

(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2008-299561

(P2008-299561A)

(43) 公開日 平成20年12月11日(2008.12.11)

(51) Int.Cl.		F I		テーマコード (参考)
G06F 13/00	(2006.01)	G06F 13/00	610S	5B017
G06F 21/24	(2006.01)	G06F 13/00	625	5J104
H04L 9/14	(2006.01)	G06F 12/14	540A	
		H04L 9/00	641	

審査請求 未請求 請求項の数 5 O L (全 11 頁)

(21) 出願番号	特願2007-144469 (P2007-144469)	(71) 出願人	000233055
(22) 出願日	平成19年5月31日 (2007.5.31)		日立ソフトウェアエンジニアリング株式会社
			東京都品川区東品川四丁目12番7号
		(74) 代理人	100095267
			弁理士 小島 高城郎
		(74) 代理人	100124176
			弁理士 河合 典子
		(74) 代理人	100111604
			弁理士 佐藤 卓也
		(72) 発明者	栗田 大樹
			東京都品川区東品川4丁目12番7号 日
			立ソフトウェアエンジニアリング株式会社
			内
		Fターム(参考)	5B017 AA03 BA07 CA16
			5J104 AA35 DA04 PA08

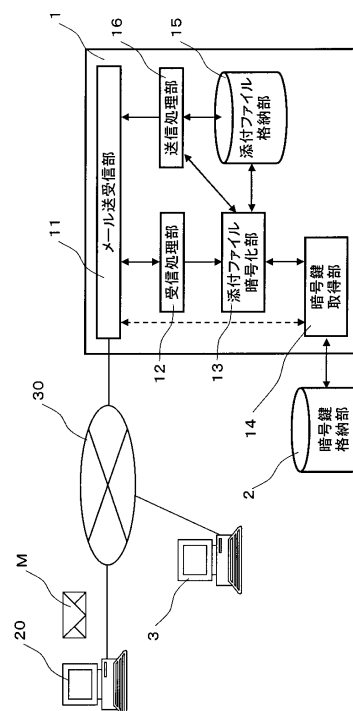
(54) 【発明の名称】 電子メール送信装置

(57) 【要約】

【課題】従来の装置に組み込みが容易かつ人手に頼らずにセキュリティを向上することが可能な電子メール送信装置を提供する。

【解決手段】ネットワーク30を介してクライアント20からの電子メールMを受信すると共に、少なくとも送信可能電子メールを送信するメール送受信部11と、電子メールMに添付ファイルの有無を検査する受信処理部112と、電子メールMの添付ファイルを送信元と宛先に基づいて特定される暗号鍵で宛先毎に暗号化して暗号化添付ファイルを作成する添付ファイル暗号化部113と、添付ファイル暗号化部113からの要求に応じて暗号鍵格納部2から暗号鍵を取得する暗号鍵取得部114と、この送信元と宛先に対応させて格納する添付ファイル格納部115と、この送信元と宛先に基づいて暗号化添付ファイルを取得してこの宛先の電子メールMの添付ファイルと入れ替えて送信可能電子メールを作成する送信処理部116と、を備えた構成を有している。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

電子メールを受信すると共に、所定の電子メールを送信するメール送受信部と、受信した前記電子メールに添付ファイルが添付されているか否かを判断する受信処理部と、受信した前記電子メールの添付ファイルを送信元と宛先に基づいて特定される暗号鍵で宛先毎に暗号化して暗号化添付ファイルを作成する添付ファイル暗号化部と、暗号鍵を格納する暗号鍵格納部と、前記添付ファイル暗号化部からの要求に応じて前記暗号鍵格納部から暗号鍵を取得する暗号鍵取得部と、前記暗号化添付ファイルを受信した前記電子メールの送信元と宛先に対応させて格納する添付ファイル格納部と、受信した前記電子メールの送信元と宛先に基づいて特定される前記暗号化添付ファイルを前記添付ファイル格納部中から取得してこの宛先の電子メールの添付ファイルと入れ替えて送信可能電子メールを作成する送信処理部と、を備え、前記メール送受信部は、添付ファイルがあった電子メールに対しては前記送信処理部が作成した前記送信可能電子メールを送信し、添付ファイルがなかった電子メールに対しては受信した前記電子メールを送信することを特徴とする電子メール送信装置。

