(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3673688号
(P3673688)
(45)発行日　平成17年7月20日(2005.7.20)　(24)登録日　平成17年4月28日(2005.4.28)

(51)Int.Cl.[7]　F I
G09C 1/00　G09C 1/00 640B
H04L 9/32　G09C 1/00 620Z
H04L 9/00 675B

請求項の数 12　(全 18 頁)

(21)出願番号　特願2000-35457(P2000-35457)
(22)出願日　平成12年2月14日(2000.2.14)
(62)分割の表示　特願平2-8366の分割
原出願日　平成2年1月19日(1990.1.19)
(65)公開番号　特開2000-206877(P2000-206877A)
(43)公開日　平成12年7月28日(2000.7.28)
審査請求日　平成12年2月14日(2000.2.14)
審判番号　不服2001-17646(P2001-17646/J1)
審判請求日　平成13年10月3日(2001.10.3)

(73)特許権者　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　中村　憲司
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】情報通信方法及び情報通信システム並びに情報提供装置、情報要求装置及び制御方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して情報を提供する情報提供装置と、前記情報の提供を要求する情報要求装置とを有する情報通信システムにおける情報通信方法であって、
前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信するステップと、
前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認するステップと、
前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信するステップと、
前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認するステップと、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信するステップとを有する情報通信方法。
【請求項２】
ネットワークを介して情報を提供する情報提供装置と、前記情報の提供を要求する情報要求装置とを有する情報通信システムであって、
前記情報要求装置は、

前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信する第２送信手段と、
デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認する第２確認手段とを有する装置であり、
前記情報提供装置は、
前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認する第１確認手段と、
前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化された前記デイジタル署名付き鍵を前記情報要求装置に送信する第１送信手段とを有し、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信する装置であることを特徴とする情報通信システム。

【請求項３】
ネツトワークを介して情報を提供する情報提供装置であって、
前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を情報要求装置から受信する手段と、
前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認する手段と、
前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信する手段とを有し、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信することを特徴とする情報提供装置。

【請求項４】
ネツトワークを介して情報を提供する情報提供装置に前記情報の提供を要求する情報要求装置であって、
前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信する手段と、
前記情報提供装置において前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報提供装置から受信する手段と、
前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認する手段とを有し、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報提供装置で暗号化された前記情報を受信することを特徴とする情報要求装置。

【請求項５】
ネツトワークを介して情報を提供する情報提供装置で実行される制御方法であって、
前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を情報要求装置から受信するステップと、
前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認するステップと、
前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信するステップと、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信するステップとを有することを特徴とする制御方法。

【請求項６】
ネットワークを介して情報を提供する情報提供装置に前記情報の提供を要求する情報要求装置で実行される制御方法であって、
前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信するステップと、
前記情報提供装置において前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報提供装置から受信するステップと、
前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認するステップと、
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報提供装置で暗号化された前記情報を受信するステップとを有することを特徴とする制御方法。
【請求項７】
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置が前記情報を送信する前に、前記情報を受信するための準備が完了したことを前記情報提供装置に通知することを特徴とする請求項１に記載の情報通信方法。
【請求項８】
前記情報要求装置は、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置が前記情報を送信する前に、前記情報を受信するための準備が完了したことを前記情報提供装置に通知することを特徴とする請求項２に記載の情報通信システム。
【請求項９】
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置から前記情報を受信する前に、前記情報を受信するための準備が完了したことを示す通知を受け取ることを特徴とする請求項３に記載の情報提供装置。
【請求項１０】
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置が前記情報を送信する前に、前記情報を受信するための準備が完了したことを前記情報提供装置に通知することを特徴とする請求項４に記載の情報要求装置。
【請求項１１】
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置から前記情報を受信する前に、前記情報を受信するための準備が完了したことを示す通知を受け取るステップをさらに有することを特徴とする請求項５に記載の制御方法。
【請求項１２】
前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後であって、前記情報提供装置が前記情報を送信する前に、前記情報を受信するための準備が完了したことを前記情報提供装置に通知するステップをさらに有することを特徴とする請求項６に記載の制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報通信方法及び情報通信システムに関し、特にネットワークを介して提供される情報を管理する技術に関するものである。
【０００２】
【従来の技術】

近年、幹線通信網における光ファイバーネツトワークの整備、衛星通信の実用化、ローカルエリアネツトワーク（ＬＡＮ）の普及等に伴い、通信の当時者以外の第３者に通信内容を知られないようにするための、暗号化・秘話化を達成したネツトワークシステムの構築が重要となつてきている。

【０００３】

また、このような通信網を介して提供した情報の内容及び量に応じて料金を徴集するいわゆる情報サービス産業が増大している。このため、これらのサービスに対しては上記暗号化・秘話化のほかに、提供した情報に対する課金の情報を同時に記録・採集することも重要となつている。

【０００４】

従来、このような通信における情報の暗号化・秘話化の方式としては、共通鍵暗号化方式と呼ばれる方式と、公開鍵暗号化方式と呼ばれる方式が知られている。

【０００５】

これらの詳細についてはD.W.Davies, W.L.Pric著、上園忠弘監訳、“ネツトワークセキユリテイ”、日経マグロウヒル社刊（昭和６０年）等に詳しく説明されている。

【０００６】

詳細は上述の文献に譲るが、これらの方式を以下にごく簡単に説明する。

【０００７】

共通鍵暗号化方式は、送信端末と受信端末の間で暗号化・復号化の鍵を共有し、この鍵により情報を暗号化・伝送及び復号化するものである。

【０００８】

この暗号化の方式としては、単純な和暗号・転置暗号から米国商務省によつて標準化されているＤＥＳと呼ばれる暗号化まで数多くの方式が知られている。

【０００９】

共通鍵方式においては、暗号化・復号化のための鍵を予め送信端末及び受信端末の間で決めなければならず、また、この鍵が第３者に知られないようにしなければならない。これは、この鍵を第３者が知つた場合には容易に暗号化された情報を解読できるからである。

