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.

グループ指向通信のためのネットワークアーキテクチャ

高橋　洋介† 　杉山　浩平† 　大崎　博之† 　今瀬　真† 　八木　毅††
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,murayama.junichi}@lab.ntt.co.jp

あらまし　本稿では、「グループ指向通信」という新しい通信形態を提案する。グループ指向通信とは、従来の 1 対 1 (ユニキャスト) 通信とは異なり、グループ間の通信を基本とする新しい通信形態である。グループ指向通信は、N 対 N 通信 (グループ通信) の一種であるが、1 対 1 通信や 1 対 N 通信を含む、すべての通信をグループ間の通信によって実現するという点に特徴がある。これにより、さまざまな社会活動を自然な形でネットワーク上で実現できるとともに、安全性・信頼性に対する利用者のニーズを満たすことができる。本稿では、さらにグループ指向通信を実現するためのネットワークアーキテクチャを設計する。その結果、グループ指向通信のためのネットワークアーキテクチャは、(1) パケット交換型であり、(2) 到達性制御が鍵となる技術であること、(3) 制御プレーンと転送プレーンの二層構造を取るべきであること、などを示す。
キーワード　グループ指向通信、ネットワークアーキテクチャ、グループ通信、セキュリティ、アドレス演算

Network Architecture for Group-Oriented Communication

Yousuke TAKAHASHI†, Kouhei SUGIYAMA†, Hiroyuki OHSAKI†, Makoto IMASE†, Takeshi YAGI††, 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,murayama.junichi}@lab.ntt.co.jp

Abstract　In this paper, we propose a novel communication paradigm called *group-oriented communication*. Different from conventional unicast-based communications, group-oriented communication is based on group-based communications. Group-oriented communication is a type of many-to-many communication, but it realizes any type of communications covering one-to-one, one-to-many, many-to-one, and many-to-many communications by combining group-based communications. With group-oriented communication, diverse social activities can be shifted onto a communication network in a straightforward way, and users' requirements on security/reliability can be fulfilled. In this paper, after carefully defining design goals, we design a network architecture for realizing group-oriented communication. Through quantitative evaluations, we show (1) the network architecture for group-oriented communication should be a packet-based network, (2) reachability control is the core of the network architecture, and (3) the network architecture should form two-layer structure consisting of a control plane and a transport plane.
Key words　Group-Oriented Communication, Network Architecture, Group Communication, Security, Address Operation

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]。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がその一因となっている。

一方、高度な情報技術による、社会活動の効率化・多様化により、通信形態の多様化・高度化も進んでいる [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次々と実用化されている。

これにともない、ネットワーク利用者の、ネットワークに対するニーズが高度化してきている。近年、既存のインターネットの、さまざまな限界が指摘されている [4]。例えば、インターネットは、1 対 1 (ユニキャスト) 通信が中心であるとともに、「接続性・コスト」が最優先されている。その結果、インターネットでは、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。このため、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が困難である。

さまざまな社会活動をネットワーク上で実現するためには、1 対 1 通信だけでなく、1 対 N (マルチキャスト) 通信や、N 対

N (グループ) 通信も重要であると考えられる。これに加えて、利用者のネットワークに対する関心が、単なる「接続性・コスト」から「安全性・信頼性」へと変化しつつある。その結果、ネットワーク利用者に対して、多様な通信を、安全かつ安心に提供できるネットワークが要求されている。

1 対 N 通信や N 対 N 通信のような、多様な通信を実現する技術として、グループ通信に関連する研究がこれまでいくつか行われている [5–10]。

文献 [6] では、グループ通信を実現するプロトコルスタック Horus を提案している。Hours では、ネットワークプロトコルのさまざまな機能をブロック化し、これらのブロックを自由に組み合わせることにより、グループ通信を含むさまざまな通信を実現している。また、文献 [7] では、端末のグループを自由に生成できるネットワークアーキテクチャ MNS (MyNetSpace) を提案している。MNS は、IP パケットにグループ識別のためのヘッダを追加することにより、IP ネットワークとの互換性を実現している。しかしこれらの方式は、基本的に IP をベースとして実現されているため、通信の安全性・信頼性が不十分である。

