ネットワーク・セキュリティと管理システムについて

Network Security and Security Management System

桂川昌治* 井上大輔*
M. Katsuragawa *D.* Inoue

Synopsis

Organizations rely increasingly on information technology to support their rapid growth and expansion into the global marketplace. Technologies such as the Internet, extranets, and Intranets are allowing companies to reach people and markets in a way never before imagined.

However, with all of the benefits that technology brings to an enterprise, it also brings increased vulnerabilities and threats. Many companies are faced with a growing concern over the impact of disgruntled employees, hackers, unauthorized users, industrial spies, and mischievous employees exploiting and compromising their information systems and networks. Because of the very nature of an open environment, your risk of revenue and information loss is greater.

At first, we explain such vulnerabilities and threats generally, then introduce the methodology and tools for network security management.

1. まえがき

今年1月から2月にかけて，中央省庁のホームページが書換えられたり，サービスプロバイダがサービス停止に追い込まれるといった事件が世間の耳目を集め，これを契機としてセキュリティ対策の必要性がますます強調されるようになってきた。

ホームページの書換えについては，15件中6件はインタネットよりバッファオーバフロー攻撃により書換えられたことが公表された。ファイアウォールの外側に設置されたWebサーバが攻撃されたようであるが，中にはファイアウォールが設置してあっても，ホームページの管理用に開けていたFTPからログインを許してしまった場合もあった。さらに，昨年末に米国CERTが再度警告していた分散サービス不能攻撃DDoS（Distributed Denial of Service）が実際に多くのサイトに大きな被害をもたらした(1)。

セキュリティ対策・管理の不備により外部からホームページの書換えができてしまうということは，単に自社だけの被害にとどまらない。企業活動に関するデマ情報を書き込んで株価操作したり，自社マシンにDDoS「ゾンビ」プログラムを挿入されることも起きかねない。つまり結果的にアタッカに加担してしまうといった深刻な反社会的行為に利用される危険をはらんでいることになる。

こうした不正アクセスに対抗するためには，ファイアウォールをはじめとする防御策を講ずるだけでなく，日々の運用でのセキュリティ管理が重要となる。

そこで本稿では，不正アクセスの概要とその対策の基本について述べた後，当社が日本語化し，販売を行なっているAXENT Technologies社（以下AXENT社）のセキュリティ管理ツールを紹介していく。

2. 不正アクセス手法について

まず，最近の不正アクセスの手口についてみてみよう。不正アクセス行為を大きく分類すると，情報収集，権限奪取，目的達成の各段階に分けられる侵入行為と，主として業務妨害やいやがらせ的に仕掛けられるサービス不能攻撃があげられる。

情報収集段階では，公開情報やツールを用いてOS/サービスのバージョンの特定などが行われ，得られた結果から既知のセキュリティホールがないかを探索する。

権限奪取段階では，得られた情報をもとにセキュリティホールを突いた攻撃もしくはパスワード攻撃などでユーザ権限，さらには管理者権限奪取を狙う。

* 情報通信開発事業部 技術部

目的達成段階では，奪取したユーザ/管理者権限を使い，不正プログラムのインストール，ホームページコンテンツ，ログファイルなど重要ファイルの変更・改ざんなどが行われる。

サービス不能攻撃は，機能麻痺，業務妨害を目的としている。この種の攻撃ツールも多数公開されており，最近では「まえがき」で紹介したように，分散型のDDoS攻撃へと進化している。上述の侵入行為が不成功に終わった場合に使用することも多いようだ。

3．不正アクセス対策の基本

不正アクセス対策では，攻撃を受けても耐えられる，もしくはできるだけ侵入を許さない状態にしておくことと，不正アクセス行為の各段階で常時監視し不正アクセス検出，緊急対応を行うことが基本である。

3・1 ファイアウォールの設置

インタネット接続においてWebサーバ，FTPサーバなどの公開サーバを保護したり，イントラネットの重要サーバを保護するための基本的対策は，やはりファイアウォールを正しく設定し設置することである。ファイアウォールはアクセス制御とイントラネットの隠匿，そして通信ログの記録・保管が主な機能である。

正しく設定されたファイアウォールは，通過を許可していないプロトコルやアドレスを持つパケット，SynFlood攻撃などのサービス不能攻撃に使用される異常なパケットを遮断するため，ほとんどの不正アクセスは拒否される（**図1**[*1]）。

3・2 セキュリティ・アセスメントと対策

ところが，ファイアウォールも万能ではない。一般公開用Webサーバや FTPサーバの場合，インタネット上の不特定多数のマシンからアクセスできることを目的に作られているので，ファイアウォールはWebや FTPなどのサービス提供に必要なポートでの通信を許可しなければならない。つまりファイアウォールで通信を許可しているサービスは，常にインタネットからの脅威にさらされていることになる。

