階層型VPNにおける効率的なアクセスポリシ管理手法

岡山聖彦[†] 山井成良[†] 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ドメインと呼ぶが，VPNドメインが階層的に構成されたネットワークでは，アクセスポリシ（認証および暗号化通信の有無やその方法など）が通信先のVPNドメインごとに異なるので，あるVPNドメインにおいて，下位VPNドメインごとに異なるアクセスポリシを設定しなければならない場合がある．しかし，従来のVPN技術では，アクセスポリシを各VPNゲートウェイが保持する静的な設定ファイルに記述するので，あるVPNドメインの管理者は下位VPNドメインの管理者と協調してアクセスポリシを設定する必要がある．このため，組織の内部構造が複雑になるにつれて，アクセスポリシ管理の手間が増大するという問題がある．そこで本論文では，このような問題を解決するための効率的なアクセスポリシ管理手法を提案する．提案手法では，アクセスポリシが階層的に表現されたデータベースと，アクセスポリシを自動的かつ再帰的に下位VPNドメインに問い合わせる機能を持つポリシサーバを各VPNドメインに導入することで，アクセスポリシ管理の手間を軽減している．提案手法の有効性は，提案手法に基づいて実装したポリシサーバを用いて実施した性能評価実験によって確認している．

An Efficient Management Method of Access Policies for Hierarchical Virtual Private Networks

Kiyohiko Okayama,[†] Nariyoshi Yamai,[†] 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, since each VPN domain has different access policy (whether VPN gateway should perform authentication and data encryption, and so on), the administrator of a VPN domain may need to configure access policies which are different from every VPN subdomain. However, in the existing VPN methods, since access policies are stored in static configuration file of each VPN gateway, the administrator of a VPN domain has to cooperate with the other administrators of its subdomains. Therefore, management cost of access policies becomes fairly large if the organization has complicated structure. In this paper, we propose an efficient management method of access policies for hierarchical VPN. To reduce management cost, we introduce databases where access policies are represented hierarchically and policy servers which can inquire access policies to lower VPN domains automatically and recursively to each VPN domains. The effectiveness of our method is confirmed by the experiment on the actual network using policy servers 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．

† 岡山大学総合情報基盤センター
Information Technology 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

また，VPN は本来，ネットワークの 2 点間に仮想的なリンク（以下，VPN リンクという）を設けるための技術である．しかし，組織のネットワークを外部から守るため，現在ではファイアウォールの導入などにより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．ここでアクセスポリシとは，接続元/接続先ホストと接続ユーザの情報に基づいて決定されるアクセス制御の方針であり，認証および暗号化通信の有無や方式，アクセスの可否といったパラメータが含まれる．

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のが自然である．以下，このような構成の VPN を階層型 VPN といい，本論文では階層型 VPN を議論の対象とする．

階層型 VPN 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 をたどる必要がある．これに対応可能な既存の VPN リンク確立方式としては，SOCKS5[1] の多段プロクシ方式，PPP/PPTP 中継方式[2]，SOCK プロトコルバージョン 5[3] の拡張方式[4]，代理サーバ方式[5]，仮想パス方式[6),7)]（以下，これらをまとめて従来手法という）などがある．従来手法はいずれも，複数の VGW を自動的にたどる機能を持つが，アクセスポリシを各 VGW が保持する静的な設定ファイルで管理するので，各 VGW で下位の VPN ドメインごとに異なるアクセスポリシを設定するためには，上位の VPN ドメインの管理者は，あらかじめ組織の内部構成を把握するとともに，必要であれば下位 VPN ドメインの管理者と自ドメインで設定すべきアクセスポリシを調整したうえで設定ファイルに登録する必要がある．このため，内部構成が複雑になるにつれて，アクセスポリシ管理の手間が増大するという問題がある．

本論文では，上述した問題を解決するための，効率的なアクセスポリシ管理手法を提案する．提案手法では，文献 7) の VPN リンク確立方式で用いられている LDAP[8] サーバのディレクトリデータベースを利用して，下位の VPN ドメインごとに異なるアクセスポリシを階層的に表現するとともに，下位 VPN ドメインが自 VPN ドメインに対して要求するアクセスポリシを自動的に問い合わせる機能を持つポリシサーバを各 VPN ドメインに導入する．これにより，自 VPN ドメインにおけるアクセスポリシの決定権を下位の VPN ドメインに委譲することが可能となるので，各 VPN ドメインの管理者は，下位の VPN ドメインが自 VPN ドメインに要求するアクセスポリシを変更しても，自 VPN ドメインの設定を変更する必要がなくなる．

以下，2 章では，従来手法の問題点を考察する．3 章では本論文で提案するアクセスポリシ管理手法について述べ，4 章では提案手法の実用性を確かめるための性能評価実験について述べる．5 章では提案手法に対する今後の課題を中心に考察を行い，最後に，6 章で本論文をまとめる．

