(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-81482
(P2007-81482A)
(43)公開日　平成19年3月29日(2007.3.29)

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

審査請求 未請求　請求項の数 17　ＯＬ　（全 19 頁）

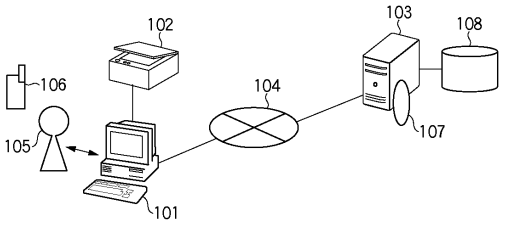
(21)出願番号　特願2005-262989 (P2005-262989)
(22)出願日　平成17年9月9日 (2005.9.9)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　須賀　祐治
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】端末認証方法及びその装置、プログラム

(57)【要約】
【課題】
信頼度が不明なローカル端末でも安全に署名を生成する仕組みを提供するために、ローカル端末を遠隔サーバが信頼できるかどうかをユーザに安全に知らせることを可能とする。
【解決手段】
電子署名の生成依頼をユーザ端末から受け付ける要求受付手段と、前記ユーザ端末を認証する要求端末認証手段と、前記ユーザ端末を介して前記生成依頼を行ったユーザを認証するユーザ認証手段と、前記要求端末認証手段と前記ユーザ認証手段とにおける認証結果に基づき、前記生成依頼に対する回答を前記ユーザ端末に通知する通知手段とを備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子署名の生成依頼をユーザ端末から受け付ける要求受付手段と、
前記ユーザ端末を認証する要求端末認証手段と、
前記ユーザ端末を介して前記生成依頼を行ったユーザを認証するユーザ認証手段と、
前記要求端末認証手段と前記ユーザ認証手段とにおける認証結果に基づき、前記生成依頼に対する回答を前記ユーザ端末に通知する通知手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
前記生成依頼に基づき、データベースに格納された秘密鍵を探索する探索手段と、
署名対象電子文書を前記ユーザ端末から受信する受信手段と、
前記秘密鍵を利用して前記署名対象電子文書の前記電子署名を生成する署名生成手段と、
前記電子署名を前記ユーザ端末に送信する送信手段と
を更に備えることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記データベースは、前記秘密鍵と、該秘密鍵のユーザを識別する複数の識別子とを互いに関連づけて格納し、
前記探索手段は、前記生成依頼に含まれた前記複数の識別子のうちの第１の識別子と関連づけられた秘密鍵を探索し、前記ユーザ認証手段は、前記第１の識別子と関連づけられた秘密鍵が前記データベースに格納されている場合に、前記ユーザを正当なユーザと認証することを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記通知手段は、前記要求端末認証手段により前記ユーザ端末が正当な端末と認証され、かつ、前記ユーザ認証手段により前記ユーザが正当なユーザと認証された場合に、前記回答に前記複数の識別子のうち第２の識別子を含めて前記通知を行うことを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記通知手段は、前記要求端末認証手段により前記ユーザ端末が正当な端末と認証されない場合、或いは、前記ユーザ認証手段により前記ユーザが正当なユーザと認証されない場合に、前記回答には前記複数の識別子のいずれも含めることなく前記通知を行うことを特徴とする請求項３又は４に記載の情報処理装置。
【請求項６】
前記受信手段は、前記秘密鍵を指定するための情報を更に受信し、
前記署名生成手段は、該受信した情報が前記複数の識別子のうち第３の識別子に一致するか否かを判定し、該第３の識別子に一致すると判定された場合に、前記電子署名の生成を行うことを特徴とする請求項２乃至５のいずれかに記載の情報処理装置。
【請求項７】
前記受信手段は、前記電子署名の生成依頼と併せて前記署名対象電子文書を受信し、
前記送信手段は、前記回答の通知と併せて前記電子署名を送信する場合に、前記電子署名を暗号化して送信することを特徴とする請求項２乃至６のいずれかに記載の情報処理装置。
【請求項８】
前記通知手段は、前記回答を、前記生成依頼を受け付けた第１のユーザ端末とは異なる第２のユーザ端末に送信することを特徴とする請求項１乃至７のいずれかに記載の情報処理装置。
【請求項９】
前記第１乃至第３の識別子は同一の識別子であることを特徴とする請求項８に記載の情報処理装置。
【請求項１０】

電子署名の生成依頼をユーザ端末から受け付ける要求受付工程と、
前記ユーザ端末を認証する要求端末認証工程と、
前記ユーザ端末を介して前記生成依頼を行ったユーザを認証するユーザ認証工程と、
前記要求端末認証工程と前記ユーザ認証工程とにおける認証結果に基づき、前記生成依頼に対する回答を前記ユーザ端末に通知する通知工程と、
を備えることを特徴とする情報処理装置の制御方法。
【請求項１１】
前記生成依頼に基づき、データベースに格納された秘密鍵を探索する探索工程と、
署名対象電子文書を前記ユーザ端末から受信する受信工程と、
前記秘密鍵を利用して前記署名対象電子文書の前記電子署名を生成する署名生成工程と、
前記電子署名を前記ユーザ端末に送信する送信工程と
を更に備えることを特徴とする請求項１０に記載の情報処理装置の制御方法。
【請求項１２】
前記データベースは、前記秘密鍵と、該秘密鍵のユーザを識別する複数の識別子とを互いに関連づけて格納し、
前記探索工程では、前記生成依頼に含まれた前記複数の識別子のうちの第１の識別子と関連づけられた秘密鍵を探索し、前記ユーザ認証工程では、前記第１の識別子と関連づけられた秘密鍵が前記データベースに格納されている場合に、前記ユーザを正当なユーザと認証することを特徴とする請求項１１に記載の情報処理装置の制御方法。
【請求項１３】
前記通知工程では、前記要求端末認証工程において前記ユーザ端末が正当な端末と認証され、かつ、前記ユーザ認証工程において前記ユーザが正当なユーザと認証された場合に、前記回答に前記複数の識別子のうち第２の識別子を含めて前記通知を行うことを特徴とする請求項１２に記載の情報処理装置の制御方法。
【請求項１４】
前記通知工程では、前記要求端末認証工程において前記ユーザ端末が正当な端末と認証されない場合、或いは、前記ユーザ認証工程において前記ユーザが正当なユーザと認証されない場合に、前記回答には前記複数の識別子のいずれも含めることなく前記通知を行うことを特徴とする請求項１２又は１３に記載の情報処理装置の制御方法。
【請求項１５】
前記受信工程では、前記秘密鍵を指定するための情報を更に受信し、
前記署名生成工程では、該受信した情報が前記複数の識別子のうち第３の識別子に一致するか否かが判定され、該第３の識別子に一致すると判定された場合に、前記電子署名の生成が行われることを特徴とする請求項１１乃至１４のいずれかに記載の情報処理装置の制御方法。
【請求項１６】
請求項１０乃至１５のいずれかに記載の方法をコンピュータに実行させるためのコンピュータプログラム。
【請求項１７】
請求項１６に記載のコンピュータプログラムを格納したコンピュータで読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、署名生成処理に関するものである。
【背景技術】
【０００２】
近年、コンピュータとそのネットワークの急速な発達及び普及により、文字データ、画像データ、音声データなど、多種の情報がデジタル化されている。デジタルデータは、経

