(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4235824号
(P4235824)

(45)発行日　平成21年3月11日(2009.3.11)　(24)登録日　平成20年12月26日(2008.12.26)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
H04L 9/32	(2006.01)	H04L	9/00	675B
H04L 9/08	(2006.01)	H04L	9/00	601F
H04L 12/58	(2006.01)	H04L	12/58	100Z

請求項の数 5　(全 14 頁)

(21)出願番号　特願2004-261760 (P2004-261760)
(22)出願日　平成16年9月9日 (2004.9.9)
(65)公開番号　特開2006-80805 (P2006-80805A)
(43)公開日　平成18年3月23日 (2006.3.23)
審査請求日　平成17年10月18日 (2005.10.18)

前置審査

(73)特許権者　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(74)代理人　100097892
弁理士　西岡　義明
(72)発明者　谷本　好史
京都市伏見区竹田向代町１３６番地　村田機械株式会社本社工場内
(72)発明者　宗宮　和男
京都市伏見区竹田向代町１３６番地　村田機械株式会社本社工場内
(72)発明者　竹内　茂樹
京都市伏見区竹田向代町１３６番地　村田機械株式会社本社工場内

最終頁に続く

(54)【発明の名称】暗号化装置

(57)【特許請求の範囲】

【請求項１】

インターネットファクシミリ、メールサーバ、パソコン等とネットワークを介して接続される暗号化装置であって、

相手先のアドレス情報と鍵情報を管理する手段と、暗号化手段と、データを送受信する送受信手段と、上記各部を制御する制御手段を備え、上記送受信手段によりインターネットファクシミリまたはパソコンから受信したデータが電子メールであるとき、上記制御手段が上記暗号化手段により上記鍵情報を用いて電子メールを暗号化し、暗号化した電子メールを上記送受信手段によりメールサーバに送信し、上記送受信手段によりインターネットファクシミリまたはパソコンから受信したデータが電子メールでなく、メール本文と送信先の宛先情報であるとき、上記制御手段が上記暗号化手段により上記鍵情報を用いてメール本文のみを暗号化し、暗号化したメール本文を上記送受信手段によりインターネットファクシミリまたはパソコンへ返信することを特徴とする暗号化装置。

【請求項２】

請求項１に記載の暗号化装置において、証明書情報を管理する手段と、署名情報を生成する署名情報生成手段を備え、電子メールまたはメール本文を暗号化するとき、上記制御手段が上記署名情報生成手段により上記証明書情報を用いて署名情報を生成し、生成された署名情報を暗号化された電子メールまたはメール本文に付与することを特徴とする暗号化装置。

【請求項３】

請求項２に記載の暗号化装置において、上記制御手段がインターネットファクシミリまたはパソコンからの電子メールまたはメール本文と宛先情報よりなるデータにインターネットファクシミリまたはパソコン固有の証明書情報が添付されているか否かを判定し、インターネットファクシミリまたはパソコン固有の証明書情報が添付されている場合、上記署名情報生成手段が添付された証明書情報を用いて署名情報を生成することを特徴とする暗号化装置。

【請求項４】

請求項１に記載の暗号化装置において、復号化手段を備え、インターネットファクシミリまたはパソコンから暗号化された電子メールまたはメール本文を受信すると、上記制御手段が上記復号化手段により電子メールまたはメール本文を復号化し、インターネットファクシミリまたはパソコンに送信することを特徴とする暗号化装置。

【請求項５】

請求項４に記載の暗号化装置において、署名情報を検証する署名情報検証手段を備え、電子メールまたはメール本文を復号化するとき、上記制御手段が上記署名情報検証手段により署名情報を検証し、検証結果を復号化された電子メールまたはメール本文に付与することを特徴とする暗号化装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、暗号化装置、特にファクシミリ装置等のクライアントからの電子メールやデータを公開鍵暗号方式を利用して暗号化する暗号化装置に関する。

【背景技術】

【０００２】

近年、ＬＡＮ（Local Area Network）等の通信回線で接続し、さらにネットワーク化したインターネット等を介して電子メールを配信するコンピュータ通信網が普及しているが、従来のファクシミリ手順は上記のようなコンピュータ通信網を利用するコンピュータ通信の通信手順とは異なるため、ファクシミリ装置からコンピュータ通信網へ直接通信することはできない。

【０００３】

しかし、ファクシミリ通信で通常送受信される原稿等のイメージデータであっても、電子メール形式に変換することにより、コンピュータ通信網を介して送受信することができるので、送信原稿を電子メールとしてインターネット通信で送受信できるようにした電子メール機能付きのインターネットファクシミリが開発されている。

【０００４】

このようなインターネットファクシミリにおいて、電子メールを利用してインターネットを介して画像データを送受信する場合、画像データを含む電子メールを送信側のメールサーバ装置及びインターネットを介して受信側のメールサーバ装置にＳＭＴＰ（Simple Mail Transfer Protocol）方式で送信し、受信側のインターネットファクシミリ装置は、ＰＯＰ３（Post Office Protocol version3）方式で受信側のメールサーバ装置にアクセスして画像データを含む電子メールを受信し、受信した画像データを画像記録部を用いて印字するようになっている。

【０００５】

一方、電子メールはその利便性、迅速性等の理由からビジネス等の現場において、ビジネスコミュニケーションのために必要不可欠なツールとなっている。しかしながら、電子メールを送信する際には、複数のコンピュータを経由して送信先メールアドレスへ配信されるため、配信途中でメールの内容が盗聴されたり、その内容が書き換えられたり、全く別の内容にすりかえられる、といった改ざんの危険性があった。また、送信メール元アドレスに自らのアドレスとは異なるメールアドレスを設定し、第三者に成りすましてメール送信が行われるといった危険性もあった。

