(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4206674号
(P4206674)

(45)発行日　平成21年1月14日(2009.1.14)　(24)登録日　平成20年10月31日(2008.10.31)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640D

請求項の数 9　(全 21 頁)

(21)出願番号	特願2002-59674(P2002-59674)
(22)出願日	平成14年3月6日(2002.3.6)
(65)公開番号	特開2002-335241(P2002-335241A)
(43)公開日	平成14年11月22日(2002.11.22)
審査請求日	平成17年3月7日(2005.3.7)
(31)優先権主張番号	09/816,777
(32)優先日	平成13年3月22日(2001.3.22)
(33)優先権主張国	米国(US)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】有効性を確認可能なログエントリを生成するシステム，および，ログエントリの有効性を確認するシステム

(57)【特許請求の範囲】

【請求項１】

有効性を確認可能なログエントリを生成するシステムであって，

ネットワークで接続される，有効性確認サーバ装置と，マスメディアサーバ装置と，ユーザ装置と，を含んで構成され，

前記ユーザ装置は，

送信または受信したメッセージ各々に係わるログエントリＰ（ただし，i番目の前記ログエントリP_iは，メッセージ内容M_iのハッシュ値$H(M_i)$と，一つ前に生成したログエントリP_{i-1}のハッシュ値$H(P_{i-1})$と，前記$H(P_{i-1})$と前記$H(M_i)$の連結値に対する当該ユーザ装置の利用者であるユーザの秘密鍵により生成されたデジタル署名$Sign_i(H(P_{i-1})||H(M_i))$と，を含む）を生成し，

公開するログエントリＰを選択して，前記マスメディアサーバ装置に公開を要求し，

前記マスメディアサーバ装置は，

前記ユーザ装置が選択したログエントリＰを出力し，

出力先装置（公開装置）または当該マスメディアサーバ装置に接続された入力装置から，公開されたログエントリＰの公開された日時を受信し，

前記公開者を特定する情報と，前記公開された日時と，を格納し，

前記有効性確認サーバ装置に，公開を要求した前記ユーザ装置を特定する情報と，前記公開者を特定する情報と，前記公開された日時と，を通知し，

公開を要求した前記ユーザ装置に，前記公開者を特定する情報と，前記公開された日時

と，を通知する
ことを特徴とする有効性を確認可能なログエントリを生成するシステム。
【請求項２】
請求項１に記載の，有効性を確認可能なログエントリを生成するシステムにおいて，
さらに，前記ネットワークに接続される，前記ログエントリのバックアップを行う証拠収集サーバ装置を備え，
前記証拠収集サーバ装置は，前記ネットワーク上で送信された前記ログエントリＰと，当該ログエントリＰの送信先と，を特定する情報とを収集してデータベースに格納する
ことを特徴とする有効性を確認可能なログエントリを生成するシステム。
【請求項３】
請求項１に記載の，有効性を確認可能なログエントリを生成するシステムを用いて生成されたログエントリの有効性を確認するシステムであって，
前記有効性確認サーバ装置は，
前記ログエントリP_iの有効性の確認を要求された場合に，
前記デジタル署名$Sign_i(H(P_{i-1})||H(M_i))$を検証し，
前記ログエントリP_iより後に生成され，かつ公開された，ログエントリP_k（ただし$k>i$）を前記マスメディアサーバ装置から取得し，
取得した前記ログエントリP_kから確認対象の前記ログエントリP_iまでのログエントリについて，ログエントリP_jに，一つ前のログエントリP_{j-1}のハッシュ値$H(P_{j-1})$が含まれているか（ただし，$k \geqq j \geqq i+1$）を検査することにより，
確認対象の前記ログエントリP_iの有効性を確認する
ことを特徴とするログエントリの有効性を確認するシステム。
【請求項４】
請求項３に記載されたログエントリの有効性を確認するシステムであって，
さらに，前記ネットワークに接続される，前記ログエントリのバックアップを維持する証拠収集サーバ装置を備え，
前記証拠収集サーバ装置は，
前記ユーザ装置が作成した１つ以上のログエントリP_m（ただし，$k-1 \geqq m \geqq i+1$）を前記有効性確認サーバ装置に送信する
ことを特徴とするログエントリの有効性を確認するシステム。
【請求項５】
請求項３に記載されたログエントリの有効性を確認するシステムであって，
前記ユーザ装置は，さらに，
前記有効性確認サーバ装置からの要求により，自ユーザ装置が作成した１つ以上のログエントリP_m（ただし，$k-1 \geqq m \geqq i+1$）を前記有効性確認サーバ装置に送信することを特徴とするログエントリの有効性を確認するシステム。
【請求項６】
請求項４に記載のログエントリの有効性を確認するシステムにおいて，
前記証拠収集サーバ装置は，
前記ネットワークを介して送信された前記ログエントリを受信した他の装置を特定する情報をデータベースに格納し，
前記特定した他の装置から前記ログエントリを取得して前記有効性確認サーバ装置に送信する
ことを特徴とするログエントリの有効性を確認するシステム。
【請求項７】
請求項４に記載のログエントリの有効性を確認するシステムにおいて，
前記証拠収集サーバ装置は，
前記ネットワークを介して送信された前記ログエントリのバックアップコピーをデータベースに維持し，
要求に応じて有効性確認サーバ装置に前記バックアップコピーを送信する

ことを特徴とするログエントリの有効性を確認するシステム。
【請求項８】
請求項４に記載のログエントリの有効性を確認するシステムにおいて，
前記証拠収集サーバ装置は，
前記ログエントリのバックアップコピーを，前記ネットワークを介して検索し，
発見した前記バックアップコピーを取得して前記有効性確認サーバ装置に送信する
ことを特徴とするログエントリの有効性を確認するシステム。
【請求項９】
請求項３ないし８いずれか一に記載のログエントリの有効性を確認するシステムにおいて，
前記有効性確認サーバ装置は，
メッセージM_iについて，ハッシュ値$H(M_i)$を計算し，
前記ログエントリP_iに含まれるメッセージのハッシュ値$H(M_i)$と比較することにより，前記メッセージM_iの有効性を確認する
ことを特徴とするログエントリの有効性を確認するシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は一般にデータの回復に関し、特にデジタル署名付きデータの回復および／または確認に関する。
【０００２】
【従来の技術】
業務および個人両方の通信のためのインターネットの使用は、過去数年間、特に電子商取引の分野で劇的に成長した。ハードウェアおよびソフトウェアの複雑さの増大を伴うこのメッセージトラフィックの大幅な増加によって、データを失う可能性も増大した。コンピュータクラッシュの数が増加しているため、現在多くのシステムはバックアップを提供している。
【０００３】
従来のデータ回復方法が多数存在するが、ユーザにとって、回復された情報が不正に変更されているかどうかをどうやって知るかという問題が発生している。これは特にコンピュータのいくつかの広く公表されたアカウントの侵入があった時に言えることである。メッセージ、特に回復されたメッセージへの不正変更があったかを検出する従来の技術の１つはデジタル署名である。米国政府はデジタル署名の標準を確立しているが、これは、その全体を引用によって本出願の記載に援用する、連邦情報処理標準公告（ＦＩＰＳ　ＰＵＢ）１８６に示されている。
【０００４】
図１は、従来のデジタル署名技術を例示する。メッセージ（Ｍ）１１０の送信機は署名生成ユニット１１２を有する。メッセージ１１０の受信機は署名検証ユニット１１４を有する。署名生成ユニット１１２はメッセージ１１０を受け取りＭ１１０に対してセキュアハッシュ１１６を行ってＨ（Ｍ）１１８を生じる。Ｈ（Ｍ）１１８と秘密鍵１２０はデジタル署名アルゴリズム（ＤＳＡ）署名１２２に入力されＨ（Ｍ）１１８に対するデジタル署名、すなわちＳｉｇｎ（Ｈ（Ｍ））１２４を生じる。Ｍ１１０とＳｉｇｎ（Ｈ（Ｍ））１２４はユーザ送信機の署名生成ユニット１１２からユーザ受信機の署名検証ユニット１１４に送信される。次にＭ１１０は署名検証ユニット１１４でハッシュ１３０されＨ（Ｍ）１３２を生じる。セキュアハッシュ１３０はセキュアハッシュ１１６と同じ関数である。Ｈ（Ｍ）１３２とＳｉｇｎ（Ｈ（Ｍ））１２４は公開鍵１３４と共にＤＳＡ検証１３６に入力されメッセージ内容が確認される。“ｎｏ”結果はメッセージ１１０が不正変更されていることを示し、“ｙｅｓ”結果は不正変更がないことを示すが、それを保証するわけではない。さらに、デジタル署名はメッセージを認証する、すなわち、メッセージが、そのメッセージが要求された出所からのものであることを受信者に保証する。

