(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
2020年10月29日(29.10.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/217811 A1

(51) 国際特許分類:
H04M 11/00 (2006.01) *H04W 12/06* (2009.01)
H04W 8/22 (2009.01) *H04W 84/12* (2009.01)
H04W 76/10 (2018.01) *H04M 1/00* (2006.01)

(21) 国際出願番号： PCT/JP2020/012825

(22) 国際出願日： 2020年3月24日(24.03.2020)

(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 2019-081068 2019年4月22日(22.04.2019) JP

(71) 出願人: キヤノン株式会社 (**CANON KABUSHIKI KAISHA**) [JP/JP]; 〒1468501 東京都大田区下丸子３丁目３０番２号 Tokyo (JP).

(72) 発明者: 皆川 篤志 (**MINAKAWA Atsushi**); 〒1468501 東京都大田区下丸子３丁目３０番２号キヤノン株式会社内 Tokyo (JP).

(74) 代理人: 阿部 琢磨, 外 (**ABE Takuma** et al.); 〒1468501 東京都大田区下丸子３丁目３０番２号キヤノン株式会社内 Tokyo (JP).

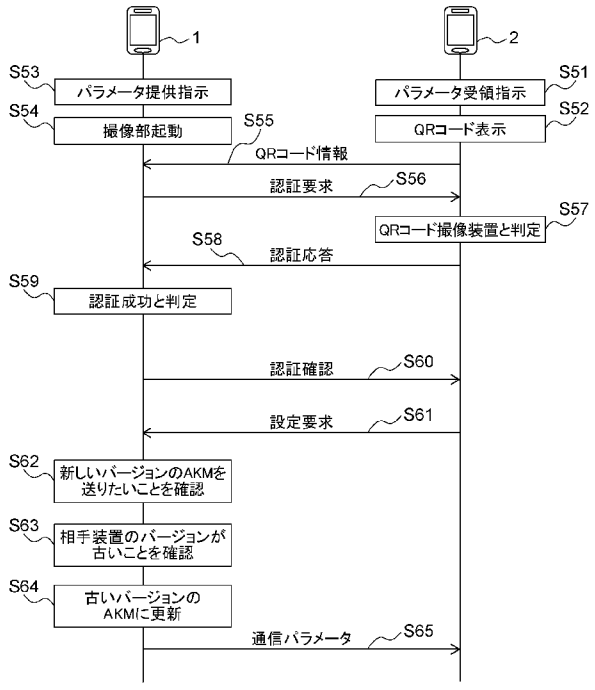
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA,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

WO 2020/217811 A1

(54) **Title:** COMMUNICATION DEVICE, CONTROL METHOD OF COMMUNICATION DEVICE, AND PROGRAM

(54) 発明の名称： 通信装置、通信装置の制御方法およびプログラム

[図5]



S51... PARAMETER RECEPTION INSTRUCTION
S52... QR CODE DISPLAY
S53... PARAMETER PROVISION INSTRUCTION
S54... IMAGING UNIT STARTUP
S55... QR CODE INFORMATION
S56... CERTIFICATE REQUEST
S57... DETERMINE AS QR CODE IMAGING DEVICE
S58... AUTHENTICATION RESPONSE
S59... DETERMINE AS AUTHENTICATION SUCCESS
S60... AUTHENTICATION CONFIRMATION
S61... SETTING REQUEST
S62... CONFIRM THAT NEW VERSION OF AKM IS TO BE SENT
S63... CONFIRM THAT VERSION OF PARTNER DEVICE IS OLDER
S64... UPDATE TO OLDER VERSION OF AKM
S65... COMMUNICATION PARAMETERS

(57) **Abstract:** This communication device determines the version of Device Provisioning Protocol (DPP) that another communication device supports, determines the type of communication parameters to be provided to the other communication device, on the basis of the determined version, and provides information indicating the determined type of the communication parameter and the communication parameter corresponding to the type of the other communication device.

[続葉有]

QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))

(57) 要約: 通信装置は、他の通信装置が対応するＤｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）のバージョンを判定し、判定されたバージョンに基づいて、当該他の通信装置に提供する通信パラメータの種別を判定し、通信パラメータの判定された種別を示す情報と、当該種別に対応する通信パラメータと、を他の通信装置に提供する。

明　細　書

発明の名称 ： 通信装置、通信装置の制御方法およびプログラム

技術分野

[0001] 本発明は、通信パラメータを提供する通信装置等に関する。

背景技術

[0002] 通信装置が無線ネットワークに接続するためには、無線通信に必要となる暗号方式、暗号鍵、認証方式、認証鍵等のさまざまな通信パラメータを当該通信装置に設定する必要がある。これらの通信パラメータを通信装置へ設定する技術として、Ｗｉ－Ｆｉ　Ｄｅｖｉｃｅ　Ｐｒｏｖｉｓｉｏｎｉｎｇ　Ｐｒｏｔｏｃｏｌ（以下、「ＤＰＰ」という）規格が策定されている（特許文献１）。

[0003] ＤＰＰでは、通信パラメータを提供するコンフィギュレータと呼ばれる装置と、通信パラメータを要求および取得するエンローリと呼ばれる装置が存在する。通信パラメータをコンフィギュレータから取得したエンローリは、ＩＥＥＥ８０２．１１規格におけるステーション（Ｓｔａｔｉｏｎ、以下「ＳＴＡ」という）またはアクセスポイント（ＡｃｃｅｓｓＰｏｉｎｔ、以下「ＡＰ」という）のいずれかとなる。

先行技術文献

特許文献

[0004] 特許文献1：米国特許出願公開２０１７／０２９５４４８号公報

発明の概要

発明が解決しようとする課題

[0005] コンフィギュレータはＤＰＰにより、通信パラメータを提供する際、ＡＫＭ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ）と呼ばれる、提供される通信パラメータの種別を識別する識別情報を付与する。

[0006] 今後、ＤＰＰのバージョンが上がり、機能拡張されることに伴い、ＡＫＭ

に新たな種別が追加され得る。しかしながら、コンフィギュレータが新たな種別のＡＫＭによって識別される種別の通信パラメータを提供しても、必ずしもエンローリが機能拡張、即ち、新たなＤＰＰのバージョンに対応しているとは限らない。このような機能拡張に対応していないエンローリは、提供された通信パラメータ中の新たな種別のＡＫＭを認識することができず、通信パラメータを不正と判定しかねない。

[0007] このため、エンローリが提供された通信パラメータを破棄してしまい、無線ネットワークへの接続ができないおそれがあった。

[0008] 本発明は上記課題に鑑みてなされたものであり、相手装置が対応するＤＰＰのバージョンに応じた種別の通信パラメータを当該相手装置へ提供できるようにすることを目的とする。

課題を解決するための手段

[0009] 上記課題を解決するため、本発明に係る通信装置は、他の通信装置が対応するＤｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）のバージョンを判定する第１の判定手段と、前記第１の判定手段により判定された前記バージョンに基づいて、前記他の通信装置に提供する通信パラメータの種別を判定する第２の判定手段と、前記第２の判定手段により判定された前記種別を示す情報と、当該種別に対応する通信パラメータと、を前記他の通信装置に提供する提供手段と、を有する。

発明の効果

[0010] 本発明によれば、相手装置が対応するＤＰＰのバージョンに応じた種別の通信パラメータを当該相手装置へ提供することができる。

図面の簡単な説明

[0011] [図1]本発明の各実施形態に係る通信システムのネットワーク構成の一例を示す図

[図2]各実施形態に係る通信装置のハードウエア構成および機能構成の一例を示す図

[図3]各実施形態に係る通信装置が実行する通信パラメータ提供処理の処理手

順の一例を示すフローチャート

[図4]図３のＳ９におけるＡＫＭ設定処理の詳細処理手順の一例を示すフローチャート

[図5]各実施形態に係る通信システムを構成するコンフィギュレータとエンローリの間で実行される認証および通信パラメータ提供処理の動作シーケンスの一例を示す図

発明を実施するための形態

[0012] 以下、添付図面を参照して、本発明を実施するための実施形態について詳細に説明する。なお、以下に説明する実施形態は、本発明の実現手段としての一例であり、本発明が適用される装置の構成や各種条件によって適宜修正または変更されるべきものであり、本発明は以下の実施形態に限定されるものではない。また、本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。

[0013] 以下、本実施形態では、通信装置が、Ｗｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）を用いて、無線ＬＡＮ通信に必要となる通信パラメータを設定される例を説明する。このＤＰＰでは、無線ＬＡＮ通信に必要な通信パラメータを保持する通信装置がコンフィギュレータ（Ｃｏｎｆｉｇｕｒａｔｏｒ）として機能し、他の通信装置に通信パラメータを提供する。一方、通信パラメータを提供される通信装置がエンローリ（Ｅｎｒｏｌｌｅｅ）として機能し、提供された通信パラメータを自装置に設定して無線ネットワークに接続する。エンローリは、アクセスポイント（ＡＰ）またはステーション（ＳＴＡ）のいずれかとして動作することができる。

