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

2005－ＣＳＥＣ－30 (63)
2005／7／22

USBデバイスを用いたデジタルフォレンジック保全方式の提案と評価

芦野 佑樹† 粉川 寛人† 佐藤 吏† 佐々木 良一†
†東京電機大学大学院工学研究科情報メディア学専攻
〒101-8457 東京都千代田区神田錦町 2-2
東京電機大学 11 号館 11 階 1102
E-mail: † {ashino, kokawa, sato}@isl.im.dendai.ac.jp, † sasaki@im.dendai.ac.jp

あらまし インターネット社会の進展に伴い，不正アクセスなどの攻撃に対処し，デジタルデータの科学的証拠性を確保し，訴訟などに備えるための技術や社会的しくみであるデジタルフォレンジック（Digital Forensic）が最近注目されている．今後は，企業の説明責任の範囲が増大にともない，財務会計情報などの情報改ざんなどを行っていないことの証拠性を確保し，訴訟に持ち込まれてもよいようにしていくことが大切となると考えた．そこで，著者らはこのようなことを可能にするために，（1）ＩＣカード機能付のＵＳＢデバイスと，（2）ヒステリシス署名技術を用い，（ａ）処理をすれば必ず記録が残るようにするとともに，（ｂ）改ざんしてないことを証明できる方式を考案した．あわせて，本提案方式のプロトタイプを開発し，評価を行ったので報告する．

キーワード USBデバイス，フォレンジック，ヒステリシス署名，チェーニングハッシュ

Proposal and evaluation of digital forensic logging system using USB Device

Yuki Ashino †, Hirohito Kokawa †, Tsukasa Sato †, Ryoichi Sasaki †
† Tokyo Denki University 2-2, Kanda-Nishiki-Cho, Chiyoda-Ku, Tokyo, 101-8457 Japan

Abstract With development of Internet society, Digital Forensic which is the technology and the social structure to prepare digital evidence for a lawsuit attracts against illegal attack has been paid attention recently. In order to achieve the accountability of a company from now on, we thought that the evidence that financial accounting information must be not altered and that proof must be secured become important in order to cope with a lawsuit. We developed the system which use (1) USB device and (2) hysteresis signature technology, and can prove (a)that logging is obtained only when user operate the PC, (b) that log is not changed. In addition, we report the system and results evaluated by using the prototype program.

Keyword USB device, Forensic, Hysteresis signature, Chaining hash

1 はじめに

インターネット社会の進展に伴い，ほとんどすべてのデータはデジタル化して扱われるようになってきた．一方，日本においても，従来は考えられなかったような場合にも訴訟が行われるようになってきた．

このような状況から，デジタルデータの証拠性を確保し，訴訟などに備えるための技術や社会的しくみが要求されるようになってきた．これが，デジタル・フォレンジック（Digital Forensic：以下ＤＦと略す．）と呼ばれているものである）．

一口でＤＦといっても，扱う範囲は広い．従来，ＤＦで主に扱っていたのは，以下のようなものである．

（１）サーバや PC などのコンピュータを対象とし，

（２）不正侵入などの攻撃を検知すれば，応急処置をするだけでなく，証拠となりうるデータを保存し，（ａ）どのような被害を受けたか，（ｂ）どこから侵入を受けたか，（ｃ）誰が侵入者かなどを分析し，

（３）その後自分が行う訴訟などに備えるものである．

この分野は，コンピュータフォレンジックとも呼ばれ，今後も重要な分野である．しかし，ＤＦとしては，さらに，いろいろな分野が重要になっていくと考えられる．

特に，今後，企業の説明責任の範囲が増大していくと，財務会計情報などの情報改ざんなどを行っていない証拠性を確保し，訴訟に持ち込まれてもよいようにしていくことが大切となる．

著者らはこのようなことを可能にするために，（１）ＩＣカード機能付のＵＳＢデバイスと，

（２）ヒステリシス署名技術を用い，（ａ）処理をすれば必ず記録が残るようにするとともに，（ｂ）改ざんしてないことを証明できる方式を考案した．あわせて，本提案方式のプロトタイプを開発し，評価を行った．

