JP 4044312 B2 2008.2.6

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

特許第4044312号

（Ｐ４０４４３１２）

(45)発行日　平成20年2月6日(2008.2.6)　(24)登録日　平成19年11月22日(2007.11.22)

(51)Int.Cl.　　ＦＩ

Ｇ０６Ｆ　12/00	*(2006.01)*	Ｇ０６Ｆ	12/00	５３７Ｚ
Ｇ０６Ｆ　21/24	*(2006.01)*	Ｇ０６Ｆ	12/00	５１７
Ｇ０６Ｆ　17/30	*(2006.01)*	Ｇ０６Ｆ	12/14	５５０Ｚ
Ｇ０６Ｑ　50/00	*(2006.01)*	Ｇ０６Ｆ	12/14	５６０Ｃ
Ｇ０６Ｑ　10/00	*(2006.01)*	Ｇ０６Ｆ	17/30	１７０Ｚ

請求項の数9　（全15頁）　最終頁に続く

(21)出願番号　特願2001-323085(P2001-323085)
(22)出願日　平成13年10月22日(2001.10.22)
(65)公開番号　特開2003-131922(P2003-131922A)
(43)公開日　平成15年5月9日(2003.5.9)
審査請求日　平成16年6月22日(2004.6.22)

(73)特許権者　503360115
独立行政法人科学技術振興機構
埼玉県川口市本町４丁目１番８号
(74)代理人　100105371
弁理士　加古　進
(72)発明者　西垣　正勝
静岡県浜松市広沢１－２３－１　合同宿舎広沢住宅２－３２
(72)発明者　原田　篤史
静岡県浜松市泉１－１８－３１　サンフォーブル１０３
(72)発明者　曽我　正和
岩手県青森市盛岡駅西通り１－２－１－８０２

最終頁に続く

(54)【発明の名称】データベース・システム

(57)【特許請求の範囲】

【請求項１】

データベース・システムであって、

データ作成者の電子署名を付与されたデータを受けて、前記電子署名を検証するデータ受領検証手段と、

前記データ受領検証手段において、前記電子署名が検証された場合、さらに、付与された前記電子署名に対してシステムの電子署名を付与して、受領したデータを格納する署名格納手段とを備え、

前記データ受領検証手段は、受領したデータがデータベースに格納されているデータに対する修正データである場合、修正対象データの電子署名に対するシステムの電子署名および修正データに対して、修正データ作成者の電子署名が付与されていることを検証するとともに、

前記署名格納手段は、該修正データ作成者の電子署名に対してシステムの電子署名を付与した後、修正対象のデータに追加して、受領した修正データおよび付与したシステムの署名を格納することを特徴とするデータベース・システム。

【請求項２】

請求項１に記載のデータベース・システムにおいて、

前記署名格納手段は、さらに、追加されている修正データをすべて反映したデータとしてまとめ、まとめた者の電子署名および該電子署名に対するシステムの電子署名を付与し、格納されているデータに対して上書きして格納することを特徴とするデータベース・シ

ステム。
【請求項３】
請求項１又は２に記載のデータベース・システムにおいて、
前記署名格納手段は、さらに、データベース中に格納されている他のデータのデータ作成者の電子署名およびシステムの電子署名も、前記システムの電子署名の対象とすることを特徴とするデータベース・システム。
【請求項４】
請求項１～３のいずれかに記載のデータベース・システムにおいて、
前記署名格納手段は、さらに、他のデータベース・システム中に格納されているデータのデータ作成者の電子署名およびシステムの電子署名も、前記システムの電子署名の対象とすることを特徴とするデータベース・システム。
【請求項５】
データベース・システムとデータを送受信する端末システムにおいて、
データベース・システムから受けたデータを閲覧する閲覧手段と、
前記端末での作成データに対して、電子署名を付与する電子署名手段とを備え、
該電子署名手段は、作成データが、前記閲覧手段で閲覧しているデータに対する修正データである場合、修正対象データの電子署名に対するシステムの電子署名および修正データに対して、修正データ作成者の電子署名を付与することを特徴とする端末システム。
【請求項６】
請求項５に記載の端末システムにおいて、
前記閲覧手段は、修正データと修正対象データとを、修正個所およびその修正データ作成者が分かるように合成して表示することを特徴とする端末システム。
【請求項７】
請求項１～４のいずれかに記載のデータベース・システムの各機能をコンピュータ・システムに構成させるためのプログラム。
【請求項８】
請求項５又は６に記載の端末システムの各機能をコンピュータ・システムに構成させるためのプログラム。
【請求項９】
請求項７又は８に記載のプログラムを格納した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、セキュリティを強化したデータベース・システムに関し、特にデータの履歴情報やバージョンを管理するデータベース・システムに関する。
【０００２】
【背景技術】
ネットワークにつながって稼動するシステムにおいて、部外者による攻撃はユーザ認証やファイヤウォールなどを適切に用意することにより、そのセキュリティを強固にすることはできる。しかし、部内者からの攻撃を防ぐことは難しい。部内者はそのシステムやデータにアクセスすることができる正規ユーザであるため、万一、彼らが悪意を持っていた場合にはシステムが悪用され内部のデータが改竄・消去されてしまう。また、悪意は無いにしても操作ミスや過失により同様の結果が起こる危険がある。
一方で、ネットワークを生かした医療データベースや遠隔地医療などの試みが活発化し、その需要や期待も高まっている。医療のネットワーク化の利点を最大限に生かすためにはカルテの電子化が不可欠である。カルテは医療情報故に、患者のプライバシ保護やデータ改竄の防止など、その電子化において高いセキュリティが要求される。
上記のような情報のセキュリティを確保するために、通常はデータをＣＤ－Ｒなどのワンタイム・ライトオンリー型デバイスに書き込むことにより、そのワンタイム・ライトオンリー性を確保していた。電子署名技術を用いれば、データの改竄を検出することが可能で

あり、これにより、データのワンタイム・ライトオンリー性をソフトウェア的に実装することもできるのだが、電子署名によってワンタイム・ライトオンリー型データベースを構築するためにはいくつかの問題が残っていた。

【０００３】

【発明が解決しようとする課題】

本発明は、特殊なハードウェアやデバイスを用いずにデータベースを安全に管理し、さらにデータの履歴情報やバージョンを管理することを目的とする。

【０００４】

【課題を解決するための手段】

上記目的を達成するために、本発明は、データ作成者の電子署名を付与されたデータを受けて、前記電子署名を検証するデータ受領検証手段と、前記データ受領検証手段において、前記電子署名が検証された場合、さらに、付与された前記電子署名に対してシステムの電子署名を付与して、受領したデータを格納する署名格納手段とを備え、前記データ受領検証手段は、受領したデータがデータベースに格納されているデータに対する修正データである場合、修正対象データの電子署名に対するシステムの電子署名および修正データに対して、修正データ作成者の電子署名が付与されていることを検証するとともに、前記署名格納手段は、該修正データ作成者の電子署名に対してシステムの電子署名を付与した後、修正対象のデータに追加して、受領した修正データおよび付与したシステムの署名を格納することを特徴とするデータベース・システムである。

