(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2006-129083
(P2006-129083A)
(43)公開日　平成18年5月18日(2006.5.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	303	5K033
H04Q 7/38	(2006.01)	H04B	7/26	109R	5K067

審査請求 未請求　請求項の数 19　ＯＬ　（全 22 頁）

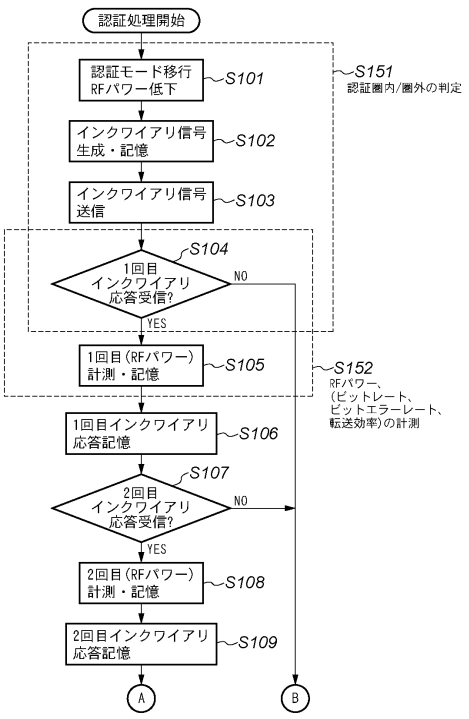
(21)出願番号　特願2004-314723 (P2004-314723)
(22)出願日　平成16年10月28日 (2004.10.28)

(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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　替地　修也
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

最終頁に続く

(54)【発明の名称】無線通信装置の接続対象検出及び認証方法

(57)【要約】
【課題】　操作者にかかる作業を簡便なものとし、且つ、それぞれの装置が単一の無線通信手段を利用しながらも、二者間の認証処理を行えるようになる。
【解決手段】　認証開始指示ボタンが操作されると、ホスト装置は、自身のＲＦパワーを下げ、通信可能距離を数十センチメートル程度にする（Ｓ１０１）。そして、ホストは、照合データと時間間隔データを内包するインクワイアリ信号を発信する（Ｓ１０３）。このインクワイアリ信号を受信できたデバイスは、照合データと自身を特定する情報を内包したインクワイアリ応答信号を、指示された時間間隔で送信する。ホストは、このインクワイアリ応答が設定された時間間隔で受信され（Ｓ１１０）、照合データを含み（Ｓ１１１）、受信信号強度が所定範囲の変化があり（Ｓ１１３）、尚且つ、インクワイアリ応答が唯一のデバイスからものである場合（Ｓ１１４）に限って、認証情報を送信する（Ｓ１１６）。
【選択図】　図１０Ａ



【特許請求の範囲】
【請求項１】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証手段と
を備えることを特徴とする無線通信装置。
【請求項２】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段により、応答時間隔データを含む探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから前記応答時間間隔で応答信号を受信した場合、前記無線通信デバイスに認証情報を送信する認証手段と
を備えることを特徴とする無線通信装置。
【請求項３】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、
前記無線通信手段で受信する信号強度を検出する検出手段と、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段により、所定探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから複数回の応答信号を受信し、且つ、各応答信号の受信強度差の絶対値が所定閾値Ｔ１より大きく、所定閾値Ｔ２未満（Ｔ２＞Ｔ１＞０）の場合、前記無線通信デバイスに認証情報を送信する認証手段と
を備えることを特徴とする無線通信装置。
【請求項４】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、
該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信した場合、当該無線通信デバイスに認証情報を送信する認証手段と
を備えることを特徴とする無線通信装置。
【請求項５】
可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置であって、
認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信手段と、
前記無線通信手段で受信する信号強度を検出する検出手段と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出手段で検出した各応答信号の受信強度差の絶対値が所定閾値Ｔ１より大きく以上、所定閾値Ｔ２未満（Ｔ２＞Ｔ１＞０）の場合、前記無線通信デバイスに認証情報を送信する認証手段と
を備えることを特徴とする無線通信装置。

【請求項６】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、探索信号を前記無線通信手段で受信する第１の受信手段と、
受信した探索情報中に含まれる照合データを含む応答信号を前記無線通信手段を介して送信する送信手段と、
該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信手段とを備え、
前記第２の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器。

【請求項７】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、
該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第１の受信手段と、
該第１の受信手段の受信に応じて応答信号を前記無線通信手段を介して送信する送信手段と、
該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信手段とを備え、
前記第２の受信手段で認証情報を受信した場合、これ以降は認証情報に基づいて前記無線通信装置と通信することを特徴とする電子機器。

【請求項８】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、
該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第１の受信手段と、
受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信手段と、
該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信手段とを備え、
前記第２の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器。

【請求項９】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法の制御方法であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信工程と、
該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証工程と
を備えることを特徴とする無線通信装置の制御方法。
【請求項１０】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段により、応答時間隔データを含む探索信号を発信する発信工程と、
該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから前記応答時間間隔で応答信号を受信した場合、前記無線通信デバイスに認証情報を送信する認証工程と
を備えることを特徴とする無線通信装置の制御方法。
【請求項１１】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、
前記無線通信手段で受信する信号強度を検出する検出工程と、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段により、所定探索信号を発信する発信工程と、
該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから複数回の応答信号を受信し、且つ、各応答信号の受信強度差の絶対値が所定閾値Ｔ１より大きく、所定閾値Ｔ２未満（Ｔ２＞Ｔ１＞０）の場合、前記無線通信デバイスに認証情報を送信する認証工程と
を備えることを特徴とする無線通信装置の制御方法。
【請求項１２】
可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、
該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を発信する発信工程と、
該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信した場合、当該無線通信デバイスに認証情報を送信する認証工程と
を備えることを特徴とする無線通信装置の制御方法。
【請求項１３】
可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置の制御方法であって、
所定の無線通信手段に対し、認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信切り換え工程と、

前記無線通信手段で受信する信号強度を検出する検出工程と、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信工程と、
該発信工程で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出工程で検出した各応答信号の受信強度差の絶対値が所定閾値Ｔ１より大きく以上、所定閾値Ｔ２未満（Ｔ２＞Ｔ１＞０）の場合、前記無線通信デバイスに認証情報を送信する認証工程と
を備えることを特徴とする無線通信装置の制御方法。

【請求項１４】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、探索信号を前記無線通信手段で受信する第１の受信工程と、
受信した探索情報中に含まれる照合データを含む応答信号を前記無線通信手段を介して送信する送信工程と、
該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信工程とを備え、
前記第２の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器の制御方法。

【請求項１５】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、
該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第１の受信工程と、
該第１の受信工程の受信に応じて応答信号を前記無線通信手段を介して送信する送信工程と、
該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信工程とを備え、
前記第２の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器の制御方法。

【請求項１６】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、
該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、
該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第１の受信工程と、
受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信工程と、
該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信工程とを備え、
前記第２の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無

線通信装置と通信することを特徴とする電子機器の制御方法。
【請求項１７】
可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置用のコンピュータプログラムであって、
認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信手段と、
前記無線通信手段で受信する信号強度を検出する検出手段と、
無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信手段と、
該発信手段で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出手段で検出した各応答信号の受信強度差の絶対値が所定閾値Ｔ１より大きく以上、所定閾値Ｔ２未満（Ｔ２＞Ｔ１＞０）の場合、前記無線通信デバイスに認証情報を送信する認証手段
として機能することを特徴とするコンピュータプログラム。
【請求項１８】
所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器用のコンピュータプログラムであって、
前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、
該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、
該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第１の受信手段と、
受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信手段と、
該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第２の受信手段
として機能し、前記第２の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とするコンピュータプログラム。
【請求項１９】
請求項１７または請求項１８に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は無線通信装置間で通信パラメータ及びアドレス識別子等の認証情報を交換する際の、無線通信装置の接続対象検出及び認証方法に関するものである。
【背景技術】
【０００２】
近年、携帯電話、ＰＤＡ(Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ)などの情報端末、パーソナルコンピュータ、及びプリンタに代表されるパーソナルコンピュータの周辺機器等、多種多様な情報機器のデータ通信や制御において、無線通信接続の利用が急増している。この無線通信接続の無線通信システムでは、公衆回線網だけに留まらず、Ｂｌｕｅｔｏｏｔｈ（Ｒ）や、ワイヤレスＬＡＮ（Ｗｉｒｅｌｅｓｓ　ＬＡＮ）等のローカルな回線も利用されている。
【０００３】
前記した情報機器以外にも、デジタルカメラ等の撮像装置、家電製品、及びアクセサリー等、様々な機器に無線通信機能が搭載されつつあり、さらに有線通信接続方法として広

