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と実装

本田 治[†] 原 義博[††] 大崎博之[†]
今瀬 真[†] 丸吉政博[†††] 松田和浩[†††]

近年のネットワーク技術の発展にともない，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し，最適なネットワークアーキテクチャを明らかにする．さらに，実現可能性を示すためにプロトタイプを実装する．

On Designing and Implementation of VPN Architecture Enabling User's Multiple Association

Osamu Honda,[†] Yoshihiro Hara,[††] Hiroyuki Ohsaki,[†]
Makoto Imase,[†] Masahiro Maruyoshi[†††]
and Kazuhiro Matsuda[†††]

Recent development of network technologies enables network communications among various social organizations and enables various social organizations to be virtualized in networks. We named the mass of virtual organizations "Cybersociety". A "person" in the cyber-society needs to establish communication associations with multiple virtual organizations with adequate security. Therefore, we believe that VPN service is applicable to realize Cybersociety because of its security. In this paper, we propose VPN architecture where a single user's host can be simultaneously associated with multiple VPNs corresponding to virtual organizations. Furthermore, we implement a prototype system to show feasibility of our VPN architecture.

1. はじめに

近年のネットワーク技術の発展により，様々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に変化すると考えられる．たとえば，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，社間取引，業務連携など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などの勤務形態をと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，ネットワーク上に我々が「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，たと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，サイバーソサイエティにおける人の仮想組織への多重帰属の実現が不可欠である．

このような背景をふまえ，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

† 大阪大学大学院情報科学研究科
Graduate School of Information Science and Technology, Osaka University
†† 大日本印刷株式会社
Dai Nippon Printing Co., Ltd.
††† NTT 情報流通プラットフォーム研究所
Information Sharing Platform Laboratories, NTT Corporation

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．本研究では，セキュリティの観点から仮想組織を VPN（Virtual Private Network）[5),6)] を用いて実現する．すなわち，本研究では，サイバーソサイエティにおいて，ホスト（端末）単位で VPN への多重帰属を実現することを目標とする．

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，IETF の ppvpn ワーキンググループにおいて検討が進められた，プロバイダ提供型 VPN（PPVPN; Provider Provisioned VPN）[5),6)] 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[7),8)]，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（端末）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，本稿では，VPN がホスト単位で構成されるとともに，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し，最適なアーキテクチャを明らかにする．さらに，このアーキテクチャに基づいたプロトタイプを実装することにより，実現性を確認する．

2 章では，従来の VPN 技術の長所と短所を述べる．3 章では，多重帰属を実現する VPN アーキテクチャの設計目標を，4 章では，考案した VPN アーキテクチャの概要と実現方法の評価結果を示す．5 章では提案した VPN アーキテクチャに基づいたプロトタイプの実装と評価結果を示す．6 章では本稿のまとめを述べる．

2. 従来の VPN

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（PPVPN），加えて，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それぞれ述べる．

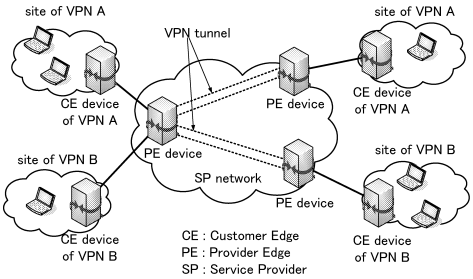

図 1 PPVPN の概念
Fig. 1 Concept of a PPVPN.

2.1 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，PPVPN アーキテクチャの検討が進められた[5),6)]．

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は，PE（Provider Edge）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 トンネルは仮想的な専用線として機能する．この VPN トンネルのためのトンネリング技術としては，IPSec（Security Architecture for Internet Protocol）[9)]，MPLS（Multi-Protocol Label Switching）[10)]，L2TP（Layer2 Tunneling Protocol）[11)] などが用いられる．

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という長所がある．しかし，VPN A の CE（Customer Edge）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ので，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という短所がある．

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，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 どうしを接続するために，共用 VPN を用意し，各 VPN

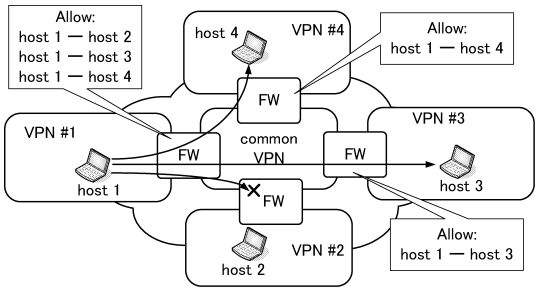

図 2 エクストラネットの概念
Fig. 2 Concept of an extranet.

