(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2023-150848
(P2023-150848A)
(43)公開日　令和5年10月16日(2023.10.16)

| (51)Int.Cl. | | F I | | テーマコード（参考） |
|---|---|---|---|---|
| G06F 21/42 | (2013.01) | G06F 21/42 | | |

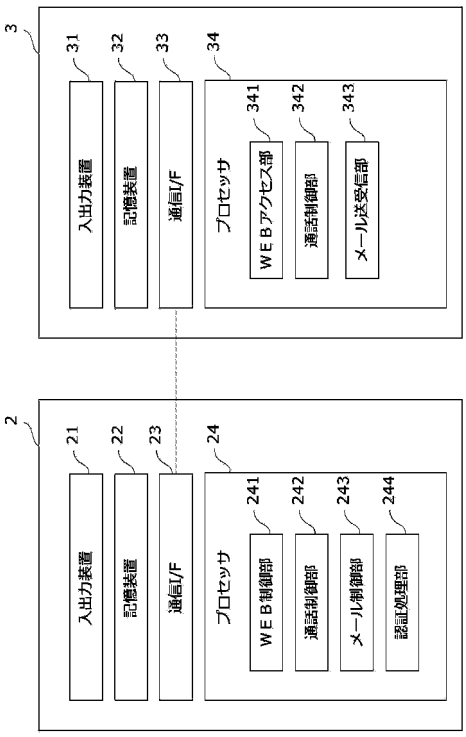
審査請求 有　請求項の数 7　ＯＬ　（全 12 頁）

(21)出願番号　特願2022-60168(P2022-60168)
(22)出願日　令和4年3月31日(2022.3.31)
(11)特許番号　特許第7081773号(P7081773)
(45)特許公報発行日　令和4年6月7日(2022.6.7)

(71)出願人　716001245
株式会社エルブズ
東京都渋谷区桜丘町２０－１１チェリーヒル２０１
(71)出願人　393012183
株式会社ＮＴＴデータ・アイ
東京都新宿区揚場町１番１８号
(74)代理人　110002860
弁理士法人秀和特許事務所
(72)発明者　田中　秀樹
東京都渋谷区桜丘町２０－１１　チェリーヒル２０１　株式会社エルブズ内
(72)発明者　山田　隆司
東京都新宿区揚場町１番１８号　株式会社ＮＴＴデータ・アイ内

(54)【発明の名称】認証方法、認証プログラム及び認証システム

(57)【要約】
【課題】認証処理に固有の情報をユーザが記憶しておく必要なくユーザ認証を行うための技術を提供する。
【解決手段】認証方法は、ユーザ装置から、ユーザへのメッセージの送信先情報の入力を受け付け、送信先情報と電話番号との組み合わせを予め記憶する記憶装置から、入力を受け付けた送信先情報に対応付けられている電話番号を読み出し、読み出された電話番号に対し発呼して通話を確立させると共に、一時的に使用する認証用のコードの入力を促す音声を出力し、確立された通話において、認証用のコードがトーン信号により入力された場合、入力を受け付けた送信先情報を宛先として、一時的に使用する認証用のＵＲＬを含むメッセージを送信し、一時的に使用する認証用のＵＲＬへのアクセスを受けた場合、ユーザを認証成功とする処理を１以上のコンピュータが実行する。
【選択図】図２



【特許請求の範囲】
【請求項１】
ユーザ装置から、ユーザへのメッセージの送信先情報の入力を受け付け、
送信先情報と電話番号との組み合わせを予め記憶する記憶装置から、入力を受け付けた前記送信先情報に対応付けられている電話番号を読み出し、
読み出された前記電話番号に対し発呼して通話を確立させると共に、一時的に使用する認証用のコードの入力を促す音声を出力し、
確立された前記通話において、前記認証用のコードがトーン信号により入力された場合、入力を受け付けた前記送信先情報を宛先として、一時的に使用する認証用のＵＲＬ（Uniform Resource Locator）を含むメッセージを送信し、
前記一時的に使用する認証用のＵＲＬへのアクセスを受けた場合、前記ユーザを認証成功とする
処理を１以上のコンピュータが実行する認証方法。
【請求項２】
一時的に使用する前記認証用のコードは、ランダムに生成される１以上の数字を含む
請求項１に記載の認証方法。
【請求項３】
一時的に使用する前記認証用のＵＲＬは、有効期限が設定され、他のユーザのための有効な認証用のＵＲＬと重複しないように生成される
請求項１又は２に記載の認証方法。
【請求項４】
前記ユーザを認証成功とする場合、前記一時的に使用する認証用のＵＲＬへのアクセスによって開始された通信のセッションを識別するための識別情報を記憶させ、当該セッションにおいて所定の情報へのアクセスを許可する
請求項１から３の何れか一項に記載の認証方法。
【請求項５】
前記送信先情報は、電子メールアドレスである
請求項１から４の何れか一項に記載の認証方法。
【請求項６】
請求項１から５の何れか一項に記載の認証方法を、１以上のコンピュータに実行させるための認証プログラム。
【請求項７】
１以上のコンピュータを備え、
請求項１から５の何れか一項に記載の認証方法を、前記１以上のコンピュータが実行するように構成された認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証方法、認証プログラム及び認証システムに関する。
【背景技術】
【０００２】
従来、ユーザにコード（ユーザＩＤやパスワード、パスコード）を一切入力させることなく、２段階のユーザ認証を実行することができる認証サーバ等が提案されている（例えば、特許文献１）。端末を操作するユーザを認証する認証サーバは、ユーザＩＤ毎に、アドレスと、当該ユーザを識別可能な第１のＵＲＬとを記憶する登録テーブルと、第１のＵＲＬに向けた第１のページ要求を受信した際に、ユーザＩＤを識別すると共に、当該ユーザＩＤを識別可能な第２のＵＲＬを生成する第２のＵＲＬ生成手段と、第２のＵＲＬが記述された第２のメッセージを、当該ユーザＩＤのアドレスを宛先として送信する第２のメッセージ送信手段と、端末から第２のＵＲＬに向けた第２のページ要求を受信した際に、端末に対して当該ユーザＩＤの認証成功とする認証手段とを有する。

