

ネットワーク不正侵入 監視システム IS1000シリーズ

IS1000シリーズは、Internet Security Systems Inc.の
開発したRealSecure Network Sensor™を横河電機の開
発した専用のハードウェアに実装したネットワーク不正
侵入監視システムである。

[主な特長]

ハードウェア

- ・ 高トラフィックに耐える大容量バッファ
- ・ 侵入者に検知されないステルス構成のネットワークI/F
- ・ 導入容易なフルタンキーシステム

IS1000は、TCP/IPをベースとするネットワークの
データリンク層からアプリケーション層まで全パケッ
トを解析し

- ・ 正常なプロトコルに隠された攻撃
- ・ 異常なプロトコルによる攻撃
- ・ 異常な構成のパケットによる攻撃
- ・ パケット群の異常な振る舞い

を検出して攻撃シグネチャに合致するものがあつた場合

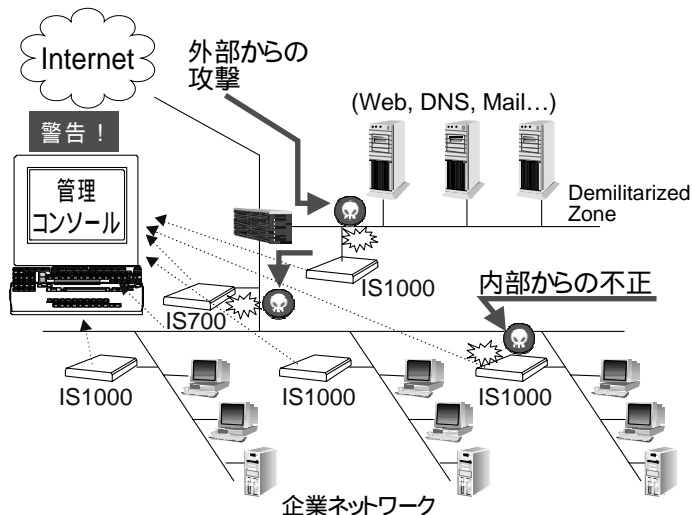
- ・ ネットワーク管理者にE-mailで通報
- ・ Firewallと連携し、セッション切断
- ・ SNMPトラップ

をリアルタイムに実行して攻撃を通報、阻止できる。

定期的に最新の攻撃シグネチャが提供される。

IS1000シリーズは、これらのWindows NTベースの1U
ラックマウント型IS700(予定)がある。

IS1000/700ネットワーク配置例



[IS1000仕様]

ソフトウェア：RealSecure Network Sensor™

対応プロトコル：TCP/IPベースプロトコル；ARP
TCP, UDP, ICMP, SNMP, RPC, FTP, DNS, RTP,
TELNET, SMTP, POP, NNTP, rsh, rcp, finger

攻撃認識：230種類以上

DoS(サービス不能攻撃), E-mail攻撃, HTTP攻撃,
事前スキャン検出等

攻撃シグネチャ：ISS社よりダウンロード

連携可能Firewall：Check Point社FireWall-1

ログ解析ツール：テキスト, グラフレポート機能

ネットワークインタフェース：

監視ポート：

I/F：10/100Base-T

NICバッファ：128 KB

構成：ステルスポート(ネットワークから認識不可能)

コンソール用ポート：

I/F：10/100Base-T

処理部：

SPARCIII/333 MHz, 1 MB/Cache Memory, 256 MB/
ECC main Memory, 9.1 GB HDD

外部インタフェース：

RS-232Cシリアルポート

UPSインタフェース

装置形状：

2Uラックマウント型

88.5 H × 483 W × 510 D (mm)

(注)RealSecure Network Sensorは別途管理コンソール
用PC(WindowsNT)が必要。

問い合わせ：T&M東京営業部COMグループ

E-mail：IS1000@csv.yokogawa.co.jp