電子化知的財産・社会基盤　8－5
（2000．6．2）

超流通技術に基づくアクセスログ管理方式の提案

河原 正治 †　　大瀧 保広 ††

†筑波技術短期大学 教育方法開発センター
††茨城大学 工学部 情報工学科

コンピュータ犯罪の痕跡を事後に検証する技術として，ログを記録することが一般的である．しかしながら，従来のログの記録方法では，管理者によるログの改ざん・消去が可能であり，証拠保全能力の確実性という観点から不十分である．また，従来技術において証拠保全に力点をおけば，プライバシーの保護が犠牲になるという問題があった．

本稿では，超流通の実装技術とログ記録手法の構造の類似性に着目し，たとえ管理者であっても，痕跡を残さずにログを改ざんすることができないようなログ記録技術を提案する．また，本手法は，記録された利用者の情報が，管理者に対して適切に保護される機構をも含む．これによって，犯行の痕跡を事後に検証する機能と利用者のプライバシを保護する機能とが両立できる．

An Access Log Management Scheme Based on Superdistribution Technology

KAWAHARA Masaji †　and　OHTAKI Yasuhiro ††

†Tsukuba College of Technology
††Ibaraki University

Keeping archives of the access logs for a computer system is a standard procedure that helps enormously in tracing computer crimes. Records generated using conventional procedures are vulnerable to alteration by a system operator and thus can be challenged when presented as evidence in legal proceedings. Moreover, the need to develop evidence of crimes conflicts with the need to ensure the privacy of those using the system.

The authors observe that the security requirements for the usage records of a superdistribution system closely resemble those for the access log of a computer system. They propose a log keeping procedure that takes advantage of this resemblance to ensure the integrity of the archive and protect it against improper access by the system operator. This procedure provides evidence of computer crimes while preserving the privacy of computer users.

1 はじめに

地球規模に広がったインターネットは犯罪の質を変えてしまった．インターネットを通じて生命や財産に関る情報がやりとりされるようになったため，それに伴って犯罪の危険性も高くなった．同時に，インターネットは犯人の追跡をより困難にしており，各国政府は犯罪捜査の基盤を確保しようと様々な検討を行っている．

アクセスログの収集と解析は，ネットワーク上のコンピュータに対する不正侵入を検知したり，アクセス元を特定するために広く用いられる手法である．しかし，巧妙な犯罪者はログファイルを改ざんしたり消去したりすることによって，犯罪の痕跡を残すまいとする．このような行為に対処するため，アクセスログの保護に関しては様々な研究成果が発表されている [1]．ログファイルの保護手法は，外部の攻撃者から自分のコンピュータを保護することが目的であるため，内部のシステム管理者自身の犯罪行為については無力である．

また，システム管理者はログを通してユーザの行動を把握することが可能であり，プライバシー保護については考慮されていない．これに対して，ネットワークアクセスにおける匿名性を保証しプライバシー保護を目指したシステムも報告されている．

Lucent Personalized Web Assistant (LPWA)[2] は，ユーザの Web アクセスを代理中継するサーバであり，アクセス対象となる Web サーバに対して匿名性を保証し，プライバシー保護を目指す．しかし，LPWA の管理者はログファイルを参照することができ，また，アクセスログを改ざん・消去したり，特定の個人に関する情報を不当に公開することが可能である．そのためユーザのプライバシーが確実に保護されているとはいえない．

Crowds[3] では，各ユーザの計算機上で中継サーバを起動することによって，多数の中継サーバを用意する．ユーザがサーバにアクセスを試みると，多数の中継サーバをランダムに経由して目的のサーバに到達する．このことによって，ユーザのプライバシーは保護されるが，犯行の痕跡の検証はより困難になる．

以上のように従来の研究では，プライバシー保護を重視すればするほど犯罪捜査が困難になり，逆に犯罪捜査の基盤を重視すればプライバシーを軽視することになる．本稿では，超流通技術を利用することによって犯行の痕跡を検証する機能と利用者のプライバシーを保護する機能とを両立できる手法について検討する．

