明　細　書

発明の名称

リレーション認証装置及びシステム

技術分野

本発明は、既存の技術とは原理的に異なるものであり、対象とする分野はシンプルでセキュリテイレベルの高い認証装置及びシステムに関する。

背景技術

背景となる技術は本人認証であり、これは個人や企業などといった要素（エレメント）の正当性を認証するものであった。本人認証であるパスワードや、その改良であるパスキーはユーザーの負担が大きく、サービス提供者が負担するコストが高く、IOTに対する適用限界があった。

先行技術文献

本発明と既存の技術（本人認証）は原理的に異なり、本発明と比較することが可能な先行技術は無く、比較可能な先行文献も無い。

発明の概要

発明が解決しようとする課題

解決しようとする課題は、先行技術の認証手続きが複雑であることから、これを簡単にすることや、セキュリテイに不安があることから、これを改善することなどである。

課題を解決するための手段

本発明は、関係継続の正当性によって認証することを最も主要な特徴とする。

発明の効果

本発明の認証システムは、ユーザーの手続きを簡略にし、コストを下げ、セキュリテイのレベルを高めるという利点がある。既存の認証システムでは実施の限界があったIOTにも適用可能である。

図面の簡単な説明

図１はリレーション認証装置の実施例のひとつを示した説明図である。

図２は本発明によるリレーション認証システムのひとつを示した説明図である。

発明を実施するための形態

多種多様に成立する関係性が、正当に継続されるように、関係継続の正当性を判定する照合部や照合システムが設定されることで実現した。

実施例１

はじめに、本発明の概要について説明する。本発明は背景技術（本人認証）とは原理的に異なり、用語や概念にも新規性があり、必要があって以下に詳細な説明が加えられている。本明細書において説明されている全ての手段やステップ、システム、施設、設備、機器、機能、技術などは、それぞれの実施例によって任意に組み合わされ、多様に構成されて本発明が適切に実施される。記載されている実施例は、すべて本発明の実施態様が適切なものになるよう組み合わされ、任意に構成されて目的を果たし効果を高める。

使用されている用語は実施例によって意味を持つ。例えば、センターは施設、基地局、システム、プラットフォーム、サーバーなどであり、実施例によってはクラウドを含む。

図１は本発明装置の１実施例を示す図であって、１は要素a、２は要素b、３はセンター、４は記憶部、５は照合部、６は要素cである。(要素a、b、cはユーザーに限られず、要素a、b、cが使用する端末や、端末に備える記憶部、処理部、出力表示部などを含み、各実施例の仕様に準ずる。）図２は本発明によるシステムのひとつを示した説明図である。システムがスタート（７）し、要素がセンターにアクセス（８）し、リレーションデータが作成（９）され、リレーションデータが記憶部に格納(１０）され、新たに要素がセンターにアクセス（１１）すると、リレーションデータが照合（１２）される。

「リレーション認証装置」及び「リレーション認証システム」という用語は広義の意味を持つものであり、情報を入力し出力し、処理し、記憶し、送受信し、システムを制御し、所定の機能を備える装置やシステムであり、形態としては、一般的にはスマートフォンやパソコン、センターやサーバー、プラットフォームなどである。

「情報」は伝達可能なものの全てであって、文字、記号、数、音声、映像、図画、コード、嗅覚対象物などを含む。

「要素」は単一の例と複数の例があり、個人、ユーザー、群や組織、システムの例などがある。政府機関、地方自治体、企業などの法人や個人、組織、機能、家電、車、交通システム、電力やガス、水道のインフラなどでもあり、認証装置およびシステムのユーザーや対象になりうるものの全てである。

センターや認証部（認証システムを含む。）などに設定される照合部（照合システムを含む。）なども要素であり、センターと個人のユーザーとの関係でも、これらは要素であって、リレーションが成立し、リレーションデータを作成する手段や当該システムやステップを備える。IOTの構成物も広く要素に含まれる。

社会における「関係」は要素と要素の間で成立する全ての関係であり、金員や物品の売買、授受、各種の情報の送受信、確認、契約や予約、さまざまな意思の伝達や表現などで

あり、情報によって形成できる関係の全てである。実施例によって関係は様々に意味を持つ。当該関係に関わる事象の全てを含む例もある。その例においては識別子は事象の内容や派生する現象なども含む。当該関係に関わる事象は分類されて、当該識別子によってそれらの分類から選別されて当該データが利用される。

本発明の実施例では、リレーションデータ（識別子）の照合によって、関係（リレーション）を成立させる手続きを進行させることの可否を判定する。リレーションは個人、通信販売会社、サービスや情報の提供会社、銀行、官公庁、病院、旅行会社などとの間でなされる生活やビジネス、教育、娯楽などの全般に関わる手続きや処理、取引き等の全てを含む。

「識別子」は文字、記号、数、音声、映像、図画、コード、嗅覚対象物などで構成される識別可能なものである。　本発明においては「識別子」を「リレーションデータ」として説明している。リレーションデータ（識別子）は要素の間で成立したリレーション（関係）を識別するために当該リレーションに付与されるものである。識別子を形成するものは識別可能なものであれば任意である。「数」は時刻である例もあり、また地点の座標位置を示す緯度経度の数値である例もある。識別可能であれば制約は無い。嗅覚対象物であっても機器や人や生物などが識別できるのであれば利用可能である。

識別子を作成する手段やシステムは、使用される端末、機器、手段、システムやセンター、クラウド、第三者の施設や機器、設備、手段、システムなどに設定される処理部など（処理システムを含む。）のいずれか、少なくともひとつに備えられている。または、これらを併用して識別子を作成する手段やシステムを備え、これらに備えられる記憶部や記憶システムに格納する手段やステップを備える。

リレーションデータを照合する手段やステップは、使用する端末、センター、認証センター、第三者の施設や機器、システムに備えられる処理部（照合部を備える処理部）や処理システムに備えられる。

ひとつの例を説明する。要素a、bは複数かつ多種である例を含む。要素aが要素bとの間で政治、経済、文化、娯楽、生活、教育、ビジネス、研究などを含む広い意味での社会における関係（一般的にはインターネットでの送受信によって発生する関係）を成立させるときに、前記関係を成立させる前記要素a、bに付与するID（識別可能な表記や多様なデータ）を作成する手段をセンター（サーバーやクラウドなどを含む。）は備える。リレーション（関係）は典型的にはインターネットを利用して形成されることが多いが、通信販売における売買、旅行やタクシー、飲食、コンサートなどの予約、銀行を利用する送金手続き、暗号資産の取引き、メールの送受信、個人や法人との契約、アプリケーションやサービスの利用、家電や車、病院、工場や交通インフラなどの制御などに関わる多種多様の関係がある。要素の種類は上記関係を成立させることが可能なものであれば制約は無い。

本発明の実施は主としてインターネットのラインで実行される。（以下において、手段は実施例に準じてステップの意味を持つ。

ひとつの例として、要素aがセンターにアクセスする手段（ステップ）を備え、センターにアクセス（ステップ）すると、センターは要素aのIDを作成する手段（ステップ）を備え、センターのIDを作成する手段（ステップ）を備え、さらに当該リレーションが実行された当該時間の任意のタイミングにおける時刻を記録する手段（ステップ）を備える。記録される数値は時刻ではなく、位置データの数値や、その他の任意の数値である例もある。数値ではなく識別可能な図画やコード、暗号である例もある。当該記録と前記要素aとセンターのIDによって構成、作成されたデータを、要素aとセンターとの当該リレーションに関わる照合データ（リレーションデータ）として記憶部に格納する手段（ステップ）を備える。