年変化などによる劣化がなく、いつまでも完全な状態で保存できる一方、容易に複製や編集・加工を施すことが可能である。

【０００３】

こうしたデジタルデータの複製、編集、加工はユーザにとって大変有益である反面、デジタルデータの保護が大きな問題となっている。特に、文書や画像データがインターネットなどの広域ネットワーク網を通して流通する場合、デジタルデータは改変が容易であるため、第三者によってデータが改ざんされる危険性がある。

【０００４】

そこで、送信されてきたデータが改ざんされたかどうかを受信者が検出するために、改ざん防止用の付加データを検証する方式としてデジタル署名という技術が提案されている。デジタル署名技術は、データ改ざんだけではなく、インターネット上でのなりすまし、否認などを防止する効果も持ち合わせている。

【０００５】

以降では、デジタル署名、ハッシュ関数、公開鍵暗号、及び公開鍵認証基盤について詳細に説明する。

【０００６】

[デジタル署名]

図１０は、署名作成処理および署名検証処理を説明するための模式図であり、図１０を参照して説明を行う。デジタル署名データ生成にはハッシュ関数と公開鍵暗号とが用いられる。

ここで、秘密鍵をＫｓ（２１０６）、公開鍵をＫｐ（２１１１）とすれば、送信者はデータＭ（２１０１）にハッシュ処理２１０２を施して固定長データであるダイジェスト値Ｈ（Ｍ）（２１０３）を算出することができる。次に、秘密鍵Ｋｓ（２１０６）を用いて固定長データＨ（Ｍ）に署名処理２１０４を施せば、デジタル署名データＳ（２１０５）を作成することができる。そして、受信者には、このデジタル署名データＳ（２１０５）とデータＭ（２１０１）とが送信される。

【０００７】

一方、受信者は、受信したデジタル署名データＳ（２１１０）を公開鍵Ｋｐ（２１１１）を用いて変換（復号）する。また、受信したデータＭ（２１０７）にハッシュ処理２１０８を施して、固定長のダイジェスト値：Ｈ（Ｍ）２１０９を生成する。検証処理２１１２では、復号により得られたデータと、ダイジェスト値Ｈ（Ｍ）とが一致するか否かを検証する。そして、この検証により両データが一致しないならば、改ざんが行われたことを検出できる。

【０００８】

デジタル署名にはＲＳＡ、ＤＳＡ（詳細は後述）などの公開鍵暗号方式が用いられている。これらのデジタル署名の安全性は、秘密鍵の所有者以外のエンティティが、署名を偽造、もしくは秘密鍵を解読することが計算的に困難であることに基づいている。

【０００９】

[ハッシュ関数]

次に、ハッシュ関数について説明する。ハッシュ関数は署名対象データを非可逆に圧縮して署名付与処理時間を短縮するためにデジタル署名処理とともに利用される。つまり、ハッシュ関数は任意の長さのデータＭに処理を行い、一定の長さの出力データＨ（Ｍ）を生成する機能を持っている。ここで、出力Ｈ（Ｍ）を平文データＭのハッシュデータと呼ぶ。

【００１０】

特に、一方向性ハッシュ関数は、データＭを与えた時、Ｈ（Ｍ'）＝Ｈ（Ｍ）となる平文データＭ'の算出が計算量的に困難であるという性質を持っている。上記一方向性ハッシュ関数としてはＭＤ２、ＭＤ５、ＳＨＡ－１などの標準的なアルゴリズムが存在する。

【００１１】

[公開鍵暗号]

次に、公開鍵暗号について説明する。公開鍵暗号は２つの異なる鍵を利用し、片方の鍵で暗号処理したデータは、もう片方の鍵でしか復号処理できないという性質を持っている。上記２つの鍵のうち、一方の鍵は公開鍵と呼ばれ、広く公開するようにしている。また、もう片方の鍵は秘密鍵と呼ばれ、本人のみが持つ鍵である。

【００１２】

公開鍵暗号方式を用いたデジタル署名としては、ＲＳＡ署名、ＤＳＡ署名、Schnorr署名などが挙げられる。ここでは例として非特許文献１に記載されているＲＳＡ署名と、非特許文献２に記載されているＤＳＡ署名を説明する。

【００１３】

[ＲＳＡ署名]

素数ｐ、ｑを生成しｎ＝ｐｑとおく。λ（ｎ）をｐ－１とｑ－１の最小公倍数とする。λ（ｎ）と素な適当なｅを選び、ｄ＝１／ｅ （ｍｏｄ λ（ｎ））とおく。公開鍵をｅおよびｎとし、秘密鍵をｄとする。またＨ（）をハッシュ関数とする。

【００１４】

[ＲＳＡ署名作成]文書Mに対する署名の作成手順

ｓ：＝Ｈ（Ｍ）＾ｄ（ｍｏｄ ｎ）を署名データとする。

【００１５】

[ＲＳＡ署名検証] 文書Mに対する署名 (s,T) の検証手順

（Ｍ）＝ｓ＾ｅ（ｍｏｄ ｎ）かどうか検証する。

【００１６】

[ＤＳＡ署名]

p, q を素数とし、 p-１は qを割り切るとする。ｇをZ_p*（位数pの巡回群Z_p から０を省いた乗法群）から任意に選択した、位数qの元（生成元）とする。 Z_p*から任意に選択したxを秘密鍵とし、それに対する公開鍵yをy:= gx mod pとおく。 H()をハッシュ関数とする。

【００１７】

[ＤＳＡ署名作成]文書Mに対する署名の作成手順

１）αをZ_q から任意に選択し、T:= (gα mod p) mod qとおく。

２）c:= H(M) とおく。

３）s:=α-１(ｃ + ｘ Ｔ) mod q とおき、(s,T) を署名データとする。

【００１８】

[ＤＳＡ署名検証] 文書Mに対する署名 (s,T) の検証手順

Ｔ = (g h(M)s^-１ y Ts^-１ mod p) mod q かどうか検証する。

【００１９】

[公開鍵認証基盤]

クライアント・サーバ間の通信においてサーバのリソースにアクセスする際には、利用者認証が必要であるが、その一つの手段として ITU-U 勧告の X.５０９ 等の公開鍵証明書がよく用いられている。公開鍵証明書は公開鍵とその利用者との結びつけを保証するデータであり、認証機関と呼ばれる信用のおける第３者機関によるデジタル署名が施されたものである。例えば、ブラウザで実装されている SSL (Secure Sockets Layer) を用いた利用者認証方式は、ユーザの提示してきた公開鍵証明書内に含まれる公開鍵に対応する秘密鍵をユーザが持っているかどうか確認することで行われる。

【００２０】

公開鍵証明書は認証機関による署名が施されていることで、公開鍵証明書内に含まれているユーザやサーバの公開鍵を信頼することができる。そのため、認証機関が署名作成のために用いる秘密鍵が漏洩され、或いは脆弱になった場合、この認証機関から発行されたすべての公開鍵証明書は無効になってしまう。認証機関によっては膨大な数の公開鍵証明書を管理しているため、管理コストを下げるためにさまざまな提案が行われている。後述する本発明によれば、発行する証明書数を抑え、かつ公開鍵リポジトリとしてのサーバアクセスを軽減する効果がある。

