3S-06

Logeasy による遠隔管理対応ログ監視サーバの開発

田島賢　麓泰丈　金子英生　千種康民
東京工科大学工学部 千種研究室

1 はじめに

Linux による C/S システムの管理作業において，サーバの保守／運用を効果的に行うために，OS，またはサーバソフトウェアの記録(ログ)を利用することは一般的に行われている．本システムは，ログ管理における負担軽減を目的として考案され，作業の自動化による即時性と保守性の向上，GUI の提供による作業能率の向上を目指し，外部環境からの遠隔管理にも対応している．

2 概要

本システムの全体像は図1に示す通りである．管理対象ネットワーク内のシステムログは，サーバとなるホストに集約され(「2.2 ログサーバの設計と構築」参照)，各ホストごとのログを Logeasy と呼ばれる常駐型プログラムが監視する(「2.1 ログ監視エージェント-Logeasy-について」参照)．動作設定や制御は，WWW サーバを介して WWW ブラウザで行い，外部環境からの管理が可能である(「2.3 WWW ブラウザからの制御」参照)．また，設定によりログ内の特定文字列に関連する URL を自動に検索させることもでき，作業を円滑に行うための機能として実装されている(「2.4 ログ内文字列の自動 URL 検索要求」参照)．図2はプログラム相関図である．

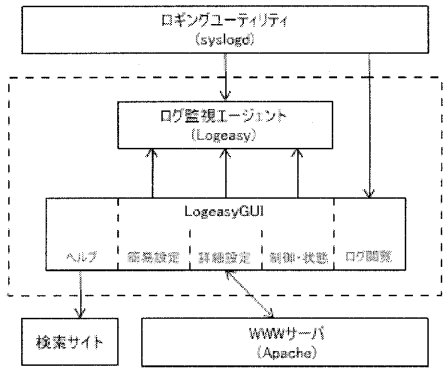

図2:プログラム相関図

2.1 ログ監視エージェント-Logeasy-について

CSV 形式の設定ファイルに従い，ログ監視と検出に伴う動作を自動で行う自律型のプログラムである．主な機能は図3に示す通りで，複数行にまたがる条件検索や，正規表現が使用可能であるなど，テキスト形式のファイルに対する文字列検索に効果的な機能を持っている．バックグランドプロセスとして動作させることが基本であり，WWW ブラウザからの操作では，CGI の外部コマンドとして実行し，WWW サーバと同権限で動作する．

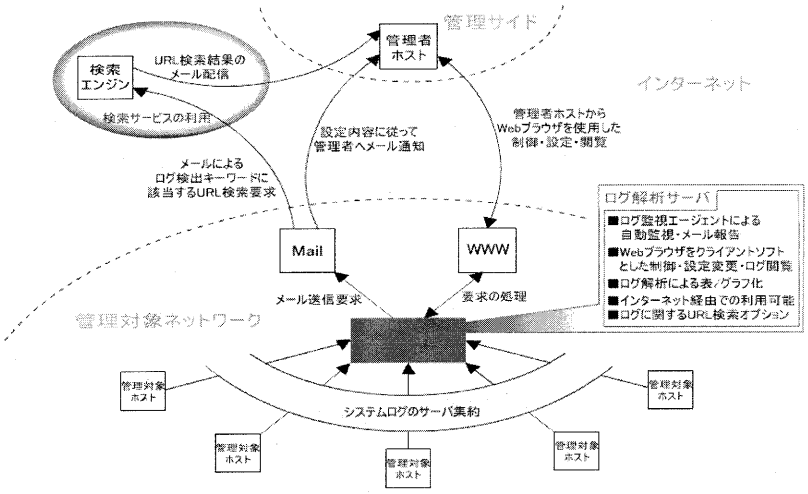

図1:システム全体像

Implementation of Remote PC Maintainance System using Logeasy
Masaru Tajima, Yasutake Fumoto, Hideo Kaneko, Yasutami Chigusa
Tokyo University of Technology
chigusa@linux.it.teu.ac.jp http://www.teu.ac.jp/linux/

