(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-505021
(P2006-505021A)
(43)公表日　平成18年2月9日(2006.2.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B085
H04L 9/32	(2006.01)	G06F	15/00	330F	5J104
		H04L	9/00	673A	
		H04L	9/00	673D	

審査請求 未請求　予備審査請求 有　（全 29 頁）

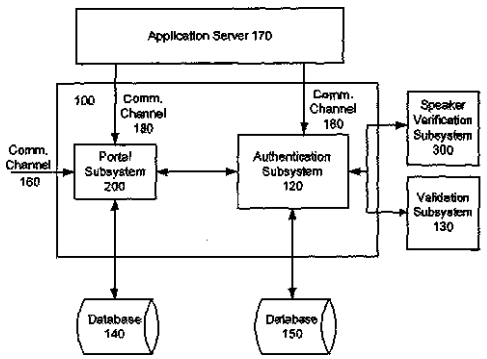
(21)出願番号　特願2003-573852 (P2003-573852)
(86)(22)出願日　平成15年2月26日 (2003.2.26)
(85)翻訳文提出日　平成16年9月30日 (2004.9.30)
(86)国際出願番号　PCT/US2003/005880
(87)国際公開番号　WO2003/075540
(87)国際公開日　平成15年9月12日 (2003.9.12)
(31)優先権主張番号　10/086,123
(32)優先日　平成14年2月28日 (2002.2.28)
(33)優先権主張国　米国 (US)

(71)出願人　503003854
ヒューレット－パッカード　デベロップメント　カンパニー　エル．ピー．
アメリカ合衆国　テキサス州　７７０７０　ヒューストン　２０５５５　ステイト　ハイウェイ　２４９
(74)代理人　110000039
特許業務法人アイ・ピー・エス
(72)発明者　ジョン・ピー・アーミントン
アメリカ合衆国ジョージア州マリエッタ　カールスゲイトドライブ４３５０
(72)発明者　パーディー・ピー・ホー
アメリカ合衆国マサチューセッツ州ボストン　ロングフェロープレースエーピーティ　＃３４０４　４

最終頁に続く

(54)【発明の名称】安全なアプリケーション環境のためのローバスト多要素認証

(57)【要約】
【課題】アプリケーション環境のためのローバストで安全な認証技法を提供する。
【解決手段】認証システムは、多要素ユーザ認証を利用する。１つの認証要素はユーザの発話パターンであり、もう１つの認証要素はワンタイムパスコードである。発話パターンおよびパスコードは、音声ポータルおよび／またはブラウザ入力を介して提供することができる。発話パターンは話者照合サブシステムに転送される一方、パスコードはパスコード確認サブシステムに転送される。ユーザが、多要素プロセスによって認証を受けると、所望の保護された１つまたは複数のアプリケーションへのアクセスを与えられる。ポリシー手順および認証手順は、これらのアプリケーションから抽出することができ、それによって、複数のアプリケーションにわたるシングルサインオンが可能になる。



【特許請求の範囲】
【請求項１】
ユーザを認証する方法であって、
（ａ）主張されたユーザのアイデンティティを受け取るステップと、
（ｂ）前記ユーザから第１の通信チャネルを介して第１の認証サンプルを受信するステップと、
（ｃ）前記ユーザとの第２の通信チャネルであって、
（ｉ）前記第１の通信チャネルに対して帯域外である第２の通信チャネル
を確立するステップと、
（ｄ）前記第２の通信チャネルを介して前記ユーザと、第２の認証サンプルに関するチャレンジ－応答プロトコルの少なくとも一部を実行するステップと、
（ｅ）前記主張されたアイデンティティに一意に関連付けられて記憶されたテンプレートに基づいて、前記第１の認証サンプルおよび前記第２の認証サンプルの少なくとも１つを検証するステップと、
（ｆ）前記認証サンプルの別のものを、（ｄ）における前記検証とは独立して検証するステップと、
（ｇ）ステップ（ｅ）およびステップ（ｆ）における前記検証に基づいて、前記ユーザにアクセスを許可するステップと
を含む方法。
【請求項２】
前記ステップ（ｄ）は、
（１）前記認証サンプルの少なくとも１つを提供するように、前記第２の通信チャネルを介して前記ユーザに指示すること、および
（２）前記指示した認証サンプルを前記第１の通信チャネルを介して受信すること
を含む
請求項１に記載のユーザを認証する方法。
【請求項３】
（１）前記認証サンプルの少なくとも１つは、発話されたものであり、
（２）発話認識技法の適用を介して、前記発話された認証サンプルをテキスト形式に変換することをさらに含む
請求項１に記載のユーザを認証する方法。
【請求項４】
（１）前記認証サンプルの少なくとも１つは、発話されたものであり、
（２）前記（ｅ）は、（ｉ）前記主張されたアイデンティティ、（ｉｉ）前記テンプレート、および（ｉｉｉ）前記発話された認証サンプルを必要とする話者照合プロトコルを適用することによって、前記ユーザの一意の音声特性を認証することを含む
請求項１に記載のユーザを認証する方法。
【請求項５】
前記検証された認証サンプルの少なくとも１つに基づいて、テンプレートデータベースを更新することをさらに含む
請求項１に記載のユーザを認証する方法。
【請求項６】
前記第１の通信チャネルは、電話によるものであり、前記第２の通信チャネルは、コンピュータネットワークである
請求項１に記載のユーザを認証する方法。
【請求項７】
（１）前記第１の認証サンプルおよび前記第２の認証サンプルは、発話形式で提供され、
（２）前記発話された認証サンプルの少なくとも１つを検証用のテキスト形式に変換することをさらに含む

請求項１に記載のユーザを認証する方法。
【請求項８】
前記認証サンプルの少なくとも１つは、バイオメトリック属性である
請求項１に記載のユーザを認証する方法。
【請求項９】
前記認証サンプルの少なくとも１つは、前記ユーザによって保持された動的に変化する属性である
請求項１に記載のユーザを認証する方法。
【請求項１０】
前記ステップ（ａ）は、前記ユーザの電話呼び出し側識別情報を確定するステップを含む
請求項１に記載のユーザを認証する方法。
【請求項１１】
前記ステップ（ｆ）は、
（１）前記別の認証サンプルに基づいて第１の文字列を生成するステップと、
（２）前記主張されたアイデンティティに基づいて第２の文字列を独立して生成するステップと、
（３）前記第１の文字列および前記第２の文字列をデジタルに比較するステップと、
（４）前記文字列が一致した場合、前記別の認証サンプルを認証するステップと
を含む
請求項１に記載のユーザを認証する方法。
【請求項１２】
共通のセッション中に、認証を必要とする複数のアプリケーション間で前記認証を共有することによって、シングルサインオンプロセスを可能にすることをさらに含む
請求項１に記載のユーザを認証する方法。
【請求項１３】
ユーザを認証する方法であって、
（ａ）主張されたユーザのアイデンティティを受け取るステップと、
（ｂ）前記ユーザから第１の通信チャネルを介して第１の認証サンプルを受信するステップと、
（ｃ）前記ユーザから第２の通信チャネルを介して第２の認証サンプルを受信するステップと、
（ｄ）前記主張されたアイデンティティに一意に関連付けられて記憶されたテンプレートに基づいて、前記第１の認証サンプルおよび前記第２の認証サンプルの少なくとも１つを検証するステップと、
（ｅ）前記認証サンプルの別のものを、（ｄ）における前記検証とは独立して検証するステップと、
（ｆ）ステップ（ｄ）およびステップ（ｅ）における前記検証に基づいて、前記ユーザにアクセスを許可するステップと
を含む方法。
【請求項１４】
（１）前記第２の通信チャネルは、前記第１の通信チャネルに対して帯域外であり、
（２）前記ステップ（ａ）と前記ステップ（ｃ）との間に、前記第１の通信チャネルがアプリケーション環境にとって十分に安全でないとの判断に応じて、前記第２の通信チャネルを使用するように前記ユーザに指示することをさらに含む
請求項１３に記載のユーザを認証する方法。
【請求項１５】
ユーザを認証する方法であって、
（ａ）認証対象の主張されたユーザのアイデンティティを取得するステップと、
（ｂ）通信チャネルを介して安全なパスコードを発話するようにユーザに指示するステ

ップと、
（ｃ）前記ユーザの音声をバイオメトリック認証するステップであって、
（ｉ）前記主張されたアイデンティティに一意の記憶された音声特性を取得すること、
（ｉｉ）前記発話された安全なパスコードに基づいて前記ユーザの音声特性を抽出すること、および
（ｉｉｉ）前記記憶された音声特性と前記抽出された音声特性とを比較すること
によってバイオメトリック認証するステップと、
（ｄ）前記安全なパスコードを認証するステップであって、
（ｉ）前記主張されたアイデンティティに対応する再生されたパスコードを取得すること、および
（ｉｉ）前記再生されたパスコードと前記発話されたパスコードとを比較すること
によって認証するステップと、
（ｅ）前記ユーザの音声および前記パスコードが、ステップ（ｃ）およびステップ（ｄ）に基づいて認証された場合、前記ユーザにアクセスを許可するステップと
を含む方法。
【請求項１６】
ユーザ認証の後に安全なアプリケーションへのアクセスを提供するシステムであって、
（ａ）ポータルサブシステムであって、
（ｉ）第１の通信チャネルを介して第１のユーザ認証サンプルを受信し、
（ｉｉ）バイオメトリックプロセスを介して前記第１の認証サンプルを認証する
ように構成されたポータルサブシステムと、
（ｂ）認証サブシステムであって、
（ｉ）前記ポータルサブシステムと、
（ｉｉ）前記第１の通信チャネルに対して帯域外の第２の通信チャネルと
に接続された認証サブシステムと、
（ｃ）前記認証サブシステムであって、
（ｉ）前記第２の通信チャネルを介してサンプルを提供するように、前記ポータルサブシステムを介してユーザに指示し、
（ｉｉ）前記第２の通信チャネルを介して前記第２の認証サンプルを受信し、
（ｉｉｉ）前記第２の認証サンプルを認証する
ように構成された前記認証サブシステムと、
（ｄ）アプリケーションサーバであって、
（ｉ）前記ポータルサブシステムおよび前記認証サブシステムに接続され、
（ｉｉ）前記第１の認証サンプルおよび前記第２の認証サンプルの双方の認証が成功すると、前記ユーザにアクセスを提供する
アプリケーションサーバと
を備えるシステム。
【請求項１７】
ユーザ認証を提供して、保護されたアプリケーションへのアクセスを制御するシステムであって、
（ａ）主張されたユーザのアイデンティティを受け取るように構成されたインタフェースと、
（ｂ）第１の通信パスに接続され、前記ユーザに関連付けられた第１の認証データを受信するように構成されたインタフェースと、
（ｃ）前記第１の通信パスに対して帯域外である第２の通信パスに接続された、前記ユーザに対するインタフェースと、
（ｄ）前記ユーザに関連付けられた第２の認証データに関するチャレンジ－応答通信の少なくとも一部を、前記第２の通信パスを介して実行する手段と、
（ｅ）前記ユーザの名目上のアイデンティティに基づいて、前記第１の認証データを検

