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

特許第4148979号
(P4148979)

(45)発行日　平成20年9月10日(2008.9.10)　(24)登録日　平成20年7月4日(2008.7.4)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 13/00	(2006.01)	G06F	13/00	610S
H04L 12/22	(2006.01)	G06F	13/00	625
H04L 12/58	(2006.01)	H04L	9/00	601E
		H04L	12/22	

請求項の数 10　(全 31 頁)　最終頁に続く

(21)出願番号　特願2007-16910(P2007-16910)
(22)出願日　平成19年1月26日(2007.1.26)
(65)公開番号　特開2008-187280(P2008-187280A)
(43)公開日　平成20年8月14日(2008.8.14)
審査請求日　平成20年4月16日(2008.4.16)

早期審査対象出願

(73)特許権者　398044628
株式会社オレンジソフト
東京都品川区東五反田一丁目８番１２号
(74)代理人　100082740
弁理士　田辺　恵基
(72)発明者　日比野　洋克
東京都品川区東五反田一丁目８番１２号

審査官　速水　雄太

最終頁に続く

(54)【発明の名称】電子メールシステム、電子メール中継装置、電子メール中継方法及び電子メール中継プログラム

(57)【特許請求の範囲】

【請求項１】

送信側電子メール端末から受信側電子メール端末に宛てた電子メールを受信する受信手段と、

上記電子メールに添付ファイルが付されていた場合、所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成する暗号化手段と、

上記添付ファイルに代えて上記暗号ファイルを添付した暗号ファイル電子メールを上記受信側電子メール端末に宛てて送信すると共に、上記暗号パスワードに対応付けた指示受付宛先を通知する送信完了メールを上記送信側電子メール端末に宛てて送信する送信手段と、

上記指示受付宛先に対する上記送信側電子メール端末からの通知指示を受け付ける受付手段と、

上記受付手段により上記通知指示を受け付けた場合、上記暗号ファイルに対応付けられた上記暗号パスワードを記したパスワード通知メールを生成し上記受信側電子メール端末に宛てて送信する通知手段と

を具えることを特徴とする電子メール中継装置。

【請求項２】

上記送信手段は、

上記暗号ファイル電子メールごとに専用の上記指示受付宛先を生成して通知し、

上記通知手段は、

上記通知指示を受け付けた上記指示受付宛先に応じて上記暗号パスワードを正しい上記受信側電子メール端末に宛てて送信する
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項３】
上記通知手段は、
上記受付手段により上記通知指示を受け付けなかった場合、上記パスワード通知メールを送信しない
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項４】
上記送信手段は、
上記送信完了メールによりＵＲＬ（Uniform Resource Locator）でなる上記指示受付宛先を上記送信側電子メール端末に宛てて送信し、
上記受付手段は、上記指示受付宛先に対しアクセスされることを上記通知指示として受け付ける
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項５】
上記送信手段は、
上記送信完了メールにより電子メールアドレスでなる上記指示受付宛先を上記送信側電子メール端末に宛てて送信し、
上記受付手段は、上記指示受付宛先に対する電子メールを上記通知指示として受け付ける
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項６】
上記暗号化手段は、
上記添付ファイルごとに異なる上記暗号パスワードを生成して暗号化する
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項７】
上記通知手段は、
上記受信側電子メール端末のユーザが認証された場合、さらに当該ユーザが上記暗号ファイルの正当な受信者又は正当な発信者であることを確認したときのみ、当該暗号ファイルに対応づけられた上記暗号パスワードを上記受信側電子メール端末に通知する
ことを特徴とする請求項１に記載の電子メール中継装置。
【請求項８】
送信側電子メール端末から受信側電子メール端末に宛てた電子メールを電子メール中継装置の受信手段により受信する受信ステップと、
上記電子メールに添付ファイルが付されていた場合、上記電子メール中継装置の暗号化手段によって所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成する暗号化ステップと、
上記電子メール中継装置の送信手段により、上記添付ファイルに代えて上記暗号ファイルを添付した暗号ファイル電子メールを上記受信側電子メール端末に宛てて送信すると共に、上記暗号パスワードに対応付けた指示受付宛先を通知する送信完了メールを上記送信側電子メール端末に宛てて送信する送信ステップと、
上記電子メール中継装置の受付手段により、上記指示受付宛先に対する上記送信側電子メール端末からの通知指示を受け付ける受付ステップと、
上記受付ステップにより通知指示を受け付けた場合、上記電子メール中継装置の通知手段により、上記暗号ファイルに対応づけられた上記暗号パスワードを記したパスワード通知メールを生成し上記受信側電子メール端末に宛てて送信する通知ステップと
を具えることを特徴とする電子メール中継方法。
【請求項９】
情報処理装置に対して、

送信側電子メール端末から受信側電子メール端末に宛てた電子メールを上記情報処理装置の受信手段により受信する受信ステップと、
上記電子メールに添付ファイルが付されていた場合、上記情報処理装置の暗号化手段によって所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成する暗号化ステップと、
上記情報処理装置の送信手段により、上記添付ファイルに代えて上記暗号ファイルを添付した暗号ファイル電子メールを上記受信側電子メール端末に宛てて送信すると共に、上記暗号パスワードに対応付けた照会用アドレスを通知する送信完了メールを上記送信側電子メール端末に宛てて送信する送信ステップと、
上記情報処理装置の受付手段により、上記指示受付宛先に対する上記送信側電子メール端末からの通知指示を受け付ける受付ステップと、
上記受付ステップにより通知指示を受け付けた場合、上記情報処理装置の通知手段により、上記暗号ファイルに対応づけられた上記暗号パスワードを記したパスワード通知メールを生成し上記受信側電子メール端末に宛てて送信する通知ステップと
を実行させることを特徴とする電子メール中継プログラム。
【請求項１０】
送信側電子メール端末から送信された電子メールを電子メール中継装置により中継し、受信側電子メール端末により当該電子メールを受信する電子メールシステムであって、
上記電子メール中継装置は、
上記送信側電子メール端末から上記受信側電子メール端末に宛てた電子メールを受信する受信手段と、
上記電子メールに添付ファイルが付されていた場合、所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成する暗号化手段と、
上記添付ファイルに代えて上記暗号ファイルを添付した暗号ファイル電子メールを上記受信側電子メール端末に宛てて送信すると共に、上記暗号ファイル電子メールに対応付けた指示受付宛先を通知する送信完了メールを上記送信側電子メール端末に宛てて送信する送信手段と、
上記指示受付宛先に対する上記送信側電子メール端末からの通知指示を受け付ける受付手段と、
上記受付手段により上記通知指示を受け付けた場合、上記暗号ファイルに対応付けられた上記暗号パスワードを記したパスワード通知メールを生成し上記受信側電子メール端末に宛てて送信する通知手段と
を具え、
上記受信側電子メール端末は、
上記暗号ファイルメールに添付された上記暗号ファイルを、上記パスワード通知メールに記された上記暗号パスワードを用いて復号化する復号化手段
を具えることを特徴とする電子メールシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は電子メールシステム、電子メール中継装置、電子メール中継方法及び電子メール中継プログラムに関し、例えば電子メール端末同士で電子メールを送受信する電子メールシステムに適用して好適なものである。
【背景技術】
【０００２】
近年、電子メールシステムにおいては、ネットワークを介してメール端末同士で電子メールを送受信するようになされており、インターネットが普及するに連れ利用者数や利用頻度が増加しつつある。
【０００３】
これに伴い電子メールシステムでは、一般的な内容の電子メール以外にも、例えば内容

の誤りが許されない重要な電子メールや、他者に見られたくない秘密の電子メール等といった様々な電子メールがやりとりされるようになっており、また一般のコンピュータ等で利用される各種ファイルやデータ等を添付して送信し得るようにもなされている。

【０００４】

しかしながら電子メールシステムでは、その構成上、ネットワーク上に存在する複数の電子メールサーバの間で電子メールを中継（転送）させるようになされている。このため、この電子メールシステムでは、標準的な送受信を行った場合に、その途中過程において当該電子メールの内容が第三者に覗かれる（いわゆる傍受又は盗聴）、或いは当該電子メールの内容が不正に書き換えられる（いわゆる改竄）等の恐れがあり、重要な内容や秘密の内容を必ずしも安全に送受信できなかった。

【０００５】

そこで電子メールシステムの中には、送信側で電子メールを暗号化した上で送信し、受信側で当該暗号化された電子メールを受信して復号化することによりセキュリティを確保するといった手法が考えられる。実際上、電子メールに適用し得る暗号化方式としては、Ｓ／ＭＩＭＥ（Secure/Multipurpose Internet Mail Extensions）やＰＧＰ（Pretty Good Privacy）等の種々の手法が提案されている。

【０００６】

しかしながら、一般的な電子メールシステムでは、電子メール端末において用いられているメールクライアントソフトウェア（いわゆるＭＵＡ（Mail User Agent））に、暗号化機能及び復号化機能が必ずしも搭載されているわけではない。

【０００７】

このため、電子メールシステムにおいて実際に電子メールを暗号化してやりとりするためには、送信側の電子メール端末に暗号化ソフトウェアが必要となり、また受信側の電子メール端末でこの暗号化方式に対応した復号化ソフトウェアが必要となる等、電子メール端末のユーザによる構成の追加・変更や煩雑な操作が要求されていた。

【０００８】

そこで、電子メールシステムの中には、送信側及び受信側の電子メール端末には暗号化ソフトウェア及び復号化ソフトウェアを搭載せず、送信側の電子メール端末が接続された送信側の電子メールサーバで電子メールの暗号化処理を行い、受信側の電子メール端末が接続された受信側の電子メールサーバで当該電子メールの復号化処理を行うようになされたものが提案されている（例えば、特許文献１参照）。

【特許文献１】特開２００６－１３７４７公報（第２図及び第５図）

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかしながら、かかる構成の電子メールシステムでは、送信側の電子メールサーバに暗号化機能を持たせるだけでなく、受信側の電子メールサーバに復号化機能を持たせる必要があるため、暗号化された電子メールを復号化できるのは、復号化機能を有する電子メールサーバに限定されてしまう。

【００１０】

このため、この電子メールシステムでは、受信側の電子メールサーバが復号化機能を持たない場合、当該電子メールサーバに接続された受信側の電子メール端末も復号化機能を有していない可能性が高いため、受信した電子メールを復号化できない恐れがある。

【００１１】

ところで電子メールシステムでは、例えば電子メール本文の重要性は低いものの添付ファイルの重要性が高い場合等に、電子メール全文ではなく、添付ファイルのみを送信側の電子メールサーバにより暗号化しセキュリティを確保することも考えられる。

【００１２】

しかしながら、添付ファイルのみを暗号化する電子メールシステムにおいても、電子メール全文を暗号化する場合と同様、暗号化された添付ファイルを復号化できるのは復号化

機能を有する受信サーバに限定されてしまうことに変わりはない。

【００１３】

このため、この電子メールシステムでは、復号化機能を有さない電子メールサーバに接続された電子メール端末が添付ファイルを正しく取得できない恐れがあるという問題があった。

【００１４】

本発明は以上の点を考慮してなされたもので、電子メールの添付ファイルを安全かつ容易に受け渡し得る電子メールシステム、電子メール中継装置、電子メール中継方法及び電子メール中継プログラムを提案しようとするものである。

【課題を解決するための手段】

【００１５】

かかる課題を解決するため本発明の電子メールシステムにおいては、送信側電子メール端末から送信された電子メールを電子メール中継装置により中継し、受信側電子メール端末により当該電子メールを受信する電子メールシステムであって、電子メール中継装置は、送信側電子メール端末から受信側電子メール端末に宛てた電子メールを受信する受信手段と、電子メールに添付ファイルが付されていた場合、所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成する暗号化手段と、添付ファイルに代えて暗号ファイルを添付した暗号ファイル電子メールを受信側電子メール端末に宛てて送信すると共に、暗号ファイル電子メールに対応付けた指示受付宛先を通知する送信完了メールを送信側電子メール端末に宛てて送信する送信手段と、指示受付宛先に対する送信側電子メール端末からの通知指示を受け付ける受付手段と、受付手段により通知指示を受け付けた場合、暗号ファイルに対応づけられた暗号パスワードを記したパスワード通知メールを生成し受信側電子メール端末に宛てて送信する通知手段とを設け、受信側電子メール端末は、暗号ファイルメールに添付された暗号ファイルを、パスワード通知メールに記された暗号パスワードを用いて復号化する復号化手段を設けるようにした。

【００１６】

これにより、送信側電子メール端末からの添付ファイルを暗号化した暗号ファイルを受信側電子メール端末に取得させると共に、当該受信側電子メール端末に対して別個の電子メールにより暗号パスワードを通知でき、元の添付ファイルを正当なユーザにのみ取得させることができる。

