(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6155675号
(P6155675)

(45)発行日　平成29年7月5日(2017.7.5)　(24)登録日　平成29年6月16日(2017.6.16)

(51)Int.Cl.　F I
G06F 21/33 (2013.01)　G06F 21/33
G06F 21/31 (2013.01)　G06F 21/31

請求項の数 8　(全 23 頁)

(21)出願番号　特願2013-22608(P2013-22608)
(22)出願日　平成25年2月7日(2013.2.7)
(65)公開番号　特開2014-153884(P2014-153884A)
(43)公開日　平成26年8月25日(2014.8.25)
審査請求日　平成28年1月28日(2016.1.28)

(73)特許権者　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人　100106149
弁理士　矢作　和行
(74)代理人　100121991
弁理士　野々部　泰平
(74)代理人　100145595
弁理士　久保　貴則
(72)発明者　田口　晋也
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
(72)発明者　金森　貴志
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内

最終頁に続く

(54)【発明の名称】認証処理方法および認証処理装置

(57)【特許請求の範囲】
【請求項１】
移動体である利用者端末（２）を認証することにより提供者端末（３）の利用可否を判定する認証処理方法において、
前記提供者端末（３）から離れて設置された認証端末（４）に設けられ、複数の前記提供者端末（３）を示すキー情報を記憶する提供者情報記憶部（４３）から、一部の前記提供者端末を示すキー情報だけを、前記利用者端末（２）のキー記憶部（２７）へ配信し記憶させる配信工程（１５０、１６０）と、
前記キー記憶部（２７）に記憶されたキー情報を前記利用者端末（２）から前記提供者端末（３）に入力する入力工程（１７４、１７５、１８３、１８７）と、
前記提供者端末に入力された前記キー情報に基づいて、前記提供者端末（３）において、前記提供者端末（３）の利用可否を判定するキー情報判定工程（１８８、１８９）とを有し、
前記配信工程は、前記利用者端末（２）に関する位置情報と前記提供者端末（３）に関する位置情報とに基づいて、前記利用者端末による前記提供者端末の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る前記利用者端末（２）と前記提供者端末（３）とを関連付け、関連付けられた前記提供者端末（３）を示す前記キー情報を、関連付けられた前記利用者端末（２）に配信し、
さらに、前記利用者端末に設けられた主認証情報記憶部（２６）に記憶された主認証情報に基づいて、前記認証端末（４）において、前記提供者端末（３）の利用可否を判定す

る主認証工程（１７１、１７２、１８１、１８２、１８４、１９０）を備え、
前記キー情報判定工程は、前記主認証工程が完了できないときに、前記主認証工程に代わって、前記提供者端末（３）の利用可否を判定することを特徴とする認証処理方法。
【請求項２】
前記配信工程は、前記利用者端末（２）に関する位置情報に含まれる前記利用者端末の現在位置、未来位置、および過去位置の少なくともひとつに基づいて前記利用者端末（２）と前記提供者端末（３）とを関連付けることを特徴とする請求項１に記載の認証処理方法。
【請求項３】
前記配信工程は、特定の前記利用者端末（２）に関連付けられるひとつまたは複数の前記提供者端末を示す前記キー情報を、特定の前記利用者端末（２）に配信することを特徴とする請求項１または請求項２に記載の認証処理方法。
【請求項４】
前記配信工程は、前記主認証工程が完了できない特定の前記提供者端末（３）を示す前記キー情報を、特定の前記提供者端末（３）に関連付けられるひとつまたは複数の前記利用者端末に配信することを特徴とする請求項１から請求項３のいずれかに記載の認証処理方法。
【請求項５】
移動体である利用者端末（２）を認証することにより提供者端末（３）の利用可否を判定する認証処理装置において、
前記提供者端末（３）から離れて設置された認証端末（４）に設けられ、複数の前記提供者端末（３）を示すキー情報を記憶する提供者情報記憶部（４３）と、
前記利用者端末（２）に設けられ、前記キー情報を記憶するキー記憶部（２７）と、
前記提供者情報記憶部から、一部の前記提供者端末を示すキー情報だけを、前記キー記憶部に配信し記憶させる配信手段（１５０、１６０）と、
前記キー記憶部（２７）に記憶されたキー情報を前記利用者端末（２）から前記提供者端末（３）に入力する入力手段（１７４、１７５、１８３、１８７）と、
前記提供者端末に入力された前記キー情報に基づいて、前記提供者端末（３）において、前記提供者端末（３）の利用可否を判定するキー情報判定手段（１８８、１８９）とを有し、
前記配信手段は、前記利用者端末（２）に関する位置情報と前記提供者端末（３）に関する位置情報とに基づいて、前記利用者端末による前記提供者端末の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る前記利用者端末（２）と前記提供者端末（３）とを関連付け、関連付けられた前記提供者端末（３）を示す前記キー情報を、関連付けられた前記利用者端末（２）に配信し、
さらに、前記利用者端末に設けられ、主認証情報を記憶する主認証情報記憶部（２６）と、
前記利用者端末（２）と前記提供者端末（３）との間、および前記提供者端末（３）と前記認証端末（４）との間に設けられ、前記主認証情報を前記提供者端末を経由して前記認証端末に送信する通信手段（５、２８、３４、４４）と、
前記認証端末（４）に設けられ、前記主認証情報に基づいて、前記提供者端末（３）の利用可否を判定する主認証手段（１７１、１７２、１８１、１８２、１８４、１９０）とを備え、
前記キー情報判定手段は、前記通信手段によって前記認証端末へ前記主認証情報を送信できないときに、前記主認証手段に代わって、前記提供者端末（３）の利用可否を判定することを特徴とする認証処理装置。
【請求項６】
前記配信手段は、前記利用者端末（２）に関する位置情報に含まれる前記利用者端末の現在位置、未来位置、および過去位置の少なくともひとつに基づいて前記利用者端末（２）と前記提供者端末（３）とを関連付けることを特徴とする請求項５に記載の認証処理装

置。
【請求項７】
前記配信手段は、特定の前記利用者端末（２）に関連付けられるひとつまたは複数の前記提供者端末を示す前記キー情報を、特定の前記利用者端末（２）に配信することを特徴とする請求項５または請求項６に記載の認証処理装置。
【請求項８】
前記配信手段は、前記主認証情報を前記認証端末へ送信できない特定の前記提供者端末（３）を示す前記キー情報を、特定の前記提供者端末（３）に関連付けられるひとつまたは複数の前記利用者端末に配信することを特徴とする請求項５から請求項７のいずれかに記載の認証処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
ここに開示される発明は、商品を受領またはサービスを受ける利用者の正規性を認証するための認証処理方法および認証処理装置に関する。
【背景技術】
【０００２】
特許文献１は、電気自動車のための充電システムにおける認証処理方法および認証処理装置を開示する。この認証処理方法では、通信不成立時に、非常用のゲスト用アカウント情報及びゲスト用認証情報に基づいてゲストアカウントでの認証を行う。そして、ゲストアカウントでの認証成立を条件に、車両用情報端末の必要最低限の諸機能（サービス）を利用可能としている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１２－２０３４２８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
従来技術の構成では、サーバによるリモート認証機能と、ローカル認証機能との両方を設けている。このために、ローカルの機器にも認証のための情報を保存する必要がある。ところが、認証情報を保存するために大量の記憶領域をローカルに設ける必要がある。また、高度のセキュリティ機能をローカルに設ける必要がある。
【０００５】
このような観点から、従来の認証処理方法および認証処理装置にはさらなる改良が求められている。
【０００６】
発明の目的のひとつは、提供者端末と利用者端末との間で利用可能な簡易な認証処理方法および認証処理装置を提供することである。
【０００７】
発明の目的の他のひとつは、認証の成立を適切に制限できる簡易な認証処理方法および認証処理装置を提供することである。
【０００８】
発明の目的の他のひとつは、提供者端末の位置情報と利用者端末の位置情報とに基づいて認証の成立を適切に制限できる簡易な認証処理方法および認証処理装置を提供することである。
【０００９】
発明の目的の他のひとつは、サーバによるリモート認証機能が利用できないときに利用可能であって、しかも提供者端末の位置情報と利用者端末の位置情報とに基づいて認証の成立を適切に制限できる簡易な認証処理方法および認証処理装置を提供することである。