本発明の一般的な実施例のひとつを説明する。本人認証とは原理的に異なる本発明の認証装置において、要素Aと要素Bの間で関係が生じたときに、前記関係を他の関係と識別する識別子を作成する手段を備え、前記識別子を記憶部に格納する手段を備えるリレーション認証装置を実現する。本人認証ではパスワードや指紋、虹彩などの生体データによって認証がなされていた。いずれもユーザー（要素）によって設定、登録されるものであって負担があった。パスワード、指紋などの認証データを設定し、管理することについては、個人も企業もリスクとコストを負っていた。さらにセキュリテイーに不安があり、ゼロトラストという概念さえ受け入れられていた。本発明の実施例のひとつににによれば、識別子は認証装置によって作成され、ユーザー（要素）の氏名、住所、評価、実績、趣向などの属性データも識別子の管理とは別に管理される。識別子はインターネットのラインには限られた時しか上げられないことから盗用されるリスクが低減される。

センターの処理部によって識別子を作成する例とセンターと要素が識別子作成を分担する例がある。センターの処理部が要素が使用する端末の処理部に対して作成の指示を実行する例などである。要素A、Bが使用する端末が前記指示を受けて識別子を作成する実施例では、特に時刻については一致せず、齟齬する可能性がある。この例に鑑みて、一致することを照合における判定の要件とはせずに、要素A、Bが使用する端末の処理部は齟齬していることを認め、一致しなくとも正当であるとの判定を行う手段（ステップ）を備えるのが良い。当該判定は要素A、Bが使用する端末の処理部に限られない。センターや認証部などの処理部による判定である例もある。本明細書に示される定められた要件を充足するとの例の一つである。齟齬する時刻を正当であると認識するように設定されている。本発明における関係は、これに関わる事象の全てを含む実施例もある。事象の内容は整理、分類する手段を備えて評価の資料にし、あるいは統計的分析の対象にする手段を備えるのが望ましい。

実施例２

リレーション認証装置において、要素Aと要素Bの当該記憶部に格納された前記識別子を照合する手段を備え、前記照合によって前記識別子が定められた要件を充足するか否かを判定する手段を備え、前記要件を充足したとの判定をしたときに、前記要素Aと要素Bの間で関係が成立する手続きを継続することを承認する手段を備えることによって新規のリレーション認証装置を実現する。識別子の照合は、ひとつの例では、装置が備える照合部の処理手段によって実行される。識別子が照合部の処理手段に送給される構成は多様であり、他の実施例においても説明がされている。これについてはプロセスが設定され、あるいは記憶部への検索指示や送給指示などの手段を備える実施例がある。本明細書に記載されているように識別子の管理や、その態様は多様であり、認証部や専用端末との連携、不正介入に対する措置などが多彩に織り込まれている。秘匿される要素のリストによる防衛などでもリスクは低減されている。

識別子は一般的には要素Aと要素Bに付与されるIDと、当該リレーションがなされた時間に記録された時刻などによって構成される。前記IDと前記時刻をセンターが設定する実施例と、いずれかの一部を要素Aや要素Bが実行する例がある。要素Aや要素Bが全く関与せず、自己のIDなども知らない実施例もある。

識別子は関係が生じるたびに、その都度更新される例と、ランダムに、あるいは定めたタイミングや任意の機会に更新する例がある。

IOTや重要インフラ、暗号資産の取引など、リスクのレベルやセキュリテイの基準が異なり任意に適用されれば良い。

実施例３

既存の本人認証システムとは原理的に異なるリレーション認証システムである。要素Aと要素Bの間で関係が生じたときに、前記関係を他の関係と識別する識別子を作成するステップ１を備え、前記識別子を記憶部に格納するステップ２を備えることによって新規のリレーション認証システムを実施する。識別子の作成や、識別子の格納方法などについても多様に実施例が示されている。

実施例４

新規のリレーション認証システムであって、要素Aと要素Bの当該記憶部に格納された前記識別子を照合するステップ３を備え、前記照合によって前記識別子が定められた要件を充足するか否かを判定するステップ４を備え、前記要件を充足したとの判定をしたときに、前記要素Aと要素Bの間で関係が成立する手続きを継続することを承認するステップ５を備える。充足すべき要件は任意であって、暗号を介在させる例や図形や図画に変換して整合性の有無を判定する例などもある。

実施例のひとつとして、当該リレーションデータをセンターと要素aの端末の記憶部に格納する手段（システムの実施例においては、手段はステップと同じ意味を持つ場合がある。）を備える。要素aが次の機会にセンターとのリレーションを申し込む（センターにアクセスするステップ）と、センターはセンターの記憶部から前記リレーションデータを検索する手段（ステップ）を備え、要素aの端末の記憶部から前記リレーションデータを検索（ステップ）し、センターの処理部（あるいは認証部の照合部など）に送給するよう送給指示を要素aの端末の処理部に通知する手段（ステップ）を備える。センターの照合部、または認証部の照合部は前記リレーションデータを照合する手段（ステップ）を備える。この照合によってリレーションデータが一致する（または定められた要件を充足する）との判定（ステップ）をすると、要素aの新たな申し込みを承認する手段（ステップ）を備え、センターが要素aの申込みのための当該手続きを承認（ステップ）したときに要素aとセンターは所定の通信手段によって手続きを実行する手段（ステップ）を備える。

また例として、要素aがセンターを介して要素bとのリレーションの成立を希望し、センターに申し込みをした時は（ステップ）、センターは、要素aの端末の記憶部から要素aと要素bとの前回のリレーションデータを検索し、照合部に送給するよう送給指示を要素aの処理部に通知する手段（ステップ）を備え、同様に要素bの端末の記憶部からは要素aと要素bとの前回のリレーションデータを検索し、照合部に送給せよとの送給指示を要素bの端末の処理部に通知する手段（ステップ）を備える。センターの照合部、または認証部の照合部はリレーションデータを照合する手段（ステップ）を備える。前記照合によってリレーションデータが一致する（または定められた要件を充足する）か否かを判定する手段（ステップ）を備える。一致する（または要件を充足する）と判定（ステップ）したときは要素aと要素bの新たなリレーション成立のための手続きの進行をセンターの処理部が承認する手段（ステップ）を備える。要素aと要素bは所定の通信手段によって手続きを実行する手段（ステップ）を備える。インターネットを利用して関係（リレーション）を成立させるときに、過去にリレーション履歴（関係履歴）が無く初回であるときは、相手先のリストがある例と無い例がある。センターが管理する要素(ユーザー）であれば、センターが運用するリストを作成する手段（ステップ）を備える。

リストが無い例では、リレーションの申し込みを受ける要素bが政府機関や自治体、企業、店舗などであって、不特定の要素aの申し込みを予定していることが多く、そうした例では、センターはリレーションの成立を承認する手段（ステップ）を備え、本発明を実施するセンターと要素aは要素bの判断に従うことになる。