HTTP，SMTP，FTPなどは，多くのサイトで通信を許可しているので，アタッカのターゲットになりやすく，多くのセキュリティホール，攻撃手法が現実に存在している。また，デフォルト設定のOS，アプリケーションでは適切なセキュリティ対策がなされていない場合がほとんどで，ここにも多くのセキュリティホールがある。

そこで，まずこれらのサーバをはじめとするネットワーク上のマシンに，セキュリティホールとなるバグや設定ミスがないかどうか予め検査し，対策しておくことが重要である。しかし，闇雲にセキュリティ対策を行なっていては，手間と費用がかかるばかりである。組織のセキュリティポリシーに基づくガイドラインを順守した対策がポイントである（図1[*2]）。

また，ネットワークシステムは日々変化し成長するため，こうしたセキュリティアセスメントと対策を日々の運用管理のなかで実施していくことがより重要となる。えてして導入時だけは確実に実施するが，あとは「ほったらかし」という状態に陥りやすい。

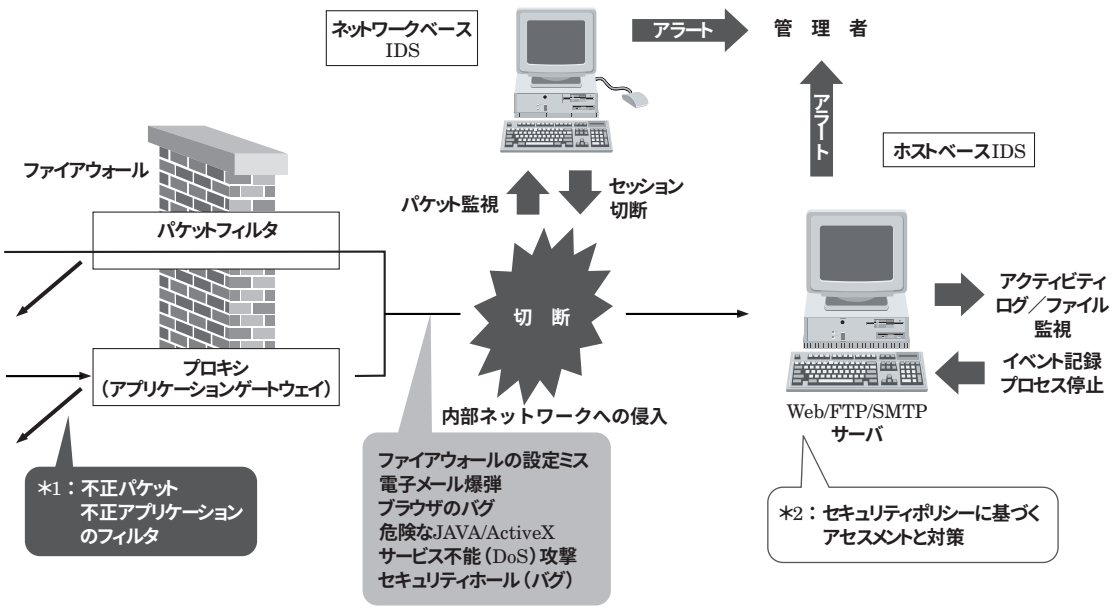


図1 不正アクセス対策

つまり，セキュリティアセスメントとは，現在の各種セキュリティに関する設定と，セキュリティガイドラインとの違いを検査し，決められたルールの順守状況を日々管理していくことに他ならない。

3・3 不正アクセスの常時監視

セキュリティ管理のもう一つの重要な要素は不正アクセスの常時監視である。図1に示すように，外部ネットワークもしくは内部からファイアウォールを“すり抜けてくる”各種の攻撃に対して，不正アクセス監視システム（IDS）による常時監視が必要となる。IDSでは次のような基本機能が求められる。

- パケット，ログなど種々の情報からの不正アクセスやそう疑われる事象の検出。
- 管理者への通知。
- セッション切断，ファイアウォール設定変更などでの緊急対応。
- 検出したデータの記録。

4．セキュリティアセスメント

現在，セキュリティアセスメントツールとしてAXENT社のEnterprise Security Manager（ESM）とNetReconを提供しており，それぞれ異なる技術を採用したこれら二つのツールを組み合せたアセスメントを推奨している。

まず，NetReconは，ネットワーク上の1台のWindowsNTマシンにインストールし，検査対象システムをネットワークから模擬攻撃して，アタッカの立場で検査を行う。OSの特定，利用可能なサービスを検出し，重大なセキュリティホールになりうる弱点を報告するネットワークベースのツールである。現在，約400個の弱点を検出することができる（Ver.3.04）。サーバなどのさまざまなアプリケーションのセキュリティホールに対応しており，アプリケーションを中心とするセキュリティ検査に特に有効である。

