

クラウド対応データセンター のセキュリティについて

目次

エグゼクティブサマリー	3
はじめに	3
データセンターにおける新たなセキュリティ問題	4
バーチャリゼーション	4
分散型アプリケーション・アーキテクチャ	5
Storage over IPネットワーク	6
ボットネットを使用した最先端のDDOS攻撃	7
クラウド対応データセンターのセキュリティ要件	7
アプリケーション識別	8
IDベースのアクセス・エンフォースメント	8
大容量で拡張性に優れたプラットフォーム設計	9
集中管理	9
まとめ—ネットワーク・セントリックな手法によるデータセンターのセキュリティの保護	10
ジュニパーネットワークスについて	11

図目次

図1: 新しいデータ・センター・インフラストラクチャで増大するリスク	4
図2: バーチャル・サーバー・ネットワーキング	5
図3: マッシュアップとSOAファンアウトの影響	6
図4: 複数のアプリケーションによるストレージレイの共有	7
図5: データセンターのセキュリティ・エンフォースメント参照モデル	10

エグゼクティブサマリー

データセンターは、サーバー、アプリケーション、その他のリソースの統合が進められ、コスト削減と効率向上を実現するための新しいテクノロジーが採用されたことにより、大きく変化しています。サーバー・バーチャライゼーション、分散型アプリケーションツール、IPベースストレージなどのテクノロジーは、データセンターのリソースの使用効率を最大化することには役立ちますが、その一方で重要な資産を保護することは非常に難しくなります。

サイバー窃盗や高度化したマルウェアに加えて、データ・センター・テクノロジーに潜んでいる新たな脆弱性にも対応する必要があります。これまで、データセンターのセキュリティは、その周辺レベルとサーバーレベルに集中していました。しかし、この手法は、最新のシステムアーキテクチャの情報とリソースを保護できるほど包括的な手法ではありません。

新たなリスクを適切に管理するには、現在のデータセンターのセキュリティ対策を再評価し、サービスの完全性を保証できるネットワーク・セントリックな機能を新しく導入する必要があります。ネットワークはデータセンター内のあらゆるデバイスに接続されているので、セキュリティの管理ポイントとして最適です。ネットワーク・セントリックな手法でデータセンターのセキュリティを実現した場合、拡張性、セキュリティポリシーの定義とエンフォースメントの統合、アプリケーション・トラフィックの監視能力、業務のオーバーヘッドの削減などの利点が得られます。

はじめに

データセンターは、業務上の必要性および技術革新に後押しされて、急速な進化を遂げています。コストを削減し、柔軟性を得るために、データセンターの統合が進められ、バーチャライゼーション、新しいアプリケーション・アーキテクチャ、クラウド・コンピューティングなど、さまざまな新しいテクノロジーが採用されています。

これらの傾向は、現在の経済環境によって加速しています。データセンターの統合により、アクセス頻度の高いシステムをリモートオフィスから中央のデータセンターまたはサードパーティ・クラウド・プロバイダに移動することができ、効率が向上します。サーバー、アプリケーション、その他のリソースを統合することで、リソースの利用率が上がり、多くの拠点でITスタッフを常駐させる必要性がなくなります。一部のアプリケーションをクラウド・サービスとして提供することによって、常時利用可能な集中化されたリソースに安全にアクセスする必要がある在宅勤務者や営業所の従業員をサポートしやすくなります。

同時に、テレフォニープレゼンス、インスタント・メッセージ、ウィキ、ブログ、ソーシャル・ネットワーキングなどの新しいコラボレーションツールによって、物理的に離れている従業員同士でも密に協力して作業を進めることができます。さらに、アプリケーション開発でサービス指向アーキテクチャ(SOA)などの分散型手法を採用すると、高度な分散型アプリケーションを構築できます。

これらの傾向は、データセンターのアーキテクチャ、およびデータセンター内のデータとシステムを十分なセキュリティで保護するために解決する必要がある問題に、大きな影響を与えています。従来のデータ・センター・モデルでは、アプリケーション、計算リソース、およびネットワークは緊密に連携しており、すべての通信が重要ポイントに置かれたセキュリティデバイスを通じていました。しかし、サーバー・バーチャライゼーションやWebサービスなどのテクノロジーによってそのような連携が消滅し、システム間がメッシュ状に接続された結果、大小さまざまな新しいセキュリティリスクが生じています。

最新のデータ・センター・アプリケーションのセキュリティを保護するには、アプリケーションの識別とIDベースの制御を実現し、ポリシーとコンプライアンスの集中管理機能を備え、高い拡張性と柔軟性を持つ包括的なセキュリティツールをネットワークに導入する必要があります。バーチャル化されたクラウド対応環境向けのセキュリティソリューションを導入する場合、これらの新たなセキュリティ問題を認識する必要があります。

