

(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.	F 1	
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)	(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
(22) 出願日	平成13年10月22日(2001.10.22)	(74) 代理人	100105371 弁理士 加古 進
(65) 公開番号	特開2003-131922 (P2003-131922A)	(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
(43) 公開日	平成15年5月9日(2003.5.9)	(72) 発明者	原田 篤史 静岡県浜松市泉1-18-31 サンフ ーブル103
審査請求日	平成16年6月22日(2004.6.22)	(72) 発明者	曾我 正和 岩手県青森市盛岡駅西通り1-2-1-8 02

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

10

20

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。

10

【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、修正箇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。

20

【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。

30

【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ア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。

40

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、患者のプライバシー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

50

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、修正箇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

10

20

30

40

50

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。

【 0 0 0 7 】

< 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、患者のプライバシー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。

【 0 0 0 8 】

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、各メーカー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 M M L (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 C D - 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。

【 0 0 0 9 】

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、C D - 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

10

20

30

40

50

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。すなわち、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】

10

20

30

40

50

(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、 $KO_n^0 \ KI_n^1 \ q_B(Q(q_A(KI_n^0)) \ KI_n^1) \ Q(q_B(Q(q_A(KI_n^0)) \ KI_n^1)) \ KI_n^1$ 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

10

20

30

40

50

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ライバイ実現機構（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ライバイ実現機構（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。

10

【0017】

また、カルテ情報が追加されて大きくなっていても、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。

20

【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。

30

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。

40

【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。

50

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。

10

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нта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。

20

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нта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нта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。

30

【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。

40

【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

50

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

10

20

30

40

50

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。

10

【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】

20

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。

30

【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において、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。

40

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ものみではなく、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

50

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。

10

【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。

20

【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。

30

【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。

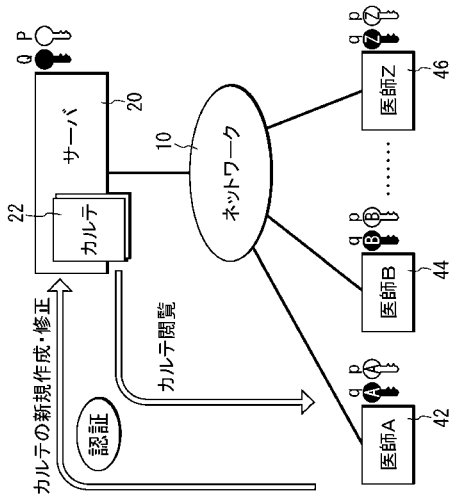
【図12】文書のバックアップを他のデータベース・システムに分散して配置するシステムを示す図である。

【符号の説明】

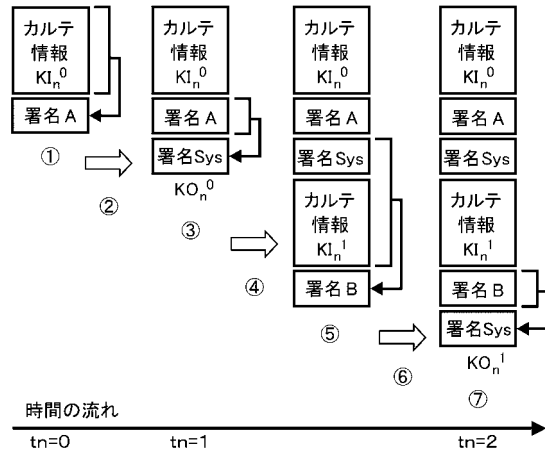
- 10 ネットワーク
- 20 サーバ
- 22 カルテ
- 42, 44, 46 端末
- 110 ネットワーク
- 120 サーバ
- 122 データ
- 130, 142, 144, 146, 148 端末

