(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2004-362129
(P2004-362129A)
(43)公開日　平成16年12月24日(2004.12.24)

| (51)Int.Cl.[7] | F I | | | テーマコード（参考） |
|---|---|---|---|---|
| G06F 13/00 | G06F | 13/00 | 610S | 5J104 |
| H04L 9/08 | H04L | 9/00 | 601B | |

審査請求 未請求　請求項の数 6　OL　（全 12 頁）

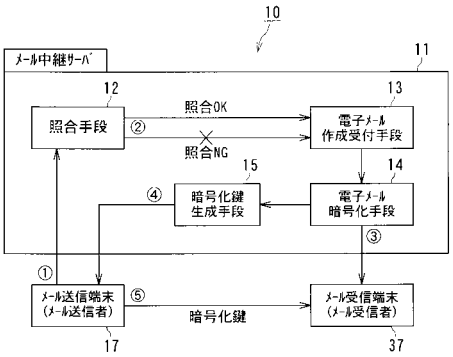
(21)出願番号　特願2003-157985(P2003-157985)
(22)出願日　平成15年6月3日(2003.6.3)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100078765
弁理士　波多野　久
(74)代理人　100078802
弁理士　関口　俊三
(74)代理人　100077757
弁理士　猿渡　章雄
(74)代理人　100122253
弁理士　古川　潤一
(72)発明者　和田　素直
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

最終頁に続く

(54)【発明の名称】電子メール暗号化配信システムおよびその方法

(57)【要約】
【課題】同一の相手であっても送信する電子メール毎に電子メールの復号化の可否を設定可能とした電子メール暗号化配信システムおよびその方法を提供する。
【解決手段】電子メール暗号化配信システム１０は、照合手段１２と、電子メール作成受付手段１３と、電子メール暗号化手段１４と、暗号化鍵生成手段１５とを備えるメール中継サーバ１１を具備し、このメール中継サーバ１１がメール暗号化配信サービスを許可した者か否かを判別する照合行程と、電子メール入力を受け付ける電子メール作成受付行程と、暗号化電子メールを作成する電子メール暗号化ステップと、指定されたアドレスに暗号化電子メールを送信する暗号化電子メール送信ステップと、暗号化電子メールを復号する使い捨て暗号化鍵を生成する暗号化鍵生成ステップと、生成された使い捨て暗号化鍵を指定されたアドレスに送信する暗号化鍵送信ステップとを実行する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
送信する電子メールを暗号化して配信するメール中継サーバを具備し、このメール中継サーバは、
電子メールを暗号化する電子メール暗号化手段と、
この電子メール暗号化手段で暗号化された電子メールを復号化する暗号化鍵を電子メールの送信者に送信する暗号化鍵生成手段とを備えることを特徴とする電子メール暗号化配信システム。
【請求項２】
前記メール中継サーバは、電子メール送信要求元が電子メール暗号化配信サービスを許可されているか否かを照合により判断する照合手段と、
電子メール送信要求元が電子メール暗号化配信サービスを許可されていると前記照合手段が判断した場合、電子メールの作成を受け付ける電子メール作成受付手段とを備えることを特徴とする請求項１記載の電子メール暗号化配信システム。
【請求項３】
前記暗号化鍵生成手段は、暗号化する電子メール毎に暗号化鍵を生成し、生成される暗号化鍵は、暗号化した電子メールの復号にのみ有効な使い捨て暗号化鍵であることを特徴とする請求項１または２記載の電子メール暗号化配信システム。
【請求項４】
メール中継サーバが送信する電子メールの作成を受け付ける電子メール作成受付行程と、この電子メール作成受付行程で入力された電子メールを暗号化した暗号化電子メールおよび前記暗号化電子メールを復号する暗号化鍵を指定された電子メールアドレスに送信する電子メール暗号化配信行程とを具備することを特徴とする電子メール暗号化配信方法。
【請求項５】
前記電子メール暗号化配信行程は、電子メール作成受付行程で入力された電子メールを暗号化して前記暗号化電子メールを作成する電子メール暗号化ステップと、
前記暗号化電子メールを受信アドレス欄の電子メールアドレスに送信する暗号化電子メール送信ステップと、
前記暗号化電子メールを復号する暗号化鍵を生成する暗号化鍵生成ステップと、
前記暗号化鍵を送信アドレス欄の電子メールアドレスに送信する暗号化鍵送信ステップとを備えることを特徴とする請求項４に記載の電子メール暗号化配信方法。
【請求項６】
メール中継サーバにアクセスし、電子メール暗号化配信サービスを要求する電子メール送信要求元に対して、電子メール暗号化配信サービスが許可されているか否かを判定する照合行程を具備することを特徴とする請求項４または５記載の電子メール暗号化配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子メールのセキュリティを確保するシステムおよびその方法に係り、特に、電子メールの暗号化を行う電子メール暗号化配信システムおよびその方法に関する。
【０００２】
【従来の技術】
以下に、従来の電子メール暗号化配信システムおよびその方法の一実施例を図面を参照して説明する。
【０００３】
図５に従来の電子メールのセキュリティを確保する電子メール暗号化配信システムの一実施例である電子メール暗号化配信システム１のシステム構成概略を表す構成概略図を示す。
【０００４】
図５に示される電子メール暗号化配信システム１は、ローカルエリアネットワーク（以下

、Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ：ＬＡＮとする）２に電気的に接続されるメールサーバ３とインターネット４との間に電子メールのセキュリティに関する処理を行うプロキシ（以下、セキュアメールプロキシとする）５を電気的に接続する。

【０００５】

セキュアメールプロキシ５は、電子メールの暗号化／複合化や、書名の添付／改竄（かいざん）の検出等を実行する。セキュアメールプロキシ５の処理操作により、メールサーバ３、電子メールユーザが利用するメールクライアント６の端末種類およびセキュリティ機能の実装の有無によらず電子メールのセキュリティ確保を実現する。

【０００６】

図６に電子メール暗号化配信システム１における電子メール送信時のメールサーバ３、セキュアメールプロキシ５およびメールクライアント６の処理操作について説明した説明図（流れ図）を示す。

【０００７】

図６によれば、電子メール暗号化配信システム１における電子メール送信は、まず、ステップＳ１で、ユーザがメールクライアント６を利用して電子メールのメッセージを作成後、入力時の文章（以下、平文とする）のままメールサーバ３に送信する。

【０００８】

メールサーバ３でメールクライアント６からの平文を受信すると、次に、ステップＳ２でメールサーバ３は、メールクライアント６から送信された電子メールの電子メールアドレスを確認し、電子メールアドレスがＬＡＮ２内か否かをチェックする。電子メールアドレスがＬＡＮ２の外部の場合（ステップＳ２でＮＯの場合）、ステップＳ３に進み、ステップＳ３でメールサーバ３は、受信した平文をセキュアメールプロキシ５へ送信する。

【０００９】

セキュアメールプロキシ５で平文を受信すると、次に、ステップＳ４でセキュアメールプロキシ５は、受信した平文を公開鍵で暗号化する。そして、ステップＳ５で、電子メール発信者の電子メールアドレスに対応する秘密鍵を用いて、当該平文のメッセージダイジェスト（ハッシュ値）を計算し、計算した値を秘密鍵で暗号化した上でメール発信者の署名として添付する。

【００１０】

メール発信者の署名を添付すると、最後に、ステップＳ６でセキュアメールプロキシ５は、メール発信者の署名が添付され、暗号化された電子メール（以下、署名付き暗号化メールとする）をインターネット４に送信する。

【００１１】

また、ステップＳ２において、電子メールアドレスがＬＡＮ２内か否かをチェックして、電子メールアドレスがＬＡＮ２の外部の場合（ステップＳ２でＮＯの場合）、ステップＳ７に進み、ステップＳ７でメールサーバ３は、受信した平文をＬＡＮ２内の電子メールアドレス（メールサーバ）へ送信する。

【００１２】

次に、電子メール暗号化配信システム１における電子メール受信時のメールサーバ３、セキュアメールプロキシ５およびメールクライアント６の処理操作について説明する。

【００１３】

図７は、電子メール暗号化配信システム１における電子メール受信時のメールサーバ３、セキュアメールプロキシ５およびメールクライアント６の処理操作について説明した説明図（流れ図）である。

【００１４】

図７によれば、電子メール暗号化配信システム１における電子メール受信時は、まず、ステップＳ１１で、セキュアメールプロキシ５が、図６に示される説明図のステップＳ６においてインターネット４に送信された署名付き暗号化をインターネット４から受信する。

