(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年11 月18 日 (18.11.2004)

PCT

(10) 国際公開番号
WO 2004/100444 A1

(51) 国際特許分類[7]: H04L 9/32, G09C 1/00

(21) 国際出願番号: PCT/JP2003/005831

(22) 国際出願日: 2003 年5 月9 日 (09.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市中原区 上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 原田 一幸 (HARADA,Kazuyuki) [JP/JP]; 〒211-8588 神奈川県 川崎市中原区 上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 酒井 宏明 (SAKAI,Hiroaki); 〒100-0013 東京都 千代田区 霞が関三丁目２番６号 東京倶楽部ビルディング Tokyo (JP).

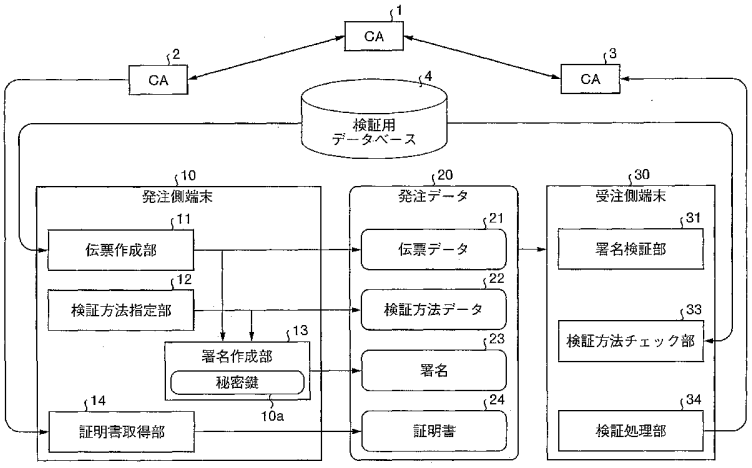
(81) 指定国 (国内): JP, US.

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: SIGNATURE RELIABILITY VERIFICATION METHOD, SIGNATURE RELIABILITY VERIFICATION PROGRAM, AND DATA COMMUNICATION SYSTEM

(54) 発明の名称: 署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システム



4...DATABASE FOR VERIFICATION
10...ORDERING SIDE TERMINAL
11...SLIP CREATION SECTION
12...VERIFICATION METHOD SPECIFICATION SECTION
13...SIGNATURE CREATION SECTION
10a...SECRET KEY
14...CERTIFICATE ACQUISITION SECTION
20...ORDERING DATA
21...SLIP DATA
22...VERIFICATION METHOD DATA
23...SIGNATURE
24...CERTIFICATE
30...ORDER RECEPTION SIDE TERMINAL
31...SIGNATURE VERIFICATION SECTION
33...VERIFICATION METHOD CHECK SECTION
34...VERIFICATION SECTION

(57) Abstract: In an ordering side terminal (10), a slip creation section (11) creates slip data (21) and a verification method specification section (12) specifies a verification method of reliability, so that verification method data (22) is created. A signature creation section (13) creates a signature (23) from the slip data (21) and the verification data (22) and a certificate acquisition section (14) acquires a certificate (24). The slip data (21), the verification method data (22), the signature (23), and the certificate (24) are transmitted as ordering data (20). In an order reception side terminal (30), a signature verification section (31) verifies the signature (23), a verification method check section (33) checks validity of the verification method indicated by the verification method data (22), and a verification section (34) verifies reliability of the certificate (24).

[続葉有]

WO 2004/100444 A1

(57) 要約: 発注側端末（１０）は、伝票作成部（１１）によって伝票データ（２１）を作成するとともに、検証方法指定部（１２）によって信頼性の検証方法を指定し、検証方法データ（２２）を作成する。署名作成部（１３）は、伝票データ（２１）および検証データ（２２）から署名（２３）を作成し、証明書取得部（１４）は証明書（２４）を取得する。これらの伝票データ（２１）、検証方法データ（２２）、署名（２３）、証明書（２４）を発注データ（２０）として送信し、受注方端末（３０）は、署名検証部３１によって署名（２３）を検証し、検証方法チェック部（３３）によって検証方法データ（２２）に示された検証方法の妥当性を確認して検証処理部（３４）によって証明書（２４）の信頼性を検証する。

明 細 書

署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システム

技術分野

この発明は、デジタル署名が施されたデータを受信し、当該データの信頼性を検証する署名信頼性検証方法および署名信頼性検証プログラム、およびデジタル署名を用いたデータ通信システムに関し、特に、送受信されるデータの信頼性を検証可能な署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システムに関する。

背景技術

近年、インターネットなどのネットワークが普及するにつれて、ネットワーク通信におけるセキュリティ技術が重要となっている。特に、商取引などをネットワーク上で実現する電子商取引では、そのデータ内容の改竄をいかに防止するかが大きな課題である。

通信データの改竄を防止するため、従来、電子署名（デジタル署名）が用いられてきた。電子署名は公開鍵暗号を利用した技術であり、送信側は自らの秘密鍵を用いて署名を作成し、受信側は送信側の公開鍵を用いて署名を復号することで、署名の作成者が送信者に間違いがないことを確かめるものである。

この時、SHA (Secure Hash Algorithm) などの技術によって、データ内容のダイジェストを作成し、デジタル署名内部に含めることで、受信側はデータ内容が改竄されていないことを確認することが出来る。

ところで、このデジタル署名では、公開鍵が信頼できることが大前提となっている。すなわち、デジタル署名は公開鍵と秘密鍵が正しい対であることを示すに過ぎないので、悪意のある者が受信側に偽の公開鍵を渡すと共に、偽の秘密鍵によって作成したデータを送信したならば、受信側は偽の公開鍵でデータを復号で

きるがために、データ内容を信頼してしまうという問題が生じる。

そこで、デジタル署名を用いる場合には、認証局（ＣＡ）に公開鍵を登録し、ＣＡからの証明書を添付することで公開鍵の正当性を証明することが一般的である。

この認証局（ＣＡ）は、それぞれが信頼関係のネットワークを構築しているので、仮に送信側が登録したＣＡと受信側が利用しているＣＡとが異なる場合であっても、ＣＡ間のネットワークによって公開鍵の証明をおこなうことができる。