【０００５】
【発明が解決しようとする課題】
しかし、デジタル署名は、解読することが非常に困難であるが不可能ではないと想定される周知のアルゴリズムに依存している。解読困難という想定は、コンピュータの能力の急速な増大と共に次第に説得力がないものになりつつある。さらに、デジタル署名は秘密鍵が秘密のものであることを前提としている。秘密鍵が危殆に瀕した場合、セキュリティはその場で、回復されたデータと共に失われる。従って、回復されたデータを確認するよりよい技術が必要である。
【０００６】
【課題を解決するための手段】
本発明によれば、データおよび／または関連する署名ログエントリを復元および／または確認する方法とシステムを含む技術が提供される。
１つの態様では、データにはデジタル署名付きユーザメッセージが含まれ、関連署名ログエントリが関連付け、たとえばリンクされる。各署名ログエントリは、最初のものを除いて、前の署名ログエントリからのデータを使用する。前の署名ログエントリからのデータは、現在の署名ログエントリのデジタル署名を形成する際１つの入力として使用される。すなわち、連鎖またはヒステリシス署名が生成される。この態様では、失われたメッセージが復元された後、署名ログが使用され、メッセージに関連するデジタル署名を対応する署名ログエントリと比較することによってメッセージを確認する。署名ログのセキュリティは、公開印刷刊行物、たとえば新聞、ニューズレター、ウェブサイト、雑誌、または定期刊行物といった公開媒体で選択されたエントリを公開することによって向上しうる。メッセージはさらに、公開エントリからメッセージの署名ログエントリに戻る形で署名ログの一貫性を検査することによって確認される。
【０００７】
本発明の態様の中にはメッセージ用ヒステリシス署名の使用を示すものもあるが、本発明はメッセージに制限されない。たとえば、業務用コンピュータシステム上の一連の業務文書の有効性について、バックアップ媒体からデータを復元した後で、業務用署名ログと各文書に関連するヒステリシス署名を使用してデータを確認することがある。また、ユーザは、ユーザ自身のコンピュータシステム上で、復元されたバックアップデータ、たとえば前の電子商取引購入の確認をしようとすることもある。
【０００８】
本発明の１つの態様では、メッセージに対して署名ログ中に生成されるエントリを有する復元メッセージを確認する方法を提供されるが、ここでエントリには、メッセージに関連する暗号化情報、たとえばデジタル署名が含まれる。次に、上記メッセージが失われた場合、要求に応答して復元メッセージが生成され、復元メッセージは署名ログを使用して確認される。
【０００９】
本発明の第２の態様では、ユーザ情報を回復および確認するシステムが提供される。このシステムには、ユーザ情報に関連する暗号化情報を有する署名ログを有するユーザシステムと、通信ネットワークを介してユーザシステムと結合されユーザ情報を復元する回復システムと、上記通信ネットワークを介してユーザシステムと結合され署名ログを使用して復元ユーザ情報を確認する確認システムとが含まれる。
【００１０】
本発明の第３の態様では、ユーザメッセージが有効かを判定するシステムが提供されるが、このシステムには、ログを有するユーザコンピュータシステムであって、ログがユーザによって送信されたメッセージに関連するログエントリを有し、ログエントリがログの前のログエントリに関連する情報を有するデジタル署名を有するユーザコンピュータシステムと、ユーザコンピュータシステムに結合されログを使用してユーザメッセージを確認する確認ユニットとが含まれる。
【００１１】

本発明の第４の態様では、メッセージ情報を確認するデータ構造を含むコンピュータ可読データ伝送媒体が提供される。このデータ構造には、ユーザメッセージのハッシュまたはユーザメッセージ自体を有する第１の部分と、署名ログエントリのハッシュを有する第２の部分と、第１の部分と第２の部分とに基づくデジタル署名とが含まれる。

【００１２】

本発明の第５の態様では、コンピュータを使用して、複数のログエントリを有する署名ログを生成する方法が提供される。まず、第１のログエントリが生成される。第１のログエントリは第１のユーザメッセージに関連する第１の暗号化値を有する。次に、第２のログエントリが生成される。第２のログエントリは、第１のログエントリに関連する第２の暗号化値と、第２のユーザメッセージに関連する第３の暗号化値と、デジタル署名とを有する。

【００１３】

本発明の第６の態様では、コンピュータシステムにおいて、複数の記録されたログエントリを有する署名ログを使用することで選択されたログエントリを確認する方法が提供される。この方法には、選択されたログエントリに対する暗号化値を計算するステップと、その暗号化値が別の記録されたログエントリの一部であるかを判定するステップとが含まれる。

【００１４】

本発明の第７の態様では、複数のユーザコンピュータシステムの１つによるトランザクションの拒否を防止するシステムが提供される。このシステムには、第１のユーザコンピュータシステムと、第１のユーザとトランザクションを行う第２ユーザコンピュータシステムと、第１のまたは第２の何れかのユーザの要求に応答してトランザクションを記録する、ログチェーンクロスコンピュータとが含まれ、この記録にはトランザクションのヒステリシス署名が含まれる。

【００１５】

本発明の第８の態様では、コンピュータシステムを使用して、公式に承認された主体、たとえば（リンクを有するかまたは有さない）公証人によってユーザのログエントリを登録する方法が提供される。この方法には、公式に承認された主体による署名ログチェーンを維持するステップであって、その際署名ログチェーンの第１のログエントリが署名ログチェーンの前の第２のログエントリに関連するステップと、ユーザからユーザログエントリを受信するステップと、ユーザログエントリに関連する暗号化値を生成するステップと、署名ログチェーンの第３のログエントリを生成するステップであって、その際第３のログエントリが暗号化値を含むステップとが含まれる。

【００１６】

本発明の第９の態様では、ユーザの署名ログを使用するコンピュータシステムによってユーザデータ項目を確認する方法が提供される。コンピュータシステムはユーザの署名ログを受信し、ユーザデータ項目に関連する暗号化値がユーザの署名ログ中の第１のログエントリにあるかを確認する。次に、コンピュータは、チェックポイントされたユーザの署名ログ中の第２の署名ログを判定した後第２のログエントリから第１のログエントリに後方連鎖することで第１のログエントリを検証し、結果はユーザに戻される。

【００１７】

本発明の第１０の態様では、コンピュータシステムを使用して、２つの時点間のデータ項目を回復する方法が提供される。この方法には、ユーザから２つの時点間のデータを回復せよという要求を受信するステップと、データ回復ユニットからデータ項目と関連署名ログエントリとを受信するステップと、関連署名ログエントリを使用してデータ項目を確認するステップと、データ項目が確認された場合、データ項目をユーザに送信するステップとが含まれる。

【００１８】

本発明の第１１の態様では、ユーザメッセージを確認するシステムが提供される。このシステムには、ユーザから複数の関連ログエントリを含む署名ログを受信する入力モジュー

ルと、ユーザメッセージから暗号化値を生成する暗号化モジュールと、暗号化値が署名ログ中にあることを確認する検証モジュールとが含まれる。

【００１９】

第１２の態様では、復元メッセージを確認するコンピュータプログラム製品が提供されるが、これは、メッセージについて署名ログ中に、メッセージに関連する暗号化情報を含むエントリを生成するコードと、メッセージが失われている場合、要求に応答して復元メッセージを生成するコードと、署名ログを使用して復元メッセージを確認するコードと、上記のコードを具現するコンピュータ使用可能媒体とを有する。

【００２０】

他の態様では、復元メッセージを確認する、搬送波中に具現されるコンピュータデータ信号が提供されるが、これは、メッセージについて署名ログ中に、メッセージに関連する暗号化情報を含むエントリを生成するプログラムコードと、上記メッセージが失われている場合、要求に応答して復元メッセージを生成するプログラムコードと、署名ログを使用して復元メッセージを確認するプログラムコードとを有する。

【００２１】

本発明のこれらと他の態様は以下の本文および添付の図面に関連してさらに詳細に説明される。

【００２２】

【発明の実施の形態】

図２は、本発明の有効性回復システムの実施形態を示す。このシステムには、ネットワーク２１０を介して互いに結合された有効性回復サーバ２１２とユーザ＿１　２１４とが含まれる。必要に応じて、ユーザ＿２　２１６、証拠収集サーバ２２０、リンクのない公証人事務所２２２、リンクのある公証人事務所２２４、マスメディアサーバ２３０、マスメディアサーバ２３０、およびログチェーンクロスサーバ２４０の１つかそれ以上が含まれ、ネットワーク２１０を介して互いに結合されることがある。ユーザ＿１　２１４とユーザ＿２　２１６はありうるユーザの例に過ぎず、他の実施形態には２人より多いユーザが含まれる。マスメディアサーバ２３０には新聞２３２および／またはウェブサイト２３４が含まれる。

【００２３】

有効性回復サーバ２１２は証拠収集サーバ２２０から回復されたメッセージおよび／または署名ログエントリを受信し、メッセージおよび／またはメッセージに関連する署名ログエントリを確認する。ユーザまたは証拠収集サーバ２２０はマスメディアサーバ２３０を介して選択された署名ログエントリを公開することを要求することがあり、リンクのない公証人事務所２２２、またはリンクのある公証人事務所２２４によって他の選択された署名ログエントリを登録する。この登録または公開によって、署名ログエントリはチェックポイントされ、後で前の署名ログエントリを個々に確認する際使用される。

【００２４】

証拠収集サーバ２２０はネットワーク２１０上で送信されたユーザメッセージに関連する情報を収集しデータベース（ＤＢ）中に格納する。この情報には、メッセージに関連する署名ログエントリとそのメッセージの送信相手先が含まれる。この実施形態では、証拠収集サーバ２２０はそのＤＢ中に全てのユーザの署名ログエントリのコピーを維持しているので、ユーザの署名ログのバックアップの役目を果たしている。メッセージを回復するため、証拠収集サーバ２２０は誰がメッセージを受信したかを知っており、受信者からメッセージを回復しようとする。代替実施形態では、証拠収集サーバ２２０はユーザによって送信されたメッセージの一部または全てのコピーを維持し、要求に応じて有効性回復サーバ２１２にバックアップコピーを供給する。他の実施形態では、証拠収集サーバ２２０には検索エンジンが含まれるが、これは有効性回復サーバ２１２の要求に応じて、ネットワーク２１０を介して失われたメッセージのバックアップコピーを検索する。検索エンジンがバックアップコピーを発見すると、証拠収集サーバはバックアップコピーを取り出し、それを有効性回復サーバ２１２に転送する。