く普及しているＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）の無線化も進められている。

【０００４】

無線通信装置で無線データ通信を行う際には、不特定の装置や意図しない装置と接続されないようにするために、認証という手続きをとることが多い。この認証に際しては、ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）コードやＥＳＳＩＤ（Ｅｘｔｅｎｄｅｄ　Ｓｅｒｖｉｃｅ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）等を認証情報の一つとして無線通信装置間で交換し、認証情報交換した特定の２つの無線通信装置が、この認証情報で１対１の関連付けを行うことで、無線通信の認証セキュリティを確保している。

【０００５】

この認証情報は、第三者に開示されてはならないものであり、この認証情報が第三者に漏洩した場合、この漏洩した認証情報を用いることによって、第三者が、装置内に格納されている書類、住所録、電子メール、個人情報、及び画像データ等にアクセスする恐れがある。また、無線通信システムや課金システム、プリントシステムが第三者によって不正利用される恐れもある。このような状況の中、これら無線通信装置のセキュリティ対策が注目されている。

【０００６】

無線通信装置を相互に認証させる認証情報の入力方法は幾つかある。具体的には、使用者が手動で入力する方法、ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｆｙ　Ｍｏｄｕｌｅ）カードを機器に挿入する方法、赤外線通信を利用して認証を行う方法、及び接続ケーブルを利用して認証を行う方法、装置内に二つの無線通信手段を持ち、片方の無線通信手段で認証を行う方法等がある。通信パラメータ及びアドレス識別子等の認証情報は、無線通信装置相互の認証が終了した後に、無線通信装置相互の記憶部に格納され、データ通信時には、格納された認証情報を用いて無線データ通信路の確保を行う。

【０００７】

セキュリティ対策を行って無線通信装置の認証を行う方法としては、２つの通信装置の間で無線通信を行う場合に、第１の装置を第２の装置のドッキングポートに部分的に係合した時点で（第１の通信手段）、第１の装置と第２の装置が自動的に第２の通信手段により接続を行い、アドレス識別子交換を行う提案がある（特許文献１）。これによると、十分に近い範囲にない通信装置にはアドレス識別子及び暗号キーの開示は行われず、セキュリティの向上が期待できる。

【０００８】

また、無線通信が可能な第１通信部と前記第１通信部とは異なる第２通信部とを有する第１通信機器と第２通信機器が、互いの第２通信部を接続すると２つの機器の間で無線通信を行うための通信パラメータを決定し、ユーザによる無線通信に必要な通信パラメータの設定を不要にする提案もある（特許文献２）。

【特許文献１】特許第３４２２６８３号公報

【特許文献２】特開２００２－３５９６２３公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

特定の２つの無線通信装置を関連付けする認証情報は、そのワード長がランダムで長いほどセキュリティの強度が高いが、使用者が手動で入力する場合は、使用者に面倒な操作をさせことになる。このため、使用者が手動で入力する認証情報は、ワード長が短く、第三者が推測しやすいコードとなることが多い。赤外線通信で認証を行う方法は、使用者に面倒な操作をさせことになり、狭すぎる指向性にも気を遣わせる不便がある。接続ケーブルで認証を行う方法も装置を互いに有線接続する必要があり、これも面倒である。

【００１０】

また、前記従来例では、無線通信装置はデータ通信前に有線接続またはドッキングポー

トに結合しなければ、通信パラメータ及びアドレス識別子等の認証情報の交換が出来ないため、使用者に面倒な操作をさせるばかりでなく、認証処理と、データ通信とにおいて各々別の無線通信手段を用いなければならず、無線通信装置の簡素化、省電力化及び小型化の妨げとなっている。

【００１１】

このように、無線通信装置の認証方法として、通信パラメータ及びアドレス識別子等の認証情報を簡便に設定し、使用者にとって使い勝手の良いシステム（無線通信システム、プリントシステム）を提供できていないという問題点があった。

【００１２】

本発明は、操作者にかかる作業を簡便なものとし、且つ、単一の無線通信手段を利用しながらも、２つの無線通信装置間の認証処理を行える技術を提供しようとするものである。

【課題を解決するための手段】

【００１３】

この課題を解決するため、例えば本発明の無線通信装置は以下の構成を備える。すなわち、

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証手段とを備える。

【発明の効果】

【００１４】

本発明によれば、操作者にかかる作業を簡便なものとし、且つ、それぞれの装置が単一の無線通信手段を利用しながらも、二者間の認証処理を行えるようになる。

【発明を実施するための最良の形態】

【００１５】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【００１６】

図１は、本発明の実施の形態に係る無線通信ホスト装置であるプリンタ装置１（以下、ホスト１）のブロック構成図である。

【００１７】

同図において、１０１はホスト１全体の制御を司るＣＰＵであり、１０２はＣＰＵ１０１のワークエリアとして使用されるＲＡＭである。１０３はＣＰＵ１０１の処理手順を記憶しているＲＯＭである。ただし、ＲＯＭは書き換えが可能な不揮発性メモリ、例えばフラッシュメモリで構成される。１０４は画像処理部であり、デジタル画像データ等をプリント可能なデジタルデータに変換するのに用いられる。１０５は各種表示を行うための表示制御部である。１０６は液晶表示器であり、デジタル画像データの確認や各種設定を行う際のメニューを表示するために使用される。１０７は発光ダイオードであり、ホスト１の処理状態を示すインジケーターとして使用される。１０８は外部記憶装置の制御部であり、メモリソケット１０９に挿入されたコンパクトフラッシュ（登録商標）やメモリースティック（登録商標）等の記憶媒体に記憶されているデジタルデータの読み込み及び、記憶媒体へのデジタルデータの書き出しの制御を行う。１１０はＵＳＢインターフェースの制御部であり、ＵＳＢコネクタ１１１で他のＵＳＢインターフェースを持つ装置と接続される。１１２は暗号処理部であり、認証情報や無線データ通信の暗号化を行うために使用される。１１３はリアルタイムクロックであり、認証期間カウントやアクセス時間記録を行うために使用される。１２０は無線通信を行うための無線通信部、１２１は無線通信を

行うためのアンテナである。１１４は各種操作を行うボタン等の制御部であり、操作キー１１５、認証処理開始を指示する操作ボタン１１６、リセットボタン１１７の操作情報をＣＰＵ１０１へ伝えるために使用される。１１８はホスト１のプリンタ機能の制御部であり、プリンタエンジン１１９でデジタルデータのプリントを行う。

【００１８】

図２は、本発明の実施の形態に係る無線通信デバイス装置の代表、すなわち、携帯もしくは可搬性の装置の代表としてのデジタルスチルカメラ２（以下、デバイス２）のブロック構成図である。

【００１９】

同図において、２０１はデバイス全体の制御を司るＣＰＵであり、２０２はＣＰＵ２０１のワークエリアとして使用されるＲＡＭである。２０３はＣＰＵ２０１の処理手順を記憶しているＲＯＭである。ただし、ＲＯＭは書き換えが可能な不揮発性メモリ、例えばフラッシュメモリで構成される。２０４は画像処理部であり、撮像された画像をデジタル画像データに変換するのに用いられる。２０５は各種表示の制御部である。２０６は液晶表示器であり、撮像した画像の確認及び各種設定を行う際のメニューを表示するために使用される。２０７は発光ダイオードであり、デバイス２の処理状態を示すインジケーターとして使用される。２０８は外部記憶装置の制御部であり、メモリソケット２０９に挿入されたコンパクトフラッシュ（登録商標）（Ｒ）やメモリースティック（Ｒ）等の記憶媒体へのデジタルデータの書き出し及び、記憶媒体に記憶されているデジタルデータの読み込みの制御を行う。２１０はＵＳＢインターフェースの制御部であり、ＵＳＢコネクタ２１１で他のＵＳＢインターフェースを持つ装置と接続される。２１２は暗号処理部であり、認証情報や無線データ通信の暗号化を行うために使用される。２１３はリアルタイムクロックであり、認証期間カウントやアクセス時間記録を行うために使用される。２２２は無線通信を行うための無線通信部、２２３は無線通信を行うためのアンテナである。２１４は各種操作を行うボタン等の制御部であり、操作キー２１５、認証処理開始を指示する操作ボタン２１６、リセットボタン２１７の操作情報をＣＰＵ２０１へ伝えるために使用される。２１８はデバイス２の撮像素子の制御部であり、ＣＣＤ２１９の制御を行う。２２０は光学ユニットの制御部であり、主としてレンズ及びその駆動系で構成される光学ユニット２２１の制御を行う。

