階層型VPNにおける仮想リンクの透過的確立手法

豊田博俊[†1] 河合洋明[†2,*1] 坂根栄作[†3]
岡山聖彦[†4] 山井成良[†4] 石橋勇人[†2]
安倍広多[†2] 松浦敏雄[†2]

インターネットの発展にともない，インターネットを介して外部から組織ネットワーク内の資源に対して安全にアクセスするための技術である VPN（Virtual Private Network）の必要性が高まっている．VPN では，外部から保護するネットワークの範囲を VPN ドメインというが，VPN ドメインが階層的に構成されたネットワーク環境（階層型 VPN）では，通信先に応じて次の階層の VPN ゲートウェイ（VGW）を選択する必要がある．そこで本論文では，DNS，ICMP，TCP を用いて利用者に透過な経路制御手法を提案する．提案する方法では，DNS サーバへの問合せや，ICMP メッセージの応答，TCP の応答により次の階層の VGW を自動的に決定する．VTun を拡張することによって提案方法を実装し，その有効性を確認した．

Transparent Establishment Methods of Virtual Links on Hierarchical VPN

Hirotoshi Toyoda,[†1] Hiroaki Kawai,[†2,*1] Eisaku Sakane,[†3]
Kiyohiko Okayama,[†4] Nariyoshi Yamai,[†4] Hayato Ishibashi,[†2]
Kota Abe[†2] and Toshio Matsuura[†2]

As the Internet evolves, VPN (Virtual Private Network), which establishes secure connections between off-site clients and on-site servers, is getting important. In VPN, a part of network which is protected from the Internet is called “VPN domain.” In the environment where VPN domains are hierarchically configured (Hierarchical VPN), the next hop VPN gateway (VGW) must be discovered depending on the destination host. In this paper, we propose some routing methods which are transparent from users. In these methods, the next hop VGW is automatically discovered by querying to DNS servers and/or receiving ICMP and TCP packets. We have implemented proposed methods by extending the VTun software. The effectiveness of these methods are experimentally confirmed.

1. はじめに

近年，インターネットを介して自組織のネットワークに安全にアクセスするための技術として，仮想プライベートネットワーク（Virtual Private Network，以後 VPN とする）が注目されており，活発に研究されている．VPN を用いると，組織外から自組織のネットワークに仮想的なリンクを構築して，組織外からでも安全に組織内にアクセスすることが可能になる．しかし，複数の下部組織を有するような大規模組織では，単純な方法では仮想的なリンクを構築できない場合がある．

たとえば，大学における次のような場合を考える．大学全体のネットワークは大学全体で定めるセキュリティポリシに基づいて，外部からのアクセスを制限するために外部ネットワークとの接続点にファイアウォールを設置しているものとする．また，学内の付属病院では，独自のセキュリティポリシに基づいて病院外（学内他部局を含む）から病院内へのアクセスを制限するためにファイアウォールを設置しているものとする．このような環境において学外から付属病院のネッ

†1 大阪市立大学
Osaka City University
†2 大阪市立大学大学院創造都市研究科
Osaka City University
†3 大阪大学サイバーメディアセンター
Osaka University
†4 岡山大学総合情報基盤センター
Okayama University
*1 現在，三菱電機情報ネットワーク株式会社
Presently with Mitsubishi Electric Information Network Corporation

トワークにアクセスしようとする場合，複数のファイアウォールを経由する必要があるため，VPN の方式によっては仮想的なリンクを構築できない．

上記のような問題に対処するため，我々はこれまでに階層型 VPN と呼ぶ方式を提案してきた[1)–9)]．これはアクセス元からアクセス先への経路上に存在する複数のファイアウォールを経由して仮想的なリンクを構築する方式であり，これまでの研究において経由すべきファイアウォールを自動的に選択する機能を導入したため，利用者はアクセス先のネットワーク構成を意識する必要がないという特徴を持つ．

ところが，従来の階層型 VPN では，利用者は階層型 VPN の必要性を意識する必要があった．すなわち，利用者が任意の場所において組織内にアクセスする場合，アクセス先の組織に階層型 VPN が導入されているかどうか，また現在の場所からアクセスする場合には VPN 接続が必要であるかどうかをあらかじめ知っており，必要であればアクセス前に事前に VPN 接続を確立しておかなければならなかった．これは従来の階層型 VPN が持つ上記の特徴を阻害し，利用者の負担を増大させることになるため，好ましくない．

