■3 群（コンピュータネットワーク）－ 7 編（コンピュータネットワークセキュリティ）

5 章 侵入検知システム

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

■概要■

IDS（Intrusion Detection System: 侵入検知システム）は，情報システムに対する不正行為や情報システムの異常を検出し，ファイルやデータベースなどに記録する，管理者へ通知するなどの機能をもつ情報システムである [1].

電子商取引など業務処理に用いられるサーバやメールサーバ，Web サーバだけでなく，普段の作業に用いるパーソナルコンピュータなど，すべての情報システムにとって，不正行為や異常などにより発生する情報セキュリティ事故は，それらが扱う様々な情報の損失や漏えいを引き起こすだけでなく，情報の破損や原因の調査，復旧のために運用停止を招き，それらに依存する業務の多くに支障をきたす．このように情報システムに依存する組織にとって不正行為や異常などにより発生する不正アクセス事故は，業務の継続性にも影響を与えかねない深刻な脅威であり，IDS はこれらを速やかに発見，防御することを可能にする機能をもった情報システムの一つである．

IDS と同じセキュリティ機能としてファイアウォール（FW: FireWall）がある．ファイアウォールは，運用ポリシーに基づいた通信制御が主な目的であり，運用側が意図するように情報システムへアクセスさせるための機能である．対する IDS は情報システムに対するセキュリティ上の脅威を積極的に検知しようとするものである．IDS に代わって開発された IDPS は通信制御を行うが，あくまで不正行為や異常を対象としており，運用ポリシーの施行などを主たる目的に置いていないところは，ファイアウォールと使用目的が異なる．

■3 群 － 7 編 － 5 章

5-1 IDS の種類

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

IDS には監視する対象によりホスト型侵入検知システム（HIDS）とネットワーク型侵入検知システム（NIDS），動作原理によって不正検出型（Misuse）や異常検出型（Anomaly）に分類することができる．

5-1-1 HIDS と NIDS

監視対象のコンピュータ上で動作する形態の IDS を HIDS（Host-based Intrusion Detection System: ホスト型侵入検知システム）と呼ぶ. HIDS は, 監視対象のコンピュータ上で動作し，コンピュータが出力するログや，システム情報を元に不正アクセスなどを検出する．例えばシステムファイルなどに加えられた変更，カーネル，メモリや I/O 上の禁止領域へのアクセス等を監視する．

実装例では, オープンソースの OSSEC（http://www.ossec.net/）, Osiris（http://osiris.shmoo.com/）のほか，米 Tripwire 社の Tripwire などの商用 IDS も存在する．HIDS の多くはシステムファイルなどの書換えや，システムリソースなどに対する不正なアクセス，コンピュータが扱うデータ，ログに記録されるイベントなどを監視することで不正アクセスなどを検出する．またアンチウイルスソフトウェアやパーソナルファイアウォールなども HIDS に分類することができるだろう．

HIDS に対し, ネットワークを流れる通信を監視する形態の IDS を NIDS（Network Intrusion Detection System: ネットワーク型侵入検知システム）と呼ぶ．電気的，光学的にネットワークケーブル上を流れる通信データを分岐するネットワークタップ（Network TAP）と呼ばれる装置や，ネットワーク機器内で通信を複製するポートミラーリングなどの機能を用いて通信データを IDS に導き，通信の内容や傾向を監視することで不正アクセスなどを検出する．

実装例ではオープンソースの Snort（http://www.snort.org/）や Bro（http://www.bro-ids.org/）のほか，IBM-ISS 社の RealSecure，米 Enterasys 社の Dragon などの商用 IDS が存在する．

5-1-2 不正検出型と異常検出型

不正行為や異常状態の特徴情報をあらかじめ定義しておき，同じものを発見しようとするタイプを不正検出型と呼ぶ．例えば，不正アクセス時に発生するパケットパターンを特徴情報として，ネットワークを流れるパケット一つひとつと比較を行い，一致した通信を不正アクセスとして処理する．このような手法による IDS をシグネチャ型とも呼ぶ.

