(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2019-180040
(P2019-180040A)
(43)公開日　令和1年10月17日(2019.10.17)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 76/10	(2018.01)	H04W	76/10		5K067
H04W 4/00	(2018.01)	H04W	4/00	111	
H04W 12/06	(2009.01)	H04W	12/06		
H04W 12/04	(2009.01)	H04W	12/04		
H04W 88/06	(2009.01)	H04W	88/06		

審査請求 未請求　請求項の数 18　ＯＬ　（全 30 頁）

(21)出願番号　特願2018-68821 (P2018-68821)
(22)出願日　平成30年3月30日 (2018.3.30)

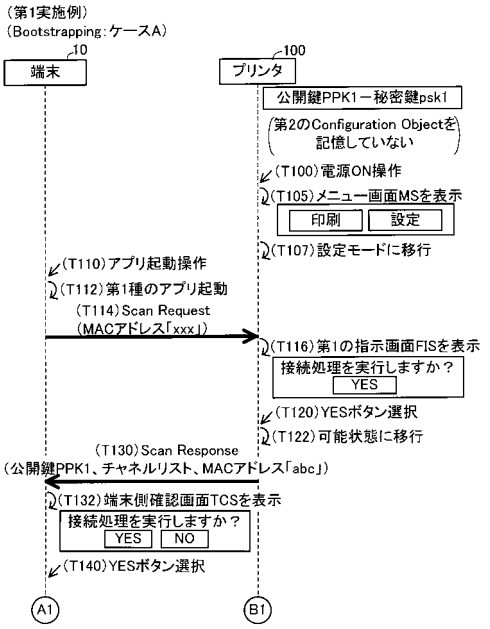
（特許庁注：以下のものは登録商標）
１．ＺＩＧＢＥＥ

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　鈴木　智詞
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内
(72)発明者　柴田　寛
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

Ｆターム(参考)　5K067 AA26 DD11 DD17 DD24 EE04 EE10

(54)【発明の名称】通信装置と通信装置のためのコンピュータプログラム

(57)【要約】　（修正有）
【課題】ユーザによって意図されていない一対の装置の間に無線接続が確立されるのを抑制する技術を提供する。
【解決手段】通信装置は、第１の外部装置から第１の無線インターフェースを介して特定信号が受信される場合に、公開鍵の送信を含む対象処理を実行すべきことを指示するための第１の指示画面を表示する。対象処理を実行すべきことが指示される場合に、通信装置は、第１の無線インターフェースを介して公開鍵を第１の外部装置に送信し、第１の外部装置から第２の無線インターフェースを介して、公開鍵が利用された認証要求が受信される場合に、第２の無線インターフェースを介して認証応答を第１の外部装置に送信する。通信装置は、認証応答送信後に第１の外部装置から第２の無線インターフェースを介して接続情報が受信される場合に、接続情報を利用して第２の外部装置との間に第２の無線インターフェースを介した無線接続を確立する。
【選択図】図３



【特許請求の範囲】
【請求項１】
通信装置であって、
表示部と、
第１の無線インターフェースと、
前記第１の無線インターフェースとは異なる第２の無線インターフェースと、
第１の外部装置から、前記第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、
前記第１の外部装置から前記特定信号が受信される場合に、公開鍵の送信を含む対象処理を実行すべきことを指示するための第１の指示画面を前記表示部に表示させる第１の表示制御部と、
前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示される場合に、前記第１の無線インターフェースを介して、前記公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示されない場合に、前記公開鍵は送信されない、前記公開鍵送信部と、
前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する認証要求受信部と、
前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、
前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、
前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、
を備える、通信装置。
【請求項２】
前記通信装置は、さらに、
前記第１の外部装置から前記特定信号が受信される場合に、前記特定信号の受信電波強度が閾値以上であるのか否かを判断する判断部を備え、
前記第１の表示制御部は、前記第１の外部装置から前記特定信号が受信され、かつ、前記受信電波強度が閾値以上でないと判断される場合に、前記第１の指示画面を前記表示部に表示させ、
前記第１の外部装置から前記特定信号が受信され、かつ、前記受信電波強度が閾値以上であると判断される場合に、前記第１の指示画面は前記表示部に表示されず、
前記公開鍵送信部は、前記第１の外部装置から前記特定信号が受信され、かつ、前記受信電波強度が閾値以上であると判断される場合に、前記対象処理を実行すべきことが指示されなくても、前記第１の無線インターフェースを介して、前記公開鍵を前記第１の外部装置に送信する、請求項１に記載の通信装置。
【請求項３】
通信装置であって、
第１の無線インターフェースと、
前記第１の無線インターフェースとは異なる第２の無線インターフェースと、
第１の外部装置から、前記第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、
前記第１の外部装置から前記特定信号が受信される場合に、前記特定信号の受信電波強

度が閾値以上であるのか否かを判断する判断部と、
前記受信電波強度が前記閾値以上であると判断される場合に、前記第１の無線インターフェースを介して、公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記受信電波強度が前記閾値以上でないと判断される場合に、前記第１の外部装置への前記公開鍵の送信は制限される、前記公開鍵送信部と、
前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する認証要求受信部と、
前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、
前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、
前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、
を備える、通信装置。
【請求項４】
前記通信装置は、さらに、
前記第１の外部装置から、前記第１の無線インターフェースを介して、前記第１の外部装置を識別する識別情報を受信する識別情報受信部を備え、
前記認証応答送信部は、前記第１の外部装置から前記識別情報が受信され、かつ、前記識別情報によって識別される前記第１の外部装置から前記識別情報を含む前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証応答を前記第１の外部装置に送信し、
前記第１の外部装置から前記識別情報が受信され、かつ、前記第１の外部装置とは異なる外部装置から、前記第２の無線インターフェースを介して、前記識別情報を含まない前記認証要求が受信される場合に、前記異なる外部装置への前記認証応答の送信は制限される、請求項１から３のいずれか一項に記載の通信装置。
【請求項５】
前記通信装置は、さらに、
表示部と、
前記第１の外部装置から前記識別情報が受信され、かつ、前記異なる外部装置から前記識別情報を含まない前記認証要求が受信される場合に、前記異なる外部装置への前記認証応答の送信を実行すべきことを指示するための第２の指示画面を前記表示部に表示させることによって、前記異なる外部装置への前記認証応答の送信を制限する第２の表示制御部を備え、
前記認証応答送信部は、前記第２の指示画面が表示されている状況において、前記認証応答の送信を実行すべきことが指示される場合に、前記第２の無線インターフェースを介して、前記認証応答を前記第１の外部装置に送信する、請求項４に記載の通信装置。
【請求項６】
前記識別情報は、前記特定信号に含まれる、請求項４又は５に記載の通信装置。
【請求項７】
前記通信装置は、さらに、
前記第１の外部装置から前記特定信号が受信された後に、前記通信装置の動作状態を不可能状態から可能状態に移行させる状態移行部であって、前記不可能状態は、前記認証要求を受信しても、前記認証応答を送信しない状態であり、前記可能状態は、前記認証要求を受信することに応じて、前記認証応答を送信する状態である、前記状態移行部を備え、

前記認証応答送信部は、前記通信装置の動作状態が前記可能状態に移行された後に、前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証応答を前記第１の外部装置に送信する、請求項１から６のいずれか一項に記載の通信装置。

【請求項８】

前記通信装置は、さらに、

前記第１の無線インターフェースを介して、前記通信装置において予め決められている第１の通信チャネルを示す通信チャネル情報を外部に送信するチャネル情報送信部を備え、

前記可能状態は、前記第１の通信チャネルが利用された前記認証要求を受信することを監視し、前記認証要求を受信することに応じて、前記認証応答を送信する状態であり、

前記認証応答送信部は、前記通信装置の動作状態が前記可能状態に移行された後に、前記第１の外部装置から前記第１の通信チャネルが利用された前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証応答を前記第１の外部装置に送信する、請求項７に記載の通信装置。

【請求項９】

前記確立部は、前記第１の通信チャネルとは異なる第２の通信チャネルを利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する、請求項８に記載の通信装置。

【請求項１０】

前記第１の無線インターフェースは、Ｂｌｕｅｔｏｏｔｈ（登録商標）方式のバージョン４．０以上に従った無線通信を実行するための無線インターフェースであり、

前記特定信号は、前記Ｂｌｕｅｔｏｏｔｈ方式のバージョン４．０以上に従ったＳｃａｎ　Ｒｅｑｕｅｓｔであり、

前記公開鍵送信部は、前記Ｂｌｕｅｔｏｏｔｈ方式のバージョン４．０以上に従ったＳｃａｎ　Ｒｅｓｐｏｎｓｅであって、前記公開鍵を含む前記Ｓｃａｎ　Ｒｅｓｐｏｎｓｅを前記第１の外部装置に送信する、請求項１から９のいずれか一項に記載の通信装置。

【請求項１１】

前記通信装置は、さらに、

所定条件が満たされる場合に、前記第１の無線インターフェースの動作モードを第１のモードから第２のモードに移行させるモード移行部であって、前記第１のモードは、前記第１の無線インターフェースが前記特定信号を解釈不可能なモードであり、前記第２のモードは、前記第１の無線インターフェースが前記特定信号を解釈可能なモードである、前記モード移行部を備え、

前記特定信号受信部は、前記第１の無線インターフェースの動作モードが前記第２のモードに移行された後に、前記第１の外部装置から、前記第１の無線インターフェースを介して、前記特定信号を受信する、請求項１から１０のいずれか一項に記載の通信装置。

【請求項１２】

前記通信装置は、さらに、

メモリと、

前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を前記メモリに記憶する記憶制御部と、を備え、

前記メモリ内に前記接続情報が記憶されていない状況において、前記通信装置の電源がＯＮされる場合に、前記所定条件が満たされ、

前記メモリ内に前記接続情報が記憶されている状況において、前記通信装置の電源がＯＮされる場合に、前記所定条件が満たされない、請求項１１に記載の通信装置。

【請求項１３】

前記通信装置は、さらに、

操作部を備え、

前記メモリ内に前記接続情報が記憶されている状況において、ユーザから前記操作部を

介した特定操作が受け付けられる場合に、前記所定条件が満たされる、請求項１２に記載の通信装置。
【請求項１４】
前記第２の外部装置は、前記第１の外部装置とは異なる装置であって、無線ネットワークの親局として動作すべき親局装置であり、
前記確立部は、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立して、前記通信装置を前記無線ネットワークに子局として参加させる、請求項１から１３のいずれか一項に記載の通信装置。
【請求項１５】
前記接続情報は、前記第２の外部装置から受信される受信情報を認証するための認証情報を含む、請求項１から１４のいずれか一項に記載の通信装置。
【請求項１６】
前記通信装置は、さらに、
前記認証応答が前記第１の外部装置に送信された後に、前記通信装置をＷｉ－Ｆｉ規格に従ったＥｎｒｏｌｌｅｅとして動作させる動作制御部であって、前記第１の外部装置は、前記Ｗｉ－Ｆｉ規格に従ったＣｏｎｆｉｇｕｒａｔｏｒとして動作する、前記動作制御部を備える、請求項１から１５のいずれか一項に記載の通信装置。
【請求項１７】
通信装置のためのコンピュータプログラムであって、
前記通信装置のコンピュータを以下の各部、即ち、
第１の外部装置から、前記通信装置の第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、
前記第１の外部装置から前記特定信号が受信される場合に、公開鍵の送信を含む対象処理を実行すべきことを指示するための第１の指示画面を前記通信装置の表示部に表示させる第１の表示制御部と、
前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示される場合に、前記第１の無線インターフェースを介して、前記公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示されない場合に、前記公開鍵は送信されない、前記公開鍵送信部と、
前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記通信装置の第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する認証要求受信部であって、前記第２の無線インターフェースは、前記第１の無線インターフェースとは異なる、前記認証要求受信部と、
前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、
前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、
前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、
として機能させる、コンピュータプログラム。
【請求項１８】
通信装置のためのコンピュータプログラムであって、
前記通信装置のコンピュータを、以下の各部、即ち、
第１の外部装置から、前記通信装置の第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、

前記第１の外部装置から前記特定信号が受信される場合に、前記特定信号の受信電波強度が閾値以上であるのか否かを判断する判断部と、
前記受信電波強度が前記閾値以上であると判断される場合に、前記第１の無線インターフェースを介して、公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記受信電波強度が前記閾値以上でないと判断される場合に、前記第１の外部装置への前記公開鍵の送信は制限される、前記公開鍵送信部と、
前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記通信装置の第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する認証要求受信部であって、前記第２の無線インターフェースは、前記第１の無線インターフェースとは異なる、前記認証要求受信部と、
前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、
前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、
前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、
として機能させる、コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本明細書では、外部装置との無線接続を確立可能な通信装置に関する技術を開示する。
【背景技術】
【０００２】
非特許文献１には、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅによって策定された無線通信方式であるＤＰＰ（Device Provisioning Protocolの略）方式が記述されている。ＤＰＰ方式は、一対の装置の間に容易にＷｉ－Ｆｉ接続を確立させるための無線通信方式である。非特許文献１には、公開鍵の共有化のための例として、Ｒｅｓｐｏｎｄｅｒが、Ｂｌｕｅｔｏｏｔｈ（登録商標）通信を利用して、公開鍵をＩｎｉｔｉａｔｏｒに送信することが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１８－３７９７８号公報
【非特許文献】
【０００４】
【非特許文献１】「DRAFT Device Provisioning Protocol Technical Specification Version 0.2.11」 Wi-Fi Alliance, ２０１７年
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上記の非特許文献１には、公開鍵の送信を制限することについて何ら開示されていない。このために、ＲｅｓｐｏｎｄｅｒがＢｌｕｅｔｏｏｔｈ通信を利用して公開鍵を送信すると、ユーザが意図しているＩｎｉｔｉａｔｏｒとは異なる装置が公開鍵を受信し得る。この結果、ユーザが意図していない一対の装置の間にＷｉ－Ｆｉ接続が確立され得る。
【０００６】

本明細書では、ユーザによって意図されていない一対の装置の間に無線接続が確立されるのを抑制し得る技術を開示する。

【課題を解決するための手段】

【０００７】

本明細書によって開示される通信装置は、表示部と、第１の無線インターフェースと、前記第１の無線インターフェースとは異なる第２の無線インターフェースと、第１の外部装置から、前記第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、前記第１の外部装置から前記特定信号が受信される場合に、公開鍵の送信を含む対象処理を実行すべきことを指示するための第１の指示画面を前記表示部に表示させる第１の表示制御部と、前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示される場合に、前記第１の無線インターフェースを介して、前記公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記第１の指示画面が表示されている状況において、前記対象処理を実行すべきことが指示されない場合に、前記公開鍵は送信されない、前記公開鍵送信部と、前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する認証要求受信部と、前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、を備えてもよい。

【０００８】

上記の構成によると、通信装置は、第１の外部装置から特定信号を受信する場合に、第１の指示画面を表示する。通信装置は、第１の指示画面が表示されている状況において、対象処理を実行すべきことが指示される場合、即ち、通信装置と第１の外部装置との間で公開鍵が利用された通信が実行されることをユーザが望む場合に、公開鍵を第１の外部装置に送信する。これにより、通信装置は、第１の外部装置から公開鍵が利用された認証要求を受信し、認証応答を第１の外部装置に送信し、第１の外部装置から接続情報を受信し、接続情報を利用して第２の外部装置との無線接続を確立する。一方、第１の指示画面が表示されている状況において、対象処理を実行すべきことが指示されない場合、即ち、通信装置と第１の外部装置との間で公開鍵が利用された通信が実行されることをユーザが望まない場合に、公開鍵は送信されない。従って、通信装置では、第１の外部装置から公開鍵が利用された認証要求が受信されず、この結果、第２の外部装置との無線接続が確立されない。このために、ユーザによって意図されていない一対の装置の間に無線接続が確立されるのを抑制し得る。