【００２０】

図３は、本実施形態に係る無線通信ホスト装置（実施形態ではプリンタ装置）１における無線通信部１２０のブロック構成図である。

【００２１】

なお、デバイス装置（実施形態ではデジタルカメラ）２における無線通信部２２２も同様な構成であるものとし、デジタルカメラにおける無線通信部２２２の説明は省略する。また、実施形態では、説明を簡単なものとするため、ＩＥＥＥ８０２．１１ｂのアドホックモードを前提にして説明するが、他の無線通信規格でも構わない。

【００２２】

図中、３０３は無線通信部の全体の制御を司る制御部であり、ＣＰＵや不揮発性メモリが内蔵されているものとする。３０４は通信プロトコルのリンク管理部、３０５は無線のベースバンド部であり、ＲＦ部３０６とアンテナ１２１で電波の送受信を行う。３０７はＲＦパワー制御部であり、電波の送受信パワーの制御を行う。３０８はＲＦパワー計測部であり、電波の送受信パワーの計測を行う。

【００２３】

以上、実施形態におけるホスト１及び、デバイス２の構成を説明した。

【００２４】

次に、上記構成に基づいて、ホスト１とデバイス２とを相互に認識し、無線通信接続に必要な通信パラメータ及びアドレス識別子等の認証情報を簡便に設定する方法を説明する。

【００２５】

図４は、それぞれ、無線通信ホスト装置であるプリンタ装置１（以下、ホスト１、総称してホストとする）と、無線通信デバイス装置であるデジタルスチルカメラ２、携帯電話３、ＰＤＡ４（以下、デバイス２、デバイス３、デバイス４、総称してデバイスとする）との認証前の状態の一例を示した図である。

【００２６】

デバイス２、３、４には、図３に示した無線通信部１２０と無線通信に用いられるアンテナ１２１と同様の構成を備えるものとする。ホストとデバイスは、この無線通信部を用いて認証情報の交換、無線データ通信路の確立及び無線データ通信を行う。

【００２７】

ここで、ホスト１と、デバイス２との間で認証を行う場合の動作の一例を簡単に説明する。

【００２８】

まず、ホスト側の認証処理を開始するために、ホスト１のボタン１１６を押下すると、ホスト１は認証モードへ移行し、通常の無線データ通信（印刷データの受信処理）よりもＲＦパワーを低下させて、ホスト１の認証圏３５１を、例えば数十センチメートルに制限する。同様にデバイス側の認証処理を開始するために、デバイス２の操作キー２１５を操作してデバイス２を認証モードへ移行すると、デバイス２は無線データ通信中よりもＲＦパワーを低下させて、デバイス２の認証圏３５２を、例えば数十センチメートルに制限する。

【００２９】

図４に示すように、ホスト１と、デバイス２、デバイス３、及びデバイス４とは、互いの認証を行わない距離、すなわち認証時のホスト１の認証圏３５１外、及びデバイス２の認証圏３５２外に置かれているため、この状態でホスト１が認証可能なデバイスを探索しても、デバイス２を発見する事ができず、認証は行われない。

【００３０】

次に、図５に示すように、ホスト１と、デバイス２を共に認証モードへ移行させた後、認証圏３５２をもつデバイス２をホスト１の認証圏３５１内に近づけると、ホスト１とデバイス２は、互いの無線通信部１２０及び２２２とアンテナ１２１及び２２３を用いて相互を検出、認識し、無線通信接続に必要な通信パラメータ及びアドレス識別子等の認証情報を交換する。なお、デバイス３と、デバイス４とは、認証モードに移行したとしても、ホスト１の認証圏３５１外であるため、相互の検出と認識及び認証情報の交換は行われない。

【００３１】

図６は、認証モードへ移行したホスト１とデバイス２の、認証処理中の動作と液晶表示器の表示の一例を示した図である。まずは、認証モードへ移行したホスト１の動作の説明をする。

【００３２】

認証モードへの移行指示を行うと、ホスト１は、無線データ通信中よりもＲＦパワーを低下させて、ホスト１の認証圏３５１を、通常の無線通信の通信圏と比較し、十分に狭い範囲（例えば数十センチメートルの範囲）に制限する。認証モードへ移行したホスト１はその液晶表示器１０６に無線接続対象とするデバイスをホスト１に接近させるように指示を表示する。このとき、液晶表示器１０６に表示する内容は文字列、アイコン及びホスト１に登録済みの実写画像等を用いると良い。なお、液晶表示器１０６での表示のほかに、発光ダイオード１０７の点灯及び点滅によるインジケーターで、ホスト１が認証処理中であることを明示しても良い。

【００３３】

次に、認証モードへ移行したデバイス２の動作の説明をする。認証モードへの移行を指示すると、デバイス２は、無線データ通信中よりもＲＦパワーを低下させて、デバイス２の認証圏３５２を、ホスト１と同様に十分に狭い範囲（例えば数十センチメートル）に制限する。認証モードへ移行したデバイス２はその液晶表示器２０６に無線接続対象とする

ホストへデバイス２を接近させるように指示を表示する。このとき、液晶表示器２０６に表示する内容は文字列、アイコン及びデバイス２に登録済みの実写画像等を用いると良い。なお、液晶表示器２０６での表示のほかに、発光ダイオード２０７の点灯及び点滅によるインジケーターで、デバイス２が認証処理中であることを明示しても良い。

【００３４】

本実施形態は、ホストとデバイスの装置間距離や指向性によるＲＦパワーの変位を利用して、本当に無線データ通信を行いたい相手装置（以下、真の接続対象とする）を検出、識別することを特徴とする。ここで、本実施形態として、ホストとデバイスとのＲＦパワーが、装置間距離や指向性でどのように変位するかを図７及び図８で説明する。

【００３５】

図７（ａ）、（ｂ）は、認証処理中のホスト１と、真の接続対象とするデバイス２（以下、真のデバイス）のＲＦパワーと装置間距離特性を示す図である。認証モードに移行した真のデバイスをホストに接近させるように位置７０１から位置７０２に移動すると、図７（ｂ）のグラフに示すようにホストの受信するＲＦパワー７０３は符号７０４から符号７０５へ変位する。このＲＦパワーの変位をホストのＲＦパワー計測部３０８で計測し、真のデバイスかどうかを判定する。逆に、認証モードに移行した真のデバイスをホストから遠ざけるように位置７０２から位置７０１に移動してもＲＦパワー７０３は変化するため、この変位をホストのＲＦパワー計測部３０８で計測し、真のデバイスかどうかを判定しても良い。また、ホスト及びデバイスのアンテナ構成により、図７（ｂ）のグラフに示すように、ホストとデバイスを接近させると、ホストの受信するＲＦパワー７０６が符号７０７から符号７０８へ低下する場合においても、上記例のように、ＲＦパワーの変位をホストのＲＦパワー計測部３０８で計測し、真のデバイスかどうかを判定できる。

【００３６】

図８（ａ）、（ｂ）は、認証処理中のホストと、真のデバイスのＲＦパワー指向特性を示す図である。認証モードに移行した真のデバイスを、ホストの認証圏３５１内にある状態で回転すると、図８（ｂ）のグラフに示すように、デバイスのアンテナの指向性により、ホストの受信するＲＦパワー８０１は符号８０２から符号８０３へ変位する。この変位をホストのＲＦパワー計測部３０８で計測し、真のデバイスかどうかを判定する。

【００３７】

ＲＦパワーの変化とビットレート、ビットエラーレート及び転送効率の変化は相関関係にある場合が多いことから、上記ＲＦパワーという記述を、ビットレート、ビットエラーレート及び転送効率等のデータ列を扱うものに置き換えて、変位の検出方法をホストのＲＦパワー計測部３０８でのＲＦパワー計測から、無線通信制御部３０３での数値計算に置き換えても上記の変位検出方法は成立する。以下、ＲＦパワー、ビットレート、ビットエラーレート及び転送効率等のデータ列を扱うものを総称して、ＲＦパワーとする。

【００３８】

図９（ａ）乃至（ｃ）は、ホスト装置とデバイス装置が認証処理を開始し、ホストの認証圏３５１内に真のデバイスと他のデバイスがある場合に、真のデバイスを検出及び識別するための処理を説明するための図である。

【００３９】

真のデバイスと他のデバイスがともに認証モードであるとして、ある時間に真のデバイスを移動または回転させたとき、ホストが真のデバイスから受信するＲＦパワーが時間の二乗に比例するとした場合、時間ｔ１からｔ２の間で、ホストが受信するＲＦパワーは、図９（ａ）のグラフのように符号９０３から符号９０４に変化する。他のデバイスは移動または回転しないため、ｔ１からｔ２の間でＲＦパワーは符号９１３から符号９１４と変化しない。

【００４０】

時間ｔ１とｔ２の近傍において、ホストは真のデバイスと他のデバイスから受信するＲＦパワーを複数回サンプリングし、１次微分値をとると、図９（ｂ）のグラフのようにホストが受信する真のデバイスからのＲＦパワー１次微分値は符号９０５から符号９０６に

