ネットワーク上の侵入検出システムについての提案

5G－4

浅香 緑†[1]　掛本 喜嗣‡

†情報処理振興事業協会(IPA)技術センター　‡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、接続されるサイトは増加している。この結果、コンピュータシステムへのネットワークからの侵入は、増加する傾向にある。しかし、各サイトのセキュリティ管理者、ネットワーク管理者が必ずしも侵入に関する豊富な知識を持っているとは限らない。

多くの場合侵入は、ログを管理者が解析することによって検出される。このためには、管理者は侵入の事例についての知識を持っていることが必要である。その上、ログは膨大な量となるため、人手による解析は難しい。これらを考え合わせると、解析の自動化は必要である。

侵入検出システム（IDS:Intrusion Detection System）は、欧米では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。また、米国のみで使用を認めているシステムが多く、これらを日本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侵入検出システムの開発を目標に、プロジェクトを発足させた。本プロジェクトは昨年度末からはじまり、調査をほぼ終え、設計の段階にはいっている。

2　従来の侵入検出システム

侵入検出のための主な手法に、

- 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。anomaly detection では、統計的解析などの手法が用いられる。

misuse detection の多くは、過去の侵入のシナリオをルールベースに持つエキスパートシステムによって検出する。これ以外に、モデルベース推論、状態遷移を用いたものもある[1]。

侵入検出システムの代表的なものにSRIのIDES (Intrusion Detection Expert System) [2] がある。IDES は、侵入のシナリオやシステムの弱点をコード化したルールベースと、ユーザの行動パターンを蓄積したプロファイルにより、侵入を検出する。

3　本システムの目的

侵入検出システムは、その目的によりデザインが異なる。まず目的として、

- ホストマシンのみ侵入検出する
- ドメイン全体の侵入検出をする

が、考えられる。また侵入にも、

1. システムに関する高度な知識を有するアタッカーによる侵入
2. 良く知られたシステムの弱点や、セキュリティホールをついてくる侵入

がある。侵入の多くは 2のケースである[3]。また、1のタイプの侵入に備えることと、システムのパフォーマンスはトレードオフの関係にある。

以上より、本システムは目的として以下を掲げる。

1. ドメイン内全てのシステムの、侵入を検出する。この時、ドメイン内のシステム数の増加にも、対応できるようにする。
2. 踏台アタック[1]の検出を行なう。
3. 良く知られたシステムの弱点や、セキュリティホールをついてくる侵入に対処する。

A Study of the Network Inrusion Detection System
†Midori Asaka,Information-technology Promotion Agency,Japan
‡Yoshitugu Kakemoto,The Japan Research Institute

[1](株)情報数理研究所より出向中

[1]次々に他のシステムに侵入してから、最終的に目的のシステムに侵入する方法。この方法をとると、どこから侵入されたか突き止めるのが困難になる。

本システムの他システムとの一番の相違点は、踏台アタックを検出することにある。また本システムは、misuse detection タイプの侵入検出システムである。

4 本システムの構成

従来の侵入検出システムで、そのターゲットとするシステムと同一のマシン上で稼働するシステムは少ない（図1）。

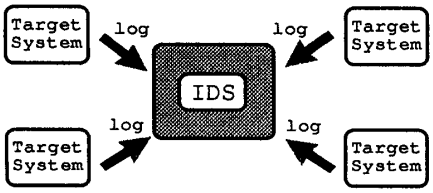

図 1: 一般的な侵入検出システム

特定の侵入検出サーバに、全てのターゲットからログを送りつけると、ターゲットの数が増えた時に、目的1 を達成するのが困難になる。また踏台アタックの検出は、特定の侵入検出サーバで行なうよりも、各ターゲットで検出する方が、容易である。このため本システムでは、各ターゲット上に侵入検出システムを分散させることにした（図2）。

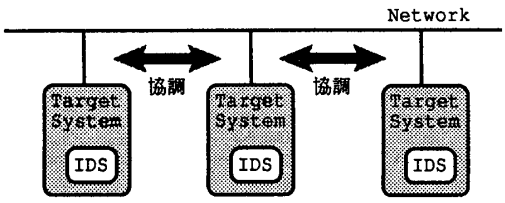

図 2: 本プロジェクトの侵入検出システム

各ターゲットは侵入検出を、基本的に自システムで行なう。しかし踏台アタックは、侵入の連鎖反応なので単独では検出できない上、踏台にされたシステムでは、アタッカーの行為が目立ちにくい傾向があるので、これを他システムと協調して検出する。

本システムの構成は、以下の通りである（図3）。

- ログ処理部： 推論部のためにログ処理を行なう。また、各システムのログのフォーマットの差異をここで吸収する。

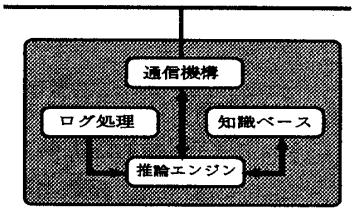

図 3: 侵入検出エージェント

- 推論エンジン部： エキスパートシステムとしての推論機構と、協調システムとしての推論機構を合わせ持つ。
- 通信機構部： 他の侵入検出エージェントと通信し、協調する。
- 知識ベース部：侵入のシナリオを持つ。

これらをまとめて、侵入検出エージェントと呼ぶ。

5 今後の課題

今後解決しなければならない問題として、

- 侵入を記述するための言語の開発
- 侵入判断のための協調、および効果的な知識ベースの分散
- 侵入検出エージェントのセキュリティ

がある。現在、知識ベース、および推論エンジンの設計の段階である。今後、通信、セキュリティの設計を並行して行なっていく予定である。

参考文献

[1] Kumer, S. and Spafford, E. H.: An Application of Pattern Matching in Intrusion Detection, *Technical Report CSD-TR-94-013* (1994).

[2] Lunt, T. F., et al.: A Real-Time Intrusion-Detection Expert System(IDES), *Final Technical Report. Computer Science Laboratory, SRI International,Melco Park, California* (1992).

[3] Illgun, K.: USTAT: A Real-Time Intrusion Detection System for UNIX, *Master's thesis, Computer Science Department, University of California, Santa Barbara* (1992).