【００２１】
公開鍵証明書の一例である非特許文献３に記載のITU-U 勧告X.５０９ v.３では被署名データとして証明対象となるエンティティ（Subject）のIDおよび公開鍵情報が含まれている。そして、これらの被署名データにハッシュ関数を施したダイジェストについて、前述したRSAアルゴリズムなどの署名演算により署名データが生成される。また、被署名データにはextensions というオプショナルなフィールドが設けられ、アプリケーション又はプロトコル独自の新しい拡張データを含ませることが可能である。
【００２２】
図１１は、X.５０９ v.３で規定されるフォーマットを示しているおり、以下、それぞれのフィールドに表示される情報を説明する。version１５０１は X.５０９ のバージョンが入る。このフィールドはオプショナルであり、省略された場合は v１ を表わす。serialNumber１５０２は認証局がユニークに割り当てるシリアル番号が入る。signature１５０３は、公開鍵証明書の署名方式が入る。issuer１５０４は、公開鍵証明書の発行者である認証局の X.５００ 識別名が入る。validity１５０５は、公開鍵の有効期限（開始日時と終了日時）が入る。
【００２３】
subject１５０６は、本証明書内に含まれる公開鍵に対応する秘密鍵の所有者の X.５００ 識別名が入る。subjectPublicKeyInfo１５０７は、証明する公開鍵が入る。issuerUniqueIdentifier１５０８及びsubjectUniqueIdentifier１５０９は、v２ から追加されたオプショナルなフィールドであり、それぞれ認証局の固有識別子、所有者の固有識別子が入る。
【００２４】
extensions１５０１は、v３ で追加されたオプショナルなフィールドであり、拡張型 (extnId)１５１１、クリティカルビット (critical)１５１２及び拡張値 (extnValue)１５１３の３つの値の集合が入る。v３ 拡張フィールドには、X.５０９ で定められた標準の拡張型だけでなく、独自の新しい拡張型も組み込むことが可能である。そのため v３ 拡張型をどう認識するかはアプリケーション側に依存することとなる。クリティカルビット１５１２はその拡張型が必須であるかまたは無視可能かを表わすものである。
【００２５】
以上、デジタル署名、ハッシュ関数、公開鍵暗号、及び公開鍵認証基盤について説明した。
【００２６】
前述のデジタル署名技術は公開鍵暗号方式をベースにしているため署名生成および署名検証に費やす計算量が膨大となる。特にＰＤＡなどの携帯端末では、公開鍵暗号方式に基づく認証方法には通常のＰＣと比較して計算コストが高くなる問題がある。そこで、機能の乏しい携帯端末でも、認証局で認証された証明書を用いた情報通信を行い、複数の認証局が発行した証明書の検証や管理等に対する作業負荷を軽減することが可能な認証代行方法が提案されている（特許文献１を参照。）
この提案方法によれば、ユーザ端末は、証明書の検証機能や電子署名機能を備える必要がなく、セキュリティの高い装置やシステムとのデータの送受信を行うことが可能となる。また、ユーザ端末は生体認証（バイオメトリクス）が可能な指紋等を入力するための生体認証データ入力部を持ち、入力された生体認証情報を認証代行サーバで検証する仕組みが提供される。これにより、ユーザ端末の盗難や紛失時にも、第３者による不法使用を確実に避けることが可能となる。
【特許文献１】特開２００１-１９７０５５号公報
【非特許文献１】R.L. Rivest, A. Shamir and L. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. ２１, n. ２, pp. １２０-１２６, Feb １９７８.
【非特許文献２】Federal Information Processing Standards (FIPS) １８６-２, Digital Signature Standard (DSS) , January ２０００

【非特許文献３】ITU-T Recommendation X.５０９/ISO/IEC ９５９４-８: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

【発明の開示】

【発明が解決しようとする課題】

【００２７】

以上のようにデジタル署名技術は、インターネット上でのなりすまし、データ改竄、否認などを防止する効果があり、その信頼基盤として公開鍵証明書が流通するインフラが整備されている。近年その信頼基盤を利用するデバイスは多様化しており、ＰＣやサーバだけでなく、情報家電や携帯電話などでも利用されつつある。しかし、信頼基盤を利用するデバイスは必ずしもユーザが信頼できるものとは限らない場面が増えている。例えば、通常利用している自身の携帯端末や社内ＰＣなどは、ユーザの秘密鍵を格納しており、ユーザは信頼して利用することができる。その一方で、第３者が利用可能なキオスク端末、出先のＰＣや複合機などの信頼性が検証できないデバイスを利用する状況も考えられる。このような状況では、特に自分の秘密鍵を用いた処理、つまり、署名作成処理を行う場合には注意を要する。

【００２８】

署名作成処理にはユーザの秘密鍵が必要であるが、通常信頼できるローカルマシンのハードディスク上や持ち運び可能なＵＳＢドングルなどに格納されている。
一方、上記のキオスク端末、出先のＰＣや複合機において作成した、またはスキャンしたドキュメントに対して署名を施す場合、ユーザが安心して秘密鍵を取り込むインターフェイスが必要となる。仮に、秘密鍵取り込みインターフェイスが備わっていても、意図した署名対象と異なるドキュメントに署名させられる脅威、即ち署名対象データが画面上に表示されても、そのドキュメントが改竄された後に署名を付与してしまう脅威が存在する。

【００２９】

上記の提案方法では、秘密鍵を持ち運ぶことなく署名代行を行う機構が提供される。しかしこの方法では、リモート端末がユーザを正しく認証しても、ローカル端末をユーザが信頼できるかどうかが不明のまま署名処理を代行することになる。

【００３０】

そこで本発明は、信頼度が不明なローカル端末でも安全に署名を生成する仕組みを提供するために、ローカル端末を遠隔サーバが信頼できるかどうかをユーザに安全に知らせることを可能とする。

【課題を解決するための手段】

【００３１】

上記課題を解決するための本発明は、電子署名の生成依頼をユーザ端末から受け付ける要求受付手段と、前記ユーザ端末を認証する要求端末認証手段と、前記ユーザ端末を介して前記生成依頼を行ったユーザを認証するユーザ認証手段と、前記要求端末認証手段と前記ユーザ認証手段とにおける認証結果に基づき、前記生成依頼に対する回答を前記ユーザ端末に通知する通知手段とを備える。

【発明の効果】

【００３２】

本発明によれば、ローカル端末を遠隔サーバが信頼できるかどうかの結果をユーザに安全に知らせることが可能となる。

【発明を実施するための最良の形態】

【００３３】

以下、図面を参照して、本発明の好適な実施形態を説明する。

【００３４】

［第１の実施形態］

本実施形態では、紙文書をスキャンして生成された画像データやあらかじめ格納されたデジタルコンテンツにデジタル署名を施した、複合コンテンツ（以下、電子文書と呼ぶ）

を生成する電子文書生成処理について説明する。

【００３５】

図１は、本実施形態に対応するシステムの一例を示した図である。図１のシステムにおいて、電子文書を生成する端末１０１及び署名代行サーバ１０３は、ネットワーク１０４に接続されている。ユーザ１０５は、端末１０１に格納されている電子文書、端末１０１に接続されたスキャナ１０２から取り込んだ画像データ、もしくは、それらの複合コンテンツに対して、端末１０１において署名処理を行ってデジタル署名を施す。

