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	16675005	氏　名	猪口　恵介
論文題目	VM リダイレクト攻撃を防ぐための安全なリモート管理機構		

1　はじめに

近年，IaaS 型クラウドの利用が広まってきている．IaaS 型クラウドはユーザに仮想マシン（VM）の提供を行い，ユーザはクラウド内の管理サーバ経由で VM を管理する．しかし，クラウドにおいては管理サーバを管理するクラウド管理者は必ずしも信頼できるとは限らず，ユーザ VM に対して様々な攻撃が行われる可能性がある．考えられる攻撃の一つとして，ユーザのアクセス先 VM を変更して，クラウド管理者によって用意された悪意ある VM に接続させる VM リダイレクト攻撃がある．VM リダイレクト攻撃が行われると，悪意ある VM 内部にインストールされたマルウェアなどによってユーザ情報を盗まれる恐れがある．

本研究では，ユーザと VM を強く結びつけることで VM リダイレクト攻撃を防ぐ *UVBond* を提案する．

2　UVBond

UVBond は，ディスク暗号化を利用してユーザと VM を強く結びつける．従来，ディスク暗号化は VM 内部で行われていたが，UVBond では図 1 のように VM の下で動作するハイパーバイザでディスクを暗号化する．本研究では，ハイパーバイザは信頼できるものとする．VM の起動時に，ユーザはハイパーバイザとディスク暗号鍵を安全に共有し，ハイパーバイザ内で VM とディスク暗号鍵を結びつける．これにより，ディスク暗号鍵を介してユーザと VM を結びつける．クラウド管理者による不正なディスク暗号鍵の登録を防ぐために，ユーザはハイパーバイザによって暗号化された確認用データを用いて正しい暗号鍵が登録されていることを確認する．

VM が起動された後，ハイパーバイザはセキュアな VM 識別子をユーザに対して発行する．VM 識別子はユーザが VM の管理を行う際にハイパーバイザに渡され，その VM 識別子に対応する VM へのアクセスのみを許可することで VM リダイレクト攻撃を防ぐ．ハイパーバイザが VM の管理コマンド単位でアクセス許可を行えるようにするために，UVBond では管理コマンドがハイパーバイザに対して発行するハイパーコール列を管理コマンドの識別に用いる．そして，ユーザが指定したハイパーコール列が正常に実行されている間だけ VM へのアクセスを許可する．

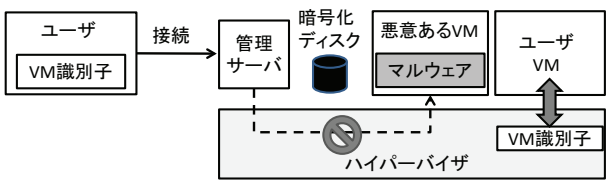

図 1: UVBond のシステム構成

UVBond では，VM が別のホストにマイグレーションされた後でも VM 識別子を使い続けることが可能である．移送元ハイパーバイザに登録されているディスク暗号鍵と VM 識別子は，移送先ハイパーバイザの公開鍵で暗号化して転送する．そのディスク暗号鍵と VM を移送先ホストでも結びつけるために，VM の仮想 CPU の状態をディスク暗号鍵で暗号化し，暗号鍵が正しい場合のみ VM を再開可能にする．

3　実験

ユーザが指定した VM に対して，指定した管理コマンドだけが実行可能であることを確認する実験を行った．実行する管理コマンドとして，VM の一時停止，再開を行うコマンドを用いた．実験の結果，VM 識別子とハイパーコール列がどちらも正しい場合は実行に成功したが，いずれかが異なる場合には失敗した．

次に，UVBond を用いた場合の VM の起動時間，およびディスク I/O 性能を測定する実験を行い，暗号化を行わない従来システムとの比較を行った．ディスク I/O 性能の測定にはベンチマークツールの fio を用いた．実験の結果，VM の起動時間は従来システムに比べて 31.5%の増加となった．ディスク I/O 性能に関しては，従来システムと比較して読み込み性能が 9.5%，書き込み性能が 3.2%の性能低下となり，いずれも 10%以下の性能低下にとどまった．

4　まとめ

本研究では，ディスク暗号化を利用してユーザと VM を強く結びつけることによって VM リダイレクト攻撃を防ぐシステム UVBond を提案した．今後の課題は，UVBond をクラウド基盤ソフトウェアに適用することである．