一方、アプリケーションレベルマルチキャスト [8] やオーバレイマルチキャスト [9] によって、グループ通信を実現する手法も提案されている [5]。例えば、文献 [10] では、アプリケーションレベルマルチキャストのアーキテクチャ TAG (Topology Aware Grouping) を提案している。TAG では、エンド–エンド遅延やネットワークの負荷が小さくなるようにマルチキャストツリーを構築するため、ネットワーク資源の効率的な利用が可能である。しかし、TAG も、基盤ネットワークとして IP ネットワークを前提としているため、通信の安全性・信頼性が不十分である。

本稿では、まず、「グループ指向通信」という新しい通信形態を提案する。グループ指向通信とは、従来の 1 対 1 (ユニキャスト) 通信とは異なり、グループ間の通信を基本とする新しい通信形態である。グループ指向通信は、N 対 N 通信 (グループ通信) の一種であるが、1 対 1 通信や 1 対 N 通信を含む、すべての通信をグループ間の通信によって実現するという点に特徴がある。これにより、さまざまな社会活動を自然な形でネットワーク上で実現できるとともに、安全性・信頼性に対する利用者のニーズを満たすことができる。

本稿では、既存の IP との比較によって、グループ指向通信のメリットを定性的に議論する。また、グループ指向通信を実現するためのネットワークアーキテクチャを設計する。グループ指向通信のためのネットワークアーキテクチャの設計目標として、「動的なエンティティ / グループのサポート」、「アドレス演算のサポート」、「エンティティ / グループのファインダビリティの実現」、「セキュリティの実現」を挙げ、それぞれについて議論する。

さらに、これらの設計目標を満たすネットワークアーキテクチャを検討する。その結果、グループ指向通信のためのネットワークアーキテクチャは、(1) パケット交換型であり、(2) 到達性制御が核となる技術であること、(3) 制御プレーンと転送プレーンの二層構造を取るべきであること、などを示す。

本稿の構成は以下の通りである。まず 2 章では、グループ指向通信の概要を説明するとともに、その機能および特性を述べる。3 章では、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設計目標を議論する。3 章では、これらの設計目標をもとに、グループ指向通信のためのネットワークアーキテクチャを設計する。最後に、5 章において本稿のまとめと今後の課題を述べる。

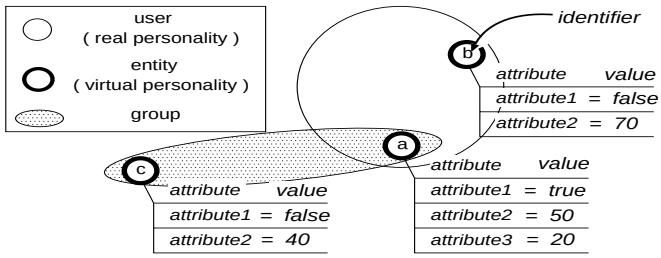

図 1: 用語の定義

2 グループ指向通信

2.1 用語の定義

本稿で用いる用語を以下のように定義する (図 1)。

「エンティティ」とは、通信の主体である。通常、ネットワーク利用者もしくは計算機上で動作しているアプリケーションがエンティティに相当する。ネットワーク利用者が、利用目的ごとに複数のエンティティ (例えば、利用者の仮想パーソナリティ) を有することも考えられる。

「グループ」とは、単一もしくは複数のエンティティの論理的な集合である。なお、グループの構成は、地理的な制約など、ネットワークの物理的な制約に縛られないことに注意されたい。

「識別子」とは、エンティティもしくはグループを識別するために付けられた名前である。

「属性情報」とは、エンティティもしくはグループの特徴をあらわす情報である。エンティティの属性情報の例として、ネットワーク利用者の情報 (名前、性別、住所、年齢) やエンティティの位置情報 (緯度、経度、標高) などが挙げられる。

2.2 概　　要

通信に対する多様な要求に応えるためには、エンティティ間の通信と、グループ間の通信の両方が必要とされる。このため、たとえグループ通信のためのプロトコルであっても、通常、エンティティ単位の通信と、グループ単位の通信の両方をサポートしなければならない。

従来のグループ間通信では、基本的に、通信の終端として「エンティティ」および「グループ」がそれぞれ別々に実現されていた。この場合、エンティティとグループに対する通信を別々に実現する必要があるため、結果としてネットワークアーキテクチャが複雑になってしまう。しかし、エンティティとグループは共通部分も多く、それぞれに対して類似した機能を提供している。

そこでグループ指向通信では、エンティティを「利用者の仮想パーソナリティ、アプリケーション、もしくはエンティティの集合である」のようにして再帰的に定義する。これにより、通信の終端として、「エンティティ」のみを実現すればよく、ネットワークアーキテクチャを簡単化できる。