しかし、このＣＡ間のネットワークを用いて公開鍵の正当性を証明する処理は、受信者側に大きな負荷がかかる。そこで、たとえば特開２００２－１３９９６号公報に公開された署名検証支援装置では、受信側に代わって送信側の公開鍵証明書の正当性を確認するようにしている。

しかしながら、このような従来のデジタル署名では、公開鍵の正当性を証明するために時間がかかるという問題点があった。近年、電子商取引の増加に伴い、処理速度の向上が求められているが、このような公開鍵の正当性証明する処理が処理遅延の原因となる。

また、個人による利用のように小口で散発的に利用するユーザでは、予め信頼しているＣＡがない場合が多く、さらに電子商取引に利用する端末自体の能力も限定されるために、電子商取引に要する時間がさらに大きくなり、ユーザの負担も大きくなるという問題点があった。

さらに、上述したようにデジタル署名は送信者を証明する手段に過ぎないため、商取引の相手として信頼に足るか否かの判断基準とはならない。特に商取引においては、データの送信元が信頼できるか否かの２値的な判断ではなく、どの程度信頼できるかが重要である。例えば、データの送信元によって取引金額の上限を幾らに設定するか、などの判断が求められる。特に数値的な信頼関係を計測できれば、将来の信頼値を予測することが可能となる。

すなわち、上述した従来のデジタル署名技術は、大規模なシステム間で頻繁にデータを送受信することが前提となっており、電子商取引の現状にそぐわないも

のであった。そのため、従来技術にかかる電子商取引では、公開鍵の認証に労力と時間とが必要となるとともに、送信元の取引相手としての信頼性を検証できないという問題点があった。

この発明は、上述した従来技術による問題点を解消するためになされたものであり、送信元の証明を簡易に実行可能で、送信元の信頼性を適切に評価可能な署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システムを提供することを目的とする。

発明の開示

上述した課題を解決し、目的を達成するため、本発明に係る署名信頼性検証方法は、デジタル署名が施されたデータを受信し、当該データの信頼性を検証する署名信頼性検証方法であって、前記受信したデータから、信頼性の検証手続きを読み出す検証手続き読み出し工程と、前記検証手続き読み出し工程によって読み出した検証手続きに従って、当該データの信頼性を検証する信頼性検証工程と、を含んだことを特徴とする。

この発明によれば、受信したデータに含まれた信頼性の検証手続きを読み出して実行することで、受信したデータの信頼性を検証することができる。

また、本発明に係る署名信頼性検証方法では、前記検証手続きは、秘密鍵によって暗号化されたデジタル署名の対象に含まれることを特徴とする。

この発明によれば、秘密鍵によって暗号化されたデジタル署名の対象に含まれた信頼性の検証手続きを読み出して実行することで、受信したデータの信頼性を検証することができる。

また、本発明に係る署名信頼性検証方法では、前記検証手続きは、信頼性の高さによって分類された複数のクラスのいずれかに対する検証手続きであることを特徴とする。

この発明によれば、信頼性の高さによって分類された複数のクラスについて、それぞれ異なる検証手続きを対応させ、データの内容によって必要な信頼性の高

さに対応する検証手続きを実行することができる。

また、本発明に係る署名信頼性検証方法は、前記検証手続き読み出し工程によって読み出した検証手続きの妥当性を確認する検証手続き確認工程をさらに含んだことを特徴とする。

この発明によれば、信頼性の検証手続き自体の妥当性を確認することで、データの信頼性をさらに正確に検証することができる。

また、本発明に係る署名信頼性検証方法は、前記受信したデータに前記信頼性検証工程による検証結果を付加して他の端末装置に送信する転送工程をさらに含めることにより、例えば信頼性９０％の検証者が付加した信頼性８０％の結果を信頼性７２％として判断できることを特徴とする。

この発明によれば、受信したデータの信頼性を検証した後、検証結果を付加して他の端末に転送することで、信頼性の検証に必要な能力を有さない端末であっても信頼性を検証したデータ通信が可能となる。

また、本発明に係る署名信頼性検証プログラムは、デジタル署名が施されたデータを受信し、当該データの信頼性を検証する署名信頼性検証方法をコンピュータに実行させる署名信頼性検証プログラムであって、前記受信したデータから、信頼性の検証手続きを読み出す検証手続き読み出し手順と、前記検証手続き読み出し手順によって読み出した検証手続きに従って、当該データの信頼性を検証する信頼性検証手順と、をコンピュータに実行させることを特徴とする。

この発明によれば、受信したデータに含まれた信頼性の検証手続きを読み出して実行させ、受信したデータの信頼性を検証することができるプログラムを実現できる。

また、本発明に係るデータ通信システムは、送信側端末が自端末の秘密鍵を用いて作成した署名を付してデータを送信し、受信側端末が送信側端末の公開鍵を用いて前記署名を復号するデータ通信ステムであって、前記送信側端末は、データ内容の信頼性を検証する検証手続きを指定する検証手続き指定手段を備え、該指定された検証手続きを前記署名対象の内部に含めて送信し、前記受信側端末は

、前記署名対象の検証手続きに従って当該データ内容の信頼性を検証することを特徴とする。

この発明によれば、送信側端末がデータ内容の信頼性を検証する検証手続きを署名対象の内部に含めて送信し、受信側端末が署名対象から取り出した検証手続きを実行することで、受信したデータの信頼性を検証することができる。

図面の簡単な説明

第１図は、データ通信システムにおけるデジタル署名の信頼性検証方法について説明する説明図であり、第２図は、検証方法の具体例について説明する説明図であり、第３図は、発注側端末の具体的な処理動作を説明するフローチャートであり、第４図は、受注側端末の処理動作を説明するフローチャートであり、第５図は、本実施の形態２にかかるデータ通信システムの概要構成を説明する説明図である。

発明を実施するための最良の形態

以下に添付図面を参照して、この発明に係る署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システムの好適な実施の形態を詳細に説明する。

（実施の形態１）

第１図は、データ通信システムにおけるデジタル署名の信頼性検証方法について説明する説明図である。同図に示すように、発注側端末１０は、受注側端末３０に発注データ２０を送信する場合に、発注者の信頼性を検証する方法を指定した検証方法データ２１を付加している。したがって、受注側端末３０は、この検証方法データ２２に示された検証方法に基づいて発注側端末１０の信頼性を検証することができる。

