様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　6 月　5 日現在

機関番号：１７１０４
研究種目：若手研究(B)
研究期間：２０１０　～　２０１２
課題番号：２２７００００３６
研究課題名（和文）　仮想マシンを用いたクラウドにおける管理者からの情報漏洩の防止

研究課題名（英文）　Preventing Information Leakage from Administrators in Clouds Using Virtual Machines
研究代表者
光来　健一（KOURAI KENICHI）
九州工業大学・大学院情報工学研究院・准教授
研究者番号：６０３７２４６３

研究成果の概要（和文）：

本研究では、仮想マシン（VM）からクラウドの管理者への情報漏洩を防ぐ機構を開発した。第一に、ハイパーバイザで VM のメモリを暗号化することで、メモリ上の機密情報を保護する。その上で、暗号化すべきでないメモリ領域を特定し、VM のマイグレーションを行えるようにした。第二に、ハイパーバイザとリモート管理クライアントの間で入出力を暗号化することで、キーボード入力や画面情報の漏洩を防止できるようにした。

研究成果の概要（英文）：

This study has developed a mechanism for preventing information leakage from virtual machines (VMs) to cloud administrators. First, the mechanism protects sensitive information in the VM's memory by encrypting the memory contents at the hypervisor level. In addition, it enables VM migration by identifying unencrypted memory regions. Second, the mechanism protects sensitive keystrokes and screen information by encrypting inputs and outputs between the hypervisor and remote management clients.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,200,000	360,000	1,560,000
2011 年度	900,000	270,000	1,170,000
2012 年度	900,000	270,000	1,170,000
年度	0	0	0
年度	0	0	0
総　計	3,000,000	900,000	3,900,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：オペレーティングシステム、仮想マシン、クラウド、セキュリティ

１．研究開始当初の背景

インターネットを介してサービスを利用するクラウドコンピューティングが普及してきている。クラウドコンピューティングには様々な利用形態があるが、Amazon EC2 に代表される IaaS と呼ばれる形態では、ユーザにコンピュータ基盤である仮想マシン（VM）をクラウドとして提供する。クラウドコンピューティングに移行する際の不安

の一つはセキュリティだと言われている。この理由の一つはクラウドを提供する企業にデータを預けなければならないことである。

特に IaaS ではシステムのすべての情報を預けることになる。また、クラウドの内部構成はユーザからは分からないため、信頼性を重視して国内の企業を選択したとしても、実際にはデータは国外のデータセンタに置かれることも考えられる。このような場合、データの管理体制が十分であるかどうか分からないことが問題である。

本研究の開始前に、研究代表者は、SSR 産学戦略的研究フォーラムの「クラウドコンピューティング環境におけるセキュリティとプライバシに関する調査研究」に参画し、クラウドの管理者による情報漏洩に関する調査を行っていた。この調査により、IaaS では VM の外部から情報漏洩がおきる危険性があることが分かってきた。

Amazon EC2 で用いられている Xen などの仮想化システムでは、特権 VM と呼ばれる特殊な VM が提供されており、管理者は特権 VM を用いてユーザの VM の管理を行っている。特権 VM は負荷分散等のためにユーザ VM を遠隔ホストに移動(マイグレーション)したり、侵入検知を行ったりするために、ユーザ VM のメモリを参照する権限を与えられている。管理者が悪意を持っていたり、管理が不十分で特権 VM に脆弱性があったりした場合、ユーザ VM のメモリの内容は容易に漏洩する。申請者がこれまでに取り組んできた特権 VM からのユーザ VM の監視の研究によって、このメモリの内容を解析することで詳細なデータ構造まで把握できることが示されている。

管理者の問題により特権 VM から情報漏洩するという問題はあまり考えられていなかった。これは自分の組織内もしくはデータセンタの信頼できる管理者によって特権 VM が正しく運用されると仮定されていたためである。そのため、VM の外部からの情報漏洩としてはディスクやネットワークについて考えられることが多かった。研究代表者も、科学技術振興調整費の重要課題解決型研究である「高セキュリティ機能を実現する次世代 OS 環境の開発」において、このようなデバイスからの情報漏洩を防ぐ研究を行ってきた。この研究はクラウド環境においても有効である。また、特権 VM の権限を分割するという研究も行われているが、情報が漏洩しにくくなるというだけであり、本質的な解決にはなっていなかった。