【００１７】

また本発明の電子メール中継装置、電子メール中継方法及び電子メール中継プログラムにおいては、送信側電子メール端末から受信側電子メール端末に宛てた電子メールを電子メール中継装置の受信手段により受信し、電子メールに添付ファイルが付されていた場合、電子メール中継装置の暗号化手段によって所定の暗号パスワードを暗号鍵として当該添付ファイルを暗号化することにより暗号ファイルを生成し、電子メール中継装置の送信手段により、添付ファイルに代えて暗号ファイルを添付した暗号ファイル電子メールを受信側電子メール端末に宛てて送信すると共に、暗号パスワードに対応付けた指示受付宛先を通知する送信完了メールを送信側電子メール端末に宛てて送信し、指示受付宛先に対する送信側電子メール端末からの通知指示を電子メール中継装置の受付手段により受け付けた場合、電子メール中継装置の通知手段により暗号ファイルに対応づけられた暗号パスワードを記したパスワード通知メールを生成し受信側電子メール端末に宛てて送信するようにした。

【００１８】

これにより、送信側電子メール端末からの添付ファイルを暗号化した暗号ファイルを受信側電子メール端末に取得させると共に、当該受信側電子メール端末に対して別個の電子メールにより暗号パスワードを通知でき、元の添付ファイルを正当なユーザにのみ取得させることができる。

【発明の効果】

【００１９】
本発明によれば、送信側電子メール端末からの添付ファイルを暗号化した暗号ファイルを受信側電子メール端末に取得させると共に、当該受信側電子メール端末に対して別個の電子メールにより暗号パスワードを通知でき、元の添付ファイルを正当なユーザにのみ取得させることができ、かくして電子メールの添付ファイルを安全かつ容易に受け渡し得る電子メールシステム、電子メール中継装置、電子メール中継方法及び電子メール中継プログラムを実現できる。
【発明を実施するための最良の形態】
【００２０】
以下、図面について、本発明の一実施の形態を詳述する。
【００２１】
（１）第１の実施の形態
（１－１）電子メールシステムの構成
図１において、第１の実施の形態における電子メールシステム１は、全体としてネットワークに接続されたメール端末装置間で電子メール（以下、単にメールと呼ぶ）を互いに送受信し得るようになされている。
【００２２】
電子メールシステム１は、第１のネットワーク群２と第２のネットワーク群３とに大きく分けられており、当該第１のネットワーク群２と当該第２のネットワーク群３とがインターネット４を介して互いに接続されている。
【００２３】
第１のネットワーク群２は、予め指定された不要な通信や不正なアクセス等を遮断し必要なデータ（パケット）のみを通過させるファイアウォール１１によって、内部のネットワークと外部のネットワーク（すなわちインターネット４）とに分離されている。
【００２４】
さらに第１のネットワーク群２は、その内部において、ファイアウォール１１と同様のファイアウォール１２により、外部のネットワークからのアクセスが一部許可された公開ネットワーク１３と、外部のネットワークからのアクセスがほぼ禁止された内部ネットワーク１４とに分離されている。
【００２５】
公開ネットワーク１３には、第１のネットワーク群２内にあるメール端末装置のメールアカウントを管理するメールサーバ１５が接続されており、管理対象となっているメール端末装置から送信されたメールＭを一時的に蓄積し、その宛先に応じて外部のネットワーク等へ当該メールＭを送信するようになされている。
【００２６】
またメールサーバ１５は、管理対象となっているメール端末装置ごとに（すなわちメールアカウントごとに）各メール端末装置宛てのメールＭを受信して蓄積するようになされており、各メール端末装置からアクセスされた際に、蓄積しているメールＭを取得させるようになされている。
【００２７】
内部ネットワーク１４には、ユーザの操作に基づきメールＭを送受信するメール端末装置１６、及び当該メール端末装置１６と同様の構成でなる他のメール端末装置（図示せず）が接続されている。
【００２８】
メール端末装置１６は、一般的なコンピュータと同様の構成を有しており、所定のＯＳ（Operating System）上でメールクライアントソフトウェア（いわゆるＭＵＡ（Mail User Agent））を実行することにより、メールＭの送信及び受信を行い得るようになされている。またメール端末装置１６は、メールＭの本文ＢＤに対して各種ファイルを添付ファイルＦＡとして添付した添付ファイルメールＭＡも送信し得るようにもなされている。
【００２９】

さらに内部ネットワーク１４には、メールＭを中継する添付ファイル暗号化装置１７が接続されている。添付ファイル暗号化装置１７は、メール端末装置１６から受信した添付ファイルメールＭＡのうち、添付ファイルＦＡのみを暗号化して暗号ファイルＦＣとし、メールサーバ１５へ送信するようになされている（詳しくは後述する）。

【００３０】

具体的に、添付ファイル暗号化装置１７は、メール端末装置１６から送信された添付ファイルメールＭＡの本文ＢＤから添付ファイルＦＡを分離し、所定の暗号鍵（暗号パスワードＰＣ）を用いて当該添付ファイルＦＡを暗号化することにより暗号ファイルＦＣを生成する。続いて添付ファイル暗号化装置１７は、暗号ファイルＦＣを本文ＢＤに添付することにより暗号ファイルメールＭＣを生成し、これをメールサーバ１５へ受け渡すようになされている。

【００３１】

因みに添付ファイル暗号化装置１７は、メール端末装置１６から添付ファイルＦＡが付されていない通常のメールＭが送信された場合、当該メールＭを変更することなくそのままメールサーバ１５へ受け渡すようになされている。

【００３２】

また添付ファイル暗号化装置１７は、元の電子メールの本文ＢＤの末尾に、暗号ファイルＦＣのパスワードを照会するための照会情報ＩＮＦを追記しており、暗号ファイルメールＭＣを受信したメール端末装置からこの照会情報ＩＮＦを基に暗号ファイルＦＣの暗号パスワードＰＣについての照会を受け、所定の認証処理により当該メール端末装置のユーザを認証した上で、当該暗号ファイルＦＣの暗号パスワードＰＣを当該ユーザに通知するようになされている。

【００３３】

このように添付ファイル暗号化装置１７は、メール端末装置１６から送信された添付ファイルメールＭＡを中継してメールサーバ１５へ受け渡すようになされており、その際、当該添付ファイルメールＭＡの添付ファイルＦＡを暗号ファイルＦＣに変換することにより、当該添付ファイルメールＭＡに代えて暗号ファイルメールＭＣを送信するようになされている。

【００３４】

なお添付ファイル暗号化装置１７は、暗号ファイルメールＭＣを受信したメール端末装置から暗号ファイルＦＣの暗号パスワードＰＣについての照会を受けた場合、正しく認証したユーザに対して当該暗号パスワードＰＣを通知し得るようにもなされている。

【００３５】

一方、第２のネットワーク群３は、ファイアウォール１１と同様の構成でなるファイアウォール２１により、内側のネットワーク２２と外側のネットワーク（すなわちインターネット４）とに分離されている。このネットワーク２２には、メールサーバ１５と同様の構成でなるメールサーバ２３、及びメール端末装置１６と同様の構成でなるメール端末装置２４が接続されている。

【００３６】

このように電子メールシステム１では、メール端末装置１６とメール端末装置２４とがインターネット４を含む各種のネットワークを介して接続されており、これらのネットワークを介して互いにデータ（実際にはパケット）を送受信し得るようになされている。

【００３７】

（１－２）添付ファイルが付された電子メールの送受信

（１－２－１）添付ファイルの暗号化及び送信

次に、電子メールシステム１において添付ファイルＦＡが付された添付ファイルメールＭＡをメール端末装置１６からメール端末装置２４へ送信する際のシーケンスについて、図２、図３、図４及び図５を用いて説明する。

【００３８】

図２において、添付ファイルメールＭＡの送信側となるメール端末装置１６は、まずシ

ーケンスＳＱ１において、図３（Ａ）に示すように、ユーザの操作に基づいて本文ＢＤに添付ファイルＦＡを付した添付ファイルメールＭＡを作成し、ＳＭＴＰ（Simple Mail Transfer Protocol）を利用して当該メールＭを添付ファイル暗号化装置１７へ送信する。

【００３９】

因みにこの場合、添付ファイルメールＭＡは、送信側メールアドレスＡＤＳ（すなわちメール端末装置１６のアドレス）から受信側メールアドレスＡＤＲ（すなわちメール端末装置２４のアドレス）へ宛てられたものとする。

【００４０】

これに応じて添付ファイル暗号化装置１７は、シーケンスＳＱ１１（図２）において添付ファイルメールＭＡを受信し、次のシーケンスＳＱ１２へ移る。

【００４１】

シーケンスＳＱ１２において添付ファイル暗号化装置１７は、所定の暗号パスワードＰＣ（詳しくは後述する）を用いて添付ファイルＦＡを暗号化することにより暗号ファイルＦＣを生成し、さらに当該暗号ファイルＦＣに対して一意となるファイル識別子ＦＩＤを割り当て、次のシーケンスＳＱ１３へ移る。

【００４２】

シーケンスＳＱ１３において添付ファイル暗号化装置１７は、図３（Ｂ）に示すように、暗号ファイルＦＣのパスワードを照会するための、当該添付ファイル暗号化装置１７のＵＲＬ（Uniform Resource Locator）、ファイル識別子ＦＩＤ及び受信側メールアドレスＡＤＲ等を含む照会情報ＩＮＦを本文ＢＤの末尾に追記し、さらに添付ファイルＦＡに代えて暗号ファイルＦＣを添付することにより暗号ファイルメールＭＣを生成し、次のシーケンスＳＱ１４へ移る。

【００４３】

シーケンスＳＱ１４（図２）において添付ファイル暗号化装置１７は、ＳＭＴＰを利用してインターネット４等の各種ネットワークを介して暗号ファイルメールＭＣをメールサーバ２３（図１）へ送信し、次のシーケンスＳＱ１５へ移る。

【００４４】

一方、暗号ファイルメールＭＣの送信先であるメール端末装置２４は、シーケンスＳＱ２１（図２）において、ＰＯＰ（Post Office Protocol）を利用してメールサーバ２３（図１）から当該暗号ファイルメールＦＣを取得（受信）する。

【００４５】

シーケンスＳＱ１５において添付ファイル暗号化装置１７は、図４に示すような、添付ファイルを送信したことを通知するための送信完了メールＭＮを生成し、メール端末装置２４へ宛ててＳＭＴＰによりメールサーバ１５へ送信する。

【００４６】

これに応じてメール端末装置２４は、シーケンスＳＱ２において、メールサーバ１５へアクセスすることにより送信完了メールを取得し、添付ファイルＦＡの暗号化及び送信が完了したことと共に、その暗号パスワードＰＣをユーザ（すなわち添付ファイルメールＭＡの送信者）に通知する。

【００４７】

ここで、メールＭ及び添付ファイルＦＡの受け渡しについて、図５（Ａ）を用いて整理する。まずメール端末装置１６は、添付ファイルメールＭＡを添付ファイル暗号化装置１７へ送信する。添付ファイル暗号化装置１７は、添付ファイルメールＭＡの添付ファイルＦＡを暗号化して暗号ファイルＦＣに置き換えることにより、元の添付ファイルメールＭＡを暗号ファイルメールＭＣに変換し、これをメールサーバ１５へ送信する。

【００４８】

メールサーバ１５は、インターネット４を介して暗号ファイルメールＭＣをメールサーバ２３へ送信し、一時蓄積させる。メール端末装置２４は、メールサーバ２３にアクセスすることにより、暗号ファイルメールＭＣを取得する。

【００４９】

このように電子メールシステム１では、メール端末装置１６からメール端末装置２４に対して添付ファイルメールＭＡを送信する際、添付ファイル暗号化装置１７からメール端末装置２４までの間において、暗号ファイルメールＭＣの状態で、すなわち添付ファイルＦＡを暗号化した暗号ファイルＦＣの状態で転送するようになされている。

【００５０】

このため電子メールシステム１では、その転送途中において仮に第三者により暗号ファイルメールＭＣが傍受（盗聴）されたとしても、暗号ファイルＦＣの暗号パスワードＰＣを知り得ない第三者によって当該暗号ファイルＦＣが添付ファイルＦＡに復号化される可能性をほぼ皆無とすることができるため、当該添付ファイルＦＡのセキュリティを維持することができる。

【００５１】

（１－２－２）暗号パスワードの通知

その後、メール端末装置２４は、暗号ファイルメールＭＣに記された照会情報ＩＮＦ（図３（Ｂ））を参照したユーザの操作により、シーケンスＳＱ２２（図２）において、添付ファイル暗号化装置１７に対して暗号ファイルＦＣの暗号パスワードＰＣを照会する。

【００５２】

具体的にメール端末装置２４は、当該メール端末装置２４が搭載しているウェブブラウザ等を介して、添付ファイル暗号化装置１７にアクセスする。このときメール端末装置２４は、照会情報ＩＮＦに基づき、ユーザの識別子となる受信側メールアドレスＡＤＲとファイル識別子ＦＩＤとを添付ファイル暗号化装置１７へ送信する。

【００５３】

因みにメール端末装置２４は、照会情報ＩＮＦに基づきＳＳＬ（Secure Socket Layer）を利用した暗号化通信によって添付ファイル暗号化装置１７にアクセスするようになされており、通信の内容が第三者により不正に解読されることを事実上不可能としている。

【００５４】

これに応じて添付ファイル暗号化装置１７は、シーケンスＳＱ１６において、メール端末装置２４のユーザに照会用パスワードＰＩを入力させるユーザ認証処理を行い、次のシーケンスＳＱ１６へ移る。

【００５５】

因みに添付ファイル暗号化装置１７は、メール端末装置２４のユーザが未登録であった場合、所定の初回認証登録処理を行うことにより、当該ユーザに対して認証用パスワードＰＥを発行した上で当該ユーザの認証処理を行うようになされている。

