(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2011-217268
(P2011-217268A)
(43)公開日　平成23年10月27日(2011.10.27)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/14	(2006.01)	H04L	9/00	641	5B084
G09C	1/00	(2006.01)	G09C	1/00	660E	5J104
G06F	13/00	(2006.01)	G06F	13/00	610S	

審査請求 未請求　請求項の数 10　ＯＬ　（全 12 頁）

(21)出願番号　特願2010-85318(P2010-85318)
(22)出願日　平成22年4月1日(2010.4.1)

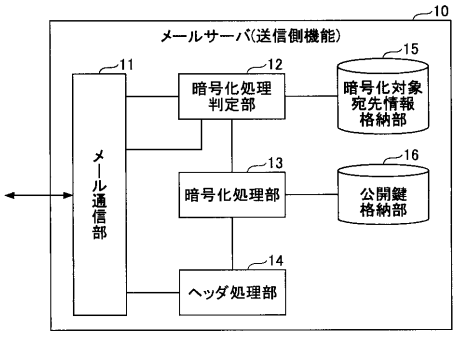
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100124844
弁理士　石原　隆治
(72)発明者　石川　寛
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B084 AA01 AA15 AB02 AB26 AB31 AB36 BB01 BB16 CB04 CB23
5J104 AA16 AA32 BA02 DA03 EA04 EA16 EA17 JA21 NA02 NA06 NA37 PA08

(54)【発明の名称】メールサーバ、メール通信システム、及びメール送受信方法

(57)【要約】
【課題】送信者端末及び受信者端末において、特別な事前準備等を行うことなく、２拠点間でのメールの暗号化通信を実現する。
【解決手段】ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信するメールサーバにおいて、ユーザ端末から受信した前記メールの宛先情報が、暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する手段と、前記メールの暗号化を行うと判定された場合に、前記宛先情報に対応する暗号鍵を暗号鍵格納手段から取得し、当該暗号鍵を用いて前記メールの本文を暗号化する手段と、前記メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加する手段とを備える。
【選択図】図４

拠点Aのメールサーバ10の機能構成図



【特許請求の範囲】
【請求項１】
ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信するメールサーバであって、
暗号化対象となるメールの宛先情報を格納した暗号化対象宛先情報格納手段と、
宛先情報毎に暗号鍵を格納した暗号鍵格納手段と、
ユーザ端末から受信した前記メールの宛先情報が、前記暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する暗号化処理判定手段と、
前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記宛先情報に対応する暗号鍵を前記暗号鍵格納手段から取得し、当該暗号鍵を用いて前記メールの本文を暗号化する暗号化処理手段と、
前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加するヘッダ処理手段と
を備えたことを特徴とするメールサーバ。
【請求項２】
前記宛先情報は、宛先ドメインであることを特徴とする請求項１に記載のメールサーバ。
【請求項３】
送信側メールサーバからメールを受信し、当該メールをユーザ端末に配信するメールサーバであって、
前記送信側メールサーバから受信するメールの本文が暗号化されている場合に、当該メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダが付加されており、
前記メールのヘッダ部分に、前記セキュアメールヘッダが含まれ、当該セキュアメールヘッダにおける前記復号化処理サーバ識別情報が、自メールサーバを示す情報であるか否かを確認することにより、前記メールに対する復号化処理を行うか否かを判定するヘッダ確認手段と、
前記ヘッダ確認手段により、復号化を行うと判定された場合に、前記メールの暗号化に用いられた暗号鍵に対応する復号鍵を用いて、前記メールの本文を復号化し、復号化を行ったメールをメール格納手段に格納する復号化手段と
を備えることを特徴とするメールサーバ。
【請求項４】
前記暗号鍵は、公開鍵であることを特徴とする請求項１ないし3のうちいずれか1項に記載のメールサーバ。
【請求項５】
送信側ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信する送信側メールサーバと、送信側メールサーバからメールを受信し、当該メールを受信側ユーザ端末に配信する受信側メールサーバとを備えたメール通信システムであって、
前記送信側メールサーバは、
暗号化対象となるメールの宛先情報を格納した暗号化対象宛先情報格納手段と、
宛先情報毎に暗号鍵を格納した暗号鍵格納手段と、
前記送信側ユーザ端末から受信した前記メールの宛先情報が、前記暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する暗号化処理判定手段と、
前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記宛先情報に対応する暗号鍵を前記暗号鍵格納手段から取得し、当該暗号鍵を用いて前記メールの本文を暗号化する暗号化処理手段と、
前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記

メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加するヘッダ処理手段と、を備え、
前記受信側メールサーバは、
前記送信側メールサーバから受信するメールのヘッダ部分に、前記セキュアメールヘッダが含まれ、当該セキュアメールヘッダにおける前記復号化処理サーバ識別情報が、自メールサーバを示す情報であるか否かを確認することにより、前記メールに対する復号化処理を行うか否かを判定するヘッダ確認手段と、
前記ヘッダ確認手段により、復号化を行うと判定された場合に、前記メールの暗号化に用いられた暗号鍵に対応する復号鍵を用いて、前記メールの本文を復号化し、復号化を行ったメールをメール格納手段に格納する復号化手段と、を備える
ことを特徴とするメール通信システム。
【請求項６】
前記宛先情報は、宛先ドメインであることを特徴とする請求項５に記載のメール通信システム。
【請求項７】
前記暗号鍵は、公開鍵であることを特徴とする請求項５又は６に記載のメール通信システム。
【請求項８】
送信側ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信する送信側メールサーバと、送信側メールサーバからメールを受信し、当該メールを受信側ユーザ端末に配信する受信側メールサーバとを備えたメール通信システムが実行するメール送受信方法であって、
前記送信側メールサーバは、暗号化対象となるメールの宛先情報を格納した暗号化対象宛先情報格納手段と、宛先情報毎に暗号鍵を格納した暗号鍵格納手段とを備え、
前記送信側メールサーバが、前記送信側ユーザ端末から受信した前記メールの宛先情報が、前記暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する暗号化処理判定ステップと、
前記暗号化処理判定ステップにより、前記メールの暗号化を行うと判定された場合に、前記送信側メールサーバが、前記宛先情報に対応する暗号鍵を前記暗号鍵格納手段から取得し、当該暗号鍵を用いて前記メールの本文を暗号化する暗号化処理ステップと、
前記暗号化処理判定ステップにより、前記メールの暗号化を行うと判定された場合に、前記送信側メールサーバが、前記メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加するヘッダ処理ステップと、
前記受信側メールサーバが、前記送信側メールサーバから受信するメールのヘッダ部分に、前記セキュアメールヘッダが含まれ、当該セキュアメールヘッダにおける前記復号化処理サーバ識別情報が、自メールサーバを示す情報であるか否かを確認することにより、前記メールに対する復号化処理を行うか否かを判定するヘッダ確認ステップと、
前記受信側メールサーバが、前記ヘッダ確認ステップにより、復号化を行うと判定された場合に、前記メールの暗号化に用いられた暗号鍵に対応する復号鍵を用いて、前記メールの本文を復号化し、復号化を行ったメールをメール格納手段に格納する復号化ステップと、
を備えることを特徴とするメール送受信方法。
【請求項９】
前記宛先情報は、宛先ドメインであることを特徴とする請求項８に記載のメール送受信方法。
【請求項１０】
前記暗号鍵は、公開鍵であることを特徴とする請求項８又は９に記載のメール送受信方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットを経由して２拠点間でセキュアにメールの送受信を行うための技術に関するものである。
【背景技術】
【０００２】
メールをセキュアに送受信するための従来技術として、S/MIME (Secure Multipurpose Internet Mail Extensions (IETF RFC 2633)) （非特許文献１）による暗号化方式がある。この方式によるメール送受信のための手順を図１を参照して説明する。
【０００３】
まず、事前準備として、拠点Bにおける受信者端末において、証明書発行サーバから証明書（公開鍵、秘密鍵）を取得し、保持する（事前１）。また、拠点Aの送信者端末において、証明書発行サーバもしくは受信者から証明書の公開鍵を取得する（事前２）。
【０００４】
そして、実際のメール送受信の段階において、送信者端末は公開鍵を用いてメールの暗号化を行い（ステップ１）、暗号化済みメールを送信する。暗号化済みメールは、通常のメール転送と同様にして、受信者端末に届けられる（ステップ２）。その後、受信者端末では、保持している秘密鍵を用いてメールの復号化を行う（ステップ３）。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】IETF RFC2633 (S/MIME (Secure Multipurpose Internet Mail Extensions))
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ところで、多くの企業において、メールサーバが設置される単位となる拠点（企業のビル等）内でのセキュリティーは保たれているのが一般的であり、複数の拠点を持つ企業内での拠点間でのメール送受信や、信頼のおける複数企業間でのメール送受信では、end-endでなく、２拠点間（拠点のメールサーバ間）でセキュアにメールの送受信ができれば十分な場合が多い。
【０００７】
２拠点間でセキュアにメールをやり取りすることを目的とした場合、従来方式ではオーバースペックな側面があり、主に以下に示す３つの課題がある。
【０００８】
（１）図１を参照して説明したように、メール送受信以外に事前準備が必要であり、メールの受信者側で証明書の取得を行っていない場合や、受信者側の公開鍵を送信者が保持していない場合は暗号化によるメール送受信はできなかった。すなわち、２拠点間の任意のユーザ間でやり取りされるメールを暗号化できなかった。
【０００９】
（２）また、送信者と受信者、両方が対応するメールクライアントを用意する必要があり、メールクライアント環境によっては対応しない可能性があった。
【００１０】
（３）更に、メールを複数の宛先に配信する場合は、各宛先のアドレス毎に発信者が上記の事前準備を行う必要があった。また、メーリングリストを用いた多数の宛先への暗号化配信を行うためには、例えば図２に示すように、メールサーバ側での特別な処理が必要であった。
【００１１】
つまり、メーリングリスト等、送信者が送信するメールの宛先アドレスと実際の受信者

