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

特許第5229741号
(P5229741)

(45)発行日　平成25年7月3日(2013.7.3)　(24)登録日　平成25年3月29日(2013.3.29)

(51)Int.Cl.		F I		
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 13/00	(2006.01)	G06F	13/00	610S
G06F 21/62	(2013.01)	G06F	21/24	166E
H04L 9/08	(2006.01)	G06F	21/24	166A
		H04L	9/00	601C

請求項の数 8　(全 26 頁)

(21)出願番号　特願2009-139648 (P2009-139648)
(22)出願日　平成21年5月19日 (2009.5.19)
(65)公開番号　特開2010-273311 (P2010-273311A)
(43)公開日　平成22年12月2日 (2010.12.2)
審査請求日　平成23年5月26日 (2011.5.26)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　312000206
キヤノンＭＪアイティグループホールディングス株式会社
東京都品川区東品川２丁目４番１１号
(73)特許権者　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100126103
弁理士　伊藤　幹郎
(72)発明者　林　淑隆
東京都港区三田３丁目１１番２８号　キヤノンＩＴソリューションズ株式会社内
最終頁に続く

(54)【発明の名称】メール暗号複合制御装置及びその制御方法、プログラム

(57)【特許請求の範囲】
【請求項１】
スレッド管理される電子メールを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置であって、
前記電子メールを宛先に対して送信する送信手段と、
前記電子メールに対して返信された電子メールを受信する受信手段と、
新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、
前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化手段と、
前記送信手段で前記新規メールと前記共通鍵データとを送信し、前記受信手段で受信した当該新規メールを含むスレッドの電子メールに対する返信メールを生成する場合に、前記返信メールの作成元の電子メールである作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化手段と、
前記記憶装置に記憶された電子メールの中より、前記返信メールを含むスレッドに対応する電子メールを抽出する抽出手段と、
前記第２の暗号化手段で暗号化された返信メールを復号するための電子メールを持たないユーザを特定すべく、前記生成された返信メールに新規の宛先が追加されたかを判定する判定手段と、
他のメール暗号復号制御装置で備える前記第２の暗号化手段で暗号化され、前記受信手

段で受信した前記返信メールを含むスレッドに対応する電子メールのうち、当該返信メールの作成元メールから得られる共通鍵データを用いて、当該暗号化された返信メールを復号する復号手段と、

を備え、

前記送信手段は、前記判定手段で前記返信メールの宛先に新規の宛先が追加されたと判定された場合に、当該新規の宛先において、前記第２の暗号化手段で暗号化された返信メールを復号させるべく、前記抽出手段で抽出した電子メールを前記新規の宛先に送信することを特徴とするメール暗号復号制御装置。

【請求項２】

前記第２の暗号化手段で電子メールを暗号化する際に用いられる前記共通鍵データは、前記第２の暗号化手段で暗号化する返信メールの作成元メールに応じて、それぞれ異なることを特徴とする請求項１に記載のメール暗号復号制御装置。

【請求項３】

前記共通鍵データ生成手段は、前記第１の暗号化手段で前記スレッドの最初のメールである前記新規メールを暗号化する際に用いる共通鍵データであるルートメールを生成し、

前記第１の暗号化手段は、共通鍵データ生成手段で生成した前記ルートメールを用いて、前記新規メールを暗号化し、

前記送信手段は、前記共通鍵データ生成手段で生成した前記ルートメールと、前記第１の暗号化手段で前記ルートメールを用いて暗号化された新規メールと、を宛先に送信することを特徴とする請求項１又は２に記載のメール暗号復号制御装置。

【請求項４】

前記送信手段は、前記判定手段で、前記返信メールの宛先に新規の宛先が追加されたと判定された場合に、当該新規の宛先に対して、前記スレッドに含まれる全ての電子メールを転送することを特徴とする請求項１乃至３のいずれか１項に記載のメール暗号復号制御装置。

【請求項５】

前記判定手段で、前記生成された返信メールに新規の宛先が追加されたと判定された場合に、当該新規の宛先を含む電子メールを前記新規メールとして宛先に送信するかを判定する送信判定手段と、

を更に備え、

前記送信手段は、前記送信判定手段で前記新規メールとして宛先に送信すると判定した場合に、前記スレッドの電子メールを前記新規の宛先に送信することなく、前記共通鍵データ生成手段で生成した共通鍵データと前記第１暗号化手段で暗号化された当該新規メールとを当該新規の宛先に送信することを特徴とする請求項１乃至４のいずれか１項に記載のメール暗号複合制御装置。

【請求項６】

前記受信手段は、前記共通鍵データ生成手段で生成された前記共通鍵データを受信し、

前記抽出手段は、前記記憶装置に記憶された電子メールの中より、前記新規メールから、前記受信した暗号化メールの作成元メールである前記返信メールに至るまでの電子メールを特定して、前記スレッドより抽出することを特徴とし、

前記復号手段は、他のメール暗号復号制御装置で備える前記第１の暗号化手段で暗号化され、前記受信手段で受信した前記新規メールを、前記受信手段で受信した前記共通鍵データを用いて復号し、また、他のメール暗号復号制御装置で備える前記第２の暗号化手段で暗号化され、前記受信手段で受信した前記返信メールを、当該返信メールの作成元メールから得られる共通鍵データを用いて復号することを特徴とする請求項１乃至５のいずれか１項に記載のメール暗号復号制御装置。

【請求項７】

スレッド管理される電子メールを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置の制御方法であって、

送信手段が、前記電子メールを宛先に対して送信する送信工程と、

受信手段が、前記電子メールに対して返信された電子メールを受信する受信工程と、
生成手段が、新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成工程と、
第１の暗号化手段が、前記共通鍵データ生成工程で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化工程と、
第２の暗号化手段が、前記送信工程で前記新規メールと前記共通鍵データとを送信し、前記受信工程で受信した当該新規メールを含むスレッドの電子メールに対する返信メールを生成する場合に、前記返信メールの作成元の電子メールである作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化工程と、
抽出手段が、前記記憶装置に記憶された電子メールの中より、前記返信メールを含むスレッドに対応する電子メールを抽出する抽出工程と、
判定手段が、前記第２の暗号化工程で暗号化された返信メールを復号するための電子メールを持たないユーザを特定すべく、前記生成された返信メールに新規の宛先が追加されたかを判定する判定工程と、
復号手段が、他のメール暗号復号制御装置で備える前記第２の暗号化工程で暗号化され、前記受信工程で受信した前記返信メールを含むスレッドに対応する電子メールのうち、当該返信メールの作成元メールから得られる共通鍵データを用いて、当該暗号化された返信メールを復号する復号工程と、
を含み、
前記送信工程は、前記判定工程で前記返信メールの宛先に新規の宛先が追加されたと判定された場合に、当該新規の宛先において、前記第２の暗号化工程で暗号化された返信メールを復号させるべく、前記抽出工程で抽出した電子メールを前記新規の宛先に送信することを特徴とするメール暗号復号制御装置の制御方法。
【請求項８】
スレッド管理される電子メールを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置において実行可能なプログラムであって、
前記メール暗号復号制御装置を、
前記電子メールを宛先に対して送信する送信手段と、
前記電子メールに対して返信された電子メールを受信する受信手段と、
新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、
前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化手段と、
前記送信手段で前記新規メールと前記共通鍵データとを送信し、前記受信手段で受信した当該新規メールを含むスレッドの電子メールに対する返信メールを生成する場合に、前記返信メールの作成元の電子メールである作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化手段と、
前記記憶装置に記憶された電子メールの中より、前記返信メールを含むスレッドに対応する電子メールを抽出する抽出手段と、
前記第２の暗号化手段で暗号化された返信メールを復号するための電子メールを持たないユーザを特定すべく、前記生成された返信メールに新規の宛先が追加されたかを判定する判定手段と、
他のメール暗号復号制御装置で備える前記第２の暗号化手段で暗号化され、前記受信手段で受信した前記返信メールを含むスレッドに対応する電子メールのうち、当該返信メールの作成元メールから得られる共通鍵データを用いて、当該暗号化された返信メールを復号する復号手段として機能させ、
前記送信手段は、前記判定手段で前記返信メールの宛先に新規の宛先が追加されたと判定された場合に、当該新規の宛先において、前記第２の暗号化手段で暗号化された返信メールを復号させるべく、前記抽出手段で抽出した電子メールを前記新規の宛先に送信することを特徴とするメール暗号復号制御装置の制御プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メール暗号複合制御システムに関し、特に暗号化電子メールにおける制御技術に関するものである。
【背景技術】
【０００２】
近年のネットワーク技術の発達により、情報のやりとりにかかるコストが格段に低下する中、個人や各企業では電子メールやウェブサービスといったインターネットを利用した各種サービスを利用することにより、効率的な情報伝達ができるようになった。
【０００３】
２００５年の個人情報保護法の施行を始めとして、特に企業を始めとした組織では情報管理について厳格な対応を求められることになり、例えば、情報漏洩対策として、社外へ外部送信する電子メールの内容チェックを行うなど、組織が予め定めた基準に合致した場合のみ、外部への情報送信を許可するといった送信制御システムを導入することが一般的になっている。
【０００４】
しかしながら、このような送信制御システムを導入しても、誤送信を始めとした情報漏洩に関する事故は後を絶たないため、情報セキュリティおける多段防御の施策として、暗号化メールの利用を検討する組織もある。
【０００５】
現在、暗号化メールとして利用可能な技術として、Ｓ／ＭＩＭＥ、ＰＧＰ（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）や、送信経路上のみを暗号化通信する製品等が販売されている。今では企業におけるメールゲートウェイでのウィルスチェックは一般的であるが、暗号化メールはＥｎｄ－Ｔｏ－Ｅｎｄの仕組みであるため、このような暗号化メールのウィルスチェックは実施不可能である。このような場合、組織外から直接、組織内部へウィルスが送り込まれることが可能である。更に言えば、暗号化メールを利用することで、組織内から機密情報が送出されたかどうかの確認も不可能であることから、暗号化メールの積極的な利用には、懸念が生じている。
【０００６】
このような状況の下、パスワード保護されたＺＩＰアーカイブを添付ファイルに利用する人が多くなってきた。パスワード保護されたＺＩＰアーカイブを添付したメールを送信し、別メールにパスワードを記述して同じ宛先へ再び送信するという手法である。この手法では、
・別経路でパスワードを送付する等しない限り、盗聴される可能性が非常に高く、添付ファイルが保護できない
・利用者が注意深く２通目を送信しない限り、誤送信する可能性が非常に高い
という特徴があり、本質的に安全な手法とは言えない。しかしながら、組織の情報管理の観点から見れば、送受信される電子メールをすべて保存しておくことで、暗号化された添付ファイルも事後確認可能であることや、人的コストの増加で対策できることから、本質的に安全でなくても積極的に利用されている理由のひとつとされている。
また、コンテンツを暗号化して送信する手法として、特許文献１に開示されている手法では、予め受信して蓄積した複数コンテンツに組み込まれた複数鍵を使用してコンテンツの復号を実施する方法を開示している。
【先行技術文献】
【０００７】
【特許文献】
【特許文献】特開２００８－１６５４８６号公報
【発明の概要】
【発明が解決しようとする課題】