【０００９】

また、本明細書によって開示される通信装置は、第１の無線インターフェースと、前記第１の無線インターフェースとは異なる第２の無線インターフェースと、第１の外部装置から、前記第１の無線インターフェースを介して、特定信号を受信する特定信号受信部と、前記第１の外部装置から前記特定信号が受信される場合に、前記特定信号の受信電波強度が閾値以上であるのか否かを判断する判断部と、前記受信電波強度が前記閾値以上であると判断される場合に、前記第１の無線インターフェースを介して、公開鍵を前記第１の外部装置に送信する公開鍵送信部であって、前記受信電波強度が前記閾値以上でないと判断される場合に、前記第１の外部装置への前記公開鍵の送信は制限される、前記公開鍵送信部と、前記公開鍵が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、前記公開鍵が利用された認証要求を受信する

認証要求受信部と、前記第１の外部装置から前記認証要求が受信される場合に、前記第２の無線インターフェースを介して、前記認証要求に対する応答である認証応答を前記第１の外部装置に送信する認証応答送信部と、前記認証応答が前記第１の外部装置に送信された後に、前記第１の外部装置から、前記第２の無線インターフェースを介して、接続情報を受信する接続情報受信部であって、前記接続情報は、前記通信装置と第２の外部装置との間に前記第２の無線インターフェースを介した無線接続を確立するための情報である、前記接続情報受信部と、前記第１の外部装置から前記接続情報が受信される場合に、前記接続情報を利用して、前記通信装置と前記第２の外部装置との間に前記第２の無線インターフェースを介した前記無線接続を確立する確立部と、を備えてもよい。

【００１０】

上記の構成によると、通信装置は、第１の外部装置から特定信号を受信する場合に、特定信号の受信電波強度が閾値以上であるのか否かを判断する。ここで、受信電波強度が閾値以上である状況は、通信装置と第１の外部装置との間の距離が比較的に小さいこと、即ち、通信装置と第１の外部装置との間で公開鍵が利用された通信が実行されることをユーザが望んでいる可能性が高いこと、を意味する。このような状況では、通信装置は、公開鍵を第１の外部装置に送信する。これにより、通信装置は、第１の外部装置から公開鍵が利用された認証要求を受信し、認証応答を第１の外部装置に送信し、第１の外部装置から接続情報を受信し、接続情報を利用して第２の外部装置との無線接続を確立する。一方、受信電波強度が閾値以上でない状況は、通信装置と第１の外部装置との間の距離が比較的に大きいこと、即ち、通信装置と第１の外部装置との間で公開鍵が利用された通信が実行されることをユーザが望んでいない可能性が高いこと、を意味する。この場合、通信装置では、公開鍵の送信が制限される。従って、通信装置では、第１の外部装置から公開鍵が利用された認証要求が受信されることが制限され、この結果、第２の外部装置との無線接続が確立されることが制限される。このために、ユーザによって意図されていない一対の装置の間に無線接続が確立されるのを抑制し得る。

【００１１】

上記の通信装置を実現するためのコンピュータプログラム、及び、当該コンピュータプログラムを記憶するコンピュータ可読記録媒体も新規で有用である。また、上記の通信装置によって実行される方法も新規で有用である。また、上記の通信装置と他の装置（例えば第１の外部装置、第２の外部装置）とを備える通信システムも、新規で有用である。

【図面の簡単な説明】

【００１２】

【図１】通信システムの構成を示す。

【図２】実施例の概略を説明するための説明図を示す。

【図３】ケースＡのＢｏｏｔｓｔｒａｐｐｉｎｇの処理のシーケンス図を示す。

【図４】Ａｕｔｈｅｎｔｉｃａｔｉｏｎの処理のシーケンス図を示す。

【図５】Ｃｏｎｆｉｇｕｒａｔｉｏｎの処理のシーケンス図を示す。

【図６】Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓの処理のシーケンス図を示す。

【図７】ケースＢのＢｏｏｔｓｔｒａｐｐｉｎｇの処理のシーケンス図を示す。

【図８】第２実施例のＢｏｏｔｓｔｒａｐｐｉｎｇの処理のフローチャート図を示す。

【図９】第２実施例のＡｕｔｈｅｎｔｉｃａｔｉｏｎの処理のフローチャート図を示す。

【図１０】ケースＣのＢｏｏｔｓｔｒａｐｐｉｎｇ及びＡｕｔｈｅｎｔｉｃａｔｉｏｎの処理のシーケンス図を示す。

【図１１】ケースＤのＢｏｏｔｓｔｒａｐｐｉｎｇ及びＡｕｔｈｅｎｔｉｃａｔｉｏｎの処理のシーケンス図を示す。

【図１２】ケースＥのＢｏｏｔｓｔｒａｐｐｉｎｇ及びＡｕｔｈｅｎｔｉｃａｔｉｏｎの処理のシーケンス図を示す。

【発明を実施するための形態】

【００１３】

（第１実施例）

（通信システム２の構成；図１）
図１に示されるように、通信システム２は、ＡＰ（Access Pointの略）６と、複数個の端末１０，５０と、プリンタ１００と、を備える。本実施例では、ユーザが各端末１０，５０を利用して、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ方式に従った無線接続（以下では「Ｗｉ－Ｆｉ接続」と記載する）を確立させる状況を想定している。
【００１４】
（各端末１０，５０の構成）
各端末１０，５０は、携帯電話（例えばスマートフォン）、ＰＤＡ、タブレットＰＣ等の可搬型の端末装置である。なお、変形例では、各端末１０，５０は、据置型のＰＣ、ノートＰＣ等であってもよい。端末１０は、ＭＡＣアドレス「ｘｘｘ」を有する。端末５０は、ＭＡＣアドレス「ｙｙｙ」を有する。ここで、各端末１０，５０は、同様の構成を有する。従って、以下では、端末１０の構成を主に説明する。
【００１５】
端末１０は、Ｗｉ－Ｆｉインターフェース１６と、ＢＴ（Ｂｌｕｅｔｏｏｔｈの略）インターフェース１８と、を備える。以下では、インターフェースを単に「Ｉ／Ｆ」と記載する。
【００１６】
Ｗｉ－ＦｉＩ／Ｆ１６は、Ｗｉ－Ｆｉ方式に従ったＷｉ－Ｆｉ通信を実行するための無線インターフェースである。Ｗｉ－Ｆｉ方式は、例えば、ＩＥＥＥ（The Institute of Electrical and Electronics Engineers, Inc.の略）の８０２．１１の規格、及び、それに準ずる規格（例えば８０２．１１ａ，１１ｂ，１１ｇ，１１ｎ，１１ａｃ等）に従って、無線通信を実行するための無線通信方式である。特に、Ｗｉ－ＦｉＩ／Ｆ１６は、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅによって策定される予定であるＤＰＰ（Device Provisioning Protocolの略）方式をサポートしている。ＤＰＰ方式は、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅによって作成された規格書のドラフトである「DRAFT Device Provisioning Protocol Technical Specification Version 0.2.11」に記述されており、端末１０を利用して一対のデバイス（例えばプリンタ１００とＡＰ６）の間に容易にＷｉ－Ｆｉ接続を確立させるための無線通信方式である。
【００１７】
ＢＴＩ／Ｆ１８は、ＢＴ方式のバージョン４．０以上に従った通信（いわゆるBlue Tooth Low Energyに従った通信）を実行するためのＩ／Ｆである。ＢＴ方式は、例えば、ＩＥＥＥ８０２．１５．１の規格、及び、それに準ずる規格に基づく無線通信方式である。
【００１８】
端末１０は、第１種のアプリケーション（以下では単に「第１種のアプリ」と記載する）４０を記憶している。第１種のアプリ４０は、プリンタ１００のベンダによって提供されるプログラムであり、例えば、プリンタ１００のベンダによって提供されるインターネット上のサーバから端末１０にインストールされる。また、端末５０は、第２種のアプリケーション（以下では単に「第２種のアプリ」と記載する）５２を記憶している。第２種のアプリ５２は、プリンタ１００のベンダとは異なる事業者によって提供されるプログラムである。第１種のアプリ４０及び第２種のアプリ５２は、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続を確立させるためのプログラムである。また、別の変形例では、第２種のアプリ５２は、端末５０の基本的な動作を実現するためのＯＳプログラムであってもよい。
【００１９】
（プリンタ１００の構成）
プリンタ１００は、印刷機能を実行可能な周辺装置（例えば、端末１０の周辺装置）である。プリンタ１００は、操作部１１２と、表示部１１４と、Ｗｉ－ＦｉＩ／Ｆ１１６と、ＢＴＩ／Ｆ１１８と、印刷実行部１２０と、制御部１３０と、を備える。各部１１２～１３０は、バス線（符号省略）に接続されている。
【００２０】

操作部１１２は、複数のキーを備える。ユーザは、操作部１１２を操作することによって、様々な指示をプリンタ１００に入力することができる。表示部１１４は、様々な情報を表示するためのディスプレイである。Ｗｉ－ＦｉＩ／Ｆ１１６は、端末１０のＷｉ－ＦｉＩ／Ｆ１６と同様である。即ち、Ｗｉ－ＦｉＩ／Ｆ１１６は、ＤＰＰ方式をサポートしている。また、Ｗｉ－ＦｉＩ／Ｆ１１６は、ＭＡＣアドレス「ａｂｃ」を有する。ＢＴＩ／Ｆ１１８は、端末１０のＢＴＩ／Ｆ１８と同様である。印刷実行部１２０は、インクジェット方式、レーザ方式等の印刷機構を備える。

【００２１】

ここで、Ｗｉ－Ｆｉ方式とＢＴ方式との相違点を記述しておく。Ｗｉ－Ｆｉ通信の通信速度（例えば最大の通信速度が６００［Ｍｂｐｓ］）は、ＢＴ通信の通信速度（例えば最大の通信速度が２４［Ｍｂｐｓ］）よりも速い。Ｗｉ－Ｆｉ通信における搬送波の周波数は、２．４［ＧＨｚ］帯又は５．０［ＧＨｚ］帯である。ＢＴ通信における搬送波の周波数は、２．４［ＧＨｚ］帯である。即ち、Ｗｉ－Ｆｉ通信における搬送波の周波数として５．０［ＧＨｚ］帯が採用される場合には、Ｗｉ－Ｆｉ通信における搬送波の周波数とＢＴ通信における搬送波の周波数とは異なる。また、Ｗｉ－Ｆｉ通信を実行可能な最大の距離（例えば約１００［ｍ］）は、ＢＴ通信を実行可能な最大の距離（例えば約数十［ｍ］）よりも大きい。

【００２２】

制御部１３０は、ＣＰＵ１３２とメモリ１３４とを備える。ＣＰＵ１３２は、メモリ１３４に格納されているプログラム１３６に従って、様々な処理を実行する。メモリ１３４は、揮発性メモリ、不揮発性メモリ等によって構成される。

【００２３】

（本実施例の概要；図２）

続いて、図２を参照して、本実施例の概要を説明する。各端末１０，５０及びプリンタ１００がＤＰＰ方式をサポートしていることを上述したが、ＡＰ６もＤＰＰ方式をサポートしている。そして、本実施例では、各デバイス６，１０（又は５０），１００がＤＰＰ方式に従った通信を実行することによって、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続を確立することを実現する。なお、端末１０によって実行される処理と端末５０によって実行される処理は、一部の処理（例えば、後述の図１１のＴ７１４、図１２のＴ８１４）を除いて同様である。従って、図２では、端末５０に関する説明を省略する。また、以下では、理解の容易化のために、各デバイスのＣＰＵ（例えばＣＰＵ１３２等）が実行する動作を、ＣＰＵを主体として記載せずに、各デバイス（例えばプリンタ１００）を主体として記載する。

【００２４】

Ｔ５では、端末１０は、ＤＰＰ方式のＢｏｏｔｓｔｒａｐｐｉｎｇ（以下では、単に「ＢＳ」と記載する）をＡＰ６と実行する。当該ＢＳは、ＡＰ６に貼り付けられているＱＲコード（登録商標）が端末１０によって撮影されることに応じて、後述のＴ１０のＡｕｔｈｅｎｔｉｃａｔｉｏｎ（以下では、単に「Ａｕｔｈ」と記載する）で利用される情報をＡＰ６から端末１０に提供する処理である。

【００２５】

Ｔ１０では、端末１０は、Ｔ５のＢＳで取得済みの情報を利用して、ＤＰＰ方式のＡｕｔｈをＡＰ６と実行する。当該Ａｕｔｈは、端末１０及びＡＰ６のそれぞれが通信相手を認証するための処理である。

【００２６】

Ｔ１５では、端末１０は、ＤＰＰ方式のＣｏｎｆｉｇｕｒａｔｉｏｎ（以下では、単に「Ｃｏｎｆｉｇ」と記載する）をＡＰ６と実行する。当該Ｃｏｎｆｉｇは、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続を確立するための情報をＡＰ６に送信する処理である。具体的には、端末１０は、当該Ｃｏｎｆｉｇにおいて、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続を確立させるための第１のＣｏｎｆｉｇｕｒａｔｉｏｎ　Ｏｂｊｅｃｔ（以下では、Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｏｂｊｅｃｔのことを単に「ＣＯ」と記載す

る）を生成して、第１のＣＯをＡＰ６に送信する。この結果、ＡＰ６では、第１のＣＯが記憶される。

【００２７】

次いで、端末１０は、Ｔ２０において、ＤＰＰ方式のＢＳをプリンタ１００と実行する。当該ＢＳは、プリンタ１００が、ＢＴＩ／Ｆ１１８を介して、後述のＴ２５のＡｕｔｈで利用される情報を端末１０に提供する処理である。

【００２８】

Ｔ２５では、端末１０は、Ｔ２０のＢＳで取得済みの情報を利用して、ＤＰＰ方式のＡｕｔｈをプリンタ１００と実行する。当該Ａｕｔｈは、端末１０及びプリンタ１００のそれぞれが通信相手を認証するための処理である。

【００２９】

Ｔ３０では、端末１０は、ＤＰＰ方式のＣｏｎｆｉｇをプリンタ１００と実行する。当該Ｃｏｎｆｉｇは、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続を確立するための情報をプリンタ１００に送信する処理である。端末１０は、当該Ｃｏｎｆｉｇにおいて、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続を確立させるための第２のＣＯを生成して、第２のＣＯをプリンタ１００に送信する。この結果、プリンタ１００では、第２のＣＯが記憶される。

【００３０】

Ｔ３５では、プリンタ１００及びＡＰ６は、記憶済みの第１及び第２のＣＯを利用して、ＤＰＰ方式のＮｅｔｗｏｒｋ　Ａｃｃｅｓｓ（以下では、単に「ＮＡ」と記載する）を実行する。ＮＡは、Ｗｉ－Ｆｉ接続を確立するための接続キーをプリンタ１００及びＡＰ６の間で共有するための処理である。

【００３１】

Ｔ４０では、プリンタ１００及びＡＰ６は、４ｗａｙ－ｈａｎｄｓｈａｋｅの通信を実行する。４ｗａｙ－ｈａｎｄｓｈａｋｅの通信の少なくとも一部の過程において、プリンタ１００及びＡＰ６は、Ｔ３５のＮＡで共有済みの接続キーによって暗号化された暗号情報を通信する。そして、暗号情報の復号が成功する場合に、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立される。これにより、プリンタ１００は、ＡＰ６によって形成される無線ネットワークに子局として参加することができ、この結果、ＡＰ６を介して、当該無線ネットワークに参加している他のデバイスとの通信を実行することができる。なお、変形例では、プリンタ１００及びＡＰ６は、４ｗａｙ－ｈａｎｄｓｈａｋｅの通信に代えて、ＳＡＥ（Simultaneous Authentication of Equalsの略、通称「Dragonfly」）の通信を実行してもよい。

