代理ゲートウェイを用いたSOCKSベースの階層的VPN構成法

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って，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．組織の構成に応じてセキュリティドメインが階層的に構成されている場合，これに対応可能な既存の方法として，SOCKSバージョン5の拡張プロトコル，SOCKSバージョン5の参照実装であるSOCKS5，および，SSLの代理サーバを各セキュリティドメインに配置する方法などが知られている．しかし，これらの方法は，セキュリティドメインの階層数の増加にともなって暗号化のオーバヘッドが増大するという問題や，クライアントに既存のVPNソフトウェアをそのまま用いることができないという問題がある．そこで本論文では，これらの問題を解決するために，代理ゲートウェイを用いたSOCKSベースの階層的VPNの構築法を提案する．提案方法では，SSLの代理サーバを階層的に配置する方法と同様に，複数のセキュリティゲートウェイを仮想パスによって接続して，これらを結合して1つのVPNリンクを確立するとともに，クライアントとセキュリティゲートウェイとの通信に代理ゲートウェイを導入することにより，クライアントとサーバを変更することなく，安全かつ効率的な通信を実現している．さらに，SOCKS5を拡張することによって代理ゲートウェイとセキュリティゲートウェイを実装し，SOCKS5に比して暗号化のオーバヘッドが小さいことを確認することによって提案方法の有効性を確認した．

A Construction Method of SOCKS Based Hierarchical Virtual Private Networks with Proxy Gateway

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

VPN is one of important technologies on the Internet. With VPN, we can access to resources in the organizational network via the Internet. As the VPN method applicable to hierarchical security domains, following methods are known: the extension of the SOCKS version 5 protocol, SOCKS5 which is the reference implementation of SOCKS version 5 protocol and the method with proxy servers of SSL protocol. However, these VPN method has problems of either efficiency or availability. In this paper, we propose a new VPN method that makes it possible to establish more efficient VPN connections across hierarchical security domains and uses existing VPN software as client. The effectiveness of our method is confirmed by the experiment on the actual network using security gateways based on our method and evaluating the result of the experiment that our method gives more efficient communications across hirarchical security domains.

1. はじめに

近年，インターネットの発展にともなって，あらゆる種類の情報がインターネット上を流れるようになってきている．それらの中には，プライバシーにかかわる個人情報など秘匿性の高い情報が含まれるので，通信の安全性を確保することが重要である．たとえば，ある組織の構成員が組織外（自宅や出張先など）からインターネットを介して組織ネットワーク内の機密情報を利用する場合には，第三者による盗聴やなりすましを防ぐ必要がある．

上述した目的を実現するためには，認証および暗号化技術を用いることが一般的であるが，その1つとして，インターネットを介して遠隔地との間に仮想的な専用ネットワークを構築するための仮想プライベートネットワーク（Virtual Private Network，以下VPN

† 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

という）がある．VPNはネットワーク上の2点間に仮想的なリンク（以下，VPNリンクという）を設けてそれらがあたかも直接接続されているように見せるための技術であり，認証および暗号化技術との組合せによって情報の安全な伝送が可能になることから，注目を集めている．

VPNには様々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実現方法では，組織内など一様なアクセスポリシーを持つ範囲（以下，セキュリティドメインという）を定義し，その外部との接点にセキュリティゲートウェイ（Security Gateway，以下SGWという）を設置する．SGWは，外部から内部あるいは内部から外部へのアクセスの可否を制御し，アクセスの許可を与えた場合には，その通信を中継する．さらに，大規模な組織では部署ごとにアクセスポリシーが異なることが一般的であるので，大規模な組織におけるセキュリティドメインはインターネットのドメインのように階層的に構成されるのが自然である．このような構成において，インターネット上のクライアントがセキュリティドメインの最も内側にあるサーバと通信しようとする場合，最も外側のセキュリティドメインに設置されたSGWから内側に向かって1つずつSGWをたどる必要がある．

階層的に構成されたセキュリティドメインに対応できる既存のVPNの構成方式として，SOCKSバージョン5[1)]プロトコル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），SOCKSバージョン5プロトコルを拡張して複数のSGWをたどる方法[3)]（以下，従来法2），および，SSLの代理サーバをSGWとしてセキュリティドメインごとに配置する方法[4)]（以下，従来法3）などが知られている．