【００１５】

セキュアメールプロキシ５が署名付き暗号化を受信したら、次にステップＳ１２でセキュ

アメールプロキシ５は、電子メールに添付された署名を電子メール送信者の公開鍵で復号する。そして、ステップＳ１３で、署名のハッシュ値と受信した電子メールのメッセージダイジェスト（ハッシュ値）とを比較して電子メールが改竄されているか否かを検査する。

【００１６】

ステップＳ１３において、電子メールが改竄されているか否かを検査して、電子メールが改竄されていない場合（ステップＳ１３でＮＯ）は、ステップＳ１４に進み、ステップＳ１４でセキュアメールプロキシ５は、電子メールのアドレスに対応する秘密鍵を用いて暗号化されている電子メールを復号化する。

【００１７】

ステップＳ１４で平文に復号された電子メールのメッセージ（以下、平文メールとする）は、ステップＳ１５で、セキュアメールプロキシ５がＬＡＮ２内にあるメールサーバ３へ配送する。そして、ステップＳ１６で、メールサーバ３が平文メールを受信する。

【００１８】

メールサーバ３が平文メールを受信した後に、ステップＳ１７で、電子メールの送信者が入力した電子メールアドレスのメールクライアント６から電子メールの配信要求があると、ステップＳ１８で、メールサーバ３は、平文メールを配信要求先へ配信する。そして、ステップＳ１９で、メールクライアント６から電子メールの配信要求をしたユーザは、メールクライアント６で平文メールを受信する。

【００１９】

また、ステップＳ１３において、電子メールが改竄されているか否かを検査して、電子メールが改竄されている場合（ステップＳ１３でＹＥＳ）は、ステップＳ２０に進み、ステップＳ２０でセキュアメールプロキシ５は、電子メールの受信を拒否する。

【００２０】

上述した電子メール暗号化配信システムおよびその方法の一例は、特開２００２－２４１４７号公報に掲載されている。（例えば、特許文献１参照）。

【００２１】

【特許文献１】

特開２００２－２４１７７号公報（［０００２］～［０００６］，［００１０］，［００１８］，［００３２］～［００３５］，［００３８］，［００４０］，［００４２］～［００４３］，［００４５］，［００４７］～［００５０］，図１，図４，図５）

【００２２】

【発明が解決しようとする課題】

従来の電子メール暗号化配信システムおよびその方法は、電子メールの送信者が送信相手を間違えて本来送信するべきでない相手に送信した場合、電子メール受信者は、電子メールの内容を確認することができる。従って、送信時の不注意等によって、本来送信するべきでない相手、すなわち、第三者に内容が漏洩してしまう問題があった。

【００２３】

また、一度、公開鍵および秘密鍵を登録すると、登録した相手は一様に暗号化された電子メールを読むことが可能となるため、電子メール毎に復号化の可否の設定をすることができず、特に重要度の高い内容が何らかの手違い等で第三者に漏洩してしまうおそれがあった。

【００２４】

本発明は、上述した事情を考慮してなされたものであり、同一の相手であっても送信する電子メールの内容の重要度や秘密度に応じて、電子メールの復号化の可否の設定を可能とした電子メール暗号化配信システムおよびその方法を提供することを目的とする。

【００２５】

また、本発明の他の目的は、電子メールの送信者が送信相手を間違えて本来送信するべきでない相手に送信した場合であっても、受信者が内容を読むことができなくなるように図ったことにある。