【００３２】

Ｔ４５では、プリンタ１００は、Ｗｉ－Ｆｉ接続がＡＰ６と確立されたことを示す完了画面を表示部１１４に表示させる。Ｔ４５の処理が終了すると、図２の処理が終了する。

【００３３】

ＤＰＰ方式では、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続を確立させるために、ユーザは、ＡＰ６が親局として動作する無線ネットワークの情報（例えばＳＳＩＤ（Service Set Identifierの略）、パスワード等）をプリンタ１００に入力する必要がない。従って、ユーザは、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続を容易に確立させることができる。

【００３４】

（各処理の説明；図３～図７）

続いて、図３～図７を参照して、図２のＴ２０～Ｔ３５において実行される各処理の詳細を説明する。なお、Ｔ５～Ｔ１５の処理は、プリンタ１００に代えてＡＰ６が利用される点を除いて、Ｔ２０～Ｔ３０の処理と同様であるので、その詳細な説明を省略する。また、図３及び図７は、端末１０とプリンタ１００との間で実行されるＢＳの各ケースを示す。これらのケースは、一つの実施例において実行される処理である。

【００３５】

（ケースＡのＢｏｏｔｓｔｒａｐｐｉｎｇ（ＢＳ）；図３）
まず、図３を参照して、図２のＴ２０のＢＳのケースＡの処理を説明する。図３の初期状態では、プリンタ１００のメモリ１３４は、プリンタ１００の公開鍵ＰＰＫ１及び秘密鍵ｐｓｋ１を予め記憶している。
【００３６】
プリンタ１００は、Ｔ１００において、ユーザから電源ＯＮ操作を受け付けることに応じて、Ｔ１０５において、メニュー画面ＭＳを表示部１１４に表示させる。画面ＭＳは、換言すればプリンタ１００のデフォルト画面であり、プリンタ１００に印刷を実行させる印刷ボタンと、プリンタ１００の各種設定（例えば印刷設定等）を指定するための設定ボタンと、を含む。
【００３７】
次いで、プリンタ１００は、メモリ１３４が第２のＣＯ（図２のＴ３０参照）をまだ記憶していないので、Ｔ１０７において、ＢＴＩ／Ｆ１１８の動作モードを移行させるための移行指示をＢＴＩ／Ｆ１１８に供給して、ＢＴＩ／Ｆ１１８の動作モードを通常モードから設定モードに移行させる。従って、メモリ１３４が第２のＣＯを記憶していない状態では、ユーザがプリンタ１００の電源をＯＮするだけで、ＢＴＩ／Ｆ１１８の動作モードが通常モードから設定モードに移行される。通常モードは、ＢＴ方式に従ったＳｃａｎ Ｒｅｑｕｅｓｔ（以下では、単に「ＳＲｅｑ」と記載する）（後述のＴ１１４）を解釈不可能なモード（即ちＳＲｅｑを受信しても無視するモード）である。設定モードは、ＳＲｅｑを解釈可能なモード（即ちＳＲｅｑを受信するとＳＲｅｑ内の情報をＣＰＵ１３２に供給するモード）である。
【００３８】
端末１０は、Ｔ１１０において、ユーザからアプリの起動操作を受け付けることに応じて、Ｔ１１２において、第１種のアプリ４０を起動する。端末１０によって実行される以降の各処理は、第１種のアプリ４０によって実現される。次いで、端末１０は、Ｔ１１４において、ＢＴＩ／Ｆ１８を介して、Ｗｉ－ＦｉＩ／Ｆ１６のＭＡＣアドレス「ｘｘｘ」を含むＳＲｅｑをプリンタ１００に送信する。当該ＳＲｅｑは、通信対象の装置とのペアリングが完了しなくても、当該装置との通信を実行可能な信号である。
【００３９】
プリンタ１００は、Ｔ１１４において、端末１０から、ＢＴＩ／Ｆ１１８を介して、ＳＲｅｑを受信することに応じて、Ｔ１１６において、Ｗｉ－Ｆｉ接続を確立するための接続処理を実行すべきことを指示するための第１の指示画面ＦＩＳを表示部１１４に表示させる。画面ＦＩＳは、接続処理を実行することを示すＹＥＳボタンを含む。
【００４０】
プリンタ１００は、Ｔ１２０において、画面ＦＩＳ内のＹＥＳボタンがユーザによって選択されることに応じて、Ｔ１２２において、不可能状態から可能状態に移行する。不可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、端末１０からＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｑｕｅｓｔ（以下では、単に「ＡＲｅｑ」と記載する）（後述の図４のＴ２００参照）を受信しても、ＤＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｒｅｓｐｏｎｓｅ（以下では、単に「ＡＲｅｓ」と記載する）（後述のＴ２１０参照）を送信しない状態である。可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、端末１０からＡＲｅｑを受信することに応じて、ＡＲｅｓを端末１０に送信する状態である。即ち、プリンタ１００は、不可能状態から可能状態に移行することによって、Ａｕｔｈ（図２のＴ２５参照）を実行可能な状態になる。具体的には、本実施例では、不可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、外部から信号を受信しても、当該信号をＣＰＵ１３２に供給しない状態である。また、可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、外部から信号を受信することに応じて、当該信号をＣＰＵ１３２に供給し、当該信号に対する応答を送信する状態である。可能状態は、ＣＰＵ１３２が外部から受信した信号を処理する状態であるので、不可能状態と比較して処理負荷が高い。なお、変形例では、不可能状態がＷｉ－ＦｉＩ／Ｆ１１６に通電されていない状態であり、可能状態がＷｉ－ＦｉＩ／Ｆ１１６に通電されている状態であってもよい。また

、別の変形例では、不可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、外部からＡＲｅｑを受信しても、ＡＲｅｑが受信されたことを示す通知をＣＰＵ１３２に供給しない状態であり、可能状態は、Ｗｉ－ＦｉＩ／Ｆ１１６が、外部からＡＲｅｑを受信することに応じて、ＡＲｅｑが受信されたことを示す通知をＣＰＵ１３２に供給する状態であってもよい。

【００４１】

なお、プリンタ１００は、Ｔ１１６で第１の指示画面ＦＩＳが表示されてから所定時間が経過してもＹＥＳボタンが選択されない場合（即ちタイムアウトの場合）には、画面ＦＩＳの表示を終了してＴ１２０以降の処理を実行せず、メニュー画面ＭＳを表示する状態に戻る。なお、変形例では、画面ＦＩＳが接続処理を実行しないことを示すＮＯボタンを含み、プリンタ１００は、画面ＦＩＳ内のＮＯボタンがユーザによって選択される場合に、画面ＦＩＳの表示を終了してもよい。

【００４２】

次いで、プリンタ１００は、Ｔ１３０において、ＢＴＩ／Ｆ１１８を介して、ＢＴ方式に従ったＳｃａｎ　Ｒｅｓｐｏｎｓｅ（以下では、単に「ＳＲｅｓ」と記載する）を端末１０に送信する。当該ＳＲｅｓは、通信対象の装置とのペアリングが完了しなくても、当該装置との通信を実行可能な信号である。また、当該ＳＲｅｓは、メモリ１３４に予め記憶されている公開鍵ＰＰＫ１と、メモリ１３４に予め記憶されているチャネルリストと、Ｗｉ－ＦｉＩ／Ｆ１１６のＭＡＣアドレス「ａｂｃ」と、を含む。チャネルリストは、Ａｕｔｈ（図２のＴ２５参照）で利用されるべき複数個の通信チャネルの値のリストである。

【００４３】

端末１０は、Ｔ１３０において、ＢＴＩ／Ｆ１８を介して、プリンタ１００からＳＲｅｓを受信することに応じて、当該ＳＲｅｓ内の各情報（即ち、公開鍵ＰＰＫ１、チャネルリスト、及び、ＭＡＣアドレス「ａｂｃ」）を取得する。次いで、Ｔ１３２では、端末１０は、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続を確立するための接続処理を実行するのか否かをユーザに問い合せる端末側確認画面ＴＣＳを表示する。画面ＴＣＳは、接続処理を実行することを示すＹＥＳボタンと、接続処理を実行しないことを示すＮＯボタンと、を含む。Ｔ１４０では、端末１０は、ユーザから画面ＴＣＳ内のＹＥＳボタンの選択を受け付ける。Ｔ１４０の処理が終了すると、ケースＡのＢＳの処理が終了する。

【００４４】

（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ（Ａｕｔｈ）；図４）

続いて、図４を参照して、図２のＴ２５のＡｕｔｈの処理を説明する。端末１０は、図３のＴ１４０において、画面ＴＣＳ内のＹＥＳボタンがユーザによって選択されることに応じて、Ｔ１４１において、端末１０の公開鍵ＴＰＫ１及び秘密鍵ｔｓｋ１を生成する。次いで、端末１０は、Ｔ１４２において、ＥＣＤＨ（Elliptic curve Diffie-Hellman key exchangeの略）に従って、生成済みの秘密鍵ｔｓｋ１と、図３のＴ１３０で取得されたプリンタ１００の公開鍵ＰＰＫ１と、を用いて、共有鍵ＳＫ１を生成する。そして、端末１０は、Ｔ１４４において、生成済みの共有鍵ＳＫ１を用いてランダム値ＲＶ１を暗号化して、暗号化データＥＤ１を生成する。

【００４５】

Ｔ２００では、端末１０は、Ｗｉ－ＦｉＩ／Ｆ１６を介して、図３のＴ１３０で取得されたＭＡＣアドレス「ａｂｃ」を送信先として、ＡＲｅｑをプリンタ１００に送信する。ＡＲｅｑは、認証の実行をプリンタ１００に要求する信号である。ここで、端末１０は、Ｔ１３０で取得されたチャネルリスト内の複数個の通信チャネルを順次利用して、ＡＲｅｑをプリンタ１００に送信することを繰り返す。当該ＡＲｅｑは、Ｔ１４１で生成された端末１０の公開鍵ＴＰＫ１と、Ｔ１４４で生成された暗号化データＥＤ１と、端末１０のｃａｐａｂｉｌｉｔｙと、を含む。

【００４６】

ｃａｐａｂｉｌｉｔｙは、ＤＰＰ方式をサポートしている機器において予め指定されている情報であり、ＤＰＰ方式のＣｏｎｆｉｇｕｒａｔｏｒのみとして動作可能であること

を示す値と、ＤＰＰ方式のＥｎｒｏｌｌｅｅのみとして動作可能であることを示す値と、Ｃｏｎｆｉｇｕｒａｔｏｒ及びＥｎｒｏｌｌｅｅのどちらとしても動作可能であることを示す値と、のいずれか１個の値を含む。なお、Ｃｏｎｆｉｇｕｒａｔｏｒは、Ｃｏｎｆｉｇ（図２のＴ３０）において、ＮＡ（図２のＴ３５）で利用されるＣＯをＥｎｒｏｌｌｅｅに送信するデバイスを意味する。一方、Ｅｎｒｏｌｌｅｅは、Ｃｏｎｆｉｇにおいて、ＣｏｎｆｉｇｕｒａｔｏｒからＮＡで利用されるＣＯを受信するデバイスを意味する。上記のように、本実施例では、端末１０が第１又は第２のＣＯを生成してＡＰ６又はプリンタ１００に送信する。従って、端末１０のｃａｐａｂｉｌｉｔｙは、Ｃｏｎｆｉｇｕｒａｔｏｒのみとして動作可能であることを示す値を含む。

【００４７】

プリンタ１００は、Ｔ２００において、端末１０から、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＡＲｅｑを受信する。上記のように、当該ＡＲｅｑは、プリンタ１００のＭＡＣアドレス「ａｂｃ」を送信先として送信される。従って、プリンタ１００は、端末１０から当該ＡＲｅｑを適切に受信することができる。

【００４８】

また、プリンタ１００は、図３のＴ１２２で可能状態に移行すると、チャネルリスト内の複数個の通信チャネルのうちの１個の通信チャネルが利用されたＡＲｅｑを受信することを監視する。上記のように、Ｔ２００のＡＲｅｑは、チャネルリスト内の複数個の通信チャネルを順次利用して送信される。従って、プリンタ１００は、端末１０から当該ＡＲｅｑを適切に受信することができる。

【００４９】

次いで、プリンタ１００は、ＡＲｅｑの送信元（即ち端末１０）を認証するための以下の処理を実行する。具体的には、まず、プリンタ１００は、Ｔ２０２において、ＥＣＤＨに従って、当該ＡＲｅｑ内の端末１０の公開鍵ＴＰＫ１と、メモリ１３４内に予め記憶されているプリンタ１００の秘密鍵ｐｓｋ１と、を用いて、共有鍵ＳＫ１を生成する。ここで、Ｔ１４２で端末１０によって生成される共有鍵ＳＫ１と、Ｔ２０４でプリンタ１００によって生成される共有鍵ＳＫ１と、は同じである。従って、プリンタ１００は、Ｔ２０４において、生成済みの共有鍵ＳＫ１を用いて、当該ＡＲｅｑ内の暗号化データＥＤ１を適切に復号することができ、この結果、ランダム値ＲＶ１を取得することができる。プリンタ１００は、暗号化データＥＤ１の復号が成功する場合には、当該ＡＲｅｑの送信元が図３のＴ１１４で受信されたＳＲｅｑの送信元のデバイスであると判断し、即ち、認証が成功したと判断し、Ｔ２０６以降の処理を実行する。一方、プリンタ１００は、仮に、暗号化データＥＤ１の復号が成功しない場合には、当該ＡＲｅｑの送信元がＴ１１４で受信されたＳＲｅｑの送信元のデバイスでないと判断し、即ち、認証が失敗したと判断し、Ｔ２０６以降の処理を実行しない。

【００５０】

プリンタ１００は、Ｔ２０６において、プリンタ１００の新たな公開鍵ＰＰＫ２及び新たな秘密鍵ｐｓｋ２を生成する。なお、変形例では、公開鍵ＰＰＫ２及び秘密鍵ｐｓｋ２は、メモリ１３４に予め記憶されていてもよい。次いで、プリンタ１００は、Ｔ２０７において、ＥＣＤＨに従って、Ｔ２００のＡＲｅｑ内の端末１０の公開鍵ＴＰＫ１と、生成済みのプリンタ１００の秘密鍵ｐｓｋ２と、を用いて、共有鍵ＳＫ２を生成する。そして、プリンタ１００は、Ｔ２０８において、生成済みの共有鍵ＳＫ２を用いて、取得済みのランダム値ＲＶ１及び新たなランダム値ＲＶ２を暗号化して、暗号化データＥＤ２を生成する。

【００５１】

Ｔ２１０では、プリンタ１００は、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＡＲｅｓを端末１０に送信する。当該ＡＲｅｓは、Ｔ２０６で生成されたプリンタ１００の公開鍵ＰＰＫ２と、Ｔ２０８で生成された暗号化データＥＤ２と、プリンタ１００のｃａｐａｂｉｌｉｔｙと、を含む。当該ｃａｐａｂｉｌｉｔｙは、Ｅｎｒｏｌｌｅｅのみとして動作可能であることを示す値を含む。

