(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6643730号
(P6643730)
(45)発行日　令和2年2月12日(2020.2.12)　(24)登録日　令和2年1月9日(2020.1.9)

(51)Int.Cl.　　F I
H04L 12/58 (2006.01)　　H04L 12/58 100F
G06F 13/00 (2006.01)　　G06F 13/00 625

請求項の数 9　(全 27 頁)

(21)出願番号　特願2017-128337(P2017-128337)
(22)出願日　平成29年6月30日(2017.6.30)
(65)公開番号　特開2018-61232(P2018-61232A)
(43)公開日　平成30年4月12日(2018.4.12)
審査請求日　平成30年10月23日(2018.10.23)
(31)優先権主張番号　特願2016-194020(P2016-194020)
(32)優先日　平成28年9月30日(2016.9.30)
(33)優先権主張国・地域又は機関
日本国(JP)

(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　592135203
キヤノンＩＴソリューションズ株式会社
東京都港区港南２丁目１６番６号
(74)代理人　100189751
弁理士　木村　友輔
(72)発明者　白井　和明
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内
(72)発明者　岡本　力
東京都品川区東品川２丁目４番１１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】情報処理装置、情報処理システム、制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
クライアント端末から送信された電子メールを中継する情報処理装置であって、
受信した電子メールに付されたファイルが当該電子メールの本文に付されたものか否かを判定する判定手段と、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離することなく、
一方、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離手段と、
前記分離手段によって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する送信手段と、
を備えたことを特徴とする情報処理装置。
【請求項２】
前記分離手段は、前記判定手段によって、前記電子メールの本文に付されたファイルと、前記電子メールの本文に付されたものではないファイルと、が前記電子メールに付されていると判定した場合、当該電子メールの本文に付されたファイルを分離せず、一方、電子メールの本文に付されたものではないファイルを分離することを特徴とする請求項１に

記載の情報処理装置。
【請求項３】
前記判定手段は、前記受信した電子メールが有する当該電子メールに付されたファイルに関する情報に基づいて判定を行うことを特徴とする請求項１及び２に記載の情報処理装置。
【請求項４】
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該ファイルの暗号化を行わず、
一方、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該ファイルの暗号化を行う暗号化手段を備えたことを特徴とする請求項１乃至３の何れか１項に記載の情報処理装置。
【請求項５】
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該ファイルに対してフィルタリングを行うためのルールを適用せず、
一方、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定しない場合は、当該ファイルに対してフィルタリングを行うためのルールを適用する制御手段を備えたことを特徴とする請求項１乃至４の何れか１項に記載の情報処理装置。
【請求項６】
電子メールの送受信を行うクライアント端末と情報処理装置とがネットワークを介して接続された情報処理システムであって、
前記クライアント端末は、
前記電子メールの送信を行うクライアント送信手段、
を備え、
前記情報処理装置は、
前記クライアント送信手段によって送信された電子メールを受信する情報処理装置受信手段と、
前記情報処理装置受信手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものか否かを判定する判定手段と、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離することなく、
一方、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離手段と、
前記分離手段によって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する情報処理装置送信手段と、
を備えたことを特徴とする情報処理システム。
【請求項７】
クライアント端末から送信された電子メールを中継する情報処理装置の制御方法であって、
前記情報処理装置は、
受信した電子メールに付されたファイルが当該電子メールの本文に付されたものか否かを判定する判定ステップと、
前記判定ステップによって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離す

ることなく、
一方、
前記判定ステップによって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離ステップと、
前記分離ステップによって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する送信ステップと、
を実行することを特徴とする情報処理装置の制御方法。
【請求項８】
クライアント端末から送信された電子メールを中継する情報処理装置で読み取り実行可能なプログラムであって、
前記情報処理装置を、
受信した電子メールに付されたファイルが当該電子メールの本文に付されたものか否かを判定する判定手段と、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離することなく、
一方、
前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離手段と、
前記分離手段によって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する送信手段と、
して機能させるためのプログラム。
【請求項９】
電子メールの送受信を行うクライアント端末と情報処理装置とがネットワークを介して接続された情報処理システムであって、
前記クライアント端末は、
前記電子メールの送信を行うクライアント送信ステップ、
を実行し、
前記情報処理装置は、
前記クライアント送信ステップによって送信された電子メールを受信する情報処理装置受信ステップと、
前記情報処理装置受信ステップによって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものか否かを判定する判定ステップと、
前記判定ステップによって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離することなく、
一方、
前記判定ステップによって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離ステップと、
前記分離ステップによって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する情報処理装置送信ステップと、
を実行することを特徴とする情報処理システムの制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メールに添付されたファイルの誤送信防止に関するものである。
【背景技術】

【０００２】
近年、電子メールシステムでは、ネットワークを介して、クライアント端末間での電子メールの送受信が行われているが、遠方と情報をかわす上では、非常に利便性の高いツールとして、利用されている。
【０００３】
しかしながら、緊急時など、電子メールに機密性の高い情報を含ませて、相手先とやり取りを行うケースも度々発生し、この場合、送信された電子メールが、相手先のメールサーバへ送信される過程で、盗聴や改竄等が行われ、機密性の高い情報を安全に送信することができない、というリスクを抱えてしまう。
【０００４】
そこで、電子メールを暗号化する手法が幾つも提案され、例えば、ＰＧＰ（Pretty Good Privacy）やS／MIME（Secure/Multipurpose Internet Mail Extensions）等の方法が提案されているが、これらの方法は、送受信側の双方で暗号化、複合化を行うことで、前述のようなリスクを回避している。
【０００５】
このような手法を用いるには、各クライアント端末に対して、暗号化、及び複合化を行うための機能を提供するソフトウェアを導入する必要があり、これらのソフトウェアの導入の検討（費用や安全性等）、導入作業、及び導入後設定作業等、利用者にとっては、いささか不便な点があることは否めない。
【０００６】
しかしながら、電子メールの利用方法として、電子メールの本文には、機密性の低い、あるいは、ない情報を入力し、機密性の高い情報を含むファイルを電子メールに添付して送信する方法がある。
【０００７】
この場合、前述の手法のように、電子メールを全て暗号化する必要性は少なく、電子メールに添付されたファイルを分離して、ファイル保管用のサーバ等へ保管して置き、その保管先に係るＵＲＬを、ファイルを分離した電子メールへ貼り付けて送信先へ当該電子メールを送信する。
【０００８】
そして、電子メールを受信したユーザは、ＵＲＬにアクセスして、パスワード等を入力してファイル保管用のサーバへログインがなされると、自身に送付される予定であったファイルをダウンロードする仕組みが存在する（例えば、特許文献１参照）。
【特許文献１】特開２００７－２５１５５４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
しかしながら、電子メールに添付されるファイルとしては、電子メールに対して、ファイルをそのまま添付するものもあれば、電子メールの背景、会社のロゴ等の画像を組み込まれるものがある。
【００１０】
この場合、電子メールの背景、会社のロゴ等の画像についてまで、電子メールから分離して、受信者がダウンロードを行うことは、受信者にとっての手間になりかねない。
【００１１】
本発明は、上記の課題を解決するためになされたものであり、添付ファイルが存在する電子メールの中継を柔軟に行うことが可能な情報処理装置、情報処理システム、制御方法、及びプログラ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】
【００１２】
上記の目的を達成するための本発明は、クライアント端末から送信された電子メールを中継する情報処理装置であって、受信した電子メールに付されたファイルが当該電子メー

ルの本文に付されたものか否かを判定する判定手段と、前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものであると判定した場合は、当該電子メールから添付ファイルを分離することなく、一方、前記判定手段によって受信した電子メールに付されたファイルが当該電子メールの本文に付されたものではないと判定した場合は、当該電子メールから添付ファイルを分離する分離手段と、前記分離手段によって添付ファイルを分離した電子メールあるいは添付ファイルを分離していない電子メールを送信する送信手段と、を備えたことを特徴とする。

【発明の効果】

【００１３】

本発明によれば、添付ファイルが存在する電子メールの中継を柔軟に行うことができる、という効果を奏する。

【図面の簡単な説明】

【００１４】

【図１】情報処理システムの概略構成を示す構成図である。

【図２】各種端末のハードウェアの概略構成を示す構成図である。

【図３】情報処理システムにおける機能構成を示す構成図である。

【図４】電子メールの添付ファイルを分離する処理を示すフローチャートである。

【図５】メール作成画面の構成を示す構成図である。

【図６】メール作成画面の構成を示す構成図である。

【図７】電子メールの構成を示す構成図である。

【図８】電子メールの構成を示す構成図である。

【図９】ＵＲＬが付された電子メールの構成を示す構成図である。

【図１０】パスワード通知用メールの構成を示す構成図である。

【図１１】ＵＲＬが付された電子メールの構成を示す構成図である。

【図１２】電子メールの構成を示す構成図である。

【図１３】情報処理システムにおける機能構成を示す構成図である。

【図１４】電子メールの添付ファイルを暗号化、分離する処理を示すフローチャートである。

【図１５】電子メールの構成を示す構成図である。

【図１６】電子メールの構成を示す構成図である。

【図１７】電子メールの構成を示す構成図である。

【図１８】電子メールの構成を示す構成図である。

【発明を実施するための形態】

【００１５】

以下、図面を参照して、本発明の実施形態を詳細に説明する

【００１６】

［第１の実施形態］

図１は、本発明の実施形態に係る情報処理システムにおけるシステム構成の一例を示す図である。尚、図１に示す各種端末の構成は一例であり、目的や用途に応じて様々な構成例があることは言うまでもない。