【００２５】
公証人事務所２２２および２２４は有資格公設または私設の公証人サービスまたは何らかの公式に承認された主体であり、ヒステリシス署名（すなわち、リンクあり）かまたは従来のログブック（すなわち、リンクなし）の何れかを使用して署名ログを維持する。すなわち、ユーザは、公証人サービスによって自分の署名ログに選択されたエントリを定期的に登録できる。こうしたチェックポイントが使用され、個々の前の署名ログエントリを確認する。
【００２６】
ここで使用されるようなヒステリシス署名は、メッセージに関連する第１の暗号化情報と、少なくとも１つの前のヒステリシス署名に関連する第２の暗号化情報とを含むデジタルデータを使用するセキュリティ機構である。第１の暗号化情報の例はメッセージ暗号化の結果である。第１の暗号化情報の別の例には、一部または全体がメッセージから形成されたデジタル署名が含まれる。第２の暗号化情報の例には少なくとも１つの前のヒステリシス署名のデジタルデータの暗号化の結果が含まれるが、ここで当初第１のヒステリシス署名は所定の値であることがある。上記の定義を使用すると、ヒステリシス署名の１つの例には、ログエントリのチェーンにおいて、各ログエントリが、最初のログエントリを除いて、前のログエントリに依存する、ログエントリのチェーン中の１つのログエントリが含まれる。
【００２７】
マスメディアサーバ２３０は、ユーザまたは証拠収集サーバ２２０の何れかの要求に応じて、広範な対象者に選択されたユーザ署名ログエントリを公開する。署名ログエントリを公開することで、それが公開された後ログエントリを不正変更することは困難になる。ログエントリを公証人によって登録することと同様、署名ログエントリの公開はエントリをチェックポイントし、特定の前の署名ログエントリを確認するために使用される。新聞発行者２３２とウェブサイト２３４という、公開者の２つの例が示される。公開者の他の例には、雑誌、書籍、定期刊行物、ニューズレター、または会議議事録の発行者が含まれる。
【００２８】
ログチェーンクロスサーバ２４０は、相互トランザクション、たとえば、連絡、商品の販売、融資、または電子商取引トランザクションが行われる時、たとえば、ユーザ＿１　２１４とユーザ＿２　２１６によって使用される。ログチェーンクロスサーバ２４０は、ヒステリシス署名を使用して署名ログ中にメッセージ転送のコピーを維持する。トランザクション上の紛争が生じた場合、ログチェーンクロスサーバ２４０はトランザクションの証人の役目を果たす。これによって何れかの当事者がトランザクションを拒否するのが防止される。代替実施形態では、ログチェーンクロスサーバ２４０はユーザ＿１　２１４とユーザ＿２　２１６の間のトランザクションの転送またはメッセージの交換を促進するが、コピーは維持しない。この場合、自分のコピーを維持するのは各ユーザの責任である。
【００２９】
図３は、図２に示される各コンピュータシステムの１つの実施形態を表すコンピュータシステム３１０の例を示す。こうした図２のコンピュータシステムには、有効性回復サーバ２１２、ユーザ＿１　２１４、ユーザ＿２　２１６、証拠収集サーバ２２０、リンクのない公証人事務所２２２、リンクのある公証人事務所２２４、マスメディアサーバ２３０、およびログチェーンクロスサーバ２４０が含まれる。コンピュータシステム３１０には、中央処理装置（ＣＰＵ）３１２、一時記憶用揮発性記憶装置３１４（たとえばＲＡＭ）、たとえばハードディスク、ＣＤ－ＲＯＭ、またはフレキシブルディスクといった、データおよびソフトウェアを格納する不揮発性記憶装置３１６、ネットワークに接続するネットワークインターフェース３１８、ディスプレイ、マウスおよびキーボードに接続するＩ／Ｏインターフェース３２０、および上記の構成要素を互いに接続するバス３２５が含まれる。別のハードウェア実施形態には、ＲＡＩＤディスク駆動装置を備えたサーバ用の多重プロセッサ Microsoft Windows NTシステムと、ユーザ用のMicrosoft Windowsオペレーテ

ィングシステムを備えたパーソナルコンピュータとが含まれる（Microsoft、Windows、Windows NTは米国Microsoft Corporationの米国およびその他の国における登録商標である）。

【００３０】

図４は、本発明の１つの実施形態のメッセージ形式４１０を示す。メッセージは、ネットワーク２１０上で、ユーザ、たとえばユーザ＿１　２１４から別のユーザ、たとえばユーザ＿２　２１６に送信される。メッセージ形式４１０には、索引番号“ｉ”４１２と、出所、たとえばユーザ＿１　２１４のユーザアドレス４１４が含まれる。さらに、宛先、たとえばユーザ＿２　２１６のアドレス（図示せず）も含まれる。メッセージ内容、M_i、メッセージ内容のハッシュ、Ｈ（M_i）４１８、前の（ｉ－１）ログエントリのハッシュ、Ｈ（P_{i-1}）、Ｈ（P_{i-1}）とＨ（M_i）の連結のデジタル署名、すなわち$Sign_i$（Ｈ（P_{i-1}）｜｜Ｈ（M_i））４２２、および公開鍵証明４２４が含まれる。メッセージ内容、M_iにはたとえば、テキスト、ＨＴＭＬ、ＸＭＬ、イメージ、ビデオクリップ、音声クリップ、デジタルデータ、またはプログラムが含まれる。１つの実施形態では、メッセージ内容（M_i）には添付ファイルが含まれる。代替実施形態では、添付ファイルは除外される。デジタル署名、$Sign_i$（Ｈ（P_{i-1}）｜｜Ｈ（M_i））４２２は、前のログエントリ、P_{i-1}からの情報がデジタル署名中に含まれているという点でヒステリシス署名である。

【００３１】

図５は、本発明の他の実施形態の別のメッセージ形式５１０を示す。メッセージの形式は図４と同様であるが、タイムスタンプ$_i$フィールド５２４が加わっている点が異なっている。１つの実施形態では、タイムスタンプ$_i$フィールド５２４はメッセージが送信された時間である。他の実施形態では、タイムスタンプ$_i$フィールド５２４は、メッセージが作成された時間またはメッセージが受信された時間のこともある。

【００３２】

図６は、本発明の実施形態のユーザの署名ログの例を示す。各ユーザは時間順で、送信および受信されたメッセージの署名ログを維持する。署名ログエントリは記号P_i、たとえば、P_1　６１０、P_2　６２０、P_{n-1}　６３０およびP_n　６４０によって表される。最初の署名ログエントリP_1　６１０はフィールド“ＩＶ”６１２を有するが、これは所定の値に設定された定数である。次のフィールドＨ（M_1）６１４は最初のメッセージ内容、M_1のハッシュである。そして第３のフィールド$Sign_1$（ＩＶ｜｜Ｈ（M_1））６１８は、Ｈ（M_1）と連結されたＩＶのデジタル署名である。次の署名ログエントリP_2　６２０はフィールドＨ（P_1）６２２を有するが、これは前の署名ログエントリP_1　６１０のハッシュである。次のフィールドＨ（M_2）６２４は第２のメッセージ内容、M_2のハッシュである。第３のフィールド$Sign_2$（Ｈ（P_1）｜｜Ｈ（M_2））６２６は、Ｈ（M_2）と連結されたＨ（P_1）のデジタル署名である。ｎ番目の署名ログエントリはP_n　６４０であるが、これにはＨ（P_{n-1}）６４２中に前の署名ログエントリP_{n-1}　６３０からの情報が含まれる。ｎ番目のメッセージ内容、M_nはハッシュされ、Ｈ（M_n）６４４を生じる。このデジタル署名はヒステリシス署名、$Sign_n$（Ｈ（P_{n-1}）｜｜Ｈ（M_n））６４６である。すなわち、P_nは［Ｈ（P_{n-1}）｜｜Ｈ（M_n）｜｜$Sign_n$（Ｈ（P_{n-1}）｜｜Ｈ（M_n））］に等しい。（ｎ－１）番目の署名ログエントリはP_{n-1}　６３０であるが、これにはＨ（P_{n-2}）６３２中に前の署名ログエントリP_{n-2}からの情報が含まれる。（ｎ－１）番目のメッセージ内容、M_{n-1}はハッシュされ、Ｈ（M_{n-1}）６３４を生じる。このデジタル署名はやはりヒステリシス署名、$Sign_{n-1}$（Ｈ（P_{n-2}）｜｜Ｈ（M_{n-1}））６３６である。すなわち、各ログエントリ、P_iは、前のログエントリ、P_{i-1}に向かって後方に連鎖する。この連鎖によって、現在の情報と共に過去の情報も知らなければならないため、デジタル署名を偽造する困難は大きく増大する。他の実施形態では、ユーザは別個の送信ログと受信ログを有することがある。

【００３３】

図７は、本発明の他の実施形態のユーザ署名ログの例を示す。この署名ログエントリは図６と同様であるが、各エントリの追加タイムスタンプフィールド、たとえば、７１６、７２６、７３６、および７４６がある点が異なっている。タイムスタンプフィールドは図５のものと同じである。

【００３４】

図８は、本発明の実施形態の署名ログファイル中のログエントリの確認を示すフロー図を示す。ｋ＞ｍである２つのログエントリP_kとP_mがある場合、P_m～P_{k-1}の計算済みハッシュがユーザの署名ログファイル中になければならず、そうでない場合署名ログは損傷している。ステップ８１０では、P_kとP_mが、たとえば有効性回復サーバ２１２によって受信される。Ｊ＞ｋであり、一時反復索引“ｊ”は当初ｋに設定される。ステップ８１２では、Ｈ（P_{j-1}）がP_{j-1}のハッシュを発見することによって計算される、すなわち次式である。

【００３５】

【数１】

$$H(P_{j-1})=H[H(P_{j-2})\|H(M_{j-1})\|Sign_{j-1}(H(P_{j-2})\|H(M_{j-1}))]$$

【００３６】

次に、ステップ８１４で、計算されたＨ（P_{j-1}）がP_jに対するユーザの署名ログ中にあるかを検査する。答えがノーであれば、ステップ８１８で署名ログは損傷している。答えがイエスであれば、ｊ－１がｍより大きいかが検査される（ステップ８２０）。ノーであれば、処理は完了し８２２、署名ログエントリP_m～P_{k-1}が確認される（P_kは前に確認されていると想定する）。イエスであれば、ｊは１つ減らされ、処理はステップ８１２に進んでＨ（P_{j-1}）を計算する。

