九州工業大学 情報工学部 情報・通信工学科 2023 年度 卒業論文 概要

コース	ソフトウェアデザイン	指導教員	光來 健一
学生番号	212C1046	氏　　名	梶原 悠大

論文題目	RISC-V における Confidential VM の柔軟かつ効率のよい監視

1　はじめに

IaaS 型クラウドが普及しているが，クラウド内には内部犯がいる可能性があり，仮想マシン (VM) の機密情報を盗聴される恐れがある．そのため，最近のクラウドは TEE と呼ばれるハードウェアで保護された Confidential VM を提供するようになっている．Confidential VM のメモリは暗号化されているため，クラウドの内部犯でさえメモリを盗聴できなくなる．近年，命令セットアーキテクチャがオープンソースで提供されている RISC-V が注目されており，VM を動かすためのハイパーバイザ拡張や Confidential VM 拡張 (CoVE) も提供されるようになってきている．CoVE はメモリが隔離された TEE VM (TVM) を Confidential VM として実行することができる．しかし，TVM 内に侵入されると機密情報の盗聴を防ぐことができない．そのため，TVM の外から安全に TVM 内のシステムの監視を行えるようにする必要がある．

本研究では，RISC-V CoVE において TVM の柔軟かつ効率のよい監視を実現する TVMmonitor を提案する．

2　TVMmonitor

TVMmonitor は図 1 のように監視用 TVM で監視ソフトウェアを実行し，共有メモリを用いて監視対象 TVM の OS から情報を取得することにより監視を行う．CoVE では TEE セキュリティマネージャ (TSM) が TVM のメモリのアクセス制御を行い，信頼できないホスト VM 内で動作するハイパーバイザが TVM の管理を行う．監視用 TVM を用いることで，TSM で監視を行うよりも柔軟に監視を行うことができる．また，TVM 間で共有メモリを用いて情報を取得することにより，仮想ネットワークを用いて通信を行うより高速に監視を行うことができる．

CoVE では TVM 間でのメモリ共有はサポートされていないため，TVMmonitor は TVM のメモリを安全に共有する機構を提供する．TVM のメモリページの属性は標準ではその TVM しかアクセスすることができない「専用」になっているため，共有したいページの属性を「共用」に変更する．そのために，監視用 TVM と監視対象 TVM はそれぞれ SBI ecall を用いて TSM を呼び出し，ページの属性を変更する．それに加えて，TSM からホスト VM 内のハイパーバイザを呼び出し，指定されたページを TVM 用の共用ページリストに登録する．

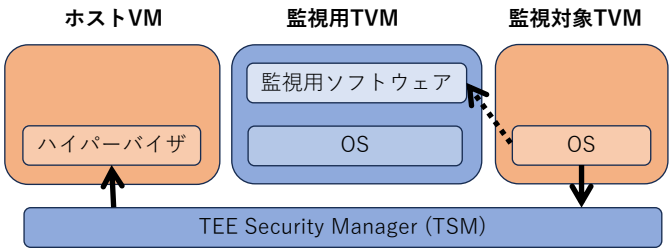

図 1. TVMmonitor のシステム構成

次に，監視用 TVM のページを監視対象 VM と共有する．まず，監視用 TVM は TSM 経由でハイパーバイザを呼び出し，属性を共用に変更したページを登録する．一方，監視対象 VM はハイパーバイザを呼び出し，その TVM 用の共用ページリストの中のページを登録された監視用 VM のページで置換する．特定の監視対象 TVM だけがメモリを共有できるようにするために，ページの登録時と置換時にそれぞれの TVM にキーを指定させ，キーが一致する時だけ TSM がページの置換を許可する．

3　実験

TVMmonitor を用いて TVM 内のプロセスの一覧が取得できることを確認する実験を行った．CoVE に対応した実機がまだないため，QEMU 上で RISC-V CPU と CoVE のエミュレーションを行った．本実験では，TVM 間で共有メモリを介した通信を行うカーネルモジュールを実装した．監視用 TVM が共有メモリにプロセス一覧の要求を書き込むと，監視対象 TVM が共有メモリにプロセス情報を書き込む．これらのカーネルモジュールを実行すると，図 2 に示すようにプロセスの一覧を取得して表示することができた．また，図 3 に示すように，指定されたキーが一致しない時にはメモリが共有できないことを確認した．

```
/host/root # insmod TVM1.ko
[   61.281112] TVM1: loading out-of-tree module taints kernel.
[   61.281112] TVM1: loading out-of-tree module taints kernel.
[   61.335775] key = 4294967205
[   61.335775] key = 4294967205
[   62.848604] 1: init
[   62.848604] 2: kthreadd
[   62.848604] 3: rcu_gp
```

図 2. プロセス取得の一覧

```
/host/root # insmod TVM2.ko
[   46.796121] TVM2: loading out-of-tree module taints kernel.
[   46.796121] TVM2: loading out-of-tree module taints kernel.
[   46.855675] key = 4294967290
[   46.855675] key = 4294967290
[   46.856988] Cannot share memory
[   46.856988] Cannot share memory
```

図 3. キーが異なる場合

4　まとめ

本研究では，RISC-V CoVE において Confidential VM の柔軟かつ効率のよい監視を実現する TVMmonitor を提案した．今後の課題は，信頼できないハイパーバイザが共有メモリを読み書きできないようにすることである．