このため、データごとにデータ作成者の電子署名によって守られており、さらに当該データが誰によって作成されたかがわかる。また、データベース・システムによる電子署名も付与されるので、そのデータの作成者でさえ前記のデータを書き換えることができなくなり、データを保護することができる。

【０００５】

前記署名格納手段は、さらに、追加されている修正データをすべて反映したデータとしてまとめ、まとめた者の電子署名および該電子署名に対するシステムの電子署名を付与し、格納されているデータに対して上書きして格納することもできる。

前記署名格納手段は、さらに、データベース中に格納されている他のデータのデータ作成者の電子署名およびシステムの電子署名も、前記システムの電子署名の対象とすることもできる。前記署名格納手段は、さらに、他のデータベース・システム中に格納されているデータのデータ作成者の電子署名およびシステムの電子署名も、前記システムの電子署名の対象とすることもできる。

また、データベース・システムとデータを送受信する端末システムにおいて、データベース・システムから受けたデータを閲覧する閲覧手段と前記端末での作成データに対して、電子署名を付与する電子署名手段とを備え、該電子署名手段は、作成データが、前記閲覧手段で閲覧しているデータに対する修正データである場合、修正対象データの電子署名に対するシステムの電子署名および修正データに対して、修正データ作成者の電子署名を付与することも本発明である。

前記閲覧手段は、修正データと修正対象データとを、修正個所およびその修正データ作成者が分かるように合成して表示することもできる。

本データベース・システムや端末システムの各機能をコンピュータ・システムに構成させるコンピュータ・プログラムおよびコンピュータ・プログラムを記録した記録媒体も本発明である。

【０００６】

【発明の実施の形態】

本発明の実施形態としては、基本的に、ワンタイム・ライトオンリー型データベースであり、データを更新するのではなく、データに付加することにより修正情報を管理する。その際、付加したデータを記入したユーザの秘密鍵で署名を施し、さらにそれをデータベース・システムの秘密鍵により署名をする。このようにして、付加したデータが、どのユーザによるものかを署名により保証することと、データ記入者本人による、改竄の証拠を残

すことなくデータを捏造する不正書き換え等を防止するデータベース・システムである。また、修正データを階層的に付加していくために、バージョン管理が必要となるデータのデータベースとしても有効である。
以下に本発明の実施形態の詳細を図面とともに説明する。
【０００７】
＜電子カルテ管理システム＞
医療システムの電子化やネットワーク化によって遠隔地医療、病院内外における患者情報の共有、緊急時の速やかな患者情報取得などが実現される。医療のネットワーク化においてカルテの電子化は不可欠である。ここで、カルテは以下のような特徴を持ち、電子カルテにおいてもこれらが踏襲される必要がある。
・医師は誰でも自分の患者のカルテを書くことができる。
・医師は誰でも自分の患者のカルテを読むことができる。
・カルテの修正は可能だが、誰が何処をどのように修正したのかが明白でなければならない。
これに加え、カルテには、患者のプライバシ保護やデータ改竄の防止など、その電子化において高いセキュリティが要求される。第三者に患者情報が漏洩したり、第三者によってカルテ情報が改竄されるという危険に対しては、適切なユーザ認証を行なってカルテの読み書きを医師に限定することにより対処が可能であろう。しかし、誤診の事実を隠すために医師自身がカルテを改竄するような事件も発生しており、ユーザ認証のみに頼る方策では電子カルテのセキュリティは完全なものとはならない。
【０００８】
すでにカルテの電子化に関する研究開発は盛んに行なわれており、各メーカが独自に電子カルテ・システムの製品化に力を入れる一方で、記述言語の策定をはじめとした各種標準化作業も進められている。しかし、これらにおけるセキュリティ対策は万全とは言えない。まず、電子カルテ用記述言語において、現段階ではセキュリティに関する要項は仕様外となっている。実際にＭＭＬ(Medical Markup Language)（http://www.seagaia.org）の現バージョンにはセキュリティに関する規定が設けられておらず、セキュリティは電子カルテを運用するアプリケーションに委ねられている。また、現在、製品化されている電子カルテ・システムは商用データベース・システムの上に実装されることが多い。このようなシステムのセキュリティは基本的にデータベース・システムのセキュリティに準じることになる（例えばロータス株式会社のNetkarte R5（http://www.lotus.co.jp/home.nsf/Content/DP1_NetKarte_R50_top）がこれに当たる）。通常のデータベース・システムでは正規ユーザにはデータの変更（証拠が残らない修正）を認めているため、データベース・システムのセキュリティ・レベルで電子カルテ・システムを運用すると、医師が自分の誤診データを改竄するという不正に対する耐性が懸念されることになると思われる。例えば、日本電気株式会社のMegaOak-NEMR（http://www.sw.nec.co.jp/igovcom/medsq/app-info/MegaOak-NEMR/index.html）においては、ワンタイム・ライトオンリー型デバイスにデータを書き込むことにより、この問題を解決している。基本的にはＣＤ－Ｒ等の特殊デバイスを使用するか、または、ファイルシステムを拡張してデータの書き込みを一回のみに制限する。
【０００９】
本発明の一実施形態である電子カルテ管理システムは、全てのカルテ・データに対してシステムに電子署名を施すことによって、各カルテ・データを電子的に封印する。
先述のMegaOak-NEMRでは、ＣＤ－Ｒ等の特殊なデバイスを用いる必要があったり、書き込み回数を制限している機構さえすりぬけてしまえばデータの改竄が可能であったりする。これに対し、本システムでは、各カルテ・データそのものが二重の電子署名により封印されているため改竄に対する耐性が高い。また、カルテ・データに対する電子署名を逐次、階層的に行なうことにより、署名の生成コストが低く、かつ、暗号ブレイクにも強い電子署名方式を実現している。
本システムにより、第三者による改竄はもちろん、カルテの作成者本人の改竄をも防ぐこ

とが可能である電子カルテ・システムが構築される。

【００１０】

（カルテ・データ）

本システムでは、システムが管理しているカルテ・データを「カルテ・オブジェクト」と呼ぶ。ｎ番目のカルテ・オブジェクトを$KO_n^{t_n}$で表す。ここで、t_nはｎ番目のカルテ・オブジェクトの「時刻情報」である。

医師が$KO_n^{t_n}$を読み、これに改変や追記等の修正をしたとする。ここで、医師が修正した実際の記述内容を「カルテ情報」と呼ぶ。このカルテ情報を$KI_n^{t_n}$で表し、システムに登録されている医師なら誰でも閲覧できる。

