(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4912809号
(P4912809)
(45)発行日　平成24年4月11日(2012.4.11)　(24)登録日　平成24年1月27日(2012.1.27)

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

請求項の数 4　(全 15 頁)

(21)出願番号　特願2006-259301 (P2006-259301)
(22)出願日　平成18年9月25日 (2006.9.25)
(65)公開番号　特開2008-79254 (P2008-79254A)
(43)公開日　平成20年4月3日 (2008.4.3)
審査請求日　平成21年2月13日 (2009.2.13)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100092657
弁理士　寺崎　史朗
(74)代理人　100114270
弁理士　黒川　朋也
(74)代理人　100124800
弁理士　諏澤　勇司
(74)代理人　100121980
弁理士　沖山　隆

最終頁に続く

(54)【発明の名称】電子署名サーバ、電子署名システム及び電子署名方法

(57)【特許請求の範囲】
【請求項１】
予め記憶されたコンテンツデータに対して、端末装置のユーザによる電子署名を付与するための電子署名サーバであって、
前記コンテンツデータに対応する乱数データを生成する乱数データ生成手段と、
前記乱数データを前記ユーザの公開鍵で暗号化して、第１暗号データを生成する暗号化手段と、
前記第１暗号データを前記端末装置に送信する送信手段と、
前記端末装置によって前記乱数データが前記ユーザの秘密鍵で暗号化されることによって生成された第２暗号データを受信する受信手段と、
前記第２暗号データを前記公開鍵で復号化する復号化手段と、
前記復号化手段で復号化されたデータが前記乱数データ生成手段で生成された乱数データと一致する場合、前記第２暗号データを前記コンテンツデータと対応付けることで、前記ユーザの電子署名を前記コンテンツデータに付与する署名付与手段と、
前記コンテンツデータ及び前記第２暗号データを対応付けて記憶する記憶手段と、
を備える電子署名サーバ。
【請求項２】
前記送信手段は、前記コンテンツデータの内容を前記ユーザが確認するためのデータを前記端末装置に送信することを特徴とする請求項１に記載の電子署名サーバ。
【請求項３】

端末装置と、予め記憶されたコンテンツデータに対して、前記端末装置のユーザによる電子署名を付与するための電子署名サーバと、を備える電子署名システムであって、
前記電子署名サーバは、
前記コンテンツデータに対応する乱数データを生成する乱数データ生成手段と、
前記乱数データを前記ユーザの公開鍵で暗号化して、第１暗号データを生成する暗号化手段と、
前記第１暗号データを前記端末装置に送信する送信手段と、
前記端末装置によって前記乱数データが前記ユーザの秘密鍵で暗号化されることによって生成された第２暗号データを受信する受信手段と、
前記第２暗号データを前記公開鍵で復号化する復号化手段と、
前記復号化手段で復号化されたデータが前記乱数データ生成手段で生成された乱数データと一致する場合、前記第２暗号データを前記コンテンツデータと対応付けることで、前記ユーザの電子署名を前記コンテンツデータに付与する署名付与手段と、
前記コンテンツデータ及び前記第２暗号データを対応付けて記憶する記憶手段と、を備え、
前記端末装置は、
前記コンテンツデータに対して電子署名の付与を要求する署名要求を前記電子署名サーバへ送信するユーザ要求送信手段と、
前記第１暗号データを前記電子署名サーバから受信する暗号情報受信手段と、
前記第２暗号データを前記電子署名サーバへ送信する暗号情報送信手段と、
前記第１暗号データを前記秘密鍵で復号化する復号化手段と、
前記第１暗号データを復号化したデータを前記秘密鍵で暗号化して前記第２暗号データを生成する暗号化手段と、を備える電子署名システム。
【請求項４】
電子署名サーバに予め記憶されたコンテンツデータに対して、端末装置のユーザによる電子署名を付与するための電子署名方法であって、
前記電子署名サーバで、前記コンテンツデータに対応する乱数データを生成する乱数データ生成ステップと、
前記電子署名サーバで前記ユーザの公開鍵を用いて前記乱数データを暗号化することによって、第１暗号データを生成する第１暗号化ステップと、
前記第１暗号データを前記電子署名サーバから前記端末装置に送信する第１送信ステップと、
前記端末装置で前記ユーザの秘密鍵を用いて前記第１暗号データを復号化する第１復号化ステップと、
前記第１復号化ステップで得られたデータを、前記端末装置で前記秘密鍵を用いて暗号化することによって、第２暗号データを生成する第２暗号化ステップと、
前記第２暗号データを前記端末装置から前記電子署名サーバに送信する第２送信ステップと、
前記電子署名サーバで前記公開鍵を用いて前記第２暗号データを復号化する第２復号化ステップと、
前記第２復号化ステップで得られたデータが前記乱数データ生成ステップで生成された乱数データと一致する場合、前記第２暗号データを前記コンテンツデータと対応付けることで、前記ユーザの電子署名を前記コンテンツデータに付与する署名付与ステップと、
を備える電子署名方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子署名サーバ、電子署名システム及び電子署名方法に関し、特に、端末装置からの署名要求に応じて、コンテンツデータに電子署名を付与するための電子署名サーバ、電子署名システム及び電子署名方法に関する。