10

【請求項 2】

前記添付ファイル暗号化部が前記添付ファイルを暗号化できなかった場合に、前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成し、前記メール送受信部が、前記送信処理部によって添付ファイルが削除された電子メールを送信することを特徴とする請求項 1 に記載の電子メール送信装置。

20

【請求項 3】

前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、この電子メールに添付ファイルが削除されていることを追記し、前記メール送受信部が、添付ファイルが削除されていることを追記された電子ファイルを送信することを特徴とする請求項 1 又は請求項 2 に記載の電子メール送信装置。

【請求項 4】

前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、前記メール送受信部が、この宛先の電子メールから添付ファイルを削除したことを送信元に通知することを特徴とする請求項 1 乃至請求項 3 のいずれか一項に記載の電子メール送信装置。

30

【請求項 5】

前記暗号鍵格納部が、前記ネットワークを介して通信可能に接続された外部のサーバとして構成されることを特徴とする請求項 1 乃至請求項 4 のいずれか一項に記載の電子メール送信装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子メールを受信して暗号化されていない添付ファイルを暗号化して送信する電子メール送信装置に関する。

【背景技術】

40

【0002】

近年の電子メールの普及に伴い、契約書、設計書等の業務書類を電子化した業務データを電子メールに添付して送信することは、日常的に行われている。ここで、業務データを添付ファイルとする電子メールのサーバとして従来の構成のものを用いる場合、電子メールはハードディスク等のローカルディスク上に保存されることになる。

【0003】

ここで、電子メールがローカルディスク上に保存されている場合、所謂ウイルス等によって意図せずに送信されることが起こりうる。その結果、不特定多数の者に公開されたり、セキュリティ上の対策が施されない状態で宛先に送信されたりして、不測の事態を招くことになりかねない。かかる事態は、過誤によっても起こりうる。

50

【0004】

この様なウイルスへの対策として、電子メールの通信路のみならず、メールボックス内においても電子メールを暗号化しておく技術が知られている（例えば、特許文献1参照）。また、電子メールを送信する場合に、添付ファイルを必ず暗号化してから送信するように取り決めておく管理方法もある。

【特許文献1】特開2006-039740号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、特許文献1に記載の従来の電子メールの通信装置では、特定の電子メール（例えば所謂暗号化メール）のみが暗号化されるだけで、その他の一般の電子メールは暗号化されずに送信されてしまうため、一般の電子メールに対しては依然としてセキュリティが十分に確保できないという問題を有していた。また、電子メールの暗号化技術は、添付ファイルのみならず電子メール全体を暗号化するものであり、一般に使用されている電子メールシステムに組み込むことは困難である。さらに、電子メールの参照には専用のメールサーバが必要となり、新たな設備の導入に繋がり経済的な負担が増大することとなる。一方、管理方法に頼るのでは、暗号鍵の共有、暗号化処理等が送信者に委ねられ、依然として過誤を排除することは困難である。

【0006】

以上の現状に鑑み、本発明の目的は、従来の装置に組み込みが容易でありかつ人手に頼らずに添付ファイルに対するセキュリティを向上することが可能な電子メール送信装置を提供する。

【課題を解決するための手段】

【0007】

上記の課題を解決すべく、本発明は以下の構成を提供する。

請求項1に係る発明は、電子メールを受信すると共に、所定の電子メールを送信するメール送受信部と、受信した前記電子メールに添付ファイルが添付されているか否かを判断する受信処理部と、受信した前記電子メールの添付ファイルを送信元と宛先に基づいて特定される暗号鍵で宛先毎に暗号化して暗号化添付ファイルを作成する添付ファイル暗号化部と、暗号鍵を格納する暗号鍵格納部と、前記添付ファイル暗号化部からの要求に応じて前記暗号鍵格納部から暗号鍵を取得する暗号鍵取得部と、前記暗号化添付ファイルを受信した前記電子メールの送信元と宛先に対応させて格納する添付ファイル格納部と、受信した前記電子メールの送信元と宛先に基づいて特定される前記暗号化添付ファイルを前記添付ファイル格納部中から取得してこの宛先の電子メールの添付ファイルと入れ替えて送信可能電子メールを作成する送信処理部と、を備え、前記メール送受信部は、添付ファイルがあった電子メールに対しては前記送信処理部が作成した前記送信可能電子メールを送信し、添付ファイルがなかった電子メールに対しては受信した前記電子メールを送信することを特徴とする。

