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	17675006	氏　名	鵜木　智矢
論文題目	強制パススルーを用いた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

IaaS 型クラウドでは，ユーザは帯域外リモート管理と呼ばれる管理手法を用いて仮想マシン (VM) の管理を行う．帯域外リモート管理では，VM の仮想デバイス（仮想ビデオカード等）から悪意あるクラウド管理者によって機密情報が盗まれてしまう危険性がある．そこで，仮想デバイスからの情報漏洩を防ぐために VSBypass [1] が提案されている．VSBypass は，仮想デバイスを仮想化システムの外側で動作させて強制パススルーを行うことにより安全な帯域外リモート管理を実現する．この仮想デバイスは**シャドウデバイス**と呼ばれる．しかし，VSBypass では VM をマイグレーションする際にシャドウデバイスの状態を転送することができないため，マイグレーション後には帯域外リモート管理を行うことができなくなる．

本研究では，マイグレーション後も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　USShadow

USShadow は VM をマイグレーションする際に，仮想化システムの外側にあるシャドウデバイスの状態も転送する．USShadow では，図 1 のようにマイグレーションの際に，移送元ホストの移送マネージャがシャドウデバイスの状態を取得し，その状態を移送先ホストの移送マネージャに送信する．一方，移送先ホストの移送マネージャは受信した状態を新しく作成したシャドウデバイスへ送り，シャドウデバイスの状態を復元する．シャドウデバイスの状態の保存・復元を仮想デバイスと同じインタフェースを持つ疑似デバイス経由で行わせることにより，移送マネージャへの改変を行わずに済ませる．

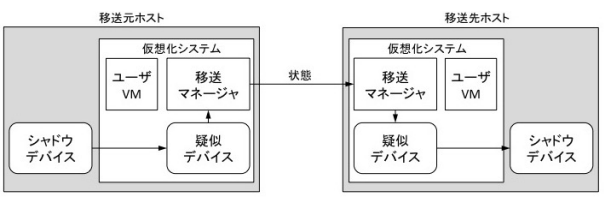

図 1: USShadow における VM マイグレーション

疑似デバイスとシャドウデバイス間での通信を可能にするために，USShadow は共有メモリを用いる．従来，仮想化システムの内外でデータをやりとりするには，ネットワーク通信を用いる必要があった．USShadow では，仮想化システムをバイパスして，直接シャドウデバイスとの間で共有メモリを確立することで，既存の仮想化システムを改変せずに利用できる．

シャドウデバイスの状態は保存・復元の際に，シャドウデバイス自身が暗号化・復号化を行う．シャドウデバイスの状態にはユーザの入力や VM からの出力などの機密情報が含まれる可能性があるためである．仮想化システムの外側で動作するシャドウデバイスで暗号化・復号化を行うことで，仮想化システム内のクラウド管理者への情報漏洩を防ぐことができる．

3　実験

USShadow の動作および性能を確認するための実験を行った．USShadow で動作する仮想化システムとして，Xen 4.4.0 と KVM 2.4.1 を用いた．まず，USShadow と先行研究の VSBypass を用いて VM マイグレーションを行い，USShadow を用いた場合にだけ，マイグレーション後も帯域外リモート管理が行えることを確認した．次に，帯域外リモート管理中のマイグレーション性能を測定した．VSBypass に比べ，USShadow では 1GB のメモリをもつ VM のマイグレーションにかかる時間が，Xen を用いた場合に 0.7 秒，KVM を用いた場合に 0.02 秒増加した．これは，シャドウデバイスの状態を扱うためのオーバヘッドである．

4　まとめ

本研究では，VM 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．今後の課題は，シャドウデバイスの状態の暗号化に用いる鍵をホスト間で安全に共有できるようにすることである．

参考文献

[1] S. Futagami, T. Unoki, and K. Kourai: VSBypass: Secure Out-of-band Remote Management of Virtual Machines with Transparent Passthrough, ACSAC 2018.