

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6789628号  
(P6789628)

(45) 発行日 令和2年11月25日 (2020. 11. 25)

(24) 登録日 令和2年11月6日 (2020. 11. 6)

(51) Int. Cl. F I  
**HO 4 W 76/10 (2018. 01)** HO 4 W 76/10  
**HO 4 W 12/02 (2009. 01)** HO 4 W 12/02  
**HO 4 W 12/06 (2009. 01)** HO 4 W 12/06  
**HO 4 W 84/12 (2009. 01)** HO 4 W 84/12  
**HO 4 W 88/08 (2009. 01)** HO 4 W 88/08

請求項の数 16 (全 14 頁)

(21) 出願番号 特願2015-246899 (P2015-246899)  
 (22) 出願日 平成27年12月18日 (2015. 12. 18)  
 (65) 公開番号 特開2017-112552 (P2017-112552A)  
 (43) 公開日 平成29年6月22日 (2017. 6. 22)  
 審査請求日 平成30年11月21日 (2018. 11. 21)

(73) 特許権者 000001007  
 キヤノン株式会社  
 東京都大田区下丸子3丁目30番2号  
 (74) 代理人 100126240  
 弁理士 阿部 琢磨  
 (74) 代理人 100124442  
 弁理士 黒岩 創吾  
 (72) 発明者 ▲浜▼地 俊文  
 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

審査官 横田 有光

最終頁に続く

(54) 【発明の名称】 通信装置、制御方法、および、プログラム

(57) 【特許請求の範囲】

【請求項 1】

基地局であって、

他の基地局が構築する第1の無線ネットワークの識別子と第1のセキュリティ情報とを  
 含む第1の通信パラメータを第1の通信装置から受信する受信手段と、

前記第1のセキュリティ情報において定められるセキュリティ方式を、セキュリティ強  
 度の高いセキュリティ方式に変更した第2のセキュリティ情報を生成する生成手段と、

前記識別子と前記第2のセキュリティ情報とを含む第2の通信パラメータを利用し、前  
 記識別子を有する第2の無線ネットワークを構築する構築手段と、

前記第1の通信装置からの通知に基づいて、前記第2の通信パラメータを前記第1の通  
 信装置とは異なる第2の通信装置に提供する提供手段と、

を有することを特徴とする基地局。

【請求項 2】

前記第1の通信装置を認証する認証手段を更に有し、

前記認証に成功した場合に、前記受信手段は、前記第1の通信パラメータを前記第1の  
 通信装置から受信することを特徴とする請求項1に記載の基地局。

【請求項 3】

前記第1の通信装置を認証するために利用する認証情報を表示する表示手段を更に有し

、  
 前記認証手段は、前記第1の通信装置から受信した認証情報に基づいて、前記第1の通

10

20

信装置を認証することを特徴とする請求項 2 に記載の基地局。

【請求項 4】

前記表示手段は、前記認証情報を含む 1 次元もしくは 2 次元のコードを表示することを特徴とする請求項 3 に記載の基地局。

【請求項 5】

前記構築手段は、前記第 2 の通信パラメータを利用する前記第 2 の無線ネットワークを構築すると共に、前記第 1 の通信パラメータを利用する第 3 の無線ネットワークを構築することを特徴とする請求項 1 から 4 のいずれか 1 項に記載の基地局。

【請求項 6】

前記第 2 の通信装置の機能情報を取得する取得手段と、

10

前記機能情報に基づいて、前記第 1 の通信パラメータと前記第 2 の通信パラメータのいずれを前記第 2 の通信装置に提供するかを選択する選択手段と、

を更に有し、

前記提供手段は、前記選択手段により選択された通信パラメータを前記第 2 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 項に記載の基地局。

【請求項 7】

前記第 1 のセキュリティ情報は、暗号方式、認証方式、暗号鍵、認証鍵の少なくともいずれか 1 つを含むことを特徴とする請求項 1 から 6 のいずれか 1 項に記載の基地局。

【請求項 8】

前記第 2 の無線ネットワークは、IEEE 802.11 シリーズ規格に準拠した無線通信を行うネットワークであることを特徴とする請求項 1 から 7 のいずれか 1 項に記載の基地局。

20

【請求項 9】

前記基地局は IEEE 802.11 シリーズ規格に規定されたインフラストラクチャモードのアクセスポイントであることを特徴とする請求項 1 から 8 のいずれか 1 項に記載の基地局。

