解　説

サイバーソサイエティを実現する仮想網技術の動向

Overview of VPN Technologies for Cyber Society

今瀬　真
大阪大学大学院情報科学研究科 情報ネットワーク学専攻
imase@ist.osaka-u.ac.jp
大崎博之
大阪大学大学院情報科学研究科 情報ネットワーク学専攻
oosaki@ist.osaka-u.ac.jp
松田和浩
日本電信電話（株）情報流通プラットフォーム研究所
matsuda.kazuhiro@lab.ntt.co.jp

近年のネットワーク技術の発展により，社会活動の多くが地理的な要因から解放され，行政の広域化だけでなく，テレワークを主体とする企業やテレエデュケーションを主体とする教育機関といった，社会構造そのものの広域分散化が進むと考えられる．このようなネットワーク上での仮想組織（サイバーソサイエティ）を実現するためには，超スケーラブルな仮想網構築技術，仮想網間接続技術および多重帰属制御技術を確立する必要がある．本稿では，サイバーソサイエティへの適用が期待されているプロバイダ提供型VPN（PPVPN）等の概要と問題点を紹介した後，この問題点を解決する技術例を紹介する．

はじめに

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．たとえば，ネットワークの高速化およびWebサービスの発展は，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や，教育におけるネットワークの活用なども進展しつつある．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，社内業務，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．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．さらに，現在盛んに研究・開発が行われている「ユビキタスネットワーク」の実現・普及がこれをさらに加速させると予想される．これらの結果，社会活動の多くが地理的な要因から解放され，行政の広域化だけでなく，テレワークを主体とする企業やテレエデュケーションを主体とする教育機関といった，社会構造そのものの広域分散化が進むと考えられる．

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ことになる（**図-1**）．このサイバーソサイエティは，従来のインターネット世界よりも，より実社会に近い社会活動が可能な場である．

本稿では，このようなサイバーソサイエティを実現するための技術課題を整理し，現在の技術動向を紹介する．

サイバーソサイエティ実現に必要なネットワーク技術

従来，プライベート網の構築には，高速ディジタル回線，フレームリレー，ATM技術を用いたセルリレー等が用いられてきたが，コスト低減と柔軟な構成変更の要求から，近年，インターネットVPN，IP-VPN，広域

