IHS INFONETICS 調査レポート抜粋

データセンター セキュリティ戦略およびベンダー リーダーシップ

抜粋

2015 年 3 月

リサーチ ディレクタ: Jeff Wilson

目次

参照リスト

重要ポイント

2015 年は、データセンター セキュリティ分野の支配権争いが激化する年となっています。とりわけ、ハイエンドのアプライアンス市場では競争が激化しています。2014 年には大きな市場シェアの変化があり、多くの購買担当者は次のような基準で新旧ベンダーを評価するようになっています。

- 購買担当者が現在求めているインターフェイスとパフォーマンス(接続とスループット)を備えたベンダーであるか。2015 年には、データセンターのパフォーマンスの足かせになるようなセキュリティ インフラストラクチャは見切りをつけられます。2016 年以降を視野に入れれば、25 G のポートがデータセンター向けの主要オファーになると予測されます。
- パフォーマンス向上と引き換えに、セキュリティの有効性や管理/ポリシー ツールを犠牲にしていないか。脅威データをリアルタイムに利用できることが、投資先の選択において新たな重要事項になっています。
- 現時点でコスト競争力のあるソリューションであり、魅力的なアップグレード パスを備えているか。たとえば、ソフトウェアやハードウェアをアップグレードしてパフォーマンスを向上させたり、新たな保護メカニズムを追加したりできるか。
- 仮想化や SDN に向けた明確なロードマップと、2015 年中盤から後半にかけての具体的な製品計画が提示されているか。また、そのコンセプト実証となる各種ハイパーバイザや SDN コントローラ プラットフォームの一部が現時点で利用可能になっているか。

今日、企業のデータセンターに影響を及ぼす最も大きな変化とは、サーバ仮想化技術とデータセンター オーケストレーション ソフトウェアの採用です。これらはデータセンター仮想化の構成要素であり、データセンターでの SDN の展開へとつながる重要な要素と言えます。回答者の 76 % は、新しいセキュリティ ソリューションを購入する重要な原動力となっているのは仮想化であると考えています。回答者はまだ SDN 対応のセキュリティ ソリューションの購入を本格的に検討していません(セキュリティ投資の優先順位としては下位のほうですが、71 % は検討要因と回答しています)。

データセンター セキュリティ ソリューションの重要な購入基準となるブランド力という点では、シスコ、McAfee、HP、Juniper、VMware が上位を占めています。本調査で質問した各基準における評価は主に全般的なブランド力と関係していますが(全体的に大規模ベンダーが高評価を獲得)、いくつかの興味深い山(Juniper は技術革新と価格の評価が高い)や、谷(シスコは一般的に価格性能比で評価の落ち込みが見られ、サービスやサポートの点でも評価が低下)が見られます。また、Palo Alto の管理機能は、ベンダーの全般的なブランド認知度やブランド力からすると驚くほど高い評価を受けています。

はじめに

市場の背景

巨大なホスティング プロバイダーから、Google や Amazon のようなクラウド セントリック企業、さらには大規模企業や中規模企業まで、世界中のあらゆる企業の IT 組織は、業務の運用とコストの抑制に必要な拡張性や俊敏性を得るために、データセンターの統合や再構築に取り組み、インフラストラクチャをクラウドに移行し、柔軟でプログラム可能なデータセンター アーキテクチャ(データセンター ネットワークのための SDN など)を実現することを目指しています。データセンターにセキュリティ ソリューションを導入しようとしている企業は、1 台のマシン(物理マシンまたは仮想マシン)を保護するサーバ ソフトウェアから、ハイパーバイザ レベルでセキュリティを提供する仮想アプライアンス、さらには複数のロケーションのデータセンターに配置される大型の物理セキュリティ アプライアンスまで、幅広いセキュリティ製品を検討する必要があります。利用可能なソリューションは数多くありますが、どのベンダーが提供するどの製品がベストかについては意見が分かれています。企業向けデータセンター事業者も、インフラストラクチャの構築手法を大きく変化させるネットワーク用 SDN、ソフトウェア デファインド ストレージ、データセンター オーケストレーション ソフトウェアの導入、新しいマルチ CPU サーバ アーキテクチャといったテクノロジーに注目しています。これらはセキュリティの導入方法を変革することになるからです。

では、エンドユーザとなる企業、すなわち現在データセンターの構築やアップグレードを行っている企業は、自身の直面するセキュリティ問題についてどのように考えているのでしょうか。本調査は、購買担当者がデータセンターのセキュリティ計画についてどう考えているかを把握するために行われました。

調査の手法と対象者の概要

2015 年 3 月に、自社でデータセンターを運用している 137 社の中規模および大規模組織(社員数 500 名以上)の IT 意思決定者に対し、Web アンケートを実施しました。本調査では、データセンターの定義を、「ローカル ネットワークで接続されたサーバ(コンピュータ システム)やストレージ システムをハウジングするための通信施設に接続されている単独の建物内の設備。一般的に SAN、冗長またはバックアップ用電源、冗長データ通信接続、環境制御(空調、消火設備)、各種セキュリティ デバイスを含む」としています。

自社のデータセンターに導入されているセキュリティ ソリューションの詳細な専門知識と、そのようなソリューションの購入に関して影響力を有している方のみを回答者としました。回答者は、主要な意思決定者か、大きな影響力を持つ人のどちらかです。

購入要因

回答者は、データセンターのセキュリティに新しい投資を行う際に、さまざまな問題に悩まされています。ここ数年間は仮想サーバのセキュリティ向上が最優先でしたが、今年はこれに変化が見られます。2015 年の最優先事項は、リアルタイムの脅威インテリジェンスを活用し、暗号化トラフィックも検査できるソリューションになっています。