【００１１】

医師はカルテ情報を記述した際、カルテ情報$KI_n^{t_n}$に署名を付し、システムに登録を依頼する。システムはカルテ情報$KI_n^{t_n}$の正当性をチェックし、それが正当であると認められた場合に限り、カルテ情報$KI_n^{t_n}$を認可し、現在のカルテ・オブジェクト$KO_n^{t_n}$にカルテ情報$KI_n^{t_n}$を加えたデータを新たなカルテ・オブジェクト$KO_n^{t_n}$として登録する。同時に、時刻情報t_nをインクリメントする。すなわち、カルテ情報とは実際のカルテの内容にあたるデータで、修正が行われるたびにその数が増加する。カルテ・オブジェクトとはシステムによって正当であると認められた実効力のあるカルテのことを意味し、複数のカルテ情報や署名がひとまとまりになって形成される。今後、単にカルテという場合はカルテ・オブジェクトを指すことにする。カルテの時刻情報とは、カルテがシステムによって認可されるごとに１つ進められるカウンタ情報である。時刻情報を見ることで、対応するカルテ$KO_n^{t_n}$が何版目のカルテであるか、つまりカルテのバージョン情報を知ることができる。

【００１２】

（システム構成）

図１は電子カルテ管理システムの構成を示す図である。本システムのサーバ２０は、カルテ２２を時刻情報とともに保存／管理する。医師Ａの端末４２～医師Ｚの端末４６はネットワーク１０を介してサーバ２０に接続している。医師Ａ～医師Ｚはシステムに正規ユーザとして登録されている。この登録されている医師は、システムのセキュリティ・ポリシーに準ずる範囲で、システムが管理する全てのカルテを閲覧／修正することができ、かつ、新たなカルテを新規作成することができる。なお、以降、医師Ａの端末とは、医師Ａがシステムにログインしている端末のことを言う。

医師がシステムに登録される際に、本システムのサーバ２０は各医師に対して公開鍵暗号の秘密鍵／公開鍵のペアを生成する。サーバ２０は秘密鍵を医師に渡し、これに対応する公開鍵はサーバ２０が管理する。なお、秘密鍵／公開鍵に関しては、ユーザである各医師が適切な手法によってペアを作り、自分の公開鍵をシステムのサーバ２０に登録してもよい。

以下、医師Ｘの秘密鍵／公開鍵をq_x／p_xとする。システム自身も秘密鍵Ｑと公開鍵Ｐを持つ。システムおよび各医師は、自分の秘密鍵を用いて任意のデータに電子署名を施すことができる。以下、データＤを秘密鍵q_xで署名したものをq_x（Ｄ）と記す。システムは、全ての公開鍵を管理しているので全ての署名を検証することができる。

医師がシステムにアクセスする際には、必ず、システムによってユーザ認証が行なわれる。すわなち、システムに登録されていない医師はカルテへのアクセスはできない。なお、本システムにおいてはユーザ認証の方式は特に問わない。パスワード、バイオメトリクスなど必要に応じた方式を採用すればよい。

また、本方式においては、システムにおける認証方式は十分なセキュリティとフレキシビリティを有するものを用いることを前提としている。すなわち、まず、システムに登録されていない外部のクラッカーがこのシステムに不正に侵入することはできない。そして、システムに登録されている正規の医師であっても自分が診察した患者のカルテ以外にはアクセスできないように本システムは運用されているとする。

【００１３】

（システムの処理の流れ）
図２は本システムにおける、カルテの新規作成、閲覧、修正の処理を示す図であり、図３は、図２の処理で特にカルテの新規作成および修正に関してのサーバ２０の処理の流れを示す図である。以降、この図２と図３を参照して本システムの処理について説明する。なお、本システムの利用者である医師がカルテへアクセスする際、サーバはアクセス要求の度にユーザ認証を行なうのが前提である。また、図２における網掛けされた部分は、新たに作成される又は新たに追加されるデータを示す。
【００１４】
まず、医師Ａが初診患者ｎのカルテを記述する。患者ｎは今回が初診であるので、カルテ$KO_n^{t_n}$は本システムのサーバ２０内には存在しない。時刻情報$t_n = 0$である。医師Ａがカルテ情報KI_n^0を書き、自らの秘密鍵q_Aを用いてそれに署名する（図２▲１▼）。そして医師Ａはカルテ情報KI_n^0とこれに対する署名$q_A(KI_n^0)$をサーバ２０に送信する。サーバ２０は医師Ａが正規ユーザであるか確認をし、医師Ａがシステムに認証されれば（Ｓ２１０）、サーバ２０はそのデータを受理する（Ｓ２１２および図２▲２▼）。
サーバ２０は受け取ったデータが新規に作成されたカルテであるなら（Ｓ２１４でＹｅｓ）、受け取ったデータであるKI_n^0と署名$q_A(KI_n^0)$の整合性を医師Ａの公開鍵p_Aを用いて検証する（Ｓ２１５）。問題がなければ（Ｓ２１６でＹｅｓ）自らの秘密鍵Ｑを用いて、$q_A(KI_n^0)$に対して更にシステムの名で署名をし（Ｓ２１８）、$Q(q_A(KI_n^0))$を作り、これらを結合した$KI_n^0 \| q_A(KI_n^0) \| Q(q_A(KI_n^0))$をカルテ・オブジェクト$KO_n^0$としてデータベースに格納する（Ｓ２２０および図２▲３▼）。なお、ここで「‖」はデータの連結を意味する。そして時刻情報t_nを０から１とする。
次に医師ＢがカルテKO_n^0を参照し、修正したいとする。医師ＢはシステムにアクセスしカルテKO_n^0の閲覧を要求する。医師Ｂがシステムに認証されれば医師ＢはカルテKO_n^0を読むことができる（図２▲４▼）。医師Ｂは修正分のデータKI_n^1を書き、自らの秘密鍵q_Bを用いて、KO_n^0中のシステムの署名$Q(q_A(KI_n^0))$とKI_n^1とに対する署名$q_B(Q(q_A(KI_n^0)) \| KI_n^1)$を生成する（図２▲５▼）。その後、医師Ｂはカルテ情報KI_n^1と署名$q_B(Q(q_A(KI_n^0)) \| KI_n^1)$とを、カルテ$KO_n^0$に対する修正としてサーバ２０に送信する。サーバ２０に医師Ｂが正規ユーザと認証されれば（Ｓ２１０でＹｅｓ）、サーバ２０はそのデータを受理する（Ｓ２１２および図２▲６▼）。
サーバ２０は受け取ったデータが新規に作成されたカルテではない（Ｓ２１４でＮｏ）ので、受け取ったKI_n^1と$q_B(Q(q_A(KI_n^0)) \| KI_n^1)$について、現在保持しているカルテ$KO_n^0$と医師Ｂの公開鍵$p_B$を用いて整合性を検証する（Ｓ２２４）。送られてきたデータが確かにKO_n^0に対する修正であり、かつ医師Ｂによって書かれたことが検証される（Ｓ２２６でＹｅｓ）と、修正者である医師Ｂの署名部分$q_B(Q(q_A(KI_n^0)) \| KI_n^1)$に対してシステムの名で署名し（Ｓ２２８）、$Q(q_B(Q(q_A(KI_n^0)) \| KI_n^1))$を生成する。これら全体を結合した、$KO_n^0 \| KI_n^1 \| q_B(Q(q_A(KI_n^0)) \| KI_n^1) \| Q(q_B(Q(q_A(KI_n^0)) \| KI_n^1))$をカルテ・オブジェクト$KO_n^1$としてデータベースに格納する（Ｓ２３０および図２▲７▼）。そして時刻情報t_nを１から２とする。
他の医師（医師Ａ、医師Ｂを含む）が更にこのカルテに修正を加えたい場合には、図２▲４▼から同様の手順を繰り返すことになる。
【００１５】
このように、カルテ・オブジェクト$KO_n^{t_n}$には、システムだけでなく、当該カルテにカルテ情報を記述した全ての医師の電子署名が含まれる。よって、カルテ・オブジェクトを完璧に改竄しよう（改竄したことが検出されないようにデータを改変しよう）とするには、システムおよび該当する全ての医師の秘密鍵を入手しなくてはならないため、改竄するのは非常に難しくなっている。また、医師がカルテへアクセスする際、アクセスする度