【００５２】
端末１０は、Ｔ２１０において、プリンタ１００から、Ｗｉ－ＦｉＩ／Ｆ１６を介して、ＡＲｅｓを受信することに応じて、当該ＡＲｅｓの送信元（即ちプリンタ１００）を認証するための以下の処理を実行する。具体的には、まず、端末１０は、Ｔ２１２において、ＥＣＤＨに従って、Ｔ１４１で生成された端末１０の秘密鍵ｔｓｋ１と、当該ＡＲｅｓ内のプリンタ１００の公開鍵ＰＰＫ２と、を用いて、共有鍵ＳＫ２を生成する。ここで、Ｔ２０７でプリンタ１００によって生成される共有鍵ＳＫ２と、Ｔ２１２で端末１０によって生成される共有鍵ＳＫ２と、は同じである。従って、端末１０は、Ｔ２１４において、生成済みの共有鍵ＳＫ２を用いて、当該ＡＲｅｓ内の暗号化データＥＤ２を適切に復号することができ、この結果、ランダム値ＲＶ１及びＲＶ２を取得することができる。端末１０は、暗号化データＥＤ２の復号が成功する場合には、当該ＡＲｅｓの送信元が図３のＴ１３０で受信されたＳＲｅｓの送信元のデバイスであると判断し、即ち、認証が成功したと判断し、Ｔ２２０以降の処理を実行する。一方、端末１０は、仮に、暗号化データＥＤ２の復号が成功しない場合には、当該ＡＲｅｓの送信元がＴ１３０で受信されたＳＲｅｓの送信元のデバイスでないと判断し、即ち、認証が失敗したと判断し、Ｔ２２０以降の処理を実行しない。

【００５３】
Ｔ２２０において、端末１０は、Ｗｉ－ＦｉＩ／Ｆ１６を介して、Ｃｏｎｆｉｒｍをプリンタ１００に送信する。Ｃｏｎｆｉｒｍは、端末１０がＣｏｎｆｉｇｕｒａｔｏｒとして動作し、かつ、プリンタ１００がＥｎｒｏｌｌｅｅとして動作することを示す情報を含む。この結果、Ｔ２２２において、Ｃｏｎｆｉｇｕｒａｔｏｒとして動作することが端末１０によって決定され、Ｔ２２４において、Ｅｎｒｏｌｌｅｅとして動作することがプリンタ１００によって決定される。Ｔ２２４の処理が終了すると、図４の処理が終了する。

【００５４】
（Ｃｏｎｆｉｇｕｒａｔｉｏｎ（Ｃｏｎｆｉｇ）；図５）
続いて、図５を参照して、図２のＴ３０のＣｏｎｆｉｇの処理を説明する。Ｔ３００では、プリンタ１００は、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＤＰＰ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｒｅｑｕｅｓｔ（以下では、単に「ＣＲｅｑ」と記載する）を端末１０に送信する。当該ＣＲｅｑは、ＣＯ（即ちプリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続を確立するための情報）の送信を要求する信号である。

【００５５】
端末１０は、Ｔ３００において、プリンタ１００から、Ｗｉ－ＦｉＩ／Ｆ１６を介して、ＣＲｅｑを受信する。この場合、端末１０は、Ｔ３０１において、端末１０のメモリ（図示省略）から、グループＩＤ「Ｇｒｏｕｐ１」と公開鍵ＴＰＫ２と秘密鍵ｔｓｋ２とを取得する。上述したように、端末１０は、図２のＴ１５のＣｏｎｆｉｇをＡＰ６と実行済みであり、この際に、グループＩＤ「Ｇｒｏｕｐ１」と公開鍵ＴＰＫ２と秘密鍵ｔｓｋ２とを生成してメモリに記憶する。グループＩＤ「Ｇｒｏｕｐ１」は、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続が確立されることによって形成される無線ネットワークを識別する情報である。なお、変形例では、ユーザによって指定された文字列がグループＩＤとして利用されてもよい。即ち、Ｔ３０１では、端末１０は、図２のＴ１５で記憶された各情報を取得する。次いで、端末１０は、Ｔ３０２において、第２のＣＯ（図２のＴ３０参照）を生成する。具体的には、端末１０は、以下の各処理を実行する。

【００５６】
端末１０は、端末１０の公開鍵ＴＰＫ２をハッシュ化することによって、ハッシュ値ＨＶを生成する。また、端末１０は、ハッシュ値ＨＶと、グループＩＤ「Ｇｒｏｕｐ１」と、図４のＴ２１０のＡＲｅｓ内のプリンタ１００の公開鍵ＰＰＫ２と、の組み合わせをハッシュ化することによって、特定値を生成する。そして、端末１０は、ＥＣＤＳＡ（Elliptic Curve Digital Signature Algorithmの略）に従って、端末１０の秘密鍵ｔｓｋ２を用いて、生成済みの特定値を暗号化することによって、電子署名ＤＳ１を生成する。この結果、端末１０は、ハッシュ値ＨＶと、グループＩＤ「Ｇｒｏｕｐ１」と、プリンタ１０

０の公開鍵ＰＰＫ２と、電子署名ＤＳ１と、を含むプリンタ用Ｓｉｇｎｅｄ－Ｃｏｎｎｅｃｔｏｒ（以下では、Ｓｉｇｎｅｄ－Ｃｏｎｎｅｃｔｏｒのことを単に「ＳＣｏｎｔ」と記載する）を生成することができる。そして、端末１０は、プリンタ用ＳＣｏｎｔと、端末１０の公開鍵ＴＰＫ２と、を含む第２のＣＯを生成する。

【００５７】

Ｔ３１０では、端末１０は、Ｗｉ－ＦｉＩ／Ｆ１６を介して、第２のＣＯを含むＤＰＰ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｒｅｓｐｏｎｓｅ（以下では、単に「ＣＲｅｓ」と記載する）をプリンタ１００に送信する。

【００５８】

プリンタ１００は、Ｔ３１０において、端末１０から、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＣＲｅｓを受信する。この場合、プリンタ１００は、Ｔ３１２において、当該ＣＲｅｓ内の第２のＣＯをメモリ１３４に記憶する。Ｔ３１２の処理が終了すると、図５の処理が終了する。

【００５９】

（Ｎｅｔｗｏｒｋ Ａｃｃｅｓｓ（ＮＡ）；図６）

上記のように、図２のＴ２０～Ｔ３０と同様に、図２のＴ５～Ｔ１５の処理が端末１０及びＡＰ６の間で実行済みである。ただし、ＡＰ６は、図３のＴ１０５～Ｔ１２４の処理を実行しない。ＡＰ６は、ＡＰ６の公開鍵ＡＰＫ１及び秘密鍵ａｓｋ１を予め記憶している。そして、ＡＰ６の公開鍵ＡＰＫ１と、ＡＰ６のチャネルリストと、ＡＰ６のＭＡＣアドレスと、をコード化することによって得られるＱＲコードが、ＡＰ６の筐体に貼り付けられている。端末１０が当該ＱＲコードを撮影することによって、端末１０及びＡＰ６の間でＴ１３４以降の各処理と同様の各処理が実行される。この結果、ＡＰ６は、ＡＰ６の公開鍵ＡＰＫ２及び秘密鍵ａｓｋ２を記憶し（図４のＴ２０６参照）、さらに、端末１０から受信される第１のＣＯを記憶する（図５のＴ３１２参照）。第１のＣＯは、ＡＰ用ＳＣｏｎｔと、端末１０の公開鍵ＴＰＫ２と、を含む。当該公開鍵ＴＰＫ２は、第２のＣＯに含まれる公開鍵ＴＰＫ２と同じである。また、ＡＰ用ＳＣｏｎｔは、ハッシュ値ＨＶと、グループＩＤ「Ｇｒｏｕｐ１」と、ＡＰ６の公開鍵ＡＰＫ２と、電子署名ＤＳ２と、を含む。当該ハッシュ値ＨＶ及び当該グループＩＤ「Ｇｒｏｕｐ１」は、それぞれ、第２のＣＯに含まれるハッシュ値ＨＶ及びグループＩＤ「Ｇｒｏｕｐ１」と同じである。電子署名ＤＳ２は、ハッシュ値ＨＶとグループＩＤ「Ｇｒｏｕｐ１」と公開鍵ＡＰＫ２との組み合わせをハッシュ化することによって得られる特定値が端末１０の秘密鍵ｔｓｋ２によって暗号化された情報であり、第２のＣＯに含まれる電子署名ＤＳ１とは異なる値である。

【００６０】

プリンタ１００は、Ｔ４００において、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、プリンタ用ＳＣｏｎｔを含むＤＰＰ Ｐｅｅｒ Ｄｉｓｃｏｖｅｒｙ Ｒｅｑｕｅｓｔ（以下では、単に「ＤＲｅｑ」と記載する）をＡＰ６に送信する。当該ＤＲｅｑは、認証の実行と、ＡＰ用ＳＣｏｎｔの送信と、をＡＰ６に要求する信号である。

【００６１】

ＡＰ６は、Ｔ４００において、プリンタ１００からＤＲｅｑを受信することに応じて、ＤＲｅｑの送信元（即ちプリンタ１００）、及び、ＤＲｅｑ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＰＰＫ２）を認証するための処理を実行する。具体的には、ＡＰ６は、Ｔ４０２において、まず、受信済みのプリンタ用ＳＣｏｎｔ内のハッシュ値ＨＶ及びグループＩＤ「Ｇｒｏｕｐ１」が、それぞれ、記憶済みの第１のＣＯに含まれるＡＰ用ＳＣｏｎｔ内のハッシュ値ＨＶ及びグループＩＤ「Ｇｒｏｕｐ１」に一致するのか否かに関する第１のＡＰ判断処理を実行する。図６のケースでは、ＡＰ６は、第１のＡＰ判断処理で「一致する」と判断するので、ＤＲｅｑの送信元（即ちプリンタ１００）の認証が成功したと判断する。なお、受信済みのプリンタ用ＳＣｏｎｔ内のハッシュ値ＨＶと、記憶済みの第１のＣＯに含まれるＡＰ用ＳＣｏｎｔ内のハッシュ値ＨＶと、が一致するということは、プリンタ用ＳＣｏｎｔ及びＡＰ用ＳＣｏｎｔが、同じ装置（即ち、端末１０）によって生成されたことを意味する。従って、ＡＰ６は、受信済みのプリ

ンタ用ＳＣｏｎｔの生成元（即ち、端末１０）の認証が成功したとも判断する。さらに、ＡＰ６は、記憶済みの第１のＣＯに含まれる端末１０の公開鍵ＴＰＫ２を用いて、受信済みのプリンタ用ＳＣｏｎｔ内の電子署名ＤＳ１を復号する。図６のケースでは、電子署名ＤＳ１の復号が成功するので、ＡＰ６は、電子署名ＤＳ１を復号することによって得られた特定値と、受信済みのプリンタ用ＳＣｏｎｔ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＰＰＫ２）をハッシュ化することによって得られる値と、が一致するのか否かに関する第２のＡＰ判断処理を実行する。図６のケースでは、ＡＰ６は、第２のＡＰ判断処理で「一致する」と判断するので、ＤＲｅｑ内の各情報の認証が成功したと判断し、Ｔ４０４以降の処理を実行する。第２のＡＰ判断処理で「一致する」と判断されることは、第２のＣＯがプリンタ１００に記憶された後に、受信済みのプリンタ用ＳＣｏｎｔ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＰＰＫ２）が第三者によって改ざんされていないことを意味する。一方、第１のＡＰ判断処理で「一致しない」と判断される場合、電子署名ＤＳ１の復号が失敗する場合、又は、第２のＡＰ判断処理で「一致しない」と判断される場合には、ＡＰ６は、認証が失敗したと判断し、Ｔ４０４以降の処理を実行しない。

【００６２】

次いで、ＡＰ６は、Ｔ４０４において、ＥＣＤＨに従って、取得済みのプリンタ１００の公開鍵ＰＰＫ２と、記憶済みのＡＰ６の秘密鍵ａｓｋ２と、を用いて、接続キー（即ち共有鍵）ＣＫを生成する。

【００６３】

Ｔ４１０では、ＡＰ６は、ＡＰ用ＳＣｏｎｔを含むＤＰＰ　Ｐｅｅｒ　Ｄｉｓｃｏｖｅｒｙ　Ｒｅｓｐｏｎｓｅ（以下では、単に「ＤＲｅｓ」と記載する）をプリンタ１００に送信する。

【００６４】

プリンタ１００は、Ｔ４１０において、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＡＰ６からＤＲｅｓを受信することに応じて、ＤＲｅｓの送信元（即ちＡＰ６）、及び、ＤＲｅｓ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＡＰＫ２）を認証するための処理を実行する。具体的には、プリンタ１００は、Ｔ４１２において、まず、受信済みのＡＰ用ＳＣｏｎｔ内のハッシュ値ＨＶ及びグループＩＤ「Ｇｒｏｕｐ１」が、それぞれ、記憶済みの第２のＣＯに含まれるプリンタ用ＳＣｏｎｔ内のハッシュ値ＨＶ及びグループＩＤ「Ｇｒｏｕｐ１」に一致するのか否かに関する第１のＰＲ判断処理を実行する。図６のケースでは、プリンタ１００は、第１のＰＲ判断処理で「一致する」と判断するので、ＤＲｅｓの送信元（即ちＡＰ６）の認証が成功したと判断する。なお、受信済みのＡＰ用ＳＣｏｎｔ内のハッシュ値ＨＶと、記憶済みの第２のＣＯに含まれるプリンタ用ＳＣｏｎｔ内のハッシュ値ＨＶと、が一致するということは、プリンタ用ＳＣｏｎｔ及びＡＰ用ＳＣｏｎｔが、同じ装置（即ち、端末１０）によって生成されたことを意味する。従って、プリンタ１００は、受信済みのＡＰ用ＳＣｏｎｔの生成元（即ち、端末１０）の認証が成功したとも判断する。さらに、プリンタ１００は、記憶済みの第２のＣＯに含まれる端末１０の公開鍵ＴＰＫ２を用いて、受信済みのＡＰ用ＳＣｏｎｔ内の電子署名ＤＳ２を復号する。図６のケースでは、電子署名ＤＳ２の復号が成功するので、プリンタ１００は、電子署名ＤＳ２を復号することによって得られた特定値と、受信済みのＡＰ用ＳＣｏｎｔ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＡＰＫ２）をハッシュ化することによって得られる値と、が一致するのか否かに関する第２のＰＲ判断処理を実行する。図６のケースでは、プリンタ１００は、第２のＰＲ判断処理で「一致する」と判断するので、ＤＲｅｓ内の各情報の認証が成功したと判断し、Ｔ４１４以降の処理を実行する。第２のＰＲ判断処理で「一致する」と判断されることは、第１のＣＯがＡＰ６に記憶された後に、ＡＰ用ＳＣｏｎｔ内の各情報（即ち、ハッシュ値ＨＶ、「Ｇｒｏｕｐ１」、及び、公開鍵ＡＰＫ２）が第三者によって改ざんされていないことを意味する。一方、第１のＰＲ判断処理で「一致しない」と判断される場合、電子署名ＤＳ２の復号が失敗する場合、又は、第２のＰＲ判断処理で「一致しない」と判断される場合には、