セキュリティドメインの外部にあるクライアントが階層的に構成されたセキュリティドメインの内部にあるサーバと通信しようとする場合，従来法1では，その経路上にあるSGWが中継サーバ（プロキシ）として動作し，次ホップのSGWへ接続してVPNリンクを確立する機能を追加することにより，隣接SGW間でそれぞれVPNリンクを確立してからそれらを結合し，従来法2では，SGWが次ホップのSGWの情報をクライアントに通知する機能を追加することにより，クライアントがサーバまでの経路上にあるSGWに対してVPNリンクを確立することを1ホップずつ繰り返す．しかし，いずれの方法においても，暗号化通信は各VPNリンクで独立して行われることから，通信の効率を考慮した場合，セキュリティドメインの階層数の増加にともなって暗号化のオーバヘッドも増大して効率が低下するという問題が発生する．また，これらの方法にSSL[5)]などを組み合わせ，クライアントとサーバの間でのみ暗号化通信機能を持ったVPNリンクを確立する方法も考えられるが，この場合はクライアントとサーバの両方にSSLなどのソフトウェアを追加しなければならない．

これに対し，従来法3では，従来法1において隣接するSGW間で確立されるコネクションを認証機能のみを持った仮想パスとしてとらえ，各区間で確立された仮想パスを用いてクライアントとサーバに隣接するSGWとの間にVPNリンクを確立することにより，階層数が増加しても暗号化のオーバヘッドが一定であるという特長を持つ．しかし，従来法3を既存のSSLソフトウェアに適用しようとする場合，クライアントに各SGWと認証を行うためのライブラリを追加しなければならないという問題がある．

これらの問題を解決するため，本論文では，代理ゲートウェイを用いたSOCKSベースの階層的VPN構成法を提案する．提案法では，クライアントとSGWの間にプロトコル変換を行う代理ゲートウェイを設置することにより，既存のVPNソフトウェアをクライアントでそのまま利用することができる．さらに，従来法3による階層的VPNへのアクセス方式に基づいて代理ゲートウェイとサーバに隣接するSGWとの間のみで1つのVPNリンクを確立することにより，従来法1および従来法2のようにセキュリティドメインの階層数が増加しても暗号化による通信効率の低下を最小限に抑えることができる．

以下，2章では，本論文が対象とするVPNのモデルと既存のVPN実現法の問題点を整理する．3章では本論文で提案する代理ゲートウェイを用いたVPNの階層的構成法について述べ，4章では提案法の実装とその有効性を確認するために実施し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．

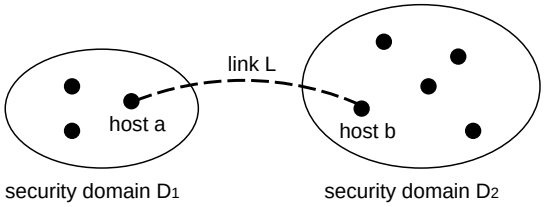

図 1 VPN の概念
Fig. 1 Concept of VPN.

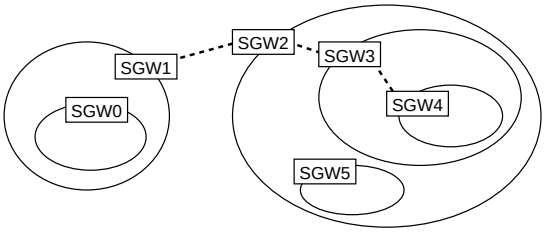

図 2 階層的なセキュリティドメインの例
Fig. 2 An example of hierarchical security domains.

