コース	—	指導教員	光來 健一
学生番号	16237050	氏　　名	武田 一希
論文題目	SEV で保護された VM を監視可能にするエージェントの SMM による隔離		

1　はじめに

近年，クラウドの仮想マシン (VM) が広く用いられているが，VM のメモリ上にある機密情報がクラウドの内部犯に盗聴されるリスクがある．このような情報漏洩を防ぐために，VM のメモリを透過的に暗号化する CPU 機構である AMD SEV が用いられている．一方，VM 内に侵入されると SEV ではメモリの保護が行えないため，侵入検知システム (IDS) を用いて VM を監視する必要がある．侵入後に IDS が無力化されるのを防ぐために IDS を VM の外で動作させる IDS オフロードが用いられているが，オフロードされた IDS は VM のメモリが暗号化されていると情報を取得することができない．そこで，監視対象 VM の内部でエージェントと呼ばれるソフトウェアを安全に動作させることにより IDS オフロードを実現する SEVmonitor [1] が提案されている．しかし，エージェントの安全性と性能にはトレードオフがある．監視対象システムをコンテナに隔離してエージェントを OS 内に配置する場合，OS が攻撃を受けるとエージェントも無効化される．監視対象システムを内部 VM に隔離してエージェントをハイパーバイザ内に配置する場合，VM 内で VM を動かすオーバヘッドが大きい．

本研究では，SEV でメモリが暗号化された VM に対して BIOS 内にエージェントを配置することで IDS オフロードを実現するシステムを提案する．

2　提案システム

本研究で提案するシステムは，SEVmonitor におけるエージェントを図 1 のように BIOS 内のシステムマネジメントモード (SMM) で動作するプログラムとして実行する．SMM は Intel や AMD 製 CPU の動作モードの一つであり，OS の下で動く BIOS によってのみ使用可能である．SMM は SMRAM と呼ばれる保護されたメモリ上にプログラムを配置し，OS でさえアクセスできない独立した実行環境を提供する．そのため，OS が攻撃を受けたとしてもエージェントを無効化することはできない．また，SMM プログラムはシステムのメモリデータを取得する最小限の処理を行うだけであるため，監視対象システムに対するオーバヘッドは小さい．

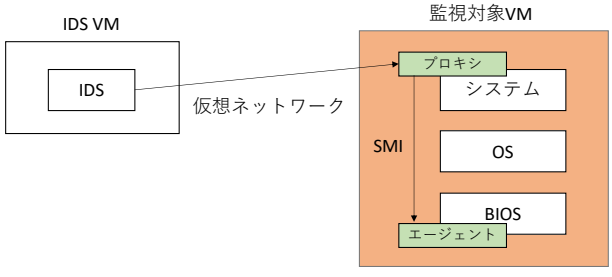

図 1. 提案システムの構成

提案システムは SEVmonitor と同様に，IDS を SEV で保護された IDS VM 内で動作させる．IDS が OS データを必要とした時には，その仮想アドレスを監視対象 VM 内で動作するプロキシに送信する．プロキシはシステムマネジメント割り込み (SMI) と呼ばれるソフトウェア割り込みを発生させることにより，BIOS 内の SMM プログラムを呼び出す．SMM プログラムは OS のメモリ上にあるページテーブルを用いて渡された仮想アドレスを物理アドレスに変換し，対応するメモリデータを取得する．取得したメモリデータはプロキシに返され，プロキシがそれを IDS に送信する．監視対象システム内で動作するプロキシや VM 間の仮想ネットワーク上での盗聴を防ぐために，メモリデータは SMM プログラムが暗号化し，IDS が復号する．

3　実験

監視対象 VM の OS のバージョン情報が格納されたメモリデータを取得する IDS を実行したところ，バージョン情報が正しく取得できることが確認ができた．次に，そのメモリデータを監視対象 VM から取得するのにかかる時間を測定した．図 2 に示すように，提案システムはエージェントを OS 内に配置する SEVmonitor より 2 倍高速であった．VM 間の通信に仮想ネットワークではなく共有メモリを用いるようにすると，SEVmonitor と同様に高速化できると考えられる．

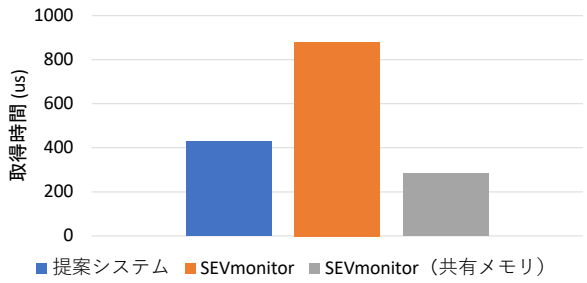

図 2. バージョン情報の取得時間

4　まとめ

本研究では，SEV でメモリが暗号化された VM に対して SMM で動作するエージェントを用いることで IDS オフロードを実現するシステムを提案した．今後の課題は，監視対象 VM 内のプロキシを用いずに SMM プログラムを呼び出せるようにすることである．

参考文献

[1] 能野, 光来. AMD SEV で保護された VM の隔離エージェントを用いた安全な監視. *CSS 2022*.