センターがリレーションを成立させるための手続きの進行や送受信を承認した以後は、所定の通信手段を使用し、要素bと要素aがリレーションの条件や内容を確認し、合意し了解したときに要素aと要素bのリレーションが正当に成立する。ひとつの例としては、センターがリレーションを成立させるための手続きの進行や送受信を承認した時刻が記録され、当該時刻によってリレーションデータを作成する。

要素a、bのいずれかがリレーションの申し込みを受ける例の一部では、当該ユーザーによって承認された相手先や内容でのリレーションに限られ、双方の確認や合意があったときにリレーションが成立する実施例もある。

実施例５

リレーションデータの異常処理の検出について説明する。リレーションデータの処理は多種多様であり、実施例の組み合わせにも制約が無く、数多くの処理例がある。（本明細書においては手段はステップの意味を持つ場合もある。）

識別子の作成、記憶部への格納、検索や処理部への送給、その他の処理や照合に至るプロセスに対して定められた過程（プロセス）を設定する手段を備え、当該処理が当該過程を経由したことを検出する手段（ステップ）を備え、当該過程を経由したことを証明するサインやスタンプ、IDを当該識別子に付与する手段（ステップ）を備え、前記定められた過程と異なる処理がなされたときに、異なる処理（異常処理）を検出する手段（ステップ）を備え、当該検出があったときに、新たな関係（リレーション）の成立に関わる手続きの進行を承認しない手段（ステップ）を備える実施例もある。

ひとつの例を示す。リレーションデータ（識別子）が偽造されて不正に使用される例である。偽造されたリレーションデータは定められたプロセスを経過せずに照合部に送給される可能性が高い。ひとつの例では、リレーションデータが記憶部から検索されずに、偽造され、または盗用されて照合部に送給される。記憶部から検索されたことを示すスタンプやサイン、IDが無いことから、定められたプロセスと異なる処理であるとの判定を実行する手段（ステップ）を処理部に備えて、リレーションを成立させる手続きの進行を承認しない手段（ステップ）を備える。

あるいは記憶部からリレーションデータを不正に検索する例では、センターの送給指示など、検索する前提や条件を充足していることを示すスタンプやサイン、IDが無いことから、定められたプロセスと異なる処理であるとの判定を実行する手段を処理部に備え、手続きの継続を承認しない手段を備える。

または、本来は不必要なプロセスを意図的に設定する手段を備え、そうしたプロセスを経由したときに、経由したことを記録する手段（ステップ）を備え、設定され定められたプロセスを経由しない手続きであれば不正な処理であると判定する手段（ステップ）を備える。この実施例は、重要なシステムやリスクの高いシステムでは有効であって、多くのプロセスを設定するのが望ましい。

当該プロセスを適宜にランダムに変更しても良い。利用者X、Yの例で説明する。Xの使用する端末Xa、及びXb（同様にYの使用する端末Ya、及びYb）の記憶部にリレーションデータを格納保存する手段（ステップ）を備える。センターや認証センター（実施例によっては、あるいはYa)の処理部が指示をXa、Xbの処理部に送信する手段（ステップ）を備える例では（実施例によっては指示にサインや暗号が伴う例もある。）、前記指示やサインが無いにも関わらずリレーションデータが当該記憶部において検索されたときは異常処理として判断する手段（ステップ）をセンターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が備える。

Xa、Xbの処理部がXa、Xbの記憶部から当該リレーションデータを検索する手段（ステップ）を備えるときにXa、Xbの処理部の当該検索処理（当該手段の作動）が無くリレーションデータが検索されたときは、異常処理として判断する手段（ステップ）をセンターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が備える。その他、Xa、Ya、Xb、Ybの記憶部に対するリレーションデータの検索について何らかのステップやフロー、手段（ステップ）や手続きなどが設定されているときに、前記ステップやフロー、手段や手続きなどが無く検索がなされたときは、異常処理として判断する手段（ステップ）をセンターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が備えるのが望ましい。

センター（サーバー、クラウド、アプリケーションの運用センターなどを含む。）や認証センターの記憶部にリレーションデータを格納保存する手段（ステップ）を備え、センターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が指示をセンターや認証センターの処理部に送信する手段（ステップ）を備える例では、前記指示やサインが無いにも関わらずリレーションデータが当該記憶部において検索されたときは異常処理として判断する手段（ステップ）をセンターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が備える。その他、記憶部に対するリレーションデータの検索について何らかのステップやフロー、手段や手続きなどが設定されているときに、前記ステップやフロー、手段や手続きなどが無く検索がなされたときは、異常処理として判断する手段（ステップ）をセンターや認証センター（実施例によっては、あるいはXa、Ya)の処理部が備えるのが望ましい。前記異常処理を検出したときは、検出されたリレーションデータを無効化する手段（ステップ）を備える。当該時点において、リレーションデータを作成する当該作成手段（ステップ）を備える例もある。当該作成手段によって新たにリレーションデータを作成し、当該記憶部に格納する手段（ステップ）を備える例もある。

前記異常処理は、各実施例において設定され構成されるステップ、フロー、プロセスなどの手続きや手順とは異なる処理であり、システムエラーの他、第三者の不正介入の可能性の高いものと推定する手段（ステップ）を備える。

異常処理の例を挙げる。検索されたリレーションデータは記憶部から送給されて処理部の処理を受けて照合されるが、そのプロセスにおいて所定の処理、送受信、照合などの対象として所定の当該処理を受けるように予定されている。

当該記憶部から検索され当該送受信部を介することが無いなどや、照合手段を備える照合の「場」（照合部）に当該リレーションデータが移行していないなどを検出する手段（ステップ）を備え、各実施例において設定され構成される任意の実施態様におけるステップ、フロー、手続きや手順、プロセスなどと異なる処理を異常処理として検出する手段（ステップ）を備える。

異常処理を検出するために意図的に検出を容易にするためのフローや手順、手段を組み込む例もある。検出することを目的として意図的に不要のプロセスを組み込み、当該プロセスを通過しないとき、当該手段の対象（リレーションデータを対象とする検出、確認、通過などを認知する手段の対象）とならないとき（対象となるべきものの不存在）などは異常処理として検出する検出手段（ステップ）を備えるのが望ましい。

前記検出手段は多様に実施可能であり所定のフローやプロセス、ステップ、手段、処理などのいずれかの（あるいは全ての）前後にリレーションデータを確認する手段（前記リレーションデータを対象とする検出、確認、通過などを認知する手段）を備える例もある。前記確認（前記検出、認知など）手段（ステップ）によって確認したときは通常の処理がなされたものとする例や、通常の処理と異なると当該処理部が判断したときは（当該判断をする手段を処理部は備え）、処理部は当該リレーションデータを無効化する手段を備える。例によっては、当該リレーションの当事者が使用する端末の記憶部に新規に作成するリレーションデータを配給する手段（ステップ）を備える。

実施例６

新規のリレーションデータを作成せずリレーション継続の正当性を承認しない実施例もある。（リスクの高いリレーションについては、手続きは中断され、当該リレーションの当事者の探索などが実行される例もある。）