【０００６】

このような危険性を回避するため、公開鍵暗号化方式（ＰＫＩ、Public Key Infrastructure）を利用した電子メールの送受信が行われている。この公開鍵暗号化方式は、メッセージを暗号化するときと復号化するときとで、同一鍵（暗号アルゴリズム）を用いる共通鍵暗号方法と、異なる鍵（暗号化は公開鍵、復号化は秘密鍵）を用いる公開鍵暗号方法とが一般に知られている。

【０００７】

公開鍵は、例えば認証局（ＣＡ：Certificate Authority）で正式にその保有者であるユーザとの関係が認証され不特定多数に公開された暗号鍵であり、秘密鍵は公開鍵と対をなす暗号鍵である。そして、公開鍵で暗号化したものは秘密鍵でしか復号することができず、逆に秘密鍵を利用して暗号化したものは公開鍵でしか復号することができない。したがって、公開鍵を利用して暗号化メールを作成し、秘密鍵を利用して電子署名を行うことができる。この電子署名を認証局で認証された公開鍵でチェックすることにより、データの改ざんの有無を検出することができる。

【０００８】

このような公開鍵暗号化方式を利用するために必要な処理は、予め暗号化機能を備えた電子メールソフトを使用し、自分の秘密鍵や送信相手のデジタル証明書等を使用端末に予めインストールし、逐一設定することにより実現している。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

上記のように、従来、電子メールの暗号化には暗号化機能を備えた電子メールソフトをインストールしなければならず、上記のようなインターネットファクシミリで暗号化メールを作成するためには、インターネットファクシミリにそのようなソフトをインストールしなければならず、設定操作が複雑となる、という問題があった。

また、インターネットファクシミリに、暗号化に必要な暗号鍵の管理機能も実装しなければならず、電子メールを暗号化する時に必要となる宛先の公開鍵や、電子メールの署名検証に必要となる送信元の公開鍵を登録しておかなければならず、多数の相手と暗号電子メールの交換を行う場合には、公開鍵登録のための多くの記憶容量を必要とするという問題もあった。

【００１０】

一方、最近のインターネットファクシミリはメールサーバ機能を搭載し、ドメイン名から対応のグローバルＩＰアドレスを求めて返答するダイナミックＤＮＳ（Domain Name System）やＩＰ網を含むインターネットで利用するプロトコルを使って音声を伝送するためのＶｏＩＰ（Voice over IP）網を介して端末同士が直接接続し、ＳＭＴＰ、ＦＴＰ（File Transfer Protocol）あるいはＳＩＰ（Session Initiation Protocol）等の制御プロトコルを用いて通信する場合も出てきている。

【００１１】

このように端末同士で直接接続して通信するようなファクシミリ装置でも暗号化メールのやり取りが切望されているが、組み込み機器では暗号化処理の負荷が大きいという問題があった。

【００１２】

本発明は、上記の問題に鑑みてなされたもので、通常のメールサーバ経由でメールの送受信を行うメールクライアントや、直接端末同士で通信するインターネットファクシミリなどでも、証明書や鍵の管理・暗号化／復号化を行わずに簡単に暗号化メールの機能を利用できるようにするための暗号化装置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】

【００１３】

上述の目的を達成するため、請求項１に係る発明の暗号化装置は、インターネットファクシミリ、メールサーバ、パソコン等とネットワークを介して接続される暗号化装置であって、相手先のアドレス情報と鍵情報を管理する手段と、暗号化手段と、データを送受信

する送受信手段と、上記各部を制御する制御手段を備え、上記送受信手段によりインターネットファクシミリまたはパソコンから受信したデータが電子メールであるとき、上記制御手段が上記暗号化手段により上記鍵情報を用いて電子メールを暗号化し、暗号化した電子メールを上記送受信手段によりメールサーバに送信し、上記送受信手段によりインターネットファクシミリまたはパソコンから受信したデータが電子メールでなく、メール本文と送信先の宛先情報であるとき、上記制御手段が上記暗号化手段により上記鍵情報を用いてメール本文のみを暗号化し、暗号化したメール本文を上記送受信手段によりインターネットファクシミリまたはパソコンへ返信することを特徴とする。

【００１５】

また、請求項２に係る発明の暗号化装置は、請求項１に記載の暗号化装置において、証明書情報を管理する手段と、署名情報を生成する署名情報生成手段を備え、電子メールまたはメール本文を暗号化するとき、上記制御手段が上記署名情報生成手段により上記証明書情報を用いて署名情報を生成し、生成された署名情報を暗号化された電子メールまたはメール本文に付与することを特徴とする。

【００１６】

さらに、請求項３に係る発明の暗号化装置は、請求項２に記載の暗号化装置において、上記制御手段がインターネットファクシミリまたはパソコンからの電子メールまたはメール本文と送信先の宛先情報よりなるデータにインターネットファクシミリまたはパソコン固有の証明書情報が添付されているか否かを判定し、インターネットファクシミリまたはパソコン固有の証明書情報が添付されている場合、上記署名情報生成手段が添付された証明書情報を用いて署名情報を生成することを特徴とする。

【００１７】

また、請求項４に係る発明の暗号化装置は、請求項１に記載の暗号化装置において、復号化手段を備え、インターネットファクシミリまたはパソコンから暗号化された電子メールまたはメール本文を受信すると、上記制御手段が上記復号化手段により電子メールまたはメール本文を復号化し、インターネットファクシミリまたはパソコンに送信することを特徴とする。

