【 別添2 】

時系列視覚化による計算機監視システム

1 背景

近年，ネットワークの普及に伴い、システムは分散して配置されより複雑化し、またセキュリティの問題も重大なものとなってきている。そのため、ネットワークセキュリティを向上するためにファイアウォールや不正侵入検知システムなどを設置するということが一般的になってきている。しかし、コンピュータシステムの維持管理作業は非常に大変で責任のあるものとなったにもかかわらず、その作業は非常に手間がかかり地道なものが多い。

システムを正常に運用していくためには、システムの状態をいつでも把握できるよう異常かどうか常に監視できるようにすべきである。システムの状態を知るために重要な情報として“ログ”がある。各計算機、ファイアウォール、不正侵入検知システムなどの“ログ”を監視することにより、異常の未然防止や不正なネットワーク活動の早期発見を行うことができる。

そのため、システムの運用では、複数のログを同時に監視し、異常が発見されたら早急に対応することが重要であると考えられる。しかし、現在ログをテキストのまま複数同時に見て解析することは、非常に大変である。

2 目的

複数のログを監視するということにおいて、非常に問題となるのは時刻を一致させて監視を行うことである。現在、各ログを個別に監視する場合が多いが、そのために実際に詳細に解析したくなったときには、時刻を一致させ、ログの関連性からシステムの異常の全体像を掴むということが非常に困難である。そのため、以前私は、複数のログの解析のために時刻に着目してその時系列を視覚化したシステムのプロトタイプを作成した。ただし、このプロトタイプでは、各ログはファイルから直接読むために多種のログに対応しづらく、またリアルタイムに解析することも厳しかった。

そのため今回開発するシステムでは、

・リアルタイムの監視に対応する
・ 多種のログに対応する
・ 異常状態を的確に判断するためのアルゴリズムを実装する

という点を取り入れた"時系列視覚化による計算機監視システム"の開発を行うことが目的である。

3 開発の内容

3.1 動作環境

システムを開発するにあたって使用した言語は Java である。そのため基本的にどの環境でも動作する。またログを保存するデータベースとして mysql を使用し、データベースに保存されているログを読み込むことを想定している。各ログをデータベースに入力するスクリプトやプログラムは汎用的に使われているものをそのまま使用することができる。

3.2 対応ログ

現在、このシステムでは、以下の3 つのセキュリティツールのログに対応する。ただしログの種類は、今後容易に追加することができるよう考慮して設計を行っている。

- Iptables – Linux で一般的に用いられるパケットフィルタ型ファイアウォール
- Snort – オープンソースで開発され、最も利用されているネットワーク型不正侵入検知システム
- Sebek – オープンソースで最も使用されているキーストロークロガー

3.3 システム構成と特徴

時系列視覚化による計算機監視システムでは、データ取得部、時系列視覚化部、詳細情報表示部の3 つのモジュールによって分かれている(図1)。

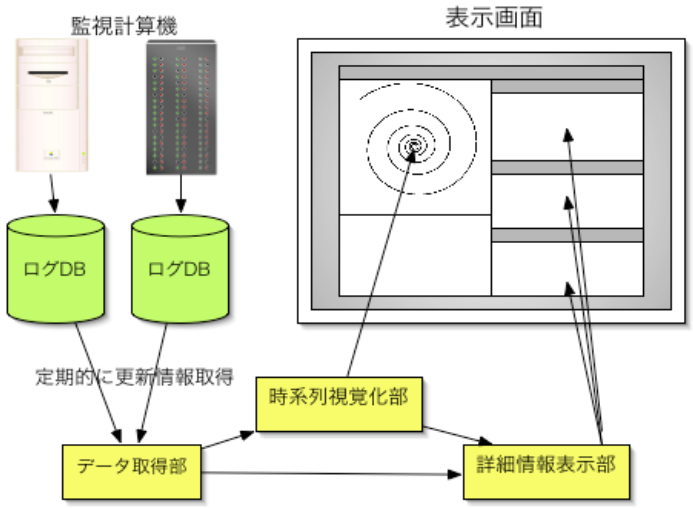

図 1: システム構成

システムの特徴としては、時系列視覚化により１週間の時系列を、１日を１周とした螺旋で表現し、さらに複数のログを時間軸を揃えて統合的に視覚化している。このことにより１週間という長期から分単位の短期まで各ログの関連、周期性を把握しながら調査することが出来る。