一方ESMは，セキュリティポリシーから導かれたガイドラインに従って，システムの内部からOSのセキュリティ設定を中心に検査を行うホストベースツールである。ESMは，セキュリティ管理者の立場で，セキュリティガイドラインを基準とし，これを順守していない事項を検出結果として報告するので，「監査」ツールであるともいえる。

図2に示すように，総合的なセキュリティアセスメントを行う上で，二つのツールを組み合せることにより精度の高いアセスメントを実現できることがわかる。たとえば，NetReconのようにスキャナだけの検査では，検査内容がアプリケーション中心となり，OSのセキュリティ設定など検査できない部分が出てくるからである。

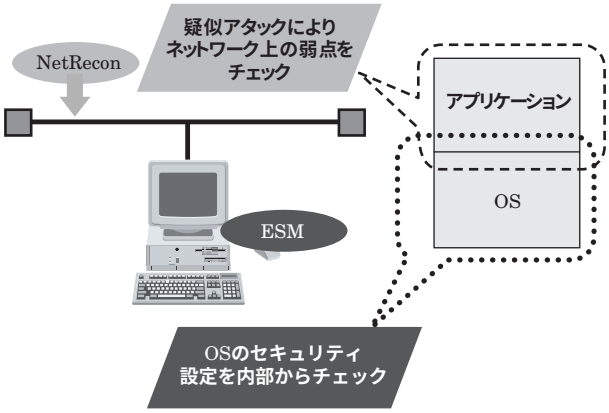


図2 AXENTセキュリティ・アセスメントツールの構成

4・1 ホストベースアセスメントツール：ESMの概要と特長

ESMの特長の一つは，マルチプラットホーム対応できめ細かく検査できることである。ESMの検査範囲は30種類以上のOS/バージョン，通算検査項目1,200以上に及ぶ。

さらに画期的な点は，これらの多数のチェック項目を平面的に管理するのではなく，組織に応じたセキュリティポリシーから導かれる15のカテゴリ（スタンダード）に分類して管理できる点にある（**表1**）。

AXENT社では，この考え方をさらに推し進め，ユーザのレベルとニーズに合わせてバランスのとれた管理を実現するために同社のノウハウを盛り込んで，五つのレベルのデフォルトポリシーとして提供している。このうちPhase 1レベルでは，最も基本的で順守すべき必須項目がまとめられている。

(1) サービス検査，セキュリティパッチ検査

起動される各種サービス（アプリケーション）がセキュリティガイドラインどおりにセッティングされているか，最新のセキュリティパッチがインストールされているかを検査する。

(2) パスワード検査

パスワードの設定・運用については，つい面倒がられるが最も重要な項目である。インタネットに公開するWebサーバにおいても，管理者権限パスワードが簡単なパスワードであると，容易に不正アクセスの被害に遭うことになりかねない。またコンテンツの更新用アカウントID，パスワードについても同様で，セキュリティポリシーに沿った形で運用されているかどうかを日々検査・管理しておく必要がある。

(3) システムのセキュリティ監査設定

システムログの設定，パスワードの最低長さ，有効期限，アカウントロックアウト設定など，デフォルトのままでは，重大なセキュリティホールにつながる設

表1　ESM の監査内容

No.	分　類	概　　要
1	Account Integrity	セキュリティポリシーを越えるような権限を持つアカウントの監視
2	Backup Integrity	バックアップされていないファイルの監視
3	File Access	セキュリティポリシーに基づくファイルアクセス設定の検査
4	File Attribute	ベースラインから変更されたアトリビュートを持つファイルの監視
5	File Find	ウイルス等データ消失につながるファイルの検査
6	Login Parameters	セキュリティポリシーに違反しているログインパラメータの監視
7	Object Integrity	オブジェクトファイルのオーナ/アクセス許可変更の監視
8	Password Strength	パスワード設定の検査
9	Startup Files	潜在的にセキュリティ違反となるスタートファイルの検査
10	System Auditing	システムアカウントと検査ログのモニタ
11	System Mail	セキュリティ消失につながる既知メッセージの検査
12	System Queues	システムキュー検査による不正アクセスの監視
13	Os Patches	インストールされているパッチの検査
14	User Files	ユーザファイルのオーナ/アクセス許可の検査

定項目は多数存在する。これらも運用開始時点だけでなく，日々の管理が必要となる。

ファイアウォール，暗号通信ツール，ワンタイムパスワードなどのセキュリティ製品などはほとんどが何らかのOSの上にインストールされることから，OS自身のセキュリティアセスメントが実施され，管理された状態でセキュリティ製品をインストールしないと，セキュリティ製品自身の信頼性すら確保できない状態になることはいうまでもない。

