

## 科学研究費助成事業 研究成果報告書

平成 28 年 5 月 28 日現在

機関番号：17104

研究種目：基盤研究(C) (一般)

研究期間：2013～2015

課題番号：25330086

研究課題名(和文) 仮想IaaSクラウドの実現に向けた高速で柔軟なVM再配置の研究

研究課題名(英文) A Study on Rapid and Flexible VM Replacement for Virtual IaaS Clouds

研究代表者

光来 健一 (Kourai, Kenichi)

九州工業大学・情報工学研究院・准教授

研究者番号：60372463

交付決定額(研究期間全体)：(直接経費) 3,700,000円

研究成果の概要(和文)：本研究では、ネステッドVMを用いて既存のIaaSクラウドの上に仮想IaaSクラウドを構築し、よりセキュアなIaaSクラウドを迅速に提供できるようにした。仮想IaaSクラウドによるコストの上昇を抑えるために、稼働率の低いVMを迅速に集約することによってコストダウンを図る瞬間マイグレーションを開発した。また、セキュリティVMと監視対象VMを独立してマイグレーションできるようにすることで、より柔軟なVM再配置を実現した。

研究成果の概要(英文)：In this study, we enabled constructing virtual IaaS clouds on top of existing IaaS clouds using nested virtual machines (VMs) and rapidly providing more secure IaaS clouds. To suppress the increase in costs due to virtual IaaS clouds, we have developed instantaneous VM migration for reducing costs by rapidly consolidating under-utilized VMs. In addition, we enabled independent migration of a security VM and its target VM to achieve more flexible VM replacement.

研究分野：情報学

キーワード：仮想化技術 クラウド 仮想マシン マイグレーション

## 1. 研究開始当初の背景

IaaS クラウドのユーザにとってセキュリティは重大な関心事になっている。これまでに、研究代表者を含め多くの研究者が、よりセキュアな IaaS クラウドを構築できるようにするための研究を行ってきた。例えば、VM の下で動作するハイパーバイザでセキュリティ機構を提供したり、セキュリティ VM と呼ばれる専用 VM から他の VM の挙動を監視したりすることができるようになってきている。しかし、このような研究成果は既存の IaaS クラウドではなかなか使えるようにならないのが現状であった。

そこで、本研究では、図 1 のように既存の IaaS クラウドの上に仮想的な IaaS クラウドを構築できるようにすることで、よりセキュアな IaaS クラウドを迅速に提供できるようにすることを目指す。仮想 IaaS クラウドは、既存の IaaS クラウドによって提供される VM (ホスト VM) の中で VM (ゲスト VM) を動作させる。そして、ホスト VM 内でセキュリティ VM を動作させたり、最新のセキュリティ機構を備えたハイパーバイザを動作させたりすることにより、ゲスト VM に高いセキュリティを提供する。

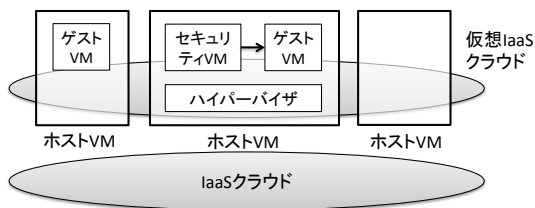


図 1 仮想 IaaS クラウド

仮想 IaaS クラウドを構築する上での一つの障害は、ホスト VM 内で動作させる必要のあるハイパーバイザやセキュリティ VM が、ゲスト VM を動作させるためのコストを上昇させてしまうことである。本研究では、多くの IaaS クラウドが VM に一定のリソースを保証して VM 単位の課金をを行っていることに着目し、ホスト VM 内に稼働率の低いゲスト VM をできるだけ集約することにより、コストダウンを図る。ただし、集約されたゲスト VM にも一定のリソースを保証できるようにするには、ホスト VM の負荷に応じてゲスト VM の再配置を行う必要がある。

