(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4543657号
(P4543657)
(45)発行日　平成22年9月15日(2010.9.15)　(24)登録日　平成22年7月9日(2010.7.9)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 3　(全 24 頁)

(21)出願番号　特願2003-373312(P2003-373312)
(22)出願日　平成15年10月31日(2003.10.31)
(65)公開番号　特開2005-136897(P2005-136897A)
(43)公開日　平成17年5月26日(2005.5.26)
審査請求日　平成18年10月31日(2006.10.31)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　暦本　純一
東京都品川区東五反田３丁目１４番１３号
株式会社ソニーコンピュータサイエンス
研究所内

審査官　速水　雄太

最終頁に続く

(54)【発明の名称】情報処理装置および方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信手段と、
前記接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成手段と、
前記生成手段により生成された前記鍵情報を前記公開鍵により暗号化し、暗号化された前記鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに前記他の情報処理装置に送信する第１の送信手段と、
前記生成手段により生成された前記鍵情報を、有線を介して前記通信管理装置に送信する第２の送信手段と
を備えることを特徴とする情報処理装置。
【請求項２】
他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信ステップと、
前記接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記鍵情報を前記公開鍵により暗号化し、暗号化された前記鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに前記他の情報処理装置に送信する第１の送信ステップと、
前記生成ステップの処理により生成された前記鍵情報を、有線を介して前記通信管理装

置に送信する第２の送信ステップと
を含むことを特徴とする情報処理方法。
【請求項３】
コンピュータを、
他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信手段と、
前記接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成手段と、
前記生成手段により生成された前記鍵情報を前記公開鍵により暗号化し、暗号化された前記鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに前記他の情報処理装置に送信する第１の送信手段と、
前記生成手段により生成された前記鍵情報を、有線を介して前記通信管理装置に送信する第２の送信手段と
して機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信システム、情報処理装置および方法、並びにプログラムに関し、特に、ハードウエアの追加を伴わずに、セキュリティが確保された無線通信を容易にかつ迅速に開始させることができるようにする通信システム、情報処理装置および方法、並びにプログラムに関する。
【背景技術】
【０００２】
近年、IEEE(Institute of Electrical and Electronics Engineers)802.11通信規格やブルートゥース（Bluetooth（登録商標））通信規格に代表される無線通信機能を備える電子機器が普及してきている。
【０００３】
これらの無線通信機能を有する機器間では、プライバシーに関する情報など、機密性が要求される情報も送受信されることから、そのような情報が第三者により盗聴、改竄されること、或いは、不正なネットワークへの侵入を防止するためのセキュリティ対策が必要になる。
【０００４】
例えば、IEEE802.11通信規格では、ユーザは、WEP(Wired Equivalent Privacy)キーと呼ばれる秘密鍵を、通信を行う機器に予め登録し、そのWEPキーを用いた暗号化通信を行わせることにより通信のセキュリティを確保している。また、ディジタル証明書を予め発行し、通信の開始時に、証明書を用いて通信相手の機器の認証を行わせることにより、正当な通信相手であるか否かを判定させ、セキュリティを確保することも行われている。
【０００５】
ところで、セキュリティ確保のために、常に、このような鍵情報の登録や証明書の発行を予め行うとすると、無線通信の接続対象の切り替えに迅速に対応することができない。例えば、２台の携帯機器を一時的に無線で接続し、あるファイルの転送を行うことや、ディジタルカメラを店舗に設置されているプリンタに一時的に無線で接続し、撮影した写真の印刷を行うこと、或いは、ビデオカメラと携帯電話を一時的に無線で接続し、携帯電話を用いてビデオカメラをリモートコントロールすること、などのような一時的な接続などに迅速に対応することができない。
【０００６】
そこで、接続対象を容易に特定し、特定した機器との間で無線通信を迅速に開始させるために、特許文献１には、リーダライタを内蔵するパーソナルコンピュータに、RFタグを内蔵する携帯電話機を近接させることで、RFタグとリーダライタの間で双方の機器の識別情報を送受信させ、その後、送受信された識別情報に基づいて、携帯電話機とパーソナルコンピュータの間でブルートゥース通信を確立させることが開示されている。

【０００７】
また、RFタグとリーダライタによる近距離の無線通信、または、双方の機器に設けられる赤外線モジュールによる近距離の無線通信により、２つの機器間で秘密鍵を共有させることも従来より提案されている。従って、近距離の無線通信で送受信される秘密鍵を用いて、例えば、特許文献１に開示されているようにして確立されるブルートゥース通信を暗号化させることにより、ユーザは、セキュリティが確保されたブルートゥース通信を、双方の機器を近接させるだけで迅速に開始させることができる。
【特許文献１】特開２００２－２０４２３９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、このようにして双方の機器間で識別情報や秘密鍵を送受信させるためには、その双方の機器に、ブルートゥース通信などの比較的離れた位置でも通信を行うことが可能な無線通信モジュールとは別に、RFタグやリーダライタ、或いは、赤外線モジュールなどの近距離の無線通信モジュールが設けられている必要がある。
【０００９】
よって、RFタグや赤外線モジュール等は、単に、それらとは別に設けられた無線通信モジュールによるブルートゥース通信などを確立させるためだけのものであるにもかかわらず、機器を近接させるだけでブルートゥース通信などを迅速に開始させることができるようにするためには用意する必要があり、その分だけコストがかかるという課題があった。
【００１０】
本発明はこのような状況に鑑みてなされたものであり、RFタグや赤外線モジュール等のハードウエアの追加を伴わずに、セキュリティが確保された無線通信を容易にかつ迅速に開始させることができるようにするものである。
【課題を解決するための手段】
【００２０】
本発明の情報処理装置は、他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信手段と、接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成手段と、生成手段により生成された鍵情報を公開鍵により暗号化し、暗号化された鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに他の情報処理装置に送信する第１の送信手段と、生成手段により生成された鍵情報を、有線を介して通信管理装置に送信する第２の送信手段とを備えることを特徴とする。
【００２１】
本発明の情報処理方法は、他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信ステップと、接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成ステップと、生成ステップの処理により生成された鍵情報を公開鍵により暗号化し、暗号化された鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに他の情報処理装置に送信する第１の送信ステップと、生成ステップの処理により生成された鍵情報を、有線を介して通信管理装置に送信する第２の送信ステップとを含むことを特徴とする。
【００２２】
本発明のプログラムは、コンピュータを、他の情報処理装置から送信されてくる公開鍵を含む接続要求を受信する受信手段と、接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報を生成する生成手段と、生成手段により生成された鍵情報を公開鍵により暗号化し、暗号化された鍵情報を、無線通信を管理する通信管理装置に接続するための情報とともに他の情報処理装置に送信する第１の送信手段と、生成手段により生成された鍵情報を、有線を介して通信管理装置に送信する第２の送信手段として機能させるためのプログラムである。
【００２６】

本発明においては、他の情報処理装置から送信されてくる公開鍵を含む接続要求が受信され、接続要求を搬送する電波の受信強度が予め設定されている閾値より高い場合、鍵情報が生成される。また、生成された鍵情報が公開鍵により暗号化され、暗号化された鍵情報が、無線通信を管理する通信管理装置に接続するための情報とともに他の情報処理装置に送信する送信される。生成された鍵情報は、有線を介して通信管理装置に送信される。

【発明の効果】

【００２７】

本発明によれば、容易に、かつ迅速に無線通信を開始させることができる。

【００２８】

また、本発明によれば、煩雑な設定を行うことなく、セキュリティが確保された無線通信を確保することができる。

【００２９】

さらに、本発明によれば、ユーザが意図しない機器との間で無線通信が行われることを防止することができる。

【発明を実施するための最良の形態】

【００４４】

以下、図を参照して本発明の実施の形態について説明する。

【００４５】

図１Ａ，Ｂは、本発明を適用した通信システムにおいて、機器間でアドホック通信を確立させる手順について示す図である。

【００４６】

PDA１と携帯電話機２には、例えば、IEEE(Institute of Electrical and Electronics Engineers)802.11通信規格（IEEE802.11a/b/g等）やブルートゥース（Bluetooth）通信規格に準拠する、電波による無線通信を行うことが可能なモジュールがそれぞれ内蔵されている。

【００４７】

例えば、ユーザがPDA１の表面に設けられるボタンを操作して接続を指示した場合、PDA１から、PDA１のアドレスなどを含む接続要求がブロードキャストされる。図１ＡのようにPDA１と携帯電話機２が近接されており、PDA１からの電波（接続要求を搬送する電波）の受信強度が予め設定されている閾値以上の強度であると判定した場合、携帯電話機２は、PDA１の要求を許可し、PDA１を通信相手とする。

【００４８】

このとき、携帯電話機２は、PDA１との通信で用いる暗号鍵を新たに生成し、生成した暗号鍵と、携帯電話機２のアドレス等の通信パラメータをPDA１に送信する。なお、PDA１からの接続要求には、PDA１により生成された公開鍵も含まれており、その公開鍵により暗号化された暗号鍵（携帯電話機２により生成された暗号鍵）と通信パラメータが携帯電話機２からPDA１に送信される。

【００４９】

PDA１は、接続要求に含めてブロードキャストした公開鍵に対応する秘密鍵（個別鍵）を有していることから、携帯電話機２から送信されてくる暗号鍵と通信パラメータを、その秘密鍵を用いて取得し、図１Ｂの実線矢印で示されるように、IEEE802.11通信規格やブルートゥース通信規格に準拠した無線通信を携帯電話機２との間で確立させる。その後、PDA１と携帯電話機２の間では、携帯電話機２により生成された暗号鍵を用いた暗号化通信が行われる。

【００５０】

このように、一方の機器からブロードキャストされた接続要求の受信強度が閾値以上である場合にのみ、アクセスポイントを介さないpeer-to-peer型のアドホック通信が双方の機器間で開始される。従って、ユーザは、煩雑な設定を行うことなく、無線通信を行いたい機器に自分が保持してる機器を近接させるといった直感的な操作で、迅速に通信を確立させることができる。