そこで，本研究では，このような問題を解決するために，透過的な動作により VPN 接続を確立する手法を提案する．本手法では，アプリケーションプログラムからの接続要求を自動的に検知し，クライアントの利用者がその動作を意識することなく VPN 接続を確立する．また，その際アプリケーションプログラムの改変を必要としないため，比較的導入が容易であるという特徴を持つ．

以下 2 章では関連する研究に触れる．3 章では透過的に階層型 VPN を確立する方法について述べ，4 章ではその実現方法を明らかにする．5 章では提案方法について評価する．

2. 関 連 研 究

階層的仮想リンクの実現方法として，セキュリティゲートウェイを多段に経由して階層型 VPN を確立する手法[10)] が提案されている．これは，トランスポート層に実装した代理サーバであるセキュリティゲートウェイが保持する静的な中継経路テーブルを利用して階層型 VPN を確立するものである．この方法では，動的に中間経路が変化するような場合，中継経路テーブルを登録し直す必要が生じ，クライアントの持つ経路テーブルを変更することを周知しなければならない．クライアントは，その静的な経路情報による動作を行うため，この変更にともなう管理コストが大きくなる．

文献 2) で提案した経路制御手法では，中継経路情報を LDAP により管理することで，上記のような管理コスト増加を抑えることができるようになった．

また，我々は VPN 確立時の利用者の認証方法や，柔軟なアクセスポリシの管理方法等を提案し，その有効性を明らかにした[3),4)]．

しかし，仮想リンクを透過的に確立する手法はこれまで提案されていなかった．

3. 仮想リンク構成の実現方法

利用者が VPN の確立動作を意識せずに透過的な階層型 VPN 接続を実現するためには，VPN の必要性を自動的に判断する機能が必要である．

本研究ではこのための方法として 2 つの方法を提案する．1 つは DNS クエリを契機とする方法（**方式 1**）であり，もう 1 つはエラー応答を契機とする方法（**方式 2**）である．両者とも，接続動作を始める際のアプリケーションの通信をモニタし，VPN 接続の必要性を自動的に判断し，動作を開始する．

以下にこれらの方法の概要を述べる．

3.1 DNS クエリを契機とする方法（方式 1）

まず，アクセス先のサーバがグローバルアドレスを有する場合の手順を示す．

この方法では，VPN の必要性を判断するソフトウェアを，クライアント上で動作させておく（これを DNS Proxy と呼ぶ）．DNS Proxy はアプリケーションがサーバの FQDN を指定して通信する際に発生する DNS クエリ（A レコード）をモニタする．

動作の概要は次のとおりである．DNS Proxy は，DNS クエリに対してサーバ宛ての ICMP エコー要求を送信し，クライアントからサーバまで直接通信できるか調査する．直接通信できない場合は，経路上のルータから ICMP 到達不可メッセージが返される．この ICMP 到達不可メッセージを DNS Proxy が取得し，このメッセージをもとに，そのルータの IP アドレスを手がかりに VPN ゲートウェイ（VGW）の情報を受け取る．

アクセス先のサーバがプライベートアドレスの場合には，接続を確立する過程でのみ一時的に使用するグローバル IP アドレスを用意する．組織外からのサーバに対する A レコードの問合せに対しては，この IP アドレスを返すようにする．DNS proxy は，このアドレスに対して ICMP エコー要求を送信することで VGW を発見でき，VPN 確立後にはサーバのプライベートアドレスを取得することになる．

3.2 エラー応答を契機とする方法（方式 2）

通信を監視するソフトウェア（VPN Agent と呼ぶ）をクライアント上で動作させておく．一般に，組織外から組織内のサーバへの通信を許可していない場合に，組織外から通信を試みると，経路上のルータから直接通信できない旨のエラー応答が返される．VPN Agent は，このエラー応答をモニタすることで VPN の必要性を判断する．

