IDC SOLUTION BRIEF

SDN データセンターのセキュリティソリューションのビジネス価値の評価

Sponsored by: Cisco

Pete Lindstrom　　Richard L. Villars
Matthew Marden
May 2015

概況

CTO、CIO、アプリケーションアーキテクトは、顧客へのサービスやビジネス成果を向上させるために、Systems of Engagement（SoE：システムオブエンゲージメント）や Systems of Insight（SoI：システムオブインサイト）に関連した広範のコンテンツサービス、ビッグデータ／アナリティクス、アーカイブ機能などを提供できるデータセンターを必要としている。そのためには、既存データセンターの強化や新たな地域における新規データセンター構築の加速、また、サービスプロバイダーが設計、構築、運用する先進的で高度なデータセンターの活用も必要となる。IDC ではビジネスとデータセンターのこのような変化を第 3 のプラットフォームへの移行と呼んでいる。

今日では、ビジネスに関するすべての変革は、ほぼすべてこの第 3 のプラットフォーム上で行われており、高付加価値で業界を変革する数十万、数百万のソリューションとサービスが存在し、エンドユーザーエクスペリエンスを変貌させる。この変革は、調達、設計、運用、開発、そして長期的なデータ／資産管理などを含む IT 部門のすべての側面に影響を及ぼす。この新たなデータセンターの世界は、よりダイナミックでデータ集約型であり、対処が必要なビジネスリスクを多くはらんでいる。その結果、次世代のネットワークアーキテクチャが重要な考慮事項となる。

この新たなアーキテクチャモデルでは、従来のネットワークアーキテクチャの技術／運用面の制約を解決し、第 3 のプラットフォームのワークロードが課すデータセンター要件を満たす必要がある。たとえば、ネットワークコントロールプレーンとデータフォワーディングプレーンを分離する Software-Defined Network（SDN; ソフトウェア定義型ネットワーク）は、クラウドコンピューティング環境を構築する上で企業が必要とする敏捷性と柔軟性をネットワークに提供する手段として考案されたものである。

シスコシステムズ（以下、シスコ）のアプリケーションセントリックインフラストラクチャ（ACI）は、自動プロビジョニングやプログラムによる管理、そして包括的なオーケストレーションに対するデータセンター運用者のニーズに対応することを目標としている。ACI では、データプレーンからコントロールプレーンを分離するのではなく、アプリケーションの要件を把握し、アプリケーションが仮想化されているかベアメタル上で実行されているかに関わらず、ネットワーク全体を自動化できるように設計されたポリシーモデルを適用する。シスコではこのアプローチを宣言型管理モデルと呼んでいる。宣言型管理モデルには、個々の自発的な協力またはコミットメントを通じて意図を相互に知らせるエージェントが含まれる。これを具体的に説明すると、たとえば、アプリケーションポリシーがその要件を宣言すると、基盤となるインフラストラクチャ（データセンタースイッチなど）は固有の機能に基づいて、それらの要件を満たす最善の方法を実行する、ということである。

クラウドコンピューティングのためのもう一つのネットワークのオプションは、OpenStack によって提供されている。OpenStack では、ネットワークサービスを消費する顧客のために、Neutron と呼ばれるデフォルトのフレームワークばかりでなく、ノースバウンドとサウスバウンドの API をセットで提供する。OpenStack のネットワークモデルはモジュール型アーキテクチャが特徴であり、各々の顧客は、要件に適したバックエンドを柔軟に選択できる。一部の顧客は最初はデフォルトのリファレンス実装で開始するが、その後、ユースケースとネットワークニーズに応じてベンダーが提供する拡張機能を利用する。

