



# ActiveScout

## 不正侵入予防システム

ActiveScoutは、偵察行為を監視することにより、攻撃前の偵察行為に対して、「デセプタ(偽装)」情報を送信することにより対応します。これにより、企業のネットワークを既知の攻撃だけでなく、未知の攻撃からも守ります。



### 侵入検知システム (IDS) の現状

主なシグネチャ型の侵入検知システム (IDS) は設定したパターンやシグネチャに合う攻撃を検出するだけで、新しい攻撃方法には対応できません。さらにIDSは大量のフォールスポジティブ (誤報) を生み出す傾向があり、そのため、セキュリティ専門家等のスタッフの時間が浪費され、本当の攻撃が無視されることにもつながります。また、Anomaly (異常) 検知システムの多くも同様にフォールスポジティブを生み出す傾向があります。なぜなら、異常の原因が無害なものか悪意なものかを正しく判断できないことがあるからです。さらに、シグネチャ型でもAnomaly検知型でもIDSは事前対応ではなく事後対応であるといえます。

従って、非常に熟練したセキュリティ専門家がシステムを絶えず調整し、シグネチャを更新し、アラートを分析/判断し、適切に対応するといった作業が不可欠です。しかし、不安な要素が多いシステムにとってはこれらの作業は多すぎるといえます。

### 偵察行為からネットワーク攻撃へ

ネットワークセキュリティの改善のカギとなるのは、攻撃についての十分な知識です。アタッカーは攻撃の前に情報収集として標的にしたネットワークを調査し、攻撃しやすい部分を探し、どの種類の攻撃を仕掛けるかを判断します。これを「偵察行為」といいます。

偵察行為は攻撃を成功させるには不可欠であり、ネットワークのトポロジ、ネットワークサービス、ベンダー、有効なユーザ/パスワード等の情報が必要です。このような情報がないと、ネットワーク攻撃を成功させるのは事実上不可能です。典型的な攻撃は次の3段階を踏むと考えられます。

1. 偵察行為
2. 情報収集
3. 偵察情報に基づいた攻撃

### ActiveScoutの発想

ネットワーク攻撃を前述の3段階のプロセスとみなすと、「なぜ、攻撃を待たずに、偵察行為に事前に対応しないのか」という疑問が当然湧いてきます。セキュリティ管理者は、実際の攻撃 (攻撃プロセスの第3段階) を待たずに、攻撃前の偵察行為に即座に対応して、自社に対する最初の脅威を無効とすべきです。これにより、攻撃を通じて、企業の重要な資産が破壊される前に、攻撃を「つぼみのうちに摘む」ことができます。無数の未知の攻撃ではなく、限られた数の既知の偵察手法からネットワークを防御することにより、フォールスポジティブの問題も事実上なくなります。

#### ※アクティブレスポンステクノロジー (Active Response Technology)

ActiveScoutは、不正アクセスやワームといった攻撃の特定に通常用いられるパターンマッチングや異常探知といった手法を使用しておりません。特許取得済みの独自技術である「アクティブレスポンステクノロジー (Active Response Technology)」により、ツールや感染源のコンピュータが自動的に行う偵察行為を探知し、その相手に送出した偽情報を元に不正アクセスか否かを判別し、防御を可能としています。自らが生成した偽情報を判別の基準としているため、誤検知が非常に少ないのも大きな特長です。

### ActiveScoutの特徴

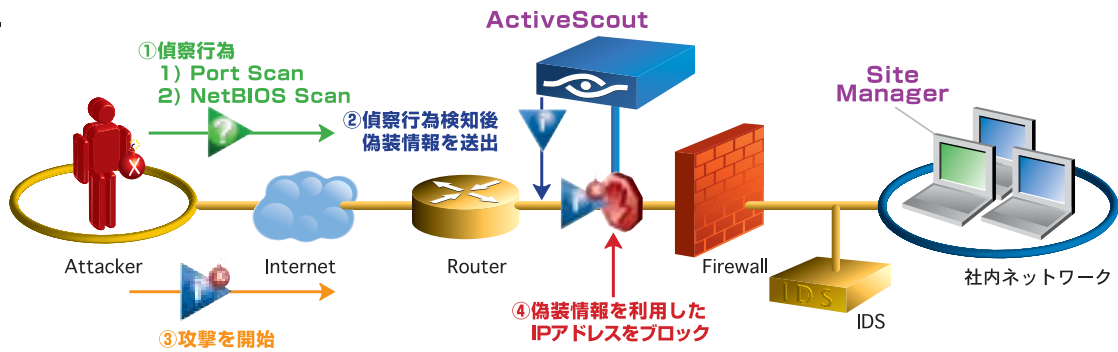
ActiveScoutは、ゲートウェイルータとファイアウォールの間に設置され、企業におけるネットワークのすべてのトラフィックを、監視することができます。ActiveScoutはハブもしくはスイッチのミラーリングポートに設置するため、パフォーマンスが低下することはありません。さらに、ActiveScoutをネットワークの外部との境界に置くことにより、その攻撃自体を無効とすることもできます。