信頼性を検証するための方法としては任意の方法を用いることができるが、ここでは検証用データベース４に検証用のデータを保存しておくとともに、検証方

法データ２２に検証用データの保存先を指定することで、受注側端末３０が検証用データベース４から検証用のデータを読み出せるようにしている。

具体的には発注側端末１０は、その内部に伝票作成部１１、検証方法指定部１２、署名作成部１３、証明書取得部１４を有する。伝票作成部１１は、注文品目や数量、金額の情報を含む伝票データ２１を作成する処理をおこなう。また、検証方法指定部１２は、受注側端末３０が信頼性を検証する際に用いる検証方法を指定し、検証方法データ２２を作成する。

一方、署名作成部１３は、伝票作成部１１が作成した伝票データ２１および検証方法データ２３のダイジェストを作成し、ダイジェストを発注側端末１０の秘密鍵１０ａを用いて暗号化し、署名２３を作成する。このダイジェストは、ハッシュ関数などを用いてデータ内容から一意に定まるデータ列を算出したものである。ここで、ダイジェストを作成する際には、ダイジェストがデータ内容から一意に定まることに加え、ダイジェストから元のデータの推測ができないことが望ましい。このダイジェスト作成方法としてはＳＨＡなどが広く用いられている。

ところで、発注側端末１０は、認証局（ＣＡ）２を信頼しており、秘密鍵１０ａに対応する公開鍵をＣＡ２に登録している。証明書取得部１４は、このＣＡ２から公開鍵の証明書２４を受信し、発注データ２０に追加する処理をおこなう。

すなわち、発注データ２０は、伝票データ２１、検証方法データ２２、署名２３および証明書２４を有することとなる。

受注側端末３０は、署名検証部３１、検証方法チェック部３３および検証処理部３４を有している。特に、検証方法の指定により、検証処理部３４は通常の証明書検証を行ってもよい。受注側端末３０が発注データ２０を受信した場合、署名検証部３１は、発注側端末１０の公開鍵を使って署名２３を復号して伝票データ２１および検証方法データ２２における改竄の有無を確認する。

また、検証処理部３４が証明書検証を行うときには、発注データ２０から証明書２４を読み出して、認証局（ＣＡ）３に証明書の問い合わせをおこなう。ここで、受注側端末３０が信頼しているＣＡ３は、発注側端末１０が信頼しているＣ

Ａ２とは異なる。しかし、ＣＡ２およびＣＡ３は、それぞれＣＡ１を信頼することで信頼関係のネットワークを構築しているので、ＣＡ３は、ＣＡ１に問い合わせを行なってＣＡ２が信頼できると判定することができ、信頼に足るＣＡ２が発行した証明書１４を信頼することができる。

さらに検証方法チェック部３３は、検証方法データ２２によって示された検証方法が妥当なものであるか否かを判定し、検証処理部３４は、検証方法データ２２によって示された検証方法を用いて発注側端末１０の信頼性を検証する。

ここで、検証方法データ２２に示される検証方法の具体列について説明する。第２図は、検証方法の具体例について説明する説明図である。同図では、「指定されたＵＲＩ（Uniform Resource Identifier）から証明書を取り出し、取り出した証明書と署名データとを比較する」という検証方法が示されており、検証用データとして「ＵＲＩ＝‘ｈｔｔｐ：／／ｘｘｘｘ／・・・」または「ＵＲＩ＝‘ｈｔｔｐ：／／ｙｙｙｙ／・・・」を指定している。

これらのＵＲＩは、検証用データベース４上の記憶領域を指定するネットワークアドレスである。したがって、受信側端末４０は、このＵＲＩを参照して検証用データベース４から指定された検証用データを読み出すことができる。

さらに、それぞれの検証用データには、取引の上限金額が設定されている。より具体的には、「ＵＲＩ＝‘ｈｔｔｐ：／／ｘｘｘｘ／・・・」に対しては上限金額「１００万円」が設定されており、「ＵＲＩ＝‘ｈｔｔｐ：／／ｙｙｙｙ／・・・」に対しては上限金額「５０００円」が設定されている。このように、検証用データごとにそれぞれ異なる上限金額を割り当てることで、取引の金額に応じて異なる検証を行うことができる。

したがって、低額の商取引用の検証用データを用いて取引相手を信頼したとしても、高額の取引を許可したことにならず、低額取引時に構築した信頼関係を悪用されて高額な損害が発生するという被害を防ぐことができる。

換言するならば、本発明にかかる通信システムでは、データの送信元が信頼できるか否かの２値的な判断ではなく、どの程度信頼できるかを取引金額の上限と

して判断することが可能となる。

つぎに、検証方法自体の妥当性の確認について説明する。検証方法の妥当性を確認するためには、たとえば過去の取引実績を証明すればよい。具体的には、過去の取引実績から成立した取引金額の最大値や、成立しなかった取引金額の最小値を求めることができる。そこで、これらの金額から、その取引相手と取引可能な金額を判定することが可能である。また、複数の保険などのサービスにその信頼性について金額の算出を依頼し、金額の平均やメジャーを算出しても良い。この保険などのサービスを用いる場合、インターネットなどのネットワーク上で依頼可能なサービスを利用したならば、検証方法の妥当性の確認と検証方法の実行を全てネットワーク上で実現可能である。

このように、検査方法の妥当性を確認可能とすることで、ＣＡからの証明書に依存することなく取引相手の信頼性を検証することが可能となる。すなわち、本発明にかかる信用性の検証では、取引相手の簡易的な証明を行うこととなり、ＣＡからの証明書を確認することが困難である場合や、証明書の確認までに要する時間が長すぎる場合などに、この簡易かつ高速な信用性の検証によってＣＡからの証明書に代えることができる。

特に低額取引などの場合のように、厳密に証明書を確認する事よりも高速にある程度の信頼性を確保する事が優先される場合や、受信側の端末に予め信頼しているＣＡが無い・証明書の確認に必要な能力が無い場合などに有用である。

さらに、ＣＡからの証明書が送信者を証明する手段に過ぎないのに対し、この信用性の検証は、商取引の相手として信頼に足るか否かの判断基準として利用することが可能である。特に、同一の公開鍵や署名であっても、異なる検証法を指定することによって取引金額に対応した信用性を確認することができる。

