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.

グループ指向通信を実現するネットワークアーキテクチャの一考察

高橋　洋介† 　杉山　浩平† 　大崎　博之† 　今瀬　真† 　八木　毅††
波戸　邦夫†† 　村山　純一††

† 大阪大学 大学院情報科学研究科
〒 565-0871 大阪府吹田市山田丘 1-5
†† 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: †{yosuke-t,k-sugi,oosaki,imase}@ist.osaka-u.ac.jp,
††{yagi.takeshi,hato.kunio,murayama.junichi}@lab.ntt.co.jp

あらまし　本稿では、インターネットにおけるセキュリティ低下や情報 S/N 比低下の問題を解決するために、グループ指向通信を実現するネットワークアーキテクチャについて考察し、多重帰属モデルを採用したアーキテクチャを提案する。複数のグループを通信目的ごとに形成することで、特定の目的に対する情報 S/N 比を高めるとともに、各グループを閉域化することでセキュリティも強化できる。従来のユーザ端末では多重帰属が困難であるため、「 Web コンセントレータ」を用いて複数のグループを終端し、複数グループへの多重帰属を実現する。ユーザ端末は Web コンセントレータに接続する。Web コンセントレータは、複数のグループからのコンテンツをポータルサイトのように集約して、ユーザ端末に送信する。グループ指向通信を実現するさまざまなネットワーク技術が提案されているが、要求条件に応じた比較評価の結果、Web コンセントレータとユーザ端末間のアクセス系ネットワークには SSL-VPN が適しており、Web コンセントレータ間のバックボーン系ネットワークでは MPLS-VPN が適していることが明らかになった。結果として、提案のアーキテクチャでは、従来の Web ベースのユーザ端末を用いて、セキュアかつ情報 S/N 比の高い通信を実現することが期待できる。
キーワード　ネットワークアーキテクチャ、グループ指向通信、VPN (Virtual Private Network)、多重帰属、セキュリティ

On Network Architecture for Realizing Group-Oriented Communication

Yousuke TAKAHASHI†, Kouhei SUGIYAMA†, Hiroyuki OHSAKI†, Makoto IMASE†, Takeshi YAGI††, Kunio HATO††, and Junichi MURAYAMA††

† Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka 565-0871, Japan
†† NTT Information Sharing Platform Laboratories, NTT Corporation
3-9-11 Midoricho, Musashino, Tokyo 180-8585, Japan
E-mail: †{yosuke-t,k-sugi,oosaki,imase}@ist.osaka-u.ac.jp,
††{yagi.takeshi,hato.kunio,murayama.junichi}@lab.ntt.co.jp

Abstract　In this paper, we disscuss a network architecture realizing group-oriented communication for solving the problem in the Internet, such as security and information Signal to Noise ratio degradation, and propose a architecture adopted the multiple-association model. The proposal architecture can increase information Signal to Noise ratio for the specific purpose by forming multiple groups for every communication purpose, and can strengthen security by closing each group. The existing user's host is difficult to associate with multiple groups. Hence, multiple groups is terminated by using Web concentrator. association with multiple groups is realized. User's hosts connect to Web concentrator. Web concentrator aggregates the contents from multiple groups as a portal site, and transmits to a user's host. Several network technologies realizing group-oriented communication are proposed. ¿From the result of the comparison evaluation according to demand requirements, however, we show that SSL-VPN is suitable for the access network between Web concentrator and user's host, and MPLS-VPN is suitable for the backbone network among Web concentrators. Consequently, it is expected that the proposal architecture realizes secure and high information Signal to Noise ratio communication using the exsisting Web based user's host.
Key words　Network Architecture, Group-Oriented Communication, VPN (Virtual Private Network), Multiple Association

1 はじめに

近年、さまざまな社会活動のネットワーク化が急速に進んでいる [1]。これは、情報処理技術の高速化・低コスト化や、ネットワーク技術 (特にインターネット技術) の爆発的な普及といった、情報通信技術の急速な発展に起因している。また、社会活動の効率化・多様化に伴い、通信形態もますます多様化・高度化している [2,3]。例えば、ネットワーク上で、商品を売買・流通する電子商取引や、情報家電やそれを用いたホームセキュリティシステムが実用化されている。

