平成 23 年度 卒業論文概要			
所　　属	機械情報工学科	指導教員	光來 健一
学生番号	08237061	学生氏名	西村 直樹
論文題目	IaaS 型クラウドにおける画面情報漏洩の防止		

1　はじめに

IaaS 型クラウドはネットワークを介してユーザに仮想マシン（VM）を提供し，ユーザは必要な時に必要なだけ VM を利用することができるようになってきている．IaaS のユーザは提供された VM（ユーザ VM）に VNC や SSH などを用いてリモートからアクセスすることで管理を行う．ユーザ VM に直接アクセスするのではなく，ユーザ VM を管理する権限をもつ VM（管理 VM）経由でアクセスすることで，ユーザ VM における障害発生時でもリモート管理を可能とすることができる．しかし，IaaS においては管理 VM が信頼できるとは限らない．ユーザ VM はクラウド内のどこで動いているか正確には分からないことが多いためである．管理 VM の権限を悪用されると，ユーザ VM の画面情報を盗まれ，表示されている機密情報が第三者に漏洩する危険がある．

本研究では，管理 VM 経由でリモート管理を行う際に，仮想マシンモニタ（VMM）が暗号化を行うことでユーザ VM の画面情報の漏洩を防ぐシステム *FBCrypt-V* を提案する．

2　クラウド管理者への画面情報漏洩

IaaS のユーザは従来，ユーザ VM 内部で VNC サーバを動かし，VNC クライアントを使って接続することでシステムの管理を行っていた．この管理方法の問題点は，ユーザ VM 内部の障害によって VNC サーバへの接続ができなくなると VM のリモート管理を行えなくなることである．ユーザ VM 内でネットワークやファイアウォールの設定を間違えるだけでも，ネットワーク経由で VNC サーバにアクセスすることができなくなる．

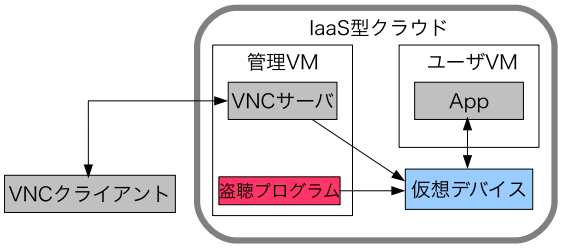

図 1　画面情報の盗聴

このような状況でもユーザ VM の管理を継続できるようにするためには，**図 1** のように管理 VM で VNC サーバを動作させることが望ましい．管理 VM とはユーザ VM の起動や停止，マイグレーションなどの制御を行える特権を持った VM のことである．管理 VM 経由でユーザ VM の仮想デバイスを通してユーザ VM にアクセスすると，ユーザ VM の障害時でもローカルコンソールからログインしているかのように操作することができ，より柔軟な VM の管理が可能になる．例えば，ユーザ VM へのネットワーク接続ができなくなってもキーボード入力などを行うことができ，OS の起動時にも起動メッセージを見ることができる．

しかし，管理 VM 経由でユーザ VM にアクセスすると情報漏洩のリスクが高まる．クラウド環境においては管理 VM が十分に信頼できるとは限らないためである．攻撃者や悪意のあるクラウド管理者によって管理 VM の権限が悪用された場合，ユーザ VM の画面情報は容易に盗聴されてしまう．ユーザ VM の画面情報は**図 1** のように，管理 VM の VNC サーバが仮想デバイスにアクセスするのと同様の方法で取得することができる．ユーザ VM の画面情報が漏洩するとシステムのセキュリティが低下したり，ユーザのプライバシが侵害されたりする．例えば，画面に表示されたパスワードやクレジットカード番号を盗み見られてしまう恐れがある．