(4) ユーザ権限検査

ユーザに与える権限は厳密に管理しなければならない。日々の運用などで必要だからとの理由で容易に管理者権限を与えてしまうことが多い。これも最低限の権限のみ与える必要がある。

(5) 重要ファイルの検査

トロイの木馬を使った不正侵入対策として，日常的に使用しているアプリケーション，OS関係の重要ファイルの検査が必要となる。データベースファイル，ホームページのコンテンツのアクセス権管理を適切に行うことで不正アクセスに備えなければならない。

(6) File Find（UNIX の場合）

管理者が認識していない場合が多いようであるが，新たにrootにsetuid, setgidされたファイルの有無には特に注意が必要である。不正プログラムの可能性がある。

4・2 ESM のアーキテクチャ

図3にESMのアーキテクチャを，**表2**にその特長を示す。企業ネットワーク規模での監査を実現する上で，監査ツールのアーキテクチャは非常に重要である。ESMで採用しているマネージャ－エージェントアーキテクチャは，ほかのアーキテクチャと比較して，特に大規模なネットワークでその能力を発揮する。他社製品に比べ，ネットワーク全体についての調査報告，マルチ/クロスプラットフォーム環境での動作といった点で優位になっている。

また，ネットワークトラフィックの通常業務への影響については，ESMの場合，監査の結果を各エージェントがマネージャに報告するときに発生する程度であり，業務に支障をきたすことはない。さらに，ESMエージェントはアイドルプロセスと同一レベルで動作するため，CPU負荷の点からも業務アプリケーションに影響しないようになっている。

図3に示すように，マネージャ－エージェント間，マネージャ－GUI間はTCP/IPでの独自方式の暗号通信で接続される。

マネージャは，ESMポリシー管理，エージェント管理，監査実行管理，監査結果管理といった管理を行うとともに，エージェントに対してESMポリシーのダウンロードや監査実行指示を出す。各マシンにインストールされたエージェントは，マネージャの指示により監査を行なった後，結果をマネージャに通知する。ESMのGUIはマネージャから独立しており，同時に複数のマネージャにログインして，全体の統計データを見ることができる。全組織の状態が1台のコンソールから，一目で把握できるようになっている。

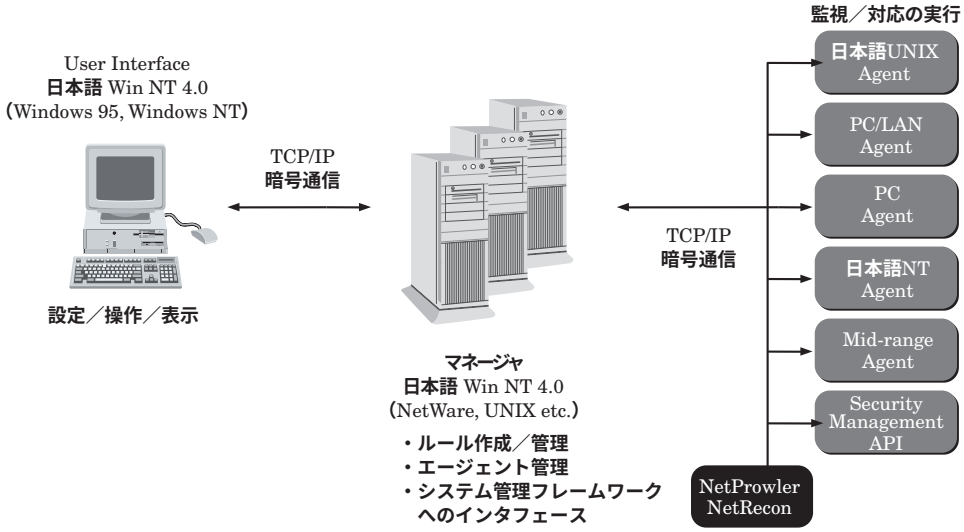


図3 マネージャーエージェントアーキテクチャ

表2 アーキテクチャ比較

	シングルシステム型	クライアント型	マネージャ・エージェント型
アーキテクチャ	対象マシン 1 台ごとにインストールし実行。	ネットワーク上の 1 台実行。ターゲットはマントして調査。	ターゲット 1 台ごとにエージェントが走る。レポートのみマネージャに上げる。
製品例	SDI：Kane Security Analyzer	ISS：System Scanne	Axent：Enterprise Security Manager
全体集計報告	不可能	可能・マシン負荷大	広範な集計・分析が可能 マシン負荷は軽い
複数 OS 対応	極めて困難	困難	50 以上に対応済み
上位情報統合	可能	不可能	実現済み
ネットワーク負荷	―	大	小・大規模ネットワークでも OK

