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	226E0132	氏　名	堀 恭介
論文題目	eBPF フレームワークを用いた VM 内の透過的なシステム監視		

1　はじめに

Amazon EC2 などの IaaS 型クラウドはユーザに仮想マシン（VM）を提供しており，VM 内にインストールされたエージェントを用いて VM 内の情報を収集し活用することが多い．このエージェント方式の問題点は VM のユーザがエージェントの保守作業を行う必要があることであり，この作業を怠ると脆弱性となる可能性がある．それに対して，もう 1 つの方式であるイントロスペクション方式では，クラウド側が VM のメモリなどに直接アクセスして VM 内の情報を取得する．しかし，AMD SEV を用いてメモリが暗号化された VM には適用できないという問題がある．

本研究では，クラウド側から VM に eBPF プログラムを動的に送り込み，VM 内の情報を安全かつ透過的に取得するシステム TeleBPF を提案する．

2　TeleBPF

TeleBPF は eBPF プログラムをエージェントとして VM に送り込み，OS 内で安全に実行する．そして，クラウド側で動作する eBPF アプリケーションが VM 内の eBPF プログラムから透過的に情報を取得する．eBPF は Linux に標準搭載されている機構であり，イベントの発生時に OS やプロセスに関する情報を取得するために用いられている．TeleBPF では必要に応じて eBPF プログラムが VM 内に動的に送り込まれるため，ユーザによる管理が不要となる．また，VM のメモリ暗号化の影響を受けずに情報を取得することができる．

TeleBPF は図 1 のように BPF アプリケーションに TeleBPF 共有ライブラリを提供し，eBPF 関連のシステムコールを VM に転送する．その際に，Zpoline[1] を用いてバイナリ書き換えを行うことによりシステムコールの呼び出しを高速に横取りする．TeleBPF 共有ライブラリはシステムコールの種類や引数を VM 内の TeleBPF プロキシに送信し，システムコールの代理実行の結果を取得する．汎用的に用いられるシステムコールについては，ファイル記述子などの値に基づいて BPF 関連の場合にのみ転送を行う．TeleBPF プロキシを保護するために，VM 内の監視対象システムはコンテナに隔離する．

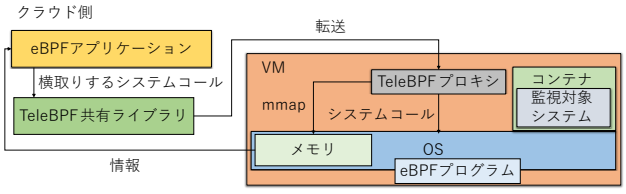

図 1. TeleBPF のシステム構成

TeleBPF は eBPF アプリケーションがリングバッファを用いて VM 内の eBPF プログラムとの間で情報を受け渡すことを可能にする．リングバッファのメモリにアクセスできるようにするために用いられる mmap システムコールを VM に転送し，取得した仮想アドレスをページテーブルを参照して物理アドレスに変換する．その際に，リングバッファが複数の物理ページにまたがる場合には連続して配置されるようにする．

3　実験

TeleBPF を用いて Microsoft Sysmon for Linux を実行し，VM 内のプロセスの生成・終了がクラウド側で監視できることを確認した．また，VM 内で実行されたプロセスの情報をシステムコールまたはリングバッファで取得するのにかかる時間を測定した．図 2 に示すように，TeleBPF ではシステムコールを用いて情報を取得すると時間がかかることが分かった．一方，リングバッファを用いると従来の 1.5 倍の時間で取得することができた．

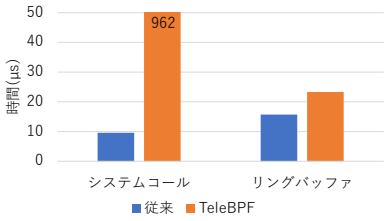

図 2. 情報取得性能

4　まとめ

本研究では，eBPF プログラムをクラウド側から VM 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，様々な監視システムに適用できるようにすることである．

参考文献

[1] K. Yasutaka et al., ”zpoline: a System Call Hook Mechanism Based on Binary Rewriting,” ATC 2023.