【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１９－１８５１４６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上記の技術によれば、ユーザＩＤやパスワード、パスコードを入力することなく２段階認証を行うことができる。しかしながら、ユーザを識別可能な第１のＵＲＬを記憶し、又は記憶させておき、第１のＵＲＬに向けた第１のページ要求を行う必要があった。本発明は、ユーザＩＤやパスワードのほか、ユーザを識別可能なＵＲＬのような、認証処理に固有の情報をユーザが記憶しておく必要なくユーザ認証を行うための技術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】
【０００５】
認証方法は、ユーザ装置から、ユーザへのメッセージの送信先情報の入力を受け付け、送信先情報と電話番号との組み合わせを予め記憶する記憶装置から、入力を受け付けた送信先情報に対応付けられている電話番号を読み出し、読み出された電話番号に対し発呼して通話を確立させると共に、一時的に使用する認証用のコードの入力を促す音声を出力し、確立された通話において、認証用のコードがトーン信号により入力された場合、入力を受け付けた送信先情報を宛先として、一時的に使用する認証用のＵＲＬ（Uniform Resource Locator）を含むメッセージを送信し、一時的に使用する認証用のＵＲＬへのアクセスを受けた場合、ユーザを認証成功とする処理を１以上のコンピュータが実行する。
【０００６】
また、一時的に使用する認証用のコードは、ランダムに生成される１以上の数字を含むものであってもよい。
【０００７】
また、一時的に使用する認証用のＵＲＬは、有効期限が設定され、他のユーザのための有効な認証用のＵＲＬと重複しないように生成されるようにしてもよい。
【０００８】
また、ユーザを認証成功とする場合、一時的に使用する認証用のＵＲＬへのアクセスによって開始された通信のセッションを識別するための識別情報を記憶させ、当該セッションにおいて所定の情報へのアクセスを許可するようにしてもよい。
【０００９】
また、送信先情報は、電子メールアドレスであってもよい。
【００１０】
なお、課題を解決するための手段に記載の内容は、本発明の課題や技術的思想を逸脱しない範囲で可能な限り組み合わせることができる。また、課題を解決するための手段の内容は、認証方法を実行するように構成されたコンピュータ等の装置若しくは１以上の装置を含むシステム、１以上のコンピュータが実行する方法、又は１以上のコンピュータに実行させるためのプログラムとして提供することができる。なお、プログラムを保持する記録媒体を提供するようにしてもよい。
【発明の効果】
【００１１】
認証処理に固有の情報をユーザが記憶しておく必要なくユーザ認証を行うための技術を提供することができる。
【図面の簡単な説明】
【００１２】
【図１】図１は、システム全体の一例を示す図である。
【図２】図２は、認証装置及びユーザ端末の構成の一例を示すブロック図である。