【００３７】

たとえば、ｋ＝５でｍ＝３であるとする。ステップ８１０ではｊ＝ｋ＝５である。ステップ８１２では、P_4に対する署名ログエントリを使用してＨ（P_4）が計算される。次に、図６から示されているように、P_5に対するユーザの署名ログ中にＨ（P_4）があるかが検査される。答えがイエスであれば、P_5が前に確認されていると想定すればP_4は確認される。（５－１）＞３（ステップ８２０）であるので、ｊは１つ減らされる（ステップ８２４でｊ＝４）。ステップ８１２でP_3に対するログエントリからＨ（P_3）が計算され、計算されたＨ（P_3）がログエントリP_4中の対応するフィールドに対して検査される。Ｈ（P_3）が署名ログ中にあるならば、P_3が確認され、ステップ８２０で、（４－１）＞３が検査される。答えはノーなので、処理はステップ８２２で終了し、結果としてP_3およびP_4が確認された。P_5は、チェックポイントによって、たとえばマスメディアサーバ２３０を使用してP_5を公開するか、または公証人２２２および２２４によってP_5を登録することで前もって確認することができる。チェックポイントの意味は、P_5がチェックポイントされた後不正変更することが困難になるということである。

【００３８】

図９は、本発明の１つの実施形態のチェックポイントの例を示す。縦軸８４０は時間を表し、相対時間ｔ＝０　８４１で始まる。最初の署名ログエントリ８４２は図６のP_nと同様の形式を有する。次のログエントリは８４４によって示される。ログエントリ８４６は時間８６２（ｔ＝ｔ１）で発生し、この例では第１のチェックポイントを表す。これは、ログエントリ８４６が公開されるかまたは公証人によって登録されたことを意味する。８４６がP_5でチェックポイントされ、８４４がP_3（P_4は図示せず）であるとする。図８が使用されP_3およびP_4を確認することがある。ｔ＝ｔ２　８６４の時間、すなわち、署名ログ８５０と８５２の間にログの損傷があるならば、ログエントリ８５２、８５４、および８５６が疑わしい。時間ｔ＝ｔ３　８６６でのチェックポイント８５６は、損傷

したログエントリが公開または登録されているため意味がない。ログエントリ８４８および８５０はまだ有効である。損傷がメッセージに対するものであって署名ログに対するものでないならば、ログエントリ８５６（チェックポイント２）から８４６（チェックポイント１）への後方連鎖を行う時に損傷が検出される見込みがある。従って、ユーザの署名ログを保護することが重要である。

【００３９】

図１０は、本発明の実施形態のログチェーンクロスサーバを使用する例を示す。アリスとボブという２人のユーザがおり、彼らはトランザクション、たとえば商品販売の提案と受け入れを行おうとしているとする。アリスは、ログエントリ９１２、９１４、９１６、および９１８を含む署名ログ９１０を有し、ボブは、ログエントリ９３２、９３４、９３６、および９３８を含む署名ログ９３０を有する。凡例は、アリスのヒステリシス署名フロー９２０とボブのヒステリシス署名フロー９４０を示す。トランザクションは、ボブとアリスの両方がトランザクションを促進するログチェーンクロスサーバ２４０に接触することによって開始される。ボブはログチェーンクロスサーバ９２２を介してアリスに自分の提案メッセージを送信する。提案メッセージに関連するログエントリ９３４がボブの署名ログ９３０に入力される。ログチェーンクロスサーバ２４０はボブからの提案を受信すると、対応する署名ログエントリをログに記録し、提案メッセージをアリスに送信する。アリスは、提案メッセージを受信すると、自分の署名ログ９１０にログエントリ９１４を記録する。次にアリスはボブの宛先と共に受け入れメッセージをログチェーンクロスサーバ２４０に送信する。アリスは受け入れメッセージに関連する署名ログエントリ９１６を自分の署名ログ９１０に入力する。ログチェーンクロスサーバ２４０は受け入れメッセージを受信すると、対応する署名ログエントリをログに記録し、メッセージをボブに伝える。ボブは受け入れメッセージを受信すると署名ログエントリ９３６を自分の署名ログ９３０に入力し、トランザクションは完了する。すなわち、トランザクション、すなわち提案および受け入れメッセージがログエントリを有する場所は、アリスのログ９１０、ボブのログ９３０、およびログチェーンクロスサーバ２４０のログと３つある。これによってアリスまたはボブが後でトランザクションを拒否することが防止される。ログチェーンクロスサーバ２４０はトランザクションの公平な証人の役目を果たす。

【００４０】

図１１は、リンクのある公証人による署名ログエントリの登録の例を示す。すなわち、公証人はヒステリシス署名または連鎖ログ１０３０を有する。ユーザはヒステリシス署名ログ１０１０を有し、これにはエントリ１０１２、１０１４、および１０１６が含まれる。公証人はヒステリシス署名ログ１０３０を有し、これにはログエントリ１０３２、１０３４、１０３６、および１０３８が含まれる。この実施形態では公証人は、マスメディアサーバ２３０を使用して、そのログエントリ、たとえばエントリ１０３４およびエントリ１０３８を定期的に公開する。ユーザは、ログエントリ、たとえばエントリ１０１４を公証人に送信することによって登録できる。次に公証人はユーザのログエントリ１０１４を公証人の署名ログ１０３０に入力し、エントリ１０３６に与える。すなわち、ユーザのログエントリは公証人のログチェーンの一部となる。

【００４１】

図１２は、本発明の実施形態のマスメディアサーバ２３０に関するフロー図を示す。ステップ１１１０では、マスメディアサーバ２３０は、ユーザログエントリP_iを公開せよというユーザ要求を受信する。次にマスメディアサーバ２３０は公開者、たとえばウェブサイト２３４または新聞２３２に、ログエントリ項目P_iを送信する。公開の後、ステップ１１１４では、マスメディアサーバ２３０は公開者からタイムスタンプ、たとえばP_iが公開された日付／時間を受信する。ステップ１１１６では、P_iが公開者のＩＤおよび／または公開の日付／時間と共に格納される。ステップ１１１８では、マスメディアサーバ２３０は有効性回復サーバ２１２に要求ユーザＩＤ、公開者、および／または公開の日付／時間を通知する。そしてステップ１１２０では、ユーザは公開者および／または公開の日付／時間を通知される。

【００４２】
図１３は、本発明の実施形態において署名ログエントリがチェックポイントされているかを判定する有効性サーバを示すフロー図を示す。ステップ１２１０では、有効性回復サーバ２１２はP_iがチェックポイントされたかを判定せよという要求を受信する。有効性回復サーバ２１２は、可能性のある公開者または公証人のユーザによって索引付けされるリストを検索する（ステップ１２１２）。次に有効性回復サーバ２１２は、可能性のある公開者または公証人があればその識別情報を含む要求をマスメディアサーバ２３０または公証人２２２または２２４に送信する。この要求はP_iが公開／公証されているかを問い合わせるものである。ステップ１２１６では、イエスの答えが公開者または公証人の名称および／または日付／時間と共にマスメディアサーバから受信される。答えがノーであれば、「公開されていない」という回答だけが戻される。
【００４３】
図１４は、ユーザ署名ログエントリ、P_iを確認する有効性回復サーバの実施形態を示す。ステップ１４２０では、有効性回復サーバ２１２は署名ログエントリP_iを確認せよというユーザ要求を受信する。P_iには$H(M_i)$ １４１０、$H(P_{i-1})$ １４１２および$Sign_i(H(M_i)||H(P_{i-1}))$ １４１４が含まれる。有効性回復サーバ２１２はまず、たとえば図１のＤＳＡ検証１３６を使用することでデジタル署名を検証する（ステップ１４２２）。ＤＳＡ検証１３６への入力は$H(M_i)||H(P_{i-1})$、$Sign_i(H(M_i)||H(P_{i-1}))$ １４１４、および公開鍵１３４である。デジタル署名が検証されるならば（ステップ１４２２のイエス結果）、有効性回復サーバ２１２はユーザからユーザ署名ログを要求し受信する（ステップ１４２４）。ステップ１４２６では、$H(M_i)$ １４１０と$H(P_{i-1})$ １４１２が、ユーザの署名ログ中の対応する値に対して検査される。こうしたハッシュ値がログ中にあるならば、ステップ１４２８で、ｋがｉより大きいかｉに等しい、チェックポイントされたP_kが探索される。図８のフロー図を使用して、ユーザの署名ログの一貫性が、チェックポイントP_kからP_iに戻って検査される（ステップ１４３０）。署名ログが損傷していないならば、肯定的な確認結果がユーザに送信される（ステップ１４３２）。
【００４４】
図１５は、ユーザメッセージ内容、M_iを確認する有効性回復サーバの実施形態を示す。ステップ１５２０では、有効性回復サーバ２１２はデータM_iを確認せよというユーザ要求を受信する。メッセージにはM_i １５１０、$H(M_i)$ １５１２、$H(P_{i-1})$ １５１４、および$Sign_i(H(M_i)||H(P_{i-1}))$ １５１６が含まれる。有効性回復サーバ２１２はまず、M_iのハッシュを計算し、それが$H(M_i)$ １５１２と同じであるか検査する（ステップ１５２１）。第２に、デジタル署名が、たとえば図１のＤＳＡ検証１３６を使用することで確認される（ステップ１５２２）。ＤＳＡ検証１３６への入力は$(H(M_i)||H(P_{i-1}))$、$Sign_i(H(M_i)||H(P_{i-1}))$ １５１６、および公開鍵１３４である。デジタル署名が検証されるならば（ステップ１３８のイエス結果）、有効性回復サーバ２１２はユーザからユーザ署名ログを要求し受信する（ステップ１５２４）。ステップ１５２６では、$H(M_i)$ １５１２と$H(P_{i-1})$ １５１４が、ユーザの署名ログ中の対応する値に対して検査される。こうしたハッシュ値がログ中にあるならば、次にステップ１５２８で、ｋがｉより大きいかｉに等しい、チェックポイントされたP_kが探索される。図８のフロー図を使用して、ユーザの署名ログの一貫性が、チェックポイントP_kからP_iに戻って検査される（ステップ１５３０）。署名ログが損傷していないならば、M_iに関する肯定的な確認結果がユーザに送信される（ステップ１５３２）。
【００４５】
表１は、障害と回復の表を示す。
【００４６】
【表１】

