(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2023-156423
(P2023-156423A)
(43)公開日　令和5年10月24日(2023.10.24)

(51)国際特許分類　FI
G06F 21/56 (2013.01)　G06F 21/56
H04L 51/08 (2022.01)　H04L 51/08
H04L 51/21 (2022.01)　H04L 51/21
G06F 21/53 (2013.01)　G06F 21/53

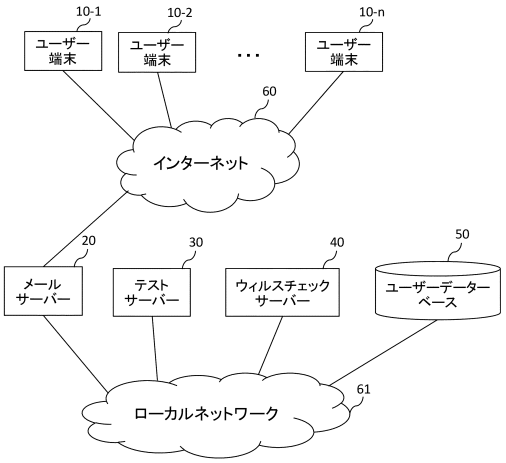
審査請求　有　請求項の数　5　OL　（全18頁）

(21)出願番号　特願2023-130663(P2023-130663)
(22)出願日　令和5年8月10日(2023.8.10)
(62)分割の表示　特願2021-107633(P2021-107633)の分割
原出願日　令和3年6月29日(2021.6.29)

(71)出願人　306029774
ビッグローブ株式会社
東京都品川区東品川四丁目１２番４号
(74)代理人　100123788
弁理士　宮崎 昭夫
(74)代理人　100127454
弁理士　緒方 雅昭
(72)発明者　加藤 理人
東京都品川区東品川四丁目１２番４号
ビッグローブ株式会社内

(54)【発明の名称】　危険性チェックシステム、危険度チェック方法及びプログラム

(57)【要約】
【課題】電子メッセージに暗号化された添付ファイルが含まれている場合であっても、ユーザーの手を煩わすことなく、添付ファイルに危険性があるかどうかをチェックする。
【解決手段】受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断し、電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するメールサーバー２０と、メールサーバー２０から送信されてきた添付ファイルとパスワードの候補とを受信するテストサーバー３０により生成され、抽出されたパスワードの候補を用いて、暗号化された添付ファイルを復号化する仮想コンピューターと、復号化された添付ファイルに危険性があるかどうかをチェックするウィルスチェックサーバー４０とを有する。
【選択図】図１



【特許請求の範囲】
【請求項１】
電子メッセージに添付された添付ファイルに危険性があるかどうかをチェックする危険性チェックシステムであって、
受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断手段と、
電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出手段とを有するメールサーバーと、
前記メールサーバーから送信されてきた前記添付ファイルと前記パスワードの候補とを受信するテストサーバーにより生成され、前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化する仮想コンピューターと、
前記復号化された添付ファイルに危険性があるかどうかをチェックするウィルスチェックサーバーとを有する、危険性チェックシステム。
【請求項２】
電子メッセージに添付された添付ファイルに危険性があるかどうかをチェックする危険性チェックシステムであって、
受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断手段と、
電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出手段と、
前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化する復号化手段と、
前記復号化された添付ファイルに危険性があるかどうかをチェックする危険性チェック手段と、
前記パスワード抽出手段にてパスワードの候補が抽出された場合に、前記添付ファイルが添付された電子メッセージの宛先に対応づけて予めユーザー毎に選択されて登録されたアプリケーションが前記復号化手段としてインストールされた仮想コンピューターを生成する仮想コンピューター生成手段とを有する、危険性チェックシステム。
【請求項３】
メールサーバーが受信した電子メッセージに添付された添付ファイルに危険性があるかどうかをウィルスチェックサーバーがチェックする危険性チェック方法であって、
前記メールサーバーが、受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断ステップと、
前記メールサーバーが、電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出ステップと、
前記メールサーバーから送信されてきた前記添付ファイルと前記パスワードの候補とを受信するテストサーバーが生成する仮想コンピューターが、前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化する復号化ステップと、
前記ウィルスチェックサーバーが、前記復号化された添付ファイルに危険性があるかどうかをチェックする危険性チェックステップとを行う、危険性チェック方法。
【請求項４】
メールサーバーが受信した電子メッセージに添付された添付ファイルに危険性があるかどうかをウィルスチェックサーバーがチェックする危険性チェック方法であって、
前記メールサーバーが、受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断ステップと、

前記メールサーバーが、電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出ステップと、
前記パスワード抽出ステップにてパスワードの候補が抽出された場合に、前記メールサーバーから送信されてきた前記暗号化された添付ファイルと前記パスワードの候補とを受信するテストサーバーが、前記添付ファイルが添付された電子メッセージの宛先に対応づけて予めユーザー毎に選択されて登録されたアプリケーションがインストールされた仮想コンピューターを生成する仮想コンピューター生成ステップと、
前記仮想コンピューターが、前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化する復号化ステップと、
前記ウィルスチェックサーバーが、前記復号化された添付ファイルに危険性があるかどうかをチェックする危険性チェックステップとを行う、危険性チェック方法。
【請求項５】
電子メッセージに添付された添付ファイルに危険性があるかどうかをチェックするコンピュータに実行させるプログラムであって、
前記コンピュータに、
受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断手順と、
電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出手順と、
前記パスワード抽出手順にてパスワードの候補が抽出された場合に、前記添付ファイルが添付された電子メッセージの宛先に対応づけて予めユーザー毎に選択されて登録されたアプリケーションがインストールされた仮想コンピューターを生成する仮想コンピューター生成手順と、
前記仮想コンピューターに、前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化させる復号化手順と、
前記復号化された添付ファイルに危険性があるかどうかをチェックする危険性チェック手順とを実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子メールやチャット、ＳＮＳ（Social NetworkingService）、各種メッセージ等の電子メッセージに添付された添付ファイルの危険性をチェックする危険性チェックシステム、危険度チェック方法及びプログラムに関し、特に、添付ファイルが暗号化されていた場合の技術に関する。
【背景技術】
【０００２】
近年の情報通信技術の発達に伴い、情報のやりとりに電子メール等を利用することが一般的となっている。電子メール等は、即時性があるとともにファイルを添付することができる等といった利点がある一方、ウィルスメールやフィッシングメール等の不正メールの問題も有している。
【０００３】
従来は、そのような問題に対応するために、ウィルスメールやフィッシングメール等の不正メールをチェックするソフトウェアをパソコン等の端末にインストールし、端末にて受信した電子メールに対してチェックをかけていた。また、ウィルスメールやフィッシングメール等の不正メールをチェックするソフトウェアをメールサーバーにインストールし、メールサーバーにおいて、自身が管理するメールアドレスに対して送受信される電子メールに対してチェックをかけていた。また、ウィルスメールやフィッシングメールのよう

な危険性は、電子メールに添付された添付ファイルにも含まれている場合がある。その場合でもウィルス等をチェックするソフトウェアを用いれば、添付ファイルに危険性があるかどうかをチェックすることができる。