本稿では，２章ＤＦの概要と利用局面についてもう少し詳しく考察し，３章では提案方式を紹介し，４章ではプロトシステムの概要と評価結果について述べた上で，５章で今後の展開計画について言及する．

２　ＤＦの概要と利用局面に関する考察

２．１　ＤＦの利用局面の検討

ＤＦとは，デジタル・フォレンジック研究会によると，「インジデント・レスポンス（コンピューターやネットワーク等の資源及び環境の不正使用，サービス妨害行為，データの破壊，意図しない情報の開示等，並びにそれらへ至るための行為（事象）等への対応等を言う．）や法的紛争・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・技術を言う」と定義されている[1]．

ここで，Forensic という英語は，ラテン語からきたものであり「法の」とか「法廷の」といった意味を持つ．したがって Forensic Medicine の言うのは法医学と訳されている．法医学というのは（１）医学を用いて，（２）死体などの検査を行うことによって科学的証拠性を確保し，（３）将来の刑事訴訟などにそなえようと言うものである．

したがって，ＤＦというのは，（１）計算機などのデジタル化技術を利用し，（２）各種のデジタルデータを保全することによりその科学的証拠性を確保し，（３）犯罪などの将来の訴訟に備えようというものと考えてよいであろう．

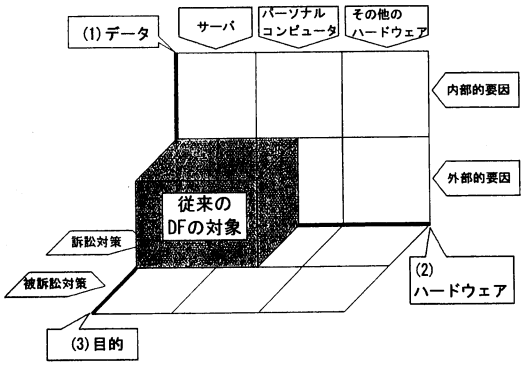

図１　従来のＤＦの適用例

２．２　従来のＤＦの適用

従来のＤＦが利用されている主な局面は，以下のとおりである（図１参照）

（１）サーバや PC などのコンピュータを対象とし，

（２）不正侵入などの攻撃を検知すれば，応急処置をするだけでなく，証拠となりうるデータを保存し，（ａ）どのような被害を受けたか，（ｂ）どこから侵入を受けたか，（ｃ）誰が侵入者かなどを分析し，

（３）その後自分が行う訴訟などに備えるものである．

これらは，コンピュータフォレンジックとも呼ばれており，「計算機科学などを利用して，デジタルの世界の証拠性（evidence）を確保し，法的問題の解決を図る手段．ログの改ざん，破壊等，これまでの手法では証拠を検出することが困難な被害を受けたコンピュータに対しても，高度なツールによってコンピュータ内のデータを調査・分析することにより，不正アクセスの追跡を行う手段を含む」という定義がなされてきた[2]．

２．３　今後重要になっていく分野

今後，以下のような分野が重要性をますと考えられる（図２参照）．

（１）サーバやＰＣなどのコンピュータだけでなく，情報家電や携帯電話，ネットワークなどを対象とした証拠性の確保も重要な対象となる．情報家電や携帯電話は日本が強い部分であり，研究対象としても重要であると考えられる．

（２）不正侵入の証拠性だけでなく，（ａ）財務会計情報などの情報改ざんや（ｂ）個人情報や機密情報などの漏洩，（ｃ）セクハラや詐欺などの不正行為がなかったかの証拠性も大切となる．米国では，Sarbanes Oxley 法（企業改革法）が制定され，効果的な内部統制を行っていくことが義務付けられるようになってきた．日本に置いても企業の透明性を確保し，アカウンタビリティ（説明責任）を問われるシーンがますます多くなっていくものと予想される．

（３）自分が訴訟に持ち込む場合だけでなく，訴訟に持ち込まれても良いようにすることも大切になる．訴訟に持ち込まれても良くするためには，（ａ）処理をすれば必ず記録が残るようにするとともに，（ｂ）改ざんしてないことを証明できる方式の確保が不可欠となる．

