

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6514218号

(P6514218)

(45) 発行日 令和1年5月15日 (2019.5.15)

(24) 登録日 平成31年4月19日 (2019.4.19)

(51) Int.Cl.

F I

G 0 6 F 21/31 (2013.01)

G 0 6 F 21/31

請求項の数 15 (全 23 頁)

(21) 出願番号	特願2016-546084 (P2016-546084)	(73) 特許権者	510330264
(86) (22) 出願日	平成27年1月27日 (2015.1.27)		アリババ・グループ・ホールディング・リミテッド
(65) 公表番号	特表2017-505484 (P2017-505484A)		ALIBABA GROUP HOLDING LIMITED
(43) 公表日	平成29年2月16日 (2017.2.16)		英国領、ケイマン諸島、グランド・ケイマン、ジョージ・タウン、ワン・キャピタル・プレイス、フォース・フロア、ピー・オー・ボックス 847
(86) 国際出願番号	PCT/US2015/013058		
(87) 国際公開番号	W02015/116577		
(87) 国際公開日	平成27年8月6日 (2015.8.6)	(74) 代理人	110001243
審査請求日	平成30年1月17日 (2018.1.17)		特許業務法人 谷・阿部特許事務所
(31) 優先権主張番号	201410040993.5		
(32) 優先日	平成26年1月28日 (2014.1.28)		
(33) 優先権主張国	中国 (CN)		

最終頁に続く

(54) 【発明の名称】 社会関係データを用いたクライアント認証

(57) 【特許請求の範囲】

【請求項 1】

コンピュータ装置で実施されるクライアント認証方法であって、
ユーザアカウントに対応する本人認証の要求をクライアント装置から受信することと、
クライアントの社会関係データと、前記ユーザアカウントの記憶された社会関係データとの照合結果として、社会関係類似性を取得することと、
前記類似性が予め設定した通過条件を満たすか否かを判定し、満たす場合、前記クライアントが前記本人認証を通過するのを可能にすることと、
を含み、
前記社会関係データは、電話番号、通信アカウント番号、アドレス帳、または立て替え払い記録のいずれかを含み、
前記クライアントの社会関係データと前記ユーザアカウントの記憶された社会関係データとの照合結果として前記類似性を取得することは、
前記クライアントの前記社会関係データを前記クライアント装置から受信することと、
前記クライアントの前記社会関係データと前記ユーザアカウントの前記記憶された社会関係データとを照合することによって前記類似性を計算することと、
を含む、方法。

【請求項 2】

前記ユーザアカウントの前記記憶された社会関係データは、
収集したデータを分析して、前記ユーザアカウントに関連する社会関係データを抽出す

10

20

ることと、

前記ユーザアカウントに関連する前記抽出した社会関係データを記憶することと、
によって、取得される、請求項1に記載の方法。

【請求項3】

前記社会関係類似性を取得することは、

前記ユーザアカウントの前記記憶された社会関係データを前記クライアント装置に送信することと、

前記クライアントの前記社会関係データと、前記ユーザアカウントの前記記憶された社会関係データとの前記照合結果を、前記クライアント装置から受信することと、

を含む、請求項1に記載の方法。

10

【請求項4】

前記類似性が予め設定したアラート条件を満たすか否かを判定し、満たす場合、本人認証を拒絶して、アラートアクションを取ることをさらに含む、

請求項1に記載の方法。

【請求項5】

前記類似性は、一致数及び／または一致レベルを含み、前記一致数は、前記ユーザアカウントの前記記憶された社会関係データと前記クライアントの前記社会関係データとの間で一致することが分かった項目の総数として定義され、前記一致レベルは、前記一致数と、前記記憶された社会関係データで発見された項目の総数との比率として定義される、請求項1に記載の方法。

20

【請求項6】

前記類似性が予め設定した通過条件を満たすか否かを判定することは、

前記一致数及び／または前記一致レベルが、それぞれ、前記一致数及び／または前記一致レベルの閾値より大きいかなんかを判定することを含む、

請求項5に記載の方法。

【請求項7】

前記類似性が予め設定したアラート条件を満たすか否かを判定し、満たす場合、本人認証を拒絶して、アラートアクションを取ることをさらに含む方法であって、前記予め設定したアラート条件は、前記一致数及び／または前記一致レベルが、それぞれ、前記一致数及び／または前記一致レベルの閾値より小さいことを含む、

30

請求項5に記載の方法。

【請求項8】

本人認証装置であって、プロセッサと、コンピュータ可読メモリ及び記憶媒体と、I/O装置と、を有するコンピュータ装置を備え、前記コンピュータ装置は、機能ユニットを有するようにプログラムされ、前記機能ユニットは、

ユーザアカウントに対応する本人認証の要求をクライアント装置から受信する認証要求受信ユニットと、

クライアントの社会関係データと、前記ユーザアカウントの記憶された社会関係データとの照合結果として、類似性を取得する照合結果取得ユニットと、

前記類似性が予め設定した通過条件を満たすか否かを判定し、満たす場合、前記クライアントが本人認証を通過できるようにする通過判定ユニットと、

40

を備え、

前記社会関係データは、電話番号、通信アカウント番号、アドレス帳、または立て替え払い記録のいずれかを含み、

前記照合結果取得ユニットは、

前記クライアントの前記社会関係データを前記クライアント装置から受信する社会関係データ受信サブユニットと、

前記クライアントの前記社会関係データと前記ユーザアカウントの前記記憶された社会関係データを照合することによって、前記類似性を計算する照合結果計算ユニットと、

を備える、装置。

50

【請求項 9】

前記ユーザアカウントの前記社会関係データを取得及び記憶する社会関係データ生成ユニットをさらに備え、前記社会関係データ生成ユニットは、

取得したデータを分析して、前記ユーザアカウントに関連する社会関係データを抽出する分析及び抽出サブユニットと、

前記ユーザアカウントに関連する前記抽出した社会関係データを記憶する記憶ユニットと、をさらに備え、前記記憶された社会関係データは、前記ユーザアカウントの前記記憶された社会関係データを構成する、請求項 8 に記載の装置。

【請求項 10】

前記照合結果取得ユニットは、

前記ユーザアカウントの前記記憶された社会関係データを前記クライアント装置に送信する社会関係データ送信サブユニットと、

前記クライアントの前記社会関係データと、前記ユーザアカウントの前記記憶された社会関係データとの前記照合結果を前記クライアント装置から受信する照合結果受信ユニットと、

を備える、請求項 8 に記載の装置。

【請求項 11】

前記類似性が予め設定したアラート条件を満たすか否かを判定し、満たす場合、前記本人認証を拒絶し、アラートアクションを取るアラート判定ユニット

をさらに備える、請求項 8 に記載の装置。

【請求項 12】

クライアント装置で実施されるクライアント認証方法であって、

ユーザアカウントに対応する本人認証の要求をサーバに送信することと、

クライアントの認証情報を前記サーバに送信して、前記クライアントの社会関係データに基づいて、前記サーバが前記クライアントを認証できるようにすることと、

前記クライアントが前記本人認証を通過したか否かの返事を前記サーバから受信することと、

を含み、

前記社会関係データは、電話番号、通信アカウント番号、アドレス帳、または立て替え払い記録のいずれかを含み、

前記クライアントの情報を前記サーバに送信することは、

前記ユーザアカウントの社会関係データを前記サーバから受信することと、

前記クライアントの社会関係データと、前記ユーザアカウントの前記社会関係データとの照合結果として類似性を計算することと、

前記照合結果の前記類似性を前記サーバに送信することと、

を含む、方法。

【請求項 13】

前記クライアントの前記社会関係データは、前記クライアント装置にローカルに記憶される、請求項 12 に記載の方法。

【請求項 14】

本人認証装置であって、プロセッサと、コンピュータ可読メモリ及び記憶媒体と、I/O 装置とを有するコンピュータ装置を備え、前記コンピュータ装置は、機能ユニットを有するようにプログラムされ、前記機能ユニットは、

クライアントの本人認証の要求をサーバに送信する認証要求送信ユニットと、

前記クライアントの認証情報を前記サーバに送信して、前記クライアントの社会関係データと、前記クライアントに関連するユーザアカウントの記憶された社会関係データとに基づいて、前記サーバが前記クライアントを認証できるようにする認証情報送信ユニットと、

前記クライアントが前記本人認証を通過したか否かの返事を前記サーバから受信する認証結果受信ユニットと、

10

20

30

40

50

を備え、
前記社会関係データは、電話番号、通信アカウント番号、アドレス帳、または立て替え
払い記録のいずれかを含み、
前記認証情報送信ユニットは、
前記ユーザアカウントの前記記憶された社会関係データを前記サーバから受信する社会
関係データ受信ユニットと、
前記クライアントの前記社会関係データと前記ユーザアカウントの前記社会関係データ
との照合結果として類似性を計算する照合結果計算ユニットと、
前記照合結果の前記類似性を前記サーバに送信する照合結果送信ユニットと、
を備える、装置。

