(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-43545
(P2020-43545A)
(43)公開日　令和2年3月19日(2020.3.19)

(51)Int.Cl.		F I		テーマコード（参考）
H04W 48/02	***(2009.01)***	H04W	48/02	5K067
H04W 12/04	***(2009.01)***	H04W	12/04	
H04W 84/12	***(2009.01)***	H04W	84/12	
H04W 76/18	***(2018.01)***	H04W	76/18	

審査請求 未請求　請求項の数 14　ＯＬ　（全 18 頁）

(21)出願番号　特願2018-171689 (P2018-171689)
(22)出願日　平成30年9月13日 (2018.9.13)

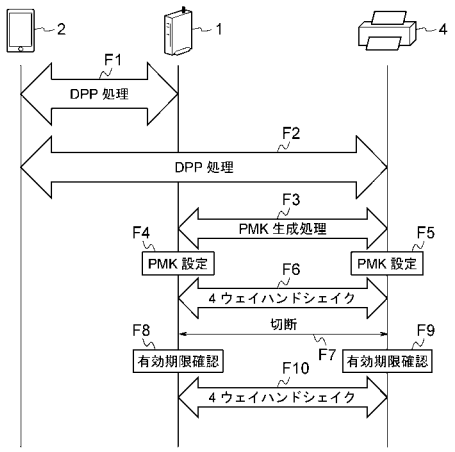
（特許庁注：以下のものは登録商標）
１．ＺＩＧＢＥＥ

(71)出願人　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　100109380
弁理士　小西　恵
(74)代理人　100109036
弁理士　永岡　重幸
(72)発明者　後藤　史英
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

Ｆターム(参考)　5K067 EE02　EE10　FF23　HH22　HH23　HH36

(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

(57)【要約】
【課題】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通信装置を提供する。
【解決手段】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。
【選択図】図４



【特許請求の範囲】
【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、ＩＥＥＥ８０２．１１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ＩＥＥＥ８０２．１１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。
【発明の詳細な説明】
【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、通信装置の制御方法およびプログラムに関する。
【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。
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。

【０００３】
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。
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。
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、ＣＭＯ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。
【０００４】
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、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。
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。
【０００５】
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】
【０００６】
【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】
【０００７】
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。
【０００８】
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。
【０００９】
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】
【００１０】
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。
【発明の効果】
【００１１】
本発明によれば、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。
【図面の簡単な説明】
【００１２】
【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】
【００１３】
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。
【００１４】
（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。
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。

【００１５】

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。

【００１６】

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ＩＥＥＥ８０２．１１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。

【００１７】

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。

【００１８】

＜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。

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。

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。

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。

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。

【００１９】

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。

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。
【００２０】
＜通信装置のハードウエア構成＞
図２は、本実施形態に係る各通信装置のハードウエア構成の一例を示す図である。
図２の通信装置１０は、制御部１１、記憶部１２、撮像部１３、入力部１４、表示部１５、無線通信部１６、アンテナ制御部１７、およびアンテナ１８を備える。制御部１１、記憶部１２、撮像部１３、入力部１４、表示部１５、無線通信部１６、およびアンテナ制御部１７は、システムバスにより通信可能に接続される。
制御部１１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（１２～１７）を制御する。すなわち、制御部１１は、各種処理の実行に際して記憶部１２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１１は、例えばＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）により構成される。
【００２１】
記憶部１２は、制御部１１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１２に記憶された制御プログラムを制御部１１が実行することにより実現される。記憶部１２は、制御部１１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１２はまた、制御部１１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１２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。
【００２２】
撮像部１３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。
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。
表示部１５は、各種表示を実行し、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）やＬＥＤ（ＬｉｇｈｔＥｍｉｔｔｉｎｇ　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。
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。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。
【００２３】
無線通信部１６は、ＩＥＥＥ８０２．１１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。
アンテナ制御部１７は、アンテナ１８の出力制御を実行する。
アンテナ１８は、無線ＬＡＮで通信するための２．４ＧＨｚ帯および／または５ＧＨｚ帯で通信可能である。
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。
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。
【００２４】

＜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。

図３に示す通信装置１０の各機能モジュールのうち、ソフトウエ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。ハードウエ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、ハードウエ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、専用ハードウエアは制御部１１の制御に基づいて動作する。