【００３６】

署名処理を行う場合、秘密鍵が必要となるが、端末１０１に格納されている秘密鍵を用いてもよいし、或いは、端末１０１に秘密鍵を取り込むインターフェイスが備えられており、そのインターフェイスから秘密鍵を取り込んで用いてもよい。更に、ネットワーク１０４を介して署名代行サーバ１０３にある秘密鍵を用いることも可能である。サーバ１０３は、署名処理を実行するための署名作成デーモン（プログラム）１０７を備え、秘密鍵を管理するための秘密鍵データベース１０８が接続されている。

【００３７】

図２は、端末１０１にてユーザ１０５が署名処理を行う際の、端末１０１のディスプレイにおける表示画面の一例を示した図である。図２において、表示画面２０１には、被署名データ表示部２０２、秘密鍵選択部２０３、署名処理実行ボタン２０４が表示されている。ユーザ１０５は、被署名データ表示部２０２から署名対象データの確認を行い、秘密鍵選択部２０３からどの秘密鍵を用いるかを選択し、署名処理実行ボタン２０４を押すことで署名処理を実行できる。

【００３８】

秘密鍵選択部２０３は、以下の３通りの方式を選択可能である。まず、（１）端末１０１に格納されている秘密鍵を用いる方式である。次に、（２）端末１０１に秘密鍵を取り込むインターフェイスが備えられており、そのインターフェイスから秘密鍵を取得して用いる方式である。更に、（３）ネットワーク１０４を介して署名代行サーバ１０３にある秘密鍵を用いる方式である。なお、同一方式であっても、複数の秘密鍵が端末１０１に格納されている場合や、秘密鍵入力インターフェイスが複数存在する場合がある。更には、異なる署名代行サーバが複数存在する場合もある。従って、それぞれの方式ごとに、更に複数の選択肢が表示される。

【００３９】

特に、（３）の方式の場合には、署名代行サーバ１０３にある、署名作成デーモン（プログラム）１０７と秘密鍵データベース１０８が用いられる。また、ユーザ１０５は、例えば携帯端末１０６のような、ネットワーク１０４とは別のチャネルを用いた通信手段を利用することもできる。

【００４０】

以下の説明では、別チャネルの通信手段として携帯端末１０６を仮定して説明を行うが、ネットワーク１０４とは別のチャネルを用いた通信手段で署名代行サーバ１０３からの情報をユーザ１０５に伝えることができればどのような手段でも構わない。例えばＦＡＸ、固定電話、携帯電話、その他のキャリアを用いた電子メール、郵便などが挙げられるが、これらに限定されるものではない。

【００４１】

図３は、端末１０１および署名代行サーバ１０３の内部ハードウエア構成の一例である。３０１はソフトウエアを実行することで装置の大部分を制御するＣＰＵである。３０２は、ＣＰＵ３０１が実行するソフトウエアやデータを一時記憶するメモリである。３０３は、ソフトウエアやデータを保存するハードディスクである。３０４は、キーボードやマウス、スキャナなどの入力情報を受け取り、またディスプレイやプリンタに情報を出力する入出力（Ｉ／Ｏ）部である。

【００４２】

[電子文書生成処理]

次に、本実施形態に対応する電子文書生成処理について説明する。図４は本実施形態の電子文書生成処理の一例を示す機能ブロック図である。

【００４３】

本実施形態に対応する電子文書生成処理では、まず、電子文書入力工程４０２において電子文書４０１が入力される。また、紙文書４０３が紙文書入力工程４０４において入力される。中間電子文書生成工程４０５では、入力された紙文書４０３を解析し中間電子文書が生成される。中間電子文書、電子文書４０１および秘密鍵４０６は、署名情報生成工程４０７に入力され署名情報が生成される。また、中間電子文書、電子文書４０１及び署名情報は、署名情報付加工程４０８において互いに関連付けられる。更に、電子文書生成工程４０９では、中間電子文書、電子文書４０１及び署名情報が統合され、電子文書４１１が生成される。電子文書４１１は、電子文書送信工程４１０により外部に送信される。

【００４４】

なお、生成・送信された電子文書４１１が、再度電子文書４０１として電子文書生成工程４０２に入力され、新たな電子文書４１１が再生成されてもよい。以下、各機能ブロックの詳細について説明する。

【００４５】

まず、図４の中間電子文書生成工程４０５の詳細について説明する。図５は本実施形態に対応する中間電子文書生成工程４０５における処理の一例を示すフローチャートである。

【００４６】

ステップＳ５０１では、紙文書入力工程４０４から得られたデータを電子化し、電子データを生成する。次に、ステップＳ５０２では、電子データを属性ごとに領域分割する。ここでいう属性とは、文字、写真、表、線画があげられる。

【００４７】

領域分割処理は、例えば文書画像中の黒画素の８連結輪郭塊や白画素の４連結輪郭塊といった集合を抽出し、その形状、大きさ、集合状態などから、文字、絵や図、表といった文書に特徴的な領域を抽出することができる。この手法は、例えば米国特許第５６８０４７８号公報に記載されている。なお、領域分割処理の実現方法は、これに限られるものではなく、他の方法を適用しても良い。

【００４８】

次にステップＳ５０３では、ステップＳ５０２において得られた領域ごとに文書情報を生成する。文書情報とは属性、ページの位置座標等のレイアウト情報、分割された領域の属性が文字であれば文字コード列や、段落や表題などの文書論理構造等があげられる。

【００４９】

次にステップＳ５０４では、ステップＳ５０２において得られた領域ごとに伝達情報に変換する。

伝達情報とは、レンダリングに必要な情報のことである。具体的には解像度可変のラスタ画像、ベクタ画像、モノクロ画像、カラー画像、それぞれの伝達情報のファイルサイズ、分割された領域の属性が文字であれば文字認識した結果のテキストがある。また、個々の文字の位置、フォント、文字認識によって得られた文字の信頼度等が挙げられる。

【００５０】

次にステップＳ５０５では、ステップＳ５０２で分割された領域とステップＳ５０３で生成された文書情報とステップＳ５０４で得られた伝達情報を関連付ける。関連付けた情報はツリー構造で記述される。これ以降、上記ステップで生成された伝達情報および文書情報を構成要素と呼ぶ。

【００５１】

ステップＳ５０６では、前段で生成された構成要素を中間電子文書として保存する。保存の形式はツリー構造を表現可能な形式であればよい。本実施形態では、構造化文書の一例であるＸＭＬ形式にて保存する。

【００５２】

次に、図４の署名情報生成工程４０７について説明する。本工程では、先に生成された中間電子文書の構成要素に対し、デジタル署名を生成する。図７は、本実施形態に対応する署名情報生成工程における処理のフローチャートであり、以下、署名情報生成工程４０７を図７を参照して説明する。

【００５３】

まず、ステップＳ８０１では、被署名データのダイジェスト値を、被署名データ毎に夫々生成する。ここで、被署名データとは、中間電子文書中に含まれる署名対象データのことであり、後述する図６における伝達情報ａ（７０１）、伝達情報ｂ（７０２）、或いは文書情報（７０３）であると考えれば理解し易い。また、ダイジェスト値を生成するために、本実施形態ではハッシュ関数を適用する。ハッシュ関数については、「背景技術」の項においてすでに説明したので、ここでの詳細な説明は省略する。

【００５４】

次に、ステップＳ８０２では、被署名データの識別子を、被署名データ毎に生成する。ここで、識別子としては、被署名データをユニークに識別可能なものであれば良い。例えば、本実施形態では、被署名データの識別子として、ＲＦＣ２３９６で規定されているＵＲＩを適用するものとするが、本発明はこれに限定されることなく、種々の値を識別子として適用可能である。