【０００４】

しかしながら、添付ファイルが暗号化されていた場合、添付ファイルに危険性があるかどうかをチェックすることができない。そこで、受信した電子メールに暗号化された添付ファイルが含まれている場合に、復号化に必要な情報をその電子メールの宛先に要求し、電子メールの宛先から通知された情報によって、暗号化された添付ファイルを復号化し、添付ファイルを含めて電子メールにウィルスが含まれているかどうかをチェックする仕組みが特許文献１に開示されている。特許文献１に開示された仕組みを用いれば、電子メールに添付された添付ファイルが暗号化されていても、添付ファイルにウィルス等の危険性があるかどうかをチェックすることができる。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２０１１－４１３２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、特許文献１に開示された仕組みにおいては、受信した電子メールに暗号化された添付ファイルが含まれている場合に、暗号化された添付ファイルを復号化するために必要な情報をその電子メールの宛先に要求することになるため、電子メールを受信したユーザーにとって煩わしさが生じてしまうという問題点がある。

【０００７】

本発明は、上述したような従来の技術が有する問題点に鑑みてなされたものであって、電子メール等の電子メッセージに暗号化された添付ファイルが含まれている場合であっても、ユーザーの手を煩わすことなく、添付ファイルに危険性があるかどうかをチェックすることができる危険性チェックシステム、危険度チェック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】

【０００８】

上記目的を達成するために本発明は、

電子メッセージに添付された添付ファイルに危険性があるかどうかをチェックする危険性チェックシステムであって、

受信した電子メッセージに暗号化された添付ファイルが添付されているかどうかを判断するファイル有無判断手段と、

電子メッセージに暗号化された添付ファイルが添付されていると判断された場合に、当該添付ファイルが添付された電子メッセージの本文またはヘッダーから、前記暗号化された添付ファイルを復号化するためのパスワードの候補を抽出するパスワード抽出手段とを有するメールサーバーと、

前記メールサーバーから送信されてきた前記添付ファイルと前記パスワードの候補とを受信するテストサーバーにより生成され、前記抽出されたパスワードの候補を用いて、前記暗号化された添付ファイルを復号化する仮想コンピューターと、

前記復号化された添付ファイルに危険性があるかどうかをチェックするウィルスチェックサーバーとを有する。

【発明の効果】

【０００９】

本発明によれば、電子メッセージに暗号化された添付ファイルが含まれている場合であっても、ユーザーの手を煩わすことなく、添付ファイルに危険性があるかどうかをチェックすることができる。

【図面の簡単な説明】
【００１０】
【図１】本発明の危険性チェックシステムの実施の一形態を示す図である。
【図２】図１に示したメールサーバーの構成を示すブロック図である。
【図３】図１に示したテストサーバーの構成を示すブロック図である。
【図４】図３に示した仮想コンピューター生成部にて生成された仮想コンピューターの構成を示すブロック図である。
【図５】図１に示したウィルスチェックサーバーの構成を示すブロック図である。
【図６】図１～図５に示した危険性チェックシステムを利用するユーザーがオプションサービス内容を登録する際の処理を説明するためのフローチャートである。
【図７】メールサーバーから送信されてユーザー端末にて表示されるオプションサービス内容設定画面の一部を示す図である。
【図８】メールサーバーから送信されてユーザー端末にて表示されるオプションサービス内容確認画面の一部を示す図である。
【図９】図１に示したユーザーデーターベースの一部を示す図である。
【図１０】図１～図５に示した危険性チェックシステムにおいて電子メールの危険性をチェックする際の処理を説明するためのフローチャートである。
【発明を実施するための形態】
【００１１】
以下に、本発明の実施の形態について図面を参照して説明する。
【００１２】
図１は、本発明の危険性チェックシステムの実施の一形態を示す図である。
【００１３】
本形態における危険性チェックシステムは図１に示すように、ユーザー端末１０－１～１０－ｎと、メールサーバー２０とがインターネット６０を介して接続可能となって構成され、メールサーバー２０と、テストサーバー３０と、ウィルスチェックサーバー４０と、ユーザーデーターベース５０とがローカルネットワーク６１を介して接続可能となって構成されている。なお、本発明にて危険度をチェックする電子メッセージは、電子メール以外に、チャットやＳＮＳ、メッセンジャーを用いた各種メッセージでもよい。扱う形態に応じで、例えば、メールサーバーは、チャットサーバーまたはＳＮＳサーバー、メッセンジャーサーバーのことを示すが、本形態では、説明を簡単にするために、電子メールを用いた例を説明する。また、本発明の危険性チェックシステムを構成するメールサーバー２０と、テストサーバー３０と、ウィルスチェックサーバー４０と、ユーザーデーターベース５０とは、各々１つではなく複数あっても構わないし、各々別々の装置ではなく２種類以上のサーバーが１つの装置で構成されていても構わないし、クラウドコンピューティングにて実現されていても構わない。
【００１４】
ユーザー端末１０は、１または複数あり、ユーザー端末１０－１～１０－ｎ（ｎは整数）として示す。ユーザー端末１０は、例えば、パーソナルコンピューターやスマートフォン、携帯電話等である。ユーザー端末１０－１～１０－ｎは、本システムを利用する各ユーザーが各々操作するものであり、ユーザーは、ユーザー端末１０－１～１０－ｎの内の自身が所有するユーザー端末１０を用いて電子メールを送受信する。なお、一人のユーザーが複数のユーザー端末１０を所有する場合もある。
【００１５】
メールサーバー２０は、契約しているユーザーのメールアドレスを管理し、そのメールアドレスに対応する電子メールの送受信を中継するメールサービスを提供するサーバー装置である。本形態においては、ユーザー端末１０－１～１０－ｎの各ユーザーが、メールサーバー２０によるメールサービスをそれぞれ契約していることで、メールサーバー２０は、提供するメールサービスについてユーザー端末１０－１～１０－ｎの各メールアドレスを管理し、各メールアドレスに対し、ＩＤとパスワードなどを用いた認証処理により対

応させたユーザー端末１０－１～１０－ｎに対して送受信される電子メールを中継することになる。なお、メッセンジャー等の場合は、メールアドレスの代わりに、アカウント名やＩＤ、電話番号などを用いてもよい。

【００１６】

図２は、図１に示したメールサーバー２０の構成を示すブロック図である。

【００１７】

図１に示したメールサーバー２０は図２に示すように、ユーザー管理部２１と、メール送受信部２２と、ファイル有無判断部２３と、パスワード抽出部２４と、仮想コンピューター生成指示部２５と、結果受信部２６と、メール保存部２７とを有している。

【００１８】

ユーザー管理部２１は、本願発明にて加入判断手段となるものである。ユーザー管理部２１は、メールサーバー２０を管理している企業が提供している電子メールサービスを契約しているユーザーのメールアドレスを管理するとともに、電子メールサービスに契約したユーザーが加入したオプションサービス内容をユーザーデーターベース５０に登録して管理する。