表1

損失	原因の例	回復
署名ログエントリ、P_i	記憶媒体の障害	バックアップファイル。 バックアップファイルがない場合、 証拠収集サーバから P_iを取り出して確認する
データ、M_i	記憶媒体の障害、 ユーザの誤り	バックアップファイル。 バックアップファイルがない場合、 証拠収集サーバから M_iおよびP_iを取り出して確認する
データセキュリティ (データまたはログエントリは損失していないが、 データまたはログエントリの有効性が不明) －ユーザは誠実	秘密鍵の漏洩、 メッセージの不正な変更または挿入	ユーザの署名ログ および チェックポイント
データセキュリティ －ユーザが不正に変更	ユーザによる ログの変更、 ユーザによる メッセージの拒否	ログチェーンクロス、 および チェックポイント

【００４７】
各縦列の見出しは、失われる情報の種類、損失の原因の例、および可能性のある回復方法である。
署名ログエントリＰ$_i$の損失は、たとえば記憶媒体の障害によって発生する。可能性のある回復方法はバックアップファイルから署名ログエントリを回復することである。バックアップファイルが存在しない場合、Ｐ$_i$のコピー、すなわち、Ｈ（Ｍ$_i$）、Ｈ（Ｐ$_{i-1}$）、およびＳｉｇｎ$_i$（Ｈ（Ｍ$_i$），Ｈ（Ｐ$_{i-1}$））が証拠収集サーバ２２０のＤＢから取り出され、有効性回復サーバ２１２は、図１４に示された手順を使用して署名ログエントリＰ$_i$を確認するよう要求される。
【００４８】
メッセージ内容Ｍ$_i$の損失が記憶媒体の障害またはユーザの誤りによって発生している場合、可能性のある回復手順にはバックアップファイルからの復元が含まれる。バックアップファイルが存在しない場合、証拠収集サーバ２２０は、メッセージ内容Ｍ$_i$と、関連する署名ログエントリＰ$_i$を取り出して戻すように要求される。次に、有効性回復サーバ２１２は、図１５に示される手順を使用してメッセージ内容Ｍ$_i$を確認するよう要求される。
【００４９】
メッセージ内容または署名ログエントリは失われていないがデータＭ$_i$または署名ログエ

ントリP_iの有効性が不明であるというようなデータセキュリティの損失は、ユーザの秘密鍵の危殆化、メッセージの不正な変更または挿入によって発生する。ユーザすなわちメッセージの作成者が誠実で、ユーザ、たとえばユーザ＿１　２１４によって維持されるユーザ署名ログが損傷していない場合、可能性のある回復手順には、図１４および図１５に示された手順を使用し、ユーザ署名ログと関連するチェックポイントを使用してM_iまたはP_iを確認することが含まれる。

【００５０】

たとえば、メッセージのユーザ／第３者による変更またはユーザによる拒否による署名ログの損傷に起因するデータセキュリティの損失がある場合、回復は原因に基づく。ユーザがトランザクションメッセージを不正変更および拒否した場合、トランザクションの際に交換されたメッセージのコピーがログチェーンクロスサーバ２４０を使用して回復される。第３者がユーザの署名ログを変更した場合、損傷以前の最後の公開／登録された署名ログエントリが使用される。この公開／登録された署名ログエントリの前の全てのログエントリは回復および確認することができる。

【００５１】

図１６は、本発明の実施形態においてデータを収集する証拠収集サーバのフロー図を示す。ステップ１７１０では、証拠収集サーバ２２０はユーザから証拠メッセージを受信する。証拠メッセージには、P_i、M_iの日付／時間、索引Ｉ、M_iの送信機のアドレスまたはＩＤ、M_iの受信機のアドレスまたはＩＤ、またはユーザの送信時間の中、１つかそれ以上が含まれる。代替実施形態では、証拠メッセージは図４または図５の何れかに示される形式のものである。ステップ１７１２では、証拠メッセージはユーザアドレスまたはＩＤによって索引付けされる証拠収集サーバのデータベース（ＤＢ）に格納される。

【００５２】

図１７は、本発明の実施形態においてデータを回復する証拠収集サーバのフロー図を示す。ステップ１８１０では、証拠収集サーバ２２０は有効性回復サーバ２１２からメッセージ内容M_iを回復せよという要求を受信する。ステップ１８１２では、証拠収集サーバ２２０はそのデータベースからM_iに関連する証拠メッセージを検索する。次にステップ１８１４で、証拠収集サーバ２２０は、M_iを受信したユーザからM_iとP_iのコピーを証拠収集サーバに戻すよう要求する。代替実施形態では、証拠収集サーバ２２０はすでにそのＤＢに格納されたM_iとP_iのコピーを有しておりこれらのコピーを使用する。また他の実施形態では、証拠収集サーバはP_iを有し、ネットワーク２１０を検索してM_iを回復する。次にP_iが検査され、受信されたP_iが証拠収集サーバのデータベース中のＰｉと同じかが調べられる（ステップ１８１６）。P_iがＤＢ中にあるならば、ステップ１８１８で、M_iとP_iは確認のため有効性回復サーバ２１２に送信される。

【００５３】

図１８は、他の実施形態においてユーザ署名ログエントリを回復する有効性回復サーバのフロー図を示す。ステップ１９１０では、ユーザ、たとえばユーザ＿１　２１４は有効性回復サーバ２１２に署名ログエントリP_iを回復せよという要求を行う。ステップ１９１２では、一時変数“ｊ”はｉに等しく設定される。次にステップ１９１４では、証拠収集サーバ２２０に対してP_jを入手して戻すようにという要求がなされる。次に有効性回復サーバ２１２は、図１に示された手順を使用し、Ｈ（Ｍ）の代わりに（Ｈ（P_{i-1}）｜｜Ｈ（M_i））によってP_jのデジタル署名を検証する（ステップ１９１６）。

【００５４】

ステップ１９１８では、P_jが検査され、チェックポイントされているかが調べられる。答えがイエスであれば、ステップ１９２０で、図８に示された手順を使用して、ユーザ署名ログの一貫性がチェックポイントP_jから署名ログエントリP_iに戻って検査される。そしてユーザの署名ログ中のP_iが損傷していないならば、P_iはステップ１９２２でユーザに戻される。ステップ１９１８の答えがノーであれば、P_jはログエントリの一時順次リストまたは待ち行列に入力され（ステップ１９２４）、ｊが１つ増やされて（ステップ１９２６）ステップ１９１４～１９１８が繰り返される。連鎖ログエントリを含むリス

トをチェックポイントしたP_jが発見されると、ステップ１９２０でＰｊからＰｉに戻ってログエントリの一貫性を検査するために使用される。

【００５５】

図１９は、他の実施形態においてユーザメッセージを回復する有効性回復サーバのフロー図を示す。ステップ２０１０では、ユーザ、たとえばユーザ＿１　２１４は有効性回復サーバ２１２にメッセージ内容M_iを回復せよという要求を行う。次にステップ２０１２では、証拠収集サーバ２２０に対してM_iおよび関連する署名ログエントリP_iを入手して戻すようにとの要求がなされる。ステップ２０１３では、M_iのハッシュがP_i中にあるかが検査される。ステップ２０１４では、一時変数“ｊ”は“ｉ”に等しく設定される。ステップ２０１６では、証拠収集サーバ２２０に対してP_jを入手し戻すようにとの要求がなされる（ｉ＝ｊの時、P_iはステップ２０１２で前に入手されているのでこのステップは省略される）。

【００５６】

次に有効性回復サーバ２１２は、図１に示された手順を使用し、Ｈ（Ｍ）の代わりに（Ｈ（P_{i-1}）｜｜Ｈ（M_i））によってP_jのデジタル署名を検証する（ステップ２０１８）。ステップ２０２０では、P_jが検査され、チェックポイントされているかが調べられる。答えがイエスであれば、ステップ２０２２で、図８に示された手順を使用して、ユーザ署名ログの一貫性がチェックポイントP_jから署名ログエントリP_iに戻って検査される。そしてユーザの署名ログ中のP_iが損傷していないならば、M_iはステップ２０２４でユーザに戻される。ステップ２０２０の答えがノーであれば、P_jはログエントリの一時順次リストまたは待ち行列に入力され（ステップ２０２６）、ｊが１つ増やされてステップ２０１６～２０２０が繰り返される。連鎖ログエントリを含むリストをチェックポイントしたP_jが発見されると、ステップ２０２２でＰｊからＰｉに戻ってログエントリの一貫性を検査するために使用される。

【００５７】

図２０は、他の実施形態の２つの時点間のユーザメッセージを回復する有効性回復サーバのフロー図を示す。この実施形態では、ユーザメッセージは図５の形式であり、タイムスタンプフィールド５２４が存在する。ステップ２０５０では、ユーザは時間ｔ１と時間ｔ２の間のメッセージM_jを回復せよという要求を有効性回復サーバ２１２に送信する。有効性回復サーバ２１２は、証拠収集サーバ２２０からM_jと関連するP_jを要求する（ステップ２０５２）。ステップ２０５４では、有効性回復サーバ２１２は図１５の手順を使用してM_jを確認する。ステップ２０５６では、有効性回復サーバ２１２または証拠収集サーバ２２０は、ｔ１とｔ２の間に別のM_jが存在するかを検査する。存在する場合、ステップ２０５２～２０５６が繰り返される。答えがノーであれば、M_jがユーザに送信される。他の実施形態では、M_jは証拠収集サーバから一括して入手される。すなわちステップ２０５２はｔ１とｔ２の間の全てのM_jを戻すようにという証拠収集サーバ２２０に対する一括要求となり、ステップ２０５４および２０５６は必要なくなる。