[0014] また、本実施形態では、通信システムが、ＩＥＥＥ（Ｔｈｅ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ，Ｉｎｃ．）８０２．１１シリーズに準拠した無線ＬＡＮシステムを用いる例を説明する。しかしながら、本実施形態における通信形態は必ずしもＩＥＥＥ８０２．１１シリーズ準拠の無線ＬＡＮには限定

されず、他の通信形態を使用することもできる。

[0015] ＜本実施形態のネットワーク構成＞

図１は、本実施形態に係る通信システムのネットワーク構成の一例を示す図である。

[0016] 図１の通信システムは、無線端末１および２と、アクセスポイント３とを備える。

[0017] 無線端末１は、無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）通信機能を有し、例えば、ＤＰＰに規定されるコンフィギュレータとして動作する。このため、無線端末１は、無線端末２に対して無線ネットワーク４に接続するための通信パラメータを提供し、アクセスポイント（ＡＰ）３に対して無線ネットワーク４を構築するための通信パラメータを提供することができる。

[0018] 無線端末２は、無線ＬＡＮ通信機能を有し、例えば、ＤＰＰに規定されるエンローリとして動作するステーション（ＳＴＡ）である。このため、無線端末２は、コンフィギュレータとして動作する無線端末１から通信パラメータを取得し、取得された通信パラメータに基づいて、ＡＰ３により構築された無線ネットワーク４に接続する。

[0019] ＡＰ３は、例えば、ＤＰＰに規定されるアクセスポイント（ＡＰ）として動作し、無線端末１から提供される通信パラメータに基づいて、無線ＬＡＮネットワーク４を構築する。

[0020] 無線ネットワーク４は、ＡＰ３により構築される、例えば無線ＬＡＮのネットワークである。

[0021] 通信パラメータは、ネットワーク識別子であるＳＳＩＤ（Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）、暗号方式、暗号鍵、認証方式等の無線通信を実行するために必要な設定項目を含む。

[0022] 通信パラメータはまた、ＡＫＭ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ）を含む。ＡＫＭとは、無線通信時に、どの認証プロトコルや鍵交換アルゴリズムを使用するかを示す情報であり、通

信パラメータの種別を識別する識別情報である。

[0023] 例えば、ＡＫＭが「ｄｐｐ」である場合、通信パラメータは、ＤＰＰに対応するＡＰに接続するための情報であるコネクタを含む。このコネクタは、ＤＰＰが定める認証プロトコルや鍵交換アルゴリズムで使用する各種情報である。

[0024] ＡＫＭが「ｓａｅ」である場合、通信パラメータは、ＤＰＰに非対応のＡＰに接続するための情報であるパスワードを含む。このパスワードは、ＷＰＡ（Ｗｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ）３での無線接続で使用される。

[0025] また、ＡＫＭが「ｐｓｋ」である場合、通信パラメータは、ＤＰＰに非対応のＡＰに接続するための情報であるＰＳＫ（Ｐｒｅ Ｓｈａｒｅｄ Ｋｅｙ）／パスフレーズが含まれる。このＰＳＫ／パスフレーズは、ＷＰＡ２での無線接続で使用される。パスワードとＰＳＫ／パスフレーズは、ＷＰＡやＩＥＥＥ（Ｔｈｅ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ，Ｉｎｃ．）８０２．１１に基づいた認証・鍵交換を実施する際の暗号鍵である。

[0026] なお、図１では、本実施形態における各無線端末は、他の無線端末との間で無線通信が可能な装置であればよく、図示される装置に限定されない。無線端末は、例えば、携帯電話、スマートフォン、デジタルカメラ、ＰＣ、ビデオカメラ、スマートウォッチ、Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ（ＰＤＡ）等の他の装置であってよい。また、図１には、２台の無線端末が図示されているが、無線端末の数は２台に限定されず、３台以上であってよい。

[0027] ＜通信装置のハードウエア構成＞

図２は、本実施形態に係る無線端末１のハードウエア構成および機能構成の一例を示す図である。なお、無線端末２の機能構成も、無線端末１と同様である。

[0028] 図２に示す各機能部は、１つ以上のＣＰＵ（不図示）が、記憶部１０６に

格納されたプログラムを実行することにより実現され得る。すなわち、後述する各フローチャートは、１つ以上のＣＰＵが、記憶部１０６に格納されたプログラムを実行し、情報の演算および加工並びに各ハードウェアの制御を実行することにより実現され得る。ただし、図２に示す各機能部の一部またはすべてが専用のハードウェアにより実現されてもよい。

[0029] 図２の無線端末１は、無線通信制御部１０１、送受信部１０２、操作部１０３、表示部１０４、制御部１０５、記憶部１０６、撮像部１０７、および画像処理部１０８を備える。無線端末１はさらに、コード生成部１０９、パラメータ処理部１１０、パラメータ更新部１１１、認証部１１２、およびアンテナ１１３を備える。

[0030] 無線通信制御部１０１は、他の無線端末との間でＩＥＥＥ８０２．１１シリーズに準拠した無線ＬＡＮ通信での無線信号の送受信を行うために、アンテナ１１３や無線回路（不図示）に対する制御を行う。無線通信制御部１０１は、無線ＬＡＮ通信を実行するチップにより構成されてよい。

[0031] 送受信部１０２は、各通信レイヤのプロトコルに応じたデータの送受信制御を、無線通信制御部１０１を介して行う。

[0032] 操作部１０３は、ユーザが無線端末１を操作するために用いられ、撮像部１０７を起動するためのボタン等が含まれてよい。なお、操作部１０３はハードウェアで構成されていてもよいし、ソフトウェアにより表示部１０４を用いて提供されるＵＩ（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）で構成されてもよい。

[0033] 表示部１０４は、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）やＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）等で構成され、各種表示処理を行う。表示部１０４はまた、スピーカ等の音声出力が可能な機能を備えてよい。

[0034] 制御部１０５は、無線端末１における動作を統括的に制御するものであり、システムバスを介して、各構成部（１０１～１０４、１０６～１１２）を制御する。すなわち、制御部１０５は、各種処理の実行に際して記憶部１０

６から必要なプログラム等をロードし、当該プログラム等を実行することで各種の機能動作を実現する。制御部１０５は、例えば１つまたは複数のＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）により構成される。

[0035] 記憶部１０６は、制御部１０５により実行される制御プログラムや、画像データ、通信パラメータ等の各種データを記憶する。後述する各種動作は、記憶部１０６に記憶された制御プログラムを制御部１０５が実行することにより実現される。記憶部１０６は、制御部１０５の主メモリ、ワークエリア等として機能し、プログラムやデータを一時的に記憶するＲＡＭ（Ｒａｍｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）を含んでよい。記憶部１０６はまた、制御部１０５が各種処理を実行するために必要となる、変更を必要としない制御プログラムやパラメータ等を記憶する不揮発性メモリであるＲＯＭ（Ｒｅａｄ　ＯｎｌｙＭｅｍｏｒｙ）を含んでよい。記憶部１０６はさらに、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、フラッシュメモリ、または着脱可能なＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カード等の外部記憶媒体を含んでよい。

[0036] 撮像部１０７は、撮像素子、レンズ等により構成され、静止画や動画の撮像を実行する。本実施形態において、撮像部１０７は、バーコード等の一次元コードや、ＱＲコード（登録商標）等の二次元コードの画像を撮像する。

[0037] 画像処理部１０８は、撮像部１０７で撮像された画像等の画像処理を行う。本実施形態において、画像処理部１０８は、撮像部１０７により撮像されたＱＲコードの画像を解析し、符号化された情報を復号してＱＲコード情報を取得する。

[0038] コード生成部１０９は、無線端末１のＱＲコード情報を生成し、生成したＱＲコード情報をＱＲコード（画像）として表示部１０４へ表示するための制御を実行する。なお、本実施形態では、撮像部１０７により読み取るべき画像がＱＲコードである例を説明するが、本実施形態で利用可能なコード情報はＱＲコードに限定されず、バーコード等の一次元コードや、他の二次元

コード等が用いられてもよい。

[0039] パラメータ処理部１１０は、無線ネットワーク４に接続するための通信パラメータの提供や取得を実行するための処理を行う。

[0040] パラメータ更新部１１１は、通信パラメータ提供処理に関する各種更新処理を行う。例えば、パラメータ更新部１１１は、通信パラメータを識別する識別情報であるＡＫＭを更新する。本実施形態では、所定のＡＫＭではエンローリが不正と判定する場合に、コンフィギュレータが通信パラメータに含めるＡＫＭを更新する。この更新されたＡＫＭの設定処理の詳細は図４を参照して後述する。