【００１０】

これに対して公開鍵暗号化方式は、対となる暗号化鍵と復号化鍵に異なるものを用い、暗号化鍵は全端末に対して公開する方式である。

【００１１】

各端末は自端末に固有の復号化鍵を保有する。そして、送信端末は公開された各端末の暗号化鍵から送信先の鍵を選び出し、この鍵により情報を暗号化して伝送する。一方、受信端末はこの鍵と対になつた復号化鍵により情報を復号化する。

【００１２】

このように、暗号化鍵から復号化鍵を割り出せないような鍵の対を用いるので、暗号化鍵が公開されていても、第３者に暗号化された情報が解読されることはない方式である。

【００１３】

また、送・受信端末間で予め鍵を決める必要がないので、送・受信端末間で予め鍵を決める時に鍵が第３者に知られてしまう可能性もない。

【００１４】

【発明が解決しようとする課題】

しかしながら、上記従来例では、次のような欠点があつた。

【００１５】

共通鍵暗号化方式においては、

（１）上述のように暗号化・復号化の鍵を予め送信端末と受信端末の間で決めなくてはならず、この暗号化・復号化の鍵を取り決めるための通信により鍵が第３者に知られる危険性がある。

（２）上記の危険を回避するために、同一の鍵を繰り返し何度も用いる様に制御しても、同一の鍵によつて暗号化された複数の情報を比較することにより、やはり第３者に鍵を見

破られる可能性がある。
（３）ＤＥＳのような複雑な暗号化を行えばこのような可能性は低くなるが、高速な暗号化・復号化が困難になり、デイジタル化された映像信号等の時間当りのデータ転送量の多いデータの暗号化ができなくなる。
【００１６】
また公開鍵暗号化方式においては、
（４）高速な暗号化・復号化処理が一般に困難である。
【００１７】
以上の両暗号化方式においては、上述した（１）～（４）に挙げた各欠点を有していることにより、従来は特に映像信号のような高速な伝送を必要とする即時通信型情報を、安全に暗号化して伝送することが困難であつた。
【００１８】
【課題を解決するための手段】
本発明は上述の課題を解決することを目的として成されたもので、上述の課題を解決する一手段として以下の構成を備える。
【００１９】
即ち、本発明の情報通信方法は、ネツトワークを介して情報を提供する情報提供装置と、前記情報の提供を要求する情報要求装置とを有する情報通信システムにおける情報通信方法であって、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信するステップと、前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認するステップと、前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信するステップと、前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認するステップと、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信するステップとを有する。
また、本発明の情報通信システムは、ネツトワークを介して情報を提供する情報提供装置と、前記情報の提供を要求する情報要求装置とを有する情報通信システムであって、前記情報要求装置は、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信する第２送信手段と、デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認する第２確認手段とを有する装置であり、前記情報提供装置は、前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認する第１確認手段と、前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化された前記デイジタル署名付き鍵を前記情報要求装置に送信する第１送信手段とを有し、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信する装置であることを特徴とする。
また、本発明の情報提供装置は、ネツトワークを介して情報を提供する情報提供装置であって、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を情報要求装置から受信する手段と、前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認する手段と、前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信する手段とを有し、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信することを特徴とする。

また、本発明の情報要求装置は、ネツトワークを介して情報を提供する情報提供装置に前記情報の提供を要求する情報要求装置であって、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信する手段と、前記情報提供装置において前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報提供装置から受信する手段と、前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認する手段とを有し、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報提供装置で暗号化された前記情報を受信することを特徴とする。

また、本発明の制御方法は、ネツトワークを介して情報を提供する情報提供装置で実行される制御方法であって、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を情報要求装置から受信するステップと、前記デイジタル署名付き要求情報を公開鍵暗号方式によって復号化した後、前記要求情報のデイジタル署名を確認するステップと、前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報要求装置に送信するステップと、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報を暗号化して前記情報要求装置に送信するステップとを有することを特徴とする。

また、本発明の制御方法は、ネツトワークを介して情報を提供する情報提供装置に前記情報の提供を要求する情報要求装置で実行される制御方法であって、前記情報の提供を要求する要求情報から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き要求情報を前記情報提供装置に送信するステップと、前記情報提供装置において前記要求情報のデイジタル署名が確認された後、前記情報を復号化するための鍵から生成され、公開鍵暗号方式によって暗号化されたデイジタル署名付き鍵を前記情報提供装置から受信するステップと、前記デイジタル署名付き鍵を公開鍵暗号方式によって復号化した後、前記鍵のデイジタル署名を確認するステップと、前記情報提供装置において前記要求情報のデイジタル署名が確認され、前記情報要求装置において前記鍵のデイジタル署名が確認された後、前記情報提供装置で暗号化された前記情報を受信するステップとを有することを特徴とする。

【００２９】

【発明の実施の形態】

以下、図面を参照して本発明に係る一実施の形態例を詳細に説明する。

【００３０】

［第１の実施の形態例］

以下まず図１乃至図４を参照して本発明に係る第１の実施の形態例を説明する。

【００３１】

図１は本発明に係る第１の実施の形態例のブロツク構成図、図２は本実施の形態例が適用されるマルチメデイアネツトワークシステムの概要の一例を示す図、図３は本実施の形態例の概略動作を示すフローチヤート、図４は図１において公開鍵による暗号化を行う部位の機能を示す図、図５は図１においてデイジタル署名を行う部位の機能を示す図である。

【００３２】

図１において、１は即時通信型情報を暗号化して伝送する第１の端末、２は暗号化された即時通信型情報を受信して復号化する第２の端末、３は伝送路である。

【００３３】

第１の端末１において、１０１は送信端末１におけるコンピユータフアイル、電子伝票等の蓄積型情報を記憶するための磁気記憶装置、１０２は蓄積型情報を送信する時に該情報が確かに第１の端末１から送信されたものであり、第３者により偽造されたものではないことを認証するためのデイジタル署名を行うデイジタル署名部、１０３は情報の宛先であ