を共用 VPN に接続する．この様子を**図 2** に示す．

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，エクストラネットでは，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という問題がある．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，スケーラビリティの確保が困難になるという問題もある．

エクストラネットを用いて，端末単位の VPN への多重帰属を実現する場合，端末ごとに VPN を構築する必要がある．このため，ファイアウォールに，ネットワークに収容される端末数規模のフィルタリング規則が必要となる．一方，本稿で提案する多重帰属を実現する VPN の実現方式の場合，端末が帰属する VPN 数とそれらの VPN に帰属する端末数の積規模のフィルタリング規則が必要となる．よって，本稿で提案する多重帰属を実現する VPN の実現方式は，エクストラネットにおける問題を解決している．

3. MAVPN の設計目標

本稿では，多重帰属を実現する VPN の実現方式を MAVPN（Multiply-Associated VPN）アーキテクチャとして提案する．以下に，MAVPN の設計目標およびその設定理由を示す．

(1) **VPN 数，端末数がスケーラブルであること**
サイバーソサイエティ上には，非常に多くの仮想組織が形成されると考えられる．よって，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，多数の VPN を収容可能とする必要がある．

(2) **端末単位で複数の VPN に同時に帰属できること**
サイバーソサイエティでは，人が複数の仮想組織に同時に帰属すると考えられる．しかし，現状の IP-VPN へのダイヤルアップ接続，IP-Sec 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．
VPN への多重帰属を実現すれば，不正な利用者によって VPN 間でパケットの中継が行われる可能性がある．このため，何らかのフィルタリング処理が必要であると考えられる．たとえば，5 章で実装するプロトタイプシステムでは，MAVPN ゲートウェイにおいて，MAC アドレスおよび IP アドレスによるフィルタリングを行っている．しかし，フィルタリング処理によって，不正なパケットの中継を完全に防ぐのは技術的に困難である．たとえば，多重帰属しているユーザが，アプリケーションゲートウェイ（メールサーバやプロキシサーバなど）を動作させている場合，不正なパケットの中継を防ぐことは困難である．このため，現実には利用ポリシなどによる制限などの導入が必要になると考えられる．

4. 階層型 MAVPN アーキテクチャ

4.1 階層型アーキテクチャ

MAVPN を実現するには，大きく分けて，次のような 3 つの処理が必要となる．まず，基盤となるネットワークを用意する．次にその上に様々な VPN を構築する．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．

これらの処理を実装するのは，複雑かつ困難であることが予想される．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，実現することが可能であると考えられる．以下では，階層化された 3 つのネットワークレベル（物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベル）ごとに，各レベルに必要な機能を議論する．そして，各ネットワークレベルをどの階層を用いて実現するのかによって，MAVPN の

表 1 用語の定義
Table 1 Definition of terms.

物理ネットワークレベルの用語	
ホスト	端末や計算機
ノード	ホスト，ルータ，スイッチなどの機器
リンク	ノード間を接続する通信回線
論理ネットワークレベルの用語	
エンティティ	ホスト上の利用者や利用者が利用するアプリケーション，サーバプログラムなど
VPN	エンティティから構成される，閉域性を持つ仮想的なネットワーク
ユーザネットワークレベルの用語	
多重帰属	エンティティが複数の VPN に同時に接続すること

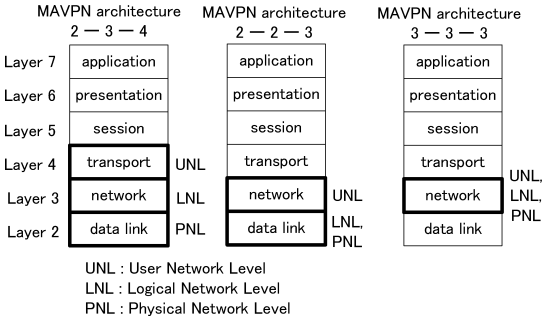

図 3 3 種類の代表的な MAVPN アーキテクチャ
Fig. 3 Three typical MAVPN architectures.

アーキテクチャが，どのような特徴を持つのかを評価する．

物理ネットワークレベルは，VPN を構築する基盤となるネットワークを提供するネットワークのレベルである．論理ネットワークレベルは，物理ネットワークレベルで提供されたネットワーク上に VPN を構築するレベルである．ユーザネットワークレベルは，複数の VPN に同時に接続（多重帰属）する際の，VPN へのアクセス制御を行うネットワークのレベルである．なお，本稿において，それぞれのネットワークレベルで用いる用語の定義を**表 1** に示す．

4.2 代表的な MAVPN アーキテクチャ

各ネットワークレベルを，どの階層におけるどのような技術を用いて実現するのかについて，3 つの MAVPN のアーキテクチャを取り上げる．広域ネットワーク接続サービスおよび PPVPN サービスは，レイヤ 2 またはレイヤ 3 のネットワークが主流であるため，物理ネットワークレベルおよび論理ネットワークレベルをそれぞれレイヤ 2 またはレイヤ 3 のネットワークで実現することとする．また，ユーザネットワークレベルをレイヤ 3 またはレイヤ 4 以上の情報を用いて実現することとする．