【背景技術】
【０００２】
サーバに記憶されているコンテンツに対して内容の証明等を行う必要性から、紙文書における捺印やサインに相当する電子署名をコンテンツデータに付与することが行われている。このような電子署名システムとしては、署名付与の対象であるコンテンツデータ（例えば、契約書データ）を署名者の端末装置（例えば、パソコン）に取得させた上で、当該端末装置において電子署名をコンテンツデータに付与するシステムがある（特許文献１参照）。
【０００３】
また、捺印やサインの代用としての個人認証技術では、サーバ等へのアクセス許可を判断するために、公開鍵と秘密鍵を用いる公開鍵暗号方式を利用した電子印鑑が知られている（特許文献２参照）。
【特許文献１】特開２００４－０８０３３５号公報
【特許文献２】特開２００４－１２６８８９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
特許文献１に記載のシステムでは、電子署名の付与に際して、ユーザが、署名付与の対象である実体（すなわち、コンテンツデータ）をサーバから端末装置へ移動又はコピーさせる必要がある。そのため、データサイズが大きいコンテンツデータに電子署名を付与したい場合、メモリ容量に制限のある端末装置（例えば、携帯電話）では、電子署名を付与できるコンテンツが制限されていた。また、第三者による改竄等の不正に対して、データの安全を保つためには専用のパソコンやＩＣカードが必要となるため、システム導入の阻害となっていた。
【０００５】
一方、特許文献２に記載の電子印鑑は、署名付与の対象である実体の移動又はコピーは伴わないものの、サーバへのアクセス許可に必要な鍵としての機能を備えるに過ぎないため、アクセスを許可された後にサーバに記憶されているコンテンツデータに電子署名を付与することはできなかった。
【０００６】
そこで、本発明は、署名を付与するユーザがメモリ容量に制限のある端末装置を使用する場合であっても、データサイズの大きいコンテンツデータに対して電子署名を付与することができる電子署名サーバ、電子署名システム及び電子署名方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の電子署名サーバは、予め記憶されたコンテンツデータに対して、端末装置のユーザによる電子署名を付与するための電子署名サーバであって、コンテンツデータに対応する乱数データを生成する乱数データ生成手段と、乱数データをユーザの公開鍵で暗号化して、第１暗号データを生成する暗号化手段と、第１暗号データを端末装置に送信する送信手段と、端末装置によって乱数データがユーザの秘密鍵で暗号化されることによって生成された第２暗号データを受信する受信手段と、第２暗号データを公開鍵で復号化する復号化手段と、復号化手段で復号化されたデータが乱数データ生成手段で生成された乱数データと一致する場合、第２暗号データをコンテンツデータと対応付けることで、ユーザの電子署名をコンテンツデータに付与する署名付与手段と、コンテンツデータ及び前記第２暗号データを対応付けて記憶する記憶手段と、を備える。
【０００８】
本発明によれば、コンテンツデータへ電子署名を付与するためにコンテンツデータを電子署名サーバから端末装置へ移動又はコピーする必要がないため、署名を付与するユーザがメモリ容量に制限のある端末装置を使用する場合であっても、データサイズの大きいコ

ンテンツデータに対して電子署名を付与することができる。

【０００９】

また、上記電子署名サーバにおいて、送信手段は、コンテンツデータの内容をユーザが確認するためのデータを端末装置に送信するように構成してもよい。このように構成することで、コンテンツデータ全体をサーバから端末装置に送信することなく、端末装置のユーザは、電子署名を付与するコンテンツデータの内容を事前に確認することができる。

【００１０】

本発明は、上記のように電子署名サーバに係る発明として記載できる他に、以下のように電子署名システム及び電子署名方法に係る発明として記述することができる。

【００１１】

本発明の電子署名システムは、端末装置と、予め記憶されたコンテンツデータに対して、端末装置のユーザによる電子署名を付与するための電子署名サーバと、を備える電子署名システムであって、電子署名サーバは、コンテンツデータに対応する乱数データを生成する乱数データ生成手段と、乱数データをユーザの公開鍵で暗号化して、第１暗号データを生成する暗号化手段と、第１暗号データを端末装置に送信する送信手段と、端末装置によって乱数データがユーザの秘密鍵で暗号化されることによって生成された第２暗号データを受信する受信手段と、第２暗号データを公開鍵で復号化する復号化手段と、復号化手段で復号化されたデータが乱数データ生成手段で生成された乱数データと一致する場合、第２暗号データをコンテンツデータと対応付けることで、ユーザの電子署名をコンテンツデータに付与する署名付与手段と、コンテンツデータ及び第２暗号データを対応付けて記憶する記憶手段と、を備え、端末装置は、コンテンツデータに対して電子署名の付与を要求する署名要求を電子署名サーバへ送信するユーザ要求送信手段と、第１暗号データを電子署名サーバから受信する暗号情報受信手段と、第２暗号データを電子署名サーバへ送信する暗号情報送信手段と、第１暗号データを秘密鍵で復号化する復号化手段と、第１暗号データを秘密鍵で復号化したデータを秘密鍵で暗号化して第２暗号データを生成する暗号化手段と、を備える。

【００１２】

また、本発明の電子署名方法は、電子署名サーバに予め記憶されたコンテンツデータに対して、端末装置のユーザによる電子署名を付与するための電子署名方法であって、電子署名サーバで、コンテンツデータに対応する乱数データを生成する乱数データ生成ステップと、電子署名サーバでユーザの公開鍵を用いて乱数データを暗号化することによって、第１暗号データを生成する第１暗号化ステップと、第１暗号データを電子署名サーバから端末装置に送信する第１送信ステップと、端末装置でユーザの秘密鍵を用いて第１暗号データを復号化する第１復号化ステップと、第１復号化ステップで得られたデータを、端末装置で秘密鍵を用いて暗号化することによって、第２暗号データを生成する第２暗号化ステップと、第２暗号データを端末装置から電子署名サーバに送信する第２送信ステップと、電子署名サーバで公開鍵を用いて第２暗号データを復号化する第２復号化ステップと、第２復号化ステップで得られたデータが乱数データ生成ステップで生成された乱数データと一致する場合、第２暗号データをコンテンツデータと対応付けることで、ユーザの電子署名をコンテンツデータに付与する署名付与ステップと、を備える。

【００１３】

なお、上記の電子署名システム及び電子署名方法に係る発明は、上記の電子署名サーバに係る発明と対応する技術的特徴を有し、同様の作用及び効果を奏する発明である。

【発明の効果】

【００１４】

本発明によれば、電子署名を付与するためにコンテンツデータを電子署名サーバから端末装置へ移動又はコピーする必要がないため、署名を付与するユーザがメモリ容量に制限のある端末装置を使用する場合であっても、データサイズの大きいコンテンツデータに対して電子署名を付与することができる。