【００１７】

図１に示すように、本実施形態に係る情報処理システム１００には、クライアント端末１０１、システム管理者が利用する管理者用クライアント端末１０２、内部メールサーバ１０４、ＮＦＳサーバ１０５、及びＷｅｂサーバ１０６が設置されており、それら端末は、ローカルエリアネットワーク（ＬＡＮ）１０３を介して相互に通信可能に接続されており、内部システムとして構築されている。

【００１８】

また、クライアント端末１０１は、広域ネットワーク１０７を介して、少なくとも１以上の外部メールサーバ１０８と相互に通信可能に接続されており、外部のシステムに存在するクライアント端末１０９と電子メールの送受信を中継している。

【００１９】
　また、ＬＡＮ１０３と広域ネットワーク１０７との間には不図示のファイアウォール装置が設置されており、あらかじめ決められた規則に従った通信制御処理が行われている。
【００２０】
　内部メールサーバ１０４は、クライアント端末１０１による電子メール中継のためのサーバ装置であり、クライアント端末１０１のＳＭＴＰ通信内容を特定し、その通信内容に応じて後述する各種の処理を行うことになる。
【００２１】
　尚、内部メールサーバ１０４は、１つの筐体として図示しているが、このような構成に限らず、メールサーバと、当該メールサーバに対して外部側へ配置されたプロキシサーバとのそれぞれの筐体を備える構成として、本発明をプロキシサーバで実行させ、メールサーバでは、電子メールの配送を主に担うような構成をとっても良い。
【００２２】
　管理者用クライアント端末１０２は、内部メールサーバ１０４の設定、管理を行うことになる。
【００２３】
　ＮＦＳサーバ１０５は、内部メールサーバ１０４において中継した電子メールに添付されたファイルを所定のディレクトリに保存する。
【００２４】
　尚、添付ファイルの分離が行われるごとに添付ファイルを格納するためにディレクトリが作成され、このディレクトリの配下に添付ファイルが保存される。また、添付ファイルの分離が行われた電子メールを保存するための領域をも備えている。
【００２５】
　Ｗｅｂサーバ１０６は、電子メールの送信先から、ＮＦＳサーバ１０５に保存された添付ファイルのダウンロードの要求を受付けると、ＮＦＳサーバ１０５において取得された該当の添付ファイルを要求元へ送信する。
【００２６】
　次に、図１に示す内部メールサーバ１０４の各種端末のハードウェア構成について、図２を用いて説明する。尚、クライアント端末１０１、管理者用クライアント端末１０２、ＮＦＳサーバ１０５、及びＷｅｂサーバ１０６についても同様な構成を備えるため説明は省略する。
【００２７】
　ＣＰＵ２０１は、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０２あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ(Basic Input / Output System)やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各クライアント装置の実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。
【００２８】
　ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＡＭ２０３にロードして、プログラムを実行することで各種動作を実現するものである。
【００２９】
　また、入力コントローラ（入力Ｃ）２０５は、キーボードや不図示のマウス等のポインティングデバイスを示す入力部２０９からの入力を制御する。ビデオコントローラ（ＶＣ）２０６は、ＣＲＴディスプレイ（ＣＲＴ）２１０等の表示器への表示を制御する。表示器はＣＲＴだけでなく、液晶ディスプレイでも構わない。
【００３０】
　メモリコントローラ（ＭＣ）２０７は、ブートプログラム、ブラウザソフトウエア、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、各種データ等を記憶するハードディスク（ＨＤ）やフロッピーディスク（登録商標　ＦＤ）或いはＰＣ

ＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。

【００３１】

通信Ｉ／Ｆコントローラ（通信Ｉ／ＦＣ）２０８は、ネットワークを介して、外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いたインターネット通信等が可能である。

【００３２】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０３内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ディスプレイ装置２１０上での表示を可能としている。また、ＣＰＵ２０１は、ディスプレイ装置２１０上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【００３３】

本発明を実現するためのパスワード通知メールの送信処理を実行するためのプログラム等は、外部メモリ２１１に記憶されており、必要に応じてＲＡＭ２０３にロードされることによりＣＰＵ２０１によって実行される。

【００３４】

本発明に係わる各処理が用いる定義情報及び各種情報テーブルについても、外部メモリ２１１に記憶されている。これらについての詳細な説明は、後述する。

【００３５】

図３は、情報処理システム１００に係る機能構成を示す模式図であり、各々の機能に関して概要を説明する。尚、この模式図に限らず図４に示すフローチャートと合わせて、各機能内容を説明する。

【００３６】

図３に示すように、クライアント端末１０１は、第１クライアント送信手段３０１を備えており、第１クライアント送信手段３０１は、ＬＡＮ１０３を介して、内部メールサーバ１０４と接続されている。

【００３７】

第１クライアント送信手段３０１は、電子メールを送信指示するためのソフトウェアによって実現される機能を備えており、例えば、図５に示すメール作成画面５００を、ディスプレイ装置２１０に表示し、差出人５０１には、電子メールの送信元アドレスが表示され、ユーザは、入力部２０９を用いて、電子メールの送信先アドレスを示す宛先５０２、及びＣＣ（Carbon Copy）５０３、電子メールのタイトルを示す件名５０４、電子メールに対して添付されたファイルを示す添付ファイル５０５、電子メール本文５０６等に対して、入力あるいは添付等を行う。

【００３８】

そして、ユーザは、電子メールを送信するにあたり、メール作成画面５００に備えられた送信ボタン５０７を押下することで、入力部２０９を用いて作成した電子メールを、宛先５０２及びＣＣ５０３に設定された送信先アドレスへ送信する。

【００３９】

また、メール作成画面５００は、添付ボタン５０８を備えており、ユーザは、添付ファイル５０５を電子メールに添付する際に、添付ボタン５０８を押下することにより、クライアント端末１０１に存在するファイルを指定するための画面（不図示）をディスプレイ装置２１０に表示し、当該画面に表示されたファイルから入力部２０９を用いて選択指定することで、添付対象となるファイルを電子メールへ添付する。

【００４０】

また、メール作成画面５００は、図６に示すように、ユーザがHTMLベースで電子メールを作成した場合、ユーザ自身が所有する画像を、電子メールの背景とする画像５０９として、あるいは、自社のロゴ等を示すような画像５１０として、電子メールの本文へ挿入することが可能である。

【００４１】

さらに、図６に示すメール作成画面５００の場合、前述のような画像を挿入することによる添付ファイルとあわせて、電子メールに対して添付することも可能であり、例えば、ユーザが選択したファイルを、添付ファイル５０５として、電子メールへ添付することが可能である。

【００４２】

クライアント端末１０１は、第１クライアント受信手段３０２を備えており、第１クライアント受信手段３０２は、ＬＡＮ１０３を介して、内部メールサーバ１０４と接続されている。

【００４３】

第１クライアント受信手段３０２は、内部システムに存在するクライアント端末１０１や内部システム以外の外部システムに存在するクライアント端末から、内部メールサーバ１０４を介して、電子メールの受信を行う。

【００４４】

内部メールサーバ１０４は、サーバメール受信手段３０３を備えており、サーバメール受信手段３０３は、クライアント端末１０１や、広域ネットワーク１０７を介して、少なくとも１以上の外部メールサーバ１０８と接続されている。

【００４５】

サーバメール受信手段３０３は、内部システムに存在するクライアント端末１０１や内部システム以外の外部システムに存在するクライアント端末１０９から電子メールの受信を行う。

【００４６】

内部メールサーバ１０４は、分離判定手段３０４、添付ファイル抽出手段３０５、添付ファイル記憶要求手段３０６、メール生成手段３０７、パスワード通知メール生成手段３０８、サーバメール送信手段３０９、及び元メール記憶手段３１０を備えている。

【００４７】

分離判定手段３０４は、サーバメール受信手段３０３、及び添付ファイル抽出手段３０５に接続されている。

【００４８】

分離判定手段３０４は、サーバメール受信手段３０３において電子メールを受信した旨の通知を受け取ると、当該電子メールの内容を解析するが、解析内容の概要としては、電子メールから分離される対象となる添付ファイルが存在する電子メールであれば、フィルタリングの対象とする。

【００４９】

電子メールに添付ファイルが存在するか否かの判定方法の例として、図７に示す電子メールの構成図を用いて説明する。尚、これらの各パートは、電子メールのヘッダー情報として存在するものである（以下、同様）。

【００５０】

図７の上段に示す電子メールは、各パートに区分けされており、電子メールの構成、例えば、当該電子メールが、multipart形式、text形式、HTML形式等を表わすパート６００、電子メールの本文に対応するパート６０２、添付ファイルに対応するパート６０４、もう一つの添付ファイルに対応するパート６０６を備えている。

【００５１】

本例では、multipart形式の電子メールにおいて、ユーザがtextベースで電子メールを作成し、２つの添付ファイルが存在することを示している。

【００５２】

図７の下段に示す電子メールは、multipart形式の電子メールにおいて、ユーザがHTMLベースで電子メールを作成した際の構成であり、text形式の本文に対応するパート６０８とHTML形式の本文に対応するパート６１０、添付ファイルに対応するパート６１２、もう一方の添付ファイルに対応するパート６１４の構成を備えている。

【００５３】

このような構成を備えた電子メールにおいて、添付ファイルに対応するパート６０４、パート６０６、パート６１２、及びパート６１４におけるfilenameに値が設定されている場合、添付ファイルが電子メールに存在するものとして判定される。

【００５４】

しかしながら、この判定を行うことで、ユーザがHTMLベースで電子メールを作成する際に、ユーザ自身が所有する画像を電子メール自身に挿入して作成した場合、これらの画像が電子メールの背景画像や会社のロゴを示す画像であって、機密性の低い画像である場合であっても、前述したfilenameに値が設定されるケースが存在することからも、本来、分離対象としなくても良いような添付ファイルも、分離対象としてしまうという問題が生じ得る。