【課題を解決するための手段】
【００１０】
本発明は上記目的を達成するために以下の技術的手段を採用する。なお、特許請求の範囲およびこの項に記載した括弧内の符号は、ひとつの態様として後述する実施形態に記載の具体的手段との対応関係を示すものであって、本発明の技術的範囲を限定するものではない。
【００１１】
開示された発明のひとつは、移動体である利用者端末（２）を認証することにより提供者端末（３）の利用可否を判定する認証処理方法において、提供者端末（３）から離れて設置された認証端末（４）に設けられ、複数の提供者端末（３）を示すキー情報を記憶する提供者情報記憶部（４３）から、一部の提供者端末を示すキー情報だけを、利用者端末（２）のキー記憶部（２７）へ配信し記憶させる配信工程（１５０、１６０）と、キー記憶部（２７）に記憶されたキー情報を利用者端末（２）から提供者端末（３）に入力する入力工程（１７４、１７５、１８３、１８７）と、提供者端末に入力されたキー情報に基づいて、提供者端末（３）において、提供者端末（３）の利用可否を判定するキー情報判定工程（１８８、１８９）とを有し、配信工程は、利用者端末（２）に関する位置情報と提供者端末（３）に関する位置情報とに基づいて、利用者端末による提供者端末の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る利用者端末（２）と提供者端末（３）とを関連付け、関連付けられた提供者端末（３）を示すキー情報を、関連付けられた利用者端末（２）に配信し、さらに、利用者端末に設けられた主認証情報記憶部（２６）に記憶された主認証情報に基づいて、認証端末（４）において、提供者端末（３）の利用可否を判定する主認証工程（１７１、１７２、１８１、１８２、１８４、１９０）を備え、キー情報判定工程は、主認証工程が完了できないときに、主認証工程に代わって、提供者端末（３）の利用可否を判定することを特徴とする。
【００１２】
この発明によると、配信工程において予め認証端末から利用者端末へ配信されたキー情報を利用して、提供者端末において提供者端末の利用可否が判定される。複数の提供者端末を示すキー情報から、一部の提供者端末を示すキー情報が配信されるから、提供者端末の利用を制限できる。しかも、提供者端末と認証端末との間におけるプロセスなしで、提供者端末において提供者端末の利用可否を判定することができる。
【００１３】
開示された発明のひとつは、移動体である利用者端末（２）を認証することにより提供者端末（３）の利用可否を判定する認証処理装置において、提供者端末（３）から離れて設置された認証端末（４）に設けられ、複数の提供者端末（３）を示すキー情報を記憶する提供者情報記憶部（４３）と、利用者端末（２）に設けられ、キー情報を記憶するキー記憶部（２７）と、提供者情報記憶部から、一部の提供者端末を示すキー情報だけを、キー記憶部に配信し記憶させる配信手段（１５０、１６０）と、キー記憶部（２７）に記憶されたキー情報を利用者端末（２）から提供者端末（３）に入力する入力手段（１７４、１７５、１８３、１８７）と、提供者端末に入力されたキー情報に基づいて、提供者端末（３）において、提供者端末（３）の利用可否を判定するキー情報判定手段（１８８、１８９）とを有し、配信手段は、利用者端末（２）に関する位置情報と提供者端末（３）に関する位置情報とに基づいて、利用者端末による提供者端末の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る利用者端末（２）と提供者端末（３）とを関連付け、関連付けられた提供者端末（３）を示すキー情報を、関連付けられた利用者端末（２）に配信し、さらに、利用者端末に設けられ、主認証情報を記憶する主認証情報記憶部（２６）と、利用者端末（２）と提供者端末（３）との間、および提供者端末（３）と認証端末（４）との間に設けられ、主認証情報を提供者端末を経由して認証端末に送信する通信手段（５、２８、３４、４４）と、認証端末（４）に設けられ、主認証情報に基づいて、提供者端末（３）の利用可否を判定する主認証手段（１７１、１７２、１８１、１８２、１８４、１９０）とを備え、キー情報判定手段は、通信手段によって認証端末へ主認証情

報を送信できないときに、主認証手段に代わって、提供者端末（３）の利用可否を判定することを特徴とする。

【００１４】

この発明によると、配信手段によって予め認証端末から利用者端末へ配信されたキー情報を利用して、提供者端末において提供者端末の利用可否が判定される。複数の提供者端末を示すキー情報から、一部の提供者端末を示すキー情報が配信されるから、提供者端末の利用を制限できる。しかも、提供者端末と認証端末との間におけるプロセスなしで、提供者端末において提供者端末の利用可否を判定することができる。

【図面の簡単な説明】

【００１５】

【図１】発明の一実施形態に係る認証システムのブロック図である。
【図２】一実施形態の利用者端末の準備処理を示すフローチャートである。
【図３】一実施形態の認証端末の準備処理を示すフローチャートである。
【図４】一実施形態の管理データの一例を示すデータリスト図である。
【図５】一実施形態の端末の位置の一例を示す平面図である。
【図６】一実施形態の管理データの一例を示すデータリスト図である。
【図７】一実施形態の端末の位置の一例を示す平面図である。
【図８】一実施形態の管理データの一例を示すデータリスト図である。
【図９】一実施形態の端末の位置の一例を示す平面図である。
【図１０】一実施形態の管理データの一例を示すデータリスト図である。
【図１１】一実施形態の端末の位置の一例を示す平面図である。
【図１２】一実施形態の利用者端末の認証処理を示すフローチャートである。
【図１３】一実施形態の提供者端末の認証処理を示すフローチャートである。
【図１４】一実施形態の認証端末の認証処理を示すフローチャートである。
【図１５】一実施形態の処理流れの一例を示すシーケンス図である。

【発明を実施するための形態】

【００１６】

以下に、図面を参照しながら発明を実施するための複数の形態を説明する。各形態において先行する形態で説明した事項に対応する部分には同一の参照符号を付して重複する説明を省略する場合がある。各形態において構成の一部のみを説明している場合は、構成の他の部分については先行して説明した他の形態を適用することができる。各実施形態で具体的に組合せが可能であることを明示している部分同士の組合せばかりではなく、特に組合せに支障が生じなければ、明示してなくとも実施形態同士を部分的に組み合せることも可能である。

【００１７】

（認証システム）

図１において、発明の一実施形態に係る認証システム１が図示されている。認証システム１は、コンピュータ資源を利用した認証処理装置を提供する。認証処理装置は、発明に係る認証処理方法を実行する。認証システム１は、移動体である利用者端末２を認証することにより提供者端末３の利用可否を判定する認証処理方法および認証処理装置を提供する。

【００１８】

認証システム１は、電動車両のための充電システム１でもある。電動車両は、外部から充電可能な電池を搭載している。例えば、電動車両は電池のみを動力源とする電気自動車、または内燃機関若しくは燃料電池といった燃料利用動力源を搭載したプラグインハイブリッド自動車とすることができる。

【００１９】

認証システム１は、認証が成立することによって何らかの利益を受ける利用者に属する利用者端末２を備える。認証システム１は、その管理下に複数の利用者端末２を備える。例えば、利用者は、認証が成立した場合に、提供者から有体または無体の商品の購入が可

能となる。図示の実施形態においては、商品は電力である。また、利用者は、認証が成立した場合に、提供者からサービスを受けることができる。図示の実施形態においては、サービスは、充電スタンドの利用である。

【００２０】

利用者端末２は、情報端末によって提供することができる。利用者端末２は、電動車両そのものに搭載された装置、または利用者が携帯することができる携帯端末とすることができる。例えば、利用者端末２は、利用者が所有する携帯電話機、スマートフォン、住宅若しくは事業所に配備される電力管理用のモニタ装置などによって提供することができる。図示の例では、利用者端末２は、電動車両である。利用者端末２の多くの機能は、電動車両に搭載されたナビゲーション装置によって提供される。

【００２１】

認証システム１は、利用者に商品またはサービスを提供する提供者に属する提供者端末３を備える。認証システム１は、その管理下に複数の提供者端末３を備える。提供者端末３は、電動車両の電池を充電するために、電動車両に電力を供給する充電スタンドである。提供者端末３の多くの機能は、充電スタンドに設置されたコンピュータによって提供される。利用者端末２と提供者端末３とは、互いにデータ通信可能に構成されている。利用者端末２と提供者端末３とは、ローカル機器とも呼ばれる。

【００２２】

認証システム１は、利用者または利用者端末２を認証する認証サービスを提供するための認証端末４を備える。ここでの認証は、利用者または利用者端末２が、提供者端末３の利用を認められているか否かを判定するための認証である。例えば、認証端末４は、利用者の本人認証、または利用者端末２が利用者に属するものであることの認証を提供する。

【００２３】

認証システム１は、ひとつまたは複数の認証端末４を備えることができる。認証端末４の数は、認証システム１に属する利用者端末２の数、および認証システム１に属する提供者端末３の数より明らかに少ない。認証端末４と利用者端末２とは、互いにデータ通信可能に構成されている。認証端末４と提供者端末３とは、互いにデータ通信可能に構成されている。認証端末４は、多くの場合に、利用者端末２および提供者端末３から離れた地区に位置付けられている。認証端末４は、リモート機器とも呼ばれる。認証端末４は、認証局、認証センタ、または認証サーバとも呼ぶことができる。

【００２４】

利用者端末２、提供者端末３、および認証端末４は、コンピュータを利用した制御装置によって提供される。制御装置は、電子制御装置（Electronic Control Unit）である。制御装置は、処理装置（ＣＰＵ）と、プログラムを記憶する記憶媒体としてのメモリ（ＭＭＲ）とを有する。制御装置は、コンピュータによって読み取り可能な記憶媒体を備えるマイクロコンピュータによって提供される。記憶媒体は、コンピュータによって読み取り可能なプログラムを非一時的に格納している。記憶媒体は、半導体メモリまたは磁気ディスクによって提供されうる。プログラムは、制御装置によって実行されることによって、制御装置をこの明細書に記載される装置として機能させ、この明細書に記載される制御方法を実行するように制御装置を機能させる。制御装置が提供する手段は、所定の機能を達成する機能的ブロック、またはモジュールとも呼ぶことができる。

【００２５】

認証システム１は、データ通信システム５を備える。データ通信システム５により、利用者端末２、提供者端末３、および認証端末４の中における二者間のデータ通信が提供されている。データ通信システム５は、無線および／または有線による種々のデータ通信装置によって提供することができる。また、利用者端末２と認証端末４との間のデータ通信は、提供者端末３を経由して提供されてもよい。この場合、後述のキー情報は、認証端末４から、提供者端末３を経由して、利用者端末２に提供される。

【００２６】

利用者端末２と提供者端末３との間には、充電のための電力接続６を形成することがで

きる。電力接続６は、充電ケーブルによる有線接続または電気磁気的な結合による無線接続によって提供することができる。データ通信システム５の一部、すなわち利用者端末２と提供者端末３との間のデータ通信は、電力接続６を経由して提供されてもよい。

【００２７】

利用者端末２と認証端末４との間のデータ通信および提供者端末３と認証端末４との間のデータ通信に比べて、利用者端末２と提供者端末３との間のデータ通信は、通信障害を生じにくい。充電スタンドから電動車両への充電が可能であるとき、利用者端末２と提供者端末３とは、互いに接近して配置されるからである。よって、提供者端末３と認証端末４との間に通信障害が生じる時でも、利用者端末２と提供者端末３との間では正常なデータ通信を実現できる場合が多い。

【００２８】

通信障害は、提供者端末３と認証端末４との間での通信ができない事象を指す。例えば、認証端末４が設置された地区、または提供者端末３が設置された地区において地震などの災害が発生し通信回線がダウンした場合を含むことができる。また、認証端末４が停電や高負荷によりダウンした場合も含むことができる。また、通信回線利用率が高くなり輻輳が生じた場合を含むことができる。さらに、提供者端末３および／または認証端末４の通信部が故障した場合も含むことができる。