【発明を実施するための最良の形態】

【００１５】
以下、図面を参照しながら、本発明に係る電子署名サーバ、電子署名システム及び電子署名方法の一実施形態を説明する。
【００１６】
まず、本発明の実施形態に係る電子署名システムの構成について説明する。本実施形態に係る電子署名システム１は、コンテンツデータに対して、端末装置１０のユーザによる電子署名を付与するためのシステムである。この電子署名システム１では、ユーザの公開鍵と秘密鍵を用いる公開鍵暗号方式によってコンテンツデータに対応する乱数データ（すなわち、コンテンツデータ以外のデータ）を暗号化及び復号化することで、ユーザの端末装置１０からの署名要求に応じて、ユーザによって選択されたコンテンツのコンテンツデータに対して電子署名を付与する。
【００１７】
この電子署名システム１は、端末装置１０と、予め記憶されたコンテンツデータ２３Ｃに対して、端末装置１０のユーザによる電子署名を付与するためのサーバ２０（以下、「電子署名サーバ２０」又は「サーバ２０」という）と、を備えている。図１は、電子署名システム１について機能的な構成を示すブロック図であり、図２は、電子署名システム１についてハードウェアの構成を示す図である。
【００１８】
この電子署名システム１において、端末装置１０は、通信モジュール１０１を用いて、通信ネットワークＮを介して、サーバ２０の通信モジュール２０１との間で通信が可能とされている。通信ネットワークＮとしては、例えば、基地局及び交換機等の機器（いずれも図示せず）から構成される移動体通信網を含む通信ネットワークを用いることができる。
【００１９】
次に、図１及び図２を参照しつつ、電子署名システム１を構成する要素及びその機能を説明する。
【００２０】
まず、端末装置１０を構成する要素及びその機能を説明する。
【００２１】
図２のハードウェア構成図に示されるように、端末装置１０は、物理的には、各種データの送受信デバイスである通信モジュール１０１と、データの処理及びハードウェアの制御等を行うＣＰＵ１０２と、記憶デバイスであるＲＯＭ１０３及びＲＡＭ１０４と、液晶ディスプレイ等から構成される映像出力デバイスである表示装置１０５と、音声出力デバイスであるスピーカー１０６と、テンキー及び十字キー等から構成される入力装置１０７と、秘密鍵情報及び公開鍵情報等のユーザ固有の情報が記憶されたＩＣカード３０が装着されるカードスロット１０８と、を備える。後述する端末装置１０の各機能は、ＲＯＭ１０３、ＲＡＭ１０４等に格納された所定のアプリケーションを用いて、ＣＰＵ１０２の制御のもとで、通信モジュール１０１、表示装置１０５、スピーカー１０６、入力装置１０７及びカードスロット１０８を動作させるとともに、ＲＯＭ１０３及びＲＡＭ１０４からのデータの読出し及び書込みや通信モジュール１０１を介したデータの送受信によって実現される。
【００２２】
このような端末装置１０の例としては、携帯電話及び通信機能を備えるパソコン、ＰＤＡ（Personal Digital Assistance）等がある。また、カードスロット１０８に装着されるＩＣカード３０の例としては、ＵＩＭ（User Identity Module）カードやフラッシュメモリカード等がある。
【００２３】
図１のブロック図に示されるように、端末装置１０は、機能的な構成要素として、通信ユニット１１（ユーザ要求送信手段、暗号情報受信手段、暗号情報送信手段）と、暗復号処理ユニット１２（復号化手段、暗号化手段）と、記憶部１３と、通知部１４と、入力部

１５と、を備える。
【００２４】
通信ユニット１１は、サーバ２０との間でデータの送受信を行う部分であり、ハードウェア上では通信モジュール１０１を主な要素として構成される。この通信ユニット１１は、ユーザ情報送受信部１１Ａ（ユーザ要求送信手段）とコンテンツ情報送受信部１１Ｂと、暗号情報送受信部１１Ｃ（暗号情報受信手段、暗号情報送信手段）と、を備えている。
【００２５】
ユーザ情報送受信部１１Ａは、ユーザによる入力部１５の操作等に応じて、ユーザ情報送受信部１１Ａは、サーバ２０の記憶部２３に記憶されているコンテンツデータ２３Ｃにユーザの署名を付与することを要求する署名要求をサーバ２０のユーザ情報送受信部２１Ａに送信する。また、ユーザによる入力部１５の操作やサーバ２０からの要求等に応じて、記憶部１３に記憶されているユーザ公開鍵１３Ａや証明書情報１３Ｂをサーバ２０のユーザ情報送受信部２１Ａに送信する。
【００２６】
コンテンツ情報送受信部１１Ｂは、署名要求の対象であるコンテンツデータ２３Ｃに関するコンテンツ情報２３Ｄ及び電子署名の付与に関する処理結果情報をサーバ２０のコンテンツ情報送受信部２１Ｂから受信する。また、コンテンツ情報送受信部１１Ｂは、ユーザがコンテンツ情報２３Ｄを確認したことをサーバ２０に通知するための確認完了通知をサーバ２０のコンテンツ情報送受信部２１Ｂに送信する。なお、コンテンツ情報２３Ｄの詳細については後述する。
【００２７】
暗号情報送受信部１１Ｃは、サーバ２０との間で暗号化されたデータの送受信を行う。具体的には、サーバ２０の暗号化処理部２２Ｂで生成された暗号データ（後述する第１暗号データ）をサーバ２０から受信すると共に、端末装置１０の暗号化処理部１２Ｂで生成された暗号データ（後述する第２暗号データ）をサーバ２０へ送信する。
【００２８】
暗復号処理ユニット１２は、データの暗号化及び復号化を行う部分であり、ハードウェア上ではＣＰＵ１０２、ＲＯＭ１０３及びＲＡＭ１０４を主な要素として構成される。
【００２９】
復号化処理部１２Ａは、記憶部１３に記憶されているユーザの鍵情報を用いて暗号データを復号化する。具体的には、記憶部１３に記憶されているユーザ秘密鍵１３Ｃで、サーバ２０の暗号化処理部２２Ｂで生成された暗号データ（第１暗号データ）を復号化して、非暗号データを生成する。
【００３０】
暗号化処理部１２Ｂは、記憶部１３に記憶されているユーザの鍵情報を用いてデータを暗号化する。具体的には、記憶部１３に記憶されているユーザ秘密鍵１３Ｃを用いて復号化処理部１２Ａで第１暗号データを復号化したデータ（すなわち、非暗号データ）を、ユーザ秘密鍵１３Ｃで暗号化して、第２暗号データを生成する。なお、この暗号化処理部１２Ｂで生成される暗号データが、署名対象のコンテンツデータと対となる署名値になる。
【００３１】
記憶部１３は、ユーザの鍵情報等のデータを記憶する部分であり、ハードウェア上では、ＲＯＭ１０３及びＲＡＭ１０４に加えて、カードスロット１０８に装着されたＩＣカードを主な要素として構成される。記憶部１３が記憶するデータとしては、公開鍵暗号方式におけるユーザ公開鍵１３Ａ、ユーザ公開鍵１３Ａの証明書情報１３Ｂ、ユーザ秘密鍵１３Ｃに加えて、後述するコンテンツ情報１３Ｄがある。ここで、証明書情報とは、電子署名サーバ２０に対して、ユーザの端末装置１０が特定のサービスを利用することが許された端末装置であることを示す情報である。このような証明書情報としては、例えば、コンテンツプロバイダのサイトへログインするためのＳＳＬクライアント認証に用いられるクライアント証明書がある。
【００３２】

