(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4702944号
(P4702944)

(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.		F I		
H04W 12/00	(2009.01)	H04Q	7/00	180
H04W 48/18	(2009.01)	H04Q	7/00	410
H04W 84/10	(2009.01)	H04Q	7/00	629
H04W 84/12	(2009.01)	H04Q	7/00	630
H04W 88/06	(2009.01)	H04Q	7/00	653

請求項の数 11　(全 14 頁)　最終頁に続く

(21)出願番号　特願2005-363860 (P2005-363860)
(22)出願日　平成17年12月16日 (2005.12.16)
(65)公開番号　特開2007-166538 (P2007-166538A)
(43)公開日　平成19年6月28日 (2007.6.28)
審査請求日　平成20年12月10日 (2008.12.10)

(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　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　大塚　充
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】通信装置およびその制御方法及び通信システム

(57)【特許請求の範囲】

【請求項１】

複数の通信方式を持つ他の通信装置と通信可能な通信装置であって、

第１の通信方式に従って無線通信する第１の通信手段と、

第２の通信方式および暗号化方式に従って無線通信する第２の通信手段と、

前記第１の通信手段を用いた通信により、前記他の通信装置の通信方式および暗号化方式を取得する取得手段と、

前記取得手段により取得された前記他の通信装置の通信方式および暗号化方式が、前記第２の通信手段の通信方式および暗号化方式に合致するか否かを判定する判定手段と、

前記判定手段により合致すると判定された場合は、前記第２の通信手段により前記第２の通信方式及び前記暗号化方式に従って前記他の通信装置と通信を行い、合致しないと判定された場合には、前記第１の通信手段により前記第１の通信方式に従って前記他の通信装置と通信を行う通信制御手段と

を備えることを特徴とする通信装置。

【請求項２】

通信装置であって、

第１の通信方式に従って無線通信する第１の通信手段と、

第２の通信方式および暗号化方式に従って無線通信する第２の通信手段と、

前記第１の通信手段を用いた他の通信装置との通信により、前記第２の通信手段の通信方式及び暗号方式により前記通信装置と通信できる情報を前記他の通信装置が有している

ことを判別する判別手段と、
前記判別手段により、前記他の通信装置が前記情報を有していると判別された場合、前記第２の通信手段により前記第２の通信方式及び前記暗号化方式に従って前記他の通信装置と通信を行い、前記他の通信装置が前記情報を有していると判別されない場合、前記第１の通信手段により前記第１の通信方式に従って前記他の通信装置と通信を行う通信制御手段と
を備えることを特徴とする通信装置。
【請求項３】
前記第１の通信方式は、近距離無線通信方式であることを特徴とする請求項１又は２に記載の通信装置。
【請求項４】
前記第１の通信方式は、非接触ＩＣカード通信、赤外線通信、Ｂｌｕｅｔｏｏｔｈ、ＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ）のいずれか１つの通信方式であることを特徴とする請求項１又は２に記載の通信装置。
【請求項５】
前記第１の通信方式により通信を行う場合に、利用者に対して前記通信装置を前記他の通信装置に近付ける旨のメッセージを出力する出力手段を更に備えることを特徴とする請求項３又は４に記載の通信装置。
【請求項６】
前記通信装置は、前記他の通信装置に対して画像データを送信する撮像装置であることを特徴とする請求項１乃至５のいずれか１項に記載の通信装置。
【請求項７】
前記通信装置は、前記他の通信装置から画像データを受信する画像出力装置であることを特徴とする請求項１乃至５のいずれか１項に記載の通信装置。
【請求項８】
請求項１に記載の通信装置と、請求項２に記載の通信装置とを備えることを特徴とする通信システム。
【請求項９】
互いに通信方式の異なる第１及び第２の通信手段を持つ通信装置の制御方法であって、
前記第１の通信手段を用いた通信により、他の通信装置の通信方式および暗号化方式を取得する取得工程と、
前記取得工程により取得された前記他の通信装置の通信方式および暗号化方式が、前記第２の通信手段の通信方式および暗号化方式に合致するか否かを判定する判定工程とを備え、
前記判定工程により合致すると判定された場合は、前記第２の通信手段の通信方式及び暗号化方式に従って前記他の通信装置と通信を行い、合致しないと判定された場合には、前記第１の通信手段の通信方式に従って前記他の通信装置と通信を行うことを特徴とする通信装置の制御方法。
【請求項１０】
通信方式の異なる第１及び第２の通信手段を有する通信装置の制御方法であって、
前記第１の通信手段を用いた他の通信装置との通信により、前記第２の通信手段の通信方式及び暗号方式により前記通信装置と通信できる情報を前記他の通信装置が有していることを判別する判別工程と、
前記判別工程において、前記他の通信装置が前記情報を有していると判別された場合、前記第２の通信手段により前記第２の通信方式及び前記暗号化方式に従って前記他の通信装置と通信を行い、前記他の通信装置が前記情報を有していると判別されない場合、前記第１の通信手段により前記第１の通信方式に従って前記他の通信装置と通信を行う通信制御工程と
を有することを特徴とする制御方法。
【請求項１１】

請求項９または請求項１０に記載された通信装置の制御方法の各工程をコンピュータにより実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、たとえば近距離無線通信方式を含む複数の通信方式を持つ通信装置に関する。

