様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月　 ６ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１０１

研究課題名（和文）信頼できない仮想化システムの外側へのサービスのセキュアなオフロード

研究課題名（英文）Secure Service Offloading outside Untrusted Virtualized Systems

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・教授

研究者番号：６０３７２４６３

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では、ネストした仮想化と呼ばれる技術を用いて仮想化システム全体を仮想化し、仮想化システムの外側にサービスを安全にオフロードできるようにした。仮想化システムの外側で仮想マシン（VM）を監視するシステムを動作させられるようにし、VMの帯域外リモート管理を行えるようにした。さらに、サービスを提供するVMを一意に特定できるようにした。これらを仮想化システムに頼らずに実現し、セキュアなクラウド基盤を構築することができた。

研究成果の学術的意義や社会的意義
本研究の学術的意義は、仮想化システム全体を仮想化する技術の新しい応用を確立したことである。この技術を用いてサービスを仮想化システムの外側にオフロードする本研究はセキュリティ分野に大きなインパクトを与え、研究領域の発展に寄与した。
本研究の社会的意義は、クラウド利用の最大の障害であるセキュリティを向上させることにより、ユーザが安心してクラウドサービスを利用できる社会に向けて着実に前進することができたことである。

研究成果の概要（英文）：This study enabled services to be securely offloaded outside the virtualized system using the technology called nested virtualization, which virtualizes the entire virtualized system. It achieved monitoring of virtual machines (VMs) and out-of-band remote management of VMs outside the virtualized system. In addition, it enabled VMs providing services to be uniquely identified. We achieved these mechanisms without relying on the virtualized system and constructed secure cloud infrastructure.

研究分野：オペレーティングシステム

キーワード：仮想化　セキュリティ　クラウド　監視システム　リモート管理　仮想化システム

１．研究開始当初の背景

クラウドなどで利用されている仮想化システムでは、仮想マシン（VM）のセキュリティや耐障害性を向上させるために、VM から仮想化インフラ側へのサービスのオフロード（図 1）が盛んに研究されてきた。VM の外側で侵入検知システムなどの監視システムを動作させることで、VM への攻撃を安全に監視することができる。研究代表者もこのような研究の黎明期から研究を行ってきた。また、VM 内の設定ミスなどの際に内部システムに依存せずに帯域外リモート管理を行う機能は既に一般的に利用されている。

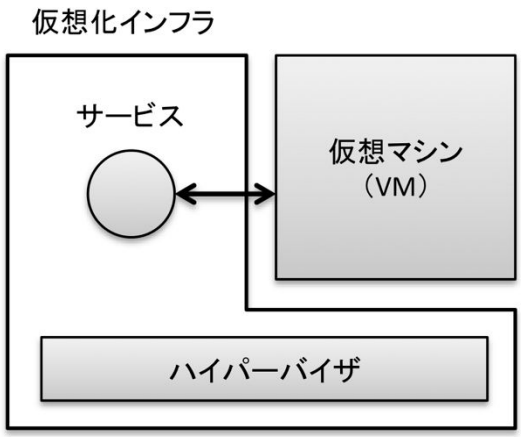

図 1 サービスのオフロード

一方、クラウドにおいては、このようなオフロードされたサービスは信頼できるとは限らない。クラウド内には信頼できない管理者が存在する可能性があるためである。実際に、2010 年には Google の管理者がユーザのプライバシー侵害を起こしている。サイバー犯罪の 28%は内部犯行であり、IT 管理者の 35%は社内の機密情報に無断でアクセスしているという報告もある。その結果、クラウド利用の最大の障害は常にセキュリティとなっている。

これまで、研究代表者は仮想化インフラの中核部分であるハイパーバイザだけを信頼してサービスを安全にオフロードする手法について研究してきた。例えば、ハイパーバイザ経由で VM を安全に監視したり、ハイパーバイザにおける暗号化により帯域外リモート管理中の情報漏洩を防いだりすることができる。この手法は、少数の信頼できる管理者がハイパーバイザを管理し、信頼できない一般の管理者が仮想化インフラのそれ以外の部分を管理することを仮定している。多くの類似研究でも同様の仮定が行われており、妥当なモデルと考えられてきた。

しかし、これまでの研究を通してこの手法の問題点も明らかになってきた。第一に、仮想化インフラ内のハイパーバイザとそれ以外の部分は密接に結びついているため、仮想化インフラ上の信頼できない管理者がハイパーバイザを攻撃できる可能性が高い。第二に、仮想化インフラのアップデートは全体として整合性を保って行う必要があるため、ハイパーバイザをアップデートできる権限を持った少数の信頼できる管理者に負担が集中する。第三に、ハイパーバイザが明確に分離されていない仮想化インフラにはこの手法を適用することが難しいため、適用範囲が限定される。