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。

【００２５】

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、ＩＥＥＥ８０２．１１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。

【００２６】

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通信に必要となる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。

【００２７】

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。

【００２８】

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。

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。

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。

【００２９】

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。

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、ＯＳＩ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。

【００３０】

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ＩＥＥＥ８０２．１１規格に準拠したパケットの送信および受信を実行する。

ステーション機能部２７は、ＩＥＥＥ８０２．１１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。

【００３１】

アクセスポイント機能部２８は、ＩＥＥＥ８０２．１１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。

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。

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。

【００３２】

＜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。

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。

【００３３】

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。

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。

【００３４】

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。
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。
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はＤＰＰの仕様どおりであるためその詳細は省略する。
Ｆ１およびＦ２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。

【００３５】
Ｆ１およびＦ２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、Ｆ３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。
Ｆ３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、Ｆ４およびＦ５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。

【００３６】
ここで、Ｆ３ないし Ｆ５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ＤＰＰ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。
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。
ＷＰＡ－Ｅｎｔｅｒｐｒｉｓｅでは、ＩＥＥＥ８０２．１Ｘ規格に基づき、ＲＡＤＩＵＳサーバからＰＭＫを配布することができる。

【００３７】
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。
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。
図５に示すＰＭＫ管理テーブル５は、ＰＭＫＩＤ５１、ＭＡＣアドレス５２、ＰＭＫ５３、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。

【００３８】
ＰＭＫＩＤ５１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ＩＥＥＥ８０２．１１規格に準拠する。ＭＡＣアドレス５２は、ＰＭＫＩＤ５１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。
ＰＭＫ５３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、ＰＭＫＩＤ５１で特定されるＰＭＫ５３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」、「ＰＳ

Ｋ」、「１Ｘ」の値で記述することができる。

【００３９】

有効期限５５は、ＰＭＫＩＤ５１で特定されるＰＭＫ５３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。

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。

【００４０】

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。

【００４１】

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。

この場合、その後にアクセスポイント１とプリント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。

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。

【００４２】

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。

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。

再接続要求に含まれるＰＭＫＩＤ５１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、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。

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。

【００４３】

一方、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、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。

【００４４】

＜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。
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。
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。
【００４５】
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。
具体的には、Ｓ６３で実行されるＰＭＫ生成処理において、Ｓ６１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。
Ｓ６４で、エンローリである通信装置１０は、ＰＭＫ管理テーブル５に、Ｓ６３で算出されたＰＭＫのエントリーとして、ＰＭＫＩＤ５１、対向装置のＭＡＣアドレス５２、およびＰＭＫ５３を設定する。エンローリである通信装置１０はさらに、Ｓ６３で算出されたＰＭＫのエントリーとして、ＰＭＫ種別５４に「ＤＰＰ」を設定し、有効期限（Ｅｘｐｉｒｙ）５５には、ステップＳ６１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。
以上のＳ６１からＳ６４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。
【００４６】
＜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Ｆ８ないしＦ１０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
Ｓ７１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ＰＭＫＩＤ５１を使用して、ＰＭＫ管理テーブル５中のＰＭＫ種別５４（ＡＫＭ情報）を参照する。
【００４７】
前回接続時のＰＭＫＩＤ５１のＰＭＫ種別５４がＤＰＰである場合（Ｓ７１：Ｙ）、Ｓ７２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ＰＭＫＩＤ５１のＰＭＫ種別５４がＤＰＰ以外である場合（Ｓ７１：Ｎ）、Ｓ７２をスキップして、Ｓ７３へ進む。
Ｓ７２で、プリンタ４は、前回接続時のＰＭＫＩＤ５１をキーにＰＭＫ管理テーブル５を参照して、ＰＭＫの有効期限（Ｅｘｐｉｒｙ）５５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（Ｓ７２：Ｙ）、Ｓ７３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（Ｓ７２：Ｎ）、Ｓ７５に進む。
Ｓ７３で接続先のＡＰを検索した結果、ＡＰの存在が確認されると、Ｓ７４で、アクセスポイント１（ＡＰ）とプリンタ４（ＳＴＡ）との間で、ＩＥＥＥ８０２．１１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。
【００４８】

