保健分野などで，次世代 OD-VPN を利用する場面を整理し、その結果に基づいて，医療機関内の情報端末などからの利用シーケンスを考察し、今後の標準化を踏ま他検討を行った。

研究成果の概要（英文）：
The technical specification of OD-VPN of each company used by the network service for medical treatments represented with this research by the present medical statement claim is investigated, Concrete examination was performed about each of solution of the subject about that it is possible for information required for (1) interconnection which is the requirements which are needed for interconnection to be sharable, that VPN can be directly built in (2) network domains, and (3) private IP addresses.
Moreover, in medical treatment, the health field, etc., the scene of using next-generation OD-VPN was arranged, the use sequence from the information terminal in a medical institution, etc. was considered based on the result, and examination besides was performed for future standardization.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	2,800,000	840,000	3,640,000

研究分野：工学
科研費の分科・細目：電気電子工学・システム工学
キーワード：社会システム工学・病診間連携、個人健康情報、社会保障

１．研究開始当初の背景

オンデマンド VPN（以下 OD-VPN）は、インターネット VPN を簡便に利用可能とする技術である。OD-VPN で利用する VPN ルータには、二階層 PKI 対応の耐タンパ性を持つ IC チップが搭載されており、VPN 構成情報をチップ内で安全に管理することができる。このため、そのICチップ内の情報操作権を信頼するVPN管理機関（以下、管理機関）が請け負うことで、管理機機関の責任の元に VPN を構築することを可能としている。また、このように、管理機関が設定･VPN 情報管理を請け負う VPN 形態をとることにより、VPN 構築時の手間やコストを削減しつつ、離れた任意多地点のネ

ットワークドメインを、要求に即応して、１つの仮想的なプライベートネットワークにすることが可能となっている。
現在、レセプトのオンライン請求を実現するための手段として OD-VPN の利用が始まっており、今後は、医療機関間における様々なサービスへの応用に関する OD-VPN への期待が高まっている。
ここで、現在、医療機関向けに OD-VPN サービスを行っているサービスドメイン（NTT データ、NTT PC コミュニケーション、富士通、三菱電機）の仕様に差異があるとともに、「接続ポリシーの指定方法・決定方法」なども異なっており、現段階で異なるサービス事業者が提供する OD-VPN サービスを利用する医療機関同士で直接安全なネットワークを構築することは極めて困難な状況にある。

２．研究の目的

VPN は、公共のネットワークを専用線と同様に利用できる技術のことを意味し、インターネット上に仮想的にプライベートネットワークを構築することができる。しかし VPN の構築には利用者にネットワークの専門知識が必要なうえ、設定などを誤ると情報セキュリティ上、多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。そのため一般的な VPN 利用方法としては、専門家が直接 VPN 接続機器を操作して VPN の設定をし、接続地点を固定するというものであり、任意な多地点を動的に接続する VPN の実現は困難な状況である。

このような背景の下、VPN 管理機関と２階層 PKI に対応した IC チップが搭載された通信機器を用いて、利用者の要求に応じて鍵情報などの VPN 構築に必要な設定情報を、ネットワークを介して安全に配送し、任意多地点間で直ちに VPN を構築する OD-VPN 技術の研究開発が進められてきた。

しかし、現状の OD-VPN は、サービスドメインと呼ばれる特定の管理機関の管理範囲にあるネットワークドメイン内のみで、VPN が構築可能であり、マルチドメイン環境と呼ばれる、複数のサービスドメインが存在する状態となっている。このため、任意の医療機関間で VPN を構築することは困難である。