る第２の端末２に特有の公開された暗号化鍵を用いて蓄積型情報を暗号化する公開鍵暗号化部、１０４は第１の端末１に特有の公開された暗号化鍵を用いて暗号化され送信されてきた蓄積型情報を、該端末１に特有の秘密の復号化鍵を用いて復号化する公開鍵復号化部、１０５はこの公開鍵復号化部１０４で復号化された蓄積型情報が、確かに第２の端末２からのものであり、第３者に偽造されたものではないことを認証するためのデイジタル署名を確認する署名確認部、１０６はＴＶカメラ１０６ａ、ＶＴＲ１０６ｂ等のデイジタル即時通信型情報を発生する即時通信型情報発生装置、１０７は第１の端末１と第２の端末２の間の通信に必要な同期をとるための同期信号発生部、１０８は即時通信型情報発生装置１０６よりの即時通信型情報からクロツク信号を抽出するクロツク抽出部、１０９は磁気記憶装置１０１より与えられたデータ鍵と一対一に対応しクロツク抽出装置１０８からのクロツク信号に同期した疑似乱数系列を発生する疑似乱数発生部、１１０は即時通信型情報発生装置１０６からの情報と疑似乱数発生部１０９からの疑似乱数との排他的論理和をとる排他的論理和ゲート、１１１は疑似乱数発生部１０９の動作状態を測定し、伝送される情報に対して支払われるべき対価に関する情報をとるための課金情報採集部、１１２は公開鍵暗号化部１０３からの情報や排他的論理和ゲート１１０からの信号を伝送路３に送信するとともに、伝送路３からの信号を受信して公開鍵復号化部１０４に出力するための通信インターフエースである。

【００３４】

第２の端末２において、２０１～２０５及び２１２は、それぞれ、第１の端末の１０１～１０５及び１１２と同様の磁気記憶装置、デイジタル署名部、公開鍵暗号化部、公開鍵復号化部、署名確認部、および通信インターフエースである。また、２０６は即時通信型情報に対し表示、記憶、処理等を行うための、ＣＲＴ２０６ａ、ＶＴＲ２０６ｂ、磁気記憶装置２０６ｃ等より成る即時通信型情報処理装置、２０７は同期信号発生部１０７で発生された同期信号を伝送路３に伝達されてきた信号の中から抽出する同期信号抽出部、２０８は伝送されてきた信号の中からクロツク成分を抽出する受信クロツク抽出部、２０９は即時通信型情報の送信側装置である第１の端末１の疑似乱数発生部１０９と同一の鍵を与えられた時に、同一の疑似乱数を発生する疑似乱数発生部、２１０は通信インターフエース２１２からの受信情報と疑似乱数発生部２０９からの疑似乱数との排他的論理和をとる排他的論理和ゲートである。

【００３５】

以上の構成より成る送信局装置である第１の端末１及び、受信局である第２の端末２等で構成される本実施の形態例のマルチメデイアネツトワークシステムのシステム構成を図２に示す。

【００３６】

図２において、１１は情報を提供してその情報に対して対価を受ける図１に示す第１の端末１に対応する送信局、２１Ａ～２１Ｃ，２Ａ２～２２ｃ，２３Ａ～２３Ｃ，２４Ａ～２４Ｃは、送信局１１からの情報を受信してそれに対して対価を支払う図１の第２の端末２と同様構成の受信局、３１は通信衛星、３２は光フアイバ等を用いて幹線通信網を提供する幹線局、３３はＣＡＴＶ等の通信網、３４はローカルエリアネツトワーク（ＬＡＮ）、３４１～３４４はＬＡＮ３４と外部との情報の交換を行うノード、３５は送信局１１と通信衛星３１との通信を行う地上局、３５１，３６１～３６３は通信衛星と地上との通信に用いられるアンテナである。

【００３７】

なお、図１における伝送路３は、図２に示す地上局３５１、通信衛星３１を用いた伝送路、あるいは幹線局３２を用いた伝送路、あるいはＣＡＴＶ網３３を用いた伝送路、あるいはＬＡＮを用いた伝送路等を総称するものである。

【００３８】

以上の構成より成る本実施の形態例システムの概略動作を図３のフローチヤートを参照して以下に説明する。

【００３９】

図２のシステムにおいて、送信局１１は受信局２１Ａ～２４Ｃの各々からの要求に従つて、映像情報その他の即時通信型情報を提供し、この情報は通信衛星３１、幹線局３２、ＣＡＴＶ網３３、あるいはＬＡＮ３４を介して情報を要求した受信局に伝送される。受信局はこの情報に対して対価を支払う。また、送信局１１と受信局２１～２４との間では、この対価の支払いを除くすべての情報の伝送は、図２に示したいずれかの伝送路を介して、即ちオンラインで行なわれる。

【００４０】

しかし、上述した如く、図２のネツトワークにおいては、次のような不正行為に対する対策を行う必要がある。

【００４１】

▲１▼第３者が対価を支払わずに、即時通信型情報を傍受する。

【００４２】

▲２▼第３者が、他の受信局を偽装して情報の要求と受信を行う。

【００４３】

▲３▼受信局が情報受信後、請求の電子伝票を改ざんする。

【００４４】

▲４▼受信局が、対価を支払わずに領収の電子伝票を偽造する。

【００４５】

本実施の形態例においては、このような不正行為を防止するために、第１の端末１である送信局１１には図１に示す公開鍵暗号化部１０３、公開鍵復号化部１０４、及び擬似乱数発生部１０９が装備され、また、第２の端末である受信局２１Ａ～２４Ｃには図１に示す公開鍵暗号化部２０３、公開鍵復号化部２０４及び擬似乱数発生部２０９が各々装備されている。

【００４６】

従つて、各受信局が情報を要求してから対価を支払うまでの手続きは次のようになる。

【００４７】

まずステツプＳ１で受信局から送信局１１へ情報を発注するフアイル（電子伝票）を送信する。この送信及び受信には後述する公開鍵方式による暗号化・復号化処理が施される。続いてフアイルを受信した送信局１１はステツプＳ２でフアイルに従つた、即時通信型情報を発注元受信局へ送信する。この伝送情報には後述するように共通鍵方式による暗号化・復号化処理が施される。

