

(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
2014 年 11 月 27 日(27.11.2014)



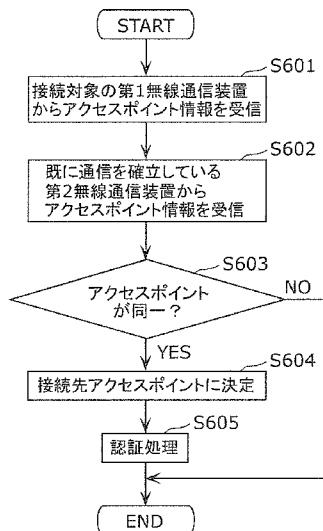
(10) 国際公開番号
WO 2014/188686 A1

- (51) 国際特許分類:
H04W 12/06 (2009.01) H04W 84/12 (2009.01)
H04W 48/20 (2009.01)
- (21) 国際出願番号: PCT/JP2014/002579
- (22) 国際出願日: 2014 年 5 月 16 日(16.05.2014)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2013-107711 2013 年 5 月 22 日(22.05.2013) JP
- (71) 出願人: パナソニック インテレクチュアル
プロパティ コーポレーション オブ アメリ
カ (PANASONIC INTELLECTUAL PROPERTY
CORPORATION OF AMERICA) [US/US]; 90503 カ
リフォルニア州、トーランス、スイート 20
0、マリナー アベニュー 20000 Cali
fornia (US).
- (72) 発明者: 大崎 勇士(OSAKI, Yuji). 中山 武司
(NAKAYAMA, Takeshi). 原田 昌明(HARADA,
Masaaki). 中務 国男(NAKATSUKASA, Kunio).
- (74) 代理人: 新居 広守, 外(NII, Hiromori et al.); 〒
5320011 大阪府大阪市淀川区西中島5丁目3番
10号タナカ・イートピア新大阪ビル6階新居
国際特許事務所内 Osaka (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, DK, DM, DO, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN,
IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR,
LS, LT, 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, 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, SZ, TZ, UG, ZM, ZW), ユーラシ

[続葉有]

(54) Title: WIRELESS CONNECTION AUTHENTICATION METHOD AND SERVER

(54) 発明の名称: 無線接続認証方法及びサーバ



- S601 Receive access point information from the first wireless communication apparatus to be connected
- S602 Receive access point information from the second wireless communication apparatus having already established the communication
- S603 Are the access points identical with each other?
- S604 Determine the identical access point as an access point with which the connection is to be established
- S605 Authenticate

(57) Abstract: A wireless connection authentication method comprises: a step (S601) of receiving first information (664) transmitted by a first access point (102 or 102A) in accordance with a message (611) transmitted from a first wireless communication apparatus (101); a step (S602) of receiving second information (665) transmitted by a second access point (102) in accordance with a message (613) transmitted from a second wireless communication apparatus (105) having already established a communication with the second access point (102); and a step (S604) of, if the first access point (102 or 102A) indicated in the first information (664) is identical with the second access point (102) indicated in the second information (665), then determining the identical access point as an access point to which the first wireless communication apparatus (101) is to be connected.

(57) 要約: 無線接続認証方法は、第1無線通信装置(101)から送信されたメッセージ(611)に従い第1アクセスポイント(102又は102A)が送信した、第1情報(664)を受信するステップ(S601)と、第2アクセスポイント(102)と既に通信が確立している第2無線通信装置(105)から送信されたメッセージ(613)に従い、第2アクセスポイント(102)が送信した第2情報(665)を受信するステップ(S602)と、第1情報(664)で示される第1アクセスポイント(102又は102A)と、第2情報(665)で示される第2アクセスポイント(102)とが同一のアクセスポイントである場合、当該同一のアクセスポイントを、第1無線通信装置(101)の接続先のアク

セスポイントに決定するステップ(S604)とを含む。

WO 2014/188686 A1



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:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称： 無線接続認証方法及びサーバ

技術分野

[0001] 本発明は、無線接続認証方法及びサーバに関する。

背景技術

[0002] 無線LANを使用する際には、無線通信装置に対してネットワーク識別子（ESSID）、周波数チャネル、暗号方式、暗号鍵、認証方式、及び認証鍵等の無線パラメータをユーザが設定する必要がある。これらの設定作業は煩雑なため、端末間で自動的に無線パラメータを設定する方法が存在する（例えば、特許文献1を参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開2009-253380号公報

発明の概要

発明が解決しようとする課題

[0004] このような無線接続認証方法では、ユーザがより簡単な操作で無線接続認証を行えることが望まれている。

[0005] そこで、本発明は、ユーザが簡単な操作で無線接続認証を行える無線接続認証方法を提供することを目的とする。

課題を解決するための手段

[0006] 本発明の一態様に係る無線接続認証方法は、第1無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバにおける無線接続認証方法であって、前記第1無線通信装置から送信された第1メッセージに従い第1無線アクセスポイントが送信した、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージを受信する第1受信ステップと、前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと既に通信が確立している第2無線通信装置から送信

された第3メッセージに従い、前記第2無線アクセスポイントが送信した、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信ステップと、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理ステップとを含む。

[0007] また、本発明の一態様に係る無線接続認証方法は、第1無線通信装置と無線アクセスポイントとの無線接続認証を行う無線接続認証方法であって、前記第1無線通信装置が、第1メッセージを第1無線アクセスポイントに送信する第1メッセージ送信ステップと、前記第1メッセージを受信した前記第1無線アクセスポイントが、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージをサーバに送信する第2メッセージ送信ステップと、前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと無線接続認証が既に完了している第2無線通信装置が、第3メッセージを前記第2無線アクセスポイントに送信する第3メッセージ送信ステップと、前記第3メッセージを受信した前記第2無線アクセスポイントが、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを前記サーバに送信する第4メッセージ送信ステップと、前記サーバが、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、前記接

続先アクセスポイントと前記第 1 無線通信装置とが無線接続認証を行う認証ステップとを含む。

[0008] なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能な CD-ROM などの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

発明の効果

[0009] 本発明は、ユーザが簡単な操作で無線接続認証を行える無線接続認証方法を提供できる。

図面の簡単な説明

[0010] [図1]図 1 は、実施の形態 1 における通信システムの構成例を示す図である。

[図2]図 2 は、実施の形態 1 における無線通信装置の構成例を示すブロック図である。

[図3]図 3 は、実施の形態 1 におけるアクセスポイントの構成例を示すブロック図である。

[図4]図 4 は、実施の形態 1 におけるサーバの構成例を示すブロック図である。

[図5]図 5 は、実施の形態 1 における既にアクセスポイントと通信を確立している無線通信装置の構成例を示すブロック図である。

[図6]図 6 は、実施の形態 1 におけるアカウント認証処理のシーケンス図である。

[図7]図 7 は、実施の形態 1 におけるアカウント認証処理のシーケンス図である。

[図8]図 8 は、実施の形態 1 におけるネットワーク接続要求のための操作例を説明するための図である。

[図9]図 9 は、実施の形態 1 における無線通信装置に格納される情報の一例を示す図である。

[図10]図 10 は、実施の形態 1 における接続要求メッセージの構成例を示す

図である。

[図11]図 1 1 は、実施の形態 1 における接続要求メッセージの構成例を示す図である。

[図12]図 1 2 は、実施の形態 1 における接続要求メッセージが送信される様子を示す図である。

[図13]図 1 3 は、実施の形態 1 におけるサーバに記憶される情報の一例を示す図である。

[図14]図 1 4 は、実施の形態 1 におけるネットワーク参加確認要求のための操作例を説明するための図である。

[図15]図 1 5 は、実施の形態 1 における参加確認メッセージの構成例を示す図である。

[図16]図 1 6 は、実施の形態 1 における認証コードの入力操作の一例を示す図である。

[図17]図 1 7 は、実施の形態 1 における認証コード情報メッセージの構成例を示す図である。

[図18]図 1 8 は、実施の形態 1 における P I N コード情報メッセージの構成例を示す図である。

[図19]図 1 9 は、実施の形態 1 における無線接続認証が完了した際の表示例を示す図である。

[図20]図 2 0 は、実施の形態 1 における無線通信装置の処理を示すフローチャートである。

[図21]図 2 1 は、実施の形態 1 におけるアクセスポイントの処理を示すフローチャートである。

[図22]図 2 2 は、実施の形態 1 におけるアクセスポイントの処理を示すフローチャートである。

[図23]図 2 3 は、実施の形態 1 におけるアクセスポイントの処理を示すフローチャートである。

[図24]図 2 4 は、実施の形態 1 におけるサーバの処理を示すフローチャート

である。

[図25]図25は、実施の形態1におけるサーバの処理を示すフローチャートである。

[図26]図26は、実施の形態1における既にアクセスポイントと通信を確立している無線通信装置の処理を示すフローチャートである。

[図27]図27は、実施の形態2におけるアカウント認証処理のシーケンス図である。

[図28]図28は、実施の形態2におけるアカウント認証処理のシーケンス図である。

[図29]図29は、実施の形態2におけるアクセスポイントの処理を示すフローチャートである。

[図30]図30は、実施の形態2におけるアクセスポイントの処理を示すフローチャートである。

[図31]図31は、実施の形態2におけるアクセスポイントの処理を示すフローチャートである。

[図32]図32は、実施の形態2におけるサーバの処理を示すフローチャートである。

[図33]図33は、実施の形態2におけるサーバの処理を示すフローチャートである。

[図34]図34は、実施の形態2における既にアクセスポイントと通信を確立している無線通信装置の処理を示すフローチャートである。

[図35]図35は、実施の形態3における無線通信装置の構成例を示すブロック図である。

[図36]図36は、実施の形態3におけるアカウント認証処理のシーケンス図である。

[図37]図37は、実施の形態3におけるアカウント認証処理のシーケンス図である。

[図38]図38は、実施の形態3における無線通信装置の処理を示すフローチャートである。

ャートである。

[図39]図39は、実施の形態3における既にアクセスポイントとの通信を確立している無線通信装置の処理を示すフローチャートである。

[図40]図40は、実施の形態におけるサーバの処理を示すフローチャートである。

発明を実施するための形態

[0011] (本発明の基礎となった知見)

本発明者は、「背景技術」の欄において記載した、無線認証接続方法に関し、以下の問題が生じることを見出した。

[0012] 自動的に無線パラメータを設定する方法として、Wi-Fi Allianceという団体によって定められたWi-Fi Protected Setup (WPS) という無線パラメータ自動設定方法が存在する。

[0013] このWPSでは、無線パラメータの設定処理用の特別なプロトコルとして、Registration (登録) プロトコルを用いてRegistrar (レジストラ) からEnrollee (エンローリー) へ無線パラメータが提供される。なお、レジストラとは、無線パラメータを管理し、エンローリーへ無線パラメータを提供する装置である。また、エンローリーとは、レジストラから提供された無線パラメータを受理する装置である。

[0014] 登録プロトコルにおけるレジストラとエンローリー間の通信は、EAP (Extensible Authentication Protocol) パケットを用いて行われる。EAPパケットとは、レジストラとエンローリー間において、暗号化及び認証を行うことなく通信できるパケットである。

[0015] 例として、レジストラとして動作するアクセスポイントから、エンローリーとして動作する無線通信装置に対して無線パラメータを提供する場合を説明する。まず、無線通信装置は、アクセスポイントが形成するネットワークを探索し、当該ネットワークに一時的に参加する。この時点では、アクセスポイントと無線通信装置におけるESSIDと周波数チャンネルは一致してい

るが、暗号鍵及び認証鍵等は一致していないため、暗号及び認証を用いた通常のデータ通信を行うことはできない。

[0016] アクセスポイントと無線通信装置は、登録プロトコルによりEAPパケットを用いたメッセージの送受信を行う。これにより、アクセスポイントから無線通信装置に対して無線パラメータが提供される。無線通信装置は、提供された無線パラメータを新たに設定することにより、アクセスポイントとの間で暗号及び認証を用いたデータ通信を行うことが可能になる。

[0017] WPSが提供する設定方式にはプッシュボタン方式と、PIN (Personal Identification Number) コード方式がある。プッシュボタン方式では無線パラメータの自動設定を行うことができるが、設定中にネットワーク内に存在する他のアクセスポイントがプッシュボタン方式による無線パラメータ設定を行っている場合、無線通信装置が他のアクセスポイントと意図せず接続される可能性がある。

[0018] PINコード方式では、無線通信装置が他のアクセスポイントと意図せず接続されることはないが、ユーザがアクセスポイントを選択し、PINコードを設定する必要がある、ユーザに手間がかかるという課題がある。

[0019] そのため、アカウント管理サーバを用いてユーザの認証を行うことでユーザの操作性を向上させる手法が提案されている（例えば、特許文献1参照）。特許文献1では、ユーザが所望のアクセスポイントに対して接続要求を送信し、接続要求を受信したアクセスポイントは接続要求を送信したユーザのユーザアカウントをアカウント管理サーバに送信する。アカウント管理サーバは、ユーザアカウントを管理するとともに、ユーザを認証してPINコードを生成し、アクセスポイントにPINコードを付与することで無線通信装置に通信許可を与える。このように、アカウント管理サーバがPINコードを生成することで、ユーザはPINコードを設定することなく、無線接続設定を行うことができる。

[0020] しかしながら、上記手法では、ユーザはネットワーク内に存在するアクセスポイントの中から所望のアクセスポイントを選択する必要があるため、ユ

ーザの負担となっていた。

[0021] 以下の実施の形態では、既にアクセスポイントと接続が確立されている無線通信装置を用いて新たにアクセスポイントと接続する無線通信装置の認証を行う。これにより、ユーザがアクセスポイントを選択することなく、無線通信装置とアクセスポイントの無線パラメータの設定できる。よって、ユーザの操作性を向上させることができる。

[0022] 本発明の一態様に係る無線接続認証方法は、第1無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバにおける無線接続認証方法であって、前記第1無線通信装置から送信された第1メッセージに従い第1無線アクセスポイントが送信した、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージを受信する第1受信ステップと、前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと既に通信が確立している第2無線通信装置から送信された第3メッセージに従い、前記第2無線アクセスポイントが送信した、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信ステップと、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理ステップとを含む。

[0023] これによれば、ユーザは、第1無線通信装置に第1メッセージを送信させる操作と、第2無線通信装置に第3メッセージを送信させる操作とのみを行えばよい。このように、ユーザは、簡単な操作で無線接続認証を行うことができる。

[0024] 例えば、前記無線接続認証方法は、さらに、前記第2無線通信装置から前

記第 1 無線通信装置に固有の第 1 コードを受信する第 3 受信ステップを含み、前記認証処理ステップは、前記第 1 コードを用いて、前記第 1 無線通信装置と前記接続先アクセスポイントとの無線接続認証に用いられる第 2 コードを生成する第 2 コード生成ステップと、前記第 2 コードを前記接続先アクセスポイントに送信する送信ステップとを含んでもよい。

[0025] これによれば、意図しない機器が誤って認証されることを防止できる。

[0026] 例えば、前記第 1 メッセージ及び前記第 2 メッセージの各々は、さらに、第 3 コードを含み、前記第 2 コード生成ステップでは、前記第 1 コード及び前記第 3 コードを用いて前記第 2 コードを生成してもよい。

[0027] これによれば、意図しない機器が誤って認証されることを防止できる。

[0028] また、本発明の一態様に係る無線接続認証方法は、第 1 無線通信装置と無線アクセスポイントとの無線接続認証を行う無線接続認証方法であって、前記第 1 無線通信装置が、第 1 メッセージを第 1 無線アクセスポイントに送信する第 1 メッセージ送信ステップと、前記第 1 メッセージを受信した前記第 1 無線アクセスポイントが、前記第 1 無線アクセスポイントを示す第 1 アクセスポイント情報を含む第 2 メッセージをサーバに送信する第 2 メッセージ送信ステップと、前記第 1 無線アクセスポイントと同一又は異なる第 2 無線アクセスポイントと無線接続認証が既に完了している第 2 無線通信装置が、第 3 メッセージを前記第 2 無線アクセスポイントに送信する第 3 メッセージ送信ステップと、前記第 3 メッセージを受信した前記第 2 無線アクセスポイントが、前記第 2 無線アクセスポイントを示す第 2 アクセスポイント情報を含む第 4 メッセージを前記サーバに送信する第 4 メッセージ送信ステップと、前記サーバが、前記第 1 アクセスポイント情報で示される前記第 1 無線アクセスポイントと、前記第 2 アクセスポイント情報で示される前記第 2 無線アクセスポイントとを比較し、前記第 1 無線アクセスポイントと前記第 2 無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第 1 無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、前記接

続先アクセスポイントと前記第 1 無線通信装置とが無線接続認証を行う認証ステップとを含む。

[0029] これによれば、ユーザは、第 1 無線通信装置に第 1 メッセージを送信させる操作と、第 2 無線通信装置に第 3 メッセージを送信させる操作とのみを行えばよい。このように、ユーザは、簡単な操作で無線接続認証を行うことができる。

[0030] 例えば、前記無線接続認証方法は、さらに、ユーザ操作に応じて、前記第 2 無線通信装置が前記第 1 無線通信装置に固有の第 1 コードを取得する取得ステップと、前記第 2 無線通信装置が、前記第 1 コードを前記サーバに送信する第 1 コード送信ステップと、前記サーバが、前記第 1 コードを用いて、前記第 1 無線通信装置と前記接続先アクセスポイントとの無線接続認証に用いられる第 2 コードを生成する第 2 コード生成ステップと、前記サーバが、前記第 2 コードを前記接続先アクセスポイントに送信する送信ステップと、前記第 1 無線通信装置が、前記第 1 コードと同一の第 3 コードを用いて第 4 コードを生成する第 4 コード生成ステップとを含み、前記認証ステップでは、前記第 1 無線通信装置及び前記接続先アクセスポイントが、前記第 2 コードと前記第 4 コードとが同一であるか否かに応じて、前記第 1 無線通信装置及び前記接続先アクセスポイントとの無線接続認証を行ってもよい。

[0031] これによれば、意図しない機器が誤って認証されることを防止できる。

[0032] 例えば、前記無線接続認証方法は、さらに、前記第 1 無線通信装置が第 5 コードを生成する生成ステップを含み、前記第 1 メッセージ及び前記第 2 メッセージの各々は、さらに、前記第 5 コードを含み、前記第 2 コード生成ステップでは、前記第 1 コード及び前記第 5 コードを用いて前記第 2 コードを生成し、前記第 4 コード生成ステップでは、前記第 3 コード及び前記第 5 コードを用いて前記第 4 コードを生成してもよい。

[0033] これによれば、意図しない機器が誤って認証されることを防止できる。

[0034] 例えば、前記第 3 メッセージ送信ステップは、前記第 1 メッセージ送信ステップの後に行われてもよい。

- [0035] 例えば、前記無線接続認証方法は、さらに、前記第1メッセージ送信ステップの後に、前記第1無線通信装置が、無線信号を送信する無線信号送信ステップを含み、前記第3メッセージ送信ステップでは、前記第2無線通信装置が前記無線信号を受信した場合に、前記第2無線通信装置が、前記第3メッセージを前記第2無線アクセスポイントに送信してもよい。
- [0036] これによれば、第3メッセージが誤って送信されることを防止できる。
- [0037] 例えば、前記第1メッセージ送信ステップは、前記第3メッセージ送信ステップの後に行われてもよい。
- [0038] また、本発明の一態様に係るサーバは、第1無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバであって、前記第1無線通信装置から送信された第1メッセージに従い第1無線アクセスポイントが送信した、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージを受信する第1受信部と、前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと既に通信が確立している第2無線通信装置から送信された第3メッセージに従い、前記第2無線アクセスポイントが送信した、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信部と、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定部と、前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理部とを備える。
- [0039] これによれば、ユーザは、第1無線通信装置に第1メッセージを送信させる操作と、第2無線通信装置に第3メッセージを送信させる操作とのみを行えばよい。このように、ユーザは、簡単な操作で無線接続認証を行うことが

できる。

[0040] なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

[0041] 以下、本発明の実施の形態について、図面を参照しながら説明する。

[0042] なお、以下で説明する実施の形態は、いずれも本発明の一具体例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

[0043] （実施の形態１）

図１は、本実施の形態における代表的な通信システム１００の構成の一例を示す図である。この通信システム１００は、無線通信装置１０１及び１０５と、アクセスポイント１０２と、サーバ１０３と、インターネット１０４とを含む。

[0044] 無線通信装置１０１は、無線ＬＡＮの通信機能とＷＰＳ機能とを有する通信機器であり、例えば、パーソナルコンピュータ、又は無線通信機能を有する家電機器である。アクセスポイント１０２は、無線ＬＡＮ及びＷＰＳ機能を有する。サーバ１０３は、無線通信装置のアカウント（ＩＤ及び認証コード等）を管理する機能と、無線通信装置を認証して当該無線通信装置に通信許可を与える機能とを有する。インターネット１０４は、世界中のコンピュータと接続可能な通信ネットワークである。無線通信装置１０５は、有線ＬＡＮ、又は無線ＬＡＮによって既にアクセスポイント１０２との接続を確立している通信機器であり、例えば、パーソナルコンピュータ、携帯電話、スマートフォン、又はタブレット端末である。以下では、無線通信装置１０５が無線ＬＡＮによってアクセスポイント１０２と接続する例を説明する。

- [0045] アクセスポイント１０２とサーバ１０３は、インターネット１０４を介して接続されている。無線通信装置１０１と無線通信装置１０５は、アクセスポイント１０２が構築するインフラストラクチャモードの無線ネットワークに接続されている。無線通信装置１０５は、既にアクセスポイント１０２と接続が確立しており、暗号を用いてインターネット１０４への接続が許可されている。
- [0046] 無線通信装置１０１とアクセスポイント１０２はそれぞれＰＩＮコードを設定する。そして、無線通信装置１０１が無線パラメータ自動設定アプリケーションを開始する。そして、設定情報通知プロトコルにより、無線通信装置１０１とアクセスポイント１０２との間で互いに保持するＰＩＮコードの一致が確認される。これにより、無線通信装置１０１は無線パラメータを取得できる。すなわち、ＰＩＮコードは、無線パラメータの設定処理に用いられるコード情報、又は、無線パラメータの設定処理において無線パラメータを提供してよいか否かの判定に用いられるコード情報である。
- [0047] ここで、設定情報通知プロトコルでは、各種メッセージの送受信にＥＡＰパケットが用いられる。そのため、無線通信装置１０１とアクセスポイント１０２とは、使用するＥＳＳＩＤ及び周波数チャネルが互いに一致すれば、無線ＬＡＮの暗号及び認証無しで設定情報通知プロトコルによる各種メッセージの送受信を行うことができる。したがって、認証が成功するまでは無線通信装置１０１はアクセスポイント１０２のみと通信可能である。また、無線通信装置１０１とサーバ１０３との通信は、アクセスポイント１０２がメッセージを転送することで行われる。無線通信装置１０１はサーバ１０３との認証が成功した場合にのみインターネット１０４に接続できる。
- [0048] 図１に示す無線通信装置１０１の構成を、図２を参照して説明する。図２は、本実施の形態における無線通信装置１０１の構成の一例を示すブロック図である。図２に示す無線通信装置１０１は、通信部２０１と、通信制御部２０２と、装置制御部２０３と、インターフェース処理部２０４と、無線パラメータ設定処理部２０５と、符号演算部２０６と、判断部２０７と、記憶

部 208 とを備える。

[0049] 通信部 201 は無線通信を行う。通信制御部 202 は通信部 201 の制御を行う。装置制御部 203 は無線通信装置 101 全体の動作を制御する。インターフェース処理部 204 は各種インターフェースの制御を行う。無線パラメータ設定処理部 205 は設定情報通知プロトコルによる無線パラメータ設定処理を行う。符号演算部 206 は各種信号及びハッシュ値などの演算を行う。判断部 207 は各種処理の判断を行う。記憶部 208 は無線パラメータ、アカウント情報、ID、及び認証コード等を記憶する。

[0050] 図 1 に示すアクセスポイント 102 の構成を、図 3 を参照して説明する。図 3 は本実施の形態におけるアクセスポイント 102 の構成の一例を示すブロック図である。図 3 に示すアクセスポイント 102 は、通信部 301 と、通信制御部 302 と、装置制御部 303 と、インターフェース処理部 304 と、無線パラメータ設定処理部 305 と、判断部 306 と、記憶部 307 とを備える。

[0051] 通信部 301 は無線通信を行う。通信制御部 302 は通信部 301 の制御を行う。装置制御部 303 は装置（アクセスポイント 102）全体の動作を制御する。インターフェース処理部 304 は各種インターフェースの制御を行う。無線パラメータ設定処理部 305 は設定情報通知プロトコルによる無線パラメータ設定処理を行う。判断部 306 は各種処理の判断を行う。記憶部 307 は無線パラメータ、アカウント情報、及びサーバの IP (Internet Protocol) アドレス等を記憶する。

