

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2021年7月1日(01.07.2021)



(10) 国際公開番号

WO 2021/131060 A1

(51) 国際特許分類:

G06F 21/31 (2013.01)

(21) 国際出願番号:

PCT/JP2019/051569

(22) 国際出願日:

2019年12月27日(27.12.2019)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(71) 出願人: 楽天グループ株式会社 (RAKUTEN GROUP, INC.) [JP/JP]; 〒1580094 東京都世田谷区玉川一丁目14番1号 Tokyo (JP).

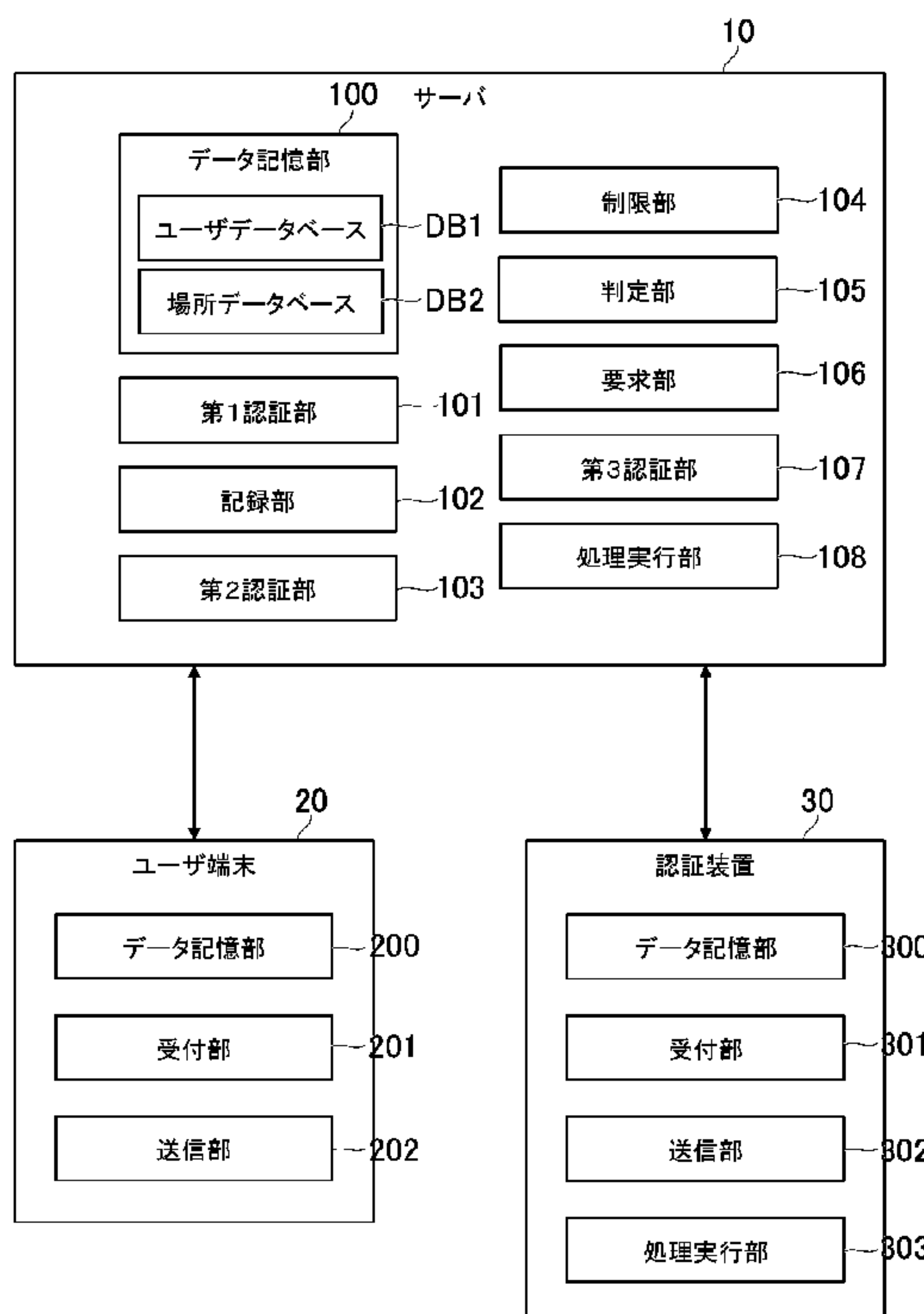
(72) 発明者: 蔡永男 (CHAE, Yeongnam); 〒1580094 東京都世田谷区玉川一丁目14番1号 楽天株式会社内 Tokyo (JP).

(74) 代理人: 特許業務法人はるか国際特許事務所 (HARUKA PATENT & TRADEMARK ATTORNEYS); 〒1020085 東京都千代田区六番町3 六番町S Kビル5階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: AUTHENTICATION SYSTEM, AUTHENTICATION DEVICE, AUTHENTICATION METHOD, AND PROGRAM

(54) 発明の名称: 認証システム、認証装置、認証方法、及びプログラム



10 Server
20 User terminal
30 Authentication device
100, 200, 300 Data storage unit
101 First authentication unit
102 Recording unit
103 Second authentication unit
104 Restriction unit
105 Determination unit
106 Requesting unit
107 Third authentication unit
108, 303 Processing execution unit
201, 301 Acceptance unit
202, 302 Transmission unit
DB1 User database
DB2 Location database

(57) Abstract: A first authentication means (101) of an authentication system (S) performs authentication on the basis of a first authentication method. When the authentication by the first authentication method is successful, a recording means (102) records an authenticated user in association with the location of that user in a storage means. A second authentication means (103) performs authentication on the basis of a second authentication method. A restriction means (104) restricts authentication by the second authentication method from succeeding when a user to be authenticated by the

[続葉有]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類 :
一 国際調査報告 (条約第21条(3))

second authentication method and the location of that user to be authenticated are not associated in the storage means (100).

(57) 要約 : 認証システム (S) の第 1 認証手段 (1 0 1) は、第 1 の認証方法に基づいて、認証をする。記録手段 (1 0 2) は、第 1 の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する。第 2 認証手段 (1 0 3) は、第 2 の認証方法に基づいて、認証をする。制限手段 (1 0 4) は、第 2 の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が記憶手段 (1 0 0) に関連付けられていない場合に、第 2 の認証方法の認証が成功することを制限する。

明 細 書

発明の名称：

認証システム、認証装置、認証方法、及びプログラム

技術分野

[0001] 本開示は、認証システム、認証装置、認証方法、及びプログラムに関する。

背景技術

[0002] 従来、第三者による成りすましを防止する認証技術が知られている。例えば、特許文献 1 には、複数のパターンの顔写真を予め登録しておき、任意のパターンの顔写真を利用して顔認証を実行するシステムが記載されている。

先行技術文献

特許文献

[0003] 特許文献 1：特開 2 0 0 8－0 7 1 3 6 6 号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、特許文献 1 に記載の顔認証は、予め登録された複数のパターンの顔写真と、認証時に撮影された顔写真と、の類似性によって判定されるので、第三者の顔が似ていれば、どのパターンの顔写真を利用したとしても認証が成功する可能性がある。このため、第三者による成りすましを防止できないことがあり、セキュリティを十分に高めることはできない。

[0005] 本開示の目的は、セキュリティを十分に高めることが可能な認証システム、認証装置、認証方法、及びプログラムを提供することである。

課題を解決するための手段

[0006] 本発明の一態様に係る認証システムは、第 1 の認証方法に基づいて、認証をする第 1 認証手段と、前記第 1 の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録す

る記録手段と、第2の認証方法に基づいて、認証をする第2認証手段と、前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限手段と、を含む。

[0007] 本発明の一態様に係る認証装置は、上記又は下記に記載の認証システムに含まれる認証装置又は当該認証システムと通信可能な認証装置であって、前記認証に必要な情報を送信する送信手段と、前記認証が成功した場合に、所定の処理を実行する処理実行手段と、を含む。

[0008] 本発明の一態様に係る認証方法は、第1の認証方法に基づいて、認証をする第1認証ステップと、前記第1の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する記録ステップと、第2の認証方法に基づいて、認証をする第2認証ステップと、前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限ステップと、を含む。

[0009] 本発明の一態様に係るプログラムは、第1の認証方法に基づいて、認証をする第1認証手段、前記第1の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する記録手段、第2の認証方法に基づいて、認証をする第2認証手段、前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限手段、としてコンピュータを機能させる。

[0010] 本発明の一態様によれば、前記第2の認証方法の認証では、入力認証情報と登録認証情報とが比較され、前記制限手段は、前記認証対象ユーザがいる場所が関連付けられたユーザの前記登録認証情報を、前記認証対象ユーザの入力認証情報との比較対象として取得し、前記認証対象ユーザがいる場所が関連付けられていないユーザの前記登録認証情報を、前記比較対象とはしないことによって、前記第2の認証方法の認証が成功することを制限し、前記

第2認証手段は、前記認証対象ユーザの前記入力認証情報と、前記比較対象として取得された登録認証情報と、に基づいて認証を行う。

[0011] 本発明の一態様によれば、前記第1認証手段は、前記第2の認証方法の認証が失敗した場合に、前記第1の認証方法に基づいて、前記認証対象ユーザの認証を行い、前記記録手段は、前記第1の認証方法の認証が成功した場合に、認証された前記認証対象ユーザと、当該認証対象ユーザがいる場所と、を関連付けて前記記憶手段に記録する。

[0012] 本発明の一態様によれば、前記認証システムは、前記認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられている場合に、前記第2の認証方法の認証で、前記認証対象ユーザが他のユーザとして認証される可能性があるか否かを判定する判定手段と、前記可能性があるとは判定された場合に、前記認証対象ユーザに対し、前記第1の認証方法又は第3の認証方法の認証を要求する要求手段と、を含む。

[0013] 本発明の一態様によれば、前記記録手段は、前記第1の認証方法で認証されたユーザがいる場所として、当該ユーザがいるエリアを前記記憶手段に記録し、前記制限手段は、前記認証対象ユーザと、当該認証対象ユーザがいるエリアと、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する。

[0014] 本発明の一態様によれば、前記認証システムは、前記第2の認証方法の認証が失敗した場合に、第3の認証方法に基づいて、前記認証対象ユーザの認証をする第3認証手段を更に含み、前記記憶手段には、前記第3の認証方法の認証が成功したとしても、認証された前記認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられない。

[0015] 本発明の一態様によれば、前記認証システムは、前記第1の認証方法又は前記第2の認証方法の何れかの選択を受け付ける受付手段を更に含み、前記第1認証手段は、前記第1の認証方法が選択された場合に、前記第1の認証方法の認証を行い、前記第2認証手段は、前記第2の認証方法が選択された場合に、前記第2の認証方法の認証を行う。

[0016] 本発明の一態様によれば、前記第2の認証方法は、認証情報の類似に基づく認証方法と、認証情報の一致に基づく認証方法と、を含む。

[0017] 本発明の一態様によれば、前記認証システムは、前記第1の認証方法及び前記第2の認証方法の各々に対応した複数の認証装置を含み、前記記録手段は、前記第1の認証方法で認証されたユーザと、当該ユーザの認証で用いられた前記認証装置の場所と、を関連付けて前記記憶手段に記録し、前記制限手段は、前記認証対象ユーザと、当該認証対象ユーザの認証で用いられる前記認証装置の場所と、が関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する。

[0018] 本発明の一態様によれば、前記第1の認証方法の認証は、ユーザ端末を利用した認証であり、前記第2の認証方法の認証は、生体認証である。

[0019] 本発明の一態様によれば、前記認証システムは、前記第1の認証方法の認証又は前記第2の認証方法の認証が成功した場合に、認証されたユーザの決済情報に基づいて、決済処理を実行する処理実行手段を更に含む。

発明の効果

[0020] 本開示によれば、セキュリティを十分に高めることが可能となる。

図面の簡単な説明

[0021] [図1]認証システムの全体構成を示す図である。

[図2]認証システムが利用される場面の一例を示す図である。

[図3]2次元コード認証が実行される様子を示す図である。

[図4]2段階認証が実行される様子を示す図である。

[図5]認証システムの処理の一例を説明するための図である。

[図6]認証システムの処理の一例を説明するための図である。

[図7]認証システムの処理の一例を説明するための図である。

[図8]認証システムの処理の一例を説明するための図である。

[図9]認証システムの処理の一例を説明するための図である。

[図10]追加認証が行われる様子を示す図である。

[図11]本実施形態の認証システムで実現される機能の一例を示す機能ブロッ

ク図である。

[図12]ユーザデータベースのデータ格納例を示す図である。

[図13]場所データベースのデータ格納例を示す図である。

[図14]本実施形態において実行される処理の一例を示すフロー図である。

[図15]本実施形態において実行される処理の一例を示すフロー図である。

発明を実施するための形態

[0022] [1. 認証システムの全体構成]

以下、認証システムの実施形態の例を説明する。図1は、認証システムの全体構成を示す図である。図1に示すように、認証システムSは、サーバ10、ユーザ端末20、及び認証装置30を含み、これらは、インターネットなどのネットワークNに接続可能である。なお、図1では、サーバ10、ユーザ端末20、及び認証装置30の各々を1台ずつ示しているが、これらは複数台あってもよい。

[0023] サーバ10は、サーバコンピュータである。サーバ10は、制御部11、記憶部12、及び通信部13を含む。制御部11は、少なくとも1つのプロセッサを含む。制御部11は、記憶部12に記憶されたプログラムやデータに従って処理を実行する。記憶部12は、主記憶部及び補助記憶部を含む。例えば、主記憶部はRAMなどの揮発性メモリであり、補助記憶部は、ROM、EEPROM、フラッシュメモリ、又はハードディスクなどの不揮発性メモリである。通信部13は、有線通信又は無線通信用の通信インタフェースであり、ネットワークNを介してデータ通信を行う。

[0024] ユーザ端末20は、ユーザが操作するコンピュータである。例えば、ユーザ端末20は、携帯電話機（スマートフォンを含む）、携帯情報端末（タブレット型コンピュータ及びウェアラブル端末を含む）、又は、パーソナルコンピュータ等である。本実施形態では、ユーザ端末20は、制御部21、記憶部22、通信部23、操作部24、表示部25、及び撮影部26を含む。制御部21、記憶部22、及び通信部23の物理的構成は、それぞれ制御部11、記憶部12、及び通信部13と同様であってよい。

[0025] 操作部 24 は、入力デバイスであり、例えば、タッチパネルやマウス等のポインティングデバイス、キーボード、又はボタン等である。操作部 24 は、操作内容を制御部 21 に伝達する。表示部 25 は、例えば、液晶表示部又は有機 EL 表示部等である。表示部 25 は、制御部 21 の指示に従って画像を表示する。

[0026] 撮影部 26 は、少なくとも 1 台のカメラを含む。例えば、撮影部 26 は、CCD イメージセンサや CMOS イメージセンサなどの撮像素子を含み、当該撮像素子が撮影した画像をデジタルデータとして記録する。画像は、静止画であってもよいし、所定のフレームレートで連続的に撮影された動画であってもよい。

[0027] 認証装置 30 は、認証に使用されるコンピュータである。例えば、認証装置 30 は、携帯電話機、携帯情報端末、又は、パーソナルコンピュータ等である。本実施形態では、認証装置 30 は、制御部 31、記憶部 32、通信部 33、操作部 34、表示部 35、及び撮影部 36 を含む。制御部 31、記憶部 32、通信部 33、操作部 34、表示部 35、及び撮影部 36 の物理的構成は、それぞれ制御部 11、記憶部 12、通信部 13、操作部 24、表示部 25、及び撮影部 26 と同様であってよい。

[0028] なお、記憶部 12、22、32 に記憶されるものとして説明するプログラム及びデータは、ネットワーク N を介して供給されるようにしてもよい。また、上記説明した各コンピュータのハードウェア構成は、上記の例に限られず、種々のハードウェアを適用可能である。例えば、コンピュータ読み取り可能な情報記憶媒体を読み取る読取部（例えば、光ディスクドライブやメモリカードスロット）や外部機器とデータの入出力をするための入出力部（例えば、USB ポート）が含まれていてもよい。例えば、情報記憶媒体に記憶されたプログラムやデータが読取部や入出力部を介して、各コンピュータに供給されるようにしてもよい。

[0029] [2. 認証システムの概要]

認証システム S は、任意の場面においてユーザの正当性を確認するために

、認証を実行する。認証は、ユーザが所定の資格を有するか否かを確認する行為であり、相手認証又は本人認証と呼ばれることもある。認証システム S は、種々のタイプの認証を実行可能であり、例えば、2次元コード認証、生体認証、パスコード認証、パスワード認証、電子スタンプ認証、又は合言葉認証を実行可能である。

