



## 侵入防止の未来

### 次の IPS として次世代ファイアウォールを使用する理由

2009 年 11 月

Palo Alto Networks  
232 E. Java Drive  
Sunnyvale, CA 94089  
408.738.7700  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

## 目次

概要 .....	3
多くの企業による侵入防止システムの採用 .....	4
アプリケーションと脅威の状況の変化 .....	4
従来の IPS と新しい脅威の対決: 一方的な勝負 .....	5
侵入防止に関する企業の新しい要件 .....	7
Palo Alto Networks が提供する機能 .....	8
侵入防止の未来は、次世代ファイアウォールにある .....	10

Copyright 2009, Palo Alto Networks, Inc. 無断複写・転載を禁じます。Palo Alto Networks、Palo Alto Networks ロゴ、PAN-OS、および App-ID は米国における Palo Alto Networks, Inc. の商標です。仕様はすべて予告なく変更される場合があります。本文書内の誤りや本文書中の情報更新義務に関し、Palo Alto Networks はいかなる責任も負わないものとします。Palo Alto Networks は、本出版物を予告なく変更、修正、権利譲渡、または他の何らかの方法で改訂する権利を留保します。

## 概要

多くの IT 組織が、主に情報セキュリティの脅威からデータセンターを保護するために侵入防止システム (IPS) を展開しています。これらの脅威が依然として存在する一方で、回避機能を持つアプリケーションを利用したり、暗号化を使用したり、ネットワーク上のクライアントをターゲットにする、まったく新しいタイプの脅威の媒介が発生しています。企業でこのような新しいタイプの脅威の媒介を十分に管理できないため、組織は IPS への取り組みを再検討しています。従来、組織は、サーバーやデータセンターの保護、サポート、およびパフォーマンスに焦点を当てて IPS の検討を行っていました。しかし今日では、多くの組織が、クライアントが脅威を伝えるパイプとしての重要性を増していることを考え、脅威をもたらす暗号化トラフィックやアプリケーションを考慮に入れて IPS の検討を行う必要に迫られています。ここで 1 つの疑問が生じます。IDS から IPS に移行して重要な管理要件が設定されたとして、スタンドアローンの IPS は、企業を脅威から保護するのに適したモデルと言えるでしょうか。

Gartner による次世代のファイアウォールに関する研究と助言では、組織が異なるモデルに移行することが提案されています。Gartner は、IT 組織が次のリフレッシュ時に、IPS の展開およびファイアウォールの展開から、IPS を組み込んだ次世代ファイアウォールに移行することを勧めています。UTM による単純なデバイス統合とは異なり、次世代ファイアウォールではまず、ポートやプロトコルではなくアプリケーションを使用してトラフィックを分類する単一のアーキテクチャが土台から設計され、企業レベルのスループットと管理機能を持つ IPS 機能が組み込まれます。

Palo Alto Networks は、次世代ファイアウォールにおけるリーダー的地位を確立しています。企業は、この次世代ファイアウォールを使用することによって、まずネットワーク上で実行するアプリケーションを制御し、次に、許可されたアプリケーションに脅威が存在しないかをスキャンできます。従来のファイアウォールと連携している従来の IPS と比較した場合でも、Palo Alto Networks の次世代ファイアウォールは、より優れた管理機能、保護機能、パフォーマンス、およびサポートを組織に提供します。

## 多くの企業による侵入防止システムの採用

2003 年、Gartner は、多くの組織における実感として、侵入検出から侵入防止への移行の必要性を表明しました。組織において実際の侵入や誤検出が多発し、情報を脅威から保護するためのより効率的な方法が求められるようになりました。このような移行は現在も継続中です。侵入防止に対する組織の要求が高まるに従って、スタンドアローンの IPS のアーキテクチャでは、企業が必要とする管理機能、保護機能、およびパフォーマンスを実現できないことが明らかになってきています。次世代の脅威や脅威の媒介から保護するためには、アプリケーションや脅威の状況の変化に応じて、侵入防止の機能も変える必要があります。しかし、ハイバリューでハイリスクのアプリケーションを安全に実現するには、何よりもまず、IPS が重要な役割を果たす必要があります。

