コース	情報通信ネットワーク	指導教員	光來 健一
学生番号	212C1161	氏　　名	山口 紘輝
論文題目	uBPF プログラムを用いたデータ一括取得による機密 VM の高速な監視		

1　はじめに

近年，クラウドによって提供される仮想マシン (VM) の利用が増加しており，その内部で機密情報が扱われることも多くなっている．それに伴い，クラウドの内部犯による VM 内の機密情報の盗聴が問題となっている．このような情報漏洩を防ぐために，最近のクラウドは CPU の隔離実行環境を用いて保護された機密 VM を提供している．機密 VM であっても内部に侵入されると盗聴を防ぐことができないため，侵入検知システム (IDS) を用いて VM の監視を行う必要がある．IDS を VM 内で動作させると侵入時に無効化される恐れがあるため，VM の外からメモリ上の OS データを監視する IDS オフロードが用いられる．機密 VM は VM の外からアクセスできないため，VM の BIOS 内で動作するエージェント経由で安全に OS データを取得するシステム [1] が提案されている．しかし，OS データが必要になるたびに SMI と呼ばれる割り込みを VM に挿入する必要があり，VM を監視するためのオーバーヘッドが大きい．

本研究では，機密 VM の BIOS に uBPF プログラムを送り込み，OS データを一括取得することにより VM の高速な監視を実現する uBPF-SV を提案する．

2　uBPF-SV

uBPF-SV は図 1 のように，機密 VM の BIOS 内でエージェントを動作させ，SMI を挿入して IDS から送り込まれた uBPF プログラムを実行する．VM の仮想 CPU のシステム管理モードを用いてエージェントを実行することにより，uBPF プログラムを監視対象システムから保護する．また，uBPF プログラムのロード時に検証を行うことにより，送り込まれたプログラムを BIOS 内で安全に実行する．uBPF プログラムを用いて IDS が必要とする OS データを一括取得することにより，VM への SMI の挿入回数を減らして監視性能を向上させることができる．

uBPF-SV は IDS ごとに必要となる uBPF プログラムを監視対象 VM に送り込む．IDS は uBPF プログラムを共有メモリに格納してから VM に SMI を挿入する．BIOS 内の SMI ハンドラによってエージェントが呼び出されると，エージェントは共有メモリ上の uBPF プログラムを uBPF ランタイムにロードする．IDS が uBPF プログラムを実行する際も同様にしてエージェントを呼び出し，エージェントが uBPF プログラムを実行して一括取得した OS データを共有メモリに格納する．IDS は共有メモリ上の OS データをキャッシュに格納し，必要になった時に利用する．

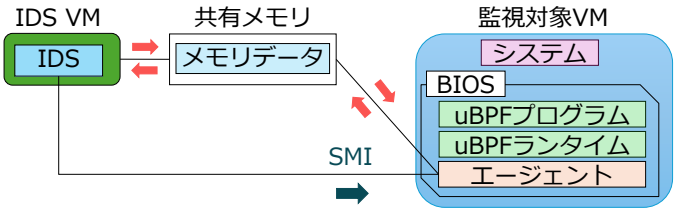

図 1. uBPF-SV のシステム構成

uBPF プログラムは監視対象システムのメモリ上の OS データを共有メモリにコピーする．しかし，uBPF プログラムは直接，システムメモリや共有メモリにアクセスすることはできないため，uBPF ランタイムによって提供されるヘルパー関数を利用する．このヘルパー関数はシステムメモリ上の OS データの仮想アドレスを物理アドレスに変換し，物理アドレスに対応するメモリデータを共有メモリにコピーする．アドレス変換に失敗した場合はシステムメモリにアクセスしないため，不正な仮想アドレスへのアクセスは行われない．また，共有メモリの範囲外のアドレスが指定された場合も検出することができる．

3　実験

uBPF-SV を用いて uBPF プログラムをロードし，OS のバージョン情報を含む 2 つの文字列を一括取得できることを確認した．次に，これら 2 つの OS データを一括取得するのにかかる時間を測定した．比較として，2 つの OS データを BIOS 内のエージェント経由で 1 つずつ取得する先行研究についても測定を行った．それぞれの取得時間を図 2 に示す．この結果から，uBPF-SV は先行研究と比べて監視性能を 58% 向上させられることがわかった．

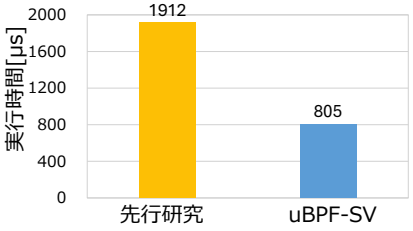

図 2. 2 つの OS データの取得時間

4　まとめ

本研究では，機密 VM を効率よく監視するために BIOS に uBPF プログラムを送り込んで OS データを一括取得する uBPF-SV を提案した．今後の課題は，uBPF プログラムを用いて OS データを解析しながら一括取得できるようにすることである．

参考文献

[1] 末永: AMD SEV で保護された VM の SMI インジェクションを用いた監視. 九州工業大学卒業論文, 2024.