2003－DSM－29 (10)
2003／4／25

# 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† 金出地 友治†† 山井 成良†† 石橋 勇人‡ 松浦 敏雄‡

**概 要**

VPNドメインが階層的に構成されたネットワーク環境では，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が，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ドメインの増加に伴って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よ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サーバへの問い合わ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VGW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† Yuji Kanadechi†† Nariyoshi Yamai††
Hayato Ishibashi‡ Toshio Matsuura‡

**Abstract**

In Virtual Private Networks(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.

†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
‡大阪市立大学学術情報総合センター, Media Center, Osaka City University

# 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．

このようなVPNでは，組織内など同一のアクセスポリシを持つ範囲をVPNドメインと呼び，VPNドメインを跨る通信を制御するVPNゲートウェイ (以下VGWという) を設置する．組織外にあるクライアントは，VGWとの間にVPNリンクを確立することにより，VPNドメイン内部のサーバと通信することが可能になる．このとき，大規模な組織ではアクセスポリシが部署ごとに異なる場合が多いので，VPNドメインをインターネットのドメインと同様に階層的に構成 (以下，階層型VPNという) するのが自然である．このような構成において，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を辿る必要がある．

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[1]プロトコルの参照実装であるSOCKS5[2]の多段プロキシ機構を利用する方式や，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式[3]などがある (以下，これらをまとめて従来法という)．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 (以下，次ホップという)VGWに通信を中継する機能を持つが，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，管理の手間が大きいという問題がある．

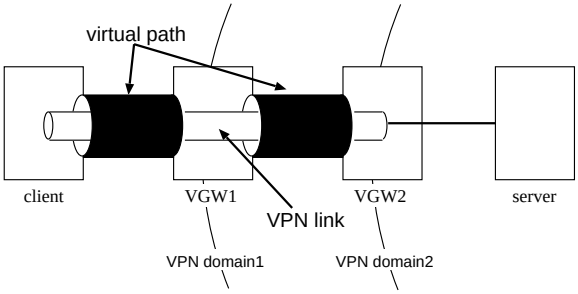


図 1: 文献[3]によるVPNリンクの確立例

そこで，本論文では，経路情報をLDAP[4]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よ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よく管理することが可能である．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た上で，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サーバへの問い合わ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．

以下，従来法の問題点を考察した後，提案法の概要と，提案法を文献[3]の方式に実装して行った性能評価実験について述べる．

# 2　従来法の問題点の考察

まず，VPNドメインの階層数を2とした場合の，文献[3]によるVPNリンクの確立例を図1に示す．図1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等のVPNドメインに相当する．組

織外にあるクライアントが，VPNドメイン2に設置されたサーバにアクセスする場合，クライアントは次ホップのVGWであるVGW1との間で仮想パスと呼ばれるコネクションの確立を試みる．必要に応じてVGW1はクライアントを認証し，仮想パスの確立に成功すると，VGW1は通信先から判断して，次ホップとなるVGW2との間に仮想パスを確立し，仮想パス間のパケットを中継する．そして，クライアントはVGW2との間でVPNリンクの確立を試み，これに成功するとサーバと通信を行なうことができる．なお，SOCKS5の多段プロキシ機構の場合も，複数のVGWを辿る手順は文献[3]と同様である．

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，このままではクライアントや途中のVGWは次ホップのVGWのIPアドレスを得ることができない．

このため，従来法では，クライアントおよび各VGWがIPと同様の経路表を持ち，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，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，クライアントの管理者(多くの場合はユーザである)は最も外側のVGWを，各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，クライアントが複数の組織へのアクセス権限を持つ場合や，組織のVPNドメイン構成が複雑な場合には，接続先のVGWの増加に伴って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

本章では，2で述べた諸問題を解決するための，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(以下，認証情報も含めて経路情報という)．例えば，SOCKS5では認証にKerberos[5]を用いており，認証時にはKerberosのレルム名が必要である．

