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 に多重帰属できる階層化 VPN アーキテクチャ

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

† 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}@lab.ntt.co.jp

あらまし　我々はこれまで，利用者が，複数の VPN に対して同時に接続（多重帰属）できる，新しい VPN アーキテクチャの提案を行った [1]．既存の VPN 技術では，利用者が単一の VPN に接続することを前提としている．しかし，利用者が複数の VPN に多重帰属できる VPN サービスを実現するためには，利用者の要求に応じて VPN への接続状態を動的に変更する機能，利用者ごとに VPN への接続の可否を判断する機能など，さまざまな機能が必要となる．本稿では，利用者が複数の VPN に多重帰属できる VPN アーキテクチャを，3 種類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）によって階層的に構成する方法を提案する．まず，これらそれぞれのネットワークレベルに要求される機能を整理する．さらに，これら 3 種類のネットワークレベルを，レイヤ 2，レイヤ 3 またはレイヤ 4 のネットワーク技術で実現した場合の利点および欠点を評価するために必要となる，スケーラビリティ，通信速度など，さまざまな評価項目について議論する．
キーワード　VPN，多重帰属，階層化 VPN アーキテクチャ，スケーラビリティ，通信速度

On Layered VPN architecture for Enabling User-Based Multiply Associated VPNs

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

† 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}@lab.ntt.co.jp

Abstract　In our previous work, we have proposed a new VPN architecture for enabling user-based multiply associated VPNs. Almost all existing VPN technologies assume that users never simultaneously access more than a single VPN. Thus, for realizing a new VPN service allowing users to simultaneously join multiple VPNs, several fundamental mechanisms, such as dynamically changing user's VPN association status according to the user's request and authorizing user's access to a group of VPNs, are required. In this paper, we propose a layered VPN architecture for realizing user-based multiply associated VPN. Our layered VPN architecture consists of three network levels such as PNL (Physical Network Level), LNL (Logical Network Level), and UNL (User Network Level). First, we discuss and classify functions required for each network level. We then present several approaches for implementing each network level using existing layer 2, 3, and 4 networking technologies, and quantitatively evaluate their advantages and disadvantages from several viewpoints including scalability and transmission speed.
Key words　VPN, Multiple Association, Layered VPN Architecture, Scalability, Transmission Speed

1. はじめに

近年のネットワーク技術の発展に伴い，購買や流通，行政機能，労働など，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ている．これによって，近い将来，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エティと称している．サイバーソサエティにおける「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．我々は，仮想組織を VPN (Virtual Private Network) を用いて実現することを想定している．

既存の VPN 技術としては，PPVPN (Provider Provisioned VPN) [2] ~ [4] やエクストラネット [5], [6] などがある．しかし，PPVPN は顧客の LAN であるサイト間で VPN を構築することを前提としたものである．また，エクストラネットはホストが多数の VPN にアクセスすると，転送性能が劣化し，また管理が困難になる．そのため，既存の VPN 技術では，利用者が，利用者単位で多数の VPN に同時に多重帰属することができない．

そこで，我々は，利用者が，多数の VPN に対して同時に多重帰属できる，新しい VPN アーキテクチャの検討を行っている [1] .我々は ,このような新しい VPN を ,MAVPN (Multiply-Asocciated VPN) と呼んでいる．本稿の目的は，以下の 2 つである．まず，MAVPN のアーキテクチャを階層的に構成することにより，既存の技術を階層的に組み合せて，比較的容易に MAVPN を実装できることを示すことである．つぎに，MAVPN を，レイヤ 2，レイヤ 3，もしくはレイヤ 4 のネットワーク技術を階層的に組み合せて実現した場合の利点および欠点を，さまざまな評価項目について評価することである．

2. 階層化 MAVPN アーキテクチャ

本章では，我々が提案する階層化 MAVPN アーキテクチャを説明する．既存の PPVPN は，サイト間を VPN トンネルで接続するという性質上，利用者ごとに任意の VPN に接続することができない．また，既存のエクストラネット技術では多数の VPN に同時に接続することができない．このような問題を解決するために，我々は MAVPN アーキテクチャを提案してきた．

MAVPN を実現するには，大きくわけて，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，比較的容易に実装することができる考えられる．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．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を表 1 に示す．

まず，物理ネットワークレベルについて述べる．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レベルである．図 1 は物理ネットワークを模式的に表した図である．図 1 のように，ルータ，スイッチ，ホストなどのノードが，リンクによって接続される．