【0008】

請求項2に係る発明は、請求項1に記載の電子メール送信装置において、前記添付ファイル暗号化部が前記添付ファイルを暗号化できなかった場合に、前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成し、前記メール送受信部が、前記送信処理部によって添付ファイルが削除された電子メールを送信することを特徴とする。

【0009】

請求項3に係る発明は、請求項1に記載の電子メール送信装置において、前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、この電子メールに添付ファイルが削除されていることを追記し、前記メール送受信部が、添付ファイルが削除されていることを追記された電子ファイルを送信することを特徴とする。

【0010】

請求項4に係る発明は、請求項1に記載の電子メール送信装置において、前記送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、前記メール送受信部が、この宛先の電子メールから添付ファイルを削除したことを送信元に通知することを特徴とする。

【0011】

請求項5に係る発明は、請求項1に記載の電子メール送信装置において、前記暗号鍵格納部が、前記ネットワークを介して通信可能に接続された外部のサーバとして構成されることを特徴とする。

【発明の効果】

10

【0012】

請求項1に係る発明によれば、電子メールを受信すると共に、所定の電子メールを送信するメール送受信部と、受信した電子メールに添付ファイルが添付されているか否かを判断する受信処理部と、受信した電子メールの添付ファイルを送信元と宛先に基づいて特定される暗号鍵で宛先毎に暗号化して暗号化添付ファイルを作成する添付ファイル暗号化部と、暗号鍵を格納する暗号鍵格納部と、添付ファイル暗号化部からの要求に応じて暗号鍵格納部から暗号鍵を取得する暗号鍵取得部と、暗号化添付ファイルを受信した電子メールの送信元と宛先に対応させて格納する添付ファイル格納部と、受信した電子メールの送信元と宛先に基づいて特定される暗号化添付ファイルを添付ファイル格納部中から取得してこの宛先の電子メールの添付ファイルと入れ替えて送信可能電子メールを作成する送信処理部と、を備え、メール送受信部は、添付ファイルがあった電子メールに対しては送信処理部が作成した送信可能電子メールを送信し、添付ファイルがなかった電子メールに対しては受信した電子メールを送信するため、従来の装置に組み込みが容易でありかつ人手に頼らずに添付ファイルに対するセキュリティを向上することが可能な電子メール送信装置を実現することができる。

20

【0013】

請求項2に係る発明によれば、上記請求項1の効果に加えて、添付ファイル暗号化部が添付ファイルを暗号化できなかった場合に、送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成し、メール送受信部が、送信処理部によって添付ファイルが削除された電子メールを送信するため、少なくとも添付ファイルのない電子メールを宛先に送信することができる。

30

【0014】

請求項3に係る発明によれば、上記請求項1の効果に加えて、送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、この電子メールに添付ファイルが削除されていることを追記し、メール送受信部が、添付ファイルが削除されていることを追記された電子ファイルを送信するため、セキュリティ上添付ファイルが削除されたことを宛先に通知することができる。

【0015】

請求項4に係る発明によれば、上記請求項1の効果に加えて、送信処理部が対応する宛先に送信する電子メールとして添付ファイルを削除した電子メールを作成した場合に、メール送受信部が、この宛先の電子メールから添付ファイルを削除したことを送信元に通知するため、セキュリティ上添付ファイルが削除されたことを送信元に通知することができる。

40

【0016】

請求項5に係る発明によれば、上記請求項1の効果に加えて、暗号鍵格納部が、ネットワークを介して通信可能に接続された外部のサーバとして構成されるため、セキュリティ向上の為に使用できる外部に資源を取り込むことができる。