[0030] 生体認証は、人間の身体的特徴又は行動的特徴を利用する認証方法である。例えば、身体的特徴を利用する生体認証には、顔認証、指紋認証、DNA 認証、掌形認証、網膜認証、虹彩認証、静脈認証、又は音声認証がある。また例えば、行動的特徴を利用する生体認証には、筆跡認証、キーストローク認証、リップムーブメント認証、まばたき認証、又は歩行認証がある。

[0031] 本実施形態では、ユーザがセキュリティゲートを通過する場面を例に挙げて、認証システム S の処理を説明する。なお、認証システム S は、後述する変形例のように、種々の場面に適用可能であり、認証システム S が適用される場面は、本実施形態の例に限られない。

[0032] 図 2 は、認証システム S が利用される場面の一例を示す図である。図 2 に示すように、セキュリティゲート S G は、回転式のドアを含み、認証装置 30 が接続されている。セキュリティゲート S G のドアは、ロック機構によりロックされており、ユーザの認証が成功すると、ロックが解除される。ロックが解除されると、ユーザはドアを押して通過することができる。ドアは、所定角度だけ回転すると再びロックされる。なお、ドアは、開閉式であってもよいし、電子錠によって開閉が制御されてもよい。

[0033] 例えば、セキュリティゲート S G は、勤務先の会社や公共施設などの任意の施設に配置され、入場する資格を有する者だけが通過することができる。セキュリティゲート S G は、複数の場所の各々に配置されている。本実施形態では、複数の認証方法が用意されており、ユーザは、認証方法を選択することができる。

[0034] 認証方法とは、認証の種類である。本実施形態では、2つの認証方法のうちの何れかをユーザが選択する場合を説明するが、認証方法は、3つ以上で

あってもよいし、１つの認証方法しか利用できない場所があってもよい。また、認証方法は、ユーザにより選択されるのではなく、認証システムＳにより自動的に選択されてもよい。認証方法は、多段階認証であってもよい。認証方法が多段階認証である場合には、複数の認証方法を組み合わせたものが、１つの認証方法に相当する。

[0035] 本実施形態では、２次元コード認証と、顔認証及びパスコード認証を組み合わせた２段階認証と、の２つの認証方法のうちの何れかをユーザが選択する場合を説明する。例えば、ユーザは、認証システムＳが提供する認証サービスを利用するにあたり、所定の利用登録を行う。利用登録は、ユーザが自ら行うのではなく、書類上で利用登録の申請が行われて、オペレータなどの操作によって行われてもよい。例えば、新規のユーザは、ユーザ端末２０を操作して、氏名やパスワード等の情報とともに、自身の顔写真と希望するパスコードを、認証システムＳが提供する認証サービスにアップロードする。これらの情報がアップロードされると利用登録が完了し、ユーザは認証サービスを利用できるようになる。

[0036] 図２に示すように、認証装置３０の表示部３５には、２次元コード認証を選択するためのボタンＢ３５ａと、２段階認証を選択するためのボタンＢ３５ｂと、が表示させる。ユーザは、ボタンＢ３５ａ、Ｂ３５ｂのうちの任意の方を選択できる。例えば、ユーザがボタンＢ３５ａを選択すると、表示部３５には、２次元コード認証の案内が表示される。

[0037] 図３は、２次元コード認証が実行される様子を示す図である。図３に示すように、ユーザは、表示部３５に表示された案内に従い、ユーザ端末２０に２次元コードを表示させる。２次元コードは、認証に必要な情報を含む。本実施形態では、この情報の一例としてトークンを説明する。トークンは、ユーザＩＤを特定できるワンタイムな情報である。２次元コードには、トークン以外の情報が含まれていてもよく、例えば、ユーザＩＤやパスワード等の情報が含まれていてもよい。トークン以外の情報によって２次元コード認証が実現されてもよい。

[0038] 例えば、ユーザ端末20には、本実施形態に係る認証サービスのアプリがインストールされている。ユーザ端末20のアプリが起動すると、ユーザ端末20は、サーバ10により発行されたトークンを取得し、トークンを含む2次元コードを表示される。なお、トークンは、予めユーザ端末20に記憶されていてもよい。

[0039] ユーザは、2次元コードを表示させたユーザ端末20を撮影部36に近づける。撮影部36が2次元コードを読み取ると、認証装置30は、2次元コードに含まれるトークンを取得し、自身の場所を一意に識別する場所IDとともにサーバ10に送信する。サーバ10は、これらの情報を受信すると、2次元コード認証を実行する。サーバ10は、2次元コード認証が成功すると、認証装置30にその旨を通知する。認証装置30が通知を受信すると、セキュリティゲートSGのロックが解除され、ユーザは、セキュリティゲートSGを通過できる。

[0040] なお、2次元コード認証が実行される前に、認証装置30の表示部35に表示されたボタンB35cが選択されると、図2の画面に戻る。図2の画面において、ユーザは、2段階認証のボタンB35bを選択し、2段階認証を実行することができる。例えば、ユーザがボタンB35bを選択すると、表示部35には、2段階認証の案内が表示される。

[0041] 図4は、2段階認証が実行される様子を示す図である。図4に示すように、ユーザは、撮影部36に自身の顔を撮影させる。ユーザは、操作部34を操作して、表示部35に表示された入力フォームF35dに、自身のパスコードを入力する。ユーザがボタンB35eを選択すると、撮影部36により撮影された画像と、入力フォームF35dに入力されたパスコードと、がサーバ10に送信され、顔認証とパスコード認証の2段階認証が実行される。図4に示すように、2段階認証が成功すると、セキュリティゲートSGのロックが解除され、ユーザは、セキュリティゲートSGを通過できる。

[0042] 上記のように、本実施形態では、2つの認証方法の中からユーザの好きな認証方法を選択することができる。2次元コード認証は、ユーザがユーザ端

末 2 0 を持参する必要があるが、2 段階認証は、ユーザが手ぶらであっても認証可能なので、2 段階認証の方が、ユーザの利便性が高い。しかしながら、互いに顔が似たユーザが同じパスコードを登録していると、セキュリティゲート S G の前にいるユーザが、どのユーザなのかを判別することができない。また、セキュリティゲート S G の前にいるユーザが、他のユーザとして認証されてしまい、他のユーザに成りすましてセキュリティゲート S G を通過する可能性もある。

[0043] この点、互いに顔が似た複数のユーザが同じパスコードを使用することを防止するために、利用登録時においてユーザにパスコードの一部だけ（例えば、パスコードの下 4 桁）を指定させ、残りの部分（例えば、パスコードの上 2 桁）は認証システム S 側で生成することが考えられる。しかしながら、ユーザは、認証システム S 側で生成した部分も覚えなければならないので、利便性が悪い。

[0044] また、互いに顔が似た複数のユーザが同じパスコードを使用する場合に、メールアドレスや電話番号などのように、これらのユーザで異なる情報の一部を入力させて追加の認証を行うことも考えられる。しかしながら、この場合も、追加の認証のための入力が必要になるので、利便性が悪い。このため、利便性の低下を防止しつつ、セキュリティを高める方法が求められている。

[0045] そこで、本実施形態では、ある場所のセキュリティゲート S G で、ユーザが 2 次元コード認証を成功させた場合に、当該ユーザと当該場所とをサーバ 1 0 に関連付けて記録しておき、次回以降は、その場所で 2 段階認証をすることができるようにしている。ユーザは、初めて行った場所では、2 段階認証を利用することができず、2 次元コード認証を利用する必要があることになる。

[0046] 例えば、互いに顔が似たユーザが同じパスコードを登録していたとしても、互いに同じ場所で 2 次元コード認証を成功させていなければ、他のユーザに成りすますことができない。このため、追加認証を求める必要がなくなり

、利便性の低下を防止しつつ、セキュリティを高めることができる。ユーザは、ある場所の2次元コード認証を成功させると、次回以降は、手ぶらでその場所に行ったとしても、セキュリティゲートSGを通過できる。

[0047] 図5～図9は、認証システムSの処理の一例を説明するための図である。図5に示すように、本実施形態では、複数の場所の各々にセキュリティゲートSGが配置されている。図5の例では、エリアA0～A3の各々に、セキュリティゲートSG00～SG32が配置されている。以降、エリアA0～A3を区別しないときは、単にエリアAと記載する。セキュリティゲートSG00～SG32を区別しないときは、単にセキュリティゲートSGと記載する。

[0048] 図5の例では、ユーザA、Bは、互いに顔が似ており同じパスコードを登録している。例えば、ユーザAは、エリアA0、A1のセキュリティゲートSGで2次元コード認証を成功させたとする。このため、ユーザAは、エリアA0、A1のセキュリティゲートSGで2段階認証が可能となる。ユーザAは、エリアA0、A1の全てのセキュリティゲートSGで2次元コード認証を成功させる必要はなく、同一エリア内の何れかのセキュリティゲートSGで2次元コード認証を成功させればよい。例えば、ユーザAがセキュリティゲートSG00で2次元コード認証を成功させると、セキュリティゲートSG00だけでなく、同一エリアの他のセキュリティゲートSG01、SG02についても2段階認証が可能となる。

[0049] また例えば、ユーザBは、エリアA1、A3のセキュリティゲートSGで2次元コード認証を成功させたとする。このため、ユーザBは、エリアA1、A3のセキュリティゲートSGで2段階認証が可能となる。ユーザBは、エリアA1、A3の全てのセキュリティゲートSGで2次元コード認証を成功させる必要はなく、同一エリア内の何れかのセキュリティゲートSGで2次元コード認証を成功させればよい。例えば、ユーザBがセキュリティゲートSG10で2次元コード認証を成功させると、セキュリティゲートSG10だけでなく、同一エリアの他のセキュリティゲートSG11～SG13に

についても２段階認証が可能となる。

[0050] 図６に示すように、例えば、ユーザＡが、エリアＡ０のセキュリティゲートＳＧ００でボタンＢ３５ｂを選択すると、２段階認証をすることができる。エリアＡ０は、ユーザＢがまだ２次元コード認証をしていないエリア（まだ訪れていないエリア）である。サーバ１０には、ユーザＢがエリアＡ０で２次元コード認証をした旨の記録が存在しないので、ユーザＡがエリアＡ０で２段階認証をしようとした場合に、ユーザＢとして認証されないようになっている。このため、サーバ１０は、２段階認証だったとしても、ユーザＡがセキュリティゲートＳＧ００を通過しようとしていることを特定できる。

[0051] また例えば、ユーザＢが、エリアＡ３のセキュリティゲートＳＧ３１でボタンＢ３５ｂを選択すると、２段階認証をすることができる。エリアＡ３は、ユーザＡがまだ２次元コード認証をしていないエリア（まだ訪れていないエリア）である。サーバ１０には、ユーザＡがエリアＡ３で２次元コード認証をした旨の記録が存在しないので、ユーザＢがエリアＡ３で２段階認証をしようとした場合に、ユーザＡとして認証されないようになっている。このため、サーバ１０は、２段階認証だったとしても、ユーザＢがセキュリティゲートＳＧ３１を通過しようとしていることを特定できる。

[0052] 図７に示すように、ユーザＢが、エリアＡ２のセキュリティゲートＳＧ２０を通過しようとする場合、初めて行く場所なので、２次元コード認証を成功させる必要がある。ユーザＢが２次元コード認証を成功させると、ユーザＢとエリアＡ２とが関連付けられてサーバ１０に記録される。即ち、ユーザＢが２段階認証を利用可能なエリアとして、エリアＡ２が追加される。ユーザＢは、次回以降、エリアＡ２で２段階認証を利用できるようになる。この点は、エリアＡ３についても同様である。ユーザＡについても同様に、ユーザＡが、新たなエリアＡで２次元コード認証を成功させると、次回以降、そのエリアＡで２段階認証を利用できるようになる。

[0053] 図８に示すように、ユーザＡが、エリアＡ２のセキュリティゲートＳＧ２０で２段階認証を選択したとする。ユーザＡは、エリアＡ２で２次元コード

認証を済ませていないが、エリア A 2 で 2 次元コード認証を済ませており 2 段階認証が可能なユーザ B と顔が似ておりパスコードも同じである。このため、2 段階認証を実行すると、認証システム S は、ユーザを判別できず、成りすましの可能性もある。図 8 のような場合には、セキュリティを高めるために、追加認証として、電話番号認証が行われる。

[0054] 図 9 に示すように、ユーザ A, B の各々がエリア A 1 で 2 段階認証を選択したとする。ユーザ A, B は、ともにエリア A 1 で 2 次元コード認証を済ませており、互いに顔が似ておりパスコードも同じである。このため、2 段階認証を実行すると、認証システム S は、ユーザを判別できず、成りすましの可能性もある。図 9 のような場合には、セキュリティを高めるために、追加認証として、電話番号認証が行われる。

[0055] 図 10 は、追加認証が行われる様子を示す図である。図 10 に示すように、図 8 又は図 9 のような状況が発生した場合、認証装置 30 の表示部 35 には、追加認証を行うことを示すメッセージが表示される。追加認証によって、セキュリティゲート S G を通過しようとしているユーザが識別される。追加認証が成功するまで、セキュリティゲート S G は、ロックされたままとなる。

[0056] 図 10 に示すように、表示部 35 には、追加認証においてユーザが入力すべき内容が表示される。本実施形態では、追加認証において、電話番号の一部の入力が要求されるものとするが、メールアドレス等の他の情報の入力が要求されてもよい。ユーザ A は、表示部 35 に表示された追加認証の案内に従い、入力フォーム F 35 g に、自身の電話番号の下 4 桁を入力する。ここでは、ユーザ A, B の電話番号の下 4 桁は異なるものとする。

[0057] ユーザがボタン B 35 h を選択すると、入力フォーム F 35 g に入力された電話番号の下 4 桁がサーバ 10 に送信され、追加認証が実行される。追加認証が成功すると、セキュリティゲート S G のロックが解除され、ユーザは、セキュリティゲート S G を通過することができる。ユーザ B についても同様にして、追加認証が行われる。

[0058] 以上のように、本実施形態の認証システムSは、ユーザが2次元コード認証を成功させた場所をサーバ10に記録しておき、次回以降に同じ場所で2段階認証できるようにすることによって、利便性の低下を防止しつつ、セキュリティを十分に高めるようにしている。以降、この技術の詳細を説明する。

[0059] [3. 認証システムにおいて実現される機能]

図11は、本実施形態の認証システムSで実現される機能の一例を示す機能ブロック図である。ここでは、サーバ10、ユーザ端末20、及び認証装置30の各々で実現される機能を説明する。

[0060] [3-1. サーバにおいて実現される機能]

図11に示すように、サーバ10では、データ記憶部100、第1認証部101、記録部102、第2認証部103、制限部104、判定部105、要求部106、第3認証部107、及び処理実行部108が実現される。

[0061] [データ記憶部]

データ記憶部100は、記憶部12を主として実現される。データ記憶部100は、認証に必要なデータを記憶する。ここでは、データ記憶部100が記憶するデータの一例として、ユーザデータベースDB1と、場所データベースDB2と、について説明する。

[0062] 図12は、ユーザデータベースDB1のデータ格納例を示す図である。図12に示すように、ユーザデータベースDB1は、ユーザに関する各種情報が格納されたデータベースである。ユーザデータベースDB1には、ユーザID、ユーザの氏名、パスワード、アップロードされた顔写真のデータ、顔写真から計算された顔の特徴量、パスコード、パスコードの登録日時、電話番号、メールアドレス、及びトークン等が格納される。ユーザデータベースDB1に格納されるこれらの情報は、ユーザ情報の一例である。

[0063] 例えば、ユーザが利用登録をすると、ユーザデータベースDB1に新たなレコードが作成される。新たなレコードには、ユーザIDに関連付けて、氏名、パスワード、パスコード、パスコードの登録日時、電話番号、メールア

ドレス、顔写真、及び当該顔写真に基づいて計算された特徴量が格納される。なお、ユーザが自らユーザIDを指定しない場合には、サーバ10は、ユーザIDを新たに発行する。

[0064] サーバ10は、ユーザに対してトークンを発行すると、当該ユーザのユーザIDに関連付けてトークンを格納する。サーバ10は、ユーザ端末20に対し、発行したトークンを送信する。ユーザ端末20は、トークンを受信すると、トークンを含む2次元コードを表示部25に表示させる。本実施形態のトークンは、ワンタイムな情報なので、2次元コード認証で使用されると無効になる。再び2次元コード認証が実行される場合には、新たなトークンが発行される。トークンは、任意の発行方法によって発行されるようにすればよく、例えば、ランダムな文字列を生成するアルゴリズムによってトークンが発行されてもよい。また、トークンに有効期限が設定される場合には、ユーザデータベースDB1に有効期限が格納されてもよい。

[0065] ユーザデータベースDB1に格納されるパスワード、顔の特徴量、パスコード、及びトークンは、認証情報の一種である。電話番号及びメールアドレスについても、認証で利用可能なので、認証情報の一種といえる。