次に，論理ネットワークレベルについて述べる．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．PPVPN においては，VPN の構成員はサイトである．しかし，MAVPN における論理ネットワークレベルでは，VPN の構成員として，ホスト上のエンティティという概念を導入する．これは，ホスト上の利用者や，利用者が使用するアプリケーション，サーバプログラムなどを想定している．本稿では，マルチユーザ OS の利用や，ASP （Application Service Provider) による顧客の VPN へのサーバ提供を考え，エンティティを定義する．図 2 は論理ネットワークを模式的に表した図である．図 2 のように，エンティティ単位の認証により，エンティティ単位の VPN を構築する．

最後に，ユーザネットワークレベルについて述べる．ユーザネットワークレベルでは，エンティティが複数の VPN に同時に接続 (多重帰属) する際の，エンティティから各 VPN へのアクセス制御を行う．より具体的には，エンティティが，意識することなく複数の VPN を使い分けることができような機能，

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	ホスト上で動作する，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

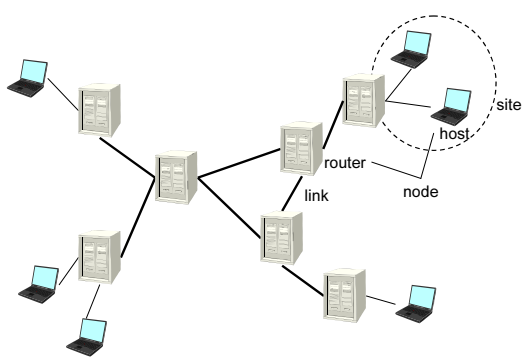

図 1　MAVPN アーキテクチャにおける物理ネットワーク
Fig. 1　Physical network level in MAVPN architecture

エンティティが多重帰属している複数の VPN 間が不正に接続されないように制御する機能を提供する．図 3 はユーザネットワークを模式的に表した図である．

3. 3 種類の代表的な MAVPN アーキテクチャ

現在，広域ネットワーク接続サービスではレイヤ 2 およびレイヤ 3 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を レイヤ 2 もしくはレイヤ 3 ネットワークで実現することを考える．また，ユーザネットワークレベルを，レイヤ 3 もしくはレイヤ 4 の情報を用いて実現する場合を考える．このような理由で，階層化された 3 つのネットワークレベルで構成される MAVPN アーキテクチャのうち，本稿では以下の 3 種類のアーキテクチャを取り上げる．

3.1 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．アーキテクチャ 2-3-4 の構成は次のようになる．

まず，物理ネットワークレベルをレイヤ 2 ネットワークにより実現する．レイヤ 2 のネットワークとして，例えば，Ethernet や MPLS [7] などの利用が考えられる．