【請求項 10】

前記基地局は Wi-Fi Direct 規格に規定された Group Owner であることを特徴とする請求項 1 から 8 のいずれか 1 項に記載の基地局。

【請求項 11】

30

前記生成手段は、前記第 1 のセキュリティ情報において定められる暗号方式を、暗号強度の高い暗号方式に変更した前記第 2 のセキュリティ情報を生成することを特徴とする請求項 1 から 10 のいずれか 1 項に記載の基地局。

【請求項 12】

前記生成手段は、TKIP (Temporal Key Integrity Protocol) を利用する前記第 1 のセキュリティ情報に基づいて、AES (Advanced Encryption Standard) を利用する前記第 2 のセキュリティ情報を生成することを特徴とする請求項 1 から 11 のいずれか 1 項に記載の基地局。

【請求項 13】

前記生成手段は、前記第 1 のセキュリティ情報において定められる認証方式を、認証強度の高い認証方式に変更した前記第 2 のセキュリティ情報を生成することを特徴とする請求項 1 から 12 のいずれか 1 項に記載の基地局。

40

【請求項 14】

前記生成手段は、WPA1 (Wi-Fi Protected Access 1) を利用する前記第 1 のセキュリティ情報に基づいて、WPA2 (Wi-Fi Protected Access 2) を利用する前記第 2 のセキュリティ情報を生成することを特徴とする請求項 1 から 13 のいずれか 1 項に記載の基地局。

【請求項 15】

無線ネットワークの構築方法であって、

他の基地局が構築する第 1 の無線ネットワークの識別子と第 1 のセキュリティ情報とを

50

含む第1の通信パラメータを第1の通信装置から受信する受信工程と、

前記第1のセキュリティ情報において定められるセキュリティ方式を、セキュリティ強度の高いセキュリティ方式に変更した第2のセキュリティ情報を生成する生成工程と、

前記識別子と前記第2のセキュリティ情報とを含む第2の通信パラメータを利用し、前記識別子を有する第2の無線ネットワークを構築する構築工程と、

前記第1の通信装置からの通知に従って、前記第2の通信パラメータを前記第1の通信装置とは異なる第2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構築方法。

【請求項16】

コンピュータを請求項1から14のいずれか1項に記載の基地局として動作させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、基地局と通信する通信装置に関する。

【背景技術】

【0002】

無線ネットワークに接続するには、無線ネットワークの識別子や暗号方式、認証方式、暗号鍵、認証鍵等の通信パラメータを設定した上で、接続処理を行う必要がある。しかしながら、通信パラメータを手動で設定するのは煩雑な操作が必要であった。

【0003】

特許文献1には、無線ネットワークを構築する基地局から通信パラメータを受信し、自装置に設定することにより、簡単に無線ネットワークに接続できる構成が開示されている。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2002-159053号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

既存の基地局から新規の基地局へ、基地局を置き換える場合、新規の基地局においても同じ識別子の無線ネットワークを構築して欲しいという要望がある。ユーザが見慣れた識別子の方が、接続する無線ネットワークとして認識しやすいためである。

【0006】

また、新規の基地局においてはよりセキュリティ強度の高い無線ネットワークを構築したいという要望がある。

【0007】

上記課題を解決するために、第1の基地局が構築する無線ネットワークの識別子を有するセキュリティ強度のより高い他の無線ネットワークを第2の基地局が簡単に構築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】

【0008】

本発明の基地局は、他の基地局が構築する第1の無線ネットワークの識別子と第1のセキュリティ情報とを含む第1の通信パラメータを第1の通信装置から受信する受信手段と、前記第1のセキュリティ情報において定められるセキュリティ方式を、セキュリティ強度の高いセキュリティ方式に変更した第2のセキュリティ情報を生成する生成手段と、前記識別子と前記第2のセキュリティ情報とを含む第2の通信パラメータを利用し、前記識別子を有する第2の無線ネットワークを構築する構築手段と、を有する。

【発明の効果】

10

20

30

40

50

## 【0009】

本発明によれば、第1の基地局が構築する無線ネットワークの識別子を有すると共にセキュリティ強度のより高い他の無線ネットワークを第2の基地局が簡単に構築することができる。

## 【図面の簡単な説明】

## 【0010】

【図1】無線ネットワーク構成図

【図2】管理装置のハードウェア構成図

【図3】管理装置のソフトウェア機能ブロック図

【図4】基地局のソフトウェア機能ブロック図

10

【図5】基地局が実現するフローチャート

【図6】シーケンスチャート

【発明を実施するための形態】

## 【0011】

以下、本実施形態について、図面を参照しながら詳細に説明する。以下では、IEEE 802.11シリーズ規格（以下、802.11規格）に準拠した無線LANシステムを用いた例について説明する。しかしこれに限らず、Bluetooth（登録商標）、ZigBee等の他の無線通信方式に準拠した無線LANシステムにも適用可能である。

