平成 30 年度 卒業論文概要			
所　　属	機械情報工学科	指導教員	光來 健一
学生番号	15237058	学生氏名	平川　禎
論文題目	信頼できないクラウドにおける仮想化システムの監視		

1　はじめに

近年，仮想化システムを用いた IaaS 型クラウドが広く使われるようになっている．IaaS 型クラウドでは，インターネットを通してユーザに仮想マシン (VM) を提供し，ユーザは自由に VM をカスタマイズして利用することができる．クラウド内のユーザの VM (ユーザ VM) は外部からの攻撃を受ける危険があるため，侵入検知システム (IDS) を用いて VM の監視を行う必要がある．その際に，監視対象のユーザ VM 内で IDS を実行すると攻撃者の侵入時に IDS を無効化され，侵入を検知できなくなる恐れがある．そこで，ユーザ VM の外側にある管理 VM で IDS を実行する IDS オフロードと呼ばれる手法が用いられている．これにより，攻撃者はユーザ VM に侵入しても IDS を無効化できず，オフロードされた IDS が安全にユーザ VM の監視を続けることができる．

しかし，クラウド内に悪意のある管理者がいた場合，管理 VM にオフロードした IDS を無効化され，ユーザ VM に不正アクセスされる可能性がある．そこで，VM の下で動作しているハイパーバイザから監視を行う手法も提案されているが，悪意のある管理者はハイパーバイザにも攻撃を行う可能性がある．これまでに，ハードウェアを用いてハイパーバイザを監視する手法が提案されてきたが，監視性能やコスト面での問題があった．

本研究では，ネストした仮想化と呼ばれる技術を用いることで，ハイパーバイザや管理 VM からなる仮想化システムを安全に監視するシステム VS-monitor を提案する．

2　VM の監視

クラウドにおけるユーザ VM は必ずしも適切な管理がされているとは限らず，クラウド外部から不正アクセスなどの攻撃を受ける可能性がある．これらの攻撃を検知するために IDS を用いてユーザ VM 内のシステムやディスク，ネットワークなどの監視を行う必要がある．しかし，ユーザ VM 上で IDS を動作させると，攻撃者の侵入時に IDS を無効化され，ユーザ VM の監視を行えなくなってしまう．そこで，図 1 のようにユーザ VM の外側にある管理 VM と呼ばれる特殊な VM で IDS を動作させ，ユーザ VM の監視を行う IDS オフロードと呼ばれる手法が提案されている．この手法を用いるとユーザ VM に侵入されたとしても，その中では IDS は動作していないため IDS を無効化されることはなく，安全に監視を続けることができる．

管理 VM はクラウドの管理者によって管理されているが，クラウド内に悪意のある管理者がいた場合，管理 VM にオフロードした IDS が容易に無効化される可能性がある．さらに，管理 VM はユーザ VM にアクセスする権限を持っているため，ユーザ VM のメモリやディスクの情報の盗聴や改ざんを行われたり，強制的に VM の起動・終了を行われたりすることも考えられる．そこで，管理 VM の下で動作する基盤ソフトウェアであるハイパーバイザから管理 VM を安全に監視する手法も提案されている．

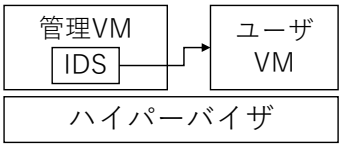


図 1　IDS オフロード

しかし，悪意のあるクラウドの管理者は管理 VM だけでなくハイパーバイザにも攻撃を行うことが考えられる．ハイパーバイザが攻撃を受けると，管理 VM の監視機能を無効化される恐れがある．また，ハイパーバイザはすべての VM を制御しており，管理 VM 以上の権限を持っているため，VM 内の情報の盗聴や改ざんだけでなく，仮想 CPU やネットワーク帯域の割り当てなどを変更される恐れもある．これまでに，CPU のシステム監視モードや専用 PCI カードを用いてハイパーバイザや管理 VM を監視するシステムが提案されてきたが，監視性能や導入コストの点で問題があった．

3　VS-monitor

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監視システムを動作させ，安全にハイパーバイザと管理 VM を監視するシステム VS-monitor を提案する．ネストした仮想化はハイパーバイザと管理 VM からなる従来の仮想化システム全体を仮想化して，クラウド VM と呼ばれる VM 内で動作させる技術である．VS-monitor では監視システムをクラウド VM の外側で動作させ，信頼できない管理者の権限はクラウド VM 内に制限する．信頼できない管理者はクラウド VM の外側の監視システムを無効化することができないため，ハイパーバイザと管理 VM を安全に監視することができる．

3.1　VM のメモリ監視

VS-monitor では，VM 内で動作しているハイパーバイザや OS のデータを VM の外側から取得するために，VM のメモ

図 2　VS-monitor のシステム構成

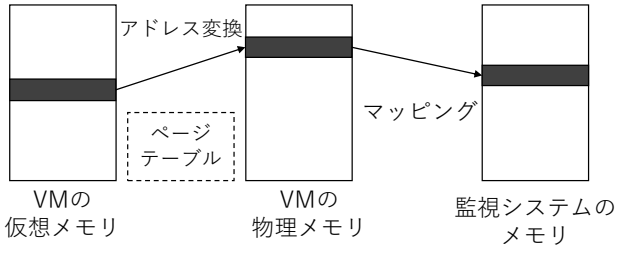
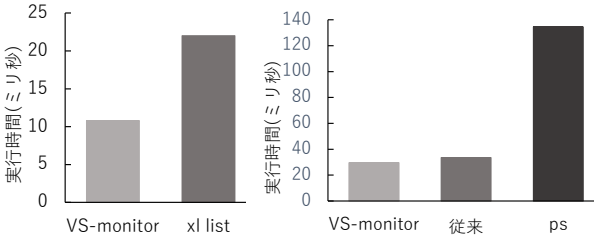