ユーザのネットワークに対するニーズも高度化しているため、既存のインターネットの限界も指摘されつつある [**?**]。例えば、インターネットが生活インフラ化しつつあり、ユーザは、インターネットに低コストで接続できる一方で、予期せぬ相手から不適切な情報を多量に送付されるスパム被害 [4] や、個人が保有する重要な個人情報が漏洩するフィッシング被害 [5] が増大している。既存のインターネットでは、一意なアドレス情報をもとに、広範囲に及ぶユーザ間の接続性を確保しているため、いったんアドレス情報が漏洩してしまうと、このような被害を防ぐことは非常に困難である。

このような背景から、ユーザのネットワークに対する関心が「接続性・コスト」から「安全性・信頼性」へ移行しつつあり、ネットワークに対する安全・安心の要求が高まっている [?]。従って、今後、ネットワークユーザに対して、安全・安心を提供できるネットワークを設計する必要があると考えられる。

インターネットのセキュリティ問題を解決する技術として、特定のグループ内のユーザだけへの到達性を確保する「グループ指向通信技術」が有望であると考えられる。この技術では、目的ごとにグループを形成し、グループ外ユーザへの到達性を制限する。これにより、グループ内では安全な通信が実現可能である。しかし、グループ内では、インターネットに比べて接続できるユーザ数がきわめて少ない。グループを形成することにより、ユーザが実際に獲得する情報中に含まれている不必要な情報 (ノイズ) を削減できる一方で、利用目的が多様化した場合には、ユーザが真に獲得したい情報 (シグナル) も「相対的」に減少する。この結果、「情報 S/N (Signal to Noise) 」が低下してしまうという問題がある。

セキュリティを高めつつ、情報 S/N 比も高めるためには、ユーザが複数のグループに同時に帰属 (多重帰属) することが有効と考えられる [6]。しかし、既存の通信技術では、ユーザが複数のグループに多重帰属することは現実的には困難である。

そこで本稿では、この問題を解決するために、多重帰属モデルを採用したグループ指向通信アーキテクチャを提案する。このアーキテクチャでは、「 Web コンセントレータ」を用いて複数のグループを終端する。ユーザ端末は Web コンセントレータに接続する。Web コンセントレータは、複数のグループからのコンテンツをポータルサイトのように集約して、ユーザ端末に送信する。グループを実現するさまざまなネットワーク技術が提案されているが、要求条件に応じた比較評価により、Web コンセントレータとユーザ端末間のアクセス系ネットワークには

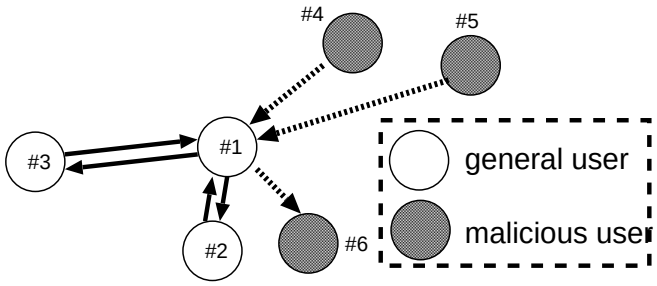

図 1: インターネットの通信モデル

SSL-VPN が適しており、Web コンセントレータ間のバックボーン系ネットワークでは MPLS-VPN が適していることを示す。

本稿の構成は次の通りである。2 章では、従来技術の問題点と解決へのアプローチを述べる。**??** 章では、本稿で提案するネットワークモデルを説明する。4 章では、提案するネットワークモデルへの適用候補となる通信技術を評価し、その選択指針を示す。5 章では、提案するネットワークアーキテクチャの全体像を示すとともに、その特性を定性的に評価する。最後に 6 章で、本稿の結論を述べる。

