階層型 VPN のための LDAP サーバを用いた経路制御手法

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[†††]

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，通信先に応じて次ホップの VPN ゲートウェイを決定する必要がある．しかし，階層型 VPN に対応可能な従来の VPN リンク確立方式では，次ホップの情報をクライアントおよび各 VPN ゲートウェイが保持する静的な経路表で管理するので，VPN ドメインの増加にともなって上位 VPN ドメインにおける管理の手間が大きくなるという問題がある．そこで本論文では，LDAP サーバを用いた経路制御手法を提案する．提案法では，LDAP サーバを用いて VPN ゲートウェイを管理することにより，認証情報も含めた経路情報を効率良く管理することができる．さらに，VPN ドメインを DNS のドメインと一致するように構成し，DNS サーバに LDAP サーバの情報を持たせることにより，クライアントおよび各 VPN ゲートウェイは，DNS サーバと LDAP サーバへの問合せによって次ホップの VPN ゲートウェイを自動的に決定する．提案法の有効性は，SOCKS5 を拡張することによってクライアントと VPN ゲートウェイを実装し，これらを用いて実施した性能評価実験によって確認している．

A Routing Method with LDAP Servers for Hierarchical Virtual Private Networks

Kiyohiko Okayama,[†] Nariyoshi Yamai,[††] Yuuji Kanadechi,[††]
Hayato Ishibashi,[†††] Kota Abe[†††] and Toshio Matsuura[†††]

VPN (Virtual Private Network) is one of important technologies on the Internet. With VPN, we can securely access to resources in the organizational network via the Internet. In VPNs having hierarchical structure, clients and VPN gateways (VGWs) have to determine the next hop VGW according to the location of the destination. However, in the existing VPN methods, administrative cost is fairly large because the locations of next-hop VGWs are managed by static routing tables. In this paper, we propose a routing method for hierarchical VPNs. In the proposed method, LDAP servers are introduced for managing the routing and authentication information of VPN gateways efficiently. Moreover, clients and VGWs can determine the next hop VGW dynamically by mapping VPN domains to DNS domains and by storing the information of LDAP servers to DNS servers. The effectiveness of our method is confirmed by the experiment on the actual network using clients and VPN gateways based on our method.

1. はじめに

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，以下 VPN という）が注目されている．VPN にはさまざまな実現方法があるが，ホスト–ホスト間で VPN リンクを構成するものと，ホスト–ネットワーク間（あるいはネットワーク–ネットワーク間）で VPN リンクを構成するものに分けられる．前者は VPN を利用するアプリケーションクライアントとサーバの両方に VPN のためのソフトウェアを組み込まなければならないのに対し，後者の多くはアプリケーションサーバへの組み込みを必要としないので，本論文では後者の VPN 実現方法を対象とする．

また，VPN は本来，ネットワークの 2 点間に仮想

† 岡山大学工学部
Faculty of Engineering, Okayama University
†† 岡山大学総合情報処理センター
Computer Center, Okayama University
††† 大阪市立大学大学院創造都市研究科
Graduate School of Creative Cities, Osaka City University

的なリンクを設けるための技術である．しかし，組織内のネットワークを外部から護るために，現在ではファイアウォールの導入などによって外部からの特定の通信を遮断することが一般的であるため，本論文では，組織内など一様なアクセスポリシを持つ範囲（以下，VPN ドメインという）を定義し，その外部との接点に VPN ゲートウェイ（以下，VGW という）を設けることにより，特定のネットワークサービスに対して外部からのアクセスを VGW が制御するような用法を前提とする．このとき，大規模な組織では，組織全体を外部から護るだけでなく，組織の内部においても，ある部署のネットワークを他部署から護りたいという要求がある（たとえば，大学の付属病院などにおいては，大学内の他部署からのアクセスも制限する必要がある）．このような場合には，VPN ドメインを組織の内部構成と同様に階層的に構成（以下，階層型 VPN という）するのが自然であり，組織外にあるクライアントが組織の最も内側の VPN ドメイン内にアクセスするには，最も外側の VPN ドメインから内側に向かって 1 つずつ VGW をたどる必要がある．

階層型 VPN に対応できる既存の VPN リンク確立方式としては，SOCKS バージョン 5 プロトコル[1]に独自の機能を追加した SOCKS5[2]の多段プロキシ機構を利用する方法（以下，従来法 1 という），PPTP の通信を中継することによって複数の VGW をたどる方法[5]（以下，従来法 2 という），SOCKS バージョン 5 プロトコルを拡張して複数の VGW をたどる方法[3]（以下，従来法 3 という），代理サーバを VGW として VPN ドメインごとに配置する方法[4]（以下，従来法 4 という），SOCKS5 を拡張して 1 つの VPN リンクのみで最も内側の VPN ドメインにアクセスする方法[6]（以下，従来法 5 という）が知られている．これらの従来法では，クライアントあるいは上位の VGW からの要求を受けた VGW が，自動的に次に接続すべき VGW（以下，次ホップの VGW という）に通信を中継する機能を持つが，いずれの方法も，クライアントおよび VGW 間の経路制御機能は，クライアントおよび各 VGW のそれぞれが保持する静的な経路表☆により実現されている．したがって，クライアントおよび各 VGW はあらかじめ次ホップの VGW の情報（ホスト名や IP アドレス，VGW との接続に必要な認証情報など）を経路表に登録しておかなければならず，経路表に登録すべき VGW の数が増加するに従って，これらの追加・変更・削除にともなう管理の手間が大きくなるという問題がある．