【００２９】

認証システム１は、少なくともひとつの認証を提供する。この実施形態では、認証システム１は、複数の種類の認証を提供する。認証システム１が提供する認証には、第１の認証と第２の認証とを含むことができる。認証が成立する場合、提供者端末３は、利用者端末２による利用を許容する。認証が不成立である場合、提供者端末３は、利用者端末２による利用を拒否し、禁止する。

【００３０】

第１の認証は、主認証とも呼ばれる。主認証においては、提供者端末３からの要請に応じて、認証端末４が利用者端末２を認証する。主認証では、利用者端末２から提供され、提供者端末３を経由して認証端末４に提供される主認証情報と、認証端末４に予め設定され記憶されている認証情報とに基づいて利用者端末２の認証が実行される。主認証のための情報は、例えば、利用者端末２に固有の情報によって提供される。主認証のための情報は、非公開情報とすることができる。

【００３１】

主認証は、高度なセキュリティを提供する高度な認証処理である。この実施形態では、主認証は、提供者端末３の利用により生じる料金を利用者に課金し、決済するための認証である。主認証は、例えば、クレジットカードのための認証によって提供される。主認証は、認証時に、リモートに設置された認証端末４を必要とすることからリモート認証とも呼ぶことができる。主認証は、課金決済のために通常に利用されている認証方式を用いて提供されるから、通常認証とも呼ぶことができる。

【００３２】

第２の認証は、副認証とも呼ばれる。副認証においては、認証端末４から利用者端末２に対して予め配信された副認証情報に基づいて、利用者端末２と提供者端末３との間で認証がなされる。ここでは、提供者端末３が利用者端末２を認証する。副認証では、認証端末４から利用者端末２に対して予め配信された副認証情報と、提供者端末３に予め設定され記憶されている副認証情報とに基づいて利用者端末２の認証が実行される。副認証情報は、複数の提供者端末３の中から、選択されたひとつまたは複数の提供者端末３を識別するための識別情報でもある。

【００３３】

副認証情報は、ひとつ又は複数の提供者端末３に関連付けられた情報とすることができる。例えば、副認証情報は、ひとつの提供者端末３に固有のキー情報によって提供することができる。副認証情報は、近隣に位置する複数の提供者端末３に共通のデータであってもよい。副認証情報は、ひとつの提供者端末３に与えられた複数のキー情報であってもよ

い。この場合、利用者を受ける時間帯などに応じて複数のキー情報を使い分けてもよい。このような利用方法は、地震などの非常事態における利用者の分散を図るために有効である。この場合、キー情報には、充電スタンドを利用可能な時間帯を示す情報を含ませることができる。また、副認証情報は、提供者端末３、すなわち充電スタンドに対して固定的に付与することができる。これに代えて、副認証情報は、提供者端末３に対して、一時的に付与されるように構成することができる。

【００３４】

副認証のための情報は、主認証のための情報に比べて低いセキュリティレベルに置かれた情報である。副認証のための情報は、例えば、提供者端末３に固有であって、しかも公開されたキー情報によって提供することができる。

【００３５】

副認証は、主認証より低いセキュリティを提供する。この実施形態では、副認証は、提供者端末３の利用により生じる料金を利用者に課金し、決済するための認証である。副認証情報の情報量は、主認証情報の情報量より少ない。よって、副認証に要する処理量は、主認証に要する処理量より格段に少ない。副認証は、主認証に比べて簡易な処理によって利用者機器２を認証するから、簡易認証とも呼ぶことができる。副認証は、認証時に、ローカルに設置された利用者端末２と提供者端末３を必要とすることからローカル認証とも呼ぶことができる。

【００３６】

（利用者端末）

利用者端末２は、制御部２１を備える。制御部２１は、主認証のための主認証処理２１ａと、副認証のための副認証処理２１ｂとを実行する。

【００３７】

利用者端末２は、位置情報提供部２２を備える。位置情報提供部２２は、利用者端末２の位置を示す位置情報を制御部２１に提供する。位置情報提供部２２は、現在、未来、および過去の少なくともひとつにおける利用者端末２の位置を示す位置情報を提供する。位置情報提供部２２は、少なくとも現在の利用者端末２の位置を示す位置情報を提供するように構成することができる。位置情報提供部２２は、未来、すなわち予測された利用者端末２の位置を示す位置情報を追加的に提供するように構成することができる。位置情報提供部２２は、過去、すなわち記録された利用者端末２の位置を示す位置情報を追加的に提供するように構成することができる。

【００３８】

位置情報提供部２２は、利用者端末２の現在の位置を検出する位置検出部２２ａを備える。位置検出部２２ａは、衛星測位装置、例えばＧＰＳ装置によって提供することができる。位置検出部２２ａは、現在における利用者端末２の位置を示す位置情報を提供する。

【００３９】

位置情報提供部２２は、ナビ機能部２２ｂを備える。ナビ機能部２２ｂは、電動車両に搭載された経路案内装置、例えばナビゲーション装置によって提供される。ナビ機能部２２ｂは、電動車両に設けられた表示装置に地図と、地図上における電動車両の位置とを表示する。さらに、ナビ機能部２２ｂは、目的地が設定されると、現在地から目的地への経路を探索し、地図上に表示することによって電動車両の運転を支援する。ナビ機能部２２ｂは、目的地、および／または現在地と目的地との間の経由地を示す位置情報を提供する。よって、ナビ機能部２２ｂは、未来における利用者端末２の位置を示す位置情報を提供する。

【００４０】

位置情報提供部２２は、運行履歴記憶部２２ｃを備える。運行履歴記憶部２２ｃは、ナビ機能部２２ｂによって提供される地図上における電動車両の運行履歴を記憶する。運行履歴は、過去における電動車両の位置を示す。運行履歴は、過去の運行の日時、曜日を示す。また、運行履歴は、過去における充電の履歴、すなわち充電のために利用した充電スタンドを識別する情報、充電日時、曜日などを含むことができる。よって、運行履歴記憶

部２２ｃは、過去における利用者端末２の位置を示す位置情報を提供する。
【００４１】
利用者端末２は、充電式電源装置２３を備える。充電式電源装置２３は、外部から充電可能な電池を含む。この電池は、電動車両の走行用動力源である。充電式電源装置２３は、制御部２１の制御下におかれる。
【００４２】
利用者端末２は、電池状態取得部２４を備える。電池状態取得部２４は、充電式電源装置２３の電池の状態を取得し、制御部２１に入力する。電池状態取得部２４は、電池に充電されている電力量、すなわち充電状態を示すＳＯＣ（State Of Charge）を電池から取得し、制御部２１に入力する。
【００４３】
利用者端末２は、認証、充電、ナビゲーションのための機能だけでなく、他の機能を提供可能である。利用者端末２は、他の機能を提供するための外部アプリ部２５を備えることができる。外部アプリ部２５には、電動車両を利用したドライブ計画を取得するための機能を備えることができる。外部アプリ部２５は、ナビ機能部２２ｂと自動的に連携することにより、ドライブ計画に基づいて自動的に目的地を設定し、経路を設定する。このような外部アプリ部２５との連携が提供される場合、目的地は利用者の操作だけに依存して設定されることなく、自動的に設定されることがある。
【００４４】
利用者端末２は、主認証のための主認証情報を記憶する主認証情報記憶部２６を備える。主認証情報は、利用者本人、または利用者端末２を認証するために必要なデータである。主認証情報は、認証端末４に記憶された認証情報と関連付けられたデータによって提供される。利用者端末２は、副認証のための副認証情報、すなわちキー情報を記憶するキー記憶部２７を備える。
【００４５】
利用者端末２は、認証端末４および提供者端末３とデータ通信するための通信部２８を備える。通信部２８は、認証端末４とのデータ通信が通信障害によって不可能である時でも、提供者端末３とのデータ通信をできるように構成されている。
【００４６】
（提供者端末）
提供者端末３は、制御部３１を備える。制御部３１は、主認証のための主認証処理３１ａと、副認証のための副認証処理３１ｂとを実行する。
【００４７】
提供者端末３は、副認証のための副認証情報、すなわちキー情報を記憶する識別情報記憶部３２を備える。識別情報記憶部３２には、その提供者端末３に予め付与された識別情報、すなわちキー情報が記憶されている。
【００４８】
提供者端末３は、充電装置３３を備える。充電装置３３は、電動車両の充電式電源装置２３に電力を供給し、電池を充電する。充電装置３３は、制御部３１の制御下におかれている。充電装置３３は、制御部３１において主認証の成立、または副認証の成立が確認された場合に電力を供給する。
【００４９】
提供者端末３は、認証端末４および利用者端末２とデータ通信するための通信部３４を備える。通信部３４は、認証端末４とのデータ通信が通信障害によって不可能である時でも、利用者端末２とのデータ通信をできるように構成されている。
【００５０】
（認証端末）
認証端末４は、制御部４１を備える。制御部４１は、主認証のための主認証処理４１ａと、副認証のための副認証処理４１ｂとを実行する。
【００５１】

認証端末４は、主認証のための認証情報を記憶する認証情報管理データベース４２を備える。認証情報管理データベース４２には、認証システム１に属する複数の利用者端末２および／または利用者を認証するための非公開のデータが記憶されている。

【００５２】

認証端末４は、副認証のための副認証情報、すなわちキー情報を含む提供者情報を記憶する提供者情報管理データベース４３を備える。提供者情報管理データベース４３には、認証システム１に属する複数の提供者端末３を識別するための識別情報、すなわちキー情報が記憶されている。さらに、提供者情報管理データベース４３には、複数の提供者端末３のそれぞれの位置を示す位置情報が記憶されている。位置情報には、それぞれの提供者端末３が属する地区を示す情報を含むことができる。提供者端末３の位置情報は、認証システム１への加入手続きにおいて提供者情報管理データベース４３に登録され、記憶される。

【００５３】

認証端末４は、利用者端末２および提供者端末３とデータ通信するための通信部４４を備える。

【００５４】

（利用者端末の準備処理）

図２に図示されるように、利用者端末２は、副認証を可能とするための準備処理１５０を実行する。認証端末４は、準備処理１５０を実行することにより、実際に副認証が必要となり、求められる前に、副認証のための副認証情報を認証端末４から受信する受信手段を提供する。