また多くのシステムでは警告やエラーがある時刻では、その瞬間ログの出力数が急激に増えることを用い、ログの出現頻度をヒストグラムと色の透明度によって表現することで、注目すべきログの箇所を知らせる。そして、カーソルで示した時系列の時刻とログの詳細が連動して表示されるため、容易に詳細まで解析していくことが可能である。

またこの時系列視覚化をリアルタイムに更新していくことで、現在の監視対象の状態を過去と比較しながら見ることが出来るため異常かどうかの判断を素早く行うことが出来ると考えられる。システム画面を図2 に示す。

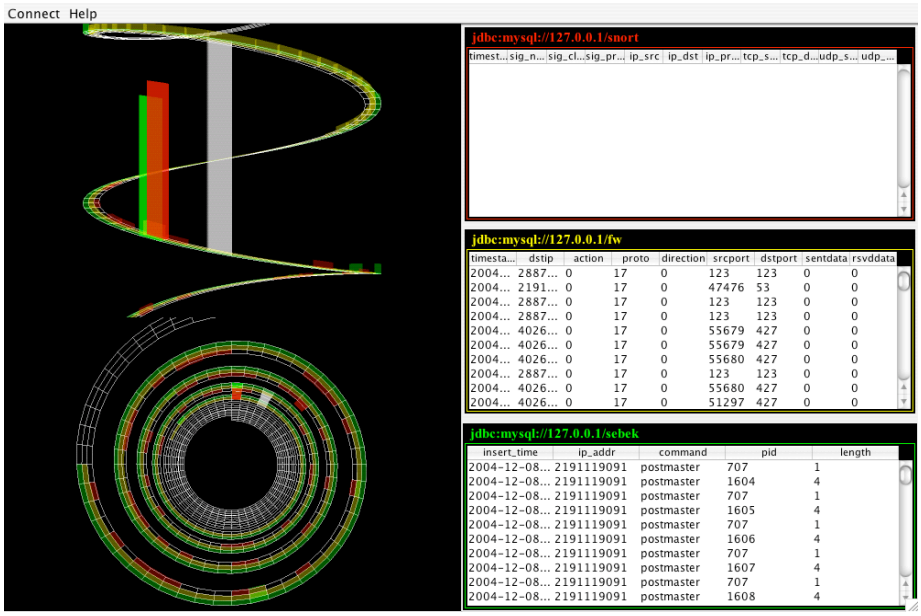

図 2:システム画面

４．従来の技術（または機能）との相違

ログを用いた解析ツールはいろいろ存在する。有名なものとしては ACID がある。ACID は、ログをデータベースに取り込み、統計解析してイベントの割合を円グラフで表現したり、異常なログをピックアップしたりしてレポートとして表示する。また製品として売られているものでこのようなことを行うツールは、他にも多く存在する。

しかし、これらは管理者が定期的にレポートを読んでおき、かつ異常が起きた場合には、ログのテキストを解析しなくてはならない。またレポートは基本的にログごとに生成されるため、ログ間の関連を調べることは困難である。

このシステムでは、視覚化によって大まかな概要を知っておきながら、異常がわかった際には即座に詳細な解析を行うことができる。

５．期待される効果

開発したシステムにより、ネットワーク管理者などの負担を減らす一つの解決策になればと思っている。特に、複数のサーバを動かしていたり、ファイアウォールや IDS などのシステムを統合して運用したりする場合には、その監視を支援するツールとして役立つと考えられる。

６．普及（または活用）の見通し

現在、私自身がこれを使用して、研究などを行っている。しかし、大量の情報を含むログでは、頻度による強調表示は必ずしも有効ではないことがわかっており、これに対する有効な視覚化手法を検討している。また計算機で多く用いられている syslog などへまだ対応ができていない。これらを解決した段階でオープンソースなどで公開し、多くのシステム運用者に使って頂きたいと考えている。

７．開発者名（ 所属）

江端　真行　（ 電気通信大学）