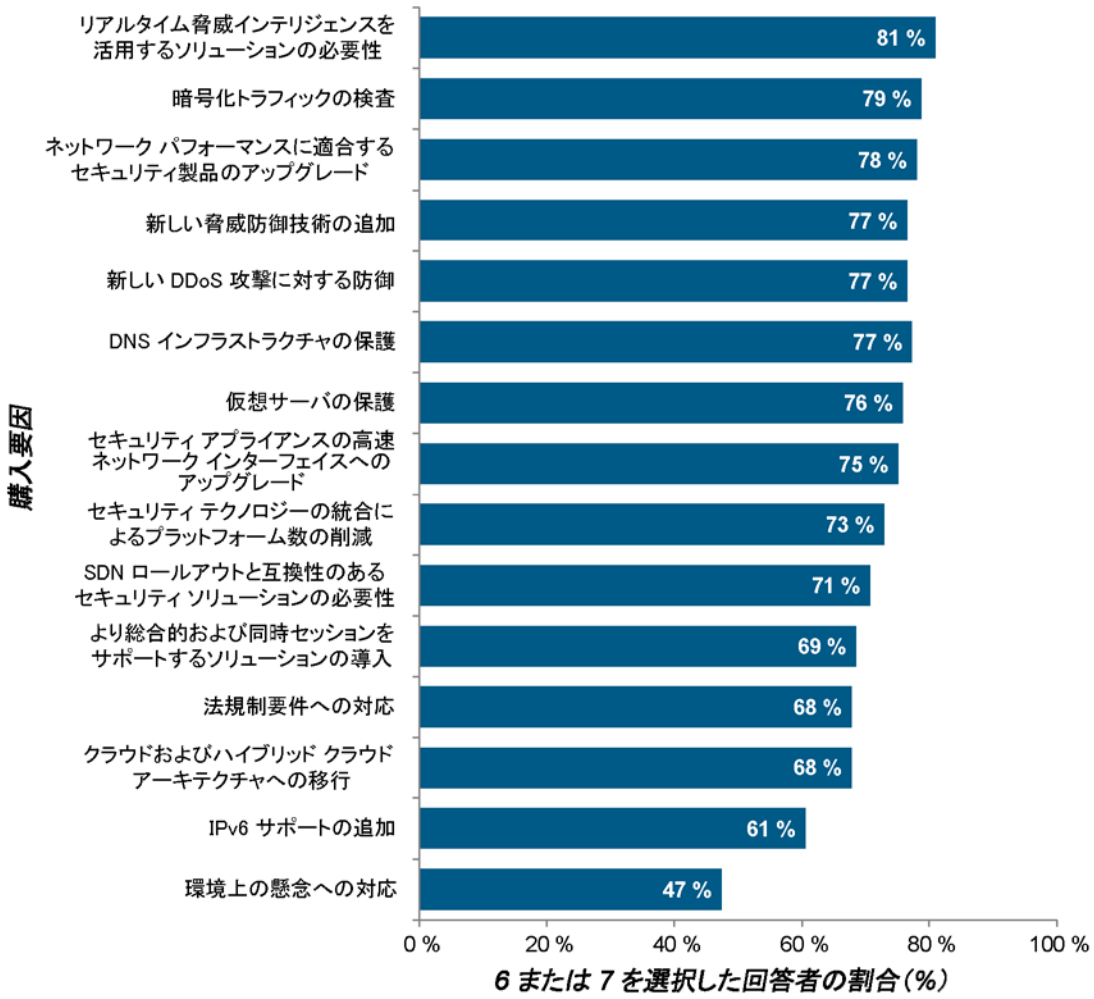
本調査では、データセンター向けの新しいセキュリティ ソリューションを購入する際のさまざまな検討要因の重要度を 1 から 7 までの数値で評価してもらいました。1 は「購入要因ではない」、4 は「ある程度は購入要因になる」、7 は「強力な購入要因になる」を示しています。次のチャートは、各機能（購入要因）について 6 または 7 を選択した回答者の比率を示しています。

脅威が大きく報道されるほど、データセンターのセキュリティ購買担当者の関心はパフォーマンスやアーキテクチャを離れ、問題の核心、すなわち損害につながるセキュリティ侵害を防ぐことに向かう傾向にあります。回答者が望んでいるのは、リアルタイムの脅威インテリジェンスに統合される形で利用でき、データセンターのスピードに対応しながら、脅威にさらされる時間を短縮できるソリューションです。データセンター セキュリティ ソリューションを提供する各ベンダーは、全般的なパフォーマンスや SDN/NFV への移行というメッセージと併せて、脅威インテリジェンスやそれとの連動性に関するメッセージを発信する必要があります。これには同等かそれ以上の重要性があるからです。

また、回答者は暗号化されたトラフィックの可視化を求めています。スノーデン氏による情報開示をきっかけに、インターネット上では Facebook、Google などをはじめとする大手サイトの多くが、HTTPS によってすべてのトラフィックを暗号化する方向にシフトしています。これは個人の自由にとっては有益ですが、セキュリティを実現する側にとっては悪夢です。暗号化トラフィックを扱う方法は、既存のアプライアンスに SSL カードを追加する方法から、総合的な SSL インスペクション インフラストラクチャを配置することまで、さまざまな方法が存在します。購買担当者は、データセンターで動作する SSL インスペクション ソリューションを求めています。