証する手段と、
（ｆ）（ｅ）とは独立に、前記第２の認証データを検証する手段と、
（ｇ）双方の認証データが検証された後に、前記ユーザにアクセスを許可する手段と
を備えるアクセスを制御するシステム。
【請求項１８】
（ｄ）前記第１の通信パスを介して前記第２の認証サンプルを提供するように、前記第２の通信パスを介して前記ユーザに指示する手段をさらに備える
請求項１７に記載のアクセスを制御するシステム。
【請求項１９】
前記第１の通信パスは電話によるものであり、
前記第２の通信パスはコンピュータネットワークである
請求項１７に記載のアクセスを制御するシステム。
【請求項２０】
（１）双方の認証データは、口頭形式で受信され、
（２）前記認証データの少なくとも１つを検証用のテキスト形式に変換するように構成された発話ツーテキストモジュールをさらに備える
請求項１７に記載のアクセスを制御するシステム。
【請求項２１】
ユーザ認証を提供して、保護されたアプリケーションへのアクセスを制御するシステムであって、
（ａ）システムインタフェースに安全なパスコードを発話するようにユーザに指示する手段と、
（ｂ）バイオメトリック認証装置であって、
（ｉ）前記発話された安全なパスコードに基づいて前記ユーザの韻律的特徴を抽出し、
（ｉｉｉ）前記抽出した韻律的特徴を、前記ユーザの記憶された韻律テンプレートと照合する
ように構成されたバイオメトリック認証装置と、
（ｄ）パスコード認証装置であって、
（ｉ）前記発話されたパスコードに対応するパスコードを再生し、
（ｉｉ）前記再生したパスコードを前記発話されたパスコードと照合する
ように構成されたパスコード認証装置と、
（ｅ）前記ユーザの音声および前記パスコードを認証した後、前記ユーザにアクセスを許可する手段と
を備えるシステム。
【請求項２２】
ユーザを認証するコンピュータ可読媒体であって、実行されると、
（ａ）主張されたユーザのアイデンティティを受け取り、
（ｂ）前記ユーザから第１の通信パスを介して第１の認証サンプルを受信し、
（ｃ）前記ユーザとの第２の通信パスであって、
（ｉ）前記第１の通信パスに対して帯域外である第２の通信パス
を確立し、
（ｅ）前記第２の通信パスを介して前記ユーザと、第２の認証サンプルに関するチャレンジ－応答プロトコルの少なくとも一部を実行し、
（ｅ）前記主張されたアイデンティティに一意に関連付けられて記憶されたテンプレートに基づいて、前記第１の認証サンプルおよび前記第２の認証サンプルの少なくとも１つを検証し、
（ｆ）前記認証サンプルの別のものを、（ｅ）における前記検証とは独立して検証し、
（ｇ）（ｅ）および（ｆ）における前記検証に基づいて、前記ユーザにアクセスを許可する

論理命令を含むコンピュータ可読媒体。
【請求項２３】
前記受信する手段の少なくとも１つは、
（１）前記認証サンプルの少なくとも１つを提供するように、前記第１の通信チャネルを介して前記ユーザに指示する手段と、
（２）前記指示した認証サンプルを前記第２の通信チャネルを介して受信する手段と、
を含む
請求項２２に記載のシステム。
【請求項２４】
前記第１の通信チャネルは、電話によるものであり、
前記第２の通信チャネルは、コンピュータネットワークである
請求項２２に記載のコンピュータ可読媒体。
【請求項２５】
（１）前記第１の認証サンプルおよび前記第２の認証サンプルは、発話形式であり、
（２）実行されると、前記発話された認証サンプルの少なくとも１つを検証用のテキスト形式に変換する論理命令をさらに含む
請求項２２に記載のコンピュータ可読媒体。
【請求項２６】
ユーザを認証するコンピュータ可読媒体であって、実行されると、
（ａ）認証対象の主張されたユーザのアイデンティティを取得し、
（ｂ）通信チャネルを介して安全なパスコードを発話するようにユーザに指示し、
（ｃ）前記ユーザの音声を、
（ｉ）前記主張されたアイデンティティに一意の記憶された音声特性を取得すること、
（ｉｉ）前記発話された安全なパスコードに基づいて前記ユーザの音声特性を抽出すること、および
（ｉｉｉ）前記記憶された音声特性と前記抽出した音声特性とを比較すること
によってバイオメトリック認証し、
（ｄ）前記安全なパスコードを、
（ｉ）前記主張されたアイデンティティに対応する再生されたパスコードを取得すること、および
（ｉｉ）前記再生されたパスコードと前記発話されたパスコードとを比較すること
によって認証し、
（ｅ）前記ユーザの音声および前記パスコードが、（ｃ）および（ｄ）に基づいて認証された場合、前記ユーザにアクセスを許可する
論理命令を含むコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータシステムに使用されるユーザ認証に関する。
【背景技術】
【０００２】
［背景］
認証技術は、一般に、保護された情報に対するユーザアクセスを許可する前に、ユーザのアイデンティティを検証するために実施される。
話者照合は、音声ベースのシステムおよび必要に応じて他の種類のシステムの双方で多く使用されるバイオメトリック認証技術である。
音声ベースのシステムは、通信ネットワーク（公衆交換電話網等）を介して（ユーザの通信デバイスを通じて）ユーザにアクセス可能な音声送信／受信デバイス（電話等）を含むことができる。

一般に、話者照合は、ユーザが、自身の固有の声の特徴について音声ベースのシステムに「教示する」エンロールメントプロセスを必要とする。

話者照合は、少なくとも３つの一般的技法、すなわち、テキスト依存／固定フレーズ（text-dependent/fixed-phrase）技法、テキスト独立／非制約（text-independent/unconstrained）技法、およびテキスト依存／指示フレーズ（text-dependent/prompted-phrase）技法によって実施されることができる。

【０００３】

テキスト依存／固定フレーズ照合技法は、エンロールメントプロセスの間、１つまたは複数のフレーズ（言葉、符号、数字、またはこれらの１つまたは複数の組み合わせを含む）を発声するようにユーザに要求することができる。

発声したこのようなフレーズ（複数可）は記録され、エンロールメントテンプレートファイルとして記憶されることができる。

認証セッションの間、ユーザは、同じフレーズ（複数可）を発声するように指示される。

次いで、発声されたフレーズは、その主張されたユーザのアイデンティティに関連付けられた記憶されたエンロールメントテンプレートファイルと比較される。

エンロールメントテンプレートファイルと発声されたフレーズ（複数可）とが互いにほぼ一致すると、ユーザのアイデンティティの検証は成功する。

記録された発話が、エンロールメントプロセス中に、または、データベース（例えば、エンロールメントテンプレートファイル）から盗難されると、この技法は、盗難されたものを認証セッション中に再生することによる攻撃を受けるおそれがある。

さらに、この技法は、テキストから発話音声へのクローニング技法（以下、「音声クローニング」）による攻撃も受けるおそれもある。

人の発話は、この音声クローニングによって、要求されたフレーズ（複数可）を発声するように（人の音声および韻律的な特徴を使用して）合成される。

【０００４】

テキスト独立／非制約照合技法は、通常、より長いエンロールメント期間（例えば１０～３０秒）と、各ユーザからのより多くのトレーニングデータとを必要とする。

この技法は、通常、エンロールメントおよび認証の間、同じフレーズ（複数可）の使用を必要としない。

その代わり、ユーザの声道の特定の音響特徴を使用して、ユーザのアイデンティティが検証される。

このような音響特徴は、当技術分野において既知の発話サンプリング／雑音フィルタリングアルゴリズムを使用して、トレーニングデータに基づき決定することができる。

音響特徴は、テンプレートファイルとして記憶される。

認証中、ユーザは、任意のフレーズを発声することができ、ユーザのアイデンティティは、（発声したフレーズに基づく）ユーザの音響特徴を、テンプレートファイルに記憶されたユーザの音響特徴と比較することによって検証される。

この技法は、ユーザが述べるあらゆるものを認証に使用できるので、ユーザにとって便利である。

さらに、記憶されたフレーズが盗難されるということもない。

しかしながら、この技法は、計算がより多くなり、記録された発話を盗難して再生することおよび／または音声クローニングによる攻撃を依然として受けるおそれがある。

【０００５】

テキスト依存／指示フレーズ照合技法は、ユーザの声道の特定の音響特徴を使用してユーザを認証する点で、上述したテキスト独立／非制約技法と類似している。

一方、ランダムに生成されるか、それ以外に予測できないパスフレーズ（例えば、ワンタイムパスコード（one-time passcode）、すなわちＯＴＰ）をユーザに実時間で繰り返すように要求することによって、単純な再生攻撃が無効にされる。