プリンタ１００は、認証が失敗したと判断し、Ｔ４１４以降の処理を実行しない。
【００６５】
プリンタ１００は、Ｔ４１４において、ＥＣＤＨに従って、記憶済みのプリンタ１００の秘密鍵ｐｓｋ２と、受信済みのＡＰ用ＳＣｏｎｔ内のＡＰ６の公開鍵ＡＰＫ２と、を用いて、接続キーＣＫを生成する。ここで、Ｔ４０４でＡＰ６によって生成される接続キーＣＫと、Ｔ４１４でプリンタ１００によって生成される接続キーＣＫと、は同じである。これにより、Ｗｉ－Ｆｉ接続を確立するための接続キーＣＫがプリンタ１００及びＡＰ６の間で共有される。Ｔ４１４が終了すると、図６の処理が終了する。
【００６６】
上述したように、接続キーＣＫがプリンタ１００及びＡＰ６の間で共有された後に、図２のＴ４０において、プリンタ１００及びＡＰ６は、接続キーＣＫを利用して、４ｗａｙ－ｈａｎｄｓｈａｋｅの通信を実行する。この結果、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立される。なお、上述したように、プリンタ１００は、プリンタ１００のチャネルリストに含まれる複数個の通信チャネルのうちの１個の通信チャネルを利用して、端末１０から図４のＴ２００のＡＲｅｑを受信する。即ち、プリンタ１００は、プリンタ１００と端末１０との双方が利用可能な通信チャネルを利用して、端末１０からＴ２００のＡＲｅｑを受信する。一方、図２のＴ４０では、プリンタ１００は、プリンタ１００とＡＰ６との双方が利用可能な通信チャネルを利用して、Ｗｉ－Ｆｉ接続をＡＰ６と確立する。ここで、端末１０が利用可能な通信チャネルと、ＡＰ６が利用可能な通信チャネルと、は異なる場合がある。本実施例では、プリンタ１００が図４のＴ２００で端末１０からＡＲｅｑを受信するための通信チャネルと、プリンタ１００が図２のＴ４０でＷｉ－Ｆｉ接続をＡＰ６と確立するための通信チャネルと、が異なる。ただし、変形例では、前者の通信チャネルと後者の通信チャネルとは同じでもよい。
【００６７】
（ケースＢのＢｏｏｔｓｔｒａｐｐｉｎｇ（ＢＳ）；図７）
続いて、図７を参照して、ＢＳの他のケースＢの処理を説明する。ケースＢは、図２のＴ５～Ｔ４０が実行された後の状態、即ち、プリンタ１００のメモリ１３４が第２のＣＯを記憶済みである状態である。
【００６８】
Ｔ５００及びＴ５０５は、図３のＴ１００及びＴ１０５と同様である。本ケースでは、プリンタ１００のメモリ１３４が第２のＣＯを記憶しているので、プリンタ１００は、ＢＴＩ／Ｆ１１８の動作モードを通常モードから設定モードに移行させない。プリンタ１００は、第２のＣＯを記憶している状況では、第２のＣＯを利用して、Ｗｉ－Ｆｉ接続をＡＰ６と確立することができる。従って、プリンタ１００においてＢＳが実行される可能性が低い。プリンタ１００は、このような状況において、ＢＴＩ／Ｆ１１８の動作モードを設定モードに移行させないので、ＳＲｅｑが端末１０からプリンタ１００に送信されても、当該ＳＲｅｑがＢＴＩ／Ｆ１１８からＣＰＵ１３２に供給されず、この結果、プリンタ１００において第１の指示画面ＦＩＳが表示されない。従って、プリンタ１００の処理負荷を軽減できる。
【００６９】
ユーザは、プリンタ１００が第２のＣＯを記憶している状態において、例えば、ＡＰ６とは異なるＡＰとプリンタ１００との間のＷｉ－Ｆｉ接続の確立を望む可能性がある。この場合、ユーザは、Ｔ５０６において、メニュー画面ＭＳ内の設定ボタンを選択する。この場合、プリンタ１００は、Ｔ５０７において、設定画面ＳＳを表示部１１４に表示させる。画面ＳＳは、プリンタ１００の印刷設定を変更するための印刷設定ボタンと、ＢＴＩ／Ｆ１１８の動作モードを変更するためのモード移行ボタンと、を含む。そして、Ｔ５０８では、ユーザは、画面ＳＳ内のモード移行ボタンを選択する。この場合、プリンタ１００は、Ｔ５０９において、ＢＴＩ／Ｆ１１８の動作モードを通常モードから設定モードに移行させる。これにより、プリンタ１００は、端末１０からＳＲｅｑを受信することに応じて、図３のＴ１１４以降の処理と同様の処理を実行することができる。

【００７０】
なお、プリンタ１００は、ＤＰＰ方式を利用せずに、通常のＷｉ－Ｆｉ方式（即ちＳＳＩＤ及びパスワードを利用する方式）に従って、ＡＰ６とのＷｉ－Ｆｉ接続を確立することもできる。この場合、プリンタ１００のメモリ１３４は、ＡＰ６とのＷｉ－Ｆｉ接続を確立するための無線設定情報（即ちＳＳＩＤ及びパスワード）を記憶する。このような状態でプリンタ１００の電源がＯＮされても、プリンタ１００は、図７のケースＢと同様に、ＢＴＩ／Ｆ１１８の動作モードを通常モードから設定モードに移行させない。プリンタ１００が無線設定情報を利用してＡＰ６とＷｉ－Ｆｉ接続を確立することができるからである。これにより、ＳＲｅｑが端末１０からプリンタ１００に送信されても、プリンタ１００において第１の指示画面ＦＩＳが表示されない。従って、プリンタ１００の処理負荷を軽減できる。

【００７１】
（本実施例の効果）
ここで、端末１０からＳＲｅｑが受信されることに応じて、第１の指示画面ＦＩＳが表示されない比較例のプリンタを想定する。そして、例えば、端末１０のユーザが、比較例のプリンタとは異なるプリンタとＡＰ６との間でＷｉ－Ｆｉ接続が確立されることを望んでいる状況、即ち、比較例のプリンタと端末１０との間でＤＰＰ方式に従った通信が実行されること望んでいない状況を想定する。この場合、比較例のプリンタは、端末１０からＳＲｅｑを受信することに応じて、図３のＴ１２２以降の処理と同様の処理を自動的に実行してＳＲｅｓを端末１０に送信する。即ち、比較例のプリンタ１００は、端末１０からＳＲｅｑを受信することに応じて、ユーザからの指示を受け付けなくても、ＳＲｅｓを端末１０に送信する。この場合、比較例のプリンタとＡＰ６との間にＷｉ－Ｆｉ接続が確立され得る。即ち、端末１０のユーザによって意図されていない一対の装置（即ち比較例のプリンタ及びＡＰ６）の間にＷｉ－Ｆｉ接続が確立され得る。

【００７２】
これに対し、本実施例のプリンタ１００は、端末１０からＳＲｅｑを受信する場合（図３のＴ１１４）に、第１の指示画面ＦＩＳを表示する（Ｔ１１６）。これにより、プリンタ１００は、画面ＦＩＳ内のＹＥＳボタンがユーザによって選択される場合（Ｔ１２０）、即ち、プリンタ１００と端末１０との間でＤＰＰ方式に従った通信（即ち、公開鍵ＰＰＫ１が利用された通信）が実行されることをユーザが望む場合に、公開鍵ＰＰＫ１等を含むＳＲｅｓを端末１０に送信する（Ｔ１３０）。この結果、プリンタ１００は、端末１０からＡＲｅｑを受信し（図４のＴ２００）、ＡＲｅｓを端末１０に送信し（Ｔ２１０）、端末１０から第２のＣＯを受信し（図５のＴ３１０）、第２のＣＯを利用してＡＰ６とのＷｉ－Ｆｉ接続を確立する（図２のＴ３５、Ｔ４０）。このために、端末１０のユーザによって意図されている一対の装置（即ちプリンタ１００及びＡＰ６）の間にＷｉ－Ｆｉ接続を確立することができる。一方、画面ＦＩＳ内のＹＥＳボタンが選択されない場合、即ち、プリンタ１００と端末１０との間でＤＰＰ方式に従った通信が実行されることをユーザが望まない場合に、公開鍵ＰＰＫ１等を含むＳＲｅｓは送信されない。従って、プリンタ１００では、端末１０からＡＲｅｑが受信されず、この結果、ＡＰ６とのＷｉ－Ｆｉ接続が確立されない。このために、端末１０のユーザによって意図されていない一対の装置（即ちプリンタ１００及びＡＰ６）の間にＷｉ－Ｆｉ接続が確立されることを抑制できる。

【００７３】
（対応関係）
プリンタ１００、端末１０、ＡＰ６が、それぞれ、「通信装置」、「第１の外部装置」、「第２の外部装置」の一例である。ＢＴＩ／Ｆ１１８、Ｗｉ－ＦｉＩ／Ｆ１１６が、それぞれ、「第１の無線インターフェース」、「第２の無線インターフェース」の一例である。図３のＴ１１４のＳＲｅｑ、プリンタ１００の公開鍵ＰＰＫ１が、それぞれ、「特定信号」、「公開鍵」の一例である。ＡＲｅｑ、ＡＲｅｓ、第２のＣＯが、それぞれ、「認証要求」、「認証応答」、「接続情報」の一例である。図２のＴ４０で確立されるＷｉ－

Ｆｉ接続が、「無線接続」の一例である。
【００７４】
チャネルリスト、図４のＴ２００で利用される通信チャネル、図２のＴ４０で利用される通信チャネルが、それぞれ、「通信チャネル情報」、「第１の通信チャネル」、「第２の通信チャネル」の一例である。メモリ１３４内に第２のＣＯが記憶されていない状態でユーザからの電源ＯＮ操作を受け付けること、及び、メモリ１３４内に第２のＣＯが記憶されている状態でユーザからのモード移行ボタンの選択を受け付けることが、「所定条件」の一例である。通常モード、設定モードが、それぞれ、「第１のモード」、「第２のモード」の一例である。ＡＰ用ＳＣｏｎｔ、第２のＣＯ内のハッシュ値ＨＶが、それぞれ、「受信情報」、「認証情報」の一例である。
【００７５】
図３のＴ１１４の処理、Ｔ１１６の処理、Ｔ１３０の処理、図４のＴ２００の処理、Ｔ２１０の処理、図５のＴ３１０の処理、図２のＴ３５及びＴ４０の処理が、それぞれ、「特定信号受信部」、「第１の表示制御部」、「公開鍵送信部」、「認証要求受信部」、「認証応答送信部」、「接続情報受信部」、「確立部」によって実行される処理の一例である。
【００７６】
（第２実施例；図８～図１２）
続いて、第２実施例を説明する。第２実施例は、ＢＳ及びＡｕｔｈにおいてプリンタ１００によって実行される処理が異なる。
【００７７】
（ＢＳの処理；図８）
まず、図８を参照して、図２のＴ２０のＢＳにおいて、プリンタによって実行される処理の詳細を説明する。ＢＴＩ／Ｆ１１８の動作モードが通常モードから設定モードに移行される場合に、図８の処理が実行される。
【００７８】
Ｓ５では、プリンタ１００は、ＢＴＩ／Ｆ１１８を介して、ＳＲｅｑを受信することを監視する。具体的には、プリンタ１００（即ちＣＰＵ１３２）は、ＢＴＩ／Ｆ１１８からＳＲｅｑが取得される場合に、Ｓ５でＹＥＳと判断して、Ｓ１０に進む。以下では、当該ＳＲｅｑの送信元の端末を「対象端末」と呼ぶ。
【００７９】
Ｓ１０では、プリンタ１００は、受信済みのＳＲｅｑの受信電波強度を取得し、当該受信電波強度が閾値以上であるのか否かを判断する。なお、当該閾値は、プリンタ１００の出荷時にプリンタ１００のベンダによって決定される値であってもよいし、プリンタ１００の出荷後にユーザによって指定される値であってもよい。ＢＴＩ／Ｆ１１８は、ＳＲｅｑを受信する際に、ＳＲｅｑの受信電波強度を特定し、特定済みの受信電波強度をプリンタ１００（即ちＣＰＵ１３２）に供給する。これにより、プリンタ１００（即ちＣＰＵ１３２）は、受信電波強度を取得することができる。プリンタ１００は、取得済みの受信電波強度が閾値以上であると判断する場合に、Ｓ１０でＹＥＳと判断して、Ｓ２５に進む。一方、プリンタ１００は、取得済みの受信電波強度が閾値未満であると判断する場合に、Ｓ１０でＮＯと判断して、Ｓ１５に進む。
【００８０】
Ｓ１５では、プリンタ１００は、第１の指示画面ＦＩＳを表示部１１４に表示させる。当該画面ＦＩＳは、図３のＴ１１６の第１の指示画面ＦＩＳと同じ画面である。即ち、画面ＦＩＳは、接続処理を実行することを示すＹＥＳボタンを含む。
【００８１】
Ｓ２０では、プリンタ１００は、画面ＦＩＳ内のＹＥＳボタンが選択されたのか否かを判断する。プリンタ１００は、画面ＦＩＳ内のＹＥＳボタンがユーザによって選択される場合に、Ｓ２０でＹＥＳと判断して、Ｓ２５に進む。一方、プリンタ１００は、Ｓ１５で画面ＦＩＳが表示されてから所定時間内にＹＥＳボタンが選択されない場合（即ち、タイ

ムアウト）に、Ｓ２０でＮＯと判断して、後述のＳ２５以降の処理を実行することなく、非実行ＥＮＤとして図８の処理を終了する。非実行ＥＮＤは、ＤＰＰ方式に従った処理を中止すること意味する。

【００８２】

Ｓ２５では、プリンタ１００は、Ｓ５でＢＴＩ／Ｆ１１８から取得されたＳＲｅｑが対象端末のＭＡＣアドレスを含むのか否かを判断する。プリンタ１００は、ＳＲｅｑがＭＡＣアドレスを含む場合に、Ｓ２５でＹＥＳと判断し、Ｓ３０において、当該ＭＡＣアドレスをメモリ１３４に記憶して、Ｓ３５に進む。一方、プリンタ１００は、ＳＲｅｑがＭＡＣアドレスを含まない場合に、Ｓ２５でＮＯと判断して、Ｓ３５に進む。

【００８３】

Ｓ３５では、プリンタ１００は、不可能状態から可能状態に移行する。なお、プリンタ１００は、既に可能状態として動作している場合には、Ｓ３５の処理をスキップして、Ｓ４０に進む。

【００８４】

Ｓ４０では、プリンタ１００は、ＢＴＩ／Ｆ１１８を介して、ＳＲｅｓを対象端末に送信する。当該ＳＲｅｓは、プリンタ１００の公開鍵ＰＰＫ１と、メモリ１３４内に予め記憶されているチャネルリストと、Ｗｉ－ＦｉＩ／Ｆ１１６のＭＡＣアドレス「ａｂｃ」と、を含む。Ｓ４０の処理が終了すると、Ａｕｔｈの処理を実行する実行ＥＮＤとして図８の処理が終了する。

【００８５】

（Ａｕｔｈの処理；図９）

続いて、図９を参照して、図２のＴ２５のＡｕｔｈにおいてプリンタ１００によって実行される処理の詳細を説明する。図８のＳ３５でプリンタ１００が可能状態に移行する場合に、図９の処理が実行される。

【００８６】

Ｓ１００では、プリンタ１００は、Ｗｉ－ＦｉＩ／Ｆ１１６を介してＡＲｅｑを受信することを監視する。以下では、当該ＡＲｅｑの送信元の端末を「特定端末」と呼ぶ。当該ＡＲｅｑは、特定端末の公開鍵と、特定端末によって生成された暗号化データと、特定端末のＭＡＣアドレスと、特定端末のｃａｐａｂｉｌｉｔｙと、を含む（図４のＴ２００参照）。プリンタ１００は、特定端末からＡＲｅｑが受信される場合に、Ｓ１００でＹＥＳと判断して、Ｓ１０５に進む。一方、プリンタ１００は、可能状態に移行してから（図８のＳ３５）所定時間内にＡＲｅｑが受信されない場合に、Ｓ１００でＮＯと判断して、非実行ＥＮＤとして図９の処理を終了する。