【００２６】
【課題を解決するための手段】
本発明に係る暗号化電子メール暗号化配信システムは、上述した課題を解決するため、請求項１に記載したように、送信する電子メールを暗号化して配信するメール中継サーバを具備し、このメール中継サーバは、電子メールを暗号化する電子メール暗号化手段と、この電子メール暗号化手段で暗号化された電子メールを復号化する暗号化鍵を電子メールの送信者に送信する暗号化鍵生成手段とを備えることを特徴とする。
【００２７】
上述した課題を解決するため、本発明に係る暗号化電子メール暗号化配信システムは、請求項２に記載したように、前記メール中継サーバは、電子メール送信要求元が電子メール暗号化配信サービスを許可されているか否かを照合により判断する照合手段と、電子メール送信要求元が電子メール暗号化配信サービスを許可されていると前記照合手段が判断した場合、電子メールの作成を受け付ける電子メール作成受付手段とを備えることを特徴とする。
【００２８】
また、上述した課題を解決するため、本発明に係る暗号化電子メール暗号化配信システムは、請求項３に記載したように、前記暗号化鍵生成手段は、暗号化する電子メール毎に暗号化鍵を生成し、生成される暗号化鍵は、暗号化した電子メールの復号にのみ有効な使い捨て暗号化鍵であることを特徴とする。
【００２９】
本発明に係る暗号化電子メール暗号化配信方法は、上述した課題を解決するため、請求項４に記載したように、メール中継サーバが送信する電子メールの作成を受け付ける電子メール作成受付行程と、この電子メール作成受付行程で入力された電子メールを暗号化した暗号化電子メールおよび前記暗号化電子メールを復号する暗号化鍵を指定された電子メールアドレスに送信する電子メール暗号化配信行程とを具備することを特徴とする。
【００３０】
上述した課題を解決するため、本発明に係る暗号化電子メール暗号化配信方法は、請求項５に記載したように、前記電子メール暗号化配信行程が、電子メール作成受付行程で入力された電子メールを暗号化して前記暗号化電子メールを作成する電子メール暗号化ステップと、前記暗号化電子メールを受信アドレス欄の電子メールアドレスに送信する暗号化電子メール送信ステップと、前記暗号化電子メールを復号する暗号化鍵を生成する暗号化鍵生成ステップと、前記暗号化鍵を送信アドレス欄の電子メールアドレスに送信する暗号化鍵送信ステップとを備えることを特徴とする。
【００３１】
また、上述した課題を解決するため、本発明に係る暗号化電子メール暗号化配信方法は、請求項６に記載したように、メール中継サーバにアクセスし、電子メール暗号化配信サービスを要求する電子メール送信要求元に対して、電子メール暗号化配信サービスが許可されているか否かを判定する照合行程を具備することを特徴とする。
【００３２】
【発明の実施の形態】
以下に、本発明に係る電子メール暗号化配信システムおよびその方法について図面を参照して説明する。
【００３３】
図１に本発明に係る電子メール暗号化配信システムの一実施例である電子メール暗号化配信システム１０のシステム構成および電子メール送信手順を概略的に説明した説明図である。
【００３４】
図１に示される電子メール暗号化配信システム１０は、受信した電子メールを暗号化して配信するメール中継サーバ１１を具備する。
【００３５】

メール中継サーバ１１は、利用者を照合により判断する照合手段１２と、利用者が正しい場合に電子メールの入力を受け付ける電子メール作成受付手段１３と、電子メール作成受付手段１３で作成された電子メールを暗号化する電子メール暗号化手段１４と、電子メール暗号化手段１４で暗号化された電子メール（以下、暗号化電子メールとする）を復号化する使い捨て暗号化鍵を生成し、電子メール入力者（送信者）に送信する暗号化鍵生成手段１５とを備える。

【００３６】

図１に示される電子メール暗号化配信システム１０を利用して電子メールを暗号化して送信する迄の手順について説明する。

【００３７】

電子メール送信要求元としての電子メール送信者は、例えば、パーソナルコンピュータ（以下、ＰＣとする）、携帯電話、携帯情報端末（以下、Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ：ＰＤＡとする）等の電子メール送信用可能な端末（以下、メール送信端末とする）１７からメール中継サーバ１１内の指定されたＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）を入力してアクセスする（図１における▲１▼に該当）。

【００３８】

電子メール送信者がアクセスすると、後段で説明する図２に示される初期画面１９がメール送信端末１７に表示される。

【００３９】

図２は、メール送信端末１７に表示される初期画面１９の一例を説明する説明図である。

【００４０】

電子メール送信要求元としての図２によれば、初期画面１９は、電子メール入力画面にログインするためのログインボタン２０と、ログインＩＤおよびパスワードを登録するためのＩＤ登録ボタン２１を有する。

【００４１】

電子メール送信者は、事前にＩＤ登録を完了させた上で、初期画面１９に表示されるログインボタン２０を押す。電子メール送信者がログインボタン２０を押すと、後段で説明する図３に示されるログイン画面２２がメール送信端末１７に表示される。