ActiveScoutの主な特徴は以下の様に挙げられます。

- ファイアウォールに到達前に攻撃を無効にする。
- 既知及び未知の攻撃からネットワークを防御する。
- すでにオーバーワーク気味のセキュリティスタッフのワークロードを軽減する。

つまりActiveScoutは、企業が直面している外部の脅威から企業の資産を守るための先進の機能を備えていると言えます。

## 対応フロー



## ActiveScoutの機能等

### ●ブロック機能

ActiveScoutは、伪装情報を利用した独自の方法で侵入者の攻撃を効果的にブロックします。ブロック機能の存在は、外部からはわかりません。

### ●先進のTCP/IP 接続リセット機能

ActiveScoutは、TCP/IP接続を自動的にリセットして不正アクセスと識別された発信元からの通信をブロックします。シーケンス番号に依存した従来のTCP/IP接続リセットは、攻撃の過程でリセットしていましたが、ActiveScoutは攻撃者のTCP/IPハンドシェイク処理が開始された時点で、接続をリセットします。

### ●モニタモードとブロックモードの切替え

ActiveScout搭載のモニタモードとブロックモードを用いることにより、モニタ機能および不正アクセスブロック機能を切り替えることができます。

### ●電子メールとレポートによる警告

オプションにより、イベント情報を指定の電子メールアドレスに通知したり、レポートを送信したりできます。

### ●グラフィカルマップ

ActiveScoutは、グラフィカル・ワールドマップを装備しており、偵察行為／不正アクセスの発信元をわかりやすく表示します。また、履歴データを使用すると、特定の時刻または時間帯のマップを表示できます。

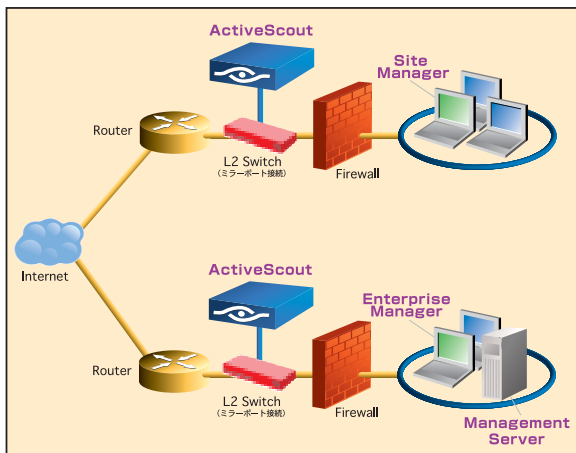


グラフィカルマップ画面

### ●統合管理Server (ManagementServer)

ManagementServerは企業内にある複数のActiveScoutを統合的に管理するサーバです。企業内に複数配置したActiveScoutの攻撃情報やPolicyを統合管理するだけでなく、収集した攻撃情報を各ActiveScoutにエスカレーションするHUBとなる事で、インターネットからの脅威に対し、全社的な対応を可能にします。

## ManagementServerを使った統合管理構成例



## 製品仕様

製品	ActiveScout Gigabit Ethernet Model (アプライアンス)	ActiveScout Fast Ethernet Model (アプライアンス)	Management Server (アプライアンス)
仕様	CPU: Dual Xeon 3.00 GHz Memory: 1 GB HDD: 80GB LAN: 10/100/1000 Base-T×6 Serial: D-SUB9	CPU: Xeon 3.00 GHz Memory: 1 GB HDD: 80GB LAN: 10/100/1000 Base-T×6 Serial: D-SUB9	
外形寸法	4.3 (H) × 70.5 (D) × 42.6 (W) cm 約17Kg		
コンソール	添付ソフトウェア SiteManager (Windows 98/NT/2000/XP、 Linux、Solaris)		添付ソフトウェア EnterpriseManager (Windows 98/NT/ 2000/XP、Linux、 Solaris)

●お問い合わせは

※本カタログに記載の会社名、商品名は、各社の商標または登録商標です。本カタログに記載の仕様については、予告なしに変更することがあります。<2005.01B>

**CTC SP**

伊藤忠テクノサイエンスグループ

**シーティシー・エスピー株式会社**

本社：〒154-0012 東京都世田谷区駒沢1-16-7

TEL.03-3419-9672 FAX.03-3419-9679

http://www.ctc-g.co.jp/ctcsp/

✉ sp-admin@ctc-g.co.jp

・霞ヶ関：TEL.03-6203-5535

・名古屋：TEL.052-203-2239

・大阪：TEL.06-6151-8860

・広島：TEL.082-212-2167

・福岡：TEL.092-734-6251