階層型VPNにおける透過的仮想リンク確立手法

河合 洋明[1] 坂根 栄作[2] 豊田 博俊[3] 岡山 聖彦[4] 河野 圭太[4]
宮下 卓也[5] 山井 成良[4] 石橋 勇人[1] 安倍 広多[1] 松浦 敏雄[1]

[1] 大阪市立大学 大学院創造都市研究科
[2] 大阪大学 サイバーメディアセンター
[3] 大阪産業大学 非常勤講師
[4] 岡山大学 総合情報基盤センター
[5] 津山工業高等専門学校

Several Methods for Transparently Establishing Virtual Links on Hierarchical VPN

Hiroaki Kawai[1] Eisaku Sakane[2] Hirotoshi Toyoda[3] Kiyohiko Okayama[4]
Keita Kawano[4] Takuya Miyashita[5] Nariyoshi Yamai[4]
Hayato Ishibashi[1] Kota Abe[1] Toshio Matsuura[1]

[1]Graduate School of Creative Cities, Osaka City University
[2]Cybermedia Center, Osaka University
[3]adjunct professor, Osaka Sangyo University
[4]Information Technology Center, Okayama University
[5]Tsuyama National College of Technology

概要

本論文では，サーバとクライアント間の通信を安全に確立する手段として利用される VPN (Virtual Private Network) が階層的に構成されている場合において，透過的な接続を確立する方法を提案する．ある組織内に存在するサーバに対し，クライアントが組織外から通信する際には，VPN による安全性を確保した手段が必要になる場合がある．さらに，場合によっては特定の部署へのアクセスを組織の内外から制限することがある．この場合，組織によっては異なるセキュリティポリシで管理されるドメインが，階層構造を構成することになる．このような条件下において，その階層構造を意識することなく透過的な接続を確立するために，サーバの FQDN (Fully Qualified Domain Name) を利用して VGW (VPN Gateway) を検索し経路を辿る方法を提案している．本論文ではこれに加えて，サーバへの接続を試みたときに，経路上のルータから返される ICMP ホスト到達不可メッセージを利用することにより VGW を辿る方法，そして，ICMP を利用せずに TCP プロトコルを修正することで VGW を辿る方法を提案し，これら 3 方式の比較，検討を行った．

1　はじめに

近年，自組織ネットワークに安全にアクセスしたいという需要が高まっている．これを実現する方法の 1 つとして，インターネットを介して仮想的に専用線を引く技術，すなわち仮想プライベートネットワーク (Virtual Private Network，以下 VPN とする) が注目されており，活発に研究されている．

VPN の技術によってネットワークの 2 点間に仮想的なリンクが張られ，これにより安全な通信を実現できる．しかしながら，不正アクセスなどから自組織のネットワークを護るためにファイアウォールを導入することなどが一般的となった現在，ネットワークの 2 点間を直接リンクできないことが多くなっている．さらに，組織によっては組織全体を外部から護るだけでなく，組織内の特定の部署のネットワークをその他の部署に対して非公開とせねばならない場合もあり得る．具体例として大学付属病院を考えれば，病院のネットワークを外部から護るのはもちろんのこと，同じ大学内からのアクセスをも制限することが好ましいと考えられる．この場合，学外から付属病院のネットワークにアクセスしようとすると，組織の最外殻にあるファイアウォールを越えるだけでなく，学内からのアクセスを制限するためのファイアウォールも越えなければならない．異なるセキュリティポリシによって形成される階層構造をもつネットワークは，情報管理の観点から必ずしも特殊なものとは言えなくなりつつあるのに対して，そこに仮想リンクを確立するのは容易ではないのが現状である．したがって，上述の階層構造を有するネットワークにおいて，容易に仮想リンクを確立するための手法を考案することは意義深いことである．また，その手法が有用なものとなるには，仮想リンク確立のための一連の手続きはエンドユーザから見れば透過的に実行される必要がある．

2　階層型 VPN における仮想リンク

この節では，まず文献 [2] に従い，階層構造を有するネットワークにおける VPN を次のように定義する．

組織など一様なアクセスポリシをもつ閉じた領域を定義し，これを VPN ドメインと呼ぶことにする．その VPN ドメインと外部との接点に VPN ゲートウェイ (以下，これを VGW とする) が設置されているとし，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が VGW によって遮断されているものとする．また，VPN ドメインはその内部に独自のセキュリティポリシをもった VPN ドメインを許容できるものとする．組織内のある特定の部署のネットワークをその他の部署から護る場合は，例えば VPN ドメインが組織の内部構成と同様に階層的に構成されていると考える (図 1)．

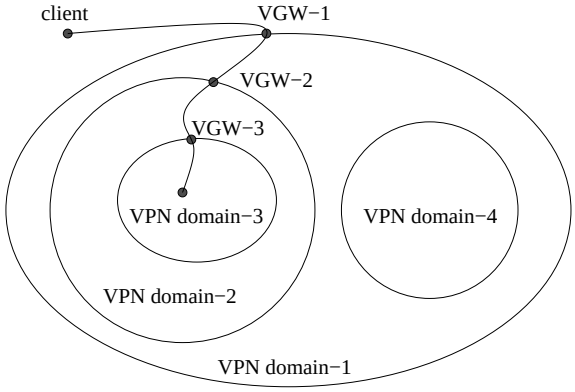

図 1: 階層型 VPN

以下では，このような階層構造における VPN を階層型 VPN と呼ぶことにする．

階層型 VPN において，組織の外部にあるクライアントが組織の最も内部にある VPN ドメインにアクセスするには，クライアントは最も外側にある VGW から目的の VPN ドメインに向かって各 VPN ドメインにおける VGW を 1 つずつ経由して辿らなければならない．したがって，クライアントは目的の VPN ドメインに至るまでの VGW の情報 (ホスト名や IP アドレス，接続に必要な認証方法など) を事前に知っておく必要がある．階層型 VPN の構造が複雑になればなるほど管理する情報も多く複雑になるので，クライアントの利便性は悪くなる一方である[1]．通常のネットワーク接続を考えてみれば，目的の VPN ドメインまでの経路がどのようになるかはエンドユーザにとって必ずしも意識する必要のない情報である．

一般に，目的の VPN ドメインまでの経路は一意的であり，基本的には静的であると考えられる．よって，最外層の VPN ドメインから目的の VPN ドメインまでの経路 (各階層の VGW の辿り方) を動的に繋ぐ機

[1] 複数の組織の階層型 VPN を考慮する場合，経路情報をクライアント側で静的に保持する方法ではそれぞれの経路情報を個別に扱わなければならない．

構を導入することによって，経路情報の取得および仮想リンクの確立を自動化できることが期待できる．さらに，これらの機能をクライアントのユーザインターフェースから隠して組込むことによって一連の手続は透過的となり，クライアントは階層型 VPN かどうかを意識する必要がなくなる．