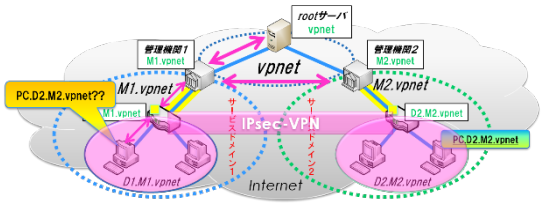
そこで、本研究では、マルチドメイン環境下において異なるサービスドメインの VPN ルータ同士が相互接続可能な OD-VPN 相互接続方法の確立を研究の目的とし、安全なネットワーク基盤を OD-VPN フレームワークを用いて構築することを目的とする。

３．研究の方法

異なるサービス事業者に属するネットワークドメインとの VPN 接続をオンデマンドで可能とするフレームワークの概略図を図１に示す。提案するシステムでは、従来インターネットの名前解決のために利用されている DNS で使用されている分散管理構造を適用・拡張することで、相互接続を可能とするフレームワークであり、現在の OD-VPN に対して新たに、以上の技術的解決策を適用することで、VPN 相互接続を実現する。

- 名前解決を実現し、名前解決の過程で VPN 構成情報を管理機関同士で共有
- 管理機関によって VPN ルータが設定され、その設定を元にルータ同士で通信用暗号鍵を直接ネゴシエートして VPN を構築
- サービス事業者の使用範囲が指定された“仮想 IP アドレス”と呼ぶ、ネットワーク内の機器に対応させる IP アドレスを OD-VPN 利用時に動的割当を行う。

図１　提案する OD-VPN フレームワーク



本研究では、これらを踏まえ以下の点について基礎的検討を行った。

- OD-VPN で利用する通信方法の暗号化方式の共通化及びその標準化
- ルータの認証に利用する認証方式の標準化
- 医療機関に特化した名前解決方法及び管理方法の検討
- 既存プロトコルの改良とその標準化
- 接続ポリシーの定義方法・合意方法などの共通化・標準化

４．研究成果

（１）　相互接続の必要性

レセプト請求のオンライン化に伴い、オンデマンド VPN が導入されることによって、医療機関がインターネットを利用して外部に接続可能なネットワーク環境を持つことになり、今後、電子化された医療情報をネットワークを介して共有・交換・利用することによる医療サービスの質向上・医療サービス業務の効率化を図ることが検討されている。以下にその検討例を挙げる。

①　医療データの２次利活用

電子カルテに蓄積されるデータは、患者の診療記録であると同時に、症例データベースの役割も担う。症例データベースが実現できた場合、以下の医療データの２次利活用方法が検討されている。

- 類似症例の分析を通じて、医療の質の向上に役立てられる。

・　過去の症状も診断要素に取り入れることによって、診断の質向上に役立てる。

医療データの２次利用を実現させるためには、多くの医療データを集めることと、集めたデータを迅速に利用できる環境が必要性である。ネットワークを介した医療情報の交換が可能となれば、これを実現できる。

② 病診連携（医療情報も含めた電子紹介状の利用）

各医療機関に集計された医療データの現状は、個々の医療機関の中で完結している。治療する医療機関を変える場合は、情報交流の主な手段である『紹介状』を用いるが、直接の診断データなどは持ち出すことが出来ないため、再診断などの無駄手間などが発生してしまって治療を受ける側の人に対しては有効でない。

これに対して電子化した診断データと紹介状をネットワーク介して送信することで、上記の課題を解決できる。

③ 病-病連携（専門医の集中配置＋病院間のネットワークを利用した診断支援）

地域医療の大きな課題として、専門医の不足が挙げられている。その解決策として、専門医を集中配置し、 病院間ネットワークを利用して医療情報の伝達を行って診断を行う策が挙げられる。

PET やマンモグラフィなどの高度医療機器を使用した検診や診断が日常的になってきている現在、地域医療においては積極的に病-病連携の環境を整え、専門医の不足に備えていく必要がある。

④ 救急医療の視点

救急患者の搬送中、救命士と医師が一体となって処置にあたることが出来れば、患者の救命率を高めることができる。ネットワークを介したリアルタイム映像配信を行うことで、医師は現場の状況を映像で把握して指示を出すことが可能となる。

