見えログ:
情報視覚化と統計解析によるログ情報解析支援システム

MieLog: Visual Interactive Browser for Inspecting Computer Logs
using Information Visualization and Statistical Analysis

高田 哲司
Tetsuji TAKADA

電気通信大学 サテライト ベンチャ ビジネス ラボラトリ
（〒182-8585 東京都調布市調布ヶ丘 1-5-1 E-mail: zetaka@vogue.is.uec.ac.jp）

ABSTRACT. It is necessary for system administrators to inspect computer logs. As the Internet becomes essential in our life, such task gets more important than before. Because it is most basic task to response the anomaly status of computer and network like an intrusion to the computer. This is the report about “MieLog: Visual Interactive Browser for Inspecting Computer Log using Information Visualization and Statistical Analysis” that was developed as MITOU software project in 2001. It was a second year in this project. Therefore, I do not wrote the basic concept and the functions of “MieLog”, I wrote this year's development result of ``MieLog'' such as its interactive functions and real-time monitoring. And that, I wrote about “Tracker” developed with network security company after MITOU software project.

1. 背景

今日、計算機とそれを結ぶネットワークの正常稼働は社会インフラとして必要不可欠であることに疑いの余地はない。しかし、これらは自動的に維持されるものではなく、多くのシステム管理者の絶え間ない努力によって維持されている。

しかし、システム管理作業はその多くが地道な作業であり、好んで行われる作業とは言えない。その中で我々が注目したのはログの調査作業である。計算機やネットワーク上で発生した事象のほとんどはログと呼ばれるファイルに記録される。いいかえると、なんらかの異常事象が計算機またはネットワーク上で発生した場合、それらはログに記録される。したがってシステム管理者は、平時においてもログ情報を監視/監査し、異常やそれに準ずる事象がなかったかどうかを確認する必要がある。また、なんらかの異常事象があった場合には、原因追及を行うためにログを調査する必要がある。また、この作業は近年の計算機やネットワークに関するセキュリティ上の問題に対応するための最も基本的な作業として、その重要性はますます増しつつある。

その一方でこの作業にはいくつかの問題がある。一つはこの作業が単調、退屈かつ時間のかかる作業であることである。なぜならばログ情報は膨大な量の文字記録であるため、その調査作業とはすなわち、それらの記録を読んで理解しなければならないことである。もう一つは、その記録ごとにそれぞれが正常か異常かを判断しなければならないからである。したがって、実際にシステム管理者の多くはこれらの作業を行っていないという現状がある。

これらの理由から、この作業を支援するような仕組みが必要であると確信し、本プロジェクトではこの作業を支援するためのインタフェースとして「見えログ」を開発した。この文書では, 平成 13 年度未踏ソフトウェア創造事業における本プロジェクトの開発成果と共に未踏ソフトウェア創造事業終了後に企業と共同で行った開発成果について述べる。

2. 目的

本プロジェクトでは、計算機に記録されているログ情報の調査を支援する目的で「見えログ」を開発した。見えログは人間が主体となり、ログ情報の調査、すなわち異常またはそれに準じる疑わしい事象を表すログメッセージの発見を支援することを目的としたシステムである。したがってその目的ゆえに、見えログはログを見る必要のある人、すなわち計算機やネットワークを管理するシステム管理者を対象とするシステムである。

本システムは、ログ情報を *General Log Format* と呼ぶ中間フォーマットに変換し、この中間フォーマットのデータを元に情報視覚化を行う。また情報視覚化の前に統計解析をログに対して行い、ログから一見しただけでは得られない種々の情報を取得する。この中間フォーマット化されたログと統計解析の結果をあわせて、ログ情報を視覚化する。見えログのシステム構成図を図 1 に示す。

また本プロジェクトでいう情報視覚化とは、単にログ情報を図的に表現するだけではなく、ユーザがシステムによって提示された図を対話的に操作できることが大きな利点である。

図 2 は見えログの視覚化画面である。見えログは大きく四つの表示領域を持つ。それらはそれぞれ左からログ種別表示領域、時刻情報表示領域、アウトライン表示領域、ログメッセージ表示領域と呼ぶ。これらそれぞれの

表示領域に表示されている情報と、その表示方法に関する説明については前年度の開発成果報告[5]ならびに参考文献[4]にゆずり、この文書ではまず今年度開発を行ったログ調査作業を支援するための対話的機能とリアルタイム監視機能について述べ、ついで製品化に向けて企業と共同で開発した機能について述べる。

