

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4512697号
(P4512697)

(45) 発行日 平成22年7月28日(2010.7.28)

(24) 登録日 平成22年5月21日(2010.5.21)

(51) Int.Cl. F I
 H O 4 L 9/32 (2006.01) H O 4 L 9/00 6 7 5 B
 G O 9 C 1/00 (2006.01) G O 9 C 1/00 6 4 0 D

請求項の数 4 (全 12 頁)

<p>(21) 出願番号 特願2005-347572 (P2005-347572)</p> <p>(22) 出願日 平成17年12月1日(2005.12.1)</p> <p>(65) 公開番号 特開2007-158489 (P2007-158489A)</p> <p>(43) 公開日 平成19年6月21日(2007.6.21)</p> <p>審査請求日 平成20年11月21日(2008.11.21)</p> <p>特許法第30条第1項適用 2005年7月15日 社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告 信学技報Vol.105 No.194」に発表</p> <p>特許法第30条第1項適用 2005年7月21日から22日 社団法人情報処理学会発行の「情報処理学会研究報告 情処研報Vol.2005 No.70」に発表</p>	<p>(73) 特許権者 800000068 学校法人東京電機大学 東京都千代田区神田錦町2-2</p> <p>(74) 代理人 100067541 弁理士 岸田 正行</p> <p>(74) 代理人 100087398 弁理士 水野 勝文</p> <p>(74) 代理人 100103506 弁理士 高野 弘晋</p> <p>(72) 発明者 佐々木 良一 東京都千代田区神田錦町2-2東京電機大学内</p> <p>(72) 発明者 芦野 佑樹 東京都千代田区神田錦町2-2東京電機大学内</p> <p style="text-align: right;">最終頁に続く</p>
--	---

(54) 【発明の名称】 デジタルフォレンジック保全装置

(57) 【特許請求の範囲】

【請求項1】

ログデータ (D_i 、 $i = 1 \sim n$) を生成し、ヒステリシス情報 (R_i 、 $i = 1 \sim n$) を演算する演算部と、
 前記ログデータ D_i と前記ヒステリシス情報 R_i を記録するログファイルを格納した記憶部と、を有する第1電子計算デバイスと、
 ヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) を演算する演算部と、
 該ヒステリシス署名情報 Y_i の演算時に使用する秘密鍵 (S_k) と、前記ヒステリシス署名情報 Y_i とをその耐タンパー領域に保存・格納する記憶部と、を有する第2電子計算デバイスと、
 からなるデジタルフォレンジック保全装置であって、
 前記第1電子計算デバイスの演算部は、1つ前のログデータ D_{i-1} と1つ前のヒステリシス情報 R_{i-1} と1つ前のヒステリシス署名情報 Y_{i-1} とから、一連のヒステリシス情報 (R_i 、 $i = 1 \sim n$) を演算して、前記第1電子計算デバイスのログファイルに順次保存し、
 前記第2電子計算デバイスの演算部は、前記第1電子計算デバイスから送信されたログファイルに保存された一連の前記ログデータ D_i 及び前記ヒステリシス情報 R_i に前記秘密鍵 S_k を適用して、順次前記ヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) を演算し、前記第2電子計算デバイスの記憶部の耐タンパー領域に保存すると共に、該ヒステリシス署名情報 Y_i を前記第1電子計算デバイスに返送して前記ログファイルの対応する位置に保

存し、

検証時には、前記第2電子計算デバイスの演算部は、前記第1電子計算デバイスのログファイルに保存されている一連のヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) と前記第2電子計算デバイスの記憶部に保存されているヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) とを対応する番号毎に番号の大きい方から小さい方へ順次比較し、 $i = 1$ から n までの総ての対応するヒステリシス署名情報 Y_i 及び Y_i を比較して一致を確認し、前記第1電子計算デバイスの記憶部のログファイルに保存されているヒステリシス署名情報 Y_i の総ての真偽を判断することを特徴とするデジタルフォレンジック保全装置。

【請求項2】

前記第2電子計算デバイスの記憶部の耐タンパー領域に保存されているヒステリシス署名情報 Y_i ($i = 1 \sim n$) が、最終のヒステリシス署名情報 (Y_n) のみであり、それより前のヒステリシス署名情報は、検証作業が開始された後に、前記第1電子計算デバイスから送付されてきたデータに基いて、前記第2電子計算デバイスの演算部で演算され、その演算されたヒステリシス署名情報 Y_i ($i = 1 \sim (n-1)$) と、前記第1電子計算デバイスの対応する番号のヒステリシス署名情報 Y_i ($i = 1 \sim (n-1)$) とを比較するものであることを特徴とする請求項1に記載のデジタルフォレンジック保全装置。

10

【請求項3】

前記第1電子計算デバイスと第2電子計算デバイスのうち少なくとも第2電子計算デバイスは、ヒステリシス署名情報の検証時を除き特定の操作者が占有するものであることを特徴とする請求項1または2に記載のデジタルフォレンジック保全装置。