データセンターを変革させる要因

データセンターの運用と投資には、多くの外部要因が直接的／間接的な影響を及ぼしている。これらの要因は、ビジネス、社会／文化／政治、そしてテクノロジーの領域に及ぶ。

- **ビジネス**
  - **すべてのサービス化：**物理的資産／デジタル資産に対する支出モデルが変化し、社内の予算編成、コスト、投資の再構築が進んでいる。
  - **産業のデジタル化：**物理的なデジタルビジネスモデルからデジタルなビジネスモデルへの移行によって、データの増加率、パフォーマンスに対するニーズ、IT の機能要件が劇的に変化している。
  - **相互に関連するビジネス：**ビジネスのエコシステムの拡大により、企業／業種にまたがる相互接続とデータ共有の標準化が進展している。
- **社会／文化／政治**
  - **データ利用の規範：**個人データおよび知的財産の収集、保持、利用に関する人々の考え方と政府の政策が変化、細分化されている。
  - **データの悪用：**国、企業、犯罪組織により、大規模で組織的なサイバー戦争が行われている。
  - **顧客との接触／エンゲージメント：**ソーシャルメディアによって顧客と企業、顧客と顧客の間の直接的なエンゲージメントの場が生まれており、それによって新鮮でアップデートされた情報が恒常的に要求されている。
- **テクノロジー**
  - **IT のモジュール化：**クラウド／コンバージド／ソフトウェア定義型／ハイパースケールのパッケージングモデルによって、IT の基本ユニットの購入と管理が変化している。
  - **データの重圧：**顧客のエンゲージメントおよびビジネスに対する洞察獲得のためにサービスプロバイダーのデータセンターで生成、収集、アーカイブされるデータの量はますます増加している。
  - **可変的な IT：**短期的なモバイルキャンペーンやアナリティクスをサポートするために、キャパシティをごくわずかな期間だけ緊急に購入、配備、再配備することが必要となっている。

こうした要因が加速する、データセンターおよび IT 資産の再編や再調整も、企業の既存のワイドエリアネットワークに大きな影響を及ぼすことになる。企業は社内データセンターをサードパーティの施設に接続するための既存の接続経路を変更する必要がある。また、多くのロケーション間で、大量の情報を予見困難なパターンで移動することが必要になってくると、トラフィックの量や変動の大幅な変化への対処も必要となる。

最新のデータセンターにおけるセキュリティの役割

こうした変化とデータセンター ワークロードの急増の背景にあるのは、データセンター セキュリティに対する俊敏性と柔軟性のニーズである。セキュリティは各々のユースケースにおいて、完全性、忠実性、可視性、コンテンツのコントロール、データのコントロールなど異なる内容を意味している。IT 部門は、データセンター内および企業全体に渡る広範なセキュリティ機能を迅速かつ高い信頼性で設定、再設定、拡張するために使用できる共通のプラットフォームを必要としている。

ネットワークレベルでは、インラインのセキュリティ機能は監視機能（侵入検知）、ポリシー指向のセグメント化（ファイアウォール）、通信暗号化（仮想プライベートネットワーク）から構成される。しかし、企業では、使用状況やリスクのレベルによって区別することなく、データセンターのリソースを一つのユニットとして扱う場合が多い。このアプローチでは、単一の大きな「ゾーン」にすべてのリソースを投入し、そのゾーンの境界の入口／出口のポイント（データセンターへの「ノース」および「サウス」のアクセスポイントと呼ばれることもある）に防御を集中することが可能である。

データセンターがさまざまな事業部門、複数のユーザー層、多様なプラットフォームに対して、多くの異なる機能を提供する多面的な集合体へと成長、進化する中で、セキュリティはこれらのよりダイナミックで豊富なリソースを、標的を絞った脅威から保護しなければならない。企業は、より詳細なレベルでリソースの共有方法、通信の監視／暗号化方法を検討する必要がある。

現代のデータセンターでは、既存のコントロールの再配備が必要な個所、そしてサーバーとその他のリソース間での「East-West」の通信をカバーするために新たな機能を追加すべき個所を決定するために、侵入検知／防止システムばかりでなくファイアウォールによるセグメンテーションの配備方法を評価しなければならない。この評価の一部には、リソースの小規模な集合、すなわち、一般的にはアプリケーション レベルの特定と、アプリケーション間のトラフィックを管理するために、より多く監視やポリシーコントロールすることが必要となる。

データセンター全体に渡って配備されるコントロールが増加するのに伴い、一元的な集中管理機能が重要な要件となる。保護されるリソースのロケーションや使用状況がますますダイナミックになる中で、セキュリティ機能はこの新しいアーキテクチャに適応する必要がある。

本 IDC Solution Brief では、データセンターが変化する中で、セキュリティ製品を使用するユーザーを対象とした IDC 調査を取り上げ、それらのセキュリティ製品によって実現可能なビジネス上のメリットの定量化を行っている。これらのメリットには、IT 部門のセキュリティスタッフの業務生産性の向上（33.5%）、セキュリティ侵害／脅威による計画外ダウンタイムの削減（80.7%）、新規アプリケーション／サービスに対するセキュリティ配備の加速（63.8%）などがあげられる。また、ユーザー数 1,000 人の企業における年間ベースでのメリットは、信頼性の改善（4 万 8,700 ドル相当）、IT スタッフの作業効率の向上（7 万 1,700 ドル相当）、運用改善による生産性の向上（9 万 2,600 ドル相当）などである。