10

【請求項 15】

前記認証情報送信ユニットは、クライアント装置にローカルに記憶された前記クライ
アントの前記社会関係データを送信するために用いられる、請求項 14 に記載の装置。

【発明の詳細な説明】**【技術分野】****【0001】**

本出願は、本人認証の分野に関し、詳細には、社会関係データを用いてクライアントの
本人認証を行う方法、装置、及び、システムに関する。

【0002】

(関連出願の参照)

20

本出願は、2014年1月28日出願の中国特許出願番号2014/10040993
.5「社会関係データを用いたクライアント認証の方法、装置、及び、システム」の外国
優先権を主張し、参照により、その全体を本明細書に組み込むものとする。

【背景技術】**【0003】**

インターネットの発展と共に、インターネットバンキング、オンラインショッピング、
ソーシャルメディア、eコマース、インスタントメッセージ、及び、ユーザに様々なサー
ビスを提供する他のアプリケーション等、インターネットベースのアプリケーションが増
加している。ユーザ管理を容易にするために、また、セキュリティ上の理由から、イン
ターネットアプリケーションの大半は、サービス利用前にユーザにログインを要求する。
例えば、ユーザは、PCまたはモバイル機器のディスプレイ上のログイン画面で、ユーザ
アカウント名及び対応するパスワード（暗証番号としても知られる）の入力を要求され、
ユーザ本人であることをサーバが検証した後でのみ、アプリケーションが提供するサー
ビスを使用するためにアカウントに入ることを許可される。

30

【0004】

「アカウント＋パスワード」認証方法の使用は、比較的容易であるが、アカウントとパ
スワードの盗難は、ユーザに不便さと経済的損失さえ引き起こす。これを防ぐために、
モバイルインターネットサービスは、認証のためのモバイル機器の結び付け等、新しい形
式のセキュリティ手段の使用を開始した。例えば、機密性の高い操作（例えば、ア
カウントへのログイン、パスワード変更、支払、アカウント情報を見る等）のために
モバイル機器でモバイルアプリケーションの使用が許可される前に、ユーザは、ユーザ
のアプリケーションアカウントを、ユーザが使用する承認されたモバイル機器に
結び付けて、ログオンしアプリケーションアカウントを使用する必要がある。詳細
には、ユーザは、機密性の高い操作を行うために承認済みの結び付けられた
モバイル通信装置だけを使用できる。この手段を用いると、ユーザアカウントに
追加のセキュリティを提供することによって、盗まれたアカウントやパスワードの
不正使用を避けることができる。ユーザがモバイル機器を交換する場合、ア
カウントとモバイル通信装置間の結び付き関係を変更または更新する手順
を使用できる。

40

【0005】

従来の技術条件においては、上記結び付き承認プロセス及び結び付き変更プロセスは、

50

S M S ベースの検証コードのみを用いて実施される。プロセスは、典型的には、次のステップを含む。

1) ユーザが、モバイル機器上で、モバイルアプリケーションが提供するユーザインタフェースを介して、結び付き要求または結び付き変更要求を提出する。

2) モバイルアプリケーションプロバイダが、動的検証コードを含む S M S メッセージをユーザに送信する。

3) ユーザは、結び付けられたモバイルアプリケーションのユーザインタフェースの案内に従って、動的検証コードを入力する。

4) システムは、モバイルアプリケーションプロバイダによる検証が成功した後、結び付き承認を完了する。

10

【0006】

実際の適用においては、上記結び付き承認プロセスは、かなり重大なセキュリティリスクを引き起こす。第1に、窃盗者は、ユーザのアカウントとパスワードを盗んだ場合、自分のモバイル機器を用いて、最初の結び付き操作を行うことができる。第2に、現在のネットワーク環境のせいで、S M S 検証コードの漏えい問題は重大である。ユーザが、承認されたモバイル機器にアカウントを既に結び付けている場合でさえ、ユーザのアカウントとパスワードを盗んだ時点で、窃盗者は、偽って S M S の宛先を変えて、または、ユーザのモバイル機器にインストールしたトロイの木馬を用いて S M S テキストメッセージ検証コードを取得して、結びつきを変更できる。このような不正な手段を用いて、窃盗者は、既に承認されたユーザのモバイル機器を、自身のモバイル機器と取り換えることが可能である。

20

【0007】

既存の技術は、クライアント装置が実際にアカウント所有者に属するか否かを識別できず、S M S 検証コードを用いて結び付き承認を達成できるだけなので、アプリケーションプロバイダは、アカウントに結び付けるクライアント装置が実際にアカウント所有者に属するか否かを判定できない。すなわち、アプリケーションプロバイダは、このようなセキュリティリスクを排除できず、結果として、窃盗者の装置がユーザアカウントに結び付くことを可能にする場合があり、違法の機会を窃盗者に提供し、合法のユーザに不要なトラブルと経済的損失を与える。

【発明の概要】

30

【0008】

本概要は、発明を実施するための形態で以下にさらに詳しく記載する概念の一部を簡単な形で紹介するものである。本概要は、発明の内容の全ての重要な特徴や不可欠な特徴を特定するものではなく、また、そのみで、発明の内容の範囲を決定する助けとして使用するものでもない。

【0009】

開示の一態様は、クライアントの本人認証の方法である。サーバは、ユーザアカウントに対応する本人認証の要求をクライアントから受信する。方法は、クライアントの社会関係データとユーザアカウントの記憶された社会関係データとの照合結果として、社会関係類似性を計算する。当該類似性が、予め設定した通過条件を満たす場合、クライアントは、本人認証を通過できる。

40

【0010】

ユーザアカウントの記憶された社会関係データを取得するために、方法は、収集したデータを分析して、ユーザアカウントに関連する社会関係データを抽出し、ユーザアカウントに関連する抽出した社会関係データを記憶する。

【0011】

社会関係類似性を取得するために、サーバは、ユーザアカウントの記憶された社会関係データをクライアントに送信してよく、クライアントの社会関係データとユーザアカウントの記憶された社会関係データとの照合結果をクライアントから受信してよい。あるいは、サーバは、クライアントの社会関係データをクライアントから受信してよく、クライア

50

ントの社会関係データとユーザアカウントの記憶された社会関係データを照合することによって、類似性を計算してよい。

【0012】

ある実施形態においては、方法は、類似性が予め設定したアラート条件を満たすか否かも判定し、満たす場合、本人認証を拒絶し、アラートアクションを取る。

【0013】

社会関係類似性は、一致数、及び／または、一致レベルを含んでよい。ここで、一致数は、ユーザアカウントの記憶された社会関係データとクライアントの社会関係データとの間で一致することが判明した項目の総数として定義され、一致レベルは、一致数と、記憶された社会関係データの中で見つけられた項目の総数と、の比率として定義される。類似性が予め設定した通過条件を満たすか否かを判定するために、方法は、一致数及び／または一致レベルが、それぞれ、一致数及び／または一致レベルの閾値より大きいかなんかを判定してよい。方法は、類似性が予め設定したアラート条件を満たすか否かをさらに判定してよく、満たす場合、本人認証を拒絶し、アラートアクションを取る。予め設定したアラート条件は、一致数及び／または一致レベルが、それぞれ、一致数及び／または一致レベルの閾値より小さいことであってよい。

10

【0014】

社会関係データは、電話番号、QQ番号、WeChat番号、通信アカウント番号、アドレス帳、または、立て替え払い記録のいずれかを含んでよい。

【0015】

20

開示の別の態様は、本人認証装置である。当該装置は、機能ユニットを有するようにプログラムされたコンピュータ装置を有する。機能ユニットは、ユーザアカウントに対応する本人認証の要求をクライアントから受信する認証要求受信ユニットと、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果として類似性を取得する照合結果取得ユニットと、類似性が予め設定した通過条件を満たすか否かを判定して、満たす場合、クライアントが本人認証を通過できるようにする通過判定ユニットと、を含む。

【0016】

本人認証装置は、ユーザアカウントの社会関係データを取得、記憶する社会関係データ生成ユニットをさらに有してよい。社会関係データ生成ユニットは、取得したデータを分析してユーザアカウントに関連する社会関係データを抽出する分析及び抽出サブユニットと、ユーザアカウントに関連する抽出した社会関係データを記憶する記憶ユニットと、を備えてよい。

30

【0017】

照合結果取得ユニットは、ユーザアカウントの記憶された社会関係データをクライアントに送信する社会関係データ送信サブユニットと、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果をクライアントから受信する照合結果受信ユニットと、を備えてよい。

