社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＭＢＬ－33（６）
2005／5／25

セッション層アーキテクチャにおけるフロー情報を用いた通信資源管理機構

栗田　弘之†　　金子　晋丈†　　森川　博之††　　青山　友紀†

† 東京大学大学院情報理工学系研究科
〒 113-8656 東京都文京区本郷 7-3-1
†† 東京大学大学院新領域創成科学研究科
〒 277-8582 千葉県柏市柏の葉 5-1-5
E-mail: †{kuri,kaneko,mori,aoyama}@mlab.t.u-tokyo.ac.jp

あらまし　現在，通信機器の利用形態やネットワークへのアクセス形態が多様化し，通信資源管理における課題が数多く存在する．そのためそれぞれのネットワークに適した柔軟なポリシーに従って通信資源を管理することが求められ，筆者らはその実現にあたってフロー情報に注目した．フロー情報はインターネットにおいてアプリケーションに依存しない通信識別情報であり，ネットワークを通過する通信のすべてのフロー情報を通信資源の管理者が把握することで通信資源管理機能の実現が可能となる．本稿ではセッション層アーキテクチャのフロー情報を利用した通信資源管理機構を示す．さらに本機構の一実現例として，LAN における通信資源管理を実現するセキュリティゲートウェイの設計と実装について述べる．セキュリティゲートウェイは，従来のファイアウォールよりも粒度の高いフィルタリングを行い，同時にユーザ認証によってネットワークアクセス制御を実現している．
キーワード　セッション層アーキテクチャ フロー情報 通信資源管理 ファイアウォール

Communication Resource Management Using Flow Information of Session Layer Architecture

Hiroyuki KURITA†, Kunitake KANEKO†, Hiroyuki MORIKAWA††, and Tomonori AOYAMA†

† Graduate School of Information Science and Technology, The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656 Japan
†† Graduate School of Frontier Sciences, The University of Tokyo
5-1-5 Kashiwanoha, Kashiwa-shi, Chiba, 277-8582 Japan
E-mail: †{kuri,kaneko,mori,aoyama}@mlab.t.u-tokyo.ac.jp

Abstract　Recently, communication resource management becomes more important because communication devices and their access forms to the Internet become diverse. We take an approach to use flow information containing IP addresses, port numbers, and transport protocol for the management. It can identify flows on the Internet keeping the independence from applications. In our approach, network administrators obtain all the flow information related to their network from session layer architecture, and manage communication resources. Finally, we show a system, Security Gateway, which controls local area communication resource as one example of our communication resource management scheme. It enables more flexible filtering than conventional firewall, and realizes network access control based on user authentication.
Key words　session-layer, flow information, communication resource management, firewall

1. はじめに

近年モバイル機器などの普及により，ユーザが複数の通信端末を使い分けることが多くなっている．また WirelessLAN の利用などユーザのネットワークへのアクセス形態も多様化している．このような状況において，共有デバイスやインターネットへの接続性をユーザに対して提供する管理者にかかる負担は増大している．

現在，ネットワークを介したコンピュータウイルスの蔓延やDoS攻撃，不正アクセスなど，ネットワーク利用における課題は数多く存在する．通信資源の管理者はこれらから通信資源を保護すると同時に，外部ネットワークに対する加害者となることがないようにユーザの通信資源利用を適切に管理しなければならない．

しかし現在一般に普及している通信資源管理機能を備えたシステムは，管理者やユーザの要求に対して柔軟に対応できているとはいえない．たとえばネットワークのセキュリティを守るはずのファイアウォールでは固定的なルールに基づくフィルタリングが行われているため，特定のポートに対するDoS攻撃を防ぐことが不可能であるほか，セキュリティを重視したフィルタリングルールではマルチメディアアプリケーションをはじめとする一部のサービス利用が制限されてしまう．一般に，ネットワークの管理ポリシーはネットワーク毎に異なるため，多様な管理ポリシーに柔軟に対応し，管理対象を自在に管理することのできる通信資源管理機構が求められている．

