(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-158489
(P2007-158489A)
(43)公開日　平成19年6月21日(2007.6.21)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 未請求　請求項の数 4　OL　（全 12 頁）

(21)出願番号　特願2005-347572 (P2005-347572)
(22)出願日　平成17年12月1日 (2005.12.1)

特許法第３０条第１項適用申請有り　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

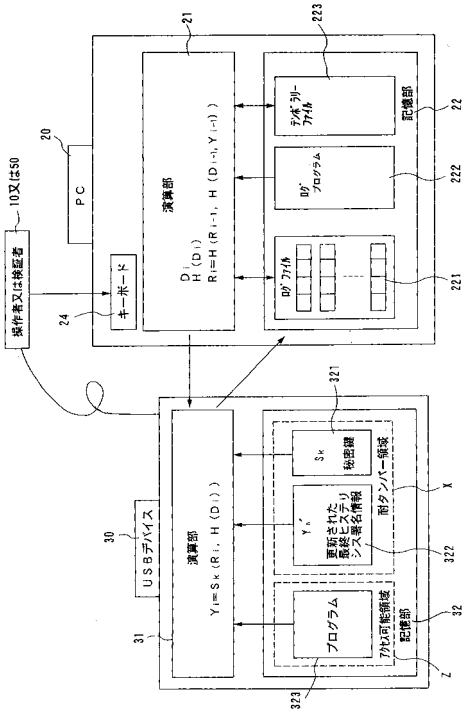
特許法第３０条第１項適用申請有り　２００５年７月２１日から２２日　社団法人情報処理学会発行の「情報処理学会研究報告　情処研報Ｖｏｌ．２００５　Ｎｏ．７０」に発表

(71)出願人　800000068
学校法人東京電機大学
東京都千代田区神田錦町２－２
(74)代理人　100067541
弁理士　岸田　正行
(74)代理人　100087398
弁理士　水野　勝文
(74)代理人　100103506
弁理士　高野　弘晋
(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
(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

最終頁に続く

(54)【発明の名称】デジタルフォレンジック保全装置

(57)【要約】
【課題】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を行う。
【解決手段】ヒステリシス署名方式を使用し、ログデータ（D_i）の生成・保存、ヒステリシス情報（R_i）の演算・保存、ヒステリシス署名情報（Y_i）の保存を行うＰＣ ２０と、ヒステリシス署名情報（Y_i）の演算・保存をするＵＳＢデバイス３０とからなり、ＵＳＢデバイス３０に保存されているヒステリシス署名情報（Y_i'）と、ＰＣ １０に保存されてステリシス署名情報（Y_i）とを比較し、対応する総てのヒステリシス署名情報が一致する場合には、ヒステリシス署名情報は真とし、いずれかのヒステリシス署名情報が不一致の場合には、ヒステリシス署名情報は偽とする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
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、
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～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～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～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～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～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。
【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～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～（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。
【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。
【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。
【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。

【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。

【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。

【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
【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。

【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】
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い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、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～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～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～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～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～ｎ）とを対応する番号毎に順次、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。
【００１４】
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】
【００１５】
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、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～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～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～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～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～ｎ）とを対応する番号毎に順次、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よい。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かいという効果がある。

【００１６】

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。

【００１７】

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充分な効果を有する。

【００１８】

また、第４の発明の場合は、既存のハードウエ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】

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～ｎ）が作成され、ログデータはテンポラリファイルに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。

【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。

【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。

【００２５】

図２は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１０はＰＣ １０とＵＳＢデバイス３０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１０がＵＳＢデバイス３０をＰＣ ２０に差込む。ヒステリシス署名の作業は、操作者１０自身が占有しているＵＳＢデバイス３０をＰＣ ２０に差込むことが前提となり、ＵＳＢデバイス３０がＰＣ １０に差込む前は、ＰＣ ２０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１０がキーボード２４を操作することにより、ＰＣ ２０内の演算部（ヒステリシスロガー等）２１でログデータD_iが生成されテンポラリーファイル２２３に記録される。（図２（作業４））