しかしながら、この技法も、高度化した音声クローニング攻撃には依然として脆弱であ

るおそれがある。
【特許文献１】仏国特許第２７９５２６４号
【特許文献２】国際公開第０１／８０５２５号
【特許文献３】国際公開第９８／２３０６２号
【特許文献４】国際公開第９８／１６９０６号
【発明の開示】
【発明が解決しようとする課題】
【０００６】
したがって、上記技法のどれよりもローバストで安全な認証技法を提供することが望ましい。
【課題を解決するための手段】
【０００７】
［概要］
改良された認証システムの例示の一実施の形態では、多要素ユーザ認証が含まれる。
セキュリティを高めるために、第１の認証要素が、第１の通信チャネルを介してユーザから受け取られ、システムは、第１の通信チャネルに対して帯域外の第２の通信チャネルを介して、第２の認証要素の入力をユーザに指示する。
第２のチャネルがそれ自体認証される場合（例えば、ユーザの管理下にあることが判明しているもの、または、ユーザの管理下になる可能性が高いもの）、第２の要素は、第１の通信チャネルを介して提供することができる。
別の例示の実施の形態では、２つ（または３つ以上）の認証要素が、指示が行われるか否かを問わず、指示がどのように行われるかを問わず、それ自体、帯域外通信チャネルを介して提供される。
限定ではなく、例えば、認証要素の１つは、認証されたブラウザセッションを介して指示されることができ、別の認証要素は、前述の音声ポータルを介して提供されることができる。
【０００８】
前述の例示の実施の形態の共通の態様では、システムは、第１の認証要素を第１の通信チャネルを介してユーザから受け取り、第１の通信チャネルに対して帯域外の第２の通信チャネルを介して、第２の認証要素に関し、ユーザと通信する。
この通信は、第２の認証要素の入力をユーザに指示することを含むことができ、かつ／または、第２の認証要素を受信することを含むことができる。
第２の認証要素に関係したチャレンジ－応答プロトコルの少なくとも或る部分が、帯域外チャネルを介して行われるということによって、セキュリティの所望の高度化が提供される。
【０００９】
ユーザは、多要素プロセスによって認証を受けると、所望の保護された１つまたは複数のアプリケーションへのアクセスを与えられる。
ポリシーおよび認証手順は、これらのアプリケーションから抽出されることができ、それによって、複数のアプリケーションにわたるシングルサインオンが可能になる。
上記例示の実施の形態およびさらに他の実施の形態は、以下にさらに詳述される。
【発明を実施するための最良の形態】
【００１０】
［詳細な説明］
Ａ．アプリケーションサーバ用の多要素認証システム
図１は、例示の一実施の形態に従って、アプリケーションサーバ（注１）１７０に接続されて、当該アプリケーションサーバ１７０用の認証を提供する多要素認証システム１００の要素および信号の流れを概略的に示している。
この例示の多要素認証システム１００は、認証サブシステム１２０に接続されたポータルサブシステム２００を含む。

また、この例示の認証システム１００は、話者照合（ＳＶ）サブシステム３００および確認サブシステム１３０も含むか、または、認証サブシステム１２０を介してこれらのサブシステムに接続されている。

【００１１】

通常、ポータルサブシステム２００は、初期ユーザ検証を行うためのユーザ情報を収容する内部または外部データベース１４０にアクセスすることができる。

例示の一実施の形態では、データベース１４０は、登録プロセス中に得られたユーザ識別情報を含むことができる。

例えば、データベース１４０は、各ユーザに関連付けられたユーザ名および／または他の識別子番号（例えば、社会保障番号、電話番号、ＰＩＮ等）を収容することができる。

ポータルサブシステム２００の例示の一実施の形態は、図２に関連して後に詳述する。

【００１２】

また、認証サブシステム１２０も、通常、エンロールメントプロセス中に取得されたユーザ情報を収容する内部または外部データベース１５０にアクセスすることができる。

例示の一実施の形態では、データベース１４０およびデータベース１５０は、同じデータベースとすることもできるし、個別のデータベースとすることもできる。

例示のエンロールメントプロセスは、図７に関連して後に詳述する。

【００１３】

次に、上記例示のサブシステムのオペレーションおよびこれらのサブシステム間の関係を、例示の環境に関連して説明することにする。

この例示の環境は、アプリケーションサーバにアクセスしようとするユーザが、まず識別され、次に、多要素認証交渉が行われて、ユーザのアイデンティティが検証される環境である。

【００１４】

（注１）所望の構成に応じて、認証システムは、もちろん、アプリケーションサーバの一部として構成されることもできる。

【００１５】

Ｂ．予備的ユーザ識別

図１を参照して、一実施の形態では、ポータルサブシステム２００は、通信チャネル１６０または１８０を介して初期ユーザ入力を受信することができる。

通信チャネルが電話回線である場合に対応して、ポータルサブシステム２００は、音声ポータルとして構成される。

受信した初期ユーザ入力は、ポータルサブシステム２００によって処理され、１つまたは複数のユーザ識別技法（またはそれらの組み合わせ）を使用して、主張されたユーザのアイデンティティを確定する。

例えば、ユーザは、自身の識別情報をポータルサブシステム２００に手動で入力することができ、ポータルサブシステムは、次に、その識別情報をデータベース１４０と照合することによって、主張されたユーザのアイデンティティを検証する。

あるいは、電話による実施態様では、ポータルサブシステム２００は、標準的な呼び出し側ＩＤ技術を使用して、ユーザの名前および／または電話番号を自動的に取得し、この情報をデータベース１４０と照合することができる。

あるいは、ユーザは、自身の情報をポータルサブシステム２００に発話することもできる。

【００１６】

図２は、ポータルサブシステム２００の例示の一実施の形態を示している。

この例示の実施の形態では、電話システムインタフェース２２０が、通信チャネル（図１では、要素１６０または１８０）を介したユーザの送受話器のインタフェースとして機能する。

この通信チャネルは、この実施の形態では、あらゆる種類の電話網（公衆交換電話網、携帯電話網、衛星ネットワーク等）とすることができる。

インタフェース２２０は、Dialogic（商標）（Intelの関連子会社）等の企業から市場で入手することができ、本明細書では詳細に説明する必要はない。

【００１７】

インタフェース２２０は、送受話器から受け取った信号を１つまたは複数のモジュールに渡す。

この１つまたは複数のモジュールは、ポータルサブシステム２００、認証サブシステム１２０、および／またはアプリケーションサーバ１７０といった他の要素によって使用可能な形態にその信号を変換する。

これらのモジュールは、発話認識（注２）モジュール２４０、テキストツー発話（注３）（「ＴＴＳ（text-to-speech）」）モジュール２５０、プッシュホンモジュール２６０、および／またはオーディオＩ／Ｏモジュール２７０を含んでよい。入来する信号のフォーマットに応じて、適切な１つまたは複数のモジュールが使用される。

【００１８】

したがって、発話認識モジュール２４０は、通常は所与の言語のユニバーサル話者モデル（すなわち、特定の人に特有のものでない）に基づいて、入来する発話言葉を英数字列（または非アルファベットベースの言語に適した他のテキスト形式）に変換する。

同様に、プッシュホンモジュール２６０は、（例えば、電話のキーパッドで押下されたキーからの）ＤＴＭＦ「プッシュホン」を認識し、それらを英数字列に変換する。

オーディオＩ／Ｏモジュール２７０では、入力部が、入来するアナログオーディオ信号を（デジタル音声メールシステムのように）そのデジタル化された表現に変換する一方、出力部は、デジタル信号（例えば、ＰＣの「．ｗａｖ」ファイル）を変換し、それを送受話器に戻して再生する。

この例示の実施の形態では、これらのモジュールのすべてが、インタープリタ／プロセッサ２８０を介して、アクセスされて制御される。

このインタープリタ／プロセッサ２８０は、ＶｏｉｃｅＸＭＬプログラミング言語（注４）でプログラムされたアプリケーションを実行するコンピュータプロセッサを使用して実施される。

【００１９】

特に、ＶｏｉｃｅＸＭＬインタープリタ／プロセッサ２８０は、アプリケーションサーバ１７０（図１参照）における呼び出し側プログラムからのＶｏｉｃｅＸＭＬ要求を解釈し、発話認識モジュール、テキストツー発話モジュール、プッシュホンモジュール、および／またはオーディオＩ／Ｏモジュールに対してそれらの要求を実行し、その結果をＶｏｉｃｅＸＭＬパラメータの形で呼び出し側プログラムに返すことができる。

また、ＶｏｉｃｅＸＭＬインタープリタ／プロセッサ２８０は、送受話器が発した信号を解釈し、それらの信号をモジュール２４０～２７０に対して実行し、その結果をアプリケーションサーバ１７０、認証サブシステム１２０または送受話器に返すこともできる。

【００２０】

ＶｏｉｃｅＸＭＬは、拡張マークアップ言語（ＸＭＬ）に基づく音声アプリケーション用のマークアップ言語である。

より具体的には、ＶｏｉｃｅＸＭＬは、ＩＥＥＥ業界標準／技術機構（ＩＥＥＥ－ＩＳＴＯ）の一プログラムであるＶｏｉｃｅＸＭＬフォーラム（http://www.voicexml.org/）によって開発されてサポートされている標準規格である。

ＨＴＭＬは、ウェブアプリケーションに対するものであるように、ＶｏｉｃｅＸＭＬは、音声アプリケーションに対するものである。

確かに、ＨＴＭＬがウェブページを表示するのに対して、ＶｏｉｃｅＸＭＬが、ダイアログおよびプロンプトを含めて、音声インタフェースをレンダリングするのに使用される環境では、ＨＴＭＬおよびＶｏｉｃｅＸＭＬは共に使用されうる。