Ｓ７２に戻り、ＰＭＫの有効期限が経過している場合（Ｓ７２：Ｎ）、Ｓ７５で、プリンタ４は、表示部１５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。

Ｓ７５で、表示部１５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１５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。

【００４９】

図８は、通信装置１０における無線ＬＡＮ接続先情報を表示するＷｉ－Ｆｉ設定メニュー８０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ＳＳＩＤが表示されている。当該ＳＳＩＤが、にＷＥＰ／ＷＰＡ／ＷＰＡ２／ＤＰＰ等により無線ＬＡＮ通信時に暗号化する場合は、ＳＳＩＤに対応して鍵マークを表示する。

図７のＳ７５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１５に「有効期限切れ（ｅｘｐｉｒｅｄ）」等と表示して、ユーザーが有効期限切れとなった無線ＬＡＮ接続先８１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。

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。

【００５０】

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。

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。

【００５１】

（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。

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。

【００５２】

実施形態２に係る通信装置１０のハードウエ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。

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。

【００５３】

＜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。

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。

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。

【００５４】

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。

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、ｄｅａｕｔｈ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。

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。

【００５５】

一方、ステップＳ９３に戻り、通信装置１０は、自装置がステーション（ＳＴＡ）モードで動作している場合（Ｓ９３：ＳＴＡ）、Ｓ９７に進み、自装置のステーション（ＳＴＡ）としての機能を停止する。

Ｓ９７では、例えば、図１０のユーザインタフェース８２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８３を表示部１５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１０は、これらの通知をユーザに提示した後、接続中のＡＰとの接続を切断し、自装置のステーション（ＳＴＡ）としての動作を終了すればよい。

あるいは、自装置がＳＴＡモードで動作している場合、通信装置１０は、ステーション（ＳＴＡ）としての動作は継続したまま、表示部１５にＰＭＫ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。

【００５６】

以上説明したように、本実施形態によれば、通信装置１０は、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。

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。

【００５７】

＜他の実施形態＞

上記の各実施形態においては、ＱＲ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、ＱＲコード等を撮像することに替えて、ＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）やＢｌｕｅｔｏｏｔｈ（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、ＩＥＥＥ８０２．１１ａｄ規格もしくはトランスファージェット（ＴｒａｎｓｆｅｒＪｅｔ）（登録商標）等による無線通信を用いてもよい。

【００５８】

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。

【００５９】

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。

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。

【００６０】

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。

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、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。

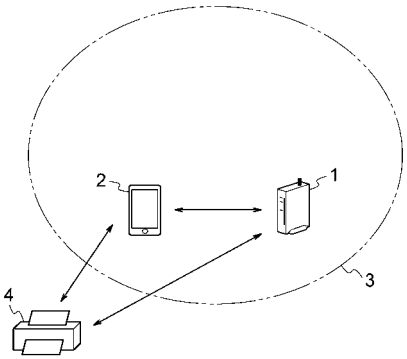
また、コンピュータが読みだしたプログラムを実行することにより、実施形態の機能が実現されるものに限定されない。例えば、プログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって上記した実施形態の機能が実現されてもよい。

【符号の説明】

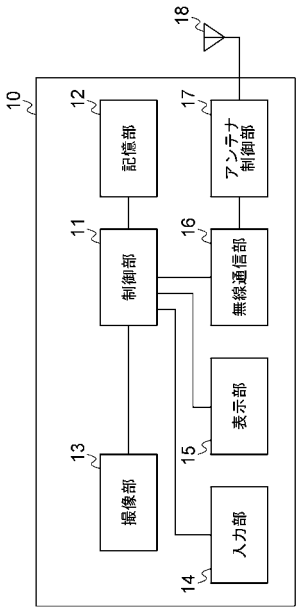
【００６１】

１…アクセスポイント、２…スマートフォン、４…プリンタ、１０…通信装置、１１…制御部、１２…記憶部、１３…撮像部、１４…入力部、１５…表示部、１６…無線通信部、１７…アンテナ制御部、１８…アンテナ、２１…通信パラメータ制御部、２２…バーコード読み取り部、２３…バーコード生成部、２４…サービス制御部、２５…パケット受信部、２６…パケット送信部、２７…ステーション機能部、２８…アクセスポイント制御部、２９…データ記憶部

