

論文の内容の要旨

論文題目 ユーザ主導型通信制御のためのセッション層構成に関する研究

氏名 金子 晋 丈

様々なネットワークの相互接続性を高めることを設計指針にしたインターネットは国や地域、組織を超えて接続され、初期の目的を十分に遂げたと言えよう。しかし、現在のインターネットはユーザのネットワーク利用を大きく制約し自由に情報をやりとりできる環境ではなくなりつつある。このようなインターネットの現状は、インターネットの設計に端を発する必然的なものである。すなわち、インターネットが様々な通信サービスやアプリケーションプロトコルを期待しつつも、それらが実際に動作する場合に必要な共通のサービスプラットフォームを具備していないことに起因している。

本論文では、インターネットの相互接続性を最大限生かしユーザが主導的に通信を制御しインターネット上で自由自在に情報を操れるようなインターネットの共通サービスプラットフォームをアーキテクチャ的観点から考察し、これからのインターネットに必要なセッション層の構成について論じている。具体的には、まず、ユーザ主導型通信制御の意義について示し、通信制御をIPアドレス、ポート番号、トランスポートプロトコルを用いた行うことの重要性を示している。そして、通信制御機能を持つセッション層と、セッション層の認証技術について述べている。IPアドレス、ポート番号、トランスポートプロトコルによって通信を管理するシステムとしてIEEE 802.11省電力モバイル端末のTCPスルーブット改善手法について述べている。さらに、セッション層を遠隔から制御するシステムを示し、このシステムが保持する通信制御情報をネットワーク管理に応用する通信資源管理機構を示している。最後に、セッション層を用いたアプリケーションサービスシステムを示すことでユーザ主導型通信制御を実現するセッション層の構成に関する議論を行っている。

第2章では、ユーザ主導型の通信制御について論じている。ユーザ主導型の通信制御とは、アプリケーションプログラムやアプリケーションサービスの制約を受けない普遍的な通信制御である。すなわち、ユーザがアプリケーションプログラムを通して情報の入手元や出力先を直接指定するのではなく、アプリケーションプログラムとは独立にユーザが通信に必要な通信チャネルを直接用意することである。さらに、ユーザ主導型通信制御を実現することで、情報をインターネット上の任意の地点から任意の地点に移動させることが可能になり、インターネットにおけるサービスをさらに豊かにする可能性があることを示している。そして、ユーザ主導型通信をインターネットで普遍的に用いるために、サービスプラットフォーム

としての構築の必要性について議論している。

第3章では、ユーザ主導型の通信制御を実現するインターネットにおけるサービスプラットフォームとしてのセッション層について論じている。セッション層は、通信をIPアドレス、ポート番号、トランスポートプロトコルに基づいてエンドツーエンドで制御する機能である。具体的には、セッション層はアプリケーションプログラム間の通信チャネルの確立に必要な情報をセッション層より上位の階層から得るのではなく、セッション層を制御する制御部から情報を得て通信相手のセッション層との間に通信チャネルを用意し、用意した通信チャネルの端点を上位層に接合することで該当するアプリケーションプログラム間の通信を実現する。そして、ユーザがセッション層の制御部を介して通信チャネルを直接制御することで、ユーザ主導型の通信制御を実現している。

第4章では、セッション層が必要とするエンドツーエンドの認証技術について論じている。ユーザが構築する通信チャネルは、ユーザの要求に応じて情報の入手元もしくは出力先だけを変更できることが期待される。特に、通信チャネルの端点をホストを超えて移動させるために必要となる認証技術について示している。具体的には、一つの公開鍵に対して時系列で複数の秘密鍵を対応づけられるKey-insulated公開鍵暗号方式を用いた認証技術について示している。通信チャネルの端点を更新する際に秘密鍵を更新することで、利用した秘密鍵の流布を防ぎ、ホストに依存しないセッション層が用いる安全な認証を実現している。

第5章では、セッション層が管理するIPアドレス、ポート番号、トランスポートプロトコル情報をホストを超えて移動させるシステムとして、IEEE 802.11省電力モバイル端末のTCPスループット改善手法について論じている。本システムは、IEEE 802.11省電力モードで動作するモバイル端末のTCPスループットの劣化を、基地局が各TCPフローに流れるTCPセグメントを制御することで改善している。そして、基地局間のTCP情報の移動を実現することで、モバイル端末のハンドオーバを実現している。

第6章では、セッション層の制御部の機能をインターネット上のサーバに配置することについて論じている。各ホストが保持するセッション層の制御情報を、ユーザ毎にまとめて単一のサーバ上で管理することで、ユーザが複数の通信チャネルを集中的に管理制御することが可能になる。セッション層の制御情報をネットワーク上を動かない固定ホストで集中的に管理することにより、通信相手との認証処理の軽減が可能になる。さらに、セルラーネットワークを用いてこのサーバをユーザが遠隔制御することで、ユーザの利便性と安全性を兼ね備えた通信制御を実現している。

第7章では、ユーザ毎に管理されたセッション層の制御情報の通信資源管理への利用について論じている。セッション層の制御情報はIPアドレス、ポート番号、トランスポートプロトコルであり、これらがインターネットにおける通信資源管理の最も基本的な情報であることに着目し、インターネットの通信資源管理に利用することを論じている。具体的には、セッション層の制御情報を管理するサーバからインターネ

ット上で通信資源管理を行うサーバにこれらの情報を伝達し、通信資源管理を行う機構を示している。特に、ローカルネットワークにおけるファイアウォールに適用し、柔軟な通信資源管理の実現を示している。

第8章では、サービスプラットフォームとしてのセッション層を用いたアプリケーションサービスについて論じている。セッション層は、柔軟な通信制御と集中的な認証管理、制御情報を用いた通信資源管理が可能であり、これらを統合的に利用したサービスとして遠隔会議システムを示している。具体的には、柔軟な通信制御を利用したマルチメディアコンテンツの切り替え、集中的な認証管理を用いた遠隔会議システムの利用制限、遠隔会議で用いる通信資源の管理を実現している。