

(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3月19日(19.03.2020)



(10) 国際公開番号

WO 2020/054478 A1

- (51) 国際特許分類:
H04W 76/38 (2018.01) *H04W 48/02* (2009.01)
H04W 12/04 (2009.01) *H04W 84/12* (2009.01)
- (21) 国際出願番号: PCT/JP2019/034434
- (22) 国際出願日: 2019年9月2日(02.09.2019)
- (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 2018-171689 2018年9月13日(13.09.2018) 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: 後藤 史英(GOTO Fumihide); 〒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,

(54) Title: COMMUNICATION DEVICE, COMMUNICATION DEVICE CONTROL METHOD, 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4]

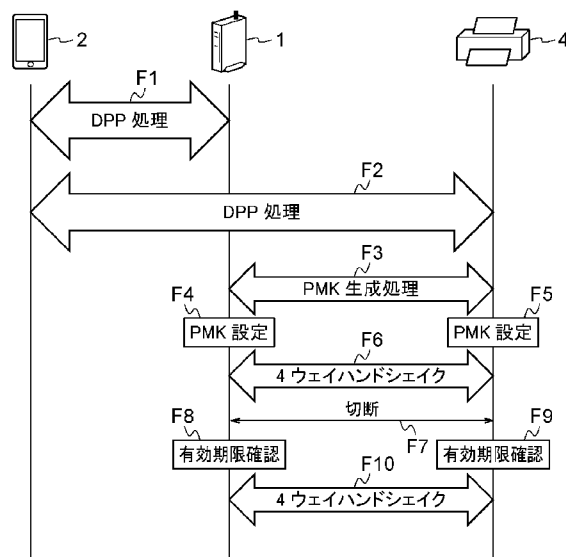


FIG. 4:
F1, F2 DPP process
F3 PMK generation process
F4, F5 PMK setting
F6, F10 4-way handshake
F7 Disconnection
F8, F9 Confirmation of expiration date

(57) Abstract: A communication device provided with: a reception means for receiving a communication parameter for wireless communication with a first communication device via a wireless network; a generation means for generating, on the basis of the communication parameter received by the reception means, cipher key information to be shared with the first communication device; an acquisition means for acquiring the expiration date of connection to the wireless network from the communication parameter received by the reception means; a connection means for connecting to the first communication device via the wireless network using the cipher key information generated by the generation means; and a control means for determining whether or not the expiration date acquired by the acquisition means has elapsed, and

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, 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))

when the expiration date has elapsed, controls the connection means so as to restrict connection to the first communication device using the cipher key information.

(57) 要約: 通信装置は、無線ネットワークを介した第1の通信装置との無線通信の通信パラメータを第2の通信装置から受信する受信手段と、受信手段により受信された通信パラメータに基づいて、第1の通信装置との間で共有すべき暗号鍵情報を生成する生成手段と、受信手段により受信された通信パラメータから、無線ネットワークへ接続する有効期限を取得する取得手段と、生成手段により生成された暗号鍵情報を使用して第1の通信装置と無線ネットワークを介して接続する接続手段と、取得手段により取得された有効期限が経過したか否かを判定し、有効期限が経過した場合には、暗号鍵情報を使用した第1の通信装置との接続を規制するよう、接続手段を制御する制御手段とを備える。

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、無線ネットワークに接続可能な通信装置に関する。

背景技術

[0002] 近年、デジタルカメラ、プリンタ、携帯電話あるいはスマートフォン等の電子機器に無線通信機能を搭載し、これらの電子機器を無線ネットワークに接続して使用するケースが増えている。

[0003] これらの電子機器を無線ネットワークに接続して使用するには、無線通信に必要となる暗号方式、暗号鍵、認証鍵等のさまざまな通信パラメータを当該電子機器に設定する必要がある。これらの通信パラメータの電子機器への設定を容易化する技術として、Wi-Fi Alliance Device Provisioning Protocol（以下、「DPP」と称する。）が策定されている。このDPPでは、ユーザは例えば電子機器のQRコード（登録商標）を読み取ることで当該電子機器を登録し、無線ネットワークへのセキュアな接続を確立することができる。

[0004] このDPPでは、通信パラメータを提供するコンフィギュレータが、アクセスポイントに接続するために必要な情報を、通信パラメータを受信して無線ネットワークに登録するエンローリに提供して、提供された通信パラメータをエンローリに設定する。

[0005] 特許文献1は、コンフィギュレータ装置から、共通管理オブジェクト（Common Managed Object：CMO）を受信することで、異なるプロビジョニング手法でプロビジョニングを実行可能な無線装置を開示する。

[0006] 具体的には、特許文献1のコンフィギュレータ装置は、異なるプロビジョニング手法のうちいずれのプロビジョニング手法を使用すべきかを示す情報を含むCMOを、無線装置へ送信する。CMOを受信した無線装置は、CM

○中の情報に基づいて、いずれのプロビジョニング手法を使用すべきかを決定し、決定されたプロビジョニング手法でプロビジョニングを実行する。

[0007] 通信パラメータをコンフィギュレータから受信するエンローリは、IEEE 802.11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（Access Point、以下「AP」という。）のいずれかとなる。

[0008] コンフィギュレータからエンローリであるSTAおよびAPのそれぞれに通信パラメータが提供された後、相互接続すべきSTAとAPは、まずSTAとAPとの間で認証処理を実行する。次に、このSTAとAPの間で、STAとAPとの間の通信における暗号鍵の基となる事前共有鍵として、Pairwise Master Key（以下「PMK」という。）を確定する必要がある。

[0009] このPMKを事前に確定した後、STAとAPとの間を接続するリンクを確立する際に、確定されたPMKを使用して4ウェイハンドシェイク等の処理を実行することにより、STAとAPとの無線通信の際の暗号化に使用される暗号鍵が生成される。事前に確定されたPMKを使用して、STAとAPとの接続の度に無線通信において使用される暗号鍵が変更されるため、無線通信のセキュリティ強度が向上する。

先行技術文献

特許文献

[0010] 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

[0011] ところで、コンフィギュレータからエンローリへ提供される通信パラメータには、無線ネットワークに接続する有効期限を設定することができる。しかしながら従来、STAとAPとの間で事前に共有されるPMKには、この有効期限の情報を持つことができなかった。このため、STAとAPとの間

で一旦PMKが確定してしまうと、その後、コンフィギュレータから提供された有効期限を使用した制御を実行することができなかった。

[0012] 本来、コンフィギュレータから通信パラメータで有効期限を設定するのは、通信パラメータの提供先のエンローリを無線ネットワークに一時的に参加させるためであり、有効期限が切れた後は当該エンローリに無線ネットワークを使用させないためである。しかしながら、エンローリ間（STAとAP間）でPMKが確立した後には、従来、設定されている有効期限に関わりなく、有効期限切れとすべきエンローリに半永久的な無線ネットワークへの接続を許容してしまうおそれがあった。

[0013] 本発明は上記課題に鑑みてなされたものであり、その目的は、無線ネットワークへの接続の有効期限が設定された通信装置において、設定された有効期限に基づいて他の通信装置との無線通信を適切に実行することが可能な通信装置を提供することにある。

課題を解決するための手段

[0014] 上記課題を解決するため、本発明に係る通信装置のある態様によれば、無線ネットワークを介した第1の通信装置との無線通信の通信パラメータを第2の通信装置から受信する受信手段と、前記受信手段により受信された前記通信パラメータに基づいて、前記第1の通信装置との間で共有すべき暗号鍵情報を生成する生成手段と、前記受信手段により受信された前記通信パラメータから、前記無線ネットワークへ接続する有効期限を取得する取得手段と、前記生成手段により生成された前記暗号鍵情報を使用して、前記第1の通信装置と前記無線ネットワークを介して接続する接続手段と、前記取得手段により取得された前記有効期限が経過したか否かを判定し、前記有効期限が経過した場合には、前記暗号鍵情報を使用した前記第1の通信装置との接続を規制するよう前記接続手段を制御する制御手段とを備える通信装置が提供される。

図面の簡単な説明

[0015] [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ェア構成の一例を示す図

[図3]各実施形態に係る通信装置の機能構成の一例を示すブロック図

[図4]各実施形態に係る通信システムを構成する通信装置間の動作シーケンスの一例を示す図

[図5]各実施形態に係る通信装置が参照するPMK管理テーブルの一例を示す図

[図6]実施形態1において通信装置が実行するPMK設定生成および設定処理の処理手順の一例を示すフローチャート

[図7]実施形態1において通信装置が実行する他の通信装置への接続判定処理の処理手順の一例を示すフローチャート

[図8]実施形態1においてPMKの有効期限が切れた場合に通信装置が表示する表示画面の一例を示す図

[図9]実施形態2において通信装置が実行する有効期限確認処理の処理手順の一例を示すフローチャート

[図10]実施形態2においてPMKの有効期限が切れた場合に通信装置が表示する表示画面の一例を示す図

発明を実施するための形態

[0016] 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。

[0017] (実施形態1)