【００１９】

メール送受信部２２は、ユーザー管理部２１にて管理するメールアドレス宛ての電子メールを受信するとともに、ユーザー管理部２１にて管理するメールアドレスから送信された電子メールをインターネット６０上に送信する。

【００２０】

ファイル有無判断部２３は、メール送受信部２２にて受信した電子メールに、暗号化された添付ファイルが添付されているかどうかを判断する。

【００２１】

パスワード抽出部２４は、ファイル有無判断部２３において、メール送受信部２２にて受信した電子メールに暗号化された添付ファイルが添付されていると判断された場合に、特定の電子メールの本文から、暗号化された添付ファイルを復号化するためのパスワード候補として文字列を抽出する。なお、Ｘで始まる拡張ヘッダーにパスワードを示す文字が含まれる場合（例えば、X-password、X-pw等）は、特定の電子メールの本文ではなくヘッダーからパスワード候補を抽出しても構わない（本説明では、本文にパスワードが記載されるものとして説明する）。パスワード候補は、例えば、１バイトからなる文字列であり、パスワード候補にする条件やパスワード候補から除外する条件が、メールサーバー２０の記憶部（不図示）に予め記憶されている。この際、パスワード抽出部２４は、添付ファイルが添付された電子メールを、パスワードの候補を抽出するための特定の電子メールとしてもよいし、添付ファイルが添付された電子メールと同じ宛先の電子メールであって、添付ファイルが添付された電子メールを受信した時刻に対して所定時間以内に受信した電子メールを、パスワードの候補を抽出するための特定の電子メールとしてもよい。さらには、添付ファイルが添付された電子メールと返信または転送関係にある電子メールを、パスワードの候補を抽出するための特定の電子メールとしてもよい。

【００２２】

仮想コンピューター生成指示部２５は、パスワード抽出部２４にてパスワードの候補が抽出された場合に、テストサーバー３０に対して仮想コンピューターを生成するように指示する。その際、仮想コンピューター生成指示部２５は、ユーザー管理部２１がユーザーデーターベース５０にて管理しているユーザー毎のオプションサービス内容を参照し、テストサーバー３０に対してオプションサービス内容に応じた仮想コンピューターを生成するように指示する。また、仮想コンピューター生成指示部２５は、パスワード抽出部２４にて抽出されたパスワードの候補と、ファイル有無判断部２３において、暗号化された添付ファイルが添付されていると判断された電子メールに添付された添付ファイルとをテストサーバー３０に送信する。

【００２３】

結果受信部２６は、ウィルスチェックサーバー４０にてウィルスチェックを行った結果

を受信する。
【００２４】
メール保存部２７は、本願発明にてメッセージ保存手段となるものである。メール保存部２７は、メール送受信部２２にて受信した電子メールを、結果受信部２６にて受信した結果に応じた記憶領域に保存する。
【００２５】
テストサーバー３０は、メールサーバー２０からの指示に従って仮想コンピューターを生成し、生成した仮想コンピューターを用いて、メールサーバー２０が受信した電子メールに添付された添付ファイルを復号化するサーバー装置である。
【００２６】
図３は、図１に示したテストサーバー３０の構成を示すブロック図である。
【００２７】
図１に示したテストサーバー３０は図３に示すように、指示受付部３１と、仮想コンピューター生成部３２と、添付ファイル送信部３３とを有している。
【００２８】
指示受付部３１は、メールサーバー２０の仮想コンピューター生成指示部２５から送信された、仮想コンピューターを生成する指示を受け付ける。
【００２９】
仮想コンピューター生成部３２は、指示受付部３１にて受け付けた指示に基づいて仮想コンピューターを生成する。仮想コンピューター生成指示部２５からは、ユーザー管理部２１がユーザーデーターベース５０にて管理しているユーザー毎のオプションサービス内容に応じた仮想コンピューターを生成するように指示されている。ユーザーデーターベース５０にて管理しているユーザー毎のオプションサービス内容の詳細は後述するが、オプションサービス内容に含まれるアプリケーションがインストールされた仮想コンピューターを生成することになる。
【００３０】
添付ファイル送信部３３は、仮想コンピューター生成部３２にて生成した仮想コンピューターによって復号化した添付ファイルを送信する。
【００３１】
図４は、図３に示した仮想コンピューター生成部３２にて生成された仮想コンピューターの構成を示すブロック図である。なお、図３に示した仮想コンピューター生成部３２にて生成された仮想コンピューターは、一般的なパーソナルコンピューター等のユーザー端末１０と同等の機能を有しているが、本発明の動作と直接関係がない構成については、生成をしなくても構わない。本発明の動作に直接関係のある構成について図示及び説明し、その他の構成は省略して説明する。
【００３２】
図３に示した仮想コンピューター生成部３２にて生成された仮想コンピューターは図４に示すように、添付ファイル受付部３２ａと、パスワード受付部３２ｂと、復号化部３２ｃとを有している。
【００３３】
添付ファイル受付部３２ａは、メールサーバー２０の仮想コンピューター生成指示部２５からテストサーバー３０に送信された添付ファイルを受け付ける。
【００３４】
パスワード受付部３２ｂは、メールサーバー２０の仮想コンピューター生成指示部２５からテストサーバー３０に送信されたパスワードの候補を受け付ける。
【００３５】
復号化部３２ｃは、添付ファイル受付部３２ａにて受け付けた添付ファイルを、パスワード受付部３２ｂにて受け付けたパスワードの候補を用いて復号化する。
【００３６】
ウィルスチェックサーバー４０は、テストサーバー３０が生成した仮想コンピューター

によって復号化された添付ファイルについて、危険性があるかどうかのチェックであるウィルスチェックを行うサーバー装置である。

【００３７】

図５は、図１に示したウィルスチェックサーバー４０の構成を示すブロック図である。

【００３８】

図１に示したウィルスチェックサーバー４０は図５に示すように、添付ファイル受信部４１と、ウィルスチェック部４２と、結果送信部４３とを有している。

【００３９】

添付ファイル受信部４１は、テストサーバー３０から送信された復号化された添付ファイルを受信する。

【００４０】

ウィルスチェック部４２は、本願発明にて危険性チェック手段となるものである。ウィルスチェック部４２は、添付ファイル受信部４１にて受信した復号化された添付ファイルについて、危険性があるかどうかのチェックであるウィルスチェックを行う。

【００４１】

結果送信部４３は、ウィルスチェック部４２にてウィルスチェックを行った結果をメールサーバー２０に送信する。なお、本発明では、ウィルスチェックサーバー４０にて、復号化された添付ファイルを受信して、危険性があるかどうかチェックし、チェック結果をメールサーバー２０に送信しているが、テストサーバー３０にて、生成した仮想コンピューターにウィルスチェックアプリケーションをインストールし、インストールされたウィルスチェックアプリケーションが、仮想コンピューター上で復号化された添付ファイルを危険性があるかどうかチェックし、チェック結果をメールサーバー２０に送信してもよい。その場合、ウィルスチェックサーバー４０は、最新のウィルスチェックアプリケーション及びウィルスチェックに必要な最新のウィルスの定義ファイルを仮想コンピューターに提供する。