が一致しない方式の場合、送信者は最終的な受信者を把握できないため、宛先のアドレス（図２の例におけるgroup1@example.com）に対応する公開鍵(g)）を準備し、当該公開鍵(g)を用いて送信するメールを暗号化することになる(図２のステップ１１)。

【００１２】

一方、メーリングリストの宛先アドレスに対応するMLサーバにおいては、事前準備として、メーリングリスト用証明書（秘密鍵(g)、公開鍵(g)）を取得するとともに、各受信者毎の公開鍵（１～３）を取得しておき、各受信者（１～３）は事前準備として証明書を取得しておく必要がある。そして、送信者端末から送信されたメールを受信するMLサーバにおいて、一旦メールを復号化し、各受信者毎に、公開鍵を用いて再暗号化したメールを送信する（図２のステップ１２）。

【００１３】

本発明は上記の点に鑑みてなされたものであり、上記の課題を解決し、送信者端末及び受信者端末において、特別な事前準備等を行うことを必要とせずに、２拠点間でのメールの暗号化通信を実現するための技術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】

【００１４】

上記の課題を解決するために、本発明は、ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信するメールサーバであって、暗号化対象となるメールの宛先情報を格納した暗号化対象宛先情報格納手段と、宛先情報毎に暗号鍵を格納した暗号鍵格納手段と、ユーザ端末から受信した前記メールの宛先情報が、前記暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する暗号化処理判定手段と、前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記宛先情報に対応する暗号鍵を前記暗号鍵格納手段から取得し、当該暗号鍵を用いて前記メールの本文を暗号化する暗号化処理手段と、前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加するヘッダ処理手段とを備えたことを特徴とするメールサーバとして構成される。

【００１５】

また、本発明は、送信側メールサーバからメールを受信し、当該メールをユーザ端末に配信するメールサーバであって、前記送信側メールサーバから受信するメールの本文が暗号化されている場合に、当該メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダが付加されており、前記メールのヘッダ部分に、前記セキュアメールヘッダが含まれ、当該セキュアメールヘッダにおける前記復号化処理サーバ識別情報が、自メールサーバを示す情報であるか否かを確認することにより、前記メールに対する復号化処理を行うか否かを判定するヘッダ確認手段と、前記ヘッダ確認手段により、復号化を行うと判定された場合に、前記メールの暗号化に用いられた暗号鍵に対応する復号鍵を用いて、前記メールの本文を復号化し、復号化を行ったメールをメール格納手段に格納する復号化手段とを備えることを特徴とするメールサーバとして構成することもできる。

【００１６】

また、本発明は、送信側ユーザ端末からメールを受信し、当該メールを、受信側メールサーバに送信する送信側メールサーバと、送信側メールサーバからメールを受信し、当該メールを受信側ユーザ端末に配信する受信側メールサーバとを備えたメール通信システムであって、前記送信側メールサーバは、暗号化対象となるメールの宛先情報を格納した暗号化対象宛先情報格納手段と、宛先情報毎に暗号鍵を格納した暗号鍵格納手段と、前記送信側ユーザ端末から受信した前記メールの宛先情報が、前記暗号化対象宛先情報格納手段に格納されているか否かを確認することにより、当該メールを暗号化するか否かを判定する暗号化処理判定手段と、前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記宛先情報に対応する暗号鍵を前記暗号鍵格納手段から取得し、当