【００５１】
また、接続要求を受信した機器である携帯電話機２により生成された暗号鍵による暗号化通信が行われるため、電波の到達範囲内に他の機器がある場合でも、その機器は、PDA１と携帯電話機２の間で送受信される情報を傍受することができない。すなわち、ユーザは、セキュリティも確保された無線通信を迅速に確立させることができる。PDA１と携帯電話機２の間で通信が確立されるまでの処理についてはフローチャートを参照して後述する。
【００５２】
図２は、PDA１の構成例を示すブロック図である。
【００５３】
CPU(Central Processing Unit)１１は、ROM(Read Only Memory)１２または記憶部１８からRAM(Random Access Memory)１３にロードされたプログラムに従って各種の処理を実行する。RAM１３にはまた、CPU１１が各種の処理を実行する上において必要なデータなどが適宜記憶される。
【００５４】
CPU１１、ROM１２、およびRAM１３は、バス１４を介して相互に接続され、このバス１４にはまた、入出力インタフェース１５も接続される。
【００５５】
入出力インタフェース１５には、各種のボタンやジョグダイヤル、或いは、出力部１７を構成する例えばLCD(Liquid Crystal Display)に重畳して設けられるタッチパネルなどからなる入力部１６、LCDなどよりなる表示部やスピーカなどよりなる出力部１７、フラッシュメモリなどよりなる記憶部１８が接続される。
【００５６】
また、入出力インタフェース１５には、IEEE802.11通信規格やブルートゥース通信規格に準拠した無線通信モジュールである無線通信部１９も接続される。無線通信部１９は、バス１４および入出力インタフェース１５を介して行われるCPU１１からの制御に従って、例えば、携帯電話機２との間でIEEE802.11通信規格に準拠した無線通信を行う。
【００５７】
入出力インタフェース１５にはまた、必要に応じてドライブ２０が接続され、磁気ディスク２１、光ディスク２２、光磁気ディスク２３、或いは半導体メモリ２４などが適宜装着される。
【００５８】
図３は、PDA１の機能構成例を示すブロック図である。図３の各機能は、図２のCPU１１により制御プログラムが実行されることで実現される。
【００５９】
無線通信制御部３１は、図２の無線通信部１９における他の機器との無線通信の確立、および、確立された無線通信の制御を行う。また、無線通信制御部３１は、接続要求送信部４１と強度判定部４２を有している。接続要求送信部４１は、ユーザからの指示に応じて、公開鍵およびPDA１のアドレス等を含む接続要求をブロードキャストする。接続要求送信部４１によりブロードキャストされる公開鍵は、鍵情報管理部３４により生成され、供給されるものである。強度判定部４２は、例えば、外部の機器が放射する電波の、無線通信部１９における受信強度を測定し、受信強度が閾値以上の強度であるか否かを判定する。
【００６０】
暗号復号処理部３２は、鍵情報管理部３４から供給される鍵情報を用いて、他の機器に送信する情報の暗号化、および、他の機器から送信されてきた情報が暗号化されている場合に、その復号を行う。
【００６１】
通信パラメータ管理部３３は、例えば、IEEE802.11通信におけるESSID(Extended Service Set ID)や、ブルートゥース通信におけるブルートゥースアドレス、ブルートゥースク

ロックなど、通信を行うために必要な各種のパラメータを管理する。

【００６２】

鍵情報管理部３４は、通信相手の機器から提供される暗号鍵を管理するとともに、公開鍵と、それに対応する秘密鍵を必要に応じて生成し、それらの鍵情報をも管理する。鍵情報管理部３４が管理する鍵情報は、適宜、暗号復号処理部３２に提供される。

【００６３】

なお、図１の携帯電話機２も、ユーザが発話したときに入力される音声信号の処理部や、基地局との通信を行う通信部などがさらに付加される点を除いて、基本的には図２および図３の構成と同様の構成を有している。従って、以下、図２および図３は、携帯電話機２の構成としても適宜引用される。

【００６４】

次に、図４のフローチャートを参照して、図１のPDA１と携帯電話機２により行われる無線通信確立処理について説明する。

【００６５】

例えば、表面に設けられる接続ボタンが押下されたとき、ステップＳ１において、PDA１の入力部１６は、ユーザからの入力（接続ボタンの操作）を受け付ける。

【００６６】

ステップＳ２において、鍵情報管理部３４は、公開鍵Ｐｋと、公開鍵Ｐｋに対応する秘密鍵Ｓｋ（公開鍵Ｐｋで暗号化された情報を復号可能な秘密鍵Ｓｋ）のペアを生成し、管理する。鍵情報管理部３４は、生成した公開鍵Ｐｋを無線通信制御部３１に供給する。このとき、PDA１のアドレス等を含む通信パラメータも通信パラメータ管理部３３から無線通信制御部３１に供給される。

【００６７】

接続要求送信部４１は、ステップＳ３において、無線通信部１９を制御し、公開鍵Ｐｋと通信パラメータを含む接続要求をブロードキャストする。接続要求には暗号化が施されていないため、PDA１１の無線通信部１９から放射される電波の到達範囲内に存在する機器は、この接続要求を受信し、公開鍵Ｐｋ等を取得することができる。

【００６８】

PDA１からの電波の到達範囲内に携帯電話機２がある場合、携帯電話機２の無線通信制御部３１は、ステップＳ２１において、PDA１から送信された接続要求を受信し、接続要求に含まれる公開鍵Ｐｋを暗号復号処理部３２に出力する。携帯電話機２の強度判定部４２は、ステップＳ２２において、接続要求の受信強度（接続要求を搬送する電波の受信強度）を測定し、ステップＳ２３に進み、受信強度が閾値以上の強度であるか否かを判定する。

【００６９】

強度判定部４２は、ステップＳ２３において、接続要求の受信強度が閾値以下であると判定した場合、処理を終了させる。従って、PDA１と携帯電話機２の間の距離が比較的離れている場合、携帯電話機２が接続要求を受信しているときでも、PDA１と携帯電話機２の間ではその後の通信は行われない。

【００７０】

一方、ステップＳ２３において、強度判定部４２は、接続要求の受信強度が閾値以上であると判定した場合、PDA１からの要求を許可し、PDA１を通信相手の機器として特定する。従って、図１Ａに示されるように、携帯電話機２に近接されるPDA１から接続要求がブロードキャストされた場合、PDA１が携帯電話機２の通信相手の機器として特定される。

【００７１】

電波の電界強度（単位面積当たりの電力密度）は、その発信源からの距離の二乗に反比例して減衰することから、接続要求を受信した機器は、接続要求をブロードキャストしている機器が近接されている機器であるのか、または比較的離れた位置にある機器であるのかを、受信する電波の電界強度に基づいて判定することができる。

【００７２】

例えば、携帯電話機２から１０センチメートル離れた位置にある機器から送信されるパケットと、携帯電話機２から１メートル離れた位置にある機器から送信されるパケットとでは、携帯電話機２におけるその受信強度は１０倍異なるため（携帯電話機２から１０センチメートル離れた位置にある機器から送信されるパケットの方が、受信強度が１０倍高いため）、出力に多少のばらつきがあったとしても、接続要求を受信する機器は、それを送信する機器が、近接されている機器であるのか否かをほぼ確実に判定することができる。

【００７３】

図４の説明に戻り、PDA１を通信相手の機器として特定した場合、携帯電話機２の鍵情報管理部３４は、ステップＳ２４において、共通鍵であるセッションキーＳを生成する。セッションキーＳは、PDA１との間で無線通信が確立された後に、送受信される情報の暗号化、暗号化された情報の復号に用いられる。なお、セッションキーＳは、このときの接続のためにランダムに生成されたものであり、図４の一連の処理毎に異なるキーが生成される。鍵情報管理部３４が生成したセッションキーＳと、通信パラメータ管理部３３が管理する携帯電話機２のアドレス等の通信パラメータは暗号復号処理部３２に出力される。

【００７４】

ステップＳ２５において、暗号復号処理部３２は、セッションキーＳと通信パラメータ（Ｚ＝（セッションキーＳ、通信パラメータ））を、PDA１から提供された公開鍵Ｐｋを用いて暗号化し、暗号化が施された情報を無線通信制御部３１に供給する。ステップＳ２６において、無線通信制御部３１は、公開鍵Ｐｋにより暗号化が施されたセッションキーＳと通信パラメータをack(Ｚ)（acknowledge(Ｚ)）としてPDA１に返信する。このように、携帯電話機２により生成されたセッションキーＳは、公開鍵Ｐｋにより暗号化されてPDA１に返信されるため、秘密鍵Ｓｋを有するPDA１のみがセッションキーＳを復号し、取得することができる。

【００７５】

PDA１の無線通信制御部３１は、ステップＳ４において、携帯電話機２から返信されるack(Ｚ)を受信し、受信したack(Ｚ)を暗号復号処理部３２に出力する。

【００７６】

ステップＳ５において、PDA１の暗号復号処理部３２は、鍵情報管理部３４が管理する秘密鍵Ｓｋを用いて、携帯電話機２から返信されたack(Ｚ)を復号し、通信パラメータと、携帯電話機２により生成されたセッションキーＳを取得する。

【００７７】

ステップＳ６において、無線通信制御部３１は、暗号復号処理部３２により取得された通信パラメータを用いて、IEEE802.11通信規格やブルートゥース通信規格に準拠した無線通信を携帯電話機２との間で確立させる。一方、ステップＳ２７において、携帯電話機２は、PDA１からの接続要求に含まれる通信パラメータに基づいて、IEEE802.11通信規格やブルートゥース通信規格に準拠した無線通信をPDA１との間で確立させる。