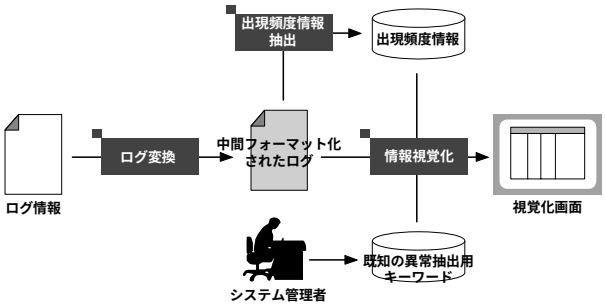


図 1: 見えログのシステム構成図

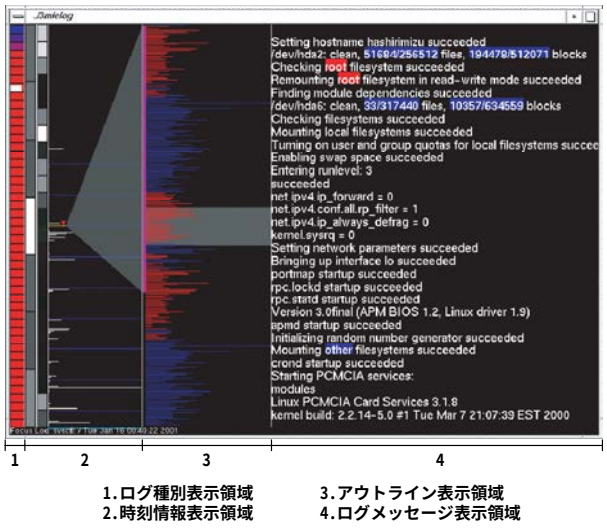


図 2: 見えログの視覚化画面

3. 対話的機能

見えログにおける対話的機能とは、ユーザが視覚化された図をもとに何らかの判断を行い、その判断に基づいて興味のある、または調査すべきログ情報を引き出し、あるいは絞りこむ作業を支援する機能である。これらの作業を視覚化システム内で対話的に行なうことが可能になれば、ログ調査におけるシステム管理者の作業負担は大幅に軽減されると考える。それは、ログ情報の「閲覧」と、疑わしいまたは異常と推測されるログメッセージの「抽出」という二つの作業を継続して繰り返しできることになるからである。これにより、従来までは別々に行われていた閲覧と抽出という作業を一つのシステム内でできることになり、その作業がシームレスに行えるようになるからである。

本プロジェクトでは様々な対話的機能を実現し、その抽出作業を実行可能にした。以降では、実現された機能を紹介する。

3.1 ログ種別表示領域における対話的機能

この表示領域では、ログ種別に基づくログメッセージのフィルタリングが可能である。フィルタリングの方法は簡単である。マウスを使って各ログ種別を表す格子をクリックすることで、各ログ種別が選択/非選択の状態に遷移する。この選択によりユーザは表示されるログ種別を自由に選択することができる。これは、既存のツールでも同じと思うかもしれないが、既存のツールとの違いはすべてのログ種別とその出現頻度がすでに既知、すなわち表示されていることである。これによりユーザは、なんらかの判断を行うことができ、その判断に基づいてログ種別を選択することができる。

もちろんユーザは、複数のログ種別を自由に選択することが可能であるとともに(図 3 上)、あるログ種別を基準として、そのログ種別よりも出現頻度の多いもの、または少ないものという基準でログ種別を選択することも可能である(図 3 下)。

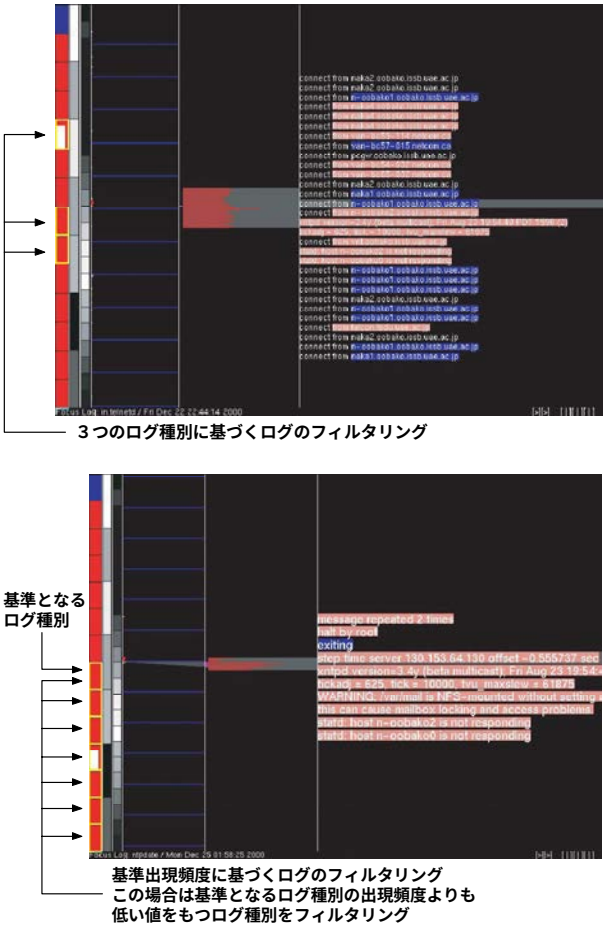


図 3: ログ種別によるフィルタリング(上)と出現頻度に基づく複数ログ種別のフィルタリング(下)

3.2 時刻情報表示領域における対話的機能

この表示領域では、時間情報に基づくフィルタリングが可能である。

周期的側面による時刻情報表示領域では、個々の周期時間単位によるフィルタリングが可能である。つまり曜日によるフィルタリングや、23 時台といった時間帯によるフィルタリングが可能である。もちろん、この二つを組み合わせたフィルタリングも可能である。つまり、木曜日の 23 時台に出力されたログのみを表示するというフィルタリングが、各時間帯を表す格子二つをマウスでクリックするだけで実行可能である(図 4)。

