クラウド環境を想定した仮想計算機リソース管理における セキュリティフレームワークの提案

岡本 慶大† 森川 泰揮† 野口 悟† 池部 実† 猪俣 敦夫† 河合 栄治‡
藤川 和利† 砂原 秀樹§†

† 奈良先端科学技術大学院大学 情報科学研究科
630-0192 奈良県生駒市高山町 8916-5

‡ 情報通信研究機構
100-0004 東京都千代田区大手町 1-8-1 KDDI 大手町ビル 21 階

§ 慶應義塾大学 メディアデザイン研究科
223-8526 神奈川県横浜市港北区日吉 4-1-1

あらまし 近年，Cloud Computing などの新たな計算機環境が提供されるようになった．そのリソースとなるサーバは VM 技術によって仮想化され，単一サーバ上で複数の VM が動作しそれらをサービスの利用者へ分配するというモデルが一般的になってきた．しかし，従来のサーバ単位で行われていたリソース分配が，サーバ内またはサーバ間にまたがることになり，サーバ内でのリソース浪費による SLA への影響や，局所集中化したデータを標的としたクラッキングなどの新たなリスクが発生しうる．そこで本論文では，クラウド環境で利用される VM について，セキュリティ要件に関する調査を行い，必要となる機能・フレームワークについて考察する．

Proposal of a Security Framework for Virtual Machine Resource Management on Cloud Computing

Yoshihiro OKAMOTO† Taiki MORIKAWA † Satoru NOGUCHI †
Minoru IKEBE † Atsuo INOMATA † Eiji KAWAI ‡
Kazutoshi FUJIKAWA † Hideki SUNAHARA §†

†Nara Institute of Science and Technology
8916-5 Takayama-Cho Ikoma-Shi Nara 630-0192 Japan
‡National Institute of Information and Communications Technology
21F KDDI Otemachi Bldg. 1-8-1 Otemachi Chiyoda-Ku Tokyo 100-0004 Japan
§National Institute of Information and Communications Technology
4-1-1 Hiyoshi Kohoku-Ku Yokohama-Shi Kanagawa 223-8526 Japan

Abstract Cloud computing is a means of providing service delivery for consumer and business needs in a simplified way, providing unbounded scale and differentiated quality of service. In this paper, we introduce some features of VM(Virtual Machine) and focus on some security issues on these new environments, also we discuss a new security framework based on VM, especially for Cloud.

1 はじめに

Google や Amazon のように，Cloud Computing と呼ばれる計算機環境を提供するプロバイダ (クラウドプロバイダ) が増加してきている．これらクラウドプロバイダは，データセンターを構築し，顧客へそのリソースの一部を

提供している．ここで利用されるサーバは導入時期などによって様々なメーカーやスペックのものが混在しているが，クラウドプロバイダは仮想計算機 (VM: Virtual Machine) 技術を利用することで，ハードウェアの違いを吸収している．また VM を利用することで，時間やユーザ数による負荷の偏りを平均化し，かつサーバの平均負荷率を上げることができる．さらに，物理的なサーバと OS が切り離されることで，マイグレーションやスナップショットを活用して，ハードウェアの障害やメンテナンス時でもサービスの継続性を向上させることに成功している．

しかし，全く関係の無い VM 同士が同一のサーバ上でリソース競合を起こす可能性もあり，VM 間のリソース隔離は SLA (Service Level Agreement) の保証を行う意味でもより重要な要素となってきている．これらの問題について筆者らは，セキュア・プラットフォームプロジェクトにおいて調査研究を進めてきた [17]

本研究では，Cloud Computing の概要および構成例と，そこで利用される VM について調査し，クラウド環境において必要となるセキュリティ上の機能やフレームワークについて考察する．

2 Cloud Computing

本節では Cloud Computing の定義と関連用語について解説する．

2.1 定義

Cloud Computing という用語は，2006 年に Google 社の CEO である Eric E. Schmidt が Search Engine Strategies Conference and Expo 2006 San Jose で行ったスピーチの中で使用したのが始まりと言われている．Cloud Computing とは，規模の経済性によって進んでいる大規模分散コンピューティングのパラダイムである．規模の経済性とは，生産規模の拡大に伴い，コストが下がり効率が上がることを意味している．すなわち，Cloud Computing とはインターネットを通じて，外部の顧客の要求に応じてサービスやプラットフォームを提供するコンピューティング形態を意味している [7].

