見えログ: 情報視覚化を用いたログ情報調査支援システム

高田 哲司　　小池 英樹

電気通信大学大学院 情報システム学研究科

1　はじめに

計算機の運用管理においてログ情報の監視/調査作業はますますその重要度を増している．しかし，その作業方法は未だにエディタによるログファイルの閲覧や独自スクリプトによる特定ログの抽出等が主であると考えられ，手作業で膨大な量のログ情報を調査するという単調かつ時間のかかる作業をシステム管理者は強いられている．

そこで本研究では，ログ情報の調査作業を支援するシステム「見えログ」を提案する．本システムではログ情報から特徴情報を抽出し，それを情報視覚化を用いて文字による表示と合わせて視覚化し，ユーザに提示する．

これにより，ユーザは様々な観点からログ情報を調査することが可能になり，既知の異常を表すログ情報はもちろん，従来の方法では発見の困難であった未知の異常を表すログ情報の検出も可能になる．

2　システム管理者の憂鬱

計算機の運用管理において，システムの稼働状況の把握，電子メイルやWWW等提供サービスの障害検出，さらに近年では不正侵入検知の目的のため，ログ情報の監視/調査作業はますますその重要度を増している．サーバとして多く使用されているUNIX系計算機では，OSやサービスを提供しているプログラムが異常やその前兆を通知する目的でログ情報を出力している．また計算機への不正侵入対策のため，監視システムやFirewallを導入し，その状況をログに出力している．したがってログ情報にはシステムの運用上，重要な情報が多数含まれているといえる．

したがって、システム管理者はなんらかの方法でログ情報を調査し、その中に運用上の問題を意味するログ情報が存在するかを確認する必要がある。しかしログ情報は、文字による記録、膨大な量、種々の形式や偏在性などの特徴ゆえ、その調査作業は非常に手間のかかる作業であるといえる。また既知の異常を表すログ情報の抽出は、grepをはじめとした特定のkeyword検索で可能だが、中には既知でないが異常を表すログが含まれている可能性もあり、その抽出は既存の調査方法では非常に困難であるといえる．

そこで本研究では，ログ情報から特徴情報を抽出し，情報視覚化を用いたログ情報調査作業を支援するシステム「見えログ」を開発した．

3　見えログ: システム概要

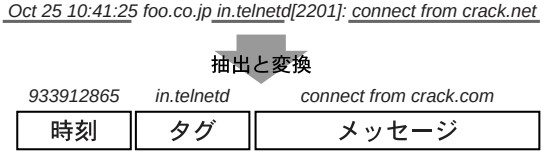

図 1: 汎用ログフォーマットとsyslogからの変換例

見えログでは，種々のログ情報を汎用ログフォーマット(図1)に変換し，これから種々の特徴情報を抽出する．この得られた情報を情報視覚化を用いて文字によるログ情報と合わせてユーザに提示する．文字情報を提供する理由は，ログ情報の調査を行うユーザ自身による正常/異常の判断を導入したいがためである．

この整形されたログ情報から抽出する特徴情報は，各単位時間あたりのログ数，タグ別ログ数，メッセージの長さ，メッセージに含まれる単語の出現頻度である．これらの情報を合わせてログ情報を視覚化した画面が図2になる．

画面は上下二分割，上位部分はさらに三分割されている．上位部分は左から各単位時間のログ数を表すヒストグラム，ログ情報のアウトライン表示，文字によるログ情報の表示となっており，下位部分はタグ別のログ数表示である．

この表示により，様々な観点から異常を表すログの検出を支援することが可能になる．例としては，まれにしか出現しないタグや単語の含まれたログ，ログ情報の出力数が極端に多いまたは少ない時間帯の存在，またメッセージの長いログや同じ長さのログが連続して出力されているなどの状況を容易に検出することが可能になる．もちろん，キーワードの指定により、異常を表す既知のログ情報の抽出も可能である．

またアウトライン表示では，メッセージ長によるフィルタリングが、ログ数ヒストグラムでは単位時間あたりのログ数によるフィルタリングが可能である。また文字表示部分から疑わしい単語を選択することで，その単語がメッセージ部に含まれるログ情報のみの表示など様々なフィルタリング処理が可能であり，疑わしいログの抽出をインタラクティブに支援する．

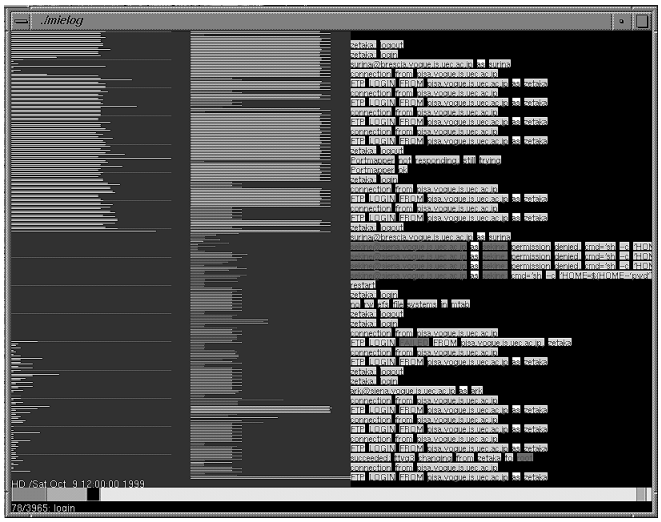

図 2: 見えログ画面

4　おわりに

本研究では，ログ情報調査作業を支援し、異常を表すログ情報の抽出を可能にするシステム「見えログ」を開発した。残念ながら，現在提示している情報で異常と思われるログ情報がどれだけ抽出できるか未評価である．今後は，システム管理者が行う定型作業や異常ログの抽出に必要な情報を調査し，システムをさらに洗練化する必要がある．

参考文献

[1] Eick S.G, Nelson M.C and Schmidt J.D, Graphical Analysis of Computer Log Files, Comm. of ACM, vol 37, No 12, pp. 50–56, Dec, 1994

[2] S.E. Hansen and E.T. Atkins, Automated System Monitoring and Notification With Swatch, USENIX Seventh System Administration Conference, pp. 145–155, Nov, 1993