各ネットワークレベルを実現するネットワーク階層の組合せを考える場合，アーキテクチャの性質に関係するのは，どの物理ネットワークレベル上にどの論理ネットワークレベルを実現するか，およびどの論理ネットワークレベル上にどのユーザネットワークレベルを実現するのかの 2 点である．よって，2-3-4，2-2-4，3-3-3 の 3 つのアーキテクチャを調査すれば，代表的な組合せをひととおり調査することになる．

(1) **アーキテクチャ2-3-4**
アーキテクチャ2-3-4 は，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルそれぞれに，異なるレイヤのネットワーク技術を用いた方式である．物理ネットワークレベルを実現するレイヤ 2 のネットワークとして，たとえば，Ethernet や MPLS などの利用が考えられる．論理ネットワークレベルを実現するレイヤ 3 のネットワークとして，MPLS-VPN [12] などの利用が考えられる．

(2) **アーキテクチャ2-2-3**
アーキテクチャ2-2-3 は，物理ネットワークレベルおよび論理ネットワークレベルにレイヤ 2 のネットワーク技術を，ユーザネットワークレベルにレイヤ 3 のネットワーク技術を用いた方式である．物理ネットワークレベルを実現するレイヤ 2 のネットワークとして，たとえば，Ethernet や MPLS などの利用が考えられる．論理ネットワークレベルを実現するレイヤ 2 のネットワークとして，たとえば，IEEE 802.1Q VLAN [13] や L2TP などの利用が考えられる．

(3) **アーキテクチャ3-3-3**
アーキテクチャ3-3-3 は，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルそれぞれにレイヤ 3 のネットワーク技術を用いた方式である．物理ネットワークレベルを実現するレイヤ 3 の技術として，たとえば，IP などの利用が考えられる．論理ネットワークレベルを実現するレイヤ 3 の技術としては，トンネリングを利用したレイヤ 3 のネットワークとして，たとえば，IPSec などの利用が考えられる．

上記の 3 種類の MAVPN アーキテクチャについて，3 つのレベル（物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベル）と，OSI 参照モデルのレイヤとの関係を**図 3** に示す．

4.3 MAVPN アーキテクチャの評価項目

前述の 3 種類の MAVPN アーキテクチャについて，その長所および短所を評価するための評価項目について述べる．

サイバーソサイエティの形成といった用途を考慮すると，MAVPN は非常に大規模なネットワーク上で運用可能でなければならない．このため，MAVPN はノード数，VPN 数，エンティティ数に関して，高いスケーラビリティを持つことが望ましい．したがって，これらのスケーラビリティについて評価する必要がある．

また，近年インターネットで扱われるコンテンツのサイズが巨大化している．このため，MAVPN における通信速度は，高速であることが望ましい．したがって，通信速度について評価する必要がある．

さらに，MAVPN においては，利用者が様々な種類のネットワークサービスを利用できることが望ましい．したがって，利用可能なサービスの数について評価する必要がある．

4.4 スケーラビリティの評価

MAVPN アーキテクチャ2-3-4，2-2-3，3-3-3 の 3 種類のアーキテクチャを，ノード数，VPN 数，エンティティ数に関するスケーラビリティという観点で評価する．

具体的な評価では，代表的なネットワーク技術を用いて MAVPN を実現することを想定し，アーキテクチャ2-3-4 では，Ethernet，IPsec，HTTP によって，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルを実現するとする．アーキテクチャ2-2-3 では，Ethernet，IEEE 802.1q VLAN，IP アドレスのフィルタリングによって，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルを実現するとする．アーキテクチャ3-3-3 では，IP，IPsec，IP アドレスのフィルタリングによって，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルを実現するとする．

(1) **ノード数のスケーラビリティ**

ノード数に関するスケーラビリティは，物理ネットワークレベルにおけるノード数のスケーラビリティによって決定される（**表 2**）．たとえば，代表的なレイヤ 2 ネットワークである Ethernet では，テーブルに収容できる MAC アドレス数によってノード数のスケーラビリティが決定される．代表的なレイヤ 3 ネットワークである IP では，アドレス数によってノード数のスケーラビリティが決定される．ノード数に関するスケーラビリティに関しては，アーキテクチャ3-3-3 が優れていると考えられる．

(2) **VPN 数のスケーラビリティ**

VPN 数に関するスケーラビリティは，論理ネットワークレベルにおける VPN のスケーラビリティによって決定される（表 2）．たとえば，代表的なレイヤ 2 ネットワークである IEEE 802.1Q Tagging VLAN では，VLAN タグ数によって VPN 数に対するスケーラビリティが決定される．一方，代表的なレイヤ 3 ネットワークの IPsec VPN では，計算機が維持管理できる IPsec トンネル数でスケーラビリティが決定される．以上の考察により，VPN 数に関するスケーラビリティに関しては，アーキテクチャ2-2-3 が優れていると考えられる．

表 2 スケーラビリティの定量的評価
Table 2 Quantitative evaluation of scalability.