【００５６】

添付ファイル暗号化装置１７は、シーケンスＳＱ１７において、メール端末装置２４のユーザに入力された照会用パスワードＰＩと登録済みの認証用パスワードＰＥとを比較し、両者が一致した場合に認証成功とみなして、ファイル識別子ＦＩＤを基に暗号ファイルＦＣに対応した暗号パスワードＰＣをメール端末装置２４へ送信する

【００５７】

これに応じてメール端末装置２４は、シーケンスＳＱ２３において暗号ファイルＦＣに対応した暗号パスワードＰＣを受信し、次のシーケンスＳＱ２４へ移る。

【００５８】

メール端末装置２４は、シーケンスＳＱ２４において、受信した暗号パスワードＰＣを用いて暗号ファイルＦＣを復号化することにより、元の添付ファイルＦＡを取得する。

【００５９】

実際上、暗号ファイルＦＣは、「パスワード付きＺＩＰ形式」と呼ばれる形式でなり、元の添付ファイルＦＡが暗号パスワードＰＣを暗号鍵として圧縮符号化されたものとなっている。このため、例えばメール端末装置２４は、ＯＳ（Operating System）として一般に広く利用されているＷｉｎｄｏｗｓ（登録商標）ＸＰを使用していれば、正しい暗号パスワードＰＣを指定することにより、当該ＯＳの標準的な機能を用いて暗号ファイルＦＣを添付ファイルＦＡに復元することができる。

【００６０】
このように電子メールシステム１では、図５（Ｂ）に示すように、添付ファイル暗号化装置１７がメール端末装置２４から暗号パスワードＰＣの照会を受けた場合、ユーザ識別子（すなわち受信側メールアドレスＡＤＲ）及び認証用パスワードＰＥを用いてユーザの認証を行い、認証成功の場合のみ、暗号パスワードＰＣをメール端末装置２４へ通知して暗号ファイルＦＣを復号化させるようになされている。
【００６１】
このため電子メールシステム１では、暗号ファイルＦＣの正当な受信者であるユーザのみに対して、添付ファイル暗号化装置１７から暗号パスワードＰＣを通知することができ、メール端末装置２４により当該暗号ファイルＦＣを復号化させて元の添付ファイルＦＡを取得させることができる。
【００６２】
（１－３）添付ファイル暗号化装置の詳細構成
（１－３－１）添付ファイル暗号化装置の回路構成
まず、添付ファイル暗号化装置１７の回路構成について説明する。図６に示すように、添付ファイル暗号化装置１７は、一般的なコンピュータ装置とほぼ同様の構成を有しており、制御部３０のＣＰＵ（Central Processing Unit）３１によって全体を統括制御するようになされている。
【００６３】
添付ファイル暗号化装置１７のＣＰＵ３１は、バス３２を介して接続されたＲＯＭ３３やハードディスクドライブ３４から基本プログラムやＯＳ等を読み出してＲＡＭ３５に展開して実行し、さらに当該ハードディスクドライブ３４から添付ファイル暗号化プログラムや暗号パスワード通知プログラム等の各種プログラムを読み出して当該ＲＡＭ３５上で実行することにより、添付ファイルＦＡの暗号化処理や暗号パスワードＰＣの通知処理等を行うようになされている。
【００６４】
（１－３－２）添付ファイルが付された電子メールの送受信
次に、添付ファイル暗号化装置１７の機能構成について説明する。図７に示すように、添付ファイル暗号化装置１７は、メール端末装置１６から添付ファイルメールＭＡが送信されると、メール受信部４１により当該添付ファイルメールＭＡを受信し、これをメール判別生成部４２へ供給する。
【００６５】
メール判別生成部４２は、ハードディスクドライブ３４に予め記憶されている、添付ファイルＦＡを暗号化する際のルールが格納された暗号化ルールデータベースＤＢ１を参照する。
【００６６】
この暗号化ルールデータベースＤＢ１は、図８に示すように、送信側メールアドレスＡＤＳに対応付けて、受信側メールアドレスＡＤＲ毎に暗号化のキーワードＫＷ及びパスワードの種類ＴＰが暗号化ルールとして格納されている。
【００６７】
ここでキーワードＫＷとしては、添付ファイルＦＡを暗号化するか否かの判断条件となるような、添付ファイルメールＭＡの「件名」欄に含まれる文字列が格納されており、そのままキーワードとなる文字列の他、全ての添付ファイルＦＡを無条件に暗号化する「全て」、全ての添付ファイルＦＡを一切暗号化しない「なし」、添付ファイルＦＡを暗号化する旨の指示と共に暗号化のパスワードを指定する「ｐａｓｓｗｏｒｄ：」のいずれかが予め選択されるようになされている。
【００６８】
またパスワードの種類ＴＰとしては、毎回新たな暗号パスワードＰＣを生成し再利用しない「使い捨て」、予め指定された暗号パスワードＰＣを毎回用いる「固定」、その都度ユーザに指定させる「毎回指定」、及び添付ファイルＦＡを暗号化しないことを意味する

「なし」といった４種類のいずれかが選択されている。

【００６９】

因みに暗号化ルールデータベースＤＢ１の内容は、メール端末装置１６のユーザや電子メールシステム１の管理者等により自在に設定され得るようになされている。

【００７０】

実際上、メール判別生成部４２は、添付ファイルメールＭＡの送信側メールアドレスＡＤＳ（すなわちメールヘッダのＦｒｏｍ：欄）及び受信側メールアドレスＡＤＲ（すなわちメールヘッダのＴｏ：欄）を基に、暗号化ルールとして、当該添付ファイルメールＭＡと対応するキーワードＫＷ及びパスワードの種類ＴＰを読み出す。

【００７１】

続いてメール判別生成部４２は、添付ファイルメールＭＡの件名欄（すなわちメールヘッダのＳｕｂｊｅｃｔ：欄）にキーワードが含まれている、又は当該キーワードが「全て」である場合、パスワードの種類ＴＰが「使い捨て」であればランダムな暗号パスワードＰＣを生成し、「固定」であれば予め指定されたパスワードを暗号パスワードＰＣとし、「毎回指定」であれば添付ファイルメールＭＡの件名欄に記入された「ｐａｓｓｗｏｒｄ：」に続く文字列を暗号パスワードＰＣとして、添付ファイルＦＡ及び当該暗号パスワードＰＣを添付ファイル暗号化部４３へ供給する。

【００７２】

これに応じて添付ファイル暗号化部４３は、暗号パスワードＰＣを用いて添付ファイルＦＡを「パスワード付きＺＩＰ形式」に変換することにより暗号化された暗号ファイルＦＣを生成し、これをメール判別生成部４２へ供給する。

【００７３】

このときメール判別生成部４２は、暗号ファイルＦＣに対して一意となるファイル識別子ＦＩＤを割り当て、当該ファイル識別子ＦＩＤに対して暗号パスワードＰＣ、送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲを対応付けて添付ファイル情報データベースＤＢ２に格納する。

【００７４】

因みに添付ファイル情報データベースＤＢ２は、ハードディスクドライブ３４（図６）に記憶されており、図８（Ｂ）に示すように、ファイル識別子ＦＩＤに暗号パスワードＰＣ、送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲが対応付けられて格納されている。

【００７５】

その後メール判別生成部４２は、元の添付ファイルメールＭＡに対して、ファイル識別子ＦＩＤが含まれる照会情報ＩＮＦ（図３（Ｂ））を本文ＢＤの末尾に追記し、さらに添付ファイルＦＡに代えて暗号ファイルＦＣを添付することにより暗号ファイルメールＭＣを生成し、これをメール送信部４４へ供給すると共に、その日時や受信側メールアドレスＡＤＲ等でなる履歴情報をログデータベースＤＢ３に格納する。

【００７６】

一方、メール判別生成部４２は、メールＭ（すなわち添付ファイルＦＡが無いメール）が供給された場合、或いは添付ファイルメールＭＡを受信し暗号化ルールに従った結果として添付ファイルＦＡを暗号化しない場合、元のメールＭ又は添付ファイルメールＭＡをそのままメール送信部４４へ供給する。

【００７７】

メール送信部４４は、受信側メールアドレスＡＤＲを管理するメールサーバ２３へ向けて暗号ファイルメールＭＣ、メールＭ又は添付ファイルメールＭＡを送信する。

【００７８】

またメール判別生成部４２は、メール送信部４４により暗号ファイルメールＭＣを送信させた後、送信完了メールＭＮを生成し、当該メール送信部４４を介してメール端末装置１６へ送信する。

【００７９】

これに応じてメールサーバ２３は、暗号ファイルメールＭＣ、メールＭ又は添付ファイルメールＭＡを受信して一時蓄積し、メール端末装置２４からのアクセスに応じて当該暗号ファイルメールＭＣ、メールＭ又は添付ファイルメールＭＡを当該メール端末装置２４へ送信する。

【００８０】

メール端末装置２４は、暗号ファイルメールＭＣを受信した場合、当該暗号ファイルメールＭＣの照会情報ＩＮＦ（図３（Ｂ））を参照したユーザの操作により、当該メール端末装置２４が搭載しているウェブブラウザ等を介して添付ファイル暗号化装置１７にアクセスし、照会情報ＩＮＦに含まれているファイル識別子ＦＩＤ及び受信側メールアドレスＡＤＲを送信する。

【００８１】

これに応じて添付ファイル暗号化装置１７のパスワード通知部４５は、ユーザ情報データベースＤＢ４を参照する。ここでユーザ情報データベースＤＢ４は、図８（Ｃ）に示すように、受信側メールアドレスＡＤＲに対応付けて、当該受信側メールアドレスＡＤＲのユーザに対して予め発行した認証用パスワードＰＥが格納されている。

【００８２】

パスワード通知部４５は、メール端末装置２４から送信された受信側メールアドレスＡＤＲに対応する認証用パスワードＰＥをユーザ情報データベースＤＢ４から読み出すと共に、メール端末装置２４のウェブブラウザを介してユーザに照会用パスワードＰＩを入力させる。

【００８３】

このときパスワード通知部４５は、認証用パスワードＰＥと照会用パスワードＰＩとを比較し、両者が一致すれば認証成功、すなわちメール端末装置２４の操作者が正当なユーザであるとみなし、添付ファイル情報データベースＤＢ２からファイル識別子ＦＩＤに対応付けられた暗号パスワードＰＣを読み出してメール端末装置２４のウェブブラウザに表示させることにより当該暗号パスワードＰＣの通知を行う。

【００８４】

またパスワード通知部４５は、認証結果を受信側メールアドレスＡＤＲや日時等と共に履歴情報としてログデータベースＤＢ３に記録するようになされており、不正なアクセスがあった場合などに管理者に当該履歴情報を参照させ得るようになされている。

【００８５】

（１－３－３）添付ファイル暗号化処理

次に、添付ファイル暗号化装置１７における添付ファイル暗号化処理手順ＲＴ１について、図９に示すフローチャートを用いて説明する。

【００８６】

添付ファイル暗号化装置１７の制御部３０（図６）は、電源が投入されＯＳが起動すると、ハードディスクドライブ３４から添付ファイル暗号化プログラムを読み出して実行することにより添付ファイル暗号化処理手順ＲＴ１を開始し、ステップＳＰ１へ移る。

【００８７】

ステップＳＰ１において制御部３０は、メール受信部４１によってメール端末装置１６からのメールＭ又は添付ファイルメールＭＡが受信されたか否かを判定する。ここで否定結果が得られると、制御部３０は再びステップＳＰ１を繰り返すことにより、メール端末装置１６からのメールＭ又は添付ファイルメールＭＡの受信を待ち受ける。

【００８８】

一方ステップＳＰ１において肯定結果が得られると、制御部３０は次のステップＳＰ２へ移る。ステップＳＰ２において制御部３０は、メール判別生成部４２により、添付ファイルＦＡがあるか否か、すなわち添付ファイルメールＭＡを受信したか否かを判定する。ここで否定結果が得られると、このことは添付ファイルＦＡが付されていないメールＭを受信したため、添付ファイルＦＡに関する処理を行う必要がないことを表しており、このとき制御部３０は次のステップＳＰ５へ移る。

