社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (32)
2009－CSEC－ 44 (32)
2009／3／6

組織的不正を想定したログ情報の改ざん防止システム

加藤 慧† 中山心太† 荒川淳平†† 三島久典††† 吉浦 裕†

†電気通信大学大学院 電気通信学研究科 〒182-8585 東京都調布市調布ヶ丘 1-5-1

††株式会社インフォクラフト 〒182-8585 東京都調布市調布ヶ丘 1-5-1 国立大学法人電気通信大学
共同研究センター402 号室内

†††日立製作所システム開発研究所 〒212-8567 神奈川県川崎市幸区鹿島田 890

E-mail: †k_kato@edu.hc.uec.ac.jp, †shinta@edu.hc.uec.ac.jp, ††arakawa@infocraft.co.jp,
†††hisanori.mishima.xd@hitachi.com, †yoshiura@hc.uec.ac.jp

あらまし 従来のログシステムにおける不正の防止は，システム管理者への信頼を前提としていた．しかし近年増加している企業等の組織的不正の場合，システム管理者は必ずしも信頼できない．そこで組織的不正の存在下でログ情報の改ざんを防止するために，(1)多数の社員 PC にログデータを配信し，ログデータが改ざんされた場合に，不正の存在が社員に知れ渡る仕組み，(2)複数の社員 PC を同時に攻撃することができず，攻撃に時間を要する仕組みから成るログ改ざん防止システムを提案する．

キーワード ログシステム，内部不正，内部告発

Preventing log information from system administrator's alteration

Kei KATO† Shinta NAKAYAMA† Jumpei ARAKAWA††
Hisanori MISHIMA††† Hiroshi YOSHIURA†

† Graduate School of Electro Communications, The University of Electro-Communications,
1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585 Japan

†† Infocraft, Inc. 402 Cooperate Research Center, The University of Electro-Communications,
1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585 Japan

††† System Development Lab. Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan

Abstract We propose a log storage system that can protect logs from the system administrator's alteration. The system stores logs in the company member's PCs so that the log alteration would be known to many members who thus would come to distrust the manager and might disclose the alteration to the public. The system also disenables the concurrent attacks to multiple PCs so that it takes long time to alter logs in all PCs consistently.

Keywords log system, internal crime, disclosure by internal member

1. はじめに

近年の相次ぐ企業の不祥事を受けて，内部統制を求める JSOX 法の施行が開始された．内部統制を推し進めるにあたっては，企業の透明性・遵法性を検証するためのログ情報が必要不可欠である．ここでのログ情報とは，PC の利用状況や操作内容，データ通信の記録ばかりでなく，会計処理の経理データ等も含む．

企業の透明性・遵法性を検証するためには，必要なログ情報を漏れなく記録した上で，改ざんを防止し真正性を維持することが重要である．しかし従来のログシステムでは，改ざんを検知することができても，改ざん自体を防止することは困難である．またログ情報の真正性はログシステムの管理者に託されているため，システム管理者を含む組織的不正に対しては脆弱である．そのため，組織的不正

の存在下で，ログ情報の改ざんおよび消去を防止する取り組みが必要である．

本研究では，ログ情報の真正性を，システム管理者ばかりでなく多数の一般社員が担保することによって，組織的不正に耐えるログ情報の改ざん防止システムを提案する．

2. 従来技術

2.1 ログシステム

ログシステムとは，ロガーシステムによるログデータの取得およびログストレージシステムによるログデータの保存・管理を行うシステムのことである（図 1）．この二つのサブシステムの設置のされ方により，ログシステムはネットワーク型とスタンドアロン型の二つのタイプに分類される[1].

