(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4345596号
(P4345596)
(45)発行日　平成21年10月14日(2009.10.14)　(24)登録日　平成21年7月24日(2009.7.24)

(51)Int.Cl.　F I
H04W 84/12 (2009.01)　H04L 12/28　310
H04W 88/08 (2009.01)

請求項の数 13　(全 31 頁)

(21)出願番号　特願2004-201661 (P2004-201661)
(22)出願日　平成16年7月8日 (2004.7.8)
(65)公開番号　特開2005-333606 (P2005-333606A)
(43)公開日　平成17年12月2日 (2005.12.2)
審査請求日　平成19年2月21日 (2007.2.21)
(31)優先権主張番号　特願2004-126213 (P2004-126213)
(32)優先日　平成16年4月22日 (2004.4.22)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　萩原　豊隆
長野県松本市芳川村井町１０５９番地　株式会社エプソンソフト開発センター内

審査官　岩田　玲彦

(56)参考文献　特開２００２－０７３５６５（ＪＰ，Ａ）
特開２００１－２８５９５６（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】無線通信ネットワークシステムにおける接続認証

(57)【特許請求の範囲】
【請求項１】
無線局と、該無線局との間で特定の無線通信回線を介して接続される１以上の無線通信端末とを備える無線通信ネットワークシステムであって、
前記無線局は、
前記無線通信端末との間で指向性を有する通信媒体を利用した指向性無線通信を行う第１の指向性無線通信部と、
前記無線通信端末との間で前記特定の無線通信回線による特定の無線通信を行う第１の無線通信部と、
前記第１の指向性無線通信部および前記第１の無線通信部を制御し、前記無線通信端末との間で前記特定の無線通信回線の接続認証を行う第１の認証処理制御部と、を備え、
前記無線通信端末は、
前記無線局との間で前記指向性無線通信を行う第２の指向性無線通信部と、
前記無線局との間で前記特定の無線通信を行う第２の無線通信部と、
前記第２の指向性無線通信部および前記第２の無線通信部を制御し、前記無線局との間で前記特定の無線通信回線の接続認証を行う第２の認証処理制御部と、を備え、
前記第１の認証処理制御部は、
前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報であって、前記無線通信端末の前記第２の指向性無線通信部から送信された情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記特

定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信するとともに、前記暗証コードを生成するための第２の暗証コード生成情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信し、

前記第１の暗証コード生成情報または第２の暗証コード生成情報のいずれか一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成し、

前記第２の認証処理制御部は、

前記第１の暗証コード生成情報を、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信した後、前記第１の指向性無線通信部から送信された前記無線局ＩＤ情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信するとともに、前記第１の指向性無線通信部から送信された前記第２の暗証コード生成情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信した場合に、前記一方の暗証コード生成情報を暗号化キーとして、前記他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する、

ことを特徴とする無線通信ネットワークシステム。

【請求項２】

請求項１記載の無線通信ネットワークシステムにおいて、

前記第１の暗証コード生成情報は、前記第２の認証処理制御部において、所定のマスク情報と排他的論理和することにより生成された第１の秘匿化暗証コード生成情報として、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信される、無線通信ネットワークシステム。

【請求項３】

請求項２に記載の無線通信ネットワークシステムにおいて、

前記所定のマスク情報は、少なくとも、前記特定の無線通信回線の接続に利用される無線端末ＩＤ情報に基づいて生成されたデータを暗号化することにより生成される、無線通信ネットワークシステム。

【請求項４】

請求項２または請求項３記載の無線通信ネットワークシステムにおいて、

前記第２の暗証コード生成情報は、前記第１の認証処理制御部において、前記第１の秘匿化暗証コード生成情報と排他的論理和することにより生成された第２の秘匿化暗証コード生成情報として、前記無線局の前記第１の指向性無線通信部から前記無線端末の前記第２の指向性無線通信部に対して送信される、無線通信ネットワークシステム。

【請求項５】

請求項１ないし請求項４のいずれかに記載の無線通信ネットワークシステムにおいて、

前記第１の無線通信部は、前記無線局ＩＤ情報の異なった複数の無線通信ユニットを備えており、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記複数の無線通信ユニットの中から、第１の条件に基づいて１つの前記無線通信ユニットを前記第１の無線通信部として選択する、無線通信ネットワークシステム。

【請求項６】

請求項１ないし請求項４のいずれかに記載の無線通信ネットワークシステムにおいて、

前記第１の無線通信部は、複数の無線通信ユニットを備えており、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記複数の無線通信ユニットの中から、第１の条件に基づいて１つの前記無線通信ユニットを前記第１の無線通信部として選択し、

前記第１の無線通信部として選択した前記無線通信ユニットに対して、あらかじめ用意

されている複数の前記無線局ＩＤ情報の中から、第２の条件に基づいて１つの前記無線局ＩＤ情報を選択して前記第１の無線通信部に設定する、無線通信ネットワークシステム。

【請求項７】

請求項１ないし請求項４のいずれかに記載の無線通信ネットワークシステムにおいて、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、あらかじめ用意されている複数の前記無線局ＩＤ情報の中から、所定の条件に基づいて１つの前記無線局ＩＤ情報を選択して前記第１の無線通信部に設定する、無線通信ネットワークシステム。