【００５８】

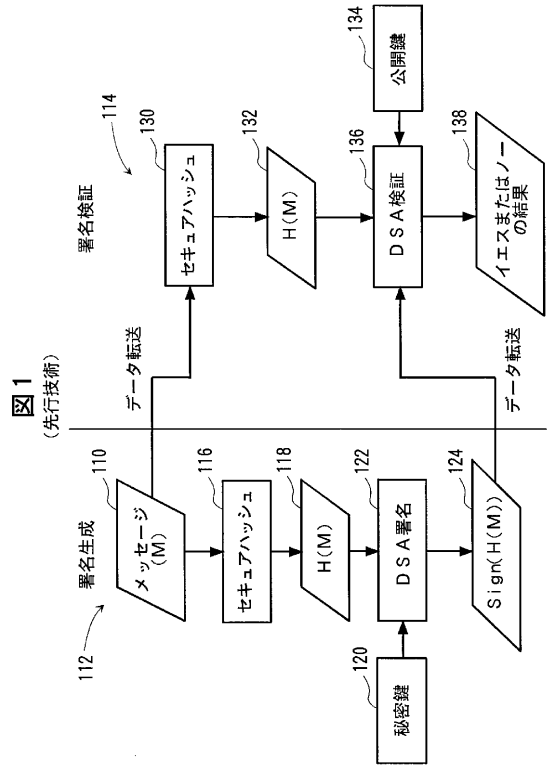
上記の実施形態は一般に特定のハードウェアおよびソフトウェアに関して説明されたが、認識されるように、本発明はさらに広範な適用可能性を有する。たとえば、ソフトウェア機能はさらに結合され、またさらには分離されることがある。同様に、ハードウェア機能もさらに結合され、またさらには分離されることがある。ソフトウェア機能がハードウェアまたはハードウェアとソフトウェアの組み合わせによって実現されることもある。同様に、ハードウェア機能がソフトウェアまたはハードウェアとソフトウェアの組み合わせによって実現されることもある。適用業務に応じて、任意の数の異なった組み合わせが行われることがある。

【００５９】

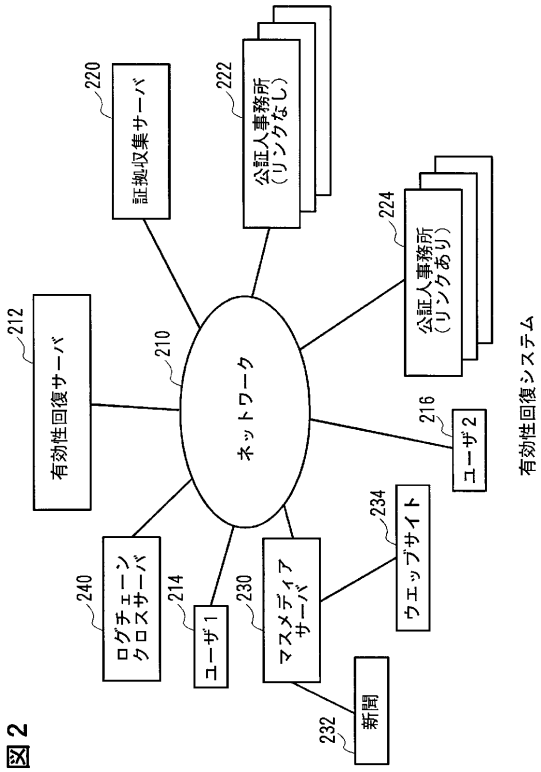
上記の教示を考慮して本発明の多くの修正および変形が可能である。従って、理解されるように、添付の請求項の範囲内で、本発明は上記で特に説明された以外の形で実施されることがある。

【００６０】
【発明の効果】
本発明によれば、データおよび／または関連する署名ログエントリを復元および／または確認することが可能になる。
【図面の簡単な説明】
【図１】従来のデジタル署名技術（先行技術）を例示する。
【図２】本発明の有効性回復システムの実施形態を示す。
【図３】図２に示されるコンピュータシステムの１つの実施形態を表すコンピュータシステムの例を示す。
【図４】本発明の１つの実施形態のメッセージ形式を示す。
【図５】本発明の他の実施形態の別のメッセージ形式を示す。
【図６】本発明の実施形態のユーザの署名ログの例を示す。
【図７】本発明の他の実施形態のユーザの署名ログの例を示す。
【図８】本発明の実施形態の署名ログファイル中のログエントリの確認を示すフロー図を示す。
【図９】本発明の１つの実施形態のチェックポイントの例を示す。
【図１０】本発明の実施形態のログチェーンクロスサーバを使用する例を示す。
【図１１】本発明の実施形態のリンクを有する公証人による署名ログの登録の例を示す。
【図１２】本発明の実施形態のマスメディアサーバ２３０に関するフロー図を示す。
【図１３】本発明の実施形態において署名ログエントリがチェックポイントされているかを判定する有効性サーバを示すフロー図を示す。
【図１４】ユーザ署名ログエントリを確認する有効性回復サーバの実施形態を示す。
【図１５】ユーザメッセージ内容を確認する有効性回復サーバの実施形態を示す。
【図１６】本発明の実施形態においてデータを収集する証拠収集サーバのフロー図を示す。
【図１７】本発明の実施形態においてデータを回復する証拠収集サーバのフロー図を示す。
【図１８】本発明の他の実施形態においてユーザ署名ログエントリを回復する有効性回復サーバのフロー図を示す。
【図１９】本発明の他の実施形態においてユーザメッセージを回復する有効性回復サーバのフロー図を示す。
【図２０】本発明の他の実施形態の２つの時点間のユーザメッセージを回復する有効性回復サーバのフロー図を示す。
【符号の説明】
２１０…ネットワーク、２１２…有効性回復サーバ、２１４…ユーザ１、２１６…ユーザ２、２２０…証拠収集サーバ、２２２…公証人事務所（リンクなし）、２２４…公証人事務所（リンクあり）、２３０…マスメディアサーバ、２３２…新聞、２３４…ウェブサイト、２４０…ログチェーンクロスサーバ

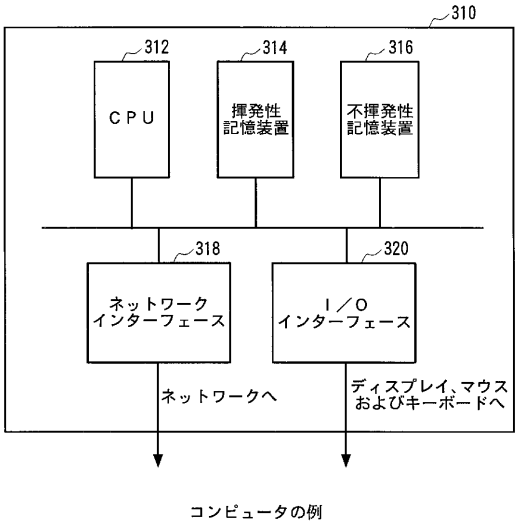
【図１】


図１
（先行技術）
署名検証
署名生成
データ転送
データ転送
メッセージ(M)
セキュアハッシュ
H(M)
DSA署名
Sign(H(M))
秘密鍵
セキュアハッシュ
H(M)
DSA検証
公開鍵
イエスまたはノーの結果
110
112
114
116
118
120
122
124
130
132
134
136
138

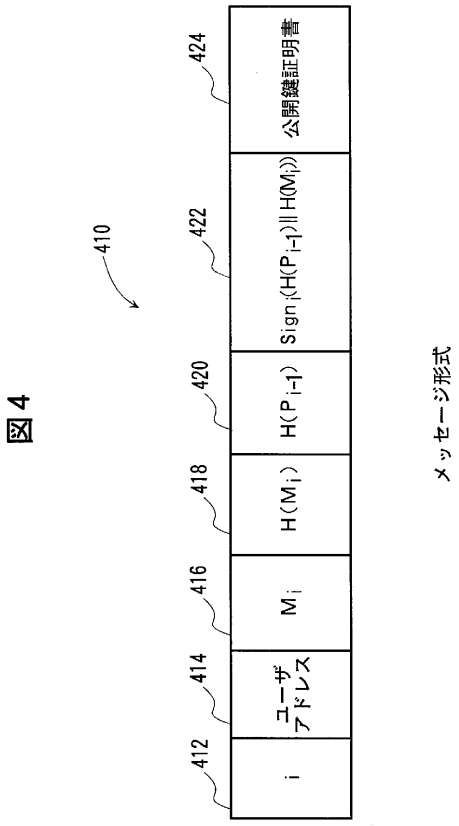
【図２】


図２
有効性回復システム
ネットワーク
有効性回復サーバ
証拠収集サーバ
公証人事務所（リンクなし）
公証人事務所（リンクあり）
ユーザ２
ユーザ１
ログチェーンクロスサーバ
マスメディアサーバ
ウェッブサイト
新聞
210
212
214
216
220
222
224
230
232
234
240