【００５５】

そして、ステップＳ８０３では、全ての署名対象データに対してステップＳ８０１及びステップＳ８０２が適用されたか否かが判定される。全ての署名対象データに対してステップＳ８０１及びステップＳ８０２が適用された場合には（ステップＳ８０３において「ＹＥＳ」）、処理をステップＳ８０４に進め、さもなければステップＳ８０１に戻る。

【００５６】

ステップＳ８０４では、ステップＳ８０１で生成された全てのダイジェスト値、及び、ステップＳ８０２で生成された全ての識別子に対し、秘密鍵４０６を用いて署名処理を実行し、署名値を算出する。署名値を算出するために、本実施形態では「背景技術」の項において説明したデジタル署名を適用する。例えば、図１０で示した署名作成処理フローにおける入力データ：Ｍ（２１０１）が、ここではステップＳ８０１で生成された全てのダイジェスト値、及びステップＳ８０２で生成された全ての識別子（このデータ群を集約データと呼ぶ）に該当する。同じく秘密鍵Ｋｓ（２１０６）は図４の秘密鍵４０６に対応する。なお、デジタル署名の具体的な演算処理については詳細な説明は、ここでは省略する。

【００５７】

ここで秘密鍵４０６は、図２の秘密鍵選択部２０３で選択された方法で利用される。ローカル端末（端末１０１）から入手する場合は上記に述べたとおりに処理される。一方、リモート端末（署名代行サーバ１０３）に署名処理を委任する場合については、図８を参照して後述する。

【００５８】

続いて、ステップＳ８０５では集約データ（ステップＳ８０１で生成された全てのダイジェスト値とステップＳ８０２で生成された全ての識別子）及びステップＳ８０４で生成された署名値を用いて署名情報を構成し、署名生成処理を終了する。

【００５９】

続いて、署名データ付加工程４０８における処理ついて、図６（Ａ）を参照して説明する。７０１及び７０２は中間電子文書生成工程４０５で生成された中間電子文書の伝達情報であり、７０３は文書情報である。また７０４及び７０５は署名情報生成工程４０７で生成された署名情報である。

【００６０】

署名情報には、前述したように被署名データにあたる伝達情報や文書情報を指し示す識別情報を埋め込んである。図６（Ａ）では、署名情報７０４には被署名データ（即ち、伝達情報７０１）を指し示す識別情報７０６が埋め込まれる。署名データと被署名データは

一対一対応でなくてもよく、例えば、署名情報７０５には被署名データの伝達情報７０２及び文書情報７０３を指し示す識別情報７０７及び７０８を埋め込んでもよい。

【００６１】

次に、電子文書生成工程４０９について図６（Ａ）及び（Ｂ）を参照して説明する。これまでの工程で生成された中間電子文書および署名データは図６（Ａ）のようにそれぞれが独立した個々のデータとして存在している。そこで、電子文書生成工程ではこれらのデータをひとつにアーカイブし電子文書を生成する。図６（Ｂ）は中間電子文書と署名データとをアーカイブ化した一例を示す模式図であり、アーカイブデータ７０９は図４の電子文書４１１に該当する。また図６（Ａ）に記載の７０１から７０５については、７０１が７１３、７０２が７１４、７０３が７１２、７０４が７１０、そして７０５が７１１にそれぞれ対応する。

【００６２】

最後に電子文書送信工程４１０において、電子文書４１１が外部に送信される。生成された電子文書４１１は再び電子文書４０１として電子文書生成工程に入力され、新たな電子文書４１１を再構成するために利用されてもよい。

【００６３】

以上、本実施形態における電子文書生成処理について説明した。

【００６４】

[署名処理を委任する場合]

次に、リモート端末（署名代行サーバ１０３）に署名処理を委任する場合について、図８を参照して説明する。図８は署名代行処理のシーケンス図であり、ユーザ１０５、端末１０１、署名作成デーモン１０７および秘密鍵データベース１０８間のプロトコルで構成される。

【００６５】

９０１において、ユーザは、被署名データ表示部２０２の表示により、署名対象データの内容を確認することができる。このとき、図２の表示例に対応する表示画面では秘密鍵選択部２０３には"（３）署名代行サーバ利用"が表示され、所望の署名代行サーバがＵＲＩに基づいて選択され、署名処理実行ボタン２０４が操作されると、以降の９０２の処理が実行される。

【００６６】

９０２では、端末１０１は、署名代行サーバ１０２がユーザ１０５を認証・識別するための識別子として、ユーザ認証データの入力をユーザ１０５から受け付ける。ユーザ認証データの入力は、キーボードによるパスワード入力に限らず端末の入力手段に応じて適当なものを選択可能である。また、パスワード利用の場合には、固定ワードだけではなく、携帯端末を用いた時刻に応じて変化するワンタイムパスワードや、異なるエンティティに署名作成権限を委譲するための使い捨てパスワードなどを利用することもできる。

【００６７】

９０３では、端末１０１は、ユーザ１０５から入力されたユーザ認証データを内包する署名生成依頼メッセージを生成し、署名代行サーバ１０２（実際には署名作成デーモン１０７が要求を受け付ける）に送信する。このとき、署名生成依頼メッセージには、署名代行サーバ１０２が管理するユーザ識別子が含まれてもよい。このユーザ識別子は端末１０１にログインする認証行為と紐付けされていてもよい。

【００６８】

９０４では、署名代行サーバ１０２が、端末認証を行い、署名生成依頼メッセージの発信元である端末１０１が信頼できる端末かどうかを判定する。

ここでの端末認証は、例えば公開鍵暗号方式による認証方式、公開鍵証明書および公開鍵認証基盤を用いた認証方式、共通鍵暗号方式による認証方式など、ユーザ１０５と署名代行サーバ１０２のポリシーに基づいた端末認証を行うことができる。

【００６９】

９０５では、署名作成デーモン１０７が、受信した署名生成依頼メッセージを解析し、

ユーザ認証データを抽出して秘密鍵データベース１０８に送信する。ここで、９０５と９０４とは並行処理されても良いし、逐次的処理されてもよい。

【００７０】

９０６では、ユーザ認証データに基づいて、所望の秘密鍵が存在するか、正当なユーザであるかどうかを判定する。もし、秘密鍵が存在し正当なユーザーと判定されれば、要求端末認証結果を署名作成デーモン１０７に返信する。ここで、要求端末認証結果には、ユーザ認証データに対応したデータが内包される。この要求端末認証結果はユーザ１０５が９０２にて入力したユーザ認証データに対応する識別子としての情報であり、ユーザ自身がそのことを確認することが可能なデータであれば、どのような形態であってもよい。例えば、所定のパスワードなどを利用することができる。

【００７１】

９０７では、署名作成データ部１０７は、９０４における端末認証で端末１０１が信頼できる端末と判定され、要求端末認証結果が秘密鍵データベース１０８から得られた場合には、要求端末認証結果を端末１０１に送信する。一方、９０４における端末認証に失敗した場合、或いは、要求端末認証結果が秘密鍵データベース１０８から得られなかった場合には、要求端末認証結果の代わりにダミーデータを端末１０１に送信する。

