

## プライベートサービスを実現する広域アクティブネットワークアーキテクチャ

柏 大, Eric Y. Chen, 富士 仁, 岡部 恵一

NTT 情報流通プラットフォーム研究所  
神奈川県横須賀市光の丘 1-1

TEL: 0468-59-2867 / kashiwa@nttmhs.tnl.ntt.co.jp

あらまし ネットワークサービス事業者には,新たな付加価値サービスの提供が望まれている。今後は,これまでエンドユーザ側で管理していた機能をネットワーク側で提供し,且つ,エンドユーザからカスタマイズ可能な“プライベートサービス”が実現していくものと考えられる。

本稿では,プライベートサービスを広域ネットワーク上で実現するためのアーキテクチャ:WANAPS (Wide-area Active Network Architecture for Private Services)を提案する。WANAPSは,サービス管理者によるプライベートサービスの適切なネットワーク装置への導入,導入後のサービス制御,および,サービス管理者,エンドユーザ両者からのサービス操作を実現する。更に,サービスコンポーネントの協調動作により,広域ネットワークサービスの特徴を生かした分散協調型の付加価値サービスを実現可能としている。

キーワード アクティブネットワーク, ネットワークサービス,  
ネットワークアーキテクチャ

## A Wide-area Active Network Architecture for Private Services

Dai Kashiwa, Eric Y. Chen, Hitoshi Fuji, Keiichi Okabe

NTT Information Sharing Platform Laboratories  
1-1, Hikarinooka Yokosuka-Shi Kanagawa, 239, Japan  
TEL: +81 468 59 2867 / kashiwa@nttmhs.tnl.ntt.co.jp

**Abstract** Network services are evolving from the traditional “black-box” model towards the “open-and-programmable” one, in which end users can implement what we call Private Services and customize the way the network handles their traffic. By shifting some computation to the network tactically, these services can significantly lighten the workload of system administrators.

This paper proposes a novel network architecture, WANAPS (Wide-area Active network Architecture for Private Services), designed for wide-area network service platforms. The WANAPS helps service administrators to identify network nodes suitable for the deployment of new private services and provides both administrator-level and user-level control of these services. The WANAPS also allow distributed collaboration by enabling communications among different service components.

key words active network, network service, network architecture

## 1. はじめに

ネットワークサービス事業者には、新たな付加価値サービスの提供が望まれている。IP (Internet Protocol)技術の普及期には、ネットワークサービスはLAN間接続やインターネット接続を実現するアクセスサービスが中心で、高速化、低価格化が進んで急速に普及していった。近年では、ネットワークサービスは高速化、低価格化に加えて、高機能化が進んでいる。高機能化されたネットワークサービスの例として、物理的に複数の利用者で共用するネットワークを、論理的にエンドユーザ毎に分離し、高セキュリティ・高品質を提供するVPNサービス等が挙げられる。更に最近では、エンドユーザ側で負担になっている機能をネットワークサービスとして提供する“付加価値”サービスが次々に生まれている。ASP (Application Service Provider) や CSP (Commerce Service Provider)はアプリケーションレベルで付加価値を提供しているが、今後は、ネットワークレベルで付加価値を提供し、これまでエンドユーザ側で管理していた機能をネットワーク側で提供するサービスも実現していくものと考えられる。これらのネットワークサービスがこれまでのサービスと大きく異なる点は、これまでエンドユーザ側で管理していた機能をネットワーク側で提供するために、エンドユーザの管理ポリシーや使い方によってサービス機能をカスタマイズする必要がある、ということである。

本稿では、エンドユーザ側の負担を減らす、ネットワークレベルでの付加価値サービスを“プライベートサービス”として定義し、これを広域ネットワーク上で実現するための広域サービス基盤アーキテクチャ:WANAPS (Wide-area Active Network Architecture for Private Services)を提案する。WANAPSは、ネットワークを高機能化するための技術であるアクティブネットワーク技術を適用し、広域サービス基盤に適した、プライベートサービスコンポーネント管理方法の特徴としている。この管理方法では、サービス管理者によるプライベートサービスの適切なネットワーク装置への導入、導入後のサービス制御、および、サービス管理者、エンドユーザ両者からのサービス操作(カスタマイズ)を実現する。更に、コンポーネント間コミュニケーションによるサービスコンポーネントの協調動作を可能にすることで、エンドユーザ側の負担を減らすだけでなく、広域ネットワークサービスの特徴を生かした分散協調型の付加価値サービスを実現可能としている。

