社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

利用者が複数の VPN に多重帰属できる VPN アーキテクチャの提案

原　義博† 大崎　博之† 今瀬　真† 田島　佳武†† 丸吉　政博††
村山　純一†† 松田　和浩††

† 大阪大学大学院情報科学研究科　〒 560–8531 豊中市待兼山町 1–3
†† 日本電信電話株式会社，NTT 情報流通プラットフォーム研究所
〒 180–8585 東京都武蔵野市緑町 3–9–11
E-mail: †{y-hara,oosaki,imase}@ist.osaka-u.ac.jp,
††{tajima.yoshitake,maruyoshi.masahiro,murayama.junichi,matsuda.kazuhiro}@lab.ntt.co.jp

あらまし　近年のネットワーク技術の発展に伴い，様々な社会組織におけるコミュニケーションがネットワークを介した通信により行われ，ネットワーク上に仮想組織が形成されると考えられる．我々は，これら仮想組織群をサイバーソサイエティと称している．サイバーソサイエティにおける「人」は，セキュリティを維持しながら，複数の仮想組織と通信可能な関係を確立する必要がある．本稿では，セキュリティの観点からネットワークとして VPN (Virtual Private Network) を利用することを想定し，利用者が，仮想組織に対応する個々の VPN に多重帰属することが可能な VPN アーキテクチャを提案する．本提案は，ホスト単位に VPN を構成でき，サイト単位に構成する PPVPN (Provider Provisioned VPN) に比べて柔軟性に優れることが特徴である．また，宛先 VPN への直接アクセスを可能とさせ，エクストラネットに比べて転送性能に優れることも特徴である．
キーワード　VPN，エクストラネット，多重帰属，テレワーク，アクセス制御

VPN Architecture Enabling Users to be Associated with Multple VPNs

Yoshihiro HARA†, Hiroyuki OHSAKI†, Makoto IMASE†, Yoshitake TAJIMA††, Masahiro MARUYOSHI††, Junichi MURAYAMA††, and Kazuhiro MATSUDA††

† Graduate School of Information Science and Technology, Osaka University
1–3 Machikaneyama–cho, Toyonaka–shi, Osaka, 560–8531 Japan
†† NTT Information Sharing Platform Laboratories, NTT Corporation　3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
E-mail: †{y-hara,oosaki,imase}@ist.osaka-u.ac.jp,
††{tajima.yoshitake,maruyoshi.masahiro,murayama.junichi,matsuda.kazuhiro}@lab.ntt.co.jp

Abstract　Recent development of network technologies enables network communications in various social organizations and enables various social organizations to be virtualized in networks. We named the mass of virtual organizations ”cyber-society”. A ”person” in cyber-society needs to establish communication association s with multiple virtual organizations with adequate security. Therefore, we beli eve that VPN service is applicable to realize cyber-society because of its security. In this paper, we propose VPN architecture where a single user’s host can b e simultaneously associated with multiple VPNs corresponding to virtual organiza tions. Because our architecture enables VPN service to be utilized per customer’ s host basis, it is more flexible than PPVPN (Provider Provisioned VPN) architec ture, which is designed per customer’s site basis. Additionally, our architectur e is superior to an extranet architecture in terms of forwarding performance, be cause it enables users to directly and simultaneously access to destination VPNs.
Key words　VPN, extranet, multiple association, telework, access control

1. はじめに

近年のネットワーク技術の発展により，さまざまな社会活動が地理的な要因から開放され，社会構造が広域分散型へと変化すると考えられる．例えば，現在，ネットワークの高速化および WEB サービスの発展 [1] は，購買や流通といった商行為を，次第にネットワーク上に移行させつつある．また， e-Japan 構想による行政機能のネットワーク化の推進 [2] や，教育におけるネットワークの活用などが進展しつつある．ビジネス分野においても，イントラネット／エクストラネットが普及し，社内システム，社間取り引き，業務連携等がネットワーク上で行われている [3]．また，テレワークや SOHO 等の勤務形態を採る労働者も増加している [4]．