【００７８】

このとき、PDA１と携帯電話機２の間では、IEEE802.11通信規格に準拠した無線通信の場合、双方の機器のMAC(Media Access Control)アドレス、IPアドレス、ESSID等の設定や、セッションキーＳをWEP(Wired Equivalent Privacy)キーとして用いることの設定などが行われる。また、ブルートゥース通信規格に準拠した無線通信の場合、ブルートゥースアドレスやブルートゥースクロックに基づく設定や、セッションキーＳを暗号鍵として用いることの設定などが行われる。

【００７９】

各種の設定が行われた後、セッションキーＳにより暗号化が施された無線通信がPDA１と携帯電話機２の間で開始される。なお、ここで開始される無線通信は、必ずしも双方の機器が近接されている必要はなく、電波の届く範囲内で有効なものである。

【００８０】

以上のように、電波の受信強度に基づいて通信相手とするか否かを判定するようにした

ため、ユーザは、機器同士を近接させるだけで無線通信を開始させることができる。

【００８１】

また、IEEE802.11通信規格やブルートゥース通信規格の無線通信モジュール（図２の無線通信部１９）を用いて、機器が近接されているか否かを判定したり、通信パラメータを送受信したりするようにしたため、RFタグ、リーダライタ、赤外線モジュールなどの、近接されている機器を検出したり、通信を確立するために必要な情報を送受信したりするためだけの専用のモジュールを機器に用意する必要がない。従って、そのような専用のモジュールを用意する場合に較べて、機器の製造コストを抑えることができる。

【００８２】

さらに、新たに生成されたセッションキーにより暗号化された無線通信が行われるため、第三者による盗聴や改竄等を防止することができる。

【００８３】

図５は、図４の処理の具体例として、図１のPDA１と携帯電話機２の間でIEEE802.11通信規格に準拠した無線通信が確立されるまでの処理について説明するフローチャートである。図５の処理は、基本的には図４の処理と同様であり、詳細な説明については適宜省略する。

【００８４】

ユーザによる接続ボタンの操作がステップＳ４１において入力部１６により受け付けられたとき、ステップＳ４２において、PDA１の鍵情報管理部３４は、公開鍵Ｐｋと秘密鍵Ｓｋのペアを生成する。接続要求送信部４１は、ステップＳ４３において、鍵情報管理部３４が生成した公開鍵Ｐｋと、通信パラメータ管理部３３が管理する通信パラメータを含む接続要求をブロードキャストする。

【００８５】

PDA１からの電波の到達範囲内に存在する携帯電話機２の無線通信制御部３１は、ステップＳ６１において接続要求を受信する。ステップＳ６２において、強度判定部４２は、接続要求の受信強度を測定し、ステップＳ６３に進み、受信強度が閾値以上の強度であるか否かを判定する。

【００８６】

強度判定部４２は、ステップＳ６３において、接続要求の受信強度が閾値以上の強度ではないと判定した場合、処理を終了させ、一方、閾値以上の強度であると判定した場合、PDA１を通信相手の機器として特定する。PDA１が通信相手の機器として特定された場合、ステップＳ６４において、携帯電話機２の鍵情報管理部３４は、PDA１とのIEEE802.11通信規格の無線通信で用いるWEPキーを新たに生成し、通信パラメータ管理部３３は、その通信を識別するESSIDを新たに生成する。生成されたESSIDとWEPキーは暗号復号処理部３２に出力される。

【００８７】

ステップＳ６５において、暗号復号処理部３２は、ESSIDとWEPキー（Ｚ＝（ESSID、WEPキー））を、公開鍵Ｐｋを用いて暗号化し、暗号化が施された情報を無線通信制御部３１に供給する。ステップＳ６６において、無線通信制御部３１は、暗号化が施されたESSIDとWEPキーを含むack(Ｚ)をPDA１に返信する。このように、新たに生成されたESSIDとWEPキーは、PDA１から提供された公開鍵Ｐｋにより暗号化されてPDA１に返信されるため、秘密鍵Ｓｋを有するPDA１のみがESSIDとWEPキーを復号し、取得することができる。

【００８８】

PDA１の無線通信制御部３１は、ステップＳ４４において、携帯電話機２から返信されたack(Ｚ)を受信し、ステップＳ４５において、暗号復号処理部３２は、鍵情報管理部３４が管理する秘密鍵Ｓｋを用いてack(Ｚ)を復号し、携帯電話機２により生成されたESSIDとWEPキーを取得する。

【００８９】

ステップＳ４６において、無線通信制御部３１は、取得されたESSIDとWEPキーに基づいて、IEEE802.11通信規格に準拠した無線通信を携帯電話機２との間で確立させる。一方、

ステップＳ６７において、携帯電話機２の無線通信制御部３１は、PDA１の無線通信制御部３１と同様に、接続要求に含まれる情報に基づいて、IEEE802.11通信規格に準拠した無線通信をPDA１との間で確立させる。

【００９０】

以上のように、ユーザは、機器同士を近接させることで、セキュリティが確保されたIEEE802.11通信規格に準拠した無線通信をそれらの機器間で確立させることができる。また、その無線通信を確立させるために、IEEE802.11通信規格の通信モジュール以外の近距離通信用のモジュールが双方の機器に設けられている必要はない。

【００９１】

ここで、図６のフローチャートを参照して、図１のPDA１と携帯電話機２により行われる他の無線通信確立処理について説明する。

【００９２】

図６の処理は、携帯電話機２からPDA１に返信されるack(Ｚ)の受信強度が閾値以上の強度であるか否かがPDA１により判定される点を除いて、図４を参照して説明した処理と同様であり、重複する説明を適宜省略する。

【００９３】

公開鍵Ｐｋにより暗号化が施されたセッションキーＳと通信パラメータを含むack(Ｚ)がステップＳ８４においてPDA１の無線通信制御部３１により受信された場合、ステップＳ８５において、PDA１の強度判定部４２は、ack(Ｚ)を搬送する電波の受信強度が閾値以上の強度であるか否かを判定する。強度判定部４２は、ステップＳ８５において、受信強度が閾値以下の強度しかないと判定した場合、例えば、通信を行うことができないことを携帯電話機２に通知し、処理を終了させる。

【００９４】

これにより、例えば、接続要求を送信する時点（ステップＳ８３の処理が行われる時点）では近接されていたが、その直後に離された場合、PDA１と携帯電話機２の間では無線通信が行われない。

【００９５】

ステップＳ８５において、携帯電話機２からの返信の受信強度が閾値以上の強度であると判定した場合、すなわち、PDA１と携帯電話機２が近接している状態が継続していると判定した場合、ステップＳ８６に進み、PDA１の暗号復号処理部３２は、秘密鍵Ｓｋを用いてack(Ｚ)を復号し、携帯電話機２により生成されたセッションキーＳと通信パラメータを取得する。その後、無線通信制御部３１は、暗号復号処理部３２により取得されたセッションキーＳと通信パラメータを用いて、携帯電話機２との間で無線通信を確立させる。

【００９６】

以上のように、接続要求に対する返信の受信強度をPDA１においても判定させることにより、無線通信を確立させる機器をより確実に特定させることができ、ユーザが意図しない機器との間で無線通信が確立されるのを防止することができる。

【００９７】

また、実際には近接されておらず、離れた位置から出力を大にして接続要求をブロードキャストする機器との間でも通信は行われないことになる。すなわち、接続要求に対する返信の受信強度の判定がPDA１において行われない場合、PDA１が、携帯電話機２と離れた位置から出力を大にして接続要求をブロードキャストすることにより、PDA１が近接されていると携帯電話機２により判定され（ステップＳ１０３の処理により受信強度が閾値以上であると判定され）、その後、PDA１と携帯電話機２の間で無線通信が確立されることになるが、PDA１でも電波の受信強度を判定させることにより、そのような無線通信の確立を防止することができる。すなわち、実際に近接されている機器間でのみ、通信が確立されることになる。

【００９８】

なお、双方の機器が出力を大にして接続要求とそれに対する返信（ack(Ｚ)）を送信し

た場合、近接していない場合でもそれらの機器間で通信が確立されてしまうことから、ブロードキャストされる接続要求と、それに対する返信に、電波の出力レベルを表す情報が含まれるようにしてもよい。

【００９９】

また、接続要求を送信したPDA１において、携帯電話機２からの返信の受信強度を測定し、通信を行うか否かを判定するのではなく、ack(Ｚ)を搬送する電波が狭い範囲内にのみ到達するように、携帯電話機２からの返信の出力が制限されるようにしてもよい。これによっても、離れた位置から出力を大にして接続要求をブロードキャストする機器と、それを受信する機器との間で通信が確立されるのを防止することができる。

【０１００】

以上においては、機器同士を近接させることによりアドホック通信を確立させる場合について説明したが、同様に、機器をアクセスポイントに近接させることによりインフラストラクチャ通信を確立させることもできる。

【０１０１】

図７Ａ，Ｂは、本発明を適用した通信システムにおいて、インフラストラクチャ通信を確立させる手順について示す図である。

【０１０２】

アクセスポイント５１には、PDA１と同様に、例えば、IEEE802.11通信規格やブルートゥース通信規格に準拠する無線通信モジュールが内蔵されている。

【０１０３】

例えば、図７Ａに示されるように、ユーザが、自身が保持するPDA１をアクセスポイント５１に近接させた状態でアクセスポイント５１への接続を指示した場合、PDA１から接続要求がブロードキャストされる。アクセスポイント５１において、その受信強度が予め設定されている閾値以上の強度であると判定されたとき、ESSID等の通信パラメータやWEPキーがアクセスポイント５１により生成される。生成された通信パラメータとWEPキーは、接続要求に含めてPDA１からアクセスポイント５１に提供された公開鍵で暗号化された後、PDA１に返信され、そのESSIDとWEPキーに基づいて、アクセスポイント５１に対する接続がPDA１により行われる。

【０１０４】

また、PDA１がアクセスポイント５１に接続する前に、他の機器が属するネットワークがアクセスポイント５１により既に管理されている場合、その機器に対して、新たに生成されたESSIDとWEPキーが通知され、それぞれの機器で設定の変更が行われる。これにより、アクセスポイント５１に既に接続していた機器と、新たにアクセスポイント５１に接続したPDA１を含むネットワークが形成される。