以下、2章では、プライベートサービスの定義を説明し、3章では、アクティブネットワーク技術の広域サービス基盤への適用性について述べる。4章では提案アーキテクチャについて述べ、5章では提案アーキテクチャの既存研究との比較評価を行い、6章でまとめと今後の課題を整理する。

## 2. プライベートサービス

プライベートサービスとは、エンドユーザ側で負担になっている機能をネットワークサービスとして提供することを目的とした新しい概念として提案するもので、本稿では以下のように定義する。

「エンドユーザがサービス機能をカスタマイズし、自分専用の使い方が可能なネットワークサービス」

プライベートサービスで提供すべき機能としては、次章で説明する“アクティブネットワーク”に関連する研究[1][2][3][4][5][11][12][13]での事例が参考になる。アクティブネットワークに関連する研究の中では、帯域制御機能、セキュリティ機能、ルーティング高度化機能等の分野における様々なネットワークアプリケーションを提案しており、これらはプライベートサービスの有力な候補となり得る。様々な提案アプリケーションの中から、ネットワークサービスとして実現することでエンドユーザの負担を減少させ、プライベートサービスとして有効と考えられる例を表1に示す。

表1 プライベートサービスの例

サービス種別	サービス内容
帯域制御	RT Stream Adaptation
	Universal Compression
	Media Conversion
	Mixing Sector Data
セキュリティ	Moving Firewall
	Back Tracking
	Authorization
	Authentication
ルーティング高度化	Active Cryptography
	Encrypted Multicast
	Enhanced NAK
	Enhanced Retransmission
	Intelligent Packet Discard
	Intelligent Routing
	Customized Routing
	Enhanced Mobile IP
Replica Selection	

## 3. アクティブネットワーク技術の適用性

### (1) 既存研究の動向

アクティブネットワーク技術は、ネットワーク装置を高機能化し、アプリケーション層まで含めた処理機能の提供、および、処理機能の動的なカスタマイズを可能とするための技術であり、プライベートサービスを実現するネットワークアーキテクチャを構築する上で有効な手段を提供する。アクティブネットワーク技術に関連した取り組みは、処理機能を提供する“プログラム”の動作方法によって、以下の二つのアプローチに分類される。各々のプログラムの動作方法、および、特徴について以下に述べる。

#### ・In-bandアプローチ

エンドユーザのパケット内に格納されたプログラムが、パケットを転送するネットワーク装置で呼び出されることでエンドユーザに付加価値機能を提供する。プログラムをエンドユーザ自らが書き換えることで、エンドユーザ毎・アプリケーション毎にカスタマイズされたネットワーク利用が実現される。アプリケ

ーション例として、QoS-awareルーティング[3]や信頼性マルチキャスト[11]等が提案されている。In-bandアプローチは、高いカスタマイズ性等の長所を持つ一方で、プログラミングの困難さ、セキュリティ確保の困難さ等の短所を持っている。

・ Out-of-bandアプローチ

プログラムを予めネットワーク装置に導入しておく、エンドユーザのパケット転送時にパケット内に格納されたアプリケーション識別情報に対応するプログラムが呼び出されることで、エンドユーザに付加価値機能を提供する。プログラムをアプリケーション管理者等が書き換えることで、エンドユーザ毎・アプリケーション毎にカスタマイズされたネットワーク利用が実現される。アプリケーション例として、動的ポリシーネットワークキング[4]や、移動型ファイアウォール[5]等が提案されている。Out-of-bandアプローチは、In-bandアプローチとは逆で、プログラミングの容易さやセキュリティ確保の容易さ等の長所を持つ一方で、低いカスタマイズ性等の短所を持っている。