つぎに、発注側端末１０の具体的な処理動作について説明する。第３図は、発注側端末１０の具体的な処理動作を説明するフローチャートである。同図に示すように、発注側端末１０が発注データ２０を作成する場合、まず、伝票作成部１１によって伝票データ２１を作成する（ステップＳ１０１）。つぎに、検証方法

指定部１２が、検証方法を指定して検証方法データ２２を作成する（ステップＳ１０２）。

その後、署名作成部１３は，伝票データ２１および検証方法データ２２のダイジェストをＳＨＡによって作成し、秘密鍵１０ａで暗号化して署名２３を作成する（ステップＳ１０３）。つづいて、証明書作成部１４は、秘密鍵１０ａに対応する公開鍵の証明書２４をＣＡ２から取得する（ステップＳ１０４）。

その後、検証方法指定部１２は、自らが指定した検証処理を実行し（ステップＳ１０５）、所望の信頼性が得られるか否かを検証する。このように、発注データ２０の送信前に検証処理を実行しておくことで、受注側端末３０における検証の結果として得られる信頼性の値を確認し、商取引に必要な信頼性が得られるか、また、必要以上の信頼性を付与していないかを確かめることができる。なお、ステップＳ１０５による事前の検証処理は、必要に応じて省略してもよい。

ステップＳ１０５の結果、所望の信頼性が得られなかった場合（ステップＳ１０６，Ｎｏ）、検証方法指定部１２は、検証方法を指定しなおす（ステップＳ１０２）。

一方、ステップＳ１０５の結果、所望の信頼性が得られたならば（ステップＳ１０６，Ｙｅｓ）、発注側端末１０は、伝票データ２１、検証方法データ２２、署名２３および証明書２４を発注データ２０として受注側端末３０に送信する。

つぎに、受注側端末３０の具体的な処理動作について説明する。第４図は、受注側端末３０の処理動作を説明するフローチャートである。同図に示すように、受注側端末３０は、発注データ２０を受信したならば（ステップＳ１０１）、署名検証部３１が発注データ２０の署名２３を読み出し、発注側端末１０の公開鍵を用いて書名を復号し、署名２３を検証する。この署名の検証は、具体的には、発注データ２０に含まれていた伝票データ２１および検証方法データ２２のダイジェストをＳＨＡによって作成し、署名２３に含まれていたダイジェスト、すなわち発注側端末１０で作成されたダイジェストと比較する処理である。

ＳＨＡによるダイジェストの作成では、元のデータが同一であれば出力されるダ

イジェストも同一となる。一方、仮に伝票データ２１や検証方法データ２２が通信経路上で改竄されたならば、発注側端末１０で作成したダイジェストと受注側端末３０で作成したダイジェストとは異なる値になる。つまり、受注側端末１０で作成したダイジェストが、発注側端末１０で作成したダイジェストと異なったならば、そのデータは改竄されていると考えることができる。

署名検証部３１は、このダイジェストの比較を行い、署名が検証できなかった、すなわちダイジェストが一致しないならば（ステップＳ２０３，Ｎｏ）、データの改竄を検出したことを示す署名エラーを出力し（ステップＳ２０４）、処理を終了する。

一方、署名が検証できた、すなわちダイジェストが一致したならば（ステップＳ２０３，Ｙｅｓ）、つぎに、検証処理部３４が証明書検証を行う場合はＣＡの証明書を検証する（ステップＳ２０５）。具体的には、このＣＡの証明書の検証処理では、受信した証明書２４をＣＡの公開鍵を用いて検証することで、証明書２４が本当にＣＡによって発行されたものであることを確かめる。確かめる方法としては、検証方法に記述して、通常のように検証サーバに問い合わせるなどの方法を用いることができる。

検証方法データ２２に示された検証方法で、取引に必要な信頼性が検証できなかった場合（ステップＳ２０６，Ｎｏ）、検証処理部３４は、検証エラーを出力し（ステップＳ２０７）、処理を終了する。

検証方法データ２２に示された検証方法で、取引に必要な信頼性が検証できた場合（ステップＳ２０６，Ｙｅｓ）、つぎに、検証方法チェック部３３が検証方法の妥当性を検証する（ステップＳ２０８）。

このステップＳ２０８によって検証方法の妥当性が検証できなかったならば（ステップＳ２０９，Ｎｏ）、検証方法チェック部３３は、妥当性エラーを出力し（ステップＳ２１０）、処理を終了する。

一方、ステップＳ２０８によって検証方法の妥当性が検証できたならば（ステップＳ２０９，Ｙｅｓ）、全ての検証を完了して（ステップＳ２１１）、処理を

終了する。

このように、署名２３および証明書２４の検証をおこなうとともに、発注側端末１０によって指定された検証方法を用いて信頼性の検証処理を行い、さらに検証方法自体の妥当性を評価することによって、発注側端末の取引相手としての信頼性を検証することができる。

なお、署名の検証、証明書などの信頼性の検証および検証方法の妥当性の評価は、必ずしも第４図に示した順序で行う必要はなく、必要に応じて処理順序を変更することができる。

また、既に説明したように、信頼性の検証は証明書の検証を含むことができるので、証明書の検証に代えることができる。

上述してきたように、本実施の形態１にかかるデータ通信システムでは、発注側端末１０が指定した検証方法によって発注側端末１０の信頼性を検証するので、発注側端末および送受信されたデータの信頼性をＣＡに依存することなく簡易に検証し、さらに発注側端末１０の取引相手としての信頼性を適切に評価することができる。

なお、上述した実施の形態１においては検証方法データ２２全体を発注データ２０に含ませるとともに、そのダイジェストを作成して署名２３に含ませることとしているが、検証方法データ２２のダイジェストを作成して署名２２に含ませて署名対象とするのではなく、検証方法データ２２全体を署名２２に含ませるようにしても良い。

（実施の形態２）

ところで、上記実施の形態１では、発注側端末が送信した発注データの信頼性を受注側端末が検証することとしているが、本発明に構成は必ずしもこれに限定されるものでなく、例えば発注側端末と受注側端末との間に介在するサーバにおいて発注側端末の信頼性を検証し、検証結果を受信側端末に送信することとしてもよい。本実施の形態２では、第５図を参照して通信の途中に介在するサーバ上で信頼性の検証をおこなうデータ通信システムについて説明する。

第５図は、本実施の形態２にかかるデータ通信システムの概要構成を説明する説明図である。同図に示すように発注側端末１０と受注側端末７０との通信は、受注側サーバ５０を介して行われる。

