(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7406893号
(P7406893)

(45)発行日　令和5年12月28日(2023.12.28)

(24)登録日　令和5年12月20日(2023.12.20)

(51)国際特許分類

		FI	
H04W	*12/0431(2021.01)*	H04W	12/0431
H04W	*84/12 (2009.01)*	H04W	84/12
H04W	*12/06 (2021.01)*	H04W	12/06

請求項の数　15　（全24頁）

(21)出願番号　特願2019-189803(P2019-189803)
(22)出願日　令和1年10月16日(2019.10.16)
(65)公開番号　特開2021-64910(P2021-64910A)
(43)公開日　令和3年4月22日(2021.4.22)
審査請求日　令和4年10月13日(2022.10.13)

(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　100223941
弁理士　高橋 佳子
(74)代理人　100159695
弁理士　中辻 七朗
(74)代理人　100172476
弁理士　冨田 一史
(74)代理人　100126974
弁理士　大朋 靖尚
(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
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】
通信装置であって、
公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ　Ｄｅｖｉｃｅ　Ｐｒｏｖｉｓｉｏｎｉｎｇ　Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証手段と、
前記認証手段による前記認証処理に成功し、さらに前記他の通信装置から設定要求を受信した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｏｆ　Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、ＳＡＥのパスワードと、ＰＭＫ（Ｐａｉｒｗｉｓｅ　Ｍａｓｔｅｒ　Ｋｅｙ）の算出に用いられる情報要素とを含む通信パラメータを提供する提供手段と、を有し、
前記通信パラメータは共有鍵を用いて暗号化されることを特徴とする通信装置。
【請求項２】
前記通信パラメータに前記情報要素を含ませるかを判定する第１の判定手段を更に有し、
前記提供手段は、前記第１の判定手段によって前記通信パラメータに前記情報要素を含ませると判定された場合に、ＳＡＥの前記パスワードと前記情報要素とを含む前記通信パラメータを提供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】
前記第１の判定手段は、前記通信パラメータに含まれるＡｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｔｙｐｅ（ＡＫＭ）にＳＡＥが含まれる場合は、

前記通信パラメータに前記情報要素を含ませると判定し、前記ＡＫＭにＳＡＥが含まれない場合は、前記通信パラメータに前記情報要素を含ませないと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４】
前記第１の判定手段は、前記通信装置が前記通信パラメータとして前記情報要素を保持している場合は、前記通信パラメータに前記情報要素を含ませると判定し、前記通信装置が前記通信パラメータとして前記情報要素を保持していない場合は、前記通信パラメータに前記情報要素を含ませないと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】
前記他の通信装置が前記情報要素を利用するかを判定する第２の判定手段を更に有し、
前記第１の判定手段は、前記第２の判定手段によって前記他の通信装置が前記情報要素を利用すると判定された場合は、前記通信パラメータに前記情報要素を含ませると判定し、前記第２の判定手段によって前記他の通信装置が前記情報要素を利用しないと判定された場合は、前記通信パラメータに前記情報要素を含ませないと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６】
前記第２の判定手段は、前記他の通信装置から受信した信号に、前記情報要素を利用したＳＡＥに対応していることを示す情報が含まれていた場合は、前記他の通信装置が前記情報要素を利用すると判定し、前記情報要素を利用したＳＡＥに対応していることを示す情報が含まれていなかった場合は、前記他の通信装置が前記情報要素を利用しないと判定することを特徴とする請求項５に記載の通信装置。
【請求項７】
前記第１の判定手段によって、前記通信パラメータに前記情報要素を含ませないと判定された場合、前記通信パラメータには、ＤＰＰのコネクタと、ＰＳＫ（Ｐｒｅ Ｓｈａｒｅｄ Ｋｅｙ）と、パスフレーズとの少なくとも何れか一つが含まれることを特徴とする請求項２から６の何れか１項に記載の通信装置。
【請求項８】
前記情報要素は、ＳＡＥのＰａｓｓｗｏｒｄ Ｉｄｅｎｔｉｆｉｅｒであることを特徴とする請求項１から７の何れか１項に記載の通信装置。
【請求項９】
前記提供手段によって前記情報要素が含まれる前記通信パラメータが提供される場合、前記通信パラメータには、ＳＡＥの前記パスワードと、前記情報要素と、ＳＳＩＤ（Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｅｒ）と、ＡＫＭが含まれることを特徴とする請求項１から８の何れか１項に記載の通信装置。
【請求項１０】
前記他の通信装置は、前記提供手段によって提供された前記通信パラメータに含まれる前記パスワードと前記情報要素と楕円曲線暗号とを用いてＰＭＫを算出し、更に前記ＰＭＫを用いて生成したＰＴＫ（Ｐａｉｒ－ｗｉｓｅ Ｔｒａｎｓｉｅｎｔ Ｋｅｙ）を用いて通信を行うことを特徴とする請求項１から９の何れか１項に記載の通信装置。
【請求項１１】
前記提供手段は、前記通信パラメータを含むＤＰＰ規格に準拠したＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｓｐｏｎｓｅを送信することで、前記他の通信装置に前記通信パラメータを提供することを特徴とする請求項１から１０の何れか１項に記載の通信装置。
【請求項１２】
前記提供手段によって提供される前記通信パラメータは、パラメータとして、Ｗｉ－Ｆｉ Ｔｅｃｈｎｏｌｏｇｙ Ｏｂｊｅｃｔと、ＳＳＩＤと、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ｔｙｐｅとを含み、更に、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ｔｙｐｅの値に応じて、Ｐｒｅ－ｓｈａｒｅｄ ｋｅｙと、ＷＰＡ２ Ｐａｓｓｐｈｒａｓｅと、ＳＡＥ ｐａｓｓｗｏｒｄと、ＳＡＥ Ｉｄｅｎｔｉｆｉｅｒと、ＤＰＰ Ｃｏｎｎｅｃｔｏｒと、Ｃ－ｓｉｇｎ－ｋｅｙ

と、の少なくとも何れか一つを含むことを特徴とする請求項１から１１の何れか１項に記載の通信装置。
【請求項１３】
前記共有鍵はＥＣＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）方式に基づいて生成されることを特徴とする請求項１から１２の何れか１項に記載の通信装置。
【請求項１４】
通信装置の制御方法であって、
公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証工程と、
前記認証工程における前記認証処理に成功し、さらに前記他の通信装置から設定要求を受信した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、前記通信パラメータがＳＡＥのパスワードと、ＰＭＫの算出に用いられる情報要素とを含む通信パラメータを提供する提供工程と、を有し、
前記通信パラメータは共有鍵を用いて暗号化されることを特徴とする制御方法。
【請求項１５】
請求項１から１３のいずれか１項に記載の通信装置としてコンピュータを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、通信パラメータの提供に関する。
【背景技術】
【０００２】
通信装置を無線ネットワークに接続するには、暗号化方式、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に設定する技術として、Ｗｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（以下、ＤＰＰと称する）規格が策定されている（特許文献１）。
【０００３】
ＤＰＰ規格では、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。通信パラメータを取得したエンローリは、無線ネットワークを構築するアクセスポイント（以下、ＡＰと称する）、もしくはＡＰが構築した無線ネットワークに接続するステーション（以下、ＳＴＡと称する）の何れかとなる。
【先行技術文献】
【特許文献】
【０００４】
【文献】米国公開特許２０１７／０２９５４４８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ＤＰＰ規格は、無線ＬＡＮのセキュリティ規格であるＷｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ ３（ＷＰＡ３）規格に対応している。ＷＰＡ３規格では、通信に用いられる暗号鍵の共有の方式として、ＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ Ｅｑｕａｌｓ）を用いることができる。
【０００６】
ＳＡＥでは仕様のアップデートによって、通信パラメータとして、パスワードに加えて、オプションの情報要素が追加された。情報要素は無線ネットワークに設定されるもので

あって、該無線ネットワークにおいて通信する際には、設定された情報要素に基づいて算出されるＰＭＫ（Ｐａｉｒｗｉｓｅ　Ｍａｓｔｅｒ　Ｋｅｙ）が用いられる。しかし現行のＤＰＰ規格は、追加されたオプションの情報要素に対応していないため、該情報要素を通信パラメータとして送信することができなかった。

【０００７】

上記を鑑み、本発明は、通信装置が他の通信装置に通信パラメータを提供する場合に、ＳＡＥのパスワードと情報要素とを提供することで、他の通信装置が該情報要素を利用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】

上記目的を達成するため、本発明の通信装置は、公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ　Ｄｅｖｉｃｅ　Ｐｒｏｖｉｓｉｏｎｉｎｇ　Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証手段と、前記認証手段による前記認証処理に成功し、さらに前記他の通信装置から設定要求を受信した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ　Ａｕｔｈｅｎｔｉｃａ ｔｉｏｎ ｏｆ Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、ＳＡＥの パスワードと、ＰＭＫ（Ｐａｉｒｗｉｓｅ Ｍａｓｔｅｒ　Ｋｅｙ）の算出に用いられる 情報要素とを含む通信パラメータを提供する提供手段とを有し、前記通信パラメータは共有鍵を用いて暗号化される。

【発明の効果】

【０００９】

本発明によれば、通信装置が他の通信装置に通信パラメータを提供する場合に、ＳＡＥのパスワードと情報要素とを提供することで、他の通信装置が該情報要素とを利用できるようになる。

【図面の簡単な説明】

【００１０】

【図１】通信装置１０１が参加する通信システムの構成を示す図である。

【図２】通信装置１０１のハードウェア構成を示す図である。

【図３】通信装置１０１が通信パラメータを提供する際に実行する処理を示すフローチャートである。

【図４】通信装置１０１が、通信装置１０２またはアクセスポイント１０３と通信パラメータを共有する場合に実行する処理の一例を示すシーケンス図である。

【図５】通信装置１０１が図３のＳ３０９で実行する処理を示すフローチャートである。

【図６】通信装置１０１が、提供する通信パラメータに含まれるパラメータの一例を示す図である。

【図７】通信装置１０２が、ＳＡＥの情報要素を用いてアクセスポイント１０３との無線接続を確立する際に実行する処理を示すシーケンスである。

【発明を実施するための形態】

【００１１】

以下、添付の図面を参照して実施形態を詳細に説明する。なお、以下の実施形態において示す構成は一例に過ぎず、本発明は図示された構成に限定されるものではない。

【００１２】

図１に、通信装置１０１が参加する通信システムの構成を示す。本実施形態において、通信システムは通信装置１０１、１０２と、アクセスポイント１０３から構成され、いずれも無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）通信機能を有する。通信装置１０１、１０２は、無線ネットワークに参加するステーション（ＳＴＡ）として動作する。また、アクセスポイント１０３は、無線ネットワークを構築するアクセスポイント（ＡＰ）として動作する。通信装置１０１、１０２およびアクセスポイント１０３は、いずれもＩＥＥＥ８０２．１１シリーズ規格であるＩＥＥＥ８０２．１１ａ／ｂ／ｇ／ｎ／ａｃ／ａｘ／ｂｅ規格の少なくとも何れか一つによる無線通信に対応していてもよい。なお、ＩＥＥＥは、Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎ

ｉｃｓ Ｅｎｇｉｎｅｅｒｓの略である。
【００１３】
また、通信装置１０１は、Ｗｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠したコンフィギュレータとして動作し、他の装置に通信パラメータを提供する提供装置として動作する。また、通信装置１０２およびアクセスポイント１０３は、ＤＰＰ規格に準拠したエンローリとして動作し、他の装置から通信パラメータを受信する受信装置として動作する。このように、通信装置１０１は、通信装置１０２およびアクセスポイント１０３と通信パラメータを共有することで、各通信装置とアクセスポイント１０３が構築する無線ネットワーク１０４において通信することができるようになる。なお、通信装置１０１は、アクセスポイント１０３が構築する無線ネットワーク１０４に接続してもよいし、接続しなくてもよい。
【００１４】
本実施形態において、通信装置１０１は、アクセスポイント１０３に対して無線ネットワーク１０４を形成するための通信パラメータを提供する。また、通信装置１０１は、通信装置１０２に対して無線ネットワーク１０４に接続するための通信パラメータを提供する。通信パラメータには、無線通信を行うために必要な設定項目が含まれ、ネットワーク識別子としてのＳＳＩＤ（Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｅｒ）、暗号化方式、暗号鍵、認証方式、およびＡＫＭなどの少なくともいずれか一つが含まれる。
【００１５】
ＡＫＭとは、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ｔｙｐｅの略であって、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値である。例えば、ＡＫＭが「ｄｐｐ」の場合、通信パラメータには、上記の設定項目に加えて、あるいは代えて、ＤＰＰ規格に対応するアクセスポイントに接続するために必要な情報であるコネクタが含まれる。コネクタは、ＤＰＰ規格によって定められた認証プロトコルや鍵交換アルゴリズムで使用される各種情報である。
【００１６】
なお、ここではＡＫＭが「ｄｐｐ」と表現される場合について説明したが、ＡＫＭの表現はこれに限らず、異なる文字列や数字などであってもよい。ＤＰＰ規格の更新に伴う仕様の変更によって、異なる文字列や数字などの表現が「ｄｐｐ」に相当する表現として割り当てられた場合、新たに割り当てられた文字列や数字がＡＫＭとして設定されている場合には通信パラメータにコネクタを含めるようにしてもよい。
【００１７】
また、ＡＫＭが「ｓａｅ」の場合、通信パラメータには、上記の設定項目に代えて、あるいは加えて、ＷＰＡ（Ｗｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ）３規格に対応するアクセスポイントに接続するための情報であるパスワードが含まれる。なお、ＳＡＥは、Ｓｉｍｕｌｔａｎｅｏｕｓ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ Ｅｑｕａｌｓ（同等性同時認証）の略である。
【００１８】
また、ＡＫＭが「ｓａｅ」の場合、通信パラメータとして、パスワードに加えて、ＳＡＥの情報要素が含まれてもよい。ＳＡＥの情報要素とは、ＳＡＥの仕様で規定されたＰａｓｓｗｏｒｄ Ｉｄｅｎｔｉｆｉｅｒ（以下、Ｉｄｅｎｔｉｆｉｅｒ）のことである。アクセスポイントは、ＢＳＳ（Ｂａｓｉｃ Ｓｅｒｖｉｃｅ Ｓｅｔ）ごとにＩｄｅｎｔｉｆｉｅｒを設定することができる。Ｉｄｅｎｔｉｆｉｅｒが設定されているアクセスポイントと接続するＳＴＡは、設定されているＩｄｅｎｔｉｆｉｅｒを知らないと、アクセスポイントと接続することができない。このように、アクセスポイントは、Ｉｄｅｎｔｉｆｉｅｒを設定することでセキュリティを向上させることができる。Ｉｄｅｎｔｉｆｉｅｒは任意の文字列であって、ユーザによって設定されてもよいし、アクセスポイントに予め設定されていてもよい。また、アクセスポイントはＩｄｅｎｔｉｆｉｅｒを使用してもよいし、使用しなくてもよい。アクセスポイントがＩｄｅｎｔｉｆｉｅｒを使用するか否かは、ユーザによって設定されてもよいし、アクセスポイントに予め設定されていてもよい。

【００１９】
なお、ここではＡＫＭが「ｓａｅ」と表現される場合について説明したが、ＡＫＭの表現はこれに限らず、異なる文字列や数字などであってもよい。ＤＰＰ規格の更新に伴う仕様の変更によって、異なる文字列や数字などの表現が「ｓａｅ」に相当する表現として割り当てられた場合、新たに割り当てられた文字列や数字がＡＫＭとして設定されている場合には通信パラメータにパスワードやＩｄｅｎｔｉｆｉｅｒを含めるようにしてもよい。
【００２０】
また、ＡＫＭが「ｐｓｋ」の場合、通信パラメータには、上記の設定項目に代えて、あるいは加えて、ＷＰＡ３規格の前の規格であるＷＰＡ２規格に対応するアクセスポイントに接続するための情報であるＰＳＫまたはパスフレーズが含まれる。なお、ｐｓｋはＰｒｅ Ｓｈａｒｅｄ Ｋｅｙ（事前共有鍵）の略である。このＰＳＫまたはパスフレーズは、ＷＰＡ２規格に準拠した無線接続で使用される。ＷＰＡ３規格のパスワードやＷＰＡ２規格のＰＳＫ、パスフレーズは、ＷＰＡ２規格やＷＰＡ３規格、ＩＥＥＥ８０２．１１シリーズ規格に準拠した認証または鍵交換を実施する際の暗号鍵である。
【００２１】
なお、ここではＡＫＭが「ｐｓｋ」と表現される場合について説明したが、ＡＫＭの表現はこれに限らず、異なる文字列や数字などであってもよい。ＤＰＰ規格の更新に伴う仕様の変更によって、異なる文字列や数字などの表現が「ｐｓｋ」に相当する表現として割り当てられた場合、新たに割り当てられた文字列や数字がＡＫＭとして設定されている場合には通信パラメータにＰＳＫまたはパスフレーズを含めるようにしてもよい。
【００２２】
本実施形態において、通信装置１０１、１０２の具体例としては、携帯電話、デジタルカメラ、ビデオカメラ、ＰＣ、ＰＤＡ、スマートフォン、およびスマートウォッチなどの電子機器があげられるが、これらに限られるものではない。通信装置１０１および１０２は、無線ネットワークに接続が可能な電子機器であればよく、携帯型でなくてもよい。また、本実施形態においてアクセスポイント１０３の具体例としては、無線ＬＡＮルーターやＰＣなどがあげられるが、これらに限定されない。アクセスポイント１０３は、無線ネットワークを構築する機能を有する電子機器であればよく、プリンタやデジタルカメラなどであってもよい。
【００２３】
なお、通信装置１０１、１０２およびアクセスポイント１０３の少なくともいずれか一台は、ＤＰＰ規格に加えて、Ｗｉ－Ｆｉ Ａｌｌｉａｎｃｅによって策定されたＷｉ－Ｆｉ Ｄｉｒｅｃｔ規格などの規格に対応していてもよい。また、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣ、ＵＷＢ、ＺｉｇＢｅｅ、ＭＢＯＡなどの他の通信規格に対応していてもよい。なお、ＵＷＢはＵｌｔｒａ Ｗｉｄｅ Ｂａｎｄの略であり、ＭＢＯＡはＭｕｌｔｉ Ｂａｎｄ ＯＦＤＭ Ａｌｌｉａｎｃｅの略である。また、ＮＦＣはＮｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎの略である。ＵＷＢには、ワイヤレスＵＳＢ、ワイヤレス１３９４、ＷｉＮＥＴなどが含まれる。あるいは、有線ＬＡＮなどの有線通信の通信規格に対応していてもよい。
【００２４】
図２は、通信装置１０１のハードウェア構成を示す図である。なお、通信装置１０２も通信装置１０１と同様のハードウェア構成を有する。なお、図２で示す各部の一部またはすべてがソフトウェアによって実現されてもよい。
【００２５】
無線通信制御部２０１は、ＤＰＰ規格に準拠した無線通信の制御を行う。また、無線通信制御部２０１は、ＤＰＰ規格に加えて、ＩＥＥＥ８０２．１１シリーズ規格に準拠した無線通信の制御や、有線ＬＡＮなどの有線通信の制御を行ってもよい。無線通信制御部２０１は、アンテナ２１３を制御して、後述の制御部２０５によって生成された無線通信のための無線信号の送受信を行う。通信装置１０１は、無線通信制御部２０１を介して、画像データや文書データ、映像データなどのコンテンツを他の通信装置と通信してもよい。

【００２６】
送受信部２０２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２０１を介して行う。
【００２７】
操作部２０３は、ユーザが通信装置１０１を操作するための各種操作を受け付ける。操作部２０３には、撮像部２０７を起動するためのボタン等が含まれてもよい。なお、操作部２０３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２０４を用いて提供されるＵＩ（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）で構成されてもよい。
【００２８】
表示部２０４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。なお、タッチパネルのように、操作部２０３と表示部２０４とを一つのモジュールで実現するようにしてもよい。また、操作部２０３と表示部２０４とは、夫々通信装置１０１と一体であってもよいし、別体であってもよい。
【００２９】
制御部２０５は、例えばＣＰＵやＭＰＵ等の１つ以上のプロセッサにより構成され、後述の記憶部２０６に記憶されたコンピュータプログラムを実行することにより、通信装置１０１全体を制御する。なお、ＣＰＵはＣｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔの、ＭＰＵはＭｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔの略である。なお制御部２０５は、ＣＰＵやＭＰＵに加えて、あるいは代えて、ＡＳＩＣ（特定用途向け集積回路）、ＤＳＰ（デジタルシグナルプロセッサ）、ＦＰＧＡ（フィールドプログラマブルゲートアレイ）等により構成されてもよい。なお、制御部２０５は、記憶部２０６に記憶されたコンピュータプログラムとＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）との協働により、通信装置１０１全体を制御するようにしてもよい。また、制御部２０５は、他の通信装置との通信において送信するデータや信号を生成する。また、制御部２０５がマルチコア等の複数のプロセッサを備え、複数のプロセッサにより通信装置１０１全体を制御するようにしてもよい。
【００３０】
記憶部２０６は、ＲＯＭやＲＡＭなどの１以上のメモリにより構成され、後述する各種動作を行うためのコンピュータプログラムや、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。ＲＯＭはＲｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙの、ＲＡＭはＲａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙの夫々略である。なお、記憶部２０６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などの記憶媒体が用いられてもよい。
【００３１】
撮像部２０７は、撮像素子、レンズ等を含み、制御部２０５によって制御されることで、静止画や動画の撮影を行う。
【００３２】
画像処理部２０８は、撮像部２０７によって撮影された画像等の画像処理を行う。また、画像処理部２０８は、撮像部２０７により撮影されたＱＲコード（登録商標）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。ＱＲコード情報には、ＤＰＰ規格における通信パラメータの共有処理に用いられる認証用の公開鍵（Ｂｏｏｔｓｔｒａｐｐｉｎｇ　Ｋｅｙ）の情報が含まれる。なお、ＱＲコード情報には、公開鍵の情報に加えて、ＱＲコードに対応する装置の識別情報（ＭＡＣアドレス、装置の名称）や、該装置がＤＰＰ規格におけるコンフィギュレータであるか、またはエンローリであるかを示す情報が含まれていてもよい。
【００３３】
コード生成部２０９は、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２０４へ表示するための制御を行う。なお、本実施形態では、コ