**(2) 広域プライベートサービス基盤への適用**

In-bandアプローチの取り組みでは、パケットに格納するのに適した軽量、安全なプログラム言語の研究が盛んに行われているが[2][3]、上記で述べた、パケットに挿入するプログラムのプログラミングの手間をどうやって低減するか、セキュリティをどうやって守るか、等に対する解決法は未成熟であり、広域サービス基盤に適用するための課題は多い。また、In-bandアプローチの高いカスタマイズ性を生かした革新的なネットワーク利用法はまだあまり示されていない。

一方、Out-of-bandアプローチの取り組みでは、ノードアーキテクチャ[6][7]やプログラム動作モデルウェア[8]、ネットワークプロセッサ等の要素技術の確立が進んでいる。これらを利用することで、プログラムを導入することで動的に提供機能をカスタマイズできるネットワーク装置が実現されようとしている。

広域プライベートサービス基盤としてアクティブネットワーク技術を適用するためには、これらの要素技術を組み合わせた統合的なアーキテクチャが必要になる。近年、アクティブネットワーク技術を広域ネットワーク上に適用するためのアーキテクチャの検討が始まっているが[14]、分散配置されたネットワーク装置へのプログラムの導入や、導入後のエンドユーザからの操作法等、サービス管理に関してプライベートサービスを提供するために必要な機構を組み込んだアーキテクチャの提案はまだ無い。

**4. 広域アクティブネットワークアーキテクチャ**

本章では、プライベートサービスを提供する広域サービス基盤に適用するための、広域アクティブネットワークアーキテクチャ：WANAPS(Wide-area Active Network Architecture for Private Service)を提案する。WANAPSでは、プライベートサービス機能を提供するプログラムを”サービスコンポーネ

ト”と呼び、これらを Out-of-band でネットワーク装置に導入することでエンドユーザにプライベートサービスを提供する。また、前章で述べた課題を解決する方法として、広域サービス基盤に適した”サービスコンポーネント管理方法”を採り入れている。以下では、WANAPSの現在の検討状況を述べる。

**(1) 概要**

WANAPSの概観を図1に示す。

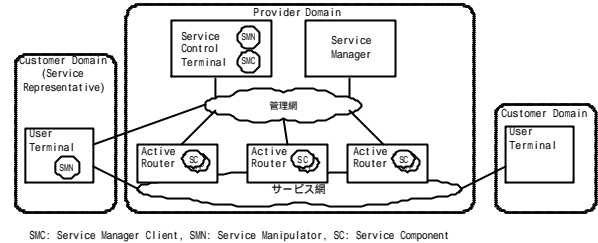


図1 WANAPS 概観

WANAPSでは、サービス機能を提供するサービスコンポーネント(SC)を広域ネットワーク上に分散配置されたアクティブルータ(Active Router)に導入し、アクティブルータが、転送するパケットの属性(送信元/宛先アドレス、プロトコル番号等)に応じて、対応するサービスコンポーネントを動作させることでエンドユーザにプライベートサービスを提供する。パケット属性とサービスコンポーネント間の対応は、予めエンドユーザとサービス管理者間で取り交わした契約(contract)に従って決定される。

アクティブルータは、エンドユーザパケットに対してプライベートサービス機能を提供する高機能ルータであり、エンドユーザパケットの送受信を行うサービス網とサービスコンポーネントの管理を行う管理網とに接続される。サービスマネージャ(Service Manager)は、サービスコンポーネントの導入、管理を行うことでサービスを制御するサーバであり、管理網に接続される。アクティブルータとサービスマネージャについては、次節以降で詳細に述べる。サービス管理端末(Service Control Terminal)は、サービスマネージャと接続してサービス制御クライアント(SMC: Service Manager Client)からサービス制御を行い、また必要に応じて、サービスマニピュレータ(SMN: Service Manipulator)からサービス操作を行うための端末であり、管理網に接続される。エンドユーザ端末(User Terminal)は、プライベートサービスの利用者端末であり、サービス網に接続される。プライベートサービスの代表利用者(Service Representative)は、エンドユーザ端末を管理網に接続し、サービスマニピュレータを利用することでサービス操作を行うことが可能となる。