本稿では、このようなアイデアに基づき、「グループ指向通信」という新しい通信形態を提案する。グループ指向通信とは、グループ間の通信を基本とする通信形態である。グループ指向通信は、N 対 N 通信 (グループ通信) の一種であるが、1 対 1 通信や 1 対 N 通信を含む、すべての通信をグループ間の通信によって実現するという点に特徴がある。

さらに、グループ指向通信では、「アドレス演算」によって、グループを柔軟かつ動的に自由に組み合わせることが可能であり、さまざまなエンティティ間での多様な通信を実現できる。また、利用目的に応じて、「エンティティ / グループの生成・変更・削除」が可能である。さらに、エンティティおよびグループの属性情報を管理することにより、「エンティティ / グループの検索」も可能である。

グループ指向通信は、一種の「グループ通信」であるため、

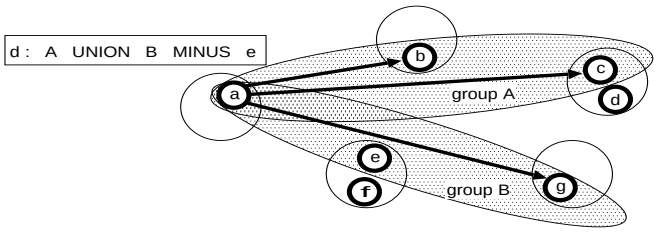

図 2: アドレス演算

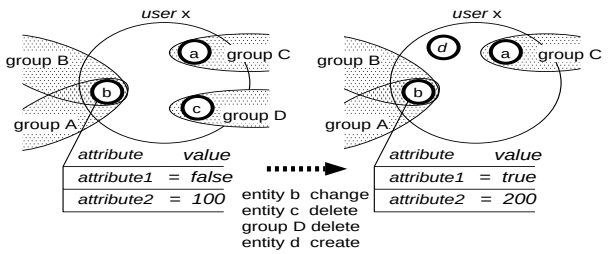

図 3: 生成・変更・削除

情報の到達性をグループ内に意図的に制限することが可能であり、情報漏洩やスパム・フィシング被害などのセキュリティリスクを低減できる。

これにより、グループ指向通信では、さまざまな社会活動を自然な形でネットワーク上で実現できるとともに、「安全性・信頼性」に対する利用者のニーズを満たすことができる。

2.3 機　　能

以下では、グループ指向通信が提供する機能を説明する。

2.3.1 アドレス演算

グループ指向通信では、「アドレス演算」によってグループを柔軟かつ動的に自由に組み合わせることが可能である (図 2)。これによって、さまざまなエンティティ間での多様な通信を実現する。具体的には、グループ指向通信では、情報の宛先アドレスとして、通信したいエンティティやグループの識別子を組み合わせた「アドレス演算式」を記述できる。これにより、例えば、ネットワーク利用者が、複数の組織に属する人から、特定のメンバを除いた人に対して情報を送信するといったことが可能となる。

アドレス演算式は、SQL の集合演算 [11] から着想を得ている。アドレス演算では、集合演算子 (UNION (和集合)、INTERSECT (積集合)、MINUS (差集合)) の被演算子として、エンティティやグループの識別子を記述することができる。例えば、図 2 では、宛先アドレスに

```
A UNION B MINUS e
```

と記述することによって、グループ A とグループ B の和集合から、エンティティ e を除いたエンティティの集合に対して情報を送信することができる。さらに、アドレス演算では、条件演算子 WHERE の被演算子として、通信したいエンティティやグループの属性情報に対する条件を指定することができる。これにより、特定の条件を満たしたエンティティだけに情報を送信することができる。例えば、宛先アドレスに、

```
A UNION B MINUS e WHERE age >= 20
```

と記述することによって、グループ A とグループ B の和集合から、エンティティ e を除いたエンティティの集合のうち、属性情報が条件 age >= 20 を満たすエンティティの集合だけに情報を送信することができる。

2.3.2 エンティティ/グループの生成・変更・削除

グループ指向通信では、利用目的に応じて、エンティティ / グループを自由に生成・変更・削除することが可能である (図 3)。

例えば、ネットワーク利用者が、必要に応じて仮想パーソナリティを複数作成し、それらを使い分けることが可能である。また、ネットワーク利用者が、必要に応じてグループを複数作成して、それらを使い分けることも可能である。同様に、エンティティ / グループを自由に削除することができる。例えば、ネットワーク利用者が、不要となった仮想人格やグループを削除することができる。