## 【0012】

なお、IEEEは、The Institute of Electrical and Electronics Engineers, Inc. の略である。また、LANはLocal Area Networkの略である。

20

## 【0013】

図1に、管理装置101、第1のアクセスポイント102（以下、AP1）、ステーション103（以下、STA1）、ステーション104（以下、STA2）、および、第2のアクセスポイント105（以下、AP2）を含むネットワークシステムを示す。

## 【0014】

AP1は、802.11規格に規定されたインフラストラクチャモード（Infrastructure mode）のアクセスポイントであり、無線ネットワーク106（以下、ネットワーク1）を構築する。なお、AP1が、Wi-Fi Direct規格に規定されたGroup Ownerとして無線ネットワーク106（以下、ネットワーク1）を構築してもよい。即ち、AP1は基地局として動作する。

30

## 【0015】

管理装置101、STA1、および、STA2は、ネットワーク1に接続するステーション（端末装置）として動作する。AP2は基地局として無線ネットワーク107（以下、ネットワーク2）を構築する。

## 【0016】

図2に、本実施形態のAP2のハードウェア構成を示す。なお、管理装置101、AP1、STA1、およびSTA2も同様のハードウェア構成を有するものとする。

## 【0017】

40

制御部201はCPU、または、MPUにより構成され、記憶部202に記憶されたプログラムを実行することによりAP2全体を制御する。また、制御部201は、他の通信装置との間で通信パラメータの設定処理を行う。なお、制御部201が実行しているOS（Operating System）との協働によりAP2全体を制御するようにしてもよい。

## 【0018】

記憶部202はROMやRAMにより構成され、後述する各種動作を行うためのプログラムや、無線通信のための通信パラメータ等の各種情報を記憶する。ここで、通信パラメータには、無線ネットワークに接続するためのパラメータとして、無線ネットワークの識別子（例えば、SSID）、および、セキュリティ情報が含まれる。セキュリティ情報に

50

は、暗号方式、暗号鍵、認証方式、および、認証鍵の情報が含まれる。なお、通信パラメータとして、前述したいずれか1つのパラメータを含むものであってもよい。また、SSIDとは、Service Set Identifierの略である。

【0019】

また、記憶部202として、ROM、RAM等のメモリの他に、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、DVDなどの記憶媒体を用いてもよい。

【0020】

通信部203はIEEE802.11シリーズに準拠した無線通信を行う。なお、通信部203は、更にNFC(Near Field Communication)に準拠した近距離無線通信を行う機能を有していてもよい。表示部204はLCDやLEDのように視覚で認知可能な情報を出力する。表示部204は、例えば通信パラメータの設定処理に必要な情報を含むQRコード(登録商標、以下省略)を表示する。なお、視覚で認知可能な情報の出力に代えて、もしくは、加えて、スピーカのように聴覚で認知可能な音を出力してもよい。また、LCDはLiquid Crystal Displayの略であり、LEDはLight Emitting Diodeの略である。また、QRコードに代えて、CPコード等、他の2次元コードであってもよいし、1次元のバーコードを表示するようにしてもよい。

10

【0021】

アンテナ制御部205は、アンテナ206を制御する。操作部207は、ユーザが各種入力等を行い、通信装置を操作するための操作部である。208は時間の経過を検知する計時部である。

20

【0022】

図3に、管理装置101の制御部が記憶部に記憶されているプログラムを読み出すことで実現されるソフトウェア機能ブロックを示す。なお、図3に示すソフトウェア機能ブロックの少なくとも一部をハードウェアにより実現してもよい。

【0023】

ハードウェアにより実現する場合、例えば、所定のコンパイラを用いることで各機能ブロックを実現するためのプログラムからFPGA上に専用回路を生成し、これを当該ソフトウェアモジュールの機能を有するハードウェアとして用いればよい。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。

30

【0024】

提供部301は、通信パラメータを他の通信装置に提供する。取得部302は、通信パラメータを他の通信装置から取得する。なお、管理装置101は、取得部302により第1の他の通信装置から取得した通信パラメータを、提供部301により第2の他の通信装置に提供する中継処理を行うこともできる。

