Trend Micro
Deep Security™

TREND MICRO™

企業のIT管理者が語る 仮想化の「本音」

セキュリティ対策だけではない Trend Micro Deep Security™のメリット

座談会で得られた「**生の声**」から
仮想化導入のメリットと問題点を洗い出します。

緊急座談会開催

トレンドマイクロ株式会社

仮想化はメリット？ デメリット？
座談会で明らかになった仮想化導入の現実

トレンドマイクロの主催によって、
14 名の有名企業の IT 管理者が参加する座談会が開催されました。
「ざっくばらんな交流の場」としたことで、普段は聞けないような現場の本音が飛び交い、
その現場の「生の声」を大別したのが、以下の６つのカテゴリです。

仮想化６つの目的と課題	座談会参加者「生の声」サマリー
導入／レガシー延命	OS やハードウェアの保守期限から解放される反面、物理環境で使用していたアプリケーションが仮想化環境でもちゃんと動くのかなど、サポートに関する声が多く聞かれました。また、まだまだ全てのシステムに対して仮想環境を導入できないという現状も浮き彫りに。
コスト	コストでは良かった点、課題点ともに多くの意見が交わされました。スペースの効率化や社内プロセスの簡素化によるメリットが挙げられたのと同時に、初期導入費用がネックになっているという声が噴出。ハードウェアの新規導入やライセンス体系などに対する本音が聞かれました。
運用／管理	仮想化環境では社内のマシンをすべて把握できるため、パッチの適用など管理がしやすいという声が多かった一方で、管理項目が変わることで手間が増えたという声も聞かれました。運用面では、社内の体制が十分に整っていないことから生じる様々な問題点が挙がりました。
バックアップ／ストレージ	手軽に仮想マシンを立てられる反面、バックアップにおいては厳しい声が多く上がりました。仮想マシンとデータの両方をバックアップしなければならないなど、特にストレージの I/O に関連した課題が多く、仮想環境特有の問題点が浮き彫りになりました。
セキュリティ	仮想環境特有の問題点がそれほど挙がらなかった反面、物理環境と同じ苦労を感じているという声が聞かれました。また、心理的な側面から仮想環境におけるセキュリティに対する信頼性がまだ十分に高まっていないことも見てとれました。
パフォーマンス	仮想マシンが増えるほどハードウェアへの負荷が大きくなり、パフォーマンスが落ちるという声が多く聞かれました。特に、仮想化環境でもネットワークやディスクの I/O は物理的なハードウェアを使用するため、この最適化やリソース管理など解決すべき課題がまだ多いようです。

仮想化が企業に及ぼす影響とは？
座談会で拾った「生の声」を一挙公開

ここに座談会で交わされた「生の声」を６つのカテゴリに分けて一挙公開します。
現場では特に「バックアップ／ストレージ」「セキュリティ」「パフォーマンス」に
多くの課題があるようです。

※（　　）は座談会参加者の業種

導入／レガシー延命

良かった点

○**レガシーシステム**上で生産管理などのシステムを構築していたが、仮想化によって**延命が可能**になった。（機械業）

○基幹業務は５～10 年かけて考える仕組みであり、安定稼働の観点から仮想化を選んだ。仮想化によって **OS のバージョンアップ毎の修正が不要**になった。（情報通信業）

○仮想化によってハードウェアの保守切れを気にせず済むようになった。ハードウェアリプレイスに関わる工数が不要になり、担当者が楽になった。（娯楽）

課題点

×仮想化に移行したいのだが、以前、物理環境で使用しているアプリが仮想化環境に対応しているかをベンダに質問したとき、不明確な答えしか返ってこなかった。サポートがないのでは移行する意味がない。（建設業）

×OS を含むアプリケーションのサポートが追いついていないため、**仮想化ベンダが一括してサポートして欲しい。**（ソフトウェア）

×金融機関などでは、異なるシステムを同居させてはいけないという、根拠のない社内規則がある。別のシステムは引き続き物理環境に分けることになるため、仮想化を導入するメリットが少なくなってしまう。（物流）

コスト

良かった点

○仮想化環境では、ゲストイメージを他の拠点に飛ばすことで容易にバックアップできる。これは**災害対策のコスト削減**につながる。（金融業）

○仮想化によってサーバを物理的に縮小でき、**固定資産を減らす**ことができる。物理的な縮小によって**スペースも有効に活かせる。**（マスコミ）

○サーバを購入するときに面倒だった稟議や社内手続きが無くなるのは何よりも大きい。（マスコミ）

課題点

×仮想化が考慮されたライセンス体系が整備されていない場合もある。物理環境と同様にサーバの筐体やリソースに対して課金することになり、SQL など CPU ライセンスで買うと金額が膨らむケースがある。（物流）