そこで，本論文では，経路情報を LDAP[7]サーバで管理することにより，次ホップの VGW を自動的に決定し，VGW 接続時に必要な認証情報を効率良く管理することのできる手法を提案する．提案法では，各 VPN ドメインに LDAP サーバを設置し，VGW の情報を LDAP サーバに登録する．LDAP サーバのディレクトリデータベースのスキームは管理者が自由に定義できるので，VGW のホスト名や IP アドレスだけでなく，VGW 接続時に必要な認証情報なども効率良く管理することが可能である．さらに，VPN ドメインを DNS[8),9)]のドメインと一致するように構成したうえで，各 VPN ドメインの LDAP サーバを DNS に登録することにより，クライアントおよび各 VPN ゲートウェイは，DNS サーバと LDAP サーバへの問合せによって次ホップの VPN ゲートウェイを自動的に決定することができる．このとき，組織内の DNS 設定によっては，DNS サーバへの問合せの結果，直接通信不能な LDAP サーバの IP アドレスを得る場合があるが，クライアントおよび VGW に再帰的な問合せ機能を導入することにより，正しい（すなわち，直接通信可能な）LDAP サーバの IP アドレスを自動的に検索することが可能である．

以下，2 章では，従来法における経路制御の問題点を考察する．3 章では本論文で提案する LDAP サーバを用いた経路制御手法について述べ，4 章では提案法を従来法 5 の実装に適用して行った性能評価実験および結果について述べる．最後に，5 章では結論と今後の課題について述べる．

2. 従来法の問題点の考察

階層型 VPN では，組織外にあるクライアントが組織内部の VPN ドメイン内のサーバにアクセスする場合，クライアントはサーバと直接通信できないので，VPN ドメインの外側から VGW を 1 つずつたどることにより，1 つ以上の VPN リンクを確立する必要がある．このとき，VPN リンクの構成という点に注目すると，以下の 3 つの方式に分類できる．

方式 1 クライアントおよび各 VGW はそれぞれが保持する経路表に従い，クライアントに近い順に隣接（直接通信可能な）する VGW との間に VPN リンクを確立する．

方式 2 クライアントからサーバに至るまでの経路上にある VGW に対して，クライアントと各 VGW との間で VPN リンクを確立することを 1 ホップ

☆ ここでいう経路表とは，ネットワーク層（IP）レベルではなく，VPN ドメインとそれに対応する次ホップの VGW の情報を記載したものである．

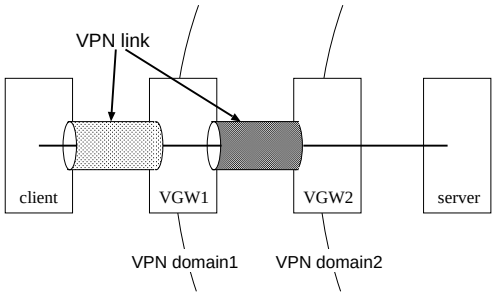

図 1 方式 1 における VPN リンクの確立例
Fig. 1 An example of VPN links in method 1.

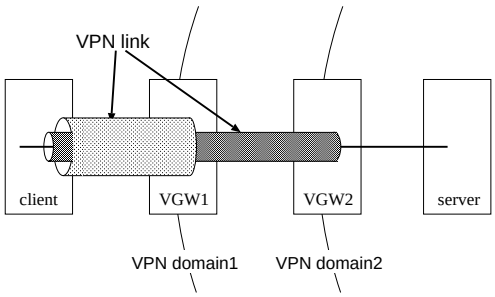

図 2 方式 2 による VPN リンクの確立例
Fig. 2 An example of VPN links in method 2.

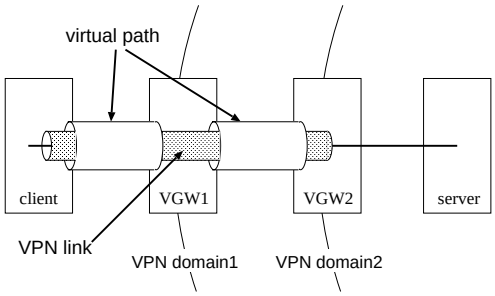

図 3 方式 3 による VPN リンクの確立例
Fig. 3 An example of VPN links in method 3.

