(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2010-22010
(P2010-22010A)
(43)公開日　平成22年1月28日(2010.1.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5B084
G06F 13/00	(2006.01)	H04L	9/00	601E	5J104
		H04L	9/00	601F	
		G06F	13/00	610S	

審査請求 未請求　請求項の数 13　ＯＬ　（全 54 頁）

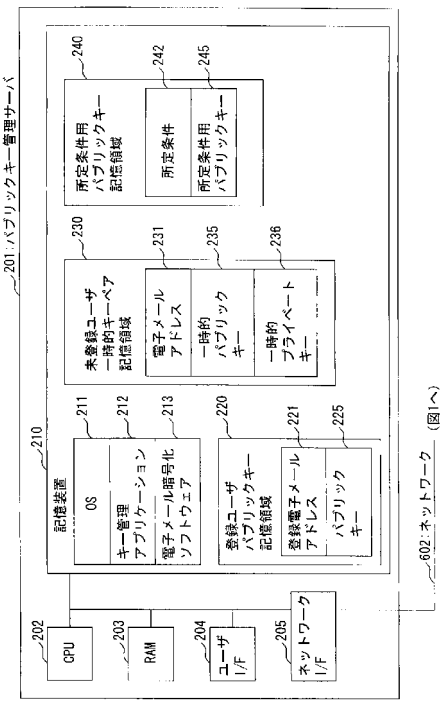
(21)出願番号　特願2009-188045 (P2009-188045)
(22)出願日　平成21年8月14日 (2009.8.14)
(62)分割の表示　特願2009-507253 (P2009-507253)の分割
原出願日　平成20年5月15日 (2008.5.15)
(31)優先権主張番号　12/072,006
(32)優先日　平成20年2月21日 (2008.2.21)
(33)優先権主張国　米国 (US)

(71)出願人　509044084
Ｚｅｎｌｏｋ株式会社
東京都中央区銀座１丁目１５番１３号９０４
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之
(74)代理人　100120525
弁理士　近藤　直樹

最終頁に続く

(54)【発明の名称】電子メール暗号化システム

(57)【要約】
【課題】未登録ユーザに暗号化メールを送信する。また、本来の宛先のメール受信端末に加えて所定条件メール代表受信端末でも暗号化メールを復号できるようにする。
【解決手段】未登録ユーザに電子メールを送信する際に、一時的パブリックキーとプライベートキーをサーバで生成し、一時的パブリックキーをサーバからメール送信端末に送り、それを用いてメールを暗号化させ、一時的プライベートキーをサーバからメール受信端末に送り、それを用いて暗号化メールを復号させる。また、所定条件を満たすメールアドレスに対しては、当該メールアドレスに対応するパブリックキーに加えて、当該所定条件に対応する所定条件用パブリックキーを対応付けて公開することにより、所定条件を満たすメールアドレスを宛先とするメールを代表受信端末で復号させる。
【選択図】図２



【特許請求の範囲】
【請求項１】
電子メール暗号化のためのパブリックキーが登録されておらず、ユーザとしてあらかじめ登録されていない受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号させるための、前記電子メール送信端末及び前記電子メール受信端末とネットワークで接続されたパブリックキー管理サーバを含む、電子メール暗号化システムであって、
前記パブリックキー管理サーバは、
端末からの電子メール暗号化ソフトウェアのダウンロード要求に応じて前記電子メール暗号化ソフトウェアを前記端末にダウンロードさせるダウンロード手段と、
既登録ユーザの登録電子メールアドレスと、前記既登録ユーザの端末のためにプライベートキーとのペアとして生成したパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、
未登録ユーザの電子メールアドレスを、一時的パブリックキーと一時的プライベートキーとのペアと対応させて記憶する未登録ユーザ一時的キーペア記憶領域と、を有し、
前記電子メール送信端末は、
前記パブリックキー管理サーバからあらかじめ取得した、前記既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それに対応する登録電子メールアドレスとを対応させて記憶する送信端末内パブリックキー記憶領域と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、
前記電子メール送信端末は、前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、
前記送信端末内パブリックキー記憶領域に対して、前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、
前記パブリックキー管理サーバに対して、前記受信者電子メールアドレスのうちで、少なくとも前記送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、を実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール送信端末から前記受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、前記登録ユーザパブリックキー記憶領域に対して、前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、既登録ユーザの登録電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、
前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのうちで、前記受信者パブリックキー検索手段による問い合わせにより前記登録ユーザパブリックキー記憶領域に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを前記未登録ユーザ一時的キーペア記憶領域に記憶させる一時的キーペア生成記憶領域と、
前記受信者パブリックキー検索手段で取得された前記既登録ユーザのためのパブリック

キー、及び前記一時的キーペア生成記憶領域で生成された前記未登録ユーザのための前記一時的パブリックキーを前記電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、

前記電子メール送信端末は、

前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

前記パブリックキー管理サーバから送信された前記既登録ユーザのためのパブリックキーを、それに対応する登録電子メールアドレスと対応させて前記送信端末内パブリックキー記憶領域にさらに記憶させる受信者パブリックキー記憶領域と、

電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、

前記電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる前記受信者電子メールアドレスを宛先とする電子メールのコンテンツを前記コンテンツ暗号化キーで暗号化する電子メールコンテンツ暗号化手段と、

前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記パブリックキー管理サーバから送信された既登録ユーザのパブリックキー及び前記未登録ユーザのための一時的パブリックキーのそれぞれで公開鍵方式によって暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、

前記電子メールコンテンツ暗号化手段によって暗号化された前記電子メールのコンテンツに、前記コンテンツ暗号化キー暗号化手段によって生成された前記暗号化されたコンテンツ暗号化キーのそれぞれを添付し、さらに前記電子メールのコンテンツが暗号化されていることが識別可能な情報を暗号化せずに添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、

前記暗号化電子メールを前記受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、

前記電子メール受信端末は、

前記電子メール送信端末から送信された前記暗号化電子メールを受信し、それに含まれる前記電子メールのコンテンツが暗号化されていることが識別可能な情報を表示するコンテンツ情報表示手段と、

前記電子メール暗号化ソフトウェアを前記ダウンロード手段からダウンロードして記憶する受信端末内ソフトウェア記憶領域と、を有し、

前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

前記受信した暗号化電子メールの前記受信者電子メールアドレスに対応する前記一時的プライベートキーを前記パブリックキー管理サーバに要求する一時的プライベートキー要求手段と、を実現するものであり、

前記パブリックキー管理サーバは、

前記電子メール受信端末からの前記受信者電子メールアドレスに対応する一時的プライベートキーの要求を受信すると、前記未登録ユーザ一時的キーペア記憶領域から前記受信者電子メールアドレスに対応する一時的プライベートキーを取得する受信者一時的プライベートキー検索手段と、

前記受信者一時的プライベートキー検索手段で取得された一時的プライベートキーを前記電子メール受信端末に送信する一時的プライベートキー送信手段と、をさらに有し、

前記電子メール受信端末は、

前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

前記受信者電子メールアドレスに対応する前記暗号化されたコンテンツ暗号化キーを前記パブリックキー管理サーバから送信された一時的プライベートキーを用いて復号し、前

記コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであることを特徴とする、電子メール暗号化システム。
【請求項２】
請求項１に記載の電子メール暗号化システムにおいて、
前記電子メール暗号化手段によって暗号化されずに前記電子メールのコンテンツに添付される、暗号化されていることが識別可能な情報は、前記電子メール暗号化ソフトウェアのダウンロード手段のネットワーク上の位置を示す情報を含むことを特徴とする、電子メール暗号化システム。
【請求項３】
請求項１に記載の電子メール暗号化システムにおいて、
前記電子メール受信端末は、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスに対応する、新しいパブリックキーとプライベートキーのペアを生成させ、それらを対応づけて記憶させるキーペア生成記憶領域と、
前記生成されたパブリックキーを含む、前記受信者電子メールアドレスに対応するユーザ登録の要求を前記パブリックキー管理サーバに送信する生成パブリックキー送信手段と、をさらに実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール受信端末からの前記ユーザ登録の要求を受信すると、それに含まれる前記生成されたパブリックキーを前記受信者電子メールアドレスと対応づけて前記登録ユーザパブリックキー記憶領域にさらに記憶させる生成パブリックキー登録手段と、をさらに有することを特徴とする電子メール暗号化システム。
【請求項４】
請求項１に記載の電子メール暗号化システムにおいて、
前記送信端末内パブリックキー記憶領域は、前記パブリックキー管理サーバからあらかじめ取得した、所定の既登録ユーザの電子メールアドレスのそれぞれに対するパブリックキー、及び前記送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアを、それに対応する電子メールアドレスと対応させて記憶するものであり、
前記コンテンツ暗号化キー暗号化手段は、前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記パブリックキー管理サーバから送信された前記既登録ユーザのパブリックキー及び前記未登録ユーザのための一時的パブリックキー、並びに前記送信者電子メールアドレスに対応するパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するものであることを特徴とする電子メール暗号化システム。
【請求項５】
請求項１に記載の電子メール暗号化システムにおいて、
前記一時的キーペア生成記憶領域は、前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのうちで、前記受信者パブリックキー検索手段による問い合わせにより前記既登録ユーザパブリックキー記憶領域に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、そこへ暗号化電子メールを送信するか否かの確認を前記電子メール送信端末に行い、送信する旨の応答があったことを条件として、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを前記未登録ユーザ一時的キーペア記憶領域に記憶させるものである電子メール暗号化システム。
【請求項６】
ユーザとして登録された受信者電子メールアドレスを宛先として、電子メール暗号化ソ

フトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号し、前記受信者電子メールアドレスが所定の条件を満たす場合には、任意の前記所定の条件を満たす受信者電子メールアドレスを宛先とする暗号化電子メールを、前記所定の条件を満たす受信者電子メールアドレスを宛先とする前記暗号化電子メールの少なくとも一部を受信することができる所定条件電子メール代表受信端末で復号することができるようにするための、前記電子メール送信端末、前記電子メール受信端末、及び前記所定条件電子メール代表受信端末とネットワークで接続されたパブリックキー管理サーバを含む、電子メール暗号化システムであって、

前記パブリックキー管理サーバは、

登録された既登録ユーザの登録電子メールアドレスと、１つ以上のパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、

前記所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを対応させて記憶する所定条件用パブリックキー記憶領域と、

電子メールアドレスとそれと対応するパブリックキーの前記登録ユーザパブリックキー記憶領域への登録の要求を受け付け、前記登録ユーザパブリックキー記憶領域に登録が要求された前記電子メールアドレスと前記パブリックキーとを対応させて記憶させるとともに、登録が要求された前記電子メールアドレスが前記所定条件用パブリックキー記憶領域に記憶された前記所定の条件を満たすかどうかを判断し、前記所定の条件を満たす場合は、登録が要求された前記電子メールアドレスに、前記所定の条件に対応する前記所定条件用パブリックキーをさらに対応可能に前記登録ユーザパブリックキー記憶領域に記憶させる所定条件電子メールアドレス登録手段と、

を有し、

前記電子メール送信端末は、

前記パブリックキー管理サーバからあらかじめ取得した、前記既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それに対応する登録電子メールアドレスとを対応可能に記憶する送信端末内パブリックキー記憶領域と、

前記電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、

前記電子メール送信端末は、前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、

前記送信端末内パブリックキー記憶領域に対して、前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、

前記パブリックキー管理サーバに対して、前記受信者電子メールアドレスのうちで、少なくとも前記送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、

を実現するものであり、

前記パブリックキー管理サーバは、

前記電子メール送信端末から前記受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、前記登録ユーザパブリックキー記憶領域に対して、前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのそれぞれが記憶されているかどうかを問い合わせ、登録ユーザの電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、

前記受信者パブリックキー検索手段で取得された前記登録ユーザのためのパブリックキーを前記電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、
前記電子メール送信端末は、
前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記パブリックキー管理サーバから送信された前記登録ユーザのためのパブリックキーを、それに対応する電子メールアドレスと対応させて前記送信端末内パブリックキー記憶領域にさらに記憶させる受信者パブリックキー記憶領域と、
電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、
前記電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる前記受信者電子メールアドレスを宛先とする電子メールのコンテンツを前記コンテンツ暗号化キーで暗号化する電子メールコンテンツ暗号化手段と、
前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記送信端末内パブリックキー記憶領域に記憶されたパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、
前記電子メールコンテンツ暗号化手段によって暗号化された前記電子メールのコンテンツに、前記コンテンツ暗号化キー暗号化手段によって生成された前記暗号化されたコンテンツ暗号化キーのそれぞれを添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、
前記暗号化電子メールを前記受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、
前記電子メール受信端末は、
前記電子メール送信端末から送信された前記暗号化電子メールを受信する電子メール受信手段と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された受信端末内ソフトウェア記憶領域と、
前記電子メール受信端末が受信する前記受信者電子メールアドレスに対するパブリックキーとペアをなす前記プライベートキーと、前記受信者電子メールアドレスとを対応させて記憶する受信端末内プライベートキー記憶領域と、を有し、
前記電子メール受信端末は、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスに対応する前記暗号化されたコンテンツ暗号化キーを前記受信端末内プライベートキー記憶領域に記憶されたプライベートキーを用いて復号し、前記コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであり、
前記所定条件電子メール代表受信端末は、
前記電子メール送信端末から送信された前記所定の条件を満たす前記暗号化電子メールの少なくとも一部を受信する代表受信端末内電子メール受信手段と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された代表受信端末内ソフトウェア記憶領域と、
前記所定条件電子メール代表受信端末が受信する前記受信者電子メールアドレスが満たす前記所定の条件に対する前記所定条件用パブリックキーとペアをなす所定条件用プライベートキーを記憶する代表受信端末内プライベートキー記憶領域と、を有し、
前記所定条件電子メール代表受信端末は、

前記代表受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスが満たす前記所定の条件に対応する前記暗号化されたコンテンツ暗号化キーを前記代表受信端末内プライベートキー記憶領域に記憶された前記所定条件用プライベートキーを用いて復号し、前記コンテンツ暗号化キーを回復する所定条件用コンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる所定条件用暗号化電子メール復号手段と、をさらに実現するものであることを特徴とする、電子メール暗号化システム。

【請求項７】

請求項６に記載の電子メール暗号化システムにおいて、前記パブリックキー管理サーバは、
新しい所定の条件とそれと対応する所定条件用パブリックキーの前記所定条件用パブリックキー記憶領域への追加の要求を受け付け、前記所定条件用パブリックキー記憶領域に登録が要求された前記新しい所定の条件と前記所定条件用パブリックキーとを対応させて記憶させるとともに、
前記登録ユーザパブリックキー記憶領域に記憶された前記登録ユーザの電子メールアドレスのそれぞれが、追加の要求がされた前記所定の条件を満たすかどうかを判断し、前記所定の条件を満たす場合は、前記所定の条件を満たす電子メールアドレスに、前記所定の条件に対応する前記所定条件用パブリックキーをさらに対応可能に前記登録ユーザパブリックキー記憶領域に記憶させる所定条件用パブリックキー追加手段、をさらに有することを特徴とする電子メール暗号化システム。

【請求項８】

請求項６に記載の電子メール暗号化システムにおいて、
前記登録ユーザの電子メールアドレスとそれに対応づけられたパブリックキーは、前記パブリックキー管理サーバによるデジタル署名が付加された電子証明書に含まれる情報として取り扱われるものであり、前記電子メール受信端末において前記デジタル署名が検証されることにより受信した暗号化電子メールの電子メールアドレスが前記パブリックキー管理サーバに真正に登録されたものであることを確認できるようになっていることを特徴とする電子メール暗号化システム。

【請求項９】

請求項８に記載の電子メール暗号化システムにおいて、
前記端末内受信者パブリックキー取得手段によるパブリックキーの取得の前に、それぞれの前記電子証明書が最新のものであるかどうかを前記パブリックキー管理サーバに問い合わせ、最新のものでなかった場合は最新のものを前記パブリックキー管理サーバから取得してそれで前記送信端末内パブリックキー記憶領域を更新する前記端末内受信者パブリックキー最新確認手段をさらに有することを特徴とする電子メール暗号化システム。

【請求項１０】

請求項９に記載の電子メール暗号化システムにおいて、
前記電子証明書が最新のものであるかどうかの前記パブリックキー管理サーバへの問い合わせは、前回の問合わせから所定のキャッシュ保持期間が経過したことを条件として行われることを特徴とする電子メール暗号化システム。

【請求項１１】

請求項６に記載の電子メール暗号化システムにおいて、
前記電子メール送信端末は、前記送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアと、前記送信者電子メールアドレスとを対応させて記憶する送信端末内プライベートキー記憶領域、をさらに有し、
前記電子メール送信端末は、前記送信者電子メールアドレスを発信元とし、前記受信者電子メールアドレスを宛先とする暗号化電子メールに対して前記プライベートキーを利用したデジタル署名を付加するものであり、前記電子メール受信端末において前記デジタル

署名が検証されることにより受信した暗号化電子メールのコンテンツの真正性が確認されることを特徴とする電子メール暗号化システム。
【請求項１２】
請求項１１に記載の電子メール暗号化システムにおいて、
前記電子メール受信端末における前記デジタル署名の検証は、前記パブリックキー管理サーバから取得したパブリックキーによって行われるものであり、それによって、受信した暗号化電子メールの送信者が前記パブリックキー管理サーバに真正に登録されたユーザであることがさらに確認されることを特徴とする電子メール暗号化システム。
【請求項１３】
請求項６に記載の電子メール暗号化システムにおいて、
前記所定の条件は、前記受信者電子メールアドレスが所定のドメインに所属するものであることを特徴とする電子メール暗号化システム。
【請求項１４】
請求項１３に記載の電子メール暗号化システムにおいて、
前記パブリックキー管理サーバは、所定の管理料金が支払われた前記所定のドメインに対して、前記所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを、前記所定条件用パブリックキー記憶領域に、対応させて記憶することを特徴とする電子メール暗号化システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般には電子メールの暗号化方法及び装置に関し、さらに詳細には、秘密鍵（プライベートキー、暗号解読鍵）を持たないユーザへも暗号化電子メールの送信を可能とし、かつ該メールの受信者による解読を可能とする、そして前記秘密鍵のドメイン内一元管理を可能とする、電子メールの暗号化方法及び装置に関する。本発明においては、さらに詳細には、送信者と同一の、または対応する電子メール暗号化ソフトウェアをあらかじめ導入しておらず、かつ自己の暗号鍵（公開鍵方式においては、パブリックキーとプライベートキーのペア）をあらかじめ持たない受信者に対しても、暗号化された電子メールの送信を可能とし、かつ該メールの受信者による復号を可能とするような、また、特定のドメイン（サーバのアドレス）に所属するというような、所定の条件に合致する任意の電子メールアドレスに所属する送受信者によって送受信される暗号化された電子メールを、その送受信者のみならず該ドメインの管理者（例えば会社、会社内特定部署、その他一般の電子メールユーザによって構成される特定のグループであってよく、特定の管理者によって管理されることを想定されている）によっても復号できるものとするような、電子メールの暗号化方法及び装置が提供される。
【０００２】
近年、通信手段としての電子メールは、私用商用を問うことなく幅広い普及を見せている。重要な情報が電子メールを用いて送受信されることも増えるに伴い、電子メール送受信における様々な危険性に対処することへの要請が高まっている。すなわち、コンテンツのネットワーク盗聴による個人情報の盗難、偽装した電子メールによるフィッシング詐欺などの危険性が高まっており、それに対する対処が広く求められている。
【０００３】
そのような危険性への対処方法の１つとして、電子メールの暗号化が挙げられる。すなわち、電子メールのコンテンツを、特定の暗号鍵を用いて暗号化した後に送信するものである。暗号化されたコンテンツは、前記特定の暗号鍵に対応した特定の復号鍵をもってのみ、本来のコンテンツに復号することができる。復号鍵は、電子メールの受信者のように、本来のコンテンツにアクセスすることが意図された者のみが保持することを前提としている。これにより、仮に悪意ある第三者に該電子メールを受信されたとしても、その第三者が復号鍵を有していない限り本来のコンテンツに復号することはできず、従って情報流出を回避できるというものである。

【０００４】
従来より知られている暗号鍵の方式として、共通鍵方式と公開鍵方式が挙げられる。共通鍵方式においては、暗号化と復号に同一の鍵を用いる。共通鍵方式で暗号化された電子メールのコンテンツは、暗号化に用いた暗号鍵と同じ鍵を復号鍵として用いることで、復号することができる。
【０００５】
公開鍵方式においては、暗号化に用いる暗号鍵（公開鍵：パブリックキー）と復号に用いる復号鍵（秘密鍵：プライベートキー）は別個のものとなる。特定のパブリックキーで暗号化された電子メールのコンテンツは、それとペアを成す特定のプライベートキーを用いることによってのみ、復号することができる。ここで、パブリックキーあるいはプライベートキーのいずれか一方から、他のキーを導くことは事実上不可能である。従って、電子メールの受信者は自己のプライベートキーを手元に管理しておき、パブリックキーを電子メールの送信者に公開して、それによって電子メールを暗号化させることによって、自分以外は復号できない暗号化された電子メールを安全かつ簡便に受信することができる。
【０００６】
本発明が提供する方法及び装置は、主に公開鍵方式を利用するものであるので、公開鍵方式による暗号化電子メールの送受信、暗号化及び復号において従来一般に用いられている構成をこれから説明する。
【０００７】
まず、電子メールを送信する端末、受信する端末のそれぞれに、公開鍵方式での暗号化及び復号を行うための暗号化ソフトウェアがあらかじめ導入されていることが必要である。そのような暗号化ソフトウェアは、電子メール送受信ソフトウェア（電子メールクライアント）にあらかじめ組み込まれた機能拡張用モジュールであってもよいし、単独のソフトウェアであってもよい。両端末に同一のソフトウェアが導入されていることは一般には要求されないものの、少なくとも受信端末においては、送信端末が暗号化に用いる特定の公開鍵方式（ＲＳＡ（登録商標）方式、ＥｌＧａｍａｌ方式など複数のアルゴリズムが存在する）に対応したソフトウェアをあらかじめ導入していることが必要である。
【０００８】
次に、少なくとも受信端末においては、受信者が用いるべきパブリックキーとプライベートキーのペアをあらかじめ所定のアルゴリズムにより生成し、保持していることが必要となる。電子メールのコンテンツは前記受信者のパブリックキーを用いて暗号化され、前記受信者のプライベートキーを用いて、暗号化された電子メールのコンテンツは復号される。
【０００９】
前記送信端末は、電子メールを暗号化するために、受信者があらかじめ生成し、保持している前記受信者のパブリックキーを、あらかじめ何らかの方法で取得していることが必要となる。
【００１０】
受信者のパブリックキーの取得は、例えば電子メールにパブリックキーを添付してあらかじめ受け渡ししておくことや、適切な管理下にある公開サーバに前記パブリックキーをあらかじめアップロードしておき、送信者が該公開サーバから該パブリックキーをあらかじめ取得しておくことなどによって行われる。
【００１１】
送信者は、受信者に送信しようとする電子メールのコンテンツを、あらかじめ取得した受信者のパブリックキーを用いて、あらかじめ導入された暗号化ソフトウェアによって暗号化し、受信者にメールサーバを介して送信する。
【００１２】
受信者は暗号化された電子メールを受信し、あらかじめ生成した自己のプライベートキーを用いて、受信端末にあらかじめ導入された前記暗号化ソフトウェアによって復号する。このような公開鍵方式の暗号化を利用したシステムでは、暗号化電子メールは、理論的