本実施形態は、無線ネットワークを介した通信相手の通信装置との無線通信に必要な通信パラメータを、当該通信パラメータを保持する通信装置から受信し、受信された通信パラメータに基づいて、通信相手の通信装置との間

で共有すべき暗号鍵情報を生成する。

[0018] 本実施形態はさらに、提供された通信パラメータから、無線ネットワークへ接続する有効期限を取得する。そして、本実施形態は、通信相手の通信装置と接続する際に、取得された有効期限が経過したか否かを判定し、有効期限が経過した場合には、暗号鍵情報を使用した通信相手の通信装置との接続を規制する。

[0019] これにより、無線通信に必要な通信パラメータを保持する通信装置から提供される通信パラメータに設定された有効期限を、通信相手の通信装置との間で共有すべき暗号鍵情報にも適用可能となる。従って、通信パラメータを提供する通信装置が設定した無線ネットワークへ接続する有効期限が、通信パラメータを提供する通信装置が介在しない通信相手の通信装置との間の接続において有効化され、有効期限を適切に用いた暗号化無線通信が実現する。

[0020] 以下、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IEEE 802.11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。

[0021] また、本実施形態では、通信装置が、Wi-Fi Alliance 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として機能し、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として機能し、提供された通信パラメータに含まれる値から、他のエンローリとの間で共有すべき暗号鍵情報を生成する。この暗号鍵情報は、DPPにおけるPairwise Master Key (PMK) であってよい。無線LAN

N通信において、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。

[0022] <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。

[0023] 図1の通信システムは、アクセスポイント1、スマートフォン2、無線LANネットワーク3、およびプリンタ4を備える。

[0024] アクセスポイント1は、DPPにおけるエンローリとして機能するアクセスポイント（AP）であり、スマートフォン2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3を構築する。

[0025] スマートフォン2は、DPPにおけるコンフィギュレータとして機能し、エンローリであるアクセスポイント2およびプリンタ4に、無線LANネットワーク3へ接続するために必要な通信パラメータを提供する。無線LANネットワーク3は、アクセスポイント1により構築される無線LANのネットワークである。

[0026] プリンタ4は、DPPにおけるエンローリとして機能するステーション（STA）であり、スマートフォン2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3のアクセスポイント1へ接続する。

[0027] 以下では、アクセスポイント1により構築される無線LANネットワーク3にプリンタ4を参加させる場合の例を説明する。プリンタ4には、スマートフォン2からアクセスポイント1に接続するための通信パラメータが提供される。

[0028] なお、図1では、本実施形態における各通信装置が、アクセスポイント1、スマートフォン2、およびプリンタ4である例が示されているが、各通信装置は、他の通信装置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。通信装置は、例えば、携帯電話、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、

3 台の通信装置が図示されているが、通信装置の数は 3 台に限定されず、2 台または 4 台以上であってよい。

[0029] <通信装置のハードウェア構成>

図 2 は、本実施形態に係る各通信装置のハードウェア構成の一例を示す図である。

[0030] 図 2 の通信装置 1 0 は、制御部 1 1、記憶部 1 2、撮像部 1 3、入力部 1 4、表示部 1 5、無線通信部 1 6、アンテナ制御部 1 7、およびアンテナ 1 8 を備える。制御部 1 1、記憶部 1 2、撮像部 1 3、入力部 1 4、表示部 1 5、無線通信部 1 6、およびアンテナ制御部 1 7 は、システムバスにより通信可能に接続される。

[0031] 制御部 1 1 は、通信装置 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（1 2～1 7）を制御する。すなわち、制御部 1 1 は、各種処理の実行に際して記憶部 1 2 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 1 1 は、例えば CPU（Central Processing Unit）により構成される。

[0032] 記憶部 1 2 は、制御部 1 1 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 1 2 に記憶された制御プログラムを制御部 1 1 が実行することにより実現される。記憶部 1 2 は、制御部 1 1 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（Random Access Memory）を含んでよい。記憶部 1 2 はまた、制御部 1 1 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 Only Memory）を含んでよい。記憶部 1 2 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。

[0033] 撮像部 1 3 は、撮像素子、レンズ等により構成され、画像や動画の撮像を

実行する。本実施形態において、撮像部 13 は、バーコード、二次元コード、QRコード（登録商標）等の画像を撮像する。

[0034] 入力部 14 は、ユーザが各種入力を行い、通信装置 10 を操作するための入力インタフェースを提供する。

[0035] 表示部 15 は、各種表示を実行し、LCD (Liquid Crystal Display) や LED (Light Emitting Diode) のように視覚で認知可能な情報を出力する機能を有する。表示部 15 はまた、スピーカ等の音声出力が可能な機能を有してよい。

[0036] 表示部 15 は、視覚情報および音声情報の少なくとも一方を出力する機能を備える。

[0037] 視覚情報を表示する場合、表示部 15 は、表示すべき視覚情報に対応する画像データを保持する Video RAM (VRAM) を備える。表示部 15 は、この VRAM に格納した画像データを、LCD や LED に表示させ続ける表示制御を実行する。

[0038] 無線通信部 16 は、IEEE 802.11 シリーズに準拠した無線 LAN 通信を実行する。無線通信部 16 は、無線 LAN 通信を実行するチップにより構成されてよい。

[0039] アンテナ制御部 17 は、アンテナ 18 の出力制御を実行する。

[0040] アンテナ 18 は、無線 LAN で通信するための 2.4 GHz 帯および／または 5 GHz 帯で通信可能である。

[0041] なお、図 2 は通信装置 10 の構成の一例を示し、上記のモジュールのすべてを備えなくともよく、あるいは必要に応じて図示されるモジュールが省略されてもよい。

[0042] 例えば、通信装置 10 がプリンタ 4 である場合、図 2 に示すモジュールに加えて印刷部を備えてよい。あるいは通信装置 10 がアクセスポイント 1 である場合、図 2 に示すモジュールのうち、例えば撮像部 13 や表示部 15 は備えなくてよい。

[0043] <通信装置 10 の機能構成>

図3は、本実施形態に係る通信装置10の機能構成の一例を示すブロック図である。

[0044] 図3に示す通信装置10の各機能モジュールのうち、ソフトウェアにより実現される機能については、各機能モジュールの機能を提供するためのプログラムが記憶部12等のメモリに記憶され、RAMに読み出して制御部11が実行することにより実現される。ハードウェアにより実現される機能については、例えば、所定のコンパイラを用いることで、各機能モジュールの機能を実現するためのプログラムからFPGA上に自動的に専用回路を生成すればよい。FPGAとは、Field Programmable Gate Arrayの略である。また、FPGAと同様にしてGate Array回路を形成し、ハードウェアとして実現するようにしてもよい。また、ASIC (Application Specific Integrated Circuit) により実現するようにしてもよい。この場合、専用ハードウェアは制御部11の制御に基づいて動作する。

[0045] なお、図3に示した機能ブロックの構成は一例であり、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、いずれかの機能ブロックが複数の機能を行うブロックに分かれてもよい。

[0046] 通信装置10は、通信パラメータ制御部21、バーコード読み取り部22、バーコード生成部23、およびサービス制御部24を備える。通信装置10はさらに、パケット受信部25、パケット送信部26、ステーション機能部27、アクセスポイント機能部28、およびデータ記憶部29を備える。なお、通信装置10が図3のモジュール全てを備えることは必須でない。また、図3の通信装置10は、IEEE 802.11規格におけるステーション (STA) およびアクセスポイント (AP) のいずれとしても機能することができるが、STAおよびAPのいずれか一方のみで機能するよう構成されてもよい。

[0047] 通信パラメータ制御部21は、通信装置間で無線LAN通信のための通信パラメータを共有する通信パラメータ共有処理を実行する。この通信パラメ

ータ共有処理においては、通信パラメータを提供する通信装置（コンフィギュレータ）が、通信パラメータを受信する通信装置（エンローリ）に、無線LAN通信に必要な通信パラメータを提供する。提供される通信パラメータは、ネットワーク識別子としてのSSID（Service Set Identifier）、暗号方式、暗号鍵、認証方式、認証鍵等の無線LAN通信を行うために必要な無線通信パラメータを含む。提供される通信パラメータはまた、DPPに規定されるコネクタ、MACアドレス、PSK、パスフレーズ、IP層での通信を行うためのIPアドレス、上位サービスに必要な情報等を含んでもよい。

[0048] 本実施形態では、通信パラメータ制御部21が実行する通信パラメータ共有処理は、DPPであるものとして説明する。しかしながら、通信パラメータ制御部21が実行する通信パラメータ共有処理は、WPS（Wi-Fi Protected Setup）またはWi-Fi Directなど他のプロトコルに基づく処理であってもよく、DPPに限定されない。

[0049] バーコード読み取り部22は、撮像部13により撮像されたバーコード、QRコード（登録商標）などの二次元コード等の画像を解析し、符号化された情報を取得する。