なお，文献 7) の VPN リンク確立方式と同様に，本論文においても，個々の VPN ドメインの範囲を DNS[9),10)] のドメインの範囲と一致☆ させることを前提とする．以下，特に明記しない限り，ドメインという用語は VPN ドメインとそれに対応する DNS ドメインの両方を指すものとする．

2. 従来手法の問題点の考察

1 章で述べたように，階層型 VPN ではドメインごとにアクセスポリシが異なる場合が多いので，上位ドメインではアクセスを中継する下位ドメインごとに異なるアクセスポリシを設定する必要が生じることがある．たとえば，**図 1** のようなドメイン構成において，大学全体のドメインに設置された VGW1 では，大学外にあるクライアントが内部にアクセスする場合には認証を行うものとする．このとき，付属病院のドメインにおいて，他組織の医師に対してこのドメイン内にあるサーバへのアクセスを許可しようとすると，VGW1 と VGW2 の両方にアカウントを登録するか，

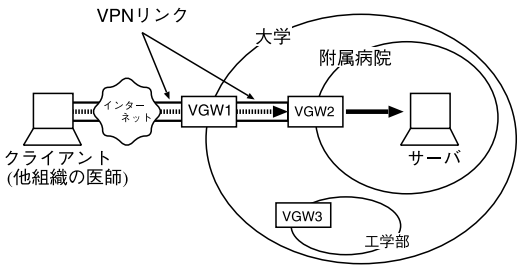

図 1 階層型 VPN
Fig. 1 An example of hierarchical VPN.

☆ VPN ドメインと DNS ドメインの階層構造は完全に一致しなくてもよい（すべての DNS ドメインが VPN ドメインを形成しなくてもよい）ことに注意する．

あるいは，外部から付属病院ドメインにアクセスする際にはVGW2でのみ認証を行い，VGW1では認証しないように設定する必要がある．後者の場合，VGW1では「中継先が付属病院ドメインの場合には認証を行わない」という設定を施さなければならない．

従来手法のうち，このような設定を行うことができるのは，文献1)，6)，7)のVPNリンク確立方式である☆．これらの方式では，アクセスポリシを各VGWの設定ファイルで保持し，接続先に対応するアクセスポリシのルールを記述する．

このとき，自ドメインにおいて接続先となる下位ドメインごとに異なるアクセスポリシを設定しようとすると，自ドメインの管理者は，VGWの設定ファイルに接続先のドメイン名と対応するアクセスポリシを列挙することになる．したがって，自ドメインの管理者は，下部組織の構造（自ドメインより下位のドメイン構成）と，各下位ドメインの管理者からのアクセスポリシ要求（自ドメインのVGWが下位ドメインにアクセスを中継する際の動作）とをあらかじめ把握したうえで，各VGWの設定ファイルに手作業で登録しなければならない．そのため，各ドメインの管理者間で調整が必要となり，特に内部構造が複雑な組織において，下位ドメインからのアクセスポリシ要求が頻繁に変更されるような場合には，上位ドメインにおけるアクセスポリシ管理の手間が大きくなるという問題がある．

なお，VGWの設定ファイルには，接続元，接続先およびユーザ名の組に対してアクセスポリシを指定することが可能である．アクセスポリシとしては，中継の可否，認証の有無とその方式，暗号化通信の有無とその方式を記述することができ，接続元および接続先には，ホスト名，IPアドレス，ドメイン名，ネットワークアドレスのいずれかが記述できる．しかし，議論の簡単化のため，以降の説明ではアクセスポリシを認証の有無のみとし，接続先のドメイン名のみに基づいて決定されるものとする．

3. アクセスポリシ管理手法の提案

3.1 提案手法の概要

2章で述べた問題は，あるドメインの管理者が自ドメインのアクセスポリシを設定する際に，下位ドメインからのアクセスポリシ要求を事前に把握しなければならないことに起因する．したがって，下位ドメインにアクセスを中継する際のアクセスポリシの決定権を，必要に応じて下位ドメインに委譲することができれば，この問題を解決できると考えられる．具体的には，上位ドメインのVGWがアクセスを中継する際の動作を下位ドメインの管理者が決定できるようにして，さらに，上位ドメインではアクセスの中継時に自動的に下位ドメインにアクセスポリシを問い合わせ，その結果に基づいて中継動作を行うようにすればよい．

上述した機能を実現するためには，各ドメインのアクセスポリシ設定に決定権の委譲を表現する方法と，アクセスの中継時にアクセスポリシを下位ドメインに問い合わせる仕組みが必要となる．以下，それぞれについて述べた後，提案手法によるVPNリンク確立手順について述べる．