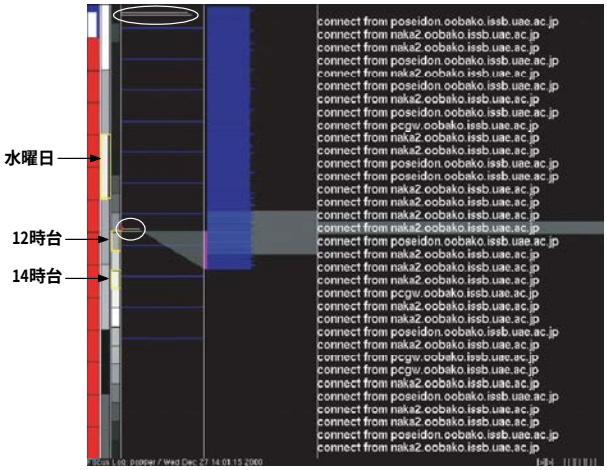


図 4: 周期的間隔によるフィルタリング：水曜日の 12 および 14 時台

またもう一方の各時間間隔別ログ出力数を表すヒストグラム表示では、ログ出力数に基づくフィルタリングが可能である。この時刻情報表示領域のヒストグラム表示におけるフィルタリング方法は次の通りである。

まずフィルタリング機能の種別を決定する。このフィルタリング機能には以下の三種類がある。

- 基準値よりもログ出力数が少ない
- 基準値とほぼ同じ出力数
- 基準値よりもログ出力数が多い

次に、マウスを使って基準値を対話的に決定する。ヒストグラム表示領域内においてマウスの中ボタンを押下することにより、基準値を表す縦線が描画されるようになる。マウスの中ボタンをその表示領域内でドラッグすることにより、この縦線を左右に移動させることができる。このようにして自分がフィルタリングの基準値にしたいと思う位置でマウスの中ボタンをはなす。このマウスをはなすという行為により、実際の決定された基準値を使って、決定したフィルタリング機能により、その条件に一致した時間帯が決定され、その結果としてその時間帯に出力されたログメッセージが表示される(図 5)。

3.3 アウトライン表示領域における対話的機能

この表示領域では、ログメッセージの長さに基づくフィルタリングが可能である。

このフィルタリング方法は、時刻情報表示領域におけるヒストグラム表示領域でのフィルタリング方法とまったく同じである(図 5)。ただし、アウトライン表示領域では時刻情報表示領域とは異なり、フィルタリング基準が「ログメッセージの長さ」になる。したがってフィルタリング機能は以下の三種類となる。

- 基準値より短いログメッセージ
- 基準値とほぼ同じ長さのログメッセージ
- 基準値よりも長いログメッセージ

またアウトライン表示領域には表示されているものの、ログメッセージ表示領域には文字として表示されていない部分が多くある。そのようなアウトライン表示部位に異常を表すと推測されるログパターンを発見した時、そのログメッセージの詳細を知りたいと誰でも思うだろう。

そんな場合のために、アウトライン表示領域の特定のログメッセージの詳細をログメッセージ表示領域で即座に閲覧できるようにする機能がある。それはその詳細を知りたいと思うアウトライン表示領域内の線をマウスでク

