横河電機のネットワークセキュリティ製品 IS1000/IS700

IS1000/IS700 Network Security Products of YOKOGAWA

荒澤 永樹*1 ARASAWA Hisaki
中村 昌文*1 NAKAMURA Masafumi
行田 茂*2 GYOUDA Shigeru

当社では2000年４月からInternet Security Systems社製のネットワークセキュリティ製品RealSecure Network Sensor，Internet Scanner，Database Scanner，RealSecure OS sensorを扱ってきており，この中のRealSecure Network Sensor用に，ステルス構成と大容量バッファを持つNICを装備した専用機を共同開発した。

Since April 2000, we have been dealing in network security products of Internet Security Systems Inc. (ISS), such as RealSecure Network Sensor, Internet Scanner, Database Scanner and RealSecure OS sensor. We have developed a device dedicated to RealSecure Network Sensor in partnership with ISS. The device has a NIC with very large buffer and a stealth configuration.

1. はじめに

インターネットを基盤とする近年のIT応用技術の発展と共に，インターネットからの不正アクセスが押し寄せて来ている。不正アクセスは，全世界をシームレスに接続する事で得られる利便性の裏返しでもある。プロセス制御システムも例外ではなく，e-ビジネスと同様に多大な被害を被る可能性が否定できない。

典型的なネットワークへの不正アクセスとして，サービス不能攻撃，データや通信の盗聴，データ改竄及び盗難がある。通常，インターネットへの接続点や重要なネットワークの接続点には，アクセスを制限するファイアウォールが置かれるが，攻撃はファイアウォールが許可しているプロトコルに仕込まれる事が多い。これはファイアウォールの限界を示しており，例えhttpプロトコルしか通さない設定をしていても，通過するパケットの中身まで調べない限り，攻撃の対象になってしまう可能性がある。更にデータ漏洩事件に見られるように，組織内部の人間によるシステムの誤使用等が無視できないことも見逃してはならない。本稿では，パケットの中身まで調べることができる Internet Security Systems社の不正侵入検知ソリューションRealSecure Network Sensorを搭載したネットワーク不正侵入システムIS1000/IS700を開発したので，それを中心に紹介する。**図１**に本器の外観を示す。

2. セキュリティ製品群

ネットワークのセキュリティを保つために，ファイアウォール，暗号化，認証，ワンタイムパスワードといった防止策に加え，更に監査(脆弱性の検出)，脆弱性への対応，攻撃の監視が重要である。

当社では，これらの用途に用いるInternet Security Systems社製のセキュリティ製品群を取り扱っており，ネットワークとシステム上に監査，監視用ツールとして**表１**の製品群を用意している。

2.1 Internet Scanner

Internet Scannerは，ネットワークに接続されたサーバー，クライアント，ネットワーク機器の脆弱性を検出するのに用いられ，システム管理者が気付いていないセ

図１　IS1000/IS700の外観

*1 T&M事業部 通信ネットワークテスティング開発部
*2 T&M事業部 東京営業部

表１　ISS社のセキュリティ製品群

カテゴリ	機　能	製　品　名	機能概要
ホストベース製品	ホスト監査	System Scanner	ホスト上の重要なファイルなどのセキュリティ監査
	ホスト監視	RealSecure OS Sensor	ホスト上での攻撃検知,対応
データベース製品	データベース監査	DataBase Scanner	データベースセキュリティ監査
ネットワークベース製品	ネットワーク監査	Internet Scanner	ネットワークからのセキュリティ監査
	ネットワーク監視	RealSecure Network Sensor	ネットワークトラフィックの攻撃検知,対応
	Sensorの管理	RealSecure Work Group Manager	RealSecure OS Sensor, Network Sensorの管理, 監視機能

キュリティ上の問題や，計画されたセキュリティポリシーの実際を監査する。期待するセキュリティレベルを明確にし，実際にその通りになっているかどうかを検証する。

図２に，予め用意されている監査する内容を集めたポリシー一覧を示した様子を示す。ポリシーは，基本的なポリシー，UNIX用，WindowsNT用，Router&Switch 用などが用意されており，この中から適切なポリシーを選択して，必要ならば内容に修正を加えた後，ユーザーの独自名でスキャンの範囲，IPアドレスの指定と共にセッションとして保存する。セッションはポリシー，スキャンの範囲，IPアドレスの指定を行って作成される。