なお，本論文では，文献7)のVPNリンク確立方式が導入されたネットワークを前提とする．この方式は，他の方式に比して暗号化通信のためのオーバヘッドが小さいだけでなく，接続先ホストFQDNのみに基づいて次に接続すべきVGWを自動的に決定するという，他の方式にはない特長を持つ．特に，2番目の特長，すなわち，事前に他ドメインの経路情報（VGWのホスト名やIPアドレス）を把握する必要がない点は，本論文で提案するアクセスポリシ管理手法との親和性が高いと考えられる．

3.2 アクセスポリシの基本的な表現方法

接続先となる下位ドメインごとに異なるアクセスポリシを設定するためには，アクセスポリシをドメイン単位で表現する必要がある．たとえば，図1のようなドメイン構成の場合，2章で述べたような運用を行おうとすると，大学ドメインのVGWにおけるアクセスポリシ設定には，接続先が工学部ドメインの場合は自ドメインでの中継時に認証を行い，付属病院ドメインの場合は認証を行わないといった動作を記述することになる．これに対し，文献7)のVPNリンク確立方式では，各ドメインに設置されたLDAPサーバのディレクトリデータベース（以下，データベースという）に経路情報を格納しているので，提案手法ではこれをそのまま利用する．

まず，各ドメインのデータベースでは，自ドメインを根とする木構造を形成し，必要に応じて下位ドメインを木のノードに割り当てたうえで，ノードの属性としてアクセスポリシを登録する．そして，アクセス制御の際には，VGWはLDAPサーバに対して接続先のドメイン名をキーとして問合せを行い，LDAPサーバでは，データベースを検索することにより，最長一致するドメインのノードに登録されたアクセスポリシを返すものとする．これにより，下位ドメインのノー

☆ 文献2)，4)，5)については，中継の可否のみしか設定できないか，あるいはアクセス制御についてまったく記述されていない．

ドの設定値が上位ドメインのノードと同じ場合には，設定を上位ドメインのノードに集約して，下位ドメインのノードを省略することができる．また，マッチしたドメインのノードにアクセスポリシが定義されていない場合には，上位ドメインのノードに登録されたアクセスポリシが適用されるものとする．

3.3 アクセスポリシ決定権の委譲

3.3.1 権限委譲の表現方法

特定の下位ドメインに対してアクセスポリシの決定権を委譲するために，提案手法では，前節で述べたデータベースのノードの属性として，権限委譲フラグ，アクセスポリシ要求および中継フラグの 3 つを追加する．権限委譲フラグは，自ドメインでのアクセスポリシの決定権を下位ドメインに委譲することを意味し，このフラグが設定された場合には，下位ドメインにアクセスポリシの問合せを行うものとする．アクセスポリシ要求には，問合せの起点となる（上位の）ドメイン名と，それに対して返すべきアクセスポリシの値の組を列挙する．これにより，問合せを受けた下位ドメインでは，問合せの起点となる上位ドメインに応じて異なるアクセスポリシを返すことができる．このとき，問合せの起点となるドメイン名にはワイルドカード文字（*）を使用して，返すべきアクセスポリシの値が同じ組を 1 つにまとめることを可能とする．

一般的に，ファイアウォールにおいて特定のホスト宛のパケットを無条件で通過させるなどの特別な設定を施さない限り，あるドメインから（下位に向かって）直接通信可能なのは隣接する下位ドメインのみであるため，接続先のドメインが隣接する下位ドメインよりもさらに下位にある場合には，問合せを中間にあるドメインが中継しなければならない．中継フラグは，上位ドメインからの問合せをさらに下位のドメインに中継するための属性であり，問合せを行う上位ドメインに応じて中継するか否かを設定できるよう，アクセスポリシ要求の属性値として登録する．ただし，つねに接続先のドメインまで問合せを中継する必要はなく，中継フラグの代わりにアクセスポリシの値を設定すれば，中間のドメインが問合せに応答することも可能である．

3.3.2 権限委譲の設定例

図 2 にデータベースの例を示す．図の左から順に，組織全体を表す okayama-u ドメインとその直下にある cne ドメイン，さらに下位にある net ドメインの各 LDAP サーバが保持しているデータベースを示している．図中において，“○” は認証あり（自ドメインでの中継時に認証を行う），“×” は認証なしを意味し，

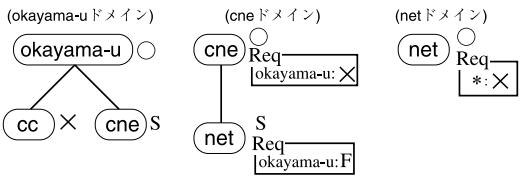

図 2 データベースの例
Fig. 2 An example of policy database.