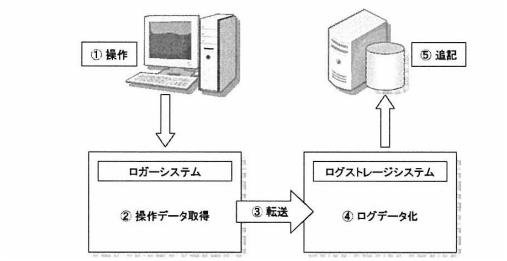

図 1　ログシステム

(1) ネットワーク型ログシステム

ログストレージシステムがサーバに設置されたログシステムのことを，ネットワーク型ログシステムと呼ぶ．ユーザが利用する PC からログデータを取得し，サーバのログストレージシステムと通信することで蓄積する．

このシステムでは，ログデータに対する権限がログストレージシステムの設置されたサーバの管理者に集中するため，内部不正を防ぐことが困難である．またログデータがサーバに集中するため，物理的攻撃に弱い．

(2) スタンドアロン型ログシステム

ユーザが利用する PC 内にロガーシステムとログストレージシステムの両方を設置したログシステムのことを，スタンドアロン型ログシステムと呼ぶ．

このシステムでは，ユーザが利用する PC はサーバに比べてセキュリティ面で脆弱であることが多い点や，サーバの監視を受けていないためユーザが不正を行いやすい点で，ログデータへの攻撃に対し脆弱である．

2.2 ログ情報保護技術

(1) デジタル署名

デジタル署名を用いることで，ログデータへの改ざん攻撃を検知することが可能となり，不正抑止効果を高めることができる．しかし，本質的には攻撃そのものを防ぐことはできない．すなわち，攻撃によって損失したログデータを復元することは困難である．

(2) WORM

WORM（Write Once Read Many）とは，一度だけ書き込むことができ，変更や消去ができない記憶メディアのことである．WORM の性質はデジタルフォレンジックの視点から有用性が高いため，WORM を利用したストレージシステムなどが開発されている．

しかし WORM を読み書きする装置が高価であるため，多数の PC に設置することは非現実的である．結果として管理者による集中的な管理がなされるため，装置の取替えや破壊といった攻撃が行える可能性がある．

(3) データセンター

顧客のデータを預かり監視・保守・運用などのサービスを提供する施設である．データセンターを利用することでデータが遠隔地に保管されるため，物理的攻撃に対して強い．ところが，契約した企業の依頼に対してデータを守ることが難しいという問題がある．例として，不正を企てている企業の役員がデータセンターに指示することによって，ログデータの改ざん等の攻撃が実行される可能性がある．顧客の指示に従わないデータセンターがビジネスとして成立するかは疑問である．

(4) ファイル分散保存システム

デジタルフォレンジックを目的としたファイル分散保存システムが提案されている[2][3]．このシステムでは，ヒステリシス署名を多数のシステム参加 PC 間で交差させることでデータの改ざんを困難にしており，また部分的なデータの破損に対しても，他の参加 PC からデータを補完することで署名の検証が行える．ただし前提として，管理者不在の小規模ネットワーク内での利用を想定してお

り，またいずれのユーザも他の参加 PC に対して管理者権限を持たないものとしている．そのため，ネットワーク内の全ての PC に対して管理者権限を持つシステム管理者による攻撃を想定していない．

3. 提案システムの前提と目標

3.1 提案システム概要

前章で指摘した問題は，ログデータの管理に際してシステム管理者が強大な権限を持つことに起因している．この問題を解消するために，ログデータの真正性をシステム管理者ばかりでなく多数の一般社員が担保することが可能な方式を提案する．方法の一部として多数の一般社員の PC にログデータを分散するが，重要なのは分散されたログデータの改ざんを防ぐことである．ログデータの真正性を一般社員が担保する仕組みについては，第 4 章で詳しく述べる．

提案システムの利用モデルを示す(図 2)．監査対象となる PC からログデータを取得し，ログ管理サーバとログ配信サーバに送信する．ログ管理サーバとは，ログストレージシステムが設置されたサーバであり，従来のネットワーク型ログシステムにおけるサーバと同一である．一方のログ配信サーバとは，送信されたログデータを複数の社員 PC に配信するためのサーバであり，複数の社員 PC はログデータのコピーを保存する．

正常業務でのログデータの運用は，従来のネットワーク型ログシステムと同様にログ管理サーバの利用を通じて行う．ログ管理サーバに保存されたログデータの真正性に疑問が生じた場合は，社員 PC に保存されたログデータを参照することで検証や復元を行う．