[0050] 具体的には、本実施形態において、バーコード読み取り部22は、通信パラメータ共有処理を実行する際に使用される公開鍵を含むQRコード等のコード情報を撮像部13によって撮像し、撮像された画像を取得する。撮像すべきコード情報は、CP（Computer Purpose）コードまたはQRコードなどの二次元コード、またはバーコードなどの一次元コードであってもよい。

[0051] 本実施形態において、コード情報は、通信パラメータ共有処理で用いられる情報を含んでよい。この通信パラメータ共有処理で用いられる情報は、認証処理に用いられる公開鍵や通信装置の識別子等の情報を含む。なお、公開鍵は、通信パラメータ共有処理の際にセキュリティを高めるために用いられる情報であり、証明書、またはパスワードなどの情報であってもよい。この公

開鍵は、公開鍵暗号方式で用いられる暗号鍵の一種である。

- [0052] バーコード生成部 23 は、バーコード、QRコードなどの二次元コード等のコード情報を生成する。バーコード生成部 23 はまた、生成されたバーコード、QRコードなどの二次元コード等を表示部 15 に表示させるよう制御する。バーコード生成部 23 が生成するコード情報は、通信パラメータ共有処理を実行する際に使用される公開鍵や通信装置の識別子等の情報を含む。
- [0053] サービス制御部 24 は、アプリケーションレイヤにおけるアプリケーションを実行する。このアプリケーションレイヤとは、OS 参照モデル（7 層）における第 5 層以上の上位レイヤにおけるサービス提供層に相当する。すなわちサービス制御部 24 は、無線通信部 16 による無線通信を使用して、通信装置間で、例えば印刷、画像ストリーミング、ファイル転送等の各種アプリケーション処理を実行する。
- [0054] パケット受信部 25 およびパケット送信部 26 は、上位レイヤの通信プロトコルを含むあらゆるパケットの送受信を実行する。具体的には、パケット受信部 25 およびパケット送信部 26 は、無線通信部 16 を制御して、対向する他の通信装置との間で IEEE 802.11 規格に準拠したパケットの送信および受信を実行する。
- [0055] ステーション機能部 27 は、IEEE 802.11 規格に定められた、無線ネットワークを統括するアクセスポイント（AP）を介して通信するインフラストラクチャモードにおけるステーション（STA）として動作する STA 機能を提供する。ステーション機能部 27 は、STA として動作する際に、AP との間で、認証処理および暗号化処理等を実行する。
- [0056] アクセスポイント機能部 28 は、IEEE 802.11 規格に定められた上記インフラストラクチャモードにおけるアクセスポイント（AP）として動作する AP 機能を提供する。アクセスポイント機能部 28 は、無線ネットワークを形成し、STA に対する認証処理、暗号化処理、および STA の管理等の処理を実行する。
- [0057] データ記憶部 29 は、各種ソフトウェア、通信パラメータ、バーコード類

等の情報を記憶部 12 へ書き込み、および記憶部 12 からこれらの情報を読み出す。

[0058] なお、通信装置 10 が専らアクセスポイント 1 として動作する場合には、例えば、バーコード読み取り部 22 およびステーション機能部 27 等は省略されてよい。

[0059] <通信システムの通信装置間の動作シーケンス>

図 4 は、本実施形態に係る通信システムの各通信装置間の動作シーケンスの一例を示す図である。

[0060] 図 4 において、アクセスポイント 1 は、無線 LAN ネットワーク 3 を構築しており、スマートフォン 2 は、アクセスポイント 1 に接続可能な通信パラメータを保持しているものとする。

[0061] なお、スマートフォン 2 が通信パラメータを取得するには、アクセスポイント 1 が DPP に対応している場合には、DPP を用いた自動設定を用いればよい。一方、アクセスポイント 1 が DPP に非対応である場合は、WPS (Wi-Fi Protected Setup)、AOSS (AirStation One-Touch Secure System) (登録商標) 等の既存プロトコルを使用してよい。

[0062] 図 4 を参照して、アクセスポイント 1 およびプリンタ 4 をエンローリとして、スマートフォン 2 をコンフィギュレータとしてそれぞれ使用し、無線ネットワークを確立する場合を説明する。アクセスポイント 1 は AP であり、プリンタ 4 は STA である。

[0063] コンフィギュレータであるスマートフォン 2 は、無線ネットワークを構成するすべてのデバイスについて、DPP における通信パラメータの設定を管理する。

[0064] F1 で、スマートフォン 2 は、DPP に従って、まずアクセスポイント 1 への通信パラメータを設定する。

[0065] F2 で、スマートフォン 2 は、DPP に従って、プリンタ 4 への通信パラメータを設定する。なお、F1 および F2 における通信パラメータ設定の詳細

細はD P Pの仕様どおりであるためその詳細は省略する。

- [0066] F 1 およびF 2 により、コンフィギュレータであるスマートフォン2が、プリンタ4およびアクセスポイント1の2つのエンローリの通信パラメータを設定する処理が完了したことになる。なお、エンローリに設定されている通信パラメータの詳細は、例えば特許文献1に開示されている。
- [0067] F 1 およびF 2 でアクセスポイント1およびプリンタ4に通信パラメータがそれぞれ設定されると、F 3 で、設定された通信パラメータに基づいて、アクセスポイント1およびプリンタ4の間で、PMK (Pairwise Master Key) を生成する。このPMKは、アクセスポイント1とプリンタ4との間で安全な無線LAN通信を保証するために算出され、STAとAPとの間の無線通信で使用される暗号鍵の基となる事前共有鍵である。
- [0068] F 3 で生成されたPMKは、アクセスポイント1およびプリンタ4の間で共有され、F 4 およびF 5 で、アクセスポイント1およびプリンタ4のそれぞれに設定される。
- [0069] ここで、F 3 ないしF 5 で生成され設定されるPMKは、本実施形態で説明するようにD P Pの仕様に基づいて設定されてよい。あるいは、PMKは、WPA (Wi-Fi Protected Access) -PersonalやWPA-Enterpriseと称される無線LANセキュリティ規格に基づいて設定されてもよい。
- [0070] WPA-Personalに基づいてPMKを設定する場合、ユーザがPSK (Pre-shared Key) を設定し、ユーザにより設定されたPSKをそのままPMKに転用してよい。あるいは、WPA-Personalでは、SSIDと、パスフレーズと呼ばれる8文字以上63文字以内の文字列からPSKを算出し、算出されたPSKをPMKに転用してもよい。
- [0071] WPA-Enterpriseでは、IEEE 802.1X規格に基づき、RADIUSサーバからPMKを配布することができる。
- [0072] 上記のように、PMKを生成する方法にはいくつかの種別がある。このた

め、本実施形態に係る通信装置 10 では、PMK を生成するための情報を定義する PMK 管理テーブルを保有し、この PMK 管理テーブルを参照して PMK 情報を管理する。

[0073] 図 5 は、通信装置 10 が保有する PMK 管理テーブルの一例を示す図である。

[0074] 図 5 に示す PMK 管理テーブル 5 は、PMK ID 51、MAC アドレス 52、PMK 53、PMK 種別 (Type) 54、および有効期限 (Expiry) 55 の各フィールドを有する。

[0075] PMK ID 51 は、それぞれの PMK を一意に識別するためのハッシュ値であり、その詳細の仕様は IEEE 802.11 規格に準拠する。MAC アドレス 52 は、PMK ID 51 で特定される PMK を使用して無線通信を行うべき対向装置の MAC アドレスを示す。

[0076] PMK 53 は、通信装置 10 と対向装置との間で生成された PMK の値を示す。PMK 種別 (Type) 54 は、PMK ID 51 で特定される PMK 53 が、どの生成手法に基づいて生成されたかを識別する。この PMK 種別 54 は、例えば、AKM (Authentication and Key Management) 情報として示されてよい。PMK 種別 54 は、DPP による生成、WPA-Personal による生成、WPA-Enterprise による生成を識別するため、例えばそれぞれ、「DPP」、「PSK」、「1X」の値で記述することができる。

[0077] 有効期限 55 は、PMK ID 51 で特定される PMK 53 を使用可能な期限を日時で設定する。有効期限 55 は、図 5 に示すように、PMK 種別 54 が DPP である場合のみ値が設定される。

[0078] 本実施形態において、DPP で PMK が生成される場合、通信装置 10 は、コンフィギュレータから受信した通信パラメータに設定されている、当該通信装置が無線ネットワークへ接続する有効期限を、PMK 管理テーブル 5 の有効期限 55 に設定する。すなわち、PMK 管理テーブル 5 は、DPP で生成された PMK に、コンフィギュレータから設定された有効期限を対応付

けて記憶する。

[0079] 図4に戻り、F4およびF5で、アクセスポイント1およびプリンタ4の間で使用するPMKが設定されたため、F6で、IEEE802.11i規格ないしWPA規格に定められた4ウェイハンドシェイク処理を実行する。この4ウェイハンドシェイク処理を、事前に確定かつ共有されたPMKを使用して実行することにより、アクセスポイント1とプリンタ4のエンローリ間の無線通信で使用される暗号鍵が生成され、生成された暗号鍵を使用した暗号化通信が可能となる。

