

プラントネットワークにおける侵入検知方式の検討

4 T-8

小林 信博、勝山 光太郎

三菱電機(株) 情報技術総合研究所

1. はじめに

近年、インターネットの普及に伴い、インターネットに接続されたローカルサイト（組織内ネットワーク）への不正侵入およびシステム破壊などの犯罪件数も増加しつつある。このような被害をうけた場合の影響を考えると、ライフラインをささえるプラントネットワークでは非常に深刻な事態を招くことが予想される。これは我々の社会生活の基盤を脅かすことにつながるので、注力すべき重要な課題の一つとして考えられる。

従来、サイトのセキュリティ管理ポリシー^[1]としては、ファイアウォールを使用する不正侵入を防止するポリシーと、収集したシステムログを使用する不正侵入後に、不正侵入者を追跡し、その行動を記録し、不正侵入者を特定するポリシーがある。一般的には、サイト外部からの攻撃に対する準備をしていますが、内部からの攻撃に対しては無防備であるケースが多いとされている。^[2]そこで、我々はプラントネットワークへの侵入をサイト内部における不正行為全般としてとらえ、これを検知する方式について報告する。

本方式においては、ネットワークから入手した通信データをもとに侵入検知を行うが、データ解析方法に応じて処理を分散することにより、効率的な解析を実現することの特徴とする。

2. 従来の侵入検知方式

侵入検知には、ログの入手と解析の2つの機能が必要となる。また、それぞれ以下の様に分類される。

2.1. ログの入手方法

1. ホスト監視型
ホスト（コンピュータ）上で情報を収集する。
2. ネットワーク監視型
ネットワーク上に流れるデータ（パケット）を収集する。

ここでホスト監視型の場合は、ホスト上に情報収集機能を追加する必要がある。

2.2. ログの解析方法^[3]

1. AID (Anomaly Intrusion Detection)
ユーザアクティビティを統計処理し、普段の行動から外れていた場合に侵入として検知する。
 2. MID (Misuse Intrusion Detection)
既に確立された侵入パターンをデータベース化しておき、それと比較して侵入を検知する。
- なお、AIDは処理が複雑になるため、システムに負荷がかかる。また、MIDはデータベースに定義されていない侵入手口は検出することができない。

3. プラントネットワークにおける侵入検知の課題

課題として、以下の3つが挙げられる。

- サイトを構成するノードが専用システムとして実現されており検知用機能の追加が難しい。
- 各専用システムに対応した検知用機能を開発するコストがかかる。
- リアルタイム性を要求されるノードもあり、機能の追加による負荷の増加が望ましくない。

従来の侵入検知方式の一つとして、エージェントを用いることにより侵入追跡機能と侵入検出機能を実

A proposal for intrusion detection system at plant network

Nobuhiro Kobayashi, Kotaro Katsuyama,
Information Technology R & D Center,
Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura-shi, Kanagawa,
247-8501, Japan

現したシステム^[4]も提案されているが、プラントネットワークにおいては、以上のような課題により、そのままでは適用できない面がある。

4. プラントネットワークにおける侵入検知システム

プラントネットワークにおける課題を考慮し、図1に示すプラントネットワークにおける侵入検知システムを提案する。システムは、データを入手してMIDによる解析を行うセンサ機能、ログデータの管理やレポートの出力、アラームの管理などを行うマネージャ機能、AIDによる解析を行うログ分析機能の3つから構成される。

5. センサ機能

プラントネットワークからのデータの入手方法は、ネットワーク監視型とした。これにより、各ノードの改修を行う必要がなく、負荷の増加も防ぐことができるので、リアルタイム性の要求される計測器や制御機器等のノードに悪影響を及ぼさない。また、データベース化された侵入パターンを利用して、比較的単純なMIDによる解析も行う。

6. マネージャ機能

マネージャ機能では、センサ機能より得られる検知用ログデータをデータベースにて管理するとともに、必要に応じてアラームを出力する。また、GUI機能により、管理者の要求に応じたレポートも作成し、どのような侵入が発生したのかを把握し易くする。更に、検知用ログデータをログ分析機能へと渡すことにより、AIDによる侵入の検出を行う。

7. ログ分析機能

ログ分析機能では、負荷の高いAIDによる解析を行う。センサ機能、マネージャ機能と別のマシン上でログ分析機能を実行することにより、データの取りこぼしや、アラームの滞留などの処理遅延を回避することが期待できる。解析手順を記述したログ分析ルールを複数持つことによって、多様なパターンへの対処と、新たな手口への対策をとることが可能になる。また、負荷に応じて解析用のマシンを追加することも可能となる。

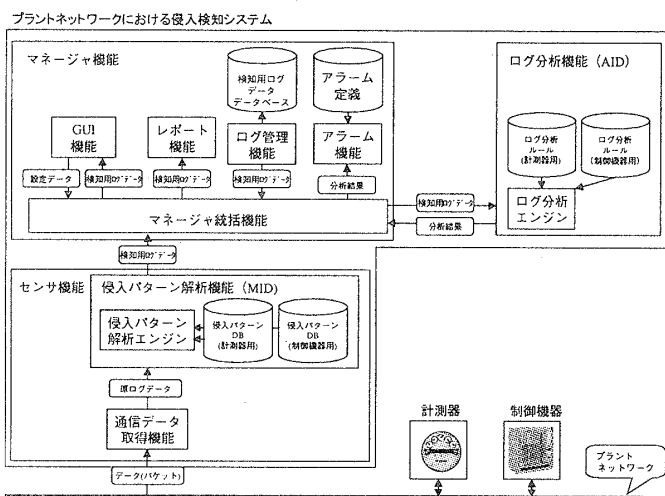


図 1 侵入検知システム構成図

8. おわりに

本稿では、ログの入手方法をネットワーク監視型とし、システムの負担となる解析機能を分散化させることで、効率的な侵入検知を可能とするプラントネットワークにおける侵入検知方式について述べた。これにより、プラントネットワーク上のノードに悪影響を及ぼすことなく、侵入を検知することが可能となる。

今後は実装を行い、評価を実施する予定である。

9. 参考文献

- [1] J. Holbrook, P. Reynolds, "Site Security Handbook." RFC1244, July 1991
- [2] "日本企業 800 社のセキュリティ白書", 日経コミュニケーション No.281, 日経BP社, 1998
- [3] S. Kumar and E. Spafford, "An application of pattern matching in intrusion detection", Technical Report 94013, Purdue University, Department of Computer Science, 1994.
- [4] 浅香 緑, "モバイルエージェントによる侵入検出システムのための情報収集方式", 電子情報通信学会論文誌 Vol.J81-D-I No.5, pp.532-539, 電子情報通信学会, 1998