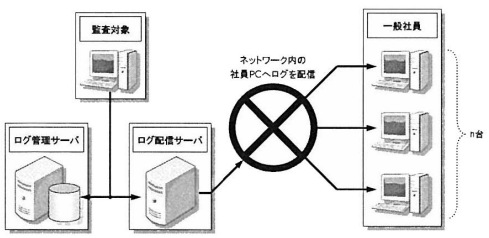

図 2 提案システムの利用モデル

3.2 攻撃モデル

内部不正において，もっとも強力な攻撃者をシステム管理者と想定すると，攻撃者は次の特性を持つと考えることができる．

i. ログ管理サーバに対して管理者権限を持つ．
ii. 社員 PC に対して管理者権限を持ち，ネットワークからアクセス可能である．

ただしシステム管理者は普段の日常業務においては善良であり，会社にとって都合の悪いログデータが発生した後に，それらを抹消する目的でログデータを改ざんする悪意を持つ．したがって，システム管理者はログデータが取得される以前に攻撃を行わない．すなわち，システム管理者によるログシステムのインストール業務は正しく行われ，社員 PC にログデータが配信される過程は妨害されないものとする．

3.3 要件定義

以上のモデルにおける社員 PC の要件は次の通りである．

i. ログデータの改ざんが困難である．
システム管理者という立場にあっても，ログデータの改ざんが困難でなくてはならない．
ii. 社員はログデータの存在を意識しない．
一般社員の業務にとってログデータは不必要であるため，社員 PC にログデータを配信・保存することで作業効率が低下するようなオーバーヘッドがあってはならない．また，一般社員がログデータを誤って消去してしまうことがないよう，ログデータの存在を意識することなく PC を利用できる状態にしておく必要がある．
iii. 正当な権限を持つ者以外はログデータを読めない．
ログデータを不必要に閲覧可能な状態にしておくことは情報漏えいのリスクを増大させることがあるため，正当な権限を持つ者以外はログデータを閲覧できないようにする必要がある．
iv. 正当な権限を持つ者はログデータを利用できる．
社員 PC に保存されたログデータを利用するためには，社員 PC からログデータを正しく収集し，閲覧できる必要がある．

4. ログ改ざん防止方式の提案

ログデータの改ざんを困難にするという要件 i を満たすために，次にあげる二つのアプローチの組み合わせによる方式を提案する．

(1) 一般社員への不正の周知
　ログデータを多数の社員 PC に保存する．ログデータが改ざんされた場合，社員 PC を用いた業務に支障を生じさせることで，多数の一般社員に不正の存在が知れ渡る．

(2) 攻撃に時間を要する仕組み
　複数の社員 PC に対して一斉に攻撃が行えないようにすることで，攻撃完了までに掛かる時間を増やす．

提案方式において，ログデータを改ざんするためには，ログデータが保存されている全ての社員 PC に対して攻撃を行う必要がある．その結果，多数の社員の業務に支障が生じることで，大きな損失が発生する．また多数の社員に不正の存在が知れ渡ることで，経営者への信用が著しく低下し，内部告発を誘発する可能性がある．経営者にとって内部告発での損失は非常に大きいため，組織的不正を抑制する効果は高いといえる．

さらに複数の社員 PC に対して一斉に攻撃が行えないようにすることで，ある社員 PC に対する攻撃を検知した時点で，他の社員 PC を保護することができる．これにより，ログデータが完全に改ざんされる前に攻撃を中断させることが可能となる（図 3）．

図 3 攻撃を中断させる仕組み

5. 提案方式の設計

5.1 一般社員への不正の周知

4 章の(1)で説明したアプローチの実現方法として，ログデータから生成した鍵で社員 PC 内の業務ファイルを暗号化する方式を提案する．図 4 のようにすることで，ログデータが改ざんされた場合，暗号化時に使用した鍵を再び生成することができなくなる．よって，業務ファイルを復号することができなくなった社員は不正を認識できる．

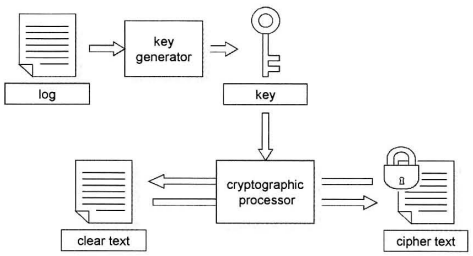

図 4 ログデータによる業務ファイルの暗号化

実装には仮想ファイルシステムを用いる．アプリケーションからの全てのファイル I/O に際してデータの暗号化・復号処理を行う仮想ファイルシステムを構築する（図 5）．社員は仮想ファイルシステムが適用された仮想ドライブを使用することで，暗号化・復号を意識することなく利用することができ，社員に対して物理ドライブを隠すこともできる．また暗号化・復号処理のために OS や個別のアプリケーションに手を加える必要がない．