該暗号鍵を用いて前記メールの本文を暗号化する暗号化処理手段と、前記暗号化処理判定手段により、前記メールの暗号化を行うと判定された場合に、前記メールのヘッダ部分に、復号化処理を行うメールサーバを示す復号化処理サーバ識別情報を含むセキュアメールヘッダを付加するヘッダ処理手段と、を備え、前記受信側メールサーバは、前記送信側メールサーバから受信するメールのヘッダ部分に、前記セキュアメールヘッダが含まれ、当該セキュアメールヘッダにおける前記復号化処理サーバ識別情報が、自メールサーバを示す情報であるか否かを確認することにより、前記メールに対する復号化処理を行うか否かを判定するヘッダ確認手段と、前記ヘッダ確認手段により、復号化を行うと判定された場合に、前記メールの暗号化に用いられた暗号鍵に対応する復号鍵を用いて、前記メールの本文を復号化し、復号化を行ったメールをメール格納手段に格納する復号化手段と、を備えることを特徴とするメール通信システムとして構成してもよい。

【発明の効果】

【００１７】

本発明によれば、上記の３つの課題が解決され、送信者端末及び受信者端末において、特別な事前準備等を行うことを必要とせずに、２拠点間でのメールの暗号化通信を実現することが可能となる。

【図面の簡単な説明】

【００１８】

【図１】従来技術におけるメール送受信手順を説明するための図である。

【図２】従来技術においてメーリングリストを用いる場合の課題を説明するための図である。

【図３】本発明の実施の形態に係るメール通信システムの全体構成図である。

【図４】拠点Aのメールサーバ１０の機能構成図である。

【図５】公開鍵格納部１６に格納される情報の例を示す図である。

【図６】拠点Bのメールサーバ２０の機能構成図である。

【図７】メールサーバ１０の動作を説明するためのフローチャートである。

【図８】ユーザ端末から送信されるメール構成の例を示す図である。

【図９】メールサーバ間でのメール構成の例を示す図である。

【図１０】メールサーバ２０の動作を説明するためのフローチャートである。

【発明を実施するための形態】

【００１９】

以下、図面を参照して本発明の実施の形態を説明する。

【００２０】

（システム構成）

図３に本発明の実施の形態に係るメール通信システムの全体構成図を示す。図３に示すように、本実施の形態のメール通信システムは、送信側のメールサーバ１０と受信側のメールサーバ２０とを備え、これらが通信ネットワーク（インターネット等）を介して通信可能に接続されている。

【００２１】

図３の例において、メールサーバ１０は拠点Aに設置され、メールサーバ１０には、メールのクライアントソフトウェアを備えたPCであるユーザ端末１が通信ネットワーク（LAN等）を介して接続されている。また、メールサーバ２０は拠点Bに設置され、メールサーバ２０には、メールのクライアントソフトウェアを備えたPCであるユーザ端末２が通信ネットワーク（LAN等）を介して接続されている。

【００２２】

なお、メールサーバ１０とメールサーバ２０とは同じ構成を有し、両メールサーバともにメール送受信機能を有するが、本実施の形態における説明の便宜上、メールサーバ１０については送信側とし、送信（他のメールサーバへの送信）に関する機能・動作を説明し、メールサーバ２０については受信側とし、受信（他のメールサーバからの受信）に関する機能・動作を説明している。ただし、もちろん、送信側機能のみを有するメールサーバ

や、受信側機能のみを有するメールサーバを提供することも可能である。

【００２３】

＜送信側のメールサーバ１０の構成＞

図４に、メールサーバ１０の機能構成図を示す。図４は、メールサーバ１０におけるメール送信（他のメールサーバへの送信）に関する機能を示すものである。

【００２４】

図４に示すように、メールサーバ１０は、メール通信部１１、暗号化処理判定部１２、暗号化処理部１３、ヘッダ処理部１４、暗号化対象宛先情報格納部１５、及び公開鍵格納部１６を有する。各機能部の処理の詳細については、後述する動作説明のところで述べることとし、以下では、各機能部の概要を説明する。

【００２５】

メール通信部１１は、通信ネットワークを介してメールを受信し、サーバ内の機能部に渡す機能、及びサーバ内のメールを通信ネットワークを介して送出する機能を有する。暗号化処理判定部２は、ユーザ端末１から受信したメールの宛先を確認することにより、当該メールの暗号化処理要否を判定する等の機能を有する。

