ぎ-13

表計算ソフトウエアをGUIとするログ解析システム logeasy

麓 泰丈*、千種 康民*、Hector Sandoval*、濱 正章**、石丸 雅彦**
*東京工科大学　**日立ソフトウエアエンジニアリング

1．はじめに

本研究グループでは、Linux マシン遠隔管理システムの構築を目的とし、ネットワーク資源の有効活用、遠隔管理、複数PCの一括管理、データベース化、自動化、自律化、等の実現を目指し研究を行っている．

本稿では、クライアント側によるログ解析システムによる可能な限りの自律診断、保守管理者への負担の軽減を目的とし、linux 遠隔管理におけるログ監視サブシステム logeasy を実現するものである．（図1）

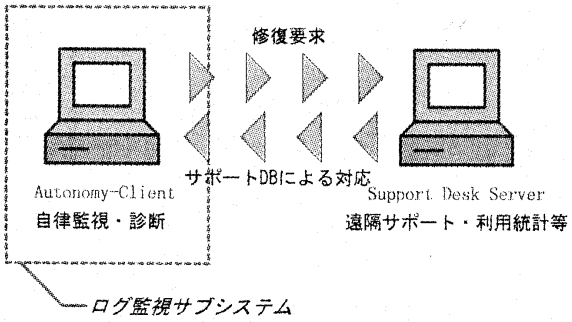

図1：システム全体の概要

2．システムの構築の方針

クライアントとなるAutonomy-Clientが、ログを元にシステムを自律的に監視、エラーなどを自動検出．直接ネットワークに繋がっていない、外部管理者にあたるSupport Desk Serverへ、電子メールという形で修復要求を送信する．

本研究では基本的に、同じLANに繋がっていない、または、セキュリティー上リモートログインの許されない、外部のワークグループの保守管理者へ注意喚起する事を目的としているため、メールで送信という手法を採用している．メールで送信という方法でログ情報を伝達する場合のセキュリティーについては、使用するメーラーの機能に依存している．

3．実現方法

3.1 カスタマイズ及び保守性の容易さ

実現においては、既存のlinux用代表的ログ解析ツールであるswatch、logsurferを踏まえ、より複雑な抽出条件を分かりやすく絞り込める物を目指した．

本プログラムでは、設定ファイルをCSV形式のファイル一つに集約させる事で、既存の表計算ソフトとの親和性を高め、編集を容易にした．これにより、よりグラフィカル、スピーディーにログ抽出条件を設定する事が可能となった．また、表計算ソフトに依存したサポート機能等も活用する事ができる．
以下にlogsurferとの機能の比較を表1にまとめた．

	Logsurfer	*Logeasey*
正規表現を利用した抽出	利用可能	利用可能
複数行に跨る条件	利用可能	利用可能
時間情報の利用	テキストデータの一つとして認識	時間幅による設定が可能
アプリケーションとの連携	特に無し	抽出情報からのグラフ化など
保守性	テキストデータによる直接編集	既存のCSV対応ソフトを利用した編集

表1：logsurferとの機能の比較

3.2 ログ抽出機能の充実

ファイルをタイマーを使って定期的に監視・自動解析、抽出したログをメール送信できる事は勿論、外部プログラムに与えて自動実行させる等の機能を

Log-analysis system using spread sheet as its GUI
Yasutake Fumoto*, Yasutami Chigusa*, Hector Sandval*
Masaaki Hama**, Masahiko Ishimaru**
* Tokyo University of Technology
** Hitachi Software Engineering Co.,Ltd.
chigusa@linux.it.teu.ac.jp
http://www.teu.ac.jp/linux/

持つ．また、ログ情報内の複雑な前後関係を解析、ファイル中の前後関係が一定条件を満たす時のみにアクションさせる等、ファイルを前後する条件を認識する機能を持つ．

図２の画面はWindows･Excelで使用したケースの一例である．既存の表計算ソフトを利用する事で、「オートフィル」や「色分け表示」等、表計算ソフト上の機能を利用でき、また「バルーン機能によるヘルプ」や「リストボックス」等で入力し易くなっている．Linux 用表計算ソフトでもこうした機能の幾つかは利用可能である．