2 従来技術の問題点と解決へのアプローチ

2.1 インターネット通信技術

インターネットの通信モデルを図 1 に示す。インターネットでは、全ユーザが一意なアドレスを保持しているため、ユーザはアドレス情報をもとに全ユーザを識別することが可能である。例えば、図 1 において、ユーザ #1 は、ユーザ #2 とユーザ #3 とのアドレスを保有しているため、それぞれのユーザに到達することが可能である。

しかし、インターネットでは全ユーザへの到達性が確保されているため、予期せぬユーザから情報を受信したり、逆に予期せぬユーザに情報送信してしまうという問題も生じる。例えば図 1 において、ユーザ#1 はユーザ #4 とユーザ #5 から情報を受信可能であるため、スパムなどの不適切な情報を大量に受信する可能性がある。予期せぬユーザからの情報受信はノイズ (N) を増加させ、情報 S/N 比を低下させる一因となる。また、ユーザ #1 はフィッシングや宛先誤りなどにより、予期せぬユーザ #6 に情報を送信してしまい、個人情報などの機密情報が漏洩してしまう恐れもある。予期せぬユーザへの情報送信は、セキュリティを低下させる一因となる。

広範な到達性はインターネットの大きな特徴となっているが、現状では、インターネットに対する関心が「接続性・コスト」から「安全性・信頼性」へ移行しており、広範な到達性が必ずしも好ましいものとは言えない。

2.2 グループ指向通信技術

インターネットの到達性に起因する問題を解決する技術として、特定グループ内のユーザへの到達性を制限する、「グループ指向通信技術」が有望であると考えられる。ここで、グループ指向通信とは、通信の主体となる「エンティティ」の論理的な集合である「グループ」間の通信を基本とする通信方式を指す

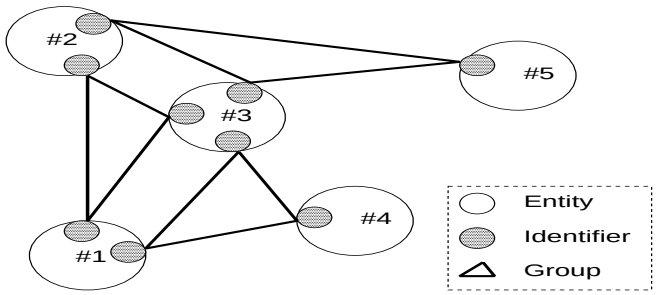

図 2: グループ指向通信技術の概要

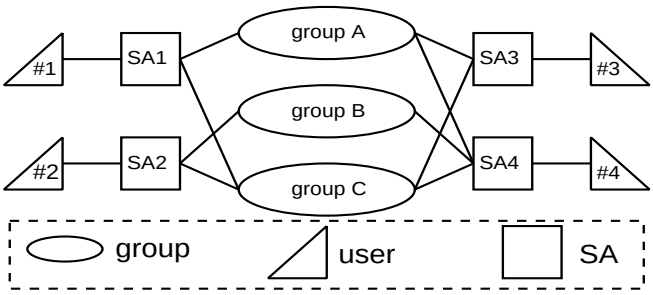

図 3: 提案のネットワークモデル

(図 2)。グループの自由な組み合わせによって、エンティティ間の多様な通信を実現する。また、グループ内で閉域性を持たせることにより、グループ外への情報流出とグループ外からの情報受信を防止する。グループ指向通信により、さまざまな社会活動を自然にネットワーク上にマッピング可能になる。

グループ指向通信では、通信目的に応じたグループを形成することで、スパム等のノイズ (N) を低減する。しかし、通信の目的が多様化した場合には、単一グループに帰属するだけではシグナル (S) が相対的に小さくなり、その結果、「情報 S/N 比」が低下してしまう恐れがある。

2.3 多重帰属通信技術

従来のグループ指向通信技術の問題を解決するためには、通信目的に応じて複数のグループを形成し、ユーザがこれらの複数のグループに同時に多重帰属できることが望ましい。グループを閉域化することで、グループのセキュリティが強化される。さらに、目的に応じて、グループを適切に選択・帰属することで、情報 S/N 比の高い通信が可能になる。