【００５５】

ステップ１５１では、利用者端末２が起動された直後か否かが、その電源スイッチがＯＦＦ状態からＯＮ状態に切換えられたか否かによって判定される。利用者端末２が起動された直後である場合、ステップ１５２へ進む。

【００５６】

ステップ１５２では、利用者端末２から認証端末４への送信処理が実行される。ここでは、現在の利用者端末２の位置を示す情報、すなわち現在位置情報が利用者端末２から認証端末４に送信される。これにより、利用者端末２が起動された時の現在位置情報が利用者端末２から認証端末４に提供される。さらに、ステップ１５２では、利用者端末２を識別し、特定することにより、認証端末４において利用者端末２を認証するための認証情報、例えばＩＤコードが送信される。また、ステップ１５２では、付加的な情報が送信される。付加的な情報には、例えば、利用者端末２の電池の状態、利用者からの指示、利用者のクレジットカード取引における信用情報、移動速度などを含むことができる。

【００５７】

利用者端末２が起動された直後ではない場合、ステップ１５３へ進む。ステップ１５３では、定期処理時刻であるか否かが判定される。定期処理時刻は、現在位置情報を定期的に利用者端末２から認証端末４に送信するために所定の時間間隔で設定されている。定期処理時刻の間隔は、数分、数時間などに設定することができる。定期処理時刻である場合、ステップ１５２へ進む。この結果、利用者端末２が起動状態にある期間中、定期的に、現在位置情報が利用者端末２から認証端末４に提供される。ステップ１５１－１５３により、利用者端末２の現在位置情報が利用者端末２から認証端末４に提供される。

【００５８】

ステップ１５４では、ナビ機能部２２ｂに目的地が設定されているか否かが判定される。この判定は、ナビ機能部２２ｂによる経路案内が実行されているか否かの判定、または未来の電動車両の位置を予測可能か否かを判定する処理とも呼ぶことができる。目的地が設定されている場合、ステップ１５５へ進む。ステップ１５５では、未来の利用者端末２の位置を示す情報、すなわち未来位置情報が利用者端末２から認証端末４に送信される。未来位置情報には、目的地を示す位置情報、および／または経路を示す位置情報を含むことができる。これにより、利用者端末２の未来位置情報が利用者端末２から認証端末４に

提供される。

【００５９】

ステップ１５６では、履歴送信時期であるか否かが判定される。履歴送信時期は、運行履歴記憶部２２ｃに記憶された運行履歴を定期的に利用者端末２から認証端末４に送信するために所定の間隔で設定されている。履歴送信時期の間隔は、数日、週、月などに設定することができる。履歴送信時期である場合、ステップ１５７へ進む。ステップ１５７では、過去の利用者端末２の位置を示す情報、すなわち過去位置情報が利用者端末２から認証端末４に送信される。過去位置情報には、運行履歴記憶部２２ｃに記憶されたデータを含むことができる。過去位置情報には、運行履歴記憶部２２ｃに所定の回数を越えて繰り返し記憶される目的地、経路などの位置情報を含むことができる。さらに、過去位置情報には、運行履歴の運行日時、曜日などを含むことができる。これにより、利用者端末２の過去位置情報が利用者端末２から認証端末４に提供される。

【００６０】

ステップ１５８では、利用者端末２が認証端末４からキー情報を受信したか否かが判定される。キー情報が受信された場合、ステップ１５９へ進む。ステップ１５９では、キー記憶部２７に記録されたキー情報が更新される。

【００６１】

ステップ１５８では、既に記憶されているキー情報を削除するように新しく受信されたキー情報を上書きすることができる。これに代えて、キー情報に所定のルールに基づいて優先度を与え、高優先度のキー情報のみを記憶してもよい。このような手法は、キー記憶部２７の記憶容量を抑制するために有効である。また、受信されたキー情報が多すぎる場合にも有効である。例えば、利用者端末２から近いほど高い優先度が付与されるようにルールを設定することができる。また、目的地までの経路において充電量が減少し充電が必要になると予想される地点に近いほど高い優先度が付与されるようにルールを設定することができる。また、目的地までの経路上において既に通過した充電スタンドのキー情報を削除し、経路上の先にある充電スタンドのキー情報を新たに取得して記憶するようにルールを設定してもよい。また、ある充電スタンドにおいて充電が終了または完了した場合、キー記憶部２７に記憶されている当該充電スタンドのキー情報を削除するようにルールを設定してもよい。このような充電後のキー情報の削除は、地震などの非常事態が発生し、充電スタンドへ電動車両が集中するような場合に、同一の利用者が充電スタンドの利用を独占してしまう事態を防ぐために有効である。

【００６２】

（認証端末の準備処理）

図３に図示されるように、認証端末４は、副認証を可能とするための準備処理１６０を実行する。認証端末４は、準備処理１６０を実行することにより、実際に副認証が必要となり、求められる前に、副認証のための副認証情報を利用者端末２へ配信する配信手段を提供する。

【００６３】

ステップ１６１では、利用者端末２の位置を示す位置情報を収集する処理が実行される。ステップ１６１では、認証システム１に属する複数の利用者端末２の位置情報が収集される。ステップ１６２では、利用者端末２の位置情報が受信される。認証端末４から利用者端末２から受信する位置情報には、現在情報、未来情報、および過去情報の少なくともひとつを含むことができる。現在情報は、利用者端末２の現在位置、すなわち利用者端末２が位置する現在地を示す。未来情報は、利用者端末２の未来の位置を示す。未来情報は、利用者によって設定された目的地、ナビ機能部２２ｂによって自動的に設定された目的地、および／またはナビ機能部２２ｂによって経路案内される経路を示す。過去情報は、利用者端末２の過去の運行履歴を示す。運行履歴には、過去の位置、過去の経路、習慣的に訪れる地点、習慣的に経由する経路などの情報を含むことができる。

【００６４】

ステップ１６３では、副認証のための副認証データ、すなわちキー情報を決定し、決定

されたキー情報を利用者端末２に対して配信する配信処理が実行される。ステップ１６３では、複数の利用者端末２に対して、キー情報が決定され、配信される。ステップ１６３においては、利用者端末２の位置情報と、提供者端末３の位置情報とに基づいて、利用者端末２による提供者端末３の利用の可能性が評価される。ステップ１６３では、利用の可能性が高い利用者端末２と提供者端末３とが関連付けられる。具体的には、利用の可能性が所定の閾値を上回ると考えられる利用者端末２と提供者端末３とが関連付けられる。さらに、ステップ１６３では、ひとつの利用者端末２に関連付けられたひとつまたは複数の提供者端末３に付与されたキー情報が決定される。すなわち、位置情報に基づいてキー情報が決定される。決定されたキー情報は、関連付けられた利用者端末２に配信、言い換えると送信される。

【００６５】

さらに、ステップ１６３では、利用者端末２から認証端末４に送信される付加的な情報に基づいて、利用者端末２と提供者端末３との関連付けを調節することができる。例えば、付加的な情報に基づいて、上記関連付けのための閾値が調節される。例えば、利用者端末２の電池の状態、利用者からの指示、利用者の信用情報、移動速度などに基づいて、利用者端末２と提供者端末３との関連付けを調節することができる。利用者端末２から電池の充電状態ＳＯＣが送信される場合、充電状態ＳＯＣが低く、近いうちに提供者端末３を利用する可能性が高いと予想される利用者端末２だけにキー情報を配信してもよい。また、利用者の信用情報に基づいて、利用者の信用度が所定水準より低い場合には、その利用者の利用者端末２は配信対象から除外するようにしてもよい。また、移動速度が速く、高速道路などを走行していると予想される利用者端末２は配信対象から除外するようにしてもよい。

【００６６】

ステップ１６３には、定常的に実行される配信処理１６３ａと、非定常的な事象をトリガとして実行される配信処理１６３ｂとを含むことができる。

【００６７】

配信処理１６３ａでは、特定の利用者端末２の位置情報と、複数の提供者端末３の位置情報とに基づいて、特定の利用者端末２とひとつまたは複数の提供者端末３とを関連付ける。この関連付けられた提供者端末３は、選択された提供者端末３として扱われる。選択された提供者端末３のキー情報は、上記特定の利用者端末２に配信される。配信処理１６３ａは、位置情報が受信される度に、または所定の時間ごとに定常的に実行することができる。配信処理１６３ａは定常配信処理とも呼ぶことができる。

【００６８】

ステップ１６４では、利用者端末２の位置情報が受信され、利用可能であるか否かが判定される。特定の利用者端末２の位置情報が利用可能である場合、ステップ１６５へ進む。ステップ１６５では、特定の利用者端末２とひとつまたは複数の提供者端末３とが関連付けられる。言い換えると、特定の利用者端末２の位置情報と複数の提供者端末３の位置情報とに基づいて、ひとつまたは複数の提供者端末３が選択される。ここでは、特定の利用者端末２の位置情報に基づいて、この特定の利用者端末２が訪れる可能性があるひとつまたは複数の提供者端末３が選択される。例えば、利用者端末２の現在情報に基づいて、利用者端末２の近くに位置する提供者端末３が選択される。例えば、利用者端末２の未来情報に基づいて、利用者端末２の未来位置の近くに位置する提供者端末３が選択される。例えば、利用者端末２の過去情報に基づいて、利用者端末２の過去位置の近くに位置する提供者端末３が選択される。

【００６９】

図４、図６、図８、図１０は、現在情報に基づく提供者端末の選択の一例を管理データ４３ａ上において示す。管理データ４３ａは、提供者情報管理データベース４３に記憶されている。管理データ４３ａは、複数の提供者端末３のそれぞれに関する、提供者端末３が所属する地区、提供者端末３の位置情報、提供者端末３の名称、および提供者端末３に固有のキー情報を福不。図示の例では、認証システム１には、１号機から１０号機の提供