2.2 関連用語

本節では，Cloud Computing と関係の深い用語について解説する．

2.2.1 XaaS

XaaS とは，”X as a Service”の総称であり，インターネット経由でクラウドプロバイダから提供されるものを示す言葉である．現在クラウドプロバイダが提供しているサービスは大まかに 3 つの XaaS に分けられる

SaaS: Software as a Service
: インターネット経由でソフトウェアパッケージを提供．例として Gmail, Google Maps 等 Google の Web サービス，Salesforce CRM[2] など

PaaS: Platform as a Service
: インターネット経由でアプリケーション実行プラットフォームを提供．例として Google App Engine[1] など

HaaS/IaaS: Hardware (Infrastructure) as a Service
: インターネット経由で，計算リソースやストレージなどのハードウェアリソースを提供．例として Amazon EC2/S3 [6] [3] など

2.2.2 Grid Computing

Grid Computing は Cloud Computing という用語が登場する前から存在した分散コンピューティングの概念である．クラウド，グリッド及びクラスタなど用語の関係を図 1 に示す．横軸にある Application-Oriented とは，従来からある大規模演算など特定の計算でリソースを消費する，いわば CUI ベースのアプリケーション，Service-Oriented とは，Web2.0 などの Web ベースのアプリケーションを意味している．縦軸の Scale とは処理の規模，すなわちサーバ数や計算能力である [7].

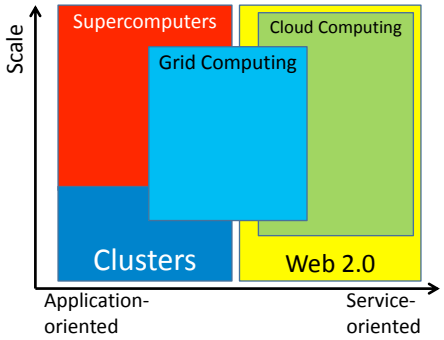

図 1: 分散コンピューティング概観

2.2.3 Surge Computing

Surge Computing[10] とは，企業が持つ社内のクラウドと，Google や Amazon が提供するようなパブリックなクラウドを，統合してプライベートクラウドとして活用するという概念である．Cloud Computing が普及してきた理由の 1 つに，自前の計算機リソースを用意する必要がないというものがあったが，ある一定以上の処理量になると自前で計算機リソースを用意したほうがコストが安くなる場合もある．既に社内にある計算機リソースは有効活用しつつ，処理能力が足りない場合などに社外のパブリッククラウドを利用することで，コストとパフォーマンスのバランスを保つことが出来る．

2.3 構成例 (Amazon EC2)

本節ではクラウド環境の例として，Amazon Elastic Compute Cloud (EC2)[6] の概要を述べる．Amazon EC2 の概観を図 2 に示す．Amazon EC2 は Amazon Web Services (AWS) [3] を構成するサービスの 1 つであり，Web 経由で制御可能な Xen ベースの VM を提供する．この VM はインスタンスと呼ばれ，イメージはストレージサービスである Amazon S3 (Simple Storage Service) に AMI (Amazon Machine Image) という形式で保存される．

インスタンスは 5 タイプの VM として起動することができ，それぞれ割り当てられる仮想 CPU，メモリ，ストレージの容量が異なり，1 仮想 CPU，メモリ 1.7GB，ストレージ 160GB，Linux の small タイプで 1 時間あたり 0.1 ドル，20 仮想 CPU，メモリ 7GB，ストレージ 1.7TB，