ずつ繰り返す．

方式 3 方式 1 の VPN リンクを認証機能のみを持った仮想パスと見なし，クライアント〜終点の VGW までの各区間において仮想パスを確立した後，クライアントと終点の VGW との間のみで 1 つの VPN リンクを確立する．

1 章で述べた従来法 1〜5 では，使用されるプロトコルや実装が異なるが，VPN リンクの構成方式としては，従来法 1 および 2 は方式 1，従来法 3 は方式 2，従来法 4 および 5 は方式 3 にそれぞれ対応する．

方式 1〜3 において，VPN ドメインの階層数が 2 の場合の VPN リンク確立例を，それぞれ，**図 1**，**図 2**，**図 3** に示す．なお，各図において，VPN ドメイン 1 が組織ネットワーク全体の VPN ドメイン，VPN ドメイン 2 が部署ネットワークなどの VPN ドメインに相当する．組織の規模によっては，VPN ドメインの階層数が 3 以上になる場合もあるが，通信を中継する VGW が増加するだけであるので，以降では説明の簡単化のため VPN ドメインの階層数を 2 として議論する．

ここで，通信の安全性を確保するために，すべての VPN リンクで通信内容の暗号化を行う場合，方式 1 および 2 では，各 VPN リンクで暗号化および復号を繰り返すので，VPN ドメインの階層数の増加にともなって暗号化通信にともなうオーバヘッドが増大する．さらに，方式 1 については，途中の VGW（VGW1）で通信内容がいったん復号されるので，VGW への不正侵入を許した場合には，通信内容が漏洩する危険性がある．これに対し，方式 3 では，VPN ドメインの階層数にかかわらず VPN リンクの数は 1 つであるため，暗号化通信にともなうオーバヘッドは方式 1 および 2 よりも小さいと考えられ，しかも，方式 1 のように途中の VGW で通信内容が復号されることはない．

以上のように，VPN リンクの構成方式は異なるものの，従来法は，クライアントからサーバの属する VPN ドメインに至るまでの各 VGW を自動的にたどる機能を持つ．このとき，クライアントは通信先のサーバの IP アドレスや FQDN のみを指定して VPN リンクの確立を試みるので，クライアントや VGW は通信先に応じて次ホップの VGW を決定しなければならない．このため，従来法では，クライアントおよび各 VGW が経路表を持ち，通信先に応じて次ホップの VGW を決定している．経路表の管理，すなわち，経路表に対するエントリの追加・変更・削除は，クライアントおよび VGW の管理者が手作業で行う．

しかし，このような経路制御方法では，クライアント（多くの場合はユーザである）や VGW の管理者は，次ホップの VGW をあらかじめ知っておかなければならない．このため，クライアントが VPN ドメインをまたがって移動する場合（たとえば，図 1 において，クライアントが VPN ドメイン 1 の外側からだけでなく，VPN ドメイン 1 の内側からもサーバにアクセスする場合）や，クライアントが複数の組織へのアクセス権限を持つ場合には，自己の経路表に次ホップの VGW の情報（ホスト名や IP アドレス）を複数登録しなければならず，これらの情報に変更があった場合には，クライアントの管理者自身が自己の経路表を変更する必要がある．また，各 VGW の管理者も同様に，1 つ下位のすべての VPN ドメインの VGW を自己の経路表に登録しなければならない．したがって，

複雑な VPN ドメイン構成を持つ組織では，経路表に登録する VGW が増加するにつれて，これらの追加・変更・削除にともなう管理の手間も増大するという問題が発生する．

3. 経路制御手法の提案

2 章で述べた問題は，クライアントおよび各 VGW の保持する経路表が，次ホップの VGW に依存することに起因する．したがって，問題を解決するためには，クライアントおよび各 VGW は経路表を持たず，アクセス時に自動的に次ホップの VGW に関する情報を入手できればよい．

本章では，これを実現するための，経路情報の管理方法と次ホップの VGW を自動的に特定するための方法について述べた後，これらを用いた VPN リンク確立手順について述べる．

3.1 経路情報の管理方法

階層的に構成された VPN ドメインにおいて，クライアントおよび VGW が次ホップの VGW に接続するためには，次ホップの VGW の IP アドレスに加え，VPN リンク確立時の認証情報も必要になる．たとえば，SOCKS5 では認証に Kerberos [10),11)] を用いており，認証時には Kerberos のレルム名や鍵配布サーバのホスト名などの情報が必要となる．このような認証情報は，VGW に接続して認証を行う場合には必要不可欠であるため，VGW の IP アドレスとともにまとめて管理できることが望ましい（以下，認証情報も含めて経路情報という）．

そこで提案法では，経路情報を効率的に管理する方法として LDAP を用いる．LDAP サーバのディレクトリデータベースは階層構造を持つので，階層的に構成された VPN ドメインごとの情報を管理するのが容易であるだけでなく，データベースオブジェクトの属性を定義することにより，さまざまな情報を扱うことができる．

具体的には，各 VPN ドメインに LDAP サーバを設置する．各 LDAP サーバのディレクトリデータベースでは，自 VPN ドメインを根とする木構造を構成し，少なくとも根ノードに自 VPN ドメインの VGW の経路情報を属性として登録する．これにより，VPN ドメイン名をキーとして LDAP サーバに問合せを行えば，次ホップの VGW に関する経路情報を得ることが可能になる．