【００１８】

また、請求項５に係る発明の暗号化装置は、請求項４に記載の暗号化装置において、署名情報を検証する署名情報検証手段を備え、電子メールまたはメール本文を復号化するとき、上記制御手段が上記署名情報検証手段により署名情報を検証し、検証結果を復号化された電子メールまたはメール本文に付与することを特徴とする。

【発明の効果】

【００１９】

請求項１に係る発明の暗号化装置によれば、インターネットファクシミリやパーソナルコンピュータ（以下、パソコンという）等から電子メールを送信すると、送信した電子メールが暗号化されてメールサーバに送信されるので、インターネットファクシミリまたはパソコン側で証明書や鍵の管理あるいは暗号化処理を行うことなく、簡単に暗号化メールの機能を利用することができる。

【００２０】

また、請求項１に係る発明の暗号化装置によれば、インターネットファクシミリまたはパソコンからメール本文と送信先の宛先情報よりなるデータを送信すると、メール本文が暗号化されて返信されるので、暗号化されたメール本文を暗号化メールの形に整形して実際の送信先に送信することができ、上記と同様に証明書や鍵の管理あるいは暗号化処理を行うことなく、簡単に暗号化メールの機能を利用することができる。

【００２１】

また、請求項２に係る発明の暗号化装置によれば、電子メールまたはメール本文が暗号化されるとき、署名情報が生成されて暗号化された電子メールまたはメール本文に付与されるので、インターネットファクシミリまたはパソコンが特別な機能を備えていなくとも、暗号化メールに簡単に署名情報を付与することができ、さらに、請求項３に係る発明の

暗号化装置によれば、インターネットファクシミリまたはパソコンからの電子メールまたはメール本文と送信先の宛先情報よりなるデータにインターネットファクシミリまたはパソコン固有の証明書情報を添付して送信すれば、インターネットファクシミリまたはパソコン固有の証明書情報により署名情報が生成されるので、暗号化装置に登録された証明書情報を共有で使用するとともに、インターネットファクシミリまたはパソコンが持つ固有の証明書も簡単に利用することができる。

【００２２】

さらに、請求項４に係る発明の暗号化装置によれば、インターネットファクシミリまたはパソコンから暗号化された電子メールまたはメール本文を送信すると、送信した電子メールまたはメール本文が復号化されてインターネットファクシミリまたはパソコンに送信されるので、インターネットファクシミリまたはパソコン側に復号化機能を設けなくとも、復号化処理を行うことができ、また、請求項５に係る発明の暗号化装置によれば、電子メールまたはメール本文が復号化されるとき、添付された署名情報が検証され、検証結果が復号化された電子メールまたはメール本文に付与されるので、インターネットファクシミリまたはパソコンが特別な機能を備えていなくとも、暗号化メールが改ざんされていないことを簡単に確認することができる。

【実施例】

【００２３】

以下、本発明の暗号化装置の実施例について、図面を用いて説明する。図１は本発明の暗号化装置がＬＡＮに接続される場合のネットワーク構成例を示す図である。

図１に示すように、暗号化装置１、インターネットファクシミリ２、メールサーバ３及びパソコン４等がＬＡＮ５に接続されている。そして、インターネットファクシミリ２またはパソコン４から電子メール（ａ）を暗号化装置１の暗号化Ｉ／Ｆに送信すると、暗号化装置１は受信した電子メールの送信先の宛先情報を抽出し、宛先アドレスが暗号化に対応しているかどうかを電話帳データベースから調べ、対応していれば、登録されている公開鍵情報を使用し電子メールを暗号化メール（Ｓ／ＭＩＭＥ形式のメール）（ｂ）に変換し、メールサーバ３に送信する。このとき、登録されている証明書情報に基づいて電子署名を付与することもできる。

なお、上記の電話帳データベースは各クライアントで使用している電話帳などからvCardやCSVあるいはLDAPなどによりデータをインポートすることが可能である。

【００２４】

また、インターネットファクシミリ２’がメール本文として暗号化される部分と送信先情報よりなるデータ（ｃ）を暗号化装置１に送信すると、暗号化装置１は受信したデータから送信先の宛先情報を抽出し、宛先アドレスが暗号化に対応しているかどうかを電話帳データベースから調べ、対応していれば、登録されている公開鍵情報を使用して受信したメール本文を所定の暗号化方式で暗号化したデータ（例えば、ＰＫＣＳ＃７）を生成する。このとき、上記と同様に、登録されている証明書情報に基づいて電子署名を付与することもできる。そして、暗号化したデータ（ｄ）をインターネットファクシミリ２’に送信することにより、インターネットファクシミリ２’は暗号化データ（ｄ）を暗号化メール（ｅ）の形に整形し、実際の送信先、例えば、外部のインターネットファクシミリ６に送信することができる。

【００２５】

一方、パソコン４がメールを受信する場合、パソコン４は自身のアカウント情報を用いてメールサーバ３より定期的に受信メールを受信し、受信メールの中に暗号化されているものがあるかどうかを判断し、暗号化された電子メール（ｆ）があった場合には、その受信メール（Ｓ／ＭＩＭＥ形式のメール）またはメールより取出した暗号データ部分（ＰＫＣＳ＃７）（ｇ）を暗号化装置１の復号化用Ｉ／Ｆに送信する。暗号化装置１は受信したデータを自装置に登録されている鍵情報を用いて復号化し、復号化されたデータ（ｈ）をパソコン４に返信する。このとき、電子署名などが付与されていた場合には、検証を行い、検証結果や署名内容などをコメントとして返信するデータに付け加えるようにすること