ード情報の画像としてＱＲコードを用いたが、これに限らず、バーコードなどの一次元コードや、ＡｚｔｅｃＣｏｄｅやＳｅｍａｃｏｄｅなどの他の二次元コードなどが用いられてもよい。なお、ＱＲコードなどの機械が読み取り可能な情報に代えて、ユーザが読みとれる形式の情報を生成してもよい。この場合、ユーザが手入力で相手装置にＱＲコード情報に相当する情報を入力することで該情報が共有されるようにしてもよい。

【００３４】

パラメータ処理部２１０は、無線ネットワーク１０４に接続するための通信パラメータの提供や取得を行うための処理を行う。

【００３５】

更新部２１１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。

【００３６】

認証部２１２は、他の装置を認証するための制御を行う。

【００３７】

なお、上記ハードウェア構成は一例であり、複数のハードウェアに対応する機能を１つのハードウェアが有するように構成されてもよいし、何れかのハードウェアが更に複数のハードウェアに分かれてもよい。

【００３８】

図３は、通信装置１０１が通信パラメータを提供する際に、記憶部２０６に記憶されたコンピュータプログラムを制御部２０５に読み出し、実行することで実現される処理を示すフローチャートである。本実施形態において、通信装置１０１はコンフィギュレータとして動作し、エンローリとして動作する通信装置１０２およびアクセスポイント１０３に通信パラメータを提供する。

【００３９】

通信装置１０１は、ユーザから通信パラメータの提供を指示されると、本フローの処理を開始する。あるいは、通信装置１０１は、ユーザから通信パラメータの共有処理の開始を指示されると本フローの処理を開始してもよいし、所定のアプリケーションの起動に応じて本フローの処理を開始してもよい。あるいは、通信装置１０１は、通信装置１０１に電源が投入されたことに基づいて本フローの処理を開始してもよい。

【００４０】

通信装置１０１は、通信装置１０２が表示するＱＲコード（を含む画像）を撮影するために撮像部２０７を起動する（Ｓ３０１）。当該ＱＲコードには、ＱＲコード情報として、通信装置１０２の認証に用いられる、通信装置１０２の公開鍵が含まれる。

【００４１】

通信装置１０１は、撮像部２０７によってＱＲコードを撮影したかを判定する（Ｓ３０２）。通信装置１０１は、ＱＲコードを撮影しなかったと判定されると（Ｓ３０２のＮｏ）、再度Ｓ３０２の処理を実行する。一方、ＱＲコードを撮影したと判定されると（Ｓ３０２のＹｅｓ）、通信装置１０１はＳ３０３の処理を実行する。ここで、通信装置１０２に対応するＱＲコードは、通信装置の表示部２０４等に表示されたものに限らず、通信装置１０２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。また、通信装置１０２に対応するＱＲコードは、例えば通信装置１０２に対する説明書等に記載されたものでもよい。あるいは、通信装置１０２が印刷機能を有している場合、通信装置１０２がＱＲコードを印刷してもよい。なお、Ｓ３０２にて、撮像部２０７の起動から所定の時間内にＱＲコードを撮影したと判定されなかった場合、通信装置１０１は、本フローの処理を終了してもよい。

【００４２】

通信装置１０１は、ＱＲコードを撮影したと判定されると（Ｓ３０２のＹｅｓ）、撮影されたＱＲコードから通信装置１０２の認証用の公開鍵（ＢｏｏｔｓｔｒａｐｐｉｎｇＫｅｙ）を含むＱＲコード情報を取得する（Ｓ３０３）。なお、通信装置１０１は、撮影したＱＲコードに、公開鍵に加えて、通信装置１０２の識別情報や、通信装置１０２がコンフィギュレータであるか、またはエンローリであるかを示す情報が含まれている場合、

これらの情報をＱＲコード情報として取得してもよい。

【００４３】

次に、通信装置１０１は、通信装置１０２に対して認証要求を送信する（Ｓ３０４）。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。通信装置１０１から通信装置１０２に送信される認証要求には、認証に用いるための認証情報と、通信装置１０１の識別情報、乱数、役割情報、および共有鍵生成用の公開鍵が含まれる。認証情報は、Ｓ３０２で撮影したＱＲコードに含まれていた、通信装置１０２の認証用の公開鍵のハッシュ値であり得る。通信装置１０１の識別情報は、通信装置１０１の認証用の公開鍵のハッシュ値であり得る。乱数は、後述する認証応答の受信時において認証のために使用され得る数値である。役割情報とは、通信装置１０１がコンフィギュレータあるいはエンローリ、もしくはその両方で動作することができることを示す情報である。本実施形態において、通信装置１０１は、コンフィギュレータとして動作できることを示す情報を役割情報として認証要求に含めるものとする。共有鍵生成用の公開鍵は、通信装置１０２との間で生成される共有鍵の生成元となる鍵であり得る。

【００４４】

通信装置１０２は、認証要求を受信すると、認証要求を送信した装置（通信装置１０１）がＱＲコードを撮影した装置であるかを判定する。この判定は、認証要求に含まれている認証情報を用いて行われる。通信装置１０２は、自装置が表示したＱＲコードに含めた公開鍵のハッシュ値を計算し、算出したハッシュ値と通信装置１０１が送信した認証要求に含まれるハッシュ値（認証情報）とを比較する。通信装置１０２が算出したハッシュ値と、通信装置１０１から受信したハッシュ値が一致した場合、通信装置１０２は通信装置１０１の認証に成功したと判定する。通信装置１０２は、認証に成功したと判定すると、認証要求に対する応答として、通信装置１０１に認証応答を送信する。一方、通信装置１０２が算出したハッシュ値と、通信装置１０１から受信したハッシュ値とが一致しなかった場合、通信装置１０２は通信装置１０１の認証に失敗したと判定する。通信装置１０２は、認証に失敗したと判定すると、通信装置１０１に認証応答を送信しない。なお、ハッシュ値の計算に用いられるハッシュ関数は、通信装置１０１と通信装置１０２との間で予め共有されているものとする。本実施形態では、通信装置１０２が、自装置の認証用の公開鍵のハッシュ値を算出するとしたが、これに限らず、通信装置１０２は予めハッシュ値を保持していてもよい。

【００４５】

通信装置１０１は、通信装置１０２にＳ３０４において認証要求を送信した後、認証応答を受信したかを判定する（Ｓ３０５）。通信装置１０１は、認証応答を受信すると本判定でＹｅｓと判定し、Ｓ３０６の処理を行う。一方、通信装置１０１は、認証応答を受信しないと本判定でＮｏと判定し、Ｓ３０５の処理を再度行う。なお、通信装置１０１は、Ｓ３０５において所定の時間内に認証応答を受信できなかった場合、本フローの処理を終了し、通信パラメータの提供処理を終了してもよい。認証応答は、例えばＤＰＰ規格で規定されたＤＰＰ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｒｅｓｐｏｎｓｅフレームである。通信装置１０２から通信装置１０１に送信される認証応答には、通信装置１０２の共有鍵生成用の公開鍵、乱数、役割情報、およびタグ情報が含まれる。共有鍵生成用の公開鍵とは、通信パラメータを暗号化するための共有鍵の生成元となる鍵である。役割情報とは、通信装置１０２がコンフィギュレータあるいはエンローリで動作することができることを示す情報である。本実施形態において、通信装置１０２は、エンローリとして動作できることを示す情報を役割情報として認証応答に含めるものとする。また、タグ情報とは、認証要求に含まれていた乱数である。このタグ情報は、通信装置１０２の共有鍵生成用の秘密鍵と、通信装置１０１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る。

【００４６】

通信装置１０１は、認証応答を受信すると（Ｓ３０５のＹｅｓ）、認証応答を送信した

通信装置１０２の認証処理を実行する（Ｓ３０６）。まず、通信装置１０１は、認証応答に含まれている通信装置１０２の共有鍵生成用の公開鍵と、通信装置１０１が保持する自装置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、通信装置１０２は、認証要求を受信した際に、通信装置１０１の共有鍵生成用の公開鍵と、通信装置１０２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。共有鍵は、例えば、ＥＣＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）方式に基づいて生成される。本実施形態において、共有鍵は、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に基づいて生成されてもよい。

【００４７】

続いて、通信装置１０１は、認証応答に含まれるタグ情報を用いて認証処理を行い、認証が成功したかを判定する。通信装置１０１は、受信したタグ情報を自装置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し（Ｓ３０６のＹｅｓ）、Ｓ３０７の処理を実行する。一方、通信装置１０１は、自装置が生成した共有鍵でタグ情報を復号できなかった場合、認証に失敗したと判定し（Ｓ３０６のＮｏ）、Ｓ３１０の処理を実行する。

【００４８】

通信装置１０１は、認証に失敗したと判定された場合（Ｓ３０６のＮｏ）、表示部２０４にエラーを示すメッセージを表示し（Ｓ３１０）、本フローの処理を終了することで、パラメータ提供処理を終了する。なお、Ｓ３１０において通信装置１０１は、エラーを示すメッセージを表示するのに加えて、あるいは代えて、音声やＬＥＤの点滅などによってユーザにエラーを通知してもよい。Ｓ３１０において、通信装置１０１は、パラメータ共有処理においてエラーが発生したことをユーザに通知できればよい。この場合に、通信装置１０１は、通信装置１０２にエラーを通知してもよい。また、通信装置１０１は、Ｓ３１０をスキップして本フローの処理を終了してもよい。

【００４９】

一方、通信装置１０１は、認証に成功したと判定された場合（Ｓ３０６のＹｅｓ）、通信装置１０２へ認証確認を送信する（Ｓ３０７）。この認証確認は、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。タグ情報は、通信装置１０２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。

【００５０】

なお、通信装置１０１は、認証応答を受信した際に、認証応答に含まれる通信装置１０２の役割情報が、自装置の役割情報と同じ場合（コンフィギュレータとコンフィギュレータ、あるいはエンローリとエンローリ）、Ｓ３０６でＮｏと判定してもよい。あるいは、通信装置１０１は、Ｓ３０６でＹｅｓと判定し、エラーを示す情報を含む認証確認を通信装置１０２に送信してもよい。

【００５１】

同様に、通信装置１０２も、認証要求を受信した際に、認証要求に含まれる通信装置１０１の役割情報が、自装置の役割情報と同じ場合（コンフィギュレータとコンフィギュレータ、あるいはエンローリとエンローリ）、エラーを示す認証応答を送信してもよい。あるいは、通信装置１０２は、認証応答を送信せずに処理を終了してもよい。

