特集3 商・材・研・究

不正侵入検知・防御システム

セキュリティ対策の定番商品に拡販の課題は運用負荷の軽減

不正侵入検知・防御システム（IDS/IPS）がセキュリティビジネスの新商材として注目を集めている。ネットワークへの不正侵入・攻撃が悪質化する中で、ファイアウォール、アンチウイルスに続く“定番商品”となりそうだ。

企業のセキュリティニーズの高まりに伴い、不正侵入検知・防御システム市場が急速に立ち上がり始めている。

侵入検知システム（IDS）は、ネットワーク上を流れるトラフィックやパケットを分析し、それが正当なものか、不正なものかを判断、不正アクセスと思われる通信を管理者に警告するもの。ファイアウォールやルーターと連携し、通信を遮断し不正アクセスを防御するものもある。

一方、不正侵入防御システム（IPS）は不正アクセスの検知に加え、自身でそれを遮断する機能を持つ。

IDS/IPSが注目を集めている理由には、従来のファイアウォールやウイルス検知システムでは防御できない攻撃が頻繁に発生し、ネットワークに甚大な被害を与えているためだ。

ファイアウォールはインターネットの外側から来る不正アクセスや攻撃を遮断するもので、具体的にはTCP/UDP通信の通用口となる「ポート」を閉じる事で、不必要な通信をさせないようにする。但し必要な通信についてはポートを開き、パケットの送受信を許可する。

しかし、攻撃者の手口は巧妙化しており、ユーザーのIPアドレスを偽造するなどして許可されたポートを潜り抜けて不正侵入を行う。スパムメールの中継やFTPサーバーを踏み台にした攻撃が、ファイアウォールが正当な通信と見なしたことでなされるケースは少なくない。

また、ファイアウォールはネットワーク内の攻撃には対処できない。今年8月、世界中で猛威を振るったMSBlastによって多くの企業が甚大な損害を被ったが、ネットワークの内部から感染したケースもあったのだ。

例えば会社のPCを自宅に持ち込んでネットワークに接続した際にMSBlastに感染、それを再び会社のネットワークに接続したため、一挙に社内ネットワークにMSBlastが蔓延したという事例が数多く見受けられた。

一方、アンチウィルス等のセキュリティシステムも、不正侵入等、ウィルス以外の攻撃は守備範囲外となる。無論、侵入者による内部システムの破壊等のアタックには対応できない。

こうしたファイアウォールやウイルス検知システムでは防ぎ切れない攻撃への対応手段としてIDS/IPSが脚光を浴びているのだ。

巧妙化する侵入の手口

ここで、ネットワークを介して行われる不正行為を詳しくみていこう。

システムに対する不正行為は主に、
・盗聴 ・パスワードの盗用
・Webや重要データの改ざん
・システム・データの破壊、
・トロイの木馬等の不正プログラムの埋め込み、
・スパムメールの中継や他サイトへの攻撃の踏み台
――等がある。

これらの不正行為の前哨となるのが「不正侵入」だ。

不正侵入の具体的な手段には、①ポートスキャン、② トロイの木馬攻撃、③パスワードクラッキング、④セキュリティホールへの攻撃、⑤DoS攻撃――等があげられる。

①は、攻撃前の偵察行動として代表的なもので、ネットワークを通じてサーバーやPCにアクセスし、アプリケーションやOSの種類を調査し侵入可能な脆弱なポートを探す行為。

次に②は、一見、無害な実行ファイルを装いながら、インストールされた場合、システムを破壊したり、外部からネットワーク経由でシステムを制御可能にする裏口（バックドア）を作るプログラム。メールの添付ファイル等によって頒布されるケースが多い。

③は、パスワードファイルを盗用、さらに暗号化されたパスワードを解析することで、正規ユーザーになりすまして内部システムへ侵入する。

④は、OSや各種のアプリケーションのバグ等、セキュリティの脆弱性を突き、内部へ侵入したり、システムを破壊したりする。

⑤は、Denial of Service attackの略で、Web、FTP、メールサーバー等、特定のサーバーに向けて大量のアクセスを行うことで、負荷を高めサーバをダウンさせたり、ユーザーへのサービス提供を妨害する。

上記の手段以外にも侵入者の手口はより巧妙化、複雑化しており、さまざまな手段を組み合わせることでファイアウォールやアンチウイルスをかいくぐりネットワークへ攻撃を仕掛けてくる。

インターネットセキュリティシステムズ・国内営業部プロダクト＆PS事業担当部長兼マーケティング部部長の多田潔氏は、「ファイアウォールやアンチウイルス等の対策を行っていたにも関わらずMSBlast等の被害にあったユーザーは非常に多い。企業はセキュリティ対策を根底から見直さなければならなくなっている」と警告する。

これらの攻撃の足掛かりとなる不正侵入に対する防御を実現するIDS/IPS製品に対する注目が集まっているのだ。

検知の主流はパターンマッチ

IDS/IPSは設置箇所によって大きく、「ネットワーク型」と「ホスト型」に分けられる。

ネットワーク型IDSは、ネットワークに設置し、送受信されるトラフィックやパケットを監視する。製品の多くはファイアウォールの内側やDMZに配置するが、外側に設置してファイアウォールに到達する前に不正侵入を遮断するシステムもある。

また、サーバーファームや部門ネットワークごとに設置することで、サーバーへの攻撃を防いだり、内部から発生した攻撃を部門内に留める等の手法も堅牢なセキュリティ環境を構築するためには有効となる。

一方、ホスト型IDSは、サーバーや

図1 不正侵入の手口とシステムへの不正行為