２．研究の目的

本研究では、ネストした仮想化と呼ばれる技術を用いて、図 2 のように仮想化システム全体を仮想化し、仮想化システムの外側にサービスを安全にオフロードできるようにすることを目的とした。このシステムでは仮想化システムとその外側のネスト用インフラは強く分離されるため、仮想化システム内の信頼できない管理者がネスト用インフラを攻撃することは難しい。また、仮想化システム全体を一般の管理者が管理し、ネスト用インフラを少数の信頼できる管理者が管理できるため、管理の責任分界点が明確になる。その上、従来のように仮想化インフラをハイパーバイザとその他の部分とに分けて考える必要がないため、どのような仮想化インフラにも適用できる。

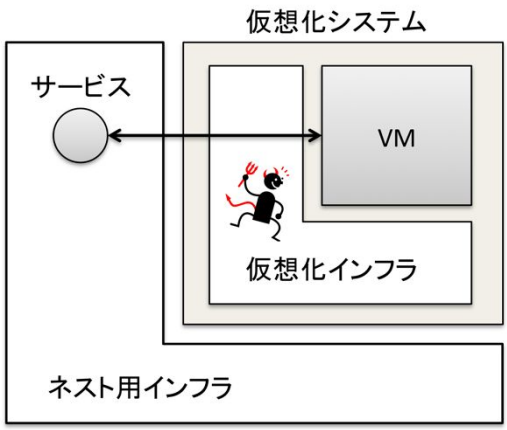

図 2 サービスのセキュア・オフロード

しかし、仮想化システムの外側で VM 用のサービスを安全に実現するのは容易ではない。VM は仮想化インフラによって実現されているにも関わらず、その仮想化インフラから得られる情報は信頼できないためである。仮想化インフラに依存しないサービスのオフロードを実現するために、本研究では以下の 3 つの課題に取り組んだ。

(1) 監視システムのセキュア・オフロード

VM を監視するシステムを仮想化システムの外側で動作させられるようにする。そのために、仮想化インフラ内の管理情報に頼らず、監視システムが VM のメモリ、ディスク、ネットワークなどから情報を安全に取得できるようにする。その上で、研究代表者が開発している VM 監

視基盤と統合することにより、既存の監視システムを動作させられるようにする。さらに、VM だけでなく、仮想化インフラの監視も行えるようにする。

(2) リモート管理システムのセキュア・オフロード

リモートユーザが仮想化システムの外側だけを経由して VM の帯域外リモート管理を行えるようにする。そのために、リモート管理に必要な仮想デバイスを仮想化システムの外側で動作させ、仮想化インフラに頼らずに VM の入出力を直接処理できるようにする。既存研究とは異なり、暗号に依存しないシステムを構築することで、リモート管理クライアントへの修正を不要にする。

(3) 仮想化システムの外側でのセキュアな VM 特定

課題(1)および課題(2)においてサービスを提供する対象となる VM を仮想化システムの外側で一意に特定できるようにする。そのために、ネスト用インフラが認識できる低レベルな VM の情報とユーザが自分の VM だと考えている実体を、VM のストレージを介して安全に結びつける。さらに、VM が別のホストにマイグレーションされたとしても追跡を続けられるようにする。

３．研究の方法

本研究では以下の手順で研究を進めた。

(1) 監視システムのセキュア・オフロード

仮想化システムの外側から VM のメモリおよびストレージの監視を行えるようにする。メモリ監視を実現するために、仮想化システム内にあるアドレス変換テーブルを用いて VM 内の OS データにアクセスする機構を開発する。信頼できない仮想化インフラに頼らずに安全に変換テーブルの情報を取得するために、CPU の仮想化支援機構を用いて VM のイベントを捕捉することにより、変換テーブルを追跡する（図 3)。変換テーブルの改ざんを防ぐには、既存研究で提案されているメモリ隔離機構を用いる。研究代表者には仮想化ソフトウェアの Xen を用いた研究実績が 10 年あるため、当初はネスト用インフラと仮想化インフラのどちらにも Xen を用いる。