【００４８】

そしてステツプＳ３で受信局から送信局１１へ受取りを確認する電子伝票を送信する。送信局１１はステツプＳ４で送信局から受信局へ対価請求の電子伝票を送信する。この電子伝票の送信及び受信には後述する公開鍵方式による暗号化・復号化処理が施される。

【００４９】

受信局はステツプＳ５でネツトワーク外の手段を用いて対価を支払う。支払いを確認した送信局１１は、ステツプＳ６で発注元の受信局へ領収の電子伝票を送信する。この電子伝票の送信及び受信においても、同様に後述する公開鍵方式による暗号化・復号化処理が施される。

【００５０】

以上の様な手続きを経て、情報の提供とそれに対する対価の支払いが行われる。

【００５１】

以上に概略を説明した図３の情報通信手順における本実施の形態例の暗号化、復号化処理を以下に詳述する。

【００５２】

本実施の形態例においては、即時通信型情報は前記及び擬似乱数発生部１０９，２０９による共通鍵方式によつて暗号化・復号化が成されて送受信される。

【００５３】

これに対して電子伝票類は、各暗号化・復号化部による公開鍵方式によつて暗号化される

。
【００５４】
まず本実施の形態例の共通鍵方式による即時通信型情報の暗号化・復号化の概略を説明する。
【００５５】
本実施の形態例の送信局１１は、送信すべき即時通信型情報の系列と、磁気記憶装置１０１よりのデータ暗号化鍵を種に、疑似乱数発生部１０９が発生した疑似乱数系列との排他的論理和をとることにより、共通鍵方式による暗号化を行なつて即時通信型情報を伝送する。
【００５６】
受信局は、この暗号化された信号と、磁気記憶装置２０１よりのデータ暗号化鍵を種に、疑似乱数発生部２０９が発生した送信局１１の疑似乱数発生部１０９が発生した疑似乱数系列と同一の疑似乱数系列との排他的論理和をとることにより復号化を行なう。
【００５７】
以上の説明において、送信局と受信局は同一の疑似乱数発生部を用いており、同一のデータ暗号化鍵を与えることにより、同一の疑似乱数系列を生成することができる。
【００５８】
次に、上述の本実施の形態例の公開鍵方式による暗号化・復号化の概略を説明する。
【００５９】
本実施の形態例においては、この公開鍵方式により、情報要求、受領、対価請求、領収等の電子伝票類及び、上記共通鍵方式におけるデータ暗号化鍵を暗号化して伝送するのに用いられる。
【００６０】
予め、送信局１１から要求元受信局へと伝送されるこの共通鍵方式におけるデータ暗号化鍵を、公開鍵暗号化方式を用いて暗号化して伝送することにより、第３者に知られること防ぐことができる。また、この種を１回の通信ごとに変更することにより、複数の通信文を比較して暗号化の疑似乱数系列を見破られるのを防ぐことができる。
【００６１】
本実施の形態例においては、このような暗号化方式を用いることにより、高ビツトレートの即時通信型情報に対しても、実時間に、高速でかつ安全度の高い暗号化を行うことが可能となる。
【００６２】
また、本実施の形態例においては、上述した不正行為のうち特に▲２▼～▲４▼を防止するために、電子伝票類を公開鍵方式による暗号化・復号化により伝送すると共に、各端末に暗号化と同時に送信元を認証するための、デイジタル署名部１０２，２０２、署名確認部１０５，２０５によるいわゆるデイジタル署名を行う機能及び該デイジタル署名の確認をする機能を有している。
【００６３】
これにより、上述した不正行為のうち特に▲２▼～▲４▼を有効に防止することができる。このため、電子伝票が第３者に偽造されたり、伝送後に改竄された場合にこれを検出することが可能となる。
【００６４】
以下、本実施の形態例における以上の公開鍵暗号化とデイジタル署名の機能を、図４及び図５を参照して説明する。
【００６５】
まず図４を参照して本実施の形態例の公開鍵暗号化方式の詳細を説明する。
【００６６】
図４において、入力の「ｘ」は、暗号化されていない電子伝票やデータ暗号化鍵等の情報、「ｋｅ」は公開鍵暗号化方式により暗号化するための鍵、「Ｅ」は鍵「ｋｅ」を用いて情報「ｘ」を暗号化する暗号化部、「ｙ」は暗号化部Ｅにより暗号化された情報、「ｋｄ

」は復号化のための鍵、「Ｄ」は鍵「ｋｄ」を用いて暗号化された情報「ｙ」を復号化する復号化部、「ｋｓ」は対となる暗号化鍵「ｋｅ」と復号化鍵「ｋｄ」を決定するための情報、「Ｆ」、「Ｇ」は情報「ｋｓ」から暗号化鍵「ｋｅ」と復号化鍵「ｋｄ」を生成する装置である。

【００６７】

情報「ｋｓ」及び復号化鍵「ｋｄ」は、各端末に固有の秘密情報として端末から外部へ漏れないように保管される。これに対し、暗号化の鍵「ｋｅ」は各端末に固有の公開情報として全端末に公開される。

【００６８】

以上の構成において、送信側の端末は、情報を伝送したい相手先端末に固有の公開された暗号化鍵を用いて情報を暗号化して送信する。暗号化鍵「ｋｅ」と、復号化鍵「ｋｄ」は対をなすものであるが、暗号化鍵「ｋｅ」から復号化鍵「ｋｄ」を推定することが事実上不可能であるような鍵の対が用いられる。このような鍵の対は一方向性関数と呼ばれる関数を利用することにより生成される。

【００６９】

この一方向性関数の好適な例として、互いに素な２つの整数を“ｐ”、“ｑ”とした時、その積ｎは（ｎ＝ｐ・ｑ）となる。即ち、“ｐ”、“ｑ”から“ｎ”は容易に求まるが、“ｎ”から“ｐ”、“ｑ”を求めることは困難であることを利用して、上述のような鍵の対を生成することができる訳である。

