侵入検出システムIDA: そのシステムデザイン

10－2

浅香 緑[†*]　情報処理振興事業協会 技術センター
掛本 喜嗣[‡]　日本総合研究所

1　はじめに

インターネットの拡大にともない、侵入事件も増加している。侵入を防ぐには、認証やアクセス制御の技術が不可欠であるが、これだけでは十分ではない。侵入を検出するために管理者はシステムログを解析するが、ログの量は膨大であり、多大な作業時間を必要とする。この問題を解決するために、自動的に侵入を検出する侵入検出システム（ IDS: Intrusion Detection System ）が、考案されている。

IDS は、米国を中心にいくつか研究例があるが、実用レベルに達しているとはいい難い[1]。また、米国のみで使用を認めているシステムが多く、これらを我国で利用することは困難である。

情報処理振興事業協会（IPA）では、広く公開でき、侵入に知識のない管理者にも使いやすいネットワーク上の侵入検出システムIDA （ Intrusion Detection Agent system ）の開発中である。本プロジェクトでは、設計をほぼ終え、実装の段階にはいっている。

2　IDA の特徴

従来からの侵入検出に用いられる手法には、

- Anomaly detection
- Misuse detection

がある。

anomaly detection は、ユーザの通常から外れた行動を検出することによって侵入を発見する。主に統計的解析を用いて検出する。この手法の問題点は、内部者の侵入は検出しにくいこと、システムが大きく、重くなる傾向があることである。

misuse detection は、過去の侵入パターンをルールベースに持つエキスパートシステムを用いて、侵入を検出する。この手法の問題点は、新しい侵入方法は検出できないことである。

IDA ではこれらの侵入検出の手法は用いない。IDA では、管理者が侵入を疑った時にそれを確認するためにとる行為をモデル化して、侵入を検出する。IDA は階層的なマルチエージェントシステムで、各エージェントは、管理者の行為を代行する。IDA は、ネットワーク上でより効率的に侵入検出をすることを目標にしている。

3　IDA の構成

IDA は2種類の階層的なエージェントから構成されている。一つは管理者が侵入検出する際に行なう、情報収集に対応しているエージェントである。これを情報収集エージェントという。情報収集エージェントは移動型エージェントである。情報収集エージェントは、自分の移動先に関する知識を持つ。もう一方のエージェントは、集められた情報から、侵入されているか解析するエージェントである。これを侵入検出マネージャエージェントという。侵入検出マネージャエージェントは、侵入検出のための知識を持つ。また情報収集エージェントにタスクを割り当てる。この他、情報収集エージェントの発行・廃棄といった管理も行なう。このようにIDA は、階層的なエージェントシステムである。

侵入検出マネージャエージェントは、ローカルエリアネットワーク上のサブネットに1個存在する。情報収集エージェントは、ローカルエリアネットワーク上のサブネットに複数存在する（図1）。

IDA を設計するに当たって我々は、システム管理者が侵入を検出する際に、どのような情報を収集

The Design of IDA: An Intrusion Detection Agent System

[†]Midori Asaka, Information-technology Promotion Agency, Japan
[‡]Yoshitugu Kakemoto, The Japan Research Institute
*情報数理研究所より出向中

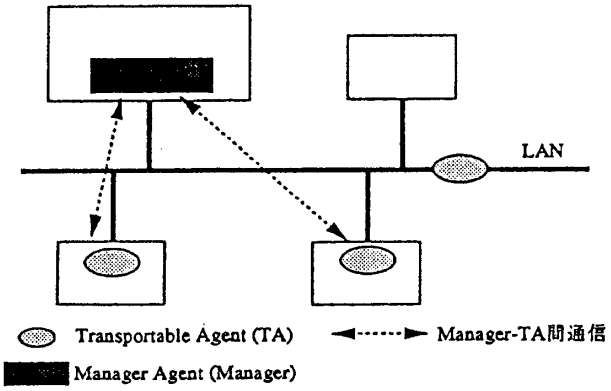

図 1: IDA の概要図

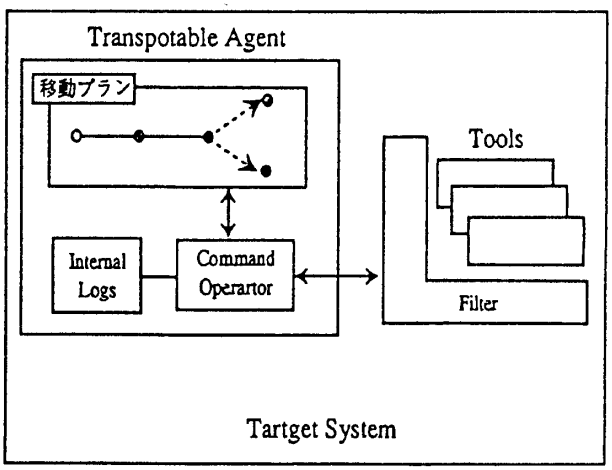

図 2: 情報収集エージェントの概念図

するかを、大きく以下のように分類した。

1. ファイルインテグリティ
2. プロセスやリソースの状態
3. ネットワークの状態
4. ユーザのログイン時間、サイト等
5. 侵入の追跡

情報収集エージェントは、上記のリストに対応した5種類の情報を収集する移動型エージェントから構成される。一種類のエージェントは、一種類の情報しか集めない。たとえば、ある情報収集エージェントは、ファイルインテグリティのチェックしか行なわない。一種類のエージェントが複数存在することも可能である。

ターゲットシステムから回収された情報に基づき、情報収集エージェントは自分の移動先を決定する。最終的に情報収集エージェントは、これらの結果を侵入検出マネージャエージェントに報告する。個々の情報収集エージェントは、侵入がおきているかどうかの判断はしない。侵入がおきているかどうかの判断は侵入検出マネージャエージェントが行なう。個々の情報収集エージェントは独立に動作し、いくつかの情報収集エージェントに同じタスクを同時に割り当てることが可能である。これによりIDAは、侵入検出に必要なタスクをを並列に処理する（図2）。

IDAでは各ターゲットシステム上にセンサが設置されている。センサは各情報収集エージェントが起動されるための事象をセンシングしている。そしてそれらの事象がセンサで検知されたとき、各情報収集エージェントは起動される。起動された情報収集エージェントは、それぞれ割り当てられた情報を収集し、マネージャエージェントに報告する。収集された情報から、マネージャエージェントは侵入されているかどうか判断する。

4 今後の課題

今後解決しなければならない問題として、

- IDAの侵入検出システムのモデルとしての妥当性の検証
- 侵入を判断のための協調、および効果的な知識ベースの構築
- エージェントのセキュリティ

がある。現在、本プロジェクトでは情報収集エージェントを実装中である。

参考文献

[1] Telesa F.Lunt: A Survey of Intrusion Detection Techniques, Computer and Security, 12 (1993)