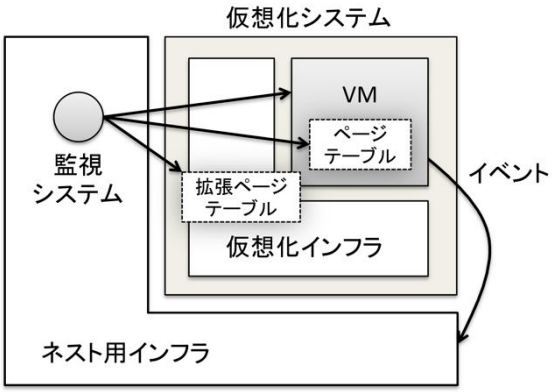

図 3 セキュアなメモリ監視

ネストした仮想化のメモリ管理は複雑であるが、ネスト用インフラから VM のメモリを操作した経験を用いてメモリ監視機構の実装を進める。一方、ストレージ監視については、ネットワーク・ストレージ上の VM のディスクイメージに監視システムからも安全にアクセスできるようにする。

次に、研究代表者が 6 年にわたって開発している VM 監視基盤と本研究で開発する監視機構を統合する。この VM 監視基盤は VM 内の OS をエミュレートし、既存の監視システムをそのままオフロードして動作させることを可能にする。統合を通して、開発中のシステムを実用的に利用するために不足している機能を洗い出し、必要な機能を実装する。

また、仮想化システムの外側から VM のネットワーク監視を行えるようにする。仮想化インフラの影響を考慮した監視を行えるように、VM が送受信した時点のパケットだけでなく、仮想化インフラによって処理される前後のパケットも取得できる機構を開発する。

開発した機構を用いて詳細な評価を行う。その一環として、仮想化ソフトウェアの KVM を用いた仮想化システムを動作させ、仮想化インフラに依存しないシステムを構築できていることを実証する。仮想化インフラの差異による挙動の違いが見つかれば、仮想化インフラに依存しないように修正を行う。さらに、VM だけでなく、仮想化インフラの監視も行えるようにする。従来の VM 監視基盤を用いることはできないため、新しく仮想化インフラ用の監視基盤を開発する。VM 監視基盤の開発手法の多くを流用できると考えられるため、短期間で開発を完了できる見込みである。

(2) リモート管理システムのセキュア・オフロード

仮想化システムの外側でテキストベースの帯域外リモート管理システムを実現する。課題(1)では VM のイベントを捕捉するだけであるのに対し、課題(2)では入出力を完全に横取りする。

VM がコンソール出力を行った際には、ネスト用インフラがそれを横取りして仮想シリアルデバイスで処理を行い、クライアントに送信する（図 4）。一方、コンソール入力を行った際には、ネスト用インフラがそれを横取りして仮想シリアルデバイスのデータを直接 VM に返す。

これまでの経験より、コンソール入出力の処理は容易に行えると考える。その上で、仮想デバイスの開発経験を活かして、ネスト用インフラ上で動作する VM 用の仮想シリアルデバイスを開発する。

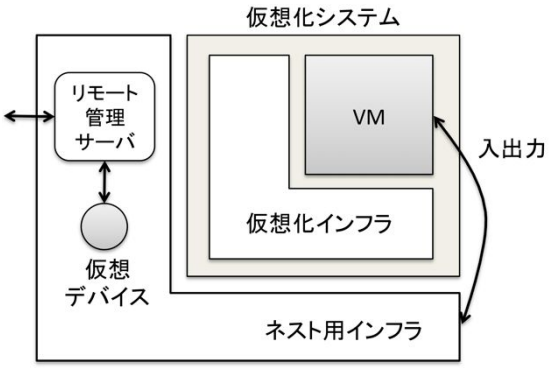

図 4 セキュアな帯域外リモート管理

仮想化システムの外側でグラフィカルな帯域外リモート管理システムを実現する。そのために、ネスト用インフラ上で動作する仮想キーボード、仮想マウス、仮想ビデオカードを開発する。これまでの経験から、仮想ビデオカードは仮想化インフラに強く依存していることが分かっており、仮想化インフラに頼らずに実装できない場合は、安全性を損なわない範囲で仮想化インフラからの情報を利用することも検討する。

(3) 仮想化システムの外側でのセキュアな VM 特定

複数の VM が起動できる研究環境を構築し、仮想化システムの外側から VM を特定できる仕組みを構築する。まず、課題(1)(2)の成果を用いて、VM のディスクアクセスを捕捉してネスト用インフラ上でディスクの暗号化・復号化を行えるようにする（図 5）。その上で、ディスクが正常に復号されたことを確認できるようにし、VM の特定につなげる。