【００５２】

通信装置１０２は、通信装置１０１から認証確認を受信すると、通信装置１０１の認証処理を実行する。具体的には、通信装置１０２は、認証確認に含まれるタグ情報を、自装置が生成した共有鍵で復号できるかを判定する。通信装置１０２は、認証確認に含まれているタグ情報を、自装置が生成した共有鍵で正しく復号できた場合、認証が成功したと判定する。認証が成功したと判定されると、通信装置１０２は、認証要求を送信した通信装置１０１を、通信パラメータの共有処理を行う相手装置として認定する。本実施形態において、通信装置１０１は、コンフィギュレータとして認定される。通信装置１０２は、認

証に成功すると、通信装置１０１に対して設定要求を送信する。一方、通信装置１０２は、タグ情報を自装置が生成した共有鍵で正しく復号できなかった場合、認証に失敗したと判定し、通信装置１０１に対して認証要求を送信しない。あるいは、通信装置１０２は、通信装置１０１にエラーを通知する。

【００５３】

設定要求は、例えばＤＰＰ規格で規定されたＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｑｕｅｓｔフレームである。設定要求には、通信装置１０２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、通信装置１０２のデバイス名などである。また、役割情報とは、受信した通信パラメータによって通信装置１０２が参加できるネットワークにおいて、通信装置１０２が希望する役割を示す情報である。具体的には、ネットワークを構築するアクセスポイントとしての役割を希望するか、あるいはネットワークに参加するステーションとしての役割を希望するかを示す情報である。本実施形態において、通信装置１０２は、ステーションとしての役割を希望することを示す役割情報を送信する。設定要求に含まれる情報は、通信装置１０２が認証要求を受信した際に生成した共有鍵で暗号化される。

【００５４】

通信装置１０１は、認証確認を送信した後、通信装置１０２から設定要求が送信されたかを判定する（Ｓ３０８）。通信装置１０１は、設定要求を受信すると、Ｓ３０８でＹｅｓと判定し、Ｓ３０９の処理を行う。一方、通信装置１０１は、認証要求を受信しないと、Ｓ３０８でＮｏと判定し、Ｓ３０８の処理を行う。なお、通信装置１０１は、Ｓ３０８において、所定の時間内に設定要求を受信しなかった場合、本フローの終了することで、通信パラメータの提供処理を終了してもよい。この場合に、通信装置１０１はユーザにエラーを通知してもよい。

【００５５】

通信装置１０１は、通信装置１０２から設定要求を受信すると（Ｓ３０８のＹｅｓ）、通信パラメータの提供処理を行う（Ｓ３０９）。本ステップの詳細は、後述の図５で説明する。通信装置１０１は、通信装置１０２に対して無線ネットワーク１０４に参加するための通信パラメータを含む設定応答を送信する。これにより、通信装置１０１と通信装置１０２との間で通信パラメータが共有される。なお、通信装置１０１がアクセスポイント１０３と通信パラメータの共有処理を行う場合、通信装置１０１は本ステップにおいて、アクセスポイント１０３に無線ネットワーク１０４を構築するための通信パラメータを含む設定応答を送信する。

【００５６】

設定応答は、例えばＤＰＰ規格で規定されたＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｓｐｏｎｓｅフレームである。設定応答には、通信パラメータが含まれる。設定応答に含まれる情報は、通信装置１０１がＳ３０６において生成した共有鍵で暗号化される。なお、通信パラメータには、ＡＫＭが含まれる他、ＡＫＭに応じてコネクタ、パスワード、ＰＳＫ、あるいはパスフレーズの少なくとも何れか一つが含まれる。ＡＫＭが「ｄｐｐ」、「ｄｐｐ＋ｓａｅ」、あるいは「ｄｐｐ＋ｓａｅ＋ｐｓｋ」のように、「ｄｐｐ」を含むものである場合、通信パラメータには少なくともコネクタが含まれる。また、ＡＫＭが「ｄｐｐ」を含むものである場合、通信パラメータにＣ－ｓｉｇｎ－ｋｅｙ（公開鍵）も含まれる。Ｃ－ｓｉｇｎ－ｋｅｙはコンフィグレータ専用の公開鍵であり、コネクタはコンフィグレータ専用の秘密鍵で暗号化されている。あるいは、ＡＫＭが「ｐｓｋ」、「ｐｓｋ＋ｓａｅ」、あるいは「ｄｐｐ＋ｓａｅ＋ｐｓｋ」のように、「ｐｓｋ」を含む場合、通信パラメータには少なくともＰＳＫまたはパスフレーズが含まれる。あるいは、ＡＫＭが「ｓａｅ」、「ｐｓｋ＋ｓａｅ」、「ｄｐｐ＋ｓａｅ」、あるいは「ｄｐｐ＋ｓａｅ＋ｐｓｋ」のように「ｓａｅ」を含む場合、通信パラメータにはパスワードが含まれる。これに加えて、ｓａｅの情報要素であるＩｄｅｎｔｉｆｉｅｒが含まれていてもよい。

【００５７】

なお、ここではＡＫＭが「ｄｐｐ」、「ｄｐｐ＋ｓａｅ」、「ｄｐｐ＋ｓａｅ＋ｐｓｋ

」、「ｐｓｋ」、「ｓａｅ」、あるいは「ｐｓｋ＋ｓａｅ」と表現される場合について説明したが、ＡＫＭの表現はこれに限らず、異なる文字列や数字などであってもよい。ＤＰＰ規格の更新に伴う仕様の変更によって、異なる文字列や数字などの表現がこれらのＡＫＭに相当する表現として割り当てられた場合に、新たに割り当てられた文字列や数字に対応する情報を通信パラメータに含めるようにしてもよい。

【００５８】

通信装置１０２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通信装置１０１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通信装置１０２は、設定応答に含まれる情報を、認証要求の受信時に生成した共有鍵で復号する。通信装置１０２は、復号して得られた通信パラメータを使用して、無線ネットワーク１０４に接続することができる。

【００５９】

以上、図３には、通信装置１０１が他の通信装置に通信パラメータを提供する際に実行される処理を示した。通信装置１０１は、ＤＰＰ規格のコンフィギュレータとして、ＤＰＰ規格のエンローリとして動作する通信装置１０２に通信パラメータを提供する。

【００６０】

なお、本実施形態において、通信装置１０１は、通信装置１０２に対応するＱＲコードを撮影することで、通信装置１０２の認証に用いられる公開鍵を取得するとしたが、これに限らず、ＮＦＣ通信やＢｌｕｅｔｏｏｔｈ通信によって取得してもよい。また、通信装置１０１は、ＰＫＥＸ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）　Ｐｒｏｔｏｃｏｌを利用して、通信装置１０２の認証に用いられる公開鍵を取得してもよい。ＰＫＥＸ　Ｐｒｏｔｏｃｏｌを用いる場合、通信装置１０１は、通信装置１０２と共有したコードを用いて通信装置１０２の認証に用いられる公開鍵を取得する。コードとは、文字や数字、記号、あるいはそれらの組み合わせなどによって構成されるものである。

【００６１】

また、本実施形態において、コンフィギュレータである通信装置１０１が通信装置１０２に対応するＱＲコードを撮影し、通信装置１０２の認証に用いる公開鍵（Ｂｏｏｔｓｔｒａｐｐｉｎｇ　Ｋｅｙの）を取得するとした。しかし、これに限らず、通信装置１０２が通信装置１０１に対応するＱＲコードを撮影し、通信装置１０１の認証に用いる公開鍵（Ｂｏｏｔｓｔｒａｐｐｉｎｇ　Ｋｅｙ）を取得するようにしてもよい。この場合、通信装置１０２は、本実施形態において通信装置１０１が行っていた図３のＳ３０１～Ｓ３０７およびＳ３１０の処理を行う。また、通信装置１０１は、本実施形態では通信装置１０２が行っていた、図３のＳ３０１～Ｓ３０７およびＳ３１０に対応する処理を行う。図３のＳ３０８以降の処理は、コンフィギュレータとして動作する通信装置が行う処理であるため、このような場合であっても、通信装置１０１が実行する。

【００６２】

図４は、通信装置１０１が、通信装置１０２またはアクセスポイント１０３と通信パラメータを共有する場合に実行する処理の一例を示すシーケンス図である。本実施形態において、通信装置１０１はＤＰＰ規格に準拠したコンフィギュレータとして、ＤＰＰ規格に準拠したエンローリである通信装置１０２またはアクセスポイント１０３に通信パラメータを提供するものとする。

【００６３】

通信装置１０２は、通信パラメータの受領をユーザから指示されると（Ｓ４０１）、通信装置１０２の表示部２０４にＱＲコードを表示し（Ｓ４０２）、認証要求を待ち受ける。なお、Ｓ４０１でユーザから通信パラメータの受領ではなく、通信の開始や通信パラメータの共有の開始を指示されてもよい。また、通信装置１０２は、認証要求を待ち受けている場合に、所定の時間内に認証要求を受信できなかった場合、通信装置１０２は認証要求の待ち受けを終了してもよい。また、通信装置１０２がＱＲコードを表示するのではなく、通信装置１０２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てもよい。この場合、Ｓ４０２はスキップされる。あるいは通信装置１０２が印刷機能