3　FBCrypt-V

本研究では，ユーザ VM の画面情報が管理 VM に漏洩するのを防ぐシステム FBCrypt-V を提案する．FBCrypt-V では**図 2** のように，仮想マシンモニタ（VMM）がユーザ VM の仮想デバイスのフレームバッファ（VFB）を二重化し，一方の VFB を暗号化する．ユーザ VM からアクセスされた場合は暗号化されていない VFB を使用し，管理 VM からの場合は暗号化された VFB を使用する．VMM はユーザ VM が VFB に行った更新を検出し，これら 2 つの VFB の間で同期をとる．管理 VM の VNC サーバは暗号化された VFB から取得した画面情報を VNC クライアントに送ることになるため，VNC クライアントでその情報を復号する．このようにして，ユーザは通常通りにユーザ VM の画面情報を取得することができる．

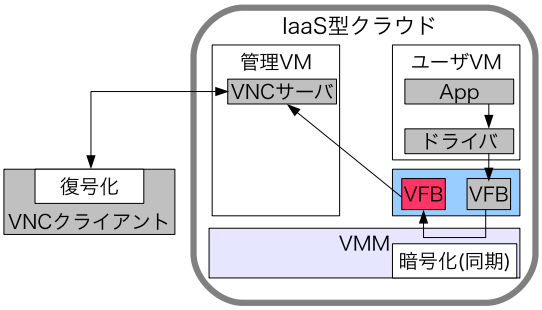

図 2　FBCrypt-V のシステム構成

FBCrypt-V を用いることで，管理 VM やユーザ VM に変更を加えることなく管理 VM への画面情報の漏洩を防ぐことができる．管理 VM からは暗号化された VFB にしかアクセスすることができず，暗号化されていない VFB へのアクセスは

VMM によって禁止される．VFB を暗号化しても管理 VM の VNC サーバはそのまま動作させることができる．VNC サーバは画面の内容を認識せず，暗号化された画面を実際の画面と考えて処理を行うためである．一方，ユーザ VM からは暗号化されていない VFB にアクセスできるため，既存のデバイスドライバをそのまま使うことができる．

3.1 VFB の二重化

FBCrypt-V はユーザ VM を起動する時に VFB の二重化を行う．従来のユーザ VM はメモリ上に確保された VFB を管理 VM と共有している．ユーザ VM を起動するとビデオドライバがメモリ上に VFB を作成する．ユーザ VM は VFB を管理 VM と共有できるようにするために，VFB として確保されたメモリ領域の情報を管理 VM に通知する．FBCrypt-V ではこの通知を VMM が横取りし，ユーザ VM のメモリを新たに確保して VFB の複製を作成する．そして VMM はユーザ VM からの通知を書き換えて，複製した VFB のメモリ領域の情報を管理 VM に渡す．このようにすることで，管理 VM がユーザ VM と同じ VFB を共有しているかのように見せる．

3.2 VFB の同期

FBCrypt-V は管理 VM 用に複製した VFB を暗号化し，これら 2 つの VFB の間の同期を取る．同期の流れを**図 3** に示す．ユーザ VM で画面が書き換えられて VFB が更新されると，画面の更新領域の情報が管理 VM に逐次通知される．VMM はこの通知を横取りし，更新領域に該当する VFB の内容を暗号化しながら管理 VM 用の VFB にコピーする．管理 VM の VNC サーバが更新領域の通知を受け取ると暗号化された VFB を読み込み，VNC クライアントに暗号化された画面情報を送る．VNC クライアントでは受信したデータを復号してから画面への描画を行う．このようにして，ユーザ VM の VFB と VNC クライアントの間で画面情報が暗号化される．