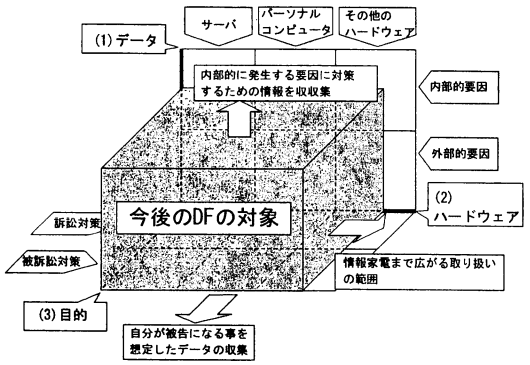

図２　今後重要になっていく分野

３　提案方式

３．１　ＤＦの適用対象

本稿で提案するシステムが対象とするＤＦは，（１）訴訟がされても十分に対処できる事，（２）日常の PC の操作に関する情報を確実に収集することを目的としている．

図３に示したように，個人が管理する PC にフォーカスしている．PC で行われる活動が合法的である事を後に証明する目的で行う．また，確実に操作情報を収集するためには，通常のプログラムが単純に生成するログデータを取り扱う以外の検討が必要である．また，PC へのログイン／ログオフと言った基本的な履歴や，ファイルへのアクセス履歴といったログデータだけでなく，操作者が作成したドキュメントファイルの他，アクセスしたウェブの内容やメールの送受信の内容も収集していくべきだと考えている．

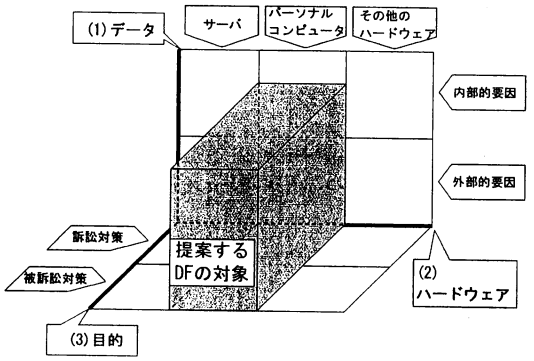

図３　提案するシステムの位置づけ

本提案するシステムに適する適用例として下記のようなものが考えられる．

（ａ）顧客情報を取り扱う PC

個人情報保護法の施行により，一人でも顧客情報を取り扱う企業は，個人情報を厳重に取り扱う義務が発生している．企業活動をする上で顧客情報を取り扱わない事は事実上無いので，どの企業も個人情報保護を徹底する必要がある．ひとたび，個人情報が流出してしまうと，損害賠償の責任ばかりではなく，企業イメージの低下に繋がってしまう．

こうした背景から，個人情報を取り扱う PC は限定される事が推奨されている．こうした PC に本システムを導入することにより，サーバが管理しているファイルアクセス以外の操作情報を記録し，操作者による不審な行動を後から追跡することが可能となる．従業員にとって見れば，この機能を入れることにより，不正を行っていないことの証明が容易になる．

（ｂ）営業担当者が持ち運ぶ PC

営業担当者は，PC を携えて社外に出る機会が多い．当然，PC には顧客情報が詰まっている．また，社外に出る機会が多い以上，会社の監視の行き届かない場所に行くことは容易であり，そこで個人情報を流出させてしまう危険は非常に高くなる．また，基本的に，社外に出てしまった PC はスタンドアロンで動かざるを得ないため，顧客情報へのアクセスを中央のサーバが監視・記録することが事実上不可能である．

こうしたシーンに，本システムを導入することで，後に営業担当者から返却された PC を調査することにより，営業担当者が情報を意図的に漏洩していないか確認することが可能となる．

