4F-5 セキュアログを利用したセキュリティ侵害検出手法

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、不正アクセスによる被害が増加している。これに対して、企業や大学、研究機関等においてイントラネットを保護する方策としては、ファイアウォールによる外部からの侵入防止が多くとられてきた[1]。更に現在は、ネットワーク内部への侵入及び内部犯行等のセキュリティ侵害行為を検知する方策も併せて重要視されつつある。この検知の際には、ネットワークを流れるトラフィックデータやホスト上のログデータが入力として利用されるが、巧妙な侵入者にはこのログを消去または改ざんされてしまう恐れがある。また、MID[2]と呼ばれる登録済のパターンと比較して不正行為を検知する方式では、既知のセキュリティ侵害行為にしか対処することができない。

そこで今回我々は、以下の機能をもつセキュリティ侵害の検出手法を提案する。

・セキュアログ機能

不正検知に必要なログを安全に収集・保管する。

・ログ分析機能

大容量・高速検索可能なDBを利用してAID[2]を行う。

本手法においては、保護する対象となるホスト上のログデータをセキュアログサーバにて収集し、高性能データベースを利用してAID処理を行うことを特徴とする。

A proposal for intrusion detection system with secure log
Nobuhiro Kobayashi, Kotaro Katsuyama,
Information Technology R & D Center,
Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura-shi, Kanagawa,
247-8501, Japan

2. システム構成

システム構成の概略を図1に示す。また、その主要コンポーネントについての説明を以下に記す。

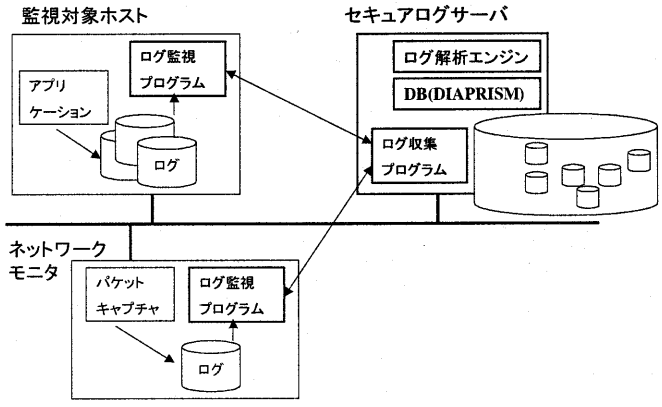

図 1 システム構成図

2.1. ログ監視プログラム

ログ監視プログラムは、監視対象ホストまたはネットワークモニタ上で動作する。指定されたログの更新をチェックし、新たに追加されたログをセキュアログサーバ上の収集プログラムへと転送する。また、ハートビート機能により、定期的に稼働状況をセキュアログサーバへと通知し、侵入者によるログ監視プログラムの停止を検出可能にする。

2.2. セキュアログサーバ

セキュアログサーバは、ログ収集プログラム、DB、ログ解析エンジンの3つのコンポーネントにて構成される。ログ収集プログラムは、ログ監視プログラムから転送されたログをDBに格納する。DBには、大容量・高速検索が可能なDIAPRISM技術[3]を利用する。ログ解析エンジンは、DB内のデータを利用してAID処理を実行し、セキュリティ侵害行為の有無を判定する。

3. セキュアログ機能

既にOSやアプリケーションにより生成されているログデータや、新たに追加されたチェックプログラムによるログデータを、監視プログラムが定期的またはイベント発生ごとにチェックする。そして新規追加分のログがあれば、これをログ収集プログラムへと転送する。その際、まずログデータからMAC (Message Authentication Code) [4] を算出し、ログ監視プログラムへ送信する。ログ監視プログラムはこのMACを保管しておく。続いて、ログデータをログ収集プログラムからログ監視プログラムへ送信する。ログ収集プログラムは、受信したログデータと保管しておいたMACとの整合性をチェックした上でDBに格納する。これにより、ログを安全な領域に格納することが可能となる。また、他のアプリケーション等を変更することなく、既存のログデータを保護することが可能なので、利便性が向上する。

4. ログ分析機能

ログ分析機能では、DIAPRISM を DB として利用し、ログによる AID を実行する。まず、ログデータから特徴データを抽出する特徴抽出ルールと、DB に格納されている特徴データと新たに入手したログデータから抽出した特徴データとの比較を行う比較ルールを予め作成する。そして、正常時のログデータ、または正常と確認されたログデータを入力して、特徴 DB を構築する。なお、特徴抽出ならびに特徴比較の際には、DIAPRISM の提供する 100 万件/2 秒での高速検索を利用することができる。

実際の稼動時には、新たに入手したログデータを入力とし、特徴抽出ルールから特徴データを抽出する。そして、この値と特徴 DB の値とを特徴比較ルールにより比較することで、セキュリティ侵害行為の有無を検出する。これら特徴抽出ルール、特徴比較ルールは検出用プラグインとして複数持つことが可能であり、プラグインの新規追加にも対応できる。また、原因追跡ルールを記述した原因追跡用プラグインを用意することで、セキュリティ侵害行為の原因を解析する機能を持たせることも可能である。

図 2 にログ分析エンジンのモジュール構成を示す。

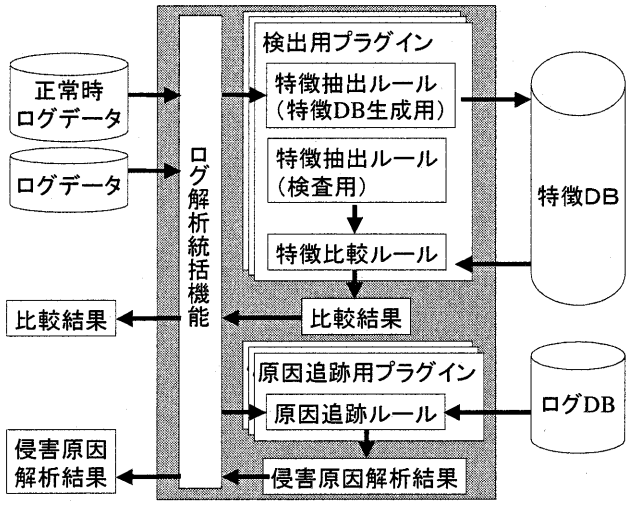

図 2 ログ分析エンジン

5. おわりに

本稿では、保護する対象となるホスト上のログデータをセキュアログサーバにて収集し、高性能データベースを利用してAID処理を行うセキュリティ侵害検出手法について述べた。これにより、不正検知に必要なログを安全に収集・保管することが可能となる。また、大容量・高速検索可能なDBを利用してAIDを行うことにより、未知のセキュリティ侵害行為を検知することが可能となる。今後は効果的な特徴抽出ルールと原因追跡手法の検討を進め、実装と評価を実施する予定である。

6. 参考文献

[1] “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

[2] S.Kumar and E.Spafford, “An application of pattern matching in intrusion detection”, Technical Report 94013, Purdue University, Department of Computer Science, 1994.

[3] DIAPRISM, 三菱電機株式会社, http://www.melco.co.jp/service/diaprism/index.html, 1999

[4] Bruce Schneier, “APPLIED CRYPTOGRAPHY SECOND EDITION”, John Wiley & Sons, Inc., p.p.31, 1996