通知部１４は、サーバ２０から送信されたデータ、端末装置１０の動作状態等をユーザに通知する部分であり、ハードウェア上では表示装置１０５及びスピーカー１０６を主な要素として構成される。この通知部１４からの音声や画像を確認することで、ユーザはサーバ２０から受信したデータ（例えば、後述するコンテンツ情報等）の内容を確認することができる。

【００３３】

入力部１５は、端末装置１０を操作する部分であり、ハードウェア上では入力装置１０７を主な要素として構成される。端末装置１０のユーザは、この入力部１５を操作することで、サーバ２０への署名要求の送信等を含む端末装置１０の操作を行なう。

【００３４】

上述のような構成とすることで、端末装置１０は、サーバ２０との間で、署名要求、暗号データ、コンテンツ情報等の各種データの送受信を行うと共に、暗号データの復号化及び非暗号データの暗号化をすることができる。

【００３５】

次に、電子署名サーバ２０を構成する要素及びその機能を説明する。このサーバ２０は、予め記憶されたコンテンツデータに対して、端末装置１０のユーザによる電子署名を付与するための電子署名サーバである。

【００３６】

図２のハードウェア構成図に示されるように、サーバ２０は、物理的には、各種データの送受信デバイスである通信モジュール２０１と、データの処理及びハードウェアの制御等を行うＣＰＵ２０２と、記憶デバイスであるＲＯＭ２０３及びＲＡＭ２０４と、入力装置２０５と、出力装置２０６とを備える。後述するサーバ２０の各機能は、ＲＯＭ２０３、ＲＡＭ２０４等に格納された所定のアプリケーションを用いて、ＣＰＵ２０２の制御のもとで、通信モジュール２０１、入力装置２０５及び出力装置２０６を動作させるとともに、ＲＯＭ２０３及びＲＡＭ２０４からのデータの読出し及び書込みや、通信モジュール２０１を介したデータの送受信によって実現される。

【００３７】

図１のブロック図に示されるように、サーバ２０は、機能的な構成要素として、通信ユニット２１（送信手段、受信手段）と、署名処理ユニット２２（乱数データ生成手段、暗号化手段、復号化手段、署名付与手段）と、記憶部２３（記憶手段）と、を備える。

【００３８】

通信ユニット２１は、端末装置１０との間でデータの送受信を行う部分であり、ハードウェア上では通信モジュール２０１を主な要素として構成される。この通信ユニット２１は、ユーザ情報送受信部２１Ａと、コンテンツ情報送受信部２１Ｂ（送信手段）と、暗号情報送受信部２１Ｃ（送信手段、受信手段）と、を備えている。

【００３９】

ユーザ情報送受信部２１Ａは、ユーザによって選択されたコンテンツデータ２３Ｃへの署名要求や、ユーザ公開鍵１３Ａ及び証明書情報１３Ｂを端末装置１０のユーザ情報送受信部１１Ａから受信する。また、ユーザ情報送受信部２１Ａは、端末装置１０から受信した署名要求に応じて、ユーザ公開鍵１３Ａ及び証明書情報１３Ｂの送信要求を含むユーザ情報要求を端末装置１０のユーザ情報送受信部１１Ａに送信する。

【００４０】

コンテンツ情報送受信部２１Ｂは、コンテンツデータ２３Ｃへの署名要求に応じて、署名を付与するコンテンツデータ２３Ｃの内容をユーザが確認するためのデータであるコンテンツ情報２３Ｄ及び電子署名の付与に関する処理結果情報を端末装置１０のコンテンツ情報送受信部１１Ｂに送信する。また、このコンテンツ情報送受信部２１Ｂは、ユーザがコンテンツ情報２３Ｄを確認したことをサーバ２０に通知するための確認完了通知を端末装置１０のコンテンツ情報送受信部１１Ｂから受信する。

【００４１】

暗号情報送受信部２１Ｃは、端末装置１０との間で暗号化されたデータの送受信を行う

。具体的には、後述する暗号化処理部２２Ｂで生成された暗号データ（第１暗号データ）を端末装置１０へ送信すると共に、端末装置１０の暗号化処理部１２Ｂで生成された暗号データ（第２暗号データ）を端末装置１０の暗号情報送受信部１１Ｃから受信する。

【００４２】

署名処理ユニット２２は、コンテンツデータに対して、端末装置１０のユーザによる電子署名を付与するための処理を行う部分であり、ハードウェア上ではＣＰＵ２０２、ＲＯＭ２０３及びＲＡＭ２０４を主な要素として構成される。

【００４３】

乱数データ生成部２２Ａは、記憶部２３に記憶されているコンテンツデータ２３Ｃに対応する乱数データを生成する。乱数データ生成部２２Ａによってコンテンツデータ２３Ｃから乱数データを発生させる仕組みには、既存のアルゴリズムを利用することができる。具体的には、ＭＤ５はＳＨＡ１といったハッシュ関数を利用することができる。

【００４４】

暗号化処理部２２Ｂは、記憶部２３に記憶されている鍵情報を用いてデータを暗号化する。具体的には、乱数データ生成部２２Ａによって生成された乱数データをユーザ公開鍵２３Ａで暗号化して、第１暗号データを生成する。なお、この暗号化処理部２２Ｂが用いるユーザ公開鍵２３Ａは、端末装置１０から受信したユーザ公開鍵１３Ａと同一のものである。

【００４５】

復号化処理部２２Ｃは、記憶部２３に記憶されている鍵情報を用いて暗号データを復号化する。具体的には、記憶部２３に記憶されているユーザ公開鍵２３Ａで、端末装置１０の暗号化処理部１２Ｂで生成された暗号データ（第２暗号データ）を復号化して、非暗号データを生成する。