このような問題は近い将来ユビキタスコンピューティング環境[1]が実現された場合，今以上にネットワークに接続される通信機器が増え，その形態も多様なものになるに従ってより顕著となり，管理者の負担が増加するであろう．

多様なネットワークポリシーに柔軟に対応し，管理対象を自由に管理することのできる通信資源管理機構の実現に当たり，筆者らはフロー情報に注目した．フロー情報はIPアドレスとポート番号のペアおよびトランスポート層プロトコルの計五つのパラメータからなり，これはインターネットにおいてアプリケーションに依存しない通信識別情報である．

ネットワークを通過する通信すべてのフロー情報を通信資源の管理者が把握することにより上記の目的を達成することが可能になる．たとえば外部からの不正に対しては，管理者が把握するフロー情報に合致しない通信フローをすべて不正なものとして排除することで対処できる．また内部からの不正やユーザ管理については，フロー情報とユーザ情報を関連づけることによって対応できる．

本稿では，これまで筆者らが検討を行ってきたユーザが簡単かつ安全に通信を行うためのサービスフレームワークであるセッション層アーキテクチャにおいて利用するフロー情報を通信資源管理に用いる手順について述べる．

セッション層アーキテクチャではユーザの通信において通信路の制御を行うためにネゴシエーションを行いフロー情報を保持している．フロー情報を保持するセッション層アーキテクチャと連携することで通信資源管理機構は粒度の細かいオンデマンドな通信資源管理の実現が可能となる．

以下ではまず2.でセッション層アーキテクチャの概要を簡単に説明する．次に，3.で通信資源管理機構に求められる役割について述べる．そして4.で実際に通信資源管理機構の設計を行い，それをふまえて5.では，通信資源管理機構の一実現例としてLANにおける通信資源管理を実現するセキュリティゲートウェイの設計と実装について述べる．最後に6.で本稿をまとめる．

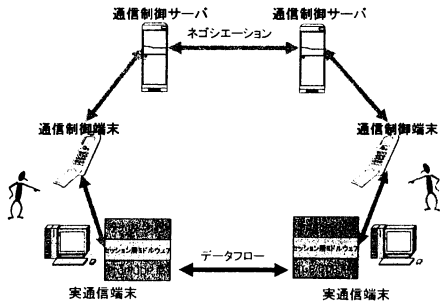

図1　セッション層アーキテクチャ

2. セッション層アーキテクチャ

セッション層アーキテクチャは，多様な通信デバイスが遍在する環境において，ユーザが簡単かつ安全に通信を行うためのサービスフレームワークであり，通信に使用するデバイスやネットワークへの接続インタフェースに依存しない柔軟な通信サービス利用を可能にする[2]．具体的には，ユーザが通信サービス利用において直接使用する機器とは異なる通信制御専用の機器を導入する．この通信制御専用の機器はユーザの通信をデバイスやアプリケーションにかかわらず一括して管理することで，ユーザの利用する多様な通信デバイス間の差異を吸収し，通信の開始や終了および通信内容の変更を統一的なインターフェースの元でユーザに提供する．

図1にセッション層アーキテクチャの全体構成を示す．図から明らかなようにセッション層アーキテクチャは三つの要素から構成される．

一つは，ユーザが実際のネットワークサービス利用に使用する端末であり，実通信端末と呼ぶ．なお，ユーザの通信サービス利用において実通信端末間のエンドツーエンド通信を実通信と呼んでいる．実通信端末にはセッション層ミドルウェアと呼ぶミドルウェアを導入し，このミドルウェアの提供するAPIによってアプリケーションから通信の下位情報が分離される．これによってアプリケーションにおける通信がデバイスやネットワークに非依存となり，アプリケーション開発が容易になるとともに，アプリケーションにおけるセキュリティの向上が実現される．

