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	246E0133	氏　名	西村　優志
論文題目	AMD SEV-SNP で保護された VM の選択的なメモリ監視機構		

1　はじめに

クラウド向けに仮想マシン (VM) 上で軽量な OS を用いてアプリケーションを 1 つだけ実行する Unikernel が提案されている．Unikernel は汎用 OS を用いる場合と比べて起動や実行が高速であるという特長がある．CPU が提供する隔離実行環境の AMD SEV-SNP を用いて VM を保護することで，クラウドによる Unikernel 内の機密情報の盗聴を防ぐこともできる．一方で，最低限のリソースしか割り当てない Unikernel には異常が発生しやすいため，挙動を監視する必要がある．しかし，最小限の機能しか持たない Unikernel 内では監視が難しい．また，Unikernel が SEV-SNP で保護されている場合には，VM 外から VM のメモリ上にある OS データを監視する手法を用いることもできない．

本研究では，Unikernel が SEV-SNP によるメモリ暗号化を選択的に解除することで Unikernel の外からの監視を可能にする ShadowMonitor を提案する．

2　ShadowMonitor

ShadowMonitor は図 1 のように，指定したメモリ領域の暗号化を部分的に解除することができる．例えば，Unikernel OS が管理しているシステム情報へのアクセスを許可することが考えられる．メモリ暗号化の制御はメモリ管理のために用いられるページテーブルを用いて Unikernel 自身が行う．そのため，機密情報が格納されたメモリ領域の暗号化をクラウドから解除することはできない．

外部の監視機構が Unikernel のメモリを解析できるようにするために，ShadowMonitor はページテーブルを複製してシャドウページテーブルを作成する．シャドウページテーブルの暗号化を解除することにより，監視機構はシャドウページテーブルを参照して仮想アドレスを物理アドレスに変換し，OS データにアクセスすることができる．シャドウページテーブルのアドレスは Unikernel がその下で動作しているハイパーバイザに通知し，監視機構はハイパーバイザからアドレスを取得する．監視機構をクラウドから保護する必要がある場合には，Unikernel と監視機構の両方を SEV-SNP で保護された機密 VM の中で実行することもできる．

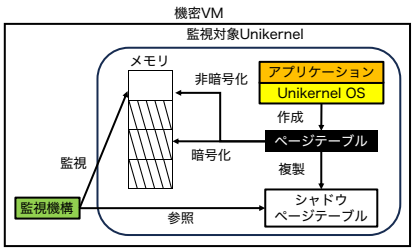

図 1. ShadowMonitor のシステム構成

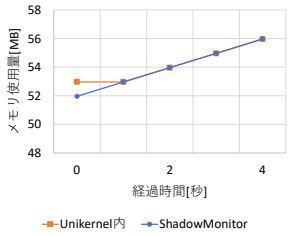

図 2. メモリ使用量

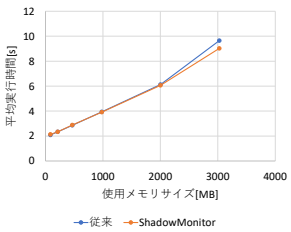

図 3. 実行時間

暗号化を解除するメモリ領域の指定は用意されたポリシの中からユーザが選択することによって行う．暗号化の制御はページ単位で行われるため，ポリシが異なる OS データが同じメモリページに含まれる可能性がある．そこで，Unikernel OS のメモリ割り当て時にポリシを指定し，ポリシごとに異なるページを割り当てることにより，同じページには同じポリシのデータのみが格納されるようにする．

3　実験

ShadowMonitor を用いて Unikernel の使用メモリ量の監視を行った結果，異常終了する前に空きメモリの枯渇を検知することができた．観測した値は図 2 のようになり，Unikernel 内で測定した値とほぼ同じであることを確認した．

ShadowMonitor によるオーバヘッドを調べるために，使用メモリ量を変えながら Unikernel の実行時間を測定した．測定結果は図 3 のようになり，ShadowMonitor を用いない場合と比べて実行時間の増加は最大 2.3%であった．

4　おわりに

本研究では，Unikernel が SEV-SNP によるメモリ暗号化を選択的に解除することで Unikernel の外からの監視を可能にする ShadowMonitor を提案した．今後の課題は，アプリケーションのデータの監視も行えるようにすることである．