に、プライベートキーを有している送信者しか復号することができないため、共通鍵方式の暗号化を利用したシステムと比べ、鍵の管理が簡単であり、安全性が高い。

【先行技術文献】

【非特許文献】

【００１３】

【非特許文献１】米国特許第７１７４３６８号

【発明の概要】

【発明が解決しようとする課題】

【００１４】

しかし、上述したような従来の公開鍵方式の暗号化を利用した構成においては、次のような問題があった。すなわち、電子メールのコンテンツを暗合化して受信者に送信する際、送信者は送信端末にあらかじめ受信者のパブリックキーを取得しておく必要があり、また、、それぞれの受信者は受信端末に、対応する暗号化ソフトウェアをあらかじめ導入し、そして受信者のパブリックキーを送信者にあらかじめ取得させる必要があるということである。

特に、例えば顧客リスト上の全ての電子メールアドレスに対して暗号化したメールを送信する場合などのように、送信先が多数である場合に、全ての受信端末において対応するソフトウェアが導入され、それらのそれぞれの受信端末のパブリックキーを取得するまで送信を待つことは非現実的である。

【００１５】

このような公開鍵方式の問題に対して、色々な試みがなされてきた。例えば、受信端末にあらかじめｒｅａｄｅｒ／ｒｅｓｐｏｎｄｅｒ ｓｏｆｔｗａｒｅ ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｇｒａｍを導入することで、前記のような暗号化電子メールの送信に際して、あらかじめしなくてはならない手順の自動化、簡略化を図る発明がある（非特許文献１）。

【００１６】

この発明によれば、従来であれば、受信端末において用いる電子メール送受信ソフトウェアを送信者の用いる暗号方式に対応したものへの変更が必要となることがあったが、ｒｅａｄｅｒ／ｒｅｓｐｏｎｄｅｒ ｓｏｆｔｗａｒｅ ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｇｒａｍを補助的ソフトウェアとして導入することにより、受信後の復号、または送信前の暗号化をその補助的ソフトウェアが実施することとなるため、受信者において、電子メール送受信ソフトウェアを変更する必要がなくなる。送受信は、通常の電子メールクライアントソフトウェアによって行われ、暗号化に関連した処理はその補助的ソフトウェアによって行われる。

【００１７】

またｒｅａｄｅｒ／ｒｅｓｐｏｎｄｅｒ ｓｏｆｔｗａｒｅ ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｇｒａｍは、受信者から送信者へパブリックキーを事前に送信する機能も有しており、これによって、受信者が暗号化電子メールを受け取る前に必要となる事前の準備作業の労力が軽減される。

【００１８】

しかしながら、この発明によっても、ｒｅａｄｅｒ／ｒｅｓｐｏｎｄｅｒ ｓｏｆｔｗａｒｅ ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｇｒａｍは、暗号化された電子メールの送受信の前に、あらかじめ受信端末に導入されている必要がある。これは、暗号化電子メールが送られてくることを想定していない受信者に対しては、暗号化電子メールを送信することができないことを意味している。また、受信者のパブリックキーを送信者が事前に取得する手順についても、ソフトウェアによる労力の軽減が図られてはいるものの、依然としてそれが必要であることに変わりはない。

【００１９】

従って、この発明によっても、受信端末における暗号化ソフトウェアの事前の導入と送信者による受信者のパブリックキーの事前の取得が、暗号化電子メール送受信に先立って

必要であるという点においては従来の技術と変わりはない。

【００２０】

また従来の電子メール暗号化システムにおいては、次のような不都合もあった。すなわち、特定の受信者に対して送信された、受信者のパブリックキーを用いて暗号化された暗号化電子メールは、その受信者のプライベートキーを持たない者によっては復号できないために、それの電子メールアドレスが所属するドメインのコンピュータシステムの管理者であっても、そのドメインに所属する電子メールユーザーの送受信する電子メールについては、それが暗号化されていれば、復号することができず、十分な管理をすることができない。

【００２１】

公開鍵形式におけるパブリックキーとプライベートキーは完全に１対１で対応しており、特定のパブリックキーで暗号化された電子メールは、それとペアを成す特定のプライベートキーを用いてのみ復号することができる。このことは公開鍵方式の安全性と利便性を保証する上での基本となる性質でもある。

【００２２】

一方で、例えば会社組織においては、全社員の送受信する電子メールを特定の管理者が閲覧し、一元的に管理するという運用も、日常的に行われている。しかしながら、公開鍵方式で暗号化された電子メールについては、管理者であっても、受信者のプライベートキーを持たない限りは復号ができないのであり、この点で公開鍵方式においては、管理者によるドメイン内等の電子メールの一元管理は、暗号化とは両立できないという不都合があった。

【００２３】

このように、従来の公開鍵を利用した電子メール暗号化システムでは、暗号化電子メールを生成して送信するためには、事前に送信者の端末に受信者のパブリックキーを記憶させておく必要があるため、それを行っていない受信者には暗号化電子メールを送信することができなかった。また、送信者と受信者の端末のそれぞれに、暗号化を行うためのソフトウェアを事前に導入しておく必要があった。また、暗号化電子メールは、それの暗号化に利用されたパブリックキーとペアをなすプライベートキーが記憶された受信者の端末でなければ復号できないため、その受信者以外の者は、管理者であっても暗号化電子メールの内容を確認することができないという問題があった。

【００２４】

本発明は上記の課題に鑑みてなされたものであり、公開鍵を利用した電子メール暗号化システムであって、未登録のユーザに暗号化電子メールを送信し、復号させることができるシステムや、所定の条件を満たす電子メールアドレスを宛先とする暗号化電子メールを、その本来の宛先以外の場所で復号することを可能とするシステム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】

【００２５】

本発明は、上記の課題を解決するために以下のような特徴を有している。本発明の構成においては、パブリックキー管理サーバを導入する。そのパブリックキー管理サーバは、電子メール暗号化ソフトウェアのユーザとして登録された電子メールアドレスに対してのパブリックキーを含む情報を記憶する、登録ユーザパブリックキー記憶領域を有すると共に、未登録ユーザのための一時的パブリックキーを含む情報を記憶する、未登録ユーザパブリックキー記憶領域を有する。

【００２６】

登録ユーザから未登録の電子メールアドレスに対して暗号化電子メールを送信する際には、まずパブリックキー管理サーバにおいて該受信者電子メールアドレスのための一時的キーペアが生成されるように構成される。

【００２７】

次に、一時的キーペアのうち一時的パブリックキーが、電子メール送信端末によって取

得される。送信者は該一時的パブリックキーを用いて、電子メールのコンテンツを暗号化し、受信者に対して送信する。

【００２８】

受信者は、受信者電子メールアドレスを用いて暗号化された電子メールを受信する。暗号化された電子メールには、復号に必要な電子メール暗号化ソフトウェアのダウンロード手段のネットワーク上の位置を好適には示す暗号化されていることが識別可能な情報が暗号化せず添付されており、受信者はあらかじめ、電子メールの暗号化と復号を行うための電子メール暗号化ソフトウェアを導入していなくとも、受信後にそれを導入することが可能となるように構成される。

【００２９】

また復号には一時的パブリックキーとペアを成す一時的プライベートキーが必要であるが、これについても受信者はパブリックキー管理サーバから、暗号化された電子メールの受信後に、取得可能であるように構成される。この取得は、受信後に受信端末に導入された電子メール暗号化ソフトウェアが実行されることにより行われるように構成される。

【００３０】

暗号化電子メールの送受信に先立っての、受信端末における暗号化ソフトウェアの事前の導入と送信者による受信者のパブリックキーの事前の取得は、共に不要となるような効果が得られるように構成される。

【００３１】

また本発明の他の構成においては、登録ユーザパブリックキー記憶領域に、それぞれの登録ユーザによって送受信される暗号化電子メールを管理するための情報である所定条件が、合わせて記憶されるように構成される。

【００３２】

所定条件とは、例えば登録ユーザの電子メールアドレスが所属するドメイン名であってよい。そして、そのドメイン名のためのパブリックキーとプライベートキーのペアが用意される。

【００３３】

登録ユーザに対して送信する電子メールを暗号化する際には、登録ユーザのためのパブリックキーのみでなく、登録ユーザが所属するドメインのためのパブリックキーも用いて、コンテンツの暗号化が行われるように構成される。ドメインのためのパブリックキーは、あらかじめパブリックキー管理サーバに登録され、そこから電子メール送信端末によって取得されるように構成される。

【００３４】

コンテンツの暗号化の方法は、まず、好適には共通鍵である別途生成した暗号化キーを用いてコンテンツ自体を暗号化し、その共通鍵を、登録ユーザのためのパブリックキーと所属ドメインのためのパブリックキーとでそれぞれ暗号化するように構成される。そして、それぞれの暗号化された暗号化キーを、送信すべき暗号化電子メールに添付するように構成される。

【００３５】

ドメイン管理者は、暗号化電子メールを代表受信端末で受信した上で、暗号化電子メールに添付された、ドメインのためのパブリックキーで暗号化された暗号化キーを、ドメイン管理者の代表受信端末にあらかじめ保持されたそのドメインのためのプライベートキーを用いて復号し、そして得られた暗号化キーを用いてコンテンツを復号することができるように構成される。

【００３６】

より詳細には、本発明は以下のような特徴を有する。

本発明は、電子メール暗号化のためのパブリックキーが登録されておらず、ユーザとしてあらかじめ登録されていない受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メー

ル送信端末から送信することにより、暗号化電子メールを受信する電子メール受信端末で暗号化電子メールを復号させるための、電子メール送信端末及び電子メール受信端末とネットワークで接続されたパブリックキー管理サーバを含み、

パブリックキー管理サーバは、

端末からの電子メール暗号化ソフトウェアのダウンロード要求に応じて電子メール暗号化ソフトウェアを端末にダウンロードさせるダウンロード手段と、

既登録ユーザの登録電子メールアドレスと、既登録ユーザの端末のためにプライベートキーとのペアとして生成したパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、

未登録ユーザの電子メールアドレスを、一時的パブリックキーと一時的プライベートキーとのペアと対応させて記憶する未登録ユーザ一時的キーペア記憶領域と、を有し、

電子メール送信端末は、

パブリックキー管理サーバからあらかじめ取得した、既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それに対応する登録電子メールアドレスとを対応させて記憶する送信端末内パブリックキー記憶領域と、

電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、

電子メール送信端末は、送信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、

送信端末内パブリックキー記憶領域に対して、受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、

パブリックキー管理サーバに対して、受信者電子メールアドレスのうちで、少なくとも送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、を実現するものであり、

パブリックキー管理サーバは、

電子メール送信端末から受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、登録ユーザパブリックキー記憶領域に対して、パブリックキーの要求に含まれる受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、既登録ユーザの登録電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、

パブリックキーの要求に含まれる受信者電子メールアドレスのうちで、受信者パブリックキー検索手段による問い合わせにより登録ユーザパブリックキー記憶領域に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを未登録ユーザ一時的キーペア記憶領域に記憶させる一時的キーペア生成記憶領域と、

受信者パブリックキー検索手段で取得された既登録ユーザのためのパブリックキー、及び一時的キーペア生成記憶領域で生成された未登録ユーザのための一時的パブリックキーを電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、

電子メール送信端末は、

送信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、

パブリックキー管理サーバから送信された既登録ユーザのためのパブリックキーを、それに対応する登録電子メールアドレスと対応させて送信端末内パブリックキー記憶領域に

さらに記憶させる受信者パブリックキー記憶領域と、
電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、
電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる受信者電子メールアドレスを宛先とする電子メールのコンテンツをコンテンツ暗号化キーで暗号化する電子メールコンテンツ暗号化手段と、
電子メールのコンテンツの暗号化に使用したコンテンツ暗号化キーを、受信者電子メールアドレスのそれぞれに対応する、パブリックキー管理サーバから送信された既登録ユーザのパブリックキー及び未登録ユーザのための一時的パブリックキーのそれぞれで公開鍵方式によって暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、
電子メールコンテンツ暗号化手段によって暗号化された電子メールのコンテンツに、コンテンツ暗号化キー暗号化手段によって生成された暗号化されたコンテンツ暗号化キーのそれぞれを添付し、さらに電子メールのコンテンツが暗号化されていることが識別可能な情報を暗号化せずに添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、
暗号化電子メールを受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、
電子メール受信端末は、
電子メール送信端末から送信された暗号化電子メールを受信し、それに含まれる電子メールのコンテンツが暗号化されていることが識別可能な情報を表示するコンテンツ情報表示手段と、
電子メール暗号化ソフトウェアをダウンロード手段からダウンロードして記憶する受信端末内ソフトウェア記憶領域と、を有し、
受信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信した暗号化電子メールの受信者電子メールアドレスに対応する一時的プライベートキーをパブリックキー管理サーバに要求する一時的プライベートキー要求手段と、を実現するものであり、
パブリックキー管理サーバは、
電子メール受信端末からの受信者電子メールアドレスに対応する一時的プライベートキーの要求を受信すると、未登録ユーザ一時的キーペア記憶領域から受信者電子メールアドレスに対応する一時的プライベートキーを取得する受信者一時的プライベートキー検索手段と、
受信者一時的プライベートキー検索手段で取得された一時的プライベートキーを電子メール受信端末に送信する一時的プライベートキー送信手段と、をさらに有し、
電子メール受信端末は、
受信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスに対応する暗号化されたコンテンツ暗号化キーをパブリックキー管理サーバから送信された一時的プライベートキーを用いて復号し、コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであることを特徴とする。

【００３７】

また本発明は、
電子メール暗号化手段によって暗号化されずに電子メールのコンテンツに添付される、暗号化されていることが識別可能な情報は、電子メール暗号化ソフトウェアのダウンロード手段のネットワーク上の位置を示す情報を含むように構成できる。

【００３８】
また本発明は、
電子メール受信端末は、
受信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスに対応する、新しいパブリックキーとプライベートキーのペアを生成させ、それらを対応づけて記憶させるキーペア生成記憶領域と、
生成されたパブリックキーを含む、受信者電子メールアドレスに対応するユーザ登録の要求をパブリックキー管理サーバに送信する生成パブリックキー送信手段と、をさらに実現するものであり、
パブリックキー管理サーバは、
電子メール受信端末からのユーザ登録の要求を受信すると、それに含まれる生成されたパブリックキーを受信者電子メールアドレスと対応づけて登録ユーザパブリックキー記憶領域にさらに記憶させる生成パブリックキー登録手段と、をさらに有するように構成できる。
【００３９】
また本発明は、
送信端末内パブリックキー記憶領域は、パブリックキー管理サーバからあらかじめ取得した、所定の既登録ユーザの電子メールアドレスのそれぞれに対するパブリックキー、及び送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアを、それに対応する電子メールアドレスと対応させて記憶するものであり、
コンテンツ暗号化キー暗号化手段は、電子メールのコンテンツの暗号化に使用したコンテンツ暗号化キーを、受信者電子メールアドレスのそれぞれに対応する、パブリックキー管理サーバから送信された既登録ユーザのパブリックキー及び未登録ユーザのための一時的パブリックキー、並びに送信者電子メールアドレスに対応するパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するものであるように構成できる。
【００４０】
また本発明は、
一時的キーペア生成記憶領域は、パブリックキーの要求に含まれる受信者電子メールアドレスのうちで、受信者パブリックキー検索手段による問い合わせにより既登録ユーザパブリックキー記憶領域に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、そこへ暗号化電子メールを送信するか否かの確認を電子メール送信端末に行い、送信する旨の応答があったことを条件として、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを未登録ユーザ一時的キーペア記憶領域に記憶させるものであるように構成できる。
【００４１】
別の観点に係る本発明は、
ユーザとして登録された受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、暗号化電子メールを受信する電子メール受信端末で暗号化電子メールを復号し、受信者電子メールアドレスが所定の条件を満たす場合には、任意の所定の条件を満たす受信者電子メールアドレスを宛先とする暗号化電子メールを、所定の条件を満たす受信者電子メールアドレスを宛先とする暗号化電子メールの少なくとも一部を受信することができる所定条件電子メール代表受信端末で復号することができるようにするための、電子メール送信端末、電子メール受信端末、及び所定条件電子メール代表受信端末とネットワークで接続されたパブリックキー管理サーバを含み、
パブリックキー管理サーバは、

登録された既登録ユーザの登録電子メールアドレスと、１つ以上のパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、
所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを対応させて記憶する所定条件用パブリックキー記憶領域と、
電子メールアドレスとそれと対応するパブリックキーの登録ユーザパブリックキー記憶領域への登録の要求を受け付け、登録ユーザパブリックキー記憶領域に登録が要求された電子メールアドレスとパブリックキーとを対応させて記憶させるとともに、登録が要求された電子メールアドレスが所定条件用パブリックキー記憶領域に記憶された所定の条件を満たすかどうかを判断し、所定の条件を満たす場合は、登録が要求された電子メールアドレスに、所定の条件に対応する所定条件用パブリックキーをさらに対応付け可能に登録ユーザパブリックキー記憶領域に記憶させる所定条件電子メールアドレス登録手段と、
を有し、
電子メール送信端末は、
パブリックキー管理サーバからあらかじめ取得した、既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それに対応する登録電子メールアドレスとを対応付け可能に記憶する送信端末内パブリックキー記憶領域と、
電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、
電子メール送信端末は、送信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、
送信端末内パブリックキー記憶領域に対して、受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、
パブリックキー管理サーバに対して、受信者電子メールアドレスのうちで、少なくとも送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、
を実現するものであり、
パブリックキー管理サーバは、
電子メール送信端末から受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、登録ユーザパブリックキー記憶領域に対して、パブリックキーの要求に含まれる受信者電子メールアドレスのそれぞれが記憶されているかどうかを問い合わせ、登録ユーザの電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、
受信者パブリックキー検索手段で取得された登録ユーザのためのパブリックキーを電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、
電子メール送信端末は、
送信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
パブリックキー管理サーバから送信された登録ユーザのためのパブリックキーを、それに対応する電子メールアドレスと対応させて送信端末内パブリックキー記憶領域にさらに記憶させる受信者パブリックキー記憶領域と、
電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、
電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる受信者電子メールアドレスを宛先とする電子メールのコンテンツをコンテンツ暗号化キーで暗号化す

る電子メールコンテンツ暗号化手段と、
電子メールのコンテンツの暗号化に使用したコンテンツ暗号化キーを、受信者電子メールアドレスのそれぞれに対応する、送信端末内パブリックキー記憶領域に記憶されたパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、
電子メールコンテンツ暗号化手段によって暗号化された電子メールのコンテンツに、コンテンツ暗号化キー暗号化手段によって生成された暗号化されたコンテンツ暗号化キーのそれぞれを添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、
暗号化電子メールを受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、
電子メール受信端末は、
電子メール送信端末から送信された暗号化電子メールを受信する電子メール受信手段と、
電子メール暗号化ソフトウェアがあらかじめ記憶された受信端末内ソフトウェア記憶領域と、
電子メール受信端末が受信する受信者電子メールアドレスに対するパブリックキーとペアをなすプライベートキーと、受信者電子メールアドレスとを対応させて記憶する受信端末内プライベートキー記憶領域と、を有し、
電子メール受信端末は、
受信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスに対応する暗号化されたコンテンツ暗号化キーを受信端末内プライベートキー記憶領域に記憶されたプライベートキーを用いて復号し、コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであり、
所定条件電子メール代表受信端末は、
電子メール送信端末から送信された所定の条件を満たす暗号化電子メールの少なくとも一部を受信する代表受信端末内電子メール受信手段と、
電子メール暗号化ソフトウェアがあらかじめ記憶された代表受信端末内ソフトウェア記憶領域と、
所定条件電子メール代表受信端末が受信する受信者電子メールアドレスが満たす所定の条件に対する所定条件用パブリックキーとペアをなす所定条件用プライベートキーを記憶する代表受信端末内プライベートキー記憶領域と、を有し、
所定条件電子メール代表受信端末は、
代表受信端末内ソフトウェア記憶領域に記憶された電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスが満たす所定の条件に対応する暗号化されたコンテンツ暗号化キーを代表受信端末内プライベートキー記憶領域に記憶された所定条件用プライベートキーを用いて復号し、コンテンツ暗号化キーを回復する所定条件用コンテンツ暗号化キー復号手段と、
復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる所定条件用暗号化電子メール復号手段と、をさらに実現するものであることを特徴とする。

【００４２】

また本発明は、
パブリックキー管理サーバは、

新しい所定の条件とそれと対応する所定条件用パブリックキーの所定条件用パブリックキー記憶領域への追加の要求を受け付け、所定条件用パブリックキー記憶領域に登録が要求された新しい所定の条件と所定条件用パブリックキーとを対応させて記憶させるとともに、
登録ユーザパブリックキー記憶領域に記憶された登録ユーザの電子メールアドレスのそれぞれが、追加の要求がされた所定の条件を満たすかどうかを判断し、所定の条件を満たす場合は、所定の条件を満たす電子メールアドレスに、所定の条件に対応する所定条件用パブリックキーをさらに対応付け可能に登録ユーザパブリックキー記憶領域に記憶させる所定条件用パブリックキー追加手段、をさらに有するように構成できる。

【００４３】

また本発明は、
登録ユーザの電子メールアドレスとそれに対応づけられたパブリックキーは、パブリックキー管理サーバによるデジタル署名が付加された電子証明書に含まれる情報として取り扱われるものであり、電子メール受信端末においてデジタル署名が検証されることにより受信した暗号化電子メールの電子メールアドレスがパブリックキー管理サーバに真正に登録されたものであることを確認できるようになっているように構成できる。

【００４４】

また本発明は、
端末内受信者パブリックキー取得手段によるパブリックキーの取得の前に、それぞれの電子証明書が最新のものであるかどうかをパブリックキー管理サーバに問い合わせ、最新のものでなかった場合は最新のものをパブリックキー管理サーバから取得してそれで送信端末内パブリックキー記憶領域を更新する端末内受信者パブリックキー最新確認手段をさらに有するように構成できる。

【００４５】

また本発明は、
電子証明書が最新のものであるかどうかのパブリックキー管理サーバへの問い合わせは、前回の問合わせから所定のキャッシュ保持期間が経過したことを条件として行われるように構成できる。

【００４６】

また本発明は、
電子メール送信端末は、送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアと、送信者電子メールアドレスとを対応させて記憶する送信端末内プライベートキー記憶領域、をさらに有し、
電子メール送信端末は、送信者電子メールアドレスを発信元とし、受信者電子メールアドレスを宛先とする暗号化電子メールに対してプライベートキーを利用したデジタル署名を付加するものであり、電子メール受信端末においてデジタル署名が検証されることにより受信した暗号化電子メールのコンテンツの真正性が確認されるように構成できる。