二つめは，ユーザの通信を一括して管理する通信制御サーバである．通信制御サーバはユーザの行う通信に関するネゴシエーションを通信制御サーバ同士で行うとともに，実通信端末上のセッション層ミドルウェアと連携し，ユーザの通信を管理する．セッション層ミドルウェアではアプリケーションと通信を明確に切り離しているため，通信制御サーバにおけるユーザの通信管理もアプリケーションに依存しない統一的なものである．通信制御サーバはユーザ自身が設置することも可能であるが，携帯キャリアやインターネットサービスプロバイダがユーザに対するサービスの一環として提供することを想定している．

最後に，三つめは通信制御端末である．通信制御端末は，サーバである通信制御サーバのユーザインターフェースとしての機

能と，実通信端末の行うサービス広告を受信するサービス発見の機能を持つ．通信制御端末はユーザが常に持ち歩くことを前提としており，携帯電話等の小型端末に通信制御端末としての機能が載ることを想定している．

通信制御端末は通信制御サーバと併せてユーザの通信を管理，制御する機能を果たしているが，ここで通信制御端末と通信制御サーバを分離させている理由は二つある．一つは小型端末である通信制御端末では消費電力や容積の問題から計算資源が限られ，通信制御サーバとしての役割を果たすことが困難であるためである．もう一つの理由は，据え置き型のサーバと異なり電波を使った通信が中心となる小型端末では，ユーザの移動によって通信環境が大きく変化し，端末へのネットワーク到達性を常時確保することが難しいためである．

ここで，アプリケーションサービスに必要なアプリケーションデータはすべて実通信端末間でエンドツーエンドで送受信され，通信管理に関するメッセージのみが通信制御サーバと通信制御端末によってやりとりされる．各構成要素間の通信については，通信制御サーバ間や実通信端末間ではインターネットを介した通信が行われる．また通信制御端末と通信制御サーバ間では無線 LAN のほか，携帯電話網の利用を想定している．同様に通信制御端末と実通信端末との間の通信方式としては無線 LAN をはじめ，Bluetooth [3]，IrDA [4] などを多様な方式を検討している．

3. 通信資源管理

本節では通信資源の管理に関する問題点を整理し，通信資源管理に求められる機能について述べる．通信資源とは通信を行う際にユーザが直接的ないし間接的に使用する物理的なデバイスとソフトウェア資源，および各リンクにおいて占有する帯域を意味する．そして，通信資源管理の目的はこれら通信資源を管理，保護し，ユーザの快適で安全な通信サービス利用環境を維持することである．快適で安全な利用環境を構築するにあたっては解決すべき問題点が存在するが，以下ではそれら問題点を三つに大別して説明する．

3.1 管理ネットワーク外部からの不正

通信資源管理における一つめの問題点は，外部ホスト，つまり管理者の管理管轄外のネットワークに接続しているホストからの攻撃である．インターネットでは誰もが自由にパケットを送り出すことができるため，悪意ある者が特定の対象に対して DoS 攻撃や総当たり攻撃などを行うこと自体を効果的に阻止することはきわめて困難である．

そのため，管理者はファイアウォールによるフィルタリングなどで，不正なパケットの内部ネットワークへの侵入を阻止することになる．しかし，ファイアウォールは外部ホストから送られたパケットが内部ホストのユーザにとって意図するものであるかを的確に判断することができないため，IP アドレスやポート番号を判断材料とする固定的なルールに基づくフィルタリングを行っている．一般にこのような固定的なルールによるフィルタリングでは，特定のポートが不特定多数のホストに対して常時開放されてしまうため，そのポートに対する DoS アタックなどからネットワーク内部のホストを守ることは困難である．また，セキュリティ維持のために用途の定まらないポートを閉じることもあるが，この場合動的なポート番号を使用するマルチメディアアプリケーションの利用が制限されることになる．このように，現在のファイアウォールは管理者にとっても，またユーザにとっても柔軟なフィルタリングが行えているとはいえない．