【図３】図３は、認証処理の一例を示す処理フロー図である。
【図４】図４は、オンラインサービスへログインするためのページの一例を示す図である。
【図５】図５は、認証装置２に登録された会員情報の一例を示す図である。
【図６】図６は、認証処理の一例を示す処理フロー図である。
【図７】図７は、認証処理の一例を示す処理フロー図である。
【発明を実施するための形態】
【００１３】
以下、図面を参照して本発明を実施するための形態について説明する。
【００１４】
＜システム構成＞
図１は、実施形態に係るシステム全体の一例を示す図である。システム１は、ユーザ端末３（３Ａ、３Ｂ）と、認証装置２とを含み、これらがネットワーク４を解して接続されている。ネットワーク４は、インターネット等の通信網であり、ネットワーク４に接続されたコンピュータは所定のプロトコルに基づいて相互に通信できるものとする。
【００１５】
認証装置２は、本実施形態に係る認証処理を行うシステムを構成するコンピュータである。ユーザ端末３からのアクセスに対し、認証装置２は認証処理を行う。また、認証装置２は、認証成功と判断した場合に、例えば、所定のオンラインサービスへのアクセス（ログイン）を許可してもよい。なお、認証装置２は、複数の装置により機能を分担して実現する認証システムであってもよいし、同一の処理を並列に実行するものであってもよい。
【００１６】
ユーザ端末３は、例えばユーザが所持するスマートフォンや携帯電話機であり、通話（電話）とデータ通信とを行うことができる。なお、本実施形態に係る認証処理は、複数のユーザ端末３を用いて行われるようにしてもよい。例えば、認証処理の一部を実行するユーザ端末３は、ユーザが所持するタブレットや、ＰＣ（Personal Computer）等のような通話機能を有しない装置であってもよい。また、認証処理の一部を実行するユーザ端末３は、固定電話機であってもよい。
【００１７】
ネットワーク４は、ＩＰ（Internet Protocol）ネットワークと、電話網（固定電話網又は移動体通信網）とを含む。また、ネットワーク４の一部は、アドホック・ネットワーク（ad hoc network）、イントラネット、ＶＰＮ（Virtual Private Network）、ＬＡＮ（Local Area Network）、無線ＬＡＮ（Wireless LAN）、ＷＡＮ（Wide Area Network）、インターネットであってもよい。
【００１８】
＜装置構成＞
図２は、認証装置２及びユーザ端末３の構成の一例を示すブロック図である。
【００１９】
認証装置２は、入出力装置２１と、記憶装置２２と、通信インターフェース（Ｉ／Ｆ）２３と、プロセッサ２４とを備えており、これらの構成要素は例えばバスを介して接続されている。入出力装置２１は、タッチパネル、液晶ディスプレイ、キーボード、ポインティングデバイス等である。記憶装置２２は、ＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）等の主記憶装置及びＨＤＤ（Hard-disk Drive）やＳＳＤ（Solid State Drive）、フラッシュメモリ等の補助記憶装置（二次記憶装置）である。主記憶装置は、プロセッサが読み出したプログラムを一時的に記憶したり、プロセッサの作業領域を確保したりする。補助記憶装置は、プロセッサが実行するプログラムや、ユーザ端末３と送受信するデータを記憶したりする。本実施形態においては、予めユーザ登録されたユーザの電話番号と電子メールアドレスとが対応付けられて記憶装置２２に格納されているものとする。通信Ｉ／Ｆ２３は、例えば有線又は無線で通信を行うネットワークアダプタや、音声通話において音声ガイダンスを送出するためのインターフェース装置であり、所定の

プロトコルに基づいたデータ通信や音声通話を実現させる。プロセッサ２４は、ＣＰＵ（Central Processing Unit）等の演算処理装置であり、プログラムを実行することにより本実施の形態に係る各処理を行う。

【００２０】

図２の例では、プロセッサ２４内に機能ブロックを示している。具体的には、プロセッサ２４は、ＷＥＢ制御部２４１、通話制御部２４２、メール制御部２４３、及び認証処理部２４４として機能する。ＷＥＢ制御部２４１は、認証装置２をＷＥＢサーバとして機能させる。すなわち、ＷＥＢ制御部２４１は、通信Ｉ／Ｆ２３を介してＨＴＴＰ（HyperText Transfer Protocol）に即した通信を行い、ユーザ端末３からのアクセスに応じて、Ｗｅｂページを構成する、ＨＴＭＬ（Hypertext Markup Language）で記述されたファイルや画像ファイル等を記憶装置２２から読み出し、送信する。なお、ＷＥＢ制御部２４１は、ＳＳＬ（Secure Socket Layer）／ＴＬＳ（Transport Layer Security）等で通信を暗号化したり、例えばＣｏｏｋｉｅを用いてセッションを管理してもよい。本実施形態では、ＷＥＢ制御部２４１は、例えばユーザがログインするためのページを含む、会員向けのオンラインサービスを提供するものとする。

【００２１】

通話制御部２４２は、ネットワーク４の一部である電話網を介して携帯電話機やスマートフォンとの音声通話を行う。例えば、通話制御部２４２は、ユーザ端末３に対し所定の音声ガイダンスを出力すると共に、ユーザ端末３からトーン信号（ＤＴＭＦ： Dual-Tone Multi-Frequency）による入力を受け付ける。

【００２２】

メール制御部２４３は、ネットワーク４を介して電子メールの送信を行う。例えば、記憶装置２２に格納されたユーザのメールアドレスを宛先として所定の電子メールを作成し、ＳＭＴＰ（Simple Mail Transfer Protocol）サーバ等の予め定められた送信サーバを利用して、ＩＭＡＰ４（Internet Mail Access Protocol versison 4）サーバやＰＯＰ３（Post Office Protocol versison 3）サーバ等のユーザが利用する受信サーバへ送信する。なお、メール制御部２４３は、認証装置２を送信サーバとして機能させるようにしてもよい。

【００２３】

認証処理部２４４は、ユーザの電話番号に対する通話と、ユーザのメールアドレスに対するメッセージの送信とを利用して、認証装置２へアクセスしたユーザの認証処理を行う。具体的には、電話と電子メールとを用いた二段階認証を行う。例えば、認証処理部２４４は、ユーザ端末３からメールアドレスの入力を受けると、入力されたメールアドレスに対応付けられた電話番号を記憶装置２２から読み出す。また、認証処理部２４４は、通話制御部２４２を介して、読み出された電話番号に発呼し、一時的に使用する認証用のコードの入力を促す音声をユーザ端末３に出力させる。また、認証処理部２４４は、同一の通話において、ユーザ端末３から認証用のコードが入力された場合に、メール制御部２４３を介して上記のメールアドレスに対し、ログイン用のリンクを含む電子メールを送信する。また、認証処理部２４４は、ＷＥＢ制御部２４１がログイン用のリンクへのアクセスを受けた場合に、上記ユーザの認証を成功とする。