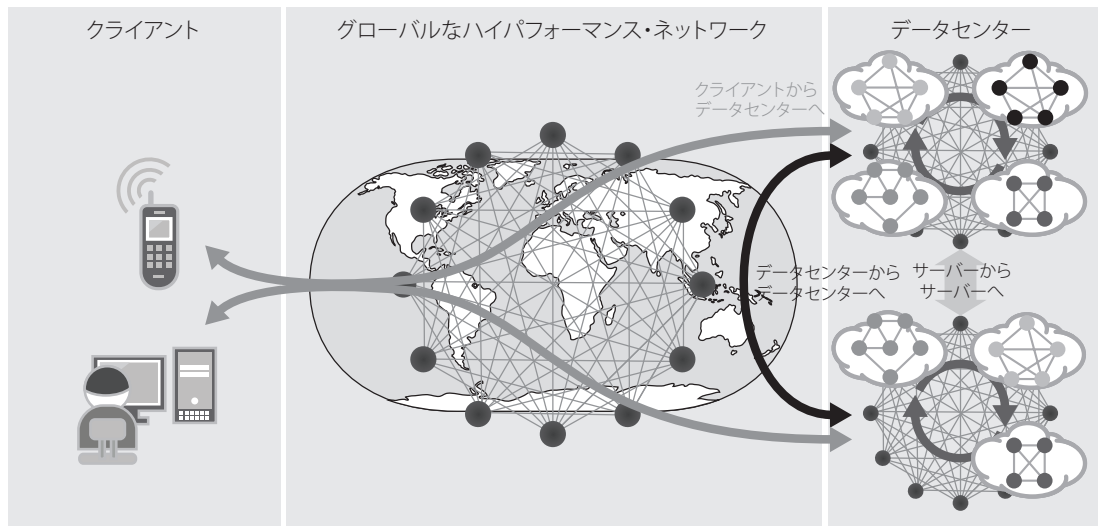


図1:新しいデータ・センター・インフラストラクチャで増大するリスク

データセンターにおける新たなセキュリティ問題

情報ネットワークおよび情報システムでは、情報の機密性、完全性、および可用性をセキュリティコントロールによって制御します。複数の大規模データセンター内のアプリケーション、データ、その他のリソースが統合された場合、システムに1つ欠陥が存在することでもたらされるリスクは増大します。従来は1つのアプリケーションを1台のサーバーでホストしていましたが、現在は複数のアプリケーションまたはコンポーネント、あるいはその両方をバーチャル化された複数のサーバーでホストしています。1台の物理サーバーで情報漏洩が発生すると、膨大な数のアプリケーションやユーザーに影響を及ぼします。

現在のデータ・センター・ネットワークでは、次に示す4つの新しいテクノロジーの重要性が高まっていますが、それによって解決しなければならないセキュリティ上の重大な問題も生じています。

- ・ サーバー・バーチャリゼーション
- ・ 分散型アプリケーション・アーキテクチャ
- ・ IPベースのストレージ・ネットワーク
- ・ ボットネットを使用した最新のDoS攻撃

バーチャリゼーション

データセンターの統合における重要なテクノロジーであるサーバー・バーチャリゼーションによって、サーバーのリソース使用率を最大化し、必要なスペース、電力、および冷却を削減することができます。ただし、バーチャルマシン (VM) 内部およびバーチャルマシン間で行われている処理を監視および制御することが難しいため、重大なセキュリティリスクが新たに発生します。

バーチャル・サーバー・テクノロジーによって、1台のホストマシン上で複数のOSインスタンスを動作させることができます。各オペレーティング・システムは、固有の「バーチャルCPU」、メモリ、I/Oの各リソースを備えたバーチャルマシンを構成します。最近では、サーバー・バーチャリゼーションが拡張されて、複数のホストで構成されるクラスター上で複数のOSインスタンスを動作させる機能が追加されています。その結果、アプリケーションは、1台のサーバーの有限の容量を超えるリソースプールを使用できます。さらに、バーチャルマシンをホストからホストへ移行したり、ホスト間で複製したりすることができるため、需要の増減に応じて動的にリソースを割り当てることができます。

バーチャル・テクノロジー・ベンダーは、同一ホスト上のバーチャルマシン間の通信を円滑化するために、イーサネットスイッチをシミュレートするソフトウェアを開発しています。バーチャルスイッチは各物理ホスト上で動作し、ゲストVM間の接続を実現します。このサーバー内ネットワークの内部では、一部のVMを同一のブロードキャスト・ドメインに接続し、残りのVMを複数のブロードキャスト・ドメインに接続することができます。