【０００８】
このように暗号化メールを利用するにあたって、情報保護（暗号化）と情報監視（内容監査）という、相反する要求があり、更には、公開鍵暗号方式における認証局のような鍵管理コスト（運用コスト）を可能な限り抑えたいという課題がある。
更に、スレッド単位で電子メールの改竄がされていないことの確かめることが困難であった（スレッド単位で電子メールの原本性を保証することが困難であった）。
即ち、暗号化メールシステムの運用コストを抑えつつ情報監視が可能であり、第三者への誤送信が発生しても容易に情報漏洩をさせない仕組みを提供することが困難であった。
更に、インターネットサービスプロバイダ（ＩＳＰ）などが提供している外部のネットワークに送信される電子メールの内容を、外部の者（ＩＳＰなど）に閲覧出来ないようにすることにより、情報漏洩を防止することが困難であった。
【０００９】
本発明の目的は、電子メールによる情報漏洩を防止しつつ、返信メールの宛先に追加されたユーザに、暗号化された電子メールを容易に確認させる仕組みを提供することである。
【課題を解決するための手段】
【００１０】
本発明の暗号復号制御装置は、スレッド管理される電子メールを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置であって、前記電子メールを宛先に対して送信する送信手段と、前記電子メールに対して返信された電子メールを受信する受信手段と、新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化手段と、前記送信手段で前記新規メールと前記共通鍵データとを送信し、前記受信手段で受信した当該新規メールを含むスレッドの電子メールに対する返信メールを生成する場合に、前記返信メールの作成元の電子メールである作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化手段と、前記記憶装置に記憶された電子メールの中より、前記返信メールを含むスレッドに対応する電子メールを抽出する抽出手段と、前記第２の暗号化手段で暗号化された返信メールを復号するための電子メールを持たないユーザを特定すべく、前記生成された返信メールに新規の宛先が追加されたかを判定する判定手段と、他のメール暗号復号制御装置で備える前記第２の暗号化手段で暗号化され、前記受信手段で受信した前記返信メールを含むスレッドに対応する電子メールのうち、当該返信メールの作成元メールから得られる共通鍵データを用いて、当該暗号化された返信メールを復号する復号手段と、を備え、前記送信手段は、前記判定手段で前記返信メールの宛先に新規の宛先が追加されたと判定された場合に、当該新規の宛先において、前記第２の暗号化手段で暗号化された返信メールを復号させるべく、前記抽出手段で抽出した電子メールを前記新規の宛先に送信することを特徴とする。
【発明の効果】
【００１１】
本発明によれば、電子メールによる情報漏洩を防止しつつ、返信メールの宛先に追加されたユーザに、暗号化された電子メールを容易に確認させることができる。
【図面の簡単な説明】
【００１２】
【図１】本発明の実施形態に係るシステムの構成例を示す模式図である。
【図２】本発明の実施形態の暗号化メール送信装置１００のハードウェア構成を示す図である。
【図３】本発明の実施形態のメールサマリの一例を示す図である。
【図４】本発明の実施形態の暗号化メールスレッドの構成例を示す図である。
【図５】本発明の実施形態の転送処理を含む暗号化メールスレッドの構成例を示す図である。

【図６】本発明の実施形態の暗号化メールの新規作成を示すフローチャートである。
【図７】本発明の実施形態のルール管理部１０５の一例である。
【図８】本発明の実施形態のメール暗号化処理を示すフローチャートである。
【図９】本発明の実施形態のメール受信処理を示すフローチャートである。
【図１０】本発明の実施形態のルートメール受信処理を示すフローチャートである。
【図１１】本発明の実施形態の関連メール移動処理を示すフローチャートである。
【図１２】本発明の実施形態の暗号化メール受信処理を示すフローチャートである。
【図１３】本発明の実施形態の親メール検索処理を示すフローチャートである。
【図１４】本発明の実施形態の検索条件選定処理を示すフローチャートである。
【図１５】本発明の実施形態の暗号化メールの返信処理を示すフローチャートである。
【図１６】本発明の実施形態の暗号化メールの復号処理を示すフローチャートである。
【図１７】本発明の実施形態の暗号化メールスレッドにおける全親スレッドの受信処理を示すフローチャートである。
【図１８】本発明の実施形態の暗号化メールの転送処理を示すフローチャートである。
【図１９】本発明の実施形態のルートメール情報の一例を示す図である。
【図２０】本発明の実施形態のルートメール情報の実施例を示す図である。
【図２１】本発明の実施形態のメールスレッドの実施例を示す図である。
【図２２】本発明の実施形態の暗号化メールスレッドの実施例を示す図である。
【図２３】本発明の実施形態の親メール検索条件選定処理を示すフローチャートである。
【発明を実施するための形態】
【００１３】
以下、添付図面を参照して、本発明を好適な実施形態に従って詳細に説明する。
【００１４】
図１は、本発明の一実施形態を示す電子メール管理装置について、システムの構成例を示す模式図である。
【００１５】
図１において、１００は暗号化メール送信装置を表し、暗号化メールを送信する機能を示した模式図である。１１０は暗号化メール受信装置を表し、暗号化メールを受信する機能を示した模式図である。広域ネットワーク網１２０は、インターネットを始めとするネットワークである。
【００１６】
暗号化メール送信装置１００は、メール入力部１０１と、メール本文変更部１０２と、スレッド検索部１０３と、スレッド暗号部１０４と、ルール管理部１０５と、送信部１０６と、メール保存部１０７と、ルートメール作成部１０８とを備える。
【００１７】
メール入力部１０１は、暗号化メール送信装置１００にデータを入力するものであり、キーボードやマウスといった入力装置である。メール入力部１０１で入力されたメールは、メール本文変更部１０２で暗号化された本文に変更され、送信部１０６で暗号化メールとして送信される。なお、メール本文変更部１０２で変更されるメール本文は、スレッド暗号部１０４に送られ、スレッド検索部１０３がメール保存部１０７から検索した電子メールスレッドもしくはルートメール作成部１０８で作成したルートメールに基づいて暗号化される。これら一連のメールスレッド暗号化処理の詳細については、後述する。
【００１８】
暗号化メール受信装置１１０は、受信部１１１と、ルール管理部１１２と、スレッド復号部１１３と、スレッド検索部１１４と、メール保存部１１５と、表示部１１６とを備える。
【００１９】
受信部１１１で受信した暗号化メールはメール保存部１１５へ保存される。利用者が当該暗号化メールの閲覧を所望した場合は、その命令を受けたスレッド復号部１１３がスレッド検索部１１４を介してメール保存部１１５より当該暗号化メールを含む電子メールス

レッドを検索し、スレッド復号処理を実施した上で、表示部１１６に表示する。これら一連のスレッド復号処理の詳細については、後述する。

【００２０】

なお、スレッド検索部１０３とスレッド検索部１１４、及びルール管理部１０５とルール管理部１１２、及びメール保存部１０７とメール保存部１１５は同一機能である。

また、図１は、説明を分かりやすくするために、暗号化メール送信装置１００と暗号化メール受信装置１１０とに分けて説明したが、暗号化メール送信装置１００に示す機能及び構成は、暗号化メール受信装置１１０にも有しており、更に、暗号化メール受信装置１１０に示す機能及び構成は、暗号化メール送信装置１００にも有している。したがって、暗号化メール送信装置１００と暗号化メール受信装置１１０は、相互に暗号化メールを送受信することが可能である。

【００２１】

図２は、暗号化メール送信装置１００（メール暗号複合制御装置）及び暗号化メール受信装置１１０（メール暗号複合制御装置）のハードウェア構成を示すブロック図である。

【００２２】

図２において、２０１はＣＰＵで、ＲＡＭ２０２やＲＯＭ２０４に格納されているプログラムやデータを用いて暗号化メール送信装置１００全体の制御を行うと共に、暗号化メール送信装置１００が行う後述の各処理を実施する。

【００２３】

ＲＡＭ２０２は、ＨＤＤ（ハードディスクドライブ）２０４や記憶媒体ドライブ２０６からロードされたプログラムやデータ、ネットワークＩ／Ｆ（インターフェース）２０５を介して外部から受信したプログラムやデータなどを一時的に記憶するためのエリアや、ＣＰＵ２０１が各種の処理を実行する際に用いるワークエリアなど、各種のエリアを適宜提供することができる。

【００２４】

ＲＯＭ２０３は、暗号化メール送信装置１００の設定データや、ブートプログラムなどを格納する。

【００２５】

ＨＤＤ２０４は、ＯＳ（オペレーティングシステム）や、暗号化メール送信装置１００が行う後述の各処理をＣＰＵ２０１に実行させるためのプログラムやデータなどを保存するためのものであり、これらはＣＰＵ２０１による制御に従って適宜ＲＡＭ２０２にロードされ、ＣＰＵ２０１による処理対象となる。

【００２６】

ネットワークＩ／Ｆ２０５は、暗号化メール送信装置１００を広域ネットワーク網１２０に接続するためのものであり、暗号化メール送信装置１００はこのネットワークＩ／Ｆ２０５を介して、広域ネットワーク網１２０に接続されている各装置とのデータ通信を行うことができる。

【００２７】

記憶媒体ドライブ２０６は、ＣＤ－ＲＯＭ、ＣＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記憶媒体に記録されているプログラムやデータを読み出し、ＲＡＭ２０２やＨＤＤ２０４に出力する。なお、ＲＡＭ２０２やＨＤＤ２０４が保持している情報のうち一部をこの記憶媒体に記録させておいてもよい。

【００２８】

キーボード２０７、及びマウスやジョイスティック等により構成されているポインティングデバイス２０８は、暗号化メール送信装置１００の操作者が操作することで、各種の指示をＣＰＵ２０１に対して入力することができる。

【００２９】

表示部２０９は、ＣＲＴや液晶画面等により構成されており、ＣＰＵ２０１による処理結果を画像や文字等をもって表示することができる。

【００３０】

外部機器接続Ｉ／Ｆ２１０は、周辺機器を暗号化メール送信装置１００に接続させるためのインターフェースである。暗号化メール送信装置１００は、この外部機器接続Ｉ／Ｆ２１０を介して、この周辺機器とのデータ送受信を行う。外部機器接続Ｉ／Ｆ２１０は、ＵＳＢやＩＥＥＥ１３９４等により構成されており、通常複数の外部機器接続Ｉ／Ｆを有する。周辺機器との接続形態は有線／無線を問わない。