## アプリケーションと脅威の状況の変化

過去数年間に渡って、アプリケーションと脅威の状況に数多くの大きな変化が見られました。個人向けのアプリケーションが普及し、ビジネスアプリケーションとの区別が次第に困難になっています（区別されていない場合も多くあります）。これらのアプリケーションをターゲットとして、脅威が企業に簡単に侵入するようになってきました。本来は主に個人間のコミュニケーションを目的とするこの種類のアプリケーションには、インスタントメッセージング、ピアツーピアでのファイル共有、Web メール、数多くのソーシャルネットワーキング用アプリケーションなどがあります。組織のポリシーによって禁止されている場合でも、このようなアプリケーションが企業ネットワーク上に存在することは、ほぼ間違いありません。これらのアプリケーションに人気があることも 1 つの原因ですが、これらのアプリケーションが通信手段を動的に調整することによってファイアウォールなどの従来の対抗手段を回避するように設計されていることにも原因があります。一般的な手法としては、ポートホッピング、非標準ポートの使用、一般的に使用されるサービス内でのトンネリング、SSL 暗号内への潜伏などがあります。

これらのアプリケーションの多くは、個人間のコミュニケーション以外にも非常に役立つことが証明されています。世界中の企業が、正当な事業目的のためにこれらのアプリケーションを日常的に導入し、一般的に、重要なプロセスの促進、顧客サービスの改善、コラボレーション、コミュニケーション、および従業員の生産性の向上に役立っています。

純粋なビジネスアプリケーションでさえ、同様の回避可能な技術を使用して、採用されているセキュリティインフラストラクチャに関係なく、すべてのユーザーによるすべてのネットワーク内でのアクセスを受け入れ、機能するように設計されています。さらに、広範に及ぶ従来のアプリケーションが、Salesforce.com、WebEx、Google Apps など、ホスト型のクラウドベースのサービスに置き換えられつつあります。その結果、HTTP と HTTPS が、企業における全トラフィックの約 3 分の 2 を占めるようになり、従来のセキュリティインフラストラクチャ特有の弱点が深刻化しています。特に、古いセキュリティインフラストラクチャでは、正当な事業目的に使用されるかどうかに関係なく、この汎用プロトコルで実行される広範なアプリケーションを、事実上、区別することができません。

一方、脅威の状況にも大きな変化が見られます。特に、ハッカーの動機は、名声を得ることや有名になることから、実際に金銭的な利益を得ることへと変化しています。これは、ハッカーがより容易な回避技術に注目するようになってきていることを意味します。その際にハッカーが使用する一般的な方法の 1 つは、アプリケーション上で、アプリケーションを介して動作する脅威を構築することです。これにより、悪意のある創作物が、ネットワーク層を保護するために設計された、大多数の企業の防御を通過できるようになります。今日のハッカーは、ユーザー中心のアプリケーションの人気が上昇していることにも、少なからず注目しています。ソーシャルネットワーキング用のアプリケーションには、ワーム、

トロイの木馬、およびエクスプロイトが見られます。ワームやボットネットは P2P ファイル共有ネットワークをターゲットとし、ワームやボットネット自体を広めるためだけでなく、コマンドや制御を伝えるために使用されます。このような送信媒介（つまり、アプリケーション）がターゲットとなる理由は、その人気の高さだけでなく、これらが持つ回避機能を利用して、脅威が企業ネットワークに無条件に侵入できることです。

## 従来の IPS と新しい脅威の対決：一方的な勝負

前述のように、アプリケーションと脅威の状況の変化を受けて、組織は侵入防止の再検討を始めています。従来、企業はまず IPS を使ってサーバーとデータセンターを保護することに焦点を当て、サーバーとデータセンターの保護、IPS ベンダーによるサポートと研究、および IPS のパフォーマンスを 3 つの要件としていました。主な IPS ベンダーは、これらの基本的な要素における差別化を実現する努力を始めています。