【００４２】

図３は、メール送信端末１７に表示されるログイン画面２２の一例を説明する説明図である。

【００４３】

図３に示されるログイン画面２２には、名前に相当するログインＩＤ入力欄２３と、パスワードを入力するパスワード入力欄２４とがある。電子メール送信者は、ログイン画面２２のログインＩＤ入力欄２３に事前登録しておいた自己のログインＩＤを、パスワード入力欄２４に事前登録しておいたパスワードとを入力する。電子メール送信者がログインＩＤおよびパスワードの入力を完了すると、メール中継サーバ１１は、電子メールを暗号化して配信する電子メール暗号化配信手順を実行する。

【００４４】

電子メール暗号化配信手順は、メール中継入力者がサーバ１１へアクセスしたメール暗号化配信サービスを許可した者か否かを判定する照合行程と、送信する電子メールの作成を受け付ける電子メール作成受付行程と、この電子メール作成受付行程で入力された電子メールを暗号化した暗号化電子メールおよびこの暗号化電子メールを復号する暗号化鍵を指定された電子メールアドレスに送信する電子メール暗号化配信行程とを具備する。

【００４５】

電子メール暗号化配信手順では、まず、メール中継サーバ１１に備えられる照合手段１２が、照合行程として、パスワードの入力者がメール暗号化配信サービスを許可した者か否かを入力したログインＩＤおよびパスワードの正誤で判別する。

【００４６】

入力したログインＩＤおよびパスワードが正しい場合、メール中継サーバ１１が備える照合手段１２が電子メールの入力画面へのログインを許可する。一方、入力したログインＩＤおよびパスワードを誤った場合、電子メールの入力画面へのログインを許可しない（図１における▲２▼）。

【００４７】

図４にメール送信端末１７に表示される電子メールの入力画面（以下、電子メール入力画面とする）２６の一例を示す。

【００４８】

図４に示される電子メール入力画面２６は、送信者の電子メールアドレス入力欄（以下、送信アドレス入力欄とする）２７と、メール受信者の電子メールアドレス入力欄（以下、受信アドレス入力欄）２８と、件名入力欄２９と、本文入力欄３０と、送信ボタン３１とを有する。また、電子メール入力画面２６の受信アドレス入力欄２８は、一般の電子メールと同様に、宛先（Ｔｏ）入力欄３３と、写し（Ｃｃ）入力欄３４と、秘写（Ｂｃｃ）入力欄３５とがある。

【００４９】

メール中継サーバ１１は、照合行程の次に電子メール作成受付行程を実行する。そして、メール中継サーバ１１は、図４に示される電子メールの電子メール入力画面２６において、電子メール送信者からの入力を受け付ける。

【００５０】

メール中継サーバ１１が電子メールの入力を受け付けを許可したら、電子メール送信者は、まず、自分の電子メールアドレスを送信アドレス欄２７に入力し、送信したい相手の電子メールアドレス、すなわち、宛先を受信アドレス欄２８に入力する。例えば、送信したい相手が１名なら、送信したい相手の電子メールアドレスを宛先（Ｔｏ）入力欄３３に入力する。

【００５１】

電子メールのアドレス入力が完了したら、次に、電子メール送信者は、件名入力欄２９を選択し、件名を入力する。件名の入力が完了したら次に、本文入力欄３０を選択し送信したい文章を作成する。入力に際しては、そのままの文章、すなわち、平文で行う。そして、電子メール入力画面２６において、送信アドレス欄２７、受信アドレス欄２８、件名入力欄２９および本文入力欄３０の入力が完了すると、電子メール送信者の電子メールの入力（作成）作業は完了する。

【００５２】

電子メール送信者は、電子メール入力画面２６において、送信アドレス欄２７、受信アドレス欄２８、件名入力欄２９および本文入力欄３０の入力が完了すると、電子メール入力画面２６内の送信ボタン３１を押す。電子メール送信者が送信ボタン３１を押すと、メール中継サーバ１１は、電子メール作成受付行程を完了して、電子メール暗号化配信ステップを実行する。