参照 1

新しいデータセンター セキュリティ ソリューションの購入要因
n=137



今日、企業のデータセンターに影響を及ぼす最も大きな変化とは、サーバ仮想化技術とデータセンター オーケストレーション ソフトウェアの採用です。これはデータセンター仮想化の構成要素であり、データセンターでの SDN の展開へとつながる重要な要素と言えます。仮想化サーバを導入するには、データセンターの新しいセキュリティ ソリューションに投資を行う必要があり、回答者の 76 % が新しいセキュリティ ソリューションの重要な購入要因として仮想化を挙げています。

企業のデータセンターの購買担当者の大半は仮想サーバに関連するセキュリティ問題の解決を目指しているものの、SDN 対応のセキュリティ ソリューションについては、購入しようという動きが始まったばかりです（優先順位は低く、重要な購入要因と答えているのは 71 % のみです）。ほとんどの企業のデータセンターには、まだ SDN インフラストラクチャは設置されていません。そのため、これはセキュリティ購入の短期的な要因にはなりません。今年は購入要因としての SDN の重要性が高まる転機の年となり、2016 年には SDN がデータセンター セキュリティ ソリューションの主要な購入要因になると予想されます。ただしこれは、今現在の各ベンダーの SDN ソリューションへの取り組みや、将来的な SDN 環境での各ソリューションの働きをカスタマー ベースにアピールすることを否定するものではありません。現時点ではこのソリューションを提供することの重要性がそれほど高くないというだけです。

データセンター セキュリティの導入戦略

セキュリティの設計者がデータセンター セキュリティ問題の解決を目指す場合、要求を満たさなければならない技術要件およびビジネス要件が数多くありますが、製品選択においては、購入するセキュリティ ソリューションの対象が、より従来的なデータセンター、一部のサーバおよびストレージが仮想化されているデータセンター、または完全に仮想化され、SDN 実装への準備が完了しているデータセンターであるかに関わらず、3 つの基本的なグループに分けることができます。

データセンター インフラストラクチャを攻撃から守るためには、今もなお、***大型の高性能アプライアンス***（ファイアウォール、IPS、DDoS など）が必要です。これらのデバイスが保護するアプリケーションおよびプロトコルは、進化し続けており、パフォーマンス要件は、依然として増え続けています。場合によっては、高性能アプライアンスは仮想化に対応可能であり、VM 間のトラフィック送信ができる場合があります。今後、SDN やデータセンター オーケストレーション プラットフォームと連動することも考えられます。

大型の高性能アプライアンスの次に来るのが、***ハイパーバイザ レベルでのサーバの保護*** です。ここでは、おなじみの名前（Juniper、Check Point、シスコ、Symantec、McAfee、Trend Micro など）に加えて、新しい名前（VMware を筆頭とする仮想化プラットフォーム ベンダーや、Catbird などの分野に特化したベンダー）が挙がります。これらの商品のセキュリティ機能はさまざまで、他のセキュリティ製品との通信範囲も異なりますが、ほとんどの回答者が、ハイパーバイザと相互通信が可能で、複数の仮想マシンの保護が可能なソリューションを備えることが必要であると認めています。これらのプラットフォームも、少しずつ、SDN やデータセンター オーケストレーションのサポートを組み入れることが予想されます。

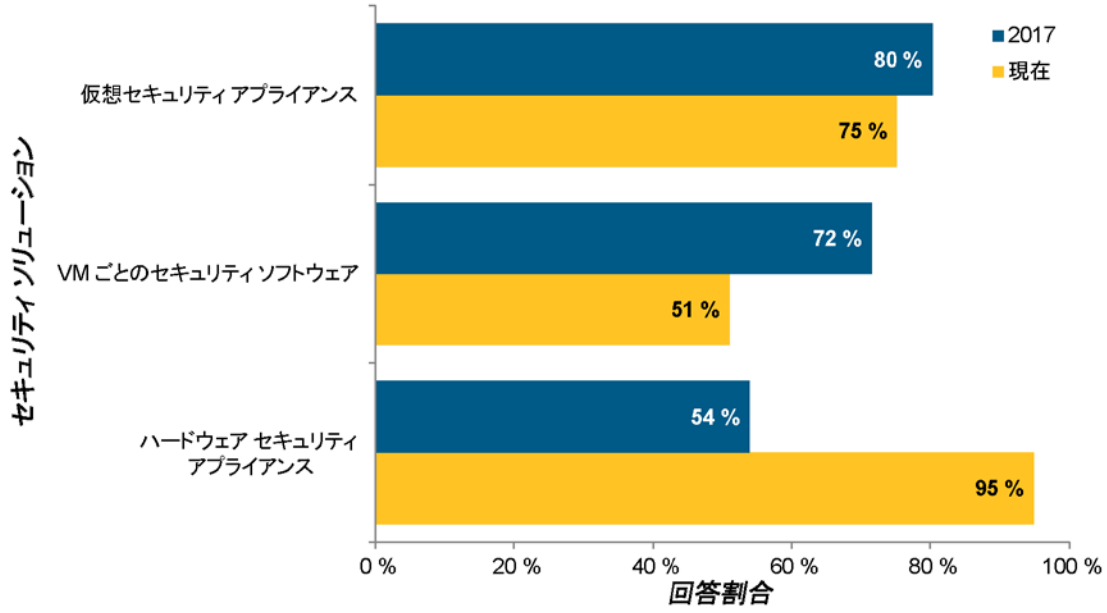
最後に、***個々のサーバ保護*** です。ここでは再び、AV から暗号化、ファイルの統合管理など、さまざまな機能を持つ製品を提供している従来型のセキュリティ ソフトウェア ベンダー（Symantec、McAfee、Trend Micro など）の名前が挙がってきます。アプライアンスやハイパーバイザのベンダーがこれらのベンダーと主要なパートナーシップを結び、個々のサーバを保護するサービスも提供するようになる可能性もあります。