上記の例に示したネットワークを介した医療機関間連携には、医療機関であればどの機関でも連携出来るように、単一のサービスドメイン内のみではなく、異なるサービスドメインのネットワークドメインとの VPN 構築が可能であることが求められる。

（２）相互接続の課題

現状のオンデマンド VPN フレームワークにおいて、相互接続を考慮した時のフレームワークの課題点・問題点を以下に説明する。

① VPN 構成情報を共有する仕組みがない

オンデマンド VPN は、VPN 機器に耐タンパ IC チップを使用し、そのチップの管理権を持った VPN 管理機関によって VPN 構築されるマネージド VPN 形式である。言い換えると、VPN 管理機関が管理できる VPN 機器同士のみが VPN を構築できるということになる。

現在のオンデマンド VPN フレームワークは、管理機関は自分の管理範囲のみのネットワークドメイン情報しか知らない。また、他のサービスドメインのネットワークドメインに関する情報を知る術がないため、他のサービスドメインの VPN 機器への VPN 接続情報設定が行えない。

② IX 方式の問題点

これを解決する相互接続方法として、IX 方式（Internet eXchange）と呼ばれる方式が考案された。この方式は、ネットワークドメイン同士が直接 VPN を構築するのではなく、管理機関と VPN を構築し、管理機関同士で VPN を構築し、その経路を利用して、サービスドメインの異なるネットワークドメイン内の機器と暗号通信を行う方式である。

IX 方式は、既存の VPN 機器の改造が少ないため、容易に導入が可能である反面、中継地点で暗号化されたデータを一度復号化してしまうため、中継地点での情報漏洩の可能性があり、OD-VPN が目指した ネットワークドメイン間の通信の安全性を “論理的”や“運用的”ではなく“技術的”に担保するという最初の目的からも大きく外れる方式となっている。このため、本来の OD-VPN は、ネットワークの管理・運用に関する責任のみを管理機関に課すことを目的としていたが、IX 方式では、コンテンツの安全性確保に関する責任についても管理機関がその一部を担うこととなるため、責任を明確に分解することが困難になる。

さらに、現在の IX 方式は、異なるサービス事業者の VPN ルータ配下で使用する機器の IP アドレス設定が非常に面倒であり、異なるサービス事業者下に属する医療機関同士で通信を行う場合には、あらかじめ何らかの手段で機器に割り当てる IP アドレスを決定しておかなくてはならない。この作業は、現状では、オンラインではなく、電話等の別の手段を利用して行っており、もはやオンデマンドなネットワークと呼べるものではない。

③ プライベート IP アドレスに関する課題

オンデマンド VPN で使用している VPN ルータ間通信の IPsec のモード（ESP トンネルモード）では、パケットの送信先にプライベート IP アドレスを指定してもインターネット環境を挟んで通信が行える。（※通常のインターネットを利用する通信は宛先がグローバル IP アドレスでなければ、通信できない。）

しかし、同じプライベート IP アドレスを接続元と接続先のネットワークドメイン内で互いに使用していた場合、パケットのルーティングが行えず、ESP トンネルモードで VPN を構築しても通信が出来ない。他のサービスドメインとの相互接続でも同様で、仮に管理機関同士でプライベート IP アドレスの伝達が行えたとしても、アドレス重複が原因で相互に通信を行うことは出来ないという課題がある。

プライベート IP アドレスはセキュリティの観点からの課題も抱えている。ネットワークドメイン内で利用しているプライベート IP アドレスを伝達してしまうことは、ネットワークドメイン内の情報の一部を外部に与えてしまうことになるので、セキュリティ上好ましくないという懸念も存在する。

（3） 相互接続方法の提案

異なるサービスドメインとのネットワークドメインとの VPN 相互接続を可能とするために、図 1 に示す新たなフレームワークを提案した。オンデマンド VPN フレームワークに DNS（Domain Name System）で使用されている分散管理構造を適用し、その用法を拡張したフレームワークである。