にユーザ認証を行なっているので第三者にカルテが漏洩することはない。

【００１６】

なお、新しい署名を生成する際には、必ず以前の署名データ（署名の一部）を使用することで新しい順に署名を連鎖的に検証していくことによって全体の改竄の有無をチェックすることができる。すなわち、本署名方式はヒステリシス署名（松本勉，岩村充，佐々木良一，松本武，暗号ブレイク対応電子署名アリバイ実現機構（その１）－コンセプトと概要－，情報処理学会コンピュータセキュリティ研究会研究発表会，2000年３月）の一種である。このため、適当な時間間隔ごとにカルテ・オブジェクト内の署名データの一部などを信頼ポイント（州崎誠一，宮崎邦彦，宝木和夫，松本勉，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－，情報処理学会コンピュータセキュリティ研究会研究発表会，2000年３月）として設定することにより、仮に不正者にシステムおよび全ての医師の秘密鍵を入手されたとしてもなお、ある程度の暗号化強度が保たれる。

【００１７】

また、カルテ情報が追加されて大きくなっていっても、それに署名を付加する際の処理時間や、生成される署名の大きさはほとんど変わらない。これは署名処理の対象になるのが新たに追加されたカルテ情報と１回前の署名とに限られるからである。また、カルテは修正されるごとにシステムにより署名されるので、ひとたびシステムに送られて登録されたカルテ・オブジェクトを改竄することは、そのカルテを書いた医師本人にさえ不可能である。

なお、カルテ情報の署名に関しては、カルテ情報に対する電子署名をそのまま計算したものでもよいし、カルテ情報を適当な一方向関数によってハッシュ化したデータに対する電子署名を用いても構わない。ハッシュ化データに対する電子署名とすることにより、電子署名を計算する時間を更に短縮することができる。その際、電子署名の検査は、電子署名を公開鍵により復号したデータとカルテ情報を同一の一方向関数によってハッシュ化したデータが一致するかをチェックすることになる。

【００１８】

（カルテの記述と表示スタイル指定）

本システムでは、複数の医師に書かれた多数のカルテ情報が、ひとまとまりになって１つのカルテを形成する。このようなデータ集合体であるカルテ・オブジェクトを記述するための手法は限定しない。本実施形態の一例として、効率よく記述するためにＸＭＬ(eXtensible Markup Language)形式を用いることができる。

ＸＭＬは、テキスト形式によるデータ記述フォーマットの次期標準であり、広い用途での利用が期待できる。ＭＭＬとの親和性も高い。多数の医師が同じ形式でカルテ情報を記述して、それを１つのカルテとしてまとめる処理はＸＭＬを用いると容易である。また、テキスト形式であるＸＭＬでカルテを記述すればデータの記述や追加が容易であり、かつ、カルテ情報の閲覧も簡単である。主要なブラウザがＸＭＬに対応しており、ネットワーク環境でブラウザを用いてカルテの閲覧、記述、修正を行なうような遠隔地医療システムにも適している。そのほか、ＸＭＬは画像や音声などのマルチメディア情報を統合することもでき、カルテの情報にレントゲン画像などを付加して送信するといった応用も可能になる。

【００１９】

図４はＸＭＬを用いたカルテの記述例を示す図であり、図４（ａ）は修正前のカルテ、図４（ｂ）は修正後のカルテである。ＸＭＬはタグを自由に定義できるので見読性の高い記述が可能である。ここでは例として修正情報を表す<modification>タグや診断症状を定義する<diagnosis>タグ、そして署名を定義する<sign>タグを定義して、カルテ情報や医師とシステムの署名をテキスト形式で記述している。

図４（ａ）のカルテの記述に医師Ｂが修正情報を追加する場合、図４（ｂ）のように以前のデータを残したまま、直後に修正情報を追加する。修正用に定義された<modification>タグを用いて、修正したい個所を指定して修正後の情報を記述するだけでよい。このタグ内に、version=1 として上述の時刻情報を埋め込むこともできる。

このように、ＸＭＬを用いると非常に簡単にカルテを記述できる。また、ＣＳＳ(Cascading Style Sheets)やＸＳＬ(eXtensible Style Language)といったスタイル指定言語を用いて表示スタイルを定義することによって、ブラウザ等でＸＭＬ文書を自由な形式で表示させるようにしてもよい。

【００２０】

図５は図４（ｂ）のカルテ情報の画面表示例を示す図である。ＸＭＬで記述されたカルテ情報を医師がブラウザ等を用いて閲覧する際に、誰がどこをどのように修正したのかが明確であるように表示している。また、閲覧のためにカルテを表示する場合、まずはカルテ情報$KI_n^{t^n}$のみを表示しておき、医師がカルテ情報を読んでいる間に、そのカルテの改竄の有無を調べるためにバックグラウンドで署名の検証をし、結果を画面に表示するような処理も同時に行わせることもできる。

上述の端末における処理は、汎用ブラウザに対する適切なプラグインを作成することによりできる。このプラグインは、汎用ブラウザとともに、上述した様にデータを表示し、かつ、署名を検証するところまでの全ての処理を実装している。

【００２１】

（電子カルテ管理システムの効果）

本システムは従来のカルテの持つ特徴を維持しつつ、高度なセキュリティとともに電子化し、カルテを記述した医師本人はもちろん、他人による電子カルテ情報の改竄をも防止することができる。

