(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年 8 月 27 日(27.08.2009)

PCT

(10) 国際公開番号
WO 2009/104285 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G06F 13/00* (2006.01)

(21) 国際出願番号: PCT/JP2008/058975

(22) 国際出願日: 2008 年 5 月 15 日(15.05.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
12/072,006 2008 年 2 月 21 日(21.02.2008) US

(71) 出願人 (米国を除く全ての指定国について): Ｚｅｎｌｏｋ株式会社(Zenlok Corporation) [JP/JP]; 〒1040061 東京都中央区銀座１丁目１５番１３号９０４ Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): アヤロン アミール(AYALON, Amir) [AU/JP]; 〒1040061 東京都中央区銀座１丁目１５番１３号９０４ Ｚｅｎｌｏｋ株式会社内 Tokyo (JP).

(74) 代理人: 熊倉 禎男, 外(KUMAKURA, Yoshio et al.); 〒1008355 東京都千代田区丸の内３丁目３番１号 新東京ビル 中村合同特許法律事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

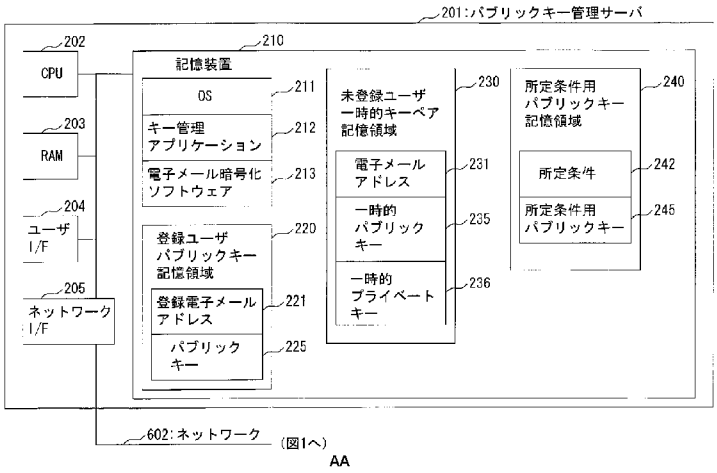
[続葉有]

(54) **Title**: ELECTRONIC MAIL CIPHERING SYSTEM

(54) 発明の名称: 電子メール暗号化システム

[図2]

FIG. 2



201 PUBLIC KEY MANAGING SERVER
204 USER I/F
205 NETWORK I/F
210 STORAGE DEVICE
212 KEY MANAGEMENT APPLICATION
213 ELECTRONIC MAIL CIPHERING SOFTWARE
220 REGISTERED USER PUBLIC KEY STORING REGION
221 REGISTERED ELECTRONIC MAIL ADDRESS
225 PUBLIC KEY
230 UNREGISTERED USER TEMPORARY KEY PAIR STORING REGION
231 ELECTRONIC MAIL ADDRESS
235 TEMPORARY PUBLIC KEY
236 TEMPORARY PRIVATE KEY
240 PRESCRIBED CONDITION PUBLIC KEY STORING REGION
242 PRESCRIBED CONDITION
245 PRESCRIBED CONDITION PUBLIC KEY
602 NETWORK
AA (TO FIGURE 1)

(57) **Abstract**: A ciphered mail is transmitted to an unregistered user. The ciphered mail can be decoded not only in a mail reception terminal being an original destination but also in a prescribed condition mail representative reception terminal. At the time of transmitting an electronic mail to the unregistered user, a temporary pubic key and a private key are generated in a server. The temporary public key is sent from the server to a mail transmission terminal and the mail is ciphered by using the temporary public key. The temporary private key is sent from the server to the mail reception terminal and the ciphered mail is decoded by using the temporary private key. The public key corresponding to a mail address satisfying a prescribed condition and a public key for prescribed condition, which corresponds to the prescribed condition, are disclosed in association with each other for the mail address satisfying the prescribed condition. Thus, the mail where the mail address satisfying the prescribed condition is set to be the destination is decoded in the mail representative reception terminal.

(57) 要約:

[続葉有]

WO 2009/104285 A1

MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

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。　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。

明 細 書

電子メール暗号化システム

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。

[0013] 非特許文献1:米国特許第7174368号

発明の開示

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。

発明を実施するための最良の形態

[0052] 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。

[0053] 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。

[0054] 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。

[0055] 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。

[0056] [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。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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。

[0068] 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。

[0069] ［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。

[0070] 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。

[0071] [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。

[0072] 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。

[0073] 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。

[0074] 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。

[0075] 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。

[0076] 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)。

[0077] 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。

[0078] 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。

[0079] 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。

[0080] 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。

[0081] 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。

[0082] 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。

[0083] 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。

[0084] 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。

[0085] 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410に記憶される(電子メール暗号化ソフトウェア413)。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 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。

[0090] 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。

[0091] 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。

[0092] 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。

[0093] 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。

[0094] 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。

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 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。

[0099] 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。

[0100] 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。

[0101] [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。

[0102] 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。

[0103] 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。

[0104] 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。

[0105] 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。

[0106] 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。

[0107] 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。

[0108] 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。

[0109] 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325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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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。

[0115] 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。

[0116] 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。

[0117] 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。

[0118] 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。

[0119] 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。

[0120] 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。

[0121] 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。

[0122] 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。

[0123] 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。

[0124] 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。

[0125] 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。

[0126] 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。

[0127] 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。

[0128] 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。

[0129] 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。

[0130] 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1

00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。

[0131] 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。

[0132] 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。

[0133] 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。

図面の簡単な説明

[0134] [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。

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

請求の範囲

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[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、

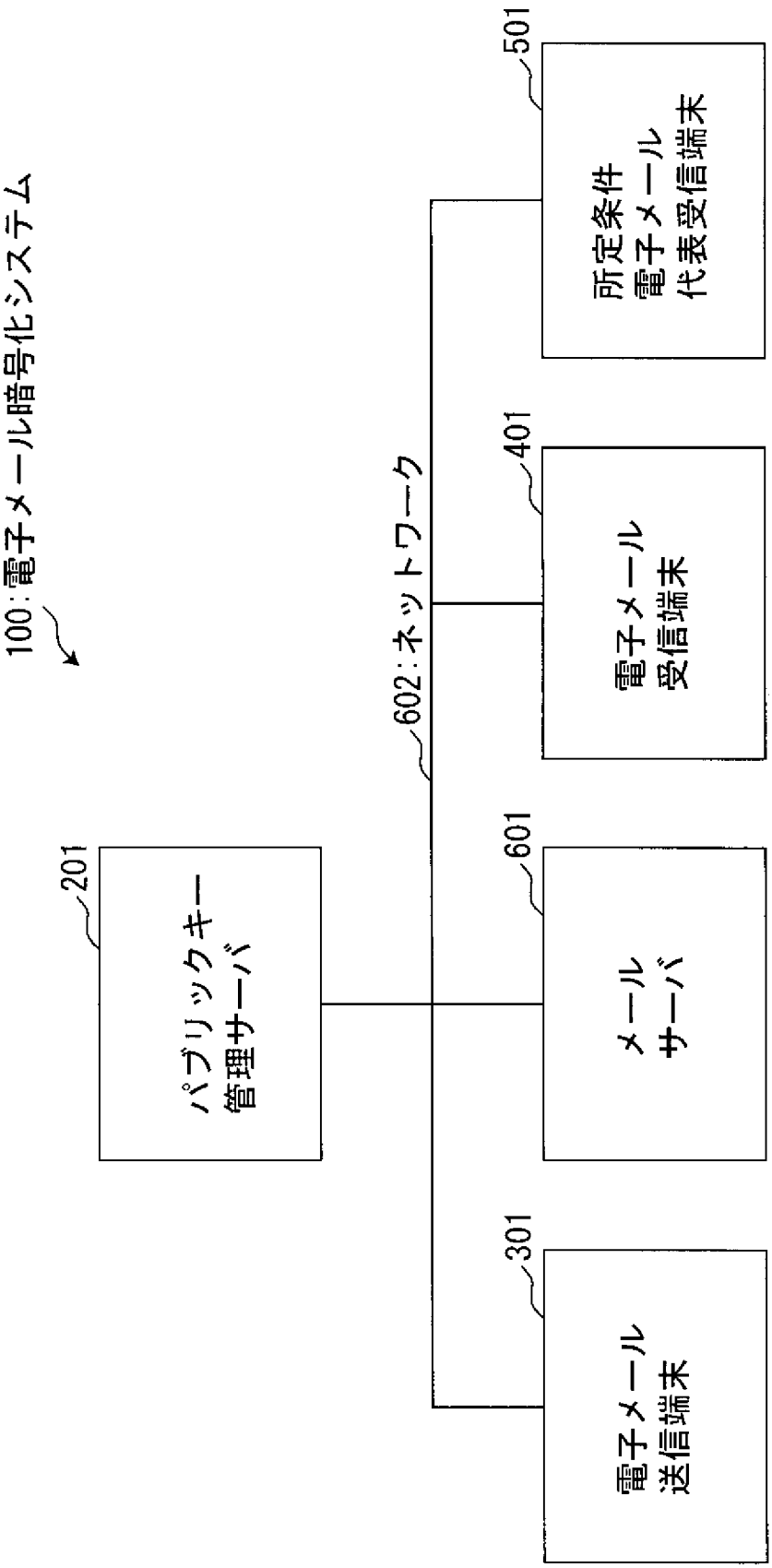
前記所定の条件は、前記受信者電子メールアドレスが所定のドメインに所属するものであることを特徴とする電子メール暗号化システム。

[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。

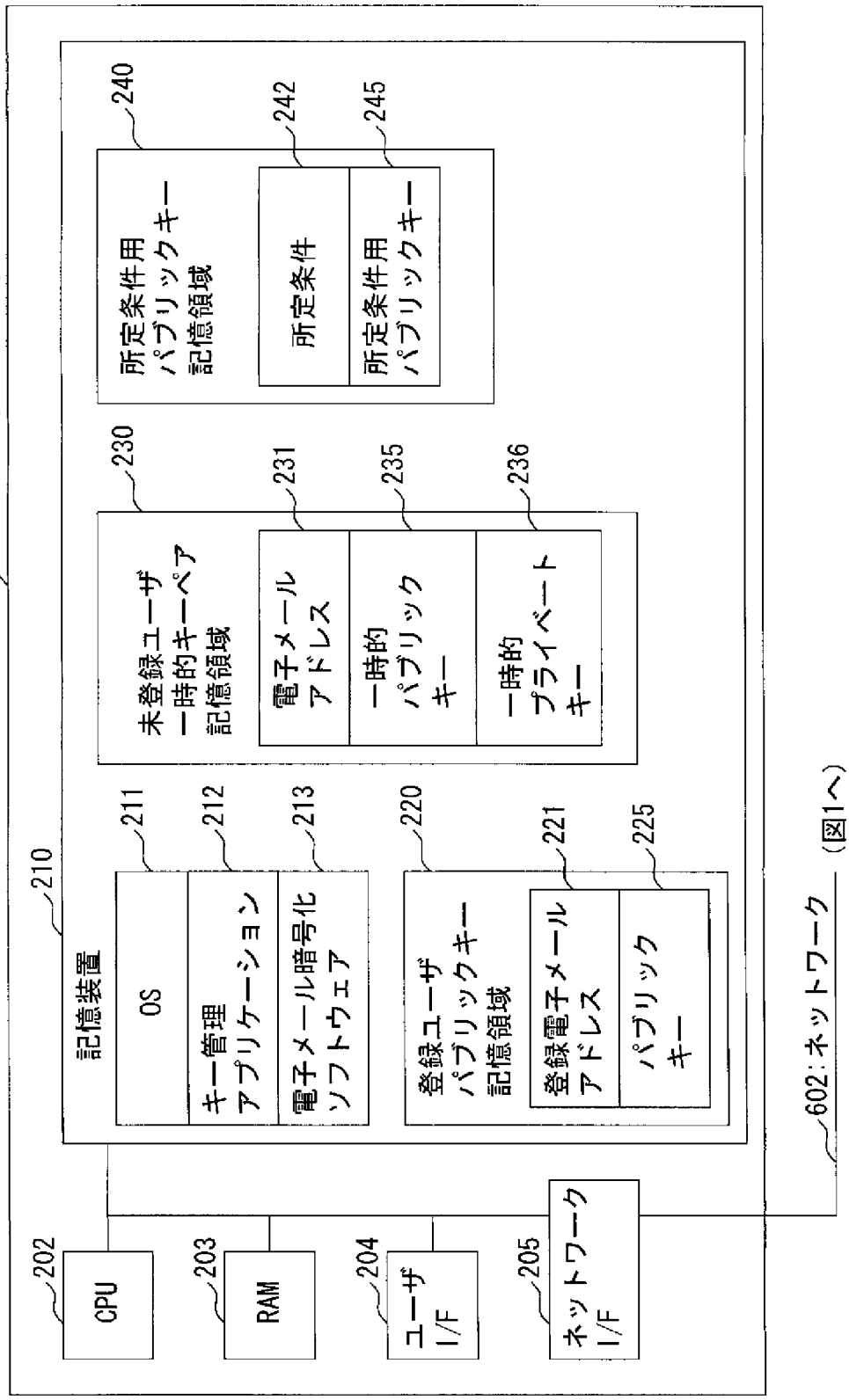
[図1]

FIG. 1


100:電子メール暗号化システム
602:ネットワーク
201
パブリックキー
管理サーバ
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

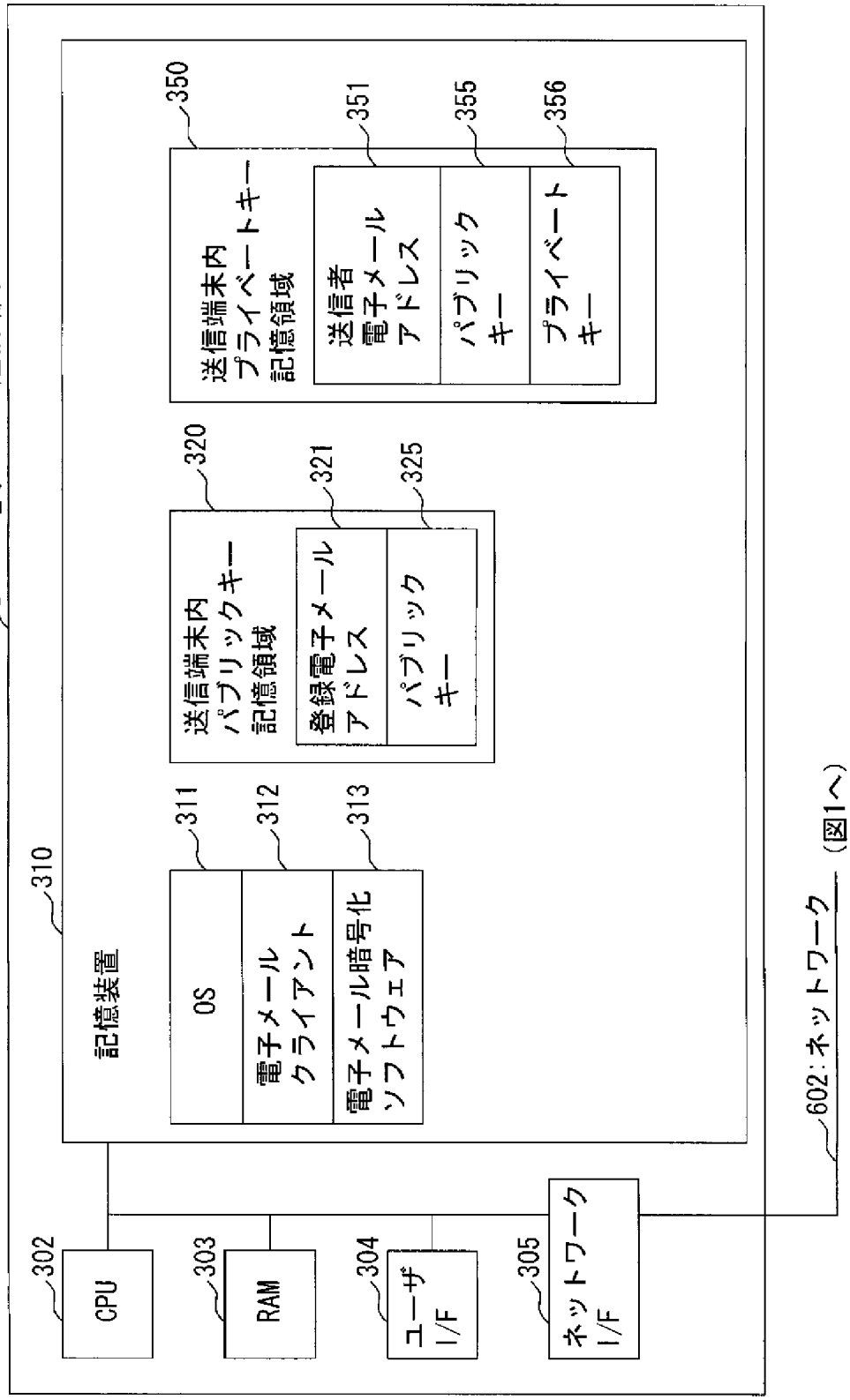
[図2]