WANAPSでは、サービス管理を、”サービス制御”と”サービス操作”という二つの概念に分けて扱っている。サービス制御は、サービスコンポーネントの導入・移動等のサービス性能やセキュリティに関わる動作を表し、サービス操作は、動作ポリシー変更・パラメータ変更等のサービス内容のチューニングに関する動作を表す(表2)。上記で述べたように、サービス

制御はサービス管理者が実施可能，サービス操作は，エンドユーザとサービス管理者の両者が実施可能となっており，セキュリティを確保しつつ，プライベートサービスのカスタマイズ性を提供することを可能としている。

表 2 サービス制御とサービス操作

動作	提供部位	内容
サービス制御	サービスマネージャ	サービスコンポーネント導入/移動/削除，開始，停止等
サービス操作	サービスマニピュレータ	スレッド呼び出し，パラメータ変更，動作レポート読み出し等

上記で説明してきた各構成要素間の関係を表す，WANAPSにおけるUML表現によるプライベートサービスの情報モデルを図2に示す。

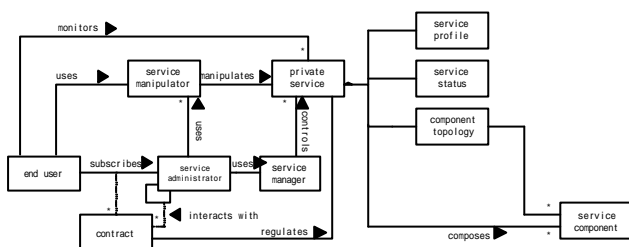
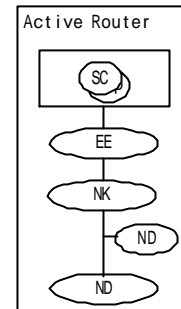


図 2 プライベートサービスの情報モデル

WANAPS では，プライベートサービス (private service) は，複数のサービスコンポーネント (service component) ,属性情報 (service profile) ,動作状態 情報 (service status) , トポロジー情報 (component topology) から構成される。プライベートサービスは，サービスマネージャ (service manager) からのサービス制御と，サービスマニピュレータ (service manipulator) からのサービス操作が可能である。サービス管理者 (service administrator) はサービスマネージャ ,サービスマニピュレータを使ったサービス制御，サービス操作が可能であり，エンドユーザ (end user) は，サービスマニピュレータを使ったサービス操作のみが可能である。エンドユーザとサービス管理者との間には，プライベートサービスの利用に関する契約 (contract) が存在し，契約値によってプライベートサービスの動作は制限を受けることになる。

## (2) アクティブルータ

アクティブルータは，サービスコンポーネントを動的に導入して様々なサービス機能を提供する高機能ルータである。エンドユーザによってカスタマイズされたサービスコンポーネントを導入することにより，プライベートサービスの提供が可能になる。図3にアクティブルータの構成を示す。



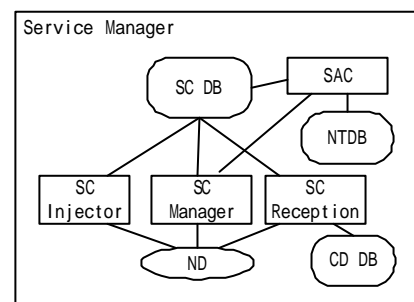
SC: Service Component, EE: Execution Engine, NK: Node Kernel, ND: Network Device

図 3 アクティブルータ

- サービスコンポーネント(SC): 導入された様々なサービスコンポーネント。エンドユーザパケットの到着に応じて実行環境部から適宜呼び出され，エンドユーザパケットに対してサービス機能を提供する。
- 実行環境(EE): サービスコンポーネント実行のための実行環境。サービスコンポーネントの実行，管理機能(開始，停止，移動等)を提供する。
- ノードカーネル(NK): エンドユーザパケットの基本操作機能(取得，複製，修正，再送信等)を提供するカーネル。エンドユーザ毎のリソース分割・保証を提供する。
- ネットワークデバイス(ND): エンドユーザパケットおよびサービス制御/操作パケットを送受信するためのデバイス。

