(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7014898号
(P7014898)

(45)発行日　令和4年2月1日(2022.2.1)

(24)登録日　令和4年1月24日(2022.1.24)

(51)国際特許分類
G06F 21/31 (2013.01)

FI
G06F 21/31 360
G06F 21/31

請求項の数　8　（全17頁）

(21)出願番号　特願2020-514963(P2020-514963)
(86)(22)出願日　平成30年8月21日(2018.8.21)
(65)公表番号　特表2020-533704(P2020-533704A)
(43)公表日　令和2年11月19日(2020.11.19)
(86)国際出願番号　PCT/CN2018/101461
(87)国際公開番号　WO2019/148815
(87)国際公開日　令和1年8月8日(2019.8.8)
審査請求日　令和2年3月12日(2020.3.12)
(31)優先権主張番号　201810113381.2
(32)優先日　平成30年2月5日(2018.2.5)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　518017211
北京智明星通科技股▲ふん▼有限公司
Ｂｅｉｊｉｎｇ Ｅｌｅｘ Ｔｅｃｈｎｏｌｏｇｙ Ｃｏ．，Ｌｔｄ．
中華人民共和国北京市海淀区知春路７号致真大厦Ｃ座六層
６ｔｈ ｆｌｏｏｒ，Ｚｈｉｚｈｅｎ Ｂｕｉｌｄｉｎｇ Ｃ，Ｎｏ．７ Ｚｈｉｃｈｕｎ Ｒｏａｄ，Ｈａｉｄｉａｎ Ｄｉｓｔｒｉｃｔ，Ｂｅｉｊｉｎｇ １００００１，Ｐ．Ｒ．Ｃｈｉｎａ
(74)代理人　110000671
八田国際特許業務法人
(72)発明者　ゲン，ヨンジャン
中華人民共和国，ペキン，ファイジャン
最終頁に続く

(54)【発明の名称】　ＩＤ認証方法、装置、サーバ及びコンピュータ読み取り可能な媒体

(57)【特許請求の範囲】
【請求項１】
ＩＤ認証装置に用いられるＩＤ認証方法であって、
前記ＩＤ認証装置が、クライアント側から送信されたログイン情報を受信し、ユーザのオリジナルハードウェア機器情報とオリジナルソフトウェア記述情報とを前記ログイン情報から抽出するステップと、
前記ＩＤ認証装置が、前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側でのオリジナル操作行動情報を収集するステップと、
前記ＩＤ認証装置が、前記ユーザのオリジナルハードウェア機器情報、オリジナルソフトウェア記述情報および前記オリジナル操作行動情報をオリジナル特徴情報として特定するステップと、
前記クライアント側から送信された、前記ユーザのＩＤ認証情報が付加される認証要求を前記ＩＤ認証装置が受信するステップと、
前記ＩＤ認証装置が前記ＩＤ認証情報に基づいて認証を行うステップと、
前記ＩＤ認証情報が正当であると特定されたとき、前記ＩＤ認証装置が前記ユーザに関する複数の次元の行動特徴情報であってハードウェア機器情報、ソフトウェア記述情報及び操作行動情報を含む行動特徴情報を収集するステップと、
前記ＩＤ認証装置が、収集された行動特徴情報に基づいて対応する次元の前記オリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うステップと、を含み、
前記ＩＤ認証装置が、前記収集された行動特徴情報に基づいて対応する次元の前記オリジ

ナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うステップは、
前記ＩＤ認証装置が、前記操作行動情報の変化幅と前記オリジナル操作行動情報との比率を照合度として定義し、所定閾値の動的な範囲を設定することと、
収集された前記ハードウェア機器情報が対応する次元のオリジナルハードウェア機器情報と同じであり、収集された前記ソフトウェア記述情報が対応する次元のオリジナルソフトウェア記述情報と同じであり、且つ前記照合度が前記所定閾値の動的な範囲にある場合に、前記ＩＤ認証装置が前記ユーザのＩＤが正当であると特定し、そうでない場合に、前記ＩＤ認証装置が前記ユーザのＩＤが不当であると特定することと、を含むことを特徴とするＩＤ認証方法。
【請求項２】
前記ＩＤ認証装置が、前記収集された行動特徴情報に基づいて対応する次元の前記オリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行った後、更に、
前記ＩＤ認証装置が、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新するステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ＩＤ認証装置が、前記クライアント側から送信された特徴情報変更要求を受信するステップと、
前記ＩＤ認証装置が、前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集するステップと、
前記ＩＤ認証装置が、改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新するステップと、を更に含むことを特徴とする請求項１に記載の方法。
【請求項４】
クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信するための第１受信手段と、
前記ＩＤ認証情報に基づいて認証を行うための認証手段と、
前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報であってハードウェア機器情報、ソフトウェア記述情報及び操作行動情報を含む行動特徴情報を収集するための第１収集手段と、
所定閾値の動的な範囲を設定し、収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うためのマッチング識別手段と、
前記クライアント側から送信されたログイン情報を受信し、前記ユーザのオリジナルハードウェア機器情報とオリジナルソフトウェア記述情報とを前記ログイン情報から抽出するための第２受信手段と、
前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側でのオリジナル操作行動情報を収集するための第２収集手段と、
前記ユーザのオリジナルハードウェア機器情報、オリジナルソフトウェア記述情報および前記オリジナル操作行動情報を前記オリジナル特徴情報として特定するための特定手段と、を備え、
前記マッチング識別手段は、
前記操作行動情報の変化幅と前記オリジナル操作行動情報との比率を照合度として算出するための算出モジュールと、
収集された前記ハードウェア機器情報が対応する次元のオリジナルハードウェア機器情報と同じであり、収集された前記ソフトウェア記述情報が対応する次元のオリジナルソフトウェア記述情報と同じであり、且つ前記照合度が前記所定閾値の動的な範囲にある場合に、前記ユーザのＩＤが正当であると特定し、そうでない場合に、前記ユーザのＩＤが不当であると特定するための特定モジュールと、を備えることを特徴とするＩＤ認証装置。
【請求項５】