2. 対象とするモデルと問題の整理

2.1 階層的 VPN モデル

VPN は，ネットワーク上の 2 点間に仮想的なリンク（VPN リンク）を設けることによって，それらがあたかも直接接続されているように見せる技術である．すなわち，セキュリティドメイン D_1 に属するホスト a とセキュリティドメイン D_2 に属するホスト b（$D_1 \neq D_2$）があるとき，a，b 間に仮想的なリンク L を用意することによって，論理的にはホスト a がセキュリティドメイン D_2（またはホスト b がセキュリティドメイン D_1）に属しているように見せることができる（**図 1**）．

このとき，ホスト a のみを論理的にセキュリティドメイン D_2 に属させる場合（端末型接続）と，セキュリティドメイン D_1 に属するすべてのホストをセキュリティドメイン D_2 に属させる場合（LAN 間接続）がある．LAN 間接続はネットワーク層以下で VPN を実現する必要があるが，従来法 1〜従来法 3 はいずれもトランスポート層あるいはセション層で実現されており，(4 章で述べる）本論文の実装も従来法 1 をベースとしているので，以下では端末型接続を前提に議論を行う．また，一般に VPN において通信内容の秘密を守ることは必須の要件ではないが，実際の運用では暗号化などによる通信内容の秘匿や認証の機能が必要とされることが多い．そこで本論文では，これらのセキュリティに関する機能を含んだ VPN 機能の実現を考える．

大学や企業などの組織における最も単純なセキュリティポリシーの与え方は，組織内部のどこでも一様なポリシーを与えることである．この場合，組織全体が 1 つのセキュリティドメインとなる．しかし，ある程度以上の規模を持つ組織では，情報へのアクセス可能性に関して内部が一様ではないことが多い．すなわち，一般に組織内の特定の部署のみがアクセス可能な情報が存在する．また，組織内部の他の部署からはアクセスできないが，外部の特定の組織からはアクセス可能な情報も考えられる．たとえば，大学のネットワークに接続された付属病院のデータを，他の学部などからはアクセスできないようにしつつ外部の病院からはアクセスできるようにする場合や，企業の中にある研究所が外部の研究機関と共同研究を行う場合などである．前者の例では大学全体が 1 つのセキュリティドメインであり，付属病院もまた 1 つのセキュリティドメインとなる．

このように，1 つの組織の中に複数のセキュリティドメインが構成されることは一般的で，しかもそれは階層的に構成される（**図 2**）．したがって，本論文では，階層的に構成されたセキュリティドメインを対象とする．

表 1 VPN に利用可能なプロトコル
Table 1 Protocols available for VPN.

	暗号化あり	暗号化なし
アプリケーション層	SSH（遠隔ログイン）	
セション層	従来法 1, 従来法 2	
トランスポート層	SSL, TLS, 従来法 3, SSH ※	
ネットワーク層	IPsec, VTun	
データリンク層		L2TP

※ポートフォワーディング機能により実現

2.2 既存の VPN 実現方法とその問題点

IP ネットワーク上で VPN を実現するために利用可能な方法には，1 章で述べた従来法 1〜従来法 3 のほかに，L2TP（Layer 2 Tunneling Protocol）[6]，IPsec（IP Security Protocol）[7),8)]，VTun（Virtual Tunnel）[9]，SSH（Secure Shell）[10]，SSL（Secure Sockets Layer），TLS（Transport Layer Security）など様々なものがある．TCP/IP のプロトコルスタックにおいて，各方法が対象とするプロトコル階層を**表 1** に示す．

これらのプロトコルのうち，利用者から意識することなく，すなわち，個別のアプリケーションへの組み込みやサービスごとの設定を必要とせずに利用できるのは，ネットワーク層以下のレベルでデータを伝送する方式（IPsec，VTun，L2TP）である．これらの方式はいずれも VPN を終端するネットワーク機器ど

うしがIPレベルで直接通信可能であることを要求する．しかし，本論文で対象とするような階層的セキュリティドメイン構成では，VPNを終端させたいSGWと外部のホストが直接通信することができないため，これらの方式ではVPNを構成することができない．

一方，SSLやTLS，および，SSHは，基本的にはクライアント–サーバが直接通信可能であることが前提であるので，階層的に構成されたセキュリティドメインにそのまま適用することはできない．また，クライアントからこれらの方式を再帰的に用いれば，セキュリティドメインの内側にあるサーバにアクセスすることも可能であるが，クライアントを利用するユーザがセキュリティドメインの構造を意識しなければならないという問題がある．