- **サーバーの保護:** 検出技術と防止技術の数はそれほど多くなく、ほとんどの IPS 技術によって、そのすべてがサポートされています。このような技術には、プロトコルアノマリ検出、ステートフルパターンマッチング、統計アノマリ検出、ヒューリスティック分析、無効または不正な形式のパケットの遮断、(回避に対抗するための) IP のデフラグメンテーションと TCP の再構築などがあります。ほとんどの IPS ベンダーは、エクスプロイトに対応するシグネチャではなく、脆弱性に対応するシグネチャを使用しています。サーバー保護の偏りを生むもう 1 つの原因として、多くの IPS ベンダーが、パフォーマンスを改善するためにサーバーからクライアントへの保護を無効にしていることがあります。
- **研究とサポート:** これは、ベンダーが実際にどの程度の研究を行っているか、および新しい攻撃や脆弱性から企業を保護するために、どれくらい迅速に対応できるか、ということの意味します。IPS ベンダーの調査チームによっても多くの研究が行われていますが、違いは確かにあるものの、研究の多くは少数の業界大手の調査会社に外部委託されています。もう 1 つの側面は、きわめて重要です。研究が誰によって行われるかに関係なく、ベンダーは、新しく出現する脅威から顧客を保護するために、タイムリーにアップデートを提供できるかどうか問われます。
- **パフォーマンス:** 組織が IPS のパフォーマンスの問題に敏感になっているのは明白です。また、Infonetics による最近の研究では、企業に帯域外 IPS を展開させる主な問題として、トラフィックやアプリケーションのレイテンシの発生、および帯域幅やパフォーマンスを挙げています (Infonetics: ユーザーの侵入防止システム計画: 北米、2009 年)。スループットとレイテンシに関して企業の期待にこたえることが、多くの顧客にとって優先事項であることは明らかです。

しかし、防御手段が成熟するとともに、攻撃者も進歩します。ファイアウォールなどの IPS は比較的良好に理解されているため、新しい攻撃では既知の弱点が悪用されます。たとえば、アプリケーションをターゲットにしたり、アプリケーションを介してトンネリングしたり、攻撃を暗号化したりすることにより、クライアントマシンを介してネットワークを攻撃する方法があります。

- **アプリケーションが伝える脅威:** 脅威の開発者は、ターゲットと送信媒介の両方としてアプリケーションを使用します。いずれの方法を使う場合でも、アプリケーションは効果的な基盤となります。また、これらのアプリケーションは回避機能を持っているため、企業の防御を容易に通過できます。回避機能を持つアプリケーションの数は増加を続けています。Palo Alto Networks は研究活動の一環として、900 個を超えるアプリケーションとその振る舞いを記録した、現在も発展中のデータベースである Applipedia を保持しています。

Applipedia に記録されている 900 個を超えるアプリケーションのうち、446 個はファイルを転送することができ、200 個はマルウェアを運ぶことがわかっており、470 個は既知の脆弱性が含まれています。

アプリケーションが伝える脅威には、十分に理解されているもの (koobface、boface、fbaction など、ソーシャルネットワークを介して移動する多くの脅威) と、理解されていないもの (MSN Messenger や P2P ファイル共有アプリケーションを使用して広がる Mariposa) があります。いずれにしても、攻撃者はアプリケーションのピギーバックが簡単であることを知っているため、クライアントを使って攻撃を開始します。

- **暗号化された脅威の媒介:** 脅威によって利用されるもう 1 つの重要な技術は、暗号化です。セキュリティ研究者は、暗号化がさまざまな脅威によって使用されるようになることを何年も前から警告していましたが、暗号化された攻撃には、ユーザー中心のアプリケーションというパイプ役が必要でした。ユーザーは、簡単にだまされて暗号化されたリンクをクリックします (多くのユーザーが、HTTPS は安全だと信じています)。これにより、企業の防御を簡単に通過する暗号化された脅威が送信されます。この方法は、信頼の度合いが非常に高いソーシャルネットワーク上では、きわめて簡単です。密接な関連のあるもう 1 つの媒介は、圧縮 (ZIP) による難読化です。従来のスタンドアローンの IPS では圧縮されたコンテンツを解凍できないため、スキャンできません。
- **データ漏洩について:** 過去 2 年間で情報セキュリティについて最も大きく報じられたニュースは、アプリケーションを介した機密データや極秘データの漏洩でした (米国政府の機関と契約業者、製薬会社、小売業者など)。ほとんどの場合、データ漏洩を引き起こしたアプリケーションは明示的に禁止されていましたが、不幸にも、従来のファイアウォールや IPS では、それらのポリシーを徹底できませんでした。これらのセキュリティ違反が注目を集めているため、このような厄介な出来事から組織を守るために、侵入防止に注目が集まり始めているのも当然です (Infonetics)。