【0025】

解析部303は、撮像部209により撮像された画像を解析し、通信パラメータの共有処理に用いられる認証情報や、他の通信装置の識別子を抽出する。ここで、他の通信装置の識別子は、他の通信装置固有の識別子であるMAC(Media Access Control)アドレスである。なお、MACアドレスに代えて、UUID(Universally Unique Identifier)であってもよい。

40

【0026】

ここでは、解析部303は、撮像されたQRコードを解析することにより認証情報や識別子を抽出する。なお、QRコードに代えて、CPコード等、他の2次元コードであってもよいし、1次元のバーコードであってもよい。

【0027】

また、解析部303は、撮像部209により撮像された画像の解析に代えて、NFC、

50

Bluetooth（登録商標、以下省略）、ZigBee、IEEE 802.11adもしくはTransferJet（登録商標）等の無線通信により、認証情報や識別子を取得してもよい。

【0028】

通知部304は、通信パラメータの変更を他の通信装置に通知する。更に、通知部304は、他の通信装置に変更後の通信パラメータを送信する。

【0029】

変更部305は、他の通信装置から取得した通信パラメータの一部または全部を変更する。ここで、変更部305は、他の通信装置の機能情報に基づいて、通信パラメータに含まれるパラメータのうち、変更するパラメータを決定し、変更する。

10

【0030】

受信部306はパケットを受信し、送信部307はパケットを送信部する。これにより、管理装置101は、他の通信装置との間で802.11規格に準拠した無線通信を行う。

【0031】

次に、図4に、AP2の制御部201が記憶部202に記憶されているプログラムを読み出すことで実現されるソフトウェア機能ブロックを示す。なお、上述と同様に、図4に示すソフトウェア機能ブロックの少なくとも一部をハードウェアにより実現してもよい。また、AP1も同様のソフトウェア機能ブロックを有する。

【0032】

20

提供部401は、通信パラメータを他の通信装置に提供する。取得部402は、通信パラメータを管理装置101から取得する。また、取得部402は、管理装置101から認証情報を取得する。

【0033】

出力部403は、通信パラメータの共有処理に用いられる認証情報や、AP2の識別子の情報を含むQRコードを生成し、表示部204へ出力する。なお、QRコードに代えて、CPコード等、他の2次元コードであってもよいし、1次元のバーコードであってもよい。

【0034】

また、QRコードの出力に代えて、NFC、Bluetooth、ZigBee、IEEE 802.11adもしくはTransferJet（登録商標）等の無線通信により、認証情報や識別子を出力してもよい。

30

【0035】

選択部404は、通信パラメータが複数存在した場合に、他の通信装置に提供する通信パラメータを選択する。登録部405は、管理装置の登録や削除の処理を実行する。AP機能部408は、AP1が基地局として動作するための制御を行う。AP機能部408は、管理装置101から取得した通信パラメータにより接続可能な無線ネットワークを構築する。また、AP機能部408は、当該無線ネットワークの維持・管理も行う。受信部406はパケットを受信し、送信部407はパケットを送信部する。これにより、AP1は、他の通信装置との間で802.11規格に準拠した無線通信を行う。

40

【0036】

変更部409は、他の通信装置から取得した通信パラメータの一部または全部を変更する。

【0037】

なお、全ての機能ブロックはソフトウェアもしくはハードウェア的に相互関係を有するものである。また、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。

【0038】

本実施形態において、管理装置101はAP2のQRコードを読み取ることで、AP2

50

の認証情報を取得する。そして、管理装置101は、当該認証情報を用いてAP2と認証処理を行う。認証に成功すると、AP2が構築する無線ネットワークの通信パラメータを設定する管理権を取得し、AP2に通信パラメータを提供する。一方、AP2は管理装置101から受信した通信パラメータに基づいて、ネットワーク2を構築する。

#### 【0039】

次に、既存の基地局(AP1)から新規の基地局(AP2)に基地局を置き替える例に詳細を説明する。図5は、ユーザから所定の指示が為された場合に、AP2の記憶部202に記憶されたプログラムを制御部201が読み出し、それを実行することで実現される処理の流れのフローチャートである。

#### 【0040】

なお、図5に示すフローチャートの少なくとも一部をハードウェアにより実現してもよい。ハードウェアにより実現する場合、例えば、所定のコンパイラを用いることで、各ステップ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。

#### 【0041】

また、図6に管理装置101、AP1、AP2、およびSTA1の間のシーケンスチャートを示す。初期状態として、AP1はネットワーク1を構築しており、管理装置101およびSTA1はネットワーク1に接続している。

