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	246E0115	氏　名	梶原 悠大
論文題目	RISC-V CoVE を用いた機密 VM の柔軟で効率的な監視機構		

1　はじめに

ユーザに仮想マシン (VM) を提供する IaaS 型クラウドの普及に伴い，内部犯に機密情報を盗聴されるリスクが高まっている．そこで，最近のクラウドはハードウェアベースの隔離実行環境 (TEE) を用いて保護された機密 VM を提供している．近年，注目されているオープンソースの CPU コアである RISC-V においても CoVE と呼ばれる拡張機能が提供され，メモリが隔離された TEE VM (TVM) の利用が可能になっている．しかし，TVM のメモリ隔離は外部からの不正アクセスを防ぐためのものであり，TVM 内部に侵入された場合には無力である．そのため，侵入検知を行う監視システムが必要であるが，TVM 内部の監視システムは攻撃者によって無効化される恐れがある．一方で，TVM の外部からの監視はメモリの隔離により困難である．

本研究では，CoVE において TVM の柔軟かつ効率的な監視を実現する TVMmonitor を提案する．

2　TVMmonitor

TVMmonitor は，図 1 のように監視用 TVM で監視システムを実行し，監視対象 TVM 内のエージェントから情報を取得して監視を行う．監視用 TVM は TEE セキュリティマネージャ (TSM) によって他の VM から隔離されているため，安全に監視を行うことができる．監視用 TVM を用いることにより，分散型の監視システムを構築することが可能である．例えば，1 つの監視用 TVM で複数の TVM を効率よく監視したり，複数の監視用 TVM で 1 つの TVM を分担して監視したりすることができる．

TVMmonitor は TVM 間でメモリを共有することにより，監視対象 TVM の情報を高速かつ安全に取得する．TVM の機密メモリは共有できないため，VM を管理するハイパーバイザとの通信に用いられる非機密メモリを利用して TVM 間の共有メモリを実現する．まず，監視用 TVM と監視対象 TVM がそれぞれ TSM を呼び出し，指定した機密メモリを非機密メモリに変換する．次に，監視用 TVM がその非機密メモリを共有メモリとして登録し，監視対象 TVM がその非機密メモリで自身の非機密メモリを置き換える．

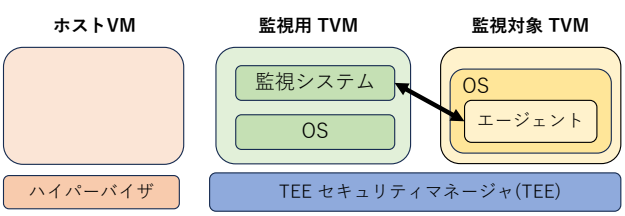
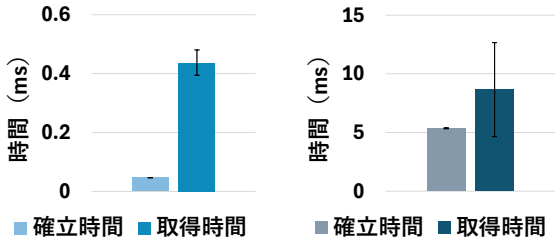


図 1. TVMmonitor のシステム構成



(a) 共有メモリ　(b) 仮想ネットワーク

図 2. システム情報の取得時間

特定の監視対象 TVM のみが監視用 TVM のメモリを共有できるように，共有 ID と認証キーの正しい組み合わせが TSM に提示された場合のみ共有を許可する．共有メモリは非機密メモリであるため，データを暗号化して書き込むことで，ハイパーバイザへの情報漏洩を防ぐ．さらに，監視対象 TVM 内のエージェントが侵害された場合に備え，監視用 TVM が TSM を介して監視対象 TVM のメモリデータを直接コピーして監視を行うこともできる．

3　実験

CoVE に準拠したシステム ACE に TVMmonitor を実装し，実機の SiFive P550 を用いて TVM 内の情報を取得する実験を行った．その結果，TVM 間の共有メモリを用いてプロセス一覧やカーネルモジュール一覧を正しく取得できた．次に，共有メモリを確立する時間と情報を取得する時間を測定した．比較として，TVM 間で仮想ネットワークを用いた場合についても測定した．図 2 に示すように，TVMmonitor の方が通信路の確立にかかる時間は 114 倍，情報を取得する時間は 19 倍高速であった．

4　まとめ

本研究では，RISC-V CoVE を用いた機密 VM の柔軟かつ効率的な監視を実現する TVMmonitor を提案した．今後の課題は，より複雑な分散監視システムを構築できるようにすることである．