動作の概要は次のとおりである．まず，サーバ側の組織内のルータ（VGW）は，許可していない通信に対して TCP の非標準の応答[*1]を返すように設定しておく．アプリケーションプログラムが通信を開始する契機としてサーバ宛てに SYN パケットを送信したとき，ルータはその応答として TCP の非標準のパケットを返す．この応答パケットに VGW の情報を載せることで，VPN Agent は VPN の接続を開始する．

3.3 仮想リンクの切断方法

VPN 接続の切断は VPN セッションを監視し，一定の時間通信が行われない場合はセッションを切断する．したがって，利用者は VPN セッションの切断に際して特別な操作を行う必要はない．

ただし，本提案手法 1 では DNS クエリを契機としているため，いったん VPN セッションを切断した後に再度 VPN 接続を行う場合には，アプリケーションの再起動が必要であるので，タイムアウト時間は長めに設定しておく必要がある．

4. 実　　装

3 章で述べた 2 つの方法について実装した．以下に動作の詳細を述べる．

4.1 方式 1 の詳細

4.1.1 グローバルアドレスでの動作

方式 1 の実装は，DNS クエリを監視する DNS Proxy と，実際の VPN 接続を担当する VTun[11] 改造版 1 からなる．

クライアント上では DNS Proxy がアプリケーションの DNS クエリを監視し，必要に応じて VTun のクライアント（VT_1C）を起動する．また，各 VGW_i 上では VTun サーバ（VT_1S_i）を動作させておく．

以下，クライアント（C1）がサーバ（S1）と通信する場合を例に方式の詳細を述べる（**図 1** 参照）．

（1） C1 上のアプリケーションは S1 の IP アドレスを取得するために DNS クエリを送信する．DNS Proxy はアプリケーションが送信する DNS クエリを監視し，A レコードを問い合わせ，DNS Proxy は S1 の IP アドレスを受け取る．

（2） DNS Proxy は S1 宛の ICMP エコー要求を送信し，S1 までの経路上のルータ（router1）から ICMP 到達不可メッセージを受信する．

（3） DNS Proxy は ICMP 到達不可メッセージの送信元である router1 の IP アドレスの TXT レコードを DNS サーバに問い合わせ，VGW_1 の情報を受け取る．

（4） DNS Proxy は C1 上で VT_1C を起動し，S1 の FQDN を VT_1C に渡す．VT_1C は S1 の FQDN を VGW_1 上の VTun サーバ（VT_1S_1）に渡すことで，VPN 接続要求を行い，VT_1S_1 からの応答を待つ．

（5） VT_1S_1 は VT_1C から受け取った S1 の FQDN を DNS サーバに問い合わせて S1 の IP アドレスを取得する．(2) から (4) までの DNS Proxy，VT_1C と同様の動作を行い，VT_1S_1 は VGW_2 上の VTun サーバ（VT_1S_2）に S1 の FQDN を渡して VPN 接続要求を行い，VT_1S_2 からの応答を待つ．以後 VT_1S_1 は VT_1C と VT_1S_2 の通信を中継する．

（6） VPN 接続要求を受けた VT_1S_2 は VT_1S_1 から渡された S1 の FQDN を DNS サーバに問い合わせ，S1 の IP アドレスを取得する．

（7） VT_1S_2 は S1 宛ての ICMP エコー要求を送信し，S1 から ICMP エコー応答を受け取る．

（8） ICMP エコー応答を受け取った VT_1S_2 は VGW_1 からの VPN 接続要求に応答し，VPN を確立する．VPN 確立後，VT_1S_2 は (6) で取得した S1 の IP アドレスを DNS Proxy に転送し，DNS Proxy は，DNS クエリを監視してその応答としてこの IP アドレスをアプリケーションへ返す．

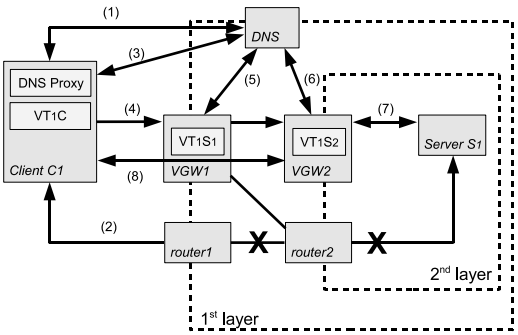

図 1 方式 1 による VPN 確立手順例
Fig. 1 VPN connection procedure by the method 1.