【００４２】

ユーザーデーターベース５０は、本システムに登録されたユーザーが希望したオプションサービス内容が、ユーザーを識別する識別子であるＩＤに対応づけて登録されているデータベース装置である。その詳細は後述する。また、メールアドレスやパスワード等も各ユーザーのＩＤに対応づけられて登録されている。ユーザーデーターベース５０は、例えば、データベースソフトウェアが実行可能に記憶されたサーバー装置でも、ＮＡＳ等のネットワークに接続された記憶装置でも、他のサーバー装置に内蔵または外付けされた記憶装置でも構わない。

【００４３】

以下に、上記のように構成された危険性チェックシステムにおける電子メールの危険性チェック方法について説明する。

【００４４】

まず、ユーザーがオプションサービス内容を登録する際の処理について説明する。

【００４５】

図６は、図１～図５に示した危険性チェックシステムを利用するユーザーがオプションサービス内容を登録する際の処理を説明するためのフローチャートである。

【００４６】

図１～図５に示した危険性チェックシステムを利用するユーザーが、オプションサービス内容を登録するために、ユーザー端末１０－１～１０－ｎの１つである例えばユーザー端末１０－１によってメールサーバー２０にアクセスすると（ステップＳ１）、ユーザー認証を行うため、例えば、ＩＤ及びパスワードを入力するための認証画面（生体認証などのその他の認証方法でも構わない）がメールサーバー２０から送信され（ステップＳ２）、ユーザー端末１０－１にて受信、表示される（ステップＳ３）。

【００４７】

ユーザー端末１０－１に表示された認証画面に対して、ユーザーに予め付与、設定され

たＩＤとパスワードが入力されて送信され（ステップＳ４）、メールサーバー２０にて受信されると（ステップＳ５）、メールサーバー２０のユーザー管理部２１において、ユーザーデーターベース５０を参照し、受信したＩＤとパスワードとを用いてユーザー認証を行う（ステップＳ６）。ユーザーデーターベース５０には、契約しているユーザーのメールアドレス等の情報が、ユーザーに予め付与、設定されたＩＤ及びパスワードと対応づけて登録されている。そのため、メールサーバー２０のユーザー管理部２１は、ユーザーデーターベース５０を参照することで、受信したＩＤとパスワードを用いてユーザー認証を行うことができ、認証が成功することで、そのＩＤとパスワードを送信してきたユーザー端末１０が、そのＩＤとパスワードに対応するメールアドレスのユーザーが所有するユーザー端末１０であると対応づけができる。

【００４８】

ユーザー認証を行った結果、照合が成功すると、契約しているユーザーであるとユーザー管理部２１において判定され、オプションサービス内容を設定登録するためのサービス内容設定画面がメールサーバー２０から送信され（ステップＳ７）、ユーザー端末１０－１にて受信、表示される（ステップＳ８）。

【００４９】

図７は、メールサーバー２０から送信されてユーザー端末１０－１～１０－ｎにて表示されるオプションサービス内容設定画面の一部を示す図である。

【００５０】

図７（ａ）に示すように、メールサーバー２０から送信されてユーザー端末１０－１にて表示されるオプションサービス内容設定画面には、電子メールサービスに関するオプションサービスとして、受信した電子メールに対する標準的な迷惑メールチェック（例えば、暗号化されていない添付ファイルのウィルスチェック、フィッシングサイトへのリンクの有無、スパムメールか否か等）や、暗号化された添付ファイルに対するウィルスチェック（フィッシングサイトへのリンクの有無などが含まれてもよい）をチェックボックスによって選択するためのオプションサービス選択領域７１が設けられている。また、オプションサービス選択領域７１における選択後に押下する次へボタン７２が表示されている。

【００５１】

図７（ａ）に示した画面に対して、ユーザー端末１０－１により、オプションサービス選択領域７１にてオプションサービスが選択されて次へボタン７２が押下されると、オプションサービス選択領域７１にて選択されたオプションサービスの内容がメールサーバー２０に送信される（ステップＳ９）。メールサーバー２０は、オプションサービス選択領域７１にて選択されたオプションサービスの内容を受信し（ステップＳ１０）、ユーザー管理部２１は、オプションサービス選択領域７１において、暗号化された添付ファイルのウィルスチェックを選択したか否か判定し、選択した場合に、図７（ｂ）に示すように、暗号化の解除（復号化）をしてウィルスチェックするファイルの拡張子またはアプリケーション名の種別を選択するための種別選択領域７３と、ウィルスチェックを行った添付ファイルの受け取り方法を選択するための受け取り方法選択領域７４と、種別選択領域７３及び受け取り方法選択領域７４における選択後に押下する次へボタン７５とが設けられた画面をユーザー端末１０－１に送信してもよい。ユーザー端末１０－１には受信した画面が表示される。暗号化の解除（復号化）をしてウィルスチェックするファイルの拡張子またはアプリケーション名の種別の選択方法としては、図７（ｂ）に示すように、例えば、暗号化された圧縮ファイルの場合、拡張子なら「.zip」、アプリケーション名なら「圧縮ファイルソフト」が記載され、文書作成ソフトの独自機能で暗号化されたファイルの場合、拡張子なら「.docx」、アプリケーション名なら具体的な製品名が記載され、それぞれの記載に対応して選択可能になっているチェックボックスが設けられている。ウィルスチェックを行った添付ファイルの受け取り方法としては、図７（ｂ）に示すように、例えば、ウィルスチェックを行った添付ファイルを暗号化したまま受け取る場合と、ウィルスチェックを行った添付ファイルを復号化した状態で場合と、ウィルスチェックを行った添付ファイルを所定のネットワークフォルダに保存する場合とが記載され、それぞれの記載

に対応して、選択可能となっているチェックボックスが設けられている。なお、選択内容に応じて、選択できる個数を制限しても構わない。

【００５２】

図７（ｂ）に示した画面に対して、ウィルスチェックを行った添付ファイルの受け取り方法が選択され、画面に表示された次へボタン７５がユーザー端末１０－１にて押下されると、種別選択領域７３及び受け取り方法選択領域７４にて選択されたオプションサービスの内容がメールサーバー２０に送信される。このように、選択されたオプションサービスの種類や階層に応じて、オプションサービス内容設定画面の送信（ステップＳ７）から選択内容の受信（ステップＳ１０）の処理を複数回行ってもよい。

【００５３】

図７（ａ）に示した画面に対して、暗号化された添付ファイルのウィルスチェックを選択せずに、次へボタン７２が押下された場合、または、図７（ｂ）に示した画面に対して、暗号化の解除（復号化）をしてウィルスチェックするファイルの拡張子またはアプリケーション名の種別を選択が選択され、ウィルスチェックを行った添付ファイルの受け取り方法が選択され、次へボタン７５が押下された場合、メールサーバー２０のユーザー管理部２１は、オプションサービス選択領域７１と、種別選択領域７３と、受け取り方法選択領域７４とにて、選択されたオプションサービスの内容が記載され、決定ボタンが設けられた確認画面をユーザー端末１０－１に送信する。