各ポリシーの先頭には，L1からL5のレベルが付けられているが，通常はこの順序でスキャンを行い，レベル毎に問題となる部分を解決しながらシステムを修正していく。

2.2 RealSecure Network Sensor

RealSecure Network Sensorはネットワークを流れる全てのパケットを捉え，各プロトコルについて攻撃シグネチャを検査し，攻撃と思われるパターンを検出した場合に，管理者への通報やFire Wall と連携動作を行い，セッションを切断するなどしてネットワークを守る。

RealSecure Network Sensorは，Internet接続部，或いは公開サーバーのあるDMZ(Demilitarized Zone)，社内のネットワークセグメントなど，攻撃から守りたいデータやサーバーなどの装置が接続されているネットワークへ設置する。**図３**にRealSecure Network Sensorの配置例を示す。Fire WallへのInternetからのアクセス状況，DMZに対する攻撃，社内サーバーへの攻撃の監視を行っている。これらのRealSecure Network Sensorは，一台のWindowsNT上で動作するWork Group Managerから制御されている。

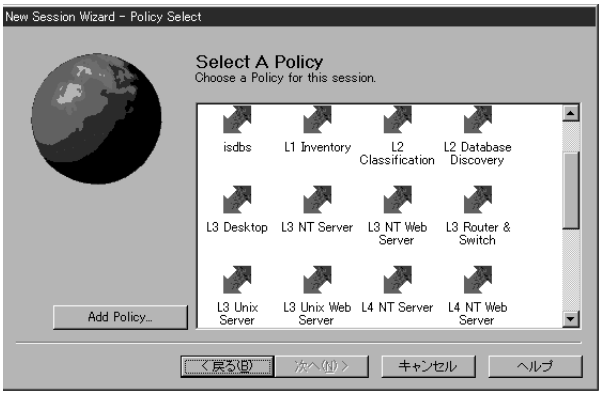

図２　Internet Scanner ポリシーの一覧

図４にWork Group Manager の画面を示す。画面は５区画に分けられ，Activity Treeウィンドウ，危険度を高，中，低と表示する３個のPriorityウィンドウ，Sensorウィンドウから成る。

画面左側のActivity TreeウィンドウにはRealSecure Network Sensorが検出した不審な動きや攻撃を，検出されたSensor毎にIPアドレスの発信元，宛先，どのような挙動が検出されたかというEventにまとめて累積表示する。画面右側の３個のPriorityウィンドウにはSensorが検出したEventの種類を優先度別に時系列で表示している。

Sensorウィンドウは稼働中のSensor状態を，Sensor名，使用しているポリシー，稼働状態，Work Group ManagerとSensorとの間で通信チャネルが確立しているかどうかをリアルタイムに表示している。

図５にRealSecure Network Sensorレポート機能を示す。レポートにはテキストレポートの他，グラフの出力があり，一見して異常な振舞いを見ることができる。RealSecure Network SensorもInternet Scannerと同様，V5.0からX-Press update機能が装備されており，新たな攻撃手法が発見された場合には，Webを通じてポリシーを短時間で提供する。

3. RealSecure Network Sensor搭載専用ハードウェアIS1000/IS700

RealSecure Network Sensor専用機としてIS1000，IS700を開発した。IS1000はUNIXをベースとし，動作安定度を主眼とした装置であり，IS700はWindowsNTを用いてコストパフォーマンスを考慮した装置である。両装置共に2U(IS1000)，1U(IS700)ラックマウント型なのでスペースを省け，データセンターなどへの導入時には余分な手間や設定の誤りを防ぐことができる。専用機は下記の特長を持つ。