データセンターに導入するセキュリティの基本戦略に関して、回答者は明らかに多層的なアプローチを好んでおり、回答者の多くはすでにハードウェア アプライアンスと仮想アプライアンスを組み合わせて導入しています。データセンター セキュリティ導入モデルを管理する際に最も費用がかかり、最も難しいという事実にもかかわらず、半数以上が、VM 単位でサーバ レベルのセキュリティ ソフトウェアを導入しています。興味深いことに、回答者の多くが、2 年後にはデータセンターでのハードウェア アプライアンスの利用が減少すると予想しています。これは仮想インフラストラクチャへの大規模な移行の一環であり、先進的な購買担当者がクラウド型ソリューションに期待していることを示しています。

将来的には SDN が導入され、データセンターでのハードウェア アプライアンスとソフトウェア アプライアンスのバランスが変わることが想定されます。来年の調査では、回答者の SDN やデータセンター オーケストレーション ツールに関する専門知識ははるかに向上していることでしょう。まず、上位層のセキュリティ テクノロジー（メッセージング、IPS、アプリケーション、Web 保護）において、ハードウェアからソフトウェアへの移行が起こります。データセンターの末端（インターネットと接続されている場所）には、DDoS 緩和とファイアウォール用のハードウェア セキュリティ インフラストラクチャが残りますが、データセンターの中心であるサービス層では、こうしたソリューションは仮想化されるはずです。

参照 2

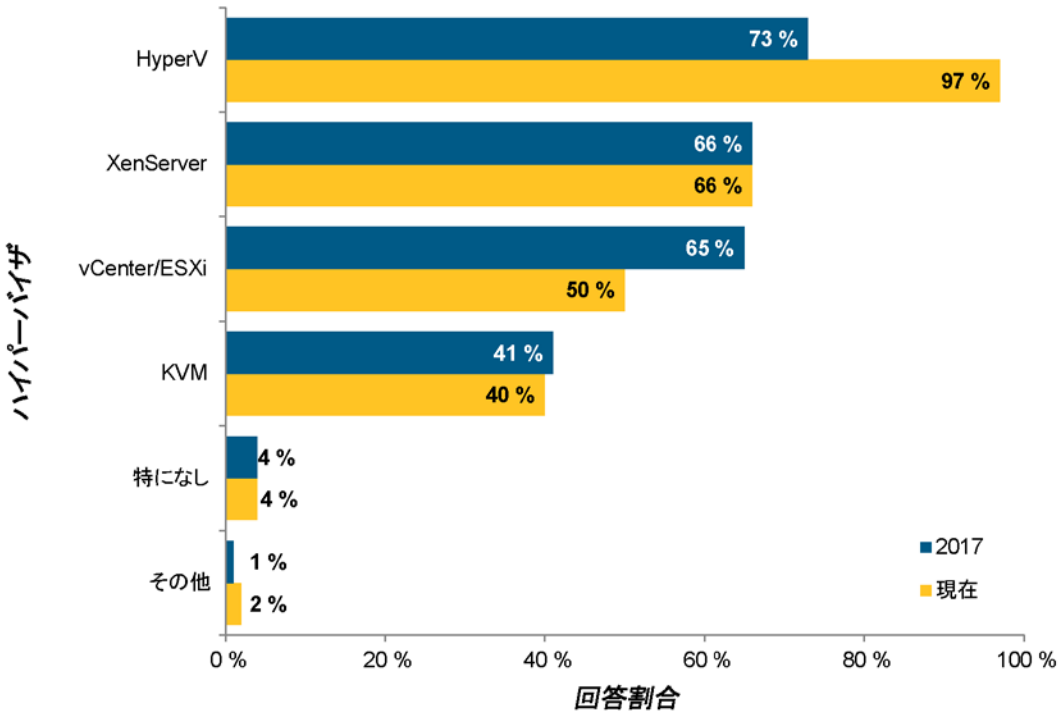
データセンターで導入されるセキュリティ ソリューション
n=137



次に、回答者の仮想セキュリティ アプライアンス ソリューションはどのハイパーバイザ プラットフォームに対応する必要があるかを尋ねました。現在のところ、企業のデータセンターは VMware（vCenter）、Citrix（XenServer）、Microsoft（HyperV）の 3 強の争いとなっていますが、KVM も VMware に大きく引き離されているわけではありません。現時点では Microsoft が優位に立っており、多くの企業が HyperV を試したり、Azure クラウド サービスに手を出したりしています。多くのサービス プロバイダーから、Microsoft の技術力はすばらしく、HyperV は人気のホスティング環境になっているという声も聞かれています。しかし、仮想セキュリティ ソリューションの市場はまだ初期段階であり、ここで勝者を断定してしまう理由はありません。ただ 1 つ言えるのは、ほとんどの仮想アプライアンスは、すべての主要なハイパーバイザ プラットフォームに対応する必要があるということです。