2 ログの重要性と現在の問題点

2.1 ログの重要性

コンピュータシステムのセキュリティを保つためには，認証や操作の履歴をログと呼ばれる記録用のファイルに蓄積することが一般的である．通常，システムの利用開始，重要なファイルに対するアクセス，認証などの情報が記録される．

ログファイル自体はアクセスの可否を制御しないが，不正なアクセスが行なわれた（あるいは行なわれなかった）ことの記録となる．たとえば，コンピュータシステムの利用の開始と終了時刻とが適切に記録されていれば，ある犯罪が行なわれた日時が判った場合に，その時刻にシステムを利用していた利用者を限定することができる．すなわち，ログファイルが適切に管理され，そこに犯行に結びつく情報が保持されていれば，犯罪追跡のための有力な手がかりとなる．逆に，ログファイルがなければコンピュータ犯罪の捜査は極めて困難なものとなる．

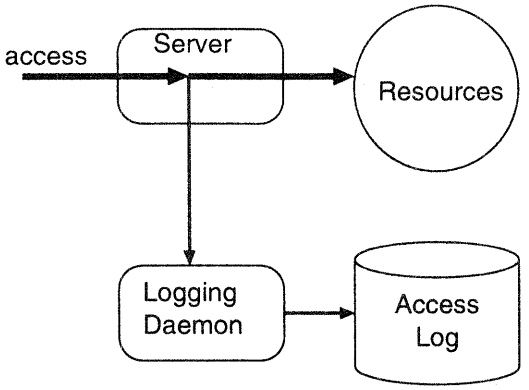

図 1: ログ記録システムの基本構造

2.2 従来のログの問題点

犯罪者の立場から見ると，このようなログファイルを改ざん・消去できれば，自らの犯罪行為を隠蔽し，発覚しないようにできる．そのため，ログファイルは一般に，通常の利用者には書き換えられないようにアクセス制御が行われ，システム管理者権限を持ったプロセスが記録する．別の見方をすれば，管理者ならばログファイルの改ざん・消去が可能であるということであり，また，不正にシステムに侵入した攻撃者が管理者権限を奪取できれば，侵入の痕跡を消せるということでもある．具体的には，たとえば次のような事件・事故が起こり得るということである．

- 犯罪者が，自宅のコンピュータからインターネットに接続し，犯罪行為を行なった後に，自分のコンピュータ上に蓄積された犯罪行為に関する記録を消去することができる．
- インターネット接続業者 (ISP) の管理者は，自システムのログを書き換えることができる．ログが犯行追跡の有力な手がかりとして利用されることを考えると，悪意の管理者によってISP 利用者が犯罪者に仕立てあげられてしまう可能性がある．

これらを整理すると，従来のログ記録方式には次のような問題点がある．

1. ログの記録の対象となるのは限定された操作のみであり，犯罪追跡にとって充分な情報が記録されていない．
2. ファイルシステム上の通常ファイルとして記録されているため，改ざんが容易であり，またその改ざんの痕跡の検出が困難であることから，犯罪捜査の証拠としての堅牢性に欠ける．
3. 管理者であればログファイルを削除することも可能であり，犯行追跡のための手がかりの保全という意味において，確実性に欠ける．

したがって，たとえ管理者といえども改ざんが不可能あるいは極めて困難なログ管理手法を実現すると同時に，利用者が望まない情報が利用者の承諾なしには公開されていないことを，利用者自身が確信できるシステムが必要である．本論文では，このための基本的な考え方を提案する．