変化する。対して他のデバイスからのＲＦパワーの１次微分値はゼロである。この１次微分値の変位を見ることにより、真のデバイスと他のデバイスの検出及び識別を行うことができる。ここで、１次微分値の変位の無かった他のデバイスは、真の接続対象ではないと識別されるため、ホストは認証情報の交換は行わない。

【００４１】

さらに、時間ｔ１とｔ２の近傍において、ホストが真のデバイスと他のデバイスから受信するＲＦパワーを複数回サンプリングし、２次微分値をとると、図９（ｃ）に示すグラフのように、ホストが受信する真のデバイスからのＲＦパワー２次微分値は符号９０７から符号９０８で一定である。対して他のデバイスからのＲＦパワーの２次微分値はゼロである。この２次微分値の変位を見ることにより、真のデバイスと他のデバイスの検出及び識別を行っても良い。

【００４２】

なお、図９（ａ）乃至（ｃ）に示してあるホストが受信するデバイスからのＲＦパワーの時間変化は一例であり、実際はホストが真のデバイスから受信するＲＦパワーが時間の２乗に比例するとも限らず、ホストが他のデバイスから受信するＲＦパワーが一定であるとも限らない。そこで、ホストでは真のデバイスの検出及び識別精度を上げるため、想定する無線通信システムに合ったサンプリング時間とサンプリング回数、及び微分回数とを選択すると良い。

【００４３】

以下、前述した真のデバイスを検出及び識別するための処理を用いて、ホストが真のデバイスとの認証処理を行う手順を説明する。

【００４４】

図１０Ａ，１０Ｂは、ホストが認証処理を開始してから認証処理を終了するまでの処理手順を示すフローチャートである。この処理手順に係るプログラムは、ＲＯＭ１０３に格納されているものである

まず、ホストに配設されているボタン等を操作して、ホストを認証モードに移行させると、ホストは送受信ＲＦパワーをデータ通信を行うモードよりも低下させて無線信号到達距離を狭め、認証圏を設定する（ステップＳ１０１）。

【００４５】

次に図１１に示すようなインクワイアリ（Ｉｎｑｕｉｒｙ：問合せ、接続要求と同義）信号１１０１を生成し記憶する（ステップＳ１０２）。インクワイアリ信号１１０１には任意のデータ列１１０２と、インクワイアリ応答の繰り返し時間間隔を指定するデータ列１１０３を内包している。任意のデータ列１１０２は、インクワイアリ信号を受信したデバイスが、この任意のデータ列１１０２（照合データでもある）をインクワイアリ応答に内包して返信するものであり、ホストが応答であるか、更には、データ列のビットレート、ビットエラーレート及び転送効率等の変位を検出するために用いられる。インクワイアリ応答の繰り返し時間間隔を指定するデータ列１１０３（時間間隔を指示する情報）は、デバイスから返信されるインクワイアリ応答の繰り返し時間間隔を判定するために用いられる。

【００４６】

ホストはインクワイアリ信号１１０１を生成すると、デバイス探索のために認証圏内にインクワイアリ信号１１０１を送信する（ステップＳ１０３）。

【００４７】

このとき、ＥＳＳＩＤ（Ｅｘｔｅｎｄｅｄ Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｅｒ）は仮の文字列、ＷＥＰキー（Ｗｉｒｅｄ Ｅｑｕｉｖａｌｅｎｔ Ｋｅｙ）無し、チャンネルは“１”に設定して送信する。ただし、認証処理が成功した場合には、認証情報として、真のＥＳＳＩＤ、ＷＥＰキー、チャンネルを送信し、それ以降はこれを用いて通信を行うものとする。

【００４８】

ホストの認証圏内に認証モードに移行しているデバイスが存在すると、デバイスから図

１２に示すようなインクワイアリ応答１２０１が返信されるため、ホストはインクワイアリ応答を受信したかどうかを判定する（ステップＳ１０４）。デバイスが返信するインクワイアリ応答１２０１には、ホストからのインクワイアリ信号１１０１で指定されたデータ列１１０２を含むデータ列１２０２と、デバイスのＲＯＭに保存されているＭＡＣアドレス等の固有コード１２０３を内包している。固有コード１２０３はホスト側でのＭＡＣアドレスフィルタリング等の無線接続制御に用いられるほか、ホスト認証情報の生成に用いられる。

【００４９】

もし、所定の許容時間範囲内で、インクワイアリ応答１２０１が返信されない場合、ホストの認証圏内に認証モードに移行しているデバイスが存在しないと判断し、ホストは認証モードを終了し、ステップＳ１１８に進み、通常のデータ通信状態にするためＲＦパワーを復帰する。

【００５０】

ホストは1回目のインクワイアリ応答１２０１を受信すると、その受信ＲＦパワーを複数回計測・記憶し（ステップＳ１０５）、インクワイアリ応答１２０１のデータ列の一部を記憶する（ステップＳ１０６）。

【００５１】

インクワイアリ応答１２０１は、インクワイアリ信号１１０１に内包されたデータ列１１０３で指定された時間間隔でホストへ返信されることから、ホストは再びインクワイアリ応答１２０１を受信したかどうかを判定する（ステップＳ１０７）。ホストは2回目のインクワイアリ応答１２０１を受信すると、その2回目の受信ＲＦパワーを複数回計測・記憶し（ステップＳ１０８）、2回目のインクワイアリ応答１２０１のデータ列の一部を記憶する（ステップＳ１０９）。

【００５２】

ホストは、１回目と2回目のインクワイアリ応答１２０１の受信ＲＦパワー及びデータ列を記憶すると、インクワイアリ応答１２０１の繰り返し時間が、データ列１１０３で指定した時間と同一かどうかを判定する（ステップＳ１１０）。ここで、インクワイアリ応答１２０１の繰り返し時間が異なっていた場合は、ホストは真のデバイスからの応答ではないと判定し、認証モードを終了する。

【００５３】

次にホストは、インクワイアリ応答１２０１に任意のデータ列１１０２が内包されているかを判定する（ステップＳ１１１）。インクワイアリ応答１２０１にホストが指定した任意のデータ列１１０２が内包されていない、または異なるデータ列が内包されていた場合は、ホストは真のデバイスからの応答ではないと判定し、認証モードを終了する。

【００５４】

次にホストは、１回目と2回目のインクワイアリ応答１２０１の受信ＲＦパワーの変位を計算する（ステップＳ１１２）。ステップＳ１１２での計算は図９を用いて説明したような処理を用いると良い。ステップＳ１１２で計算された結果を元に、ホストは受信したインクワイアリ応答１２０１のＲＦパワーの変位が、システムの規定する所定範囲内に収まっているかどうかを判定する（ステップＳ１１３）。

【００５５】

ここで、ＲＦパワーの変位が無い、または変位がシステムの規定する範囲外であった場合は、ホストは認証モードを終了する。

【００５６】

なお、ここで言う変位は、その正負の符号は無視するため、差分の絶対値を取る。そして、その変位が実質的に０（正確には０に近い閾値Ｔ１以下）か、閾値Ｔ２（Ｔ２＞Ｔ１＞０）以上の場合には、認証失敗として判定し、ホストは認証モードを終了する。

【００５７】

また、ＲＦパワーの変位がシステムの規定する範囲内（閾値Ｔ１より大きく、Ｔ２未満）であった場合は、ＲＦパワーが変位したデバイスが唯一かどうかを、インクワイアリ応

答のデータのデバイス固有コードが一致するかどうかに基づいて判定する（ステップＳ１１４）。認証圏内にＲＦパワーが変位したデバイスが複数あった場合は、ホストは認証モードを終了する。ＲＦパワーが変位したデバイスが唯一であった場合は、ホストはそのデバイスを真のデバイスと認識し、真のデバイスの認証情報を生成し記憶する（ステップＳ１１５）。

【００５８】

次に、生成した認証情報を真のデバイスへ送信する（ステップＳ１１６）。その後、真のデバイスへ認証終了を通知し（ステップＳ１１７）、認証モードを終了してＲＦパワーを復帰する（ステップＳ１１８）。認証処理終了後、すぐに無線データ通信を行わない場合は、認証モード終了後ＲＦパワーをＯＦＦにして、ホストをアイドル状態にしても良い。

【００５９】

以上のフローが終了すると、ホストとデバイスは交換した認証情報を用いてで無線通信路３５３を確保し、無線データ通信を行うことができるようになる。実施形態の場合、ホストはプリンタ、デバイスはデジタルカメラであるので、デジタルカメラで撮像された画像のプリント出力処理が行われることになる。