このような広域分散型の社会構造では，ネットワーク上に「サイバーソサイエティ」と称する仮想組織群が形成される．サイバーソサイエティにおける「人」は，例えばビジネス上は複数の会社に雇用されている．このため，同時に複数の役割を持つことになり，セキュリティを維持しながら複数の仮想組織に容易に接続できる必要がある．つまり，多重帰属の実現が不可欠である．

このような背景を踏まえ，本研究では，サイバーソサイエティにおいて仮想組織への多重帰属をネットワークサービスとして実現することを目標とする．ここでサービスとは，商業的な意味のサービスではなく，ネットワーク管理者やサービスプロバイダがネットワークを介して利用者に提供する機能を意味する．この目標の実現に向けた従来のネットワークサービスとしては，現在， IETF の ppvpn ワーキンググループにおいて検討が進められている，プロバイダ提供型 VPN (PPVPN; Provider Provisio ned VPN) がある． PPVPN は，限定されたユーザ間での通信サービスを提供でき，仮想組織を実現する環境として適している．従来の PPVPN では， VPN はサイトの集合であり，あるサイト内の全ユーザが共通の VPN に帰属することが前提となっている． PPVPN 間を接続する技術としては，エクストラネットが存在し，複数の仮想組織への多重帰属を実現する技術として適している．

しかし，既存の PPVPN では，サイト単位で VPN を構成するため，ホスト単位で VPN を構成できない．このため，同一の VPN サイトに属するサイバーソサイエティ上の「人」が異なる仮想組織に帰属することができない．また，既存のエクストラネットでは，サイバーソサイエティ上の「人」が組織への多重帰属を実現できるものの，接続される VPN 数が増えると転送性能の劣化や管理負荷の増加などの問題が生じる．このような問題を解決するために，本研究では， VPN がホスト単位で構成されると共に，ホストが多数の VPN に多重帰属できる，新しい VPN アーキテクチャを提案する．

2 章では，従来の VPN 技術として， PPVPN とエクストラネットについて紹介し，それぞれの長所と短所を述べる． 3 章では，多重帰属を実現する VPN アーキテクチャを提案する．4 章では，提案した VPN アーキテクチャの実現例を示す．5 章では提案した VPN アーキテクチャの応用例を示す． 6 章では本稿のまとめを述べる．

2. 従来の VPN

2.1 PPVPN (Provider Provisioned Virtual Private Network)

現在， IETF の ppvpn ワーキンググループにおいて，プロバイダ提供型 VPN (PPVPN; Provider Provisioned VPN) アーキテクチャの検討が進められている [5]〜[7]．従来，企業などの組織が安全な組織内ネットワークを構築するにあたり，各地に散らばる LAN を専用線で接続する方法が用いられてきた．専用線の利用は非常に安全であるが，回線費用が非常に高価になるという問題がある． PPVPN サービスは，サービスプロバイダが，サービスプロバイダネットワーク内に仮想的な専用網を構築し，専用線よりも安価に，顧客に提供することを目的としたネットワークサービスである．

図 1 は PPVPN を模式的に表した図である．サービスプロバイダネットワークを介さずに通信可能できる，顧客のネットワークをサイトと呼ぶ．図 1 の CE (Customer Edge) 機器とは，顧客のサイトの出口に設置される機器である． CE 機器には顧客のホストが接続される． PE (Provider Edge) 機器とは，サービスプロバイダネットワーク (SP Network) 内にあり，CE 機器と直接接続される機器である．サービスプロバイダは，PE 機器間に VPN トンネルと呼ばれるトンネルを設定することにより， PPVPN サービスを提供する． VPN トンネルの片端に投入されたパケットは，反対側の片端に転送される．また，トンネルの両端以外からトンネルにパケットを投入することはできない．図 1 の例では， VPN A の CE 機器から PE 機器に送られたパケットは， VPN トンネルを通り， VPN A の CE 機器に転送される．このように，VPN トンネルは仮想的な専用線として機能する．また， VPN トンネルのためのトンネリング技術としては， IPSec ， MPLS ， L2TP ， GRE ，IP-in-IP などが用いられる．