[0052] 図 1 に示すサーバ 103 の構成を、図 4 を参照して説明する。図 4 は本実施の形態におけるサーバ 103 の構成の一例を示すブロック図である。図 4 に示すサーバ 103 は、通信部 401 と、通信制御部 402 と、装置制御部 403 と、インターフェース処理部 404 と、認証処理部 405 と、符号演算部 406 と、判断部 407 と、記憶部 408 とを備える。

[0053] 通信部 401 は通信を行う。通信制御部 402 は通信部 401 の制御を行う。装置制御部 403 は装置（サーバ 103）全体の動作を制御する。イン

ターフェース処理部404は各種インターフェースの制御を行う。認証処理部405は各種認証処理を行う。符号演算部406は各種信号及びハッシュ値などの演算を行う。判断部407は各種処理の判断を行う。記憶部408は無線パラメータ、アカウント情報、及び認証コード等を記憶する。

[0054] 図1に示す既にアクセスポイント102との接続を確立している無線通信装置105の構成を、図5を参照して説明する。図5は本実施の形態における既にアクセスポイント102との接続を確立している無線通信装置105の構成の一例を示すブロック図である。図2に示す無線通信装置105は、通信部501と、通信制御部502と、装置制御部503と、インターフェース処理部504と、無線パラメータ設定処理部505と、判断部506と、記憶部507と、表示部508とを備える。

[0055] 通信部501は無線通信を行う。通信制御部502は通信部501の制御を行う。装置制御部503は無線通信装置105全体の動作を制御する。インターフェース処理部504は各種インターフェースの制御を行う。無線パラメータ設定処理部505は設定情報通知プロトコルによる無線パラメータ設定処理を行う。判断部506は各種処理の判断を行う。記憶部507は無線パラメータ及びアカウント情報等を記憶する。表示部508は各種表示を行う。

[0056] 次に、無線通信装置101、アクセスポイント102、サーバ103、及び無線通信装置105の間で行われるアカウント認証シーケンスを、図6及び図7を用いて説明する。

[0057] 図6及び図7は、本実施の形態におけるアカウント認証シーケンスを示すシーケンス図である。

[0058] まず、無線通信装置101において、ユーザの操作等によって無線パラメータ自動設定アプリケーションが起動される(S101)。図8は、ユーザの操作例を示す図である。例えば、ユーザは、無線通信装置101（例えば冷蔵庫）に設けられている、ネットワーク接続を行うための操作ボタン651を押す。これにより、無線パラメータ自動設定アプリケーションが起動さ

れる。

- [0059] 上記操作が行われると、無線通信装置１０１は周辺の無線ネットワークを探索する（Ｓ１０２）。次に、無線通信装置１０１は、探索された複数の無線ネットワークを順次選択し、選択した無線ネットワークに参加する。この例では、アクセスポイント１０２の無線ネットワークが選択され、無線通信装置１０１はアクセスポイント１０２の無線ネットワークに参加する（Ｓ１０３）。しかし、この時点では、無線通信装置１０１とアクセスポイント１０２には共通の暗号鍵及び認証鍵等が設定されていない。そのため、無線通信装置１０１はアクセスポイント１０２の無線ネットワークにおいて特定の信号（報知信号及びＥＡＰパケット等）のみでしかアクセスポイント１０２と通信できない状態であり、暗号及び認証を用いた通常のデータ通信を行うことはできない。ここでは、無線通信装置１０１とアクセスポイント１０２の間においてＥＡＰパケットを用いて各種メッセージの送受信が行われる。
- [0060] 次に、無線通信装置１０１はランダム値を生成する（Ｓ１０４）。次に、無線通信装置１０１は、ランダム値とＩＤとを含む接続要求メッセージ６１１をアクセスポイント１０２に送信する（Ｓ１０５）。
- [0061] 図９は、無線通信装置１０１が備える記憶部２０８に記憶されている情報の一例を示す図である。図９に示すように、記憶部２０８は、ＩＤ６６１と、認証コード６６２とを記憶している。
- [0062] ＩＤ６６１は、無線通信装置１０１を識別するための識別子であり、例えば、無線通信装置１０１の型番、製造番号、又はこれらの組合せである。なお、ＩＤ６６１は任意の数字又は文字の組合せであってもよい。
- [0063] 認証コード６６２は、無線通信装置１０１を識別するための識別子であり、例えば、無線通信装置１０１の型番、製造番号、又はこれらの組合せである。なお、認証コード６６２は任意の数字又は文字の組合せであってもよい。また、ここでは、ＩＤ６６１と認証コード６６２とを個別に記載しているが、ＩＤ６６１及び認証コード６６２の一方のみが用いられてもよい。言い換えると、ＩＤ６６１と認証コード６６２は同一のコード（識別子）であっ

てもよい。

[0064] 図10は、接続要求メッセージ611の構成例を示す図である。接続要求メッセージ611は、無線通信装置101がネットワークへの接続をサーバ103に要求するためのメッセージである。言い換えると、接続要求メッセージ611は、無線通信装置101がアクセスポイント102への接続をサーバ103に要求するためのメッセージである。この接続要求メッセージ611は、記憶部208に記憶されているID661と、ステップS104で生成されたランダム値663とを含む。

[0065] なお、接続要求メッセージ611は、必要に応じて上記以外の情報（例えば、当該メッセージの種別を示す情報、並びにメッセージの送信元及び送信先を示す情報等）を含むが、これらの情報は図10には図示していない。また、これらの情報が含まれる点は、後述する各種メッセージにおいても同様である。

[0066] アクセスポイント102は、接続要求メッセージ611を受信した場合、受信した接続要求メッセージ611にアクセスポイント情報664を付加することで接続要求メッセージ612を生成し、生成した接続要求メッセージ612をサーバ103へ送信する（S106）。

[0067] 図11は、接続要求メッセージ612の構成例を示す図である。図11に示すように、接続要求メッセージ612は、接続要求メッセージ611に含まれていたID661及びランダム値663と、アクセスポイント情報664とを含む。アクセスポイント情報664は、接続要求メッセージ612の送信元のアクセスポイントを示す情報である。よって、この例では、アクセスポイント情報664は、アクセスポイント102を示す。

[0068] なお、ここでは、アクセスポイント102が、接続要求メッセージ611にアクセスポイント情報664を付加する例を述べたが、無線通信装置101がアクセスポイント情報664を含む接続要求メッセージ611を生成してもよい。この場合、アクセスポイント情報664は、接続要求メッセージ611の送信先のアクセスポイントを示す。

[0069] サーバ103は、接続要求メッセージ612を受信した場合、受信した接続要求メッセージ612に含まれるID661の有効性を確認し（S107）、ID661が有効である場合は、受信したID661を持つ無線通信装置101をアクセスポイント102への接続要求がある端末として登録する（S108）。

[0070] ここで、ステップS102において、複数の無線ネットワークが探索された場合には、複数のアクセスポイントの各々に対してステップS103及びS105を行う。これにより、サーバ103は、異なるアクセスポイントを経由した複数の接続要求メッセージ612を受信する。例えば、図12に示すように、無線通信装置101に近くにアクセスポイント102（AP1）と、アクセスポイント102A（AP2）が存在する場合、アクセスポイント102を経由した接続要求メッセージ612と、アクセスポイント102Aを経由した接続要求メッセージ612とが、サーバ103で受信される。

[0071] この場合、図13に示すように、2つの接続要求メッセージ612に対応する情報（ID671、ランダム値672及びアクセスポイント情報673）がサーバ103に登録される。ここで、2つの接続要求メッセージ612は、当該メッセージを経由したアクセスポイントが異なるため、アクセスポイント情報673で示されるアクセスポイントが異なる。なお、図13では、2つの接続要求メッセージ612のID671及びランダム値672が同一であるが、これらの少なくとも一方が異なってもよい。

[0072] 次に、既にアクセスポイント102と接続が確立している無線通信装置105において、ユーザの操作等によって参加登録アプリケーションが起動される（S109）。図14は、ユーザの操作例を示す図である。例えば、ユーザは、無線通信装置105（例えばスマートフォン）において、ネットワーク参加確認を行うための操作メニュー652を選択する。これにより、参加登録アプリケーションが起動される。

[0073] 次に、無線通信装置105は参加確認メッセージ613をアクセスポイン

ト 102 に送信する (S 110)。アクセスポイント 102 は参加確認メッセージ 613 を受信した場合、参加確認メッセージ 613 にアクセスポイント情報 665 を付加することで参加確認メッセージ 614 を生成し、生成された参加確認メッセージ 614 をサーバ 103 に送信する (S 111)。

[0074] 図 15 は、参加確認メッセージ 614 の構成例を示す図である。図 15 に示すように、参加確認メッセージ 614 は、アクセスポイント情報 665 を含む。アクセスポイント情報 665 は、参加確認メッセージ 614 の送信元のアクセスポイントを示す情報である。よって、この例では、アクセスポイント情報 665 は、アクセスポイント 102 を示す。

[0075] なお、ここでは、アクセスポイント 102 が、参加確認メッセージ 614 にアクセスポイント情報 665 を付加する例を述べたが、無線通信装置 105 がアクセスポイント情報 665 を含む参加確認メッセージ 613 を生成してもよい。この場合、アクセスポイント情報 665 は、参加確認メッセージ 613 の送信先のアクセスポイントを示す。

[0076] また、いずれの場合でも、アクセスポイント情報 665 は、無線通信装置 105 が既に通信を確立しているアクセスポイント 102 を示す。また、アクセスポイント情報 665 は、無線通信装置 101 の接続先のアクセスポイント 102 を示す。

[0077] サーバ 103 は、参加確認メッセージ 614 を受信した場合、アクセスポイント 102 への接続要求がある端末が存在するかを確認する。具体的には、サーバ 103 は、参加確認メッセージ 614 に含まれるアクセスポイント情報 665 で示されるアクセスポイントと、同一のアクセスポイントを示すアクセスポイント情報 673 が存在するかを確認する (S 112)。

[0078] 例えば、図 13 に示すように、アクセスポイント情報 673 として AP 1 (アクセスポイント 102) と AP 2 (アクセスポイント 102A) とが登録されている場合、サーバ 103 は、アクセスポイント情報 665 で示される AP 1 (アクセスポイント 102) を、無線通信装置 101 の接続先に決定する。

- [0079] 次に、サーバ１０３は、接続先に決定されたアクセスポイント１０２に認証コード要求メッセージ６１５Ａを送信する（Ｓ１１３）。アクセスポイント１０２は、認証コード要求メッセージ６１５Ａを受信した場合、無線通信装置１０５に認証コード要求メッセージ６１５Ｂを送信する（Ｓ１１４）。
- [0080] 無線通信装置１０５は、認証コード要求メッセージ６１５Ｂを受信した場合、ユーザの操作等に応じて認証コードを生成する（Ｓ１１５）。例えば、図１６に示すように、ユーザは、入力メニュー６５３に認証コードを入力する。ここで、入力される認証コードは、無線通信装置１０１に固有の数字又は文字列であり、無線通信装置１０１の記憶部２０８に記憶されている認証コード６６２と同一である。例えば、ユーザは、無線通信装置１０１（例えば、家電機器）の筐体、又は取扱説明書等に記載されている認証コードを確認し、当該認証コードを入力メニュー６５３に入力する。
- [0081] なお、ユーザは、無線通信装置１０１の筐体、又は取扱説明書等に記載されているバーコード又は二次元バーコード等を、無線通信装置１０５（例えばスマートフォン）で撮影してもよい。これにより、無線通信装置１０５は、認証コードを取得できる。
- [0082] 次に、無線通信装置１０５は、アクセスポイント１０２に認証コード情報メッセージ６１６Ａを送信する（Ｓ１１６）。図１７は、認証コード情報メッセージ６１６Ａの構成例を示す図である。図１７に示すように、認証コード情報メッセージ６１６Ａは、ステップＳ１１５で生成された認証コード６６６を含む。
- [0083] アクセスポイント１０２は、認証コード情報メッセージ６１６Ａを受信した場合、認証コード情報メッセージ６１６Ａに含まれる認証コード６６６を含む認証コード情報メッセージ６１６Ｂをサーバ１０３に送信する（Ｓ１１７）。例えば、認証コード情報メッセージ６１６Ｂの構成例は、図１７に示す認証コード情報メッセージ６１６Ａの構成例と同じである。
- [0084] サーバ１０３は、認証コード情報メッセージ６１６Ｂを受信した場合、受信した認証コード情報メッセージ６１６Ｂに含まれる認証コード６６６の有

効性を確認する（S 1 1 8）。認証コード 6 6 6 が有効である場合は、サーバ 1 0 3 は、アクセスポイント 1 0 2 への接続要求がある端末である無線通信装置 1 0 1 の無線パラメータ設定のための P I N コードを、接続要求メッセージ 6 1 2 に含まれていたランダム値 6 6 3 と、認証コード情報メッセージ 6 1 6 B に含まれていた認証コード 6 6 6 を用いて生成する（S 1 1 9）。

[0085] 次に、サーバ 1 0 3 は、図 1 8 に示すように、生成した P I N コード 6 6 7 を含む P I N コード情報メッセージ 6 1 7 をアクセスポイント 1 0 2 に送信する（S 1 2 0）。アクセスポイント 1 0 2 は、P I N コード情報メッセージ 6 1 7 を受信した場合、無線パラメータ自動設定アプリケーションを起動し、付加されている P I N コード 6 6 7 を無線パラメータ自動設定アプリケーションに設定する（S 1 2 1）。アクセスポイント 1 0 2 は、P I N コードを設定した後、P I N コード生成完了メッセージを無線通信装置 1 0 1 に送信する（S 1 2 2）。

[0086] 無線通信装置 1 0 1 は、P I N コード生成完了メッセージ 6 1 8 を受信した場合、ステップ S 1 0 4 で生成されたランダム値と、記憶部 2 0 8 に記憶されている認証コード 6 6 2 とを用いて P I N コードを生成する（S 1 2 3）。次に、無線通信装置 1 0 1 は、生成された P I N コードを無線パラメータ自動設定アプリケーションに設定する（S 1 2 4）。次に、無線通信装置 1 0 1 は、設定情報通知プロトコルを開始するためにプロトコル開始要求メッセージ 6 1 9 をアクセスポイント 1 0 2 に送信する（S 1 2 5）。

[0087] アクセスポイント 1 0 2 は、無線通信装置 1 0 1 からプロトコル開始要求メッセージ 6 1 9 を受信した場合、プロトコル開始メッセージ 6 2 0 を無線通信装置 1 0 1 に送信する（S 1 2 6）。そして、無線通信装置 1 0 1 とアクセスポイント 1 0 2 は、W P S の登録プロトコルに従いプロトコルメッセージ 6 2 1 を交換する（S 1 2 7）。ここで、無線通信装置 1 0 1 に設定された P I N コードとアクセスポイント 1 0 2 に設定された P I N コードとが一致することが、無線通信装置 1 0 1 とアクセスポイント 1 0 2 の双方で確

認された場合のみ、アクセスポイント１０２の無線パラメータが無線通信装置１０１に送信され、送信された無線パラメータが無線通信装置１０１に設定される。

[0088] 次に、アクセスポイント１０２は、設定情報通知プロトコルが終了した後、プロトコル終了メッセージ６２２を無線通信装置１０１に送信し（Ｓ１２８）、ＷＰＳ成功メッセージ６２３をサーバ１０３に送信する（Ｓ１２９）。サーバ１０３は、ＷＰＳ成功メッセージ６２３を受信した場合、無線通信装置１０１にインターネットへの接続を許可する処理を行う（Ｓ１３０）。

[0089] 無線通信装置１０１は、プロトコル終了メッセージ６２２を受信した場合、一旦、ネットワークを離脱し、アクセスポイント１０２から取得したパラメータを用いることにより、再びアクセスポイント１０２の無線ネットワークに接続する（Ｓ１３１）。ここで、無線通信装置１０１には、アクセスポイント１０２と共通の暗号鍵及び認証鍵等が設定されている。よって、無線通信装置１０１は、暗号及び認証を用いた通常のデータ通信をおこなうことが可能である。

[0090] また、サーバ１０３は、接続を許可する処理を行った後、アクセスポイント１０２に接続許可メッセージ６２４Ａを送信する（Ｓ１３２）。アクセスポイント１０２は、接続許可メッセージ６２４Ａを受信した場合、無線通信装置１０５に接続許可メッセージ６２４Ｂを送信する（Ｓ１３３）。無線通信装置１０５は、接続許可メッセージ６２４Ｂを受信した場合、例えば、図１９に示す、無線通信装置１０１とアクセスポイント１０２との無線接続認証が完了した旨を示すメッセージ６５４を、ユーザに表示する。

[0091] 以上のように、本実施の形態に係る通信システム１００は、無線通信装置１０１とアクセスポイント１０２との無線接続認証を行う。具体的には、無線通信装置１０１が、接続要求メッセージ６１１を第１無線アクセスポイント（アクセスポイント１０２又はアクセスポイント１０２Ａ）に送信する（Ｓ１０５）。接続要求メッセージ６１１を受信したアクセスポイント１０２（又はアクセスポイント１０２Ａ）が、当該第１無線アクセスポイントを示

すアクセスポイント情報 664 を含む接続要求メッセージ 612 をサーバ 103 に送信する (S106)。

[0092] 次に、第 1 無線アクセスポイントと同一又は異なる第 2 無線アクセスポイント (アクセスポイント 102) と無線接続認証が既に完了している無線通信装置 105 が、参加確認メッセージ 613 を第 2 無線アクセスポイントに送信する (S110)。参加確認メッセージ 613 を受信した第 2 無線アクセスポイントが、当該第 2 無線アクセスポイントを示すアクセスポイント情報 665 を含む参加確認メッセージ 614 をサーバ 103 に送信する (S111)。

[0093] 次に、サーバ 103 が、アクセスポイント情報 664 で示される第 1 無線アクセスポイントと、アクセスポイント情報 665 で示される第 2 無線アクセスポイントとを比較し、その結果、第 1 無線アクセスポイントと第 2 無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、無線通信装置 101 の接続先の無線アクセスポイントである接続先アクセスポイントに決定する (S112)。

[0094] 最後に、接続先アクセスポイントと無線通信装置 101 とが無線接続認証を行う (S125～S128)。

[0095] 以上により、サーバ 103 は、無線通信装置 101 が通信可能な複数の無線アクセスポイント (例えば、アクセスポイント 102 及び 102A) が存在する場合であっても、無線通信装置 105 から送信された参加確認メッセージ 613 に従い接続対象の無線アクセスポイント (アクセスポイント 102) が送信したアクセスポイント情報 665 を用いて、無線通信装置 101 の接続対象の無線アクセスポイントを適切に決定できる。

[0096] また、ユーザは、無線通信装置 101 に接続要求メッセージ 611 を送信させる操作と、無線通信装置 105 に参加確認メッセージ 613 を送信させる操作とのみを行えばよい。例えば、ユーザは、図 8 に示すように、無線通信装置 101 (冷蔵庫) に設けられている操作ボタン 651 を押し、その後、図 14 に示すように、無線通信装置 105 (スマートフォン) において操

作メニュー 6 5 2 を選択するという簡単な操作のみを行えばよい。このように、本実施の形態に係る無線接続認証方法は、ユーザが簡単な操作で無線接続認証を行うことができる。

[0097] 一方、ユーザが、ネットワーク内に存在する複数のアクセスポイントの中から所望のアクセスポイントを選択する場合には、ユーザが、機器の設定等に不慣れな場合には、適切に所望のアクセスポイントを選択することが困難な場合がある。

[0098] また、ユーザがアクセスポイントに設けられているボタン等を操作する場合には、無線通信機器（例えば家電機器）とアクセスポイントとが離れて配置されている場合もある。このような場合には、ユーザは、離れて配置されている無線通信機器とアクセスポイントとの両方の操作を行う必要があり、ユーザにとって手間がかかるという課題がある。さらに、アクセスポイントの設置場所によっては、アクセスポイントに設けられているボタン等を容易に操作できない場合もある。一方で、本実施の形態では、例えば、ユーザが所有するスマートフォンを操作ればよいので、ユーザの手間を低減できる。

[0099] さらに、本実施の形態では、アクセスポイントにボタン等を設ける必要がないので、システム全体のコストを低減できる。また、ユーザ操作が簡略化されることにより、不慣れなユーザによる不必要な操作の発生を低減できるので、機器の劣化又は故障を抑制できるとともに、不要な電力消費を低減できる。

[0100] このように、本実施の形態では、既に所望のアクセスポイントとの接続を確立している端末を用いて新たにネットワークに接続する端末の無線パラメータが設定される。また、サーバ 1 0 3 は、新たにネットワークに接続する端末と、既に所望のアクセスポイントとの接続を確立している端末とから送信されたメッセージに、同一のアクセスポイントを示す情報が含まれるかを判断する。これにより、無線通信を行うことができるアクセスポイントが複数存在する場合であっても、意図しないアクセスポイントに接続されることを防止できる。また、ユーザがアクセスポイントを選択する必要がないので

、ユーザの操作性が向上する。

[0101] さらに、無線通信装置 105 は、ユーザ操作に応じて、無線通信装置 101 に固有の認証コード 666（第 1 コード）を取得する（S 115）。次に、無線通信装置 105 は、認証コード 666 をサーバ 103 に送信する（S 116 及び S 117）。具体的には、無線通信装置 105 は、認証コード 666 を含む認証コード情報メッセージ 616A（616B）を、アクセスポイント 102 を介してサーバ 103 に送信する。

[0102] また、サーバ 103 は、認証コード 666 を用いて、無線通信装置 101 と接続先アクセスポイント（アクセスポイント 102）との無線接続認証に用いられる PIN コード 667（第 2 コード）を生成する（S 119）。次に、サーバ 103 は、PIN コード 667 をアクセスポイント 102 に送信する（S 120）。

[0103] また、無線通信装置 101 が、認証コード 666 と同一の認証コード 662（第 3 コード）を用いて PIN コード（第 4 コード）を生成する（S 123）。無線通信装置 101 及びアクセスポイント 102 は、認証コード 662 と、無線通信装置 101 で生成された認証コードとが同一であるか否かに応じて、無線通信装置 101 及びアクセスポイント 102 との無線接続認証を行う（S 125～S 128）。

[0104] これにより、無線 LAN において無線通信装置 101 とアクセスポイント 102 に安全かつ自動的に同一の PIN コードを設定することができる。また、例えば、無線通信装置 101 が保持している認証コード 662 と、無線通信装置 105 に対してユーザが入力した認証コード 666 とを用いて、2 つの PIN コードが生成されるので、意図しない機器が誤って認証されることを防止できる。

[0105] さらに、無線通信装置 101 は、ランダム値 663（第 5 コード）を生成する（S 104）。また、接続要求メッセージ 611 及び 612 の各々は、さらに、ランダム値 663 を含む。

[0106] サーバ 103 は、認証コード 666 及びランダム値 663 を用いて PIN

コード 667 を生成する (S119)。無線通信装置 101 は、認証コード 662 及びランダム値 663 を用いて認証コードを生成する (S123)。

[0107] これにより、設定される PIN コードが、ランダム値及び認証コードを用いて生成されるため、設定ごとに異なる PIN コードが生成される。これにより、安全性を向上できる。さらに、認証コードは暗号化されたネットワークでのみ通信されるため、安全性が高い。

[0108] また、認証コードの入力には新たにネットワークに接続する無線通信装置 101 (例えば家電機器) が用いられず、無線通信装置 105 (例えばスマートフォン) が用いられる。これにより、キーボード又はタッチパネルを有さないようなユーザインターフェースが乏しい無線通信装置 101 に対しても無線パラメータを設定することが可能である。

[0109] 次に、各装置における処理の流れを説明する。まず、無線通信装置 101 が設定情報通知プロトコルを実行する際の処理手順を、図 20 を用いて説明する。

[0110] 図 20 は、本実施の形態における無線通信装置 101 の処理を示すフローチャートである。なお、この処理は、アクセスポイント 102 が構築する無線ネットワークに無線通信装置 101 が接続した際に開始される。なお、この時点では、無線通信装置 101 とアクセスポイント 102 には共通の暗号鍵及び認証鍵等が設定されていない。そのため、無線通信装置 101 は、アクセスポイント 102 の無線ネットワークにおいて特定の信号 (報知信号及び EAP パケット等) のみでしかアクセスポイント 102 と通信できない状態であり、暗号及び認証を用いた通常の日データ通信を行うことはできない。ここでは、無線通信装置 101 及びアクセスポイント 102 の間において EAP パケットを用いて各種メッセージの送受信が行われる。

[0111] まず、無線通信装置 101 は、PIN コードの生成に必要なランダム値 663 を生成する (S201)。そして、無線通信装置 101 は、ランダム値 663 と ID 661 とを含む接続要求メッセージ 611 をアクセスポイント 102 に送信する (S202)。無線通信装置 101 は、接続要求メッセー

ジ611の送信後、アクセスポイント102からPINコード生成完了メッセージ618を受信するか、プロトコル失敗メッセージを受信するまで待機する(S203及びS204)。無線通信装置101は、プロトコル失敗メッセージを受信した場合(S204でYES)、この処理を終了する。