【００２２】

＜ダブルチェック・データベース・システム＞

本発明はカルテに限らず、ワンタイム・ライトオンリー型の電子データや、バージョン管理を行なう必要のあるデータを管理する際にも有効である。本発明の他の実施形態の詳細を以下に説明する。

本ダブルチェック・データベース・システムは、操作ミスや破壊行為からデータを守ることのできるデータベース・システムである。上述の電子カルテ管理システムでは、データに修正を行う場合に、データそのものを上書きするのではなく、修正情報を付加していくことにより電子カルテにワンタイム・ライトオンリーの性質を与えていた。これを通常のデータ（ワンタイム・ライトオンリー型以外のデータ）に対して応用することにより、部内者（そのデータの読み／書きの権利を与えられているユーザ）が過失により、またはクラッカーだけでなく部内者が故意にデータを破壊するという攻撃を防止することができるデータベース・システムを実現する。

【００２３】

（システム構成）

図６は本ダブルチェック・データベース・システムの構成を示す図である。本システムのサーバ１２０はデータ１２２を保存・管理する。部下Ａ～部下Ｚが用いる端末１４２～１４８と上司の端末１３０はネットワーク１１０を介してサーバ１２０にも接続されている。

そして、部下Ａ～Ｚはデータ１２２の閲覧、新規作成、修正（追加）をする権限を持つ。上司は、部下が作成したデータを定期的に検証し、承認する立場にある者とする。部下Ａ～Ｚはシステムに保存するデータに対して修正を行えるが、修正前のデータそのものを修正後のデータによって上書きすることはできず、修正前のデータの後に修正情報を付加することのみが可能である。上司のみが、修正前のデータに付加された修正情報を検証し、修正前のデータを修正情報に反映させた修正後のデータで上書きすることができる。

【００２４】

（処理の詳細）

図７は処理の流れとシステムが保持するデータの変化を示す図である。この図７を用いて、本システムの処理を説明する。なお、以下で取り扱うデータは上述の電子カルテ管理システムで用いたＸＭＬ等のテキストのデータでもよいし、コンピュータ上で走るアプリケーション・プログラム等のデータでもよい。また、図７における網掛けされた部分は、新

たに作成される又は新たに追加されるデータを示している。
まず部下Ａがデータ１を新規作成する。Ａは自分の秘密鍵を用い、データ１に対して署名をする。Ａはデータ１および署名文をサーバ１２０に送信する。サーバ１２０は適切なユーザ認証および署名の検証を行った上で、データ１に対して署名を施す。サーバ１２０はデータ１＋Ａの署名文＋システムの署名文を保存する。ここで、署名は上述の電子カルテ管理システムと同様階層的に行われ、システムはＡの署名文に対する署名のみを行う（図７▲１▼）。
次に、部下Ｂがシステムにデータ閲覧を要求してデータ１をＢの端末１４４に表示し、Ｂはそれに対して修正を行い、修正データに対して署名をする。その後、修正情報および署名文をサーバ１２０に送信する。サーバ１２０は適切なユーザ認証および署名の検証を行い、Ｂによる修正情報と署名文に対してシステムの署名を施す。サーバ１２０はＢによる修正情報と署名文とシステムの署名文を、現在保持しているデータ１の後に付加して保存する。なお、この時点ではデータ１そのものは上書きされない（図７▲２▼）。
再び部下Ａがサーバ１２０にデータ閲覧を要求する。サーバ１２０はデータ１に対してＢの修正を施した内容をＡの端末１４２に表示する。ＡはＢによって修正されたデータ１を読み、それに対してさらに修正を行い、修正データに対して署名をする。Ａは修正情報とＡの署名文をシステムに送信し、サーバ１２０はＡによる修正情報と署名文を現在保持しているデータ１とＢの修正情報の後に付加して保存する。なお、この時点でもデータ１及びＢによる修正情報は上書きされない（図７▲３▼）。
部下が作成したデータを検証・承認することのできる上司は、定期的にデータに対する修正情報を検証する。ここでは、Ａが新規作成したデータ１、データ１に対するＢによる修正、Ａによる修正をチェックし、問題がないと承認した場合にそれらの修正情報をデータ１に反映し、上司は署名をする。上司はデータ１に修正情報を反映したデータ２および署名文をサーバ１２０に送信する。サーバ１２０は適切なユーザ認証および署名の検証を行った上で、サーバ１２０は保持しているデータ群を修正反映後のデータ２と上司の署名およびシステムの署名で上書きする。これによりデータ１そのものが上書きされる（図７▲４▼）。
さらに、このデータ２に部下Ｃにより修正が加えられる場合は、図７▲２▼から同様の手順を繰り返す（図７▲５▼）。
【００２５】
（ダブルチェック・データベース・システムの効果）
本システムは、データの修正が行われる場合に、修正前のデータを修正後のデータで上書きするのではなく、修正前のデータに修正情報を付加することによって、修正の過程がデータとして残るようになっている。そのため、上司が部下によるデータの修正の過程を定期的に検証し、異常を発見した場合に異常が発生する前のデータへと書き戻すことが可能であり、部内者によるデータの破壊に対抗することができる。
対象システムがデータベースなどの場合は、データを検索したり加工したりすることが頻繁に起こる。その際、検索や加工の要求が来るたびに毎回、データと修正情報から最新データを生成する方式では効率が悪い。このような場合には、データを常に最新情報に上書きすることにし、修正前のデータに戻すための情報を付加していく方式とすればよい。
なお、データの検閲を行うスーパーバイザとして上司を例に採り説明したが、実際には部下どうしでデータのダブルチェックを行っても構わない。
【００２６】
＜他の実施形態＞
（システムの信頼性の向上をはかる）
次に、上述の同一文書における修正データの署名を連鎖させるだけにとどまらず、本方式を異なった文書間においても署名を交換して利用し合うように拡張することで、文書の改竄をより困難にし、システム全体の信頼性を向上させることもできる。
図８は、システムが文書２に対する署名の生成の際に、文書１の署名データも使用することによって、文書１の署名が文書２の署名に取り込まれる例を示す図である。図８におい

て、Ｃによって作成された文書２に対して、システムにより署名を行うときに、Ｃによる署名のみならず、文書１のＢによる修正１に対するシステムの署名も用いて署名を行う。この図８の例においては、文書１の「修正１」部分を完全に改竄（改竄したことが検出されないようにデータを改変）しようとするには、文書１における「修正１」以降の署名をすべて偽造することはもちろん、更に文書２において新規データに対するシステムによる署名とそれ以降の署名も全て偽造しなくてはならず、明らかに他文書の署名を利用しない場合よりも文書改竄は困難になる。また、システム及び文書１の作成・修正に関わった全ての文書作成者の秘密鍵が漏洩することにより、文書１が信頼できなくなった場合でさえも、文書２が信頼できるならば、文書２に署名が渡された時点（ここが「信頼ポイント」と呼ばれる）までの文書１の信頼性を確保できる。