アーキテクチャ	ノード数に対するスケーラビリティ
2-3-4	約 130,000（高性能スイッチが，テーブルに収容可能な最大 MAC アドレス数[14]）
2-2-3	約 130,000（高性能スイッチが，テーブルに収容可能な最大 MAC アドレス数[14]）
3-3-3	2^{32}（IPv4 のアドレス数），2^{64}（IPv6 のアドレス数）
アーキテクチャ	VPN 数に対するスケーラビリティ
2-3-4	約 10,000/(VPN あたりの平均ノード数)（高性能ルータが維持可能な IPsec トンネル数[15),16)]）
2-2-3	4096^2（2 重スタック時のタグ数[17)]）
3-3-3	約 10,000/(VPN あたりの平均ノード数)（高性能ルータが維持可能な IPsec トンネル数[15),16)]）

(3) **エンティティ数のスケーラビリティ**

エンティティ数に関するスケーラビリティは，ユーザネットワークレベルのスケーラビリティによって決定される．

アーキテクチャ2-3-4 は，ユーザネットワークレベルにレイヤ 4 以上の情報を利用できるため，エンティティ数が物理ネットワークレベルもしくは論理ネットワークレベルにおける論理アドレス数などの制約を受けない．よって，エンティティ数に関しては，他の MAVPN アーキテクチャと比較して最も優れたスケーラビリティを実現できると考えられる．

アーキテクチャ2-2-3 および 3-3-3 は，エンティティ数がレイヤ 3 ネットワークにおける論理アドレス数などの制約を受ける．しかし，IPv6 を適用すれば，エンティティ数の制限は解消される．

4.5 通信速度の評価

通信速度は，物理ネットワークレベル，論理ネットワークレベル，ユーザネットワークレベルの各ネットワークレベルで行われる処理の複雑さに関係する．一般的に，ネットワークレイヤが高くなるほど行われる処理は複雑になり，扱う情報も増えるため，通信速度が低下すると考えられる．よって各ネットワークレベ

表 3 評価項目と各アーキテクチャの評価
Table 3 Evaluation criteria for MAVPN architectures.

評価項目		2-3-4	2-2-3	3-3-3
スケーラビリティ	ノード数	×	×	○
	VPN 数	×	○	×
	エンティティ数	○	△	△
通信速度		×	○	△
利用可能なサービス数		×	○	○
総合評価		×	○	△

○：優れている △：多少問題がある ×：問題がある

ルを実現するネットワーク階層が低いほど通信速度は優れていると考えられる．

4.6 利用可能なサービス数の評価

利用可能なサービスの数は，利用者が利用可能なプロトコルの種類に依存するため，ユーザネットワークレベルを実現するネットワーク技術を考える必要がある．

アーキテクチャ2-3-4 は，ユーザネットワークレベルにおいてレイヤ 4 の情報を取り扱うため，ユーザネットワークレベルにおいてレイヤ 3 の情報を取り扱う他の MAVPN アーキテクチャよりも，利用者が利用可能なプロトコルの数が少ない．このため，利用者が利用可能なサービスの数は他の MAVPN アーキテクチャよりも劣っていると考えられる．

4.7 総 合 評 価

以上の評価結果の一覧を**表 3** に示す．3 章で述べたように，MAVPN ではノード数および VPN 数に関するスケーラビリティを実現することが特に重要である．近年，レイヤ 2 のスケーラビリティを向上させる広域イーサネット技術[17),18)] が登場しており，アーキテクチャ2-2-3 のノード数のスケーラビリティの問題は容易に解決できると考えられる．このため，アーキテクチャ2-2-3 が最も優れていると判断した．今回評価した項目に関しては，このように，アーキテクチャ2-3-4，2-2-3，3-3-3 のうち，アーキテクチャ2-2-3 が総合的に最も優れているという結果になった．次章では，アーキテクチャ2-2-3 に基づいてプロトタイプを実装した結果を示す．

5. MAVPN プロトタイプシステムの実装と評価

5.1 MAVPN のサービス利用手順

利用者の視点から見た MAVPN のサービス利用手順は以下のようなものになる．

(1) 利用者は端末を手元のネットワーク機器に接続する．
(2) 端末上で MAVPN 端末ソフトウェアを起動する．
(3) 端末ソフトウェアに表示される，帰属が許可されている VPN の名前リストから，接続する VPN を複数選択する（もしくは端末ソフトウェアを起動すると，あらかじめ定めておいた複数の VPN に自動的に接続される）．
(4) 通信相手の端末名を指定して通信を行う．
(5) 端末ソフトウェアから，切断する VPN を選択して切断する（もしくは端末ソフトウェアを終了するとすべての VPN から切断される）．