【００５５】

そこで、電子メールに添付したファイルを示す添付ファイルと、電子メールに挿入された画像を示す添付ファイルとを識別するために、図８に示す電子メールの構成図を用いて説明する。

【００５６】

図８に示す電子メールは、multipart形式の電子メールにおいて、ユーザがHTMLベースで電子メールを作成した際の構成であり、図７の下段に示す電子メールと同様な構成を備えるが、パート６１４が異なる。

【００５７】

パート６１４に示されるように、図８の例では、ContentIDが設定されており、このContentIDが設定されているパートの場合、この添付ファイルは、filenameに値が設定されている場合であっても、電子メールの本分に挿入された画像を示す添付ファイルに限定される。

【００５８】

したがって、ContentIDが設定されているか否かによって、電子メールの本分に挿入された画像を示す添付ファイルであるか否かの判定を行うことが可能となる。

【００５９】

添付ファイル抽出手段３０５は、分離判定手段３０４、及び添付ファイル記憶要求手段３０６に接続されている。

【００６０】

添付ファイル抽出手段３０５は、分離判定手段３０４によって、電子メールから分離対象となる添付ファイルが存在する旨の通知を受取ると、当該電子メールから添付ファイルを取得する。

【００６１】

添付ファイル記憶要求手段３０６は、添付ファイル抽出手段３０５、添付ファイル記憶手段３１１、及びメール生成手段３０７に接続されている。

【００６２】

添付ファイル記憶要求手段３０６は、添付ファイル抽出手段３０５によって添付ファイルが分離された旨の通知を受取ると、ＮＦＳサーバ１０５に対してこの分離したファイルを記憶することを要求する。

【００６３】

メール生成手段３０７は、添付ファイル記憶要求手段３０６、及びパスワード通知メール生成手段３０８に接続されている。

【００６４】

メール生成手段３０７は、添付ファイル記憶要求手段３０６によって添付ファイルの記憶がなされると、添付ファイルが分離された電子メールに対して、Ｗｅｂサーバ１０６を介してＮＦＳサーバ１０５に記憶された添付ファイルを取得するためのシステムに接続するためのＵＲＬを付与する。

【００６５】

その例を図９及び図１１に示す。図９に示す電子メール８００は、図５に示すメール作

成画面５００で作成された電子メールに基づくものであり、電子メールの送信元アドレスを示す差出人８０１、電子メールの送信先アドレスを示す宛先８０２、ＣＣ（Carbon Copy）８０３、電子メールのタイトルを示す件名８０４、電子メール本文に対して新たに挿入したメッセージ８０５、前述したＵＲＬ８０６、及び元の電子メールの本文８０７を備えている。

【００６６】

一方、図１１に示す電子メール８００は、図６に示すメール作成画面５００で作成された電子メールに基づくものであり、電子メールの送信元アドレスを示す差出人８０１、電子メールの送信先アドレスを示す宛先８０２、ＣＣ（Carbon Copy）８０３、電子メールのタイトルを示す件名８０４、電子メール本文に対して新たに挿入したメッセージ８０５、前述したＵＲＬ８０６、及び元の電子メールの本文８０７、元のメールの画像５０９及び画像５１０に対応する画像８０８及び画像８０９を備えている。

【００６７】

つまり、添付ファイル５０５に表示される添付ファイルは、電子メールから分離されて、ＵＲＬが付され、電子メールの本文に挿入された画像５０９及び画像５１０は、電子メールから分離されることなく送信先で当該電子メールが送信される。

【００６８】

パスワード通知メール生成手段３０８は、メール生成手段３０７、及びサーバメール送信手段３０９に接続されている。

【００６９】

パスワード通知メール生成手段３０８は、メール生成手段３０７によって生成した電子メールを送信先に送信した後、その電子メールを受取ったユーザが、前述したＵＲＬによってＮＦＳサーバ１０５にアクセスする際に、パスワード等の入力を要求するため、その入力の際に必要となるパスワード等の情報を通知するための電子メールを生成する。

【００７０】

その例を図１０に示す。図１０に示すパスワード通知用メール９００は、メール作成画面５００で作成された電子メールに基づくものであり、電子メールの送信元アドレスを示す差出人９０１、電子メールの送信先アドレスを示す宛先９０２、及びＣＣ（Carbon Copy）９０３、電子メールのタイトルを示す件名９０４、前述したパスワード等の情報（宛先のメールアドレス、電子メールのＩＤ、パスワード等）を示すメッセージ９０５を備えている。

【００７１】

このパスワード等の情報については、ＮＦＳサーバ１０５の所定の領域に記憶しておき、ユーザからのＮＦＳサーバ１０５へのアクセス時に用いられる。

【００７２】

サーバメール送信手段３０９は、クライアント端末１０１や、広域ネットワーク１０７を介して、少なくとも１以上の外部メールサーバ１０８と接続されている。

【００７３】

詳細には、サーバメール送信手段３０９は、メール生成手段３０７、パスワード通知メール生成手段３０８、第１クライアント受信手段３０２、及び第２クライアント受信手段３１３に接続されている。

【００７４】

サーバメール送信手段３０９は、メール生成手段３０７によって電子メールが生成された旨の通知を受けると、宛先に対して、当該電子メールを送信する。また、パスワード通知メール生成手段３０８によってパスワード通知用メールが生成された旨の通知を受けると、まず、差出人に対して、当該パスワード通知用メールを送信し、所定時間経過した後、宛先に対して、当該電子メールを送信する。

【００７５】

元メール記憶手段３１０は、サーバメール受信手段３０３に接続されており、サーバメール受信手段３０３によって受信した電子メールを記憶する。

【００７６】
ＮＦＳサーバ１０５は、添付ファイル記憶手段３１１、及び添付ファイル取得手段３１２を備えている。
【００７７】
添付ファイル記憶手段３１１は、添付ファイル記憶要求手段３０６、及び添付ファイル取得手段３１２に接続されており、添付ファイル記憶要求手段３０６から添付ファイルを記憶することの要求を受付けると、添付ファイルを格納するためにディレクトリを作成して、このディレクトリの配下に添付ファイルを記憶する。
【００７８】
尚、前述したように、添付ファイルの分離が行われるごとに添付ファイルを格納するためにディレクトリが作成され、また、メール生成手段３０７で生成した電子メールを保存するための領域に当該電子メールをも保存する。
【００７９】
添付ファイル取得手段３１２は、添付ファイル記憶手段３１１、添付ファイル受付手段３１６、及び添付ファイル送信手段３１７に接続されている。
【００８０】
添付ファイル取得手段３１２は、ＵＲＬが付された電子メールを受取ったクライアント端末１０９から、添付ファイルのダウンロードの要求を添付ファイル受付手段３１６から受付けると、添付ファイル記憶手段３１１に記憶している要求された添付ファイルを取得して、添付ファイル送信手段３１７に当該添付ファイルを出力する。
【００８１】
クライアント端末１０９は、第２クライアント受信手段３１３、添付ファイル要求手段３１４、及び添付ファイル受信手段３１５を備えている。
【００８２】
第２クライアント受信手段３１３は、サーバメール送信手段３０９に接続されており、電子メールやパスワード通知用メールを受信する。
【００８３】
添付ファイル要求手段３１４は、添付ファイル受付手段３１６に接続されており、ユーザが電子メールに添付されたＵＲＬをクリックすると、添付ファイル受付手段３１６は、ユーザに対して画面（不図示）を表示し、パスワード通知用メールで通知したメッセージ９０５に係る情報の入力をユーザへ要求する。
【００８４】
入力された情報と、ＮＦＳサーバ１０５の所定の領域に記憶されたパスワード等の情報とを比較して、一致すると認証がなされる。
【００８５】
そして認証がなされると、当該ユーザが参照可能な添付ファイルが画面（不図示）に表示され、ユーザがダウンロードを望む添付ファイルを指定して、ダウンロード実行の要求を受付ける。
【００８６】
添付ファイル受信手段３１５は、添付ファイル送信手段３１７に接続されており、ＮＦＳサーバ１０５で取得した添付ファイルを添付ファイル送信手段３１７から受信する。
【００８７】
Ｗｅｂサーバ１０６は、添付ファイル受付手段３１６、及び添付ファイル送信手段３１７を備えている。
【００８８】
添付ファイル受付手段３１６は、添付ファイル要求手段３１４、及び添付ファイル取得手段３１２に接続されている。
【００８９】
前述したように、添付ファイル受付手段３１６は、添付ファイル要求手段３１４から添付ファイルのダウンロードの要求を受付けると、添付ファイル取得手段３１２にその旨を