【００２６】

暗号化処理部１３は、暗号化処理判定部１２により暗号化対象であると判定されたメールに対する暗号化処理を行う等の機能を有する。ヘッダ処理部１４は、メールのヘッダを追加する等の処理を行う機能を有する。

【００２７】

暗号化対象宛先情報格納部１５は、暗号化処理判定部１２から参照されるものであり、暗号化対象となる宛先情報を格納している。本実施の形態では、宛先情報として宛先ドメイン（メールアドレスの@より後の文字列）を格納している。暗号化対象宛先情報格納部１５に格納されている宛先ドメインを有する宛先へのメールが、暗号化対象であると判定されることになる。この宛先情報は、システム管理者等により、予め暗号化対象宛先情報格納部１５に登録されるものである。

【００２８】

公開鍵格納部１６は、宛先情報毎に公開鍵を格納している。図５に、公開鍵格納部１６に格納される情報の例を示す。図５に示すように、本実施の形態では、公開鍵格納部１６は、宛先ドメイン毎に公開鍵を格納している。公開鍵格納部１６に格納する情報も、システム管理者等により予め準備しておくものであるが、準備しておくべき公開鍵は、ユーザ毎ではなく宛先ドメイン毎なので、準備すべき公開鍵の数は、ユーザ数に比べて非常に少ない数である。

【００２９】

＜受信側のメールサーバ２０の構成＞

図６に、メールサーバ２０の機能構成図を示す。図６は、メールサーバ２０におけるメール受信（他のメールサーバからの受信）に関する機能を示すものである。

【００３０】

図６に示すように、メールサーバ２０は、メール通信部２１、ヘッダ確認部２２、復号化部２３、メール取得部２４、メール受信処理部２５、秘密鍵格納部２６、及びメール格納部２７を有する。各機能部の処理の詳細については、後述する動作説明のところで述べることとし、以下では、各機能部の概要を説明する。

【００３１】

メール通信部２１は、通信ネットワークを介してメールを受信し、サーバ内の機能部に渡す機能、及びサーバ内のメールを通信ネットワークを介して送出する機能を有する。ヘッダ確認部２２は、他のメールサーバから受信したメールにおけるヘッダ部分を確認し、所定のヘッダの有無や復号化処理の要否等を判定する機能を有する。

【００３２】

また、復号化部２３は、ヘッダ確認部２２により、復号化処理を要すると判定されたメールに対して、秘密鍵格納部２６に格納されている自身の秘密鍵を用いて復号化処理を行

う機能を有する。メール受信処理部２５は、復号化処理等を行う必要がないメールに対して、通常のメール受信処理を行って、メール格納部２７に格納する機能を有する。

【００３３】

メール取得部２４は、ユーザ端末２からメールを取得するための一般的なプロトコルに従って、メール格納部２７に格納されたメールを取得し、ユーザ端末２に配信する機能を有する。秘密鍵格納部２６は、メールサーバ２０の秘密鍵を格納し、メール格納部２７は、ユーザ端末２に提供されることになるメールを格納する。なお、秘密鍵格納部２６に格納される秘密鍵は、システム管理者等により予め準備しておくものである。

【００３４】

メールサーバ１０とメールサーバ２０のそれぞれは、メモリやハードディスク等の記憶手段及びCPUを備える一般的なコンピュータに、各機能部に対応する処理を行うためのプログラムを搭載することにより実現できる。当該プログラムは、可搬メモリやディスク等の記録媒体から上記コンピュータにインストールしてもよいし、ネットワーク上のサーバから上記コンピュータにダウンロードし、インストールすることとしてもよい。

【００３５】

（システムの動作）

次に、本実施の形態におけるメール通信システムの動作について説明する。

【００３６】

＜送信側のメールサーバ１０の動作＞

まず、図７のフローチャートを参照して送信側のメールサーバ１０の動作を説明する。

【００３７】

拠点Aにおけるユーザ端末１から、通常のメール送信と同様にして、平文メールが送信され、メールサーバ１０は、当該メールを受信する（ステップ１０１）。ここでのメール構成、すなわち、図３での区間αにおけるメール構成の例を図８に示す。図８に示すように、このメールは、送信元アドレス及び宛先アドレスを含むヘッダと、平文の本文とからなる。