【００８９】
一方ステップＳＰ２において肯定結果が得られると、制御部３０は、添付ファイルメールＦＡに関する処理を行うべく、次のステップＳＰ３へ移る。ステップＳＰ３において制御部３０は、添付ファイルメールＭＡの送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲを基に、暗号化ルールデータベースＤＢ１（図８（Ａ））から暗号化ルールとしてキーワードＫＷ及びパスワードの種類ＴＰを読み出し、次のステップＳＰ４へ移る。
【００９０】
ステップＳＰ４において制御部３０は、読み出した暗号化ルール（すなわちキーワードＫＷ及びパスワードの種類ＴＰ）に従い、添付ファイルＦＡを暗号化するか否かを判定する。ここで否定結果が得られると、このことは元の添付ファイルメールＭＡをそのままメール送信部４４から送信すべきであることを表しており、このとき制御部３０は次のステップＳＰ５へ移る。
【００９１】
ステップＳＰ５において制御部３０は、メール送信部４４（図７）により受信側メールアドレスに宛ててメールＭ又は添付ファイルメールＭＡを送信させて当該メールＭ又は添付ファイルメールＭＡに関する一連の処理を完了し、再度ステップＳＰ１へ戻って次のメールＭ又は添付ファイルメールＭＡを待ち受ける。
【００９２】
一方、ステップＳＰ４において肯定結果が得られると、制御部３０は次のステップＳＰ６へ移る。ステップＳＰ６において制御部３０は、添付ファイル暗号化部４３（図７）により、暗号化ルール（すなわちキーワードＫＷ及びパスワードの種類ＴＰ）に従った暗号パスワードＰＣを用いて添付ファイルＦＡを暗号化することにより暗号ファイルＦＣに変換し、次のステップＳＰ７へ移る。
【００９３】
ステップＳＰ７において制御部３０は、メール判別生成部４２により、メールの本文ＢＤの末尾に照会情報ＩＮＦ（図３（Ｂ））を追記し、次のステップＳＰ８へ移る。
【００９４】
ステップＳＰ８において制御部３０は、メール判別生成部４２によって、暗号ファイルＦＣをメールの本文ＢＤに添付することにより暗号ファイルメールＭＣを生成し、次のステップＳＰ９へ移る。
【００９５】
ステップＳＰ９において制御部３０は、メール送信部４４から受信側メールアドレスＡＤＲへ向けて暗号ファイルメールＭＣを送信させ、次のステップＳＰ１０へ移る。
【００９６】
ステップＳＰ１０において制御部３０は、メール判別生成部４２によって送信完了メールＭＮを生成し、これをメール送信部４４から送信側メールアドレスＡＤＳへ向けて送信させることにより、一連の添付ファイル暗号化処理を終了し、再度ステップＳＰ１へ戻り次のメールＭ又は添付ファイルメールＭＡを待ち受ける。
【００９７】
その後制御部３０は、添付ファイル暗号化装置１７の電源が切断されるか管理者等によって添付ファイル暗号化プログラムが停止されるまで、この添付ファイル暗号化処理手順ＲＴ１を繰り返すようになされている。
【００９８】
（１－３－４）暗号パスワード通知処理手順
次に、添付ファイル暗号化装置１７がメール端末装置２４から暗号パスワードＦＣの照会を受けて通知する際の暗号パスワード通知処理手順ＲＴ２について、図１０のフローチャートを用いて説明する。
【００９９】
添付ファイル暗号化装置１７の制御部３０は、電源が入力されＯＳが起動すると、ハー

ドディスクドライブ３４から暗号パスワード通知プログラムを読み出して実行することにより暗号パスワード通知処理手順ＲＴ２を開始し、ステップＳＰ１１へ移る。

【０１００】

ステップＳＰ１１において制御部３０は、パスワード通知部４５（図７）により、メール端末装置２４から暗号ファイルメールＭＣに添付されていた暗号ファイルＦＣの暗号パスワードＦＣに関する照会を受けたか否かを判定する。ここで否定結果が得られると、制御部３０は再びステップＳＰ１１を繰り返すことにより、メール端末装置２４からの暗号パスワードＦＣの照会を待ち受ける。

【０１０１】

一方ステップＳＰ１１において肯定結果が得られると、制御部３０は次のステップＳＰ１２へ移る。ステップＳＰ１２において制御部３０は、パスワード通知部４５によって、メール端末装置２４からファイル識別子ＦＩＤ及び受信側メールアドレスＡＤＲを取得し、次のステップＳＰ１３へ移る。

【０１０２】

ステップＳＰ１３において制御部３０は、パスワード通知部４５によって、ユーザ情報データベースＤＢ４を参照することにより受信側メールアドレスＡＤＲに対応した認証用パスワードＰＥを取得し、次のステップＳＰ１４へ移る。

【０１０３】

ステップＳＰ１４において制御部３０は、パスワード通知部４５によって、メール端末装置２４のユーザに対して照会用パスワードＰＩを入力させ、次のステップＳＰ１５へ移る。

【０１０４】

ステップＳＰ１５において制御部３０は、認証用パスワードＰＥ及び照会用パスワードＰＩを比較し、両者が一致したか否か、すなわち認証に成功したか否かを判定する。ここで否定結果が得られると、このことはメール端末装置２４のユーザが正当なユーザではない可能性があることを表しており、このとき制御部３０は、所定のエラーメッセージをメール端末装置２４の表示画面上に表示させる等した上で、暗号パスワードＰＣの通知に関する処理を中断し、再度ステップＳＰ１１へ戻る。

【０１０５】

一方ステップＳＰ１５において肯定結果が得られると、このことはメール端末装置２４のユーザが既に登録された正当なユーザであると見なし得ることを表しており、このとき制御部３０は、次のステップＳＰ１６へ移る。

【０１０６】

ステップＳＰ１６において制御部３０は、パスワード通知部４５によって添付ファイル情報データベースＤＢ２（図８（Ｂ））を参照し、メール端末装置２４から送信されたファイル識別子ＦＩＤに対応する送信側メールアドレスＡＤＳ、受信側メールアドレスＡＤＲ及び暗号パスワードＰＣを読み出して、次のステップＳＰ１７へ移る。

【０１０７】

ステップＳＰ１７において制御部３０は、メール端末装置から送信された受信側メールアドレスＡＤＲが添付ファイル情報データベースＤＢ２から読み出した送信側メールアドレスＡＤＳ又は受信側メールアドレスＡＤＲと一致するか否かを判定する。

【０１０８】

ここで否定結果が得られると、このことはメール端末装置２４のユーザがユーザ情報データベースＤＢ４に登録されたユーザではあるものの、暗号ファイルＦＣの正当な受信者或いは正当な送信者のいずれでも無いことを表しており、このとき制御部３０は、所定のエラーメッセージをメール端末装置２４の表示画面上に表示させる等した上で、暗号パスワードＰＣの通知に関する処理を中断し、再度ステップＳＰ１１へ戻る。

【０１０９】

一方ステップＳＰ１７において肯定結果が得られると、このことはメール端末装置２４のユーザが暗号ファイルＦＣの正当な受信者又は正当な送信者であることを表しており、

このとき制御部３０は次のステップＳＰ１８へ移る。

【０１１０】

ステップＳＰ１８において制御部３０は、暗号パスワードＰＣをメール端末装置２４へ送信することにより、一連の暗号パスワードＰＣを通知する処理を終了し、再度ステップＳＰ１１へ戻ることにより、次の暗号パスワードＰＣの照会を待ち受ける。

【０１１１】

その後制御部３０は、添付ファイル暗号化装置１７の電源が切断されるか管理者等によって暗号パスワード通知プログラムが停止されるまで、この暗号パスワード通知処理手順ＲＴ２を繰り返すようになされている。

【０１１２】

（１－４）動作及び効果

以上の構成において、第１の実施の形態における電子メールシステム１の添付ファイル暗号化装置１７は、メール端末装置１６から添付ファイルメールＭＡが送信されると、送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲに対応付けられた暗号化ルールに従って添付ファイルＦＡを暗号化することにより暗号ファイルＦＣとし、当該暗号ファイルＦＣを添付した暗号ファイルメールＭＣを受信側メールアドレスＡＤＲに宛てて送信し、メール端末装置２４に受信させる。

【０１１３】

これにより電子メールシステム１の添付ファイル暗号化装置１７は、添付ファイルＦＡを暗号化した暗号ファイルＦＣの状態で各種ネットワークを経由させメール端末装置２４に受信させることができるので、元の添付ファイルＦＡのセキュリティを維持し、第三者により元の添付ファイルＦＡの内容が知られたり改竄されたりする可能性を事実上皆無とすることができる。

【０１１４】

特に電子メールシステム１では、暗号化ルールデータベースＤＢ１（図８（Ａ））のキーワードが「全て」であった場合、添付ファイル暗号化装置１７により全ての添付ファイルＦＡを自動的に暗号化することができるので、ユーザに煩わしい暗号化作業をさせずに済み、また当該ユーザがうっかり暗号化を忘れたまま添付ファイルＦＡを送信してしまうといった人為的ミスを未然に防止することができる。

【０１１５】

これに加えて電子メールシステム１では、暗号化ルールデータベースＤＢ１（図８（Ａ））のキーワードＫＷに対応した文字列が添付ファイルメールＭＡの件名欄に含まれる場合、暗号化の可否やパスワードをユーザに敢えて指示させることもできるので、例えばユーザが添付ファイルＦＡをどうしても暗号化したくない場合や、特定の暗号パスワードＰＣを用いたい場合等に柔軟に対応することができる。

【０１１６】

さらに電子メールシステム１では、暗号化ルールとしてパスワードの種類が「使い捨て」であった場合、個々の暗号ファイルＦＣに対して互いに異なる暗号パスワードＰＣを生成することができるので、仮にある暗号ファイルＦＣの暗号パスワードＰＣが第三者に知られたとしても、当該暗号パスワードＰＣでは他の暗号ファイルＦＣを復号化し得ないため、情報漏洩を最小限に食い止めることができる。

【０１１７】

一方、添付ファイル暗号化装置１７は、暗号ファイルメールＭＣを受信したメール端末装置２４からのＳＳＬを用いたセキュアなアクセスを受け、当該メール端末装置２４の受信側メールアドレスＡＤＲ及びユーザに入力された照会用パスワードＰＩを基に当該ユーザの認証処理を行い、認証が成功し且つ当該ユーザが暗号ファイルＦＣの正当な受信者又は正当な送信者であった場合にのみ当該暗号ファイルＦＣの暗号パスワードＰＣを通知する。

【０１１８】

これにより電子メールシステム１の添付ファイル暗号化装置１７は、暗号ファイルメー

ルＭＣの正当な受信者又は正当な送信者であるメール端末装置２４のユーザに対してのみ暗号ファイルＦＣの暗号パスワードＰＣを安全に通知することができるので、当該暗号パスワードＰＣを第三者に知られないようにすることができ、暗号ファイルＦＣが不正に復号化される危険性を実質的に皆無とすることができる。

【０１１９】

また電子メールシステム１では、添付ファイル暗号化装置１７が添付ファイルＦＡを暗号化した際の暗号パスワードＰＣを添付ファイル情報データベースＤＢ２（図８（Ｂ））によって管理しているため、元の添付ファイルメールＭＡを送信したメール端末装置１６のユーザにより当該暗号パスワードＰＣを把握させ、或いはメール端末装置２４のユーザに対して別のメールや郵便、電話、ファクシミリ等の通信手段によって当該暗号パスワードＰＣを通知させるといった煩雑な作業をさせずに済む。

【０１２０】

さらに電子メールシステム１では、添付ファイル暗号化装置１７により暗号ファイルＦＣを暗号化する際、圧縮方式として広く利用されているＺＩＰ方式とパスワードによる暗号化とを組み合わせた「パスワード付きＺＩＰ形式」としているため、暗号ファイルメールＭＣを受信したメール端末装置２４により正しい暗号パスワードＰＣを取得できた場合、当該メール端末装置２４によってほぼ確実に元の添付ファイルＦＡに復元させることができる。

【０１２１】

また電子メールシステム１は、暗号ファイルメールＭＣの送信後、暗号パスワードＰＣを記載した送信完了メールＭＮを添付ファイルメールＭＡの送信者であるメール端末装置１６のユーザへ送信する。これにより電子メールシステム１では、仮にメール端末装置２４のユーザが暗号パスワードＰＣをうまく照会できなかった場合等に、ユーザの手作業により、送信完了メールＭＮに記されている暗号パスワードＰＣを電子メールに転記して送信すれば、当該暗号パスワードＰＣを通知することもできる。

【０１２２】

以上の構成によれば、第１の実施の形態における電子メールシステム１は、添付ファイル暗号化装置１７によって、メール端末装置１６から送信された添付ファイルメールＭＡの添付ファイルＦＡを暗号化ルールに従って暗号化すると共に暗号パスワードＰＣを管理し、認証された正当なユーザに対してのみ当該暗号パスワードＰＣを通知することにより、添付ファイルＦＡを自動的に暗号化することができると共にユーザに手間をかけさせず安全に暗号パスワードＰＣを正当なユーザにのみ通知することができるので、メール配信の仕組みを利用して添付ファイルＦＡを安全かつ容易に受け渡すことができる。

【０１２３】

（２）第２の実施の形態

（２－１）電子メールシステムの構成

第２の実施の形態における電子メールシステム５０は、第１の実施の形態における電子メールシステム１と比較して、添付ファイル暗号化装置１７に代えて添付ファイル暗号化装置５７が設けられている点が異なるものの、他は同様に構成されている。

【０１２４】

この添付ファイル暗号化装置５７は、添付ファイル暗号化装置１７と一部同様の動作を行うようになされており、メール端末装置１６から送信された添付ファイルメールＭＡの本文ＢＤから添付ファイルＦＡを分離し、所定の暗号鍵（暗号パスワードＰＣ）を用いて当該添付ファイルＦＡを暗号化することにより暗号ファイルＦＣを生成する。続いて添付ファイル暗号化装置１７は、暗号ファイルＦＣを本文ＢＤに添付することにより暗号ファイルメールＭＣを生成し、これをメールサーバ１５へ受け渡すようになされている。