3.2 管理ネットワーク内部からの不正

二つめの問題点は管理ネットワーク内部からの不正つまり，管理者が提供する通信資源の不正利用である．特に有線 LAN においては元々空間的な利用の制約があることから認証の重要性が軽視されており，ハブやスイッチ等の空きポートを悪用したネットワークの無断利用を防ぐ手だてはないのが現状である．

管理者が特定のユーザに対してのみ通信資源の利用を許可し，不正利用を排除したいと考えた場合，MAC アドレスによるフィルタリングや RADIUS のような認証サーバを用いた IEEE802.1x [5] によるユーザ認証などの方法がある．しかし，MAC アドレスによるフィルタリングは端末識別情報による利用制限であるため，共有端末ではユーザを識別することができず、ユーザの個人端末を繋ぐ場合は端末識別の管理コストが増大する．また認証サーバの導入にはコストがかかるほか，ユーザはデバイスを利用する際に認証情報を入力する必要があり，一人のユーザが同時に多端末を利用する状況では管理コストとユーザの負荷が大きい．

3.3 正規ユーザの管理

通信資源管理における三つめの問題点は，正規ユーザによる通信資源利用状況管理の必要性である．これには大きく二つの意味があり，一つが他ネットワークへの加害行為の排除，もう一つがユーザ間の占有帯域の調整である．

まず，管理者は自らの管理する通信資源からウイルスの蔓延や外部ホストに対する攻撃を初めとする他ネットワークへの加害行為を速やかに検知し，それらを即座に止める責任がある．しかし現在の一般的な利用状況管理では，問題のあるパケットやフローの情報からユーザを即座に識別することは困難である．

また，VoIP [6] をはじめとするマルチメディアアプリケーションやコンテンツ配信サービスではサービス利用において一定の帯域を維持することが求められ，サービス品質保証のための帯域制御の重要性が増している．このようなサービスを実現する上でも，フローとユーザの対応づけは必須である．

4. 通信資源管理機構

4.1 アプローチ

多様なネットワークポリシーに柔軟に対応し、管理対象を自由に管理することのできる通信資源管理機構の実現に当たり、筆者らはフロー情報に注目した．フロー情報は IP アドレスとポート番号のペアおよびトランスポート層プロトコルの計五つのパラメータからなり，これはインターネットにおけるアプリケーションに依存しない通信識別情報である．また，管理者がユーザの行う通信のフロー情報を把握することで管理対象のネットワークを出入りするすべての通信フローの制御が可能になる．

つまり，通信資源の管理機構がすべてのフロー情報を一括し

て管理することにより，3. で述べた通信資源管理上の問題点を解決するための機能を統一的に実現することができる．まず，外部からの不正に対しては，機構がもつフロー情報に合致しない通信フローをすべて不正なものとして排除することで対処できる．また内部からの不正やユーザ管理については，フロー情報とユーザ情報を関連づけることによって，利用者の不明な通信を拒否できるほかネットワーク利用における責任の所在をはっきりさせることでネットワーク内で発生する偶発的もしくは意図的なトラブルの解決も容易になる．

このように，フロー情報を用いることでユーザやフローを基本単位とする柔軟な通信資源管理を実現でき，多様な管理ポリシーに対応することができる．

ここで，これまで筆者らがユーザ主体のネットワーキング実現に向け検討を進めてきたセッション層アーキテクチャがフロー情報を保持していることから，本稿では通信資源管理機能の実現にあたりセッション層アーキテクチャとの連携による解決を図る．具体的な通信資源管理機構の設計に先立ち，次節ではセッション層アーキテクチャにおいてフロー情報が果たしてきた役割について述べる．

4.2 セッション層アーキテクチャにおけるフロー情報の役割

セッション層アーキテクチャでは，ユーザは通信サービス利用において最初に通信相手とネゴシエーションを行う．この通信相手とは，たとえば利用するサービスがビデオチャットである場合には文字通り会話をする相手であり．ストリーミングによる音楽配信サービスを利用する場合には音楽配信サービスを提供するオンラインストアである．通信開始時のネゴシエーションは実通信端末間で直接通信をすることなく通信制御端末と通信制御サーバを介して行われる．このネゴシエーションによって，実通信において使用する IP アドレスとポート番号のペアおよびトランスポート層プロトコル，すなわちフロー情報が決定される．

