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	13675019	氏　名	重田　一樹
論文題目	クラウド内部からの攻撃を考慮した仮想マシンの安全なリモート監視機構		

1　はじめに

IaaS 型クラウドにおいてユーザの仮想マシン（ユーザ VM）への攻撃を安全に検知するために，侵入検知システム（IDS）のオフロードが提案されている．この手法は IDS を同一ホスト上の別の VM（管理 VM）上で動作させることを可能にする．これにより，IDS が攻撃を検知する前に攻撃者によって無力化される事態を防ぐことができる．しかし，信頼できるとは限らないクラウド内では IDS オフロードの安全性を保証するのは難しい．クラウドの内部攻撃者によって管理 VM 上の IDS を無効化される恐れがあるためである．

本研究では，IDS をクラウド外部の信頼できるホストにオフロードする *IDS* **リモートオフロード**を提案する．

2　IDS リモートオフロード

IDS リモートオフロードは，IDS を監視ホストと呼ばれるクラウド外部の信頼できるホスト上で動作させる．そして，クラウド内部の仮想マシンモニタ（VMM）にアクセスすることで安全にユーザ VM の監視を行う．VMM はリモートアテステーションを用いることで信頼する．IDS リモートオフロードを実現するシステムである RemoteTrans の構成は図 1 のようになる．

IDS が監視するユーザ VM のメモリ情報は，監視ホストが管理 VM を経由して VMM にアクセスすることで取得する．この際に，管理 VM でリクエストおよびレスポンスが改ざんされていないことを保証するために整合性チェックを行う．VMM がリクエストとレスポンスに対するメッセージ認証コード (MAC) を計算し，監視ホストでそれを検証する．また，管理 VM での盗聴を防ぐために，VMM 内でメモリ情報を暗号化し，監視ホストで復号する．

ユーザ VM は VMM を経由してパケットを送受信するため，すべてのパケットを VMM 内に保存しておき，管理 VM が VMM から取得したパケットを監視ホストに送る．管理 VM におけるパケットの改ざんを検出するために，VMM でパケットに対して MAC を計算し，監視ホストで整合性を検証する．監視ホストは IDS がパケットをキャプチャできるように，tap デバイスにパケットを書き込む．

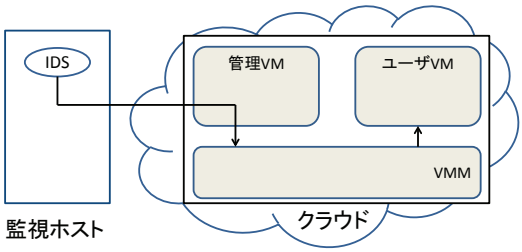

図 1: RemoteTrans におけるユーザ VM の監視

ユーザ VM のディスクは管理 VM 上にあるため，ネットワーク・ブロックデバイス（NBD）を用いて監視ホストにマウントする．管理 VM によるディスクの改ざんを防ぐために，ディスクはユーザ VM 内の OS レベルで暗号化しておき，監視ホストで復号する．

既存の IDS を監視ホスト上にオフロードできるようにするために，VM Shadow [1] を RemoteTrans 上に移植した．VM Shadow では，ユーザ VM 内で提供されている proc ファイルシステムを Shadow proc ファイルシステムとして提供する．Shadow proc ファイルシステムは OS 内部の情報を提供するために，ユーザ VM のメモリから直接情報を取得する．

3　実験

Shadow proc ファイルシステムの構築にかかる時間を従来システムと RemoteTrans とで比較した．その結果，RemoteTrans では，従来システムの 3.5 倍程度の時間がかかることがわかった．通信がボトルネックとなっており，Shadow proc ファイルシステムを構築するためのデータ送受信は 3,392 回行われていた．

4　まとめ

本研究では，IDS をクラウド外部の信頼できるホストにオフロードする IDS リモートオフロードを提案した．この手法により，IDS は安全にクラウド内の VM を監視することができる．今後の課題は，IDS リモートオフロードのオーバヘッド削減である．

参考文献

[1] 飯田貴大, 光来健一. VM Shadow : 既存 IDS をオフロードするための実行環境. 第 119 回 OS 研究会, 2011.