経路情報を効率的に管理する方法として，提案法では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，組織の最も外側のVPNドメインを根とする木構造を構成し，各VPNドメインを木のノードに割り当てた上で，経路情報をノードの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サーバに問い合わせを行えば，経路情報を得ることが可能になる．

## 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が，提案法では，DNSのSRVレコード[6]を利用する．

SRVレコードとは，インターネットの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．例えば，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い合わせを行えばよい．

したがって，VPNドメインをDNSのドメインと一致するように構成すれば，クライアントやVGWは指定したVPNドメインの経路情報を管理するLDAPサーバを特定することが可能になる．この方法では，VPNドメインの構成に制約が生じるが，大規模な組織では，組織の構造に合わせてイ

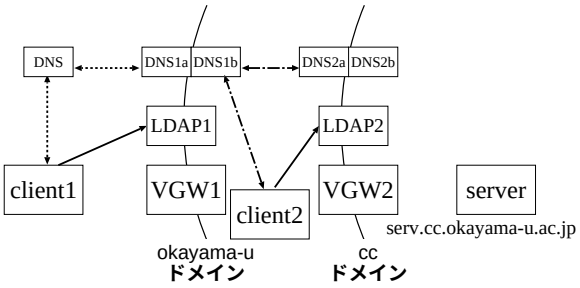


図 2: 方法1の構成例

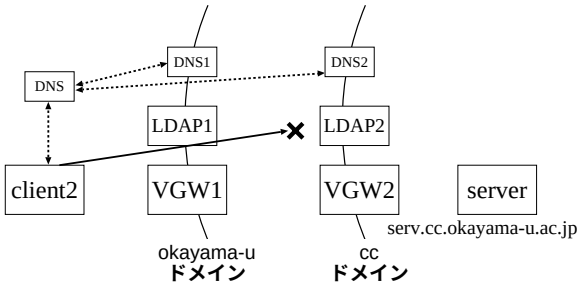


図 3: 方法2の構成例

ンターネットのドメインが構成されており，ファイアウォールなどもこれに合わせて設置されることが多いので，実用上は問題ないと考えられる．以下，VPNドメインを単にドメインという．

DNSを利用してLDAPサーバの(ネットワーク上の)位置を管理する場合，DNSサーバの構成方法が問題となる．VPNをファイアウォールの一種として捉えた場合，DNSサーバの構成方法としては，以下の2つが考えられる．

**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

方法1の構成例を図2に示す．図2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い合わせを処理し，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，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とした場合，前者の場合はDNS1aからLDAP1の情報を，後者の場合はDNS2aからLDAP2の情報を得るが，DNS1aおよびDNS2aの管理者はそれぞれのサブドメイン以下の内部構造を把握しなければならないので，管理の手間が大きい．

一方，方法2では，1つのドメインに1つのDNSサーバを設置し，フィルタリング等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3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に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．

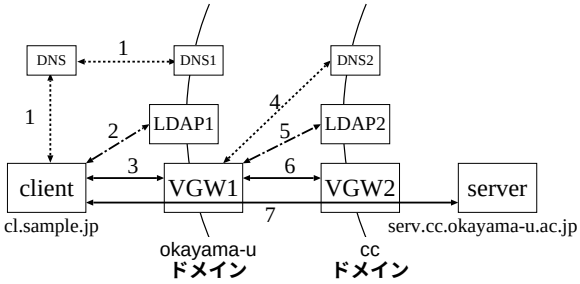


図 4: 提案法によるVPNリンク確立手順の例

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に再帰的なアクセス機能を導入する．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．たとえば，図3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．