【0018】

照合結果取得ユニットは、クライアントの社会関係データをクライアントから受信する社会関係データ受信サブユニットと、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データを照合することによって類似性を計算する照合結果計算ユニットと、も備えてよい。

40

【0019】

ある実施形態においては、本人認証装置は、類似性が予め設定したアラート条件を満たすか否かを判定し、満たす場合、本人認証を拒絶し、アラートアクションを取るアラート判定ユニットを有する。

【0020】

クライアント認証方法の別の実施形態に従って、クライアントは、ユーザアカウントに対応する本人認証の要求をサーバに送信し、クライアントの認証情報をサーバに送信して

50

、クライアントの社会関係データに基づいて、サーバがクライアントを認証できるようにする。次に、クライアントは、クライアントが本人認証を通過したか否かの返事をサーバから受信する。

【0021】

クライアントの社会関係データは、クライアント装置にローカルに記憶されてよい。

【0022】

クライアントの情報をサーバに送信するために、クライアントは、最初に、ユーザアカウントの社会関係データをサーバから受信し、クライアントの社会関係データと、ユーザアカウントの社会関係データとの照合結果として、類似性を計算し、次に、照合結果の類似性をサーバに送信してよい。

10

【0023】

本人認証装置の別の実施形態によると、当該装置は、機能ユニットを有するようにプログラムされたコンピュータ装置を有する。機能ユニットは、ユーザアカウントに対応する本人認証の要求をサーバに送信する認証要求送信ユニットと、クライアントの認証情報をサーバに送信して、クライアントの社会関係データとクライアントに関連するユーザアカウントの社会関係データに基づいて、サーバがクライアントを認証するのを可能にする認証情報送信ユニットと、クライアントが本人認証を通過したか否かの返事をサーバから受信する認証結果受信ユニットと、を備える。

【0024】

認証情報送信ユニットは、クライアント装置にローカルに記憶されたクライアントの社会関係データの送信に用いられる。一実施形態においては、認証情報送信ユニットは、ユーザアカウントの社会関係データをサーバから受信する社会関係データ受信ユニットと、クライアントの社会関係データとユーザアカウントの社会関係データとの照合結果として、類似性を計算する照合結果計算ユニットと、照合結果の類似性をサーバに送信する照合結果送信ユニットと、を備える。

20

【0025】

本開示の他の特徴及び利点を以下に記載するが、それらは、一部、記載より明らかである、または、その適用の実践によって理解されよう。この適用の目的及び他の利点は、特に指摘した構造の記載、請求項、及び図面を、実現、達成することによって、得ることができる。

30

【図面の簡単な説明】

【0026】

【図1】社会関係データを用いたクライアント認証プロセスの実施例を示すブロックフロー図である。

【図2】社会関係データを用いたクライアント認証装置の実施例の機能ブロックを示す概略図である。

【図3】社会関係データを用いたクライアント認証プロセスの別の実施例を示すブロックフロー図である。

【図4】社会関係データを用いたクライアント認証装置の別の実施例の機能ブロックを示す概略図である。

40

【図5】社会関係データを用いたクライアント認証システムの実施例の機能ブロックを示す概略図である。

【発明を実施するための形態】

【0027】

本開示を、添付の図面と例示の実施形態と共に詳細に記載する。記載中、例えば、「技術」という語は、上記文脈及び本開示を通して許可される方法、装置、システム、及び／またはコンピュータ可読命令を指してよい。

【0028】

この記載において、プロセスの記載の順序は、限定として解釈してはならず、任意の数の記載のプロセスブロックを任意の順で組み合わせて、方法または代替方法を実施してよ

50

い。実施形態は、説明の便利さだけのために順次的なステップで記載されている。矛盾のない限り、本開示に記載の実施例及び実施形態と、その特性及び特徴は、自由に組み合わせてよい。さらに、本開示の技術を実践するために、実施形態に記載のあらゆるステップが必要なわけではない。

【0029】

図1は、社会関係データを用いたクライアント認証プロセスの実施例を示すブロックフロー図である。

【0030】

ブロックS101：ユーザアカウントに対応するクライアントの本人認証要求をクライアントから受信する。

10

【0031】

本明細書に記載の方法は、社会関係データを用いてクライアントの本人認証をする。「クライアント」という語は、ユーザが使用するクライアント端末またはクライアント装置を指す。方法は、クライアント端末で発見されたユーザの社会関係データと、ユーザアカウントの記憶された社会関係データとの間の類似性を、2つのデータを照合することによって決定する。クライアントが本人認証を通過するか否かは、照合の結果として決定された類似性によって判定される。本人認証は、クライアント端末が特定のユーザアカウントの所有者によって所有されるか否かという問いに答えるものである。

【0032】

この記載においては、クライアント端末は、モバイル機器、例えば、従来型の携帯電話、スマートフォン、パーソナルコンピュータ、PDA、iPad（登録商標）、及び、他の端末装置を含むが、それらに限定されない。社会関係データに基づいた本人認証の方法は、最初に装置とアカウントを結び付ける手順と、装置とアカウントの結び付きのその後の変更に限定されない適用シナリオを有するが、クライアント端末の本人認証をする必要がある多くの他のシナリオも含んでよい。例えば、セキュリティを強化するために、アプリケーションは、ユーザに、正確なアカウント名とパスワードの提供を要求するだけでなく、ユーザが使用するモバイル機器がユーザに属することを検証することを要求してよい。同様の本人認証が必要とされる任意の状況で、開示の方法を用いてよい。

20

【0033】

開示の方法を使用するために、特定のユーザアカウントに対応する本人認証の要求が、最初に、認証を行っている途中のクライアントから受信される。クライアントからの要求は、アカウント名、パスワード、及び、本人認証の要求に関連する他の情報を含んでよい。方法を実施するサーバは、要求を受信し、最初に、アカウント名とパスワードを検証する。これを行うために、サーバは、記憶されたアカウント情報内で、提供されたアカウント名に対応するアカウントを探し、識別されたアカウントのパスワード情報を取得し、パスワード情報を受信したパスワードと比較し、パスワードが一致すると、次の操作に進み、一致しないと、パスワードエラーを示す返事を返してよい。

30

【0034】

アカウント名とパスワードの検証に成功すると、プロセスは、ブロックS102に進み、社会関係データに基づいた本人認証の操作を開始する。実際には、事前に判定を行って、この追加の認証プロセスが必要か否かを決定してよい。この判定は、受信した要求がこのような認証を必要とすることを明示的に示すものを含むか否か、ユーザが行っている現在の操作が機密性の高い種類（例えば、ログオン、支払等）に属することを要求が示しているか否か、または、現在のユーザアカウントが、このような本人認証を必要とする安全レベルを有するか否か、に基づいて行われてよい。事前の判定が肯定である場合、プロセスはブロックS102に進む。

40

【0035】

ブロックS102：クライアント端末のクライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果として類似性を取得する。

【0036】

50

開示の社会関係データに基づいたクライアントの本人認証方法は、次の類似性基準を用いる。すなわち、現在のユーザアカウントの既存の記憶された社会関係データが、クライアントで発見された社会関係データと十分な類似性を有して一致する場合、クライアントは、本人認証を通過するとみなされる。すなわち、クライアント端末は、現在のアカウントの所有者であるユーザによって所有されていると考えられる。

【0037】

社会関係データは、対人社会関係を反映する任意のデータであってよく、現在のユーザアカウントと他のユーザとの社会関係の関係表によって表されてよい。社会関係データは、特定のユーザアカウントの所有者が本人であることを少なくとも間接的に反映すること
10
を特徴としてよい。開示の方法は、社会関係データのこの本人証明に関連した特性を利用して、認証を行っている途中のクライアントが、ユーザアカウントを所有するユーザに属し、従って本人認証を通過できるか否かを判定する。

【0038】

社会関係データに含まれる電話番号のリストを例に取ろう。クライアントに記憶されたアドレス帳の電話番号リストが、サーバに記憶されたユーザアカウントの電話番号に十分な類似性を持って一致することが分かると、クライアント端末はユーザアカウントの所有者に属し、従って、認証を通過できると結論付けてよい。

【0039】

サーバに記憶された社会関係データは、電話番号リストを含んでよいが、他の社会関係データ、例えば、ユーザのQQ番号リスト、ユーザのWeChat番号リスト、過去の連絡先番号リスト、及び、現在のユーザと他のユーザとの社会関係を反映し得る任意の他のデータも含んでよい。同様に、クライアント端末に記憶された社会関係データは、電話番号リストを含んでよいが、ユーザのQQ番号リスト、ユーザのWeChat番号リスト、過去の連絡先番号リスト、及び、現在のユーザと他のユーザとの社会関係を反映し得る任意の他のデータ等の、他の社会関係データも含んでよい。
20