具体的には、現在のマルチドメイン環境のオンデマンド VPN フレームワークに、以下の仕組みを追加する。

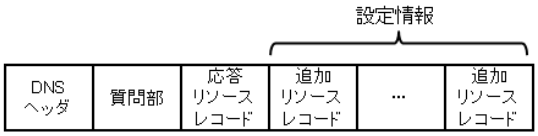
- 各サービスドメイン、各ネットワークドメインにドメイン名をつけ、各管理機関は配下のネットワークドメインのドメイン名とそのネットワークドメインで利用している OD-VPN ルータの IP アドレスの関係を管理する。
- ルータ配下の機器にドメイン名から構成される名前＝URL（Uniform Resource Locator）を付与する。
- サービスドメインの VPN 管理機関のドメイン名と IP アドレスを管理する「root サーバ」を新たに設置

これにより、以下の機能を用いることで VPN 相互接続を実現できる。

- オンデマンド VPN フレームワークに参加する機器に対する名前解決（URL を問い合わせると IP アドレスが回答として返る）の仕組みを導入。
- 名前解決を行うその過程で、root サーバや管理機関が連携し、VPN 構築に必要な情報を管理機関同士で共有。
- 共有した情報を元に VPN 構成情報が生成され、管理機関によって VPN ルータへその構成情報が設定される。
- 設定された情報を元に、VPN ルータ同士で IKE プロトコルを用いて通信用暗号鍵を直接ネゴシエートし、IPsec-VPN を構築。

このフレームワークにおいて、通常の DNS メッセージの追加領域部分を使用して VPN 構成情報共有を実現する。そのメッセージ形式の概略を図 2 に示す。

図 2　拡張 DNS メッセージの形式



次に、プライベートイ IP アドレスに関する課題を解決するために、本研究で提案する相互接続では、ネットワークドメイン内で実際使用しているプライベート IP アドレスとは異なる IP アドレスを利用して VPN 構築後の通信を行う。この時に使用するアドレスを仮想 IP アドレス（Vir IP）と呼び、以下の特徴を有する。

- OD-VPN 利用時において、マルチドメイン環境内で唯一な IP アドレス
- OD-VPN 利用時において、その時のみ一時的に有効で、ネットワークドメイン内で使用しているアドレスクラスとは別クラスの IP アドレス

以下に、これらを実現する手法を具体的に説明する。

- 仮想 IP アドレス＝クラス A のプライベートアドレス。利用可能アドレス数が多いクラス A のプライベート IP アドレス空間をサービスドメインごとに振り分け、接続要求ごとにアドレスを動的に割当てる。（※但し、各ネットワークドメイン内の機器に元から割り当てるアドレスはクラス B、C のプライベートアドレス空間を使用しなければならない。）
- 動的に割り当てる仮想 IP アドレスは、VPN 構成情報設定時に、VPN ルータの仮想 IP アドレス対応テーブルに設定される。
- OD-VPN ルータに対して外向き（ネットワークドメイン内から外部へ）のパケットが入力された場合、仮想 IP アドレス対応テーブルが参照され、送信元 IP アドレスを VPN セッションに割り当てられた仮想 IP アドレスに変換し、仮想 IP アドレスに対応づけられたグローバル IP アドレスを宛先とした IPsec パケットが生成され、ルーティングされる。（図 3 上部）
- 内向き（外部からネットワークドメイン内へ）パケットが入力された場合、IPsec パケットの暗号化を解いた後、仮想 IP アドレスに対応したネットワークドメ

イン内のプライベート IP アドレス宛へパケットがルーティングされる。（図３下部）

この仮想 IP アドレスを利用することにより、アクセス先ネットワークドメイン内の機器とアクセス元ネットワークドメイン内の機器とで同じプライベート IP アドレスを使用したとしても、アドレス衝突を回避して通信が可能となる。
また、通信相手に対しては内部情報であるプライベート IP アドレスが伝達されるのではなく、一時的かつ異なるアドレスクラスの IP アドレスが伝達されるので、セキュリティ性の懸念を解消することが出来る。