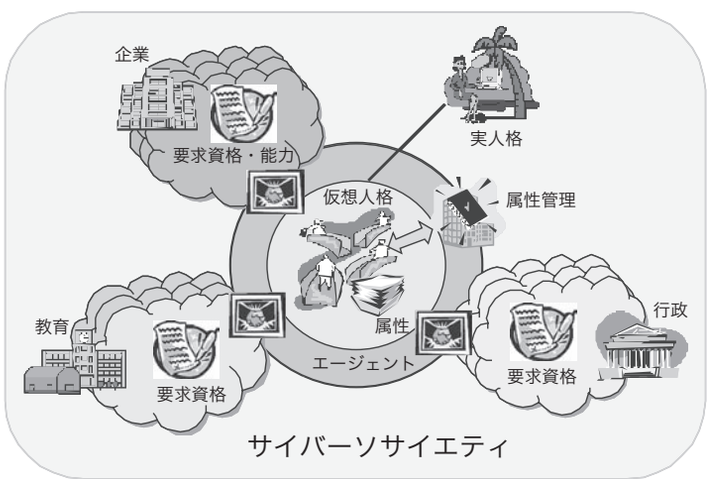

図-1　サイバーソサイエティの概念

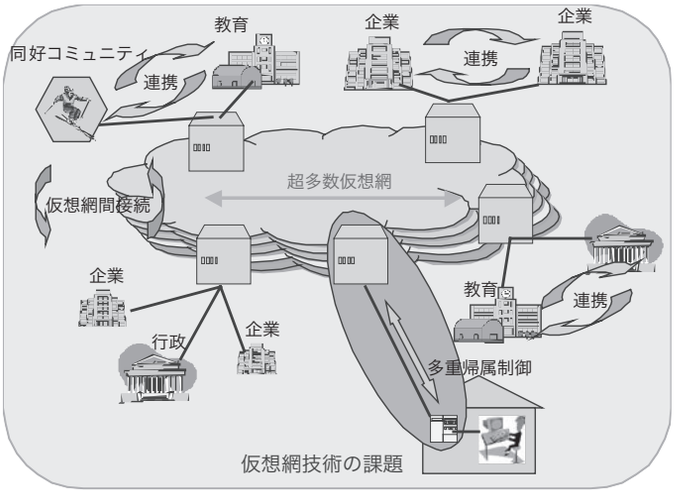

図-2　サイバーソサイエティ実現に必要なネットワーク技術

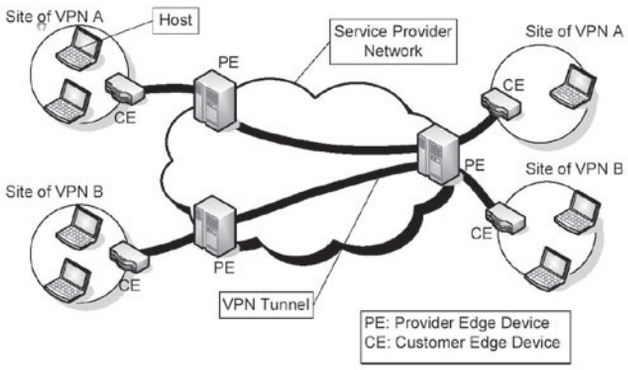

図-3　PPVPNの概念

VLAN（Virtual LAN）による仮想プライベート網（VPN：Virtual Private Network）が普及してきた．インターネットVPNはインターネットを基盤として，端末―端末間での通信の暗号化によりVPNに必要なセキュリティを確保する技術である．IP-VPNはMPLS（Multi-Protocol Label Switching）という，サービスプロバイダ網内をカプセル化転送する技術を用いて閉域性を実現している．広域VLANはEthernetによるVLAN技術をメトロエリアに展開したものである．

しかし，サイバーソサイエティを実現するためには，さらに次の技術を確立する必要がある（**図-2**）．

◆超スケーラブルな仮想網構築技術

サイバーソサイエティを実現するには，物理的に単一のネットワークを論理的に自在に分割し，数万以上の超多数のVPNを収容可能とする必要がある．現在のVPN技術では管理アドレス数の点で実現可能なVPN数に制限がある．

◆仮想網間接続技術

既存の仮想網構築技術では，組織の変更や組織に対応するVPN間の接続性を柔軟に変更する機構が不十分である．さらにVPN内およびVPN間の通信がベストエフォート型であり，通信の公平性が確保できていない．

◆多重帰属制御技術

現状のIP-VPNへのダイヤルアップ接続，IP-Sec（Security Architecture for Internet Protocol）技術によるインターネットVPNでは，接続先を切り替えるためにユーザが接続を明示的に切り替える必要がある．現在，ネットワークサービスは常時接続・定額料金が一般的になっており，利便性を考慮すると同時に複数のVPNに帰属するような機構が必要になる．

現状のVPN技術

ここでは，多数のVPNを実現する技術としてプロバイダ提供型，VPN間を接続する技術としてエクストラネットの概要と問題点について述べる．

◆PPVPN

これまで，IETFのLayer 2 Virtual Private Networksワーキンググループや Layer 3 Virtual Private Networks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きた[1)～3)]．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-3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（Service Provider Network）を介さない顧客のローカルネットワークをサイト（Site）と呼ぶ．図-3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機器には顧客の端末が接続される．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-3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

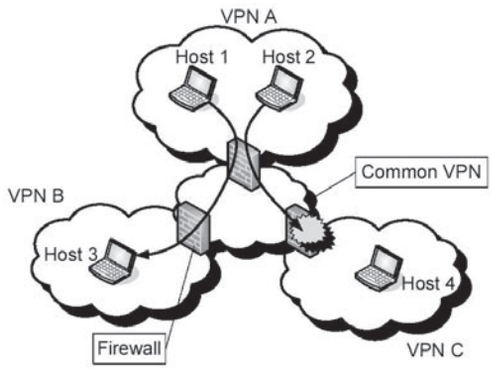

図-4　エクストラネットの概念

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（Layer2 Tunneling Protocol）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PPVPN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．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-3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端末は，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，同一サイト内の各端末が，それぞれ異なるVPNに帰属することができない．