次世代データセンター向けセキュリティソリューションのビジネスメリット

次世代データセンター向けのセキュリティソリューションは、企業がデータセンターへの投資から最大の価値を生み出せるものでなければならない。このためには、これらのセキュリティソリューションは統合的かつポリシーベースで、堅牢、俊敏、スケーラブルであり、それによって価値を生み出すものである必要がある。これらの特徴を有する、適切に設計、導入されたセキュリティソリューションは、ビジネスを支援／推進するデータセンターの能力を損なわずにセキュ

リティソリューションの管理と配備に要する時間と労力を節減し、業務／ビジネスに対するセキュリティ脅威の影響を軽減することによって価値を持つ。つまり、次世代のデータセンターを実現するセキュリティソリューションには、以下のようなの特長が必要となる。

- **統合による効率向上とリスク軽減：**企業の従来のデータセンター環境をサポートしているソリューション、および次世代のデータセンター環境で使用される他のセキュリティ製品の両方と統合可能なセキュリティ製品によって時間の節減およびリスクの軽減が可能である。これは、統合によって、セキュリティチームによるポリシー再適用時間の最小化、高コストで非効率な IT セキュリティのサイロ化の解消、アプリケーション／サービスが潜在的なセキュリティ脅威にさらされる時間の短縮が可能になるためである。
- **簡素化による管理負担の軽減：**次世代データセンターのセキュリティ製品は、自動化とオーケストレーションに依存する環境で使用される。このような環境に適合するためには、セキュリティ製品自体もサービスとしてのプロビジョニングが可能となるようにポリシーベースでなければならない。これは、次世代データセンターの全体的なアーキテクチャをサポートするだけではなく、IT スタッフがセキュリティの設定、構成、配備に関わる運用時間を節減する場合に IT 部門のセキュリティスタッフの生産性にとってもプラスとなる。
- **堅牢な機能によるセキュリティ脅威の影響の最小化：**次世代データセンターのセキュリティ製品は、データセンターと外部間、そしてデータセンター内のトラフィックのすべてをカバーするものであり、全範囲のセキュリティ機能を提供できなければならない。これによって、企業ではセキュリティ脅威のユーザーやビジネスへの影響の最小化、ユーザーへの生産的な時間の供与、そして事業中断の最小化が可能になる。
- **アプリケーションを通じてビジネスを支援する俊敏性とスケーラビリティ：**次世代のデータセンターはアプリケーション開発サイクルの加速とアプリケーションの管理負担軽減によってビジネス業務を支援できるように構成される。アプリケーションやサービスを速やかに市場投入するためには、セキュリティ製品は、必要な時に、最小限の時間で配備される必要がある。

シスコ アプリケーション セントリック インフラストラクチャ

ソフトウェア定義型ネットワーク（SDN）は、データプレーン機能からコントロールプレーン機能が分離されるが、限定的な技術的用語で定義される場合がある。ソフトウェア定義型セキュリティでは、SDN の理念や基本的なアーキテクチャが利用されているが、より多くの環境への統合によって機会が広がっている。SDN の「ハブとスポーク」アプローチにおいては、セキュリティポリシーが定義、評価されるコントローラーと、ポリシーを実施する実行ノードが結合され、すべてが動的にリアルタイムで行われる。アプリケーション層まで抽象化されたポリシーの利用によって、該当するポリシーが適切な実行ノードで適用されることが可能となり、柔軟性および使用されているアプリケーションのコンポーネントとの整合性が維持される。結果として、セキュリティアーキテクチャは効率的な管理が容易になり、効率を最大化できる可能性が出てくる。

シスコのアプリケーションセントリックインフラストラクチャ（Application Centric Infrastructure：ACI）は、現代のデータセンターのデータ／セキュリティのニーズに対応できるように設計されている。これは、一元集中的なコントローラーである APIC（Application Policy Infrastructure Controller）によって管理される。APIC は、データセンターの物理／仮想両方のすべてのセキュリティデバイスをコントロールする。これによって、セキュリティデバイスは、保護しなければならないリソースと緊密に整合される。このコントローラーは、シスコのネットワークおよびセキュリティデバイスのプロビジョニングと管理を可能にし、サードパーティのセキュリティベンダーのエコシステムもサポートする。そして、サードパーティのサポートのために、より多くの機能が組み込まれている。