ここでの共通のテーマは、アプリケーションとコンテンツの制御、SSL の解読、コンテンツの解凍による脅威の探知など、新しい脅威を防ぐために必要な管理のレベルです。これらはすべて、従来の IPS の機能では対応できません。IPS の大きな欠点は、IDS から移行するための作業を行っても、ネガティブセキュリティモデルが維持されることであり、そのように設計されていることです。簡単に言うと、IPS は「見つけてから対処する」というモデルに依存しています。このモデルは、アプリケーションを介して移動する多くの新しい脅威に対処するのに必要とされる管理には、あまり役に立ちません。また、すべてのトラフィックの解読や分類を行うことができるアーキテクチャやプラットフォームとしての役割を果たすこともできません。

## 侵入防止に関する企業の新しい要件

アプリケーションと脅威に関する現在の状況では、完全な侵入防止を実現するための新しい要件が必要です。これには従来の IPS 要件も含まれます。今日の経済環境においては、より多くのネットワークセキュリティ機器を無秩序に導入することを提案するのは不適切です。しかし、組織が直面している新しいタイプの脅威にも取り組む必要があります。レベルの高いこれらの要件とは、管理、保護、パフォーマンス、およびサポートです。

- 最初に、ポート、プロトコル、暗号化、または回避手段に関係なく、ネットワーク上で許可するアプリケーション（およびアプリケーションの機能）を管理します。これには 2 つの理由があります。1 つ目は、企業がネットワーク上に存在することを望まないアプリケーションがいくつかあることです。2 つ目の理由は、アプリケーションが伝える脅威が出現したことにより、どのアプリケーションがネットワーク上にあるかを制御することで、攻撃対象を減らす効果があることです。
- 2 番目に、脅威を見つけるために、許可されたアプリケーションのトラフィックをスキャンします（暗号化または圧縮されている場合でも、機密データまたは極秘データを見つけるためにスキャンする可能性があります）。
- 3 番目に、実際のトラフィックにおいて、サーバーとクライアントの両方を保護するために完全スキャンを有効にした状態で、1 秒間に数ギガビットのスループットと低いレイテンシで、この処理を行います。
- 4 番目の重要な要件はベンダーに対するものです。ベンダーは、強力な最先端技術を研究し、進化を続ける新しい脅威からの保護を迅速に開発することにより、企業顧客を支援する必要があります。

最後に、ネットワークセキュリティのアーキテクチャと未来に関する通達について述べておきます。Gartner は最近、次世代ファイアウォールに関する通達を発表し、その中で、企業に対して IPS から次世代ファイアウォールへの移行に関する具体的な助言を行っています。

- まだネットワーク侵入防止を展開していない場合は、ファイアウォールの次回のリフレッシュ時に、すべてのベンダーに NGFW 機能を要求すること。
- ネットワークファイアウォールとネットワーク侵入防止の両方を展開済みの場合は、両方の技術のリフレッシュサイクルを同期させて、NGFW 機能に移行すること。
- 管理された境界セキュリティサービスを使用する場合は、次の契約更新時に管理された NGFW サービスに移行すること。

出典: Gartner

## Palo Alto Networks が提供する機能

次世代ファイアウォールによって、Palo Alto Networks は、管理、保護、パフォーマンス、研究/サポートという要件にこたえる独自の位置付けを得ています。