PPVPN には，次のような長所が存在する．まず， PPVPN では，サービスプロバイダと契約した顧客以外の者は，顧客の VPN トンネルを利用できないため，顧客は，第三者から，自 VPN を遮断することができる．また PPVPN では，サービスプロバイダネットワークのアドレス体系と，顧客に提供される PP VPN のアドレス体系が独立しているため，顧客は，提供された VPN のアドレス体系を自由に決めることができる．

しかし，従来の PPVPN には，次のような短所も存在する．文献 [5] によると，PPVPN においては， VPN を構成する最小の単位はサイトである．図 1 の例で説明すると， VPN A の CE 機器に接続されたサイト内の全ホストは， VPN A に帰属することが前提となっている．そのため，PPVPN では， VPN アクセスのために，サイト単位の認証は必要であっても，ユーザ単位の認証を必要としない [6]．このような理由で，PPVPN では，同一サイト内の各ホストが，それぞれ異なる VPN に帰属することができない．

2.2 エクストラネット

異なる VPN に帰属する端末と通信を行うための技術として，

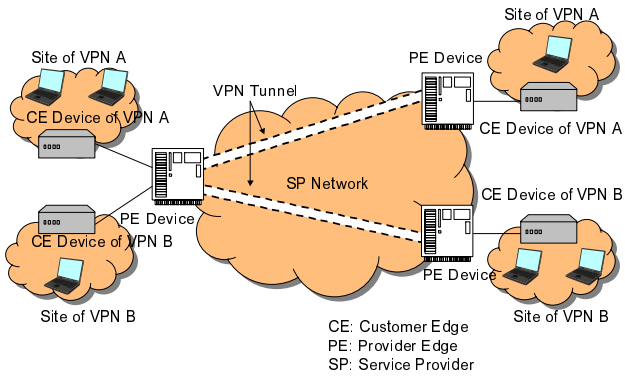

図 1　PPVPN のモデル図

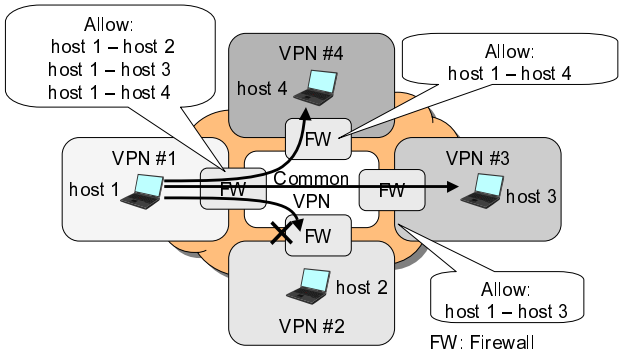

図 2　エクストラネットのモデル図

エクストラネットが存在する [8], [9]．エクストラネットを利用することにより，ある組織の VPN に帰属しながら，別組織の VPN のホストと通信することができる．

既存のエクストラネットでは，一般に，多数の VPN 同士を接続するために，共用 VPN を用意し，各 VPN を共用 VPN と接続する．この様子を図 2 に示す．図 2 では，VPN #1 〜 #4 の 4 つの VPN を，共用 VPN を介して接続している．各 VPN はそれぞれ異なるポリシーで運営されているため， VPN と共用 VPN の間にファイアウォールを設置し，パケットフィルタリングやアドレス変換を行う． VPN 間で通信を行う場合，2 箇所のファイアウォールでパケットフィルタリングを行う．

エクストラネットには，次のような長所が存在する．まず，各 VPN が，自 VPN のポリシーに従い，ファイアウォールのフィルタリングルールを設定することができるため，異なる VPN 間を接続してもセキュリティが保たれる．また，共用 VPN を介して多数の VPN と接続することができる．これにより，多数の VPN を一つのインターフェースで利用することができる．

ただし，エクストラネットには次のような短所も存在する．各 VPN はそれぞれ独自のアドレス体系で運用されているため， VPN 間の接続に際して，アドレスを整合させなければならない． NAT [10] によるアドレス変換などを利用することは可能だが， NAT を利用する場合，利用できるアプリケーションの種類が制限される．また， VPN 間のセキュリティを適切に保つために，ファイアウォールのフィルタリングルールを適切に設定しなければならない．接続する VPN の数が増えると，フィルタリングルールも増加し， VPN 間の接続ポリシーも複雑になるため，管理負荷が増大する．さらに，パケット単位のフィルタリングが，フィルタリングルール増加時に，転送性能の劣化を引き起こすと考えられる．