【0040】

クライアント端末の社会関係データと、ユーザアカウントの既存の記憶された社会関係データとを照合した類似性結果を取得するために、ユーザアカウントに対応する社会関係データを最初に作成する必要がある。これは次の2ステップで行われてよい。(1) 収集したデータを分析して、ユーザアカウントに関連する社会関係データを抽出する(2) ユーザアカウントに関連する抽出した社会関係データを記憶する。以下に、それぞれ、記載する。
30

【0041】

(1) 収集したデータを分析して、ユーザアカウントに関連する社会関係データを抽出する。

【0042】

社会関係データを最初に収集する。収集したデータは、ユーザアカウント間で行われた商取引の金融記録、資金振替記録、立て替え払い記録(ユーザが他者によって行われた支払い)、通信記録、または、他のソーシャルネットワーク関係記録を含んでよい。データは、サーバシステム内の内部データから収集されてもよく、別のサーバまたはシステムの様々なアプリケーションデータから、その別のサーバまたはシステムによって開かれたポートを訪れることによって、取得されてもよい。
40

【0043】

次に、収集したデータは、分析されて、特定のユーザアカウントに関連する任意の社会関係データを抽出し、不要な情報を取り除く。このプロセスは、データクリーニングとも呼ばれる。

【0044】

データクリーニングは、データベースサービスの技術である。その名が示すように、データクリーニングは、データの汚れた部分を取り除く。情報処理技術が発展するにつれて、多くの産業及び分野で大量のデータが蓄積されるようになった。現在の世界の条件を正
50

確に反映し、日々の操作と決定を有効に支持するためにデータの正確性を維持するよう、データクリーニングが必要である。データクリーニングの1つの目的は、データに存在する矛盾を検出し、無効データや空データを排除または訂正してデータ品質を向上させることである。データクリーニングは、通常、一定の規則セットに従って、汚れたデータをきれいにする。

【0045】

別の見方をすれば、基準に合わないデータを取り除き、有用なデータを抽出するために、データクリーニングは、汚れたデータをきれいにすることに加えて、データ収束、データマイニング、及び、データフィルタリングも行う。データクリーニングは、上記目的のために、本開示で使用するとう有用である。これは、関与するデータは、様々なアプリケーションからのデータを収集したものであり得るからである。データは、異なる商取引及び異なるアプリケーションからだけではなく、異なる時間の履歴データを含み得るので、データクリーニングが必要になる。一方、開示の方法は、一定の種類のデータ（異なるアカウント間で行われた商取引の金融記録、振替記録、立て替え払い記録、通信記録、または、他のソーシャルネットワーク関係記録等）を分析するので、他の関連の無いデータは、汚れたデータとみなされ得る。他方、開示の方法は、収集されたデータから、特定のユーザアカウントに対応する社会関係データを抽出するので、特定のユーザアカウントに関連のない他のデータは、汚れたデータとみなされ得る。

10

【0046】

データクリーニングは、上記の種類の汚れたデータを取り除き、同時に、一定の論理ルールを用いて、特定のユーザアカウントと他のユーザ間の関係表を分析、抽出する。例えば、データクリーニングを通して、特定のアカウントAがアカウントBと金融取引があり、アカウントBが電話番号1を連絡先として登録している場合、電話番号1は、アカウントAと社会関係があると見なされると結論付けてよい。

20

【0047】

上記方法を用いて、アカウントAと（金融取引と通信を含む）社会関係を有する電話番号のリストを取得してよい。リストは、アカウントA／電話番号1、アカウントA／電話番号2等のように示してよい。データクリーニングを通して、特定のアカウントに接続された他の社会関係データも、アカウントA／QQ番号1、アカウントA／QQ番号2等のように示して、取得してよい。

30

【0048】

ユーザ間の電話通信、金融取引、及び、他の社会関係は、動的なことが多いので、上記データ収集及びデータクリーニングプロセスは、前のアカウント及び新しく追加されたアカウントの社会関係を含む最新の関係リストを作成するために、定期的にバックエンドで行われてよい。

【0049】

データ収集及びデータクリーニングを更新するための定期的な時間設定は、適用シナリオに応じて、実施が異なると、異なるとよい。データクリーニングによって取得された特定のユーザアカウントに関連する社会関係データは、電話番号に限られないことに注意されたい。例えば、特定のユーザアカウントに関連する社会的連絡先名のリストであってよい。これらの実施の変形形態は全て、開示の範囲内である。

40

【0050】

(2) ユーザアカウントに関連する抽出された社会関係データを記憶すること。

【0051】

データクリーニングによって取得されたユーザアカウントに関連する社会関係データは、データベース、データファイル、または、データテーブルに記憶される。記憶されたデータは、ユーザアカウントの記憶された社会関係データを構成する。本開示では、ユーザアカウントに対応する社会関係データが、必要に応じて適切に記憶、読み出される限り、データを記憶する方法やフォーマットを制限しない。

【0052】

50

記憶された社会関係データを用いて、ユーザアカウントに対応する社会関係データをクライアントから受信すると、ブロック S 1 0 2 のプロセスを行って、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果として、類似性を取得してよい。類似性を取得するために、類似性照合操作を行う。この操作は、クライアントまたはサーバで行われてよい。これらの 2 つの異なるアプローチに対応して、照合類似性を取得する 2 つの異なる方法があってよい。第 1 の方法は、クライアント側で類似性を取得することで、第 2 の方法は、サーバ自体で類似性を計算することである。いずれかの方法を用いて、開示の方法を実施してよい。これらの 2 つのアプローチについて、以下にさらに記載する。

【0053】

10

(1) クライアントで類似性照合

このアプローチを用いて、類似性照合操作をクライアントで行う。サーバは、ユーザアカウントの記憶された社会関係データをクライアントに送信することと、照合結果の類似性をクライアントから受信すること、という行為を行うことによって、照合結果の類似性を最終的に取得する。

【0054】

サーバは、最初に、記憶された社会関係データを送信する。これを行うために、サーバは、最初に、ユーザアカウントに従って記憶された社会関係データを調べ、ユーザアカウントに対応する社会関係データを抽出し、次に、抽出したデータをクライアントに送信する。例示の実施例においては、サーバは、ユーザアカウントに対応する社会関係のある電話番号のリストを記憶された社会関係データベースから抽出し、そのリストをクライアントに送信する。他の実施形態においては、QQ 番号リストまたはソーシャルネットワークのアカウント番号のリスト等、異なる種類の社会関係データを取得して、クライアントに送信してよい。

20

【0055】

クライアント端末がモバイル通信装置である例示の実施例においては、サーバは、電話番号リストをクライアント端末に送信する。しかしながら、他の実施形態においては、認証を受けるべきクライアントは、モバイル通信装置でない場合がある。このような状況では、認証を受けるべきクライアントの種類を最初に判定する。従来型の携帯電話またはスマートフォン等のモバイル通信装置の場合、ユーザアカウントに対応する電話番号リスト（または、ソーシャルネットワークの連絡先リスト）をクライアント端末に送信する。クライアントが電話帳を持っていないと判定される場合（例えば、通常の PC の場合）、クライアントが類似性照合操作を行うために、電話番号リストではなく、QQ 番号リスト等のソーシャルネットワークの連絡先リストの方が適しているであろう。クライアントに送信された社会関係データの変形形態は、実施の種類の問題だけであり、本開示の範囲を逸脱しない。

30

【0056】

より簡単な実施としては、ユーザアカウントに対応する社会関係データを暗号化せずにクライアントに送信する場合がある。これは、簡単に実施できるが、欠点がある。ソーシャルネットワーク電話番号等の社会関係データは、ユーザの個人情報の一部であり、プライバシーのために、他人に不必要に公開されるべきではない。このようなデータの送信中、悪意の攻撃者が、不正な傍受によって、このような情報を取得し、情報を不法に拡散して、ユーザ及びインターネットにセキュリティリスクをもたらす得る。このような問題を避けるために、社会関係データは、クライアント端末に送信する前に暗号化することが好ましい。

40

【0057】

一実施形態においては、AES (Advanced Encryption Standard) 暗号化アルゴリズムを用いて、社会関係データを暗号化する。AES は、米商務省標準技術局 (NIST) がデータ暗号化に用いる暗号化アルゴリズムである。AES は、最も普及している対称鍵暗号技術の 1 つであり、互いに全く同じ暗号鍵と復号鍵を

50

使用する一種の可逆暗号化アルゴリズムである。AESアルゴリズムを使って、暗号鍵によってソーシャルネットワーク電話番号のリストを暗号化する場合、受信モバイル通信装置は、同じ鍵を用いて受信した情報を復号し、暗号化されていないソーシャルネットワーク電話番号のリストを取得してよい。3DES等の他の暗号化方法も用いてよい。

