ノートPCの仮想化を実現するエンジン vRAS™ と応用ソフトウェア SV-PC™

vRAS™ Personal Computer Virtualization Engine and SV-PC™ Application Software

中嶋　宏　　嘉村　幸一郎
■ NAKAJIMA Hiroshi　■ KAMURA Koichiro

異種のオペレーティングシステム（OS）とアプリケーションが動作する環境を一つの物理コンピュータ上で動作させることができる，仮想化技術の利用がサーバなどで進んでいる。ノートPC（パソコン）でも，ハードウェア性能の向上により仮想化技術が利用され始めている。

東芝は，クライアント環境の機能と性能を維持しながら，仮想サーバ環境をノートPC上で同時に動作できる仮想化エンジンvRASを開発するとともに，これをベースにしたソフトウェア製品SV-PCを開発した。SV-PCを導入することにより，ノートPCのセキュリティの強化と運用管理性能の大幅な向上を実現できる。

In recent years, virtualization technologies that can simultaneously run multiple operating systems (OSs) in a computer have been employed in server products.　Hardware-assisted virtualization technologies are also being embedded in many notebook PCs, giving them the capability to run multiple OSs.

To enhance manageability and security in PCs, Toshiba has developed the vRAS PC virtualization engine that can run client and server OSs simultaneously, as well as the SV-PC application software that provides new solutions enabling PC managers to maintain PCs efficiently and prevent the leakage or loss of important data from PCs using vRAS.

1　まえがき

サーバなどのシステムでは，コンピュータの物理資源（ハードウェア）を仮想化して，同一物理マシン上で，OSやアプリケーションを含む環境を複数同時に実行する仮想化が普及している。また，PCのハードウェア性能の向上に伴い，仮想化ソフトウェアがOSに搭載されるような，PCなどのクライアント環境の仮想化も一般で利用され始めている。

このような状況のなかで東芝は，同一PC上で，Windows®(注1)などのクライアント環境と仮想サーバ環境を，性能や機能を損なわずに同時に実行できる仮想化プラットフォーム“仮想化エンジンvRAS”を開発した。ここでは，vRASの特長と，これを応用したソフトウェア製品“SV-PC”について述べる。

2　vRAS

vRASは，同一PC上で，クライアント環境のOSとアプリケーションを通常のPCと同様の機能と性能で動作させながら，仮想サーバ環境のサービスOSとサービスアプリケーションをバックグラウンドで同時に動作させることができる，ハイパーバイザ型の仮想化ソフトウェアである（**図1**）。

2.1　vRAS でのPC仮想化の利点

PCをvRASで仮想化することには，次のような利点がある。

(注1)，(注3)　Windows，Active Directoryは，Microsoft Corporationの米国及びその他の国における商標又は登録商標。

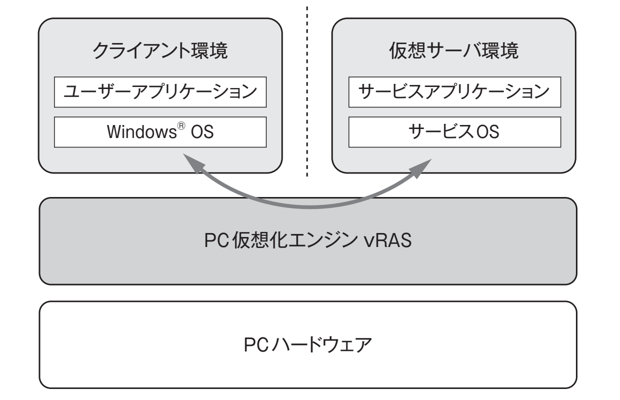

図1. vRASによるPC仮想化 ― vRASにより，クライアント環境と仮想サーバ環境それぞれの仮想マシンが，一つのノートPC上で同時に動作する。
Virtualization by vRAS

(1)　クライアント環境の完全分離によるセキュリティ強化

仮想化により，クライアント環境はPCハードウェア及び仮想サーバ環境から完全に分離される。仮想化した各環境（以下，仮想マシンと呼ぶ）から見えるデバイスはvRASで管理され，クライアント環境の仮想マシンからは，アクセス可能として定義されたデバイス以外はアクセスできず，デバイスの存在を認識できない。これは，実際のPCのハードウェア構成を参照するのではなく，vRASで仮想化したデバイス構成を参照しているからである。

応用として，データを多量にコピーされるおそれがある

USB (Universal Serial Bus) メモリや光ディスク装置 (ODD) などのデバイスを，仮想マシンから完全に遮蔽 (しゃへい) することが可能になる。セキュリティ対策ソフトウェアでは，これらをOSの機能やアプリケーション自身で実現しているが，ソフトウェアで構成されている以上，解除される可能性がある。しかしvRASでは，デバイス管理はクライアント環境の外にあることから設定変更や解除することができない。