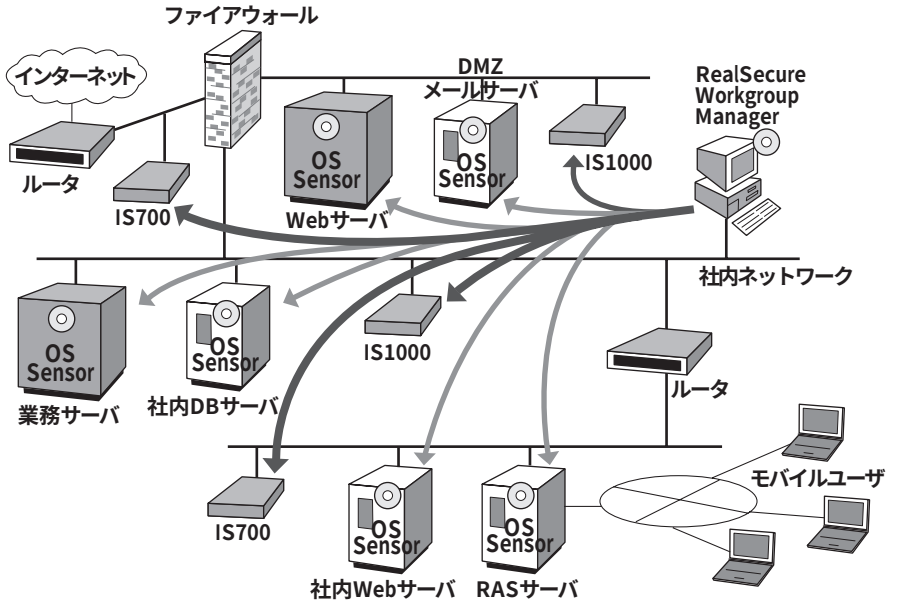

図３　RealSecure Network Sensor の配置例

(1) ステルス監視

ネットワーク監視型不正侵入検出装置は，侵入者にその存在を知られないようにする必要がある。IS1000，IS700ではネットワーク監視ポートをIPアドレスを持たないステルス設定としており，侵入者が入り込むインターネットの接続点に設置した場合でも，ポートスキャン等によりその存在を知ることはできない。

(2) パケットキャプチャ能力

前述したように，IS1000，IS700ではネットワークをステルス監視する。ステルス監視はネットワークに対し，自らの存在を通知しないためその存在を知られないが，TCP/IPで通常行っているネットワークトラフィックのネゴシエーションはできないという問題がある。

TCP/IPプロトコルを使って二台のコンピュータ間でパケットを送る場合，データ受信側コンピュータのバッファの残りが送信データに対して少ない場合，バッファが空くまでの間，送信を保留させることがある。**図６**に示すように，WS1はSEQ 400でSize 100のパケットを送信しようとするが，WS2の受信バッファが空いていない場合，WS2はSize 0で