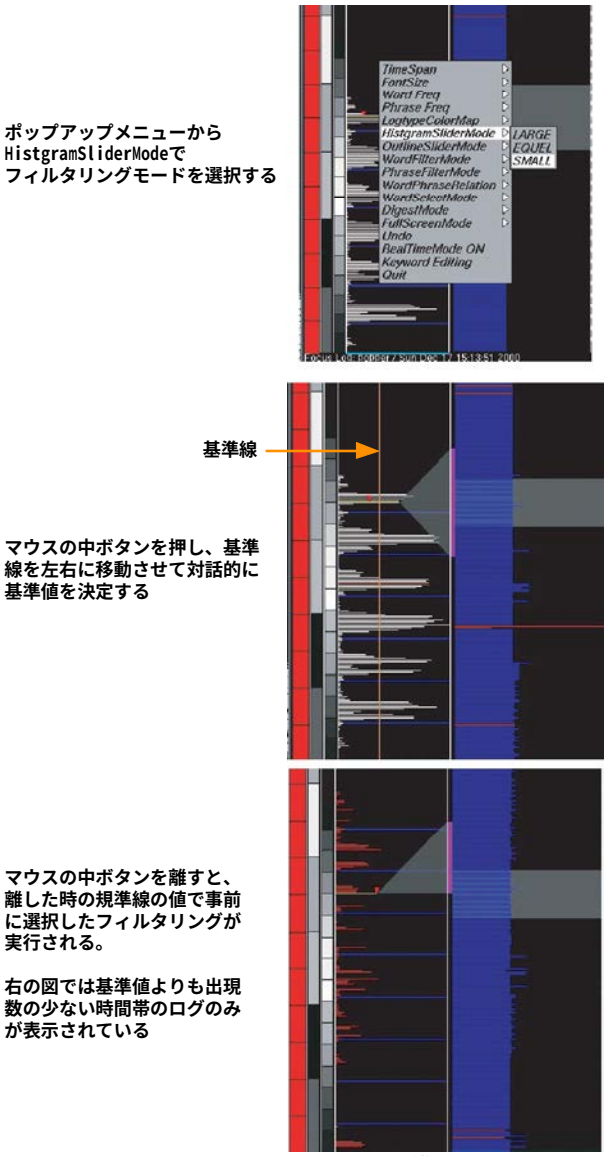


図 5: 時間間隔ごとのログ出力数を基準としたフィルタリング

リックする。すると、クリックした線が画面中央に自動的に移動し、その詳細がログメッセージ表示領域に表示されるようになる。

3.4 ログメッセージ表示領域における対話的機能

この表示領域では、ログメッセージに含まれる単語や句に基づくフィルタリングが可能である。

まずはじめに、今回の開発では出現頻度に基づくログメッセージのハイライト処理を単語単位だけではなく、連続した二単語に基づく「句」にも拡張した(図 6)。

これにともない、フィルタリング処理も単語単位だけではなく句単位でのフィルタリングも可能にした。その方法は次の通りである。まずはじめに、ポップアップメニューから句を基準としてフィルタリングを行うことを明示する。それはポップアップメニューから``WordPhra

seRelation"という項目を選択し、そのサブメニューから``PHRASE"を選択することで行える。その次にマウスで自分がフィルタリングのキーワードとしたい句を選択することで、フィルタリング処理は実行され、その結果が表示される(図 7)。

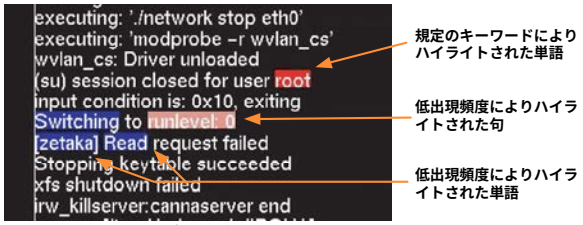
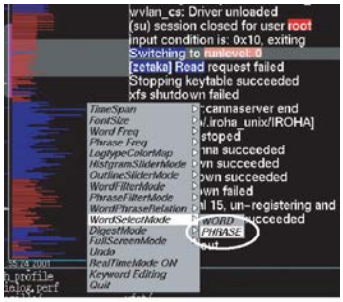
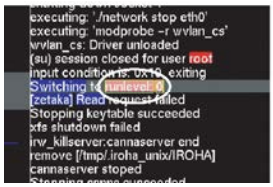


図 6: 句を単位としたハイライト処理

1．ポップアップメニューから WordSelectModeを選択し、PHRASEを選ぶ



2．フィルタリングしたい句を選択する



3．フィルタリング処理が行われる

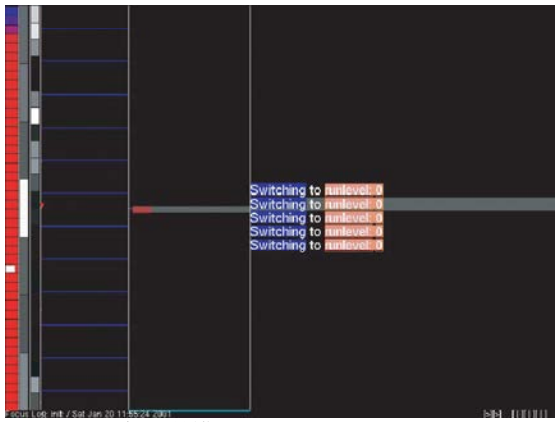


図 7: 句を基準としたフィルタリング

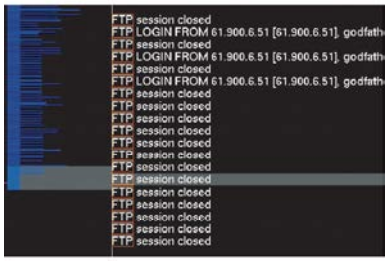
また複数の単語または句によるフィルタリングも可能である(図 8)。ここでは単語を例として説明を行う。

見えログでは単語や句を単位としてフィルタリングを行うことが可能であるが、さらにそれらを複数使用してフィルタリングをすることも可能である。もちろん段階的に繰り返しフィルタリングを行うことも可能である。

複数の単語を使ってフィルタリングを行うには、それら複数の単語をどのように組み合わせてフィルタリングするかという問題がある。見えログでは、この組み合わせとして論理積(AND)と論理和(OR)を使用することができる。論理積ではキーワードとして選択された複数の単語の全てが含まれるログメッセージを抽出し、論理和ではキーワードとして選択された複数の単語のどれか一つでも含まれるログメッセージを抽出する。またこれとは別に論理否定(NOT)も利用可能であり、指定した単語(群)を含まないログメッセージを抽出することができる。これらのフィルタリング機能はポップアップメニューを通じて指定される(図 9)。