【０１０５】

例えば、図７Ｂに示されるように、PDA１がアクセスポイント５１に接続する前に、機器５２と機器５３からなるネットワークがアクセスポイント５１により管理されていた場合、PDA１からの接続要求を受信することに応じて新たに生成されたESSIDとWEPキーが機器５２と機器５３にも通知され、それぞれの機器において設定の変更が行われる。これにより、PDA１、機器５２、機器５３からなるネットワーク６１が新たに形成される（インフラストラクチャ接続型の無線通信が確立される）。

【０１０６】

従って、ユーザは、他の機器に設定されているものと同じESSIDとWEPキーをPDA１に設定するなどの煩雑な操作を行うことなく、アクセスポイント５１にPDA１を近接させるだけで、PDA１をネットワークに迅速に参加させることができる。

【０１０７】

また、アクセスポイント５１により新たに生成されたESSIDとWEPキーによりネットワークの設定が各機器において変更されるため、よりセキュアなネットワークを形成することができる。例えば、ESSIDやWEPキーが悪意のある者に知られた場合でも、新たな機器がネットワークに参加する毎にESSIDやWEPキーが更新されることから、悪意のある者に知られ

たESSIDとWEPキーでは、設定が更新されたネットワークで送受信される情報の盗聴等を行うことが不可能になる。

【０１０８】

図８は、アクセスポイント５１の機能構成例を示すブロック図である。なお、アクセスポイント５１も基本的には図２に示されるPDA１の構成と同様の構成を有している。従って、適宜、図２をアクセスポイント５１の構成としても引用する。

【０１０９】

図８の無線通信制御部７１は、図２の無線通信部１９において行われる他の機器との無線通信を制御する。無線通信制御部７１は、ネットワーク管理部８１と強度判定部８２を有しており、そのうちのネットワーク管理部８１は、ネットワークに参加する機器に対して、ルータ機能やDHCP(Dynamic Host Configuration Protocol)機能を提供とともに、新たに生成したESSIDやWEPキーを、ネットワークに既に参加している機器に通知する処理などを行う。強度判定部８２は、図３のPDA１の強度判定部４２と同様に、外部の機器が放射する電波の受信強度を測定し、受信強度が予め設定されている閾値以上の強度であるか否かを判定する。

【０１１０】

暗号復号処理部７２は、他の機器に送信する情報の暗号化、および、他の機器から送信されてきた情報が暗号化されている場合に、その復号を行う。

【０１１１】

通信パラメータ管理部７３は、例えば、IEEE802.11通信におけるESSIDや、ブルートゥース通信におけるブルートゥースアドレス、ブルートゥースクロックなど、通信を行うために必要な各種のパラメータを管理する。

【０１１２】

鍵情報管理部７４は、ネットワークに参加する機器に提供するWEPキー等の暗号鍵を生成する。

【０１１３】

次に、図９のフローチャートを参照して、図７ＡのPDA１とアクセスポイント５１の間で行われる無線通信確立処理について説明する。

【０１１４】

操作ボタンが押下され、ネットワークに参加することがユーザにより指示された場合、ステップＳ１２１において、PDA１の入力部１６はそれを受け付け、ステップＳ１２２において、鍵情報管理部３４は、公開鍵Ｐｋと、公開鍵Ｐｋに対応する秘密鍵Ｓｋを生成する。接続要求送信部４１は、ステップＳ１２３において、公開鍵Ｐｋと通信パラメータを含む接続要求をブロードキャストする。

【０１１５】

PDA１からの電波の到達範囲内に存在するアクセスポイント５１の無線通信制御部７１は、ステップＳ１４１において、PDA１によりブロードキャストされた接続要求を受信する。ステップＳ１４２において、アクセスポイント５１の強度判定部８２は、接続要求の受信強度を測定し、ステップＳ１４３に進み、測定した受信強度が閾値以上の強度であるか否かを判定する。

【０１１６】

強度判定部８２は、ステップＳ１４３において、接続要求の受信強度が閾値以下の強度であると判定した場合、処理を終了させ、一方、閾値以上の強度であると判定した場合、PDA１からの要求を許可し、ネットワークへの参加を承認する。

【０１１７】

ステップＳ１４４において、アクセスポイント５１の通信パラメータ管理部７３と鍵情報管理部７４は、ESSIDとWEPキーをそれぞれ新たに生成し、生成したESSIDとWEPキーを暗号復号処理部７２に出力する。

【０１１８】

ステップＳ１４５において、暗号復号処理部７２は、ESSIDとWEPキー（Ｚ＝（ESSID、W

EPキー））を、PDA１から提供された公開鍵Ｐｋを用いて暗号化し、暗号化が施された情報を無線通信制御部７１に出力する。ステップＳ１４６において、ネットワーク管理部８１は、暗号化が施されたESSID、WEPキーをack(Ｚ)としてPDA１に返信する。

【０１１９】

また、複数の機器からなるネットワークを既に管理している場合、ネットワーク管理部８１は、ステップＳ１４７において、ネットワークに参加する全ての機器に対して、ステップＳ１４４で生成したESSIDとWEPキーを提供し、それぞれの機器における設定を更新させる。新たに生成されたESSIDとWEPキーは、例えば、ネットワーク内でそれまで用いられていたWEPキーにより暗号化されて各機器に送信されるため、新たに生成されたESSIDとWEPキーが第三者により傍受されることはない。

【０１２０】

一方、PDA１の無線通信制御部３１は、ステップＳ１２４において、アクセスポイント５１から返信されるack(Ｚ)を受信し、ステップＳ１２５において、暗号復号処理部３２は、秘密鍵Ｓｋを用いてack(Ｚ)を復号し、アクセスポイント５１により生成されたESSIDとWEPキーを取得する。

【０１２１】

ステップＳ１２６において、無線通信制御部３１は、暗号復号処理部３２により取得されたESSIDとWEPキーに基づいてアクセスポイント５１に接続し、アクセスポイント５１が管理するネットワークに参加する。

【０１２２】

これにより、アクセスポイント５１により新たに生成されたESSIDで識別される機器からなるインフラストラクチャ接続型のネットワークが形成され、それらの機器の間で、アクセスポイント５１を介した情報を送受信することが可能になる。

【０１２３】

以上のように、インフラストラクチャ通信であっても、ユーザは、RFタグやリーダライタなどのモジュールをIEEE802.11通信規格などのモジュールとは別に用意することなく、自分が保持する機器をアクセスポイントに近接させるだけで、それを確立し、ネットワークを構築することができる。また、ESSIDやWEPキーが新たに生成され、それによりネットワークに参加する各機器において設定が変更されるため、ユーザは、よりセキュアなネットワークを構築することができる。

【０１２４】

以上においては、ユーザは、自分が保持する機器をアクセスポイントに近接させることにより、機器をネットワークに参加させるとしたが、このアクセスポイントは、例えば、屋内の天井付近などの、ユーザが機器を近接させることができないような場所に設置されていることが多い。従って、天井付近などに設置されているアクセスポイントとは別に、ユーザが機器を容易に近接させることができるような場所に、新たに生成したESSIDやWEPキーを提供するのみで、ネットワークを管理する機能を有さないダミーポイントを設置するようにしてもよい。この場合、ユーザは、自分が保持する機器をダミーポイントに近接させることで、その機器を、アクセスポイントにより管理されるネットワークに参加させることができる。

【０１２５】

図１０Ａ，Ｂは、本発明を適用した通信システムにおいて、ダミーポイントに機器を近接させることでインフラストラクチャ通信を確立させる手順について示す図である。

【０１２６】

図１０Ａのダミーポイント１０１－１、ダミーポイント１０１－２は、アクセスポイント５１とは異なり、ユーザがPDA１を容易に近接させることができる場所に設置され、それぞれ、ケーブル１１１－１、ケーブル１１１－２を介して有線でアクセスポイント５１に接続されている。

【０１２７】

ダミーポイント１０１－１およびダミーポイント１０１－２は、IEEE802.11通信規格や

ブルートゥース通信規格に準拠した無線通信機能を有し、電波の受信強度から、PDA１が近接されたと判定した場合、新たに生成するESSIDやWEPキーをPDA１に提供する。また、このとき、ダミーポイント１０１－１、ダミーポイント１０１－２は、PDA１に提供したものと同じESSIDとWEPキーをケーブル１１１－１、ケーブル１１１－２を介してアクセスポイント５１に送信する。

【０１２８】

その後の処理は、図７Ａ，Ｂの場合と同様である。すなわち、アクセスポイント５１は、ダミーポイント１０１－１またはダミーポイント１０１－２から通知されたESSIDとWEPキーを、ネットワークに既に参加している全ての機器に通知して設定を更新させるとともに、ダミーポイント１０１－１またはダミーポイント１０１－２からESSIDとWEPキーを取得したPDA１の接続を許可し、図１０Ｂに示されるように、PDA１を含むネットワーク６１を形成する。

【０１２９】

これにより、PDA１を近接させることができない場所にアクセスポイント５１が設置されている場合でも、ユーザは、ダミーポイント１０１－１またはダミーポイント１０１－２にPDA１を近接させることで、アクセスポイント５１が管理するネットワークにPDA１を参加させることができる。

【０１３０】

図１１は、アクセスポイント５１とダミーポイント１０１－１の機能構成例を示すブロック図である。なお、ダミーポイント１０１－２も、図１１に示されるダミーポイント１０１－１の構成と同様の構成を有し、アクセスポイント５１に接続される。また、図８のアクセスポイント５１と同じ部分には同じ符号を付してある。

【０１３１】

ダミーポイント１０１－１も、ネットワークを管理する機能部が設けられていない点を除いて図８のアクセスポイント５１と同様の構成を有している。すなわち、無線通信制御部１２１は、近接された機器との間で行われるIEEE802.11通信規格やブルートゥース通信規格に準拠した無線通信を制御し、強度判定部１３１は、外部の機器から放射される電波の受信強度を測定し、受信強度が予め設定されている閾値以上の強度であるか否かを判定する。