【００５４】

図８は、メールサーバー２０から送信されてユーザー端末１０－１～１０－ｎにて表示されるオプションサービス内容確認画面の一部を示す図である。

【００５５】

図７（ａ）に示した画面に対して、暗号化された添付ファイルのウィルスチェックを選択せずに、次へボタン７２が押下された場合、または、図７（ｂ）に示した画面に対して、暗号化の解除（復号化）をしてウィルスチェックするファイルの拡張子またはアプリケーション名の種別を選択が選択され、ウィルスチェックを行った添付ファイルの受け取り方法が選択され、次へボタン７５が押下された場合、図８に示すように、オプションサービス選択領域７１と、種別選択領域７３と、受け取り方法選択領域７４とにて、選択されたオプションサービスの内容が記載された確認画面がユーザー端末１０－１に送信され、ユーザー端末１０－１にて表示される。ユーザー端末１０－１に表示された確認画面には、図８に示すように決定ボタン７６が設けられているため、この決定ボタン７６を押下することで、図７に示した画面にて選択したオプションサービスの内容が決定される。なお、図８は、図７（ａ）に示した画面に対して、「標準的な迷惑メールチェック」と、「暗号化された添付ファイルのウィルスチェック」とが選択され、更に、図７（ｂ）に示した画面に対して、暗号化の解除（復号化）をしてウィルスチェックするファイルの拡張子またはアプリケーション名の種別を選択が選択され、ウィルスチェックを行った添付ファイルの受け取り方法として、「添付ファイルを復号化した状態で受け取る」が選択された場合の例を示している。

【００５６】

決定ボタン７６が押下されると、メールサーバー２０のユーザー管理部２１において、ステップＳ１０にて受信されたオプションサービスの内容が設定され、ユーザーデーターベース５０に登録される（ステップＳ１１）。

【００５７】

図９は、図１に示したユーザーデーターベース５０の一部を示す図である。

【００５８】

図９は、ユーザーとそのユーザーが希望したオプションサービス内容との対応関係を示している。図９に示すようにユーザーデーターベース５０には、図７（ａ）に示したオプションサービス選択領域７１にて選択されたことで、ユーザーが加入しているオプションサービスと、図７（ｂ）に示した種別選択領域７３にて選択された復号化してウィルスチェックするファイルの種別と、図７（ｂ）に示した受け取り方法選択領域７４にて選択さ

れた添付ファイルの受け取り方法とが、ユーザーのＩＤに対応づけて登録される。なお、説明のため各データを文章等で記載しているが、それぞれに対応する識別子を定めておき、識別子で管理してもよい。

【００５９】

一方、ユーザー認証を行った結果、照合できなかった場合は、契約しているユーザーではないとユーザー管理部２１において判定し、ユーザー認証ができなかった旨がメールサーバー２０から通知され（ステップＳ１２）、ＩＤとパスワードを送信したユーザー端末１０－１にて受信、表示される（ステップＳ１３）。

【００６０】

次に、図１～図５に示した危険性チェックシステムにおいて電子メールの危険性をチェックする際の処理について説明する。

【００６１】

図１０は、図１～図５に示した危険性チェックシステムにおいて電子メールの危険性をチェックする際の処理を説明するためのフローチャートである。

【００６２】

メールサーバー２０が、メール送受信部２２において、ユーザー管理部２１にて管理するメールアドレス宛ての電子メールを他のメールサーバーからインターネット６０経由で受信すると（ステップＳ２１）、まず、ユーザー管理部２１において、ユーザーデーターベース５０を検索し、受信した電子メールの宛先であるメールアドレスに対応するユーザーが、本オプションサービスに加入しているかどうかを判断する（ステップＳ２２）。図８に示したように、ユーザーデーターベース５０には、受信した電子メールについて、暗号化された添付ファイルを復号化してウィルスチェックを行う等のオプションサービスがユーザーＩＤと対応づけて設定、登録されており、ユーザーＩＤは別途、メールアドレスと対応づけて管理されているため、ユーザー管理部２１においては、受信した電子メールの宛先であるメールアドレスに対応するユーザーがどのサービスに加入しているかどうかを判断することができる。本形態の説明では、暗号化された添付ファイルを復号化してウィルスチェックを本オプションサービスとし、本オプションサービスの処理を基に説明し、その他のオプションサービスの処理の説明は省略する。なお、メールサーバー２０においては、ユーザー管理部２１にて管理するメールアドレス宛ての電子メールを受信すると、受信した電子メールに、メッセージＩＤが未付与の場合、メッセージＩＤを付与する。通常、メセージＩＤは、ユーザー端末でメールを送信する際にメールソフトで付与され、送信する際のメールソフトで未付与の場合、メールを送信する側のメールサーバーが付与され、送信側メールサーバーで未付与の場合、メールを受信した側のメールサーバーが付与する順番で、メールに付与される。

【００６３】

受信した電子メールの宛先であるメールアドレスに対応するユーザーに対応して、加入しているオプションサービスとして、暗号化された添付ファイルについてのウィルスチェックを行う本オプションサービスがユーザーデーターベース５０に登録されている場合、ファイル有無判断部２３が、メール送受信部２２にて受信した電子メールに、暗号化された添付ファイルが添付されているかどうかを判断する（ステップＳ２３）。ここで、暗号化された添付ファイルとしては、圧縮ファイル形式にし、解凍（圧縮を解除）する際に、パスワードを要求するものだけでなく、文書作成ソフトや表計算ソフト等のアプリケーションソフトが有するファイルを開く際にパスワードを要求される暗号化機能を用いたファイルも含まれる。

【００６４】

ファイル有無判断部２３において、メール送受信部２２にて受信した電子メールに暗号化された添付ファイルが添付されていると判断された場合、パスワード抽出部２４が、特定の電子メールの本文から、暗号化された添付ファイルを復号化するためのパスワードの候補として文字列を抽出する。例えば、暗号化された添付ファイルが添付された電子メールを特定の電子メールとして、この電子メールの本文から、１バイトからなる文字列を、

暗号化された添付ファイルを復号化するためのパスワードの候補として抽出する（ステップＳ２４）。そのため、抽出されるパスワードの候補は複数の場合もある。この際、メールサーバー２０の記憶部に記憶されているパスワード候補を抽出するための条件情報を用いて、パスワード候補である確率を算出し、確率が既定値より高い文字列を抽出するようにしてもよい。条件情報は、例えば、上記の１バイトからなる文字列であることの他に、近辺に「パスワード」や「ＰＷ」等のパスワードであることを示す語句があることや、十数文字以下の連続した文字列であることや、半角の日付やメールアドレス、電話番号等のパスワード候補から除外する文字列の形式等が登録されていることが考えられる。また、パスワード抽出部２４は、添付ファイルが添付された電子メールと同じ宛先の電子メールであって、添付ファイルが添付された電子メールを受信した時刻に対して、例えば３０分以内等、所定時間以内に受信した電子メールを、パスワードの候補を抽出するための特定の電子メールとしてもよい。さらには、受信した電子メールに付与されているメッセージＩＤを用いて、同一の送信者から返信や転送された電子メールや、ReferencesやIn-Reply-Toヘッダーを含む電子メール等のように、添付ファイルが添付された電子メールと返信または転送関係にある電子メールを、パスワードの候補を抽出するための特定の電子メールとしてもよい。また、パスワード抽出部２４は、添付ファイルが添付された電子メールを特定の電子メールとしてパスワードの候補を抽出する方法と、添付ファイルが添付された電子メールを受信した時刻に対して所定時間以内に受信した電子メールを特定の電子メールとしてパスワードの候補を抽出する方法と、添付ファイルが添付された電子メールと返信または転送関係にある電子メールを特定の電子メールとしてパスワードの候補を抽出する方法とのいずれかの方法でパスワードの候補を抽出してみて、パスワードの候補が抽出できなかった場合に他の方法でパスワードの候補を抽出してみてもよいし、これらの全ての方法でパスワードの候補を抽出してみてもよい。