FIG. 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)

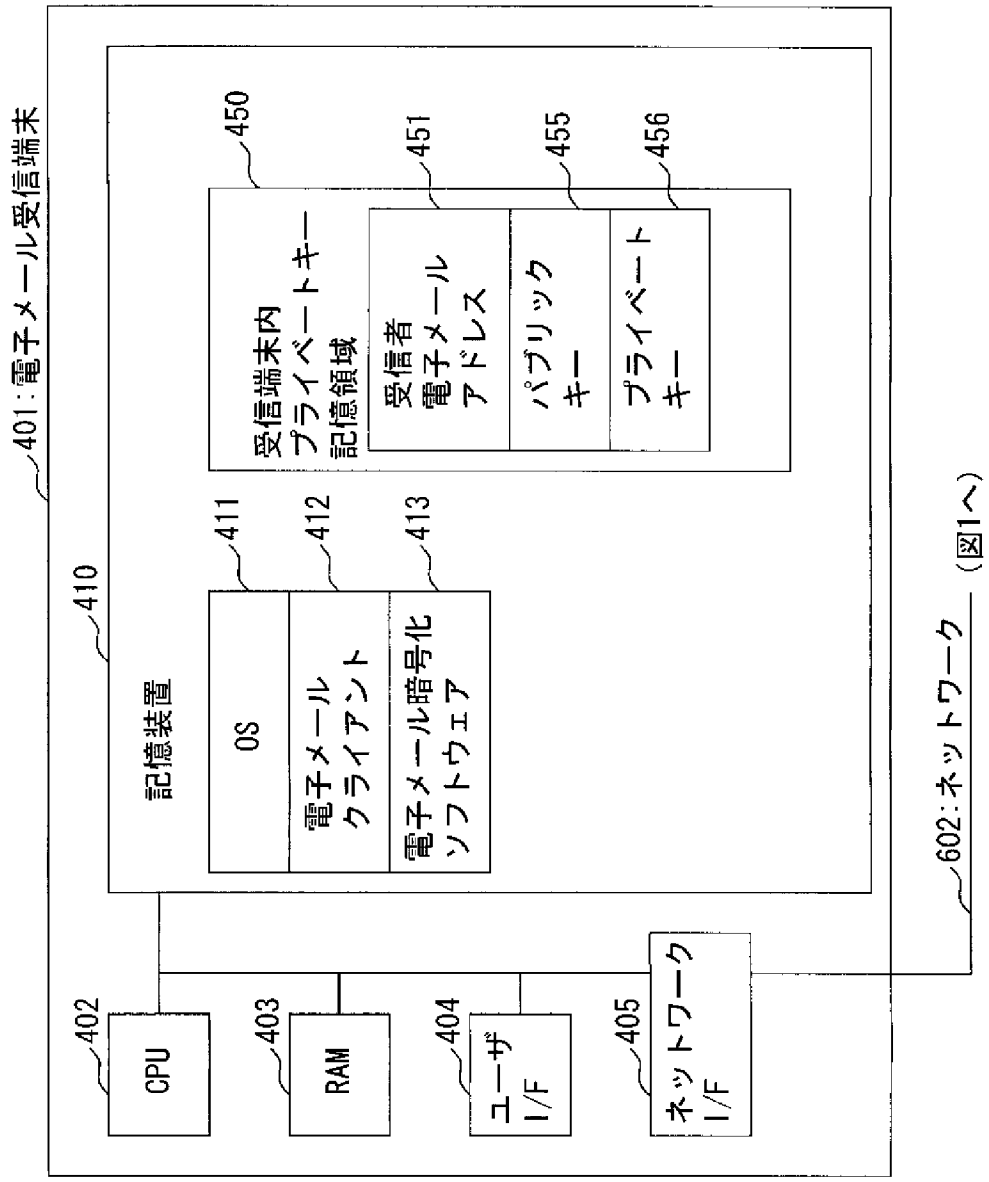
[図3]

FIG. 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)

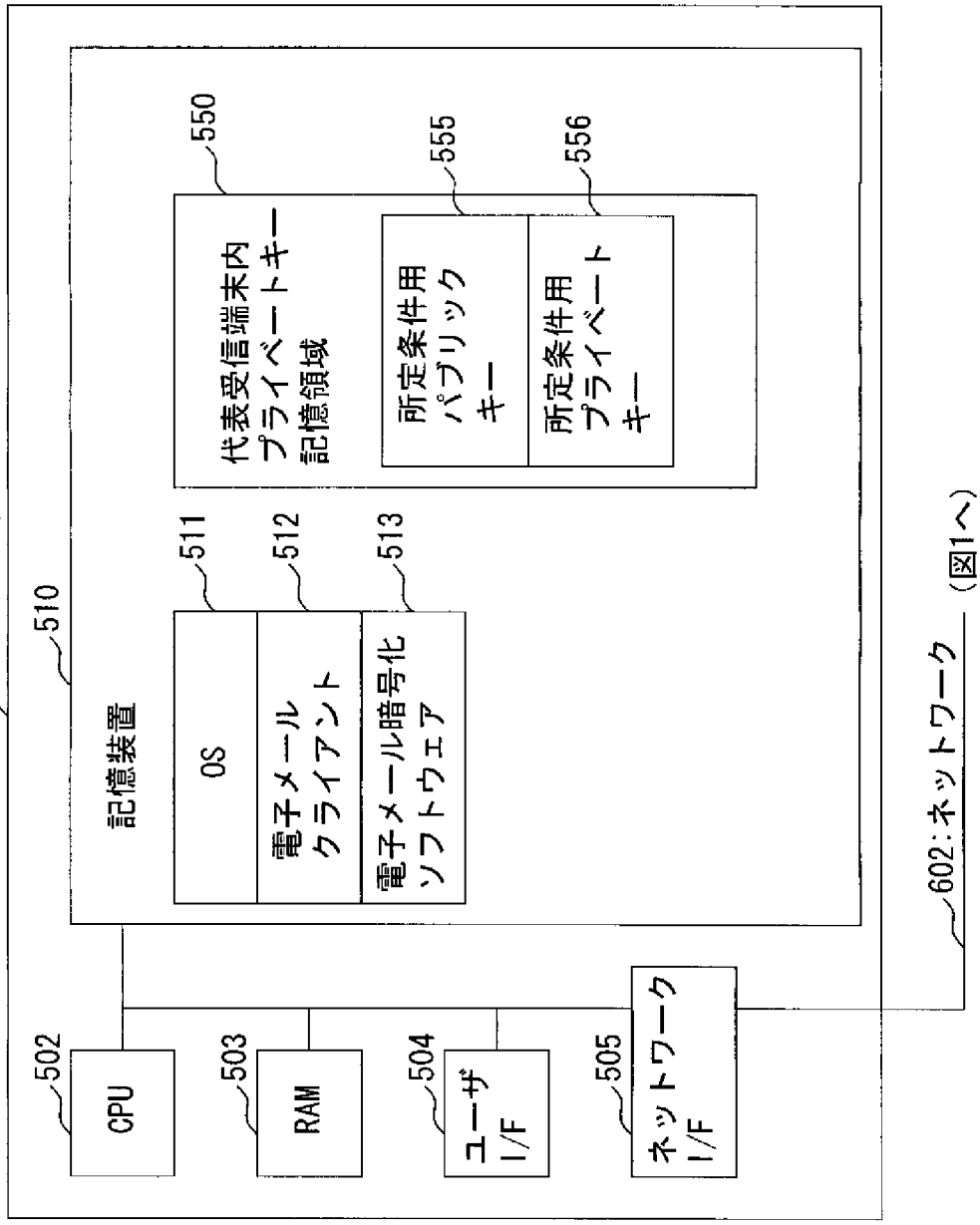
[図4]

FIG. 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]

FIG. 5


501:所定条件電子メール代表受信端末
510
記憶装置
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
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
502
CPU
503
RAM
504
ユーザ
I/F
505
ネットワーク
I/F
602:ネットワーク
(図1へ)

[図6]

FIG. 6

mQCNAzMRY/IAAAEEAOloTOU0f4w7FDRMM6kA/6XazXxJ/HH8dsmb6E7RuYfVlXsd
kCwxUBOkyW+AYhkHbYUwnB5qBoFUyLrbLGuwKHW1KnAwgbeZLTH5nqQLpA0RLGVZ
v3tzImKUdyyxBphZWC4IeEgUbl9cc+piOsEJ8QzF7gnqwWo/Ku6tTP1JpWPZAAUR
tBdNYXJrIENveCA8bWFya0Bhd2UuY29tPokAlQMFEDQvYTHurUz9SaVj2QEB/hMD
/ix6pAa+4ZgFQNRAc7fC+I4uGWvXoI8N8wtgiJi//8KclvjtvTylLPKVBDsylihs
bVOjD3NUEkH95TNI3QhVeCwJPl2e3GgFl253hj8Jai9snHj75pXjQXq0NxQ/JRSr
EAqrFM7+yRLPs7zDwsMoc2Ox5emq4joVa3syZUEwW7LxiQEVAwUQNLELtdZUWxzP
wQD1AQFWIQf/RtyM8Rw01RdQXH5fA2jLaQlwD/VG1dlxqAcLKVQIKR77iBPdfcrW
LyexGgQmltuVTGs5U1XPf7dff21NP79aglvD9hll82L5wZQybNpy2o6/66EPp4OW
Fl/WG7JhuCRfy53H983ERZnqGD4YeBafLHI9oGAixZ9G/+cFsxPde3Lv7Ij/1Hwp
eNAHJQibBkpdq29Kye/+PHgE0HTMSapYXN/YVTCpEFzE46YnD/BjzZ/E1UClvcsW
ZVoqPR46HARVQNu+MfoR/WSBAOj65Dt5oBZTcLoQ7TyDcd4gvLhdzLUo+kboGTjt
HLvesaAWKLSWtKY6G8Iy7R5+Ms0helLFaIkARgQQEQIABgUCOG/pBQAKCRAXWVXO
Q77mqABMAKCgO+LVARom7t/XmRw4w4TO9IkM9gCgh2URPU7tqECsr+WuVfC/v/7e
vVWJAD8DBRA02GubUX4eqU/cq8ERAgUbAKCO913wXBCqiBfQBT5F6koRZRRvbQCf
fJ+Y14jFEx+cfCdDIUjjD014/diJAEYEEBECAAYFAjvQk5wACgkQVZbdDOm/ZT0n
TQCfdqn38SRRYeIG3+LIPq8dODr39JwAmgOH2/N2hjA2Z/4QMOjrQ4gIgpAPiQBG
BBARAgAGBQI7zAqEAAoJEKFQ/C2FqPeL7C8AnRr7d0vN+E1W218XjItFonLw42qT
AJ4xUrPsSduizUQnOuzdR8x2x4yEyIkARgQQEQIABgUCOjcVtAAKCRDe3YS5RDds
3Dz/AJ9UaB2vKuteTC+gm80f028DPbmCegCg3ZM1Rt2WMDS/wHW7nQJ/xnyg8PuJ
AD8DBRA6ynJX/W+IxiHQpxsRAjd/AKCSXqSmTnrzlnpgYwMESQiKQxfOywCeNuUy
0q65a+C/ayC7t6F6ih9+bcW0GU1hcmsgQ294IDxtamNAYXBhY2hlLm9yZz6JAJUD
BRA54aHP7q1M/UmlY9kBASf1BACwKxBv5osTZpJIiKsdim/P2LHOtU91Ne8kxTdr
78Q86cHSz8V0ExA/FWKkOPgEHAIncXItNH0t3pGtUbAcYuT830Y7OJgLZdEWszQc
bsp72nlK0ceZ6SFRE/ouDlcnyaiou2814JGlttqi08yO6LcX3sQD8wDaQhoUoCe9
wg/eaokAlQMFEDrLUyUbCAxFJxmvNQEB3XgD/2M9X5cgqjItm4vH9CjkAEOvfYh0
KjDTy9/WA0mVDcXvV9RZGMMnWmSKg1yDZp4A8lWEQkk6VxZEMwW1PTtsFlOAyEQT
2QiRQtS6tFTj8X9aZ6a0PeYF5PyS20hvJzYXpbogkemBFtUDmsfXToSoO6Uz1E3q
eTYYIMB01pImXvdpiQBGBBARAgAGBQI70JOfAAoJEFWW3Qzpv2U9XQYAmwfOqWaT
wJFN0bz/9PL1xJRO0J+ZAKCHUML3L2N1yqR0CXTO2C40fDjsMokAPwMFEDrKcnL9
b4jGIdCnGxECMsMAoPGRixfMANAdwK0OwFjayMH0GV0PAJ4kP7UxlR3DkU/5wTOZ
dGL/zRRHJrQZTWFyayBDb3ggPG1qY0ByZWRoYXQuY29tPokAlQMFEDnhofnurUz9
SaVj2QEBJxcD/017e1bFJGNcISL2dIvINhnXnzHxL6B66exG+8+1pFkR8e/EvgEv
XHMs2+AqDfUxkb1PNSoq/u/m/VpJGEWoObuSkiwiqUYrmXcJGE1UQyHMLDKSLQQh
G4PkeSp0T2yX+Fk+5F3vIOdK53jsD21zXqB5QD7TjCLSGkU+BiLuLGX6iQBGBBAR
AgAGBQI70JOfAAoJEFWW3Qzpv2U9p6kAn3lo65wMqy/XbG+RgeJlrQQk0v5tAJ9e
zLVU5oVtfnH6JvAZFvi8sudRhokARgQQEQIABgUCO8wKigAKCRChUPwthaj3i4gq
AKC67ZkCrpAZWQKPJdwTw6zn6GsyVwCfQyoy5lGIuGBu0je6You3NEakk36JAD8D
BRA6ynJ4/W+IxiHQpxsRAsw3AKCqcCFo5uzU7XEom82HnvX7kSPDtACeIqOnzHMb
ArpmDAcknLxcmsjp2J4=