参照 3

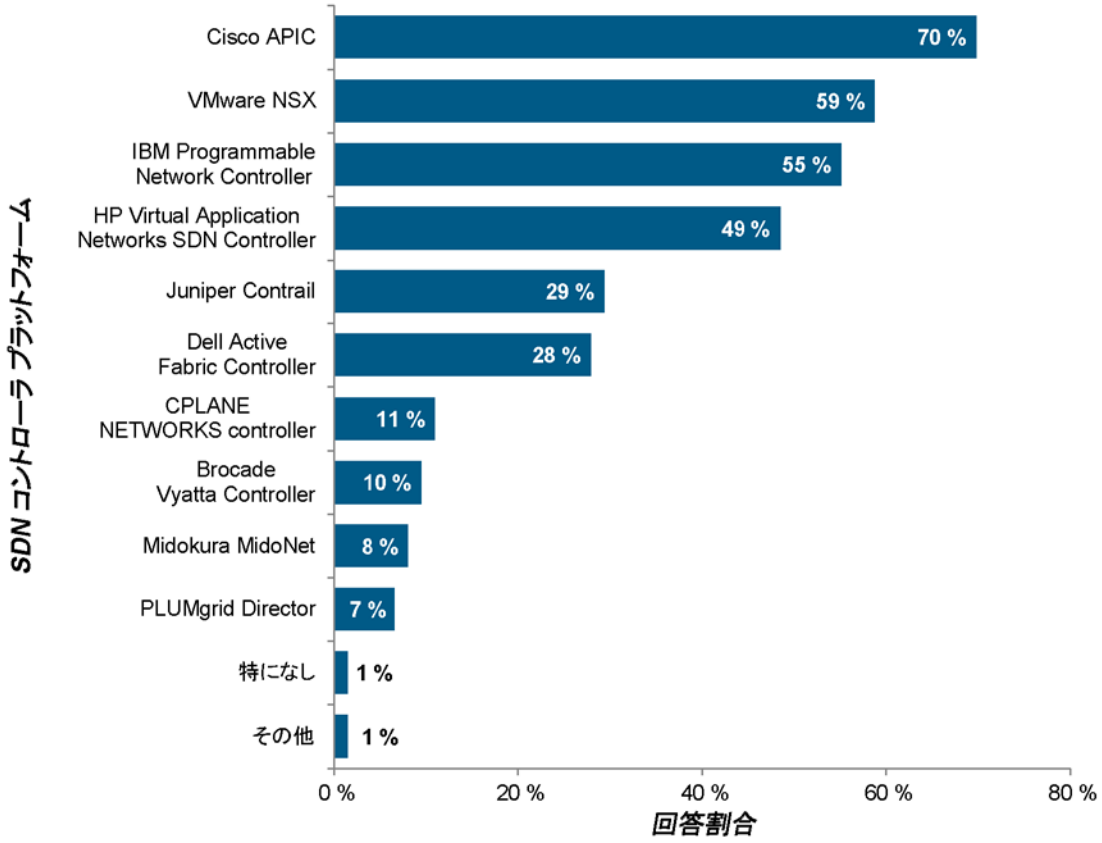
ハイパーバイザの互換性
n=137



サーバ仮想化に続き、ほとんどの企業のデータセンターが導入するであろうテクノロジーの 1 つは SDN です。データセンター分野の SDN においても、現時点ではさまざまな意見があります。しかし、現実的に見れば、今はまだ SDN の導入サイクルのかなり初期段階です。現在どの SDN コントローラを評価しているかを回答者に尋ねたところ、シスコ、VMware、IBM、HP をはじめ、さまざまなプラットフォームが挙がりました。実際のところ、SDN コントローラの競争がセキュリティ テクノロジーの競争に影響するかどうかは不明です。ほとんどのコントローラはあらゆるセキュリティ ベンダーの製品と連携できるからです。ただし、ここからわかることがあります。長期的にはどのようなセキュリティ ベンダーのサービスを選択することもできますが、Juniper Contrail を選択したデータセンター事業者は第 1 段階として Juniper vSRX 仮想アプライアンスを導入する可能性が非常に高いということです。コントローラ ベンダーの選択は、仮想セキュリティ製品の初期市場での成功の指標になるかもしれません。