異常処理は所定のフロー、ステップ、手段、手続き、処理、プロセスなどと異なる処理であって、所定のフロー、プロセスなどは実施態様によって異なり任意に設定される。所定のフロー、ステップ、手段、手続き、処理などが正常に実行される都度、当該のフロー、ステップ、手段、手続き、処理などが実行されたときにスタンプ（文字、記号など）をリレーションデータなどに付与する手段（ステップ）を備え、当該スタンプの有無を確認する手段（ステップ）を備え、当該スタンプが無いと判断したときは手続きを中断する手段（ステップ）を備える。当該リレーションデータをキャンセル（無効化）する手段（ステップ）を備え、当該時点で新たにリレーションデータを作成する手段（ステップ）を備える例もある。

異常処理の検出の具体的態様も任意であり、検出した時の対応（リレーションデータを無効化するか否かや新規のリレーションデータを作成するか否か、新規のリレーションデータを配給するか否かなど）も任意である。

実施例７

初回のリレーションである例では、リレーションの申し込みをした相手である要素bの属性、実績が不明であることから、申し込みをしたユーザー（要素a）に警告を与える手

段（ステップ）をセンターや要素aが使用する端末の処理部や処理システムが備え、要素aが確認をする手段（ステップ）を備え、当該確認があったときに、要素aの端末からセンターへ通知する手段（ステップ）を備え、センターは当該リレーションの成立を承認する手段（ステップ）を備える例もある。前記警告は前記端末の出力部によって実施される映像や文言、音声などでなされる表示であるのが一般である。または要素aが誤って、関係履歴の無い要素bにリレーションを申し込む例でも、要素aがセンターの指示を受けて確認を実行する手段（ステップ）や、センターが要素aの端末に警告を与える手段（ステップ）を備えるのが良い。

センターは、当該要素の通常のリレーションとは異なる種類や内容や数値の異常性を検出する手段（ステップ）を備えて、上記確認を実行する手段（ステップ）や、ユーザーの端末やリレーションの相手などに警告を与える手段（ステップ）を備える実施例もある。リレーションの内容や質、数量、金額の異常性を検出する（異常値検知の）手段（ステップ）や手法は任意である。一般的には統計的手法を利用する。

実施例８

リスクの大きなリレーションである例では、当該要素（ユーザー）が定められた地点に所在することを条件とする実施例もある。例として、当該要素が任意に定める地点であって、第三者が所在することが困難である地点や、警察署の近傍や銀行内部など安全性の高い場所などをリレーションを実行する地点として定める手段（ステップ）を備える。当該要素または当該端末が当該の定められた位置に所在することを、ブルートウース、局所電波、ICタグ、GPSなどの任意の手法で当該端末の位置の緯度経度や定められた位置との関連を確認する手段（ステップ）を備えることによって、当該要素の所在する位置と定められた位置を照合する手段（ステップ）を備える。例として定められた数値（位置の座標数値）と所在する位置の確認をする手段（ステップ）を備える。当該要素の所在位置が、定められた当該位置と一致するか否かを確認する手段（ステップ）を備え、確認をした時に、または当該端末が備える確認手段（ステップ）によって（当該位置を）確認したときに手続きの進行を承認するとの手段を備えるのが望ましい。こうした手段と本発明が併用されることで犯罪防止や安全性が向上する。

実施例９

マルウェアやウィルスの対処も本発明と併用されるのが望ましい。外部からの受信によって取得したデータ１からAIによって趣旨や内容を抽出する手段（ステップ）を備え、抽出された趣旨や内容によって新たにAIがデータ２を作成する手段（ステップ）を備える。前記データ２を外部から仮想的に隔絶された内部のシステムに送給する手段（ステップ）を備える。趣旨や内容を抽出した後の残余のデータ、またはデータ１は内部のシステムには送給せずに、これとは別の、内部のシステムとは隔絶されたシスムに備えられた分析部に送給する手段（ステップ）を備え、当該分析部は当該データを分析、あるいはウィ

ルスを培養する手段（ステップ）を備え、マルウェアやウィルスが認められた時は、当該データ１の送信者を探索し、または対処する手段（ステップ）を備えるのが良い。

実施例１０

認証装置及びシステムにおいて、要素と他の要素との間で過去において正当に成立した関係(または不成立となった関係）を関係履歴として記録する手段（ステップ）を備え、前記記録を（本明細書に記載されている実施例に示される）当該記憶部に記憶する手段（ステップ）を備える。記憶手段や記憶するステップは、センター（広義であって、プラットフォームやクラウドなどを含む。）や要素a、bが使用する端末などの処理部や処理システム、記憶部や記憶システムなどによって実行（ステップ）される。あるいは併用する専用端末の記憶部や記憶システムなどに格納する例などがある。記録を格納する手段やシステム、形態やツールなどは任意である。関係履歴の記録を前記要素（ユーザー）の端末やシステムに提供する手段（ステップ）を備え、要素a、bが使用する端末などの故障や紛失などの時に、新たにリレーションを成立させる条件や資格を回復する手段（ステップ）を備える。前記関係履歴を相手の要素やセンターなどに送給する手段（ステップ）を備え、当該関係履歴を送給する手段（ステップ）を備え、新たにリレーションを申し込みをする手段（ステップ）を備え、過去の実績として関係履歴を評価する手段（ステップ）を備え、新たにリレーションを成立させる手続きを可能とする手段（ステップ）を備える。

あるいは不成立であった履歴を記録する手段（ステップ）を要素a、bが使用する端末やセンターなどの記憶部に格納する手段（ステップ）を備え、不正防止のための資料にすることや、評価の資料にすることも望ましい。

実施例１１

認証装置及びシステムにおいて、要素が他の要素と関係（リレーション）を成立させるときに、他の要素の名称やIDなどを表記し、（リレーションの相手となる）要素を指定可能なリストとして前記要素に提供する手段（ステップ）を備える。リストは、これを利用する当該要素が識別可能で、申し込み先の相手を指示可能な表記であれば良い。表記は当該要素が認知可能な形態であれば良い。第三者には識別不可能な表記にし、不正に使用されることを防止するのが望ましい。当該要素が使用する端末の記憶部にリストを格納する例もある。端末の記憶部から検索する手段（ステップ）を備え、あるいはセンターからリストを端末に送給する手段（ステップ）を備えて、端末の出力表示部にリストを表示する手段（ステップ）を備える例において、当該端末のユーザー（要素）によって指紋や暗証番号などによって開示する手段（ステップ）を備え、第三者に対しては秘匿する手段（ステップ）を備えるのが良い。センターの記憶部に格納する例もあり、同様に当該要素の指紋や暗証番号などによって（センターから端末に送給する手段（ステップ）を備え）開示する手段（ステップ）を備え、前記開示する手段が実行されないときは前記リストを当該端末に送給しない手段（ステップ）を備えるのが良い。リストが秘匿されることによって

第三者が不正にリレーションを成立させることを防止でき、不正に関係履歴の無い相手先とのリレーションを成立させようとしたときも、当該要素に警告する手段（ステップ）を備え、また確認をする手段（ステップ）を備えて、当該要素とは無関係にリレーションを成立させる第三者の試みを防止することができる。リストを、要素a、bが使用する端末とは別に、これと併用する専用端末の記憶部に格納する例がある。この例においても、同様に当該要素の指紋や暗証番号などによって開示する手段（ステップ）を備える構成にし、秘匿する手段（ステップ）を備えるのが良い。