5．不正アクセス監視システム

最近特に注目されている不正アクセス監視システム（IDS）は，ファイアウォールなどのフィルタ装置と協調して，より高い精度で不正アクセスを検出・防止するシステムである。

AXENT 社の Intruder Alert（以下ITA）は，エージェントソフトウェアを監視対象マシンにインストールし，ログインなどのイベントやファイルアクセスや改ざんなどのアクション，および各種ログを監視するホストベースツールであり，NetProwler は，ネットワーク上を流れるパケットを監視するネットワークベースツールである。

これらのツール/技術には**表3**に示すように，各種の攻撃方法に対して，それぞれ得意/不得意があることがわかる。セキュリティアセスメントの場合と同様，IDS 導入の一つのポイントは，この二つの技術を組み合わせて導入することにより，両者の得意とするところを生かして不正アクセス監視の精度を向上させることである。

次にそれぞれの概要と特長を見てみよう。

表3 ホストベースとネットワークベースの比較（1）

主なアタック方法	ホストベース	ネットワークベース
対応製品	ITA	NetProwler
Denial of Service	△	◎
スキャニング & プロービング	○	◎
パスワードへのアタック	○	△
管理権限の横取り	◎	―
不正プログラム挿入	◎	△
ファイル等の破壊行為	◎	△
機密情報の盗み取り	○	○

5・1 ホストベースIDS：ITAの概要と特長

ホストベースIDSでは，syslogやC2監査ログなど，OSや各種アプリケーションが出力するログの中から，既知の不正アクセスに伴うログパターンを検出する方法が一般的である。ITAではこれらのログパターンをルール形式で記述している。たとえばWindowsNTでは，Administratorでログオンに失敗すると，NTのセキュリティログの一部に“ログオンの失敗”と“Administrator”の文字列が記録される。ITAにはこれらを検出すべきキーワードとして検出データベース（ITAルール）に登録する。

しかし，現在のホストベースIDSは1台のマシンのログを監視するタイプが多いが，1台のログだけでは不正アクセスかどうか判別できない。この例では，Administratorでログオンに失敗したとき，このログが，管理者が実際に誤ったものか，アタッカがネットワーク上のマシンに順次ログオンを試みているものか判別できない。

そこでITAでは，各監視対象マシンのエージェントが相互に検出したイベント情報を交換できるようにしている（**図4**）。ESMと同様，マネージャーエージェントアーキテクチャにより，1台のマシンのログだけでなく，他のマシンつまりネットワーク上で発生している事象を総合的に見て判断できるようになっている。図4の場合は，1分間に同一ドメイン内の異なる3台のマシンでAdministratorログオン失敗を検出すると，不正なログオン行為とみなして管理者に警報する。

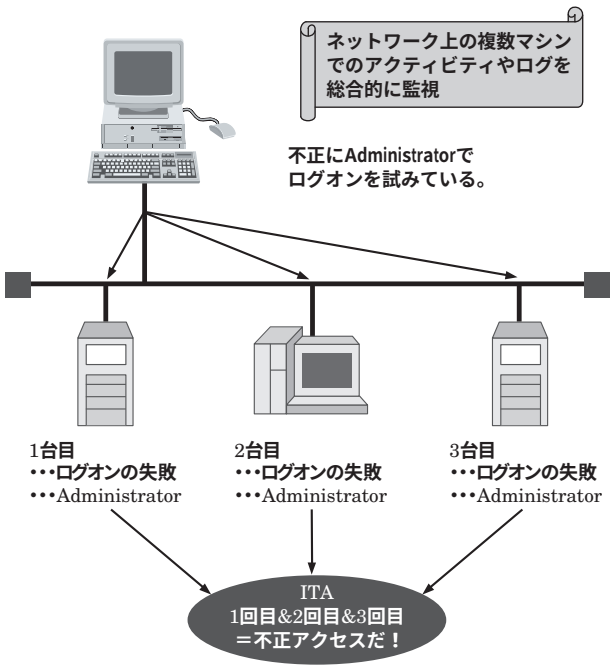


図4 ITAにおけるログ/アクティビティ監視

ITAのもう一つの特長はファイル監視機能である。ファイルの書換えやファイル操作を行うタイプの不正アクセスに対して特に有効である。たとえば，「トロイの木馬」はNotePadのようによく使用されるプログラムに“ウイルス”として不正プログラムを挿入しておき，ユーザが起動したときに感染するタイプの不正アクセスである。よく知られた「トロイの木馬」には，パスワード入力をモニタしてネットワーク経由で盗聴するプログラムがある。