階層型 VPN において透過的な仮想リンク確立手法を設計する上で，本論文では次のような方針で議論する．

- 既存のアプリケーションにはできるだけ変更を加えない．
- アプリケーションは TCP を利用して通信するものとする．

この方針の下で透過的に仮想リンクを確立するために，次のような手続きを基本として考える．

1. アプリケーションはネットワーク接続を試みる．
2. VPN の確立が必要かどうかを判定し，必要に応じて VPN を確立する．
3. アプリケーションが VPN の下で接続できるようにする．

この基本手続きを設計・実装する方法は一意ではなく，幾つか考えることができる．例えば，各 VGW を繋ぐ情報を予め用意し参照させるディレクトリサービスを構築する方法，あるいは既存のプロトコルスタックを修正し VPN ドメインの存在の有無を知る方法などである．

本論文ではまず第 3 節で DNS に VPN ドメイン情報を付加して参照する方法を議論する．また，プロトコルスタックを修正する方法として第 4 節では ICMP を用いた方法，第 5 節では TCP を用いた方法について議論する．第 6 節では各方法を比較する．最後に，第 7 節で今後の課題を述べる．

3 DNS ドメインを利用した VPN 確立法

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．そのため VPN ドメインの外側から VGW を 1 つずつたどって VPN を確立する必要がある．

インターネット上に存在するホストやネットワークにつけられる識別子である DNS ドメインを使用した階層型 VPN (以下，DNS 法) とは，サーバの Fully Qualified Domain Name(以下，FQDN) を利用して VGW を検索することにより階層型 VPN を構成する方法である [1, 2, 3, 4].

3.1 DNS 法の前提条件

DNS 法を使用するためには，以下の条件を満たす必要がある．

- VPN ドメインと DNS ドメインを 1 対 1 で対応させる．
- VPN ドメインでは，アクセスポリシは一様でなければならない．
- クライアントの利用者は 1 人でなければならない．

3.2 DNS 法の設定

DNS 法を使用するためには，以下のように設定を行っておく必要がある．

- DNS サーバには，VPN ドメインに対する SRV レコードとして VGW のアドレスを設定する．
- 外部からの SRV レコード要求に対して，SRV レコード又は NX Domain を応答できるように設定する．
- クライアント上で DNS の名前解決要求 (以下，DNS クエリ) を横取りする DNS Proxy を動作させる．

3.3 DNS 法の動作

クライアント (以下，C1) から接続したいサーバ (以下，S1) に VPN を確立して TCP で通信する場合の DNS 法の動作は次の通りである．ここでは，図 2 のような VPN ドメインが 2 つあり，各 VPN ドメインと外部との接点に VGW があるように構成を想定している．

1. C1 のプログラム (以下，*Program*) は，DNS を用いて S1 の FQDN から A レコードを引こうとする．

2. DNS Proxy は，*Program* の DNS クエリを横取りする．*Program* が出した DNS クエリに書かれた S1 の FQDN が serv.ex.example.com だとした場合，DNS Proxy は_vpn.ex.example.com の SRV レコードを DNS1 へ要求する．

3. DNS Proxy は，SRV レコードの応答により VGW1 の情報 (アドレス) を得る．そこで，DNS Proxy は S1 の FQDN，ユーザ認証を行うためのユーザ名，パスワード，証明書等の認証情報を VGW1 に渡して VPN 接続要求を行う．

4. DNS Proxy から VPN 接続要求を受けた VGW1 は，DNS Proxy から受け取った S1 の FQDN を利用して 2 で述べたように SRV レコードを要求する．VGW1 は SRV レコードを受信すると VGW2 がわかる．VGW1 は S1 の FQDN と認証情報を VGW2 に渡し C1 からの VPN 接続要求を VGW2 にリレーする．以後 VGW1 は，C1 からの通信を VGW2 にリレーし，VGW2 からの通信を C1 にリレーする．

5. VGW1 から VPN 接続要求を受けた VGW2 は，VGW1 から受け取った S1 の FQDN を利用して 2 で述べたように SRV レコードを要求を行う．VGW2 は NX Domain を受信して，VGW1 から受け取った認証情報を用いてユーザ認証を行う．

   - ユーザ認証に成功した場合，VGW1 から受け取った VPN 接続要求を受けて VPN を確立する．
   - ユーザ認証に失敗した場合，VGW1 を経由して DNS Proxy にユーザ認証に失敗した事を通知する．

   VGW2 は VPN 確立後に S1 の A レコードを要求し，それに対する A レコード応答を受信した後に VGW1 を経由して S1 の IP アドレスを DNS Proxy に送信する．

6. DNS Proxy は S1 の IP アドレスを *Program* に返す．

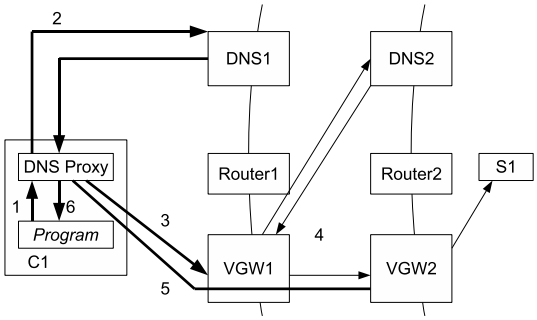

図 2: DNS 法

3.4 DNS 法の留意点

DNS 法を用いる場合，以下に述べるような点に留意する必要がある．

3.4.1 無駄な DNS クエリ

DNS 法では，アプリケーションが *www.example.com* や *www.osaka-cu.ac.jp* 等の DNS クエリを出すと，DNS Proxy は DNS クエリを横取りして SRV レコードを要求を行い，

- SRV レコード応答を受信すると，VPN 接続要求を行う．
- NX Domain を受信すると，VPN を確立しないと判断して A レコードを要求する．

アプリケーションが出した DNS クエリの多くが VPN を確立する必要がない場合でも，DNS Proxy はまず SRV レコードを要求するため無駄が多い．

この無駄を軽減するために，DNS Proxy にネガティブキャッシュ機能を持たせる事が考えられる．DNS Proxy は，SRV レコード要求に対して一度でも NX Domain を受信するかタイムアウトしたドメインをネガティブキャッシュに記録しておく．DNS Proxy はアプリケーションが出した DNS クエリから FQDN を取り出し，これがネガティブキャッシュに記録しているドメインと一致する場合には，A レコードを問い合わせるようにしておく．

3.4.2 DNS クエリの再送

DNS 法では，アプリケーションが *Server* の FQDN から A レコードを引こうとして DNS クエリを出して

から，DNS Proxy が VPN を確立して，サーバの IP アドレスをアプリケーションに返すまでに，アプリケーションは DNS クエリを再送する可能性がある．アプリケーションが DNS クエリを再送した場合，DNS Proxy は，VPN を確立している過程であれば，これを無視する必要がある．

