ネットワークの不正アクセス検知方式の検討

1Z－7

藤井 誠司、大越 丈弘、河内 清人、勝山 光太郎
三菱電機(株) 情報技術総合研究所

1. はじめに

インターネットの普及に伴い、インターネットに接続した組織内ネットワークへの不正侵入およびシステムの破壊などの犯罪行為が近年増加している。これに対する対策技術として、侵入検知システムがある。侵入検知システムは、ネットワークのパケットやホスト上のログを監視し、不正アクセスを検知し、システム管理者に通知したり、不正アクセスのパターンから自動的に不正アクセスへの対策を実施するシステムである。

本稿では、ネットワーク上を流れるパケットを監視する侵入検知システムの改良手法について述べる。本稿で述べる手法は、パケットの取得および解析する機能を複数個で構成し、それぞれが並列に動作することにより、パケットの解析のスループットを向上させ、ネットワーク負荷の高い場合や高速なネットワークに対応できることを特徴とする。

2．ネットワーク型侵入検知システム

図1は、UNIX などの OS で使用されるネットワークモニタプログラム[1]を応用したネットワーク型侵入検知システムである。以下に示す要素から構成される。

●パケット取得機能

イーサネットデバイスドライバであり、ネットワーク上を流れるパケットを取得する。

●パケット分析機能

取得したパケットを分析し、不正アクセスであるか否かの判定を行う。

●不正アクセス分析データベース

不正アクセスの特徴を記録したデータを蓄積し、パケット分析機能が分析するために参照する。

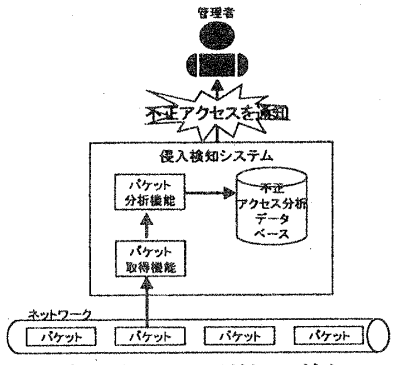

図1 ネットワーク型侵入検知システム

ネットワーク型侵入検知システムは、不正アクセスの検知を次の手順で実行する。

(1)ネットワーク上に流れるパケットをパケット取得機能が取得する。

(2)取得されたパケットは、パケット分析機能に渡される。

(3)パケット解析部は、取得したパケットで、不正アクセスデータベースの中のデータを検索する。

(4)一致したデータが存在した場合は、不正アクセスが行われていると判断し、管理者に通知する。

(5)一致したデータが存在しない場合は、解析対象のパケットは不正アクセスとは関係なしと判断し、次のパケットを解析する。

3．侵入検知システムの課題

図1に示すネットワーク型侵入検知システムには、次の示す課題が考えられる。

(1) パケットの取りこぼしによる不正アクセスの検出不能

ネットワーク上に膨大なパケットが流れる不正アクセスや高速なネットワークに構成されたネット

A proposal for network-based intrusion detection system
Seiji Fujii, Takehiro Ohkoshi, Kiyoto Kawauchi, Kotaro Katsuyama,
Information Technology R & D Center, Mitsubishi Electric Corporation

ワーク環境のように、単位時間あたり流れるパケット量が多い場合、単一のパケット取得機能で、パケットを取得するために、パケット取得機能がパケットの取りこぼしをする場合がある。パケットの取りこぼしを発生すると、不正アクセスが検知できない。

（2）分析の性能低下による不正アクセスの検出不能

単一のパケット分析機能でパケットを分析するため、パケット取得機能がパケットを取得する速度がパケット分析機能のパケットを分析する速度を上回る場合には、分析できないパケットが増加し、不正アクセスが検知できない。

4．提案する改良手法

そこで本稿では、上記のような課題を解決する手段として、図2示す構成の改良手法を提案する。

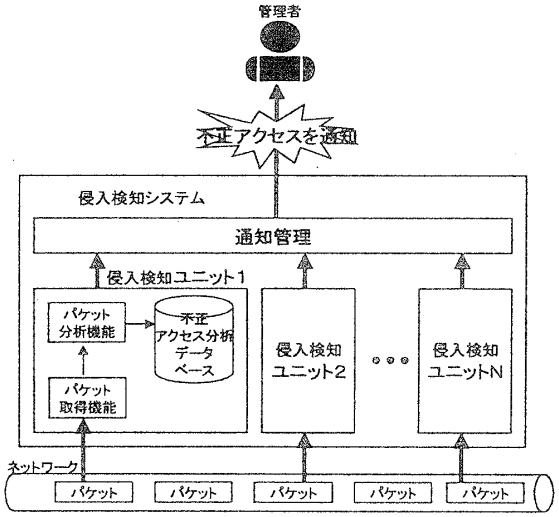

図2 提案する侵入検知システムの構成

本手法の特徴は、パケット取得機能、パケット分析機能および不正アクセス分析データベースから一つの侵入検知ユニットを構成し、侵入検知システムを複数の侵入検知ユニットと侵入検知ユニットから報告される不正アクセス情報を管理し、管理者へ通知する通知管理によって構成する。

また、各侵入検知ユニットに蓄積される不正アクセス分析データベースのデータは、図3に示すように、元のデータを分割して、分割したデータをそれぞれの侵入検知ユニットに配分する。

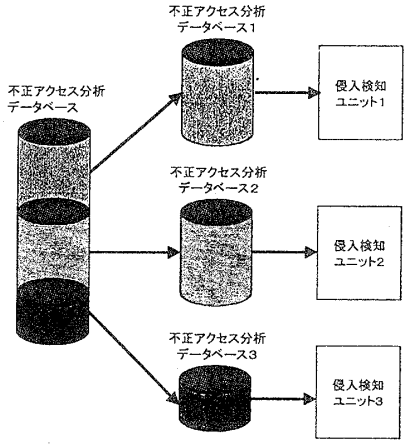

図3 不正アクセスデータの分配

また、同一の不正アクセスデータを持つ侵入検知ユニットのグループを構成することにより、データを分割したことより起きるパケットの取りこぼしを防ぐ。

以上により、侵入検知ユニットが複数個存在することにより、1つのユニットがパケットを取りこぼしたとしても、他のユニットでそれを取得することが可能になる。

また、不正アクセスデータベースを分割することにより、パケット分析機能の負荷を低下させ、パケットの分析の処理速度の低下を防ぎ、検知漏れを少なくすることが可能となる。

5．おわりに

本稿では、複数個でパケットの取得および解析する機能を構成し、それぞれが並列に動作することにより、パケットの解析のスループットを向上させ、ネットワーク負荷の高い場合や高速なネットワークに対応できる侵入検知システムの改良手法について述べた。今後は、本手法のプロトタイピングを行い、評価を実施し、本提案方式の有効性ついて検証する。

6．参考文献

[1] W.Richard Stevens,"TCP/IP Illustrated, Volumel The Protocols", Addison-Wesley Publishing Company, 1994