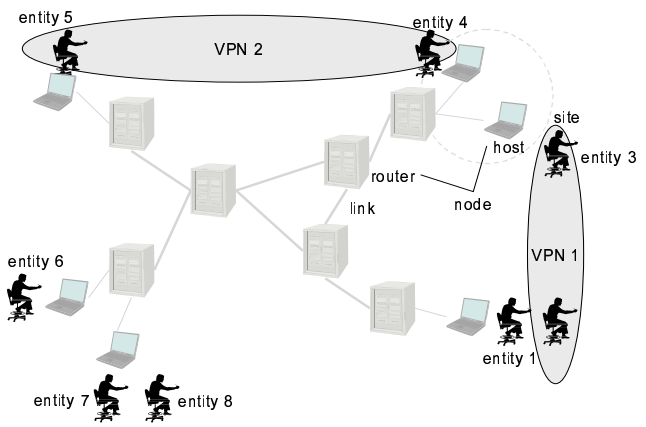

図 2　MAVPN アーキテクチャにおける論理ネットワーク
Fig. 2　Logical network level in MAVPN architecture

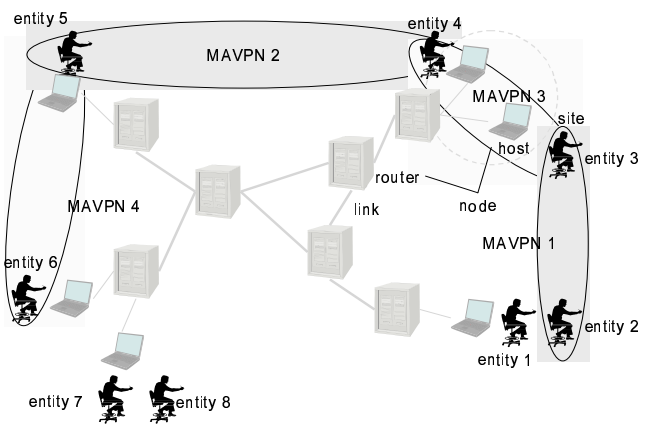

図 3　MAVPN アーキテクチャにおけるユーザネットワーク
Fig. 3　User network level in MAVPN architecture

次に，論理ネットワークレベルをレイヤ 3 ネットワークにより実現する．レイヤ 3 のネットワークとして，MPLS-VPN [8] などの利用が考えられる．

そして，ユーザネットワークレベルをレイヤ 4 以上の情報を利用して実現する．具体的な実現方法として，論理ネットワークレベルを転送されるパケットに含まれる レイヤ 4 以上の情報を利用して，エンティティからのパケットを，エンティティが多重帰属している VPN に対して配送する方法などが考えられる．

3.2 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．アーキテクチャ 2-2-3 の構成は次のようになる．

まず，物理ネットワークレベルをレイヤ 2 ネットワークにより実現する．レイヤ 2 のネットワークとして，例えば，Ethernet や MPLS などの利用が考えられる．

次に，論理ネットワークレベルをレイヤ 2 ネットワークにより実現する．レイヤ 2 のネットワークとして，例えば，IEEE 802.1Q VLAN [9] や L2TP [10] などの利用が考えられる．

そして，ユーザネットワークレベルをレイヤ 3 の情報を用いて実現する． 具体的な実現方法として，論理ネットワークレベルを転送されるパケットに含まれるレイヤ 3 情報を利用して，エンティティからのパケットを，エンティティが多重帰属している VPN に対して配送する方法などが考えられる．

3.3 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．アーキテクチャ 3-3-3 の構成は次のようになる．

まず，物理ネットワークレベルをレイヤ 3 ネットワークにより実現する．レイヤ 3 のネットワークとして，例えば，IP などの利用が考えられる．

論理ネットワークレベルをトンネリングを利用したレイヤ 3 ネットワークにより実現する．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，例えば，IPSec [11] などの利用が考えられる．

ユーザネットワークレベルをレイヤ 3 の情報を用いて実現する． 具体的な実現方法として，論理ネットワークレベルを転送されるパケットに含まれる レイヤ 3 情報を利用して，エンティティからのパケットを，エンティティが多重帰属している VPN に対して配送する方法などが考えられる．

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 4 に示す．

4. MAVPN アーキテクチャの評価項目

本稿では，3. 章で述べた 3 種類の MAVPN アーキテクチャ

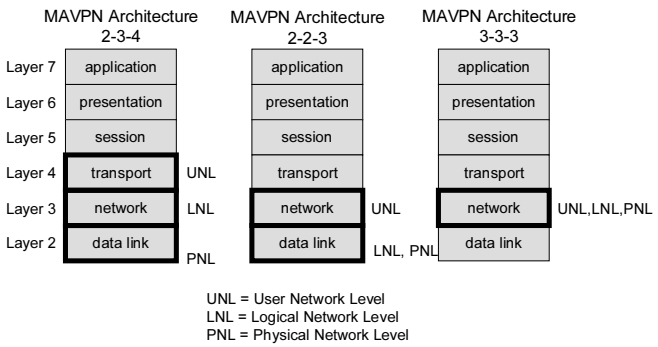

図 4　3 種類の代表的な MAVPN アーキテクチャ
Fig. 4　Three typical MAVPN architectures

について，その利点および欠点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．従って，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．従って，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．従って，利用可能なサービスの数について評価する必要がある．

最後に，MAVPN においては，エンティティの VPN への接続の状態や，VPN の構成を管理し，利用者の要求によって変更できることが望ましい．このため，エンティティや VPN 管理の容易さについて評価する必要がある．

5. MAVPN の評価

5.1 スケーラビリティ (ノード数，**VPN** 数，エンティティ数)

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．

5.1.1 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．以下，それぞれの MAVPN アーキテクチャについて議論する．

- アーキテクチャ 2-3-4

  物理ネットワークレベルがレイヤ 2 ネットワークによって実現されている．このため，ノード数に関するスケーラビリティという点では，物理ネットワークレベルにレイヤ 3 ネットワークを用いているアーキテクチャ 3-3-3 よりも劣っていると考えられる．例えば，代表的なレイヤ 2 ネットワークである Ethernet では，代表的なレイヤ 3 ネットワークである IP よりもノード数に関するスケーラビリティで劣る．