２．研究の目的

本研究では、管理者に起因した特権 VM からの情報漏洩を防げるようにし、その仕組みが正しく動作していることをユーザが確認できるシステムの構築を目的とした。従来、情報漏洩の防止によく用いられてきた手法はメモリへのアクセス制限であるが、マイグレーションを行う際にはユーザ VM のメモリを遠隔ホストに送る必要があるため、アクセスそのものを制限することはできない。そこで、ユーザ VM のメモリの内容を必要に応じて暗号化して特権 VM に見せるという手法を用いる。また、情報漏洩が起こらないことをユーザが確信できなければ安心してクラウドを利用できないため、情報漏洩が防止されていることを明示的にユーザに見せるインタフェースも必要である。

本研究の目標は以下の三項目である。

(1) マイグレーションを行う際に特権 VM から情報が漏洩しない仕組みの構築

マイグレーションを行うために特権 VM はハイパーバイザの機能を用いてユーザ VM のメモリを参照する必要がある。ハイパーバイザがユーザ VM のメモリを暗号化して特権 VM に見せることで、特権 VM からユーザ VM のメモリ上の情報が直接見えないようにする。特権 VM は暗号化されたメモリイメージをそのまま遠隔ホストに送信し、遠隔ホストではハイパーバイザが復号化することで特権 VM にはメモリの内容を見せない。

(2) 監視のために必要な情報だけを特権 VM に見せる仕組みの構築

ユーザ VM のメモリ上の情報を見る必要がある場合には、ハイパーバイザがそのメモリ領域については暗号化を行わないようにする。例えば、監視を行うために動いているプロセスの一覧が必要となるが、プロセスの名前を見せることに問題はないと考えられる。どの部分を特権 VM に見せてよいかはユーザ VM からハイパーバイザに登録できるようにする。見せてよい部分はこれまでの研究で得られた知見を基にして列挙する。

特権 VM に見せるべきではないが、監視を行うために必要な情報も存在することが、これまでの研究成果から分かっている。例えば、Windows のプロセスを監視するためには、まずユーザ VM のメモリ全体をスキャンしてプロセスを見つける必要がある。このような情報についてはハイパーバイザが代わりに処理を実行できるようにする。そのために、ハイパーバイザが安全で柔軟に処理を行えるようにする仕組みを開発する。

(3) 情報漏洩を防ぐ仕組みが正しく動作していることをユーザが確認できる仕組みの構築

(1)(2)の手法ではハイパーバイザが情報漏洩の防止に重要な役割を担っているため、このような機能を持ったハイパーバイザが改

ざんされることなく動作していることを保証する必要がある。そのために、リモート・アテステーション技術を用いて正しいハイパーバイザが動作していることをチェックできるようにする。従来のリモート・アテステーションは特権VMと検証者との間で行われていたが、特権VMが検証中に重要な役割を果さないような仕組みを開発する。検証結果については、ユーザが安全に確認できるようにする。

３．研究の方法

以下の手順で研究を進めた。

(1) サスペンド・レジュームにおける情報漏洩の防止

まず、VMのサスペンド・レジュームを行う際に、特権VMからの情報漏洩を防げるようにする。サスペンド・レジュームはユーザVMのメモリイメージを遠隔ホストに送信する代わりにディスクに書き出す機能であり、VMのマイグレーションで使われている技術と非常に似た技術を用いて実現されている。

① メモリの暗号化処理の追加

特権VMに暗号化されたユーザVMのメモリを見せられるようにするために、ハイパーバイザの中の当該部分に暗号化処理を追加する。OSを修正せずに動かせる完全仮想化の場合はすべてのメモリを暗号化すればよいと考えられる。しかし、性能向上のためにOSを一部修正している準仮想化の場合は単純にすべてのページを暗号化するわけにはいかない。例えば、ページテーブルの書き換えが必要になる。そのため、特権VMがメモリのどの部分の内容を見られるようにする必要があるかを調査し、そのメモリの内容を特権VMに見せてよいかどうかを検討する。