3.4.3 DNS 法の時間の制約

DNS 法では，アプリケーションが *Server* の FQDN から A レコードを引くために DNS クエリを出し，DNS Proxy が横取りして VPN を確立して *Server* の IP アドレスをアプリケーションに返すまでに長時間かかると，アプリケーションが DNS サーバとの通信がタイムアウト[2] していると判断する可能性がある．

アプリケーションがタイムアウトしていると判断することを回避するために，DNS Proxy はアプリケーションが問い合わせた FQDN の A レコードに，使用されていないプライベート IP アドレス (以下，*w.x.y.z*) を返す事が考えられる．DNS Proxy がタイムアウトを回避するために，*w.x.y.z* を返すとアプリケーションは TCP で通信を開始するが，*w.x.y.z* は使用されていないため，TCP のタイムアウト[3] を回避しなければアプリケーションは *w.x.y.z* と通信できないことがわかり，アプリケーションは終了するので TCP のタイムアウトを回避する必要がある．DNS Proxy は，VPN 確立後に目的とする *Server* の IP アドレスを VGW から受け取ると，アプリケーションの通信を横取りしてアプリケーションに返したプライベート IP アドレスと正しい Server の IP アドレスの変換を行う．

TCP のタイムアウトを回避するには，アプリケーションが TCP SYN を送ってからタイムアウトする前に *Server* から TCP SYN と TCP ACK が返ってこない場合に仮の TCP SYN と TCP ACK をアプリケーションに渡すようにする．このときにシーケンス番号を記録しておく．その後文献 [5] のようにウインドウサイズ 0 をアプリケーションに知らせることで TCP の通信を停止させ，Server から TCP SYN+ACK が返ってきた場合に TCP の通信を再開する．TCP の通信を再開した後は Server からの通信を受け取り，記憶しておいたシーケンス番号+α のシーケンス番号に変更する．

3.4.4 VPN の切断契機

DNS 法を利用して，VPN を確立した場合，確立した VPN をいつ切断するのかという問題がある．DNS 法では，VPN が必要かどうかの判定に FQDN を用いる．このため，一度 VPN が確立してアプリケーションに *Server* の IP アドレスが渡った後に，VPN を切断すると，新たにアプリケーションが *Server* と通信しようとしたときは，*Server* の IP アドレスがわかっているため DNS クエリを出さない．このため VPN を確立しないのでアプリケーションは *Server* と通信できなくなる．

3.4.5 IP アドレスの重複

クライアント側と VPN サーバ側でプライベート IP アドレスを使用している場合，IP アドレスが重複する可能性がある．現時点では解決方法は見つかっていない．

4 ICMP を使用した VPN 確立法

インターネットでは，組織外にあるクライアントが直接通信できないサーバと通信しようとすると，経路上のルータから ICMP ホスト到達不可メッセージが返ってくることが期待できる．この ICMP メッセージを利用して，階層型 VPN を構成する方法を提案する (以下，ICMP 法)．

4.1 ICMP 法の実現方法

ICMP 法を実現するには，以下の三つの方法が考えられる．

ICMP 法 1: DNS Proxy はアプリケーションが接続したい *Server* の FQDN を用いて A レコードを要求するときに出す DNS クエリを横取りする．DNS Proxy は，*Server* の A レコードを要求してそれに対する A レコード応答を受け取ると，*Server* に ICMP エコー要求を送信する．DNS Proxy は

[2] DNS のタイムアウトは BIND4.9 から 8.2 までのリゾルバでは，約 75 秒，BIND8.2.1 以降のリゾルバでは約 15 秒である [6].
[3] TCP のタイムアウトは FreeBSD で約 75 秒である [7].

Server への経路上のルータから ICMP ホスト到達不可メッセージを受信すると，VGW を検索して認証情報と VPN 接続要求を VGW に送信する．

ICMP 法 2: アプリケーションが接続したい *Server* と通信を試みた時に，*Server* との経路上のルータから ICMP ホスト到達不可メッセージを受信すると，VGW を検索して認証情報と VPN 接続要求を VGW に送信する．

ICMP 法 3: アプリケーションが *Server* と通信を試みた時に，*Server* との経路上のルータから VGW のアドレスが付加された ICMP ホスト到達不可メッセージを受信すると認証情報と VPN 接続要求を VGW に送信する．

4.2 ICMP 法 1

ICMP 法 1 について考察を述べる．

4.2.1 ICMP 法 1 の前提条件

ICMP 法 1 を使用するためには，以下の条件を満たす必要がある．

- クライアントとサーバの間には，ICMP をフィルタリングする経路を含まない．
- クライアントの利用者は 1 人でなければならない．

4.2.2 ICMP 法 1 の設定

ICMP 法 1 を使用するためには，以下の設定を行っておく必要がある．

- ルータの IP アドレスを *a.b.c.d* とした場合，DNS サーバに VGW のアドレスを *d.c.b.a*.in-addr.arpa の TXT レコードとして設定する．
- クライアント上で DNS の名前解決要求 (以下，DNS クエリ) を横取りする DNS Proxy を動作させる．

4.2.3 ICMP 法 1 の動作

クライアント (以下，C1) から接続したいサーバ (以下，S1) に VPN を確立して TCP で通信する場合の ICMP 法 1 の動作は次の通りである．ここでは，図 3 のように VPN ドメインが 2 つあり，各 VPN ドメインと外部との接点に VGW があるような構成を想定している．

1. C1 のプログラム (以下，*Program*) は DNS を用いて S1 の FQDN から A レコードを引こうとする．
2. DNS Proxy は *Program* が出した DNS クエリを横取りする．*Program* が出した DNS クエリに書かれた S1 の FQDN の A レコードを DNS1 に要求する．
3. DNS1 は DNS Proxy から問い合わせられた FQDN の A レコードを返す．
4. DNS Proxy は A レコードの応答を受け取ると，S1 対して ICMP エコー要求を送信する．
5. ICMP エコー要求を送信したときに，S1 までの経路上の *Router1* から ICMP ホスト到達不可メッセージを受信する．DNS Proxy は受信した ICMP ホスト到達不可メッセージのソース IP アドレス (*a.b.c.d*) から VGW1 を検索する．VGW1 の検索は，*d.c.b.a*.in-addr.arpa. の TXT レコードを引くことで行う．ICMP エコー応答が返ってきた場合，S1 と直接通信できるので，9 を行う．
6. DNS Proxy は TXT レコードの応答を受信すると VGW1 の情報 (アドレス) を得る．DNS Proxy は VGW1 へ S1 の FQDN と認証情報を VGW1 に渡し，VGW1 に対して VPN 接続要求を行う．
7. VGW1 は DNS Proxy から受け取った S1 の FQDN の A レコードを DNS2 に要求する．VGW1 は DNS2 から A レコードの応答を受信し，その A レコードに書かれた IP アドレスに対して ICMP エコー要求を送ると，S1 までの経路上の *Router2* から ICMP ホスト到達不可メッセージを受信する．5 と同様に VGW2 を検索し，TXT レコードの応答を受信する．VGW1 は S1 の FQDN と認証情報と DNS Proxy からの VPN 接続要求を VGW2 にリレーする．