*1 たとえば，通信の切断要求パケット（FIN）で応答する．

4.1.2 プライベートアドレスでの動作

プライベートアドレスを利用している組織の場合には，接続を確立する過程でのみ一時的に使用するグローバルアドレスを用意した上で，4.1.1 項の手順の中で以下の変更を加える．

> 手順 (1) および手順 (5) で DNS サーバが返すアドレスを上記のグローバルアドレスに変更する．最後に手順 (6) で S1 が返すアドレスは，S1 に割り当てられたプライベートアドレスとする．

なお，プライベートネットワークを利用する場合には，クライアントとサーバがそれぞれのセグメント内において偶然に同じアドレスを割り当てられること（IP アドレスの衝突）が起こりうる．このような IP アドレスの衝突が発生した場合，クライアント側，サーバ側のそれぞれで未使用の IP アドレス（仮アドレス）を見つけてこれを通信相手の IP アドレスとし，サーバ側に最も近い VGW において送信元の IP アドレスを仮アドレスに，また宛先となっている仮アドレスを本来のアドレスにそれぞれ変換する方法[13] で回避できる[⋆1]．

文献 2) では LDAP を用いて中間経路情報を管理しているが，LDAP サーバの場所も DNS サーバに登録する必要があるため，経路情報の管理コストは方式 1 と同程度である．

ただし，この文献 2) の方法では SRV レコードを利用しているため，VPN ドメインは DNS ドメインのいずれかと一致している必要があるという制約があった．本提案方式では途中のルータが直接応答するため，このような制約はない．

4.2 方式 2 の詳細

方式 2 の実装は，クライアントの通信を監視する VPN Agent と，実際の VPN 接続を担当する VTun 改造版 2 と，エラー応答に VGW の情報を付加する[⋆2] TCP FIN Responder（以下，TFR と呼ぶ）からなる．

VPN Agent はクライアントの通信を監視し，必要に応じて VTun クライアント（VT_2C）を起動する．また，組織内の各ルータでは TFR を，各 VGW_i では VTun サーバ（VT_2S_i）を動作させておく．

クライアント（C1）がサーバ（S1）と TCP で通信する場合を例に本方式の詳細を述べる（**図 2** 参照）．

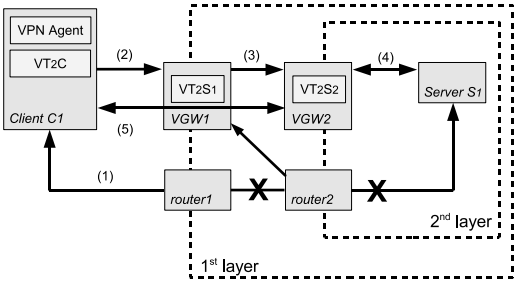

図 2 方式 2 による VPN 確立手順例
Fig. 2 VPN connection procedure by the method 2.

(1) C1 上のアプリケーションプログラムは S1 と TCP を用いて通信するために S1 宛ての SYN パケットを送信する．VPN Agent はこの SYN パケットを記録しておく．ルータ（router1）上で動作している TFR は S1 宛ての SYN パケットに対して VGW_1 の情報を付加した FIN パケットで応答する．

(2) VPN Agent は C1 上で VTun クライアント（VT_2C）を起動し，SYN パケットを VT_2C に渡す．VT_2C は SYN パケットを VGW_1 上の VT_2S_1 に渡すことで，VT_2S_1 に VPN 接続要求を行い，VT_2S_1 からの応答を待つ．

(3) VT_2S_1 は VPN 接続要求を受けると，VPN 用に確保している IP アドレスの中から 1 つを取り出してクライアント用に予約し（以下，**IP_1** と呼ぶ），FreeBSD の divert 機能を利用して IP_1 を宛先とするパケットを受信できるように IPFW の設定を変更する．VT_2S_1 は VT_2C から受け取った SYN パケットの送信元 IP アドレスを IP_1 に書き換えて S1 に送信し，(1) と (2) の VPN Agent，VT_2C と同様の動作を行い，IP_1 を確保している IP アドレスの中に戻し，VT_2S_1 は VGW_2 上の VT_2S_2 に VPN 接続要求を行い，VT_2S_2 からの応答を待つ．以後 VT_2S_1 は VT_2C と VT_2S_2 の通信を中継する．

