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	202C1110	氏　　名	西村 優志
論文題目	AMD SEV で保護された VM 内の OS が制御可能なメモリ監視機構		

1　はじめに

クラウド向けに仮想マシン (VM) を用いて軽量な OS とともに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高速に起動・実行が行うことが可能である．また，AMD SEV と呼ばれる CPU のセキュリティ機構を用いて VM のメモリを保護することにより，Unikernel 内の機密情報が盗聴されることを防ぐこともできる．Unikernel の異常を検知するためには挙動を監視する必要があるが，最小限の機能だけを提供する Unikernel 内では高度な監視は難しい．しかし，VM のメモリが SEV で保護されている場合には，VM 外の監視機構が VM のメモリ上にある Unikernel のデータを監視することもできない．

本研究では，SEV で保護された VM 内の Unikernel OS が制御可能なメモリ監視機構を備えたシステムである ShadowMonitor を提案する．

2　ShadowMonitor

ShadowMonitor は図 1 のように，VM 内の機密情報を含まないメモリ領域は暗号化しないようにし，それ以外のメモリは暗号化したままにする．例えば，Unikernel が管理している空きメモリのサイズなどのシステム情報は一般的に機密情報ではない．暗号化しないようにしたメモリ上のデータを VM 外の監視機構から取得し，それを解析することによってシステムの監視を行う．SEV は VM 内のページテーブルを用いてメモリ暗号化を制御する．ページテーブルエントリ (PTE) の C ビットが 1 の時に対応するページが SEV によって暗号化される．ShadowMonitor は暗号化しないようにするページに対応する，PTE の C ビットを 0 にすることで VM 外からのアクセスを可能にする．

ShadowMonitor は監視機構が VM のメモリを解析できるようにするために，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．VM 外の監視機構は物理アドレスを用いて VM のメモリにアクセスするため，Unikernel の仮想アドレスを物理アドレスに変換する必要がある．しかし，SEV では VM 内のページテーブルは必ず暗号化されるため，

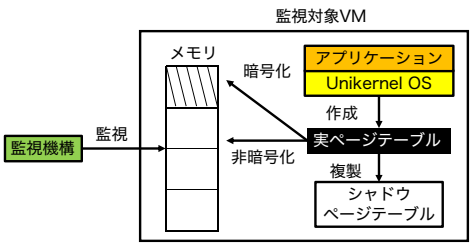

図 1. ShadowMonitor のシステム構成

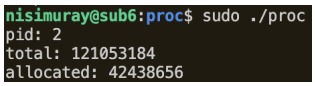

図 2. 取得できたシステム情報

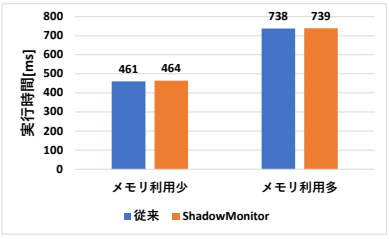

図 3. シャドウページテーブルのオーバヘッド

暗号化しないようにして VM 外から参照できるようにすることはできない．そこで，Unikernel OS がページテーブルに使われるページを新たに割り当てた時にそのページを複製して暗号化しないようにする．ただし，OS の起動の初期段階で割り当てられたページは暗号化しないようにすることができないため，後でページの内容をコピーしてから暗号化を解除し，コピーしておいた内容を書き戻す．

VM 外の監視機構はシャドウページテーブルを参照することでアドレス変換を行う．VM のメモリ上でシャドウページテーブルを特定できるようにするために，ShadowMonitor は実ページテーブルのページディレクトリの次のページにシャドウページテーブルのページディレクトリを配置する．これにより，CPU レジスタから取得したページディレクトリのアドレスからシャドウページテーブルのアドレスを計算することができる．

3　実験

ShadowMonitor を Unikernel の一つの Nanos に実装し，VM 外から OS の情報を取得する実験を行った．その結果，シャドウページテーブルを用いてアドレス変換を行い，暗号化しないようにしたシステム情報が図 2 のように取得できることを確認した．次に，シャドウページテーブルを作成するオーバヘッドを調べるために，アプリケーションの実行時間を測定した．図 3 に示すように，ShadowMonitor による実行時間の増加は 1%未満であったため，オーバヘッドは十分に小さいといえる．

4　まとめ

本研究では，SEV で保護された VM 内の Unikernel OS が制御可能なメモリ監視機構を備えたシステムである ShadowMonitor を提案した．今後の課題は，暗号化しないようにする情報を指定できるようにすることである．