【００３１】

バス２１１は上述の各部をつなぐものである。

【００３２】

なお、暗号化メール送信装置１００のハードウェア構成は図２に示した構成を有するとして説明するが、必ずしも同図の構成を有することに限定するものではなく、暗号化メール送信装置１００が行う処理として説明する以下の処理が実行可能な構成であれば、暗号化メール送信装置１００の構成は適宜変形してもよい。

【００３３】

また、暗号化メール受信装置１１０のハードウェア構成については、これらには一般のコンピュータを適用するので、周知の如く、概ね図２に示した構成を有する。更には、暗号化メール送信装置１００及び暗号化メール受信装置１１０は同一のハードウェア上で構成してもよい。

【００３４】

次に、メールスレッドについて図３及び図２１を用いて説明する。

【００３５】

図３はメールサマリの一例を示す図である。メールサマリ３００は利用者のクライアント端末装置に保存されているメールの一部を表示したものである。また、ひとつの話題について差出人及びメール受信者の間でやりとりされた複数のメールを時系列に並べたものを、メールスレッドと呼ぶ。

【００３６】

メールサマリ３００において、メール３０１を基点としたメール３０２、メール３０３、メール３０４及びメール３０５が第一のメールスレッドを構成している。メール３０２、メール３０３、メール３０４及びメール３０５はすべて直前のメールへの返信処理であることを示している。

【００３７】

また、メール３０６を基点としてメール３０７及びメール３０８は第二のメールスレッドを構成している。なお、メール３０８については、メール３０７の返信処理ではなく、メール３０６を差出人ｈａｙａｓｈｉが宛先ｕｍｅｄａへ転送したことを示している。

【００３８】

このように、複数メールからなるメールスレッドの構成を判断する第一の手法として、ＲＦＣ（Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ）２８２２に記述されている、Ｍｅｓｓａｇｅ－ＩＤ、Ｉｎ－Ｒｅｐｌｙ－ＴｏもしくはＲｅｆｅｒｅｎｃｅの各ヘッダ情報を参照する手法がある。

【００３９】

第一の手法について、図２１を用いて詳しく説明する。メール２１０１は電子メールの一例であり、ＲＦＣ２８２２に記述されているように、メール２１０１が唯一のものであると識別するために、Ｍｅｓｓａｇｅ－ＩＤヘッダ２１０２を有している。また、メール２１０３は電子メールを返信した場合の一例であり、メール２１０１に対する返信処理を実施したものである。

【００４０】

ＲＦＣ２８２２に記述されているように、返信処理において返信元となるメールの識別情報をＩｎ－Ｒｅｐｌｙ－Ｔｏヘッダに記載するべきであるとされており、メール２１０３において、Ｉｎ－Ｒｅｐｌｙ－Ｔｏヘッダ２１０４が付与されており、その値としてメール２１０１のＭｅｓｓａｇｅ－ＩＤヘッダ２１０２の値が記載されている。

【００４１】

メール２１０１を送信しメール２１０３を受信した差出人のクライアント端末装置では、これらのヘッダ情報を参照することで、メール２１０１の返信がメール２１０３であるとわかることから、メール２１０１とメール２１０３がメールスレッドを構成すると判断することができる。

【００４２】

同様に、メール２１０６においても、Ｉｎ－Ｒｅｐｌｙ－Ｔｏヘッダ２１０８の値は、メール２１０３のＭｅｓｓａｇｅ－ＩＤヘッダ２１０５の値となっている。従って、メール２１０６も前記メールスレッドを構成するメールの一部であると判断できる。

【００４３】

メールスレッドを構成するメールであると判断する第二の手法として、任意につけられたタグと呼ばれるものを使用する手法がある。タグは、クライアント端末利用者が任意に付与することもあれば、電子メールシステムで自動的に付与する場合もある。システムで自動化する場合は、例えば、複数の差出人をグループ化したものを利用する場合や、ある特定のヘッダ情報が同一のものに対して付与する場合がある。

【００４４】

メールスレッドの構成を判断する第三の手法として、件名が同じものを集めるという手法がある。返信メールや転送メールの場合、基になるメールの件名に返信を表す「Ｒｅ：」や、転送を表す「Ｆｗ：」といった形式的な文字列を付与する。従って、このような文字列を除いた件名を持つ同一のメールがメールスレッドを構成すると判断する手法である。

【００４５】

なお、前記第二及び前記第三の手法では、条件に該当する複数通のメールが検出されるため、時間順で並べるために各メールにおける送信時刻が参照される。

【００４６】

以上、メールスレッドの構成判断手法について説明したが、以降の例では第一の手法（ＲＦＣ２８２２）を主体として説明する。

【００４７】

次に、メールスレッド構造を利用したメールスレッド暗号化の概要について、図４及び図５を用いて説明する。

【００４８】

図３におけるメール３０１を基点とした第一のメールスレッドが暗号化メールスレッドである場合の構成例の一部を、図４に示す。暗号化メール構造４０２はメール３０１に相当し、暗号化メール構造４０５はメール３０２に相当する。このとき、メール本文部は暗号化された状態（４０３及び４０６）にある。

【００４９】

メールスレッド暗号化方式における復号処理は、当該メールの親メールの本文部を共通鍵ファイルとして使用する特徴を持つ。従って、暗号化本文４０６の復号鍵は、親メールにあたる暗号化メール構造４０２の暗号化本文４０３を復号したメール本文４０４である。即ち、メール本文４０４を共通鍵ファイルとして暗号化本文４０６を復号し、メール本文４０７を得る。

【００５０】

このとき、共通鍵ファイルであるメール本文４０４を得るためには、暗号化本文４０３を復号しなければならない。この復号鍵となるのがルートメール構造４００のルートメール本文４０１である。ルートメールの詳細については、後述する。

【００５１】

図３におけるメール３０３を基点とした第二のメールスレッドが暗号化メールスレッドである場合の構成例の一部を、図５に示す。暗号化メール構造５０２はメール３０６に相当し、暗号化メール構造５０５はメール３０７に相当し、暗号化メール構造５０８はメール３０８に相当する。暗号化メール構造５０８は暗号化メール構造５０２と転送処理関係にある。従って、暗号化メール構造５０８の暗号化本文５０９を復号する共通鍵ファイル

は、暗号化メール構造５０２の復号したメール本文５０４であり、暗号化メール構造５０５の暗号化本文５０６を復号する共通鍵ファイルと同一である。

【００５２】

このようにメールスレッド暗号化方式では、暗号化された本文部を復号するために親メールを連鎖的に復号していく必要がある。従って、ルートメールを含むメールスレッドを構成するすべてのメールを所持していない限り、暗号化本文を復号できない構造を特徴としている。

【００５３】

次に、メールスレッド暗号化方式において、メールを新規作成する場合の手順について、図１、図６、図７、図８を用いて説明する。

【００５４】

図６に暗号化メールを新規作成する場合のフローを示す。ステップＳ６０１において、利用者が図１におけるメール入力部１０１を操作することにより、新規メールを作成する。新規作成したメールを第一メールと呼び、この時点で第一メールは暗号化されていない。

【００５５】

続いて、ステップＳ６０２において、第一メールが暗号化の対象であるかどうかを確認する。即ち、図１においてメール本文変更部１０２へ送られた第一メールに対して、ルール管理部１０５が動作ルールを参照する。

【００５６】

図７に、動作ルール７００の一例を示す。動作ルールとは、作成されたメールの内容や宛先などの各種条件に応じて、システムがどのような動作を行うかを記述した管理テーブルである。例えば、動作ルール７０１は「宛先が組織外を含む場合は暗号化する」を示し、動作ルール７０２は、「キーワード検査の結果に“社外秘”を含む場合は暗号化する」を示し、動作ルール７０３は「添付ファイルがある場合は暗号化する」を示す。

【００５７】

図６に戻って、ステップＳ６０２で「いいえ」の場合、即ち、暗号化対象外のメールであると判断した場合は、ステップＳ６１０において第一メールは非暗号化状態のまま送信部１０６へ送られ、送信処理を完了する。続くステップＳ６０９において、第一メールは非暗号化状態のままメール保存部１０７に保存される。

【００５８】

第一メールが暗号化対象であると判断した場合（ステップＳ６０２で「はい」の場合）、ステップＳ６０３へ進み、当該第一メールを作成した利用者に新規スレッド作成許可があるかどうかをルール管理部１０５で参照する。例えば、図７における動作ルール７０４は「利用者ｈａｙａｓｈｉ及びｔａｎａｋａには新規作成許可がある」ことを示している。当該利用者に新規スレッド作成許可がない場合（ステップＳ６０３で「いいえ」の場合）は、その旨を当該利用者に通知し、処理を停止する。

【００５９】

当該利用者に新規スレッド作成許可がある場合（ステップＳ６０３で「はい」の場合）、ステップＳ６０４に進み、ルートメール作成部１０８においてルートメールを作成する。ルートメールとは、前記暗号化メール構造４００及び前記暗号化メール構造５００に示したように暗号化メールスレッドの基点となる特殊なメールであり、第一メールの本文部の暗号／復号処理の共通鍵ファイルとなるメールである。ルートメールの詳細については、後述する。

【００６０】

ステップＳ６０４で作成されたルートメールを共通鍵ファイルとして、ステップＳ６０５において、第一メールの暗号化処理を実施する。ここで、図８を用いて暗号化処理について説明する。

【００６１】

図８のステップＳ８０１において、前記第一メールの暗号化対象となるメール本文を抽

出する。続いて、ステップＳ８０２において、前記ルートメールを共通鍵ファイルとして抽出したメール本文を暗号化する。このとき、ルートメールの作成時にパスフレーズの利用を指定することで、パスフレーズを利用者が入力し、暗号化強度を向上することもできる。パスフレーズを始めとしたルートメールの詳細については、後述する。

【００６２】

続くステップＳ８０３において、暗号化されたメール本文はメールサーバーで処理できるようにテキスト文字列に変換され、前記第一メールの本文と差替えられる。また、第一メールのヘッダ部には、前記ルートメールから連鎖していることを示すために、ＲＦＣ２８２２に基づいたＩｎ－Ｒｅｐｌｙ－Ｔｏ（もしくはＲｅｆｅｒｅｎｃｅヘッダ）が付与される。このとき、前記ルートメールに付与したＭｅｓｓａｇｅ－ＩＤの識別子がヘッダ値として付与される。これらルートメールを基点とした連鎖関係の詳細については、後述する。

【００６３】

図６に戻って、ステップＳ６０６で前記ルートメールは送信部１０６より送信される。続いて、ステップＳ６０７で暗号化された第一メールが送信部１０６より送信される。送信完了後、ステップＳ６０８において、前記ルートメールはメール保存部１０７に保存され、続くステップＳ６０９において、前記暗号化第一メールもメール保存部１０７へ保存され、新規作成処理を終了する。