[0066] 認証情報とは、認証時に参照される情報である。認証情報は、認証方法によって呼び名が異なる。例えば、電子スタンプ認証であれば、スタンプのマルチタッチパターンが認証情報となり、合言葉認証であれば、合言葉が認証情報となる。認証情報は、任意の目的で利用されてよい。本実施形態では、顔の特徴量、パスコード、電話番号、及びトークンは、ユーザがセキュリティゲートを通過するために利用される。なお、顔写真が認証情報に相当してもよい。

[0067] 顔の特徴量は、顔の特徴を数値化した情報であり、例えば、色合い、顔のパーツの相対位置、大きさ、又は形状などの特徴が示されている。本実施形態では、顔写真が示す顔の特徴量を予め計算しておくものとするが、顔の特徴量は、認証時にその場で計算されてもよい。複数の顔写真が登録される場合には、顔写真ごとに、顔の特徴量が計算される。顔認証自体は、種々の手

法を適用可能であり、例えば、主成分分析、線形判別分析、弾性マッチング、又は隠れマルコフモデルといった手法を利用可能であり、特徴量は、これらの手法に応じた計算式で計算されるようにすればよい。例えば、顔の特徴量は、多次元のベクトルで示されるものとするが、配列や単一の数値といった他の形式で示されてもよい。

[0068] パスコードは、先述したように、認証のために用いられる所定桁数の番号である。パスコードは、P I N (Personal Identification Number) 又は暗証番号と呼ばれることもある。パスコードとパスワードは、似た概念であるが、パスコードが数字のみから構成されるのに対し、パスワードは、任意の種類の記号によって構成される点で異なる。また、本実施形態では、パスコードは、桁数が決められているのに対し、パスワードは、任意の桁数で設定可能な点でも異なる。パスコードは、桁数が決められていなくてもよい。

[0069] なお、ユーザデータベース D B 1 に格納される情報は、図 1 2 の例に限られず、ユーザに関する任意の情報が格納されてよい。例えば、正当に認証されたユーザに対し、一定期間だけ有効な認証情報が発行される場合には、当該認証情報がユーザデータベース D B 1 に格納されてもよい。また例えば、ユーザの生年月日、住所、クレジットカード番号、又は銀行口座の番号といった任意のユーザ情報がユーザデータベース D B 1 に格納されてよい。

[0070] 図 1 3 は、場所データベース D B 2 のデータ格納例を示す図である。図 1 3 に示すように、場所データベース D B 2 は、複数の場所の各々で 2 次元コード認証を成功させたユーザに関する情報が格納されたデータベースである。例えば、場所データベース D B 2 には、場所 I D、エリア名、及びユーザ I D が格納される。場所 I D は、エリアを一意に識別する情報である。エリア名についても、エリアを一意に識別する情報といえる。

[0071] 場所データベース D B 2 に格納されたユーザ I D は、場所 I D が示す場所で 2 次元コード認証を成功させたユーザのユーザ I D である。場所 I D とユーザ I D が同じレコードに格納されていることは、場所 I D とユーザ I D が関連付けられていることに相当する。本実施形態では、場所データベース D

B 2 にユーザ I D と場所 I D が関連付けられる場合を説明するが、ユーザデータベース D B 1 又は他のデータベースに、これらの関連付けが格納されてもよい。

[0072] [第 1 認証部]

第 1 認証部 1 0 1 は、制御部 1 1 を主として実現される。第 1 認証部 1 0 1 は、第 1 の認証方法に基づいて、認証をする。本実施形態では、2次元コード認証は、第 1 の認証方法に相当する。このため、本実施形態で2次元コード認証と記載した箇所は、第 1 の認証方法と読み替えることができる。第 1 の認証方法は、任意の認証方法であってよく、2次元コード認証に限られない。ただし、第 1 の認証方法は、後述する第 2 の認証方法よりも精度が高いものとする。精度とは、認証の信頼度又はセキュリティレベルである。

[0073] 例えば、第 1 の認証方法の認証は、ユーザ端末 2 0 を利用した認証である。ユーザ端末 2 0 を利用した認証とは、ユーザ端末 2 0 から認証情報が出力される認証である。この認証情報は、ユーザ端末 2 0 に予め記憶されていてもよいし、特にユーザ端末 2 0 に予め記憶されず、ワンタイムで発行されてもよい。例えば、ユーザ端末 2 0 に認証情報そのものを表示させること、ユーザ端末 2 0 に認証情報を含むコード情報を表示させること、ユーザ端末 2 0 から認証情報を送信させること、又はユーザ端末 2 0 から認証情報を音声出力することによって行われる認証は、ユーザ端末 2 0 を利用した認証に相当する。

[0074] また例えば、第 1 の認証方法は、入力認証情報と登録認証情報との一致によって成否が判定され、第 2 の認証方法は、入力認証情報と登録認証情報との類似によって成否が判定される。

[0075] 入力認証情報とは、入力された認証情報である。入力認証情報は、コンピュータに対して入力された認証情報である。別の言い方をすれば、入力認証情報は、登録認証情報と比較される情報、又は、認証時のクエリとなる情報ということもできる。入力認証情報は、ユーザの操作により入力された認証情報であってもよいし、撮影部 3 6 などのセンサの検出結果により入力され

た認証情報であってもよい。

[0076] 登録認証情報とは、予め登録された認証情報である。登録認証情報は、認証時の正解となる認証情報である。別の言い方をすれば、登録認証情報は、入力認証情報と比較される情報であり、認証時のインデックスとなる情報である。登録認証情報は、ユーザの利用登録時に登録される。登録認証情報は、事後的に変更可能である。

[0077] 一致とは、入力認証情報と、登録認証情報と、が同一であることを意味する。ここでの一致は、部分一致ではなく、完全一致を意味する。このため、認証情報の一致が判定される場合には、認証情報が一部でも異なっていれば、認証が失敗する。例えば、トークンを利用した認証では、トークンの一致が判定される。また例えば、パスコード認証では、パスコードの一致が判定される。また例えば、パスワード認証では、パスワードの一致が判定される。

[0078] 類似とは、入力認証情報と、登録認証情報と、が似ているか否かである。別の言い方をすれば、類似とは、入力された認証情報と、登録された認証情報と、の差又は違いである。例えば、生体認証では、生体認証情報の類似が判定される。生体認証では、特徴量化された認証情報が利用されるので、特徴量の差（距離）が閾値未満であれば類似となり、差が閾値以上であれば非類似となる。

[0079] 第1の認証方法は、認証情報の完全一致によって成否が判定され、第2の認証方法は、認証情報が違っていても、その違いが閾値未満であれば成功となる。また例えば、第1の認証方法は、認証情報の類似によって成否が判定されてもよいが、この場合、成否の判定における閾値が第2の認証方法よりも小さい。即ち、第1の認証方法は、第2の認証方法よりも成功と判定される条件（基準）が厳しいものとする。例えば、第1の認証方法は、パスワード認証であってもよい。また例えば、第1の認証方法は、顔認証よりも条件が厳しい指紋認証であってもよい。また例えば、第1の認証方法は、多段階認証であってもよい。この場合、第1の認証方法は、第2の認証方法

よりも認証の段階数が多くてもよい。

[0080] 例えば、第1認証部101は、2段階認証が失敗した場合に、2次元コード認証に基づいて、認証対象ユーザの認証を行うようにしてもよい。

[0081] 認証対象ユーザは、入力認証情報によって認証されるユーザである。別の言い方をすれば、認証対象ユーザは、認証システムSが正当性（誰であるか）を確認するユーザである。例えば、2次元コード認証又はパスコード認証のように、ユーザが自分で入力認証情報を入力する場合には、入力認証情報を入力したユーザは、認証対象ユーザに相当する。また例えば、生体認証のように、ユーザが検出されることによって入力認証情報が入力される場合には、検出対象となったユーザは、認証対象ユーザに相当する。

[0082] 第1認証部101は、第2の認証方法の認証が失敗した場合に、認証対象ユーザに対し、強制的に2次元コード認証を要求してもよいし、ユーザが2次元コード認証を選択した場合に2次元コード認証をしてもよい。本実施形態では、第1認証部101は、2次元コード認証が選択された場合に、2次元コード認証を行うものとする。

[0083] [記録部]

記録部102は、制御部11を主として実現される。記録部102は、2次元コード認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けてデータ記憶部100に記録する。記録部102は、2次元コード認証が成功したことを条件として、認証されたユーザと、当該ユーザがいる場所と、を関連付ける。

[0084] ユーザと場所を関連付けるとは、ユーザを識別する情報と、場所を識別する情報と、を互いに検索可能に記録することである。本実施形態では、ユーザIDと場所IDを場所データベースDB2に格納することが、ユーザと場所とを関連付けることに相当する。なお、ユーザは、ユーザ名などの他の情報によって識別されてもよい。場所は、エリア名などの他の情報によって識別されてもよい。

[0085] 例えば、ある認証対象ユーザの2段階認証が失敗した後に、2次元コード

認証が実行されることがあるので、記録部 102 は、当該 2 次元コード認証が成功した場合に、認証された当該認証対象ユーザと、当該認証対象ユーザがいる場所と、を関連付けてデータ記憶部 100 に記録する。例えば、2 段階認証が失敗した後に、認証対象ユーザが 2 次元コード認証を選択すると、2 次元コード認証が実行される。この場合に、記録部 102 は、2 次元コード認証が成功したことを条件として、認証対象ユーザのユーザ ID と、その場所の場所 ID と、を関連付ける。

[0086] 本実施形態では、エリアが場所に相当するので、記録部 102 は、2 次元コード認証で認証されたユーザがいる場所として、当該ユーザがいるエリアをデータ記憶部 100 に記録する。場所は、エリアのように一定の広さを有する領域でなくてもよく、緯度経度又は座標のようにピンポイントで表現されるものであってもよい。また、認証装置 30 を利用して認証が行われるので、記録部 102 は、2 次元コード認証で認証されたユーザと、当該ユーザの認証で用いられた認証装置 30 の場所と、を関連付けてデータ記憶部 100 に記録することになる。

[0087] [第 2 認証部]

第 2 認証部 103 は、制御部 11 を主として実現される。第 2 認証部 103 は、第 2 の認証方法に基づいて、認証をする。本実施形態では、2 段階認証は、第 2 の認証方法に相当する。このため、本実施形態で 2 段階認証と記載した箇所は、第 2 の認証方法と読み替えることができる。第 2 の認証方法は、任意の認証方法であってよく、2 段階認証に限られない。ただし、第 2 の認証方法は、第 1 の認証方法よりも精度が低いものとする。その代わりに、第 2 の認証方法は、第 1 の認証方法よりも利便性が高いものとする。

[0088] 利便性は、認証対象ユーザの使い勝手の良さ（手軽さ）である。例えば、認証時にユーザ端末 20 を利用しなくてよいことは、利便性が高いことに相当する。また例えば、認証対象ユーザによる認証時の入力量が少ないことは、利便性が高いことに相当する。例えば、第 2 の認証方法は、顔認証だけであってもよいし、パスコード認証だけであってもよい。また例えば、第 2 の

認証方法は、顔認証以外の生体認証であってもよいし、電子スタンプ認証であってもよい。

[0089] 例えば、２段階認証では、入力認証情報と登録認証情報とが比較される。第２認証部１０３は、認証対象ユーザの入力認証情報と、比較対象として取得された登録認証情報と、に基づいて認証を行う。比較対象として取得されなかった登録認証情報は、２段階認証では用いられないことになる。このため、２段階認証では、比較対象として取得されなかった登録認証情報のユーザとして認証されることはない。

[0090] 本実施形態では、ユーザが認証方法を選択できるので、第２認証部１０３は、２段階認証が選択された場合に、２段階認証を行う。第２認証部１０３は、２段階認証が選択されたことを条件として、２段階認証を行う。例えば、２段階認証は、認証情報の類似に基づく認証方法と、認証情報の一致に基づく認証方法と、を含む。２段階認証は、これらに限られず、任意の組み合わせを適用可能である。

[0091] [制限部]

制限部１０４は、制御部１１を主として実現される。制限部１０４は、２段階認証における認証対象ユーザと、当該認証対象ユーザがいる場所と、がデータ記憶部１００に関連付けられていない場合に、２段階認証が成功することを制限する。制限部１０４は、これらに関連付けられている場合には、２段階認証が成功することを制限しない。

[0092] 制限とは、２段階認証の成功を禁止することである。例えば、認証が成功する条件（認証情報の一致又は類似）が満たされたとしても、強制的に認証失敗とすることは、制限に相当する。また例えば、認証対象ユーザがいる場所が関連付けられたユーザの登録認証情報しか、入力認証情報との比較対象としないことは、制限に相当する。また例えば、認証処理をそもそも実行しないことは、制限に相当する。

[0093] 例えば、制限部１０４は、認証対象ユーザがいる場所が関連付けられたユーザの登録認証情報を、認証対象ユーザの入力認証情報との比較対象として

取得する。比較対象とは、認証時のインデックスになることである。制限部 104 は、認証対象ユーザがいる場所が関連付けられていないユーザの登録認証情報を、比較対象とはしないことによって、2段階認証が成功することを制限する。即ち、制限部 104 は、認証対象ユーザがいる場所が関連付けられていないユーザの登録認証情報は、比較対象から除外する。

[0094] 本実施形態では、エリアが場所に相当するので、制限部 104 は、認証対象ユーザと、当該認証対象ユーザがいるエリアと、がデータ記憶部 100 に関連付けられていない場合に、2段階認証が成功することを制限する。また、制限部 104 は、認証対象ユーザと、当該認証対象ユーザの認証で用いられる認証装置 30 の場所と、が関連付けられていない場合に、2段階認証が成功することを制限する。

[0095] [判定部]

判定部 105 は、制御部 11 を主として実現される。判定部 105 は、認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられている場合に、2段階認証で、認証対象ユーザが他のユーザとして認証される可能性があるか否かを判定する。他のユーザとは、認証対象ユーザ以外のユーザである。認証対象ユーザが他のユーザとして認証される可能性とは、認証対象ユーザではないユーザとして誤って認証される可能性である。以降、この可能性を誤認証の可能性と記載する。

[0096] 例えば、入力認証情報と登録認証情報との類似によって判定される認証方法では、判定部 105 は、複数の登録認証情報が入力認証情報と類似する場合に、誤認証の可能性があると判定する。例えば、認証対象のユーザが、認証対象のユーザと他のユーザとを含む複数のユーザの各々として認証される状態は、誤認証の可能性があると相当する。

[0097] また例えば、判定部 105 は、入力認証情報と複数の登録認証情報の各々との類似度を取得し、当該取得された類似度の差に基づいて、誤認証の可能性があるか否かを判定してもよい。本実施形態の顔認証では、ベクトル空間上における特徴量の距離が類似度に相当するので、判定部 105 は、各登録

認証情報の距離の差に基づいて、誤認証の可能性があるか否かを判定する。
この差が閾値以上の場合には、誤認証の可能性がないことに相当し、この差が閾値未満の場合には、誤認証の可能性のあることに相当する。

[0098] また例えば、判定部 105 は、入力認証情報に類似するとされた登録認証情報の類似度と、入力認証情報に類似しないとされた登録認証情報の類似度と、を取得し、当該取得された類似度の差に基づいて、誤認証の可能性があるか否かを判定してもよい。この差が閾値以上の場合には、誤認証の可能性がないことに相当し、この差が閾値未満の場合には、誤認証の可能性のあることに相当する。即ち、認証対象ユーザと認証されずに、他のユーザと認証される状態は、誤認証の可能性のあることに相当する。

[0099] 本実施形態では、2段階認証が実行されるので、判定部 105 は、顔認証とパスコード認証の両方において、認証対象ユーザが他のユーザとして認証される可能性があるか否かを判定する。顔認証における誤認証の可能性の判定方法は、上述した通りである。パスコード認証は、認証情報の一致によって判定されるので、例えば、入力認証情報と一致する登録認証情報が複数存在する場合には、誤認証の可能性のあることに相当する。判定部 105 は、顔認証で誤認証の可能性があり、かつ、パスコード認証で誤認証の可能性がある場合に、誤認証の可能性があると判定する。

[0100] [要求部]

要求部 106 は、制御部 11 を主として実現される。要求部 106 は、誤認証の可能性があると判定された場合に、認証対象ユーザに対し、2次元コード認証又は第3の認証方法の認証を要求する。第3の認証方法は、第1の認証方法でも第2の認証方法でもない認証方法である。第3の認証方法は、第1の認証方法よりも精度が高くても低くてもよい。また、第3の認証方法は、第1の認証方法よりも精度が高くても低くてもよい。

[0101] 本実施形態では、電話番号認証は、第3の認証方法に相当する。このため、本実施形態で電話番号認証と記載した箇所は、第3の認証方法と読み替えることができる。第3の認証方法は、任意の認証方法であってよく、電話番