（ｃ）アウトソース先へ貸し出す PC

業務の一部または全体をアウトソーシングしてコスト低減を図る企業が増えてきた．こうした背景から，企業がアウトソース先に PC を供与するシーンが増えてきた．企業はアウトソース先からのアウトプットを元に工程を管理しているが，実際にアウトソース先が正確に作業をこなしているかの判断が難しい．また，企業が所有する個人情報を共有する必要がある事から，円滑な情報の共有による作業効率の向上が図れないでいた．

このようなシーンで，供与する PC に本提案するシステムを導入することで，アウトソース先から情報漏洩を監視する以外にも，作業内容を管理することができる．結果，円滑な情報共有が可能となり，作業効率の向上が図れるようになる．

3．2　評価指標

本システムを評価するに当たって，下記の４項目を上げる．

（１）改竄されていないことが証明できること

記録されたデータが加筆，修正，削除が行われていない事を証明できなければならない．また，データの正当性を第三者によって検証が行える事が望ましい．

（２）全ての操作記録が残っていること

操作に関する全ての情報を収集できる事が望ましい．例えば，PC の操作記録をファイルアクセスのみに限定しても，それが故意による物なのか，プログラムによるものなのかの判断は難しい．そのため，PC の操作記録を可能な限り収集し，操作者の意図が分かるようにする必要がある．

（３）運用性に問題はない

使いやすくなければ，操作者の負担がかかるため，運用者は継続してシステムを利用しようとは考えなくなる．運用性の大きな指標は，操作者がシステムを導入することによりパフォーマンスが大幅に低下したり，操作範囲に制約が発生しないようにする必要がある．

（４）導入コストが低い

現在までのソリューションの多くは，大変高価である．そのため，リスクに投資することのできない中小企業は，なかなか導入に踏み切れない．こうした事から，導入コストは，ＤＦツールを評価する上で必要な要素である．

また，仮に導入コストが低くても，運用時のコストが高くてはメリットが少ないので運用コストも考慮する．なお，ここで議論する運用コストは，ランニングコストの他に PC の処理リソースも含める．

3．3　提案システムの構成

本提案では，以下の２つのアーキテクチャの構成要素として扱う．これらのアーキテクチャについては，図４に示した．

（１）USB デバイス

USB デバイスは，下記の要素によって構成されている．

（ａ）アクセス可能領域

USB インターフェースを用いて PC からアクセスができる領域である．ここには IC チップに相当する暗号演算ソフトウェアもこの領域に配置される．暗号演算ソフトウェアは，ヒステリシス署名を処理を行う．

（ｂ）耐タンパー領域

操作者でもアクセスできないばかりでなく，物理的にも守られた領域である．ここに格納されている情報は，アクセス可能領域に含まれる暗号演算ソフトウェアのみに限定されている．この領域にはヒステリシス署名に必要な最終ヒステリシス署名情報と秘密鍵が含まれる．

（２）PC

（ａ）ロガー

ログデータを生成するプログラムである．本稿ではこのロガーを限定しない．ロガーには，例えば OS のログイン情報を記録する監査プログラムや，キーボードの入力情報を出力するキーロガーもなども含まれる．

