平成 26 年度　卒業論文概要			
所　　属	機械情報工学科	指導教員	光来 健一
学生番号	11237068	学生氏名	美山 翔平
論文題目	クラウドにおけるネストした仮想化を用いた安全な監視機構		

1　はじめに

近年，急速に普及している IaaS 型クラウドはネットワークを介して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．その一方で，クラウド内の VM は十分に管理されているとは限らず，外部から侵入されて機密情報が漏洩する危険がある．そのため，侵入検知システム（IDS）を用いて VM を監視することが重要となっている．VM 内で IDS を動作させると侵入時に無効化されてしまう危険があるため，IDS を安全に実行するために IDS オフロードと呼ばれる手法が提案されている．この手法は IDS を別の VM 上で動作させ，監視対象 VM の外から監視を行うことを可能にする．これにより IDS が攻撃を検知する前に攻撃者によって無効化されることを防ぐことができる．しかし，クラウドは十分に信頼できるとは限らないため，クラウド内で IDS オフロードを行っても，IDS が正しく動作していることを保証できない．これまで，VM の下で動作するハイパーバイザを信頼する手法が提案されてきたが，クラウドの一般の管理者が仮想化システムの一部しか管理できなくなるという問題があった．

本研究では，仮想化システムの外側で IDS を動作させ，安全に VM を監視するシステム *V-Met* を提案する．

2　クラウドにおける IDS オフロード

IDS オフロードは図 1 のように IDS を管理 VM で動作させ，監視対象 VM の外から監視する手法である．監視対象 VM に攻撃者が侵入したとしてもそこでは IDS が動作していないため，IDS を攻撃されて無効化される危険性がない．また，管理 VM では IDS 以外のサービスを動作させないようにすることで，攻撃を受けにくくすることができる．オフロードされた IDS は外から監視対象 VM を監視するために，監視対象 VM のメモリを解析し，情報を取得する．それにより，監視対象 VM 内のプロセスやネットワークなどの監視を行い，攻撃を検知することが可能である．

しかし，IaaS 型クラウド上の管理 VM を用いて IDS オフロードを行うとセキュリティ上の問題が生じる．IaaS 型クラウドにおいては管理 VM を用いて業務を行っているクラウドの管理者全員が必ずしも信頼できるとは限らない．そのため，管理 VM にオフロードした IDS が無効化されてしまう危険性がある．その上，ユーザは IDS が正しく動作していることを確かめることも難しい．

従来，VM の下で動作するハイパーバイザを信頼してクラウドにおいて安全に IDS オフロードを行う手法が提案されてきた．例えば，信頼できるハイパーバイザ内で IDS を動かす手法や，クラウドの外で IDS を動作させ，ハイパーバイザ経由で監視を行う手法などが挙げられる．しかし，ハイパーバイザはクラウドの信頼できる一部の管理者のみが管理することになるため，一般の管理者は管理できなくなるという問題があった．

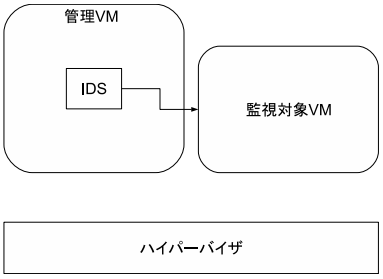

図 1　IDS オフロード

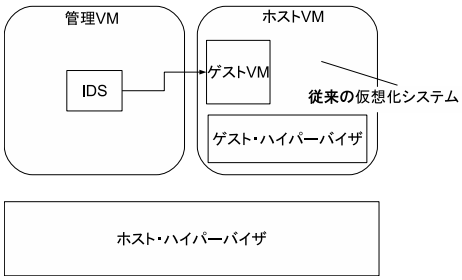

図 2　V-Met のシステム構成

3　V-Met

本研究では図 2 のように，**ネストした仮想化**を用いて仮想化システムの外側で IDS を動作させ，安全に VM を監視するシステム V-Met を提案する．ネストした仮想化は，従来の仮想化システム全体を VM 内で動作させることを可能にする技術である．本研究では，従来の仮想化システムにおける VM とハイパーバイザをそれぞれゲスト VM，ゲスト・ハイパーバイザと呼び，仮想化システムを動作させる VM とハイパーバイザをそれぞれホスト VM，ホスト・ハイパーバイザと呼ぶ．

V-Met では，仮想化システムの外側にあるホスト管理 VM 上の IDS からゲスト VM を監視するため，クラウドの一般の管理者は IDS を攻撃することができない．一方で，クラウドの一般の管理者にホスト VM 内の仮想化システム全体の管理権限を与えることができるため，従来通りの管理を行うことが可能となる．

3.1　ゲスト VM のメモリ監視

V-Met はホスト管理 VM からゲスト VM のメモリ上のデータにアクセスするために，図 3 のように 2 回のアドレス変換を行う．まず，監視対象データの仮想アドレスをゲスト VM 内