20

【請求項4】

前記第1電子計算デバイスがパーソナルコンピュータであり、前記第2電子計算デバイスがUSBデバイスであり、該USBデバイスと該パーソナルコンピュータの接続部を相互に接続した場合に、該パーソナルコンピュータとUSBデバイスの操作および動作または検証作業が可能となることを特徴とする請求項1乃至3に記載のデジタルフォレンジック保全装置。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、コンピュータやネットワーク等の資源および環境の不正使用、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への対応等を行うデジタルフォレンジックに関する。

30

【背景技術】

【0002】

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り、これらのデジタルデータに証拠性を確保し、訴訟等に備えるための技術や社会的仕組みが要求されるようになってきた。これらはデジタル・フォレンジック (Digital Forensic、以下「DF」という。) と呼ばれるものであるが、DFとはインシデント・レスポンス (コンピュータやネットワーク等の資源および環境の不正使用、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等への対応等をいう。) や法的紛争・訴訟に対し、電磁的記録の証拠保全および調査・分析を行うとともに、電磁的記録の改竄・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・技術をいい、今後企業の説明責任の範囲が増大していくことから、財務会計情報など情報改竄等を行っていない証拠性を確保し、訴訟に持込まれてもよいようにしておくことが大切となる。

40

【0003】

従来、デジタルデータの改竄を防止する技術としては、デジタル署名生成者は、署名対象となるデジタル化されたデータあるいはその特徴値 (圧縮値であるハッシュ値に、自分自身が秘密裏に保持する秘密鍵を作用させることで、データMに対するデジタル署名Aを生成する。そして、データMに付されたデジタル署名Aを上記秘密鍵と対の公開鍵を作用

50

させることで得た結果と、データMあるいはそのハッシュ値とを比較し、両者が一致しない場合には、デジタル署名Aが生成された後にデータMに何らかの改竄が加えられた可能性があるため、両者が一致する場合に限り、デジタル署名AがデータMに対してなされたものであることを認証できるという、いわゆるデジタル署名方式が使用されている。

【0004】

また、デジタル署名生成者が、自分自身が生成したデータに特殊な情報を加えて、デジタル署名の不正な生成を行うことを防止するため、デジタル署名生成者は、署名対象となるデータ M_n あるいはそのハッシュ値と1つ前に生成したデジタル署名 A_{n-1} の生成に関わる情報と時刻データに、自分自身が秘密裏に保持する秘密鍵を作用させることで、データ M_n に対するデジタル署名 A_n を生成し、デジタル署名 A_n の次に生成されるデジタル署名 A_{n+1} には、1つ前に生成したデジタル署名 A_n の生成に関わる情報が反映されることにより、デジタル署名生成者が自分自身が生成した別のデータ M_n を加えて新たにデジタル署名 A_n を生成し、これらを元のデータ M_n およびデジタル署名 A_n と置き換えるような不正な行為を行うと、デジタル署名 A_{n+1} との間で整合が取れなくなりデータの改竄が防止されるという、いわゆるヒステリシス署名方式も採用されている。

10

【0005】

また、下記特許文献1には、生成したデジタル署名とデータを含むデジタル署名付きデータの配布に先立ち、当該デジタル署名付きデータのログデータをログリストに登録し、デジタル署名検証者がデジタル署名生成者からログリストを入手し、検証すべきデジタル署名付きデータのログデータが前記ログリストに登録されているか否かを調べることで、当該検証すべきデジタル署名付きデータが前記デジタル署名生成者により配布されたものであるか否かを検証する方法が示されている。

20

【0006】

さらに、下記特許文献2には、デジタル署名に複数のログデータの情報を取り込んで、生成してログテーブルに登録し、ログテーブルにおけるログデータの連鎖を検証する際には、複数のログデータに登録されているリンク情報をもとに、破損していない他のログデータの整合性から検証するもので、利用者が他の利用者のログリストによる補間やサービス提供機関を利用することなく、一部のログデータが欠落しても、ログリストの連鎖構造を用いたログデータの検証が可能となるものが示されている。

【特許文献1】特開2001-331104号公報

30

【特許文献2】特開2005-12490号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、上記のいわゆるデジタル署名方式では、データにデジタル署名生成者自身が何らかの改竄を加えて新たにデジタル署名を生成して、元のデータおよびデジタル署名と置き換えるような不正な行為を防止することができない。また、いわゆるヒステリシス署名方式ではログデータを登録したログリストの完全な保存が必須とされ、ログデータに欠落した部分があると、ログリストにあるログデータの連鎖を利用しているため、他の正当なログデータの検証に支障が生じることになる。また上記特許文献1に示された方式では、利用者間の手間、サービス提供機関の不在、検証時間が長くなるという問題がある。

40

【0008】

また、上記特許文献2に記載された方法は、プログラムが複雑になり、またログデータの真正性を確かめるための検証時間が長くなるという問題があり、上述したいずれの従来方法を使用しても、(1)サーバやPC等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、応急処置をすると共に証拠となり得る情報を保存し、(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)誰が侵入者か等を分析し、(3)その後自分が行う訴訟等に備えるには不十分であった。