【００７２】

９０８では、端末１０１は、署名代行サーバ１０３から受信した要求端末認証結果を表示する。このとき、端末１０１が不正端末であった場合、或いは、ユーザが正当なユーザでなかった場合には、画面には正しい情報が表示されないこととなる。

【００７３】

９０９では、ユーザ１０５は、端末１０１に表示された要求端末認証結果が９０２にて入力したユーザ認証データと対応する内容であるかを確認する。要求端末認証結果は、例えばパスワード形式で表示されるが、これに限らず端末１０１の表示機能に依存した適当な手段で提供することができる。このとき、ユーザ１０５は乱数表に対応付けを確認することもあり得る。

【００７４】

９１０では、ユーザ１０５が端末１０１を信頼できると判断した場合、確認通知を端末１０１に入力する。この確認通知には、キーボード入力によるパスワードに限らず、端末の他の入力手段に応じて適当なものを選択可能である。なお、パスワードの場合には、固定ワードだけではなく、携帯端末を用いた時刻に応じて変化するワンタイムパスワードや、異なるエンティティに署名作成権限を委譲するための使い捨てパスワードなどを利用することができる。ここで、確認通知は、前述のユーザ認証データ及び要求端末認証結果と関連づけられた識別子としての情報であって、署名代行サーバ１０２に対し、ユーザ１０５が署名を許可したか否かを判定するために利用される。

【００７５】

９１１では、端末１０１は、被署名データのハッシュ関数による演算結果であるダイジェストを、確認通知とともに署名作成デーモン１０７に送信する。ここで、ダイジェストの代わりに被署名データそのものを送信してもよい。

【００７６】

９１２では、署名作成デーモン１０７は、被署名データまたはそのダイジェストと、確認通知とを秘密鍵データベース１０８に送信する。秘密鍵データベース１０８では、確認通知と関連づけられた秘密鍵を探索する。即ち、確認通知が、秘密鍵と予め関連づけられたユーザ１０５の識別子に一致するか否かを判定する。この結果、確認通知がユーザ１０５の識別子と一致し、秘密鍵が存在する場合には、該秘密鍵を利用して被署名データまたはダイジェストに対して署名処理を施し署名データを生成する。

【００７７】

９１３では、生成された署名データを署名作成デーモン１０７に戻し、９１４では、署名データを端末１０１に返信する。９１５では、端末１０１が、署名データを電子文書生成工程４０９に応じてアーカイブして電子文書４１１を生成する。

【００７８】
以下、端末１０１が不正端末であった場合について説明する。不正端末である場合には、署名代行サーバ１０２が端末認証９０４においてそのことを検知する。よって、９０７では、正しい要求端末認証結果が返却されない。そのため、ユーザ１０５は、端末１０１に表示された内容に基づいて９０９において、端末１０１が不正端末であることを認知することができる。これにより、以降の処理、つまり秘密鍵を用いた遠隔署名処理を中断できる。

【００７９】
また仮に、端末１０１が９０８から９１０を省略して、９１１にて確認通知を不正に送信して不正に遠隔署名を依頼しようとても、正しい確認通知はユーザ１０５しか知りえない。従って、そのような確認通知と関連づけられた秘密鍵を探索しても、秘密鍵は存在しないので、係る確認通知は不正なものと直ちに判断することができる。これにより、署名代行サーバ１０３側で不正を検知し、署名データの生成を中止することができる。このようにして、不正端末を介した署名データの作成を防止して、安全に遠隔署名を実行させる仕組みを提供することができる。

【００８０】
以上、署名処理を委任する場合について説明した。本方式によれば、信頼度が不明なローカル端末であっても安全に署名生成する仕組みを提供することができる。即ち、ローカル端末（端末１０１）を遠隔サーバ（署名代行サーバ１０３）が信頼できるかどうかの結果をユーザに安全に知らせることができるので、ユーザはその信頼性を確認した上で、ローカル端末を利用するか否かを決定することができる。また、これらの仕組みは、特殊なデバイスが不要でパスワードの組が記載された乱数表だけを持てば実現可能であるため、導入コストが低いというメリットがある。

【００８１】
［第２の実施形態］
以上に説明した第１の実施形態では、署名処理の委任を大きく分けてローカルとリモート間の４ウェイのプロトコル（９０３、９０７、９１１及び９１４）で構成されている。これに対し、本実施形態では、署名データを事前に要求端末認証結果に埋め込んでおくことにより、２ウェイのプロトコルで構成することができる。

【００８２】
本実施形態では、図８の９１１以降のフローは行わない。その代わりに、９１１にて送信される被署名データまたはダイジェスト、および、９１４で受信される署名データを、それぞれ９０３および９０７で同時に送信する。

【００８３】
９０３では、署名生成依頼メッセージに加え、被署名データまたはダイジェストもあわせて、端末１０１から署名代行サーバ１０３へ送信する。被署名データまたはダイジェストは、９０３における送信より前に予め送信しておいてもよい。このようにすれば、署名代行サーバ１０３は、９０７における要求端末認証結果の送信に先だって、所望の秘密鍵を探索し、その秘密鍵を用いて被署名データまたはダイジェストに対して署名処理を行うことができる。また、９０６では、ユーザ認証結果と併せて署名データが、秘密鍵データベース１０８から署名作成デーモン１０７に返信される。

【００８４】
９０７では、要求端末認証結果に加え、署名データを送信することができるが、端末１０１が不正である場合に備え、署名データは暗号化して送信することとする。暗号化された署名データは、９１０においてユーザ１０５から端末１０１に確認通知が入力された場合に、端末１０１において復号することができる。

【００８５】
以上、２ウェイ（９０３及び９０７）のプロトコルでの実施形態を説明した。これにより、簡素化されたデータフローで第１の実施形態と同様の効果が得られる。

【００８６】

［第３の実施形態］

前述の第１及び第２の実施形態では、図８の９０８で端末１０１が表示する要求端末認証結果が不正に改ざんされていることを想定しているため、ユーザは３つの関連づけされたパスワードを管理する必要がある。この３つとは、ユーザ認証データ、要求端末認証結果、及び確認通知である。また、これにより、上記の実施形態を実現するためのプロトコルも複雑な処理となる。

【００８７】

そこで、本実施形態では、新たなエンティティとしてユーザ１０５が信頼できる携帯端末１０６を想定し、携帯端末１０６が表示するデータは信頼できるとの前提において、より簡素化されたプロトコルによりシステムを構築する。

【００８８】

図９は、本実施形態に対応する署名代行処理のシーケンスの一例を示す図であり、図８でのユーザ１０５、端末１０１、署名作成デーモン１０７及び秘密鍵データベース１０８に加え、携帯端末１０６が追加されている。以下、本実施形態におけるシーケンスについて説明する。なお、本実施形態では、第２の実施形態（２ウェイのプロトコル）を変形したものについて説明するが、本実施形態は第１の実施形態についても同様に適用可能である。

【００８９】

図９において、１００１から１００６までは、第２の実施形態の９０１から９０６までと同様であるため説明を省略し、１００７以降の処理について説明する。

【００９０】

図８の９０７での処理は、図９において１００７ａおよび１００７ｂに分割される。まず１００７ａでは、暗号化された署名データが端末１０１に送信され、１００７ｂでは、要求端末認証結果が、端末１０１ではなく、信頼できる携帯端末１０６に送信される。要求端末認証結果は、前述の実施形態と同じく１００２で入力したユーザ認証データと予め関連づけられた他のデータでもよい。また、署名代行サーバ１０２が発信元であることが確認できるのであれば、要求端末認証結果とユーザ認証データが同一であっても構わない。