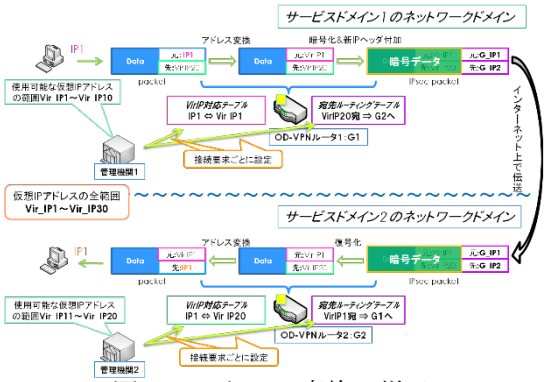


図３　アドレス変換の様子

（４）　上位プレイヤのセキュリティ機能
提案する相互接続方法におけるフレームワークでは、上位プレイヤ（管理機関・root サーバ）の通信路はインターネットを利用することを想定している。このため、インターネット上に存在する様々な脅威（メッセージの改ざん･盗聴･なりすましなど）によって、VPN が誤って構築され､それが原因で情報漏洩を引き起こすという危険性が高まることや､VPN が構築されない事態になることが指摘される。そこで、本研究では、上位プレイヤ間の通信路に適したセキュリティ機能を持たせることを検討した。まず、それぞれの通信路に対する要件を検討し、次にその要件を満たすセキュリティ機能を定めたので、それについて以下で説明する。

① 管理機関と root サーバ間の通信路のセキュリティ要件
- 交換するメッセージが改ざんされていないことを検知できること
- 管理機関側からの視点で、アクセス先が正しい root サーバなのかを検証するために、メッセージ源認証が可能であること

② 管理機関間同士の通信路のセキュリティ要件
- 交換するメッセージが改ざんされていないことを検知できること
- 正しい管理機関と情報共有するために、相互にアクセス先相手の管理機関を認証可能なこと

そして、上記の要件に対して、本研究では以下のセキュリティ機能を定めた。

１．管理機関と root サーバ間の通信路のセキュリティ機能

TSIG（Transaction SIGnature）を利用して、DNS サーバとクライアントで共有する秘密鍵を使用した MAC(Message Authentication Code)を用いた、DNS メッセージ完全性・DNS メッセージ源認証を実施する。

２．管理機関同士の通信路のセキュリティ機能

SSL（Secure Socket Layer）を利用し、サーバ認証・クライアント認証の双方向認証を行うとともに、SSL 上で交換するデータの完全性検証を実施する。
上記のセキュリティ機能を提案する DNS 拡張 OD-VPN フレームワークに適用することによって、各々の通信路上のセキュリティ要件を満たし、安全に提案フレームワークを利用して正しく VPN を構築することが可能となる。

（５）　提案する相互接続シーケンス
提案手法における相互接続のシーケンス例を図４に示す。具体的なシーケンスは以下の通りとなる。

① PC1 がアクセス先 URL（PC.D2.M2.vpnet）を指定し、DNS request を送る。
② OD-VPN ルータから管理機関へ VPN request と DNS request を送る。
③ 管理機関１は接続要求された URL を判断し、管理下に属さない場合には、root サーバに DNS request して、root サーバから問い合わせ先の情報を得る。この時 TSIG によって、返信されたメッセージを検証して、データの正当性を確認する。
④ 管理機関１は管理機関２へ DNS request を送る。同時に管理機関同士で必要な相互接続情報を交換する。この時、SSL 確立する際の公開鍵証明書を利用した相互認証を行う。また、互いに通知した仮想 IP アドレスの対応付けを行っておく。
⑤ 管理機関同士での情報交換が終わると、各管理機関は VPN 構成情報を生成し、配下のルータに対して設定を行う。また、このとき、ルータへ DNS answer（仮想