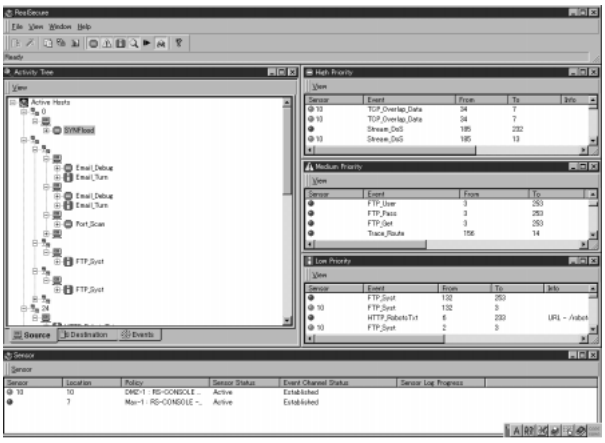

図４　Work Group Manager 画面

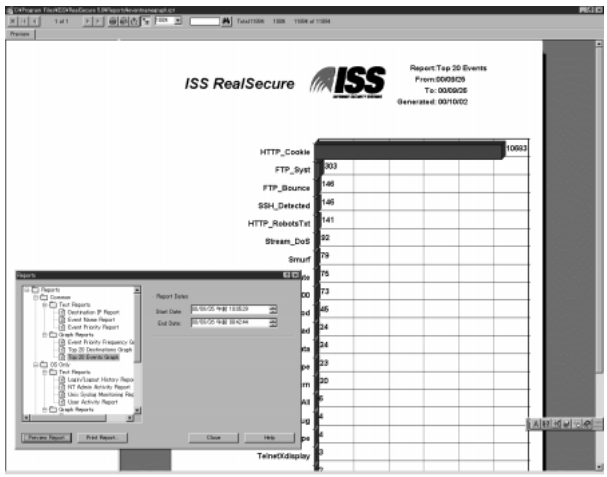

図５　レポート作成画面と生成したグラフ

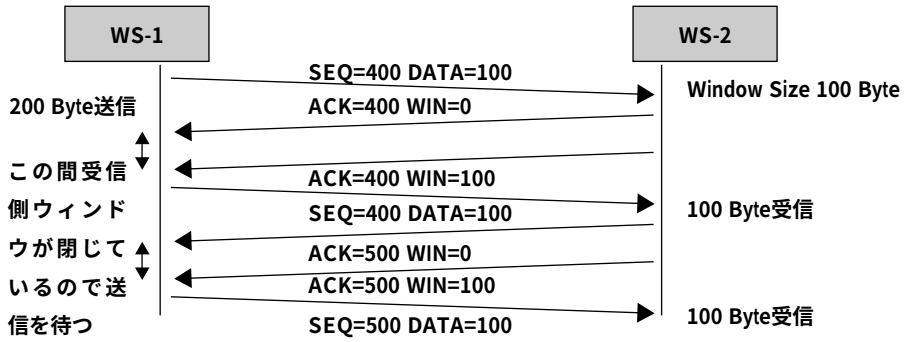

図6　TCP Window Sizeによるフロー制御

同一SEQナンバーを返送し，WS1に対してバッファに十分な空きが無いことを知らせる。WS1は，再度パケット送信を試み，WS2のバッファが空いたとき，WS2はSizeを０ではない値でACKを返送し，WS1からデータが送られる。

しかし，ステルス構成の場合にはバッファ容量が少ないことを通知できないので，授受されるパケットを全て取り込まなければならない。

一般的なEthernetに使用されるNICは，数十Byteから３KB程度の大きさのバッファを持っているが，これらをステルス構成にして使用しようとする場合，バッファの容量に配慮しないと大きなパケットが到来した時にNICバッファオーバーフローを起こしてしまい，パケットを正しくキャプチャできなくなる。

IS1000，IS700ではバッファサイズを最低64 KB以上に大きく取り，パケットを最大限キャプチャして，パケット内容の解析を行うRealSecure Network Sensorのネットワーク監視動作をより確かなものにしている。

(3) セキュリティ設定

インストールしたままのOSのデフォルト設定では，意図しない状態で不要なサービスが動いているため，その上でRealSecure Network Sensor を稼働させるのはセキュリティ上問題がある。IS1000/IS700ではRealSecure Network Sensorの動作に最大限のリソースを向け，コンソールポートへのアタックを考慮したOSのセキュリティ設定を，工場出荷時に行っている。そのため，導入時のOS設定など誤りを誘発する作業が不要である。

WindowsNT，Solarisの各OS共サービス制限，ポートの制限，アカウントの制限を行い，侵入を防止している。しかし，最終的なガードは管理者権限のパスワードとなるので，ハッキングされ難いパスワードの設定が重要である。

6. おわりに

ネットワークセキュリティのソリューションとしてInternet Scanner，RealSecure Network Sensor，IS1000/IS700を実例を基に紹介してきた。データセンター，ISP（Internet Service Provider），ASP（Application Service Provider），企業のインターネット接続点など適用する範囲は広範囲に亘る。

ネットワークセキュリティレベルは，色々な要因で必ず下がり始める。これを常に一定のレベルに保つためにも，適切なセキュリティ監査，監視製品を定期的に使用する事が望まれる。

参考文献

(1) Hacking Exposed : Network Security Secrets and Solutions Stuart McClure, Joel Scambray, George Kurtz Osborne/ McGraw-Hill 1999

(2) http://www.fish.com/survey/

(3) http://www.2600.com/　http://www.rootshell.com/ http://www.lohp,com