“S” は権限委譲フラグ，“F” は中継フラグ，“Req” はアクセスポリシ要求をそれぞれ意味する．

図 2 の各データベースは，接続先のドメイン名をキーとして検索され，okayama-u ドメインのデータベースを検索する際，検索キーが cc.okayama-u.ac.jp（あるいはそのサブドメイン）であれば，ノード cc にマッチして「認証なし」が適用される．これは，okayama-u ドメインの VGW では認証を行わないことを意味する．また，検索キーに cc および cne 以外のドメインが指定された場合には，すべてノード okayama-u にマッチして「認証あり」が適用される．このように，上位ドメインと同様のアクセスポリシを適用する場合には，下位ドメインに対応するノードを登録しないことによってデータベースを小さくすることができる．

一方，検索キーが cne.okayama-u.ac.jp の場合には，okayama-u ドメインのデータベースでは cne ノードにマッチし，その属性として権限委譲フラグ（S）が設定されているため，cne ドメインにアクセスポリシを問い合わせる．問合せを受けた cne ドメインでは，cne.okayama-u.ac.jp をキーとしてデータベースを検索するとノード cne にマッチし，そこに登録されたアクセスポリシ要求（Req）が適用される．この例では，アクセスポリシ要求の属性値として設定された「認証なし」を返すので，okayama-u ドメインの VGW では認証を行わずにアクセスを中継する．

また，検索キーが net.cne.okayama-u.ac.jp の場合には，okayama-u ドメインのデータベースではノード cne にマッチし，検索キーが cne.okayama-u.ac.jp の場合と同様に，cne ドメインにアクセスポリシを問い合わせる．問合せを受けた cne ドメインでは，net.cne.okayama-u.ac.jp をキーとしてデータベースを検索した結果，ノード net にマッチし，そこに登録されたアクセスポリシ要求の属性値として中継フラグ（F）が得られるので，okayama-u ドメインからの問合せを net ドメインに中継する．そして，okayama-u ドメインから（cne ドメインを介して）問合せを受けた net ドメインでは，検索の結果，ノード net に登録されたアクセスポリシ要求が適用される．この例では，

アクセスポリシ要求のドメイン名の部分にワイルドカード（*）が指定されており，すべての問合せに対して「認証なし」を応答する．したがって，okayama-u ドメインの VGW では，接続先が net.cne.okayama-u.ac.jp ドメインの場合は認証を行うことなくアクセスを中継する．次に，cne ドメインでは，データベースの検索によりノード net に登録された権限委譲フラグが得られるので，net ドメインにアクセスポリシを問い合わせる．net ドメインは「認証なし」を応答するので，cne ドメインの VGW においても認証を行うことなくアクセスを中継する．最後に，net ドメインでは，データベースの検索により「認証あり」が得られるので，接続元ホストに対して認証を行い，認証に成功した場合は net ドメイン内の接続先ホストにアクセスを中継する．

図 2 において，cne ドメインのノード net のように権限委譲フラグと中継フラグの両方が設定されている場合，いずれも下位ドメインに対してアクセスポリシを問い合わせるが，前者は自ドメインが問合せの起点，後者はより上位のドメインが問合せの起点であることに注意する．

なお，組織のネットワークを外部から守るという点と，一般的に上位の部署は下位の部署を統括する役割を持つという点から，外部に近い上位ドメインが下位ドメインよりも強い権限を持つ必要があると考えられる．このため，データベースのノードに通常のアクセスポリシの値（認証の有無）と権限委譲フラグの両方が登録された場合には，前者を優先する．これは，下位ドメインにアクセスポリシの決定権を委譲している場合でも，一時的に無効にできることを意味する．

3.3.3 権限委譲の有効性と適用条件

提案手法におけるアクセスポリシ決定権の委譲は，全面的委譲，すなわち，下位ドメインのアクセスポリシ要求を上位ドメインが無条件に受け入れることを意味する．今後の課題として，5 章で述べる部分的委譲を検討する必要があるが，全面的委譲か部分的委譲かにかかわらず，一般的には，組織全体の安全性が損なわれないよう，上位ドメイン管理者と下位ドメイン管理者との間であらかじめ合意を形成することが適用条件になると考えられる．

一方，上位ドメインがあらかじめ下位ドメインに対して権限を委譲しておけば，委譲するという方針自体が変わらない限り，上位ドメインにおけるデータベース設定を変更する必要がない．たとえば，共同研究などの理由により，他組織のユーザに組織内の下位ドメインにあるサーバなどを一時的に利用させたい場合，従来手法であれば，認証を必要とするすべての VGW でアカウントを作成するか，あるいは上位ドメインでは認証を行わないように設定する必要があるため，いずれの場合も各ドメインの管理者間での調整と上位ドメインにおける設定作業が必要となる．これに対し，アクセスポリシの決定権をあらかじめ下位ドメインに委譲しておけば，下位ドメイン管理者によるアクセスポリシ要求の変更のみで上位ドメインでの認証を一時的に無効にできるため，上位ドメインでは他組織ユーザに対するアカウント作成やデータベースの設定変更をまったく行う必要がない．

