仮想シリアルコンソールを用いたクラウドの安全なリモート管理

梶原達也[†1] 光来健一[†1,†2]

1. はじめに

近年、ネットワークを経由して，ユーザに仮想マシン（VM) を提供する IaaS 型クラウドサービスが広まっている．提供された VM（ユーザ VM）を管理するために，ユーザに対して仮想シリアルコンソールが提供されている．ユーザは SSH などリモート接続ソフトウェアを利用して管理 VM と呼ばれる VM にログインし，仮想シリアルコンソールに接続することでユーザ VM にアクセスできる．

しかし，クラウドにおいては，管理 VM を経由して仮想シリアルコンソールを利用すると情報漏洩の危険性が高まる．これは，ユーザ VM のキーボード入力を処理する管理 VM が必ずしも信頼できるとは限らないためである．例えば，悪意を持ったクラウド管理者が攻撃を行う可能性も考えられる．このような場合には，管理 VM 内でキーボード入力を盗聴するプログラムを動作させるだけで，パスワード等の機密情報を簡単に盗まれてしまう．

本研究では，クラウドにおいて仮想シリアルコンソールを用いる際に，管理 VM へのキーボード入力の漏洩を防ぐ SCCrypt を提案する．

2. SCCrypt

SCCrypt では， SSH クライアントと仮想マシンモニタ（VMM）の間でキーボード入力情報を暗号化する．SCCrypt は，図 1 のように SSH クライアントに対して行ったキーボード入力を暗号化して送信する．SSH サーバが入力情報を仮想シリアルデバイスに送ると，従来は仮想シリアルデバイスがユーザ VM 内のシリアルドライバに入力を送っていた．これではシリアルドライバが暗号化された入力を受け取ることになるため，SCCrypt では仮想シリアルデバイスが VMM を呼び出して入力をシリアルドライバに渡す．その際に，VMM は入力情報の復号化を行う．

また，SCCrypt では，SSH クライアントと VMM の間でスクリーン出力情報を暗号化する．従来，ユーザ VM からの出力はシリアルドライバが管理 VM の仮想シリアルデバイスに送っていたが，これでは管理 VM に出力情報が漏洩する．そこで SCCrypt では，VMM がシリアルドライバからの出力を受け取って暗号化し，仮想シリアルデバイスに送るようにする．暗号化された出力情報は SSH サーバから SSH クライアントへと送信され，SSH クライアントで復号化する．これにより，ユーザ VM には意識させずに管理 VM 上では出力情報が暗号化された状態となり，盗聴されても情報が漏洩することはない．

SCCrypt では，管理 VM にログインしてコマンドを実行するのではなく，SSH でリモートコマンドを実行する．この方法では，コマンドの文字列を通常のキーボード入力とは別に扱うことができるため，コマンドだけを暗号化せずに SSH サーバに送ることができる．また，sudo コマンドを用いることでユーザには仮想シリアルコンソールに接続するコマンドの実行のみ管理権限を与える．

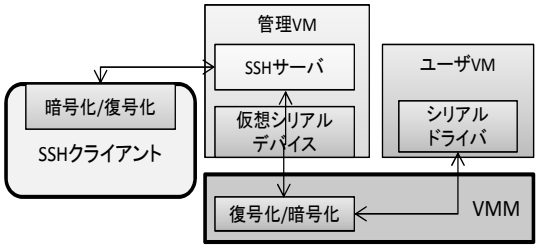

図 1 SCCrypt のシステム構成

3. 実　　験

SCCrypt を Xen 4.1.3 と OpenSSH 6.0p1 に実装し，従来通りのシステムを使う場合と SCCrypt を使う場合で，VM のコンソールリングに書き込む時間および読み込む時間を比較する実験を行った．結果は図 2 の通りである。SCCrypt での処理時間の増加は，

†1 九州工業大学
Kyusyu Institute of Technology
†2 独立行政法人科学技術振興機構, CREST
JST, CREST

暗号化・復号化のためにハイパーコールを呼び出すことが主な理由として考えられる．出力の値が非常に大きいのは入力時と異なり，読み込むデータ数が増えるためと考えられる．

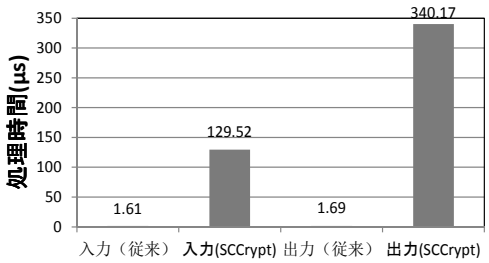

図 2 実験

4. ま と め

本研究では仮想シリアルコンソールを用いて安全にVM を操作できる SCCrypt を提案した．SCCrypt は管理 VM での情報漏えいを防ぐために SSH クライアントと VMM で暗号化・復号化を行う．

今後の課題は暗号化の方式をストリーム暗号のような安全性の高い暗号方式に変更することである．また，現在は準仮想化の VM に対してのみ実装を行っているので、完全仮想化の VM にも対応できるようにする予定である．

参 考 文 献

1) T. Egawa, N. Nishimura, and K. Kourai, Dependable and Secure Remote Management in IaaS Clouds, Proc. CloudCom 2012, 2012.