(4) VT_2S_2 は VPN 接続要求を受けると，VPN 用に確保している IP アドレスの中から 1 つを取り出してクライアント用に予約し（以下，**IP_2** と呼ぶ），divert 機能を利用して IP_2 を宛先とするパケットを受信できるように IPFW の設定を変更する．VT_2S_2 は VT_2S_1 から受け取った SYN パケットの送信元 IP アドレスを IP_2 に書き換えて S1 に送信し，S1 から SYN+ACK パケットを受け取る．

⋆1 未実装．
⋆2 これは，TCP の非標準の応答であるため通信経路上で遮断される可能性がないとはいえない．しかし，多くの ISP ではこの種のパケットを遮断していないので，実際に問題になる可能性が残るのはクライアント側の組織内の IPS（Intrusion Protection System）によって遮断される場合のみである．

(5) VT_2S_2 は VT_2S_1 からの VPN 接続要求に応答し，VPN を確立する．VT_2S_2 は VPN 用のアドレスとして IP_2 を C1 に割り当て，以後 C1 の物理インタフェースの IP アドレスと IP_2 を相互にアドレス変換する．

(6) VPN 確立後，VT_2S_2 は S1 から受け取った SYN+ACK パケットを VPN を利用して C1 に送信し，C1 は，ACK パケットを VPN を利用して S1 に送信し，TCP コネクションを確立する．

5. 評　　価

5.1 節では，実装した両方式について特徴を比較し各方式を利用するための前提条件を明らかにする．また，5.2 節では接続を確立するのに要する時間を測定し，実用的な環境下での使用に耐えるかどうかを確認する．

5.1 両方式の比較

両方式とも通信開始時のパケットをモニタする仕組みを持ち，その中に含まれる VPN 接続を必要とするパケットを契機とし，階層型 VPN 接続を確立する動作を始める．そのため，利用者は VPN 接続確立のための動作を意識する必要がないという透過的動作を実現できている．

方式 1 では ICMP パケットを利用するため，クライアントとサーバ間の経路上で ICMP パケットがフィルタリングされている場合には利用できないが，方式 2 は ICMP パケットがフィルタリングされていても利用可能である．

方式 1 は VPN 確立後にサーバの A レコードを問い合わせるため，VPN を確立して通信したいサーバにプライベート IP アドレスを割り当てることができる．一方，方式 2 ではグローバル IP アドレスを割り当てる必要がある．

方式 1 では，DNS クエリを契機とするため，アプリケーションはサーバの IP アドレスではなく，FQDN を指定して通信しなければならないが，方式 2 はサーバの IP アドレスを指定して通信する場合でも利用可能である．

方式 2 では 4.2 節で述べた機能をルータへ追加する必要があるが，方式 1 ではその必要はない．

各方式を利用するための前提条件の主なものを**表 1** にまとめておく．

5.2 接続時間の評価

階層構造を持つ VPN 接続を，透過的動作によって確立するのに要する時間を評価するために，実験環境として**図 3** のようなネットワークを構築した．それぞれの計算機は 100BASE-TX により接続されている．なお，各計算機の CPU は Pentium M 2.00 GHz，メモリは 1 GB，OS は FreeBSD6.1-RELEASE である．

表 1 各方式の前提条件
Table 1 Conditions for each method.

	方式 1	方式 2
ICMP の到達性	必要	不要
プライベートアドレスの使用	可	否
ルータへの追加機能	不要	必要

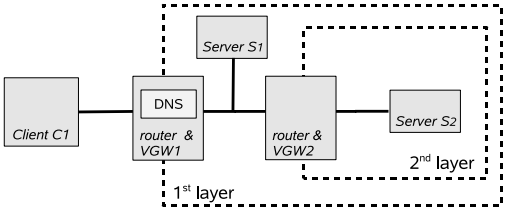

図 3 実験環境
Fig. 3 Experimental environment.

表 2 VPN 確立時間
Table 2 VPN connection establishment time.