【0009】

50

また、今後は、(1)サーバやPC等のコンピュータだけでなく、情報家電や携帯電話、ネットワーク等を対象とした証拠性の確保も重要な対象となる。(2)不正侵入の証拠だけでなく、(a)財務会計情報などの改竄や、(b)個人情報や機密情報などの漏洩、(c)詐欺等の不正行為がなかったかの証拠性も大切となり、企業の透明性を確保し、説明責任を問われるケースが多くなることが予想される。(3)自分が訴訟に持込む場合だけでなく、訴訟に持込まれても良いようにすることも大切になる。そして、訴訟に持込まれても良くするには、(a)処理をすれば記録が残るようにするとともに、(b)改竄していないことを証明できる簡単な装置の確保が不可欠となる。

【0010】

本発明はこのような状況に鑑みてなされたものであり不正アクセス等の攻撃に対処し、デジタル情報の科学的証拠性を確保し、訴訟等に備えるたことのできる装置を提供することにある。

【課題を解決するための手段】

【0011】

上記の課題を解決する第1発明は、ログデータ(D_i、i=1~n)を生成し、ヒステリシス情報(R_i、i=1~n)を演算する演算部と、ログデータD_iとヒステリシス情報R_iを記録するログファイルを格納した記憶部とを有する第1電子計算デバイスと、ヒステリシス署名情報(Y_i、i=1~n)を演算する演算部と、ヒステリシス署名情報Y_iの演算時に使用する秘密鍵(S_k)と、ヒステリシス署名情報Y_iとをその耐タンパー領域に保存・格納する記憶部とを有する第2電子計算デバイスとからなるデジタルフォレンジック保全装置であって、第1電子計算デバイスの演算部は、1つ前のログデータD_{i-1}と1つ前のヒステリシス情報R_{i-1}と1つ前のヒステリシス署名情報Y_{i-1}とから、一連のヒステリシス情報(R_i、i=1~n)を演算して、第1電子計算デバイスのログファイルに順次保存し、第2電子計算デバイスの演算部は、第1電子計算デバイスから送信されたログファイルに保存された一連のログデータD_i及びヒステリシス情報R_iに秘密鍵S_kを適用して、順次ヒステリシス署名情報(Y_i、i=1~n)を演算し、第2電子計算デバイスの記憶部の耐タンパー領域に保存すると共に、ヒステリシス署名情報Y_iを第1電子計算デバイスに返送してログファイルの対応する位置に保存し、検証時には、第2電子計算デバイスの演算部は、第1電子計算デバイスのログファイルに保存されている一連のヒステリシス署名情報(Y_i、i=1~n)と第2電子計算デバイスの記憶部に保存されているヒステリシス署名情報(Y_i、i=1~n)とを対応する番号毎に番号の大きい方から小さい方へ順次比較し、i=1からnまでの総ての対応するヒステリシス署名情報Y_i及びY_iを比較して一致を確認し、第1電子計算デバイスの記憶部のログファイルに保存されているヒステリシス署名情報Y_iの総ての真偽を判断することを特徴とするデジタルフォレンジック保全装置である。

【0012】

第2発明は、第1発明において、前記第2電子計算デバイスの記憶部の耐タンパー領域に保存されているヒステリシス署名情報(Y_i、i=1~n)が、最終のヒステリシス署名情報(Y_n)のみであり、それより前のヒステリシス署名情報は、検証作業が開始された後に、前記第1電子計算デバイスから送付されてきたデータに基づいて、前記第2電子計算デバイスの演算部で演算され、その演算されたヒステリシス署名情報(Y_i、i=1~(n-1))と、前記第1電子計算デバイスの対応する番号のヒステリシス署名情報(Y_i、i=1~(n-1))とを比較するものであることを特徴とする請求項1に記載のデジタルフォレンジック保全装置である。

【0013】

第3の発明は、第1または第2発明において、前記第1電子計算デバイスと第2電子計算デバイスのうち少なくとも第2電子計算デバイスは、ヒステリシス署名情報の検証時を除き特定の操作者が占有するものであることを特徴とする請求項1または2に記載のデジタルフォレンジック保全装置である。

【 0 0 1 4 】

第4の発明は、第1乃至第3の発明において、前記第1電子計算デバイスがパーソナルコンピュータであり、前記第2電子計算デバイスがUSBデバイスであり、該USBデバイスと該パーソナルコンピュータの接続部を相互に接続した場合に、該パーソナルコンピュータとUSBデバイスの操作および動作または検証作業が可能となることを特徴とする請求項1乃至3に記載のデジタルフォレンジック保全装置である。

