平成 28 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	13237010	学生氏名	鵜木 智矢
論文題目	クラウドにおける安全なリモート管理に対応した VM マイグレーション		

1　はじめに

近年，ネットワーク経由でユーザに仮想マシン（VM）を提供するサービスである IaaS 型クラウドが広く普及している．ユーザが VM を管理するために，クラウドは帯域外リモート管理と呼ばれる管理手法を提供している．帯域外リモート管理は，仮想キーボードなどの仮想デバイスを用いて VM にアクセスする管理手法である．帯域外リモート管理の問題点は，クラウドの管理者によって仮想デバイスからユーザの入出力が容易に盗聴されることである．そこで，仮想デバイスからの情報漏洩を防ぐためのシステムである VSBypass[1] が提案されている．VSBypass は仮想化システムの外側で動作する仮想デバイス（シャドウデバイス）を用いて VM に安全にアクセスすることを可能にしている．しかし，マイグレーションにより VM を他のホストに移動させると，シャドウデバイスを用いた帯域外リモート管理が行えなくなるという問題があった．

本研究では，VM のマイグレーション時にシャドウデバイスの状態も転送することで，マイグレーション後にシャドウデバイスを用いた帯域外リモート管理を可能にするシステム USShadow を提案する．

2　安全な帯域外リモート管理

帯域外リモート管理は，仮想化システムが VM に提供している仮想キーボードや仮想ビデオカードなどの仮想デバイスを用いて VM にアクセスする管理手法である．ネットワーク経由で VM にアクセスする管理手法と比べて，VM 内のネットワークに設定ミスがあっても管理が行えるなどの利点がある．その一方で，クラウドの管理者であればユーザが VM に対して行った入出力を仮想デバイスから容易に盗聴することができる．クラウドの管理者は必ずしも信頼できるとは限らないため，悪意のある管理者にパスワードなどの機密情報を盗まれる恐れがある．

そこで，仮想デバイスからの情報漏洩を防ぐためのシステムである VSBypass が提案されている．VSBypass は，図 1 のように仮想化システムの外側で動作する仮想デバイス（シャドウデバイス）を用いて安全な帯域外リモート管理を実現する．VSBypass で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全体を VM 内で動作させることにより，シャドウデバイスの安全な実行を可能にしている．仮想化システム内の仮想デバイスを経由することなく帯域外リモート管理を行えるため，クラウドの管理者への情報漏洩を防ぐことができる．

しかし，VSBypass では VM のマイグレーションを行うと，シャドウデバイスを用いた帯域外リモート管理が行えなくなるという問題があった．VM マイグレーションとは VM を異

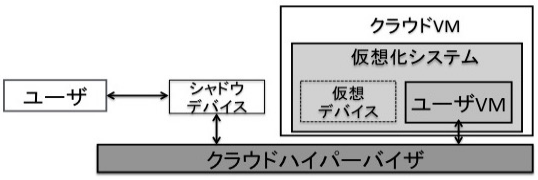

図 1　VSBypass

なるホストに移動させる技術であり，負荷分散を行う際やホストをメンテナンスする際に用いられる．VM マイグレーションでは仮想 CPU やメモリ，仮想デバイスの状態を転送する必要があるが，シャドウデバイスの状態を転送することはできなかった．これは，シャドウデバイスが仮想化システムの外側にあり，通常の仮想デバイスのように状態を保存したり復元したりすることができないためである．シャドウデバイスの状態が失われると，VM やユーザから正常にアクセスすることができなくなる．

3　USShadow

本研究では，VM マイグレーションの際にシャドウデバイスの状態も転送することで，マイグレーション後にシャドウデバイスを用いた帯域外リモート管理を可能にするシステム USShadow を提案する．USShadow のシステム構成は図 2 のようになる．従来の仮想化システムを動作させる VM をクラウド VM と呼び，その下で動作する基盤ソフトウェアをクラウドハイパーバイザと呼ぶ．クラウド VM 内におけるマイグレーション対象の VM をユーザ VM と呼び，マイグレーションを行う移送ツールが仮想化システム内で動作する．USShadow では，仮想化システム全体を仮想化するため様々な仮想化システムに対応できる．

3.1　VM マイグレーションの拡張

USShadow は，VM マイグレーションを以下のように拡張する．マイグレーション元の移送ツールはシャドウデバイスと通信することにより，その状態を取得する．この際に，シャドウデバイスで暗号化された状態を取得することにより，仮想化システム内の管理者への情報漏洩を防ぐ．移送ツールは暗

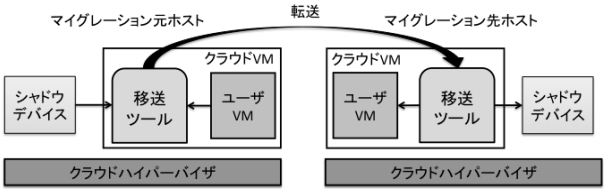

図 2　USShadow における VM マイグレーション

号化されたシャドウデバイスの状態をマイグレーション先に送り，シャドウデバイスを停止する．マイグレーション先の移送ツールはマイグレーション元から暗号化されたシャドウデバイスの状態を受信すると，新たに起動したシャドウデバイスと通信を行うことによりその状態を送る．シャドウデバイスでは受け取った状態を復号し，状態の復元を行う．