【００２７】

図９は多数の文書間で幾重にも署名の交差を行うシステムを示す図である。図９において、各文書における黒丸および矢印は、各文書の署名を他の文書の署名に利用していることを示している。

図８では２文書間の署名交差の例であったが、同様のしくみで、図９のように多数の文書間で幾重にも署名の交差を行うようにすると、完全に改竄しようとする場合、１つの文書を改竄するために同時に多数の文書の署名を改竄しなくてはならなくなり、文書の改竄困難性は飛躍的に増大する。そして、他文書中に多数の信頼ポイントを置くことで各文書の信頼性も向上する。

【００２８】

図１０は異なるデータベース間の文書の署名を交差させるシステムを示す図である。図９は１つのデータベース・システム内の異なる文書の署名を交差させる例であったが、この図１０に示すシステムは更にこれを拡張して、異なるデータベース間の文書の署名を交差させる。

【００２９】

図８～１０で説明した上述のシステムでは、改竄対象となるデータの後に多くの修正データが存在するほど改竄の手間が増加することになる。

署名の交差のタイミングは文書が修正される際にシステムによって行われるが、文書に対する修正が頻繁になされるとは限らない。そこで、文書に修正がなされなくても、システムが定期的に（例えば１日１回）署名交差を行うようにするとよい。その場合、修正データが無い部分に対してはシステムの署名が二重に掛かるようになる。図１１はシステムによる定期的な署名交差により署名が二重にかかっているところを示す図である。図１１において、決められた時刻に、ＤＢシステム１では、その時の最終の自システムのシステム署名と、ＤＢシステム２のシステム署名とを用いて、新たにシステムによる署名が作成されて付与されたことを示している。

【００３０】

（故意または事故により破壊された文書を復旧する）

図１２は文書のバックアップを他のデータベース・システムに分散して配置するシステムを示す図である。実際の運用では、文書の改竄や破損が検出できるだけでは不十分であり、改竄や破損で壊れた文書を正しい文書に書き戻すための復旧処理が必要である。そこで図１２に示すように、文書のバックアップをとっておいて、それを別の場所に保存するように図１１のシステムを拡張している。

システムの管理者が悪意を持ってデータベース・システム内の全てのデータを破壊することをも防ぐためには、バックアップ用データは同一システム内にのみではなく、他のデータベース・システムにも分散して配置するべきである。

【００３１】

図１２において、データベース・システム１は、自身の管理する文書１のバックアップ・データを秘密分散の技法などを用いてｎ－１個のデータ片２～ｎに分割し、それぞれに署名を付す。そして、各データ片と対応する署名を署名交差の際にシステム２～ｎのｎ－１個の文書へ付加する。データベース・システム２～ｎはこれを受けて、データ片とその署

名データに対して更に署名を施す。このようなバックアップは、他の文書にバックアップ片を組み込むことから、署名交差とも見なせ、セキュリティの向上にも関与する。そして、何らかの理由で文書１の破損が認められた場合には、システム２～ｎは文書２～ｎに付加されていたデータ片をシステム１に提出する。システム１は送られてきたデータ片を結合してバックアップ・データを復元し、文書を復旧することができる。また、秘密分散の技法を適切に用いることで、各データ片から文書１の情報が漏洩することを防ぐことや、ｎ－１個すべてのデータ片が集まらなくてもバックアップ・データを復元できるようにすることも可能である。

【００３２】

上述のデータベース・システムを構成するためのプログラムは、格納した記録媒体から読み出したり、通信回線を介して受信等をしたプログラムを実行する等により、本発明の構成を実現することもできる。この記録媒体には、フロッピー・ディスク、ＣＤ、ＤＶＤ、磁気テープ、ＲＯＭカセット等がある。また、通信回線としては、インターネット等がある。

【００３３】

【発明の効果】

上記の発明により、特殊なハードウェアやデバイスを用いずにデータベースを安全に管理し、さらにデータの履歴情報やバージョンを管理することが可能となった。

【図面の簡単な説明】

【図１】電子カルテ管理システムの構成を示す図である。

【図２】電子カルテ管理システムのカルテの新規作成、閲覧、修正の処理を示す図である。

【図３】電子カルテ管理システムのカルテの新規作成、修正の際のサーバの処理の流れを示す図である。

【図４】ＸＭＬを用いたカルテの記述例を示す図である。

【図５】カルテ情報の画面表示例を示す図である。

【図６】ダブルチェック・データベース・システムの構成を示す図である。

【図７】ダブルチェック・データベース・システムの処理の流れとシステムが保持するデータの変化を示す図である。

【図８】他の文書の署名を取り込んで書名をするシステムを示す図である。

【図９】多数の文書間で署名の交差を行うシステムを示す図である。

【図１０】異なるデータベース間で文書の署名を交差させるシステムを示す図である。

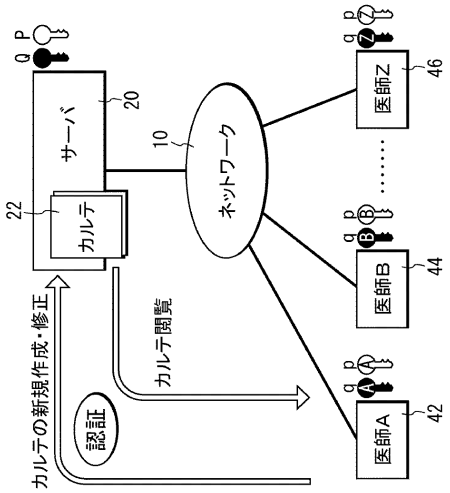
【図１１】システムによる定期的な署名交差により署名が二重にかかっているところを示す図である。

【図１２】文書のバックアップを他のデータベース・システムに分散して配置するシステムを示す図である。

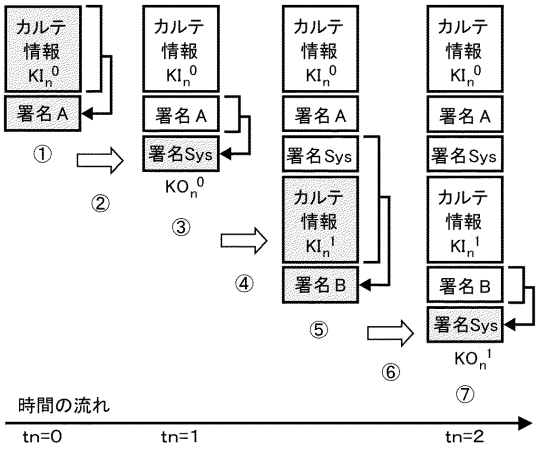
【符号の説明】

１０　ネットワーク
２０　サーバ
２２　カルテ
４２，４４，４６　端末
１１０　ネットワーク
１２０　サーバ
１２２　データ
１３０，１４２，１４４，１４６，１４８　端末