以上のことから，アクセスポリシ決定権の委譲は，下位ドメインのアクセスポリシ要求が比較的頻繁に変更されるような場合に有効である．

3.4 アクセスポリシ自動問合せ

3.4.1 ポリシサーバの導入

これまでに述べたデータベースに基づいて，アクセスポリシの検索や下位ドメインに対する問合せあるいは中継を行うために，提案手法では，ポリシサーバを導入する．ポリシサーバは，VGW と対をなすように各ドメインに設置し，同じドメインの VGW からの要求を受けて LDAP サーバを検索し，結果として得られたアクセスポリシを VGW に返す．このとき，LDAP サーバの検索結果として権限委譲フラグが得られた場合には，自動的に下位ドメインのポリシサーバに問合せを行う．

一方，上位ドメインからの問合せを受けたポリシサーバは，自ドメインの LDAP サーバを検索し，アクセスポリシ要求が得られればそれを上位ドメインのポリシサーバに返す．このとき，アクセスポリシ要求の属性値として中継フラグを取得した場合には，さらに下位のポリシサーバに問合せを中継し，その結果を上位ドメインのポリシサーバに返す．

なお，ネットワーク上のポリシサーバの位置（ホスト名または IP アドレス）を特定する方法として，文献 7) の LDAP サーバを特定する方法と同様に，DNS サーバの SRV レコード[11] を利用するものとする．

3.4.2 一括問合せ機能とキャッシュ機能

3.4.1 項で述べたポリシサーバの導入により，上位ドメインにおいて事前に下位ドメインからのアクセスポリシ要求を把握する必要はなくなるが，アクセスポリシの問合せにともなう通信が発生するため，データベースの設定によってはオーバヘッドが大きくなることが予想される．特に，接続先のドメインに至るまでのすべてのドメインにおいて，アクセスポリシの問合せが接続先，すなわち，最下位ドメインのポリシサー

バへ中継されるように設定されている場合，クライアントが途中の VGW に接続するたびに，接続先ドメインのポリシサーバまで問合せが発生することになる．

そこで提案手法では，ポリシサーバに一括問合せ機能とキャッシュ機能を追加する．あるドメインのポリシサーバに対して，上位ドメインから問合せがあった場合，LDAP サーバの検索結果として上位ドメインからの問合せの中継を意味する中継フラグと，自ドメインのアクセスポリシ決定権を下位ドメインに委譲していることを意味する権限委譲フラグの両方が得られた場合には，必ずそのドメインを起点とする問合せが生じることは明らかである．そこで，上位ドメインからの問合せを中継する際のメッセージに，自らを起点とする問合せのメッセージを多重化して送信し，その結果得られた自ドメインに対するアクセスポリシ要求をキャッシュするものとする．これにより，クライアントが自ドメインの VGW に接続した際には，下位ドメインに対して問合せを行うことなくアクセスポリシを決定することができる．

ポリシサーバにおけるアクセスポリシのキャッシュは，一括問合せ時だけでなく，通常の問合せ時や自ドメインの LDAP サーバを検索する際にも行う．これにより，同一接続先に対する 2 回目以降のアクセス時には LDAP サーバの検索を行う必要がないので，アクセスポリシの決定にともなって生じる通信のオーバヘッドを大幅に削減できると考えられる．

このとき，キャッシュとして保存されるのは接続先，すなわち，自組織内のドメインに対するアクセスポリシであるので，一般的なキャッシュに比してあまり大きくならないと考えられる．このため，キャッシュには有効期限を設けないが，下位ドメインにおけるアクセスポリシ要求の変更に対応するため，上位ドメインに対するキャッシュ削除機能を導入する．具体的には，下位ドメインにおいてアクセスポリシ要求の設定を変更すると，キャッシュ削除要求メッセージを直上ドメインのポリシサーバに送信する．このメッセージは組織の最上位ドメインのポリシサーバまで中継され，これを受信した各ポリシサーバは，メッセージの送信元ドメインに関するキャッシュを削除するものとする．

3.5 VPN リンク確立手順

提案手法を文献 7) 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 3** に示す．ただし，文献 7) の VPN リンク確立方式に含まれる機能（認証および経路の自動決定）に関する通信は割愛し，アクセスポリシの決定に関する通信手順のみを示す．

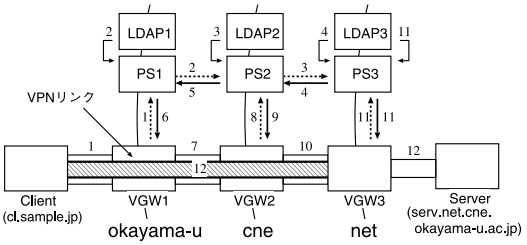

図 3 提案手法による VPN リンク確立例
Fig. 3 An example of VPN links of our method.