（ｂ）ログプログラム（ヒステリシスロガー）

ヒステリシス署名付きのログデータを作成しログファイルに書き出す．

（ｃ）操作ロック機能

USB デバイスが挿入されていない時（ヒステリシス署名が施せない時）に，PC の操作をできなくさせる．

（ｄ）ログファイル

ヒステリシスロガーによって作成されたログデータを蓄積する．

（３）操作者

USB デバイスを所持しており，PC を操作する時に USB ハブに USB デバイスを差し込んで操作し，操作が終了した後，USB デバイスを抜く．

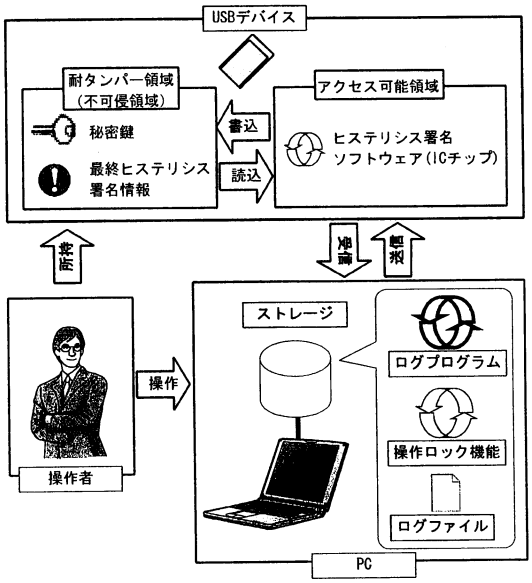

図４　システムの構成

上記のアーキテクチャに加えて，本システムは下記の前提条件を課す．

（ａ）USB デバイス内の耐タンパー領域内のデータは抽出及び改竄は困難である．
（ｂ）PC 上で動作するログプログラムは改竄されていな事を保証する．

提案システムで使用するヒステリシス署名について，簡単に説明する．
ヒステリシス署名は，デジタル署名をする際，過去署名した情報を反映させる方式である[3]．そのため，現在から過去にいたるまでの署名した全情報がお互いに相関し合うため，万一，署名の偽造や意図的な削除を困難にさせる．ヒステリシス署名の処理フローを図５に示す．

D_i ：i 番目の署名対象の文章

R_i ：i 番目の連鎖データ

$H(x)$ ：x のハッシュ値

$S_{ing}(x)$ ：x の署名データ

Y_i ：i 番目の連鎖署名データ

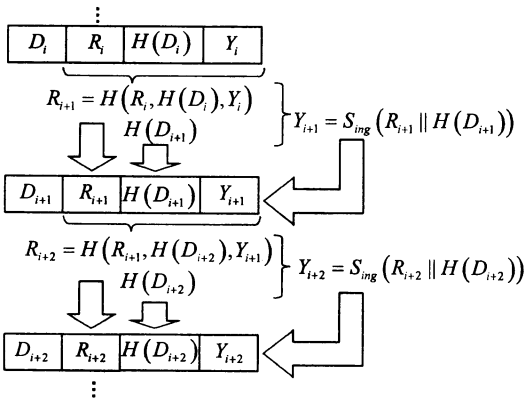

図５　ヒステリシス署名の概要

本提案システムでは，ヒステリシス署名をログファイルの保全性確保のために用いている．ログファイルは，頻繁に追記することを前提としている．ファイル全体を単純にデジタル署名するのではなく，追記するデータにヒステリシス署名を施す方法を採っている．

３．４　処理フロー

（１）操作者が所持している USB デバイスを PC に差し込まれていないと，PC はロックされており何人も操作できない．

（２）操作者が USB デバイスを PC に差し込むと，PC のロックが解除されて操作できるようになる（図６）．

（ａ）操作者が PC の操作を行うと，PC に常駐しているヒステリシスロガーがログデータ D_{i+1} を生成し，USB デバイスに図５に示す R_{i+1} と Y_{i+1} を送付する．

（ｂ）R_{i+1} と Y_{i+1} を受け取った USB デバイス内部にあるヒステリシス署名ソフトウェアは，USB デバイス内部に格納されている最終ヒステリシス署名情報 R_i，Y_i と秘密鍵を読み込み，ヒステリシス署名を行う．

（ｃ）ヒステリシス署名の処理結果 R_{i+1} Y_{i+1} は，最終ヒステリシス署名情報として上書きされる．また，R_{i+1} Y_{i+1} は PC のヒステリシスロガーに送られる．

（ｄ）ヒステリシスロガーは USB デバイスで作成された処理結果 R_{i+1} Y_{i+1} とログデータ D_{i+1} をストレージにあるログファイルに追記する．なお，このストレージは特別な機能は持っていない．

（３）上記のフローを USB デバイスが差し込まれている間続ける．操作者が USB デバイスを取り外すと，PC はロックされ何人も操作できない状態になる．

（４）ログファイルに記録されたデータを検証する際は，下記の流れで検証を行う．

（ａ）検証者は，PC に記録されているログファイルに記録された最後のログデータ R と Y の情報が USB デバイスの耐タンパー領域に記録されている最終ヒステリシス署名情報が一致しているか USB デバイス上のソフトウェアに問い合わせる．