## (3) サービスマネージャ

サービスマネージャは，サービスコンポーネントの格納，導入，管理を行うサーバであり，図4に示す以下の部位から構成される。



SC DB: Service Component DataBase,  
SAC: Service Area Controller,  
NT DB: Network Topology DataBase,  
CD DB: Certificated Developer DataBase,  
SC Injector: Service Component Injector,  
SC Manager: Service Component Manager,  
SC Reception: Service Component Reception,  
ND: Network Device

図 4 サービスマネージャ

- サービスコンポーネントデータベース(SCDB): 認証済みのサービスコンポーネントを格納するデータベース。
- サービスエリアコントローラ(SAC): サービスコンポーネントを動作させるアクティブルータの範囲(サービスエリア)を判断するためのオブジェ

- ・ ネットワークトポロジデータベース(NTDB)：アクティブルータ，サービスコンポーネントのトポロジー，および，エンドユーザの収容情報を管理するデータベース
- ・ 認証済開発者データベース(CDDB)：サービスコンポーネントを開発可能な正規の開発者情報を格納するデータベース
- ・ サービスコンポーネントインジェクタ(SC Injector)：サービスコンポーネントをアクティブルータに導入する操作を行うポータル
- ・ サービスコンポーネントマネージャ(SC Manager)：アクティブルータ上のサービスコンポーネントの管理を行うオブジェクト
- ・ サービスコンポーネントレセプション(SC Reception)：サービスコンポーネントの開発者からの受入を行うポータル
- ・ ネットワークデバイス(ND)：サービス制御パケットを送受信するためのデバイス

#### (4) サービスコンポーネント管理方法

WANAPSは，広域サービス基盤に適した，サービスコンポーネント管理方法の特徴としている。サービスマネージャからアクティブルータへのサービスコンポーネントの導入時には，サービスマネージャが，導入すべきアクティブルータ候補を特定し，必要に応じてエンドユーザが選択する方式を採っており，広域サービス基盤上に存在する多数のネットワーク装置の適切な位置への導入を可能としている。また，導入後のサービス制御，サービス操作は，“コンポーネントネットワーク”と呼ばれる，サービス毎に構築されるサービスマネージャとサービスコンポーネント間を結ぶネットワークを使って行われ，サービスマネージャからのサービス制御と，サービスマネージャからのサービス操作を可能としている。更に，コンポーネントネットワークを使ったメッセージ交換により，広域ネットワークサービスとしての特徴を生かした高付加価値機能の実現を可能としている。以下，サービスコンポーネントのアクティブルータへの導入方法，および，導入後の制御・操作方法について詳細に述べる。

##### (i) 導入方法

WANAPSでは，以下の3つのステップを行うことで，プライベートサービスを構成するサービスコンポーネントがアクティブルータへ導入される。

サービスコンポーネントが開発者によって作成され，サービスマネージャに送信される。サービスマネージャは，開発者が保存を申請したサービスコンポーネントをセキュリティ，インタフェースの利用ルールなどの面で検査し，検査が通ればサービスコンポーネントデータベースに保管する。この際，開発者は，予め登録されており，保存を申請した際にその登録情報と比較して，正規の登録者であるかみなされたときに保存ができる。利用者からサービスマネージャに，プライベ

ートサービスの利用要求が送信されると，サービスマネージャは，サービスエリアコントローラが“サービスエリア”を判断し，サービスコンポーネントインジェクタを通して，サービスエリア内の適切なアクティブルータにサービスコンポーネントを導入する。

上記で述べた“サービスエリア”の概念について説明する。サービスコンポーネントの動作位置は，サービスの種類や属性によって変化する。WANAPSでは，サービスの種類や属性によって変化する“サービスコンポーネントが動作すべきアクティブルータの範囲”を“サービスエリア”という概念で管理する。表1に挙げたプライベートサービス例の動作位置を整理すると表3のようになる。