また，保護したいデータを，仮想サーバ環境に置くことで，クライアント環境から直接操作することはできなくなり，別の物理マシン上に動作しているサーバに存在するデータと同様になる。

(2) クライアント環境の保守，管理が容易　　クライアント環境のユーザーアプリケーションとOSは，仮想マシンのイメージデータとして管理することで，バックアップ保存や障害時の復元が容易になる。後述のSV-PCでは，この仮想マシンイメージを配信することでシステムを実現している。

(3) クライアント環境の動作に影響しないバックグラウンドの仮想サーバによるサービス実行　　クライアント環境の仮想マシンが停止していても，仮想サーバは動作を継続できる。

(4) 同一マシン上での異種OSの同時実行　　一般的な仮想化の特長であるが，同一PC上で異なるOSを同時に実行できる。これにより，サービスアプリケーションに適したOSを利用できる。

2.2　デバイス パススルーによる仮想化

デバイスを仮想化する方式を**図2**に示す。従来の仮想化ソフトウェアでは，デバイスはソフトウェアでエミュレーションする方式で実現されている。そのため，仮想マシンから使用できるデバイスが一部に限られたり，仮想化しない場合に比べて入出力性能が大きく低下するという問題があった。したがって，ノートPCなどのクライアント環境でよく使用されるグラフィック表示，動画再生，及び操作時の応答性が要求されるアプリケーションには利用できなかった。しかし，今回開発したvRASでは，Intel社のハードウェアによる仮想化支援機能を利用して，ノートPCが持つ様々なデバイスのサポートや，仮想化による性能低下を最小に抑えることができる (**図3**)。

そのハードウェア仮想化支援機能の一つにIntel®(注2) VT-dがある。Intel® VT-dは，デバイスとメモリ間のCPUを介さないデータ転送 (DMA : Direct Memory Access) の物理アドレスを，個々の仮想マシン上の仮想物理アドレスにハードウェアで変換することができる。これにより，仮想マシンから直接デバイスを制御する“パススルー”方式が可能になった。

このパススルー方式は，一つのデバイスを複数の仮想マシンで共有することはできないが，性能がほとんど低下せず，また，クライアント環境のデバイスドライバがそのまま使用できる利点がある。

PCの多種多様なデバイスを仮想マシンから使用できるようにするとき，従来のように一つ一つのデバイスをソフトウェアエミュレーションする仮想化方式では，刻々と増えるデバイスに対応していくことが難しい。vRASでは，仮想化により各デバイスを抽象化することはせず，利便性と性能を重視し，一つの仮想マシンから様々なデバイスを直接使用できるように，ハー

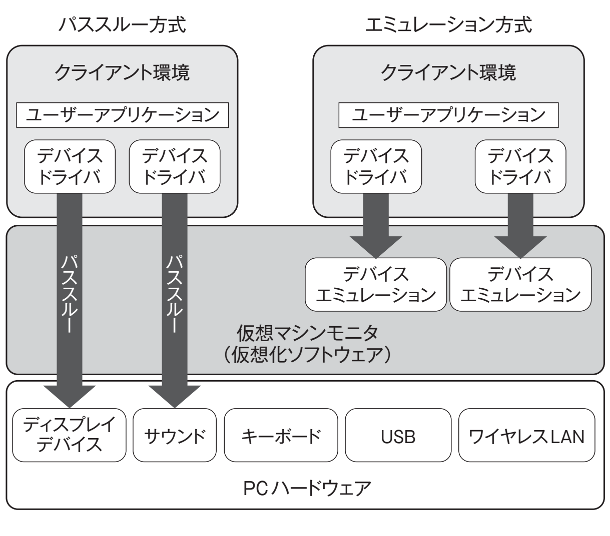

図2. デバイスの仮想化方式 ― エミュレーションは，ハードウェアの動作を仮想化ソフトウェアでエミュレートして実現するが，パススルーは実際のハードウェアデバイスを動作させる。