（ｂ）USB デバイス上のソフトウェアは，検証者から送られてきた R と Y と，耐タンパー領域に記録されている最終ヒステリシス署名情報と比較し，一致していれば真を，一致していなければ偽を返す．

（ｃ）検証者は，USB デバイスの回答が偽の場合は検証を失敗とする（ログファイルは改竄されていると判断する）．真であった場合は，USB デバイスに対応する公開鍵で検証を継続し，最初に記録したログファイルまで検証が合格した段階

で，ログファイルは改竄されていないと判断を行う．

4　プロトタイプの開発と評価

実際にプロトタイプを用いて開発を行った．今回開発したプロトタイプは，計算量及び実用性の面で評価を行うために，セキュリティの面での評価は行わなかった．

4．1　構成

プロトタイプシステムは，下記の構成である．

（1）開発環境

Windows2000

開発言語　C#

開発ツール　VisualStudio2003 Academic Edition

（2）USBデバイスには市販のUSBメモリを用いた．USBメモリの中に（4）で用いるヒステリシス署名に必要な鍵情報及び，連鎖情報を格納した．なお，提案システムではヒステリシス署名の演算はUSBデバイス内で行うが，今回のプロトタイプではPC上で演算を行う．また，耐タンパー領域に格納するべき秘密鍵や最終ヒステリシス署名情報は，PC上のファイルとして保管した．

（3）操作者の操作記録として，アクティブウィンドウが変更される度に時刻とアクティブウィンドのタイトルをログファイルとして書き出すソフトを使用した．

（4）ログファイルの変更部分のみを抜き出して，ヒステリシス署名を行って書き出すロガープログラムを作成した．

4．2　評価

評価は表1の環境で実施した．

表1　評価環境

CPU	Pentium IV 3.2GHz
RAM	1GB
OS	Windows2000
USBメモリ	社名:株式会社バッファロー
	型番:PUF-C128M/U2
	容量:128MB

（1）正当性の検証

ヒステリシス署名を用いることで，ログファイルが改竄されていない事を証明することができる．改竄すると改竄されたことを検出することを実際に確認することができた．

デジタルフォレンジックの最も重要な事は，データが改竄されていない事の証明と，第三者によって正当性が検証できることである．その条件を十分に満たしている事が分かった．

また，ヒステリシス署名に用いた秘密鍵はUSBデバイスの耐タンパー領域にあるため，ログファイルに記録されているログデータの捏造も不可能である事から，3．2の評価指標（1）を十分満たしていると判断できる．