VMホスト内スイッチは、物理ネットワーク監視用のデバイスでは監視できません。1台のサーバー上の複数のVM間で送受信されるト

ラフィックは、サーバー外部のデータ・センター・ネットワークに送出されることはなく、通常のネットワークベースのセキュリティ・プラットフォームによって隠蔽されています。このようにサーバー内のバーチャルマシン間通信を監視および制御する手段がないということは、重大なセキュリティリスクを生みます。バーチャル化されたドメイン内にエンフォースメント・ポイントが存在しないため、ワームなどの不正トラフィックが何のチェックも受けずにバーチャルマシン間で、場合によっては物理的なデータ・センター・ネットワークに、伝播する可能性があります。このように監視する手段が存在しないことは、コンプライアンス上でも問題になります。そのため、このようなインフラストラクチャの新しい階層のセキュリティを保護するための新たなセキュリティツールを導入し、ベストプラクティスを実行する必要があります。

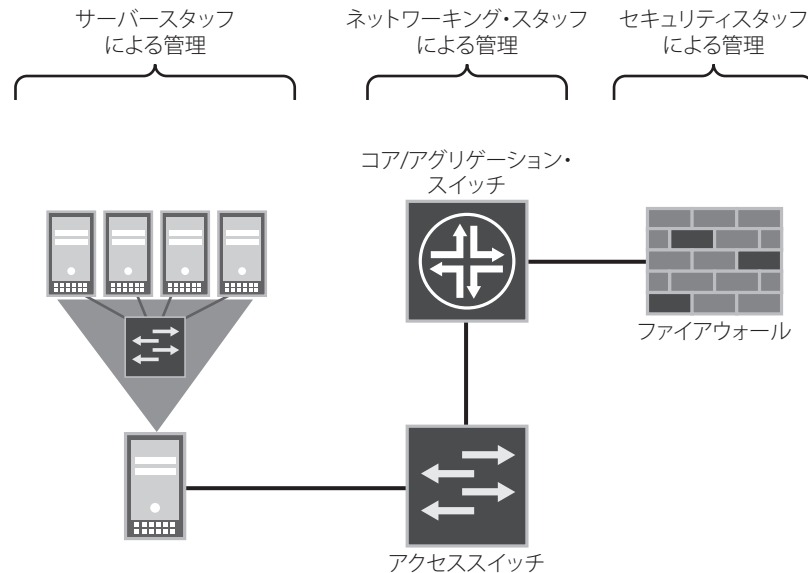


図2: バーチャル・サーバー・ネットワーキング

分散型アプリケーション・アーキテクチャ

現在は、モノリシック・アプリケーション開発から、再利用可能な共通サブコンポーネントを利用する分散型アプリケーション・アーキテクチャへと、大きな転換が行われています。分散型アプリケーション・アーキテクチャでは、アプリケーション開発の速度と効率が向上しますが、トランザクションごとに複数のフローが存在する、高度に分散された通信パターンが作成されることによるリスクが発生します。

たとえば、インターネット・アプリケーションの多くは、異なるサーバーから配信される異なる要素のマッシュアップです。たとえば、「igoogle」セッションは、異なるサーバー上で動作する複数の専用アプリケーションにアクセスし、返された結果を集約して、ユーザーのブラウザに配信する必要があります。このようなアプリケーションの多くは、サービス指向アーキテクチャで構築されています。SOAでは機能が複数の単位、すなわちサービスに分割されています。サービスはネットワーク経由でアクセスできるように開発されているため、サービスを組み合わせることで再利用することによってアプリケーションを構成できます。これらのサービスは、サービス間でデータを渡したり、複数のサービスを統合して1つのアクティビティを実行したりすることによって相互に通信します。

結果的に、各マッシュアップ・アプリケーション・フロントエンドが通常は大量のバックエンド・アプリケーションに接続し、ユーザーセッションごとにファンアウト階層が構築され、クライアントによる対話操作のたびに大量のTCP接続が使用されることとなります。このような高度な分散型環境のセキュリティを保護するには、これらのフローをすべて、1つのトランザクションを実行する1人のユーザーに関連付ける機能が必要です。ユーザー情報が適宜提供され、ユーザー信用情報に基づいて各アプリケーション要素への適切なアクセスが許可されるように、ユーザーIDと信用情報を複数のマッシュアップ・アプリケーションおよびバックエンド・サービスに送信し共有させる必要があります。

マッシュアップ、SOA、および同様の分散型アプリケーション・テクノロジーには多くの利点がありますが、アクセス権を付与するのは困難です。高度な分散型アプリケーション環境では、データプライバシーというセキュリティ上の問題もあります。現在、多くのシステムでクライアント通信が狙われるようになり、通信ストリームが盗聴される可能性が高まっているため、通信を暗号化することは必須になっています。

SOAベースのアプリケーションでXMLを使用することによってもたらされるセキュリティ上の問題もあります。XMLは、大量のデータセット、すなわちパケットを使用するという特徴があります。サーバー間でそのような大量のデータセット（およびパケット）を転送するには、高帯域のTCPセッションを複数必要としますが、各セッションをセキュリティ・エンフォースメント・システムによって検査する必要があります。データセンター全体でファイアウォールから必要とされる総帯域幅は大幅に増加します。