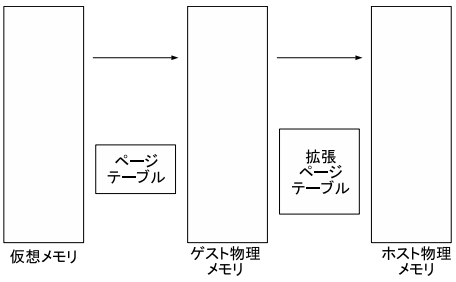

図 3　V-Met におけるアドレス変換の流れ

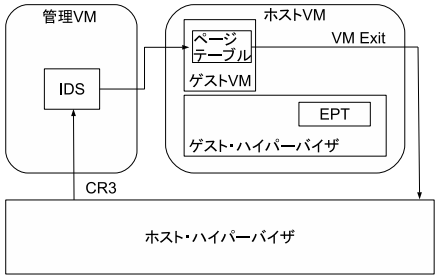

図 4　ページテーブルのアドレス取得

の物理アドレス (ゲスト物理アドレス) に変換する．仮想アドレスはコンパイル時に決まる論理的なアドレスであり，ゲスト物理アドレスはゲスト VM に割り当てられたメモリ上のアドレスである．この変換はゲスト VM 内のページテーブルを用いて行われる．次に，ゲスト物理アドレスをホスト VM における物理アドレス (ホスト物理アドレス) に変換する．この変換はゲスト・ハイパーバイザ内の拡張ページテーブル（EPT）を用いて行われる．

3.2　ゲスト VM のページテーブルの参照

ゲスト VM 内のページテーブルのアドレスは，ゲスト VM の仮想 CPU の CR3 レジスタに格納されている．信頼できないゲスト・ハイパーバイザに依存せずに CR3 レジスタの値を取得するために，V-Met は図 4 のように，ゲスト VM が CR3 の値を変更する時に VM Exit を発生させて，ホスト・ハイパーバイザに直接，制御を移す．ホスト・ハイパーバイザでは CR3 レジスタに書き込もうとしている値を取得し，その値を保存しておく．そして，IDS がホスト・ハイパーバイザを呼び出した時に CR3 レジスタの値を返す．

3.3　ゲスト VM の拡張ページテーブルの参照

ゲスト・ハイパーバイザ内にある拡張ページテーブルのアドレスは，ゲスト VM の仮想 CPU の VMCS 領域に格納されている．V-Met は，ゲスト VM が VM Exit を起こしてホスト・ハイパーバイザに制御を移した時に，VMCS 領域のホスト物理アドレスを保存しておく．そして，IDS がホスト・ハイパーバイザを呼び出した時に，保存しておいた VMCS 領域から拡張ページテーブルの先頭アドレスを取得する．信頼できないゲスト・ハイパーバイザ内の VMCS 領域や拡張ページテーブルへの改ざんは CloudVisor [1] の技術を用いることで検出することができる．

3.4　VM Shadow の移植

V-Met では既存の IDS に修正を加えることなく動作を可能にする VM Shadow を V-Met に移植した．VM Shadow はゲスト VM 内のプロセスやネットワークの情報を Shadow proc ファイルシステムとして IDS に提供する．VM Shadow で行われるアドレス変換を V-Met における 2 段階のアドレス変換で置き換えた．

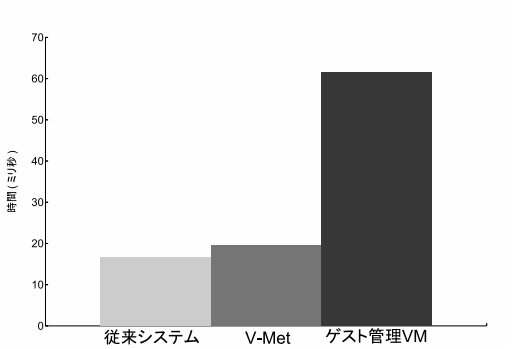

図 5　プロセス情報取得時間

4　実験

ゲスト VM 内のプロセス情報を取得する IDS をホスト管理 VM で実行し，取得時間を測定した．比較のために，従来手法を用いてゲスト管理 VM からゲスト VM 内のプロセス情報を取得した場合と，ネストした仮想化を用いない従来システムにおいて VM 内のプロセス情報を取得した場合の取得時間も測定した．実験には，Intel Xeon E3-1270v3 の CPU，16GB のメモリを搭載した PC を使用し，ホスト VM には 6 GB のメモリを割り当て，ゲスト VM には 2GB のメモリを割り当てた．仮想化ソフトウェアには Xen 4.4 を用い，ホスト管理 VM，ゲスト管理 VM の OS には Linux 3.13.0，ゲスト VM の OS には Linux 2.6.27 を用いた．

89 個のプロセス情報を取得するのにかかる時間を 10 回計測した．平均値を図 5 に示す．V-Met における取得時間は従来システムにおける取得時間より 16% 速いことがわかった．これは拡張ページテーブルを参照する必要があるためと考えられる．一方，V-Met における取得時間はゲスト管理 VM における取得時間の 3 倍速かった．これは，ゲスト管理 VM にはネストした仮想化によるオーバーヘッドがあるためと考えられる．

5　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で動作させるようにすることで，安全に VM のメモリ監視を可能にするシステム V-Met を提案した．V-Met では，クラウドの一般の管理者が従来の仮想化システム全体を管理することができる．今後の課題は，ホスト管理 VM からゲスト VM のディスクやネットワークの監視も行えるようにすることである．

参考文献

[1] F. Zhang, J. Chen, H. Chen, and B. Zang. CloudVisor: Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization. In Proc. SOSP'11, 2011.