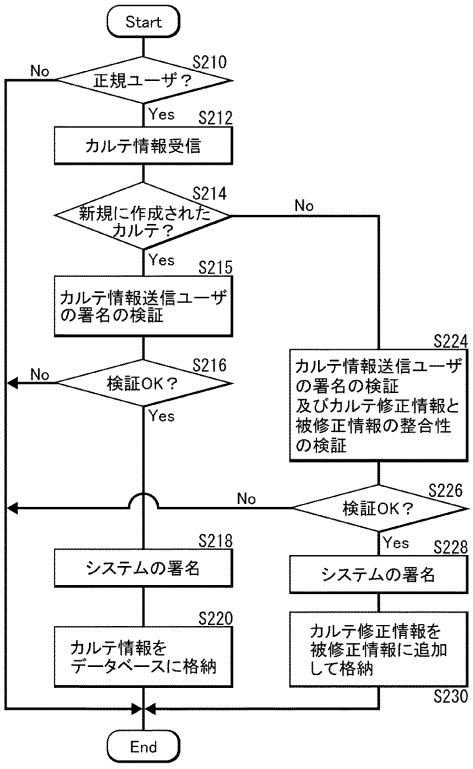
【図１】



【図２】



【図３】



【図４】

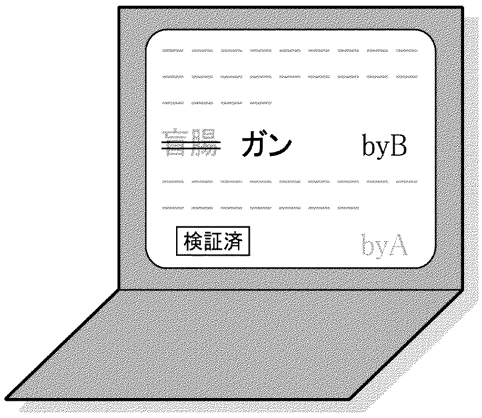
(a)

```
<karte>
  <KI>
    <name> 静岡太郎 </name>
    <diagnosis> 盲腸 </diagnosis>
  </KI>
  <sign name= "A"> mEgx90s8... </sign>
  <sign name= "SYS"> h8s2fsa...</sign>
</karte>
```

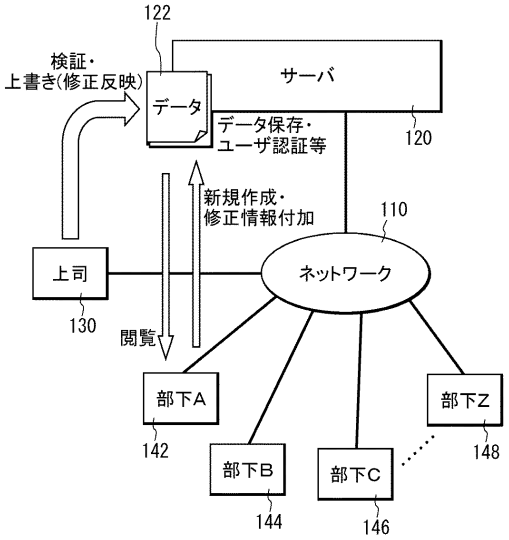
(b)

```
<karte>
  <KI>                                   ┐
    <name> 静岡太郎 </name>              │
    <diagnosis> 盲腸 </diagnosis>        │ 以前のデータは
  </KI>                                  │ そのまま残す
  <sign name="A"> mEgx90s8... </sign>    │
  <sign name="SYS"> h8s2fsa...</sign>    ┘
  <KI>                                   ┐
    <modification version=1>             │
      <diagnosis> ガン </diagnosis>      │ 修正情報
      <sign name="B"> u82sxUlw...</sign> │ を追加
    </modification>                      │
  </KI>                                  │
  <sign name="SYS"> y23lsaA.. </sign>    ┘
</karte>
```

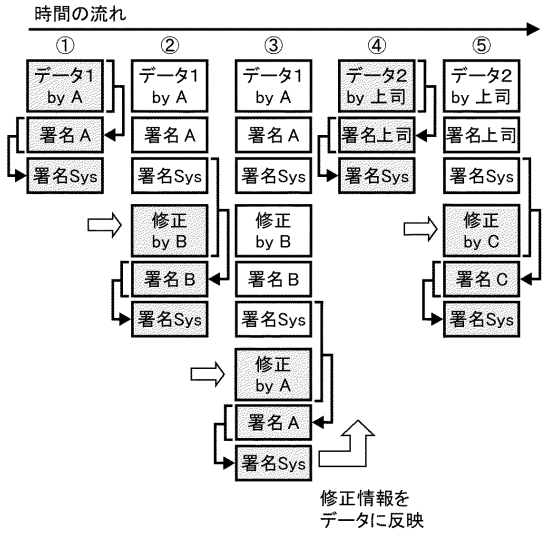
【図５】


ガン
byB
検証済
byA

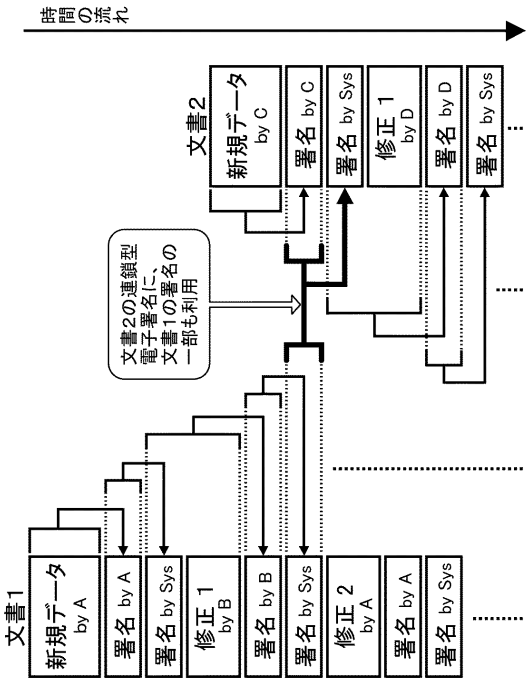
【図６】


122
検証・
上書き(修正反映)
データ
サーバ
データ保存・
ユーザ認証等
120
新規作成・
修正情報付加
110
上司
130
ネットワーク
閲覧
部下A
142
部下B
144
部下C
146
部下Z
148