収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新するための第１更新手段を更に備えることを特徴とする請求項４に記載の装置。
【請求項６】
前記クライアント側から送信された特徴情報変更要求を受信するための第３受信手段と、前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集するための第３収集手段と、
改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新するための第２更新手段と、を更に備えることを特徴とする請求項４に記載の装置。
【請求項７】
サーバであって、
プロセッサと、メモリと、通信インターフェースと、バスとを備え、
前記メモリは、コンピュータの実行指令を記憶し、前記プロセッサと前記メモリとは、前記バスを介して接続され、前記サーバが運転する時、前記プロセッサが前記メモリに記憶されるコンピュータの実行指令を実行することにより、前記サーバは、請求項１から３の何れか一項に記載の方法のステップを実行することを特徴とするサーバ。
【請求項８】
コンピュータプログラムが記憶されるコンピュータ読み取り可能な記憶媒体であって、
当該プログラムがプロセッサによって実行される時、請求項１から３の何れか一項に記載の方法のステップが実施されることを特徴とするコンピュータ読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理技術分野に関し、特にＩＤ認証方法、装置、サーバ及びコンピュータ読み取り可能な媒体に関する。
【背景技術】
【０００２】
ＩＤ認証技術は、コンピュータネットワークにおいて操作者ＩＤを確認する手順を指し、モバイルスマート端末の迅速な発展とともに、モバイルスマート端末でＩＤ認証を行う手順は、ますます普及している。例えば、ＡＰＰ（Ａｐｐｌｉｃａｔｉｏｎ、アプリケーションプログラム）アカウントログイン、ネットワーク決済等の操作が存在する。
【０００３】
現在、よく用いられるＩＤ認証方法は、静的パスワード、スマートカード、動的パスワード、ショートメッセージパスワード、デジタル署名、生体認証等を含む。通常、携帯電話でアカウントログインを行う際、初回のアカウントのログインには、アカウント名及び静的パスワードによる認証方式が採用される。認証の安全性を更に強化するために、長時間ログインされていないときや、他の要素が変化したとき、チャレンジ方式を起動してＩＤ認証を行う。つまり、まず、ユーザに静的パスワードを入力させ、その後、ユーザの初回登録時にバインディングされた携帯電話へ動的パスワードを送信し、ユーザに再度ショートメッセージパスワードを入力させる。チャレンジ式ＩＤ認証法により、パスワードの安全性がある程度向上するが、ユーザＩＤ認証手順の利便性と柔軟性が制限される。また、クラウド計算技術が飛躍的に発展する昨今、ハッカーは、数千台や一万台以上のサーバを制御してパスワードを総当たり攻撃によって解読することも可能である。
【０００４】
一旦当該ユーザの応用アカウントが総当たり攻撃によって解読された後、ユーザのゲームマネー、ゲームアイテム等の仮想物品の紛失が発生し、更にユーザと他のユーザとの間のチャット情報の漏洩および財産損失等も発生する恐れがある。
【０００５】
このように、従来の移動スマート端末でのＩＤ認証手順に安全面上の潜在危険が存在する

ため、移動スマート端末でのユーザＩＤ認証手順の安全性を全体として向上させる方法が早急に求められている。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

これに鑑みて、本発明の実施例は、ＩＤ認証の安全性と正確性を効果的に向上可能であるＩＤ認証方法、装置、サーバ及びコンピュータ読み取り可能な媒体を提供する。

【課題を解決するための手段】

【０００７】

第１態様では、本発明の実施例は、ＩＤ認証方法を提供する。前記方法は、クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信するステップと、前記ＩＤ認証情報に基づいて認証を行うステップと、前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集するステップと、収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うステップと、を含む。

【０００８】

上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記ユーザから送信された認証要求を受信する前に、更に、前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出するステップと、前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集するステップと、前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定するステップとを、含む。

【０００９】

上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うステップは、収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出することと、対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、前記ユーザＩＤが不当であると特定することと、対応する照合度が所定閾値を超える行動特徴情報が１つも存在しないとき、前記ユーザＩＤが正当であると特定することと、を含む。

【００１０】

上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行った後、更に、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新するステップを含む。

【００１１】

上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記クライアント側から送信された特徴情報変更要求を受信するステップと、前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集するステップと、改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新するステップと、を更に含む。