- アーキテクチャ 2-2-3

  物理ネットワークレベルがレイヤ 2 ネットワークによって実現されている．このため，アーキテクチャ 3-3-3 と比較して，ノード数に関するスケーラビリティは劣っていると考えられる．一方，物理ネットワークレベルとして同じレイヤ 2 ネットワークを用いるアーキテクチャ2-3-4 とは同程度のスケーラビリティを有していると考えられる．

- アーキテクチャ 3-3-3

  物理ネットワークレベルがレイヤ 3 ネットワークによって実現されている．このため，アーキテクチャ 2-3-4 と比較して，ノード数に関するスケーラビリティは優れていると考えられる．

以上の考察により，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．

5.1.2 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．以下，それぞれの MAVPN アーキテクチャについて議論する．

- アーキテクチャ 2-3-4

  論理ネットワークレベルにおいて，VPN 数に関してどの程度のスケーラビリティを実現できるかは，論理ネットワークレベルにどのようなレイヤ 3 ネットワークを用いるかによって決まる．例えば，MPLS VPN を用いる場合，MPLS のラベルをスタックすることによって高い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

  論理ネットワークレベルにおいて，VPN 数に関してどの程度のスケーラビリティを実現できるかは，論理ネットワークレベルにどのようなレイヤ 2 ネットワークを用いるかによって決まる．例えば，IEEE 802.1Q Tagging VLAN を用いる場合，タグをスタックすることによって高いスケーラビリティを得ることができる．

- アーキテクチャ 3-3-3

  論理ネットワークレベルにおいて，VPN 数に関してどの程度のスケーラビリティを実現できるかは，論理ネットワークレベルにどのようなレイヤ 3 ネットワークを用いるかによって決まる．例えば，現在，一般的なトンネリング技術である IPSec を用いる場合，VPN に接続しているエンティティ間でメッシュ状にトンネルを生成する必要があるため，トンネル数の制約によって VPN 数に関するスケーラビリティが制限

されると考えられる．例えば，IPSec の最大トンネル数 (SA の数) はノードに搭載されているメモリ量等の制約を受ける．

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2-3-4 およびアーキテクチャ 2-2-3 が優れていると考えられる．

5.1.3 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．以下，それぞれの MAVPN アーキテクチャについて議論する．

- アーキテクチャ 2-3-4

  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 以上の情報を用いる．この場合，エンティティの識別にレイヤ 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等の制約を受けない．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

  アーキテクチャ 2-2-3 は，ユーザネットワークレベルにレイヤ 3 の情報を用いているため，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等の制約を受ける．例えば，代表的なレイヤ 3 ネットワークである IPv4 を用いる場合，エンティティ数の上限は IP アドレス数の上限 (2^{32}) によって制限される．しかし，IPv6 が利用されつつあるため，エンティティ数の制限は解消される．このため，近い将来，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3-3-3

  アーキテクチャ3-3-3 は，アーキテクチャ2-2-3 と同様に，ユーザネットワークレベルにレイヤ 3 の情報を用いているため，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等の制約を受ける．しかし，アーキテクチャ 2-2-3 の場合と同様に，今後エンティティ数の制限は解消される．このため，近い将来，優れたスケーラビリティを実現できると考えられる．

以上の考察により，エンティティ数に関するスケーラビリティに関しては，今後はどのアーキテクチャにおいても優れたスケーラビリティを得ることができると考えられる．

5.2 通 信 速 度

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，通信速度という観点で評価する．通信速度のスケーラビリティに関しては，最も複雑な処理が行われる，ユーザネットワークレベルにおける通信速度を考える必要がある．以下，それぞれのアーキテクチャについて議論する．

- アーキテクチャ 2-3-4

  ユーザネットワークレベルにおいて，レイヤ 4 以上の情報を取り扱う必要がある．このため，一般に他の 2 つのアーキテクチャよりも，ユーザネットワークレベルの動作が低速となることが予想される．よって，他の 2 つのアーキテクチャよりも通信速度が劣っていると予想される．

- アーキテクチャ 2-2-3

  ユーザネットワークレベルにおいて，レイヤ 3 の情報を取り扱う必要がある．このため，ユーザネットワークレベルにおいてレイヤ 4 の情報を取り扱うアーキテクチャ 2-3-4 よりも，一般にユーザネットワークレベルの動作が高速となることが予想される．よって，アーキテクチャ2-3-4 よりも通信速度が優れていると考えられる．