【背景技術】

【０００２】

従来、複数の通信方式を切り替えて通信を行う通信装置があった。この種の通信装置において、複数の通信方式のそれぞれに通信可能かを確認してから通信方式を選択するものがある（例えば、特許文献１等参照）。また、非接触ＩＣインターフェースのような近距離無線通信方式を使用して通信先の端末が対応するプロトコル一覧を取得する通信装置がある。この通信装置は、そのプロトコルに自端末が対応しているときに試し通信を行い、成功した場合にそのプロトコルで通信を行う（例えば、特許文献２等参照）。また、非接触ＩＣインターフェースのような近距離無線通信方式を使用して、Bluetooth（登録商標）通信で同期を確立する端末の情報を交換するものがある（例えば、特許文献３または特許文献４または特許文献５等参照）。また、情報通信網の通信セキュリティにおいて、通信の対象となる情報にセキュリティレベルを設定し、通信相手のセキュリティレベルが通信の対象となる情報のセキュリティレベル以上の場合に限って通信を行う通信装置がある（例えば、特許文献６等参照）。

【特許文献１】特開２００３－８６８１号公報

【特許文献２】特開２００３－１９８５６８号公報

【特許文献３】特開２００３－３２１７５号公報

【特許文献４】特開２００３－３２１７６号公報

【特許文献５】特開２００３－３２２６１号公報

【特許文献６】特開平０６－２４４８３３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

上述した従来の技術では以下のような問題があった。すなわち、複数の通信方式を切り替える場合に、それぞれの通信方式が通信可能かを確認したり、試し通信を行ったりすることによって通信方式を決定するのでは、通信のセキュリティが確保されていることを確認することができない。複数の無線通信方式を備え、第一の無線通信方式の情報を第二の無線通信方式によって取得するのでは、第二の無線通信方式による通信が行えない場合に代替となる通信手段がない。通信の対象となる情報にセキュリティレベルを設定して通信相手のセキュリティレベルが通信の対象となる情報のセキュリティレベル以上の場合に限って通信を行うのでは、セキュリティが確保されない場合に代替となる通信手段がない。

【０００４】

本発明は、通信できる確実性を向上でき、さらに、機密性の高い通信を実現することを目的とする。

【課題を解決するための手段】

【０００５】

上記課題を解決するため、本出願に係る発明は以下の構成を備える。すなわち、複数の通信方式を持つ他の通信装置と通信可能な通信装置であって、

第１の通信方式に従って無線通信する第１の通信手段と、

第２の通信方式および暗号化方式に従って無線通信する第２の通信手段と、

前記第１の通信手段を用いた通信により、前記他の通信装置の通信方式および暗号化方式を取得する取得手段と、

前記取得手段により取得された前記他の通信装置の通信方式および暗号化方式が、前記

第２の通信手段の通信方式および暗号化方式に合致するか否かを判定する判定手段と、
前記判定手段により合致すると判定された場合は、前記第２の通信手段により前記第２の通信方式及び前記暗号化方式に従って前記他の通信装置と通信を行い、合致しないと判定された場合には、前記第１の通信手段により前記第１の通信方式に従って前記他の通信装置と通信を行う通信制御手段とを備えることを特徴とする。

【０００６】

あるいは、通信装置であって、
第１の通信方式に従って無線通信する第１の通信手段と、
第２の通信方式および暗号化方式に従って無線通信する第２の通信手段と、
前記第１の通信手段を用いた他の通信装置との通信により、前記第２の通信手段の通信方式及び暗号方式により前記通信装置と通信できる情報を前記他の通信装置が有していることを判別する判別手段と、
前記判別手段により、前記他の通信装置が前記情報を有していると判別された場合、前記第２の通信手段により前記第２の通信方式及び前記暗号化方式に従って前記他の通信装置と通信を行い、前記他の通信装置が前記情報を有していると判別されない場合、前記第１の通信手段により前記第１の通信方式に従って前記他の通信装置と通信を行う通信制御手段と
を備えることを特徴とする。

【発明の効果】

【０００７】

本発明によれば、通信できる確実性を向上でき、さらに、機密性の高い通信を実現することができる。

【発明を実施するための最良の形態】

【０００８】

［第１の実施形態］
＜通信システムの構成＞
図１は、本発明の第１の実施形態に係る通信装置の構成を示す図である。通信システム全体は通信装置１及び通信装置２により構成されている。通信装置１は通信手段としてＮＦＣインターフェースおよびＩＥＥＥ８０２．１１ｂインターフェースを持つ。通信装置２は、通信手段としてＮＦＣインターフェース、およびＩＥＥＥ８０２．１１ａインターフェースおよびＩＥＥＥ８０２．１１ｂインターフェースを持つ。詳しくは以下の通りである。

【０００９】

通信装置１において、ＣＰＵ１０１は装置全体の動作を制御する。ＲＯＭ１０２にはＣＰＵ１０１により実行される制御プログラム等が格納されている。また、ＲＯＭ１０２には、図５等で説明する通信情報テーブル５０１が格納されている。通信情報テーブルには、当該装置がサポートする通信方式及び暗号化方式を表すパラメータが格納されている。ＲＡＭ１０３には制御データが格納される。ＮＦＣインターフェース１０４は、近距離でのみ通信可能な電磁界を発生させることにより通信を行う。ＩＥＥＥ８０２．１１ｂインターフェース１０５は、無線ＬＡＮ（ローカルエリアネットワーク）規格の一つである。これら構成要素は、バス１０６で接続されている。ＮＦＣインターフェースの代表的なものには、特許文献２、特許文献３、特許文献４、特許文献５で使用されているような非接触ＩＣカードとリーダライタの組み合わせによって構成される非接触ＩＣインターフェースがある。なおＮＦＣインターフェースは、ＩＳＯ／ＩＥＣ　ＩＳ　１８０９２という国際規格である。