【発明の効果】

【 0 0 1 5 】

第1発明は、ログデータ (D_i 、 $i = 1 \sim n$) を生成し、ヒステリシス情報 (R_i 、 $i = 1 \sim n$) を演算する演算部と、前記ログデータとヒステリシス情報を記録するログファイル 10 を格納した記憶部を有する第1電子計算デバイスと、ヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) を演算する演算部と、該ヒステリシス署名情報の演算時に使用する秘密鍵 (S_k) と、前記ヒステリシス署名情報と前記秘密鍵とをその耐タンパー領域に保存・格納する記憶部とを有する第2電子計算デバイスとからなるデジタルフォレンジック保全装置であって、前記第1電子計算デバイスで生成された前記ログデータに基づく一連のヒステリシス情報 (R_i 、 $i = 1 \sim n$) を前記第1電子計算デバイスのログファイルに順次保存し、前記第2電子計算デバイスにおいて、前記第1電子計算デバイスから送付されたログファイルに保存された一連のデータに前記秘密鍵を適用して、順次前記ヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) を演算し、前記記憶部の耐タンパー領域に保存すると共に、該ヒステリシス署名情報を前記第1電子計算デバイスに返送して前記ログファイルの対応する位置に保存し、検証時には、前記第1電子計算デバイスのログファイルに保存されている一連のヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) と前記第2電子計算デバイスの記憶部に保存されているヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) とを対応する番号毎に 20 順次、比較し、 $i = 1$ から n までの総ての対応するヒステリシス署名情報を比較して、前記第1電子計算デバイスの記憶部のログファイルに保存されているヒステリシス署名情報の総ての真偽が判断されることを特徴とするデジタルフォレンジック保全装置であり、ヒステリシス署名方式が採用され、かつ秘密鍵とヒステリシス署名情報が格納・保存される領域は何人も侵入することのできない第2電子計算デバイスの耐タンパー領域であるから、捏造が不可能であり、改竄されないという効果がある。また従来のデジタル署名の場合は、1つの情報にしか署名ができないので、ログデータのように情報が次々と1つのファイルに追記される場合には、ログデータがファイルに追加されるたびに、デジタル署名を 30 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が、本発明においては、ヒステリシス署名を適用しているので、その必要がなく、従来のデジタル署名と比較して効率が良い。またヒステリシス署名の構造は比較的単純であって、既存のライブラリーを組合わせて実現可能であり、導入コストも運用コストと低いという効果がある。さらに、ヒステリシス署名を適用しているので、検証者が、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。さらに検証時間も短いという効果がある。

【 0 0 1 6 】

第2発明は、第1発明において、前記第2電子計算デバイスの記憶部の耐タンパー領域に保存されているヒステリシス署名情報 (Y_i 、 $i = 1 \sim n$) が、最終のヒステリシス署名情報 (Y_n) のみであり、それより前のヒステリシス署名情報は、検証作業が開始された後に、前記第1電子計算デバイスから送付されてきたデータに基づいて、前記第2電子計算デバイスの演算部で演算され、その演算されたヒステリシス署名情報 (Y_i 、 $i = 1 \sim (n - 1)$) と、前記第1電子計算デバイスの対応する番号のヒステリシス署名情報 (Y_i 、 $i = 1 \sim (n - 1)$) とを比較するものであることを特徴とするデジタルフォレンジック保全装置であるから、第1の発明の効果に加えて、第2電子計算デバイスの記憶部の容量を小さくでき、デバイスの簡素化が可能となる。特に、第2電子計算デバイスをUSBデバイスとする場合に効果が大きい。

【 0 0 1 7 】

10

20

30

40

50

第3の発明は、第1または第2発明において、前記第1電子計算デバイスと第2電子計算デバイスのうち少なくとも第2電子計算デバイスは、ヒステリシス署名情報の検証時を除き特定の操作者が占有するものであることを特徴とするデジタルフォレンジック保全装置であり、第4の発明は、第1乃至第3の発明において、前記第1電子計算デバイスがパーソナルコンピュータであり、前記第2電子計算デバイスがUSBデバイスであり、該USBデバイスと該パーソナルコンピュータの接続部を相互に接続した場合に、該パーソナルコンピュータとUSBデバイスの操作および動作または検証作業が可能となることを特徴とするデジタルフォレンジック保全装置であるから、第1または第2の発明の効果に加えて、操作者が、第2電子計算デバイスまたはUSBデバイスを適正に管理する限り、第3者はPCを操作することができないので、第3者によって、ログデータの窃取および改竄がされることがなく、操作者の管理上の負担、第3者によって、改竄されるかもしれないという精神的負担が軽減される。特に操作者の暗号番号を併用する場合はなりすましに対してより十分な効果を有する。

10

【0018】

また、第4の発明の場合は、既存のハードウェアの活用であるから、装置の購入費、さらには運用コストが小さくなり導入が容易となるという効果がある。

【発明を実施するための最良の形態】

【0019】

以下、本発明の実施の形態を図面に基づいて説明する。

【0020】

20

図1は本発明の実施の形態に係るDF保全装置の構成の概要の説明図である。

図1において、10は操作者、20はパーソナルコンピュータ(以下「PC」という。)、30はUSBデバイスであり、操作者10はUSBデバイス30を占有する。

【0021】

PC 20には、演算部(ヒステリシスロガー等)21、記憶部22を有し、記憶部22にはログファイル221、ログプログラム222、テンポラリーファイル223が格納されている。操作者がPC 20を操作すると、演算部(ヒステリシスロガー等)21でログデータ(D_i 、 $i = 1 \sim n$)が作成され、ログデータはテンポラリーファイルに223に記録される。演算部21はさらにテンポラリーファイルに記録されたログデータを使用し、ログプログラム222を引出して、ログデータ D_i のハッシュ値 $H(D_i)$ 、ヒステリシス情報 R_i を生成しログファイル221に順次記録・保存する。なお、演算部21は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でもよい。