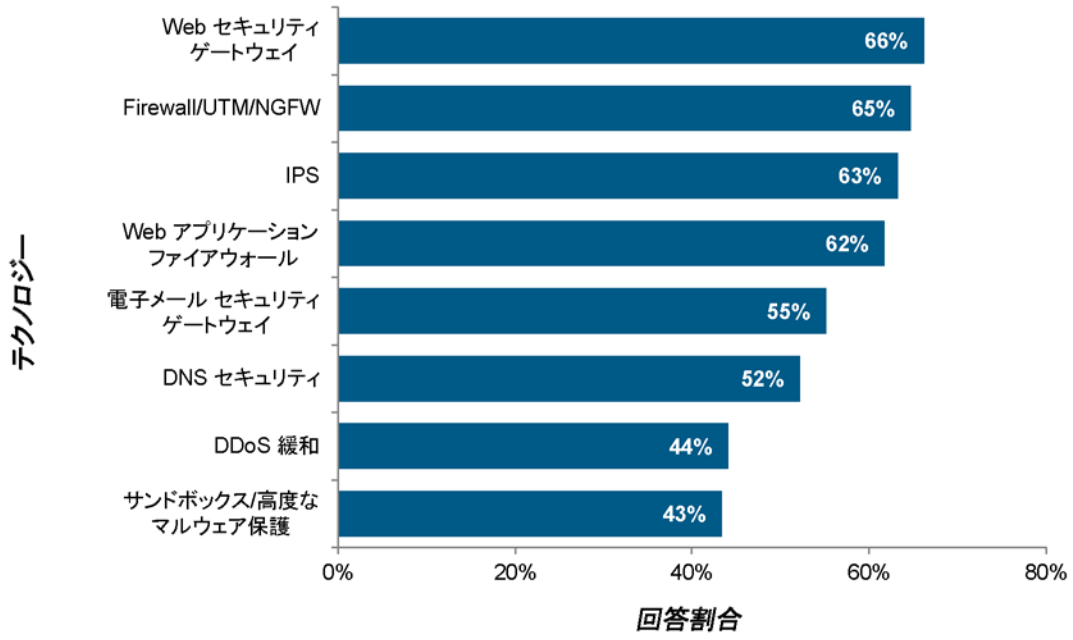
参照 4

評価中の SDN コントローラ プラットフォーム
n=137



さらに、仮想アプライアンスを使用して 2015 年末までに導入する計画があるセキュリティ テクノロジーについて尋ねました。上位 4 製品には、コア ネットワーク製品（ファイアウォールと IPS）とアプリケーションおよびコンテンツ製品（Web セキュリティ ゲートウェイと WAF）が混在しています。一般的な見方によれば、テクノロジーが高次の層（SWG や WAF など）になるほど仮想アプライアンス形式での導入が多いと考えられます。これは、アプリケーション自身がすでに仮想インフラストラクチャ上で動作しているためです。市場では仮想ファイアウォール製品が日々増え続けており、データセンターで仮想化されるネットワーク インフラストラクチャが増えるにつれて、仮想化されるネットワーク セキュリティ ツールも増加すると言われています。

参照 5 **仮想アプライアンスとして導入されるセキュリティ テクノロジー n=137**

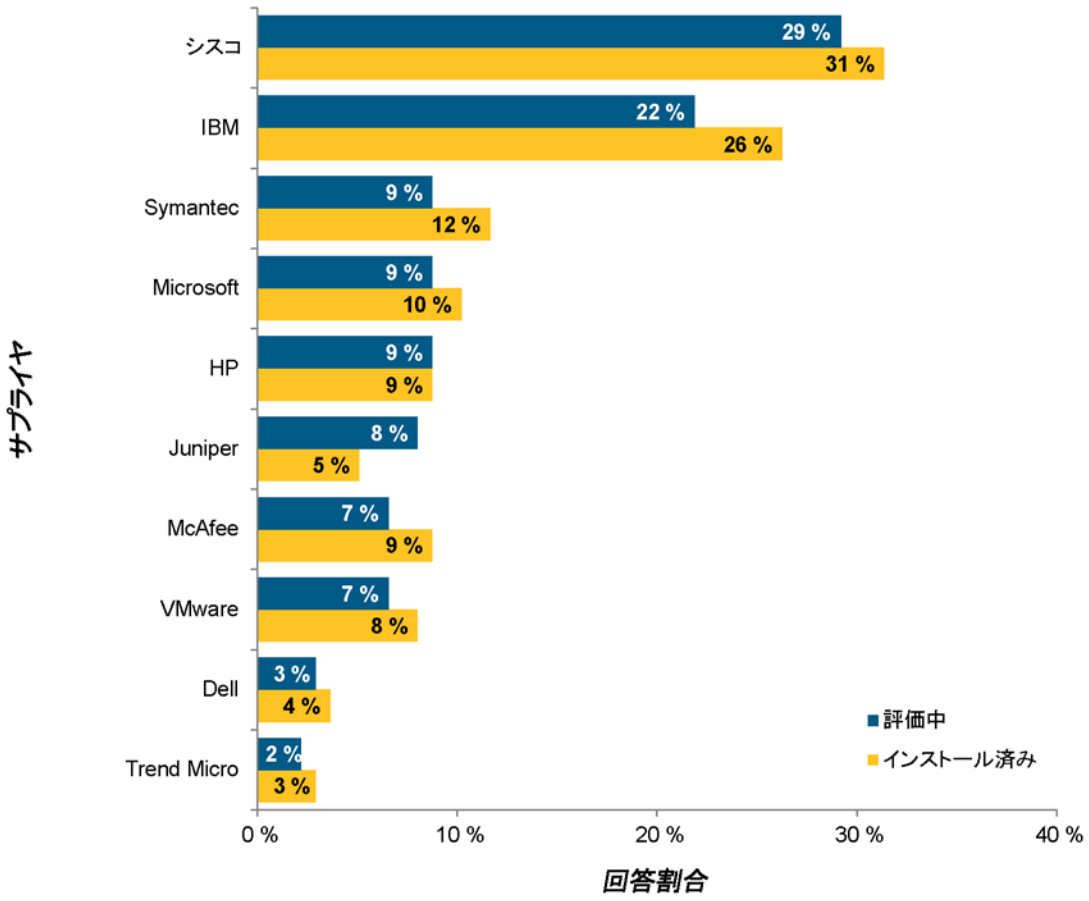


導入済みおよび評価中のソリューション サプライヤ

自由回答形式の質問で、現在使用しているデータセンター セキュリティ ソリューションのベンダーと、2016 年の導入に向けて評価しているソリューションのベンダーを尋ねました。

この市場は断片化しているため、導入済みベンダーの顔ぶれも多岐にわたり、仮想化ベンダー、アプリケーション/データベース ベンダー、サーバ/データセンター大手、クライアント セキュリティ ベンダー、ネットワーク セキュリティ ベンダー、データセンターのネットワーク統合ビジネスに大きな関心を寄せているベンダーなどが混在しています。ここで上位に名を連ねたベンダーは、データセンターやクラウド セキュリティの分野で主導権を握れる可能性があります。そのためには、適切な製品の組み合わせ（特に、納得のいくコストでパフォーマンスのアップグレードを提供することを重視）や、セキュリティ有効性に関する大きな実績、優れたソリューションや統合製品の提供、さらには隣接分野での強みを活かすことがポイントになります（たとえば HP や IBM はサーバやストレージ ビジネスをデータセンター向けセキュリティの販売に活かしており、シスコや Juniper はセキュリティ、スイッチング、ルーティングを組み合わせた強力なオファーを提示しています）。