【００４７】

また本発明は、
電子メール受信端末におけるデジタル署名の検証は、パブリックキー管理サーバから取得したパブリックキーによって行われるものであり、それによって、受信した暗号化電子メールの送信者がパブリックキー管理サーバに真正に登録されたユーザであることがさらに確認されるように構成できる。

【００４８】

また本発明は、
所定の条件は、受信者電子メールアドレスが所定のドメインに所属するものであるように構成できる。

【００４９】

また本発明は、
パブリックキー管理サーバは、所定の管理料金が支払われた所定のドメインに対して、

所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを、所定条件用パブリックキー記憶領域に、対応させて記憶するように構成できる。

【００５０】

本発明において、サーバ、端末などの用語は、装置の具体的形態を限定するものではなく、それが有する一般的な機能を備えた装置を表わすために使用されている。１つの構成要素が有する機能が２つ以上の構成要素によって実現されてもよく、２つ以上の構成要素が有する機能が１つの構成要素によって実現されてもよい。本願のシステムの発明は、それぞれの構成要素の有する機能が逐次的に実行される方法の発明として把握することもできる。その場合において、各構成要素は記載された順序に実行されるものに限定されるものではなく、全体としての機能が矛盾なく実行され得る限りにおいて、自由な順序でそれを実行することができる。また、１つのステップが有する機能が２つ以上のステップによって実現されてもよく、２つ以上のステップが有する機能が１つのステップによって実現されてもよい。これらの発明は、所定のハードウェアにおいて本発明の機能を実現するためにハードウェアを機能させるプログラムとしても成立し、それを記録した記録媒体としても成立する。プログラムとしては、端末を動作させるプログラムとしても成立するし、サーバを動作させるプログラムとしても成立する。

【発明の効果】

【００５１】

本発明によると、暗号化のためのパブリックキーを公開していない未登録ユーザに電子メールを送信する際に、一時的パブリックキーと一時的プライベートキーをサーバで生成し、一時的パブリックキーをサーバから電子メール送信端末に送り、それを用いて電子メールを暗号化させ、一時的プライベートキーをサーバから電子メール受信端末に送り、それを用いて暗号化電子メールを復号させることにより、未登録のユーザに暗号化した電子メールを送信することができる。さらに本発明によると、所定条件を満たす電子メールアドレスに対しては、当該電子メールアドレスに対応するパブリックキーに加えて、当該所定条件に対応する所定条件用パブリックキーを対応付けて公開することにより、所定条件を満たす電子メールアドレスを宛先とする電子メールは、パブリックキーとペアをなすプライベートキーを有する本来の宛先の電子メール受信端末に加えて、所定条件用パブリックキーとペアをなす所定条件用プライベートキーを有する所定条件電子メール代表受信端末でも復号することができる。

【図面の簡単な説明】

【００５２】

【図１】図１は、電子メール暗号化システム１００のサーバ及び端末に関連する構成を表わすブロック図である。

【図２】図２は、パブリックキー管理サーバ２０１の詳細ブロック図である。

【図３】図３は、電子メール送信端末３０１の詳細ブロック図である。

【図４】図４は、電子メール受信端末４０１の詳細ブロック図である。

【図５】図５は、ドメイン代表電子メール受信端末５０１の詳細ブロック図である。

【図６】図６は、パブリックキーの例を示す図である。

【図７】図７は、プライベートキーの例を示す図である。

【図８】図８は、公開鍵方式の暗号化と復号の動作のイメージを表わす図である。

【図９】図９は、電子メール暗号化システム１００の構成の概要の概念図である。

【図１０】図１０は、暗号化電子メールを送信する際のシステムの動作の概要を示す図である。

【図１１】図１１は、電子メール暗号化ソフトウェアのプラグインがインストールされた電子メールクライアントのユーザインターフェースのイメージ図である。

【図１２】図１２は、電子メール暗号化システム１００によって提供されるサービスの種類を表わす表である。

【図１３】図１３は、所定条件用キーの概要を表わす概念図である。

【図１４】図１４は、未登録ユーザへの暗号化電子メールの送信の動作フローの概念図である。
【図１５】図１５は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図である。
【図１６】図１６は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図１５の続きである。
【図１７】図１７は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図１６の続きである。
【図１８】図１８は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図１７の続きである。
【図１９】図１９は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図１８の続きである。
【図２０】図２０は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図１９の続きである。
【図２１】図２１は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の、特に電子メールアドレスの追加に係る動作を表わす動作フロー図である。
【図２２】図２２は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の、特に所定条件の追加に係る動作を表わす動作フロー図である。
【図２３】図２３は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図である。
【図２４】図２４は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図２３の続きである。
【図２５】図２５は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図２４の続きである。
【図２６】図２６は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図２５の続きである。
【図２７】図２７は、本願発明の第２の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図で、図２６の続きである。
【図２８】図２８は、電子メール暗号化ソフトウェアによって表示される、電子メールのコンテンツの編集ウィンドウと送信ボタンのイメージ図である。
【図２９】図２９は、電子メール暗号化ソフトウェアによって生成される、コンテンツが暗号化されていることが識別可能な情報を示す説明文のイメージ図である。
【図３０】図３０は、電子メール暗号化ソフトウェアによって復号される、回復された本来のコンテンツを表示している画面のイメージ図である。
【図３１】図３１は、電子メール暗号化ソフトウェアによって生成される、ユーザ登録のためのＵＲＬアクセスによる確認のためのメッセージを表示している画面のイメージ図である。
【図３２】図３２は、電子メール暗号化ソフトウェアによって生成される、未登録ユーザへの電子メールの処理の選択肢を表示している画面のイメージ図である。
【図３３】図３３は、電子メール暗号化ソフトウェアによって生成される、受信した電子メールが暗号化されていることを表わすフラグを表示している画面のイメージ図である。
【発明を実施するための形態】
【００５３】
これから図面を参照して本発明の実施形態に係る電子メール暗号化システム１００の説明を行う。本発明は、第１の実施形態と第２の実施形態によって説明される。第１の実施形態は、未登録ユーザへの暗号化電子メールの送信を可能とする実施形態であり、第２の実施形態は、ドメイン代表電子メール受信端末でドメインに所属する任意の暗号化電子メールを復号できるようにする実施形態である。電子メール暗号化システム１００は、第１の実施形態及び第２の実施形態のいずれも実施可能なハードウェア構成を有するものであるが、第１の実施形態、第２の実施形態のいずれを実施するのかに応じて、それに含まれ

る、それぞれの実施形態に対応する構成が使用される。

【００５４】

図１は、電子メール暗号化システム１００のサーバ及び端末に関連する構成を表わすブロック図である。図２は、パブリックキー管理サーバ２０１の詳細ブロック図である。図３は、電子メール送信端末３０１の詳細ブロック図である。図４は、電子メール受信端末４０１の詳細ブロック図である。図５は、ドメイン代表電子メール受信端末５０１の詳細ブロック図である。

【００５５】

第１の実施形態は、具体的には、電子メール暗号化のためのパブリックキーが登録されておらず、ユーザとしてあらかじめ登録されていない受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号させる実施形態である。

【００５６】

第２の実施形態は、具体的には、ユーザとして登録された受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号し、前記受信者電子メールアドレスがあらかじめ登録されたドメインである登録ドメインに所属する場合には、前記登録ドメインに所属する任意の同一ドメイン内受信者電子メールアドレスを宛先とする暗号化電子メールを、前記任意の同一ドメイン内受信者電子メールアドレスを宛先とする前記暗号化電子メールを受信することができるドメイン代表電子メール受信端末で復号することができるようにする実施形態である。

【００５７】

［電子メール暗号化システム１００のハードウェア構成］

電子メール暗号化システム１００はパブリックキー管理サーバ２０１を含み、パブリックキー管理サーバ２０１は、電子メール送信端末３０１、電子メール受信端末４０１、所定条件電子メール代表受信端末５０１とネットワーク６０２を介して接続される。また、パブリックキー管理サーバ２０１には、メールサーバ６０１がネットワーク６０２を介して接続される。

【００５８】

次に、パブリックキー管理サーバ２０１の構成の説明をする。図２には、パブリックキー管理サーバ２０１のハードウェア構成が示されている。図１を参照すると、パブリックキー管理サーバ２０１は、ＣＰＵ２０２、ＲＡＭ２０３、ユーザインターフェース（ユーザＩ／Ｆ）２０４、ネットワークインターフェース（ネットワークＩ／Ｆ）２０５、記憶装置２１０から構成される。記憶装置２１０は、その記憶領域に、動作に応じて変化しない静的なデータとして、ＯＳ２１１、キー管理アプリケーション２１２、電子メール暗号化ソフトウェア２１３を記憶し、動作に応じて変化する動的なデータとして、登録ユーザパブリックキー記憶領域２２０、未登録ユーザ一時的キーペア記憶領域２３０、及び所定条件用パブリックキー記憶領域２４０を記憶する。ＣＰＵ２０２は、コンピュータソフトウェアに基づき情報処理を行うプロセッサである。ＲＡＭ２０３は、実行されるソフトウェアがその上に読み込まれるメモリ空間と、読み込まれたソフトウェアがＣＰＵ２０２によって実行される際に必要となるワークエリア等を提供するメモリである。ＯＳ２１１は、ハードウェアに密接な基本的な情報処理を行うオペレーティングシステムである。キー管理アプリケーション２１２は、ＯＳ２１１上で動作するアプリケーションソフトウェアである。ＯＳ２１１、キー管理アプリケーション２１２が記憶装置２１０から読み出されて一時的記憶装置であるＲＡＭ２０３の所定の領域に展開され、キー管理アプリケーション２１２がＯＳ２１１とともにＣＰＵ２０２によって実行されることにより、パブリック

キー管理サーバ２０１の所定の機能を実現する。記憶装置２１０は、ソフトウェアやデータなどの情報を記憶・管理する構成要素であり、典型的にはハードディスクドライブなどの形態である。ユーザＩ／Ｆ２０４は、操作者との間でデータの入出力を行うためのＩ／Ｆである。ネットワークＩ／Ｆ２０５は、ネットワークに接続して情報の入出力を行うためのＩ／Ｆである。

【００５９】

登録ユーザパブリックキー記憶領域２２０は、電子メール暗号化システム１００による電子メール暗号化のためのパブリックキーが記憶されており、ユーザとして登録されているそれぞれのユーザの登録電子メールアドレス２２１とパブリックキー２２５とを対応づけて記憶する。電子メール暗号化のためのパブリックキー２２５は、既登録ユーザが自己の端末のためにプライベートキーとのペアとして生成したパブリックキーであり、これをパブリックキー管理サーバ２０１によって公開し、電子メールの送信者にパブリックキー２２５を利用して電子メールを暗号化させるための公開鍵である。パブリックキー２２５は、既登録ユーザの端末から事前に取得される。第２の実施形態においては、登録ユーザパブリックキー記憶領域２２０には、既登録ユーザの登録電子メールアドレスが所定条件２４２を満たす場合、その所定条件２４２に対応する所定条件用パブリックキー２４５と同一のキーも、パブリックキー２２５の一部として記憶されるか、あるいは少なくともパブリックキー２２５と対応付け可能に記憶される。

電子メール暗号化ソフトウェア２１３は、これがパブリックキー管理サーバ２０１で実行されるのではなく、第１の実施形態において、電子メール受信端末４０１へダウンロードするためのデータとしてのソフトウェアである。

【００６０】

未登録ユーザ一時的キーペア記憶領域２３０は、第１の実施形態において使用される構成であり、電子メール暗号化システム１００に電子メール暗号化のためのパブリックキーが記憶されておらず、ユーザとしてあらかじめ登録されていない受信者電子メールアドレス２３１と、一時的パブリックキー２３５、一時的プライベートキー２３６のペアとを対応づけて記憶する。一時的パブリックキー２３５、一時的プライベートキー２３６は、電子メールの受信者が電子メール暗号化システム１００に登録されていない未登録ユーザであって、そのパブリックキーがパブリックキー管理サーバ２０１に記憶されていない場合に、その未登録ユーザに対して暗号化した電子メールを最初に送信する際に使用される鍵である。一時的パブリックキー２３５、一時的プライベートキー２３６は、暗号化電子メールを送信しようとする受信者が未登録ユーザであった場合に、パブリックキー管理サーバ２０１で生成される一時的なパブリックキーとプライベートキーのペアであり、暗号化のために電子メール送信端末３０１に送信され、復号のために電子メール受信端末４０１に送信される。

【００６１】

所定条件用パブリックキー記憶領域２４０は、第２の実施形態において使用される構成であり、電子メールアドレスがそれを満たすかどうか判断するための所定条件２４２と、その所定条件に対応するパブリックキーであるドメイン用パブリックキー２４５とを対応づけて記憶する。所定条件２４２とは、電子メールアドレスに対して、それが満たされているかどうかを判断することができる基準のことである。所定条件の具体例としては、以下のようなものが考えられる。まず、所定条件が、電子メールアドレスが所定のドメインに所属していることが考えられる。例えば「ドメイン名＝”ｚｅｎｌｏｋ．ｃｏｍ”」が所定条件であった場合、電子メールアドレス”Ｘ００１@ｚｅｎｌｏｋ．ｃｏｍ”，”Ｘ００２@ｚｅｎｌｏｋ．ｃｏｍ”などがその所定条件を満たす電子メールアドレスである。他には、所定条件が、電子メールアドレスが所定のドメインに所属しており、かつ、登録ユーザが所定人数以下であることが考えられる。例えば「ドメイン名＝”ｚｅｎｌｏｋ．ｃｏｍ”」、かつ、所定人数＝５０が所定条件であった場合、電子メールアドレス”Ｘ００１@ｚｅｎｌｏｋ．ｃｏｍ”～ ”Ｘ０５０@ｚｅｎｌｏｋ．ｃｏｍ”などがその所定条件を満たす電子メールアドレスである。他には、電子メールアドレスが所定のサブ

ドメインの集合（ゾーン）に所属していることが考えられる。例えば「サブドメインの集合＝”ｚｅｎｌｏｋ．ｃｏｍ”」が所定条件であった場合の、電子メールアドレス”ａａａ@ｘｘｘ．ｚｅｎｌｏｋ．ｃｏｍ”，”ａａａ@ｙｙｙ．ｚｅｎｌｏｋ．ｃｏｍ”などがその所定条件を満たす電子メールアドレスである。他には、電子メールアドレスが所定のドメインに所属しており、かつ、アカウント名が所定の文字列から始まることが考えられる。例えば「ドメイン名＝”ｚｅｎｌｏｋ．ｃｏｍ”、かつ、アカウント名の最初の文字列＝”ａ”」が所定条件であった場合の、電子メールアドレス”ａ００１@ｚｅｎｌｏｋ．ｃｏｍ”，”ａ００２@ｚｅｎｌｏｋ．ｃｏｍ”などがその所定条件を満たす電子メールアドレスである。これらの所定条件は、典型的には、判断ロジック（例えば、上記の最初の例のように、電子メールアドレスのドメイン部分（「@」に続く部分）の文字列（所定部分の文字列）が所定文字列であるかどうか）がキー管理アプリケーション２１２に記載されており、所定条件２４０にはその判断ロジックで使用される所定文字列（例えば、上記の最初の例のように、所定文字列として「ｚｅｎｌｏｋ．ｃｏｍ」）が記憶される。

【００６２】

次に、電子メール送信端末３０１の構成の説明をする。図３には、電子メール送信端末３０１のハードウェア構成が示されている。図３を参照すると、電子メール送信端末３０１は、ＣＰＵ３０２、ＲＡＭ３０３、ユーザインターフェース（ユーザＩ／Ｆ）３０４、ネットワークインターフェース（ネットワークＩ／Ｆ）３０５、記憶装置３１０から構成される。記憶装置３１０は、その記憶領域に、動作に応じて変化しない静的なデータとして、ＯＳ３１１、電子メールクライアント３１２、電子メール暗号化ソフトウェア３１３を記憶し、動作に応じて変化する動的なデータとして、送信端末内パブリックキー記憶領域３２０、送信端末内ドメインパブリックキー記憶領域３４０、及び送信端末内プライベートキー記憶領域３５０を記憶する。ＣＰＵ３０２、ＲＡＭ３０３、ユーザＩ／Ｆ３０４、ネットワークＩ／Ｆ３０５、記憶装置３１０、ＯＳ３１１は、パブリックキー管理サーバ２０１の対応する構成と、それぞれ同様の構成を有する。電子メールクライアント３１２は、電子メールをネットワーク６０１を介してメールサーバ６０２との間で送受信するためのソフトウェアである。電子メールクライアント３１２は、典型的には、Ｏｕｔｌｏｏｋ　Ｅｘｐｒｅｓｓ（登録商標）、Ｔｈｕｎｄｅｒｂｉｒｄ（登録商標）などのソフトウェア製品の形態である。電子メール暗号化ソフトウェア３１３は、電子メールを暗号化したり、暗号化電子メールアドレスを復号したりするためのソフトウェアである。典型的には、電子メール暗号化ソフトウェア３１３は、電子メールクライアント３１２に組み込まれて機能を追加するプラグインソフトウェアの形態である。ＯＳ３１１、電子メールクライアント３１２、電子メール暗号化ソフトウェア３１３が記憶装置３１０から読み出されてＲＡＭ３０３に展開され、電子メール暗号化ソフトウェア３１３が組み込まれた電子メールクライアント３１２がＯＳ３１１とともにＣＰＵ３０２によって実行されることにより、電子メール送信端末３０１の所定の機能を実現する。

【００６３】

送信端末内パブリックキー記憶領域３２０は、パブリックキー管理サーバ２０１からあらかじめ取得した、登録ユーザのうちの所定の登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキー３２５と、それに対応する登録電子メールアドレス３２１とを対応付け可能に記憶する。登録電子メールアドレス３２１は、暗号化電子メールを送信しようとする受信者の電子メールアドレスである。パブリックキー３２５とそれに対応する登録電子メールアドレス３２１の取得は、典型的には、電子メール暗号化ソフトウェア３１３の動作によって、その登録電子メールアドレス３２１への最初の暗号化電子メールの送信時に行われていたものである。

【００６４】

送信端末内プライベートキー記憶領域３５０は、送信者電子メールアドレス３５１に対するパブリックキー３５５とプライベートキー３５６のペアと、送信者電子メールアドレス３５１とを対応づけて記憶する。パブリックキー３５５とプライベートキー３５６のペ

アは、電子メール送信端末内３０１で公知のアルゴリズムにより生成される。

【００６５】

次に、電子メール受信端末４０１の構成の説明をする。図４には、電子メール受信端末４０１のハードウェア構成が示されている。図４を参照すると、電子メール受信端末４０１は、ＣＰＵ４０２、ＲＡＭ４０３、ユーザインターフェース（ユーザＩ／Ｆ）４０４、ネットワークインターフェース（ネットワークＩ／Ｆ）４０５、記憶装置４１０から構成される。記憶装置４１０は、その記憶領域に、動作に応じて変化しない静的なデータとして、ＯＳ４１１、電子メールクライアント４１２、電子メール暗号化ソフトウェア４１３を記憶し、動作に応じて変化する動的なデータとして、受信端末内プライベートキー記憶領域４５０を記憶する。ＣＰＵ４０２、ＲＡＭ４０３、ユーザＩ／Ｆ４０４、ネットワークＩ／Ｆ４０５、記憶装置４１０、ＯＳ４１１、電子メールクライアント４１２、電子メール暗号化ソフトウェア４１３は、電子メール送信端末３０１に含まれる対応する構成と、それぞれ同様の構成を有する。

【００６６】

受信端末内プライベートキー記憶領域４５０は、受信者電子メールアドレス４５１に対するパブリックキー４５５とプライベートキー４５６のペアと、受信者電子メールアドレス４５１とを対応づけて記憶する。

なお、第１の実施形態は、未登録ユーザへの暗号化電子メールの送信を可能とする実施形態であるので、電子メール受信端末４０１において電子メール暗号化ソフトウェア４１３と受信端末内プライベートキー記憶領域４５０は暗号化電子メールの送信時点では存在せず、その後の処理によって追加されることとなる。一方、第２の実施形態においては、電子メール暗号化ソフトウェア４１３と受信端末内プライベートキー記憶領域４５０は当初より存在するものである。パブリックキー４５５とプライベートキー４５６のペアは、電子メール受信端末４０１のために公知のアルゴリズムにより生成される。

【００６７】

次に、所定条件電子メール代表受信端末５０１の構成の説明をする。図５には、所定条件電子メール代表受信端末５０１のハードウェア構成が示されている。図５を参照すると、所定条件電子メール代表受信端末５０１は、ＣＰＵ５０２、ＲＡＭ５０３、ユーザインターフェース（ユーザＩ／Ｆ）５０４、ネットワークインターフェース（ネットワークＩ／Ｆ）５０５、記憶装置５１０から構成される。記憶装置５１０は、その記憶領域に、動作に応じて変化しない静的なデータとして、ＯＳ５１１、電子メールクライアント５１２、電子メール暗号化ソフトウェア５１３を記憶し、動作に応じて変化する動的なデータとして、代表受信端末内プライベートキー記憶領域５５０を記憶する。ＣＰＵ５０２、ＲＡＭ５０３、ユーザＩ／Ｆ５０４、ネットワークＩ／Ｆ５０５、記憶装置５１０、ＯＳ５１１、電子メールクライアント５１２、電子メール暗号化ソフトウェア５１３は、電子メール送信端末３０１の対応する構成と、それぞれ同様の構成を有する。

【００６８】

代表受信端末内プライベートキー記憶領域５５０は、所定条件電子メール代表受信端末５０１が受信することができる、所定の条件を満たす任意の受信者電子メールアドレス４５１の電子メールを復号するための、所定条件用パブリックキー５５５とペアをなす所定条件用プライベートキー５５６を記憶する。所定条件用プライベートキー５５６は、所定条件用パブリックキー５５５とのペアとして、通常、１つの所定条件に対して１つのペアが生成される。所定条件用パブリックキー５５５をパブリックキー管理サーバ２０１に記憶させた後は、所定条件電子メール代表受信端末５０１での復号のためには、少なくとも所定条件用プライベートキー５５６が必要であるが、管理上、所定条件用パブリックキー５５５とペアにして記憶しておくのが望ましい。また、所定条件用プライベートキー５５６は、所定条件（例えば、ドメイン名）と対応付けて記憶させておくと、所定条件用プライベートキー５５６で復号できるかどうかの判断が、所定条件電子メール代表受信端末５０１において電子メールアドレスが所定条件を満たすかどうかを判断することによって簡単に行うことができる。所定条件用パブリックキー５５５と所定条件用プライベートキー

５５６のペアは、所定条件電子メール代表受信端末５０１のために公知のアルゴリズムにより生成される。

【００６９】

メールサーバ６０１は宛先となった電子メールアドレスを有する電子メールを受け取って保管しておく記憶領域であるメールボックスをネットワーク上に提供するサーバであり、具体的には、宛先となる電子メールアドレスのドメイン名（サーバ名）に対応するネットワーク上のＰＯＰサーバなどのメールサーバである。ここに保管された電子メールは、電子メール受信端末の電子メールクライアントからアクセスされることにより、最終的な宛先である電子メール受信端末によって受信される。ネットワーク６０２は、典型的には、インターネットなどの、電子メールの送受信のためのプロトコルを使用することが可能なネットワークである。