を有している場合、Ｓ４０２でＱＲコードを印刷してもよい。
【００６４】
一方、通信装置１０１は、通信パラメータの提供をユーザから指示されると（Ｓ４０３）、通信装置１０２の表示するＱＲコードを撮影するために撮像部２０７を起動する（Ｓ４０４）。なお、通信装置１０１は、通信パラメータの提供ではなく、通信の開始を指示されてもよい。通信装置１０１は、通信装置１０２が表示するＱＲコードを撮影し、撮影したＱＲコードからＱＲコード情報を取得する（Ｓ４０５）。通信装置１０１は、ＱＲコード情報として、通信装置１０２の認証に用いられる公開鍵を少なくとも取得する。
【００６５】
ＱＲコードが示す情報を取得した通信装置１０１は、認証要求を生成し、通信装置１０２に送信する（Ｓ４０６）。通信装置１０２は、受信した認証要求に含まれる情報に基づいて、通信装置１０１がＱＲコードを撮影した装置であるかを判定する（Ｓ４０７）。認証要求を送信した通信装置１０１がＱＲコードを撮影した装置であると判定すると、通信装置１０２は、認証応答を生成し、通信装置１０１に送信する（Ｓ４０８）。通信装置１０１に認証応答を送信した通信装置１０２は、通信装置１０１から認証確認が送信されるのを待ち受ける。
【００６６】
認証応答を受信した通信装置１０１は、認証応答の内容に基づいて、通信装置１０２の認証処理を行う（Ｓ４０９）。通信装置１０１は、通信装置１０２の認証に成功した場合、通信装置１０２に認証確認を送信する（Ｓ４１０）。通信装置１０１から認証確認を受信した通信装置１０２は、認証確認の内容に基づいて通信装置１０１の認証処理を行う。通信装置１０２は、自装置が生成した共有鍵を用いて、認証確認に含まれるタグ情報を正しく復号できた場合、認証に成功したと判定する。
【００６７】
通信装置１０２は、認証に成功したと判定すると、通信パラメータの設定処理を行うために、通信装置１０１に設定要求を送信する（Ｓ４１１）。通信装置１０２は、設定要求を送信すると、通信装置１０１から設定応答が送信されるのを待ち受ける。設定要求を受信した通信装置１０１は、通信パラメータを含めた設定応答を通信装置１０２に送信する（Ｓ４１２）。設定応答を受信した通信装置１０２は、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１０４に接続する。
【００６８】
なお、本実施形態では、通信装置１０１が通信装置１０２に通信パラメータを提供する場合を例として説明したが、通信装置１０１がアクセスポイント１０３に通信パラメータを提供する場合も同様の処理が実行される。アクセスポイント１０３は、通信装置１０１から受信した通信パラメータを用いて無線ネットワーク１０４を構築することができる。
【００６９】
以上、図４には、通信装置１０１が通信装置１０２またはアクセスポイント１０３に通信パラメータを提供する際に実行される処理の一例を示した。通信装置１０１は、ＤＰＰ規格のコンフィギュレータとして、ＤＰＰ規格のエンローリとして動作する通信装置１０２またはアクセスポイント１０３に通信パラメータを提供する。
【００７０】
図５に、通信装置１０１が図３のＳ３０９において実行する処理を示すフローチャートである。本実施形態において、通信装置１０１は、無線ＬＡＮのセキュリティ規格であるＷｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　３（ＷＰＡ３）規格に対応しているものとする。通信装置１０１は、ＷＰＡ３規格に対応していることから、暗号鍵の共有の方式としてＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｏｆ　Ｅｑｕａｌｓ）を用いることができる。また、通信装置１０１は、ＡＫＭ＝「ｓａｅ」の場合に、通信パラメータとして、パスワードだけなく、ＳＡＥのオプションの情報要素も提供できるものとする。ＳＡＥのオプションの情報要素とは、ＳＡＥの仕様のアップデートによって追加されたＰａｓｓｗｏｒｄ　Ｉｄｅｎｔｉｆｉｅｒ（以下、Ｉｄｅｎｔｉｆｉｅｒ

）のことである。
【００７１】
　ＩｄｅｎｔｉｆｉｅｒはＳＡＥの仕様のアップデートによって追加されたため、アップデート後のＳＡＥ仕様に対応していない通信装置は、通信パラメータとしてＩｄｅｎｔｉｆｉｅｒを受信しても、無効な情報として判定してしまう虞がある。また、通信装置１０１が通信装置１０２とアクセスポイント１０３との両方に通信パラメータを提供する場合であって、一方がＩｄｅｎｔｉｆｉｅｒに対応していない場合は、相互接続性を確保するためにＩｄｅｎｔｉｆｉｅｒを提供しない方が適切である。
【００７２】
　本フローチャートの処理は、通信装置１０１が図３のＳ３０８でＹｅｓと判定した場合に開始される。
【００７３】
　通信装置１０１は、まず、自装置が提供する通信パラメータのＡＫＭが「ｓａｅ」を含むものであるかを判定する（Ｓ５０６）。具体的には、通信装置１０１は、提供する通信パラメータのＡＫＭが「ｓａｅ」、「ｐｓｋ＋ｓａｅ」、「ｄｐｐ＋ｓａｅ」、あるいは「ｄｐｐ＋ｐｓｋ＋ｓａｅ」であるかを判定する。なお、通信パラメータのＡＫＭは、通信パラメータの提供先である通信装置１０２あるいはアクセスポイント１０３が、ＤＰＰとＰＳＫとＳＡＥとの何れに対応しているかに基づいて通信装置１０１が選択する。通信装置１０１は、相手装置が対応している暗号鍵の共有の方式を含むＡＫＭを選択してもよい。あるいは通信装置１０１は、通信装置１０２に通信パラメータを提供する場合に、通信装置１０２を接続させたいアクセスポイント１０３が対応している暗号鍵の共有の方式を含むＡＫＭを選択するようにしてもよい。あるいは、通信装置１０１は、何れの暗号鍵の共有の方式に対応した通信パラメータを提供するかをユーザに選択させ、ユーザ選択に応じたＡＫＭを選択するようにしてもよい。通信装置１０１は、提供する通信パラメータのＡＫＭが「ｓａｅ」を含む場合は、Ｓ５０６でＹｅｓと判定し、Ｓ５０１の処理を行う。一方、提供する通信パラメータのＡＫＭが「ｓａｅ」を含まない場合は、Ｓ５０６でＮｏと判定し、Ｓ５０５の処理を行う。
【００７４】
　通信装置１０１は、相手装置である通信装置１０２またはアクセスポイント１０３に通信パラメータの提供を行う（Ｓ５０５）。通信装置１０１は、通信パラメータを含む設定応答を相手装置に送信する。この場合に、通信装置１０１は、ＡＫＭに応じて適切な通信パラメータを提供する。例えばＡＫＭが「ｄｐｐ」を含むものであった場合、通信装置１０１は、コネクタを含む通信パラメータを提供する。あるいはＡＫＭが「ｐｓｋ」を含むものであった場合は、通信装置１０１はＰＳＫまたはパスフレーズを含む通信パラメータを提供する。通信装置１０１は、Ｓ５０５の処理を行うと本フローを終了する。
【００７５】
　一方、Ｓ５０６でＹｅｓと判定された場合、通信装置１０１は、まず自端末が提供する通信パラメータとして、Ｐａｓｓｗｏｒｄ　Ｉｄｅｎｔｉｆｉｅｒを保有しているかを判定する（Ｓ５０１）。例えば、通信装置１０１が提供する通信パラメータとして、Ｐａｓｓｗｏｒｄ　Ｉｄｅｎｔｉｆｉｅｒがユーザによって入力されている場合、通信装置１０１は本ステップでＹｅｓと判定する。あるいは、通信装置１０１が既にアクセスポイント１０３に接続済みであって、アクセスポイント１０３がＩｄｅｎｔｉｆｉｅｒを設定している場合、通信装置１０１は本ステップでＹｅｓと判定する。あるいは、通信装置１０１が、Ｉｄｅｎｔｉｆｉｅｒを含んだ通信パラメータの提供をユーザあるいはアプリケーションから指示されている場合、通信装置１０１は本ステップでＹｅｓと判定する。通信装置１０１は本ステップでＹｅｓと判定すると、Ｓ５０３の処理を行う。一方、通信装置１０１は、本ステップでＮｏと判定すると、Ｓ５０４の処理を行う。
【００７６】
　通信装置１０１は、通信パラメータを提供する相手装置がＰａｓｓｗｏｒｄ　Ｉｄｅｎｔｉｆｉｅｒを利用するかを判定する（Ｓ５０２）。具体的には、通信装置１０１は、相

手装置がＳＡＥのアップデート後の仕様に対応しているかを判定する。通信装置１０１は、相手装置から受信した認証応答、設定要求、あるいはビーコンの少なくとも何れか一つに含まれる情報に基づいて本ステップの判定を行う。通信装置１０１は、受信した信号の、アップデート後のＳＡＥ仕様（Ｉｄｅｎｔｉｆｉｅｒを利用するＳＡＥ仕様）に対応していることを示すビットが立っているか否かに基づいて判定してもよい。この場合、通信装置１０１はビットが立っている場合は本ステップでＹｅｓと判定し、ビットが立っていない場合は本ステップでＮｏと判定する。なお、該ビットは、認証応答、設定要求、あるいはビーコンに限らず、相手装置が送信する何れの信号に含まれていてもよい。また、該ビットは、Ｉｄｅｎｔｉｆｉｅｒの利用を要求する、あるいはＩｄｅｎｔｉｆｉｅｒに対応することを示すものであってもよい。また、アップデート後のＳＡＥ仕様（Ｉｄｅｎｔｉｆｉｅｒを利用するＳＡＥ仕様）に対応していることを示す情報は、ビットではなく他の形式によって示されてもよい。この場合、アップデート後のＳＡＥ仕様に対応していない相手装置は、アップデート後のＳＡＥ仕様に対応していないことを示す情報を含む信号を送信してもよいし、あるいはアップデート後のＳＡＥ仕様に関する情報を含まない信号を送信してもよい。

【００７７】

また、通信装置１０１は、本ステップにおいて、ＤＰＰ規格の認証応答や設定要求などに含まれる、相手装置が対応するＳＡＥまたはＤＰＰのバージョン情報に基づいて判定してもよい。相手装置が対応するＳＡＥの仕様に関する情報、Ｉｄｅｎｔｉｆｉｅｒの利用に対応するかの情報、またはＩｄｅｎｔｉｆｉｅｒの利用を要求するかの情報の少なくとも何れか一つを取得することができなかった場合、通信装置１０１はＮｏと判定してもよい。通信装置１０１は、本ステップでＹｅｓと判定するとＳ５０３の処理を行う。一方、本ステップでＮｏと判定した場合、通信装置１０１はＳ５０４の処理を行う。

【００７８】

通信装置１０１は、相手装置に提供する通信パラメータとして、Ｉｄｅｎｔｉｆｉｅｒのパラメータを設定する（Ｓ５０３）。

【００７９】

ここで、図６に、通信装置１０１が提供する通信パラメータに含まれるパラメータの一例を示した。Ｐａｒａｍｅｔｅｒ６０２は、通信パラメータにどのようなパラメータが含まれるかを示す。Ｎａｍｅ６０３は、各パラメータの名称を示す。Ｔｙｐｅ６０４は、各パラメータのデータ型を示す。Ｖａｌｕｅは、各パラメータとして設定されうる値を示す。なお、Ｖａｌｕｅは全てのパラメータに設定されているものではなく、任意の値をとり得るものや、値が特に設定されないものについては空欄になっている。

【００８０】

Ｗｉ－Ｆｉ　Ｔｅｃｈｎｏｌｏｇｙ　Ｏｂｊｅｃｔは、通信パラメータに含まれるパラメータが何れの通信方式に対応したパラメータであるかを示す情報である。例えばｗｉ－ｆｉ＿ｔｅｃｈ＝ｉｎｆｒａの場合、通信パラメータとして含まれているパラメータは、インフラストラクチャ方式の無線通信に対応したパラメータである。その他にも、例えば通信装置１０１は、Ｗｉ－Ｆｉ　Ａｗａｒｅ規格に準拠した無線通信に対応するパラメータを提供する場合、ｗｉ－ｆｉ＿ｔｅｃｈ＝ｎａｎとする。あるいは、Ｗｉ－Ｆｉ　Ｄｉｒｅｃｔ規格に準拠した無線通信に対応するパラメータを提供する場合、通信装置１０１はｗｉ－ｆｉ＿ｔｅｃｈ＝ｐ２ｐとする。通信装置１０１は、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅによって策定された無線通信規格に準拠した無線通信に対応するパラメータを提供する場合、ｗｉ－ｆｉ＿ｔｅｃｈとして該無線通信規格に対応する情報を設定することができる。本実施形態において、通信装置１０１は、インフラストラクチャ方式の無線通信に対応する通信パラメータを提供するので、通信装置１０１が提供する通信パラメータにはｗｉ－ｆｉ＿ｔｅｃｈ＝ｉｎｆｒａが含まれる。