② サスペンド･レジュームの際にのみ暗号化

特権VMはユーザVMを作成する時など、サスペンド・レジュームを行う時以外でもユーザVMのメモリにアクセスすることがあるため、常に暗号化を行うわけにはいかない。まず、サスペンド・レジューム以外で特権VMがユーザVMのメモリにいつアクセスしているか調べる。次に、サスペンド・レジュームの時だけ特権VMにユーザVMのメモリを暗号化して見せられるようにする。

(2) マイグレーションにおける情報漏洩の防止への適用

(1)で開発した技術をVMのマイグレーションに適用し、マイグレーションを行う際に特権VM経由で情報が漏洩しないようにする。特に、VMを一時停止させずに移動させるライブマイグレーションの場合、サスペンド・レジュームとはメモリのアクセスパターンが異なるため、そのまま適用できない場合は再検討を行う。

(3) 暗号化を行うメモリ領域の制御

特権VMに必要な情報のみを暗号化せずに見せられるようにする汎用的な仕組みを開発する。(1)(2)でもマイグレーションやサスペンドに特化した暗号化の制御を行う必要があると予想されるが、より汎用的にメモリの暗号化の制御を行えるようにする。そのために、ユーザVMからハイパーバイザに対して特権VMに見せてよいメモリ領域を登録できる仕組みを構築する。登録方法については、申請者がこれまでに行ってきた特権VMからユーザVMの監視を行う研究から得られた知見を基に検討する。

(4) ハイパーバイザによる監視処理の実現

特権VMに見せたくない情報を処理できるようにするために、ハイパーバイザ内に監視処理を行う処理系を作成する。この処理系を用いて、ハイパーバイザがユーザVMのメモリの情報を使った処理を代行する。処理結果は特権VMに渡されるため、その中に見せたくない情報が含まれてしまわないように注意する必要がある。そのため、ハイパーバイザ内の処理系で行える処理には何らかの制限が必要である。どのような処理を行える処理系を作成すれば必要十分であるかを検討した上で開発を行う。

(5) システムの信頼性の見える化

リモート・アテステーション技術を利用して、開発するシステムの中核をなすハイパーバイザの正しさをユーザが確認できるようにする。従来のリモート・アテステーションでは特権VMは信頼できると仮定していたため、特権VMが信頼できない状況で利用できる仕組みを検討する。また、管理VMによるユーザVMのメモリの参照やリソース割り当ての変更などをユーザが確認できる仕組みを導入することで、ユーザが管理者の行動を監視できるようにする。

(6) 開発したシステムの有効性の評価

開発したシステムの有効性についてセキュリティと性能の両面から評価を行う。暗号化のオーバヘッドは小さくはないが、トータルではオーバヘッドは増大しないと期待される。マイグレーションを行う際にはメモリイメージがネットワーク経由で送信されるため、セキュリティのためには暗号化して送信するべきである。この場合、暗号化を行う箇所が特権VMからハイパーバイザに変わるだけである。

４．研究成果

(1) 情報漏洩防止と VM マイグレーションの両立

ユーザ VM のメモリから管理 VM への情報漏洩を防止できるようになった。特権 VM に暗号化されたユーザ VM のメモリを見せられるようにするために、ハイパーバイザの中に暗号化・復号化の処理を追加した。具体的には、特権 VM がユーザ VM のメモリにアクセスしようとした際にはハイパーバイザが自動的にメモリ内容の暗号化を行う。アクセスを終了すると復号化を行うため、ユーザ VM は暗号化されていないメモリにアクセスすることができる。

調査の結果、特権 VM はユーザ VM の起動、サスペンド・レジューム、マイグレーションのためにユーザ VM のメモリの一部を参照したり、書き換えたりする必要があることが分かった。そこで、ハイパーバイザがこのようなメモリ領域を認識できるようにし、当該メモリ領域についてはユーザ VM のメモリ暗号化を行わないようにした。