◆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，エクストラネットがある．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の端末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，複数のVPN同士を接続するために，共用VPNを用意し，各VPNを共用VPNに接続する．この様子を**図-4**に示す．図-4では，3つのVPNを，共用VPN（図-4のCommon VPN）を介して接続している．各VPNはそれぞれ異なる方針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（図-4のFirewall）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カ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の方針に従い，ファイアウォールのフィルタリング規則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を介して複数のVPNと接続することができる．これにより，複数のVPNを1つのインタ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（Network Address Translation）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規則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，フィルタリング規則も増加し，VPN間の接続方針も複雑になるため，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，フィルタリング規則増加時に，転送性能の劣化を引き起こすと考えられる．

超スケーラブルな仮想網構築技術

超スケーラブルな仮想網を構築するには，次のような3つの処理が必要となる．

(1) 基盤となるネットワークを用意する．
(2) その上にさまざまなVPNを構築する．
(3) さらに利用者が複数のVPNを同時にかつ安全に利用できるように，各VPNへのアクセスを制御する．

これらの処理は，PPVPNやエクストラネットを単純に利用するだけでは実現困難である．しかし，これらの3つの処理を既存のネットワーク技術によって階層的に構成することにより，比較的容易に実装することができると考えられる．たとえば，従来のPPVPNサービスは，基盤となるネットワークの上に論理的なネットワークを構築し，顧客に提供するサービスであると考えることができる．このとき，複数のVPNを制御する階層を追加することは容易であると考えられる．

そこで，上記の(1)を物理ネットワークレベルに，(2)を論理ネットワークレベルに，(3)をユーザネットワークレベルに対応させ，それを実現するネットワーク階層の候補と技術をまとめたものを**表-1**に示す．

表-1に示す各ネットワークレベルの代表的な組合せ（アーキテクチャ）を評価した結果を，**表-2**に示す．表-2では，物理ネットワークレベルをレイヤxで，論理ネットワークレベルをレイヤyで，ユーザネットワーク

ネットワークレベル	実現するネットワーク階層	実現するネットワーク技術の例
ユーザネットワークレベル	L4 以上	URL によるアクセス制御
	L3	IP アドレスによるアクセス制御
論理ネットワークレベル	L3	IPSec VPN
	L2	VLAN，MPLS
物理ネットワークレベル	L3	IP
	L2	Ethernet

表-1　超スケーラブルな仮想網を実現するためのネットワーク階層と技術

評価項目	2-2-3	2-3-4	3-3-3
ノード数のスケーラビリティ	×	×	○
VPN 数のスケーラビリティ	○	×	×
エンティティ数のスケーラビリティ	△	○	△
通信速度	○	×	△
利用できるサービスの多様性	○	×	○