[0112] また、無線通信装置101は、PINコード生成完了メッセージ618を受信した場合(S203でYES)、認証コード662(パスワード)と予め生成したランダム値663とを用いてPINコードを生成する(S205)。PINコードを生成する方法は暗号アルゴリズム又はハッシュアルゴリズムを用いる方法など、いずれの方法でもよい。

[0113] 無線通信装置101は、PINコードを生成した後、無線パラメータ自動設定アプリケーションにPINコードを設定する(S206)。そして、無線通信装置101は、設定したPINコードを用いて設定情報通知プロトコルを実行する(S207)。設定情報通知プロトコルでは、エンローリーとレジストラが互いのPINコードが一致するか否かを判定することにより、互いの正当性を認証する。そのため、エンローリーは同一のPINコードを持つレジストラから無線パラメータを取得することができる。

[0114] 無線通信装置101は、設定情報通知プロトコルが終了した後、設定情報通知プロトコルが成功したか否かを判断する(S208)。ここで、設定情報通知プロトコルの成功とは、エンローリーのPINコードと一致するPINコードを保持するレジストラからの無線パラメータの取得が完了したことを示す。設定情報通知プロトコルが失敗した場合(S208でNO)、無線通信装置101はこの処理を終了する。

[0115] 一方、設定情報通知プロトコルが成功した場合(S208でYES)、無線通信装置101は、取得した無線パラメータを用いてアクセスポイント102が構築している無線ネットワークに接続する(S209)。こうすることにより、無線通信装置101には、アクセスポイント102と共通の暗号鍵及び認証鍵等が設定される。これにより、無線通信装置101は、暗号及び認証を用いた通常のデータ通信を行うことが可能となる。

[0116] 次に、アクセスポイント１０２が設定情報通信プロトコルを実行する際の処理手順を、図２１、図２２及び図２３を用いて説明する。

[0117] 図２１、図２２及び図２３は、本実施の形態におけるアクセスポイント１０２の処理を示すフローチャートである。なお、この処理はアクセスポイント１０２が構築している無線ネットワークに無線パラメータ自動設定の実行を要求する無線通信装置１０１が参加した際に開始される。なお、この時点では、無線通信装置１０１とアクセスポイント１０２には共通の暗号鍵及び認証鍵等が設定されていない。そのため、無線通信装置１０１は、アクセスポイント１０２の無線ネットワークにおいて特定の信号（報知信号及びＥＡＰパケット等）のみでしかアクセスポイント１０２と通信できない状態であり、暗号及び認証を用いた通常の日データ通信を行うことはできない。ここでは、無線通信装置１０１及びアクセスポイント１０２の間においてＥＡＰパケットを用いて各種メッセージの送受信が行われる。

[0118] まず、アクセスポイント１０２は、無線通信装置１０１から接続要求メッセージ６１１を受信するのを待つ（Ｓ３０１）。アクセスポイント１０２は、無線通信装置１０１から接続要求メッセージ６１１を受信した場合（Ｓ３０１でＹＥＳ）、接続要求メッセージ６１１に含まれるランダム値６６３及びＩＤ６６１と、当該アクセスポイント１０２を示すアクセスポイント情報６６４とを含む接続要求メッセージ６１２をサーバ１０３に送信する（Ｓ３０２）。

[0119] アクセスポイント１０２は、接続要求メッセージ６１２を送信した後、既にアクセスポイント１０２との接続を確立している無線通信装置１０５から参加確認メッセージ６１３を受信するか、サーバ１０３から拒否通知メッセージを受信するまで待つ（Ｓ３０３及びＳ３０４）。

[0120] アクセスポイント１０２は、拒否通知メッセージを受信した場合（Ｓ３０４でＹＥＳ）、プロトコル失敗メッセージを無線通信装置１０１に送信し（Ｓ３０５）、この処理を終了する。ここで、無線通信装置１０５及びアクセスポイント１０２には共通の暗号鍵及び認証鍵等が設定されているため、無

線通信装置 105 及びアクセスポイント 102 は、暗号及び認証を用いた通常のデータ通信を行うことができる。

[0121] アクセスポイント 102 は、無線通信装置 105 から参加確認メッセージ 613 を受信した場合（S303 で YES）、当該アクセスポイント 102 を示すアクセスポイント情報 665 を含む参加確認メッセージ 614 をサーバ 103 に送信する（S306）。アクセスポイント 102 は、参加確認メッセージ 614 を送信した後、サーバ 103 から認証コード要求メッセージ 615A を受信するか、拒否通知メッセージを受信するまで待つ（S307 及び S308）。アクセスポイント 102 は、拒否通知メッセージを受信した場合（S308 で YES）、プロトコル失敗メッセージを無線通信装置 101 に送信し、拒否通知メッセージを無線通信装置 105 に送信し（S309）、この処理を終了する。

[0122] アクセスポイント 102 は、認証コード要求メッセージ 615A を受信した場合（S307 で YES）、無線通信装置 105 に認証コード要求メッセージ 615B を送信する（S310）。アクセスポイント 102 は、認証コード要求メッセージ 615B を送信した後、無線通信装置 105 から認証コード 666 を含む認証コード情報メッセージ 616A を受信するまで待つ（S311）。ここで、認証コード 666 とは無線通信装置 101 に固有の数字又は文字列である。

[0123] アクセスポイント 102 は、認証コード情報メッセージ 616A を受信した場合（S311 で YES）、認証コード情報メッセージ 616A に含まれる認証コード 666 を含む認証コード情報メッセージ 616B をサーバ 103 に送信する（S312）。アクセスポイント 102 は、認証コード情報メッセージ 616B を送信した後、サーバ 103 から PIN コード情報メッセージ 617 を受信するか、拒否通知メッセージを受信するまで待つ（S313 及び S314）。アクセスポイント 102 は、拒否通知メッセージを受信した場合（S314 で YES）、プロトコル失敗メッセージを無線通信装置 101 に送信し、拒否通知メッセージを無線通信装置 105 に送信し（S3

15)、この処理を終了する。

[0124] 一方、アクセスポイント102は、PINコード情報メッセージ617を受信した場合(S313でYES)、PINコード情報メッセージ617に含まれるPINコード667を無線パラメータ自動設定アプリケーションに設定する(S316)。そして、アクセスポイント102は、無線通信装置101にPINコード生成完了メッセージ618を送信する(S317)。次に、アクセスポイント102は、設定したPINコード667を用いて設定情報通知プロトコルを無線通信装置101との間で実行する(S318)。

[0125] 次に、アクセスポイント102は、設定情報通知プロトコルが成功したか否かを判断する(S319)。ここで、設定情報通知プロトコルの成功とは、レジストラが保持するPINコードとエンローリーが保持するPINコードとが一致し、レジストラからエンローリーに対しての無線パラメータの提供が完了した場合を示す。設定情報通知プロトコルが成功した場合(S319でYES)、アクセスポイント102は、WPS成功メッセージ623をサーバ103に送信する(S320)。アクセスポイント102は、WPS成功メッセージを送信した後、サーバ103から接続許可メッセージ624Aを受信するまで待つ(S321)。アクセスポイント102は、接続許可メッセージ624Aを受信した場合(S321でYES)、接続許可メッセージ624Bを無線通信装置105に送信し(S322)、この処理を終了する。

[0126] 一方、設定情報通知プロトコルが失敗した場合(S319でNO)、アクセスポイント102は、WPS失敗メッセージをサーバ103に送信する(S323)。アクセスポイント102は、WPS失敗メッセージを送信した後、サーバ103から接続失敗メッセージを受信するまで待つ(S324)。アクセスポイント102は、接続失敗メッセージを受信した場合(S324でYES)、接続失敗メッセージを無線通信装置105に送信し(S325)、この処理を終了する。

[0127] 次に、無線通信装置１０１がインターネット１０４に接続する際に、認証を行うサーバ１０３の処理手順を、図２４及び図２５を用いて説明する。図２４及び図２５は本実施の形態におけるサーバ１０３の処理を示すフローチャートである。

[0128] まず、サーバ１０３は、アクセスポイント１０２から接続要求メッセージ６１２を受信するのを待つ（Ｓ４０１）。サーバ１０３は、アクセスポイント１０２から接続要求メッセージを受信した場合（Ｓ４０１でＹＥＳ）、接続要求メッセージ６１２に含まれるＩＤ６６１が有効なＩＤであるか否かを確認する（Ｓ４０２）。例えば、サーバ１０３は、記憶部４０８に保存しているアカウント管理情報を参照し、予め有効なＩＤとして登録されたＩＤと受信したＩＤ６６１とが一致すれば、受信したＩＤ６６１は有効と判断する。

[0129] ここで、受信したＩＤ６６１が無効であった場合（Ｓ４０２でＮＯ）、サーバ１０３は、拒否通知メッセージをアクセスポイント１０２に送信し（Ｓ４１６）、この処理を終了する。一方、受信したＩＤ６６１が有効であった場合（Ｓ４０２でＹＥＳ）、サーバ１０３は、接続要求メッセージ６１１を送信した無線通信装置１０１のＩＤ６６１を登録する（Ｓ４０３）。

[0130] 次に、サーバ１０３は、アクセスポイント１０２から参加確認メッセージ６１４を受信するまで待つ（Ｓ４０４）。サーバ１０３は、参加確認メッセージ６１４を受信した場合（Ｓ４０４でＹＥＳ）、参加確認メッセージ６１４に含まれるアクセスポイント情報６６５で示されるアクセスポイントが、接続要求メッセージ６１２に含まれるアクセスポイント情報６６４で示されるアクセスポイントと同一か否かを確認する（Ｓ４０５）。

[0131] ここで、アクセスポイントが異なる場合（Ｓ４０５でＮＯ）、サーバ１０３はアクセスポイント１０２からの参加確認メッセージ６１４を受信するまで待つ（Ｓ４０４）。一方、アクセスポイントが同一、すなわち、参加確認メッセージ６１４がアクセスポイント１０２から送信されていた場合（Ｓ４０５でＹＥＳ）、サーバ１０３はアクセスポイント１０２に認証コード要求

メッセージ615Aを送信する(S406)。

[0132] 次に、サーバ103はアクセスポイント102から認証コード情報メッセージ616Bを受信するまで待つ(S407)。サーバ103は、アクセスポイント102から認証コード情報メッセージ616Bを受信した場合(S407でYES)、認証コード情報メッセージ616Bに含まれる認証コード666が、接続要求が行われたIDに紐付けされた認証コードであるか否かを確認する(S408)。例えば、サーバ103は、記憶部408に保存しているアカウント管理情報を参照し、予めIDに紐付けされた認証コードと受信した認証コード666とが一致すれば、受信した認証コード666は有効と判断する。ここで、認証コードは無線通信装置101に固有のコードであるため、この処理により、無線通信装置105の正当性を確認することができる。

[0133] ここで、受信した認証コード666が無効であった場合(S408でNO)、サーバ103は拒否通知メッセージをアクセスポイント102に送信し(S416)、この処理を終了する。一方、受信した認証コードが有効であった場合(S408でYES)、サーバ103は接続要求メッセージ612に含まれるランダム値663と、認証コード情報メッセージ616Bに含まれる認証コード666とを用いてPINコード667を生成する(S409)。

[0134] 次に、サーバ103は、生成したPINコード667を含むPINコード情報メッセージ617をアクセスポイント102に送信する(S410)。PINコード情報メッセージ617を送信した後、サーバ103は、アクセスポイント102からWPS成功メッセージ623を受信するか、WPS失敗メッセージを受信するのを待つ(S411及びS412)。

[0135] サーバ103は、WPS成功メッセージ623を受信した場合(S411でYES)、無線通信装置101にインターネット104への接続を許可する処理を行う(S414)。次に、サーバ103は、アクセスポイント102に接続許可メッセージ624Aを送信し(S415)、この処理を終了す

る。また、サーバ103は、WPS失敗メッセージを受信した場合（S412でYES）、アクセスポイント102に接続失敗メッセージを送信し（S413）、この処理を終了する。

[0136] 次に、無線通信装置101がインターネット104に接続する際に、認証手続きを行う無線通信装置105の処理手順を、図26を用いて説明する。

[0137] 図26は、本実施の形態における無線通信装置105の処理を示すフローチャートである。なお、無線通信装置105とアクセスポイント102には既に共通の暗号鍵及び認証鍵等が設定されている。そのため、無線通信装置105はアクセスポイント102の無線ネットワークにおいて暗号及び認証を用いた通常の日タ通信を行うことができる。

[0138] まず、無線通信装置105は、参加確認メッセージ613をアクセスポイント102に送信し（S501）、アクセスポイント102から認証コード要求メッセージ615Bを受信するのを待つ（S502）。

[0139] 無線通信装置105は、認証コード要求メッセージ615Bを受信した場合（S502でYES）、ユーザの操作等に応じて認証コード666を生成する（S503）。ここで、認証コード666とは無線通信装置101固有の数字又は文字列である。次に、無線通信装置105は、生成した認証コード666を含む認証コード情報メッセージ616Aをアクセスポイント102に送信する（S504）。

[0140] 無線通信装置105は、認証コード情報メッセージ616Aを送信した後、アクセスポイント102から接続許可メッセージ624Bを受信するか、拒否通知メッセージを受信するか、接続失敗メッセージを受信するのを待つ（S505、S506及びS507）。無線通信装置105は、アクセスポイント102から接続許可メッセージ624Bを受信するか、拒否通知メッセージを受信するか、接続失敗メッセージを受信した場合（S505でYES、S506でYES又はS507でYES）、この処理を終了する。

[0141] （実施の形態2）

次に図面を参照しながら実施の形態2を詳細に説明する。上記実施の形態

1では、ユーザにより、無線通信装置101の操作が行われた後、既にアクセスポイント102と通信を確立している無線通信装置105の操作が行われた。本実施の形態では、ユーザにより、無線通信装置105の操作が行われた後に、無線通信装置101の操作が行われる。

[0142] なお、本実施の形態における通信システム100の構成の概要、並びに、無線通信装置101、アクセスポイント102、サーバ103、及び既にアクセスポイント102と通信を確立している無線通信装置105の構成の概要は、図1から図5を用いて説明した実施の形態1と同じであり、説明は省略する。

[0143] 以下、無線通信装置101、アクセスポイント102、サーバ103及び無線通信装置105の間で行われるアカウント認証シーケンスを、図27及び図28を用いて説明する。

[0144] 図27及び図28は、本実施の形態におけるアカウント認証シーケンスを示すシーケンス図である。なお、以下の図では、既に説明した処理と同様の処理には同一の符号を付しており、重複する説明を省略する場合がある。

[0145] まず、既にアクセスポイント102と接続が確立している無線通信装置105において、ユーザの操作等に応じて参加登録アプリケーションが起動される(S109)。次に、無線通信装置105は、参加要求メッセージ613Aをアクセスポイント102に送信する(S110A)。アクセスポイント102は、参加要求メッセージ613Aを受信した場合、参加要求メッセージ613Aにアクセスポイント情報665を付加することで参加要求メッセージ614Aを生成し、生成された参加要求メッセージ614Aをサーバ103に送信する(S111A)。なお、参加要求メッセージ614Aの構成は、例えば、図15に示す参加確認メッセージ614の構成と同様である。次に、サーバ103は、アクセスポイント102に認証コード要求メッセージ615Aを送信する(S113)。なお、ステップS113～S117の処理は図6で説明した処理と同じであり、説明は省略する。

[0146] サーバ103は、アクセスポイント102から認証コード情報メッセージ

6 1 6 Bを受信した場合、受信した認証コード情報メッセージ6 1 6 Bに含まれる認証コード6 6 6の有効性を確認する（S 1 1 8）、認証コード6 6 6が有効である場合は、サーバ1 0 3は、受信した認証コード6 6 6に紐付けされたIDを持つ無線通信装置1 0 1をアクセスポイント1 0 2への接続要求がある端末として登録する（S 1 0 8 A）。次に、無線通信装置1 0 1において、ユーザの操作等によって無線パラメータ自動設定アプリケーションが起動される（S 1 0 1）。なお、ステップS 1 0 1～S 1 0 6の処理は図6で説明した処理と同じであり、説明は省略する。

[0147] サーバ1 0 3は、アクセスポイント1 0 2から接続要求メッセージ6 1 2を受信した場合、アクセスポイント1 0 2への接続要求がある端末が存在するかを確認する。具体的には、サーバ1 0 3は、参加確認メッセージ6 1 4に含まれるアクセスポイント情報6 6 5で示されるアクセスポイントと、接続要求メッセージ6 1 2に含まれるアクセスポイント情報6 6 4で示されるアクセスポイントとが同一であるか否かを確認する（S 1 1 2）。端末が存在する場合（アクセスポイント情報6 6 5及び6 6 4で示されるアクセスポイントが同一である場合）、サーバ1 0 3は、受信した接続要求メッセージ6 1 2に含まれるID 6 6 1の有効性を確認し（S 1 0 7）、ID 6 6 1が有効である場合は、アクセスポイント1 0 2への接続要求がある端末である無線通信装置1 0 1の無線パラメータ設定のためのPINコードを、接続要求メッセージ6 1 2に含まれていたランダム値6 6 3と、認証コード情報メッセージ6 1 6 Bに含まれていた認証コード6 6 6を用いて生成する（S 1 1 9）。なお、これ以降の処理（S 1 2 0～S 1 3 3）は図7で説明した処理と同じであり、説明は省略する。

[0148] 本実施の形態によれば、実施の形態1の効果に加え、無線通信装置1 0 5が新たに無線ネットワークに参加する無線通信装置を予め登録することで、無線通信装置1 0 1が無線ネットワーク参加要求を行う場合に、速やかに無線パラメータの設定を行うことができる。

[0149] 次に、各装置における処理の流れを説明する。なお、本実施の形態におけ

る無線通信装置１０１が設定情報通知プロトコルを実行する際の処理手順は、図２０を用いて説明した実施の形態１と同じであり、説明は省略する。

[0150] 次に、アクセスポイント１０２が設定情報通信プロトコルを実行する際の処理手順を、図２９、図３０及び図３１を用いて説明する。図２９、図３０及び図３１は本実施の形態におけるアクセスポイント１０２の処理を示すフローチャートである。

[0151] まず、アクセスポイント１０２は、無線通信装置１０５から参加要求メッセージ６１３Ａを受信するのを待つ（Ｓ３０３Ａ）。アクセスポイント１０２は、参加要求メッセージ６１３Ａを受信した場合（Ｓ３０３ＡでＹＥＳ）、当該アクセスポイント１０２を示すアクセスポイント情報６６５を含む参加要求メッセージ６１４Ａをサーバ１０３に送信する（Ｓ３０６Ａ）。

[0152] アクセスポイント１０２は、参加要求メッセージ６１４Ａを送信した後、サーバ１０３から認証コード要求メッセージ６１５Ａを受信するのを待つ（Ｓ３０７）。アクセスポイント１０２は、認証コード要求メッセージ６１５Ａを受信した場合（Ｓ３０７でＹＥＳ）、無線通信装置１０５に認証コード要求メッセージ６１５Ｂを送信する（Ｓ３１０）。なお、ステップＳ３１０～Ｓ３１２の処理は図２２で説明した処理と同じであり、説明は省略する。

[0153] アクセスポイント１０２は、認証コード情報メッセージ６１６Ｂを送信した後、サーバ１０３から拒否通知メッセージを受信するか、無線通信装置１０１から接続要求メッセージ６１１を受信するまで待つ（Ｓ３０４及びＳ３０１）。アクセスポイント１０２は、拒否通知メッセージを受信した場合（Ｓ３０４でＹＥＳ）、無線通信装置１０５に拒否通知メッセージを送信し（Ｓ３０５Ａ）、この処理を終了する。

[0154] 一方、アクセスポイント１０２は、無線通信装置１０１から接続要求メッセージ６１１を受信した場合（Ｓ３０１でＹＥＳ）、接続要求メッセージ６１１に含まれるランダム値６６３及びＩＤ６６１と、当該アクセスポイント１０２を示すアクセスポイント情報６６４とを含む接続要求メッセージ６１２をサーバ１０３に送信する（Ｓ３０２）。なお、以降の処理（Ｓ３１３～

S 3 2 5) は図 2 2 及び図 2 3 で説明した処理と同じであり、説明は省略する。

[0155] 次に、無線通信装置 1 0 1 がインターネット 1 0 4 に接続する際に、認証を行うサーバ 1 0 3 の処理手順を、図 3 2 及び図 3 3 を用いて説明する。図 3 2 及び図 3 3 は本実施の形態におけるサーバ 1 0 3 の処理を示すフローチャートである。

[0156] まず、サーバ 1 0 3 は、アクセスポイント 1 0 2 から参加要求メッセージ 6 1 4 A を受信するのを待つ (S 4 0 4 A)。サーバ 1 0 3 は、アクセスポイント 1 0 2 から参加要求メッセージ 6 1 4 A を受信した場合 (S 4 0 4 A で Y E S)、アクセスポイント 1 0 2 に認証コード要求メッセージ 6 1 5 A を送信する (S 4 0 6)。なお、ステップ S 4 0 6 ~ S 4 0 7 の処理は図 2 4 で説明した説明した処理と同じであり、説明は省略する。

[0157] サーバ 1 0 3 は、認証コード情報メッセージ 6 1 6 B を受信した場合 (S 4 0 7 で Y E S)、認証コード情報メッセージ 6 1 6 B に付加されている認証コード 6 6 6 が、有効な認証コードか否かを確認する (S 4 0 8)。例えば、サーバ 1 0 3 は、記憶部 4 0 8 に保存しているアカウント管理情報を参照し、予め有効な I D として登録された I D に紐付けされた認証コードと受信した認証コード 6 6 6 とが一致すれば、受信した認証コードは有効と判断する。

[0158] ここで、受信した認証コード 6 6 6 が無効であった場合 (S 4 0 8 で N O)、サーバ 1 0 3 は拒否通知メッセージをアクセスポイント 1 0 2 に送信し (S 4 1 6)、この処理を終了する。一方、受信した認証コードが有効であった場合 (S 4 0 8 で Y E S)、サーバ 1 0 3 は認証コード 6 6 6 に紐付けされた無線通信装置の I D を登録する (S 4 0 3 A)。

[0159] サーバ 1 0 3 は、無線通信装置の I D を登録した後、アクセスポイント 1 0 2 から接続要求メッセージ 6 1 2 を受信するのを待つ (S 4 0 1)。サーバ 1 0 3 は、接続要求メッセージ 6 1 2 を受信した場合 (S 4 0 1 で Y E S)、接続要求メッセージ 6 1 2 に含まれるアクセスポイント情報 6 6 4 で示

されるアクセスポイントが、参加要求メッセージ614Aに含まれるアクセスポイント情報665で示されるアクセスポイントと同一か否かを確認する(S405)。

[0160] ここで、アクセスポイントが異なる場合(S405でNO)、サーバ103はアクセスポイント102からの接続要求メッセージ612を受信するまで待つ(S401)。アクセスポイントが同一、すなわち接続要求メッセージ612がアクセスポイント102から送信されていた場合(S405でYES)、サーバ103は接続要求メッセージ612に含まれるID661が有効なIDであるか否かを確認する(S402)。例えば、サーバ103は、記憶部408に保存しているアカウント管理情報を参照し、予め有効なIDとして登録されたIDと受信したID661が一致すれば、受信したID661は有効と判断する。

[0161] ここで、受信したIDが無効である場合(S402でNO)、サーバ103は、拒否通知メッセージをアクセスポイント102に送信し(S416)、この処理を終了する。一方、受信したID661が有効であった場合(S402でYES)、サーバ103は、接続要求メッセージ612に含まれるランダム値663と、認証コード情報メッセージ616Bに含まれる認証コード666とを用いてPINコード667を生成する(S409)。なお、これ以降の処理(S410～S415)は図25で説明した処理と同じであり、説明は省略する。

[0162] 次に、無線通信装置101がインターネット104に接続する際に、認証手続きを行う無線通信装置105の処理手順を、図34を用いて説明する。図34は本実施の形態における無線通信装置105の処理を示すフローチャートである。

[0163] まず、無線通信装置105はアクセスポイント102に参加要求メッセージ613Aを送信する(S501A)。なお、これ以降の処理(S502～S507)は図26で説明した処理と同じであり、説明は省略する。

[0164] (実施の形態3)

次に図面を参照しながら実施の形態 3 を詳細に説明する。本実施の形態では、上記実施の形態 1 の変形例を説明する。本実施の形態では、無線通信装置 101 は、接続要求メッセージ 611 を送信した後に、無線信号を送信する。そして、無線通信装置 105 は、無線通信装置 101 から送信される無線信号を受信した場合に、参加確認メッセージ 613 を送信する。これにより、参加確認メッセージ 613 が誤って送信されることを防止できる。

[0165] なお、本実施の形態における通信システム 100 の構成の概要、並びに、アクセスポイント 102、サーバ 103、及び既にアクセスポイントの通信を確立している無線通信装置 105 の構成の概要は、図 1、図 3、図 4、及び図 5 を用いて説明した実施の形態 1 と同じであり、説明は省略する。