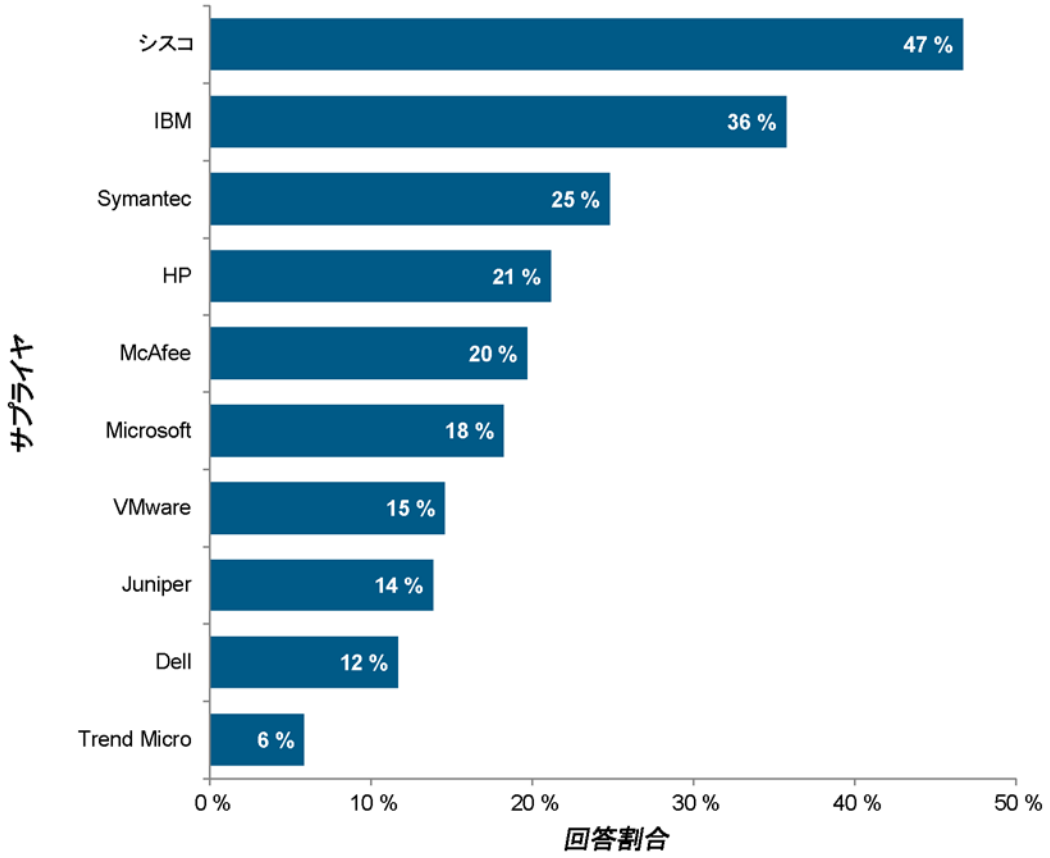
参照 6　　導入済みおよび評価中のデータセンター セキュリティ ソリューション サプライヤ n=137



データセンター セキュリティ ソリューションのトップ サプライヤとしての認知度（回答者の認識）

自由回答形式の質問で、データセンター セキュリティ ソリューションにおけるトップ 3 のサプライヤはどこであるかを尋ねました。この評価基準は「純粋ブランド認知」と呼ばれており、全体的なブランド力がよくわかります。通常は、ベンダーの規模（製品ポートフォリオの範囲など）が大きければ大きいほど、ブランドの露出（TV コマーシャルや製品紹介など）が高ければ高いほど、この質問の評価も高くなります。総合的なブランド力は、製品や技術面でのリーダーシップをしのぎます。たとえば IBM は数十年間にわたってデータセンターの主力ベンダーの地位にありますが、他のベンダーほど幅広い製品を提供していないにもかかわらず、その地位を維持しています（大規模なビジネスの統合を経ても、IBM のブランドは損なわれていません）。総合的にはシスコが首位に立っています。その他の上位ベンダーには、消費者向けセキュリティ（McAfee）、デスクトップ OS およびアプリケーション（Microsoft）、幅広い IT ソリューション（HP）などの主要ブランドが挙げられています。データ セキュリティ分野、とりわけ仮想化での中心的な存在である VMware などの主要企業は、まだトップ 5 に食い込んでいません。