者端末３が属している。それぞれの提供者端末３に付与されたキー情報は、３桁の数字である。

【００７０】

図５、図７、図９、図１１は、現在情報に基づく提供者端末３の選択の一例を地図平面４３ｂの上において示す。図中において、利用者端末２の位置は三角形で示されている。提供者端末３の位置は、四角形で示されている。図示の例では、地図平面４３ｂはＡ地区、Ｂ地区、Ｃ地区、Ｄ地区に４分割されている。利用者端末２の未来の経路は破線で示されている。利用者端末２の運行履歴は一点鎖線で示されている。

【００７１】

図４および図５は、現在情報が利用される一例を示す。認証端末４は、利用者端末２すなわちＡ車の現在位置を受信すると、この現在位置に基づいて、利用者端末２と同じ地区に属する提供者端末３を選択し、それらのキー情報をＡ車に配信する。この例では、Ｃ地区に属する６号機と７号機のキー情報が利用者端末２に配信される。図示の例に代えて、Ａ車から所定の距離範囲内、例えば１０ｋｍ圏内に位置する提供者端末３のキー情報をＡ車の利用者端末２に配信してもよい。

【００７２】

図６および図７は、未来情報が利用される一例を示す。利用者端末２すなわちＡ車において、ナビ機能部２２ｂに目的地が設定され、経路案内が実行される。認証端末４は、利用者端末２から目的地および／または経路を受信すると、この未来情報に基づいて、経路の近傍に位置する提供者端末３、および目的地の近傍に位置する提供者端末３を選択し、それらのキー情報をＡ車に配信する。この例では、経路に沿って７号機、６号機、１号機、２号機、および５号機のキー情報が利用者端末２に配信される。

【００７３】

図８および図９は、過去情報が利用される一例を示す。利用者端末２すなわちＡ車において、ナビ機能部２２ｂに運行履歴のデータが蓄積される。認証端末４は、利用者端末２から運行履歴を受信すると、この過去情報に基づいて、過去の運行経路の近傍に位置する提供者端末３を選択し、それらのキー情報をＡ車に配信する。この例では、過去の運行経路に沿って５号機、８号機、９号機、および１０号機のキー情報が利用者端末２に配信される。認証端末４は、過去の運行履歴から、今後に利用者端末２が向かうと推測される地区、施設、経路などを推定し、それら推定位置の近傍に位置する提供者端末３のキー情報を配信するようにしてもよい。認証端末４は、特定の曜日、時間に向かっていることが多い商業施設が運行履歴から特定できる場合、その商業施設への経路の近傍に位置する提供者端末３のキー情報を配信してもよい。

【００７４】

図３に戻り、ステップ１６６では、選択された提供者端末３のキー情報が上記特定の利用者端末２に送信される。これにより、特定の利用者端末２に対して、その特定の利用者端末２が訪れ、利用する可能性が高いと予想されるひとつまたは複数の提供者端末３のキー情報が配信される。

【００７５】

ステップ１６６におけるキー情報の配信は、利用者端末２の正規性が認証された場合にのみ実行されるように構成することができる。例えば、利用者端末２から認証端末４へ送信される位置情報には、利用者端末２を識別し、特定するためのＩＤコードを付与することができる。認証端末４は、提供者端末３の利用、すなわち充電を禁止すべき利用者端末２のＩＤコードを記憶することができる。この場合、認証端末４は、利用者端末２のＩＤコードが、充電を禁止すべきＩＤコードと一致する場合、キー情報を配信しないようにすることができる。このようなキー情報を配信するか否かを決定するための利用者端末２と認証端末４との間の認証処理は、キー情報の利用を制限し、キー情報の不当な拡散、キー情報の不正な利用を阻止するために貢献する。

【００７６】

配信処理１６３ｂでは、非定常的な事象に応答して配信処理が実行される。非定常的な

事象として、キー情報が必要となる事態の発生を利用することができる。例えば、提供者端末３と認証端末４との間における通信障害の発生は、キー情報が必要となる事態のひとつである。また、利用者端末２または提供者端末３からの要求を、非定常的な事象としてもよい。

【００７７】

配信処理１６３ｂでは、特定の提供者端末３と認証端末４との間における通信障害の発生が認証端末４において検出される。通信障害が検出されると、特定の提供者端末３の位置情報と、複数の利用者端末２の位置情報とに基づいて、特定の提供者端末３とひとつまたは複数の利用者端末２とを関連付ける。この関連付けられた利用者端末２は、選択された利用者端末２として扱われる。上記特定の提供者端末３のキー情報は、選択された利用者端末２に配信される。配信処理１６３ｂは非定常配信処理とも呼ぶことができる。

【００７８】

ステップ１６７では、特定の提供者端末３と認証端末４との間において通信障害があるか否かが判定される。通信障害がある場合、ステップ１６８へ進む。ステップ１６８では、特定の提供者端末３とひとつまたは複数の利用者端末２とが関連付けられる。言い換えると、特定の提供者端末３の位置情報と複数の利用者端末２の位置情報とに基づいて、ひとつまたは複数の利用者端末２が選択される。ここでは、特定の提供者端末３の位置情報に基づいて、この特定の提供者端末３を訪れる可能性があるひとつまたは複数の利用者端末２が選択される。例えば、複数の利用者端末２の現在情報に基づいて、特定の提供者端末３の近くに位置する利用者端末２が選択される。例えば、複数の利用者端末２の未来情報に基づいて、特定の提供者端末３の近くを通過または到達する可能性がある利用者端末２が選択される。例えば、複数の利用者端末２の過去情報に基づいて、特定の提供者端末３の近くを通過または到達する可能性がある利用者端末２が選択される。

【００７９】

ステップ１６９では、特定の提供者端末３のキー情報が、選択された利用者端末２に送信される。これにより、通信障害の下にある特定の提供者端末３を訪れ、利用する可能性が高いと予想されるひとつまたは複数の利用者端末２に対して、特定の提供者端末３のキー情報が配信される。ステップ１６９では、ステップ１６６と同様に、利用者端末２と認証端末４との間の認証処理が実行されてもよい。

【００８０】

図１０および図１１は、通信障害の発生に応答する処理の一例を示す。提供者端末３の６号機と認証端末４との間において通信障害が発生した場合が図示されている。認証端末４は、６号機との間において通信障害が発生すると、この通信障害を検出する。認証端末４は、通信障害が検出されると、通信障害が発生している６号機の近傍に位置する利用者端末２および／またはこの６号機を利用する可能性がある利用者端末２を選択する。認証端末４は、６号機のキー情報を、選択された利用者端末２に配信する。この例では、６号機の近傍に位置するＣ車の利用者端末２と、６号機に向けて接近しつつあるＤ車の利用者端末２とに、６号機のキー情報が配信される。

【００８１】

準備処理１５０、１６０は、複数の提供者端末３を示すキー情報を記憶する提供者情報記憶部４３から、一部の提供者端末を示すキー情報だけを、利用者端末２のキー記憶部２７へ配信し記憶させる配信工程を提供する。言い換えると、準備処理１５０、１６０は、複数の提供者端末３を示すキー情報を記憶する提供者情報記憶部４３と、利用者端末２に設けられ、キー情報を記憶するキー記憶部２７と、提供者情報記憶部から、一部の提供者端末を示すキー情報だけを、キー記憶部に配信し記憶させる配信手段とを提供する。提供者情報記憶部４３は、提供者端末３から離れて設置された認証端末４に設けられている。

【００８２】

準備処理１５０、１６０によって提供される配信工程は、利用者端末２に関する位置情報と提供者端末３に関する位置情報とに基づいて、利用者端末２による提供者端末３の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る利用者端末２と提供者端末

３とを関連付ける。さらに、関連付けられた提供者端末３を示すキー情報を、関連付けられた利用者端末２に配信する。配信工程は、利用者端末２に関する位置情報に含まれる利用者端末２の現在位置、未来位置、および過去位置の少なくともひとつに基づいて利用者端末２と提供者端末３とを関連付ける。配信工程は、特定の利用者端末２に関連付けられるひとつまたは複数の提供者端末３を示すキー情報を、特定の利用者端末２に配信する。

【００８３】

準備処理１５０、１６０によって提供される配信手段は、利用者端末２に関する位置情報と提供者端末３に関する位置情報とに基づいて、利用者端末２による提供者端末３の利用の可能性を評価し、この利用の可能性が所定の閾値を上回る利用者端末２と提供者端末３とを関連付ける。さらに、関連付けられた提供者端末３を示すキー情報を、関連付けられた利用者端末２に配信する。配信手段は、利用者端末２に関する位置情報に含まれる利用者端末２の現在位置、未来位置、および過去位置の少なくともひとつに基づいて利用者端末２と提供者端末３とを関連付ける。配信手段は、特定の利用者端末２に関連付けられるひとつまたは複数の提供者端末３を示すキー情報を、特定の利用者端末２に配信する。

【００８４】

（利用者端末の認証処理）

図１２に図示されるように、利用者端末２は、提供者端末３を利用する場合に、自らの認証を求めるための認証処理１７０を実行する。利用者端末２は、認証処理１７０を実行することにより、主認証を要求する主認証要求手段を提供する。利用者端末２は、認証処理１７０を実行することにより、副認証を要求する副認証開始手段を提供する。

【００８５】

図示の例のように提供者端末３が充電スタンドである場合、利用者端末２と提供者端末３との間のデータ通信は、充電ケーブルに付設された通信線、または電力線を経由して有線的に提供することができる。また、利用者端末２と提供者端末３との間のデータ通信は、短距離用の無線通信によって提供することができる。

【００８６】

ステップ１７１では、利用者端末２から提供者端末３へ主認証の実行が求められる。ステップ１７１では、主認証のための主認証情報が利用者端末２から提供者端末３へ送信される。ステップ１７２では、主認証によって充電が許可されたか否か、すなわち提供者端末３の利用が許可されたか否かが判定される。主認証が成立し、充電が許可されるとステップ１７３へ進む。ステップ１７３では、充電処理、すなわち受電処理が実行される。

【００８７】

ステップ１７２において充電が許可されない場合、ステップ１７４へ進む。ステップ１７４では、提供者端末３から利用者端末２へキー情報の要求があったか否かが判定される。キー情報の要求がある場合、すなわち提供者端末３においてキー情報の利用を許容している場合、ステップ１７５へ進む。