[0080] 次に、F6の4ウェイハンドシェイク処理実行後、アクセスポイント1とプリンタ4との間で暗号化通信を実行中に、F7で、アクセスポイント1とプリンタ4との間の接続が切断されたものとする。

[0081] この場合、その後にアクセスポイント1とプリンタ4との間の再接続処理において、F3ないしF5で設定されたPMKを使用して、無線LAN接続処理が実行される。

[0082] 具体的には、F8およびF9で、まず、プリンタ4は、F5で設定されたPMKのPMKID51を含む再接続要求をアクセスポイント1に送信する。なお、プリンタ4は、再接続要求を送信する前に、プリンタ4で管理するPMK管理テーブル5を参照し、DPPにより生成されたPMKの有効期限が経過している場合には、表示部15を介して接続エラーを通知して終了してもよい。あるいは、プリンタ4は、当該PMKの有効期限が経過している旨をアクセスポイント1に通知してもよい。

[0083] プリンタ4からPMKのPMKID51を含む再接続要求を受信したアクセスポイント1は、図5に示すPMK管理テーブル5を参照し、PMKID51で指定されるPMKのPMK種別54がDPPにより生成された場合は、有効期限55を参照する。

[0084] 再接続要求に含まれるPMKID51のPMKが、DPPにより生成されたPMKであって、有効期限55が有効期限内である場合、F10で、IEEE802.11i規格ないしWPA規格に定められた4ウェイハンドシェ

イク処理が実行される。

[0085] 再接続要求に含まれるPMK ID 51のPMKがDPP以外で生成され、PMK管理テーブル5に有効期限55が設定されていない場合も同様に、F10で、IEEE 802.11i規格ないしWPA規格に定められた4ウェイハンドシェイク処理が実行される。

[0086] この4ウェイハンドシェイク処理を、事前に確定かつ共有されたPMKを使用して実行することにより、アクセスポイント1とプリンタ4のエンローリ間の通信で使用される新たな暗号鍵が再生成され、再生成された暗号鍵を使用した暗号化通信が可能となる。

[0087] 一方、再接続要求に含まれるPMK ID 51のPMKが、DPPにより生成されたPMKであって、かつ有効期限55が経過している場合、アクセスポイント1はプリンタ4との間の再度の接続を規制し、4ウェイハンドシェイク処理を行わない。このPMKの有効期限切れの場合の処理の詳細は、図7を参照して後述する。

[0088] <PMK設定処理の詳細処理フロー>

図6は、図4のF3ないしF5のPMK生成および設定処理の詳細処理手順の一例を示すフローチャートである。

[0089] S61で、エンローリである通信装置10は、コンフィギュレータから、無線通信に必要となる通信パラメータを受信する。ここで、通信パラメータを受信するエンローリは、アクセスポイント1およびプリンタ4であり、コンフィギュレータは、スマートフォン2である。

[0090] S62で、エンローリである通信装置10は、S61で受信した通信パラメータに含まれる有効期限を取得し、有効期限が経過しているか否かを確認する。S61で受信した通信パラメータに含まれる有効期限がすでに経過している場合（S62：N）、S63でのエンローリ間での認証およびPMK生成処理をスキップして、処理を終了する。一方、S61で受信した通信パラメータに含まれる有効期限内である場合（S62：Y）、S63に進む。

[0091] S63で、アクセスポイント1（AP）とプリンタ4（STA）とのエン

ローリ間で、認証およびPMK生成処理を実行する。

[0092] 具体的には、S 6 3で実行されるPMK生成処理において、S 6 1でコンフィギュレータから受信した通信パラメータの中の一部の要素に基づいて、予め定められた算出方法に従い、アクセスポイント1およびプリンタ4の間で共有すべきPMKを算出する。PMK算出の具体的な詳細はDPP仕様書に記載されているため省略する。

[0093] S 6 4で、エンローリである通信装置10は、PMK管理テーブル5に、S 6 3で算出されたPMKのエントリとして、PMK ID 5 1、対向装置のMACアドレス5 2、およびPMK 5 3を設定する。エンローリである通信装置10はさらに、S 6 3で算出されたPMKのエントリとして、PMK種別5 4に「DPP」を設定し、有効期限（E x p i r y）5 5には、ステップS 6 1で受信した通信パラメータに含まれていた有効期限を設定する。

[0094] 以上のS 6 1からS 6 4の処理を実行することにより、コンフィグレータが設定した、エンローリが無線通信に接続する有効期限の情報を、エンローリである通信装置間の無線通信の接続処理に引き継ぐことが可能となる。

[0095] <エンローリ間の接続処理の詳細処理フロー>

図7は、図4のF 8ないしF 10のエンローリ間（APとSTA間）での接続処理の詳細処理手順の一例を示すフローチャートである。図7を参照して、通信装置10であるプリンタ4（STA）がアクセスポイント1（AP）に再接続する例を説明する。

[0096] S 7 1で、エンローリ（STA）であるプリンタ4は、アクセスポイント1（AP）への再接続処理を実行する際に、前回アクセスポイント1へ接続した際のPMK ID 5 1を使用して、PMK管理テーブル5中のPMK種別5 4（AKM情報）を参照する。

[0097] 前回接続時のPMK ID 5 1のPMK種別5 4がDPPである場合（S 7 1：Y）、S 7 2に進んで、PMKが有効期限内か否かを判定する。一方、前回接続時のPMK ID 5 1のPMK種別5 4がDPP以外である場合（S

7 1 : N) 、 S 7 2 をスキップして、 S 7 3 へ進む。

[0098] S 7 2 で、プリンタ 4 は、前回接続時の PMK I D 5 1 をキーに PMK 管理テーブル 5 を参照して、 PMK の有効期限 (E x p i r y) 5 5 を確認する。 PMK が有効期限内であるもしくは有効期限が設定されていない場合 (S 7 2 : Y) 、 S 7 3 で、プリンタ 4 は、接続先の AP (アクセスポイント 1) を検索する。一方、 PMK の有効期限が経過している場合 (S 7 2 : N) 、 S 7 5 に進む。

[0099] S 7 3 で接続先の AP を検索した結果、 AP の存在が確認されると、 S 7 4 で、アクセスポイント 1 (AP) とプリンタ 4 (S T A) との間で、 I E E E 8 0 2 . 1 1 規格に従った認証処理、アソシエーション処理を実行した上で、 4 ウェイハンドシェイク処理を実行する。

[0100] S 7 2 に戻り、 PMK の有効期限が経過している場合 (S 7 2 : N) 、 S 7 5 で、プリンタ 4 は、表示部 1 5 に接続エラーを表示して、アクセスポイント 1 への再接続処理を実行することなく処理を終了する。

[0101] S 7 5 で、表示部 1 5 に接続エラーを表示させる場合、再度通信パラメータ設定からやり直してよい。通信パラメータ設定をやり直す手順としては、表示部 1 5 に通信パラメータ設定を設定するようユーザに促すメッセージを表示してもよく、ユーザの指示なく自動的にコンフィギュレータと通信を実行して通信パラメータを取得してもよい。

[0102] 図 8 は、通信装置 1 0 における無線 LAN 接続先情報を表示する W i - F i 設定メニュー 8 0 のユーザインタフェースの一例を示す。図 8 において、扇型マークの表示は無線 LAN であることを示し、その左に S S I D が表示されている。当該 S S I D が、 W E P / W P A / W P A 2 / D P P 等により無線 LAN 通信時に暗号化する場合は、 S S I D に対応して鍵マークを表示する。

[0103] 図 7 の S 7 5 で説明したとおり、 PMK の有効期限が経過している場合は、表示部 1 5 に「有効期限切れ (e x p i r e d) 」等と表示して、ユーザが有効期限切れとなった無線 LAN 接続先 8 1 を選択できないよう入力を

規制すればよい。あるいは有効期限切れとなった無線LAN接続先81を選択しようとした場合、通信パラメータの再設定を促してもよい。

[0104] あるいは、PMKの有効期限が経過した無線LAN接続先の情報を、Wi-Fi設定メニュー80の選択肢から削除してもよいし、PMKの有効期限が経過した無線LAN接続先との暗号鍵の情報自体を削除して自動または手動での接続対象外としてもよい。

[0105] 以上説明したように、本実施形態によれば、通信装置は、コンフィギュレータから提供された通信パラメータから、無線ネットワークへ接続する有効期限を取得する。そして、通信装置は、通信相手の通信装置と接続する際に、取得された有効期限が経過したか否かを判定し、有効期限が経過した場合には、暗号鍵情報を使用した通信相手の通信装置との接続を規制する。

[0106] これにより、無線通信に必要な通信パラメータを保持するコンフィギュレータから提供される通信パラメータに設定された有効期限を、エンローリ間で共有すべき暗号鍵情報にも適用可能となる。従って、コンフィギュレータが設定した無線ネットワークへ接続する有効期限を、コンフィギュレータが介在しないエンローリ間の接続においても有効化され、有効期限を適切に用いた暗号化無線通信が実現する。

