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	16675034	氏　名	二神 翔太
論文題目	強制パススルー機構を用いた安全な帯域外リモート管理		

1　はじめに

近年，ユーザに仮想マシン（VM）を提供する IaaS 型クラウドの利用が増えている．Iaa 型クラウドでは，ユーザが VM を管理できるようにするために，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．この管理手法では，ユーザが VM の仮想デバイスに直接アクセスするため，VM 内の設定に依存せずにリモート管理を行うことができる．しかし，VM の仮想デバイスを管理してい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．悪意のある管理者がいた場合，VM の仮想デバイスから帯域外リモート管理の入出力を容易に盗聴することができる．従来，仮想化システムの一部を信頼してこのような情報漏洩を防ぐ手法が提案されてきたが，管理者が比較的容易に信頼する部分を攻撃できる，仮想化システム全体の管理を行えなくなる，といったいくつかの問題があった．

本研究では，仮想化システムの外側で安全に帯域外リモート管理を実現する *VSBypass* を提案する．

2　VSBypass

VSBypass は**強制パススルー**と呼ぶ手法を用いて安全な帯域外リモート管理を実現する．そのために，ネストした仮想化と呼ばれる技術を用いて，図 1 のように，従来の仮想化システム全体を VM 内で動作させる．VSBypass はユーザ VM による仮想デバイスへの入出力を横取りし，仮想化システム内にある仮想デバイスの代わりに，仮想化システムの外側で動作する**シャドウデバイス**を用いて入出力処理を行う．これにより，信頼できない仮想化システム内の仮想デバイスに依存せずに帯域外リモート管理を行うことができるため，入出力に含まれる機密情報がクラウドの管理者に漏洩するのを防ぐことができる．

VSBypass はシャドウデバイスで発生した仮想割り込みをユーザ VM に転送する．その際に，シャドウデバイスは仮想割り込みを仮想化システム経由でユーザ VM に送る．これは仮想割り込み機構が仮想化システム内にあり，ユーザ VM に直接，仮想割り込みを送ることが難しいためである．仮想割り込みには機密情報が含まれていないため，仮想化システムを経由しても情報が漏洩する恐れはない．

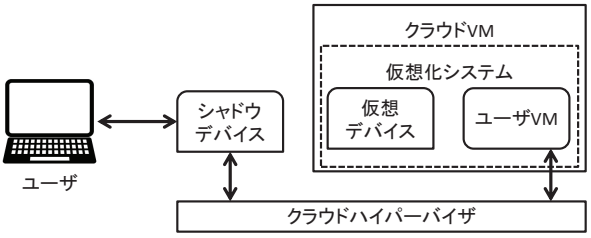

図 1: VSBypass のシステム構成

VSBypass では，帯域外リモート管理のための機構が仮想化システムの外側で動作するため，管理者による攻撃がより難しくなる．また，仮想化システム内に信頼する部分を設ける必要がないため，一般の管理者であっても仮想化システム全体を管理することができる．さらに，仮想化システムにほとんど依存しないため，異なる仮想化システムに対応するのが容易である．

3　実験

VSBypass の有効性を調べる実験を行った．実験には，Intel Xeon E3-1290v2 の CPU と 8GB のメモリを搭載したマシンを用いた．このマシンで VSBypass を動作させ，仮想化システムとして Xen 4.4 を動作させた．帯域外リモート管理として，SSH と VNC を用いた．

まず，仮想化システム内の仮想デバイスで盗聴を行い，VSBypass では盗聴できないことを確認した．次に，帯域外リモート管理における応答時間を測定した．SSH を用いた場合，VSBypass では従来システムより 1.3 ミリ秒増加して 3.0 ミリ秒になった．一方，VNC では応答時間のばらつきが大きく，グラフィックモードの場合は平均で 14.5 ミリ秒増加して 64.2 ミリ秒となり，テキストモードの場合は 1.8 ミリ秒増加して 9.2 ミリ秒となった．いずれにしても，リモート管理への影響はみられなかった．

4　まとめ

本研究では，強制パススルー機構を用いて，仮想化システムの外側で帯域外リモート管理を実現する VSBypass を提案した．今後の課題は，Xen 以外の仮想化システムにも適用できるようにすることである．