元の画面

"FTP"という単語によるフィルタリング



"FTP"と"LOGIN"という単語のAND条件によるフィルタンリング

図 8: 複数の単語によるフィルタリング

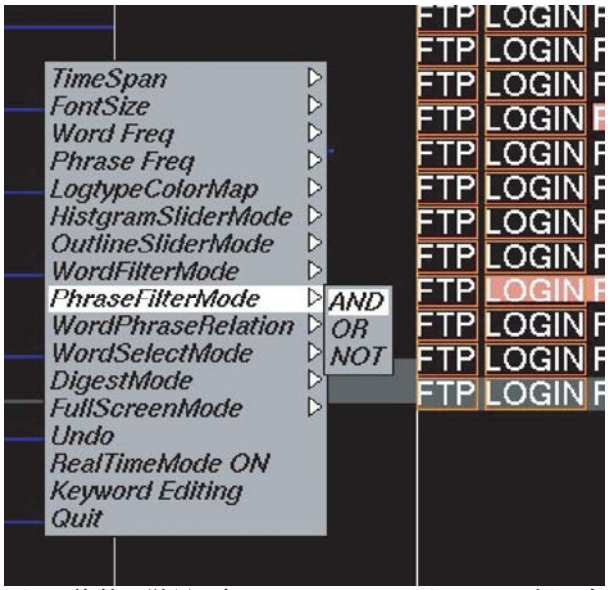


図 9: 複数の単語や句のフィルタリングにおける組み合わせ方法

複数の単語や句によるフィルタリングは以下の通りである。まずはじめに単語によるフィルタリングか句によるフィルタリングをするのかをポップアップメニューの``WordSelectMode"のサブメニューを使って指定する。次に、複数のキーワードまたはキーフレーズを指定した時のフィルタリング処理におけるそれらの組み合わせ方法を指定する。単語の場合は``WordFilterMode"、句の場合には``PhraseFilterMode" のサブメニューを使ってそ

れを行う(図 9)。そして、フィルタリングのキーワードまたはキーフレーズを Shift キーを押したまま、マウスの左ボタンで順次選択していく。そして最後のキーワードまたはキーフレーズを選択する時には Shift キーを押さずにマウスの左ボタンを使って選択しする。これにより複数の単語または句を使って、指定した組み合わせ条件フィルタリング処理を行い、その結果が表示される(図 8)。

3.5 ログメッセージ要約機能

見えログにはログメッセージの重複を省くログメッセージ要約機能がある(図 10)。

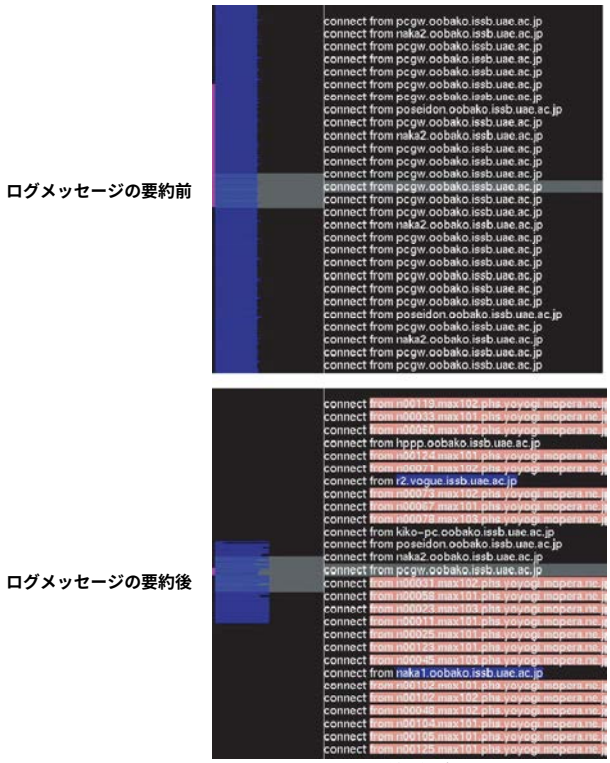


図 10： ログメッセージ要約機能

ログには膨大な量のメッセージが記録されている。それゆえ、ログメッセージの調査には非常に多くの時間がかかる。しかし、ログが膨大な量になる原因の一つには、正常事象に関わるログメッセージがログに記録されることが挙げられる。そこで見えログでは、同一のログメッセージが複数存在する場合にその重複を省くことによる表示ログの減量を可能にした。つまり表示されるログメッセージはすべて内容の異なるログメッセージになる。つまり要約された状態にすることができる。

図 10 を見るとわかるが、図中の上の表示にはまったく同じログメッセージが多数記録されている。ここで要約処理を行いログメッセージを要約すると図中の下の表示になる。アウトライン表示部位に注目して欲しい。上の図では多数のログメッセージがあることを示しているが、下の図を見るとログメッセージは全種類で若干数しかないことを表示している。また、上の表示ではなかった出現頻度の少ない単語や句の含まれたログメッセージを発見することもできることを示している。

3.6 異常キーワード定義の追加機能

見えログでは、異常であることが既知であるログメッセージを抽出するためにキーワードを定義する必要がある。これまではユーザがエディタを使用してキーワードを定義したファイルを作成する必要があった。しかし、これでは調査作業が閲覧/調査とキーワード定義の二つに分割されてしまい望ましくない。また、ひとたびキーワード定義を変更したら、その変更は見えログが再起動されるまで表示に反映されないという問題があった。

そこで今回の開発では、キーワードやキーフレーズ定義用に GUI を作成した(図 11)。これはポップアップメニューから起動される。この GUI を使えばテキストエディタを使わずにキーワード定義を行うことができる。また、このツールを通して行われたキーワードはこのツールを終了すると同時に表示に反映されるため、見えログ自身を再起動する必要はない。またこの GUI は、キーワード定義用ツールとして単体でも使用することが可能である。

