4-2 仮想マシンのライブマイグレーションによるDDoS攻撃の抑止・防御システムの構築

4-2 A Load Balancing System for Mitigating DDoS Attacks using Live Migration of Virtual Machines

安藤類央　三輪信介　門林雄基　篠田陽一
ANDO Ruo, MIWA Shinsuke, KADOBAYASHI Youki, and SHINODA Yoichi

要旨

近年のプロセッサの性能の劇的な向上は、一つの物理マシンに複数の OS を仮想的に稼動される技術を再び実用的なものにした。とりわけ、ライブマイグレーションと呼ばれる稼動中の OS を動的に他の物理マシンに移動する技術は、資源利用の効率化、負荷分散などに対して有効である。

本稿では、この仮想マシンのライブマイグレーションを用いて、DoS（Denial of Service：サービス不能）攻撃に対する抑止・防御システムの構築について述べる。同システムでは、仮想マシンモニタというソフトウェアを用い、DoS 攻撃の検出のために、仮想化された OS の修正を行う。次に、ライブマイグレーションによる対応策について解説する。

Recently, rapid advances of CPU processor make it possible to provide illusion that several operating systems is running at the same time, in multiplex way. Particularly, transferring virtualized OS technology called live migration, which moves virtual machine from one physical machine to another is promising technology for effective resource utilization and load balancing.

In this paper we propose a system for mitigating and protecting DoS (Denial of Service) attacks using live migration of virtual machine. In proposed system, we apply virtual machine monitor and modify the operating system which is virtualized. Then, we illustrate the detailed countermeasure for DoS attacks using live migration.

[キーワード]
仮想化技術，セキュリティ，サービス不能攻撃，ライブマイグレーション，負荷分散
Virtualization technology, Security, Denial of service attacks, Live migration, Load balancing

1 はじめに

近年のプロセッサの性能向上は、複数の OS（オペレーティングシステム）を同時に走らせる仮想化を可能にした。特に、1960 年代のメインフレームの時代に用いられた仮想マシンモニタは、ここ数年のプロセッサ技術の刷新により、再び実用化されることとなった。仮想マシンモニタは、資源利用の効率化、負荷分散、ディザスタリカバリ、そして電力消費の削減などの効果があり、本論文では、仮想マシンモニタを用いて、近年、情報通信インフラストラクチャに深刻な影響を及ぼしている DoS（Denial of Service：サービス不能）攻撃に対する抑止、防御システムへの適用について述べる。

2 仮想化技術

仮想化とは、広義には、ソフトウェアから見える論理的なコンピュータ資源と、物理的なコンピュータ資源の対応を、多対一にする技術であると言える。電子回路でいうマルチプレクサを、ソフトウェアのレイヤで行っていると言える。ここ数年のプロセッサの性能、特にクロックスピードの劇的な向上によって、ソフトウェアから見て、複数のオペレーティングシステム

を同時に走らせているという仮想状態を提供することを可能にした。

2.1 構造による分類

仮想化技術は、仮想化がどのレイヤで行われているかによって分類することができる。仮想化技術の構造に分類は以下がある。

- 物理パーティション：ハードウェアを物理的に分離し、複数の OS を載せたものである。同時に OS を稼動させることはできないが、一つのシステムの障害や管理は、他のシステムにまったく影響しない。
- 論理パーティション：物理的パーティションとほぼ同じだが、パーティションモニタによってシステムを分離する。物理パーティションと同じく独立性が高い。
- 仮想マシン（OS）：OS 上においてハードウェアのエミュレーションと OS の仮想化を行う。CPU、メモリ、デバイスなどはすべて OS 上で仮想化される。
- ホスティング：リソースモニタを用いてアプリケーションごとに CPU、メモリ、デバイスなどの資源を割り当てる。独立性は低いが集約度は高い。
- 仮想マシンモニタ：仮想マシンのオーバーヘッドを低減するため、ハードウェアと OS の間に位置する点が、仮想マシンと異なる。リソースの変更が可能であり、ハードウェアの近くに位置するので独立性が高い。