通知する。
【００９０】
添付ファイル送信手段３１７は、添付ファイル取得手段３１２、及び添付ファイル受信手段３１５に接続されている。
【００９１】
添付ファイル送信手段３１７は、添付ファイル取得手段３１２において取得された添付ファイルを、当該添付ファイルを要求した添付ファイル受信手段３１５に対して送信する。
【００９２】
図４には、本発明の実施形態に係る情報処理システムにおける電子メールの添付ファイルを分離する処理を表すフローチャートが示されている。尚、各ステップで実行される処理については、内部メールサーバ１０４のＣＰＵ２０１の制御の下、処理が実行される。
【００９３】
ステップＳ４０１では、サーバメール受信手段３０３は、クライアント端末１０１の第１クライアント送信手段３０１によって送信された電子メールを受信し、ステップＳ４０２では、分離判定手段３０４は、ステップＳ４０１によって受信した電子メールに分離する対象となる添付ファイルが存在するか否かを判定する。
【００９４】
この判定を行うには、前述したように、添付ファイルに対応するパートを参照し、filenameに値が設定されている場合、添付ファイルが存在するものとするが、さらに、ContentIDが設定されている場合、この添付ファイルは、filenameに値が設定されている場合であっても、画像を示す添付ファイルであるとして、添付ファイルが存在しないものとして判定を行う。
【００９５】
さらに、図６に示すメール作成画面５００によって、前述のような画像を挿入することによる添付ファイルとあわせて、電子メールに対して添付する場合、例えば、ユーザが選択したファイルを、添付ファイル５０５として、電子メールへ添付する場合、画像を挿入することによる添付ファイルについては、分離対象の添付ファイルと見做さず、電子メールに対して添付した添付ファイルに対しては、分離対象の添付ファイルとして見做す。
【００９６】
添付ファイルが存在すると判定した場合、ステップＳ４０３へ処理を進め、添付ファイルが存在すると判定しない場合、ステップＳ４１２へ処理を進める。
【００９７】
ステップＳ４０３では、添付ファイル抽出手段３０５は、電子メールから分離対象となる添付ファイルを取得し、添付ファイル記憶要求手段３０６は、添付ファイルをＮＦＳサーバ１０５に記憶するため、添付ファイル記憶手段３１１に対して添付ファイルを記憶することを要求し、添付ファイル記憶手段３１１は、当該添付ファイルをＮＦＳサーバ１０５に記憶する。
【００９８】
ステップＳ４０４では、メール生成手段３０７は、添付ファイルを分離した電子メールであって、Ｗｅｂサーバ１０６を介してＮＦＳサーバ１０５に記憶された添付ファイルを取得するためにシステムへ接続するためのＵＲＬが付与された電子メールを生成する。例えば、図９あるいは図１１に示す電子メールを生成する。
【００９９】
ステップＳ４０５では、サーバメール送信手段３０９は、クライアント端末１０９の第２クライアント受信手段３１３に対して、ステップＳ４０４において生成した電子メールを送信する。
【０１００】
さらに、ＮＦＳサーバ１０５の所定の領域に対して、ステップＳ４０４において生成した電子メールを記憶することも可能である。

【０１０１】
ステップＳ４０６では、パスワード通知メール生成手段３０８は、電子メールの送信先となるユーザが当該電子メールに付されたＵＲＬをクリックすることによってＮＦＳサーバ１０５にアクセスする際に、パスワード等の入力を要求するため、その入力の際に必要となるパスワード等の情報を通知するためパスワード通知用メールを生成する。例えば、図１０に示す電子メールであり、宛先には、元の電子メールの送信元のメールアドレスを設定する。
【０１０２】
ステップＳ４０７では、サーバメール送信手段３０９は、ステップＳ４０６において生成したパスワード通知用メールをクライアント端末１０１の第１クライアント受信手段３０２へ送信する。
【０１０３】
ステップＳ４０８では、パスワード通知メール生成手段３０８は、ステップＳ４０６において、パスワード通知用メールを送信してから所定時間経過したか否かを判定し、所定時間経過したと判定したらステップＳ４０９へ処理を進める。
【０１０４】
ステップＳ４０９では、パスワード通知メール生成手段３０８は、ステップＳ４０６と同様に、パスワード通知用メールを生成するが、この場合、例えば、図１０に示す電子メールを生成する。宛先には、ステップＳ４０６とは異なり、元の電子メールの送信先のメールアドレスが設定される。
【０１０５】
ステップＳ４１０では、サーバメール送信手段３０９は、ステップＳ４１０において生成したパスワード通知用メールをクライアント端末１０９の第２クライアント受信手段３１３へ送信する。
【０１０６】
ステップＳ４１１では、元メール記憶手段３１０は、ステップＳ４０１において受信した電子メールを内部メールサーバ１０４の所定領域へ記憶する。
【０１０７】
ステップＳ４１２では、サーバメール送信手段３０９は、ステップＳ４０１において受信した電子メールをクライアント端末１０９の第２クライアント受信手段３１３へ送信する。
【０１０８】
尚、本実施形態では、添付ファイルに対応するパートを参照し、filenameに値が設定されている場合、添付ファイルが存在するものとし、さらに、ContentIDが設定されている場合、この添付ファイルは、filenameに値が設定されている場合であっても、画像を示す添付ファイルであるとして、添付ファイルが存在しないものとして判定を行っている。
【０１０９】
この判定方法よりも、より正確に判定を行うため、添付ファイルに対応するパートを参照し、filenameに値が設定されており、Content-Typeが添付ファイルが画像を示す添付ファイルである種別であり、さらに、ContentIDが設定されている時に、画像を示す添付ファイルであるとして、添付ファイルが存在しないものとして判定を行っても良い。尚、この場合、Content-Typeには、例えば、image/*といった画像を示す値が設定されている。
【０１１０】
この判定例として、図１２に示す電子メールの構成において、添付ファイルに対応するパート６１６、６１８、６２０、及び６２２において、全てのパートにおけるfilenameに値が設定されているが、パート６１６及びパート６１８には、ContentIDが設定されておらず、電子メールに添付したファイルを示す添付ファイルが存在すると判定し、一方、パート６２０及びパート６２２には、ContentIDが設定されているため、電子メールに挿入された画像を示す添付ファイルが存在するとして、添付ファイルが存在しないものとして判定する。

【０１１１】
尚、先述したように、より正確に判定を行うため、全てのパートに対して、Content-Typeにimage/*の値が設定されていることを条件として判定を行っても良い。
【０１１２】
また、ユーザがHTMLベースで電子メールを作成した場合、スタイルシート（ＣＳＳ）を用いて、電子メールを装飾する場合がある。
【０１１３】
この場合も、装飾自身は、機密性が低いにもかかわらず、電子メールにスタイルシートが組み込まれているため、filenameに値が設定されていることから、分離対象と見做してしまう。
【０１１４】
そこで、同様に、添付ファイルに対応するパートを参照し、filenameに値が設定され、さらに、ContentIDが設定されている場合、分離対象と見做さないことで、スタイルシートを分離してしまうことを防ぐことができる。
【０１１５】
また、前述したように、より正確に判定を行うために、Content-Typeをも参照し、Content-Typeに、text/cssといったスタイルシートを示す値が設定されていることを条件に判定を行っても良い。
【０１１６】
同様に、この判定例として、図１２に示す電子メールの構成において、添付ファイルに対応するパート６２４には、ContentIDが設定されているため、分離対象外となる。
【０１１７】
さらに、Content-Typeを参照すると、text/cssが設定されているので、このパート６２４は、スタイルシートに関するものであるため、分離対象としないとして判定することができる。
【０１１８】
尚、ステップＳ４０２において、分離対象となる添付ファイルが存在しない場合、ステップＳ４１２の処理の前において、電子メールに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。
【０１１９】
保留した際は、監査者によって承認がなされた後、ステップＳ４１２の処理を行っても良い。
【０１２０】
また、分離対象となる添付ファイルが存在する場合にも、ステップＳ４０３の後、添付ファイルが分離された電子メール及び当該添付ファイルに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。
【０１２１】
保留した際は、監査者によって承認がなされた後、ステップＳ４０４の処理を行っても良い
【０１２２】
［第２の実施形態］
次に、第２の実施形態について説明するが、第１の実施形態では、添付ファイルに対して、分離対象となるか否かを判定したが、第２の実施形態では、添付ファイルに対して、暗号化の対象となるか否かを判定する。
【０１２３】
尚、第２の実施形態における構成及び処理は、第１の実施形態とほぼ同様な構成及び処理を行うため、同一の構成及び処理については説明を省略し、同一の符号を用いて説明を行う。

【０１２４】
図１３は、情報処理システム１００に係る機能構成を示す模式図であり、各々の機能に関して概要を説明する。尚、この模式図は、図３を改良したものである。
【０１２５】
図３と異なる点は、内部メールサーバ１０４が、暗号化判定手段３１８、及び暗号化手段３１９を備えている点である。
【０１２６】
暗号化判定手段３１８は、サーバメール受信手段３０３と添付ファイル抽出手段３０５と接続されており、サーバメール受信手段３０３において電子メールを受信した旨の通知を受け取ると、当該電子メールの内容を解析するが、解析内容の概要としては、電子メールに暗号化対象となる添付ファイルが存在する電子メールであれば、フィルタリングの対象とする。
【０１２７】
電子メールに暗号化対象となる添付ファイルが存在するか否かの判定方法としては、第１の実施形態で記載した方法と同様な方法をとり、第２の実施形態では、第１の実施形態では分離対象となる添付ファイルが存在する場合を暗号化対象となる添付ファイルが存在する場合とし、一方、第１の実施形態では分離対象となる添付ファイルが存在しない場合を暗号化対象とする添付ファイルが存在しない場合として判定している。
【０１２８】
そして、添付ファイル抽出手段３０５は、暗号化判定手段３１８によって、電子メールから暗号化対象となる添付ファイルが存在する旨の通知を受取ると、当該電子メールから添付ファイルを取得する。
【０１２９】
暗号化手段３１９は、添付ファイル抽出手段３０５とメール生成手段３０７と接続されており、暗号化判定手段３１８によって暗号化対象となる添付ファイルに対して暗号化を行うとともに、複合するためのパスワードを発行する。
【０１３０】
メール生成手段３０７は、暗号化手段３１９によって添付ファイルの暗号化がなされると、暗号化された添付ファイルを電子メールへ添付する。
【０１３１】
パスワード通知メール生成手段３０８は、メール生成手段３０７によって生成した電子メールを送信先に送信した後、暗号化手段３１９によって発行したパスワードを通知するための電子メールを生成する。
【０１３２】
サーバメール送信手段３０９は、メール生成手段３０７によって電子メールが生成された旨の通知を受けると、宛先に対して、当該電子メールを送信し、パスワード通知メール生成手段３０８によってパスワード通知用メールが生成された旨の通知を受けると、差出人か宛先、あるいは双方に対して、当該パスワード通知用メールを送信する。
【０１３３】
尚、受信した電子メールに対して、分離判定手段３０４によって判定を行うか、暗号化判定手段３１８によって判定を行うかは、予め何れの判定を用いるかを設定しておいても良いし、送信先に応じて、何れの判定を行うかを決定しても良い。
【０１３４】
図１４には、本発明の実施形態に係る情報処理システムにおける電子メールの添付ファイルに対するする処理を表すフローチャートが示されている。尚、各ステップで実行される処理については、内部メールサーバ１０４のＣＰＵ２０１の制御の下、処理が実行される。
【０１３５】
ステップＳ４２０では、サーバメール受信手段３０３は、ステップＳ４０１によって受信した電子メールに対して、分離判定を行うか、あるいは暗号化判定を行うかを判定し、