これに対し，従来法1〜従来法3は，階層的に構成されたセキュリティドメインに対応することができ，かつ，クライアントを利用するユーザがその構成を意識する必要がない．たとえば，セキュリティドメインの階層数が3であり，外部から最も内側のセキュリティドメインにあるホストにアクセスしようとする場合，従来法1〜従来法3におけるVPNリンクは，それぞれ，**図3**，**図4**，および，**図5**のように構成される．従来法1および従来法2において，イニシエータはsocksクライアント，SGW1〜SGW3はsocksサーバ，ターゲットはアプリケーションサーバに対応し，従来法3においては，イニシエータはSSL対応のアプリケーションクライアント，SGW1〜SGW3はSSLの代理サーバ，ターゲットはSSL対応のアプリケーションサーバに対応する．いずれの方法においても，イニシエータおよび各SGWは，ターゲットに到達するために次に接続すべきSGWを決定するための経路表を持つ．以下，イニシエータと直接通信を行うSGWを始点SGW，ターゲットと直接通信を行うSGWを終点SGW，始点SGWと終点SGWの間にあるSGWを中継SGWという．

従来法1〜従来法3は，いずれも，イニシエータが階層的に構成されたセキュリティドメインのSGWをたどることにより，イニシエータから終点SGWまでの間にVPNリンクを構成し，VPNリンクの暗号化通信機能を用いて秘匿性の高い通信をイニシエータ–ターゲット間で行うことができるが，VPNリンクの確立方法が以下のように異なる．

従来法1 イニシエータおよび各SGWはそれぞれが保持する経路表に従い，イニシエータに近い順に隣接する（直接通信可能な）SGWとの間にVPNリンクを確立する．

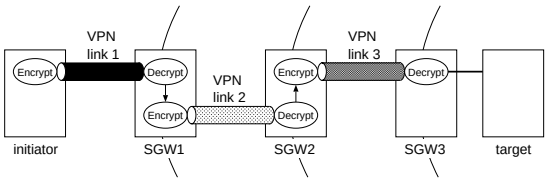

図3 従来法1によるVPNリンクの構成例
Fig. 3 An example of VPN links with existing method 1.

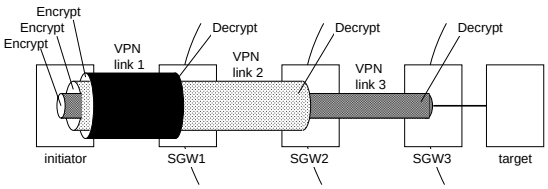

図4 従来法2によるVPNリンクの構成例
Fig. 4 An example of VPN links with existing method 2.

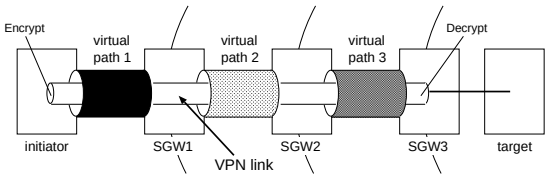

図5 従来法3によるVPNリンクの構成例
Fig. 5 An example of VPN link with existing method 3.

従来法2 イニシエータからターゲットに至るまでの経路上にあるSGWに対して，イニシエータと各SGWとの間でVPNリンクを確立することを1ホップずつ繰り返す．

従来法3 従来法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，イニシエータ〜終点SGWまでの各区間において仮想パスを確立した後，イニシエータと終点SGWとの間のみで1つのVPNを確立する．

従来法1および従来法2において，各VPNリンクでは必要に応じて認証および暗号化通信を行うことができるが，これらは各VPNリンクごとに独立している．したがって，すべてのVPNリンクで暗号化通信を行おうとした場合，イニシエータや各SGWにおいて暗号化および復号が繰り返されるので，セキュリティドメインの階層数の増加にともなって通信効率が低下するという問題がある．これを解決するための方法として，従来法1や従来法2で確立するVPNリンクでは暗号化通信を行わなず，その代わりにイニシエータ–ターゲット間でSSLなどのVPNソフトウェアを利用して暗号化通信を行うためのVPNリンクを確立することが考えられる．これにより，セキュリティド