（作業５）操作者１０は、ログデータD_iがテンポラリーファイル２２３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２１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ＵＳＢデバイス３０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２２１に保存される。

（作業９）ＵＳＢデバイス３０の演算部３１に、プログラム３２３と秘密鍵（S_K）３２１が読込まれ、ＰＣ ２０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１０）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１１）また、ヒステリシス署名情報（Y_i）はＰＣ ２０に送付され、ログファイル２２１に追記・保存される。

（作業１２）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１３）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）以降の作業を繰返す。上記フローがＵＳＢデバイスが差込まれている間続けられる。

（作業１４）ログデータの署名処理が総て終了したとき、操作者１０がＵＳＢデバイス３０を抜くとＰＣ １０の動作は終了する。

【００２６】

次に、ログファイル２２１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。

【００２７】

図４は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５０はＰＣ ２０と操作者１０の占有するＵＳＢデバイスを受取り、ＰＣ ２０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５０はＵＳＢデバイスをＰＣ ２０に差込む。この場合、ＰＣ ２０から検証しようとする情報のみをフロッピー（登録商標）、ＣＤ等にコピーして、他のＰＣを使用して検証するようにしてもよい。

（作業３）ＰＣ ２０からログファイル２２１に保存されている最終のヒステリシス署名情報Y_nがＵＳＢデバイ３０に送付される。

（作業４）ＵＳＢデバイス３０の演算部３１において、ＰＣ ２０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判断して、ＰＣ １０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、ＰＣ １０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ＰＣ ２０からＵＳＢデバイスに送付される。

（作業７）ＵＳＢデバイス３０の演算部において、ＰＣ ２０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）ＰＣ ２０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）ＰＣ ２０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判断し、ＰＣ １０に対して偽の表示を返す。（作業５）。

（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以降の作業を繰返す。

（作業１２）総てのヒステリシス署名情報（Y_n～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、ＰＣ ２０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ＰＣ ２０からＵＳＢデバイス３０を抜くことによりＰＣ １０の動作は終了する。

【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３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、操作者のパー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。
（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しているが、ヒステリシス署名情報の総て（Y_1'～Y_n'）を保存し、これらと、ＰＣ　１０のログファイル２２１に保存されているヒステリシス署名情報（Y_1～Y_n）を比較検証するようにしてもよい。