【００１０】

通信装置２において、ＣＰＵ１０７は装置全体の動作を制御する。ＲＯＭ１０８にはＣＰＵ１０７により実行される制御プログラム等が格納されている。また、ＲＯＭ１０８には、図５等で説明する通信情報テーブル５０１及び５０２が格納されている。ＲＡＭ１０９には制御データが格納される。ＮＦＣインターフェース１１０は、近距離でのみ通信可

能な電磁界を発生させることにより通信を行う。ＩＥＥＥ８０２．１１ａインターフェース１１１は、無線ＬＡＮ（ローカルエリアネットワーク）規格の一つである。ＩＥＥＥ８０２．１１ｂインターフェース１１２は、無線ＬＡＮ（ローカルエリアネットワーク）規格の一つである。これら構成要素は、バス１１３で接続されている。

【００１１】

無線ＬＡＮ規格のＩＥＥＥ８０２．１１ａ、ＩＥＥＥ８０２．１１ｂは、通信を暗号化することにより通信のセキュリティを確保することが可能な通信方式である。通信装置１のＮＦＣインターフェース１０４と通信装置２のＮＦＣインターフェース１１０を使用して、通信装置１は通信装置２に実装されている通信インターフェースの通信方式および暗号化方式を取得する。

【００１２】

＜通信手順＞

図２および図３は、通信装置１が通信装置２に実装されている通信インターフェースの通信方式および暗号化方式を取得してデータ通信を行う際の動作シーケンスである。図２は、通信方式および暗号化方式取得の結果ＩＥＥＥ８０２．１１ｂで通信を行う際の手順を示す。図３は、通信方式および暗号化方式取得の結果ＮＦＣで通信を行う際の手順を示す。

【００１３】

図２において、通信装置１を通信装置２へ近づけることによりＮＦＣインターフェース１０４と１１０との間で通信が開始される（ステップＳ２００）。通信方式および暗号化方式を要求するメッセージが通信装置１から通信装置２へ送信される（ステップＳ２０１）。その応答として、通信装置２に実装されている通信インターフェースの通信方式および暗号化方式が通信装置２から通信装置１へ送信される（ステップＳ２０２）。通信方式および暗号化方式のデータ例は図４、図５、図６を使用して後述する。

【００１４】

通信装置２に実装されている通信インターフェースの通信方式および暗号化方式を取得した通信装置１は、通信方式および暗号化方式が、通信装置１がサポートする通信方式及び暗号化方式に合致するか否かを判定する（ステップＳ２０３）。通信方式および暗号化方式が合致する場合は、図２に示すようにＮＦＣインターフェース１０４と１１０を使用する通信を終了する（ステップＳ２０４）。そしてＩＥＥＥ８０２．１１ｂインターフェース１０５，１１２を使用して通信を開始し（ステップＳ２０５）、データ通信を行った後（ステップＳ２０６）、通信を終了する（ステップＳ２０７）。ステップＳ２０３までが通信方式及び暗号化方式を判定する方式判定フェーズであり、ステップＳ２０４移行が通信フェーズである。

【００１５】

図３においては、ステップＳ２００からＳ２０３までは当然ながら図２と共通している。ただし図３ではステップＳ２０３の判定で、取得した通信方式及び暗号化方式が、通信装置１のサポートする通信方式及び暗号化方式に合致しないと判定されている。そのため、ＮＦＣインターフェース１０４と１１０を使用する通信が継続され、ＮＦＣインターフェース１０４と１１０を使用してデータ通信が行われた後（ステップＳ３０１）、通信が終了される（ステップＳ３０２）。なおステップＳ２０３における判定は、通信方式及び暗号化方式のそれぞれについてなされる。すなわち通信方式と暗号化方式の両方が一致した場合にはじめて図２の手順となる。なお通信装置１、通信装置２の動作アルゴリズムについては、それぞれ図７、図８を参照して後述する。

【００１６】

＜通信情報および通信情報テーブルの例＞

図４に、通信方式および暗号化方式を示すデータ（通信情報という）４０１のデータ構造の一例を示す。この通信情報が、図２及び図３のステップＳ２０２で通信装置２から通信装置１に対して送信される。さて、通信情報においては、通信方式、通信パラメータ、通信パラメータ長が各１バイトのデータで表され、通信パラメータ長の長さ（たとえばバ

イト数）分の通信パラメータ値がそのあとに続く。加えて暗号化方式に関する情報として、暗号化方式、暗号鍵種別、暗号鍵長が各１バイトのデータで表され、暗号鍵長の長さ（たとえばバイト数）分の暗号鍵値がそのあとに続く。