メインの階層数が増加しても暗号化のオーバヘッドは最小限に抑えられるが，イニシエータおよびターゲットの両方に従来法1や従来法2とは異なるVPNソフトウェアを追加しなければならないという問題が発生する．

これに対し，従来法3では，VPNリンクを確立するのはつねにイニシエータ–終点SGW間のみであるので，従来法1あるいは従来法2にSSLなどを組み合わせる方法と同様，セキュリティドメインの階層数が増加しても暗号化のオーバヘッドは最小限に抑えられる．しかし，従来法3はイニシエータが各SGWと認証を行うためにSSLのプロトコルを拡張しているので，イニシエータに対してそのためのライブラリを追加しなければならないという問題がある．

3. 代理ゲートウェイを用いたSOCKSベースの階層的VPN構成法

3.1 前提条件

セキュリティドメインが階層的に構成されたネットワークにおいてVPNによる効率的な通信を行おうとする場合，2.2節で述べた問題を解決するためには，少なくとも以下の2つの条件を満たす必要がある．

条件1 暗号化のオーバヘッドが小さいこと

条件2 ユーザに対する利便性を考慮し，イニシエータで既存のVPNソフトウェアがそのまま利用できること

さらに，実際のインターネット環境における管理・運用を考慮した場合，以下のような条件を満足する方式を検討するのが自然であると考えられる．

条件3 各SGWごとに独立して認証の有無やユーザ管理などの管理が行えること

条件4 ターゲットが属するセキュリティドメインにおいてプライベートアドレスが利用されている場合を考慮し，NAT（Network Address Transrator）[11),12)]に対応できること

3.2 VPNリンク確立方法の検討

通信の効率を考えた場合，3.1節で述べた条件1を満たすのは，従来法1あるいは従来法2にSSLなどを組み合わせる方法と，従来法3である．しかし，上述したように，いずれの方法もイニシエータにソフトウェアを追加する必要があるので，そのままでは条件2を満たすことができない．特に，従来法1あるいは従来法2にSSLなどを組み合わせる方法では，ターゲットに対してもSSLなどに対応するための変更が必要となる．

そこで，本論文では，従来法3のVPNリンク確立手順に加え，プロトコル変換を行うための代理ゲートウェイを追加することを考えた（以下，提案法という）．例として，提案法においてセキュリティドメインの階層数を3とした場合のVPNリンクの構成を**図6**に示す．

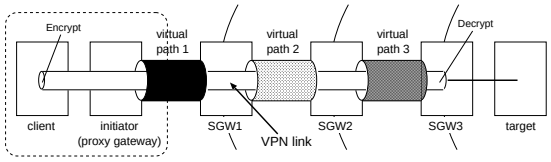

図6 提案法によるVPNリンクの構成例
Fig. 6 An example of VPN link with our method.

提案法では，クライアントと始点SGWの間に代理ゲートウェイを設置し，クライアントから送信された既存のVPN実現方法によるVPNリンク確立要求を代理ゲートウェイが受ける．そして，代理ゲートウェイがイニシエータとなって従来法3と同様に終点SGWまでの各区間に仮想パスを確立し，その後クライアント–終点SGW間で既存のVPN実現方法によるVPNリンクを確立する．提案法によるVPNリンクの確立は，次のような手順で実現できる．

(1) クライアントが既存のVPN実現方法のプロトコルを用いて終点SGWとの接続を試みる．

(2) クライアントから送出されたパケットを検知したイニシエータ（代理ゲートウェイ）は，そのパケットを転送せずに保持する．そして，イニシエータはパケットの宛先IPアドレスに従って経路表を検索し，セキュリティドメインの最も外側にあるSGW（始点SGW）に対してコネクションの確立を試みる．

(3) コネクションが確立すると，イニシエータは自己のIPアドレスとポート番号，および，ターゲットのIPアドレスとポート番号をSGWに対して送信する．

(4) SGWは受け取った情報に基づいて認証方法を決定し，イニシエータとの間で認証を行う．

(5) 認証に成功した場合（認証が必要ない場合を含む）には，SGWは経路表を参照して自己が終点SGWであるかどうかを調べる．終点SGWでなければ，経路表に基づいて隣接するSGWとの間に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．