【００８７】

Ｓ１０５では、プリンタ１００は、図８のＳ３０で記憶済みの対象端末のＭＡＣアドレスと、Ｓ１００で受信されたＡＲｅｑ内の特定端末のＭＡＣアドレスと、が一致するのか否かを判断する。プリンタ１００は、対象端末のＭＡＣアドレスと特定端末のＭＡＣアドレスとが一致する場合、即ち、特定端末が対象端末に一致する場合に、Ｓ１０５でＹＥＳと判断して、Ｓ１２０に進む。一方、プリンタ１００は、対象端末のＭＡＣアドレスと特定端末のＭＡＣアドレスとが一致しない場合、即ち、特定端末が対象端末とは異なる場合に、Ｓ１０５でＮＯと判断して、Ｓ１１０に進む。なお、プリンタ１００は、Ｓ３０の処理がスキップされた場合、即ち、メモリ１３４内にＭＡＣアドレスが記憶されていない場合にも、Ｓ１０５でＮＯと判断して、Ｓ１１０に進む。

【００８８】

Ｓ１１０では、プリンタ１００は、Ｗｉ－Ｆｉ接続を確立するための接続処理を実行すべきことを指示するための第２の指示画面ＳＩＳを表示部１１４に表示させる。第２の指示画面ＳＩＳは、接続処理を実行することを示すＹＥＳボタンを含む。

【００８９】

Ｓ１１５では、プリンタ１００は、画面ＳＩＳ内のＹＥＳボタンが選択されたのか否かを判断する。プリンタ１００は、画面ＳＩＳ内のＹＥＳボタンがユーザによって選択され

る場合に、Ｓ１１５でＹＥＳと判断して、Ｓ１２０に進む。一方、プリンタ１００は、Ｓ１１０で画面ＳＩＳが表示されてから所定時間が経過してもＹＥＳボタンが選択されない場合（即ちタイムアウトの場合）には、画面ＳＩＳの表示を終了する。この場合、プリンタ１００は、後述のＳ１２０以降の処理を実行することなく、非実行ＥＮＤとして図９の処理を終了する。なお、変形例では、画面ＳＩＳが接続処理を実行しないことを示すＮＯボタンを含み、プリンタ１００は、画面ＳＩＳ内のＮＯボタンがユーザによって選択される場合に、Ｓ１１５でＮＯと判断して、非実行ＥＮＤとして図９の処理を終了してもよい。

【００９０】

Ｓ１２０では、プリンタ１００は、認証処理及び動作決定処理を実行する。認証処理は、プリンタ１００が通信相手を認証するための処理（即ち図４のＴ２０２～Ｔ２１０）である。動作決定処理は、プリンタ１００がＣｏｎｆｉｇｕｒａｔｏｒ又はＥｎｒｏｌｌｅｅとして動作することを決定するための処理（即ちＴ２２０～Ｔ２２４）である。プリンタ１００は、Ｓ１２０の処理が終了する場合に、Ｃｏｎｆｉｇを実行する実行ＥＮＤとして図９の処理を終了する。

【００９１】

（ケースＣのＢＳ及びＡｕｔｈ；図１０）

続いて、図１０を参照して、図８及び図９の処理によって実現されるケースＣのＢＳ及びＡｕｔｈの処理を説明する。ケースＣは、端末１０とプリンタ１００との間の距離が比較的に小さい状況を想定している。

【００９２】

Ｔ６００～Ｔ６１４は、図３のＴ１００～Ｔ１１４と同様である。プリンタ１００は、Ｔ６１６において、端末１０とプリンタ１００との間の距離が比較的に小さいので、ＳＲｅｑの受信電波強度が閾値以上であると判断する（図８のＳ１０でＹＥＳ）。また、プリンタ１００は、受信済みのＳＲｅｑがＭＡＣアドレス「ｘｘｘ」を含むと判断する（Ｓ２５でＹＥＳ）。この結果、プリンタ１００は、Ｔ６２０において、ＳＲｅｑ内のＭＡＣアドレス「ｘｘｘ」をメモリ１３４に記憶し（Ｓ３０）、Ｔ６２２において、不可能状態から可能状態に移行する（Ｓ３５）。

【００９３】

Ｔ６３０～Ｔ６５０は、図３のＴ１３０～Ｔ１４０及び図４のＴ１４１～Ｔ２００と同様である。Ｔ６５２では、プリンタ１００は、Ｔ６２０で記憶されたＭＡＣアドレス「ｘｘｘ」と、Ｔ６５０で受信されたＡＲｅｑ内のＭＡＣアドレス「ｘｘｘ」と、が一致すると判断する（図９のＳ１０５でＹＥＳ）。この場合、プリンタ１００は、図４のＴ２０２～Ｔ２２４と同様の処理を実行して、図１０の処理を終了する。その後、各デバイス６，１０，１００によって、図５及び図６と同様の処理が実行されて、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立される（図２のＴ４０）。

【００９４】

（ケースＤのＢＳ及びＡｕｔｈ；図１１）

続いて、図１１を参照して、図８及び図９の処理によって実現されるケースＤのＢＳ及びＡｕｔｈの処理を説明する。ケースＤは、端末１０とプリンタ１００との間の距離が比較的に大きい状況を想定している。

【００９５】

Ｔ７００～Ｔ７１４は、図３のＴ１００～Ｔ１１４と同様である。本ケースＤでは、端末１０とプリンタ１００との間の距離が比較的に大きいので、プリンタ１００は、Ｔ７１６において、ＳＲｅｑの受信電波強度が閾値未満であると判断して（図８のＳ１０でＮＯ）、Ｔ７１７において、第１の指示画面ＦＩＳを表示部１１４に表示させる（Ｓ１５）。そして、プリンタ１００は、Ｔ７１８において、第２の指示画面ＳＩＳ内のＹＥＳボタンが所定時間内に選択されなかった（即ちタイムアウト）と判断し（Ｓ２０でＮＯ）、画面ＦＩＳの表示を終了して図１１の処理を終了する。

【００９６】

ケースＤに示されるように、プリンタ１００と端末１０との間の距離が比較的に大きい状況では、端末１０のユーザは、ＤＰＰ方式に従った通信（即ち公開鍵ＰＰＫ１が利用された通信）がプリンタ１００と端末１０との間で実行されることを望んでいない可能性が高い。例えば、端末１０がプリンタ１００からかなり離れた位置に存在しており、端末１０のユーザが、プリンタ１００とは異なるプリンタとＡＰ６との間でＷｉ－Ｆｉ接続が確立されることを望んでいる状況を想定する。このような状況において、仮に、プリンタ１００が、端末１０からＳＲｅｑを受信することに応じて、図１０のＴ６２０以降の処理を自動的に実行してＳＲｅｓを端末１０に送信すると（Ｔ６３０）、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立され得る。即ち、端末１０のユーザによって意図されていない一対の装置（即ち、プリンタ１００及びＡＰ６）の間にＷｉ－Ｆｉ接続が確立され得る。

【００９７】

これに対し、ケースＤでは、プリンタ１００は、端末１０からＳＲｅｑを受信する場合（Ｔ７１４）に、ＳＲｅｑの受信電波強度が未満であると判断して、第１の指示画面ＦＩＳを表示部１１４に表示させることによって、公開鍵ＰＰＫ１の送信を制限する（Ｔ７１７）。端末１０のユーザは、プリンタ１００がＷｉ－Ｆｉ接続を確立することを望んでいないので、画面ＦＩＳ内のＹＥＳボタンを選択しない。この結果、プリンタ１００は、タイムアウトと判断し（Ｔ７１８）、ＳＲｅｓを端末１０に送信しない。従って、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立されるのを抑制することができる。即ち、端末１０のユーザによって意図されていない一対の装置の間にＷｉ－Ｆｉ接続が確立されるのを抑制することができる。なお、ケースＤにおいて、端末１０のユーザが、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立されることを望んでいる場合には、画面ＦＩＳ内のＹＥＳボタンがユーザによって選択される。この場合、図４のＴ２０２以降の処理が実行され、プリンタ１００とＡＰ６との間にＷｉ－Ｆｉ接続が確立される。従って、ユーザの意図に応じたＷｉ－Ｆｉ接続を確立させることができる。

【００９８】

（ケースＥのＢＳ及びＡｕｔｈ；図１２）

続いて、図１２を参照して、図８及び図９の処理によって実現されるケースＥのＢＳ及びＡｕｔｈの処理を説明する。ここで、端末１０は、プリンタ１００のベンダによって提供される第１種のアプリ４０を備える。このため、端末１０のユーザが、プリンタ１００がＷｉ－Ｆｉ接続を確立することを望む可能性は高い。一方、端末５０は、プリンタ１００のベンダとは異なる事業者によって提供される第２種のアプリ５２を備える。このため、端末５０のユーザが、プリンタ１００がＷｉ－Ｆｉ接続を確立することを望む可能性は低い。そして、ケースＥは、端末１０のユーザが、プリンタ１００とＡＰ６との間でＷｉ－Ｆｉ接続が確立されることを望んでおり、かつ、端末５０のユーザが、プリンタ１００とは異なるプリンタと、ＡＰ６とは異なるＡＰと、の間でＷｉ－Ｆｉ接続が確立されることを望んでいる状況を想定している。

【００９９】

ケースＥでは、まず、図１０のＴ６００～Ｔ６２２と同様の処理が端末１０及びプリンタ１００によって実行される。この結果、プリンタ１００は、端末１０のＭＡＣアドレス「ｘｘｘ」をメモリ１３４に記憶し（Ｔ６２０）、不可能状態から可能状態に移行する（Ｔ６２２）。

【０１００】

その後、端末１０からプリンタ１００にＡＲｅｑが送信される前（即ち図１０のＴ６５０の前）に、Ｔ８１０において、端末５０のユーザによって第２種のアプリ５２の起動操作が端末５０に実行され、Ｔ８１２において、第２種のアプリ５２が起動される。この結果、端末５０は、第２種のアプリ５２に従って、以下の各処理を実行する。なお、端末５０は、Ｔ８１０以降の処理を実行する前に、図２のＴ５～Ｔ１５と同様の処理を上記の異なるＡＰと実行済みである。

【０１０１】

Ｔ８１４では、端末５０は、ＳＲｅｑをプリンタ１００に送信する。ここで、第２種のアプリ５２は、プリンタ１００のベンダによって提供される第１種のアプリ４０とは異なり、端末５０のＭＡＣアドレス「ｙｙｙ」を含まないＳＲｅｑを送信する。従って、プリンタ１００において、端末５０のＭＡＣアドレス「ｙｙｙ」が記憶されない。

【０１０２】

プリンタ１００は、Ｔ８１４において、ＢＴＩ／Ｆ１１８を介して、端末５０からＳＲｅｑを受信する場合（図８のＳ５でＹＥＳ）に、Ｔ８１６において、端末５０とプリンタ１００との間の距離が比較的に小さいことに起因して、当該ＳＲｅｑの受信電波強度が閾値以上であると判断し（Ｓ１０でＹＥＳ）、当該ＳＲｅｑがＭＡＣアドレスを含まないと判断する（Ｓ２５でＮＯ）。

【０１０３】

Ｔ８３０～Ｔ８５０は、端末５０の公開鍵ＴＰＫ５、秘密鍵ｔｓｋ５、共有鍵ＳＫ５、ランダム値ＲＶ５、暗号化データＥＤ５、及び、ＭＡＣアドレス「ｙｙｙ」が利用される点を除いて、図１０のＴ６３０～Ｔ６５０と同様である。なお、第２種のアプリ５２は、端末側確認画面ＴＣＳを表示しない。従って、端末５０は、図１０のＴ６３２及びＴ６４０の処理を実行しない。

【０１０４】

Ｔ８５２では、プリンタ１００は、Ｔ８１６で記憶されたＭＡＣアドレス「ｘｘｘ」と、Ｔ８５０で受信されたＡＲｅｑ内のＭＡＣアドレス「ｙｙｙ」と、が一致しないと判断する（図９のＳ１０５でＮＯ）。この場合、プリンタ１００は、Ｔ８５２において、第２の指示画面ＳＩＳを表示部１１４に表示させる（Ｓ１１０）。そして、プリンタ１００は、Ｔ８５４において、画面ＳＩＳ内のＹＥＳボタンが所定時間内に選択されなかった（即ちタイムアウト）と判断し（図４のＳ１１５でＮＯ）、画面ＳＩＳの表示を終了して図１２の処理を終了する。

【０１０５】

仮に、プリンタ１００が、端末５０からＡＲｅｑを受信することに応じて（Ｔ８５０）、図４のＴ２０２以降の処理を自動的に実行してＡＲｅｓを端末５０に送信すると、プリンタ１００と上記の異なるＡＰとの間にＷｉ－Ｆｉ接続が確立され得る。即ち、端末５０のユーザによって意図されていない一対の装置（即ち、プリンタ１００及び上記の異なるＡＰ）の間にＷｉ－Ｆｉ接続が確立され得る。

【０１０６】

これに対し、ケースＥでは、プリンタ１００は、端末５０からＡＲｅｑを受信する場合（Ｔ８５０）に、メモリ１３４内の端末１０のＭＡＣアドレス「ｘｘｘ」とＡＲｅｑ内の端末５０のＭＡＣアドレス「ｙｙｙ」とが一致しないので、第２の指示画面ＳＩＳを表示部１１４に表示させることによって、ＡＲｅｓの送信を制限する（Ｔ８５２）。端末５０のユーザは、プリンタ１００がＷｉ－Ｆｉ接続が確立されることを望んでいないので、画面ＳＩＳ内のＹＥＳボタンを選択しない。この結果、プリンタ１００は、タイムアウトと判断し（Ｔ８５４）、ＡＲｅｓを端末５０に送信しない。従って、プリンタ１００と上記の異なるＡＰとの間にＷｉ－Ｆｉ接続が確立されるのを抑制することができる。即ち、端末５０のユーザによって意図されていない一対の装置の間にＷｉ－Ｆｉ接続が確立されるのを抑制することができる。なお、ケースＥにおいて、端末５０のユーザが、プリンタ１００と上記の異なるＡＰとの間にＷｉ－Ｆｉ接続が確立されることを望んでいる場合には、画面ＳＩＳ内のＹＥＳボタンがユーザによって選択される。この場合、図４のＴ２０２以降の処理が実行され、プリンタ１００と上記の異なるＡＰとの間にＷｉ－Ｆｉ接続が確立される。従って、ユーザの意図に応じたＷｉ－Ｆｉ接続を確立させることができる。

【０１０７】

（対応関係）

ＭＡＣアドレス「ｘｘｘ」、端末５０が、それぞれ、「識別情報」、「異なる外部装置」の一例である。図８のＳ５の処理、Ｓ１０の処理、Ｓ４０の処理、Ｓ１００の処理、図４のＴ２１０の処理、図５のＴ３１０の処理、図２のＴ３５及びＴ４０の処理が、それぞ

れ、「特定信号受信部」及び「識別情報受信部」、「判断部」、「公開鍵送信部」、「認証要求受信部」、「認証応答送信部」、「接続情報受信部」、「確立部」によって実行される処理の一例である。

【０１０８】

以上、本発明の具体例を詳細に説明したが、これらは例示にすぎず、特許請求の範囲を限定するものではない。特許請求の範囲に記載の技術には以上に例示した具体例を様々に変形、変更したものが含まれる。上記の実施例の変形例を以下に列挙する。

【０１０９】

（変形例１）共有鍵（例えばＳＫ１）を生成するための処理（例えば、図４のＴ１４２、Ｔ２０２）は、ＥＣＤＨに従った上記の実施例の処理に限らず、ＥＣＤＨに従った他の処理であってもよい。また、共有鍵を生成するための処理は、ＥＣＤＨに従った処理に限らず、他の方式（例えば、ＤＨ（Diffie-Hellman key exchangeの略）等）に従った処理が実行されてもよい。また、上記の実施例では、電子署名ＤＳ１及びＤＳ２が、ＥＣＤＳＡに従って生成されたが、他の方式（例えば、ＤＳＡ（Digital Signature Algorithmの略）、ＲＡＳ（Rivest-Shamir-Adleman cryptosystemの略）等）に従って生成されてもよい。