参照 7　　データセンター セキュリティ ソリューションの トップ サプライヤとしての認知度（回答者の認識）
n=137



データセンター セキュリティ ソリューション サプライヤのリーダーシップ

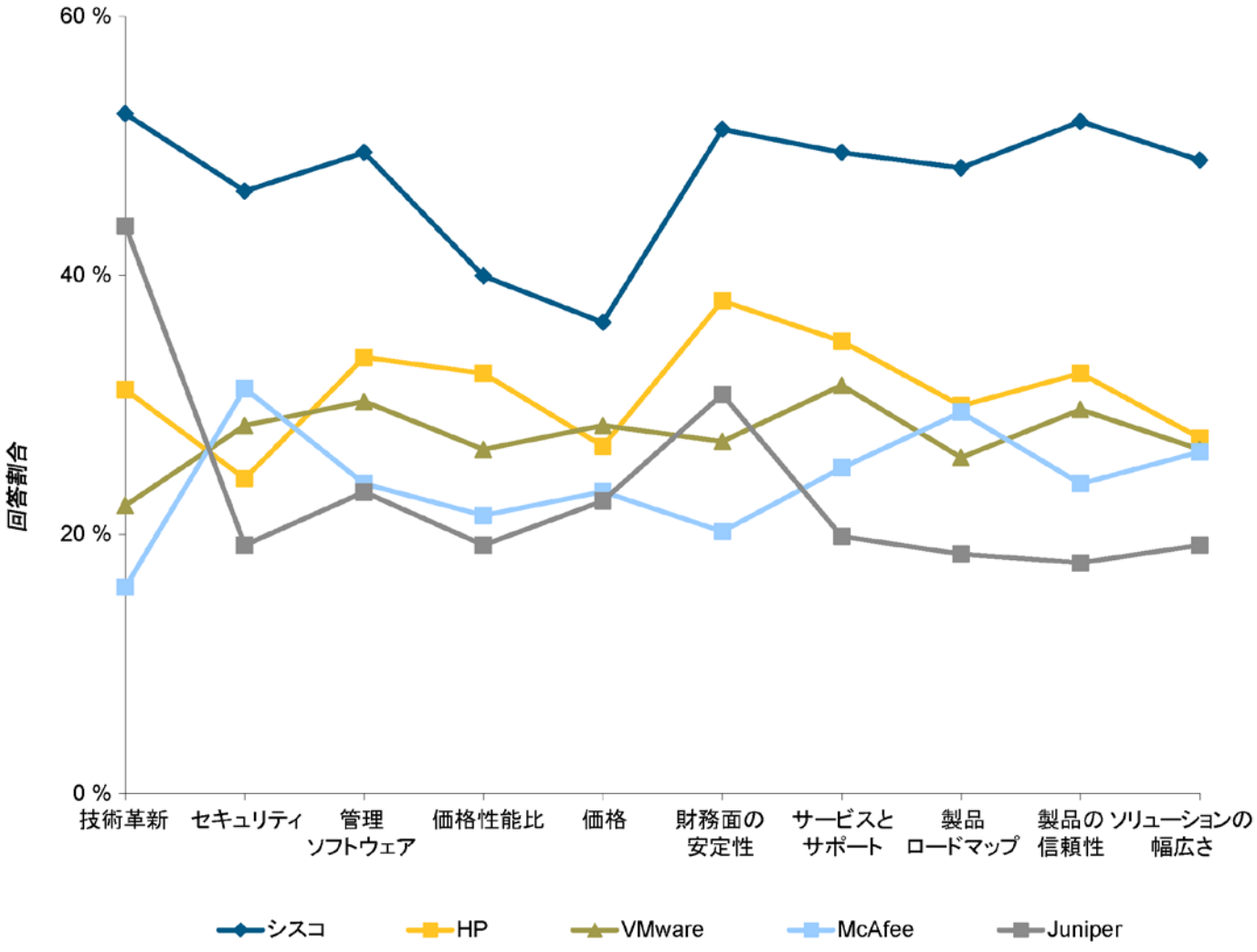
回答者に重要な購買基準を 10 個示し、それぞれの基準でトップ 3 に入るデータセンター セキュリティ サプライヤを 11 社のベンダーから選択してもらいました。次のグラフは、各基準についてそのベンダーをトップ 3 に選んだ回答者の比率です。

この種の質問は有名なサプライヤに有利になる傾向があります。そこで、偏りを排除するために、各サプライヤにどの程度なじみがあるかに基づいて回答者の比率を調整しています。次のチャートは、最も意見が多かったサプライヤ 5 社についての結果です。

シスコは全体的に高い評価を受けています（最も低いスコアでも、他者のスコアを上回っています）。多くの購買担当者がシスコを選択しているのは、シスコはセキュリティ分野にとどまらず、大きなビジョンを提供する戦略的なパートナーであるからです。シスコは、2012 年からデータセンターを対象とした一連のソリューションを新しく展開しており、現在はそれが Sourcefire 製品群として完全に統合されています。サービス プロバイダーのデータセンターにセキュリティ ソリューションを提供するうえでシスコの大きな弱点と言えるのは DDoS 緩和製品がないことですが、この弱点はまもなく解消されるものと考えられます。

参照 8

データセンター セキュリティ ソリューション サプライヤのリーダーシップ
n=137



レポート執筆者

Jeff Wilson

Cybersecurity Technology リサーチ ディレクタ
IHS Infonetics
+1 408.583.3337 | jeff.wilson@ihs.com
Twitter：@securityjeff

IHS INFONETICS RESEARCH に関して

Infonetics Research は、1990 年より情報産業に従事する国際的な市場調査およびコンサルティング アナリスト会社であり、現在は IHS（NYSE：IHS）の一部として活動しています。Infonetics は、世界の全地域で新たな技術や確立した技術を定義、追跡するリーダーとして、お客様がより効率的に計画立案、戦略化、競争ができるような支援をしています。

レポートの転載および顧客調査

IHS Infonetics のレポートあるいは顧客調査の抜粋の配布に関しては、以下にお問い合わせください。

南北アメリカ
+1 855 323-3363
+1 719 265-1535
Technology_US@ihs.com

ヨーロッパ、中東およびアフリカ（EMEA）
+44 1344 328300
Technology_EMEA@ihs.com

アジア太平洋：
+604 291-3600
Technology_APAC@ihs.com