[0107] (実施形態2)

以下、実施形態2を、図9および図10を参照して、上記の実施形態1と異なる点についてのみ詳細に説明する。実施形態1では、DPPにおける通信パラメータ設定およびPMK設定の各処理を実行した後、無線LANによる暗号化通信を実行し、再接続時に有効期限を確認する例を説明した。これに対して、本実施形態では、再接続すべき事象が発生していなくても、周期的にPMKに設定された有効期限を確認し、有効期限が到来した時点で、ユーザに通知するとともに無線LAN通信を切断する。

[0108] これにより、コンフィギュレータが介在しないエンローリ間の無線通信接続中であっても、コンフィギュレータが設定した無線ネットワーク接続の有効期限を有効化し、有効期限の到来をユーザに迅速に認識させることが可能

となる。

[0109] 実施形態2に係る通信装置10のハードウェア構成および機能構成は、図2および図3にそれぞれ示される実施形態1と同様である。

[0110] 実施形態2に係る通信装置10が実行する動作シーケンスは、図4に示される実施形態1と同様である。

[0111] <実施形態におけるPMK有効期限確認処理の詳細処理フロー>

図9は、本実施形態において、通信装置10が実行するPMKの有効期限確認および無線LAN通信の切断処理の詳細処理手順の一例を示すフローチャートである。

[0112] S91で、エンローリである通信装置10は、PMKに有効期限が設定されている場合、所定の周期で、PMK管理テーブル5を参照して、現在、対向する他のエンローリである通信装置との間の無線通信で使用しているPMKの有効期限55を確認する。

[0113] S92で、現在使用しているPMKの有効期限55が有効期限内である場合（S92：N）、通信装置10は、S94で所定の時間待機した後、S91に戻り、PMKの有効期限を確認する処理を繰り返す。

[0114] 一方、現在使用しているPMKの有効期限55が経過している場合（S92：Y）、S93に進んで、自装置が無線ネットワーク上で、APモードとSTAモードのいずれで動作しているかを判定する。

[0115] S93で、通信装置10は、自装置がアクセスポイント（AP）モードで動作している場合（S93：AP）、S95に進み、APに接続中であるSTAとの接続をすべて切断する。具体的には、S95で、通信装置10は、接続中であるSTAに、deathパケットを送信することにより、すべてのSTAとの接続を切断してよい。

[0116] S96で、通信装置10は、すべてのSTAとの接続を切断した後、自装置のアクセスポイント（AP）としての機能を停止する。S96では、AP機能を停止する際に、表示部15を介して、ネットワーク機能（AP機能）を終了させる旨をユーザに通知してもよい。

[0117] 一方、ステップS 9 3に戻り、通信装置1 0は、自装置がステーション（S T A）モードで動作している場合（S 9 3：S T A）、S 9 7に進み、自装置のステーション（S T A）としての機能を停止する。

[0118] S 9 7では、例えば、図1 0のユーザインタフェース8 2の例に示すように、接続先へのアクセス有効期限が終了した旨の表示8 3を表示部1 5を介して通知し、さらにネットワーク機能を終了させる旨の通知を表示してよい。通信装置1 0は、これらの通知をユーザに提示した後、接続中のA Pとの接続を切断し、自装置のステーション（S T A）としての動作を終了すればよい。

[0119] あるいは、自装置がS T Aモードで動作している場合、通信装置1 0は、ステーション（S T A）としての動作は継続したまま、表示部1 5にP M Kの有効期限が切れた旨のみを通知し、ユーザにネットワークからの切断をするか否かを判断させてもよい。

[0120] 以上説明したように、本実施形態によれば、通信装置1 0は、周期的にP M Kに設定された有効期限を確認し、有効期限が到来した時点で、ユーザに通知するとともに無線L A N通信を切断する。

[0121] これにより、コンフィギュレータが介在しないエンローリ間の無線通信接続中であっても、コンフィギュレータが設定した無線ネットワーク接続の有効期限を有効化し、有効期限の到来をユーザに迅速に認識させることが可能となる。

[0122] <他の実施形態>

上記の各実施形態においては、Q Rコード等の画像（コード情報）を読み取っ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送受信する例を説明した。しかしながら、Q Rコード等を撮像することに替えて、N F C（N e a r F i e l d C o m m u n i c a t i o n）やB l u e t o o t h（登録商標）等の無線通信を用いて通信パラメータを設定してもよい。あるいは、I E E E 8 0 2 . 1 1 a d規格もしくはトランスファージェット（T r a n s f e r J e t）（登録商標）等による無線通信を用いてもよい。

。

[0123] QRコードを読み取る場合、表示部15に表示されているQRコードだけでなく、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コードを読み取ってもよい。あるいは、取り扱い説明書や通信機器の販売時の梱包や包装に貼り付けられているQRコードを読み取ってもよい。QRコードに替えて、一次元のバーコード、QRコード以外の二次元コードを読み取ってもよい。さらに、QRコードなどの機械可読な情報に替えて、ユーザが読み取れる形態の情報であってもよい。

[0124] また、上記の各実施形態においては、通信装置間で、IEEE802.11準拠の無線LAN通信を実行する例を説明したが、本実施形態はこれに限定されない。IEEE802.11準拠の無線LAN通信に替えて、例えば、近距離の無線通信方式であるUWB(Ultra Wide Band)を用い、例えばワイヤレスUSB(Universal Serial Bus)により無線通信を実行してもよい。あるいは、Bluetooth、ZigBee、NFC等の無線通信方式で無線通信を実行してもよい。UWBでは、ワイヤレスUSBの他、ワイヤレス1394、WINET等を利用することができる。

[0125] また、上記の各実施形態においては、インフラストラクチャモードにおいて、無線LANのアクセスポイント(AP)が無線通信用の通信パラメータを提供する例を説明したが、これに限定されない。アクセスポイント(AP)を介さない無線通信において、例えば、Wi-Fi Direct(登録商標)のグループオーナーが、無線通信用の通信パラメータを提供してもよい。

[0126] なお、上述した各実施形態は、その複数を組み合わせたり、適宜改良乃至はそれを応用した形態としてもよい。

[0127] 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がプログラムを読み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。

[0128] また、上述した各実施形態を、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。

[0129] 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。

[0130] 上述の実施形態によれば、無線ネットワークへの接続の有効期限が設定された通信装置において、設定された有効期限に基づいて他の通信装置との無線通信を適切に実行することができる。

[0131] 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。

[0132] 本願は、2018年9月13日提出の日本国特許出願特願2018-171689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] 無線ネットワークを介した第1の通信装置との無線通信の通信パラメータを第2の通信装置から受信する受信手段と、
- 前記受信手段により受信された前記通信パラメータに基づいて、前記第1の通信装置との間で共有すべき暗号鍵情報を生成する生成手段と、
- 前記受信手段により受信された前記通信パラメータから、前記無線ネットワークへ接続する有効期限を取得する取得手段と、
- 前記生成手段により生成された前記暗号鍵情報を使用して、前記第1の通信装置と前記無線ネットワークを介して接続する接続手段と、
- 前記取得手段により取得された前記有効期限が経過したか否かを判定し、前記有効期限が経過した場合には、前記暗号鍵情報を使用した前記第1の通信装置との接続を規制するよう、前記接続手段を制御する制御手段と、
- を備えることを特徴とする通信装置。
- [請求項2] 前記生成手段により生成された前記暗号鍵情報に、前記取得手段により取得された前記有効期限を対応付けて記憶する記憶手段をさらに備え、
- 前記制御手段は、前記記憶手段に記憶された前記有効期限を参照することにより、前記有効期限が経過したか否かを判定する、
- ことを特徴とする請求項1に記載の通信装置。
- [請求項3] 前記接続手段は、前記第1の通信装置に接続する際に、前記生成手段により事前に生成された前記暗号鍵情報から、前記第1の通信装置との間の無線通信を暗号化する暗号鍵を生成する、
- ことを特徴とする請求項1または2に記載の通信装置。
- [請求項4] 前記制御手段は、前記第1の通信装置に接続する際に、前記有効期限が経過したか否かを判定し、前記有効期限が経過した場合には、前記接続手段に、前記第1の通信装置に接続させない、

ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載の通信装置

。

[請求項5] 前記制御手段は、所定の周期で前記有効期限が経過したか否かを判定し、前記有効期限が経過した場合には、前記接続手段に、前記第 1 の通信装置との間の無線通信を切断させる、

ことを特徴とする請求項 1 から 4 のいずれか 1 項に記載の通信装置

。

[請求項6] 前記制御手段は、前記有効期限が経過した場合に、前記無線ネットワークへ接続する前記有効期限が経過した旨の通知を表示装置に表示させ、前記無線ネットワークが接続先として選択されないよう入力を規制する、

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] 前記制御手段は、前記有効期限が経過した場合に、前記有効期限が経過した前記無線ネットワークを表示装置に表示させないように制御する、