（2）操作記録性

本システムは，USBデバイスが差し込まれてい

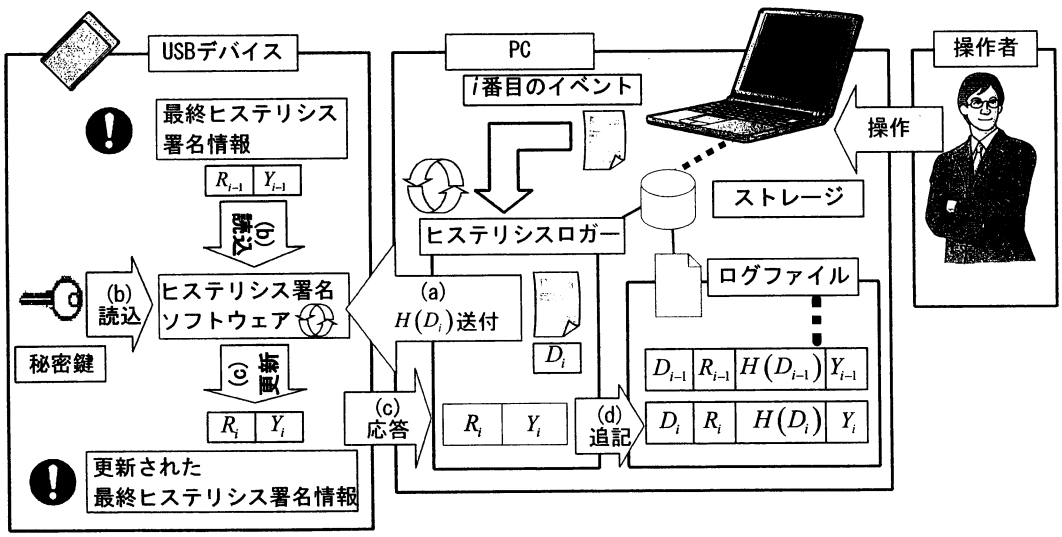

図6　処理フロー

なければ PC を操作することができない．また，USB デバイスが差し込む事により，PC のロックが解除されて操作できるようになると同時に，ヒステリシスロガーが正常に動作する条件が整う．本システムでは，USB デバイスの挿入により，操作者が操作している時に確実にログデータの採取及び記録が可能であることが分かった．

本プロトタイプでは実装していないが，USB デバイスが操作者を識別できる情報を所有していた場合は，さらに操作者を特定することも可能である．そのため，なりすましにも十分効果を発揮すると考えられる．

以上のことから，操作記録性は高いと判断した．

（３）使いやすさ

USB メモリを必ず挿さなければ，PC を利用することができないという単純なルールであるので，使用者の負担が小さいことが確認できた．

また，表 1 の評価環境で鍵長 1024 ビットで試したところ，1 回分のヒステリシス署名にかかる時間は平均して 0.18 秒であった．そのため，操作者は操作者はストレス無く利用することができる．デバイス上で暗号化するとどのくらい時間がかかるのかについては，今後，測定していく予定である．

（４）導入・運用コスト

プロタイプを開発するにあたり，ソースコードの量は 1500 ステップほどであった．また，暗号化処理モジュールは，.NET Framework に付属していたライブラリを使用した．ヒステリシス署名の機能は.NET Framework のライブラリには含まれていないため，新たに開発する必要があったが，ヒステリシス署名の構造は複雑な物ではなく，既存のライブラリの組み合わせて実現が可能だった．

また，PC のほとんどが USB インターフェースを持っていることから，本システムを導入する際に新たなインターフェースを用意する必要がないため，導入に際する新たなハードウェアを購入する必要が無い．

以上のことから，本システムの開発に必要なコストは低いとの判断に達した．

4．3　結論

従来の方式では，専用のストレージを利用する方法と暗号理論を利用したがある．専用のストレージを利用する方法として代表的なのが WORM*1 がある．この WORM は，一度書き込むと読み出ししかできない WORM 領域をストレージ上に作成する機能である．WORM 領域に入ったファイルは後から削除したり，改変することはできない．最も身近な WORM は CD-R や DVD-R のメディアが上げられる．しかしながら，これらのメディア 1 枚当たりの容量に制約があり，また，複数枚を管理する場合のファイルへのアクセシビリティは悪くなる．そのため，CD-R や DVD-R では運用コストが悪くなる．また，WORM 領域を作成できるハイエンドのストレージ装置[4]を導入するとアクセシビリティが向上する反面，WORM 機能を有したストレージ装置は大変高額である．そのため，導入コストは大変高くなってしまう．

暗号理論を利用する方式として通常のデジタル署名と，Bruce Schneier，John Kelsey が 1998 年に提案したセキュアログ方式（以下，SK 方式と略す）がある[5]．

通常のデジタル署名でも，データの正当性を検証することが可能である．しかしながら，デジタル署名は 1 つのデータにしか施す事ができない．そのため，ログデータのようにデータが次々と 1 つのファイルに追記されるようなシーンで利用する場合，ログデータがファイルに追記されるたびにログファイル全体のデジタル署名を施す必要がある．また，ファイルが次々と生成されていくようなシーンも，ファイルが追加されるたびに，デジタル署名を施す対象の全ファイルを読み込んで署名を行う必要がある．こうしたことから，通常のデジタル署名では，非常に非効率であり，デジタルフォレンジックの目的である証拠保全の観点から適用は難しい．