【００６５】

パスワード抽出部２４において、パスワードの候補が抽出された場合、仮想コンピューター生成指示部２５が、テストサーバー３０に対して、テストサーバー３０上に仮想コンピューターを生成する旨を指示する（ステップＳ２５）。テストサーバー３０上に生成される仮想コンピューターは、後述するように、暗号化された添付ファイルを復号化するためのものであるため、仮想コンピューター生成指示部２５は、記憶部を参照し、テストサーバー３０への仮想コンピューターの生成指示とともに、暗号化された添付ファイルの拡張子に対応する暗号化された添付ファイルの復号化に必要なアプリケーションをテストサーバー３０に通知し、生成した仮想コンピューターへそのアプリケーションのインストールも指示する。この際、メールサーバー２０は、復号化する添付ファイルと、当該添付ファイルが添付された電子メールとを関連付けするための識別子である関連付けＩＤを生成し、仮想コンピューター生成指示とともにテストサーバー３０に通知する。なお、関連付けＩＤは、復号化する添付ファイルが添付された電子メールに付与されたメッセージＩＤを用いてもよい。

【００６６】

一方、パスワード抽出部２４において、パスワードの候補を抽出できなかった場合、メール保存部２７において、メール送受信部２２にて受信した、暗号化された添付ファイルが添付された電子メールを、宛先のメールアドレスに対応し、受信メールボックスと迷惑メールボックスとも異なる第３のメールボックスとなる安全性不明メールボックスに保存するとともに、安全性が不明な電子メールを受信した旨が記載された電子メールを宛先のメールアドレスに対応する受信メールボックスに保存する。

【００６７】

また、仮想コンピューター生成指示部２５は、ファイル有無判断部２３にて電子メールに添付されたと判断された暗号化された添付ファイルと、パスワード抽出部２４にて抽出されたパスワードの候補とをテストサーバー３０に送信する。（ステップＳ２６）。

【００６８】

一方、メール送受信部２２にて受信した電子メールの宛先であるメールアドレスに対応

するユーザーが、本オプションサービスに加入していない場合や、メール送受信部２２にて受信した電子メールに、暗号化された添付ファイルが添付されていない場合は、メール保存部２７が、メール送受信部２２にて受信した電子メールを、その宛先であるメールアドレスに対応する受信メールボックスに保存する（ステップＳ２７）。なおその際、メール送受信部２２にて受信した電子メールの宛先であるメールアドレスのユーザーが別途、受信した電子メールに対する標準的な迷惑メールチェックを行うオプションサービスに加入している場合、暗号化された添付ファイルのチェックは行わないものの、加入しているオプションサービスに応じたウィルスやフィッシング、スパムメール等のチェックをすることになる。

【００６９】

テストサーバー３０は、指示受付部３１において、仮想コンピューターの生成指示を仮想コンピューター生成指示部２５から受信すると（ステップＳ２８）、仮想コンピューター生成部３２において、仮想コンピューター生成指示部２５から通知された拡張子が付与された添付ファイルに対応するアプリケーションと、仮想コンピューター生成指示部２５から通知されたアプリケーションとがインストールされた仮想コンピューターをテストサーバー３０上に生成する（ステップＳ２９）。

【００７０】

そして、仮想コンピューター生成指示部２５から送信された添付ファイルを仮想コンピューターの添付ファイル受付部３２ａにて受け付けるとともに、仮想コンピューター生成指示部２５から送信されたパスワードの候補を仮想コンピューターのパスワード受付部３２ｂにて受け付けると（ステップＳ３０）、仮想コンピューターの復号化部３２ｃが、暗号化された添付ファイルをパスワード候補を用いて復号化する（ステップＳ３１）。例えば、暗号化された添付ファイルを実行すると、パスワード入力欄が表示出力され、復号化部３２ｃが、そのパスワード入力欄にパスワード候補を入力する。この際、暗号化された添付ファイルは、圧縮ファイル形式にし、解凍（圧縮を解除）する際に、パスワードを要求するものや、文書作成ソフトや表計算ソフト等のアプリケーションソフトが有するパスワードによる暗号化機能を用いたファイルが考えられるため、圧縮ファイルに対応する解凍ソフトや、復号化する際にファイルに対応するアプリケーションソフトが必要となるが、仮想コンピューターには、仮想コンピューター生成指示部２５から通知された拡張子が付与された添付ファイルに対応するアプリケーションがインストールされているため、復号化部３２ｃは、暗号化された添付ファイルをパスワード候補を用いて復号化することができる。なお、仮想コンピューターにインストールするアプリケーションに応じて、暗号化された添付ファイルをチェックするオプションサービスの料金を変えてもよい。

【００７１】

ここで、仮想コンピューター生成指示部２５によるテストサーバー３０に対する、仮想コンピューターを生成する旨を指示と、添付ファイル及びパスワードの候補の送信とは同時であってもよいし、仮想コンピューター生成指示部２５による仮想コンピューターを生成する旨の指示に対してテストサーバー３０が仮想コンピューターを生成した後、その旨をテストサーバー３０からメールサーバー２０に通知し、メールサーバー２０にてその通知を受信した後に添付ファイル及びパスワードの候補をテストサーバー３０に送信してもよい。

【００７２】

また、パスワード抽出部２４が、添付ファイルが添付された電子メールを特定の電子メールとしてパスワードの候補を抽出する方法と、添付ファイルが添付された電子メールを受信した時刻に対して所定時間以内に受信した電子メールを特定の電子メールとしてパスワードの候補を抽出する方法と、添付ファイルが添付された電子メールと返信または転送関係にある電子メールを特定の電子メールとしてパスワードの候補を抽出する方法とのいずれかの方法でパスワードの候補を抽出した場合であって、仮想コンピューター生成指示部２５から送信されたパスワードの候補を用いて添付ファイルを復号化できなかった場合、その旨をテストサーバー３０からメールサーバー２０に通知し、メールサーバー２０の