このように，利用者は，端末をネットワークに接続し，端末ソフトウェアを起動して利用者 ID とパスワードを入力するだけで複数の VPN に接続されることが望ましい．また，端末ソフトウェアに表示される VPN のリストから，接続や切断を行う VPN を随時指定できることが望ましい．

5.2 実装の目標

5.1 節で述べたようなサービスの実現性を示すことを目標として，プロトタイプを実装する．具体的には，以下の要求を満たすことを目標とする．

(1) 利用者が複数の VPN を意識せず同時に利用できる．
(2) VPN を論理的な名前で指定できる．
(3) 利用者端末のアドレスが自動的に設定される．
(4) 利用者単位で VPN へのアクセス制御が可能である．

本プロトタイプでは，4.7 節の結果から，基盤となるネットワークをレイヤ 2 技術で実現し，その上に VPN をレイヤ 2 技術で実現し，利用者の複数 VPN へのアクセスをレイヤ 3 技術を用いて制御するというアーキテクチャを採用する．具体的には，基盤となるネットワークを Ethernet で，VPN を IEEE 802.1Q VLAN[13)] で，利用者の VPN へのアクセスを IP を利用して制御する．

本プロトタイプは，認証 VLAN と呼ばれる既存技術を参考に実装を行う．認証 VLAN は既存の VLAN に認証機能を追加し，利用者単位のアクセス制御を実現するものである．本プロトタイプは，利用者が複数の VLAN を同時に利用できる認証 VLAN を目標とする．また，認証 VLAN と同程度のセキュリティ水準を実現することを目標とする．具体的には，同一のサイト（LAN）に接続されている端末どうしは信頼しあうという前提を置く．このため，同一サイト内の端末による盗聴は想定外とする．また，MAC アドレス詐称も想定外とする．

なお，MAVPN プロトタイプシステムは，4 章で説明したアーキテクチャ2-2-3 を採用しているため，4 章

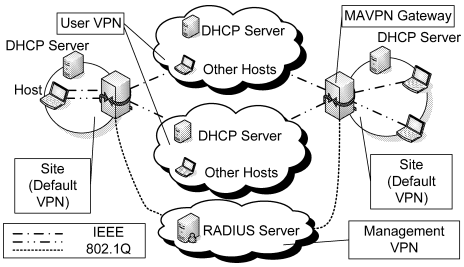

図 4 プロトタイプの論理的なネットワーク構成
Fig. 4 Logical network structure of our prototype system.

の評価項目は，ノード数に対するスケーラビリティ以外を満たす．1 章で述べたように，MAVPN は，単一のサービスプロバイダによって提供される，PP-VPN フレームワークを前提としており，収容されるノードの数はそれほど多くはならないと考えられる．さらに，近年さかんに研究されている，イーサネットのスケーラビリティを向上させる広域イーサネット技術[17),18)]を用いることにより，ノード数に対するスケーラビリティを満たすことが可能であると考えられる．

5.3 プロトタイプの実装

(1) ネットワーク構成

プロトタイプの論理的なネットワークは**図 4** のように構成する．

利用者に提供する VPN（図 4 の User 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 Ethernet を仮想的に分割する技術である．本プロトタイプでは，実装を簡単にするために，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 IP アドレス空間は重複しないものとする．

端末は MAVPN ゲートウェイ（図 4 の 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 で多重化し，MAVPN ゲートウェイがこのアクセス回線を IEEE 802.1Q VLAN による VPN へブリッジする．これにより端末は複数のレイヤ 2 VPN を利用できる．また，MAVPN ゲートウェイは利用者の認証機能を持ち，VPN 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 VPN に接続する．端末がどの VPN にも帰属していない初期状態では，サイト（図 4 の Site）内でのみ通信可能とする．このため，サイトを初期 VPN（図 4 の Default VPN）と呼ぶ．利用者の端末が用いる IP アドレスは，各 VLAN 内に設置された DHCP サーバにより，VLAN の IP アドレス空間から割り当てられる．ただし，サーバなどの IP アドレスは，各 VLAN の IP アドレス空間から静的に割り当てる．

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（図 4 の 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 VPN（図 4 の Management VPN）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 VPN の名前，パスワードの 3 つからなる．すなわち，利用者は，帰属が許可された VPN の数だけアカウントを持つ．

(2) 通信方式

次に，本プロトタイプにおける通信の方式について説明する．端末は，最初にサイトに接続されたときに，初期 VPN 用のインタフェースを作成し，サイト内の DHCP サーバから初期 VPN 用の IP アドレスを取得する．その後，端末ソフトウェアが MAVPN ゲートウェイと通信することで，VPN への帰属および離脱を実現する．

(3) 端末ソフトウェア

端末は VLAN に帰属するために，MAVPN ゲートウェイに対して帰属の認証要求を行わなければならない．認証は，VPN に新たに帰属するとき，および帰属している VPN から離脱するときに実行される．

