ユビキタスネットワーク社会を支えるセッション層アーキテクチャ

青山 友紀

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．

筆者らは，広く普及したインターネットにより構築されるユビキタスネットワーク社会における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検討している．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，設計したセッション層アーキテクチャと，セッション層アーキテクチャを用いた 4 つのネットワークサービス— WWW 閲覧システム，ローミングシステム，遠隔会議システム，IPTV システム—および、これらのネットワークサービスを構築する上で必要となる複数チャネル連携技術について述べる．

2　セッション層アーキテクチャ

2.1　ユーザ主導型通信

今日，我々はアプリケーションプログラムや通信端末が遍在するユビキタス社会の入口に立っており，これからのネットワーキングはひとつのアプリケーションプログラムや通信端末を使い続けるのではなく，それらをコンテキストに応じて選択し利用し切替えるものになる．このような動的で分散的なネットワーキングにおいてセキュリティとモビリティは必要不可欠な機能となる．

本稿では，セキュリティのための認証機構とモビリティのための柔軟性を併せ持つユーザ主導型通信を実現するセッション層アーキテクチャについて説明する．ユーザ主導型通信の説明に先立ち，これまでのセキュリティとモビリティについて述べる．また，ユーザ主導型通信の一つの実現形態としてセッション層アーキテクチャを提示する．

ユーザ主導型通信は，これまでの端末を主体とした通信ではなくユーザを主体とした通信を可能にするものである．これにより，我々の日常的なコミュニケーションと同様に，誰と話しているかが分かっている安心感や，時間や場所，メディアを変えてコミュニケーションが「継続」する連続性を通信機構として実現することが可能となる．ユーザ主導型通信とは，インターネットに求められているセキュリティが通信相手の認証であり，チャネルの抽象化に基づくモビリティサポートにおいても通信相手との認証処理が必須であることに着目した，セキュリティとモビリティの問題を同時に解決する通信アーキテクチャに他ならない．

ユーザ主導型通信における「ユーザ」とは，通信サービスを享受するユーザやサービスを提供するプロバイダである．１人のユーザが複数の通信サービスを享受する場合には，同一のアイデンティティですべてのサービスを享受する場合もあれば，サービスをそれぞれ異なるアイデンティティで享受する場合もある．

ユーザ主導型通信は，これらのアイデンティティを暗号学的な識別情報を用いて区別する．したがって，通信相手の識別は，暗号学的に通信相手のアイデンティティを認証することで可能となる．認証処理の完了したアイデンティティ間にはアソシエーションが構築され，以後，この認証関係に基づいて通信が行われる．アソシエーションはアイデンティティ間に実際の通信チャネルを構築する．（図 1 ）

本稿では，少なくとも 1 つのアイデンティティを保持し，アソシエーションを終端する通信端末を制御端末と呼ぶ．なお，アソシエーションは，認証関係に基づいて通信チャネル情報の交換を安全に行うた

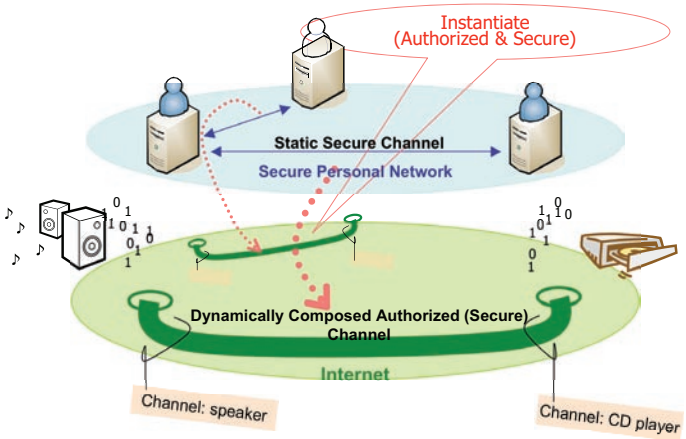

図 1: ユーザ主導型通信

めのチャネルであり，音声や画像などの実データを送受信するチャネルではない．そして，アソシエーションを用いて，実データを送受信するための通信チャネルを識別するのに必要な IP アドレスとポート番号，トランスポート層プロトコルを相互に交換することで，実データを送受信する通信チャネルを認証情報に基づいて構築することが可能になり，結果として情報の送受信を安全かつ柔軟に行うことが可能になる．以下では，実データのフローを終端する通信端末を実通信端末と呼ぶ．アイデンティティを保持する制御端末とそのアイデンティティが利用する実通信端末は安全に通信できることが前提となる．

2.2 セッション層アーキテクチャの構成

セッション層アーキテクチャ（図 2）は，アプリケーションプログラムと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完全に分離し，通信チャネルをユーザが直接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．これまでは通信チャネルをアプリケーションプログラム自体が構築していたのに対し，セッション層アーキテクチャではユーザ自身が必要に応じてアプリケーションプログラム間の通信チャネルを構築することでユーザの主導性を確保している．

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エンド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をユーザが主導的に管理するために通信制御サーバを導入している．