分散型アプリケーション・アーキテクチャには、短期間でアプリケーション開発や、アプリケーション・コンポーネントの再利用といった大きな利点がありますが、アプリケーションフローを特定のユーザーに関連付けることができる拡張性の高いハイパフォーマンスなセキュリティソリューションが必要になります。

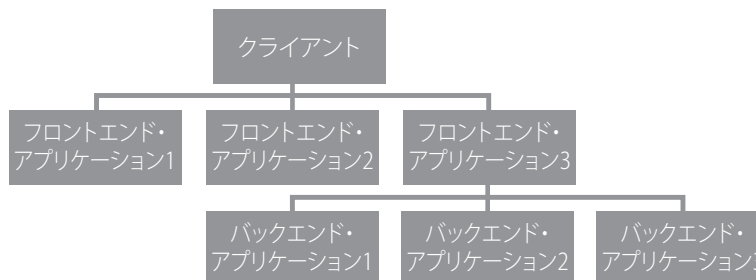


図3: マッシュアップとSOAファンアウトの影響

Storage over IPネットワーク

経済的な理由により、多くの組織でIPベースのストレージ・テクノロジーが配備されています。共通のIPインフラストラクチャを活用してデータ通信、音声通話、映像配信をサポートすることによって、規模の経済性が実現し、運用が簡素化されます。また、ネットワーク・ファイル・システム（NFS）や共通インターネット・ファイル・システム（CIFS）などのネットワーク接続ストレージ（NAS）テクノロジーや、iSCSIなどのストレージ・エリア・ネットワーク（SAN）テクノロジーによって、大容量のストレージプールを導入できるようになり、必要なネットワーク相互接続の数や管理の手間が減少します。さらに、必要なストレージ容量の予測精度が向上し、ストレージアレイの容量増加を詳細に管理できるといった利点も得られます。

Storage over IPネットワークの導入によって、柔軟性とコスト面での利点がありますが、セキュリティリスクも高まります。ストレージ・ネットワークはIPインフラストラクチャの一部のため、DoS攻撃やその他のマルウェア攻撃から保護する必要があり、それを怠れば重要なデータの利用不可やデータの破損、アプリケーションが正常に動作しなくなるといった問題が発生する可能性があります。IPネットワーク上の競合によってデータ可用性が失われる場合もあります。たとえば、レイテンシやデータロスの発生を嫌うストレージトラフィックが、大量のデータ通信や映像配信の影響を受ける可能性があります。

ストレージアレイはさまざまなアプリケーションにアクセス可能なため、権限昇格が行われる可能性もあります。新しいアプリケーションがオンライン化されることによって、ビジネスに欠かせないデータとそうでないデータが同じアレイ上に存在することも珍しくありません。ストレージベンダーは、アレイ上のストレージアクセス（データ保存時）を保護するツールは提供していますが、それらのツールはネットワーク間を移動するデータ（データ移動時）の脆弱性は解決しません。IPベースのネットワーク上にストレージを統合することで利益を得るためには、データセンターのIPインフラストラクチャ全体のデータの可用性、完全性、および機密性を保証する機能が必要です。