【００２４】

ユーザ端末３は、入出力装置３１と、記憶装置３２と、通信Ｉ／Ｆ３３と、プロセッサ３４とを備えており、これらの構成要素は例えば信号線を介して接続されている。入出力装置３１は、入力装置と出力装置とを含み、例えば、タッチパネル、液晶ディスプレイ、物理ボタン、スピーカー、イヤホンジャック、マイクロフォン等の少なくとも一部を含む。記憶装置３２は、ＲＡＭやＲＯＭ等の主記憶装置及びＨＤＤやＳＳＤ、フラッシュメモリ等の補助記憶装置である。主記憶装置は、プロセッサが読み出したプログラムを一時的に記憶したり、プロセッサの作業領域を確保したりする。補助記憶装置は、プロセッサが実行するプログラムやユーザの操作に関する情報等を記憶する。通信Ｉ／Ｆ３３は、例えば有線又は無線で通信を行うネットワークアダプタや、アナログ音声インターフェースを

搭載した音声通話モジュールであり、所定のプロトコルに基づいたデータ通信や音声通話を実現させる。プロセッサ３４は、ＣＰＵ等の演算処理装置であり、プログラムを実行することにより本実施の形態に係る各処理を行う。

【００２５】

ユーザ端末３についても、プロセッサ３４内に機能ブロックを示している。具体的には、プロセッサ３４は、ＷＥＢアクセス部３４１、通話制御部３４２及びメール送受信部３４３として機能する。ＷＥＢアクセス部３４１は、通信Ｉ／Ｆ３３を介してＷｅｂサーバからＷｅｂページを構成するデータを取得し、入出力装置３１に表示されるＷｅｂブラウザ上に表示させる。通話制御部３４２は、電話網を介したユーザ端末３への発呼に基づきユーザの呼び出しを行うと共に、入出力装置２１を介して受け付けるユーザの操作に応じて音声通話を確立させる。また,通話制御部３４２は、入出力装置２１を介して受け付けるユーザの操作に応じて、通話対象の装置に対してトーン信号を送信する。メール送受信部３４３は、ネットワーク４に接続されたメールサーバを介して電子メールを受信し、入出力装置３１に表示させる。

【００２６】

＜認証処理＞

図３は、認証処理の一例を示す処理フロー図である。ユーザ端末３のＷＥＢアクセス部３４１は、認証画面においてユーザからメールアドレスの入力を受け付け、認証装置２へ送信する（図３：Ｓ１）。本ステップにおいては、ユーザ端末３から認証装置２が提供するオンラインサービスへアクセスされ、会員がログインするためのページ（認証画面）が表示されているものとする。図４は、オンラインサービスへログインするためのページの一例を示す図である。図４の例では、ユーザ端末３の入出力装置３１に、メールアドレスを入力するためのテキストボックス３１１と、テキストボックス３１１に入力された情報を送信するための「送信」ボタン３１２とを含むＷｅｂページが表示されている。なお、オンラインサービスへアクセスするためのＵＲＬは、例えば一般的な検索エンジンでサービスの名称を検索することによりユーザは容易に知ることができる。また、本実施形態に係る処理を実行するためのアプリケーションを起動させると自動的にログインするためのページへアクセスするようにしてもよい。

【００２７】

また、本実施形態では、認証装置２の記憶装置２２に、会員登録されたユーザの電話番号とメールアドレスとが対応付けられて格納されているものとする。図５は、認証装置２に登録された会員情報の一例を示す図である。図５のテーブルは、「ＩＤ」、「電話番号」、「メールアドレス」の各属性を含む。「ＩＤ」のフィールドには、ユーザを一意に特定するための識別情報が登録されている。「電話番号」のフィールドには、ユーザが所持する電話機の電話番号が登録されている。「メールアドレス」のフィールドには、ユーザが使用する電子メールのアドレスが登録されている。

【００２８】

認証装置２の認証処理部２４４は、通信Ｉ／Ｆ２３を介してユーザ端末３からメールアドレスを受信すると（図３：Ｓ２）、記憶装置２２からメールアドレスに対応付けられた電話番号を抽出する（図３：Ｓ３）。本ステップでは、図５に示したテーブルからメールアドレスを検索し、抽出されたレコードの「メールアドレス」のフィールドに登録された情報を読み出す。

【００２９】

また、認証処理部２４４は、記憶装置２２からレコードを抽出できたか判断する（図３：Ｓ４）。記憶装置２２から認証処理部２４４がレコードを抽出できなかった場合（Ｓ４：ＮＯ）、認証装置２のＷＥＢ制御部２４１は、通信Ｉ／Ｆ２３を介してユーザ端末３へ所定のエラー画面を送信する（図３：Ｓ５）。本ステップでは、例えばユーザ登録が見つからない旨のメッセージを含むＷｅｂページが送信される。一方、ユーザ端末３のＷＥＢアクセス部３４１は、受信したエラー画面を入出力装置３１へ表示させる（図３：Ｓ６）。

