M-052

フィンガプリントを用いた信頼できるログの転送方式の提案
A Proposal for Trusted Log Transferring by Finger Print

友野 敬大† 上原 稔† 島田 裕次†
AKIHIRO TOMONO MINORU UEHARA YUJI SHIMADA

1. はじめに

近年、米国企業に留まらず、日本企業の不祥事が公になり、内部統制の必要性は急速に高まっている。本論では、内部統制を実現する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。

企業はコンプライアンスに基づき、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くてはならない。実際のログ（生ログ）は、何も加工されていないため、その証拠能力は高いと言えるが、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。

そこで、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せずとも、低コストで大容量のストレージを利用できる。このシステムでは、一部分においてログを保証しているが、それだけではディジタルフォレンジックを考えると十分ではないと言える。そこでディジタルフォレンジックに対応するべく、中継サーバにおける悪意ある管理者および第三者によるログの改ざん、転送時のログの欠損を検出し、信頼できるログ転送方式を提案する。

2 章で本研究の関連研究、3 章で転送方式の提案、4 章でシステムの評価、5 章でまとめと今後の課題について言及する。

2. 関連研究

2.1 ディジタルフォレンジック

ディジタルフォレンジックとは「インシデント・レスポンスや的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」と定義されている[1]。

ディジタルデータの法的証拠能力という問題を考える。日本の法律では、いまだに物的証拠のみ証拠能力を持つとされている。そのため、コンピュータを証拠として採用するときには、保存されているデータではなく、データを格納している媒体すなわち HDD などそのものが必要になる。

ディジタルデータのような電磁的記録単体では証拠として認められていない。そのため、電磁的記録を出力した書類などを法廷に提出しなければならないが、それらを作成するまでの過程で改変される可能性があるので、その真実性に疑問がもたれることになる。実際には、ディジタルデータと関連する物的証拠や証言を組み合わせて、法廷で用いる。通常フォレンジック調査では、対象 HDD から 100% 物理コピーをしたのち、ハッシュ値を残すなどしてその証拠性を保つ必要がある。

2.2 VLSD

VLSD 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[2]。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[3]。

2.3 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[4]。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. ネットワーク間におけるログの保証

ディジタルフォレンジックにおいて重要なのは、ログの整合性である。ログを転送する際、あるいは、一時的にログを保管するサーバで改ざんが行われてはならない。万が一、これがあった場合に、それを検出できる用意をしておく必要がある。ディジタルフォレンジックにおけるログは、その証拠性が問われる。実際にログが法廷において有効であるかどうかを判断できなければならないからである。

[4]のシステムでは、一部分においてこれを実装しているが、転送するたびに検証する必要があるので、改良する。いくつかのモデル例を挙げ、その実用性を考える。ただし、今回のログ転送において着目するのは、中継サーバにおける悪意ある管理者や第三者を想定するものである。クライアントから排出されるログは改ざんやパケット損失していないものとして考える。

(a) サーバのみへ転送

まず、基本的な形としてクライアントからログが発生した段階で、そのログのハッシュを作成する。これをストレージでログと一緒に保管することで、途中に通過するサーバで行われるログの改ざんなどを検出できる。図 1 に示す。

†東洋大学 Toyo University

しかし、これでは中継するサーバが複数台ある場合、そのどこかで改ざんがあったのか知ることはできない。

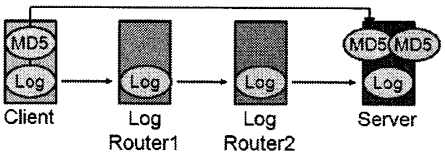

図 1　ハッシュファイルの流れ-モデル(a)

(b) 隣接するルータへの転送

次に、それぞれのサーバでログファイルからハッシュを作成する場合を考える。一見すべてのマシン間でログが保証されるように思えるが、もし LogRouter1 でログの改ざんが行われた場合、改ざんされたログとハッシュが転送されると、LogRouter2 以降ではこれを知るすべがない。

(c) 上流へのブロードキャスト

(a)、(b)ともに重大な欠陥がある。これらを補う方法を考えなければならない。クライアントからのログが正しいものだと仮定すると、このハッシュを基準にするのが確実だと言える。途中で経過するサーバにもそれぞれハッシュファイルを保管することを考える。それぞれのサーバで、クライアントマシンのハッシュと比較することで、改ざんを検出する。