30

【0022】

USBデバイス30は演算部31と記憶部32を有し、記憶部32には秘密鍵(S_k)321と更新された最終ヒステリシス情報(Y_n 、 $i = n$)322とプログラム323が格納されている。演算部31は、プログラム323を引出しPC 20から送付されてきたデータに対してヒステリシス署名(Y_i)を行う。

【0023】

記憶部32のプログラム323の格納された領域はアクセス可能領域(Z)であるが、秘密鍵(S_k)321と更新された最終のヒステリシス署名情報(Y_n)322とが格納されている領域は、物理的に守られた操作者10でもアクセスできない耐タンパー領域(X)である。

40

【0024】

USBデバイス20を占有している操作者10は、PC 10を操作する時に、PC 10にUSBデバイスを差込んで操作し、操作が終了した後にUSBデバイスを抜く。USBデバイスが挿入されていない時には、機械的またはプログラムによりPCの操作ができない。なお、本実施の形態においては、(a)USBデバイス内の耐タンパー領域内の更新された最終のヒステリシス署名情報は抽出及び改竄が不可能であり、(b)PC上で動作するログプログラムは改竄されていないことを前提とする。

50

【 0 0 2 5 】

図 2 は本発明の実施の形態に係る D F 保全装置におけるヒステリシス署名情報等の演算・保存処理のフォローの説明図であり、図 3 は図 2 における各種データの生成、保存の詳細説明図である。図 2、3 に基いて、ヒステリシス署名の処理のフォローを説明する。

(作業 1) 操作者 1 0 は P C 1 0 と U S B デバイス 3 0 を準備してヒステリシス署名の作業をスタートする。

(作業 2) 操作者 1 0 が U S B デバイス 3 0 を P C 2 0 に差込む。ヒステリシス署名の作業は、操作者 1 0 自身が占有している U S B デバイス 3 0 を P C 2 0 に差込むことが前提となり、U S B デバイス 3 0 が P C 1 0 に差込む前は、P C 2 0 はロックされており何人も操作することができない。

(作業 3) 操作者 1 0 がキーボード 2 4 を操作することにより、P C 2 0 内の演算部 (ヒステリシスロガー等) 2 1 でログデータ D_i が生成されテンポラリーファイル 2 2 3 に記録される。(図 2 (作業 4))

(作業 5) 操作者 1 0 は、ログデータ D_i がテンポラリーファイル 2 2 3 に記録されたら、キーボードを操作して演算ウインドーに切替える。

(作業 6) 演算部 2 1 でログデータ D_i のハッシュ値 $H(D_i)$ と、ログファイルの中から 1 つ前 ($i-1$ 番目) のデータ R_{i-1} 、 $H(D_{i-1})$ 、 Y_{i-1} を使用してヒステリシス情報 $R_i = H(R_{i-1}, H(D_{i-1}), Y_{i-1})$ が演算される。

(作業 7) R_i 、 $H(D_i)$ が U S B デバイス 3 0 に送付される。

(作業 8) 同時に、 D_i 、 R_i 、 $H(D_i)$ がログファイル 2 2 1 に保存される。

(作業 9) U S B デバイス 3 0 の演算部 3 1 に、プログラム 3 2 3 と秘密鍵 (S_K) 3 2 1 が読み込まれ、P C 2 0 から送付された R_i と $H(D_i)$ を使用してヒステリシス署名情報 $Y_i = S_K(R_i, H(D_i))$ が演算される。この場合、さらに機密性を高めるために、 R_i 、 $H(D_i)$ のハッシュ値を使用して、 $Y_i = S_K(H(R_i, H(D_i)))$ としてもよい。

(作業 1 0) ヒステリシス署名情報 (Y_i) は 1 つ前のヒステリシス署名情報 (Y_{i-1}) に上書きされ最終ヒステリシス署名情報 (Y_n) となる。

(作業 1 1) また、ヒステリシス署名情報 (Y_i) は P C 2 0 に送付され、ログファイル 2 2 1 に追記・保存される。

(作業 1 2) ログデータの署名処理が総て終了したか (即ち、 $i=n$ となったか) 確認される。

(作業 1 3) ログデータの署名作業が終了していない場合には、処理番号を 1 つ繰り上げて i 番を $i+1$ 番として (作業 6) 以降の作業を繰り返す。上記フローが U S B デバイスが差込まれている間続けられる。

(作業 1 4) ログデータの署名処理が総て終了したとき、操作者 1 0 が U S B デバイス 3 0 を抜くと P C 1 0 の動作は終了する。

【 0 0 2 6 】

次に、ログファイル 2 2 1 に記録されたヒステリシス署名情報の検証処理について説明する。

【 0 0 2 7 】

図 4 は本発明の実施の形態に係る D F 保全装置におけるのヒステリシス署名情報の検証のフォローの説明図であり、図 5 は図 4 における各種データの検証に係る演算・比較の詳細説明図である。図 2、3 に基き、また図 1 を参照しながら、ヒステリシス署名の検証処理のフォローを説明する。