40

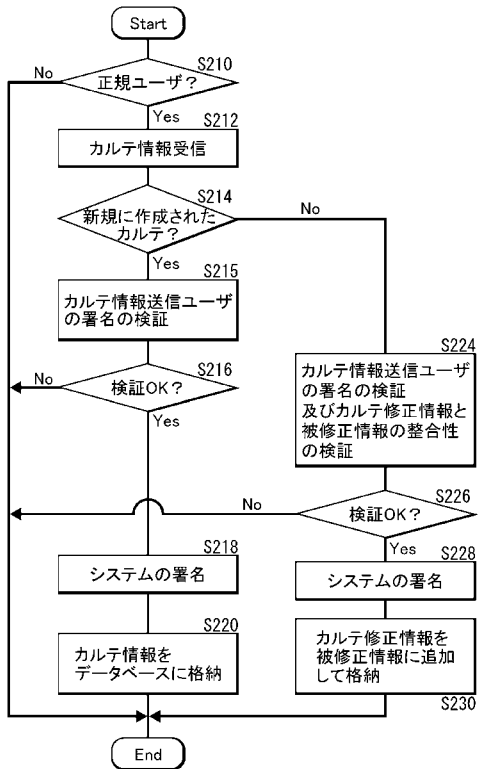
【図1】



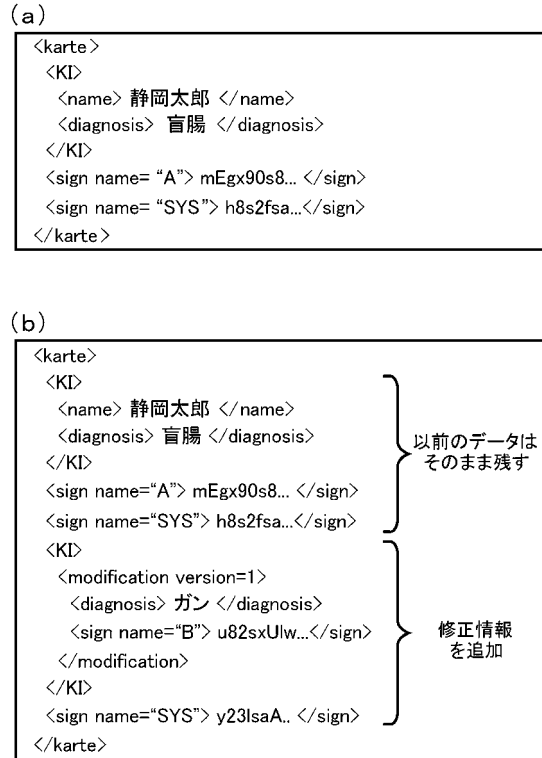
【図2】



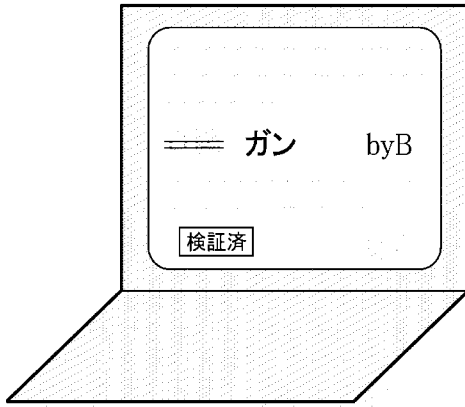
【図3】



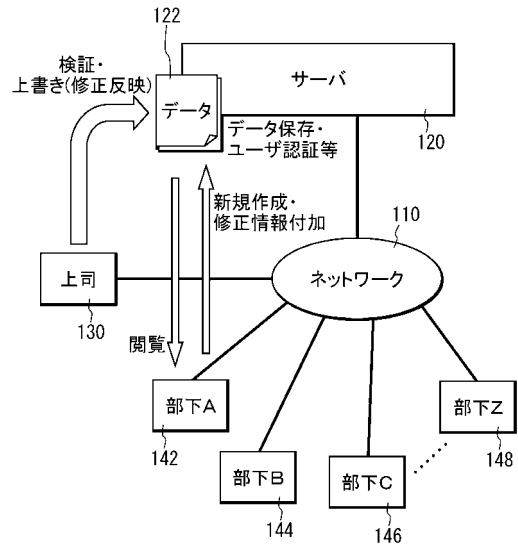
【図4】



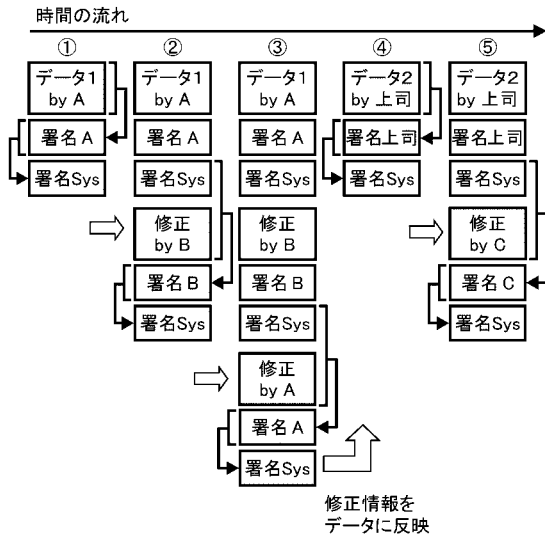
【図5】



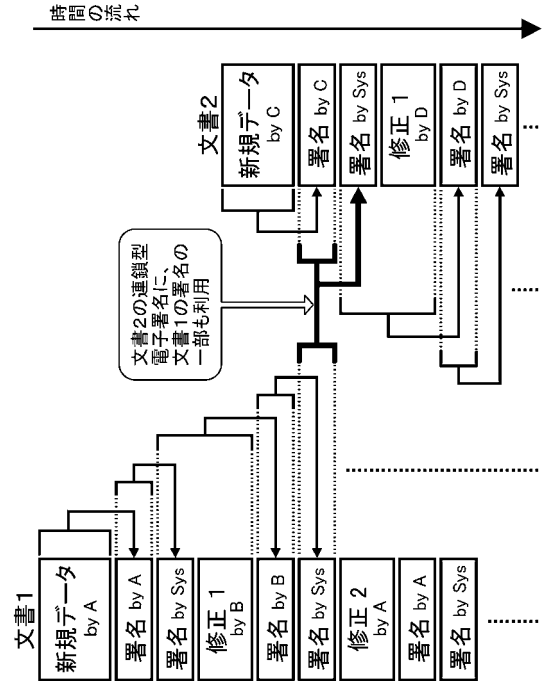
【図6】



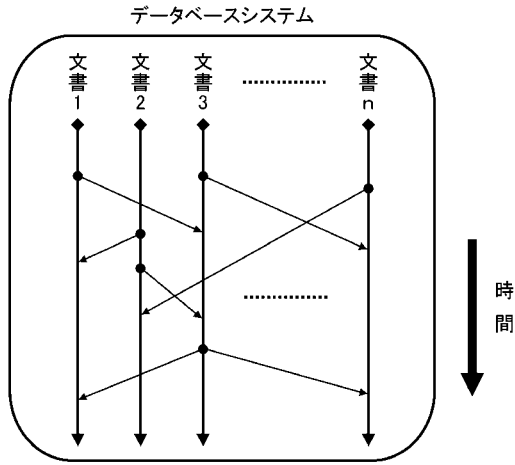