【００８８】

ステップ１７５では、利用者端末２から提供者端末３へ副認証の実行が求められる。言い換えると、利用者端末２から提供者端末３へキー情報が送信される。ステップ１７６では、利用者端末２は、キー記憶部１７に記憶されたキー情報を自動的に送信する。これに代えて、利用者端末２は、キー記憶部１７に記憶されたキー情報を表示装置に表示し、その表示を見た利用者による手入力を促し、入力結果を送信することができる。このような構成は、キー情報を使用することの利用者への通知、およびキー情報を利用することへの利用者の意思確認のために有効である。

【００８９】

ステップ１７６では、副認証によって充電が許可されたか否か、すなわち提供者端末３の利用が許可されたか否かが判定される。副認証が成立し、充電が許可されるとステップ１７３へ進む。

【００９０】

ステップ１７６において副認証が成立しない場合、処理を終了する。ステップ１７４に

おいてキー情報が要求されない場合、すなわち提供者端末３が副認証を受け付けない場合も、処理を終了する。すなわち、主認証も副認証も成立しない場合、充電処理は実行されない。

【００９１】

（提供者端末の認証処理）

図１３に図示されるように、提供者端末３は、利用者端末２からの要求に応答して認証処理１８０を実行する。提供者端末３は、認証処理１８０を実行することにより、副認証を実行する副認証処理手段を提供する。副認証は、認証端末４から利用者端末２へ予め配信され、利用者端末２から提供者端末３へ送信される副認証情報に基づいて実行される認証である。提供者端末３は、認証処理１８０を実行することにより、利用者端末２から提供者端末３へ送信される主認証情報を中継し、認証端末４へ送信する中継手段を提供する。

【００９２】

ステップ１８１では、利用者端末２から主認証が要求されているか否かが判定される。主認証が要求されている場合ステップ１８２へ進む。ステップ１８２では、提供者端末３から認証端末４へ主認証が要求される。ここでは、上述の認証処理１７０において利用者端末２から提供者端末３へ送信された主認証情報が提供者端末３から認証端末４へ送信される。

【００９３】

ステップ１８３では、提供者端末３と認証端末４との間において通信障害が発生しているか否かが判定される。通信障害が発生していない場合、ステップ１８４へ進む。ステップ１８４では、主認証が成立したか否かが判定される。言い換えると、利用者端末２による提供者端末３の利用を許可するか拒否するかが判定される。主認証が成立しない場合、処理を終了し、利用を拒否する。

【００９４】

ステップ１８４において主認証が成立する場合、ステップ１８５へ進む。ステップ１８５では、利用者端末２に対して充電許可を返信する。すなわち、提供者端末３から利用者端末２へ利用の許可が通知される。ステップ１８６では、提供者端末３から利用者端末２への充電処理、すなわち給電処理が実行される。これにより、利用者端末２の充電が実行される。

【００９５】

ステップ１８３において、通信障害が発生している場合、主認証を完了できない。よって、主認証によって利用者端末２を認証し、提供者端末３における利用の許否を判定することができない。通信障害が発生している場合、ステップ１８７へ進む。ステップ１８７では、提供者端末３から利用者端末２へキー情報が要求される。言い換えると、提供者端末３は、副認証を実行可能であることを利用者端末２へ通知する。

【００９６】

ステップ１８３とステップ１８７とは、副認証の利用を制限する副認証制限手段を提供する。認証システム１においては、主認証が主要な認証手法として位置付けられている。キー情報を利用した副認証は、主認証に比べて簡易な認証方式である。よって、副認証の過剰な利用、不正な利用を抑制し、阻止するために、副認証の利用、すなわちキー情報の受け入れは制限されることが望ましい。また、副認証を利用可能とする時間帯を設定してもよい。また、時間帯ごとに異なるキー情報を配信し、複数の利用者端末２のそれぞれについて、提供者端末３を利用可能な時間帯を設定してもよい。このような制限は、提供者端末３への多数の利用者端末２の集中を抑制するために有効となる。

【００９７】

ステップ１８８では、利用者端末２から送信されたキー情報と、提供者端末３に記憶されたキー情報とが照合される。言い換えると、キー情報を利用した副認証処理が実行される。ステップ１８９では、副認証が成立したか否かが判定される。利用者端末２から送信されたキー情報と、提供者端末３に記憶されたキー情報とが一致する場合、副認証が成立

したと判定することができる。利用者端末２から送信されたキー情報と、提供者端末３に記憶されたキー情報とが不一致の場合、または利用者端末２からキー情報が得られない場合には、副認証は不成立とされる。

【００９８】

ステップ１８９において副認証が成立する場合、ステップ１８５へ進む。副認証が不成立である場合、処理を終了する。

【００９９】

（認証端末の認証処理）

図１４に図示されるように、認証端末４は、提供者端末３からの要求に応答して認証処理１９０を実行する。認証端末４は、認証処理１９０を実行することにより、主認証を実行する主認証処理手段を提供する。主認証は、利用者端末２から、提供者端末３を経由して、認証端末４へ送信される主認証情報に基づいて実行される認証である。

【０１００】

ステップ１９１では、提供者端末３から主認証が要求されているか否かが判定される。主認証が要求されている場合ステップ１９２へ進む。ステップ１９２では、利用者端末２から提供者端末３へ送信され、提供者端末３によって中継されることによって認証端末４へ送信された主認証情報に基づいて主認証が実行される。ここでは、利用者端末２が正規のものであるか否かが認証される。この認証は、利用者端末２が提供者端末３の利用を認められた正規のものであるか否かの判定ともいうことができる。ステップ１９３では、主認証が成立したか否かが判定される。主認証が成立する場合、ステップ１９４へ進む。ステップ１９４では、提供者端末３に対して主認証が成立したこと、すなわち利用者端末２が提供者端末３の利用を認められたものであることを回答する。認証が成立しない場合、ステップ１９５へ進む。ステップ１９５では、提供者端末３に対して主認証が不成立であること、すなわち利用者端末２が提供者端末３の利用を認められたものではないことを回答する。

【０１０１】

ステップ１７４、１７５、１８３、１８７は、キー記憶部２７に記憶されたキー情報を利用者端末２から提供者端末３に入力する入力工程を提供する。ステップ１８８、１８９は、提供者端末３に入力されたキー情報に基づいて、提供者端末３において、提供者端末３の利用可否を判定するキー情報判定工程を提供する。ステップ１７４、１７５、１８３、１８７は、キー記憶部２７に記憶されたキー情報を利用者端末２から提供者端末３に入力する入力手段を提供する。ステップ１８８、１８９は、提供者端末３に入力されたキー情報に基づいて、提供者端末３において、提供者端末３の利用可否を判定するキー情報判定手段を提供する。

【０１０２】

ステップ１７１、１７２、１８１、１８２、１８４、１９０は、利用者端末２に設けられた主認証情報記憶部２６に記憶された主認証情報に基づいて、認証端末４において、提供者端末３の利用可否を判定する主認証工程を提供する。キー情報判定工程は、主認証工程が完了できないときに、主認証工程に代わって、提供者端末３の利用可否を判定する。配信工程は、主認証工程が完了できない特定の提供者端末３を示すキー情報を、特定の提供者端末３に関連付けられるひとつまたは複数の利用者端末２に配信する。

【０１０３】

認証システム１は、利用者端末２に設けられ、主認証情報を記憶する主認証情報記憶部２６を備える。認証システム１は、利用者端末２と提供者端末３との間、および提供者端末３と認証端末４との間に設けられ、主認証情報を提供者端末３を経由して認証端末４に送信する通信手段５、２８、３４、４４を備える。さらに、認証システム１は、認証端末４に設けられ、主認証情報に基づいて、提供者端末３の利用可否を判定する主認証手段１７１、１７２、１８１、１８２、１８４、１９０を備える。キー情報判定手段は、通信手段によって認証端末へ主認証情報を送信できないときに、主認証手段に代わって、提供者端末３の利用可否を判定する。配信手段は、主認証情報を認証端末４へ送信できない特定

の提供者端末３を示すキー情報を、特定の提供者端末３に関連付けられるひとつまたは複数の利用者端末２に配信する。

【０１０４】

（認証端末の認証処理）

図１５には、端末２、３、４の間におけるデータの流れ、および処理の手順が図示されている。認証システム１は、利用者端末２による提供者端末３の利用の可否を判定するために、主認証１１１と、副認証１１２とを実行する。図示の例では、主認証１１１は主要な認証方式として利用される。副認証１１２は、通信障害のように、主認証１１１が利用できないときに補助的な認証方式として利用される。

【０１０５】

主認証１１１では、利用者端末２から要求が送信される。主認証の要求は、提供者端末３によって中継され、認証端末４に受信される。認証端末４は、主認証処理を実行し、その結果を、提供者端末３へ送信する。提供者端末３は、主認証の結果に基づいて、利用者端末２への充電サービスの提供可否を決定し、利用者端末２へ返信する。この結果、認証システム１は、主認証の結果に基づいて、利用者端末２による提供者端末３の利用の可否を決定する。

【０１０６】

副認証１１２は、準備手順１１３と、認証手順１１４とを含む。準備手順１１３は、認証手順１１４に先立って実行される。準備手順１１３は、さらに、定常手順１１３ａと、非定常手順１１３ｂとを有する。

【０１０７】

定常手順１１３ａでは、利用者端末２の位置情報と提供者端末３の位置情報とに基づいて、利用者端末２による提供者端末３の利用の可能性が評価され、利用の可能性が高い利用者端末２と提供者端末３とが関連付けられる。定常手順１１３ａでは、利用者端末２の位置情報が利用者端末２から認証端末４へ送信される。認証端末４は、利用可能な提供者端末３を示すキー情報を利用者端末２へ送信する。

【０１０８】

非常手順１１３ｂでは、何らかの事象に応答して、上記評価と、関連付けとが実行される。非定常手順１１３ｂでは、利用者端末２の位置情報が利用者端末２から認証端末４へ送信される。さらに、認証端末４は、関連付けを実行するためのトリガとなる事象を検出する。図示の例では、通信障害の発生が検出される。ここで、関連付けのトリガとなる事象は、特定の利用者端末２または特定の提供者端末３を決定できる事象である。関連付けの後、認証端末４は、主認証なしで利用可能な提供者端末３を示すキー情報を利用者端末２へ送信する。