## 3.3 VPNリンクの確立手順

提案法を文献[3]のVPNリンク確立方式に適用した場合の，VPNリンク確立手順の例を図4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はすべてのサブドメインのSRVレコードを保持しており，外部からの問い合わせに対して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，組織外のクライアント(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．なお，DNSの設定によってはLDAP2のFQDNとIPアドレスを得る場合があるが，この場合は3.2で述べた再帰問い合わせを行ない，最終的に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LDAP1のFQDNを比較し，jpまでは同じであることがわかる．そこで，クライアントはjpよりも下位のドメイン名をキーとして，クライアントが接続すべきVGWの情報を再帰的にLDAP1に問い合わせる．この例では，ac.jpに対する問い合わせに失敗し，okayama-u.ac.jpに対する問い合わせの結果，VGW1の経路情報を得る．

**(3)** クライアントはVGW1に対し，文献[3]の方法にしたがっ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LDAP2のFQDNを比較し，okayama-uまでは同じであることがわかる．そこで，VGW1はokayama-uよりも下位のドメイン名(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，文献[3]の方法にしたがって仮想パスを確立する．

**(7)** クライアントは文献[3]の方法にしたがって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．

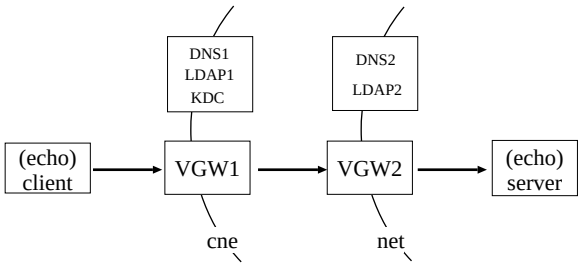


図 5: 実験ネットワークの構成

# 4 実験と評価

提案法は，クライアントやVGWに対してあらかじめ次ホップのVGWを登録する必要がないので，従来法に比して管理の手間が小さいことは明らかである．しかし，提案法はDNSサーバやLDAPサーバへの問い合わせが発生するため，提案法を文献[3]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 実験環境

実験環境として，図5のような実験ネットワークを構築した．実験において，ドメインの階層数は少なくとも2以上である必要があるため，cneおよびnetという2つのドメインを構成し，それぞれのドメインに，VGW，LDAPサーバ，DNSサーバを配置している．さらに，cneドメインには，Kerberosの鍵配布サーバであるKDCを配置している．図5において，DNSサーバおよびLDAPサーバ(さらに，cneドメインにでは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．なお，実験に使用した各計算機は，

表 1: 実験結果

| | 従来法 | 提案法 |
|---|---|---|
| 確立時間 (ms) | 851.19 | 883.97 |

学内ネットワークを利用して，100Mbps あるいは 10Mbps のリンクにより接続した．

### 4.2 実験結果と考察

実験は，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，従来法および提案法を適用した場合の VPN リンク確立方式のそれぞれについて，VPN リンクの確立を 400 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．いずれの場合も，VGW1 と VGW2 において Kerberos による認証を行っている．

実験の結果を表 1に示す．従来法と提案法の差は約 32ms 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，提案法は従来法に比して 1 つの VGW あたり約 16ms 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ので，階層数の増加は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，クライアントおよび VGW における経路情報管理の手間の軽減を目的とした，LDAP サーバを用いた経路制御手法を提案し，性能評価実験によって実用上問題がないことを確認した．

今後は，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 サーバで効率よく管理するための手法を検討する予定である．

## 参考文献


[1] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: *SOCKS Protocol Version 5*, RFC1928 (1996).

[2] NEC: *SOCKS Home Page*, http://www.socks.nec.com/index.html.

[3] 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).

[4] M. Wahl, T. Howes, S.Kille.: *Lightweight Directory Access Protocol (v3)*, RFC 2251 (1997).

[5] Kohl, J. and Neuman, C.: *The Kerberos Network Authentication Service (V5)*, RFC1510 (1993).

[6] A.Gulbrandsen, P. Vixie, L. Esibov.: *A DNS RR for specifying the location of services (DNS SRV)*, RFC 2782 (2000).