【０１３２】

暗号処理部１２２は、接続要求に含めてPDA１から提供される公開鍵Ｐｋを用いて、通信パラメータ管理部１２３により生成されるESSIDと鍵情報管理部１２４により生成されるWEPキーに暗号化を施し、無線通信制御部１２１からPDA１に提供させる。

【０１３３】

通信パラメータ管理部１２３は、ESSIDなどの通信パラメータを管理し、鍵情報管理部１２４は、近接されたPDA１等に提供するWEPキーを生成する。通信パラメータ管理部１２３が管理するESSIDと鍵情報管理部１２４が管理するWEPキーは、暗号処理部１２２に出力されるとともに、有線通信制御部１２５にも出力される。

【０１３４】

有線通信制御部１２５は、アクセスポイント５１との間の有線の通信を管理し、通信パラメータ管理部１２３から供給されたESSIDと鍵情報管理部１２４から供給されたWEPキーをケーブル１１１－１を介してアクセスポイント５１に送信する。

【０１３５】

アクセスポイント５１の有線通信制御部１４１は、ダミーポイント１０１－１から送信されてくるESSIDとWEPキーを受信し、それを無線通信制御部７１に出力する。無線通信制御部７１のネットワーク管理部８１は、ネットワークに参加している全ての機器に、ダミーポイント１０１－１から送信されてきたESSIDとWEPキーを無線で送信し、設定を更新させる。また、ネットワーク管理部８１は、ダミーポイント１０１－１から提供されるESSIDとWEPキーを取得したPDA１からの接続を許可し、PDA１をネットワークに参加させる。

【０１３６】

次に、図１２のフローチャートを参照して、図１０ＡのPDA１、アクセスポイント５１、ダミーポイント１０１－１により行われる通信確立処理について説明する。

【０１３７】

PDA１がダミーポイント１０１－１に近接されることで、PDA１とダミーポイント１０１－１の間で行われる処理は、図５、図９等を参照して説明したPDA１とアクセスポイント５１の間で行われる処理と同様である。

【０１３８】

すなわち、ステップＳ１８１において、PDA１の入力部１６は、例えば、ダミーポイント１０１－１にPDA１が近接された状態でユーザにより行われる接続ボタンの操作を受け付け、ステップＳ１８２において、鍵情報管理部３４は、公開鍵Ｐｋと、公開鍵Ｐｋに対応する秘密鍵Ｓｋを生成する。接続要求送信部４１は、ステップＳ１８３において、公開鍵Ｐｋと通信パラメータを含む接続要求をブロードキャストする。

【０１３９】

ダミーポイント１０１－１の無線通信制御部１２１は、ステップＳ１６１において、PDA１からブロードキャストされた接続要求を受信する。ステップＳ１６２において、強度判定部１３１は、接続要求の受信強度を測定し、ステップＳ１６３に進み、受信強度が閾値以上の強度であるか否かを判定する。

【０１４０】

強度判定部１３１は、ステップＳ１６３において、接続要求の受信強度が閾値以上の強度ではないと判定した場合、処理を終了させ、一方、閾値以上の強度であると判定した場合、ステップＳ１６４に進む。

【０１４１】

ステップＳ１６４において、ダミーポイント１０１－１の通信パラメータ管理部１２３は、ESSIDを新たに生成し、生成したESSIDを暗号処理部１２２と有線通信制御部１２５に出力する。また、鍵情報管理部１２４は、WEPキーを新たに生成し、生成したWEPキーを暗号処理部１２２と有線通信制御部１２５に出力する。

【０１４２】

ステップＳ１６５において、暗号処理部１２２は、ESSIDとWEPキー（Ｚ＝（ESSID、WEPキー））を公開鍵Ｐｋを用いて暗号化し、暗号化が施された情報を無線通信制御部１２１に出力する。ステップＳ１６６において、無線通信制御部１２１は、暗号化が施されたESSIDとWEPキーをack(Ｚ)としてPDA１に返信する。

【０１４３】

ステップＳ１６７において、有線通信制御部１２５は、通信パラメータ管理部１２３から供給されたESSIDと、鍵情報管理部１２４から供給されたWEPキーをケーブル１１１－１を介して有線でアクセスポイント５１に送信する。このとき、ESSIDとWEPキーの他、PDA１のMACアドレス等の情報もアクセスポイント５１に送信され、アクセスポイント５１におけるアクセス制御に用いられる。

【０１４４】

一方、ステップＳ１８４において、PDA１の無線通信制御部３１は、ダミーポイント１０１－１から返信されたack(Ｚ)を受信し、ステップＳ１８５において、暗号復号処理部３２は、秘密鍵Ｓｋを用いてack(Ｚ)を復号し、ESSIDとWEPキーを取得する。

【０１４５】

ステップＳ１８６において、無線通信制御部３１は、暗号復号処理部３２により取得されたESSIDとWEPキーに基づいて、IEEE802.11通信規格に準拠した無線通信を確立させ、アクセスポイント５１に接続する。このとき、ステップＳ２０１において、有線を介して送信されてくるESSIDとWEPキーを受信したアクセスポイント５１のネットワーク管理部８１は、ステップＳ２０２に進み、そのESSIDとWEPキーを、ネットワークに既に参加している機器に無線を介して送信し、設定を更新させる。

【０１４６】

これにより、ダミーポイント１０１－１により新たに生成されたESSIDで識別される、P

DA１を含む機器のグループによりインフラストラクチャ接続型のネットワークが確立され、ネットワーク間で、アクセスポイント５１を介した情報の送受信が行われる。

【０１４７】

以上の処理により、アクセスポイント５１がPDA１を直接近接させることができない場所に設置されている場合でも、ユーザは、ダミーポイント１０１－１等にPDA１を近接させることで、アクセスポイント５１が管理するネットワークにPDA１を参加させることができる。

【０１４８】

なお、PDA１がダミーポイントに近接されたとき、ESSIDやWEPキー等の情報の他に、あるサイトのURL(Uniform Resource Locator)がダミーポイントからPDA１に提供され、図１２の処理によりPDA１がアクセスポイント５１に接続した後、アクセスポイント５１を介して、URLで指定されるサイトにPDA１によるアクセスが行われるようにしてもよい。

【０１４９】

図１３は、ダミーポイントから提供されるURLに基づいて、PDA１によりアクセスポイント５１への接続が行われ、続けて、URLで指定されるサイトへのアクセスが行われる通信システムの構成例を示す図である。

【０１５０】

図１３においては、壁面に、LCDなどのディスプレイやポスターなどよりなる提示部１５１－１乃至１５１－３が設けられている。例えば、提示部１５１－１によりカメラの広告が提示され、提示部１５１－２により地図が提示され、提示部１５１－３によりパーソナルコンピュータの広告が提示されている。

【０１５１】

提示部１５１－１乃至１５１－３の直下には、それぞれ、図示せぬケーブルを介してアクセスポイント５１に接続されるダミーポイント１０１－１乃至１０１－３が設けられる。なお、アクセスポイント５１は、壁面より上の、ユーザがPDA１を近接させることが困難な場所に設置されている。

【０１５２】

ダミーポイント１０１－１は、アクセスポイント５１に接続するためのESSIDやWEPキーの他に、提示部１５１－１が提示するカメラの詳細な情報を提供する広告サイトのURLをPDA１に提供し、ダミーポイント１０１－２は、ESSIDやWEPキーの他に、提示部１５１－２が提示する地図の詳細な情報を提供するサイトのURLをPDA１に提供する。また、ダミーポイント１０１－３は、アクセスポイント５１に接続するためのESSIDやWEPキーの他に、提示部１５１－３が提示するパーソナルコンピュータの詳細な情報を提供する広告サイトのURLをPDA１に提供する。

【０１５３】

従って、例えば、図１３に示されるように、ユーザがダミーポイント１０１－１にPDA１を近接させた場合、PDA１により、図１２の処理によりアクセスポイント５１に対する接続が行われ、その後、ダミーポイント１０１－１から提供されるURLに基づいて、提示部１５１－１が提示するカメラの広告サイトに対するアクセスが行われる。カメラの広告サイトへのアクセスが行われたとき、PDA１の画面上には、カメラの詳細な情報が表示される。従って、ユーザは、PDA１を広告（ダミーポイント）に近接させるだけで、その広告が紹介する商品の詳細な情報をPDA１の画面上で確認することができる。

【０１５４】

なお、図１３の例においては、提示部１５１－１乃至１５１－３とダミーポイント１０１－１乃至１０１－３が異なる位置に設けられているが、提示部１５１－１乃至１５１－３が紙媒体のポスターである場合、その裏側にダミーポイント１０１－１乃至１０１－３がそれぞれ設けられるようにしてもよい。これにより、ユーザは、広告にPDA１をかざすといった、より直感的な動作で商品の詳細をPDA１を用いて確認したりすることができる。

【０１５５】

以上においては、実際に近接している機器間でのみ通信が確立されるように、接続要求に対する返信の受信強度を、接続要求をブロードキャストした機器であるPDA１側でも測定するとしたが（例えば図６）、図１３等に示されるように、ダミーポイント１０１－１乃至１０１－３におけるそれぞれの接続要求の受信強度に基づいて、アクセスポイント５１が、PDA１がいずれかのダミーポイントに実際に近接されているか否かを判断し、接続を許可するか否かを決定するようにしてもよい。

【０１５６】

図１４Ａ，Ｂは、ダミーポイント１０１－１乃至１０１－３とPDA１の位置関係の例を示す図である。

【０１５７】

PDA１がブロードキャストする接続要求を受信したダミーポイント１０１－１乃至１０１－３は、ケーブル１１１－１乃至１１１－３を介して、それぞれ、その受信強度をアクセスポイント５１に通知する。