VM 再配置はいくつかのゲスト VM を別のホスト VM に移動 (マイグレーション) することによって行うことができる。しかし、マイグレーションの完了までには時間がかかるため、VM 再配置を迅速に行うのは難しい。その上、マイグレーション処理はホスト VM の負荷をさらに高めてしまう。また、セキュリティ VM を用いて VM を監視している場合、VM 再配置を柔軟に行うのは難しい。研究代表者がこれまでに開発した機構を用いることでセキュリティ VM をマイグレーシ

ョンできるようにになったが、監視対象の VM と一緒にマイグレーションする必要がある。そのため、双方の VM の負荷が高い場合には十分な余裕のあるホスト VM を見つけるのが難しくなる。

## 2. 研究の目的

VM 再配置は既存のサーバ統合でも問題になっているが、本研究では、仮想 IaaS クラウドのアーキテクチャを活かして迅速で柔軟な VM 再配置を実現する。そのために、仮想 IaaS クラウドのプロトタイプを構築し、以下の課題に取り組む。

### (1) ホスト VM 間の瞬間マイグレーション

ホスト VM の負荷が高くなった場合、ゲスト VM を同一物理サーバ上の余裕のあるホスト VM にマイグレーションすることで、迅速な VM 再配置を可能にする。ホスト・ハイパーバイザとゲスト・ハイパーバイザを連携させることにより、ネットワーク転送やメモリコピーを行うことなく、ホスト VM 間でゲスト VM のマイグレーションを瞬時に完了させられるようにする。さらに、このマイグレーション手法を応用して、ゲスト・ハイパーバイザのソフトウェア若化 (予防保守) の高速化を行う。研究代表者はこれまでもハイパーバイザのソフトウェア若化の高速化に取り組んできたが、さらなる高速化が期待できる。

### (2) セキュリティ VM の柔軟なマイグレーション

セキュリティ VM を監視対象 VM とは独立にマイグレーションして、別々のホスト VM 上で動作させられるようにすることで、より柔軟な VM 再配置を可能にする。これらの VM が同一物理サーバの別々のホスト VM 上で動作する場合には、ハイパーバイザ間の連携を通してセキュリティ VM が監視対象 VM のメモリを直接参照することにより、同一ホスト VM 内と同等の性能でのメモリ監視を可能にする。一方、これらの VM を別々の物理サーバ上で動作させる場合には、監視対象 VM をネットワーク経由で監視できるようにし、転送データ量ができるだけ少なくなるように最適化する。さらに、研究代表者がこれまでに開発してきた VM 監視基盤にこれらのリモートメモリ監視機構を組み込む。

### (3) VM の物理配置に応じた最適化

(1)(2)のようにゲスト VM のマイグレーション先を意識した高速化を行えるようにするために、仮想 IaaS クラウドからホスト VM の物理的な配置を認識できるようにする。そして、できるだけ同一物理サーバ上のホスト

VM間でマイグレーションできるようにするために、余裕のあるホストVMが残るようにゲストVMを集約する。ホストVMは別の物理サーバにマイグレーションされる可能性もあるため、随時、ホストVMの物理配置に関する情報を更新できるようにする。また、VM再配置の結果、セキュリティVMと監視対象VMの位置関係が変わった場合には、利用するメモリ監視機構をシームレスに切り替えられるようにする。

### 3. 研究の方法

以下の手順で研究を進めた。

#### (1) ホストVM間の瞬間マイグレーション

VMの中でVMを動作させる技術(ネステッドVM)に対応した仮想化ソフトウェアであるXen-Blanketを用いて、まず、仮想IaaSクラウドの基本部分を構築する。物理サーバ1台、ホストVM2つ、ゲストVM1つから成る最小構成の構築を行い、ホストVM間の通常のマイグレーションの動作確認および性能評価を行う。この過程で、性能や安定性に大きな問題が見つかった場合には、ネステッドVMに対応した別の仮想化ソフトウェアであるLinux KVMの利用を検討する。