号認証に限られない。例えば、第3の認証方法は、パスワード認証、合言葉認証、メールアドレス認証、又は顔認証以外の生体認証であってもよい。ユーザが登録した個人情報を第3の認証方法で利用する場合には、その全部の入力が要求されてもよいし、誤認証の可能性のあるユーザ同士で相違する部分だけの入力が要求されてもよい。

[0102] [第3認証部]

第3認証部107は、制御部11を主として実現される。第3認証部107は、2段階認証が失敗した場合に、電話番号認証に基づいて、認証対象ユーザの認証をする。電話番号認証の場合、認証情報の一致によって認証の成否が決まるので、第3認証部107は、入力認証情報と登録認証情報が一致するか否かを判定し、認証を行う。本実施形態では、データ記憶部100には、電話番号認証が成功したとしても、認証された認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられない。これらが関連付けられるのは、あくまで2次元コード認証が成功された場合である。

[0103] [処理実行部]

処理実行部は、制御部11を主として実現される。処理実行部108は、2次元コード又は2段階認証が成功した場合に、所定の処理を実行する。所定の処理は、認証が成功した場合に実行が許可される処理である。本実施形態では、セキュリティゲートSGのロックを解除するための処理が所定の処理に相当する場合を説明するが、所定の処理は、任意の処理を適用可能である。例えば、所定の処理は、サーバ又は端末へのログイン処理、コンピュータのロックを解除する処理、データの閲覧を許可する処理、データの書き込みを許可する処理、自動ドアを開閉する処理、電子投票を許可する処理、又は公的文書の取得を許可する処理であってよい。

[0104] 処理実行部108は、自らロック解除の制御をしてもよいが、本実施形態では、認証装置30の処理実行部303がロック解除の制御を実行するので、処理実行部108は、認証装置30に対し、認証結果を通知する。例えば、処理実行部108は、認証が失敗した場合には、認証が成功したことを示

す通知を送信せず、認証が成功した場合に、認証が成功したことを示す通知を送信する。なお、ユーザによる認証が一定回数成功しなかった場合には、ユーザが入力したパスコードが格納されたレコード、又は、ユーザと顔が類似する特徴量が格納されたレコードの認証情報がロックされて使用できなくなるようにしてもよい。

[0105] [3-2. ユーザ端末において実現される機能]

図11に示すように、ユーザ端末20では、データ記憶部200、受付部201、及び送信部202が実現される。なお、本実施形態では、ユーザ端末20が認証システムSに含まれる場合を説明するが、ユーザ端末20は、認証システムSと通信可能な外部装置であってもよい。

[0106] [データ記憶部]

データ記憶部200は、記憶部22を主として実現される。データ記憶部200は、登録申請に必要なデータを記憶する。例えば、データ記憶部200は、ユーザの顔写真のデータを記憶する。また例えば、データ記憶部200は、ユーザID及びパスワードを記憶してもよい。また例えば、データ記憶部200は、2次元コードの生成プログラムや認証サービスのアプリを記憶してもよい。

[0107] [受付部]

受付部201は、制御部21を主として実現される。受付部201は、ユーザが登録申請をするための入力操作を受け付ける。例えば、受付部201は、ユーザID、パスワード、顔写真のファイル名等、パスコード、電話番号、及びメールアドレスの入力を受け付ける。なお、受付部201が受け付ける入力操作は、これらに限られず、他の種々の入力操作を受け付け可能である。例えば、受付部201は、2次元コードを表示させる操作を受け付けてもよい。

[0108] [送信部]

送信部202は、制御部21を主として実現される。送信部202は、受付部201により受け付けられた入力操作に基づいて、登録申請をするため

のデータを送信する。例えば、送信部 202 は、ユーザによる入力操作に基づいて、ユーザ ID、パスワード、顔写真のデータ、パスコード、電話番号、及びメールアドレスをサーバ 10 に送信する。なお、送信部 202 が送信するデータは、これらに限られず、他の種々のデータを送信可能である。

[0109] [3-3. 認証装置において実現される機能]

図 11 に示すように、認証装置 30 では、データ記憶部 300、受付部 301、送信部 302、及び処理実行部 303 が実現される。なお、本実施形態では、認証装置 30 が認証システム S に含まれる場合を説明するが、認証装置 30 は、認証システム S と通信可能な外部装置であってもよい。また、本実施形態では、第 1 の認証方法及び前記第 2 の認証方法の各々に対応した複数の認証装置 30 が存在するものとする。

[0110] [データ記憶部]

データ記憶部 300 は、記憶部 32 を主として実現される。データ記憶部 300 は、認証に必要なデータを記憶する。例えば、データ記憶部 300 は、サーバ 10 の IP アドレス等の情報を記憶する。また例えば、データ記憶部 300 は、表示部 35 に入力フォームやボタンなどを表示させるためのデータ（例えば、HTML データや画像データ）を記憶する。

[0111] [受付部]

受付部 301 は、制御部 31 を主として実現される。受付部 301 は、入力操作を受け付ける。入力操作は、認証に必要な入力操作であればよく、本実施形態では、受付部 301 は、2 次元コード認証又は 2 段階認証の何れかの選択を受け付ける。受付部 301 は、認証に必要な情報の入力操作も受け付ける。顔認証についてはユーザの入力操作は要しないので、受付部 301 は、パスコードの入力操作を受け付ける。

[0112] なお、受付部 301 は、認証システム S で利用する認証の種類に応じた入力操作を受け付けられればよく、例えば、指紋認証が利用される場合には、ユーザがカメラやセンサなどの上に指を置く入力操作を受ける。また例えば、筆跡認証が利用される場合には、ユーザがタッチパネルなどの上で文字を書く

入力操作を受け付ける。また例えば、パスワード認証又は合言葉認証が利用される場合には、受付部 301 は、パスワード又は合言葉の入力操作を受け付ける。合言葉は、認証装置 30 にマイクを備えておき、当該マイクによって検出されるようにすればよい。

[0113] [送信部]

送信部 302 は、制御部 31 を主として実現される。送信部 302 は、入力操作に基づいて、認証に必要な情報を送信する。送信部 302 は、認証情報そのものを送信してもよいし、認証情報を特定するための情報を送信してもよい。

[0114] なお、本実施形態では、第 1 認証部 101 と第 2 認証部 103 がサーバ 10 により実現される場合を説明するので、送信部 302 は、サーバ 10 にデータを送信する場合を説明するが、他のコンピュータによって第 1 認証部 101 と第 2 認証部 103 が実現される場合には、当該他のコンピュータにデータを送信してもよい。例えば、第 1 認証部 101 と第 2 認証部 103 が別々のコンピュータで実現される場合には、送信部 302 は、これらのコンピュータに情報を送信すればよい。

[0115] 本実施形態では、第 1 の認証方法が 2 次元コード認証なので、送信部 302 は、2 次元コードに含まれる認証情報を送信する。サーバ 10 側で 2 次元コードの解析を実行する場合には、送信部 302 は、2 次元コードの撮影画像を送信する。また、第 2 の認証方法が 2 段階認証なので、送信部 302 は、撮影部 36 により撮影された撮影画像（顔写真）と、入力されたパスコードと、を送信する。なお、認証装置 30 側で顔の特徴量が計算されてもよく、この場合には、送信部 302 は、画像の代わりに、当該計算された顔の特徴量を送信する。また、第 3 の認証方法が電話番号認証なので、送信部 302 は、入力された電話番号を送信する。

[0116] なお、送信部 302 は、認証システム S で利用する認証の種類に応じた情報を送信すればよく、例えば、指紋認証が利用される場合には、送信部 302 は、ユーザの指の画像を送信してもよいし、画像から計算された指の特徴

量を送信してもよい。また例えば、筆跡認証が利用される場合には、送信部 302 は、ユーザがタッチパネルなどの上に書いた文字の画像を送信してもよいし、タッチ位置の変化を示す座標情報を送信してもよい。また例えば、パスワード認証又は合言葉認証が利用される場合には、送信部 302 は、ユーザが入力したパスワード又は合言葉を送信する。

[0117] [処理実行部]

処理実行部 303 は、制御部 31 を主として実現される。処理実行部 303 は、2次元コード認証又は2段階認証が成功した場合に、所定の処理を実行する。追加認証として電話番号認証が行われる場合には、処理実行部 303 は、電話番号認証が成功した場合に、所定の処理を実行する。所定の処理の意味は、先述した通りであり、認証が成功した場合に実行が許可される処理である。

[0118] 本実施形態では、認証が成功した場合に、セキュリティゲート SG のロックが解除されるので、処理実行部 303 は、認証が成功したことを示す通知を受信した場合には、ロック機構のモータを回転等させることによってロックを解除し、認証が成功したことを示す通知を受信しなかった場合には、ロックを解除しない。なお、サーバ 10 の処理実行部 108 は、認証が成功したことを示す通知ではなく、ロック機構を解除させるための信号を送信してもよく、この場合には、認証装置 30 の処理実行部 303 は、当該信号に基づいてロックを解除すればよい。

[0119] [4. 本実施形態において実行される処理]

図 14 及び図 15 は、本実施形態において実行される処理の一例を示すフロー図である。図 14 及び図 15 に示す処理は、制御部 11, 31 が、それぞれ記憶部 12, 32 に記憶されたプログラムに従って動作することによって実行される。下記に説明する処理は、図 11 に示す機能ブロックにより実行される処理の一例である。なお、認証処理が実行されるにあたり、利用登録が完了しているものとする。

[0120] 図 14 に示すように、まず、認証装置 30 は、認証方法を選択するための

ボタン B 3 5 a, B 3 5 b を表示部 3 5 に表示させ (S 1)、操作部 3 4 の検出信号に基づいて、選択された認証方法を特定する (S 2)。S 2 においては、ボタン B 3 5 a が選択された場合に 2 次元コード認証が選択されたと判定され、ボタン B 3 5 b が選択された場合に 2 段階認証が選択されたと判定される。

[0121] 2 次元コード認証が選択された場合 (S 2 ; 2 次元コード認証)、認証装置 3 0 は、2 次元コード認証の案内を表示部 3 5 に表示させる (S 3)。S 3 における表示部 3 5 の画面表示は、図 3 の上の状態となる。ユーザは、2 次元コード認証の案内に従い、ユーザ端末 2 0 を操作して 2 次元コードを表示させる。例えば、ユーザ端末 2 0 は、サーバ 1 0 に対し、トークンの発行依頼を送信する。サーバ 1 0 は、発行依頼を受信するとトークンを発行し、ユーザ端末 2 0 に送信する。ユーザ端末 2 0 は、受信したトークンを含む 2 次元コードを表示させる。なお、トークンの発行の際に、ユーザ ID やパスワードの入力が求められてもよい。また、表示部 3 5 に表示されたボタン B 3 5 c が選択された場合、S 1 の処理に戻る。

[0122] 認証装置 3 0 は、撮影部 3 6 の検出信号に基づいて、2 次元コードを検出し (S 4)、2 次元コードに含まれるトークンを取得する (S 5)。ユーザは、ユーザ端末 2 0 に表示された 2 次元コードを撮影部 3 6 の方にかざして読み取らせる。2 次元コードの読み取り方法自体は、2 次元コードの規格に沿った手順で実行されるようにすればよい。

[0123] 認証装置 3 0 は、サーバ 1 0 に対し、場所 ID とトークンを送信する (S 6)。場所 ID は、認証装置 3 0 の記憶部 3 2 に記憶されているものとする。認証装置 3 0 は、これらの情報を送信することによって、サーバ 1 0 に 2 次元コード認証の実行を要求する。

[0124] サーバ 1 0 は、場所 ID とトークンを受信すると、ユーザデータベース DB 1 に基づいて、2 次元コード認証をする (S 7)。S 7 においては、サーバ 1 0 は、ユーザデータベース DB 1 を参照し、受信したトークンがユーザ ID に関連付けられているユーザがいるか否かを判定する。受信したトーク

ンがユーザIDに関連付けられているユーザがいる場合は認証成功となり、このユーザがいない場合には認証失敗となる。

[0125] 2次元コード認証が失敗した場合（S 7；失敗）、サーバ10は、認証装置30に対し、所定のエラーメッセージを送信し（S 8）、本処理は終了する。この場合、認証装置30の表示部35に、エラーメッセージが表示され、認証が失敗したことがユーザに通知される。その後、S 1の処理が再び実行され、他の認証方法の選択が受け付けられてもよい。

[0126] 一方、2次元コード認証が成功した場合（S 7；成功）、サーバ10は、S 7において受信した場所IDとユーザIDとを関連付けて場所データベースDB2に記録する（S 9）。S 9においては、サーバ10は、場所データベースDB2のうち、S 7において受信した場所IDが格納されたレコードに、S 7において受信したユーザIDを格納する。なお、このレコードに、S 7において受信したユーザIDが既に格納されている場合には、このユーザIDは重複して格納されない。

[0127] サーバ10は、認証装置30に対し、認証が成功したことを示す認証成功通知を送信する（S 10）。認証成功通知は、所定形式のデータが送信されることにより行われ、認証が成功したユーザの名前が含まれるものとする。

[0128] 認証装置30は、通知を受信すると、セキュリティゲートSGのロックを解除し（S 11）、認証が成功したユーザの名前を表示部35に表示させ（S 12）、本処理は終了する。ユーザは、自身の名前が表示部35に表示されたことを確認し、セキュリティゲートのドアを押して通過する。なお、この場合には、サーバ10にユーザの氏名や現在日時などの情報が通行記録として残してもよい。

[0129] 一方、S 2において、2段階認証が選択された場合（S 2；2段階認証）、図15に移り、認証装置30は、2段階認証の案内を表示部35に表示させる（S 13）。S 13における表示部35の画面表示は、図4の上の状態となる。ユーザは、2段階認証の案内に従い、撮影部36に顔を向けて撮影させ、パスコードを入力する。なお、表示部35に表示されたボタンB 35

f が選択された場合、S 1 の処理に戻る。

[0130] 認証装置 3 0 は、撮影部 3 6 の検出信号に基づいて、撮影画像を取得し（S 1 4）、操作部 3 4 の検出信号に基づいて、ユーザによるパスコードの入力を受け付ける（S 1 5）。S 1 5 においては、認証装置 3 0 は、入力フォーム F 3 5 d に対する 4 桁のパスコードの入力を受け付ける。例えば、パスコードを入力するためのソフトウェアテンキーが表示部 3 5 に表示される。なお、本実施形態では、パスコードを 4 桁とするが、パスコードは、任意の桁数であってよい。例えば、パスコードは、4 桁未満であってもよいし、5 桁以上であってもよい。

[0131] 認証装置 3 0 は、ユーザがボタン B 3 5 e を選択したことに応じて、サーバ 1 0 に対し、場所 I D、S 1 4 で取得した撮影画像、及び S 1 5 で入力されたパスコードを送信する（S 1 6）。認証装置 3 0 は、これらの情報を送信することによって、サーバ 1 0 に 2 段階認証の実行を要求する。

[0132] サーバ 1 0 においては、場所 I D、撮影画像、及びパスコードを受信すると、制御部 1 1 は、場所データベース D B 2 を参照し、受信した場所 I D に関連付けられたユーザ I D を特定する（S 1 7）。サーバ 1 0 は、ユーザデータベース D B 1 を参照し、S 1 7 で特定したユーザ I D に関連付けられた顔の特徴量とパスコードを取得する（S 1 8）。S 1 8 において取得された特徴量とパスコードは、2 段階認証における比較対象となる。S 1 8 において取得されなかった特徴量とパスコードは、比較対象とはならない。S 1 8 の処理によって、S 1 7 で受信した場所 I D が関連付けられていないユーザ I D のユーザとして認証されることを防止できる。

[0133] サーバ 1 0 は、S 1 7 で受信した撮影画像及びパスコードと、S 1 8 で取得した顔の特徴量とパスコードと、に基づいて、2 段階認証をする（S 1 9）。S 1 9 においては、サーバ 1 0 は、S 1 8 で取得した特徴量とパスコードの組み合わせの中に、S 1 7 で受信した撮影画像の特徴量が類似し、かつ、S 1 7 で受信したパスコードと一致する組み合わせがあるか否かを判定する。この組み合わせが 1 つでもあれば認証成功となり、この組み合わせがな

ければ認証失敗となる。

[0134] 2段階認証が失敗した場合（S 1 9；失敗）、S 8の処理に移行し、エラーメッセージが送信される。一方、2段階認証が成功した場合（S 1 9；成功）、サーバ1 0は、誤認証の可能性はあるか否かを判定する（S 2 0）。S 2 0においては、サーバ1 0は、S 1 9で判定した組み合わせが複数存在するか否かを判定する。誤認証の可能性があると判定されない場合（S 2 0；N）、S 1 0の処理に移行し、セキュリティゲートS Gのロックが解除される。