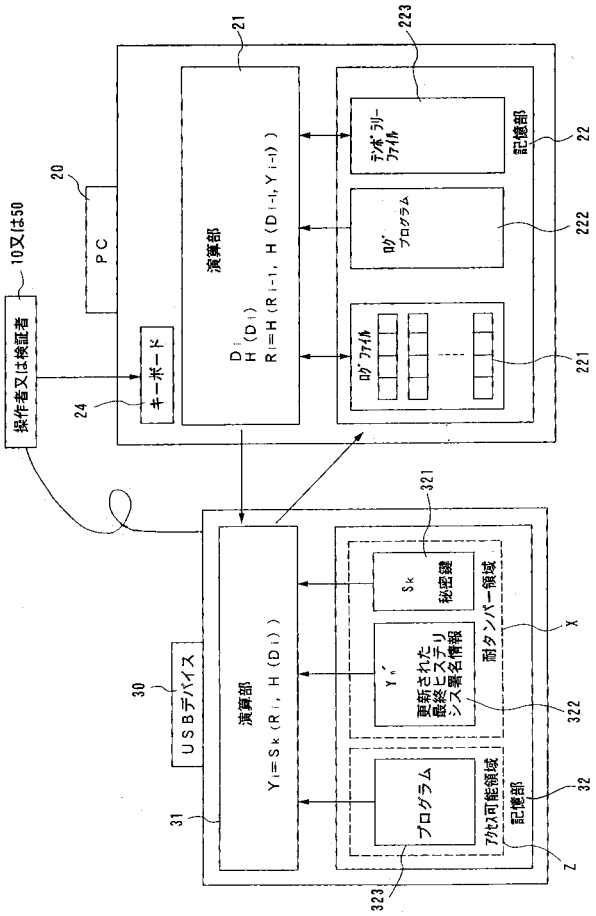
【図面の簡単な説明】

【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。

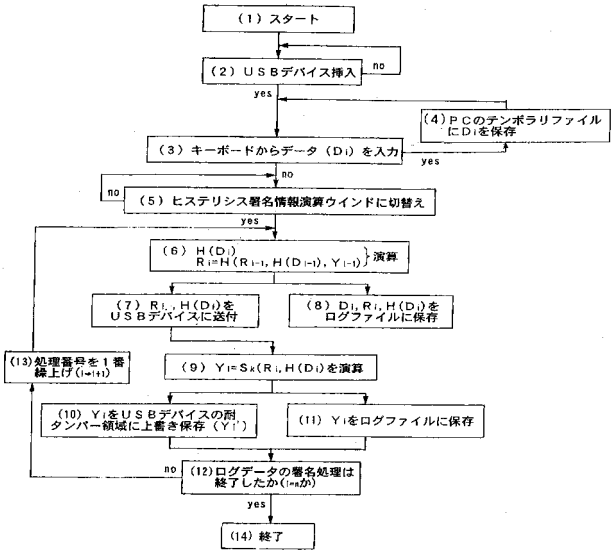
【符号の説明】

【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
　３０・・ＵＳＢデバイス
　　３１・・演算部
　　３２・・記憶部
　　３２１・・秘密鍵（S_K）
　　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番目の署名対象の文章データ（ログデータ）
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）

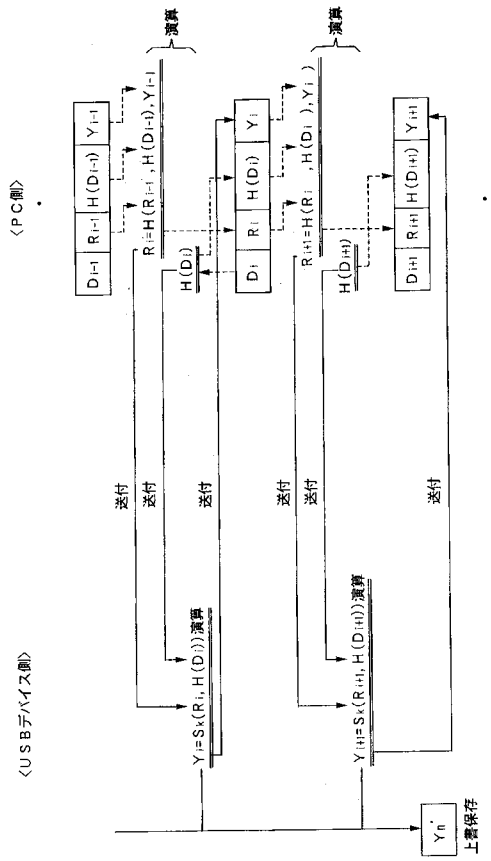
【図１】


操作者又は検証者
10又は50
PC
20
キーボード
24
演算部
21
記憶部
22
テンポラリファイル
プログラム
ログファイル
221
222
223
USBデバイス
30
31
演算部
記憶部
32
秘密鍵
Sk
耐タンパー領域
X
322
321
323
プログラム
アクセス可能領域
Z