実通信端末は実通信端末間の通信を開始する前にネゴシエーションによってフロー情報を得ることができ，フロー情報に合致する接続のみを受け付けることが可能になる．また，ユーザがアプリケーションサービスを利用している間，通信制御サーバがフロー情報を保持しているためユーザは通信制御端末を使って自分の行っている通信を統一されたインターフェースの元で管理できる．

このようにセッション層アーキテクチャでは通信制御サーバがユーザの行う通信のフロー情報を一括して管理している．次節では通信資源管理機構においてこのフロー情報をいかに利用するかについて述べる．

4.3 システム概要

通信資源管理機構は通信制御サーバの管理するフロー情報を必要とする．しかし，通信制御サーバは通信資源管理機構が管理すべき実通信端末のネットワークとは別のネットワークに設置されていることが一般的である．そのため，通信資源管理機構は通信制御サーバからフロー情報を入手する必要がある．また，一般にネットワークの管理ポリシーはネットワークごとに異なり，管理者が通信資源管理機構に対して求める機能も様々である．これらをふまえ，本機構では通信資源の管理者がそれぞれの管理ポリシーに基づき，必要な機能をもつ通信資源管理サーバを管理ネットワーク内に設置する．

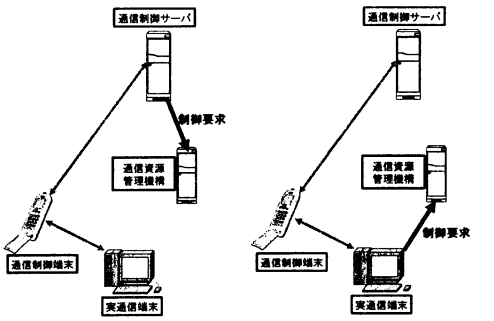

図 2　制御要求の二通りの実現形態

通信資源管理サーバは通信制御サーバとの通信モジュールと 3. で述べた問題点を解決するための機能モジュールを持つ．通信モジュールは通信制御サーバとの間の制御メッセージに含まれる認証情報に基づいたユーザ認証を行い，認証を経た後に機能モジュールがフロー情報に基づき通信資源管理を行う．

その動作はきわめて動的であり，ユーザが今まさに行おうとしている通信に対するオンデマンドな要求に対して柔軟な対応ができる．また，ユーザ認証によってユーザを識別するため，ユーザ単位での粒度の細かい管理が可能となる．

4.4 制御要求の実現形態

以下ではまず，通信資源管理に必要なフロー情報がセッション層アーキテクチャにおいてどこで保持されているか，という観点から，セッション層アーキテクチャから通信資源管理機構への制御要求に関する実現形態を探る．

セッション層アーキテクチャでは通信制御サーバによってフロー情報が管理され，そのフロー情報が実通信端末に伝えられることによってアプリケーションサービスにおける通信が開始される．そのため，セッション層アーキテクチャでは通信制御サーバと実通信端末がフロー情報を保持しており，潜在的にはどちらからでも通信資源管理機構に対する制御要求を行うことが可能である．以下では，制御要求を通信制御サーバから行う場合と実通信端末から行う場合 (図 2) について，制御要求に必須な認証情報の安全性と遅延時間の観点から比較，検討を行う．

4.4.1 認証情報の安全性

制御要求におけるセキュリティを考えた場合，制御要求に含まれる認証情報の流出をいかにして防ぐかが問題となる．認証情報の流出は，管理者にとって不正なユーザの通信資源利用を許してしまうだけでなく，ユーザに対して金銭的被害を与える可能性がある．

