ライセンス管理を目的としたログ活用手法の提案

友野　敬大†　　上原　稔††　　島田　裕次††

東洋大学大学院工学研究科情報システム専攻†　　東洋大学総合情報学部総合情報学科††

1. はじめに

近年，米国企業に留まらず，日本企業でも不祥事が多発し，内部統制の必要性が急速に高まっている．企業では，コンプライアンス確保のために，内部統制を実現するためのツールを選択し，活用する必要がある．しかし，現在の普及品はどれも高価であり，導入コストだけではなくデータ量に応じた運用コストについても考慮しなければならない．

実際のログ（以下，生ログとする）は，何も加工されていないため，その証拠能力は比較的高いものと考えられるが，ログはシステムの規模に比例して，確実に保存領域を圧迫していく．我々はOSの機能を利用し，半永久的にログを保存可能なシステムを開発した．VLSDを用いて容量を確保するので，NASやSANなどといったストレージシステムを導入しなくても，低コストで大容量のストレージを利用できる．ログは，システムの最終防衛的な意味合いをもつとともに，さらに企業改善につながる情報を多分に含んでいると考えられる．これらの情報は，的確に利用すれば企業に利益をもたらす．また，業務上不必要なソフトウェアやユーザの操作を把握することによって，内部統制を実現する上でのリスク回避にも対応できる．

一方，今日では，企業や学校などの組織において，ソフトウェアを購入したにも関わらず，利用されていない場合が少なからずある．高価なソフトウェアのライセンスが正しく利用されていない場合，それは無駄なコストと言える．企業改善をする上で，遊休ライセンスを起因とする無駄なコストは削減すべきである．また，インターネットを通じて不正入手したソフトウェアや違法コピーなど，ソフトウェアの管理責任についても強く問われている．そこで，ログからソフトウェアの利用率を導出し，有効にライセンスが活用されているか，不正なソフトウェアが利用されていないかどうかを確認し，適切に管理する方法についても提案する．

2. 関連研究

2.1 VLSD

VLSD(Virtual Large Scale Disk)とは、Javaによるソフトウェア RAID と NBD の実装を含む大規模ストレージ構築のためのツールキットである。VLSDは100% pure Javaであり、Javaが動作するプラットフォームの上ならVLSDも動作する。NBD を用いることで、ファイルシステムに依存しないディスクレベル分散ストレージの実現が可能となる。これにより、高価なストレージの必要性がなくなる。

暗号化や書き込み禁止ディスクを実現するクラスを持ち、これらを組み合わせることで、不正アクセスなどのセキュリティの問題を解決する。

2.2 ログ管理システム

内部統制を実現するのにログ管理は重要であることは、前述のとおりであるが、容量の問題やコストの問題は無視できない。それらの問題を解決するために、我々はVLSD を用いて、半永久的にログを保存可能なシステムの開発に成功した。このシステムは、OS にあらかじめ備わっている機能を用いて実装される。排出されるログを上書きするのではなく、ストレージに保存し続ける。本大学では、常時稼働しているサーバが25台あるので、それらから遊休資源を確保し、ストレージを構築する。

3. ライセンス管理を目的としたログ活用法

3.1 システム概要

ライセンス管理方法として，ユーザが業務時間中にどの程度，どのようなアプリケーションを使用したかという観点が挙げられる．すなわち，アプリケーションを利用した時間を求めれば，実際に必要なものなのかを判断する材料になり得る．例えば，ある一定期間使用されてないアプリケーションのライセンスはもちろん無駄と言えるが，利用時間がごくわずかなものに関して言えば，操作するユーザおよびインストールするマシンを限定し，統一することで遊休ライセンスを解消できる．

また，自動的にログを収集するエージェントをクライアントマシンに配置することで，ユーザに余計な負担をかけずにログを収集する．自動収集エージェント（以降，エージェントとする）は，業務に関係のないアプリケーションの使用や不審な操作も検出する．これにより，組織におけるインストールされているアプリケーションの状況を把握することで，関係する法的なリスクを回避することができる．

3.2 自動収集エージェント

エージェントは，アプリケーションがアクティブになったときに，そのウィンドウハンドルを取得する．さらに，取得したウィンドウハンドルから，そのプロセスIDやプロセス名などの情報を取得する．エージェントは，そのアプリケーションがアクティブである間，ウィンドウハンドルを保持し続け，時間を測定する．そして，他のウィンドウハンドルがアクティブになったときにログを書き出す．書き込む際，日付，ユーザ名及びホスト名などを取得する．ログの書式を図1に示す。

```
"Data","PID","Process","User","Host","Title","Time"
```

図1　書き出されるログの書式

3.3 データベース

エージェントによって書き出されたログをデータベースに格納し，管理および活用する．データベースには

The Proposal for Exploit Log Aiming License Management

Akihiro Tomono, Minoru Uehara, Yuji Shimada

† Dept. of Open Information Systems, Toyo Univ.

†† Dept. of Information Sciences & Arts, Toyo Univ.

