日本ネットワークアソシエイツ　McAfee IntruShield

高精度な検知・防御機能でセキュアネットワークを実現
McAfee IntruShieldが切り拓く次世代IDS/IPS

日本ネットワークアソシエイツ株式会社
販売推進本部プロダクトマーケティング部
Network Protection担当
返田　恵氏

セキュリティ市場を牽引するトップベンダー、日本ネットワークアソシエイツが満を持して発売した不正侵入検知・防御システム「McAfee® IntruShield®」。同製品は信頼性の高い検知とハイパフォーマンスの両立によって、真のセキュアネットワーク構築を強力にサポートする。

2003年8月11日に発生した「W32/Lovsan.worm」こと「MSブラスト」が世界中の企業に甚大な被害をもたらしたことは記憶に新しい。ファイアウォールやアンチウィルス等のセキュリティ対策を講じていたにも関わらず、多くの企業や団体がその猛威にさらされたのだ。

今回のMSブラストの件が証明しているように、感染経路の多様化、侵入手法の巧妙化、そして攻撃手法の複合化等、ネットワークに対する攻撃はより高度化・高速化且つ複雑化している。すなわち、従来のようにネットワークの特定の部分だけを防御する単一のソリューションではなく、ビジネスインフラ全体を考慮し、重要度、柔軟性に応じてネットワークの各ポイントに最適なセキュリティ対策を講じなければならなくなっているのだ。

こうした課題に対応するべく、日本ネットワークアソシエイツが新たに打ち出したのが「Protection-in-Depth™」ソリューション。これは、多様化・複合化が進むセキュリティ侵入・攻撃に対して、広範なソリューションとともに、専門化された製品群を提供することにより、PC等のデスクトップからサーバー、ネットワークのエッジからコアにいたるまでをカバーする、統合的なセキュリティソリューションを提供するというもの。

その中核となる製品が、侵入検知・防御システム「McAfee IntruShield」だ。

既存の侵入検知・防御システムに不満

複雑化するネットワークへの攻撃に対する防衛策として不正侵入検知システム（IDS）の導入が進んでいる。しかし、導入した製品に、ユーザーから数々の問題点が指摘されているのも確か。

1つが「誤検知の多さ」だ。IDSは、シグネチャに基づきパターンマッチングを行い、疑わしいと判断したパケットや動作に対してアラームを管理者に通知し、攻撃を未然に防ぐ。しかし、実際にはそれが正しいパケットであるか、不正なパケットであるかの判断は管理者側が行わなければならない。そのため、大量にアラームが発生した場合、管理者の分析にかかる負荷の増大が問題となっていた。

IDS製品には疑わしいトラフィックやサービスを自動的に停止させる機能を保有するものもあるが、不正な通信だけでなくビジネスに必要な通信を遮断してしまうケースもある。

また、パフォーマンスも課題となっている。正確な検知を行うためにはネットワークを流れるトラフィックをつぶさに捉え分析する必要があるが、サーバーファームやバックボーン等、トラフィックが集中する個所にIDSを設置した場合、IDS自身がボトルネックになったり、大量のトラフィックに対応し切れず、ここでも誤検知を招いてしまうことがある。

日本ネットワークアソシエイツ・販売推進本部プロダクトマーケティング部Network Protection担当の返田恵氏は、「SlammerやMSブラストは、数分で世界中に広がってしまいました。これからは、攻撃を「検知」するだけでなく、その攻撃が自社ネットワークに入り込む前に策を講じる「防御」が必要です。そのためには、In-Lineでの運用に耐えうるだけの堅牢なシステムがなくてはなりません。また、正確な防御は、正確な検知があってこそはじめて可能となります。数多くの侵入検知・防御システムが市場に投入される中、これまでの製品が抱えていた誤検知、パフォーマンス、コスト等の課題を解決し、ユーザーのニーズに真に応えられるものがMcAfee IntruShieldです」と自信を見せる。