次に、同一物理サーバ上のホストVM間でゲストVMを瞬時にマイグレーションできるようにするために、ホストVM間でゲストVMのメモリをスワップする機構を開発する。マイグレーション先に空のゲストVMを作成し、そのメモリをマイグレーション元のゲストVMのメモリと交換することで、瞬間マイグレーションを実現する(図2)。それぞれのゲストVMは別々のゲスト・ハイパーバイザによって管理されているため、ハイパーバイザを連携させる仕組みも開発する。加えて、この機構を用いてマイグレーションを行うツールを開発する。

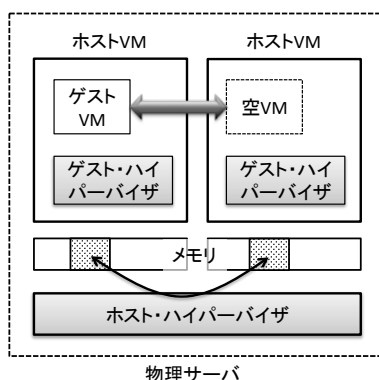


図2 瞬間マイグレーション

さらに、瞬間マイグレーションを応用してソフトウェア若化(予防保守)の高速化を行う。すべてのゲストVMを同一物理サーバ上の別のホストVMに瞬時にマイグレーションすることで、ゲスト・ハイパーバイザを必要

な時に即座に再起動できるようになる。しかし、ホストVM間でメモリをスワップする方式ではマイグレーション先に十分な空きメモリが必要となるため、ゲストVMとともに物理メモリを移動させる方式を専用に開発する。

これらの開発が完了した後、ホストVMとゲストVMの様々な構成について、様々なワークロードを用いてマイグレーションおよびソフトウェア若化の性能評価を行う。

#### (2) セキュリティVMの柔軟なマイグレーション

(1)でのノウハウの蓄積を待つために、先に、セキュリティVMをマイグレーションして監視対象VMとは別の物理サーバ上で動作させられるようにする。そのために、監視対象VMが動作している物理サーバのハイパーバイザ経由で、セキュリティVMがリモートの監視対象VMのカーネルメモリ上のデータを取得できるようにする(図3)。既存のセキュリティVMはページ単位でメモリにアクセスするため、リモートメモリ監視機構にもまずは同じインタフェースを実装する。この機構を研究代表者がこれまでに開発してきたVM監視基盤であるVM Shadowに組み込み、既存の監視ソフトウェアを動作させて性能評価を行う。

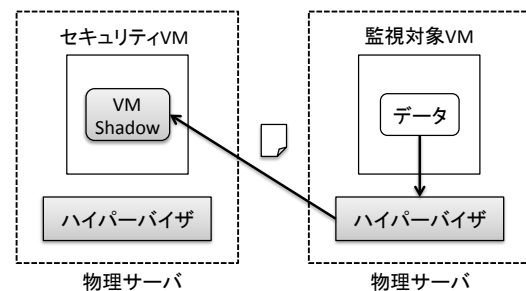


図3 リモートメモリ監視

ネットワーク経由でメモリページ単位の転送を行うと監視性能が著しく低下することが予想されるため、メモリアクセスのインタフェースの最適化を行う。具体的には、監視するカーネルデータに応じて、必要なメモリ領域だけをまとめて転送したり、圧縮したりすることで、転送データ量を削減する。また、スクリプトをハイパーバイザに送ることで、リスト構造などをもつカーネルデータも一括で取得できるようにする。

セキュリティVMと監視対象VMを同一物理サーバ上の別々のホストVMで動作させる場合に、メモリ監視の高速化を行う。そのために、監視対象VMのメモリの一部をセキュリティVMに共有させる機構を開発し、セキュリティVMが直接、監視対象VMのメモリを監視できるようにする。この機構の実現にはハイパーバイザ間の連携が必要となるが、