3.2 シャドウデバイスとの通信

従来，仮想デバイスの状態を保存・復元するために，移送ツールと仮想デバイスの間で OS を介したプロセス間通信が用いられていた．USShadow ではシャドウデバイスがクラウド VM の外側にあるため，シャドウデバイスとプロセス間通信を行うことはできない．ネットワークを経由して通信するという方法が考えられるが，ネットワーク通信はオーバヘッドが大きい．また，シャドウデバイスに対してネットワーク経由でのアクセスを許可することになるため，仮想化システム内の管理者や外部の攻撃者からの攻撃を受けるリスクが高くなる．

そこで，USShadow では図 3 のように，クラウドハイパーバイザを経由してシャドウデバイスとの通信を行う．仮想化システムへの改変を避けるために，ウルトラコールと呼ばれる機構を開発して仮想化システムを経由せずにクラウドハイパーバイザにアクセスできるようにした．ウルトラコールは CPU の機能を利用することでクラウドハイパーバイザに直接制御を移す．既存の仮想デバイスとの通信と異なり，シャドウデバイスは移送ツールのメモリ上のバッファに直接アクセスすることにより 4KB のデータを扱うことができる．これを可能にするために，クラウドハイパーバイザは移送ツール内のページテーブルを参照して，バッファの仮想アドレスを物理アドレスに変換する．そして，シャドウデバイスにイベントを送り，この物理アドレスを通知するとともに制御を移す．

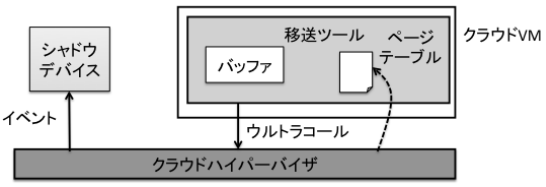

図 3　シャドウデバイスとの通信

3.3 シャドウデバイスの状態の保存・復元

シャドウデバイスの状態を保存する場合，シャドウデバイスは図 4 のように状態を暗号化して，移送ツールのバッファに書き込む．シャドウデバイスの状態はレジスタの値などで構成される．シャドウデバイスは移送ツールのバッファに直接アクセスすることはできないため，通知された物理アドレスに対してメモリマップを行ってからアクセスする．一方，シャドウデバイスの状態を復元する場合，渡されたバッファ内のデータを復号し，シャドウデバイスのレジスタなどに書き込む．

4 実験

USShadow における VM のマイグレーション性能を計測し，マイグレーション後の帯域外リモート管理の動作確認を行った．シャドウデバイスとしては仮想シリアルデバイスを用いた．比較対象として，従来の仮想化システムと従来のネストした仮想化システムを用いた．実験環境には，Intel Xeon

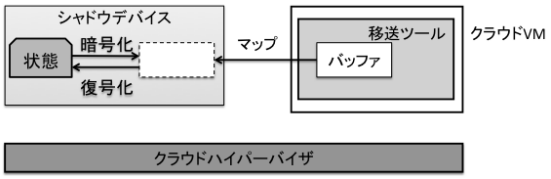

図 4　シャドウデバイスの保存・復元

E3-1226v3 の CPU，8GB のメモリを搭載したマシンを 2 台用い，ギガビットイーサネットで接続した．仮想化システムには Xen 4.4 を用い，ホスト VM には 3GB，その中のユーザ VM には 256MB のメモリを割り当てた．

図 5 に VM マイグレーションにかかった時間，図 6 にダウンタイムを示す．USShadow では従来のネストした仮想化システムに比べ，3 秒程度マイグレーション時間が増加した．また，ダウンタイムは従来のネストした仮想化システムより 0.3 秒長かった．これは，シャドウデバイスの状態を扱うのにかかる時間によるものと考えられる．シャドウデバイスの状態の保存・復元にかかる時間を計測したところ，保存に 4.4 ミリ秒，復元に 4.3 ミリ秒かかることが分かった．一方，従来の仮想化システムと比べると，マイグレーション時間，ダウンタイムともに大幅に性能が低下していることが分かる．これはネストした仮想化のオーバヘッドのためであるが，このオーバーヘッドを削減するために様々な研究が行われている．VM マイグレーション後にシャドウデバイスに接続して帯域外リモート管理を行ったところ，VM マイグレーション前の状態から正常に再開できることが確認できた．

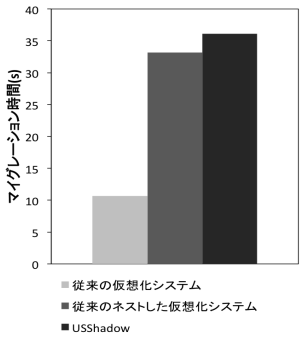

図 5　マイグレーション時間

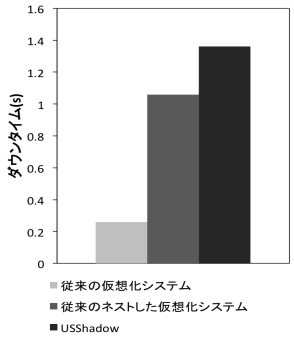

図 6　ダウンタイム

5 まとめ

本研究では，VM マイグレーションの際にシャドウデバイスの状態も転送することで，マイグレーション後にシャドウデバイスを用いた帯域外リモート管理を可能にするシステム USShadow を提案した．USShadow では，仮想化システムの外側で動作するシャドウデバイスの状態を安全に転送することができる．今後の課題は，USShadow を KVM など様々な仮想化システムに対応させていくことである．

参考文献

[1] 二神翔太，光來健一．VSBypass : ネストした仮想化を用いた VM の安全な帯域外リモート管理．SWoPP2016.