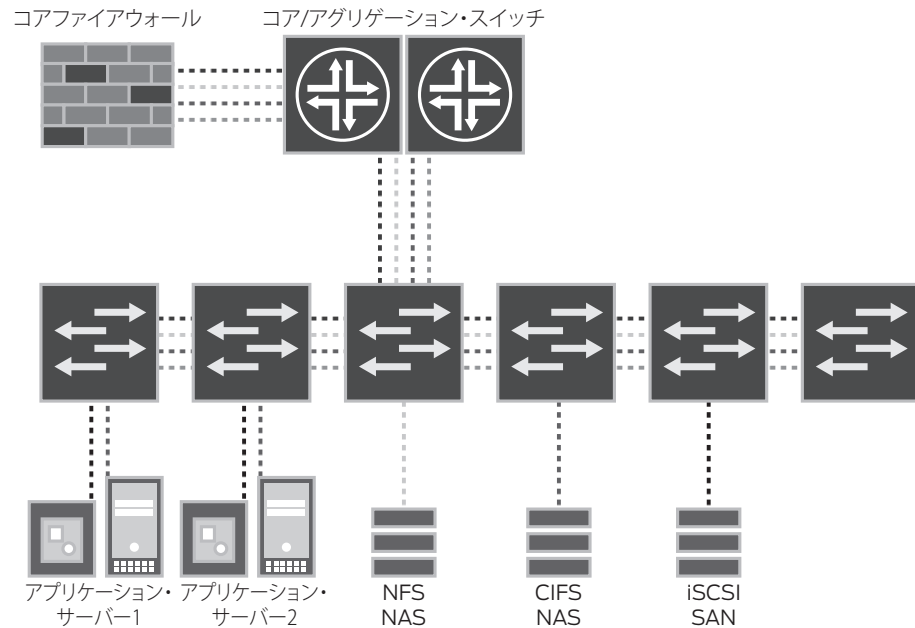


図4:複数のアプリケーションによるストレージアレイの共有

ポットネットを使用した最先端のDDoS攻撃

サイバー攻撃の頻度と巧妙さが増すことによって、重大で持続的なセキュリティ上の課題が生じます。従来は、「ブラックハット」コミュニティに信頼性を持たせるために、悪意のあるハッカーがランダムにシステムに狙いを定めていました。しかし、現在では、ブラウザベースの「クラウド」コンピューティング、モバイル・データ・プラットフォーム、ソーシャル・ネットワーキングの組み合わせによって新しいタイプの脅威が発生しています。すなわち、誰にも気づかれずにWeb経由で伝播したマルウェアが高度に組織化されたポットネットを構成し、ポットネットがネットワークにコールバックチャンネルを開いて機密データを漏洩させます。現在、クライアント側攻撃の65%が、ブラウザ・エクスプロイトによるものです。サイバー犯罪者は、ユーザー作成コンテンツが公開されているWebサイト、サードパーティ広告、高トラフィックWebアプリケーションの内部に不正なコードを埋め込んで、サーバーとクライアントの情報を漏洩させます。データが漏洩した場合、その事実の公表が義務付けられたことにより、その損害はより多くの人が知ることになります。近年、民間部門と公共部門の両方から絶え間なくデータ漏洩の被害が公表されています。従来のセキュリティメカニズムでは、OSエクスプロイト、ブラウザ攻撃、そして最近増加しているプラグイン/ウィジェットの脆弱性を通じて複数の前線攻撃を仕掛けるサイバー犯罪者に対する十分な防御力を提供できません。

クラウド対応データセンターのセキュリティ要件

今日のデータ・センター・インフラストラクチャのバーチャル化された分散システムで利用されている新しいテクノロジーによってもたらされるリスクを効果的に管理するには、現在のセキュリティ対策を再評価し、新しいセキュリティソリューションを導入する必要があります。データセンターのセキュリティの大部分は、ホストベースの侵入検知、アイデンティティ・エンフォースメント、アンチウィルス、その他のソフトウェアエージェントをインストールすることによって、サーバーレベルで適用されています。しかし、この手法は拡張性に乏しく、多彩なネットワーク接続デバイスに対応できないため、運用面で大きな問題が生じます。

異機種が混在し、常に変化し続けるデータ・センター・インフラストラクチャには、そのあらゆる部分で動作する統合されたセキュリティレイヤーが必要です。そのようなネットワークは、伝送されているアプリケーション・トラフィックの監視機能を備え、ポリシー・エンフォースメント・デバイスを実装する場所として最適です。マネージャは、次の特徴を持つネットワーク・セントリックなセキュリティソリューションを追求する必要があります。

アプリケーション識別

データセンターの資産を保護するには、アプリケーションのコンテキストおよび伝送内容を識別できるだけの十分なインテリジェンスを備えたエンフォースメント・ゲートウェイ、ファイアウォール、監視システムなどのネットワークセキュリティ製品が必要です。ポリシー定義およびセキュリティ・エンフォースメントという観点から見ると、従来のTCP/IPセッションの「5タプル」は、ビジネス・セキュリティ・ポリシーを定義または設定するには不十分です。

セキュリティ製品には、特定のアプリケーション・インスタンス内で実行できるアクションを正確に定義できる、アプリケーション識別機能が必要です。また、アプリケーションの使用状況プロファイルやその他の重要なアプリケーションレベルの情報を収集するために、アプリケーション・インフラストラクチャ内部の監視機能が必要です。

前述したように、今日のデータセンターでは、共有ホストまたはリソースプール上で複数のアプリケーション・インスタンスが動作する可能性があります。アプリケーションを区別するために、異なるTCPポート番号または異なるバーチャルIPアドレス上でアプリケーションを動作させる手法があります。この手法は、アプリケーション・インスタンスを新たに追加するたびに、ネットワーク・セキュリティ・ポリシーを変更して使用するTCPポート番号またはバーチャルIPアドレスを追加する必要があるため、運用面で非常に問題があります。

最近のアプリケーションは、HTTP URLまたはSQL Bindのプリペンド値のようなアプリケーション固有の状況依存データを使用して、アプリケーション処理要求を適切なアプリケーション・インスタンスに転送します。そのため、単純にポート80からアプリケーション・サーバーのIPアドレスに接続（すなわちポート80からgoogle.comに接続）しているというだけでは、セッションが業務用なのか私用なのかをネットワークおよびセキュリティの運用チームが判断できません。

TCP/IPのヘッダー情報にのみ依存するのではなく、別の方法でアプリケーション・インスタンス、アプリケーション・トランザクション、およびアプリケーション・アクションを識別できる新しいタイプのセキュリティツールが必要になります。プロトコル属性のような内部特性に基づいてアプリケーションを識別する機能は必要不可欠です。詳細な監視機能がなければ、規制やビジネスプロセスで要求されるレベルでセキュリティを保護することはできません。