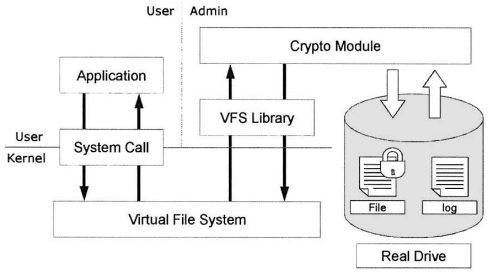

図 5 仮想ファイルシステム

また，社員 PC には随時，新しいログデータが配信されてくるため，複数のログファイルが存在することになる．そこで，鍵を生成するために必要なログファイルを業務ファイル毎に記録するマッピングファイルが必要となる（図 6）．

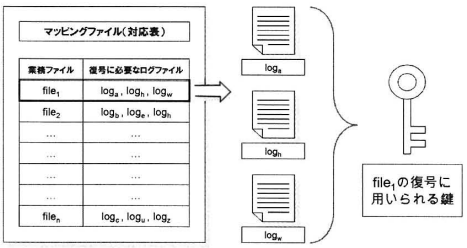

図 6 鍵生成時におけるマッピングファイルの利用

5.2 攻撃に時間を要する仕組み

4 章の(2)で説明したアプローチについて考察するため，これまでに提案した方式への攻撃方法を検討する．

社員 PC に保存されているログファイルが改ざんされた場合でも，改ざん前と同様に業務ファイルが使用可能であれば，社員は不正を認識することができない．つまり，攻撃者は暗号化・復号処理を行わないように仮想ファイルシステムを改ざんすることで，社員に気付かれずにログファイルの改ざんを行うことが可能となる．具体的な攻撃手順を次に示す．

step1. 仮想ファイルシステムを通じて業務ファイルを復号する．
step2. 復号した平文業務ファイルのコピーを，仮想ファイルシステムを経由せずに別のディスク領域へ保存する．
step3. 暗号化・復号処理を行わないように仮想ファイルシステムを改ざんする．
step4. step2 でコピーした平文業務ファイルで，暗号化された業務ファイルを上書きする．

step1 では，全ての業務ファイルにアクセスし復号を行う必要があるため，処理に多量の時間を要する．また step2・step4 においても，別のディスク領域に大量のデータを書き込むため，時間がかかることになる．

また step3 において，仮想ファイルシステムの改ざんを Trusted Platform Module（TPM）によって防ぐ方式を検討した．これは TPM の Trusted Chain によってソフトウェア保護機能を利用するものである．TPM による保護機能を停止させるためには，TPM を搭載する PC を直接操作する必要があるため（Physical Presence），システム管理者はリモートから複数の社員 PC に対して一斉攻撃を行うことができない．よって個別の社員 PC の設置場所を訪問し，直接操作する必要が生じるため，攻撃に多大な時間を要する．[1]

[1]Windows Vista では，Administrator 権限を持つユーザが TPM のオーナーパスワードを所持している場合，Physical Presence が必要とされずに，リモート操作で TPM の機能を停止することができる．この点への対応は今後の課題である．

6. 評価

6.1 仮想ファイルシステムの評価

指定したディレクトリをミラーリングし，仮想ドライブとしてマウントする仮想ファイルシステムを実装した．仮想ファイルシステムは，Linux では FUSE 等が有名であるが，今回 windows 上で実装するにあたり，Dokan を利用した[4][5].

50MB のファイルの読み込みが完了するまでの時間を 100 回計測し，その平均値を得た．実験に使用したマシンの詳細は次の通りである(表 1).