【００６４】

ここで、ステップＳ６０４で作成するルートメールについて説明する。

【００６５】

前述のように、ルートメールは暗号化メールスレッドの基点となるものであり、第一メールの作成時等において自動的に作成されるものである。ルートメール作成時において当該ルートメールには、以下の何れか一つ以上の情報が記載される。

（１）メール識別子に関する情報

（２）暗号化用の補助情報

（３）メールスレッド管理方法に関する情報

（４）第一メールの送信情報を証明する情報

このようなルートメール情報について、図１９を用いて詳しく説明し、図２０に実施例を示す。

【００６６】

図１９におけるルートメール情報１９００は、ルートメールに記載されるルートメール情報の一例を示している。ルートメール識別子１９０１、第一メール識別子１９０２はメール識別子に関する情報である。ルートメール識別子１９０１は当該ルートメールを唯一のものであると判断するための任意の文字列情報であり、前記ＲＦＣ２８２２のＭｅｓｓａｇｅ－ＩＤに相当する。また、第一メール識別子１９０２は、例えば、図６におけるステップＳ６０１で作成した前記第一メールのＭｅｓｓａｇｅ－ＩＤを示す。

【００６７】

図２０において、ルートメール２０００はルートメールの実施例を示す。ヘッダ情報２００１（Ｍｅｓｓａｇｅ－ＩＤ）が前記ルートメール識別子１９０１の実施例であり、ヘッダ情報２００２（Ｘ－ＣｒｙｐｔＴｈｒｅａｄ－Ｍａｉｌ）が前記第一メール識別子１９０２の実施例である。

【００６８】

暗号化補助文字列１９０３は、ルートメール自体を共通鍵ファイルとするときの暗号強度を強化させるために、ランダムな文字列を予め記載しておくものである。図２０において、暗号化補助文字列２００３が前記暗号化補助文字列１９０３の実施例である。暗号化補助文字列２００３は、メール本文領域に記述される。

【００６９】

ルートメール識別子１９０１、第一メール識別子１９０２、及び暗号化補助文字列１９０３はルートメール情報として必須項目である。

【００７０】
メールスレッド管理情報として、公開範囲１９０４、失効時間１９０５、及びパスフレーズ１９０６がある。これらの情報は、前記第一メールを基点としたメールスレッドの管理に関する情報であり、任意項目である。公開範囲１９０４は、予め指定した範囲外へのメール送信を制限するものである。後述する暗号化メールスレッドからの返信や転送処理において利用される。失効時間１９０５は、暗号化メールスレッドの失効時間を指定するものである。
【００７１】
パスフレーズ１９０６は、メールの暗号化及び復号処理において、利用者にパスフレーズの入力を強要するものである。例えば、前記ステップＳ８０２のメール本文の暗号化処理において、当該暗号化メールスレッドのルートメールにパスフレーズの記載がある場合、パスフレーズの入力が強要され、入力したパスフレーズとルートメールに記載されたパスフレーズが一致しないと、暗号化処理に失敗することとなる。なお、パスフレーズ１９０６には、入力すべきパスフレーズがそのまま記載されるのではなく、例えば、ＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）を始めとしたハッシュ関数の値を記載しておき、入力されたパスフレーズのハッシュ値と比較する方式が望ましい。
【００７２】
第一メールの送信情報を証明する情報として、証明書１９０７及び送信時刻１９０８がある。証明書１９０７は第一メールの送信者を証明するものであり、送信時刻１９０８は、第一メールの送信時刻を証明する情報（タイムスタンプ）を示す。これらの証明情報は、前述のように管理コストの増大を招くため、暗号化システムの安全性や信頼性とのバランスを考慮して利用できるよう、任意項目である。
【００７３】
図２０において、領域２００４に前記メールスレッド管理情報及び前記証明書に関する情報の実施例である。領域２００４はメール本文であり、前記暗号化補助文字列２００３と空行を挟んで区別される。図２０の実施例では、公開範囲を＊@ｅｘａｍｐｌｅ．ｃｏ．ｊｐに制限し、パスフレーズを有効にし、失効時間や送信者証明及び送信時刻証明は設定されていない。即ち、ルートメール２０００を基点とする暗号化メールスレッドは、暗号／復号処理に際してパスフレーズの入力が必要であり、且つｅｘａｍｐｌｅ．ｃｏ．ｊｐドメイン以外への送信ができない、という管理がなされている。
【００７４】
ここで、ルートメール２０００を基点とする暗号化メールスレッドの例を、図２２に示す。メール２２０１はルートメール２０００である。メール２２０１にはメール識別子であるヘッダ情報２２０２（Ｍｅｓｓａｇｅ－ＩＤ）が付与されている。メール２２０１はルートメールであるため、第一メール識別子を示すヘッダ情報２２０３が付与されており、その値はメール２２０４のメール識別子であるヘッダ情報２２０５の値と同一である。
【００７５】
さらに、メール２２０４はルートメール２２０１を基点としたメールスレッドを示すためのヘッダ情報２２０６（Ｉｎ－ｒｅｐｌｙ－ｔｏ）を持つ。ヘッダ情報２２０６の値は、ルートメール識別子２２０２の値と同一である。以下、同様にして、メール２２０７、メール２２０８と暗号化メールスレッドを構成している。
【００７６】
また、ヘッダ情報２２０９（Ｃｏｎｔｅｎｔ－ｔｙｐｅ）は、その値がａｐｐｌｉｃａｔｉｏｎ／ｘ－ｃｒｙｐｔｔｈｒｅａｄ－ｍａｉｌである場合、暗号化メールスレッドを構成する暗号化メールであることを示すものである。
【００７７】
次に、図１における暗号化メール受信装置１１０における暗号化メール受信の処理について、図９～図１４、及び図２３を用いて説明する。
【００７８】
暗号化メールの新規作成において（図６）、ステップＳ６０６でルートメールを、ステ

ップＳ６０７で暗号化された第一メールを送信している。このように、本システムでは複数の種類のメールを送信するため、暗号化メール受信装置１１０における受信部１１１では、受信したメールの種類によって処理をわける必要がある。図９にメール受信処理を示す。

【００７９】

ステップＳ９０１で受信したメールがルートメールかどうかを判断する。判断基準には、例えば、図２２におけるルートメール識別子２２０３があるか否かで判断することができる。ルートメールと判断した場合は（ステップＳ９０１で「はい」の場合）、ステップＳ９０２へ進み、ルートメール受信処理を行う。

【００８０】

ルートメール受信処理を、図１０に示す。ステップＳ１００１において、利用者にルートメール受信許可があるかどうか、ルール管理部１１２の動作ルールで判断する。図７で例示した動作ルール７００において、動作ルール７０５がルートメール受信許可に関するものである。動作ルール７０５の例示では、利用者ｈａｙａｓｈｉとｔａｎａｋａにルートメール受信許可が与えられている。

【００８１】

ルートメール受信許可がある場合（ステップＳ１００１で「はい」の場合）、ステップＳ１００２へ進み、受信したルートメールをメール保存部１１５に保存する。続くステップＳ１００３で検索するメール（検索メール）をルートメールに設定し、ステップＳ１００４で関連メール移動処理を実施する。

【００８２】

関連メール移動処理とは、電子メールの遅延配送を考慮した処理である。電子メールは送信順に受信が保証されるシステムではない。例えば、図６における暗号化メールの新規作成において、ルートメールと第一メールを送信したとき、先に第一メールを受信する場合がある。このとき、第一メールの基点となるルートメールが存在しないため、暗号化メールスレッドを構成することができない。このような状況でルートメールを受信したときの処理となる。

【００８３】

図１１に関連メール移動処理を、図１４に検索条件選定処理を示す。

ステップＳ１４０１で「いいえ」と判定されるのは、ＷＥＢメールの場合である。また、ＳＭＴＰで送受信するメールは、ステップＳ１４０１で「はい」と判定される。即ち、ＷＥＢメールは、一般にＭｅｓｓａｇｅ－ＩＤを有していないためである。したがって、ＷＥＢメールの場合は、ステップＳ１４０４又はＳ１４０５の処理が実行されることとなる。後述する図２３もこれと同様である。すなわち、Ｓ２３０１で「いいえ」と判定されるのは、ＷＥＢメールの場合である。また、ＳＭＴＰで送受信するメールは、ステップＳ２３０１で「はい」と判定される。

【００８４】

ステップＳ１１０１において、検索条件を選定する。図１４に移って、ステップＳ１４０１において、検索メールに設定したメールにＭｅｓｓａｇｅ－ＩＤヘッダ情報が存在しているかを確認する。ここでは、図１０におけるステップＳ１００３で検索メールにルートメールを設定しているためルートメール識別子が存在し、ステップＳ１４０２へ進み、検索キーにＭｅｓｓａｇｅ－ＩＤ値、検索範囲を「なし」にする。検索範囲を指定しないのは、Ｍｅｓｓａｇｅ－ＩＤのみでメールを一意に特定できるためである。

【００８５】

ステップＳ１４０１で「いいえ」の場合、即ち、Ｍｅｓｓａｇｅ－ＩＤヘッダ情報が存在しない場合、ステップＳ１４０３に進む。ステップＳ１４０３では、検索メールにタグが付与されているかどうかを確認する。タグが付与されている場合（ステップＳ１４０３で「はい」の場合）は、ステップＳ１４０４に進み、検索キーにタグ値、検索範囲を「時刻（未来）」とする。時刻（未来）とは、検索メールが送信された時刻より未来の時刻を示すものである。関連メール移動処理の目的は、遅延配送された検索メールよりも前に受

信した検索メールを基点としたメールを検出することにある。即ち、本来ならば検索メールより後に受信すべきメールを先に受信していないかを確認することである。

【００８６】

ステップＳ１４０３でタグが付与されていない場合（「いいえ」の場合）は、ステップＳ１４０５に進み、検索キーに件名、検索範囲を「時刻（未来）」とする。なお、以降では検索キーにＭｅｓｓａｇｅ－ＩＤ値を設定した場合を例示して説明する。

【００８７】

図１１に戻って、ステップＳ１１０２において、設定した検索キー（Ｍｅｓｓａｇｅ－ＩＤ値）をＩｎ－ｒｅｐｌｙ－ｔｏヘッダ情報に持つメールを一時保存領域から検索する。一時保存領域とは、前記第一メールのように遅延配送された基点を持たないメールを一時的に保存しておく領域である。検索キーがＭｅｓｓａｇｅ－ＩＤ値であるので、検索結果は一意に決まる。

【００８８】

検索結果があった場合（ステップＳ１１０３で「はい」の場合）、ステップＳ１１０４へ進み、検索メールを検索結果メールに設定し、検索結果メールは一時保存から通常の保存領域へ移動する（ステップＳ１１０５）。その後、ステップＳ１１０１へ戻り、再度、一時保存のメール検索（検索結果で見つかったメールを親とするメールを検索）を実施する。即ち、これら一連の処理は、一時保存されているメールから暗号化メールスレッドを構成するすべてのメールを検索するための処理である。すべてのメールを検索すると（ステップＳ１１０３で「いいえ」の場合）、関連メール移動処理を終了する。