3. MAVPN アーキテクチャの提案

PPVPN の問題は， VPN の構成単位がサイト単位に限定されることである．また，エクストラネットの問題は，ホストから多数の VPN への同時アクセスを可能とさせると，ファイアウォールでのフィルタリング処理負荷が増大することである．これらの問題を解決するために，本稿では，構成単位をホスト単位とし，ホストが複数の VPN に同時に接続できる VPN アーキテクチャを提案する．このような VPN アーキテクチャを利用することにより，一つのサイトの中に複数の VPN が存在できる．また，一つのホストが複数の VPN に多重帰属することも可能になる．以下では，この VPN を MAVPN (Multiply-Associated VPN) と呼ぶ．

MAVPN のアーキテクチャを図 3 に示す．このアーキテクチャでは，それぞれのホストに対して MAPVN サービスが提供される． MAVPN サービスは，ホストに対して，転送系のインターフェースと制御系のインターフェースを介して提供される．利用者データの転送に関わる機能は転送系のインターフェースを介して提供され，その他の機能は制御系のインターフェースを介して提供される．

ホストに提供される機能の概要は次の通りである．

a)　転送系インターフェースを介して提供

– VPN アクセス機能

物理層ではサイトに対してネットワークへのアクセス回線が一本提供される．一方，データリンク層あるいはネットワーク層では VPN への論理的なアクセス回線を複数本提供される．

– ホスト認証能機

VPN へのアクセス回線単位で，認証機能が提供される．すなわち，VPN への接続要求に対する認証は，サイト単位でなくホスト単位に行われる．

– VPN アドレッシング

ホストに対して，VPN へのアクセス回線ごとに，ホストが用いるアドレスが割り当てられる．このアドレスは，該当する VPN の管理者が独自に規定した VPN のアドレス空間から割り当てられる．このため，割り当てられたアドレスが重複することを許容できなければならない．

b)　制御系インターフェースを介して提供

MAVPN アーキテクチャでは，サイト内の (例えばルータなどの) 転送装置が，不正な動作により， VPN 間を接続することなどを防がなければならない．よって，サイト内の転送装置に対して，制御系のインターフェースを介して，転送装置の制御機能が提供される (図 3) ．

4. MAVPN の実現例

4.1 ホストベース VPN

MAVPN の実現例を示す前に，まず，構成単位をホスト単位

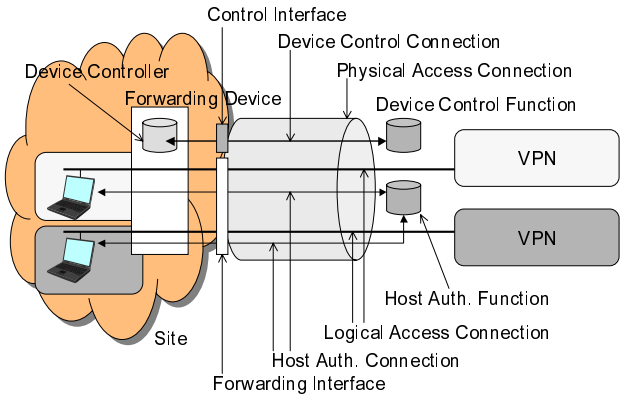

図 3　MAVPN のアーキテクチャ

とする VPN の実現例を示す．このような実現例をホストベース VPN と呼ぶことにする．この実現例では，サービスプロバイダ提供型のホストベース VPN サービスを仮定している．

ホストベース VPN の実現例として， 図 4 のように，サービスプロバイダネットワークへのアクセス回線を， IEEE802.1Q の VLAN [11] と PPP [12] との組み合わせで構成する方法が考えられる．サービスプロバイダネットワーク内では， VLAN-ID 毎に異なる VPN へ接続する．サイト内では， VLAN スイッチを用いれば，ホストを VLAN 毎に分離して配置することが可能となる．また，各ホストが PPPoE [13] を用いて，サービスプロバイダネットワークにアクセスすれば，ホスト単位に VPN の選択と接続認証することが可能となる．各ホストがポート VLAN で異なるセグメントに配置されていれば，ホスト間でアドレスが重複することを許容できる．サービスプロバイダネットワークと CE 機器との制御インターフェースは，例えば IPSec 上で SNMP を用いることができる．この際， SNMP のマネージャはサービスプロバイダネットワーク内に機器制御サーバとして設置され，サイト内の CE 機器は SNMP エージェントとして動作する．