受注側サーバ５０は、発注データ２０を受信した場合に、実施の形態１に示した受注側端末３０と同様に、発注側端末１０の信頼性を検証した後、転送処理部５１によって発注データ６０を作成して受注側端末７０に送信する。したがって、受注側端末７０は、信頼性の検証が既に終了した発注データ６０を受信することとなる。

なお、その他の構成および動作は実施の形態１に示したデータ通信システムと同様であるので、同一の構成要素には同一の符号を付して説明を省略する。

受注側サーバ５０の具体的な処理動作は、第４図に示した実施の形態１における受注側端末３０の処理と略同一である。違いとしては、発注データ２０の検証が終了した後に，転送処理部５０が発注データ６０を作成して受信側端末７０に送信する点である。

この発注データ６０は、既に各種の検証が終了しているので、その内部に伝票データ２１と検証結果６１とを有する。受注側端末７０は、この検証結果６１を信頼度１００％のサーバで検証してもらうことにより、自端末で検証処理を行うことなく信頼度数値を取得することができる。

したがって、この実施の形態２に示したデータ通信システムでは、例えば受信側端末７０が携帯電話やＰＤＡ（携帯情報端末）などの処理能力が限定された端末であっても発注側端末および送受信されたデータの信頼性をＣＡに依存することなく簡易に検証し、さらに発注側端末１０の取引相手としての信頼性を適切に評価することができる。

なお、上述した実施の形態１および実施の形態２では、電子商取引を行う場合の発注側端末と受注側端末について説明したが、本発明の利用はこれに限定されるものではなく、データ通信において信頼性の確認をおこなう場合に広く適用することができる。

また、実施の形態１および実施の形態２で説明した署名検証方法は、あらかじめ用意されたプログラムをコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

産業上の利用可能性

以上のように、本発明にかかる署名信頼性検証方法、署名信頼性検証プログラムおよびデータ通信システムは、送信元の証明簡易化および高速化、さらに送信元の信頼性の評価に対して有用である。

請 求 の 範 囲

1． デジタル署名が施されたデータを受信し、当該データの信頼性を検証する署名信頼性検証方法であって、

前記受信したデータから、信頼性の検証手続きを読み出す検証手続き読み出し工程と、

前記検証手続き読み出し工程によって読み出した検証手続きに従って、当該データの信頼性を検証する信頼性検証工程と、

を含んだことを特徴とする署名信頼性検証方法。

2． 前記検証手続きは、秘密鍵によって暗号化されたデジタル署名の中に含まれることを特徴とする請求の範囲第１項に記載の署名信頼性検証方法。

3． 前記検証手続きは、信頼性の高さによって分類された複数のクラスのいずれかに対する検証手続きであることを特徴とする請求の範囲第１項または第２項に記載の署名信頼性検証方法。

4． 前記検証手続き読み出し工程によって読み出した検証手続きの妥当性を確認する検証手続き確認工程をさらに含んだことを特徴とする請求の範囲第１項、第２項または第３項に記載の署名信頼性検証方法。