[0041] 認証部１１２は、他の通信装置を認証するための制御（認証処理）を行う。

[0042] アンテナ１１３は、無線ＬＡＮで通信するための２．４ＧＨｚ帯および／または５ＧＨｚ帯等の帯域で通信可能である。

[0043] なお、上記機能ブロックは一例であり、複数の機能ブロックが１つの機能ブロックを構成するようにしてもよいし、何れかの機能ブロックが更に複数の機能を行うブロックに分かれてもよい。

[0044] ＜コンフィギュレータの通信パラメータ提供処理＞

図３および図４を参照して、コンフィギュレータとして動作する無線端末１が、エンローリとして動作する無線端末２を無線ネットワークへ接続させるために、ＤＰＰで規定された通信パラメータを提供する処理を説明する。

[0045] 無線端末１において、例えば、操作部１０３がパラメータ提供の指示をユーザから入力されたことをトリガに、図３に示す通信パラメータ提供処理が起動される。

[0046] Ｓ１で、無線端末１の制御部１０５は、無線端末２が表示するＱＲコードを含む画像を撮像するために撮像部１０７を起動する。Ｓ１で撮像されるＱＲコードには、無線端末２の認証用の公開鍵が含まれる。

[0047] Ｓ２で、制御部１０５は、撮像部１０７がＱＲコードを撮像したか否かを判定する。ここで、無線端末２が表示するＱＲコードは、無線端末２の表示

部１０４等に表示されたものに限らず、無線端末２の筐体や付属品に貼り付けられたラベル等に印刷されたものであってもよい。あるいは、ＱＲコードは、例えば無線端末２に対する説明書等に記載されたものでもよい。なお、Ｓ１で撮像部１０７を起動してから所定の時間内にＱＲコードを撮像できなかった場合、無線端末１は、タイムアウトして通信パラメータの提供処理を終了してもよい。

[0048] ＱＲコードが撮像されたと判定されない場合（Ｓ２：Ｎ）、Ｓ２に戻って、無線端末１の制御部１０５は、ＱＲコードの撮像を待ち受ける。

[0049] 一方、ＱＲコードが撮像されたと判定された場合（Ｓ２：Ｙ）、Ｓ３に進み、無線端末１の画像処理部１０８は、撮像されたＱＲコードから、無線端末２の認証用の公開鍵を含むＱＲコード情報を取得する。

[0050] Ｓ４で、無線端末１の認証部１１２は、送受信部１０２を介して、無線端末２に対して認証要求を送信する。

[0051] Ｓ４でコンフィギュレータである無線端末１がエンローリである無線端末２に送信する認証要求は、例えばＤＰＰ規格で規定されたＤＰＰ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｒｅｑｕｅｓｔフレームである。

[0052] この認証要求は、認証に用いるための認証情報と、無線端末１の識別情報、乱数、共有鍵生成用の公開鍵を含む。この認証情報は、Ｓ３で取得されたＱＲコードに含まれる無線端末２の認証用の公開鍵のハッシュ値であってよい。無線端末１の識別情報は、無線端末１の認証用の公開鍵のハッシュ値であってよい。乱数は、後述する認証応答の受信時に、認証のために使用され得る。共有鍵生成用の公開鍵は、無線端末１と無線端末２との間で生成される共有鍵の生成元となる鍵であってよい。

[0053] Ｓ４で送信された認証要求を受信した無線端末２は、認証要求の送信元装置がＱＲコードを撮像した無線端末１であるか否かを判定する。認証要求の送信元装置がＱＲコードを撮像した無線端末１であるか否かの判定は、認証要求に含まれている認証情報を用いて行われてよい。

[0054] 具体的には、無線端末２は、自装置の表示部１０４に表示したＱＲコード

に含めた公開鍵のハッシュ値を計算し、計算されたハッシュ値と、認証要求に含まれるハッシュ値（認証情報）とを比較し、両者が一致した場合に検証が成功したと判定する。なお、このときのハッシュ値の計算に用いられるハッシュ関数は、認証要求を送信する無線端末１との間で予め合意されているものとする。

[0055] Ｓ４で無線端末２に認証要求を送信した後、Ｓ５で、無線端末１の送受信部１０２は、無線端末２から認証応答を受信するのを待ち受ける。無線端末２から認証応答を受信しない間（Ｓ５：Ｎ）、Ｓ５に戻って認証応答の待ち受け処理を繰り返すが、時間内に無線端末２から認証応答を受信できなかった場合、タイムアウトして通信パラメータの提供処理を終了してもよい。

[0056] 認証応答は、具体的に、例えばＤＰＰ規格で規定されたＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｓｐｏｎｓｅフレームである。この認証応答は、無線端末２の共有鍵生成用の公開鍵、乱数、タグ情報を含む。

[0057] 無線端末２から認証応答を受信すると（Ｓ５：Ｙ）、Ｓ６で、無線端末１の認証部１１２は、受信された認証応答の内容を検証し、認証に成功したか否かを判定する。

[0058] 具体的には、まず、無線端末１の認証部１１２は、認証応答に含まれている無線端末２の共有鍵生成用の公開鍵と、無線端末１自身の共有鍵生成用の秘密鍵の双方を用いて共有鍵を生成する。なお、これはコンフィギュレータとして動作する無線端末１の共有鍵生成方法であり、エンローリとして動作する無線端末２は、無線端末１の共有鍵生成用の公開鍵と、無線端末２の共有鍵生成用の秘密鍵の双方を用いて共有鍵を生成する。

[0059] 共有鍵は、例えば、ＥＣＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）方式に基づいて生成されてよい。以下、共有鍵は、このＥＣＤＨ方式に基づいて生成されるものとするが、この方式に限定されるものではなく、その他の公開鍵暗号方式で生成してもよい。

[0060] 共有鍵の生成に続いて、無線端末１の認証部１１２は、認証応答に含まれるタグ情報を用いて認証成功か否かを判定する。このタグ情報は、具体的に

は、無線端末１が送信した認証要求に含まれている乱数が、無線端末２の共有鍵生成用の秘密鍵と、無線端末１の共有鍵生成用の公開鍵の双方を用いて生成された共有鍵で暗号化されたものである。

[0061] 無線端末１の認証部１１２は、認証応答に含まれるタグ情報を自身が生成した共有鍵で正しく復号できた場合に、認証に成功したと判定する。無線端末１の認証部１１２は、自身が生成した共有鍵でタグ情報を復号できた場合に認証成功と判定し、復号できなかった場合に認証失敗と判定する。

[0062] Ｓ６で認証に失敗したと判定された場合（Ｓ６：Ｎ）、Ｓ１１に分岐し、無線端末１の制御部１０５は表示部１０４に認証エラーを示すメッセージを表示して、パラメータ提供処理を終了する。一方、認証成功と判定された場合（Ｓ６：Ｙ）、Ｓ７に進み、無線端末１の認証部１１２は、送受信部１０２を介して、無線端末２へ認証確認を送信する。

[0063] この認証確認は、具体的には、例えばＤＰＰ規格で規定されたＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｎｆｉｒｍフレームである。この認証確認は、タグ情報を含む。このタグ情報は、無線端末２が送信した認証応答に含まれている乱数が、生成された共有鍵で暗号化されたものである。

[0064] Ｓ８で、無線端末１の送受信部１０２は、Ｓ７で認証確認を送信後、エンローリである無線端末２から通信パラメータの設定要求が送信されるのを待ち受ける。

[0065] 一方、無線端末２は、Ｓ７で無線端末１から送信された認証確認を受信し、認証確認に含まれているタグ情報を自身が生成した共有鍵で正しく復号できた場合に、認証成功と判定する。

[0066] 認証成功と判定されると、無線端末２は、認証要求を送信した無線端末１をコンフィギュレータと認定して、無線端末１に対して通信パラメータの設定要求を送信する。

[0067] この設定要求は、具体的には、例えばＤＰＰ規格で規定されたＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｑｕｅｓｔフレームである。この設定要求は、無線端末２のデバイス情報および役割情報が含まれる。デバイス情報と

は、無線端末２のデバイス名等である。また、役割情報とは、通信パラメータ受信後の役割を示す情報であり、「アクセスポイント（ＡＰ）」または「ステーション（ＳＴＡ）」である。設定要求に含まれる情報は、無線端末２が認証応答に含まれるタグ情報の生成時に使用した共有鍵で暗号化される。