【００８９】

図１０に戻って、ステップＳ１００４で関連メール移動処理を実施すると、

・ルートメール　→　第一メールの順で受信した場合は、ルートメールのみ

・第一メール　→　ルートメールの順で受信した場合は、ルートメールと第一メールがメール保存部１１５に保存される。なお、第一メールを先に受信した場合の処理については、後述する。

【００９０】

ルートメール受信許可がない場合（ステップＳ１００１で「いいえ」の場合）、受信したルートメールを基点とする暗号化メールスレッドを受信することができないため、差出人へ通知を行うかどうかを判断する（ステップＳ１００５）。図７で例示した動作ルール７００において、動作ルール７０６が差出人通知に関するものである。動作ルール７０６の例示では、利用者ｈａｙａｓｈｉ、ｔａｎａｋａ、ｕｍｅｄａに差出人通知許可が与えられている。

【００９１】

差出人通知許可がある場合（ステップＳ１００５で「はい」の場合）、差出人通知を行う（ステップＳ１００６）。この場合は、ルートメールの受信ができない旨を通知する。差出人通知が許可されていない場合（ステップＳ１００５で「いいえ」の場合）は、ステップＳ１００６をスキップする。

【００９２】

続いて、受信できないルートメールを基点とする暗号化メールスレッドを構成するメールが一時保存されていた場合、これらをすべて消去する。ステップＳ１００７で検索メールにルートメールを設定し、図１１における関連メール移動処理と同様に、一時保存からメールを検索し、消去する（ステップＳ１００８～Ｓ１００１）。関連するすべてのメールを検索・削除した後（ステップＳ１００９で「いいえ」の場合）、受信拒否としてルートメール受信処理を終了する。

なお、ステップＳ１００７からＳ１０１１までの処理は、定期的に実行してもよい。

【００９３】

図９に戻って、ステップＳ９０１でルートメールでないと判断した場合（「いいえ」の場合）、暗号化メールであるかどうかを判断する（ステップＳ９０３）。判断基準には、前記ヘッダ情報２２０９（Ｃｏｎｔｅｎｔ－ｔｙｐｅ）の値が、ａｐｐｌｉｃａｔｉｏｎ

／ｘ－ｃｒｙｐｔｔｈｒｅａｄ－ｍａｉｌであるか否かで判断することができる。暗号化メールであると判断した場合は（ステップＳ９０３で「はい」の場合）、ステップＳ９０４へ進み、暗号化メール受信処理を行う。

【００９４】

暗号化メール受信処理を、図１２に示す。受信した暗号化メールは、暗号化メールスレッドを構成するための親メールを特定する必要がある。ステップＳ１２０１において、検索メールに受信した暗号化メールを設定し、ステップＳ１２０２において親メールの検索を実施する。

【００９５】

図１３に親メール検索処理を、図２３に親メール検索条件選定処理を示す。

【００９６】

ステップＳ１３０１において、親メールの検索条件を選定する。図２３に移って、ステップＳ２３０１において、検索メールに設定した暗号化メールにＩｎ－ｒｅｐｌｙ－ｔｏヘッダ情報が存在しているか確認する。例えば、図２２における暗号化メール２２０４にはヘッダ情報２２０６（Ｉｎ－ｒｅｐｌｙ－ｔｏ）が存在する。従って、ステップＳ２３０２へ進み、検索キーにＩｎ－ｒｅｐｌｙ－ｔｏ値、検索範囲を「なし」にする。検索範囲を指定しないのは、Ｉｎ－ｒｅｐｌｙ－ｔｏ値であるＭｅｓｓａｇｅ－ＩＤのみでメールを一意に特定できるためである。

【００９７】

ステップＳ２３０１で「いいえ」の場合、即ち、Ｉｎ－ｒｅｐｌｙ－ｔｏヘッダ情報が存在しない場合、ステップＳ２３０３に進む。ステップＳ２３０３では、検索メールにタグが付与されているかどうかを確認する。タグが付与されている場合（ステップＳ２３０３で「はい」の場合）は、ステップＳ２３０４に進み、検索キーにタグ値、検索範囲を「時刻（過去）」とする。時刻（過去）とは、検索メールが送信された時刻より過去の時刻を示すものである。親メール検索処理では、検索メールよりも未来のメールを検索対象とする必要はない。

【００９８】

ステップＳ２３０３でタグが付与されていない場合（「いいえ」の場合）は、ステップＳ２３０５に進み、検索キーに件名、検索範囲を「時刻（過去）」とする。なお、以降ではステップＳ２３０２で検索キーにＩｎ－ｒｅｐｌｙ－ｔｏ値を設定した場合を例示して説明する。

【００９９】

図１３に戻って、ステップＳ１３０２において、設定した検索キー（Ｉｎ－ｒｅｐｌｙ－ｔｏ値）をＭｅｓｓａｇｅ－ＩＤヘッダ情報に持つメールを保存メールから検索する。検索キーがＩｎ－ｒｅｐｌｙ－ｔｏ値（Ｍｅｓｓａｇｅ－ＩＤ）であるので、検索結果は一意に決まる。ステップＳ１３０３へ進み、検索結果を確認する。検索キーを持つメールが保存されていない場合（ステップＳ１３０３で「いいえ」の場合）は、親メール検索に失敗する。検索キーを持つメールがあった場合（ステップＳ１３０３で「はい」の場合）は、ステップＳ１３０４に進む。

【０１００】

ここで、検索キーがＩｎ－ｒｅｐｌｙ－ｔｏ値でない場合、即ち、検索キーがタグ、もしくは件名の場合はステップＳ１３０５へ進み、検索結果の中から最新のメールをひとつ選択し、これを親メールとする。検索キーがＩｎ－ｒｅｐｌｙ－ｔｏ値の場合は検索結果が一意に決まるため、ステップＳ１３０５をスキップし、親メール検索処理を終了する。

【０１０１】

図１２に戻って、ステップＳ１２０３において親メールの検索が成功した場合（「はい」の場合）、ステップＳ１２０４へ進み、受信した暗号化メールをメール保存部１１５に保存する。続いて、ステップＳ１２０５で検索メールに前記暗号化メールを設定し、ステップＳ１２０６で前記暗号化メールを親に持つ暗号化メールが一時保存されていないかを確認し、暗号化メール受信処理を終了する。

【０１０２】
親メール検索で親メールが検出されなかった場合（ステップＳ１２０３で「いいえ」の場合）、ステップＳ１２０７へ進み、差出人通知が許可されているかをルール管理部１１２の動作ルールで確認する。差出人通知が許可されている場合（ステップＳ１２０７で「はい」の場合）は、ステップＳ１２０８で差出人通知を実施する。この場合、暗号化メールの受信に際して親メールが発見できなかった旨を通知する。差出人通知が許可されていない場合（ステップＳ１２０７で「いいえ」の場合）は、ステップＳ１２０８をスキップする。ステップＳ１２０９に進み、前期暗号化メールを一時保存領域に保存し、暗号化メール受信処理を終了する。
【０１０３】
図９に戻って、ステップＳ９０３で暗号化メールでないと判断した場合（「いいえ」の場合、ステップＳ９０５へ進み、全親スレッドメールであるかどうかを判断する。全親スレッドメールの詳細については、後述する。全親スレッドメールであると判断した場合は、ステップＳ９０６へ進み、全親スレッドメール受信処理を実施する。
【０１０４】
全親スレッドメールでないと判断した場合（ステップＳ９０５で「いいえ」の場合）、ステップＳ９０７へ進み、差出人通知かどうかを判断する。差出人通知であると判断した場合（ステップＳ９０７で「はい」の場合）、差出人通知受信処理を実施する（ステップＳ９０８）。差出人通知受信処理では、受信した通知データを表示部１１６に表示したり、通知の原因となった暗号化メールへの通知マークを自動的に付与したりすることで、利用者への通知を実施する。
【０１０５】
以上の条件に当てはまらないメールは（ステップＳ９０７で「いいえ」の場合）、ステップＳ９０９へ進み、通常メールとして受信する。
【０１０６】
次に、暗号化メールの返信処理について、図１５を用いて説明する。
【０１０７】
ステップＳ１５０１で返信対象となるメールを、検索メールに設定する。続くステップＳ１５０２においてメール復号処理を実施するが、本発明における暗号化メールスレッド構造の場合、返信対象となる暗号化メールを復号するためには、当該暗号化メールスレッドをルートメールまで遷移し、第一メールから順に復号していく必要がある。
【０１０８】
このような暗号化メールの復号処理について、図１６を用いて説明する。
【０１０９】
ステップＳ１６０１で暗号化メールを保存するスタックを初期化する。ステップＳ１６０２で検索メールに復号対象となる暗号化メールを設定し、ステップＳ１６０３において親メールを検索する、復号するためには、親メールを含むすべての暗号化メールスレッドを構成するメールが必要であるため、親メール検索に失敗した場合（ステップＳ１６０４で「いいえ」の場合）、暗号化メールの復号処理に失敗して終了する。
【０１１０】
親メール検索に成功した場合（ステップＳ１６０４で「はい」の場合）、続くステップＳ１６０５で検索結果のメールがルートメールであるかどうかを判断する。ルートメールでない場合（ステップＳ１６０５で「いいえ」の場合）、ステップＳ１６０６へ進み、検索結果のメールをメールスタックへプッシュする。続く、ステップＳ１６０７にて、検索メールに検索結果の暗号化メールを設定し、ステップＳ１６０３に戻る。これら一連の処理を実施することで、復号対象メールからルートメールまでの暗号化メールスレッドを抽出することができる。
【０１１１】
ステップＳ１６０５でルートメールであった場合（「はい」の場合）、ステップＳ１６０８においてルートメール情報を抽出する。続くステップＳ１６０９で、ルートメール情

報のうち、メールスレッド管理情報を参照し、例えば、図１９における失効時間１９０５を確認することで、有効な暗号であるかどうかを判断する。暗号が無効であると判断した場合（ステップＳ１６０９で「いいえ」の場合）、メール復号処理を失敗して終了する。

【０１１２】

暗号が有効であると判断した場合（ステップＳ１６０９で「はい」の場合）、暗号化メールスレッドを利用した復号処理を実施する。ステップＳ１６１０に進み、共通鍵ファイルとしてルートメールを設定する。続くステップＳ１６１１で、前記メールスタックが空でない間、メールスタックから暗号化メールを取り出し（ステップＳ１６１２）、共通鍵ファイルを参照して、暗号化メール本文を復号する（ステップＳ１６１３）。このとき、必要であればパスフレーズ１６１８の入力が必要となる。