もできる。

【００２６】

上記の暗号化・復号化用Ｉ／Ｆとしては、暗号化装置１にそれぞれ暗号化用のメールアドレス、復号化用のメールアドレスを設けてインターネットファクシミリ２やパソコン４等のクライアントとの間で電子メールにより暗号化・復号化を行うことができる。

また、暗号化・復号化用Ｉ／Ｆの他の例として、暗号化装置１にそれぞれ暗号化用のＵＲＬ（ＣＧＩ）、復号化用のＵＲＬ（ＣＧＩ）を設けてクライアントとの間でＨＴＴＰプロトコルにより暗号化・復号化を行うことも可能である。

【００２７】

次に、本発明の暗号化装置の構成について図２のハードウェア構成ブロック図及び図３の機能ブロック図により説明する。

暗号化装置１は図２のハードウェア構成図に示すように、ＣＰＵ１１、ＲＯＭ（Read Only Memory）１２、ＲＡＭ（Random Access Memory）１３及びＬＡＮインターフェース（Ｉ／Ｆ）１４から構成され、各部がバス１５を介して接続されている。

【００２８】

ＣＰＵ１１はバス１５を介して暗号化装置１のハードウェア各部を制御するとともに、ＲＯＭ１２に記憶されたプログラムに基づいて各種のプログラムを実行し、ＲＯＭ１２は暗号化装置１の動作に必要な種々のプログラムを予め記憶している。また、ＲＡＭ１３はＳＲＡＭ等で構成され、プログラムの実行時に発生する一時的なデータや証明書情報を記憶するとともに、電話帳データベースとして相手先のアドレスや公開鍵等の情報を記憶している。

また、ＬＡＮ　Ｉ／Ｆ１４はＬＡＮ５に接続され、ＬＡＮ５からの信号を受信する一方、ＬＡＮ５に対して信号やデータを送信するものであり、信号変換やプロトコル変換などのインターフェース処理を実行する。

【００２９】

一方、図３はこの暗号化装置１を機能で表した機能ブロック図であり、制御部２１、証明書情報管理部２２、相手先情報管理部２３、メールサーバ管理部２４、暗号化部２５、復号化部２６、電子署名生成部２７、電子署名検証部２８、データ送受信部２９からなり、制御部２１は図２のＣＰＵ１１によって構成され、証明書情報管理部２２、相手先情報管理部２３、メールサーバ管理部２４はＲＡＭ１３により構成されている。また、暗号化部２５、復号化部２６、電子署名生成部２７、電子署名検証部２８、データ送受信部２９は、図２のＣＰＵ１１、ＲＯＭ１２及びＲＡＭ１３によって構成され、各部の機能はソフトウェアプログラムによって実行される。

【００３０】

制御部２１は暗号化装置１の各部を制御し、証明書情報管理部２２は図４に示す証明書情報を記憶している。証明書情報としては、相手先から暗号メールを送信してもらうための自身の公開鍵や秘密鍵、認証局名、有効期限、所有者が記憶されており、暗号化装置１を使用する全てのクライアントに共通のものと、個々のインターネットファクシミリやパソコン（ＰＣ）のみが使用する証明書情報が記憶されている。

【００３１】

相手先情報管理部２３は図５に示すように、登録されている送信先や送信元等の各宛先のメールアドレスに対応付けて、暗号化に必要な公開鍵、認証局名、有効期限を記憶している。また、メールサーバ管理部２４はメールサーバ３のプライベートＩＰアドレスを記憶している。

【００３２】

暗号化部２５は送信先の公開鍵を用いて電子メール全体または電子メール本文のみを暗号化し、復号化部２６は秘密鍵を用いて暗号化メールまたは暗号化メール本文を復号化する。また、電子署名生成部２７は電子メールに秘密鍵を用いて電子署名を生成し、電子署名検証部２８は電子メールの送信元の公開鍵を使用して当該電子メールに添付された電子署名を検証することにより、電子メールの完全性、すなわち、改ざんされていないことを

確認する。

【００３３】

また、データ送受信部２９はクライアントからの電子メールやデータの送受信を行うものであり、図６に示すような、復号化用のメールアドレス（decode@server.com）、暗号化用のメールアドレス（encode@server.com）が割り当てられており、インターネットファクシミリ２やパソコン４等のクライアントとの間で電子メールによりデータの送受信を行うことができる。

なお、上記のメールアドレスに代えて、図７に示すように復号化用のＵＲＬ（www.server/decode.cgi）、暗号化用のＵＲＬ（www.server/encode.cgi）を割り当て、クライアントとの間でＨＴＴＰプロトコルによりデータの送受信を行うことも可能である。

【００３４】

上記のように、インターネットファクシミリ２から電子メール（ａ）を送信するか、またはインターネットファクシミリ２’からメール本文として暗号化される部分と送信先情報よりなるデータ（ｃ）を暗号化装置１に送信すると、電子メールまたはメール本文が暗号化されるが、このときの暗号化装置１の作用を図８のフローチャートにより説明する。

【００３５】

暗号化メールアドレス（encode@server.com）を介してデータ送受信部２９がデータを受信すると、制御部２１は図８のフローチャートに示す暗号化プログラムを開始し、まず受信したデータが電子メールか否かを判定する（ステップ１０１）。受信したデータが電子メールであると判定した場合には、制御部２１は受信した電子メールから送信先の宛先情報を抽出し、相手先情報管理部２３に記憶されているデータに基づいて宛先アドレスが暗号化に対応した宛先アドレスか否かを判定し（ステップ１０２）、暗号化に対応していない宛先アドレスであった場合には、ステップ１０４に移る。