【0058】

暗号鍵の管理に関しては、サーバとクライアント端末は、予め設定した鍵を持ち続けてもよく、または、セキュリティ向上のために、定期的に更新、配布される鍵を用いてもよい。暗号化を用いるべきか否か、どの暗号化アルゴリズムを用いるべきか、及び、どの暗号鍵管理方法を用いるべきかは、異なる実施において、実際の需要に応じて決定されてよく、選択は、本開示によって制限されず、本開示の範囲に影響を与えない。

10

【0059】

ユーザアカウントに対応する社会関係データを受信すると、クライアントは、受信したデータをローカルのユーザの社会関係データと照合し、照合結果をサーバに送信する。サーバは、照合結果をクライアントから受信する。

【0060】

照合結果の類似性は、一致数及び／または一致レベルを含んでよい。一致数は、ユーザアカウントの記憶された社会関係データと、クライアントの社会関係データとの間で一致することが判明した項目の総数として定義され、一致レベルは、一致数と、記憶された社会関係データの項目の総数との比率として定義される。例えば、クライアントに送信された社会関係データが、ユーザアカウントの社会的に関連する電話番号のリストを有する場合、クライアントは、クライアントのアドレス帳から電話番号リストを抽出して、社会的に関連する受信した電話番号リストとクライアントの抽出した電話番号リストを比較して、両方のリスト上で一致した全ての電話番号を識別してよい。一致する電話番号の総数が、一致数である。

20

【0061】

あるいは、クライアントは、社会的に関連した電話番号の受信したリストを、クライアントのローカルアドレス帳と直接比較してよい。受信したリストの電話番号のいずれかが、ローカルアドレス帳にもある場合、照合に成功したと見なされる。言い換えると、電話番号は、本開示に従った一致条件を満たす。この場合、クライアントのローカルアドレス帳にも表れる受信したリスト内の電話番号の総数が、一致数である。クライアントに送信された社会関係データが、社会的に関連する当事者のQQ番号のリストを有する場合、クライアントは、上記と同様の方法を用いて、受信したQQ番号をローカルのQQ番号と比較して、一致数を取得してよい。

30

【0062】

例示のための特定の実施形態においては、ユーザアカウントの記憶された社会関係データ（すなわち、クライアントに送信された社会関係データ）は、ユーザアカウントの社会的に関連した電話番号のリストである。実施例のリストは、10の電話番号を含み、そのうちの5つの電話番号は、（照合成功の結果として）ローカルクライアントアドレス帳の電話番号と一致していることが分かった。従って、クライアントから受信した照合結果の類似性は、一致数が5で、一致レベル0.5（ $5/10=0.5$ ）を有する。

40

【0063】

上記例示の実施例の照合結果の類似性は、一致数と一致レベルの両方を含む。しかしながら、一致数または一致レベルのどちらか一方でも、ユーザアカウントの記憶された社会関係データと、クライアントの社会関係データの一致条件を反映し得るので、クライアントは、両方ではなく、それらのいずれか一方を報告してよい。それでも、サーバは、クライアントが本人認証を通過できるか否かを判定可能である。しかしながら、一致数と一致レベルは、一致数が、照合に成功したデータ項目の総数を表す絶対的な値であり、一致レベルが、一致の相対的レベルを表す比率という、それぞれ、異なる意味を有し、両方が、同じ次元に属さないことを考慮すると、本人認証のためのより正確な意思決定を容易にするために、両方の値が、クライアントによって報告されることが好ましい。

50

【0064】

他の実施形態においては、一致数及び／または一致レベル以外のパラメータは、ユーザアカウントの記憶された社会関係データと、クライアントの社会関係データとの間の類似性を十分に示すことができる限り、照合結果の類似性として使用されてよい。このような実施は、全て、本開示と同じ範囲内の技術スキームの一部とみなされる。

【0065】

上記の例示の実施形態においては、照合結果の類似性は、クライアントからサーバにアップストリームに報告され、サーバは、予め設定した閾値を用いて本人認証の結果を判定する（ブロックS103に関連して記載する）。変形形態として、予め設定した閾値は、サーバからクライアントにダウンストリームに送信されてもよく、クライアントが、一致数及び／または一致レベルを計算し、クライアント自体が閾値に基づいて本人認証の結果を決定し、次に、その結果をアップストリームにサーバに報告するようにしてもよい。この場合、サーバは、一致数及び／または一致レベルではなく、代わりに、照合結果に従ったより具体的な指示を受信する。例えば、サーバは、クライアントが認証を通過したか否かの明確な指示をクライアントから受信してよい。閾値がクライアントにダウンストリームに送信されるこのような変形形態は、開示の範囲内とみなされる。

10

【0066】

さらに、上記予め設定した閾値は、ユーザアカウントの記憶された社会関係データと共にクライアントに送信されてよく、または、クライアント側に予め記憶されてもよい。後者の変形形態は、各認証行為に対して、クライアントに予め設定した閾値を送信する必要がなく、従って、手順が簡単になる。また、前者の変形形態は、クライアントに送信する記憶された社会関係データに従って、閾値の調整が簡単になるという利点がある。従って、各変形形態には、それぞれ、長所と短所があり、2つの変形形態間の選択は、具体的な適用の需要に応じて行ってよい。

20

【0067】

(2) サーバでの類似性照合

上記は、類似性照合をクライアントで行う実施形態である。しかしながら、本開示によると、類似性照合は、代わりにサーバで行われてよい。どちらのアプローチも本開示の範囲内である。

【0068】

サーバを用いて類似性照合を行うアプローチの場合、サーバは、次のステップを行って、照合結果の類似性を取得する。すなわち、サーバは、クライアントに記憶された社会関係データをユーザから受信して、クライアントに記憶された社会関係データと、サーバに記憶されたユーザアカウントの社会関係データとの照合結果として、類似性を計算する。

30

【0069】

このアプローチを用いると、クライアントは、ローカルに記憶された社会関係データを開示の方法の実施に使用するサーバに送信する。一実施形態においては、クライアントは、クライアントのローカルに記憶された社会関係データを、アカウント名及びパスワードと共に、サーバにアップストリームに送信する。あるいは、サーバがアカウント名及びパスワードの検証に成功した後、クライアントは、クライアントのローカルに記憶された社会関係データをサーバに送信してよい。クライアントとサーバが手順を互いに理解している限り、どちらの手順も受け入れられる。

40

【0070】

クライアントに記憶された社会関係データをクライアントから受信すると、サーバは、最初に、受信したデータが、復号を必要とするか否かを判定し、必要であれば、復号を行う。例えば、受信したデータが可逆暗号化アルゴリズムAESを用いて暗号化されている場合、サーバは、暗号化に用いたのと同じ鍵を用いてデータを復号する。クライアントとサーバ間の合意がある限り、または、サーバが復号化を適切に行うことを可能にする明確な指示が受信したデータに含まれる限り、任意の暗号化方法を用いてよい。

【0071】

50

データクリーニングによって特定のユーザアカウントに対応する記憶された社会関係データがサーバで生成されると想定すると、サーバは、類似性照合を行うために、ユーザアカウントの社会関係データを読み出し、または、抽出してよい。例えば、社会関係データが関係データベースに記憶されている場合、サーバは、SQL文を用いてユーザアカウントの社会関係データをデータベースから読み出し、さらに、クライアントから受信した社会関係データと一致する社会関係データをデータベースから読み出す。データベース構造が許す限り、サーバは、クライアントから受信した社会関係データと一致する社会関係データを直接、読み出してよい。例えば、クライアントが、クライアントアドレス帳、または、クライアントアドレス帳から抽出した電話番号リストを送信する場合、サーバは、このステップで、ユーザアカウントの全ての社会関係データから社会的に関連する電話番号のリストを抽出する。

10

【0072】

次に、サーバは、クライアントに記憶された社会関係データと、サーバに記憶されたユーザアカウントの社会関係データとの照合結果として、類似性を計算する。類似性照合プロセスは、クライアントからのデータソースと、サーバからのデータソースという、2つの社会関係データソースを比較して、両方のデータソースで（照合に成功した結果）一致することが分かったデータ項目の数を決定するプロセスである。これによって、一致数が分かる。例えば、クライアントから受信した社会関係データがクライアントアドレス帳であり、サーバのユーザアカウントに対応する記憶された社会関係データが10の電話番号を含み、そのうちの5つがクライアントから受信した社会関係データと一致することが分かった場合、この実施例において、一致数は、5である。

20

【0073】

簡単な照合プロセスも使用されてよい。最初に、ユーザアカウントに対応する記憶された社会関係データを読み出す代わりに、クライアントの受信した社会関係データを、サーバの記憶された社会関係データに対して、一項目ずつ、直接、照合し、各成功した照合を加算して一致数を取得してよい。照合時間を低減し、照合効率を向上させるために、データは、最初に、順に並べられてもよく、木構造等のシーケンシャル構造を用いて、編成されてもよい。具体的な照合方法は、本開示の一部ではなく、いかなる方法にも限定されない。