【００６０】

以上、図１０Ａ、１０Ｂを用いて述べたホストの認証フローにおいて、真のデバイスの判定条件は、以下のプロセス（Ｓ１５１）～（Ｓ１５６）に示すように分けることができる。

・ステップＳ１５１：ステップＳ１０１からステップＳ１０４において、ホスト認証圏内か認証圏外かの判定、
・ステップＳ１５２：ＲＦパワー、ピットレート、ビットエラーレート、及び転送効率の計測、
・ステップＳ１５３：インクワイアリ応答の繰り返し時間が、ホストの指定した繰り返し時間と同一かの判定、
・ステップＳ１５４：インクワイアリ応答にホストが指定した任意のデータ列が含まれているかを判定、及び、
・ステップＳ１５５：ＲＦパワー、ピットレート、ビットエラーレート、及び転送効率の変位があるかを判定、
・ステップＳ１５６：ＲＦパワー、ピットレート、ビットエラーレート、及び転送効率が変位したデバイスが唯一かどうかを判定する。

【００６１】

なお、プロセス（Ｓ１５１）で判定する認証圏内、認証圏外の設定距離はいくらでも構わないが、認証圏が広すぎるとセキュリティの強度が低下し、さらに真のデバイス判定が困難になることから、できるだけ短距離であることが望ましい。つまり、実施形態で示しているように数十センチメートル程度が妥当であろう。

【００６２】

また、プロセス（Ｓ１５２）と同様のプロセスは図１０Ａ、１０Ｂの例では２回繰り返しているが、複数回繰り返してデバイスの検出精度を上げても良い。

【００６３】

上記プロセス（Ｓ１５３）から（Ｓ１５５・Ｓ１５６）は順序は問わず、また、上記ステップに限らず他の判定ステップを組み合わせたり、判定ステップを減らしても構わない。特に、ステップＳ１５１乃至Ｓ１５５の判定の少なくとも１つと、ステップＳ１５６との組み合わせで、デバイスが特定できる場合には、それを真のデバイスと判定しても構わない。

【００６４】

次に、デバイス側のホストとの認証処理を行う手順を説明する。図１３は、デバイス（実施形態ではデジタルカメラ）が認証処理を開始してから認証処理を終了するまでのフローチャートである。このフローチャートに対応するプログラムは、ＲＯＭ２０３に格納さ

れるものでもある。

【００６５】

まず、デバイスに配設されているボタン等を操作して、デバイスを認証モードに移行させると、デバイスは送受信ＲＦパワーをデータ通信を行うモードよりも低下させて無線信号到達距離を狭め、認証圏を設定する（ステップＳ２０１）。このとき、無線のパラメータは、ホスト側の認証処理開始時と同様にする。

【００６６】

ここで、デバイスの認証圏内に認証モードに移行しているホストが存在すると、ホストは図１１に示すようなインクワイアリ信号１１０１を送信してデバイスを探索しているため、デバイスはインクワイアリ信号を受信したかどうかを判定する（ステップＳ２０２）。

【００６７】

もし、認証圏内に認証モードに移行しているホストが存在しない場合はインクワイアリ信号は受信されない。この場合には、ステップＳ２１０に進んで、デバイスは認証モードし、通常のデータ通信状態にするためＲＦパワーを復帰する。

【００６８】

また、デバイスがインクワイアリ信号を受信すると、図１２に示すような１回目のインクワイアリ応答１２０１を生成し記憶する（ステップＳ２０３）。このインクワイアリ応答１２０１には、ホストから指定された任意のデータ列１１０２を含むデータ列１２０２と、デバイスのＲＯＭに保存されているＭＡＣアドレス等の固有コード１２０３を内包している。

【００６９】

次に、デバイスは１回目のインクワイアリ応答１２０１をホストに対して複数回送信する（ステップＳ２０４）。１回目のインクワイアリ応答送信後、デバイスは２回目のインクワイアリ応答１２０１を生成、記憶し（ステップＳ２０５）、２回目のインクワイアリ応答１２０１をホストに対して複数回送信する（ステップＳ２０６）。なお、１回目と２回目のインクワイアリ応答は、インクワイアリ応答の繰り返し時間を指定するデータ列１１０３で指定された繰り返し時間間隔でホストに送信する。先に説明したように、ホストが真のデバイスかそうでないかを判定するパラメータの一つとなるためである。

【００７０】

プロセス（Ｓ２５１）と同様のプロセスは図１３の例では２回繰り返しているが、システムの構成により複数回繰り返しても良い。また、インクワイアリ応答１２０１の生成と記憶を１回だけ行うようにしても良い。

【００７１】

インクワイアリ応答１２０１を送信したデバイスは、ホストからの認証情報を受信したかを判定し（ステップＳ２０７）、ホストから認証情報が送信されない、またはホストからの認証情報を受信できない場合は認証モードを終了する。ホストから認証情報を受信したならば、デバイスはその認証情報を記憶する（ステップＳ２０８）。その後、ホストへ認証終了を通知し（ステップＳ２０９）、認証モードを終了してＲＦパワーを復帰する（ステップＳ２１０）。

【００７２】

以上のフローが終了すると、ホストとデバイスは交換した認証情報を用いてで無線通信路３５３を確保し、無線データ通信を行うことができるようになる。

【００７３】

図１４Ａ，１４Ｂは、図１０Ａ、１０Ｂで述べたホストの認証プロセスフローと、図１３で述べたデバイスの認証プロセスフローを合わせて示した認証処理フローである。処理内容は、既に説明した通りであるので、省略するが、特に図１４Ａのプロセス（Ｓ３０１）を繰り返し行うことで、真のデバイスの検出を容易にし、かつ、他の第三者のデバイスが認証情報を傍受するのを防ぐことができる。

【００７４】

なお、ホストとデバイスの双方に表示部を備え、認証処理が正常に完了した場合には、それぞれの表示部に、認証成功を示す表示（メッセージやＬＥＤ点灯等）を行うようにすることが望ましい。万が一、一方のみに認証成功の表示が行われた場合には、意図しないデバイスやホストと認証処理をしてしまったことがわかるので、再度上記の処理を行えば良い。

【００７５】

以上説明したように本実施形態によれば、２つの無線通信装置が互いに認証を行う際には、それぞれのＲＦパワー下げる、すなわち、通信可能範囲を例えば数十センチメートル程度の距離でないと送受信できない状態することで、単一の無線通信手段を利用しながらも、他のデバイスや他のホストが圏内に入り込むことを除外することが可能となる。そして、ホストは、自身が設定したデータ列を含むインクワイアリ応答が、自身が設定した所定時間間隔で受信でき、尚且つ、そのインクワイアリ応答の受信強度に変化がある場合に限って、該当するインクワイアリ応答を発信したデバイスが認証対象デバイスとして判定する。従って、ホストの近くに意図しない他のデバイスが存在する場合であっても、目的とするデバイスをその範囲内にて移動、回転等を行えば、他のデバイスと容易に区別され、認証処理が完了することになる。

【００７６】

換言すれば、本実施形態にしたがえば、無線通信装置相互の接続対象の検出及び認証からデータ通信に至るまでを、単一の無線通信手段のみを用いて行うことができるため、無線通信装置の簡素化、省電力化及び小型化に有効である。また、無線通信装置相互の接続対象の検出及び認証時にはＲＦパワーをデータ通信を行う状態よりも低下させて、無線信号到達距離を狭めることから、認証情報の傍受の危険性が少なく高セキュリティである。さらに、第１の無線通信装置が真の接続対象とする第２の無線通信装置を検出する際には、ＲＦパワー、ビットレート、ビットエラーレート及び転送効率等の変位を利用することから、第１及び第２の無線通信装置の認証圏内に、真の接続対象ではない無線通信装置が存在する状況においても、意図しない無線通信装置間での認証情報の交換を避けることができる。第１及び第２の無線通信装置間の認証情報の交換は、真の接続対象とする無線通信装置を相互に検出した後、自動で継ぎ目が無いように行われることから、表示部や操作部の無い無線通信装置にも適用可能であり、使用者が認証情報を手動で設定したり、難しい操作をしたりすることを必要とせずに無線通信装置の認証を行うことができ、高セキュリティな無線通信システムとサービスを簡便に提供することができる。

【００７７】

なお、実施形態では、ホストとしてプリンタ装置、デバイスとしてデジタルカメラについて説明したが、これらの装置によって本願発明が限定されるものではない。要は、お互いに、ＲＦパワー制御、並びに受信パワーの計測を行え、ホスト、デバイスそれぞれが相手と通信するための単一の通信手段を備えれば良い（図４に示されるデバイス３、４（形態電話やＰＤＡ）は通信手段を２つ備えているが、ホストと通信する手段は１つのみである点に注意されたい）。