これに対し異常検知型では，何らかの方法で正常な状態を定義し，これに当てはまらない状態の発生を検出する．例えば午前 9 時から午後 5 時を勤務時間とする会社で，深夜の午前 1 時に社内ネットワーク上の業務用 DB へ何者かがアクセスしていたなら，たいていの管理者は異常を察知するだろう. 一部の異常検知型 IDS では, このような手法を用いているほか，通信プロトコルの異常を監視する，通信量などの変化を監視する手法などが存在する．

5-1-3 IDPS

通信を遮断する機能をもった IDS を IDPS（Intrusion Detection and Prevention System: 侵入検知防御システム）と呼ぶ．不正行為や異常が検知された場合に TCP の RST 信号を送り返すなどにより，TCP セッションを切断する機能などをもつ IDS も存在するが，IDPS はファイアウォール装置のように, 物理的, 論理的にネットワークの経路上に配置することにより，より積極的に通信の制御を行う．これにより DoS（通信妨害攻撃手法）や，各種スキャン行為などが発生した際に通信元の IP アドレスレンジを一定時間フィルタするなど, より細かく通信を遮断することが可能となる．

IDPS とファイアウォール装置との違いは，ファイアウォール装置がレイヤ 3～4 での通信制御であるのに比べ, IDPS ではパケットに含まれるアプリケーションデータなどレイヤ 5(アプリケーション層）以上の情報を検査して通信を制御できる点である．ただしファイアウォール装置の中にも DoS やスキャンの検知，防御機能をもつものが存在しており，両者の違いが徐々に少なくなっている．

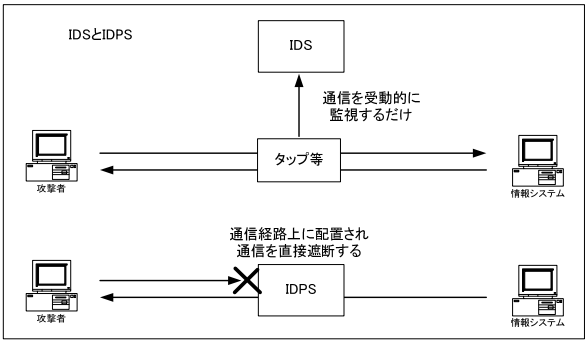

図 5・1　IDS と IDPS

5-1-4 そのほかの IDS

近年研究, 開発が進みつつある IDS として PIDS（Protocol-based Intrusion Detection System），APIDS（Application Protocol-based Intrusion Detection System）などが存在する．PIDS は HTTPD に対するリクエストだけを監視するなど，より高いレイヤのプロトコルに特化した不正行為や異常の監視を行う．APIDS ではアプリケーションやシステム間での通信を PIDS と同様に監視する．例えばバックエンドシステムの SQL サーバ上で動作し，フロントエンドシステムの Web サーバ上で動作する PHP などから送られる SQL リクエストを監視するなどである．

PFW（Personal Fire Wall: パーソナルファイアウォール）は WindowsXP/Vista や 2003 サーバなどに付属するセキュリティセンターやアンチウイルスソフトウェアのメーカーが提供するセキュリティソフトウェアのように，IDS 機能やファイアウォール機能をエンドノードにも実装させ，情報システム全体をよりセキュアにしようとするもので，先に紹介した HIDS に分類することができる．先のセキュリティセンターのようにオペレーティングシステムに実装され，またアンチウイルスソフトウェアをベースとした総合セキュリティソフトウェアとして提供されているため，今後広く普及するものと予想する．

以上のように様々な IDS が存在するが，単に IDS と記載した場合，暗黙にネットワーク型の IDS を指す場合が多い. また本章の執筆時点では商用 NIDS の多くが, 防御機能をもつ IDSP に変化しつつある．本章では NIDS，IDPS も含めたものとして，IDS の単語を用いて解説する．

■3 群 － 7 編 － 5 章

5-2 IDS の歴史

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

侵入検知のコンセプトは古く，J.P. Anderson により 1980 年に発表された“Computer Security Threat Monitoring and Surveillance”の中に見ることができる．Anderson はコンピュータの監査情報を分析するための自動化ツールなどを提案し，この中でユーザの振る舞いを統計的に分析することで，なりすましなどを発見できるだろうと述べている [2)]．