表-2　代表的なアーキテクチャの評価

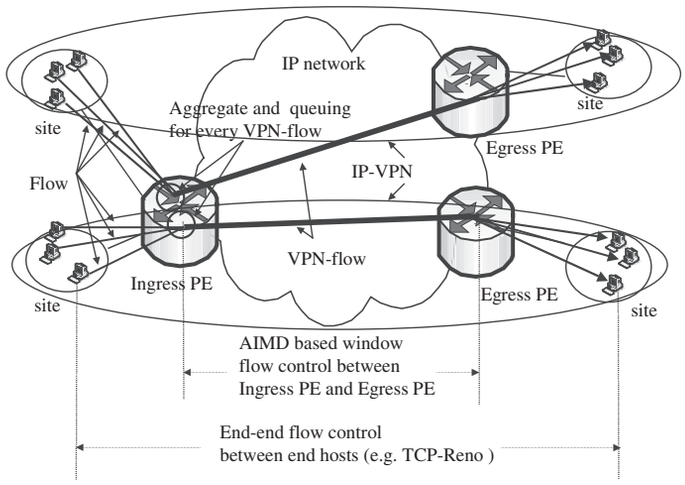

図-5　AIMD型のウィンドウフロー制御を利用したIP-VPN公平性制御機構I2VFC

レベルをレイヤzで実現したアーキテクチャをアーキテクチャ x-y-z と表現している．

これから，既存の技術を組み合わせて超スケーラブルな仮想網を実現する場合，基盤となる物理的なネットワークをレイヤ2で実現し，その上にVPNをレイヤ2で実現し，利用者から複数のVPNへのアクセスをレイヤ3の情報を用いて制御するという，アーキテクチャ 2-2-3 が最も適しているといえる．筆者らは，このアーキテクチャを，MAVPN（Multiply-Associated VPN）アーキテクチャと名づけた[4]．

多重帰属制御技術の章では，この結果に基づいたプロトタイプの概要と実行結果を紹介する．

仮想網間接続技術

VPN間の接続においては，VPNの接続を柔軟に変更する技術に加えて，VPN間およびVPN内における公平性の確保が重要である．前者については，多重帰属制御技術と密接に関連するので，次章で紹介することとし，本章では，公平性の確保について述べる．

PPVPNのフレームワーク上のIP-VPNでは，IPネットワークがベストエフォート型のネットワークであるために，あるVPNが大量のトラフィックを発生させた場合に，他のVPNのスループットが不当に低く抑えられるという問題が発生する．

そこで，公平なIP-VPNサービスを，できるだけ低コストで実現することを考える．IP-VPNサービスが公平であるとは，「VPN間公平性」（inter-VPN fairness，VPNを契約している顧客間の公平性）および「VPN内公平性」（intra-VPN fairness，同じVPNに収容されている利用者間の公平性）の両方が満たされていることと定義する．

筆者らは，VPN間公平性およびVPN内公平性を，低コストで実現するための，IP-VPN公平性制御機構I2VFC（Inter- and Intra-VPN Fairness Control）を考案した（**図-5**）[5]．I2VFCは，IP-VPNのサービスプロバイダの，PE機器上で動作する，ウィンドウフロー制御である．具体的には，入口側のPE機器（入側PEルータ）において，VPNに収容されている複数のフロー（パケットの流れ）を，単一のVPNフローとして集約する．さらに，入口側のPE機器と，出口側のPE機器（出側PEルータ）の間で，AIMD（Additive Increase and Multiplicative Decrease）型のウィンドウフロー制御を行う．提案するI2VFCは，VPN間公平性の基準を，IP-VPNのサービスプロバイダが自由に規定できること，また，PE機器のみを変更するだけでよく，既存のIPネットワークへ容易に導入できるという点に特徴がある．

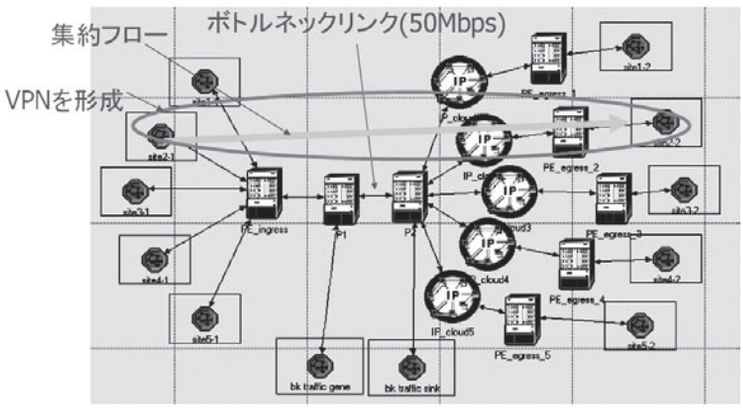

図-6　シミュレーション環境のトポロジとフロー多重帰属制御技術

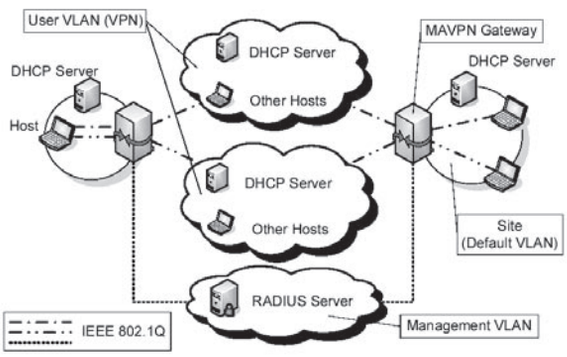

図-7　プロトタイプの論理的なネットワーク構成

I2VFCの効果を，ネットワーク環境をソフトウェアでシミュレーションするOPNETを用いて評価した．**図-6**にシミュレーション環境のトポロジとフローを示す．