このため，認証要求を行う端末ソフトウェアが必要である．端末ソフトウェアの機能は以下の 3 つである．

- MAVPN ゲートウェイに対して，利用者の ID，帰属する VPN の名前，パスワードを送信する．
- VPN への帰属が完了したら VPN アクセスのための IEEE 802.1Q インタフェースを作成し，DHCP 要求を出す．
- VPN から離脱したら，VPN アクセスのための IEEE 802.1Q インタフェースを削除する．

(4) MAVPN ゲートウェイ

MAVPN ゲートウェイは，利用者認証によって端末の VLAN への接続制御を行う．MAVPN ゲートウェイの主な機能は，以下の 2 つである．

- 利用者からの接続要求を受けて利用者認証を行う．
- 認証の結果に応じて端末の接続制御を行う．

5.4 設計目標の実現

以上のように端末と MAVPN ゲートウェイの実装を行い，動作確認を行った．

実装目標 (1)〜(4) が実現できていることを確認するためには，プロトタイプシステムが次の各項目を満たすことを確認すればよい．

(1) 利用者が複数の VPN を意識せず同時に利用でき

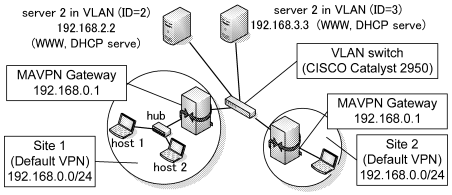

図 5 動作確認用ネットワークの物理的な構成
Fig. 5 Physical network structure for evaluations.

るかどうか
利用者が通信を行う際に通信相手先の VPN を指定しないこと．VPN を指定しないで利用者が送信したパケットに対し，その宛先の VPN に応じて自動的に適切な VLAN タグが付与されていること．

(2) VPN を論理的な名前で指定できるかどうか
VPN の論理的な名前（とパスワード）を指定するだけで，利用者が VPN に帰属できること．

(3) 利用者端末のアドレスが自動的に設定されるかどうか
VPN へ帰属すると，VPN へのアクセスに使用する IP アドレスが，利用者端末の IEEE 802.1 q インタフェースに自動的に割り振られること．

(4) 利用者単位で VPN へのアクセス制御ができるかどうか
同一サイト内の利用者が，異なる VPN に帰属できること．さらに，利用者/端末は，帰属している VPN のみと通信可能なこと．

動作確認用ネットワークの物理的な構成は，**図 5** のとおりである．

プロトタイプのネットワーク中には 2 つのサイトが存在する．サイト 1 は MAVPN ゲートウェイ 1，端末 1 と端末 2 で構成されている．サイト 2 は MAVPN ゲートウェイ 2 と端末 3 で構成されている．VPN は IEEE 802.1Q VLAN で構成される．サーバ 1 は vpn2 という名前の VPN（VLAN ID は 2）に，サーバ 2 が vpn3 という名前の VPN（VLAN ID は 3）につねに帰属している．各 VPN のネットワークアドレスは重複しないものとし，vpn2 のネットワークアドレスを 192.168.2.0 とし，vpn3 のネットワークアドレスを 192.168.3.0 とする．また，サーバ 1 とサーバ 2 上には，ともに DHCP サーバと WWW サーバが動作している．

このようなネットワーク構成で，端末 1，端末 2 および端末 3 を利用する利用者のアカウント情報を**表 4** のように規定した．ここでは，user1 が端末 1 を，user2 が端末 2 を，user3 が端末 3 を利用するものとする．

表 4 プロトタイプの動作確認に用いるアカウント情報
Table 4 Account data of prototype system.

利用者 ID	帰属が許可された VPN	パスワード
user1	vpn2	xxx
user1	vpn3	xxx
user2	vpn3	yyy
user2	vpn4	yyy
user3	vpn4	zzz

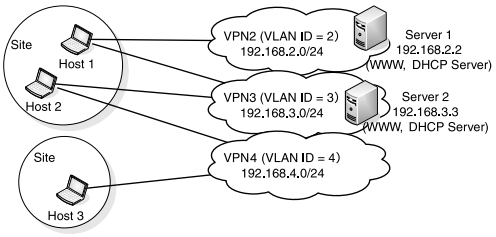

図 6 動作確認用ネットワークの論理的な構成
Fig. 6 Logical network structure for evaluations.

図 7 端末の画面
Fig. 7 GUI of a host.

表 4 のようなアカウント情報に基づき，各端末がそれぞれ許可された VPN に多重帰属すると，論理的なネットワーク構成は**図 6** のようになる．

このネットワークで，実装の目標 (1) から (4) を満たしていることを確認した．

最初に，利用者が複数の VPN を意識せず同時に利用できる（実装の目標 (1)），VPN を論理的な名前で指定できる（実装の目標 (2)），利用者端末のアドレスが自動的に設定される（実装の目標 (3)）を確認する．**図 7** に示すような端末画面により，端末 1 から user1 が端末ソフトウェアを用いて，VPN の名前とパスワードを入力し，vpn2 と vpn3 に多重帰属すると，vpn2 と vpn3 用のアドレスが割り当てられ，user1 の端末の静的ルーティングテーブルは**表 5** のようになった．このことより，VPN の名前を指定するだけで VPN へ

表 5 多重帰属時の端末 1 の静的ルーティングテーブル
Table 5 Static routing table of Host 1 associated multi VPNs.