【0074】

30

一致数に加えて、一致レベルも計算してよい。上記の例示の実施例においては、一致数が5で、ユーザアカウントの記憶された社会関係データからの電話番号のリストが、全体で10の電話番号を有するので、一致レベルは、 $5 / 10 = 0.5$ と計算される。

【0075】

上記は、照合結果の類似性を取得する2つの代替アプローチである。2つのアプローチは、照合操作が異なった場所で起こるという点で互いに異なる。第1のアプローチにおいては、クライアントは、類似性照合を行い、その結果をサーバにアップストリームに報告する。第2のアプローチにおいては、クライアントは、クライアントの社会関係データをサーバにアップストリームに送信して、サーバが類似性を計算してよい。機能的に、これら2つのアプローチは、交換可能である。しかしながら、実際には、各アプローチには、それぞれ、強みと欠点がある。クライアントベースのアプローチを用いると、クライアントは、ローカルの社会関係データをアップストリームに送信する必要がないので、プライバシーに関する懸念が少なくなる。同時に、データクリーニングによってサーバで取得されるデータ量が制限されるので、サーバからクライアントへのダウンストリームのデータトラフィックも制限される。サーバベースのアプローチを用いると、データ処理は、サーバで行われ、より信頼できる。さらに、サーバは、クライアントから受信したデータを集約することによって、より完全でより信頼できる社会関係データを取得する。しかしながら、データをクライアントからサーバに転送するアップストリームトラフィックが混雑する場合があります、プライバシーの懸念もある。各アプローチの特性を考慮して、異なる適用の実際の需要に基づいて選択が行われてよい。

40

50

【0076】

ブロックS103：類似性が予め設定した通過条件を満たすか否かを判定し、満たす場合、クライアントが本人認証を通過できるようにする。

【0077】

ブロックS102は、データ照合の結果として、類似性を取得した。ブロックS103で、予め設定した条件を用いて、クライアントが本人認証を通過し得るか否かをテストする。

【0078】

この記載において、予め設定した通過条件とは、クライアントが本人認証を通過するために照合結果の類似性が満たす必要のある条件を指す。詳細には、一致数及び／または一致レベルは、それぞれ、本人認証を通過するために一致数及び／または一致レベルの閾値よりも大きい（または、以上）必要がある。例示の実施例においては、ブロックS102で取得された一致数は5で、一致レベルは0.5である。一致数の予め設定した閾値が4で、一致レベルの予め設定した閾値が0.4である場合、認証中のクライアントは、本人認証を通過したとみなされる。閾値は、経験的に設定されてよい。ある実施形態においては、閾値は、認証結果の正確性を向上させるために、記憶された社会関係データのデータ項目数及びデータ種類に応じて調整されてよい。

10

【0079】

より厳しい実施形態においては、ブロックS102は、一致数と一致レベルの両方の値を取得し、認証条件を満たすために、両方の値は、それぞれの予め設定した閾値より大きい必要がある。これは、認証エラーを減らすためのより保守的なアプローチである。

20

【0080】

しかしながら、他の実施形態においては、条件を緩めてもよい。例えば、ブロックS102は、一致数と一致レベルのうちの1つの値のみを取得して、その閾値のみに基づいて、認証を行うことを可能にしてよい。例えば、クライアントが一致数のみを報告する場合、一致数が閾値より大きいことだけを必要とする。あるいは、主要な値に基づいた条件を用いてよい。例えば、ブロックS102が一致数と一致レベルの両方の値を取得した場合でさえ、ブロックS103は、2つの値のうちの1つのみを主要な値として満たすことを必要とする。例えば、一致レベルが、主要な値として設定されてよい。この場合、一致レベルが予め設定した閾値より大きい限り、クライアントは、一致数が一致数の予め設定した値より大きいか否かに関わらず、認証条件を満たしたと考えられる。あるいは、2つの値のいずれか1つに基づいた条件を用いてよい。一致数と一致レベルのうちの1つが予め設定した閾値を満たす限り、クライアントは、認証条件を満たすと考えられる。これらの実施形態においては、条件を比較的緩くしても、本開示の目的は、閾値の適切な選択によって達成し得る。

30

【0081】

オプションで、照合結果の類似性が、予め設定した認証条件を満たさない場合、類似性が予め設定されたアラート条件を満たすか否かをさらに判定してよく、満たす場合、本人認証を拒絶して、アラートアクションを取る。詳細には、ブロックS102で取得した一致数及び／または一致レベルが、それぞれ、一致数及び／または一致レベルの閾値より小さい場合、クライアント装置は、特定のユーザアカウントの所有者には属せずに、盗まれた装置に属する可能性がある結論付けてよい、従って、認証は拒絶し、さらに、アラートアクションを取ってよい。

40

【0082】

認証を通過させる閾値と同様、固定の経験値または実際の条件に従って動的に調整された変数値のいずれかを用いて、アラート閾値も予め設定してよい。アラート条件については、認証を拒絶してアラートアクションを取るために、一致数と一致レベルの両方が各アラート値より小さいことを要求することによって、厳しい要件を設定してもよく、または、2つのうちの1つだけがアラート値より小さいことを要求することによって、あまり厳しくない要件を設定してもよい。

50

【0083】

サーバが閾値（通過のための一致数閾値、通過のための一致レベル閾値、アラートのための一致数閾値、アラートのための一致レベル閾値）をクライアントにダウンストリームに送信し、クライアントが、一致数及び一致レベルを計算し、認証条件を満たすか否かを直接決定するブロックS102に記載のような実施形態においては、ブロックS102でサーバが受信した情報は、クライアントが認証と通過したか否か、または、認証に失敗した場合、アラートアクションが取られたか否かを明確に示している。この場合、閾値に基づいて、サーバがクライアント認証またはアラート条件を判定する必要はない。

【0084】

通過閾値及びアラート閾値は、同じ値に設定してよいが、異なる値に設定されてもよい。例えば、通過閾値は、アラート閾値より大きくてよい。閾値の程度を例に取る。一致レベルに関する予め設定した通過閾値を0.5とし、一致レベルに関する予め設定したアラート閾値を0.2とする。そうすると、0.5より大きい照合結果の類似性は、クライアントが認証を通過するのを可能にし、0.2より小さい照合結果の類似性は、クライアント認証を拒絶するだけでなく、アラートアクションをトリガしてよい、一方、0.2及び0.5に一致する結果の類似性は、クライアント認証を拒絶するが、アラートアクションをトリガしない。

【0085】

一実施形態においては、照合結果の類似性が通過閾値とアラート閾値との間になる場合、サーバは、プロセスに対してより積極的なアプローチを取ってよい。具体的には、サーバは、新しい通信プロセスを開始して、別の社会関係データの照合条件を計算し、その新しい照合結果に基づいてさらなる判定を行ってよい。例えば、電話番号に加えて、サーバは、さらに、QQ番号を用いて、クライアントデータをサーバデータに照合して、QQ番号に基づいて照合結果の新しい類似性を取得し、照合結果の新しい類似性を各閾値と比較することによって、クライアントが認証を通過できるか否かを判定してよい。この手順は、クライアントの本人認証をより正確に行うために、結果及びサーバポリシーに応じて、一度または複数回、行われてよい。

【0086】

ブロックS103を実行した後、クライアントが認証を通過できるか否かについて明確な結論が引き出され、サーバは、それに従って、次のアクションを行ってよい。例えば、クライアントが認証を通過できるという結論の場合、サーバは、本人確認を示す返事をクライアントに送信し、クライアントが認証に失敗し、さらにアラートをトリガしたという結論の場合、サーバは、拒絶を示す返事をクライアントに送信し、さらに、ユーザアカウントをロックアップし、他のユーザに通知してよい。他の状況においては、サーバは、拒絶を示す返事をクライアントに送信するだけでよい。適用の異なる需要に従って他のアクションを取ってよい。

【0087】

本明細書に開示の方法に関連して、本開示は、本明細書に記載の方法を実施するコンピュータベースの装置も提供する。

【0088】

上記技術は、コンピュータ実行命令を含む1つまたは複数の非一時的コンピュータ可読媒体の支援を得て実施されてよい。非一時的コンピュータ実行命令によって、コンピュータプロセッサは、本明細書に記載の技術に従って、アクションを行うことができる。コンピュータ可読媒体は、コンピュータデータを記憶する任意の適切なメモリ装置であってよいことは理解されたい。このようなメモリ装置は、ハードディスク、フラッシュメモリ装置、光データ記憶装置、及び、フロッピーディスクを含むが、それらに限定されない。さらに、コンピュータ実行命令を含むコンピュータ可読媒体は、ローカルシステムのコンポーネント（単数または複数）、または、複数の遠隔システムのネットワークにわたって分配されたコンポーネントからなってもよい。コンピュータ実行命令のデータは、有形の物理的メモリ装置で配布されてもよく、電子的に送信されてもよい。