【０１５８】

例えば、図１４Ａに示されるように、ダミーポイント１０１－１乃至１０１－３のそれぞれにおいて受信される接続要求の受信強度に基づいて、PDA１が、他の２つとの距離に較べて、１つのダミーポイント１０１－２に十分近接されていると判定した場合のみ、アクセスポイント５１はPDA１からの要求を許可する。

【０１５９】

従って、PDA１が位置Ｐ１に位置している場合、アクセスポイント５１は、ダミーポイント１０１－１とダミーポイント１０１－３における受信強度に較べて、ダミーポイント１０１－２における受信強度が高いため、PDA１がダミーポイント１０１－２に近接されていると判断し、PDA１からの接続を許可する。一方、例えば、PDA１が位置Ｐ１よりも若干上方の位置Ｐ２に位置し、ダミーポイント１０１－１とダミーポイント１０１－２における接続要求の受信強度がほぼ等しいものとして測定されることにより、アクセスポイント５１はPDA１による接続を認めない。

【０１６０】

このように、それぞれのダミーポイントにおける受信強度を比較することで、PDA１がダミーポイントに近接されているのかをより確実に識別することができる。また、実際にはダミーポイントに近接されていないにもかかわらず、出力を大にして接続要求をブロードキャストするPDA１の接続を防止することができる。

【０１６１】

例えば、図１４Ｂに示されるように、PDA１がいずれのダミーポイントにも近接されていない場合、ダミーポイント１０１－１乃至１０１－３において受信される接続要求の受信強度は同程度のものとしてそれぞれ測定され、この場合、アクセスポイント５１に対するPDA１の接続は許可されない。

【０１６２】

図１４ＢのPDA１が出力を大にして接続要求をブロードキャストしており、それぞれのダミーポイントにおける接続要求の受信強度を比較しない場合、受信強度が所定の閾値以上の強度であれば、アクセスポイント５１に対するアクセスが許可されることになるが、それぞれのダミーポイントにおける接続要求の受信強度を比較することにより、それを防止することができる。すなわち、いずれのダミーポイントにも近接されていない機器によりアクセスポイント５１に対するアクセスが行われるのを防止することができる。

【０１６３】

ここで、図１５のフローチャートを参照して、以上のように、それぞれのダミーポイントにおける接続要求の受信強度に基づいて、接続を許可するか否かを決定するアクセスポイント５１の処理について説明する。

【０１６４】

ステップＳ２１１において、ネットワーク管理部８１（図１１）は、ダミーポイント１０１－１乃至１０１－３における接続要求の受信強度を有線通信制御部１４１を介して取

得する。

【０１６５】

ステップＳ２１２において、ネットワーク管理部８１は、他の２つのダミーポイントと較べて、高い受信強度を測定する１つのダミーポイントがあるか否かを判定する。例えば、３つのダミーポイントにおける接続要求の受信強度の比が算出され、その中で最も高い比が、予め設定されている閾値より高いか否かが判定される。

【０１６６】

ネットワーク管理部８１は、ステップＳ２１２において、そのようなダミーポイントがないと判定した場合、処理を終了させる。これにより、例えば、図１４Ｂに示されるように、いずれのダミーポイントにも近接されていない機器に対しては接続が許可されない。

【０１６７】

一方、ステップＳ２１２において、ネットワーク管理部８１は、他の２つのダミーポイントと較べて、高い受信強度を測定する１つのダミーポイントがあると判定した場合、ステップＳ２１３に進み、その機器は、高い受信強度を測定するダミーポイントに十分近接されていると判断し、その機器の接続を許可する。その後、ダミーポイントから提供されたESSIDやWEPキーに基づいて、接続が許可された機器によるアクセスポイント５１への接続が行われる。

【０１６８】

以上においては、３つのダミーポイント１０１－１乃至１０１－３における接続要求の受信強度を比較するとしたが、ダミーポイントの数は３つに限られない。すなわち、接続要求の受信強度を比較することで、機器がいずれかのダミーポイントに近接されているのかを判断することができれば、ダミーポイントはいくつ設けられていてもよい。

【０１６９】

また、以上においては、ダミーポイントは壁面などに固定して設けられているとしたが、例えば、図１６に示されるように、携帯型の機器として用意されるようにしてもよい。

【０１７０】

図１６は、携帯型のダミーポイント１２１（以下、携帯型ダミーポイント１２１と称する）と、パーソナルコンピュータ１２２が近接されている状態を示す図である。

【０１７１】

携帯型ダミーポイント１２１は、パーソナルコンピュータ１２２に近接され、図１２を参照して説明したようにしてパーソナルコンピュータ１２２から送信される電波の受信強度が所定の閾値より高いと判定した場合、ESSIDやWEPキー等を生成し、それをパーソナルコンピュータ１２２に提供する。また、このとき、携帯型ダミーポイント１２１は、パーソナルコンピュータ１２２に提供したそれらの情報を図示せぬアクセスポイントにも送信し、パーソナルコンピュータ１２２からのアクセスが許可されるようにアクセスポイントの設定を変更させる。

【０１７２】

これにより、パーソナルコンピュータ１２２は、アクセスポイントが管理するネットワークに参加することが可能となる。

【０１７３】

この携帯型ダミーポイント１２１は、例えば、ホットスポット（商標）のように、ワイヤレスのインターネット接続のサービスを提供する空間に用意される。この場合、例えば、携帯型ダミーポイント１２１はサービスの管理者が所有し、その管理者が、サービスの料金を支払ったユーザのパーソナルコンピュータに携帯型ダミーポイント１２１を近接させて、インターネットへの接続を許可するなどによって携帯型ダミーポイント１２１が利用される。

【０１７４】

また、例えば、会議室などに携帯型ダミーポイント１２１が用意されている場合において、会議の参加者がそれぞれ自分のパーソナルコンピュータに携帯型ダミーポイント１２１を近接させ、参加者のパーソナルコンピュータからなるネットワークを構築するときな

どにも携帯型ダミーポイント１２１は利用される。

【０１７５】

なお、携帯型ダミーポイント１２１からアクセスポイントに対してESSIDやWEPキー等の情報を送信する場合、その送信は、携帯型ダミーポイント１２１とアクセスポイントが近接され、上述したように受信電波の強度に基づいて判定が行われ、閾値以上の強度であると判定された場合に行われるようにしてもよい。当然、携帯型ダミーポイント１２１からアクセスポイントに対するESSIDやWEPキー等の情報の送信は、携帯型ダミーポイント１２１に接続されたケーブルを介して有線により行われたり、非接触ICタグや赤外線などを用いた近距離間の無線通信により行われるようにしてもよい。これにより、ESSIDやWEPキー等の情報が第三者に知られてしまうことを防止することができる。

【０１７６】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。

【０１７７】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１７８】

この記録媒体は、図２に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク２１（フレキシブルディスクを含む）、光ディスク２２（CD-ROM(Compact Disk-Read Only Memory), DVD(Digital Versatile Disk)を含む）、光磁気ディスク２３（MD（登録商標）(Mini-Disk)を含む）、もしくは半導体メモリ２４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM１２や記憶部１８などで構成される。

【０１７９】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１８０】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

【図面の簡単な説明】

【０１８１】

【図１】アドホック通信を確立させる手順について示す図である。

【図２】PDAの構成例を示すブロック図である。

【図３】PDAの機能構成例を示すブロック図である。

【図４】図１のPDAと携帯電話機により行われる無線通信確立処理について説明するフローチャートである。

【図５】図４の処理の具体例について説明するフローチャートである。

【図６】図１のPDAと携帯電話機により行われる他の無線通信確立処理について説明するフローチャートである。

【図７】インフラストラクチャ通信を確立させる手順について示す図である。

【図８】アクセスポイントの構成例を示すブロック図である。

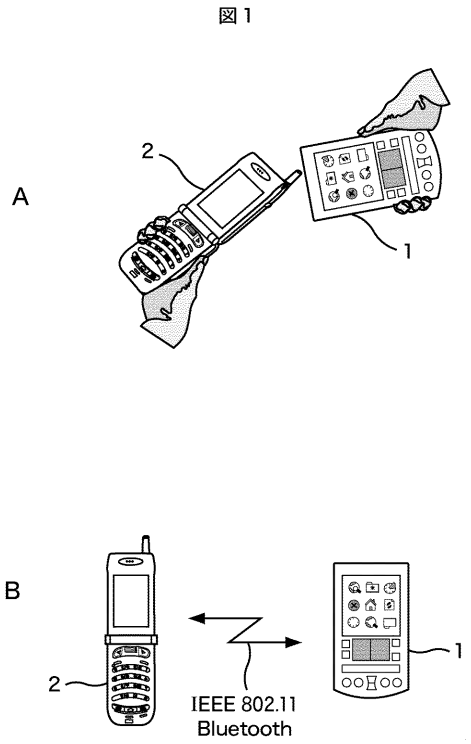
【図９】PDAとアクセスポイントにより行われる処理について説明するフローチャートである。