また，自 VPN ドメイン以下の VPN ドメインを木構造のノードに割り当て，下位の VPN ドメインの VGW の経路情報を対応するノードの属性として登録する方法も考えられる．この場合，自 VPN ドメインよりも下位の VPN ドメインでは，LDAP サーバを設置する必要はないので，各 VPN ドメインに LDAP サーバを設置する場合に比して管理の手間は小さくなる．ただし，自 VPN ドメインの管理者は下位 VPN ドメインの構造を把握しなければならず，下位 VPN ドメインの VGW が自 VPN ドメインの LDAP サーバにアクセスできるように設定する必要があることに注意する．

3.2 VPN ドメインに対する LDAP サーバの特定方法

経路情報を LDAP サーバで管理する場合，接続先の VGW に対応する LDAP サーバを特定する方法が問題となる．これを解決するには，LDAP サーバの情報を管理する仕組みを新たに実現する方法も考えられるが，この場合には導入や管理のコストが高くなる．そこで，提案法では，クライアントがサーバにアクセスする際，上位から下位に向かって隣接する各 VPN ドメインの VGW を 1 つずつ順番にたどることを前提としたうえで，標準的なインターネットの名前管理システムである DNS を利用する．DNS では，インターネット使用されるホストの名前空間をドメインの概念を用いて階層化し，ドメインごとに DNS サーバを置いてホスト名や IP アドレスなどのリソースを管理している．したがって，VPN ドメインを DNS ドメインと一致するように構成し，さらに，DNS で規定されている SRV レコード [12)] を利用すれば，DNS サーバへの問合せによって LDAP サーバを特定することが可能となる．

SRV レコードは，DNS ドメインに対するアプリケーションサーバを登録するためのリソースレコードである．SRV レコードには，サービス（TCP や UDP のポート）に対応するサーバの FQDN を定義することができ，サービス名，プロトコル名（TCP あるいは UDP），ターゲットドメイン名の 3 つ組をキーとして DNS サーバに問い合わせることにより，ターゲットドメインのサーバの FQDN を得る．たとえば，岡山大学（okayama-u.ac.jp）の LDAP サーバを検索する場合には，“_ldap._tcp.okayama-u.ac.jp” という文字列をキーとして問合せを行えばよい．以下，VPN ドメインと DNS ドメインとを区別する必要がない場合には，単にドメインと表記する．

3.3 DNS サーバの設定

一般的に，ファイアウォールが導入された組織ネットワークにおいて，DNS サーバの構成方法としては，以下の 2 つが考えられる．

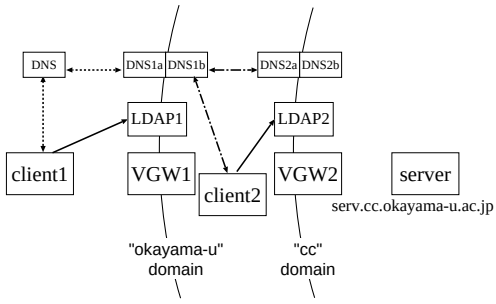

図 4 方法 1 の構成例
Fig. 4 An example structure of method 1.

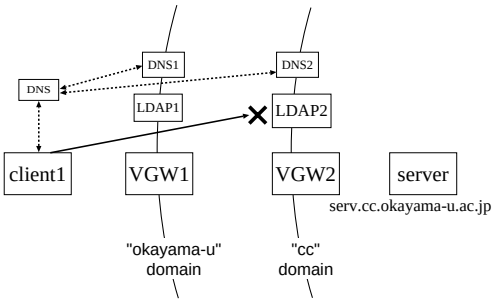

図 5 方法 2 の構成例
Fig. 5 An example structure of method 2.

方法 1 ドメインの内側と外側で DNS サーバを分ける場合

方法 2 ドメインを 1 つの DNS サーバで管理する場合

以下では，それぞれの方法において提案法を適用することを考える．

まず，方法 1 の構成例を**図 4** に示す．図 4 では，DNS1a および DNS2a がドメインの外側，DNS1b および DNS2b がドメインの内側からの問合せを処理し，DNS1b および DNS2b にはドメインの外側から直接アクセスできないものとする．このとき，各ドメインの LDAP サーバの情報はドメインの外側の DNS サーバに登録され，さらに，自ドメイン以下の任意のサブドメイン名をキーとする SRV レコードの問合せに対して，登録された LDAP サーバの FQDN を返すように設定する（たとえば，DNS1a は okayama-u ドメイン以下の任意のサブドメインをキーとした問合せに対して LDAP1 の FQDN を返す）．この場合，組織外および okayama-u ドメインにあるクライアント（client1 および client2）が cc ドメイン内部にあるサーバにアクセスしようすると，それぞれ 1 回の（SRV レコードの）問合せで正しい LDAP サーバの FQDN を得ることができる．ただし，3.1 節で複数の VPN ドメインの経路情報を 1 つの LDAP サーバにまとめた場合と同様に，DNS1a および DNS2a の管理者はすべてのサブドメイン名を把握しなければならない．