【０１２５】

（２－２）添付ファイルが付された電子メールの送受信

次に、電子メールシステム５０において、添付ファイルＦＡが付された添付ファイルメールＭＡをメール端末装置１６からメール端末装置２４へ送信する際のシーケンスについ

て、図２、図３、図４及び図５とそれぞれ対応する図１１、図１２、図１３及び図１４を用いて説明する。

【０１２６】

図１１において、メール端末装置１６、添付ファイル暗号化装置５７及びメール端末装置２４は、第１の実施の形態におけるメール端末装置１６、添付ファイル暗号化装置１７及びメール端末装置２４と同様に、それぞれシーケンスＳＱ１～ＳＱ２、ＳＱ１１～ＳＱ１５及びＳＱ２１の処理（すなわち図中の一点鎖線以前の処理）を行う。

【０１２７】

この場合、添付ファイル暗号化装置５７は、シーケンスＳＱ１３において、図３（Ｂ）と対応する図１２（Ｂ）に示すように、本文ＢＤに照会情報ＩＮＦ（図３（Ｂ））を追記せず暗号ファイルＦＣを添付することにより暗号ファイルメールＭＣ２を生成し、次のシーケンスＳＱ１４においてメールサーバ２３（図１）へ送信するようになされている。

【０１２８】

また添付ファイル暗号化装置５７は、シーケンスＳＱ１５において、図１３に示すように所定のＵＲＬ（Uniform Resource Locator、以下これを照会アドレスＡＤＡと呼ぶ）が記された送信完了メールＭＮ２をメール端末装置１６へ送信するようになされている。

【０１２９】

ここで送信完了メールＭＮ２に記された指示受付宛先としての照会アドレスＡＤＡは、添付ファイル暗号化装置５７によって、添付ファイルメールＭＡの宛先ごとに専用のアドレスが生成されると共に、各アドレスが個別に管理されるようになされている。

【０１３０】

メール端末装置１６は、シーケンスＳＱ３１において、送信完了メールＭＮ２に記された照会アドレスＡＤＡ（図１３）を参照したユーザ（すなわち添付ファイルメールＭＡの送信者）の操作により、当該メール端末装置１６が搭載しているウェブブラウザ等を介して、添付ファイル暗号化装置１７にアクセスする。

【０１３１】

一方、添付ファイル暗号化装置５７は、シーケンスＳＱ４１において、添付ファイルメールＭＡ専用のアドレス（すなわち照会アドレスＡＲ）に対してアクセスされたことをアクセス受付部６１（図１５）により検出すると、メール端末装置２４のユーザに暗号パスワードＰＣを通知する旨の指示を受け付けたものとみなし、次のシーケンスＳＱ４２へ移る。

【０１３２】

シーケンスＳＱ４２において、添付ファイル暗号化装置５７は、暗号パスワードＰＣを記したパスワード通知メールＭＰを生成し、シーケンスＳＱ１３及びＳＱ１４において添付ファイルメールＭＡを送信したときと同様に、ＳＭＴＰを利用してインターネット４等の各種ネットワークを介し、パスワード通知メールＭＰをメールサーバ２３（図１）へ送信する。

【０１３３】

これに応じてメール端末装置２４は、シーケンスＳＱ５１において、ＰＯＰ、ＩＭＡＰ又はグループウェアの独自プロトコル等を利用してメールサーバ２３（図１）から当該パスワード通知メールＭＰを取得（受信）し、次のシーケンスＳＱ５２へ移る。

【０１３４】

シーケンスＳＱ５２においてメール端末装置２４は、ユーザの操作等に基づき、受信したパスワード通知メールＭＰに記されている暗号パスワードＰＣを用いて暗号ファイルＦＣを復号化することにより、元の添付ファイルＦＡを取得する。

【０１３５】

このように第２の実施の形態における電子メールシステム５０では、第１の実施の形態と異なり、メール端末装置１６から照会アドレスＡＤＡにアクセスされると、添付ファイル暗号化装置５７からメール端末装置２４に対して、暗号ファイルメールＭＣ２と別個の電子メールでなるパスワード通知メールＭＰにより暗号ファイルＦＣの暗号パスワードＰ

Ｃを通知するようになされている。

【０１３６】

因みに、第１の実施の形態と同様に、第２の実施の形態におけるメールＭ及び添付ファイルＦＡの受け渡しについて整理すると、図５と対応する図１４のように表すことができる。

【０１３７】

かくして第２の実施の形態における電子メールシステム５０では、メール端末装置２４のユーザが添付ファイル暗号化装置５７にアクセスすること無く暗号パスワードＰＣを取得できるため、第１の実施の形態のような、添付ファイル暗号化装置５７に対するメール端末装置２４のユーザの登録を不要とすることができる。

【０１３８】

（２－３）添付ファイル暗号化装置の詳細構成

次に、添付ファイル暗号化装置５７の詳細構成について説明する。添付ファイル暗号化装置５７は、第１の実施の形態における添付ファイル暗号化装置１７（図６）と比較して、制御部３０に対応する制御部６０を有している以外はほぼ同様の回路構成を有しているため、その説明は省略する。

【０１３９】

一方、添付ファイル暗号化装置５７は、図７との対応部分に同一符号を付した図１５に示すように、第１の実施の形態における添付ファイル暗号化装置１７と全体的に類似しているものの、一部異なる機能構成を有している。

【０１４０】

具体的に添付ファイル暗号化装置５７は、制御部３０のパスワード通知部４５（図７）に代えて、制御部６０にアクセス受付部６１が設けられている。また添付ファイル暗号化装置５７は、添付ファイル情報データベースＤＢ２（図８）に代えて、図１６に示す添付ファイル情報データベースＤＢ１２を有しているほか、ユーザ情報データベースＤＢ４が省略されている。

【０１４１】

添付ファイル情報データベースＤＢ１２は、ファイル識別子ＦＩＤごとに異なる照会アドレスＡＤＡが格納されている。

【０１４２】

この第２の実施の形態では、メール端末装置１６のユーザが送信完了メールＭＮ２（図１３）を参照し、照会アドレスＡＤＡをクリック等することにより、当該メール端末装置１６にインストールされているウェブブラウザ等を介して当該照会アドレスＡＤＡ、すなわち添付ファイル暗号化装置５７にアクセスすることになる。

【０１４３】

このとき添付ファイル暗号化装置５７は、アクセス受付部６１によりメール端末装置１６からアクセスされたことを検出すると、添付ファイル情報データベースＤＢ２から照会アドレスＡＤＡに対応付けられた暗号パスワードＰＣ及び受信側メールアドレスＡＤＲを読み出し、これらをメール判別生成部４２へ供給する。

【０１４４】

メール判別生成部４２は、本文に暗号パスワードＰＣを記し受信側メールアドレスＡＤＲへ宛てたパスワード通知メールＭＰを生成し、これをメール送信部４４からメールサーバ２３へ向けて送信する。

【０１４５】

これに応じてメールサーバ２３は、パスワード通知メールＭＰを受信して一時蓄積し、メール端末装置２４からのアクセスに応じて当該パスワード通知メールＭＰを当該メール端末装置２４へ送信する。

【０１４６】

このように添付ファイル暗号化装置５７は、照会アドレスＡＤＡに対するアクセスを検出すると、当該照会アドレスＡＤＡに対応付けられた暗号パスワードＰＣを、当該照会ア

ドレスＡＤＡに対応付けられた受信側メールアドレスＡＤＲへ送信するようになされている。

【０１４７】

（２－４）添付ファイル暗号化処理及び暗号パスワード通知処理

次に、添付ファイル暗号化装置５７における添付ファイル暗号化処理手順及び暗号パスワード通知処理手順について説明する。

【０１４８】

添付ファイル暗号化装置５７による添付ファイル暗号化処理手順は、第１の実施の形態における添付ファイル暗号化装置１７による添付ファイル暗号化処理手順ＲＴ１（図９）と比較し、一部の処理が異なっている。

【０１４９】

具体的に添付ファイル暗号化装置５７の制御部６０は、添付ファイル暗号化処理手順ＲＴ１におけるステップＳＰ７の処理を省略し、ステップＳＰ８において暗号ファイルメールＭＣ２を生成し、ステップＳＰ９において当該暗号ファイルメールＭＣ２を送信させ、さらにステップＳＰ１０において送信完了メールＭＮ２を送信するようになされている。

【０１５０】

一方、添付ファイル暗号化装置５７は、図１０と対応する図１７に示す暗号パスワード通知処理手順ＲＴ３に従い、パスワード通知メールＭＰをメール端末装置２４へ送信するようになされている。

【０１５１】

すなわち添付ファイル暗号化装置５７の制御部６０は、電源が入力されＯＳが起動すると、ハードディスクドライブ３４から暗号パスワード通知プログラムを読み出して実行することにより暗号パスワード通知処理手順ＲＴ３を開始し、ステップＳＰ２１へ移る。

【０１５２】

ステップＳＰ２１において制御部６０は、アクセス受付部６１（図１５）により、照会アドレスＡＤＡにアクセスされたか否かを判定する。ここで否定結果が得られると、制御部６０は再びステップＳＰ２１を繰り返すことにより、メール端末装置１６からの照会アドレスＡＤＡへのアクセスを待ち受ける。

【０１５３】

ステップＳＰ２２において制御部６０は、アクセス受付部６１によって、添付ファイル情報データベースＤＢ１２を参照することにより照会アドレスＡＤＡに対応付けられた暗号パスワードＰＣ及び受信側メールアドレスＡＤＲを取得し、次のステップＳＰ２３へ移る。

【０１５４】

ステップＳＰ２３において制御部６０は、暗号パスワードＰＣを本文に記したパスワード通知メールＭＰを生成し、次のステップＳＰ２４へ移る。

【０１５５】

ステップＳＰ２４において制御部６０は、受信側メールアドレスＡＤＲに宛ててパスワード通知メールＭＰを送信することにより、一連の暗号パスワードＰＣを通知する処理を終了し、再度ステップＳＰ２１へ戻ることにより、次の照会アドレスへのアクセスを待ち受ける。

【０１５６】

（２－５）動作及び効果

以上の構成において、第２の実施の形態における電子メールシステム５０の添付ファイル暗号化装置５７は、メール端末装置１６から添付ファイルメールＭＡが送信されると、送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲに対応付けられた暗号化ルールに従って添付ファイルＦＡを暗号化することにより暗号ファイルＦＣとし、当該暗号ファイルＦＣを添付した暗号ファイルメールＭＣ２を受信側メールアドレスＡＤＲに宛てて送信し、メール端末装置２４に受信させる。

【０１５７】

さらに添付ファイル暗号化装置５７は、照会アドレスＡＤＡを記した送信完了メールＭＮ２をメール端末装置１６へ送信する。これに応じてメール端末装置１６のユーザにより照会アドレスＡＤＡにアクセスされると、添付ファイル暗号化装置５７は、メール端末装置２４に対して、暗号ファイルメールＭＣ２と別個の電子メールでなるパスワード通知メールＭＰにより暗号ファイルＦＣの暗号パスワードＰＣを通知する。

【０１５８】

すなわち添付ファイル暗号化装置５７は、第１の実施の形態における添付ファイル暗号化装置１７と同様に、添付ファイルＦＡを暗号化した暗号ファイルＦＣの状態で各種ネットワークを経由させメール端末装置２４に受信させ、さらに当該暗号ファイルＦＣの復号化に必要な暗号パスワードＰＣを別個の電子メールとして送信するため、仮に暗号ファイルメールＭＣ２が第三者により盗聴されたとしても、暗号パスワードＰＣまでは知られないため、暗号ファイルＦＣが解読され添付ファイルＦＡの内容が知られ、或いは改竄される可能性を事実上皆無とすることができる。

【０１５９】

このとき電子メールシステム５０では、メール端末装置１６のユーザにより照会アドレスＡＤＡにアクセスされるだけで、パスワード通知メールＭＰを送信することができるため、当該ユーザにパスワード通知メールＭＰを作成させる、或いは郵便、電話、ファクシミリ等の通信手段によって当該暗号パスワードＰＣを通知させるといった煩雑な作業をさせずに済む。

【０１６０】

また電子メールシステム５０では、例えばユーザの手作業により暗号パスワードＰＣをコピーアンドペーストによりパスワード通知メールＭＰの文章中に貼り付ける際に、ダブルクリックによる単語選択をした場合に「－」や「＝」等の記号が選択されないために不完全なパスワードを通知してしまう、といった人為的なミスを誘発させずに済む。

【０１６１】

さらに電子メールシステム５０では、送信完了メールＭＮ２に記された照会アドレスＡＤＡをメール端末装置１６のユーザに敢えて手作業でクリックさせるため、このときに当該ユーザに送信先の電子メールアドレスを確認させることができる。このため電子メールシステム５０では、仮に暗号ファイルメールＭＣ２の送信先アドレスを誤って第三者に暗号ファイルＦＣを送信してしまったとしても、ユーザが当該送信先アドレスを誤ったことに気付き、照会アドレスＡＤＡにアクセスせずパスワード通知メールＭＰを送信しないことにより、第三者が当該暗号ファイルＦＣを復号化し得ないため、添付ファイルＦＡの内容を当該第三者に知られずに済む。