シミュレーションでは，ボトルネックルータが代表的なアクティブキュー管理機構であるRED（Random Early Detection）を採用したルータの場合，VPN数が5，10，20のすべての場合に，VPN間の公平性がほぼ完全に実現できることを確認した．ボトルネックルータがDropTailルータの場合，VPN数が5，10，20のすべての場合に，VPN間の公平性が30%程度の誤差の範囲内で実現できることを確認した．今後は，VPN数が増加するなどネットワークの状況に変化が起こった場合に，制御のパラメータの設定を自動的に行う方法についても検討する予定である．

多重帰属制御技術

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，端末から多数の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．筆者らは，これらの問題を解決するアーキテクチャMAVPNを考案し，プロトタイプを実装した．ここでは，その概要と実行結果について述べる．

図-7に，実装したプロトタイプの論理的なネットワーク構成を示す．利用者に提供するVPNはIEEE 802.1Q VLANで実現する．IEEE 802.1Qは，Ethernetフレームに12ビットのVLAN IDを含むタグを付加することでVLANを実現する技術である．今回のプロトタイプでは，簡単のために，各VLANはそれぞれ1つのIPサブネットを構成するものとし，各VLANのIPアドレス空間は重複しないことを前提とした．

端末はMAVPNゲートウェイ（MAVPN Gateway）という機器を介してVLANに接続する．端末からMAVPNゲートウェイ間へのアクセス回線をIEEE 802.1Qで多重化することにより，端末は複数のVLANに同時に帰属できる．端末の用いるアドレスについては，各VLANに設置されたDHCPサーバによって，各VLANのIPアドレス空間からIPアドレスが割り当てられる．ただし，外部からのアクセスを受けるようなサーバ類では，DHCPを用いず，各VLANのIPアドレス空間から静的にアドレスを割り当てる．

MAVPNゲートウェイは，端末からのアクセス回線であるIEEE 802.1Q VLANをVPNであるIEEE802.1Q VLANにブリッジすることにより，端末はVPNをEthernetとして利用できる．また，MAVPNゲートウェイは利用者の認証機能を持ち，VLANへの帰属を許可された利用者の端末からのアクセス回線のみをVLANに接続する．端末が最初にMAVPNゲートウェイに接続し，どのVLANにも帰属していない状態では，同一サイト内でのみ通信可能である．つまり，図-7におけるサイト（Site）が認証VLANにおける初期VLANに相当する．

利用者の認証に用いる利用者のアカウント情報は，RADIUSサーバ（RADIUS Server）によってすべてのMAVPNゲートウェイに提供される．RADIUSサーバは管理用の特別なVLAN（Management VLAN）に設置される．また，RADIUSサーバに保存されるアカウント情報は，利用者のID，帰属が許可されているVLANのID，パスワードの3つからなる．すなわち，各利用者は，帰属するVLANの数だけパスワードを持つことになる．

図-8は，端末とVPNの接続状況である．

図-9は，端末ソフトウェアの起動時の画面である．利用者は利用者IDを入力し，帰属したいVPN名を選択してログインボタンをクリックする．今回は，各利用者

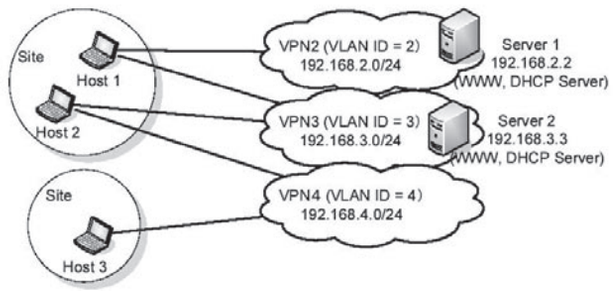

図-8　端末とVPNの接続状況

図-9　端末ソフトウェアの画面

が，自分が利用できるVPNの名前の一覧を持っているという前提でインタフェースを設計したため，VPN名一覧が端末ソフトウェアに表示されている．

図-10は，他のVPNや端末との通信の様子を示す画面である．端末1（Host1）からVPN2との通信や，端末1（Host1）からVPN3との通信および端末2（Host2）と端末3（Host3）との通信が可能であることを確認した．