【００１２】

第２態様では、本発明の実施例は、ＩＤ認証装置を提供する。前記装置は、クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信するための第１受信手段と、前記ＩＤ認証情報に基づいて認証を行うための認証手段と、前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集するための第１収集手段と、収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うためのマッチング識別

手段と、を備える。
【００１３】
上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記装置は、前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出するための第２受信手段と、前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集するための第２収集手段と、前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定するための特定手段と、を更に備える。
【００１４】
上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記マッチング識別手段は、収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出するための算出モジュールと、対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、前記ユーザＩＤが不当であると特定し、対応する照合度が所定閾値を超える行動特徴情報が１つも存在しないとき、前記ユーザＩＤが正当であると特定するための特定モジュールと、を備える。
【００１５】
上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記装置は、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新するための第１更新手段を更に備える。
【００１６】
上記態様と何れか一項の可能な実現形態では、１つの実現形態が更に提供され、前記装置は、前記クライアント側から送信された特徴情報変更要求を受信するための第３受信手段と、前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集するための第３収集手段と、改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新するための第２更新手段と、を更に備える。
【００１７】
第３態様では、本発明の実施例は、サーバを提供し、当該サーバは、プロセッサと、メモリと、通信インターフェースと、バスとを備え、前記メモリは、コンピュータの実行指令を記憶し、前記プロセッサと前記メモリとは、前記バスを介して接続され、前記サーバが運転する時、前記プロセッサが前記メモリに記憶されるコンピュータの実行指令を実行することにより、前記サーバは、第１態様の何れか一項に記載の方法のステップを実行する。
【００１８】
第４態様では、本発明の実施例は、コンピュータ読み取り可能な記憶媒体を提供し、当該記憶媒体にコンピュータプログラムが記憶され、当該プログラムがプロセッサによって実行される時、第１態様の何れか一項に記載の方法のステップが実施される。
【発明の効果】
【００１９】
本発明の実施例に係るＩＤ認証方法、装置、サーバ及びコンピュータ読み取り可能な媒体では、ＩＤ認証情報によって認証を行うことを基に、更にユーザの使用習慣を表せる行動特徴情報を用いてユーザ行動習慣を分析し、更に現在ログインユーザと履歴ユーザとが一致するか否かを判断するため、従来技術における単一の認証方式よりも、ＩＤ認証の安全性と正確性を効果的に向上可能である。
【図面の簡単な説明】
【００２０】
本発明の実施例における解決手段をより明確に説明するために、以下、実施例における説明に用いられる図面について、簡単に説明し、当然ながら、以下に説明される図面は、本発明の一部の実施例に過ぎず、当業者にとって、創造の労力をかけない前提で、これらの

図面に基づき、他の図面を得ることもできる。
【図１】本発明の実施例に係るＩＤ認証方法のフローの模式図である。
【図２】本発明の実施例に係る別のＩＤ認証方法のフローの模式図である。
【図３】本発明の実施例に係る別のＩＤ認証方法のフローの模式図である。
【図４】本発明の実施例に係る別のＩＤ認証方法のフローの模式図である。
【図５】本発明の実施例に係るＩＤ認証装置の構成のブロック図である。
【図６】本発明の実施例に係る別のＩＤ認証装置の構成のブロック図である。
【図７】本発明の実施例に係る別のＩＤ認証装置の構成のブロック図である。
【図８】本発明の実施例に係る別のＩＤ認証装置の構成のブロック図である。
【図９】本発明の実施例に係る別のＩＤ認証装置の構成のブロック図である。
【図１０】本発明の実施例に係るサーバの構成のブロック図である。
【発明を実施するための形態】
【００２１】
本発明の解決手段がよりよく理解できるように、本発明の実施例を本発明の図面を参照しながら以下に詳細に説明する。
【００２２】
明らかに、かかる実施例は、本発明の実施例の全部ではなく、一部の実施例に過ぎない。当業者が本発明の実施例に基づき、創造的労力を要しない前提で得たすべての他の実施例はいずれも本発明の保護範囲に含まれる。
【００２３】
本発明の実施例で使用される用語は、特定の実施形態のみを説明するためのものであり、本発明を限定するものではない。上下文に明確に他の意味を示さない限り、本発明の実施例及び添付の特許請求の範囲に使用される単数形の「１種」、「前記」及び「当該」が複数形も含むことも意図されている。
【００２４】
本明細書で使用される「及び／又は」という用語は、関連対象を説明する関連関係に過ぎず、３つの関係が存在してもよいと示し、例えば、Ａ及び／又はＢは、Ａが単独で存在することと、Ａ及びＢが同時に存在することと、Ｂが単独で存在することとの３つの場合を示す。また、本明細書に記載の記号「／」は、一般的に前後の関連対象が「又は」の関係であることを示す。
【００２５】
本発明の実施例において用語「第１」、「第２」、「第３」などを用いてＸＸＸを説明することがあるが、これらのＸＸＸはこれらの用語に限定されないことは、理解されるべきである。これらの用語は、ＸＸＸを互いに区分するためにのみ使用される。例えば、本発明の実施例の範囲から逸脱しない限り、第１ＸＸＸが第２ＸＸＸと称されてもよく、類似的に、第２ＸＸＸも第１ＸＸＸと称されてもよい。
【００２６】
文脈に応じて、本明細書で使用される「もし」という用語は、「…とき、」又は「…際、」又は「確定に応答し」又は「検出に応答し」と解釈されてもよい。類似的に、文脈に応じて、語句「もし…確定」又は「もし…（説明する条件又はイベント）を検出」は、「…確定するとき」又は「確定に応答し」又は「…（説明する条件又はイベント）を検出するとき」又は「（説明する条件又はイベント）の検出に応答し」と解釈されてもよい。
【００２７】
本発明の実施例は、ＩＤ認証方法を提供し、当該方法は、クライアント側に対応するサーバ一側で実行される。
【００２８】
本発明の実施例におけるユーザ機器は、ユーザにデータ連通性を供給する機器を指し、ユーザは、ユーザ機器に取り付けられたクライアント側を介してアカウントログイン操作を行ってＩＤ認証を完成可能であり、ユーザ機器は、具体的に、移動端末、例えば、複数種の応用機能を有するスマート携帯電話、タブレットＰＣ、車載の移動装置等を指してもよ