- アーキテクチャ 3-3-3

  ユーザネットワークレベルにおいて，レイヤ 3 の情報を取り扱う必要がある．このため，アーキテクチャ 2-3-4 と比較して，通信速度が優れていると考えられる．一方，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 2-2-3 とは同程度の通信速度を有していると考えられる．

以上の考察により，回線速度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 および 3-3-3 が優れていると考えられる．

5.2.1 利用可能なサービスの数

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，利用可能なサービスの数という観点で評価する．利用者が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．以下，それぞれのアーキテクチャについて評価する．

- アーキテクチャ 2-3-4

  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．

- アーキテクチャ 2-2-3

  ユーザネットワークレベルにおいてレイヤ 3 の情報を取り扱うため，ユーザネットワークレベルにおいてレイヤ 4 の情報を取り扱うアーキテクチャ 2-3-4 よりも，利用者が利用可能なプロトコルの数が多い．この

ため，利用者が利用可能なサービスの数はアーキテクチャ 2-3-4 よりも優れていると考えられる．

- アーキテクチャ 3-3-3

  ユーザネットワークレベルにおいてレイヤ 3 の情報を取り扱うため，ユーザネットワークレベルにおいてレイヤ 4 の情報を取り扱うアーキテクチャ 2-3-4 よりも，利用者が利用可能なサービスの数が優れていると考えられる．また，アーキテクチャ 3-3-3 は利用するトンネリング技術によって，利用者が利用可能なサービスが制限される．例えば，現在，一般的なトンネリング技術である IPSec を用いる場合，利用者が利用可能なサービスの数は制限される．このため，ユーザネットワークレベルにおいてレイヤ 3 の情報を取り扱うアーキテクチャ2-2-3 よりも，利用者が利用可能なサービスの数は劣っていると考えられる．

以上の考察により，利用者が利用可能なサービスの数は，アーキテクチャ 2-2-3，3-3-3，2-3-4 の順に優れていると考えれられる．

5.3 VPN の管理

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の，管理の容易さという観点での評価は，今後の課題とする．

5.4 総 合 評 価

以上の評価結果の一覧を表 2 に示す．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．よって今後，我々はアーキテクチャ 2-2-3 に注目し，プロトタイプ作成などを行う予定である．

表 2　評価項目と各アーキテクチャの評価
Table 2　Evaluation of each architecture

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		×	○	○
多様なサービス (通信方式)		×	○	△
総合評価		×	○	△

○: 優れている　△: 多少問題がある　×: 問題がある

6. まとめと今後の課題

本稿では，利用者が，複数の VPN に対して同時に多重帰属できる，新しい VPN アーキテクチャを提案した．まず，利用者が複数の VPN に多重帰属できる VPN アーキテクチャを提案し，そこで必要となる機能を議論した．本稿で提案した VPN アーキテクチャは，3 種類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) によって階層的に構成されている．そこで，これらそれぞれのネットワークレベルに要求される機能を整理した．さらに，各ネットワークレベルをレイヤ 2，レイヤ 3，もしくはレイヤ 4 で実現した，3 種類の代表的な VPN アーキテクチャについて評価を行い，アーキテクチャ 2-2-3 が優れているという結論を得た．今後の課題としては，管理の容易さ，セキュリティ，信頼性など，より多くの評価項目での評価や，アーキテクチャ 2-2-3 を利用した，既存のネットワーク技術の組み合わせによる MAVPN のプロトタイプ実装などが挙げられる．

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．

文　　献

[1] 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, “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,” 進学技報 *IN2003-50*, vol. 103, July 2003.

[2] M. Carugi *et al.*, “Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks <draft-ietf-l3vpn-requirements-00.t
Internet Draft, Apr. 2003.

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

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

[5] 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.

[6] 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.

[7] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol label switching architecture,” *Request for Comments (RFC) 3031*, Jan. 2001.

[8] E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” *Request for Comments (RFC) 2547*, Mar. 1999.

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

[10] W. Townsley *et al.*, “Layer two tunneling protocol ”L2TP”,” *Request for Comments (RFC) 2661*, aug 1999.

[11] S. Kent and R. Atkinson, “Security architecture for the internet protocol,” *Request for Comments (RFC) 2401*, Nov. 1998.