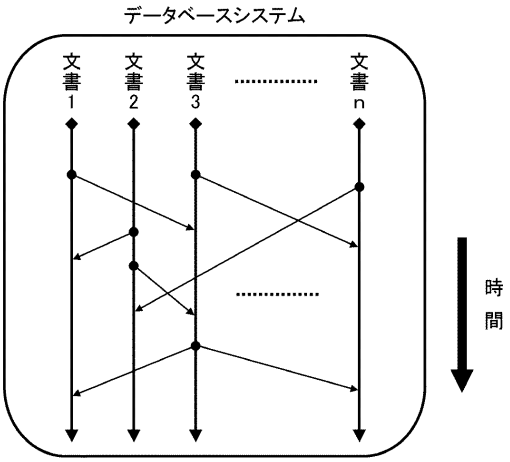
【図７】


時間の流れ
①
②
③
④
⑤
データ1 by A
署名 A
署名Sys
修正 by B
署名 B
修正 by A
データ2 by 上司
署名上司
修正 by C
署名 C
修正情報を
データに反映

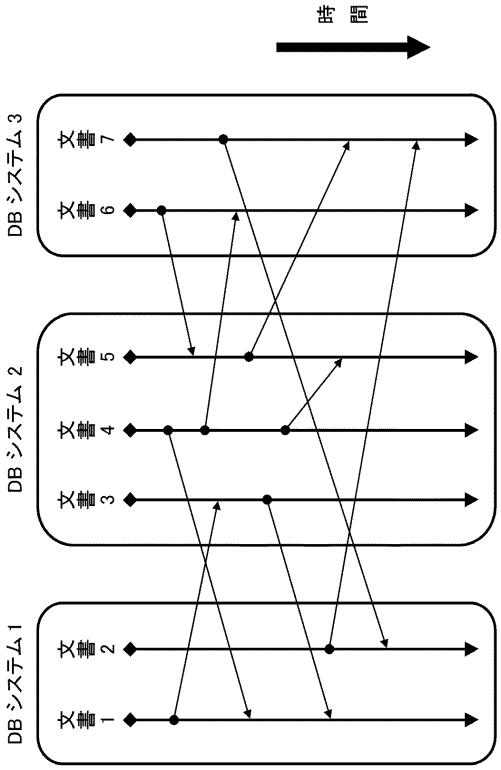
【図８】


時間の流れ
文書2
新規データ by C
署名 by C
署名 by Sys
修正 1 by D
署名 by D
署名 by Sys
文書2の連鎖型電子署名に、文書1の署名の一部も利用
文書1
新規データ by A
署名 by A
署名 by Sys
修正 1 by B
署名 by B
署名 by Sys
修正 2 by A
署名 by A
署名 by Sys

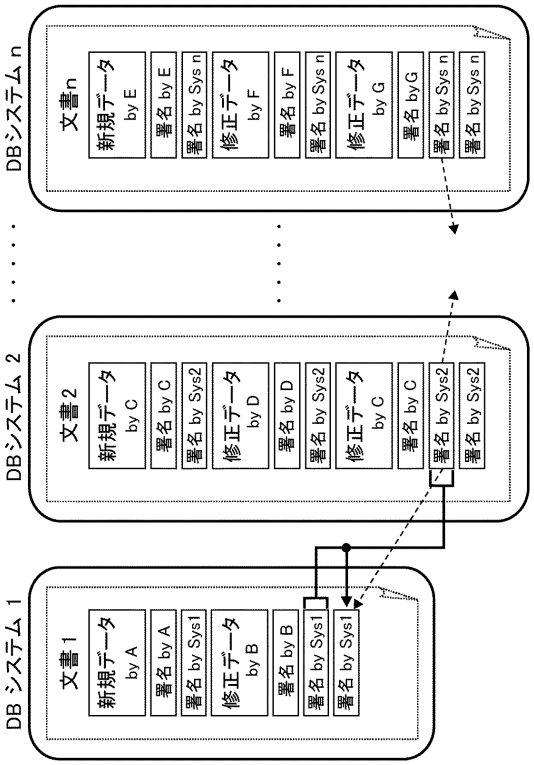
【図９】



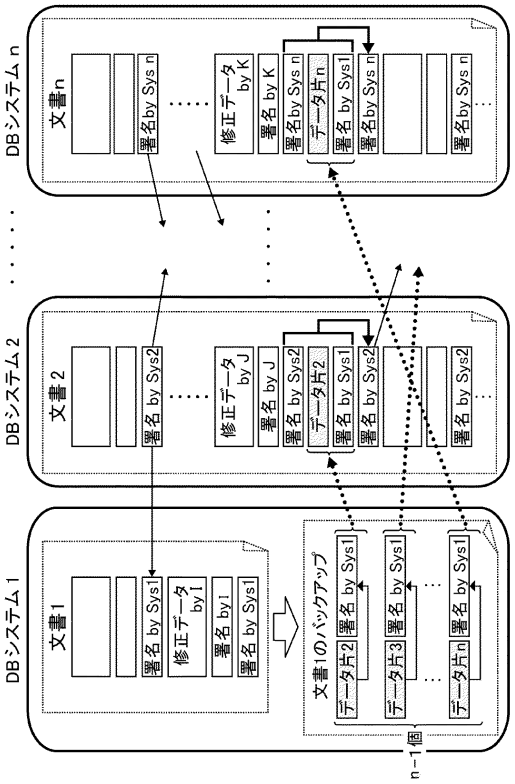
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.			FI		
Ｇ０９Ｃ	*1/00*	*(2006.01)*	Ｇ０６Ｆ	17/60	１２６Ｋ
			Ｇ０６Ｆ	17/60	５１２
			Ｇ０９Ｃ	1/00	６４０Ｄ

(72)発明者　田窪　昭夫
神奈川県横浜市栄区桂台南２－３７－６

審査官　石川　正二

(56)参考文献　特開平１０－２８３２６３（ＪＰ，Ａ）
特開平０６－２２４８９６（ＪＰ，Ａ）
特開平０６－３１５０３６（ＪＰ，Ａ）
特開平１０－２８３２６４（ＪＰ，Ａ）
特開平１０－２８９５２３（ＪＰ，Ａ）
特開平１０－０８３２９７（ＪＰ，Ａ）
松本　勉，暗号ブレイク対応電子署名アリバイ実現機構（その１）－コンセプトと概要－，情報処理学会研究報告　２０００－ＤＰＳ－９７　２０００－ＣＳＥＣ－８，日本，社団法人情報処理学会，２０００年　3月２２日，第2000巻，第30号，pp.13-17，CSDB:NG-2001-00133-003
洲崎　誠一，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－ＤＰＳ－９７　２０００－ＣＳＥＣ－８，日本，社団法人情報処理学会，２０００年　3月２２日，第2000巻，第30号，pp.19-24，CSDB:NG-2001-00133-004

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　12/00
G06F　17/30
G06F　21/24
G06Q　10/00
G06Q　50/00
G09C　 1/00