図 3 において，組織のドメイン（okayama-u）の下位に cne ドメイン，さらにその下位に net ドメインが設置されている．各ドメインには，VGW，ポリシサーバ（PS），LDAP サーバ（LDAP）が設置されているものとする．一方，各 LDAP サーバのデータベースは，図 2 のように設定されているものとする．この例では，すべての上位ドメイン（okayama-u および cne）において，接続先のドメインまでアクセスポリシの問合せが行われる．

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 net ドメイン内のサーバ（serv.net.cne.okayama-u.ac.jp）にアクセスする手順を以下に示す．

(1) クライアントが VGW1 に対しコネクションを確立すると，VGW1 は PS1 にアクセスポリシを問い合わせる．
(2) PS1 が通信先のサーバの FQDN を用いて LDAP1 を検索すると，データベースのノード cne にマッチする．このノードには権限委譲フラグが登録されているので，PS1 は PS2 にアクセスポリシを問い合わせる．
(3) PS2 が通信先のサーバの FQDN を用いて LDAP2 を検索すると，データベースのノード net にマッチし，okayama-u へのアクセスポリシ要求として中継フラグを取得する．この例では，ノード net に登録された権限委譲フラグも得られるので，PS2 は okayama-u ドメインからの問合せの中継と，cne ドメインを起点とする問合せを，PS3 に対して一括して行う．
(4) PS3 が通信先のサーバの FQDN を用いて LDAP3 を検索すると，okayama-u ドメインと cne ドメインからのいずれの問合せに対しても，データベースのノード net に登録されたアクセスポリシ要求（認証なし）にマッチするので，結果を PS2 に返す．
(5) PS2 は，自ドメイン（cne）に対するアクセスポ

リシ要求をキャッシュするとともに，okayama-u ドメインに対するへのアクセスポリシ要求を PS1 に返す．

(6) PS1 は，自ドメイン（okayama-u）に対するアクセスポリシ要求をキャッシュするとともに，そのアクセスポリシを VGW1 に返す．

(7) VGW1 は取得したアクセスポリシ（認証なし）に従い，認証は行わず，クライアント-VGW1 間で確立されたコネクションを仮想パスとする．さらに，VGW1 は VGW2 に対してコネクションを確立し，以降パケットを透過的に転送する．

(8) VGW2 は PS2 にアクセスポリシを問い合わせる．

(9) PS2 は一括問合せで取得したアクセスポリシのキャッシュがあるので，それを VGW2 に返す．

(10) VGW2 は取得したアクセスポリシ（認証なし）に従い，認証は行わず，VGW1-VGW2 間で確立されたコネクションを仮想パスとする．さらに，VGW2 は VGW3 に対しコネクションを確立し，以降パケットを透過的に転送する．

(11) VGW3，PS3 も同様に動作し，アクセスポリシとして「認証あり」を得るので，クライアントと認証を行う．認証に成功すると，VGW2-VGW3 間で確立されたコネクションを仮想パスとする．

(12) VGW3 は，クライアントとの間で VPN リンクを確立するとともに，接続先のサーバとコネクションを確立し，以降パケットを透過的に転送する．これにより，クライアント–サーバ間での通信が可能となる．

4. 実験と評価

3 章で述べたとおり，提案手法では下位ドメインに対するアクセスポリシの自動問合せを実現することにより，下位ドメインに対してアクセスポリシの決定権を委譲すれば，下位ドメインからのアクセスポリシ要求に変更があっても，上位ドメインのデータベースを変更する必要がない．しかし，提案手法では，LDAP サーバの検索や下位ドメインに対するアクセスポリシの問合せの際に通信が生じるので，VPN リンク確立に要する時間の増加が予想される．このため，提案手法を実装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り，提案手法の有効性の検証を行った．

4.1 実装と実験環境

4.1.1 提案手法の実装

提案手法の実装は，実装が広く公開されている SOCKS5 をベースとする文献 7) の VPN リンク確立方式を対象とした．開発は FreeBSD バージョン 4 を搭載する AT 互換機上で行い，3.4 節で述べたポリシサーバを新規に作成するとともに，VGW の実装を変更してポリシサーバへのアクセス機能を組み込んだ（いずれも C 言語で記述）．

なお，提案手法の実装は従来手法をベースとしているため，2 章で述べた従来手法とほぼ同内容のアクセスポリシを記述することができる．具体的には，3.2 節で述べたデータベースの各ノードに対して，必要に応じて接続元およびユーザ名を追加することにより対応している．ただし，データベースの検索に接続先の FQDN を利用するため，接続先として指定できるのは現状ではドメイン名のみである．