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8] 前記暗号鍵情報は、IEEE 802.11 規格に準拠する Pairwise Master Key (PMK) である、

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] 前記通信パラメータは、Device Provisioning Protocol (DPP) により、前記第 1 の通信装置から前記通信装置に設定される、

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] 前記制御手段は、前記通信装置が IEEE 802.11 規格に準拠

するアクセスポイント（ＡＰ）として動作する場合、前記接続手段に、前記通信装置に接続しているすべての第１の通信装置との無線通信を切断させて、前記アクセスポイントの機能を停止させるよう、前記第１の通信装置との接続を規制する、

ことを特徴とする請求項１から９のいずれか１項に記載の通信装置。

[請求項11] 前記制御手段は、前記通信装置がＩＥＥＥ８０２．１１規格に準拠するステーション（ＳＴＡ）として動作する場合、前記無線ネットワークへ接続する前記有効期限が経過した旨の通知を表示装置に表示させる、

ことを特徴とする請求項１から９のいずれか１項に記載の通信装置。

[請求項12] 前記第１の通信装置は、Device Provisioning Protocol（ＤＰＰ）におけるエンローリであり、前記第２の通信装置は、ＤＰＰにおけるコンフィギュレータである、

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] 無線ネットワークを介した第１の通信装置との無線通信の通信パラメータを第２の通信装置から受信するステップと、

受信された前記通信パラメータに基づいて、前記第１の通信装置との間で共有すべき暗号鍵情報を生成するステップと、

受信された前記通信パラメータから、前記無線ネットワークへ接続する有効期限を取得するステップと、

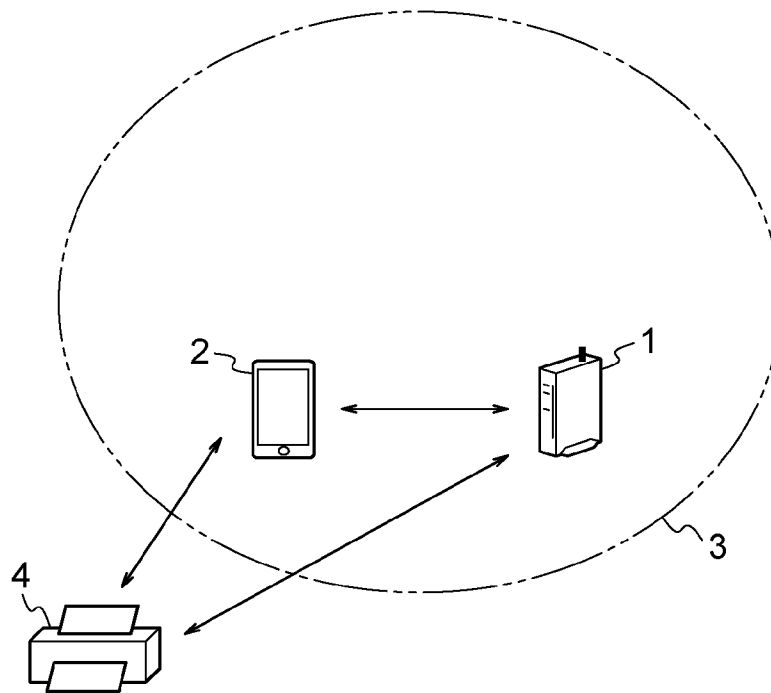
生成された前記暗号鍵情報を使用して、前記第１の通信装置と前記無線ネットワークを介して接続するステップと、

取得された前記有効期限が経過したか否かを判定し、前記有効期限が経過した場合には、前記暗号鍵情報を使用した前記第１の通信装置との接続を規制するステップと、

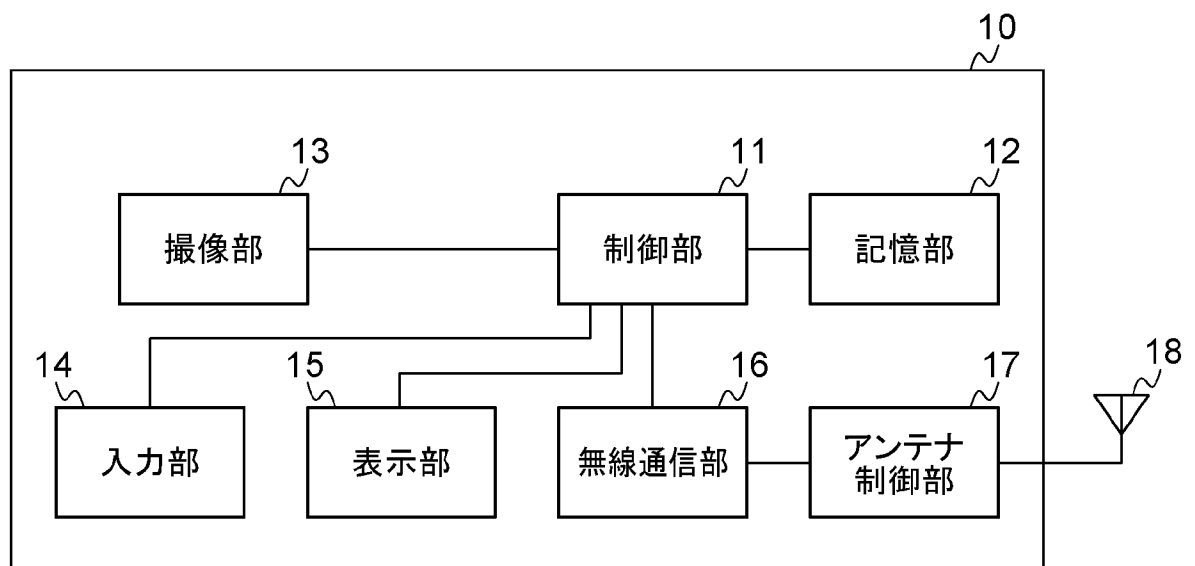
を備えることを特徴とする通信装置の制御方法。

[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。

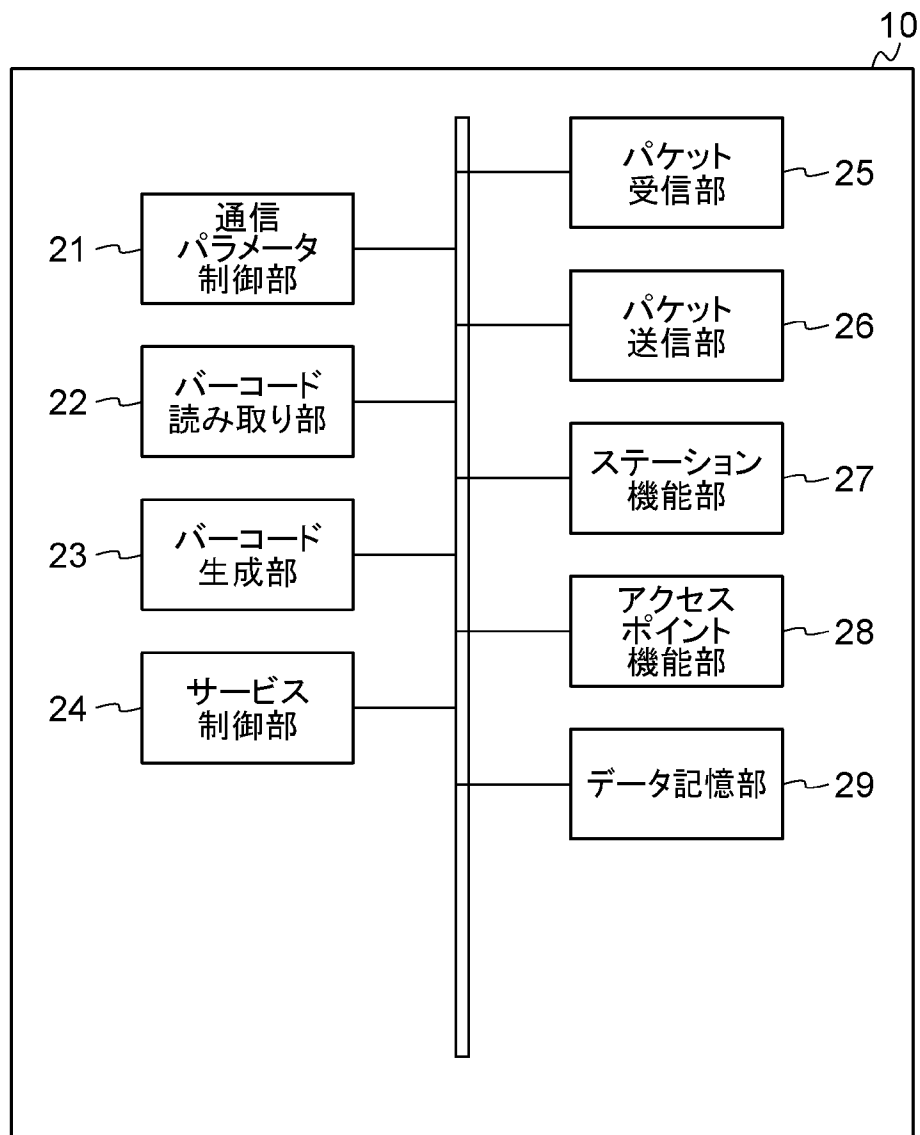
[図1]