上記は，多重帰属を手動で行っているが，VPNへの帰属条件を規定したポリシーに基づき自動制御を行う方法の検討も行われている[6]．現在，アーキテクチャの検討を終了し，プロトタイプを開発中である．

今後の課題

サイバーソサイエティを実現するには，以上述べたネットワーク層での対処とともに，ミドルウェア層，アプリケーション層の課題についても解決する必要がある．

たとえば，現在のインターネットでのいわゆるハンドル名による匿名性は，実人格とネットワーク上の仮想人格の対応関係を証明する機構がなく重要な社会活動を行う組織に対しては適用できない．反対に現在のテレワークのように雇用者が被雇用者を実人格で特定できるような仕組みでは，性別・年齢・障害等に対してユニバーサル性の実現は困難である．今後は，これらの課題についても検討が必要である．

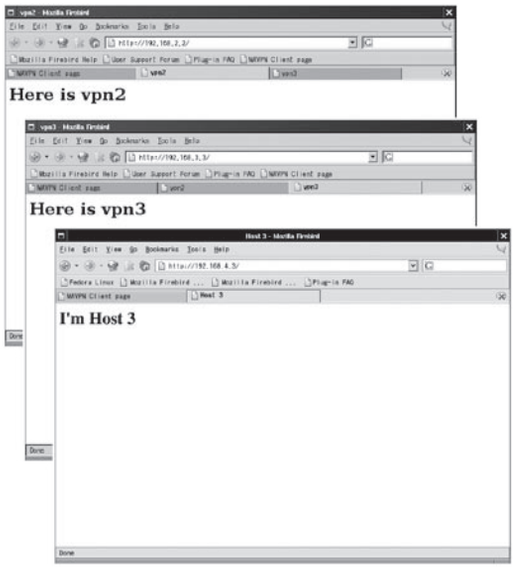

図-10　他のVPNや端末との通信の様子

おわりに

サイバーソサイエティを実現するための技術課題および実現技術の状況について紹介した．筆者らは，大阪大学とNTT情報流通プラットフォーム研究所との産学協同による研究を進めており，大学の学術的に優れた技術と企業の有用な技術を融合させて，数年後にはサイバーソサイエティを実現する技術を確立したいと考えている．

参考文献

1）Carugi, M. et al.: Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks, InternetDraft, draft-ietf-l3VPN-requirements-00.txt（Apr. 2003）.
2）Nagarajan, A. : Generic Requirements for Provider Provisioned VPN, Internet Draft, draft-ietf-l3VPN-generic-reqts-01.txt（Aug. 2003）.
3）Callon, R. et al.: A Framework for Layer 3 Provider Provisioned Virtual Private Networks, Internet Draft, draft-ietf-l3VPN-framework-00.txt（Mar. 2003）.
4）Hara, Y., Ohsaki, H., Imase, M., Tajima, Y., Maruyoshi, M. and Murayama, J. : On Layered VPN Architecture for Enabling User-based Multiply Associated VPNs, in Proceedings of the International Conference on Information Networking (ICOIN) 2004, pp.303-312（Feb. 2004）.
5）本田，大崎，今瀬，村山，松田：AIMD型のウィンドウフロー制御を利用したIP-VPN公平性制御機構，電子情報通信学会，IN研究会（May 2004）.
6）木村，山口，安本，東野：ポリシーに基づく多重帰属の制御が可能なVPNアーキテクチャの提案，電子情報通信学会IN研究会（Mar. 2004）.

（平成16年11月30日受付）