サイエンティフィック・システム研究会
2007 年度システム技術分科会第 2 回会合資料　　2008 年 1 月 30 日

# 仮想化技術の現状と方向性

産業技術総合研究所　須崎有康

## ■アブストラクト

現在、盛んに開発が進められている仮想化技術について Xen, KVM (Kernel-based Virtual Machine)などの個々の仮想化ソフトウェアの実装技術や CPU に付加された仮想化対応機能などの現状を紹介する。また、仮想化技術が新たに開拓するセキュリティ、組み込み、OS マイグレーションについても取り上げ、今後の仮想化の方向性を紹介する。

## ■ 概要

### 1. 歴史

仮想マシンの開発は IBM CP/67 や IBM 370/VM をはじめとするメインフレームより始まった。この時代は仮想化支援のためのハードウェアがあり、ハード・ソフト一体の開発であった。この状況で 1974 年に Popek ,Goldberg が「仮想化の命令要件」[1]を発表するに当たり、仮想化のために必要となる命令セットが明確にあった。

現在の PC に標準装備されている CPU IA32 (32bit Intel Architecture)は非力であり、かつ個人利用のみのため仮想化を想定していなかったが、その能力向上と共に複数の OS 起動のために仮想化技術が開発されるようになった。IA32 では仮想化を想定していないため、命令セットに非特権のセンシティブ命令(CPU の真の姿が見えてしまう命令、あるいは以後の実行に影響を与える命令)を含み、仮想化を困難にしていた。

この問題を克服して最初に PC 上での仮想化の有効性を示したのは 90 年代後半の VMWare Workstation(主要開発者は Stanford 大学の Mendel Rosenblum)である。VMware ではセンシティブ命令などを動的に置き換える技術である“Dynamic Translation”[2]を開発し、OS の変更なしに効率的に複数起動を可能にした。

Dynamic Translation とは異なるアプローチとして、Cambridge 大学の Ian Pratt を中心に 2000 年初頭から“Para-Virtualization”が開発された[3]。Para-Virtualization では、仮想化される OS 自体に修正を加え、仮想化に問題がある処理は HyperVisor に依頼する。HyperVisor は OS と CPU の間の低レベルに位置し、OS 毎に仮想的な PC 環境を提供する。

これらの仮想化ソフトウェアの開発と平行して、IA32 での仮想化の問題点が明らかになってきた。Robin ,Irvine は仮想化のための IA32 命令要件[4]を発表した。また、Intel と AMD では、HyperVisor 作成を支援するため、特権レベルとは別に新たなモード(Intel では root/non-root、AMD では host/guest)を付加し、仮想化の障害になる命令を実行した場合にモード切替を起こす仮想化支援を加えた。

### 2. 今後の方向性

仮想化技術の開発は、セキュリティ強化を中心に OS の一括管理や組込み分野も適用されるようになった。セキュリティでは VM による隔離(isolataion)を用いて同一 CPU 内で複数の OS のセキュリティが他に影響しないため、サーバ集約を加速させた。組込み分野としては ARM 用(ARM 社開発の Acorn RISC Machine)の Xen を Samsung や MontaVista で開発されており、セキュリティの強化を目指している。

また、仮想マシンは仮想ディスクファイルを起動イメージとして利用するため、ソフトウェアをインストールした仮想ディスクファイルを配信することで各 PC 毎のインストールの手間を削減する。但し、仮想ディスクファイルは大規模になるため、更新が起こった場合にその差分だけ管理する方式が必要になる。この管理手法としては、Stanford 大学の Collective[5]、Moka5 の LivePC、産総研の OS Circular[6]などの研究開発が進んでいる。

### References

[1] G.J.Popek and R.P.Goldberg , “Formal Requirements for Virtualizable Third Generation Architectures”, CACM 17 (7): 412 -421. (1974).
[2] US Patent : 6,397,242, Virtualization system including a virtual machine monitor for a computer with a segmented architecture
[3] P.Barham, et.al., “Xen and the Art of Virtualization”, SOSP (2003).
[4] J.S.Robin and C.E. Irvine, ″Analysis of the Intel Pentium’s Ability to Support a Secure Virtual Machine Monitor″. USENIX Security Symposium. (2000)
[5] R.Chandra, et.al., ″The Collective: A Cache Based System Management Architecture,″ (NSDI’05), Boston, (2005).
[6] K.Suzaki,et.al., OS Circular: Internet Client for Reference , USENIX LISA 07.