IP アドレス）なども返信する。

⑥ ルータは、要求元の DNS アプリに対して DNS answer として仮想 IP アドレスを返信する。

⑦ 仮想 IP アドレスに対してアプリケーションが通信開始する。

⑧ 仮想 IP アドレス向けのパケットがルータに届くと、ルータ同士で IKE を行い、ネットワークドメイン間の IPsec-VPN を構築する。ルータに届いたパケットは、送信元のプライベート IP アドレスをアドレス対応テーブルに基づいて仮想 IP アドレスに変換し、カプセル化（暗号化＋新 IP ヘッダ付加）して配送される。

⑨ 相手先ルータではカプセル化が解かれ、仮想 IP アドレスに対応するプライベート IP アドレスに送信先アドレスを変換し、そのアドレスを持つ端末にパケットが配送される。返送はパケットに含まれている PC1 の仮想 IP アドレス向けに返送される。

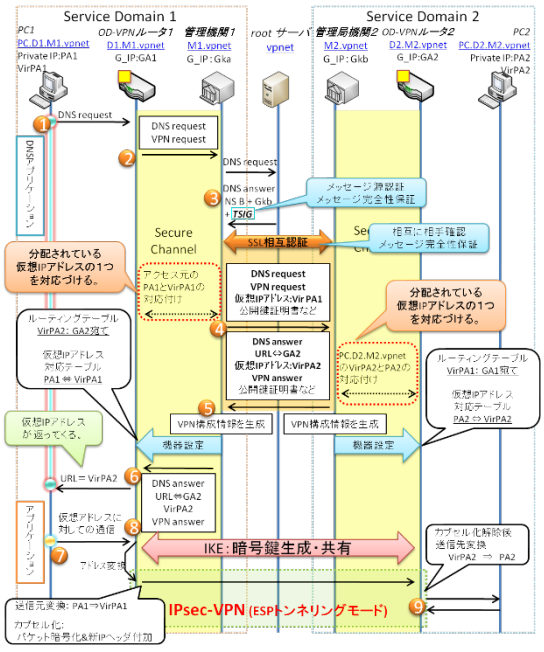


図４　相互接続のシーケンス

このように、本研究では、異なるサービスドメインのネットワークドメイン同士が OD-VPN フレームワークを利用して相互接続を行うことを実現するために、“DNS で利用される分散管理構造を適用・拡張した「DNS 拡張 OD-VPN フレームワーク」”、“アクセス元とアクセス先の機器に対して一時的かつ動的に割り当てる「仮想 IP アドレス」”を現状のマルチドメイン環境に適用・採用することを提案した。また、提案するフレームワークの安全性を検討し、提案手法を安全に利用するための設計指針を明らかにした。

さらに、評価用プロトタイプシステムを実装し、提案した相互接続手法の評価を行った。実験から得られた通信速度・レスポンス性能等の値から、提案する手法による VPN 構築が過度のオーバーヘッドを有しないこと、及び、攻撃試験の結果より、ネットワーク上の脅威を検知可能であり、安全な VPN の構築が可能であることを示し、提案手法の実現可能性及び実用性を明らかにした。

５．主な発表論文等

〔雑誌論文〕（計１件）

・小尾高史、大山永昭、シームレスなサービス利用を可能とするセキュアネットワーク基盤の実現に向けて, 月刊基金, 査読無, 5, 2011, pp. 2-4

６．研究組織

(1)研究代表者

小尾 高史　（Obi　Takashi）

東京工業大学・像情報工学研究所・准教授

研究者番号：40280995

(2)連携研究者

大山 永昭　（Ohyama Nagaaki）

東京工業大学・像情報工学研究所・教授

研究者番号：50160643