さらに、エンティティ / グループの属性情報を自由に変更することができる。例えば、ネットワーク利用者が、エンティティの属性情報 (例えば、仮想人格の属性情報) を変更することが可

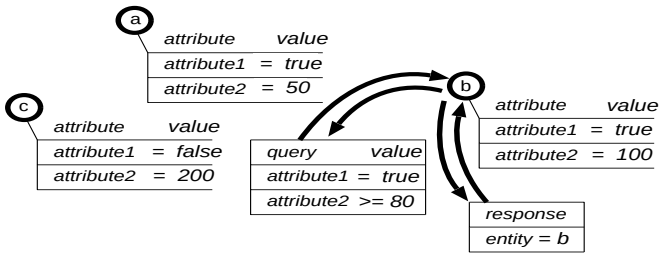

図 4: エンティティ/グループの検索

能である。

2.3.3 エンティティ/グループの検索

グループ指向通信では、エンティティおよびグループの属性情報を管理することにより、エンティティおよびグループを検索することが可能である (図 4)。具体的には、エンティティの識別子や属性情報をキーとして、エンティティを検索することができる。例えば、ネットワーク利用者が、エンティティの属性情報を利用して、(エンティティの位置情報が属性情報として登録されていれば) 地理的に近いエンティティを検索することが可能である。

同様に、グループの識別子や属性情報をキーとして、グループを検索することができる。例えば、ネットワーク利用者が、グループの属性情報を利用して、(実社会における組織名がグループの属性情報として登録されていれば) その組織に対応するグループを検索することが可能である。

予期しない第三者からの通信を防ぐために、エンティティ / グループの識別子や属性情報は、必要に応じて公開・非公開を選択することができる。これによって、利用者が通信したい公開・非公開を選択することができる。

2.3.4 安全な通信

グループ指向通信では、エンティティ / グループ間で、信頼性があり、なおかつ安全な通信を行うことが可能である (図 5)。例えば、ネットワーク利用者が、通信相手のエンティティもしくはグループと安全に情報を交換することが可能である。また、グループ指向通信は一種のグループ間通信であるため、情報の到達性をグループ内に意図的に制限することが可能であり、情報漏洩やフィッシング / スパム被害などのセキュリティリスクを低減できる。

さらに、エンティティ / グループに対する情報の到達性 (プレゼンス) をリアルタイムに検知することが可能である。例えば、ネットワークの利用者が、通信相手のエンティティもしくはグループが現在アクティブかどうかを知ることが可能である。

2.4 特　　性

以下では、グループ指向通信を、IP と比較することにより、グループ指向通信の特性を議論する。本稿における用語の定義では、IP では、エンティティは「ネットワークインターフェース」に相当し、エンティティの識別子は「 IP アドレス」に相当する。グループは「マルチキャストグループ」に相当し、グループの識別子は「 IP アドレス (マルチキャストアドレス) 」

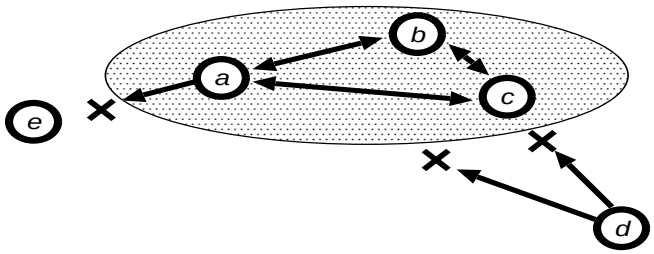

図 5: 安全な通信

に相当する。

2.4.1 アドレス演算

グループ指向通信では、「アドレス演算」によってグループを柔軟かつ動的に自由に組み合わせることが可能である。アドレス演算式によって、さまざまなエンティティの組み合せを記述できるため、エンティティ間での多様な通信を簡単かつ効率的に実現できる。

一方、IP では、宛先アドレスとして単一の識別子 (IP アドレス) しか記述できない。IP オプションのソースルーティングや XCAST [12] を用いれば、(ルータが対応しているという条件のもとで) 複数の宛先アドレスを記述できるが、非常に限定的である。

2.4.2 エンティティ/グループの生成・変更・削除

グループ指向通信では、エンティティを自由に生成・変更・削除することができる。これは、エンティティの識別子が、エンティティの物理アドレスから分離していることによって可能となる。