【図１０】ダミーポイントに機器を近接させることでインフラストラクチャ通信を確立させる手順について示す図である。

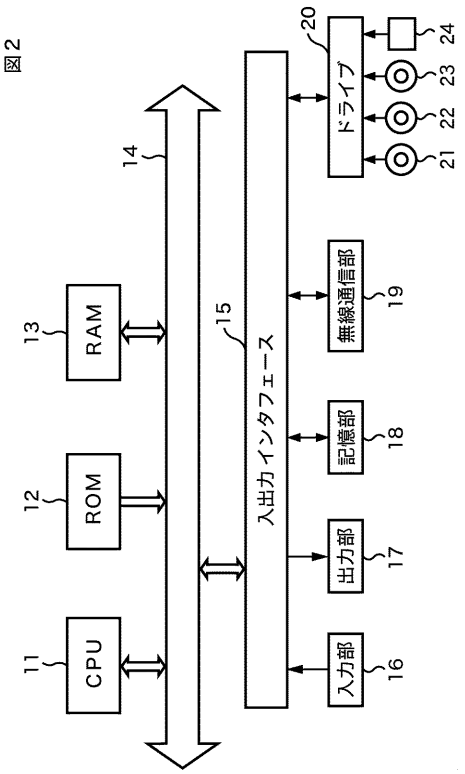
【図１１】アクセスポイントとダミーポイントの構成例を示すブロック図である。

【図１２】PDA、アクセスポイント、ダミーポイントにより行われる通信確立処理について説明するフローチャートである。
【図１３】本発明を適用した通信システムの構成例を示す図である。
【図１４】ダミーポイントとPDAの位置関係の例を示す図である。
【図１５】アクセスポイントの処理について説明するフローチャートである。
【図１６】携帯型のダミーポイントとパーソナルコンピュータが近接されている状態を示す図である。
【符号の説明】
【０１８２】
１　PDA,　２　携帯電話機,　３１　無線通信制御部,　３２　暗号復号処理部,　３３　通信パラメータ管理部,　３４　鍵情報管理部,　４１　接続要求送信部,　４２　強度判定部,　７１　無線通信制御部,　７２　暗号復号処理部,　７３　通信パラメータ管理部,　７４　鍵情報管理部,　８１　ネットワーク管理部,　８２　強度判定部,　１０１－１乃至１０－３　ダミーポイント