8. VGW1 から VPN 接続要求を受けた VGW2 は，VGW1 から受け取った S1 の FQDN の A レコードを DNS2 に要求する．A レコードの応答に書かれた IP アドレスに対して ICMP エコー要求を送ると ICMP エコー応答を受信する．ICMP エコー応答を受信した VGW2 は，VGW1 から受け取った認証情報を用いてユーザ認証を行う．

   - ユーザ認証に成功した場合，VGW1 から受け取った VPN 接続要求を受けて VPN を確立する．
   - ユーザ認証に失敗した場合，VGW1 を経由して DNS Proxy にユーザ認証に失敗した事を通知する．

   VGW2 は VPN 確立後に VGW1 を経由して S1 の IP アドレスを DNS Proxy に送信する．

9. DNS Proxy は S1 の IP アドレスを *Program* に返す．

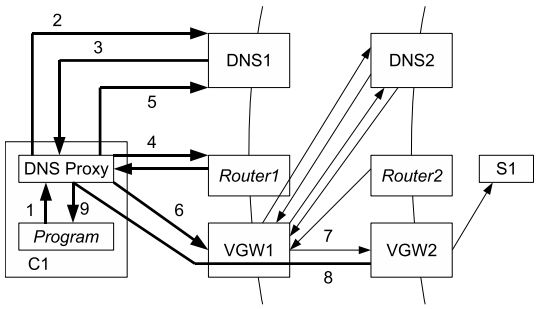

図 3: ICMP 法 1

4.2.4 ICMP 法 1 の留意点

ICMP 法 1 を用いる場合，以下に述べるような点に留意する必要がある．

4.2.4.1 A レコードが引けない場合の対処法

Client から *Server* の A レコードが引けない，又は，*Server* にプライベート IP アドレスが割り当てられている場合，ICMP エコー要求を送信できない．

この状況を回避するには，DNS サーバが外部からの問い合わせに対して，組織に割り当てられているグローバル IP アドレスの中から，外部から直接通信できない IP アドレス (以下，ダミーアドレス) を返すようにする必要がある．

DNS サーバが外部からの問い合わせに対してダミーアドレスを返すようにすると，*Client* 上の DNS Proxy はダミーアドレスに ICMP エコー要求を送信する．*Client* からダミーアドレスに ICMP エコー要求を送信すると，*Client* からダミーアドレスまでの経路上のルータから，ICMP ホスト到達不可メッセージが返ってくる．ICMP ホスト到達不可メッセージを受け取った DNS Proxy は ICMP ホスト到達不可メッセージのソース IP アドレスから，VGW を検索する．DNS Proxy は *Server* の FQDN を VGW に渡して VGW に VPN 接続要求を出す．DNS Proxy から *Server* の FQDN を受け取った VGW は，*Server* の FQDN から A レコードを引く．VGW は得られた A レコードに書かれている IP アドレスに対して ICMP エコー要求を送信し，ICMP エコー応答を受け取る．そして，DNS Proxy からの VPN 接続要求に対して応答し，*Client* と VPN を確立する．その後アプリケーションへ正しい *Server* の A レコードを返す．

4.2.4.2 DNS クエリの再送

3.4.2 と同じ問題が存在する．

4.2.4.3 ICMP 法 1 の時間の制約

3.4.3 と同じ問題が存在する．

4.2.4.4 VPN の切断契機

3.4.4 と同じ問題が存在する．

4.2.4.5 IP アドレスの重複

3.4.5 と同じ問題が存在する．

4.2.4.6 認証問題

あるユーザ A が VGW2 だけで認証できるとする．この場合に ICMP 法 1 で VPN を確立するためには，VGW2 を見つける必要がある．*Client* は *Server* に対し

て ICMP エコー要求を送信すると，*Router1* が ICMP ホスト到達不可メッセージを返す．*Client* は ICMP ホスト到達不可メッセージの送信元 IP アドレスから VGW1 を検索して，VGW1 へ VPN 確立に必要な情報を渡す．VGW1 は *Server* に ICMP エコー要求を送信するが，VGW1 から *Server* に直接通信できる場合，VGW1 へは *Server* から ICMP エコー応答が返ってくるので，VGW1 は次の VGW がないと判断して VPN を確立しようとユーザ認証を行う．しかし，ユーザ A は VGW1 では認証できないので VPN を確立できない．

この問題を解決するには，あらかじめ特殊なパケットをルータで拒否するように設定しておく必要がある．特殊なパケットとは，IP ヘッダのプロトコル番号に使われていないプロトコル番号を使用したパケットである．VGW は認証に失敗した場合に特殊なパケットを *Server* に送信するようにしておくと，ルータは特殊なパケットが届いた場合に ICMP ホスト到達不可メッセージを送信すれば次の階層の VGW を検索できる．

4.3 ICMP 法 2

ICMP 法 2 について考察を述べる．

4.3.1 ICMP 法 2 の前提条件

ICMP 法 2 を使用するためには，以下の条件を満たす必要がある．

- クライアントとサーバの間には，ICMP をフィルタリングする経路を含まない．
- クライアントの利用者は 1 人でなければならない．
- サーバはグローバル IP アドレスを持たなければならない．

4.3.2 ICMP 法 2 の設定

ICMP 法 2 を使用するためには，以下の設定を行っておく必要がある．

- ルータの IP アドレスを *a.b.c.d* とした場合，DNS サーバに VGW のアドレスを *d.c.b.a.*in-addr.arpa の TXT レコードとして設定する．
- クライアント上に，クライアントの通信を監視して VPN が必要ならば VPN を確立するプログラム (以下，*VPN Agent*) を動作させる．

4.3.3 ICMP 法 2 の動作

クライアント (以下，C1) から接続したいサーバ (以下，S1) に VPN を確立して TCP で通信する場合の ICMP 法 2 の動作は次の通りである．ここでは，図 4 のように VPN ドメインが 2 つあり，各 VPN ドメインと外部との接点に VGW があるような構成を想定している．