【００３８】

図７のステップ１０２において、メールサーバ１０における暗号化処理判定部１２は、取得したメールのヘッダに含まれる宛先アドレスの中の宛先ドメインを抽出し、当該宛先ドメインが暗号化対象宛先情報格納部１５に格納されているか否かを判定することにより、宛先ドメインが暗号化対象のドメインであるか否かを判定する。

【００３９】

宛先ドメインが暗号化対象宛先情報格納部１５に格納されていない場合（ステップ１０２のNo)、暗号化処理判定部１２は、以下の手続きを行わずに、そのまま通常のメール送信と同様に、メールを送信する（ステップ１０３）。

【００４０】

宛先ドメインが暗号化対象宛先情報格納部１５に格納されている場合（ステップ１０２のYes)、メールの処理は、暗号化処理部１３に渡され、暗号化処理部１３が、暗号化処理を行う（ステップ１０４）。ここでは、暗号化処理部１３は、当該メールの宛先ドメインに対応した公開鍵を公開鍵格納部１６から取得し、当該公開鍵を用いてメールの本文（添付ファイル等を含む）を暗号化する。

【００４１】

更に、ヘッダ処理部１４は、通常の S/MIME の手続きに応じて必要となるヘッダの付加等のヘッダ処理を行うとともに、メールサーバ間での暗号化・復号化処理を行うことを示すためのヘッダ （本例では、X-SecureMail で始まるヘッダ）をメールに追加する（ステップ１０５）。このヘッダは、セキュアメールヘッダと呼ぶことができる。

【００４２】

そして、上記のようにして暗号化された本文と、追加されたセキュアメールヘッダとを含むメールが、メール通信部１１を介してメールサーバ２０に送信される（ステップ１０６）。

【００４３】
図９に、メールサーバ２０に送信されるメールのメール構成、すなわち、図３における区間βにおけるメールのメール構成の例を示す。図９に示すように、当該メールは、ヘッダと、暗号化された本文を含む。ヘッダは、通常のS/MIME処理にて付与されるヘッダに加えてセキュアメールヘッダを含む。
【００４４】
本例において、セキュアメールヘッダは、暗号化を行った送信元（ソース）のサーバを示すX-SecureMail-Sourceのヘッダ情報と、復号化を行う宛先（ターゲット）のサーバを示すX-SecureMail-Targetのヘッダ情報を含む。また、図９に示す例では、X-Secure-Mail-Keyヘッダが含まれている。このX-Secure-Mail-Keyヘッダの情報を用いて、宛先のメールサーバは、送信元のメールサーバの認証を行うことができる。
【００４５】
＜受信側のメールサーバ２０の動作＞
次に、図１０のフローチャートを参照して受信側のメールサーバ２０の動作を説明する。
【００４６】
拠点Bのメールサーバ２０は、図９に示した構成を持つメールを、拠点Aのメールサーバ１０から受信する（ステップ２０１）。当該メールを受信したメールサーバ２０において、ヘッダ確認部２２は、メールのヘッダ部分を参照し、メールにセキュアメールヘッダが付加されているか否か（具体的には、X-SecureMailがあるか否か） の判定を行う（ステップ２０２）。セキュアメールヘッダが付加されていない場合、メールはメール受信処理部２５に渡され、通常のメール受信処理が行われることにより、メールはメール格納部２７に格納される（ステップ２０３、２０７）。
【００４７】
図１０のステップ２０２において、セキュアメールヘッダが付加されていると判定された場合、ステップ２０４に進み、ヘッダ確認部２２は、自身（メールサーバ２０）が、X-SecureMail-Target ヘッダに記述されているサーバ名(svr2.example2.com)に該当するか否かを判定することにより、当該メールは、自身が復号化するメールであるか否かを判定する（ステップ２０４）。なお、メールサーバ２０のサーバ名は、メモリ等の記憶手段に格納されており、ヘッダ確認部２２は、当該格納されている情報と、X-SecureMail-Target ヘッダの情報とを比較する。
【００４８】
ステップ２０４において、自身（メールサーバ２０）が、X-SecureMail-Target ヘッダに記述されているサーバ名(svr2.example2.com)に該当しないと判定された場合、当該メールは、復号化対象でないので、例えば、当該メールをX-SecureMail-Target ヘッダに記述されたサーバに転送する処理を行う（ステップ２０５）。
【００４９】
ステップ２０４において、自身（メールサーバ２０）が、X-SecureMail-Target ヘッダに記述されているサーバ名(svr2.example2.com)に該当すると判定された場合、当該メールは、復号化対象なので、メールは復号化部２３に渡される。
【００５０】
そして、復号化部２３は、秘密鍵格納部２６に格納されている自身の秘密鍵を用いて、メールの本文を復号化する（ステップ２０６）。なお、復号化処理自体は、通常の S/MIME の方式を利用することができる。
【００５１】
復号化されたメールは、復号化部２３によりメール格納部２７に格納される（ステップ２０７）。これにより、拠点Bのユーザ端末２からの要求に基づき、メール取得部２４により、平文のメールがユーザ端末２に届けられる。このメールは、図３における区間γのメールであり、図８に示した構成と同様の構成を有する。
【００５２】