(1)で蓄積されたノウハウを活用することで、比較的容易に実装できると考えられる。

構築した仮想 IaaS クラウドに開発した機構を統合し、実際の IaaS クラウドに近い環境で様々なマイグレーションを行いながら監視性能の評価を行う。

### (3) VM の物理配置に応じた最適化

まず、IaaS クラウドを構築するためのクラウド管理基盤ソフトウェアについての調査を行い、OpenStack などいくつかの候補の中からどれを利用するかを比較検討する。他の候補としては、CloudStack や Eucalyptus などが考えられる。

次に、クラウド管理基盤ソフトウェアを用いて、必要最小限の構成として制御ノード 1 台、計算ノード 2 台からなる IaaS クラウドを構築し、その上に仮想 IaaS クラウドを構築する。そして、IaaS クラウド側には物理位置を指定してホスト VM を作成する機能を追加し、仮想 IaaS クラウド側にはホスト VM の物理位置を取得する機能を追加する。これらの機能を用いて、セキュリティ VM と監視対象 VM の位置関係の動的な変化に応じて、メモリ監視機構をシームレスに切り替える仕組みを開発する。

## 4. 研究成果

### (1) ホスト VM 間の瞬間マイグレーション

VM の中で VM を動作させる技術 (ネステッド VM) に対応した仮想化ソフトウェアとして Xen-Blanket を用いることを検討したが、その過程で提案手法を実現するにあたってのアーキテクチャ上の問題が見つかった。そこで、ネステッド VM を実験的にサポートし始めた Xen 4.2 を用いることにした。ホスト VM 間でゲスト VM のメモリをスワップする機構を実装し、それを用いたマイグレーション機構を開発した。実験の結果、開発したマイグレーション手法はゲスト VM のメモリのサイズにあまり依存せずにマイグレーションを行えることが分かった。768MB のメモリをもつゲスト VM をマイグレーションすると、従来のマイグレーション手法と比べて 40% 高速化できた。

次に、ホスト VM 間でのマイグレーションにおけるダウンタイムの削減について検討した。その結果、ゲスト VM のメモリをスワップする方式ではある程度以上、ダウンタイムが削減できないことが分かった。そのため、ゲスト VM 間でメモリを高速にコピーする方式、および、ゲスト VM 間でメモリを移動する方式を開発した。実験によりこれらの二つの手法の詳細な比較を行い、どちらの方式もダウンタイムを同程度に削減できることが分かった。一方、マイグレーション時間はメモリを移動する方式のほうが短いことが分かったため、こちらの方式を採用した。これにより、提案手法は従来のマイグレーション手法の最大 5.8 倍高速にマイグレーションを行うことができるようになった。

開発した手法を用いてホスト VM 間の瞬間マイグレーションの評価を行った。本評価においては、仮想 IaaS クラウドと既存の IaaS クラウドでの従来のマイグレーションおよび Xen-Blanket を用いた高速マイグレーションとの比較を行った。その結果、提案手法によるマイグレーションは 6~22 倍高速であることが分かった。それに加えて、マイグレーション時にはネットワーク負荷とメモリ負荷はほぼゼロとなり、CPU 負荷も従来の 30% 以下となることが分かった。

さらに、瞬間マイグレーションを活用して仮想 IaaS クラウドのインスタンス配置を動的に最適化できるシステムの開発も行った。

### (2) セキュリティ VM の柔軟なマイグレーション

別のホストにマイグレーションしたセキュリティ VM から監視を行えるようにするために、セキュリティ VM がリモートの監視対象 VM のカーネルメモリ上のデータを取得できるようにした。このリモートメモリ監視機構を VM 監視基盤である VM Shadow に組み込み、既存の監視ソフトウェアを動作させられるようにした。監視性能を測定した結果、ナイーブな実装では監視に従来の 15 倍の時間を要することが分かった。その内訳を調査したところ、通信に 64% の時間が費やされていることがわかった。