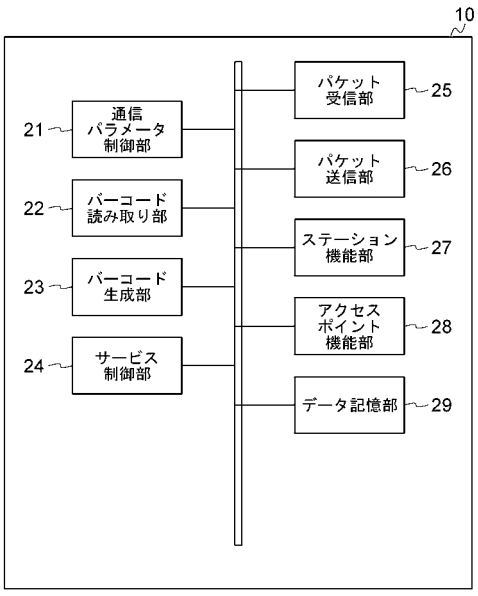
【図１】


1
2
3
4

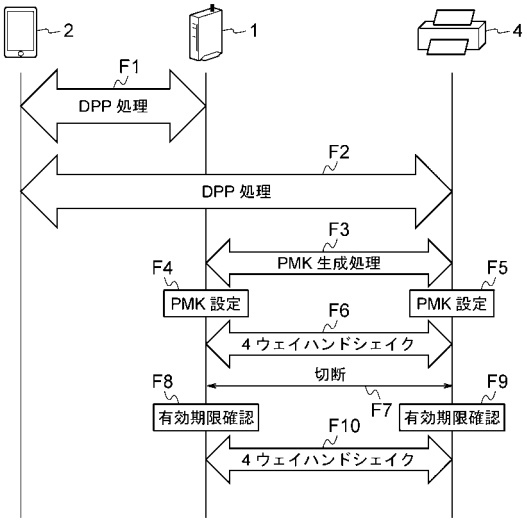
【図２】


10
11
12
13
14
15
16
17
18
記憶部
制御部
撮像部
入力部
表示部
無線通信部
アンテナ制御部

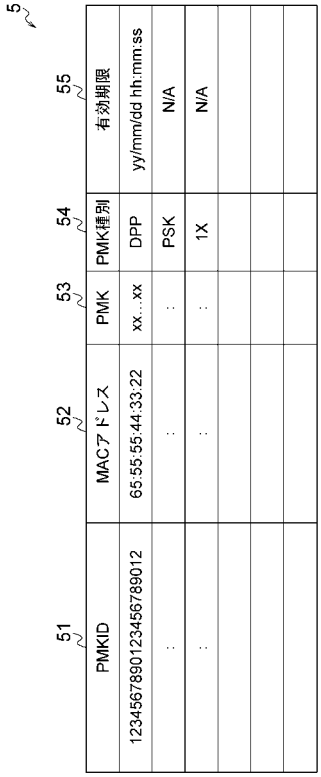
【図３】


10
21
22
23
24
25
26
27
28
29
通信パラメータ制御部
バーコード読み取り部
バーコード生成部
サービス制御部
パケット受信部
パケット送信部
ステーション機能部
アクセスポイント機能部
データ記憶部

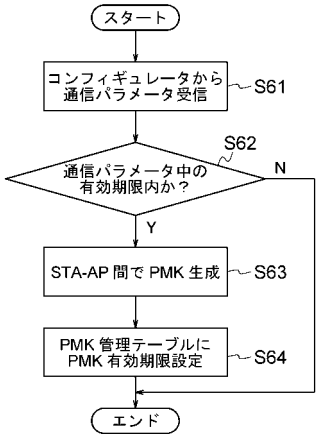
【図４】


1
2
4
F1
DPP 処理
F2
DPP 処理
F3
PMK 生成処理
F4
PMK 設定
F5
PMK 設定
F6
4 ウェイハンドシェイク
切断
F7
F8
有効期限確認
F9
有効期限確認
F10
4 ウェイハンドシェイク