VM を別のホストにマイグレーションした際にも仮想化システムの外側で VM を追跡できるようにする。ネスト用インフラから VM のマイグレーションを検出するのは容易ではないが、課題(1)の成果を活かして、ネットワーク監視を通してマイグレーション先を特定することを検討する。

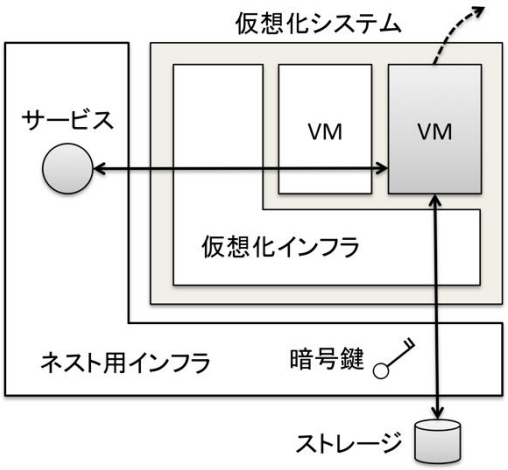

図 5 セキュアな VM 特定

４．研究成果

(1) 監視システムのセキュア・オフロード

仮想化システムの外側から VM のメモリ、ストレージ、ネットワークの監視を行えるようにした。メモリ監視については、アドレス変換テーブルを用いて VM 内の OS データにアクセスする機構を開発した。ストレージ監視については、VM のディスクイメージに安全にアクセスする機構を開発した。ネットワーク監視については、VM が送受信した時点および仮想化インフラによって処理される前後のパケットを取得する機構を開発した。さらに、これらの監視機構をこれまでに開発してきた VM 監視基盤と統合した。

次に、開発した監視システムの詳細な性能を測定した。メモリ監視については、ハイパーバイザ呼び出しの高速化により従来より 41%性能が向上した。ストレージ監視についても、2 つの仮想ディスクによる二重の先読み効果により性能が 20%向上した。一方、ネットワーク監視についてはネストのオーバヘッドのより 10%程度の性能低下が見られた。一方、既存の IDS を動作させた場合、従来とほぼ同じ性能が実現できた。この成果はセキュリティに関するトップレベルの国際会議に採択された。

仮想化システム内の VM だけでなく、それを支えるハイパーバイザと管理 VM の監視も安全に行えるようにした。そのために、ハイパーバイザのメモリを監視して VM の CPU やメモリに関する情報を取得できるようにし、管理 VM のメモリを監視して VM のネットワークに関する情報を取得できるようにした。また、仮想化システム内で VM を動作させた場合に加えて、コンテナを動作させた場合にも仮想化システムの外側から監視を行えるようにした。その結果、コンテナが消費した CPU 時間、メモリ量、ディスク帯域、ネットワーク帯域を安全に取得できるようになり、コンテナのディスクも監視できるようになった。

(2) リモート管理システムのセキュア・オフロード

まず、仮想化システムの外側でテキストベースの帯域外リモート管理システムを実現した。このシステムは VM がコンソール出力を行った際に、それを横取りして仮想シリアルデバイスで処理を行い、クライアントに出力を送信する。コンソール入力を行った際には、それを横取りして仮想シリアルデバイスが保持しているクライアントからの入力を VM に返す。また、仮想シリアルデバイスで発生した仮想割り込みを VM に転送する機構の開発も行った。

次に、仮想化システムの外側でグラフィカルなリモート管理システムを実現した。このシステムは VM が入力命令を実行した際に、それを横取りして仮想キーボードや仮想マウスで処理を行う。VM が画面出力を行った際には、それを横取りして仮想ビデオカードで処理を行う。さらに、仮想化システムとして Xen だけでなく KVM にも対応し、テキストベースおよびグラフィカルなのリモート管理を行えるようにした。そして、仮想化システムの外側で実現したリモート管理について詳細な性能評価を行った。この成果はセキュリティに関するトップレベルの国際会議に採択された。

また、開発したシステムを用いてリモート管理を行っている際にも VM をマイグレーションできるようにした。仮想化システムによってグラフィクスの扱いが異なることが判明したため、Xen と KVM とに個別に対応した。

(3) 仮想化システムの外側でのセキュアな VM 特定

仮想化システムの外側から VM を特定する仕組みを二つ検討し、実装を行った。一つ目は、VM 自身に識別子を安全に登録させる手法である。VM 内からネスト用インフラに直接、識別子を登録できる機構を開発し、その識別子を用いて VM に安全にアクセスできるようにした。二つ目は、VM の起動時に暗号化ストレージと VM を安全に結びつける手法である。VM の起動時に識別子を発行し、それを用いて指定した VM にだけアクセスできる機構を開発した。