【０１１０】

（変形例２）図８のＳ２５、Ｓ３０、及び、図９のＳ１０５の処理が省略されてもよい。この場合、例えば、図１０のＴ６１４において、端末１０は、ＭＡＣアドレス「ｘｘｘ」を含まないＳＲｅｑをプリンタ１００に送信してもよい。本変形例では、「識別情報受信部」が省略可能である。

【０１１１】

（変形例３）図８のＳ１５及びＳ２０の処理が省略されてもよい。この場合、プリンタ１００は、Ｓ１０でＮＯと判断する場合に、非実行ＥＮＤとして図８の処理を終了する。本変形例では、Ｓ１０でＮＯの場合にＳＲｅｓを送信しないことが、「公開鍵の送信は制限される」の一例である。

【０１１２】

（変形例４）図９のＳ１１０及びＳ１１５の処理が省略されてもよい。この場合、プリンタ１００は、Ｓ１０５でＮＯと判断する場合に、非実行ＥＮＤとして図９の処理を終了する。本変形例では、Ｓ１０５でＮＯの場合にＡＲｅｓを送信しないことが、「認証応答の送信は制限される」の一例である。また、本変形例では、「第２の表示制御部」が省略可能である。

【０１１３】

（変形例５）例えば、図３のＴ１３０でプリンタ１００から送信されるＳＲｅｓは、チャネルリスト及びＭＡＣアドレス「ａｂｃ」を含まなくてもよい。即ち、当該ＳＲｅｓは、少なくとも公開鍵ＰＰＫ１を含めばよい。この場合、プリンタ１００は、Ｔ１２２で不可能状態から可能状態に移行することに応じて、プリンタ１００が利用可能な全ての無線チャネルのうちの１個の無線チャネルが利用されたＡＲｅｑを受信することを監視する。また、端末１０は、図４のＴ２００において、端末１０が利用可能な全ての無線チャネルを順次利用して、ＡＲｅｑをブロードキャストによって順次送信する。本変形例では、「チャネル情報送信部」が省略可能である。

【０１１４】

（変形例６）例えば、図３のＴ１１４において、プリンタ１００は、端末１０から、ＳＲｅｑとは異なる信号であって、ＢＴ方式に従った信号（例えば、Ａｄｖｅｒｔｉｓｅ信号）を受信することに応じて、Ｔ１１６において、第１の指示画面ＦＩＳを表示部１１４に表示させてもよい。本変形例では、当該異なる信号が、「特定信号」の一例である。また、この場合、プリンタ１００は、Ｔ１３０において、公開鍵ＰＰＫ１等を含む上記のＢＴ方式に従った信号（例えば、Ａｄｖｅｒｔｉｓｅ信号）を端末１０に送信してもよい。

【０１１５】

（変形例７）プリンタ１００は、図３のＴ１３０でＳＲｅｓを端末１０に送信した後に、

不可能状態から可能状態に移行してもよい。即ち、第１の外部装置から特定信号が受信された後に、不可能状態から可能状態に移行されればよい。

【０１１６】

（変形例８）例えば、図１０のＴ６１４のＳＲｅｑがＭＡＣアドレス「ｘｘｘ」を含まなくてもよい。この場合、端末１０は、Ｔ６３０において、プリンタ１００からＳＲｅｓを受信することに応じて、ＢＴＩ／Ｆ１８を介して、ＭＡＣアドレス「ｘｘｘ」をプリンタ１００に送信してもよい。この結果、プリンタ１００において、ＭＡＣアドレス「ｘｘｘ」がメモリ１３４に記憶される。本変形例では、「特定信号」は、「識別情報」を含まなくてもよい。

【０１１７】

（変形例９）プリンタ１００が、常に可能状態として動作してもよい。本変形例では、「状態移行部」が省略可能である。

【０１１８】

（変形例１０）プリンタ１００のＢＴＩ／Ｆ１１８が、常に設定モードとして動作してもよい。本変形例では、「モード移行部」が省略可能である。

【０１１９】

（変形例１１）図１０のＴ６１４において、端末１０は、ＢＴＩ／Ｆ１８を介して、ＭＡＣアドレス「ｘｘｘ」に代えて、端末１０のデバイス名を含むＳＲｅｑをプリンタ１００に送信してもよい。この場合、Ｔ６２０において、プリンタ１００は、ＳＲｅｑ内の端末のデバイス名をメモリ１３４に記憶する。また、図１０のＴ６５０では、プリンタ１００は、端末１０から、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＭＡＣアドレス「ｘｘｘ」に代えて、端末１０のデバイス名を含むＡＲｅｑを受信し、メモリ１３４に記憶済みのデバイス名とＡＲｅｑ内のデバイス名とが一致する場合に、図４のＴ２０２以降の処理を実行する。本変形例では、端末１０のデバイス名が、「識別情報」の一例である。一般的に言えば、「識別情報」は、「第１の外部装置」を識別する情報であればよい。

【０１２０】

（変形例１２）図２のＴ３５において、端末１０とプリンタ１００との間でＮＡの処理が実行されて、端末１０とプリンタ１００との間でＷｉ－Ｆｉ接続が確立されてもよい。即ち、「第２の外部装置」は、「第１の外部装置」と同じ装置であってもよい。

【０１２１】

（変形例１３）上記の実施例では、端末１０を利用して、プリンタ１００とＡＰ６との間のＷｉ－Ｆｉ接続が確立される。これに代えて、例えば、端末１０を利用して、ＷＦＤ方式のＧ／Ｏ（Group Ownerの略）として動作するプリンタ１００（即ち親局として動作するデバイス）と、他のデバイス（即ち子局として動作するデバイス）と、の間のＷｉ－Ｆｉ接続が確立されてもよい。即ち、「第２の外部装置」は、「親局装置」でなくてもよい。

【０１２２】

（変形例１４）プリンタ１００が、ＢＴＩ／Ｆ１１８に代えて、ＢＴ方式とは異なる無線通信方式（例えば、ＺｉｇＢｅｅ方式）に従った無線インターフェースを備えていてもよい。本変形例では、当該無線インターフェースが、「第１の無線インターフェース」の一例である。

【０１２３】

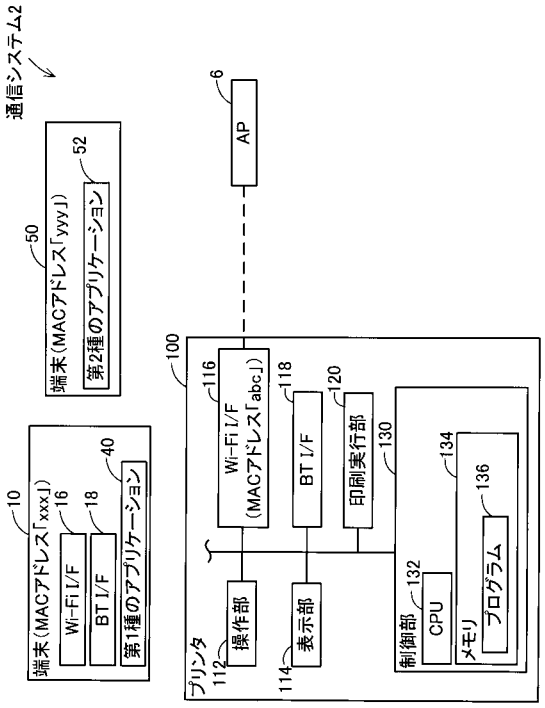
（変形例１５）Ｔ８５０において、端末５０は、ＭＡＣアドレス「ｙｙｙ」を含まないＡＲｅｑをプリンタ１００に送信してもよい。この場合、プリンタ１００は、端末５０から、Ｗｉ－ＦｉＩ／Ｆ１１６を介して、ＡＲｅｑを受信することに応じて、ＡＲｅｑ内にＭＡＣアドレスが含まれていないと判断して、第２の指示画面ＳＩＳを表示部１１４に表示させてもよい。

【０１２４】

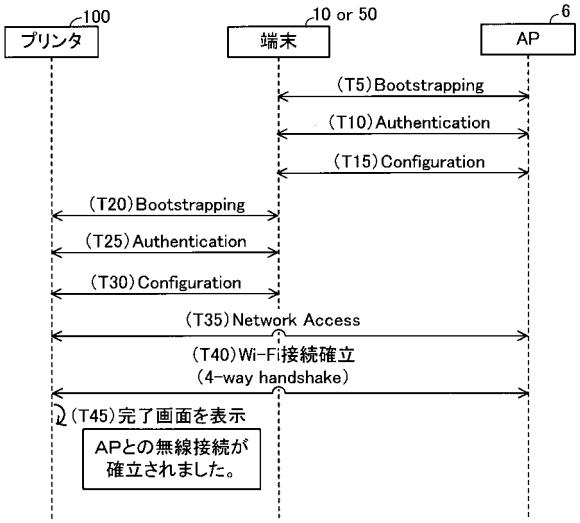
（変形例１６）「通信装置」は、プリンタでなくてもよく、スキャナ、多機能機、携帯端末、ＰＣ、サーバ等の他のデバイスであってもよい。

【０１２５】
（変形例１７）上記の各実施例では、図２～図１２の各処理がソフトウェア（即ちプログラム１３６）によって実現されるが、これらの各処理のうちの少なくとも１つが論理回路等のハードウェアによって実現されてもよい。
【０１２６】
また、本明細書または図面に説明した技術要素は、単独であるいは各種の組合せによって技術的有用性を発揮するものであり、出願時請求項記載の組合せに限定されるものではない。また、本明細書または図面に例示した技術は複数目的を同時に達成するものであり、そのうちの一つの目的を達成すること自体で技術的有用性を持つものである。
【符号の説明】
【０１２７】
２：通信システム、６：ＡＰ、１０，５０：端末、１６，１１６：Ｗｉ－ＦｉＩ／Ｆ、１８，１１８：ＢＴＩ／Ｆ、４０：第１種のアプリケーション、５２：第２種のアプリケーション、１００：プリンタ、１１２：操作部、１１４：表示部、１２０：印刷実行部、１３０：制御部、１３２：ＣＰＵ、１３４：メモリ、１３６：プログラム

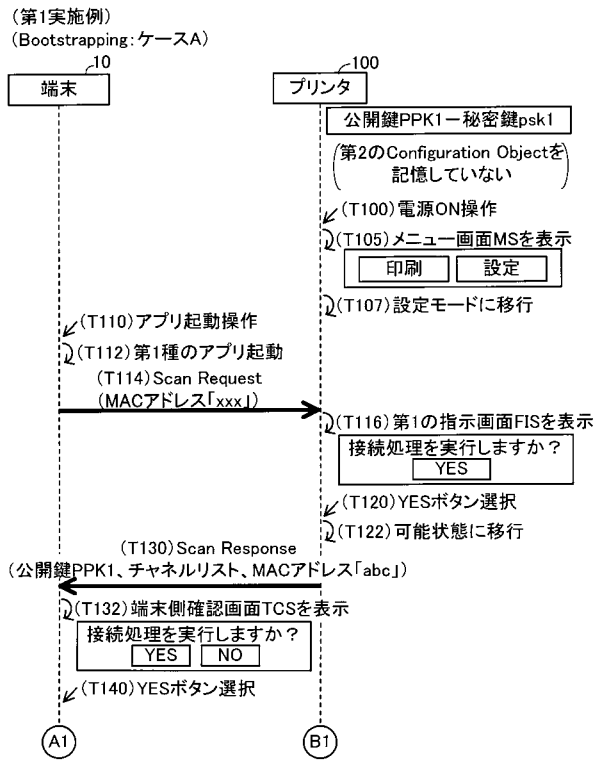
【図１】



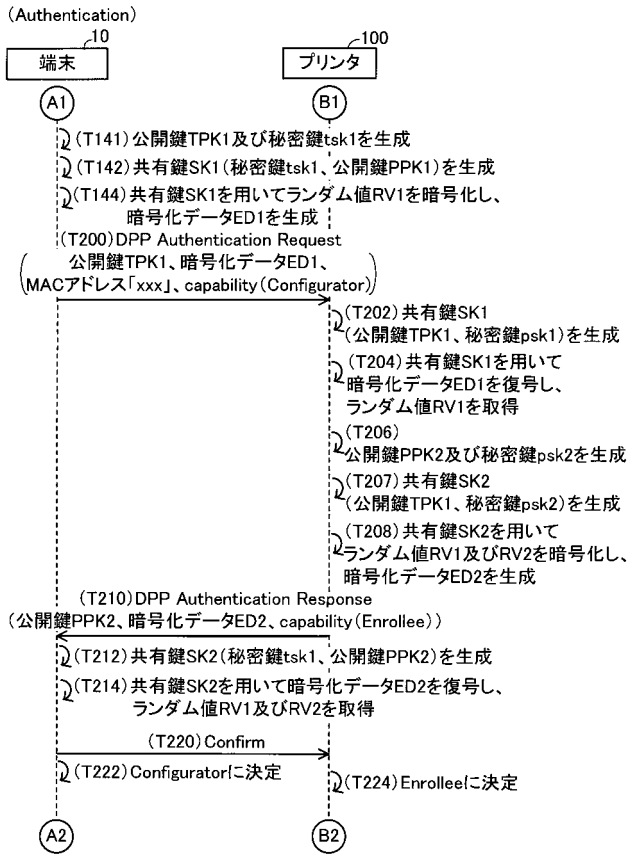
【図２】



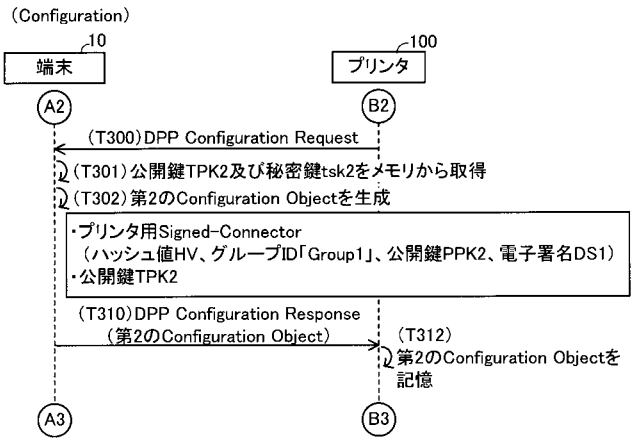
【図３】


(第1実施例)
(Bootstrapping:ケースA)
端末
10
プリンタ
100
公開鍵PPK1ー秘密鍵psk1
(第2のConfiguration Objectを記憶していない
(T100)電源ON操作
(T105)メニュー画面MSを表示
印刷
設定
(T107)設定モードに移行
(T110)アプリ起動操作
(T112)第1種のアプリ起動
(T114)Scan Request
(MACアドレス「xxx」)
(T116)第1の指示画面FISを表示
接続処理を実行しますか？
YES
(T120)YESボタン選択
(T122)可能状態に移行
(T130)Scan Response
(公開鍵PPK1、チャネルリスト、MACアドレス「abc」)
(T132)端末側確認画面TCSを表示
接続処理を実行しますか？
YES
NO
(T140)YESボタン選択
A1
B1