(作業 1) 検証者 5 0 は P C 2 0 と操作者 1 0 の占有する U S B デバイスを受取り、P C 2 0 を検証モードに切換えて検証作業をスタートする。

(作業 2) 検証者 5 0 は U S B デバイスを P C 2 0 に差込む。この場合、P C 2 0 から検証しようとする情報のみをフロッピー (登録商標)、C D 等にコピーして、他の P C を使用して検証するようにしてもよい。

(作業 3) P C 2 0 からログファイル 2 2 1 に保存されている最終のヒステリシス署名情報 Y_n が U S B デバイス 3 0 に送付される。

(作業4) USBデバイス30の演算部31において、PC20から送られてきた最終のヒステリシス署名情報 Y_n と耐タンパー領域に格納されている最終のヒステリシス署名情報(Y_n)とを比較する。

(作業5)作業4の結果、 Y_n と Y_n とが不一致($Y_n \neq Y_n$)の場合は、USBデバイスはヒステリシス署名情報(Y_n)に不正の可能性があるとして判断して、PC10に対して偽の表示を返す。

(作業6) Y_n と Y_n とが一致($Y_n = Y_n$)する場合は、 R_{n-2} と $H(D_{n-2})$ と Y_{n-2} を使用して、PC10の演算部で $R_{n-1} = H(R_{n-2}, H(D_{n-2}), Y_{n-2})$ が演算され、これに加えて $H(D_{n-1})$ がPC20からUSBデバイスに送付される。

10

(作業7)USBデバイス30の演算部において、PC20から送られてきた R_{n-1} と $H(D_{n-1})$ に秘密鍵 S_K を使用して、 $Y_{n-1} = S_K(R_{n-1}, H(D_{n-1}))$ を演算される。

(作業8)PC20からヒステリシス署名情報 Y_{n-1} がUSBデバイスに送付される。

(作業9)PC20から送られてきたヒステリシス署名情報 Y_{n-1} と作業7において演算した Y_{n-1} とを比較する。

【0028】

作業9の結果、 Y_{n-1} と Y_{n-1} とが不一致($Y_{n-1} \neq Y_{n-1}$)の場合はUSBデバイス30はヒステリシス署名情報 Y_{n-1} は不正の可能性があるとして判断し、PC10に対して偽の表示を返す。(作業5)。

20

(作業10) Y_{n-1} と Y_{n-1} とが一致($Y_{n-i} = Y_{n-i}$ 、 $i=1$)する場合は、総ての検証が終了したか($n-i=1$ か)を確認する。

(作業11)すべての作業が終わっていない場合には、さらに1つ前に戻り($i=i+1$)、作業6以降の作業を繰り返す。

(作業12)総てのヒステリシス署名情報($Y_n \sim Y_1$)が一致した場合、即ち最初に記録したログファイルまで検証が真と判断されたときに、PC20の全ヒステリシス署名情報は加筆、修正、削除等の改竄されていないことになる。

(作業13)総てのヒステリシス署名情報の検証がなされ、真または偽の判断がなされたところで作業は終了し、検証者50がPC20からUSBデバイス30を抜くことによりPC10の動作は終了する。

30

【0029】

上述の通り、本実施の形態により、(1)記録された情報が加筆、修正、削除等の改竄が行われていないことが第三者によって検証できる。

(2)また、総ての操作記録が残り、操作に関する総て情報を収集できるので、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、それが故意によるものなのか、プログラムによるものなのか、PCの操作記録を可能な限り収集し、操作者の意図を知ることができる。

(3)使い易くなければ、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が、本実施の形態に係るシステムを導入することにより、操作者のパフォーマンスが大幅に低下したり、操作範囲に制約が生じることはない。評価環境として、CPU: Pentium(登録商標) IV3.2GHz、RAM: 1GB、OS: Windows(登録商標) 2000、USBメモリ: 株式会社バッファロー(型番PUF-C128M/U2)、容量 128MB、鍵長1024ビットで検証した結果、1回分のヒステリシス署名に要する時間は、平均して0.2秒除弱であり、検証者に大きな負担が掛かることはなかった。

40

(4)従来のソリューションと異なり、導入・運用コストが低く、資金に余裕のない中小の企業でも実施できる。

【0030】

なお、本実施の形態においては、USBデバイス30には最終のヒステリシス署名情報(Y_n)のみを保存することになっているが、ヒステリシス署名情報の総て($Y_1 \sim Y_n$)を保存し、これらと、PC10のログファイル221に保存されているヒステリ

50

シス署名情報 ($Y_1 \sim Y_n$) を比較検証するようにしてもよい。

【図面の簡単な説明】

【0031】

【図1】本発明の実施の形態に係るDF保全装置の構成の概要の説明図である。

【図2】本発明の実施の形態に係るDF保全装置におけるヒステリシス署名情報等の演算・保存処理のフォローの説明図である。

【図3】図2における各種データの演算・保存の詳細説明図である。

【図4】本発明の実施の形態に係るDF保全装置におけるのヒステリシス署名情報の検証のフォローの説明図である。

【図5】図4における各種データの検証に係る演算・比較の詳細説明図である。

10

【符号の説明】

【0032】

100・・・DF保全装置

10・・・操作者

20・・・PC(第1電子計算デバイス)