[0166] 図 35 は、本実施の形態における無線通信装置 101 の構成の一例を示すブロック図である。図 35 に示す無線通信装置 101 は、図 2 に示す構成に加え、出力信号強度制御部 209 と、計時部 210 とを備える。出力信号強度制御部 209 は、無線信号の出力強度を制御する。計時部 210 は、タイマ処理及び時刻を管理する。

[0167] 次に、無線通信装置 101、アクセスポイント 102、サーバ 103 及び無線通信装置 105 の間で行われるアカウント認証シーケンスを、図 36 及び図 37 を用いて説明する。

[0168] 図 36 及び図 37 は、本実施の形態におけるアカウント認証シーケンスを示すシーケンス図である。なお、ステップ S101～S108 の処理は図 6 で説明した処理と同じであり、説明は省略する。

[0169] 無線通信装置 101 は、接続要求メッセージ 611 をアクセスポイント 102 に送信した後、無線信号（ビーコン）の送出を開始する（S141）。無線通信装置 101 は、PIN コード生成完了メッセージ 618 を受信するまで、無線信号の送信強度を徐々に大きくする。

[0170] また、既にアクセスポイント 102 と接続が確立している無線通信装置 105 において、ユーザの操作等によって参加登録アプリケーションが起動された後、無線通信装置 105 は、無線通信装置 101 から無線信号を受信す

るのを待つ（S 1 4 3）。無線通信装置 1 0 5 は、無線信号を受信した場合に、参加確認メッセージ 6 1 3 をアクセスポイント 1 0 2 に送信する（S 1 1 0）。なお、これ以降の処理（S 1 1 1～S 1 3 3）は図 6 及び図 7 で説明した処理と同じであり、説明は省略する。

[0171] 以上のように、本実施の形態では、無線通信装置 1 0 1 は、接続要求メッセージ 6 1 1 を第 1 無線アクセスポイント（例えば、アクセスポイント 1 0 2 又は 1 0 2 A）に送信した後に、無線信号を送信する（S 1 4 2）。無線通信装置 1 0 5 は、上記無線信号を受信した場合（S 1 4 3）に、参加確認メッセージ 6 1 3 を第 2 無線アクセスポイント（アクセスポイント 1 0 2）に送信する（S 1 1 0）。

[0172] このように、既にアクセスポイント 1 0 2 との接続を確立している無線通信装置 1 0 5 が新たに無線ネットワークに参加する無線通信装置 1 0 1 から送信される無線信号を受信するまで、参加確認メッセージを送信しない。これにより、実施の形態 1 の効果に加え、新規登録を要求する無線通信装置 1 0 1 と離れた位置にいるユーザから、誤って参加確認メッセージ 6 1 3 が送信されることを防ぐことができる。

[0173] 次に、各装置における処理の流れを説明する。まず、本実施の形態における無線通信装置 1 0 1 が設定情報通知プロトコルを実行する際の処理手順を、図 3 8 を用いて説明する。

[0174] なお、ステップ S 2 0 1 及び S 2 0 2 の処理は図 2 0 で説明した処理と同じであり、説明は省略する。無線通信装置 1 0 1 は、接続要求メッセージ 6 1 1 を送信した後、無線信号（ビーコン）の送信を開始する（S 2 1 0）。

[0175] 無線通信装置 1 0 1 は、無線信号の送信を開始後、アクセスポイント 1 0 2 から P I N コード生成完了メッセージ 6 1 8 を受信したか否かを判断する（S 2 0 3）。無線通信装置 1 0 1 は、P I N コード生成完了メッセージ 6 1 8 を受信していない場合（S 2 0 3 で N O）、アクセスポイント 1 0 2 からプロトコル失敗メッセージを受信したか否かを判断する（S 2 0 4）。無線通信装置 1 0 1 は、プロトコル失敗メッセージを受信した場合（S 2 0 4

でYES)、この処理を終了する。

[0176] 無線通信装置101は、プロトコル失敗メッセージを受信していない場合(S204でNO)、現在の無線信号の送信出力強度が上限値であるか否かを判断する(S211)。送信出力強度が上限値である場合(S211でYES)、無線通信装置101はステップS203に戻る。送信出力強度が上限値でない場合(S211でNO)、無線通信装置101は、無線信号の送信出力強度を変更してから一定時間が経過しているか否かを判断する(S212)。一定時間が経過していない場合(S212でNO)、無線通信装置101はステップS203に戻る。一定時間が経過している場合(S212でYES)、無線通信装置101は無線信号の送信出力強度を上げ(S213)、ステップS203に戻る。

[0177] 一方、無線通信装置101は、アクセスポイント102からPINコード生成完了メッセージ618を受信した場合(S203でYES)、認証コード662とランダム値663とを用いてPINコードを生成する(S205)。なお、ステップS206～S209の処理は図20で説明した処理と同じであり、説明は省略する。

[0178] なお、本実施の形態におけるアクセスポイント102が設定情報通信プロトコルを実行する際の処理手順は図21、図22及び図23で説明した実施の形態1と同じであり、説明は省略する。

[0179] また、本実施の形態における無線通信装置101がインターネット104に接続する際に、認証を行うサーバ103の処理手順は図24及び図25で説明した実施の形態1と同じであり、説明は省略する。

[0180] 次に、無線通信装置101がインターネット104に接続する際に、認証手続きを行う無線通信装置105の処理手順を、図39を用いて説明する。

[0181] 図39は、本実施の形態における無線通信装置105の処理を示すフローチャートである。なお、無線通信装置105とアクセスポイント102には既に共通の暗号鍵及び認証鍵等が設定されている。そのため、無線通信装置105はアクセスポイント102の無線ネットワークにおいて暗号及び認証

を用いた通常のデータ通信を行うことができる。

[0182] まず、無線通信装置 105 は、無線通信装置 101 から無線信号を受信するまで待つ (S510)。無線通信装置 105 は、無線通信装置 101 から無線信号を受信した場合 (S510 で YES)、アクセスポイント 102 に参加確認メッセージ 613 を送信する (S501)。なお、これ以降の処理 (S502 ~ S507) は図 26 で説明した処理と同じであり、説明は省略する。

[0183] 以上、実施の形態 1 ~ 3 で説明したように、本実施の形態に係るサーバ 103 は、第 1 無線通信装置 (無線通信装置 101) と無線アクセスポイント (アクセスポイント 102) との通信を確立するための無線接続認証を行うサーバ 103 であって、図 40 に示す処理を行う。

[0184] まず、サーバ 103 に含まれる第 1 受信部は、第 1 無線通信装置 (無線通信装置 101) から、第 1 無線アクセスポイント (例えば、アクセスポイント 102 又は 102A) を示す第 1 アクセスポイント情報 (アクセスポイント情報 664) を受信する (S601)。具体的には、第 1 受信部は、第 1 アクセスポイント情報 (アクセスポイント情報 664) を含む第 2 メッセージ (接続要求メッセージ 612) を受信する。また、第 2 メッセージ (接続要求メッセージ 612) は、第 1 無線通信装置 (無線通信装置 101) から送信された第 1 メッセージ (接続要求メッセージ 611) に従い第 1 無線アクセスポイント (例えば、アクセスポイント 102 又は 102A) が送信したメッセージである。

[0185] 次に、サーバ 103 に含まれる第 2 受信部は、第 1 無線アクセスポイント (アクセスポイント 102 又は 102A) と同一又は異なる第 2 無線アクセスポイント (アクセスポイント 102) と既に通信が確立している第 2 無線通信装置 (無線通信装置 105) から、第 2 無線アクセスポイント (アクセスポイント 102) を示す第 2 アクセスポイント情報 (アクセスポイント情報 665) を受信する (S602)。具体的には、第 2 受信部は、第 2 アクセスポイント情報を含む第 4 メッセージ (参加確認メッセージ 614 又は参

加要求メッセージ 614A)を受信する。また、第4メッセージ(参加確認メッセージ 614又は参加要求メッセージ 614A)は、第2無線通信装置(無線通信装置 105)から送信された第3メッセージ(参加確認メッセージ 613又は参加要求メッセージ 613A)に従い、第2無線アクセスポイント(アクセスポイント 102)が送信したメッセージである。

[0186] なお、実施の形態1で説明したように、ステップS601の後にステップS602が行われてもよいし、実施の形態2で説明したように、ステップS602の後にステップS601が行われてもよい。

[0187] 次に、サーバ103に含まれる決定部は、第1アクセスポイント情報で示される第1無線アクセスポイントと、第2アクセスポイント情報で示される第2無線アクセスポイントとを比較する(S603)。そして、決定部は、第1無線アクセスポイントと第2無線アクセスポイントとが同一の無線アクセスポイントである場合(S603でYES)、当該同一の無線アクセスポイントを、第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する(S604)。

[0188] 次に、サーバ103に含まれる認証処理部は、上記接続先アクセスポイントと第1無線通信装置との無線接続認証を行うための処理を行う(S605)。例えば、認証処理部は、図24及び図25に示すステップS406～S416の処理を行う。

[0189] なお、上記第1受信部及び第2受信部は、例えば、図4に示す通信部401及び通信制御部402等により実現される。また、決定部は、例えば、図4に示す判断部407等により実現される。認証処理部は、例えば、図4に示す認証処理部405により実現される。

[0190] 以上により、サーバ103は、第1無線通信装置(無線通信装置 101)が通信可能な複数の無線アクセスポイント(例えば、アクセスポイント 102及び102A)が存在する場合であっても、第2無線通信装置(無線通信装置 105)から送信された第3メッセージに従い接続対象の無線アクセスポイント(アクセスポイント 102)が送信した第2アクセスポイント情報

を用いて、第1無線通信装置の接続対象の無線アクセスポイントを決定できる。また、ユーザは、第1無線通信装置に第1メッセージを送信させる操作と、第2無線通信装置に第3メッセージを送信させる操作とのみを行えばよい。このように、ユーザは、簡単な操作で無線接続認証を行うことができる。

[0191] また、サーバ103は、第2無線通信装置から第1無線通信装置に固有の第1コード（認証コード666）を受信する。サーバ103は、第1コードを用いて、第1無線通信装置と接続先アクセスポイントとの無線接続認証に用いられる第2コード（PINコード667）を生成する。サーバ103は、第2コードを接続先アクセスポイントに送信する。これにより、意図しない機器が誤って認証されることを防止できる。

[0192] また、第1メッセージ及び第2メッセージの各々は、さらに、第3コード（ランダム値663）を含む。サーバ103は、第1コード及び第3コードを用いて第2コードを生成する。なお、第3コードは、ランダム値663に限定されず、任意のコードであってもよい。これにより、意図しない機器が誤って認証されることを防止できる。

[0193] 以上、本発明の実施の形態に係る通信システムについて説明したが、本発明は、この実施の形態に限定されるものではない。

[0194] 例えば、上記実施の形態では、IEEE802.11の無線LANを例に説明したが、ワイヤレスUSB、又はBluetooth（登録商標）等の他の通信方式に本実施の形態を適用しても良い。

[0195] また、上記実施の形態では、本実施の形態に係る特徴的な処理を行う通信システムについて説明したが、本発明は、上記通信システムに含まれる、無線通信装置、アクセスポイント、又は、サーバとして実現されてもよい。また、本発明は、通信システム、無線通信装置、アクセスポイント、又は、サーバにおける無線接続認証方法として実現されてもよい。

[0196] また、上記各実施の形態において、各構成要素は、専用のハードウェアで構成されるか、各構成要素に適したソフトウェアプログラムを実行すること

によって実現されてもよい。各構成要素は、CPU又はプロセッサなどのプログラム実行部が、ハードディスク又は半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。ここで、上記各実施の形態のサーバなどを実現するソフトウェアは、次のようなプログラムである。

[0197] すなわち、このプログラムは、コンピュータに、第1無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバにおける無線接続認証方法を実行させるプログラムである。このプログラムは、コンピュータに、前記第1無線通信装置から送信された第1メッセージに従い第1無線アクセスポイントが送信した、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージを受信する第1受信ステップと、前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと既に通信が確立している第2無線通信装置から送信された第3メッセージに従い、前記第2無線アクセスポイントが送信した、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信ステップと、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理ステップとを実行させる。

[0198] さらに、本発明は上記プログラムであってもよいし、上記プログラムが記録された非一時的なコンピュータ読み取り可能な記録媒体であってもよい。また、上記プログラムは、インターネット等の伝送媒体を介して流通させることができるのは言うまでもない。

[0199] また、ブロック図における機能ブロックの分割は一例であり、複数の機能

ブロックを一つの機能ブロックとして実現したり、一つの機能ブロックを複数に分割したり、一部の機能を他の機能ブロックに移してもよい。また、類似する機能を有する複数の機能ブロックの機能を単一のハードウェア又はソフトウェアが並列又は時分割に処理してもよい。

[0200] また、上記処理に含まれるステップが実行される順序は、本発明を具体的に説明するために例示するためのものであり、同様の結果が得られる範囲において上記以外の順序であってもよい。また、上記ステップの一部が、他のステップと同時（並列）に実行されてもよい。

[0201] 以上、一つまたは複数の態様に係る通信システムについて、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

産業上の利用可能性

[0202] 本発明は、無線LANの簡易接続方法等として有用である。また、本発明は、公衆無線LANの接続等の用途にも応用できる。

符号の説明

[0203] 100 通信システム
 101、105 無線通信装置
 102、102A アクセスポイント
 103 サーバ
 104 インターネット
 201、301、401、501 通信部
 202、302、402、502 通信制御部
 203、303、403、503 装置制御部
 204、304、404、504 インターフェース処理部
 205、305、505 無線パラメータ設定処理部
 206、406 符号演算部

207、306、407、506 判断部
208、307、408、507 記憶部
209 出力信号強度制御部
210 計時部
405 認証処理部
508 表示部
611、612 接続要求メッセージ
613、614 参加確認メッセージ
613A、614A 参加要求メッセージ
615A、615B 認証コード要求メッセージ
616A、616B 認証コード情報メッセージ
617 PINコード情報メッセージ
618 PINコード生成完了メッセージ
619 プロトコル開始要求メッセージ
620 プロトコル開始メッセージ
621 プロトコルメッセージ
622 プロトコル終了メッセージ
623 WPS成功メッセージ
624A、624B 接続許可メッセージ
651 操作ボタン
652 操作メニュー
653 入力メニュー
654 メッセージ
661、671 ID
662、666 認証コード
663、672 ランダム値
664、665、673 アクセスポイント情報
667 PINコード

請求の範囲

[請求項1]

第1無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバにおける無線接続認証方法であって、

前記第1無線通信装置から送信された第1メッセージに従い第1無線アクセスポイントが送信した、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージを受信する第1受信ステップと、

前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと既に通信が確立している第2無線通信装置から送信された第3メッセージに従い、前記第2無線アクセスポイントが送信した、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信ステップと、

前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、

前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理ステップとを含む

無線接続認証方法。

[請求項2]

前記無線接続認証方法は、さらに、

前記第2無線通信装置から前記第1無線通信装置に固有の第1コードを受信する第3受信ステップを含み、

前記認証処理ステップは、

前記第1コードを用いて、前記第1無線通信装置と前記接続先アクセスポイントとの無線接続認証に用いられる第2コードを生成する第

2コード生成ステップと、

前記第2コードを前記接続先アクセスポイントに送信する送信ステップとを含む

請求項1記載の無線接続認証方法。

[請求項3]

前記第1メッセージ及び前記第2メッセージの各々は、さらに、第3コードを含み、

前記第2コード生成ステップでは、前記第1コード及び前記第3コードを用いて前記第2コードを生成する

請求項2記載の無線接続認証方法。

[請求項4]

第1無線通信装置と無線アクセスポイントとの無線接続認証を行う無線接続認証方法であって、

前記第1無線通信装置が、第1メッセージを第1無線アクセスポイントに送信する第1メッセージ送信ステップと、

前記第1メッセージを受信した前記第1無線アクセスポイントが、前記第1無線アクセスポイントを示す第1アクセスポイント情報を含む第2メッセージをサーバに送信する第2メッセージ送信ステップと、

前記第1無線アクセスポイントと同一又は異なる第2無線アクセスポイントと無線接続認証が既に完了している第2無線通信装置が、第3メッセージを前記第2無線アクセスポイントに送信する第3メッセージ送信ステップと、

前記第3メッセージを受信した前記第2無線アクセスポイントが、前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを前記サーバに送信する第4メッセージ送信ステップと、

前記サーバが、前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポ

イントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定ステップと、

前記接続先アクセスポイントと前記第1無線通信装置とが無線接続認証を行う認証ステップとを含む

無線接続認証方法。

[請求項5]

前記無線接続認証方法は、さらに、

ユーザ操作に応じて、前記第2無線通信装置が前記第1無線通信装置に固有の第1コードを取得する取得ステップと、

前記第2無線通信装置が、前記第1コードを前記サーバに送信する第1コード送信ステップと、

前記サーバが、前記第1コードを用いて、前記第1無線通信装置と前記接続先アクセスポイントとの無線接続認証に用いられる第2コードを生成する第2コード生成ステップと、

前記サーバが、前記第2コードを前記接続先アクセスポイントに送信する送信ステップと、

前記第1無線通信装置が、前記第1コードと同一の第3コードを用いて第4コードを生成する第4コード生成ステップとを含み、

前記認証ステップでは、前記第1無線通信装置及び前記接続先アクセスポイントが、前記第2コードと前記第4コードとが同一であるか否かに応じて、前記第1無線通信装置及び前記接続先アクセスポイントとの無線接続認証を行う

請求項4記載の無線接続認証方法。

[請求項6]

前記無線接続認証方法は、さらに、

前記第1無線通信装置が第5コードを生成する生成ステップを含み、

前記第1メッセージ及び前記第2メッセージの各々は、さらに、前

記第 5 コードを含み、

前記第 2 コード生成ステップでは、前記第 1 コード及び前記第 5 コードを用いて前記第 2 コードを生成し、

前記第 4 コード生成ステップでは、前記第 3 コード及び前記第 5 コードを用いて前記第 4 コードを生成する

請求項 5 記載の無線接続認証方法。

[請求項7] 前記第 3 メッセージ送信ステップは、前記第 1 メッセージ送信ステップの後に行われる

請求項 4 ～ 6 のいずれか 1 項に記載の無線接続認証方法。

[請求項8] 前記無線接続認証方法は、さらに、
前記第 1 メッセージ送信ステップの後に、前記第 1 無線通信装置が、無線信号を送信する無線信号送信ステップを含み、

前記第 3 メッセージ送信ステップでは、前記第 2 無線通信装置が前記無線信号を受信した場合に、前記第 2 無線通信装置が、前記第 3 メッセージを前記第 2 無線アクセスポイントに送信する

請求項 7 記載の無線接続認証方法。

[請求項9] 前記第 1 メッセージ送信ステップは、前記第 3 メッセージ送信ステップの後に行われる

請求項 4 ～ 6 のいずれか 1 項に記載の無線接続認証方法。

[請求項10] 第 1 無線通信装置と無線アクセスポイントとの通信を確立するための無線接続認証を行うサーバであって、

前記第 1 無線通信装置から送信された第 1 メッセージに従い第 1 無線アクセスポイントが送信した、前記第 1 無線アクセスポイントを示す第 1 アクセスポイント情報を含む第 2 メッセージを受信する第 1 受信部と、

前記第 1 無線アクセスポイントと同一又は異なる第 2 無線アクセスポイントと既に通信が確立している第 2 無線通信装置から送信された第 3 メッセージに従い、前記第 2 無線アクセスポイントが送信した、

前記第2無線アクセスポイントを示す第2アクセスポイント情報を含む第4メッセージを受信する第2受信部と、

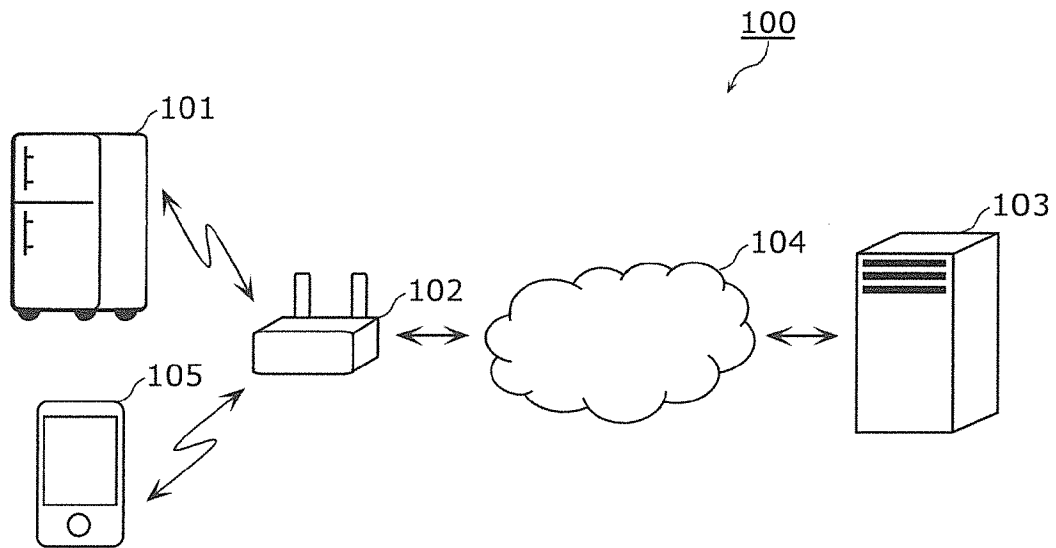
前記第1アクセスポイント情報で示される前記第1無線アクセスポイントと、前記第2アクセスポイント情報で示される前記第2無線アクセスポイントとを比較し、前記第1無線アクセスポイントと前記第2無線アクセスポイントとが同一の無線アクセスポイントである場合、当該同一の無線アクセスポイントを、前記第1無線通信装置の接続先の無線アクセスポイントである接続先アクセスポイントに決定する決定部と、

前記接続先アクセスポイントと前記第1無線通信装置との無線接続認証を行うための処理を行う認証処理部とを備える

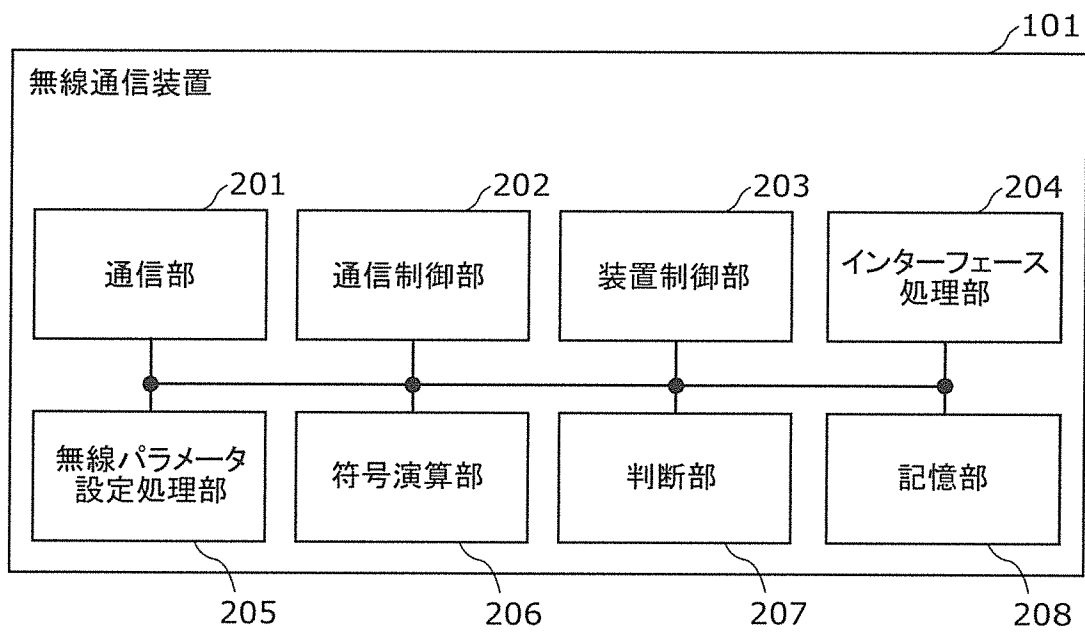
サーバ。

[請求項11] 請求項1記載の無線接続認証方法をコンピュータに実行させるための
プログラム。

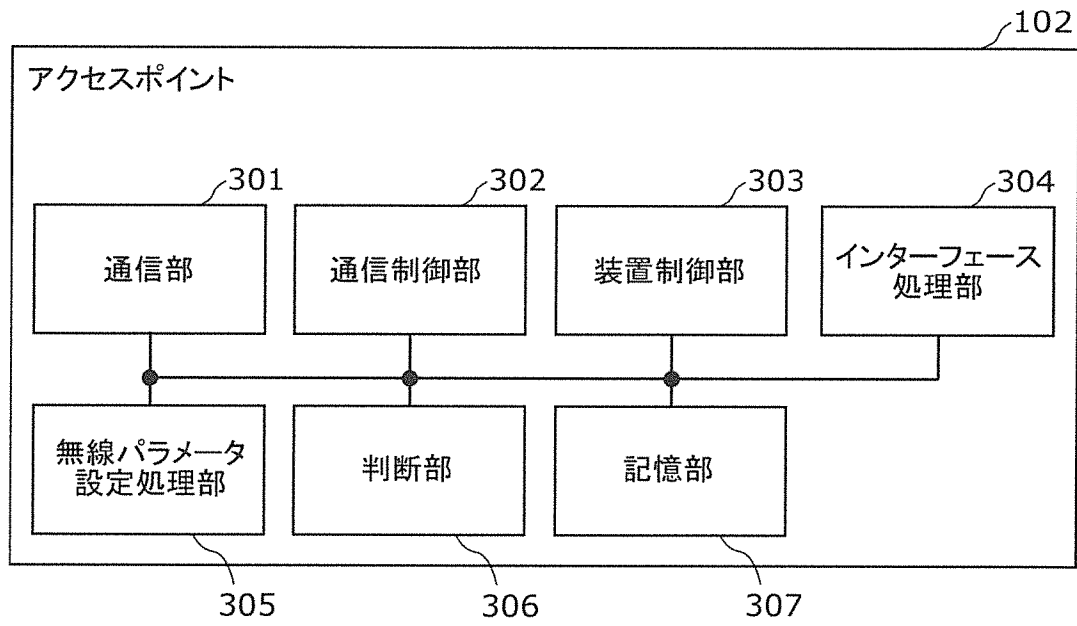
[図1]