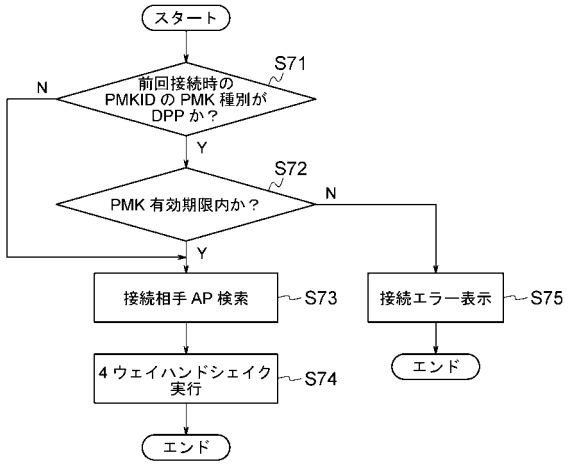
【図５】


5
51 PMKID
123456789012345678901234567890 12
52 MACアドレス
65:55:55:44:33:22
53 PMK
xx…xx
54 PMK種別
DPP
PSK
1X
55 有効期限
yy/mm/dd hh:mm:ss
N/A
N/A

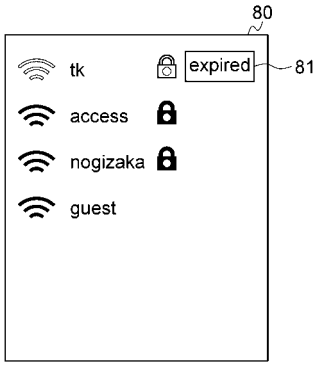
【図６】


スタート
コンフィギュレータから通信パラメータ受信
S61
S62
通信パラメータ中の有効期限内か？
N
Y
STA-AP 間で PMK 生成
S63
PMK 管理テーブルに PMK 有効期限設定
S64
エンド

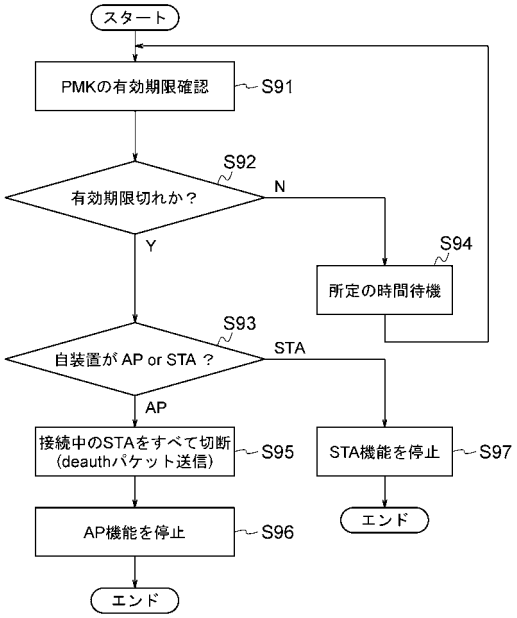
【図７】


スタート
S71
前回接続時の PMKID の PMK 種別が DPP か？
N
Y
S72
PMK 有効期限内か？
N
Y
接続相手 AP 検索
S73
接続エラー表示
S75
4 ウェイハンドシェイク実行
S74
エンド
エンド

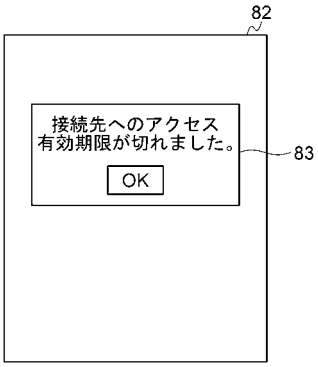
【図８】


80
tk
expired
81
access
nogizaka
guest

【図９】


スタート
PMKの有効期限確認
S91
S92
有効期限切れか？
N
Y
S94
所定の時間待機
S93
自装置がAP or STA ？
STA
AP
接続中のSTAをすべて切断
(deauthパケット送信)
S95
STA機能を停止
S97
AP機能を停止
S96
エンド
エンド

【図１０】


82
接続先へのアクセス
有効期限が切れました。
OK
83