【発明を実施するための最良の形態】

【0017】

以下、実施例を示した図面を参照しつつ本発明の実施の形態について説明する。

50

図 1 は、本発明による電子メール送信装置の一実施例を模式的に示すブロック構成図である。電子メール送信装置 1 は、図 1 に示すように、ネットワーク 30 を介して通信可能に接続されたクライアント 20 からの電子メール M を受信すると共に、所定の電子メールを送信するメール送受信部 11 と、受信した電子メール M に添付ファイルが添付されているか否かを判断する受信処理部 12 と、受信した電子メール M の添付ファイルを送信元と宛先に基づいて特定される暗号鍵で宛先毎に暗号化して暗号化添付ファイルを作成する添付ファイル暗号化部 13 と、添付ファイル暗号化部 13 からの要求に応じて暗号鍵格納部 2 から暗号鍵を取得する暗号鍵取得部 14 と、暗号化添付ファイルを電子メール M の送信元と宛先に対応させて格納する添付ファイル格納部 15 と、電子メール M の送信元と宛先に基づいて特定される暗号化添付ファイルを添付ファイル格納部 15 中から取得してこの宛先の電子メール M の添付ファイルと入れ替えて送信可能電子メールを作成する送信処理部 16 と、を備え、メール送受信部 11 は、添付ファイルがあった電子メールに対しては送信処理部 16 が作成した送信可能電子メールを送信し、添付ファイルがなかった電子メールに対しては受信した電子メールを送信するように構成されている。

10

【0018】

ここで、暗号鍵格納部 2 は、電子メールの送信元と宛先毎に暗号鍵を格納するように構成され、電子メール送信装置 1 に含まれるものであっても、アクセス可能に構成された外部のサーバ 3 であっても、又はその両方からなるのでもよい。外部のサーバとして構成される場合、暗号鍵は、例えば、LDAP (Lightweight Directory Access Protocol) に対応しセキュリティ対策が施された環境で管理することも可能である。

20

【0019】

図 2 は、受信処理部が行う処理について説明するフローチャートである。メール送受信部 11 が電子メールを受信したとき、受信処理部 12 は、受信した電子メールの所定の箇所を検査して (S101) 添付ファイルがあるか否かを判断し (S102)、添付ファイルがあると判断したとき、添付ファイルを暗号化して送信可能な電子メールを作成し、送信する暗号化添付ファイル電子メール作成送信処理が行われる (S103)。

【0020】

ここで、添付ファイルがあるか否かの判断は、電子メールの構成によって異なるが、例えば MIME (Multipurpose Internet Mail Extensions) という規約に従う電子メールの場合は、「Content-Type」という項目に「multipart/mixed」が設定されているか否かを判断することによって、実現できる。

30

【0021】

ステップ S102 で添付ファイルがないと判断されたとき、メール送受信部 11 は、受信した電子メールをそのまま送信して (S104) 処理は終了する。

【0022】

以下、暗号化添付ファイル電子メール作成送信処理について説明する。まず、暗号鍵を取得する処理について説明する。図 3 は、電子メールアドレスに基づいて暗号鍵を暗号鍵格納部から取得する処理例について説明するフローチャートである。まず、暗号鍵取得部 14 は、添付ファイル暗号化部 13 からの要求に応じて、暗号鍵格納部 2 から暗号鍵の読み込み処理を行う (S211)。

40

【0023】

図 4 は、暗号鍵格納部が暗号鍵を格納するレコードの構成を示す説明図である。暗号鍵 402 は、図 4 に示すように、宛先のメールアドレス 401 と対応付けられて暗号鍵格納部 2 の送信元用のレコード内に格納されている。ステップ S211 では、例えば、送信元と宛先のメールアドレスに対応する暗号鍵を暗号鍵格納部 2 から読み込む処理が行われる。

【0024】

次に、暗号鍵取得部 14 は、ステップ S211 での読み込み処理で暗号鍵を読み込むことができたか否かを判断し (S212)、暗号鍵を読み込むことができたと判断した場合、読み込んだ暗号鍵を要求元の添付ファイル暗号化部 13 に出力し (S213)、読み込

50

むことができていないと判断した場合、要求元の添付ファイル暗号化部 1 3 に適切に読み込みができなかったことの通知を出力する (S 2 1 3)。

【0025】

図 5 は、暗号鍵格納部のほかに上記の外部のサーバにも暗号鍵を格納可能な構成における、図 3 に対応するフローチャートである。この構成では、暗号鍵取得部 1 4 は、例えば、図 1 に破線で示すようにメール送受信部 1 1 を介して外部のサーバ 3 から暗号鍵を読み込む。以下では、図 3 を用いて説明したステップと同一のものについては同一の符号を付し、その説明を省略する。