Device virtualization models

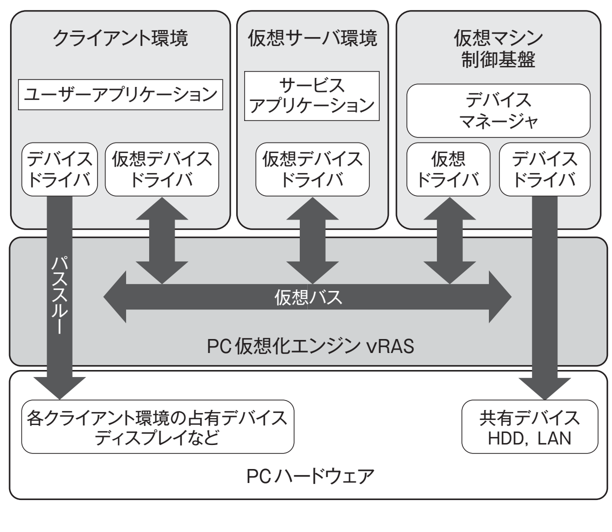

図3. vRASの構成 ― パススルーと仮想ドライバにより，仮想化しながらもPCの機能と性能を維持する。

Structure of vRAS

(注2)　Intelは，Intel Corporationの米国及びその他の国における商標又は登録商標。

一般論文

ドディスク装置（HDD）及びLANインタフェース以外はすべてパススルーするようにした。

2.3　共有デバイスの仮想化

複数の仮想マシンで共有するデバイス（HDDやLAN）に対して，クライアント仮想マシン上で動作する仮想デバイスドライバを開発した。仮想デバイスドライバは，ほかの仮想マシンと共有しながらデバイスにアクセスするためのドライバで，制御基盤と呼ばれる仮想マシンを管理するOSのバックエンドドライバである仮想ドライバと仮想バスで接続される。これにより，デバイス自体はソフトウェアで仮想化されているにもかかわらず，ハードウェアデバイスそのもののエミュレーションではないので，少ないオーバヘッドで実デバイスにアクセスできる。このため，共有するデバイスに対しても性能が向上した。

2.4　性能

仮想マシンから直接制御するデバイスに対する性能は，パススルー方式により従来のエミュレーション方式に比べ大幅に改善し，仮想化によるオーバヘッドは，仮想化されていないPCと比べて5％以下に抑えられた。また，共有デバイスに対する性能は，仮想デバイスドライバの導入により向上し，オーバヘッドは10％以下になった。

3　SV-PC

SV-PCは，PCのセキュリティを強化し，セキュリティ対策に伴って増加する運用管理負荷を軽減しながら，モバイルPCの利便性を維持することが可能なPC用ソフトウェア製品である。SV-PCはvRASを利用して，PCのシステム環境を均一化する“ワークグループデスクトップ”機能と，ドキュメントやメールデータなどPC上の重要なデータを保護する“My Docマネージャ”機能から構成される。

3.1　システム構成

一例として，SV-PCを社内LANで使用する場合のシステム構成を**図4**に示す。Active Directory®(注3)サーバと，SV-PCをインストールした複数のPCから構成される。これらのPCは社内LANなどの同一サブネットワーク上に接続される。イメージ作成用PCと管理サーバ用PCは管理者が利用し，一般のユーザーである社員はクライアント用PCを利用する。

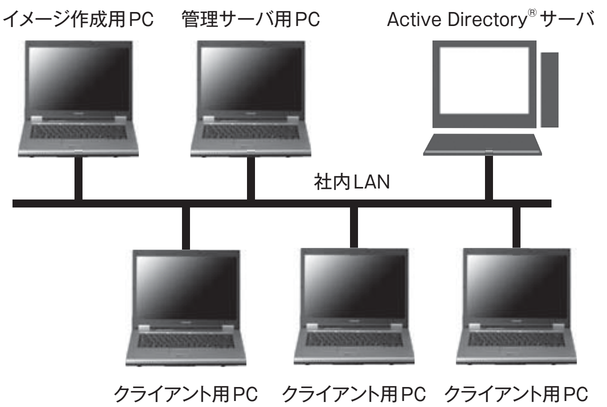

図4．SV-PCのシステム構成例 — 管理サーバ用，イメージ作成用，及びクライアント用のSV-PCを同一サブネットワーク上に接続し，管理サーバ用SV-PCからマスタイメージを配信する。

Example of SV-PC system configuration

図5．ワークグループデスクトップの画面 — 管理者はこの画面を使って管理下のPCのシステム環境を一元管理する。

Top display of Workgroup Desktop

3.2　PCのシステム環境の均一化

仮想化されたPC上では，OSとアプリケーションを含むPCのシステム環境をイメージデータとして扱うことが可能になる。これによって，PCのシステム環境の保守と管理が容易になる。

SV-PCのワークグループデスクトップ機能（**図5**）は，同じOSとアプリケーションを利用する部門や職種などのグループ単位にマスタイメージを作成し，このマスタイメージをグループ内の各クライアント用PCへ一斉に配信する。これにより，管理者がマスタイメージを更新することで，社員の使うクライアント用PCのシステム環境を更新し，均一化できる。