	平均（ミリ秒）	
	1 階層	2 階層
方式 1	115	117
方式 2	133	147

また，C1 が S1 と通信するために VGW1 と VPN を確立する場合と，C1 が S2 と通信するために VGW2 と VPN を確立する場合のそれぞれで仮想リンクの確立に要する時間を 10 回計測し，平均値を算出した（**表 2**）．

方式 1，方式 2 を実装して実験した結果，利用者が意識することなく VPN を利用できることを確認した．また，VPN 確立までにかかる時間は約 0.1 秒であり，TCP のタイムアウトの懸念もなく実用上問題ないと考えられる．

VPN 確立に要するステップの少ない方式 2 が方式 1 より VPN 確立に時間がかかったのは方式 2 の動作手順の (3)，(4) で行う IPFW の設定変更に時間がかかっているためであると考えられる．

表 2 に示した結果より，1 階層をたどるのにかかる時間は方式 1 では約 2 ミリ秒，方式 2 では約 14 ミリ秒である．組織の規模によっては多段の階層をたどることもありうるが，この程度の遅延時間ならば実用上許容範囲であろう．

6. おわりに

本論文では，企業や大学等の大規模で階層構造を有する組織に対して利用者が透過的に仮想リンクを確立できるシステムを提案し実装した．さらに動作実験を行い提案法の有用性を確認した．

提案した 2 つの方式は，それぞれ前提条件を満たさないと利用できない．いずれの方式を用いるかは，サーバ側の管理者が決めることであるが，サーバとクライアント間で特定のパケットが通過するかどうかにも依存するので，単純には決められない．たとえば，両方の方式を実装し，まず方式 1 を試して，それに失敗した場合（ICMP によるエラーを受信した場合，あるいは，タイムアウトした場合）に限り方式 2 を試すようにすれば，可用性を高めることができる．

謝辞 本研究は，総務省特定領域重点型研究開発，大規模組織における仮想ネットワーク構築に関する研究開発（041108001）の補助による．

参考文献

1) 岡山聖彦，山井成良，石橋勇人，安倍広多，松浦敏雄：代理ゲートウェイを用いた SOCKS ベースの階層的 VPN 構成法，情報処理学会論文誌，Vol.42, No.12, pp.2860–2868 (2001).
2) 岡山聖彦，山井成良，金出地友治，石橋勇人，安倍広多，松浦敏雄：階層型 VPN のための LDAP サーバを用いた経路制御手法，情報処理学会論文誌，Vol.45, No.1, pp.46–55 (2004).
3) 福井健太，岡山聖彦，山井成良，石橋勇人，松浦敏雄：階層型 VPN における効率的なアクセスポリシ管理手法，情報処理学会論文誌，Vol.47, No.4, pp.1136–1145 (2006).
4) 大西宇泰，岡山聖彦，山井成良，石橋勇人，松浦敏雄：階層型 VPN における証明書を利用したアクセス制御手法，情報処理学会研究報告 2004-DSM-34 Vol.2004, No.77, pp.25–30 (2004).
5) 岡山聖彦，山井成良，河野圭太，石橋勇人，松浦敏雄：階層型 VPN における QoS およびアクセスポリシを考慮した経路選択手法，情報科学技術フォーラム情報技術レターズ，Vol.4, pp.293–296 (2005).
6) 岡山聖彦，山井成良，石橋勇人，安倍広多，松浦敏雄：階層型 VPN における効率的なアクセスポリシ管理手法，情報処理学会論文誌，Vol.47, No.4, pp.1136–1145 (2006).
7) 大西宇泰，岡山聖彦，山井成良，石橋勇人，松浦敏雄：階層型 VPN における証明書を利用したアクセス制御手法，情報処理学会分散システム/インターネット運用技術研究会研究報告，2004-DSM-34-5, pp.25–30 (2004).
8) 土居正行，岡山聖彦，山井成良，石橋勇人，安倍広多，松浦敏雄：階層型 VPN における他ドメインの証明書を用いたユーザ単位のアクセス制御，情報処理学会分散システム/インターネット運用技術研究会報告，2006-DSM-40, pp.67–72 (2006).
9) Okayama, K., Yamai, N., Ishibashi, H., Abe, K. and Matsuura, T.: An Efficient Management Method of Access Policies for Hierarchical Virtual Private Networks, *2nd IEEE/CreateNet/ICST International Conference on COMmunication System softWAre and MiddlewaRE* (*COMSWARE2007*) (2007).
10) 萱嶋 信，寺田真敏，藤山達也，小泉 稔，加藤恵理：多重ファイアウォール環境に適した VPN 構築方式の提案，電子情報通信学会論文誌 D-I, Vol.J82-D-I, No.6, pp.772–778 (1999).
11) Virtual Tunnels over TCP/IP networks (2007-2). http://vtun.sourceforge.net/
12) 河合洋明，坂根栄作，豊田博俊，岡山聖彦，山井成良，石橋勇人，安倍広多，松浦敏雄：階層型 VPN における利用者から透過な仮想リンク構成方式の提案，情報処理学会分散システム/インターネット運用技術研究会報告，2007-DSM-44, pp.71–76 (2007).
13) 青柳禎矩，高橋ひとみ，斉藤匡人，間 博人，徳田英幸：Shepherd：利用者主導型仮想プライベート・サブネットワーク構築機構，電子情報通信学会技術研究報告，NS2006-202, pp.227–232 (2007-3).