【００８１】

Ｓｅｒｖｉｃｅは、前述のＷｉ－Ｆｉ　Ｔｅｃｈｎｏｌｏｇｙ　Ｏｂｊｅｃｔの値に応じて設定されるオプションのパラメータである。Ｓｅｒｖｉｃｅは通信パラメータに含まれ

てもよいし、含まれなくてもよい。
【００８２】
ＳＳＩＤは、通信装置１０１から通信パラメータを提供された通信装置が接続すべきネットワークのネットワーク名を示す情報である。
【００８３】
ＡＫＭとは、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値である。ＡＫＭに「ｄｐｐ」が含まれる場合、通信装置１０１は、通信パラメータに、ＤＰＰ ＣｏｎｎｅｃｔｏｒとＣ－ｓｉｇｎ－ｋｅｙを含ませる。また、ＡＫＭに「ｐｓｋ」が含まれる場合、通信装置１０１は、通信パラメータに、Ｐｒｅ－ｓｈａｒｅｄ ｋｅｙ（ＰＳＫ）またはＷＰＡ２ Ｐａｓｓｐｈｒａｓｅ（パスフレーズ）を含ませる。また、ＡＫＭに「ｓａｅ」が含まれる場合、通信装置１０１は、通信パラメータに、ＳＡＥ ｐａｓｓｗｏｒｄを含ませる。
【００８４】
更に、通信装置１０１は、通信パラメータとしてＩｄｅｎｔｉｆｉｅｒを設定する場合、提供する通信パラメータとしてＳＡＥ Ｉｄｅｎｔｉｆｉｅｒ６０１を含める。このＳＡＥ Ｉｄｅｎｔｉｆｉｅｒ６０１は、任意の文字列であらわされるパラメータである。なお、本実施形態では、ＷＰＡ２ Ｐａｓｓｐｈｒａｓｅ ａｎｄ／ｏｒ ＳＡＥ ｐａｓｓｗｏｒｄの後に含まれるとしたが、これに限らず、図６に示した何れのパラメータの後あるいは前に含まれてもよい。あるいは、通信装置１０１は、Ｉｄｅｎｔｉｆｉｅｒを設定する場合に、ＳＡＥ ｐａｓｓｗｏｒｄの後続にＩｄｅｎｔｉｆｉｅｒをつなげたものをＳＡＥ ｐａｓｓｗｏｒｄとすることで、Ｉｄｅｎｔｉｆｉｅｒを設定してもよい。この場合、通信装置１０１は、通信パラメータとしてＳＡＥ Ｉｄｅｎｔｉｆｉｅｒ６０１を設定しなくてもよい。また、通信装置１０１は、通信パラメータとして図６に示したものの全てを提供する必要はなく、少なくとも何れか一つを提供すればよい。
【００８５】
図５の説明に戻る。通信装置１０１は、Ｓ５０３の処理を行った後、Ｓ５０５の処理を行う。この場合、通信装置１０１が提供する通信パラメータには、Ｉｄｅｎｔｉｆｉｅｒが含まれる。
【００８６】
一方、Ｓ５０２でＮｏと判定された場合、通信装置１０１は提供する通信パラメータとして、Ｉｄｅｎｔｉｆｉｅｒのパラメータを設定しない（Ｓ５０４）。そして、通信装置１０１は通信パラメータを提供する（Ｓ５０５）。この場合、通信装置１０１が提供する通信パラメータには、Ｉｄｅｎｔｉｆｉｅｒは含まれない。通信装置１０１は、Ｓ５０５の処理を行うと、本フローの処理を終了する。
【００８７】
以上のように、通信装置１０１は、図５の処理を行うことで、ＳＡＥのＩｄｅｎｔｉｆｉｅｒを利用する相手装置にはＩｄｅｎｔｉｆｉｅｒを提供し、利用しない装置にはＩｄｅｎｔｉｆｉｅｒを提供しないように制御できる。これにより、通信装置１０１は、適切にＳＡＥのＩｄｅｎｔｉｆｉｅｒを提供することができる。
【００８８】
なお、本実施形態では、ＳＡＥのＩｄｅｎｔｉｆｉｅｒを通信パラメータに含む場合も含まない場合も、ＡＫＭはいずれも「ｓａｅ」であるとしたが、これに限らず、Ｉｄｅｎｔｉｆｉｅｒを含む場合と含まない場合とで異なるＡＫＭを用いるようにしてもよい。あるいは、ＳＡＥのＩｄｅｎｔｉｆｉｅｒを利用する場合としない場合とで異なるＡＫＭを用いるようにしてもよい。具体的には、通信パラメータにＩｄｅｎｔｉｆｉｅｒを含む場合や、Ｉｄｅｎｔｉｆｉｅｒを利用する場合のＡＫＭは、「ｓａｅｉｄ」とし、Ｉｄｅｎｔｉｆｉｅｒを含まない場合や利用しない場合のＡＫＭは「ｓａｅ」とするようにしてもよい。あるいは、各ＡＫＭは、文字列ではなく互いに区別できる数字などで表現されてもよい。
【００８９】

また、本実施形態では、通信装置１０１は、ＡＫＭの値や、相手装置がＩｄｅｎｔｉｆｉｅｒを利用するかに基づいて、通信パラメータとしてＩｄｅｎｔｉｆｉｅｒを利用するか否かを判定したが、これに限らない。通信装置１０１は、通信装置１０２に通信パラメータを提供する場合に、既にアクセスポイント１０３に提供した通信パラメータにＩｄｅｎｔｉｆｉｅｒが含まれているか否かに基づいて判定を行ってもよい。具体的には、通信装置１０１は、アクセスポイント１０３に提供した通信パラメータにＩｄｅｎｔｉｆｉｅｒが含まれていた場合は、通信装置１０２に提供する通信パラメータにもＩｄｅｎｔｉｆｉｅｒを含めると判定する。一方、通信装置１０１は、アクセスポイント１０３に提供した通信パラメータにＩｄｅｎｔｉｆｉｅｒが含まれていなかった場合は、通信装置１０２に提供する通信パラメータにもＩｄｅｎｔｉｆｉｅｒを含めないと判定する。通信パラメータの提供装置は、ＡＰにＩｄｅｎｔｉｆｉｅｒを含むＢＳＳの通信パラメータを提供したか否かに基づいて、ＳＴＡにＩｄｅｎｔｉｆｉｅｒを提供するか判定することで、該ＢＳＳに接続するための適切な通信パラメータを提供することができる。

【００９０】

図７は、通信装置１０２が通信装置１０１から取得したＳＡＥの情報要素を用いてアクセスポイント１０３との無線接続を確立する際に実行する処理を示すシーケンス図である。

【００９１】

通信装置１０２は、アクセスポイント１０３からビーコンを受信することで、アクセスポイント１０３を検出する（Ｓ７０１）。アクセスポイント１０３は、自装置が構築している無線ネットワークにＩｄｅｎｔｉｆｉｅｒが設定されている場合、自装置が構築している無線ネットワークに参加するためには、Ｉｄｅｎｔｉｆｉｅｒが必要であることを示す情報を含ませる。

【００９２】

あるいは、通信装置１０２は、特定のチャネルまたは全チャネルにおいてプローブリクエストを送信することで、アクセスポイント１０３を検索してもよい。この場合、通信装置１０２は、送信したプローブリクエストに対する応答として、アクセスポイント１０３からプローブレスポンスを受信することで、アクセスポイント１０３を検出する。なお、アクセスポイント１０３が構築している無線ネットワークに参加するためには、Ｉｄｅｎｔｉｆｉｅｒが必要であることを示す情報は、プローブレスポンスに含まれていてもよい。

【００９３】

通信装置１０２は、アクセスポイント１０３を検出すると、Ｉｄｅｎｔｉｆｉｅｒを用いて、ＰＷＥを算出する（Ｓ７０２）。ＰＷＥは、ｐａｓｓｗｏｒｄ　ｅｌｅｍｅｎｔの略である。

【００９４】

ＳＡＥでは、楕円曲線暗号を利用してＰＷＥの算出を行う。アクセスポイント１０３と通信装置１０２とは事前に楕円曲線ｙ＾２＝ｘ＾３＋ａｘ＋ｂ　ｍｏｄ　ｐのパラメータａおよびｂを共有しておく。

【００９５】

通信装置１０２は、ＤＰＰによって通信装置１０１から提供されたパスワードの後続にＩｄｅｎｔｉｆｉｅｒをつなげたものをｂａｓｅとして、ｐｗｄ－ｓｅｅｄという情報を以下の式を用いて算出する。なお、ｂａｓｅ　＝　ｐａｓｓｗｏｒｄ｜｜ｉｄｅｎｔｉｆｉｅｒである。

ｐｗｄ－ｓｅｅｄ　＝　Ｈ　（ＭＡＸ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ）｜｜ＭＩＮ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ），　ｂａｓｅ｜｜ｃｏｕｎｔｅｒ）

なお、ＳＴＡ－Ａ－ＭＡＣおよびＳＴＡ－Ｂ－ＭＡＣは夫々、通信装置１０２およびアクセスポイント１０３のＭＡＣアドレスである。ＭＡＸ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ）は通信装置１０２またはアクセスポイント１０３のＭＡＣアドレスのうち、値が大きいもののことである。ＭＩＮ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ）は、通信装置１０２またはアクセスポイント１０３のＭＡＣアドレスのうち、値が小さいもののことである。ｃｏｕｎｔｅｒは、ｐｗｄ－ｓｅｅｄの初回の計算では１に設定され

ている。通信装置１０２は、ＭＡＸ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ）、にＭＩＮ（ＳＴＡ－Ａ－ＭＡＣ，　ＳＴＡ－Ｂ－ＭＡＣ）をつなげたものと、ｂａｓｅにｃｏｕｎｔｅｒをつなげたものを変数として、ハッシュ値を算出します。算出されたハッシュ値が、ｐｗｄ－ｓｅｅｄになる。

【００９６】

続いて、通信装置１０２は、算出したｐｗｄ－ｓｅｅｄを用いて、以下の式のように以下の式のように鍵導出関数（Ｋｅｙ　ｄｅｒｉｖａｔｉｏｎ　ｆｕｎｃｔｉｏｎ、ＫＤＦ）による計算を行うことで、ｐｗｄ－ｖａｌｕｅを算出する。

ｐｗｄ－ｖａｌｕｅ　＝　ＫＤＦ－Ｈａｓｈ－Ｌｅｎｇｔｈ（ｐｗｄ－ｓｅｅｄ，　“ＳＡＥ Ｈｕｎｔｉｎｇ　ａｎｄ　Ｐｅｃｋｉｎｇ”，　ｐ）

“ＳＡＥ Ｈｕｎｔｉｎｇ　ａｎｄ　Ｐｅｃｋｉｎｇ”は、この鍵導出関数によって導出される鍵の目的を識別するための文字列である。ｐは予め決められている素数である。上記の計算により、ｐｗｄ－ｓｅｅｄは、素数ｐのビット長に等しい長さまで拡張される。