【0089】

本開示においては、「モジュール」は、一般的に、特定のタスクまたは機能を行うように設計された機能性を指す。モジュールは、特定のタスクまたは機能に関連付けられた目的を達成するためのハードウェア、ソフトウェア、計画、もしくは、スキーム、または、それらの組み合わせであってよい。さらに、別個のモジュールという記載は、物理的に分かれた装置を使用すること必ずしも示唆しない。むしろ、その記載は、機能的なことのみにあり、幾つかのモジュールの機能が、1つの組み合わせられた装置またはコンポーネントで行われてよい。コンピュータベースのシステムで用いられると、プロセッサ、記憶装置、及び、メモリ等の通常のコンピュータコンポーネントは、1つまたは複数のモジュールとして機能して、様々な各機能を行うようにプログラムされてよい。

10

【0090】

図2は、社会関係データを用いたクライアント認証装置の実施例の機能ブロックを示す概略図である。当該装置は、1つまたは複数のプロセッサ202と、I/O装置204と、アプリケーションプログラム（単数または複数）を記憶するメモリ206と、を有する典型的なコンピュータ装置ハードウェアに基づいてよい。コンピュータ装置200は、以下の機能モジュールを有するようにプログラムされる。

【0091】

認証要求受信ユニット208は、ユーザアカウントに対応する本人認証の要求をクライアントから受信するようにプログラムされる。

【0092】

20

照合結果取得ユニット210は、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果として、類似性を取得するようにプログラムされる。

【0093】

通過判定ユニット212は、類似性が予め設定した通過条件を満たすか否かを判定し、満たす場合、クライアントが本人認証を通過できるようにプログラムされる。

【0094】

さらに、社会関係データ生成ユニットは、ユーザアカウントの社会関係データを取得、記憶するようにプログラムされてよい。社会関係データ生成ユニットは取得したデータを分析してユーザアカウントに関連する社会関係データを抽出する分析及び抽出サブユニットと、ユーザアカウントに関連する抽出した社会関係データを記憶する記憶ユニットと、をさらに備えてよい。記憶された社会関係データは、ユーザアカウントの記憶された社会関係データを構成する。

30

【0095】

照合結果取得ユニット210は、ユーザアカウントの記憶された社会関係データをクライアントに送信する社会関係データ送信サブユニットと、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとの照合結果をクライアントから受信する照合結果受信ユニットと、を備えてよい。

【0096】

照合結果取得ユニット210は、クライアントの社会関係データをクライアントから受信する社会関係データ受信サブユニットと、クライアントの社会関係データと、ユーザアカウントの記憶された社会関係データとを照合することによって類似性を計算する照合結果計算ユニットも備えてよい。

40

【0097】

コンピュータ装置200は、類似性が予め設定したアラート条件を満たすか否かを判定し、満たす場合、本人認証を拒絶し、アラートアクションを取るアラート判定ユニットをさらに備えてよい。

【0098】

照合結果としての類似性は、本明細書に規定したように、一致数及び／または一致レベルを含んでよい。類似性が予め設定した条件を満たすか否かの判定は、図1に示す方法に

50

関連して本明細書に記載している、よって、ここでは繰り返さない。

【0099】

図3を参照して、クライアント側で実施されるクライアント認証方法を以下に記載される。この方法は、図1に示す方法の代替方法である。

【0100】

ブロックS301：ユーザアカウントに対応する本人認証の要求をサーバに送信する。

【0101】

ユーザは、ログオン、支払、装置結び付け等の一定の操作をクライアント装置で行う必要があるため、クライアントアプリケーションは、本人認証を要求するために、アカウント名、パスワード、及び、他の情報をユーザインタフェースを通して入力するようにユーザに要求してよい。クライアント装置は、本人認証要求をサーバに送信し、サーバで、社会関係データに基づいた開示のクライアント認証方法を実施する。サーバは、最初に、アカウント名とパスワードが正しいか否かを検証し、次に、ユーザが行っている操作と、サーバ上のその特定のユーザアカウントのセキュリティレベルとに基づいて、社会関係に基づいたさらなるクライアントの本人認証プロセスを開始する必要があるか否かを判定する。

10

【0102】

ブロックS302：クライアントの認証情報をサーバに送信して、クライアントの社会関係データに基づいて、サーバがクライアントの認証を行うことを可能にする。

【0103】

このプロセスは、クライアントの社会関係データと、サーバに記憶された社会関係データとの照合結果として類似性を判定することを含む。図1及び図2を関連して本明細書に記載した両方のアプローチ、すなわち、クライアントでの類似性照合と、サーバでの類似性照合を用いてよい。

20

【0104】

クライアントベースのアプローチを用いて、クライアントの認証情報をサーバに提供して、クライアントの社会関係データに基づいて、サーバがクライアントを認証できるようにする行為は、ユーザアカウントの社会関係データをサーバから受信するステップと、クライアントの社会関係データとユーザアカウントの社会関係データとの照合結果として類似性を計算するステップと、類似性をサーバに送信するステップと、を伴う。サーバは、受信した類似性を用いて、クライアントが本人認証を通過するか否かを判定する。

30

【0105】

ある実施形態においては、照合結果の類似性を用いて、クライアントが本人認証を通過するか否かを判定する行為は、クライアント装置で行われてよい。例えば、サーバが、通過認証閾値（単数または複数）と、アラート閾値（単数または複数）をユーザアカウントの社会関係データと共に、クライアント装置に送信する場合、あるいは、クライアント装置が必要な閾値（単数または複数）を既に有する場合、クライアント装置自体が、照合結果の計算した類似性を、当該閾値（単数または複数）と比較して、クライアントが認証を通過するか否かを判定してよい。クライアントが本人認証通過に失敗すると、クライアント装置は、照合結果の類似性を、アラート閾値（単数または複数）とさらに比較して、アラートアクションを行うべきか否かを判定してよい。

40

【0106】

上記実施形態においては、クライアント装置が送信した照合結果の類似性は、一致数及び／または一致レベルではなく、クライアントが認証を通過したか否か、及び、アラートアクションを取る必要があるか否か等、照合結果に由来するより高度な情報である。

【0107】

サーバベースのアプローチを用いると、類似性照合は、サーバで行われ、結果として、クライアントでのタスクは簡単になり、クライアントのローカルの社会関係データをサーバに送信するだけになる。一実施形態においては、クライアントの社会関係データは、クライアント装置にローカルに記憶される。

50

【0108】

ブロックS303：クライアントが本人認証を通過したか否かの返事をサーバから受信する。

【0109】

サーバから返事を受信すると、クライアントは、返事に応じてさらなるアクションを取ってよい。返事が、クライアントが本人認証を通過したことを示す場合、クライアント装置はユーザアカウントの所有者に属すると見なされ、従って、ユーザは、ログオン、支払、及び、装置結び付け等の機密性の高い操作を引き続き行うことを許可される。返事が、クライアントが本人認証に失敗したことを示す場合、装置はユーザアカウントの所有者に属さない可能性があることを示唆し、従って、ユーザは、機密性の高い操作を引き続き行うことを許可されない。ユーザは、クライアントが本人認証を通過しなかったことをユーザインタフェースのダイアログウインドウを通して、通知されてよい。

10

【0110】

さらに詳細な記載については、図1及び図2の実施形態に関する記載を参照してよく、ここでは繰り返さない。

【0111】

図3の方法に対応して、クライアントの本人認証装置も記載する。

【0112】

図4は、社会関係データを用いたクライアント認証のためのコンピュータ装置400の実施例の機能ブロックを示す概略図である。当該装置は、1つまたは複数のプロセッサ402と、I/O装置404と、アプリケーションプログラムを記憶するメモリ406と、を有する典型的なコンピュータ装置ハードウェアに基づいてよい。コンピュータ装置400は、以下の機能モジュールを有するようにプログラムされる。

20

【0113】

認証要求送信ユニット408は、ユーザアカウントに対応する本人認証の要求をサーバに送信するようにプログラムされる。

【0114】

認証情報送信ユニット410は、クライアントの認証情報をサーバに送信して、クライアントの社会関係データに基づいて、サーバがクライアントを認証できるようにプログラムされる。

30

【0115】

認証結果受信ユニット412は、クライアントが本人認証を通過したか否かの返事をサーバから受信するようにプログラムされる。

【0116】

ある実施形態においては、認証情報送信ユニット410は、クライアント装置にローカルに記憶されたクライアントの社会関係データを送信するために用いられる。

【0117】

別の実施形態においては、認証情報送信ユニット410は、ユーザアカウントの社会関係データをサーバから受信する社会関係データ受信ユニットと、クライアントの社会関係データとユーザアカウントの社会関係データとの照合結果として、類似性を計算する照合結果計算ユニットと、照合結果の類似性をサーバに送信する照合結果送信ユニットと、を備える。