(平成 19 年 6 月 11 日受付)
(平成 19 年 12 月 4 日採録)

豊田 博俊

平成 3 年筑波大学第一学群自然学類卒業．平成 6 年筑波大学教育研究科教科教育専攻修了．平成 13 年大阪市立大学理学研究科後期博士課程単位取得退学．平成 7 年米国フェルミ国立加速器研究所にて客員研究員（2 年間）．平成 11 年大阪産業大学教養部非常勤講師．平成 19 年より大阪市立大学非常勤講師．日本物理学会員．

河合 洋明

平成 17 年大阪学院大学情報学部情報学科卒業．平成 19 年大阪市立大学大学院創造都市研究科都市情報学専攻情報基盤研究分野修了．平成 19 年三菱電機情報ネットワーク株式会社入社．

坂根　栄作（正会員）

平成 12 年 3 月大阪市立大学大学院理学研究科物理学専攻後期博士課程単位修得退学．博士（理学）．平成 18 年 1 月大阪大学サイバーメディアセンター特任助手，平成 19 年 4 月より同特任助教．グリッドコンピューティング，主に運用管理技術に関する研究を行う．日本物理学会，電子情報通信学会各会員．

岡山　聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．平成 17 年同大学総合情報基盤センター助手．平成 19 年同助教．博士（工学）．インタネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

山井　成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，総合情報基盤センター）助教授を経て，平成 18 年より同教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

石橋　勇人（正会員）

昭和 62 年京都大学大学院工学研究科修士課程情報工学専攻修了．平成元年同博士後期課程情報工学専攻退学後，京都大学大型計算機センター助手，大阪市立大学学術情報総合センター講師等を経て平成 19 年より大阪市立大学大学院創造都市研究科教授．博士（情報学）．オーバレイネットワーク，ネットワークセキュリティ，システム管理・運用等に関する研究に従事．人工知能学会，電子情報通信学会，IEEE，ACM 各会員．

安倍　広多（正会員）

平成 4 年大阪大学基礎工学部情報工学科卒業．平成 6 年同大学大学院博士前期課程修了．同年 NTT 入社．平成 8 年大阪市立大学学術情報総合センター助手．平成 12 年同講師．平成 15 年同大学院創造都市研究科講師．平成 17 年同助教授，平成 19 年同准教授，現在に至る．博士（工学）．オペレーティングシステム，P2P システム，分散システム管理技術等に興味を持つ．IEEE，電子情報通信学会各会員．

松浦　敏雄（フェロー）

昭 50 年大阪大学基礎工学部情報工学科卒業．昭 54 年同大学院基礎工学研究科（情報工学専攻）後期博士課程退学後，同大学基礎工学部助手．平 4 年同大学情報処理教育センター助教授，平 7 年大阪市立大学教授．平成 15 年同大学大学院創造都市研究科教授，現在に至る．博士（工学）．分散システム運用技術，情報教育等に興味を持つ．ACM，IEEE，電子情報通信学会各会員．