図 11： キーワード/キーフレーズ定義用 GUI

4. リアルタイム監視機能

本プロジェクトでは、見えログにリアルタイムによるログ監視機能を実装した。

昨年度開発では、すでに存在する、つまり記録済みのログ情報を静的に表示する機能しか実装できなかった。しかしながら、ログの監視の必要性からリアルタイムでログを表示する機能は必要不可欠であった。そこで今年度は擬似的、すなわち若干の時間差は生じるものの、ログ情報をリアルタイムで追従表示する機能を実装した。

また本機能の導入に伴い、従来との互換性を考え、見えログは二つの動作モードを持つことになった。一つは従来通りの動作である記録済みログの静的表示と調査のための対話的処理が実行可能な``Post Mortem"モード、もう一つは今回導入されたリアルタイム監視を行う``Real-Time"モードである。これらの動作モードの切り替えは、ユーザがポップアップメニューを通じて簡単に切り替えることが可能である。

``Real-Time"モードでは、ログに記録された最新の情報を表示領域で可能な限り表示する。つまりログファイルの最後尾に記録されている部分を可能な限り表示することとなる。また現在の実装では、``Real-Time"モードで動作している時には、ログ調査のための対話的機能を使用することができない。したがって、リアルタイムにログを監視している際に、なんらかの異常と思われるログを発見し、その詳細を調査する必要が生じた場合には、動作モードを``Post-Mortem"モードに切り替え、対話的機能を用いて調査を行わなければならない。

また、実際にログが記録されてから見えログの画面に表示されるまでの時間差だが、現在のところ 10〜30 秒程度の遅れが存在する。これはログの出力される量や、

見えログの処理を行う計算機の能力にも依存する。なお現在のところ、遠隔計算機のログをネットワークを介してリアルタイム監視することはできない。

5. 強化された機能

今回の開発では、対話的機能とリアルタイム監視機能のほかに従来までの機能を強化した開発項目もある。それは視覚化方法と操作方法である。

・二種類のログ種別の色付け機能
ログ種別表示領域およびアウトライン表示領域ではタグ情報の出現頻度に基づき赤 - 青による色付けがなされている。しかしタグ情報の出現頻度は分布に偏りがあるため中間色が使われることは少なく、それゆえに個々のタグ情報の区別が視覚的に難しいという問題があった。
そこでこの問題を改善するため、各タグ情報の出現頻度に基づく色付けのほかにタグの種類数に基づく色付けを可能にした。これにより中間色が使われるようになり、タグの数が多くなったとしても、従来よりも容易に視覚的に識別することを可能にした(図 12)。

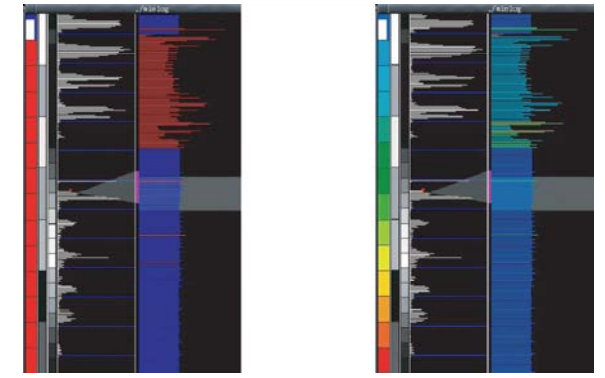


図 12 : ログ種別における二種類の色付け方法

・ログ種別毎分類表示
アウトライン表示領域では、表示対象となっているログメッセージが一つの表示領域内にすべて表示されているため、特定のログ種別がアウトラインのどの線に該当するかが認識しにくいという問題がある。原理的には、ログ種別の色がアウトライン表示領域でのログメッセージを表す線の色と同一であるため認識可能なはずのだが、実際には上記の色付けに関する問題ゆえにその認識が困難である。また特定のログ種別だけ抽出して表示することで解決できると思われるが、この場合には他のログメッセージが表示されなくなるため、他のログメッセージとの関係がわからなくなるとともに、該当ログ種別の実際のログ出力パターンも不明になるという問題がある。
そこで今回の開発では、この問題を改善するために新たな表示方法を実装した。それはアウトライン表示領域きを拡張し、ログ種別ごとにアウトライン表示を行う視覚化手法である(図 13)。
これにより、各ログ種別毎のログメッセージ出力状態をパターンとして認識できるようになる。他のログ種別のメッセージとの相関や、各ログ種別ごとの出力パターンも、その認識が可能になる。