ただし既存のネットワーク技術では、ユーザ端末が複数のグループに同時に帰属するといった通信を実現することは容易ではない。例えば、既存の VPN 技術を用いて、アドレス体系の異なる複数の VPN (= グループ) に同時に接続した場合、VPN 間でアドレス空間が重複していれば情報の送信先を特定できないといった問題が発生してしまう。

3 提案のネットワークモデル

従来のネットワーク技術およびユーザ端末を活用しつつ、グループへの多重帰属通信を実現するために、図 3 に示すネットワークモデルを提案する。このモデルでは、バックボーンネットワークは、複数のグループ (例えば VPN) によって構成される。これらのグループは SA (Security Agent) と呼ばれる端末によって終端される。SA はユーザごとに配備される。SA は、複数のグループに多重帰属できる機能を有している。SA がどのグループに帰属するかは、その SA に対応するユーザの通信目的によって決定される。また、各 SA には、「 Web コンセントレータ」を配備する (図 4)。Web コンセントレータは、ユーザ端末上で動作する汎用的な Web ブラウザに対してタブブラウジングの機能を提供する。ユーザ端末と SA 間はポイント-ポイント通信で接続される。セキュリティを維持する観点から、ここもグループ指向通信 (例えば VPN) によって構成することが

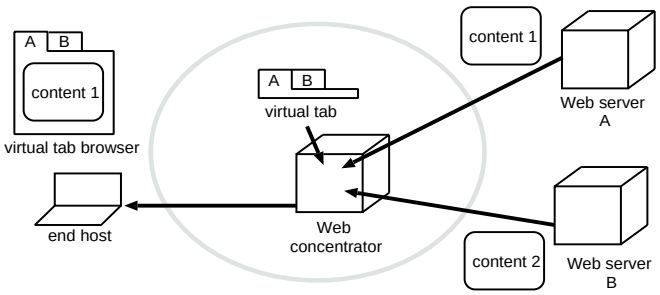

図 4: 多重帰属を実現する Web コンセントレータ

望ましい。

提案するネットワークモデルの核となるアイデアは、「 Web コンセントレータが、複数のグループからのコンテンツを集約し、多重帰属を自然な形で行うことができるという意味での、仮想的なタブブラウジングの機能をユーザ端末に対して提供する」というものである。ここで、ユーザ端末は、グループ指向通信への参加者が直接操作する端末を指す。ユーザは、ユーザ端末上で動作している汎用的な Web ブラウザを利用して、複数のグループと通信する。グループの選択・作成・変更・削除等も、Web ブラウザを介して行う。これにより、参加者に対して直感的なグループ指向通信のインターフェースを提供することが可能となる。また、汎用的な Web インターフェースを利用するため、ネットワークドライバやアプリケーションの変更も不要である。

4 グループ指向通信技術の選択

提案のネットワークモデルにおいては、ユーザ端末と SA 間を構成するアクセス系ネットワークと、SA 間を構成するバックボーン系ネットワークにどのような通信技術を選択するかが重要な問題である。そこで、グループ指向通信への要求条件と、従来の通信技術の比較評価により、提案のネットワークモデルを実現するために適した通信技術を明らかにする。

4.1 グループ指向通信への要求条件

利用者の安心・安全に対する要求を考え、ここでは、グループ指向通信への一般的な要求条件として、接続性・汎用性・セキュリティを考える。

- 接続性

接続性については、ポータビリティとスケーラビリティが要求される。グループ指向通信では、エンティティとして高機能

な固定端末以外に、低機能な移動端末を許容したり、エンティティの地理的移動を許容することで、エンティティ間の多様な通信を実現することが望ましい。このため、ポータビリティが要求される。また、ネットワーク全体として多数のグループを収容する必要があり、グループによっては多数のユーザ端末を収容する必要があることから、スケーラビリティも重要である。

- 汎用性

汎用性については、レイヤと性能の視点で考える必要がある。グループ指向通信ではエンティティ間で汎用的なアプリケーションを利用可能とし、従来技術と高い親和性を持たせることが望ましい。従って、グループ指向通信は低レイヤで実現される方が望ましい。また、映像通信や音声通信アプリケーションの適用も考慮すると、通信性能もこれらを実現できる程度に高いことが望ましい。