5． 前記受信したデータに前記信頼性検証工程による検証結果を付加して他の端末装置に送信する転送工程をさらに含んだことを特徴とする署名信頼性検証方法。

6． デジタル署名が施されたデータを受信し、当該データの信頼性を検証する署名信頼性検証方法をコンピュータに実行させる署名信頼性検証プログラムであ

って、

前記受信したデータから、信頼性の検証手続きを読み出す検証手続き読み出し手順と、

前記検証手続き読み出し手順によって読み出した検証手続きに従って、当該データの信頼性を検証する信頼性検証手順と、

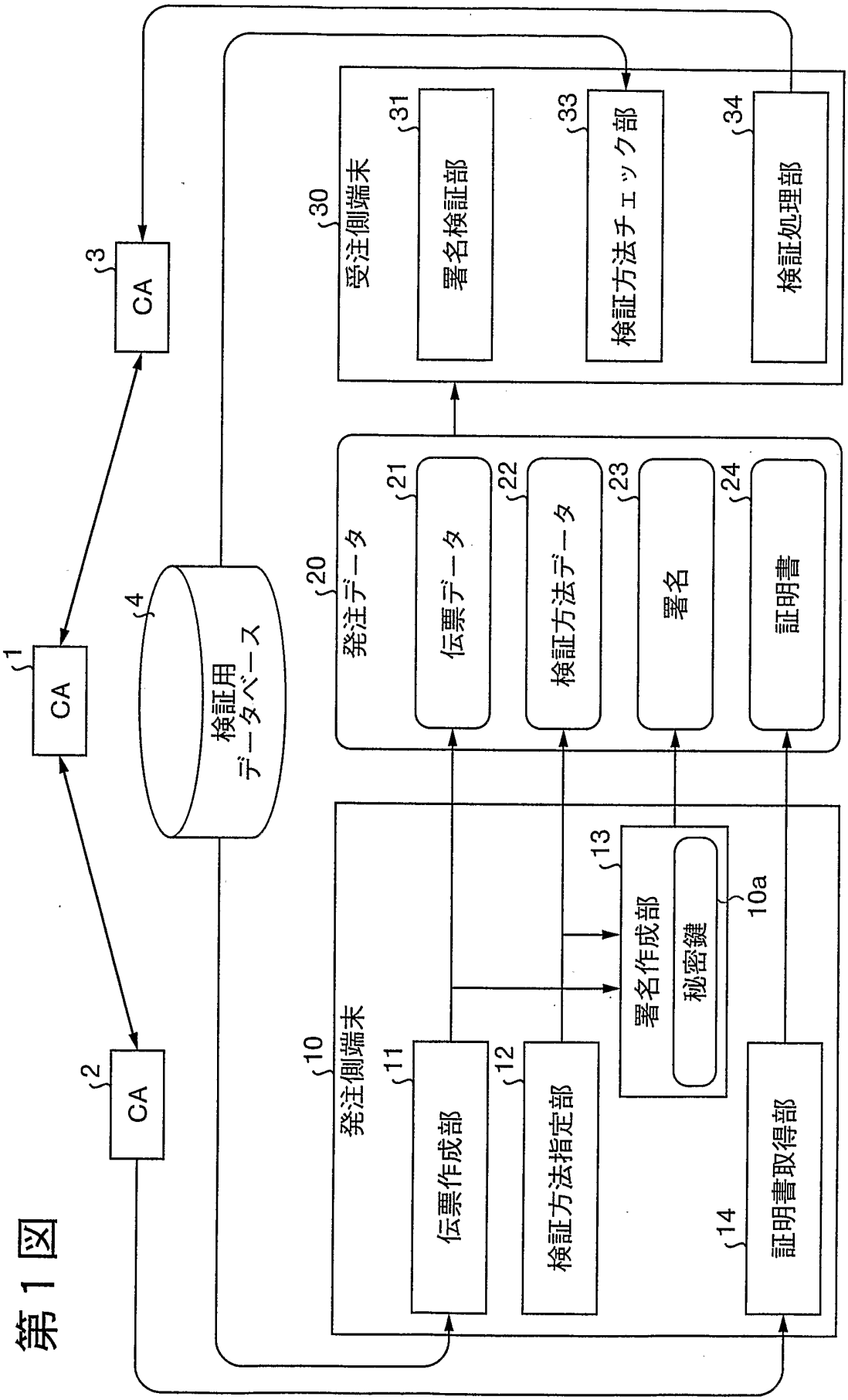
をコンピュータに実行させることを特徴とする署名信頼性検証プログラム。

7． 送信側端末が自端末の秘密鍵を用いて作成した署名を付してデータを送信し、受信側端末が送信側端末の公開鍵を用いて前記署名を復号するデータ通信システムであって、

前記送信側端末は、データ内容の信頼性を検証する検証手続きを指定する検証手続き指定手段を備え、該指定された検証手続きを前記署名の内部に含めて送信し、

前記受信側端末は、前記署名の対象から取り出した検証手続きに従って当該データ内容の信頼性を検証することを特徴とするデータ通信システム。

第１図

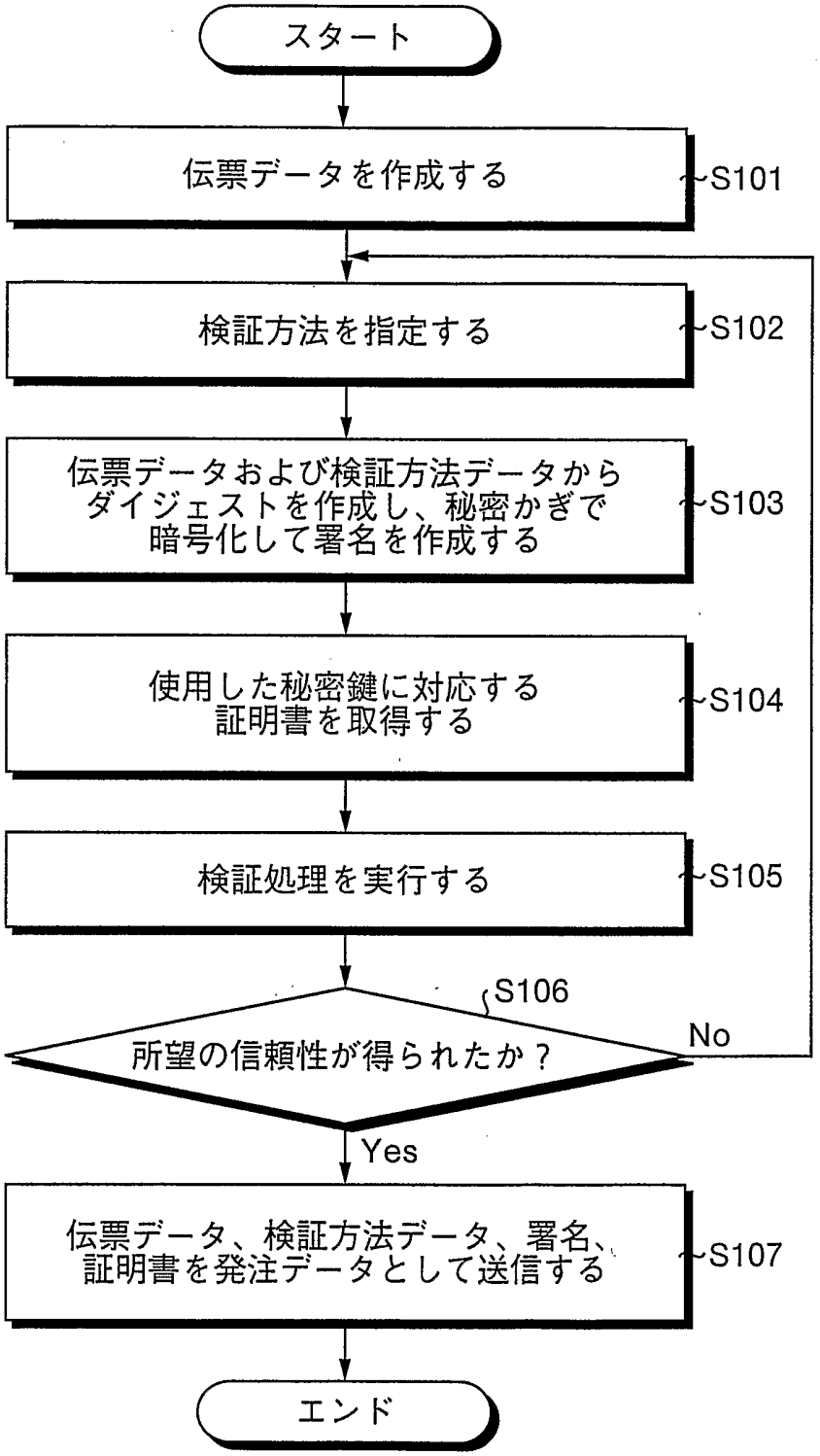

CA
1
CA
2
CA
3
検証用
データベース
4
発注側端末
10
伝票作成部
11
検証方法指定部
12
署名作成部
13
秘密鍵
10a
証明書取得部
14
発注データ
20
伝票データ
21
検証方法データ
22
署名
23
証明書
24
受注側端末
30
署名検証部
31
検証方法チェック部
33
検証処理部
34