1. C1 のプログラム (以下，*Program*) は S1 と通信しようとする．
2. *Program* が通信を試みた時に，C1 は S1 までの経路上の *Router1* から ICMP ホスト到達不可メッセージを受信する．*VPN Agent* は C1 が ICMP ホスト到達不可メッセージを受信したことを見つけると，ICMP ホスト到達不可メッセージのソース IP アドレス (*a.b.c.d*) から VGW1 を検索する．VGW1 の検索は，*d.c.b.a.*in-addr.arpa の TXT レコードを引くことで行う．
3. *VPN Agent* は TXT レコードの応答を受信すると VGW1 の情報 (アドレス) を得る．*VPN Agent* は VGW1 へ S1 の IP アドレスと認証情報を VGW1 に渡し，VGW1 に対して VPN 接続要求を行う．
4. VGW1 は *VPN Agent* から受け取った S1 の IP アドレスに対して ICMP エコー要求を送信すると，S1 までの経路上の *Router2* から ICMP ホスト到達不可メッセージを受信する．2 と同様に VGW2 を検索し，TXT レコードの応答を受信する．VGW1 は S1 の IP アドレス，認証情報および DNS Proxy からの VPN 接続要求を VGW2 にリレーする．
5. VGW1 から VPN 接続要求を受けた VGW2 は，VGW1 から受け取った S1 の IP アドレスに対して ICMP エコー要求を送信すると S1 からの ICMP エコー応答を受信する．ICMP エコー応答を受信した VGW2 は，VGW1 から受け取った認証情報を用いてユーザ認証を行う．

- ユーザ認証に成功した場合，VGW1 から受け取った VPN 接続要求を受けて VPN を確立する．
- ユーザ認証に失敗した場合，VGW1 を経由して *VPN Agent* にユーザ認証に失敗した事を通知する．

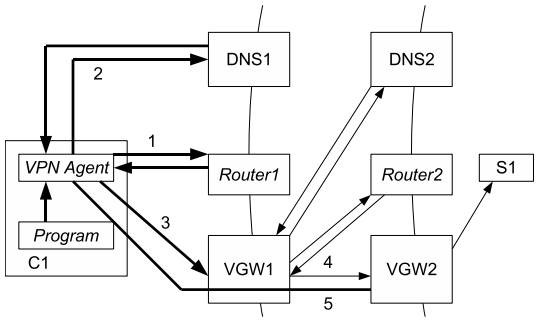

図 4: ICMP 法 2

4.3.4 アドレス変換

ICMP 法 2 では，VPN 確立後にクライアントから送信するパケットの送信元 IP アドレスをクライアントに割り当てられた VPN 用の IP アドレスに変換し，サーバから送られたパケットの宛先 IP アドレスを 4.3.3 の 1 で送信したパケットの送信元 IP アドレスに変換する必要がある．

4.3.5 ICMP 法 2 の留意点

ICMP 法 2 を用いる場合，以下に述べるような点に留意する必要がある．

4.3.5.1 ICMP 法 2 の時間の制約

ICMP 法 2 では，アプリケーションが通信を開始して，組織のルータから ICMP ホスト到達不可メッセージを受け取ると，VPN を確立しようとするが，VPN 確立前にアプリケーションの通信がタイムアウトする可能性がある．

TCP のタイムアウトを回避するには，3.4.3 で述べた方法を行うことが考えられる．

4.3.5.2 認証問題

4.2.4.6 と同じ問題が存在する．

4.4 ICMP 法 3

ICMP 法 3 について考察を述べる．

4.4.1 ICMP 法 3 の前提条件

ICMP 法 3 を使用するためには，以下の条件を満たす必要がある．

- クライアントとサーバの間には，ICMP をフィルタリングする経路を含まない．
- クライアントの利用者は 1 人でなければならない．
- ルータは VGW の情報 (アドレス) を知らせる機能を持たなければならない．
- サーバはグローバル IP アドレスを持たなければならない．

4.4.2 ICMP 法 3 の設定

ICMP 法 3 を使用するためには，以下の設定を行っておく必要がある．

- ルータは VPN 接続が必要なホストに対して外部からの通信を見つけると VGW の情報を送信するように設定する．
- クライアント上に，クライアントの通信を監視して VPN が必要ならば VPN を確立するプログラム (以下，*VPN Agent*) を動作させる．

4.4.3 ICMP 法 3 の動作

クライアント (以下，C1) から接続したいサーバ (以下，S1) に VPN を確立して TCP で通信する場合の ICMP 法 3 の動作は次の通りである．ここでは，図 5 のような VPN ドメインが 2 つあり，各 VPN ドメインと外部との接点に VGW があるように構成を想定している．

1. C1 のプログラム (以下，*Program*) は S1 と通信しようとする．

2. *Router1* は，C1 から S1 への通信を見つけると，VGW1 の情報を付加した ICMP ホスト到達不可メッセージを C1 へ送信する．

3. C1 は VGW1 の情報が付加された ICMP ホスト到達不可メッセージを受信する．*VPN Agent* は C1 が ICMP ホスト到達不可メッセージを受信したことを見つけると，VGW1 の情報アドレスを得る．*VPN Agent* は S1 の IP アドレスと認証情報を VGW1 に渡し，VGW1 に対して VPN 接続要求を行う．

4. VGW1 は *VPN Agent* から受け取った S1 の IP アドレスに対して ICMP エコー要求を送信すると，S1 までの経路上の *Router2* から VGW2 の情報が付加された ICMP ホスト到達不可メッセージを受信する．VGW1 は S1 の IP アドレスと認証情報と *VPN Agent* からの VPN 接続要求を VGW2 にリレーする．

5. VGW1 から VPN 接続要求を受けた VGW2 は，VGW1 から受け取った S1 の IP アドレスに対して ICMP エコー要求を送信すると S1 からの ICMP エコー応答を受信する．ICMP エコー応答を受信した VGW2 は，VGW1 から受け取った認証情報を用いてユーザ認証を行う．そして，

   - ユーザ認証に成功した場合，VGW1 から受け取った VPN 接続要求を受けて VPN を確立する．
   - ユーザ認証に失敗した場合，VGW1 を経由して *VPN Agent* にユーザ認証に失敗した事を通知する．

4.4.4 アドレス変換

ICMP 法 3 では，4.3.4 と同様に VPN 確立後にクライアントから送信するパケットの送信元 IP アドレスをクライアントに割り当てられた VPN 用の IP アドレスに変換し，サーバから送られたパケットの宛先 IP アドレスを 4.4.3 の 1 で送信したパケットの送信元 IP アドレスに変換する必要がある．

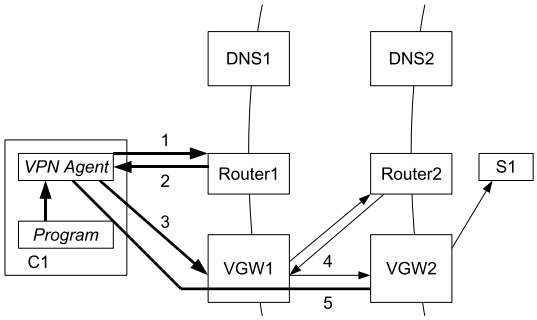

図 5: ICMP 法 3

4.4.5 ICMP 法 3 の留意点

ICMP 法 3 を用いる場合，以下に述べるような点に留意する必要がある．

4.4.5.1 ICMP 法 3 の時間の制約

4.3.5.1 と同じ問題がある．

4.4.5.2 一般のクライアントが影響を受ける可能性がある

ICMP 法 3 では，ICMP ホスト到達不可メッセージに VGW のアドレスを付加するため，VPN に関係のないクライアントが何らかの影響を受ける可能性がある．