パスワード抽出部２４において上述した３つ方法のうち他の方法にてパスワードの候補を抽出してみてもよい。

【００７３】

圧縮ファイルの場合はファイルが解凍され、アプリケーションソフトが有するパスワードによる暗号化機能の場合はファイルが開け、仮想コンピューターが添付ファイルを復号化することができた場合、テストサーバー３０の添付ファイル送信部３３が、復号化された添付ファイルを、その添付ファイルとともにメールサーバー２０から受信した関連付けＩＤとともにウィルスチェックサーバー４０に送信する（ステップＳ３２）。なお、圧縮ファイルの場合は復号化されると、解凍したファイルが出現するが、アプリケーションソフトが有するパスワードによる暗号化機能の場合は、そのファイルを閉じるとまた暗号化されたファイルが残るため、アプリケーションソフトが有するパスワードによる暗号化機能を使用しないように、ファイルの設定をしてから復号化されたファイルを記憶する。

【００７４】

一方、仮想コンピューターの復号化部３２ｃにおいて添付ファイルを復号化できなかった場合、その旨を、その添付ファイルとともにメールサーバー２０から受信した関連付けＩＤとともにメールサーバー２０に通知する。メールサーバー２０のメール保存部２７は、受信した関連付けＩＤに対応する暗号化された添付ファイルが添付された電子メールを宛先のメールアドレスに対応する安全性不明メールボックスに保存するとともに、安全性が不明な電子メールを受信した旨が記載された電子メールを宛先のメールアドレスに対応する受信メールボックスに保存する。

【００７５】

テストサーバー３０の添付ファイル送信部３３から送信された復号化された添付ファイルをウィルスチェックサーバー４０の添付ファイル受信部４１が受信すると（ステップＳ３３）、ウィルスチェック部４２において、添付ファイル受信部４１にて受信した復号化された添付ファイルについて、ウィルスやフィッシング、スパムメールの危険性があるかどうかのチェックを行う（ステップＳ３４）。なお、関連付けＩＤに対応する暗号化された添付ファイルが添付されていた電子メールの添付ファイル以外の電子メールのヘッダーや本文についても危険性があるかどうかのチェックを行う。

【００７６】

ウィルスチェック部４２において、復号化された添付ファイルの危険性のチェックが行われると、ウィルスチェックサーバー４０の結果送信部４３が、そのチェック結果を、その復号化された添付ファイルの関連付けＩＤとともに、メールサーバー２０に送信する（ステップＳ３５）。

【００７７】

ウィルスチェックサーバー４０の結果送信部４３から送信されたチェック結果をメールサーバー２０の結果受信部２６が受信し（ステップＳ３６）、危険性がなかった場合（ステップＳ３７）、メール保存部２７は、ユーザー管理部２１を介してユーザーデーターベース５０を参照して、チェック結果とともに受信した関連付けＩＤに対応する電子メールのユーザーＩＤに対応して登録されている添付ファイルの受け取り方法を呼び出し、その受け取り方法を判定し、ユーザーデーターベース５０に登録された受け取り方法に応じて、関連付けＩＤに対応する電子メールを提供する（ステップＳ３８）。例えば、添付ファイルの受け取り方法として、添付ファイルを暗号化された状態で受け取る方法が登録されている場合、メール保存部２７は、チェック結果とともに受信した関連付けＩＤに対応する電子メールを、添付ファイルを暗号化されたままの状態で電子メールに添付しておき、その電子メールの宛先のメールボックスに保存するとともに、危険性がない電子メールを受信した旨が記載された電子メールを宛先のメールアドレスに対応する受信メールボックスに保存する。また、添付ファイルの受け取り方法として、添付ファイルを復号化した状態で受け取る方法が登録されている場合、メール保存部２７は、テストサーバー３０から復号化した添付ファイルを取得し、関連付けＩＤに対応する電子メールから暗号化された添付ファイルを削除し、復号化した添付ファイルをその電子メールに添付して、その電子

メールの宛先のメールボックスに保存するとともに、暗号化された添付ファイルを復号化したファイルに交換した旨が記載された電子メールを宛先のメールアドレスに対応する受信メールボックスに保存する。また、添付ファイルの受け取り方法として、添付ファイルを特定のフォルダに保存する方法が登録されている場合、メール保存部２７は、添付ファイルを関連付けＩＤに対応する電子メールから削除するとともに、添付ファイルを暗号化されたままのファイルあるいはテストサーバー３０から取得した復号化されたファイルの状態で所定の記憶領域となる特定のフォルダに保存し、添付ファイルが添付されていた電子メールの宛先のメールボックスに当該電子メールとを保存するとともに、危険性がない電子メールを受信した旨と、添付ファイルが保存されたフォルダへのアクセス手段となるリンクが記載された電子メールとを宛先のメールアドレスに対応する受信メールボックスに保存する。この際、ウィルスチェックサーバー４０からは、ウィルスチェックが行われた添付ファイルに付与された関連付けＩＤが通知されているため、メールサーバー２０においては、ウィルスチェックサーバー４０から受信したチェック結果が、メール送受信部２２にて受信された電子メールのうちどの電子メールに添付された添付ファイルのものであるかを判断することができる。なお、添付ファイルを復号化した状態で電子メールに添付してその電子メールの宛先のメールボックスに保存したり、添付ファイルを復号化された状態で特定のフォルダに保存したりする場合は、メールサーバー２０は、テストサーバー３０から復号化された添付ファイルを受信することになる。また、添付ファイルを復号化した状態で電子メールに添付または特定のフォルダに保存した場合、元の暗号化された添付ファイルを、所定の記憶領域となる保存用フォルダに、ユーザー端末１０から所定期間アクセス可能な状態で保存しておいてもよい。

【００７８】

一方、危険性があった場合は、メール保存部２７は、チェック結果とともに受信した関連付けＩＤに対応する、暗号化された添付ファイルが添付された電子メールを宛先のメールアドレスに対応する迷惑メールボックスに保存する（ステップＳ３９）とともに、危険性がある電子メールを受信した旨が記載された電子メールを宛先のメールアドレスに対応する受信メールボックスに保存する。

【００７９】

その後、テストサーバー３０は、メールサーバー２０の仮想コンピューター生成指示部２５による指示により、テストサーバー３０上に生成した仮想コンピューターと添付ファイルを削除する。

【００８０】

このようにして、暗号化された添付ファイルが添付された電子メールを受信した場合、その電子メールに関係する特定の電子メールから、暗号化された添付ファイルを復号化するためのパスワードの候補を抽出し、抽出されたパスワードの候補を用いて、暗号化された添付ファイルを復号化し、復号化された添付ファイルに危険性があるかどうかをチェックするため、電子メールに暗号化された添付ファイルが含まれている場合であっても、ユーザーの手を煩わすことなく、添付ファイルに危険性があるかどうかをチェックすることができる。

【００８１】

なお、本発明の危険性チェックシステムにて行われる方法は、コンピューターに実行させるためのプログラムに適用してもよい。また、そのプログラムを記憶媒体に格納することも可能であり、ネットワークを介して外部に提供することも可能である。