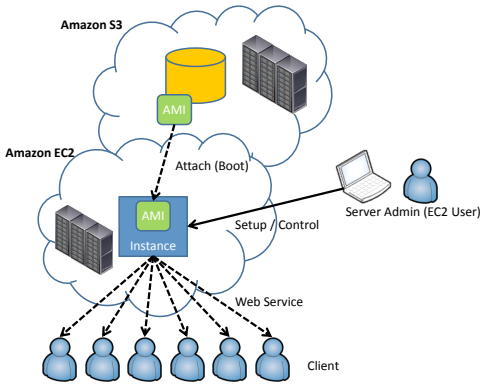

図 2: Amazon EC2

Linux の high-CPU extra Large タイプでも 1 時間あたり 0.8 ドルの従量制となっている．データ転送に関しても従量制で，In-coming で 1GB あたり 0.1 ドル，Out-going で 1GB あたり 0.17 ドル (月 10TB まで) が必要となる．また，オプションとして永続的なストレージを提供する Amazon EBS (Elastic Block Store) や ELB (Elastic Load Balancing) なども利用可能で，こちらも保存したデータ量や転送量に応じた従量制となっている．地理的に離れた場所へのマイグレーションは標準で利用可能であり，追加の費用は必要ない．

3 既存 VM 技術

本節では，Amazon EC2 で利用されている VM である Xen について，その概要とアーキテクチャについて述べる．

3.1 Xen

Xen [4] は Xensource が開発するオープンソースの Hypervisor である．2003 年に発表された論文 [4] で高いパフォーマンスが注目され，商用 Linux ベンダのサポートも受けながら現在も開発が進んでいる．その後，Citrix Systems に買収され商用製品 XenServer[16] も登場したが，オープンソースの開発も継続して行われている．

3.1.1 Xen のアーキテクチャ

Xen のアーキテクチャを図 3 に示す．Xen において VM は Domain と呼ばれる．Xen は Hypervisor タイプであるが，VMM 自身に管理機能を持たせず，Domain0 と呼ばれる特権を持つ VM を，Hypervisor 管理用の HostOS のような存在として利用している．また，GuestOS を DomainU と呼ぶ．

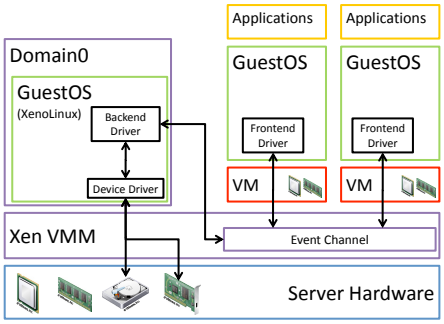

図 3: Xen のアーキテクチャ

GuestOS からの I/O リクエストは，Xen VMM の Event Channel 経由で Domain0 上の Linux の Backend Driver に転送される．Backend Driver はリクエストをデバイスドライバに渡し，物理的なディスク，ネットワークへのアクセスが行われる．このような構成を取っているのは，デバイスドライバのサポートを Domain0 の OS に任せることができ，Hypervisor を小型化できるからである．Domain0 で動作する OS は，準仮想化と呼ばれる，カーネル部分を Xen 対応に書き換えられた Linux などであり，Linux カーネルでサポートされているほぼ全てのハードウェアが利用できるというメリットがある．Hypervisor の小型化は，オーバーヘッドの削減と，攻撃対象となる部分を減らすことに貢献している．

元々コードの大半を Linux から流用している関係で Linux との親和性が高く，GuestOS の準仮想化カーネルコードが最近 Linux のメインラインカーネルに統合された．他にも NetBSD，FreeBSD，Solaris 等が Xen の準仮想化カーネルを持つ．また，Live Migration をサポートしており，共有ディスクを持つサーバ間を無停止で移動できる．VMware vMotion [14] と違い標準機能であり，追加ライセンス費用が必要無い点が異なる．

3.1.2 リソース制限機能

Xen では Domain(Domain0 および DomainU) 毎にリソース設定が可能である．以下に各リソース毎の制御法を述べる．

CPU:
: Domain ごとに仮想 CPU の数，仮想 CPU と物理 CPU のマッピング，利用率のしきい値，スケジューリング優先度を設定可能である．設定は，Domain 設定ファイル (デフォルトでは/etc/xen/に格納されている) に静的に書き込む方法や，稼働中の Domain に対しては，xm コマンドなどを用いて動的に設定変更が可能である．xm コマンドの発行自体は管理者が手動で行う必要がある．