【００５３】

電子メール暗号化配信ステップは、電子メール作成受付行程で入力され作成された電子メールを暗号化して暗号化された電子メール（以下、暗号化電子メールとする）を作成する電子メール暗号化ステップと、暗号化電子メールを指定されたアドレスに送信する暗号化電子メール送信ステップと、暗号化電子メールを復号する暗号化鍵を生成する暗号化鍵生成ステップと、暗号化鍵を指定されたアドレスに送信する暗号化鍵送信ステップとを備える。

【００５４】

電子メール暗号化配信ステップの電子メール暗号化ステップは、メール中継サーバ１１が備える電子メール暗号化手段１４でなされる。電子メール暗号化手段１４は、電子メール送信者が入力した電子メールの本文、すなわち、本文入力欄３０に記載される内容を暗号化する。

【００５５】

次に、電子メール暗号化ステップが完了すると、電子メール暗号化手段１４は、暗号化電子メール送信ステップを実行する。電子メール暗号化手段１４は、受信アドレス入力欄２８に入力された電子メールアドレスへ電子メールを送信する（図１における▲３▼）。

【００５６】

一方、電子メール暗号化配信ステップの暗号化鍵生成ステップは、メール中継サーバ１１が備える暗号化鍵生成手段１５でなされる。暗号化鍵生成手段１５は、上記メール暗号化ステップにおいて暗号化された電子メールに限って復号可能な暗号化鍵（以下、使い捨て暗号化鍵とする）を生成する。

【００５７】

次に、暗号化鍵生成ステップが完了すると、暗号化鍵生成手段１５は、暗号化鍵送信ステップを実行する。暗号化鍵生成手段１５は、生成した使い捨て暗号化鍵を電子メール送信者、すなわち、送信アドレス入力欄２７に入力された電子メールアドレスへ電子メールを送信する（図１における▲４▼）。

【００５８】

電子メール暗号化手段１４が実行する暗号化電子メール送信ステップ（図１における▲３▼）および暗号化鍵生成手段１５が実行する暗号化鍵送信ステップ（図１における▲４▼）が完了すると、電子メール暗号化配信ステップは完了する。

【００５９】

電子メール受信者は、電子メール暗号化配信ステップが完了したら、メール中継サーバ１１から配信された電子メールを、例えば、ＰＣ、携帯電話、ＰＤＡ等の電子メールの受信可能なメール受信端末３７を用いて受信する（図１における▲５▼）。ここで、受信されるメールは、暗号化電子メールである。

【００６０】

この暗号化された電子メールを電子メール受信者が読むためには、暗号化鍵生成手段１５で生成された暗号化鍵を使って暗号化された電子メールを復号する必要がある。復号することで暗号化された電子メールは平文となり読むことが可能となる。

【００６１】

但し、暗号化鍵生成手段１５で生成される暗号化鍵は、その回に限り暗号化された電子メールを復号することができる使い捨て暗号化鍵である為、暗号化電子メールの受信者は、たとえ同じ送信者から受信した暗号化電子メールであっても、電子メール受信する度に使い捨て暗号化鍵を入手する必要がある。

【００６２】

一方、電子メール送信者は、電子メール暗号化配信ステップが完了したら、メール中継サーバ１１から受信した暗号化鍵を送信するか否かを判断する。送信した電子メールを読んでもらいたい場合は、電子メールを送信した相手にメール中継サーバ１１を経由せずに電子メールの受信者に暗号化鍵を送信すれば良い（図１における▲４▼）。尚、電子メールアドレスの入力ミス等で送信した電子メールを読まれたくない場合は、使い捨て暗号化鍵を送信しなければ良い。

【００６３】

尚、本実施の形態の説明では、メール中継サーバ１１は照合手段１２を備えるとしているが、照合手段１２は必ずしも必要ではない。メール中継サーバ１１の指定したアドレスに電子メールを平文で送信するようにしても良い。照合手段１２がない場合においては、照合行程も不要となる。

【００６４】

また、図３および図４に示されるログイン画面２２および電子メール入力画面２６については、一実施例であり、図に示されるものに限定されない。例えば、電子メール入力画面２６において、電子メールアドレスを登録管理できるアドレス帳を呼び出すボタンやシグネチャー（署名）を添付するボタンを設ける等、一般的に使用され得る形態であれば差し支えない。

【００６５】

さらに、図３に示されるログイン画面２２において、電子メール送信者がある一定回数ログインを失敗した場合、強制的にログイン画面２２から図に示されないログイン失敗画面等を表示する他のＵＲＬへ移動させたり、ログインを受け付けなくする等の方法を採っても良い。