まず，実通信端末から通信制御要求を行う場合については，認証情報を実通信端末に入力すること自体に危険性がある．これは，ユーザ自身の所有物ではなく共有端末を実通信端末として一時的に利用する場合，ユーザが悪意ある者の設置した端末を使用してしまい認証情報を盗まれる可能性があるためである．認証情報をネットワークに流す際に暗号化を施したとしても，認証情報の入力段階でスパイウェアやキーロガー等によって情

報が盗まれることに対しては何の効力もない．これに対して，通信制御サーバから制御要求を行う場合にはあらかじめ認証情報を通信制御サーバに蓄えておくか，あるいは通信制御端末上で入力する方法が考えられる．通信制御端末は携帯電話のようなユーザ専用の端末であり，いずれの場合においても信頼できない端末に対して直接認証情報を入力することがないため安全である．

次に，認証情報を暗号化するための鍵交換について考える．ネットワーク内に設置された実通信端末からの制御要求では，実通信端末と通信資源管理サーバの間で事前に鍵交換を行っておくことが可能である．一方，ユーザが持ち込んだ実通信端末からの制御要求と通信制御サーバからの制御要求では，実通信端末の行うサービス広告に通信資源管理サーバの公開鍵を含めることで，こちらも通信資源管理サーバに対して安全に制御要求を行うことができる．

また，通信資源利用に対する課金モデルの構築を考えると，携帯キャリアやプロバイダによって管理される通信制御サーバから制御要求を行う場合において，ユーザの通信資源利用に対する代理課金や通信制御サーバ間の連携によるローミングサービスの展開が可能である．

4.4.2 遅　　延

次に，制御要求にかかる遅延時間の検討を行う．セッション層アーキテクチャでは，フロー情報が通信制御サーバによって決定された後に実通信端末に伝えられるため，通信制御サーバが直接ネットワーク資源管理制御機構に対して制御要求を行った場合の方が遅延は少ない．加えて，通信制御サーバから制御要求を行った場合には，通信制御サーバ間のネゴシエーションによって制御要求の完了を確認した上で，実通信端末に対して通信開始要求を行うことが可能である．それに対し，実通信端末で制御要求を行う場合には，通信相手側の制御要求の完了を確認できないまま通信を開始するため，通信相手がファイアウォールのフィルタリング設定の変更等が完了していない可能性があり，通信路が確立される前に送られたデータが相手に届かないという問題がある．セッション層アーキテクチャのプロトコルを拡張することにより，実通信端末から制御要求を行った場合でも通信相手側の制御要求の完了を事前に確認することは可能であるが，通信を開始する前に必要なネゴシエーションの手順が増えるため遅延時間が増大する．

4.5 管理機能の実現手法

以下では通信制御サーバから制御要求を行うモデルについて，本機構における制御要求を用いた通信資源管理機能の具体的な実現手法について述べる．

4.5.1 フロー情報を用いた動的なフィルタリング

管理ネットワーク外のホストによる攻撃からの保護はフロー情報を用いた動的なフィルタリングによって実現される．まず初期状態として，管理ネットワークのゲートウェイを通過する通信を内部から外部，外部から内部ともにすべて禁止する．そして，通信制御サーバからの制御要求を受理した通信資源管理サーバが，フロー情報に基づいたフィルタリングルールの動的変更を行うことでユーザが行う特定の通信を可能にする．フロー情報では，内部ホストの IP アドレスとポート番号だけでなく，通信相手の IP アドレスとポート番号，およびトランスポート層のプロトコルが指定され，フィルタリングルール変更の際にはこれらすべての情報を使用する．またユーザの通信が終了した場合，再度通信制御サーバが制御要求を行い，通信開始時に設定したフィルタリングルールを削除する．これによって，外部ネットワークとの通信時に発生するセキュリティ上の危険性は最小限にとどまり，内部ホストを DoS アタックなどの攻撃から守ることも可能になる．また，ポート番号のみに基づいたフィルタリングではないため，セキュリティのためにアプリケーションサービス利用が制限されることもなく，固定的なフィルタリングルールの設定が不要であることから管理者の負担も軽い．