次に，方法 2 は，1 つのドメインに 1 つの DNS サーバを設置し，フィルタリングなどの設定によってドメインの外側からも DNS サーバにアクセス可能にする方法である．この場合の構成例を**図 5** に示す．方法 2 の場合，DNS の設定は方法 1 よりも単純であるが，組織外にあるクライアントが cc ドメイン内部のサーバにアクセスしようとした場合，cc ドメインの DNS サーバ（DNS2）から LDAP2 の情報を得る．このとき，組織外からは LDAP2 と直接通信できないので，次ホップの VGW を特定することができず，アクセスに失敗する．

これを解決するために，本研究では，クライアントおよび各 VGW に DNS サーバに対する再帰的な問合せ機能を導入する．具体的には，あるドメインの LDAP サーバとの通信に失敗した場合，自動的に 1 つ上位のドメインをキーとして SRV レコードを検索し，これを LDAP サーバとの通信が成功するまで繰り返すようにする．たとえば，図 5 の例では，クライアントが cc.okayama-u.ac.jp ドメインの LDAP サーバである LDAP2 との接続に失敗すると，1 つ上位のドメイン（okayama-u.ac.jp）をキーとして SRV レコードを検索する．これにより，検索の結果得られた LDAP1 に VGW の経路情報を問い合わせて，次ホップの VGW である VGW1 を特定することができる．

なお，ここでは，クライアントが LDAP2 に対して通信を試みた場合，okayama-u.ac.jp ドメインに設置されたファイアウォールの設定などにより，たとえばクライアントに対して通信不能を意味する ICMP エラーを返すなど，クライアントが通信の失敗を即座に検出できることを想定している．もし，ファイアウォールの設定によってこのようなエラーが返されない場合には，クライアントは LDAP2 への通信がタイムアウトするまで待たされることになる．

3.4 LDAP サーバに対する再帰問合せ

クライアントおよび VGW は DNS サーバへの問合せによって LDAP サーバを特定するが，クライアントはサーバの IP アドレスや FQDN のみを指定してアクセスを試みるため，サーバの FQDN だけでは，次ホップの VGW のドメイン名が分からない．このため，クライアントおよび VGW に対して，上述した DNS サーバへの再帰的問合せと同様に，LDAP サーバに対しても再帰的な問合せを行うようにする．

具体的には，クライアントおよびは VGW は自己の FQDN とサーバの FQDN とを比較し，一致する部分よりも 1 つ下位のドメイン名をキーとして LDAP

サーバに問合せを行い，問合せに失敗した場合には，さらに下位のドメイン名をキーとして，成功するまで再帰的に問合せを繰り返す．たとえば，図 5 において，クライアントの FQDN が “cl.sample.jp” である場合，クライアントはサーバの FQDN（serv.cc.okayama-u.ac.jp）と比較して “jp” までは同じことが分かるので，1 つ下位である “ac.jp” をキーとして LDAP1 に問合せを行うが，LDAP1 はこのドメインに関する情報を保持していないため失敗する．そこで，さらに下位である “okayama-u.ac.jp” をキーとして再び問い合わせることにより，VGW1 の経路情報を得る．なお，クライアントの FQDN が分からない場合には，サーバの FQDN の最上位ドメインから問合せを開始する．

VGW においても同様に，自己のドメイン名とサーバの FQDN を比較する．図 5 において，VGW1 が自己の FQDN とサーバの FQDN を比較すると，“okayama-u.ac.jp” まで一致するため，“cc.okayama-u.ac.jp” をキーとして LDAP2 に問合せを行った結果，VGW2 の経路情報を得る．一方，VGW2 では，自己の FQDN とサーバの FQDN との比較の結果ドメイン名の部分が完全に一致するので，VGW2 はサーバと直接通信可能であることが分かる．

以上のように，クライアントおよび VGW は自己のドメインを基準とし，下位ドメインに向かって再帰的に問合せを行うので，VPN ドメインと DNS ドメインの階層構造が完全に一致する必要はない．たとえば，組織の最上位の DNS ドメインでは VPN ドメインを構成せず（つまり，VGW を設置しない），1 つ下位の DNS ドメインが VPN ドメインとして並列に構成されている場合でも，クライアントは再帰的問合せによって適切な次ホップの VGW の経路情報を得る．また，DNS ドメインの階層数が 3 以上の組織において，中間の DNS ドメインでは VPN ドメインを構成しない場合☆でも，上位ドメインの VGW は再帰的問合せによって適切な次ホップの VGW の経路情報を得る．このとき，3.1 節で述べたように，下位ドメインには LDAP サーバを設置せず，これらのドメインの経路情報を上位ドメインの LDAP サーバが管理している場合があるが，VGW は自己のドメイン以下を問合せのキーとして使用するので，誤って自己よりも上位ドメインの経路情報を得ることはない．