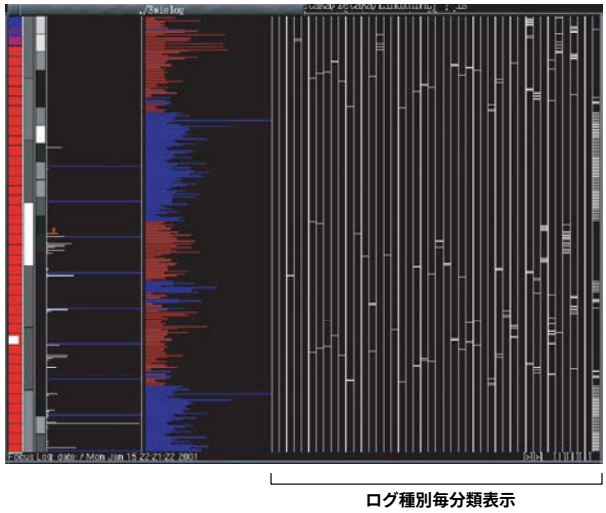


図 13 : ログ種別毎分類表示

・キーボードによる操作
従来、見えログの操作はそのほとんどをマウスに依存していた。
しかし、ログを閲覧するシステム管理者はその業務上 GUI よりも CUI の操作になれ親しんでいる人たちが多いといえる。そこで今回の開発では、可能な限り多くの対話的機能をキーボードでも操作可能にした。これにより、キーボードの操作に慣れている人は、マウスではなくキーボードを使用することが可能になり、より迅速に見えログを操作することができるようにした。

6. 企業との共同開発成果

ここでは、未踏ソフトウェア創造事業におけるプロジェクト終了後にシーア・インサイト・セキュリティ(株)と共同で開発した成果について述べる。尚、同社で見えログを製品化するにあたり、製品名を「SEER Tracker」としており、以下では Tracker と呼ぶ。

6.1 コンバータの追加

見えログでは中間フォーマットを採用しているため、種々のログへの対応が可能である反面、変換プログラムの存在が必要不可欠であった。見えログでは二種類の変換プログラムだけにとどまっていたが、Tracker では以下のようなログの変換が可能となった。

・Linux の syslog とログインログ(wtmp、utmp)
・Solaris の syslog とログインログ(wtmp、utmp)
・HP-UX の syslog とログインログ(wtmp、utmp)
・Apache の access_log 及び error_log

6.2 外観の変更

Tracker では大幅にブラウザの外観が変更された。基本的に変更がなされたのは色である。見えログでは黒地に白を基調としていたがこれは長時間画面を見る場合には疲れやすい組み合わせと言えた。特にログの調査では文字を読む必要があることから、これを白地に黒を基調

とすることで、長時間作業をしても疲れにくい画面構成に変更した(図 14)。

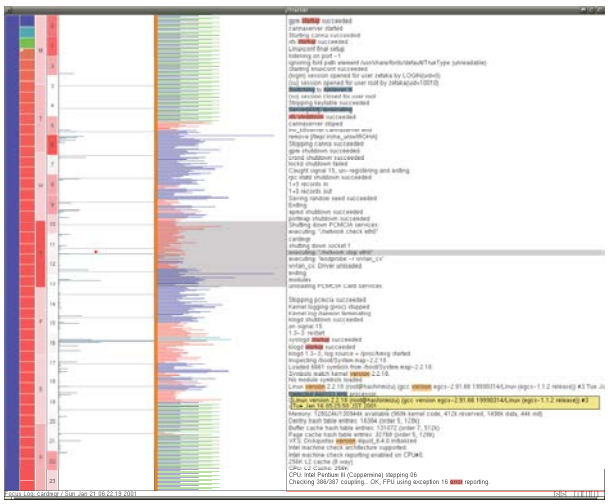


図 14 : SEER Tracker の画面

また、ログメッセージ表示領域においてのハイライト処理に用いられていた色も、以前は統一性に欠けるものであったためこれを変更した。具体的には以下のようになった。

・ユーザが設定したキーワード	ピンク
・閾値以下の単語・句	青
・上記２つを同時に満たす単語・句	赤
・マウスでポイントした単語・句	オレンジ

また、見えログではホスト情報を表示する領域がなかったため、複数ホストのログが混ざったログを調査するときにどのログがどのホストから出力されたものなのか認識できないという問題があった。Tracker ではホスト情報を表示する領域が新たに追加された。

6.3 検索機能

以前はログメッセージ表示領域で特定の単語でフィルタリングなどをしたい場合にはその単語をクリックすることでこれを行っていたが、それにはその単語を見つけるという作業が必要であった。そこで、Tracker では検索用の GUI を用意した(図 16)。図のテキスト入力部分に探したい単語を入力して Find ボタンを押すと一致する単語を含むログを抽出する。単語はスペースを空けて複数指定することも可能である。但し、この機能はワードフィルタの延長であるため、入力された単語とログ中の単語は完全に一致している必要がある。

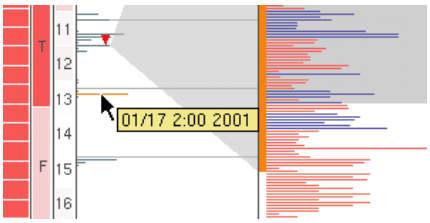
図 16 : 検索機能の GUI

6.4 ポップアップ機能

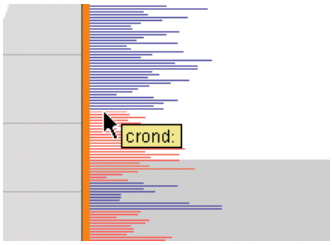
見えログでは、マウスでクリックすることで様々な対話的な操作を可能としていたが、クリックしようとするものが何であるかわかりにくいという欠点があった。これを解決するためにポップアップ機能が実装された。