IDベースのアクセス・エンフォースメント

送信元IPアドレスだけで判断するのではなく、ユーザーIDに基づいてアプリケーションおよびリソースへのアクセスを制御する機能も必要です。従来は、ユーザーロケーション（IPアドレスで表現される）を管理し、その情報に基づいてアクセス権限を割り当てていましたが、今日の従業員は社外を移動しながらデータセンター内の複数のサーバー上で動作するアプリケーション要素に接続するので、従来の手法は使用できません。代わりに、IT部門は、あらゆるタイミングであらゆる場所からデータセンターに接続するあらゆるユーザー（従業員、請負業者、ベンダー、その他の定義済みロール）に、ユーザーロールに基づいてアクセス権を提供できるようにする必要があります。

IPアドレスは、たとえばモバイルユーザーがある場所から別の場所に移動しているために、ユーザーに一時的に割り当てられているだけの可能性があるため、ユーザーアクセスをロケーションだけで判断して許可または拒否することはできません。また、ネットワークアドレス変換（NAT）およびプロキシ・ネットワークで変換された大量のアドレスは、さまざまなロールのさまざまなユーザーに割り当てられる可能性があり、特定のユーザーには関連付けられていません。

多数のアプリケーションが存在するクラスタへのユーザーアクセスを制御するには、IDとロールに基づいたセキュリティポリシーを設定できるネットワーク・セキュリティ・ソリューションが必要です。それらの製品には、ユーザーIDをアプリケーション・アクセス情報に関連付けて、これに基づいてセキュリティを判断する機能が必要です。また、複数のデータセンターにアクセスするコラボレーションツールの使用が増加している状況に対応するために、アイデンティティ・フェデレーション（IF）機能を備えたネットワーク・セキュリティ・ソリューションも必要です。IFは、外部計算環境から提供されるサービスを、セキュリティを保護しながらシームレスに統合できる機能です。

業界内では、異なるネットワーク間でIDと権限に関する情報を交換し、共通するユーザーIDの概念を共有することを支援する目的で、SAML (Security Assertion Markup Language)、XACML (Extensible Access Control Markup Language)、IF-MAP (Interface for Metadata Access Point) など、多くの標準テクノロジーが規定されています。これらのテクノロジーを使用することで、ネットワーク・セキュリティ・デバイスは、ID属性に基づくポリシー設定を容易に実行できます。セキュリティソリューションを検討する場合、これらの標準テクノロジーや、その他のIDスタア・テクノロジーをサポートしていることを重視する必要があります。

大容量で拡張性に優れたプラットフォーム設計

データセンターのセキュリティ保護を目的とするネットワークベースのデバイスには、今日のアプリケーションで扱われる多様で大容量のトラフィックを処理できる能力が必要です。データセンター内部のファイアウォールには、極めて高いスループットレートでの処理能力、および複数の内部ドメイン間でLANレートで伝送される大量のトラフィックを検査および制御できる能力が必要です。

また、データセンターのファイアウォールは、大量のセッションの開始と終了を短時間で処理する必要があります。今日のデータセンターでは、膨大な数のユーザーが特定の計算リソースにアクセスしています。その結果、ファイアウォールには、数万件の新しいセッションの開始と既存のセッションの終了を処理すると同時に、数百万件のセッションを管理する能力が必要です。

データセンターに対する要求、すなわちストレージトラフィックに必要とされる信頼性およびSOA/マッシュアップ・アプリケーション・アーキテクチャに伴うTCPセッション数と大きなパケットサイズを考えると、極めて高い処理能力を持つ専用ハードウェアとして設計されたファイアウォールを使用する必要があります。また、データセンターのセキュリティ・プラットフォームは、ビジネスの成長に合わせて段階的に拡張できるように設計する必要があります。そのように設計することで、サービス処理能力を必要に応じて追加できるだけでなく、その追加に合わせてネットワークを物理的または論理的に再設計する必要がありません。

集中管理

今日のデータセンターは高度に分散化および複雑化しており、データ・センター・インフラストラクチャ全体に一貫したセキュリティポリシーを導入することは難しい問題です。そのためには、統合されたセキュリティポリシーの定義、コンプライアンス情報の集約など、すべての機能を一元管理できる管理コンソールなどを備えた包括的なセキュリティソリューションが必要です。

堅牢な集中管理システムでは、ユーザー、アプリケーション、およびリソースドメインをきめ細かく制御できる具体性およびエンフォースメント・ポイントごとにカスタマイズする必要のない抽象性を併せ持つセキュリティポリシーを定義できます。ポリシーを一元的に作成できるので、マネージャは、データセンター内のシステムごとにセキュリティポリシーを定義する必要はなく、ポリシーの寄せ集めによって潜在的な脆弱性が生じることも回避できます。

