

IDS製品調査

2002.12

不正アクセス検知の分類

- **不正検知(Misuse Detection)**
 - あらかじめ定義されているデータパターンや通信パターンと合致したものをアラートとして報告
- **異常検知(Anomaly Detection)**
 - 通常時のアクセス(ユーザの行動やトラフィック)と異なった場合にアラートとして報告
- **ホスト型(Host based IDS)**
 - 監視対象のコンピュータ上で動作してログや通信データから不正アクセスを検知する
- **ネットワーク型(Network based IDS)**
 - ネットワーク上の通信データをキャプチャ(sniffing)し不正アクセスを検知する
- **インライン型(In-Line based IDS)**
 - ネットワークセグメントの境界で動作し不正なパケットを検知・破棄する

カテゴリ別IDS比較

| | ホスト型IDS(HIDS) | ネットワーク型IDS(NIDS) | インライン型IDS |
|----|--|---|---|
| 長所 | <ul style="list-style-type: none">・OSやアプリケーションのログファイルを監視できる・ネットワークの構成および速度に依存しない・誤検知が少ない | <ul style="list-style-type: none">・ネットワークを調査するアクセスを検知できる・ホストの種類・数に依存しない・ホストに負担をかけない | <ul style="list-style-type: none">・パケットをとりこぼさない・ネットワークを調査するアクセスを検知できる・ホストの種類・数に依存しない・ホストに負担をかけない |
| 短所 | <ul style="list-style-type: none">・ホストスキャンなどネットワークを調査するアクセスは検知できない・検知自体の負荷がホストにかかる・対応OSが限られる・対象機器毎にインストールおよび設定が必要 | <ul style="list-style-type: none">・高トラフィック時には、データを取りこぼす可能性がある・誤検知(FalsePositive)が多い | <ul style="list-style-type: none">・通信速度がIDSの性能に依存する(高トラフィック時には、パフォーマンスが悪くなる)・IDSが停止すると、ネットワークが停止するリスクがある |

製品動向

- ネットワーク型IDS
 - Gigabit対応の製品がリリースされた。
 - セッション管理機能やパケットログの記録機能を追加した製品がリリースされた。 誤検知を軽減できる。
- ホスト型IDS
 - ログ監視機能だけでなく、ネットワークのトラフィック監視やファイアウォール機能を追加した製品がリリースされた。
 - LKMタイプのrootkitやバッファオーバーフローエクスプロイトの兆候を検知することを目的にシステムコールやプロセスのステータスを監視する製品がリリースされた。
 - カーネルにセキュアなアクセスモデルを実装した上で動作する製品がある。
- インライン型IDS
 - ウィルススキャン連動型製品がリリースされた。
- カスタマイズ
 - snort シグネチャをインポートできる製品がリリースされた。
 - API公開によりモジュールの開発が可能な製品がリリースされた。
- マネジメントツール
 - ネットワーク障害と不正アクセスの監視を統合管理できる製品がある。
 - スキャナ製品との連動により、誤検知(FalsePositive)を軽減できる製品がある。