これらの技術を用いることで、ユーザ VM のメモリからの情報漏洩を防ぎつつ、ユーザ VM のサスペンド・レジュームやマイグレーションを行うことができるようになった。管理 VM がユーザ VM のメモリをマイグレーション先のホストに送る際には、ハイパーバイザがそのメモリを自動的に暗号化する。管理 VM が参照するメモリ領域は暗号化しないが、これらのメモリ領域には機密情報は含まれないため安全性は低下しない。マイグレーション先ホストでは、受信したメモリをハイパーバイザが自動的に復号化し、ユーザ VM を復元する。

マイグレーションの場合には暗号鍵をホスト間で受け渡す必要があるため、暗号鍵を安全に管理する方式を考案した。この方式とリモート・アテステーション技術を組み合わせることで、マイグレーション先のハイパーバイザの信頼性を確認できるようにした。

さらに、ユーザ VM を停止させずにマイグレーションを行うライブマイグレーションにも対応した。まず、ユーザ VM と特権 VM が同時にメモリにアクセスできるようにするために、ユーザ VM のメモリを複製してから暗号化するようにした。これにより、特権 VM には暗号化されたメモリにアクセスさせつつ、ユーザ VM は暗号化されていないメモリにアクセスすることができる。次に、ページテーブルなどの暗号化しないメモリ領域の情報をユーザ VM のメモリに埋め込んでマイグレーション先ホストに通知できるようにした。これらの工夫によりライブマイグレーションを実現し、ダウンタイムを 1 秒以内に抑えることができた。

類似研究が国際的にも行われるようになってきたが、情報漏洩を防止しつつ、ライブマイグレーションを可能にしたのが本研究の特色である。今後は暗号化・復号化の負荷を減らしていくことが必要である。

(2) クラウドの安全なリモート管理の実現

クラウドのリモート管理を行う際に、クラウド管理者による情報漏洩が防止できるようになった。VNC 等のリモート管理ソフトウェアを用いてリモート管理を行うと、ユーザによるキーボードやマウス入力が特権 VM 経由でユーザ VM に送られ、VM の画面情報が特権 VM 経由でリモート管理クライアントに送られる。これらには機密情報が含まれる可能性があるため、ハイパーバイザとリモート管理クライアントの間で暗号化を行い、その間の管理 VM へ情報が漏洩しないようにした。

キーボード入力に関しては、リモート管理クライアントでキーボード入力を暗号化し、特権 VM で動作するリモート管理サーバを経由して、ハイパーバイザで復号化を行う。従来のハイパーバイザはキーボード入力を認識できなかったため、ユーザ VM と特権 VM の通信を監視することにより、リモート管理サーバからユーザ VM に渡されるキーボード入力をハイパーバイザが横取りできるようにした。

画面情報に関しては、ユーザ VM 内のゲスト OS への変更を加えずに済ませるために、画面情報を保持するフレームバッファを二重化した。ユーザ VM には既存のフレームバッファを提供する一方、特権 VM には暗号化したフレームバッファを提供する。これにより、ゲスト OS は従来通りにフレームバッファに画面情報を書き込むことができるが、特権 VM からは画面上に表示された機密情報を盗むことができない。これら二つのフレームバッファは画面が更新されるたびに同期をとる。同期にかかるオーバヘッドを削減するために、リモート管理クライアントから画面情報を要求された時にだけ同期を行うようにした。また、変更された画面領域を検出することで、同期をとる領域を最小限に抑えることができるようにした。

さらに、仮想化専用 OS を動作させる準仮想化環境だけでなく、汎用 OS をそのまま動作させる完全仮想化環境にも対応した。キーボード入力については、準仮想化環境では特権 VM がユーザ VM 内のバッファに直接書き込むのに対して、完全仮想化環境ではゲスト OS の命令をエミュレーションする際に読み出される。そこで、命令エミュレーションの際にキーボード入力の復号化を行うようにした。一方、画面情報については、完全仮想化環境でもフレームバッファの二重化で対応できたが、異なるタイミングで同期をとる必要があった。具体的には、管理 VM が更新領