【００７８】

従って、例えばホストはデスクトップパーソナルコンピュータ等の情報処理装置（ホスト）であり、もう一方もＰＤＡやノートタイプのパーソナルコンピュータでも構わないであろう。

【００７９】

なお、実施形態では、デバイス装置とホスト装置の少なくとも一方が移動可能であることを前提として説明したが、ホスト装置とデバイス装置は、お互いに、ＲＦパワー制御、並びに受信パワーの計測を行えれば良い。従って、ホスト装置及びデバイス装置に、実施形態の図７、図８で説明したＲＦパワー制御と同様の効果のあるＲＦパワー変調処理を行う回路またはソフトウェアが搭載されている場合、一方が移動しなくとも、お互いの認証圏内であれば、装置に配設されたボタンやキーを操作することによってＲＦパワー変調処理を行い、実施形態に沿った方法で認証処理を行うことができる。

【００８０】
パーソナルコンピュータ等の汎用情報処理装置はホストもしくはデバイスとして機能する場合には、当然、図１０Ａ，１０Ｂまたは図１３に示す処理を行うプログラムがインストールされることになるわけであるから、当然、本発明はそのようなコンピュータプログラムをも含むことになる。さらにまた、通常、コンピュータプログラムはＣＤ－ＲＯＭ等のコンピュータ可読記憶媒体に格納されていて、それをコンピュータにセットして、システムにコピーもしくはインストールすることで実行可能になるわけであるから、そのようなコンピュータ可読記憶媒体も本願発明の範疇になることも明らかである。

【図面の簡単な説明】

【００８１】

【図１】実施形態における無線通信ホスト装置となるプリンタ装置のブロック構成図である。

【図２】実施形態における無線通信デバイス装置となるデジタルカメラのブロック構成図である。

【図３】実施形態における無線通信ホスト装置内の無線通信部のブロック構成図である。

【図４】実施形態におけるホスト装置と無線通信デバイス装置の認証前の状態の一例を示す図である。

【図５】実施形態における無線通信ホスト装置と無線通信デバイス装置の認証処理中の状態を示す図である。

【図６】実施形態における認証処理中の無線通信ホスト装置と無線通信デバイス装置それぞれの表示部の状態の一例を示す図である。

【図７】実施形態における無線通信ホスト装置と認証対象の無線通信デバイス装置の認証処理中のＲＦパワーの距離特性の一例を示した図である。

【図８】実施形態における無線通信ホスト装置と認証対象の無線通信デバイス装置の認証処理中のＲＦパワーの放射特性の一例を示す図である。

【図９】実施形態におけるホストが認証対象の無線通信デバイス装置を識別する際に用いる無線信号の特性を示す図である。

【図１０Ａ】実施形態における無線通信ホスト装置における認証処理手順を示すフローチャートである。

【図１０Ｂ】実施形態における無線通信ホスト装置における認証処理手順を示すフローチャートである。

【図１１】実施形態における無線通信ホスト装置が発信するインクワイアリ信号のデータフォーマットを示す図である。

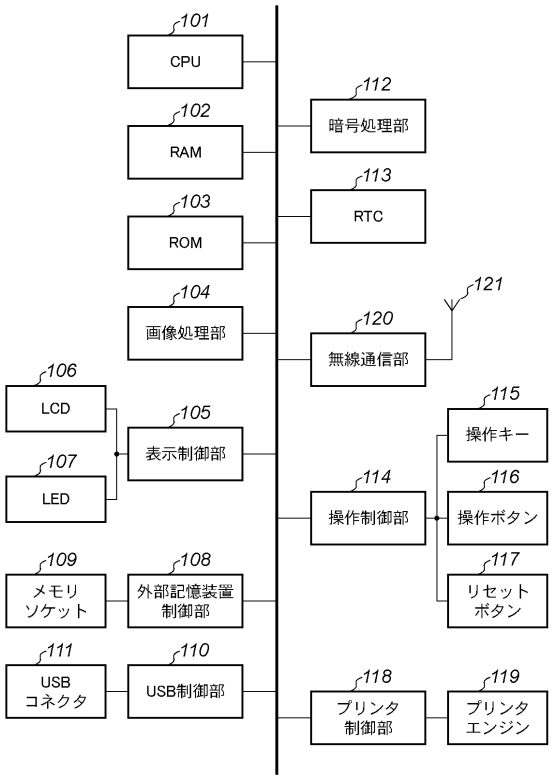
【図１２】実施形態における無線通信デバイス装置が応答するインクワイアリ応答信号のデータフォーマットを示す図である。

【図１３】実施形態における無線通信デバイス装置における認証処理手順を示すフローチャートである。

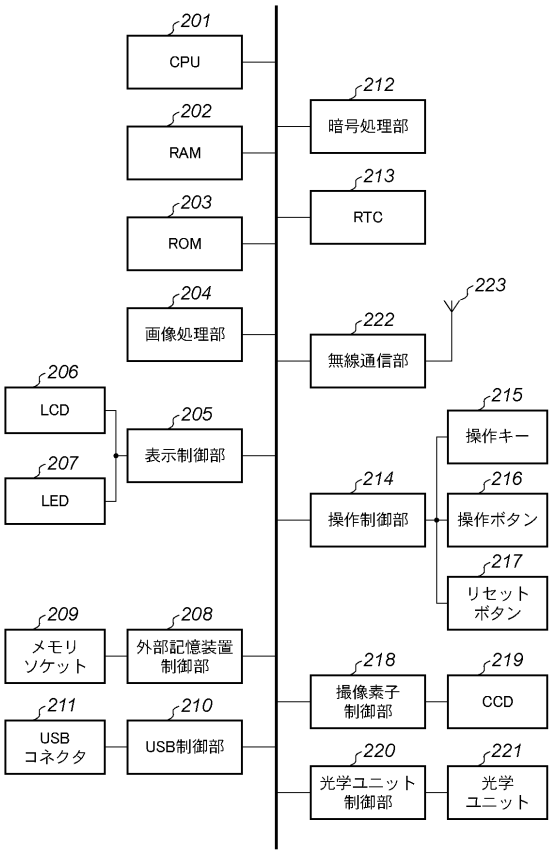
【図１４Ａ】実施形態における無線通信ホスト装置と無線通信デバイス装置の処理の関係を並列して示すフローチャートである。

【図１４Ｂ】実施形態における無線通信ホスト装置と無線通信デバイス装置の処理の関係を並列して示すフローチャートである。

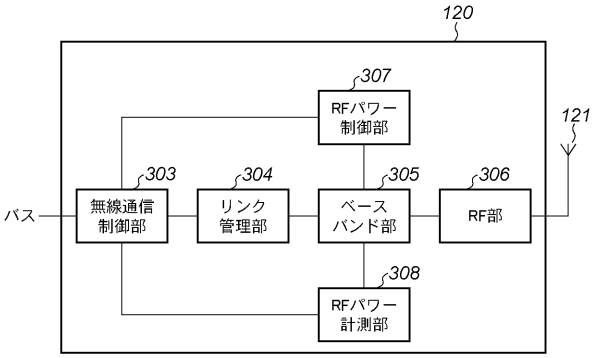
【図１】


101
CPU
102
RAM
103
ROM
104
画像処理部
106
LCD
107
LED
105
表示制御部
109
メモリ
ソケット
108
外部記憶装置
制御部
111
USB
コネクタ
110
USB制御部
112
暗号処理部
113
RTC
120
無線通信部
121
114
操作制御部
115
操作キー
116
操作ボタン
117
リセット
ボタン
118
プリンタ
制御部
119
プリンタ
エンジン

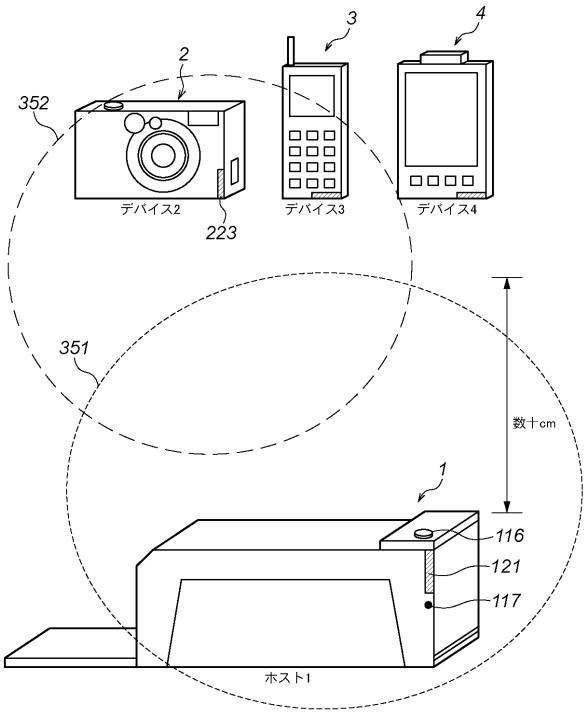
【図２】


201
CPU
202
RAM
203
ROM
204
画像処理部
206
LCD
207
LED
205
表示制御部
209
メモリ
ソケット
208
外部記憶装置
制御部
211
USB
コネクタ
210
USB制御部
212
暗号処理部
213
RTC
223
222
無線通信部
214
操作制御部
215
操作キー
216
操作ボタン
217
リセット
ボタン
218
撮像素子
制御部
CCD
219
220
光学ユニット
制御部
221
光学
ユニット