パブリックキーの例

[図7]

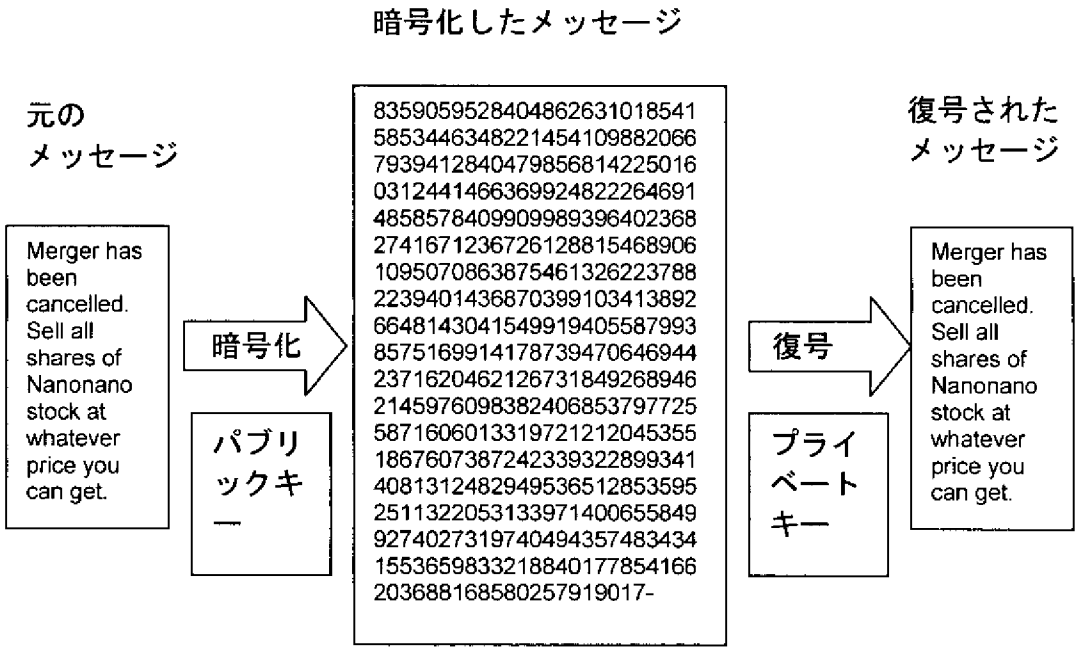
FIG. 7

プライベートキーの例

[図8]

FIG. 8

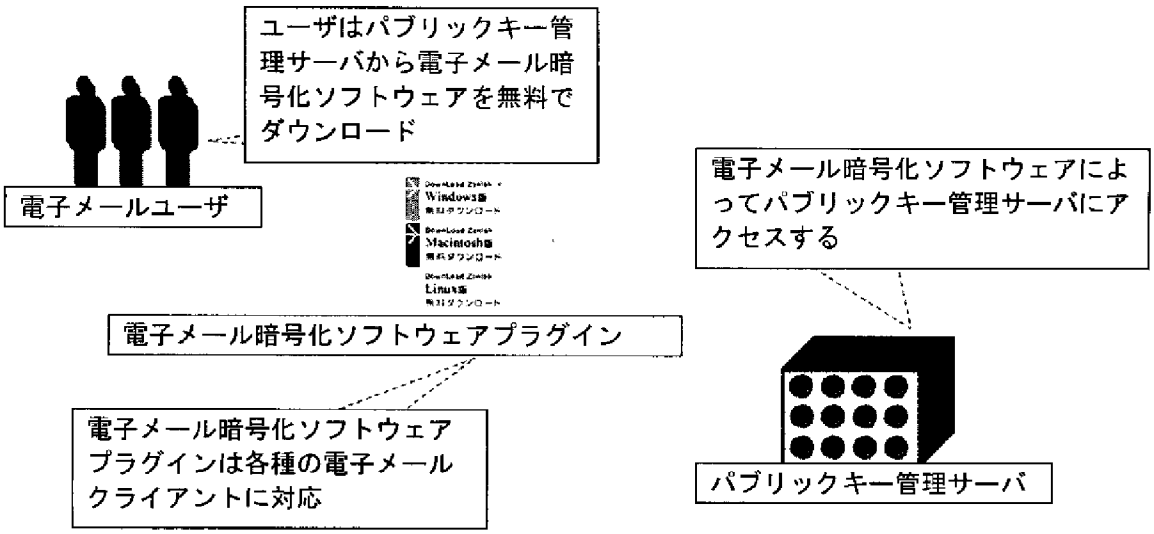
PRIOR ART



公開鍵方式の暗号化及び復号の例

[図9]

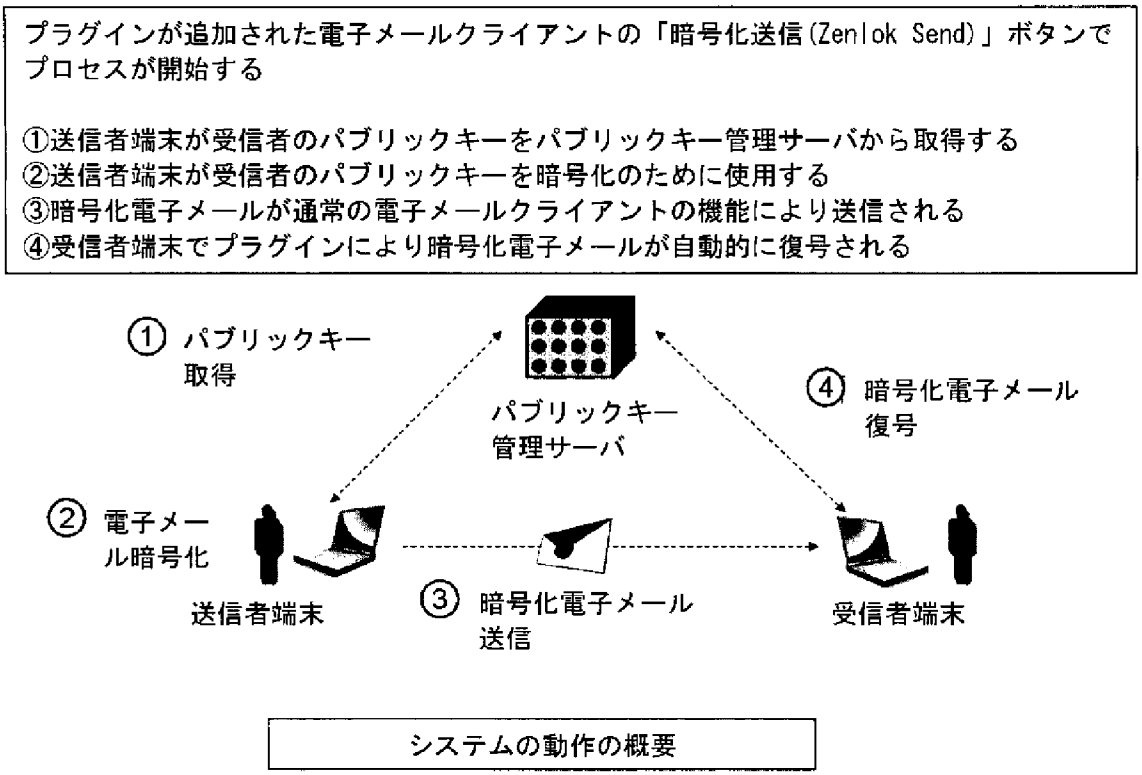
FIG. 9



システムの構成の概要

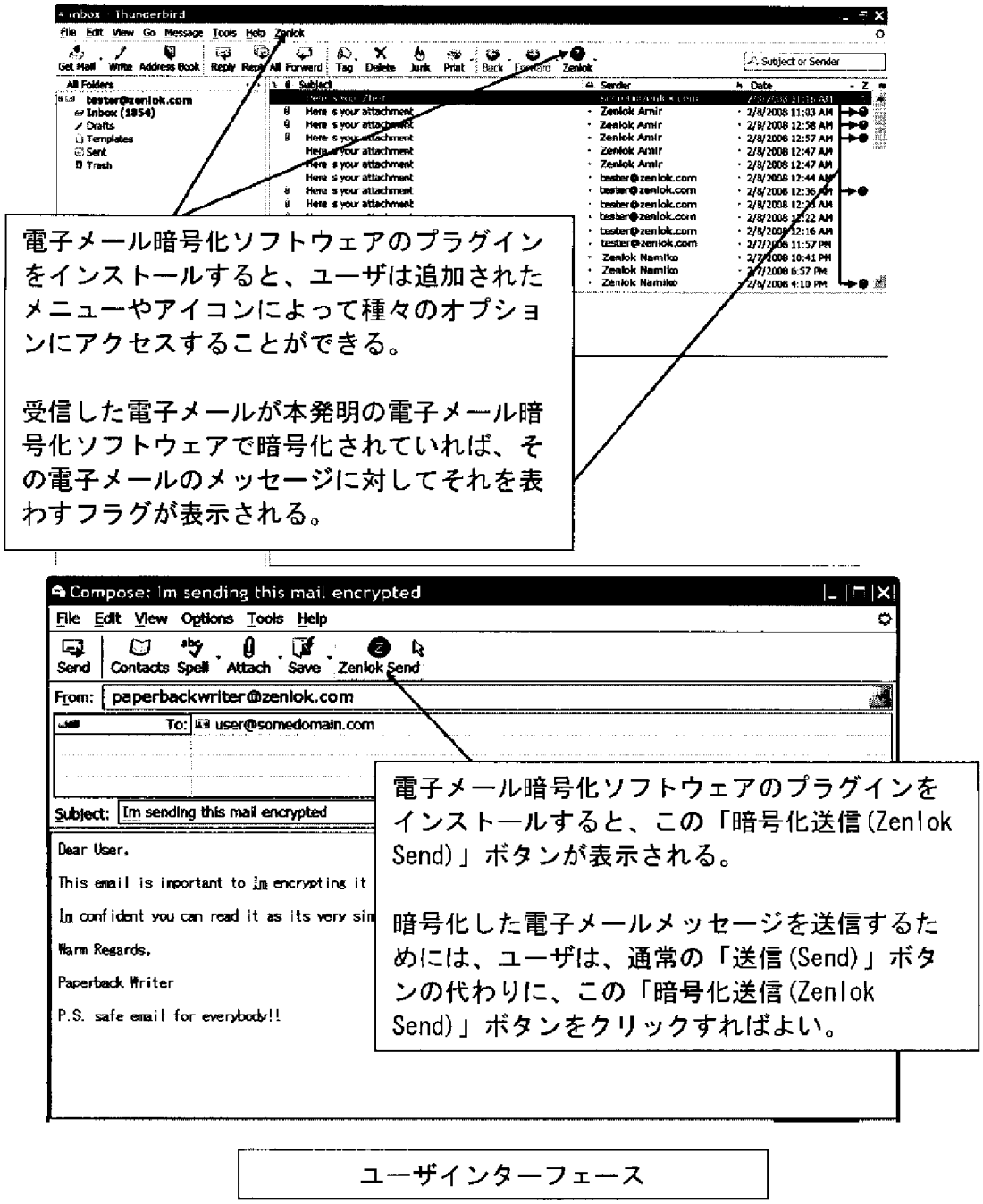
[図10]

FIG. 10


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(Zenlok Send)」ボタンでプロセスが開始する
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
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
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
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
① パブリックキー取得
パブリックキー管理サーバ
④ 暗号化電子メール復号
② 電子メール暗号化
送信者端末
③ 暗号化電子メール送信
受信者端末
システムの動作の概要

[図11]