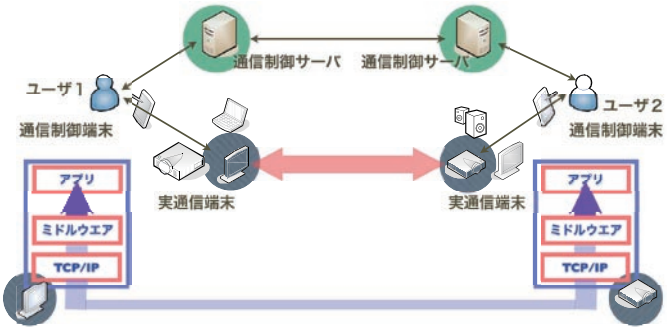

図 2: セッション層アーキテクチャの構成

セッション層ミドルウエアは，ユーザの要求に応じて，通信相手のセッション層ミドルウエアとの通信チャネルを確立するとともに，ユーザの希望するアプリケーションプログラムにも接続し，それぞれから流れてくるデータを相互にプロキシ転送する．なお，セッション層アーキテクチャで動作するアプリケーションプログラムは自デバイス内のセッション層ミドルウエアからの接続要求を待ち受けているだけで，既存のアプリケーションプログラムのように別のアプリケーションプログラムに接続要求を出したり，ネットワークを介した接続を受け付けたりはしない．

一方，通信制御サーバは，ユーザが新しい通信チャネルを構築する時や通信チャネルをハンドオフし別のアプリケーションプログラムに接続する時，および通信チャネルを破棄する時に，IP アドレスやポート番号などの必要な情報を通信相手の通信制御サーバとの間でやりとりし，やりとりした情報を保存することでユーザが利用している通信チャネルをすべて管理している．すべての通信チャネルは，通信チャネルの両端の IP アドレスとポート番号，およびトランスポート層プロトコルによって識別され，セッション層アーキテクチャにおける制御管理の最小単位となっている．

3 WWW閲覧システム

本アーキテクチャを既存のアーキテクチャと併用した例として，現在最も一般的なネットワークサービスの一つである WWW 閲覧サービスに本アーキテクチャを導入した WWW 閲覧システムを実装した（図 3）．

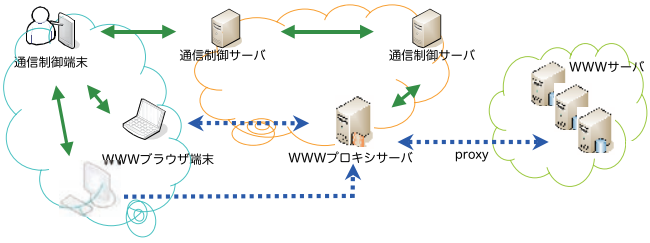

図 3: WWW 閲覧システムの構成図

本システムは，従来の WWW 閲覧サービスに比べ，ユーザとネットワーク管理者の双方にメリットのあるシステムである．WWW 閲覧を行うユーザと閲覧したサイトの履歴を利用デバイスに依存することなく関連付けることができるため，ユーザに関連付けた履歴を利用し，WWW プロキシがユーザに履歴を提示することができる．ネットワーク管理者は本アーキテクチャを用いることでファイアウォールにおける粒度の細かいフィルタリングや通信トラヒック量に応じた課金を行うことが可能となる．

4 ローミングシステム

本アーキテクチャの保持するフロー情報をファイアウォールの動的な制御に利用する前年度の通信資源管理制御機構をさらに発展させたローミングシステムを実装した．本システムでは，ネットワーク資源の管理者である ISP（Internet Service Provider）の他にユーザの身元を保証する第三者機関である IDP（IDentity Provider）を導入し，ローミングを実現している．

本システムではユーザと IDP，IDP と ISP 間に通信チャネルを張り，IDP と ISP 間の通信セッションが継続している期間に限りネットワーク資源を利用できるようにするものである．ユーザと IDP，IDP と ISP 間の通信をユーザ主導型通信とすることで，認証有効期限を反映したチャネルの利用を可能にしている．従って認証が切れると，IDP と ISP 間のセッションは切断され，自動的にネットワーク資源は利用不可能となる（図 4）．

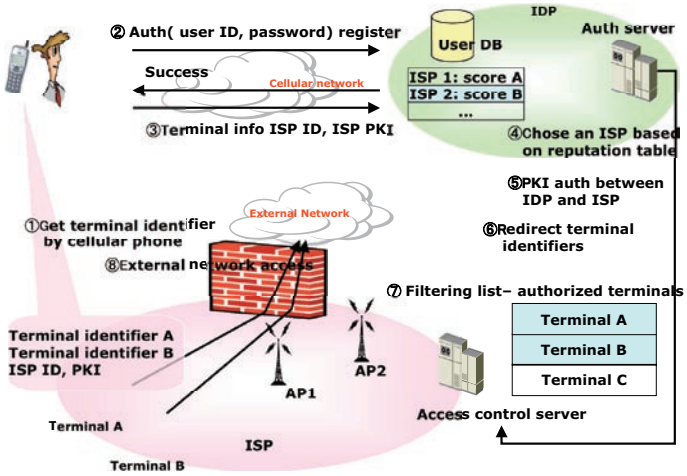

図 4: ローミングシステム

5 複数通信チャネルの連携技術の基礎的検討および実装

関連性のある複数のチャネルをまとめて管理，制御する機構を通信チャネル制御機構に導入することで，単一の通信チャネルでは実現できなかった複雑なネットワークサービスを実現することができる．複数チャネルの連携のために，本アーキテクチャに以下の機構を新たに設計し，導入した．