ネットワークの柔軟な配置もMcAfee IntruShieldの大きな特徴だ

SPANモード

Tapモード

In-lineモード

複数の手法の組み合わせで誤検知を回避

McAfee IntruShieldの特徴を見ていこう。

システムは、ハードウエア（センサ）とマネジメントソフトウエア「IntruShield Security Management（ISM）」の2製品で構成される。

センサはネットワークの帯域別に、2Gbpsに対応した「IntruShield 4000」、600Mbpsの「IntruShield 2600」、100Mbpsの「IntruShield 1200」の3タイプが用意されており、ネットワークの速度や規模に応じて柔軟な選択が可能だ。

ISMは、センサの動作に関わる情報の管理およびレポート作成機能を担うアプリケーションシステム。

McAfee IntruShieldの最大の特徴は、①シグネチャ検知、②アノマリ検知、③DoS攻撃検知 ── の3つを組み合わせた非常に高精度な検知を実現する点にある。

①のシグネチャ検知は、既知の攻撃からシステムを的確に保護する強力なシグネチャ検知機能。特許出願中の「ステートフルシグネチャ検知エンジン」により、データパケット内のステート情報を活用し、複数トークンのマッチングを使用して、パケットをまたがる攻撃シグネチャや順序の異なるパケットストリームに存在する攻撃シグネチャを検知することで、コンテキストに応じた検知を実現する。

②のアノマリ検知は、未知の攻撃を特定し、攻撃検知率を向上するもので、「統計的異常」、「プロトコル異常」、「アプリケーション異常」等のアノマリの検知技術を使用し、総合的なアノマリ検知を実現。バッファオーバーフロー等の攻撃に効果的な防御を可能とする。

そして、③のDoS攻撃検知は、比類のない精度で攻撃を検知し、素早く攻撃阻止アクションを実行、しきい値を定義する検知に加え、自己学習型プロファイルベースのDoS攻撃検知を行う。DoSプロファイルには、事前に定義されたしきい値の他、DoS攻撃検知のための自己学習パラメータも含んでいる。プロファイルは、一定範囲のIPアドレス用や個別のホスト用に作成可能。センサー1台で数百のプロファイルをサポート可能だ。通常のトラフィック動作から外れたトラフィックにはすべて、DoS条件のフラグが立つため、数Gbpsのトラフィックでも、IntruShieldの高精度なDoS攻撃検知機能によって攻撃を発見することが可能だ。

これらの3つの検知手法を組み合わせ、分析を行うため、誤検知を回避、担当者の負荷軽減を実現している。

パフォーマンスについても、設計の初期段階から侵入の検知のみならず防御までを想定して開発された専用ハードウェアと、独自のASICによる高速なパケット処理により、ネットワークのパフォーマンスを損なうことなく正確な検知を実現する。

さらに特筆すべき機能が「Virtual IDS」だ。

これは単一のセンサでVLANやCIDRごとに複数のポリシーを設定できる機能。例えば、部門別、役職別ごとにネットワーク、サーバーへ接続するための条件定義を変えたい場合、従来のIDSでは1ポリシーごとにシステムを導入しなければならなかった。しかしVirtual IDS機能を用いることで、柔軟なポリシー設定をネットワークの各部位に適用できるため、管理負担の軽減や設備投資コストの大幅な削減が可能となる。IntruShield 4000では最大1000のVirtual IDSをサポートすることができるので、大規模ネットワークでも十分に活用できる。

McAfee IntruShieldの先進性と優位性は、2002年にラスベガスで開催されたNetWorld+Interopにおける「Best of Interop」アワードやNetwork World誌のBLUE RIBBON賞をはじめとした数々の受賞や、OSECやNSSグループ等の調査機関によるパフォーマンステストでの優れた実績からも証明されている。また、世界各国ですでに多くの政府系機関・金融をはじめとした企業・教育機関でも導入されており、その実績は折り紙つきだ。

堅牢なセキュリティは、高精度な検知機能があって初めて実現される。信頼性の高い検知機能と防御機能を実現するというコンセプトから生まれたMcAfee IntruShieldが企業のセキュアネットワークの実現を強力にバックアップしそうだ。

お問い合わせ先
日本ネットワークアソシエイツ株式会社
〒150-0043 東京都渋谷区道玄坂1-12-1
渋谷マークシティウエスト20階
TEL：03-5428-1413
URL：http://www.nai.com/japan/intrushield/