- セキュリティ

セキュリティについては、閉域化と暗号化が要求される。グループ指向通信では、セキュリティの向上も目指している。通信範囲をグループ内に限定することで、スパムやフィッシング等の問題を解決できる。ただし、閉域ネットワークが、オープンなネットワーク上にオーバレイする形で構成されている場合には、通信範囲をグループ内に限定していたとしても、悪意のある利用者がグループ内の通信を盗聴・改竄している可能性がある。このため、このような不正な通信を防止することが必要である。従って、グループ指向通信では通信内容の暗号化が必要と言える。

4.2 グループ指向通信技術の比較

以上のような要求条件に基づいて、既存のネットワーク技術を比較・評価する。ここで評価項目は、接続性 (ポータビリティ、スケーラビリティ)、汎用性 (レイヤ、性能) およびセキュリティ (閉域化、暗号化) とした。これらの評価項目について、既存の通信技術として、MPLS-VPN [7]、IPsec VPN [8]、SSL VPN [9]、SNS [?]、SMTP [10]、JXTA [11] および MNS [12] を比較・評価した。比較結果をまとめて表**??** に示す。各通信技術の評価結果を以下に示す。

- MPLS-VPN [7]

エンティティは仮想ネットワークインターフェースに対応し、レイヤ 3 の IP アドレスで識別する。キャリアあるはプロバイダのネットワーク内で、ユーザ端末を固定的に接続することを前提とする。このため、通信内容は暗号化されない。ユーザ端末が VPN ゲートウェイの LAN 外に移動した場合、セキュリティは保持できない。リモート接続として利用することは難しいため、ポータビリティに乏しいと考えられる。ラベルスタッキング機能により、スケーラビリティには優れる。

- IPsec VPN [8]

エンティティはネットワークインターフェースに対応し、レイヤ 3 の IP アドレスで識別する。多くの OS で利用可能であるが、設定がやや難解であるため、ユーザ端末の変更に柔軟に対応できるとは言えない。そのため、ポータビリティも充分とは言えない。また、クライアント / サーバモデルのため、サーバがボトルネックとなりユーザ接続数の増加を許容できない。よってスケーラビリティも充分とは言えない。インターネット上での利用を前提とするため、通信内容は暗号化される。

- SSL-VPN [9]

エンティティは SSL モジュールに対応し、IP アドレスとポート番号で識別するが、レイヤ 5 に相当する。クライアント / サーバモデルであるため、スケーラビリティも充分でない。通信内容は SSL で暗号化される。IPsec VPN に類似するが、レイヤが異なり汎用の Web 端末で利用できるため、ポータビリティに優れる点で異なる。

- SNS [?]

エンティティはユーザの仮想人格に対応し、レイヤ 7 に相当するアカウント名で識別する。SNS はクライアント / サーバモデルであるが、多数のユーザアクセスを時系列的に逐次処理し、同時接続数を削減することで、スケーラビリティを高めることができる。SNS も汎用の Web 端末で利用できるため、ポータビリティに優れる。

- SMTP [10]

エンティティは MUA (Mail User Agent) に対応し、レイヤ 7 に相当するメールアドレスで識別する。コネクションレス型のネットワークを形成し、スケーラビリティに優れる。エンドユーザ端末は、メールサーバへの到達性さえ維持すえば、任意のサイトからアクセス可能なため、ポータビリティにも優れる。通信内容は暗号化されない。

- JXTA [11]

エンティティはピアに対応し、レイヤ 7 に相当するピア ID で識別する。P2P モデルであり、スケーラビリティに優れる。通信内容は SSL で暗号化される。汎用の Java VM 上で利用できるため、ポータビリティに優れる。

- MyNetSpace [12]

エンティティはネットワークインターフェースに対応し、レイヤ 3 の IP アドレスで識別する。集中型アーキテクチャであるので、スケーラビリティに乏しい。OS に依存した機能を用いており、利用するためには特別な設定も必要となるため、ポータビリティにも乏しい。通信内容は暗号化されない。