メモリ:
: メモリに関しては，割り当てるメモリ量と，割り当て可能な最大値を Domain ごとに設定できる．稼働中の Domain についても，Domain0 上で xm コマンドなどを用いて，または商用製品の XenServer の管理画面から動的に変更が可能である．しかし VMware のような高度なメモリ管理機構は持っておらず，メモリのオーバーコミットなども不可能である．

ディスク, ネットワーク:
: ディスクやネットワーク等の I/O に関してのリソース制限は，Hypervisor の機能としては持っていない．しかし，これらのトラフィックは Domain0 を通過し，かつ Domain0 上で動作している OS は Linux であるので，リソース制御を行うモジュールの開発も自由に行えるというメリットもある．実際に，Domain0 の Device Mapper のレイヤで，GuestOS のディスク I/O 帯域保障を行う dm-ioband[5] の開発が行われている．

4　セキュリティに関する考察

本章では，クラウド環境で利用される VM について，セキュリティの要素について考察する．

4.1　リソース不足によるサービス不能

VM に対して外部から DoS 攻撃などが行われ，サービス不能となる場合が考えられる．また，VM 上で動作している OS がマルウェアに感染し，計算機リソースを食いつぶしたり，踏み台として他の VM へ攻撃を仕掛けることも十分に考えられる．このような攻撃に対しては，リソースを求めてマイグレーションする，もしくは攻撃されてリソースを浪費している VM へのリソースの提供を絞る，そもそもの攻撃パケットをファイアウォールで防ぐなどの対処法が考えられる．

VMware では，VMsafe と呼ばれる API を主なセキュリティベンダーにライセンシングし，Hypervisor レイヤで VM のメモリや I/O，プロセスを監視し，マルウェアによる被害を防ぐ製品の開発を推進している [12]．また，vSheild Zones[15] によって従来 VM 上の OS 毎に構築を行っていたファイアウォールを統合し，透過的にフィルタリングする．但しこれらは現状 VMware でしか使用できず，他の Hypervisor 向けには別の実装が必要となる．

4.2　Hypervisor に対するマルウェア

マルウェアは OS の脆弱性を利用して管理者権限の乗っ取り，データの盗聴・改ざんなどを行ってきたが，Hypervisor もソフトウェアである以上，マルウェアの攻撃対象になり得る．実際に 2009 年に英 VAserv 社の VM サーバインフラが zero-day 攻撃を受け，ホスティングしていた 10 万の Web サイトが消滅するという事件も発生している [11]．実際に攻撃を受けていなくても，脆弱性の対策には Hypervisor および VM の再起動が必要になる場合もあり，この場合はホスティングしている全てのサービスが一斉停止を余儀なくされる．

TPM (Trusted Platform Module) デバイスなどを活用することによって信頼の連鎖を作り，完全に信頼されたソフトウェアしか起動させない研究も行われている [8].

4.3　ネットワークの認証と暗号化

VM とクライアントまたは VM 間での通信は従来のネットワークとほぼ同じであるが，Web ベースでのやりとりが主となるため，現在通信している相手が正規の通信相手であるかを確認・認証する技術はこれまで以上に重要なものとなる．また，VM のマイグレーションに関して，メモリデータが暗号化されずにネットワークを流れるので，中間者攻撃を受ける可能性があることが指摘されている [9]．これに関して VMware および Xen は，性能上の問題を理由に，マイグレーション専用に L2 的に隔離されたネットワークもしくは暗号化アプライアンスの利用を推奨しているが，本来ならば Hypervisor の機能としても持つべきものであると考える．

4.4　データセンター規模の障害

電源トラブル，火災などデータセンター単位での障害が発生する可能性もある．VM を利用してリソース集約等を行っている場合はより被害が甚大になる可能性がある．クラウド環境であるならば，こういった大規模かつ地域的な障害についても隠蔽されるべきである．

VM を利用する場合，遠隔地へのバックアップ，スナップショット作成や，VM のマイグレーションのサポートによってある程度影響を抑えることができる．遠隔地でのディスク同期 [18] や，NEMO を用いたマイグレーション [19]，VMware Storage vMotion[13] 等の技術を組み合わせることで遠隔地へのマイグレーションは可能になると思われるが，現状では帯域やジッタに大きく左右されると推測できる．