【００９１】

１００８では、１００７ｂで受信した要求端末認証結果に基づき、ユーザ１０５が端末１０１を信頼できると判断すれば、確認通知がユーザ１０５により端末１０１に入力される。確認通知は、１００７ｂを介して要求端末認証結果と共にユーザ１０５に渡されることも考えられる。この場合には１トランザクションにつき１つのパスワードを管理するだけでよい。

【００９２】

ユーザ１０５による確認通知のへの入力を受けて、端末１０１では１００９で暗号化された署名データの復号処理を行い、１０１０で、電子文書生成工程４０９に応じてアーカイブして電子文書４１１を生成する。

【００９３】

このようにしてユーザが管理すべきパスワードの数を減らすことができる。具体的に、第１及び第２の実施形態では、１トランザクションにつき３つのパスワードを管理しなければならなかったが、本実施形態では、ユーザは１つのパスワードを管理すればよい。よって、ユーザの利便性を大きく向上させることができる。

【００９４】

＜他の暗号アルゴリズムによる実施形態＞

前述の実施形態では暗号処理（秘匿化）方法に関して触れていないが、公開鍵暗号方式による暗号処理方法だけでなく、共通鍵暗号方式による暗号処理方法への適用は容易である。よって、他の暗号アルゴリズムを適用することによって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【００９５】

＜ソフトウエアなどによる他の実施の形態＞

本発明は、複数の機器（例えばホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムの一部として適用しても、ひとつの機器（たとえば複写機、ファクシミリ装置）からなるものの一部に適用してもよい。

【００９６】

また、本発明は上記実施の形態を実現するための装置及び方法及び実施の形態で説明した方法を組み合わせて行う方法のみに限定されるものではなく、上記システムまたは装置内のコンピュータ（ＣＰＵあるいはＭＰＵ）に、上記実施の形態を実現するためのソフトウエアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【００９７】

またこの場合、前記ソフトウエアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【００９８】

この様なプログラムコードを格納する記憶媒体としては、例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９９】

また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているＯＳ(オペレーティングシステム)、あるいは他のアプリケーションソフト等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【０１００】

更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【図面の簡単な説明】

【０１０１】

【図１】本発明の実施形態に対応するシステムの構成例を示す図である。

【図２】本発明の実施形態に対応する署名処理を行う際の表示画面の一例を示す図である。

【図３】本発明の実施形態に対応する装置のハードウエア構成の一例を示す図である。

【図４】本発明の実施形態に対応する電子文書生成工程の機能ブロック図の一例である。

【図５】本発明の実施形態に対応する中間電子文書生成工程のフローチャートの一例である。

【図６】本発明の実施形態に対応する中間電子文書及び電子化データを説明するための図である。

【図７】本発明の実施形態に対応する署名データ生成工程のフローチャートの一例である。

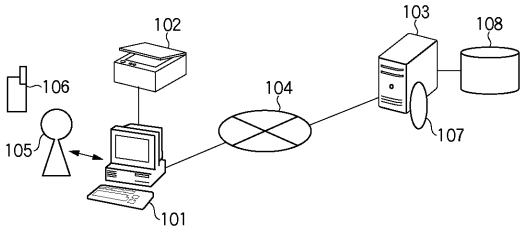
【図８】本発明の第１の実施形態に対応する署名代行処理のシーケンスの一例を示す図である。

【図９】本発明の第３の実施形態に対応する署名代行処理のシーケンスの一例を示す図である。

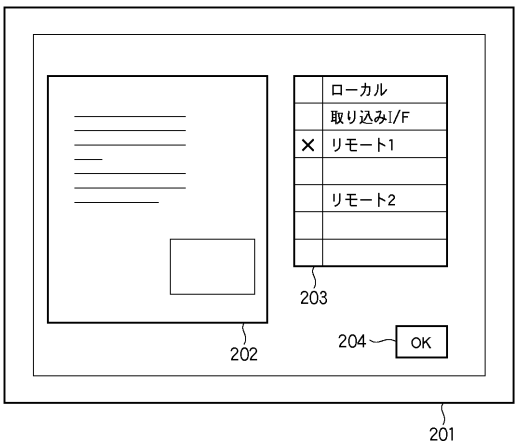
【図１０】署名作成処理および署名検証処理の一般例を表す模式図である。

【図１１】公開鍵証明書X.５０９v.３のデータフォーマットを説明するための図である。

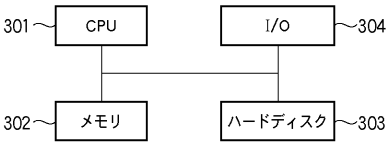
【図１】



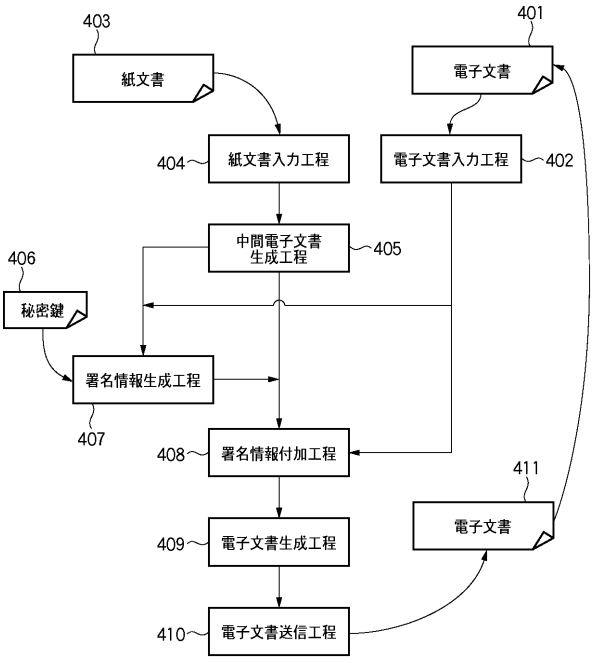
【図２】



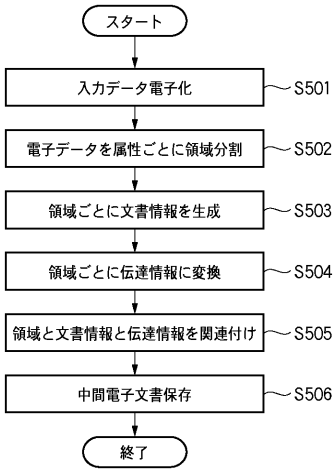
【図３】



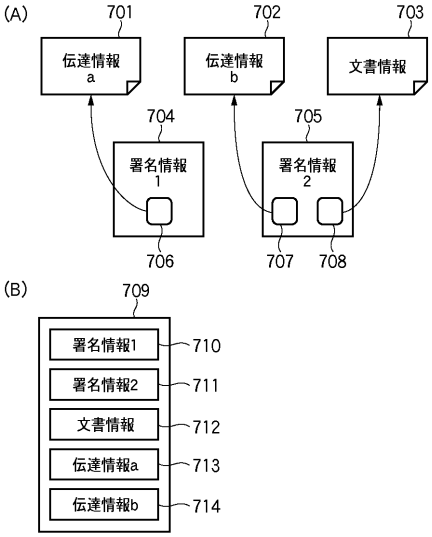
【図４】



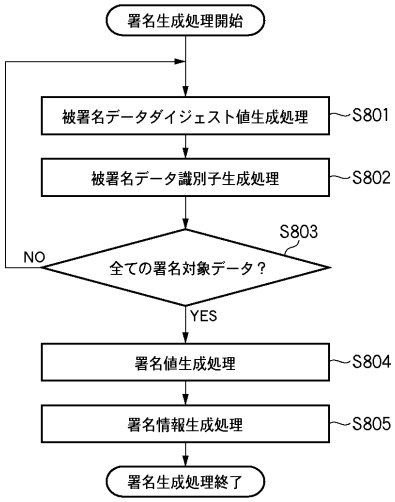
【図５】


スタート
入力データ電子化
S501
電子データを属性ごとに領域分割
S502
領域ごとに文書情報を生成
S503
領域ごとに伝達情報に変換
S504
領域と文書情報と伝達情報を関連付け
S505
中間電子文書保存
S506
終了

