論文概要

学科	情報・通信工学科	指導教員	光来健一
学生番号	１８２Ｃ１１４７	氏名	堀恭介
題目	eBPF プログラムを用いた VM 内のシステムの監視		

1　はじめに

仮想マシン（VM）を提供する IaaS 型クラウドでは，高度なサービスを提供するために VM 内のシステムの監視を行っている．VM 内の情報を取得するための手法として，エージェント方式とイントロスペクション方式が用いられている．しかし，エージェント方式では VM 内にエージェントをインストールする必要があるため，エージェントの保守を怠ると脆弱性になる可能性がある．イントロスペクション方式は VM のメモリを解析して OS データを取得するため，開発や適用が難しく，最近の CPU の機能を用いて VM のメモリが暗号化されると利用できない．

そこで，本研究ではクラウド側から VM に eBPF プログラムを送り込んで安全に実行し，VM 内のシステムを監視するシステム TeleBPF を提案する．

2　TeleBPF

TeleBPF は図 1 のように，クラウド側で eBPF アプリケーションを動作させ，VM 内の OS に eBPF プログラムを動的に送り込んで情報を取得する．eBPF は Berkeley パケットフィルタを拡張した Linux の機構であり，OS 内の指定した箇所で性能などを監視するために用いられている．eBPF プログラムは実行時に検査器を用いてチェックされるため OS 内で安全に実行することができ，開発も比較的容易である．

TeleBPF では，BPF Compiler Collection (BCC) を用いて開発された既存の eBPF アプリケーションを実行することができる．そのために，BCC の共有ライブラリを実行時に置き換え，その共有ライブラリが BPF 関連のシステムコールの呼び出しを VM に転送する．具体的には，VM 内で動作するプロキシと通信し，VM 内の OS に対してシステムコールを実行させる．その際に，システムコールの引数をシリアライズすることでバイト列に変換して送信し，プロキシで元のデータ構造に復元する．システムコール実行後にも通信を行い，実行結果を eBPF アプリケーションに返す．

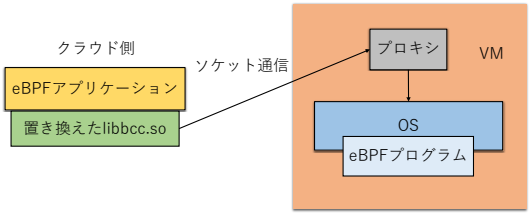

図 1: TeleBPF のシステム構成

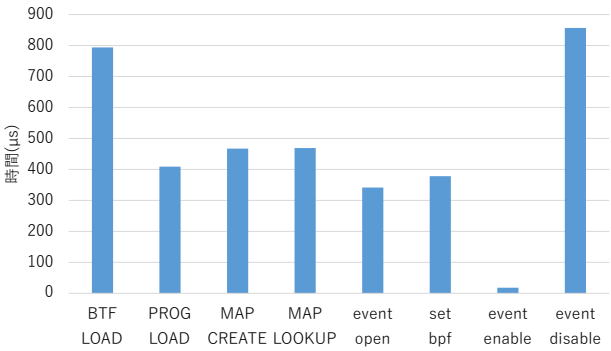

図 2: プロキシ経由での実行オーバヘッド

3　実験

TeleBPF を用いて read システムコールの実行回数を取得する eBPF アプリケーションを実行し，BPF 関連のシステムコールをプロキシ経由で実行するのにかかる時間を測定した．比較として，TeleBPF を用いずにこの eBPF アプリケーションを実行した場合についても測定を行った．実験の結果，それぞれのシステムコールの実行オーバヘッドは図 2 のようになった．これは eBPF アプリケーションの実行時間全体の 16% であった．

4　まとめ

本研究では，eBPF プログラムをクラウド側から VM 内の OS に送り込み，VM 内の情報を安全に取得するシステム TeleBPF を提案した．今後の課題は，様々な BPF 関連のシステムコールに対応することである．