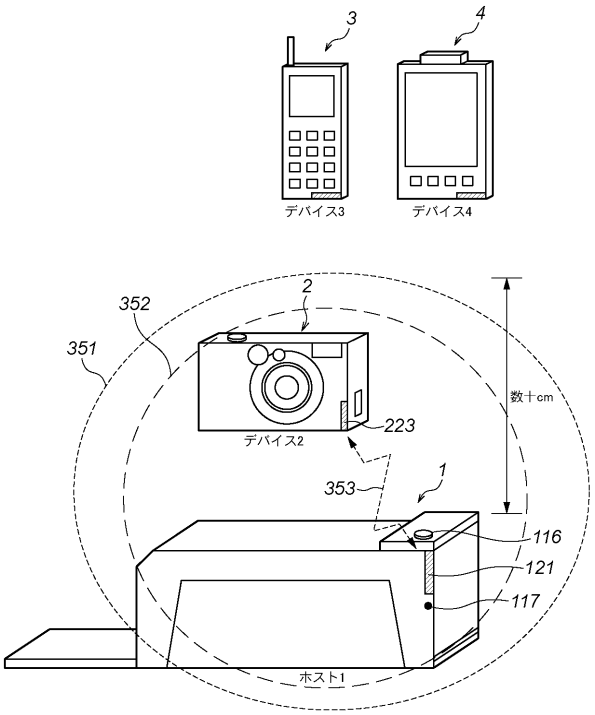
【図３】


120
307
RFパワー
制御部
121
303
無線通信
制御部
304
リンク
管理部
305
ベース
バンド部
306
RF部
バス
308
RFパワー
計測部

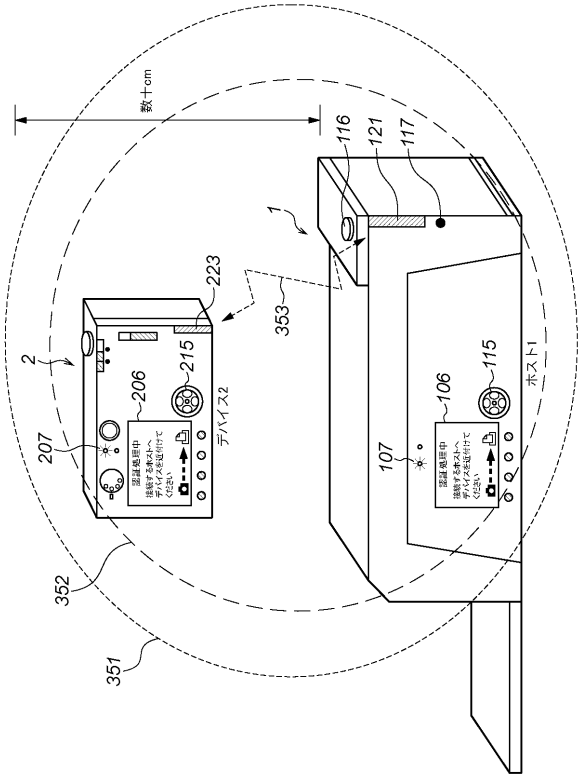
【図４】


3
4
2
352
デバイス2
223
デバイス3
デバイス4
351
数十cm
1
116
121
117
ホスト1

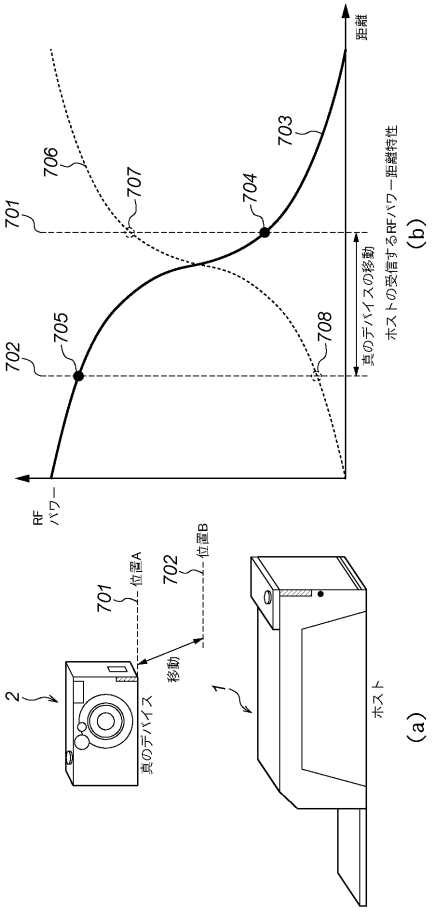
【図５】


3
4
デバイス3
デバイス4
2
352
351
223
デバイス2
数十cm
353
1
116
121
117
ホスト1

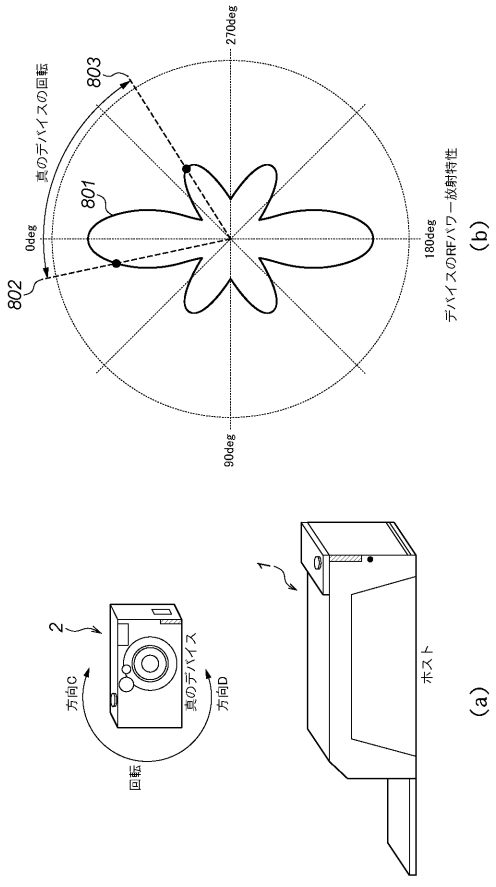
【図６】


数十cm
116
121
117
1
223
353
2
215
206
207
デバイス2
106
115
ホスト1
107
352
351

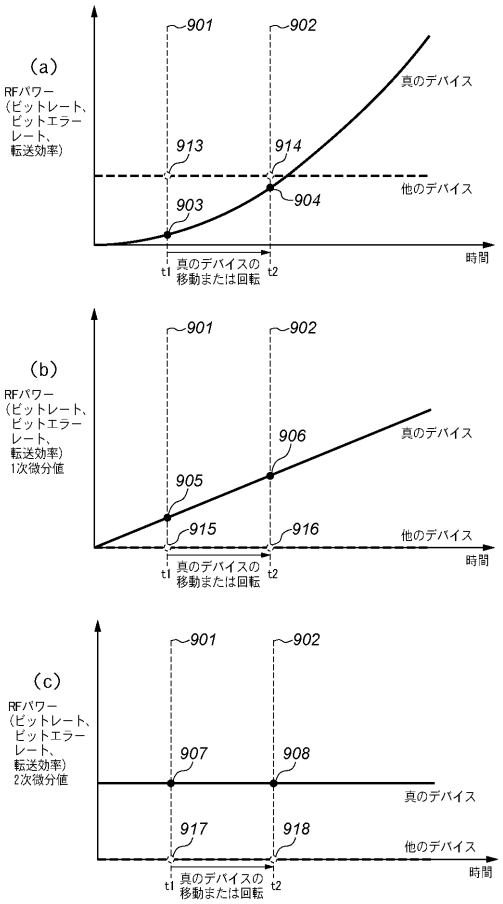
【図７】


距離
706
703
707
701
704
(b)
真のデバイスの移動
ホストの受信するRFパワー－距離特性
705
702
708
RF
パワー
位置A
位置B
701
702
移動
2
真のデバイス
1
ホスト
(a)