SV-PCでは，管理者がイメージ作成用PCで作成したマスタイメージを管理サーバ用PCにアップロードし，この管理サーバ用PCから各クライアント用PCへ配信する。管理サーバ用PC上で，管理者は配信のステータス確認をはじめ，クライアントの登録や，マスタイメージ管理，自動配信の設定，手動配信などをすることができる。

3.3　PC内のデータの漏えい防止

SV-PCでは，My Docマネージャ機能でPC内のデータを管理する。

My Docマネージャ機能では，仮想サーバ環境上に保管されたユーザーデータに対するセキュリティの強化と管理性能の向上を図った。そのポイントは，脅威の対象を悪意の第三者だけでなくエンドユーザーまで広げ，データの持出しを制御する機能を統合して提供している点である[1]。

vRAS上でユーザーが利用するWindows® の仮想マシンと管理者が利用する仮想サーバを同時に動かす。そして，**図6**に示すように，ユーザープロファイルやドキュメントなどのユーザーデータをWindows® のクライアント環境から分離して仮想サーバ環境上に配置し，ユーザー固有のデータに対する暗号化を行う。これによって，PC紛失時やHDD取外しによるデータの漏えい防止を実現した。

(1) PC内データのアクセス制御　My Docマネージャ機能では，Active Directory® にログオンできる社内LANの環境では，クライアント環境のWindows® 側から同一PC内の仮想サーバ環境へアクセスすることが許可され，ユーザーデータが利用できる。一方，Active Directory® にログオンできない社外の環境では，同一PC内の仮想サーバへのアクセスを禁じることにより，ユーザーデータを利用禁止にする。

(2) モバイルPCの利便性維持　PCのモバイル利用を実現するため，My Docマネージャ機能では，管理者による持出し制御機能を備えている。PCの持出し希望者は，持出し申請を行い，管理者から持出し許可とともに貸し出される期限制限付きの利用キーを使用することにより，期限内は外出先でユーザーデータを利用できる。

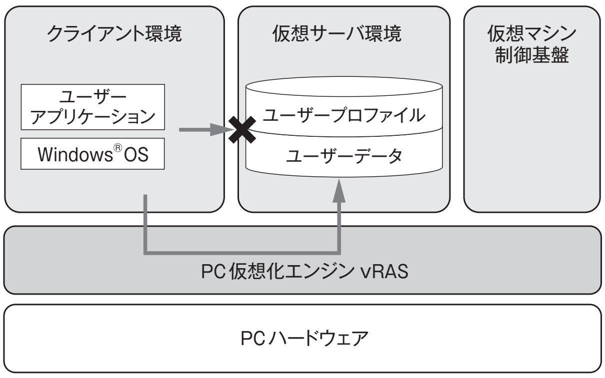

図6. My Docマネージャの仕組み ― 重要なデータをWindows® のクライアント環境から分離し，仮想サーバ環境上に保管して管理する。

Basic mechanism of My Doc Manager function

(3) 管理者によるユーザーデータ管理　管理者は，ネットワーク上に分散するSV-PCの仮想サーバ環境にあるユーザーデータへネットワーク経由でアクセスが可能であり，あたかも1台の物理サーバ上のデータにアクセスするように，各SV-PC上のユーザーデータの閲覧や共有設定などができる。

(4) PC内ユーザーデータの複製　仮想サーバ環境にあるユーザーデータを，PCのシャットダウン時に社内LAN上のファイルサーバやNAS (Network Attachment Storage) 上に複製することにより，ユーザーデータのバックアップとPC紛失時の情報特定を実現した。

4　あとがき

当社は，ノートPC上で仮想化を行うための仮想化エンジンvRASの開発に取り組み，この技術を，社内に分散するPCのセキュリティを強化し管理性を向上させるという目的に応用し，ソフトウェア製品SV-PCを製品化した。

今後も，vRASの応用技術を開発するとともに，更に市場ニーズに応えるため，SV-PCの機能の拡充を図っていく。

文　献

(1) 押切　洋．東芝のクライアント仮想化．すべてわかる仮想化大全2010．日経BP社，2009，p.226－229.

中嶋　　宏　NAKAJIMA Hiroshi
PC＆ネットワーク社 PC開発センター　サーバ・ネットワーク設計部主務。仮想化技術の応用ソフトウェア開発に従事。
PC Development Center

嘉村　幸一郎　KAMURA Koichiro
PC＆ネットワーク社 PC開発センター　サーバ・ネットワーク設計部主査。仮想化技術の応用ソフトウェア開発に従事。
PC Development Center