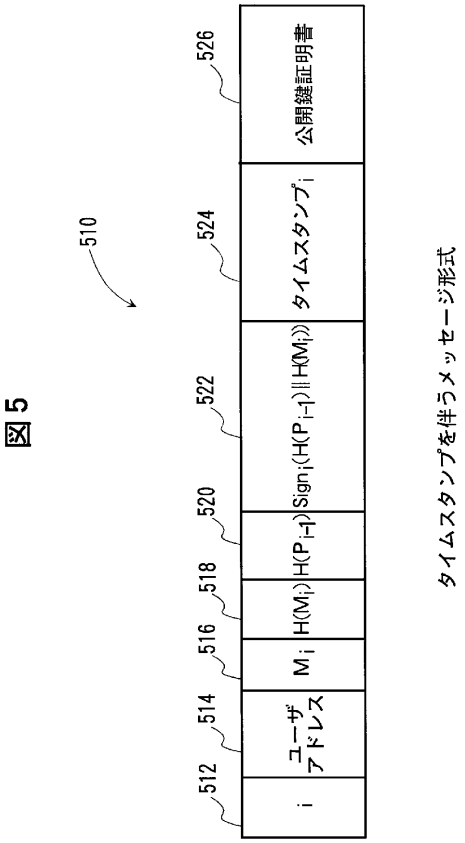
【図３】


図３
CPU
揮発性記憶装置
不揮発性記憶装置
ネットワークインターフェース
I／Oインターフェース
ネットワークへ
ディスプレイ、マウスおよびキーボードへ
コンピュータの例
310
312
314
316
318
320

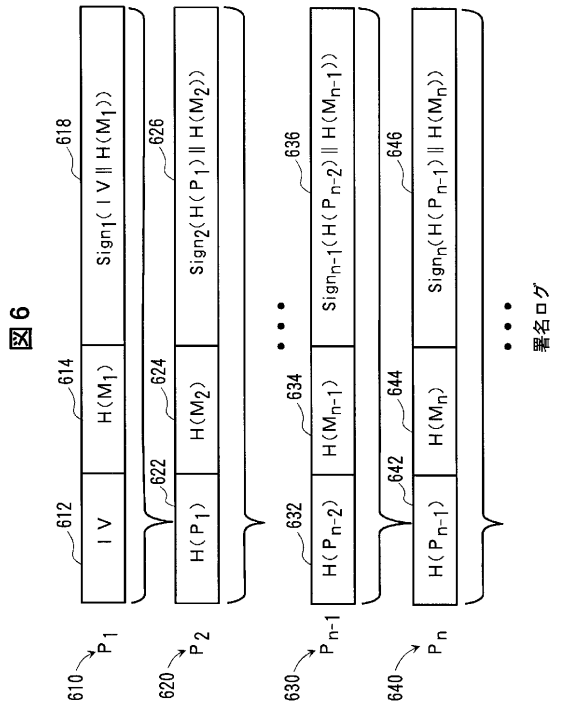
【図４】


図４
メッセージ形式
i
ユーザアドレス
Mi
H(Mi)
H(Pi-1)
Sign(H(Pi-1)||H(Mi))
公開鍵証明書
410
412
414
416
418
420
422
424