×HA サーバ、FA サーバと冗長構成が組めるメリットはあるが、ハードウェア自体の機能が上がってくるのだから値段も上がる。だから仮想化は高くつく。（物流）

×運用上、ノードを部門ごとに細かく切っていかなくてはならず、知らないうちに監視ノードが増えてしまう。**手間もコストもかかる。**メリットってなに?と思ってしまう。（金融業）

運用／管理

良かった点

○ネットワークでは見えているのに、物理的に場所がわからないマシンが 100 台ぐらいある。これらを**仮想化で一元化**するのは、運用コストの面でも期待できる。（物流）

○仮想化は単体のセキュリティが落ちる問題があるが、何かが起きたときの対処や守りやすさは向上している。管理者に一定のスキルレベルは求められるが、**全体的に管理のしやすさは向上**している。（物流）

○共通の会議室に置いてある PC を**シンクライアント化**して仮想化した。**パッチを当てる担当者の手間などを、集約化により解決**できた。（金融業）

課題点

×使用されているのにサービス管理者がわからないという仮想サーバがあちこちにある。中を開けてみないとわからないのだが、誰の権限で開けるのかという問題もある。（医療）

×物理環境と仮想環境では管理項目も変わってくる。今まで 1500 台規模の物理サーバを管理していく前提でデータベースを構築していたので、仮想に変わっていくといっても既存の管理体制をすぐに壊すわけにはいかない。**構成管理の複雑化が問題**だ。（システム）

×M&A で他社と合併したが、両社で管理の方法に違いがある。管理の仕方が異なる２社が合併した環境で扱いに悩む部分がある。統合はしにくいと思う。（金融業）

バックアップ／ストレージ

良かった点

○サーバ仮想化におけるカプセル化によって、サーバがファイルとして保存されるようになった。これにより、**システムのバックアップを容易に取得**できるようになった。（ソフトウェア）

○VMwareの基本機能であるスナップショット機能により、システム変更時に障害が発生した場合でも**容易にロールバック**できたり、無停止で仮想サーバのシステムバックアップを取得できている。（ソフトウェア）

課題点

×大原則はV2V（仮想環境同士の連携）が問題なくできることだが、その中でI/Oが高いものに関しては**ストレージ構成を考えないとボトルネック**になってしまう。（娯楽）

×VMware標準のVCBマウントを使っているが、容量の大きいVCBマウントを使うとハードディスクが一日中回りっぱなしになってしまう。**ストレージへの影響**が心配。（建設業）

×仮想マシンが増えてくると、データと仮想マシン両方のバックアップが必要になる点が面倒になる。仮想サーバは立てやすいので、乱立すると管理者の手が回らなくなってしまう。（娯楽）

セキュリティ

良かった点

○仮想化により、物理的なハードウェアを**セキュリティの高いデータセンターのラック内に集約**することが可能になった。また、HDDやUSBメモリといったハードウェアデバイスによるデータの持ち出しを防ぐことができる。（ソフトウェア）

○コンソールも物理から仮想になったことで、コンソールへのアクセスをADの**ユーザアカウント**に対して設定し、**制限できる**ようになった。（コンサルティング）

○複数のシステムが限られた「箱」に集約されることにより、仮想サーバ単体ごとのセキュリティ対策ではなく、**VMwareのAPI（VMsafe）を利用した仮想アプライアンスで包括的なセキュリティソリューションが期待できるようになった。**（ソフトウェア）

課題点

×ブレードはスイッチがあるため、業務システムの仮想マシンをファイアウォールで守ろうとすると、その分だけセグメントを作らなければいけない。面倒がるとセキュリティレベルが落ちることになる。（娯楽）

×**パッチをあてる作業は仮想でも同じだから、管理は楽になっていない。**電源を落とせるマシンが少ないので、立ち上げたまま放置されているマシンも面倒を見なくてはいけないのが困る。（ソフトウェア）

×仮想化環境はディスクの追加、パッチあてなどもかなりやりやすい。だが結局、障害は心理的な部分。本当の意味での信頼性がついてこないと、テスト導入のレベルから抜け出せないという悩みはどこも持っているようだ。（建設業）

パフォーマンス

良かった点

○仮想化を支えるそれぞれのマシンのCPUやメモリといったハードウェアリソースを共有のリソースとして扱うことにより、サーバ機器の本来もつ**パフォーマンスを効率的に使用**できるようになった。（ソフトウェア）