仮想マシンモニタ成功の理由は次の 2 点がある。(1) ホスト OS にデバイスドライバの一元管理を行わせることで、ゲスト OS のドライバの実装と運用を容易にしたこと。(2) プロセッサベンダが完全仮想化という仮想マシンモニタ用の機能を提供したことで、仮想マシンモニタの実装と運用が容易になったこと。

仮想マシンと仮想マシンモニタは、個人的な用途としての効果としては大差がないが、サーバなどの負荷やオーバーヘッドが問題になる場合は、仮想マシンモニタの利用が有効であると考えられる。

2.2 稼動レイヤ・インストラクションセットによる分類

仮想化技術には、稼動レイヤ・インストラクションによる分類が可能である。稼動レイヤは、アプリケーションとシステムの二つに分けることができる。アプリケーションレイヤでは、マルチプログラミング、中間言語、バイナリトランスレーションなどがある。システムレイヤでは、デバイスや OS が仮想化される、仮想マシン、仮想マシンモニタなどがこれにあたる。

アプリケーションレベルの仮想マシン

- 同一のインストラクションセット：アプリケーションにことなるリソースを割り当てるマルチプログラミング
- 異なるインストラクションセット：JAVA などの中間言語、バイナリトランスレーション、ユーザモードの QEMU など

システムレベルの仮想マシン

- 同一のインストラクションセット：VMWARE GX、XEN、KVM などの仮想マシンモニタがこれにあたる。
- 異なるインストラクションセット：CPU を全部仮想化し、異なるインストラクションセットに対応する。QEMU、MAC をエミュレートする VIRTUAL PC などがこれにあたる。

現在負荷分散やデバッグなどで開発が進んでいるのが、システムレベルで同一のインストラクションセットを仮想化する技術である。

2.3 仮想マシンモニタ

仮想マシンモニタとは、ハードウェアとオペレーティングシステムの間に位置し、仮想化したハードウェアをオペレーティングシステムに提供する。通常は、仮想マシンモニタ上で複数のシステムが稼動することが可能である。近年のプロセッサの性能の劇的な向上により、仮想的に同時に複数のオペレーティングシステムが稼動させることが可能である。ハードウェアとオペレーティングシステムの間に位置するため、一つのオペレーティングシステムに不具合が生じても、他のシステムには影響を及ぼすことがなく、頑健な稼動環境を提供することができる。また、ハードウェアを直接エミュレーションし