4.5　インターオペラビリティ

サーバの構成やメーカーの差を VM で吸収することはできたが，今度は異なる Hypervisor 間での互換性の問題が発生する．例えば，VMware で構成した VM をそのまま Xen で動作させることは不可能である．VM 間でのインターオペラビリティが確保されれば，前述した Hypervisor

の脆弱性の問題を他の Hypervisor 上に移動させることで一時的に回避できる可能性がある．

VM 間でのバイナリ互換性の確保や，統合管理が可能な VM 管理ツールなどの開発を行う必要があると考えられる．

5 おわりに

Cloud Computing という新たな計算機環境の普及により，ユーザはインターネット経由で様々なサービスを利用することが可能になった．Cloud Computing の構成要素はこれまでの分散コンピューティング技術の組み合わせであるが，SaaS プロバイダを通じて一般ユーザへの普及が進んだという点で異なる．しかしながら，そのクラウド基盤を支えている VM 技術はセキュリティにおいて完全とは言えない部分がいくつかあり，今後のクラウド基盤の安全性に影響を与える可能性は否定できない．

5.1 今後の課題

クラウド環境のベースとなる VM へのセキュリティフレームワークの適用が挙げられる．このフレームワークは異種 Hypervisor へ対応可能で，各機能はモジュール化されている．ある 1 つのシステム向けに開発されたセキュリティモジュールが別のシステムでも適用可能なように設計される．これは脆弱性への対応を Hypervisor のベンダに頼らなくても独自に対応可能とし，かつクラウドプロバイダやユーザにとって必要な機能のみを利用できるような構成を検討し，実証検証を実施する予定である．

参考文献

[1] Google App Engine. http://code.google.com/intl/ja/appengine/.

[2] Salesforce CRM. http://www.salesforce.com/jp/.

[3] Amazon Web Services. http://aws.amazon.com/.

[4] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *the 19th ACM Symposium on Operating Systems Principles (SOSP '03)*, December 2003.

[5] dm-ioband. http://people.valinux.co.jp/řyov/dm-ioband/.

[6] Amazon Elastic Compute Cloud. http://aws.amazon.com/ec2/.

[7] Ian Foster, Yong Zhao, Ioan Raicu, and Shiyong Lu. Cloud computing and grid computing 360-degree compared. Dec 2008.

[8] Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, and Dan Boneh. Terra: a virtual machine-based platform for trusted computing. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP '03)*, pp. 193–206, New York, NY, USA, 2003. ACM Press.

[9] Farnam Jahanian Jon Oberheide, Evan Cooke. Empirical Exploitation of Live Virtual Machine Migration. Technical report, Electrical Engineering and Computer Science Department. University of Michigan, Feb 2008.

[10] Above the Clouds: Surge Computing / Hybrid Computing. http://berkeleyclouds.blogspot.com/2009/05/surge-computing.html.

[11] Webhost hack wipes out data for 100,000 sites. http://www.theregister.co.uk/2009/06/08/webhost_attack/.

[12] VMware VMsafe. http://www.vmware.com/technology/security/vmsafe.html.

[13] VMware. Storage vMotion. http://www.vmware.com/files/jp/pdf/storage_vmotion_datasheet.pdf.

[14] VMware. vMotion. http://www.vmware.com/pdf/vmotion_datasheet.pdf.

[15] VMware vShield Zone. http://www.vmware.com/products/vshield-zones/.

[16] Citrix XenServer. http://www.citrix.com/xenserver/.

[17] セキュア・プラットフォーム推進コンソーシアム. 平成２０年度「セキュア・プラットフォームに関する技術動向調査報告書」. 調査報告書, 社団法人 電子情報技術産業協会 (JEITA), March 2009.

[18] 広渕崇宏, 小川宏高, 中田秀基, 伊藤智, 関口智嗣. 仮想クラスタ遠隔ライブマイグレーションにむけた仮想計算機ストレージの透過的再配置機構の評価 (クラスタとグリッド技術). 情報処理学会研究報告. [ハイパフォーマンスコンピューティング], Vol. 2008, No. 99, pp. 7–12, 2008.

[19] 島慶一. NEMO BS を用いた Xen ゲスト計算機のオフリンクライブマイグレーション. Technical report, WIDE Project, Sep 2009.