[0068] 無線端末２からの設定要求が受信されない間（Ｓ８：Ｎ）、Ｓ８に戻り、無線端末２からの設定要求を待ち受け、一方、無線端末２から設定要求が受信されると（Ｓ８：Ｙ）、Ｓ９に進む。

[0069] Ｓ９で、無線端末１のパラメータ処理部１１０およびパラメータ更新部１１１は、無線端末２に提供すべき通信パラメータに、ＡＫＭを設定する処理を実行する。このＡＫＭ設定処理の詳細は、図４を参照して後述する。

[0070] Ｓ１０で、無線端末１のパラメータ処理部１１０は、送受信部１０２を介して、無線端末１に通信パラメータを提供する。

[0071] 具体的には、無線端末１のパラメータ処理部１１０は、無線端末２に対して無線ネットワーク４を構築するための通信パラメータを含む設定応答を、送受信部１０２を介して送信する。この設定応答は、例えばＤＰＰ規格で規定されるＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｓｐｏｎｓｅフレームである。設定応答には、通信パラメータ、パラメータの有効期限、無線端末１のコンフィギュレータ専用の公開鍵、役割情報等が含まれる。設定応答に含まれる情報は、Ｓ７でタグ情報の生成時に使用した共有鍵で暗号化される。

[0072] なお、Ｓ１０で提供される通信パラメータは、コネクタ、パスワード、ＰＳＫ／パスフレーズ、およびＡＫＭを含む。エンローリとして動作する無線端末２は、ＡＫＭの値に基づいて、コネクタ、パスワード、ＰＳＫ／パスフレーズのそれぞれが通信パラメータに含まれるか否かを判定することができる。

[0073] 無線端末２は、設定要求を送信後、コンフィギュレータとして動作する無線端末１から設定応答が送信されるのを待ち受ける。設定応答を受信した無線端末２は、設定応答に含まれる通信パラメータを、タグ情報生成時に使用

した共有鍵で復号する。無線端末２は、復号して得られた通信パラメータを自装置に設定し、無線ネットワーク４に接続可能となる。

[0074] ＜無線端末１のＡＫＭ設定処理詳細＞

次に、図４を参照して、図３のＳ９で無線端末１が実行するＡＫＭ設定処理の詳細を説明する。

[0075] ＤＰＰの機能拡張に対応している無線端末１が、機能拡張によって追加されたＡＫＭを含む通信パラメータを、ＤＰＰの機能拡張に対応していない無線端末２に提供する場合を考える。この場合、無線端末２は、通信パラメータに含まれるＡＫＭの値が未知であるため不正であると判定し、その結果、通信パラメータを破棄してしまい、無線ネットワーク４に接続することができない。

[0076] 本実施形態では、無線端末２においてＡＫＭの値が不正であると判定されることのないよう、無線端末２が認識できるＡＫＭを含む通信パラメータを提供する。

[0077] 以下、本実施形態において、ＤＰＰの機能拡張に対応していない無線端末２でも認識できるＡＫＭに更新された通信パラメータを、無線端末１が無線端末２に提供する処理を説明する。

[0078] 図４は、ＤＰＰの機能拡張によって追加されたＡＫＭを含む通信パラメータを提供したい無線端末１が、無線端末２が機能拡張に対応しているか否かを判定して、無線端末２に通信パラメータを提供する処理を示すフローチャートである。

[0079] 図３に示すＳ８で通信パラメータの設定要求を受信すると（Ｓ８：Ｙ）、Ｓ９１で、無線端末１の制御部１０５は、無線端末２に提供しようとする通信パラメータに含まれるＡＫＭが、ＤＰＰの機能拡張で追加されたＡＫＭであるか否かを判定する。

[0080] 機能拡張で追加されたＡＫＭとは、例えば、ＷＰＡ３の後継である「ＷＰＡ４」の通信パラメータを示す値や、「ＤＰＰとＷＰＡ３の両方」のように複数の通信パラメータを示す値である。

[0081] 無線端末２に提供する通信パラメータに含まれるＡＫＭが機能拡張で追加されたＡＫＭでないと判定された場合（Ｓ９１：Ｎ）、Ｓ９２およびＳ９３をスキップしてＳ９４に進む。Ｓ９４で、無線端末１のパラメータ処理部１１０は、パラメータ更新部１１１によりＡＫＭを変更せずに、設定応答として、送受信部１０２を介して通信パラメータを無線端末２に送信する。

[0082] 一方、機能拡張で追加されたＡＫＭであると判定された場合（Ｓ９１：Ｙ）、Ｓ９２に進み、無線端末１の制御部１０５は、無線端末２が機能拡張に対応しているか否かを判定する。即ち、本ステップにおいて、無線端末２がＤＰＰのいずれのバージョンに対応しているかが判定される。

[0083] 無線端末２が機能拡張に対応しているか否かは、例えば、無線端末２が送信する認証応答や設定要求に含まれる情報から判定することができる。具体的には、認証応答や設定要求中の所定のフィールドに、所定のフラグビットが立っているか否かに基づいて判定することができる。また、認証応答や設定要求に含めて通知される、例えば「１」や「２」のような数字によって示されるバージョン情報に基づいて判定してもよい。なお、バージョン情報には、後者の数字等で直接示されるバージョンの情報の他、前者のフラグビット等によって示される無線端末２の対応機能の情報を含むものとする。また、無線端末２が機能拡張に対応しているか否かを判定できる情報を無線端末２から受信できない場合、無線端末２は機能拡張に対応していないと判定してもよい。例えば、上記の所定のフィールドや、バージョンを示す情報そのものが、認証応答や設定要求に含まれていない場合に、機能拡張に対応していないと判定してもよい。

[0084] 無線端末２のバージョンが古くなく機能拡張に対応していると判定された場合（Ｓ９２：Ｎ）、パラメータ処理部１１０は、パラメータ更新部１１１によりＡＫＭを変更せずに、設定応答として、送受信部１０２を介して通信パラメータを無線端末２に送信する。

[0085] 他方、無線端末２が機能拡張に対応していないと判定された場合（Ｓ９２：Ｙ）、Ｓ９３に進む。

[0086] Ｓ９３で、無線端末１のパラメータ更新部１１１は、通信パラメータに含まれるＡＫＭを、機能拡張で追加されたＡＫＭではない値、つまり機能拡張以前から対応されていたＡＫＭの値に更新する。

[0087] Ｓ９４で、無線端末１のパラメータ処理部１１０は、設定応答として、ＡＫＭが更新された通信パラメータを、送受信部１０２を介して、無線端末２に送信する。

[0088] なお、ＡＫＭの更新処理は、具体的には、無線端末１が送りたいＡＫＭが、例えば「ＤＰＰとＷＰＡ３の両方」のように複数の接続先の情報を示す値の場合、機能拡張前に対応していた「ｄｐｐ」もしくは「ｓａｅ」のいずれかの値に更新する。また、ＷＰＡのように「１」や「２」といった数字によって規格のバージョンが識別される接続先の情報であれば、送りたいＡＫＭが、例えば「ＷＰＡ４」もしくは「ＷＰＡ４とＷＰＡ３の両方」を示す値の場合、前方規格であるＷＰＡ３を示す「ｓａｅ」を選択してＡＫＭを更新する。また、送りたいＡＫＭに基づかずに、必ず所定のＡＫＭ、例えば「ｄｐｐ」に更新してもよい。

[0089] ＜コンフィギュレータとエンローリ間での通信パラメータ提供処理の動作シーケンス＞

図５は、コンフィギュレータである無線端末１とエンローリである無線端末２との間の通信パラメータ提供処理の動作シーケンスの一例を示す。

[0090] Ｓ５１で、無線端末２は、操作部１０３を介して、通信パラメータ受領の指示をユーザから受け付ける。

[0091] Ｓ５２で、無線端末２は、表示部１０４にＱＲコードを表示して、無線端末１からの認証要求を待ち受ける。なお、所定の時間内に認証要求を受信できなかった場合、無線端末２は、認証要求の待ち受けを終了してもよい。また、無線端末２は、必ずしもＱＲコードを表示するための表示部１０４等を備えていなくともよい。無線端末２の筐体や付属品に貼り付けられたラベル等にＱＲコードが印刷されている場合、Ｓ５２をスキップしてもよい。この場合、無線端末２は、Ｓ５１でパラメータ受領の指示を受け付けると、Ｓ５