【０１１３】

暗号化メールの復号に失敗した場合（ステップＳ１６１４で「いいえ」の場合）、メール復号処理を失敗して終了する。復号に成功した場合（ステップＳ１６１４で「はい」の場合）、復号した暗号化メール本文を共通鍵ファイルに設定し（ステップＳ１６１５）、ステップＳ１６１１に戻る。このようにメールスタックが空になるまで暗号化メールの復号処理を実施し、復号対象メールの親メールまで復号する。

【０１１４】

ステップＳ１６１９で前記親メール本文を共通鍵ファイルとして、復号対象メールを復号する。ステップＳ１６１９での復号処理に失敗した場合（ステップＳ１６２０で「いいえ」の場合）、メール復号処理を失敗して終了する。復号処理に成功した場合（ステップＳ１６２０で「はい」の場合）、メール復号処理を終了する。

【０１１５】

図１５に戻って、ステップＳ１５０３で返信元メールの復号処理に失敗した場合、メール返信処理を終了する。復号処理に成功した場合は、復号した返信元メールを利用者へ提示して返信メールの入力を行う（ステップＳ１５０４）。

【０１１６】

ステップＳ１５０４で返信メールを入力した後、返信メールを配送するが、このとき、返信元メールに対して返信宛先が利用者によって修正される場合がある。この場合、本発明における暗号化メールスレッド方式では、新規宛先側には当該暗号化メールスレッドを構成するルートメールを始めとした返信元メールまでの一連の親メールが存在しないことから、返信メールを受信してもその内容を復号することができないため、新規に追加された宛先のみ処理をわける必要がある。従って、ステップＳ１５０５で作成された返信メールに宛先の追加があるか否かを確認する。

【０１１７】

追加宛先がない場合（ステップＳ１５０５で「いいえ」の場合）、前記返信元メールを共通鍵ファイルとして作成した返信メールを暗号化処理する（ステップＳ１５０６）。続くステップＳ１５０７及びステップＳ１５０８において、すべての返信宛先に対して暗号化した返信メールを配信する。

【０１１８】

すべての宛先への返信を終了後、ステップＳ１５０９で作成した暗号化メールをメール保存部１１５に保存し、メール返信処理を終了する。

【０１１９】

ステップＳ１５０５で宛先の追加があった場合（「はい」の場合）、ステップＳ１５１０へ進み、追加されたすべての宛先について、以下の処理を実施する。

【０１２０】

ステップＳ１５１１において、動作ルールを確認し、その宛先や返信メールの内容から暗号化するルールであるかを判断する。暗号化するルールでない場合（ステップＳ１５１１で「いいえ」の場合）、暗号化メールの返信を非暗号化することになるため、ステップＳ１５２１へ進み、返信禁止の旨を表示し、ステップＳ１５１０へ戻る。

【０１２１】

暗号化するルールである場合（ステップＳ１５１１で「はい」の場合）、ステップＳ１５１２へ進み、動作ルールを確認し、全親スレッドが送信できるか否かを確認する。新規宛先が暗号化された返信メールを受信した場合、その復号のためにルートメールを含む当該暗号化メールスレッドを持っていなければならない。全親スレッドとは、当該暗号化メールスレッドを構成する全親メールを意味する。図７に例示した動作ルール７００において、動作ルール７０７は、利用者ｈａｙａｓｈｉ及びｔａｎａｋａに全スレッド受信許可の例である。

【０１２２】

当該宛先に対して全親スレッド送信許可がある場合（ステップＳ１５１２で「はい」の場合）、メール保存部１０７より全親スレッドを抽出する（ステップＳ１５１３）。続くステップＳ１５１４で、ステップＳ１５０６と同様に、返信元である親メールを共通鍵ファイルとして作成した返信メールを暗号化する。続くステップＳ１５１５で全親スレッドを送信し、ステップＳ１５１６で前記暗号化した返信メールを送信し、ステップＳ１５１０に戻る。

【０１２３】

全親スレッドが送信不可であると判断した場合（ステップＳ１５１２で「いいえ」の場合）、直前のステップＳ１５１１で暗号化すべきメールであると判断しているため、ステップＳ１５１７において新規スレッドとして作成できるか否かを動作ルールで確認する。新規スレッド作成許可がない場合（ステップＳ１５１７で「いいえ」の場合）、ステップＳ１５２１へ進み、返信禁止の旨を利用者へ提示する。

【０１２４】

新規スレッド作成許可がある場合（ステップＳ１５１７で「はい」の場合）、ルートメールを作成し（ステップＳ１５１８）、ルートメールを共通鍵ファイルといて返信メールを暗号化する（ステップＳ１５１９）。続くステップＳ１５２０でルートメールを送信し、ステップＳ１５１６で暗号化された返信メールを送信し、ステップＳ１５１０へ戻る。

【０１２５】

ステップＳ１５１０において、すべての追加宛先に対しての返信処理を終了すると、ステップＳ１５２２へ進む。動作ルールを参照した結果、追加宛先があるにも関わらず当該追加宛先へ全く返信処理が実施されていない場合（ステップＳ１５２２で「いいえ」の場合）、宛先の指定に不正があるものとみなし、既存宛先の有無に関わらずメール返信処理を終了する。追加宛先への返信があった場合（ステップＳ１５２２で「はい」の場合）、ステップＳ１５０６へ進み、既存宛先に対しての返信処理を実施する。

【０１２６】

図１５のステップＳ１５１５で送信した全親スレッドメールは、図９のメール受信処理において、ステップＳ９０６を通して処理される。全親スレッド受信処理について、図１７を用いて説明する。

【０１２７】

ステップＳ１７０１において動作ルールを参照し、全親スレッドの受信許可があるか否かを確認する。受信許可がない場合（ステップＳ１７０１で「いいえ」の場合）、ステップＳ１７０５へ進み、差出人通知許可があるか否かを動作ルールで確認する。差出人通知が許可されている場合（ステップＳ１７０５で「はい」の場合）、差出人へ全親スレッドの受信不可である旨を通知する（ステップＳ１７０６）。差出人通知許可がない場合（ステップＳ１７０５で「いいえ」の場合）、ステップＳ１７０６をスキップし、全親スレッドの受信を拒否する。

【０１２８】

全親スレッドの受信が許可されている場合（ステップＳ１７０１で「はい」の場合）、全親スレッドをメール保存部１１５に保存する（ステップＳ１７０２）。続くステップＳ１７０３で検索メールに全親スレッド内での最終メールを設定し、関連メール移動処理を実施する（ステップＳ１７０４）。これは、全親スレッドに続く暗号化メールを先に受信していないかを確認するための処理となる。

【０１２９】
次に、暗号化メールの転送処理について、図１８を用いて説明する。
【０１３０】
ステップＳ１８０１で転送対象となるメールを、検索メールに設定する。続くステップＳ１８０２において、メール返信処理と同様に、転送対象となる暗号化メールを復号する。転送元メールの復号処理に失敗した場合（ステップＳ１８０３で「いいえ」の場合）、メール転送を終了する。
【０１３１】
転送元メールの復号に成功した場合（ステップＳ１８０３で「はい」の場合）、復号した転送元メールを利用者へ提示して転送メールの入力を行う（ステップＳ１８０４）。
【０１３２】
メール転送では転送元メールの宛先は継承されないため、ステップＳ１８０５からの一連の処理において、すべての宛先が対象となる。ステップＳ１８０６において、暗号化するルールではなかった場合（「いいえ」に場合）、暗号化メールを非暗号化で転送することになるため、ステップＳ１８１６に進み、転送禁止を利用者へ提示し、ステップＳ１８０５へ戻る。
【０１３３】
暗号化するルールであった場合（ステップＳ１８０６で「はい」の場合）、ステップＳ１８０７へ進み、動作ルールを確認し、全親スレッドが送信できるか否かを確認する。宛先が暗号化された転送メールを受信した場合、その復号のためにルートメールを含む当該暗号化メールスレッドを持っていなければならない。
【０１３４】
当該宛先に対して全親スレッド送信許可がある場合（ステップＳ１８０７で「はい」の場合）、メール保存部１０７より全親スレッドを抽出する（ステップＳ１８０８）。続くステップＳ１８０９で、転送元である親メールを共通鍵ファイルとして作成した転送メールを暗号化する。続くステップＳ１８１０で全親スレッドを送信し、ステップＳ１８１１で前記暗号化した転送メールを送信し、ステップＳ１８０５に戻る。
【０１３５】
全親スレッドが送信不可であると判断した場合（ステップＳ１８０７で「いいえ」の場合）、直前のステップＳ１８０６で暗号化すべきメールであると判断しているため、ステップＳ１８１２において新規スレッドとして作成できるか否かを動作ルールで確認する。新規スレッド作成許可がない場合（ステップＳ１８１２で「いいえ」の場合）、ステップＳ１８１６へ進み、転送禁止の旨を利用者へ提示する。
【０１３６】
新規スレッド作成許可がある場合（ステップＳ１８１２で「はい」の場合）、ルートメールを作成し（ステップＳ１８１３）、ルートメールを共通鍵ファイルとして作成した転送メールを暗号化する（ステップＳ１８１４）。続いて、ルートメールを送信し（ステップＳ１８１５）、暗号化した転送メールを送信し（ステップＳ１８１１）、ステップＳ１８０５へ戻る。
【０１３７】
ステップＳ１８０５から一連の処理をすべての宛先に対して実施した後、ステップＳ１８１７へ進み、全く転送が実施されなかった場合（「いいえ」の場合）は、メール転送処理を終了する。ひとつ以上の宛先へ暗号化メール転送処理が実施された場合（ステップＳ１８１７で「はい」の場合）は、作成した暗号化メールをメール保存部１０７に保存する（ステップＳ１８１８）。
【０１３８】
次に、メールゲートウェイ上で送受信される暗号化メールを監査する方法について、説明する。
【０１３９】
本発明における暗号化メールスレッド方式では、ルートメールを含むすべてのメールを

所持していない限り、暗号化メールを復号することができない特徴がある。しかしながら、共通鍵ファイルである親メールのみ所持していることで、暗号化メールは復号することが可能である。この特徴を利用し、メールゲートウェイ上で監査目的に暗号化メールを復号する場合、直前のメールを復号した上で所持すればよい。

【０１４０】

以上、一実施形態について示したが、本発明は、例えば、システム、装置、方法、プログラムもしくは記録媒体等としての実施態様を取ることが可能であり、具体的には、暗号化メール送信装置及び暗号化メール受信装置については、それぞれ複数の機器から構成されるシステムに適用しても、ひとつの機器からなるシステムに適用してもよい。

【０１４１】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な内容で構成されることは言うまでもない。

【０１４２】

また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのソフトウェアによって表されるプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１４３】

さらに、本発明を達成するためのソフトウェアによって表されるプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１４４】