【００９７】

次に、通信装置１０２は、ｘ＝ｐｗｄ－ｖａｌｕｅを楕円曲線ｙ＾２＝ｘ＾３＋ａｘ＋ｂ　ｍｏｄ　ｐに代入し、ｙを求める。以上の計算を行うことで、アクセスポイント１０３はＰＷＥ＝（ｘ，ｙ）を求めることができる。

【００９８】

続いて通信装置１０２は、算出したＰＷＥから、アクセスポイント１０３に送信するｃｏｍｍｉｔ　ｓｃａｌａｒとＣＯＭＭＩＴ－ＥＬＥＭＥＮＴを求める。まず通信装置１０２は、秘密の値ｒａｎｄと、一時的に秘密の値ｍａｓｋを決定する。また、通信装置１０２は、アクセスポイント１０３と素数ｒを共有する。通信装置１０２は、以下の夫々を計算し、ｃｏｍｍｉｔ　-ｓｃａｌａｒとＣＯＭＭＩＴ－ＥＬＥＭＥＮＴを算出する。

ｃｏｍｍｉｔ　ｓｃａｌａｒ＝（ｒａｎｄ＋ｍａｓｋ）ｍｏｄ　ｒ

ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ＝ｉｎｖｅｒｓｅ（ｓｃａｌａｒ－ｏｐ（ｍａｓｋ，　ＰＷＥ））

通信装置１０２は、アクセスポイント１０３に対してＡｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｑｕｅｓｔを送信する（Ｓ７０２）。この場合に、送信されるＡｕｔｈｅｎｔｉｃａｔｉｏｎ　ｒｅｑｕｅｓｔには、通信装置１０２が算出したｃｏｍｍｉｔ　ｓｃａｌａｒとＣＯＭＭＩＴ－ＥＬＥＭＥＮＴを含む、ＳＡＥ　ｃｏｍｍｉｔｍｅｎｔ　ｍｅｓｓａｇｅが含まれる。

【００９９】

ｃｏｍｍｉｔ　ｓｃａｌａｒとＣＯＭＭＩＴ－ＥＬＥＭＥＮＴを含むＳＡＥ　ｃｏｍｍｉｔｍｅｎｔ　ｍｅｓｓａｇｅを受信したアクセスポイント１０３は、ＰＭＫの生成を行う（Ｓ７０３）。ＰＭＫとはＰａｉｒｗｉｓｅ　Ｍａｓｔｅｒ　Ｋｅｙの略である。まずアクセスポイント１０３は以下の計算を行い、ｓｈａｒｅｄ　ｓｅｃｒｅｔ　ｅｌｅｍｅｎｔであるＫを以下の式から生成する。なお、受信した通信装置１０２のｃｏｍｍｉｔ　ｓｃａｌａｒとＣＯＭＭＩＴ－ＥＬＥＭＥＮＴは、夫々ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒおよびＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴとする。

Ｋ＝ｓｃａｌａｒ－ｏｐ（ｒａｎｄ，　（ｅｌｅｍ－ｏｐ（ｓｃａｌａｒ－ｏｐ（ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒ，　ＰＷＥ），　ＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ））

続いて、アクセスポイント１０３は、算出したＫから秘密の値ｋを算出する。

ｋ＝Ｆ（Ｋ）

関数Ｆは、Ｋ＝（ｘ，ｙ）の場合、Ｆ（Ｋ）＝ｘを返すような関数である。

【０１００】

続いて、アクセスポイント１０３は、算出したｋを使って以下の式からｋｅｙｓｅｅｄを算出する。

ｋｅｙｓｅｅｄ＝Ｈ（＜０＞３２，　ｋ）

＜０＞３２は、値０の３２オクテットで構成されることを示す記号である。アクセスポ

イント１０３は、＜０＞３２とｋを変数として、ハッシュ値を算出する。
【０１０１】
次にアクセスポイント１０３は算出したｋｅｙｓｅｅｄをつかって、ｋｃｋ＿ａｎｄ＿ｐｍｋを算出する。
ｋｃｋ＿ａｎｄ＿ｐｍｋ＝ＫＤＦ－Ｈａｓｈ－５１２（ｋｅｙｓｅｅｄ，“ＳＡＥ ＫＣＫ ａｎｄ ＰＭＫ”，（ｃｏｍｍｉｔ－ｓｃａｌａｒ＋ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒ）ｍｏｄ ｒ）
ＫＤＦ－Ｈａｓｈ－５１２（）は鍵導出関数である。“ＳＡＥ ＫＣＫ ａｎｄ ＰＭＫ”は、この鍵導出関数によって導出される鍵の目的を識別するための文字列である。
【０１０２】
続いてアクセスポイント１０３は、算出したｋｃｋ＿ａｎｄ＿ｐｍｋから、以下の式によってＫＣＫとＰＭＫを算出する。
ＫＣＫ ＝ Ｌ（ｋｃｋ＿ａｎｄ＿ｐｍｋ，０，２５６）
ＰＭＫ ＝ Ｌ（ｋｃｋ＿ａｎｄ＿ｐｍｋ，２５６，２５６）
ＫＣＫもＰＭＫも計算結果は２５６ビットとなる。具体的には、ＫＣＫは、ｋｃｋ＿ａｎｄ＿ｐｍｋの０ビットから２５５ビット（最初の２５６ビット）として算出される。また、ＰＭＫは、ｋｃｋ＿ａｎｄ＿ｐｍｋの２５６ビットから５１１ビット（次の２５６ビット）として算出される。
【０１０３】
アクセスポイント１０３は、ここまでの計算を行うと、ＳＡＥ ｃｏｍｍｉｔｍｅｎｔ ｍｅｓｓａｇｅに対する応答であるＳＡＥ ｃｏｎｆｉｒｍａｔｉｏｎ ｍｅｓｓａｇｅに含めるためのｃｏｎｆｉｒｍの算出を行う。
ｃｏｎｆｉｒｍ ＝ ＣＮ（ＫＣＫ，ｓｅｎｄ－ｃｏｎｆｉｒｍ，ｃｏｍｍｉｔ－ｓｃａｌａｒ，ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ，ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒ，ＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ）
ｓｅｎｄ－ｃｏｎｆｉｒｍおよびｃｏｍｍｉｔ－ｓｃａｌａｒは、アクセスポイント１０３が決定した秘密の値ｒａｎｄと、一時的に秘密の値ｍａｓｋを用いて算出したものである。ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒおよびＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴは、通信装置１０２から受信したものである。ｓｅｎｄ－ｃｏｎｆｉｒｍは、リプレイ防止カウンターとしてＳＡＥで用いられるカウンターの値である。ＣＮ（）はハッシュ値を計算する関数である。
【０１０４】
アクセスポイント１０３は、ｃｏｎｆｉｒｍを算出すると、ｃｏｎｆｉｒｍを含めたＳＡＥ ｃｏｎｆｉｒｍａｔｉｏｎ ｍｅｓｓａｇｅを含むＡｕｔｈｅｎｔｉｃａｔｉｏｎ ｒｅｓｐｏｎｓｅを通信装置１０２に送信する（Ｓ７０５）。
【０１０５】
Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｒｅｓｐｏｎｓｅを受信した通信装置１０２は、同様にＫＣＫとＰＭＫを算出する。また、アクセスポイント１０３を認証するために、ｖｅｒｉｆｉｅｒを以下の式から算出する。
ｖｅｒｉｆｉｅｒ ＝ ＣＮ（ＫＣＫ，ｐｅｅｒ－ｓｅｎｄ－ｃｏｎｆｉｒｍ，ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒ，ＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ，ｃｏｍｍｉｔ－ｓｃａｌａｒ，ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴ）
ｐｅｅｒ－ｃｏｍｍｉｔ－ｓｃａｌａｒおよびＰＥＥＲ－ＣＯＭＭＩＴ－ＥＬＥＭＥＮＴは、アクセスポイント１０３が算出したｃｏｍｍｉｔ－ｓｃａｌａｒおよびＣＯＭＭＩＴ－ＥＬＥＭＥＮＴになる。ｃｏｍｍｉｔ－ｓｃａｌａｒおよびＣＯＭＭＩＴ－ＥＬＥＭＥＮＴは、通信装置１０２が算出したものになる。また、ｐｅｅｒ－ｓｅｎｄ－ｃｏｎｆｉｒｍは、アクセスポイント１０３から受信したＳＡＥ ｃｏｎｆｉｒｍａｔｉｏｎ ｍｅｓｓａｇｅから推定される、アクセスポイント１０３のＳＡＥで用いられるカウンターの値である。アクセスポイント１０３が算出したｃｏｎｆｉｒｍと、通信装置１０２が算出したｖｅｒｉｆｉｅｒが一致した場合、通信装置１０２はアクセスポイント１０３を認証

する。
【０１０６】
アクセスポイント１０３を認証した通信装置１０２は、同様にＰＭＫの算出を行う（Ｓ７０６）。ＰＭＫを算出した通信装置１０２は、アクセスポイント１０３にＡｓｓｏｃｉａｔｉｏｎ　ｒｅｑｕｅｓｔを送信する（Ｓ７０７）。通信装置１０２からＡｓｓｏｃｉａｔｉｏｎ　ｒｅｑｕｅｓｔを受信したアクセスポイント１０３は、応答としてＡｓｓｏｃｉａｔｉｏｎ　ｒｅｓｐｏｎｓｅを通信装置１０２に送信する（Ｓ７０８）。
【０１０７】
通信装置１０２とアクセスポイント１０３とは、４　ｗａｙ　ｈａｎｄｓｈａｋｅを行う（Ｓ７０９）。４　ｗａｙ　ｈａｎｄｓｈａｋｅでは、通信装置１０２とアクセスポイント１０３とはそれぞれのＭＡＣアドレスを共有する。なお、通信装置１０２とアクセスポイント１０３とはそれぞれのＭＡＣアドレスを共有済みなので、本ステップでのＭＡＣアドレスの共有は省略されてもよい。また、通信装置１０２とアクセスポイント１０３とは、夫々が決定した乱数の共有を行う。通信装置１０２とアクセスポイント１０３とは、共有したＭＡＣアドレスおよび乱数と、算出したＰＭＫから、ＰＴＫ（Ｐａｉｒ－ｗｉｓｅ　Ｔｒａｎｓｉｅｎｔ　Ｋｅｙ）を生成する。通信装置１０２とアクセスポイント１０３とは、生成したＰＴＫを用いて通信を行うことができる。
【０１０８】
以上の処理を行うことで、通信装置１０２とアクセスポイント１０３とは、暗号鍵の共有の方式としてＳＡＥを用いて通信を確立することができる。
【０１０９】
このように、暗号鍵の共有の方式としてＳＡＥを用いる場合、通信装置１０２はパスワードにＩｄｅｎｔｉｆｉｅｒを続けたものに対して楕円曲線暗号を用いてＰＭＫを算出した。暗号鍵の共有の方式としてＳＡＥを用いる場合、パスワードだけでなくＩｄｅｎｔｉｆｉｅｒも用いてＰＭＫを算出するため、仮にパスワードが同じでもＩｄｅｎｔｉｆｉｅｒが異なれば、異なるＰＭＫが算出される。
【０１１０】
一方、暗号鍵の共有の方式としてＰＳＫを用いる場合、通信装置１０２およびアクセスポイント１０３は、ＰＳＫまたはパスフレーズをそのままＰＭＫとして用いる。そのため、図７のＳ７０２やＳ７０６で示したような算出処理は不要となる。
【０１１１】
暗号鍵の共有の方式としてＰＳＫを用いる場合と比べ、ＳＡＥを用いる場合、単にパスフレーズやＰＳＫをそのままＰＭＫとして用いるのではなく、楕円曲線暗号を用いてＰＭＫを算出するため、セキュリティ強度が高い。また、ＳＡＥを用いる場合、パスワードだけではなく、Ｉｄｅｎｔｉｆｉｅｒを設定することで、ユーザは簡単にネットワーク毎に異なるＰＭＫを設定することができる。また、ユーザはネットワーク毎にＩｄｅｎｔｉｆｉｅｒを設定することで、ネットワーク毎に異なるＰＭＫが必要になるため、セキュリティ強度を高めることができる。
【０１１２】
なお、本実施形態において、通信装置１０１は、アクセスポイント１０３が形成する無線ネットワーク１０４に関する通信パラメータを提供するとした。しかし、これに限らず、通信装置１０１は、Ｗｉ－Ｆｉ　Ｄｉｒｅｃｔ規格に準拠したグループオーナーが形成する無線ネットワークに関する通信パラメータを提供するようにしてもよい。
【０１１３】
なお、図３および図５に示した通信装置１０１のフローチャートの少なくとも一部または全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コンピュータプログラムからＦＰＧＡ上に専用回路を生成し、これを利用すればよい。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。

