セッション層アーキテクチャを用いたネットワークサービスの構築

金子 晋丈

1　はじめに

現在のインターネットは，ネットワークのより広範な相互接続を設計指針としたため，通信サービスを意識した設計が行われていない．これは，OSI の階層モデルで定義されているプレゼンテーション層やセッション層が存在していないことからも明らかである．筆者は，広く普及したインターネットでより豊かな通信サービスの実現に向け，セッション層アーキテクチャを設計している．セッション層アーキテクチャは，既存のインターネット上に柔軟で規模拡張性の高い認証フレームワークを構築するものである．本稿では，セッション層アーキテクチャを用いたネットワークサービスとして，通信資源管理制御機構と遠隔会議システムについて述べる．

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，アプリケーションプログラム間をつなぐ通信チャネルをアプリケーションプログラムから完全に分離して，ユーザが直接構築し制御管理するユーザ主導型のネットワークアーキテクチャである．これまでのアプリケーションプログラムでは，アプリケーションプログラムが通信相手のアプリケーションプログラムとの間に通信チャネルを直接確立するのに対し，セッション層アーキテクチャではユーザが必要に応じてアプリケーションプログラム間に通信チャネルを構築する．したがって,（1）ユーザは通信を行うときにそれぞれのユーザの状況に最適なアプリケーションプログラムを選択することが可能である．また，ユーザは通信チャネルを構築する際に通信相手と相互に認証するが，この認証処理はアプリケーションプログラムが動作する通信デバイスとは別の認証専用の通信デバイスで行う．そのため,（2）利用するアプリケーションプログラムやアプリケーションプログラムが

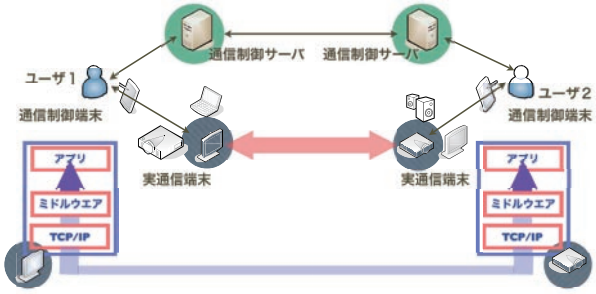

図 1: セッション層アーキテクチャ

動作する通信デバイスに依らず安全な認証を行うことが可能になる．

セッション層アーキテクチャでは，ユーザの要求に応じて通信チャネルを構築するために各通信デバイスにセッション層ミドルウエアを導入し，それぞれの通信チャネルの構築の際の認証処理，およびユーザが通信チャネルを制御管理するために通信制御サーバを導入している（図 1）．

3　ネットワーク資源管理制御機構

3.1　ネットワーク資源管理制御

セッション層アーキテクチャにおけるフロー情報が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ことに着目し，これをネットワーク資源管理制御に用いるのがネットワーク資源管理機構である．ここでネットワーク資源管理制御とは，ネットワーク管理者の管理ポリシーに基づき，ファイアウォールにおけるフィルタリングやルータにおける優先制御を行うことである．一般にネットワーク管理ポリシーはネットワーク毎に異なるため，ネットワーク管理者はそれぞれの管理ポリシーに基づいて必要な管理機能を持つネットワーク資源管理サーバを設置し，認証情報とフロー情報を含んだ制御要求を受け付ける．以下では，ネットワーク

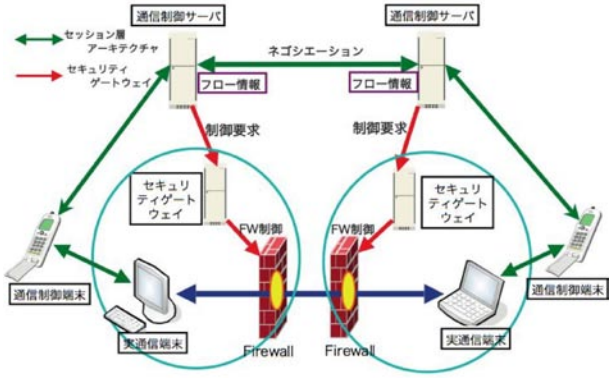

図 2: セキュリティゲートウェイ

資源管理制御機構の一例として，フィルタリング精度の高い柔軟な FW であるセキュリティゲートウェイについて述べる．

3.2 セキュリティゲートウェイ

現在の FW 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判断できないため，IP アドレスやポート番号による固定的なフィルタリングを行っている．しかし，一般にこのような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い，内部ホストを DoS アタックなどから防ぐことが不可能である．これに対しセキュリティゲートウェイではフロー情報を利用し，ユーザの要求に動的に対応したフィルタリングを行う．これにより DoS アタックを含めたあらゆる不正なパケットの内部ネットワークへの侵入を防ぐとともに，管理者がフィルタリングルールをあらかじめ設定する手間を省くことができる．セッション層アーキテクチャを用いたセキュリティゲートウェイの構成を図 2 に示す．筆者は，セキュリティゲートウェイの実装を行い，その動作を確認した．

4 遠隔会議システム

遠隔会議システムに要求される事項を列挙する．

1. 通信相手に制御を許可する会議リソース（公開リソース）の決定
2. 会議中に限った公開リソースの自由な制御
3. 会議参加者に限定した公開リソースの制御

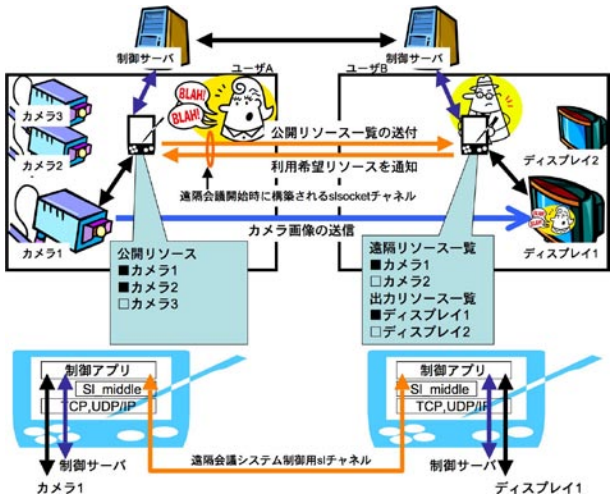

図 3: 遠隔会議システム

上述の要件を満たすシステムとして，通信制御を通信相手側が遠隔から安全に行う機構を構築した（図 3）．具体的には，通信制御機能を通信相手からでも制御可能にするプロキシソフトウエアを，セッション層アーキテクチャを利用した通信アプリケーションとして作成した．セッション層アーキテクチャを用いることで，会議中に限り通信制御機能を通信相手に委譲することが可能 (2) になるだけでなく，会議参加者に限定した制御も可能 (3) になる．

作成した遠隔会議システムは以下のように動作する．まず，ユーザ A が公開を許可するリソースを選択する．次にセッション層アーキテクチャを用いて発呼処理をおこない遠隔会議を開始（プロキシソフトウエア間の通信が確立）する．開始後，ユーザ A が公開を許可したリソースの一覧をユーザ B 側に提示し，ユーザ B がリソースを選択すると，プロキシソフトウエアがあたかもユーザ A がそのリソースを選択しユーザ B との通信を希望しているかのように動作する．その後，ユーザ B は，通信制御サーバを介してユーザ A からの通信開始要求が届くが，これはあらかじめユーザ B が希望したものであるため自動的に通信が開始されることになる．

5 おわりに

本稿では，セッション層アーキテクチャを用いたネットワークサービスとして，ネットワーク資源管理制御機構と遠隔会議システムについて述べた．