【００１７】

通信方式、通信パラメータ、暗号化方式、暗号鍵種別を識別するための値は、一例として図４の表４０２のように定義されている。表４０２によれば、通信方式フィールドに記述された値０ｘ０１はＩＥＥＥ８０２．１１ａを、値０ｘ０２はＩＥＥＥ８０２．１１ｂを、その通信情報の送信元がサポートすることを示す。なお「０ｘ」は１６進数であることを意味する。また通信パラメータフィールドに記述された値０ｘ０９は、その通信パラメータがＩＥＥＥ８０２．１１規格におけるＥＳＳＩＤであることを示す。通信パラメータフィールドに記述された値が０ｘ０９であれば、それに続く通信パラメータ長および通信パラメータ値によりＥＳＳＩＤが示される。また、暗号化方式フィールドに記述された値０ｘ１１はＷＥＰ６４ビットを、値０ｘ１２はＷＥＰ１２８ビットを、値０ｘ１３はＷＰＡを、その通信情報の送信元がサポートすることを示す。暗号化鍵種別フィールドの値０ｘ１９は、そのフィールドに続く鍵情報がＷＥＰキーであることを、値０ｘ１ａは、そのフィールドに続く鍵情報がＰｒｅ－Ｓｈａｒｅｄキーであることを示す。暗号化鍵種別フィールドに続けて、鍵長および鍵の値が示される。

【００１８】

図５に、通信装置２から通信装置１へ送信される通信方式および暗号化方式のデータすなわち通信情報の一例を示す。なお、通信装置２のＲＯＭ１０８に保存された通信情報テーブル５０１，５０２には、通信情報そのものが保存されている。したがって、図２，３のステップＳ２０２においては、通信装置２において通信情報テーブル５０１，５０２が読み出されて、その内容が要求に対する応答として通信装置１に対して送信される。同様に、通信装置１のＲＯＭ１０２にも、通信装置１がサポートする通信方式及び暗号化方式を示す通信情報テーブル（本例ではテーブル５０２）が保存されており、受信した通信情報（すなわちテーブル５０１および５０２）と照合される。この例ではテーブル５０２が一致することになる。もちろん通信装置１が複数の通信インターフェースをもつなら、各インターフェースについて通信情報テーブルが保存されている。そこで、各インターフェースに対応する通信情報テーブルそれぞれを、受信した通信情報と照合（あるいは比較）する。一致した通信情報があれば、その通信情報で示される通信方式及び暗号化方式で通信が開始される。なお、複数の通信方式及び暗号化方式が一致した場合には、そのうちのどの方式を用いるかを定めた規則をあらかじめ決めておいても良い。規則の例としては、もっとも通信速度の速い方式を選択したり、あるいは、暗号化強度の最も強い方式を選択するなどの規則がある。各装置がサポートする通信方式及び暗号化方式のうちから、あらかじめ順序を付した表を用意しておくなどすれば、規則にしたがって通信方式及び暗号化方式を選択できる。また、複数の方式が利用可能な場合には、利用者に選択させても良い。この場合には選択肢を示したユーザインターフェースを表示部に表示し、利用者の選択に応じた方式を利用する。

【００１９】

通信装置２にはＮＦＣインターフェース以外に２つの通信インターフェース１１１，１１２が実装されている。そこで、図５の通信情報５０１，５０２の２つのデータが通信装置１へ送信される。通信情報５０１は、通信方式がＩＥＥＥ８０２．１１ａ、ＥＳＳＩＤが“ｗｌａｎ０”、暗号化方式が１２８ビットＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）、暗号鍵種別がＷＥＰキーで暗号鍵値が“ｓａｍｐｌｅｗｅｐｋｅｙ０”であることを示している。この情報は、図４のテーブル４０２にしたがって図５の通信情報５０１に含まれる各コードを読み解くことで得られる。通信情報５０２は、通信方式がＩＥＥＥ８０２．１１ｂ、ＥＳＳＩＤが“ｗｌａｎ１”、暗号化方式が１２８ビットＷＥＰ、暗号鍵種別がＷＥＰキーで暗号鍵値が“ｓａｍｐｌｅｗｅｐｋｅｙ１”であることを示している。

【００２０】

図４、図５は、通信方式および暗号化方式の情報をバイナリデータで表現したものであるが、別の例としてタグ付きのテキストで表現することもできる。その一例を図６に示す。この場合には、通信装置２は図６のテキストデータ６０１，６０２をテーブル５０１，５０２の代わりに持つ。また、通信装置１はテキストデータ６０２をテーブル５０２の代わりに持つ。したがって通信情報を受信した通信装置１では、タグ付きのテキストを最上位のタグ（図６の例では＜８０２．１１ａ＞および＜８０２．１１ｂ＞）単位で、通信情報を比較する。具体的には、通信装置１が持つテキストデータ６０２と、受信したテキストデータ６０１及び６０２とをそれぞれ比較する。

【００２１】

一致したテキストデータがあれば（たとえばテキストデータ６０２）、そのテキストデータを解析して通信方式および暗号化方式の情報を得る。そして得られた情報に従って通信を実行する。

【００２２】

＜通信装置１による制御手順＞

図７に、通信装置１の動作アルゴリズムを示す。ステップＳ７０１では、通信装置１が通信装置２へ近づけられることにより、ＮＦＣインターフェース１０４を使用する通信が開始される。

【００２３】

ステップＳ７０２では、ＮＦＣインターフェース１０４を使用する通信により通信方式および暗号化方式を要求するメッセージを通信装置２へ送信する。

【００２４】

ステップＳ７０３では、図４、図５、図６の例で示されるような通信方式および暗号化方式に関するデータ（通信情報）を通信装置２から受信する。

【００２５】

ステップＳ７０４では、ステップＳ７０３で通信装置２から受信した通信情報で示される通信方式および暗号化方式が、通信装置１に実装されている通信方式および暗号化方式に合致するか否かが判別される。この判定は、上述のように、受信した通信情報と通信装置１が持つ通信情報テーブルとを照合することで行える。通信方式および暗号化方式が合致する場合はステップＳ７０５へ進み、通信方式および暗号化方式が合致しない場合はステップＳ７０９へ進み、処理が続けられる。