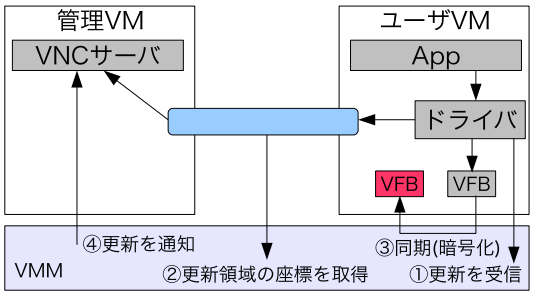

図 3　画面更新時の VFB の同期

画面情報の暗号化は RC5 [1] をベースとした暗号アルゴリズムを用いて，2 ピクセル単位で行う．RC5 は VFB で 1 ピクセルを表現するのに使われている 32 ビットをブロックサイズとすることができる．しかし，今回用いた VNC サーバはクライアントにピクセルデータを送信する際に，32 ビットのうち色情報が格納されていない上位 8 ビットをクリアしている．このため，32 ビット単位で暗号化を施すと送信時にデータが欠損してしまうため VNC クライアントにおいて復号できなくなる．そこで，安全性および実装の容易さを考慮して 2 ピクセル分の 48 ビットをブロックサイズとした．

4 実験

FBCrypt-V を用いた場合と従来システムを用いた場合について，VNC クライアントにおけるレスポンスタイムの比較を行った．実験にはギガビットイーサネットで接続された 2 台のマシンを用いた．サーバマシンでは VMM として FBCrypt-V を実装した Xen 4.1.1，管理 VM とユーザ VM の OS には Linux 2.6.39.3 を用いた．クライアントマシンでは VNC クライアントとして FBCrypt-V を実装した TightVNC Java Viewer 2.0.95 を用い，Windows 7 上で動作させた．

この実験では，ユーザ VM のスクリーンセーバを解除するために VNC クライアントに対してキーボード入力を行ってから，全画面が再描画されるまでの時間を測定した．また，レスポンスタイムの内訳として，暗号化・復号化処理，VNC クライアントの処理，VNC サーバの処理，ユーザ VM の処理にかかる時間を調べた．暗号化・復号化されるデータ量はおよそ 1.4MB であった．測定結果を**図 4** に示す．

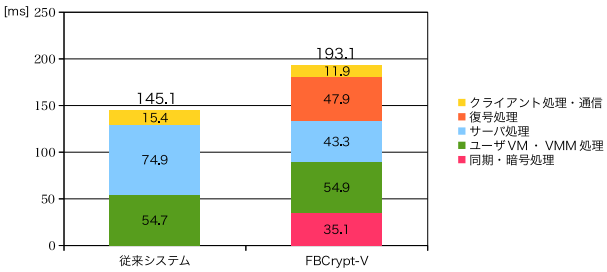

図 4　キーボード入力から画面描画までの処理時間の内訳

FBCrypt-V を用いた場合，従来システムに比べて約 48ms の遅延が発生した．遅延の主な理由は，同期・暗号化と復号化の処理がキーボード入力から画面描画までの間で行われるためであると考えられる．しかし，この遅延時間は同期・暗号化と復号化の処理時間の合計よりも小さい．これは，VNC サーバでの処理にかかる時間が従来システムより短くなっているためである．今回の実験では VNC サーバ内の処理内容は全く同じはずであるため，VM のスケジューリングが 1 つの原因として考えられる．この原因の特定は今後の課題である．

5 まとめ

本研究では管理 VM 経由でリモート管理を行ってもユーザ VM の画面情報の漏洩を防ぐシステム FBCrypt-V を提案した．FBCrypt-V はユーザ VM の VFB を VMM 内で二重化して暗号化し，VNC クライアントで復号する．そのため管理 VM で画面情報を盗聴されても，データは暗号化されているため情報が漏洩することはない．今後の課題としては，VNC クライアントからのキーボードやマウスの入力情報を暗号化する FBCrypt [2] と統合することである．

参考文献

[1] R. L. Rivest. The RC5 Encryption Algorithm. *Proc. Workshop FSE*, 1994.

[2] 江川友寿, 光来健一. 管理 VM へのキーボード入力情報情報漏洩の防止. 第 118 回 OS 研究会, 2011.