【００７０】

このように本実施の形態例においては、公開された暗号化鍵を用いて情報を暗号化して伝送し、この暗号化鍵からは推定できない秘密の復号化鍵を用いて復号化することにより、復号化鍵の伝送を行うことなく安全性の高い暗号化伝送を行うことができる。

【００７１】

続いて本実施の形態例のデイジタル署名機能の詳細を図５を参照して説明する。

【００７２】

図５において、「ｓ」は署名済み通信文である。また、図４と同じ機能を持つ部位は同じ記号を付し、詳細説明を省略する。

【００７３】

以上の構成において、デイジタル署名の伝送時においては、送信側の端末が該端末に固有の復号化鍵を用いてもとの情報に復号操作を施して送信する。そして、受信側の端末で公開された暗号化鍵を用いて、この復号操作を施された情報に暗号操作を施す。暗号操作と復号操作は数学的に逆関数の関係にあるので、このような操作を施しても、受信され暗号操作された情報は、送信端末で復号化操作を施す前のものに戻すことができる。復号化の鍵「ｋｄ」は、上述した様に送信端末の秘密方法として保管されており、公開された暗号化鍵「ｋｅ」から推定することはできない。従つて、受信端末は伝送されてきた署名済み通信文「ｓ」に対して、公開された暗号化鍵を用いて暗号化操作を施すことにより、元の通信文である情報「ｘ」が得られる。

【００７４】

この結果、この情報「ｘ」がたしかに、その暗号化鍵を公開した端末から発行されたものであることを認証できる。復号化鍵を知らない第３者により偽造された情報は、適切な暗号化処理が施されていない情報となつてしまう。適切でない暗号化鍵により暗号化処理を施しても、意味をなさない信号（情報）が得られるのみである。

【００７５】

以上の処理を行なう場合の各位部の具体的役割を具体例に従い以下に説明する。

【００７６】

以下の説明は、受信局２４Ｂが送信局１１から情報を受け取つて対価を支払う場合を例として行なう。他の局における通信においても、全く同様の動作であることは勿論である。

【００７７】

まず、図１の端末２である受信局２４Ｂは、図３のステツプＳ１の処理を行なう。即ち、

即時通信型情報を要求する電子伝票（発注伝票）を磁気記憶装置２０１中に作成する。続いて、デイジタル署名部２０２によつて、この電子伝票に対して受信局２４Ｂに固有の秘密の署名用復号化鍵を用いてデイジタル署名を行なう。更に、暗号化装置２０３により、このデイジタル署名を含む電子伝票を送信局１１に固有の公開された暗号化鍵を用いて暗号化し、通信インターフエース２１２を介して伝送路３へ送出する。

【００７８】

受信局２４ＢはノードＳ４３によつてＬＡＮ３４に接続されており、この署名され、暗号化された受信局２４Ｂよりの伝票は、ノードＳ４３を介してＬＡＮ３４に送られ、ノードＳ４４、ノードＳ４１を通り、送信局１１へ達する。

【００７９】

この伝票は、通信インターフエース１１２により送信局１１内部に取り込まれる。そして、この信号は公開鍵復号化部１０４により、送信局１１に固有の秘密の復号化鍵を用いて復号化される。この復号化情報には、受信局２４Ｂより伝送されてきたデイジタル署名が含まれており、署名確認装置１０５により受信局２４Ｂより伝送されてきたデイジタル署名の確認が行なわれ、受信局２４Ｂよりの電子伝票であることが認証される。そしてこの電子伝票は磁気記憶装置１０１へ記憶される。

【００８０】

次に送信局１１は、図３のステツプＳ２の処理を実行する。即ち、まず即時通信型情報を送信する時に用いる共通鍵暗号化のデータ鍵を決定する。続いて、このデータ鍵に対して、デイジタル署名部１０２による署名を行なう。そして、公開鍵暗号化部１０３で公開鍵による暗号化処理を行ない、このデータ鍵を受信局２４Ｂへ伝送する。受信局２４Ｂは受信信号を復号化し、署名を確認して、データ鍵を受け取る。そして、このデータ鍵を用いて疑似乱数発生部２０９をセツトアツプし、即時通信型情報の受信準備を整える。その後、送信局１１へ受信準備が完了したことを通報する。

【００８１】

送信局１１はこの受信準備完了の連絡を受け取ると、受信局２４Ｂへ伝送したのと同一のデータ鍵を用いて疑似乱数発生部１０９をセツトアツプし、しかる後に同期信号発生部１０７を付勢して同期信号を発生させ、即時通信型情報端末群１０６の要求に基づいたいずれかの装置の動作を開始し、この装置から出力される信号系列と疑似乱数系列との排他的論理和をとることにより暗号化する。そして、通信インターフエース１１２を介して暗号化信号を受信局２４Ｂへと伝送する。通信インタフエース２１２によりこの暗号化信号を受けとつた受信局２４Ｂでは、同期信号抽出部２０７でこの信号中の同期信号を検出して疑似乱数発生部２０９を起動する。

【００８２】

排他的論理和ゲート２１０で送信局１１よりの暗号化された即時通信型情報と、疑似乱数発生部２０９よりの疑似乱数系列との排他的論理和をとることにより復号化処理を行ない、ＣＲＴ２０６ａ、ＶＴＲ２０６ｂ等へ入力する。

【００８３】

送信局１１の疑似乱数発生部１０９と、受信局２４Ｂの疑似乱数発生部２０９には、それぞれ自装置の動作時間を測定して課金情報を測定する課金情報採集部１１１，２１１が接続されており、この課金情報採集部１１１，２１１によつて伝送された情報の量に応じた対価の請求、及び支払いが可能となつている。

【００８４】

本実施の形態例においては、それぞれ自装置の動作時間を測定して課金情報を測定する課金情報採集部１１１，２１１が接続されているため、課金情報の収集情報を表示出力等することにより、送信側、受信側共に課金情報を把握することができ、後日の支払いの準備が速やかに行なえる。