分離判定を行うと判定した場合は、ステップＳ４２８へ処理を進め、暗号化判定を行うと判定した場合は、ステップＳ４２１へ処理を進める。

【０１３６】

この判定方法の一例として、前述したように、予め何れの判定を用いるかを設定しておいても良いし、送信先に応じて、何れの判定を行うかを設定しておいてもよい。

【０１３７】

また、サーバメール受信手段３０３に限らず、分離判定手段３０４や暗号化判定手段３１８によって判定を行っても良い。

【０１３８】

ステップＳ４２１では、暗号化判定手段３１８は、ステップＳ４０１によって受信した電子メールに暗号化対象となる添付ファイルが存在するか否かを判定し、存在すると判定した場合は、ステップＳ４２２へ処理を進め、存在すると判定しない場合は、ステップＳ４２７へ処理を進める。

【０１３９】

この判定方法の一例として、前述したように、第２の実施形態では、第１の実施形態では分離対象となる添付ファイルが存在する場合を暗号化対象となる添付ファイルが存在する場合とし、一方、第１の実施形態では分離対象となる添付ファイルが存在しない場合を暗号化対象とする添付ファイルが存在しない場合として判定している。

【０１４０】

ステップＳ４２２では、添付ファイル抽出手段３０５は、電子メールから暗号化対象となる添付ファイルを取得し、暗号化手段３１９は、当該添付ファイルを暗号化して、複合するためのパスワードを発行する。

【０１４１】

ステップＳ４２３では、メール生成手段３０７は、ステップＳ４２２において暗号化された添付ファイルに置き換えられた電子メールを生成する。

【０１４２】

ステップＳ４２４では、サーバメール送信手段３０９は、クライアント端末１０９の第２クライアント受信手段３１３に対して、ステップＳ４２３において生成した電子メールを送信する。

【０１４３】

ステップＳ４２５では、パスワード通知メール生成手段３０８は、ステップＳ４２２で発行された暗号化された添付ファイルを複合するためのパスワード等の情報を通知するためパスワード通知用メールを生成する。

【０１４４】

ステップＳ４２６では、サーバメール送信手段３０９は、ステップＳ４２５において生成したパスワード通知用メールをクライアント端末１０１の第１クライアント受信手段３０２、あるいは、クライアント端末１０９の第２クライアント受信手段３１３、あるいはクライアント端末１０１の第１クライアント受信手段３０２及びクライアント端末１０９の第２クライアント受信手段３１３の双方へ送信する。

【０１４５】

ステップＳ４２７では、サーバメール送信手段３０９は、クライアント端末１０９の第２クライアント受信手段３１３に対して、ステップＳ４０１において受信した電子メールを送信する。

【０１４６】

ステップＳ４２８では、分離処理を行うが、詳細は図４に示すステップＳ４０２からステップＳ４１２における処理を行う。

【０１４７】

本処理を行った結果を図１５に示す。パート６１６及びパート６１８（図１２参照）は、暗号化対象となるため（ContentIDが含まれないため）、暗号化された添付ファイルは、例えば、パート６２６に示すように暗号化ZIP等のファイル（XXX.zipのファイルとして

まとめられる。）として電子メールへ添付され、パート６２０、６２２、及び６２４は、暗号化対象とならないため、そのままのパートとして残存する。

【０１４８】

尚、ステップＳ４２１において、暗号化対象となる添付ファイルが存在しない場合、ステップＳ４２７の処理の前において、電子メールに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。

【０１４９】

保留した際は、監査者によって承認がなされた後、ステップＳ４２７の処理を行っても良い。

【０１５０】

また、暗号化対象となる添付ファイルが存在する場合は、一度、電子メールの送信を保留しておき、監査者によって承認がなされた後、ステップＳ４２２以降の処理を行っても良い。

【０１５１】

さらに、暗号化対象となる添付ファイルが存在する場合にも、ステップＳ４２２において、添付ファイルが取得された電子メール及び当該添付ファイルに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である

【０１５２】

［第３の実施形態］

次に、第３の実施形態について説明をするが、第１の実施形態及び第２の実施形態では、HTML形式の電子メールに付された画像やスタイルシートに対して分離、及び暗号化を回避していたが、第３の実施形態は、リッチテキスト形式の電子メールに対しての分離、及び暗号化に関するものである。

【０１５３】

Microsft（登録商標）社製品であるExchangeやOffice365（登録商標）をベースとする電子メールのシステム環境下において、クライアント端末から電子メールに対して装飾等を行うことが可能なリッチテキスト形式の電子メールが送信されると、電子メールが所定の形式のメッセージとして変換され、ファイル（winmail.dat、win.dat、以下装飾用ファイル）が添付された電子メールが送信される。

【０１５４】

従って、このような電子メールを内部メールサーバ１０４が受信すると、ファイルが添付されていることを検知して、ユーザが電子メールに対してファイルを意図して添付していないにもかかわらず、当該ファイルを分離、あるいは暗号化してしまう。

【０１５５】

例えば、図１６の上段には、リッチテキスト形式で作成された電子メールの各パートが示されているが、パート１０００は、電子メールの本文に関するパート１００２と、リッチテキスト形式で作成された電子メールに関するパート１００４とを含んでおり、この構成を備えた電子メールがクライアント端末から送信されたとする。

【０１５６】

すると、内部メールサーバ１０４は、従来の方法では、filenameに値（winmail.dat）が設定されているため、分離対象と見做す、あるいは、暗号化対象と見做し、システムで自動的に付された装飾用ファイルを分離あるいは暗号化してしまう。

【０１５７】

そして、電子メールの受信者は、分離して保管した先を示すＵＲＬや暗号化された装飾用ファイルが添付された電子メールを見ると、予想していなかったファイルが添付されていることに違和感を覚えたり、この添付された装飾用ファイルの確認等を行うため、業務に支障が生じるといった問題がある。

【０１５８】

また、電子メールの受信側のシステム環境において、このようなファイルを悪意等のあるファイルが電子メールへ添付されたと誤認して処理を行ってしまうといった問題も生じうる。

【０１５９】

また、ユーザによっては、リッチテキスト形式によって施された装飾にこだわらないユーザが多くいることから、このような問題を解消すべく方法を以下に説明する。

【０１６０】

まず、図１７の上段に示すパート１０００のように、電子メールの本文に関するパート１００２、リッチテキスト形式で作成された電子メールに関するパートであり、ユーザが意図して添付していない装飾用ファイルに関するパート１００８から構成される電子メールが、クライアント端末１０１の第１クライアント送信手段３０１から送信されたとする。

【０１６１】

この場合、ステップＳ４０２では、分離判定手段３０４は、ステップＳ４０１によって受信した電子メールに分離対象となる添付ファイルが存在するか否かを判定する。

【０１６２】

この判定を行うには、添付ファイルに対応するパートを参照し、filenameに値が設定されている場合（winmail.dat、win.datが設定）、添付ファイルが存在するものとするが、さらに、Content-Typeに、リッチテキスト形式で作成された電子メールによってシステムで自動添付された装飾用ファイルである種別（application/ms-tnef）である場合、この添付ファイルは、filenameに値が設定されている場合であっても、添付ファイルが存在しないものとして見做す。

【０１６３】

但し、装飾用ファイルを解析（展開）した結果、ユーザが意図して添付したファイルが装飾用ファイル内に存在することを特定できると、分離対象となる添付ファイルが存在するものとして判定を行う。

【０１６４】

尚、装飾用ファイルは、電子メールの本文とその本文の装飾に係る情報を含むファイルと、ユーザが意図して添付したファイルとを含む構成を備えている。

【０１６５】

そして、ステップＳ４１２の前処理として、添付ファイル抽出手段３０５は、電子メールから装飾用ファイルを分離し、ステップＳ４１２において、サーバメール送信手段３０９は、装飾用ファイルが分離された電子メールをクライアント端末１０９の第２クライアント受信手段３１３へ送信する。

【０１６６】

その例を図１７の下段に示すが、電子メールの本文に関するパート１００２が残り、リッチテキスト形式で作成された電子メールに関するパート１００８が削除された状態で、電子メールを送信する。

【０１６７】

一方、ステップＳ４２１では、暗号化判定手段３１８は、ステップＳ４０１によって受信した電子メールに暗号化対象となる添付ファイルが存在するか否かを判定し、存在すると判定した場合は、ステップＳ４２２へ処理を進め、存在すると判定しない場合は、ステップＳ４２７へ処理を進める。

【０１６８】

この判定方法の一例として、前述したように、分離対象となる添付ファイルが存在する場合を暗号化対象となる添付ファイルが存在する場合とし、一方、分離対象となる添付ファイルが存在しない場合を暗号化対象とする添付ファイルが存在しない場合として判定している。

【０１６９】

そして、ステップＳ４２７の前処理として、添付ファイル抽出手段３０５は、電子メー

ルから装飾用ファイルを分離し、ステップＳ４２７において、サーバメール送信手段３０９は、装飾用ファイルが分離された電子メールをクライアント端末１０９の第２クライアント受信手段３１３へ送信する。