い。
【００２９】
本発明の実施例におけるサーバは、ユーザＩＤ認証へ算出サービスを供給する機器であり、サービスの要求に応答可能であり、サービスを担いつつ保証する能力を有し、プロセッサ、ハードディスク、メモリ、システムバス等によって構成される。
【００３０】
図１に示すように、前記方法は、下記のステップを含む。
【００３１】
ステップ１０１では、クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信する。
【００３２】
ただし、ＩＤ認証情報は、ユーザがクライアント側でアカウントログインを行うときに入力されてもよく、或いは、クライアント側で保存された後で自動的に記入されてもよい。ＩＤ認証情報は、一般的に、ユーザ名とパスワード、電子証明書等の各類の情報を含んでもよい。
【００３３】
ステップ１０２では、前記ＩＤ認証情報に基づいて認証を行う。
【００３４】
ステップ１０３では、前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集する。
【００３５】
上記ＩＤ認証情報とは異なり、本発明の実施例における行動特徴情報は、ハードウェア機器情報、ソフトウェア記述情報と操作行動情報を指す。行動特徴情報の次元は、上記３種の行動特徴情報のうち、収集され得る情報種別を指す。
【００３６】
ただし、ハードウェア機器情報は、ユーザ機器の所在する物理位置、ユーザ機器がアクセスするネットワーク環境、ユーザ機器の機器型番、プロセッサの型番、メモリの型番、規格及び容量、スクリーンサイズ等の複数の次元の情報を含んでもよい。
【００３７】
ソフトウェア記述情報は、クライアント側名称、クライアント側記憶経路、クライアント側バージョン番号、クライアント側オペレーティングシステムタイプ、クライアント側オペレーティングシステムバージョン、クライアント側内で使用される言語等の複数の次元の情報を含んでもよい。
【００３８】
操作行動情報は、ユーザがタッチ操作を行うときにタッチパネルをスライドする軌跡、クライアント側での使用手順における消費決済行動、アプリケーションプログラム内の各操作対象に対する処理行動等の複数の次元の情報を含んでもよい。
【００３９】
ステップ１０４では、収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行う。
【００４０】
オリジナル特徴情報は、予め収集された或いは予め設定された行動特徴情報であり、ユーザに対応する履歴統計情報として、新たに収集された行動特徴情報と照合し、新たに収集された行動特徴情報が当該ユーザの使用習慣にマッチングするか否かを特定する。
【００４１】
本発明の実施例に係るＩＤ認証方法では、ＩＤ認証情報によって認証を行うことをもとに、更にユーザの使用習慣を表せる行動特徴情報を用いてユーザ行動習慣を分析し、更に現在ログインユーザと履歴ユーザとが一致するか否かを判断するため、従来技術における単一の認証方式に比べ、ＩＤ認証の安全性と正確性を効果的に向上可能である。
【００４２】

更に言えば、如何にしてオリジナル特徴情報を取得するかについて、本発明の実施例は、対応する実現フローをここに提供し、図２に示すように、以下のステップを含む。

【００４３】

ステップ２０１では、前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出する。

【００４４】

ハードウェア機器情報とソフトウェア記述情報は、静的情報に属するため、ユーザがログインを行うときに直接収集してもよい。収集の方式としては、クライアント側を介して収集した後、データをログイン要求或いは認証要求に含めてサーバに送信してもよく、または、クライアント側によってサーバとの間の専用インターフェース（例えば、ＡＰＩ）を用いて関連データをサーバに伝送してもよい。

【００４５】

なお、ユーザのプライバシー需要に応じて、本発明の実施例で言及されたハードウェア機器情報、ソフトウェア記述情報と操作行動情報は、ユーザから承認されないと操作できない。具体的な承認手順は、クライアント側のインストール手順やアカウント初回登録手順等のような手順に実施可能である。

【００４６】

ステップ２０２では、前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集する。

【００４７】

操作行動情報がユーザのクライアント側での操作情報であるため、周期的に収集される必要がある。具体的に、１分ずつ１回収集するか、或いは１時間ずつ１回収集すると設定可能である。

【００４８】

ステップ２０３では、前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定する。

【００４９】

ハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報は、後続の検索と処理が便利になるように、ユーザごとに、対応するエントリにそれぞれ記憶される必要がある。