Destination	Gateway	Genmask	Iface
192.168.3.0	*	255.255.255.0	eth0.3
192.168.2.0	*	255.255.255.0	eth0.2
192.168.0.0	*	255.255.255.0	eth0
default	192.168.3.1	0.0.0.0	eth0.3
default	192.168.2.1	0.0.0.0	eth0.2

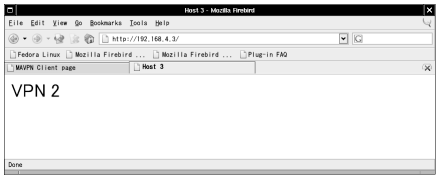

図 8 端末 1 から vpn2 へのアクセス
Fig. 8 Access from Host 1 to vpn2.

帰属できている．すなわち実装の目標 (2) が実現されていることがいえる．この表では，192.168.3.0/24 宛てのパケットは，利用者が意識することなく自動的に eth0.3 に出される．eth0.3 は VLAN ID 3 の IEEE 802.1Q インタフェースであり，すなわち vpn3 に通じる．同様に，192.168.2.0/24 宛てのパケットは eth0.2，すなわち vpn2 に出される．この状態で，Host 1 から Server 1，Server 2 に ping や ssh，http によるアクセスが可能であることを確認した．**図 8** は Host 1 から vpn2 の Server 1 に http でアクセスした様子である．このように，同一のブラウザで複数の VPN に http アクセスが可能であることを確認した．これらのことから，利用者が VPN を指定せずに送信したパケットに対して，自動的にその宛先の VPN に応じて自動的に適切な VLAN タグと IP アドレスが付与されている．すなわち実装の目標 (1) と (3) が実現されていることがいえる．

利用者単位で VPN へのアクセス制御が可能である（実装の目標 (4)）を確認する．

そのため，まず，同一サイト内の各端末がそれぞれ別の VPN に帰属できることを確認する．端末 1 から user1 が vpn2 のみに，端末 2 から user2 が vpn3 のみにそれぞれ帰属した状態で通信を行った．このとき，端末 1 は vpn2 と，端末 3 は vpn3 とそれぞれ通信が可能であることを確認した．また，端末 1 が vpn3 と，端末 2 が vpn2 と通信できないことも確認した．よって端末 1 と端末 2 はそれぞれ別の VPN に帰属していることが分かる．

次に，端末単位の VPN を動的に構築できることを確認する．端末 2 上の user2 と，端末 3 上の user3 がともに vpn4 に帰属した状態で通信を行った．vpn4 には DHCP サーバが存在しないため，vpn4 のネットワークアドレスを 192.168.4.0/24 と定め，端末 2 と端末 3 にはアドレスを手動で設定した．このとき，端末 2 から端末 3 へアクセスが可能であった．

最後に，認証されていない利用者端末からのフレームがフィルタリングされることを確認する．具体的には，端末 1 上の user1 が vpn2（VLAN ID が 2）に帰属している状態で，端末 2 上の user2 が認証を行わずに，不正に VLAN ID 2 の IEEE 802.1Q インタフェースを作成した．このとき，端末 2 は vpn2 と通信できないことが確認された．これらのことから，同一サイト内の各利用者は，異なる VPN に帰属できており，かつ帰属している VPN のみと通信可能である．すなわち実装目標 (4) が実現されていることがいえる．

6. おわりに

本稿では，サイバーソサイエティの実現に向けた，利用者の多重帰属を実現する階層型の MAVPN アーキテクチャを提案し，その評価を行った．さらに，MAVPN のプロトタイプ実装を行った．既存のネットワーク技術を用いたプロトタイプ実装により，我々の提案する，利用者の多重帰属を実現する VPN の実現可能性を示した．具体的には，VLAN で実現した複数の VPN に対して，端末が多重帰属できるようなプロトタイプを作成した．このプロトタイプで，端末が端末単位に複数の VPN を透過的に利用できることを確認した．また，認証によって端末単位のアクセス制御が可能であることを確認した．

今後の課題としては，プロトタイプのセキュリティレベル，およびスケーラビリティをさらに向上させることがあげられる．また，VPN 間でアドレス空間が重複することを許容するプロトタイプや，利用者の VPN からの離脱方法を改良したプロトタイプの作成があげられる．さらに，これらの作成したプロトタイプが，VPN 数や帯域幅に対してどの程度のスケーラビリティを持つかを評価することがあげられる．