【００３０】
Ｓ３において記憶装置２２から認証処理部２４４がレコードを抽出できた場合（図３：Ｓ４：ＹＥＳ）、認証装置２のＷＥＢ制御部２４１は、通信Ｉ／Ｆ２３を介してユーザ端末３へ所定の案内画面を送信する（図３：Ｓ７）。本ステップでは、例えばユーザ認証のために架電される旨のメッセージ含むＷｅｂページが送信される。一方、ユーザ端末３のＷＥＢアクセス部３４１は、受信した案内画面を入出力装置３１へ表示させる（図３：Ｓ８）。
【００３１】
また、認証処理部２４４は、認証処理に用いるコードを生成する（図３：Ｓ９）。認証処理に用いるコードは、一時的に使用する認証用のコードであり、例えば１桁以上の乱数であってもよい。また、認証用のコードは、数字に限定されず、「＃」や「＊」のように押しボタンダイヤル信号の規格に含まれる符号を含む１以上のランダムな文字列によって構成されるコードであってもよい。また、認証処理に用いるコードは、例えば所定の有効期限が設定され、一時的に記憶装置２２に記憶される。
【００３２】
その後、認証処理は端子「Ａ」を介して図６へ遷移する。図６は、認証処理の一例を示す処理フロー図（２）である。認証装置２の通話制御部２４２は、Ｓ３において抽出された電話番号へ電話網を介して架電する（図６：Ｓ１０）。一方、ユーザ端末３の通話制御部３４２は、通信Ｉ／Ｆ２３を介して自装置への発呼を示す情報を受信すると、入出力装置２１を介してユーザを呼び出す（図６：Ｓ１１）。本ステップでは、ユーザの操作に応じて認証装置２との音声通話が確立される。
【００３３】
また、認証装置２の通話制御部２４２は、Ｓ１１で確立した通話において、生成したコードを音声により送信する（図６：Ｓ１２）。一方、ユーザ端末３の通話制御部３４２は、通信Ｉ／Ｆ２３を介して音声を受信し、スピーカー等を介して出力する（図６：Ｓ１３）。また、通話制御部３４２は、同一の通話において、ユーザの操作に基づいてトーン信号を送信する（図６：Ｓ１３）。本ステップでは、ユーザが押下したプッシュボタンに応じてＤＴＭＦに即した信号が送信される。
【００３４】
認証装置２の通話制御部２４２がトーン信号を受信すると（図６：Ｓ１５）、認証処理部２４４は、ユーザ端末３へユーザが入力した内容とＳ９において生成されたコードとが一致するか判断する（図６：Ｓ１６）。ユーザ端末３へユーザが入力した内容とＳ９において生成されたコードとが一致しないと判断された場合（Ｓ１６：ＮＯ）、認証処理部２４４は所定のエラー処理を実行する（図６：Ｓ１７）。本ステップでは、認証処理部２４４は、通話制御部２４２にエラーである旨の音声ガイダンスを送信させてもよい。また、認証処理部２４４は、特別な処理を行わないようにしてもよいし、メール制御部２４３にエラーである旨のメッセージを含む電子メールを送信させてもよい。
【００３５】
一方、ユーザ端末３へユーザが入力した内容とＳ９において生成されたコードとが一致すると判断された場合（Ｓ１６：ＹＥＳ）、処理は端子「Ｂ」を介して図７へ遷移する。図７は、認証処理の一例を示す処理フロー図（３）である。そして、認証装置２の認証処理部２４４は、一時的に使用する認証用のＵＲＬ（Uniform Resource Locator）を生成する（図７：Ｓ１８）。本ステップでは、第三者が推測できない程度に十分な長さを有するランダムな文字列を含むＵＲＬを生成する。認証処理に用いるＵＲＬも、例えば所定の有効期限が設定され、一時的に記憶装置２２に記憶される。また、生成されたＵＲＬは、他のユーザのための有効な（すなわち、有効期限を超過していない）認証用のＵＲＬと重複していないか判断され、仮に重複していた場合には再度生成されるようにしてもよい。
【００３６】
そして、認証装置２のメール制御部２４３は、Ｓ１８において生成されたメールを含む電子メールを作成し、Ｓ２において受信したユーザのメールアドレスを宛先として送信す

る（図７：Ｓ１９）。一方、ユーザ端末３のメール送受信部３４３は、ネットワーク４に接続された受信サーバを介して電子メールを受信する（図７：Ｓ２０）。また、メール送受信部３４３は、ユーザ端末３の記憶装置３２に記憶されているメーラーをユーザの操作に基づいて起動し、電子メールを表示させる。

【００３７】

ユーザ端末３のＷＥＢアクセス部３４１は、ユーザの操作に基づいて、電子メールの本文に含まれるＵＲＬへアクセスする（図７：Ｓ２１）。例えば、メーラーは、電子メールの本文に含まれるＵＲＬをユーザがポインティングデバイスを介して指定する操作（例えばクリック又はタップ）を行った場合、ユーザ端末３の記憶装置３２に記憶されているインターネットブラウザを起動し、指定されたＵＲＬへ接続させる。