【００２１】

次に図１に戻って、ポータルサブシステム２００が、ユーザの入力を英数字列に変換した後、その英数字列は、データベース１４０に渡されて、記憶されたユーザプロファイル

と照合される。
ユーザが、この段階で自身の識別情報をどのように提供しようとも、このような識別情報は、通常、予備的なものとみなされる。
その理由は、詐称者が、（例えば、入力すべきデータを盗用したり、ユーザの電話にアクセスしたり、音声クローニング技術を使用してユーザになりすましたりすることによって）識別情報を提供するのが比較的容易だからである。
したがって、この段階で得られるアイデンティティは、後述する追加の技法を使用して確定されるように、正当と判明することもあるし、正当でないと判明することもある「主張されたアイデンティティ」とみなされる。
【００２２】
高信頼認証を必要とするアプリケーションでは、主張されたユーザのアイデンティティは、認証サブシステム１２０に渡され、認証サブシステム１２０は、後述するように多要素認証プロセスを実行する。
【００２３】
（注２）時に、発話ツーテキスト（「ＳＴＴ（speech-to-text）」）モジュールと呼ばれることがある。
（注３）時に、発話シミュレーションまたは発話合成と呼ばれることがある。
（注４）ＶｏｉｃｅＸＭＬは単なる例示にすぎない。
プレーンＸＭＬ、MicrosoftのＳＯＡＰ、多種多様な他の既知の音声プログラミング言語（ＨＰまたは他社が提供）等の他の言語も使用可能であることが、当業者には容易に理解されよう。
【００２４】
Ｃ．第１の要素認証
認証サブシステム１２０は、通信チャネル１６０からポータルサブシステム２００を介して、または、通信チャネル１８０を介して、認証プロセス用の認証サンプル（より一般的には、第１の認証要素）を入力するようにユーザに指示する。
【００２５】
認証サンプルは、バイオメトリックデータ（注５）の形態を取ることができる。
このバイオメトリックデータとしては、発話（例えば、通信チャネル１６０からポータル２００を介して）、網膜パターン、指紋、手書き、キーストロークパターン、あるいは、ユーザに固有であり、したがって盗難も偽造も容易にされない他の或るサンプル（例えば、アプリケーションサーバ１７０を介し通信チャネル１８０を介して）等がある。
【００２６】
例示として、認証サンプルが、音声パケットまたはユーザの他の或る発話表現を含むものと仮定する。
この音声パケットは、発話された入力が、通常、ユニバーサル発話認識モジュールを使用してテキストに変換されることができず、音声ポータルのオーディオＩ／Ｏモジュールを介して渡されてユーザ特有の音声テンプレートと比較される点を除いて、前述した同じＶｏｉｃｅＸＭＬ技術を使用してポータルサブシステム２００で得られることができる。
【００２７】
例えば、認証サブシステム１２０は、主張されたユーザのアイデンティティに関連付けられたテンプレート音声ファイルをデータベース１５０から検索することができ、または、それ以外にテンプレート音声ファイルにアクセスすることができる。
テンプレート音声ファイルは、エンロールメントプロセス中に作成されて、データベース１５０に記憶されることができる。
一実施の形態では、認証サブシステム１２０は、受信した音声パケットおよび検索したテンプレート音声ファイルを、話者照合サブシステム３００に転送することができる。
【００２８】
図３は、話者照合サブシステム３００の例示の一実施の形態を示している。
この例示の実施の形態では、話者認識モジュール３１０が、音声パケットを英数字（ま

たは他のテキスト）形式に変換する一方、話者照合モジュール３２０が、音声パケットをユーザの音声テンプレートファイルと比較する。

話者照合の技法は、当技術分野において既知であり（例えば、SpeechWorks社から提供されているＳｐｅｅｃｈＳｅｃｕｒｅ、Nuance社から提供されているＶｅｒｉｆｉｅｒ等を参照）、本明細書ではさらに詳細に説明する必要はない。

話者が照合されると、これらの音声パケットは、テンプレート適合モジュール３３０を介して、ユーザの音声テンプレートファイル（おそらく音声テンプレートファイルへの更新として）に追加されることもできる。

【００２９】

上記は、ユーザの音声テンプレートが、例えば、エンロールメントプロセス中に事前に生成された結果として利用可能であることを仮定する。

例示のエンロールメントプロセスは、図７に関連して後述される。

【００３０】

次に図１に戻って、話者照合サーバ３００は、発話と音声テンプレートとが（規定された許容範囲内で）一致すると確定すると、肯定結果を認証サブシステム１２０に返す。

【００３１】

他の形態の認証サンプルが発話の他に提供される場合、他のユーザ認証技法が、話者照合サブシステム３００の代わりに配備されることができる。

例えば、指紋照合サブシステムは、Veridicom/Gemplus社から提供されているＭａｔｃｈ－Ｏｎ－Ｃａｒｄスマートカード、DigitalPersona社から提供されている「U. are U.」製品等を使用することができる。

同様に、虹彩／網膜スキャン照合サブシステムは、Iridian Technologies社から提供されているＩｒｉｓ　Ａｃｃｅｓｓ製品、EyeDenitify社から提供されているＥｙｅｄｅｎｔｉｆｉｃａｔｉｏｎ　７．５製品を使用することができる。

これらのおよびさらに別の市販のユーザ照合技術は、当技術分野において既知であり、本明細書で詳述する必要はない。

【００３２】

（注５）バイオメトリックデータは、高度に安全であるだけでなく、ユーザが常に持っているものであるので、好ましい。

しかし、それは必要とされない。

たとえば、あまり安全でない用途またはあるクラスのユーザが共通のアイデンティティを共有することを可能にする用途では、最初の認証要素はバイオメトリックでないデータの形態をとる場合がある。

【００３３】

Ｄ．第２の要素認証

多要素認証プロセスの例示の一実施の形態の別の態様では、認証サブシステム１２０は、ポータルサブシステム２００を介して、安全なパスコード（例えば、ＯＴＰ）（より一般的には、第２の認証要素）の発話またはそれ以外の入力を行うようにユーザに指示することもできる。

主張されたユーザのアイデンティティと丁度同様に、安全なパスコードは、直接（例えば、英数字列として）提供されることもできるし、音声入力を介して提供されることもできる。

【００３４】

音声入力の場合、認証サブシステム１２０は、音声パケットを、安全なパスコードを含む英数字（または他のテキスト）列に変換する。

例えば、認証サブシステム１２０は、音声サンプルを発話認証モジュール２４０（図２参照）または３１０（図３参照）に渡して、その発話入力を英数字（または他のテキスト）列に変換することができる。

【００３５】

例示の安全な一実施態様では、安全なパスコード（または他の第２の認証要素）は、チ

ャネル１８０等の（その認証要素がユーザによって与えられるチャネルに対して）帯域外の安全なチャネルを介して、ユーザによって、システムに提供されることができる。

例示の帯域外のチャネルは、（ユーザのウェブブラウザへの接続を介した）アプリケーションサーバ１７０への安全な接続、または、その認証要素が与えられるチャネルとは物理的に別の（または同等に保護された）他のあらゆる入力を含んでよい。

【００３６】

別の例示の安全な実施態様では、帯域外チャネルは、安全なパスコードの入力をユーザに指示するのに使用されることができる。

ここで、安全なパスコードは、第１の認証要素が提供される（注６）のと同じチャネルを介して、その後、提供されうる。

この例示の実施態様では、第２のチャネルが、ユーザによって制御される可能性が最も高い意味で信頼される（または有効に認証される）場合に、第２のチャネルを介して第２の認証要素の入力を指示するだけで十分であり、ユーザが、第２のチャネルを介して第２の認証要素を提供する必要は（必ずしも）ない。

例えば、第２のチャネルが、ユーザに一意に関連付けられた電話（例えば、住宅回線、携帯電話等）である場合、電話に応答する人は、実際にそのユーザであると考えられる。

他の信頼されるチャネル、または、有効に認証されるチャネルには、状況に応じて、物理的に安全で、かつ、アクセス制御されるファクシミリ装置、バイオメトリック方式の下で暗号化される、または、それ以外にユーザによってのみ解読可能な電子メール等が含まれる。

【００３７】

いずれの例示の実施態様においても、第２の認証要素に関するチャレンジ－応答通信の少なくとも一部を帯域外チャネルを介して行うことによって、通信の帯域外部分の高度化されたセキュリティが、通信全体に利用される。

【００３８】

第２の例示の実施態様の別の態様では、第２の通信チャネルを介してユーザに指示することは、ユーザに安全なパスコードを送信することを含むこともできる。

次いで、ユーザは、この安全なパスコードが有効である或る期間中に、このパスコードを返信することが予想される。

例えば、システムは、ＯＴＰを生成して、ユーザに送信することができ、ユーザは、そのＯＴＰの有効期限が切れる前に、同じＯＴＰを返信しなければならない。

あるいは、ユーザは、システムが保持するＯＴＰジェネレータに整合したＯＴＰジェネレータを有することもできる。

【００３９】

ワンタイムパスコード（ＯＴＰ）および他の形態の安全なパスコードを実施する多くの方式が存在する。

例えば、いくつかの既知で工業所有権を有するトークンベース方式には、ＲＳＡ（例えば、ＳｅｃｕｒＩＤ）またはActivCard社（例えば、ＡｃｔｉｖＣａｒｄ　Ｇｏｌｄ）から入手可能なトークン等のハードウェアトークンが含まれる。

同様に、いくつかの既知の公有方式には、Ｓ／Ｋｅｙメカニズムまたは簡易認証／セキュリティレイヤ（ＳＡＳＬ（Simple Authentication and Security layer））メカニズムが含まれる。

実際には、非常に簡易な方式は、電子メール、ファックス、場合によっては郵便さえも使用して、帯域幅および／または時刻表の制約に応じてＯＴＰを安全に送信することができる。