【図7】



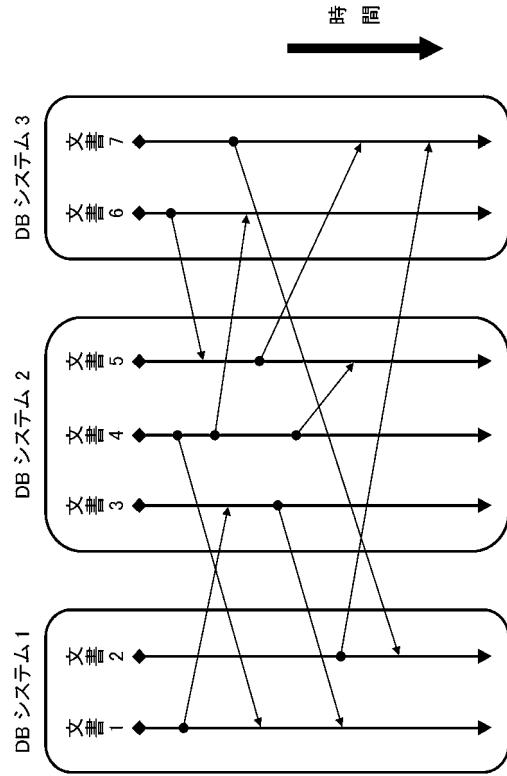
【図8】



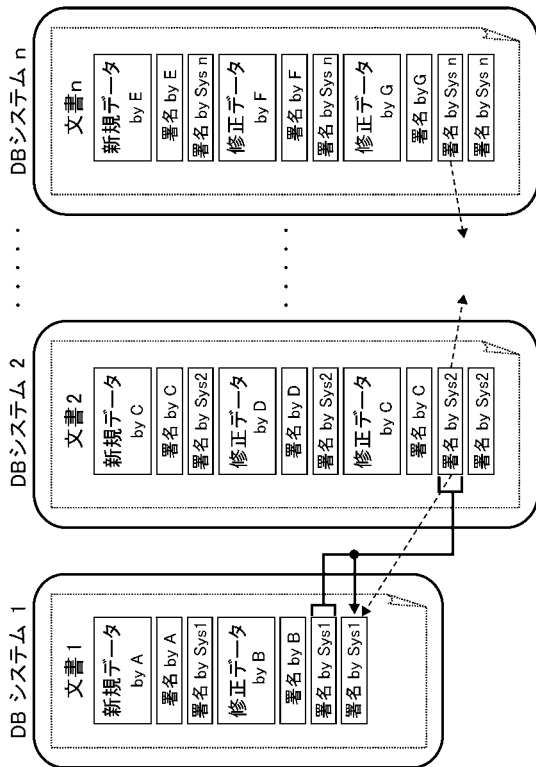
【 図 9 】



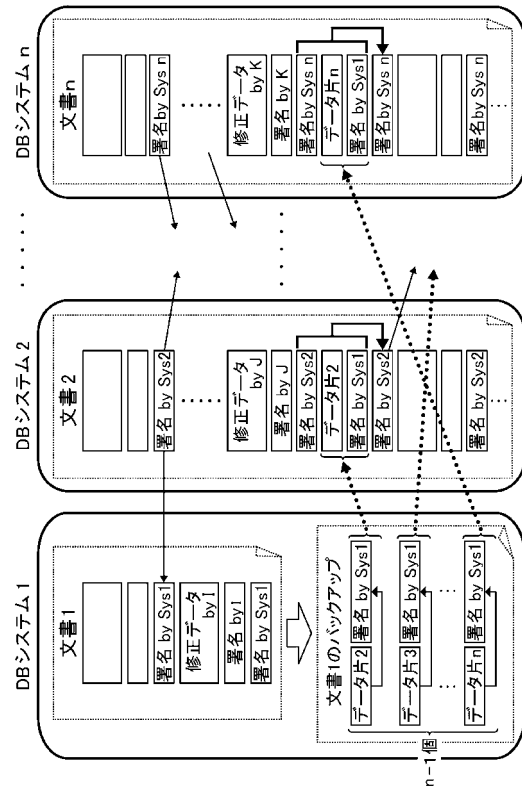
【 図 10 】



【 図 11 】



【 図 12 】



フロントページの続き

(51)Int.Cl. F I
G 0 9 C 1/00 (2006.01) G 0 6 F 17/60 1 2 6 K
 G 0 6 F 17/60 5 1 2
 G 0 9 C 1/00 6 4 0 D

(72)発明者 田窪 昭夫
 神奈川県横浜市栄区桂台南2 - 3 7 - 6

審査官 石川 正二

(56)参考文献 特開平10 - 2 8 3 2 6 3 (J P , A)
 特開平06 - 2 2 4 8 9 6 (J P , A)
 特開平06 - 3 1 5 0 3 6 (J P , A)
 特開平10 - 2 8 3 2 6 4 (J P , A)
 特開平10 - 2 8 9 5 2 3 (J P , A)
 特開平10 - 0 8 3 2 9 7 (J P , 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. , D B 名)

G06F 12/00
 G06F 17/30
 G06F 21/24
 G06Q 10/00
 G06Q 50/00
 G09C 1/00