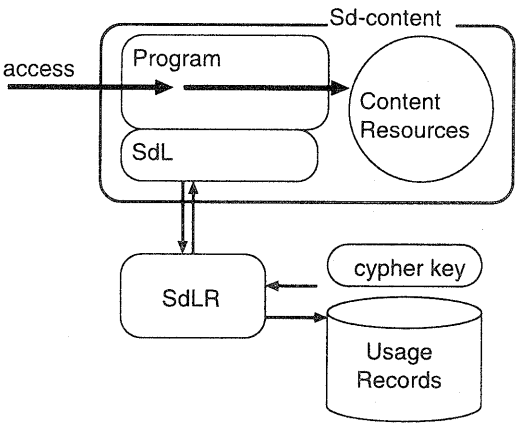

図 2: 超流通システムにおける SdLR の基本構造

3 ログ記録システムと SdLR の比較

3.1 基本構造の類似性

ログ記録システムは，一般に，特定のイベントの発生，例えばサーバなどを通じて，パスワードファイルなどの資源へのアクセスが発生したときに記録される．この構造を図 1 に示す．

そのログファイル自身へのアクセスをイベントとしてログファイルに記録することはできないため，管理者によるログファイルの改ざんあるいは削除が行なわれると，その痕跡が残らない．本稿で提案するアクセスログ管理手法の第一の目的は，管理者であってもログファイルを改ざん・削除できないようにすること，あるいは改ざん・削除した場合に明らかな痕跡が残るようにすることである．

ところで，超流通システムでは，利用者の手元のマシンにおいて，類似の構造がある．

超流通は使用量に応じた課金を行なうコンテンツ流通システムであり，所有に対してではなく利用に対して課金を行なう．超流通システムで流通されるコンテンツ（以下，超流通コンテンツ）には，使用許諾条件などが記述された Superdistributuon Label (以下 SdL) が付加されている．利用者の手元のマシンには，SdL Reader (以下 SdLR) が付加されており，SdL の記述に従って，超流通コンテンツの実行制御が行なわれる．超流通コンテンツの内部は，プログラム部分とプログラム以外の資源とにわけて考えることができる．超流通コンテンツを利用者が使用すると，コンテンツ ID とその使用量が使用記録として記録され，これを回収することによって，利用者からの料金の徴収と権利者への分配が行なわれる．この構造を図 2 に示す．

ここで，使用記録は，利用者が管理するマシン内に存在し，超流通コンテンツがアクセスされる度に更新される．

使用記録には，利用者 ID，使用したコンテンツ毎のコンテンツ ID および使用量が記録されており，これらの情報を不正に改ざんあるいは消去することができれば，料金の徴収を免れたり，不正に料金を入手することができる．したがって，使用記録は利用者の攻撃から保護されていなければならない．また，暗号化された超流通コンテンツを復号するための暗号鍵は，利用者の手元のマシンにあらかじめ格納されている．そして利用者によって読み出されないようにしなければならない．

この二つの図を比較すると，超流通システムにおいて利用者の手元のマシンで行なわれる処理の構造が，ログ記録システムの構造と高い類似性をもつことがわかる．

3.2 SdLR における保護手法

超流通システムでは，使用記録や暗号鍵を，利用者の攻撃から保護する方法の一つとして以下の方式が提案されている．

第一に使用記録や鍵が保持されるメモリは，コンピュータの主記憶や二次記録媒体とは独立しており，SdLR のみがアクセス可能となるようにアクセス制限が施される．これによって，不正なプロセスによって，ソフトウェア的に使用記録を改ざんすることを防止し，また暗号鍵が読み出されることを防止する．

メモリを直接プローブすることによる使用記録の改ざんを防止し，暗号鍵の読み出しを防止するために，これらのメモリは保護容器に格納される．保護容器は，メモリセルへの物理的なアクセスを検出し，その時点で，メモリ内に記録している情報を消去する「情報の容器」である．

したがって，使用記録を保持するメモリを内蔵する保護容器に物理的な攻撃を加えることで，利用者は使用記録を消去することができる．すると消去された使用記録分の料金の徴収を免れることができるかのように思われる．しかし同時に利用者は，暗号鍵を失い，そのため，以後，暗号化された超流通コンテンツを利用することができなくなる．

保護容器内が攻撃を受けたかどうかは，たやすく検査できる．攻撃が誰の管理下で起きたか，起きなかったかは，引渡し毎に確認されるから容易に定まる．そこで多くの善良な利用者は，使用記録を保全することを選択するだろう．同時に，保護容器が十分に機能していることは，内部に格納された使用記録が，SdLR が許可する範囲内でのみ読み出され，それ以外の方法では読みとられていないことの証明にもなる．

