

# 仮想計算機におけるソケットアウトソーシングによる オーバーレイネットワークの利用

保田次郎<sup>†</sup> 齊藤剛<sup>††</sup> 新城靖<sup>††</sup>  
佐藤聡<sup>††</sup> 中井央<sup>†††</sup> 板野肯三<sup>††</sup>

## 1. はじめに

ホスト型の VMM(Virtual Machine Monitor) における高速な入出力手法に、準仮想化とアウトソーシング<sup>1)</sup>がある。準仮想化はハードウェアのエミュレーションを行わず、ゲスト OS のデバイスドライバを専用のものに置換し、デバイス操作のレベルで入出力要求をホスト OS へ委譲することで高速化を図る。これに対し、アウトソーシングとは、ゲスト OS の入出力要求をより高いレベルでホスト OS へ委譲する手法である。これをソケットに対して適用したものがソケットアウトソーシングである。

ソケットアウトソーシングは本来、高速化のための手法として考案された。しかし副次的に、通常の準仮想化ではホスト OS でデバイスレベルの情報しか得られないのに対し、ソケット API という、より抽象度の高いレベルの情報得られるという機能も存在する。これにより、ホスト OS へ委譲された通信要求に機能を実行することが容易となる。

そこで本研究では、その有用性を探るため、ゲスト OS から委譲された通信要求を SSH(Secure Shell) や IM(Instant Messenger) が形成するオーバーレイネットワークに乗せることを提案する。これにより、既存のアプリケーションを一切変更することなくオーバーレイネットワークに乗せることを可能とする。

## 2. 外部ヘルパ に対する VMM の拡張

ソケットアウトソーシングにおいて、ゲスト OS のアプリケーションの通信要求は、まずゲスト OS のカーネルのソケット層へ伝えられる。次に VMRPC<sup>1)</sup> によって要求がホスト OS のユーザ空間で動く VMM へ伝えられ、VMM はホスト OS のソケット層を通じて通信処理を行う。本研究ではこの経路のうち、VMM 以降を変更して通信要求をオーバーレイネットワークに乗せる。

VMM 自身に暗号化や IM を用いた通信を行うためのプログラムを組み込む方法が考えられる。しかし、VMM はスレッドやシグナルなどを高度に利用する複雑なプログラムであり、同じくスレッドやシグナルを必

要とする通信機能を整合性を保って組み込むことは極めて難しい。そこで、本研究ではオーバーレイネットワークを用いた通信を外部ヘルパと呼ぶ独立したプログラムに行わせ、VMM と外部ヘルパの間をプロセス間通信で結ぶことで、この問題を解決する。図 1 は、このように変更した通信経路を示している。すなわち、VMM に伝えられた通信要求をディスパッチャを通じて外部ヘルパへと伝え、外部ヘルパがオーバーレイネットワークを用いた通信を行う。どの外部ヘルパを用いるかは、VMM 内のディスパッチャテーブルを参照して決める。外部ヘルパを用いた通信手順を以下に示す。

ディスパッチャと外部ヘルパは 2 本の Unix Domain Socket(データ用とイベント用) によってやりとりを行う。ゲスト OS から connect 要求を受け取った場合、ディスパッチャはデータ用ソケットを通じて外部ヘルパに connect 要求とポート番号を送信し、接続を識別するための ID(接続 ID) を受け取る。外部ヘルパ側で接続処理が完了するとイベント用ソケットから CONNECTED イベントと接続 ID が送られてくるため、これをゲスト OS に通知する。

ゲスト OS から accept 要求を受け取った場合、ディスパッチャは connect の場合と同様に外部ヘルパに accept 要求とポート番号を送信する。外部ヘルパ側で接続の受け入れが成功すると ACCEPTED イベントと接続 ID が送られてくるため、これをゲスト OS に通知する。

ゲスト OS からデータ送信要求を受け取った場合、ディスパッチャは対応する外部ヘルパに対して write 要求と接続 ID、データの長さ、データの順に送信を行い、実際に送信できた長さをゲスト OS に返す。

ゲスト OS からデータ受信要求を受け取った場合、対応する外部ヘルパに対して read 要求と接続 ID、受信したいデータの長さを送信し、データを受け取る。その後、受信したデータの長さでデータをゲスト OS に返す。もし指定した長さ分データを受信できなかった場合、ARRIVED イベントと接続を表す接続 ID が送られてくるのを待って再度 read 要求を送ることで、残りのデータを受信する。

<sup>†</sup> 筑波大学情報学群情報科学類  
<sup>††</sup> 筑波大学システム情報工学研究科  
<sup>†††</sup> 筑波大学図書館情報メディア研究科