4.1.2 実 験 環 境

実験環境として，**図 4** のような実験ネットワークを構築した．一括問合せの効果を検証するためにドメインの階層数は 3 とし，各ドメインに VGW，ポリシサーバ，LDAP サーバに加え，LDAP サーバとポリシサーバを特定するための DNS サーバと，認証に使用する Kerberos[12] の鍵配布サーバ（KDC）を配置している．本実験では，すべてのサーバを VGW と同じ計算機で動作させたが，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，実験に利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．

実験は，組織外にある echo クライアントが，組織の最も内側のドメインにある echo サーバに対してコネクションを確立する試行を 100 回行い，コネクション確立に要した時間の平均値を算出した．このとき，従来手法として文献 7) の方式を用い，提案手法については，キャッシュと一括問合せの有無による影響を比較するため，キャッシュデータがすでに存在する場

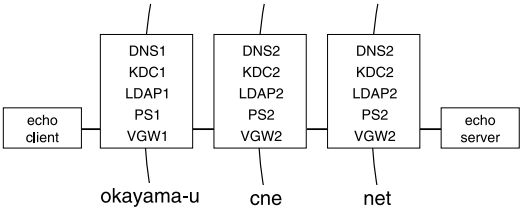

図 4 実験ネットワークの構成
Fig. 4 The structure of the experimental network.

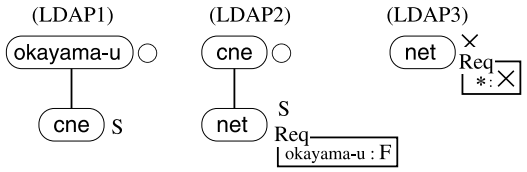

図 5 各 LDAP サーバのデータベース（認証なし）
Fig. 5 Database of each LDAP server (with no authentication).

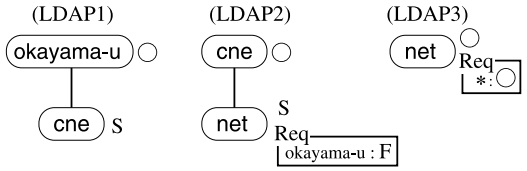

図 6 各 LDAP サーバのデータベース（認証あり）
Fig. 6 Database of each LDAP server (with authentication).

合（方法 1），キャッシュデータがなく一括問合せを行う場合（方法 2），キャッシュデータがなく一括問合せも行わない場合（方法 3）のそれぞれについて試行を実施した．さらに，認証に要する時間と提案手法の導入によるコネクション確立時間の増加分を比較するため，これらの 4 つの方法に対して，すべての VGW で認証を行う場合と行わない場合を組み合わせた（合計 8 通り）．なお，各ドメインのポリシデータベースは，すべての VGW で認証を行わない場合は**図 5**，すべての VGW で認証を行う場合は**図 6** のように設定した．いずれも，アクセスポリシの問合せに最も時間がかかる場合を想定し，すべての上位ドメインからの問合せが，最下位ドメイン（net）まで中継されるように設定している．

4.2 実験結果と考察

実験結果を**表 1** に示す．認証の有無にかかわらず，従来手法と，提案手法において最も時間がかかる方法 3 の差は約 180 ms である．ドメインの階層数は 3 であるため，提案手法は従来手法に比して 1 階層あたり約 60 ms 増加していることになる．組織の規模によっては，ドメインの階層数が 3 を超えることも考えられるが，組織内は比較的高速かつ低遅延のリンクで構成されることが多いことや，認証を行う場合には認証に要する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．

一方，一度 VPN リンクが確立すると，経路上のすべてのポリシサーバにキャッシュができるので，表 1 の方法 1 から分かるように，2 回目以降の VPN リンク確立に要する時間は従来手法に比べて約 20 ms しか増加しない．したがって，組織内の特定のアプリケーションサーバに対して頻繁にアクセスがある場合には，キャッシュが非常に有効であるといえる．

表 1 実験結果
Table 1 Result of the experiment.

	コネクション確立時間（ms）	
	認証なし	認証あり
従来手法	64	1,313
方法 1	84	1,330
方法 2	231	1,479
方法 3	245	1,487

また，方法 2 と方法 3 の比較によって，一括問合せの有効性が確認できる．本実験ではドメインの階層数が 3 であったため，一括問合せによって通信が削減できるのは cne ドメインから net ドメインへの 1 区間分の問合せ（約 10 ms）であるが，問合せおよび応答メッセージの多重化によるオーバヘッドを無視すれば，一括問合せによる削減区間数は階層数 n（$n > 2$）に対して $\sum_{k=1}^{n-2} k$（$= (n-2)(n-1)/2$）であるので，一括問合せの有効性は階層数が増えるにつれて大きくなると予想される．