【0026】

ステップ S 2 1 1 での暗号鍵格納部からの暗号鍵の読み込み処理の後の、ステップ S 2 1 2 での処理で暗号鍵を読み込むことができていないと判断した場合、暗号鍵取得部 1 4 は、例えば上記のようにメール送受信部 1 1 を介して外部のサーバに対して暗号鍵の読み込み処理を行う (S 2 2 4)。

【0027】

次に、暗号鍵取得部 1 4 は、ステップ S 2 2 4 での読み込み処理で暗号鍵を読み込むことができたか否かを判断し (S 2 2 5)、暗号鍵を読み込むことができたと判断した場合、読み込んだ暗号鍵を要求元の添付ファイル暗号化部 1 3 に出力し (S 2 1 3)、読み込むことができていないと判断した場合、要求元の添付ファイル暗号化部 1 3 に適切に読み込みができなかったことの通知を出力する (S 2 2 6)。

【0028】

この実施例では、暗号鍵格納部から暗号鍵を読み込むことができない場合に外部のサーバに対して読み込み処理を行う構成になっているが、読み込み処理を行う順番を逆にした構成でも、外部のサーバに対してのみ読み込み処理を行う構成でもよい。

【0029】

図 6 は、暗号化添付ファイル電子メール作成送信処理のうちの添付ファイル暗号化部が行う処理例について説明するフローチャートである。まず、添付ファイル暗号化部 1 3 は、受信した電子メール中の宛先のメールアドレスの総数 N を取得して (S 3 0 1) アドレスカウンタ c n t を 1 に設定する (S 3 0 2)。

【0030】

次に、添付ファイル暗号化部 1 3 は、アドレスカウンタ c n t で特定される順番の宛先のメールアドレスを取得し (S 3 0 3)、さらに、電子メールから添付ファイルを取得する (S 3 0 4)。ここで、添付ファイルの取得の方法は、電子メールの構成によって異なるが、例えば、M I M E (Multipurpose Internet Mail Extensions) の場合は、以下のように行う。

【0031】

M I M E の場合は、Content-Type 内の boundary= 以下の文字列が添付ファイルを特定可能な情報 (以下、添付ファイル情報) であるため、添付ファイル情報が記載されているこの部分を切り出し、切り出した部分のヘッダからファイルタイプ及びファイル名を取得する。次に、添付ファイルのデータを取得すると共にヘッダから添付ファイルのエンコードの方法についての情報を取得し、エンコードの方法に応じたデコードを行って添付ファイルを復元し取得する。

【0032】

次に、添付ファイル暗号化部 1 3 は、宛先のメールアドレスを含む所定の情報を、添付ファイル格納部 1 5 へ格納する (S 3 0 5)。図 7 は、添付ファイル格納部が宛先のメールアドレスを格納するレコード構成の説明図である。図 7 において、このレコードは、送信元メールアドレス 7 0 1、タイムスタンプ 7 0 2、宛先メールアドレス 7 0 3、添付ファイル 7 0 4 等からなる。

【0033】

ここで、送信元メールアドレス 7 0 1 は、電子メールのヘッダ内の F R O M に記載の送信元のメールアドレスを格納し、タイムスタンプ 7 0 2 は、この電子メールが到着した時

10

20

30

40

50

間を例えば1／100秒の桁まで格納し、宛先メールアドレス703は、電子メールのヘッダ内のTO、CC、BCCに記載の宛先のメールアドレスを格納し、添付ファイル704は、宛先メールアドレス703に応じて添付する添付ファイルを格納するフィールドである。上記のステップS305では、宛先のメールアドレス703に加え、送信元メールアドレス701及びタイムスタンプ702も対応させて格納される。

【0034】

次に、添付ファイル暗号化部13は、暗号鍵取得部14を介して上記のように宛先のメールアドレスに応じた暗号鍵の読み込み処理を行い（S306）、暗号鍵を読み込むことができたか否かを判断する（S307）。