4.3 アクセス通信技術の選択

以上の評価結果をもとに、提案のネットワークモデルのアクセス系ネットワークに適用すべき通信技術を選択する。アクセス系ネットワークへの要求条件としては、ポータビリティ・暗号化・レイヤ (6 以下) が重視されると考えられる。

- ポータビリティ

提案のネットワークモデルでは、SA は固定的に設置され、ユーザ端末のアクセスポイントとして動作する。一方、ユーザ端末は固定端末だけでなく、携帯電話、PDA などの移動端末も想定する必要がある。従って、単に端末が移動するだけでなく、異なる端末からもアクセスできることが望まれる。

- 暗号化

ポータビリティに起因して、多様な端末による、多様な形態でのアクセスが要求されるため、セキュリティを維持するためには通信内容の暗号化が必須である。

- レイヤ

表 1　要求条件と通信技術の比較表

		MPLS-VPN	IPsec VPN	SSL-VPN	SNS	SMTP	JXTA	MyNetSpace
接続性	ポータビリティ	×	△	○	○	○	○	×
	スケーラビリティ	○	×	×	○	○	○	×
汎用性	レイヤ	3	3	5	7	7	7	3
	性能	○	×	×	○	×	×	○
セキュリティ	閉域化	○	○	○	○	×	○	○
	暗号化	×	○	○	×	○	○	×

○: 可能　△: 一部が可能　×: 不可能か、非標準の機能が必要

ユーザ端末から SA に対しては、Web アクセスを前提とするため、レイヤは 6 以下であること、もしくはそれ以上のレイヤの場合はアプリケーションを Web に限定することが必要となる。

- その他

ユーザ端末と SA は 1:1 で接続することを想定しているためスケーラビリティは要求されない。

これらの要求条件と通信技術の比較表 (表 **??**) を照合すると、アクセス系ネットワークの通信技術には SSL-VPN が最も適していると考えられる。

4.4　バックボーン通信技術の選択

次に、提案のネットワークモデルのバックボーン系ネットワークに適用すべき通信技術を選択する。バックボーン系ネットワークへの要求条件としては、スケーラビリティおよび転送性能が重視されると考えられる。

- スケーラビリティ

提案のネットワークモデル上で、さまざまな社会活動をネットワーク化する場合、少なくとも数百万以上の SA を収容可能であることが望ましい。また、数万以上のグループを形成できることが望ましい。

- 転送性能

バックボーン系ネットワークは、多数のユーザによって、多様な用途で共用されるため、例えば、映像通信や音声通信アプリケーションも使用可能な転送性能が要求される。ただし、リソースを共用するため、全ての通信品質を公平に高める必要はなく、優先制御等を適用して経済的に、個々の品質要求を満たすことが重要である。

- その他

バックボーン系ネットワークはキャリアあるいはプロバイダに閉じることを想定しているので、暗号化は要求されない。また、SA は固定設置を想定しているので、ポータビリティも要求されない。

これらの要求条件と通信技術の比較表 (表 **??**) を照合すると、バックボーン系ネットワークの通信技術には MPLS-VPN が最も適していると考えられる。

5　アーキテクチャ評価

本章では、多重帰属モデルを採用したグループ指向通信アーキテクチャの全体像まとめるとともに、その効果について考察する。

提案のアーキテクチャでは、バックボーン系ネットワークにスケーラビリティと転送性能を重視して MPLS-VPN 技術を適用し、利用目的ごとに複数の VPN を構成する。これらの VPN は、ユーザごとに設置された SA で終端される。SA は、利用目的に応じて、複数の VPN を終端する。SA とユーザ端末はポータビリティを重視して SSL-VPN で接続する。SA 内には、Web コンセントレータを配備し、複数の VPN のコンテンツをポータルサイト的に集約してユーザ端末に送信する。ユーザ端末はタブブラウジング機能を利用して、選択的に複数の VPN にアクセスする。