実施例１２

リストを備えるひとつの例について説明する。センターによって要素のリストを作成する手段（ステップ）を備える。リストは要素の評価（実績なども）も付加して作成する手段（ステップ）を備える。当該要素の当該評価はリレーションの相手に通知する手段（ステップ）をセンターに備える。トラブルや不正が無い年月とリレーションの実績や履歴数によって評価がなされる。要素a、bは評価の高い相手とのリレーションを希望するのが一般である。トラブルや不正が無い年月が長く、リレーションの内容が良質で規模が大きいものであれば評価は高くなる。

センターは、要素が使用する端末に、当該要素との間で実績のある要素を一覧できるリストを送給する手段（ステップ）を備える。リストを判読不可能である（秘匿された形態）状態で送給する手段を備えるのが望ましい。この例では、送給を受けた端末は判読可能な状態に変換する手段（ステップ）を備える。ひとつの例としては、当該要素が暗証番号や生体データを入力する手段（ステップ）を備え、あるいは暗号やコードを端末に入力する手段（ステップ）を備える。この実施例によれば、リストが第三者に対して秘匿されることが可能になる。その効果として、当該要素が知らない、過去に実績の無い要素とのリレーションが当該端末によって実行されるリスクが低減され、当該端末が不正に使用されて当該要素に損害を与えることを防止することができる。

実施例１３

リストを秘匿する手段としてUSBメモリーやクラウド、メモなどの記録媒体が併用される例もあり、リカバリー（端末の故障や紛失したときの手続きを回復する手段）のために併用される例もある。リカバリーについてはリストの利用以外に、リレーションデータをUSBメモリーやクラウド、メモ、その他の任意の手段によって保管する手段（ステップ）を備え、当該リレーションデータをセンターに送信することで、センターと要素との関係において、当該資格を回復させる手段（ステップ）とすることもできる。

リレーションデータは、センターが要素の当該資格を確認することに利用できればよく、任意の時機に任意のリレーションデータを、センターの判断で当該要素が使用する端末などに送給する手段（ステップ）を備える。当該要素はUSBメモリーやクラウド、メモ、その他の任意の手段（ステップ）によって保管する手段（ステップ）を備える。リカバリーの際に当該要素が任意の端末で前記リレーションデータをセンターに送信する手段

（ステップ）を備える。センターは受信したリレーションデータが真正であるか否かを判断する手段（ステップ）を備える。真正であと判断した時は当該要素の資格を回復する手段（ステップ）を備える。当該資格を回復した要素には前記リストを当該端末に送給する手段（ステップ）を備える。

実施例１４

リレーションを申し込む要素aと申し込みを受けた要素bがセンターによってリレーションを成立させる手続きを承認されると、要素aと要素bは、任意の通信手段（センターが介在する例と介在しない例がある。）で送受信を行う手段（ステップ）を備える。正当に、またトラブルが無く要素a、bによってリレーションが成立したときに、センターは要素a、bに新しいリレーションデータを付与する手段（ステップ）を備える。付与する手段（ステップ）や対象についてはいくつかの形態がある。要素a、bの端末、設備や施設の機器と、これらが備える当該記憶部や処理部である例、センターの設備、施設の機器と、これらが備える当該記憶部や処理部である例、システムの記憶部や処理部である例、認証を専門的に担当する認証部の設備や施設の機器と、これらが備える当該記憶部や処理部である例、クラウドの記憶部や処理部である例、要素a、bの端末の他に要素a、bが使用する専用端末と、これらが備える記憶部や処理部などが付与の対象として使用される例などがある。

実施例１５

リレーションデータは文字、記号、数、音声、映像、図画、コード、嗅覚対象物などで構成され、識別性があり識別可能であれば識別素材は任意である。識別の手段（ステップ）や手法、主体は人によるか、動物によるか、機器によるかも任意である。典型的にはリレーションデータは文字、記号、数によって構成される。リレーションが、要素a、b（多数でも可能。要素の数は任意であり、センターと要素とのリレーションでは要素は単数である例もある。）によってリレーションが正当に成立した時刻や、要素a、bの少なくとも1人（またはひとつ）が所在した位置（緯度経度）のX、Yの座標の数値と、センターによって要素に対して付与されたIDが組み合わされてリレーションデータを形成する手段（ステップ）を備える。これらのリレーションデータを作成する手段（ステップ）をセンターも備える。リレーションデータの作成者は、センターに限定せず、要素a、bのいずれか、あるいはリレーションデータ作成を専門に担当する施設やシステムを作成者として作成手段（ステップ）を備える例もある。

実施例１６

別の実施例のひとつを示す。センターはリレーションが成立した時刻に要素a、bの端末と、これに関連するシステムや施設、機器、認証部などが備える処理部に、共通する同じ時刻を記録するように指示する手段（ステップ）を備える。（時差を無視した地球の全地域で共通する時刻が望ましい。この例ではセンターが独自に経時的に進行する時刻を管理する手段、機能を備える。）またセンターが作成する要素a、b（または要素a、bが使用する端末）のIDを要素a、bの端末とこれに関連するシステムや施設、機器、認証部などが備える処理部に送給する手段を備える。要素a、b（または要素a、bが使用する端末）のIDと時刻がインターネットのラインに送給されることがないのでリレーションデータが盗用されるリスクを低減することができる。

実施例１７

ひとつの例として、本発明を実施する装置及びシステムは、リレーションデータを分担して記憶部に格納する手段（ステップ）を備える。あるいは要素a、bの端末とこれに関連するシステムや施設、機器、認証部などが備える処理部はリレーションデータを記憶部に格納する手段を備える。

典型的な実施例では、センターはリレーションが成立した時刻に要素a、bの端末に共通する同じ時刻を記録するように指示する手段（ステップ）を備える。要素a、b（または要素a、bが使用する端末）にIDを付与する手段（ステップ）を備え、上記時刻と上記IDでリレーションデータを作成する手段（ステップ）を要素a、bの端末の処理部は備える。新たに要素a、bが新しくリレーションを成立させる機会に、前記端末の処理部は、前記リレーションデータをセンターの指示を受けてセンターに送給する手段（ステップ）を備える。センターあるいは認証部の照合部は当該リレーションデータを照合する手段（ステップ）を備える。この手段（ステップ）の構成は、事前においてインターネットのラインにリレーションデータを出さないことを目的としている。当該リレーションデータがインターネットのラインに出るのは照合される時点に限られることから盗用や偽造のリスクを減少させることができる。

実施例１８

リレーションデータを分散して格納する手段（ステップ）を備え、照合される時点で照合部に送給する手段（ステップ）を備える構成も同じ効果を持つ。照合部に送給されるまでは要素a、bが使用する端末の記憶部と、これと併用する専用端末の記憶部と、センターの記憶部と、これと併用される記憶部、その他の併用される記憶部にリレーションデータを分散して格納する手段を備える。照合する時点において当該記憶部から（分散して格納

された）リレーションデータを照合部に送給する手段（ステップ）を備える実施例もある。この構成によればリレーションデータがインターネットのラインに出るのは照合の時点に限定されるので盗用されるリスクが減少する。

実施例１９

この実施例では分散されたリレーションデータのパーツ（部分）を検索する手段として、前記パーツに検索のためのIDを付与する手段（ステップ）を備える。当該リレーションデータのパーツを当該IDによって検索する手段（ステップ）を備える。当該記憶部から当該パーツを取り出して照合部に送給する手段（ステップ）を備える。