【００８５】

また、通信の最後にこの収集課金情報を伝送することにより、後日のトラブルを未然に防止することも可能となる。

【００８６】
即時通信型情報の伝送が終了すると、受信局２４Ｂは図３のステツプＳ３の処理を実行する。即ち、送信局１１へ受領の電子伝票（受取り確認伝票）を上述と同様の制御で署名、暗号化して送る。
【００８７】
これに対して送信局１１は、図３ステツプＳ４の対価請求の電子伝票を上述同様やはり署名、暗号化して受信局２４Ｂへ送る。
【００８８】
受信局２４Ｂはステツプ５に示す様に、対価を銀行経由、その他の方法で送信局１１側へ支払う。
【００８９】
これに対して送信局１１は、ステツプＳ６で示す様に領収の電子伝票を署名、暗号化して受信局２４Ｂへ送信して１単位の情報サービス取り引きが終了する。
【００９０】
以上説明した様に本実施の形態例によれば、このような手続きを踏むことにより、即時通信型情報はその暗号化鍵を第３者に知られたり推定されたりすることなく高速実時間に安全な暗号化を行つて伝送することができ、また、電子伝票類の偽造、あるいは改竄を防止することができる。
【００９１】
更に、すべての通信が暗号化されているので、第３者にはどのような情報の取り引きが行なわれたかということも知られることがなく通信の秘密が内容だけでなく、その有無まで守られる。
［他の実施の形態例］
本発明は以上のシステムにおける暗号化・復号化処理に限定されるものではなく、また、上述の実施の形態例の構成、制御に限定されるものではない。あらゆるデータ伝送システムに本発明に係る暗号化、復号化処理が適用できる。
【００９２】
本発明を他のシステムに応用した、本発明に係る第２の実施の形態例を図６乃至図８を参照して以下に説明する。
【００９３】
近年電子会議、あるいはテレビ会議と呼ばれる、ネツトワークを利用した会議システムが普及しはじめている。このような会議システムは、事業所内に設けられたＬＡＮと公衆回線を利用して、人物や物体を写すテレビカメラからの信号や、書画の画像、あるいはイメージスキヤナの信号を遠隔地にある会議室同志で伝送するものである。通常、事業所内に設けられたＬＡＮには複数の電子会議室が接続されており、また、情報は公衆回線網を介して伝達されるので、他の会議室からの会議の盗視聴や、第３者による情報の傍受などを避けるため、情報を暗号化する必要がある。
【００９４】
図６は本実施の形態例のこのような会議システムの概略図であり、図６において、５はある企業における第１の事業所、６は同企業の第２の事業所であり、両事業所は公衆回線７を介して接続される。
【００９５】
第１の事業所５において、５１は事業所５の第１の会議室Ａ、５２，５３はこの事業所の第２、第３の会議室Ｂ，Ｃ、５１１～５１５は会議室Ａにある装置群であり、５１１は制御装置、５１２はデイスプレイ、５１３は書画提示用ＣＲＴ、５１４はテレビカメラ、５１５はイメージスキヤナ、５５１～５５５はノード、５６１はＬＡＮの伝送線路、５６２はＬＡＮから分岐した伝送線路であり、これらの伝送線路には同軸ケーブルや光フアイバが用いられる。
【００９６】
また、第２の事業所６においても、同様の会議室６１，６２、ノード６５１～６５５、イ

ンターフエース６４及び伝送路６６１，６６２が配置されている。

【００９７】

以上の構成を備える本実施の形態例の会議システムにおける図６に示す会議室に設置された制御装置を除く、各装置の暗号化を行う通信インターフエースの概略構成を図７、図８に示す。

【００９８】

図７はテレビカメラ、イメージスキヤナ等の情報を送り出す送信機器用のインターフエースの構成図、図８はデイスプレイ、ＣＲＴ等の情報を受け取る受信機器用のインターフエースの構成図である。

【００９９】

図７、図８において、７１，８１はこれらの情報機器、７２，８２は情報信号からクロツク成分をとり出すクロツク抽出回路、７３，８３は疑似乱数発生回路、７４，８４は通信の同期、疑似乱数の発生、情報機器の自動等を制御する制御回路、７５，８５は排他的論理和をとる排他的論理和ゲート、７６，８６は信号を伝送線路へ送受信するための送受信回路である。

【０１００】

以上の構成を備える本実施の形態例の動作を以下説明する。以下の説明は、会議室Ａ５１と会議室Ｂ６１の間で会議を行う場合を例として行なう。会議室５２，５３，６２等もこれらの会議室と同様の機能をもつており、他の会議室間の場合も全く同様の動作であることは勿論である。

【０１０１】

各会議室の制御装置、例えば制御装置５１１，６１１は、前記第１の実施の形態例で説明した公開鍵暗号化による情報暗号化機能を持つているものとする。

【０１０２】

まず会議室５１の制御装置５１１は、会議室５１と会議室の間の会議の開始に先立ち、会議室５１と会議室６１にある機器の各々に対する共通鍵暗号化のデータ鍵を決定する。そして、上述した第１の実施の形態例と同様の公開鍵方式によつてこのデータ鍵を暗号化し、会議室６１の制御装置６１１宛に送信する。次に制御装置５１１は、会議室５１にあるすべての機器の制御回路７４，８４に対してもこのデータ鍵を伝送し、各機器の暗号化通信インターフエースをセツトアツプする。

【０１０３】

制御装置６１１も同様に、会議室６１の各機器の制御回路に対してデータ鍵を伝送してセツトアツプを行う。

【０１０４】

この後、各機器の制御回路からの同期信号を用いて各機器を同期させ、通信を開始する。

【０１０５】

この状態では、各送信機器からの情報はすべて先に決定したデータ鍵を種にした疑似乱数系列との排他的論理和によつて暗号化されて伝送されていることになる。また、各受信機器は同一の疑似乱数系列により信号を復号化して受け取ることになる。なお、この間の暗号化・復号化は、上述した第１実施の形態例と同様にして行なわれる。