グループ指向通信に対しては、接続性・汎用性・セキュリティが要求されるが、これらに対する提案アーキテクチャの効果は以下の通りである、

- 接続性

ポータビリティに関しては、アクセス系の SSL-VPN 機能により、ユーザ端末は任意のサイトからインターネット経由で SA へアクセス可能である。また、スケーラビリティに関しては、ネットワーク内への SA 収容能力が対象となるが、これは、MPLS-VPN のスケーラビリティに依存する。MPLS-VPN は、ラベルスタック機能により、充分なスケーラビリティを有しており、数百万の SA を収容することも可能と考えられる。

- 汎用性

レイヤに関しては、Web コンセントレータに制約され、アプリケーションは Web ベースのものに限定される。転送性能に関しては、バックボーン系は充分な性能が期待できるが、ユーザ端末間では、Web コンセントレータがボトルネックになると予想される。Web コンセントレータの転送性能は、コスト要求とのトレードオフ関係はあるが、ユーザ単位で向上させることが可能である。

- セキュリティ

閉域化に関しては、アクセス系ネットワークとバックボーン系ネットワークの双方において、VPN 機能によって実現される。暗号化に関しては、インターネット経由の通信も予想されるアクセス系ネットワークでは、SSL-VPN 機能として実現される。バックボーン系ネットワークでは、暗号化を想定していないが、これは、キャリアあるいはプロバイダのネットワーク内で、SA を固定的に接続するので、特に問題にはならないと考えられる。

これらの結果から、提案のアーキテクチャでは、アプリケーションは Web ベースのものに限定されるが、従来のユーザ端末

を用いて、セキュアで情報 S/N 比の高い通信を実現することが期待できる。

6 むすび

インターネットは広範な到達性という特徴を有する反面、スパムやフィッシングに起因するセキュリティ低下や情報 S/N 比低下の問題を抱えている。この問題を解決するためには、本稿で提案したグループ指向通信アーキテクチャが有効である。提案のアーキテクチャでは、Web コンセントレータを用いた多重帰属モデルを採用する。このモデルでは、Web コンセントレータが複数のグループを終端し、複数のグループからのコンテンツをポータルサイトのように集約して、ユーザ端末に送信する。従来の通信技術を比較評価した結果、提案のネットワークモデルのアクセス系ネットワークには SSL-VPN、バックボーン系ネットワークには MPLS-VPN が適していることがわかった。結論として、提案のアーキテクチャでは、アプリケーションが Web ベースに限定されるが、従来のユーザ端末を用いて、セキュアで情報 S/N 比の高い通信を実現することが期待できる。

文　献

[1] 今瀬 真, 大崎 博之, 松田 和浩, “サイバーソサイエティを実現する仮想網技術の動向,” 情報処理, vol. 46, pp. 169–174, Feb. 2005.

[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, May 2003.

[3] 総務省, “平成 16 年 通信利用動向調査報告書,” May 2004. Also available as `http://www.johotsusintokei.soumu.go.jp/yusei/`.

[4] 総務省, “迷惑メールへの対策の在り方に関する研究会 最終報告書,” 2005. Also available as `http://www.soumu.go.jp/s-news/2005/pdf/050722_2_02_00.pdf`.

[5] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Indiana University: Bloomington-Working Paper. http://www.informatics. indiana. edu/fil/papers. asp, last accessed*, vol. 23, Dec. 2006.

[6] 本田 治, 原 義弘, 大崎 博之, 今瀬 真, 丸吉 政博, 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 クチャの提案と実装,” 情報処理学会論文誌, vol. 47, pp. 2236–2246, July 2006.

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

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

[9] T. Dierks and C. Allen, “The TLS protocol,” *Request for Comments (RFC) 2246*, Jan. 1999.

[10] J. B. Postel, “Simple mail transfer protocol,” *Request for Comments (RFC) 821*, Aug. 1982.

[11] B. Traversat *et al.*, “Project JXTA 2.0 super-peer virtual network,” *Sun Microsystem White Papers*, May 2003. Also available as `https://research.sun.com/spotlight/misc/jxta.pdf`.

[12] 三村 和, 飛岡 良明, 森川 博之, 青山友紀, “サービス指向グルーピング機構を用いたユーザ主導ネットワークの構築,” 第 *13* 回マルチメディア通信と分散処理 (*DPS*) ワークショップ, pp. 290–294, Nov. 2005.