なお、上述した各実施形態及びその変形例を組み合わせた構成もすべて本発明に含まれるものである。

【０１４５】

本発明によれば、電子メールはメールスレッド暗号化方式によって連鎖的に本文部を暗号化することができ、更にメールスレッド単位の原本保証性を確保できる。また、誤送信が発生した場合では、誤送信先がメールスレッド全体を所持していない限り、内容の閲覧はできないため、情報セキュリティが確保できる。更に、メールスレッド暗号化方式は電子メールの本文部が共通鍵ファイルとなるため鍵管理コストが軽減され、メールゲートウェイ上に電子メール本文部を保存しておくことで、情報監視が可能となる。また、ルートメールに記載される情報によって、メールスレッド単位で電子メールの送受信を含めた情報管理が可能となる等の効果を奏する。

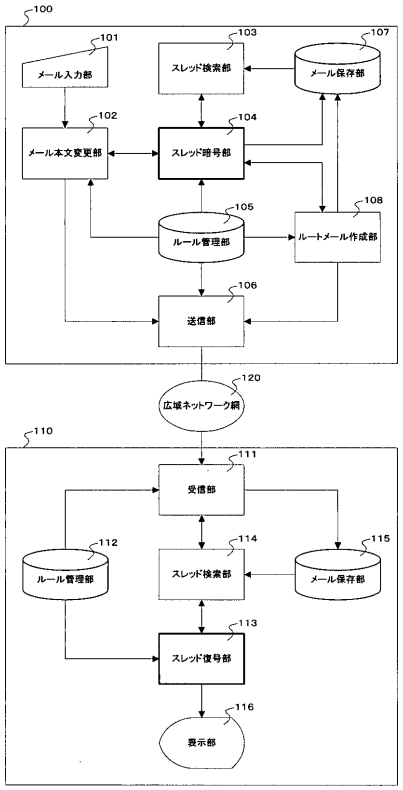
【符号の説明】

【０１４６】

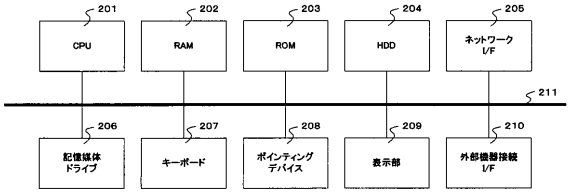
１００　暗号化メール送信装置
１０１　メール入力部
１０２　メール本文変更部
１０３　スレッド検索部
１０４　スレッド暗号部
１０５　ルール管理部
１０６　送信部
１０７　メール保存部
１０８　ルートメール作成部
１１０　暗号化メール受信装置
１１１　受信部
１１２　ルール管理部
１１３　スレッド復号部
１１４　スレッド検索部

１１５　メール保存部
１１６　表示部
１２０　広域ネットワーク網
２０１　ＣＰＵ
２０２　ＲＡＭ
２０３　ＲＯＭ
２０４　ＨＤＤ
２０５　ネットワークＩ／Ｆ
２０６　記憶媒体ドライブ
２０７　キーボード
２０８　ポインティングデバイス
２０９　表示部
２１０　外部機器接続Ｉ／Ｆ
２１１　バス

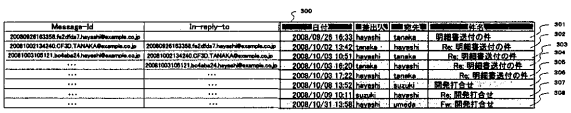
【図１】



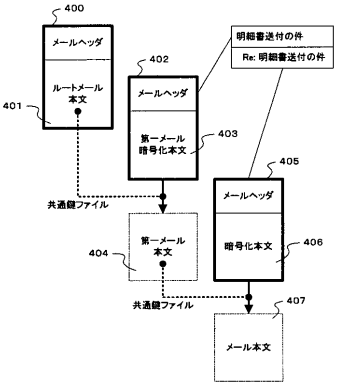
【図２】



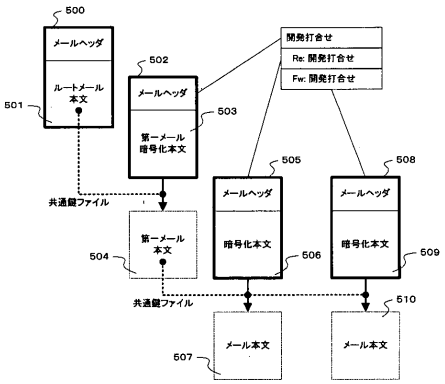
【図３】



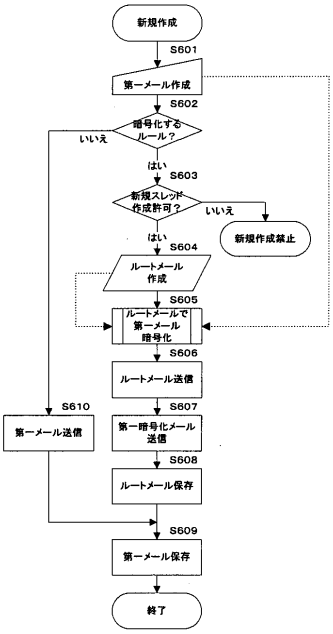
【図４】



【図５】



【図６】

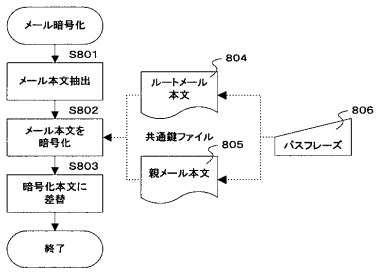


【図７】

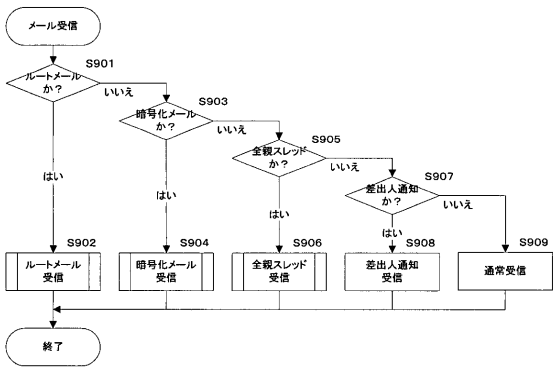
700

条件	動作	
eaddr != *.example.co.jp	暗号化	701
keywords == [社外秘]	暗号化	702
attachment > 0	暗号化	703
user == [hayashi,tanaka]	新規作成許可	704
user == [hayashi,tanaka]	ルートメール受信許可	705
user == [hayashi,tanaka,umeda]	差出人通知許可	706
user == [hayashi,tanaka]	全スレッド受信許可	707