参考文献

1) Vaughan-Nichols, S.J.: Web Services: Beyond the Hype, *IEEE Computer*, Vol.35, No.2, pp.18–21 (2002).
2) 大山永昭：電子政府の現状と課題，情報処理，Vol.44, No.5, pp.455–460 (2003).
3) 総務省：平成 16 年通信利用動向調査報告書 (2004). 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 (2002). http://www.soumu.go.jp/s-news/2002/020705_4.html
5) Nagarajan, A.: Generic Requirement for Provider Provisioned Virtual Private Networks (PPVPN), Request for Comments (RFC) 3809 (2004).
6) Carugi, M. and McDysan, D.: Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs), Request for Comments (RFC) 4031 (2005).
7) 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，電子情報通信学会技術研究報告 IN2000-101, Vol.100, pp.39–46 (2000).
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，電子情報通信学会技術研究報告 SSE99-171, Vol.99, pp.61–66 (2000).
9) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, Request for Comments (RFC) 2401 (1998).
10) Rosen, E., Viswanathan, A. and Callon, R.: Multiprotocol Label Switching Architecture, Request for Comments (RFC) 3031 (2001).
11) Townsley, W., et al.: Layer Two Tunneling Protocol L2TP, Request for Comments (RFC) 2661 (1999).
12) Rosen, E. and Rekhter, Y.: BGP/MPLS VPNs, Request for Comments (RFC) 2547 (1999).
13) IEEE standards for local and metropolitan area networks: Virtual Bridged Local Area Networks, IEEE Standard 802.1Q-1998 (1998).
14) Alcatel Japan: OmniSwitch 7800. http://www.hucom.co.jp/product/auth/pic/Omni77007800.pdf
15) Juniper Networks: NetScreen-ISG2000. http://www.juniper.co.jp/products/integrated/dsheet/110011.pdf
16) Nortel: VPN Router 5000. http://www.nortel.com/products/01/contivity/collateral/vpn_router.pdf
17) Chiruvolu, G., Ge, A., Elie-Dit-Cosaque, D., Ali, M. and Rouyer, J.: Issues and Approaches on Extending Ethernet Beyond LANs, *IEEE Communications Magazine*, pp.80–86 (2004).
18) Seaman, M.: Large Scale Q-in-Q Scalable Address Learning (2003). http://www.ieee802.org/1/files/public/docs2003/ScalableQinQLearning.pdf

(平成 17 年 7 月 4 日受付)
(平成 18 年 4 月 4 日採録)

本田 治（正会員）

平成 10 年大阪大学基礎工学部情報工学科退学．平成 12 年同大学大学院博士前期課程修了．平成 17 年同大学院博士後期課程退学．現在，同大学院情報科学研究科助手．分散システム，大規模ネットワーク，トラヒック制御等に関する研究に従事．博士（工学）．電子情報通信学会会員．

原 義博

平成 16 年大阪大学大学院情報科学研究科博士前期課程修了．同年大日本印刷株式会社入社．現在，RFID や携帯電話を活用したシステムの開発に従事．

大崎 博之

平成 7 年大阪大学大学院基礎工学研究科物理系専攻博士前期課程修了．同年日本学術振興会特別研究員．平成 9 年大阪大学大学院基礎工学研究科物理系専攻博士後期課程修了．同年同大学院基礎工学研究科情報数理系助手．平成 11 年同大学情報処理教育センター助手．平成 12 年同大学サイバーメディアセンター助手．平成 14 年同大学大学院情報科学研究科情報ネットワーク学専攻助教授．工学博士．この間，高速ネットワークにおけるトラヒック制御等の研究に従事．IEEE，電子情報通信学会各会員．

今瀬 真（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 52 年同大学大学院修士課程修了．同年日本電信電話公社武蔵野研究所入所．NTT マルチメディアネットワーク研究部長等を歴任．平成 14 年 4 月大阪大学大学院情報ネットワーク学専攻教授．現在，同職．ネットワーク理論，分散アルゴリズム，情報ネットワーク等の研究，開発に従事．工学博士．応用数理学会会員．

丸吉　政博

平成 12 年名古屋大学工学部情報工学科卒業．平成 14 年同大学大学院情報工学専攻修士課程修了．同年日本電信電話株式会社に入社．NTT 情報流通プラットフォーム研究所勤務．IP-VPN，ホームゲートウェイ，広域イーサネットサービスの研究開発に従事．現在，NTT アクセスサービスシステム研究所．

松田　和浩

昭和 58 年北海道大学工学部電子工学科卒業．昭和 60 年同大学大学院電子工学専攻修士課程修了．同年 NTT に入社．以来，LSI CAD システム，プロトコル処理用 LSI，コンテンツ・デリバリ・ネットワークの研究開発に従事．現在，フォトニックネットワーク制御方式の研究開発に従事．NTT 未来ねっと研究所主幹研究員．電気学会，IEEE 各会員．