エレクトロニックコマース・セキュリティ特集

UDC［681.324：343.45］：343.98

侵入検知システム
Intrusion Detection System

武内春夫　Haruo Takeuchi
福士賢二　Kenji Fukushi

要　旨

ネットワークへの不正アクセスを検知する侵入検知システム（IDS）の概要と動向を解説した後，IDSの代表例としてEMERALDを紹介する。また，当社セキュリティビジネスにおける侵入検知システムの位置付けを述べる。

1．まえがき

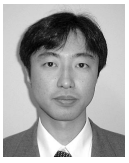
インターネットにおける不正アクセスが社会的な問題になっており，ファイアウォールだけではインターネットを通してやってくる不正アクセスに対抗しきれないことが一般的な認識になってきた。また，ネットワーク犯罪の大半は，イントラネットの利用者がそのイントラネット内部のターゲットに対して引き起こしている。このようなイントラネットの内外に起因する不正アクセスを監視するために，侵入検知システム（IDS；Intrusion Detection System）の必要性が高まっている。

米国FBI/CSIの調査[1]によれば，米国の組織の約50%以上がIDSを導入済みである。日本ではまだほとんど導入されていないが，IDSはファイアウォールと共にネットワークセキュリティの必須ツールになると思われる。

本稿では，IDSの概要と動向を述べた後，代表的なIDSの例としてEMERALD[2]を紹介する。

武内春夫

システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部



福士賢二

システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部　開発第四チーム

2．侵入検知システムとは何か

IDSとはネットワークやコンピュータに対する不正アクセスを検知して対応措置を講じるシステムであり，次のような機能を持つ。

- ネットワークやコンピュータを常時監視し，不正アクセスを検知する。
- 不正アクセスを検知した場合，次のような対応措置をとる。

－ファイアウォール設定情報の変更
－ 攻撃に使用されているTCPセッションの切断
－ 管理者への通知

図1にIDSの概念を示す。ここで侵入検知は以下のように行なわれる。

①ハッカーが，インターネットからファイアウォールを通って，イントラネット上のホスト／サーバマシンに侵入する。WWWサービスやメールサービスなどのセキュリティホールを利用することにより，ファイアウォールをすり抜けてくる侵入手段が知られている。

②IDSは，ネットワーク上のパケットやホスト上のログを監視し，既知の攻撃パターンやネットワーク／コンピュータの定常状態に関する情報（プロフィール）をもとに，侵入を検知する。

③侵入を検知したなら，侵入に対する対応措置をとる（この図では，ネットワーク管理者に警報を通知する）。

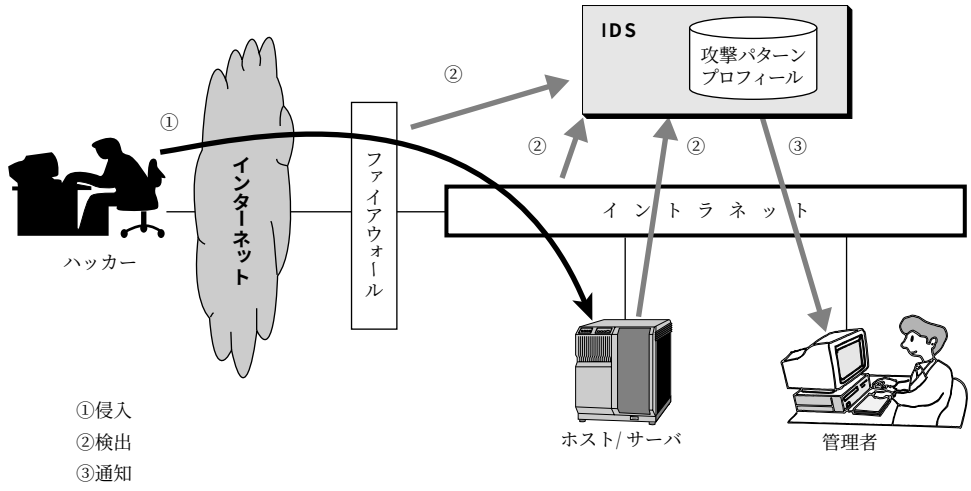


図1　侵入検知システムの概念図
Fig. 1　Concept of intrusion detection system

なお，IDSが持っている攻撃パターン／プロフィールのデータベースは，新種の攻撃に対応できるように，常に最新の状態に更新し続けることが重要である。

3．侵入監視形態

IDSは監視形態によって，ネットワーク監視型とホスト監視型に分けられる。

ネットワーク監視型のIDSはネットワーク上のIPパケットを監視して，次のような疑わしいアクセスの兆候を見つける。たとえば，不正なヘッダーを持つIPパケット，passwdなどの文字列を含むIPパケット，ポートスキャン，異常に多数の接続要求など。

