論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻　情報・通信工学分野

学生番号	246E0104	氏　名	岩井 正輝
論文題目	VM 内情報を利用可能な P4 プログラムの安全な実行基盤		

1　はじめに

近年，ネットワークスイッチにおいて P4 言語を用いてパケットの転送処理をプログラムできるようになっている．仮想マシン (VM) をネットワークに接続する際に用いられる仮想スイッチについても，仮想 P4 スイッチが開発されている．VM のユーザが仮想スイッチに P4 プログラムをロードできるようになれば，VM ごとに柔軟なパケット処理を実現できる．加えて，P4 プログラムの中で VM 内の情報も利用できれば，よりきめ細かいパケット処理が可能となる．しかし，クラウドにおいて仮想スイッチは信頼できるとは限らないため，ユーザがロードした P4 プログラムを改ざんされたり，P4 プログラムが利用する VM 内の情報を盗聴されたりするリスクがある．逆に，ユーザの P4 プログラムの挙動が仮想スイッチに影響を及ぼす可能性もある．

本研究では，VM 内情報を利用するユーザの P4 プログラムをクラウドの仮想スイッチの外部で安全に実行する P4 Shield を提案する．

2　P4 Shield

P4 Shield は図 1 のように，ユーザごとに用意される P4 のための VM (P4 VM) の中でユーザの P4 プログラムを実行する．クラウドからの攻撃を防ぐために，P4 VM は CPU によって保護される機密 VM として作成する．また，P4 プログラムを P4 VM に分離することで，クラウドの仮想スイッチを保護する．仮想スイッチはユーザ VM が送受信するパケットを対応する P4 VM に送り，P4 プログラムを実行する．P4 プログラムはユーザ VM 内の情報を利用して転送の可否を判断し，その結果を基に仮想スイッチがパケットを転送する．

P4 VM 内では複数の P4 プログラムが実行されることがあるため，uBPF を用いて P4 プログラム同士を隔離実行する．P4 Shield は P4 プログラムを uBPF バイトコードにコンパイルし，P4 VM 内の uBPF ランタイムにロードする．ロード時に検証を行うことにより，P4 プログラムの安全な実行が保証される．また，ロード時に JIT コンパイルを行うことにより，P4 プログラムの高速な実行を可能にする．

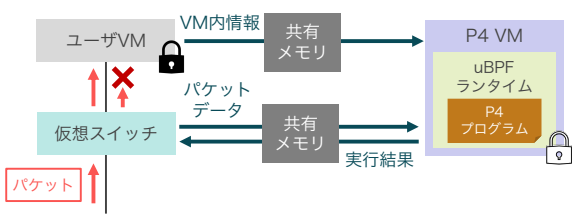

図 1. P4 Shield のシステム構成

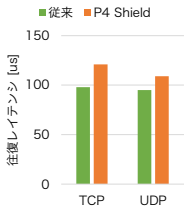

図 2. レイテンシ

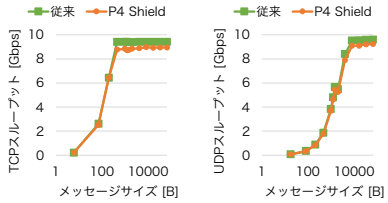

図 3. スループット

P4 プログラムはユーザ VM が P4 VM との間の共有メモリに格納した VM 内情報を取得して利用する．従来の P4 プログラムはパケットデータにしかアクセスできないため，P4 Shield はユーザ VM 内の情報を取得するための API を P4 の外部関数として提供する．外部関数を用いることにより，P4 言語を拡張せずに VM 内情報を利用することができる．外部関数は共有メモリにアクセスできないため，uBPF ランタイムが提供するヘルパー関数を呼び出してアクセスする．

3　実験

P4 Shield を用いて，ユーザ VM 内の情報を活用したパケットフィルタリングを行った．この実験では，TCP メモリの枯渇時に新規 TCP 接続を拒否する P4 プログラムをロードした．大量の TCP 接続を行ったところ，既存接続は活かしたまま新規接続要求パケットのみを破棄できることを確認した．

P4 Shield のオーバヘッドを調べるために，リモートホストからユーザ VM への TCP と UDP の転送性能を測定した．往復レイテンシは図 2 に示すように，従来の仮想スイッチを用いた場合と比較して TCP で 23 %，UDP で 15 %増加した．スループットは図 3 に示すように，TCP で 5 %，UDP で 4 %の増加にとどまった．

4　まとめ

本研究では，VM 内情報を利用できるように拡張した P4 プログラムをユーザごとに用意される P4 VM で安全に実行する P4 Shield を提案した．今後の課題は，VM 内情報を取得するための API を整備することである．