

# Xsigo I/O 仮想化による VMware 環境の最適化



「バーチャルマシンの可動性が、サーバ I/O 仮想化の必要性を促進しています」。

ジョン・ハンフリー  
(JOHN HUMPHREYS) 氏  
IDC Enterprise Virtualization  
調査プログラム 担当副社長

## サーバ仮想化のメリット

VMware ESX Server に代表される仮想化技術は、サーバ使用率の最大化にきわめて重要な役割を果たします。通常、データセンタの非仮想サーバの平均使用率はかなり低く、ガートナー社によれば 15% 未満とされています。OS の仮想化では、サーバ上で複数のオペレーティングシステムやアプリケーションの同時実行を可能にすることで使用率を劇的に高めます。

バーチャルマシンでは、サーバのメンテナンスを行う際にアプリケーションをオフラインにする必要がないため、ビジネス継続性が改善されます。ハードウェアの抽象レイヤーでバーチャルマシンを実行すると、サービス中断時間を限りなくゼロに近づけながら、1 つのサーバから別のサーバへアプリケーションを容易に移行することができます。

しかし何と言っても、最も重要なメリットはコスト面です。今日の I/O インフラは、単一のサーバ上で複数のアプリケーションを実行したり、サーバ間でアプリケーションを移行したりすることを前提に設計されていません。サーバのプロセッサの仮想化にはメリットがある反面、新たな課題も生み出します。この課題を解決するには、サーバの接続性を同時に仮想化することが最善の方法です。

## サーバ仮想化による I/O 問題

VMware ESX などの仮想化ソフトウェアは、プロセッサリソースの共有を容易にします。しかし、このモデルでは、サーバ I/O という別のリソースまでもが共有されてしまいます。既存の I/O インフラは従来型のサーバ使用を前提として設計されているため、この仮想化による新しい使用ケースでは、次のような I/O 問題が発生します。

**I/O ボトルネック**：バーチャルマシンが持つ動的性質と、サーバリソースの高い使用率により、サーバ I/O の負荷は大幅に増大します。トラフィック負荷の増大と、予期せぬトラフィックパターンは、アプリケーションの実行速度の低下を引き起こすことがあります。

最も単純な改善策は、単に I/O を増やす、すなわちイーサネットまたは FC 接続を追加することです。しかし、最近の 1U サーバやブレードサーバでは、利用できる I/O スロット数は制限される傾向にあります。これらのデバイスの多くは、1 個か 2 個の PCI-Express スロットを備え、例えばポートの総数は 4 個のイーサネットインタフェースと 2 個のファイバチャネルインタフェースに制限されてしまいます。これは従来の環境には適合しますが、4 ~ 20 のオペレーティングシステムを実行する仮想サーバ環境では、この接続数の制限が原因で I/O がパフォーマンスのボトルネックになることがあります。

**予測不可能なパフォーマンス**：複数のアプリケーションで共通のリソースを共有する場合、特定のアプリケーションのパフォーマンスを予測することはできません。非基幹アプリケーションが、より基幹的なタスクで必要となる帯域幅やプロセッサリソースを消費してしまうこともあります。VMware ESX はトラフィックシェイピングポリシーを提供しますが、これらのポリシーはハードウェアにオフロードされる必要があります。

「大規模フラットネットワーク」のセキュリティリスク：今日のストレージおよびネットワークセキュリティ技術は、バーチャルマシンの要求を満たすように設計されていません。今日、セキュリティは2つの方法で制御されています。1つ目は、最も確実なのは物理接続であるということ、すなわち接続する必要のないサーバを接続してはならないということです。

もう1つは、ネットワークおよびストレージアクセスのI/Oカードレベルでの制御です。I/Oカードの一意の識別番号を使用して、接続性を規則化することができます。これを行うには、たとえば、特定のI/Oカードに対してのみディスクアクセスを許可するようにストレージネットワークを構成します。このカードはワールドワイドに一意の固有名を持っており、他のカードは該当のストレージにアクセスできません。この結果、セキュリティは確保されます。

複数のVMで1セットのI/Oカードを共有した場合、このセキュリティは破壊されます。この場合、すべてのVMが同一のストレージリソースにアクセスする可能性があるためです。また、ユーザーがVMに可動性（VMotion イベントを介した移行機能を備えるなど）を求める場合、複数のサーバ全体でのアクセスを許可するには、構成を「opened up」にする必要があります。

極端なケースとして、任意のサーバに任意のVMを稼働させるための柔軟性が要求される導入パターンを想定します。

これを実現するには、システムが「フラットネットワーク」上に構成されており、完全にオープンストレージである必要があります。このケースでは、すべてのサーバがすべてのリソースへのアクセスを許可されることになり、セキュリティ管理の基本概念が危うくなるモデルです。

Cybertrustのセキュリティ専門家、A. ブライアン・サーティン氏は、企業が犯すセキュリティ上の失敗で最も多い3つのうち1つに「大型フラットネットワーク」を挙げています。それでもなお、この「大規模フラットネットワーク」は、バーチャルマシンの大規模導入を実現させるために一部の企業で採用されています。