4 超流通技術に基づくログ記録システム

4.1 提案手法の基本構造

以上の考察に基づいて，超流通技術に基づくログ記録システムを構築する．

ログファイルは，保護容器内でアクセス制御されたメモリに格納する．SdLR は，従来のログを記録するデーモンプロセスに相当し，これだけがログファイルにアクセスできる．

サーバは，超流通コンテンツとして実装し，SdLR にイベントを通知することでログの記録を依頼する．アクセスの対象となる資源は，超流通コンテンツ内に含んでも，外部にあってもよい．

このように構成することで，利用者はログファイルを改ざんできなくなる．利用者はログファイルを格納する保護容器に攻撃を加え，ログファイルを消去することはできる．しかし，攻撃が誰の責任のもとで起きたかは確認される．

自分の計算機に対して不正な，しかし攻撃でないアクセスが行なわれた場合には，それは証拠が保全されていることの証明であると同時に，システムが善良に管理されたことの証明ともなる．

逆に攻撃があったならば，管理者自身がそれを行なったか，またはそれを見過ごした可能性があることになる．ログの削除について，利用者がまず最初に疑われるような前例が蓄積されれば，改ざんの試みは少なくなるであろう．

4.2 捜査機関へのログの提出とプライバシーの保護

前章で述べたような方法で構成されたログ記録システムでは，ログファイルがSdLRの管理下にある．したがって，ログファイルにアクセスするユーティリティを超流通コンテンツとして実装すれば，超流通コンテンツとSdLRの間で適切な認証と実行制御が行なわれ，目的に応じた様々なログの操作が実現できる．

たとえば次のような機能が考えられる．

- 保護容器が攻撃されていないことを確認する機能
- ログの内容を管理者に表示する機能
- 条件（時間帯，アクセス対象など）を満足するログのエントリが存在するかどうかのみを表示する機能
- 正当な捜査機関に対してのみログの転送を許可する機能
- 管理者の同意があって初めて，ログの転送を許可する機能
- 転送されるログの項目を管理者が指定できる機能

これによって，予期できない犯罪に関しても事後に証拠を収集することを可能にする機能と，捜査が行なわれていない日常において，勝手にログが回収されていないことの確信を人々に提供する機能の二つを両立させることができる．

4.3 Crowds との組合せ

以上で述べた基本構成と，Crowds の構成を組み合わせることができる．

Crowds と同様に，超流通技術に基づくログ記録システムを有する多数のマシン上に代理中継サーバを起動する．利用者がネットワークを通してサーバにアクセスすると，これらの中継サーバをランダムに中継した後に，目的のサーバに到達する．このとき，利用者がサーバにアクセスする時に使用する中継サーバの選択を，超流通技術に基づくログ記録システムをもつものに制限する．

これらによって，アクセス対象のマシンに対して，利用者の手元のマシンの情報を隠蔽することができ，Crowds と同様の意味において利用者のプライバシーが保護される．

また，捜査機関が犯行の痕跡を追跡する場合には，Crowds の場合と同様に，アクセス対象のサーバのログから，順次，代理中継サーバを遡りながら利用者のマシンを特定することになる．多数の代理中継サーバを経由する場合，中継地点でログが改ざん・消去されると捜査が行き詰まることになる．しかし代理中継サーバが超流通技術に基づくログ記録システム上で実行されていれば，次のような利点がある．

- 経路の途中でログが改ざんや消去が行なわれた場合には痕跡が残るため，ログが消失している危険性が少ない．
- 捜査機関は，必要なログの情報のみを取り出しながら，追跡を行なうプログラムを構成できる．