【０１６２】

また添付ファイル暗号化装置５７は、暗号ファイルメールＭＣ２ごとに専用の照会アドレスＡＤＡを生成し、これを送信完了メールＭＮ２に記してメール端末装置１６へ送信するため、もとの添付ファイルメールＭＡを送信したメール端末装置１６のユーザ以外に当該照会アドレスＡＤＡが知られることが無く、当該ユーザの意に反してパスワード通知メールＭＰが送信されることを未然に防止することができる。

【０１６３】

さらに電子メールシステム５０では、第１の実施の形態と同様、添付ファイル暗号化装置５７により暗号ファイルＦＣを暗号化する際、圧縮方式として広く利用されているＺＩＰ方式とパスワードによる暗号化とを組み合わせた「パスワード付きＺＩＰ形式」としているため、暗号ファイルメールＭＣ２を受信したメール端末装置２４に暗号パスワードＰＣを通知することにより、当該メール端末装置２４によってほぼ確実に元の添付ファイルＦＡに復元させることができる。

【０１６４】

以上の構成によれば、電子メールシステム５０は、添付ファイル暗号化装置５７によって、メール端末装置１６から送信された添付ファイルメールＭＡの添付ファイルＦＡを暗号化し暗号ファイルメールＭＣ２をメール端末装置２４へ送信すると共に送信完了メール

ＭＮ２をメール端末装置１６へ送信し、当該送信完了メールＭＮ２に記された照会アドレスＡＤＡにアクセスされたことに応じてパスワード通知メールＭＰを送信することにより、添付ファイルＦＡを自動的に暗号化することができると共にユーザに手間をかけさせず安全に暗号パスワードＰＣを正当なユーザにのみ通知することができるので、メール配信の仕組みを利用して添付ファイルＦＡを安全かつ容易に受け渡すことができる。

【０１６５】

（３）他の実施の形態

なお上述した第２の実施の形態においては、送信完了メールＭＮ２に照会アドレスＡＤＡと共に暗号パスワードＰＣを記すようにした場合について述べたが（図１３）、本発明はこれに限らず、当該送信完了メールＭＮ２に暗号パスワードＰＣを記さず照会アドレスＡＤＡのみを記しても良い。これにより、メール端末装置１６のユーザに対して、暗号パスワードＰＣの管理に気を遣わせずに済む。

【０１６６】

また上述した第２実施の形態においては、照会アドレスＡＤＡにアクセスされたときに限りパスワード通知メールＭＰを送信するようにした場合について述べたが、本発明はこれに限らず、例えば添付ファイル暗号化装置５７が、暗号ファイルメールＭＣを送信すると共に、無条件でパスワード通知メールＭＰを通知するようにしても良く、或いは添付ファイルメールＭＡの「件名」欄に所定のキーワードを含むことにより、これらを切り換えるようにする等しても良い。

【０１６７】

さらに上述した第１の実施の形態においては、暗号化ルールデータベースＤＢ１（図８（Ａ））により、送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲに応じた暗号化ルールを定めるようにした場合について述べたが、本発明はこれに限らず、例えば受信側メールアドレスＡＤＲに関わらず送信側メールアドレスＡＤＳのみに応じて暗号化ルールを定めるようにし、或いは反対に送信側メールアドレスＡＤＳに関わらず受信側メールアドレスＡＤＲのみに応じて暗号化ルールを定めるようにし、さらには送信側メールアドレスＡＤＳ及び受信側メールアドレスＡＤＲに関わらず唯一の暗号化ルールを定めるようにしても良い。

【０１６８】

さらに上述した第１の実施の形態においては、メールの本文ＢＤ（図３（Ｂ））の末尾に照会情報ＩＮＦを追記するようにした場合について述べたが、本発明はこれに限らず、例えば特定の受信側メールアドレスＡＤＲに対する暗号ファイルメールＭＣの本文ＢＤに当該照会情報ＩＮＦを追記しないようにし、或いはパスワードの種類ＴＰ（図８（Ａ））が「固定」である場合に当該照会情報ＩＮＦを追記しないようにする等、種々の条件により当該照会情報ＩＮＦを本文ＢＤに追記しないようにしても良い。

【０１６９】

これにより、暗号ファイルメールＭＣを傍受した第三者に対して、暗号パスワードＰＣを取得するための手段があることを敢えて知らせないようにすることができる。

【０１７０】

さらに上述した第１の実施の形態においては、暗号化ルールのキーワード（図８（Ａ））としてキーワードとなる文字列、「全て」、「なし」、或いは「ｐａｓｓｗｏｒｄ：」のいずれかが予め選択されるようにした場合について述べたが、本発明はこれに限らず、例えば「なし」を選択できないようにし、或いは無条件で「ｐａｓｓｗｏｒｄ：」とする等、選択対象を制限するようにしても良い。

【０１７１】

またキーワードの記載箇所としては、添付ファイルメールＭＡの件名欄以外にも、本文ＢＤの冒頭や末尾、或いは宛先欄等の様々な箇所としても良い。

【０１７２】

さらに上述した第１の実施の形態においては、暗号化ルールのパスワードの種類ＴＰ（図８（Ａ））として、「使い捨て」、「固定」、「毎回指定」、及び「なし」の４種類の

いずれかが選択されるようにした場合について述べたが、本発明はこれに限らず、例えば「なし」を選択できないようにし、或いは無条件で「使い捨て」とする等、選択対象を制限するようにしても良い。

【０１７３】

さらに上述した実施の形態においては、添付ファイルＦＡを暗号化する際、「パスワード付きＺＩＰ形式」の暗号ファイルＦＣに変換するようにした場合について述べたが、本発明はこれに限らず、当該添付ファイルＦＡを種々のファイル形式でなる暗号ファイルＦＣに変換するようにしても良い。この場合、任意の暗号パスワードＰＣを暗号鍵として指定でき、またメール端末装置２４により容易かつ確実に当該暗号ファイルＦＣを復号化できることが望ましい。

【０１７４】

さらに上述した第２の実施の形態においては、添付ファイル暗号化装置５７によって、添付ファイルメールＭＡの宛先ごとに専用の照会アドレスＡＤＡを生成するようにした場合について述べたが、本発明はこれに限らず、例えば添付ファイルメールＭＡに複数の添付ファイルＦＡが添付されている場合に、添付ファイルＦＡごとに異なる暗号パスワードＰＣを用いてそれぞれ暗号化し、添付ファイルＦＡごとに専用の照会アドレスＡＤＡを生成する等しても良い。

【０１７５】

さらに上述した第２の実施の形態においては、添付ファイルメールＭＡの宛先ごとに生成した専用の照会アドレスＡＤＡが記された送信完了メールＭＮ２をメール端末装置１６へ送信し、当該メール端末装置１６のユーザの操作により、ウェブブラウザ等を介して照会アドレスＡＤＡにアクセスされた場合に、パスワード通知メールＭＰを生成・送信するようにした場合について述べたが、本発明はこれに限らず、例えば添付ファイルメールＭＡの宛先ごとに専用の照会電子メールアドレスを生成した上で、当該照会電子メールアドレスが返信先に指定され、或いは当該照会電子メールアドレスが本文中に記された送信完了メールＭＮ２をメール端末装置１６へ送信し、当該メール端末装置１６のユーザの操作により、照会電子メールアドレスへ宛てて電子メールが返信又は送信された場合に、パスワード通知メールＭＰを生成及び送信する等しても良い。

【０１７６】

さらに上述した第２の実施の形態においては、図１１のシーケンスＳＱ４２において、パスワード通知メールＭＰにより暗号パスワードＰＣをメール端末装置２４のユーザに通知するようにした場合について述べたが、本発明はこれに限らず、例えばインスタントメッセージにより暗号パスワードＰＣを通知し、又は暗号パスワードＰＣを記載した文書を自動生成してファクシミリにより送信することにより通知し、或いは音声合成等により音声化した暗号パスワードＰＣを電話により通知する等、種々の通知手段を用いるようにしても良い。

【０１７７】

さらに上述した第２の実施の形態においては、添付ファイルＦＡのみを暗号化し、メール本文ＢＤは平文のままとする場合について述べたが、本発明はこれに限らず、メール本文も暗号化するようにしても良い。この場合、例えば添付ファイルメールＭＡの件名欄に所定のキーワードを記述することにより、メール本文ＢＤも暗号化することを指定できるようにすればよい。

【０１７８】

さらに上述した実施の形態においては、添付ファイルＦＡに対してメール判別生成部４２（図７）により添付ファイル情報データベースＤＢ２（図８（Ｂ））における一意のファイル識別子ＦＩＤを割り当てるようにした場合について述べたが、本発明はこれに限らず、例えばメールヘッダに含まれ事実上一意である「Ｍｅｓｓａｇｅ－Ｉｄ」を利用して暗号ファイルＦＣを特定する等しても良い。

【０１７９】

さらに上述した第１の実施の形態においては、メール端末装置２４から添付ファイル暗

号化装置１７に対してアクセスする際にウェブブラウザを介してＳＳＬを利用したセキュアな通信を用いるようにした場合について述べたが、本発明はこれに限らず、例えばｔｅｌｎｅｔとＳＳＬとを組み合わせたセキュアな通信やＦＴＰ（File Transfer Protocol）とＳＳＬとを組み合わせたセキュアな通信等により暗号パスワードＰＣを通知するようにしても良い。

【０１８０】

さらに上述した第１の実施の形態においては、添付ファイル暗号化装置１７が暗号パスワードＰＣを通知するようにした場合について述べたが、本発明はこれに限らず、例えば添付ファイル暗号化装置１７と別に、ユーザ情報データベースＤＢ４を有すると共に当該添付ファイル暗号化装置１７の添付ファイルＤＢにアクセス可能な暗号パスワード通知用サーバを用意しておき、当該暗号パスワード通知用サーバが暗号パスワード通知処理手順ＲＴ２（図１０）を実行しメール端末装置２４に対して暗号パスワードＰＣを通知するようにしても良い。この場合、添付ファイル暗号化装置１７と暗号パスワード通知用サーバとの間の通信についてはセキュリティが確保されていることが望ましい。

【０１８１】

同様に、第２の実施の形態においても、添付ファイル暗号化装置５７が照会アドレスＡＤＡに基づいたアクセスを受け付けるようにした場合について述べたが、本発明はこれに限らず、例えば添付ファイル暗号化装置５７と別に、メール端末装置１６等からのアクセスを受け付けパスワード通知メールＭＰを送信するパスワード通知サーバを用意しておくようにしても良い。この場合パスワード通知サーバは、例えば添付ファイル暗号化装置５７との連携により当該パスワード通知サーバが照会アドレスＡＤＡを生成して管理し、当該照会アドレスＡＤＡに対するアクセスに基づき、パスワード通知メールＭＰをメール端末装置２４へ送信するようにしても良い。

【０１８２】

さらに上述した第１の実施の形態においては、メール端末装置２４から添付ファイル暗号化装置１７に正しくアクセスされた際に暗号パスワードＰＣを通知し、第２の実施の形態においては、メール端末装置１６から照会アドレスＡＤＡにアクセスされた際に添付ファイル暗号化装置５７がパスワード通知メールＭＰを送信するようにした場合について述べたが、本発明はこれに限らず、例えば両者を組み合わせるようにしても良い。

【０１８３】

この場合、添付ファイル暗号化装置１７は、受信側メールアドレスＡＤＲが既に登録されたものであれば、第１の実施の形態の手法を用い、当該受信側メールアドレスＡＤＲが登録されていなければ、第２の実施の形態の手法を用いるようにすれば良い。

【０１８４】

さらに上述した第１及び第２の実施の形態においては、添付ファイル暗号化装置１７及び５７を独立した装置として第１のネットワーク群（図１）内の内部ネットワーク１４に接続するようにした場合について述べたが、本発明はこれに限らず、例えばメールサーバ１５に添付ファイル暗号化プログラム及び暗号パスワード通知プログラムをインストールして添付ファイル暗号化処理手順ＲＴ１（図９）並びに暗号パスワード通知処理手順ＲＴ２（図１０）及びＲＴ３（図１７）を実行させることにより、当該メールサーバ１５に添付ファイル暗号化装置１７及び５７の機能を実装するようにする等、ネットワーク上の種々の情報処理装置に添付ファイル暗号化処理手順ＲＴ１（図９）並びに暗号パスワード通知処理手順ＲＴ２（図１０）及びＲＴ３（図１７）を実行させることにより添付ファイル暗号化装置１７及び５７の機能を実装するようにしても良い。

【０１８５】

この場合、添付ファイル暗号化装置１７及び５７の機能が実装される情報処理装置としては、一般的なコンピュータ装置やサーバ装置等、図６に示したような回路構成を有していれば良い。

【０１８６】

さらに上述した第１の実施の形態においては、制御部３０において添付ファイル暗号化

処理手順ＲＴ１（図９）及び暗号パスワード通知処理手順ＲＴ２（図１０）を実行することによりソフトウェアによって添付ファイルＦＡの暗号化処理及び暗号パスワードＰＣの通知処理を実行するようにした場合について述べたが、本発明はこれに限らず、例えばメール受信部４１、メール判別生成部４２（図７）、添付ファイル暗号化部４３、メール送信部４４及びパスワード通知部４５をそれぞれハードウェアによって実現することにより、添付ファイルＦＡの暗号化処理及び暗号パスワードＰＣの通知処理を実行するようにしても良い。