そこで、セキュリティ VM が監視対象 VM のメモリ情報を 4KB のページ単位で取得するように最適化し、その情報を適切にキャッシュするようにした。これにより、リモート監視にかかる時間を従来の 3.6 倍にまで削減することができた。また、メモリのリモート監視だけでなく、ネットワークとディスクのリモート監視にも対応した。

開発した機構を用いて VM のリモート監視の評価を行った。メモリ監視については性能が従来の 8% 程度にまで低下したが、ディスク監視については 3% 程度の性能低下で済むことが分かった。一方、VM 監視基盤を用いて既存の監視ソフトウェアを動作させたところ、ディスクの整合性検査では性能が 8% 低下したが、マルウェア検査では 13% 向上した。パケット検査では攻撃の検出時間の増加は 2% 程度であった。これより、リモート監視を行っても、監視性能の低下はわずかであるか、状況によっては性能が向上することが分かった。

ここまでで、セキュリティ VM だけを監視対象 VM とは別のホストにマイグレーションすることができるようになった。それに加えて、同一ハイパーバイザ上で動作している監視対象 VM とセキュリティ VM を、監視を継続したまま一緒にマイグレーションする機構も開発した。また、セキュリティ VM と監視対象 VM が同一ホスト上の別々のホスト VM で動作している場合には、ホスト・ハイパーバイザ経由で直接監視できるように最適化を

行った。

さらに、セキュリティ VM の機能拡張を行い、監視対象 VM に気づかれることなく、セキュリティ VM を経由した帯域外リモート管理を行えるようにした。さらに、ハイパーバイザに機能を追加することで、セキュリティ VM に侵入されたとしてもリモート管理の情報が漏洩しないようにした。また、AMT と呼ばれる監視用ハードウェアを仮想化した仮想 AMT をセキュリティ VM 上で動かせるようにした。

### (3) VM の物理配置に応じた最適化

検討の結果、Eucalyptus を用いて IaaS クラウドおよび仮想 IaaS クラウドを構築することとした。そして、IaaS クラウドと仮想 IaaS クラウドを連携させ、ゲスト VM がどの物理サーバ上で動作しているかを検出する機構を開発した。この機構は、ゲスト VM を管理する Eucalyptus のフロントエンドとホスト VM を管理する Eucalyptus のフロントエンドの情報を突き合わせて物理サーバを特定する。この機構を用いることで、仮想 IaaS クラウド上のゲスト VM の位置情報を管理できるようになり、物理ノードと仮想ノードの両方における負荷分散を考慮したインスタンス配置を行えるようになった。

## 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 3 件)

- ① Sho Kawahara and Kenichi Kourai, Virtual Machine Co-migration for Out-of-band Remote Management, 査読有, IPSJ Journal of Information Processing, Vol. 24, No. 4, 2016, 印刷中.
- ② Kenichi Kourai and Hisato Utsunomiya, Co-migration of Virtual Machines with Synchronization for IDS Offloading, IPSJ Transactions on Advanced Computing Systems, 査読有, Vol. 7, No. 4, pp. 45-55, 2014.
- ③ Kenichi Kourai, Takeshi Azumi, and Shigeru Chiba, Efficient and Fine-grained VMM-level Packet Filtering for Self-protection, International Journal of Adaptive, Resilient and Autonomic Systems, 査読有, Vol. 5, No. 2, pp. 83-100, 2014.

[学会発表] (計 18 件)

- ① 三宮浩太, 光来健一, クラウドにおけるライブラリ OS を用いたインスタンス構成の動的最適化, 第 135 回 OS 研究会, 2015 年 11 月 24 日, 東京都文京区.
- ② Kenichi Kourai and Tastuya Kajiwara, Secure Out-of-band Remote Management Using Encrypted Virtual Serial

Consoles in IaaS Clouds, the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2015 年 8 月 22 日, Helsinki (Finland).