【0035】

ステップS307で暗号鍵を読み込むことができたとは判断したとき、添付ファイル暗号化部13は、読み込んだ暗号鍵を用いて添付ファイルを暗号化して暗号化添付ファイルを作成し（S308）、暗号化添付ファイルを送信元メールアドレス701、タイムスタンプ702及び宛先メールアドレス703で特定されるレコード中の対応する添付ファイル704のフィールドに格納する（S309）。

【0036】

ここで、ステップS308で行う暗号化の方法は特に限定されないが、例えば、DES（Data Encryption Standard）暗号化方法、RSA公開鍵方式等の公開鍵を用いる暗号化方式等を暗号化に用いることができる。また、暗号化添付ファイルの宛先側で行われる復号化のために、例えば暗号化添付ファイルのアイコンをダブルクリック等して暗号入力

10

20

【0037】

ステップS307で暗号鍵を読み込むことができていないと判断したとき、又はステップS309で暗号化添付ファイルを格納したとき、添付ファイル暗号化部13は、アドレスカウンタcntが宛先のメールアドレスの総数Nと等しいか否かを判断し（S310）、等しいと判断したとき、処理は終了し、等しくないと判断したとき、アドレスカウンタcntを1増加させ（S311）、ステップS303から上記の処理を繰り返す。

【0038】

図8は、暗号化添付ファイル電子メール作成送信処理のうちの送信処理について説明するフローチャートである。まず、送信処理部16は、受信した電子メール中の宛先のメールアドレスの総数Nを取得して（S401）アドレスカウンタcntを1に、エラーカウンタerrorを0に設定する（S402）。

30

【0039】

次に、送信処理部16は、受信した電子メールから添付ファイルを削除して電子メール本体とする（S403）。添付ファイルの削除の方法は電子メールの構成によって異なるが、例えば、上記のMIMEの場合は、Content-Type内のboundary=以下の文字列が添付ファイル情報であるため、これを削除する。

【0040】

次に、送信処理部16は、電子メールからアドレスカウンタcntで特定される順番の宛先のメールアドレスを取得し（S404）、送信元のメールアドレスと宛先のメールアドレスとに基づいて対応する添付ファイルを添付ファイル格納部15から読み込む処理を行い（S405）、対応する添付ファイルを読み込むことができたか否かを判定する（S406）。

40

【0041】

ステップS406で添付ファイルを読み込むことができたとは判断したとき、送信処理部16は、電子メール本体をコピーすると共に読み込んだ添付ファイルを添付して送信可能電子メールを作成しこの宛先への電子メールとし（S407）、ステップS406で添付ファイルを読み込むことができていないと判断したとき、エラー処理として、添付ファイルを削除したこと及びその理由を電子メール本体に追記し、もって電子メールとし、読み

50

込むことができなかったレコードを記憶し（S 4 0 8）、エラーカウンタ e r r を 1 増加させる（S 4 0 9）。

【0 0 4 2】

図 9 は、エラー処理において電子メール本体に追記する内容の一例を示す図である。追記の内容として、図 9 に示すように、例えば、添付ファイルが削除されたこと、削除の理由および連絡先が少なくとも記載される。ここで、上記の連絡先は、本発明にかかる電子メール送信装置が適用されるシステムの管理者の連絡先等をいう。

【0 0 4 3】

ステップ S 4 0 7 で添付ファイルが添付された送信可能電子メールが作成されたとき、又は、ステップ S 4 0 9 でエラーカウンタ e r r が 1 増加されたとき、受信処理部 1 2 は、ステップ S 4 0 7 で添付ファイルが添付された送信可能電子メール又はステップ S 4 0 8 でエラー処理が施されて得られた電子メールを対応する宛先に送信する（S 4 1 0）。

【0 0 4 4】

次に、ステップ S 4 1 0 で電子メールを対応する宛先に送信したとき、送信処理部 1 6 は、アドレスカウンタ c n t が宛先のメールアドレスの総数 N と等しいか否かを判断し（S 4 1 1）、等しくないと判断したとき、アドレスカウンタ c n t を 1 増加させ（S 4 1 2）、ステップ S 4 0 4 以降の上記の処理を繰り返す。