【００５０】

更に言えば、ステップ１０４について、収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うことの実施に対し、本発明の実施例は、図３に示すように、対応するフローを提供する。当該フローは、下記のステップを含む。

【００５１】

ステップ１０４１では、収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出する。対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、ステップ１０４２を実行し、そうでなければ、ステップ１０４３を実行する。

【００５２】

ハードウェア機器情報とソフトウェア記述情報のような静的情報に関しては、各次元で収集された行動特徴情報とオリジナル特徴情報が何れも特定値であるため、マッチングを行う際、同じであることと異なることとの２種の照合度が存在することが一般的である。よって、直接０と１００％で同じであることと異なることとを表せる。対応する所定閾値は、１００％と設定されてもよい。

【００５３】

操作行動情報のような動的情報に関しては、各次元で収集された情報が何れも動的に変化するものである可能性があるが、変化幅が総的なユーザ行動傾向に影響しないときには、当該変化幅がユーザ操作の正常変化範囲内にあると理解され得る。したがって、変化幅と

オリジナル特徴情報との比率が照合度として定義され得ると同時に、操作行動情報の所定閾値について動的な範囲を設定する必要もある。この動的範囲は、照合度が範囲内であれば、行動が合理であり、同一のユーザ操作に属すると見なされ、照合度が範囲外であれば、行動が不合理であり、同一のユーザ操作に属しないと見なされてもよい。

【００５４】

照合度の具体的な計算を行う際、クラスタリング分析に基づいて大量のユーザＩＤ特徴情報の履歴データを分類してから、ニューラルネットワークまたはベイジアン方法に基づいて数学的モデルを取得し、プリセット閾値を得て、最終的に各ＩＤ特徴タイプの重みと数学的モデルとに基づいて照合度を総合的に算出する。具体的な算出手順は、ここで繰り返し説明しない。

【００５５】

ステップ１０４２では、前記ユーザＩＤが不当であると特定する。

【００５６】

ステップ１０４３では、前記ユーザＩＤが正当であると特定する。

【００５７】

また、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新する。

【００５８】

また、補足説明すべきことは、ユーザが同一のアプリケーションプログラムを使用する手順において、携帯電話を取り換えたり、アクセスネットワークを変更したり、異なる地理位置でログインしたりする可能性があるため、サーバ側で記憶されたオリジナル特徴情報を変更して誤識別を回避させるメカニズムをユーザへ提供する必要がある。対応するフローは、図４に示すように、下記のステップを含む。

【００５９】

ステップ３０１では、前記クライアント側から送信された特徴情報変更要求を受信する。

【００６０】

ステップ３０２では、前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集する。

【００６１】

ステップ３０３では、改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新する。

【００６２】

本発明の実施例は、ＩＤ認証装置を更に提供し、図５に示すように、前記装置は、

クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信するための第１受信手段４１と、

前記ＩＤ認証情報に基づいて認証を行うための認証手段４２と、

前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集するための第１収集手段４３と、

収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うためのマッチング識別手段４４と、を備える。

【００６３】

好ましくは、図６に示すように、前記装置は、

前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出するための第２受信手段４５と、

前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集するための第２収集手段４６と、

前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定するための特定手段４７と、を更に備える。

【００６４】

好ましくは、図７に示すように、前記マッチング識別手段４４は、
収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出するための算出モジュール４４１と、
対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、前記ユーザＩＤが不当であると特定し、対応する照合度が所定閾値を超える行動特徴情報が１つも存在しないとき、前記ユーザＩＤが正当であると特定するための特定モジュール４４２と、を備える。

【００６５】

好ましくは、図８に示すように、前記装置は、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新するための第１更新手段４８を更に備える。

【００６６】

好ましくは、図９に示すように、前記装置は、
前記クライアント側から送信された特徴情報変更要求を受信するための第３受信手段４９と、
前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集するための第３収集手段４１０と、
改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新するための第２更新手段４１１と、を更に備える。

【００６７】

本発明の実施例に係るＩＤ認証装置では、ＩＤ認証情報によって認証を行うことをもとに、更にユーザの使用習慣を表せる行動特徴情報を用いてユーザ行動習慣を分析し、更に現在ログインユーザと履歴ユーザとが一致するか否かを判断するため、従来技術における単一の認証方式に比べ、ＩＤ認証の安全性と正確性を効果的に向上可能である。

【００６８】

本発明の実施例は、サーバ５０を提供し、図１０に示すように、少なくとも１つのプロセッサ５１、通信バス５２、メモリ５３および少なくとも１つの通信インターフェース５４を備える。

【００６９】

プロセッサ５１は、汎用の中央処理装置（ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ、ＣＰＵ）、マイクロプロセッサ、特定用途向け集積回路（ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ、ＡＳＩＣ）、又は本願の解決手段の実行を制御するための１つまたは複数の集積回路であってもよい。

【００７０】

通信バス５２は、上記ユニットの間で情報を伝送する通路を含んでもよい。

【００７１】

通信インターフェース５４は、送受信器のような如何なる装置も使用し、他の機器や通信ネットワーク、例えば、イーサネット（登録商標）、無線アクセスネットワーク（ｒａｄｉｏ ａｃｃｅｓｓ ｎｅｔｗｏｒｋ、ＲＡＮ）、無線ＬＡＮ（ｗｉｒｅｌｅｓｓ ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋｓ、ＷＬＡＮ）等と通信を行う。