実施例２０

要素a、bが使用する端末の記憶部と、これと併用する専用端末の記憶部にリレーションデータやリレーションデータのパーツを格納しない実施例もある。この実施例では、要素a、bが使用する端末の記憶部に当該リレーションデータやリレーションデータのパーツを検索するためのIDを格納する手段を備える。照合部に併設される記憶部に当該リレーションデータやリレーションデータのパーツを格納する手段を備える。当該記憶部から当該リレーションデータやリレーションデータのパーツを取り出す手段（ステップ）を備え、照合部に送給する手段（ステップ）を備える実施例もある。この実施例によればリレーションデータがインターネットのラインに出ることによるリスクは軽減される。

実施例２１

照合部の照合手段によって照合され、定められた要件を充足していると判定される根拠は多種多様である。要素a、bやセンター、認証部などの記憶部から取り出され照合部に送給されたリレーションデータが一致することで照合要件を充足すると判定する例や、一致するのではなく、定められた要件に従って「整合」（当該要件を満たしていること）することで照合要件を充足すると判定する例、送給されたリレーションデータによって定められた要件を充足する例などがある。この例における「要件」は様々であり整合、重合、混合によって有意性を持つことなどであり任意である。リレーションデータに暗号が組み合わされて要件を充足する例もある。

本発明を実施するシステムによれば、照合部の照合手段によって照合され、要件を充足していると判定されたときは、当該要素a、bのリレーションを成立させる手続きの継続を承認する手段（ステップ）を備える。当該要素a、bはセンターと照合部、記憶部と処理部、ユーザーとユーザーが使用する専用端末などの実施例もある。照合され要件を充足していないと判定されたときは、当該要素a、bのリレーションを成立させる手続きの継続を承認しない手段（ステップ）を備える。リレーションを成立させる手続きの継続が承認されると、所定の送受信手段の利用を可能にする手段（ステップ）を備える。送受信手段は

センターが管理運用する通信手段でもよく、あるいは他の通信事業者が管理運用する通信手段でもよい。

実施例２２

要素a、bの属性データはセンターによって格納、保管され、利用や運用などがなされる例もあるが評価システムが併用されるのが望ましい。　明細書に記載されている手順、方法、手法、ステップ、手段、機能、構成、機器、装置、取り扱いなど、また各態様の実施例など、多種多様にいずれも任意に組み合わされて実施される。

前記センターがリレーションデータを作成するのが一般であるが、実施例のひとつとして、リレーションの任意のタイミングで記録される時刻は世界標準時としてもよく、またはセンターが独自に進行させる時刻でも良い。時差を配慮しない地球の全地域に共通する時刻でも良い。経時的に進行するものであればよい。記録される時刻に付帯される要素a、bのIDは利用者やセンターに由来するものである必要はなく、作成者の任意とし、当該リレーションデータによって利用者を検索し特定する識別性を有する手段を備えればよく、リレーションデータと利用者が直接に関連つけられないデータ形式とするのが望ましい。当該リレーションデータによって利用者を検索する手段、もしくは利用者のIDによってリレーションデータを検索する手段に第三者がアクセスすることを防止する手段を備えるのが望ましい。

ひとつの例として、リレーションデータが作成されると、作成者のシステムの記憶部に格納保存される例１と、リレーションの当事者に配給される例２、インターネットなどのネットワークに送給される例３があり、例１は例２、例３と併用されるのが一般とされ、例１では主としてセンター（サーバーやサイト、クラウド、取引所などを含む。）を例とするが、ひとつの例として、センターのシステムの記憶部１に、センターが関わるリレーションに付与されるリレーションデータを格納保存する手段（ステップ）を備え（記憶部１、２はトラブルに備える目的によって設置）、センターのシステムの記憶部２に利用者（要素、ユーザー）に関わるリレーションに付与されるリレーションデータを格納保存する手段（ステップ）を備え、いずれかの利用者がリレーションの申請をしたときに当該利用者のIDとセンターのIDによって当該リレーションデータ（当該利用者とセンターとのリレーションに付与されたデータ）を記憶部１、２から検索する手段（ステップ）を備え、リレーションデータを照合する照合部に移行する手段（ステップ）を備え、承認の申請を受けたリレーション成立の手続きにセンターと異なる相手（複数であり、また不特定多数である例を含む。）が存在するときは、相手のID（複数であり、また不特定多数である例では「群」としてIDを付与する手段（ステップ）を備える。）によって記憶部から（相手に付与された）リレーションデータを検索する手段（ステップ）を備え、これら（当該リレーションに関わる当事者）のリレーションデータを照合する手段（ステップ）を備えて、定められた要件を充したと判定したときは当該リレーションを承認する手段（ステップ）を備える。

例２において、当該リレーションに相手が存在せず利用者と前記センターとのリレーションである例では、リレーション手続きの申請者のリレーションデータを記憶部２にお

いて当該利用者のIDによって検索する手段（ステップ）を備え、これに前後してセンターの処理部は利用者の端末の処理部にリレーションデータの送信を指示する手段（ステップ）を備える。

例によっては利用者に送信を指示する手段（ステップ）を備える。利用者は端末を操作して端末の記憶部からリレーションデータを取り出しセンターに送給する手段（ステップ）を備える例もある。利用者の端末の処理部は前記指示を受けて記憶部から利用者とセンターの最後のリレーションに付与されたリレーションデータ（利用者とセンターのIDが付与されている。）を検索する手段（ステップ）を備える。端末の記憶部はリレーションデータ専用の記憶部Bを備え、リレーションデータ以外のデータは記憶部Aに格納保存する手段（ステップ）を備える。前記処理部が記憶部Bにアクセスすることを制限する手段（ステップ）を備え、処理部ⅱが記憶部Bに前置され、処理部は処理部ⅱにセンターの処理部から送信されたサイン（文字、記号、数列など任意の記述によって作成）を添付する手段（ステップ）を備える。センターの処理部は前記サインを端末の処理部に送信する手段（ステップ）を備える。

前記サインが添付された指示にのみ従う手段（ステップ）を記憶部は備える。記憶部Bを独立して備える専用端末を使用する例があり、利用者が使用する端末とは有線、無線（非接触であり、ブルーツース他任意である。）によって送受信する手段（ステップ）を備え、前記と同じくセンターの処理部から送信される前記サインが添付された時のみ処理部の指示に従う手段（ステップ）を備える。前記サインを伴う指示を受けると端末と専用端末の処理部は記憶部から当該リレーションデータを検索する手段（ステップ）を備え、（専用端末の処理部は前記送受信部を介して前記端末の処理部にリレーションデータを送給する手段（ステップ）を備え）、端末の処理部は送受信部を介してセンターの処理部に当該リレーションデータを送給する手段（ステップ）を備え、センターの処理部は当該データを照合の「場」に移行する手段（ステップ）を備え、当該「場」でセンターの記憶部で保存されたリレーションデータと端末の記憶部や専用端末の記憶部から送旧されたリレーションデータを照合する手段（ステップ）を備え、定められた要件を充したと判定されたときにセンターと申請者のリレーションを承認する手段を備える。