図 4 の実現例は，サイト内の各ホストが，それぞれ異なる VPN に帰属することができる．これにより， VPN の構成単位がサイト単位に限定されるという， PPVPN の問題を解決している．

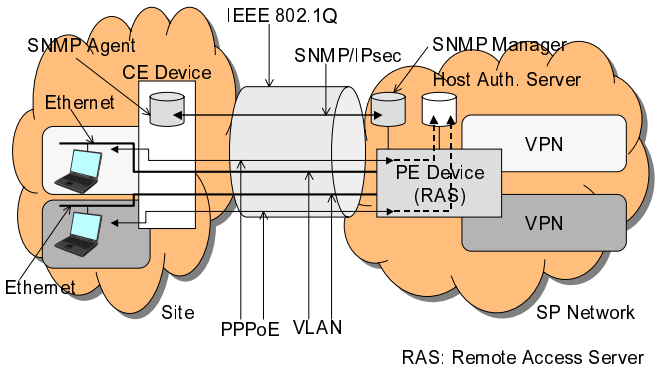

図 4　ホストベース VPN の実現例

4.2　ホストベース MAVPN

図 5 に，一つのホストが複数の VPN に同時に接続できる，MAVPN の実現例を示す．このような実現例を，ホストベース MAVPN と呼ぶことにする．この実現例では，サービスプロバイダ提供型のホストベース MAVPN サービスを仮定している．

ホストベース MAVPN は，ホストベース VPN の実現例と同様に， IEEE802.1Q の VLAN と PPP との組み合わせで構成する．ホストベース MAVPN では，一つのホストを複数の VLAN セグメントに割り当てる．このとき，ホストは一つのアクセス回線で複数の VLAN を扱う必要がある．ホストが VLAN のタグ付けをサポートしていない場合，ホストと VLAN スイッチの間で， VLAN-ID に替わる別の識別子が必要になる．ホストは複数の VLAN セグメントからアドレスを与えられることになるため，複数のアドレスを持つ．さらに，ホストは複数の PPPoE セッションを用いて，複数の VPN への接続が認証される必要がある．

従来のエクストラネットでは，接続する VPN の数が増えると，フィルタリングルールが増加し， VPN 間の接続ポリシーも複雑になる．このため，接続の管理負荷が増大するという問題が存在した．また，パケット単位のフィルタリングが，フィルタリングルール増加時に，転送性能の劣化を引き起こすという問題も存在した．ホストベース MAVPN では，ホストが目的の VPN に直接接続されることで，これらの問題を解決している．目的の VPN を選択する際には，ホストの認証によってセキュリティを確保する．このため，パケットフィルタリングが必要ない．よってパケットフィルタリングによる転送性能の劣化が存在せず，エクストラネットに比べて性能が向上する．また，フィルタリングルールが必要ないため，エクストラネットに比べて管理負荷が減少する．

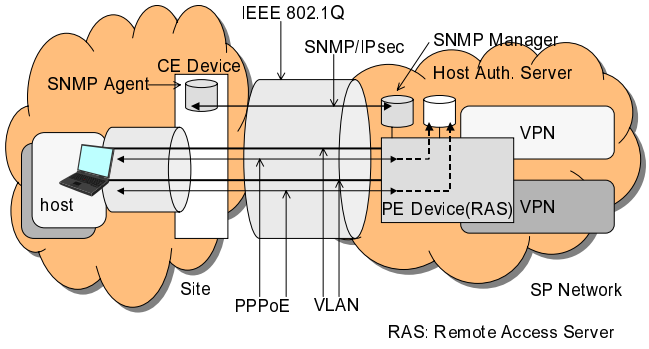

図 5　ホストベース MAVPN の実現例

5.　MAVPN の応用例

5.1　ホストベース VPN の応用例

まず，ホストベース VPN の応用例を示す．ホストベース VPN をサーバ用途に応用した場合，クライアント用途に応用した場合の 2 つに分けて，その応用例を挙げる．