表3 サービス別サービスコンポーネント動作位置

サービス種別	サービス内容	サービスエリア	
		動作範囲	動作密度
帯域制御	RT Stream Adaptation	PATH	Any
	Universal Compression	PATH	Any
	Media Conversion	PATH	Any
	Mixing Secors Data	PATH	Any
セキュリティ	Moving Firewall	EDGE/WHOLE	Any
	Back Tracking	EDGE/WHOLE	Any
	Authorization	WHOLE/EDGE	Any
	Authentication	WHOLE/EDGE	Any
	Active Cryptography	EDGE/WHOLE	Any
ルーティング高度化	Encrypted Multicast	EDGE	ALL
	Enhanced NAK	PATH	ALL
	Enhanced Retransmission	PATH	ALL
	Intelligent Packet Discard	WHOLE	ALL
	Intelligent Routing	WHOLE	ALL
	Customized Routing	WHOLE	ALL
	Enhanced Mobile IP	WHOLE	ALL
Replica Selection	WHOLE	ALL	

表3に示すように，サービスエリアは，“動作範囲”および“動作密度”の2つの属性から構成される。“動作範囲”はサービスコンポーネントが動作する候補となるアクティブルータの範囲を表したもので，“PATH”はサービスの参加者間を結ぶパスを表し，“EDGE”はサービスの参加者を収容する境界アクティブルータを表し，“WHOLE”はサービスを提供する全アクティブルータを表している。“動作密度”は上記範囲の中でサービスコンポーネントが動作すべきアクティブルータの密度を表し，“ALL”は範囲内全アクティブルータを表し，“ANY”は範囲内の任意のアクティブルータを表している。サービスマネージャでは，サービスコンポーネントをサービスコンポーネントデータベース(SCDB)に登録する際に，サービスエリアの属性として上記動作範囲および動作密度の情報を併せて登録する。

のプライベートサービスの利用要求時には，まず，サービスエリアコントローラ(SAC)がサービスエリア属性値と利用者の収容情報から，要求されたプライベートサービスのサービスエリアを特定する。この際，“EDGE”属性であれば，サービスの参加エンドユーザを収容する境界アクティブルータを候補とし，“WHOLE”属性であれば，サービス参加者と同一契約者を収容する境界アクティブルータとそれらを接続する中間アクティブルータを候補とし，“PATH”属性であれば，サービスの参加エンドユーザを収容する境界アクティブルータとルーティング情報から算出された境界アクティブルータ間経路上のアクティブル

ータを候補とする。次に、SACは“動作密度”属性を検査し、“ALL”であれば、サービスエリア内の全アクティブルータを、サービスコンポーネントを導入すべきルータとして選択し、“ANY”であれば、エンドユーザにサービスエリア情報(ルータトポロジー、混雑状況等)を示した上で、サービスコンポーネントを導入すべきルータの選択を依頼する。選択後、サービスコンポーネントインジェクタ(SC Injector)が選択されたアクティブルータにサービスコンポーネントを導入する。導入は、管理網を通して“サービス導入パケットフォーマット”を用いて行われる。このパケットフォーマットには、サービスコンポーネント、および、サービス動作情報、認証情報等が格納され、サービスマネージャから各アクティブルータへ送信される。

(ii)導入後の制御・操作方法

サービスコンポーネントの導入後の制御は、“コンポーネントネットワーク”と呼ばれるサービス毎に構築される、サービスマネージャとサービスコンポーネント間を結ぶネットワーク(図5)を使って行われる。