○仮想サーバおよびVMwareの**ホストのパフォーマンス**を、リアルタイムでもヒストリカルでも**グラフィカルに確認**することが可能になった。これにより、パフォーマンスの劣化に対する**トラブルシューティングが容易**になった。（ソフトウェア）

課題点

×**負荷の大きいタスクを動かすと他の仮想マシンが遅く**なったり落ちたりした。ハードウェアのアラートを管理するツールがリソースを消費しすぎ、ある日突然エラーが出ることがあった。（情報通信業）

×データベース系のディスクのI/Oが追い付かず、**パフォーマンスに大きな影響が出る。**ストレージメーカーでは、アプリからのトータルのスループットについてどこも保証できないため、もう少し良いツールはないものかと正直悩んでいる。（IT）

×保証まで考えていくと、仮想化のメリットが出しづらい。ミッションクリティカル系のサーバだと、バックアップなどいろいろな要件が出てきて逆に仮想環境が足かせになることもある。（システム）

仮想化環境への移行時にはセキュリティ対策も同時に

Trend Micro Deep Security™で解決する仮想化環境の問題

座談会の結果、仮想化環境におけるセキュリティ対策の重要性は理解していても、具体的な対策に悩んでいる現状が明らかになりました。たとえば、トレンドマイクロの次世代サーバに対応した保護ソリューション「Trend Micro Deep Security」なら、物理、仮想化などの環境にとらわれることなく一貫性のあるセキュリティ対策を実現できるほか、セキュリティ以外の問題にも有効です。

導入／レガシー延命

レガシー環境も安心して活用!

- Windows 2000などサポート切れOSの脆弱性も“仮想パッチ”でサーバを保護
- ネットワークレベルで脆弱性をブロックするため、上位のアプリケーションへの影響を最小限にすることが可能
- Windows NTなどのさらに古いOSに対しては、Trend Micro Deep Security Virtual Applianceで保護

コスト

さまざまな面でコスト削減に寄与!

- “仮想パッチ”で緊急性の高い脆弱性も一時的に保護することができ、パッチマネジメントにかける工数を削減
- 6つのセキュリティ機能を1つの製品で実装することで、個別で買うよりもセキュリティ製品のコストを抑制
- サーバ台数規模に応じて導入できるため、スモールスタートが可能

運用／管理

物理、仮想環境の統合管理により手間を大幅に削減!

- 複数のセキュリティ機能を1つの管理マネージャで管理することで、管理コストの抑制とログの相関分析が可能
- 物理サーバ、仮想サーバ、クラウドコンピューティングといった様々なサーバ環境に対応し、エージェント型と仮想アプライアンス型のセキュリティモジュールを利用することで、混在したサーバ環境も統一したセキュリティポリシーで保護することが可能

セキュリティ

ゲストOS単位で高度なセキュリティ対策を実現!

- ゲストOS間の不正な通信も検知・ブロック
- vMotionなど、仮想プラットホーム間をゲストOSが移動してもセキュリティポリシーを引き継ぐことで可用性を保持
- ゲストOS毎にウイルス対策ソフトをインストールすることなく、エージェントレスウイルス対策が可能

Trend Micro Deep Security（以下、Deep Security）4つの特長

特長1 仮想パッチ機能で脆弱性を悪用した攻撃から保護！ パッチ運用作業の負荷軽減とリスク低減を両立！

- 推奨スキャン機能が自動でサーバの脆弱性を検出し、仮想パッチを適用
- OSからミドルウェアまでの脆弱性に対応
- 計画的なパッチ適用作業を実現

特長2 サーバに必要な6つのセキュリティ対策を 1つのエージェントに実装！

- IPS/IDS機能
- ホスト型ファイアウォール機能
- Webアプリケーションの保護機能
- 改ざん検知機能でファイル、レジストリの改ざんを検知
- セキュリティログ監視機能
- ウイルス対策

特長3 環境にとらわれない一貫性のあるセキュリティ対策を実現！ 運用管理をシンプルに可視化！

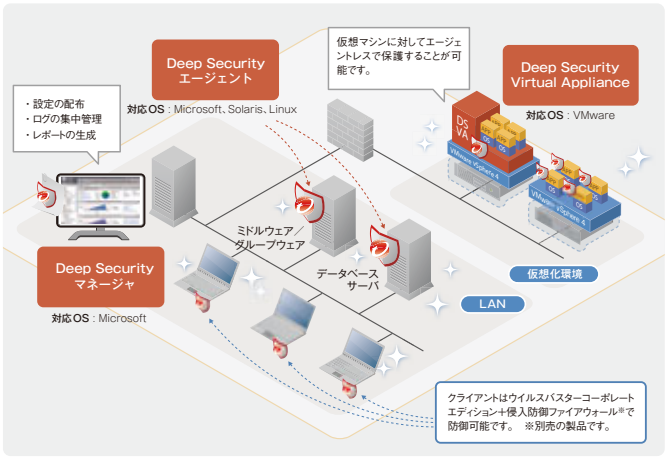
- 物理環境、仮想化環境、クラウドコンピューティング環境のサーバに導入が可能
- Windows、Linux、Solarisと主要なサーバOSに対応
- Deep Securityマネージャによる設定の一元管理とレポートの生成