２での処理を行わずに認証要求を待ち受ける。

[0092] 一方、Ｓ５３で、無線端末１は、操作部１０３を介して通信パラメータ提供の指示をユーザから受ける。

[0093] Ｓ５４で、無線端末１は、無線端末２が表示するＱＲコードを撮像するために撮像部１０７を起動する。

[0094] Ｓ５５で、無線端末１の撮像部１０７は、無線端末２の表示するＱＲコードを撮像することで、当該ＱＲコードが示すＱＲコード情報を取得する。

[0095] ＱＲコードが示すＱＲコード情報を取得した無線端末１の認証部１１２は、Ｓ５６で、送受信部１０２を介して認証要求（ＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｑｕｅｓｔ）を生成して、無線端末２に送信し、無線端末２は、この認証要求を受信する。

[0096] Ｓ５７で、無線端末２は、Ｓ５６で無線端末１から受信した認証要求の内容を検証する。認証要求を検証する処理の詳細は、図３を参照して上述したとおりである。

[0097] 認証要求の送信元の無線端末１がＱＲコードを撮像した装置であることが検証されると、Ｓ５８で、無線端末２は、認証応答（ＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｓｐｏｎｓｅ）を生成して、無線端末１に送信する。無線端末１へ認証応答を送信した無線端末２は、無線端末１から認証確認が送信されるのを待ち受ける。

[0098] Ｓ５９で、無線端末１は、Ｓ５８で無線端末２から受信した認証応答の内容を検証する。認証応答を検証する処理の詳細は、図３を参照して上述したとおりである。

[0099] Ｓ６０で、無線端末１の認証部１１２は、認証成功と判定すると、送受信部１０２を介して、無線端末２へ認証確認（ＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｎｆｉｒｍ）を送信する。

[0100] 無線端末１から認証確認を受信した無線端末２は、認証確認の内容を検証する。無線端末２は、自身が生成した共有鍵でタグ情報を正しく復号できた場合に認証に成功したと判定する。

[0101] 認証に成功したと判定されると、Ｓ６１で、無線端末２は、通信パラメータの設定処理を行うために設定要求（ＤＰＰ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｒｅｑｕｅｓｔ）を送信し、無線端末１から設定応答が送信されるのを待ち受ける。

[0102] Ｓ６２で、無線端末２から設定要求を受信した無線端末１のパラメータ処理部１１０は、送信すべき通信パラメータに機能拡張で追加されたＡＫＭが含まれているか否かを判定する。

[0103] 機能拡張で追加されたＡＫＭであると判定されると、Ｓ６３で、無線端末１のパラメータ処理部１１０は、無線端末２が機能拡張に対応しているか否かを判定する。

[0104] 無線端末２が機能拡張に対応していないと判定すると、Ｓ６４で、無線端末１のパラメータ更新部１１１は、通信パラメータに含まれるＡＫＭを、機能拡張以前から対応されていたＡＫＭ、すなわち無線端末２が認識可能なＡＫＭに更新する。

[0105] ＡＫＭを更新した無線端末１は、Ｓ６５で、送受信部１０２を介して、更新されたＡＫＭを含む通信パラメータを、設定応答（ＤＰＰ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｒｅｓｐｏｎｓｅ）に含めて無線端末２に送信する。なお、更新されたＡＫＭは、設定応答におけるＡＫＭフィールドに格納されて送信される。

[0106] 設定応答を受信した無線端末２は、受信された設定応答に含まれる通信パラメータを用いて無線ネットワーク４に接続する。

[0107] また、図３～図５を参照して説明した処理と同様の処理によって、コンフィギュレータである無線端末１が、エンローリであるアクセスポイント（ＡＰ）３に対して通信パラメータを提供することができる。ＡＰ３は、無線端末１から提供された通信パラメータで無線ネットワーク４を構築することができる。

[0108] なお、上記で説明した通信パラメータ提供処理は、各図に示す順序に限定されない。

[0109] 例えば、無線端末１は、ＤＰＰの機能拡張で追加されたＡＫＭであるか否かを判定する（図４のＳ９１）前に、無線端末２が機能拡張に対応しているか否かを判定（図４のＳ９２）してもよい。また、無線端末１は、認証確認を送信する（図３のＳ７）前に、受信した認証応答に含まれる情報に基づいて無線端末２が機能拡張に対応しているか否かを判定してもよい。この場合、設定要求を受信した（図３のＳ８：Ｙ）後に、機能拡張で追加されたＡＫＭであると判定すると（図４のＳ９１：Ｙ）、無線端末２が機能拡張に対応しているか否かを判定せずにＡＫＭを更新することができる。

[0110] 以上説明したように、本実施形態によれば、通信パラメータ提供処理において、コンフィギュレータである通信装置は、機能拡張で追加された値ではないＡＫＭに更新した通信パラメータを、エンローリに提供することができる。通信パラメータを提供されたエンローリである通信装置は、正常にＡＫＭを認識することができ、通信パラメータが不正に判定されて無線接続不可となることが有効に防止され、無線接続の利便性が向上する。

[0111] 上述の実施形態においては、ＱＲコード（登録商標）の画像を利用して通信パラメータの設定を行うための情報を通信装置間でやり取りする構成について説明したが、エンローリ認証用の公開鍵を含む情報を提供する手段はこれに限定されない。

[0112] 例えば、ＱＲコード（登録商標）の撮像に替えて、ＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）やＢｌｕｅｔｏｏｔｈ（登録商標）などの無線通信を用いてもよい。また、ＩＥＥＥ８０２．１１ａｄもしくはトランスファージェット（ＴｒａｎｓｆｅｒＪｅｔ）（登録商標）等の無線通信を用いてもよい。

[0113] なお、読み取るべきＱＲコード（登録商標）は、表示部に表示されているＱＲコードだけではなく、通信機器の筐体にシールなどの形態で貼り付けられているＱＲコードであってよい。また、読み取るべきＱＲコード（登録商標）は、取り扱い説明書や通信機器の販売時の段ボールなどの包装に貼り付けられているものであってもよい。また、ＱＲコードでなく、バーコード等

の一次元コード、他の二次元コード等であってもよい。また、ＱＲコードなどの機械可読能な情報に替えて、ユーザ可読な形式の情報であってもよい。

[0114] また、上述の実施形態において、装置間の通信をＩＥＥＥ８０２．１１シリーズ準拠の無線ＬＡＮ通信により行う場合について説明したが、本実施形態に適用可能な無線通信方式はこれに限定されない。例えば、ワイヤレスＵＳＢ、ＭＢＯＡ（Ｍｕｌｔｉ　ＢａｎｄＯＦＤＭ　Ａｌｌｉａｎｃｅ）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ）、ＺｉｇＢｅｅ、ＮＦＣ等の無線通信媒体を用いて実施してもよい。また、ＵＷＢは、ワイヤレスＵＳＢ、ワイヤレス１３９４、ＷＩＮＥＴ等を含む。また、各実施形態において、無線ＬＡＮのアクセスポイントに接続するための通信パラメータを提供する例を説明したが、本実施形態で提供可能な通信パラメータはこれに限定されない。例えば、通信装置は、Ｗｉ－Ｆｉ　Ｄｉｒｅｃｔ（登録商標）のグループオーナに接続するための通信パラメータを提供してもよい。

[0115] また、本発明は、上述の実施形態の１以上の機能を実現するプログラムによっても実現可能である。すなわち、そのプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータ（またはＣＰＵやＭＰＵ等）における１つ以上のプロセッサーがプログラムを読出し実行する処理により実現可能である。また、そのプログラムをコンピュータ可読な記録媒体に記録して提供してもよい。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

[0116] また、上述した実施形態を、複数の機器、例えば、ホストコンピュータ、インタフェース機器、撮像装置、ウェブアプリケーション等から構成されるシステムに適用してもよく、１つの機器からなる装置に適用してもよい。

[0117] また、コンピュータが読みだしたプログラムを実行することにより、実施形態の機能が実現されるものに限定されない。例えば、プログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって上記した実施

形態の機能が実現されてもよい。

[0118] 本発明は上記実施の形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために以下の請求項を添付する。

[0119] 本願は、２０１９年４月２２日提出の日本国特許出願特願２０１９－０８１０６８を基礎として優先権を主張するものであり、その記載内容の全てをここに援用する。

請求の範囲

[請求項1] 通信装置であって、

他の通信装置が対応するＤｅｖｉｃｅ　Ｐｒｏｖｉｓｉｏｎｉｎｇ　Ｐｒｏｔｏｃｏｌ（ＤＰＰ）のバージョンを判定する第１の判定手段と、

前記第１の判定手段により判定された前記バージョンに基づいて、前記他の通信装置に提供する通信パラメータの種別を判定する第２の判定手段と、

前記第２の判定手段により判定された前記種別を示す情報と、当該種別に対応する通信パラメータと、を前記他の通信装置に提供する提供手段と、

を有することをする通信装置。

[請求項2] 前記他の通信装置からＤＰＰ規格に準拠した信号を受信する受信手段を更に有し、

前記受信手段により受信された前記信号に基づいて、前記第１の判定手段は、前記他の通信装置が対応するＤＰＰのバージョンを判定することを特徴とする請求項１に記載の通信装置。