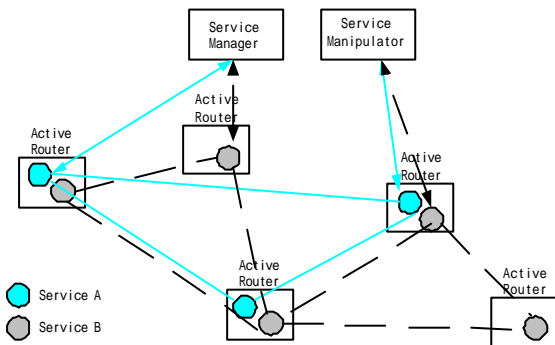


図5 コンポーネントネットワーク概念図

コンポーネントネットワークは、サービスが提供されている間動的に再構築されるもので、サービスコンポーネント間協調動作のためのコミュニケーションパスを提供するものである。コンポーネントネットワークを使ったコミュニケーションは、サービスコンポーネントが自律分散的に行うものであり、サービス制御情報の伝達や協調動作のためのメッセージ交換等が行われる。この自律分散型モデルの適用により、サービスマネージャ・サービスマニピュレータのサービス管理負荷は低減し、更に、サービスコンポーネントの協調動作によって、広域ネットワークサービスとしての特徴を生かした高付加価値機能が実現可能となる。協調動作による高付加価値機能の例として、分散DDoS アタック対策[9]や、P2P 型情報共有等が提案されているが、今後、プライベートサービスとしても注目が集まっていくものと考えられる。コンポ-ネットワークでは、サービスマネージャからのサービス制御情報、サービスマニピュレータからのサービス操作情報が、“サービス制御パケットフォーマット”、“サービス操作パケットフォーマット”を用いてアクティブルータ間で送受信される。これらのパケットフォーマットには、サービスコンポーネントの制御情報、操作情報、および 認証情報が格納される。

コンポーネントネットワークにおいて、メッセージを交換する方式には、以下の要求条件が求められる。

- ・ メッセージが誤り無く届く信頼性
- ・ 多数のコンポーネントに対応するスケーラビリティ
- ・ アクティブルータ以外のレガシールータを越しのメッセージ交換

現在、コンポーネントネットワークのメッセージ交換法に関しては詳細を検討中であるが、これらの要求条件を満たす方式として、信頼性マルチキャストプロトコル[10]の利用を候補として考えている。

5. 評価

WANAPSの、サービスコンポーネント管理方法における、広域サービス基盤としての有効性を評価するため、サービスコンポーネントの導入方法、制御・操作方法、コミュニケーション方法に関して代表的なアクティブネットワークシステム/プロジェクトと比較した結果を表4に示す。尚、各システム/プロジェクトにおいて、例えばWANAPSの“サービスコンポーネント”に対応する用語として、“コード”[11]、“ボックス”[12]、“アクティブプログラム”[13]など様々な呼び方が存在するが、表4では比較の統一性のためにWANAPSでの用語に置き換えて記述してある。

表4から、サービスコンポーネントの導入方法、制御・操作方法、コミュニケーション方法に関して、既存のシステム/プロジェクトでは未定義または非常にシンプルな方法を採用しており、広域サービス基盤への適用は難しいことが分かる。

表4 サービスコンポーネント管理方法の比較

システム/プロジェクト名	アプローチ	導入方法	制御・操作方法	コミュニケーション方法
ANTS	In-band	エンドユーザがパケット内に挿入	パケット内のサービスコンポーネントは制御・操作不可能	アクティブルータ内サービスコンポーネントを媒体として可能
PLAN	In-band	エンドユーザがパケット内に挿入	パケット内のサービスコンポーネントは制御・操作不可能	アクティブルータ内サービスコンポーネントを媒体として可能
DAN	Hybrid	パケットの到着時にアクティブルータがサーバからダウンロード	未定義	未定義
Netscript	Hybrid	サービス管理者が位置を指定してアクティブルータへダウンロード	サービス管理者からの制御・操作可能	未定義
WANAPS	Out-of-band	サービスマネージャが導入候補位置を特定し、サービス管理者がその中から選択したアクティブルータへダウンロード	コンポーネントネットワークを使ったサービスコンポーネントは制御・操作と、エンドユーザからの操作	コンポーネントネットワークを使ったメッセージ交換

WANAPSでは、導入方法に関して、サービスマネージャが、導入すべきアクティブルータ候補を特定し、必要に応じてエンドユーザが選択する方式を採っており、広域サービス基盤上に存在する多数のネットワーク装置の適切な位置への導入を可能としている。また、制御・操作方法に関しては、サービス管理者とエンドユーザとで権限を分け、サービスコンポーネントの導入・移動等のサービス性能やセキュリティに関わる動作(サービス制御)はサービス管理者のみが実施可能とし、動作ポリシー変更・パラメータ変更し等のサービス内容のチューニングに関する動作(サービス操作)は利用者から実施可能としており、これにより、利用者からの不正なサービス操作やリソースの不正使用等のセキュリティ侵害を防ぎつつ、プライベートサービスのカスタマイズ性を提供することを可能としている。更に、コミュニケーション方法に関しては、