【００２６】

通信装置２から受信した通信情報がたとえば図５あるいは図６に示されるような通信情報５０１および通信情報５０２（あるいは６０１と６０２）であるとする。本実施形態においては、通信装置１はＩＥＥＥ８０２．１１ｂインターフェースを実装しているので、通信装置１が持つ通信情報テーブルは通信情報５０２（あるいは６０２）である。したがって、通信情報テーブル５０２は受信した通信情報と合致する。そこで、一致した通信情報で示される通信方式と暗号化方式を用いて、通信装置１と通信装置２とは通信可能である。すなわちこの例では、通信装置１と通信装置２とは、ＩＥＥＥ８０２．１１ｂインターフェースという共通の通信方式をサポートすることがわかる。さらに通信装置１と通信装置２とは、１２８ビットＷＥＰという共通の暗号化方式をサポートすることもわかる。一方、たとえば通信装置１の暗号化方式がＷＰＡ（Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ）あるいは６４ビットＷＥＰの場合は、暗号化方式が合致しないので通信方式および暗号化方式が合致しないと判定される。なおここでいう暗号化方式には暗号鍵の内容も含む。すなわち方式が同じであっても鍵が一致しなければ、方式が一致するとは判定されない。

【００２７】

ステップＳ７０５では、ＮＦＣインターフェース１０４を使用する通信を終了する。ステップＳ７０６では、ステップＳ７０４における判定により、通信装置１と通信装置２とで合致したと判定された共通の通信方式および暗号化方式にしたがって通信を開始する。本実施形態では、ＩＥＥＥ８０２．１１ｂ、１２８ビットＷＥＰで通信を開始する。ステ

ップＳ７０７では、ステップＳ７０６で開始された通信方式でデータ通信を行う。ステップＳ７０８では、ステップＳ７０６で開始された通信方式による通信を終了する。

【００２８】

ステップＳ７０９では、ＮＦＣインターフェース１０４を使用する通信を継続し、データ通信を行う。ステップＳ７１０では、ＮＦＣインターフェース１０４を使用する通信を終了する。

【００２９】

＜通信装置２による制御手順＞

図８に、通信装置２の動作アルゴリズムを示す。ステップＳ８０１では、通信装置１が通信装置２へ近づけられることにより、ＮＦＣインターフェース１１０を使用する通信が開始される。

【００３０】

ステップＳ８０２では、通信装置１から通信方式および暗号化方式を要求するメッセージを受信したか否かを判定する。メッセージを受信したときはステップＳ８０３へ進み、メッセージを受信しないときは再度ステップＳ８０２へ進んでメッセージの受信を待つ。

【００３１】

ステップＳ８０３では、通信方式および暗号化方式の要求に応答して、図４、図５、図６の例に示されるようなデータすなわち通信情報を通信装置２から通信装置１へ送信する。

【００３２】

ステップＳ８０４では、ＮＦＣインターフェース１１０を使用する通信が終了されて通信装置２に実装されているＮＦＣ以外の通信方式で通信が開始されたか否かが判別される。ＮＦＣ以外の通信方式で通信が開始される場合はステップＳ８０５へ進み、ＮＦＣで通信が継続されるばあいはステップＳ８０７へ進み、処理が続けられる。なお、ステップＳ８０４は、実際の処理上は行われなくとも良い。すなわち、ステップＳ８０３でいったん処理を終了し、その後通信装置２は、通信装置１により開始された通信の方式にしたがってステップＳ８０５またはステップＳ８０７のいずれかからデータ通信を実行してもよい。

【００３３】

ステップＳ８０５では、通信装置１により開始された通信方式で通信を行う。ステップＳ８０６では、ステップＳ８０４で開始された通信方式による通信を終了する。

【００３４】

一方ステップＳ８０７では、ＮＦＣインターフェース１１０を使用する通信が継続されてデータ通信を行う。ステップＳ８０８では、ＮＦＣインターフェース１１０を使用する通信を終了する。

【００３５】

以上の構成及び手順により、本実施形態の通信装置は、通信の機密性を確保しつつ通信方式及び暗号化方式に関する情報を取得可能である。また、取得した通信方式にしたがって通信を行う場合でも、通信の機密性を確保できる。また、取得した通信方式で通信を行えない場合でも、確実に通信を行えしかも通信の機密性を確保できるという効果を奏する。

【００３６】

［第２の実施形態］

図９は、本発明の第２の実施形態に係る通信システムの構成および動作概略を示す図である。本発明の第２の実施形態においては、本発明の第１の実施形態における通信装置１に相当するものとしてデジタルカメラ（ＤＳＣ）９０１、通信装置２に相当するものとしてプリンタ９０２が使用されている。