また中継サーバの管理者やネットワーク利用者は，捜査機関にログを開示する条件を制御できる．

- 中継サーバの管理者は，中継したログのみを選択的に公開することができるため，必要最小限の情報提供を行なうことができ，捜査に協力しやすい．

- 犯行の痕跡の追跡によって，利用者を特定するためには，多数の中継サーバの管理者の同意が必要であるため，多数の中のある割合が賛成しないと犯人の計算機にたどりつかない．これは，凶悪な犯罪を防止するためには，自己のプライバシーをある程度犠牲にすることを受け入れるというモデルに合致する．

4.4 巨大なログファイルへの対策

ログファイルの記録場所は，保護容器内のメモリであり，物理的な上限がある．そのため，インターネット接続業者のようなサーバの場合には，現実問題としてログファイルが巨大になり，保護容器内に収まり切らない危険性がある．

これに対して，超流通における使用記録の回収と同様に，記録されたログを，例えばログの保管を専門とする機関に送信することが考えられる．この場合に，ログファイルのどの部分がどこに転送されたのかを示すインデックス情報のみを保護容器内に保持することで，保護容器内の記録情報を削減できる．

ログの重要度によっては，管理者の手元の記録媒体に保管することも考えられる．ただし，この記録媒体は，一旦記録した内容を修正しようとすると，その痕跡が残るものでなければならず，また媒体の識別が可能なIDを有する必要がある．保護容器内には，外部媒体のIDとそれに記録した日時など，ログファイルを書き出した対象を特定できる記録を保管する．

一旦記録した内容を修正するとその痕跡が残るメモリを対改ざんメモリと呼ぶことにする．このようなメモリは (1) 1ビットの情報を記録でき，(2) その情報を反転 ($0 \rightarrow 1, 1 \rightarrow 0$) することができない，という性質を持つ．

類似の機能を実現するものとして，1度のみ書き込み可能なデバイスが存在するが，一般にこれらは，初期状態が例えば0と決まっており，これを1の状態に書き換えることことによって，記録を行なうものである．したがって，$1 \rightarrow 0$ の改ざんは不可能であっても，$0 \rightarrow 1$ の方向の改ざんが可能であるため，そのままでは上記の条件を満足しない．

対改ざんメモリは，このような $0 \rightarrow 1$ の方向の書き換えのみが可能なデバイスの2bitを1単位して実現することができる．初期状態は00であり，情報を保持していないことを示す．情報の0の記録パターンは01とし，情報の1の記録パターンは10とする．状態11は情報を保持していない．01および10の状態からは11の状態にしか移行できないため，一旦記録した情報を抹消することはできるが，改ざんはできない．また，抹消した場合にはその痕跡が残る．

5 おわりに

超流通はディジタル情報自身に自己防御機能を持たせる技術である．これを既存の技術と組み合わせることによって，様々な応用が可能である．これまでに，無料・有料コンテンツの著作権処理システムに関して多くの研究成果が公表されている．超流通技術の動向については，`http://www.supperdistribution.org/` を参照されたい．本稿では，新たな応用としてプライバシーと証拠能力とを両立させ得るアクセスログ管理について概略を述べた．

不正アクセス禁止法に関する議論の中で，アクセスログ保存の義務づけに関してはプライバシー保護の観点から強い反対があった．電子商取引，行政，教育，医療などの幅広い分野でのインター

ネット利用が強力に進められているが，どのように犯罪を未然に防ぎ，そして事後に犯人を検挙する かが重要になる．プライバシーが保護される形で犯罪捜査に関する証拠を保全する技術は健全なディジタル社会を享受するためには不可欠なものである．

参考文献

[1] 高田哲司, 小池英樹: 逃げログ: 削除まで考慮にいれたログ情報保護手法, 情報処理学会論文誌, Vol. 41, No. 3, pp. 823–831 (2000).

[2] Gabber, E., Gibbons, P. B., Kristal, D. M., Matias, Y. and Mayer, A.: Web Access with LPWA, *Comm.ACM*, Vol. 42, No. 2, pp. 42–47 (1999).

[3] Reiter, M. K. and Rubin, A. D.: Anonymous Web Transactions with Crowds, *Comm.ACM*, Vol. 42, No. 2, pp. 32–38 (1999).