- 企業向けサーバハウジングサービス

企業に対して，企業内の重要なサーバを設置する場所を提供するサーバハウジングサービスでの利用が考えられる．災害な

どが発生した場合，本社とは別の，災害に耐え得る場所に，重要なサーバを設置しておくことは重要である．ホストベース VPN を応用すると，図 6 のように，ハウジングサービスプロバイダは，ハウジング用のサイトを一つ用意することで，異なる VPN に属する多数の企業に対し，安全なサーバ設置場所を提供することができる．ハウジング用のサイトを多数の顧客で共有することになり，安価なサービスを提供できる．

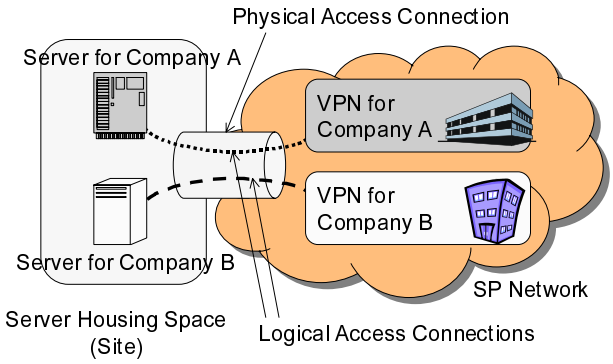

図 6　企業向けサーバハウジングサービス

- ホームユーザ用 VPN サービス

ホストベース VPN により，ホスト単位の VPN を構築できるようになると，図 7 のような，ホームユーザによる VPN の構築が容易になると考えられる．例えば，趣味のサークルの VPN，家族の VPN など，1 ユーザを構成単位とするグループに VPN を提供することができるようになる．

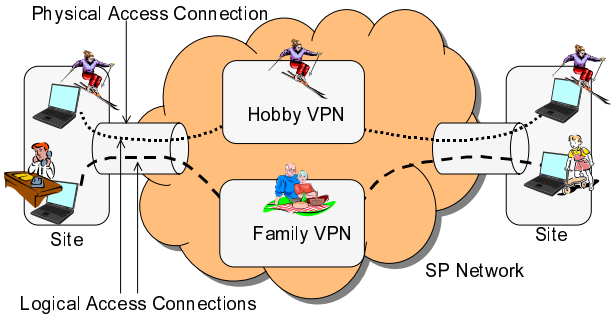

図 7　ホームユーザ向け VPN サービス

5.2　ホストベース MAVPN の応用例

ホストベース MAVPN をサーバ用途に応用した場合，クライアント用途に応用した場合の 2 つに分けて，その応用例を挙げる．

- ホスティングサービス

ホスティングサービスプロバイダが企業や個人にサーバを貸し出すサービスが広く行われている．ホストベース MAVPN を応用することにより，ホスティングサービスプロバイダは，より安価なホスティングサービスを顧客に提供できる．図 8 のように，物理的に一つのサーバを，ホストベース MAVPN を用いて多数の VPN に多重帰属させることにより，多数の顧客に対して提供する．このため，安価にホスティングサービスを提供することができる．

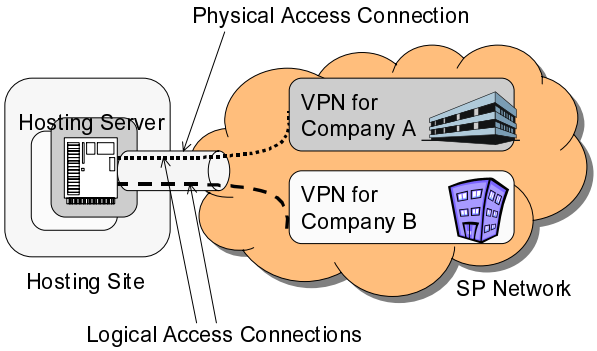

図 8　ホスティングサービス

- B2B 向け企業ネットワークの構築

B2B (Business To Business) の企業間商取引においては，様々な企業が VPN を用いてエクストラネットを構築し，商取引を行う．ホストベース MAVPN を導入することにより，図 9 のように，同一企業の構成員のみからなる企業 VPN に加えて，他の企業の構成員と， B2B 用の VPN を構築することができる．