### Xsigo はどのように役立つか

Xsigo I/O 仮想化コントローラは、サーバ仮想化によって生じるI/O問題に対応する仮想I/Oを提供します。仮想I/Oには、次のようなメリットがあります。

- パフォーマンスボトルネックを排除する容易に拡張可能な接続性
- きめ細かなQoSにより、特定のバーチャルマシン上で設計どおりのI/Oパフォーマンスを実現
- VMごとに専用I/Oリソースを割り当てるにより、セキュリティを確保
- 移行可能なI/Oにより、サーバ間でVMを移動してもセキュリティを維持

## 仮想 I/O で物理 I/O を置き換え

Xsigo は、仮想サーバに最適な接続を実現するために仮想 I/O を採用しています。Xsigo では、サーバの物理 I/O カード (NIC と HBA) を、仮想 NIC と仮想 HBA で置き換えます。

これらの仮想リソースは、アプリケーションによって物理カードとまったく同様に認識されますが、はるかに柔軟な管理が可能です。仮想 I/O には、次のようなメリットがあります。

- vNIC と vHBA を瞬時に実装できる。
- I/O 接続を追加した際にサーバの再起動が必要ない。
- 仮想 I/O リソースは、ハイパーバイザーによって物理カードと同様に認識される。
- VM は特定の I/O リソースと関連付けることができ、セキュリティを確保できる。
- 仮想 I/O は、物理サーバ間で移行可能。
- QoS 機能により、特定の VM に対して使用が許可される帯域幅を制御できる。

これらの特長により、バーチャルマシンの管理上の大きなメリットが得られます。

## Xsigo による I/O ボトルネックの排除

Xsigo では、より多くの帯域幅をサーバに提供することでボトルネックを排除します。また、拡張された帯域幅は、VM によってより効率的に使用されます。

**帯域幅の拡張** : Xsigo では、10Gb の帯域幅を各サーバに単一のパイプで提供します。これは、VM 全体、あるいはストレージおよびネットワークトラフィック全体で動的に割り当て可能です。ネットワークトラフィックが今の瞬間に 10Gb を必要としていれば、全帯域幅をこれに割り当てることが可能です。また、次の瞬間にストレージトラフィックが 10Gb を必要とすれば、10Gb 全てをストレージに割り当てることが可能です。一方、旧来の接続では、スループットと柔軟性が劣ります。

**VM による効率的な使用** : 仮想 NIC と仮想 HBA は ESX を介して個々のバーチャルマシンに割り当てることができ、リソースを完全に制御することができます。さらに必要な場合、任意の時点において任意の VM が外部パイプの 10Gb の全帯域幅を利用することも可能です。

## Xsigo によるバーチャルマシンのセキュリティ拡張

仮想接続を特定の VM と関連付けることで、セキュリティを拡張することができます。このレベルまで管理を細分化することにより、従来のサーバに適用するのと同じ管理手法を使用したセキュリティ管理が可能になります。

**I/O を介した制御：**最も簡単なセキュリティデバイスは I/O です。特定のサーバ上の VM がネットワークにアクセスする必要がない場合は、単に I/O を関連付けません。たとえば、サーバ上の VM は、単にネットワーク上の vNIC と関連付けただけで、パブリック ネットワークから保護されます。同時に、高速サーバ上のセキュリティを犠牲にすることなく、別のサーバにパブリックネットワークへのアクセスを許可することができます。

**識別番号を介した制御：**仮想 I/O リソースを VM と関連付けることで、セキュリティ管理を簡素化することができます。仮想リソースはそれぞれ一意の識別番号 (WWN または MAC アドレス) を有しており、すべてのネットワークおよびストレージセキュリティ手段の完全な効率性が維持されます。さらに、I/O リソースとその識別番号は、VM とともにサーバ間で移動が可能です。これはすなわち、IT マネージャは「大型フラットネットワーク」やオープンストレージを敢えて実装する必要がないことを意味します。

## Xsigo による予測可能なパフォーマンスの実現

各 VM が自身の専用仮想 I/O リソースを持っている場合、QoS (サービス品質) プロファイルを仮想 I/O リソースごとに構成することにより、VM ごとの I/O フロー制御が可能になります。

各 vNIC または vHBA に対して、CIR (認定情報レート) で最小帯域幅を保証し、PIR (ピーク情報レート) で、リソースが消費できる帯域幅の最大量を制限します。

バーチャルマシン上で稼働するアプリケーションの設定を適切に調整することで、IT マネージャは、基幹アプリケーションのために設計どおりのネットワークパフォーマンスを確保することができます。

## 要約

Xsigo I/O 仮想化コントローラ が持つ仮想 I/O 機能により、VMware ESX を実行する仮想化データセンターでは、拡張能力を改善できるほか、トラフィック分離によるセキュリティ確保、QoS によるパフォーマンス保証が可能になります。同時に、これらの特長は、バーチャルマシン上のアプリケーション稼働率を高めるだけでなく、電力と不動産スペースを消費する物理サーバの必要性を削減します。