[0135] 一方、誤認証の可能性があると判定された場合（S 2 0；Y）、サーバ1 0は、ユーザデータベースD B 1に基づいて追加認証情報を生成し、認証装置3 0に対し、追加認証情報の入力を要求する（S 2 1）。追加認証情報の入力の要求は、追加認証情報として生成されたユーザ情報の項目が何であることを識別する情報が含まれているものとする。本実施形態では、追加認証は電話番号認証なので、サーバ1 0は、2段階認証が成功したユーザの電話番号を取得して、追加認証情報を生成する。この追加認証情報は、追加認証における正解になる認証情報なので、登録認証情報に相当する。

[0136] 認証装置3 0は、要求を受信すると、追加認証情報の入力を受け付けるための画面を表示部3 5に表示させる（S 2 2）。S 2 2における表示部3 5の画面表示は、図1 0の下の状態となる。

[0137] 認証装置3 0は、操作部3 4の検出信号に基づいて、ユーザによる追加認証情報の入力を受け付ける（S 2 3）。S 2 3においては、認証装置3 0は、入力フォームF 3 5 gに対する追加認証情報の入力を受け付ける。例えば、電話番号を入力するためのソフトウェアキーボードが表示部3 5に表示される。認証装置3 0は、ユーザがボタンB 3 5 hを選択したことに応じて、サーバ1 0に対し、S 2 3で入力された追加認証情報を送信する（S 2 4）。認証装置3 0は、追加認証情報を送信することによって、サーバ1 0に追加認証の実行を要求する。

[0138] サーバ1 0は、追加認証情報を受信すると、サーバ1 0は、追加認証をす

る（S 2 5）。S 2 5においては、サーバ1 0は、入力された追加認証情報と、Sで生成された追加認証情報と、が一致するか否かを判定し、これらが一致するユーザがいる場合は認証成功となり、これらが一致しないユーザがいない場合には認証失敗となる。追加認証が成功した場合（S 2 5；成功）、S 1 0の処理に移行する。この場合、S 9の処理は実行されない。追加認証が失敗した場合（S 2 5；失敗）、S 8の処理に移行する。

[0139] 本実施形態の認証システムSによれば、2段階認証における認証対象ユーザと、当該認証対象ユーザがいる場所と、が場所データベースDB 2に関連付けられていない場合に、2段階認証が成功することを制限することによって、成りすましを防止し、セキュリティを高めることができる。例えば、認証システムS側でパスコードの一部を生成する場合には、パスコードが覚えにくくなってしまい利便性が低下するが、認証システムSによれば、2段階認証を採用したとしてもパスコードの長さは変わらないので、このような利便性の低下を防止できる。また例えばメールアドレスや電話番号等の追加認証情報を入力させる場合には、入力が煩雑になり利便性が低下するが、認証システムSによれば、2次元コード認証を成功させたユーザが同じエリアにいない限りは追加認証情報を入力させる必要がないので、このような利便性の低下を防止できる。

[0140] また、認証システムSは、認証対象ユーザがいる場所が関連付けられていないユーザの登録認証情報を、比較対象とはしないことによって、2段階認証が成功することを制限することによって、2段階認証時の比較対象となる登録認証情報を減らすことができる。このため、認証を高速化し、サーバ1 0の処理負荷を軽減することができる。

[0141] また、認証システムSは、2段階認証が失敗した場合に、2次元コード認証に基づいて、認証対象ユーザの認証を行い、2次元コード認証が成功した場合に、認証された認証対象ユーザと、当該認証対象ユーザがいる場所と、を関連付けて記録することによって、セキュリティを高めることができる。

[0142] また、認証システムSは、2段階認証で、認証対象ユーザが他のユーザと

して認証される可能性があると判定された場合に、認証対象ユーザに対し、2次元コード認証又は電話番号認証を要求することによって、セキュリティを高めることができる。

[0143] また、認証システムSは、2次元コード認証で認証されたユーザがいる場所として、当該ユーザがいるエリアを場所データベースDB2に記録することによって、あるエリア内のセキュリティゲートSGで2次元コードをすれば、そのエリア内の他のセキュリティゲートSGで2段階認証が可能になるので、ユーザの利便性を向上させることができる。

[0144] また、認証システムSは、2段階認証が失敗した場合に、電話番号認証に基づいて、認証対象ユーザの認証を行うので、セキュリティを効果的に高めることができる。また、電話番号認証が成功したとしても、認証された認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられないことによって（即ち、電話番号認証が成功しても2段階認証を許可しないことによって）、2段階認証を許可するために、より精度の高い2次元コード認証を要求し、セキュリティを効果的に高めることができる。

[0145] また、認証システムSは、2次元コード認証又は2段階認証の何れかの選択を受け付けることによって、ユーザに好きな認証方法を選択させ、利便性を高めることができる。

[0146] また、認証システムSは、認証情報の類似に基づく認証方法と、認証情報の一致に基づく認証方法と、を含む2段階認証によって、セキュリティを効果的に高めることができる。

[0147] また、認証システムSは、2次元コード認証及び2段階認証の各々に対応した複数の認証装置30を利用して認証することによって、認証装置30を利用した認証におけるセキュリティを高めることができる。

[0148] また、認証システムSは、ユーザ端末20を利用した認証と、生体認証と、によって、セキュリティを効果的に高めることができる。

[0149] [5. 変形例]

なお、本発明の態様は、以上に説明した実施の形態に限定されるものでは

ない。本発明の態様の趣旨を逸脱しない範囲で、適宜変更可能である。

[0150] 例えば、実施形態では、ユーザがセキュリティゲート S G を通過する場面
を例に挙げたが、認証システム S は、ユーザが商品を購入したりサービスを利用したりする場面にも適用可能である。この場合、例えば、認証装置 30 は、自動販売機、券売機、POS 端末、又は店舗における支払端末である。ユーザは、認証装置 30 の撮影部 36 に顔を向けて操作部 34 からパスコードを入力し、顔認証とパスコード認証が成功すると、決済処理が実行され、商品を購入したり、サービスを利用したりすることができる。

[0151] 処理実行部 108 は、2次元コード認証又は2段階認証が成功した場合に、
認証されたユーザの決済情報に基づいて、決済処理を実行する。決済処理の際に参照される決済情報は、認証が成功したユーザに関連付けられた決済情報である。

[0152] 決済情報は、決済をするために必要な情報であり、例えば、クレジットカード情報、電子バリュー（例えば、電子マネー又はポイント）のアカウント情報、仮想通貨のアカウント情報、銀行口座情報、又はデビットカード情報などである。決済情報は、ユーザ登録時などに登録され、例えば、ユーザデータベース DB1 に、ユーザ ID に関連付けて決済情報が格納されているものとする。なお、決済情報は、ユーザデータベース DB1 とは異なるデータベースに格納されていてもよい。

[0153] 処理実行部 108 は、決済情報に応じた決済処理を実行すればよく、例えば、クレジットカード情報に基づく与信処理、電子バリューの残高を減少させる処理、仮想通貨の残高を減少させる処理、銀行口座から引き落としや振り込みをする処理、又はデビットカード情報が示す口座の残高を減少させる処理などを実行する。処理実行部 108 は、認証が失敗した場合には決済処理を実行せず、認証が成功した場合に決済処理を実行する。

[0154] 決済処理が実行された場合、認証装置 30 の表示部 35 又は店舗の端末などに、その旨が表示され、ユーザは商品を受け取ったり、サービスを利用したりする。例えば、認証装置 30 が店舗などに設置されたデジタルサイネー

ジ装置である場合、サーバ10から認証成功通知を受信すると、認証が成功したことを示すメッセージが表示部35に表示される。店舗のスタッフは、当該メッセージを確認すると、ユーザに商品を渡したりサービスを提供したりする。なお、メッセージは、認証装置30ではなく、店舗のスタッフが操作する端末などの他のコンピュータに転送されて表示されてもよい。また例えば、認証装置30が自動販売機であれば、サーバ10から認証成功通知を受信すると、認証装置30は、ユーザが指定した商品を排出したり、コーヒーやインスタント食品などの商品を調理したりする。

[0155] 上記変形例によれば、顔が類似する他のユーザが成りすまして決済し、不正に商品を購入したりサービスを利用したりすることを防止し、商品の購入時やサービスの利用時におけるセキュリティを十分に高めることができる。また、ユーザからしてみれば手ぶらで店舗に行ったとしても、セキュリティを担保した決済が可能になるので、ユーザビリティを向上させることができる。店舗からしてみても、クレジットカードの読取装置などの専用の装置を用意しなくても決済が可能となるので、店舗の利便性を向上させることもできる。

[0156] また例えば、認証装置30の撮影部36で撮影された画像に基づいて、生体認証が実行される場合を説明したが、赤外線センサ又は超音波センサなどといった他のセンサを利用して生体認証が実行されてもよい。認証システムSは、利用する生体認証に応じたセンサを含めばよい。また例えば、2段階認証で誤認証の可能性がある場合に、追加認証が行われる場合を説明したが、追加認証は行われなくてもよい。追加認証の代わりに、2次元コード認証が要求されるようにしてもよい。

[0157] また例えば、認証装置30に対して認証情報が入力される場合を説明したが、ユーザ端末20又は他のコンピュータに対して認証情報が入力されてもよい。例えば、ユーザがユーザ端末20を操作して2次元コード認証を成功させた場合に、ユーザと、ユーザ端末20の場所と、が関連付けられてユーザデータベースDB1に格納されてもよい。この場合、ユーザ端末20の場

所は、GPS情報や無線基地局情報等の任意の測位方法を利用して取得されるようにすればよい。

[0158] また例えば、主な機能がサーバ10で実現される場合を説明したが、各機能は、複数のコンピュータで分担されてもよい。例えば、サーバ10、ユーザ端末20、及び認証装置30の各々で機能が分担されてもよい。例えば、認証処理がサーバ10で実行されるのではなく、ユーザ端末20又は認証装置30で実行されてもよい。また例えば、認証システムSが複数のサーバコンピュータを含む場合には、これら複数のサーバコンピュータで機能が分担されてもよい。また例えば、データ記憶部100で記憶されるものとして説明したデータは、サーバ10以外のコンピュータによって記憶されてもよい。

請求の範囲

- [請求項1] 第1の認証方法に基づいて、認証をする第1認証手段と、
前記第1の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する記録手段と、
第2の認証方法に基づいて、認証をする第2認証手段と、
前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限手段と、
を含む認証システム。
- [請求項2] 前記第2の認証方法の認証では、入力認証情報と登録認証情報とが比較され、
前記制限手段は、
前記認証対象ユーザがいる場所が関連付けられたユーザの前記登録認証情報を、前記認証対象ユーザの入力認証情報との比較対象として取得し、
前記認証対象ユーザがいる場所が関連付けられていないユーザの前記登録認証情報を、前記比較対象とはしないことによって、前記第2の認証方法の認証が成功することを制限し、
前記第2認証手段は、前記認証対象ユーザの前記入力認証情報と、前記比較対象として取得された登録認証情報と、に基づいて認証を行う、
請求項1に記載の認証システム。
- [請求項3] 前記第1認証手段は、前記第2の認証方法の認証が失敗した場合に、前記第1の認証方法に基づいて、前記認証対象ユーザの認証を行い、
前記記録手段は、前記第1の認証方法の認証が成功した場合に、認証された前記認証対象ユーザと、当該認証対象ユーザがいる場所と、

を関連付けて前記記憶手段に記録する、

請求項 1 又は 2 に記載の認証システム。

[請求項4]

前記認証システムは、

前記認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられている場合に、前記第 2 の認証方法の認証で、前記認証対象ユーザが他のユーザとして認証される可能性があるか否かを判定する判定手段と、

前記可能性があるとは判定された場合に、前記認証対象ユーザに対し、前記第 1 の認証方法又は第 3 の認証方法の認証を要求する要求手段と、

を含む請求項 1 ～ 3 の何れかに記載の認証システム。

[請求項5]

前記記録手段は、前記第 1 の認証方法で認証されたユーザがいる場所として、当該ユーザがいるエリアを前記記憶手段に記録し、

前記制限手段は、前記認証対象ユーザと、当該認証対象ユーザがいるエリアと、が前記記憶手段に関連付けられていない場合に、前記第 2 の認証方法の認証が成功することを制限する、

請求項 1 ～ 4 の何れかに記載の認証システム。

[請求項6]

前記認証システムは、前記第 2 の認証方法の認証が失敗した場合に、第 3 の認証方法に基づいて、前記認証対象ユーザの認証をする第 3 認証手段を更に含み、

前記記憶手段には、前記第 3 の認証方法の認証が成功したとしても、認証された前記認証対象ユーザと、当該認証対象ユーザがいる場所と、が関連付けられない、

請求項 1 ～ 5 の何れかに記載の認証システム。

[請求項7]

前記認証システムは、前記第 1 の認証方法又は前記第 2 の認証方法の何れかの選択を受け付ける受付手段を更に含み、

前記第 1 認証手段は、前記第 1 の認証方法が選択された場合に、前記第 1 の認証方法の認証を行い、

前記第2認証手段は、前記第2の認証方法が選択された場合に、前記第2の認証方法の認証を行う、

請求項1～6の何れかに記載の認証システム。

[請求項8] 前記第2の認証方法は、認証情報の類似に基づく認証方法と、認証情報の一致に基づく認証方法と、を含む、

請求項1～7の何れかに記載の認証システム。

[請求項9] 前記認証システムは、前記第1の認証方法及び前記第2の認証方法の各々に対応した複数の認証装置を含み、

前記記録手段は、前記第1の認証方法で認証されたユーザと、当該ユーザの認証で用いられた前記認証装置の場所と、を関連付けて前記記憶手段に記録し、

前記制限手段は、前記認証対象ユーザと、当該認証対象ユーザの認証で用いられる前記認証装置の場所と、が関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する、

請求項1～8の何れかに記載の認証システム。

[請求項10] 前記第1の認証方法の認証は、ユーザ端末を利用した認証であり、前記第2の認証方法の認証は、生体認証である、

請求項1～9の何れかに記載の認証システム。

[請求項11] 前記認証システムは、前記第1の認証方法の認証又は前記第2の認証方法の認証が成功した場合に、認証されたユーザの決済情報に基づいて、決済処理を実行する処理実行手段を更に含む、