【符号の説明】

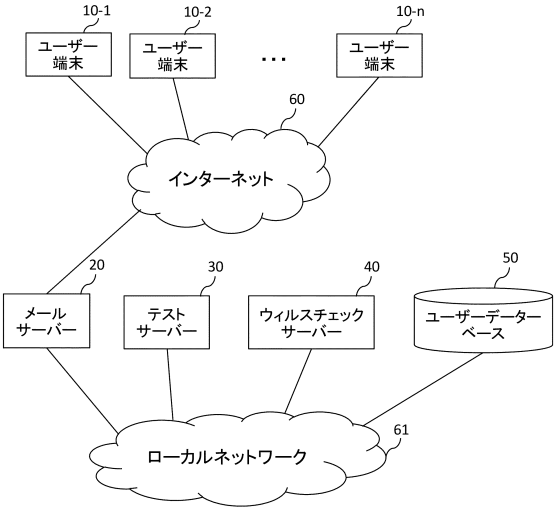
【００８２】

１０－１～１０－ｎ　ユーザー端末
２０　メールサーバー
２１　ユーザー管理部
２２　メール送受信部
２３　ファイル有無判断部

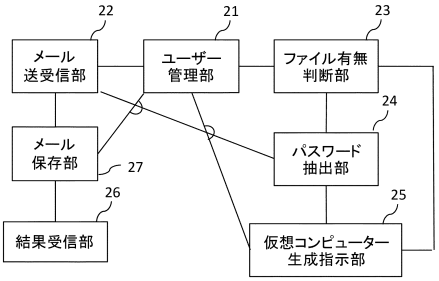
２４　パスワード抽出部
２５　仮想コンピューター生成指示部
２６　結果受信部
２７　メール保存部
３０　テストサーバー
３１　指示受付部
３２　仮想コンピューター生成部
３２ａ　添付ファイル受付部
３２ｂ　パスワード受付部
３２ｃ　復号化部
３３　添付ファイル送信部
４０　ウィルスチェックサーバー
４１　添付ファイル受信部
４２　ウィルスチェック部
４３　結果送信部
５０　ユーザーデーターベース
６０　インターネット
６１　ローカルネットワーク
７１　オプションサービス選択領域
７２，７５　次へボタン
７３　種別選択領域
７４　受け取り方法選択領域
７６　決定ボタン

【図面】

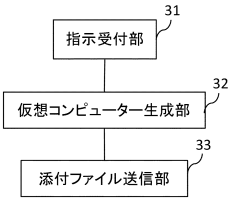
【図１】



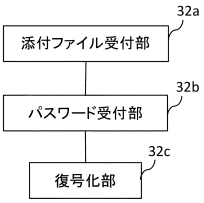
【図２】



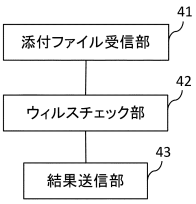
【図３】


31
指示受付部
32
仮想コンピューター生成部
33
添付ファイル送信部

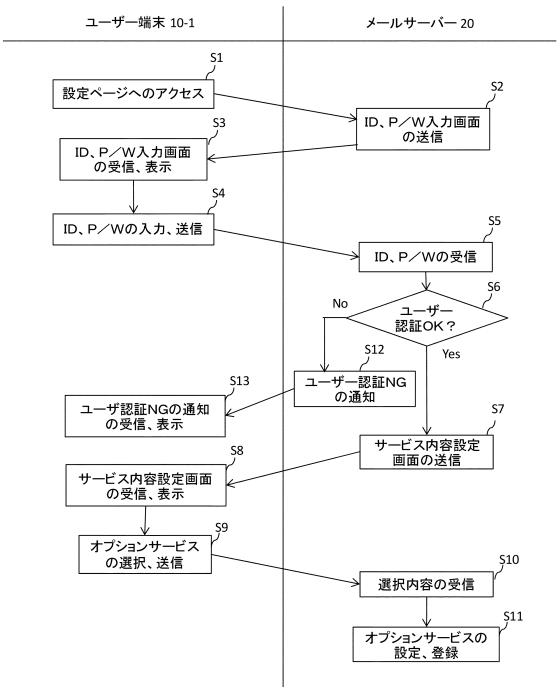
【図４】


32a
添付ファイル受付部
32b
パスワード受付部
32c
復号化部

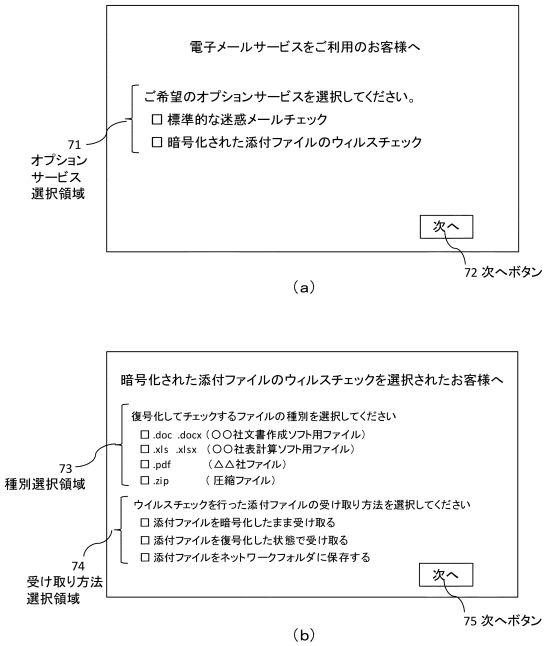
【図５】


41
添付ファイル受信部
42
ウィルスチェック部
43
結果送信部

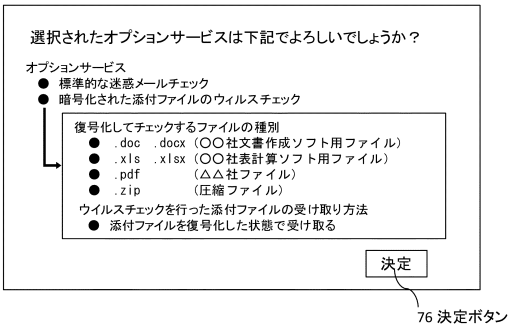
【図６】


ユーザー端末 10-1
メールサーバー 20
S1
設定ページへのアクセス
S2
ID、P／W入力画面の送信
S3
ID、P／W入力画面の受信、表示
S4
ID、P／Wの入力、送信
S5
ID、P／Wの受信
S6
ユーザー認証OK？
No
Yes
S12
ユーザー認証NGの通知
S13
ユーザ認証NGの通知の受信、表示
S7
サービス内容設定画面の送信
S8
サービス内容設定画面の受信、表示
S9
オプションサービスの選択、送信
S10
選択内容の受信
S11
オプションサービスの設定、登録

【図７】



【図８】



【図９】

ID	加入しているオプションサービス	復号化してチェックするファイルの種別	受け取り方法
111111	標準的な迷惑メールチェック 暗号化された添付ファイルのウィルスチェック	.doc .docx（〇〇社文書作成ソフト用ファイル） .xls .xlsx（〇〇社表計算ソフト用ファイル） .pdf （△△社ファイル） .zip （圧縮ファイル）	添付ファイルを復号化した状態で受け取る
222222	標準的な迷惑メールチェック 暗号化された添付ファイルのウィルスチェック	.zip （圧縮ファイル）	添付ファイルを暗号化したまま受け取る
333333	標準的な迷惑メールチェック	—	—
…	…	…	…

【図１０】