【0 0 4 5】

ステップ S 4 1 1 でアドレスカウンタ c n t が宛先のメールアドレスの総数 N と等しいと判定したとき、送信処理部 1 6 は、エラーカウンタ e r r が 0 であるか否かを判定し（S 4 1 3）、0 であると判定したとき処理は終了し、0 でないと判定したときステップ S 4 0 8 で記憶したレコード番号からエラー処理対象の各宛先のメールアドレスを取得して送信元にエラーメールを送信する（S 4 1 4）。

【0 0 4 6】

図 1 0 は、エラーメールに記載する内容の一例を示す図である。エラーメールに記載する内容として、図 1 0 に示すように、例えば、電子メールの送信時刻、添付ファイルを削除して送信した宛先のメールアドレスのリスト、添付ファイルが削除されたこと、及び削除の理由が少なくとも記載される。

【図面の簡単な説明】

【0 0 4 7】

【図 1】本発明による電子メール送信装置の一実施例を模式的に示すブロック構成図である。

【図 2】受信処理部が行う処理について説明するフローチャートである。

【図 3】電子メールアドレスに基づいて暗号鍵を暗号鍵格納部から取得する処理例について説明するフローチャートである。

【図 4】暗号鍵格納部が暗号鍵を格納するレコードの構成を示す説明図である。

【図 5】暗号鍵格納部のほかに上記の外部のサーバにも暗号鍵を格納可能な構成における、図 3 に対応するフローチャートである。

【図 6】暗号化添付ファイル電子メール作成送信処理のうちの添付ファイル暗号化部が行う処理例について説明するフローチャートである。

【図 7】添付ファイル格納部が宛先のメールアドレスを格納するレコード構成の説明図である。

【図 8】暗号化添付ファイル電子メール作成送信処理のうちの送信処理について説明するフローチャートである。

【図 9】エラー処理において電子メール本体に追記する内容の一例を示す図である。

【図 1 0】エラーメールに記載する内容の一例を示す図である。

【符号の説明】

【0 0 4 8】

- 1 電子メール送信装置
- 2 暗号鍵格納部

10

20

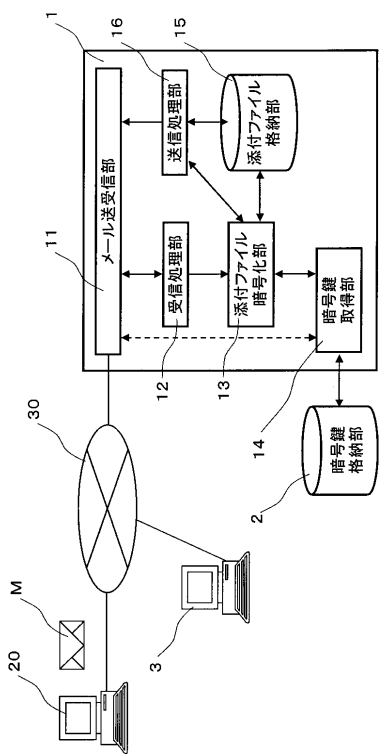
30

40

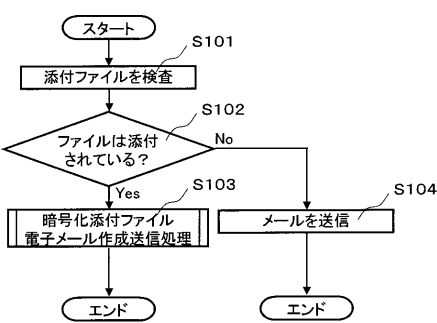
50

- 3 外部サーバ
- 1 1 メール送受信部
- 1 2 受信処理部
- 1 3 添付ファイル暗号化部
- 1 4 暗号鍵取得部
- 1 5 添付ファイル格納部
- 1 6 送信処理部
- 2 0 クライアント
- 3 0 ネットワーク
- 4 0 1 宛先のメールアドレス
- 4 0 2 暗号鍵
- 7 0 1 送信元メールアドレス
- 7 0 2 タイムスタンプ
- 7 0 3 宛先メールアドレス
- 7 0 4 添付ファイル
- M 電子メール