例２において、いずれかの利用者がリレーションの申請をしたときに当該利用者と相手のIDによって当該リレーションデータを記憶部２から検索する手段（ステップ）を備え、リレーションデータを照合の「場」に移行する手段（ステップ）を備え、これに前後してセンターの処理部は相手の端末の処理部にリレーションデータの送信を指示する手段（ステップ）を備える。例によっては相手に送信を指示する手段（ステップ）を備える。相手は端末を操作して端末の記憶部からリレーションデータを取り出しセンターに送給する。

相手の端末の処理部は前記指示を受けて記憶部から申請者と相手の最後のリレーションに付与されたリレーションデータ（申請者と相手のIDが付与されている。）を検索する手段（ステップ）を備えるが、端末の記憶部はリレーションデータ専用の記憶部Bを備え、リレーションデータ以外のデータは記憶部Aに格納保存する手段（ステップ）を備え、前記処理部が記憶部Bにアクセスすることを制限する手段（ステップ）を備え、処理部ⅱが記憶部Bに前置され、処理部は処理部ⅱにセンターの処理部から送信されたサイン

（文字、記号、数列など任意の記述によって作成）を添付する手段（ステップ）を備える。センターの処理部は前記サインを端末の処理部に送信する手段（ステップ）を備える。前記サインが添付された指示にのみ従う手段（ステップ）を記憶部は備える。

記憶部Bを独立して備える専用端末を使用する例があり、端末とは有線、無線（非接触であり、ブルーツース他任意である。）によって送受信する手段（ステップ）を備え。前記と同じくセンターの処理部から送信される前記サインが添付された時のみ処理部の指示に従う手段（ステップ）を備える。前記サインを伴う指示を受けると端末と専用端末の処理部は記憶部から当該リレーションデータを検索する手段（ステップ）を備える。専用端末の処理部は前記送受信部を介して前記端末の処理部にリレーションデータを送給する手段（ステップ）を備える。端末の処理部は送受信部を介してセンターの処理部に当該リレーションデータを送給する手段（ステップ）を備え、センターの処理部は当該データを照合の「場」に移行する手段（ステップ）を備え、当該「場」（照合部）でセンターの記憶部で保存されたリレーションデータと端末の記憶部や専用端末の記憶部から送給されたリレーションデータを照合する手段（ステップ）を備え、定められた要件を充したと判定されたときに申請者と相手とのリレーションの成立を承認する手段を備える。

実施例２３

例３では分散管理、ブロックチェーン、Web3と言われるネットワークに象徴されるシステムであって、不特定多数が確認可能であっても特定のデータの所在が定まっていない例においては特定のデータを検索対象とすることはできないが、リレーションデータをネットワークに保存する手段（ステップ）を備え、前記リレーションデータを検索する手段（ステップ）を備えることによってリレーション認証システムを機能させることが可能である。当該利用者のリレーションに付与されたリレーションデータ（少なくとも初期の設定時のリレーションデータ）を最後のリレーションの内容（当該利用者の取り引きの内容と結果）に付与する手段（ステップ）を備え、当該リレーションデータを前記ネットワークにおいて検索する手段（ステップ）を備え、当該リレーションデータに付帯するリレーションの内容を確認する手段（ステップ）を備えることが望ましい。

センターが関与せず利用者XとYによって実行されるリレーションの例があり、この例ではXとYのいずれかがリレーションデータを作成する手段（ステップ）を備えるか、または当該アプリケーションによって自動的にリレーションデータを作成する手段（ステップ）を備え、両者が当該端末のシステムの記憶部に格納保存する手段（ステップ）を備え、リレーションの申請がなされると自動的にリレーションデータを相互に送受信する手段（ステップ）を備え、端末の処理部は照合する手段（ステップ）を備え、リレーションデータが定められた要件を充したと判定されたときにリレーション成立を可能とする手段（ステップ）を備えるとするのが望ましい。

この例において、XとYのリレーションの内容やリレーションデータは前記ネットワークでは「分散管理」によって格納保存する手段（ステップ）を備え、必要に応じてリレーションデータを検索する手段（ステップ）を備え、リレーションデータに付帯するリレーションの内容を確認する手段（ステップ）を備え、当該内容に基づいて確認された資産状

況を回復する手段（ステップ）を備えるのが望ましい。
リレーション認証システムによれば、センター（アプリケーションの運用者やサーバーなどを含む。）は利用者のデバイス（パソコンやスマートフォンなど）の処理部に記憶部から検索しセンターにリレーションデータを送信するよう指示する手段（ステップ）を備え、指示を受けるとデバイスの処理部は利用者の操作がなくとも当該指示に従う手段（ステップ）を備えることから、例として資格や条件を備えた全ての利用者に一括してリレーションを申請する手段（ステップ）を備え、利用者も資格や条件を備えていれば一括して他の利用者にリレーションを申請する手段（ステップ）を備える例がある。

実施例２４

広い意味での認証装置及びシステムにおいて、政府機関や企業や個人などの要素（社会を構成するエレメント）によって生成される人為的な行為や事象によって構築される、社会における関係（人為的な行為や事象によって成立する関係性）を成立させるときに、前記関係を成立させる前記要素に付与する識別子（識別可能な表記であり、コード、図柄、音声などを含み任意のもの）を作成する手段（ステップ）を備え、（任意の形態、手法によって）前記要素に前記識別子を付与する手段（ステップ）を備え、前記識別子を（利用可能な任意のものであってクラウドなどを含む記憶部に記憶する手段（ステップ）を備え、前記要素の間において（初回や次回を含む。）新たに関係を成立させるときに、前記記憶された前記識別子を照合する手段（ステップ）を備え、前記照合によって前記識別子が定められた要件を充足するか否かを判定する手段（ステップ）を備え、充足したとの判定をしたときに、前記新たな関係を成立させることを承認する手段（ステップ））を備える。

実施例２５

広い意味での認証装置及びシステムにおいて、前記要素が社会における関係を成立させるときに、前記関係を成立させる前記要素に付与する識別子を作成するステップ１を備え、前記要素に前記識別子を付与するステップ２を備え、前記識別子を記憶部に記憶するステップ３を備え、前記要素の間において新たに関係を成立させるときに、前記記憶された前記識別子を照合するステップ４を備え、前記照合によって前記識別子が要件を充足するか否かを判定するステップ５を備え、充足したとの判定をしたときに、前記新たな関係を成立させることを承認するステップ６を備える。

実施例２６

認証システムにおいて、　本発明の実施は主としてインターネットのラインで実行される。例として、要素aがセンターにアクセスする（ステップ１）。センターは要素aのIDを作成する（ステップ２）。センターのIDと要素aのIDにさらに当該リレーション
が実行された時間帯の任意のタイミングでの時刻を記録する（ステップ３）。当該記録と前記IDによって作成されたデータを、要素aとセンターとの照合データ（リレーショ