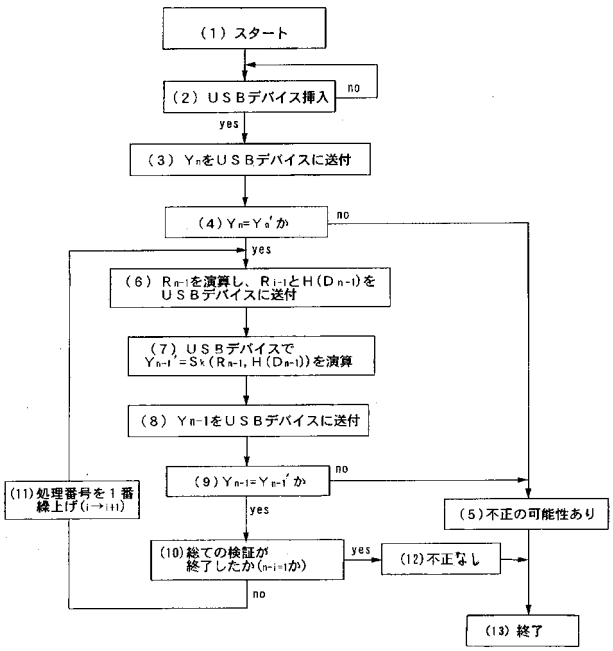
【図２】


(1) スタート
(2) USBデバイス挿入
no
yes
(4) PCのテンポラリファイルにDiを保存
(3) キーボードからデータ(Di)を入力
yes
no
no
(5) ヒステリシス署名情報演算ウインドに切替え
yes
(6) H(Di)
Ri=H(Ri-1, H(Di-1), Yi-1)
演算
(7) Ri, H(Di)をUSBデバイスに送付
(8) Di, Ri, H(Di)をログファイルに保存
(13)処理番号を1番繰上げ(i→i+1)
(9) Yi=Sk(Ri, H(Di))を演算
(10) YiをUSBデバイスの耐タンパー領域に上書き保存(Yi')
(11) Yiをログファイルに保存
no
(12)ログデータの署名処理は終了したか(i=nか)
yes
(14) 終了

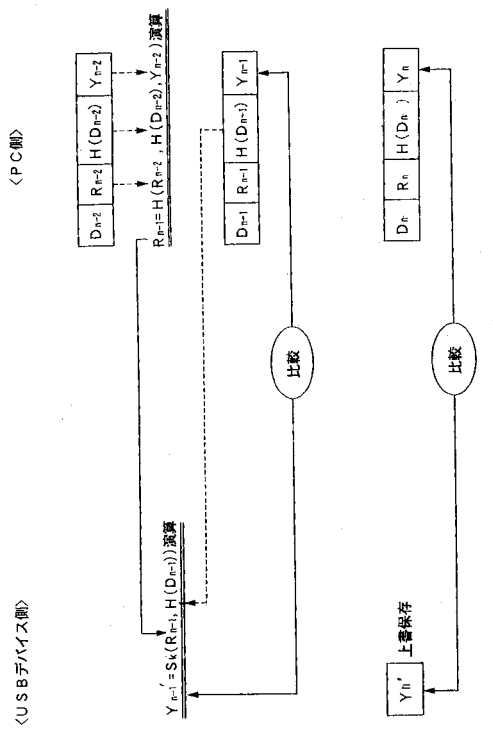
【図３】


〈PC側〉
〈USBデバイス側〉
演算
演算
Di-1
Ri-1
H(Di-1)
Yi-1
Ri=H(Ri-1, H(Di-1), Yi-1)
Di
Ri
H(Di)
Yi
Ri+1=H(Ri, H(Di), Yi)
Di+1
Ri+1
H(Di+1)
Yi+1
H(Di)
H(Di+1)
送付
送付
送付
送付
送付
送付
Yi=Sk(Ri, H(Di))演算
Yi+1=Sk(Ri+1, H(Di+1))演算
Yn'
上書保存

【図４】


(1) スタート
(2) USBデバイス挿入
no
yes
(3) YnをUSBデバイスに送付
(4) Yn=Yn'か
no
yes
(6) Rn-1を演算し、Ri-1とH(Dn-1)をUSBデバイスに送付
(7) USBデバイスでYn-1'=Sk(Rn-1, H(Dn-1))を演算
(8) Yn-1をUSBデバイスに送付
(9) Yn-1=Yn-1'か
no
yes
(11)処理番号を1番繰上げ(i→i+1)
(5)不正の可能性あり
(10)総ての検証が終了したか(n-i=1か)
yes
(12)不正なし
no
(13) 終了

【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

Ｆターム(参考) 5J104 AA08 AA09 AA16 EA04 EA15 EA22 LA02 LA06 NA02 NA12
NA27 NA35 NA37 NA38 NA40 NA42