なお，本機構ではフィルタリングをフロー情報に基づいて行うため，IP アドレスとポート番号を偽装されたパケットはファイアウォールを通過してしまう．しかし，セッション層アーキテクチャではサーバアプリケーションを含め動的なポート番号を使用するため，利用されているポート番号を推定しパケットを偽装することはきわめて難しい．

4.5.2 制御要求におけるユーザ認証および帯域制御

制御要求時に行われるユーザ認証において正当な認証情報を持たない制御要求は排除されるため，ネットワーク内部からの不正なネットワークアクセスも同時に拒否される．これにより，管理者の意図しないユーザによるネットワーク利用を防ぐことが可能である．同時に，ユーザの利用状況をシステムや管理者が把握することも容易になり，ユーザ間の占有帯域調整をフローレベルで実現できる．また，ユーザ認証と連携した課金モデルの導入により，特定のユーザの通信を優先させることや，ユーザの要求に基づいて特定のアプリケーションにおける通信を優先させるなどといった商用サービスにも展開できる．

5. セキュリティゲートウェイ

本節では通信資源管理機構の一例として，LAN における通信資源管理を実現するセキュリティゲートウェイの設計と実装，およびその基本的な性能評価について述べる．

5.1 設　　計

通信資源管理機構は，セッション層アーキテクチャが動作する場合に汎用的な通信資源管理機能を提供することが可能である．ここでは，4.5 で述べた通信資源管理機構を LAN に適用した通信資源管理サーバ（セキュリティゲートウェイ）について述べる．

セキュリティゲートウェイの提供する通信資源管理機能は二つある．一つめは，フィルタリング精度の高い柔軟なファイアウォールによって，外部ホストからの攻撃に対しネットワークのセキュリティを高めることであり，二つめは，ネットワーク内部のホストからのネットワークアクセスを制御することである．セキュリティゲートウェイは実通信端末から構成される内部ネットワークとインターネットに接続された外部ネットワークの境界に設置され，制御要求を受け付けることでその役割を果たす．セキュリティゲートウェイはインターネットカフェや無線 LAN ホットスポットなどの商用サービスにおいても有効であり，セキュリティゲートウェイにおける認証・課金処理に

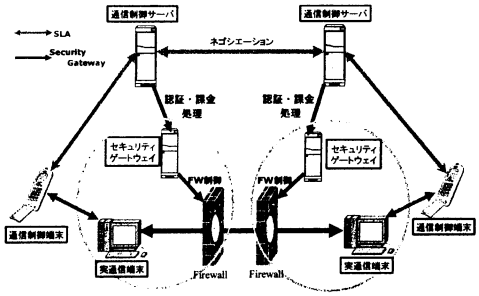

図 3　セキュリティゲートウェイのシステム構成

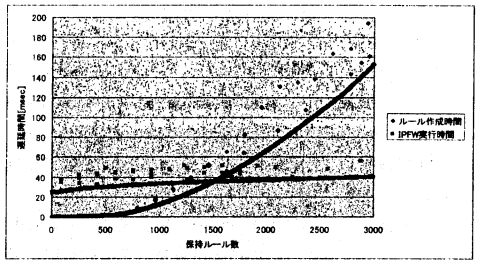

図 4　保持ルール数の増加に対する遅延時間の変化

よって統一的なサービス管理を行うことができる．またユーザにとっても，セッション層アーキテクチャを利用することで，認証情報を共有端末に直接入力する必要が無くなりセキュリティが向上する．

5.2 実　　装

セッション層アーキテクチャおよびセキュリティゲートウェイからなるシステム全体の構成を図 3 に示す．実通信端末および通信制御端末に関しては WindowsXP 上で開発，動作確認を行った．また，通信制御サーバおよびセキュリティゲートウェイについては FreeBSD5.3 上で開発を行った．セキュリティゲートウェイではフィルタリングルールの変更に際して FreeBSD における IPFW を利用しており，動作確認も同じく FreeBSD5.3 上で行った．