SK 方式は，ヒステリシス署名と同様に次々とデータが追記されていくようなシーンに適している．データの正当性の証明には，秘密鍵を必要とする MAC（Message Authentication Code）を用いる．この秘密鍵を所持した者は，全ログデータを最初から捏造することも可能であるため，論文中ではこの検証を行う者を「適度に信頼された者」としている．しかし，現実にはこのような前提が成立しない場合も少なくない．

ヒステリシス署名を用いている本提案では，検証者を，ログファイルと，ログファイルに記録された最終ログデータの情報が USB デバイス内部に記録された最終ヒステリシス署名情報の一致を

*1WORM（Write Once Read Many）読み取り専用ディスク．ストレージ装置にオプション機能として備えられている．

確認できる者であれば誰でも検証を行う事ができるとしている．また，検証者は，仮に USB デバイスを手に入れたとしても，検証前に記録されているログデータを改竄することはできない．

以上の結果から，本提案はデジタルフォレンジック保全システムとして適切であるとの結論に達した．

5　今後の展開

本稿では，プロトタイプを通じて検討を行った．今後さらに議論を深める上で，今後のロードマップを以下にまとめた．

（1）ヒステリシス署名の処理

本稿で提案するシステムは，USB デバイス内でヒステリシス署名の処理を行っている．しかし，今回開発したプロトタイプでは，PC 内部でヒステリシス署名の処理を行っている．

今後の議論を深めていく上では，USB デバイス上でヒステリシス署名を行う上で必要な要件を整理する必要がある．

（2）記録のタイミング

4．2の評価では，ヒステリシス署名に係る時間は問題ないと結論づけた．しかし，1秒間に処理できるヒステリシス署名の処理には限界がある．無理に処理しようとすると，その分 USB デバイス及び PC に負荷をかけることになる．この問題を避けるために，ログデータを一度ため込んでまとまったデータをヒステリシス署名の処理を施すと言った議論が必要となる．

（3）操作記録の範囲

プロトタイプでは，操作しているウィンドウのキャプションのみを採集していた．今後は，入力したキー情報，マウスの位置や操作情報，スクリーンショットなどもログの対象に含めるべきだろう．また，より確実な操作情報を収集するためには，ウェブの閲覧した内容や，メールの送受信内容も記録する必要がある．こうした採集するためには，アプリケーションのレベルではなく，デバイスドライバ層で情報の収集，解析，記録の処理を行う必要があると考える．

（4）ログファイルの取り扱い

ログファイルは，PC 上に記録される．そのため，通常のファイルと同様に追記，編集，削除が可能な存在である．悪意ある操作者が，ログファイルの信頼性を無くすために，1ビットの変更を加える可能性がある．この場合，ヒステリシス署名による検証が継続できないだけでなく，記録された操作記録の信頼性を無くすことが可能である．こうした問題を対処するために，ログファイルを安全な場所に待避させたり，PC 以外の場所へ転送する必要があると考える．

6　おわりに

今後のＤＦは，不正侵入者を訴える手段から，企業の説明責任を果たすための手段として活用される場が広がっていくだろう．それだけではなく，組織内のセクシャルハラスメントなどの，これまでインフォメーションテクノロジーとは無縁であった問題とも関係していくことになると考える．今回提案したシステムが，コンピュータ社会に置いて安全と安心を提供するための一つの手段になれればと期待している．

参考文献

[1] http://www.digitalforensic.jp/C-F.html

[2] http://www.cyberpolice.go.jp/column/explanation03.html

[3] 岩村充，宮崎邦彦，松本勉，佐々木良一，松木武：電子署名におけるアリバイ証明問題と経時証明問題 －ヒステリシス署名とデジタル古文書の概念－，コンピュータサイエンス誌 bit Vol.32, No.11, 共立出版（2000）

[4] http://storage-system.fujitsu.com/jp/news/sp/it_solution_2005/01/

[5] Bruce Schneier, John Kelsey “Cryptographic Support for Secure Logs on Untrusted Machine” The Seventh USENIX Security Symposium Proceedings, USENIX Press, January 1998