【０１０６】

このようにして電子会議を行うことによつて、例えば会議室Ｃ５２や会議室Ｄ５３からの会議の盗視聴を防止することができる。

【０１０７】

また、公衆回線を情報が伝わる間に第３者に傍受される危険も回避できる。

【０１０８】

以上、第１の実施の形態例及び第２の実施の形態例を用いて本発明の詳細を説明したが、本発明の適用範囲はこれらの実施の形態例に限られるものではない。

【０１０９】

即ち、本発明は高速、実時間の暗号化を必要とする即時通信型情報と、より安全度の高い

暗号化や、発信者の認証を必要とする蓄積型情報とを同一の媒体を介して通信するマルチメデイアネツトワークにおいては、どのような形態のものでも適用が可能であり、ネツトワークの形態や端末の種類に依存するものでないことは明らかである。

【０１１０】

【発明の効果】

以上説明したように本発明によれば、ネツトワークを介して提供可能な情報を要求する要求情報だけでなく、その要求情報が要求する情報を復号化するための鍵に対する偽装、改ざん、偽造等の不正行為を防止することができ、その結果、その要求情報が要求する情報を非常に安全に伝送することができる。

【図面の簡単な説明】

【図１】本発明に係る第１の実施の形態例のブロツク構成図である。

【図２】本実施の形態例が適用されるマルチメデイアネツトワークシステムの概要の一例を示す図である。

【図３】本実施の形態例の概略動作を示すフローチヤートである。

【図４】図１において公開鍵による暗号化を行う部位の機能を示す図である。

【図５】図１においてデイジタル署名を行う部位の機能を示す図である。

【図６】本発明に係る第２の実施の形態例の会議システム構成図である。

【図７】第２の実施の形態例における送信機器用のインターフエースの構成図である。

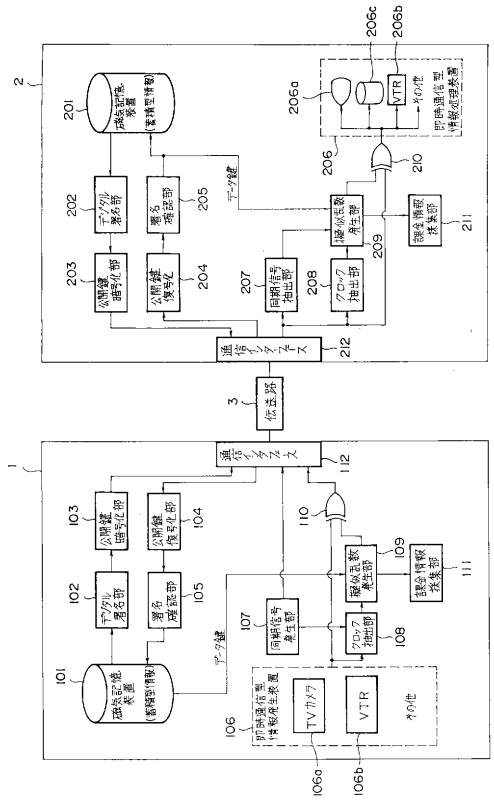
【図８】第２の実施の形態例における受信機器用のインターフエースの構成図である。

【符号の説明】

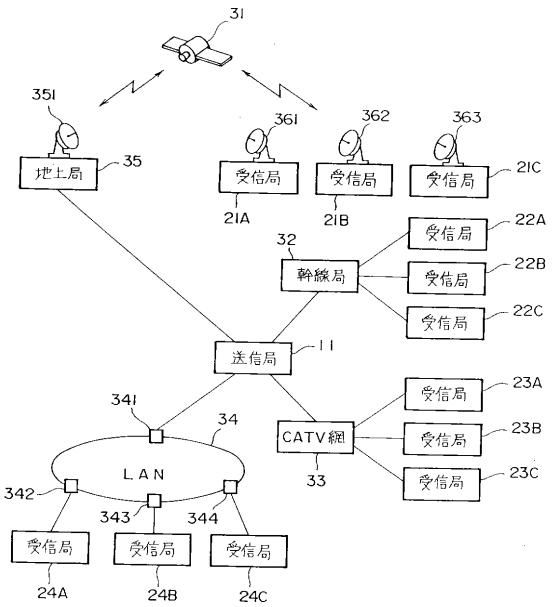
１、２　通信端末
３　伝送路
５，６　企業の事業所
７　公衆回線
１１　送信局
２１Ａ～２４Ｃ　受信局
３１　通信衛星
３２　幹線局
３３　通信網
３４　ローカルエリアネツトワーク（ＬＡＮ）
３５　地上局
５１～５３，６１，６２　会議室
５４，６４　インタフエース
７１，８１　情報機器
７２，８２　クロツク抽出回路
７３，８３　疑似乱数発生回路
７４，８４　制御回路
７５，８５，１１０，２１０　排他的論理和ゲート
７６，８６　送受信回路
１０１，２０１　磁気記憶装置
１０２，２０２　デイジタル署名部
１０３，２０３　公開鍵暗号化部
１０４，２０４　公　開鍵復号化部
１０５，２０５　署名確認部
１０６，２０６　即時通信型情報発生装置
１０６ａ，２０６ａ　ＴＶカメラ
１０６ｂ，２０６ｂ　ＶＴＲ
１０７，２０７　同期信号発生部
１０８，２０８　クロツク抽出部
１０９，２０９　疑似乱数発生部

１１１，２１１　課金情報採集部
１１２，２１２　通信インターフエース
３４１～３４４，５５１～５５５　ノード
５１１　制御装置
５１２　デイスプレイ
５１３　書画提示用ＣＲＴ
５１４　テレビカメラ
５１５　イメージスキヤナ
Ｄ　復号化部
Ｅ　暗号化部
Ｄ　復号化部