【０１１４】

また、図４に示した通信装置１０１のシーケンスおよび図７に示した通信装置１０２のシーケンスの少なくとも一部または全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コンピュータプログラムからＦＰＧＡ上に専用回路を生成し、これを利用すればよい。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。

【０１１５】

以上、実施形態を詳述したが、本発明は例えば、システム、装置、方法、プログラム若しくは記録媒体（記憶媒体）などとしての実施態様をとることが可能である。具体的には、複数の機器（例えば、ホストコンピュータ、インターフェース機器、撮像装置、ｗｅｂアプリケーションなど）から構成されるシステムに適用してもよいし、また、一つの機器からなる装置に適用してもよい。

【０１１６】

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、ＡＳＩＣ）によっても実現可能である。

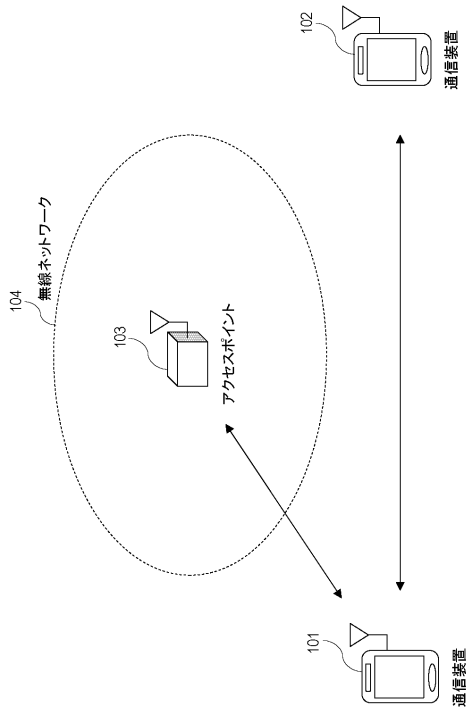
【符号の説明】

【０１１７】

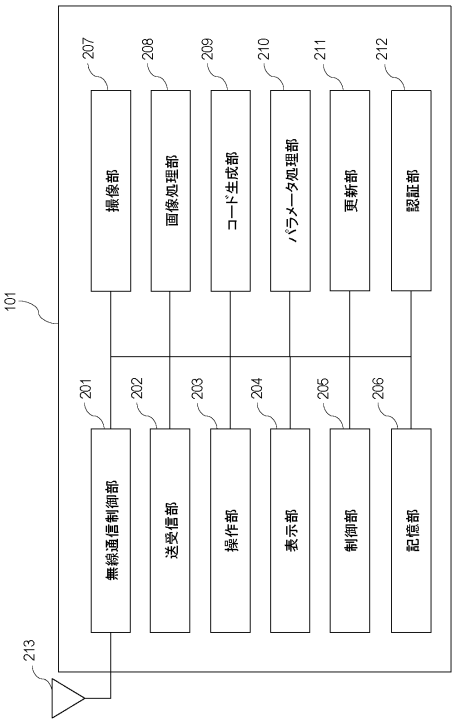
１０１、１０２　通信装置
１０３　アクセスポイント
１０４　無線ネットワーク

【図面】

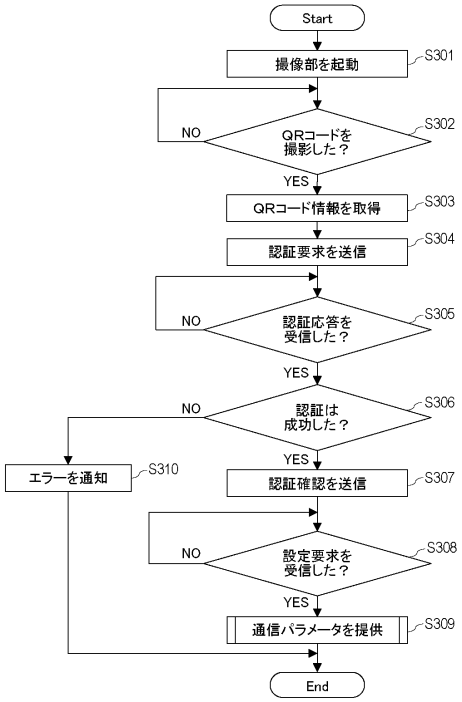
【図１】


102
通信装置
104
無線ネットワーク
103
アクセスポイント
101
通信装置

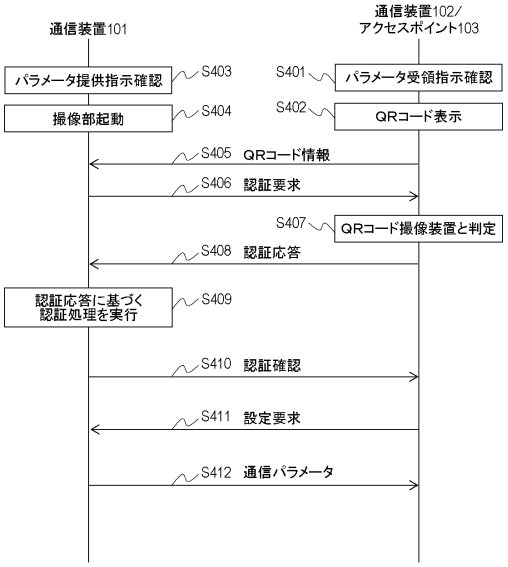
【図２】


207
208
209
210
211
212
撮像部
画像処理部
コード生成部
パラメータ処理部
更新部
認証部
101
201
202
203
204
205
206
無線通信制御部
送受信部
操作部
表示部
制御部
記憶部
213

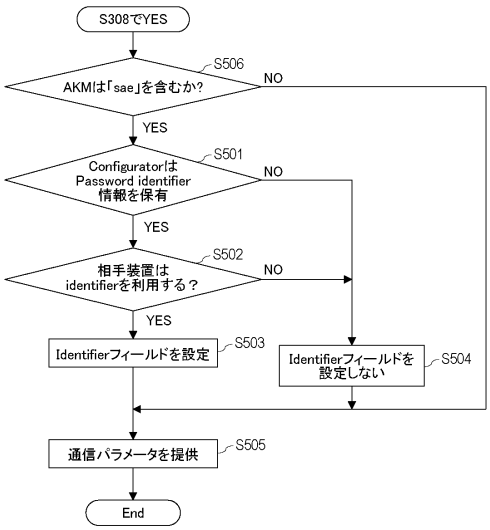
【図３】


Start
撮像部を起動
S301
NO
QRコードを撮影した？
S302
YES
QRコード情報を取得
S303
認証要求を送信
S304
NO
認証応答を受信した？
S305
YES
NO
認証は成功した？
S306
YES
エラーを通知
S310
認証確認を送信
S307
NO
設定要求を受信した？
S308
YES
通信パラメータを提供
S309
End

【図４】


通信装置101
通信装置102／
アクセスポイント103
パラメータ提供指示確認
S403
S401
パラメータ受領指示確認
撮像部起動
S404
S402
QRコード表示
S405
QRコード情報
S406
認証要求
S407
QRコード撮像装置と判定
S408
認証応答
認証応答に基づく認証処理を実行
S409
S410
認証確認
S411
設定要求
S412
通信パラメータ

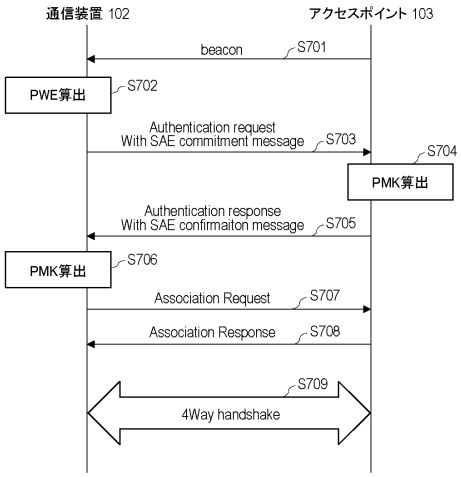
【図５】



【図６】

602 Parameter	603 Name	604 Type	605 Value
DPP Configuration object	configurationObject	OBJECT	
Wi-Fi Technology object:	wi-fi_tech	STRING	infra
Service	svc	STRING	
Discovery object:	discovery	OBJECT	
SSID	ssid	STRING	alpha numeric
Credential object	cred	OBJECT	
Authentication and key management type	akm	STRING	psk, dpp, sae, psk+sae, dpp+sae, dpp+psk+sae
Pre-shared key	psk_hex	STRING	
WPA2 Passphrase and/or SAE password	pass	STRING	
SAE Identifier 601	identifier	STRING	
DPP Connector	signedConnector	STRING	
C-sign-key	csign	JWK	

【図７】



フロントページの続き

ヤノン株式会社内

審査官　齋藤 浩兵

(56)参考文献　特表２０１６－５３８７７０（ＪＰ，Ａ）
特開２０１９－０２９９８９（ＪＰ，Ａ）
特開２０１８－０４２０５８（ＪＰ，Ａ）
特開２０１８－０４２０５７（ＪＰ，Ａ）
特表２０１８－５３８７５８（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　４／００－９９／００