図2に，ネットワーク監視形IDSの概念図を示す。

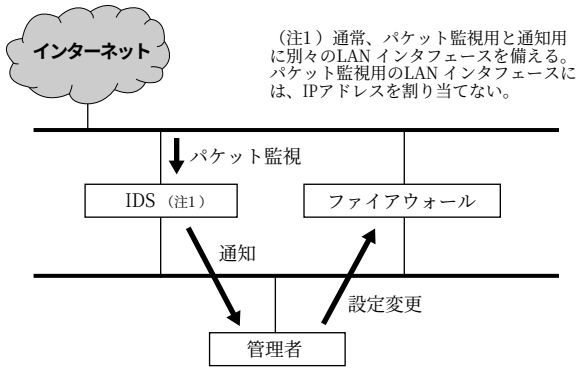


図2　ネットワーク監視形IDS
Fig. 2　Network-based IDS

IDSは，ファイアウォールの外側を流れるIPパケットを監視している。IDS自身に対する攻撃を防ぐために，IDSはファイアウォールの外側から見えなくされている（ステルスモード[1)]）。警報を受けた管理者（または管理プログラム）が対応措置をとる。たとえば，ファイアウォールの設定変更によって，外部からのアクセスを遮断する。

一方，ホスト監視型のIDSは監視対象ホスト，サーバマシン上でシステムログやアプリケーションログを監視し，次のような疑わしいアクセスを見つける。たとえば，多数のログイン失敗，重要なファイルへのアクセス／パスワードの変更，通常時間帯以外のログインなど。

図3に，ホスト監視形IDSの概念図を示す。この場

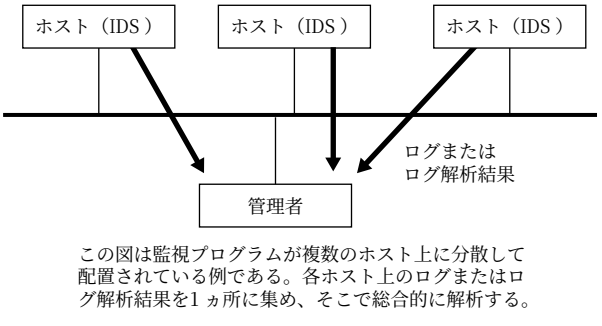


図3　ホスト監視形IDS
Fig. 3　Host-based IDS

合，IDSはイントラネット上の複数のホストに分散して配置され，ホスト上の活動を監視し，ログを管理者（または管理プログラム）に転送する。ホスト上である程度のログ解析を行ない，解析結果だけを管理者に転送するIDSはエージェント／マネージャ型のIDSと呼ばれる。

4．侵入検知技術

IDSは，検知する対象によって，不正アクセス検知型（misuse detection）と異常検知型（anomaly detection）に分類される。

不正アクセス検知型IDSは，既知の不正アクセスを検知する。

一方，異常検知型IDSは，ネットワークやホストに対するアクセスの異常を検知する。アクセス異常の原因は，既知の不正アクセス，未知の不正アクセス，ネットワークやホストの故障などである。

不正アクセス検知型IDSの一般的な侵入検知技術はシグネチャ解析である。アクセスパターンの特徴を示すものをシグネチャと呼ぶ。シグネチャは，数値，文字列，ルールなどの形態をとる。既知の攻撃パターンのシグネチャを前もってデータベースに蓄積しておき，現時点のアクセスパターンのシグネチャと合致するシグネチャがデータベースの中で見つかれば，“攻撃あり”と認識する。エキスパートシステムのルールをシグネチャとして使用する例として，図４に一般的バッファオーバーフロー攻撃検知用のルールを示す。このルールは異常に長いパラメータを持つEXECコマンドの実行を監視しており，それを検知した時点でALERTメッセージを発する。

```
一般的バッファオーバーフロー攻撃検知用のルール
1  rule[BSM_LONG_SUID_EXEC(*):
2  [+e:bsm_event]
3  [? | e.header_event_type == ‘AUE_EXEC ||
4  e.header_event_type == ‘AUE_EXECVE]
5  [? | e.subject_euid!= e.subject_ruid]
6  [? | contains (e.exec_args, "^＼＼") == 1]
7  [? | e.header_size>‘NORMAL_LENGTH]
8  ==>
9  [! | printf("ALERT: Buffer overrun attack ＼
10 on command %s＼n", e.header_command)]
11 ]
```

図４　一般的バッファオーバーフロー攻撃用ルール
Fig. 4　Rule for general overflow attacks

異常検知型IDSの侵入検知技術の中に，統計的異常解析と呼ばれる手法がある。これは，パケット数，パケット長，パケットタイプ，パケット受信間隔などに関する累積値や平均値などの統計情報を利用して，ネットワークやコンピュータに対するアクセスの定常状態からかけ離れたアクセスパターンを検知することにより，異常を検知する方法である。この手法は既知および未知の攻撃パターンを検知できる。

図５は統計的異常解析の概念を示す。ネットワークやコンピュータに対するアクセスの定常状態を示す統計情報（長期プロフィール）を監視開始前の訓練期間中に蓄積しておく。監視開始後，ネットワークやコンピュータに対する現時点のアクセス状態を示す短期的な統計情報（短期プロフィール）を観測する。短期プロフィールを長期プロフィールと比較し，両者の差がしきい値を超えていれば，異常ありと判断する。なお，短期プロ