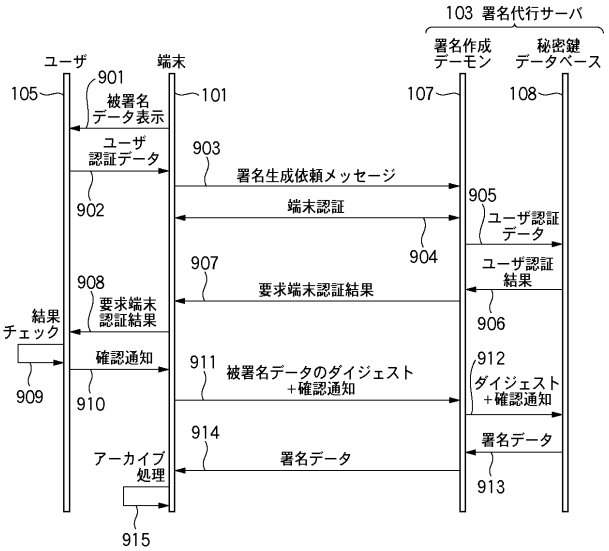
【図６】


(A)
701
伝達情報 a
702
伝達情報 b
703
文書情報
704
署名情報 1
705
署名情報 2
706
707
708
(B)
709
署名情報1
710
署名情報2
711
文書情報
712
伝達情報a
713
伝達情報b
714

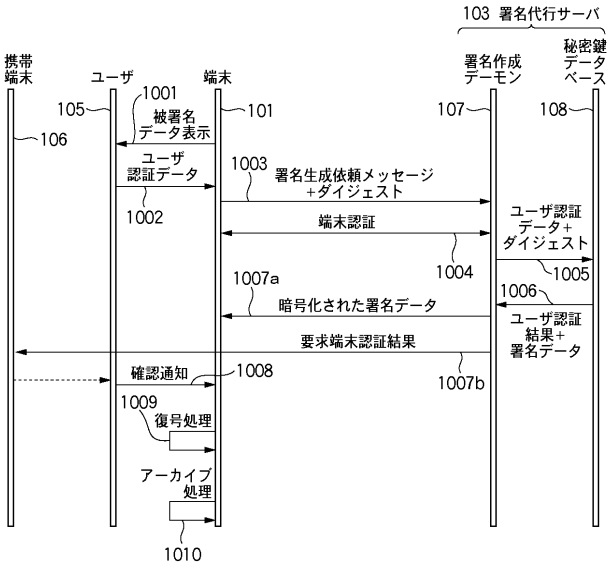
【図７】


署名生成処理開始
被署名データダイジェスト値生成処理
S801
被署名データ識別子生成処理
S802
S803
全ての署名対象データ？
NO
YES
署名値生成処理
S804
署名情報生成処理
S805
署名生成処理終了

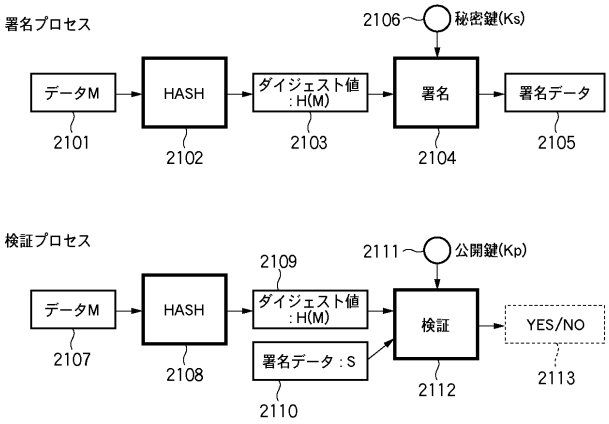
【図８】


103 署名代行サーバ
ユーザ
端末
署名作成 デーモン
秘密鍵 データベース
105
901
被署名 データ表示
101
107
108
ユーザ 認証データ
903
署名生成依頼メッセージ
902
端末認証
905
ユーザ認証 データ
904
907
ユーザ認証 結果
908
要求端末認証結果
906
結果 チェック
要求端末 認証結果
確認通知
911
被署名データのダイジェスト +確認通知
912
ダイジェスト +確認通知
909
910
914
署名データ
アーカイブ 処理
913
915

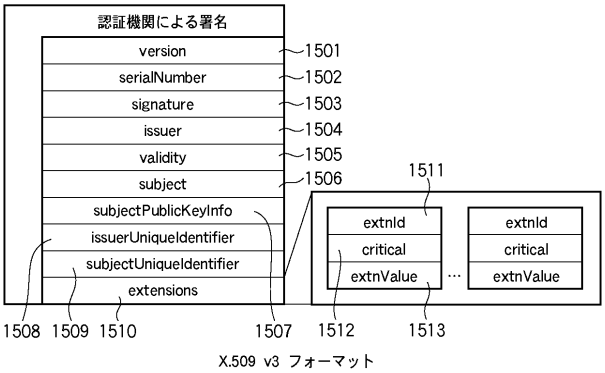
【図９】


103 署名代行サーバ
携帯端末
ユーザ
端末
署名作成デーモン
秘密鍵データベース
106
105
1001
被署名データ表示
101
107
108
ユーザ認証データ
1002
1003
署名生成依頼メッセージ+ダイジェスト
端末認証
1004
ユーザ認証データ+ダイジェスト
1005
1007a
暗号化された署名データ
1006
ユーザ認証結果+署名データ
要求端末認証結果
1007b
確認通知
1008
1009
復号処理
アーカイブ処理
1010

【図１０】


署名プロセス
2106
秘密鍵(Ks)
データM
HASH
ダイジェスト値 : H(M)
署名
署名データ
2101
2102
2103
2104
2105
検証プロセス
2111
公開鍵(Kp)
2109
データM
HASH
ダイジェスト値 : H(M)
検証
YES/NO
署名データ : S
2107
2108
2110
2112
2113

【図１１】


認証機関による署名
version
serialNumber
signature
issuer
validity
subject
subjectPublicKeyInfo
issuerUniqueIdentifier
subjectUniqueIdentifier
extensions
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
extnId
critical
extnValue
1512
1513
X.509 v3 フォーマット

フロントページの続き

Ｆターム(参考) 5J104 AA07 AA09 JA21 KA01 KA02 KA05 LA03 LA06 NA02 NA12
NA38 PA07