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	13675013	氏　名	梶原　達也
論文題目	クラウドにおける仮想シリアルコンソールを用いた 安全なリモート管理		

1　はじめに

IaaS クラウドでは，ユーザは提供された仮想マシン（ユーザ VM）をネットワーク経由でリモート管理する．ユーザ VM の障害などが原因で VM 内のリモート管理サーバにアクセスできない場合には，ユーザ VM をローカルに管理する権限を持った VM（管理 VM）を経由してユーザ VM の管理を行う．この管理手法は**帯域外リモート管理**と呼ばれる．しかし，管理 VM を管理している IaaS クラウドの管理者は必ずしも信用できるとは限らない．そのため，リモート管理で用いる仮想シリアルコンソールの入出力が管理 VM 上で盗聴されると，機密情報が漏洩する危険がある．

本研究では IaaS クラウドにおいて仮想シリアルコンソールを用いた安全な帯域外リモート管理を可能にするシステム *SCCrypt* を提案する．

2　SCCrypt

SCCrypt は，信頼できない管理 VM に対して入出力を暗号化した仮想シリアルコンソールを提供する．この仮想シリアルコンソールは図 1 のように管理 VM から暗号化されたコンソール入力を受け取り，それを復号してユーザ VM に送る．また，ユーザ VM からはコンソール出力を受け取り，それを暗号化して管理 VM に送る．この暗号化・復号化はクラウド内の信頼できる仮想マシンモニタ（VMM）で行う．

ユーザは，SCCrypt に対応した SSH などのリモート管理クライアントを用いて管理 VM にアクセスし，暗号化された仮想シリアルコンソールに接続することでユーザ VM の管理を行う．ユーザによるコンソール入力は，SSH クライアントにおいて暗号化され，管理 VM 上の SSH サーバに送信される．SSH サーバは暗号化された入力をそのまま仮想シリアルコンソールに送る．一方，仮想シリアルコンソールから受け取ったユーザ VM からのコンソール出力は，暗号化された状態で SSH サーバに送られる．そして，そのまま SSH クライアントに送信され，復号される．

我々は SCCrypt を準仮想化および完全仮想化の二種類の VM に対して実装した．仮想化対応 OS を動作させる準仮想化については，管理 VM 上の仮想シリアルデバイスから VMM を呼び出すことで入出力の暗号化・復号化を行うようにした．既存の OS を動作させる完全仮想化については，ユーザ VM による仮想シリアルデバイスへのアクセスを VMM がトラップし，入出力の暗号化・復号化を行うようにした．

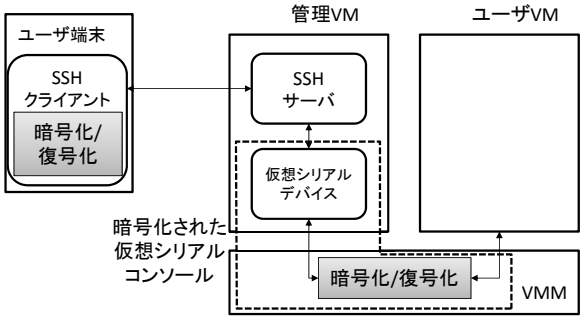

図 1: SCCrypt のシステム構成

3　実験

SCCrypt の安全性を確認するために，管理 VM 上の仮想シリアルデバイスでコンソール入出力を盗聴した．その結果，コンソール入出力は暗号化された状態で記録され，管理 VM に情報が漏洩していないことが確認できた．

SCCrypt の性能を調べるために，SCCrypt と従来システムで文字入力から表示までの応答時間を比較した．準仮想化では，SCCrypt のほうが応答時間が 0.14ms 長くなったが，完全仮想化ではほぼ同じであった．また，一度に大量の文字を出力させてスループットを測定したところ，SCCrypt と従来システムで出力スループットに大きな差は生じなかった．ただし，SCCrypt では一時的に出力が止まる場合があることが確認された．

4　まとめ

本研究では，IaaS クラウドにおいて仮想シリアルコンソールを利用して安全な帯域外リモート管理を可能にするシステム SCCypt を提案した．今後の課題は SSH 以外のリモート管理ソフトウェアを用いて仮想シリアルコンソールにアクセスできるようにすることである。