図 3　メモリ監視の手順



(a) リソース割り当て情報の取得時間　　(b) プロセス一覧の取得時間

図 4　実験結果

リの解析を行う．そのために，図 3 のような手順でアドレス変換を行い，VM 内のデータにアクセスする．まず，監視するデータの仮想アドレスを特定し，そのアドレスを VM 内で使われている物理アドレスに変換する．このアドレス変換には VM 内のハイパーバイザや OS が管理しているアドレス変換表であるページテーブルを使用する．次に，変換した物理アドレスを指定して VM のメモリの一部を監視システムのメモリにマッピングすることで，監視システムからのアクセスを可能にする．

3.2　ハイパーバイザの監視

クラウド VM 内で動作するハイパーバイザの監視を行うために，VS-monitor はハイパーバイザのページテーブル特定する．このページテーブルのアドレスはクラウド VM の仮想 CPU の CR3 レジスタから取得することができる．クラウド VM 内ではハイパーバイザ以外のページテーブルも使われるため，ハイパーバイザの起動時に CR3 レジスタの値を記録する．ただし，CR3 レジスタには多くのページテーブルが設定され，それらのすべてが常に有効というわけではない．そこで，いくつかの値を記録しておき，メモリ監視時に有効なページテーブルを用いる．

VS-monitor の監視システムは特定したページテーブルを用いてハイパーバイザのデータにアクセスする．監視システムの開発を容易にするために，LLView[1] をハイパーバイザの監視に適用した．LLView は管理 VM にオフロードした IDS にアドレス変換を行うコードを自動挿入するツールであり，監視システムの開発者が煩雑なアドレス変換を行う必要がなくなる．LLView を用いることで，VS-monitor ではハイパーバイザのシンボルテーブルとヘッダファイルを利用して監視システムを開発することができる．

3.3　管理 VM の監視

クラウド VM 内で動作する管理 VM の監視を行うために，VS-monitor は管理 VM のページテーブルを特定する．このページテーブルのアドレスはハイパーバイザの中に格納されているため，ハイパーバイザのメモリを解析することによって取得する．まず，VS-monitor はハイパーバイザのページテーブルを用いてハイパーバイザ内の VM リストにアクセスし，管理 VM を見つける．次に，管理 VM の仮想 CPU のデータの中からページテーブルのアドレスを取得する．VS-monitor はこのページテーブルを用いて管理 VM 内のデータのアドレス変換を自動化するために，管理 VM 用の LLView を提供する．この LLView の中で管理 VM のページテーブルを取得するプログラムについてはハイパーバイザ用の LLView を用いて開発した．

4　実験

VS-monitor を用いた監視性能を調べるための実験を行った．実験には Intel Core i7 7700 の CPU，8GB のメモリを搭載したマシンを使用した．クラウド VM には 2GB，その中の管理 VM には 1490MB のメモリを割り当てた．仮想化ソフトウェアには Xen 4.10.1，管理 VM の OS には Linux 4.4 を用いた．

まず，VM のリソース割り当て情報を取得する時間を測定した．比較として管理 VM で xl list コマンドを実行してリソース割り当て情報を取得した場合の実行時間も測定した．情報を取得するのにかかる時間をそれぞれ 10 回測定した時の平均を図 4(a) に示す．VS-monitor におけるリソース割り当て情報の取得時間は管理 VM で xl list コマンドを実行する時間の 49% であった．これは管理 VM ではネストした仮想化のオーバーヘッドが大きいためと考えられる．

次に，管理 VM のプロセス一覧を取得する時間を測定した．比較として，管理 VM で ps コマンドを実行してプロセス一覧を取得した場合と，ネストした仮想化を用いずに従来手法でユーザ VM のプロセス一覧を取得した場合の実行時間も測定した．プロセス一覧を取得するのにかかる時間をそれぞれ 10 回測定した時の平均を図 4(b) に示す．VS-monitor におけるプロセス一覧の取得時間は管理 VM で ps コマンドを実行する時間の 22% であった．これも管理 VM を仮想化したことによるオーバーヘッドが原因と考えられる．一方，VS-monitor は従来手法と比べて 12% 高速であったが，大きな差はなかった．

5　まとめ

本研究では，ネストした仮想化を用いて仮想化システムの外側で監視システムを動作させ，ハイパーバイザと管理 VM を安全に監視するシステム VS-monitor を提案した．VS-monitor では信頼できない管理者の権限をクラウド VM 内に制限することで，監視システムへの攻撃を防ぎ安全に仮想化システムを監視することができる．今後の課題は，ハイパーバイザの常に有効なページテーブルを 1 回で取得できるようにすることである．また，ハイパーバイザや管理 VM への実際の攻撃を検知できるようにする必要がある．

参考文献

[1] 植木あずさ．LLVM の中間表現を用いた IDS オフロードの開発支援．九州工業大学卒業論文，2015.