【００３８】

一方、認証装置２の認証処理部２４４は、ネットワーク４を介してＵＲＬへの接続要求を受信すると（図７：Ｓ２２）、受信したＵＲＬが有効であるか判断する（図７：Ｓ２３）。本ステップでは、ユーザ端末３からアクセスが要求されたＵＲＬが記憶装置２２に記憶され、且つ設定された有効期限を超過していないか判断する。有効でないと判断された場合（Ｓ２３：ＮＯ）、認証処理部２４４は、所定のエラー処理を行う（図７：Ｓ２４）。例えば、認証処理部２４４は、例えばアクセス先のＵＲＬが無効である旨の表示を含むＷｅｂページをＷＥＢ制御部２４１に送信させる。

【００３９】

Ｓ２３において、ＵＲＬが有効であると判断された場合（Ｓ２３：ＹＥＳ）、認証処理部２４４は、認証成功として所定の処理を行う（図７：Ｓ２５）。本ステップでは、ユーザ端末３のインターネットブラウザのＣｏｏｋｉｅにセッションを管理するための情報を記憶させ、ＷＥＢ制御部２４１は、セッションを識別するための識別情報として当該Ｃｏｏｋｉｅを記憶装置２２に記憶させると共に、その後に受信する当該Ｃｏｏｋｉｅを含む要求に対し、所定の情報へのアクセスを許可するようにしてもよい。例えば、会員向けのページへリダイレクトさせ、所定のオンラインサービスにログインさせるようにしてもよい。

【００４０】

＜効果＞

以上のような認証処理によれば、ユーザは電子メールアドレスの入力、電話による音声ガイダンスに従った操作、及び電子メールに記載された接続先へのアクセスにより認証を受けることができる。すなわち、ユーザは、ユーザＩＤやパスワードのほか、ユーザを識別可能なＵＲＬのような、認証処理に固有の情報を記憶しておくことを必要とせずに、電話及び電子メールを用いた二段階認証を受けることができる。なお、電話により通知すると共に入力させるコードをワンタイムパスワードと捉えれば、認証処理は、いわゆる二要素認証であるといえる。また、電話により通知すると共に入力させるコードは、ＣＡＰＴＨＡのようにボットによるアクセスを排除する効果を奏する。なお、図６のＳ１２及びＳ１３においては、生成されたコードそのものを音声で通知するのではなく、コードの入力を促す様々な音声ガイダンスを出力するようにしてもよい。例えば、複数の数字のうち最大のものを入力させたり、複数の数字の合計を入力させるための音声ガイダンスを出力するようにしてもよい。すなわち、電話機のボタン操作によって、ユーザーに、選択式（択一式）問題の回答を入力させたり、計算問題の回答を入力させることで、ボットによるアクセスを排除する効果を高めることができる。

【００４１】

＜その他＞

上述した実施形態の構成は例示であり、本発明の課題や技術的思想を逸脱しない範囲で可能な限り組み合わせたり、変更したりすることができる。

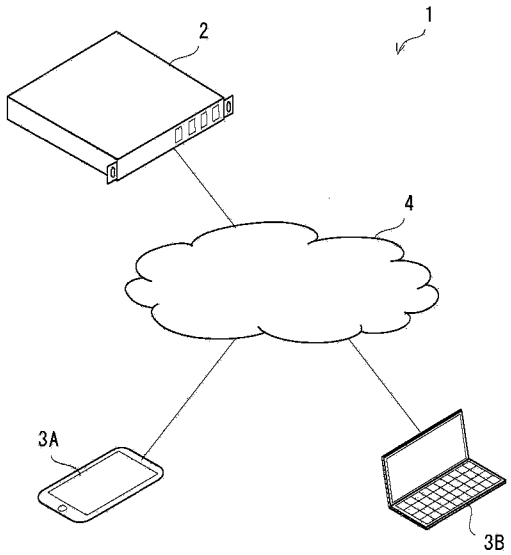
【００４２】

例えば、電子メールに代えて所定のＳＮＳ（Social networking service）が備えるメッセージ送信機能を利用し、ユーザへのメッセージの送信先情報を宛先として認証用のＵ