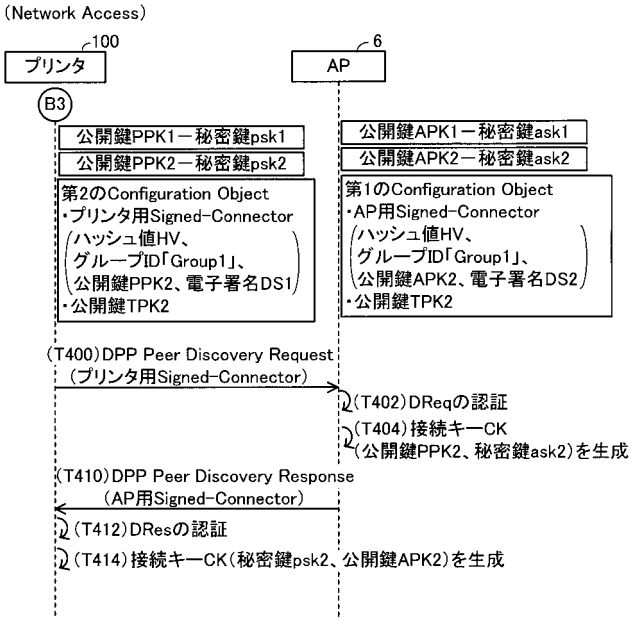
【図４】


(Authentication)
端末
10
プリンタ
100
A1
B1
(T141)公開鍵TPK1及び秘密鍵tsk1を生成
(T142)共有鍵SK1(秘密鍵tsk1、公開鍵PPK1)を生成
(T144)共有鍵SK1を用いてランダム値RV1を暗号化し、暗号化データED1を生成
(T200)DPP Authentication Request
公開鍵TPK1、暗号化データED1、
MACアドレス「xxx」、capability(Configurator)
(T202)共有鍵SK1
(公開鍵TPK1、秘密鍵psk1)を生成
(T204)共有鍵SK1を用いて暗号化データED1を復号し、ランダム値RV1を取得
(T206)
公開鍵PPK2及び秘密鍵psk2を生成
(T207)共有鍵SK2
(公開鍵TPK1、秘密鍵psk2)を生成
(T208)共有鍵SK2を用いてランダム値RV1及びRV2を暗号化し、暗号化データED2を生成
(T210)DPP Authentication Response
(公開鍵PPK2、暗号化データED2、capability(Enrollee))
(T212)共有鍵SK2(秘密鍵tsk1、公開鍵PPK2)を生成
(T214)共有鍵SK2を用いて暗号化データED2を復号し、ランダム値RV1及びRV2を取得
(T220)Confirm
(T222)Configuratorに決定
(T224)Enrolleeに決定
A2
B2

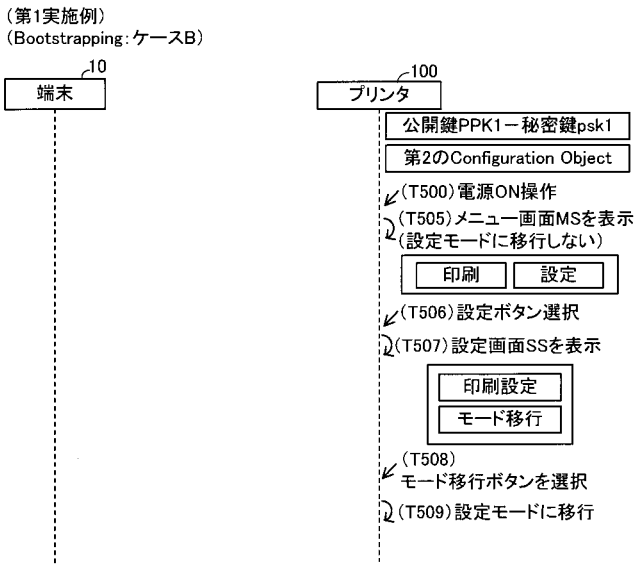
【図５】


(Configuration)
端末
10
プリンタ
100
A2
B2
(T300)DPP Configuration Request
(T301)公開鍵TPK2及び秘密鍵tsk2をメモリから取得
(T302)第2のConfiguration Objectを生成
・プリンタ用Signed-Connector
(ハッシュ値HV、グループID「Group1」、公開鍵PPK2、電子署名DS1)
・公開鍵TPK2
(T310)DPP Configuration Response
(第2のConfiguration Object)
(T312)
第2のConfiguration Objectを記憶
A3
B3

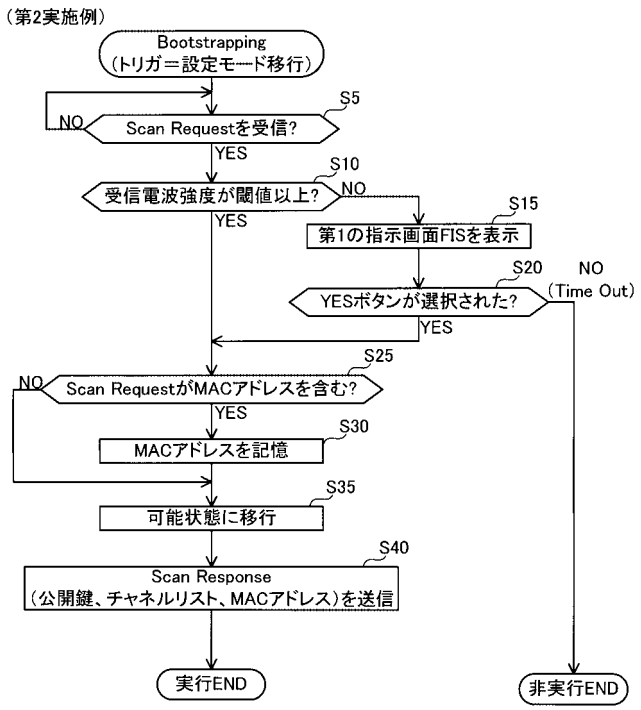
【図６】


(Network Access)
プリンタ
100
AP
6
B3
公開鍵PPK1ー秘密鍵psk1
公開鍵PPK2ー秘密鍵psk2
第2のConfiguration Object
・プリンタ用Signed-Connector
(ハッシュ値HV、
グループID「Group1」、
公開鍵PPK2、電子署名DS1)
・公開鍵TPK2
公開鍵APK1ー秘密鍵ask1
公開鍵APK2ー秘密鍵ask2
第1のConfiguration Object
・AP用Signed-Connector
(ハッシュ値HV、
グループID「Group1」、
公開鍵APK2、電子署名DS2)
・公開鍵TPK2
(T400)DPP Peer Discovery Request
(プリンタ用Signed-Connector)
(T402)DReqの認証
(T404)接続キーCK
(公開鍵PPK2、秘密鍵ask2)を生成
(T410)DPP Peer Discovery Response
(AP用Signed-Connector)
(T412)DResの認証
(T414)接続キーCK(秘密鍵psk2、公開鍵APK2)を生成

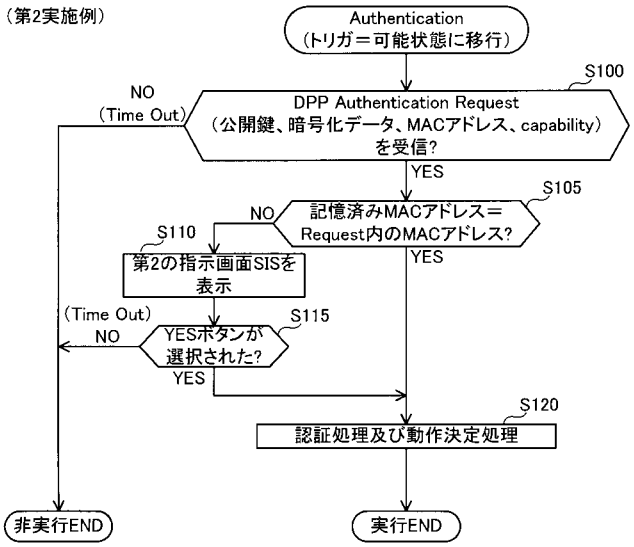
【図７】


(第1実施例)
(Bootstrapping：ケースB)
10
端末
100
プリンタ
公開鍵PPK1－秘密鍵psk1
第2のConfiguration Object
(T500)電源ON操作
(T505)メニュー画面MSを表示
(設定モードに移行しない)
印刷
設定
(T506)設定ボタン選択
(T507)設定画面SSを表示
印刷設定
モード移行
(T508)
モード移行ボタンを選択
(T509)設定モードに移行

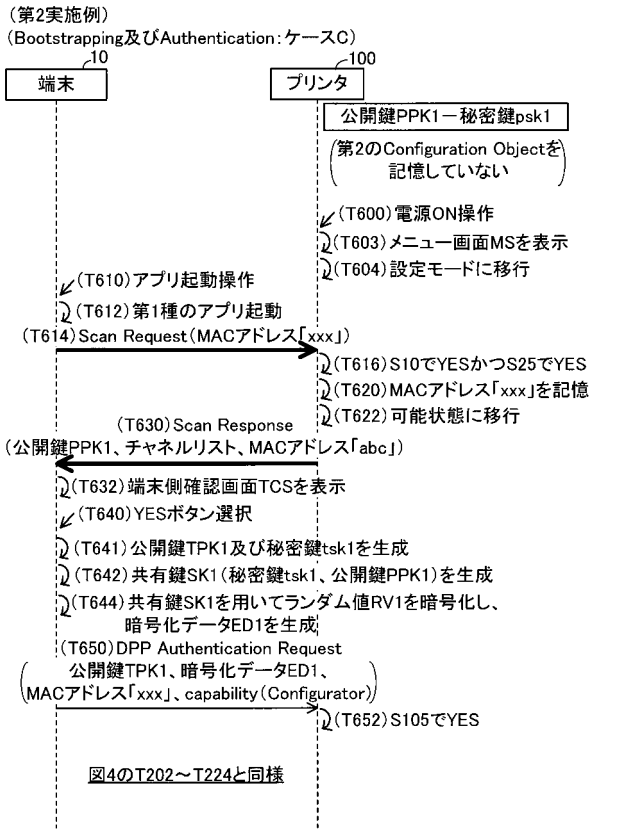
【図８】


(第2実施例)
Bootstrapping
(トリガ＝設定モード移行)
S5
NO
Scan Requestを受信?
YES
S10
受信電波強度が閾値以上?
NO
YES
S15
第1の指示画面FISを表示
S20
NO
(Time Out)
YESボタンが選択された?
YES
S25
NO
Scan RequestがMACアドレスを含む?
YES
S30
MACアドレスを記憶
S35
可能状態に移行
S40
Scan Response
(公開鍵、チャネルリスト、MACアドレス)を送信
実行END
非実行END

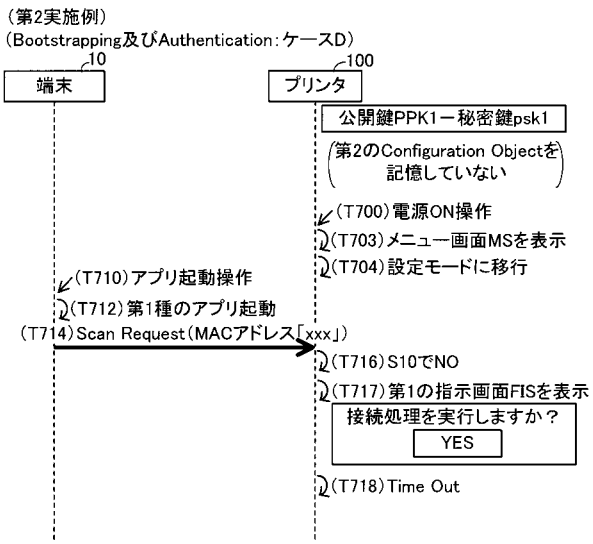
【図９】


(第2実施例)
Authentication
(トリガ＝可能状態に移行)
S100
NO
(Time Out)
DPP Authentication Request
(公開鍵、暗号化データ、MACアドレス、capability)
を受信?
YES
S105
NO
記憶済みMACアドレス＝
Request内のMACアドレス?
YES
S110
第2の指示画面SISを
表示
(Time Out)
S115
NO
YESボタンが
選択された?
YES
S120
認証処理及び動作決定処理
非実行END
実行END

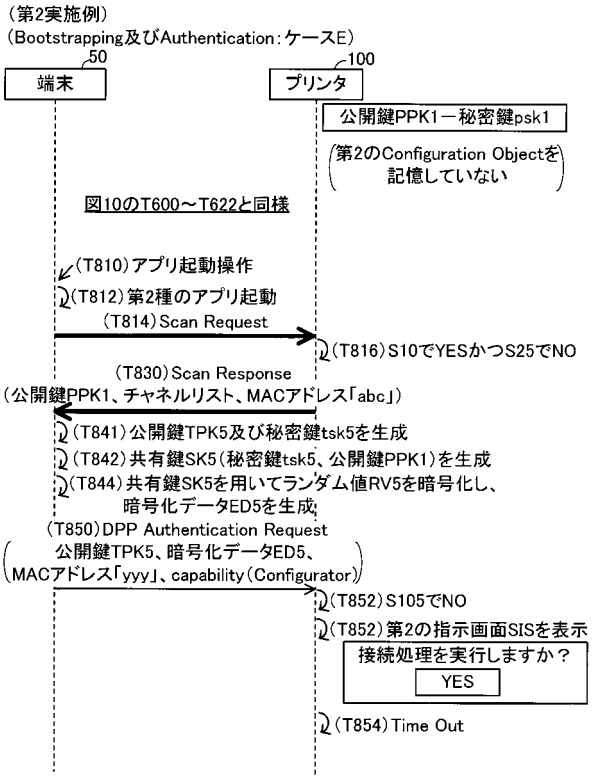
【図１０】


(第2実施例)
(Bootstrapping及びAuthentication：ケースC)
10
端末
100
プリンタ
公開鍵PPK1－秘密鍵psk1
(第2のConfiguration Objectを
記憶していない
(T600)電源ON操作
(T603)メニュー画面MSを表示
(T604)設定モードに移行
(T610)アプリ起動操作
(T612)第1種のアプリ起動
(T614)Scan Request(MACアドレス「xxx」)
(T616)S10でYESかつS25でYES
(T620)MACアドレス「xxx」を記憶
(T622)可能状態に移行
(T630)Scan Response
(公開鍵PPK1、チャネルリスト、MACアドレス「abc」)
(T632)端末側確認画面TCSを表示
(T640)YESボタン選択
(T641)公開鍵TPK1及び秘密鍵tsk1を生成
(T642)共有鍵SK1(秘密鍵tsk1、公開鍵PPK1)を生成
(T644)共有鍵SK1を用いてランダム値RV1を暗号化し、
暗号化データED1を生成
(T650)DPP Authentication Request
公開鍵TPK1、暗号化データED1、
MACアドレス「xxx」、capability(Configurator)
(T652)S105でYES
図4のT202～T224と同様

【図１１】


(第2実施例)
(Bootstrapping及びAuthentication:ケースD)
10
端末
100
プリンタ
公開鍵PPK1ー秘密鍵psk1
(第2のConfiguration Objectを記憶していない
(T700)電源ON操作
(T703)メニュー画面MSを表示
(T704)設定モードに移行
(T710)アプリ起動操作
(T712)第1種のアプリ起動
(T714)Scan Request(MACアドレス「xxx」)
(T716)S10でNO
(T717)第1の指示画面FISを表示
接続処理を実行しますか？
YES
(T718)Time Out

【図１２】


(第2実施例)
(Bootstrapping及びAuthentication:ケースE)
50
端末
100
プリンタ
公開鍵PPK1ー秘密鍵psk1
(第2のConfiguration Objectを記憶していない
図10のT600～T622と同様
(T810)アプリ起動操作
(T812)第2種のアプリ起動
(T814)Scan Request
(T816)S10でYESかつS25でNO
(T830)Scan Response
(公開鍵PPK1、チャネルリスト、MACアドレス「abc」)
(T841)公開鍵TPK5及び秘密鍵tsk5を生成
(T842)共有鍵SK5(秘密鍵tsk5、公開鍵PPK1)を生成
(T844)共有鍵SK5を用いてランダム値RV5を暗号化し、暗号化データED5を生成
(T850)DPP Authentication Request
公開鍵TPK5、暗号化データED5、
MACアドレス「yyy」、capability(Configurator)
(T852)S105でNO
(T852)第2の指示画面SISを表示
接続処理を実行しますか？
YES
(T854)Time Out