☆ たとえば，“cc” ドメインの直下に “exp” ドメインがあり，“exp” および “okayama-u” ドメインには VPN ドメインを構成するが，“cc” ドメインには VPN ドメインを構成しない場合などが考えられる．

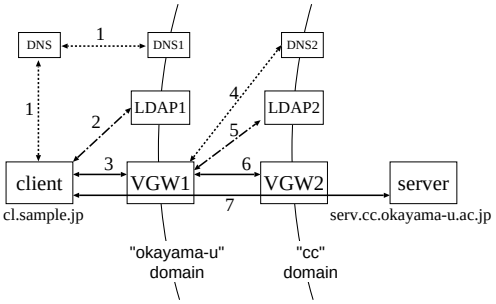

図 6 提案法による VPN リンク確立手順の例
Fig. 6 An example of procedure for making VPN link with proposed method.

3.5 VPN リンクの確立手順

提案法を従来法 5 に適用した場合の，VPN リンク確立手順の例を**図 6** に示す．図において，組織のドメイン（okayama-u.ac.jp）の下位に cc というドメインが設置されており，各ドメインに VGW，LDAP サーバ，DNS サーバが置かれている．また，LDAP1 および LDAP2 はそれぞれ，VGW1 および VGW2 の経路情報を管理し，DNS1 および DNS2 はそれぞれ，LDAP1 および LDAP2 に対する SRV レコードを保持するものとする．ただし，DNS1 は外部からの任意のサブドメインをキーとした SRV レコードの問合せに対して，LDAP1 の FQDN を返すように設定されているものとする．

このような構成において，組織外にあるクライアント（cl.sample.jp）が cc ドメイン内のサーバ（serv.cc.okayama-u.ac.jp）にアクセスする手順を以下に示す．

(1) クライアントは最寄りの DNS サーバを経由して，cc.okayama-u.ac.jp に対する LDAP サービスの SRV レコードを DNS1 に対して問い合わせ，LDAP1 の FQDN と IP アドレスを得る．

(2) クライアントは自己の FQDN とサーバの FQDN を比較し，LDAP1 に対して 3.4 節で述べた再帰問合せを行う．この例では，ac.jp に対する問合せに失敗し，okayama-u.ac.jp に対する問合せの結果，VGW1 の経路情報を得る．

(3) クライアントは VGW1 に対し，従来法 5 と同様にして仮想パスを確立する．

(4) VGW1 は cc.okayama-u.ac.jp に対する LDAP サービスの SRV レコードを DNS2 に対して問い合わせ，LDAP2 の FQDN と IP アドレスを得る．

(5) VGW1 は自己の FQDN とサーバの FQDN を比較し，okayama-u までは同じであることが分かる．そこで，VGW1 は 1 つ下位のドメイン名（cc）

をキーとして次ホップの VGW の情報を LDAP2 に問い合わせ，VGW2 の経路情報を得る．

(6) VGW1 は VGW2 に対し，従来法 5 と同様にして仮想パスを確立する．

(7) クライアントは従来法 5 と同様にして VGW2 との間に VPN リンクの確立を試み，成功した場合はサーバとの通信が可能となる．

以上のように，提案法では，クライアントや各 VGW は従来法における経路表を用いることなく，通信先のサーバの FQDN に基づいて自動的に次ホップの VGW の情報を得ることができる．各ドメインの管理者は，VGW の経路表の代わりに LDAP サーバと DNS サーバとを管理する必要があるが，従来法と違い，あるドメインの管理者は下位ドメインの経路情報をあらかじめ知る必要がないので，下位ドメインにおける経路情報の変更による影響をまったく受けない．同様に，クライアントの管理者（ユーザ）も，ある組織に対して最初に接続すべき VGW のホスト名や IP アドレスを知る必要がまったくないので，ユーザがアクセスを開始する際のネットワーク上の位置が頻繁に変化する場合や，ユーザが複数の組織にアクセス権限を持つ場合には，特に有効であると考えられる．

なお，VPN リンク確立方式にかかわらず，サーバに至るまでの各 VGW においてユーザの認証を行う場合には，認証を行うための秘密情報（暗号鍵など）を各 VGW に登録する必要がある．したがって，ユーザはどの VPN ドメインにどの秘密情報を登録するかを意識する必要があるが，ユーザが VGW に対して直接登録するのでなければ，VGW のホスト名や IP アドレスを把握する必要はない．また，各 VGW がクライアントのアクセス時に対話的にパスワードの入力を要求するような認証方法を用いる場合でも，VGW がユーザに対して VPN ドメインを提示するように実装すれば，ユーザは VPN ドメインとパスワードの対応関係のみを把握すればよく，通過する VPN ドメインの順序や VGW のホスト名などを把握する必要はない．さらに，Kerberos などのように，秘密情報を事前に登録しておけばアクセス時にはユーザと VGW が対話的に通信を行う必要のない認証方式であれば，通常の利用時には VPN ドメインの存在も意識する必要はない．