【０１０９】

認証手順１１４では、利用者端末２は、まず、主認証を要求する。提供者端末３は、通信障害によって主認証を完了できない場合に、利用者端末２に対して副認証を要求する。利用者端末２は、副認証情報であるキー情報を提供者端末３へ送信する。提供者端末３は、キー情報に基づいて副認証処理を実行する。提供者端末３は、副認証の結果に基づいて、利用者端末２への充電サービスの提供可否を決定し、利用者端末２へ返信する。この結果、認証システム１は、主認証が利用できないときに、副認証の結果に基づいて、利用者端末２による提供者端末３の利用の可否を決定する。

【０１１０】

（他の実施形態）

以上、発明の好ましい実施形態について説明したが、発明は上述した実施形態に何ら制限されることなく、種々変形して実施することが可能である。上記実施形態の構造は、あくまで例示であって、発明の技術的範囲はこれらの記載の範囲に限定されるものではない。発明は、実施形態において示された組み合わせに限定されることなく、それぞれ独立して実施可能である。発明のいくつかの技術的範囲は、特許請求の範囲の記載によって示され、さらに特許請求の範囲の記載と均等の意味及び範囲内での全ての変更を含むものであ

る。

【０１１１】

例えば、制御装置が提供する手段と機能は、ソフトウェアのみ、ハードウェアのみ、あるいはそれらの組合せによって提供することができる。例えば、制御装置をアナログ回路によって構成してもよい。

【０１１２】

上記実施形態では、主認証が利用できないときにだけ、副認証である簡易認証の結果に基づいて、利用者端末２による提供者端末３の利用の可否を決定した。これに代えて、キー情報を利用する簡易認証だけを用いて利用者端末２による提供者端末３の利用の可否を決定してもよい。この場合、キー情報を認証端末４から利用者端末２へ配信する処理において認証端末４が利用者端末２を認証することが望ましい。キー情報の配信段階においてセキュリティ性の高い認証を採用することにより、キー情報を利用する簡易認証においても不正使用を抑制できる。また、この場合には、提供者端末３と認証端末４との間のデータ通信が不要となる。この結果、通信の負荷軽減、さらには提供者端末３と認証端末４との間の通信機能の削除が可能となる。

【０１１３】

また、上記実施形態では、主認証が利用可能であるときには副認証は実行されない。これに代えて、主認証が利用可能であるときには、副認証を併用してもよい。この場合、利用者端末２が提供者端末３を利用する際には、必ずキー情報が利用者端末２から提供者端末３へ送信される。

【０１１４】

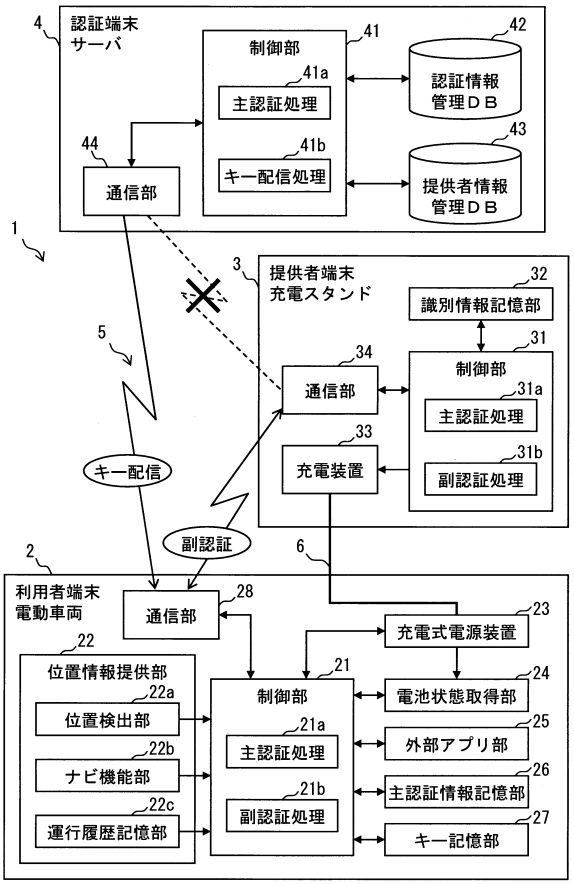
上記実施形態では、副認証におけるキー情報は、利用者端末２から提供者端末３へデータ通信によって送信されるものとした。これに代えて、キー情報は提供者端末３に手入力されてもよい。この場合、利用者端末２は、提供者端末３からキー情報を求められると、キー情報を表示装置に表示し、利用者に対して手入力を求める。提供者端末３には、キー情報を手入力するための手入力装置が設けられる。提供者端末３は、利用者の手入力を経由して、キー情報を利用者端末２から取得することとなる。

【符号の説明】

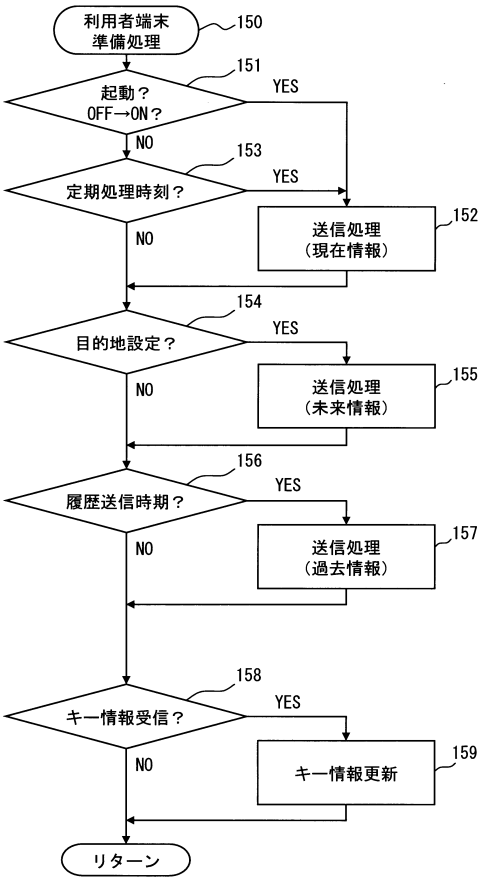
【０１１５】

１　認証システム、
２　利用者端末（電動車両）、　２１　制御部、　２２　位置情報提供部、
２２ａ　位置検出部、　２２ｂ　ナビ機能部、　２２ｃ　運行履歴記憶部、
２３　充電式電源装置、　２４　電池状態取得部、　２５　外部アプリ部、
２６　主認証情報記憶部、　２７　キー記憶部、　２８　通信部、
３　提供者端末（充電スタンド）、　３１　制御部、　３２　識別情報記憶部、
３３　充電装置、　３４　通信部、
４　認証端末（サーバ）、　４１　制御部、　４２　認識情報管理データベース、
４３　提供者情報管理データベース、　４４　通信部、
５　データ通信システム、　６　電力接続。

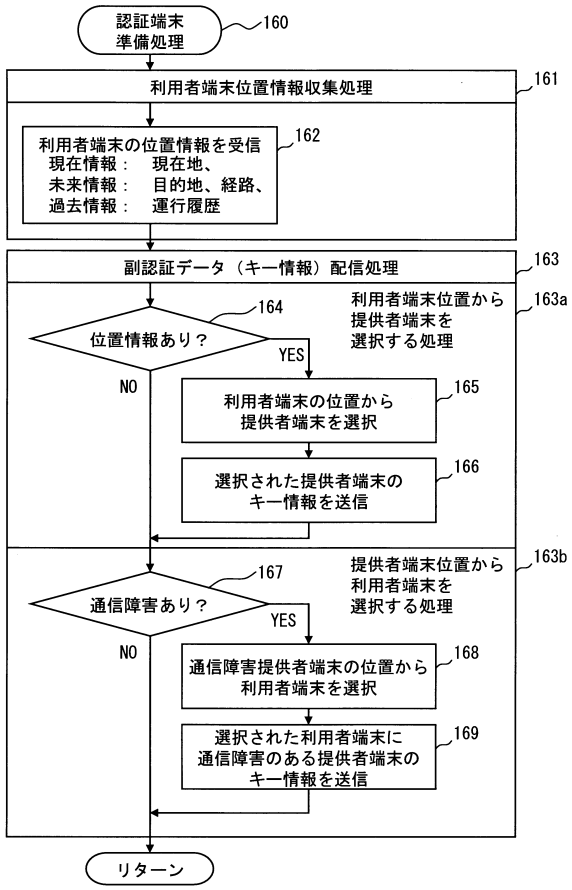
【図１】



【図２】



【図３】

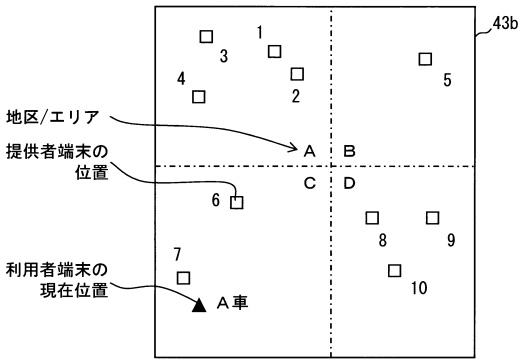


【図４】

43a

地区 エリア	提供者端末位置 緯度／経度範囲	提供者端末名 充電スタンド	副認証情報 キー情報
A	***.**～***.** ***.**～***.**	1号機	123
		2号機	456
		3号機	789
		4号機	012
B	***.**～***.** ***.**～***.**	5号機	345
C	***.**～***.** ***.**～***.**	6号機	678
		7号機	901
D	***.**～***.** ***.**～***.**	8号機	234
		9号機	567
		10号機	890