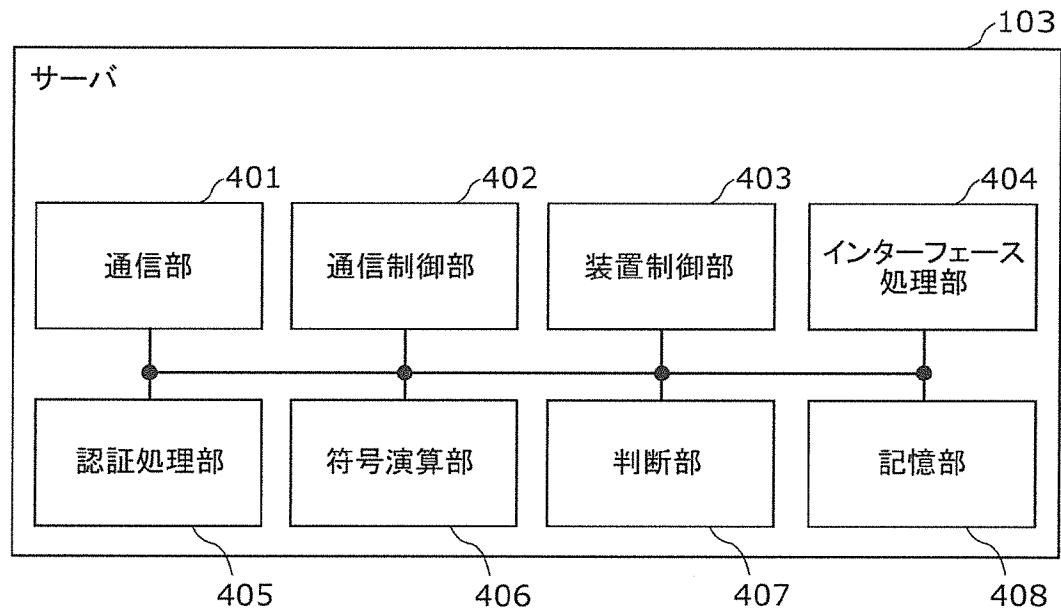
[図2]



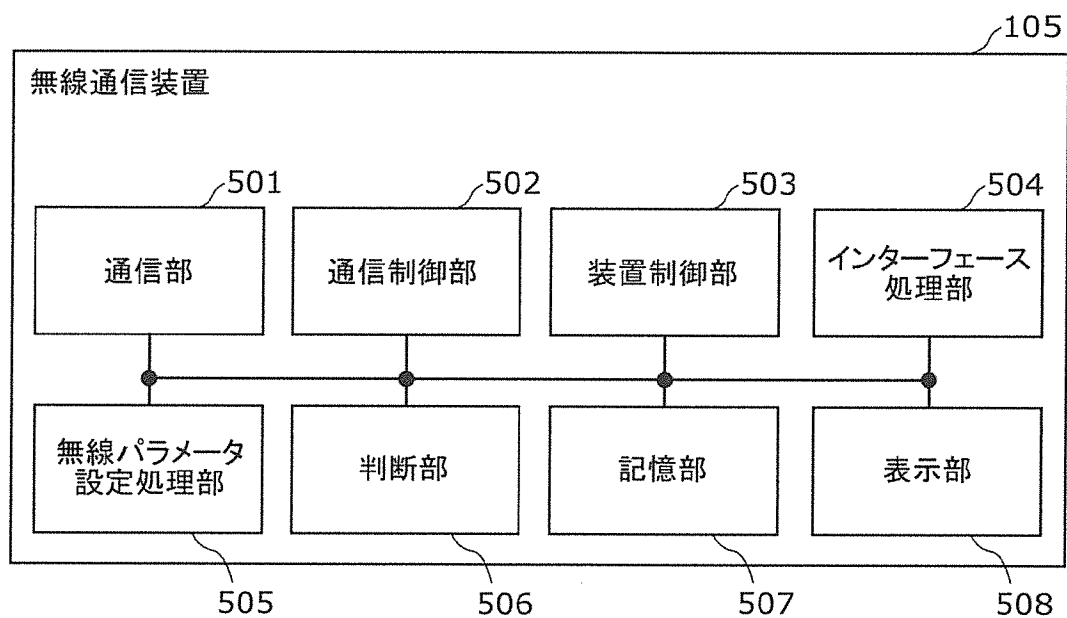
[図3]



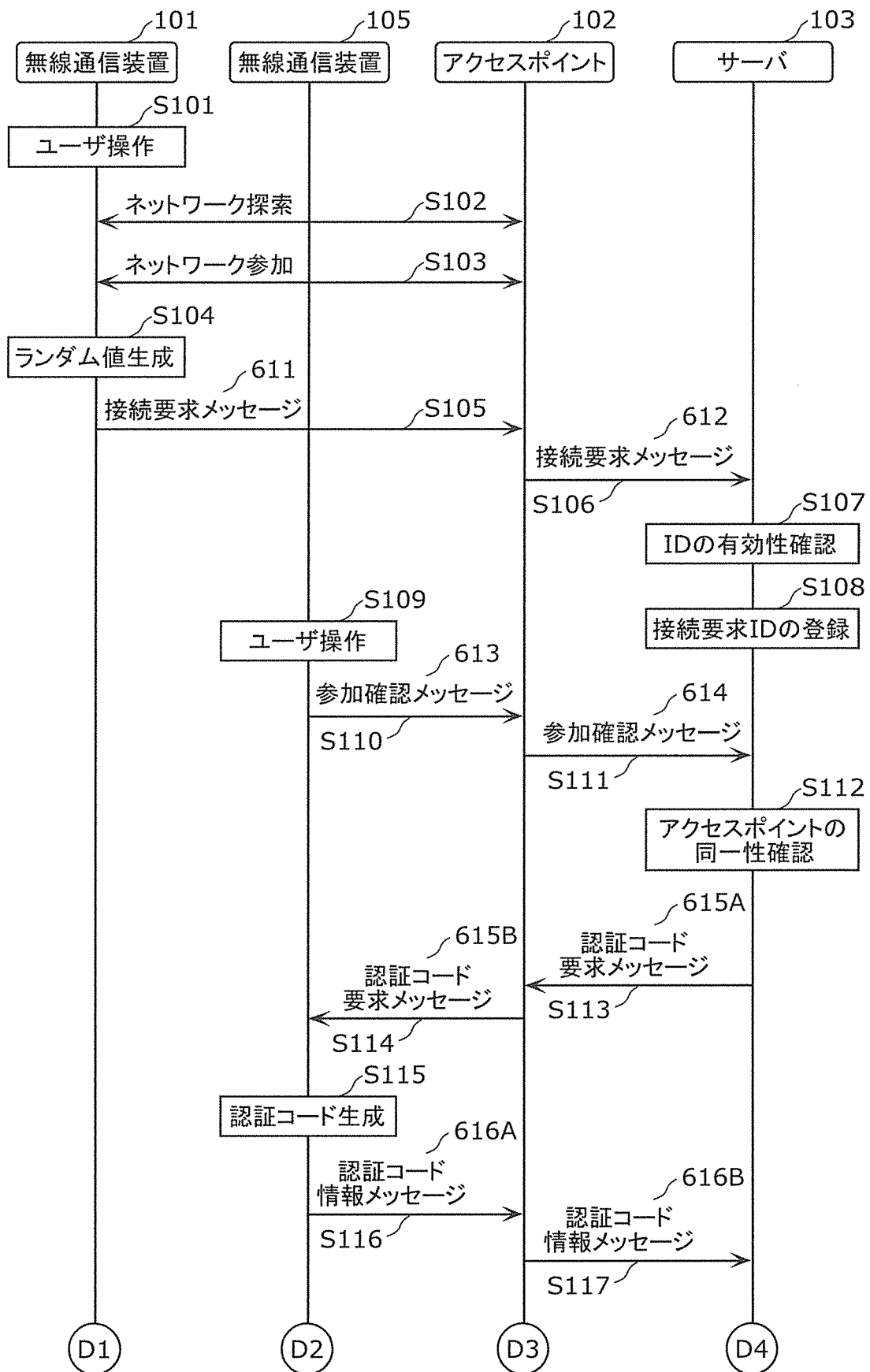
[図4]



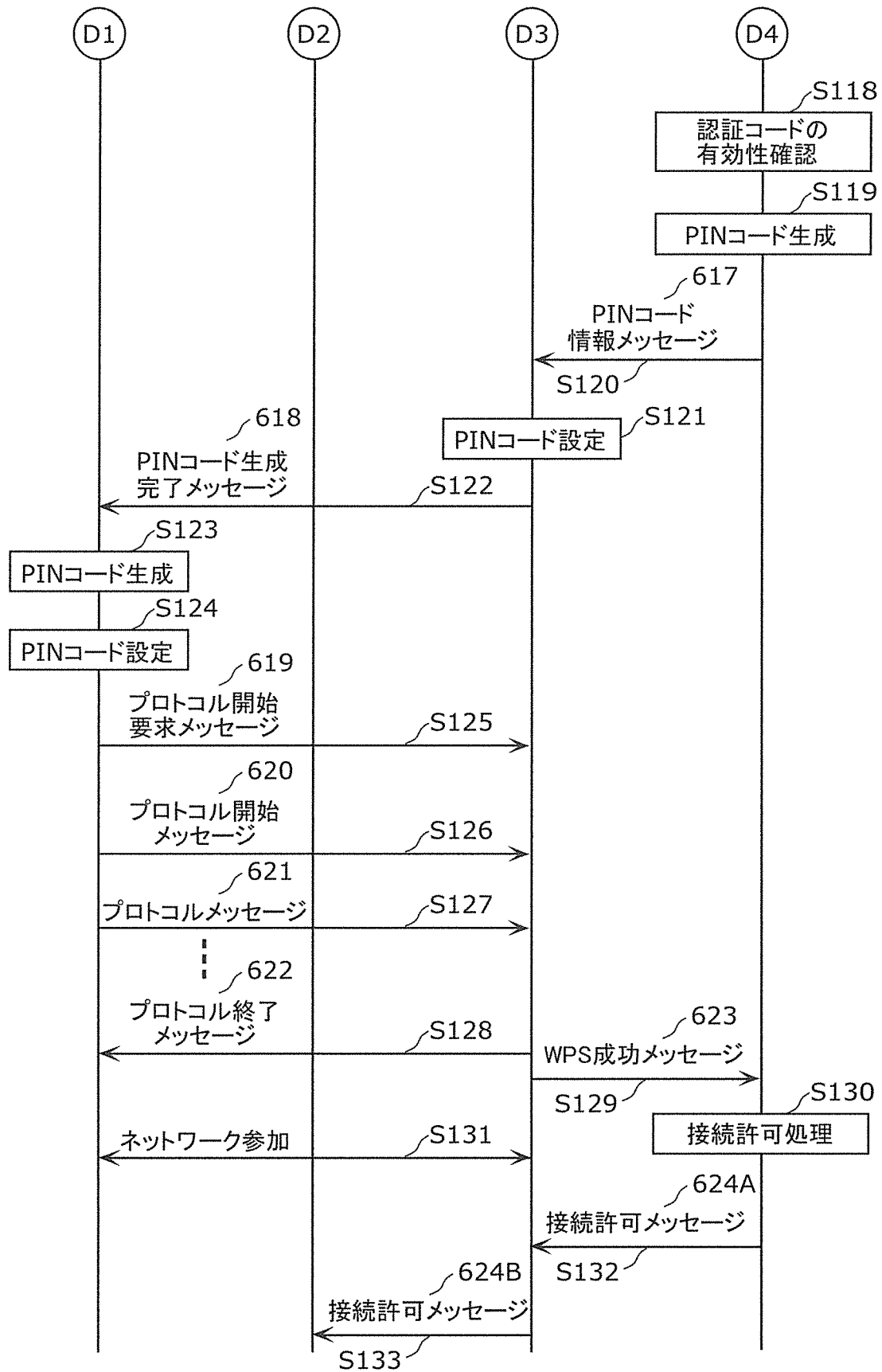
[図5]



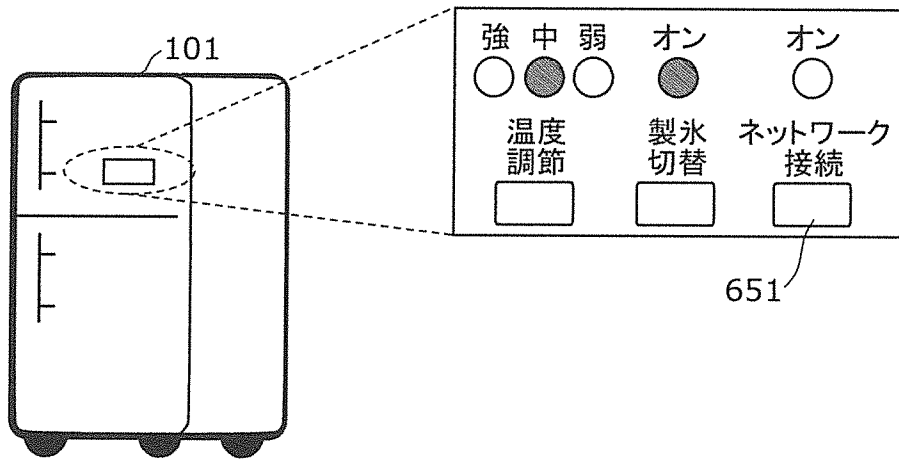
[図6]



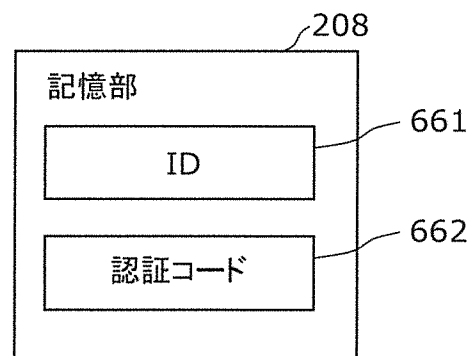
[図7]



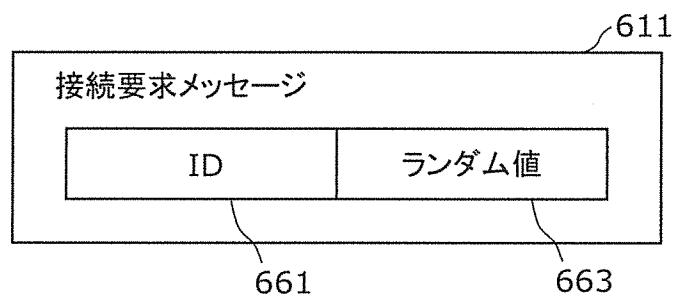
[図8]



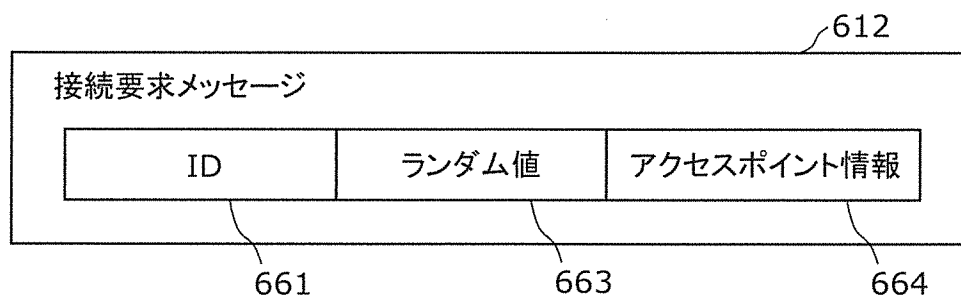
[図9]



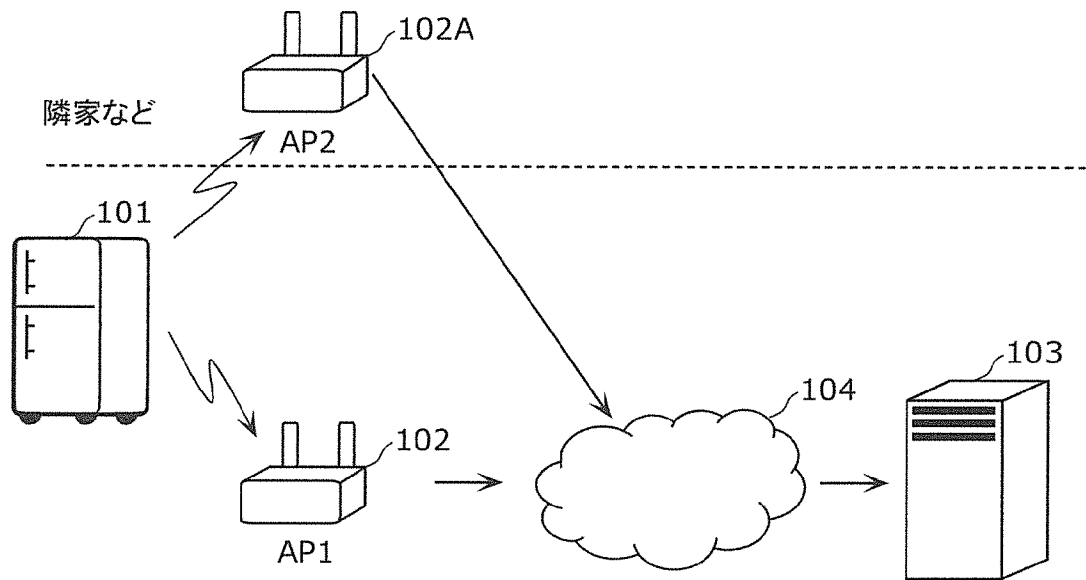
[図10]



[図11]



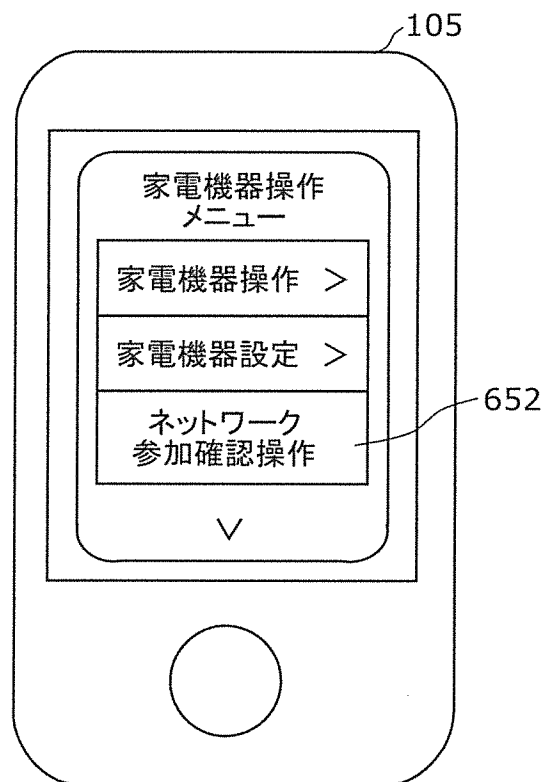
[図12]



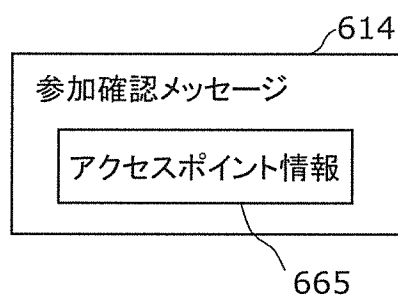
[図13]

ID	ランダム値	アクセスポイント情報
0001	12345678	AP1
0001	12345678	AP2

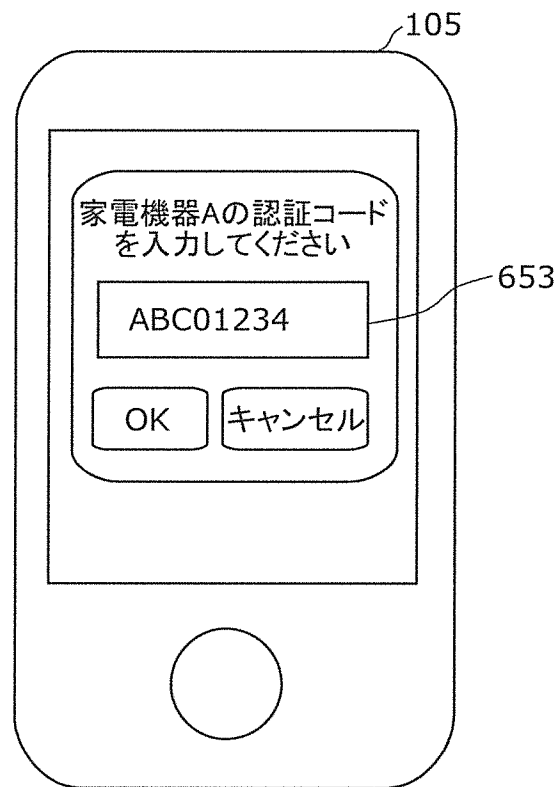
[図14]



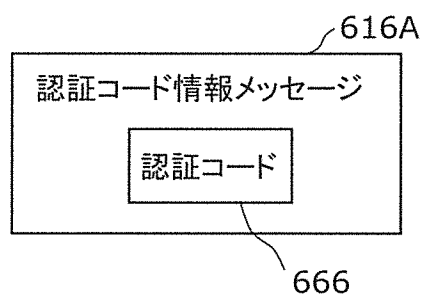
[図15]



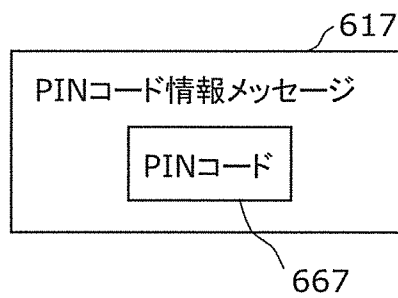
[図16]



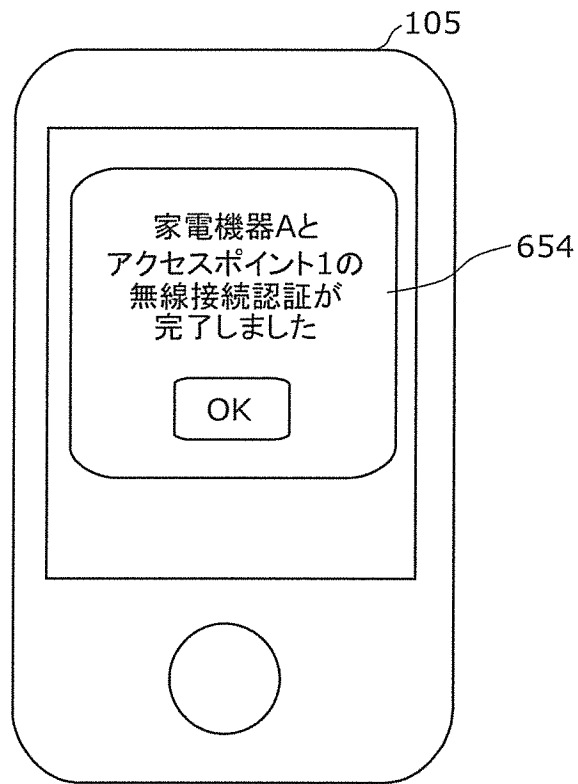
[図17]