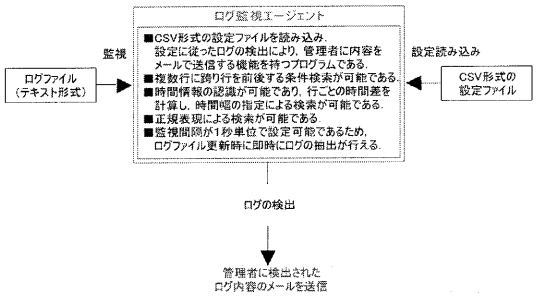

図 3：Logeasy 概要

2.2 ログサーバの設計と構築

システムロギングとカーネルメッセージの確保という2つの機能を持つユーティリティソフトウェアに syslogd がある．syslogd はネットワークをサポートしており，syslogd が稼動しているホストでのメッセージを，別の syslogd が稼動しているホストへ転送し，ファイルに記録する機能を有している．この機能を有効にすることで，ネットワーク内の全ホストのログを 1 台のホストに集約し，ログサーバとして動作させる．

2.3 WWW ブラウザからの制御

WWW サーバである Apache が提供する機能を使用する．まず，アクセスには認証を必要とし，認証には Apache の HTTP 認証であるホストベース認証，パスワードベース認証を組み合わせて使用する．パスワードベース認証には BASIC 認証を用いており，パスワードファイルの生成には htpasswd コマンドを使用したハッシュ関数を使用している．また，プロキシサーバ経由や DHCP クライアントからのアクセスを，CGI でのフィルタを使用して許可しないことでもセキュリティ面の向上を図る．GUI の主な操作は CGI により処理され，図4に示すように，各機能ごとに項目分けされている．項目には下記の5つがある．

- ［標準設定］－簡易な動作設定(図4)
- ［詳細設定］－Logeasy が使用する CSV 形式の設定ファイルをテーブルで編集
- ［動作設定・状況］－Logeasy の制御と動作状況を稼働時間や状態などの情報から確認
- ［ログ閲覧］－ログサーバに集約されるログから検索条件に該当したログを表示
- ［ホーム］－初期画面．操作方法などのヘルプドキュメントやその他の情報

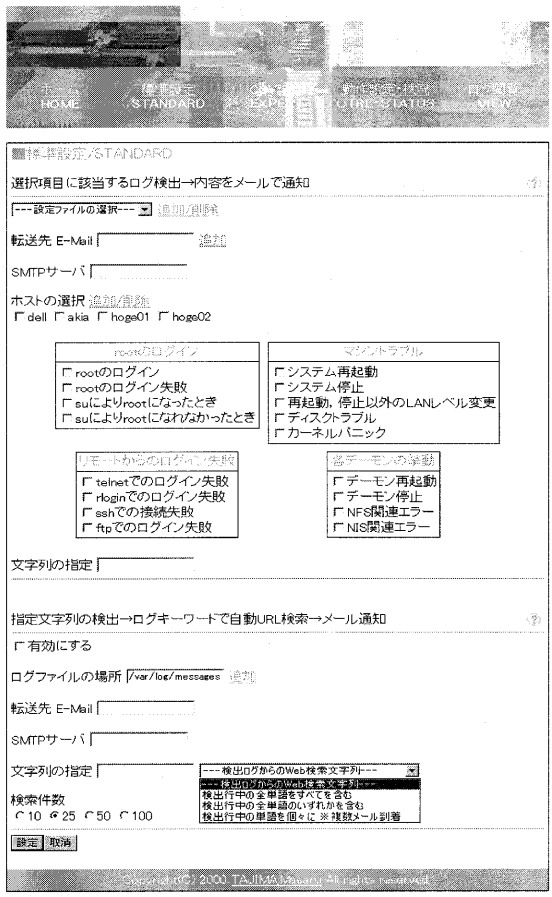

図4：標準設定画面（サンプル）

2.4 ログ内文字列の自動 URL 検索要求

これは，管理者の情報収集に関する負担軽減を目的とした機能である．文字列を指定し，その文字列がログから検出された際に，自動でログ内のプログラム名，メッセージなどに含まれる単語に関連する URL 検索要求を行う．この機能は，インターネットサーチエンジンである goo のメールによる検索サービスを利用している．検索結果は指定する管理者のメールアドレスへ goo から返信される．

3 まとめ

システム全体の現状は試用段階にある．主な課題として，WWW サーバの負荷低減を目的とした CGI プログラムの改良や Logeasy の高速化，WWW サーバや syslogd のセキュリティ強化などが挙げられる．

4 参考文献

[1] 麓，千種，他：「表計算ソフトウェアを GUI とするログ解析システム logeasy」，第 60 回情報処理学会全国大会 3，pp. 537－538 (2000)