集中管理システムは、ポリシー定義を統合できるだけでなく、他の分野のセキュリティ運用オーバーヘッドを大幅に減らすこともできます。今日のデータセンターには、スイッチ、ルーター、サーバー・プラットフォーム、オペレーティング・システム、アプリケーション・プラットフォーム、アプリケーション・インスタンスなど、さまざまなハードウェアとソフトウェアが導入されています。これらのシステムをすべて安全かつ最新の状態に維持するには、大変な労力を必要とします。さまざまな機器のアップデートとパッチを自動的に受信し、ITスタッフが手動で広めることができる管理システムを導入することによって、その労力を大幅に減らすことができます。たとえば、集中管理システムが自動的に検索およびダウンロードした最新の脆弱性に対するパッチを、オペレータの都合の良いときに管理された方法でさまざまなエンフォースメント・ポイントに手動で適用できます。

最後に、インテリジェントなセキュリティ情報およびイベント管理 (SIEM) 機能を備えた集中管理ツールをネットワークベースのセキュリティ・コンプライアンスと接続すると、アプリケーション使用状況とユーザー・アクセス・パターンを詳細に監視し、リアルタイムに、または履歴として、表示することができます。このように統合された情報は、コンプライアンス・レポートの生成、監査、その他の規制要件への対応に欠かせません。また、一元化されたSIEMシステムによって、IT部門がデータセンターのリソースとインフラストラクチャを最適化するために必要な情報を入手できます。SIEMツールには、コンテキストおよびトランザクションの分析機能など、綿密な分析機能が必要です。IT部門は、これらの機能を活用して詳細なL7のディープ・インスペクション (DI) イベントをネットワークフロー情報と相互に関連付けることによって、アプリケーション使用状況の傾向をリアルタイムに監視できます。