【００７０】

［電子メール暗号化システム１００の動作の概要］

次に、図６から図１４を参照して、電子メール暗号化システム１００の構成と動作の概要を説明する。電子メール暗号化システム１００は、公開鍵方式の暗号を利用した暗号化システムである。公開鍵方式では、お互いにペアをなすが、一方からは他方を求めることは実質的な不可能なパブリックキーとプライベートキーを利用したものであり、パブリックキーで暗号化したメッセージは、それとペアをなすプライベートキーでなければ復号できないという性質を有する。図６は、パブリックキーの例を示す図である。図７は、プライベートキーの例を示す図である。図８は、公開鍵方式の暗号化と復号の動作のイメージを表わす図である。図９は、電子メール暗号化システム１００の構成の概要の概念図である。電子メールユーザに対して電子メール暗号化ソフトウェアのプラグインが提供され、電子メール暗号化ソフトウェアの働きにより、それぞれの電子メールユーザの端末はパブリックキー管理サーバにアクセスし、暗号化電子メールの送受信のためのサポートを受ける。図１０は、暗号化電子メールを送信する際のシステムの動作の概要を示す図である。プラグインが追加された電子メールクライアントの「暗号化送信」ボタン（図１１の「Zenlok Send」ボタン）を押すことによって、暗号化電子メールの送信プロセスが開始される。まず、（１）送信者端末が受信者のパブリックキーをパブリックキー管理サーバから取得する。次に、（２）送信者端末が受信者のパブリックキーを暗号化のために使用する。その次に、（３）暗号化電子メールが通常の電子メールクライアントの機能により送信される。そして、（４）受信者端末でプラグインにより暗号化電子メールが自動的に復号される。

【００７１】

図１１は、電子メール暗号化ソフトウェアのプラグインがインストールされた電子メールクライアントのユーザインターフェースのイメージ図である。図１１の上部に示すように、電子メール暗号化ソフトウェアのプラグインをインストールすると、ユーザは追加されたメニューやアイコンによって種々のオプションにアクセスすることができる。受信した電子メールが本発明の電子メール暗号化ソフトウェアで暗号化されていれば、その電子メールのメッセージに対してフラグが表示される。図１１の下部に示すように、電子メール暗号化ソフトウェアのプラグインをインストールすると、「暗号化送信(Zenlok Send)」ボタンが表示される。暗号化した電子メールメッセージを送信するためには、ユーザは、通常の電子メールクライアントの「送信(Send)」ボタンの代わりに、この「暗号化送信(Zenlok Send)」ボタンをクリックすればよい。図１２は、電子メール暗号化システム１００によって提供されるサービスの種類を表わす表である。電子メール暗号化システム１００による各種のサービスをユーザに提供する場合には、サービスを広く拡布する観点から、いくつかのサービスは無料で提供し、また、サービス提供者の利益の観点から、いくつかのサービスは有料で提供することが望ましい。具体的には、暗号化ソフトウェアプラグインをユーザに対してダウンロードして電子メールクライアントに追加すること、ユーザがサーバからパブリックキーを取得すること、ユーザが電子メールメッセージを暗号化すること、ユーザが電子メールメッセージを復号すること、といった基本的な電子メール

暗号化のサービスは無料で提供される。また、個人の同一性の認証（サーバによる証明）、所定条件用パブリックキー（コーポレートマスターキー）の提供、マスメーリングシステム（キーの一括管理システム）の提供という付加的なサービスは、有料で提供される。図１３は、所定条件用キーの概要を表わす概念図である。所定条件用キーがない場合、ユーザは、自分を宛先とする電子メールしか復号できない。一方、所定条件用キー（通常、ドメイン単位で会社に対して発行されるため、「コーポレートマスターキー」とも呼ぶ）を有する会社は、所定条件と所定条件用パブリックキーをパブリックキー管理サーバに管理させることができ、それによって、電子メールアドレスがその会社のドメインに所属することがその所定条件とすると、そのドメインに所属するすべての暗号化電子メールを、所定条件用プライベートキーを有する代表受信端末で復号できる。図１４は、未登録ユーザへの暗号化電子メールの送信の動作フローの概念図である。登録ユーザである送信者から、未登録ユーザである受信者への最初の暗号化電子メールの送信のフローの概略が示されている。まず、（１）送信者が送信者端末からパブリックキー管理サーバに対して受信者のパブリックキーを要求する。（２）パブリックキー管理サーバは、受信者が未登録ユーザであった場合には、一時的パブリックキーと一時的プライベートキーのペアを生成し、一時的パブリックキーを送信者端末に送信する。（３）送信者端末では、一時的プライベートキーで電子メールを暗号化し、それを受信者の受信者端末に送信する。この暗号化電子メールには、電子メール暗号化ソフトウェアのダウンロード先の情報を含む電子メールが暗号化されている旨の注記が付加されている。（４）暗号化電子メールを受信した受信者は、電子メールに含まれるダウンロード先の情報に従って電子メール暗号化ソフトウェアをダウンロードし、パブリックキー管理サーバにユーザとして登録する。（５）受信者の受信者端末がパブリックキー管理サーバに暗号化電子メールを復号するための一時的プライベートキーを要求する。（６）パブリックキー管理サーバが受信者の受信者端末に一時的プライベートキーを送信する。これによって、受信者の受信者端末で暗号化電子メールの復号が可能となる。

【００７２】

［電子メール暗号化システム１００の動作－第１の実施形態］

次に、電子メール暗号化システム１００の動作について詳細に説明する。まず、第１の実施形態に説明する。図１５から図２０は、本願発明の第１の実施形態に係る、電子メール暗号化システム１００の動作を表わす動作フロー図である。

【００７３】

まず、電子メール送信端末３０１は、受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける（ステップＳ１０１）。受信者電子メールアドレスは、複数であってもよく、また、典型的には、ＣＣやＢＣＣなどに記載されたものも含む。これは、電子メールクライアント３１２上で電子メール暗号化ソフトウェア３１３がＣＰＵ３０２によって実行されることにより実現されるステップであり、このことはこれ以降の電子メール暗号化ソフトウェア３１３が関係するステップにおいても同様である。暗号化して送信する要求は、例えば図２８に示すように、電子メールのコンテンツ１００２の編集ウィンドウに表示されるボタン１００１を押すことで要求が受け付けられる。この例において、電子メール暗号化ソフトウェア３１３は、既存の電子メール送受信ソフトウェアである電子メールクライアント３１２に組み込まれたプラグインソフトウェアモジュールである。

【００７４】

次に、電子メール送信端末３０１は、送信端末内パブリックキー記憶領域３２０に対して、受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキー３２５をそこから取得する（ステップＳ１０３）。取得されたパブリックキー３２５はＲＡＭ３０３に記憶される。

【００７５】

次に、電子メール送信端末３０１は、パブリックキー管理サーバ２０１に対して、受信

者電子メールアドレスのうちで、少なくとも送信端末内パブリックキー記憶領域３２０に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する（ステップＳ１０５）。要求は、ネットワークＩ／Ｆ３０５を経由し、ネットワーク６０２を介してパブリックキー管理サーバ２０１により受信される。

【００７６】

パブリックキー管理サーバ２０１は、電子メール送信端末３０１から受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、登録ユーザパブリックキー記憶領域２２０に対して、パブリックキーの要求に含まれる受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、既登録ユーザの登録電子メールアドレスに対応するパブリックキー２２５をそこから取得する（ステップＳ１０７）。これは、キー管理アプリケーション２１２がＣＰＵ２０２によって実行されることにより実現されるステップであり、このことはこれ以降のキー管理アプリケーション２１２が関連するステップにおいても同様である。取得されたパブリックキー２２５はＲＡＭ２０３に記憶される。

【００７７】

次に、パブリックキー管理サーバ２０１は、ステップＳ１０７において登録ユーザパブリックキー記憶領域２２０に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを未登録ユーザ一時的キーペア記憶領域２３０に記憶させる（ステップＳ１０９）。

【００７８】

次に、パブリックキー管理サーバ２０１は、ステップＳ１０７の受信者パブリックキーの検索で取得された既登録ユーザのためのパブリックキー２２５、及び生成された未登録ユーザのための一時的パブリックキー２３５を電子メール送信端末３０１に送信する（ステップＳ１１１）。送信されたそれぞれのパブリックキーは、ネットワークＩ／Ｆ２０５を経由し、ネットワーク６０２を介して電子メール送信端末３０１により受信される。

【００７９】

次に、電子メール送信端末３０１は、パブリックキー管理サーバ２０１から送信された既登録ユーザのためのパブリックキー２２５を、それに対応する登録電子メールアドレスと対応させて送信端末内パブリックキー記憶領域３２０にさらに記憶させる（ステップＳ１１３）。これは、電子メール暗号化ソフトウェア３１３がＣＰＵ３０２によって実行されることにより実現されるステップであり、このことはこれ以降の電子メール暗号化ソフトウェア３１３が関連するステップにおいても同様である。

【００８０】

次に、電子メール送信端末３０１は、電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成する（ステップＳ１１５）。共通鍵方式の暗号化キーは毎回新たに生成し、また一度使用した暗号化キーは破棄することが望ましいが（ワンタイム・キー）、何度も同じ鍵を用いることも可能である。共通鍵方式の暗号化キーを用いるのは、暗号化のための計算量が小さく、コンピュータの負担が少ないこと、及び、コンテンツの暗号化を公開鍵（パブリックキー）で行うと、それに対応するただ１つの秘密鍵（プライベートキー）でしか復号できず、宛先が複数の電子メールの暗号化には使用が難しいことといった理由による。

【００８１】

次に、電子メール送信端末３０１は、ステップＳ１０１で受け付けられた要求に含まれる受信者電子メールアドレスを宛先とする電子メールのコンテンツをコンテンツ暗号化キーで暗号化する（ステップＳ１１７）。暗号化されたコンテンツは、例えば添付ファイルとして電子メールに添付されてもよいし、そうでなくともよい。

【００８２】

次に、電子メール送信端末３０１は、電子メールのコンテンツの暗号化に使用した「コ

ンテンツ暗号化キー」を、受信者電子メールアドレスのそれぞれに対応する、パブリックキー管理サーバ２０１から送信された登録ユーザのパブリックキー２２５及び未登録ユーザのための一時的パブリックキー２３５のそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する「暗号化されたコンテンツ暗号化キー」を生成する（ステップＳ１１９）。パブリックキー管理サーバ２０１から送信された登録ユーザのパブリックキー２２５に代えて送信端末内パブリックキー記憶領域３２０に記憶されたパブリックキー３２５を使用してもよい。これは、電子メール暗号化ソフトウェア３１３がＣＰＵ３０２により実行されることで実現されるものである。なお、多数の受信者に対して暗号化メールを送信する場合でも、受信者電子メールアドレスそれぞれに対してのコンテンツ暗号化キー暗号化処理を操作者が個別に行う必要はなく、電子メール暗号化ソフトウェア３１３が透過的にこれらの処理を行う。

【００８３】

次に、電子メール送信端末３０１は、暗号化された電子メールのコンテンツに、生成された暗号化されたコンテンツ暗号化キーのそれぞれを添付し、さらに暗号化されていることが識別可能な情報を暗号化せずに添付する（ステップＳ１２１）。なお、好適には、その暗号化されていることが識別可能な情報には、電子メール暗号化ソフトウェア４１３（パブリックキー管理サーバ２０１内に記憶されている電子メール暗号化ソフトウェア２１３）のダウンロード手段のネットワーク上の位置を示す情報が含まれる。また、一時的パブリックキー２３５を使用した場合は、それが一時的なものであることを示すフラグ等の情報を暗号化電子メールに添付してもよい。

【００８４】

そして、電子メール送信端末３０１は、暗号化電子メールを受信者電子メールアドレスに送信させる（ステップＳ１２３）。この送信は、典型的には、電子メールクライアント３１２がＣＰＵ３０２によって実行されることにより実現される、。暗号化電子メールはメールサーバ６０１を経由し、ネットワーク６０２を介して転送され、電子メール受信端末４０１により受信される。

【００８５】

電子メール受信端末４０１は、電子メール送信端末３０１から送信された暗号化電子メールを受信し、それに含まれる電子メールのコンテンツが暗号化されていることが識別可能な情報を表示する（ステップＳ１２５）。電子メールに電子メール暗号化ソフトウェア４１３（電子メール暗号化ソフトウェア２１３）のダウンロード手段のネットワーク上の位置を示す情報が含まれている場合は、それも表示される。これは、電子メールクライアント４１２がＣＰＵ４０２によって実行されることにより実現されるステップである。受信した電子メールには、本来のコンテンツではなく（本来のコンテンツは未だ暗号化された状態である）、例えば図２９のような、コンテンツが暗号化されていることが識別可能な情報を示す説明文１００３が表示される。ダウンロード手段のネットワーク上の位置を示す情報は、典型的には、図２９における説明文１００３中の特定の単語から張られた、ダウンロード先のＷｅｂサイトへのリンク１００４である。

【００８６】

次に、電子メール受信端末４０１は、パブリックキー管理サーバ２０１に記憶されている電子メール暗号化ソフトウェア２１３をパブリックキー管理サーバ２０１のダウンロード手段からダウンロードして電子メール暗号化ソフトウェア４１３として記憶する（ステップＳ１２７）。これは、ＯＳ４１１上で動作する通信機能を有するソフトウェア（例えばＷｅｂブラウザなど。図示していない）がＣＰＵ４０２によって実行されることにより実現されるステップである。ダウンロード手段は、典型的には、ネットワーク６０２を介して接続された、パブリックキー管理サーバ２０１からそれが記憶する電子メール暗号化ソフトウェア２１３がダウンロード可能なようにパブリックキー管理サーバ２０１が構成されるものである。なお、ダウンロード手段は、パブリックキーを管理するサーバと物理的には異なるサーバであってもよく、この場合、それらをまとめてパブリックキー管理サーバ２０１として把握可能である。ダウンロードされた暗号化ソフトウェアは記憶装置４

１０に記憶される（電子メール暗号化ソフトウェア４１３）。
【００８７】
次に、電子メール受信端末４０１は、受信した暗号化電子メールの受信者電子メールアドレスに対応する一時的プライベートキーをパブリックキー管理サーバに要求する（ステップS１２９）。これは、電子メール暗号化ソフトウェア４１３がＣＰＵ４０２によって実行されることにより実現されるステップである。電子メール暗号化ソフトウェア４１３は、典型的には、その電子メール暗号化ソフトウェア４１３が初めて電子メール受信端末４０１上で実行されたことを電子メール暗号化ソフトウェア４１３によって実行されているプロセスが検知し、暗号化電子メールに対応する一時的プライベートキーが必要であると判断する。あるいは、暗号化電子メールに、一時的なパブリックキーを利用して暗号化されたものであることを示すフラグ等の情報が添付されている場合は、その情報があることを確認した場合に、一時的プライベートキーが必要であると判断する。一時的プライベートキー２３６の要求は、ネットワークＩ／Ｆ４０５を経由し、ネットワーク６０２を介してパブリックキー管理サーバ２０１により受信される。
【００８８】
パブリックキー管理サーバ２０１は、電子メール受信端末４０１からの受信者電子メールアドレスに対応する一時的プライベートキーの要求を受信すると、未登録ユーザ一時的キーペア記憶領域２３０からその受信者電子メールアドレスに対応する一時的プライベートキー２３６を検索して取得する（ステップＳ１３１）。これは、キー管理アプリケーション２１２がＣＰＵ２０２によって実行されることにより実現されるステップである。取得された一時的プライベートキー２３６はＲＡＭ２０３に記憶される。
【００８９】
次に、パブリックキー管理サーバ２０１は、取得された一時的プライベートキー２３６を電子メール受信端末４０１に送信する（ステップＳ１３３）。送信されたそれぞれのパブリックキーは、ネットワークＩ／Ｆ２０５を経由し、ネットワーク６０２を介して電子メール受信端末４０１により受信される。
【００９０】
電子メール受信端末４０１は、受信者電子メールアドレスに対応する暗号化されたコンテンツ暗号化キーをパブリックキー管理サーバ２０１から送信された一時的プライベートキー２３６を用いて復号し、コンテンツ暗号化キーを回復する（ステップＳ１３５）。これは、電子メール暗号化ソフトウェア４１３がＣＰＵ４０２によって実行されることにより実現されるステップである。宛先の数が複数ある場合は、少なくともその数に応じた複数の暗号化されたコンテンツ暗号化キーが生成されており、そのそれぞれが暗号化電子メールに添付されているが、受信端末４０１が受信した一時的プライベートキー２３６を用いて復号できるのは、その一時的プライベートキー２３６に対応する一時的パブリックキー２３５で暗号化されたコンテンツ暗号化キーのみである。
【００９１】
次に、電子メール受信端末４０１は、復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる（ステップＳ１３７）。この時点で、受信者は電子メールの本来のコンテンツにアクセスすることが可能となる。図３０は、回復された本来のコンテンツ１００５を表示している画面である。これによって、図２８に示した送信者によって暗号化される前のコンテンツ１００２が回復される。このように、ユーザとして登録しておらず、暗号化のためのパブリックキーを公開していないユーザに対して、安全かつ確実に暗号化電子メールを送信することができる。
【００９２】
なお、ユーザとして登録していなかった受信者に対しては、最初の暗号化電子メールの復号時に、受信者電子メールアドレスに対応するパブリックキーをパブリックキー管理サーバ２０１に登録してユーザとして登録すれば、パブリックキー管理サーバ２０１がそのパブリックキーを公開することにより、そのユーザに対して暗号化電子メールを送信することができる。以下のステップは、そのための追加的なステップである。

【００９３】
電子メール受信端末４０１で、受信者電子メールアドレスに対応する、新しいパブリックキーとプライベートキーのペアが生成され、それらが、受信者電子メールアドレス４５１、パブリックキー４５５、プライベートキー４５６として、それぞれ対応づけて受信端末内プライベートキー記憶領域４５０に記憶される（ステップＳ１５１）。パブリックキー４５５は電子メール送信端末３０１での電子メールの暗号化に必要であり、プライベートキー４５６は電子メール受信端末４０１内での暗号化電子メールの復号に必要である。従って、暗号化電子メールの復号のためには、少なくともプライベートキー４５６が記憶されている必要がある。電子メール受信端末４０１は、生成されて記憶されたパブリックキー４５５を含む、受信者の受信者電子メールアドレス４５１に対応するユーザ登録の要求を、パブリックキー管理サーバ２０１に送信する（ステップＳ１５３）。ここで、プライベートキー４５６は送信されないため、受信者のパブリックキー４５５を用いて暗号化された電子メールは、電子メール受信端末４０１でしか復号できない。なお、ステップＳ１５１及びＳ１５３は、好適には、その電子メール暗号化ソフトウェア４１３が初めて電子メール受信端末４０１上で実行されたことを電子メール暗号化ソフトウェア４１３のプロセスが検知し、それによって自動的に実行される。

【００９４】
パブリックキー管理サーバ２０１は、電子メール受信端末４０１からのユーザ登録の要求を受信すると、それに含まれる生成されたパブリックキーを受信者電子メールアドレスと対応づけて登録ユーザパブリックキー記憶領域２２０にさらに記憶させる（ステップＳ１５５）。これは、キー管理アプリケーション２１２がＣＰＵ２０２によって実行されることにより実現されるステップである。なお、この記録が行われる前の段階で、ユーザ登録の要求に含まれる電子メールアドレスに対して、パブリックキー管理サーバ２０１から、図３１に示すような、登録確認のためのコンテンツ１００６を含む電子メールを送信してもよい。図３１は、電子メール暗号化ソフトウェアによって生成される、ユーザ登録のためのＵＲＬアクセスによる確認のためのメッセージを表示している画面のイメージ図である。好適には、そのコンテンツ１００６には、パブリックキー管理サーバ２０１により設定された、パブリックキー管理サーバ２０１の管理下にある特定のアクセス確認のためだけに用いるＵＲＬ１００７が含まれており、ユーザによりその特定のＵＲＬ１００７へのアクセスが行われたことをパブリックキー管理サーバ２０１が確認することによって、登録を要求しているユーザが、その電子メールアドレスのメールボックスをネットワーク上に真正に有していることを確認する。

【００９５】
今回の最初の受信者に対して、これ以降に暗号化電子メールを送信する際には、前記ユーザ登録で新たに記憶された、該受信者の登録電子メールアドレス２２１に対応するパブリックキー２２５が公開されて用いられることになるため、一時的キーペアは不要となる。従って、今回の暗号化電子メール送信に用いられた一時的パブリックキー２３５、一時的プライベートキー２３６はこの時点で破棄されてよい。なお、仮にユーザ登録が行われなかったとしても（受信者がユーザ登録を拒否したとしても）、電子メール受信端末４０１に暗号化メールの復号をさせるように構成することもできるし、前記受信者による暗号化メールの復号には必ず該受信端末４１０からのユーザ登録を伴うよう構成することも可能である。後者のように構成すると、暗号化電子メールの送信により、本願発明に係る電子メール暗号化ソフトウェアの拡布が促進される。後者の場合、暗号化電子メールの復号の前の段階で、電子メール受信端末４１０からのユーザ登録の要求が行われるようにステップの順番を変更すればよい。

【００９６】
未登録ユーザによる復号に際して必ずユーザ登録を要求するように構成した場合でも、ユーザ登録が無料であれば、その未登録ユーザは登録することに抵抗を感じることはなく、電子メールの暗号化という利益の方がユーザにより高く評価される可能性が高い。このような構成は、電子メール暗号化ソフトウェアの普及に大きく貢献するものである。電子

メール暗号化ソフトウェアが広く普及したとすれば、既に述べたように情報流出の危険性が低減し、より安全な電子メール通信が可能となる。

【００９７】

またステップＳ１１９においては、コンテンツ暗号化キーを、さらに送信者電子メールアドレスに対応するパブリックキーによっても、公開鍵方式で暗号化するよう構成することが可能である。

すなわち、ステップＳ１１９において、電子メール送信端末３０１は、電子メールのコンテンツの暗号化に使用したコンテンツ暗号化キーを、受信者電子メールアドレスのそれぞれに対応する、パブリックキー管理サーバ２０１から送信された登録ユーザのパブリックキー２２５及び未登録ユーザのための一時的パブリックキー２３５、及び、それに加えて送信者電子メールアドレスに対応するパブリックキー３２５のそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成する。続くステップＳ１２１においては、生成された暗号化されたコンテンツ暗号化キーのそれぞれが暗号化された電子メールに添付される。

【００９８】

送信者は、ステップＳ１２３における暗号化電子メールの送信が実行された後、電子メールクライアント３１２を介して該送信された暗号化電子メールにアクセスし、送信端末内プライベートキー記憶領域３５０から取得した送信者のプライベートキー３５６を用いて、該暗号化電子メールを復号することができる。このような構成により、送信済みのアイテムが暗号化されていても、送信者自身が暗号化されたコンテンツを復号して確認することができるようになる。この復号は、電子メール暗号化ソフトウェア３１３によって実行される。