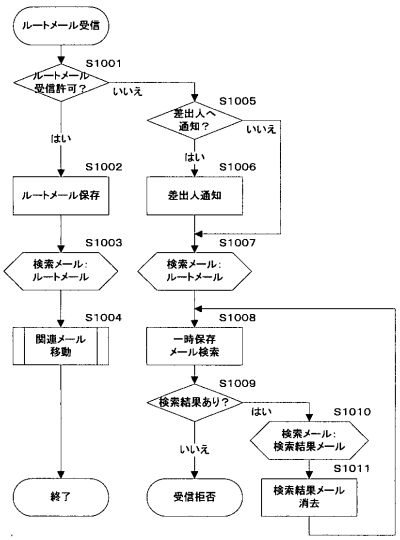
【図８】



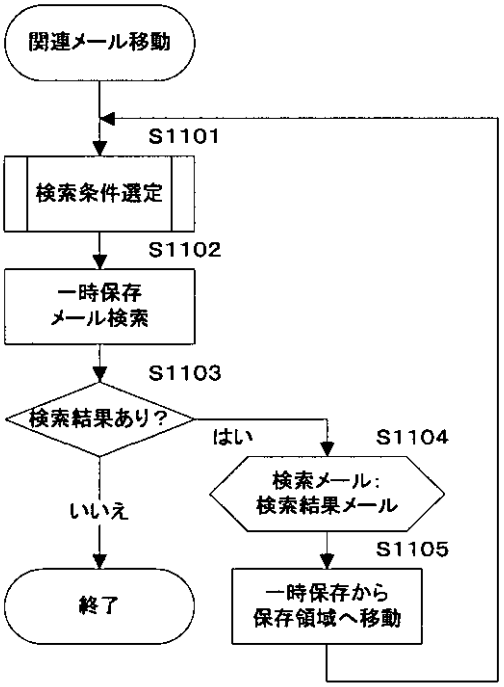
【図９】



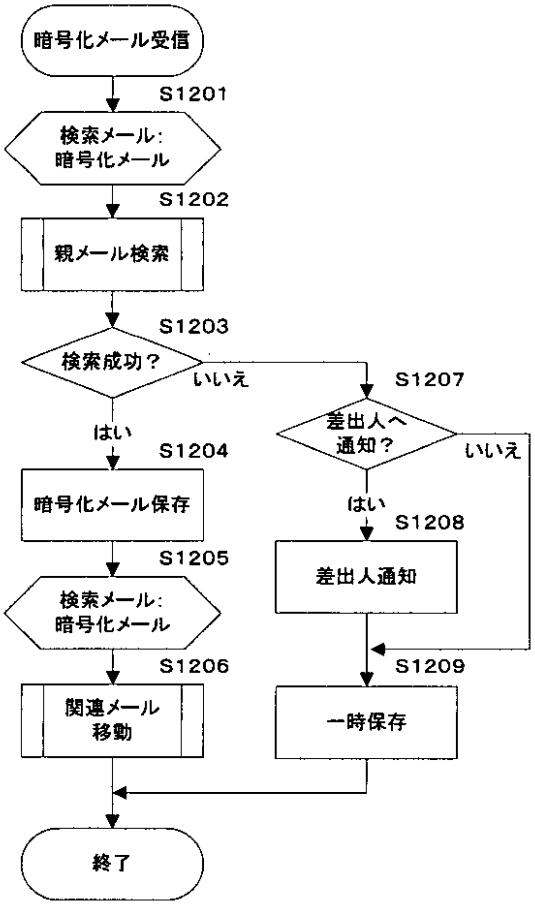
【図１０】



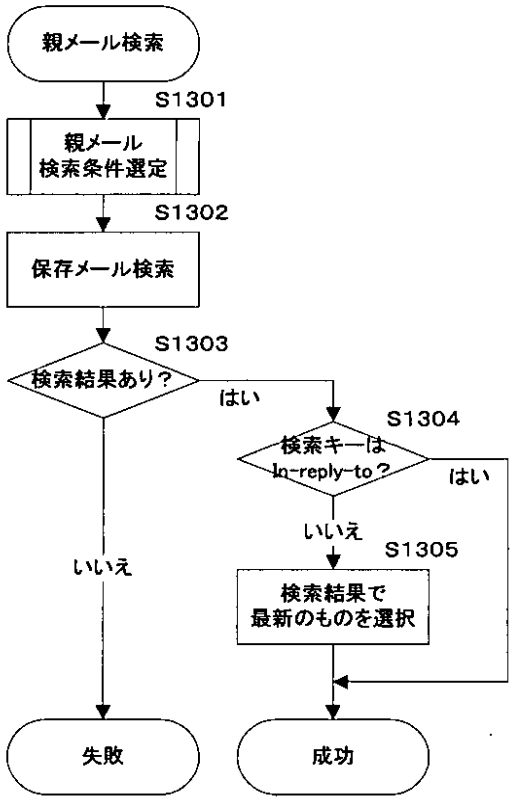
【図１１】



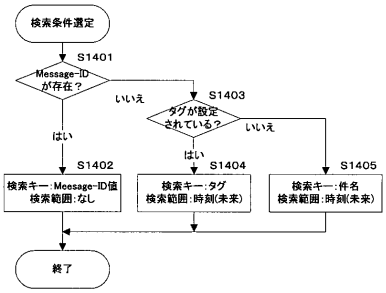
【図１２】



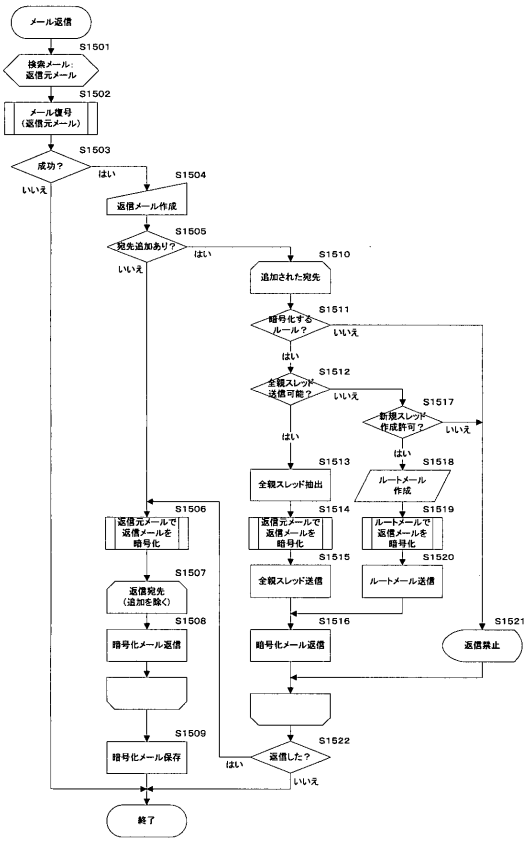
【図１３】



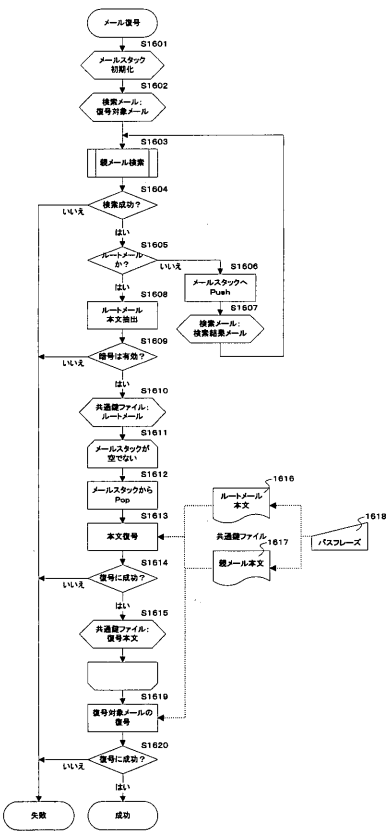
【図１４】



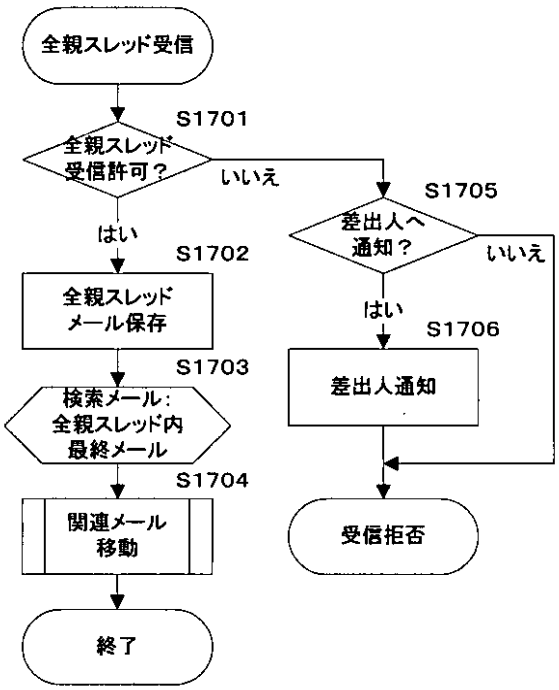
【図１５】



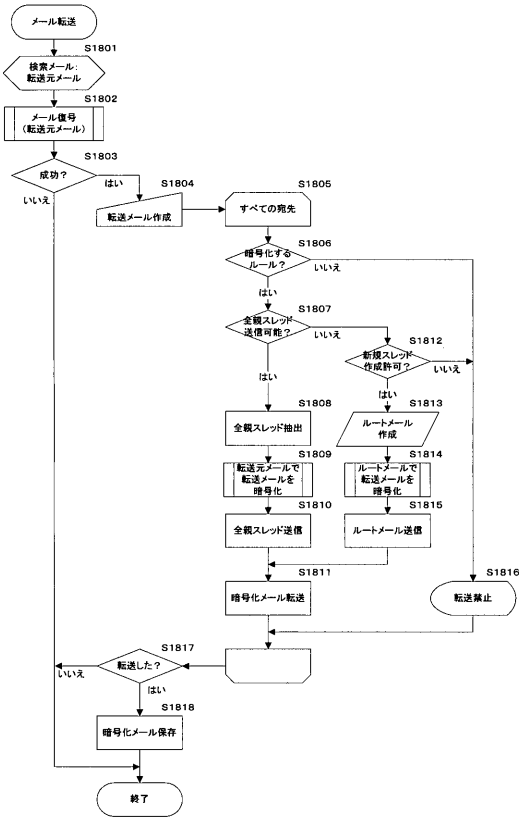
【図１６】



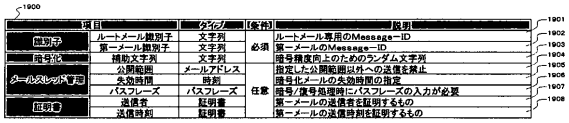
【図１７】



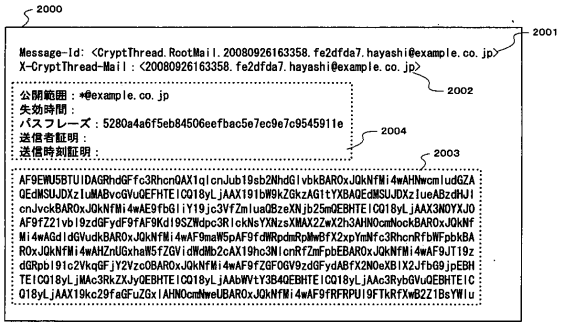
【図１８】



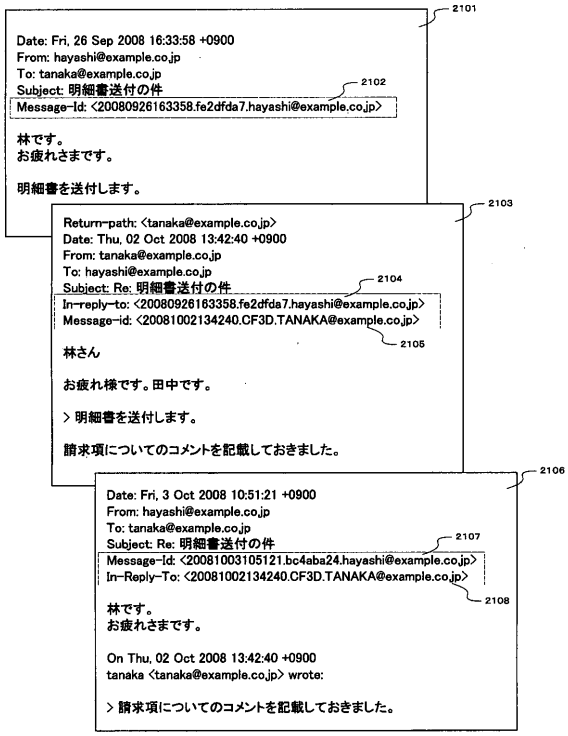
【図１９】



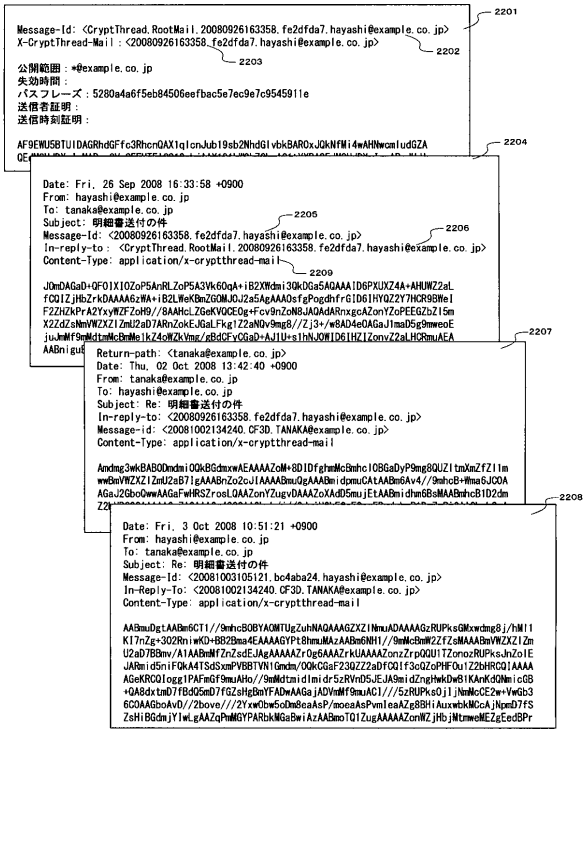
【図２０】



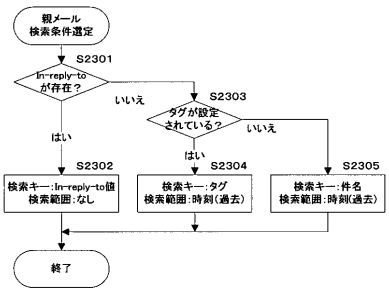
【図２１】



【図２２】



【図２３】



フロントページの続き

審査官　石田　信行

(56)参考文献　特開２００７－２６６６７４（ＪＰ，Ａ）
特開平０９－０５４７３３（ＪＰ，Ａ）
特開２０００－１７２５８６（ＪＰ，Ａ）
特開２００１－２２２４７７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４
Ｈ０４Ｌ　　９／０８
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　１３／００