（実施の形態のまとめ、効果）

上述した本実施の形態の技術を用いることにより、２拠点間の任意のユーザ通しでやり取りされる全てのメールの暗号化が可能となり、本文や添付ファイル等のメール本文を暗号化し、セキュアな送受信を実現できる。

【００５３】

また、グループ会社間等、異なるセキュリティ・ポリシーや異なるネットワークを構築する必要がありながら、よりセキュアにメールを送受信する際に、両者のネットワーク環境への運用ルールの変更を最小限に抑えて、かつセキュリティを向上させることが可能となる。

【００５４】

更に、発信者、受信者においては、証明書の取得やメールクライアントにおける暗号化・複合化処理を伴わないため、クライアントを操作する各ユーザ個別の処理は不要となり、かつ事前の証明書の交換作業が不要であることから、送受信時のクライアントで必要だった作業が軽減され、利用者の利便性が向上する。また、２拠点間の全てのメールが、メールサーバ通しの公開鍵・秘密鍵を利用して暗号化／復号化されるため、メーリングリスト等の特殊なアドレスを用いる場合であっても、従来のように、全ての宛先ユーザの鍵情報を準備する等の特殊処理は不要である。

【００５５】

本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

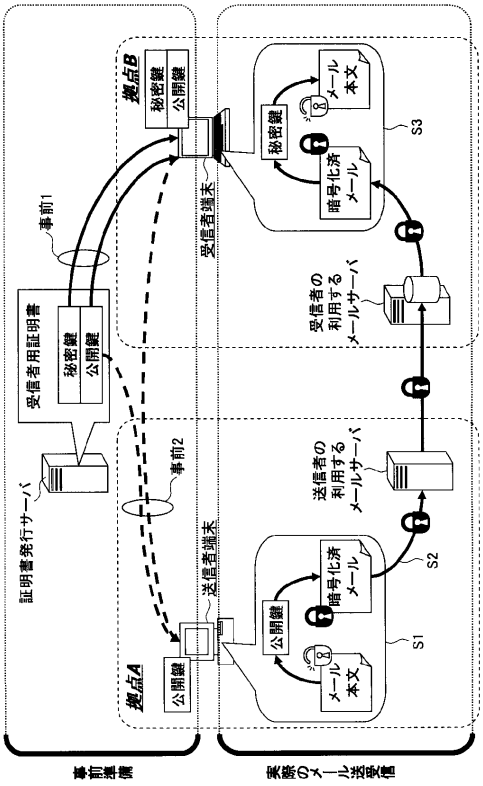
【符号の説明】

【００５６】

１、２　ユーザ端末
１０、２０　メールサーバ
１１　メール通信部
１２　暗号化処理判定部
１３　暗号化処理部
１４　ヘッダ処理部
１５　暗号化対象宛先情報格納部
１６　公開鍵格納部
２１　メール通信部
２２　ヘッダ確認部
２３　復号化部
２４　メール取得部
２５　メール受信処理部
２６　秘密鍵格納部
２７　メール格納部