コンポーネントネットワークの構築によるメッセージ交換により、多数のコンポーネント間で同時に知識を共有し、協調動作による広域ネットワークサービスとしての特徴を生かした高付加価値サービスの提供を可能としている。

## 6. まとめと今後の課題

本稿では、“プライベートサービス”を定義し、これを広域ネットワーク上で実現するためのアーキテクチャ:WANAPSについて提案を行った。WANAPSは、プライベートサービスを構成するサービスコンポーネントの管理方法に関して、適切なネットワーク装置への導入、セキュア且つカスタマイズ可能な制御・操作、コンポーネント間コミュニケーションによる協調動作、を可能としており、広域サービス基盤に適した特徴を有している。

我々は現在、以下の検討課題について取り組んでいる。

- ・ コンポーネントネットワークメッセージ交換の詳細プロトコル設計、詳細メッセージフォーマット定義
- ・ アクティブルータのリソース保証機構の詳細化
- ・ アクティブルータの高速化

今後は、上記課題に取り組みながら、WANAPSの詳細設計と、アクティブルータ、サービスマネージャ等の試作を並行して行っていく予定である。

## 参考文献

- [1] D.L.Tennenhouse, J.M.Smith, W.D.Sincoskie, D.J.Wetherall, and G.J.Minden, "A Survey of Active Network Research," IEEE Communications Magazine, pp.80-86, January 1997.
- [2] Michael Hicks, Pankaj Kakkar, Jonathan T. Moore, Carl A. Gunter, and Scott Nettles, "PLAN: A packet language for active networks," In Proceedings of the International Conference on Functional Programming Languages. ACM, 1998.
- [3] Ano, S. et al, "QoS Routing and Congestion Management over Stream Code-based Active Internetworking System," IEICE Transactions on Communications, Vol.E-84-B, No.6, June 2001.
- [4] Kei Kato, Masaru Ishizuka, and Shugo Shiba, "Active Policy Networking," WTC T6, May 2000.
- [5] Eric Y. Chen and Hitoshi Fuji, "A Security Framework for Agent-Based Active Networks", Proceedings of M2USIC'2000, Petaling Jaya, Malaysia, October 2000.
- [6] Biswas, J., et al., "The IEEE P1520 Standards Initiative for Programmable Network Interfaces" IEEE Communications Magazine, Special Issue on Programmable Networks, October, 1998.
- [7] FAIN Consortium, FAIN: Future Active IP Networks, Project IST 10561 FAIN, <http://www.ist-fain.org>.
- [8] BANG - The Broadband Active Network Generation project. <http://www.fokus.gmd.de/research/cc/glone/projects/bang/>
- [9] David Moore, Geoffrey Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity," to appear in the 2001 USENIX Security Symposium.
- [10] T. Sano, N. Yamanouchi, T. Shiroshita, and O. Takahashi. *Flow and congestion control for bulk reliable multicast protocols -- toward coexistence with tcp*. RM meeting, Sept. 1997. Available via <http://info.isl.ntt.co.jp/rmtp/rmtpdesc.ps.gz>
- [11] David J. Wetherall, John Guttag, and David L. Tennenhouse. ANTS: A Toolkit for Building and Dynamically Deploying Network Protocols. In IEEE OPENARCH, April 1998.
- [12] Da Silva, S., Florissi, D. and Yemini, Y., "NetScript: A Language-Based Approach to Active Networks", Technical Report, Computer Science Dept., Columbia University January 27, 1998.
- [13] D. Scott Alexander. Alien: A Generalized Computing Model of Active Networks. PhD thesis, University of Pennsylvania, to appear December 1998.
- [14] Marcus Brunner, Bernhard Plattner, and Rolf Stadler, "SERVICE CREATION AND MANAGEMENT IN ACTIVE TELECOM NETWORKS," Communication of the ACM, Vol.44, No.4, April 2001.