【００４６】

署名付与部２２Ｄは、復号化処理部２２Ｃで復号化されたデータ（非暗号データ）が乱数データ生成部２２Ａで生成された乱数データと一致する場合、端末装置１０の暗号化処理部１２Ｂで生成された暗号データ（第２暗号データ）をコンテンツデータ２３Ｃと対応付けることで、ユーザの電子署名をコンテンツデータ２３Ｃに付与する。換言すれば、署名付与部２２Ｄは、復号化処理部２２Ｃで復号化することで得られた乱数データを、乱数データ生成部２２Ａで生成された乱数データと照合することで、第２暗号データがユーザ本人の電子署名として安全に利用できるものであることを確認する。そして、２つのデータ（すなわち、乱数データ）が一致する場合、署名付与部２２Ｄは、第２暗号データをユーザの署名値としてコンテンツデータ２３Ｃと対応付けるデータを生成する。これにより、サーバ２０は、ユーザの電子署名（署名値）として第２暗号データをコンテンツデータ２３Ｃに付与する。この署名付与部２２Ｄによるコンテンツデータ２３Ｃと第２暗号データとの対応付けに関するデータは、第２暗号データと対にされて署名データ２３Ｆとして記憶部２３に記憶される。

【００４７】

記憶部２３は、コンテンツデータ、乱数データ、ユーザの鍵情報等のデータを記憶する部分であり、ハードウェア上では、ＲＯＭ２０３及びＲＡＭ２０４を主な要素として構成される。記憶部２３が記憶するデータとしては、ユーザ公開鍵２３Ａと、ユーザ証明書２３Ｂと、コンテンツデータ２３Ｃと、コンテンツ情報２３Ｄと、乱数データ２３Ｅと、署名データ２３Ｆとがある。

【００４８】

ユーザ公開鍵２３Ａは、上述のように、端末装置１０から受信したユーザ公開鍵１３Ａと同一のものである。また、ユーザ証明書２３Ｂは、端末装置１０から受信した証明書情報１３Ｂと同一のものである。

【００４９】

コンテンツデータ２３Ｃは、電子署名の対象となるコンテンツである。このコンテンツデータ２３Ｃの内容は特に制限されず、サーバ２０で生成したものであっても、任意の手

段を介して外部から取得したものであってもよい。このようなコンテンツとしては、例えば、捺印や印鑑証明が必要な書類のデータがあり、より具体的には、請負契約書、売買契約書、口座開設申込書等のデータがある。

【００５０】

コンテンツ情報２３Ｄは、コンテンツデータ２３Ｃの内容をユーザが確認するためのデータである。このコンテンツ情報２３Ｄは、端末装置１０からの署名要求に応じてサーバ２０の記憶部２３から読出されるものであり、署名要求の対象であるコンテンツデータ２３Ｃに関する情報（例えば、コンテンツの名称、概要等）を含んでいる。

【００５１】

乱数データ２３Ｅは、乱数データ生成部２２Ａで生成された乱数データと同一であり、上述した署名付与部２２Ｄにおける処理のために記憶部２３に記憶されるものである。

【００５２】

署名データ２３Ｆは、上述のように、第２暗号データと、署名付与部２２Ｄによるコンテンツデータ２３Ｃと第２暗号データとの対応付けに関するデータを含むものである。なお、第２暗号データと対応付けに関するデータとは対にされている。

【００５３】

上述のような構成とすることで、電子署名サーバ２０は、予め記憶されたコンテンツデータ２３Ｃに対して、端末装置１０のユーザによる電子署名を付与することができる。また、コンテンツデータ２３Ｃを使用する時に、署名データ２３Ｆを参照することで、コンテンツデータ２３Ｃを電子署名が付与されたコンテンツデータとして、改竄等の不安なく、安全に取り扱うことができる。

【００５４】

引き続き、図３から図５を参照しつつ、本発明の実施形態に係る電子署名方法を説明する。

【００５５】

図３から図５は、図１及び図２に示された電子署名システム１において、公開鍵と秘密鍵を用いる公開鍵暗号方式によって、電子署名サーバ２０に予め記憶されたコンテンツデータ２３Ｃに対して、端末装置１０のユーザによる電子署名を付与するための処理を示すシーケンス図である。なお、図中において、Ｓは処理のステップを示す。

【００５６】

まず、コンテンツデータに対して電子署名を付与するにあたって、端末装置１０において、ユーザは、入力部１５を介して電子署名を付与したいコンテンツ（すなわち、コンテンツデータ２３Ｃ）を選択する（Ｓ１）。具体的には、電子署名を付与することができるコンテンツが請負契約書、売買契約書、口座開設申込書等といったように複数存在する場合、それらの中から電子署名を付与したいコンテンツ（書類）を選択する。ユーザが電子署名を付与したいコンテンツを選択した後、端末装置１０は、コンテンツデータ２３Ｃに対してユーザの電子署名の付与を要求する署名要求を、ユーザ情報送受信部１１Ａを介して、サーバ２０のユーザ情報送受信部２１Ａに送信する（Ｓ２）。

【００５７】

サーバ２０は、ユーザ情報送受信部１１Ａからの署名要求をユーザ情報送受信部２１Ａで受信した後、署名要求の内容を確認して、ユーザによって選択されたコンテンツのコンテンツデータ２３Ｃが記憶部２３に記憶されていることを確認する（Ｓ３）。サーバ２０は、コンテンツデータ２３Ｃの確認後、サーバ２０は、記憶部１３に記憶されているユーザ公開鍵１３Ａ及び証明書情報１３Ｂの送信要求を含むユーザ情報要求を、ユーザ情報送受信部２１Ａを介して、端末装置１０のユーザ情報送受信部１１Ａに送信する（Ｓ４）。

【００５８】

端末装置１０は、サーバ２０からのユーザ情報要求をユーザ情報送受信部１１Ａで受信した後、記憶部１３に記憶されているユーザ公開鍵１３Ａ及び証明書情報１３Ｂを読出し（Ｓ５）、ユーザ情報送受信部１１Ａを介してサーバ２０のユーザ情報送受信部２１Ａに送信する（Ｓ６）。