【００９９】

ところで、ステップＳ１０１で暗号化電子メールの送信を要求する時点において、一般に送信者は、受信者電子メールアドレスのそれぞれが登録ユーザパブリックキー記憶領域２２０に登録された既登録ユーザであるか否かを知らない。その一方で、未登録の受信者が暗号化電子メールを復号するには、電子メール暗号化ソフトウェア４１３をダウンロードするなどのステップを踏む必要があり、このことは、従来の技術による場合と比較すれば大幅に手間が軽減されたものではあるが、それを負担と感じる受信者がいる可能性もある。したがって未登録ユーザに対しては暗号化メール送信のキャンセルを送信者が望む場合もあり、そのようなキャンセルを送信者が選択できれば都合がいい。

【０１００】

そのような場合に対しては、以下のような構成を採ると好適である。すなわち、パブリックキー管理サーバ２０１によって実行されるステップＳ１０９は、ステップＳ１０５におけるパブリックキーの要求に含まれる受信者電子メールアドレスのうちで、ステップＳ１０７で実行された受信者パブリックキー検索による問い合わせにより登録ユーザパブリックキー記憶領域２２０に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、そこへ暗号化電子メールを送信するか否かの確認を電子メール送信端末３０１に行い、送信する旨の応答があったことを条件として、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを未登録ユーザ一時的キーペア記憶領域２３０に記憶させるように構成するとよい。

【０１０１】

図３２はそのような確認を行う画面の一例として、電子メール暗号化ソフトウェアによって生成される、未登録ユーザへの電子メールの処理の選択肢を表示している画面のイメージ図である。これは、パブリックキー管理サーバ２０１による確認要求を受信した、電子メール送信端末３０１上の電子メール暗号化ソフトウェア３１３の機能により表示される確認画面である。この確認画面には、メールの送信自体をキャンセルする旨の選択肢１００８、登録ユーザにのみ暗号化してメールを送信し、未登録ユーザには送信を行わない旨の選択肢１００９、すべてのユーザに暗号化してメールを送信する旨の選択肢１０１０

が表示され、送信者はそのいずれかを選択できる。電子メール暗号化ソフトウェア３１３によるプロセスは、それらのいずれの選択肢が選択されたのかに基づき、それぞれ、電子メールの破棄、未登録ユーザの宛先からの削除、すべての宛先への送信、のいずれかを行う。

【０１０２】

［電子メール暗号化システム１００の動作－第２の実施形態］

第２の実施形態においては、宛先として暗号化電子メールを受信する電子メール受信端末４０１のみならず、受信者電子メールアドレスの満たす所定条件に対応した所定条件電子メール代表端末５０１によっても、暗号化電子メールの復号が可能となる。

【０１０３】

すなわち、登録ユーザパブリックキー記憶領域２２０において、ある受信者の登録電子メールアドレス２２１に対して、１つ以上のパブリックキー２２を対応付けて記憶させることが可能であり、それらのうちの幾つかは、所定条件用パブリックキー記憶領域２４０における、ある所定条件２４２に対応づけて記憶された所定条件用パブリックキー２４５と同一のキーであってよい。この所定条件用パブリックキー２４５に対応する所定条件用プライベートキーを有する所定条件電子メール代表受信端末５０１は、その所定条件用プライベートキーを用いて、前記受信者に送信された暗号化電子メールを復号できることになる。

【０１０４】

なお、各々の電子メールアドレスがいかなる所定条件を満たすかの判断は、第１には電子メールアドレスの登録ユーザパブリックキー記憶領域２２０への登録時に行われる。すなわち、登録が要求された電子メールアドレスが所定条件用パブリックキー記憶領域２４０に記憶された所定条件２４２のそれぞれを満たすかどうかを判断し、特定の所定の条件２４２を満たす場合は、登録が要求された電子メールアドレスに、その所定条件２４２に対応する所定条件用パブリックキー２４５をさらに対応させて登録ユーザパブリックキー記憶領域２２０に記憶させる。

【０１０５】

図２１から図２７までは、所定条件電子メール代表受信端末５０１により復号可能な暗号化電子メールの送信を可能とする第２の実施形態のフローチャートである。

【０１０６】

所定条件２４２と、その所定条件を満たす電子メールアドレスとの対応付けの確認は、新しい電子メールアドレスが追加されたときや、新しい所定条件が追加されたときに行うことができる。まず、新しい電子メールアドレスが追加されたときについて説明する。図２１を参照する。パブリックキー管理サーバ２０１は、電子メールアドレスとそれと対応するパブリックキーの登録ユーザパブリックキー記憶領域２２０への登録の要求を登録しようとするユーザの端末から受け付ける（ステップＳ２０１）。パブリックキー管理サーバ２０１は、登録ユーザパブリックキー記憶領域２２０に登録が要求された電子メールアドレスとパブリックキーとを対応させて記憶させる（ステップＳ２０３）。パブリックキー管理サーバ２０１は、登録が要求された電子メールアドレスが所定条件用パブリックキー記憶領域２４０に記憶された所定条件２４２を満たすかどうかを判断し、所定条件２４２を満たす場合は、登録が要求された電子メールアドレスに、所定条件２４２に対応する所定条件用パブリックキー２４５をさらに対応付け可能に登録ユーザパブリックキー記憶領域２２０に記憶させる（ステップＳ２０５）。好適には、登録が要求された電子メールアドレスに対応するパブリックキー２２５の一部として、所定条件２４２に対応する所定条件用パブリックキー２４５が記憶されるが、登録が要求された電子メールアドレスと所定条件用パブリックキー２４５とは、少なくとも対応付けが可能であればよい。

【０１０７】

次に、新しい所定条件が追加されたときについて説明する。図２２を参照する。パブリックキー管理サーバ２０１は、新しい所定の条件と、それと対応する所定条件用パブリックキーの所定条件用パブリックキー記憶領域への追加の要求を新しい所定条件を登録しよ

うとするユーザの端末から受け付ける（ステップＳ２１１）。このユーザは、好適には、所定の管理料金を支払うことにより、所定条件用パブリックキーのパブリックキー管理サーバ２０１への記憶が許可されたものである。この追加の要求は、例えば、パブリックキー管理サーバ２０１の操作者が直接ユーザＩ／Ｆ２０４を介して行ってもよいが、パブリックキー管理サーバ２０１の管理下にある、特定のＵＲＬからネットワーク６０２を介してユーザが直接行ってもよい。パブリックキー管理サーバ２０１は、所定条件用パブリックキー記憶領域に登録が要求された新しい所定の条件と所定条件用パブリックキーとを対応させて記憶させる（ステップＳ２１３）。パブリックキー管理サーバ２０１は、登録ユーザパブリックキー記憶領域に記憶された登録ユーザの電子メールアドレスのそれぞれが、追加の要求がされた所定の条件を満たすかどうかを判断し、所定の条件を満たす場合は、所定の条件を満たす電子メールアドレスに、所定の条件に対応する所定条件用パブリックキーをさらに対応付け可能に登録ユーザパブリックキー記憶領域に記憶させる（ステップＳ２１５）。好適には、所定の条件を満たす電子メールアドレスに対応するパブリックキー２２５の一部として、所定条件２４２に対応する所定条件用パブリックキー２４５が記憶されるが、所定条件を満たす電子メールアドレスと所定条件用パブリックキー２４５とは、少なくとも対応付けが可能であればよい。例えば、所定の条件２４２として「ドメインが”Ｚｅｎｌｏｋ．ｃｏｍ”である」という条件が新たに記憶され、所定条件用パブリックキー２４５として対応するパブリックキーが新たに記憶された場合、登録ユーザパブリックキー記憶領域２２０に既に記憶されている登録電子メールアドレス２２１のうち「ドメイン名が”Ｚｅｎｌｏｋ．ｃｏｍ”である」電子メールアドレス２２１に対しては、その追加された所定条件用パブリックキー２４５がパブリックキー２２５として対応づけられ、新たに追加されて記憶される。これにより、前記電子メールアドレス２２１に対して送信された暗号化電子メールは、「ドメイン名が”Ｚｅｎｌｏｋ．ｃｏｍ”である」に対応づけて記憶された所定条件用パブリックキー２４５とペアを成す所定条件用プライベートキーを有する端末（所定条件電子メール代表受信端末５０１）によっても、復号可能となる。

【０１０８】

これらの新しい所定条件２４２を満たす電子メールアドレスの登録や、新しい所定条件２４２の登録は、任意の時点で行うことができるが、使用しようとする電子メール暗号化アドレスや所定条件２４２の登録は、少なくとも、暗号化電子メールを送信する前には行っておく必要がある。

【０１０９】

これから、使用しようとする電子メール暗号化アドレスや所定条件２４２が登録されていることを前提として、暗号化電子メールを送信する動作について説明する。まず、電子メール送信端末３０１は、受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける（ステップＳ３０１）。受信者電子メールアドレスは、複数であってもよく、また、典型的には、ＣＣやＢＣＣなどに記載されたものも含む。これは、電子メールクライアント３１２上で電子メール暗号化ソフトウェア３１３がＣＰＵ３０２によって実行されることにより実現されるステップであり、このことはこれ以降の電子メール暗号化ソフトウェア３１３が関連するステップにおいても同様である。図２８は、電子メール暗号化ソフトウェアによって表示される、電子メールのコンテンツの編集ウィンドウと送信ボタンのイメージ図である。暗号化して送信する要求は、例えば図２８が示すように、電子メールのコンテンツ１００２の編集ウィンドウに表示されるボタン１００１を押すことで要求が受け付けられる。（この例において、電子メール暗号化ソフトウェア３１３は、既存の電子メール送受信ソフトウェアである電子メールクライアント３１２に組み込まれたプラグインソフトウェアモジュールである。

【０１１０】

次に、電子メール送信端末３０１は、送信端末内パブリックキー記憶領域３２０に対して、受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されている１つ以上のパブリックキー３２

５をそこから取得する（ステップＳ３０３）。取得されたパブリックキー３２５はＲＡＭ３０３に記憶される。送信端末内パブリックキー記憶領域３２０において、ある受信者の登録電子メールアドレス３２１に対応づけて記憶されているパブリックキー３２５は複数であってもよく、それらのうちの幾つかは、所定条件用パブリックキー記憶領域２４０における、ある所定条件２４２に対応づけて記憶された所定条件用パブリックキー２４５と同一のキーであってよい。それら全てのパブリックキー３２５が、ここでは取得される。

【０１１１】

次に、電子メール送信端末３０１は、パブリックキー管理サーバ２０１に対して、受信者電子メールアドレスのうちで、少なくとも送信端末内パブリックキー記憶領域３２０に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する（ステップＳ３０５）。要求は、ネットワークＩ／Ｆ３０５を経由し、ネットワーク６０２を介してパブリックキー管理サーバ２０１により受信される。

【０１１２】

パブリックキー管理サーバ２０１は、電子メール送信端末３０１から受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、登録ユーザパブリックキー記憶領域２２０に対して、パブリックキーの要求に含まれる受信者電子メールアドレスのそれぞれが登録電子メールアドレスとして記憶されているかどうかを問い合わせ、既登録ユーザの登録電子メールアドレスに対応するパブリックキー２２５をそこから取得する（ステップＳ３０７）。これは、キー管理アプリケーション２１２がＣＰＵ２０２によって実行されることにより実現されるステップであり、このことはこれ以降のキー管理アプリケーション２１２が関連するステップにおいても同様である。取得されたパブリックキー２２５はＲＡＭ２０３に記憶される。登録ユーザパブリックキー記憶領域２２０において、ある受信者の登録電子メールアドレス２２１に対応づけて記憶されているパブリックキー２２５は一般に複数であってよく、それらのうちの幾つかは、所定条件用パブリックキー記憶領域２４０における、ある所定条件２４２に対応づけて記憶された所定条件用パブリックキー２４５と同一のキーであってよい。それら全てのパブリックキー２２５が、ここでは取得される。

【０１１３】

次に、パブリックキー管理サーバ２０１は、ステップＳ３０７の受信者パブリックキーの検索で取得された既登録ユーザのためのパブリックキー２２５を電子メール送信端末３０１に送信する（ステップＳ３１１）。送信されたそれぞれのパブリックキーは、ネットワークＩ／Ｆ２０５を経由し、ネットワーク６０２を介して電子メール送信端末３０１により受信される。

【０１１４】

次に、電子メール送信端末３０１は、パブリックキー管理サーバ２０１から送信された既登録ユーザのためのパブリックキー２２５を、それに対応する電子メールアドレスと対応させて送信端末内パブリックキー記憶領域３２０にさらに記憶させる（ステップＳ３１３）。これは、電子メール暗号化ソフトウェア３１３がＣＰＵ３０２によって実行されることにより実現されるステップであり、このことはこれ以降の電子メール暗号化ソフトウェア３１３が関連するステップにおいても同様である。

【０１１５】

次に、電子メール送信端末３０１は、電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成する（ステップＳ３１５）。共通鍵方式の暗号化キーは毎回新たに生成し、また一度使用した暗号化キーは破棄することが望ましいが（ワンタイム・キー）、何度も同じ鍵を用いることも可能である。共通鍵方式の暗号化キーを用いる理由は、第１の実施形態の説明において上述したとおりである。

【０１１６】

次に、電子メール送信端末３０１は、ステップＳ３０１で受け付けられた要求に含まれる受信者電子メールアドレスを宛先とする電子メールのコンテンツをコンテンツ暗号化キーで暗号化する（ステップＳ３１７）。暗号化されたコンテンツは、例えば添付ファイル

として電子メールに添付されてもよいし、そうでなくともよい。

【０１１７】

次に、電子メール送信端末３０１は、電子メールのコンテンツの暗号化に使用した「コンテンツ暗号化キー」を、受信者電子メールアドレスのそれぞれに対応する、送信端末内パブリックキー記憶領域３２０に記憶された１つ以上のパブリックキー３２５のそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する「暗号化されたコンテンツ暗号化キー」を生成する（ステップＳ３１９）。ここで、所定条件２４２を満たす受信者電子メールアドレスには、所定条件用パブリックキー２４５と同一のキーを含む複数のパブリックキー３２５が対応付けられている。これは、電子メール暗号化ソフトウェア３１３がＣＰＵ３０２により実行されることで実現されるものである。なお、例えば多数の受信者に対して暗号化メールを送信する場合でも、受信者電子メールアドレスそれぞれに対してのコンテンツ暗号化キー暗号化処理を操作者が個別に行う必要はなく、電子メール暗号化ソフトウェア３１３が透過的にこれらの処理を行う。

【０１１８】

次に、電子メール送信端末３０１は、暗号化された電子メールのコンテンツに、生成された暗号化されたコンテンツ暗号化キーのそれぞれを添付することによって、暗号化電子メールを生成する（ステップＳ３２１）。なお、好適には、その暗号化電子メールには、それが暗号化されていることが識別可能な情報を暗号化せずに添付する。

【０１１９】

そして、電子メール送信端末３０１は、暗号化電子メールを受信者電子メールアドレスに送信させる（ステップＳ３２３）。この送信は、典型的には、電子メールクライアント３１２がＣＰＵ３０２によって実行されることにより実現される。暗号化電子メールはメールサーバ６０１を経由し、ネットワーク６０２を介して転送され、電子メール受信端末４０１により受信される。また所定条件電子メール代表受信端末５０１も、所定条件２４２を満たす前記暗号化電子メールの少なくとも一部を受信できるように設定されている。これは例えば、メールサーバ６０１による所定条件電子メール代表受信端末５０１への自動転送や、プロバイダが提供するメールボックスの管理者用のメニューを利用すること、所定条件電子メール代表受信端末５０１に、所定条件２４２を満たす受信者電子メールアドレスのそれぞれのアカウント（及びパスワード）を設定すること、などによって実現される。また、所定条件電子メール代表受信端末５０１は、例えば電子メール管理用に構成された、自動的に管理対象の電子メールアドレスを宛先とする電子メールを受信するサーバとすることもでき、電子メール受信端末４０１が前記暗号化電子メールを所定条件電子メール代表受信端末５０１に対して転送することでもよい。

【０１２０】

電子メール受信端末４０１は、電子メール送信端末３０１から送信された暗号化電子メールを受信する（ステップＳ３２５）。これは、電子メールクライアント４１２がＣＰＵ４０２によって実行されることにより実現されるステップである。図２９は、電子メール暗号化ソフトウェアによって生成される、コンテンツが暗号化されていることが識別可能な情報を示す説明文のイメージ図である。受信した電子メールには、本来のコンテンツではなく（本来のコンテンツは未だ暗号化された状態である）、例えば図２９に示すような、コンテンツが暗号化されていることが識別可能な情報を示す説明文１００３が表示される。

【０１２１】

次に、電子メール受信端末４０１は、受信者電子メールアドレスに対応する暗号化されたコンテンツ暗号化キーを受信端末内プライベートキー記憶領域４５０に記憶されたプライベートキー４５６を用いて復号し、コンテンツ暗号化キーを回復する（ステップＳ３３５）。これは、電子メール暗号化ソフトウェア４１３がＣＰＵ４０２によって実行されることにより実現されるステップである。受信者電子メールアドレスが所定条件４２４を満たす場合、複数の暗号化されたコンテンツ暗号化キーが生成されており、そのそれぞれが暗号化電子メールに添付されているが、受信端末４０１が復号することができるのは、受

信端末内プライベートキー記憶領域４５０に記憶されたプライベートキー４５６とペアを成すパブリックキーで暗号化された、コンテンツ暗号化キーのみである。

【０１２２】

次に、電子メール受信端末４０１は、復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる（ステップＳ３３７）。この時点で、受信者は電子メールの本来のコンテンツにアクセスすることが可能となる。図３０は、回復された本来のコンテンツ１００５を表示している画面のイメージ図である。これによって、図２８に示した送信者によって暗号化される前のコンテンツ１００２が回復される。このように、暗号化のためのパブリックキーを公開しているユーザに対して、安全かつ確実に暗号化電子メールを送信することができる。

【０１２３】

所定条件電子メール代表受信端末５０１は、電子メール送信端末３０１から送信された所定条件２４２を満たす暗号化電子メールの少なくとも一部を受信する（ステップＳ３３９）。所定条件電子メール代表受信端末５０１は、例えば、所定条件２４２が電子メールアドレスがあるドメインに所属することであった場合、そのドメインに所属する任意の電子メールを受信できるように設定される。受信した暗号化電子メールには、本来のコンテンツではなく（本来のコンテンツは未だ暗号化された状態である）、例えば図２９に示すような、コンテンツが暗号化されていることが識別可能な情報を示す説明文１００３が表示される。

【０１２４】

次に、所定条件電子メール代表受信端末５０１は、受信者電子メールアドレスが満たす所定条件２４２に対応する暗号化されたコンテンツ暗号化キーを、代表受信端末内プライベートキー記憶領域５５０に記憶された所定条件用プライベートキー５５６を用いて復号し、コンテンツ暗号化キーを回復する（ステップＳ３４１）。これは、電子メール暗号化ソフトウェア５１３がＣＰＵ５０２によって実行されることにより実現されるステップである。受信者電子メールアドレスが所定条件４２４を満たす場合、複数の暗号化されたコンテンツ暗号化キーが生成されており、そのそれぞれが暗号化電子メールに添付されているが、所定条件電子メール代表受信端末５０１が復号することができるのは、所定条件電子メール代表受信端末内プライベートキー記憶領域５５０に記憶されたプライベートキー５５６とペアを成すパブリックキーで暗号化された、コンテンツ暗号化キーのみである。

【０１２５】

次に、所定条件電子メール代表受信端末５０１は、復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号してコンテンツを回復させる（ステップＳ３４３）。この時点で、所定条件電子メール代表受信端末５０１の操作者は電子メールの本来のコンテンツにアクセスすることが可能となる。図３０は、回復された本来のコンテンツ１００５を表示している画面のイメージ図である。これによって、図２８に示した送信者によって暗号化される前のコンテンツ１００２が回復される。このように、暗号化のためのパブリックキーを公開しているユーザであって、それの登録電子メールアドレスが所定条件を満たす場合、そのユーザ送信する暗号化電子メールには、その所定条件に対応するパブリックキーで暗号化されたコンテンツ暗号化キーが添付されることとなり、当該所定条件に関する管理者は、そのユーザに対する暗号化電子メールを、当該ユーザに関係なく復号することができる、安全性と管理の確実性を両立させることができる。

【０１２６】

パブリックキーが各記憶領域に記憶される形式はどのようなものであってもよい。パブリックキーが記述されたテキストファイルが各サーバ、端末内の特定のフォルダに電子メールアドレスと対応づけて格納されていてもよいし、または既存の特定のデータベース管理用ソフトウェアが管理できるファイル形式で、電子メールアドレスと対応づけて記憶されていてもよい。

【０１２７】

他には、パブリックキーを、パブリックキー管理サーバ２０１によるデジタル署名が付

加された電子証明書に含まれる情報として取り扱うことも可能である。この場合、電子メール受信端末４０１においてそのデジタル署名が検証されることにより、受信した暗号化電子メールの電子メールアドレスがパブリックキー管理サーバ２０１に真正に登録されたものであることを確認できるため、電子メールにおける相手方の信頼情報としても用いることが可能となる。さらに、電子証明書は、Ｘ．５０９規格のものとすることができ、この場合、標準的な電子メールクライアントであればその電子証明書を処理することができる。

【０１２８】

また、好適には、ステップＳ３０３における送信端末内受信者パブリックキー取得によるパブリックキーの取得の前に、それぞれの電子証明書が最新のものであるかどうかをパブリックキー管理サーバ２０１に問い合わせ、最新のものでなかった場合は最新のものをパブリックキー管理サーバ２０１から取得して、それで送信端末内パブリックキー記憶領域３２０を更新する。最新のものであるかどうかの判断には、電子証明書のシリアル番号のような、電子証明書を一意に識別できる情報を用いることが望ましい。これによって、パブリックキーが更新されていたり、所定条件用パブリックキーが追加されていたような場合に、最新のパブリックキーを受信端末で取得することができ、確実に暗号化電子メールを復号することができる。また、ユーザ登録を脱退したユーザについては、パブリックキー管理サーバ２０１から、その脱退ユーザに対する電子証明書を無効化するための情報を受信端末に送信することにより、その電子証明書を無効化することも可能である。

【０１２９】

なお、電子証明書が最新のものであるかどうかの問い合わせを、毎回の暗号化電子メール送信時に、全ての電子証明書について行えば、ネットワーク６０２にトラフィック増大をもたらしたり、電子メール暗号化ソフトウェアの円滑な動作を妨げる場合も考えられる。電子証明書は、それが最新であることが確認されてから所定のキャッシュ保持期間が経過するまでは最新のものと扱うこととして、電子証明書が最新のものであるかどうかのパブリックキー管理サーバ２０１への問い合わせは、前回の問い合わせから所定のキャッシュ保持期間が経過したことを条件として行われるようシステムを構成することもできる。これによって、システムの信頼性の確保と円滑な動作を両立させることができる。