第２図

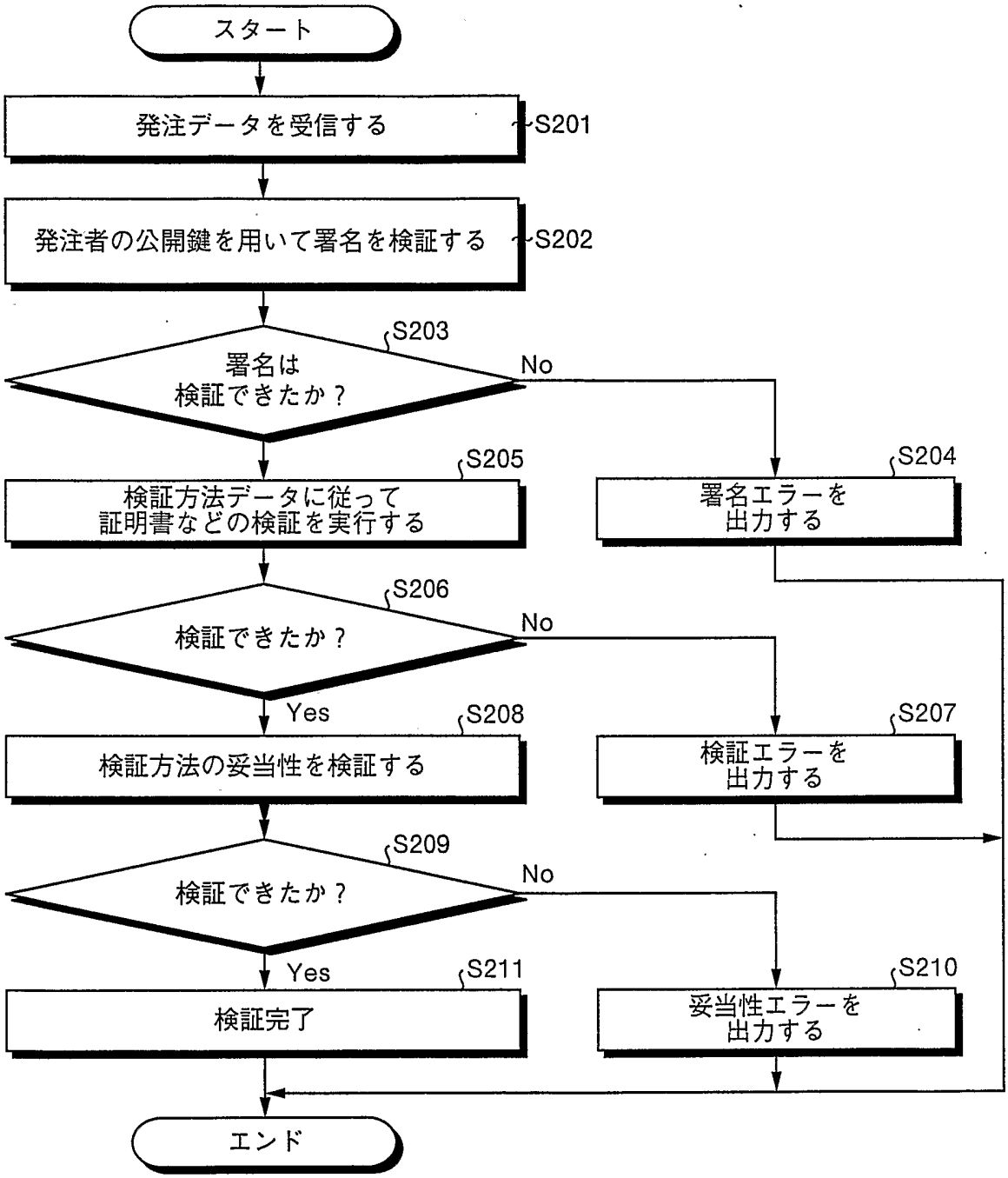
40

検証方法	検証用データ	上限金額
指定されたURIから証明書を取り出し、署名データを比較する	URI='http://xxxx/'	100万円
指定されたURIから証明書を取り出し、署名データを比較する	URI='http://yyyy/'	5000円
・ ・ ・	・ ・ ・	・ ・ ・