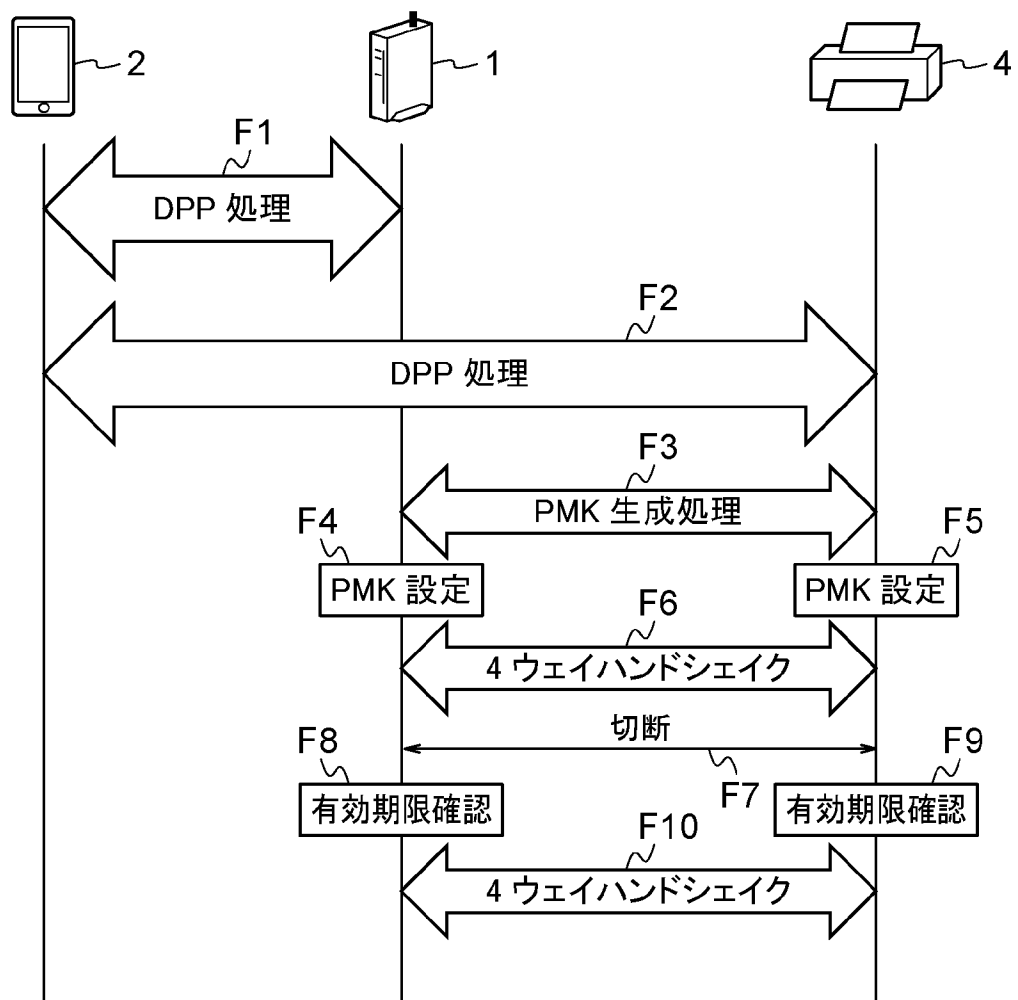
[図2]



[図3]



[図4]

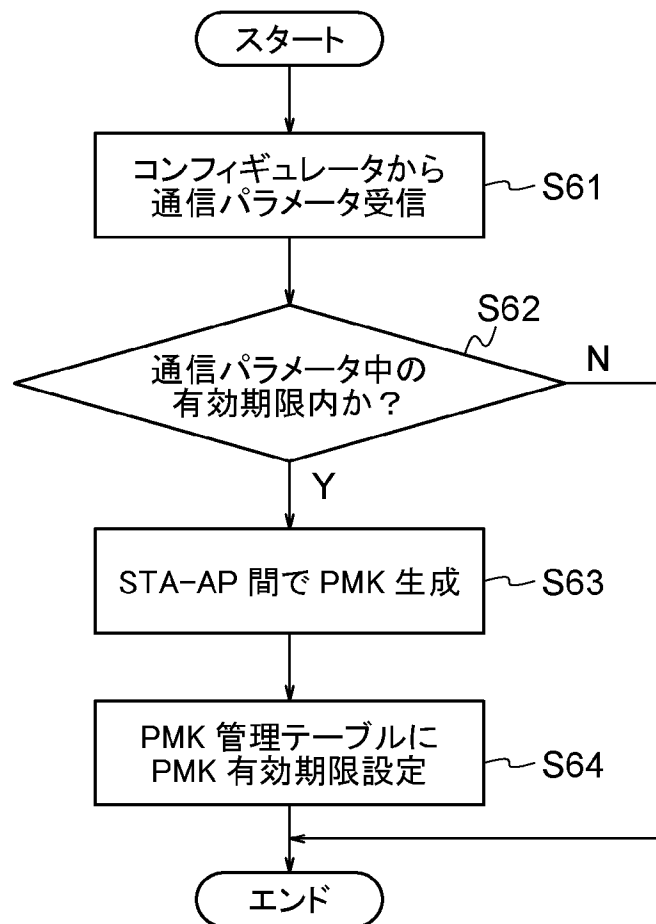


[図5]

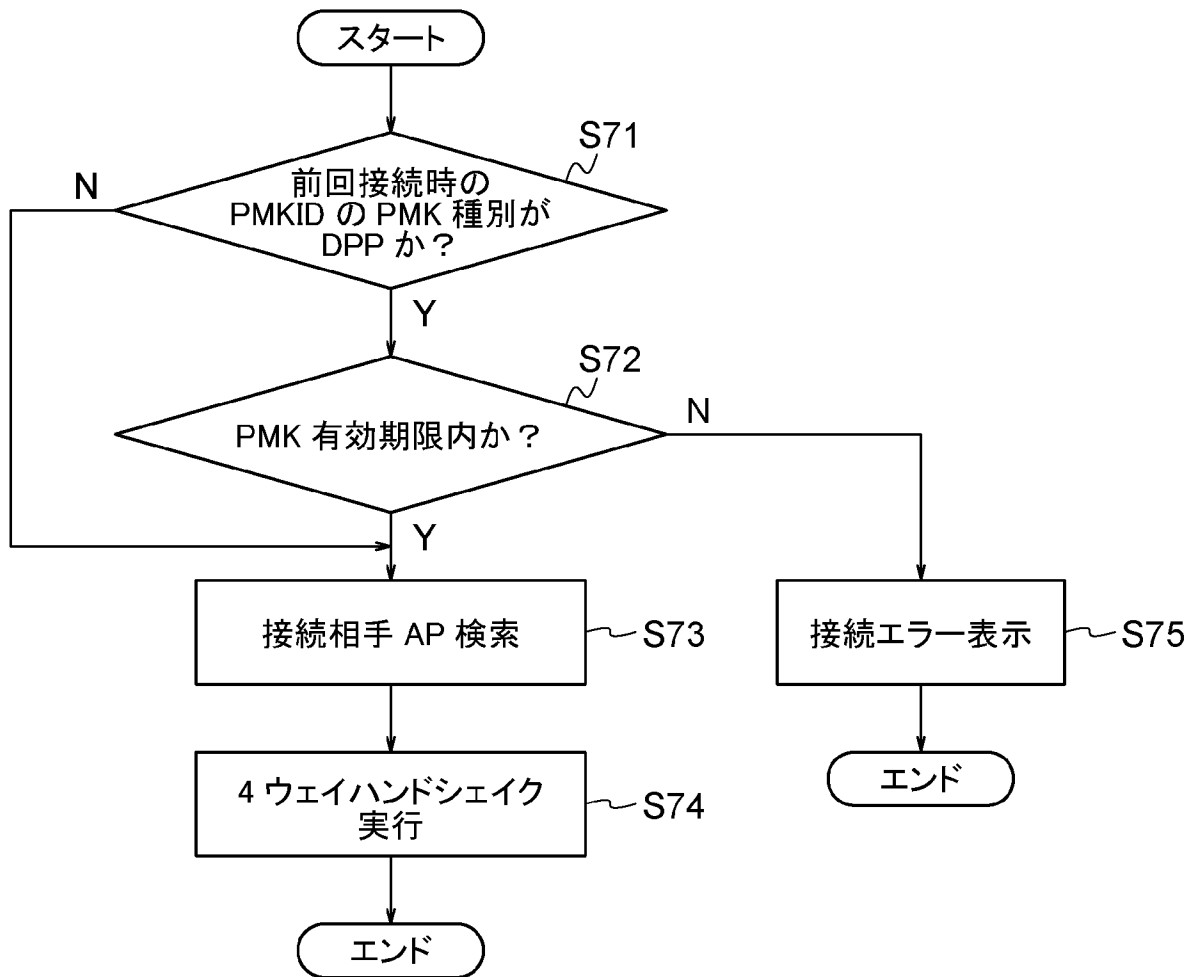
5

51 PMKID	52 MACアドレス	53 PMK	54 PMK種別	55 有効期限
1234567890123456789012	65:55:55:44:33:22	xx...xx	DPP	yy/mm/dd hh:mm:ss
:	:	:	PSK	N/A
:	:	:	1X	N/A