【０１７０】

次に、図１８の上段に示すパート１０００のように、電子メールの本文に関するパート１０１０、リッチテキスト形式で作成された電子メールに関するパートであり、ユーザが意図して添付したファイル（ＡＡＡＡＡ.docs、ＢＢＢＢＢ.xlsx）に関するパート１０１２から構成される電子メールが、クライアント端末１０１の第１クライアント送信手段３０１から送信されたとする。

【０１７１】

ステップＳ４０２では、分離判定手段３０４は、前述したような処理を行うが、装飾用ファイルと見做した後、装飾用ファイルを解析（展開）し、ユーザが意図して添付したファイルが存在することを特定できると（装飾用ファイルにＡＡＡＡＡ.docs、ＢＢＢＢＢ.xlsxのファイルが存在）、分離対象となる添付ファイルが存在するものとして判定を行う。

【０１７２】

ステップＳ４０３では、添付ファイル抽出手段３０５は、電子メールから分離対象となる添付ファイル（装飾用ファイルのＡＡＡＡＡ.docs、ＢＢＢＢＢ.xlsxのファイル）を取得し、添付ファイル記憶要求手段３０６は、添付ファイルをＮＦＳサーバ１０５に記憶するため、添付ファイル記憶手段３１１に対して添付ファイルを記憶することを要求し、添付ファイル記憶手段３１１は、当該添付ファイルをＮＦＳサーバ１０５に記憶する。

【０１７３】

尚、電子メールの本文とその本文の装飾に係る情報を含むファイルは削除し、ＮＦＳサーバ１０５に対して当該ファイルの記憶は要求しない。その後、ステップＳ４０４以降の処理を行う。

【０１７４】

一方、ステップＳ４２１では、前述のステップＳ４０２で行った処理と同様な判定方法で、分離対象となる添付ファイルが存在する場合を暗号化対象となる添付ファイルが存在する場合とし、一方、分離対象となる添付ファイルが存在しない場合を暗号化対象とする添付ファイルが存在しない場合として判定している。

【０１７５】

ステップＳ４２２では、添付ファイル抽出手段３０５は、電子メールから暗号化対象となる添付ファイル（装飾用ファイルのＡＡＡＡＡ.docs、ＢＢＢＢＢ.xlsxのファイル）を取得し、暗号化手段３１９は、添付ファイルを暗号化して、複合するためのパスワードを発行する。

【０１７６】

この際に、装飾用ファイルに含まれる電子メールの本文とその本文の装飾に係る情報を含むファイルは削除し、暗号化は行わない。

【０１７７】

ステップＳ４２３では、メール生成手段３０７は、暗号化された添付ファイル（ＡＡＡＡＡ.docs、ＢＢＢＢＢ.xlsxのファイル）に置き換えられた電子メールを生成する。

【０１７８】

この処理によって生成された電子メールの構成例を図１８の下段に示しているが、電子メールの本文に関するパート１０１０を残し、リッチテキスト形式で作成された電子メールに関するパート１０１２が削除され、その代わりに、装飾用ファイルに含まれるユーザが意図して添付したファイルに関するパート１０１４（ＡＡＡＡＡ.docs）及びパート１０１６（ＢＢＢＢＢ.xlsx）を含む電子メールを生成する。

【０１７９】

次に、図１６の下段に示すパート１０００のように、電子メールの本文に関するパート１００２、ユーザが意図的に装飾用ファイルを添付したことを示すパート１００６から構

成される電子メールが、クライアント端末１０１の第１クライアント送信手段３０１から送信されたとする。

【０１８０】

この場合、システムで自動的に装飾用ファイルを添付していないことから、分離対象とする、及び、暗号化対象とする。

【０１８１】

そのため、ステップＳ４０２及びステップＳ４２１では、Content-Typeに、ユーザが意図して装飾用ファイルを添付したことを示す種別（application/octet-stream）である場合、添付ファイルが存在するものとして判定される。

【０１８２】

尚、この装飾用ファイル内に添付ファイルが存在するかしないかに関わらず、この装飾用ファイルにより、添付ファイルが存在するものとして判定される。

【０１８３】

また、第１の実施形態と同様に、ステップＳ４０２において、分離対象となる添付ファイルが存在しない場合、ステップＳ４１２の処理の前において、電子メールに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。

【０１８４】

保留した際は、監査者によって承認がなされた後、ステップＳ４１２の処理を行っても良い。

【０１８５】

また、分離対象となる添付ファイルが存在する場合にも、ステップＳ４０３の後、添付ファイルが分離された電子メール及び当該添付ファイルに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。

【０１８６】

保留した際は、監査者によって承認がなされた後、ステップＳ４０４の処理を行っても良い。

【０１８７】

さらに、第２の実施形態と同様に、ステップＳ４２１において、暗号化対象となる添付ファイルが存在しない場合、ステップＳ４２７の処理の前において、電子メールに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。

【０１８８】

保留した際は、監査者によって承認がなされた後、ステップＳ４２７の処理を行っても良い。

【０１８９】

また、暗号化対象となる添付ファイルが存在する場合は、一度、電子メールの送信を保留しておき、監査者によって承認がなされた後、ステップＳ４２２以降の処理を行っても良い。

【０１９０】

さらに、暗号化対象となる添付ファイルが存在する場合にも、ステップＳ４２２において、添付ファイルが取得された電子メール及び当該添付ファイルに対してルールを適用することで、従来のフィルタリング処理を行い、当該電子メールの送信を保留したり禁止したりすることも可能である。

【０１９１】

その他の電子メールの構成の例として、電子メールの本文に関するパート（Content-Typeがtext/plain）が存在しないメールが、クライアント端末１０１の第１クライアント送信手段３０１から送信されたとしする。

【０１９２】

この場合、前述したように装飾用ファイルを削除するが、ステップＳ４１２の処理の前、ステップＳ４０３の後、ステップＳ４２７の処理の前、及びステップＳ４２２において、新たに電子メールの本文に関するパートを生成して、装飾用ファイル内の電子メールの本文とその本文の装飾に係る情報を含むファイルにおける電子メールの本文を、生成したパートとする。

【０１９３】

装飾用ファイル内のユーザが意図して添付したファイルについては前述した通り、電子メールへ添付される。

【０１９４】

そして、この後、電子メールに対してフィルタリング処理を行っても良い。

以上、本発明に依れば、添付ファイルが存在する電子メールの送受信を行う上で、柔軟な運用を行いつつ、セキュリティー向上を図ることができる。

【０１９５】

また、本発明は、例えば、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とることが可能である。

【０１９６】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記憶した記録媒体は本発明を構成することになる。プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク等を用いることができる。

【０１９７】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータで稼働しているＯＳ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１９８】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１９９】

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。

【０２００】

さらに、本発明を達成するための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。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

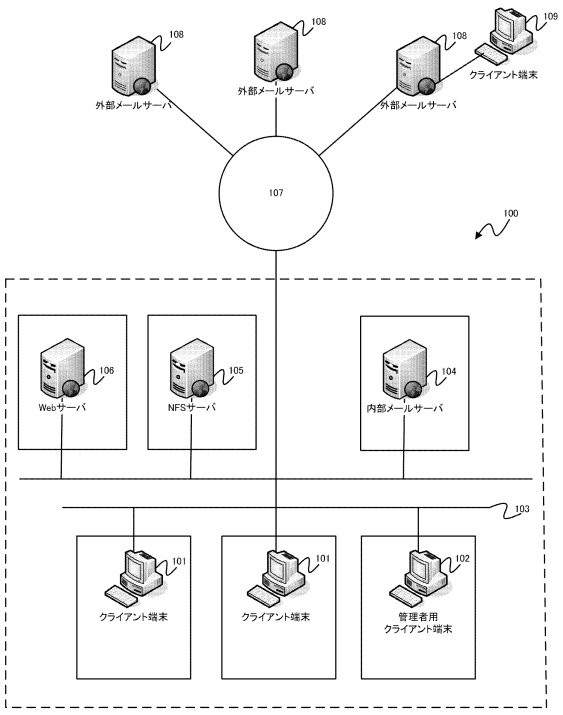
【符号の説明】

【０２０１】

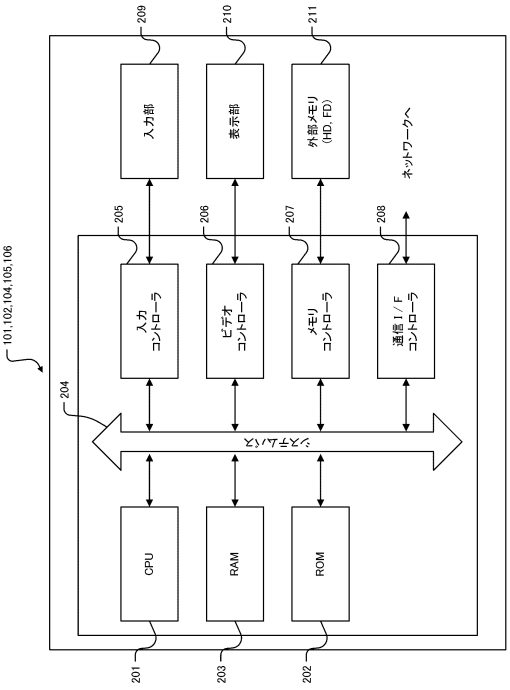
１００　　情報処理システム
１０１　　クライアント端末
１０２　　管理者用クライアント端末
１０３　　ローカルエリアネットワーク（ＬＡＮ）
１０４　　内部メールサーバ