一方、宛先アドレスが暗号化に対応した宛先であった場合には、制御部２１は暗号化部２５により電子メールを暗号化させる（ステップ１０３）。すなわち、暗号化部２５は相手先情報管理部２３に登録されている当該宛先の公開鍵情報を使用し、受信した電子メールを暗号化メールに変換する。

【００３６】

次に、制御部２１は署名を付与する設定となっているか否かを判定し（ステップ１０４）、署名を付与しないと判定した場合には、ステップ１０６に移る。ステップ１０４で署名を付与すると判定した場合には、制御部２１は電子署名生成部２７に電子署名を生成させ、生成させた電子署名を暗号化メールに付加する（ステップ１０５）。すなわち、電子署名生成部２７は、インターネットファクシミリ２から送信された電子メール全体からハッシュ関数（一方的要約関数）を利用してメッセージダイジェストを生成し、生成したメッセージダイジェストを証明書情報管理部２２に管理している秘密鍵で暗号化して電子署名を生成する。

なお、署名を付与するか否かの設定は暗号化装置１への設定により任意に変更することが可能である。

【００３７】

そして、電子署名の付加が完了すると、制御部２１は暗号化メールの送信元アドレスをインターネットファクシミリ２のアドレスに変換した（ステップ１０６）後、データ送受信部２９によりメールサーバ管理部２４に記憶されているメールサーバ３のプライベートＩＰアドレスに宛てて暗号化メール（ｂ）を送信する（ステップ１０７）。

【００３８】

一方、ステップ１０１で受信したデータが電子メールでなく、メール本文として暗号化される部分と送信先情報よりなるデータであった場合には、制御部２１は、受信した送信先の宛先情報を抽出し、相手先情報管理部２３に記憶されているデータに基づいて宛先アドレスが暗号化に対応した宛先アドレスか否かを判定し（ステップ１０８）、暗号化に対応していない宛先アドレスであった場合には、ステップ１１０に移る。一方、宛先アドレスが暗号化に対応した宛先であった場合には、上記と同様に制御部２１は暗号化部２５に

よりメール本文を暗号化させる（ステップ１０９）。すなわち、暗号化部２５は当該宛先の公開鍵情報を使用し受信したメール本文を所定の暗号化方式で暗号化したデータを生成する。

【００３９】

次に、制御部２１は署名を付与する設定となっているか否かを判定し（ステップ１１０）、署名を付与しないと判定した場合には、ステップ１１２に移る。ステップ１１０で署名を付与すると判定した場合には、制御部１は上記と同様に電子署名生成部２７に電子署名を生成させ、生成した電子署名を暗号化したメール本文に付加した（ステップ１１１）後、データ送受信部２９により暗号化データ（ｄ）をインターネットファクシミリ２’に返送する。これにより、インターネットファクシミリ２’は暗号化データ（ｄ）を暗号化メール（ｅ）の形に整形し、実際の送信先、例えば、インターネットファクシミリ６に送信することができる。

【００４０】

以上のように、インターネットファクシミリやパソコン等のクライアントから電子メールを送信すると、送信した電子メールが暗号化されてメールサーバに送信され、クライアントからデータを送信すると、送信したデータが暗号化されて返信されるので、クライアント側で証明書や鍵の管理あるいは暗号化処理を行うことなく、簡単に暗号化した電子メールを相手先に送信することができる。

【００４１】

上記の実施例では、電子署名生成部２７に電子署名の生成を行わせる場合に、証明書情報管理部２２に記憶されている証明書情報を使用したが、クライアントから暗号化データとともにクライアント固有の証明書情報を送信することにより、クライアント固有の証明書情報を使用して電子署名を生成することも可能であり、このようにクライアント固有の証明書情報を使用して電子署名を生成する場合の暗号化装置１の作用を図９のフローチャートにより説明する。

【００４２】

暗号化メールアドレス（encode@server.com）を介してデータ受信部２９がデータを受信すると、制御部２１は図９のフローチャートに示す暗号化プログラムを開始し、上記と同様に、まず受信したデータが電子メールか否かを判定する（ステップ２０１）。受信したデータが電子メールであると判定した場合には、制御部２１は受信した電子メールから送信先の宛先情報を抽出し、相手先情報管理部２３に記憶されているデータに基づいて宛先アドレスが暗号化に対応した宛先アドレスか否かを判定し（ステップ２０２）、暗号化に対応していない宛先アドレスであった場合には、ステップ２０４に移る。一方、宛先アドレスが暗号化に対応した宛先であった場合には、制御部２１は暗号化部２５により電子メールを暗号化させる（ステップ２０３）。

【００４３】

次に、制御部２１は署名を付与する設定となっているか否かを判定し（ステップ２０４）、署名を付与しないと判定した場合には、ステップ２０８に移る。ステップ２０４で署名を付与すると判定した場合には、制御部２１は電子メールにクライアントの証明書が添付されていたか否かを判定する（ステップ２０５）。証明書を受信していたと判定した場合には、制御部２１は電子署名生成部２７に受信した証明書に基づき電子署名を生成させ、生成された電子署名を暗号化された電子メールに付加する（ステップ２０６）。

【００４４】

一方、ステップ２０５で証明書を受信していないと判定した場合には、制御部２１は電子署名生成部２７に証明書情報管理部２２に記憶されている証明書に基づき電子署名を生成させ、生成させた電子署名を暗号化された電子メールに付加する（ステップ２０７）。