【００７２】

メモリ５３は、読み取り専用メモリ（ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＲＯＭ）や静的情報と指令を記憶可能な他のタイプの静的記憶機器、ランダムアクセスメモリ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ、ＲＡＭ）や情報と指令を記憶可能な他のタイプの動的記憶機器であってもよく、電気的に消去可能なプログラマブル読み取り専用メモリ（ｅｌｅｃｔｒｉｃａｌｌｙ ｅｒａｓａｂｌｅ ｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＥＥＰＲＯＭ）、読み取り専用光ディスク（ｃｏｍｐａｃｔ ｄｉｓｃ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＣＤ－ＲＯＭ）或いは他の光ディスク記憶媒体、光学ディスク記憶媒体（コンパクトディスク、レーザ光ディスク、ＣＤ、ＤＶＤ、ブルーレイディスク等を含む）、磁気ディスク記憶媒体または他の磁気記憶機器であってもよく

、または、指令或いはデータ構造形式を有する所望のプログラムコードを付加や記憶可能でありながら、コンピュータによってアクセスされる如何なる他の媒体であってもよいが、それらに限定されない。メモリは、独立存在してもよく、バスを介してプロセッサと接続してもよい。メモリは、プロセッサに集積されてもよい。

【００７３】

ただし、メモリ５３は、本願の解決手段を実行するためのアプリケーションプログラムコードを記憶し、プロセッサ５１によって制御して実行される。プロセッサ５１は、メモリ５３に記憶されるアプリケーションプログラムコードを実行し、前記サーバが運転する時、前記プロセッサ５１が前記メモリ５３に記憶されるコンピュータの実行指令を実行することにより、前記サーバは、以下のフローを実行可能である。つまり、

クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信することと、

前記ＩＤ認証情報に基づいて認証を行うことと、

前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集することと、

収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うこととが実行される。

【００７４】

好ましくは、前記ユーザから送信された認証要求を受信する前に、前記フローは、更に、

前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出することと、

前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集することと、

前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定することとを含む。

【００７５】

好ましくは、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うことは、具体的に、

収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出することと、

対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、前記ユーザＩＤが不当であると特定することと、

対応する照合度が所定閾値を超える行動特徴情報が１つも存在しないとき、前記ユーザＩＤが正当であると特定することとのように実行されてもよい。

【００７６】

好ましくは、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行った後、前記フローは、更に、

収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新することを含む。

【００７７】

好ましくは、前記フローは、更に、

前記クライアント側から送信された特徴情報変更要求を受信することと、

前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集することと、

改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新することとを含む。

【００７８】

本発明の実施例に係るサーバでは、ＩＤ認証情報によって認証を行うことをもとに、更にユーザの使用習慣を表せる行動特徴情報を用いてユーザ行動習慣を分析し、更に現在ログインユーザと履歴ユーザとが一致するか否かを判断するため、従来技術における単一の認

証方式に比べ、ＩＤ認証の安全性と正確性を効果的に向上可能である。
【００７９】
本発明の実施例は、コンピュータ読み取り可能な記憶媒体を更に提供し、当該記憶媒体にコンピュータプログラムが記憶され、当該プログラムがプロセッサによって実行されたときに以下の方法ステップは実施される。つまり、
クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信することと、
前記ＩＤ認証情報に基づいて認証を行うことと、
前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集することと、
収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うこととが実施される。
【００８０】
好ましくは、前記ユーザから送信された認証要求を受信する前に、当該フローは、更に、
前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出することと、
前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集することと、
前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定することとを含む。
【００８１】
好ましくは、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行うことは、具体的に、
収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出することと、
対応する照合度が所定閾値を超える行動特徴情報が少なくとも１つ存在するとき、前記ユーザＩＤが不当であると特定することと、
対応する照合度が所定閾値を超える行動特徴情報が１つも存在しないとき、前記ユーザＩＤが正当であると特定することとのように実行されてもよい。
【００８２】
好ましくは、前記収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行った後、前記フローは、更に、収集された前記行動特徴情報と、対応するＩＤマッチング識別結果とに基づいて、記憶された前記オリジナル特徴情報と、対応する所定閾値とを更新することを含む。
【００８３】
好ましくは、当該フローは、更に、
前記クライアント側から送信された特徴情報変更要求を受信することと、
前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集することと、
改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新することとを含む。
【００８４】
本発明の実施例に係るコンピュータ読み取り可能な媒体では、ＩＤ認証情報によって認証を行うことをもとに、更にユーザの使用習慣を表せる行動特徴情報を用いてユーザ行動習慣を分析し、更に現在ログインユーザと履歴ユーザとが一致するか否かを判断するため、従来技術における単一の認証方式に比べ、ＩＤ認証の安全性と正確性を効果的に向上可能である。
【００８５】
当業者であればわかるように、説明の便宜および簡潔さのために、上述したシステム、装置、及び手段の特定の作業手順については、上記方法実施例における対応する手順を参照