請求項1～10の何れかに記載の認証システム。

[請求項12] 請求項1～11の何れかに記載の認証システムに含まれる認証装置又は当該認証システムと通信可能な認証装置であって、

前記認証に必要な情報を送信する送信手段と、

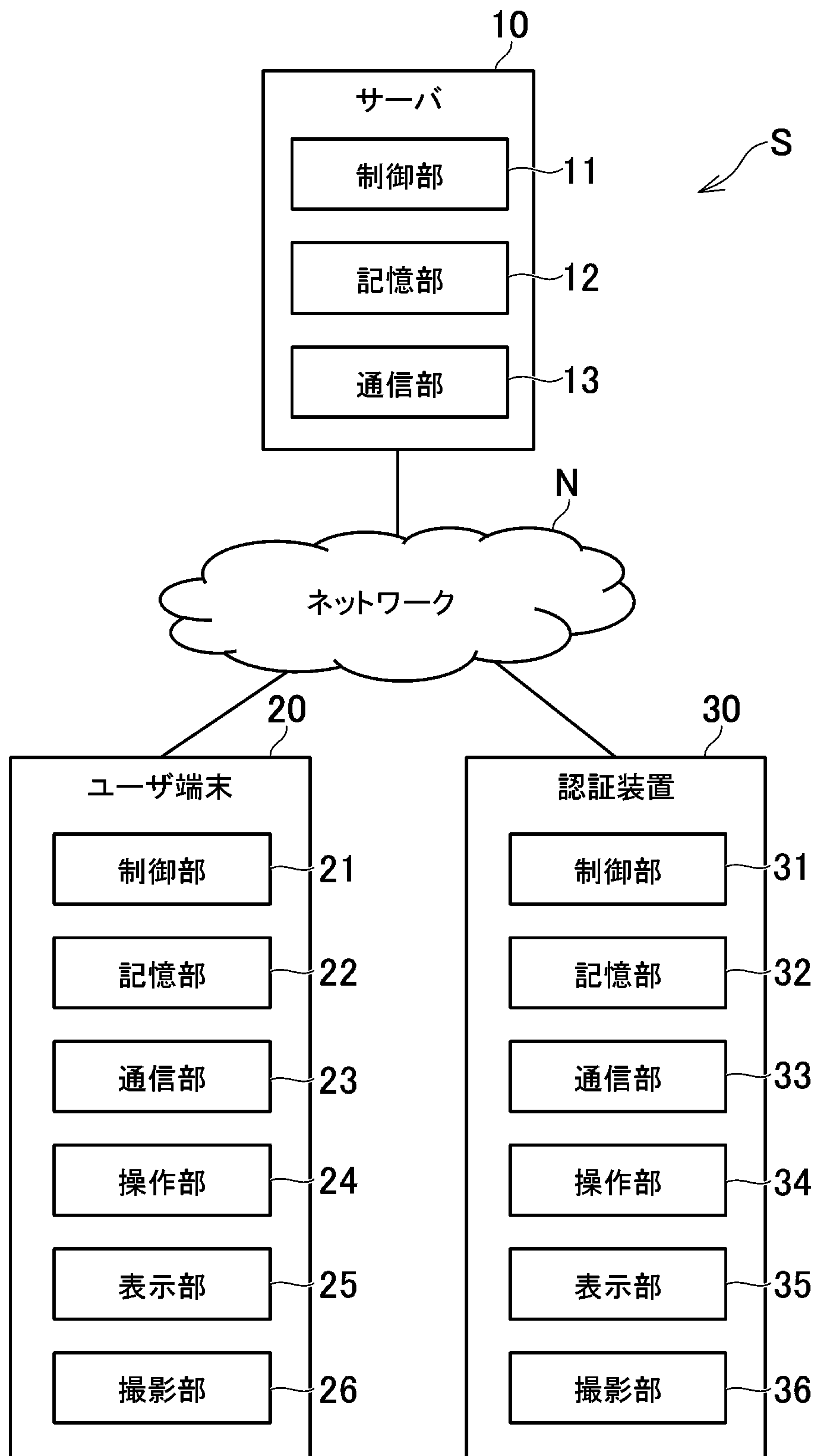
前記認証が成功した場合に、所定の処理を実行する処理実行手段と

、

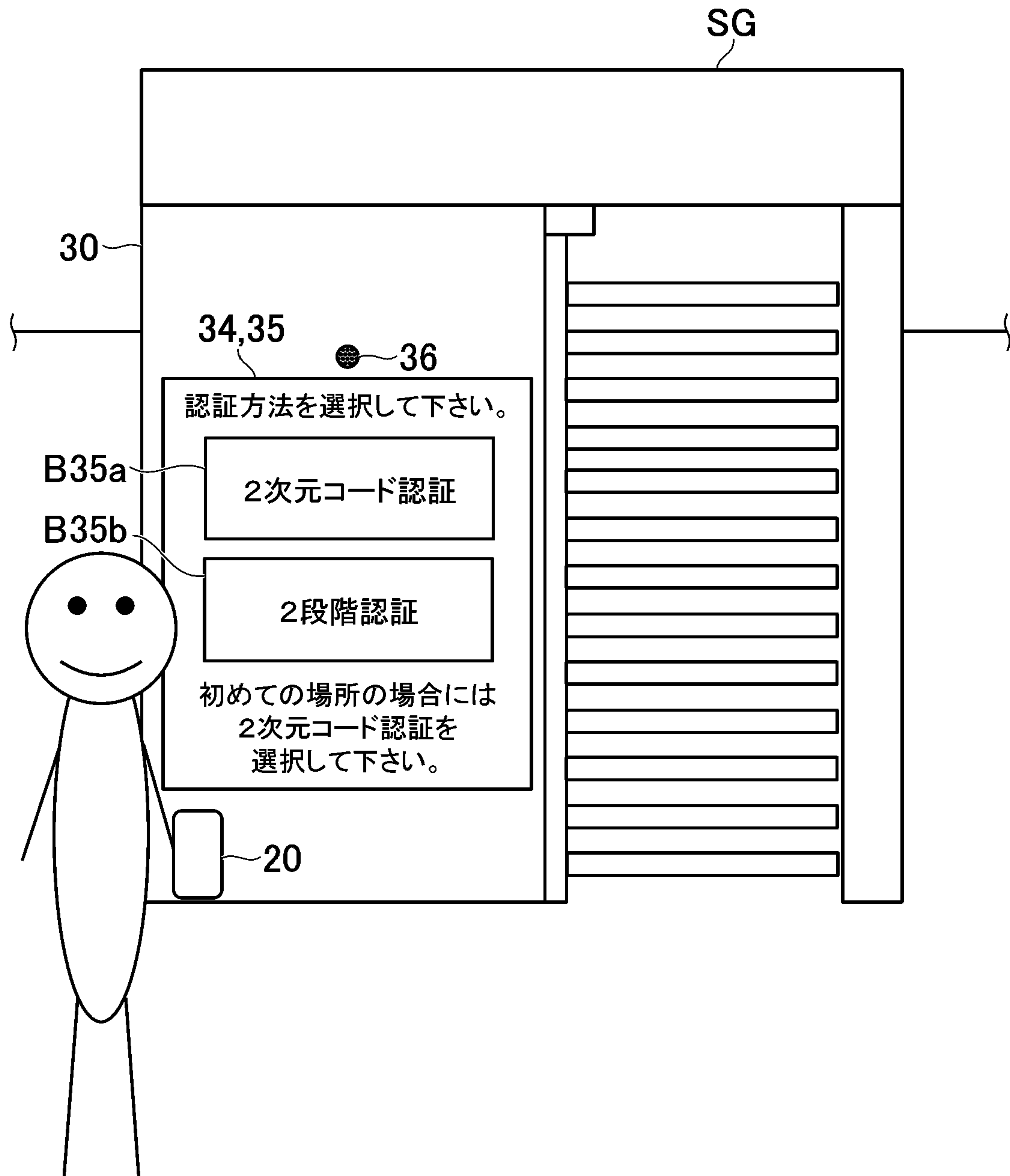
を含む認証装置。

- [請求項13] 第1の認証方法に基づいて、認証をする第1認証ステップと、
前記第1の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する記録ステップと、
第2の認証方法に基づいて、認証をする第2認証ステップと、
前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限ステップと、
を含む認証方法。
- [請求項14] 第1の認証方法に基づいて、認証をする第1認証手段、
前記第1の認証方法の認証が成功した場合に、認証されたユーザと、当該ユーザがいる場所と、を関連付けて記憶手段に記録する記録手段、
第2の認証方法に基づいて、認証をする第2認証手段、
前記第2の認証方法における認証対象ユーザと、当該認証対象ユーザがいる場所と、が前記記憶手段に関連付けられていない場合に、前記第2の認証方法の認証が成功することを制限する制限手段、
としてコンピュータを機能させるためのプログラム。

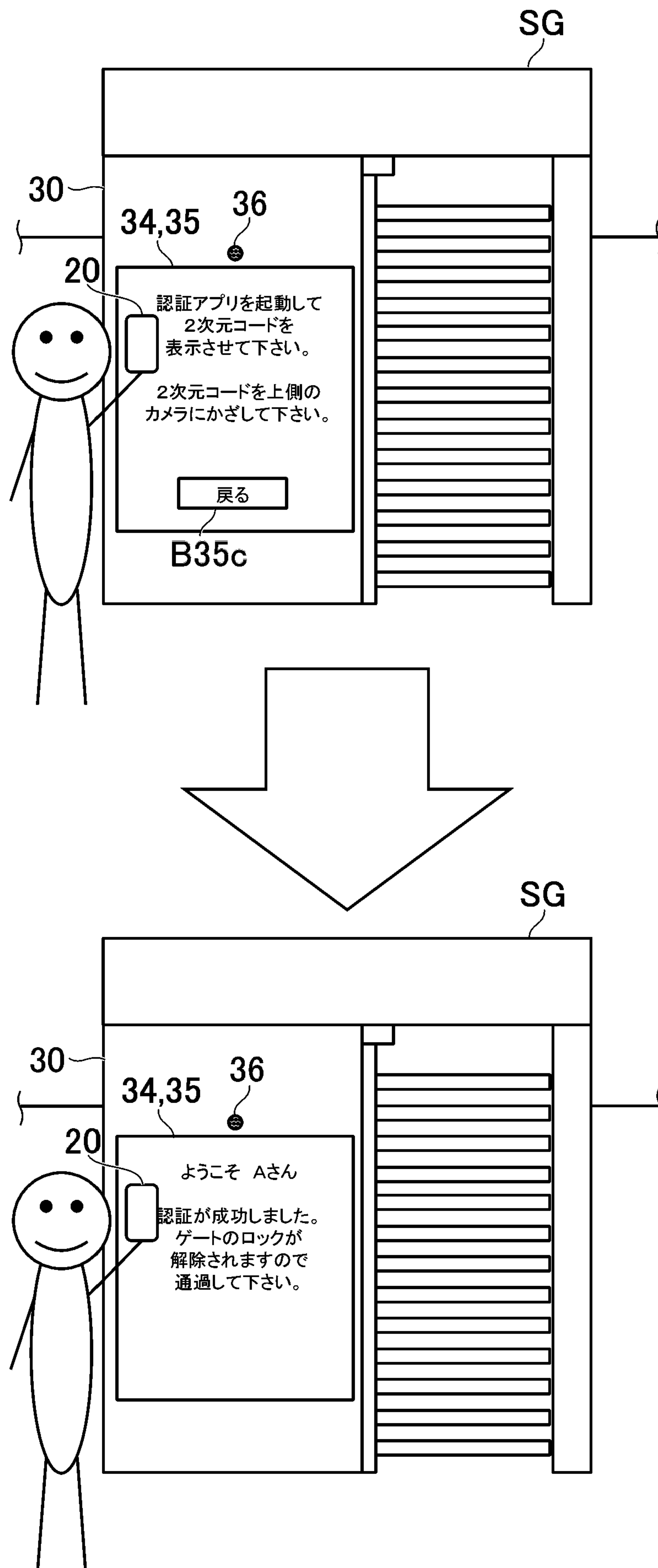
[図1]



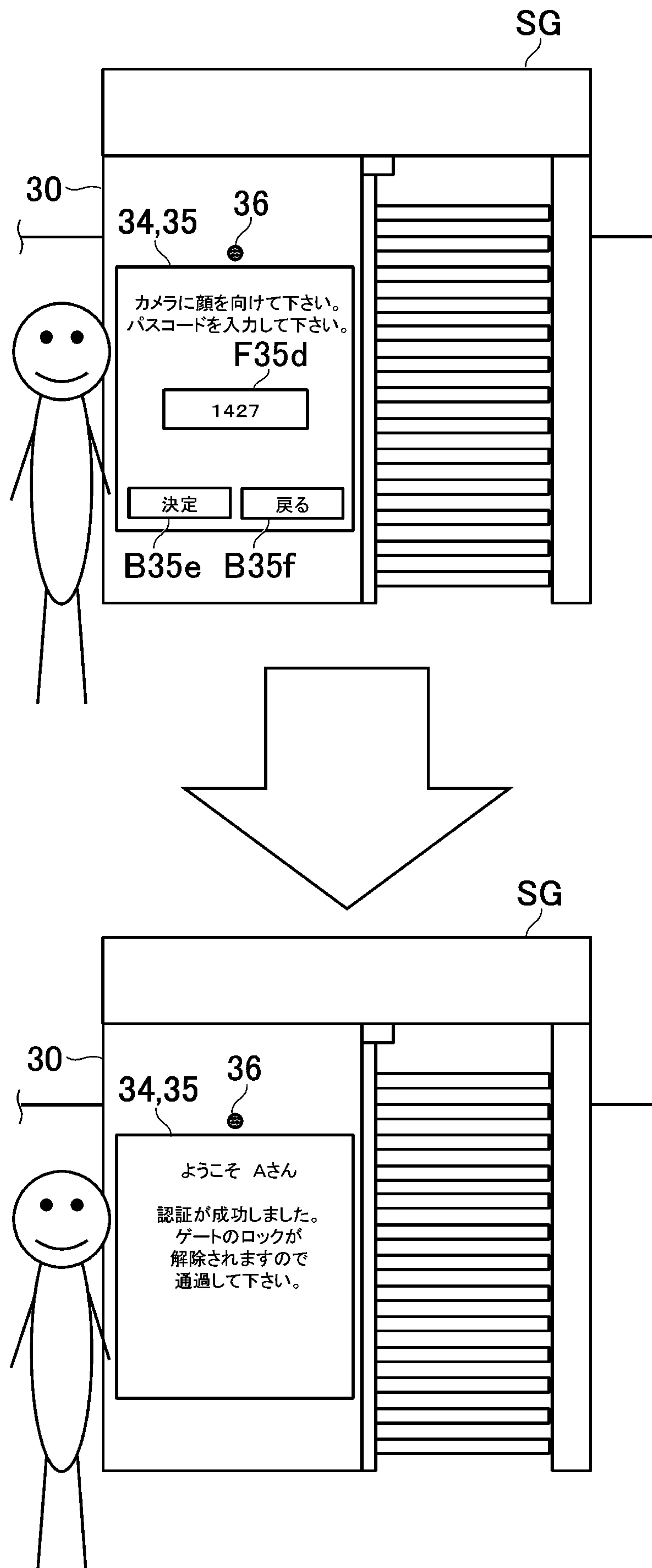
[図2]



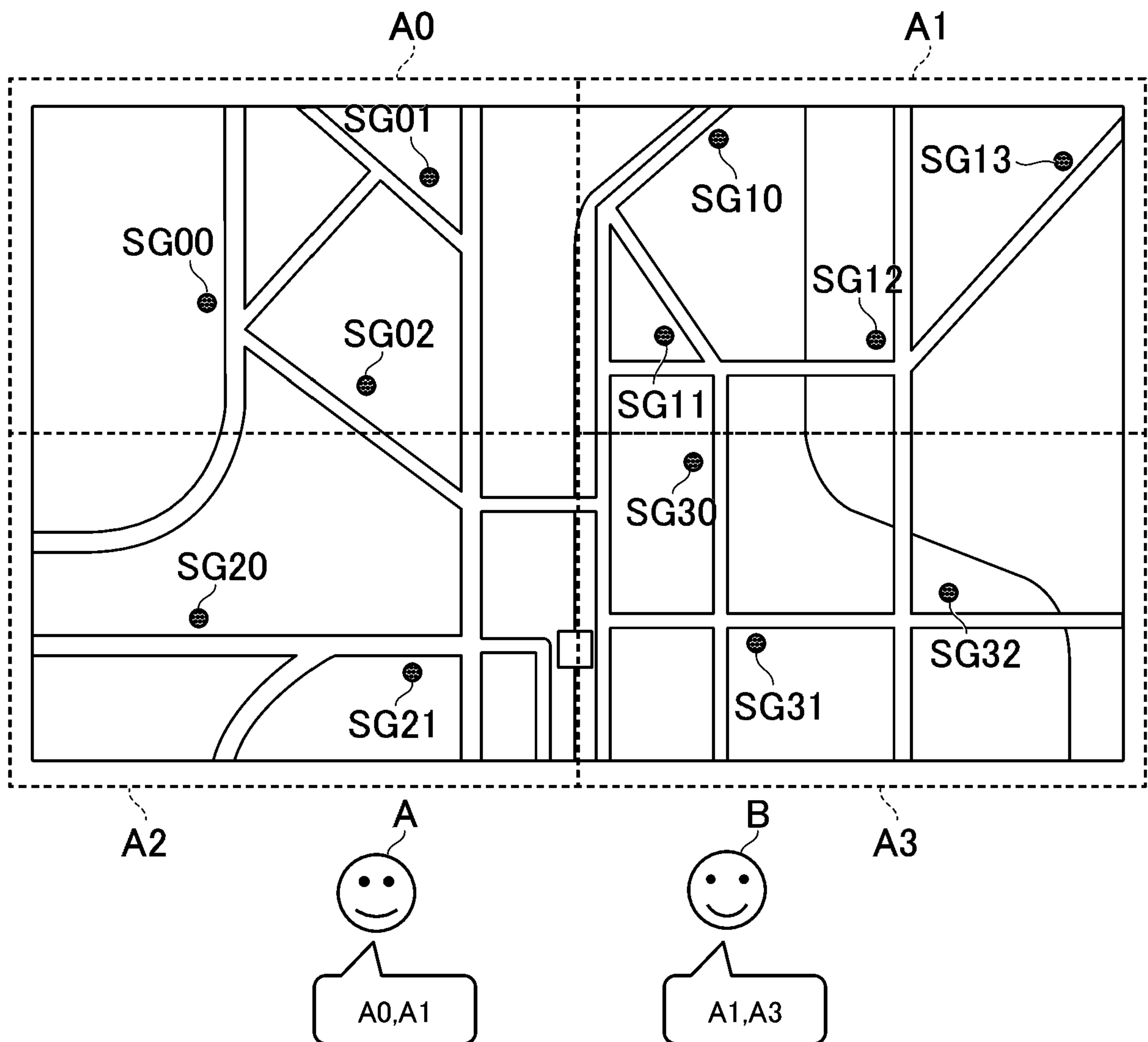
[図3]