その上、一般に、方式が異なることに関連して、コスト、利便性のレベル、および所与の目的の実用性も異なる。

上記方式および他のＯＴＰ方式は、当技術分野においてよく理解されており、本明細書で詳細に説明する必要はない。

【００４０】

（注６）もちろん、第２の認証要素は、第２の通信チャネルを介して提供されることもできる。
これは、さらに大きなセキュリティを提供する。
しかしながら、これは、システムが配備された特定のユーザ環境に応じて、便利さまたは望ましさが劣る場合がある。
【００４１】
Ｅ．オペレーションの結合
上述した例示の予備的なユーザ識別プロセス、第１の要素認証プロセスおよび第２の要素認証プロセス（注７）は、高度化されたセキュリティを有する認証システム全体を形成するように結合されうる。
【００４２】
図４は、予備的なユーザ識別と共に２要素認証を含む結合されたシステムのオペレーションのこのような例示の一実施の形態を示している。
この実施の形態は、双方のユーザ認証入力（バイオメトリックデータに安全なパスコードを加えたもの）が発話形式で提供される場合を示している。
【００４３】
認証入力は、２つのサブプロセスによって処理されることができる。
第１のサブプロセスでは、主張されたユーザのアイデンティティに関連付けられた音声テンプレートファイル（例えば、エンロールメントプロセス中にユーザの入力から作成されたファイル）が検索されることができる（ステップ４０２）。
次に、認証サンプルからの音声パケットが、音声テンプレートファイルと比較されることができる（ステップ４０４）。
音声パケットが、規定された許容範囲内で音声テンプレートファイルとほぼ一致するかどうかが確定される（ステップ４０６）。
一致しないと確定されると、否定結果が返される（ステップ４０８）。
一致すると確定されると、肯定結果が返される（ステップ４１０）。
【００４４】
第２のサブプロセス（注８）では、英数字（または他のテキスト）列（例えば、安全なパスコードを含むファイル）が、発話をテキストに変換することによって、計算されることができる（ステップ４１２）。
例えば、図２のポータルサブシステム２００が使用される場合、ユーザ入力されたパスコードは、発話認識モジュール２４０（音声入力用）またはプッシュホンモジュール２６０（キーパッド入力用）を使用して、英数字（または他のテキスト）列に変換される。
次に、英数字（または他のテキスト）列が、正しいパスコード（パスコードアルゴリズムを介して計算されたもの、または、安全な記憶装置から検索されたもののいずれか）と比較されることができる（ステップ４１４）。
英数字（または他のテキスト）列が、正しいパスコードとほぼ一致するかどうかが確定される（ステップ４１６）。
一致しないと確定されると、否定結果が返される（ステップ４１８）。
一致すると確定されると、肯定結果が返される（ステップ４２０）。
【００４５】
第１のサブプロセスおよび第２のサブプロセスからの結果が、検査される（ステップ４２２）。
いずれかの結果が否定である場合、ユーザは、認証されなかったことになり、否定結果が返される（ステップ４２４）。
双方の結果が肯定である場合、ユーザの認証は成功し、肯定結果が返される（ステップ４２６）。
【００４６】
（注７）便宜上、２つの認証要素を結合したものを示す。
より一般的な多要素認証システムは、３つ以上の要素を含むことが可能であるというこ

とが当業者には容易に理解されよう。
（注８）第１のサブプロセスおよび第２のサブプロセスは、ほぼ同時に実行されることもできるし、任意の順序で実行されることもできる。
【００４７】
Ｆ．例示のアプリケーション環境における認証の結合
１．プロセスフローの例示
図５は、バイオメトリック認証およびＯＴＰ認証の双方用の音声入力を必要とする例示のアプリケーション環境の状況における図４の例示の２要素認証プロセスを示している。
この例示のプロセスは、ある特殊化された状況でさらに説明される。
この特殊化された状況では、ユーザは、第１の通信チャネルを介して第１の認証要素を提供し、第２の通信チャネルを介して第２の認証要素の入力の指示を受け、かつ、第１の通信チャネルを介して第２の認証要素を提供する（注９）。
【００４８】
ユーザは、ポータルサブシステム２００に接続して、アプリケーションサーバ１７０へのアクセスを要求する（ステップ５０２）。
例えば、ユーザは、自身の会社の社員システムにアクセス（または自身の銀行の預金口座システムにアクセス）して、自身の最新の給与の直接振り込み状態へのアクセスを要求する従業員（または銀行の顧客）とすることができる。
【００４９】
ポータルは、（ａ）予備的なユーザの識別、（ｂ）第１の要素（例えばバイオメトリック）認証、および（ｃ）第２の要素（例えば、安全なパスコードまたはＯＴＰ）認証、のための情報を求める（ステップ５０４）。
例えば、（ａ）ポータルは、ユーザが発話した通りの主張されたユーザのアイデンティティ（例えば、従業員ＩＤ）を取得することができ、（ｂ）ポータルは、ユーザがポータルに発話すると、音声サンプルを取得することができ、（ｃ）ポータルは、ユーザが保持するトークンからユーザがＯＴＰを読み上げると、そのＯＴＰを取得することができる。
【００５０】
（ｂ）の音声サンプルは、（ａ）のユーザの自己識別情報から、（ｃ）のＯＴＰのユーザの読み上げから、または他の或るプロトコルに従って、取得されうる。
例えば、ユーザは、事前にプログラミングされた文字列を想起するように要求されたり、ポータルからの可変のチャレンジ（例えば、今日の日付は何日か？）に応答するように要求されうる（注１０）。
【００５１】
ステップ５０６のように、ポータルは、主張されたアイデンティティの存在（および、場合によっては、あらゆる関連付けられたアクセス権）を（企業の）社員アプリケーションまたは（銀行の）顧客アプリケーションにおいてチェックすることによって、主張されたアイデンティティが認証されることを確認することができる。
任意選択で、このアプリケーションは、それ自身の認証プロセス（例えば、母親の旧姓、社会保障番号、または他の既知のチャレンジ－応答プロトコルの読み上げ）を含み、主張されたユーザのアイデンティティを予備的に検証することができる。
この予備的な検証は、ユーザがＯＴＰを提供する前後のいずれでも行われうる。
【００５２】
ユーザが読み上げたＯＴＰは、発話認識モジュール（例えば、図２の要素２４０）に転送される（ステップ５０８）。
【００５３】
確認サブシステム１３０（例えば、トークン認証サーバ）（図１参照）は、ＯＴＰを計算し、ユーザのトークン上にあるものと比較する（ステップ５１０）（注１１）。
（多くの一般的なＯＴＰの実施態様のように）ＯＴＰの計算が、ユーザのトークンデバイスのものと一致するシードすなわち「トークンシークレット（token secret）」を必要とする場合、そのトークンシークレットは、データベースから安全に検索される（ステッ

プ５１２）。
次いで、トークン認証サーバは、ユーザが読み上げたＯＴＰを、生成したＯＴＰと比較し、一致するかどうかを報告する。
【００５４】
また、ユーザが読み上げたＯＴＰ（または、ＯＴＰが音声サンプルとして使用されない場合には他の音声サンプル）は、話者照合モジュール（例えば、図２の要素３２０）にも転送される。
話者照合モジュール３２０は、適当な音声テンプレートを検索して、その音声テンプレートを音声サンプルと比較し、一致するのか（それとも一致しないのか）を報告する（ステップ５１４）。
音声テンプレートは、当該音声テンプレートへのインデックスとしてユーザＩＤを使用して、例えば、音声テンプレートデータベースから検索されることができる（ステップ５１６）。
【００５５】
ＯＴＰおよびユーザの音声の双方が検証され、ユーザが認証されたと確定されると、「成功」が、アプリケーションサーバ１７０に（例えば、音声ポータル２００を介して）報告され、ユーザのアクセスが許可される（この例では、ユーザの給与情報を見ることが許可される）（ステップ５１８）。
ＯＴＰまたはユーザの音声のいずれかが認証されないと、ユーザは拒否され、任意選択で、再試行するように指示される（例えば、アクセスが得られるか、プロセスがタイムアウトするか、または、失敗が多すぎる結果、プロセスが停止されるまで）。
アクセスが許可されようとされまいと、ユーザのアクセスの試みは、任意選択で、監査目的で記録されることができる。
【００５６】
（注９）２つのチャネルが同じタイプのものである場合（例えば、共に音声ベース）、それら２つのチャネルが、たとえ互いに対して帯域外となる場合（例えば、一方が陸上回線であり、他方が携帯電話である場合）であっても、上述した他方の例示の環境（異なる通信チャネルを介した異なる認証要素）の特別な場合に対して、図示したプロセスを適合させる方法は、当業者に容易に理解されよう。
（注１０）ユーザがＯＴＰを読み上げることから音声サンプルを取得できるということは、ユーザが、第２の認証要素（例えばＯＴＰ）の入力指示を受ける前に、第１の認証要素（例えば音声サンプル）を提供する必要がなかったことを示す。
例えば、双方の認証要素が同時に提供される場合、指示は、ユーザが双方の認証要素を提供する前に行われるべきである。
実際に、第１の認証要素は、第２の認証要素に先行する必要はない。
したがって、ラベル「第１」および「第２」は、時間的な関係を必要とするものではなく、２つの認証要素を区別するだめだけに使用されるものであると、ユーザは理解すべきである。
実際には、本明細書で示すように、２つの認証要素は、共通の伝達手段を介して（例えば、単一の発話入力の一部として）提供されることもできる。
（注１１）この例示のプロセスフローは、ユーザがＯＴＰジェネレータを有する状況を示している。
ユーザが返信するＯＴＰが、システムがユーザに事前に送信したＯＴＰである場合の実施態様に、この例示のプロセスフローを適合させる方法は、当業者に容易に理解されよう。
【００５７】
２．システムの実施態様の例示
図６は、話者照合（例えば、第１の要素認証の一タイプ）にＯＴＰ認証（例えば、第２の要素認証の一タイプ）を加えたものに基づく２要素認証の別のより詳細な例示の実施態様を示している。