ITAでは，ファイルの生成/変更日付等のファイル属性，チェックサム，MD5メッセージダイジェスト等を常時監視しておき，監視対象ファイルが「トロイの木馬」を仕込まれたファイルで書き換えられた段階，すなわち感染する前に直ちに警告する仕組みとなっている（**図5**）。

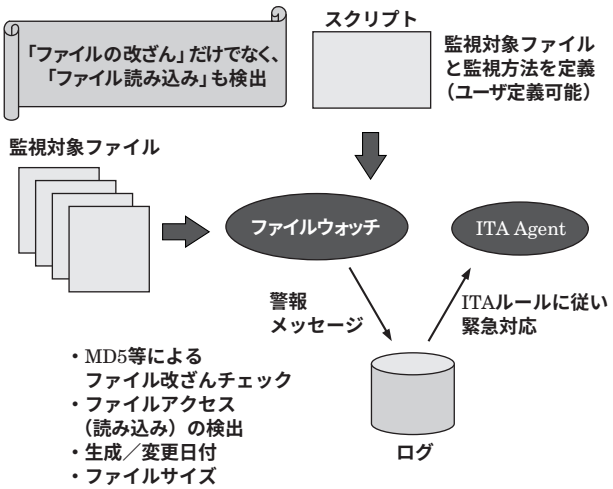


図5 ITAにおけるファイルウォッチ機能

5・2 ネットワークベースIDS：NetProwlerの概要と特長

現在国内で市販されている多くのIDSが，ネットワークベースおよび送受信パケット監視タイプである。SynFlood攻撃はじめ大量のパケットを送りつけて，コンピュータを麻痺させてしまう各種のサービス不能攻撃やポートスキャンに対しては，AXENT社のNetProwlerのようなネットワークベースIDSによるパケット監視が特に効果的である。

NetProwlerでは「攻撃シグネチャ」と呼ばれる不正アクセスで使用されるパケットのパターンを記述したデータを保持し，これらと実際のネットワーク上を流れているパケットを比較して検出している。

ファイアウォールも，受信した一つのパケットのヘッダおよびデータを解析して，その通過の可否を制御しているが，ネットワークIDSの特長は，一つのパケットを

単独で解析するだけでなく，DoS攻撃の検出に有効なカウンタベースでの解析や，一連のパケットの内容・順番を判断するシーケンシャルベースでの解析ができることである。

また，検出時の対応としては，管理者への報告・警告だけでなく，不正アクセスまたはそう疑われるセッションの切断，ファイアウォール設定変更によるパケットの一時的遮断などを自動実行する緊急対応機能が実装されている（**表4**）。

AXENT社には，ウイルス対策ソフトと同様，新たな攻撃手法を常時モニタに検出するためのシグネチャを開発する研究・開発チーム「SWAT Team」があり，その成果をWebで公開している。最近の具体的成果として，Trinoo，TFN，TFN 2 K，StachelDrachtといったDDoS攻撃におけるアタッカと攻撃元となる「ゾンビ」プロセスとの間の通信を検出するシグネチャが提供されている。

しかし，最近のネットワーク・インフラの劇的進歩はネットワークベースIDSにとっては厳しい環境をもたらしている（**表5**）。

表4　ITA/NetProwlerにおける不正アクセス検出時の対応

No.	項　目	概　　要
1	Append to File	発生したイベントログを指定ファイルに追加する。
2	Send E-mail	指定したアドレスに電子メールを送信する。
3	Notify	イベントメッセージ＋オプションメッセージを指定したITA ユーザに通知する。
4	Pager Action	エージェントマシンのモデムからページャを呼び出す。
5	Kill Process	イベントのトリガとなったプロセスを kill する。（UNIX） イベントが発生したユーザのプロセスをすべて終了する。（NT）
6	Excute Command	指定したOS/ユーザコマンド、シェルコマンドをバックグランドで実行する。
7	Disable User Account	ユーザアカウントを使用できなくする。
8	Run Shared Action	他の ITA ルールを実行する。
9	Raise Flag	イベントの発生を期限付きで他のエージェントに通知するフラグを ON にする。
10	Cancel Flag	フラグを OFF にする。
11	Start Timer	ITA ルールで使用するタイマの呼び出し。
12	Cansel Timer	タイマを OFF にする。
13	SNMP Trap	SNMP Trap 発行。
—	（NetProwler）	RST パケットの送信。
—	（NetProwler）	ファイアウォールの設定変更。

表5　ホストベースとネットワークベースの比較（2）

	ホストベース（ITA）	ネットワークベース（NP）
インタネット監視	F/W と異なる技術を使用	F/W と同じ技術を使用
イントラネット監視	マシン単位で対応	セグメント単位で対応
検知時対応策	多	少
スイッチングネットワーク対応	依存しない	セグメント毎に設置要
暗号化対応	依存しない	検知不能
ネットワーク速度/ トラフィック対応	依存しない 特別なマシン不要	限界あり（パケット落ち） 高速マシン必要
Denial of Service 対応	不得意	得意