4.4.5.3 認証問題

4.2.4.6 と同じ問題が存在する．

5 TCP プロトコルを修正した VPN 確立法

ICMP 法は，*Server* への経路上で ICMP パケットがフィルタリングされている場合には使用できない．ここでは，そのような場合であっても TCP プロトコルを修正することによって階層型 VPN を構成する方法について述べる (以下，TCP 法)．

TCP 法では，VPN 接続が必要なホストに対して，外部から SYN パケットが送信されると，ルータが FIN

パケットで応答する[4]．クライアントはFINパケットを契機にVPNを確立する．

5.1 TCP法の前提条件

TCP法を使用するためには，以下の条件を満たす必要がある．

- クライアントの利用者は1人でなければならない．
- ルータはVGWの情報(アドレス)を知らせる機能を持たなければならない．
- サーバはグローバルIPアドレスを持たなければならない．

5.2 TCP法の設定

TCP法を使用するためには，以下の設定を行っておく必要がある．

- ルータはVPN接続が必要なホストに対して外部からのTCP確立要求を見つけるとVGWの情報を送信するように設定する．
- クライアント上に，クライアントの通信を監視してVPNが必要ならばVPNを確立するプログラム(以下，*VPN Agent*)を動作させる．
- VGWは複数のIPアドレスをアドレスプールとしてVPN用に確保しておく．

5.3 TCP法の動作

クライアント(以下，C1)上から接続したいサーバ(以下，S1)にVPNを確立してTCPで通信する場合のTCP法の動作は次の通りである．ここでは，図6のようなVPNドメインが2つあり，各VPNドメインと外部との接点にVGWがあるように構成を想定している．

1. C1のプログラム(以下，*Program*)はS1とTCPコネクションを試みる．C1のOSは，SYNフラグを立てたTCPパケットをS1に送信する．
2. S1への経路上の*Router1*はSYNフラグが立っているTCPパケットを検出すると，FINフラグを立てたTCPパケットのデータ部分にVGW1のアドレスを付けた上で，S1のIPアドレスをソースIPアドレスにして返信する．
3. C1のOSはSYNフラグを立てて送信したTCPパケットに対して，コネクションを確立する前のタイミングでFINフラグが立っているTCPパケットを受信するとVGW1の情報を得る．C1は最初に送信したTCPパケットの送信元IPアドレス(以下，*C1.IP*)とポート番号(以下，*C1.Port*)，宛先IPアドレス(以下，*S1.IP*)とポート番号(以下，*S1.Port*)，シーケンス番号(以下，*Seq*)と認証情報をVGW1に渡し，VPN接続要求を行う．
4. VGW1は*VPN Agent*からVPN接続要求を受けると*C1.IP*，*C1.Port*，*S1.IP*，*S1.Port*，*Seq*を記録しておく．さらに，VGW1はSYNフラグを立てたTCPパケットをS1に送信する．この際のTCPパケットの詳細は以下のとおりである．
   - 送信元IPアドレスはVGW1が確保しているIPアドレス(IP_1)に変換する．なぜなら，複数ユーザがS1と通信を試みたときに送信元IPアドレスをユーザ毎にVGW1が確保しているIPアドレスの中の一つを割り当てなければS1側でユーザの識別が出来なくなる．このため送信元IPアドレスをIP_1に変換する必要がある．
   - 送信元ポート番号は，*VPN Agent*から受け取った*C1.Port*にする．
   - 宛先IPアドレスは，*VPN Agent*から受け取った*S1.IP*にする．
   - 宛先ポート番号は，*VPN Agent*から受け取った*S1.Port*にする．
   - シーケンス番号は，*VPN Agent*から受け取った*Seq*にする．
5. *Router2*はSYNフラグが立っているTCPパケットを検出すると，FINフラグを立てたTCPパケットを送信元(VGW1)に返す．VGW1は*Router2*からFINフラグの立っているTCPパケットを受信するとVGW2の情報を得る．VGW1

[4]標準のTCPプロトコルでは，SYNに対してFINは返さない．

は C1 に割り当てた IP_1 を回収する．VGW1 は VGW2 の情報を得て，*VPN Agent* から受け取った *C1.IP*，*C1.Port*，*S1.IP*，*S1.Port*，*Seq*，認証情報を VGW2 に渡し VPN 接続要求を行う．

6. VGW2 は VGW1 から *C1.IP*，*C1.Port*，*S1.IP*，*S1.Port*，*Seq* を受け取り記録しておく．

   - 送信元 IP アドレスは VGW2 が確保している IP アドレス (IP_b) に変換する．さらに，VGW2 は SYN フラグを立てた TCP パケットを S1 に送信する．この際の TCP パケットの詳細は以下のとおりである．
   - 送信元ポート番号は，VGW1 から受け取った *C1.Port* にする．
   - 宛先 IP アドレスは，VGW1 から受け取った *S1.IP* にする．
   - 宛先ポート番号は，VGW1 から受け取った *S1.Port* にする．
   - シーケンス番号は，VGW1 から受け取った *Seq* にする．

   VGW2 は S1 から SYN フラグと ACK フラグが立った TCP パケットを受信する．SYN フラグと ACK フラグの立った TCP パケットを受信した VGW2 は，VGW1 から受け取った認証情報を用いてユーザ認証を行う．そして，

   - ユーザ認証に成功した場合，VGW1 から受け取った VPN 接続要求を受けて VPN を確立する．
   - ユーザ認証に失敗した場合，VGW1 を経由して *VPN Agent* にユーザ認証に失敗した事を通知する．

7. VGW2 は S1 から受け取った SYN フラグ，ACK フラグの立った TCP パケットの宛先 IP アドレス (IP_b) を VGW1 から受け取った *C1.IP* に変更して VGW1 を経由して *VPN Agent* に返す．*VPN Agent* は VGW2 から SYN フラグ，ACK フラグの立った TCP パケットを *Program* に渡す．

8. *Program* は S1 からの SYN フラグ，ACK フラグの立った TCP パケットを受信すると ACK フラグを立てた TCP パケットを S1 に送信する．