【０１８７】

同様に第２の実施の形態においても、制御部６０において添付ファイル暗号化処理手順ＲＴ１（図９）及び暗号パスワード通知処理手順ＲＴ３（図１７）を実行することによりソフトウェアによって添付ファイルＦＡの暗号化処理及び暗号パスワードＰＣの通知処理を実行するようにした場合について述べたが、本発明はこれに限らず、例えばメール受信部４１、メール判別生成部４２（図１５）、添付ファイル暗号化部４３、メール送信部４４及びアクセス受付部６１をそれぞれハードウェアによって実現することにより、添付ファイルＦＡの暗号化処理及び暗号パスワードＰＣの通知処理を実行するようにしても良い。

【０１８８】

さらに上述した第１及び第２の実施の形態においては、添付ファイル暗号化プログラム及び暗号パスワード通知プログラムをハードディスクドライブ３４に格納するようにした場合について述べたが、本発明はこれに限らず、添付ファイル暗号化プログラム及び暗号パスワード通知プログラムを例えばＲＯＭ３３に予め記憶させておく他、図示しないＣＤ－ＲＯＭ（Compact Disc-Read Only Memory）や小型メモリーカード等の挿脱可能な記憶媒体から読み出し、或いはネットワークインタフェース３６や図示しないＵＳＢ（Universal Serial Bus）インタフェース等を介して外部のコンピュータ等から受信する等、当該添付ファイル暗号化プログラム及び暗号パスワード通知プログラムを外部から取得して実行するようにしても良い。

【０１８９】

さらに上述した実施の形態においては、受信手段としてのメール受信部４１と、暗号化手段としてのメール判別生成部４２及び添付ファイル暗号化部４３と、送信手段としてのメール送信部４４と、受付手段としてのアクセス受付部６１と、通知手段としてのメール判別生成部４２及びメール送信部４４とによって電子メール中継装置としての添付ファイル暗号化装置５７を構成する場合について述べたが、本発明はこれに限らず、その他種々の回路構成でなる受信手段と、暗号化手段と、送信手段と、受付手段と、通知手段とによって電子メール中継装置を構成するようにしても良い。

【産業上の利用可能性】

【０１９０】

本発明は、電子メールを利用して添付ファイルを受け渡す種々のネットワークでも利用できる。

【図面の簡単な説明】

【０１９１】

【図１】電子メールシステムの全体構成を示すブロック図である。

【図２】第１の実施の形態におけるメール及び添付ファイルの送受信シーケンスを示すシーケンスチャートである。

【図３】第１の実施の形態におけるメールの内容の例を示す略線図である。

【図４】第１の実施の形態における送信完了メールの例を示す略線図である。

【図５】第１の実施の形態におけるメール及び添付ファイルの流れを示す略線図である。

【図６】添付ファイル暗号化装置の回路構成を示すブロック図である。

【図７】第１の実施の形態における添付ファイル暗号化装置の機能構成を示すブロック図である。

【図８】第１の実施の形態におけるデータベースの構成を示す略線図である。

【図９】添付ファイル暗号化処理手順を示すフローチャートである。
【図１０】第１の実施の形態における暗号パスワード通知処理手順を示すフローチャートである。
【図１１】第２の実施の形態におけるメール及び添付ファイルの送受信シーケンスを示すシーケンスチャートである。
【図１２】第２の実施の形態におけるメールの内容の例を示す略線図である。
【図１３】第２の実施の形態における送信完了メールの例を示す略線図である。
【図１４】第２の実施の形態におけるメール及び添付ファイルの流れを示す略線図である。
【図１５】第２の実施の形態における添付ファイル暗号化装置の機能構成を示すブロック図である。
【図１６】第２の実施の形態におけるデータベースの構成を示す略線図である。
【図１７】第２の実施の形態における暗号パスワード通知処理手順を示すフローチャートである。
【符号の説明】
【０１９２】
１、５０……電子メールシステム、１６、２４……メール端末装置、１７、５７……添付ファイル暗号化装置、３０、６０……制御部、３１……ＣＰＵ、３４……ハードディスクドライブ、４１……メール受信部、４２……メール判別生成部、４３……添付ファイル暗号化部、４４……メール送信部、４５……パスワード通知部、６１……アクセス受付部、Ｍ……メール、ＭＡ……添付ファイルメール、ＭＣ、ＭＣ２……暗号ファイルメール、ＭＮ、ＭＮ２……暗号通知メール、ＭＰ……パスワード通知メール、ＦＡ……添付ファイル、ＭＡ……暗号ファイル、ＰＣ……暗号パスワード、ＩＮＦ……照会情報、ＡＤＳ……送信側メールアドレス、ＡＤＲ……受信側メールアドレス、ＡＤＡ……照会アドレス、ＦＩＤ……ファイル識別子、ＰＥ……認証用パスワード、ＰＩ……照会用パスワード、ＤＢ１……暗号化ルールデータベース、ＤＢ２……添付ファイル情報データベース、ＤＢ４……ユーザ情報データベース。

【図１】

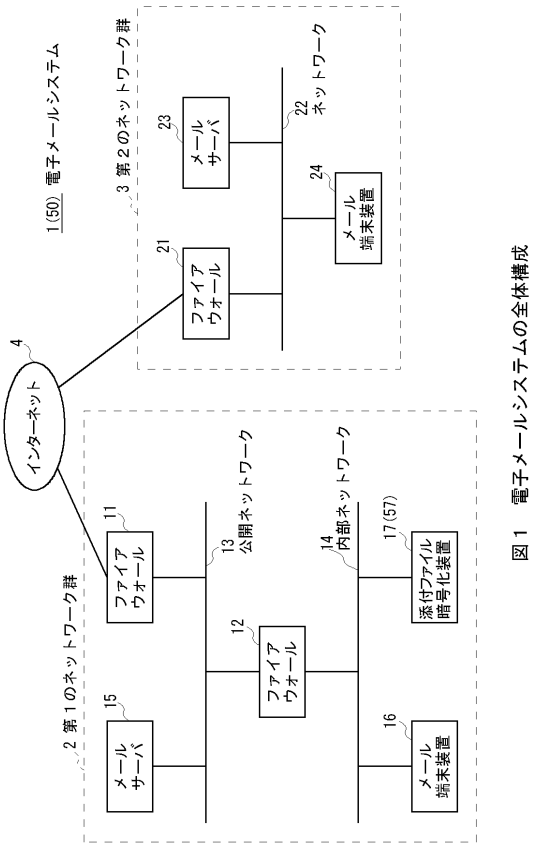


図１　電子メールシステムの全体構成

【図２】

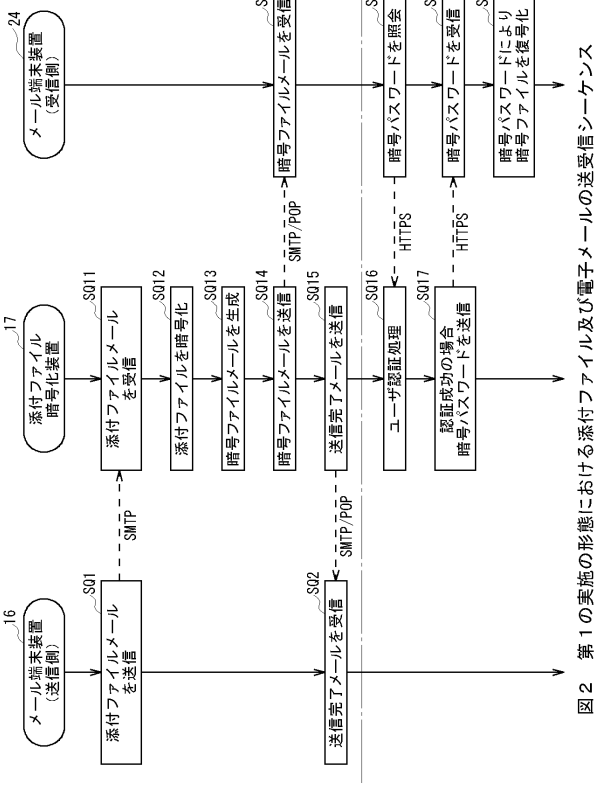
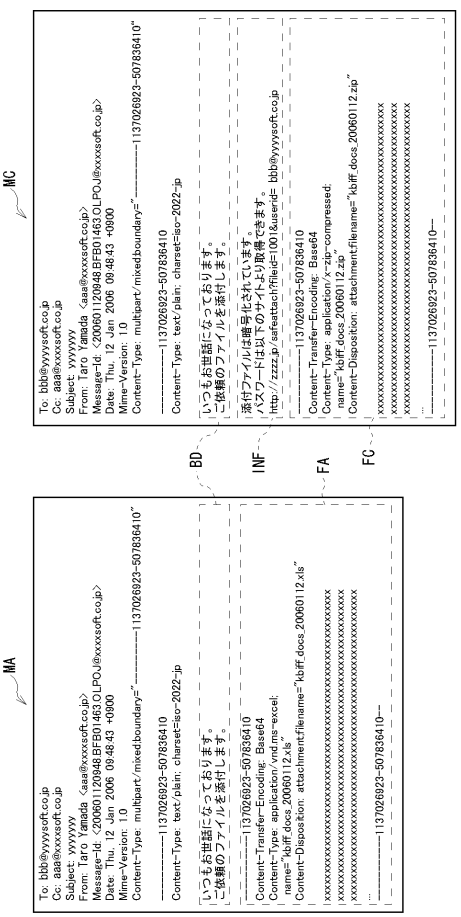


図２　第１の実施の形態における添付ファイル及び電子メールの送受信シーケンス

【図３】



（A）暗号化前のメールの内容　　（B）暗号化後のメールの内容

図３　第１の実施の形態におけるメールの内容の例

【図４】

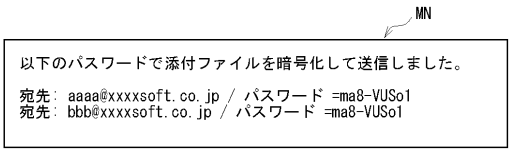


図４　第１の実施の形態における送信完了メールの例

【図５】

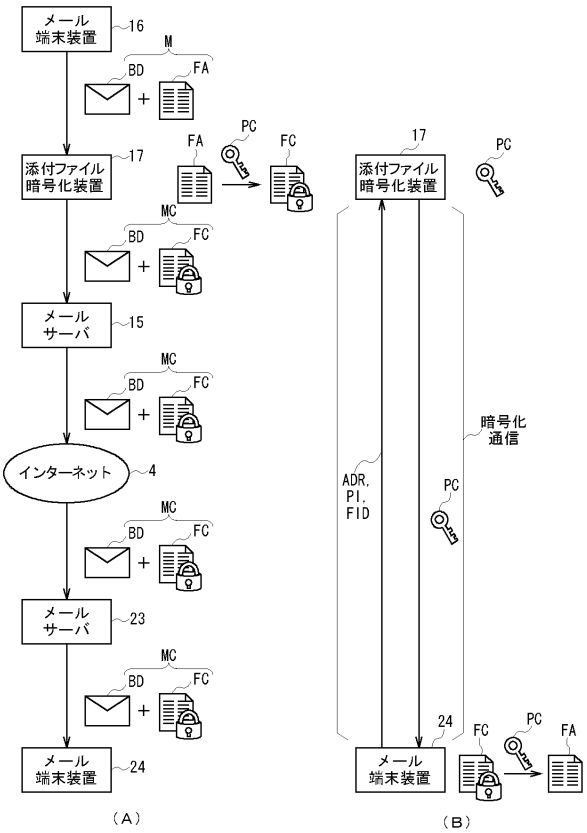


図５　第１の実施の形態におけるメール及び添付ファイルの流れ

【図６】

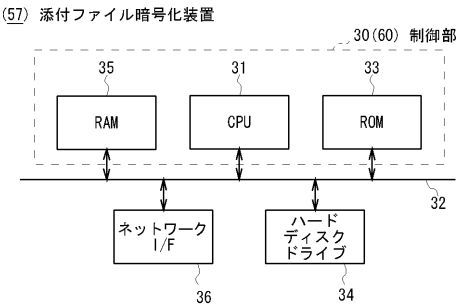
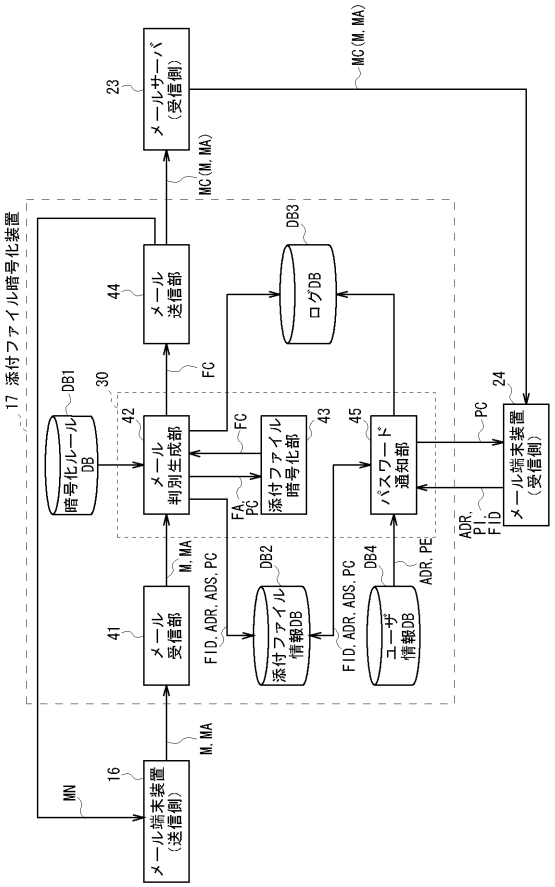