#### 【0042】

まず、管理装置101は、AP1から、無線ネットワーク1の識別子(ここでは、SSID)を含む通信パラメータを取得する。ここでは、管理装置101はAP1に対してAP情報要求信号を送信する(F601)。AP1は当該要求信号を受信すると、ネットワーク1に接続するための通信パラメータ情報を含む応答信号を管理装置101に送信する(F602)。管理装置101は、当該応答信号を受信することで、AP1から通信パラメータを取得する。なお、これに代えて、HTTPなどのデータ通信を用いてAP1から通信パラメータを取得してもよいし、WPS(Wi-Fi Protected Setup)によりAP1から通信パラメータを取得してもよい。

#### 【0043】

また、管理装置101は、AP1に接続している間にSTA1のセキュリティに関する機能情報の取得を行ってもよい。具体的には管理装置101が、AP1を介してSTA1に機能情報要求信号をユニキャスト送信する。なお、機能情報要求信号は、UPnPもしくはBonjourに準拠したパケットである。ここで、UPnPとはUniversal Plug and Playの略である。

#### 【0044】

なお、ユニキャストに代えて、マルチキャストやブロードキャスト送信を行ってもよい。マルチキャストまたはブロードキャストで送信することにより、1つの要求信号で複数の装置から応答を受信することが可能である。

#### 【0045】

機能情報要求信号を受信したSTA1はAP1を介して、STA1の機能情報を含む応答信号を送信する。なお、応答信号は、STA1が暗号方式としてAESやTKIPに対応しているか否かを示す暗号機能情報を含む。ここで、AESはAdvanced Encryption Standardの略であり、TKIPはTemporal Key Integrity Protocolの略である。また、AESの方がTKIPよりも暗号強度が高い。

#### 【0046】

また、STA1が認証方式として、WPA2やWPA1に対応しているか否かを示す認証機能情報を含む。ここで、WPAとはWi-Fi Protected Access

10

20

30

40

50

の略である。また、W P A 2の方がW P A 1よりも認証強度が高い。

【0047】

なお、これに代えて、機能情報としてS T A 1のバージョン情報を含むようにしてもよい。この場合、予めバージョン情報に対応する暗号方式や認証方式が定められているものとする。

【0048】

管理装置101は、S T A 1からの応答信号を受信することにより、S T A 1のセキュリティに関する機能情報を取得する。

【0049】

なお、応答信号に、S T A 1が対応する通信方式（I E E E 8 0 2 . 1 1 a c等）や、S T A 1が利用可能な周波数帯（2 . 4 G H zまたは5 G H z等）などの情報を含めてもよい。

【0050】

次に、A P 2は、ユーザの操作に応じて、A P 2の認証情報および公開鍵の情報を含むQ RコードをA P 2の表示部に表示する（S 5 0 1、F 6 0 3）。なお、これに代えて、A P 2の筐体にシールなどに記載された形態でQ Rコードを貼り付けてもよい。また、A P 2の取扱説明書や販売時の段ボールなどの包装などの付属物に貼り付けてもよい。また、A P 2やA P 2の付属物に直接Q Rコードを記載しておいてもよい。

【0051】

管理装置101は、撮像部209を介してA P 2のQ Rコードを読み取り、A P 2の認証情報、および、A P 2の公開鍵を取得する（F 6 0 4）。そして、A P 2は、管理装置101に管理権を与えるための認証処理を行う（S 5 0 2、F 6 0 5）。

【0052】

ここでは、管理装置101はA P 2の認証情報をA P 2の公開鍵で暗号化して、A P 2に送信する。A P 2は、受信した暗号データを、該公開鍵に対応するA P 2の秘密鍵を用いて復号する。復号した結果、A P 2の認証情報を得ることができれば、認証は成功となる。

【0053】

なお、該認証処理に際して、A P 2は管理装置101およびS T A 1の機能情報を取得する。

【0054】

認証に成功した場合（S 5 0 3のY e s）、A P 2は管理装置101を、管理権を有する装置として登録する（F 6 0 6）。また、管理装置101は認証処理に成功すると、通信パラメータ（パラメータ1）を、A P 2のQ Rコードから取得した公開鍵を用いて暗号化してA P 2に送信する（F 6 0 7）。これにより、通信パラメータを送信する際のセキュリティを高めることができる。