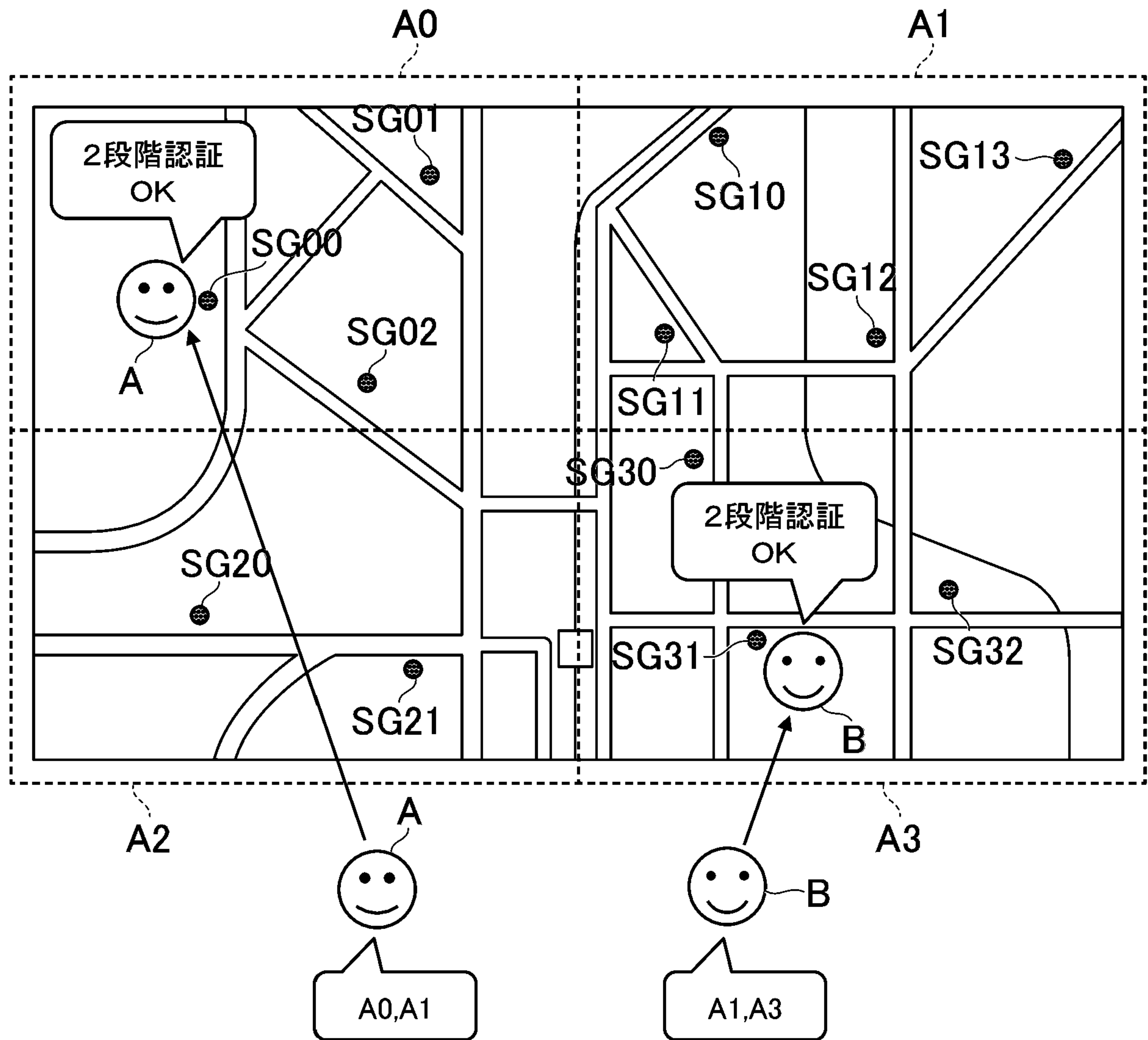
[図4]



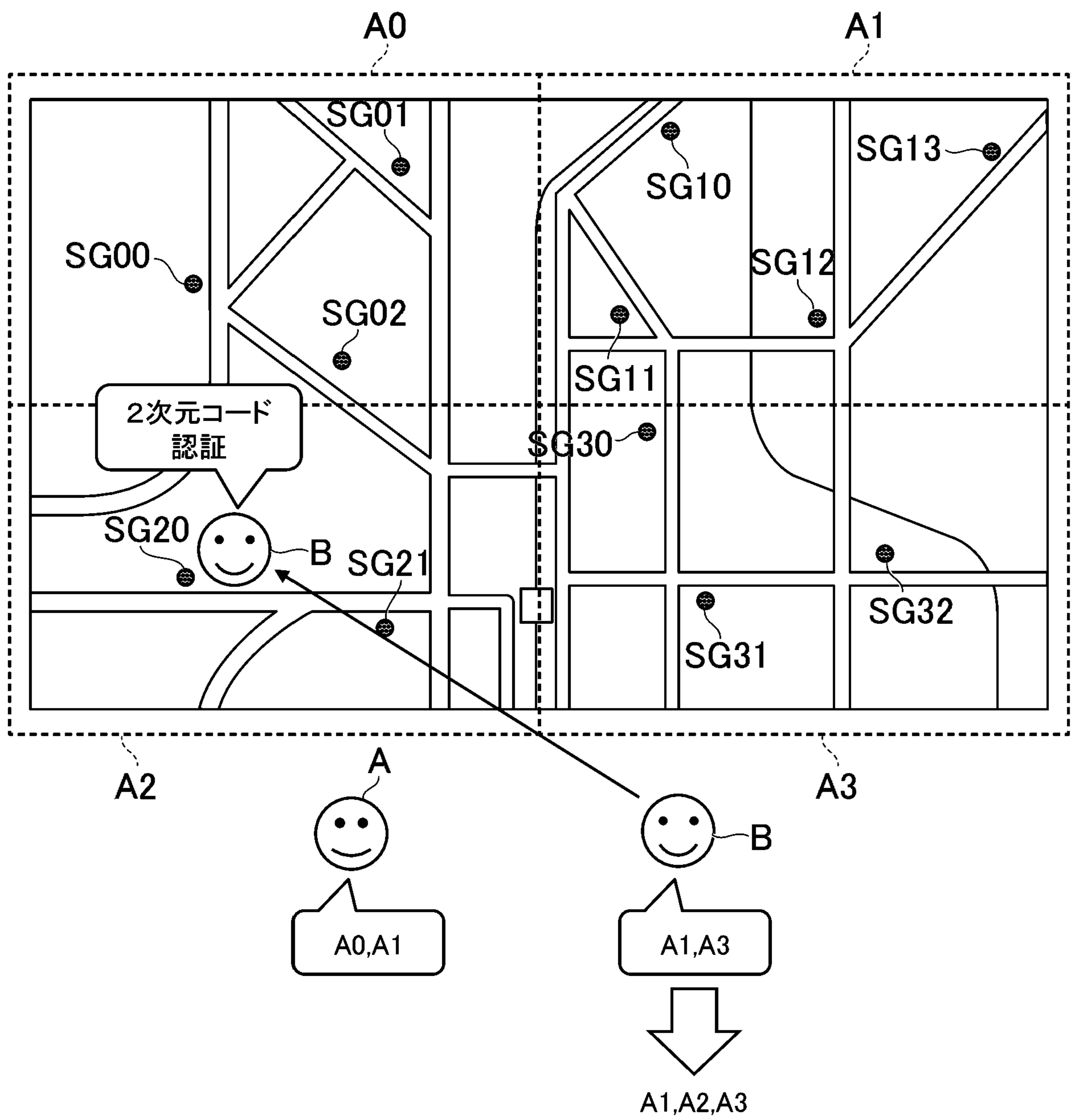
[図5]



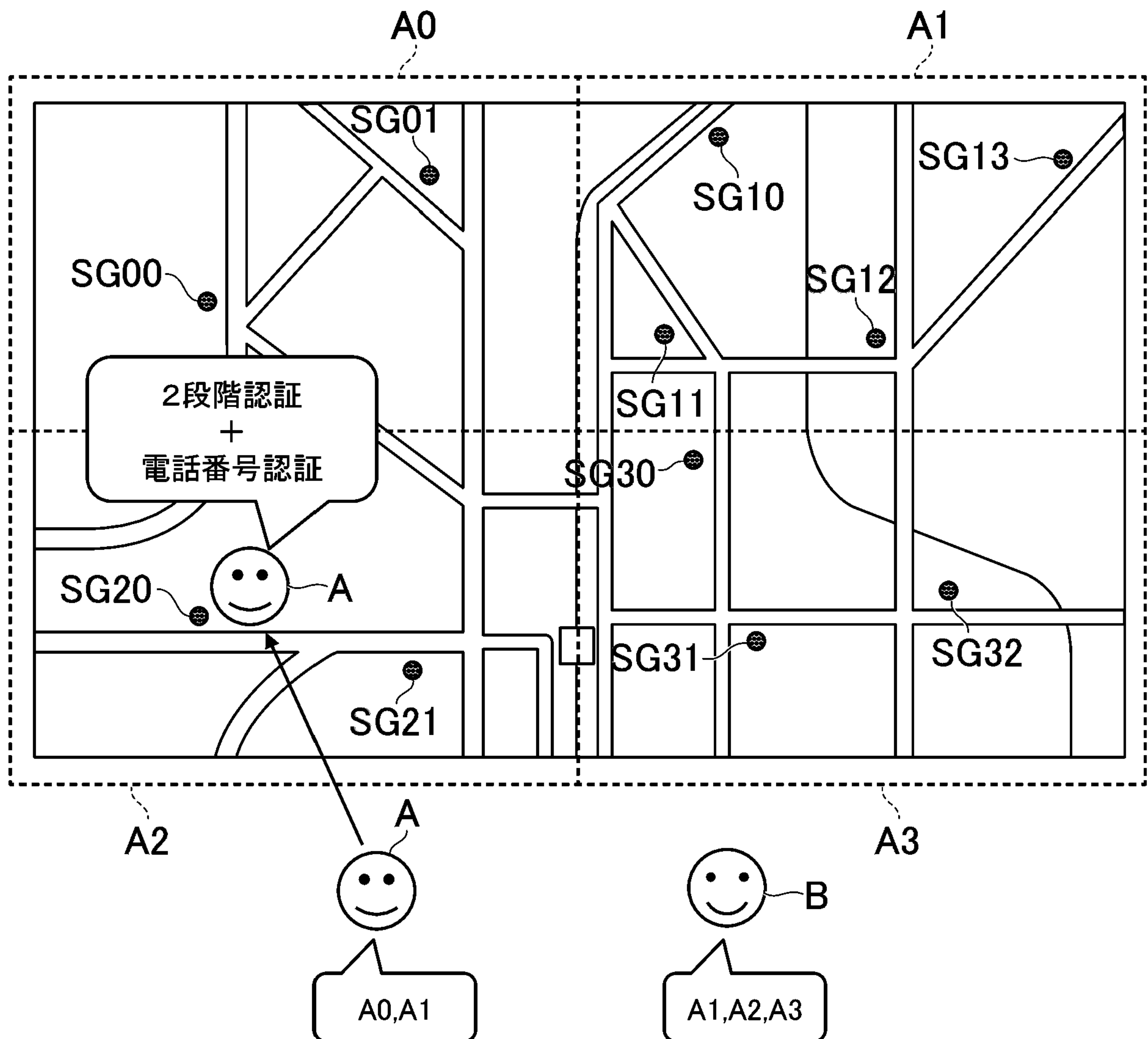
[図6]



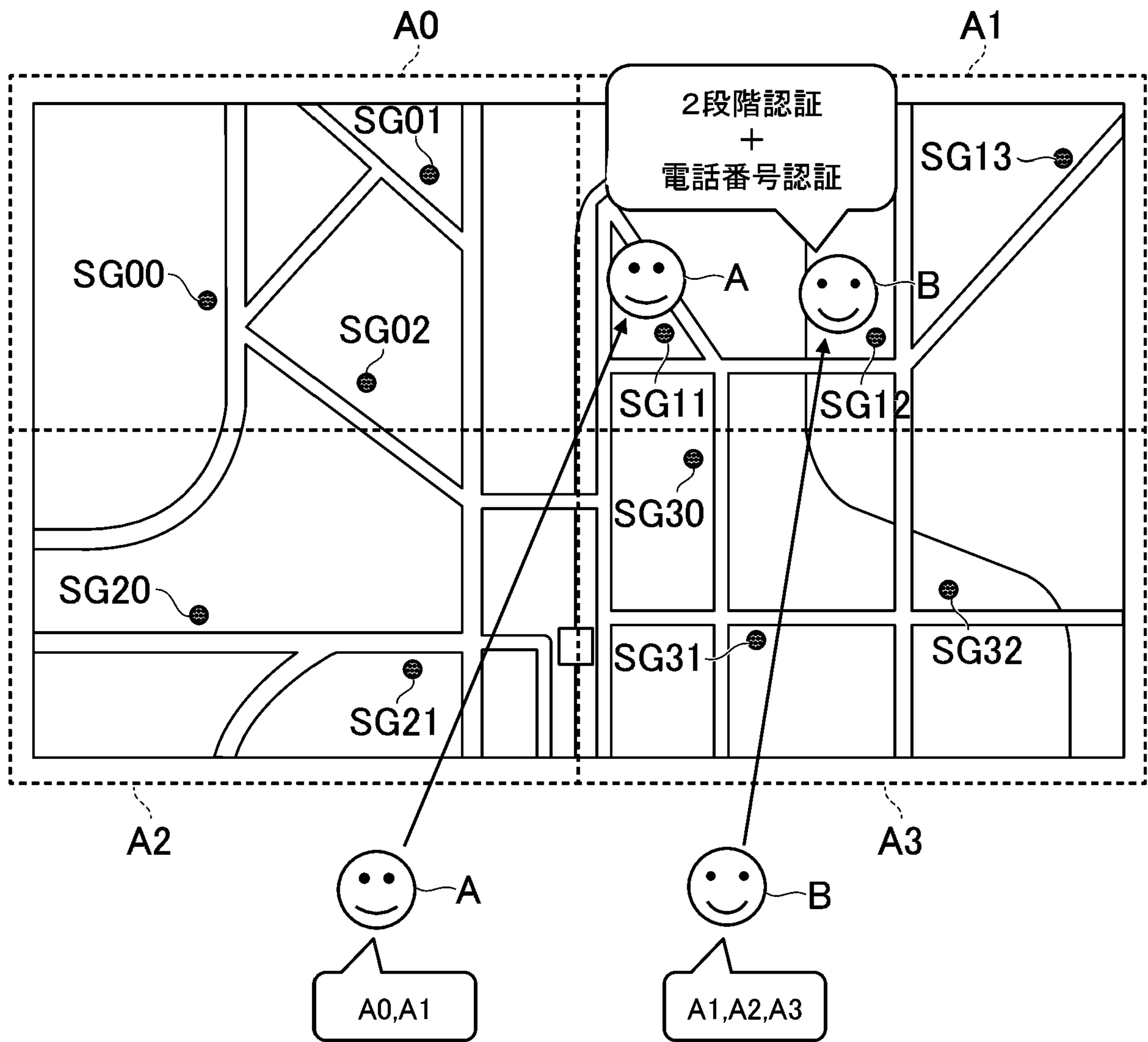
[図7]



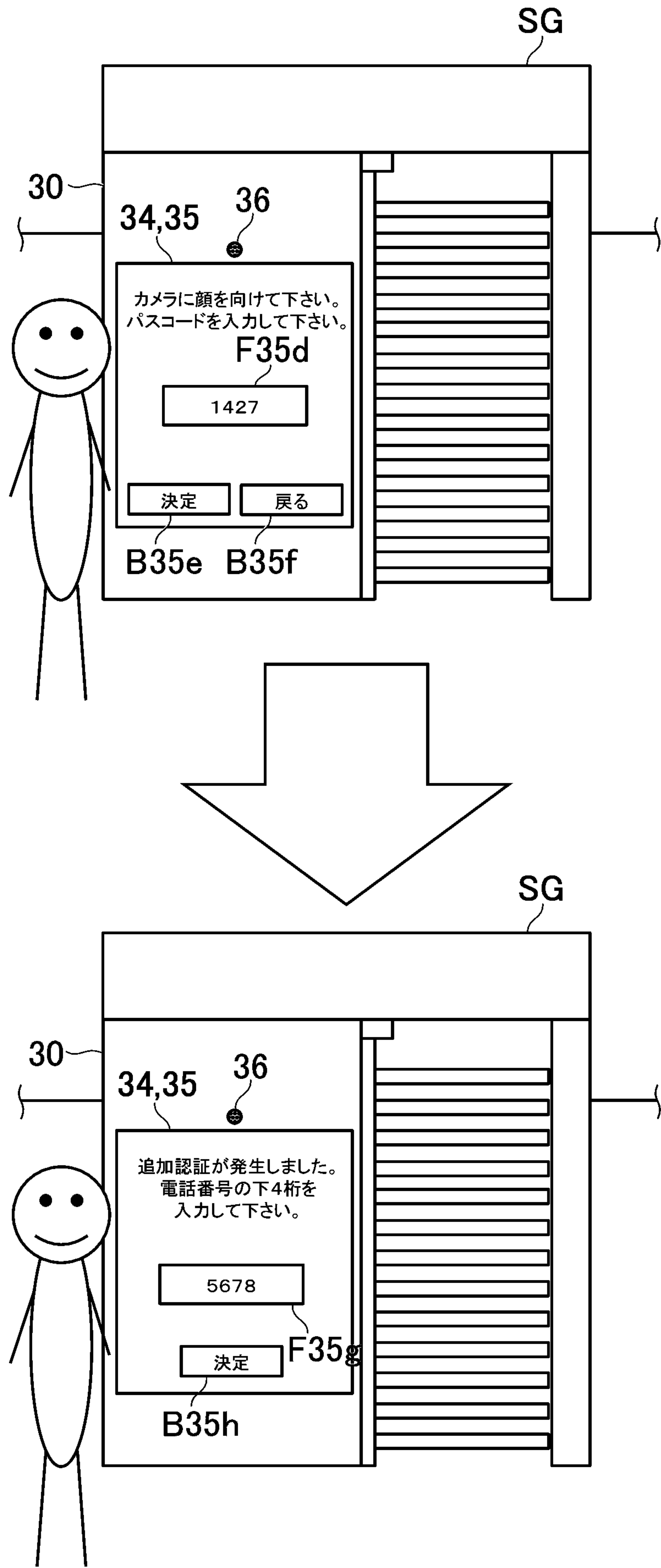
[図8]