(6) 隣接するSGWをたどりながら，終点SGWに到達するまで(3)〜(5)と同様の処理を繰り返す．

(7) 終点SGWは，イニシエータに対してコネク

ション確立完了メッセージを送信する．これを受け取ったイニシエータは，保持していたクライアントからのパケットを仮想パスを用いて終点SGWに送出する．

(8) クライアントは既存のVPN実現方法のプロトコルを用いて終点SGWとの間にVPNリンクの確立を試み，成功すれば終点SGWはクライアントからのパケットをターゲットに転送する．クライアント–終点SGW間で確立されたVPNリンクにおいては，既存のVPN実現方法に基づいた暗号化通信を行う．

上述した手順において，イニシエータを認証するための情報はこれを必要とするSGWのみが知っておけばよいので，条件3を満たす．さらに，ターゲットが属するセキュリティドメインにおいてNATが使用されている場合であっても，直接通信するのはイニシエータも含めて隣接する階層のSGWどうしであるので，それぞれの区間の通信においてはNATが必要なく，しかも，クライアント–ターゲット間で送受信されるパケットは，仮想パスにおいて特別な処理を行うことなく透過的に転送されるので条件4も満たす．

以上のことから，提案法では上述した手順を用いることによって3.1節の条件をすべて満たすことができる．

4. 実装と評価

3章で述べたように，提案法ではクライアントに既存のVPN実現方法を用いることができるので，ユーザに対する利便性が高いことは明らかである．そこで，暗号化のオーバヘッドによる通信効率について提案法の有効性を検証するため，提案法を実装して性能評価を行った．本章では，実装方法と性能評価について述べる．

4.1 実装方法

提案法のVPNリンク確立法は従来法3に基づいているが，実装としては従来法1のみが広く公開されている．さらに，提案法の代理ゲートウェイが対応する既存のVPN実現方式を従来法1に限定すれば，提案法は従来法1のVPNリンクを仮想パスとして扱うことによって実現できる．従来法1はセション層で動作し，基本的にはクライアントからサーバへの1方向のTCPおよびUDPのトラヒックを対象としているが，クライアントではrunsockというコマンドを用いて任意のアプリケーションを対応させることが可能であり，アプリケーションに対する組み込みやサービスごとの設定を行う必要がないので，実用上問題はない．したがって，FreeBSD3.2Rおよび4.1Rを搭載したAT互換機を対象とし，従来法1（SOCKS5）のsocksサーバのソースコード（C言語を使用）を変更することによってSGWおよび代理ゲートウェイを実装した．従来法1のsocksサーバでは，認証や暗号化通信の有無の組合せをそれぞれmethodとして定義しており，methodの識別番号を用いてVPNリンク確立時に交渉する機能を持つ．そこで，提案法を示す新たなmethodを定義し，交渉によってこのmethodが選択された場合には，3.2節で述べた手順に従ってsocksサーバが動作するように，以下の機能を追加することによってSGWを実現した．

(1) 代理ゲートウェイとの認証機能

(2) （認証に必要な）次ホップのSGWの情報を代理ゲートウェイに通知する機能

これにより，従来のmethodが選択された場合，提案法のSGWは従来法1のSGWとしても動作する．また，代理ゲートウェイについては，クライアントからのVPN確立要求に従って，提案法を示す新たなmethodの識別番号を用いてSGWと交渉する機能と，終点SGWに至るまでの各SGWと認証を行うための機能を従来法1のsocksサーバに追加することによって実現した．

一方，クライアントについては，socksクライアントのソースコードにはいっさいの変更を加えていない．なお，イニシエータ–各SGW間の認証と，クライアント–終点SGW間の認証および暗号化通信については，従来法1と同様にKerberos[13),14)]の認証および暗号化通信機能を用いている．