【００６６】

一方、図４に示される電子メール入力画面２６において、送信アドレス欄２７に自分の電子メールアドレスを入力するとしているが、事前登録の際に送信先の電子メールアドレスを登録させて、電子メール入力画面２６における送信アドレス欄２７を登録時に設定した電子メールアドレスとして入力を省略できる様に設定しても良い。

【００６７】

また、ログイン後の電子メール入力画面２６において、暗号化鍵を電子メールの送信者以外にも、特定の宛先の受信者に対して配信するか否かを設定可能に構成しても良い。

【００６８】

以上、電子メール暗号化配信システム１０およびその方法によれば、同一の相手であっても送信する電子メールの内容の重要度や秘密度に応じて、電子メールの復号化の可否の設定を可能とした電子メール暗号化配信システムおよびその方法を提供することができる。

【００６９】

また、電子メールの送信者が送信相手を間違えて本来送信するべきでない相手に送信した場合であっても、使い捨て暗号化鍵がないと内容を読むことができないので、第三者に内容が漏洩するのを防止することができる。

【００７０】

【発明の効果】

本発明に係る電子メール暗号化配信システムおよびその方法によれば、同一の相手であっても送信する電子メールの内容の重要度や秘密度に応じて、電子メールの復号化の可否の設定を可能とした電子メール暗号化配信システムおよびその方法を提供することができる。

【００７１】

また、電子メールの送信者が送信相手を間違えて本来送信するべきでない相手に送信した場合であっても、使い捨て暗号化鍵がないと内容を読むことができないので、第三者に内容が漏洩する事がない。

【図面の簡単な説明】

【図１】本発明に係る電子メール暗号化配信システムの一実施例の構成概略を表したシステム構成概略図。

【図２】本発明に係る電子メール暗号化配信システムにおいて、メール送信端末に表示される初期画面の一例を示した説明図。

【図３】本発明に係る電子メール暗号化配信システムにおいて、メール送信端末に表示されるログイン画面の一例を示した説明図。

【図４】本発明に係る電子メール暗号化配信システムにおいて、メール送信端末に表示される電子メールの入力画面の一例を示した説明図。

【図５】従来の電子メールのセキュリティを確保する電子メール暗号化配信システムの一実施例におけるシステム構成概略を表す構成概略図。

【図６】電子メール暗号化配信システムにおける電子メール送信時の処理操作について説明した説明図。

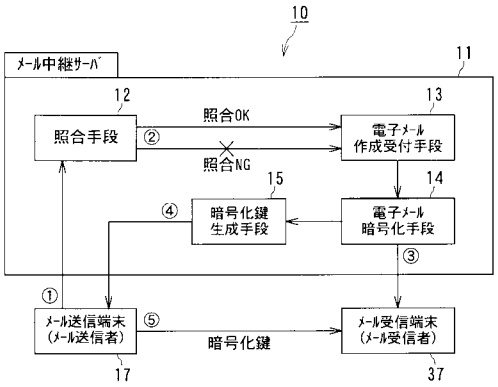
【図７】電子メール暗号化配信システムにおける電子メール受信時の処理操作について説明した説明図。

【符号の説明】

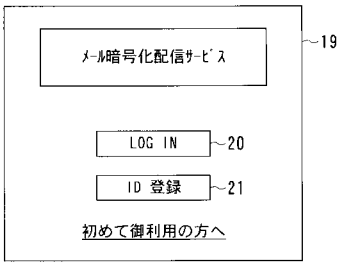
１０　電子メール暗号化配信システム
１１　メール中継サーバ
１２　照合手段
１３　電子メール作成受付手段

１４　電子メール暗号化手段
１５　暗号化鍵生成手段
１７　メール送信端末
１９　初期画面
２０　ログインボタン
２１　ＩＤ登録ボタン
２２　ログイン画面
２３　ログインＩＤ入力欄
２４　パスワード入力欄
２６　電子メール入力画面
２７　送信アドレス入力欄
２８　受信アドレス入力欄
２９　件名入力欄
３０　本文入力欄
３１　送信ボタン
３３　宛先（Ｔｏ）入力欄
３４　写し（Ｃｃ）入力欄
３５　秘写（Ｂｃｃ）入力欄
３７　メール受信端末