また，運用上の制約として，各 VPN ドメインの管理者が下位 VPN ドメインの情報を把握する必要がないように設定するためには，VPN ドメインの構成を DNS ドメインの階層構造に一致させたうえで，各 VPN ドメインに LDAP サーバを設置する必要があることがあげられる．ただし，下位 VPN ドメインに対する依存性をある程度許すのであれば，3.4 節で述べたように，VPN ドメインの構成を DNS ドメインの階層構造に完全に一致させる必要はない．さらに，もう 1 つの制約として，同一の VPN ドメインにアクセスポリシが例外的に異なるサーバが存在する場合には，提案法のみでは対応できないことがあげられる．たとえば，図 6 の “cc” ドメイン内に，外部に公開する Web サーバを設置する場合などがこれに相当する．このような例外的なサーバについては，ファイアウォールのフィルタリング設定などにより，VGW を通過することなく外部からアクセスできるようにする必要がある．

4. 実験と評価

3 章で述べたとおり，提案法を導入するためには LDAP サーバの設置や SRV レコードの設定が必要であるが，VPN ドメインと LDAP サーバの構成によっては，下位ドメインにまったく依存することなく VPN ドメインを運用することが可能である．特に，クライアントは次ホップの VGW を意識する必要がないので，ユーザに対する利便性が従来法よりも高いといえる．しかし，提案法では DNS サーバや LDAP サーバへの問合せが発生するため，VPN リンク確立に要する時間の増大が予想される．このため，提案法を従来法 5 の実装に適用して実験環境を構築し，VPN リンクの確立時間を計測することによって提案法の有効性の検証を行った．

4.1 実装と実験環境

提案法の実装は，実装が広く公開されている従来法 1（SOCKS5）をベースとする従来法 5 を対象とした．開発は，FreeBSD バージョン 4.X を搭載する AT 互換機上で行い，従来法 5 の socks サーバのソースコード（C 言語で記述）を変更することによって提案法のクライアントと VGW を実現した．具体的には，3.2 節および 3.3 節で述べた DNS サーバへの問合せ機能を加え，さらに，LDAP の実装の 1 つである OpenLDAP [13]（FreeBSD にバイナリパッケージとして付属）ライブラリを利用して，3.4 節で述べた LDAP サーバへの問合せ機能を追加している．なお，今回は FreeBSD を用いて実装を行ったが，SOCKS5 および OpenLDAP は他の UNIX や Windows 系の OS でも動作するため，他の OS への移植は比較的容易であると考えられる．また，通信先となるサーバの FQDN から次ホップの VGW を自動的に得る機能は特定の OS や実装に依存しないので，従来法 2 および

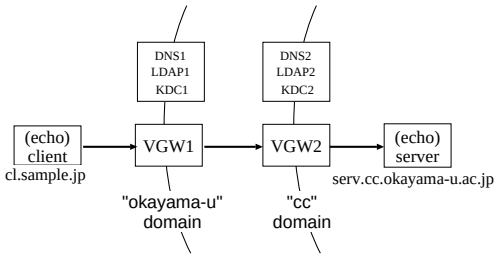

図 7 実験ネットワークの構成
Fig. 7 The structure of the experimental network.

4 のように，SOCKS 以外プロトコルをベースとした実装に関しても，クライアントおよび VGW が，自己の経路表を参照して次ホップの VGW を特定する機能を置き換えることによって適用可能であると考えられる．

一方，実験環境としては，**図 7** のような実験ネットワークを構築した．ドメインの階層数を 3 以上に設定しても，通信を中継する VGW が増えるだけであるため，階層数は必要最小限である 2 とし，okayama-u および cc という 2 つのドメインを構成したうえで，それぞれのドメインに，VGW，LDAP サーバ，DNS サーバ，および，Kerberos の鍵配布サーバである KDC を配置している（各 KDC のレルム名は，それぞれのドメイン名と同一とした）．図 7 において，DNS サーバ，LDAP サーバ，および，KDC を 1 台の計算機に割り当てているが，これらのサーバに同時にアクセスすることはないので，実験への影響はないと考えられる．また，DNS サーバについては，3.3 節で述べた再帰的なアクセスが発生しないよう，okayama-u ドメイン外部にあるクライアントが cc ドメインの LDAP サーバの SRV レコードを問い合わせた場合，okayama-u ドメインの LDAP サーバ（LDAP1）の FQDN が得られるように設定した．

なお，実験に使用した各計算機は，学内ネットワークを利用して，100 Mbps のリンクにより接続した．

4.2 実験結果と考察

実験は，okayama-u ドメインの外側にある echo（ポート番号 7）クライアントが，（最も内側の）cc ドメインにある echo サーバにアクセスする場合の，VPN リンク確立に要する時間を計測した．実際の計測は，従来法 5 および提案法に対して，VGW1 および VGW2 において Kerberos による認証を行う場合と行わない場合のそれぞれについて，VPN リンクの確立を 100 回実施し，echo クライアントのアクセス開始から echo サーバとの間でコネクションが確立するまでの時間の平均値を算出した．

表 1 実験結果
Table 1 Results of experiment.