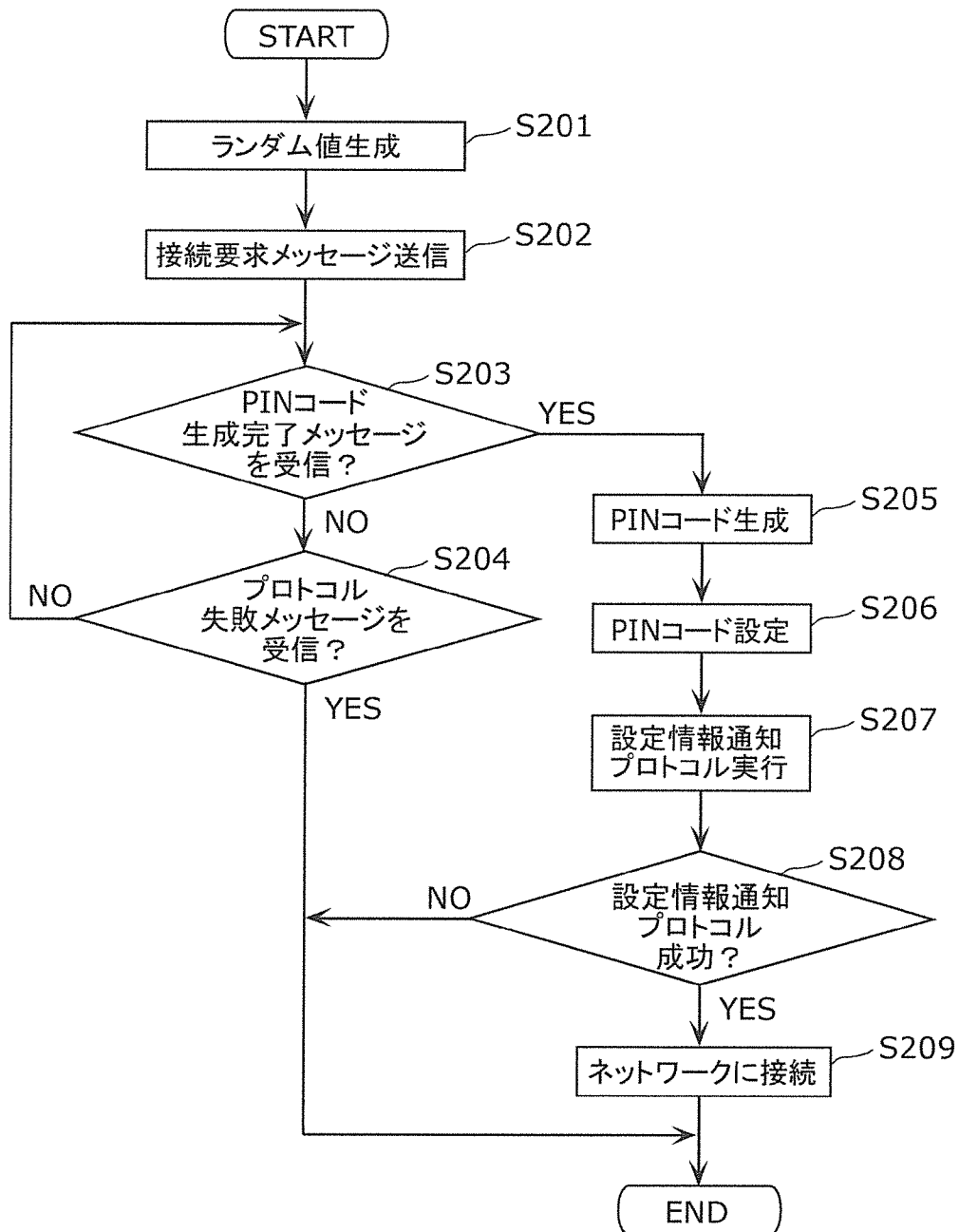
[図18]



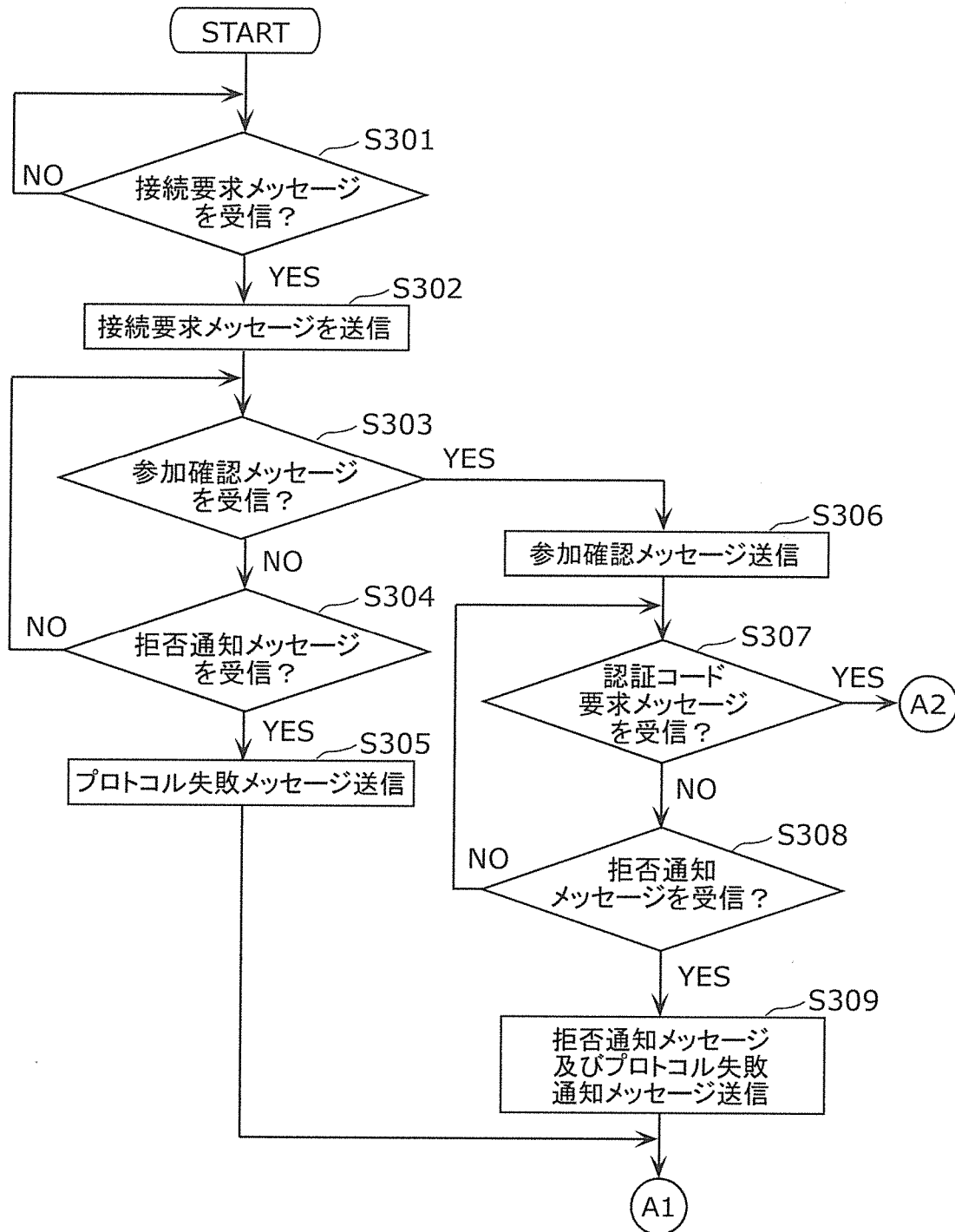
[図19]



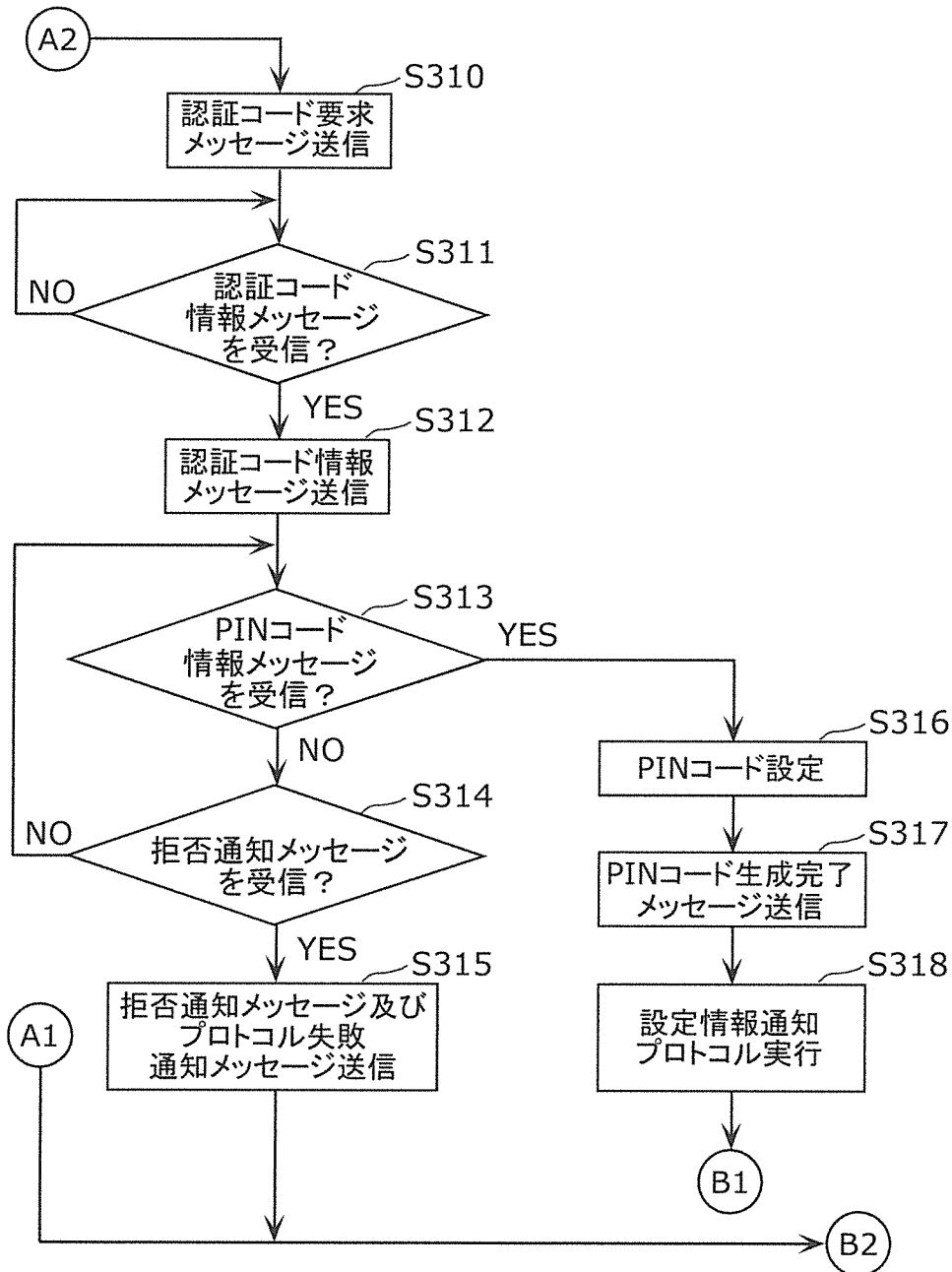
[図20]



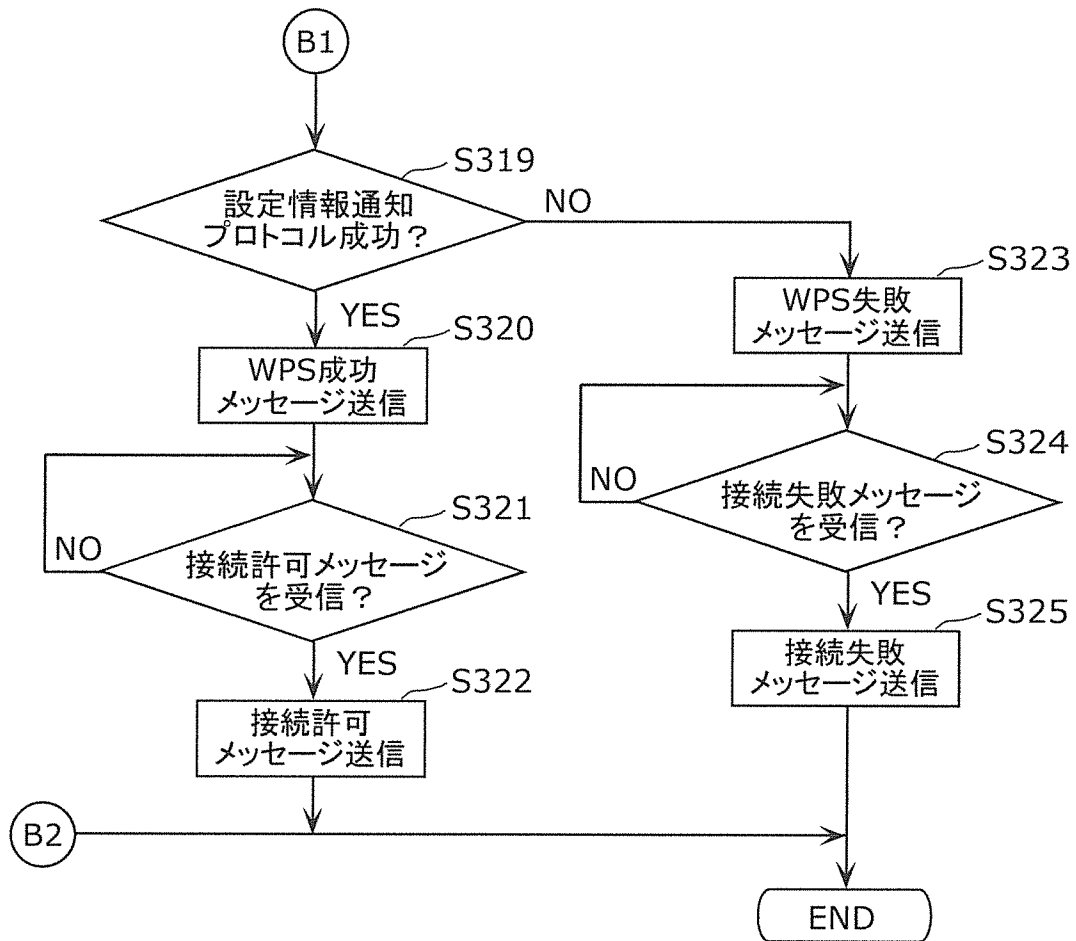
[図21]



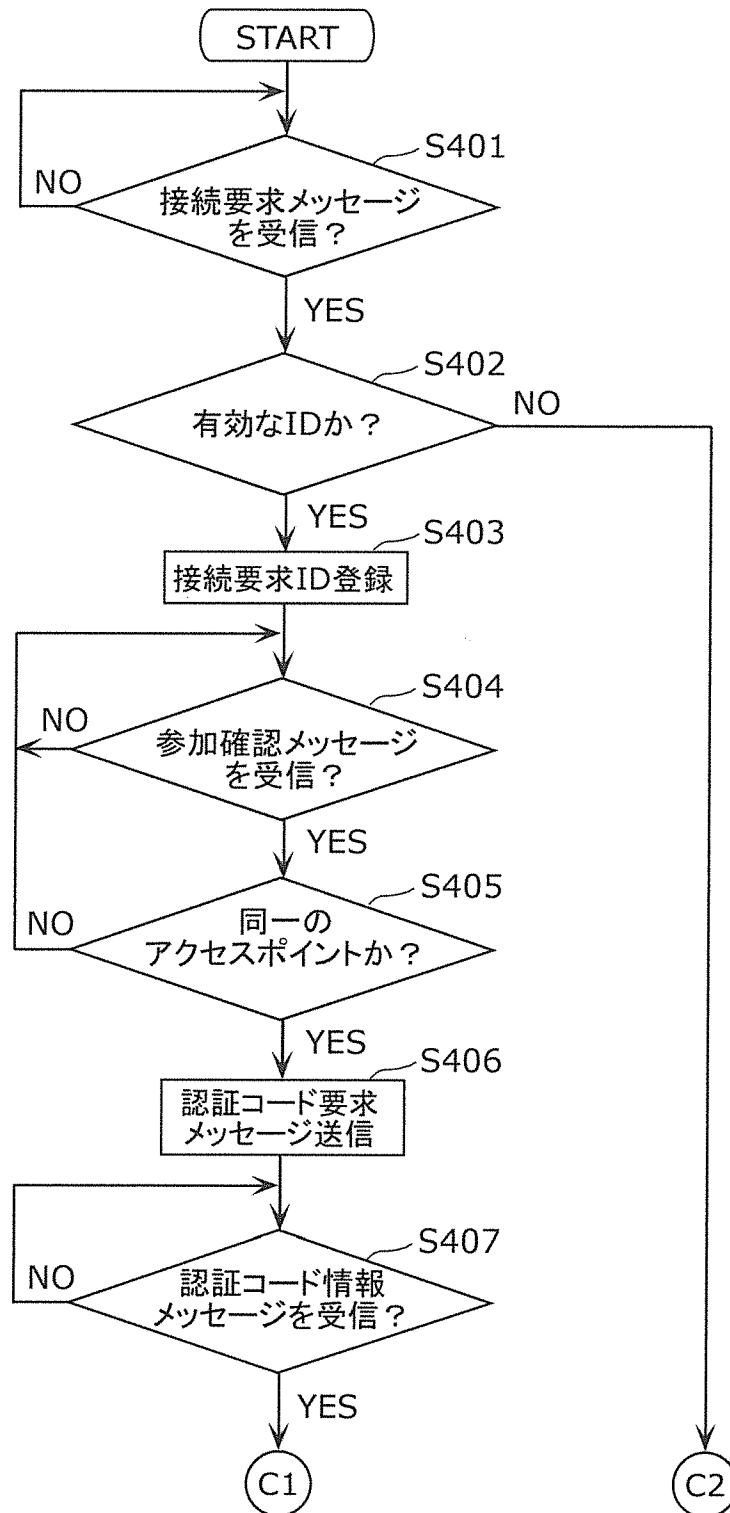
[図22]



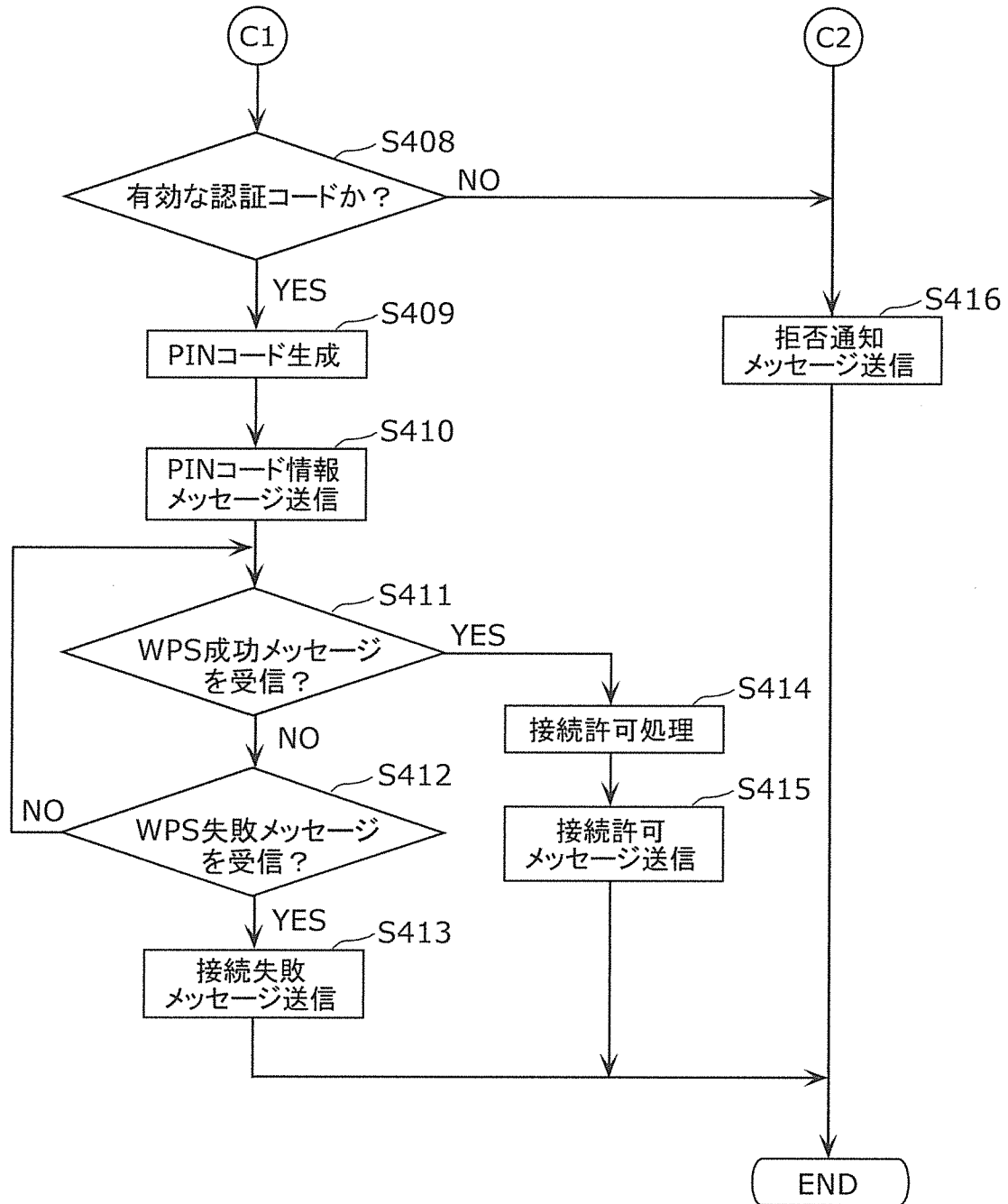
[図23]



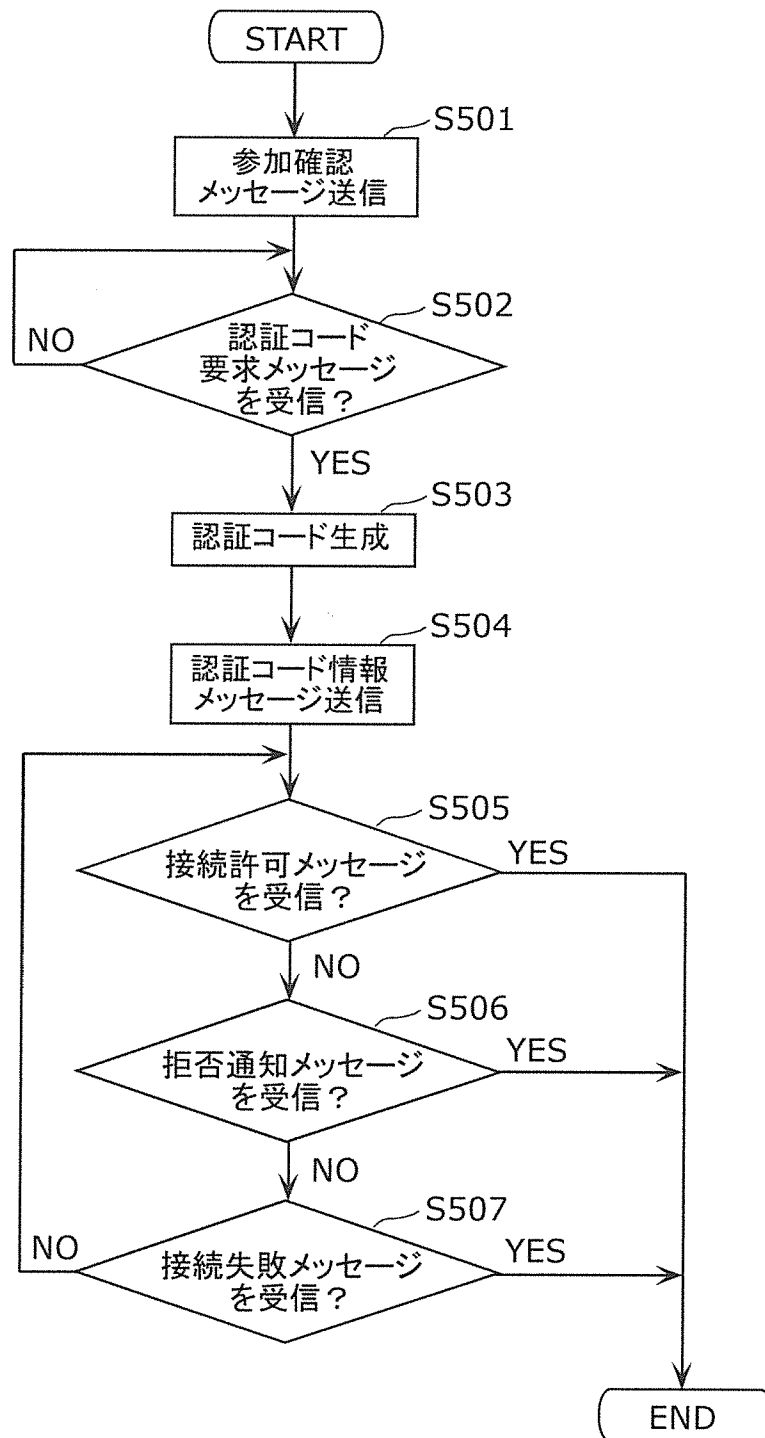
[図24]