その後様々な侵入検知手法が研究，開発される．1983 年には Stanford 大学でユーザの振る舞いを統計的に分析し，普段と異なる異常行動を検出するモデルの侵入検知手法をコンピュータにより処理させる，IDES（Intrusion Detection Expert System）の研究発表がされている [3)]．

1990 年には L.T. Heberlein らによって最初の NIDS が提案された．この NIDS は今日主流となるシグネチャ型に代表される不正検出型ではなく異常検出型であった [4)]．

1992 年には先の J.P. Anderson によりシステムファイルの改変を監視することで異常検知を行うホスト型 IDS である Tripwire が開発される．

そして 1994 年に最初の商用ネットワーク型 IDS である RealSecure が米 Internet Security Systems 社（後に IBM に買収され IBM Internet Security System 社に名称変更）から，続く 1995 年に NetRanger が米 WheelGroup 社（後に CISCO に買収され Cisco Secure IDS に名称変更）より発表される．これらの商用 IDS はシグネチャ型の NIDS であった [5)]．

1990 年代後半からは，様々な IDS が研究，開発され，数多くの商用製品が市場に提供された．2000 年を過ぎてからは不正行為を自動的に防御する機能を組み入れた IDPS や，ハードウェア化による高速 NIDS/IDPS，ファイアウォール，スパムフィルタ，アンチウイルスゲートウェイなどの機能と統合した UTM（Unified Threat Management）などに進化している．また IDS などが出力するメッセージの共通フォーマットが IETF において検討されている [6)]．

■3 群 － 7 編 － 5 章

5-3 IDS の構造

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

IDS の構造について，オープンソースで入手可能なシグネチャ型の NIDS である Snort を例にして解説する．

Snort はパケットキャプチャ部，プリプロセッサ部，検知エンジン部，アウトプットプロセッサ部の四つの主なモジュールにより構成されている．**図 5･2** にその構成を示す．

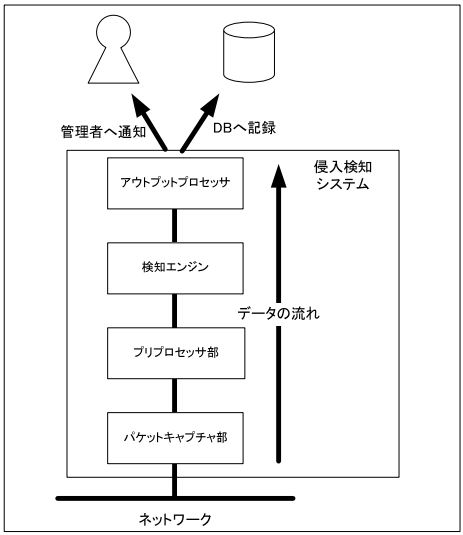

図 5・2　IDS の構造

5-3-1 パケットキャプチャ部

NIDS では，ネットワーク上を流れるパケットを獲得し調査しなければならない．たいていの NIDS は，パケットキャプチャエンジン部によりネットワーク上を流れるパケットデータを取り込み，上位層に渡す．Snort であればこの部分は*BSD 系の BPF，Linux や Windows の PCAP ライブラリなどが行う．

大量のトラフィックが流れたなどの場合，パケットキャプチャ部の性能不足により，通信の取りこぼしを発生させることがある．そのためバッファの大きな専用のネットワークインタフェース（NIC）を用いて，大トラフィックに対応するなどの手法が存在する．一時期の商用 NIDS にはこの手法が多く見られた．

5-3-2 プリプロセッサ部

パケットキャプチャ部で取り込んだパケットを，検知エンジン部に渡す前に様々な加工を行う処理部である．たとえば，フラグメント化されたパケットや，ストリーム通信を組み立

てて検知エンジン部が認識できる形式に加工する，SMTP や HTTP の通信など，様々な種類のエンコードデータを正規化する，通信プロトコルの実装が正しいか調査するなどである．旧い設計の NIDS では，これらの機能をもたなかったために，NIDS の回避（Evation 攻撃）が可能であった．例えばフラグメントに対応できない NIDS において，“ABCDE”の文字列が含まれたパケットは検知できるが，二つのフラグメントパケットとして，1 個目のパケットには“ABC”，2 個目のパケットに“DE”の文字列をもったパケットは，受信するコンピュータでフラグメントパケットの再構築を行うことにより“ABCDE”の文字列として処理されるが，フラグメントパケットの再構築機能をもたない NIDS では検知できないといった現象が発生する．