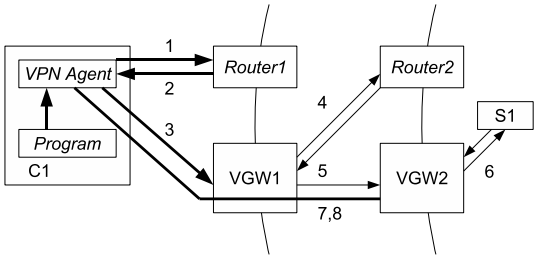

図 6: TCP 法

5.4 アドレス変換

TCP 法では，VGW を辿るときと，VPN 確立後に IP アドレスの変換が必要である．

- VGW を辿るときの IP アドレスの変換: VPN 接続要求を受けた VGW が VPN 用に確保していたアドレスプールの中から IP アドレス (IP_a) を VPN 接続要求を行ったクライアント用に予約する．クライアントから VPN 接続要求を受けた VGW は，5.3 の 4 と同様に送信元 IP アドレスを IP_a に設定して TCP SYN をサーバに送信する．
  - サーバまでの経路上のルータから TCP SYN に対して TCP FIN が返ってきた場合，IP_a をクライアントには割り当てずにアドレスプールにもどす．
  - サーバから TCP SYN に対して TCP ACK が返ってきた場合，クライアントと VPN を確立して IP_a をクライアントに割り当てる．
- VPN 確立後の IP アドレスの変換: 4.3.4 と同様にクライアントから送信するパケットの送信元 IP アドレスをクライアントに割り当てられた VPN 用の IP アドレスに変換し，サーバから送られたパケットの宛先 IP アドレスを 5.3 の 1 で送られたパケットの送信元 IP アドレスに変換する必要がある．

5.5 TCP 法の留意点

TCP 法を用いる場合，以下に述べるような点に留意する必要がある．

5.5.1 TCP 法の時間の制約

4.3.5.1 と同じ問題が存在する.

5.5.2 一般のクライアントが影響を受ける可能性がある

TCP 法では，SYN に対して FIN を返すため，この VPN 接続に関係のない一般のクライアントが何らかの影響を受ける可能性がある.

5.5.3 認証問題

4.2.4.6 と同じ問題が存在する.

6 各方法の比較

ここでは，前述の階層型 VPN の構築方法についての検討を行う．本章では，VPN 接続を確立するのに要する時間，VPN 接続を確立するために必要な条件の二点について比較を行う.

6.1 コネクション確立時のオーバーヘッド

各方法において，クライアント (以下，C1) のアプリケーション (以下，*Program*) が *Server*(以下，S1) の FQDN を用いて VPN を確立して，*Server* と TCP コネクションを確立するまでの時間を比較する.

所要時間を比較するために以下のように定義して評価を行う.

- C1 から階層型 VPN を導入している組織までの通信時間を t_a とする.
- 組織内の通信にかかる時間を t_b とする.
- VPN 確立にかかる時間を t_c とする.
- 通過する VGW の数を n とする.

6.1.1 DNS 法

DNS 法の動作を，定義した行程毎に分解して所要時間の見積もりを行う.

1. C1 は組織の DNS サーバに SRV レコードを要求する (t_a).
2. C1 は組織の DNS サーバから SRV レコードの応答を受信する (t_a).
3. C1 は VGWi(ここでは $i = 1$ となる) に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_a).
4. VGWi は組織の DNS サーバに SRV レコードを要求する (t_b).
5. VGWi は組織の DNS サーバから SRV レコードの応答を受信する (t_b).
6. VGWi は VGW$(i+1)$ に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_b).
7. 4〜6 を $(n-1)$ 回繰り返す.
8. VGWn は組織の DNS サーバに SRV レコードを要求する (t_b).
9. VGWn は組織の DNS サーバから NX Domain を受信する (t_b).
10. VGWn は組織の DNS サーバに A レコードを要求する (t_b).
11. VGWn は組織の DNS サーバから A レコードの応答を受信する (t_b).
12. VGWn は C1 と VPN を確立する (t_c).
13. VGWn は C1 に S1 の A レコードを渡す $(t_a + t_b n - 1))$.
14. C1 は S1 と TCP コネクションを確立する $(3(t_a + t_b n))$.

DNS 法にかかる時間は，$(4t_b)n+4t_a+t_c+3(t_a+t_b n)$ となる.

6.1.2 ICMP 法 1

ICMP 法 1 の動作を，定義した行程毎に分解して所要時間の見積もりを行う．

1. C1 は組織の DNS サーバに A レコードを要求する (t_a).
2. C1 は組織の DNS サーバから A レコードの応答を受信する (t_a).
3. C1 は S1 に ICMP エコー要求を送信する (t_a).
4. C1 は S1 への経路上のルータから ICMP ホスト到達不可メッセージを受信する (t_a).
5. C1 は受信した ICMP ホスト到達不可メッセージのソース IP アドレスから VGW を検索するために組織の DNS サーバに TXT レコードを要求する (t_a).
6. C1 は組織の DNS サーバから TXT レコードの応答を受信する (t_a).
7. C1 は VGWi(ここでは，$i = 1$ となる) に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_a).
8. VGWi は組織の DNS サーバに A レコードを要求する (t_b).
9. VGWi は組織の DNS サーバから A レコードの応答を受信する (t_b).
10. VGWi は S1 に ICMP エコー要求を送信する (t_b).
11. VGWi は S1 への経路上のルータから ICMP ホスト到達不可メッセージを受信する (t_b).
12. VGWi は受信した ICMP ホスト到達不可メッセージのソース IP アドレスから VGW$(i+1)$ を検索するために組織の DNS サーバに TXT レコードを要求する (t_b).
13. VGWi は組織の DNS サーバから TXT レコードの応答を受信する (t_b).
14. VGWi は VGW$(i+1)$ に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_b).
15. 8〜14 を $(n-1)$ 回繰り返す.
16. VGWn は組織の DNS サーバに A レコードを要求する (t_b).
17. VGWn は組織の DNS サーバから A レコードの応答を受信する (t_b).
18. VGWn は S1 に ICMP エコー要求を送信する (t_b).
19. VGWn は S1 から ICMP エコー応答を受け取る (t_b).
20. VGWn は C1 と VPN を確立する (t_c).
21. VGWn は C1 に S1 の A レコードを渡す $(t_a + t_b(n-1))$.
22. C1 は S1 と TCP コネクションを確立する $(3(t_a + t_b n))$.

ICMP 法 1 にかかる時間は，$(3t_b)n + 8t_a - 4t_b + t_c + 3(t_a + t_b n)$ となる．

6.1.3 ICMP 法 2

ICMP 法 2 の動作を，定義した行程毎に分解して所要時間の見積もりを行う．

1. C1 は組織の DNS サーバに A レコードを要求する (t_a).
2. C1 は組織の DNS サーバから A レコードの応答を受信する (t_a).
3. C1 は S1 に TCP SYN を送信する (t_a).
4. C1 は S1 への経路上のルータから ICMP ホスト到達不可メッセージを受信する (t_a).
5. C1 は受信した ICMP ホスト到達不可メッセージのソース IP アドレスから VGW を検索するために組織の DNS サーバに TXT レコードを要求する (t_a).
6. C1 は組織の DNS サーバから TXT レコードの応答を受信する (t_a).
7. C1 は VGWi(ここでは，$i = 1$ となる) に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_a).