【００５９】
サーバ２０は、ユーザ公開鍵１３Ａ及び証明書情報１３Ｂをユーザ情報送受信部２１Ａで受信した後、記憶部２３にユーザ公開鍵２３Ａ及びユーザ証明書２３Ｂとして記憶する（Ｓ７）。なお、本実施形態では、ユーザ公開鍵１３Ａに証明書情報１３Ｂを添付した場合のみを説明するが、証明書情報１３Ｂは、端末装置１０からサーバ２０へのアクセスに際して、端末装置１０のユーザが正当なユーザであることを確認するためデータであるため、ユーザ認証が不要な場合や他の手段でユーザ認証を行う場合には、証明書情報１３Ｂの送信は必須ではない。
【００６０】
サーバ２０は、ユーザ公開鍵１３Ａ及び証明書情報１３Ｂを受信した後、先に受信した署名要求で選択されたコンテンツに対応するコンテンツ情報２３Ｄを記憶部２３から読出し（Ｓ８）、コンテンツ情報送受信部２１Ｂを介して、端末装置１０のコンテンツ情報送受信部１１Ｂに送信する（Ｓ９）。
【００６１】
端末装置１０は、コンテンツ情報送受信部１１Ｂでコンテンツ情報２３Ｄを受信した後、受信したコンテンツ情報２３Ｄをコンテンツ情報１３Ｄとして記憶部１３に記憶するとともに、通知部１４を介してユーザに通知することで、コンテンツ情報の確認を求める（Ｓ１０）。通知されたコンテンツ情報が自ら選択したコンテンツに対応する内容であることをユーザが確認した後、入力部１５を介して端末装置１０を操作することで、コンテンツ情報送受信部１１Ｂを介して、コンテンツ情報２３Ｄを確認したことをサーバ２０に通知するための確認完了通知をサーバ２０のコンテンツ情報送受信部２１Ｂに送信する（Ｓ１１）。
【００６２】
サーバ２０は、コンテンツ情報送受信部１１Ｂからの確認完了通知をコンテンツ情報送受信部２１Ｂで受信した後、乱数データ生成部２２Ａで、ユーザが選択したコンテンツのコンテンツデータ２３Ｃに対応する乱数データを生成する（Ｓ１２：乱数データ生成ステップ）。乱数データを生成した後、サーバ２０は、乱数データを記憶部２３に乱数データ２３Ｅとして記憶する（Ｓ１３）。また、サーバ２０は、記憶部２３に記憶されているユーザ公開鍵２３Ａを用いて乱数データ２３Ｅを暗号化することによって、第１暗号データを生成する（Ｓ１４：第１暗号化ステップ）。その後、サーバ２０は、暗号情報送受信部２１Ｃを介して、第１暗号データを端末装置１０の暗号情報送受信部１１Ｃに送信する（Ｓ１５：第１送信ステップ）。
【００６３】
端末装置１０は、第１暗号データを暗号情報送受信部１１Ｃで受信した後、復号化処理部１２Ａでユーザ秘密鍵１３Ｃを用いて第１暗号データを復号化して、非暗号データを生成する（Ｓ１６：第１復号化ステップ）。なお、この非暗号データは、乱数データ２３Ｅと同一のデータとなる。また、第１暗号データは、ユーザ公開鍵２３Ａで暗号化されたデータであるため、公開鍵暗号方式の特徴上、記憶部１３に記憶されているユーザ秘密鍵１３Ｃ以外では復号化することができない。
【００６４】
端末装置１０は、復号化処理部１２Ａで非暗号データを生成した後、その非暗号データ（第１暗号データを復号化したデータ）を、暗号化処理部１２Ｂでユーザ秘密鍵１３Ｃを用いて暗号化することによって、第２暗号データを生成する（Ｓ１７：第２暗号化ステップ）。端末装置１０は第２暗号データを生成した後、暗号情報送受信部１１Ｃを介して、第２暗号データをサーバ２０の暗号情報送受信部２１Ｃに送信する（Ｓ１８：第２送信ステップ）。
【００６５】
サーバ２０は、暗号情報送受信部２１Ｃで第２暗号データを受信した後、復号化処理部２２Ｃでユーザ公開鍵２３Ａを用いて第２暗号データを復号化して、非暗号データを生成する（Ｓ１９：第２復号化ステップ）。復号化処理部２２Ｃで非暗号データを生成した後

、サーバ２０は、署名付与部２２Ｄで、第２暗号データを復号化することで得られたデータ（非暗号データ）が、記憶部２３に記憶されている乱数データ２３Ｅ（すなわち、乱数データ生成部２２Ａで生成された乱数データ）と一致するか否かを判断する（Ｓ２０）。

【００６６】

第２暗号データを復号化することで得られた非暗号データが乱数データ２３Ｅと一致する場合、第２暗号データをコンテンツデータ２３Ｃと対応付けることで、ユーザの電子署名をコンテンツデータに付与する（Ｓ２１：署名付与ステップ）。この対応付けは、具体的には、署名付与部２２Ｄが第２暗号データをユーザの署名値としてコンテンツデータ２３Ｃと対応付けるデータを生成することによって行われる。このような処理により、サーバ２０は、ユーザの電子署名をコンテンツデータに付与した後、コンテンツデータ２３Ｃと第２暗号データとの対応付けに関するデータを、第２暗号データと対にした上で、署名データ２３Ｆとして記憶部２３に記憶する（Ｓ２２）。

【００６７】

一方、第２暗号データを復号化することで得られた非暗号データが乱数データ２３Ｅと一致しない場合、署名の付与及び署名データの記憶に関する処理を行うことなく、処理を続行する。

【００６８】

サーバ２０は、上述した非暗号データと乱数データ２３Ｅとの一致を判断した後、署名の付与及び署名データの記憶に関する処理を行ったか否かに関する情報として処理結果情報を生成し（Ｓ２３）、コンテンツ情報送受信部２１Ｂを介して、端末装置１０のコンテンツ情報送受信部１１Ｂに送信する（Ｓ２４）。

【００６９】

端末装置１０は、コンテンツ情報送受信部１１Ｂで処理結果情報を受信した後、通知部１４を介して、処理結果をユーザに通知する（Ｓ２５）。

【００７０】

上述のような処理により、電子署名サーバ２０に予め記憶されたコンテンツデータ２３Ｃに対して、端末装置１０のユーザによる電子署名を付与することができる。

【００７１】

以上説明した本実施形態に係る電子署名サーバ２０の作用及び効果について説明する。

【００７２】

本実施形態に係る電子署名サーバ２０は、コンテンツデータ２３Ｃへ電子署名を付与するためにコンテンツデータ２３Ｃをサーバ２０から端末装置１０へ移動又はコピーする必要がないため、署名を付与するユーザがメモリ容量に制限のある端末装置を使用する場合であっても、データサイズの大きいコンテンツデータに対して電子署名を付与することができる。