【００３７】

ＤＳＣ９０１をプリンタ９０２に近づけることによりＮＦＣで通信が開始され、プリンタ９０２に実装されている通信方式および暗号化方式を要求するメッセージがＤＳＣ９０

１からプリンタ９０２へ送信される（Ｓ９１１）。
【００３８】
プリンタ９０２に実装されている通信方式がＩＥＥＥ８０２．１１ｂであり、その暗号化方式が１２８ビットＷＥＰである場合、その情報がプリンタ９０２からＤＳＣ９０１へ送信される（Ｓ９１２）。
【００３９】
プリンタ９０２に実装されている通信方式および暗号化方式がＤＳＣ９０１に実装されているか否かが判別される。
【００４０】
ＤＳＣ９０１の通信方式としてＩＥＥＥ８０２．１１ｂが実装されていてその暗号化方式が１２８ビットＷＥＰである場合、通信方式および暗号化方式が合致する。そこで、通信方式をＩＥＥＥ８０２．１１ｂとし、暗号化方式を１２８ビットＷＥＰとする通信が、ＤＳＣ９０１とプリンタ９０２との間で開始され、ＤＳＣ９０１から画像データがプリンタ９０２へ送信される。
【００４１】
たとえばＤＳＣ９０１の通信方式としてＩＥＥＥ８０２．１１ｂが実装されていてその暗号化方式がＷＰＡの場合、通信方式および暗号化方式の一方が合致しないので、ＮＦＣによる通信が継続されてＤＳＣ９０１から画像データがプリンタ９０２へ送信される。
【００４２】
図１０に、ＤＳＣ９０１の動作アルゴリズムを示す。ステップＳ１００１、Ｓ１００２、Ｓ１００３、Ｓ１００４、Ｓ１００５、Ｓ１００６、Ｓ１００７、Ｓ１００８、Ｓ１０１０、Ｓ１０１１は、本発明の第１の実施形態における通信装置１の動作アルゴリズム（図７）に示されるステップＳ７０１、Ｓ７０２、Ｓ７０３、Ｓ７０４、Ｓ７０５、Ｓ７０６、Ｓ７０７、Ｓ７０８、Ｓ７０９、Ｓ７１０とそれぞれ同一の処理である。
【００４３】
ただし、図１０のステップＳ１００９において、ＮＦＣで通信が継続されることをＤＳＣ９０１の使用者へ通知する。たとえば、ＮＦＣで通信できるようにＤＳＣ９０１をプリンタ９０２へ近づけた状態を維持するような指示を、ＤＳＣ９０１の表示部に表示する。一例として、「プリンタと接触させてください」というようなメッセージがＤＳＣ９０１の表示部に表示される。
【００４４】
以上のように本実施形態によれば、第１実施形態の効果に加えて、第１実施形態の通信システムをディジタルカメラ及びプリンタに適用したことで、ディジタルカメラとプリンタとの間で、情報を秘匿した通信を実現することができる。また、ＮＦＣにより通信を行う場合には、その旨を示すメッセージをディジタルカメラに表示することで、利用者に確実な通信環境の構築を促すことができる。
【００４５】
［第３の実施形態］
本発明の第１の実施形態および第２の実施形態では、近距離無線通信方式としてＮＦＣを使用している。これに対して、それ以外の近距離無線通信方式として、赤外線通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ）を使用することもできる。
【００４６】
また、本発明の第１の実施形態および第２の実施形態では、通信を暗号化してセキュリティを確保する無線通信方式としてＩＥＥＥ８０２．１１ａ、ＩＥＥＥ８０２．１１ｂを使用している。これに限らず、数十メートルの通信距離があり、通信を暗号化してセキュリティを確保することができる通信方式ならば、その他の通信方式や今後規格化される通信方式も使用することができる。
【００４７】
また、本発明の第１の実施形態および第２の実施形態では、通信を暗号化する暗号化方

式としてＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）、ＷＰＡ（Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ）を使用している。しかし、その他の暗号化方式や、今後規格化される暗号化方式も使用可能である。

【００４８】

なお本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。また本発明の目的は、前述の実施形態の機能を実現するプログラムコードを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータが記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体およびプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００４９】

また、本発明には、プログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた場合についても、本発明は適用される。その場合、書き込まれたプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される。