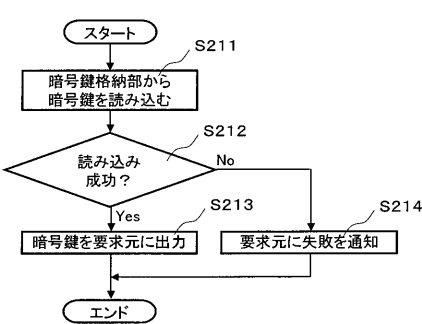
【図 1】



【図 2】



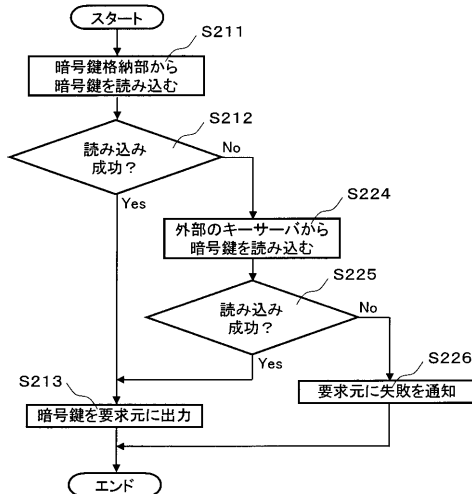
【図 3】



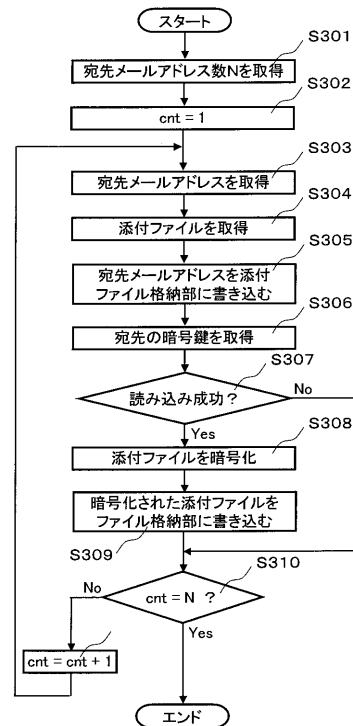
【図 4】

401 メールアドレス	402 暗号化鍵
abcdef@xxx.yyy.jp	ashfgoawufghil
:	:

【図 5】



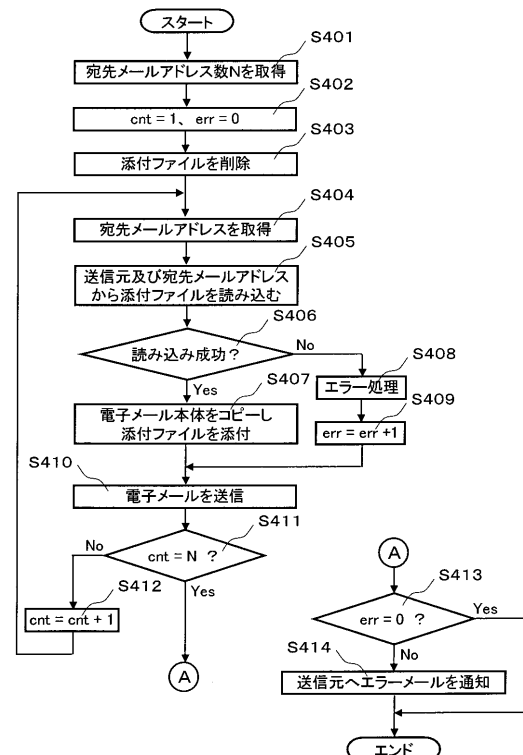
【図 6】



【図 7】

701	送信元メールアドレス	xxx@aaa.bbb.jp
702	タイムスタンプ	20061012091000
703	宛先メールアドレス	yyy@ooo.ppp.jp
704	添付ファイル	

【図 8】



【図 9】

<管理者からのお知らせ>
本メールは、受信者の暗号化キーを取得できなかったため、添付ファイルを削除してお送りしております。
添付ファイルが必要な場合は、送信元のメール管理者までお問い合わせください。
連絡先：mail_admin@xxx.yyy.jp

:
:

【図 10】

〇〇時△△分××秒に送信したメールは、下記のユーザへは添付ファイルを削除して送信しました（下記ユーザの暗号化キーを取得できなかったため）。

・ abcde@xxx.yyy.jp
・ fg hij@xxx.zzz.jp
・
宛先をご確認ください。