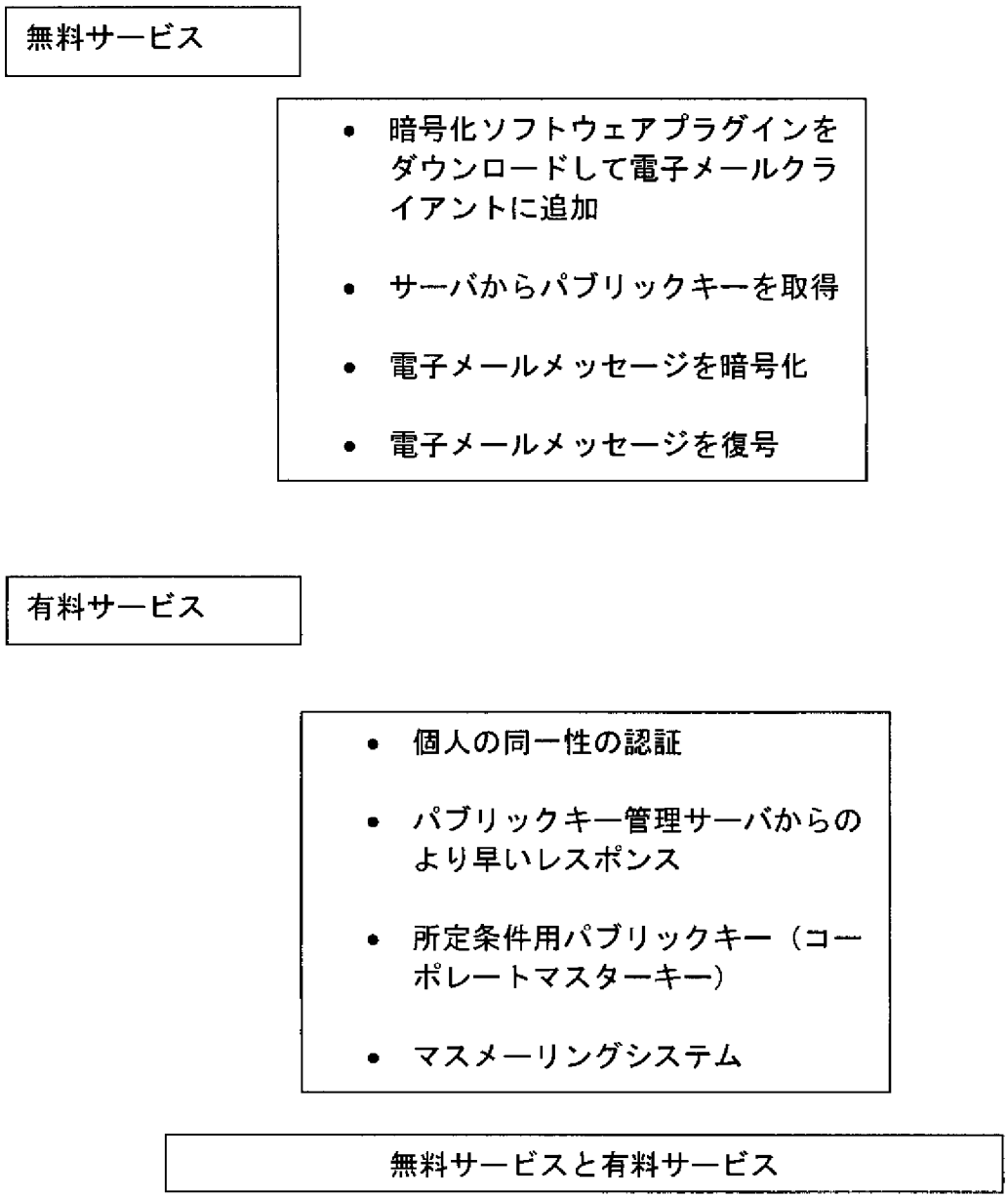
FIG. 11



ユーザインターフェース

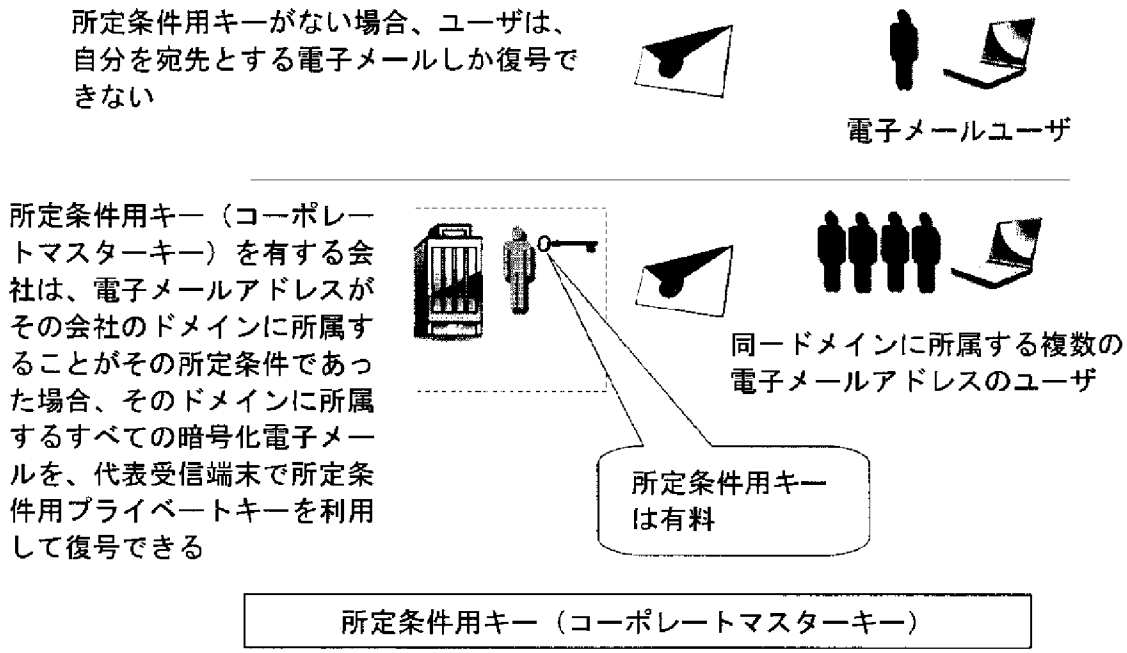
[図12]

FIG. 12


無料サービス
暗号化ソフトウェアプラグインをダウンロードして電子メールクライアントに追加
サーバからパブリックキーを取得
電子メールメッセージを暗号化
電子メールメッセージを復号
有料サービス
個人の同一性の認証
パブリックキー管理サーバからのより早いレスポンス
所定条件用パブリックキー（コーポレートマスターキー）
マスメーリングシステム
無料サービスと有料サービス

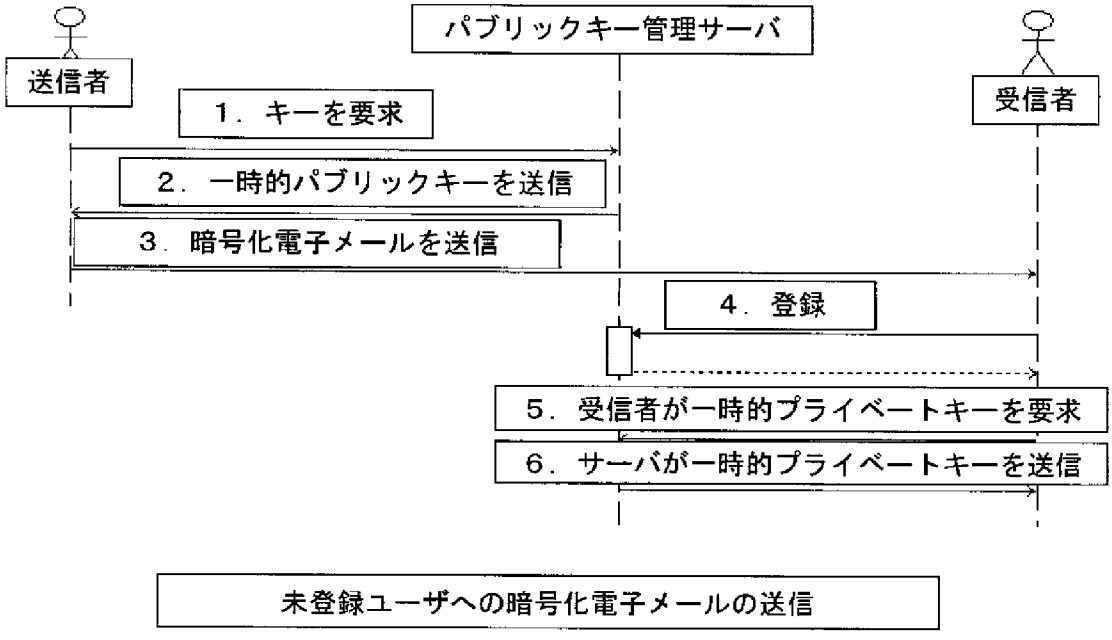
[図13]

FIG. 13



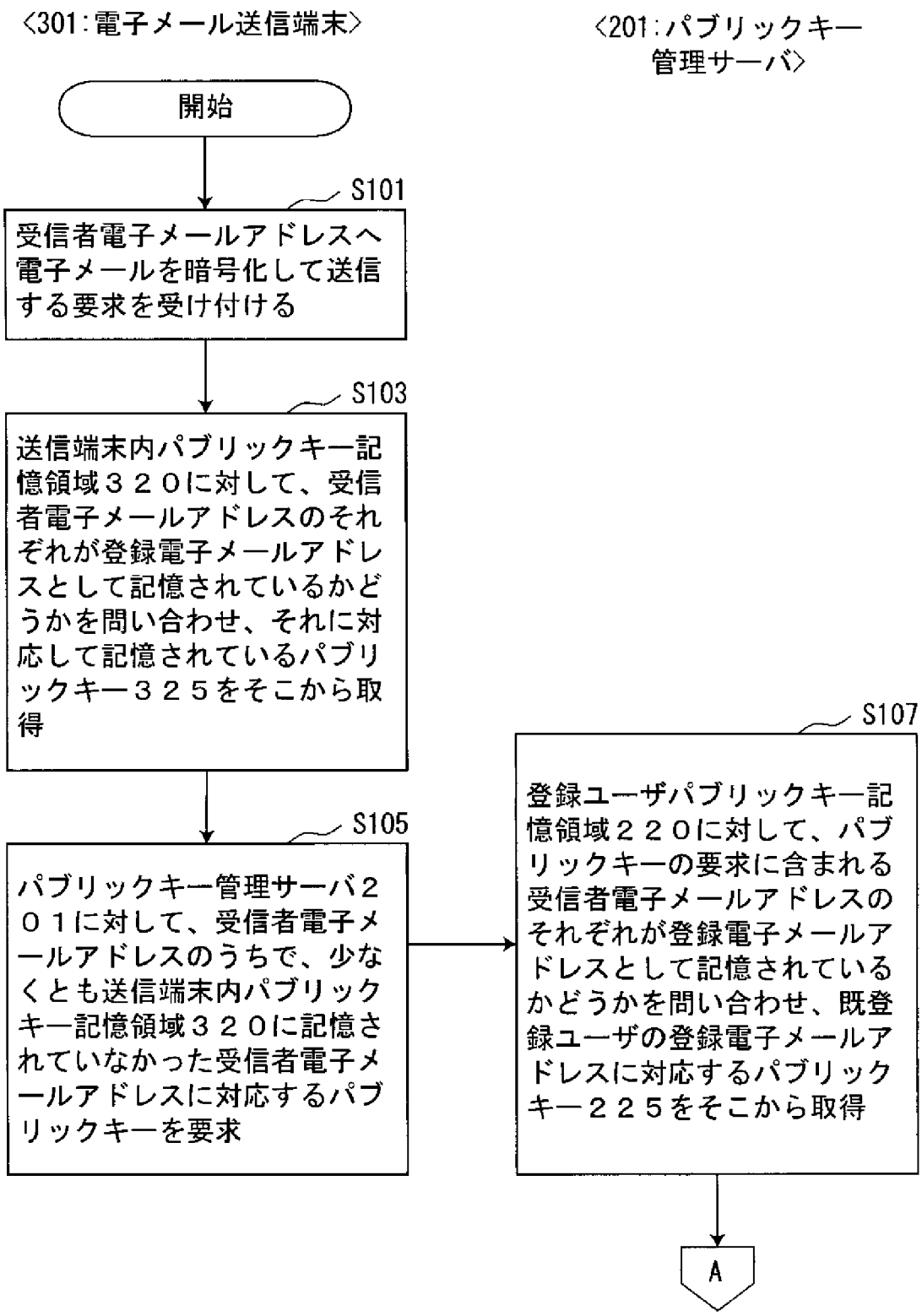
[図14]

FIG. 14



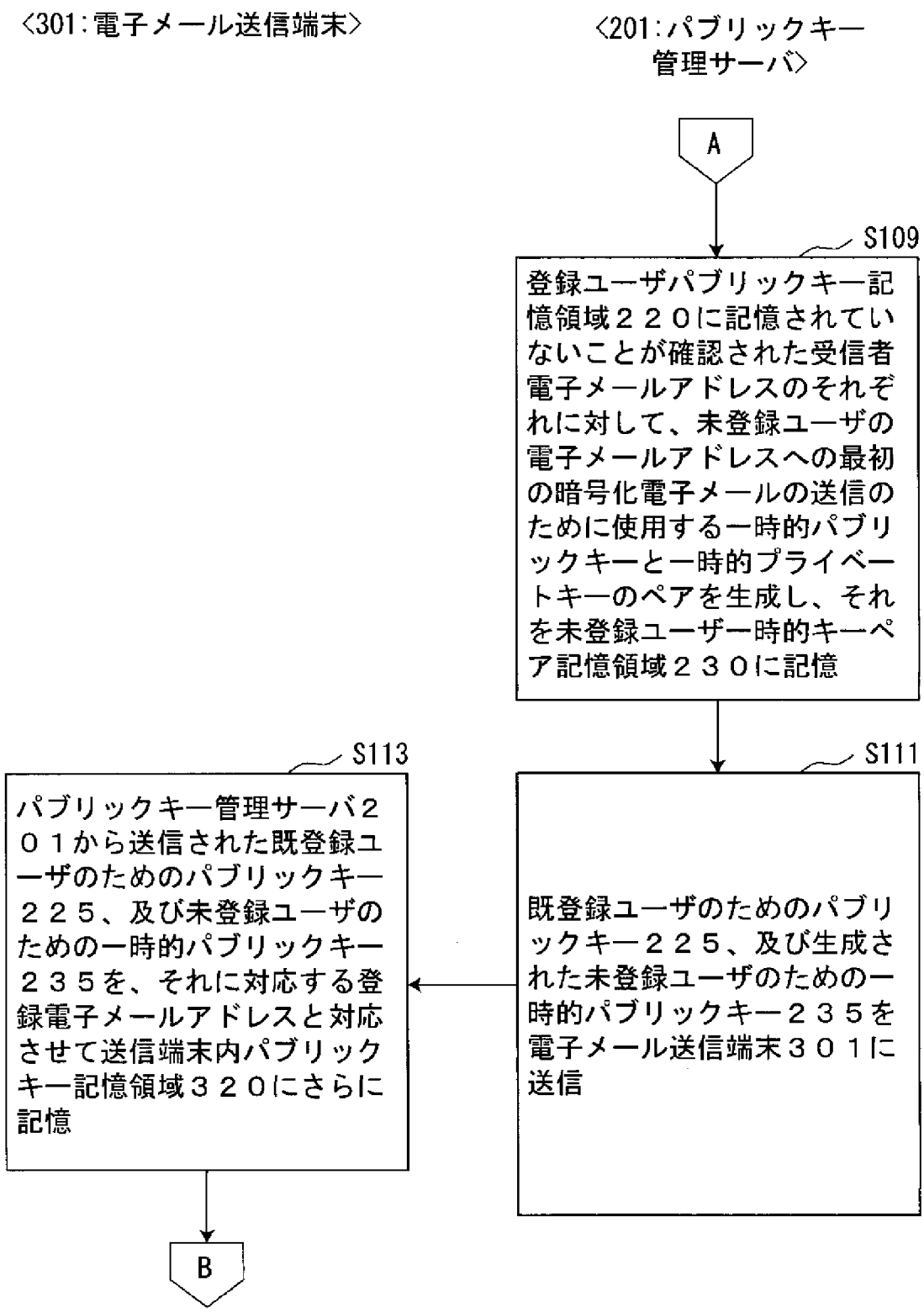
[図15]

FIG. 15


〈301：電子メール送信端末〉
〈201：パブリックキー管理サーバ〉
開始
S101
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
S103
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
S105
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
S107
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
A

[図16]

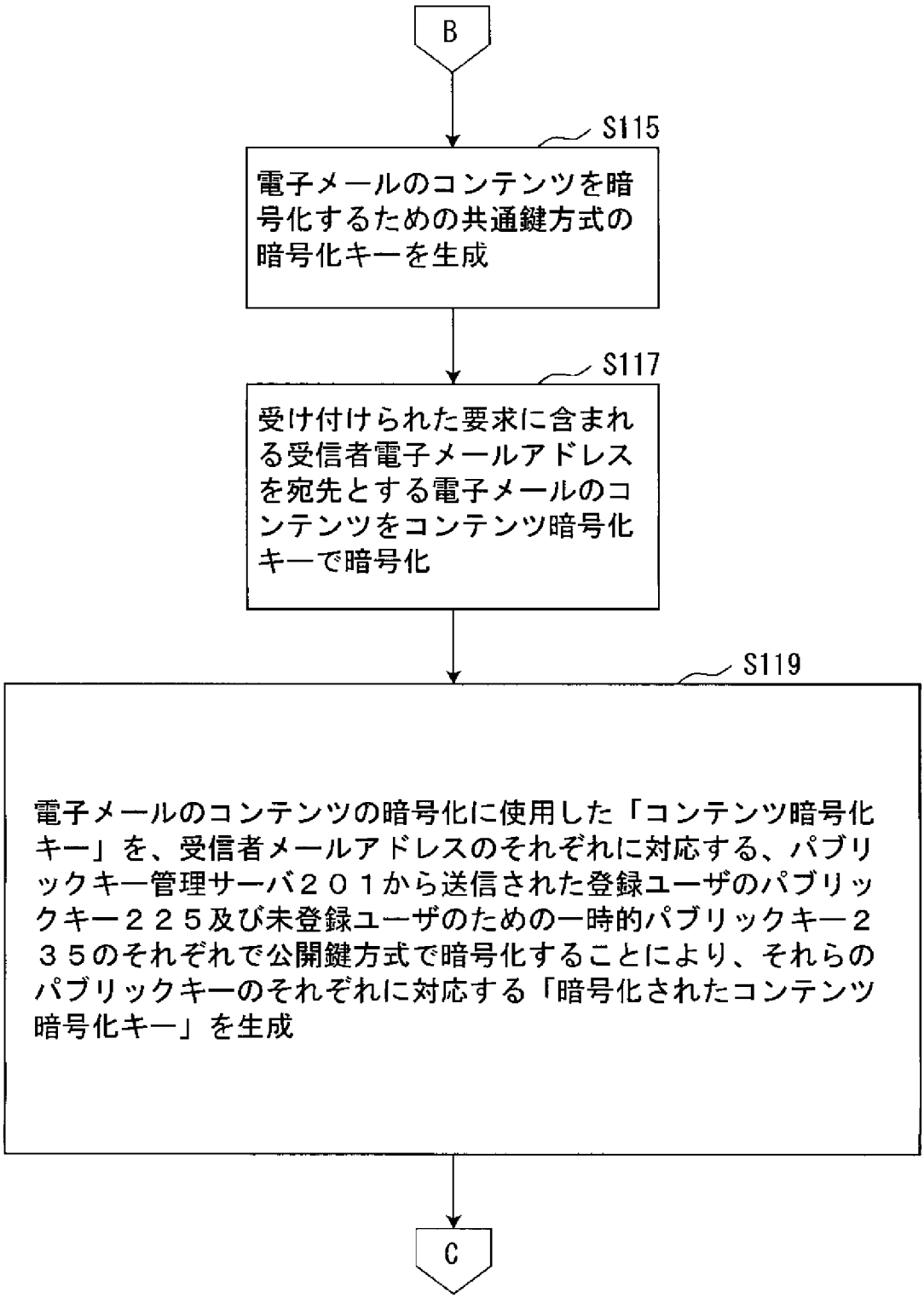
FIG. 16


<301:電子メール送信端末>
<201:パブリックキー管理サーバ>
A
S109
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ー時的キーペア記憶領域２３０に記憶
S111
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
S113
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、及び未登録ユーザのための一時的パブリックキー２３５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
B