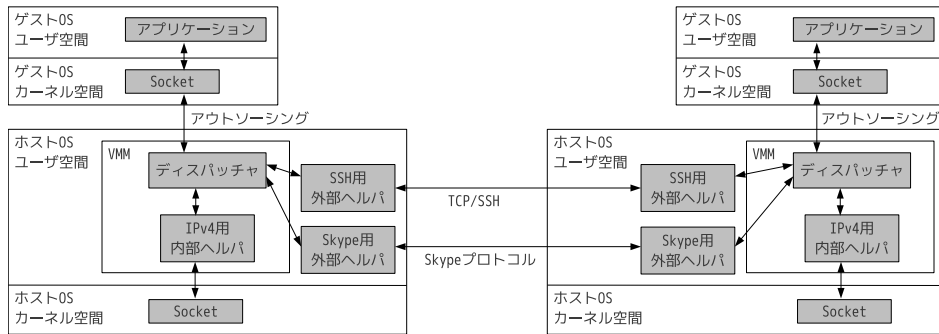


図 1 外部ヘルパを用いたオーバーレイネットワークの利用

### 3. SSH オーバレイネットワークの利用

SSH とは、暗号化された通信路を用いてリモートホストのシェルを利用するためのプロトコルである。これにはポートフォワーディングという機能があり、簡単に暗号化されたトンネルを形成することができる。本研究では、この SSH のポートフォワーディングを利用する外部ヘルパを実装する。外部ヘルパは、connect 用と accept 用の 2 本の SSH 通信路を必要とする。

SSH 用外部ヘルパは、VMM から connect 要求を受けると、connect 用 SSH 通信路を通じて通信先の SSH 用外部ヘルパへ connect 要求を送信する。また、接続 ID を生成して VMM に返す。その connect 処理が完了したら、VMM に CONNECTED イベントを通知する。

VMM から accept 要求を受けると、指定されたポート番号を記憶しておき、接続 ID を生成して VMM に返す。その後、accept 用 SSH 通信路を通じて相手の外部ヘルパから connect 要求が来ると、外部ヘルパはその要求に含まれるポート番号を見て、そのポート番号を accept 用に記憶しているかどうか調べる。記憶していなければ accept 用 SSH 通信路を通じてエラーの通知を行う。記憶していれば新たに接続 ID を生成し、VMM に ACCEPTED イベントを通知する。

VMM から write 要求を受けると、指定された接続 ID の通信路が確立されていれば、その接続 ID と write 内容を用いて write 要求を外部へ送信する。

外部からデータを受信すると、その接続 ID に関連付けられたバッファを受信した内容を書き込む。また、以前の VMM からの read 要求が完了していなければ、VMM に ARRIVED イベントを通知する。

VMM から read 要求を受けると、その接続 ID に関連付けられたバッファを検査し、データを返す。

### 4. Skype オーバレイネットワークの利用

本研究では、IM として Skype を用いる。Skype は独自のオーバーレイネットワークを形成しており、複雑な設定なしにファイアウォールや NAT(Network Address Translation) を越えて通信を行う機能がある。更に、通信路は Skype によって暗号化されており、安全

な通信を行うことができる。我々は、このネットワークを利用して RPC(Remote Procedure Call) を行う SkypeRPC<sup>3)</sup> を開発した。この SkypeRPC は、Skype のユーザ認証を用いるため、通信相手をユーザレベルで指定できる。

本研究では、この SkypeRPC を用いた外部ヘルパを実装する。実装する機能については SSH のそれと同様で、SSH 通信路を用いて通信を行う部分を SkypeRPC に置き換える形となる。

### 5. 関連研究

既存のアプリケーションの通信を暗号化する手法として、Kernel-level SSL<sup>2)</sup> がある。これは OS のカーネルに SSL(Secure Socket Layer) 通信処理を埋め込み、その OS 上で動作するアプリケーションの通信を暗号化する。しかしカーネルレベルで実装するため、コーディングやメンテナンスが難しくなる。

本研究では、ゲスト OS の通信を VMM で暗号化するため、ホスト OS のユーザレベルで実装を行う。そのため、コーディングやデバッグをカーネルレベルより簡単に行うことができる。

### 6. おわりに

本稿では、ソケットアウトソーシングの仕組みと、その外部ヘルパによるオーバーレイネットワークの利用方法について述べた。今後は、その実装と評価を行う。

### 参考文献

- 1) Eiraku, H., Shinjo, Y., Pu, C., Koh, Y. and Kato, K.: Fast Networking with Socket-Outsourcing in Hosted Virtual Machine Environments, *24th ACM Symposium on Applied Computing*, Vol. 2009, pp. 310-317 (2009).
- 2) 光来健一, 千葉滋: インターネットにおけるパーソナルネットワークの構築, 情報処理学会研究報告. [システムソフトウェアとオペレーティング・システム], Vol. 2001, No. 78, pp. 83-90 (2001-07-26).
- 3) 金子直矢, 新城靖, 佐藤聡, 中井央, 板野肯三: インスタントメッセージを用いたネットワークファイルシステムの実現, 第 20 回コンピュータシステムシンポジウム, ポスター・デモセッション (2008).