【０１３０】

また、電子メール暗号化システム１００において、電子メール送信端末３０１が、送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアと、送信者電子メールアドレスとを対応させて記憶する送信端末内プライベートキー記憶領域３５０をさらに有するよう構成した上で（なお、これまでに述べた第２の実施形態において該送信端末内プライベートキー記憶領域３５０は必須の構成要素ではない）、さらに電子メール送信端末３０１が、送信者電子メールアドレスを発信元とし、受信者電子メールアドレスを宛先とする暗号化電子メールに対して送信端末内プライベートキー記憶領域３５０より取得されたプライベートキー３５６を利用したデジタル署名を付加するものであり、電子メール受信端末においてデジタル署名が検証されることにより受信した暗号化電子メールのコンテンツの真正性が確認されるよう、システムを構成することも可能である。これによって、暗号化電子メールが改竄されていないことが保証される。なお、パブリックキー管理サーバ２０１に送信者電子メールアドレスに対応するパブリックキーを要求し、それにより取得したパブリックキーでデジタル署名を検証すれば、送信者のプライベートキー３５６はその送信者のみがアクセスできるよう管理されるものであるため、送信された暗号化電子メールが、真正にパブリックキー管理サーバ２０１に登録された送信者から発信されたものであることを確認することもできる。

【０１３１】

なお、図３３に示すように、電子メール受信端末の電子メールクライアントには、受信した電子メールのうち、本発明に係る電子メール暗号化システム１００によって暗号化された電子メールに対して、フラグ１０１１が表示される。図３３は、電子メール暗号化ソフトウェアによって生成される、受信した電子メールが暗号化されていることを表わすフ

ラグを表示している画面のイメージ図である。このフラグを表示させるか否かの判断は、暗号化したコンテンツを含むファイルの拡張子が電子メール暗号化システム１００に特有のものであるかどうかで行うこともでき、また、パブリックキー管理サーバ２０１から取得したパブリックキーで復号可能であるかどうかを判断することで行うこともでき、また、暗号化電子メールに対してデジタル署名が付加されていた場合はそのデジタル署名がパブリックキー管理サーバ２０１から取得したパブリックキーで正当なものと検証されたかどうかで判断することもできる。また、受信した暗号化電子メールに所定条件用パブリックキーで暗号化されたコンテンツ暗号化キーが添付されていた場合には、フラグの色を変えるなどして、所定条件を満たす電子メールであることを識別可能に表示することもできる。

【０１３２】

ここで、所定条件用パブリックキー記憶領域２４０において管理される所定条件の典型的な例としては、受信者電子メールアドレスが所定のドメインに所属するものであるという条件が挙げられる。ドメインの管理者は、任意のドメイン管理用端末、または任意のドメイン管理用サーバを前記所定条件電子メール代表受信端末５０１として用い、ドメインに所属する電子メールアドレスに送信された暗号化電子メールを復号、管理する。

例えば会社内の電子メールアドレスを同一ドメインに所属させ、前記のような所定条件用キーペアを導入して管理するとすれば、ある社員の電子メール受信端末が使用できないような状況であったとしても、管理者によってその社員が受信した暗号化電子メールの内容を確認することが可能となる。

【０１３３】

このように、所定条件用キーペアによる暗号化電子メールの管理は、会社、行政官庁、学校、その他の法人、その他の組織による組織内電子メールの管理において特に有用性が高い。個人ユーザの登録は無料とする一方で、所定の条件と所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを所定条件用パブリックキー記憶領域２４０へ登録するためには、管理料金の支払いが必要であっても、それらの組織はそれに見合う十分な価値を認めるものと考えられる。このようにすれば、ユーザであるそれらの組織も電子メールの簡便かつ安全な暗号化と適切な一元管理という利益を享受することができるとともに、電子メール暗号化システム１００の管理主体に経済的な利益をもたらすものともなる。

【０１３４】

以上説明してきた第１の実施形態と第２の実施形態は、適宜、組み合わせて実施することができる。例えば、未登録ユーザへの暗号化電子メールの送信が可能であり、かつ、所定条件用パブリックキーが使用されていて代表受信端末での受信も可能であるような形態で実施することができる。

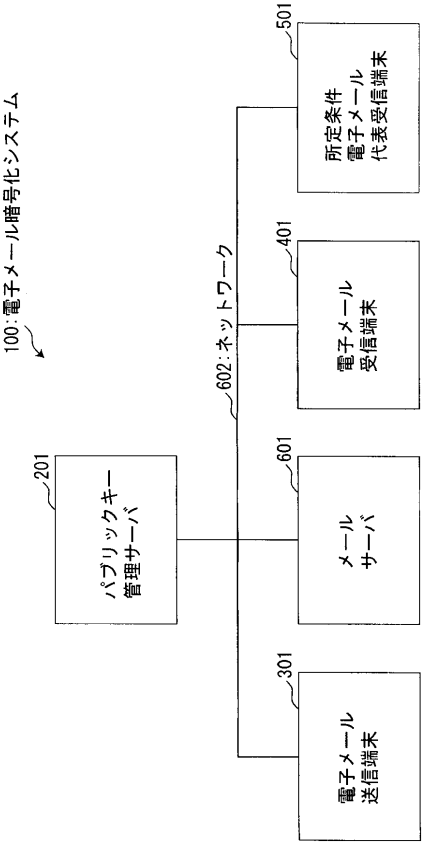
【符号の説明】

【０１３５】

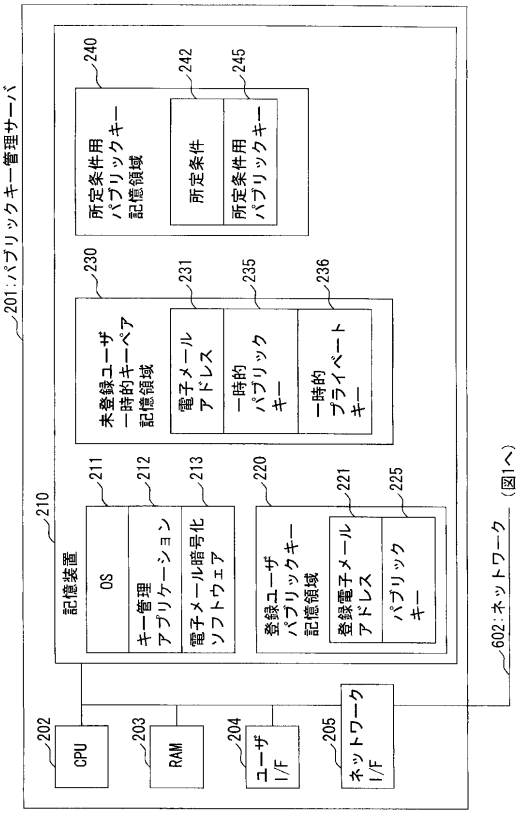
１００　電子メール暗号化システム
２０１　パブリックキー管理サーバ
２０２　ＣＰＵ
２０３　ＲＡＭ
２０４　ユーザＩ／Ｆ
２０５　ネットワークＩ／Ｆ
２１０　記憶装置
２１１　ＯＳ
２１２　キー管理アプリケーション
２１３　電子メール暗号化ソフトウェア
２２０　登録ユーザパブリックキー記憶領域
２２１　登録電子メールアドレス
２２５　パブリックキー

２３０　未登録ユーザ一時的キーペア記憶領域
２３１　電子メールアドレス
２３５　一時的パブリックキー
２３６　一時的プライベートキー
２４０　所定条件用パブリックキー記憶領域
２４２　所定条件
２４５　所定条件用パブリックキー
３０１　電子メール送信端末
３０２　ＣＰＵ
３０３　ＲＡＭ
３０４　ユーザＩ／Ｆ
３０５　ネットワークＩ／Ｆ
３１０　記憶装置
３１１　ＯＳ
３１２　電子メールクライアント
３１３　電子メール暗号化ソフトウェア
３２０　送信端末内登録ユーザパブリックキー記憶領域
３２１　登録電子メールアドレス
３２５　パブリックキー
３５０　送信端末内プライベートキー記憶領域
３５１　送信者電子メールアドレス
３５５　パブリックキー
３５６　プライベートキー
４０１　電子メール受信端末
４０２　ＣＰＵ
４０３　ＲＡＭ
４０４　ユーザＩ／Ｆ
４０５　ネットワークＩ／Ｆ
４１０　記憶装置
４１１　ＯＳ
４１２　電子メールクライアント
４１３　電子メール暗号化ソフトウェア
４５０　受信端末内プライベートキー記憶領域
４５１　送信者電子メールアドレス
４５５　パブリックキー
４５６　プライベートキー
５０１　所定条件電子メール代表受信端末
５０２　ＣＰＵ
５０３　ＲＡＭ
５０４　ユーザＩ／Ｆ
５０５　ネットワークＩ／Ｆ
５１０　記憶装置
５１１　ＯＳ
５１２　電子メールクライアント
５１３　電子メール暗号化ソフトウェア
５５０　代表受信端末内プライベートキー記憶領域
５５５　所定条件用パブリックキー
５５６　所定条件用プライベートキー
６０１　メールサーバ
６０２　ネットワーク

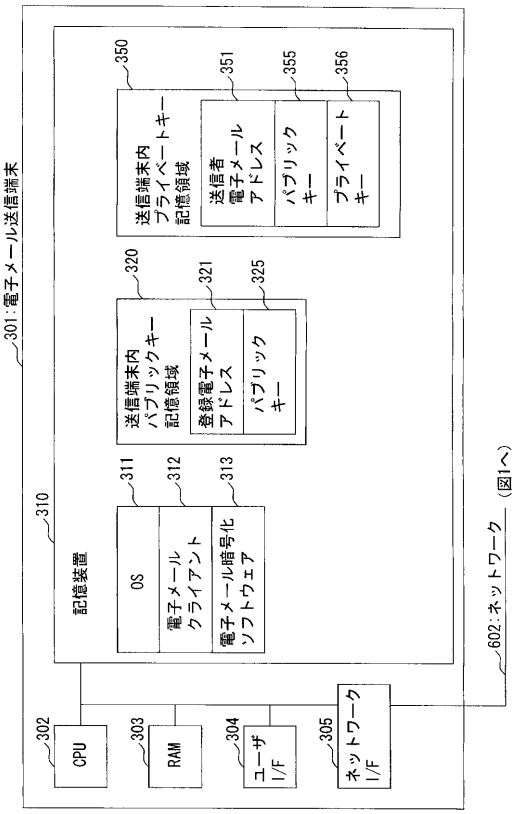
【図１】


100:電子メール暗号化システム
201
パブリックキー
管理サーバ
602:ネットワーク
601
メール
サーバ
301
電子メール
送信端末
401
電子メール
受信端末
501
所定条件
電子メール
代表受信端末

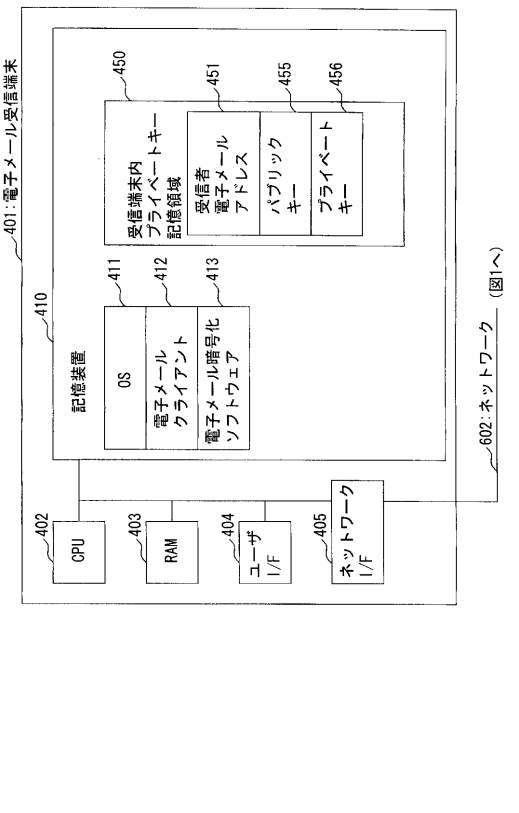
【図２】


201:パブリックキー管理サーバ
210
記憶装置
211
OS
212
キー管理
アプリケーション
213
電子メール暗号化
ソフトウェア
220
登録ユーザ
パブリックキー
記憶領域
221
登録電子メール
アドレス
225
パブリック
キー
230
未登録ユーザ
一時的キーペア
記憶領域
231
電子メール
アドレス
235
一時的
パブリック
キー
236
一時的
プライベート
キー
240
所定条件用
パブリックキー
記憶領域
242
所定条件
245
所定条件用
パブリックキー
202
CPU
203
RAM
204
ユーザ
I/F
205
ネットワーク
I/F
602:ネットワーク
(図1へ)

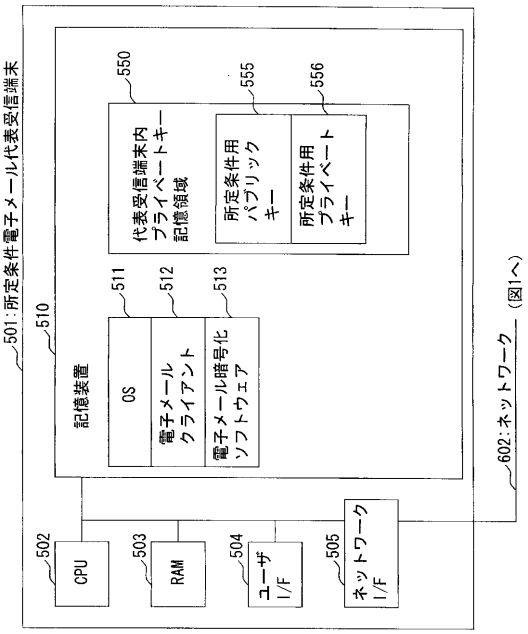
【図３】


301:電子メール送信端末
310
記憶装置
311
OS
312
電子メール
クライアント
313
電子メール暗号化
ソフトウェア
320
送信端末内
パブリックキー
記憶領域
321
登録電子メール
アドレス
325
パブリック
キー
350
送信端末内
プライベートキー
記憶領域
351
送信者
電子メール
アドレス
355
パブリック
キー
356
プライベート
キー
302
CPU
303
RAM
304
ユーザ
I/F
305
ネットワーク
I/F
602:ネットワーク
(図1へ)

【図４】


401:電子メール受信端末
410
記憶装置
411
OS
412
電子メール
クライアント
413
電子メール暗号化
ソフトウェア
450
受信端末内
プライベートキー
記憶領域
451
受信者
電子メール
アドレス
455
パブリック
キー
456
プライベート
キー
402
CPU
403
RAM
404
ユーザ
I/F
405
ネットワーク
I/F
602:ネットワーク
(図1へ)

【図５】



【図６】

```
mQCNAzMRY/IAAAEEAOloTOU0f4w7FDRMM6kA/6XazXxJ/HH8dsmb6E7RuYfVlXsd
kCwxUBOkyW+AYhkHbYUwnB5qBoFUyLrbLGuwKHWlKnAwgbeZLTH5nqQLpA0RlGVZ
v3tzImKUdyyxBphZWC4IeEgUbl9cc+piOsEJ8QzF7gnqwWo/Ku6tTPlJpWPZAAUR
tBdNYXJrIENveCA8bWFya0Bhd2UuY29tPokAlQMFEDQvYTHurUz9SaVj2QEB/hMD
/ix6pAa+4ZgFQNRAc7fC+I4uGWvXoI8N8wtgiJi//8Kclvjtv7ylLPKVBDsylihs
bVOjD3NUEkH95TNI3QhVeCwJP12e3GgFl253hj8Jai9snHj75pXjQXqONxQ/JRSr
EAqrFM7+yRLPs7zDwsMoc2Ox5emq4joVa3syZUEwW7LxiQEVAwUQNLELtdZUWxzP
wQDlAQbWfQf/RtyM8Rw01RdQXH5fA2jLaQ1wD/VGldlxgAcLKVQIKR77iBPdfcrW
LyexGgQmltuVTGs5UlXPf7dff2lNP79aglvD9hll82L5wZQybNpy2o6/66EPp4OW
Fl/WG7JhuCRfy53H983ERZnqGD4YeBafLHl9oGAixZ9G/+cFsxPde3Lv7Ij/lHwp
eNAHJQibBkpdq29Kye/+PHqE0HTMSapYXN/YVTCpEfzE46YnD/BjzZ/ElUClvcsW
ZVoqFR46HARVQNu+MfoR/WSBAOj65Dt5oBZTcLoQ7TyDcd4gvLhdzLUo+kboGTjt
HLvesaAWKLSWtKY6G8Iy7R5+Ms0helLFaIkARgQQEQIABgUCOGjpBQAKCRAXWVXO
Q77mqABMAKCgO+LVARom7t/XmRw4w4TO9IkM9gCgh2URPU7tqECsr+WuVfC/v/7e
vVWJAD8DBRA02GubUX4eqU/cq8ERAgUbAKCO9l3wXBCqiBfQBT5F6koRZRRvbQCf
fJ+Y14jFEx+cfCdDIUjjD0l4/diJAEYEEBECAAYFAjvQk5wACgkQVZbdDOm/ZT0n
TQCfdqn38SRRYeIG3+LIPqBdODr39JwAmgOH2/N2hjA2Z/4QMOjrQ4qIgpAPiQBG
BBARAgAGBQI7zAqEAAoJEKFQ/C2FqPeL7C8AnRr7d0vN+ElW218XjItFonLw42qT
AJ4xUrPsSduizUQnOuzdR8x2x4yEyIkARgQQEQIABgUCOjcVtAAKCRDe3YS5RDds
3Dz/AJ9UaB2vKuteTC+gm80f028DPbmCegCq3ZM1Rt2WMDS/wHW7nQJ/xnyg8PuJ
AD8DBRA6ynJX/W+IxiHQpxsRAjd/AKCSXqSmTnrzlnpgYwMESQiKQxfOywCeNuUy
0q65a+C/ayC7t6F6ih9+bcW0GUlhcmsgQ294IDxtamNAYXBhY2hlLm9yZz6JAJUD
BRA54aHP7qlM/UmlY9kBASflBACwKxBv5osTZpJIiKsdim/P2LHOtU91Ne8kxTdr
78Q86cHSz8V0ExA/FWKkOPgEHAIncXItNH0t3pGtUbAcYuT830Y7OJqLZdEWszQc
bsp72nlKOceZ6SFRE/ouDlcnyaiou2814JGlttqi08yO6LcX3sQD8wDaQhoUoCe9
wg/eaokAlQMFEDrLUyUbCAxFJxmvNQEB3XgD/2M9X5cgqjItm4vH9CjkAEOvfYh0
KjDTy9/WA0mVDcXvV9RZGMMnWmSKglyD7p4A8lWEQkk6VxZEMwWlPTtsFlOAyEQT
2QiRQtS6tFTj8X9aZ6a0PeYF5PyS20hvJzYXpbogkemBFtUDmsfXToSoO6UzlE3q
eTYYIMB01pImXvdpiQBGBBARAgAGBQI70JOfAAoJEFWW3QzpvZU9XQYAmwfOqWaT
wJFN0bz/9PL1xJRO0J+ZAKCHUML3L2N1yqR0CXTO2C40fDjsMokAPwMFEDrKcnL9
b4jGIdCnGxECMsMAoPGRixfMANAdwK0OwFjayMH0GV0PAJ4kP7UxlR3DkU/5wTOZ
dGL/zRRHJrQZTWFyayBDb3ggPGlqY0ByZWRoYXQuY29tPokAlQMFEDnhofnurUz9
SaVj2QEBJxcD/017elbFJGNcISL2dIvINhnXnzHxL6B66exG+8+lpFkR8e/EvgEv
XHMs2+AqDfUxkblPNSoq/u/m/VpJGEWoObuSkiwiqUYrmXcJGElUQyHMLDKSLQQh
G4PkeSp0T2yX+Fk+5F3vIOdK53jsD2lzXgB5QD7TjCLSGkU+BiLuLGX6iQBGBBAR
AgAGBQI70JOfAAoJEFWW3Qzpv2U9p6kAn3lo65wMqy/XbG+RqeJlrQQk0v5tAJ9e
zLVU5oVtfnH6JvAZFvi8sudRhokARgQQEQIABgUCO8WKigAKCRChUPwthaj3i4gq
AKC67ZkCrpAZWQKPJdWTw6zn6GsyVwCfQyoy5lGIuGBu0je6You3NEakk36JAD8D
BRA6ynJ4/W+IxiHQpxsRAsw3AKCqcCFo5uzU7XEom82HnvX7kSPDtACeIqOnzHMb
ArpmDAcknLxcmsjp2J4=
```

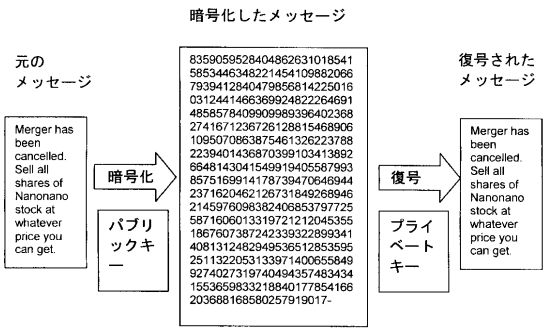
パブリックキーの例

【図７】

```
OWdFYqGfHBTZNSxFxlHS6NwpjQlw8RlginnkkqiUlkqePlGlL4NMgXh0la0t
EykFBXXkQix7ZqqCzTT+AYlj4MuOfN8IZlGiKFj2tK4q6+wmj9h2LVOjKtel
R3nYIKlUBRebw73vGhGVua25A6rxzt/h93hpWubtoeRWkNIgrRo=
b8DlurTu6f3EQtecBY5mECQAfrMlAm3UgEk0hotq84+UaNAv+DHO9Tyvrscm
ERCqabcbjSOs3vdt83IRElw2AdCvclTnmi0T5g3L3qdPMk9j0Yf5773+ZdEH
nRhY/a2ghcUAAbc2L2HuMOZTlMkbcwsrrkKeshhPD+z9YomjHuFK/PPAdF8m
5MeLmLq54acirtvJbCZZ96pSKZBy8jJ4zGyxxeKAXxXHrJbw0YE4D9leBnAE
qmSJz6yS9iDnDa8gvNLlpoICrkeBW3+EaHd2NKh8rv3NiwpTdlOmQ93Nhctp
cqNgizD0SdHeTMqavBMLWlyzCOOVQ0EAko/F0PUhNxC7DwQFgLRPs2JGUWK7
0fOFCH+lFlYEDUitHh3wZGYBAYjHX9ZIPZjQQ3A3lOGD9r+oTZ1/h5AjukDp
n0KALFEQX63honYcOBChzhlT+Ade/uHgPkiPAkp9jiFuAmC0t7Z28cYEhglE
N5wwKFmI+tHwhzNx8K67iAa6Ia2yTfDG2+Jx77ss6YpVxbdfDLCPfMLnL7Mj
nJbib7rJ3x9miQBcBcprptavCeD+IJprWyT2kKJcYvMY9YYCvOAFcDPlpXyV
jKP7e/pElsBj5VJYPvf4aqQqS76Uj8fsA3h34yjOuUtaoAi0ZYvf6APEzjlW
Q0y01HX/ZlIuMadSWU+bL4MCVxBnAhlUgyO2hmp0E/phpKwrJkWc3liecWTi
2JXHkNbiFdsh+epoONV2BH+XkHsuVg24J6SvL6/KClZpZ23a7R5WtRwjdkO7
dehHUDrcTNT7iJmNFpQ0blJ85vq42LDM2H12RsQGzX0i59uNIz30ivrghQ4h
f9cJjtUq8ldns+xeuDBF/MUo6804zNDBXk4ww36NcdTGzCCzpC7wuGzXjinf
U3DhEojpO2ZF+iCehqzjzgEKvMbgpJccClIxn9R8Qylmnypwl2bxvH7tCtc
KhoWgi59nY44v0DgFQV+Nk7wlxdH0+ME9aWWY0wkQ24NJWmj2EfU+yBHuV+C
gBcjK/FmxHEtm77g5zmjr0Msd8E/HjTTpiH7AFGhjH5+kOJGjk4wYD5Qokjy
6gODEEr27jhi8MwspxdNzl2UNNlZPIn39zhqUBRXXoqlZY5twzAfdhvZefpr
6ChwhxZqSgOGUtXhKv4SCQFNrUWTtel8rG3GxEkED5hqebMDTNliBmUA=
```