[図17]

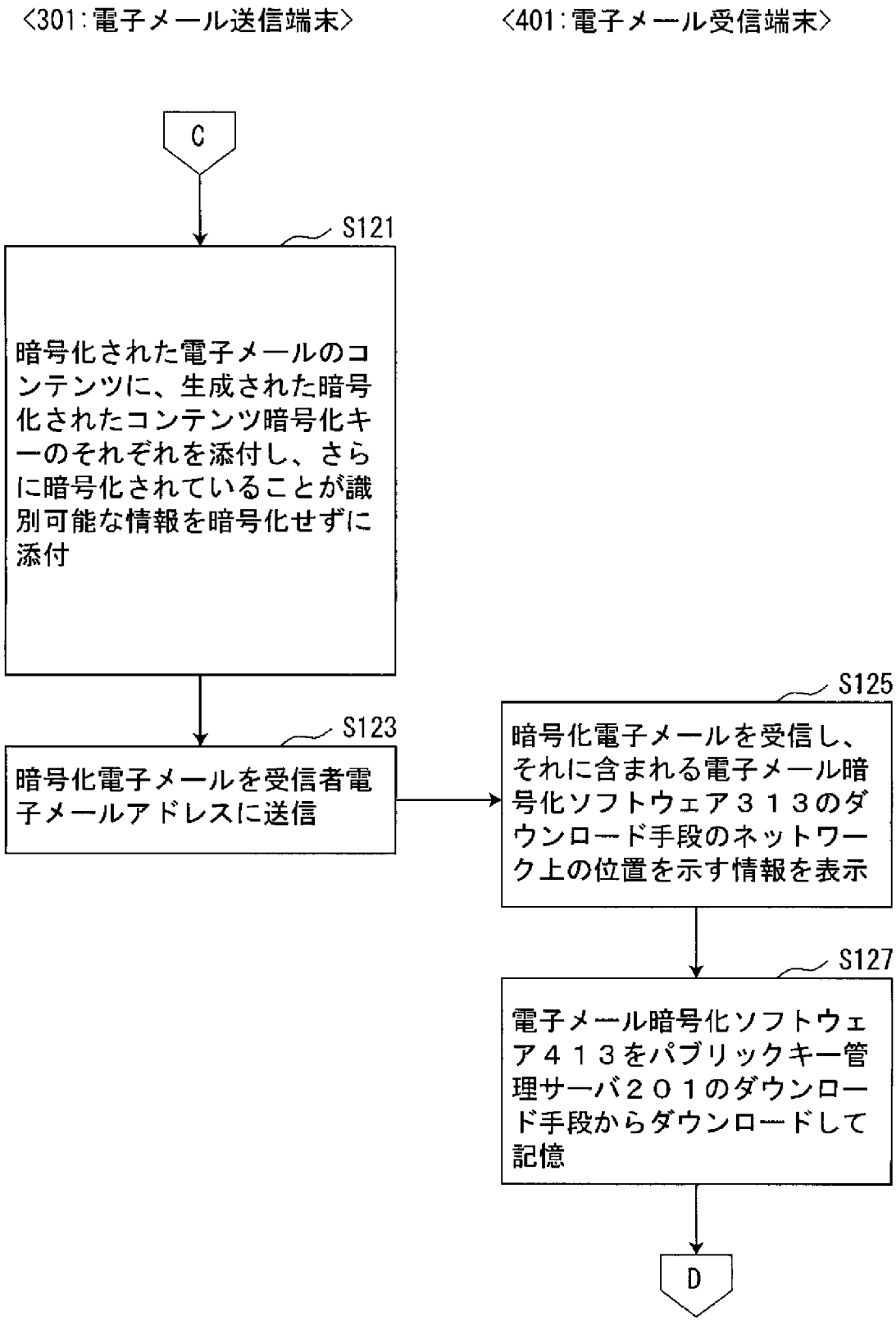
FIG. 17

<301:電子メール送信端末>



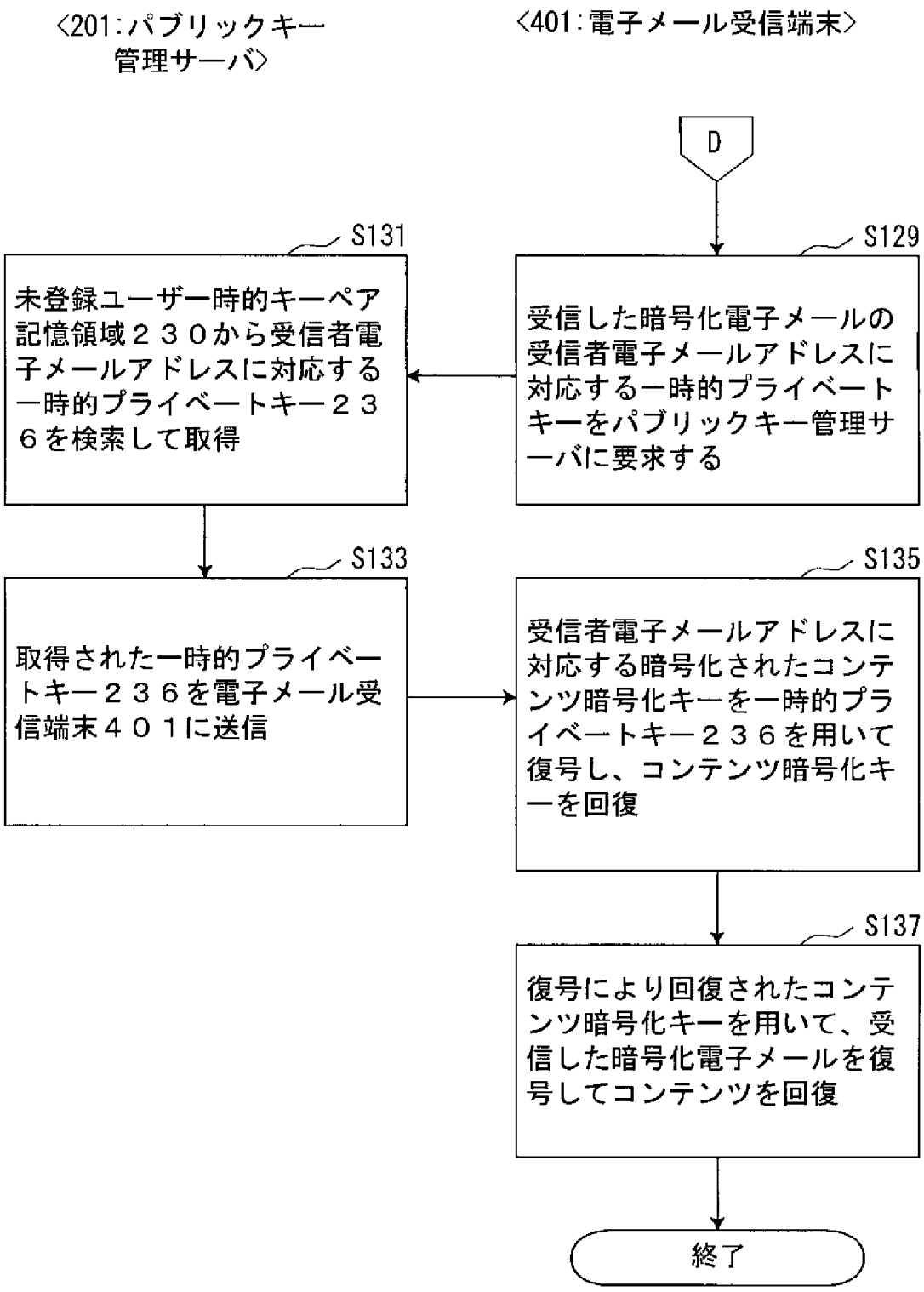
[図18]

FIG. 18


〈301：電子メール送信端末〉
〈401：電子メール受信端末〉
C
S121
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
S123
暗号化電子メールを受信者電子メールアドレスに送信
S125
暗号化電子メールを受信し、それに含まれる電子メール暗号化ソフトウェア３１３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表示
S127
電子メール暗号化ソフトウェア４１３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記憶
D

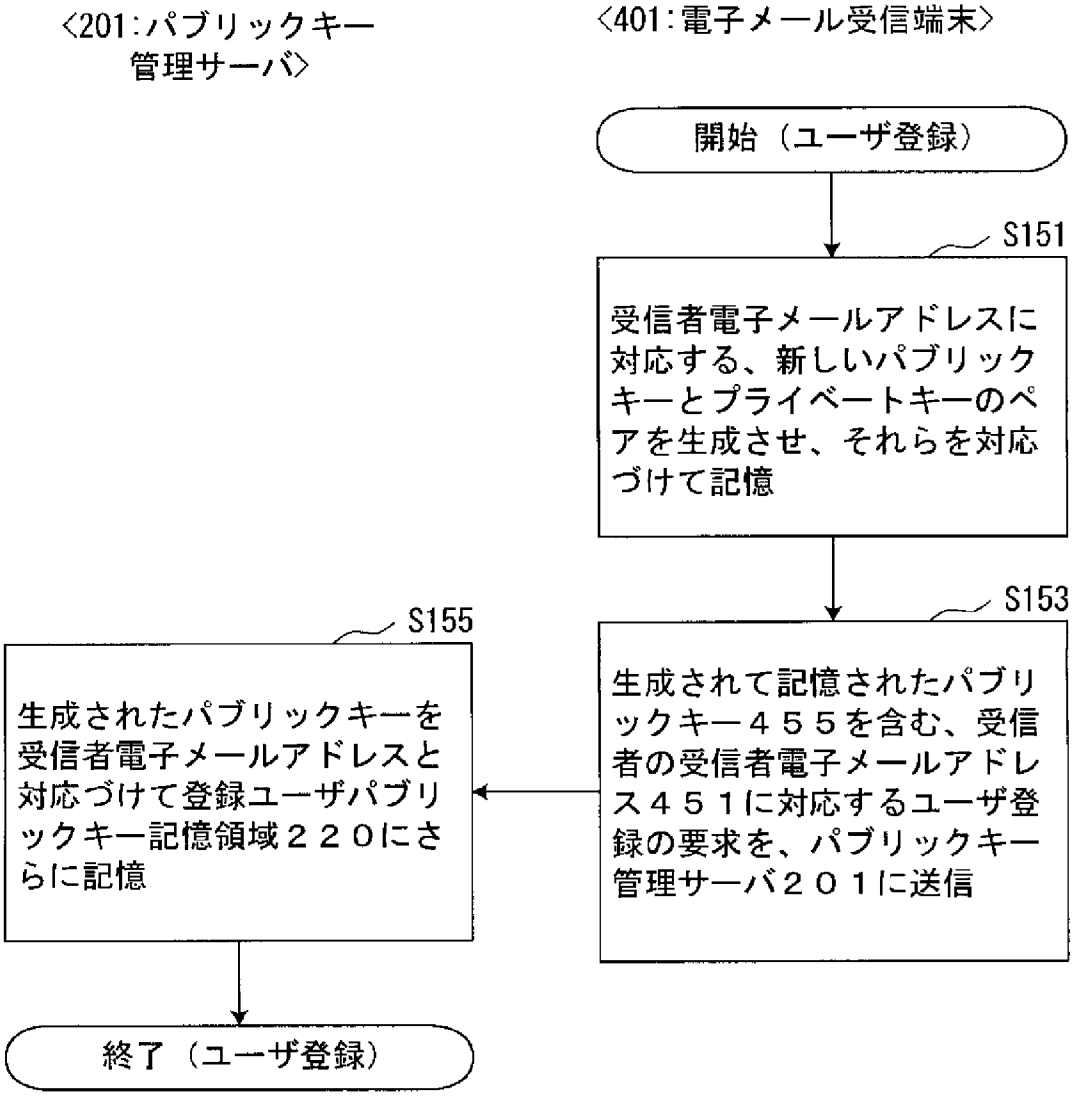
[図19]

FIG. 19


〈201：パブリックキー管理サーバ〉
〈401：電子メール受信端末〉
D
S129
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
S131
未登録ユーザー時的キーペア記憶領域２３０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２３６を検索して取得
S133
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
S135
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
S137
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
終了

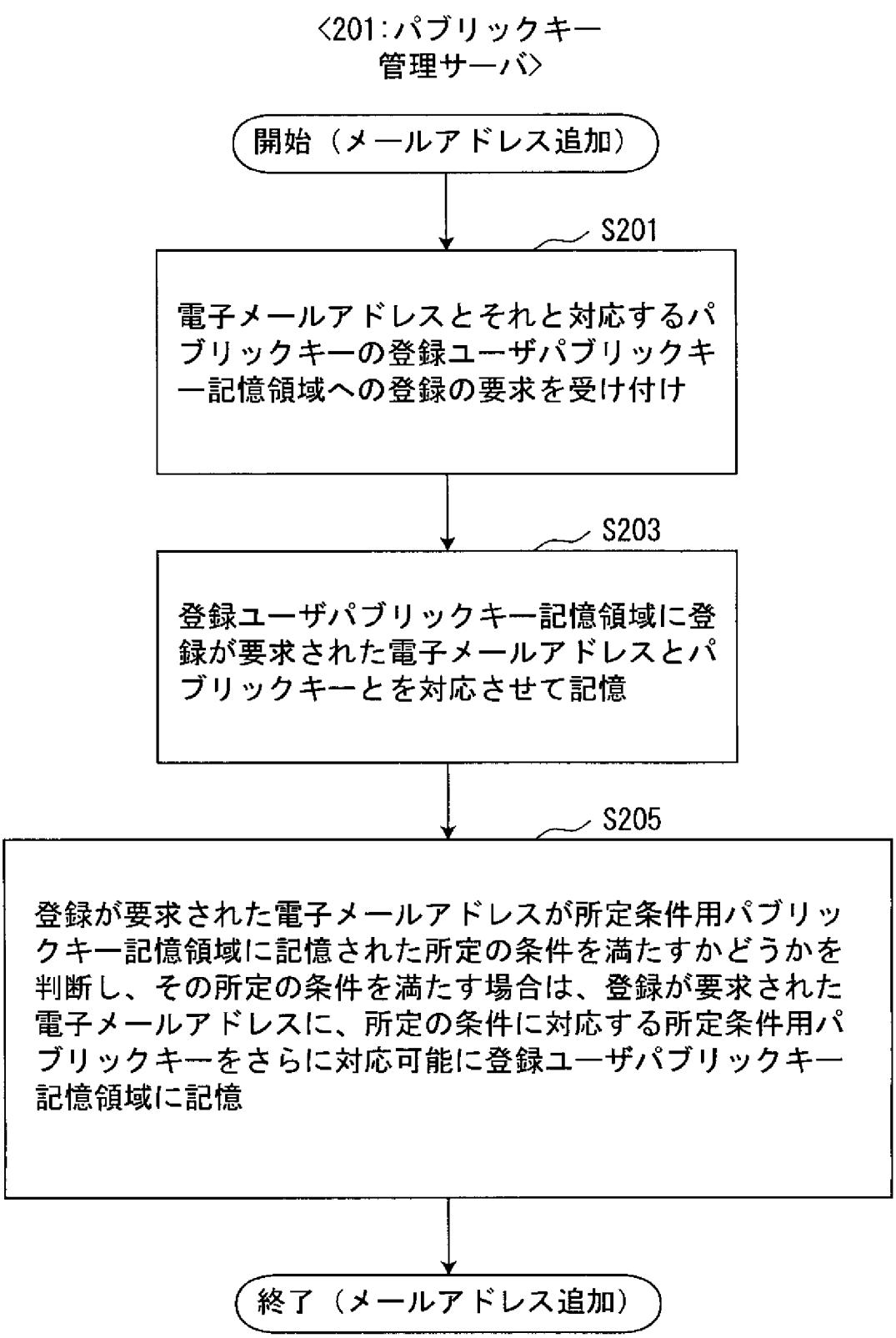
[図20]