5.2.1 開発ソフトウェア

ここではセキュリティゲートウェイ上で動作する SG_FIREWALL について述べる．SG_FIREWALL はサーバプログラムとして動作し，通信制御サーバからの制御要求を受け付ける．制御要求を受け取るとまず制御要求に含まれる認証情報を SG_FIREWALL があらかじめ保持しているユーザの認証情報と照合しユーザ認証を行う．ユーザ認証を経た後その制御要求を受理するために必要な IPFW の適用ルールをフロー情報を参照することによって作成する．

IPFW においてフィルタリングルールを追加．削除する際の書式はそれぞれ以下のようになっている．

```
ipfw add ルール番号 トランスポート層プロトコル
    from 送信元 IP アドレス 送信元ポート番号
    to 送信先 IP アドレス 送信先ポート番号
ipfw delete ルール番号
```

IPFW におけるルール番号は本来，フィルタリングルールの優先順位を決定するものであるが，セキュリティゲートウェイでは，一度設定したルールを後で削除する際に使用する．そのため SG_FIREWALL は内部にテーブルを持ち，現在適用しているフィルタリングルールをルール番号とともに管理する．適用するルールを作成するとプログラム内部から IPFW を呼び出し，IPFW に対して新しいルールの追加を行う．

5.3 性能評価

ここでは，今回作成したセキュリティゲートウェイの簡単な性能評価として，制御要求に要する遅延時間の測定を行った．制御要求にかかる遅延時間は三つの要因からなる．一つは通信制御サーバとセキュリティゲートウェイ間の RTT であり両者のネットワーク的な距離に依存する．二つめは，制御要求を受け取ってから IPFW に適用するルールの作成に要する時間である．最後に三つめの要素は，IPFW の実行に要する時間である．

ここでは，ルール作成と IPFW の実行にかかる時間のスケーラビリティに注目し測定を行った．測定結果を図 4 に示す．図 4 からルール作成に要する時間は保持ルール数が増加するに従ってほぼ線形に増大していることがわかる．これは，新しいルールに対するルール番号を決定する際に保持ルールに対して線形探索を行っていることによる．測定結果から通常の利用環境では制御要求に要する遅延時間は十分に実用可能な値であるといえるが，保持ルール数が数千以上に達するような環境では，ルール番号決定処理により効率的なアルゴリズムを利用することで遅延時間の改善が可能である．

6. おわりに

本稿では通信資源の管理を統一的におこなう通信資源管理機構に求められる役割を明確にし，セッション層アーキテクチャを用いた通信資源管理機構の実現手法について述べた．本機構はセッション層アーキテクチャの管理するフロー情報を利用し，柔軟かつ安全な通信資源管理を行うことを目指したものである．また本稿では通信資源管理機構の一例として LAN における通信資源管理を行うセキュリティゲートウェイの設計と実装についても説明を行った．セキュリティゲートウェイは，従来のファイアウォールよりも粒度の高いフィルタリングを行い，同時にユーザ認証によってネットワークアクセス制御を実現している．

文　　献

[1] M.Weiser, "The Computer for the 21st Century", Scientific American, Vol.265 ,No.3, pp94-104, Sep. 1991.

[2] 金子晋丈, 森川博之, 青山友紀, "通信路管理を実現するセッション層アソシエーション", 電子情報通信学会技術研究報告, MoMuC2004-20, May 2004.

[3] Bluetooth SIG, http://www.bluetooth.com/

[4] Infrared Data Association, http://www.irda.org/

[5] IEEE Standards for Local and Metropolitan Area Networks, "Port based Network Access Control", IEEE Std 802.1x-2001, Jun. 2001.

[6] T. J. Kostas, M. S. Borella, I. Sidhu, G. M. Schuster, J. Grabiec, and J. Mahler, "Real-time voice over packet switched networks", IEEE Network, 12(1):18–27, Jan. 1998.