一方、IP では、エンティティ (ネットワークインターフェース) が識別子 (IP アドレス) に一対一に対応しているため、エンティティの生成・変更・削除を自由に行うことができない。

また、グループ指向通信では、エンティティやグループの識別子の公開・非公開を自由に選択することができる。例えば、エンティティ / グループの識別子を非公開とすることで、予期しない第三者からの通信を防ぐことができ、セキュリティの向上が可能となる。

グループ指向通信では、グループを自由に生成・変更・削除することができる。IP でも、IGMP を用いてマルチキャストグループを自由に生成・変更・削除することは可能である。しかし、すべてのルータが IGMP に対応している必要がある。また、IGMP は攻撃に弱いなど、セキュリティ上の問題も指摘されている [13]。

2.4.3 エンティティ/グループの検索

グループ指向通信では、エンティティの識別子や属性情報をキーとして、エンティティを検索することができる。例えば、名前・住所・年齢・性別などをエンティティの属性情報として登録しておき、これらをキーとしてエンティティを検索することが可能である。これにより、高機能なネットワークサービスを容易に実現でき、さまざまな社会活動をネットワーク上に容易に移行できると考えられる。

一方、IP には識別子 (IP アドレス) の検索機能はない。DNS を用いた、単純なホスト名から IP アドレスの名前解決は可能であるが、非常に限定的である。また、エンティティ (ネットワークインターフェース) の属性情報は登録できないため、当然ながらエンティティの属性情報をキーとしたエンティティ検索もできない。

グループ指向通信では、グループの識別子や属性情報をキーとして、グループを検索することができる。例えば、実社会における組織の名称・所在地・活動目的などをグループの属性情報として登録しておき、これらをキーとしてグループを検索することが可能である。これにより、高機能なネットワークサービスを容易に実現でき、さまざまな社会活動をネットワーク上に容易に移行できると考えられる。

一方、IP には、グループの識別子 (マルチキャストアドレス) の検索機能はない。また、マルチキャストアドレスは単なる IP アドレスである。このため、2.4 節で述べたように、グループ (マルチキャストグループ) の属性情報は登録できず、当然ながらエンティティの属性情報をキーとしたエンティティ検索もできない。

2.4.4 安全な通信

グループ指向通信では、エンティティ / グループ間で、信頼性があり、なおかつ安全な通信を行うことが可能である。

一方、IP は、そもそも信頼性のないネットワークを前提として設計された通信プロトコルである。IPsec や SSL/TLS など、ネットワークの安全性を向上させるプロトコルも利用可能であるが、これらは (IP のプロトコルに含まれないという意味で) 標準のプロトコルではない。また、IP では、エンティティはネットワークインターフェースであるため、通信相手が実際にアクティブかどうかを確認することはできない。ICMP 等により、ネットワークインターフェースが稼働しているかどうかが分かるだけである。

以上のように、グループ指向通信は、既存の IP のさまざまな問題を解決する可能性を持った通信形態である。しかし、このようなグループ指向通信のメリットの多くは、ネットワークを高機能化することによって得られるものである。このため、ネットワークの高機能化を前提としたグループ指向通信を、実際のネットワークとして本当に実現できるかどうかが問題となる。

そこで次章以降では、どのようなネットワークアーキテクチャであれば、グループ指向通信を実現できるかを検討する。

3 ネットワークアーキテクチャの設計目標

本章では、まず、ネットワークアーキテクチャの設計目標を議論する。ネットワークアーキテクチャの設計目標として、通信速度や効率など性能面の設計目標と、柔軟性や安全性など機能面の設計目標が考えられる。

ネットワークの高速化といった性能面の設計目標は重要ではあるが、ハードウェアやソフトウェア技術の進歩によって解決できる部分も多いと考えられる。そこで、本稿では、特に機能面の設計目標に着目し、グループ指向通信のためのネットワークアーキテクチャの設計目標を議論する。

3.1 動的なエンティティ/グループのサポート

実社会のサービス・組織・団体等をネットワーク上にマッピングするためには、ネットワーク利用者が柔軟にエンティティやグループを操作できる必要がある。

新たなエンティティやグループを、動的に制限なく生成・削除できることや、既存のエンティティやグループの属性情報を、動的に制限なく変更できる必要がある。

また、既存のエンティティやグループに対して、その識別子を動的に制限なく生成・変更できることや、エンティティやグループの識別子に、動的に別名を付けられることが望ましい。また、エンティティやグループの識別子を、動的に公開 / 非公開にできるべきである。