【0055】

一方、認証処理に失敗した場合（S 5 0 3のN o）、A P 2は図5に示す処理を終了する。この場合、A P 2は、ユーザにエラー通知を行うようにしてもよい。

【0056】

A P 2は、パラメータ1を受信する（S 5 0 4）と通信パラメータの生成処理を実施するか否かを判定する（S 5 0 5）。

【0057】

次に、通信パラメータの生成処理（F 6 0 8）について説明する。

【0058】

まず、A P 2は、管理装置101から取得した通信パラメータのセキュリティ方式（認証方式と暗号方式の組み合わせ）を、セキュリティ強度の高い方式に変更するか否かを判定する（S 5 0 5）。ここでは、S T A 1、および、管理装置101の機能情報、および、取得した通信パラメータのセキュリティ方式の少なくとも一部に基づいて、A P 2はセキュリティ強度を変更するか否かを判定する。

10

20

30

40

50

## 【0059】

例えば、通信パラメータのセキュリティ方式がWPA1-TKIPであり、STA1、および、管理装置101がWPA2-AESに対応していれば、管理装置101は、通信パラメータのセキュリティ方式をWPA2-AES変更すると判定する。一方、STA1もしくは管理装置101がWPA2-AESに対応していなければ、通信パラメータのセキュリティ方式を変更しないと判定する。

## 【0060】

なお、STA1の機能情報は考慮することなく判定を行ってもよい。この場合、AP2は認証処理に際してSTA1の機能情報を取得する必要はない。

## 【0061】

10

また、例えば、通信パラメータのセキュリティ方式がWPA2-AESであり、セキュリティ方式を変更してもセキュリティを高めることができない場合は、通信パラメータのセキュリティ方式を変更しないと判定する。

## 【0062】

セキュリティ方式を変更すると判定され場合（S505のYes）、AP2は、通信パラメータのセキュリティ方式を変更して、新たな通信パラメータ（パラメータ2）を生成する（S506）。ここでは、暗号方式についてTKIPからAESに変更し、認証方式についてWPA1からWPA2に変更する。なお、TKIPとAESとで同じ長さ（鍵長）の暗号鍵を利用可能であれば、暗号鍵については変更せず、利用可能でなければ新たな暗号鍵を生成する。

20

## 【0063】

同様に、WPA1とWPA2とで同じ長さ（鍵長）の認証鍵を利用可能であれば、認証鍵については変更せず、利用可能でなければ新たな認証鍵を生成する。なお、S506においては無線ネットワークの識別子の変更は行わない。即ち、変更前の通信パラメータに含まれる識別子の情報と、変更後の通信パラメータに含まれる識別子の情報は同一である。

## 【0064】

また、暗号方式と認証方式のいずれか一方だけを変更するようにしてもよい。

## 【0065】

セキュリティ方式の変更が完了すると、AP2は構築する無線ネットワーク（ネットワーク2）の通信パラメータとして、パラメータ2を設定する（S507、F609）。なお、パラメータ2とパラメータ1の両方を無線ネットワークとして設定することも可能である。

30

## 【0066】

上述の実施形態では更に、変更前と変更後の鍵長に応じて、暗号鍵や認証鍵を変更しないようにしているので、AP1に接続していた端末の設定を大きく変えることなく、AP2に接続できるようになる。

## 【0067】

一方、変更しないと判定された場合（S505のNo）、AP2は構築する無線ネットワーク（ネットワーク2）の通信パラメータとして、パラメータ1を設定する（S507）。

40

## 【0068】

このようにして、AP2のセキュリティ方式はAP1のセキュリティ方式からセキュリティ強度の高い方式に変更されているため、セキュリティの高いデータ通信が可能となる。

## 【0069】

管理装置101は、AP2への通信パラメータの設定が完了するとAP2に接続する（F610）。管理装置101はAP1に電源OFFを指示し（F611）、AP1の電源をOFFにする。これにより、AP1が構築した無線ネットワーク1を終了させることができる。なお、これに代えて、管理装置101がユーザに対してAP1の電源をOFFに

50

する旨の指示を表示部 204 に表示するようにしてもよい。

【0070】

また、電源OFFに代えて、AP1に通信パラメータを変更するように指示してもよい。このように、無線ネットワーク1を終了させる、もしくは、AP1が通信パラメータを変更することで、STA1等が古いAP1の無線ネットワーク1に接続してしまうことを防止できる。

【0071】

次にAP2は当該通信パラメータをSTA1に設定するための処理を行う。なお、この処理は、通信パラメータを変更しなかった場合には省略してもよい。

【0072】

まず、STA1は、通信パラメータの設定を開始するためのユーザ指示を受け付けると、STA1の認証情報を含むQRコードを表示部に表示する(F612)。なお、ユーザ指示に代えて、管理装置101等からの所定の信号を受信したことに応じて、QRコードを表示するようにしてもよい。また、QRコードに代えて、他の種類の2次元コードや、バーコード等の1次元コードを表示するようにしてもよい。また、コードの表示に代えて、NFCやBluetooth、ZigBee、IEEE802.11ad、TransferJet等の無線通信により、認証情報を送信してもよい。