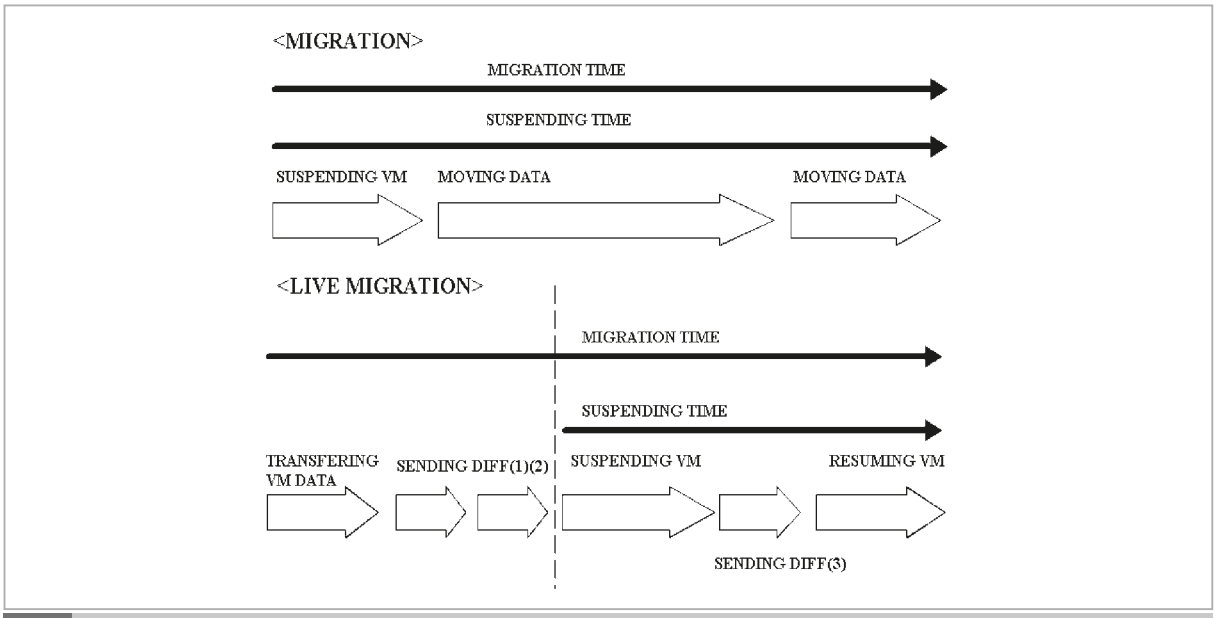

図1 ライブマイグレーション

ているため、オペレーティングシステムに割り当てる資源を動的に変更することができる。

3 ライブマイグレーション

仮想マシンのマイグレーションとは、稼動中の仮想マシンを、一つの物理マシンから他の物理マシンに移動させるものである。詳細には、ハードディスクを共有しつつ、一つの物理マシンのメモリ状態を他のマシンに稼動される。通常のマイグレーションでは、一度全メモリの状態を記憶してから転送するため、転送中には、仮想マシンが提供するサービスの応答が中止される時間がある。これに対し、ライブマイグレーションではスナップショットの差分を転送するため、通常のマイグレーションに比べ、転送中に仮想マシンのサービスの中止時間を小さくすることができる。

4 サービス不能攻撃の防止・抑止への適用

本節では、仮想マシンの移行技術による、サービス不能攻撃の防止・抑止への適用を述べる。第一には、脆弱性を利用した攻撃について、あるアドレスに対応した同一サービスを提供する目的で、システムの移行する方法、第二に、防御法としての負荷分散に適用する方法について述べる。

4.1 サービス不能攻撃

サービス不能攻撃（DoS：Denial of Service Attack）とは、悪意のあるユーザ（ノード）が、帯域（ネットワーク資源）の浪費、CPU やメモリ（サーバ資源）の浪費、そして脆弱性攻撃などを多発させ、対象となったサーバのサービスを停止させるものである。情報通信セキュリティにおいて、DoS 攻撃は恒常的に問題となっており、防御側は、負荷分散装置、ロードバランサーで対応する場合が多い。本論文では、仮想マシンモニタのライブマイグレーションを用いた防御システムを提案する。ライブマイグレーションを用いることで、より高粒度な負荷分散が可能になり、提案システムは特に脆弱性攻撃よるDoS に対して有効である。

4.2 DoS攻撃に対する防御

本節では、ライブマイグレーションを用いたDoS 攻撃に対する抑止、防御法について述べる。図 2 は、HA（High Availability）クラスタ上に構築したサービスを、複数の仮想マシンで負荷分散したものである。ここで、VM 1-1 と VM 2-1 は、VM 3-1 と VM 4-1 に比べ少ない資源が割り当てられており、VM 2-1 に DoS（サービス不