5-3-3 検知エンジン

検知エンジン部はプリプロセッサ部やパケットキャプチャ部から受け取ったパケットを，シグネチャ型の NIDS であれば，あらかじめ与えられている不正アクセスなどの特徴情報と比較を行う．もし両者がマッチした場合は，あらかじめ与えられた手順に従ってアウトプットプロセッサに渡すなどの処理を行う．

これら不正アクセスなどの特徴情報をシグネチャと呼び，シグネチャを IDS が理解できる書式で記述した情報をルールと呼ぶ．**図 5･2** に Snort のルールの例を示す．

```
alert tcp any any -> any any (msg:"ALERT 00"; content:"MESSAGE";)
```

図 5・2　ルールの構造

このルールはプリミティブな Snort ルールの例である．この例で先頭部分の alert をルールアクションと呼ぶ．ルールアクションでは，ルールに記述されたシグネチャにマッチした場合，どのような動作を行うべきか Snort に指示する．ルールアクション以降はシグネチャである．順にプロトコル，通信元 IP アドレス，ポート番号，通信の方向，通信先 IP アドレス，ポート番号が記述される．any はワイルドカードを示し，すべての条件にマッチする．続く( )で囲まれた部位をルールオプションと呼び，更に詳しい特徴情報や，ルールに関する付帯情報等が記述される．この例では，msg:によってこのルールにマッチした場合に出力するメッセージを定義し，content:によってパケットに含まれるべきデータを記述する．このルールの例では tcp のパケットに"MESSAGE"の文字列が含まれていた場合にアラートとして扱うよう Snort に指示している．Snort ルールの詳細については，Snort ユーザマニュアルを参照すること．

5-3-4 アウトプットプロセッサ部

検知エンジン部によってシグネチャにマッチしたパケットは，アラートとして管理者に通知したり，ファイルやデータベースなどに記録したりするため，アウトプットプロセッサ部に渡される．アウトプットプロセッサ部は，例えば検知エンジン部でアラートとして扱うべきルールのシグネチャにマッチした場合に，IP アドレスやイベントの種類，パケットに含まれるデータなどの様々な情報をテキストデータとしてログファイルに書き出したり，データベースに格納できる形式に変換してデータベースの API に渡したりする．

5-3-5 アラートマネージャ

IDS に含まれる機能ではないが，IDS を用いて実際に不正アクセス監視を行うために，アラートマネージャは必須ともいえる重要な要素である．IDS によって検出されたアラートなどは，アウトプットプロセッサ部によってファイルやデータベースなどに記録される．しかしそのままでは，人が読めるような形式ではないか，読めたとしても冗長で，どのような脅威が存在するのか知るための情報として扱いづらい．このために情報を分析，集計し，管理者に通知する，レポートを作成する，分析結果をビジュアライズするなどの処理を行い，管理者を手助けする役割をもつのがアラートマネージャである．

■3 群 － 7 編 － 5 章

5-4 IDS に関する問題

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

侵入検知の技術は未完成であり，様々な問題を抱えている．その一部を以下に記す．

IDPS も含む IDS における大きな問題の一つに，フォールスポジティブ（False Positive）とフォールスネガティブ（False Negative）がある．フォールスポジティブは正常な通信や振る舞いを IDS が異常として検出する現象で「誤検知」とも呼ばれ，IDS の機能や処理能力の不足，シグネチャの完成度不足などが主な原因である．フォールスネガティブは IDS が検出しなければならないはずの通信や振る舞いを見逃してしまうもので，シグネチャの不備，機能や処理能力の不足など，様々な原因により発生する．IDS の処理能力については，専用 LSI などによる侵入検知システムのハードウェア化などで対応しつつあるが，例えば暗号化通信の復号のように，IDS では対応しきれない問題も多い．