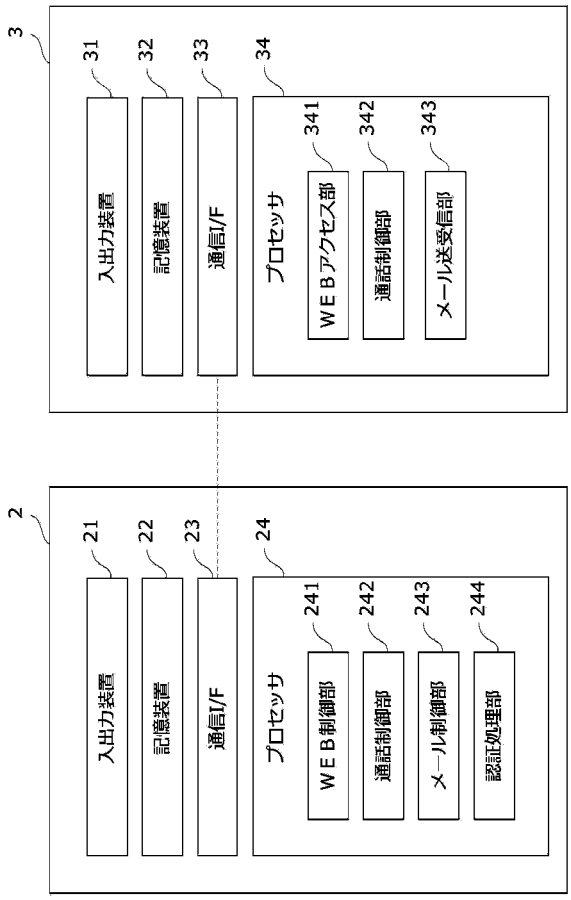
ＲＬを送信するようにしてもよい。
【００４３】
　また、上述した実施形態では、認証処理を会員向けのオンラインサービスへのアクセスを制御するために利用するものとして説明したが、このような例には限定されない。上述した認証処理は、認証が成功した場合に、例えば決済処理を実行したり、その他の処理を実行するために用いることもできる。
【００４４】
　また、認証装置２の認証処理部２４４は、図７のＳ１８で生成される認証用のＵＲＬを、いわゆる短縮ＵＲＬへさらに変換し、メール制御部２４３がＳ１９でメール送信するようにしてもよい。短縮ＵＲＬは、例えば、所望のＵＲＬと文字数の短いＵＲＬ（短縮ＵＲＬ）とを対応付け、短縮ＵＲＬへのアクセスを所望のＵＲＬへリダイレクトすることにより接続可能にするものである。短縮ＵＲＬも、所定のドメイン名に例えばランダムな文字列を結合することにより生成される。このようにすれば、Ｓ１９において送信されるメールを短くすることができ、また、メール本文のレイアウトが崩れることを抑制できる。なお、短縮ＵＲＬは、認証装置２が生成するようにしてもよいし、既存のＵＲＬ短縮サービスを利用してもよい。既存のＵＲＬ短縮サービスには、短縮ＵＲＬの有効期限を設定できるものもある。Ｓ１８において生成された認証用のＵＲＬに対して設定される有効期限に代えて、又はこれに加えて、短縮ＵＲＬの有効期限を設定してもよい。両者に有効期限を設定することで、所定期間が経過した一時的なＵＲＬをより確実に無効化することができる。
【００４５】
　また、本発明は上述の処理を実行するコンピュータプログラムを含む。また、当該プログラムを記録した、コンピュータ読み取り可能な記録媒体として提供するようにしてもよい。当該プログラムが記録された記録媒体については、コンピュータが読み出して実行することにより、上述の処理が可能となる。
【００４６】
　ここで、コンピュータ読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータから読み取ることができる記録媒体をいう。このような記録媒体のうちコンピュータから取り外し可能なものとしては、フレキシブルディスク、光磁気ディスク、光ディスク、磁気テープ、メモリカード等がある。また、コンピュータに固定された記録媒体としては、ハードディスクドライブやＲＯＭ等がある。
【符号の説明】
【００４７】
１：システム
２：認証装置
２１：入出力装置
２２：記憶装置
２３：入出力Ｉ／Ｆ
２４：プロセッサ
２４１：ＷＥＢ制御部
２４２：通話制御部
２４３：メール制御部
２４４：認証処理部
３：ユーザ端末
３：認証サーバ
３１：入出力装置
３２：記憶装置
３３：通信Ｉ／Ｆ
３４：プロセッサ