さらに、全体の認証プロセスは、アプリケーションサーバ１７０から抽出され、複数のアプリケーション間で共有されることもできる。

【００５８】

エンロールメントプロセス中、ユーザの音声テンプレートが取得されて、そのユーザのユーザＩＤの下で記憶される。

また、ユーザは、トークンカード（ＯＴＰジェネレータ）を与えられ、このトークンカードも、そのユーザのユーザＩＤの下でエンロールメントされる。

【００５９】

セッションを開始するために、ユーザは、自身の電話６１０からシステムに電話をかける。

音声ポータルサブシステム２００は、ユーザに挨拶し、ユーザのアプリケーション選択を求める。

ユーザは、匿名の電話主（この時点では、電話主は特定されていない）用のデフォルトホームページ上で利用可能な選択メニューごとに自身のアプリケーション選択を指定する。

ユーザの選択が、認証されたアイデンティティを必要とするものである場合、システムは、ユーザのアイデンティティを求める。

ユーザの選択が、アイデンティティの高セキュリティ認証を必要とするものである場合、システムは、上述したような強力な２要素認証を実行する。

音声ポータルサブシステムの要素は、図６に示すように、電話システムインタフェース２２０、発話認識モジュール２４０、ＴＴＳモジュール２５０、プッシュホンモジュール２６０およびオーディオＩ／Ｏモジュール２７０である。

ＶｏｉｃｅＸＭＬインタープリタ／プロセッサ２８０は、上記モジュールを制御し、さらに、ポータルホームページサーバ１８０とのインタフェース、および、このポータルホームページサーバ１８０を通じた下流側のアプリケーションサーバ１７０とのインタフェースとなる（注１２）。

【００６０】

この例示の実施の形態では、主張されたユーザのアイデンティティが確定されると、ポータルホームページサーバ１８０は、ポリシーサーバ６５０に記録されたユーザの個人ホームページのセキュリティ（すなわち、アクセス）要件をチェックし、（例えば、図５のステップ５０６で述べた技法を使用して）必要なあらゆる予備的な認証／認可を行い、次いで、利用可能なアプリケーションのメニューをユーザに発話したり、表示したり、または、それ以外にアクセス可能にする。

純粋な音声ベースのユーザアクセス構成では、このメニューは、音声ポータルサブシステム２００のＴＴＳモジュール２５０によって、ユーザに発話されることができる。

ユーザが音声およびウェブアクセスを組み合わせたものを有する場合には、メニューは、ブラウザ６２０を介してユーザに表示されることができる。

【００６１】

次に図６を参照して、この例示の実施態様では、Netegrity社のＳｉｔｅＭｉｎｄｅｒ製品スイート形式のミドルウェアが、さまざまなアプリケーションからポリシーおよび認証を抽出するのに使用される。

この抽出によって、マルチアプリケーション（例えば、株式取引、請求書支払い等）システムは、独自のユーザディレクトリおよび個々の各アプリケーションへのアクセス制御システムを構築するのではなく、統合された１組のセキュリティサービスおよび管理サービスを共有することが可能になる。

その結果、システムは、「シングルサインオン」プロセスを使用して多くのアプリケーションに対応することができる（注１３）。

【００６２】

各アプリケーションサーバ１７０は、プラグインモジュール形式のＳｉｔｅＭｉｎｄｅｒウェブエージェント６４０を有し、このウェブエージェント６４０は、すべてのアプリ

ケーションサーバにサービスを提供する共有ポリシーサーバ６５０と通信する。
各サーバのウェブエージェント６４０は、そのサーバ上のすべてのＨＴＴＰ（ＨＴＭＬ、ＸＭＬ等）トラフィックを仲介する（注１４）。
ウェブエージェント６４０は、ユーザのリソース（例えば、株式取引アプリケーション）要求を受信し、そのリソースが高信頼認証を必要とするものであることをポリシーストアから決定する。
ポリシーサーバ６５０は、ユーザのトークンデバイス上に表示されたワンタイムパスコードの発話をユーザに指示するように、ウェブエージェント６４０に指令する。
第２のチャネルも電話回線である場合、この指示は、ＴＴＳモジュール２５０を起動するために、ＶｏｉｃｅＸＭＬインタープリタ／プロセッサ２８０を通るＶｏｉｃｅＸＭＬコールを介して実行されうる。
第２のチャネルがユーザのブラウザである場合、この指示は、適当な手段によって実行されることになる。

【００６３】

次いで、ウェブエージェント６４０は、ＶｏｉｃｅＸＭＬ要求を音声ポータルサブシステム２００に書き込み、要求されたＯＴＰを受信する。
次いで、音声ポータルサブシステム２００は、ＯＴＰをウェブエージェント６４０に返信し、ウェブエージェント６４０は、ポリシーサーバ６５０にＯＴＰを渡す。
システム構成に応じて、ＯＴＰは、発話認識モジュール２４０内でオーディオからテキストに変換されて、その形式で転送されることもできるし、オーディオ形式で発話認識モジュール２４０を迂回して転送されることもできる。
前者は、ＯＴＰが比較的単純であり、かつ／または、発音ミスを起こしにくい場合に、ユニバーサル発話認識プロセス（例えば、発話認識モジュール２４０）で行われることがある。

【００６４】

しかしながら、図６に示すように、多くの場合、精度を増すために、話者に応じた発話認識プロセスを使用することが好ましい。
その場合、ポリシーサーバ６５０は、ユーザＩＤおよびＯＴＰを話者照合サブシステム３００に転送することができる。
図３に関連して説明したように、話者照合サブシステム３００は、エンロールメントされたユーザの音声テンプレートをデータベース（例えば、エンタープライズディレクトリ）１５０から検索し、話者認識モジュール３１０は、そのテンプレートを使用して、オーディオをテキストに変換する。
いずれの場合も、次に、パスコードが、テキスト形式でポリシーサーバ６５０に返信され、ポリシーサーバ６５０は、そのパスコードをパスコード確認サブシステム１３０に転送する。

【００６５】

ポリシーサーバ６５０は、話者照合サブシステム３００に頼らないで、ユーザＩＤおよびＯＴＰ（テキスト形式で受信された場合）をパスコード認証検証サーバ１３０に転送することができる。
あるいは、必要に応じて、ポリシーサーバ６５０は、すべての音声ポータルサブシステム２００および／または話者照合サブシステム３００の一部を利用して、必要なあらゆる発話－テキスト変換を行うこともできる。

【００６６】

確認サブシステム１３０は、（Ｆ．１節で前述したように）アクセスを承認すると、ユーザが認証を受けて株式取引を完了できることをポリシーサーバ６５０に通知する。
確認サブシステム１３０またはポリシーサーバ６５０は、暗号化された認証クッキーを作成して、この認証クッキーをポータルホームページサーバ１８０に戻すこともできる（注１５）。

【００６７】

認証クッキーは、（例えば、他のアプリケーションによる）さらなる認証要求のサポートに使用されることができ、その結果、ユーザは、同じセッション中に複数のアプリケーションにアクセスする際、自身を再認証する必要はない。

例えば、ユーザは、自身の株式取引を完了した後、同様に高信頼認証を必要とする請求書支払いアプリケーションを選択することができる。

既存の認証クッキーは、請求書支払いアプリケーションの認証ポリシーを満たすために使用される。

したがって、ユーザが認証プロセスを繰り返す必要は省かれる。

セッションの終了時（すなわち、アプリケーションがそれ以上望まれていない場合）には、このクッキーは、破棄されることができる。

【００６８】

（注１２）図示した実施態様では、ポータルホームページサーバは、通信がアプリケーションサーバ１７０へ／から転送される通信チャネル１８０として機能する。

もちろん、より一般的には、ポータルホームページサーバ１８０の機能は、アプリケーションサーバ１７０の一部として実施することもできる。

（注１３）図６で説明する例示の実施態様では、認証は、ウェブエージェント６４０およびポリシーサーバ６５０を使用することによって、アプリケーションサーバから抽出される。

このような抽出が望ましくない場合、それらの要素によって実行される機能は、アプリケーションサーバ１７０に組み込まれ、そのサーバ内で実行される。

（注１４）ウェブエージェントモジュールは、ポータルホームページサーバ１８０においても同様の機能を実行する。

（注１５）あるいは、特定の構成に応じて、アプリケーションサーバ１７０に直接。

【００６９】

Ｇ．ユーザエンロールメント

通常は、認証前に、ユーザのＩＤをユーザのトークンに関連付けておく必要がある。

同様に、ユーザの音声サンプルは、話者照合中にユーザの音声テンプレートと比較されていた。

したがって、通常は、認証前にユーザの音声テンプレートを関連付けて記録しておく必要がある。

ユーザを対応する認証データに関連付ける両タイプの関連付けは、通常、エンロールメントプロセス中に行われる（もちろん、実際には、両タイプの認証データを扱う合成プロセスを含むこともできるし、適当にプロセスを分離することもできる）。

このように、安全なエンロールメントは、詐称者による認可されていないアクセスの可能性を低減するのに重要な役割を果たす。

【００７０】

図７は、上記に示した例の音声テンプレート部の例示のエンロールメントプロセスを示している。

この例示のエンロールメントプロセスは、登録フェーズおよびトレーニングフェーズを含む。

【００７１】

図７の例示の登録ステップにおいて、ユーザは、エンロールメントセッションで使用されるユーザＩＤおよび／または他の認証素材（複数可）（例えば、登録パスコード等）の提供を受ける（ステップ７０２）。

