内部統制のためのログ管理システム

友野 敬大† 鈴木 秀平† 上原 稔†
東洋大学工学部情報工学科‡

1. はじめに

内部統制とは、一般に企業などの内部において、違法行為や不正、ミスやエラーなどが行われることなく、組織が健全かつ有効・効率的に運営されるよう各業務で所定の基準や手続きを定め、それに基づいて管理・監視・保証を行うことである。そのための一連の仕組みを内部統制システムという。内部統制システムの実現には認証、認可、監査の 3 つの要素が必要である。本研究で注目している監査は、定義された評価基準に基づき、精密な検査をそれぞれのシステムに対して実施し、評価することである。プログラムの改ざんや不正使用があった場合、認証および認可のログも含まれるので、ログ監査が適切に行われていない内部統制システムは脆弱であるともいえる。言い換えれば、ログの監査は内部統制システムにおいて、要となる。しかし、ログは随時出力されるため、膨大な容量が必要となるうえ、今日では内部統制システムを構築するのには多大なコストが必要となる。

Linux の Syslog、windows のイベントログなど、OS にはもともとログを管理する機能を搭載しているものもある。ただ、ある一定期間を過ぎると古いログは上書きされてしまうので、参照することができない。そこで、本研究では、端末から収集したこれらのファイルを、効率的に長期間保存しておき、必要な情報を抽出するために管理するシステムを提案し、開発する。

2. 関連研究

(1)NTsyslog [1]

NTSyslog は、Windows のイベントログを Syslog に変換して、 Syslog サーバに転送するソフトウェアのことである。SourceForge.net NTSyslog Project にて開発された。

A Log Management System for Internal Control
†Akihiro Tomono, Shuhei Suzuki, Minoru Uehara
‡Dept. of Information and Computer Sciences, Toyo Univ.

(2)Syslog-ng [2]

Syslog-ng とは、フリーの Syslog ソフトウェアで、さまざまな機能のサポートやセキュリティ面が考慮された。これにより、アプリケーション名や受信したログの内容に応じて、ログの出力先を指定でき、効率的にログ検索が行える。

(3)Logrotate

一定期間あるいは一定サイズなどの指定されたタイミングでログファイルを切り分け、ログのローテーションを行う。

(4)VLSD [3]

教室や会社の遊休資源（HDD の空き容量）を連携し、1 つの大きな仮想ストレージを構築して用いる。これにより高価なストレージの必要性がなくなる。このような分散型ストレージは、HDD 代のみとなるので集中型の費用と比較すると、そのコストを大幅にカットすることができる。

3. システム概要

本研究では、クライアントマシン（Linux と Windows XP）とサーバマシン(Linux)を作成し、クライアントマシンでのログをサーバマシンに送り、収集する。Linux から Linux にログを送る際は Syslog-ng を用いることによって実現する。Windows から Linux に送る際は、NTsyslog を用いてイベントログを Syslog 形式に変換し、サーバに転送することで、規格を統一して管理の一元化を目指す。現段階では、収集対象は、Syslog、イベントログ、Apache ログ、Tomcat ログである。

ログ収集用サーバに集められたログは、Logrotate によってローテーションを行い、比較的古いものから Near-Line ストレージに、それ以上に古いものを Off-Line ストレージに保存する。システム構成図は図 1 に示す。

また、サーバマシンの Syslog から必要な情報を取得するために、ログ検索を行えるようにする。例えば、次のような検索を行う。

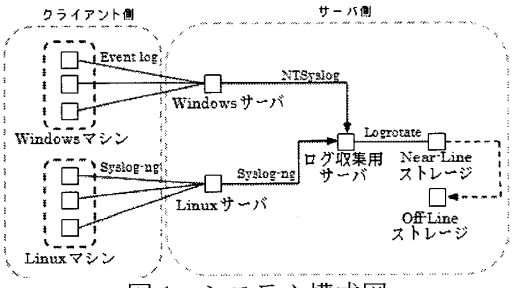

図1　システム構成図

・ユーザのコンピュータの利用時間の集計
・1台のコンピュータの利用時間の集計
・アプリケーションの同時実行数の集計
・アプリケーションの利用時間の集計

これらは Syslog-ng の設定といくつかのプログラムを組み合わせることにより実現させる。

4. 設計

(1) 収集および管理

Windows マシンは NTsyslog、Linux マシンは Syslog-ng を用いてログ転送を行う。それぞれ同 OS のサーバに転送したのち、規格を統一してログ収集サーバに転送する。ログの種類を表すディレクトリはあらかじめ用意しておき、年月に関しては cron で毎日作成する。また、そこに日付ごとに保存する。ログを保存するためのディレクトリは図2のような階層を持つ。

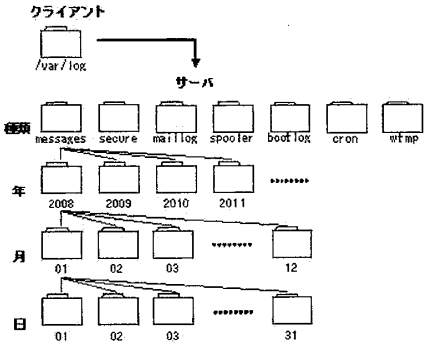

図2　サーバ側ディレクトリ

(2) 参照および検索

保存したログは個々に分かれているが、それらを 1 つのログファイルかのように参照できる必要がある。例えば、messages ディレクトリ以下に保存されているログファイルを全て読み込み、コマンドライン上に古いものから順番に表示させる。また必要によって日付を指定し、その部分だけを表示させるシェルコマンドも設ける。加えて、表示したものから任意の文字列だけを抽出して表示しなおすシェルコマンドを実装する。

表示したものの中から、前述したような情報を得るためにプログラムを作成する。

5. 評価

実験中に発生したログを日付によって分割し、それに対してログを連結して表示させるスクリプトを実行した。全体のログを表示させたものと、引数を指定し Messages の 1 月分のログのみを表示させてもの、キーワード検索を実行したものの表示時間の結果を表 1 に示す。キーワードは“error”を指定した。

表1　logcat 実行時間

	real[s]	user[s]	sys[s]
全体	5.808	0.050	3.146
1月分	0.370	0.009	0.241
キーワード	0.281	0.001	0.246

30 日間保存したログの総量はおよそ 6,530KB で 1 日当たりの平均はおよそ 218KB、最大のサイズは 1,632KB だった。

6. 今後のまとめ

VLSD（現段階では約 70TB）を利用することによりログの膨大なサイズ問題は解決し、理論上、長期間の保存が可能になる。
また、ログ検索も引数を用いた検索を行うことで時間短縮に成功した。

現段階では、ユーザのログイン時間の検索は、正式にログイン・ログアウトしている場合のみ実行可能である。今後、予期せぬ down にも対応する必要がある。同時に、他の検索も実装する。

また、ログの収集対象を増やすことで実用性を高める。

参考文献

[1]Windows イベントログを SYSLOG で管理する
http://pooh.gr.jp/item-161.html
[2] 安全性の高いログ・サーバへの乗り換えのススメ
http://www.atmarkit.co.jp/fsecurity/rensai/unix_sec09/unix_sec01.html
[3] チャイエリアント, 上原稔, 森秀樹 "PC 教室のための仮想的大規模ストレージの構築", マルチメディア、分散、協調とモーバイル(DICOMO 2007)シンポジウム論文集, pp.617-622, (2007.7.4-6)