【図面の簡単な説明】

【００５０】

【図１】本発明の実施形態に係る通信装置１および通信装置２の構成を示す図。

【図２】本発明の実施形態に係る通信装置１および通信装置２の動作シーケンスおよび動作概念を示す図。

【図３】本発明の実施形態に係る通信装置１および通信装置２の動作シーケンスおよび動作概念を示す図。

【図４】本発明の実施形態に係る通信方式および暗号化方式のデータ構造の一例を示す図。

【図５】本発明の実施形態に係る通信方式および暗号化方式のデータの一例を示す図。

【図６】本発明の実施形態に係る通信方式および暗号化方式のデータの一例を示す図。

【図７】本発明の実施形態に係る通信装置１の動作アルゴリズムを示す図。

【図８】本発明の実施形態に係る通信装置２の動作アルゴリズムを示す図。

【図９】本発明の第２の実施形態に係るデジタルカメラとプリンタで行われる通信の動作概念を示す図。

【図１０】本発明の第２の実施形態に係るデジタルカメラの動作アルゴリズムを示す図。

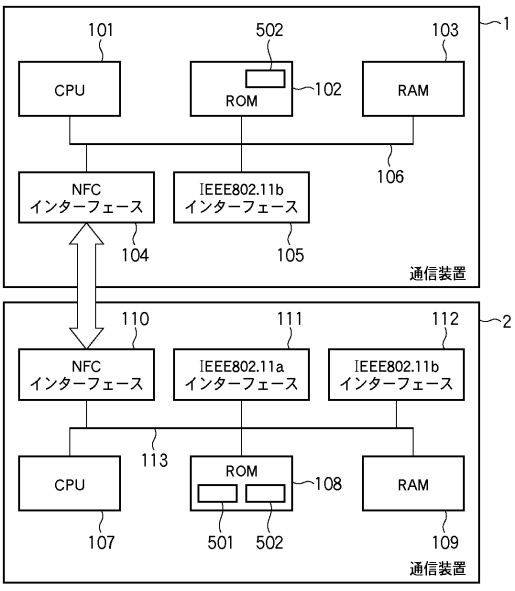
【符号の説明】

【００５１】

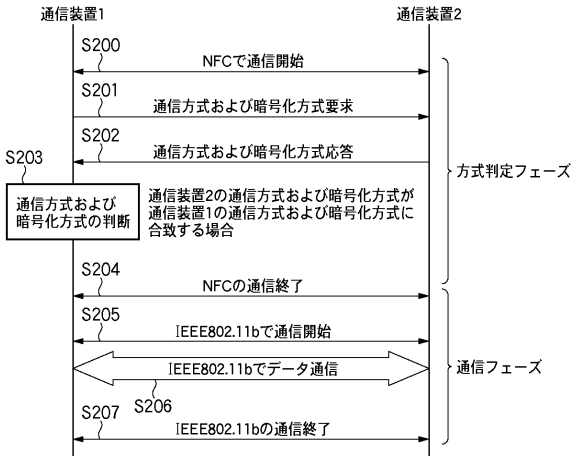
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ
１０４　ＮＦＣインターフェース
１０５　ＩＥＥＥ８０２．１１ｂインターフェース
１０６　バス
１０７　ＣＰＵ
１０８　ＲＯＭ
１０９　ＲＡＭ
１１０　ＮＦＣインターフェース

１１１　ＩＥＥＥ８０２．１１ａインターフェース
１１２　ＩＥＥＥ８０２．１１ｂインターフェース
１１３　バス
９０１　デジタルカメラ（ＤＳＣ）
９０２　プリンタ

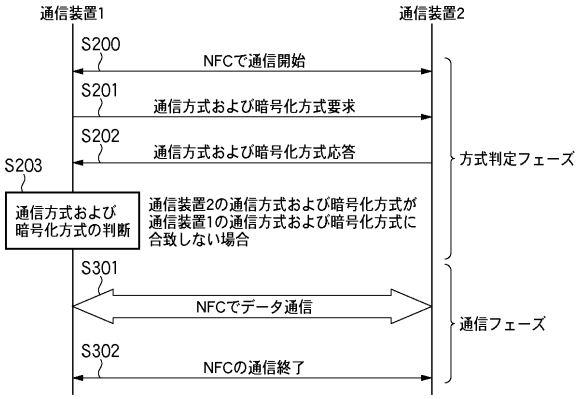
【図１】



【図２】



【図３】



【図４】

通信方式	通信パラメータ	通信パラメータ長
通信パラメータ値		
暗号化方式	暗号鍵種別	暗号鍵長
暗号鍵値		

401

通信方式	0x01	IEEE802.11a
	0x02	IEEE802.11b
通信パラメータ	0x09	ESSID
暗号化方式	0x11	WEP 64 bit
	0x12	WEP 128 bit
	0x13	WPA
暗号鍵種別	0x19	WEP key
	0x1a	Pre-Shared key

402

【図５】

0x01	0x09	0x05	0x77	0x6c	0x61
0x6e	0x30	0x12	0x19	0x0d	0x73
0x61	0x6d	0x70	0x6c	0x65	0x77
0x65	0x70	0x6b	0x65	0x79	0x30

501

0x02	0x09	0x05	0x77	0x6c	0x61
0x6e	0x31	0x12	0x19	0x0d	0x73
0x61	0x6d	0x70	0x6c	0x65	0x77
0x65	0x70	0x6b	0x65	0x79	0x31

