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

学生番号	15675039	氏　名	美山　翔平
論文題目	クラウドにおける仮想化システム外部からの安全な VM 監視		

1　はじめに

IaaS 型クラウドはユーザに仮想マシン（VM）を提供し，ユーザは自由にシステムを構築することができる．一方，クラウド内のユーザ VM はインターネット経由での攻撃を受けやすいため，侵入検知システム（IDS）を用いた監視が必要とされている．そのために，IDS をユーザ VM の外側で動作させて安全に監視を行う IDS オフロードと呼ばれる手法が提案されている．しかし，クラウドにおいては管理者が信頼できるとは限らないため，オフロードした IDS が正しく動作していることを保証するのは難しかった．従来，仮想化システム内の一部を信頼する手法が提案されてきたが，クラウド管理者が従来通りの管理を行えなくなるなどの問題があった．

本研究では，仮想化システムの外部から安全に VM を監視するシステム V-Met を提案する．

2　V-Met

V-Met はネストした仮想化と呼ばれる技術を用いて仮想化システムの外部で IDS を動作させることを可能にする．これまで，仮想化システムの外側のハードウェア上で監視を行うシステムが提案されてきたが，既存の高機能な IDS を動作させることは難しかった．V-Met では，図 1 のように仮想化システム全体を**クラウド** *VM* と呼ばれる VM 内で動作させ，クラウド VM の外側で既存の IDS を動作させる．

V-Met において，仮想化システムの中からその外側へのアクセスはクラウド VM に提供される仮想ハードウェアのインタフェースに限定される．そのため，従来システムに比べて，仮想化システム内部のクラウド管理者が IDS を攻撃するのはより困難になる．また，仮想化システムの一部を信頼する必要がなくなるため，クラウド管理者に仮想化システム全体を管理する権限を与えることができる．これにより，クラウド管理者は従来通りの管理を行うことが可能となる．

V-Met はオフロードした IDS が仮想化システム内のユーザ VM のメモリ，ネットワーク，ディスクから情報を取得することを可能にする．IDS はクラウド VM のメモリ上にあるユーザ VM のメモリを特定して，ユーザ VM のメモリ上にあるデータへのアクセスを行う．

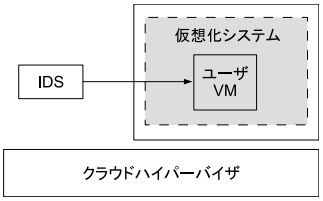
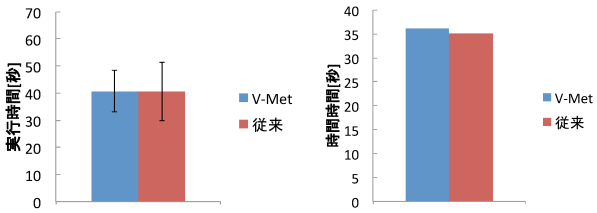


図 1: V-Met のシステム構成

データを特定するために，ユーザ VM のページテーブルと EPT の二つの変換表を用いてアドレス変換を行う．また，ユーザ VM が送受信したネットワークパケットはクラウド VM の境界とユーザ VM の境界の二箇所で取得する．ユーザ VM のディスクについては，ネットワーク共有またはクラウド VM の仮想ディスクの解析を通して IDS からアクセスする．

3　実験

V-Met におけるユーザ VM の監視性能を調べるために，オフロードした chkrootkit と Tripwire の実行時間を測定した．比較のために，従来の IDS オフロードを行った際の実行時間も測定した．実験結果は図 2 のようになった．chkrootkit の実行時間は V-Met と同程度となり，Tripwire の実行時間は約 2.7%増加した．



(a) chkrootkit　　(b) Tripwire

図 2: オフロードした IDS の実行時間

4　まとめ

本研究では，ネストした仮想化を用いて IDS を仮想化システムの外側にオフロードするシステム V-Met を提案した．今後の課題は，ユーザ VM だけでなく，仮想化システム全体を監視できるようにすることである．