【００７３】

また、電子署名サーバ２０において、コンテンツ情報送受信部２１Ｂは、コンテンツデータ２３Ｃの内容をユーザが確認するためのデータ（コンテンツ情報２３Ｄ）を端末装置１０に送信するように構成されている。このように構成することで、コンテンツデータ全体をサーバ２０から端末装置１０に送信することなく、端末装置１０のユーザは、電子署名を付与するコンテンツデータ２３Ｃの内容を事前に確認することができる。

【００７４】

上記の電子署名システム１及び電子署名方法も、上記の電子署名サーバ２０に対応する技術的特徴を有し、同様の作用及び効果を奏する。

【００７５】

また、本実施形態に係る電子署名システム１及び電子署名方法では、端末装置１０に装着されるＩＣカード３０等に記憶されている公開鍵及び秘密鍵を用いるため、他に専用のパソコンやＩＣカードを導入することなく、第三者による改竄等の不正に対してデータを安全に管理することができるシステムを容易に導入することができる。

【００７６】

さらに、本実施形態に係る電子署名システム１及び電子署名方法では、携帯電話等の端末装置１０及びサーバ２０にて安全に管理できる鍵情報を利用するため、ユーザの確認性・信憑性を高めた電子署名を安全に利用することが可能となり、コンテンツの改竄防止、否認防止をすることができる。

【００７７】

また、本実施形態に係る電子署名システム１及び電子署名方法では、ユーザは端末装置１０を所持していれば、電子署名を付与したいコンテンツに対して、プラットフォームに依存することなく電子署名を利用することができる。

【００７８】

なお、本発明は、上述した実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変更が可能であることは勿論である。

【００７９】

例えば、上述の実施形態では、コンテンツデータに対応する乱数データとして、既存のアルゴリズムに基づいてコンテンツデータから発生させた乱数データを用いているが、任意の乱数発生器を用いてコンテンツデータとは無関係に乱数データを発生させた後に、その乱数データをコンテンツデータと対応付けることによって、コンテンツデータに対応する乱数データを生成してもよい。

【００８０】

また、上述の実施形態では、コンテンツデータの代わりとしてコンテンツの名称、概要等のデータを含むコンテンツ情報を用いているが、コンテンツ情報をサーバ２０から端末装置１０に送信して、ユーザに通知することは必須ではない。また、端末装置１０において記憶部の容量等のハードウェア条件が許す場合には、コンテンツ情報ではなくコンテンツデータそのものを電子署名サーバ２０から端末装置１０に送信して、ユーザが確認するように構成してもよい。

【００８１】

また、電子署名サーバに記憶されるコンテンツ情報は、電子署名サーバがコンテンツデータから作成するようにしてもよいし、コンテンツデータとあわせて外部から入力されたデータを用いるようにしてもよい。

【図面の簡単な説明】

【００８２】

【図１】本発明の一実施形態に係る電子署名サーバを備える電子署名システムについて機能的な構成を示すブロック図である。

【図２】本発明の一実施形態に係る電子署名サーバを備える電子署名システムについてハードウェアの構成を示す図である。

【図３】本発明の一実施形態に係る電子署名方法において、コンテンツ選択から公開鍵情報及び証明書情報の記憶までを示すシーケンス図である。

【図４】本発明の一実施形態に係る電子署名方法において、コンテンツ情報の読出しから第１暗号データの復号化までを示すシーケンス図である。

【図５】本発明の一実施形態に係る電子署名方法において、第２暗号データの生成から処理結果情報の表示までを示すシーケンス図である。

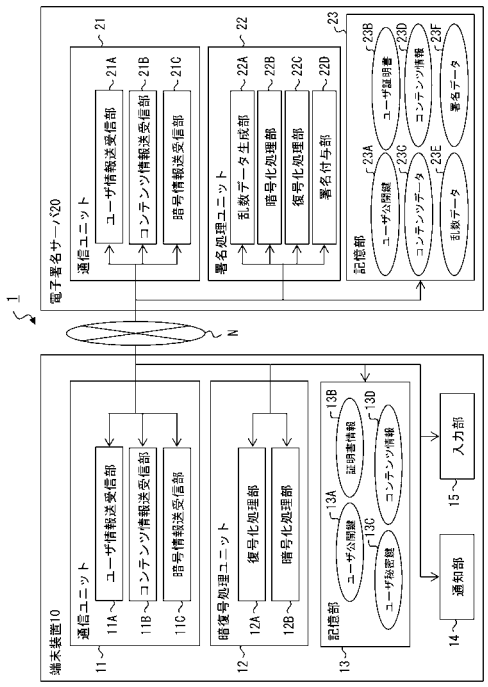
【符号の説明】

【００８３】

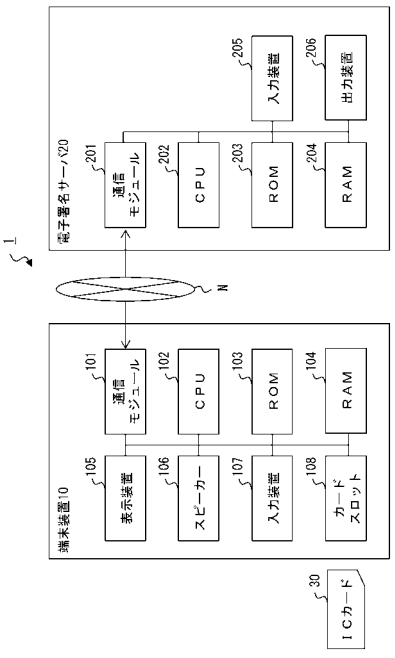
１…電子署名システム、１０…端末装置、１１…通信ユニット、１１Ａ…ユーザ情報送受信部、１１Ｂ…コンテンツ情報送受信部、１１Ｃ…暗号情報送受信部、１２…暗復号処理ユニット、１２Ａ…復号化処理部、１２Ｂ…暗号化処理部、１３…記憶部、１３Ａ…ユーザ公開鍵、１３Ｂ…証明書情報、１３Ｃ…ユーザ秘密鍵、１３Ｄ…コンテンツ情報、１４…通知部、１５…入力部、２０…電子署名サーバ（サーバ）、２１…通信ユニット、２１Ａ…ユーザ情報送受信部、２１Ｂ…コンテンツ情報送受信部、２１Ｃ…暗号情報送受信部、２２…署名処理ユニット、２２Ａ…乱数データ生成部、２２Ｂ…暗号化処理部、２２Ｃ…復号化処理部、２２Ｄ…署名付与部、２３…記憶部、２３Ａ…ユーザ公開鍵、２３Ｂ