4.2 性能評価

4.2.1 実験方法

性能評価は，**図7**に示すようにイニシエータとターゲットとの間に3つのSGWを配置し，イニシエータからターゲットに対して実際に通信を行うことによって実施した．4.1節で述べたように，実装が広く公開されているのは従来法1のみであるので，実験は提案法と従来法1について行った．このとき，提案法に基づいて実装したSGWは従来法1のSGWとしても動

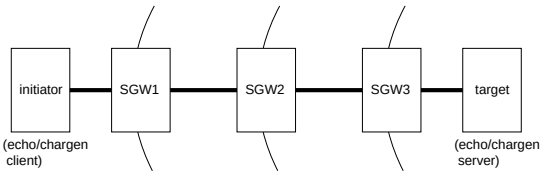

図7 実験環境の構成
Fig. 7 The structure of the experimental environment.

作することから，イニシエータのホストには socks クライアントと代理ゲートウェイを置き，socks クライアントを代理ゲートウェイあるいは始点 SGW のいずれかに接続することにより，提案法と従来法 1 を切り替えている．なお，各ホストは，学内ネットワークを利用して，100 Mbps あるいは 10 Mbps のリンクにより接続した．

実験には echo（ポート番号 7）および chargen（ポート番号 19）サービスの 2 種類を用い，echo については，echo クライアントが echo サーバに接続後，echo クライアントから比較的小さいデータを echo サーバに送信し，同じデータを echo クライアントが echo サーバから受信するという処理を 1,000 回繰り返して終了するものとし，chargen については，chargen クライアントが chargen サーバに接続後，比較的大きいデータを chargen サーバから 100 回受信して終了するものとした．前者は telnet や rlogin などによる対話的な通信，後者は ftp などによるバッチ処理的な通信に相当する．以下，echo サービスを利用した実験を実験 1，chargen サービスを利用した実験 2 という．

それぞれの実験において，送受信するデータサイズによる提案法と従来法 1 との違いを明らかにするため，実験 1 については echo クライアントから echo サーバに送信するデータ量を 128，512，1,024（単位はいずれも bytes）の 3 種類，実験 2 については chargen サーバから chargen クライアントが受信するデータ量を 100，500，1,000（単位はいずれも Kbytes）の 3 種類とした．また，起動するクライアントが 1 つである場合，TCP の slow start の影響により，リンクの帯域に余裕があってもスループットが低下してしまう可能性があることから，この影響を軽減するため，いずれの実験においてもイニシエータでは 2 つのクライアントを起動して並列実行した．

実際の計測は，VPN リンクの確立方法（提案法および従来法 1），データサイズ（各実験とも 3 種類）のすべての組合せに対して，実験 1 は 100 回，実験 2 は 20 回の試行を実施し，イニシエータの接続開始から VPN リンク確立までに要した時間（以下，connect 時間という）と，VPN リンク確立後，データの送受信を完了するまでに要した時間（以下，data 時間という）の平均値を算出した．なお，認証と暗号化通信については，いずれの実験においても，すべての SGW で認証を行い，かつ，すべての VPN リンクで暗号化通信を行うものとした．

4.2.2 実験結果と考察

実験結果として，実験 1 および実験 2 のそれぞれにおける 1 試行あたりの平均所要時間を**表 2** および**表 3** に示す．各表におけるデータ量は，クライアントが 1 度に送信あるいは受信するデータの大きさを意味する．

表 2 実験 1 の結果
Table 2 Result of experiment 1.

データ量 (bytes)	従来法 1		提案法	
	connect (秒)	data (秒)	connect (秒)	data (秒)
128	1.361	8.631	1.529	5.771
512	1.401	15.210	1.566	9.850
1024	1.409	21.106	1.487	14.995

表 3 実験 2 の結果
Table 3 Result of experiment 2.