FIG. 20


〈201：パブリックキー管理サーバ〉
〈401：電子メール受信端末〉
開始（ユーザ登録）
S151
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
S153
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
S155
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
終了（ユーザ登録）

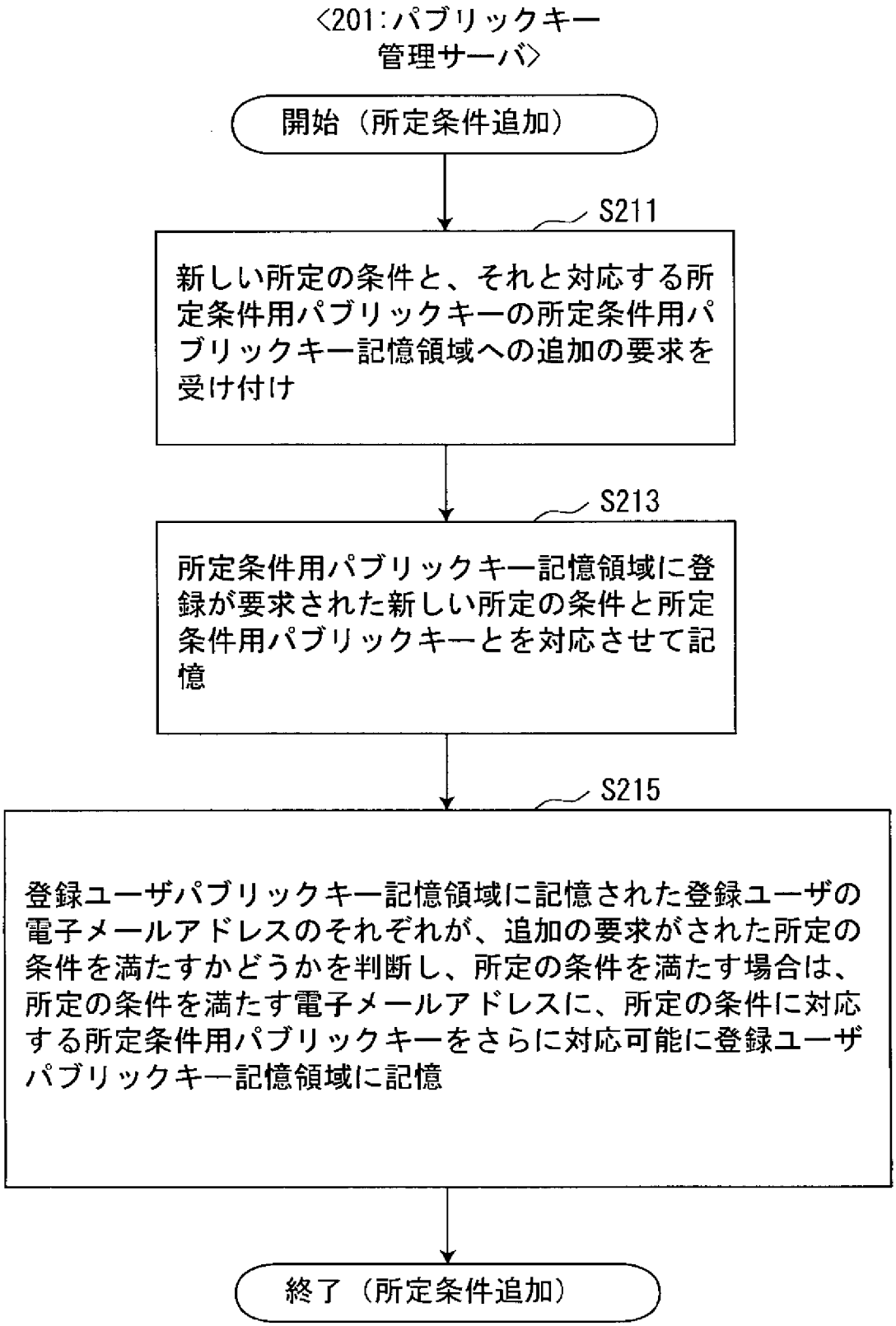
[図21]

FIG. 21


<201:パブリックキー
管理サーバ>
開始（メールアドレス追加）
S201
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
S203
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
S205
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、その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可能に登録ユーザパブリックキー記憶領域に記憶
終了（メールアドレス追加）

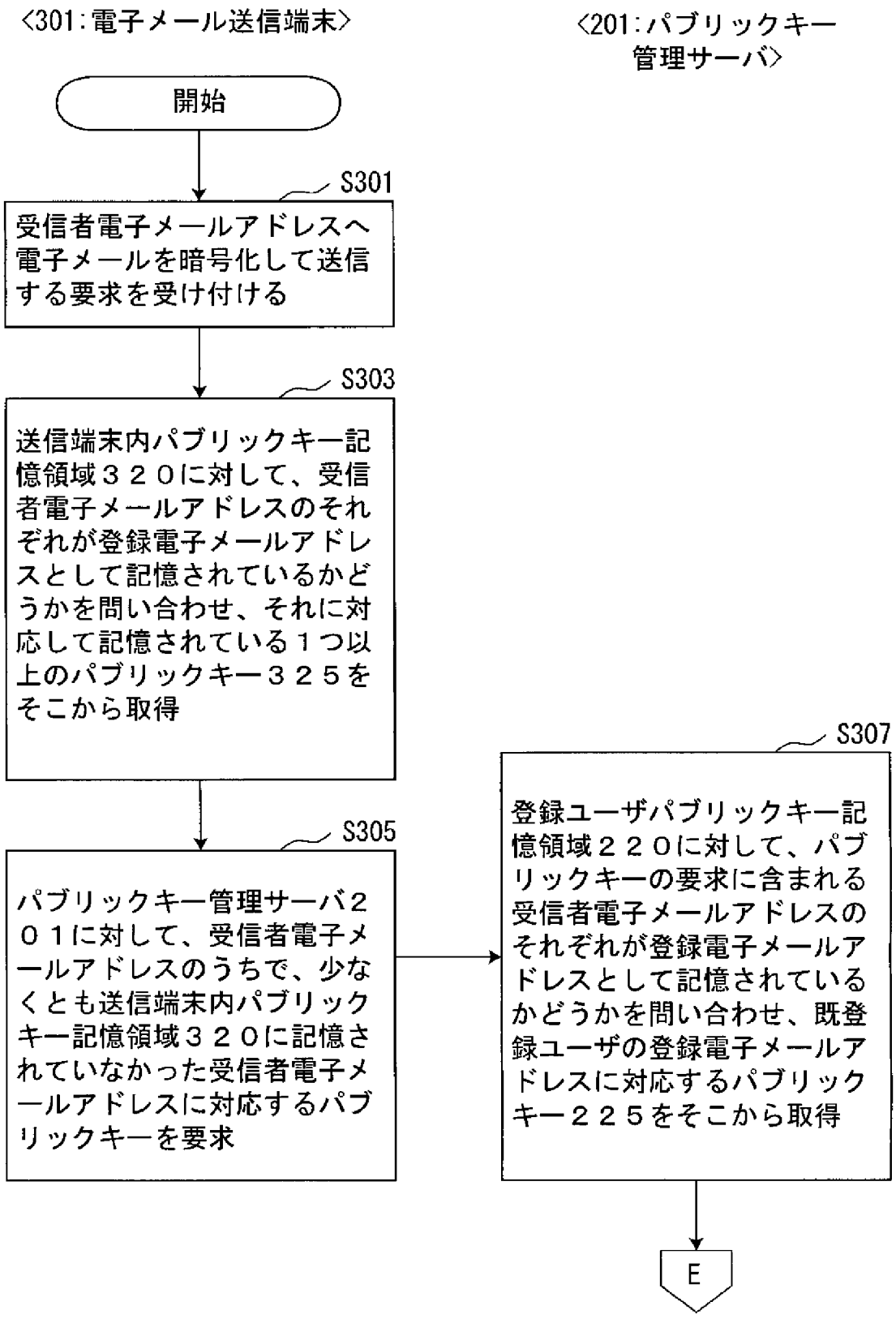
[図22]

FIG. 22


<201:パブリックキー
管理サーバ>
開始（所定条件追加）
S211
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
S213
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
S215
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可能に登録ユーザパブリックキー記憶領域に記憶
終了（所定条件追加）

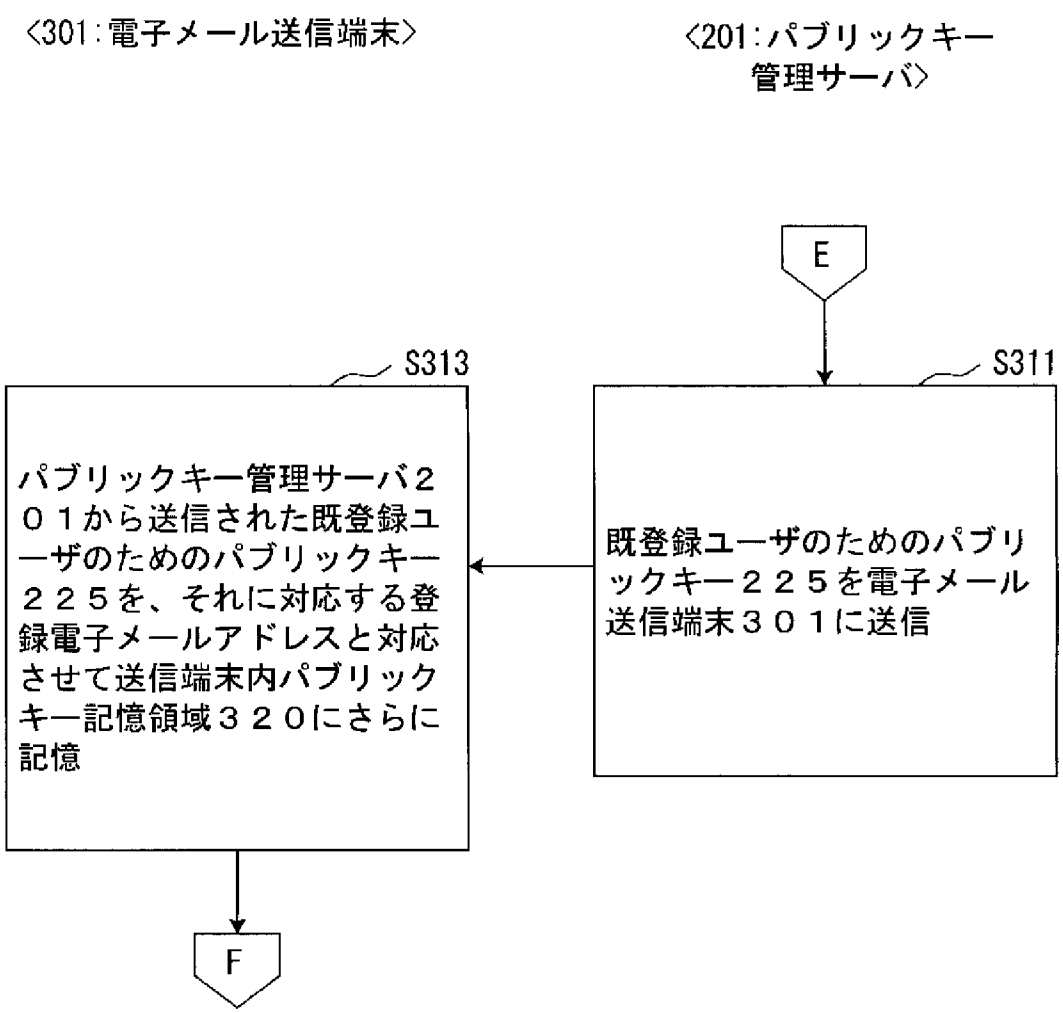
[図23]

FIG. 23


〈301:電子メール送信端末〉
〈201:パブリックキー管理サーバ〉
開始
S301
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
S303
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３２５をそこから取得
S305
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
S307
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
E

[図24]