今日ネットワーク技術が進歩し，10Gbps を越える広帯域ネットワークがあたりまえのようになっている．ネットワークの広帯域化に従い IDS に対する性能要求は厳しくなりつつある．特にネットワーク機器の一部として通信を制御する IDPS に対しては，ネットワーク機器並の性能，信頼性が求められる．しかしながら IDS は，その目的上すべての通信を取り込み，パケットを再構築して情報を復元し，不正アクセスなどの特徴をもたないか入念に検査するなどの処理を行わなければならず，レイヤ 2，3 層の情報だけで処理を行うほかのネットワーク機器と比べて高い処理能力が要求されるため，スイッチやルータなどと同様の性能を出すことは難しい．これはファイアウォール装置とも共通する問題点である．ハードウェア化による高性能化なども進んでいるが，スイッチやルータなどの性能に追いつくことは難しい．また高い性能をもつ IDS は非常に高価であり，以降で紹介するコスト対効果の側面とあいまって IDS に対する投資効果の非効率さが問題視されることがある．

運用上の問題として，IDS は不正アクセスなどを予測し，完全に予防できるものではないことがあげられる．IDS は不正アクセスや異常状態の検出及び記録，通知を目的としており，それらを防ぐことはできない．これを補うために IDPS では通信の遮断機能を与えられたが，先に述べたフォールスポジティブ，フォールスネガティブのように検知精度が不十分なため，運用者の期待どおりに動作するとは限らない．また IDS を有効に活用するには検知精度の不十分さを補うため，専門分析員による二次解析が必要である．このため自前で分析員を組織するか，監視センターなどの専門業者に監視業務を委託するなどが必要となり，運用コストの増大につながる．また IDS の運用においては，情報システムが正常に動作し，脅威などが存在しないかぎり，運用者に対するフィードバックはなく，IDS に対する投資効果が見えづらい．このような要因によるものなのか，米国に比べて日本国内では IDS の導入が進んでいない [7]．

IDS の運用において最も深刻なのは，利用者のプライバシー保護である．多くの運用者はユーザの通信内容に介入しないよう注意しているだろう．また電気通信事業法において通信の検閲が制限されている場合もある．しかし IDS の運用は，運用者などが意識していなくともこれらの問題に抵触していると考えられる．この点については十分に議論されているとはいえず，グレーな状態で運用が続いている．

■3 群 － 7 編 － 5 章

5-5 まとめ

（執筆者：渡辺勝弘・鶴岡信彦）［2009 年 7 月 受領］

これまで解説したように，現在の形態の IDS/IDPS を取り巻く環境は徐々に厳しくなっており，また有効性が疑問視されている．これらを補うかたちで今後はパーソナルファイアウォールなどのエンドノードセキュリティ対策に見られるホストベース型が普及し，更に異常を検出する機能をもったネットワークスイッチやルータなどのネットワーク機器が登場するであろう．また，これまで IDS が適用されていなかった分野やアドホックな形態のネットワークシステムなどの新たな分野への適用するため，PIDS や APIDS のようにより高いレイヤでの侵入検知や，行動ベースによるアノマリ型の普及，NIDS，HIDS やファイアウォール装置の統合監視など，様々な侵入検知手法へ分化していくものと思われる．

■参考文献

1) FAQ: Network Intrusion Detection Systems
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html
2) Computer Security Technology Plannning Study James P. Anderson October 1972
http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf
3) History of IDS at SRI.
http://www.sdl.sri.com/programs/intrusion/history.html
4) Heberlein, L.T., Dias, G.V., Levitt, K.N., Mukherjee, B., Wood, J. ,and Wolber, D., “A network security monitor” Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society
5) Intrusion Detection Overview of the Technology Jamie French
http://www.whitehats.ca/downloads/malik/malik_ids_overview.pdf
6) The Intrusion Detection Message Exchange Format (IDMEF)
http://tools.ietf.org/html/rfc4765
7) 内田勝也，“第３回情報セキュリティ調査結果 情報セキュリティ調査からみた日米情報セキュリティ比較，”情報セキュリティ大学院大学，2005．http://www.uchidak.com/chuo/2006_Japan_CSI.pdf