【図５】

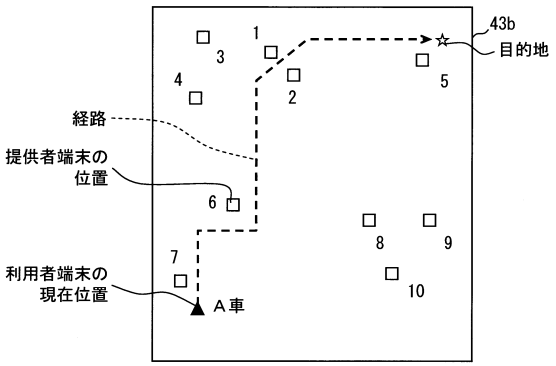


【図６】

43a

地区 エリア	提供者端末位置 緯度／経度範囲	提供者端末名 充電スタンド	副認証情報 キー情報
A	***.**～***.** ***.**～***.**	1号機	123
		2号機	456
		3号機	789
		4号機	012
B	***.**～***.** ***.**～***.**	5号機	345
C	***.**～***.** ***.**～***.**	6号機	678
		7号機	901
D	***.**～***.** ***.**～***.**	8号機	234
		9号機	567
		10号機	890

【図７】

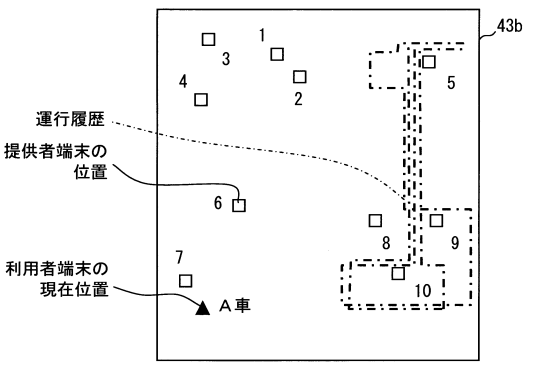


【図８】

43a

地区 エリア	提供者端末位置 緯度／経度範囲	提供者端末名 充電スタンド	副認証情報 キー情報
A	***.**～***.** ***.**～***.**	1号機	123
		2号機	456
		3号機	789
		4号機	012
B	***.**～***.** ***.**～***.**	5号機	345
C	***.**～***.** ***.**～***.**	6号機	678
		7号機	901
D	***.**～***.** ***.**～***.**	8号機	234
		9号機	567
		10号機	890

【図９】

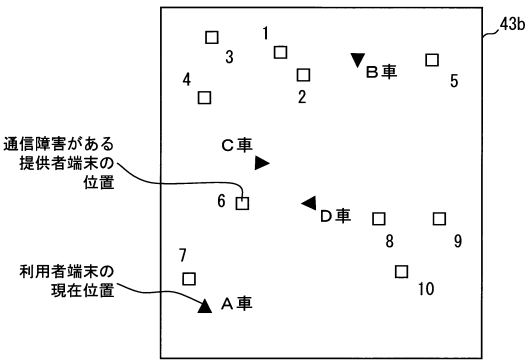


【図１０】

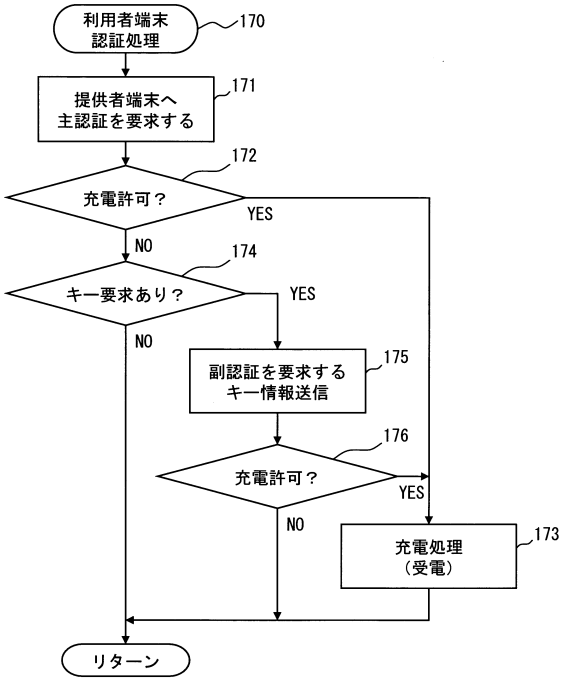
43a

地区 エリア	提供者端末位置 緯度／経度範囲	提供者端末名 充電スタンド	副認証情報 キー情報
A	***.**～***.** ***.**～***.**	1号機	123
		2号機	456
		3号機	789
		4号機	012
B	***.**～***.** ***.**～***.**	5号機	345
C	***.**～***.** ***.**～***.**	6号機	678
		7号機	901
D	***.**～***.** ***.**～***.**	8号機	234
		9号機	567
		10号機	890

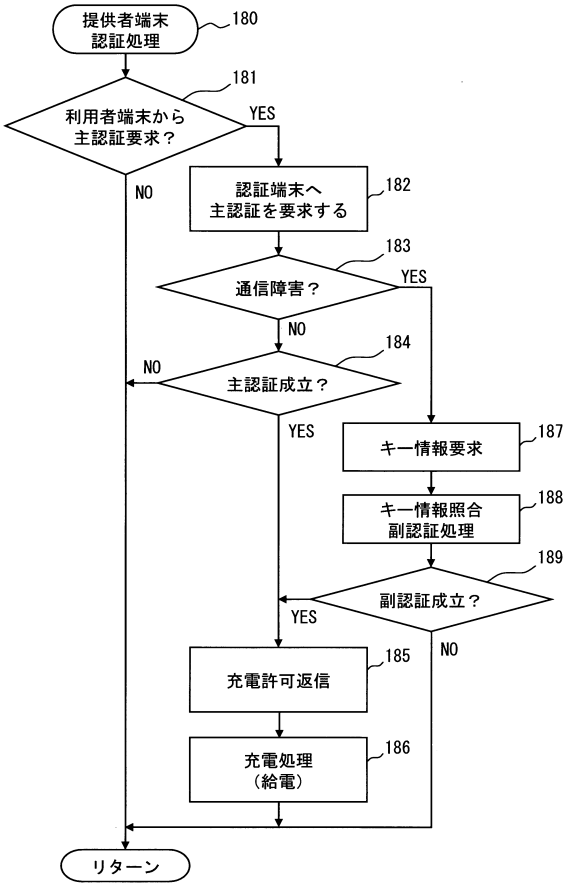
【図１１】



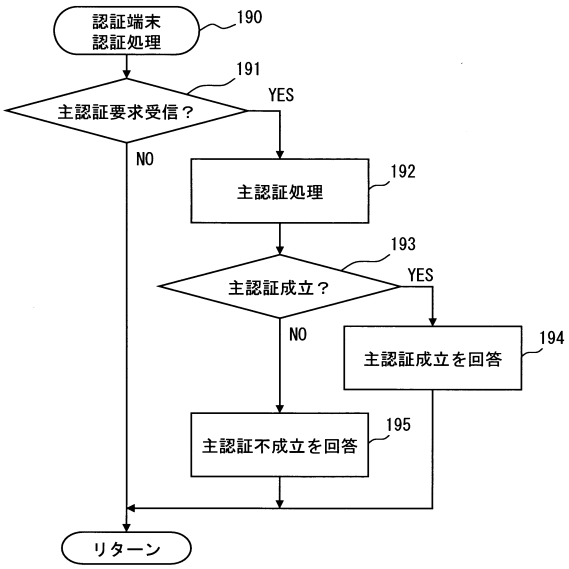
【図１２】



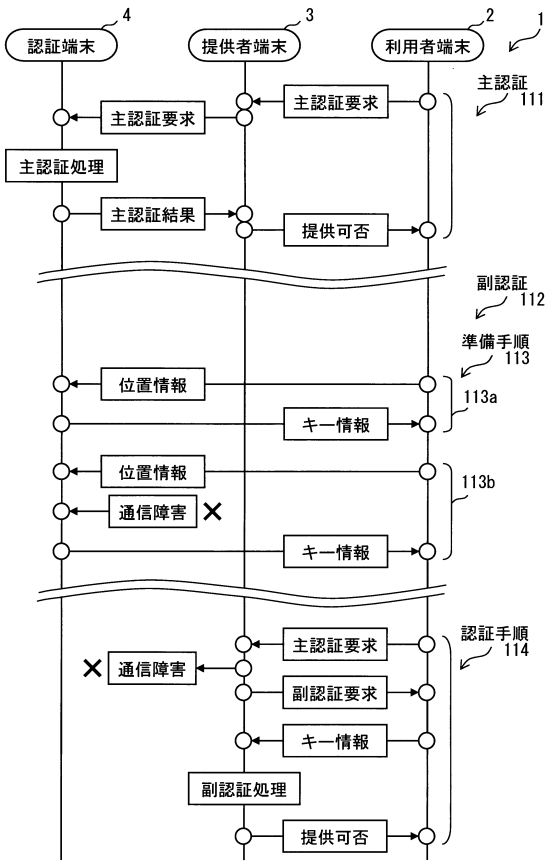
【図１３】


提供者端末
認証処理
180
利用者端末から
主認証要求？
181
YES
NO
認証端末へ
主認証を要求する
182
通信障害？
183
YES
NO
主認証成立？
184
NO
YES
キー情報要求
187
キー情報照合
副認証処理
188
副認証成立？
189
YES
NO
充電許可返信
185
充電処理
（給電）
186
リターン

【図１４】


認証端末
認証処理
190
主認証要求受信？
191
YES
NO
主認証処理
192
主認証成立？
193
YES
NO
主認証成立を回答
194
主認証不成立を回答
195
リターン

【図１５】


認証端末
4
提供者端末
3
利用者端末
2
1
主認証
111
主認証要求
主認証要求
主認証処理
主認証結果
提供可否
副認証
112
準備手順
113
位置情報
113a
キー情報
位置情報
通信障害
113b
キー情報
認証手順
114
主認証要求
通信障害
副認証要求
キー情報
副認証処理
提供可否

フロントページの続き

審査官　上島　拓也

(56)参考文献　特開２０１１－２２７５４１（ＪＰ，Ａ）
特開２０１２－１２８６３３（ＪＰ，Ａ）
特開２００９－１１０４６５（ＪＰ，Ａ）
特開２０１２－０５３８２１（ＪＰ，Ａ）
特開２０１１－０４４１１２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１