3.2 アドレス演算のサポート

さまざまな社会活動をネットワーク化するためには、1 対 1 通信以外にも 1 対 N 通信や N 対 N 通信を実現する必要がある。グループ指向通信では「アドレス通信」によってこれらの通信を実現する。

従って、さまざまなエンティティやグループとの多様な通信を実現するために、情報の宛先アドレスとして「アドレス演算式」を記述できる必要がある。

3.3 エンティティ / グループのファインダビリティの実現

通信したいエンティティやグループを、迅速かつ容易に発見

できること (ファインダビリティ) は重要である。

適切なエンティティやグループを選択し、信頼性のある通信を実現するために、エンティティやグループの識別子や属性情報をキーとして、動的に確実にエンティティやグループを検索できる必要がある。

3.4 セキュリティの実現

ネットワーク利用者のニーズが高度化し、安全性への関心が高まっている。そのため、重要な個人情報のやり取りや、企業間取引などの機密情報のやり取りをセキュアに実現する必要がある。よって、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ではセキュリティが重要である。

まず、信頼できるエンティティとだけ通信するために、安全な方法でエンティティを認証し、動的かつ確実にアクセス許可を付与できる必要がある。

また同時に、通信内容を改竄されることを防止するか、少なくとも改竄されたことを確実に検出できる必要がある。

これらに加えて、エンティティやグループ間の通信が、予期しない第三者に干渉されないように、エンティティやグループが通信していることやその通信内容を、第三者のエンティティやグループから秘匿できる必要がある。

確実に相手に届く信頼性のある通信を実現するためには、エンティティやグループがアクティブであることを、リアルタイムに確実に確認できることが望ましい。

信頼性のある通信を実現するために、通信履歴 (形態・内容) が確実に記録・保存され、後からの追跡調査が可能であることが望ましい。

エンティティやグループ間で安全な通信を行うためには、通信内容を検疫し、ウィルスやスパムの排除が可能であることが望ましい。

4 ネットワークアーキテクチャの設計

本章では、前章の設計目標を満たすネットワークアーキテクチャを設計する。

4.1 前 提 条 件

本稿では、ネットワークアーキテクチャの設計にあたり、「コアネットワークはサービスプロバイダによって保有されていること」および「 IP ネットワークとの互換性は必須ではない」ことを前提とする。まず、これらの前提条件の妥当性を議論する。

本稿では、プロバイダ提供型 VPN フレームワーク [14] を前提とする。プロバイダ提供型 VPN フレームワークでは、コアネットワークはサービスプロバイダによって管理されているため、安全性を実現することが可能である。安全なネットワークを実現するためには、信頼の鎖をどのように実現するかが鍵となる。サービスプロバイダがコアネットワークを保有することにより、コアネットワークの安全性が可能となる。また、コアネットワーク内のネットワーク機器を、サービスプロバイダの管理下に置くことにより、ネットワークの監視 (トレーサビリティ) および不正ユーザの排除の実現が可能となる。

グループ指向通信は、IP とは大きく異なる通信形態である。1 章で議論したように、グループ指向通信のネットワークアーキテクチャに、既存の IP ネットワークとの互換性を持たせることは困難である。グループ指向通信では、アドレス演算式によって通信相手の指定が可能であり、N:N 通信も可能である。このような高度な通信を、IP ネットワークと同じアドレス体系や API (例えば、BSD ソケット API) で実現することは困難である。また前述のように、本稿では、コアネットワークはサービスプロバイダによって保有されていることを前提としている。このため、既存の IP ネットワークとの互換性は必ずしも必須ではないと考えられる。