【００４５】

そして、電子署名の付加が完了すると、制御部２１は暗号化メールの送信元アドレスをインターネットファクシミリ２のアドレスに変換した（ステップ２０８）後、データ送受信部２９により送信メールサーバ管理部２４に記憶されているメールサーバ３のプライベ

ートＩＰアドレスに宛てて暗号化メール（ｂ）を送信する（ステップ２０９）。

【００４６】

一方、ステップ２０１で受信したデータが電子メールでなく、メール本文として暗号化される部分と送信先情報よりなるデータであった場合には、制御部２１は、受信した送信先の宛先情報を抽出し、相手先情報管理部２３に記憶されているデータに基づいて宛先アドレスが暗号化に対応した宛先アドレスか否かを判定し（ステップ２１０）、暗号化に対応していない宛先アドレスであった場合には、ステップ２１２に移る。一方、宛先アドレスが暗号化に対応した宛先であった場合には、上記と同様に制御部２１は暗号化部２５によりメール本文を暗号化させる（ステップ２１１）。

【００４７】

次に、制御部２１は署名を付与する設定となっているか否かを判定し（ステップ２１２）、署名を付与しないと判定した場合には、ステップ２１６に移る。ステップ２１２で署名を付与すると判定した場合には、制御部２１は受信したデータにクライアントの証明書が添付されていたか否かを判定する（ステップ２１３）。証明書を受信していたと判定した場合には、制御部２１は電子署名生成部２７に受信した証明書に基づき電子署名を生成させ、生成された電子署名を暗号化されたメール本文に付加する（ステップ２１４）。

【００４８】

一方、ステップ２１３で証明書を受信していないと判定した場合には、制御部２１は電子署名生成部２７に証明書情報管理部２２に記憶されている証明書に基づき電子署名を生成させ、生成された電子署名を暗号化されたメール本文に付加する（ステップ２１５）。この後、制御部２１はデータ送受信部２９により暗号化データ（ｄ）をインターネットファクシミリ２’に返送する（ステップ２１６）。

以上のように、クライアントから暗号化するデータをクライアント固有の証明書情報と共に受信した場合には、その証明書情報を利用して電子署名が生成されるので、暗号化装置に登録された証明書情報を共有で使用するとともに、クライアントが持つ固有の証明書情報も簡単に利用することができる。

【００４９】

また、上記のように、クライアントが暗号化メールを受信した場合、この受信メールまたは受信メールより取出した暗号データ部分（ｆ）を暗号化装置１に送信し、復号化することができるが、この復号化を行う場合の暗号化装置１の作用を図１０のフローチャートにより説明する。

【００５０】

インターネットファクシミリ２（またはパソコン４）は自身のアカウント情報を用いてメールサーバ３より定期的に受信メールを受信し、受信メールの中に暗号化されているものがあるかどうかを判断し、暗号化メール（ｆ）が有った場合には、インターネットファクシミリ２はこの受信メールまたは受信メールから取り出した暗号データ部分を復号化装置１の復号化メールアドレス（decode@server.com）に向けて送信する。

【００５１】

そして、復号化装置１のデータ受信部２９が復号化メールアドレス（decode@server.com）を介してデータ（ｇ）を受信すると、制御部２１は図１０のフローチャートに示す復号化プログラムを開始し、まず受信したデータが電子メールか否かを判定する（ステップ３０１）。受信したデータが電子メールであると判定した場合には、制御部２１は受信した電子メールが暗号化メールか否かを判定し（ステップ３０２）、暗号化メールでないと判定した場合には、ステップ３０４に移る。一方、ステップ３０２で受信した電子メールが暗号化メールであると判定した場合には、制御部２１は復号化部２６により暗号化メールを復号化させる（ステップ３０３）。すなわち、復号化部２６は証明書情報管理部２２に記憶されている秘密鍵を用いて暗号化メールを電子メールに復号化する。

【００５２】

次に、制御部２１は電子メールに電子署名が添付されているか否かを判定し（ステップ３０４）、電子署名が添付されていないと判定した場合には、ステップ３０６に移る。一

方、電子署名が添付されていると判定した場合には、制御部２１は電子署名検証部２８により電子署名の検証を実行させ、検証結果を復号化した電子メールに付加する（ステップ３０５）。すなわち、電子署名検証部２８は相手先情報管理部２３に記憶されている電子メールの送信元の公開鍵を利用して電子署名を復号化してメッセージダイジェストを生成する。次に、電子署名検証部２８は復号化した電子メール全体から送信元と同じハッシュ関数にてメッセージダイジェストを生成し、復号化した送信側メッセージダイジェストと電子メールから生成した受信側メッセージダイジェストを比較して一致するかどうかを判定することにより、電子メールの改ざんの有無を判断する。この判断結果により、制御部２１が復号化した電子メールに電子署名検証結果、例えば、「このメールは正当なメールです。」等のコメント及び署名内容を付加した後、復号化電子メール（ｈ）を受信先へ返送する（ステップ３０６）。

【００５３】

一方、ステップ３０１において、受信したデータが電子メールでなく、メール本文であると判定した場合には、制御部２１はメール本文が暗号化されているか否かを判定し（ステップ３０７）、暗号化されていないと判定した場合には、ステップ３０９に移る。一方、メール本文が暗号化されていると判定した場合には、制御部２１は復号化部２６により暗号化されているメール本文を復号化させる（ステップ３０８）。

