IaaS 型クラウドにおけるキーボード入力情報漏洩の防止

江川友寿[†] 光来健一[†,††]

1. はじめに

近年，ネットワークを介してサービスを提供するクラウドコンピューティングの利用が広がっている．その一形態として，ユーザに仮想マシン（VM）を提供する IaaS 型クラウドがある．ユーザはハードウェアを用意することなく，必要な時に必要なだけの VM を使用することができる．しかし，クラウドならではのセキュリティリスクとして，ユーザに提供される VM（ユーザ VM）の管理者とクラウドの管理者が異なることが挙げられる．クラウドの管理者は管理 VM を用いてユーザ VM を管理しており，ユーザ VM へのキーボード入力も管理 VM によって処理されている．クラウドの管理者が管理 VM でキーボード入力を盗聴するプログラムを動作させると，ユーザ VM に対するキーボード入力を盗むことができ，パスワード等の機密情報が漏洩する恐れがある．

本研究では，クラウドの管理者が不正アクセスを行ったとしても，ユーザ VM へのキーボード入力情報が漏洩しないシステム FBCrypt を提案する．

2. クラウド管理者への情報漏洩

IaaS 型クラウドでは，ユーザは VNC を用いて VM の操作を行うことが多い．VNC は VM の画面をユーザの PC に表示し，ユーザからのキーボードやマウスの入力を VM に送るためのソフトウェアである．仮想化ソフトウェア Xen[?)] において，VNC サーバは管理 VM と呼ばれる特殊な VM 上で動作しており，ユーザの PC の VNC クライアントから接続される．このような構成をとることにより，ユーザ VM のネットワークが正常に動作していなくても管理を行うことができるという利点がある．

その一方で，クラウドの管理者が管理 VM からユーザ VM へのキーボード入力を盗聴できてしまうという問題がある．VNC サーバは図 1 のようにクライアントからのキーボード入力を受け取り，ユーザ VM に渡す．VNC サーバを改ざんすることで，クラウドの管理者はキーボード入力を容易に盗聴することができる．従来は管理 VM の管理者はユーザ VM の管理者と同じであったり，十分に信用することができたが，クラウド環境では信用できるかどうか分からない場合がある．

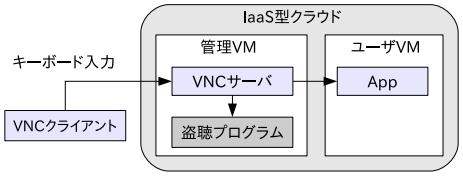

図 1 キーボード入力の盗聴

3. FBCrypt

この問題を解決するために，VNC クライアントとユーザ VM を動作させているサーバの仮想マシンモニタ（VMM）の間でキーボード入力情報を暗号化する FBCrypt を提案する．FBCrypt は，図 2 のようにユーザが VNC 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 VNC サーバに送信する．VNC サーバがキーボード入力をユーザ VM に渡す際に，VMM が間に入って復号化を行う．このシステムでは VMM は信用できると仮定する．これにより，管理 VM 内ではキーボード入力は暗号化されているため，盗聴されても情報が漏洩する心配がない．

3.1 VNC クライアントでの暗号化

FBCrypt はストリーム暗号を用いてキーボード入力を一文字単位で暗号化して VNC サーバに送る．ストリーム暗号は 1 バイト単位での暗号化が可能であり，平文のデータサイズと暗号化済みのデータサイズが常に一致する．また，キーボード入力のようなリアルタイム処理において，ストリーム暗号はブロック暗号と比較して処理が高速である．現在の実装では，OpenSSL ライブラリのストリーム暗号（RC4）アルゴリズムを VNC クライアントに組み込んでいる．