既存のセキュリティ関係が既に確立されている場合には、登録素材は、オンラインプロセス（電子メール等）を介して提供されることができる。

そうでない場合には、登録は、ユーザが個人的に認証を受けることができる環境で行われることが多い。

例えば、エンロールメントが、ユーザの雇用者によって行われる場合、既知の従業員の簡単な対面認証で十分とすることができる。

あるいは、エンロールメントが第３者機関に外部委託される場合、ユーザは、適当な書式（複数可）の識別情報（例えば、パスポート、運転免許証等）の提示を要求されることがある。

【００７２】

ユーザは、次に、登録期間中に提供されたユーザＩＤおよび／または他の素材（複数可）を使用して、自身のアイデンティティを検証することができ（ステップ７０４）、音声テンプレートの作成に進むことができる（ステップ７０８）。

【００７３】

通常、ユーザは、自身の一意の音声特性を認識するようにシステムを「トレーニング」するために、一連のフレーズをシステムに繰り返すように指示される（ステップ７０６）。

【００７４】

ユーザのアイデンティティに関連付けられた音声テンプレートファイルは、ユーザの繰り返したフレーズに基づいて作成される（ステップ７０８）。

例えば、ユーザの音声は、発話サンプリング／雑音フィルタリングアルゴリズムによって処理されることができ、このアルゴリズムは、音声を、音声テンプレートファイルに記憶される音素に分解する。

【００７５】

音声テンプレートファイルは、ユーザのアイデンティティを認証するために、認証セッション中に、後に使用するためにデータベースに記憶される（ステップ７１０）。

【００７６】

Ｈ．結論

上記すべての説明において、さまざまなサブシステム、モジュール、データベース、チャネルおよび他のコンポーネントは、単なる例示にすぎない。

一般に、説明した機能は、上記に示した特定のコンポーネントおよびデータフローを使用して実施することもできるし、所望のシステム構成に適したさらに他のコンポーネントおよびデータフローを使用しても実施することができる。

例えば、システムは、２つの認証要素の観点から説明されているが、さらに高度なセキュリティは、３つまたは４つ以上の認証要素を使用することによって達成することができる。

さらに、認証要素は、多くの場合、特定の種類の入力（例えば音声）によって提供されるものとして説明されていたが、実際には、認証要素は、実質的にあらゆる種類の通信チャネルを介して提供されることができる。

また、ラベル「第１」および「第２」は、任意の特定の順序付けまたは階層を示すためのものと意図されないことにも留意すべきである。

したがって、「第１」と記載された技法またはケースは、「第２」と記載された技法またはケースに代えて使用されることができ、その逆も可能である。

また、さまざまなコンポーネントは、ハードウェア、ソフトウェア、またはそれらの組み合わせで実施できることも、当業者には容易に理解されよう。

このように、上記例は、特定の例示の実施の形態を示しており、他の実施の形態、変形および変更は、これらの例示の実施の形態から、当業者には明らかである。

したがって、本発明は、上述した特定の実施の形態に限定されるべきではなく、特許請求項によって規定される。

【図面の簡単な説明】

【００７７】

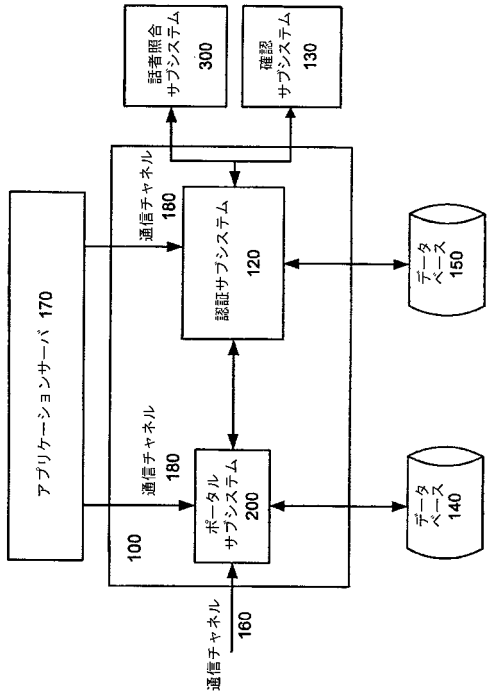
【図１】アプリケーションサーバに接続されて、当該アプリケーションサーバ用のユーザ認証を提供する例示の多要素認証システムの概略図である。

【図２】図１に示す例示の多要素認証システムの例示のポータルサブシステムを示す図である。

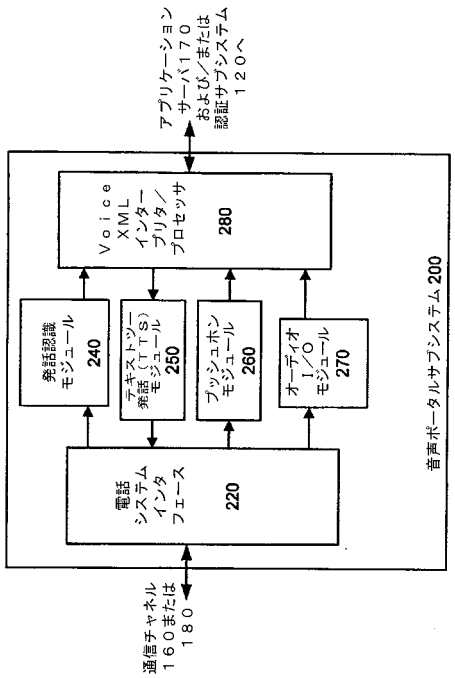
【図３】図１に示す例示の多要素認証システムの例示の話者照合サブシステムを示す図で

ある。
【図４】発話されたＯＴＰを使用して話者照合およびトークン認証の双方を行う例示の２要素認証プロセスのフローチャートである。
【図５】例示のアプリケーション環境の状況における図４の２要素認証プロセスを示す図である。
【図６】複数のアプリケーション間で認証を共有でき、話者照合にＯＴＰ認証（音声で提供されるものまたはウェブベースのもののいずれか）を加えたものに基づく２要素認証のより詳細な例示の実施態様を示す図である。
【図７】例示のユーザエンロールメント／トレーニングプロセスを示す図である。
【符号の説明】
【００７８】
１２０・・・認証サブシステム
１３０・・・確認サブシステム
１４０、１５０・・・データベース
１６０、１８０・・・通信チャネル
１７０・・・アプリケーションサーバ
２００・・・ポータルサブシステム
２２０・・・電話システムインタフェース
２４０・・・発話認識モジュール
２５０・・・テキストツー発話（ＴＴＳ）モジュール
２６０・・・プッシュホンモジュール
２７０・・・オーディオＩ／Ｏモジュール
２８０・・・ＶｏｉｃｅＸＭＬインタープリタ／プロセッサ
３００・・・話者照合サブシステム
３１０・・・発話認識モジュール
３２０・・・話者照合モジュール
３３０・・・テンプレート適合モジュール
６１０・・・ユーザの電話
６２０・・・ＰＣ上のユーザブラウザ
６３０・・・ホームページ、アプリケーション（ＨＴＭＬ＋ＶｏｉｃｅＸＭＬ）
６４０・・・ＳｉｔｅＭｉｎｄｅｒ（登録商標）ウェブエージェントモジュール
６５０・・・ＳｉｔｅＭｉｎｄｅｒ（登録商標）ポリシーサーバ

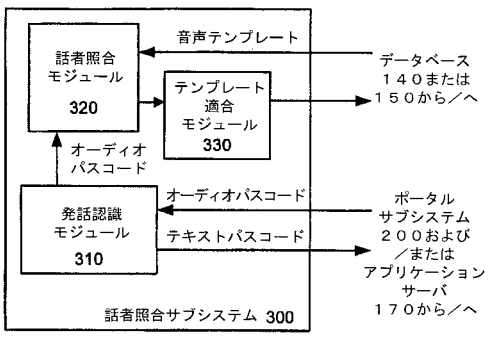
【図１】


話者照合サブシステム 300
確認サブシステム 130
通信チャネル 180
認証サブシステム 120
データベース 150
アプリケーションサーバ 170
通信チャネル 180
ポータルサブシステム 200
データベース 140
100
通信チャネル 160

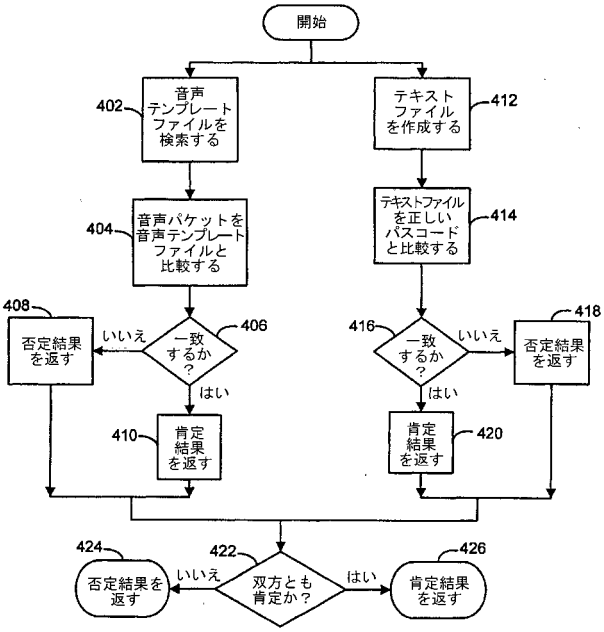
【図２】


アプリケーションサーバ170および/または認証サブシステム120へ
VoiceXMLインタープリタ/プロセッサ 280
発話認識モジュール 240
テキストツー発話(TTS)モジュール 250
プッシュトゥトークモジュール 260
オーディオI/Oモジュール 270
電話システムインタフェース 220
音声ポータルサブシステム 200
通信チャネル160または180