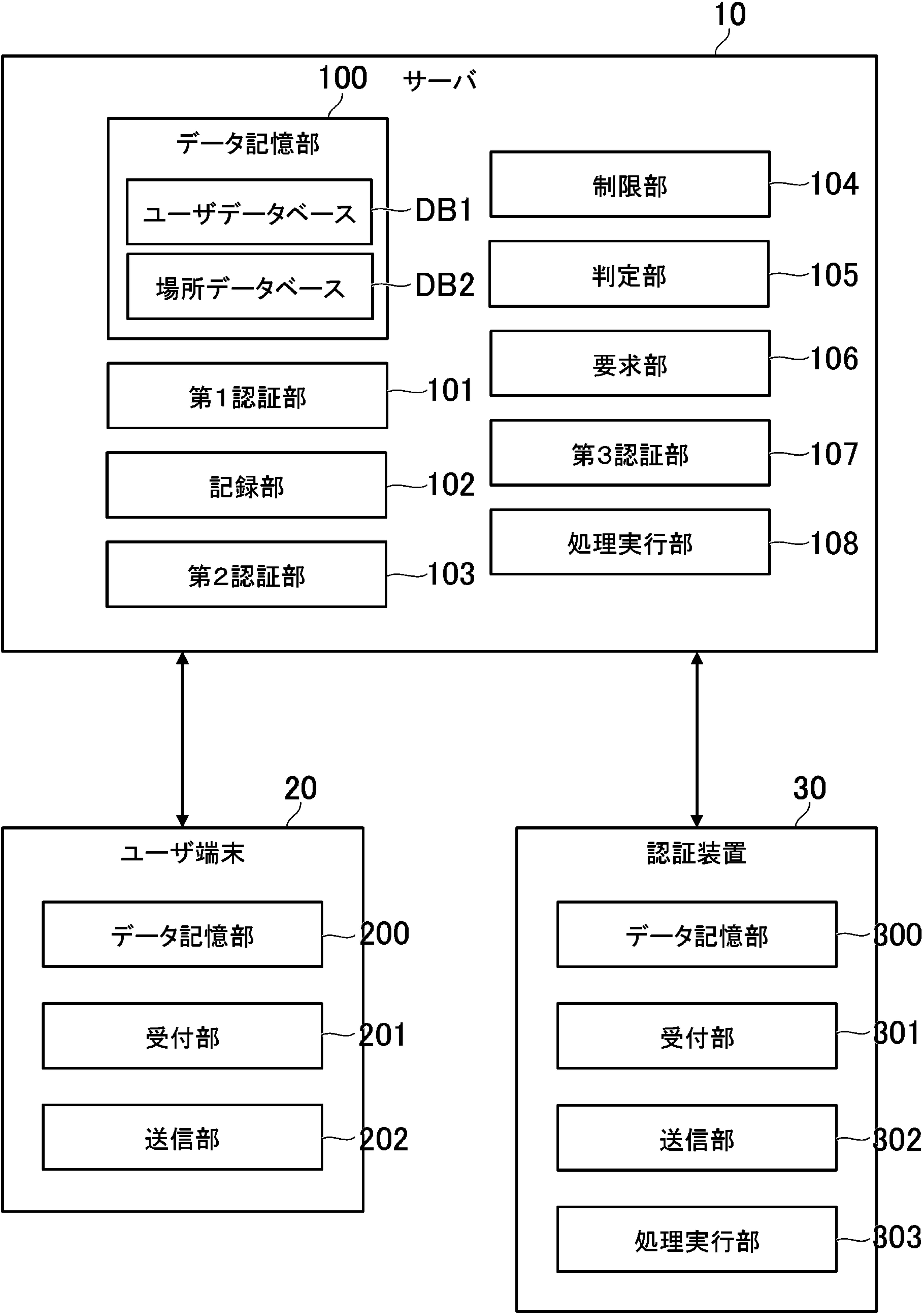
[図9]



[図10]



[図11]



[図12]

DB1

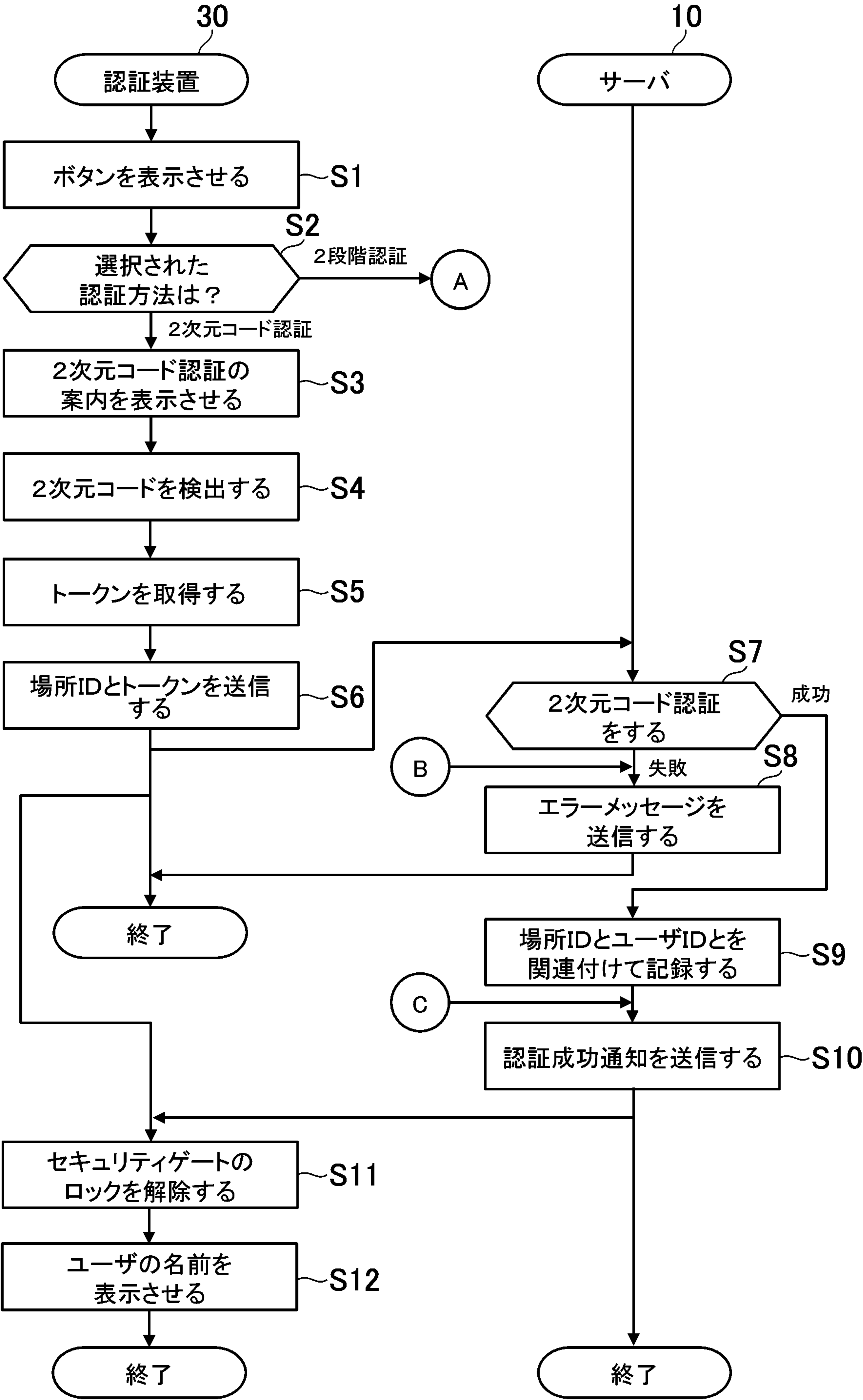
ユーザID	氏名	パスワード	顔写真	顔の特徴量	パスコード	登録日時	電話番号	メールアドレス	トークン
u00001	A	*****	aaa.jpg	(a1,a2,a3,...)	1427	2019/6/20 16:43:51	090-1234-5678	aaa123@mailadd.com	xb23ac
u00002	B	*****	bbb.jpg	(b1,b2,b3,...)	1427	2019/3/12 11:20:05	080-1876-5234	987bbb@abcmail.jp	jab15z
u00003	C	*****	ccc.jpg	(c1,c2,c3,...)	9128	2019/6/5 21:15:41	03-9999-1111	ccc555ccc@xyzfirm.com	1ca7dk
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

[図13]

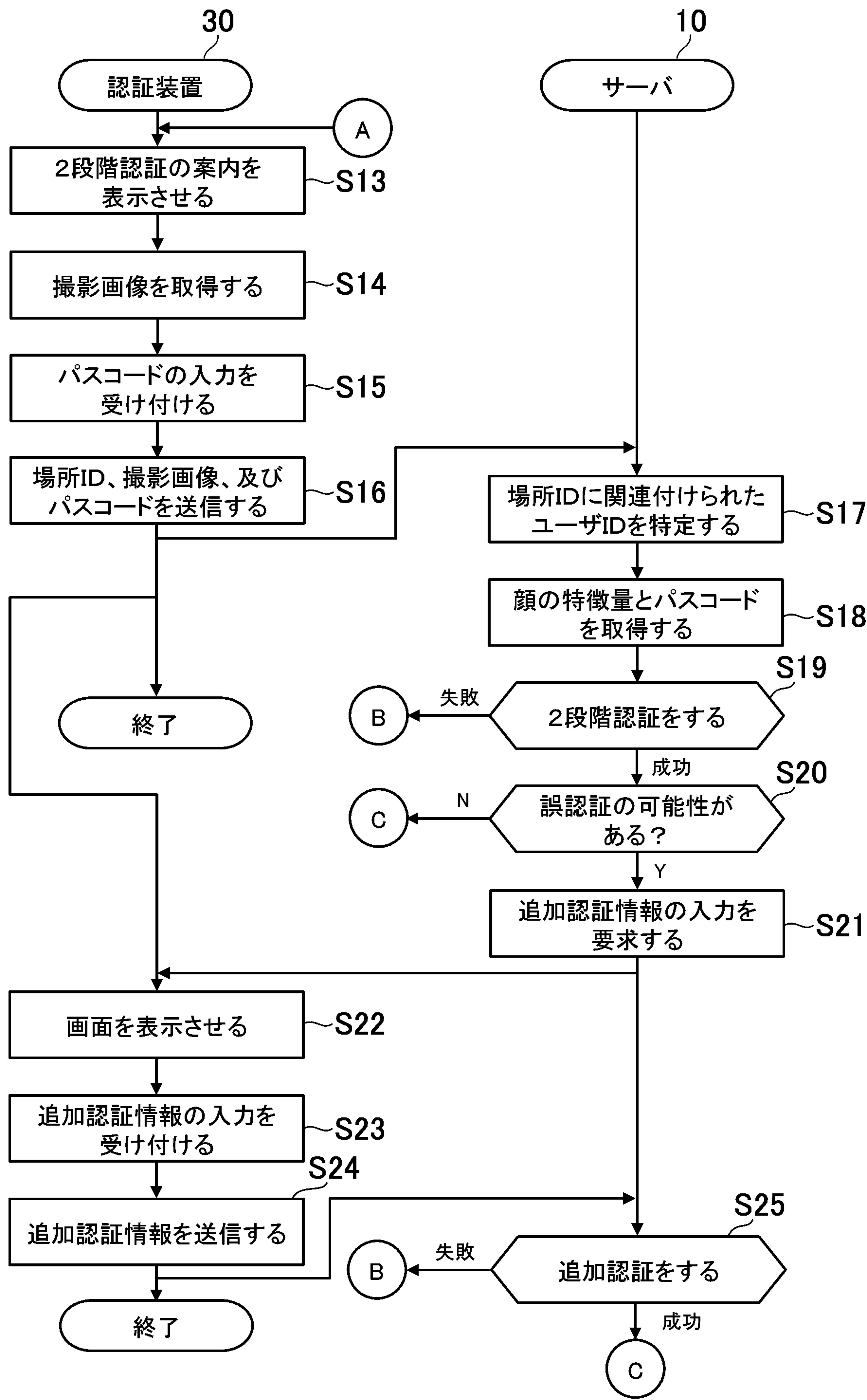
DB2

場所ID	エリア名	ユーザID
p00000	A0	u00001
		u00003
		u00012
		・ ・ ・
p00001	A1	u00001
		u00002
		u00005
		・ ・ ・
p00002	A2	u00005
		u00017
		u00022
		・ ・ ・
・ ・ ・	・ ・ ・	・ ・ ・

[図14]



[図15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/051569

A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. G06F21/31 (2013.01) i FI: G06F21/31 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int. Cl. G06F21/31 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2020 Registered utility model specifications of Japan 1996-2020 Published registered utility model applications of Japan 1994-2020 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2019-168915 A (SEGA GAMES CO., LTD.) 03 October 2019, paragraphs [0004], [0007], [0018]-[0103], [0129], [0130], [0158], [0162], fig. 1, 5, paragraphs [0004], [0007], [0018]-[0103], [0129], [0130], [0158], [0162], fig. 1, 5, paragraphs [0004], [0007], [0018]-[0103], [0129], [0130], [0158], [0162], fig. 1, 5	1-2, 4-6, 8-10, 12-14 7-12 3
Y	JP 2011-54120 A (KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.) 17 March 2011, paragraph [0097]	7-12
Y	JP 2016-157294 A (HITACHI SOLUTIONS, LTD.) 01 September 2016, abstract	11-12
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 30.01.2020		Date of mailing of the international search report 10.02.2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2019/051569

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 2019-168915 A	03.10.2019	(Family: none)	
JP 2011-54120 A	17.03.2011	(Family: none)	
JP 2016-157294 A	01.09.2016	(Family: none)	

国際調査報告		国際出願番号 PCT/JP2019/051569
A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/31(2013.01)i FI: G06F21/31		
B. 調査を行った分野		
調査を行った最小限資料（国際特許分類（IPC）） G06F21/31		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922 - 1996年 日本国公開実用新案公報 1971 - 2020年 日本国実用新案登録公報 1996 - 2020年 日本国登録実用新案公報 1994 - 2020年		
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2019-168915 A（株式会社セガゲームス）03.10.2019（2019 - 10 - 03） 段落[0004], [0007], [0018]-[0103], [0129]-[0130], [0158], [0162], 図1, 5	1-2, 4-6, 8-10, 12-14
Y	段落[0004], [0007], [0018]-[0103], [0129]-[0130], [0158], [0162], 図1, 5	7-12
A	段落[0004], [0007], [0018]-[0103], [0129]-[0130], [0158], [0162], 図1, 5	3
Y	JP 2011-54120 A（コニカミノルタビジネステクノロジーズ株式会社）17.03.2011 （2011 - 03 - 17） 段落[0097]	7-12
Y	JP 2016-157294 A（株式会社日立ソリューションズ）01.09.2016（2016 - 09 - 01） 要約	11-12
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献		
国際調査を完了した日 30.01.2020		国際調査報告の発送日 10.02.2020
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 上島 拓也 5S 6293 電話番号 03-3581-1101 内線 3546

PCT/JP2019/051569

引用文献			公表日	パテントファミリー文献	公表日
JP	2019-168915	A	03.10.2019	(ファミリーなし)	
JP	2011-54120	A	17.03.2011	(ファミリーなし)	
JP	2016-157294	A	01.09.2016	(ファミリーなし)	