【0073】

管理装置101は、STA1のQRコードを読み取ることでSTA1の公開鍵情報を含む認証情報を取得する(F613)。なお、STA1がQRコードに代えて他のコードを表示している場合には、当該コードを読み取ることで認証情報を取得すればよい。また、STA1がQRコードに代えて無線通信により認証情報を送信している場合には、対応する無線通信により認証情報を受信すればよい。

【0074】

そして、管理装置101は取得したSTA1の認証情報をAP2に送信することで(F614)、STA1とAP2とが通信パラメータの共有処理を開始するためのトリガをかける。

【0075】

AP2は管理装置から通信パラメータ共有処理のトリガを受けて、STA1から機能情報を取得する(S508、F615、F616)。次に、受信したSTA1の認証情報を用いて、STA1と通信パラメータ共有処理を実行する。この際、AP2はSTA1の機能情報を元にパラメータ1とパラメータ2のどちらを提供するか判断し、STA1に通信パラメータを提供する(S509、F617)。ここでも、認証情報に含まれるSTA1の公開鍵を用いて通信パラメータを暗号化してSTA1に送信するので、通信パラメータを共有する際のセキュリティを高めることができる。

【0076】

これにより、通信パラメータを受信したSTA1は、AP2に接続し、データ通信が可能な状態となる(F618)。また、AP2のセキュリティ方式はAP1のセキュリティ方式からセキュリティ高度の高い方式に変更されているため、セキュリティの高いデータ通信が可能となる。

【0077】

以上のように、本実施形態によれば、AP1からAP2に置き換える際に、AP1が構築する無線ネットワーク1の識別子を有する無線ネットワーク2をAP2が簡単に構築することができる。

【0078】

更に、通信パラメータのセキュリティ方式をセキュリティ強度が高い方式へ自動的に変更するため、セキュリティとユーザの利便性が向上する。また、APやSTAの能力として対応可能な範囲内でセキュリティ方式を選択するため、セキュリティ方式の変更による接続性の低下を防止することも可能となる。

【0079】

10

20

30

40

50

なお、上述の実施形態において、A P 2 が所定のセキュリティ方式（例えば、A E S）に対応していない場合、管理装置 1 0 1 は図 5 に示す処理をエラー終了してもよい。これにより、セキュリティの低い無線ネットワークが新たに構築される可能性を低減することができる。

【0080】

また、上述の実施形態では、管理装置 1 0 1 は変更後の通信パラメータを A P 2 に設定した。しかし、A P 2 において複数のネットワークを同時並行的に構築することが可能な場合、パラメータ 1 とパラメータ 2 の通信パラメータの両方を設定するようにしてもよい。

【0081】

10

これにより、A P 2 においてもネットワーク 1 と同等の無線ネットワークも構築されるため、接続性を向上させることができる。なお、S T A がパラメータ 1 の設定でネットワーク 2 に接続してきた場合に H T T P などのデータ通信を用いて A P 2 から S T A にパラメータ 2 を提供し、パラメータ 2 の設定への切り替えを促してもよい。また、A P 2 は、一方の無線ネットワークへ接続する S T A が所定期間、存在しない場合には、当該無線ネットワークを終了してもよい。これにより、セキュリティの低下を軽減することが可能となる。

【0082】

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でも実現可能である。また、1 以上の機能を実現する回路（例えば、A S I C）によっても実現可能である。