【図１】

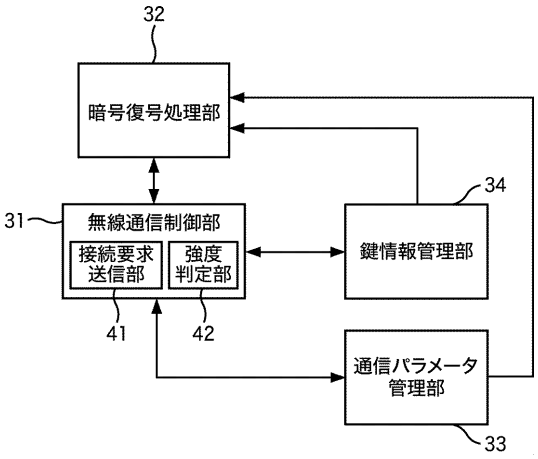


【図２】



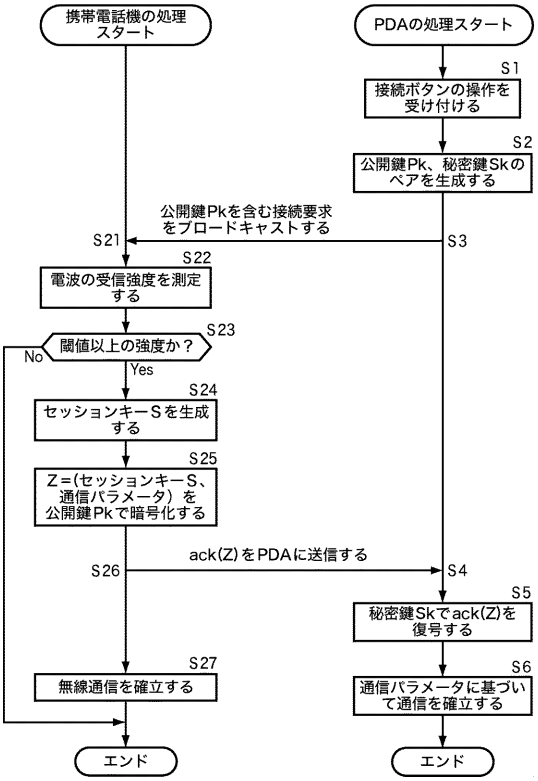
【図３】

図３



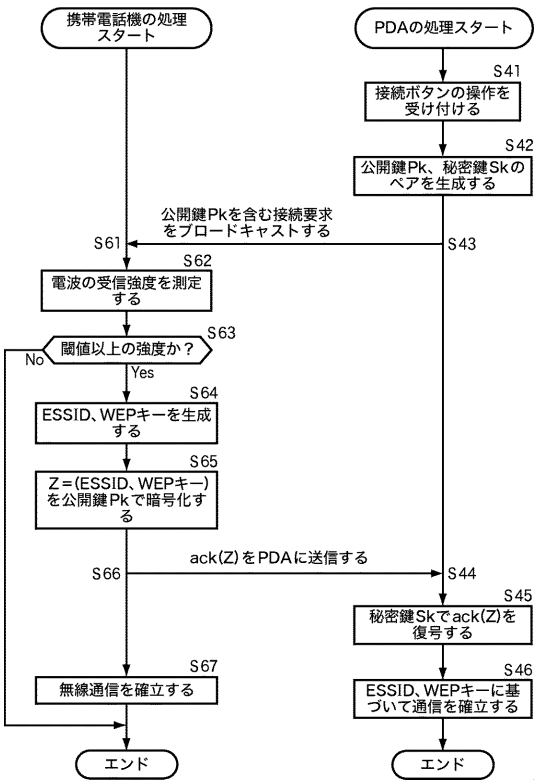
【図４】

図４



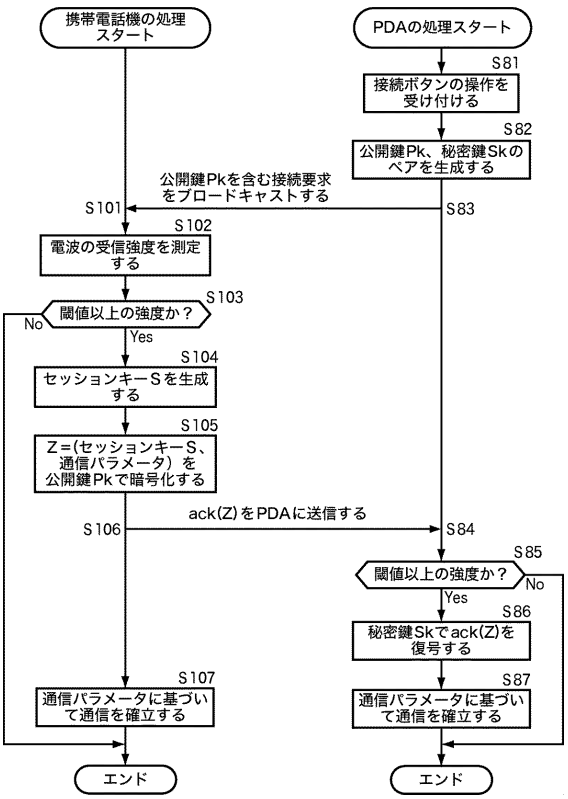
【図５】

図５



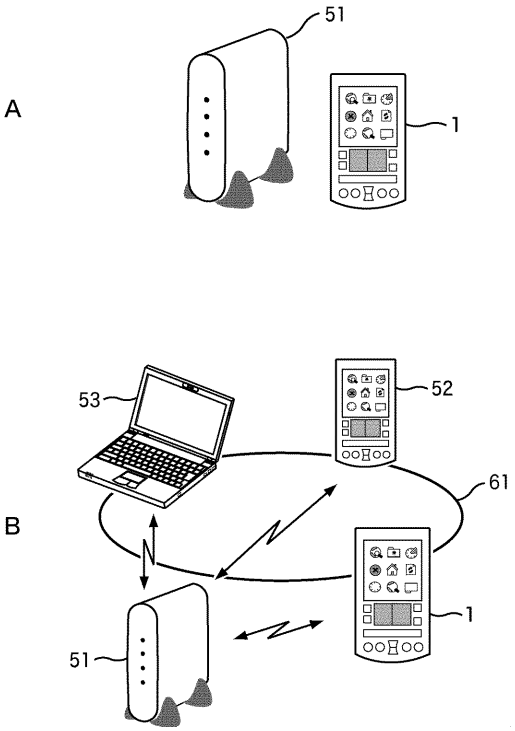
【図６】

図６



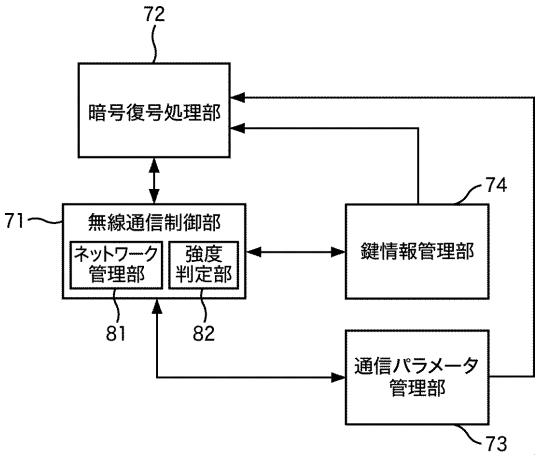
【図７】

図７



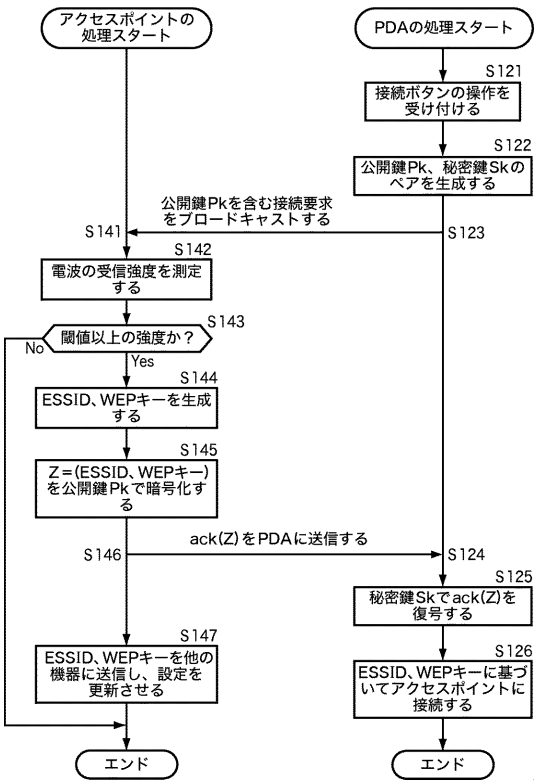
【図８】

図８



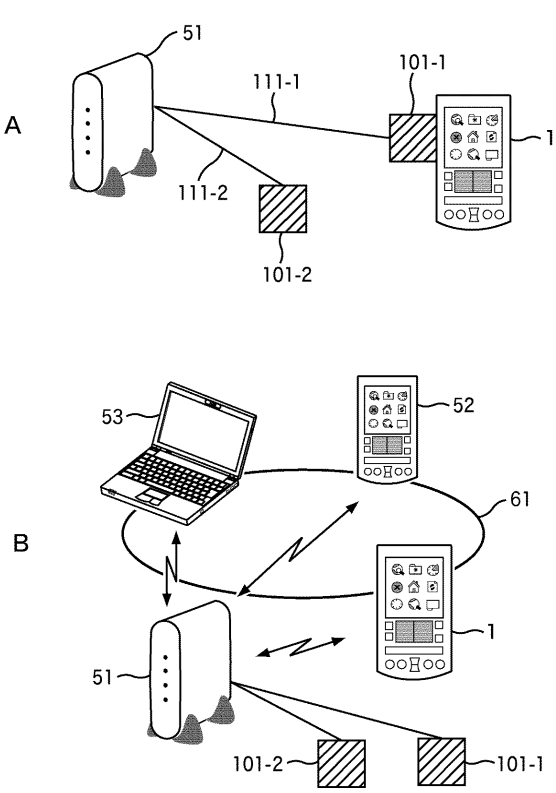
【図９】

図９

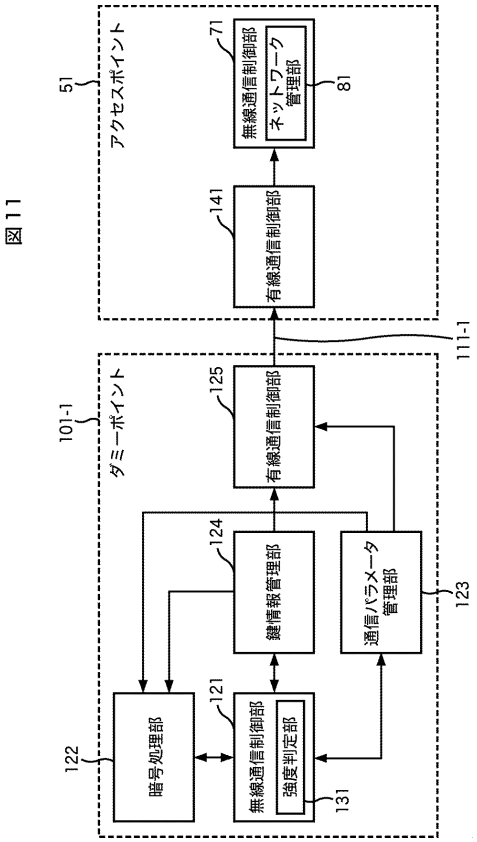


【図１０】

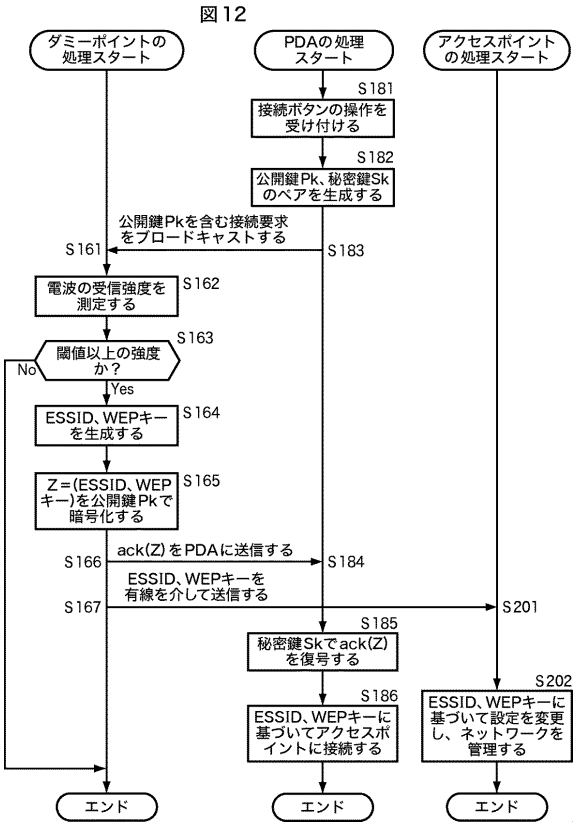
図１０



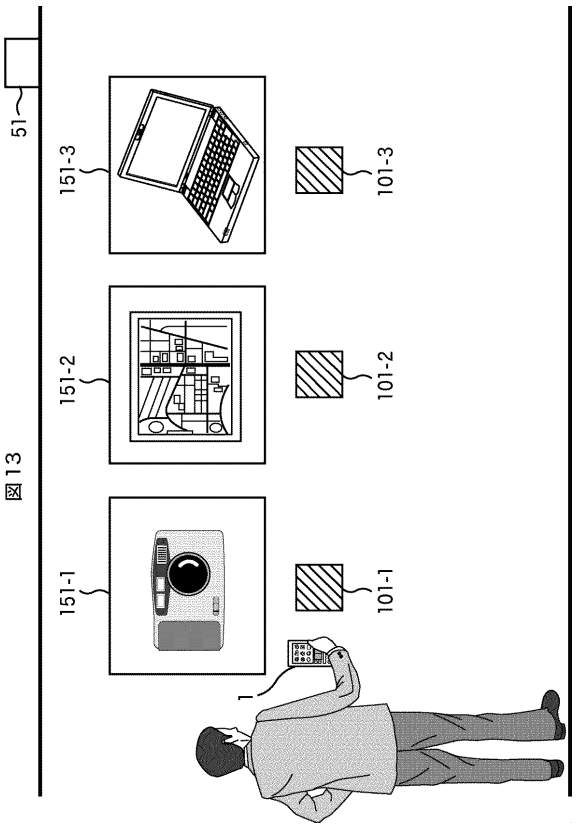
【図１１】



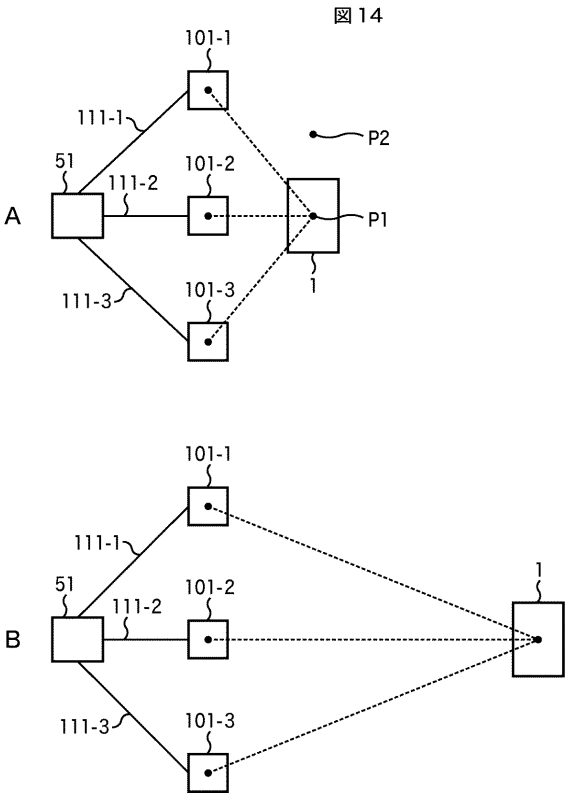
【図１２】



【図１３】

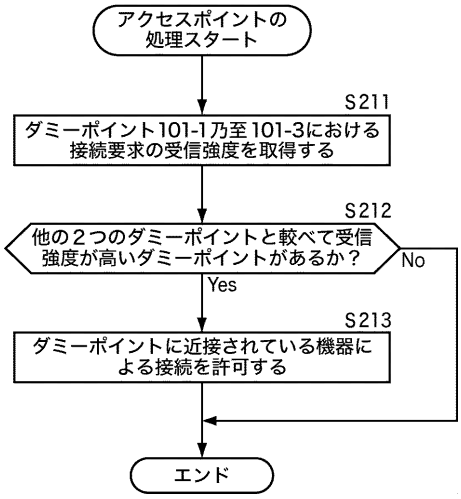


【図１４】



【図１５】

図15



【図１６】

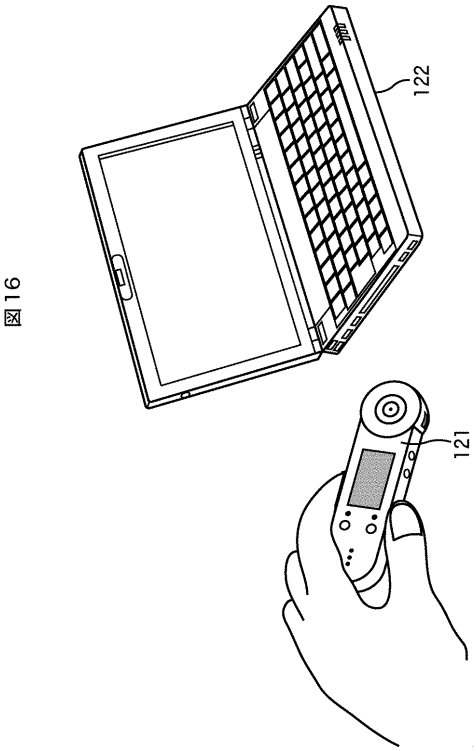


図16

フロントページの続き

(56)参考文献　特表２００１－５００３２７（ＪＰ，Ａ）
特開２００１－１５６７０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８