**管理:** 管理に関して、Palo Alto Networks の次世代ファイアウォールには、複数の利点があります。第 1 に、これはファイアウォールであるため、信頼された境界を通過するトラフィックがすべてチェックされます。第 2 に、Palo Alto Networks の App-ID テクノロジは、ファイアウォールのトラフィック分類エンジンです。つまり、App-ID は、ポート、プロトコル、暗号化、または回避技術に関係なく、アプリケーションを分類し、ポリシーに従って管理します。Palo Alto Networks の User-ID テクノロジにより、さらに高度な管理が実現されるため、組織は、ポリシーにおいて企業ディレクトリユーザーやグループの情報も使用できます。アプリケーションとユーザーのポリシーを管理する権限を IT スタッフとセキュリティスタッフに与えることには、大きなメリットがあります。ネットワークのセキュリティポリシーを作成して管理する作業が大幅に簡素化できることはその 1 つです。

**保護:** Palo Alto Networks の Content-ID テクノロジでは、すべての主要な IPS と脅威のスキャンテクノロジを、ストリームベースのスキャンエンジンに統合します。また、同じエンジンに、クレジットカードの番号やカスタムの正規表現など、特定の種類の機密データを探すためにスキャンする機能が含まれています。次に示すような証明済みの脅威検出および防止 (IPS) メカニズムを使用して、トラフィックを一度だけスキャンすることによって、脆弱性の悪用、バッファオーバーフロー、DoS 攻撃、およびポートスキャンが、クレジットカードの番号などの機密データとともに検出されます。

- プロトコルアノマリベースの保護では、長過ぎる URI や長過ぎる FTP ログインの使用など、RFC 非準拠のプロトコルの使用を検出します。
- ステートフルパターンマッチングでは、到着順や順序などの要素を考慮して、複数のパケットに渡る攻撃を検出します。
- 統計アノマリ検出では、レートベースの DoS フラッディング攻撃を防ぎます。
- ヒューリスティックベースの分析では、ポートスキャンやホストスイープなど、異常なパケットやトラフィックのパターンを検出します。
- 攻撃に対する他の保護機能として、無効または不正な形式のパケットの遮断、IP デフラグメンテーション、TCP の再構築などを利用して、攻撃者が使用する回避と難読化から保護が行われます。

Palo Alto Networks は、多くの IPS ベンダーと同様に、脆弱性に対応するシグネチャを主に使用しています。また、これらを何千個も保持しています。ここでのもう 1 つの重要な要素は、Palo Alto Networks の次世代ファイアウォールは、脅威を見つけるために、SSL 暗号化されたインバウンドとアウトバウンドのトラフィックおよび圧縮されたコンテンツをスキャンできることです。このことは、企業での SSL 暗号化されたトラフィックの量を考えると、きわめて重要です。

**パフォーマンス:** Palo Alto Networks の次世代ファイアウォールは、独自の Single Pass Parallel Processing (SP3) アーキテクチャに基づいているため、コンテンツと脅威の完全スキャンを実施しながら、高スループット (最大 5 Gbps) で低レイテンシ (1 ミリ秒未満) のネットワークセキュリティを実現します。Palo Alto Networks は、過去に IPS では解決が困難だったパフォーマンスの問題を、SP3 アーキテクチャを使って解決します。このアーキテクチャでは、次に示す 2 つの補足的なコンポーネントを組み合わせます。

- **シングルパスソフトウェア:** Palo Alto Networks のシングルパスソフトウェアは、1 パケットごとに処理を 1 回実行します。パケットを処理するときに、ネットワーク機能、ポリシー照合、アプリケーションの識別と復号、および脅威とコンテンツのスキャンが、すべて 1 回だけ実行されます。これにより、1 つのセキュリティデバイスで複数の機能を実行するのに必要な処理のオーバーヘッドの量が大幅に削減されます。このシングルパスのトラフィック処理により、すべてのセキュリティ機能を有効にした状態で、非常に高いスループットと低いレイテンシが実現します。また、単一のポリシーに完全に統合されるという付加的なメリットも得られるため、企業ネットワークのセキュリティをシンプルかつ簡単に管理できるようになります。
- **並列処理ハードウェア:** Palo Alto Networks の次世代ファイアウォールでは、シングルパスソフトウェアを高速で実行できるように、並列処理ハードウェアを使用します。まず、Palo Alto Networks のエンジニアは、データプレーンと制御プレーンを個別に設計しました。このように分離することで、一方の負荷が高くなっても他方が悪影響を受けることがなくなります。並列処理ハードウェアの 2 つ目の重要な要素は、ネットワーク、セキュリティ、コンテンツと脅威のスキャン、および管理という、複数の重要な機能を実行するために連携して機能する離散的な専門の処理グループを使用することです。

