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　情報創成工学分野

学生番号	21675029	氏　名	能野　智玄
論文題目	AMD SEV で保護された VM に対する VM 内隔離環境を用いた安全な監視		

1　はじめに

ユーザに仮想マシン (VM) を提供する IaaS 型クラウドにおいては，VM のメモリ上にある機密情報を内部犯に盗まれるリスクがある．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 ではメモリ上の機密情報が保護できないため，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には IDS を VM の外で動作させる IDS オフロードが有効であるが，オフロードされた IDS は SEV を用いて暗号化された VM のメモリから情報を取得することができない．

本研究では，SEV を用いてメモリが暗号化された VM の内部でエージェント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システム SEVmonitor を提案する．

2　SEVmonitor

SEVmonitor は図 1 のように監視対象 VM の内部でメモリデータを取得するためのエージェントを安全に動作させる．エージェントを導入することにより，SEV を用いて VM のメモリが暗号化されていても，オフロードされた IDS はエージェント経由で VM のメモリデータを取得して OS データを解析することができる．また，SEVmonitor は IDS も SEV を用いてメモリが暗号化された IDS VM 内で安全に実行する．これにより，攻撃者は IDS を攻撃することによって IDS が取得した監視対象 VM 内の機密情報を盗むことはできない．IDS とエージェントは VM 間の暗号化された仮想ネットワークまたは共有メモリを用いて通信する．

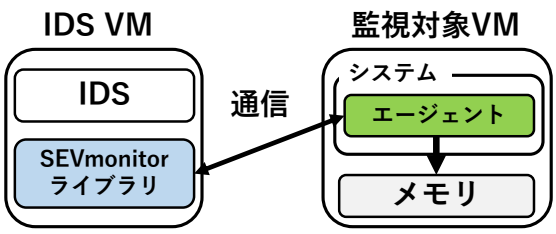

図 1: SEVmonitor のシステム構成

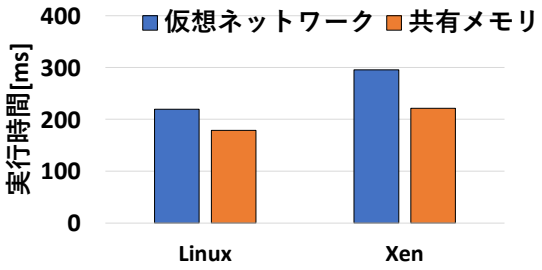

図 2: システム情報の取得時間

監視対象 VM 内に配置されるエージェントは VM 内の監視対象システムに侵入されたとしても無効化されず，安全に動作し続けることができなければならない．SEVmonitor は監視対象 VM 内でシステムを隔離環境に閉じ込め，その外側にエージェントを配置する．用いる隔離環境によって様々なトレードオフが存在するため，SEVmonitor はコンテナと VM の 2 種類の隔離環境を用い，エージェントをそれぞれ OS カーネルまたはハイパーバイザ内に配置する．

3　実験

SEVmonitor の監視性能を調べるために，多くの IDS が用いる proc ファイルシステムの構築に必要な OS データを監視対象 VM から取得する時間を測定した．この実験では Linux カーネルまたは Xen ハイパーバイザ内にエージェントを配置した．図 2 に示すように，カーネル内エージェントはハイパーバイザ内エージェントより 26〜40%高速であった．これはカーネル内では取得する OS データの仮想アドレスを変換する必要がないためと考えられる．また，仮想ネットワークを用いて通信を行うより共有メモリを用いた方が 18〜25%高速になった．

4　まとめ

本研究では，SEV を用いてメモリが暗号化された VM の内部でエージェントを隔離して安全に動作させ，IDS オフロードを可能するシステム SEVmonitor を提案した．今後の課題は様々な IDS を実行できるようにすることである．