ンデータ）とする（ステップ４）。当該リレーションデータをセンターと要素aの端末の記憶部に格納する（ステップ５）。要素aが次の機会にセンターとのリレーションを申し込む（ステップ６、センターにアクセスする）と、センターはセンターの記憶部から前記リレーションデータを検索する（ステップ７）。要素aの端末の記憶部から前記リレーションデータを検索する（ステップ８）。センターの処理部（あるいは認証部の照合部）に送給せよとの指示を要素aの端末の処理部に通知する手段を備える（ステップ９）。センターの照合部、または認証部の照合部はリレーションデータを照合する手段を備える（ステップ１０）。この照合によって前記リレーションデータが一致する（あるいは定められた要件を充足する）と判定する（ステップ１１）と要素aの新たな申し込みについては、センターが当該の申込の手続きの継続を承認する（ステップ１２）。
ひとつの実施例において、要素aがセンターを介して要素bとのリレーションの成立を希望し、センターに申し込みをした時は、センターは、要素aの端末の記憶部から要素aと要素bとの前回のリレーションデータを検索し（ステップ１３）、要素bの端末の記憶部から要素aと要素bとの前回のリレーションデータを検索し（ステップ１４）、センターの処理部または照合部（あるいは認証部の処理部または照合部）に送給せよとの指示を要素aと要素bの端末の処理部に通知する（ステップ１５）。センターの照合部、または認証部の照合部は前記リレーションデータを照合し判定する（ステップ１６）。この照合によってリレーションデータが一致する（あるいは定められた要件を充足する）か否かを判定する（ステップ１６）。一致する（あるいは定められた要件を充足する）と判定したときは要素aと要素bの新たなリレーション成立の手続きの継続をセンターの処理部が承認する（ステップ１６）。

実施例２７

認証システムにおいて、前記要素が他の要素と関係（リレーション）を成立させるときに、他の要素を表記し当該要素を指定可能なリストを前記要素に提供する（ステップ１）。当該要素が使用する端末の記憶部にリストを格納する例もあるが、指紋や暗証番号などによって当該端末の出力表示部において開示される（ステップ２、前提として秘匿する手段を備えるのが良い）方法が良い。センターの記憶部に格納する例もあり、同様に当該要素の指紋や暗証番号などによって開示する（ステップ２）。前記開示する手段が実行されないときは前記リストを秘匿する手段を備える（ステップ３）。リストが秘匿されれば第三者が不正にリレーションを成立させることを防止することができる（ステップ４）。不正に関係履歴の無い相手先とのリレーションを成立させようとしたときも、当該要素に警告をし（ステップ５）、また確認をする手段を備え（ステップ６）、当該要素とは無関係にリレーションを成立させる試みを防止する（ステップ７）。リストを、要素a、bが使用する端末とは別に、これと併用する専用端末の記憶部に格納する例がある。

この例においても、同様に当該要素の指紋や暗証番号などによって開示する構成にし、秘匿するのが良い。

実施例２８

要素aが要素b（要素a、bは複数かつ多数である例を含む。）との間で政治、経済、文化、娯楽、生活、教育、ビジネス、研究などを含む広い意味での社会における関係を成立させるときに、前記関係を成立させる前記要素a、bに付与する識別子（IDなど）を作成する（ステップ１）。過去にリレーション履歴（関係履歴）が無く初回であるときは相手先のリストがある例と無い例がある。センターが管理する要素（ユーザー）であれば、センターが運用するリストを作成している。リストが無い例では、リレーションの申し込みを受ける要素bが政府機関や自治体、企業、店舗などであって、不特定の要素aの申し込みを予定していることが多いので、センターはリレーションの成立を承認する（ステップ２）。本発明を実施するセンターは要素bの判断に従う（ステップ３）。

センターがリレーションを成立させるための手続きや送受信を承認した以後は、要素bと要素aがリレーションの条件や内容を確認する（ステップ４）。合意し了解したときに要素aと要素bのリレーションが正当に成立する（ステップ５）。要素a、bのいずれかがリレーションの申し込みを受ける例では、当該ユーザーによって承認された相手先や内容でのリレーションに限ってリレーションを成立させるための手続きを承認する（ステップ６）、要素aと要素bとの確認や合意があったときにリレーションが成立する（ステップ７）。

実施例２９

要素と他の要素との関係を関係履歴としてセンターの記憶部に記憶する（ステップ１１）。前記関係履歴を前記要素が使用する端末に提供する（ステップ１２）。

実施例３０

要素と他の要素との関係を関係履歴としてセンターの記憶部に記憶する手段を備え、前記関係履歴を前記要素が使用する端末に提供する手段を備える。要素Aがセンターとの間で関係を成立させ、要素Bがセンターとの間で関係を成立させ、要素Bが要素Aとの間で関係を成立させる。センターは要素Aと要素Bのいずれかから、あるいは両者からリレーションを成立させる申し入れを受けると、センターと要素A、センターと要素Bの識別子を照合する手段を備え、当該識別子の有効性を確認する手段を備え、有効性を確認した時に、センターと要素A、センターと要素Bの識別子から要素Aと要素BのIDを抽出する手段を備え、当該関係に関わる時刻（時刻以外の数値や記号などの例もある。）などを付加する手段を備え、要素Aと要素Bの関係に付与される識別子を作成する手段を備える。

関係履歴の管理や識別子の作成と管理などはセンターが担当するのが合理的であるが、機能や手段などをセンターや端末などがどのように分担するかはコストやリスク、セキュリテイの基準などによって配慮される。要素とセンターとの間に付与される識別子は任意に更新する手段（ステップ）を備え、要素の存否、名称や住所、信用状況などの属性の変化を反映させる手段（ステップ）を備える。実施例のひとつとして、要素の前記属性データはセンターが格納保存する手段（ステップ）を備え、管理する手段（ステップ）を備える。関係の類別や特性に応じて、また要素の属性や権限に応じて要素の属性データの利用（提供など）を実行する手段（ステップ）を備える。この例においては要素の属性データは要素の権限や、要素間の約定などで設定された条件に適応するよう分類し管理する手段（ステップ）を備える。

産業上の利用可能性

取引先の確認や、多種多様なIOTにおけるセキュリティなどにおいて、既存の技術では不可能であった分野についても認証システムとして利用できる。特になりすましを防止する効果は大きい。

符号の説明

１　要素ａ
２　要素ｂ
３　センター
４　記憶部
５　照合部
６　要素ｃ
７　スタート
８　センターにアクセス
９　リレーションデータの作成
１０　データの格納
１１　センターにアクセス
１２　データの照合

請求の範囲

［請求項１］

認証装置において、要素Aと要素Bの間で関係が生じたときに、前記関係を他の関係と分別する識別子を作成する手段を備え、前記識別子を記憶部に格納する手段を備えることを特徴とするリレーション認証装置。

［請求項２］

請求項１記載のリレーション認証装置において、前記記憶部に格納された前記識別子を照合する手段を備え、前記照合によって前記識別子が定められた要件を充足するか否かを判定する手段を備え、前記要件を充足したとの判定をしたときに、当該要素の間で関係が成立する手続きを継続することを承認する手段を備えることを特徴とするリレーション認証装置。

［請求項３］

認証システムにおいて、要素Aと要素Bの間で関係が生じたときに、前記関係を他の関係と分別する識別子を作成するステップ１を備え、前記識別子を記憶部に格納するステップ２を備えることを特徴とするリレーション認証システム。

［請求項４］

請求項３記載のリレーション認証システムにおいて、前記記憶部に格納された前記識別子を照合するステップ３を備え、前記照合によって前記識別子が定められた要件を充足するか否かを判定するステップ４を備え、前記要件を充足したとの判定をしたときに、当該要素の間で関係が成立する手続きを継続することを承認するステップ５を備えることを特徴とするリレーション認証システム。