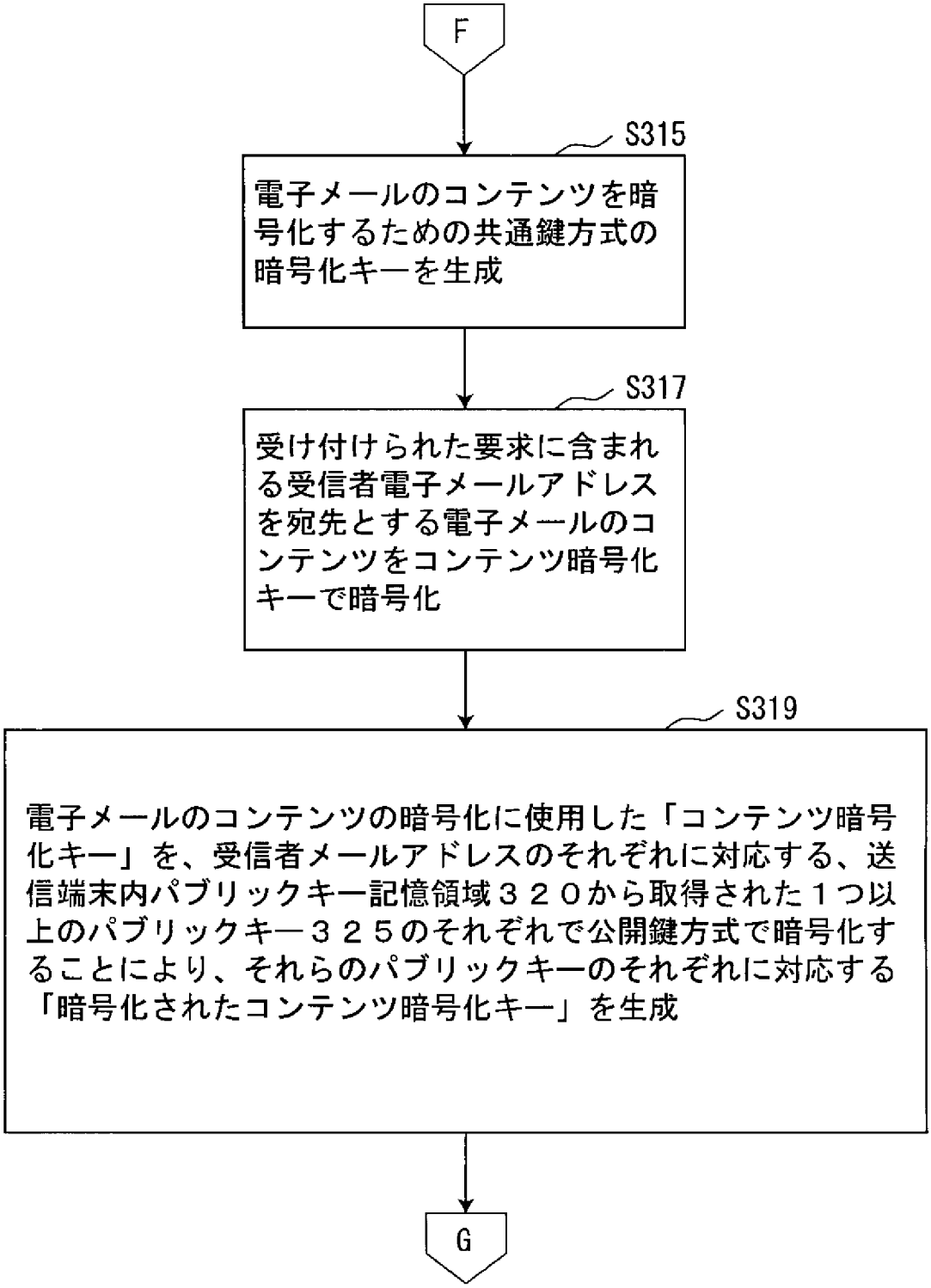
FIG. 24


〈301：電子メール送信端末〉
〈201：パブリックキー管理サーバ〉
E
S311
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
S313
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
F

[図25]

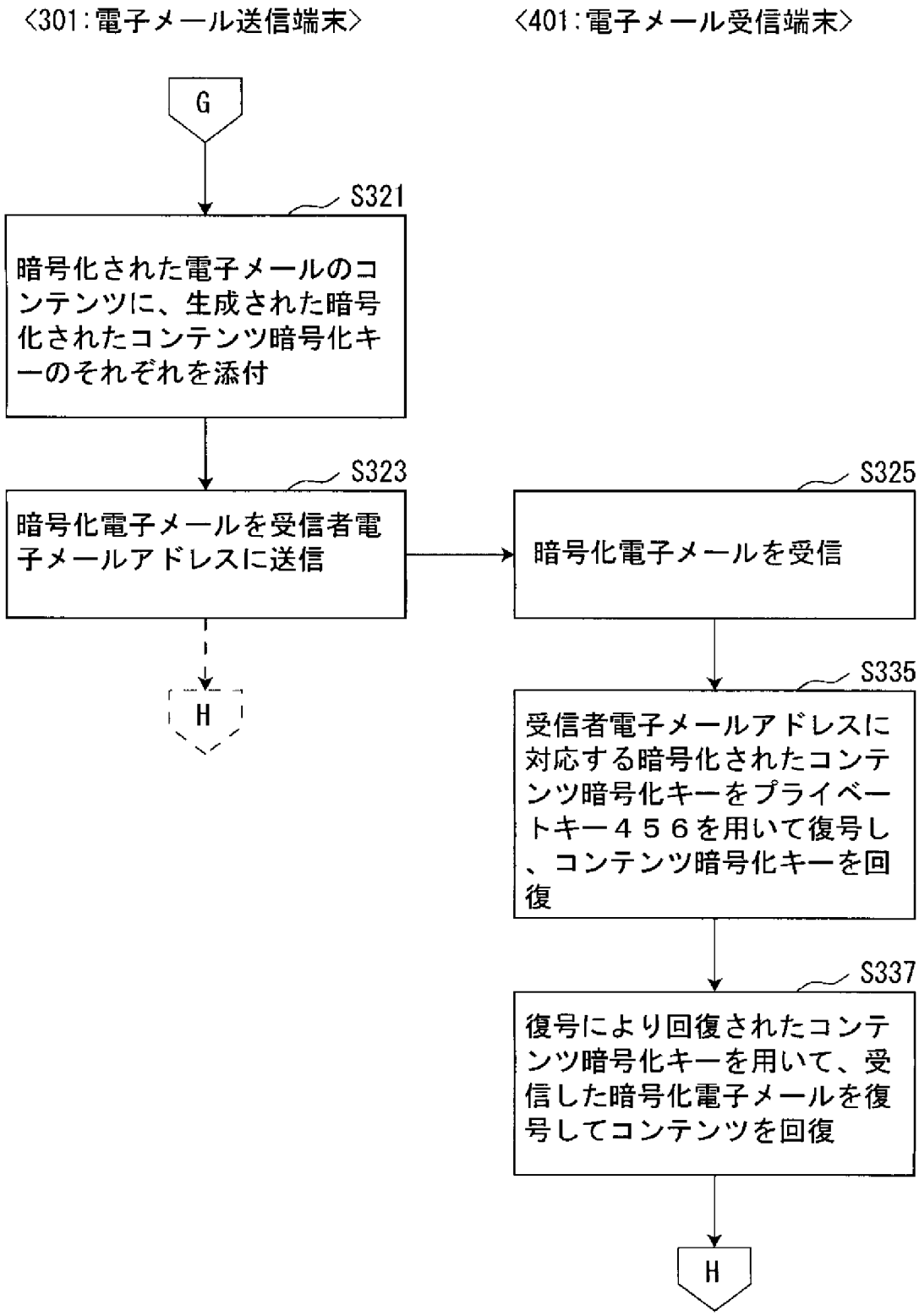
FIG. 25

<301:電子メール送信端末>



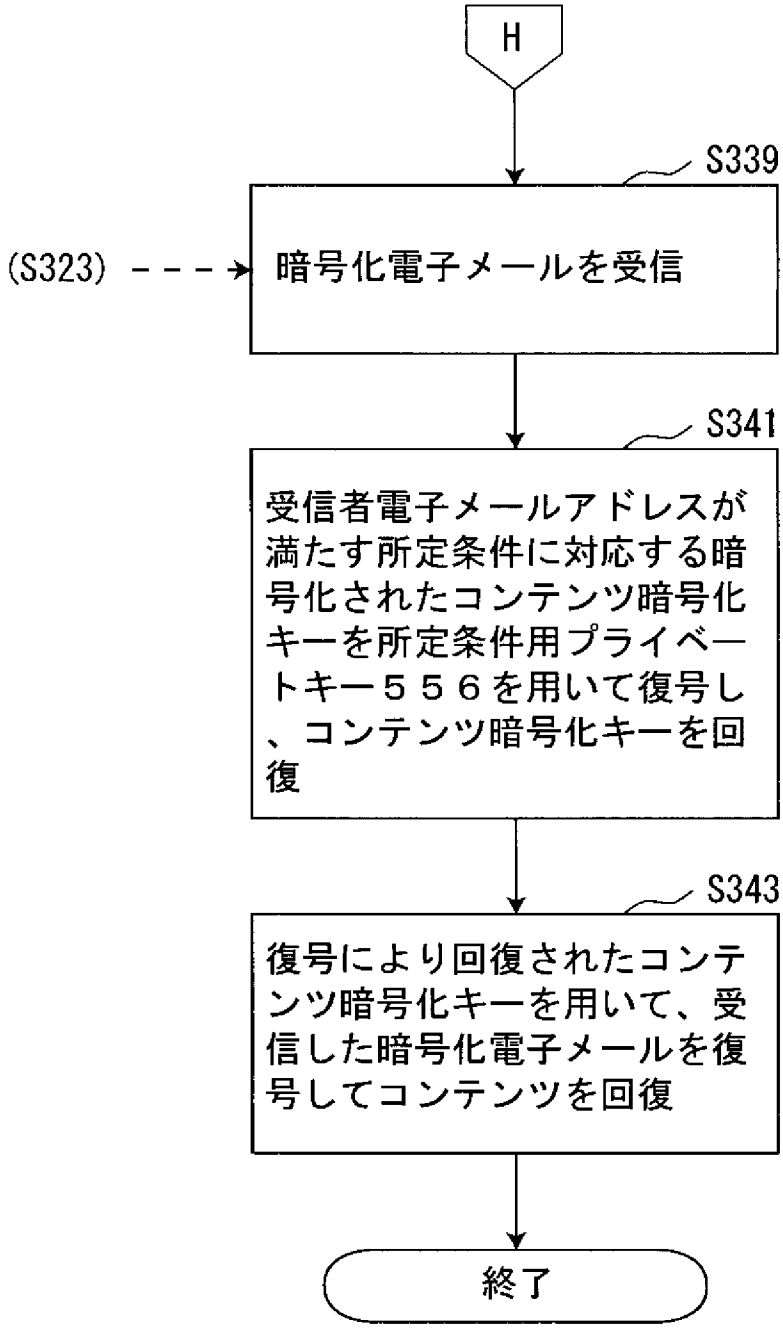
[図26]

FIG. 26


〈301：電子メール送信端末〉
〈401：電子メール受信端末〉
G
S321
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
S323
暗号化電子メールを受信者電子メールアドレスに送信
H
S325
暗号化電子メールを受信
S335
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
S337
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
H

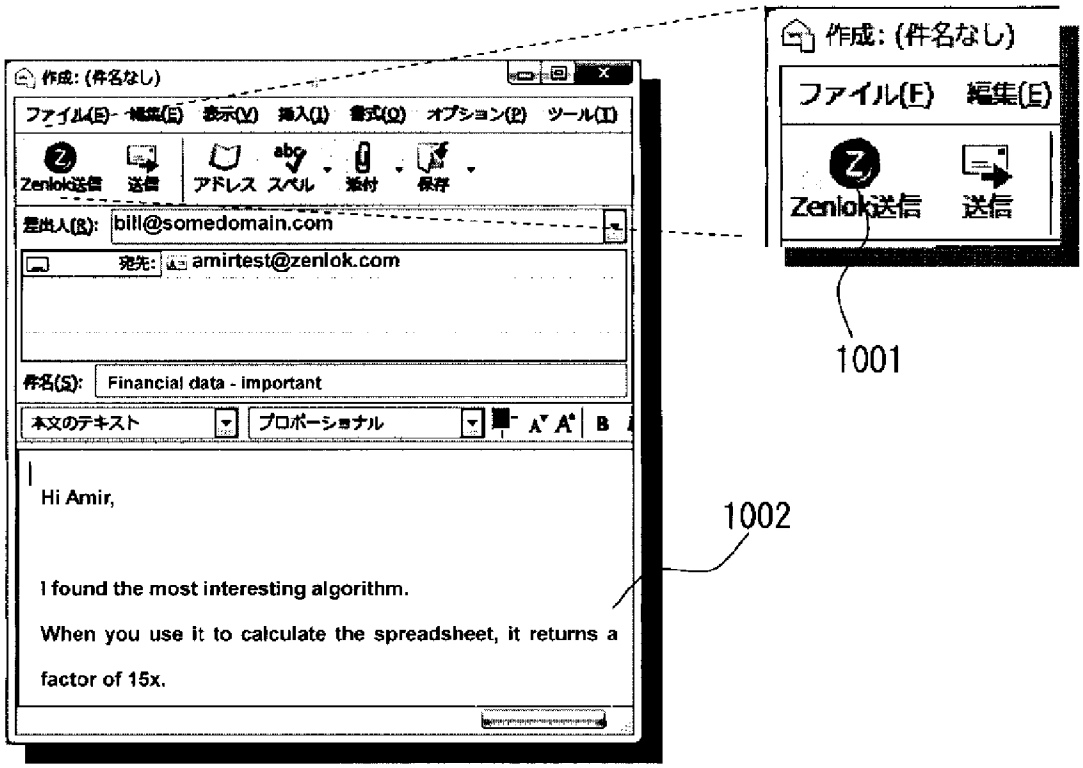
[図27]

FIG. 27


<501:所定条件電子メール代表受信端末>
H
S339
(S323)
暗号化電子メールを受信
S341
受信者電子メールアドレスが満たす所定条件に対応する暗号化されたコンテンツ暗号化キーを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
S343
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
終了

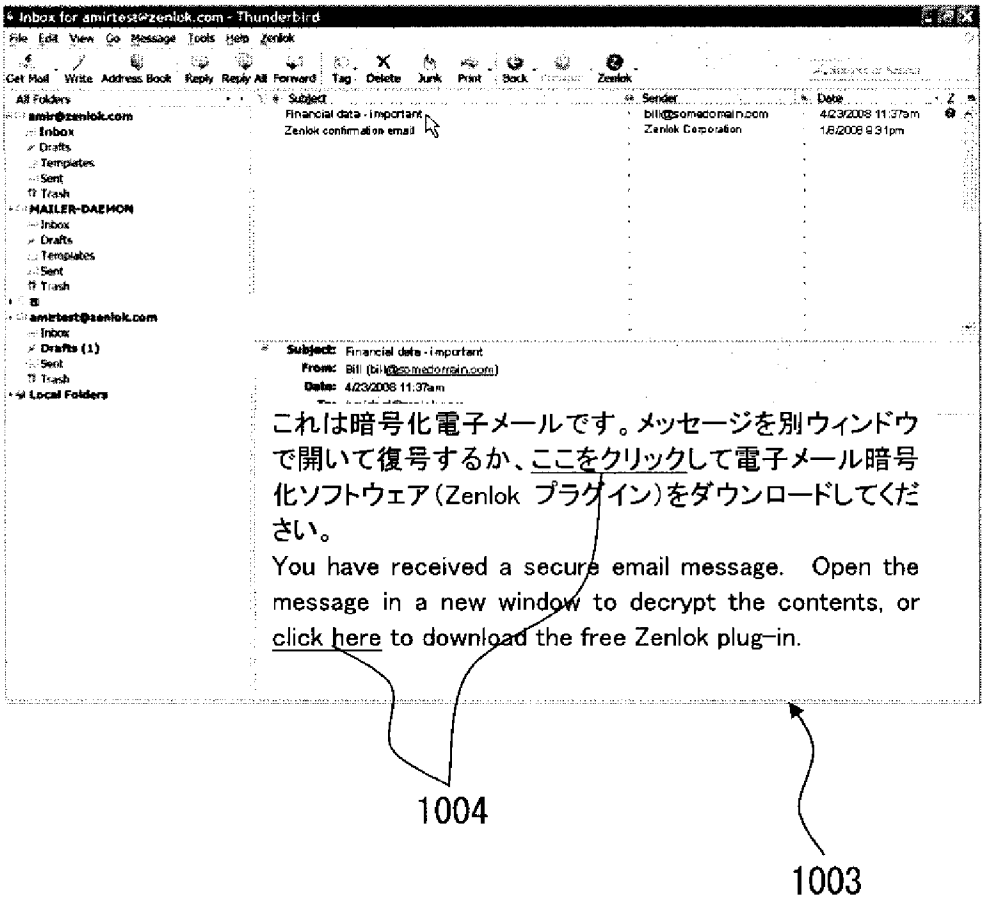
[図28]