Cisco ACI は、企業が既存のセキュリティアーキテクチャを導入することで物理的なセキュリティコントロールへの投資を維持しつつ、ハードウェアまたは仮想マシンへの機能コントロールの追加でにより重要性がますます高まっている East-West の通信を保護する。現代の企業のダイナミックなリソースに対応することで、ポリシーの作成やアプリケーションプロファイルへの適合、そして環境全体への配信を可能にする。リソースが移動した場合には、適切なポリシーはリソースと共に移動する。

シスコのセキュリティソリューションにすでに多大な投資を行い、既存のセキュリティポリシーを確立している企業に対して、ACI はデータセンターを完全に見直すのではなく、データセンターアーキテクチャの変革を安全に進める方法を提供する。ACI は、それと同時に、仮想化と分散アーキテクチャの新たなニーズに対処することが可能であり、適切なセキュリティレベルを企業に確実に提供する。

次世代データセンター向けセキュリティソリューションのビジネスメリットを定量化する

表 1 は、継続的な IDC の調査に基づいて、企業が次世代データセンターにおけるセキュリティソリューションの使用によって実現できるビジネス価値の測定指標を示したものである。

図 1 は、ユーザー数 1,000 人の企業における次世代データセンターのセキュリティソリューションの使用に関連する IT スタッフとユーザーの生産性向上の年間価値を示したものである。

表 1

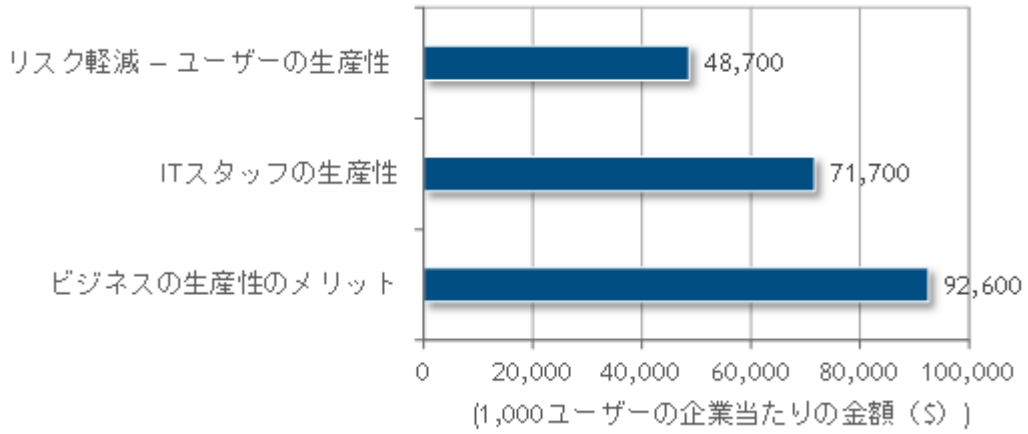
次世代データセンターにおけるセキュリティ製品利用による改善

	(%)
IT スタッフの生産性メリット	
セキュリティ管理の時間節減	33.5
プロアクティブに識別できるセキュリティ脅威の増加	50.9
セキュリティ脅威への対応時間の短縮	82.1
リスク軽減– ユーザーの生産性のメリット	
計画外ダウンタイムの低減	80.7
ビジネスの生産性のメリット	
セキュリティ配備に要する時間の短縮	63.8

Source: IDC, 2015

図 1

1,000 ユーザーの企業における次世代データセンターの セキュリティソリューション使用の一般的な年間便益額



Source: IDC, 2015

付録：方法論

本文書で使用したデータは、データセンターでセキュリティソリューションを使用している企業を対象に IDC が毎年実施しているインタビューに基づいて作成した。ビジネス価値の結果は IT ユーザー数が 1,000 人の平均的企業におけるメリットの金額に換算することによって正規化されている。IT スタッフの業務に関連する便益の定量化にあたっては、時間節減および効率向上に、平均年間給与額（会社負担分を含む）として 10 万ドルを乗じた。また、その他の IT 以外の従業員の時間節減と生産性向上の便益の定量化にあたっては、同給与額として 7 万ドルを乗じた。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年に渡り、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

グローバル本部

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com