データ量 (Kbytes)	従来法 1		提案法	
	connect (秒)	data (秒)	connect (秒)	data (秒)
100	1.347	28.158	1.527	26.381
500	1.451	144.204	1.551	131.400
1000	1.383	290.694	1.482	259.829

表 2 および表 3 から分かるように，data 時間については，いずれの実験についても提案法が従来法 1 よりも小さく，しかも，データ量に応じてその差が広がっている．この差は，従来法 1 ではイニシエータから終点 SGW までの各区間で確立された 3 つの VPN リンクで独自の暗号化通信を行うのに対し，提案法ではイニシエータ–終点 SGW 間の VPN リンクのみで暗号化通信を行うことから，暗号化のオーバヘッドによるものであると考えられる．また，各実験の data 時間について従来法 1 と提案法を比較すると，データ量にかかわらず，実験 1 では従来法 1 が提案法の約 1.5 倍，実験 2 では従来法 1 が提案法の約 1.1 倍となっている．VPN リンク確立方法による差は実験 1 の方が大きいが，実験 1 は実験 2 に比べて 1 度に送受信するデータ量が小さいので，暗号化のオーバヘッドによる差がより顕著に現れているものと思われる．

一方，connect 時間を比較すると，いずれの実験においても従来法 1 よりも提案法の方が 80〜180 ミリ秒程度大きくなっている．これは，従来法 1 に比べ，提案法では代理ゲートウェイを追加していることが原因であると考えられるが，data 時間に比べて connect 時間の差は小さく，実験 1 や実験 2 のような手順による通信においては，実用上問題にならないと考えられる．

以上のことから，提案法は従来法 1 に比して暗号化のオーバヘッドが少なく，より効率的な通信が行える

といえる．なお，従来法2および従来法3についての実験は行っていないが，原理上，同じ認証方式および暗号化通信方式を用いたと仮定すれば，従来法2においてイニシエータ–終点SGWのVPNリンクのみで暗号化通信を行った場合と従来法3の通信効率は提案法とほぼ同等，従来法2においてすべてのVPNリンクで暗号化通信を行った場合には，イニシエータにおいて暗号化を多重に行うので，従来法1よりも悪化することが考えれらる．

5. おわりに

本論文では，階層的に構成されたセキュリティドメインにおいて，既存のVPNリンク確立方法に対して既存のVPNソフトウェアに対応するための代理ゲートウェイを導入することにより，クライアントに特別なソフトウェアを追加することなく効率的な暗号化通信を実現する方法を提案した．さらに，SOCKS5を拡張することによってSGWと代理ゲートウェイを実装し，実験によりその有効性を確認した．

今後の課題としては，イニシエータおよびSGWが保持する経路表を効率的に管理する方法の検討があげられる．現状では，経路表は従来法と同様にイニシエータおよびSGWのそれぞれが設定ファイルとして静的に管理しているが，セキュリティドメインとSGWの対応関係をたとえばDNSサーバで管理することにより，SGWの情報をあらかじめ知っておかなくても正しいSGWにアクセスできるようになると考えられる．

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) 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) Dierks, T. and Allen, C.: *The TLS Protocol Version 1.0*, RFC2246 (1999).
6) Pall, G.S., Palter, B., Rubens, A., Townsley, W.M., Valencia, A.J. and Zorn, G.: *Layer Two Tunneling Protocol "L2TP"*, RFC2661 (1999).
7) Kent, S. and Atkinson, R.: *Security Architecture for the Internet Protocol*, RFC2401 (1998).
8) Thayer, R., Doraswamy, N. and Glenn, R.: *IP Security Document Roadmap*, RFC2411 (1998).
9) Krasnyansky, M.: Virtual Tunnels over TCP/IP networks. http://vtun.sourceforge.net/
10) SSH Communications Security: SSH Secure Shell. http://www.ssh.org/
11) Egevang, K. and Francis, P.: *The IP Network Address Translator (NAT)*, RFC1631 (1994).
12) Srisuresh, P. and Holdrege, M.: *The IP Network Address Translator (NAT) Terminology and Considerations*, RFC2663 (1999).
13) Kohl, J. and Neuman, C.: *The Kerberos Network Authentication Service (V5)*, RFC1510 (1993).
14) Linn, J.: *The Kerberos Version 5 GSS-API Mechanism*, RFC1964 (1996).

(平成13年5月8日受付)
(平成13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，大阪大学工学部助手．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）．インター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）．

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．同年京都大学大型計算機センター助手．平成 10 年より大阪市立大学学術情報総合センター講師．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．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，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．