8. VGWi は S1 に ICMP エコー要求を送信する (t_b).
9. VGWi は S1 への経路上のルータから ICMP ホスト到達不可メッセージを受信する (t_b).
10. VGWi は受信した ICMP ホスト到達不可メッセージのソース IP アドレスから VGW($i+1$) を検索するために組織の DNS サーバに TXT レコードを要求する (t_b).
11. VGWi は組織の DNS サーバから TXT レコードの応答を受信する (t_b).
12. VGWi は VGW($i+1$) に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_b).
13. 8〜12 を ($n-1$) 回繰り返す.
14. VGWn は S1 に ICMP エコー要求を送信する (t_b).
15. VGWn は S1 から ICMP エコー応答を受け取る (t_b).
16. VGWn は C1 と VPN を確立する (t_c).
17. C1 は S1 と TCP コネクションを確立する ($3(t_a + t_b n)$).

ICMP 法 2 にかかる時間は，$(5t_b)n + 7t_a - 3t_b + t_c + 3(t_a + t_b n)$ となる.

6.1.4 ICMP 法 3

ICMP 法 3 の動作を，定義した行程毎に分解して所要時間の見積もりを行う.

1. C1 は組織の DNS サーバに A レコードを要求する (t_a).
2. C1 は組織の DNS サーバから A レコードの応答を受信する (t_a).
3. C1 は S1 に TCP SYN を送信する (t_a).
4. C1 は S1 への経路上のルータから VGWi(ここでは，$i = 1$ となる) の情報 (アドレス) が付加された ICMP ホスト到達不可メッセージを受信する (t_a).
5. C1 は VGWi に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_a).
6. VGWi は S1 に ICMP エコー要求を送信する (t_b).
7. VGWi は S1 への経路上のルータから VGW($i+1$) の情報 (アドレス) が付加された ICMP ホスト到達不可メッセージを受信する (t_b).
8. VGWi は VGW($i+1$) に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_b).
9. 6〜8 を ($n-1$) 回繰り返す.
10. VGWn は S1 に ICMP エコー要求を送信する (t_b).
11. VGWn は S1 から ICMP エコー応答を受け取る (t_b).
12. VGWn は C1 と VPN を確立する (t_c).
13. C1 は S1 と TCP コネクションを確立する ($3(t_a + t_b n)$).

ICMP 法 3 にかかる時間は，$(3t_b)n + 5t_a - t_b + t_c + 3(t_a + t_b n)$ となる.

6.1.5 TCP 法

TCP 法の動作を，定義した行程毎に分解して所要時間の見積もりを行う.

1. C1 は組織の DNS サーバに A レコードを要求する (t_a).
2. C1 は組織の DNS サーバから A レコードの応答を受信する (t_a).
3. C1 は S1 に TCP SYN を送信する (t_a).
4. C1 は S1 への経路上のルータから VGWi(ここでは，$i = 1$ となる) の情報 (アドレス) が付加された TCP FIN を受信する (t_a).
5. C1 は VGWi に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_a).
6. VGWi は S1 に TCP SYN を送信する (t_b).
7. VGWi は S1 への経路上のルータから VGW($i+1$) の情報 (アドレス) が付加された TCP FIN を受信する (t_b).

表 1: コネクション確立時のオーバーヘッド

	VPN 確立時間とオーバーヘッド	TCP 確立時間
DNS 法	$(4t_b)n + 4t_a + t_c$	$3(t_a + t_b n)$
ICMP 法 1	$(8t_b)n + 8t_a - 4t_b + t_c$	$3(t_a + t_b n)$
ICMP 法 2	$(5t_b)n + 7t_a - 3t_b + t_c$	$3(t_a + t_b n)$
ICMP 法 3	$(3t_b)n + 5t_a - t_b + t_c$	$3(t_a + t_b n)$
TCP 法	$(2t_b)n + 4t_a + t_c$	$3(t_a + t_b n)$

8. VGWi は VGW$(i+1)$ に VPN 確立に必要な情報を渡し，VPN 接続要求を行う (t_b).
9. 6〜8 を $(n-1)$ 回繰り返す.
10. VGWn は S1 に TCP SYN を送信する (t_b).
11. VGWn は S1 から TCP SYN,ACK を受け取る (t_b).
12. VGWn は C1 と VPN を確立する (t_c).
13. VGWn は VPN 確立後に S1 から受信した TCP SYN,ACK を C1 に送信する $(t_a + t_b(n-1))$.
14. C1 は S1 に TCP ACK を送信する $(t_a + t_b n)$.

TCP 法にかかる時間は，$(2t_b)n+4t_a+t_c+3(t_a+t_b n)$ となる.

上述した各方法による所要時間をまとめたものが表 1 である.

6.2 導入に際しての前提条件

本章では，各方法を導入するための前提条件を比較する.

条件 1 VPN ドメインと DNS ドメインを 1 対 1 で対応させる.

条件 2 VPN ドメインでは，アクセスポリシは一様でなければならない.

条件 3 クライアントの利用者は 1 人でなければならない.

条件 4 クライアントとサーバの間には，ICMP をフィルタリングする経路を含まない.

条件 5 サーバはグローバル IP アドレスを持たなければならない.

条件 6 ルータは VGW の情報 (アドレス) を知らせる機能を持たなければならない.

本論文で述べている 5 つの方法について，導入するに当たって必要である前提条件をまとめたものが表 2 である.

表 2: 各方法の前提条件

	前提条件					
	1	2	3	4	5	6
DNS 法	√	√	√	-	-	-
ICMP 法 1	-	-	√	√	-	-
ICMP 法 2	-	-	√	√	√	-
ICMP 法 3	-	-	√	√	√	√
TCP 法	-	-	√	-	√	√

7 おわりに

本論文では，階層的に構成された組織において，ICMP，TCP を用いて透過的に VPN を確立する方法を提案し，DNS 法と合わせて比較，検討を行った.

今後の課題としては，提案した方法を実装し，VPN 確立にかかる時間の検証実験や，有効性を確認することがあげられる.

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, 情報処理学会研究報告 2003-DSM-30, Vol.2003, No.96. pp.25-30 (2003).

[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] 木澤政雄, 山井成良, 岡山聖彦, 横平徳美: 長期的なリンクダウン状態に対する TCP 通信の維持, マルチメディア, 分散, 協調とモバイル (DICOMO 2005) シンポジウム pp. 345–348 (2005).

[6] Paul Albitz, Cricket Liu 著, 高田広章, 小島育夫 監訳, 小館光正 訳: 『DNS&BIND』, オライリー・ジャパン (2005).

[7] W.Richard Stevens 著, 橘康雄 訳, 井上尚司 監訳: 『詳解 TCP/IP Vol.1』, ピアソン・エディケーション (2000).