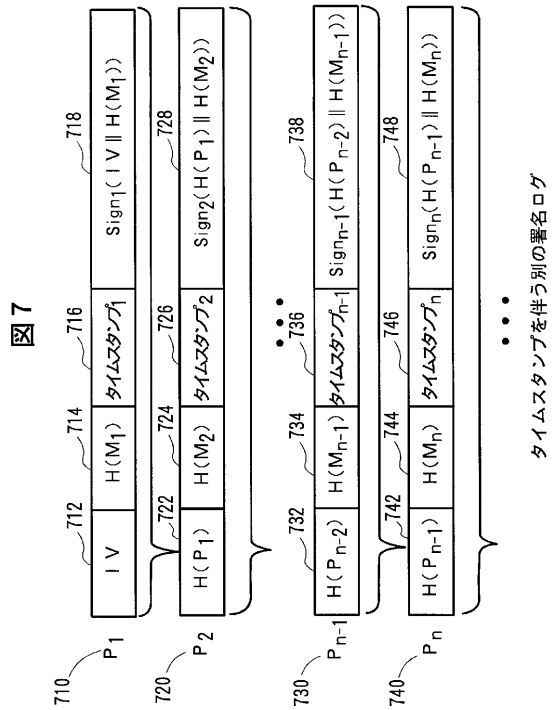
【図５】



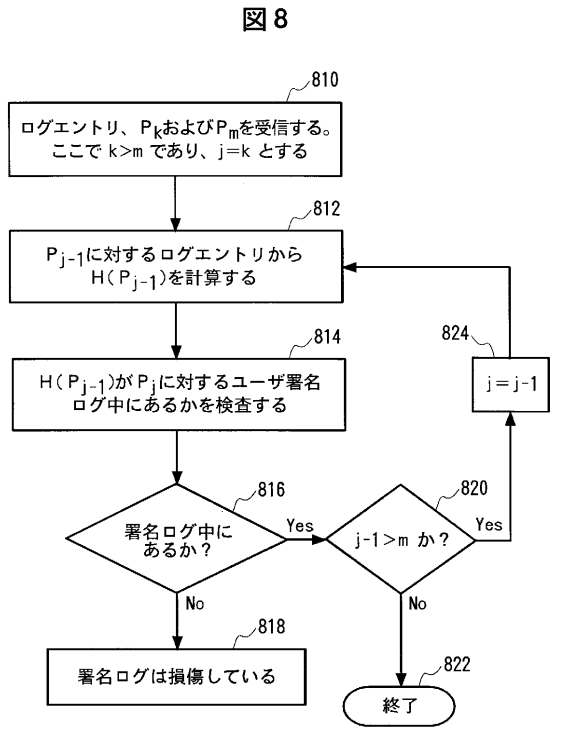
【図６】



【図７】



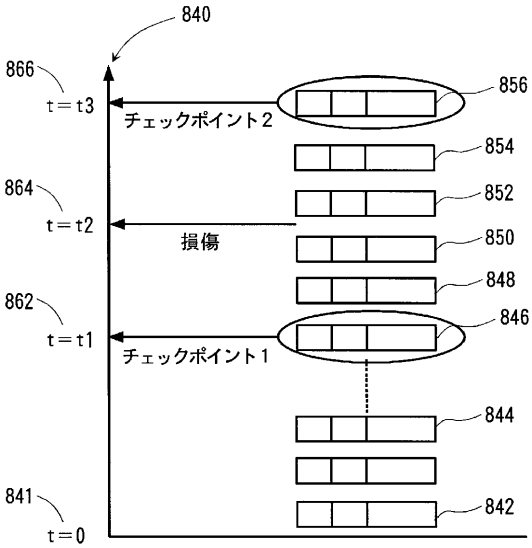
【図８】



ログエントリの確認ー後方連鎖

【図９】

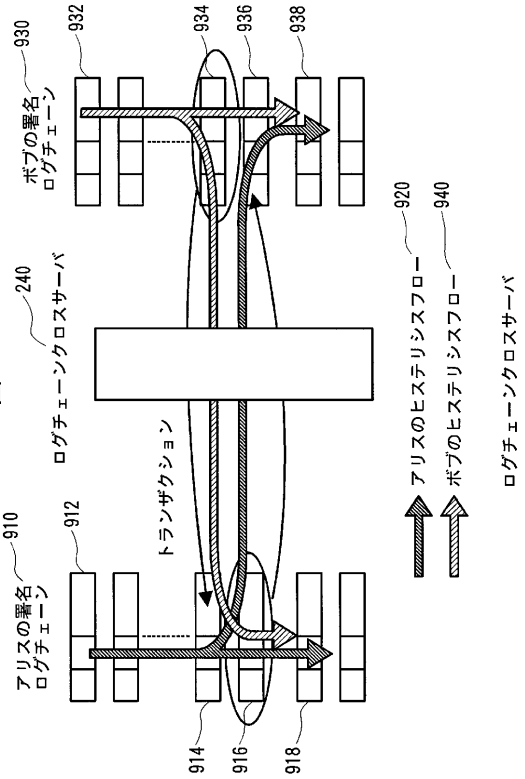
図9



ログエントリのチェックポイント
（たとえば、公開または公証）

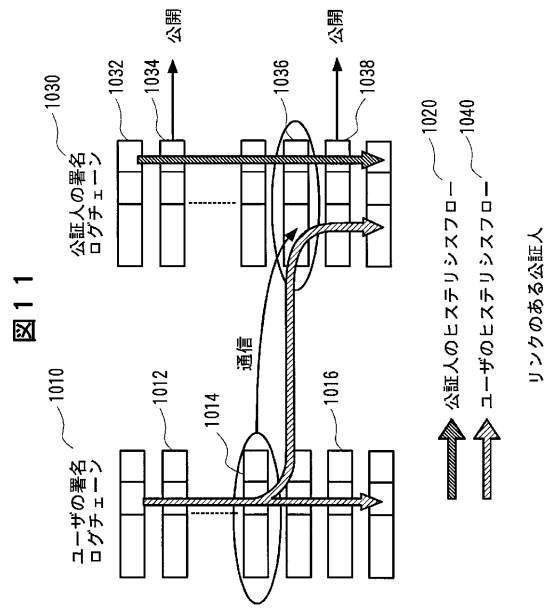
【図１０】

図１０



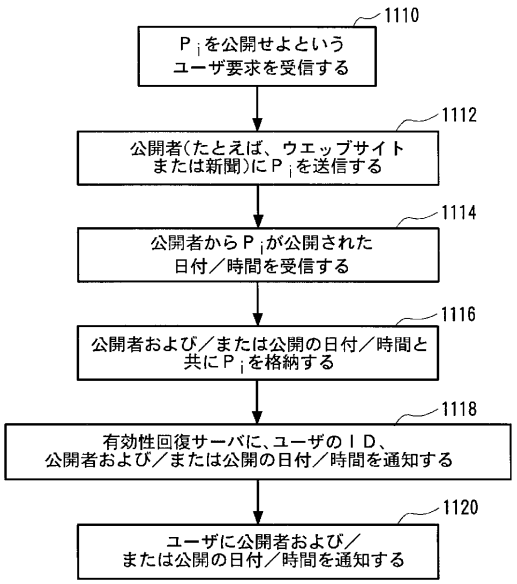
【図１１】

図１１



【図１２】

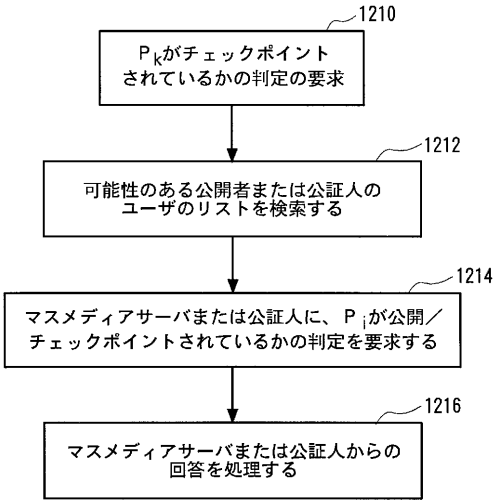
図１２



マスメディアサーバ

【図１３】

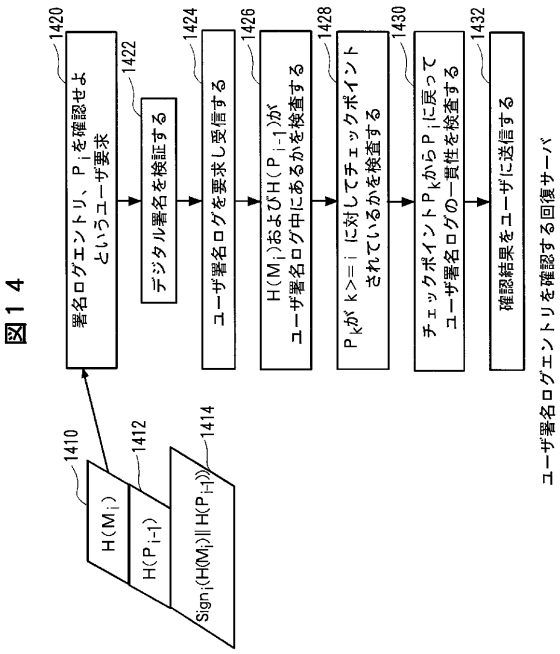
図１３



署名ログエントリがチェックポイント
されているかを判定する回復サーバ

【図１４】

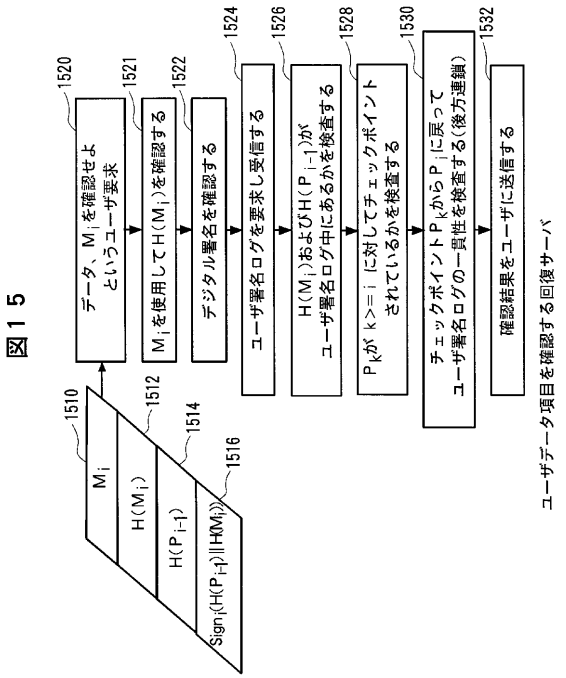
図１４



ユーザ署名ログエントリを確認する回復サーバ

【図１５】

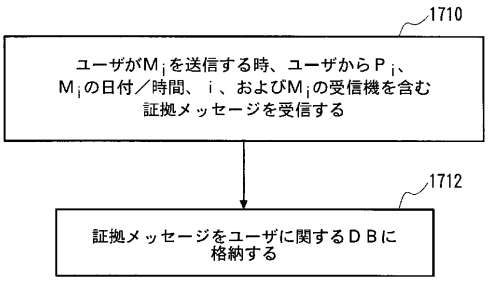
図１５



ユーザデータ項目を確認する回復サーバ

【図１６】

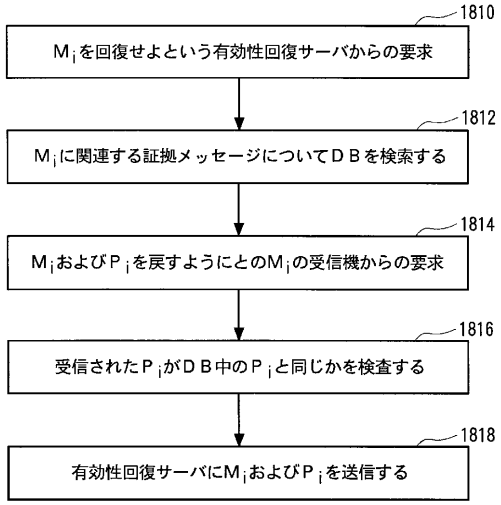
図１６



データを収集する証拠収集サーバ

【図１７】

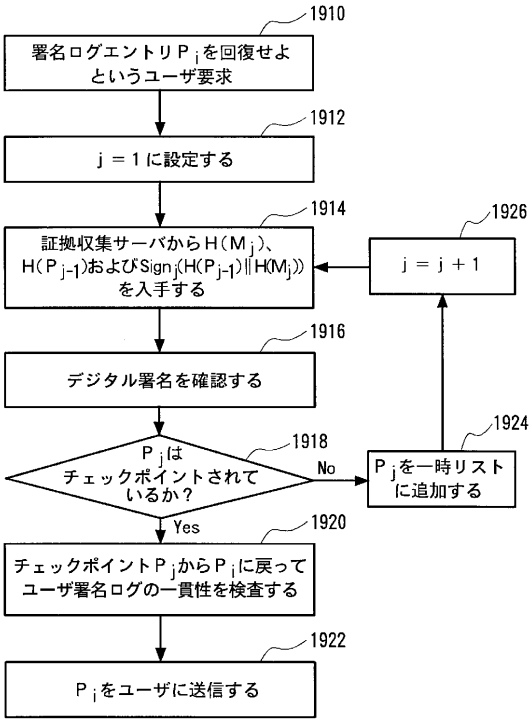
図１７



データを回復する証拠収集サーバ

【図１８】

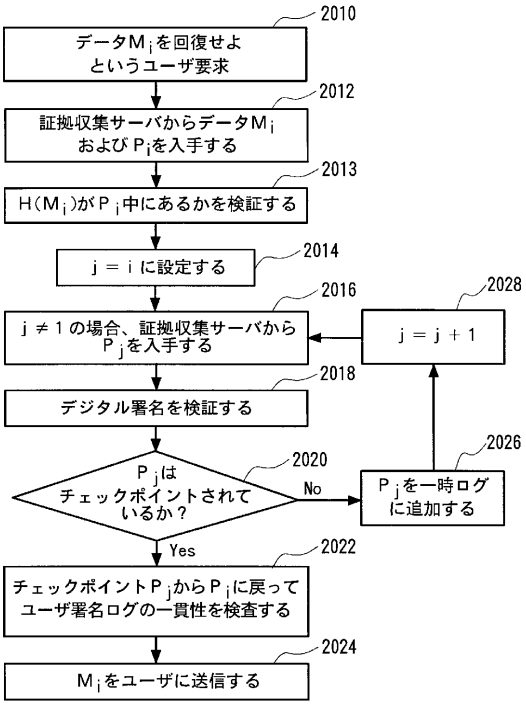
図１８



ユーザ署名ログエントリを回復する回復サーバ

【図１９】

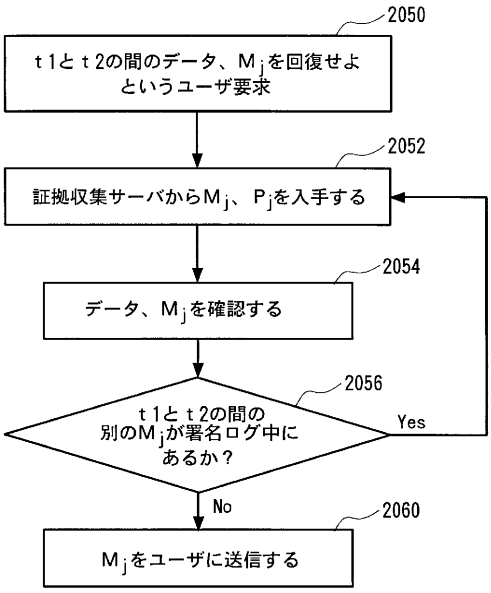
図１９



ユーザデータ項目を回復する回復サーバ

【図２０】

図２０



２つの時点間のユーザデータを回復する回復サーバ

フロントページの続き

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　佐々木　良一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　豊島　久
東京都江東区新砂一丁目６番２７号　株式会社日立製作所公共システム事業部内
(72)発明者　松木　武
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所情報サービス事業部内

審査官　速水　雄太

(56)参考文献　洲崎 誠一 他，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－，情報処理学会研究報告 ２０００－ＣＳＥＣ－８，社団法人情報処理学会，２０００年，Ｖｏｌ．２０００，Ｎｏ．３０，第１９－２４頁
Warwick Ford，Michael S．Baum 著，山田慎一郎 訳，日本ベリサイン株式会社 監修，ディジタル署名と暗号技術，株式会社プレンティスホール出版，１９９７年，第２７６頁
Bruce Schneier，Applied Cryptography：Protocols，Algorithms，and Source Code in C，John Wiley & Sons，Inc.，１９９６年，Second Edition，pp．75-79

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32
G09C　1/00