4.2 回線交換 **vs** パケット交換

ネットワークアーキテクチャの設計について、通信モデルの観点から議論する。

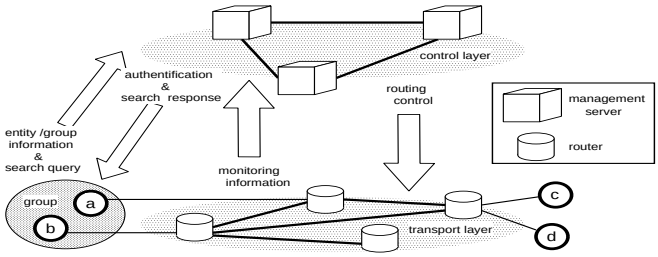

図 6: グループ指向通信のネットワークアーキテクチャ

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は、パケット交換型のネットワークであるべきであろう。グループ指向通信の大きな特徴として、アドレス演算によって、柔軟かつ動的な宛先アドレスの指定が可能であることが挙げられる。このような動的なアドレス演算を実現するネットワークアーキテクチャは、静的な回線交換型ではなく、動的なパケット交換型が適している。逆に言えば、アドレス演算のダイナミクスは、回線交換型のネットワークアーキテクチャには不適である。また、回線交換型のネットワークはステートフルであるため、エンティティ数やグループ数に関するスケーラビリティに問題がある。エンティティやグループを、自由に制限無く生成・変更・削除できるようにするためには、スケーラビリティの上でもパケット交換型が有利である。

4.3 核となるネットワーク技術

次に、パケット交換型のネットワーク上で、どのように設計目標を実現するかについて議論する。

通信の本質は情報を伝達することである。3 章に示した設計目標の大部分は、「どのように情報を伝達させるか」または「どのように情報の伝達を防ぐか」に帰着する。これはつまり、ネットワーク内での情報の到達を適切に制御することができれば、設計目標の大部分が実現される ということを意味している。

例えば、第三者のエンティティからの到達性を適切に制御することによって、不正なエンティティからのアクセスを防ぎ、安全性を高めることができる。また、エンティティからネットワークへの到達性を適切に制御することにより、エンティティのアクセス認証も実現できる。さらに、情報の到達性を特定のグループのエンティティ内に適切に制御することによって、閉域性を有するグループ間通信を実現できる。識別子の公開・非公開についても、エンティティの識別子への到達性を適切に制御することによって実現が可能である。

4.4 階層構造化されたネットワークアーキテクチャ

以上の議論より、情報の到達性制御が、設計目標を実現するための核となる技術であることが明らかとなった。しかし、到達性制御によってさまざまな機能を実現すると、ネットワークの機能が肥大化し、結果としてネットワークアーキテクチャが複雑になってしまう恐れがある。

ネットワークアーキテクチャの複雑化を防ぐためには、転送系と制御系を分離する、つまり、ネットワークアーキテクチャを「転送プレーン」と「制御プレーン」の階層構造によって実現することが望ましいと考えられる (図 6)。

つまり、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は、IP のような転送系と制御系を統合したフラットなネットワークアーキテクチャではなく、MPLS のような転送系と制御系を分離したネットワークアーキテクチャとすべきと考えられる。

転送プレーンはパケット転送のためのレイヤであり、パケットのスイッチングおよびトラヒックの監視を行う。一方、制御プレーンはネットワーク制御のためのレイヤであり、到達性制御 (パケットのスイッチング規則の制御)、エンティティおよび

グループの管理、識別子および属性情報の管理を行う。

4.5 転送プレーン

転送プレーンは、高速にパケットのスイッチングを行う複数のルータによって構成される。

転送プレーンにおけるルータのルーティングテーブルは、制御プレーンによって決定される。グループの生成や削除は、ルーティングテーブルの変更によって実現する。同様に、ルーティングテーブルを適切に管理することによって、不正なエンティティから他のエンティティへの到達性を制限し、不正な利用を排除することができる。また、ルーティングテーブルを適切に管理することによって、グループに属するエンティティ以外への到達性を制限し、グループ間通信を実現する。

転送プレーンでは、追跡可能性 (トレーサビリティ) や通信内容の検疫を実現するために、トラヒックの監視を行う。パケットのペイロードをモニタリングすることにより、通信内容の検疫を実現する。これにより、ウィルスやスパムの排除なども可能となる。ただし現実的には、通信速度の低下を防ぐために、特定のエンティティ / グループに対するトラヒックのみをモニタリングすべきだと考えられる。ここで、モニタンリングしたパケットのペイロードを制御プレーンに通知し、制御プレーンがそれらの情報を適切に保存することにより、追跡可能性 (トレーサビリティ) の実現も可能となる。

また、エンティティから送信されるトラヒック量を監視することにより、エンティティがアクティブかどうかを検出することができる。この情報を制御プレーンに通知することにより、エンティティの存在確認 (プレゼンス) の実現が可能である。

4.6 制御プレーン

制御プレーンは、到達性制御や、エンティティ / グループの管理を行う複数の管理サーバによって構成される。

制御プレーンの管理サーバは、転送プレーンにおけるルータのルーティングテーブルを制御する。例えば、グループが生成 / 削除された時には、ルーティングテーブルを更新することによって、グループの生成 / 削除を実現する。