表 1 実験に使用したマシン

OS	Windows XP Professional
CPU	Pentium4 3.8GHz
RAM	3GB
HDD(250GB)速度	43.71MB/s (Read)

その結果，50MB のファイルを読み込むまでの平均時間は 0.297 秒であり、ユーザが遅延を体感することはない。読み込み速度は 168MB/s であり、HDD の読み込み速度を大きく上回っている。これは HDD のキャッシュメモリが有効に働いているためと考えられる．

6.2 安全性の評価

(1) ログファイルに対する攻撃

社員に不正を認識させるためには，攻撃を受けたことで使用頻度の高い業務ファイルが使用できなくなるようにすればよい．攻撃者がログファイルを攻撃した際に，一台の社員 PC において業務ファイルの復号に失敗する確率は以下の式で表わされる．

$$\text{復号失敗率} = 1 - \left(\frac{{}_{n-x}C_a}{{}_nC_a} \right)^m$$

n:ログファイル総数
m:使用頻度の高い業務ファイル数
x:一つの業務ファイルの復号に必要なログファイル数
a:攻撃を受けるログファイル数

ログデータは一日単位で配信され，かつ社員 PC は一年間分のログデータを保存しているという仮定の下で，ログ総数 n=250，また使用頻度の高い業務ファイル数 m=10 と設定した．攻撃を受けるログファイル数を a，一

つの業務ファイルの復号に必要なログファイル数を x としたときの不正認識率を示す．表 2 で示された不正認識率は一人の社員に対するものである．

表 2 不正認識率

		攻撃を受けるログファイル数 a			
		1	5	10	20
復号に必要な業務ファイル数 x	1	3.9	18.0	33.0	56.0
	5	18.3	63.9	87.2	98.5
	10	33.5	87.2	98.4	100.0
	20	56.6	98.5	100.0	100.0

単位：%

実際には多数の社員について同様の不正認識率が成り立つ．例として，a=5, x=10 の時，提案システムに 100 人の社員が参加している場合は，80 人以上の社員が不正を認識できる．

(2) 仮想ファイルシステムに対する攻撃

5 章 5.2 において，仮想ファイルシステムを書き換える攻撃について考察した．また TPM を用いる方式の検討を行った．

6.3 データ量の評価

ログデータを社員 PC に配信することで発生するデータ量について考察する．

教職員数 400 人程度の規模をもつ大学にヒヤリングを行った結果，一年間で発生する財務データベースのダンプファイルは，およそ 2GB のデータ量となることが明らかとなった．これは，全ての社員 PC にダンプファイルのコピーを保存すると仮定しても，昨今のハードディスクの性能を考えればほとんど問題とならないデータ量である．またログデータが一日単位で配信されると仮定すると，一日に配信されるデータ量はおよそ 10MB となり，データ通信量としても問題ない．

7. まとめ

組織的不正の存在下でログ情報の改ざんおよび消去を防止するために，(1)多数の社員 PC にログデータを配信し，ログデータが改ざんされた場合は，不正の存在が社員に知れ渡る仕組み，(2)複数の社員 PC を同時に攻撃することができず，攻撃に時間を要する仕組みから成るログ改ざん防止システムを提案した．

これらを実現するために，ログファイルから鍵を生成し業務ファイルの暗号化・復号を行う方式，ならびに仮想ファイルシステムを用いることで透過性のある方式を提案した．また仮想ファイルシステム Dokan の性能，ログファイルへの攻撃に対する安全性，発生するデータ量についての評価を行い，提案システムの有効性と実現可能性を示した．

今後は提案システムの実装を行う予定である．

参考文献

[1]芦野佑樹，佐々木良一，“セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価，” 情報処理学会論文誌 Vol49, No.2, pp.999-1009, 2008

[2]大津一樹，宇田隆哉，伊藤雅仁，市村 哲，田胡和哉，星 徹，松下 温，“アクセス制御機構を持つ P2P 共有ファイルシステム，”2005 年 暗号と情報セキュリティシンポジウム(SCIS2005), vol.1, pp.13-18, 2005

[3]東森ひろこ，手塚 伸，宇田隆哉，“デジタルフォレンジックを目的としたファイル分散保存システムの提案，” コンピュータセキュリティシンポジウム 2008(CSS2008), pp.127-132, 2008

[4]荒川淳平，淺川浩紀 “意識しないで自然に使えるデータ管理システム Decas，” 第 49 回プログラミング・シンポジウム, pp.65-72, 2008

[5]Dokan, http://dokan-dev.net/

[6]Trusted Computing Group, https://www.trustedcomputinggroup.org/home