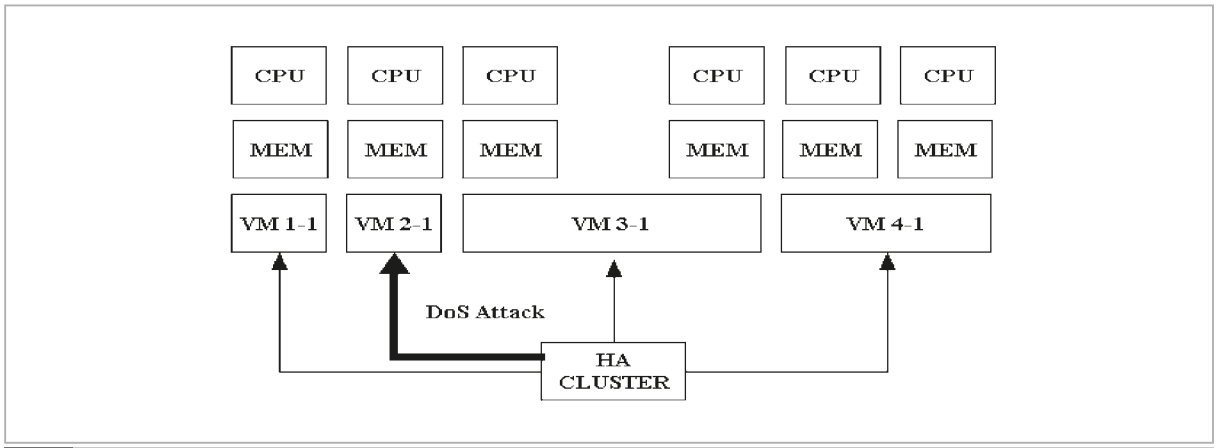

図2 攻撃前のバランサーの状態

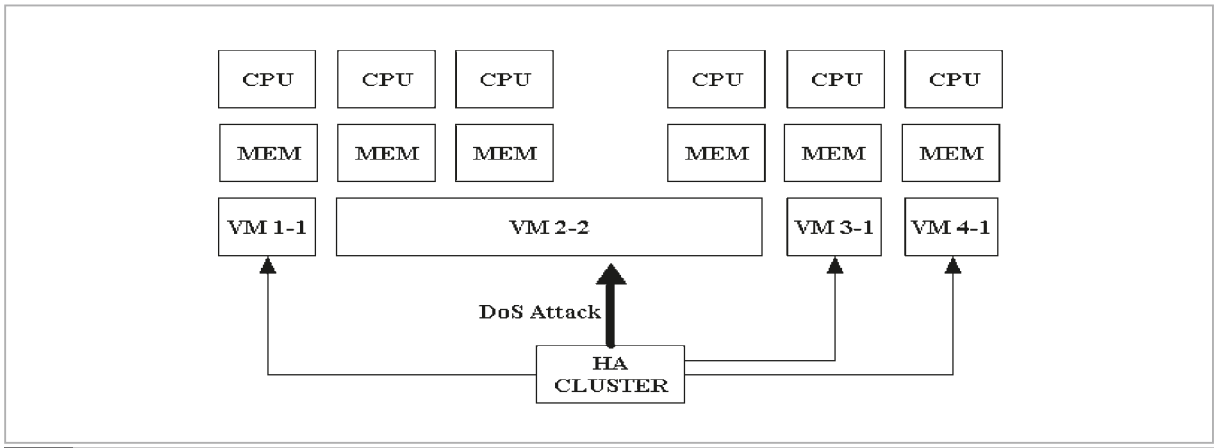

図3 攻撃後のバランサーの状態

能）攻撃がかけられているとする。

攻撃後の抑止システムを図 3 に示す。ライブマイグレーションを用いて、DoS 攻撃を受けている VM 2-2 に多い資源を割り当てる。これにより、VM 2-2 に意図的にかけられている高負荷にミッションクリティカルなサービスが影響を受けることなく、攻撃を抑止することができる。

また、特定の脆弱性を利用した DoS 攻撃に対しては、仮想マシンのバージョンを入れ替えることによる回避が可能である。また、動的なフィルタリングルールの適用も可能であると想定される。

5 まとめ

近年のプロセッサの性能の劇的な向上は、一つの物理マシンに複数の OS を仮想的に稼動される技術を再び実用的なものにした。近年のプロセッサの性能向上は、複数の OS（オペレーティングシステム）を同時に走らせる仮想化を可能にした。特に、1960 年代のメインフレームの時代に用いられた仮想マシンモニタは、ここ数年のプロセッサ技術の刷新により、再び実用化されることとなった。とりわけ、ライブマイグレーションと呼ばれる稼動中の OS を動的に他の物理マシンに移動する技術は、資源利用の効率化、負荷分散などに対して有効である。