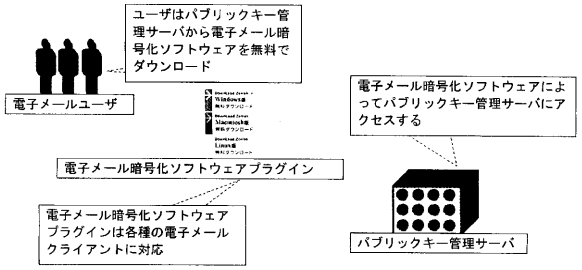
プライベートキーの例

【図８】



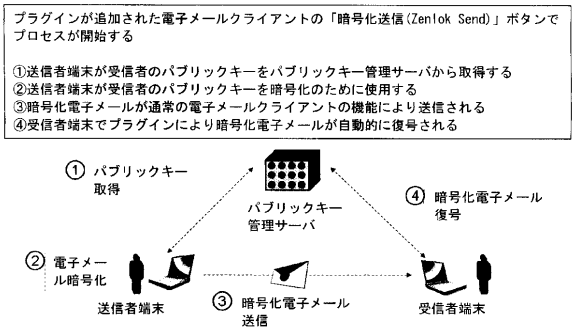
公開鍵方式の暗号化及び復号の例

【図９】



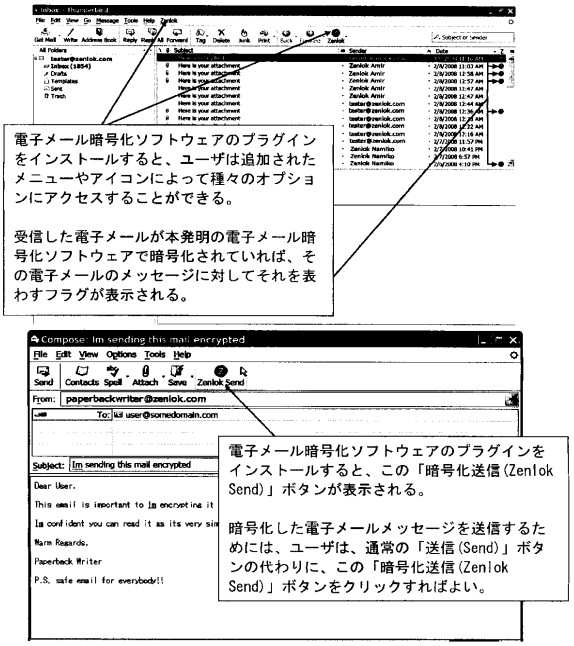
システムの構成の概要

【図１０】



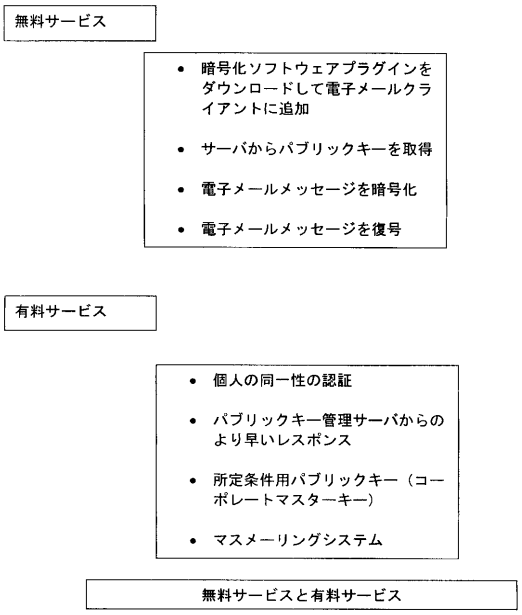
システムの動作の概要

【図１１】



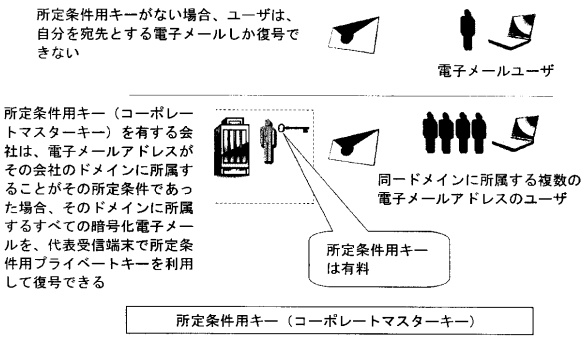
ユーザインターフェース

【図１２】



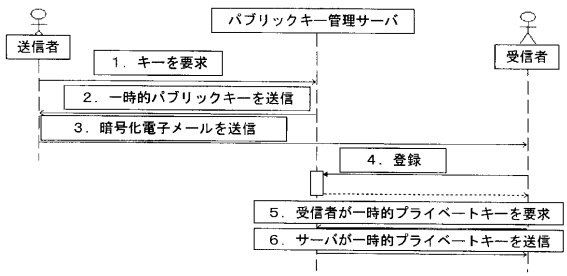
無料サービスと有料サービス

【図１３】



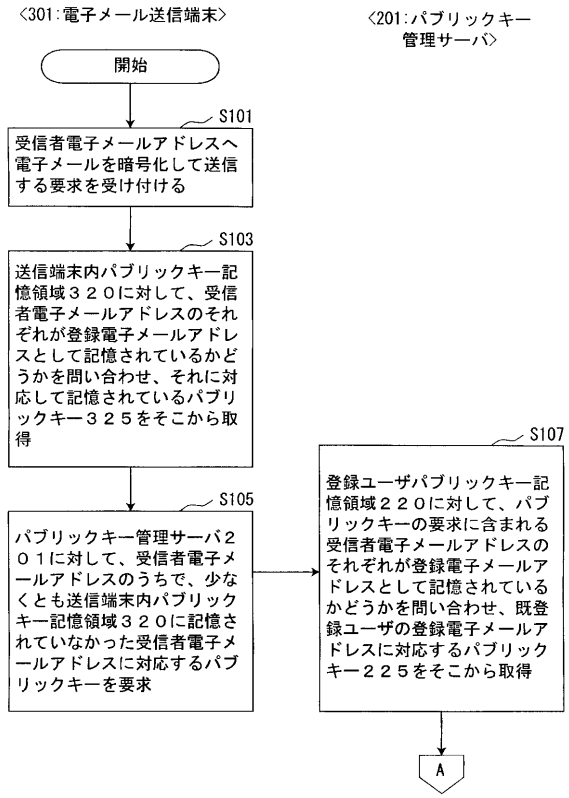
所定条件用キー（コーポレートマスターキー）

【図１４】

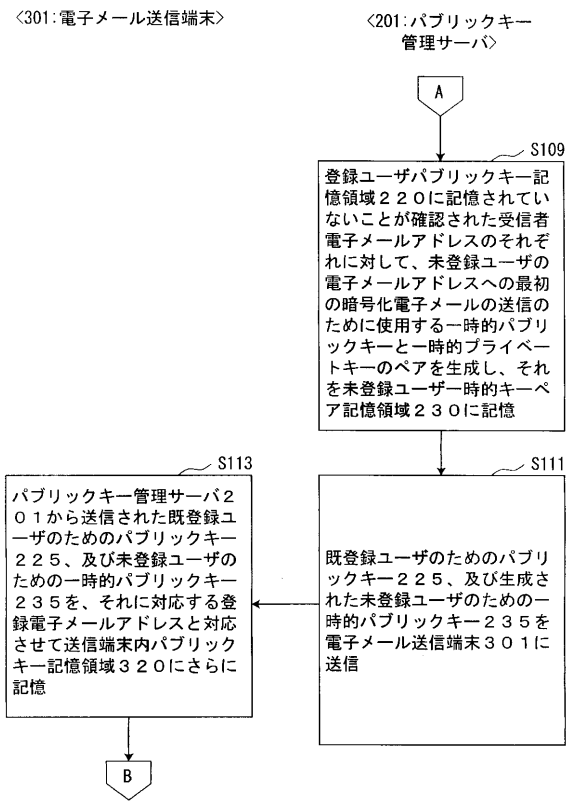


未登録ユーザへの暗号化電子メールの送信

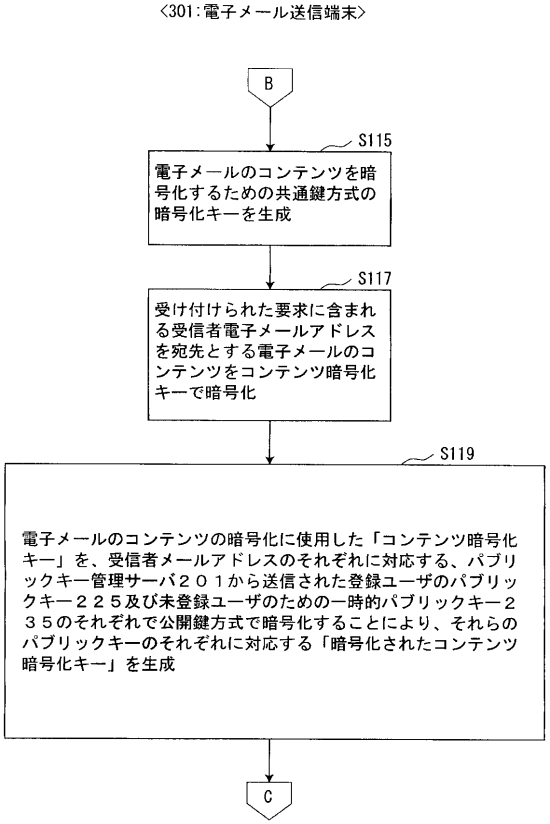
【図１５】



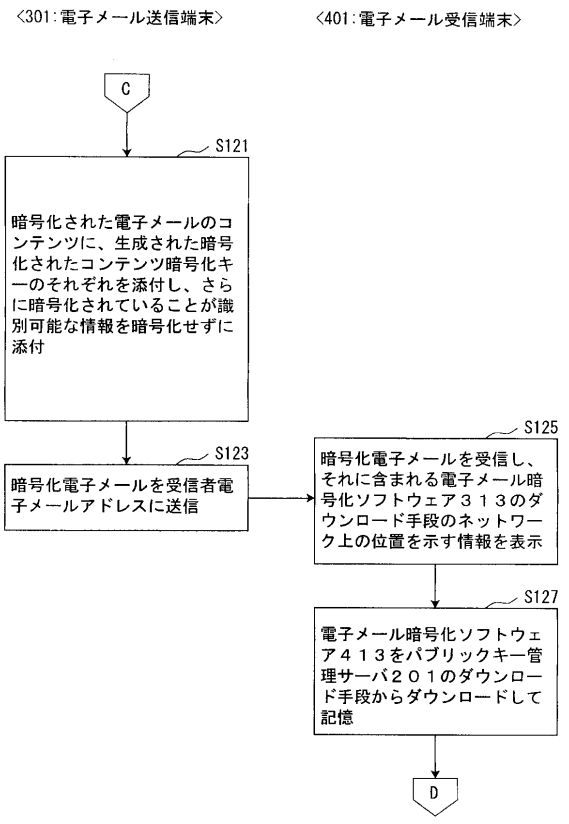
【図１６】



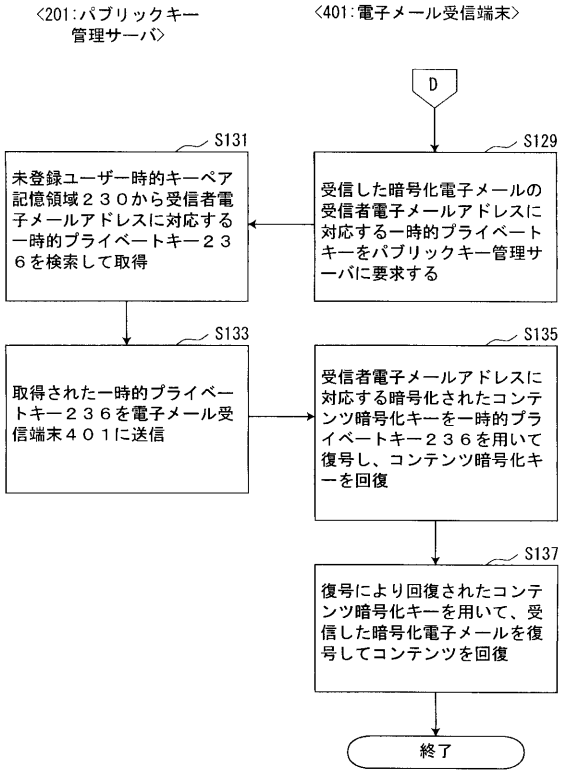
【図１７】



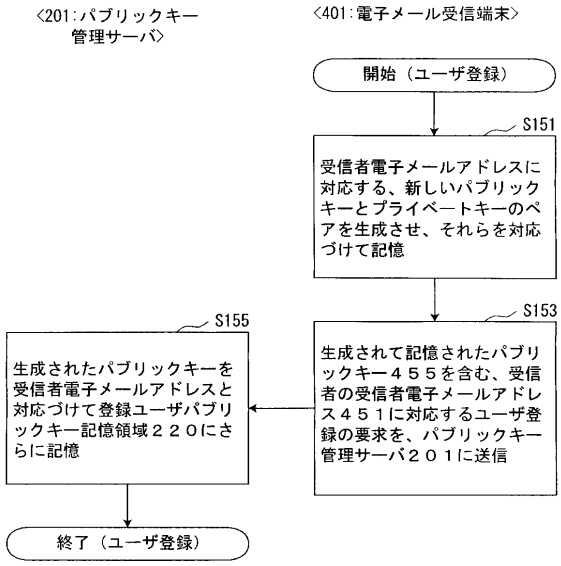
【図１８】



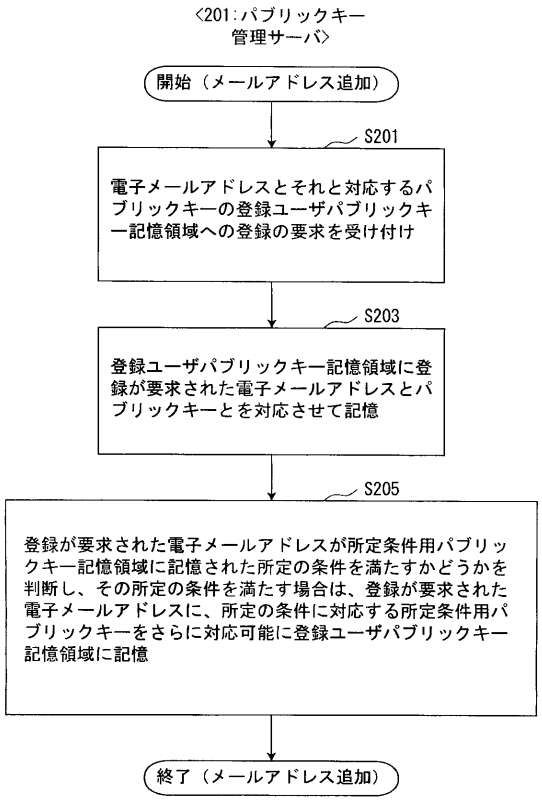
【図１９】



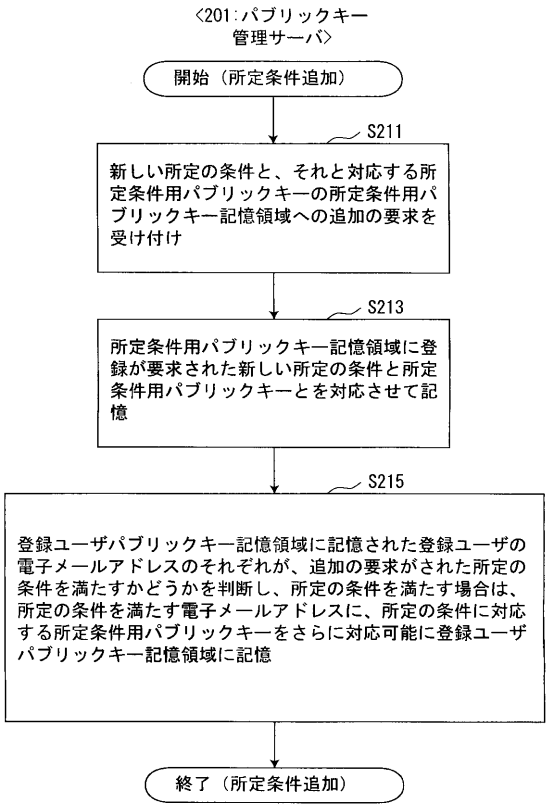
【図２０】



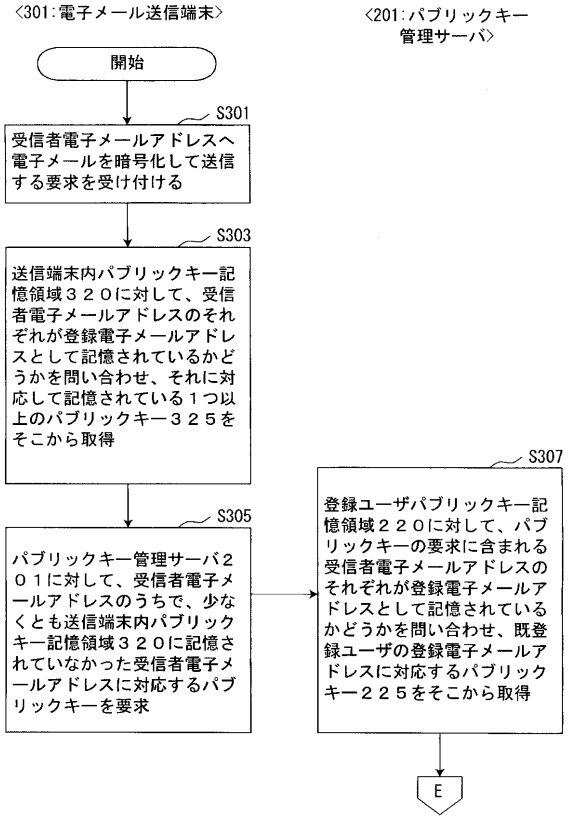
【図２１】



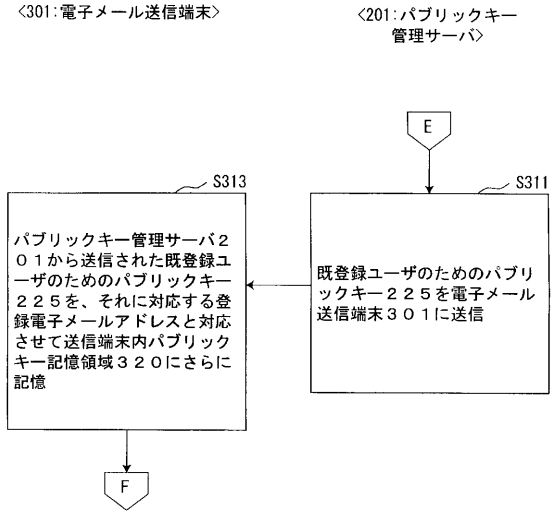
【図２２】



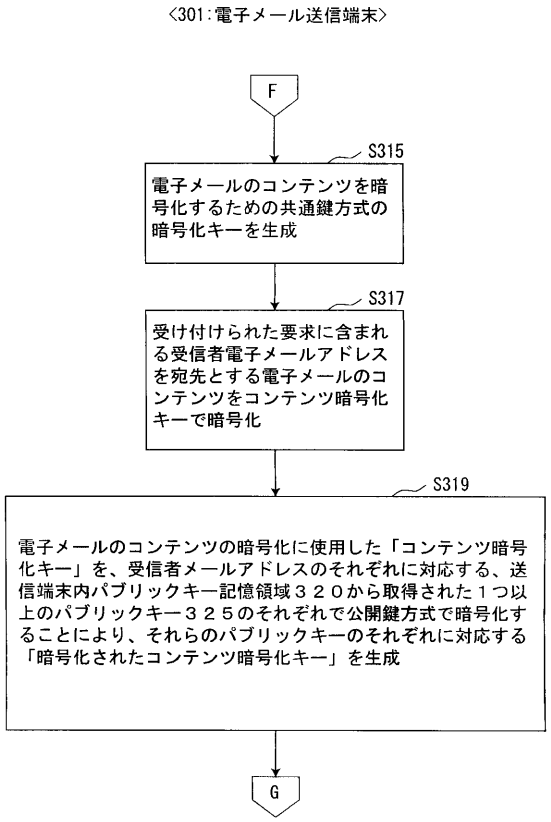
【図２３】



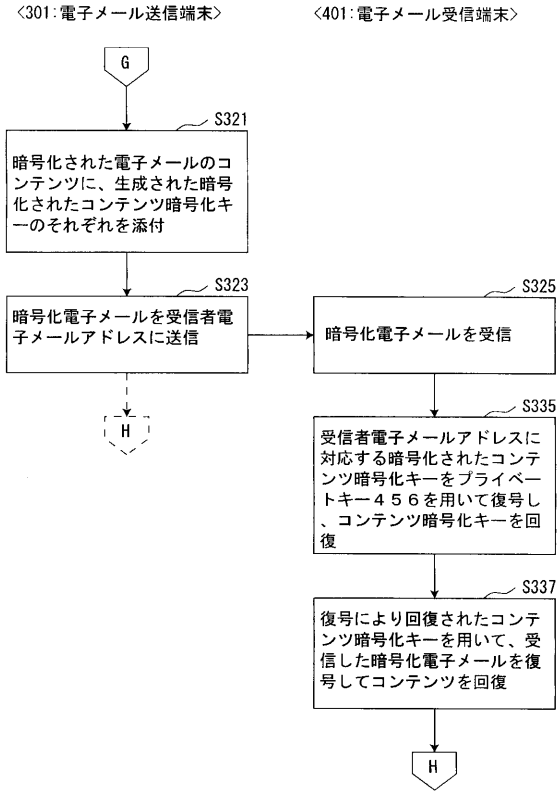
【図２４】



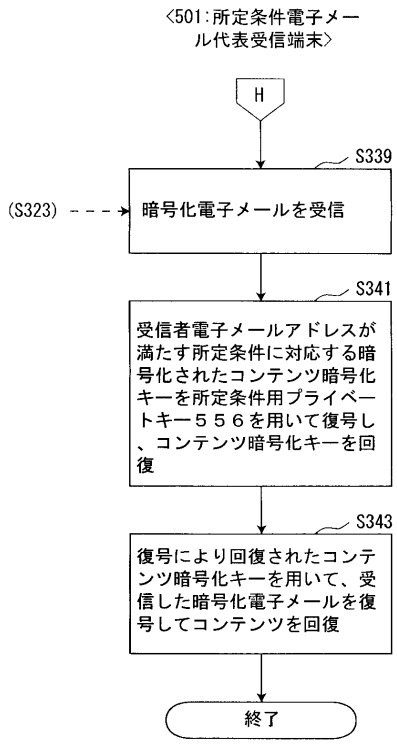
【図２５】



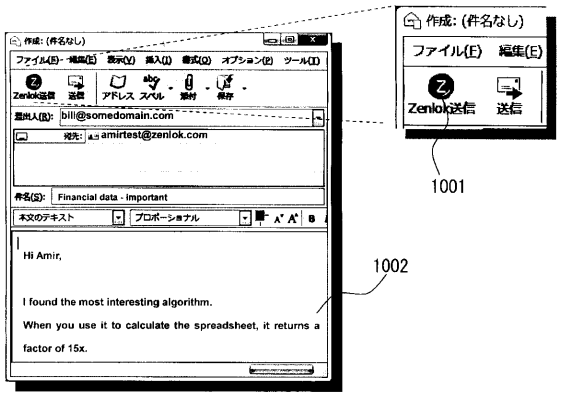
【図２６】



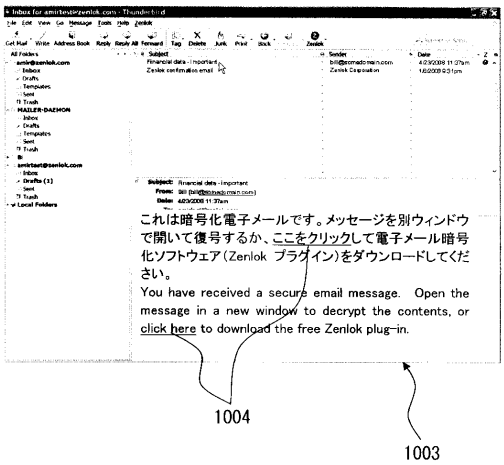
【図２７】



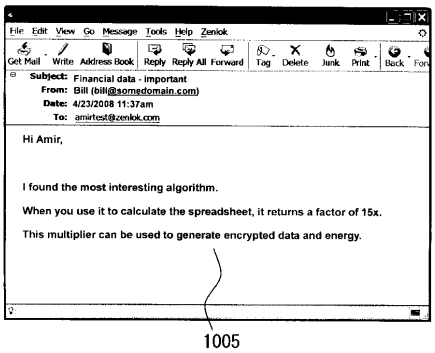
【図２８】



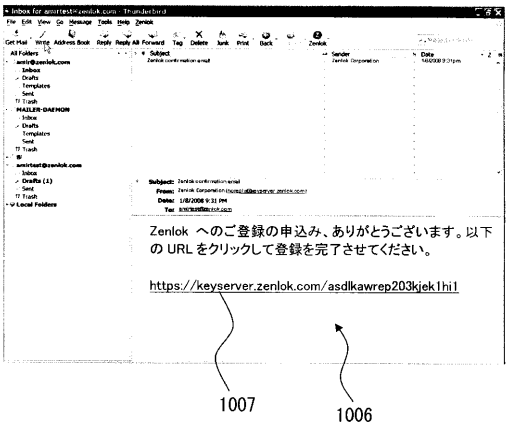
【図２９】



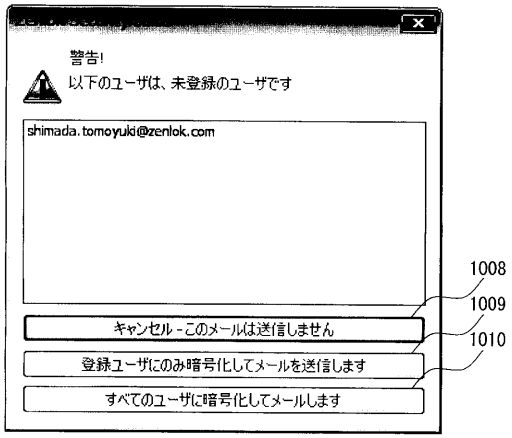
【図３０】



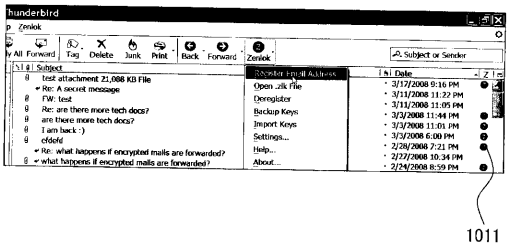
【図３１】



【図３２】



【図３３】



【手続補正書】
【提出日】平成21年8月17日(2009.8.17)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
電子メール暗号化のためのパブリックキーが登録されておらず、ユーザとしてあらかじめ登録されていない受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号させるための、前記電子メール送信端末及び前記電子メール受信端末とネットワークで接続されたパブリックキー管理サーバを含む、電子メール暗号化システムであって、
前記パブリックキー管理サーバは、
端末からの電子メール暗号化ソフトウェアのダウンロード要求に応じて前記電子メール暗号化ソフトウェアを前記端末にダウンロードさせるダウンロード手段と、
既登録ユーザの登録電子メールアドレスと、前記既登録ユーザの端末のためにプライベートキーとのペアとして生成したパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、
未登録ユーザの電子メールアドレスを、一時的パブリックキーと一時的プライベートキーとのペアと対応させて記憶する未登録ユーザ一時的キーペア記憶領域と、を有し、

前記電子メール送信端末は、
前記パブリックキー管理サーバからあらかじめ取得した、前記既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それに対応する登録電子メールアドレスとを対応させて記憶する送信端末内パブリックキー記憶領域と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、
前記電子メール送信端末は、前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、
前記送信端末内パブリックキー記憶領域に対して、前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、
前記パブリックキー管理サーバに対して、前記受信者電子メールアドレスのうちで、少なくとも前記送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、を実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール送信端末から前記受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、前記登録ユーザパブリックキー記憶領域に対して、前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、既登録ユーザの登録電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、
前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのうちで、前記受信者パブリックキー検索手段による問い合わせにより前記登録ユーザパブリックキー記憶領域に記憶されていないことが確認された受信者電子メールアドレスのそれぞれに対して、未登録ユーザの電子メールアドレスへの最初の暗号化電子メールの送信のために使用する一時的パブリックキーと一時的プライベートキーのペアを生成し、それを前記未登録ユーザ一時的キーペア記憶領域に記憶させる一時的キーペア生成記憶領域と、
前記受信者パブリックキー検索手段で取得された前記既登録ユーザのためのパブリックキー、及び前記一時的キーペア生成記憶領域で生成された前記未登録ユーザのための前記一時的パブリックキーを前記電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、
前記電子メール送信端末は、
前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記パブリックキー管理サーバから送信された前記既登録ユーザのためのパブリックキーを、それに対応する登録電子メールアドレスと対応させて前記送信端末内パブリックキー記憶領域にさらに記憶させる受信者パブリックキー記憶領域と、
電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、
前記電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる前記受信者電子メールアドレスを宛先とする電子メールのコンテンツを前記コンテンツ暗号化キーで暗号化する電子メールコンテンツ暗号化手段と、
前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記パブリックキー管理サーバから送信された既登録ユーザのパブリックキー及び前記未登録ユーザのための一時的パブリックキーのそれぞれで公開鍵方式によって暗号化することにより、それらのパブリックキーのそ

れぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、
前記電子メールコンテンツ暗号化手段によって暗号化された前記電子メールのコンテンツに、前記コンテンツ暗号化キー暗号化手段によって生成された前記暗号化されたコンテンツ暗号化キーのそれぞれを添付し、さらに前記電子メールのコンテンツが暗号化されていることが識別可能な情報を暗号化せずに添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、
前記暗号化電子メールを前記受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、
前記電子メール受信端末は、
前記電子メール送信端末から送信された前記暗号化電子メールを受信し、それに含まれる前記電子メールのコンテンツが暗号化されていることが識別可能な情報を表示するコンテンツ情報表示手段と、
前記電子メール暗号化ソフトウェアを前記ダウンロード手段からダウンロードして記憶する受信端末内ソフトウェア記憶領域と、を有し、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信した暗号化電子メールの前記受信者電子メールアドレスに対応する前記一時的プライベートキーを前記パブリックキー管理サーバに要求する一時的プライベートキー要求手段と、を実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール受信端末からの前記受信者電子メールアドレスに対応する一時的プライベートキーの要求を受信すると、前記未登録ユーザ一時的キーペア記憶領域から前記受信者電子メールアドレスに対応する一時的プライベートキーを取得する受信者一時的プライベートキー検索手段と、
前記受信者一時的プライベートキー検索手段で取得された一時的プライベートキーを前記電子メール受信端末に送信する一時的プライベートキー送信手段と、をさらに有し、
前記電子メール受信端末は、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスに対応する前記暗号化されたコンテンツ暗号化キーを前記パブリックキー管理サーバから送信された一時的プライベートキーを用いて復号し、前記コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであることを特徴とする、電子メール暗号化システム。
【請求項２】
請求項１に記載の電子メール暗号化システムにおいて、
前記電子メール暗号化手段によって暗号化されずに前記電子メールのコンテンツに添付される、暗号化されていることが識別可能な情報は、前記電子メール暗号化ソフトウェアのダウンロード手段のネットワーク上の位置を示す情報を含むことを特徴とする、電子メール暗号化システム。
【請求項３】
請求項１に記載の電子メール暗号化システムにおいて、
前記電子メール受信端末は、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスに対応する、新しいパブリックキーとプライベートキーのペアを生成させ、それらを対応づけて記憶させるキーペア生成記憶領域と、
前記生成されたパブリックキーを含む、前記受信者電子メールアドレスに対応するユー

ザ登録の要求を前記パブリックキー管理サーバに送信する生成パブリックキー送信手段と、をさらに実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール受信端末からの前記ユーザ登録の要求を受信すると、それに含まれる前記生成されたパブリックキーを前記受信者電子メールアドレスと対応づけて前記登録ユーザパブリックキー記憶領域にさらに記憶させる生成パブリックキー登録手段と、をさらに有することを特徴とする電子メール暗号化システム。
【請求項４】
請求項１に記載の電子メール暗号化システムにおいて、
前記送信端末内パブリックキー記憶領域は、前記パブリックキー管理サーバからあらかじめ取得した、所定の既登録ユーザの電子メールアドレスのそれぞれに対するパブリックキー、及び前記送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアを、それに対応する電子メールアドレスと対応させて記憶するものであり、
前記コンテンツ暗号化キー暗号化手段は、前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記パブリックキー管理サーバから送信された前記既登録ユーザのパブリックキー及び前記未登録ユーザのための一時的パブリックキー、並びに前記送信者電子メールアドレスに対応するパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するものであることを特徴とする電子メール暗号化システム。