シングルパスソフトウェアと並列処理ハードウェアを組み合わせることは、ネットワークセキュリティにおける完全に独自の技術であり、Palo Alto Networks の次世代ファイアウォールは、この技術により、非常に高いレベルのパフォーマンスを達成できます。この他に、重要度は低くてもより現実的な点として、Palo Alto Networks の次世代ファイアウォールはポート密度が非常に高いため、セグメント化が進行する大規模なネットワークの保護を簡素化し、コストを削減することができます。

**研究/サポート:** すでに述べたように、研究とサポートは顧客にとって重要です。ベンダーは、組織のネットワーク保護を支援するのに十分な知識を持ち、また迅速に回答できるでしょうか。これは、測定するのが特に困難です。遍在性を考えると、Microsoft の脆弱性を検査することで、これらの両方を推測できます。Palo Alto Networks には、過去 6 か月間に、どの IPS ベンダーの調査チームよりも Microsoft の脆弱性を多く発見したという実績があります。第 2 位のベンダーが発見した数は、Palo Alto Networks の半数でした。検討が必要なもう 1 つの側面は、応答性です。脆弱性 MS08-067 をターゲットとする Conficker を例とすると、Microsoft が脆弱性を発表した数時間後に、Palo Alto Networks はその脆弱性に対する保護をリリースしました (Palo Alto Networks は、Microsoft Active Protections Program に参加しています)。さらに、Palo Alto Networks は、最初の変種の登場から数日以内に Conficker のダウンロードトラフィックを認識しブロックすることに成功しています。

要約すると、Palo Alto Networks の次世代ファイアウォールは、現代の脅威に対する防御のために組織が必要とする管理、保護、パフォーマンス、研究、サポートを実現します。従来の IPS と比較するには、以下の表を参照してください。

要件	Palo Alto Networks の次世代ファイアウォール	従来の IPS
アプリケーションの管理	900 個を超えるアプリケーション。	脅威など、少数の不良アプリケーションを処理できます。
許可されたトラフィックのスキャンによる脅威の検出	可能。SSL 暗号化および圧縮されたコンテンツにおいて 1000 個のシグネチャに対応。	可能。1000 個のシグネチャに対応。SSL 暗号化および圧縮されたコンテンツには非対応。
現実世界における 1 Gbps 以上のパフォーマンス	可能。	ベンダーにより異なります。
研究とサポート	トップクラス。他の IPS ベンダーより多くの Microsoft の脆弱性を発見しています (過去 6 か月に 6 個)。	不要な情報が多く、動きが少ない。最高レベルの企業内 IPS 調査チームは、過去 6 か月間に 3 つの Microsoft の脆弱性を発見しています。過去 2 年間、何もしていないチームもあります。

図 1: IPS 製品では対応できない機能を提供する Palo Alto Networks の次世代ファイアウォール

## 侵入防止の未来は、次世代ファイアウォールにある

回避機能を持つアプリケーションと暗号化を使用する脅威によって、アプリケーションと脅威をめぐる状況が変化しています。従来の IPS では、これらの新しい脅威の媒介を制御することができません。このために、管理、保護、パフォーマンス、研究/サポートに焦点を当てた、侵入防止に対する新しい企業要件が発生しています。ユーザーとアプリケーションに対する強力な管理、すべての関連する IPS 技術、高パフォーマンスのプラットフォーム、および強力な研究とサポートのおかげで、Palo Alto Networks は、これらの要件にこたえる独自の位置付けを得ています。これらすべてによって、企業は、まずネットワーク上で実行するアプリケーションを管理し、次に、許可されたアプリケーションに脅威が存在しないかをスキャンできます。さらに、Gartner は、企業が従来のスタンドアロン型の IPS 展開から次世代ファイアウォールに移行するべきであると述べています。これは、IDS を IPS に変換することから始まった移行が、最終的には次世代ファイアウォールに行き着くことを示しています。