† 九州工業大学
†† 独立行政法人科学技術振興機構，CREST

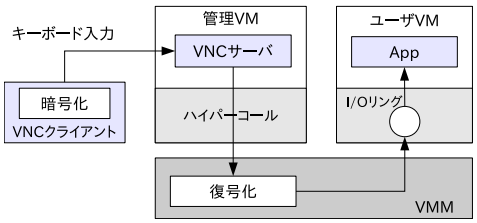

図 2 FBCrypt の構成

3.2 VMM 内での復号化

管理 VM 内で動作する VNC サーバは，VNC クライアントから受け取った暗号化されたキーボード入力情報をハイパーコールを用いて VMM に渡す．従来は VNC サーバがユーザ VM との間で共有している I/O リングにキーボード入力情報を直接書き込んでいたため，VMM はキーボード入力の内容を知ることができなかった．I/O リングとはキーボード入力を VM 間でやりとりするための専用の共有メモリのことである．VMM に新たなハイパーコールを追加し，そのハイパーコールを呼び出すように VNC サーバを修正した．暗号化されたキーボード入力情報を受け取った VMM は，それを復号化し I/O リングに書き込む．ユーザ VM は従来通りに I/O リングから復号化されたキーボード入力情報を読み出すことができるため，修正を加える必要はない．

3.2.1 I/O リングの特定

復号化したキーボード入力情報を I/O リングに書き込めるようにするために，VMM は I/O リングが置かれているメモリのアドレスを特定する．I/O リングのメモリアドレスはユーザ VM と VNC サーバの間で共有するために，ユーザ VM が管理 VM に通知している．VMM は XenBus と呼ばれる VM 間の通信路を監視することで，I/O リングのメモリアドレスを取得する．この手法は管理 VM に依存しないため，I/O リングのアドレスの詐称を防ぐことができる．また，ユーザ VM の修正は不要である．

3.2.2 I/O リングへのアクセス禁止

FBCrypt では復号化後のキーボード入力情報を I/O リングに書き込むため，復号化された情報を管理 VM から見られないように，I/O リングへのアクセスを禁止する．管理 VM が I/O リング内の情報を読み書きするためには，I/O リングが置かれているメモリページをマップする必要がある．VM がこのようなメモリマップを行うにはページテーブルを変更しなければならないが，ページテーブルの変更は VMM しか行うことができない．この仕組を利用して，管理 VM から I/O リングのメモリページのマップが要求された時には，その要求を拒否する．

表 1 キーボード入力の処理時間（μs）

	VNC クライアント	VNC サーバ	合計
従来システム	39	3.8	42.8
FBCrypt	54.5	34.7	89.2

4. 実　　験

キーボード入力一回あたりに要する処理時間を従来システムと FBCrypt で比較した．VNC クライアント側ではキーボード入力の送信処理にかかる時間を測定し，VNC サーバ側では受信処理にかかる時間を測定した．実験には Intel Core 2 Quad Q9550 2.83GHz の CPU のマシンを使用した．管理 VM であるドメイン 0 には 3GB，ユーザ VM であるドメイン U には 512MB のメモリを割り当てた．結果を表 1 に示す．測定値はキーボード入力を 100 回行った際の平均値である．

VNC クライアント側では，処理時間の差が 15.5μs であることから，ストリーム暗号は十分に高速であることがわかる．一方，VNC サーバ側では，処理時間が 10 倍となっている．これは従来システムでは VNC サーバから I/O リングへ直接キーボード入力情報を書き込んでいた処理を，ハイパーコール経由で行うようにし，さらに復号化を行っているためである．しかし，処理時間全体としては，FBCyrpt は従来システムと比較して 46.4μs しか増加しておらず，ユーザは FBCrypt による遅延を体感することなくキーボード入力を行えることがわかる．

5. ま と め

本研究では IaaS 型クラウドにおいて，ユーザのキーボード入力情報がクラウド管理者に漏洩するのを防ぐシステム FBCrypt を提案した．FBCrypt では，ユーザ PC の VNC クライアントでキーボード入力情報を暗号化し，サーバの VMM 内で復号化する．これにより，管理 VM へのキーボード入力情報の漏洩を防ぎつつ，ユーザ VM にキーボード入力情報を渡すことが可能になった．

参 考 文 献

1) Barham et al, Xen and the Art of Virtualization, In Proc. of the 19th Symposium on Operating Systems Principles, pages 164–177, 2003.