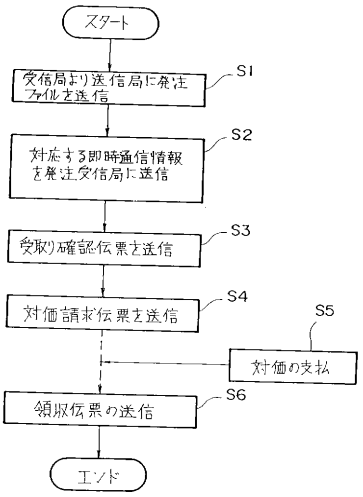
【図１】



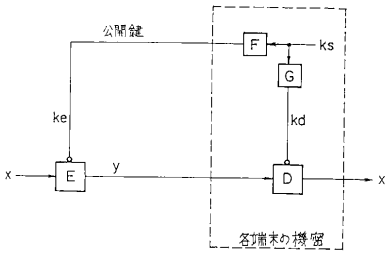
【図２】



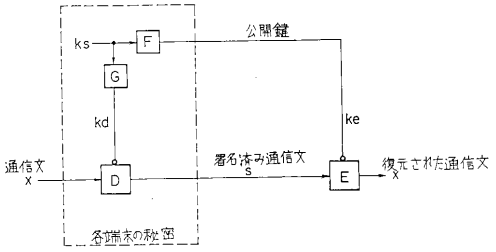
【図３】


スタート
受信局より送信局に発注ファイルを送信
S1
対応する即時通信情報を発注受信局に送信
S2
受取り確認伝票を送信
S3
対価請求伝票を送信
S4
S5
対価の支払
領収伝票の送信
S6
エンド

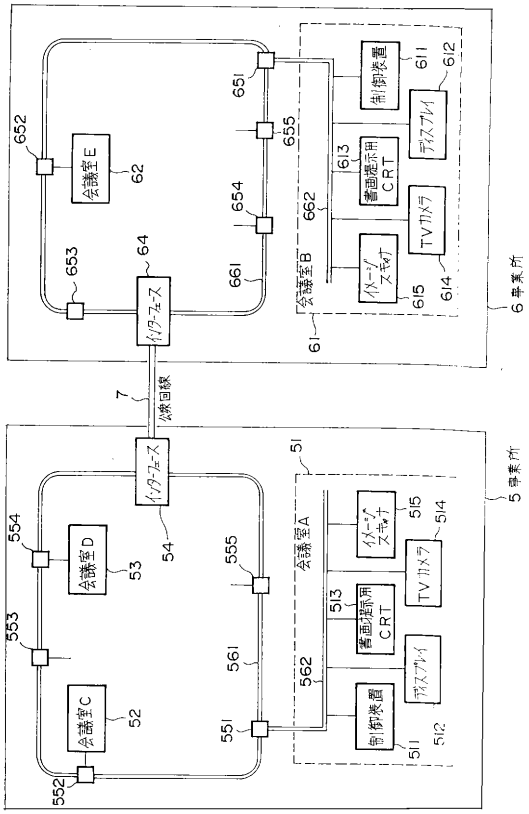
【図４】


公開鍵
F
ks
G
ke
kd
x
E
y
D
x
各端末の機密

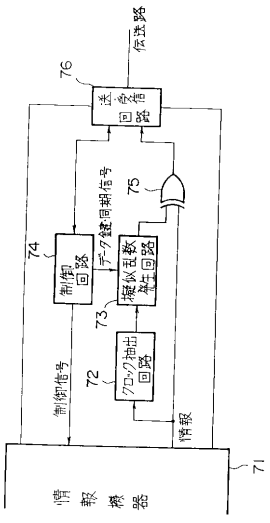
【図５】


ks
F
公開鍵
G
kd
ke
通信文
x
D
署名済み通信文
s
E
復元された通信文
x
各端末の秘密

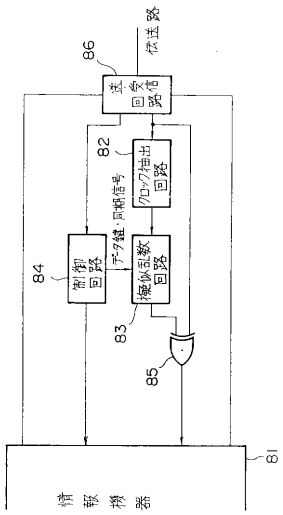
【図６】


会議室E
62
651
652
655
654
653
64
インターフェース
661
662
会議室B
61
制御装置
611
612
ディスプレイ
613
書画提示用CRT
TVカメラ
イメージスキャナ
615
614
6 事業所
7 公衆回線
インターフェース
54
51
会議室A
554
会議室D
53
555
553
561
562
551
会議室C
52
552
イメージスキャナ
515
514
TVカメラ
513
書画提示用CRT
ディスプレイ
制御装置
511
512
5 事業所

【図７】


伝送路
76
送受信回路
75
74
制御回路
データ鍵同期信号
擬似乱数発生回路
73
72
ブロック抽出回路
制御信号
情報
71
情報機器

【図８】



フロントページの続き

合議体
審判長　西川　正俊
審判官　山中　実
審判官　橋本　正弘

(56)参考文献　特開昭６４－１６１４３（ＪＰ，Ａ）
特開昭６１－９０５２（ＪＰ，Ａ）
特開昭６２－１９０９４３（ＪＰ，Ａ）
「データ保護と暗号化の研究」，日本経済新聞社，ｐ．５９－６０，１５３－１６３，２０１－２０７（昭和５８年7月２９日第1版第1刷発行）
「ネットワーク・セキュリティ」，日経マグロウヒル社，昭６０，ｐ．２３４－２３５（特に、図9．２　署名済み通信文の公開鍵サイファ化）
「暗号通信における3階層復号形鍵配送方式」，電子情報通信学会論文誌，ＶＯＬ．Ｊ７０－Ｄ，Ｎｏ．１２，ｐｐ２７２２－２７２９（１９８７）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
Ｈ０４Ｌ９／０２
Ｇ０９Ｃ１／００