後者の手法について、VM の起動時に発行した識別子を用いて VM のセキュアな管理を実現できるようにした。VM 管理は複雑なハイパーバイザ呼び出しを伴うため、識別子と VM 管理を結びつけるためにハイパーバイザ呼び出しのオートマトンを利用した。ハイパーバイザ呼び出しがオートマトンに受理されない状態にならない限りは、識別子によって指定された VM への操作を許可する。また、VM のマイグレーション後にも同じ識別子を用いて VM 管理を行えるようにした。

セキュアな VM 管理についての詳細な性能評価を行った。VM に対して管理コマンドを安全に実行するためのオーバヘッド、VM の起動やマイグレーションを行う際のオーバヘッド、ネスト用インフラでディスクの暗号化・復号化を行うオーバヘッドなどを測定した。この成果はクラウドに関する国際会議に採択され、ベストペーパー賞を受賞した。

５．主な発表論文等

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 18 件）

① Keisuke Inokuchi and Kenichi Kourai. UVBond: Strong User Binding to VMs for Secure Remote Management in Semi-Trusted Clouds. The 11th IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2018), 2018.
② Shota Futagami, Tomoya Unoki, and Kenichi Kourai. Secure Out-of-band Remote Management of Virtual Machines with Transparent Passthrough. The 2018 Annual Computer Security Applications Conference (ACSAC 2018), 2018.
③ 鵜木智矢，二神翔太，光来健一．シャドウデバイスを用いた帯域外リモート管理に対応した VM マイグレーション．情報処理学会第 30 回コンピュータシステム・シンポジウム (ComSys 2018)，2018 年．
④ 植木康平，光来健一．VM 内コンテナを用いたサービス単位のオートスケール機構．日本ソフトウェア科学会第 35 回大会，2018 年．
⑤ Kenichi Kourai, Naoto Fukuda, and Tomohiro Kodama. Efficient Page-cache Encryption for Smart Devices with Non-volatile Main Memory. The 33rd ACM/SIGAPP Symposium on Applied Computing (SAC 2018), 2018.
⑥ 森川智紀，光来健一．クラウドにおける VM 内コンテナを用いた低コストで迅速な自動障害復旧．情報処理学会第 142 回 OS 研究会，2018 年．
⑦ 二神翔太，鵜木智矢，光来健一．強制パススルー機構を用いた VM の安全な帯域外リモート管理．情報処理学会第 29 回コンピュータシステムシンポジウム，2017 年．
⑧ 猪口恵介，光来健一．クラウドにおける VM リダイレクト攻撃を防ぐためのリモート管理機構．日本ソフトウェア科学会第 34 回大会，2017 年．
⑨ Shohei Miyama and Kenichi Kourai. Secure IDS Offloading with Nested Virtualization and Deep VM Introspection. The 22nd European Symposium on Research in Computer Security (ESORICS 2017), 2017.
⑩ 鵜木智矢，光来健一．シャドウデバイスを用いた帯域外リモート管理を継続可能な VM マ

イグレーション．情報処理学会第 140 回 OS 研究会，2017 年．

⑪ 美山翔平，光来健一．V-Met:IaaS 型クラウドにおける仮想化システム外部からの安全な VM 監視．情報処理学会第 139 回 OS 研究会，2017 年．

⑫ Kenichi Kourai and Kouta Sannomiya. Seamless and Secure Application Consolidation for Optimizing Instance Deployment in Clouds. The 8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2016), 2016.

⑬ Kenichi Kourai and Hiroki Ooba. VMBeam: Zero-copy Migration of Virtual Machines for Virtual IaaS Clouds. The 35th IEEE Symposium on Reliable Distributed Systems (SRDS 2016), 2016

⑭ 美山翔平，光来健一．クラウドにおける仮想化システム外部からの安全な VM 監視機構．日本ソフトウェア科学会第 33 回大会，2016 年．

⑮ 二神翔太，光来健一．ネストした仮想化を用いた VM の安全な帯域外リモート管理．SWoPP 松本 2016，2016 年．

⑯ Kenichi Kourai and Kazuki Juda. Secure Offloading of Legacy IDSes Using Remote VM Introspection in Semi-trusted Clouds. The 9th IEEE International Conference on Cloud Computing (CLOUD 2016), 2016.

⑰ 猪口恵介，光来健一．クラウドのリモート管理における VM リダイレクト攻撃の防止．情報処理学会第 137 回 OS 研究会，2016 年．