…ユーザ証明書、２３Ｃ…コンテンツデータ、２３Ｄ…コンテンツ情報、２３Ｅ…乱数データ、２３Ｆ…署名データ、Ｎ…通信ネットワーク。

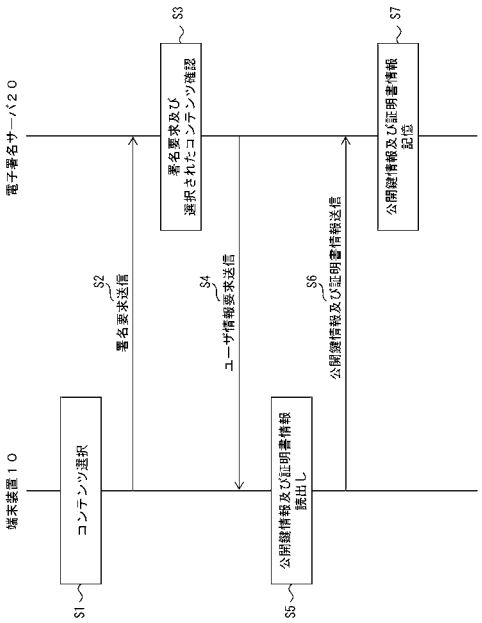
【図１】



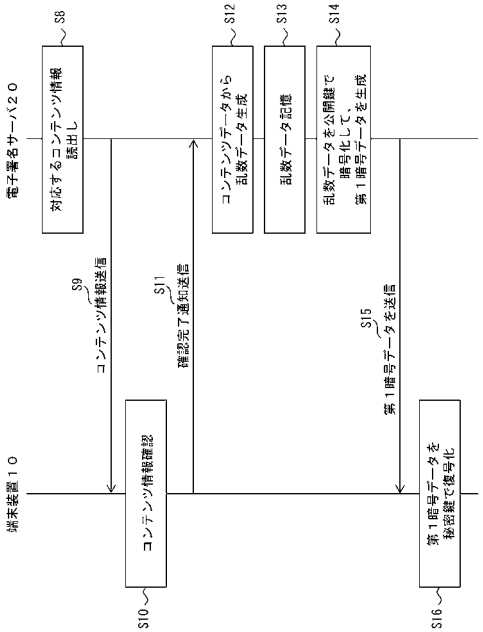
【図２】



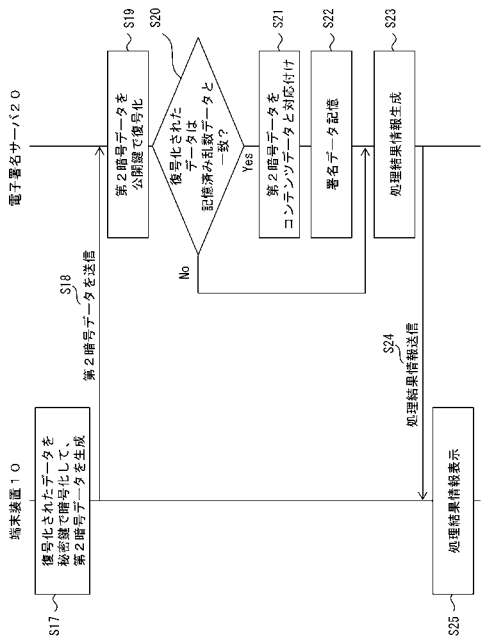
【図３】


電子署名サーバ２０
端末装置１０
コンテンツ選択
署名要求及び
選択されたコンテンツ確認
公開鍵情報及び証明書情報
読出し
公開鍵情報及び証明書情報
記憶
S1
S2
署名要求送信
S3
S4
ユーザ情報要求送信
S5
S6
公開鍵情報及び証明書情報送信
S7

【図４】


電子署名サーバ２０
端末装置１０
対応するコンテンツ情報
読出し
コンテンツ情報確認
コンテンツデータから
乱数データ生成
乱数データ記憶
乱数データを公開鍵で
暗号化して、
第１暗号データを生成
第１暗号データを
秘密鍵で復号化
S8
S9
コンテンツ情報送信
S10
S11
確認完了通知送信
S12
S13
S14
S15
第１暗号データを送信
S16

【図５】


電子署名サーバ２０
端末装置１０
復号化されたデータを
秘密鍵で暗号化して、
第２暗号データを生成
第２暗号データを
公開鍵で復号化
復号化された
データは
記憶済み乱数データと
一致？
Yes
No
第２暗号データを
コンテンツデータと対応付け
署名データ記憶
処理結果情報生成
処理結果情報表示
S17
S18
第２暗号データを送信
S19
S20
S21
S22
S23
S24
処理結果情報送信
S25

フロントページの続き

(72)発明者　山本　博昭
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

審査官　青木　重徳

(56)参考文献　特開２００４－２３４０６（ＪＰ，Ａ）
特開２００４－５２４７７９（ＪＰ，Ａ）
特開２００３－１６０２０９（ＪＰ，Ａ）
特開２００４－１２６８８９（ＪＰ，Ａ）
特開２００６－２０３１９（ＪＰ，Ａ）
特開２０００－１１１１３（ＪＰ，Ａ）
特表２００１－５１２５８９（ＪＰ，Ａ）
岡本康介，鈴木美幸，“電子企業印を共有できる電子署名サーバー”，ＦＩＴ２００２　情報科学技術フォーラム　一般講演論文集　第４分冊　インターネット　ネットワーク・モバイルコンピューティング　教育・人文科学　情報システム，日本，社団法人電子情報通信学会，社団法人情報処理学会，２００２年　９月１３日，Ｍ－４，ｐ．４１－４２
Malleswar Kalla, johnny S.K. Wong, Armin R. Mikler, Stephen Elbert, “Achieving non-repudiation of Web based transactions”, Journal of Systems and Software, [online], １９９９年１１月　1日, Volume 48, Issue 3, p.165-175, [retrieved on 2012-01-05]. Retrieved from the Internet, ＵＲＬ, <http://www.sciencedirect.com/science/article/pii/S0164121299000552>

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