１０５　ＮＦＳサーバ
１０６　Ｗｅｂサーバ
１０７　広域ネットワーク
１０８　外部メールサーバ
１０９　クライアント端末
２０１　ＣＰＵ
２０２　ＲＡＭ
２０３　ＲＯＭ
２０４　システムバス
２０５　入力コントローラ
２０６　ビデオコントローラ
２０７　メモリコントローラ
２０８　通信Ｉ／Ｆ（インターフェース）コントローラ
２０９　入力部
２１０　ディスプレイ装置
２１１　外部メモリ

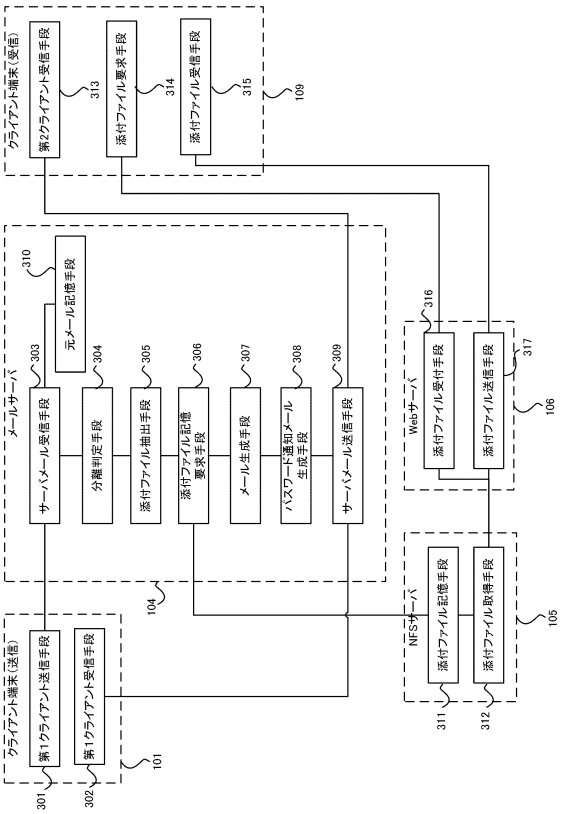
【図１】



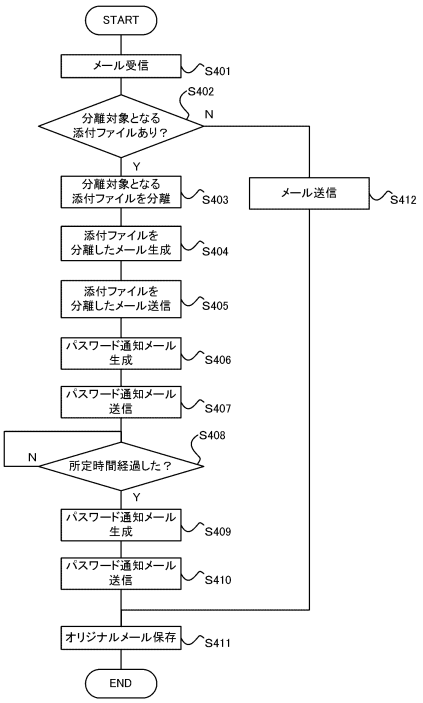
【図２】



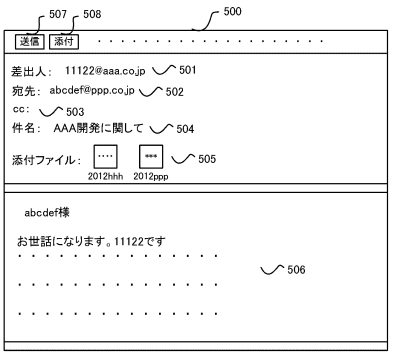
【図３】


クライアント端末（受信）
第2クライアント受信手段
313
添付ファイル要求手段
314
添付ファイル受信手段
315
109
メールサーバ
310
元メール記憶手段
303
304
305
306
307
308
309
サーバメール受信手段
分離判定手段
添付ファイル出力手段
添付ファイル記憶要求手段
メール生成手段
パスワード通知メール生成手段
サーバメール送信手段
104
Webサーバ
316
添付ファイル受付手段
添付ファイル送信手段
317
106
NFSサーバ
添付ファイル記憶手段
添付ファイル取得手段
105
クライアント端末（送信）
第1クライアント送信手段
第1クライアント受信手段
101
301
302
311
312

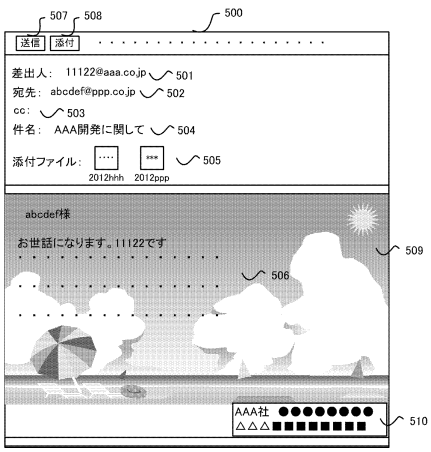
【図４】


START
メール受信
S401
S402
分離対象となる添付ファイルあり？
N
Y
分離対象となる添付ファイルを分離
S403
メール送信
S412
添付ファイルを分離したメール生成
S404
添付ファイルを分離したメール送信
S405
パスワード通知メール生成
S406
パスワード通知メール送信
S407
S408
N
所定時間経過した？
Y
パスワード通知メール生成
S409
パスワード通知メール送信
S410
オリジナルメール保存
S411
END

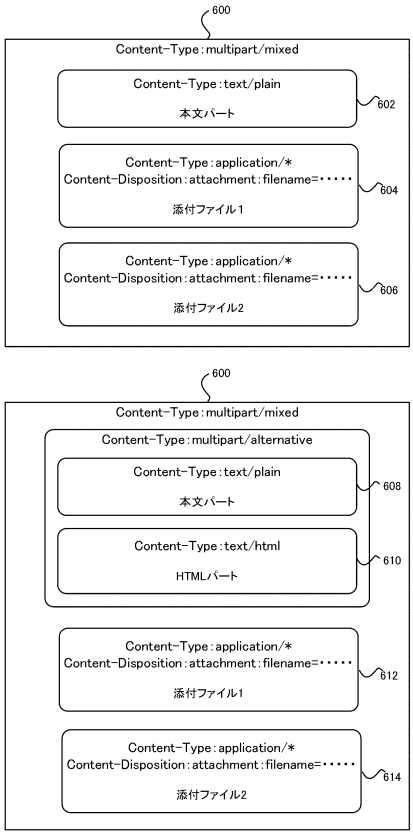
【図５】


507
508
500
送信
添付
差出人： 11122@aaa.co.jp
501
宛先： abcdef@ppp.co.jp
502
cc：
503
件名： AAA開発に関して
504
添付ファイル：
505
2012hhh
2012ppp
abcdef様
お世話になります。11122です
506

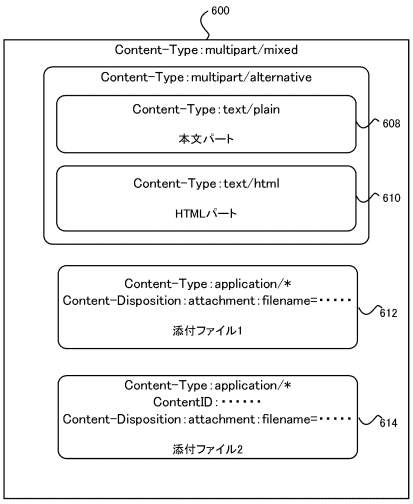
【図６】


507
508
500
送信
添付
差出人： 11122@aaa.co.jp
501
宛先： abcdef@ppp.co.jp
502
cc：
503
件名： AAA開発に関して
504
添付ファイル：
505
2012hhh
2012ppp
abcdef様
お世話になります。11122です
509
506
AAA社
510

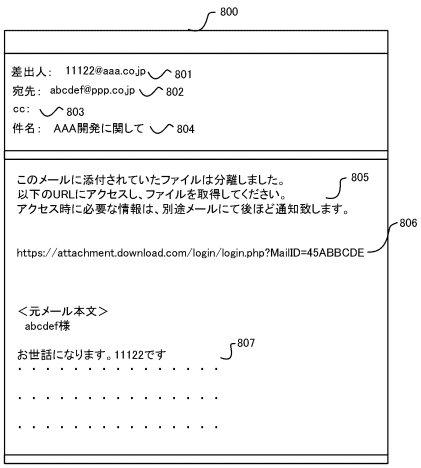
【図７】


600
Content-Type:multipart/mixed
Content-Type:text/plain
本文パート
602
Content-Type:application/*
Content-Disposition:attachment:filename=・・・・・
添付ファイル1
604
Content-Type:application/*
Content-Disposition:attachment:filename=・・・・・
添付ファイル2
606
600
Content-Type:multipart/mixed
Content-Type:multipart/alternative
Content-Type:text/plain
本文パート
608
Content-Type:text/html
HTMLパート
610
Content-Type:application/*
Content-Disposition:attachment:filename=・・・・・
添付ファイル1
612
Content-Type:application/*
Content-Disposition:attachment:filename=・・・・・
添付ファイル2
614

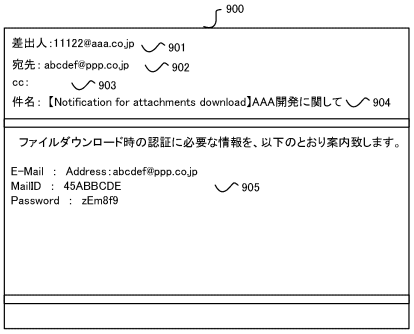
【図８】


600
Content-Type:multipart/mixed
Content-Type:multipart/alternative
Content-Type:text/plain
本文パート
608
Content-Type:text/html
HTMLパート
610
Content-Type:application/*
Content-Disposition:attachment:filename=・・・・・
添付ファイル1
612
Content-Type:application/*
ContentID:・・・・・・
Content-Disposition:attachment:filename=・・・・・
添付ファイル2
614