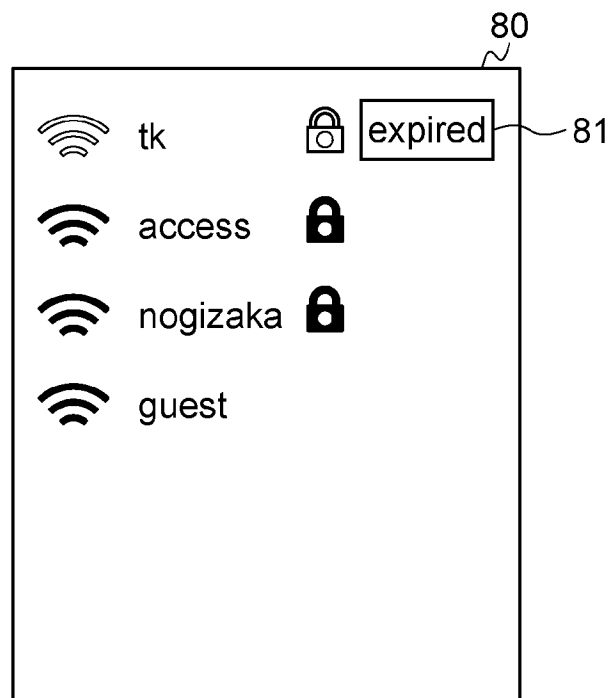
[図6]



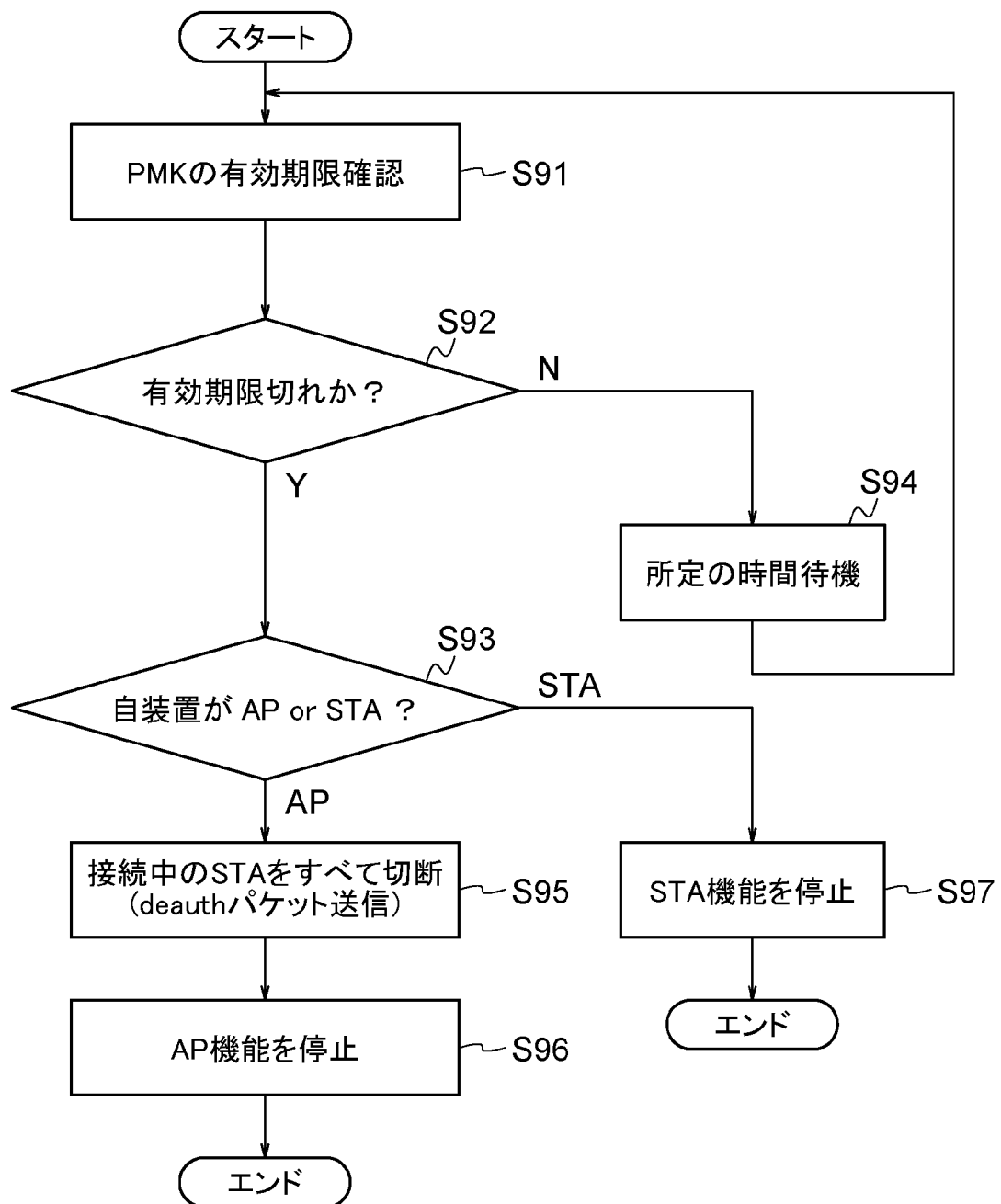
[図7]



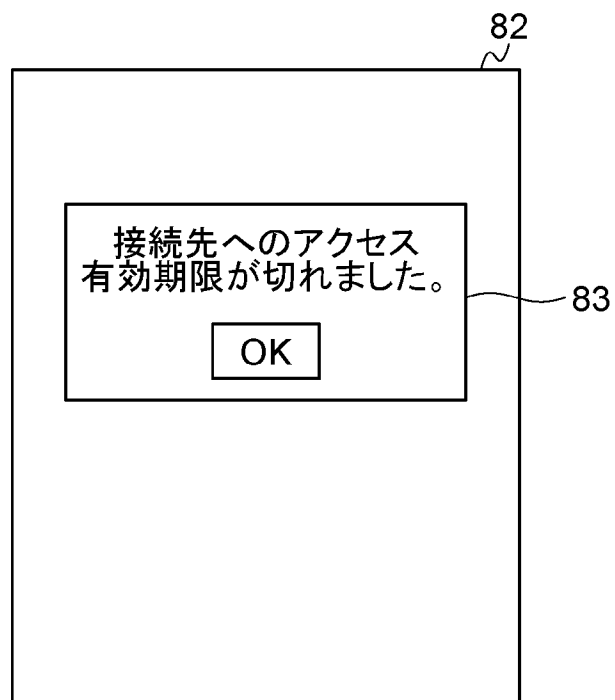
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/034434

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04W76/38 (2018.01) i, H04W12/04 (2009.01) i, H04W48/02 (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)

Int.Cl. H04W4/00-99/00

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
Y	JP 2011-040820 A (BUFFALO CO., LTD.) 24 February 2011, paragraphs [0026], [0037], [0058]-[0062] & US 2011/0033052 A1, paragraphs [0033], [0044], [0065]-[0069] & CN 101998391 A	1-14
Y	JP 2005-286941 A (FUJI PHOTO FILM CO., LTD.) 13 October 2005, paragraphs [0032]-[0034] (Family: none)	1-14
A	JP 2014-140101 A (NEC ACCESS TECHNICA, LTD.) 31 July 2014, entire text, all drawings (Family: none)	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
07 November 2019 (07.11.2019)

Date of mailing of the international search report
19 November 2019 (19.11.2019)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04W76/38(2018.01)i, H04W12/04(2009.01)i, H04W48/02(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 (IPC))

Int.Cl. H04W4/00-99/00

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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
Y	JP 2011-040820 A (株式会社バッファロー) 2011.02.24, [0026], [0037], [0058]-[0062] & US 2011/0033052 A1, [0033], [0044], [0065]-[0069] & CN 101998391 A	1-14
Y	JP 2005-286941 A (富士写真フイルム株式会社) 2005.10.13, [0032]-[0034] (ファミリーなし)	1-14
A	JP 2014-140101 A (NECアクセステクニカ株式会社) 2014.07.31, 全文, 全図 (ファミリーなし)	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

07.11.2019

国際調査報告の発送日

19.11.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

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)

齋藤 浩兵

電話番号 03-3581-1101 内線 3534

5 J

3794