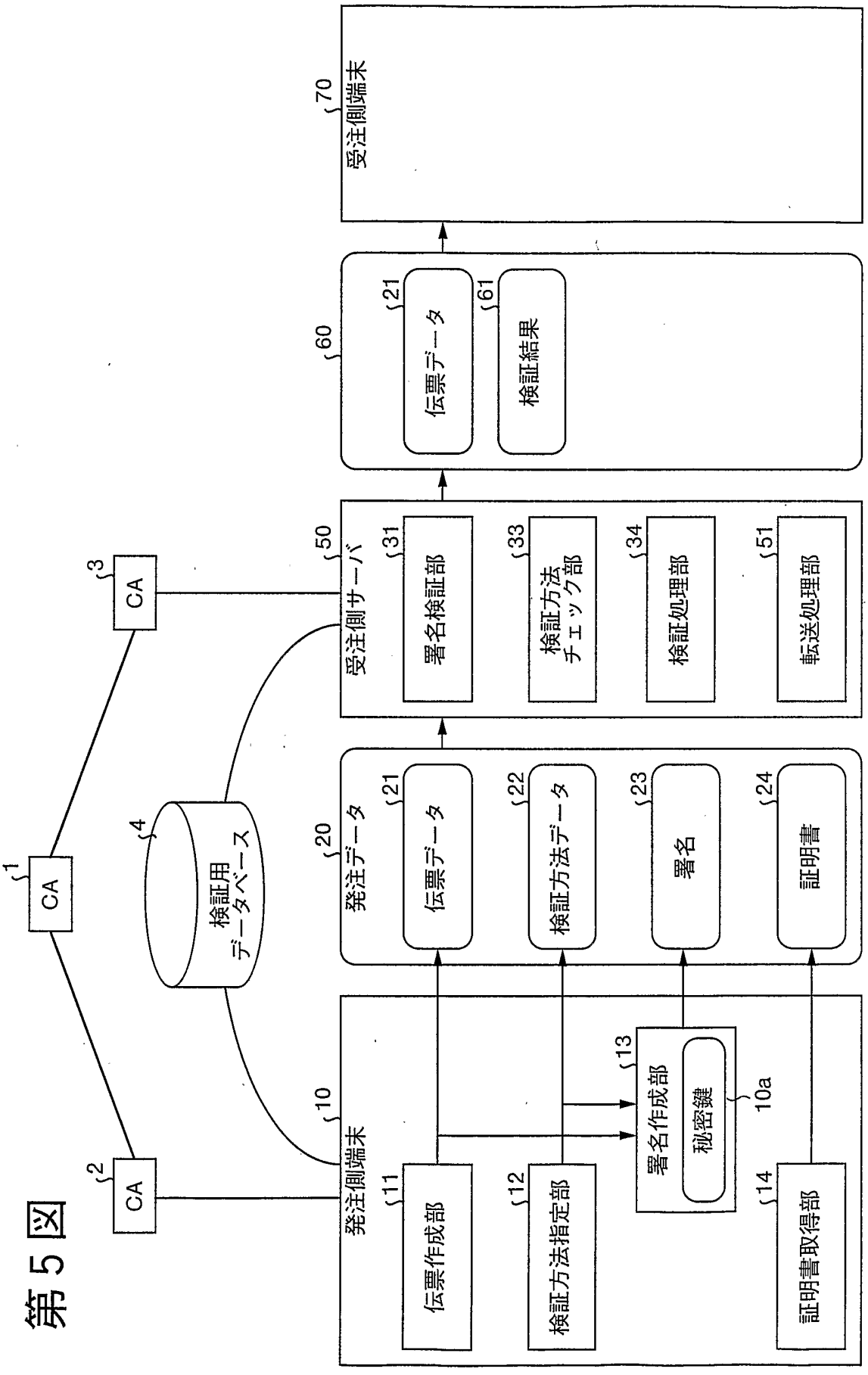
第３図


スタート
伝票データを作成する
S101
検証方法を指定する
S102
伝票データおよび検証方法データから
ダイジェストを作成し、秘密かぎで
暗号化して署名を作成する
S103
使用した秘密鍵に対応する
証明書を取得する
S104
検証処理を実行する
S105
S106
所望の信頼性が得られたか？
No
Yes
伝票データ、検証方法データ、署名、
証明書を発注データとして送信する
S107
エンド

第4図


スタート
発注データを受信する
S201
発注者の公開鍵を用いて署名を検証する
S202
S203
署名は
検証できたか？
No
S204
署名エラーを
出力する
S205
検証方法データに従って
証明書などの検証を実行する
S206
検証できたか？
No
Yes
S207
検証エラーを
出力する
S208
検証方法の妥当性を検証する
S209
検証できたか？
No
Yes
S210
妥当性エラーを
出力する
S211
検証完了
エンド

第5図


CA
1
CA
2
CA
3
検証用
データベース
4
発注側端末
10
伝票作成部
11
検証方法指定部
12
署名作成部
13
秘密鍵
10a
証明書取得部
14
発注データ
20
伝票データ
21
検証方法データ
22
署名
23
証明書
24
受注側サーバ
50
署名検証部
31
検証方法
チェック部
33
検証処理部
34
転送処理部
51
60
伝票データ
21
検証結果
61
受注側端末
70

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/05831

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-208960 A (Fuji Xerox Co., Ltd.), 26 July, 2002 (26.07.02), Fig. 2 (Family: none)	1,2,6,7 3,4,5
X Y	JP 2001-69137 A (Nippon Telegraph And Telephone Corp.), 16 March, 2001 (16.03.01), Fig. 4 (Family: none)	1,2,6,7 3,4,5
X	JP 11-175512 A (Hitachi, Ltd.), 02 July, 1999 (02.07.99), Fig. 3 (Family: none)	1,6,7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 July, 2003 (29.07.03)	12 August, 2003 (12.08.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/05831

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-331088 A (Mitsubishi Electric Corp.), 30 November, 2000 (30.11.00), Fig. 2 (Family: none)	1,2,6,7
Y	JP 2002-351966 A (Hitachi, Ltd.), 06 December, 2002 (06.12.02), Figs. 4 to 8 (Family: none)	3
Y	JP 2000-227755 A (Pitney Bowes Inc.), 15 August, 2000 (15.08.00), Fig. 3 & EP 1022685 A	3
Y	JP 2000-122973 A (Fujitsu Ltd.), 28 April, 2000 (28.04.00), Fig. 1 (Family: none)	4
Y	JP 2001-521329 A (Signa Works Corp.), 06 November, 2001 (06.11.01), Fig. 1 & US 6026166 A	5
A	JP 10-313308 A (KDD Kabushiki Kaisha), 24 November, 1998 (24.11.98), Fig. 4 (Family: none)	1-7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０５８３１

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ ９／３２ ，　Ｇ０９Ｃ １／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ ９／３２ ，　Ｇ０９Ｃ １／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ ２００２－２０８９６０ Ａ（富士ゼロックス株式会社）２００２．０７．２６，第２図（ファミリーなし）	１，２，６，７
Y		３，４，５
X	ＪＰ ２００１－６９１３７ Ａ（日本電信電話株式会社）２００１．０３．１６，第４図（ファミリーなし）	１，２，６，７
Y		３，４，５

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　２９．０７．０３	国際調査報告の発送日　12.08.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 石田 信行　５Ｍ　９４６９ 電話番号　０３－３５８１－１１０１　内線　３５９８

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ １１－１７５５１２ Ａ（株式会社日立製作所） １９９９．０７．０２，第３図（ファミリーなし）	１，６，７
Ｘ	ＪＰ ２０００－３３１０８８ Ａ（三菱電機株式会社） ２０００．１１．３０，第２図（ファミリーなし）	１，２，６，７
Ｙ	ＪＰ ２００２－３５１９６６ Ａ（株式会社日立製作所） ２００２．１２．０６，第４－８図（ファミリーなし）	３
Ｙ	ＪＰ ２０００－２２７７５５ Ａ （ピットニイ ボウズ インコーポレーテッド） ２０００．０８．１５，第３図 ＆ ＥＰ １０２２６８５ Ａ	３
Ｙ	ＪＰ ２０００－１２２９７３ Ａ（富士通株式会社） ２０００．０４．２８，第１図（ファミリーなし）	４
Ｙ	ＪＰ ２００１－５２１３２９ Ａ （シグナワークス コーポレーション） ２００１．１１．０６，第１図 ＆ ＵＳ ６０２６１６６ Ａ	５
Ａ	ＪＰ １０－３１３３０８ Ａ（日本電信電話株式会社） １９９８．１１．２４，第４図（ファミリーなし）	１－７