LL-3 階層型VPNのためのLDAPサーバを用いた経路制御手法

A Routing Method with LDAP Servers for Hierarchical Virtual Private Networks

岡山 聖彦† 金出地 友治†† 山井 成良‡ 石橋 勇人§ 松浦 敏雄§

Kiyohiko Okayama Yuji Kanadechi Nariyoshi Yamai Hayato Ishibashi Toshio Matsuura

1 まえがき

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．ネットワーク接続型VPNの場合，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する(以下，階層型VPNという)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．いずれもクライアントからの要求に応じて自動的に複数のVGWを辿る機能を持つが，クライアントおよびVGW間の経路制御機能は静的な経路表により実現されているので，管理の手間が大きいという問題がある．

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，次に接続すべき(以下，次ホップという)VGWを自動的に決定する手法を提案する．提案手法では，各VPNドメインにLDAPサーバを設置し，VGWの情報(IPアドレスなど)をLDAPサーバに登録する．さらに，各VPNドメインのLDAPサーバをDNSに登録することにより，クライアントやVGWが適切なLDAPサーバから次ホップのVGWの情報を自動的に得ることができる．

以下，既存のVPNリンク確立方式の問題点を考察した後，提案手法の概要と，提案手法を文献[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 問題点の考察

1で述べた既存のVPNリンク確立方式では，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，クライアントおよび各VGWは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 階層型VPNのためのLDAPサーバを用いた経路制御手法の提案

本章では，2で述べた問題点を解決するための，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，提案手法では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，提案手法では，DNSのSRVレコード[5]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ドメインをインターネットのドメインと対応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

†岡山大学工学部，Faculty of Engineering, Okayama University

††岡山大学大学院自然科学研究科，Graduate School of Natural Science and Technology, 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

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．

3.3 VPNリンクの確立手順

提案手法を文献[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1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，LDAP2への直接接続に失敗するので，上位のドメインに向かって再帰的に問い合わせを行う．

(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)～(6) VGW1はクライアントと同様の手順を実行し，VGW2との間に仮想パスを構成する．

(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．

4 実験と評価

提案手法は，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，静的な経路表を用いる方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，提案手法はDNSサーバやLDAPサーバへの問い合わせが発生するため，提案手法を文献[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手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1とほぼ同じ構成の実験ネットワークを構築した．実験ネットワークでは，DNS1とLDAP1，DNS2とLDAP2をそれぞれ1台の計算機に割り当てているが，DNSサーバとLDAP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，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，VPN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VPN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，文献[3]のVPNリンク確立方式(以下，従来手法という)と，提案手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．

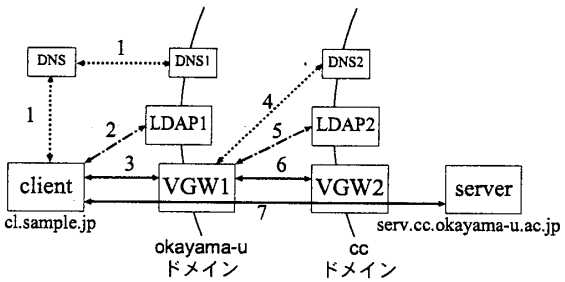

図 1: 提案手法によるVPNリンク確立手順の例

	従来手法	提案手法
確立時間(ms)	851.19	883.97

表 1: 実験結果

実験の結果を表1に示す．従来手法と提案手法の差は約30msであり，この差はDNSサーバおよびLDAPサーバに問い合わせを行う時間のみであるので，提案手法は従来手法に比して1つのVGWあたり約15ms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，提案手法は実用上問題ないと考えられる．

5 あとがき

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