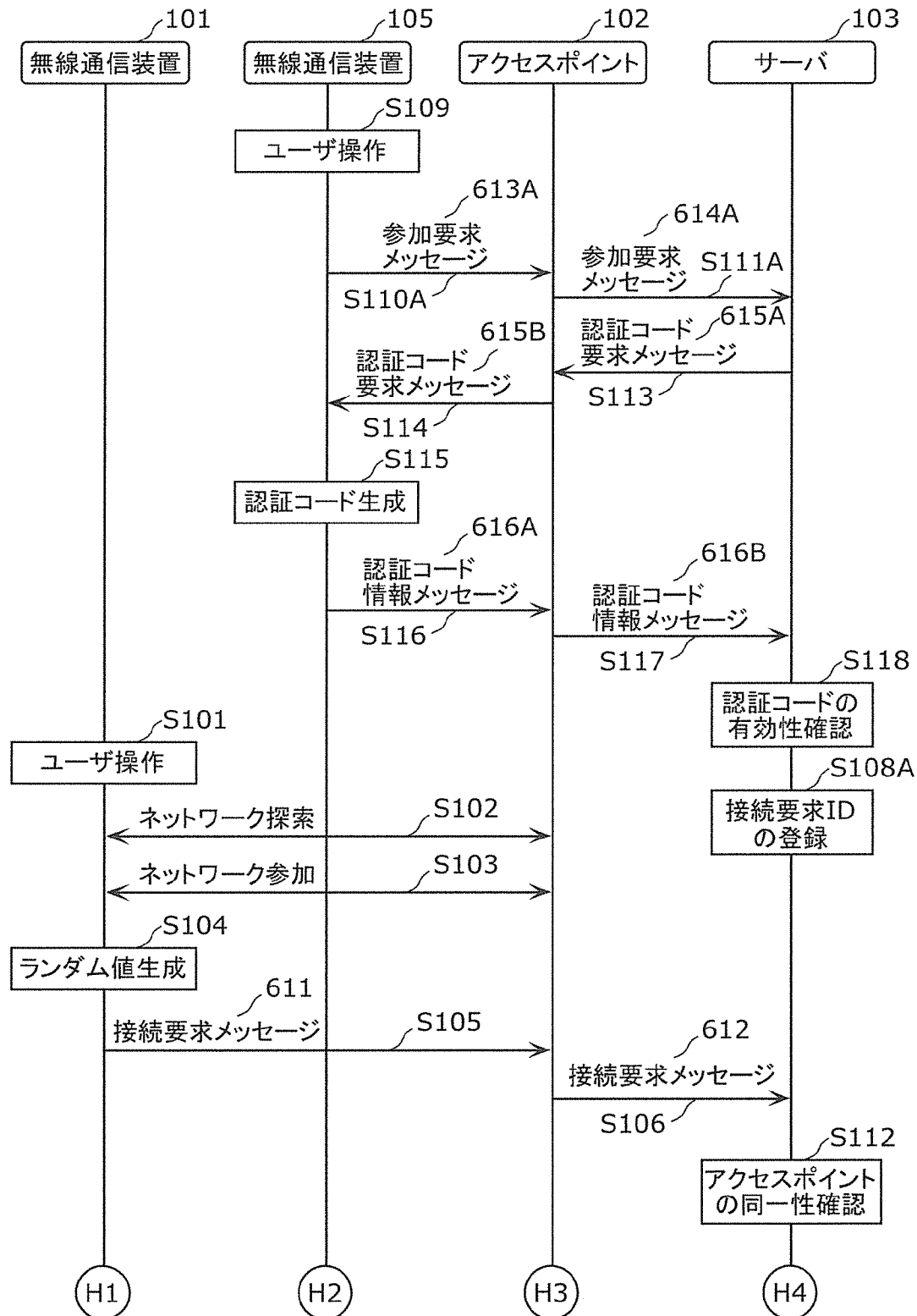
[図25]



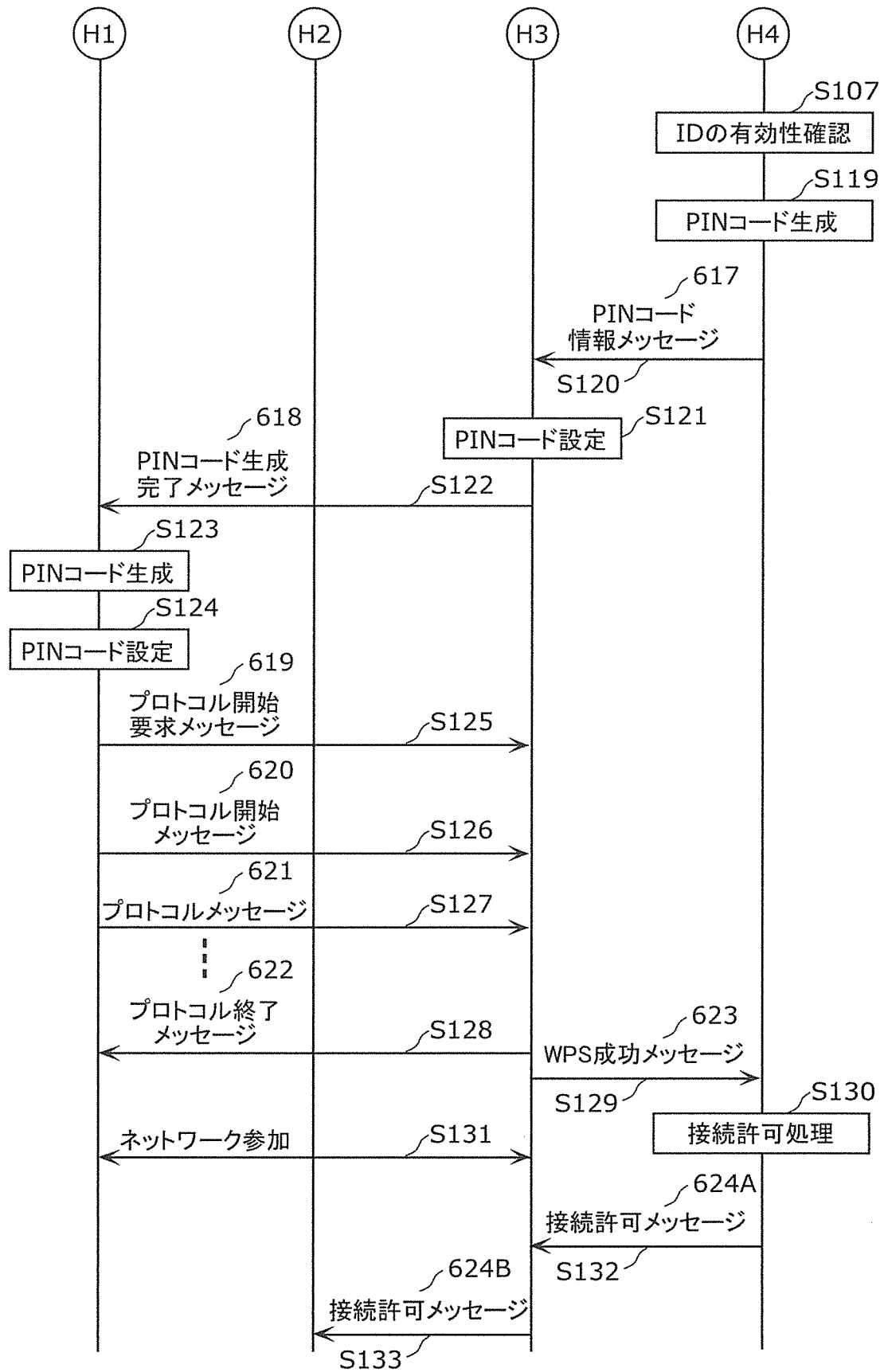
[図26]



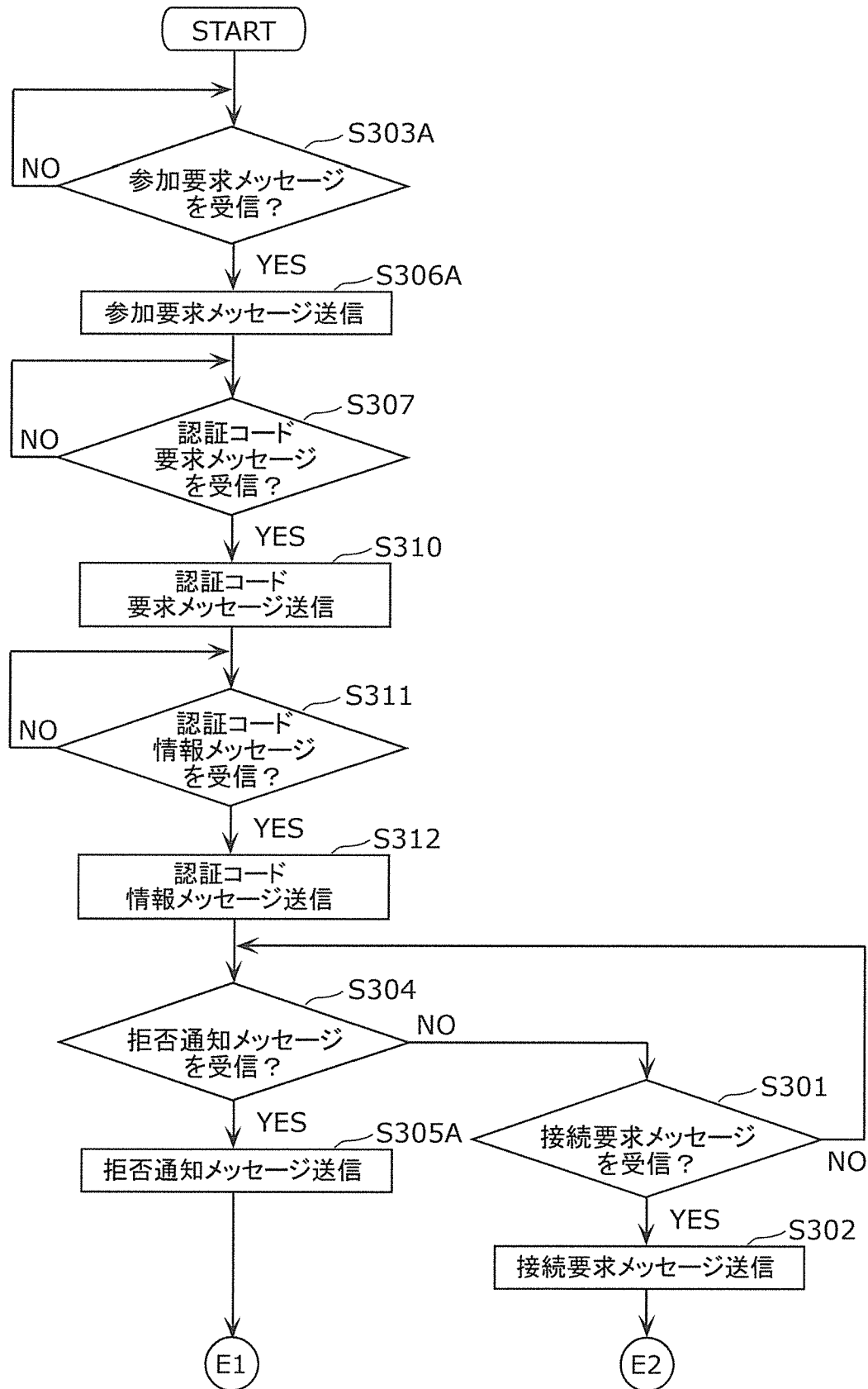
[図27]



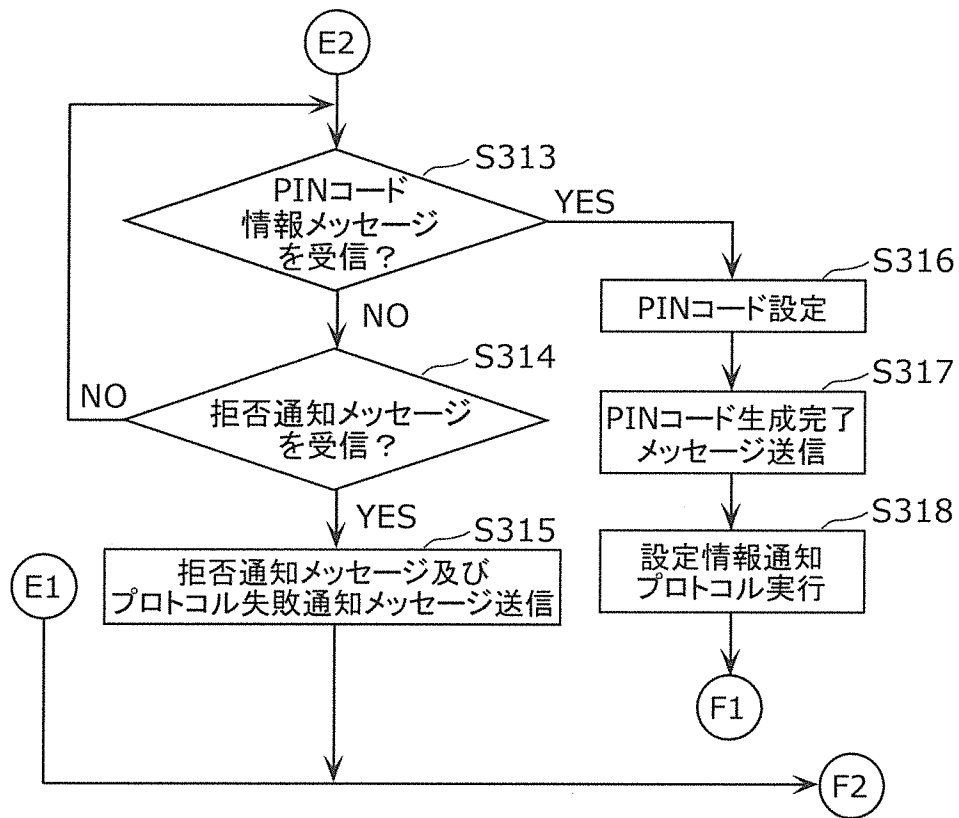
[図28]



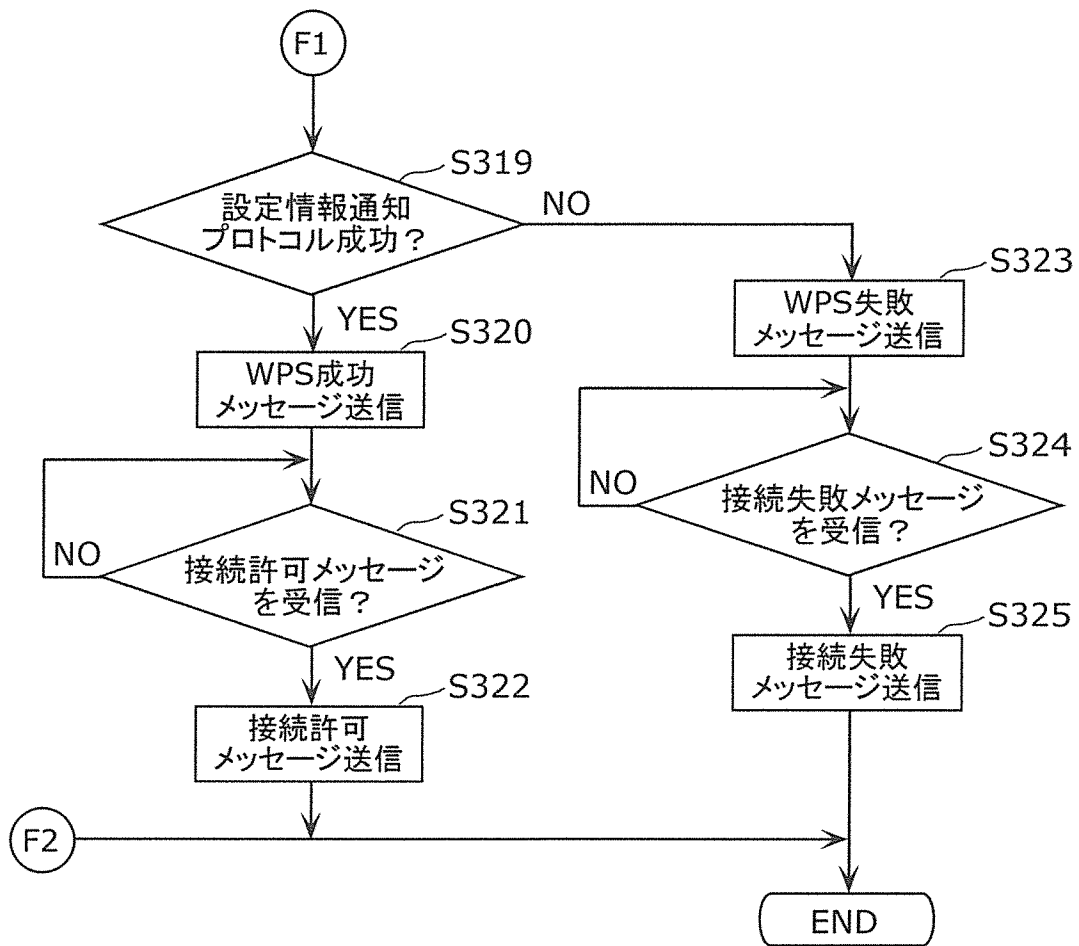
[図29]



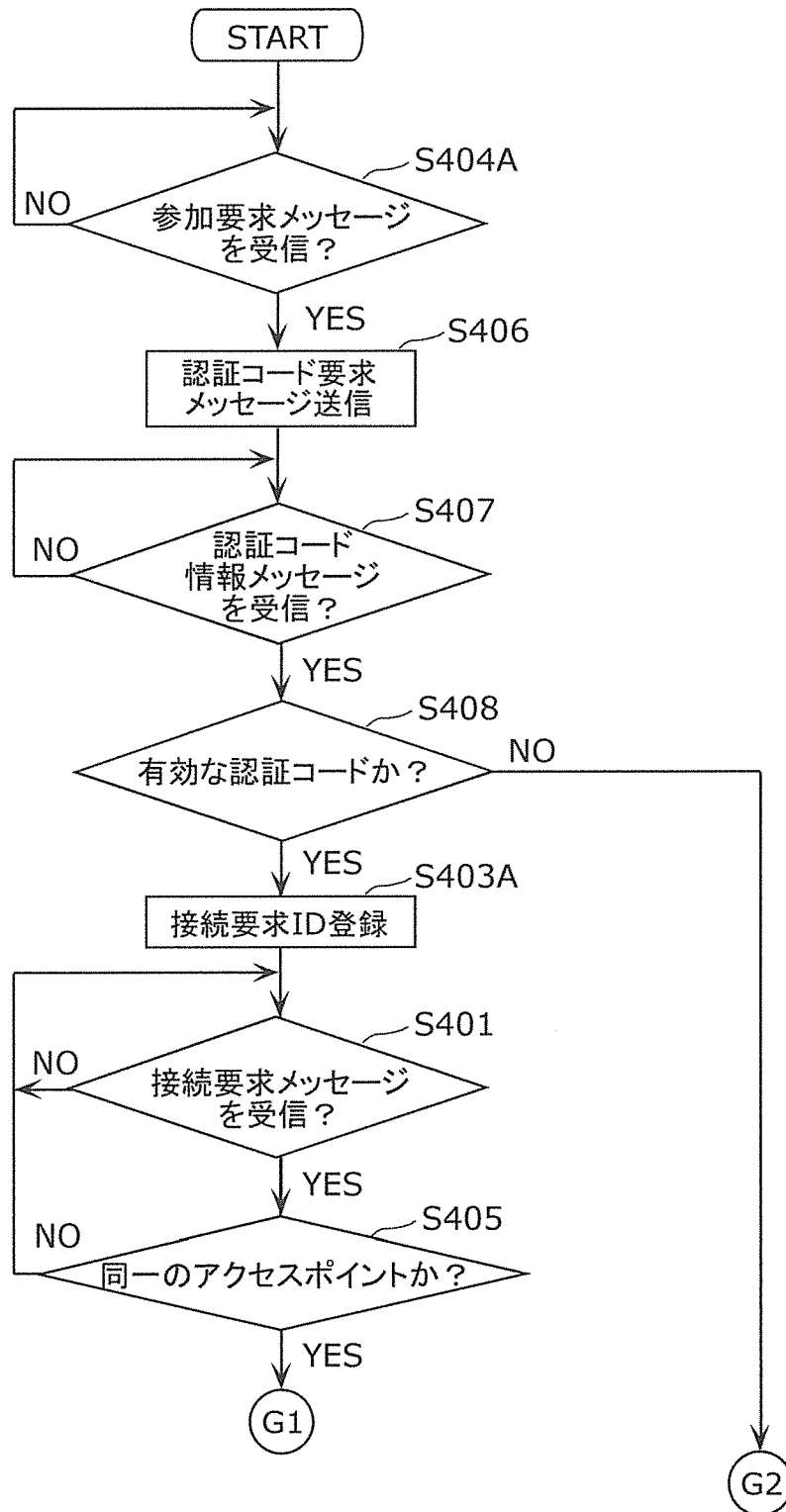
[図30]



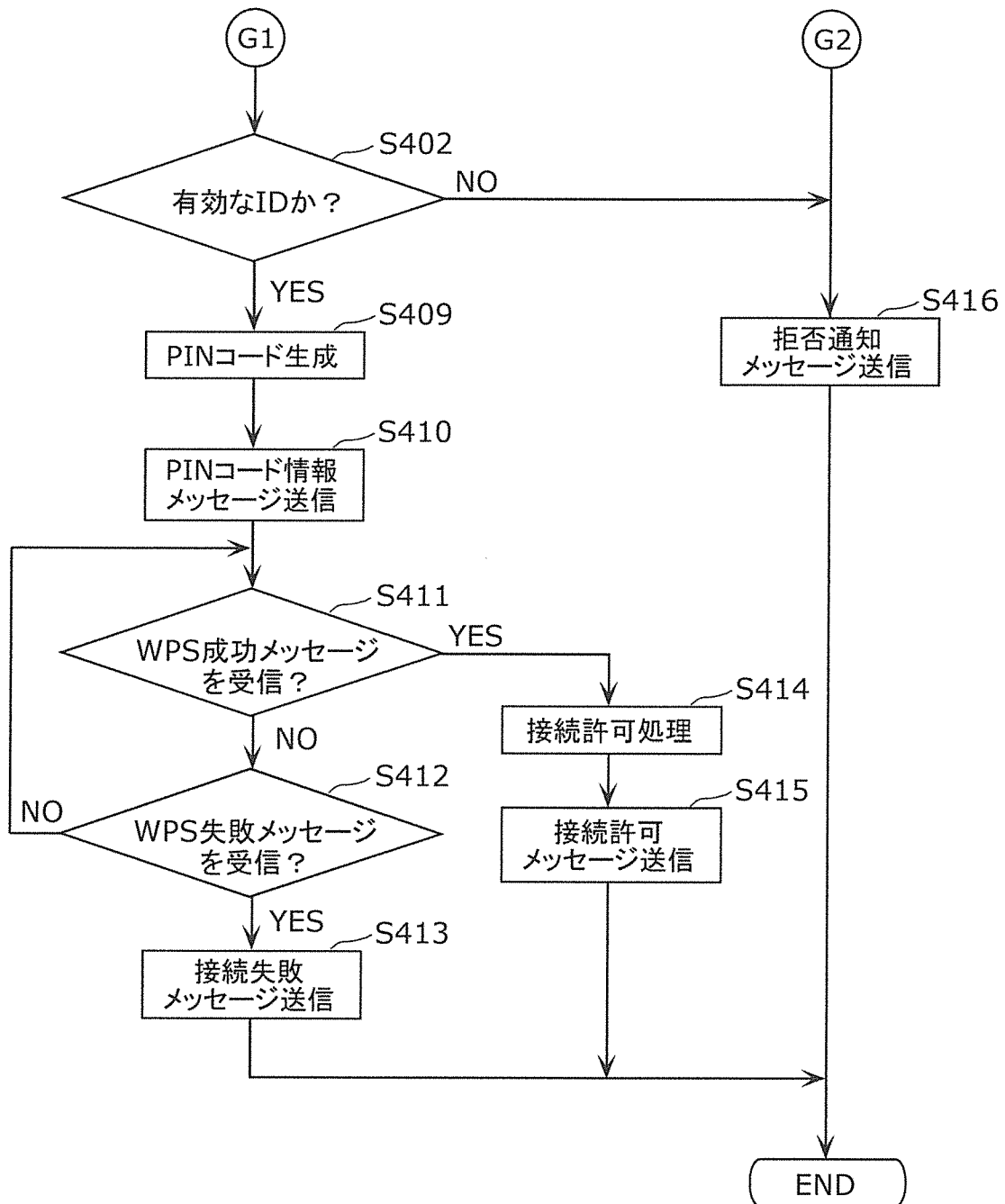
[図31]