図６　添付ファイル暗号化装置の回路構成

【図７】



【図８】

図７　第１の実施の形態における添付ファイル暗号化装置の機能構成

DB1　ADS　KW　TP

送信側メールアドレス	受信側メールアドレス	キーワード	パスワードの種類
aaa@xxxxsoft.co.jp	bbb@yyyysoft.co.jp	<全て>	使い捨て
	eee@zzzz.ne.jp	"%%%"	固定："opqrstu"
ccc@xxxxsoft.co.jp	fff@vvvvoffice.co.jp	<なし>	なし
	ggg@wwwwdesign.co.jp	"password"	毎回指定
：	：	：	：

（A）暗号化ルールデータベース

DB2　FID　PC　ADS　ADR

ファイル識別子	暗号パスワード	送信側メールアドレス	受信側メールアドレス
1001	a3b4c5d6	aaa@xxxxsoft.co.jp	bbb@yyyysoft.co.jp
1002	thankyou	ccc@xxxxsoft.co.jp	ggg@wwwwdesign.co.jp
：	：	：	：

（B）添付ファイル情報データベース

DB4　ADR　PE

受信側メールアドレス	認証用パスワード
bbb@yyyysoft.co.jp	4321hijk
ggg@wwwwdesign.co.jp	cdef4567
：	：

（C）ユーザ情報データベース

図８　第１の実施の形態におけるデータベースの構成

【図９】

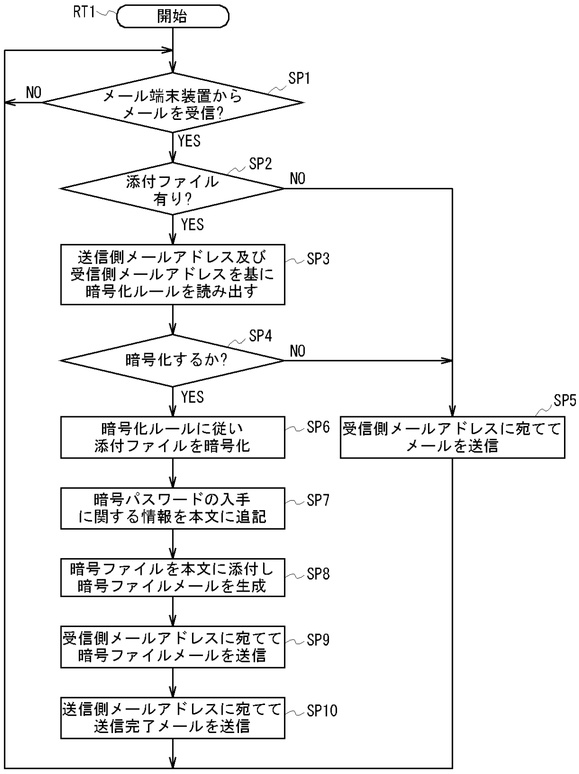


図９　添付ファイル暗号化処理手順

【図１０】

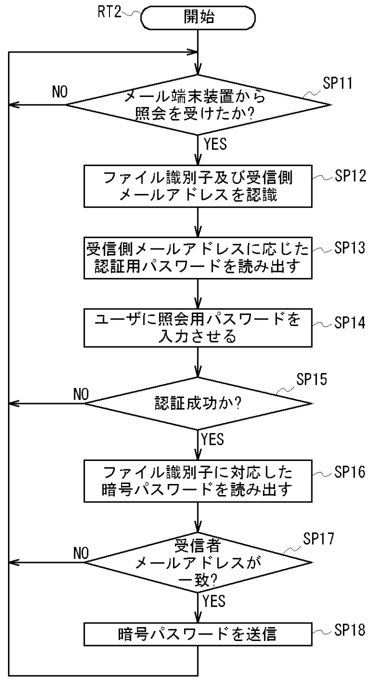


図１０　第１の実施の形態における暗号パスワード通知処理手順

【図１１】

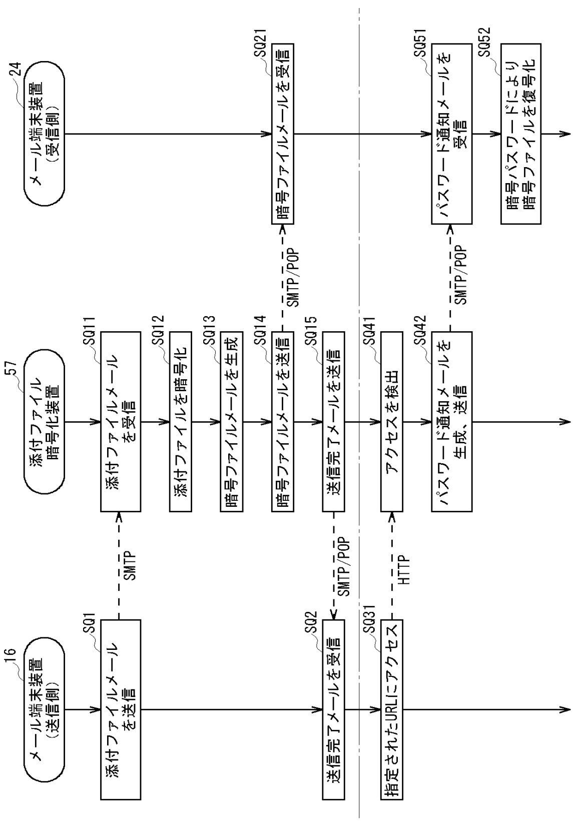


図１１　第２の実施の形態における添付ファイル及び電子メールの送受信シーケンス

【図１２】

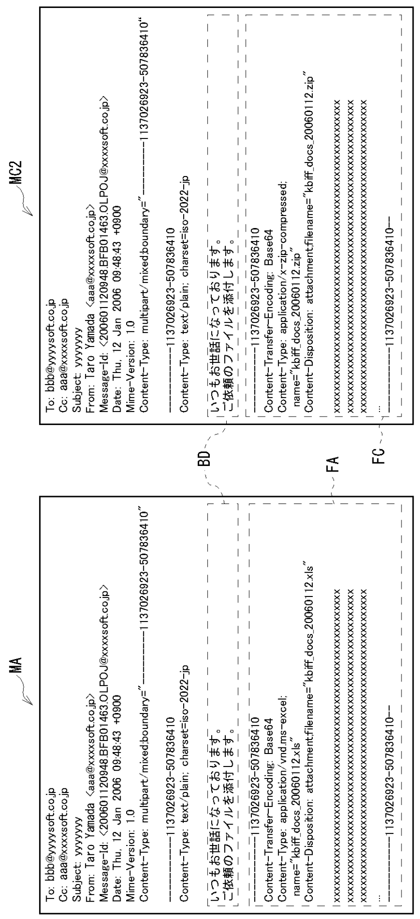


図１２　第２の実施の形態におけるメールの内容の例

【図１３】

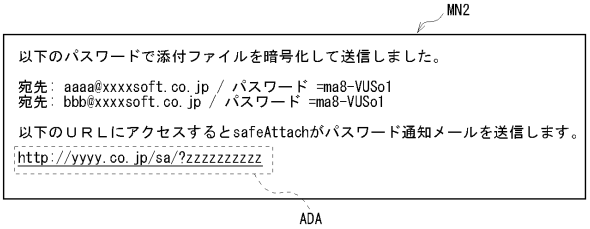


図１３　第２の実施の形態における送信完了メールの例

【図１４】

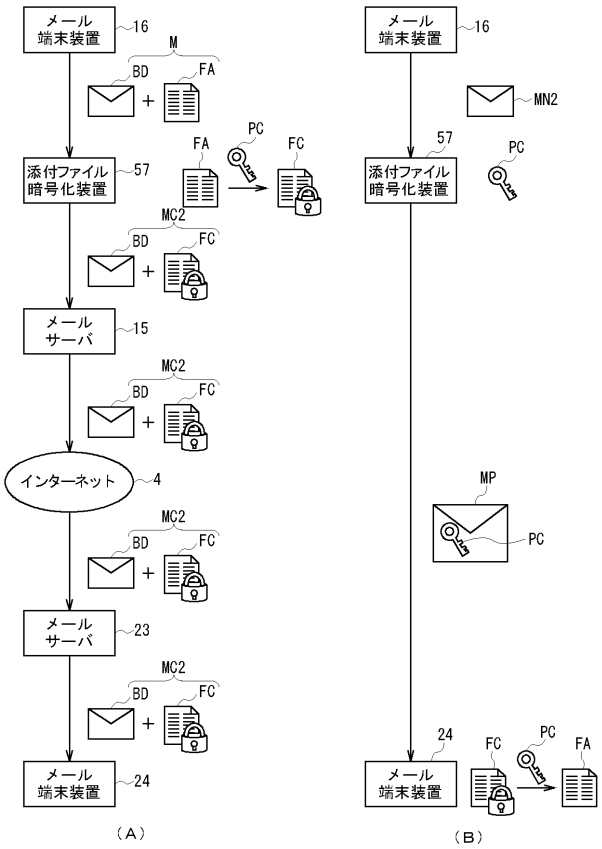


図１４　第２の実施の形態におけるメール及び添付ファイルの流れ

【図１５】

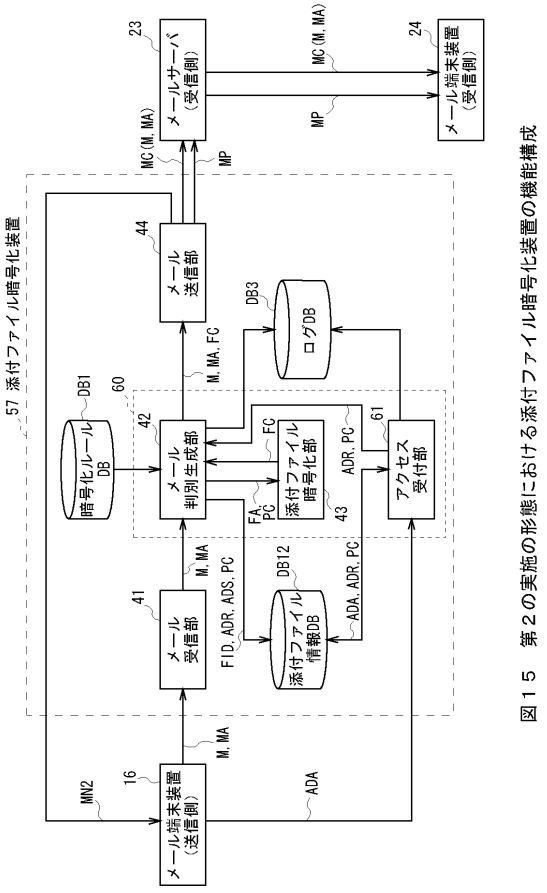


図１５　第２の実施の形態における添付ファイル暗号化装置の機能構成

【図１６】

（Ａ）暗号化ルールデータベース

DB1

送信側メールアドレス (ADS)	受信側メールアドレス (ADR)	キーワード (KW)	パスワードの種類 (TP)
aaa@xxxxsoft.co.jp	bbb@yyyysoft.co.jp	＜全て＞	使い捨て
	eee@zzzz.ne.jp	"%%%"	固定："opqrstu"
ccc@xxxxsoft.co.jp	fff@vvvvoffice.co.jp	＜なし＞	なし
	ggg@wwwwdesign.co.jp	"password:"	毎回指定
…	…	…	…

（Ｂ）添付ファイル情報データベース

DB12

ファイル識別子 (FID)	暗号パスワード (PC)	照会アドレス (ADA)	受信側メールアドレス (ADR)
1001	a3b4c5d6	yyyy.co.jp/sa/?zzzzzzzzzz	bbb@yyyysoft.co.jp
1002	thankyou	yyyy.co.jp/sa/?xxxxxxxxxx	ggg@wwwwdesign.co.jp
…	…	…	…

図１６　第２の実施の形態におけるデータベースの構成

【図１７】

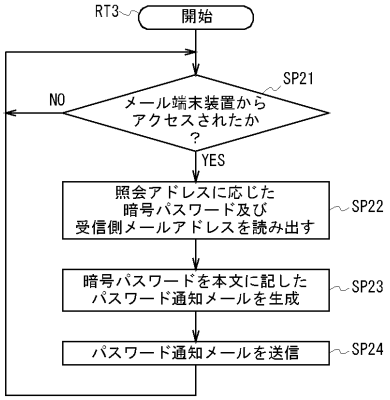


図１７　第２の実施の形態における暗号パスワード通知処理手順

フロントページの続き

(51)Int.Cl. F I
H04L 12/58 100Z

(56)参考文献 特開2007-150454（JP, A）
特開2007-324710（JP, A）
特開2003-178007（JP, A）
特開2005-285111（JP, A）
特開2007-281622（JP, A）

(58)調査した分野(Int.Cl., DB名)
H04L 9/08
G06F 13/00
H04L 12/22
H04L 12/58