	コネクション平均確立時間 (ms)	
	認証なし	認証あり
従来法 5	20.72	962.10
提案法	44.48	987.43

実験の結果を**表 1** に示す．認証の有無にかかわらず，従来法 5 と提案法の差は約 25 ms であり，今回の実験ではドメインの階層数を 2 としているため，提案法は従来法 5 に比して 1 つの VGW あたり約 12 ms 増加していることになる．組織の規模によっては，VGW を 3 つ以上経由する場合も考えられるが，組織内は比較的高速なリンクで構成されることや，表 1 から分かるように，認証を行う場合には，経路情報の問合せによる時間の増加よりも，認証に必要な時間の方がはるかに大きいことから，階層数の増加はあまり問題にならないと考えられる．

また，クライアントがインターネット上にある場合には，組織の最も外側の VGW へのアクセスに時間を要することが考えられる．しかし，一般的なネットワークアプリケーションにおいても，通常は DNS による名前解決を行ってからアプリケーションサーバにアクセスするので，提案法は実用上問題ないと考えられる．

5. おわりに

本論文では，階層型 VPN に対応した既存の VPN リンク確立方式における経路情報の管理方法に注目し，クライアントおよび VGW において下位ドメインに依存しない経路情報管理の実現を目的とした，LDAP サーバを用いた経路制御手法を提案した．さらに，既存の VPN リンク確立方式の拡張によって提案法を実装し，これを用いて性能評価実験を行うことにより，提案法が実用上問題がないことを確認した．

今後は，認証情報を含めた経路情報だけでなく，アクセスの可否や認証および暗号化の有無などのアクセスポリシを複数の LDAP サーバで効率良く管理するための手法を検討する予定である．

謝辞 本研究の一部は，文部科学省科学研究費平成 13〜14 年度基盤研究（C）（2）課題番号 13680421 の補助を受けている．ここに記して感謝の意を表する．

参考文献

1) Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: SOCKS Protocol Ver-

sion 5, RFC1928 (1996).
2) NEC: SOCKS Home Page. http://www.socks.nec.com/index.html
3) Kayashima, M., Terada, M., Fujiyama, T. and Ogino, T.: SOCKS V5 Protocol Extension for Multiple Firewalls Traversal, Internet Draft (1997). draft-ietf-aft-socks-multiple-traversal-00.txt.
4) 萱島 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).
5) 齋藤彰一，泉 裕，上原哲太郎，國枝義敏：多段のファイアウォールを越える PPP/PPTP 中継システムの実装と評価，情報処理学会論文誌, Vol.43, No.11, pp.3478–3488 (2002).
6) 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).
7) Wahl, M., Howes, T. and Kille, S.: Lightweight Directory Access Protocol (v3), RFC 2251 (1997).
8) Mockapetris, P.V.: Domain names — concepts and facilities, RFC 1034 (1987).
9) Mockapetris, P.V.: Domain names — implementation and specification, RFC 1035 (1987).
10) Kohl, J. and Neuman, C.: The Kerberos Network Authentication Service (V5), RFC1510 (1993).
11) Linn, J.: The Kerberos Version 5 GSS-API Mechanism, RFC1964 (1996).
12) Gulbrandsen, A., Vixie, P. and Esibov, L.: A DNS RR for specifying the location of services (DNS SRV), RFC 2782 (2000).
13) OpenLDAP Foundation: OpenLDAP Home Page. http://www.openldap.org/

(平成 15 年 5 月 8 日受付)
(平成 15 年 10 月 16 日採録)

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．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を経て，現在岡山大学総合情報処理センター助教授．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）．

金出地友治

平成 13 年岡山大学工学部情報工学科卒業．平成 15 年同大学院自然科学研究科博士前期課程修了．同年同総合情報処理センター研究支援推進員．ネットワークセキュリティの研究に従事．

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．平成 10 年大阪市立大学学術情報総合センター講師．平成 14 年同助教授．平成 15 年より同大学院創造都市研究科助教授．博士（情報学）．高速ネットワーク，ネットワーク管理システム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 年講師．平成 15 年同大学院創造都市研究科講師．博士（工学）．マルチスレッド機構の実装，オペレーティングシステムの設計等に興味を持つ．電子情報通信学会会員．

松浦 敏雄（正会員）

昭和 50 年大阪大学基礎工学部情報工学科卒業．昭和 54 年同大学院基礎工学研究科（情報工学専攻）博士後期課程退学後，同年大阪大学基礎工学部情報工学科助手．平成 4 年同大学情報処理教育センター助教授．平成 7 年大阪市立大学生活科学部教授．平成 8 年同大学学術情報総合センター教授．平成 15 年同大学院創造都市研究科教授，現在に至る．工学博士．ソフトウェア開発環境，ユーザインターフェイス，マルチメディア，情報教育等に興味を持つ．ACM，IEEE，電子情報通信学会各会員．