21・・・演算部(ヒステリシスロガー等)

22・・・記憶部

221・・・ログファイル

222・・・ログプログラム

223・・・テンポラリーファイル

20

30・・・USBデバイス

31・・・演算部

32・・・記憶部

321・・・秘密鍵(SK)

322・・・更新された最終ヒステリシス情報(Y_n)

323・・・プログラム

X・・・耐タンパー領域

Z・・・アクセス領域

50・・・検証者

D_i ・・・ i 番目のログデータ

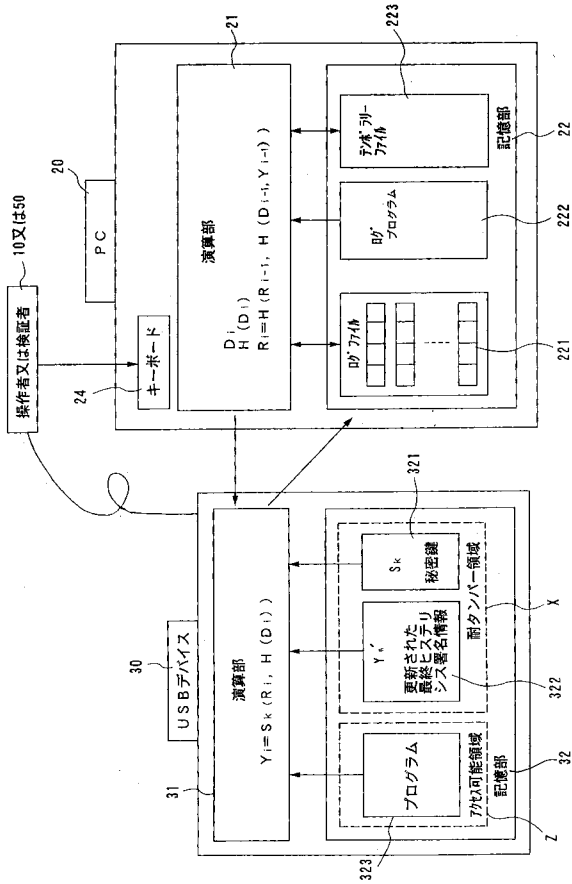
30

R_i ・・・ i 番目のヒステリシス情報

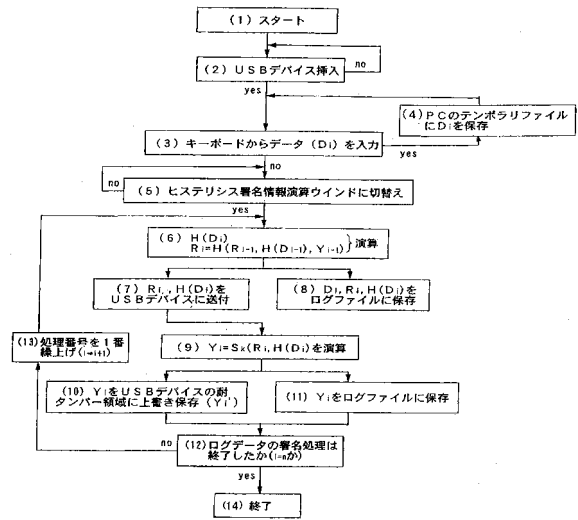
$H(x)$ ・・・ x のハッシュ値

Y_i ・・・ i 番目のヒステリシス署名情報(PCのログファイルに保存)