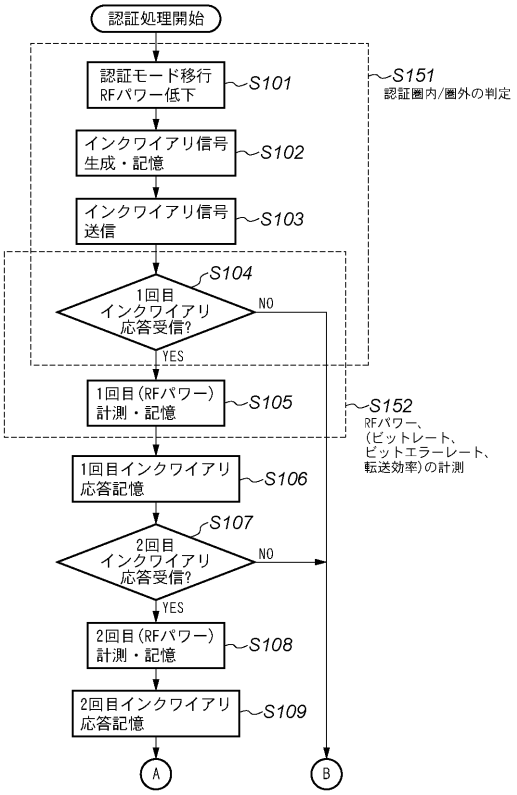
【図８】


270deg
803
真のデバイスの回転
801
0deg
180deg
802
90deg
デバイスのRFパワー－放射特性
(b)
1
2
方向C
真のデバイス
方向D
回転
ホスト
(a)

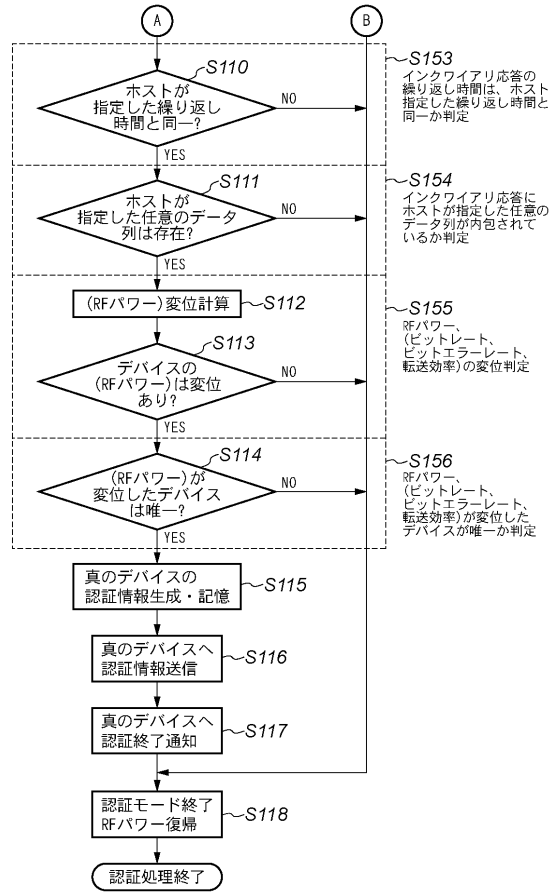
【図９】



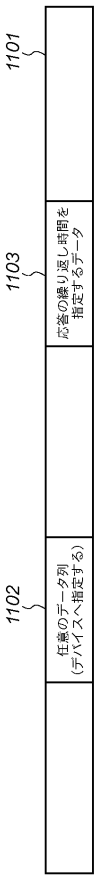
【図１０Ａ】



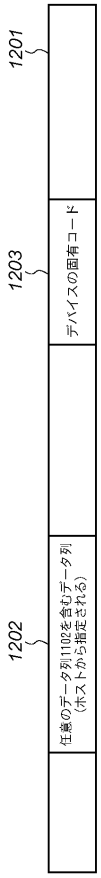
【図１０Ｂ】



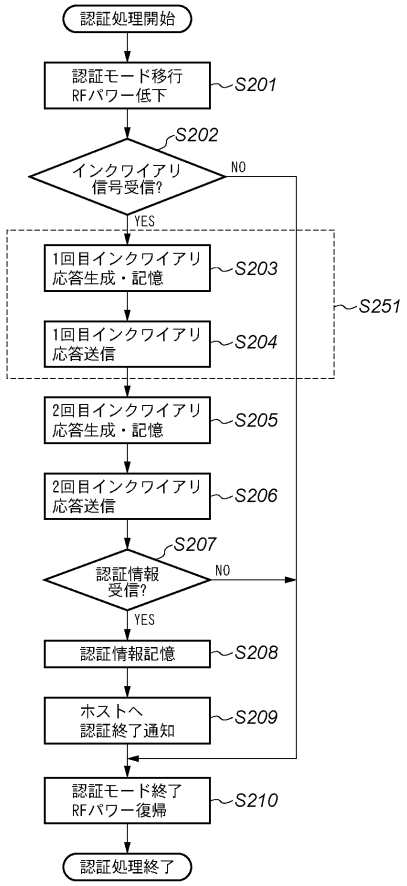
【図１１】



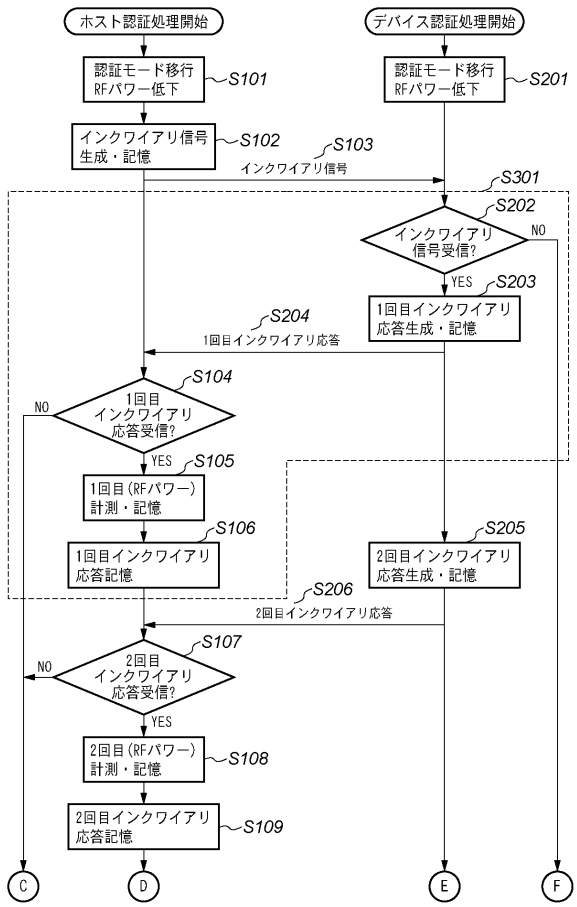
【図１２】



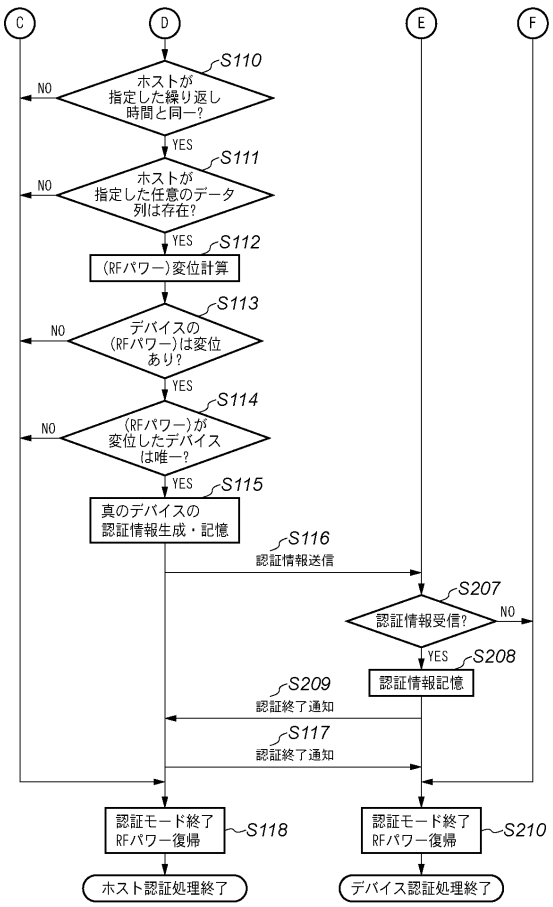
【図１３】



【図１４Ａ】



【図１４Ｂ】



フロントページの続き

Ｆターム(参考) 5K033 AA08 CB01 DA01 DA17 EA06 EA07
5K067 AA30 BB04 BB21 DD17 DD24 DD51 EE02 EE12 HH22 HH36