たとえば，

- 電子商取引きの発展に伴い，SSLなどの暗号通信が普及しつつあるが，暗号パケットは解析できない。
- ギガビットネットワークも登場しているが，このような広帯域でのパケットをすべて解析するのは事実上困難である。
- スイッチングネットワークが今や常識となりつつあるが，すべてを解析するには全部のセグメントにIDSを設置する必要がある。
- ウイルス対策ソフトの場合と同様「アンチIDSモード」で動作する攻撃方法が開発されつつある。[2]

こうした状況を総合的に勘案すると，現段階においては，IDS導入の基本は，ホストベースとネットワークベースという二つの異なる技術を組み合わせて配置することにより，それぞれの得意とするところを生かして不正アクセス監視の精度を向上させることであるといえる。

5・3 IDSの実装例と運用

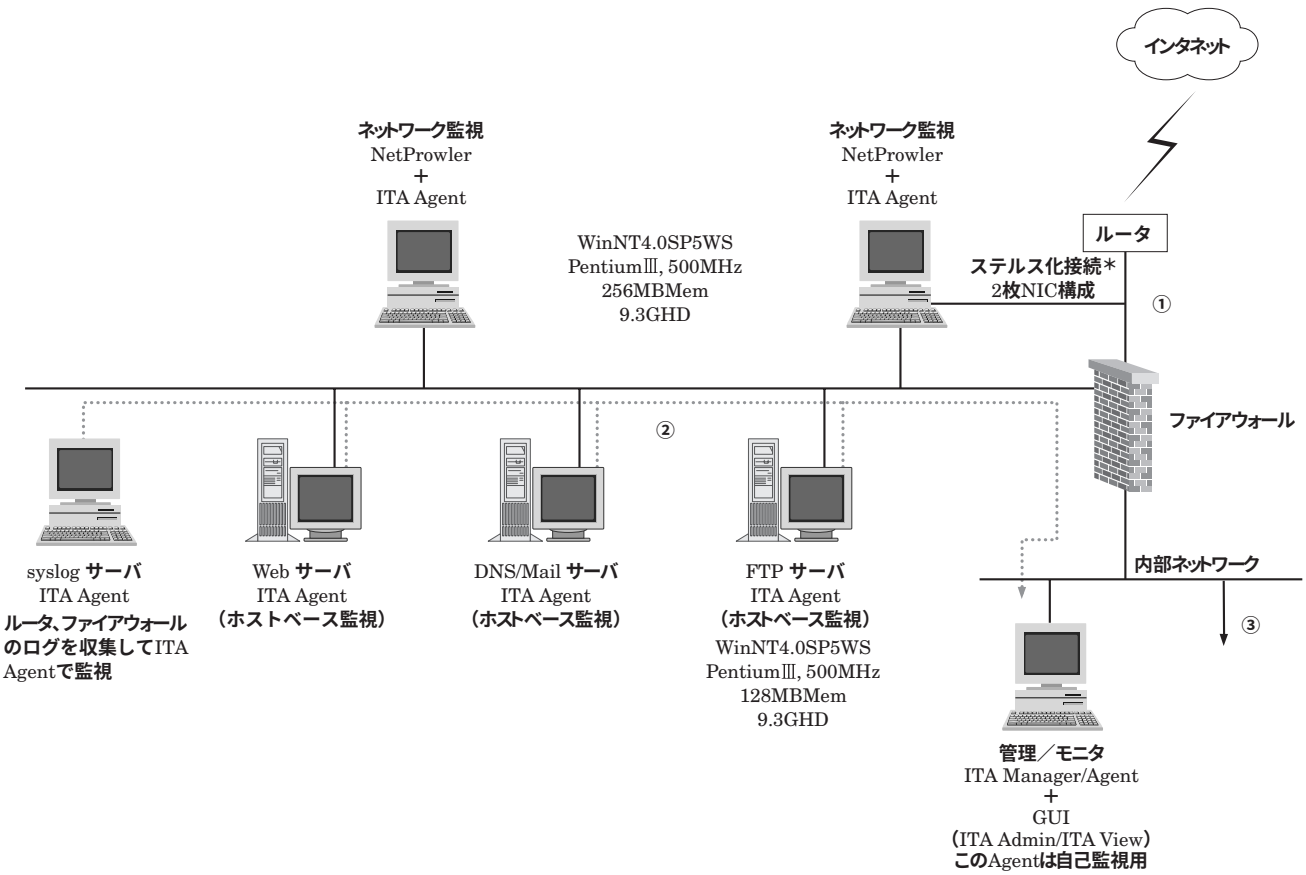
図6にAXENT社のIDSを使用したインタネット接続における実装例を示す。

① バリアセグメント

- ルータ直下のバリアセグメントはネットワークベースのNetProwlerをステルス化して監視する。監視結果はDMZ（Demilitarizied Zone）にIP接続し，ファイアウォール経由で内部ネットワーク上のITAマネージャに通知する。
- 同時にルータおよびファイアウォールのsyslogを②のDMZ上のsyslogサーバに転送してITAエージェントで監視する。