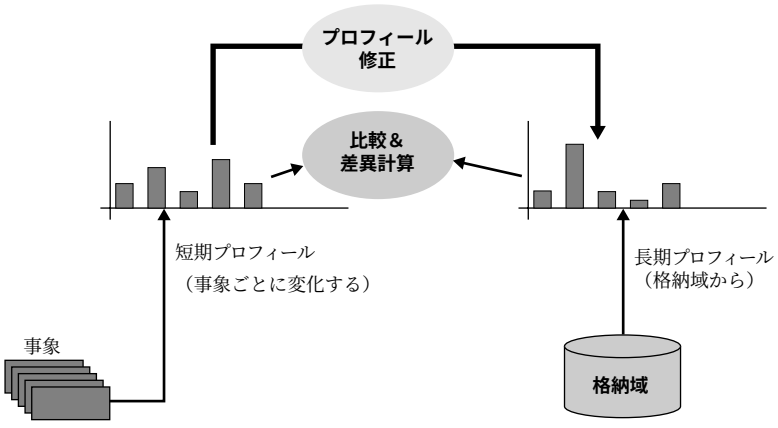


図５　統計的異常解析の概念図
Fig. 5　Concept of statistical anomaly analysis

フィールは，逐次，長期プロフィールに織り込まれ，長期プロフィールは常に最近の一定期間の傾向を反映するように修正される。

5．侵入検知システムの例

IDSは米国を中心に研究開発されており，製品と研究システムを含めると80以上のシステムが存在する。製品としてはISS社のRealSecure[3)*1)]がトップシェアを誇っている。また，研究開発中のシステムとしてはSRI International社のEMERALDが著名である。SRI International社は1983年からIDSを研究しており，その実績をもとに作られているEMERALDはネットワーク監視型，ホスト監視型，不正アクセス検知型，異常検知型のすべての特長を備えている。特に，その未知攻撃検知能力は市販製品に例がなく，また既知不正アクセス検知能力は市販製品をはるかに凌駕しており，次世代のIDS製品として期待される。

EMERALDは次のような特長を備える。

1） 既知攻撃と未知攻撃を検知；シグネチャ解析による既知攻撃の検知，および統計的解析による未知攻撃の検知機能を持つ
2） 階層的解析スキーム；複数の解析ユニットをネットワーク上に分散配置し，階層的に解析可能
3） 協調したグローバルな攻撃に対応可能
4） インタオペラビリティ；IDS間，IDSとアプリケーション間の標準インタフェースであるCIDF(Common Intrusion Detection Framework)をサポートする

図６にEMERALDの概念図を示す。EMERALDは

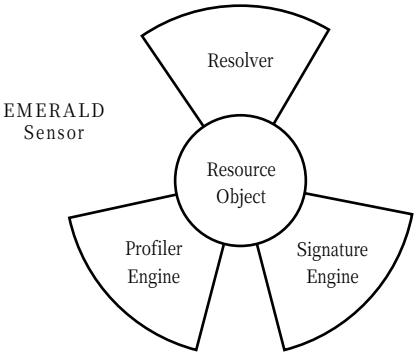


図６　EMERALDの概念図
Fig. 6　Concept of EMERALD

Sensorを単位としてネットワークやコンピュータ内に配置され，複数のSensorが連携して分散階層型のIDSを構成する。Sensorは４モジュールで構成されている。Signature EngineとProfiler Engineは，それぞれ不正アクセスと異常を検知し，Resolverに通知する。Resolverは，警報通知などの対応措置をとる。Resource Objectは侵入検知対象のネットワークやコンピュータに関する設定情報である。

6．あ　と　が　き

IDSの概要と動向を述べ，代表的なIDSの例としてEMERALDを紹介した。理想的な侵入検知システムの要件は，

1） 未知の攻撃を検知できること。
2） リアルタイムに検知と対応を行なうこと。
3） 誤った警報を発しない(false positiveがない)。
4） 侵入を見逃さない(false negativeがない)。

などであり，その理想に近づくために，AI手法，ニューラルネット，遺伝子アルゴリズム，統計的手法などを使用した研究開発の試みが行なわれている。

インターネットの重要性が高まるとともにネットワークセキュリティの重要性が高まっており，IDSに対する期待は大きい。当社は今後，プロダクトとサービスの両面からIDSビジネスを立ち上げていく予定である。

- セキュリティプロダクト；大規模広域分散ネットワークに対応できるIDSとして，SRI International社のEMERALDを導入し商品化する。
- セキュリティサービス；不正アクセス監視代行サービスをサービスウェアとして立ち上げる。

7．参　考　文　献

1） CSI, "Computer Security ISSUES & TRENDS", spring 2000.
2） EMERALD, http://www.sdl.sri.com/emerald/
3） RealSecure, http://www.isskk.co.jp/
4） IDS一覧, http://www-nks.informatik.tucottbus.de/~sobirey/ids.html
5） Stephen Northcutt, "Network Intrusion Detection",New Riders., 1999

＊1）RealSecureはISS社の商標。