- ③ 美山翔平, 光来健一, V-Met:クラウドにおけるネストした仮想化を用いた安全な監視機構, SWoPP 別府 2015, 2015 年 8 月 4 日, 大分県別府市.
- ④ Kenichi Kourai and Hiroki Ooba, Zero-copy Migration for Lightweight Software Rejuvenation of Virtualized Systems, the 6th ACM Asia-Pacific Workshop on Systems, 2015 年 7 月 27 日, Koto-ku (Tokyo).
- ⑤ Kenichi Kourai and Kouki Oozono, Virtual AMT for Unified Management of Physical and Virtual Desktops, the 39th IEEE Computer Software and Applications Conference, 2015 年 7 月 1 日, Taichung (Taiwan).
- ⑥ 川原翔, 光来健一, 帯域外リモート管理の継続を可能にする VM マイグレーション, 第 132 回 OS 研究会, 2015 年 2 月 26 日, 長崎県長崎市.
- ⑦ 大庭裕貴, 光来健一, 仮想化システムの軽量なソフトウェア若化のためのゼロコピー・マイグレーション, 第 132 回 OS 研究会, 2015 年 2 月 26 日, 長崎県長崎市.
- ⑧ Sho Kawahara and Kenichi Kourai, The Continuity of Out-of-band Remote Management across Virtual Machine Migration in Clouds, the 7th IEEE/ACM International Conference on Utility and Cloud Computing, 2014 年 12 月 9 日, London (UK).
- ⑨ 大庭裕貴, 光来健一, 仮想化システムのソフトウェア若化のための軽量な VM マイグレーション, コンピュータシステムシンポジウム 2014, 2014 年 11 月 20 日, 東京都江東区.
- ⑩ 重田一樹, 光来健一, クラウドの内部攻撃者に対する安全なリモート VM 監視機構, コンピュータセキュリティシンポジウム 2014, 2014 年 10 月 23 日, 北海道札幌市.
- ⑪ 梶原達也, 光来健一, 仮想シリアルコンソールを用いた VM の安全な帯域外リモート管理, SWoPP 新潟 2014, 2014 年 7 月 28 日, 新潟県新潟市.
- ⑫ 三宮浩太, 光来健一, クラウドにおけるアプリケーション単位での VM 構成の動的最適化, 第 129 回 OS 研究会, 2014 年 5 月 14 日, 沖縄県那覇市.
- ⑬ 土田賢太郎, 光来健一, CacheShadow ファイルシステム: 仮想ディスクと VM 内キャッシュの統合, 第 128 回 OS 研究会, 2014 年 3 月 6 日, 富山県富山市.
- ⑭ 大藪弘記, 光来健一, 仮想マシンと物理

マシンの一元管理を可能にする仮想 AMT,  
第 128 回 OS 研究会, 2014 年 3 月 6 日, 富  
山県富山市.

- ⑮ 大庭裕貴, 光来健一, ネストした VM を  
用いた仮想化システムの高速度なソフトウ  
ェア若化, 第 127 回 OS 研究会, 2013 年  
12 月 3 日, 東京都江東区.
- ⑯ Kenichi Kourai and Hisato Utsunomiya,  
Synchronized Co-migration of Virtual  
Machines for IDS Offloading in Clouds,  
the 5th IEEE International Conference  
on Cloud Computing Technology and  
Science, 2013 年 12 月 2 日, Bristol  
(UK).
- ⑰ 重田一樹, 光来健一, クラウド上の仮想  
マシンの安全なリモート監視機構,  
SWoPP 北九州 2013, 2013 年 8 月 1 日, 福  
岡県北九州市.
- ⑱ 川原翔, 光来健一, 帯域外リモート管理  
の継続が可能なマイグレーション手法,  
SWoPP 北九州 2013, 2013 年 7 月 31 日, 福  
岡県北九州市.

## 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