すればよいため、ここで繰り返し述べない。

【００８６】

本発明に供されるいくつかの実施例において、開示されたシステム、装置および方法は、他の方法で実施され得ることが理解されるべきである。例えば、上述した装置実施例は単に概略的なものであり、例えば、前記手段の区分は１つの論理的な機能区分であり、実際の実装は別の区分方法を有してもよい。例えば、複数の手段やユニットが結合されてもよく、または別のシステムに統合されてもよく、またはいくつかの特徴が無視されるか実行されなくてもよい。さらに、表示または説明された相互結合または直接結合または通信接続は、いくつかのインターフェース、装置または手段を介した間接結合または通信接続であってもよく、電気的、機械的または他の形態であってもよい。

【００８７】

上記分離部品として説明された手段は、物理的に分離されてもよく、或いは、物理的に分離されなくてもよく、手段として表示される部品は、物理手段であってもよく、或いは、物理手段でなくてもよく、即ち、１か所に配置されていても、複数のネットワークセルに分散していてもよい。この実施例の解決案の目的を達成するために、手段の一部または全部を実際のニーズに応じて選択することができる。

【００８８】

また、本発明の各実施例における各機能手段は、１つの処理手段に組み込まれていてもよいし、物理的に単独で存在してもよいし、２つ以上が一体化としてもよい。上記統合された手段は、ハードウェアの形態でも、または、ハードウェアプラスソフトウェア機能手段の形態でも実現可能である。

【００８９】

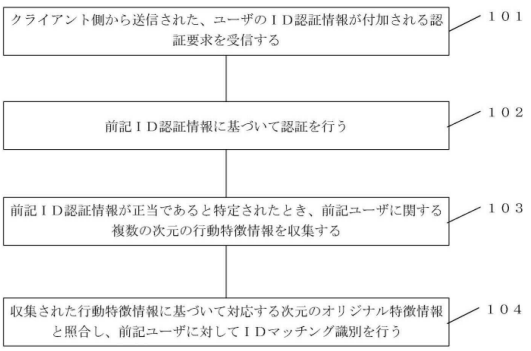
ソフトウェア機能手段として実現された上記統合の手段は、コンピュータ読み取り可能な記憶媒体に格納されてもよい。上記ソフトウェア機能手段は、記憶媒体に格納され、コンピュータ装置（パーソナルコンピュータ、サーバ、又はネットワーク装置などであってもよい）またはプロセッサ（Ｐｒｏｃｅｓｓｏｒ）が本発明の各実施例で説明した方法に関する一部のステップを実行するためのいくつかの指令を含む。上記記憶媒体には、Ｕディスク、リムーバブルハードディスク、読み取り専用メモリ（ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＲＯＭ）、ランダムアクセスメモリ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ、ＲＡＭ）、磁気ディスク、又は光ディスクなどのプログラムコードを格納可能な様々な他の媒体が含まれる。

【００９０】

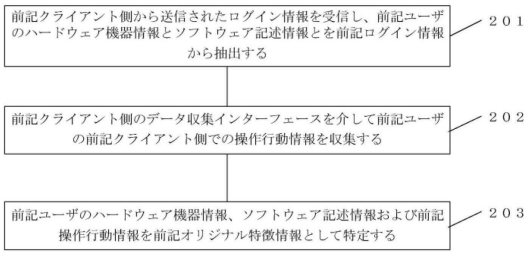
以上説明は、本発明の好適な実施例に過ぎず、本発明を限定するものではない。本発明の精神および原理の範囲内でなされた変更、均等物による置換、改良などは、何れも本発明の保護範囲に含まれるべきである。

【図面】

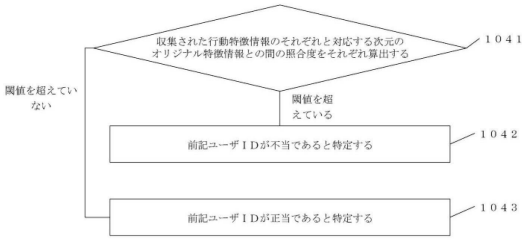
【図１】


クライアント側から送信された、ユーザのＩＤ認証情報が付加される認証要求を受信する
１０１
前記ＩＤ認証情報に基づいて認証を行う
１０２
前記ＩＤ認証情報が正当であると特定されたとき、前記ユーザに関する複数の次元の行動特徴情報を収集する
１０３
収集された行動特徴情報に基づいて対応する次元のオリジナル特徴情報と照合し、前記ユーザに対してＩＤマッチング識別を行う
１０４

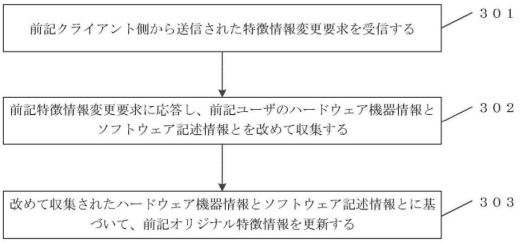
【図２】


前記クライアント側から送信されたログイン情報を受信し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを前記ログイン情報から抽出する
２０１
前記クライアント側のデータ収集インターフェースを介して前記ユーザの前記クライアント側での操作行動情報を収集する
２０２
前記ユーザのハードウェア機器情報、ソフトウェア記述情報および前記操作行動情報を前記オリジナル特徴情報として特定する
２０３