特長4 ホスト型のセキュリティ対策で、 ロケーションや環境に依存せず適切にサーバを保護

- VMware ESX、Xen、Hyper-Vなどの仮想化プラットホームに依存せず、ゲストOSを保護
- 従来のネットワーク型セキュリティ対策製品では防げないゲストOS間の攻撃や不正なトラフィックを検知/防御
- ホスト型だからできる詳細なログ集積機能による原因分析

Trend Micro Deep Securityであれば、仮想化環境のセキュリティ強化と サーバセキュリティの運用管理コストの最小化を実現します。

Trend Micro Deep Security構成図



環境に応じた買い方が可能

製品名・主な機能 ＼ お客様の環境	小規模環境／検証目的で購入したいお客様	物理環境を保護したいお客様	仮想化環境を保護したいお客様	SaaS、PaaS、IaaSサービス事業者様
Trend Micro Deep Security マネージャ	1ライセンス	1ライセンス	1ライセンス	Security Service License（月額ライセンス）＋ Trend Micro Availability Service（有償24時間サポートサービス）
Trend Micro Deep Security エージェント	5ライセンス	必要サーバ台数 ※仮想ハードウェアも1台と数えます	必要サーバ台数 ※仮想ハードウェアも1台と数えます	
Trend Micro Deep Security Virtual Appliance			必要CPUソケット数 ※1ソケットにつき最大12コアまで	

Trend Micro Deep Securityシステム要件

対応OS：エージェント	Microsoft	・Windows 2000 ・Windows Server 2003（32/64ビット）SP2以降 ・Windows Server 2008（32/64ビット）
	Solaris	・8, 9, 10 on SPARC ・10 on x86（64ビット）
	Linux	・Red Hat 4, 5（32 / 64ビット） ・SuSE 9, 10 ・Cent OS 5
	UNIX系	・HP-UX 11i（11.23, 11.31） ・AIX 5.3 ※HP-UX、AIX用エージェントでは、改ざん検知およびログ分析機能のみが提供されます。
	仮想化環境	ゲストマシンが左記OS要件を満たす場合、VMware ESX、Xen、Hyper-Vなどの仮想化プラットフォーム上でも通常の環境と同じようにエージェントの機能が提供されます。
対応OS：管理マネージャ	Microsoft	・Windows Server 2003（32/64ビット） ・Windows Server 2008（32/64ビット）
仮想パッチで保護可能なソフトウェア例	データベースサーバ	Oracle、MySQL、Microsoft SQL Server
	Webアプリケーションサーバ	Microsoft IIS、Apache、Apache Tomcat
	メールサーバ	Microsoft Exchange Server、IBM Lotus Domino
	バックアップサーバ	Computer Associates、Symantec、EMC
	ストレージマネジメントサーバ	Symantec、Veritas
	メールクライアント	Microsoft Outlook Express、Microsoft Outlook、Windows Vista Mail、IBM Lotus Notes、Lpswitch IMail Client
	その他	Samba、IBM Websphere、IBM Lotus Domino Web Access

※システム要件に記載されているOSの種類やハードディスク容量などは、OSのサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

製品に関する詳細はこちらから ▶ http://www.trendmicro.co.jp/tmds

TREND MICRO™ トレンドマイクロ株式会社

東京本社
〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
TEL.03-5334-3601（法人お問合せ窓口） FAX.03-5334-3639

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル13階
TEL.06-6350-0330 FAX.06-6350-0591

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24 名古屋桜通ビル7F
TEL.052-955-1221 FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7 サンエフビル7階
TEL.092-471-0562 FAX.092-471-0563

www.trendmicro.co.jp

TRENDMICRO、ウイルスバスター、およびTrend Micro Deep Securityは、トレンドマイクロ株式会社の登録商標です。
各社の社名および製品名は各社の商標または登録商標です。
記載内容は2011年3月現在のものです。内容は予告なく変更される場合があります。
Copyright © 2011 Trend Micro Incorporated. All rights reserved.

お問い合わせ先

C33-DSK-MRM-C001