② DMZ

- インタネットに公開するサーバ群は通常DMZ上に設置し，ファイアウォール設定でインタネットからDMZ上のサーバへの接続のみを許可するようにし，また内部ネットワークへの直接接続は拒否するようにする。
- NetProwlerによりDMZ上のパケットを監視するとともに，ITAエージェントを各アプリケーションサーバに配置しログ監視およびファイル監視を行う。異常を検知するとファイアウォール経由で内部ネットワーク上のITAマネージャに通知する。



＊ステルス化接続：ネットワークに対して自機のIPが見えない形で接続すること（受信のみ行う）。

図6 インタネット接続におけるIDS導入例

③　内部ネットワーク

ITA ManagerおよびGUIは，「Trusted」な内部ネットワーク上に設置して収集したデータのモニタ・管理を行うようにする。

「イタチごっこ」と表現されるように，新たな攻撃方法が続々出現している現在，セキュリティを適切に確保できるかどうかは，機器やツール導入後の運用・管理にかかっていると言える。注意すべき点をいくつかあげる。

(1) ウィルスのデータファイルと同様，常にベンダから提供される攻撃シグネチャを更新し，新たな攻撃に対応できるようにする。

(2) DoS攻撃は高い確度でネットワークベースIDSで検出できるので，アラート情報（ソースIPアドレス）に従い，ルータ，ファイアウォールで一時的に遮断する。

(3) 単純DoS攻撃のようにいわば「わかりやすい」攻撃は検出も比較的容易であるが，現在のIDSは「False Positive」の考え方に基づいているため，IDSが出力するメッセージには許可されたユーザによる正常アクセスの記録も多数含まれる。このなかからアタッカが不正アクセスの準備段階でよく使用する手口を検出することができれば，ソースIP（たいてい，踏み台からやってくる）からの挙動に注目して，その後の対策が立てやすくなる（ポートスキャンのあとには多分アプリケーションのバグを突いたバッファオーバフロー攻撃などがやってくるはずだ…などなど）。

(4) ITAのファイル監視において，対象ファイルの書換えアラートには正規ユーザも含めて注意する。

(5) ESMにより，いつのまにか不正なプログラムがインストールされていないかどうかを，新たにrootにsetuid，setgidされたファイルの有無でチェックする。

6. あ と が き

「今後，インタネットでの新たなビジネス展開に対応したサービス（＝プロトコル）はますます増えてくるだろう。ここで，これらのサービスを自由に，かつ効率よく活用することを考えると，インタネットへの間口を広げておく必要がある。つまり一律にフィルタするファイアウォールに対し，ファイアウォールの門をある程度開く，もしくはファイアウォールの門を開放する必要が出てくる。このため，ファイアウォールは普段は門を開放し，不正アクセスを検出したら，直ちに門を閉めることができなければならない。

このときのセキュリティを確保するためには，さらに，

(1) ネットワークに侵入されてもサーバには侵入されないよう，サーバ自身のセキュリティも高め要塞化する。

(2) 精度の高い不正アクセス監視を実現するために，IDSの高度化，リアルタイム化が必要であり，その役割はますます重要になると予想する。」（日本ヒューレット・パッカード セキュリティ・ソリューション・センター長 佐藤慶浩氏）

近い将来，ネットワークセキュリティの実現イメージはこのようなものになるだろう。つまり，システムを防御するとともに，ネットワークを有効に活用するためには，サーバの要塞化およびIDSが不可欠になってくると考えられる。

さらには，IDSとセキュリティアセスメントのデータベースを有機的に統合した，総合的なセキュリティ管理システムが必要になると予想される。

参 考 文 献

(1) 日経オープンシステム，2000/3

(2) “ Insertion, Evasion, and Denial of Service : Eluding Network Intrusion Detection ” Thomas H.Ptacek, Timothy N.Newsham Secure Networks, Inc.

◆ 執筆者紹介

桂 川 昌 治
1982年入社。主として，ネットワーク/通信システムの技術業務に従事。現在，情報通信開発事業部技術部セキュリティシステム課長。

井 上 大 輔
1986年入社。主として，ネットワーク/通信システムの技術業務に従事。現在，情報通信開発事業部技術部セキュリティシステム課主任。