また、新たにエンティティがネットワークに接続する場合は、制御プレーンの管理サーバがエンティティを認証する。認証が得られた場合のみ、転送プレーンにおけるルータのルーティングテーブルを更新し、エンティティのアクセスを許可する。

制御プレーンの管理サーバは、エンティティやグループの管理を行う。エンティティ / グループの生成・変更・削除の時には、エンティティ / グループのディレクトリ情報を更新する。例えば、エンティティの生成時には、エンティティの識別子がディレクトリ情報として新たに登録される。同様に、エンティティ/グループの属性情報が登録・変更された時には、エンティティ / グループのディレクトリ情報を更新する。転送プレーンから通知されるエンティティのプレゼンス情報も、エンティティ / グループのディレクトリ情報として登録される。エンティティ / グループに関する情報を一括してディレクトリで登録・管理することにより、エンティティやグループの検索も実現できる。

このようなディレクトリ情報を利用することにより、アドレス演算を実現する。宛先アドレスとして、アドレス演算式が記述されたパケットがルータに到着すると、制御プレーンは、アドレス演算式の計算結果をもとにルータのルーティングテーブルを更新する。エンティティ / グループのディレクトリ情報をデータベースの形式で格納し、データベースの集合演算を利用することにより、アドレス演算式の計算結果を容易に求めることができる。

5 まとめと今後の課題

本稿では、「グループ指向通信」という新しい通信形態を提案した。グループ指向通信とは、従来の 1 対 1 通信とは異なり、グループ間の通信を基本とする新しい通信形態である。グループ指向通信は、N 対 N 通信 (グループ通信) の一種であるが、1 対 1 通信や 1 対 N 通信を含む、すべての通信をグループ間の通信によって実現するという点に特徴がある。本稿では、既存の IP との比較によって、グループ指向通信のメリットを定性的に議論した。また、グループ指向通信を実現するためのネットワークアーキテクチャを設計した。その結果、グループ指向通信のためのネットワークアーキテクチャは、(1) パケット交換型であり、(2) 到達性制御が核となる技術であること、(3) 制御プレーンと転送プレーンの二層構造を取るべきであること、などを示した。

今後の課題としては、本稿で設計したグループ指向通信のためのネットワークアーキテクチャのさらなる詳細検討や、グループ指向通信プロトコルの開発、数学的解析によるグループ指向通信の特性分析などが挙げられる。

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] 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/adapter.Main`.

[3] 総務省, “平成 16 年度版 情報通信白書,” May 2004. available at `http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/html/G2702300.html`.

[4] 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.

[5] A. El-Sayed, L. Roca, V. andMathy, and Rhone-Alpes, “A survey of proposals for an alternative group communication service,” *IEEE Network*, vol. 17, pp. 46–51, Jan. 2003.

[6] R. van Renesse, K. P. Birman, and S. Maffeis, “Horus: a flexible group communication system,” *Communications of the ACM*, vol. 39, no. 4, pp. 76–83, 1996.

[7] 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.

[8] M. Castro, P. Druschel, A.-M. Kermarrec, and A. Rowstron, “Scribe: a large-scale and decentralized application-level multicast infrastructure,” *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 1489–1499, Oct. 2002.

[9] S. Banerjee, C. Kommareddy, K. Kar, B. Bhattacharjee, and S. Khuller, “Construction of an efficient overlay multicast infrastructure for real-time applications,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 2, pp. 1–11, Apr. 2003.

[10] M. Kwon and S. Fahmy, “Topology-aware overlay networks for group communication,” *Proceedings of the 12th international workshop on network and operating systems support for digital audio and video*, pp. 127–136, May 2002.

[11] I. R. B. Warehouse, “SQL Self-Study Guide.” `http://www-06.ibm.com/jp/software/data/developer/library/manual/informix/docs/62rbw/sqlself.pdf`, Sept. 2002.

[12] R. Boivie, N. Feldman, W. Livens, D. Ooms, and O. Paridaens, “Explicit Multicast (Xcast) Basic Specification,” *Internet-Drafts, Jan*, pp. 1–29, June 2002.

[13] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, “Internet Group Management Protocol, Version 3,” *Request for Comments (RFC) 3376*, Oct. 2002.

[14] M. Carugi and D. McDysan, “Service requirements for layer 3 provider provisioned virtual private networks (PPVPNs),” *Request for Comments (RFC) 4031*, Apr. 2005.