MySQL を用いる．格納されたログの情報に対して検索を行い，プロセス ID が一致するものの利用時間の和をとる．データベースの構造を図 2 に示す。

Field	Type	Null	Key	Default	Extra
lid	int(10) unsigned	NO	PRI	NULL	auto_increment
date	char(32)	NO			
ps	varchar(32)	NO			
psn	mediumtext	NO			
usr	char(64)	NO			
host	char(64)	NO			
app	mediumtext	NO			
time	int(10) unsigned	NO			

図 2　データベースの構造

4. 考察

アクティブなウィンドウが切り替わるたびにログが出力されるため，その量は膨大なものになると予想される．実際に運用した場合を考える．エージェントを起動したまま作業をした結果，ホスト 1 台あたり 8 時間でおよそ 300KB，ログが 1,300 行となった．これをホスト 512 台としたとき，ログのサイズが 154MB 必要になる．行数はおよそ 67 万行となり，当然データベースで処理する行数もそれに比例して多くなる．そのため，適切なログ保存用のストレージを構築する必要がある．前述の通り，VLSD を用いてこの問題を解決する．サーバから遊休資源を確保し，ストレージを構築するが，その規模についても再考しなければならない．関連研究で挙げたログ管理システムでは，本大学で常時稼働しているサーバ 25 台から遊休資源を確保することを考えている．実際には，中小企業において常時稼働しているサーバ台数はそこまで多くはない．仮に，常時稼働しているサーバが 5 台だとする．それぞれ 500GB ずつ遊休資源を収集して，RAID6 でストレージを構築する．これにより 1.5TB の要領を確保できる．ログの必要領域から算出すると，充分である．

さらに，ライセンス料の低減について考える．我々は，研究用に VMware Workstation を導入している．1 ライセンスあたりおよそ 2.5 万円なので，遊休ライセンスが数本あれば 10 数万円近くのコストを無駄にしていることになる．研究室だけではなく，企業においても同様なことが言える．高価なアプリケーションであればあるほど，早急に対応が必要である．また，大学におけるキャンパスアグリーメントでは大学全体で一括してライセンス契約をするので，リプレイスなどの際にライセンス数をその都度見直さなければ，利用していないライセンスについても支払が発生しさらに大きな単位の無駄を生じることになる．本システムでは，Windows API によって得られる情報を利用することによって実現されるので，そのコストは大きく削減できると考える．

図 3 中に示されているプロセス ID が”-1”になっているものは，何もアクティブではない状態のときに見られる．すなわち，スクリーンセーバやユーザロックである時間を測定している．このとき，プロセス名は取得できないので，意図的に”0”を値として代入している．また，ユーザ Yasu において，プロセス名が取得できていないアプリケーションがある．生ログを調査した結果，これは Eclipse であることがわかった．Eclipse とは，IBM によって開発された統合開発環境(IDE)の 1 つである．このように，アプリケーション側でプロダクト名が設定されていない場合は，その値は NULL となり，参照することができない．この場合は，プロセス ID からアプリケーション名を得ることができる．

lid	ps	usr	psn	SUM(time)
15	<3256>	uehara_minoru	VMware Workstation	4530
16	<2732>	uehara_minoru	2007 Microsoft Office system	2873
61	<6048>	uehara_minoru	Windows(R) Internet Explorer	1499
18	<-1>	uehara_minoru	0	1070
2	<4076>	uehara_minoru	Microsoft(R) Windows(R) Operating System	991
432	<6036>	uehara_minoru	Google Chrome	295
421	<1788>	uehara_minoru	Tera Term Pro	44
4	<4476>	uehara_minoru	APPGet	35
1	<3052>	uehara_minoru	Sleipnir	21
294	<2492>	uehara_minoru	Windows Internet Explorer	18
114	<456>	uehara_minoru	Winamp	3
196	<5332>	uehara_minoru	Trend Micro Internet Security	3
483	<2784>	Yasu	Microsoft Office 2003	9499
757	<2744>	Yasu		2709
471	<1328>	Yasu	Microsoft(R) Windows(R) Operating System	474
472	<-1>	Yasu	0	184
534	<3964>	Yasu	Trend Micro Internet Security	2
768	<460>	Yasu	BOINC client	2

図 3　収集したログの一部

5. 今後の課題

前述の通り，エージェントによって取得できない情報がいくつかあることが判明した．エージェントは，FileVersionInfo の ProductName をプロセス名として参照している．FileVersionInfo が保持する情報にはこれ以外にも，内部名やオリジナルファイル名など，判別に利用できる可能性があるものが多くある．記録するフィールドを再考し，ログの書式を検討する必要がある．

また、現段階では，データベースは必要なときに構築する仕様になっている．エージェントは 1 つの区切りでログを書き出すので，それをトリガとしてデータベースを構築する方法が考えられる．必要保存領域は多くなるが，管理者の負担を減らすことができる．リアルタイムでログとデータベースを同期させる必要があるのかについて検討する必要があると考える．

6. まとめ

本論文では，ログからクライアントのアプリケーション利用状況を読み出し，ライセンス管理に役立てる提案をした．企業などの組織において，ライセンス違反や不正入手および違法コピーが発覚した場合，法的な処罰を受けるだけでなく，社会的信頼は大きく損なわれるのは言うまでもない．ライセンス管理に留まらず，クライアント PC の状況を把握するのは，これから，より一層重要視されると考えられる．

参考文献

1)上原 稔　“教育環境における仮想大規模ストレージのためのツールキット”，マルチメディア通信と分散処理ワークショップ，pp.205-210, 2006 年 11 月

2)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，協調とモバイル（DICOMO2007）シンポジウム論文集，pp.617-622，2007 年 7 月

3)上原 稔　“仮想大規模ストレージにおけるセキュリティ”，情報処理学会研究報告書，pp.61-66，2007 年 11 月

4)Akihiro Tomono, Minoru Uehara, Makoto Murakami, Motoi Yamagiwa: "A Log Management System for Internal Control", In Proc. of 2009 International Conference on Network-Based Information Systems(NBiS2009), pp.432-439, (2009.8.19-21)