【００５４】

次に、制御部２１はメール本文に電子署名が添付されているか否かを判定し（ステップ３０９）、電子署名が添付されていないと判定した場合には、ステップ３０６に移る。一方、電子署名が添付されていると判定した場合には、制御部２１は電子署名検証部２８により電子署名の検証を実行させ、検証結果を復号化したメール本文に付加した（ステップ３１０）後、復号化した電子メール本文（ｈ）を受信先へ返送する（ステップ３０６）。

【００５５】

以上のように、暗号化された電子メールまたはデータを暗号化装置に送信すれば、復号化されて返送されるので、インターネットファクシミリに復号化機能が含まれていなくとも、暗号化メールの復号化を行うことが可能となり、また、電子メールまたはデータが復号化されるとき、添付された署名情報が検証され、検証結果が復号化された電子メールまたはデータに付加されるので、暗号化メールの改ざんの有無を容易に確認することができる。

【００５６】

なお、上記の実施例では、暗号化装置にそれぞれ暗号化用のメールアドレス、復号化用のメールアドレスを設けて、インターネットファクシミリとの間で電子メールにより暗号化・復号化を行ったが、上記したように、暗号化装置にそれぞれ暗号化用のＵＲＬ、復号化用のＵＲＬを設けてインターネットファクシミリとの間でＨＴＴＰプロトコルにより暗号化・復号化を行うことも可能である。

【００５７】

また、上記の実施例では、暗号化装置にインターネットファクシミリから電子メールの暗号化処理や暗号化電子メールの復号化処理を依頼する例を説明したが、パソコン等の他のクライアントから暗号化処理や復号化処理を行わせるようにすることも可能である。

【００５８】

さらに、上記の実施例では、電子署名を付与するか否かをユーザによる暗号化装置への設定により決定するようにしたが、クライアントから電子署名を付与するか否かを別途指示するようにすることも可能である。

【図面の簡単な説明】

【００５９】

【図１】本発明の暗号化装置が接続されるネットワーク構成の一例を示す図である。

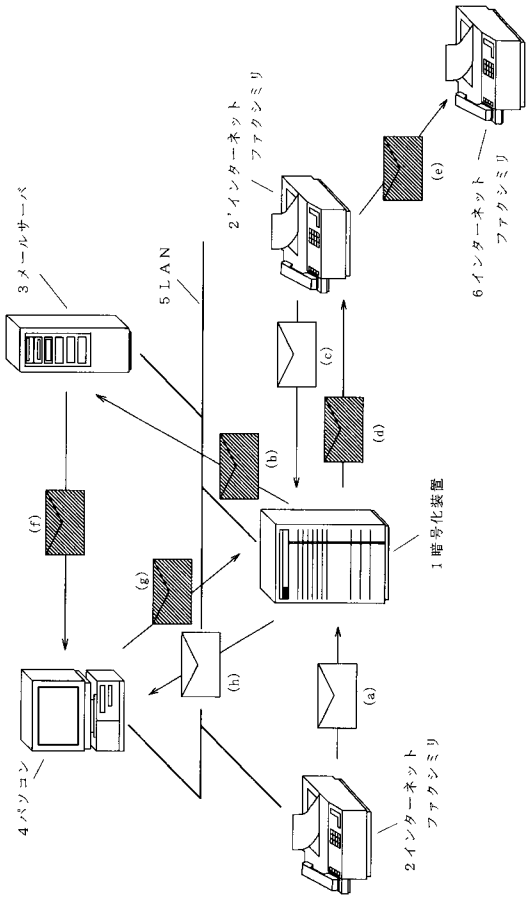
【図２】本発明の暗号化装置のハードウェア構成を示すブロック図である。

【図３】本発明の暗号化装置の構成を示す機能ブロック図である。

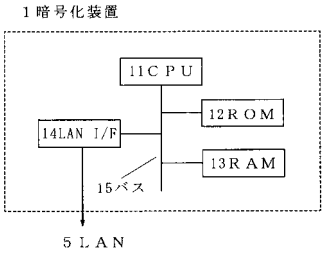
【図４】証明書情報管理部に登録される証明書情報の一例を示す図である。

【図５】相手先情報管理部に登録される情報の一例を示す図である。
【図６】暗号化装置に割り当てられる、暗号化用のメールアドレス、復号化用のメールアドレスの一例を示す図である。
【図７】暗号化装置に割り当てられる暗号化用のＵＲＬ、復号化用のＵＲＬの一例を示す図である。
【図８】電子メールまたはメール本文を暗号化する場合の暗号化装置の作用を示すフローチャートである。
【図９】クライアント固有の証明書情報を使用して電子署名を生成する場合の暗号化装置の作用を示すフローチャートである。
【図１０】暗号化メールまたはメールより取出した暗号データ部分を復号化する場合の暗号化装置の作用を示すフローチャートである。
【符号の説明】
【００６０】
１　暗号化装置
２、２’、６　インターネットファクシミリ
３　メールサーバ
４　パソコン
５　ＬＡＮ
１１　ＣＰＵ
１２　ＲＯＭ
１３　ＲＡＭ
１４　ＬＡＮ　Ｉ／Ｆ
２１　制御部
２２　証明書情報管理部
２３　相手先情報管理部
２４　メールサーバ管理部
２５　暗号化部
２６　復号化部
２７　電子署名生成部
２８　電子署名検証部
２９　データ送受信部

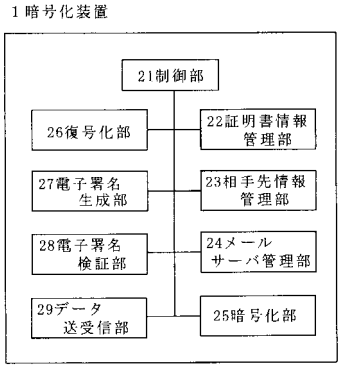
【図１】



【図２】



【図３】



【図４】

証明書情報

公開鍵	秘密鍵	認証局	有効期限	所有者
123456789	ABCDEFG	xxxｾｷｭﾘﾃｨ	2010/1/1	共有
987654321	MNLKIJHG	ooｾｷｭﾘﾃｨ	2006/1/1	ＰＣ１