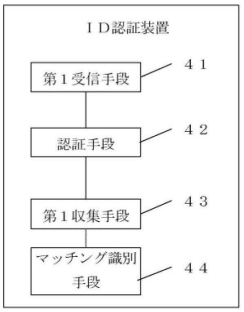
【図３】


収集された行動特徴情報のそれぞれと対応する次元のオリジナル特徴情報との間の照合度をそれぞれ算出する
１０４１
閾値を超えていない
閾値を超えている
前記ユーザＩＤが不当であると特定する
１０４２
前記ユーザＩＤが正当であると特定する
１０４３

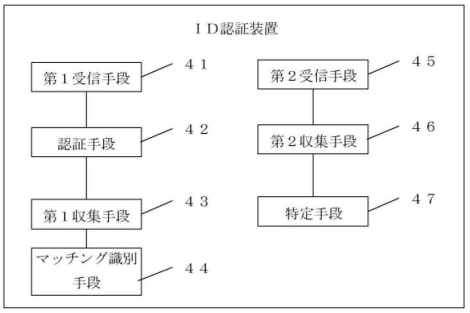
【図４】


前記クライアント側から送信された特徴情報変更要求を受信する
３０１
前記特徴情報変更要求に応答し、前記ユーザのハードウェア機器情報とソフトウェア記述情報とを改めて収集する
３０２
改めて収集されたハードウェア機器情報とソフトウェア記述情報とに基づいて、前記オリジナル特徴情報を更新する
３０３

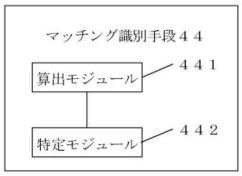
【図５】


ＩＤ認証装置
第１受信手段
４１
認証手段
４２
第１収集手段
４３
マッチング識別手段
４４

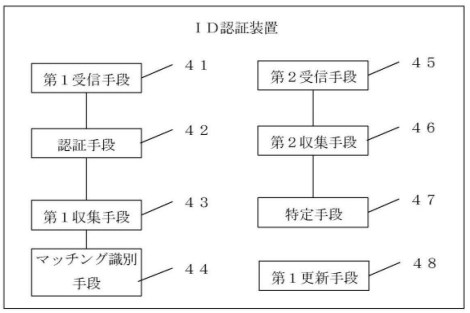
【図６】


ＩＤ認証装置
第１受信手段
４１
認証手段
４２
第１収集手段
４３
マッチング識別手段
４４
第２受信手段
４５
第２収集手段
４６
特定手段
４７

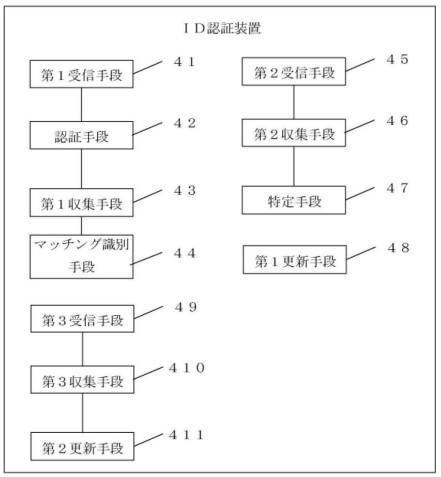
【図７】


マッチング識別手段４４
算出モジュール
４４１
特定モジュール
４４２

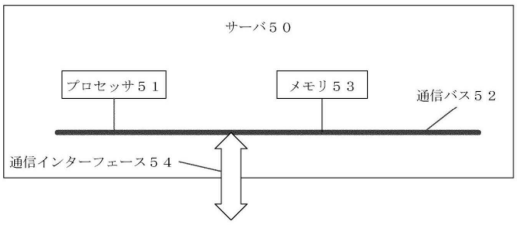
【図８】


ＩＤ認証装置
第１受信手段
４１
認証手段
４２
第１収集手段
４３
マッチング識別手段
４４
第２受信手段
４５
第２収集手段
４６
特定手段
４７
第１更新手段
４８

【図９】


ＩＤ認証装置
第１受信手段
４１
認証手段
４２
第１収集手段
４３
マッチング識別手段
４４
第３受信手段
４９
第３収集手段
４１０
第２更新手段
４１１
第２受信手段
４５
第２収集手段
４６
特定手段
４７
第１更新手段
４８

【図１０】


サーバ５０
プロセッサ５１
メモリ５３
通信バス５２
通信インターフェース５４

フロントページの続き

ディストリクト，ジゼン ビルディング シー，ジチュン ロード ナンバー７，フロア ５ス

審査官　岸野 徹

(56)参考文献　国際公開第２０１１／００１０２６（WO，Ａ１）
米国特許出願公開第２０１７／０２３０４１７（ＵＳ，Ａ１）
特開２０１７－１３８７２９（ＪＰ，Ａ）
特開２００８－１５８６８３（ＪＰ，Ａ）
特開２００３－０９９４０３（ＪＰ，Ａ）
特開２０１５－０８８１２２（ＪＰ，Ａ）
特開２０１７－０２１４０３（ＪＰ，Ａ）
特開２０１４－１４９８１１（ＪＰ，Ａ）
特開２０１７－２０７９７８（ＪＰ，Ａ）
特開２０１１－０５９８３７（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１