40

【0118】

社会関係データに基づいたクライアントの本人認証システムについてさらに記載する。

【0119】

図5は、社会関係データを用いたクライアント認証システムの実施例の機能ブロックを示す概略図である。

【0120】

システム500は、社会関係データを用いてクライアントの本人認証を行うサービス装置501と、クライアントの本人認証のためのサービス装置501と共に用いるクライア

50

ント装置502と、を備える。サービス装置501は、サーバであることが好ましいが、本開示に従って社会関係データを用いてクライアントの本人認証を行うようにプログラムされた任意の他の装置であってよい。クライアント装置502は、通常、モバイル通信装置、パーソナルコンピュータ、PDA、または、i Padである。例えば、クライアント装置502は、サービス装置501と通信して、ローカルに記憶された社会関係データと、クライアント装置502の社会関係データとサービス装置501に記憶された社会関係データと照合した類似性結果等、必要なデータをアップロードまたはダウンロードできるスマートフォンであってよい。サービス装置501は、クライアント装置502と通信するサーバ上に配置されて、本明細書に記載のサーバ側の機能を行ってよい。

【0121】

10

本開示に記載の技術は、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドデバイス、ポータブルデバイス、タブレットデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラム可能消費者装置、ネットワークPC、マイクロコンピュータ、大規模メインフレームコンピュータ、または、それらの1つまたは複数を含む任意の分散環境を含むが、それらに限定されない、一般的なコンピュータ設備もしくは環境、または、特殊なコンピュータ設備もしくは環境で実施されてよい。

【0122】

典型的な構成においては、コンピュータ装置は、1つまたは複数のプロセッサ(CPU)、入力/出力インタフェース、ネットワークインタフェース、及び、メモリを備える。

20

【0123】

メモリは、揮発性メモリ、ランダムアクセスメモリ(RAM)、及び/または、リードオンリメモリ(ROM)もしくはフラッシュメモリ(フラッシュRAM)等の他の形態の不揮発性メモリ等、コンピュータ可読媒体を含んでよい。コンピュータ装置の内部メモリは、一種のコンピュータ可読メモリ媒体である。

【0124】

コンピュータ可読媒体は、永久媒体、非永久媒体、取り外し可能媒体、取り外し不能媒体を含み、情報を記憶するための任意の方法または技術で形成されてよい。記憶される情報は、コンピュータ可読命令、データ構造、プログラムモジュール、または、他のデータのセットであってよい。コンピュータ記憶媒体の例は、相変化メモリ(PRAM)、スタティックランダムアクセスメモリ(SRAM)、ダイナミックランダムアクセスメモリ(DRAM)、他の種類のランダムアクセスメモリ(RAM)、リードオンリメモリ(ROM)、電氣的消去可能プログラム可能ROM(EEPROM)、フラッシュメモリ、もしくは、他のメモリ技術、CD-ROMリードオンリメモリ(CD-ROM)、デジタル多用途ディスク(DVD)、もしくは、他の光記憶装置、磁気カセット、磁気テープディスク記憶装置、もしくは、他の磁気記憶装置、または、コンピュータ装置によってアクセス可能な情報の記憶に使用し得る任意の他の非送信媒体を含むが、それらに限られない。本開示の定義に従うと、コンピュータ可読媒体は、変調データ信号及び搬送波等の一時的コンピュータ可読媒体(一時的媒体)は含まない。

30

【0125】

40

モジュールは、特に、機械実行可能コマンド及びコードに基づいて、コンピュータプログラムモジュールを用いて実施されてよい。一般的に、コンピュータプログラムモジュールは、特定のタスクを行ってもよく、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造等の特定の抽象データ型を実施してもよい。本開示に記載の技術は、分散コンピュータ環境等で実践されて、通信ネットワークを介して接続された遠隔処理装置によってタスクを行うことができる。分散コンピュータ環境において、プログラムモジュールは、メモリ装置を含むローカルまたは遠隔のコンピュータ記憶媒体のいずれに配置されてもよい。

【0126】

本明細書の様々な実施形態を、実施例と環境を用いて、徐々に詳しくなるように記載し

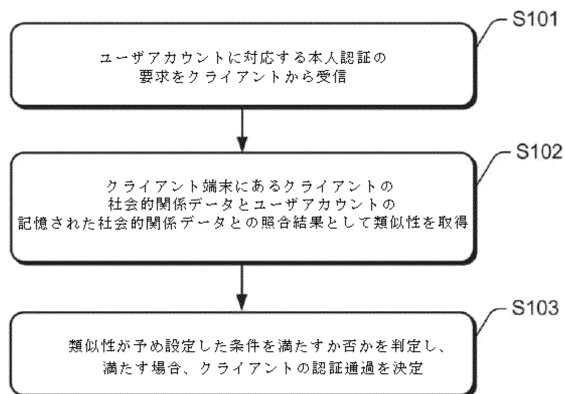
50

た。各実施形態は、一定の開示の態様に焦点を当てていることがあるので、異なる実施形態は、互いに異なり得るが、同じ部分を共有してもよい。

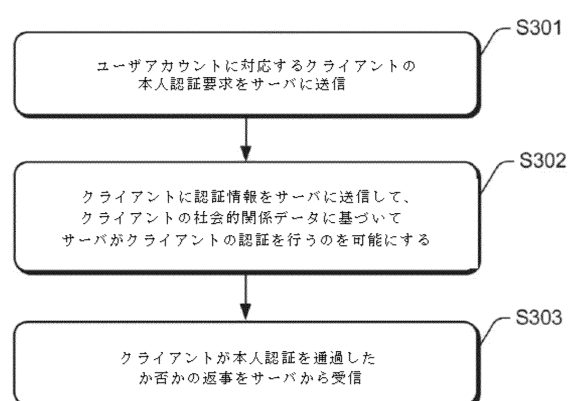
【0127】

例示の実施形態を用いて、本開示の本発明の概念及び実施を説明した。例示の実施形態は、本開示の方法と核となる概念をより良く理解できるようにのみ使用している。本開示の概念に基づいて、当業者は、例示の実施形態及び適用分野を変更してよい。

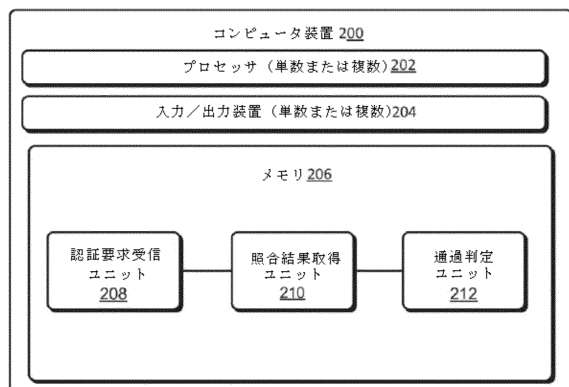
【図1】



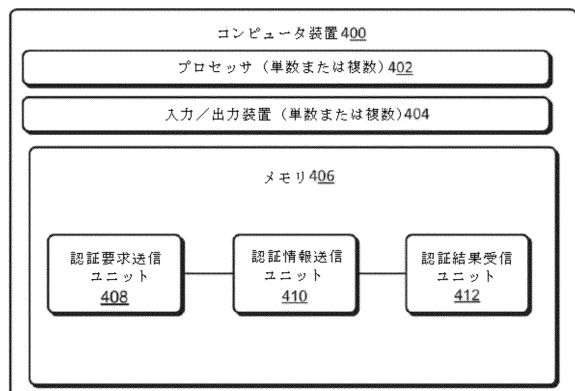
【図3】



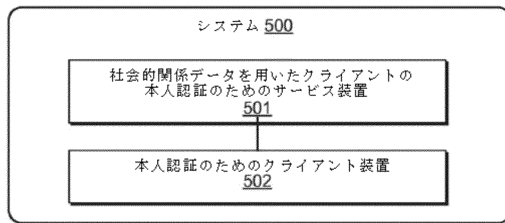
【図2】



【図4】



【図 5】



フロントページの続き

(72)発明者 カイ ツァオ

中華人民共和国 311121 ハンチョウ ユー ハン ディストリクト ウェスト ウェン
イー ロード ナンバー 969 ビルディング 3 5/エフ アリババ グループ リーガル
デパートメント内

審査官 岸野 徹

(56)参考文献 特開2012-203756 (JP, A)

特開2011-198170 (JP, A)

特開2013-069142 (JP, A)

特開2010-197980 (JP, A)

特開2012-238325 (JP, A)

特開2011-059837 (JP, A)

特開2013-041416 (JP, A)

特開2010-119048 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/31