【図５】

宛先アドレス帳管理テーブル

メールアドレス	公開鍵	認証局	有効期限
ifax@sample.com	123456789	xxxｾｷｭﾘﾃｨ	2010/1/1
pc2@sample.com	685423795	xxxｾｷｭﾘﾃｨ	2010/1/1

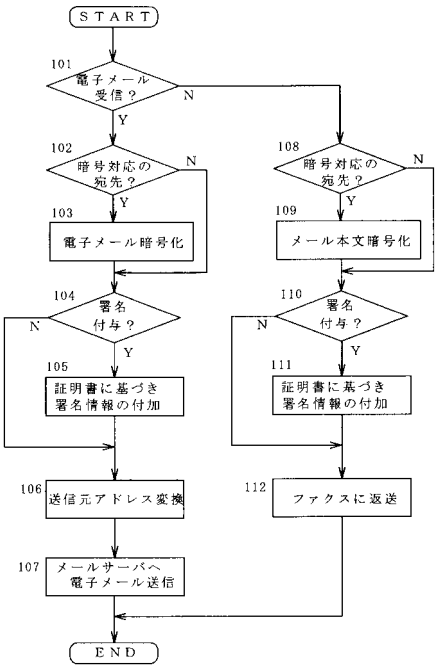
【図６】

復号化メールアドレス	暗号化メールアドレス
decode@server.com	encode@server.com

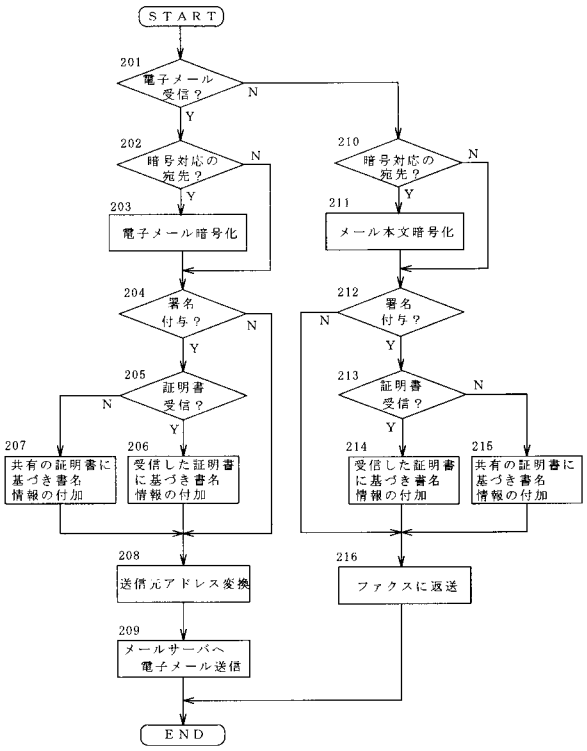
【図７】

復号化ＵＲＬ	暗号化ＵＲＬ
www.server/decode.cgi	www.server/encode.cgi

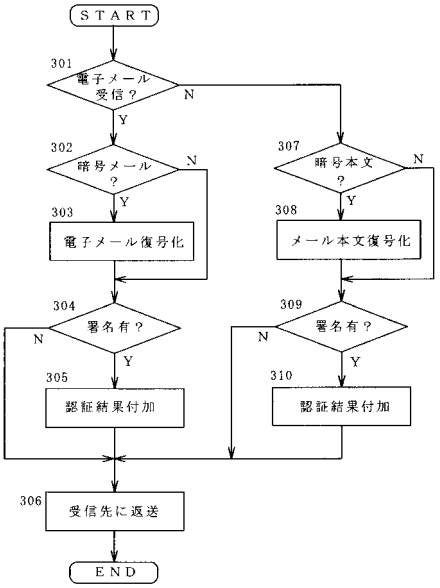
【図８】



【図９】


START
201
電子メール受信？
N
Y
202
暗号対応の宛先？
N
Y
203
電子メール暗号化
204
署名付与？
N
Y
205
証明書受信？
N
Y
207
共有の証明書に基づき書名情報の付加
206
受信した証明書に基づき書名情報の付加
208
送信元アドレス変換
209
メールサーバへ電子メール送信
210
暗号対応の宛先？
N
Y
211
メール本文暗号化
212
署名付与？
N
Y
213
証明書受信？
N
Y
214
受信した証明書に基づき書名情報の付加
215
共有の証明書に基づき書名情報の付加
216
ファクスに返送
END

【図１０】


START
301
電子メール受信？
N
Y
302
暗号メール？
N
Y
303
電子メール復号化
304
署名有？
N
Y
305
認証結果付加
307
暗号本文？
N
Y
308
メール本文復号化
309
署名有？
N
Y
310
認証結果付加
306
受信先に返送
END

フロントページの続き

審査官　青木　重徳

(56)参考文献　特開２００１－３２０４０３（ＪＰ，Ａ）
特開平１１－１５０５５４（ＪＰ，Ａ）
特開２００２－０２４１４７（ＪＰ，Ａ）
特開平１１－１７５４１９（ＪＰ，Ａ）
特開２００１－１１１６０６（ＪＰ，Ａ）
特開２００１－３２０３６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　１２／５８