以上のことから，提案手法による VPN リンク確立時間の増加は実用上問題にならないと考えられる．

5. 考察と今後の課題

最後に，提案手法に対する性能評価以外の考察と，今後の課題を以下にまとめる．

- 他の VPN リンク確立方式への適用可能性
  提案手法は文献 7) の VPN リンク確立方式を前提としているが，アクセスポリシのデータベース（LDAP サーバ）とポリシサーバは VGW から独立して実装しているため，提案手法は他の VPN リンク確立方式[1),2),4),5)] にも比較的容易に適用可能である．
  具体的には，他の VPN リンク確立方式の VGW（に相当するプログラム）を拡張し，提案手法で定義されている VGW–ポリシサーバ間のアクセスポリシ問合せプロトコルを組み込めばよいと考えられる．
- アクセスポリシ決定権の部分的な委譲
  アクセスポリシ決定権の委譲をより柔軟に行うためには，下位ドメインのアクセスポリシ要求を上位ドメインが無条件に受け入れるのではなく，部分的な委譲，すなわち，下位ドメインが選択可能なアクセスポリシ要求の値を上位ドメインが制限できるような機能が必要である．
  部分的な委譲の実現方法としては，上位ドメイン

のデータベースに下位ドメインが選択可能なアクセスポリシの値を列挙できるようにしたうえで，アクセスポリシ要求の問合せ時にデータベースの内容と問合せ結果を照合することが考えられる．他の方法も含め，詳細については今後検討する予定である．

- アクセスポリシの問合せ方法
  提案手法ではアクセスポリシの問合せを組織外のホストが各ドメインの VGW にアクセスする際に行うものとしているが，これ以外の方法として，上位ドメインがアクセスポリシ決定権を委譲している下位ドメインに対して定期的に問合せを行う方法や，下位ドメインが上位ドメインに定期的にアクセスポリシ要求を行う方法，さらに，提案手法とこれらの方法を組み合わせた方法などが考えられる．定期的に問合せを行う利点として，接続先ドメインへの初回アクセスがより高速になることがあげられるが，問合せのためのトラフィックが増加する可能性がある．このため，今後提案手法との詳細な比較を行ったうえで，定期的な問合せ方法への対応を検討する予定である．
- 新規ドメインへの対応
  3.2 節で述べたように，提案手法のデータベースでは，ドメインのサブツリー全体に同一のアクセスポリシを適用する場合，サブツリーのルートドメインに対応するノードのみを設定すればよい．このような状況において，サブツリー内にドメインが新設された場合，上位ドメインでは新規ドメインに対するアクセスポリシを検討する必要があるが，現在の提案手法の枠組みではサブツリー全体のアクセスポリシが新規ドメインにも適用される．これに対し，フェイルセーフの観点から，組織ネットワークの入口となる最上位ドメインのデータベースでは，既存のすべての下位ドメインに対するノードを設定したうえで，未知のドメインに対しては中継を拒否するような運用方法も考えられる．ただし，提案手法の実装では，あるドメインのノードがデータベースから省略されている場合は上位ドメインの設定値が適用されてしまうので，これを抑制するような機能を追加する予定である．

6. おわりに

本論文では，階層型 VPN に対応した既存の VPN リンク確立方式のアクセスポリシ管理方法に注目し，下位ドメインの設定変更に依存しない効率的なアクセスポリシ管理手法を提案した．さらに，既存の VPN リンク確立方式の拡張によって提案手法を実装し，これを用いて性能評価実験を行うことにより，提案手法による VPN リンク確立時間の増加が実用上問題がないことを確認した．

今後は，5 章で述べた課題に加え，VPN リンク確立時の認証に必要となるアカウント情報を異なるドメイン間で効率良く管理するための手法などを検討する予定である．

謝辞 本研究の一部は，総務省戦略的情報通信研究開発推進制度（特定領域重点型研究開発プログラム，課題番号 041108001）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) NEC: SOCKS Home Page. http://www.socks.nec.com/index.html
2) 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).
3) Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: SOCKS Protocol Version 5, RFC1928 (1996).
4) 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.
5) 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).
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) 岡山聖彦，金出地友治，山井成良，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).
8) Wahl, M., Howes, T. and Kille, S.: Lightweight Directory Access Protocol (v3), RFC 2251 (1997).
9) Mockapetris, P.V.: Domain names — concepts and facilities, RFC 1034 (1987).
10) Mockapetris, P.V.: Domain names — implementation and specification, RFC 1035 (1987).
11) Gulbrandsen, A., Vixie, P. and Esibov, L.: A DNS RR for specifying the location of services (DNS SRV), RFC 2782 (2000).

12) Kohl, J. and Neuman, C.: The Kerberos Network Authentication Service (V5), RFC1510 (1993).

(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 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．平成 17 年同大学総合情報基盤センター助手．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，岡山大学総合情報基盤センター助教授．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）．

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．平成元年同大学院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，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（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．