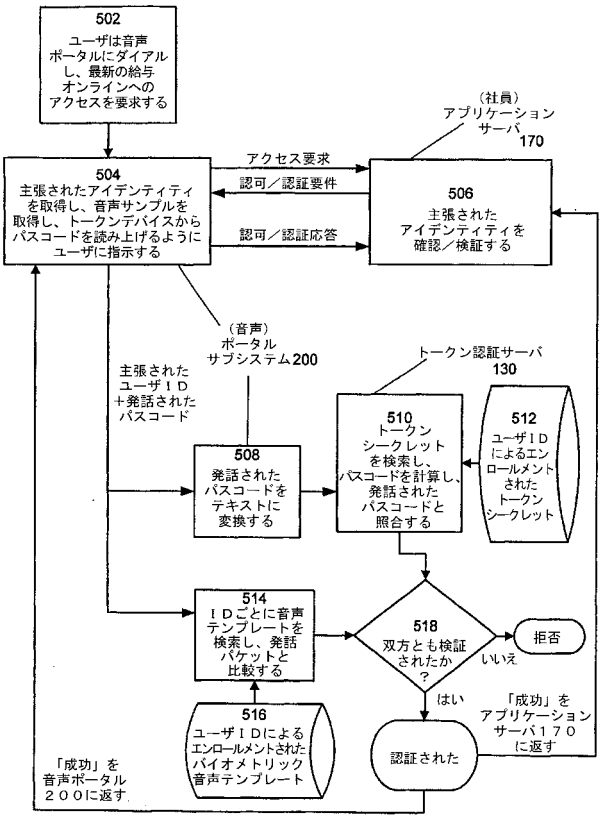
【図３】


話者照合モジュール 320
音声テンプレート
データベース140または150から/へ
テンプレート適合モジュール 330
オーディオパスコード
発話認識モジュール 310
オーディオパスコード
テキストパスコード
ポータルサブシステム200および/またはアプリケーションサーバ170から/へ
話者照合サブシステム 300

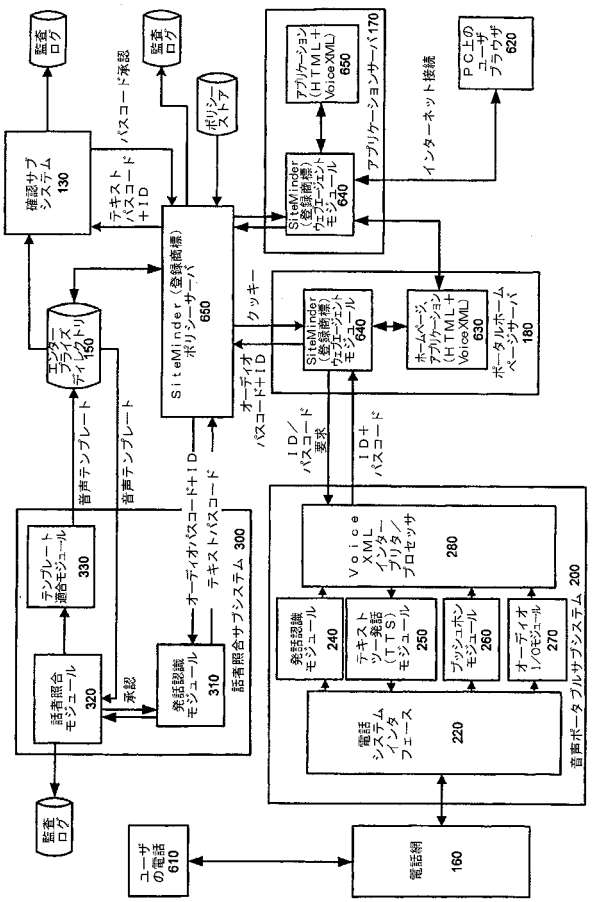
【図４】


開始
402 音声テンプレートファイルを検索する
404 音声パケットを音声テンプレートファイルと比較する
406 一致するか?
いいえ
はい
408 否定結果を返す
410 肯定結果を返す
412 テキストファイルを作成する
414 テキストファイルを正しいパスコードと比較する
416 一致するか?
いいえ
はい
418 否定結果を返す
420 肯定結果を返す
422 双方とも肯定か?
いいえ
はい
424 否定結果を返す
426 肯定結果を返す

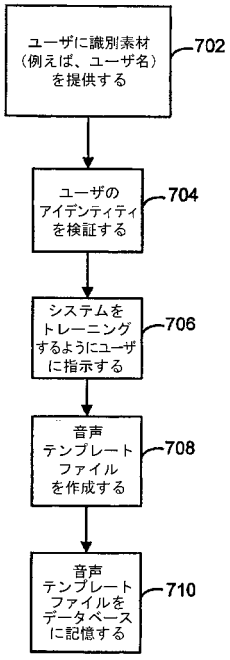
【図５】


502
ユーザは音声ポータルにダイアルし、最新の給与オンラインへのアクセスを要求する
（社員）アプリケーションサーバ170
504
主張されたアイデンティティを取得し、音声サンプルを取得し、トークンデバイスからパスコードを読み上げるようにユーザに指示する
アクセス要求
認可／認証要件
認可／認証応答
506
主張されたアイデンティティを確認／検証する
（音声）ポータルサブシステム200
主張されたユーザＩＤ＋発話されたパスコード
トークン認証サーバ130
508
発話されたパスコードをテキストに変換する
510
トークンシークレットを検索し、パスコードを計算し、発話されたパスコードと照合する
512
ユーザＩＤによるエンロールメントされたトークンシークレット
514
ＩＤごとに音声テンプレートを検索し、発話パケットと比較する
518
双方とも検証されたか？
いいえ
拒否
はい
「成功」をアプリケーションサーバ１７０に返す
516
ユーザＩＤによるエンロールメントされたバイオメトリック音声テンプレート
認証された
「成功」を音声ポータル２００に返す

【図６】


監査ログ
確認サブシステム130
テキストパスコード＋ＩＤ
パスコード承認
監査ログ
ポリシーストア
アプリケーション（ＨＴＭＬ＋VoiceXML）650
SiteMinder（登録機構）ウェブエージェントモジュール640
アプリケーションサーバ170
インターネット接続
ＰＣ上のユーザブラウザ620
エンタープライズディレクトリ150
SiteMinder（登録機構）ポリシーサーバ660
クッキー
SiteMinder（登録機構）ウェブエージェントモジュール640
ホームページアプリケーション（ＨＴＭＬ＋VoiceXML）630
ポータルホームページサーバ180
音声テンプレート
音声テンプレート
オーディオパスコード＋ＩＤ
ＩＤ／パスコード要求
ＩＤ＋パスコード
テンプレート適合モジュール330
オーディオパスコード＋ＩＤ
テキストパスコード
話者照合サブシステム300
VoiceXMLインタープリタ／プロセッサ280
発話認識モジュール240
テキストツースピーチ（ＴＴＳ）モジュール250
プッシュボンモジュール260
オーディオＩ／Ｏモジュール270
話者照合モジュール320
承認
発話認識モジュール310
電話システムインタフェース220
音声ポータブルサブシステム200
監査ログ
ユーザの電話610
電話網160

【図７】


ユーザに識別素材（例えば、ユーザ名）を提供する
702
ユーザのアイデンティティを検証する
704
システムをトレーニングするようにユーザに指示する
706
音声テンプレートファイルを作成する
708
音声テンプレートファイルをデータベースに記憶する
710

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/05880

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00 G10L17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F G10L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 795 264 A (LENOIR OLIVIER) 22 December 2000 (2000-12-22) abstract; figure 1 page 1, line 1-29 page 2, line 21 -page 3, line 15 page 4, line 12-31 page 5, line 19 -page 6, line 6	1,2,6,9, 10,18, 19,23,24
Y	page 8, line 17 -page 9, line 30	3-5,7,8, 13,14, 20,25

Y	WO 01 80525 A (SUN MICROSYSTEMS INC) 25 October 2001 (2001-10-25) abstract; figure 1 page 1, line 22 -page 2, line 20 page 3, line 29 -page 4, line 25 page 9, line 16-22	13,14

	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 July 2003	18. 09. 03

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lopez Moncl s, I

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/05880

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 23062 A (NETIX INC T) 28 May 1998 (1998-05-28) abstract page 3, line 24 -page 5, line 3 page 7, line 15 -page 10, line 10	3,4,7,8, 20,25
Y	WO 98 16906 A (KOMMER ROBERT VAN ;TELECOM PTT (CH); MOSER THOMAS (CH)) 23 April 1998 (1998-04-23) abstract page 6, line 1-30 page 8, line 23 -page 9, line 13	5

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/05880

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-14, 16-20, 22-25

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/US 03/05880

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-14, 16-20, 22-25

   A method for authenticating a user using an out-of-band communication channel

2. Claims: 15, 21, 26

   A method for authenticating a user using his voice

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/05880

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2795264 A	22-12-2000	FR 2795264 A1	22-12-2000
		AU 6287300 A	02-01-2001
		CA 2377425 A1	21-12-2000
		EP 1190549 A2	27-03-2002
		WO 0078009 A2	21-12-2000
WO 0180525 A	25-10-2001	AU 4529201 A	30-10-2001
		WO 0180525 A1	25-10-2001
WO 9823062 A	28-05-1998	AU 7304798 A	10-06-1998
		CN 1244984 A	16-02-2000
		EP 0938793 A1	01-09-1999
		JP 2001505688 T	24-04-2001
		WO 9823062 A1	28-05-1998
		US 2003046083 A1	06-03-2003
WO 9816906 A	23-04-1998	WO 9816906 A1	23-04-1998
		AT 227868 T	15-11-2002
		AU 7293096 A	11-05-1998
		CZ 9901257 A3	11-08-1999
		DE 69624848 D1	19-12-2002
		EP 0932885 A1	04-08-1999
		JP 2001503156 T	06-03-2001
		US 6556127 B1	29-04-2003

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

Ｆターム(参考) 5B085 AE03 AE27
5J104 AA03 AA07 KA01 KA04 KA18 NA05 NA38 PA07