域を特定するためにハイパーバイザに問い合わせる際に行う。実際に Windows を動作させて、リモート管理の入出力が安全に暗号化されることを確認した。

この研究についても、画面情報の暗号化・復号化の高速化が今後の課題である。

(3) ハイパーバイザによる安全な監視処理

特権 VM がユーザ VM のメモリにアクセスする必要性を減らすために、ハイパーバイザ内でユーザ VM の監視を行えるようにした。例えば、特権 VM においてきめ細かいパケットフィルタリングを行うには、ユーザ VM 内のプロセスなどの情報が必要となる。そこで、ハイパーバイザでこのような情報を取得し、特権 VM でのパケットフィルタリングをサポートできるようにした。また、ユーザ VM 内のプロセス・スケジューリングを調整する機構をハイパーバイザに埋め込み、特権 VM はスケジューリング・ポリシーだけを提供する仕組みも構築した。

ハイパーバイザ内でのパケットフィルタリングの研究は国際的に高く評価され、国際会議においてベストペーパー賞を受賞した。今後の課題はより汎用的な仕組みを構築することである。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① Tomohisa Egawa, Naoki Nishimura, and Kenichi Kourai, Security Enhancement of Out-of-band Remote Management in IaaS Clouds, IPSJ Transactions on Advanced Computing Systems, 査読有, 2013, 掲載確定.
② Hidekazu Tadokoro, Kenichi Kourai, and Shigeru Chiba, Preventing Information Leakage from Virtual Machines' Memory in IaaS Clouds, IPSJ Transactions on Advanced Computing Systems, 査読有, Vol.5, 2012, pp.101-111.
③ Kenichi Kourai and Shigeru Chiba, Fast Software Rejuvenation of Virtual Machine Monitors, IEEE Transactions on Dependable and Secure Computing, 査読有, Vol.8, 2011, pp.839-851.
④ 田所秀和, 光来健一, 千葉滋, 実用性を考慮した仮想マシン間プロセススケジューラ, 情報処理学会論文誌:コンピューティングシステム, 査読有, Vol.4, 2011, pp.100-114.

〔学会発表〕（計 12 件）

① 江川友寿, IaaS クラウドの帯域外リモート管理における情報漏洩の防止, 第 60 回 CSEC 研究会, 2013 年 3 月 14 日, 東京.
② 大薗弘記, 仮想デスクトップと PC の一元管理を可能にする仮想 AMT, 第 10 回ディペンダブルシステムワークショップ, 2012 年 12 月 12 日, 神戸.
③ Tomohisa Egawa, Dependable and Secure Remote Management in IaaS Clouds, the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2012), 2012 年 12 月 5 日, Taipei.
④ Kenichi Kourai, A Self-protection Mechanism against Stepping-stone Attacks for IaaS Clouds, the 9th IEEE International Conference on Autonomic and Trusted Computing (ATC 2012), 2012 年 9 月 7 日, Fukuoka.
⑤ 江川友寿, IaaS 環境における安全な帯域外リモート管理機構, SWoPP 島根 2012, 2012 年 8 月 1 日, 鳥取.
⑥ 西村直樹, IaaS における管理 VM への画面情報漏洩の防止, 第 120 回 OS 研究会, 2012 年 2 月 29 日, 東京.
⑦ 塩田裕司, OUassister: 仮想マシンのオフラインアップデート機構, ディペンダブルシステムワークショップ&シンポジウム, 2011 年 12 月 14 日, 京都.
⑧ 江川友寿, 管理 VM へのキーボード入力情報漏洩の防止, SWoPP 鹿児島 2011, 2011 年 7 月 27 日, 鹿児島.
⑨ 田所秀和, IaaS 環境における VM のメモリ暗号化による情報漏洩の防止, 第 117 回 OS 研究会, 2011 年 4 月 13 日, 沖縄.
⑩ 安積武志, 踏み台攻撃だけを抑制できる VMM レベル・パケットフィルタリング, 第 116 回 OS 研究会, 2011 年 1 月 24 日, 福岡.
⑪ Hidekazu Tadokoro, A Secure System-wide Process Scheduler across Virtual Machines, the 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'10), 2010 年 12 月 14 日, Tokyo.
⑫ 安積武志, 仮想マシンモニタによるきめ細かいパケットフィルタリング, 第 114 回 OS 研究会, 2010 年 4 月 22 日, 静岡.

６．研究組織

(1)研究代表者

光来　健一（KOURAI KENICHI）
九州工業大学・大学院情報工学研究院・准教授
研究者番号：60372463