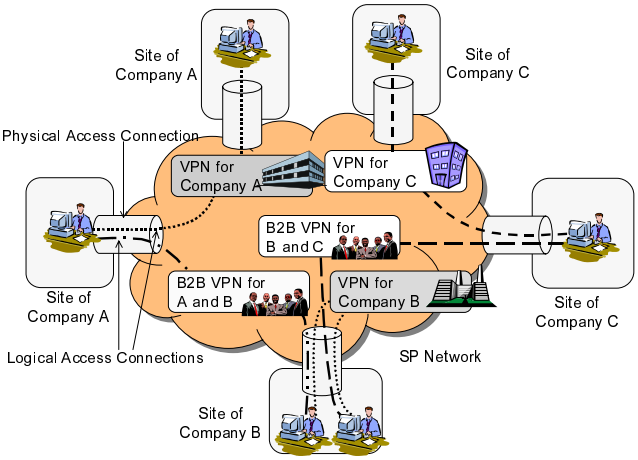

図 9　B2B 向け企業ネットワークサービス

謝　　辞

本研究の一部は，平成 14 年度科学技術振興調整費「サイバーソサエティを実現する仮想網技術」の援助による．

6. む　す　び

本稿では，サイト単位ではなく，ホスト単位で構成される，MAVPN アーキテクチャを提案した．また， MAVPN アーキテクチャにより，ホストが，複数の VPN に対して同時に帰属できることを示した．さらに，本稿で提案した MAVPN アーキテクチャと，従来の VPN アーキテクチャを比較し， MAVPN アーキテクチャの優位性を示した．今後の課題としては，階層化した MAVPN アーキテクチャの提案， MAVPN アーキテクチャの性能評価， MAVPN のプロトタイプ実装などが挙げられる．

文　献

[1] S. J. Vaughan-Nichols, "Web Services: Beyond the Hype," *IEEE COMPUTER*, vol. 35, pp. 18–21, Feb. 2002.

[2] 大山 永昭, "電子政府の現状と課題," 情報処理, vol. 44, pp. 455–460, May 2003.

[3] 総務省, "平成 13 年 通信利用動向調査報告書," May 2002. available at `http://www.johotsusintokei.soumu.go.jp/yusei/adapter.Main`.

[4] 日本テレワーク協会, "日本テレワーク人口等に関する実体調査," July 2002. available at `http://www.soumu.go.jp/s-news/2002/020705_4.html`.

[5] M. Carugi *et al.*, "Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks `<draft-ietf-l3vpn-requirements-00.txt>`," *Internet Draft*, Apr. 2003.

[6] A. Nagarajan, "Generic Requirements for Provider Provisioned VPN `<draft-ietf-l3vpn-generic-reqts-01.txt>`," *Internet Draft*, Aug. 2003.

[7] R. Callon *et al.*, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks `<draft-ietf-l3vpn-framework-00.txt>`," *Internet Draft*, Mar. 2003.

[8] 三好 潤, 今井田 伊佐宗, 飯盛 可織, 村山 純 一, 栗林 伸一, "VPN 間通信におけるポリシーに基づくサービス制御方式 の検討," 信学技報 *SSE99-171*, vol. 99, Mar. 2000.

[9] 原 博之, 村山 純一, 飯盛 可織, 今井田 伊佐宗, "ポリシーベース IP-VPN 方式," 信学技報 *IN2000-101*, vol. 100, pp. 39–46, Oct. 2000.

[10] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," *Request for Comments (RFC) 1631*, May 1994.

[11] IEEE Standards for Local and Metropolitan Area Networks, "Virtual bridged local area networks," *IEEE Standard 802.1Q-1998*, Dec. 1998.

[12] W. Simpson, "The Point-to-Point Protocol (PPP)," *Request for Comments (RFC) 1661*, July 1994.

[13] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)," *Request for Comments (RFC) 2516*, Feb. 1999.