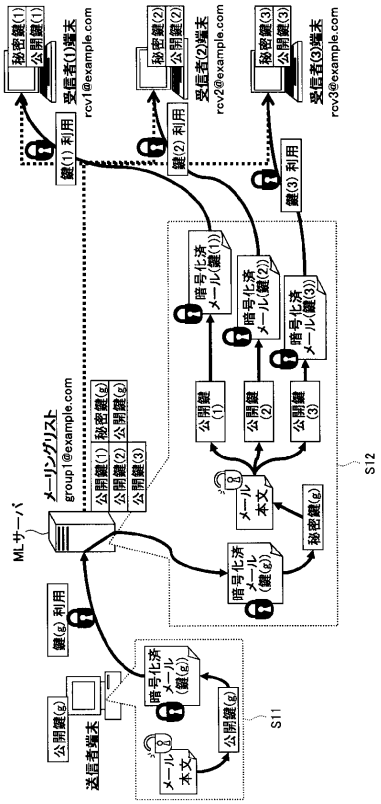
【図１】

従来技術におけるメール送受信手順を説明するための図



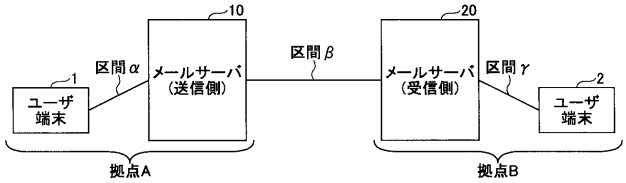
【図２】

従来技術においてメーリングリストを用いる場合の課題を説明するための図



【図３】

本発明の実施の形態に係るメール通信システムの全体構成図



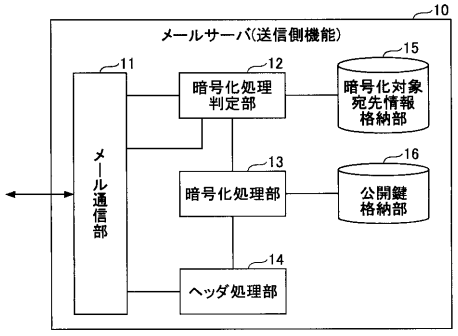
【図５】

公開鍵格納部16に格納される情報の例を示す図

宛先情報	公開鍵
宛先ドメイン1	公開鍵1
宛先ドメイン2	公開鍵2
⋮	⋮

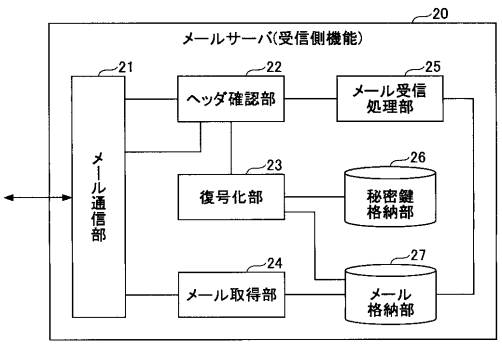
【図４】

拠点Aのメールサーバ10の機能構成図



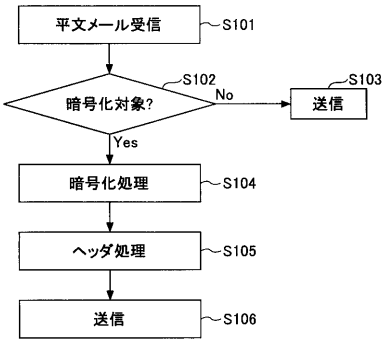
【図６】

拠点Bのメールサーバ20の機能構成図



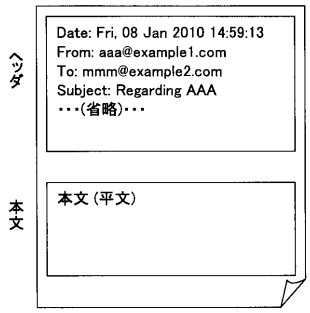
【図７】

メールサーバ10の動作を説明するためのフローチャート



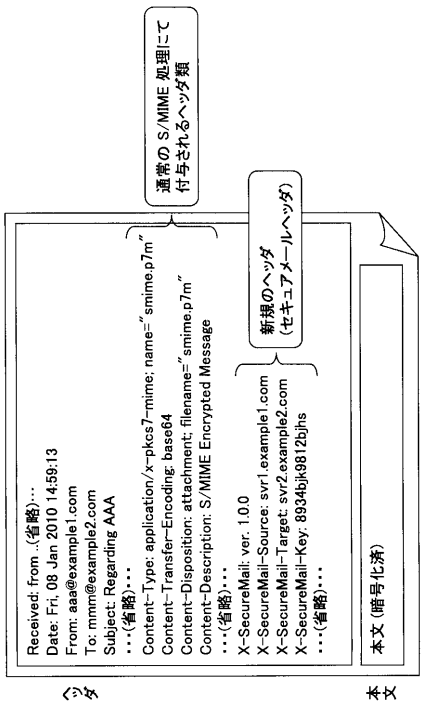
【図８】

ユーザ端末から送信されるメール構成の例を示す図



【図９】

メールサーバ間でのメール構成の例を示す図



【図１０】

メールサーバ20の動作を説明するためのフローチャート