[請求項3] 前記受信手段により受信される前記信号は、前記他の通信装置が対応するＤＰＰのバージョンを示す情報を含むことを特徴とする請求項２に記載の通信装置。

[請求項4] 前記受信手段により受信される前記信号に、前記他の通信装置が対応するＤＰＰのバージョンを示すフィールドが含まれないことに基づいて、前記第１の判定手段は、前記他の通信装置が対応するＤＰＰのバージョンを判定することを特徴とする請求項２に記載の通信装置。

[請求項5] 前記受信手段により受信される前記信号は、前記通信装置に通信パラメータを要求する信号であることを特徴とする請求項２から４のいずれか１項に記載の通信装置。

[請求項6] 前記他の通信装置を認証するための認証処理を行う認証手段を更に

有し、

前記認証手段による前記認証処理において前記他の通信装置の認証に成功した場合に、前記提供手段は、前記第２の判定手段により判定された前記種別を示す情報と、当該種別に対応する通信パラメータと、を前記他の通信装置に提供することを特徴とする請求項１から５のいずれか１項に記載の通信装置。

[請求項7] 前記他の通信装置の公開鍵の情報を含むコードを撮像する撮像手段を更に有し、

前記認証手段は、前記撮像手段により撮像された前記コードに含まれる前記公開鍵の情報を用いて、前記認証処理を行うことを特徴とする請求項６に記載の通信装置。

[請求項8] 前記提供手段は、前記第２の判定手段により判定された前記種別に対応する通信パラメータを暗号化して前記他の通信装置に提供することを特徴とする請求項１から７のいずれか１項に記載の通信装置。

[請求項9] 前記第２の判定手段により判定された前記種別を示す情報は、ＡＫＭ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ）フィールドに格納されて、前記他の通信装置に提供されることを特徴とする請求項１から８のいずれか１項に記載の通信装置。

[請求項10] 前記第１の判定手段により判定された前記バージョンに基づいて、前記ＡＫＭフィールドに格納される情報が、前記第２の判定手段により判定された前記種別を示す情報となるように更新する更新手段を更に有することを特徴とする請求項９に記載の通信装置。

[請求項11] 前記第１の判定手段により判定された前記バージョンに基づいて、前記提供手段が、前記他の通信装置に複数の種別の通信パラメータを提供するか、１つの種別の通信パラメータを提供するかを決定する決定手段を更に有することを特徴とする請求項１から１０のいずれか１項に記載の通信装置。

[請求項12] 前記通信装置は、ＤＰＰ規格に準拠したコンフィギュレータであり

、前記他の通信装置は、ＤＰＰ規格に準拠したエンローリであることを特徴とする請求項１から１１のいずれか１項に記載の通信装置。

[請求項13] 通信装置の制御方法であって、

他の通信装置が対応するＤｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）のバージョンを判定する第１の判定工程と、

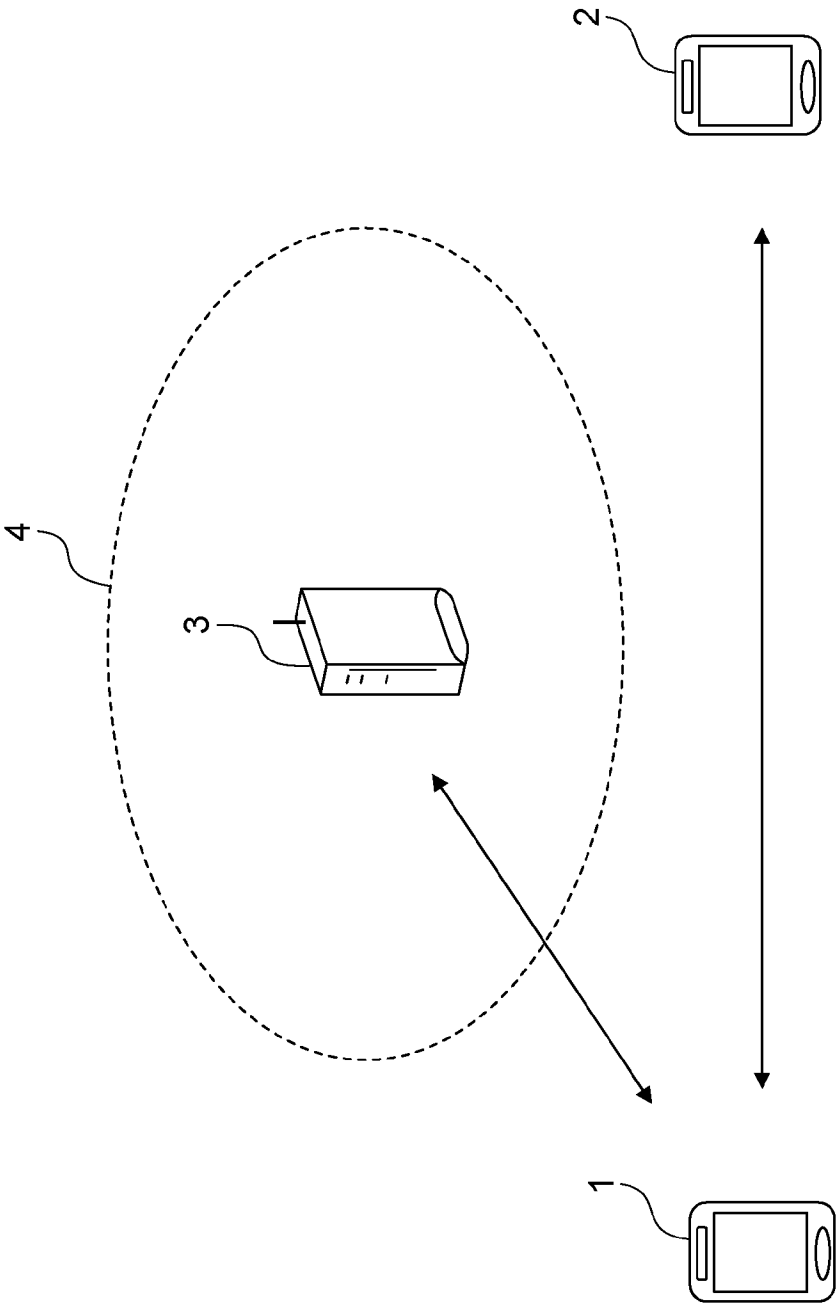
前記第１の判定工程において判定された前記バージョンに基づいて、前記他の通信装置に提供する通信パラメータの種別を判定する第２の判定工程と、