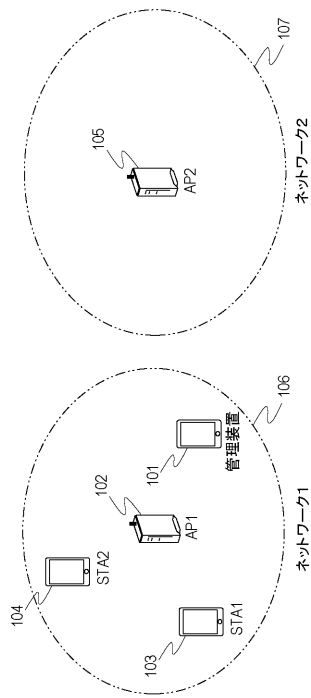
20

【符号の説明】

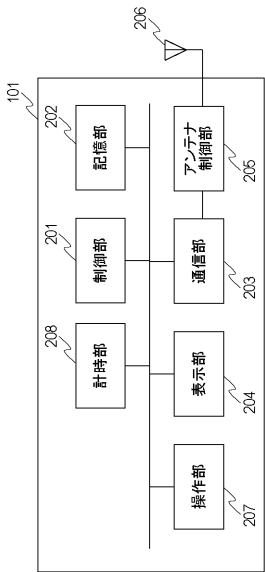
【0083】

- 1 0 1 管理装置
- 1 0 2 アクセスポイント 1
- 1 0 3 S T A 1
- 1 0 5 アクセスポイント 2

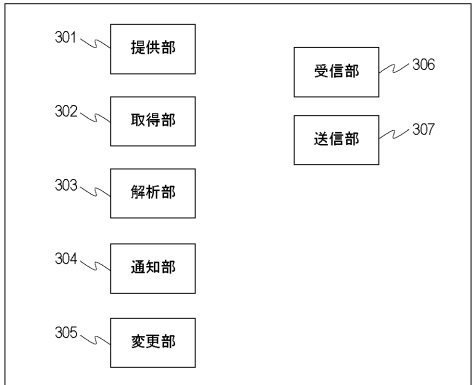
【図 1】



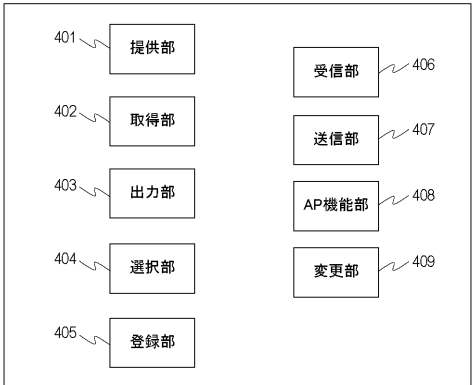
【図 2】



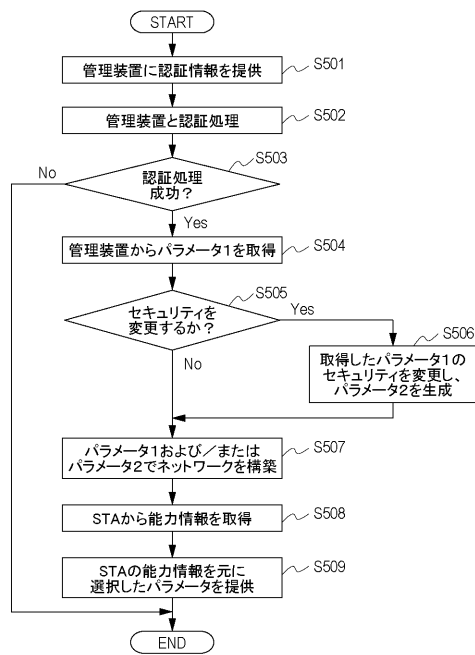
【図 3】



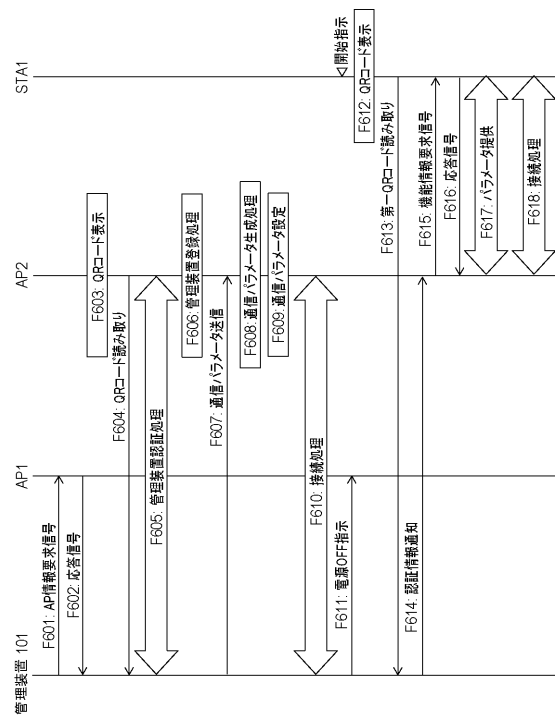
【図 4】



【図 5】



【図 6】



---

フロントページの続き

- (56)参考文献 特開2013-046290 (JP, A)  
特開2005-311653 (JP, A)  
特開2008-213294 (JP, A)  
特開2015-119426 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04B 7/24- 7/26  
H04W 4/00-99/00