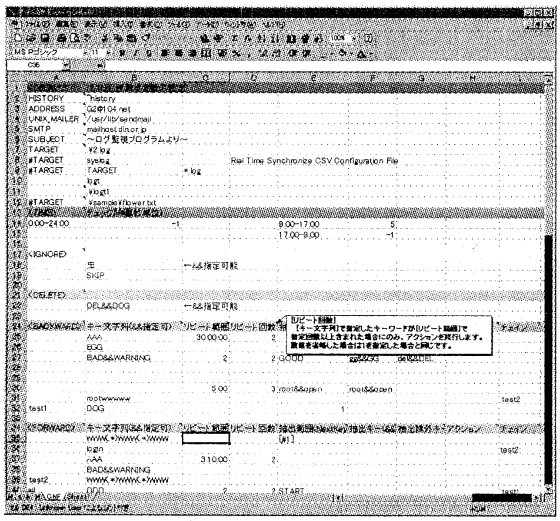

図２：Windows 用 Excel での使用例

３．３ ログ抽出時のアクション

基本的に１行による抽出条件で全ての条件設定が可能である．複雑な条件設定には、それら単　純な条件行を、組み合わせてリンクさせる事でより複雑な条件を設定する事ができる．

他にもログの自動整理機能や、部分削除時の自動バックアップ機構、再起動時のメール重複再送信抑止機構等、数々の機能を持つ．さらに、既存の表計算ソフトウェアに依存したヘルプ機能や、強力なGUIを活用した設定が可能である．

３．４ 正規表現による検索、及び記憶装置

Perl 上で許される殆どの正規表現が、パターンマッチに利用できる．また、一行中５つまでの記憶装置に対応している．

例えば、下記の様な行、

‥PAM_pwdb[28]: (su) session opened‥

を正規表現、

‥PAM_pwdb[(.*)]: (su) session opened‥

で抽出し、28を利用した検索キーを使用するなどといったlogsurfer同様の正規表現機能が簡単に利用できる設定方法が提供されている．

３．５ 時間概念の導入

自動的にログ内に含まれる時間情報を認識可能、ユーザーが単に時間幅を設定するだけで、行毎の時間差を自動的に読みとり、その時間幅に該当する部分だけを抽出する等の機能を持つ．

解析可能なフォーマットとしては、以下の様な時間情報を含む行を認識できる事が確認出来ている．

例）‥‥Apr 31 04:02:39‥‥‥‥‥‥‥‥

‥‥04:02:39 Apr 31‥‥‥‥‥‥‥‥

‥‥1999/08/14 01:10:23‥‥‥‥‥‥

‥‥8/14/1999 01:10:23‥‥‥‥‥‥

３．６ 拡張性

Perl スクリプト言語の採用によりLinux、Windows等OSを問わずに使用する事が可能である．

４．結果とまとめ

本研究ではlogsurferの上位互換にあたるプログラムを目指す事を出発点に、Perlを用い機種を選ばないプログラムを実現させた．また、表計算ソフトと組み合わせる事により、入力のし易さや、見やすさ、データベース性等を追求した．

今回、表計算ソフトと組み合わせる事の利点については入力のし易さ等ばかりが目立つが、表計算ソフトに依存した機能をそのまま使える事で、他にも様々な潜在的な可用性を含む事が考えられる．

例えば、出力結果のデータベース化やグラフ化等が考えられる．Perlによる僅かなソースコードを追加するだけで、出力をCSVデータとして取り出す事も可能になる．ログ抽出からグラフ化までの一連の作業をマクロ化し、それをワンボタンで行う等といった処理も、表計算ソフトによっては容易であろう．