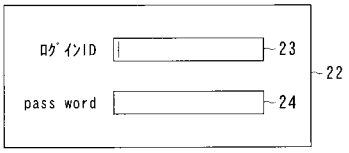
【図１】



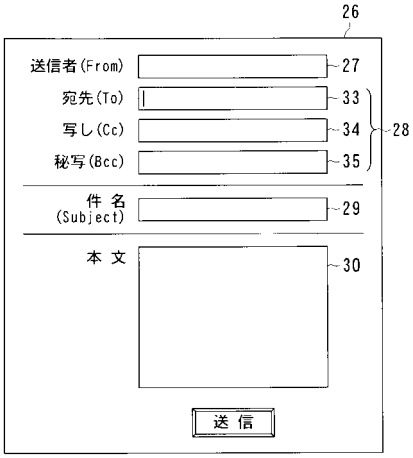

【図２】



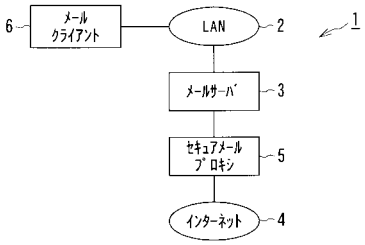

【図３】



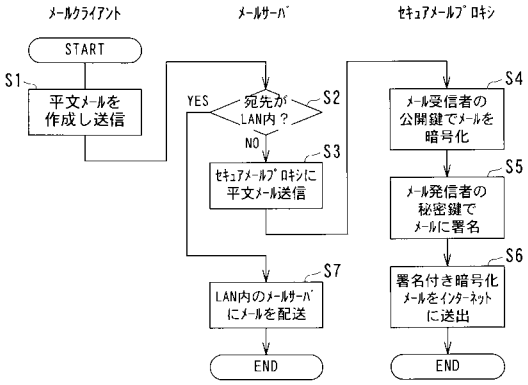

【図４】



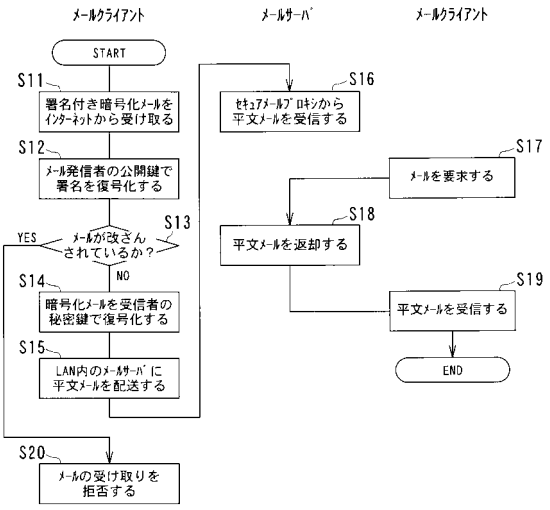
【図５】


6
メール
クライアント
LAN
2
1
メールサーバ
3
セキュアメール
プロキシ
5
インターネット
4

【図６】


メールクライアント
メールサーバ
セキュアメールプロキシ
START
S1
平文メールを
作成し送信
YES
宛先が
LAN内？
S2
NO
S3
セキュアメールプロキシに
平文メール送信
S7
LAN内のメールサーバ
にメールを配送
END
S4
メール受信者の
公開鍵でメールを
暗号化
S5
メール発信者の
秘密鍵で
メールに署名
S6
署名付き暗号化
メールをインターネット
に送出
END

【図７】


メールクライアント
メールサーバ
メールクライアント
START
S11
署名付き暗号化メールを
インターネットから受け取る
S12
メール発信者の公開鍵で
署名を復号化する
S13
YES
メールが改ざん
されているか？
NO
S14
暗号化メールを受信者の
秘密鍵で復号化する
S15
LAN内のメールサーバに
平文メールを配送する
S20
メールの受け取りを
拒否する
S16
セキュアメールプロキシから
平文メールを受信する
S17
メールを要求する
S18
平文メールを返却する
S19
平文メールを受信する
END

フロントページの続き

Ｆターム(参考) 5J104 AA16 AA34 BA02 EA01 EA04 EA15 EA16 JA03 JA21 MA05
NA02 PA08