３４１：ＷＥＢアクセス部
３４２：通話制御部
３４３：メール送受信部
４：ネットワーク

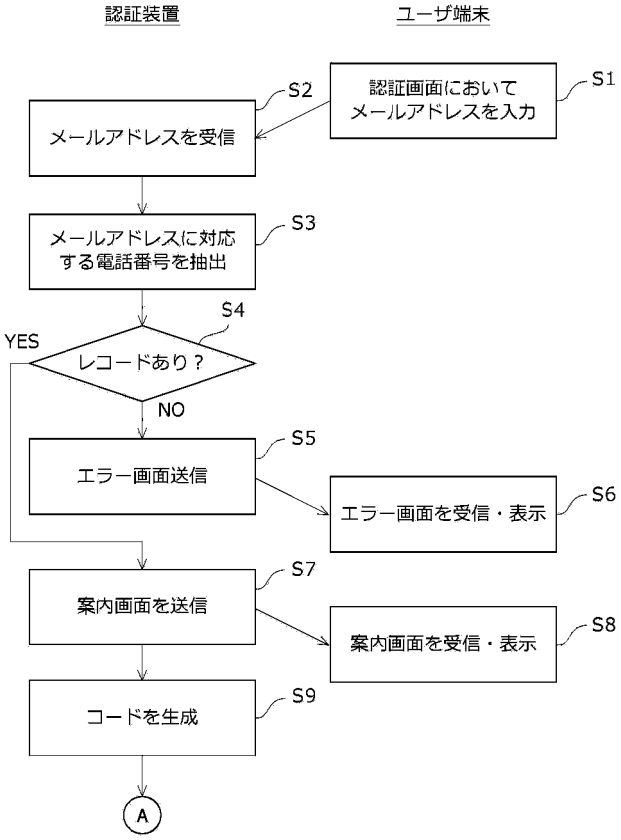
【図１】



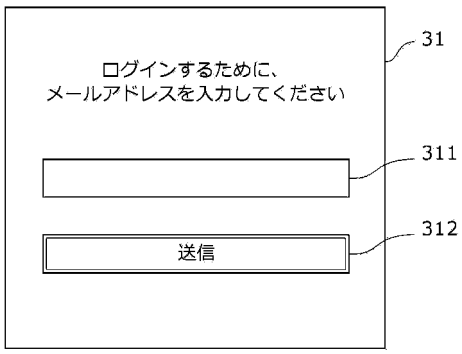

【図２】



【図３】



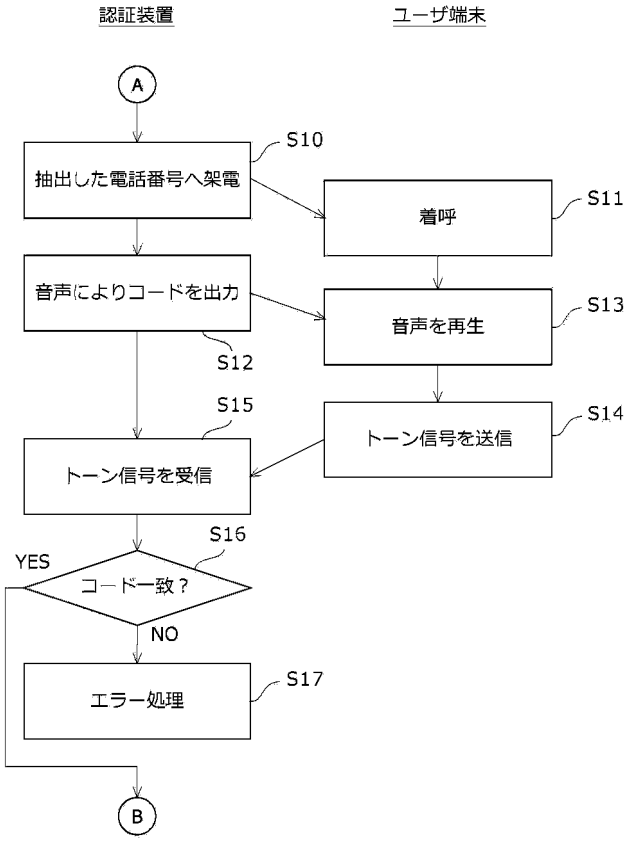

【図４】



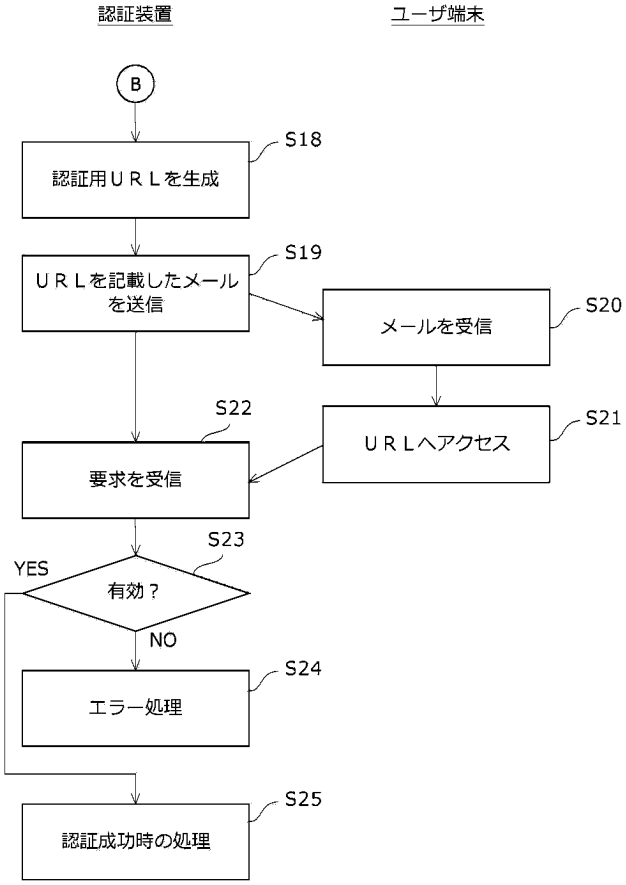

【図５】

| ID | メールアドレス | 電話番号 |
|---|---|---|
| 1 | a@a.a | 111-1111-1111 |
| 2 | b@b.b | 222-2222-2222 |
| 3 | c@c.c | 333-3333-3333 |
| ... | ... | ... |

【図６】



【図７】


認証装置
ユーザ端末
B
S18
認証用ＵＲＬを生成
S19
ＵＲＬを記載したメールを送信
メールを受信
S20
S22
S21
ＵＲＬへアクセス
要求を受信
S23
YES
有効？
NO
S24
エラー処理
S25
認証成功時の処理