（1）アプリケーションプログラムがデータ通信ミドルウエアから接続してきた複数のチャネルに対して，通信相手の同一性を確認する機構（2）アプリケーションプログラムがデータ通信ミドルウエアから接続してきた複数のチャネルに対して，それぞれをどのような用途に使うかを認知する機構（3）通信開始時やモビリティサポート時，通信終了時に，関係するチャネルをユーザのインタラクションなしに常にセットで扱う機構

上記機構を導入するにあたり，データ通信ミドルウウエアおよび通信制御サーバに改変を加えた．また，本アーキテクチャではユーザ主導で通信チャネルが構築されるため，ユーザビリティの観点からユーザインタフェースにも改造を施した．

6 遠隔会議システム

連携機構を導入した本アーキテクチャをマルチメディア通信に応用した例として遠隔会議システムを作成した（図 5）．本システムは，本アーキテクチャ

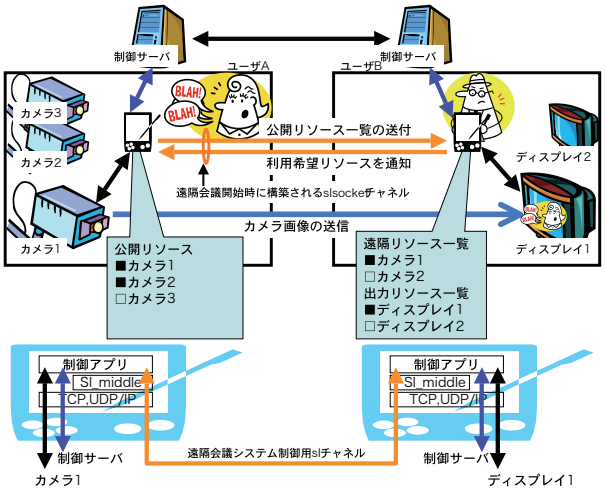

図 5: 遠隔会議システムの構成図

で動作する PC 付きディスプレイやスピーカ，カメラ，マイクなどのマルチメディアリソースを用いて，ユーザ自身がネットワーク越しに相手のリソースを自在に制御することで，高い臨場感を保ったまま円滑な会議進行を支援するアプリケーションである．

本アーキテクチャを利用することにより，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 になるだけでなく，会議参加者に限定した制御も可能になる．

システムの実現にあたって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開発した．プロキシは複数チャネル連携機構を利用し，制御情報の伝達に使われる制御用チャネルとマルチメディアデータが流れるデータチャネルの連携を実現している．

7 IPTV システム

近年爆発的に普及しつつあるインターネットを利用したマルチメディアコンテンツ配信サービスに本アーキテクチャを適用した例として IPTV（IP テレビ）システムを実装した．

本アーキテクチャはユーザとコンテンツプロバイダの両者にメリットを生む．ユーザは，一度認証が完了した後，状況に応じて自由にコンテンツの配信先となる利用ディスプレイデバイスを切り替えることが可能となる．コンテンツプロバイダは，複数のコンテンツサーバ間でコンテンツの配信元を自由に切り替えることができるため，容易に冗長性を実現

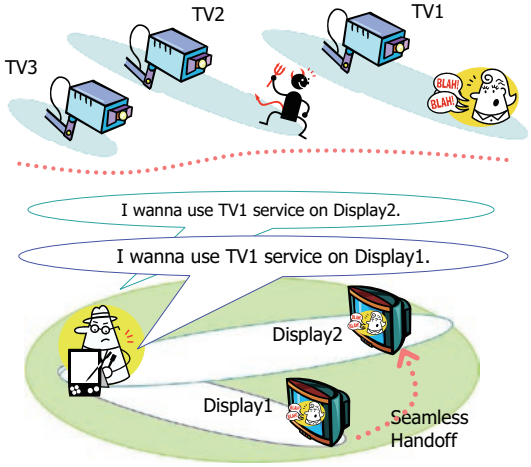

図 6: IPTV システム

図 7: IPTV システム動作状況

することができ，サービスの信頼性，安定性を高めることができる．

本システム（図６）の実現には，ユーザの接続要求やチャネル切り替え要求に自動で応答する機構が必要となるため，自動応答で通信資源の管理・制御を行うプログラムを作成した．自動応答プログラムは，複数チャネル連携機構を利用し，制御チャネルを通じて送られてくる制御要求をデータチャネルに反映させている（図７）．

8 おわりに

本稿では，ユーザが通信相手との通信チャネルを通信アプリケーションとは独立に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セッション層アーキテクチャについて示し，開発したセッション層アーキテクチャを用いた通信サービスについて報告した．