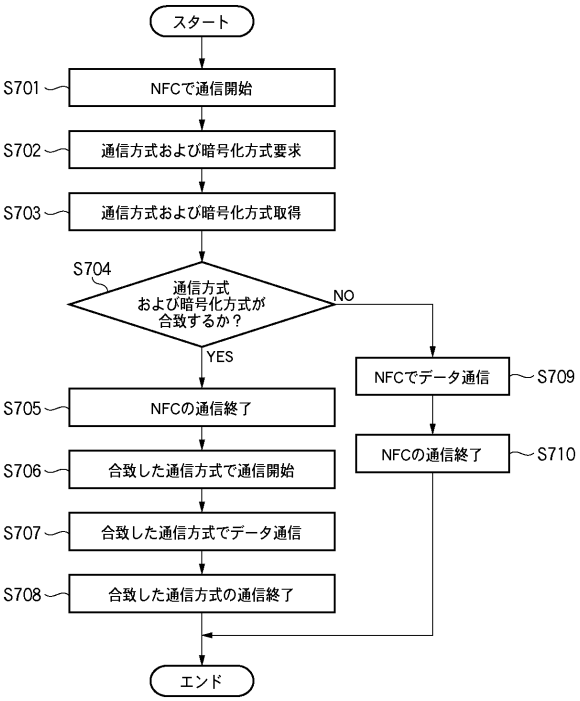
502

【図６】

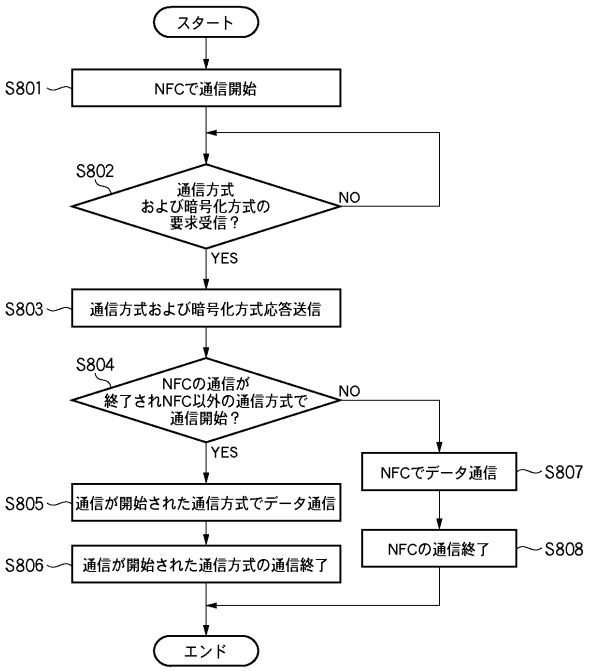
601
602

```
<802.11a>
        <essid>wlan0</essid>
        <security>wep128bit</security>
        <wepkey>samplewepkey0</wepkey>
</802.11a>
<802.11b>
        <essid>wlan1</essid>
        <security>wep128bit</security>
        <wepkey>samplewepkey1</wepkey>
</802.11b>
```

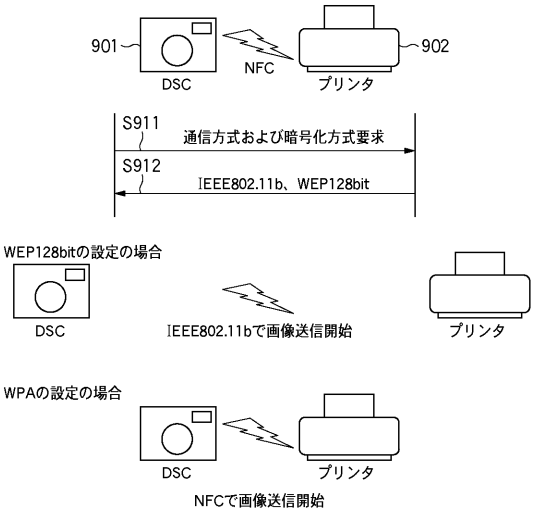
【図７】



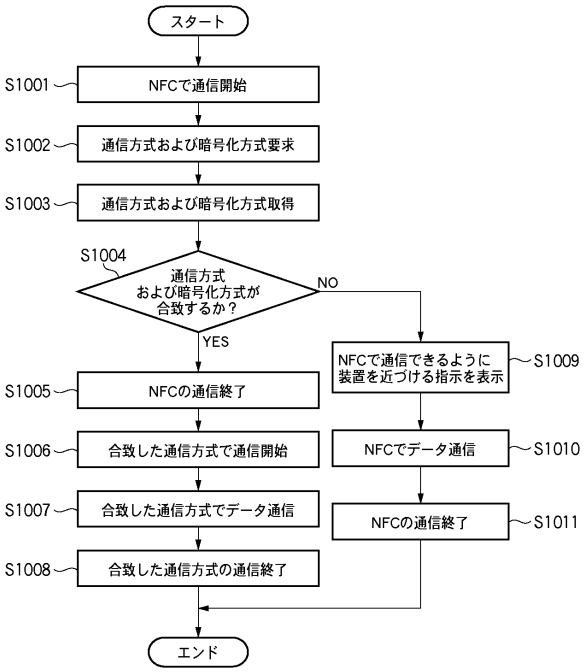
【図８】



【図９】


901
DSC
NFC
プリンタ
902
S911
通信方式および暗号化方式要求
S912
IEEE802.11b、WEP128bit
WEP128bitの設定の場合
DSC
IEEE802.11bで画像送信開始
プリンタ
WPAの設定の場合
DSC
プリンタ
NFCで画像送信開始

【図１０】


スタート
S1001
NFCで通信開始
S1002
通信方式および暗号化方式要求
S1003
通信方式および暗号化方式取得
S1004
通信方式
および暗号化方式が
合致するか？
NO
YES
S1005
NFCの通信終了
S1006
合致した通信方式で通信開始
S1007
合致した通信方式でデータ通信
S1008
合致した通信方式の通信終了
NFCで通信できるように
装置を近づける指示を表示
S1009
NFCでデータ通信
S1010
NFCの通信終了
S1011
エンド

フロントページの続き

(51)Int.Cl. FI
H04L 12/28 300Z

審査官 ▲高▼須 甲斐

(56)参考文献 特開２００５－２１０３２８（ＪＰ，Ａ）
特開２００３－２４２４６１（ＪＰ，Ａ）
特開２００５－０９９９４５（ＪＰ，Ａ）
特開２００４－１３５２５８（ＪＰ，Ａ）
特開２００５－１６７９４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｂ７／２４ － Ｈ０４Ｂ７／２６
Ｈ０４Ｗ４／００ － Ｈ０４Ｗ９９／００
Ｈ０４Ｌ１２／２８