FIG. 28


作成: (件名なし)
ファイル(F) 編集(E)
Zenlok送信 送信
1001
作成: (件名なし)
ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) オプション(P) ツール(T)
Zenlok送信 送信 アドレス スペル 添付 保存
差出人(R): bill@somedomain.com
宛先: amirtest@zenlok.com
件名(S): Financial data - important
本文のテキスト プロポーショナル
Hi Amir,
I found the most interesting algorithm.
When you use it to calculate the spreadsheet, it returns a factor of 15x.
1002

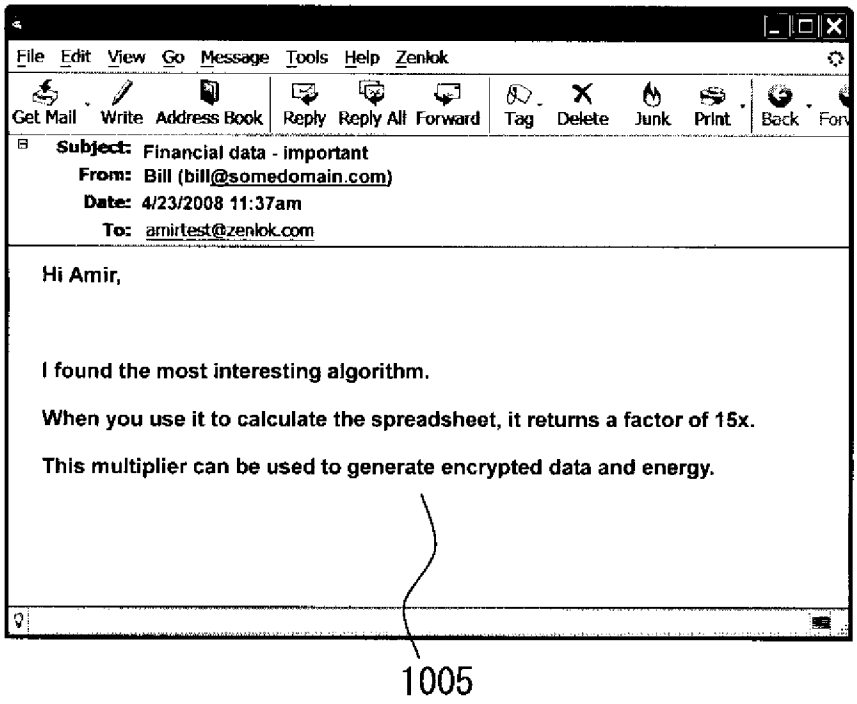
[図29]

FIG. 29


Inbox for amirtest@zenlok.com - Thunderbird
File Edit View Go Message Tools Help Zenlok
Get Mail Write Address Book Reply Reply All Forward Tag Delete Junk Print Stop Zenlok
All Folders
amir@zenlok.com
Inbox
Drafts
Templates
Sent
Trash
MAILER-DAEMON
Inbox
Drafts
Templates
Sent
Trash
amirtest@zenlok.com
Inbox
Drafts (1)
Sent
Trash
Local Folders
Subject
Financial data - important
Zenlok confirmation email
Sender
bill@somedomain.com
Zenlok Corporation
Date
4/23/2008 11:37am
1/8/2008 9:31pm
Subject: Financial data - important
From: Bill (bill@somedomain.com)
Date: 4/23/2008 11:37am
これは暗号化電子メールです。メッセージを別ウィンドウで開いて復号するか、ここをクリックして電子メール暗号化ソフトウェア(Zenlok プラグイン)をダウンロードしてください。
You have received a secure email message. Open the message in a new window to decrypt the contents, or click here to download the free Zenlok plug-in.
1004
1003

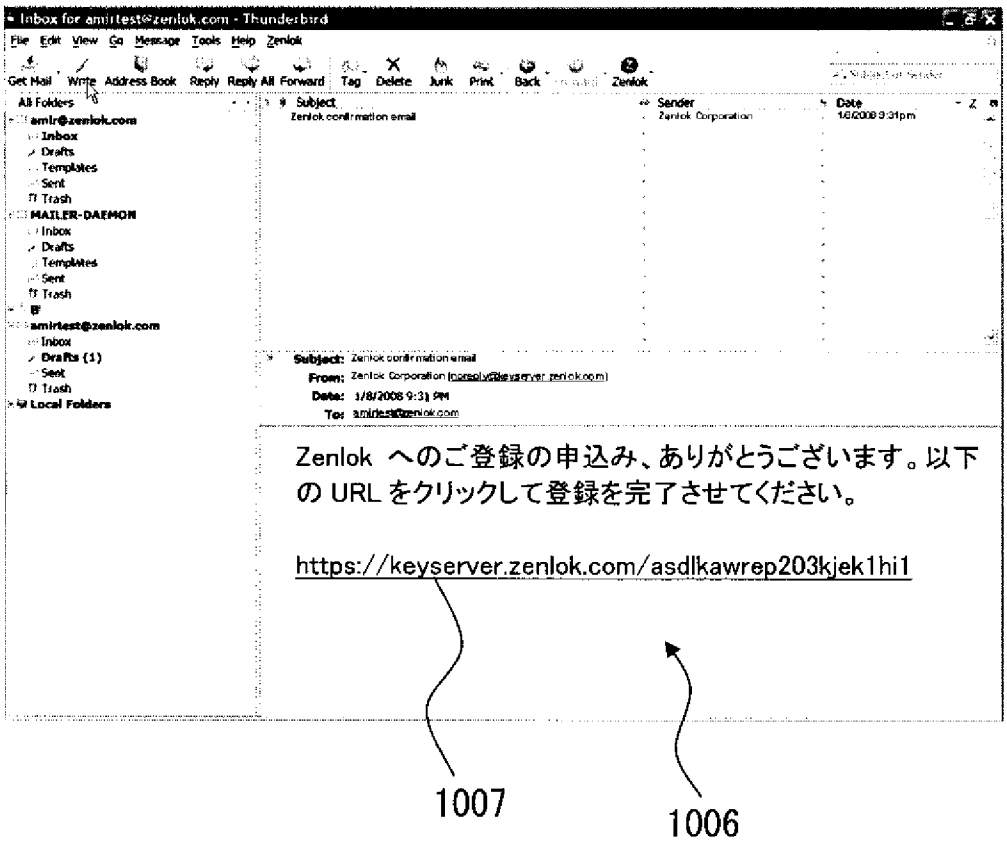
[図30]

FIG. 30


File Edit View Go Message Tools Help Zenlok
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Subject: Financial data - important
From: Bill (bill@somedomain.com)
Date: 4/23/2008 11:37am
To: amirtest@zenlok.com
Hi Amir,
I found the most interesting algorithm.
When you use it to calculate the spreadsheet, it returns a factor of 15x.
This multiplier can be used to generate encrypted data and energy.
1005

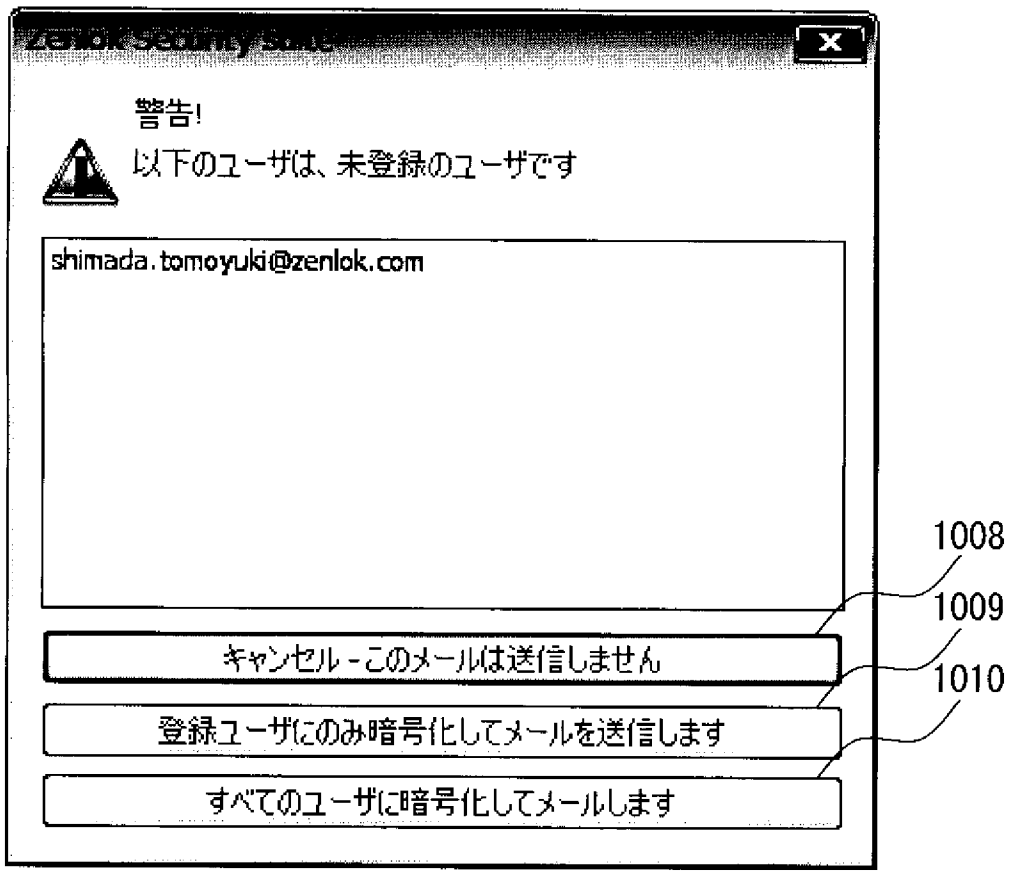
[図31]

FIG. 31


Inbox for amirtest@zenlok.com - Thunderbird
File Edit View Go Message Tools Help Zenlok
Get Mail Write Address Book Reply Reply All Forward Tag Delete Junk Print Back Zenlok
All Folders
amir@zenlok.com
Inbox
Drafts
Templates
Sent
Trash
MAILER-DAEMON
Inbox
Drafts
Templates
Sent
Trash
amirtest@zenlok.com
Inbox
Drafts (1)
Sent
Trash
Local Folders
Subject
Zenlok confirmation email
Sender
Zenlok Corporation
Date
1/6/2008 9:31pm
Subject: Zenlok confirmation email
From: Zenlok Corporation
Date: 1/8/2008 9:31 PM
To:
Zenlok へのご登録の申込み、ありがとうございます。以下の URL をクリックして登録を完了させてください。
https://keyserver.zenlok.com/asdlkawrep203kjek1hi1
1007
1006

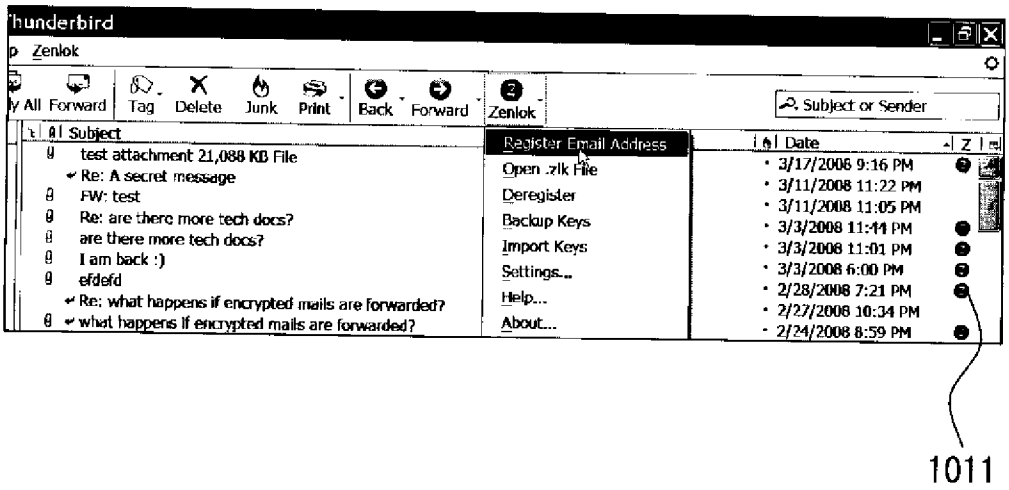
[図32]

FIG. 32


警告!
以下のユーザは、未登録のユーザです
shimada.tomoyuki@zenlok.com
キャンセル - このメールは送信しません
登録ユーザにのみ暗号化してメールを送信します
すべてのユーザに暗号化してメールします
1008
1009
1010

[図33]

FIG. 33


hunderbird
p Zenlok
y All Forward
Tag
Delete
Junk
Print
Back
Forward
Zenlok
Subject or Sender
Subject
test attachment 21,088 KB File
Re: A secret message
FW: test
Re: are there more tech docs?
are there more tech docs?
I am back :)
efdefd
Re: what happens if encrypted mails are forwarded?
what happens if encrypted mails are forwarded?
Register Email Address
Open .zlk File
Deregister
Backup Keys
Import Keys
Settings...
Help...
About...
Date
3/17/2008 9:16 PM
3/11/2008 11:22 PM
3/11/2008 11:05 PM
3/3/2008 11:44 PM
3/3/2008 11:01 PM
3/3/2008 6:00 PM
2/28/2008 7:21 PM
2/27/2008 10:34 PM
2/24/2008 8:59 PM
1011

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/058975

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F13/00*(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2005-517348 A (Surety, Inc.), 09 June, 2005 (09.06.05), Par. Nos. [0027], [0035], [0037] to [0054], [0085], [0087], [0093] to [0097] & US 2003/0147536 A1 & EP 1479188 A & WO 2003/067809 A1 & CA 2475489 A & CN 1647442 A	1-4,6-14
Y	JP 9-46330 A (Toshiba Corp.), 14 February, 1997 (14.02.97), Par. Nos. [0012], [0024] to [0033], [0051] to [0054] & US 6289105 B1	1-4,6-14

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
18 July, 2008 (18.07.08)	29 July, 2008 (29.07.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/058975

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2006-313434 A (Canon Inc.), 16 November, 2006 (16.11.06), Par. No. [0027] (Family: none)	6-14
Y	JP 2005-150888 A (Hitachi, Ltd.), 09 June, 2005 (09.06.05), Par. Nos. [0009], [0041] & US 2005/0102522 A1	8-10
A	JP 2002-368823 A (Fuji Xerox Co., Ltd.), 20 December, 2002 (20.12.02), Par. No. [0102] & US 2005/0102522 A1	5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０５８９７５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F13/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８年

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2005-517348 A (シュアテイ　インコーポレイテッド) 2005.06.09, 段落【0027】, 【0035】, 【0037】～【0054】, 【0085】, 【0087】, 【0093】～【0097】 & US 2003/0147536 A1 & EP 1479188 A & WO 2003/067809 A1 & CA 2475489 A & CN 1647442 A	1-4,6-14
Y	JP 9-46330 A (株式会社東芝) 1997.02.14, 段落【0012】, 【0024】～【0033】, 【0051】～【0054】 & US 6289105 B1	1-4,6-14

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

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

国際調査を完了した日 １８．０７．２００８	国際調査報告の発送日 ２９．０７．２００８
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　４１８０ 速水　雄太 電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2006-313434 A (キャノン株式会社) 2006.11.16, 段落【0027】（ファミリーなし)	6-14
Y	JP 2005-150888 A (株式会社日立製作所) 2005.06.09, 段落【0009】, 【0041】 & US 2005/0102522 A1	8-10
A	JP 2002-368823 A (富士ゼロックス株式会社) 2002.12.20, 段落【0102】 & US 2005/0102522 A1	5