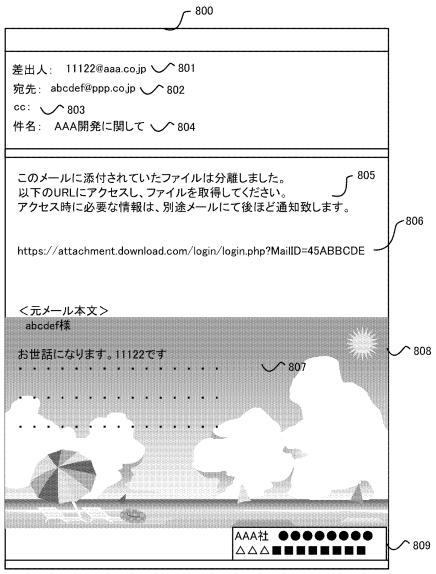
【図９】


800
差出人: 11122@aaa.co.jp
801
宛先: abcdef@ppp.co.jp
802
cc:
803
件名: AAA開発に関して
804
このメールに添付されていたファイルは分離しました。
以下のURLにアクセスし、ファイルを取得してください。
アクセス時に必要な情報は、別途メールにて後ほど通知致します。
805
https://attachment.download.com/login/login.php?MailID=45ABBCDE
806
＜元メール本文＞
abcdef様
お世話になります。11122です
807

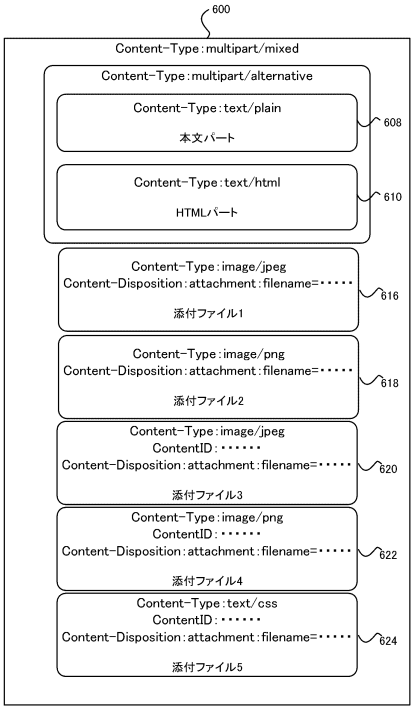
【図１０】


900
差出人:11122@aaa.co.jp
901
宛先:abcdef@ppp.co.jp
902
cc:
903
件名:【Notification for attachments download】AAA開発に関して
904
ファイルダウンロード時の認証に必要な情報を、以下のとおり案内致します。
E-Mail : Address:abcdef@ppp.co.jp
MailID : 45ABBCDE
905
Password : zEm8f9

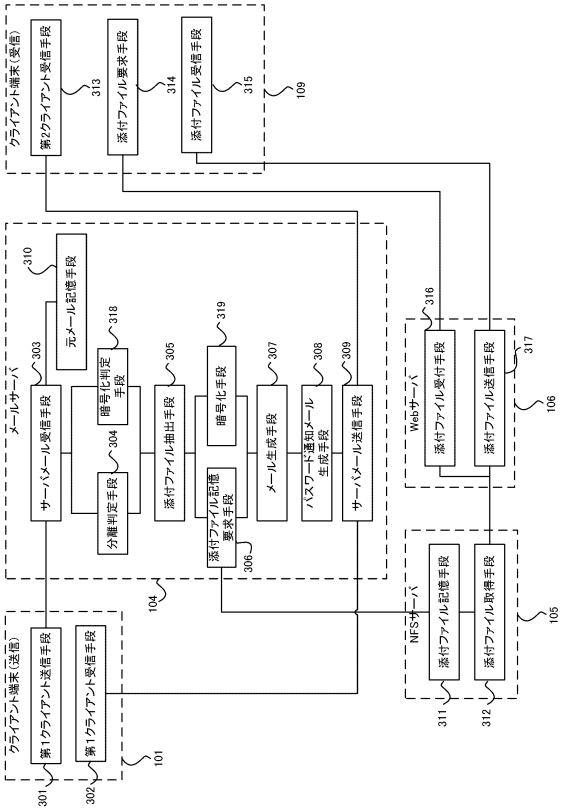
【図１１】



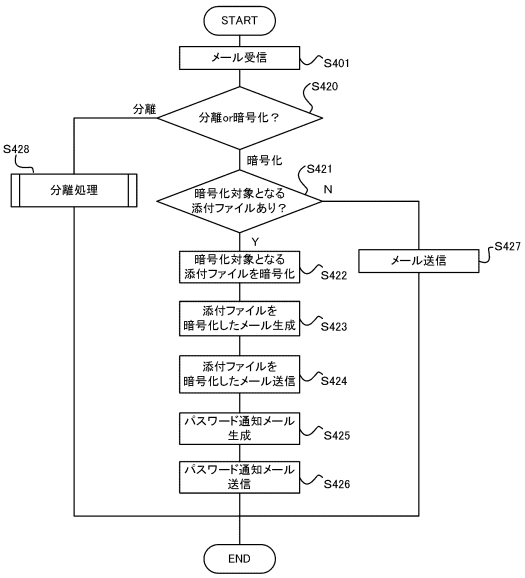
【図１２】



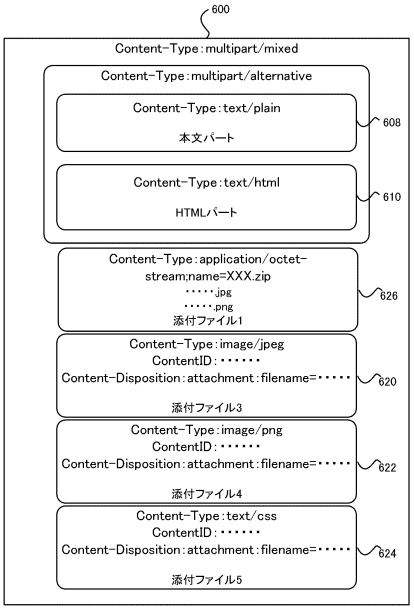
【図１３】



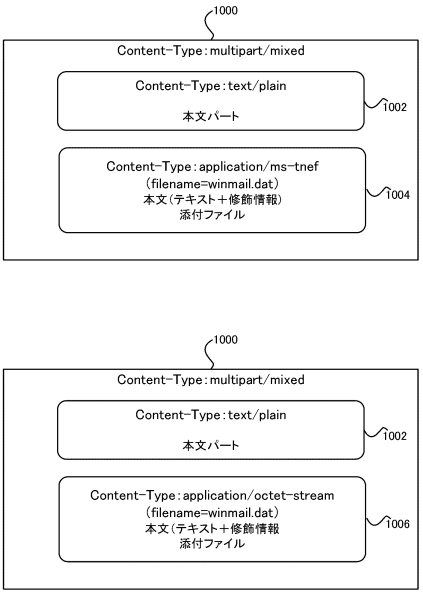
【図１４】



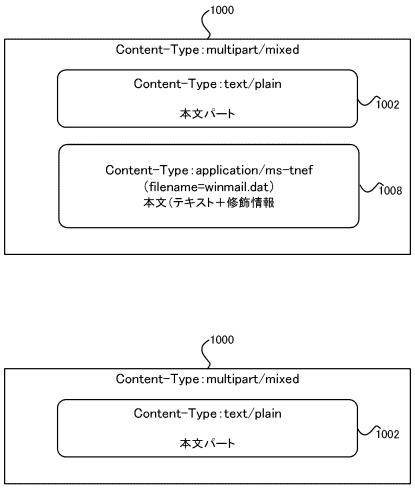
【図１５】



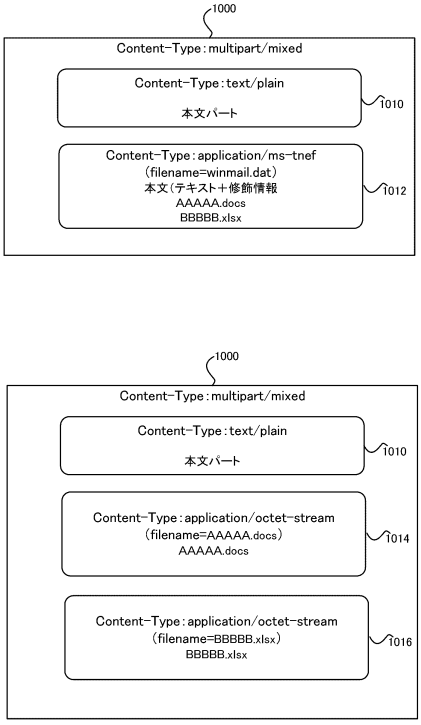
【図１６】



【図１７】



【図１８】



フロントページの続き

(72)発明者　中市　秀哉
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内

審査官　中川　幸洋

(56)参考文献　特開２００８－１０９３８１（ＪＰ，Ａ）
特開２０１５－０８４４６２（ＪＰ，Ａ）
特開２００３－０３０１１７（ＪＰ，Ａ）
特開２００１－２２２４７６（ＪＰ，Ａ）
特開２０００－１０１６３４（ＪＰ，Ａ）
遠藤哲，「メールの添付ファイルを実現するMIMEのマルチパートとは？」，[オンライン]，２０１１年　2月２４日，[検索日 2019.9.6]，インターネット：<https://ascii.jp/elem/000/000/588/588971/>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　１２／００－９５５
Ｇ０６Ｆ　　１３／００