SQL Slammer も検知、防止する
次世代型侵入防止システム “ ActiveScout アプライアンス ” 発表

2003 年 2 月 3 日 株式会社アズジェント
(店頭登録銘柄・コード番号 4288)

ワールドクラスのセキュリティソリューション提供を主業務とする株式会社アズジェント (代表取締役社長：杉本 隆洋 所在地：東京都中央区日本橋) は、この度、ForeScout Technologies 社 (フォアスカウトテクノロジーズ社、米国、Executive Chairman of the Board, Co-Founder： Hezy Yeshurun) の侵入防止システム「ActiveScout」をプレインストールした「ActiveScout アプライアンス」発表いたします。

【背景】

新たなセキュリティホールが日々発見され、不正アクセスが増加の傾向にある今日、企業において社内のネットワークを守ることは最重要課題となってきています。ファイアウォールやアンチウィルスソフトウェアはもちろん、侵入検知システム (IDS: Intrusion Detection System) 等によって、侵入を検知し、対策を行うことが重要です。

しかしながら、従来の IDS は①既知の攻撃にしか対応できない、②誤検出が多い、③実際に攻撃を受けてから警告を発するため、事後の対応しかできない (侵入されてしまったことの検出) 、④パフォーマンススケールの限界によるパケットの取りこぼし、という問題がありました。

この為、米国では IDS ではなく、IPS (Intrusion Prevention System) が登場し始めました。

このような背景のもと、アズジェントではコロンブスのたまご的発想といえる Recon (リコン) 概念に基づき、ActiveResponse 技術 (特許取得) を用いて未知の攻撃にも対処できる「ActiveScout」を搭載した「ActiveScout アプライアンス」を発表します。多くの攻撃は、サーバに対して偵察行動 (Recon) を行い、その結果得られた情報を元に行われます。「ActiveScout アプライアンス」はファイアウォールの外側に実装され、ActiveResponse 技術を使用して攻撃を検知、防止する IPS です。

ActiveResponse 技術とは、ネットワークトラフィックをモニターし、ポートスキャンなどの攻撃の兆候 (Recon) を検知すると、攻撃者に向けて、特定の目印をつけ、偽情報のレスポンスを戻します。例えば共有ホルダに対する NetBIOS スキャンを検知した場合、NetBIOS プロトコルを使用する共有ホルダの偽情報を返答します。攻撃者であれば、この偽情報を利用して侵入を試みるので「ActiveScout アプライアンス」は単独、またはファイアウォールと連携して該当通信をブロックします。また、攻撃の兆候を検知した段階ではなく、実際の攻撃が発生した際にアラートを発しますので、誤検出はありません。

さらに、攻撃兆候の判断に多くの IDS のようにシグネチャの利用や個々のパケット検査を行うわけではなく、

偵察行動を元に検出する為、既知の手法だけでなく、新たに登場した攻撃手法をブロックすることが可能です。

「ActiveScout アプライアンス」は、ファイアウォールとの連携が可能で、ファイアウォール製品に CheckPoint 社の VPN-1/FireWall-1 を使用している場合、検出した侵入行為をファイアウォールの設定にフィードバックすることで効率的な防御を行うことが可能となります。

アズジェントでは、「ActiveScout」を Celestix 社のアプライアンスにプレインストールの上、販売をいたします。また、2003 年 2 月 5～7 日に開催される Net&Com2003 に出展いたします。(ブース No. Hall5 5420)

【ActiveScout アプライアンス】

販売予定時期：2003 年 2 月下旬

販売目標： 100 台 (初年度)

販売予定価格：

1,550,000 円 (トラフィック量： 0.5Mbps) ～

特徴

- 誤検出の排除
  攻撃者に対して偽情報を提供し、その返答に基づいて正確に判断する為、誤検出がありません。
- 既知、未知の攻撃に対応
  シグネチャやパケットの検査でなく、実際のアクティビティを元に検出するので、既知・未知に関わらず、検出をすることが可能です。
- 運用、管理の簡易化
  シグネチャのアップデート、ログ分析等の設定を必要としません。また、兆候検知、ブロックを自動的に行います。さらに、ファイアウォールの外側間の本体 (Scout) と管理コンソール (SiteManager) から構成されている為、既存のネットワーク構成に変更を行う必要はありません。
- ファイアウォール製品との連携
  ファイアウォール製品と連携をとることにより、効率的な防御を行います。特に ActiveScout アプライアンスは SAMP (Suspicious Activity Monitoring Protocol) を使用して CheckPoint 社の VPN-1/FireWall-1 と連携をとることが可能です。(OPSEC 認定)
- 現在、IDS を使用しているユーザも ActiveScout アプライアンスを導入することにより、IDS の誤検出を約 90%削減できます。
- IDS の様にパケットのデータ部を全てシグネチャによる検査を行う必要がない為、パケットの取りこぼしが少ない。

【会社概要】

会社名：	**株式会社アズジェント**（Asgent, Inc.）
所在地：	**〒**103-0016 **東京都中央区日本橋小網町** 19-7
代表取締役社長：	**杉本 隆洋**（**すぎもと たかひろ**）
TEL：	03-5643-2581
FAX：	03-5643-2571
資本金：	7 **億** 6,800 **万円**
取引銀行：	**みずほ銀行**