ポップアップ機能はマウスでポイントした部分に関連する情報をポップアップ形式で表示する機能である。ポップアップ機能はほぼ全ての表示領域で実装されており、各領域ごとに適切な情報を表示する(図 15)。

タイムヒストグラム表示領域



アウトライン表示領域



ログメッセージ表示領域

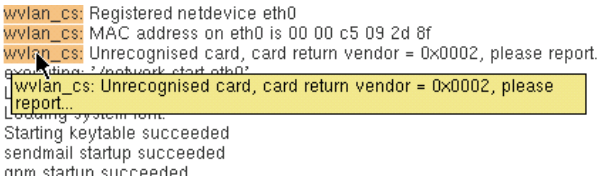


図 15 : ポップアップの例

6.5 パフォーマンスの改善

見えログでは、ブラウザが中間フォーマットのログを読み込む時にかかる時間がログの行数に対して指数関数的に増えるという問題があった。また、ブラウザ操作時にも、マウスがポイントしたオブジェクトに対するレスポンスが全体の単語数に対して指数関数的に遅くなるという問題もあった。
Tracker ではこの２つの問題を改善し、ログの読み込み時間に関してはログの行数に対してほぼ比例となるように改善し、マウスのポイントレスポンスに関しては単語数の差がかなり大きくてもほとんど差を感じない程度にまで改善された。

7. 今後の課題

見えログにおける今後の課題は以下の通りである。

・使用評価
本システムは、まだ開発者のあいだでしか使われていない。したがって、実際にログを見ている人に本システムを利用していただき、実際に現場での経験に基づくアイデアを提案していただくことがシステムの改良には必要不可欠であると考えている。したがって、なんらかの方法で評価を行う必要がある。

・種々のログへの対応

見えログでは、その入力が中間フォーマット化されたログである。この仕組みにより、見えログは種々のログに対応可能という利点を持っている。しかし、それは種々のログを中間フォーマットに変換するプログラムの存在が必要不可欠である。企業との共同開発により変換プログラムは増えたが、まだ充分とは言えない。したがって、種々のシステムやプログラムのログに対応するために、より多くのログ変換プログラムを用意する必要がある。

・リアルタイム監視処理の改良
今回の開発におけるログのリアルタイム監視処理は、プロトタイプ実装と言える。とはいえ、この実装により様々な問題点が明らかになったのも確かである。今回の経験をもとに、よりユーザが期待するリアルタイム監視処理を実装する必要がある。
早急な課題としては、ログが記録されてから実際に見えログにて表示されるまでの時間短縮、ならびにネットワークを介した遠隔計算機の監視可能化が挙げられる。これにより、見えログは単なるログ情報調査支援システムとしてだけでなく、ログ監視コンソールとしての機能を果たすことも可能になる。

・さらなる対話処理の実装
ログ調査において必要ならびに有用と思われる対話機能をさらに追加実装する必要がある。特に必要と考えているのは、調査済みのログメッセージを調査対象外にする機能である。これにより調査済みで問題視する必要のないログメッセージを視覚化対象から排除することで冗長な調査作業をなくすことが可能になると考える。また使用評価に基づき要望の多い対話処理を実装する必要があるだろう。

8. おわりに

本文書では、ログの調査作業を支援するシステム「見えログ」について、平成 13 年度の開発成果とその後の事業化における開発成果に焦点を当てて、その報告を行った。

今年度の開発ではログの調査を支援する「対話的機能」とリアルタイムでログを追従監視する「リアルタイム監視機能」について、その詳細を述べた。これらの機能の実現により、見えログはより実用的なシステムになったと確信している。しかし、これらの機能は開発者の間で発案されたアイデアであり、実際の現場にて評価を行う必要がある。実際にログを見るシステム管理者に評価をしてもらい、現実的に必要だが見えログには実装されていない対話的機能を提案してもらうことは、見えログをよりよいシステムとするために必要不可欠であろう。

今後も開発を継続するとともに、なんらかの方法で評価を行いたいと考えている。

参加企業及び機関

本プロジェクトの遂行において、開発を主として多大なる協力を頂いたシーア・インサイト・セキュリティ(株)のメンバーの皆様には謹んで感謝の意を表する。

(株) Seer Insight Security
mail: info@seerinsight.co.jp
url: http://www.seerinsight.co.jp/

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 (1994).

[2] Cox, K.C., Eick, S.G., Wills, G.J. and Brachman, R.J.: Visual Data Mining: Recognizing Telephone Calling Fraud, *Journal of Data Mining and Knowledge Discovery* , Vol.1, No.2, pp.225-231, (1997).

[3] Lee, W. and Stolfo, S.: Data Mining Approaches for Intrusion Detection, *Proc. 7th USENIX Security Symposium* , Jan, (1998).

[4] 高田哲司、小池英樹: 見えログ: 情報視覚化とテキストマイニングを用いたログ情報ブラウザ, 情報処理学会論文誌 Vol.41, No.12, pp.3265-3275, (2000).

[5] 高田哲司: 見えログ: 情報視覚化とテキストマイニングを用いたログ情報解析支援システム, ITX2001(IPA Technology Expo), Nov, (2001).

[6] 警視庁: ハイテク犯罪に関するアンケート、http://www.npa.go.jp/hightech/enquete/index.htm, Sep, (1998).