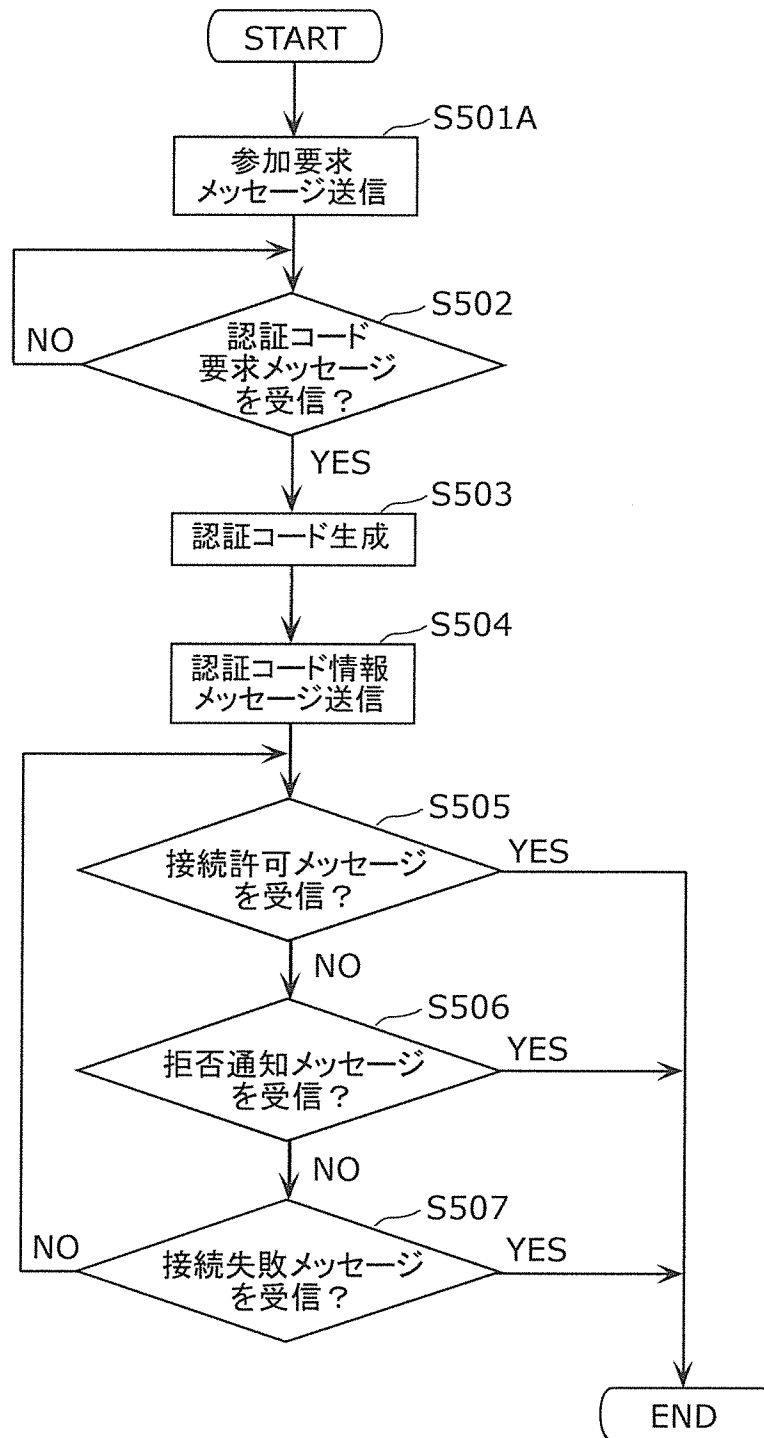
[図32]



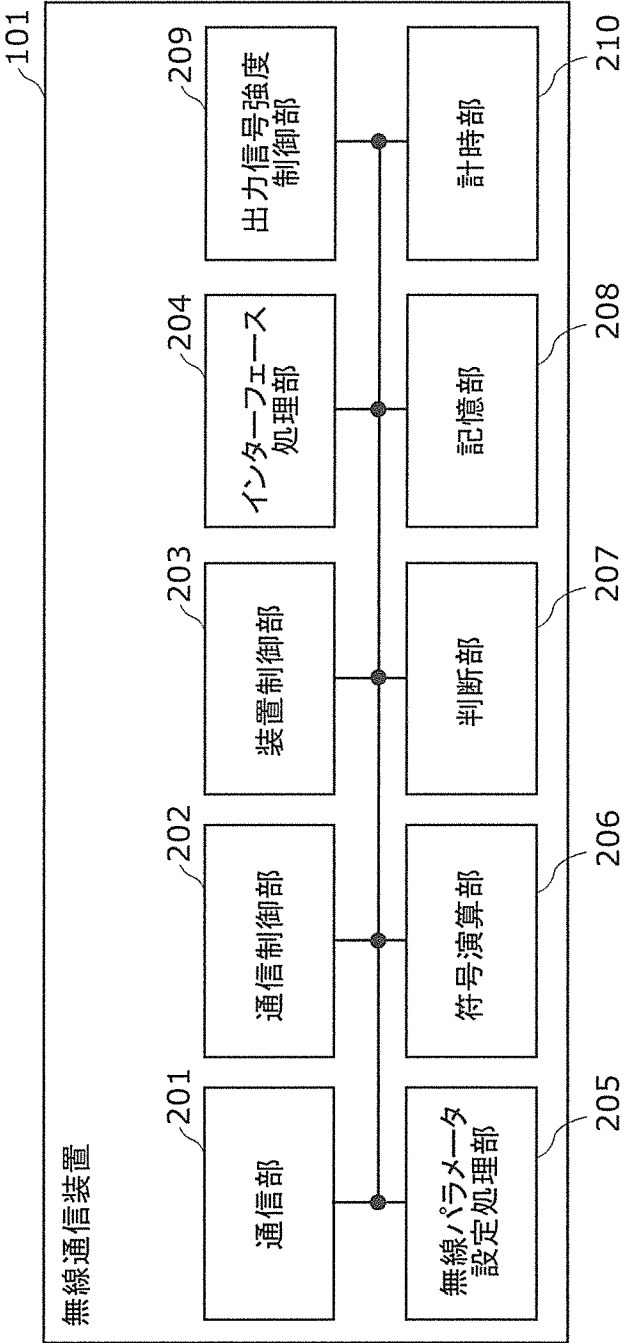
[図33]



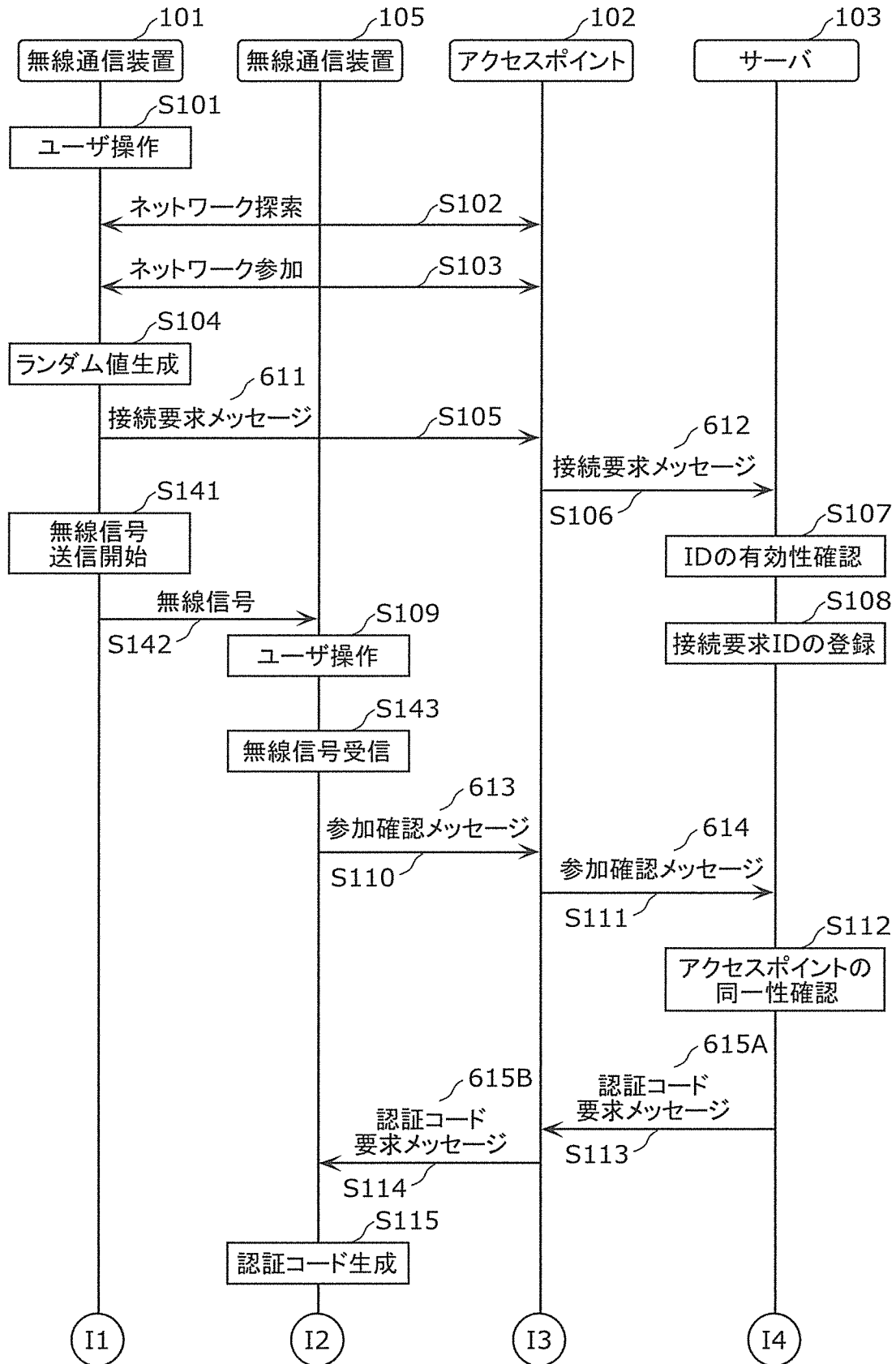
[図34]



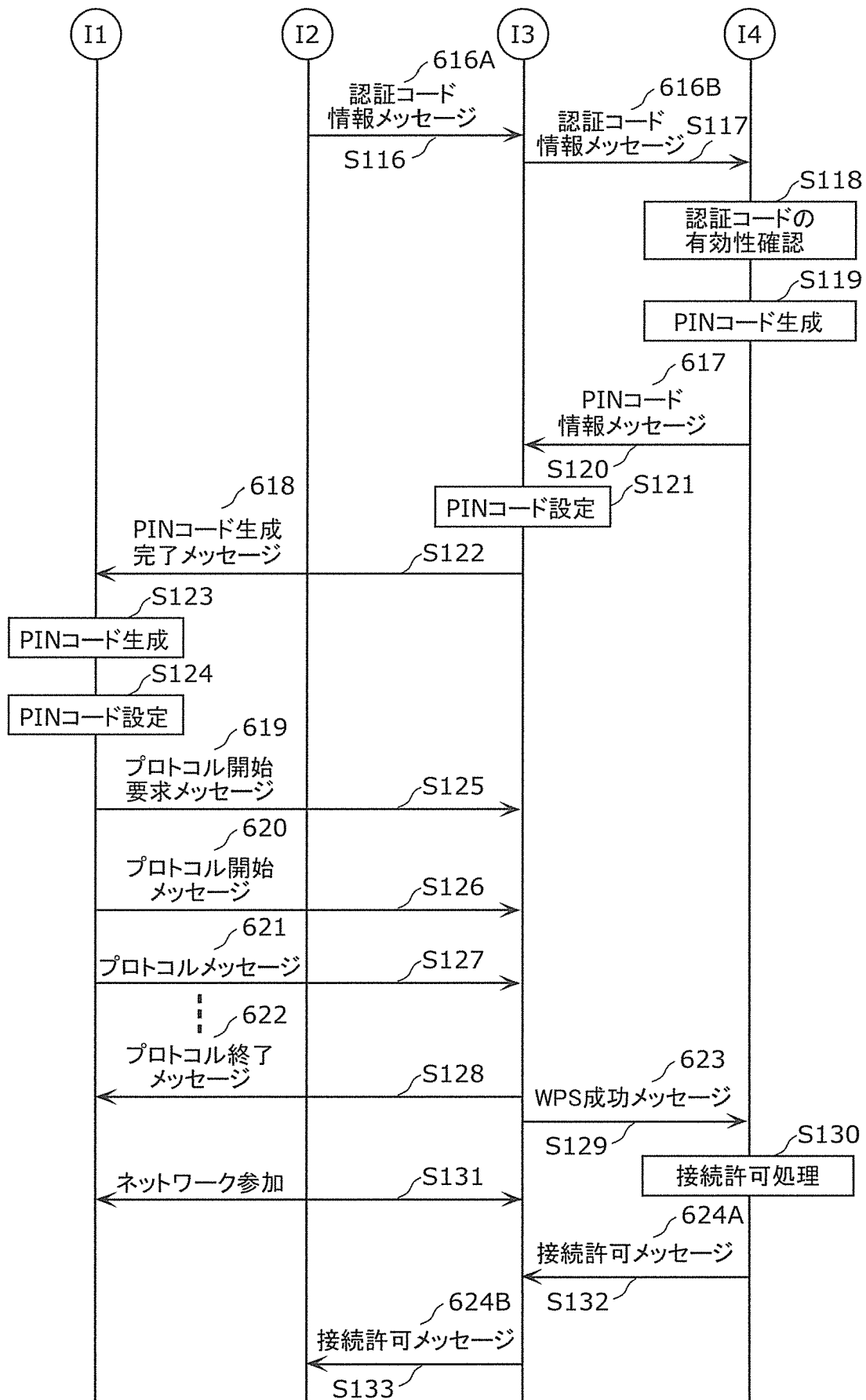
[図35]



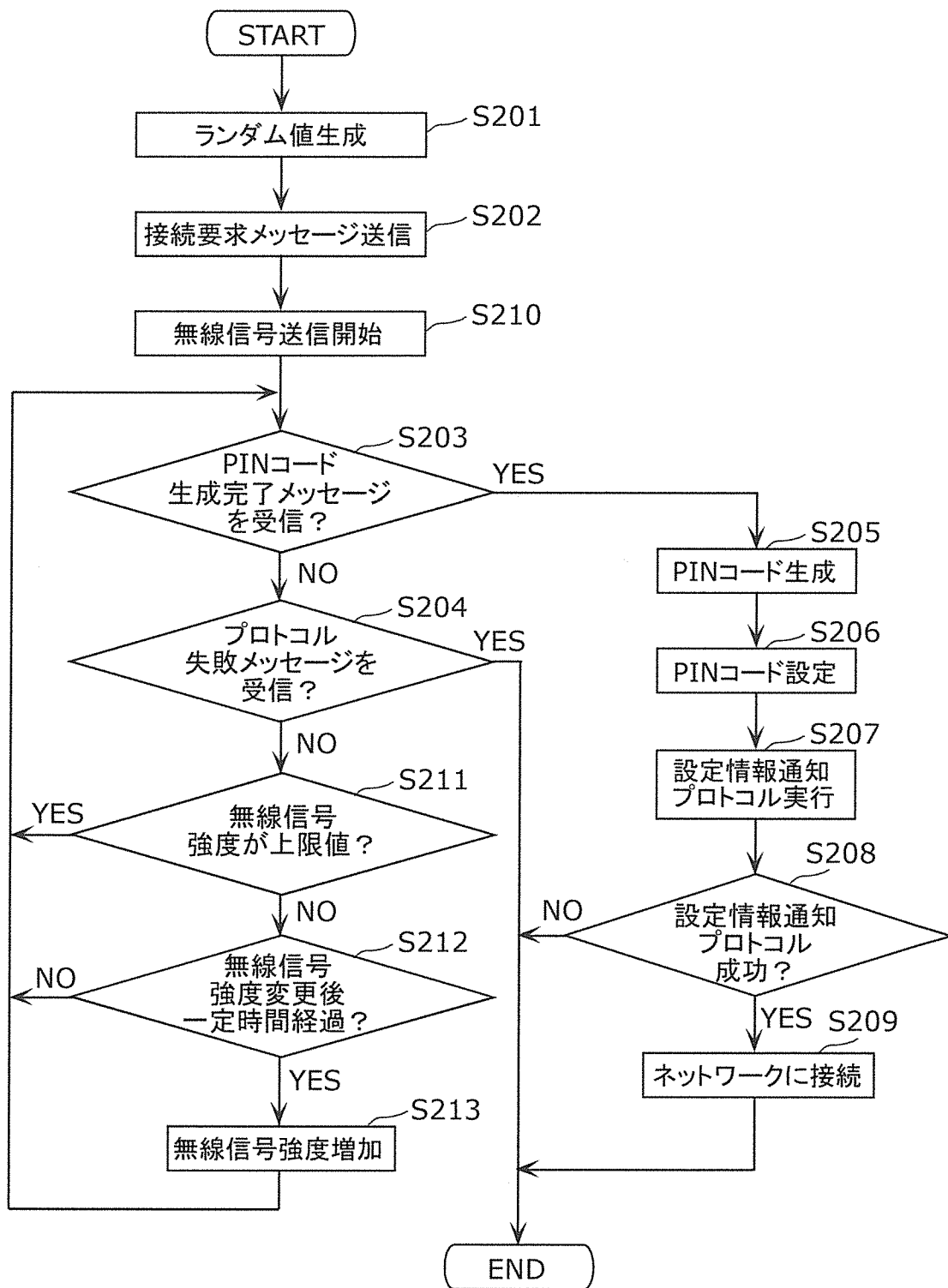
[図36]



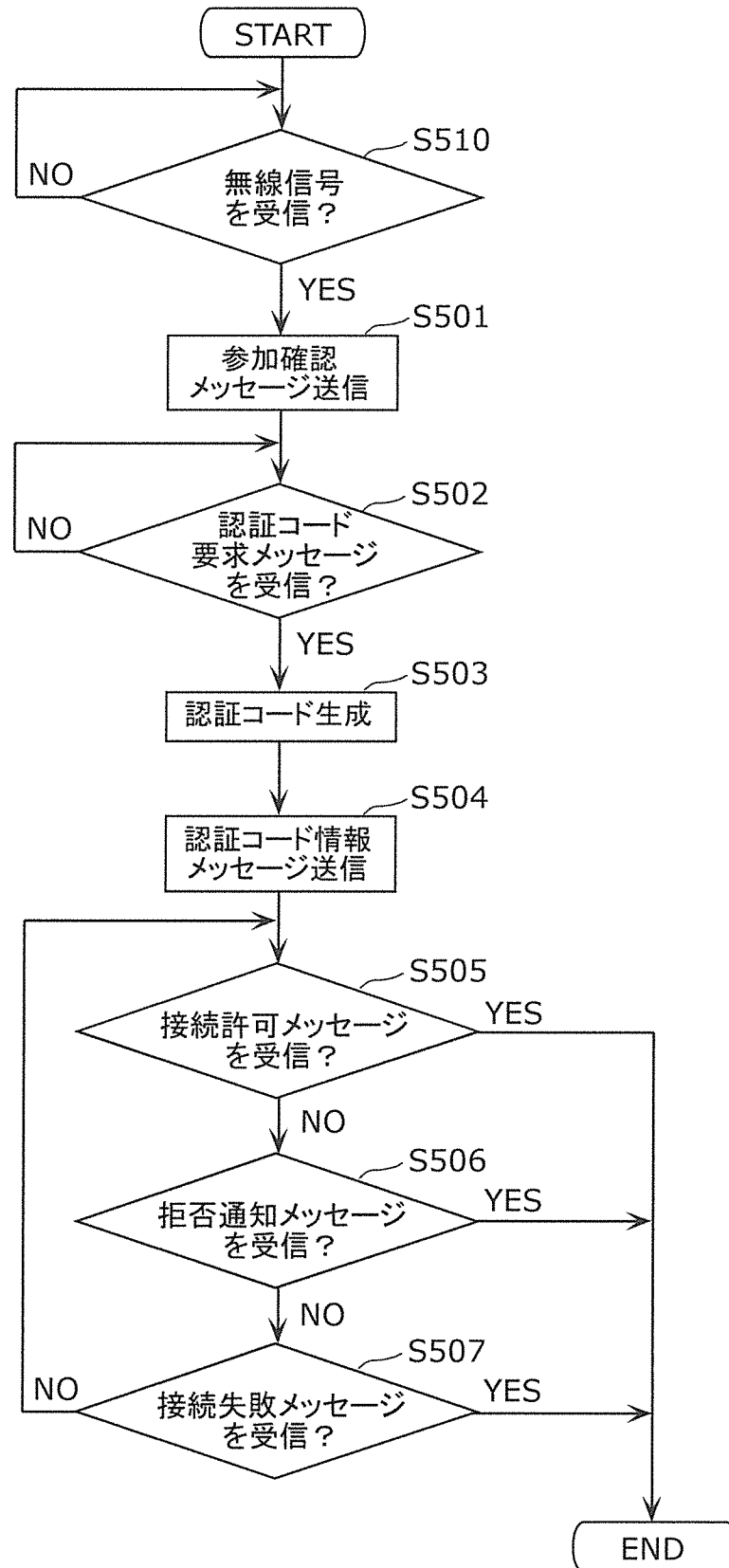
[図37]



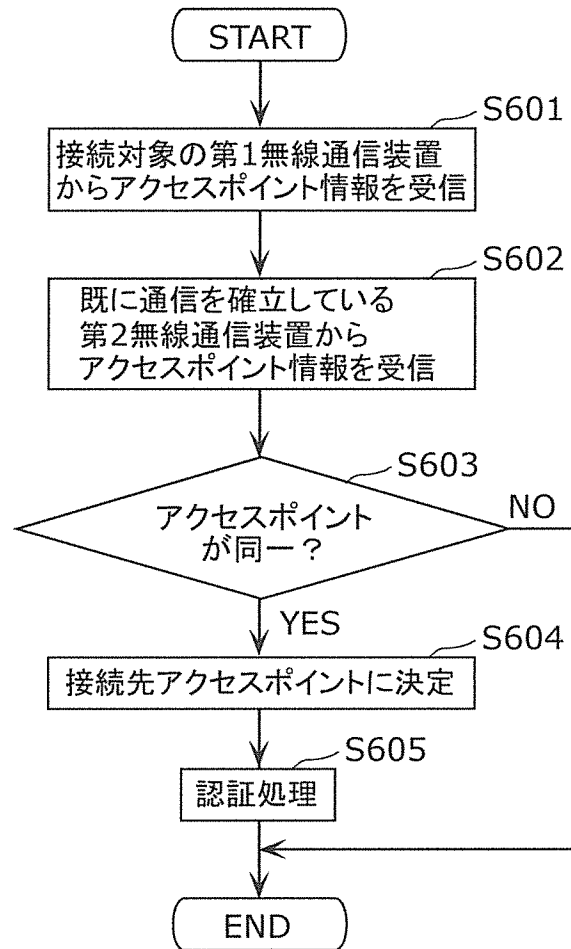
[図38]



[図39]



[図40]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/002579

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/06(2009.01)i, H04W48/20(2009.01)i, H04W84/12(2009.01)i

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)

H04W4/00-99/00, H04B7/24-7/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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.
A	JP 2009-253380 A (Canon Inc.), 29 October 2009 (29.10.2009), entire text; all drawings & US 2010/0299730 A1 & WO 2009/123074 A1	1-11
A	JP 2010-56916 A (Canon Inc.), 11 March 2010 (11.03.2010), entire text; all drawings & US 2010/0054121 A1 & EP 2160059 A2 & CN 101662818 A & KR 10-2010-0026995 A	1-11
A	JP 2012-186516 A (Silex Technology, Inc.), 27 September 2012 (27.09.2012), entire text; all drawings (Family: none)	1-11

☐ 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
04 August, 2014 (04.08.14)

Date of mailing of the international search report
12 August, 2014 (12.08.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04W12/06(2009.01)i, H04W48/20(2009.01)i, H04W84/12(2009.01)i

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（I P C））

Int.Cl. H04W4/00-99/00, H04B7/24-7/26

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 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
A	JP 2009-253380 A（キヤノン株式会社）2009.10.29, 全文, 全図 & US 2010/0299730 A1 & WO 2009/123074 A1	1-11
A	JP 2010-56916 A（キヤノン株式会社）2010.03.11, 全文, 全図 & US 2010/0054121 A1 & EP 2160059 A2 & CN 101662818 A & KR 10-2010-0026995 A	1-11
A	JP 2012-186516 A（サイレックス・テクノロジー株式会社） 2012.09.27, 全文, 全図（ファミリーなし）	1-11

☐ 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矛盾するものではなく、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

0 4 . 0 8 . 2 0 1 4

国際調査報告の発送日

1 2 . 0 8 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

東 昌秋

5 J

3 1 3 9

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 4