(d) 中間ハッシュを含めてサーバへ転送

LogRouter におけるハッシュを減らしたものが(d)である。クライアントマシンのハッシュと各々を比較すればよいのだから、最終的に 1 つの場所にまとめられればよい。容量問題を解決した VLSD に保存していくのが適切である。ログファイルと一緒にハッシュも半永久的に保存できる。図 2 に示す。まず、クライアントマシンのハッシュと VLSD に転送されたログのハッシュを比較する。一致した場合は、経路途中で改ざんがなかったことを表す。すなわち、これはディジタルフォレンジックに対応するログであると言える。これが一致しない場合は、クライアントマシンと LogRouter1、そして LogRouter2 とを順番に比較して、改ざんされた場所を特定する。

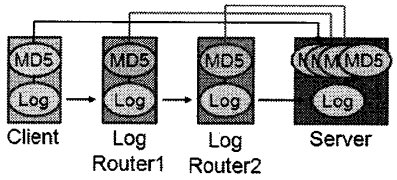

図 2　ハッシュファイルの流れ-モデル(d)

4. 評価

本論第 4 節における考察を行う。ログに対して MD5 によるハッシュを作成すると 128 ビットすなわち 16 文字の英数字の羅列が出力される。Syslog が出力するログの 1 つのレコードがおよそ 100 バイトとするとかなり少ない。ここで、レコード毎にハッシュを取った場合を考える。1 つのログファイルに対して実行した場合とレコード毎に実行した場合とでは大きく違う。記録されたログのレコードの数だけハッシュを計算する必要がある。レコード毎にハッシュを取れば、ファイル毎のものに比べ、精度が増す。改ざんされたログのレコードだけ、あるいはその複数行だけ検出することができる。よりディジタルフォレンジックに耐えうる形となる。

MD5 によるハッシュは、その脆弱性が発見されている。異なるドキュメントから同一のハッシュ値が求められるというものである。すなわち、ハッシュの一意性が失われたことになる。しかし、ログとしての意味を持ち、かつハッシュ値を同じにするのは難しいと考える。例えば、ある特定のログのレコードを削除する。その分、意味を持ち、正当なレコードを追加する必要があるからである。また、ユーザ名や実行時間などレコードの一部分のみの改変は、前述と同様に難しい。ログのレコードごとのハッシュ値を求めれば、改ざんしにくくなるログが得られる。

クライアントマシンからのログを転送する際、コネクション数にも注意するべきである。コネクション数はクライアントマシンの数に比例する。もしこれが膨大で転送に支障があり、ログが正常に転送されていないと判断されると、改ざんと同様に有効性はなくなると考えられる。

例えば、1Mbps の回線でログを転送した場合、1 日平均のログを 220KB とすると、1.76 秒かかる。1 秒間に 1 万トランザクション処理できると仮定すると、およそ 5,600 クライアントに対応できる計算になる。本大学の PC 教室のクライアントマシンは、500 台なので、大学の PC 教室全体や中小規模の企業でも十分に間に合うと考えられる。

5. まとめ

本論文では、我々が開発したログ管理システムにおけるネットワーク間のログの保証方法の提案をした。法廷で用いられるログは、改ざんされていないことが必須である。そのため、ログを保証する機能の実装の有無は、必然的に問われるだろう。ネットワーク間のログの保証は、ログの整合性につながる。ログの整合性を証明することは、ディジタルフォレンジックにおいて重要な要素である。前述のとおり、ハッシュを用いれば、ネットワーク間のログの信頼性は保証される。これにより、ディジタルフォレンジックに対応するログを保存することが可能になる。

謝辞

本研究は科研費基盤(C)「PC グリッドによる高信頼・高効率な分散仮想ストレージの研究(19500066)」により援助されています。

参考文献

[1] 辻井 重男 他, “ディジタルフォレンジック事典”, 日科技連, pp.33-36, 2006 年 12 月
[2] 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
[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.T, Minoru.U, : ”A Log Management System for Internal Control”, to Appear