【請求項５】
ユーザとして登録された受信者電子メールアドレスを宛先として、電子メール暗号化ソフトウェアが実行されることによってパブリックキーを利用して暗号化された暗号化電子メールをユーザとして登録された送信者電子メールアドレスを発信元として電子メール送信端末から送信することにより、前記暗号化電子メールを受信する電子メール受信端末で前記暗号化電子メールを復号し、前記受信者電子メールアドレスが所定の条件を満たす場合には、任意の前記所定の条件を満たす受信者電子メールアドレスを宛先とする暗号化電子メールを、前記所定の条件を満たす受信者電子メールアドレスを宛先とする前記暗号化電子メールの少なくとも一部を受信することができる所定条件電子メール代表受信端末で復号することができるようにするための、前記電子メール送信端末、前記電子メール受信端末、及び前記所定条件電子メール代表受信端末とネットワークで接続されたパブリックキー管理サーバを含む、電子メール暗号化システムであって、
前記パブリックキー管理サーバは、
登録された既登録ユーザの登録電子メールアドレスと、１つ以上のパブリックキーとを対応させて記憶する登録ユーザパブリックキー記憶領域と、
前記所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを対応させて記憶する所定条件用パブリックキー記憶領域と、
電子メールアドレスとそれと対応するパブリックキーの前記登録ユーザパブリックキー記憶領域への登録の要求を受け付け、前記登録ユーザパブリックキー記憶領域に登録が要求された前記電子メールアドレスと前記パブリックキーとを対応させて記憶させるとともに、登録が要求された前記電子メールアドレスが前記所定条件用パブリックキー記憶領域に記憶された前記所定の条件を満たすかどうかを判断し、前記所定の条件を満たす場合は、登録が要求された前記電子メールアドレスに、前記所定の条件に対応する前記所定条件用パブリックキーをさらに対応可能に前記登録ユーザパブリックキー記憶領域に記憶させる所定条件電子メールアドレス登録手段と、
を有し、
前記電子メール送信端末は、
前記パブリックキー管理サーバからあらかじめ取得した、前記既登録ユーザのうちの所定の既登録ユーザの登録電子メールアドレスのそれぞれに対するパブリックキーと、それ

に対応する登録電子メールアドレスとを対応可能に記憶する送信端末内パブリックキー記憶領域と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された送信端末内ソフトウェア記憶領域と、を有し、
前記電子メール送信端末は、前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
受信者電子メールアドレスへ電子メールを暗号化して送信する要求を受け付ける電子メール暗号化送信要求受付手段と、
前記送信端末内パブリックキー記憶領域に対して、前記受信者電子メールアドレスのそれぞれが前記登録電子メールアドレスとして記憶されているかどうかを問い合わせ、それに対応して記憶されているパブリックキーをそこから取得する端末内受信者パブリックキー取得手段と、
前記パブリックキー管理サーバに対して、前記受信者電子メールアドレスのうちで、少なくとも前記送信端末内パブリックキー記憶領域に記憶されていなかった受信者電子メールアドレスに対応するパブリックキーを要求する受信者パブリックキー要求手段と、
を実現するものであり、
前記パブリックキー管理サーバは、
前記電子メール送信端末から前記受信者電子メールアドレスに対応するパブリックキーの要求を受信すると、前記登録ユーザパブリックキー記憶領域に対して、前記パブリックキーの要求に含まれる前記受信者電子メールアドレスのそれぞれが記憶されているかどうかを問い合わせ、登録ユーザの電子メールアドレスに対応するパブリックキーをそこから取得する受信者パブリックキー検索手段と、
前記受信者パブリックキー検索手段で取得された前記登録ユーザのためのパブリックキーを前記電子メール送信端末に送信する要求パブリックキー送信手段と、をさらに有し、
前記電子メール送信端末は、
前記送信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記パブリックキー管理サーバから送信された前記登録ユーザのためのパブリックキーを、それに対応する電子メールアドレスと対応させて前記送信端末内パブリックキー記憶領域にさらに記憶させる受信者パブリックキー記憶領域と、
電子メールのコンテンツを暗号化するための共通鍵方式の暗号化キーを生成するコンテンツ暗号化キー生成手段と、
前記電子メール暗号化送信要求受付手段によって受け付けられた要求に含まれる前記受信者電子メールアドレスを宛先とする電子メールのコンテンツを前記コンテンツ暗号化キーで暗号化する電子メールコンテンツ暗号化手段と、
前記電子メールのコンテンツの暗号化に使用した前記コンテンツ暗号化キーを、前記受信者電子メールアドレスのそれぞれに対応する、前記送信端末内パブリックキー記憶領域に記憶されたパブリックキーのそれぞれで公開鍵方式で暗号化することにより、それらのパブリックキーのそれぞれに対応する暗号化されたコンテンツ暗号化キーを生成するコンテンツ暗号化キー暗号化手段と、
前記電子メールコンテンツ暗号化手段によって暗号化された前記電子メールのコンテンツに、前記コンテンツ暗号化キー暗号化手段によって生成された前記暗号化されたコンテンツ暗号化キーのそれぞれを添付することによって、暗号化電子メールを生成する電子メール暗号化手段と、
前記暗号化電子メールを前記受信者電子メールアドレスに送信させる電子メール送信手段と、をさらに実現するものであり、
前記電子メール受信端末は、
前記電子メール送信端末から送信された前記暗号化電子メールを受信する電子メール受信手段と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された受信端末内ソフトウェア記

憶領域と、
前記電子メール受信端末が受信する前記受信者電子メールアドレスに対するパブリックキーとペアをなす前記プライベートキーと、前記受信者電子メールアドレスとを対応させて記憶する受信端末内プライベートキー記憶領域と、を有し、
前記電子メール受信端末は、
前記受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスに対応する前記暗号化されたコンテンツ暗号化キーを前記受信端末内プライベートキー記憶領域に記憶されたプライベートキーを用いて復号し、前記コンテンツ暗号化キーを回復するコンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる暗号化電子メール復号手段と、
をさらに実現するものであり、
前記所定条件電子メール代表受信端末は、
前記電子メール送信端末から送信された前記所定の条件を満たす前記暗号化電子メールの少なくとも一部を受信する代表受信端末内電子メール受信手段と、
前記電子メール暗号化ソフトウェアがあらかじめ記憶された代表受信端末内ソフトウェア記憶領域と、
前記所定条件電子メール代表受信端末が受信する前記受信者電子メールアドレスが満たす前記所定の条件に対する前記所定条件用パブリックキーとペアをなす所定条件用プライベートキーを記憶する代表受信端末内プライベートキー記憶領域と、を有し、
前記所定条件電子メール代表受信端末は、
前記代表受信端末内ソフトウェア記憶領域に記憶された前記電子メール暗号化ソフトウェアがプロセッサによって実行されることにより、
前記受信者電子メールアドレスが満たす前記所定の条件に対応する前記暗号化されたコンテンツ暗号化キーを前記代表受信端末内プライベートキー記憶領域に記憶された前記所定条件用プライベートキーを用いて復号し、前記コンテンツ暗号化キーを回復する所定条件用コンテンツ暗号化キー復号手段と、
前記復号により回復されたコンテンツ暗号化キーを用いて、受信した暗号化電子メールを復号して前記コンテンツを回復させる所定条件用暗号化電子メール復号手段と、をさらに実現するものであることを特徴とする、電子メール暗号化システム。
【請求項６】
請求項５に記載の電子メール暗号化システムにおいて、前記パブリックキー管理サーバは、
新しい所定の条件とそれと対応する所定条件用パブリックキーの前記所定条件用パブリックキー記憶領域への追加の要求を受け付け、前記所定条件用パブリックキー記憶領域に登録が要求された前記新しい所定の条件と前記所定条件用パブリックキーとを対応させて記憶させるとともに、
前記登録ユーザパブリックキー記憶領域に記憶された前記登録ユーザの電子メールアドレスのそれぞれが、追加の要求がされた前記所定の条件を満たすかどうかを判断し、前記所定の条件を満たす場合は、前記所定の条件を満たす電子メールアドレスに、前記所定の条件に対応する前記所定条件用パブリックキーをさらに対応可能に前記登録ユーザパブリックキー記憶領域に記憶させる所定条件用パブリックキー追加手段、をさらに有することを特徴とする電子メール暗号化システム。
【請求項７】
請求項５に記載の電子メール暗号化システムにおいて、
前記登録ユーザの電子メールアドレスとそれに対応づけられたパブリックキーは、前記パブリックキー管理サーバによるデジタル署名が付加された電子証明書に含まれる情報として取り扱われるものであり、前記電子メール受信端末において前記デジタル署名が検証されることにより受信した暗号化電子メールの電子メールアドレスが前記パブリックキー

管理サーバに真正に登録されたものであることを確認できるようになっていることを特徴とする電子メール暗号化システム。

【請求項８】

請求項７に記載の電子メール暗号化システムにおいて、

前記端末内受信者パブリックキー取得手段によるパブリックキーの取得の前に、それぞれの前記電子証明書が最新のものであるかどうかを前記パブリックキー管理サーバに問い合わせ、最新のものでなかった場合は最新のものを前記パブリックキー管理サーバから取得してそれで前記送信端末内パブリックキー記憶領域を更新する前記端末内受信者パブリックキー最新確認手段をさらに有することを特徴とする電子メール暗号化システム。

【請求項９】

請求項８に記載の電子メール暗号化システムにおいて、

前記電子証明書が最新のものであるかどうかの前記パブリックキー管理サーバへの問い合わせは、前回の問合わせから所定のキャッシュ保持期間が経過したことを条件として行われることを特徴とする電子メール暗号化システム。

【請求項１０】

請求項５に記載の電子メール暗号化システムにおいて、

前記電子メール送信端末は、前記送信者電子メールアドレスに対するパブリックキーとプライベートキーのペアと、前記送信者電子メールアドレスとを対応させて記憶する送信端末内プライベートキー記憶領域、をさらに有し、

前記電子メール送信端末は、前記送信者電子メールアドレスを発信元とし、前記受信者電子メールアドレスを宛先とする暗号化電子メールに対して前記プライベートキーを利用したデジタル署名を付加するものであり、前記電子メール受信端末において前記デジタル署名が検証されることにより受信した暗号化電子メールのコンテンツの真正性が確認されることを特徴とする電子メール暗号化システム。

【請求項１１】

請求項１０に記載の電子メール暗号化システムにおいて、

前記電子メール受信端末における前記デジタル署名の検証は、前記パブリックキー管理サーバから取得したパブリックキーによって行われるものであり、それによって、受信した暗号化電子メールの送信者が前記パブリックキー管理サーバに真正に登録されたユーザであることがさらに確認されることを特徴とする電子メール暗号化システム。

【請求項１２】

請求項５に記載の電子メール暗号化システムにおいて、

前記所定の条件は、前記受信者電子メールアドレスが所定のドメインに所属するものであることを特徴とする電子メール暗号化システム。

【請求項１３】

請求項１２に記載の電子メール暗号化システムにおいて、

前記パブリックキー管理サーバは、所定の管理料金が支払われた前記所定のドメインに対して、前記所定の条件とその所定の条件を満たす受信者電子メールアドレスのためのパブリックキーである所定条件用パブリックキーとを、前記所定条件用パブリックキー記憶領域に、対応させて記憶することを特徴とする電子メール暗号化システム。

フロントページの続き

(72)発明者　アヤロン　アミール
東京都中央区銀座１丁目１５番１３号９０４　Ｚｅｎｌｏｋ株式会社内

Ｆターム(参考) 5B084 AA01 AA15 AB02 BB16 CB04
5J104 AA16 AA32 EA01 EA04 EA08 EA17 JA03 JA21 NA02 NA05
NA36 NA37 PA08