前記第２の判定工程において判定された前記種別を示す情報と、当該種別に対応する通信パラメータと、を前記他の通信装置に提供する提供工程と、

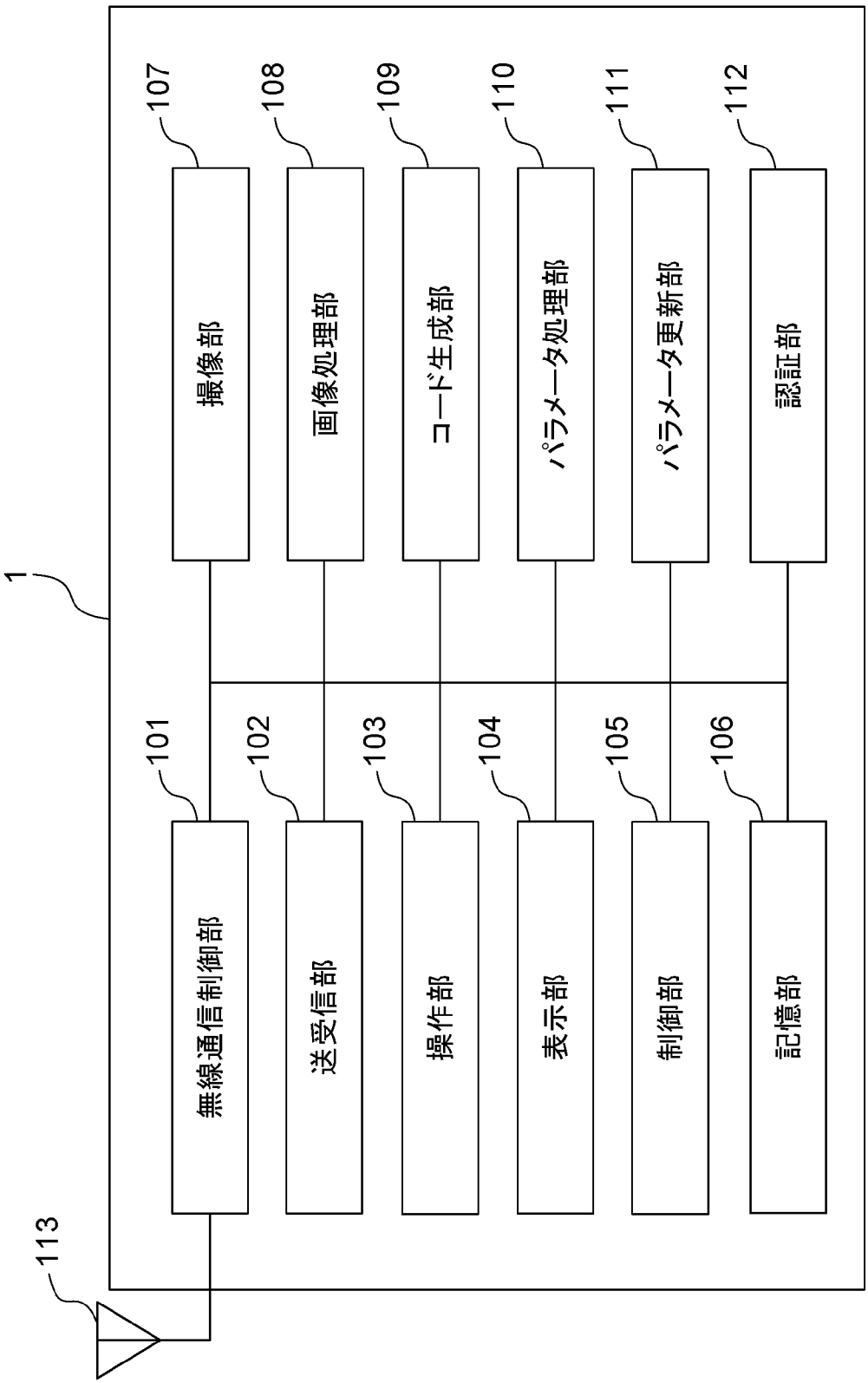
を有することを特徴とする制御方法。

[請求項14] コンピュータを、請求項１から１２のいずれか１項に記載の通信装置の各手段として機能させるためのプログラム。

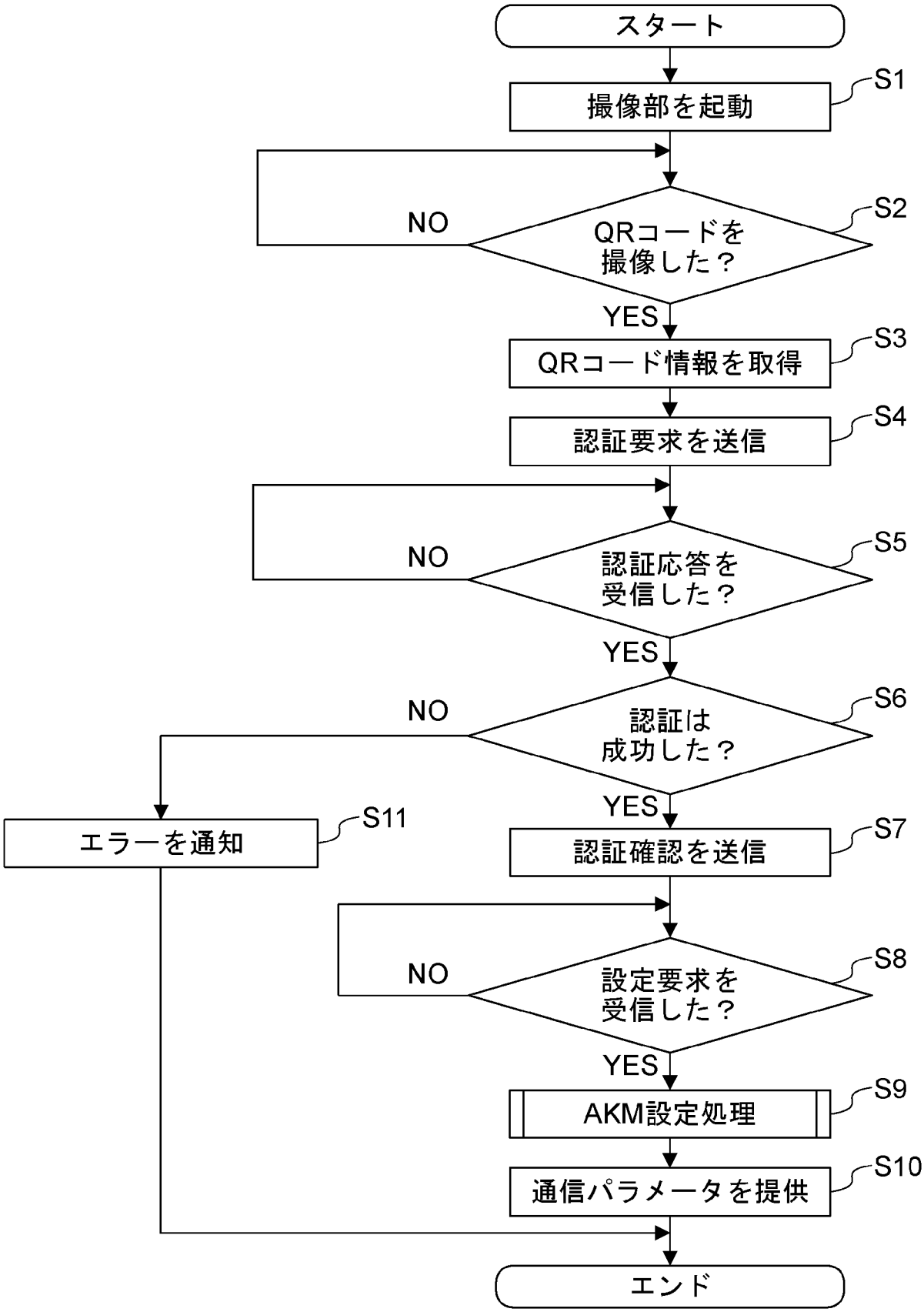
[図1]



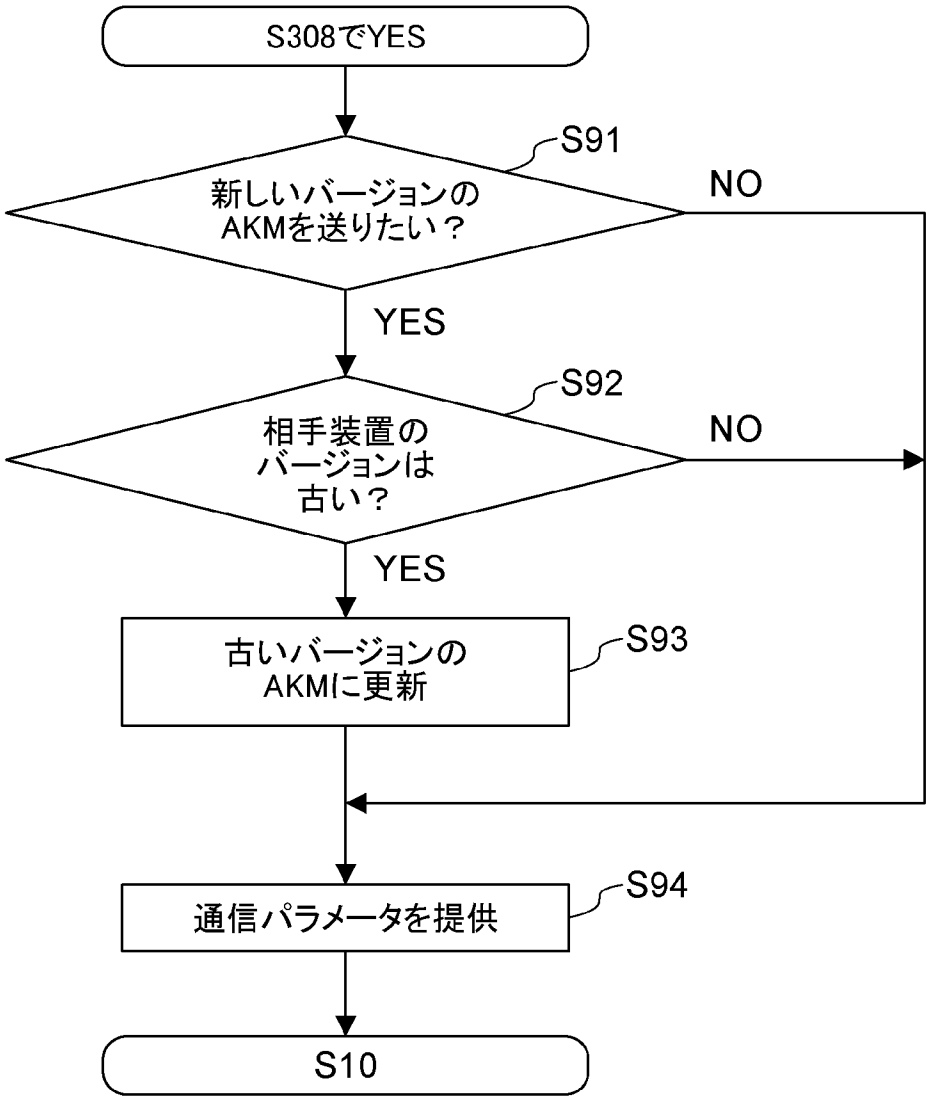
[図2]