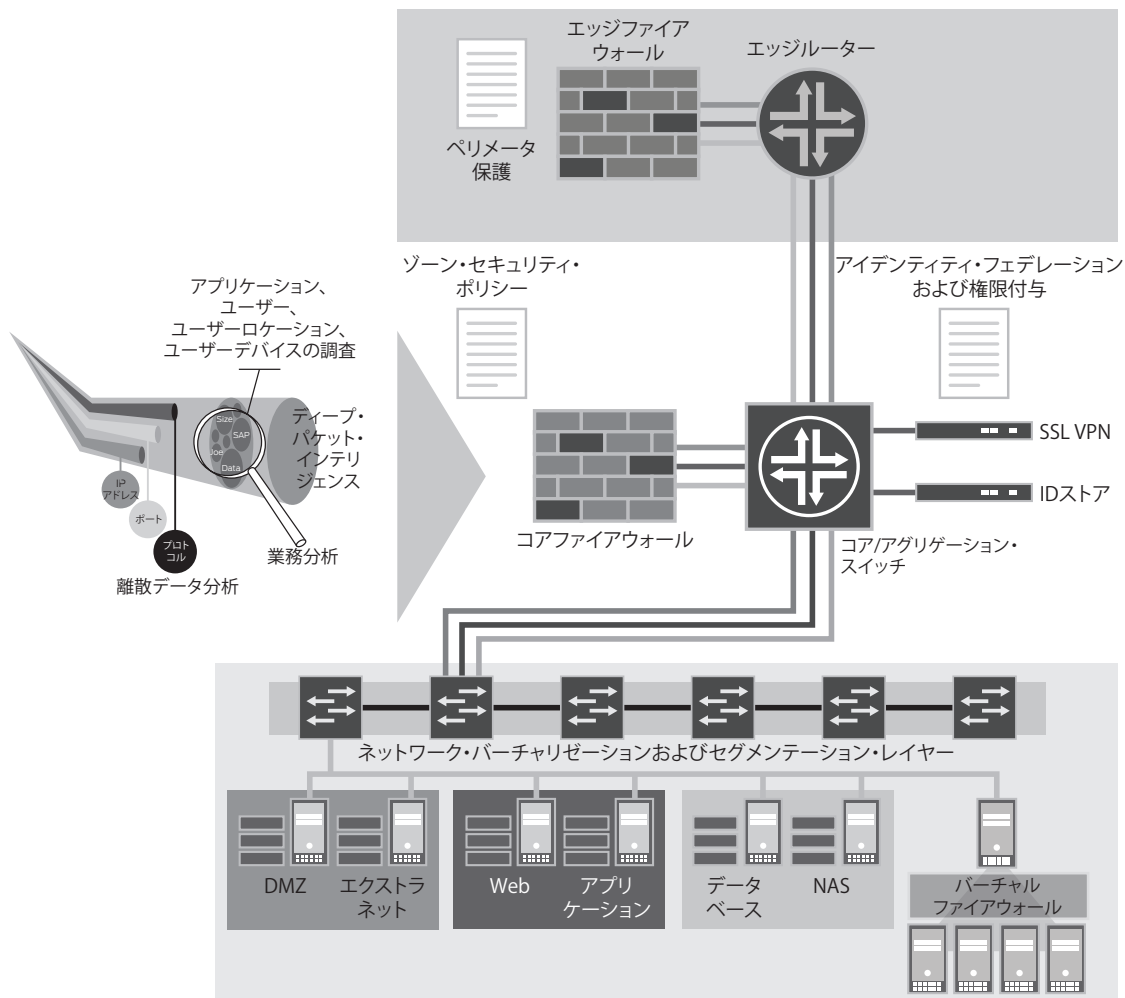


図5: データセンターのセキュリティ・エンフォースメント参照モデル

まとめ—ネットワーク・セントリックな手法によるデータセンターのセキュリティの保護

今日では、組織が業務を遂行するにあたって、データセンターへの依存度はますます高まっています。リソースの集中化およびサーバー・バーチャライゼーション、分散型アプリケーションモデル、IPベースストレージなどのテクノロジーの導入が進められることによって、データセンターは進化し続けます。経済面で利点が得られる一方、その副産物として、ますます多様性を増すセキュリティリスクに対してかつてないほどデータセンターの脆弱性が増えています。

サイバー窃盗や高度化したマルウェアに加えて、データ・センター・テクノロジーに潜んでいる新たな脆弱性からも防御する必要があります。たとえば、管理されていないバーチャルマシンのネットワーク、マッシュアップやSOAに伴う新しい通信パターン、IPインフラストラクチャベースのストレージ・ネットワークはどれも、それぞれに固有の新しいセキュリティ上の問題をもたらします。

データセンターを進化させ、それによって成功するためには、新しいリスクを踏まえた上で、既存の情報セキュリティのベストプラクティス、テクノロジー、および設計手法を見直す必要があります。ネットワーク・セントリックな手法でバーチャル化されたクラウド対応データセンターのセキュリティを保護することで、拡張性、ポリシーの定義とエンフォースメントの統合、業務のオーバーヘッドの削減など、多くの利点が得られます。データ・センター・インフラストラクチャ向けのセキュリティソリューションを評価する際、アプリケーション識別、IDベースのポリシー・エンフォースメント、集中管理、膨大な量の処理を実行するアプライアンスを重視する必要があります。

ネットワークはデータセンター内のあらゆるデバイスに接続されているので、総合的なセキュリティツール群の管理ポイントとして最適です。さらに、テクノロジーの進化により、セキュリティデバイスをネットワーク内のごく少数のポイントにのみ物理的に接続し、論理的に複数のネットワーク・セグメントに拡張して処理させることができます。ネットワーク・セントリックな手法を使用することによって、分散環境に統合されたセキュリティポリシーを導入し、データ・センター・サービスを事実上あらゆる場所のあらゆるユーザーに提供することが、容易に実現できます。

ジュニパーネットワークスについて

ジュニパーネットワークスは、ハイ・パフォーマンス・ネットワーキングのリーダーです。サービスおよびアプリケーションの一元化されたネットワークにおける展開を加速するのに不可欠な、即応性と信頼性の高い環境を構築するハイ・パフォーマンスなネットワーク・インフラストラクチャを提供するジュニパーネットワークスは、お客様のビジネス・パフォーマンスの向上に貢献します。ジュニパーネットワークスに関する詳細な情報は、以下のURL でご覧になれます。

<http://www.juniper.net/jp/>

日本

ジュニパーネットワークス株式会社
東京本社
〒163-1035
東京都新宿区西新宿3-7-1
新宿パークタワー N棟35階
電話 03-5321-2600
FAX 03-5321-2700

西日本事務所
〒541-0041
大阪府大阪市中央区北浜1-1-27
グランリュウ大阪北浜

米国本社

Juniper Networks, Inc.
1194 North Mathilda Ave
Sunnyvale, CA 94089
USA

電話 888-JUNIPER
(888-586-4737)
または408-745-2000
FAX 408-745-2100

URL <http://www.juniper.net>

アジアパシフィック

Juniper Networks (Hong Kong) Ltd.
26/F
Cityplaza One
1111 King' s Road,
Talkoo Shing, Hong Kong

電話 852-2332-3636
FAX 852-2574-7803

ヨーロッパ、中東、アフリカ

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin
Ireland

電話 35-31-8903-600
FAX 35-31-8903-601

URL <http://www.juniper.net/jp/>

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

Juniper Networks、Junos、NetScreen、ScreenOS、Juniper Networksロゴは、米国およびその他の国におけるJuniper Networks Inc.の登録商標または商標です。また、その他記載されているすべての商標、サービスマーク、登録商標、登録サービスマークは、各所有者に所有権があります。ジュニパーネットワークスは、本資料の記載内容に誤りがあった場合、一切責任を負いません。ジュニパーネットワークスは、本発行物を予告なく変更、修正、転載、または改訂する権利を有します。

2000332-001 JP Jan 2010