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	11675003	氏　名	江川　友寿
論文題目	IaaS クラウドにおけるセキュアな帯域外リモート管理		

1　はじめに

IaaS クラウドにおいて，ユーザは提供された VM（ユーザ VM）をリモートから管理する．ユーザ VM を管理する権限を持つ VM（管理 VM）を経由したリモート管理を行うことで，ユーザ VM の障害時でも管理が可能となる．この管理形態は帯域外リモート管理と呼ばれる．しかし，IaaS クラウドにおいては管理 VM が必ずしも信頼できるとは限らない．よって，帯域外リモート管理に伴うキーボード入力やビデオ出力は管理 VM 上の攻撃者によって容易に盗聴されてしまい，重大な情報漏洩につながる危険がある．

本研究では IaaS クラウドにおいても安全な帯域外リモート管理を可能にするシステム *FBCrypt* を提案する．

2　FBCrypt

FBCrypt は，**図 1** のように VNC クライアントと IaaS クラウド内の仮想マシンモニタ（VMM）でユーザ VM に対する入出力の暗号化・復号化を行うことで，管理 VM への情報漏洩を防ぐ．これにより，攻撃者が管理 VM を不正に改ざんして盗聴を試みたとしても，管理 VM を経由する入出力情報が漏洩することはない．また，この暗号化はユーザ VM には透過的に行われるため，ユーザ VM 内のシステムへの変更は不要である．

ユーザ VM へのキーボード入力は，入力時に VNC クライアントによって暗号化され，管理 VM 内の仮想キーボード経由でユーザ VM に渡される時に VMM によって復号化される．復号化を行う際に，VMM は攻撃者による入力の改ざんを検出するために，メッセージ認証コードを用いて整合性の検査を行う．また，リプレイ攻撃を防ぐためにストリーム暗号を用いて暗号化を行う．

ユーザ VM からのビデオ出力は，ユーザ VM による画面の更新時に VMM によって暗号化されてビデオメモリに書き込まれ，VNC クライアントによって復号化される．ビデオメモリの暗号化をユーザ VM に対して透過的に行うために，VMM は管理 VM 内の仮想ビデオカード用にビデオメモリを複製し，ユーザ VM 用のビデオメモリとの間で暗号化しながら同期をとる．

FBCrypt はリモートアテステーションを用いて，IaaS クラウド内で正しい VMM が動作していることを保証する．リモートアテステーションとは，耐タンパ性ハードウェア（TPM）によってプラットフォームの完全性を第三者機関で検証する仕組みである．

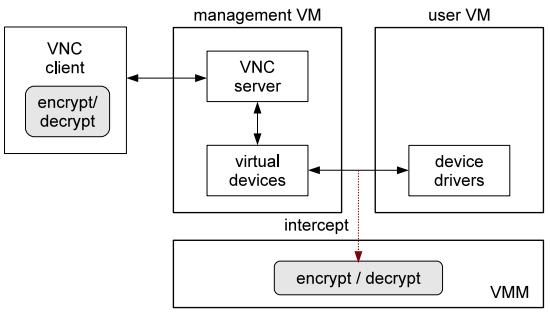

図 1: FBCrypt の構成

3　実験

FBCrypt の有効性を確認するために，管理 VM 上の VNC サーバ内でキーボード入力とビデオメモリを盗聴するプログラムを動作させた．その結果，ユーザ VM に対する入出力は暗号化されて記録されており，管理 VM に情報が漏洩していないことを確認した．

次に，FBCrypt と従来システムで，キーボード入力と画面更新におけるレスポンスタイムを比較した．FBCrypt の導入により，キーボード入力は従来より 0.77ms，画面更新（800 × 600）は 46ms の遅延が発生した．

また，画面更新（800 × 600）における VNC クライアントと IaaS クラウドのサーバの CPU 使用率を調査した．FBCrypt の導入により，VNC クライアントの CPU 使用率は従来より 6.6 %上昇して 12.3 %，IaaS クラウド側は従来より 32.8 %上昇して 53.2 %となった．

4　まとめ

本研究では，IaaS クラウドにおいて安全な帯域外リモート管理を可能にするシステム FBCrypt を提案した．FBCrypt は，VNC クライアントと VMM でユーザ VM に対する入出力の暗号化を行い，クラウドへの情報漏洩を防ぐ．今後の課題は，SSH など VNC 以外のリモート管理ソフトウェアに FBCrypt を対応させることである．