本稿では、この仮想マシンのライブマイグレーションを用いて、DoS（Denial of Service: サービス不能）攻撃に対する抑止・防御システムの構築について述べた。同システムでは、仮想マシンモニタというソフトウェアを用い、DoS 攻撃の検出のために、仮想化された OS の修正を行う。負荷分散ソフトウェア（バランサー）とライブマイグレーションによる、DDoS 攻撃の抑止・防御システムの概要を示した。

参考文献

1 C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live Migration of Virtual Machines, In 2nd USENIX Symposium on Networked Systems", Design and Implementation(NSDI 05), p.273286, May 2005.

2 安藤類央，門林雄基，篠田陽一，“KVM を用いた完全仮想化上のインシデント駆動型チェックポインタの実装”、情報処理学会コンピュータセキュリティシンポジウム 2007、第 38 回研究報告 2007年11月2日.

3 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Incident-Driven Memory Snapshot for Full-Virtualized OS Using Interruptive Debugging Techniques", ISA 2008 The 2nd International Conference on Information Security and Assurance, Apr. 2008, Busan, Korea.

4 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Asynchronous nortification channel for exploitation-robust secure OS on virtual machine monitor", The 2nd Joint Workshop on Information Security, Aug. 2007, Tokyo, Japan.

5 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Asynchronous Pseudo Physical Memory Snapshot and Forensics on Paravirtualized VMM Using Split Kernel Module", ICISC 2007, The 10th International Conference on Information Security and Cryptology, Nov. 29-30, Seoul, Korea.

6 Nguyen Anh Quynh, Ruo Ando, and Yoshiyasu Takefuji, "Centralized Security Policy Support for Virtual Machine", USENIX, 20th Large Instllation System Administration Conference, Dec. 3-8, 2006 Washington, D.C.

7 Greg Goth, "Virtualization: Old Technology Offers Huge New Potential", IEEE Distributed Systems Online, Vol.8, No.2, 2007.

8 Paul A. Karger, Mary Ellen Zurko, Douglas W. Bonin, Andrew H. Mason, and Clifford E. Kahn, "A Retrospective on the VAX VMM Security Kernel", IEEE Trans. Software Eng.17(11): pp.1147-1165, 1991.

9 Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield, "Xen and the art of virtualization", In Proceedings of the 19th Symposium on Operating System Principles (SOSP 2003), Bolton Landing, NY, Oct. 2003.

10 Tal Garfinkel and Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", In the Internet Society’s 2003, Symposium on Network and Distributed System Security (NDSS), pp.191-206, Feb. 2003.

11 Nguyen Anh Quynh, Ruo Ando, and Yoshiyasu Takefuji, "Centralized Security Policy Support for Virtual Machine", USENIX, 20th Large Installation System Administration Conference, Dec. 2006.

12 Uhlig, R, Neiger, G, Rodgers, D, Santoni, A. L, Martins, F. C. M, Anderson, A. V, Bennett, S. M, Kagi, A, Leung, F. H, and Smith, L, "Intel Virtualization Technology", IEEE Computer Vol.38, Issue 5, pp.48-56, May 2005.

安藤類央（あんどうるお）
情報通信セキュリティ研究センター トレーサブルネットワークグループ研究員　博士（政策・メディア）
ネットワークセキュリティ、ソフトウェアセキュリティ

三輪信介（みわしんすけ）
情報通信セキュリティ研究センター トレーサブルネットワークグループ研究員　博士（情報科学）
ネットワークセキュリティ

門林雄基（かどばやしゆうき）
情報通信セキュリティ研究センター トレーサブルネットワークグループ客員研究員　博士（工学）
ネットワークセキュリティ

篠田陽一（しのだよういち）
情報通信セキュリティ研究センター長
工学博士
ネットワーク、次世代インターネットアーキテクチャ