1
101
無線通信制御部
102
送受信部
103
操作部
104
表示部
105
制御部
106
記憶部
107
撮像部
108
画像処理部
109
コード生成部
110
パラメータ処理部
111
パラメータ更新部
112
認証部
113

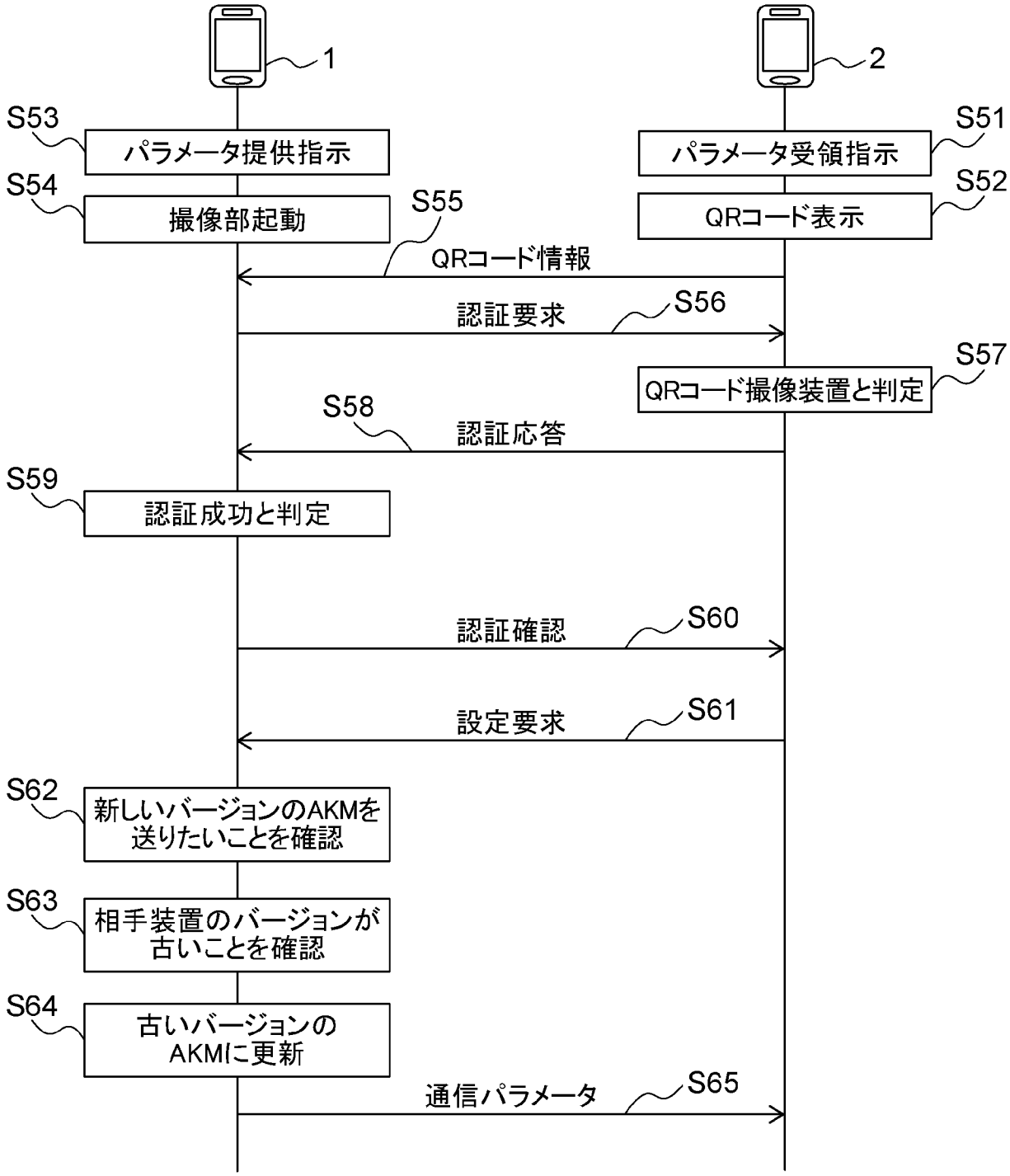
[図3]


スタート
撮像部を起動
S1
NO
QRコードを
撮像した？
S2
YES
QRコード情報を取得
S3
認証要求を送信
S4
NO
認証応答を
受信した？
S5
YES
NO
認証は
成功した？
S6
YES
エラーを通知
S11
認証確認を送信
S7
NO
設定要求を
受信した？
S8
YES
AKM設定処理
S9
通信パラメータを提供
S10
エンド

[図4]


S308でYES
S91
新しいバージョンの
AKMを送りたい？
NO
YES
S92
相手装置の
バージョンは
古い？
NO
YES
古いバージョンの
AKMに更新
S93
通信パラメータを提供
S94
S10

[図5]


1
2
S53
パラメータ提供指示
S51
パラメータ受領指示
S54
撮像部起動
S55
S52
QRコード表示
QRコード情報
認証要求
S56
S57
QRコード撮像装置と判定
S58
認証応答
S59
認証成功と判定
認証確認
S60
設定要求
S61
S62
新しいバージョンのAKMを送りたいことを確認
S63
相手装置のバージョンが古いことを確認
S64
古いバージョンのAKMに更新
通信パラメータ
S65

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/012825

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. H04M11/00(2006.01)i, H04W8/22(2009.01)i, H04W76/10(2018.01)i, H04W12/06(2009.01)i, H04W84/12(2009.01)i, H04M1/00(2006.01)i
FI: H04W8/22, H04M1/00 Q, H04M11/00 302, H04W12/06, H04W76/10 130, H04W84/12
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. H04M11/00, H04W8/22, H04W76/10, H04W12/06, H04W84/12, H04M1/00

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.
A	Device Provisioning Protocol Specification, Version 1.1, Wi-Fi Alliance, 03 December 2018, pp. 30, 31, 53-57, 82, in particular, sections 4.3.3, 6.3.6.1	1-14
A	WO 2019/021770 A1 (CANON INC.) 31 January 2019, fig. 3	1-14
A	JP 2018-42058 A (CANON INC.) 15 March 2018, paragraphs [0034]-[0042]	1-14

☐ 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	Date of mailing of the international search report
05.06.2020	16.06.2020
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/JP2020/012825

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
WO 2019/021770 A1	31.01.2019	JP 2019-29989 A fig. 3	
JP 2018-42058 A	15.03.2018	US 2019/0215878 A1 paragraphs [0041]-[0049] CN 109691220 A KR 10-2019-0049774 A	

国際調査報告

国際出願番号
PCT/JP2020/012825

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04M 11/00(2006.01)i; H04W 8/22(2009.01)i; H04W 76/10(2018.01)i; H04W 12/06(2009.01)i; H04W 84/12(2009.01)i; H04M 1/00(2006.01)i
FI: H04W8/22; H04M1/00 Q; H04M11/00 302; H04W12/06; H04W76/10 130; H04W84/12

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））

H04M11/00; H04W8/22; H04W76/10; H04W12/06; H04W84/12; H04M1/00

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
A	Device Provisioning Protocol Specification, Version 1.1, Wi-Fi Alliance, 2018.12.03, p.p.30,31,53-57,82 特に、第４．３．３節，第６．３．６．１	１－１４
A	WO 2019/021770 A1 (キヤノン株式会社) 31.01.2019 (2019-01-31) 図３	１－１４
A	JP 2018-42058 A (キヤノン株式会社) 15.03.2018 (2018-03-15) 段落［００３４］－［００４２］	１－１４

☐ 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	国際調査報告の発送日
05.06.2020	16.06.2020

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）
小林　正明 5J 4241
電話番号 03-3581-1101 内線 3576

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/012825

引用文献	公表日	パテントファミリー文献	公表日
WO 2019/021770 A1	31.01.2019	JP 2019-29989 A 図３	
JP 2018-42058 A	15.03.2018	US 2019/0215878 A1 [0041]-[0049] CN 109691220 A KR 10-2019-0049774 A	