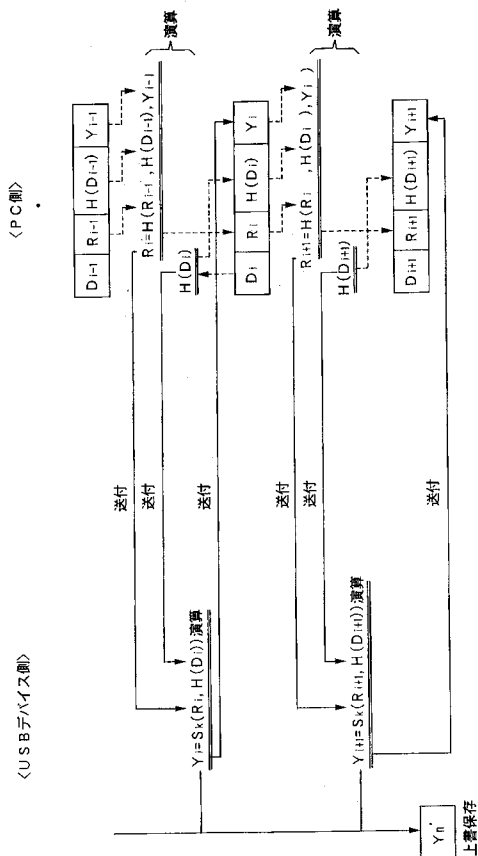
【図1】



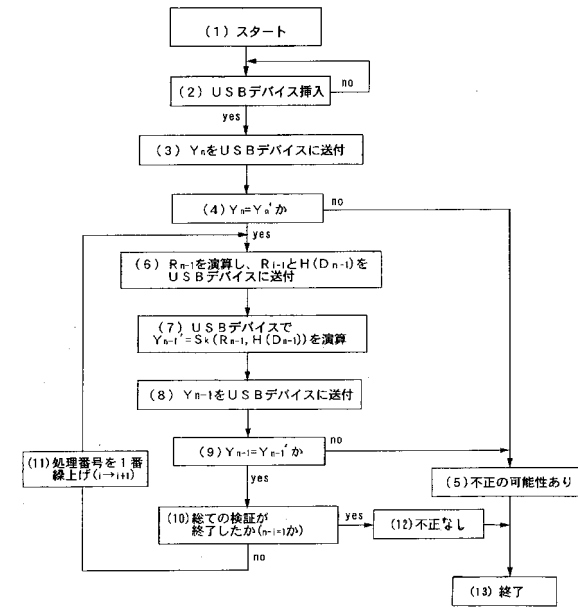
【図2】



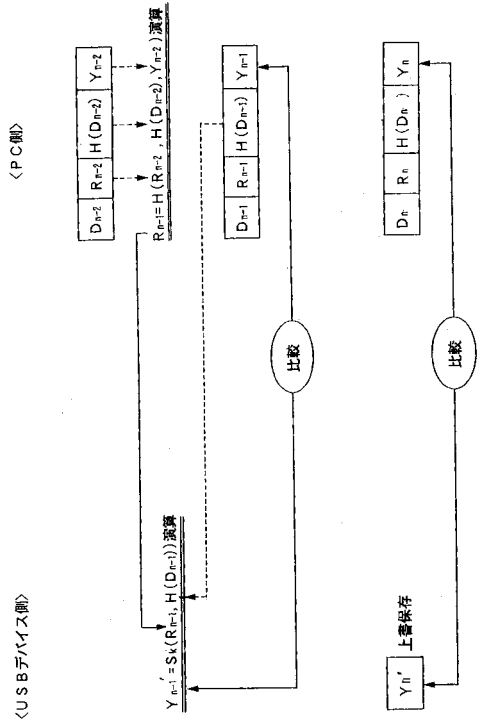
【図3】



【図4】



【 図 5 】



 フロントページの続き

- (72)発明者 粉川 寛人
東京都千代田区神田錦町 2 - 2 東京電機大学内
- (72)発明者 佐藤 吏
東京都千代田区神田錦町 2 - 2 東京電機大学内

審査官 松平 英

- (56)参考文献 川口 信隆 Nobutaka KAWAGUCHI, フォレンジックコンピューティングのための安全で効率的なロギングアーキテクチャの提案 Secure Efficient Logging Architecture for Forensic Computing, 情報処理学会研究報告 Vol. 2003 No. 126 IPSJ SIG Technical Reports, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2003年12月19日, 第2003巻 第126号, p. 7~12
- 小畑 直裕 Naohiro OBATA, フォレンジックコンピューティングのための効率的なログ署名手法の提案 Efficient log authentication for Forensic Computing, 情報処理学会研究報告 Vol. 2005 No. 58 IPSJ SIG Technical Reports, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2005年6月3日, 第2005巻 第58号, p. 31~36
- 篠田 光秋 Mitsuaki Shinoda, 紙文書を伴うヒステリシス署名システムの提案と評価 Proposal and evaluation of hysteresis signature system with paper document, 情報処理学会研究報告 Vol. 2003 No. 74 IPSJ SIG Technical Reports, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2003年7月18日, 第2003巻 第74号, p. 77~82
- 上田 祐輔 YUSUKE UEDA, データ喪失を想定したヒステリシス署名方式評価手法の提案 Evaluation Method Supposing Data Loss for Hysteresis Signature Systems, 情報処理学会論文誌 第45巻 第8号 IPSJ Journal, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2004年8月15日, 第45巻 第8号, p. 1966~1976
- 洲崎 誠一 Seiichi Susaki, 暗号ブレイク対応電子署名アリバイ実現機構(その2) - 詳細方式 - Alibi Establishment for Electronic Signatures: How to prove that you did not make the electronic signature in question even when the base cryptosystem was collapsed Part 2. Concrete Schemes and Evaluation, 情報処理学会研究報告 Vol. 2000 No. 30 IPSJ SIG Notes, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2000年3月22日, 第2000巻 第30号, p. 19~24
- 洲崎 誠一 SEIICHI SUSAKI, 電子署名アリバイ実現機構 - ヒステリシス署名と履歴交差 Alibi Establishment for Electronic Signatures, 情報処理学会論文誌 第43巻 第8号 IPSJ Journal, 日本, 社団法人情報処理学会 Information Processing Society of Japan, 2002年8月15日, 第43巻 第8号, p. 2381~2393

(58)調査した分野(Int.Cl., DB名)

H04L	9/00
G09C	1/00
H04K	1/00