【請求項８】

請求項１ないし請求項７のいずれかに記載の無線通信ネットワークシステムにおいて、

前記第１の指向性無線通信部は、複数の前記無線通信端末との間で前記指向性無線通信を行うための複数の指向性無線通信ユニットを備える、無線通信ネットワークシステム。

【請求項９】

１以上の無線通信端末との間で特定の無線通信回線を介して接続される無線局であって、

前記無線通信端末との間で指向性を有する通信媒体を利用した指向性無線通信を行う指向性無線通信部と、

前記無線通信端末との間で前記特定の無線通信回線による特定の無線通信を行う無線通信部と、

前記指向性無線通信部および前記無線通信部を制御し、前記無線通信端末との間で前記特定の無線通信回線の接続認証を行う認証処理制御部と、を備え、

前記認証処理制御部は、

前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報であって、前記無線通信端末から送信された情報を、前記指向性無線通信部によって受信した場合に、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記指向性無線通信部から前記無線通信端末に対して送信するとともに、前記暗証コードを生成するための第２の暗証コード生成情報を、前記指向性無線通信部から前記無線通信端末に対して送信し、

前記第１の暗証コード生成情報または第２の暗証コード生成情報のいずれか一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する、

ことを特徴とする無線局。

【請求項１０】

無線局との間で特定の無線通信回線を介して接続される無線通信端末であって、

前記無線局との間で指向性を有する通信媒体を利用した指向性無線通信を行う指向性無線通信を行う指向性無線通信部と、

前記無線局との間で前記特定の無線通信を行う無線通信部と、

前記指向性無線通信部および前記無線通信部を制御し、前記無線局との間で前記特定の無線通信回線の接続認証を行う認証処理制御部と、を備え、

前記認証処理制御部は、

前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報を、前記指向性無線通信部から前記無線局に対して送信した後、前記無線局から前記指向性無線通信により送信された情報であって、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を受信するとともに、前記無線局から前記指向性無線通信により送信された情報であって、前記暗証コードを生成するための第２の暗証コード生成情報を、前記指向性無線通信によって受信した場合に、前記一方の暗証コード生成情報を暗号化キーとして、前記他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する、

ことを特徴とする無線通信端末。

【請求項１１】
無線局と１以上の無線通信端末との間で実行される特定の無線通信回線の接続認証方法であって、
前記無線局において、前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報を、指向性を有する通信媒体を利用した指向性無線通信により前記無線通信端末から受信した場合に、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記指向性無線通信により前記無線通信端末に対して送信するとともに、前記暗証コードを生成するための第２の暗証コード生成情報を、前記指向性無線通信により前記無線通信端末に対して送信し、
前記無線局において、前記第１の暗証コード生成情報または第２の暗証コード生成情報のいずれか一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成し、
前記無線通信端末において、前記第１の暗証コード生成情報を、前記無線局に対して前記指向性無線通信により送信した後、前記無線局から前記指向性無線通信により送信された前記無線局ＩＤ情報を受信するとともに、前記無線局から前記指向性無線通信により送信された前記第２の暗証コード生成情報を受信した場合に、前記一方の暗証コード生成情報を暗号化キーとして、前記他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する、
ことを特徴とする接続認証方法。
【請求項１２】
１以上の無線通信端末との間で特定の無線通信回線を介し接続される無線局において、前記特定の無線通信回線の接続認証をコンピュータに実行させるためのコンピュータプログラムであって、
前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報を、指向性を有する通信媒体を利用した指向性無線通信により前記無線通信端末から受信した場合に、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記指向性無線通信により前記無線通信端末に対して送信するとともに、前記暗証コードを生成するための第２の暗証コード生成情報を、前記指向性無線通信により前記無線通信端末に対して送信する機能と、
前記第１の暗証コード生成情報または第２の暗証コード生成情報のいずれか一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する機能と、
を前記コンピュータに実現させるためのプログラムを含むことを特徴とするコンピュータプログラム。
【請求項１３】
無線局との間で特定の無線通信回線を介して接続される無線通信端末において、前記特定の無線通信回線の接続認証をコンピュータに実行させるためのコンピュータプログラムであって、
前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報を、指向性を有する通信媒体を利用した指向性無線通信により前記無線局に対して送信した後、前記無線局から前記指向性無線通信により送信された情報であって、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を受信するとともに、前記無線局から前記指向性無線通信により送信された情報であって、前記暗証コードを生成するための第２の暗証コード生成情報を受信した場合に、前記一方の暗証コード生成情報を暗号化キーとして、前記他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する機能、
をコンピュータに実現させるためのプログラムを含むことを特徴とす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】
この発明は、ブルートゥース（Bluetooth）のような近距離無線通信規格を利用してデータ伝送を行うことが可能な無線通信ネットワークシステムにおいて、無線局としての制御機能を有する無線通信端末（以下、「アクセスポイント」とも呼ぶ）と、無線局によって制御される無線通信端末（以下、単に「端末」とも呼ぶ）との間で無線通信を可能とするために実行される接続認証の技術に関する。
【背景技術】
【０００２】
ブルートゥース（「ＢＴ」と略す場合もある。）規格による無線通信機能（以下、「ＢＴ機能」とも呼ぶ。）を搭載した電子機器（無線通信端末）、例えば、携帯電話やデジタルカメラなど種々の電子機器(以下、「ＢＴ端末」とも呼ぶ。)の開発が見込まれている。そして、今後、これらのＢＴ端末を対象にした各種サービスの提供の普及が予想される。一例として、携帯電話やデジタルカメラ等で撮像した写真（電子データの表す画像）をプリントするサービス（以下、「写真プリントサービス」と呼ぶ。）が考えられる。
【０００３】
写真プリントサービスは、例えば以下のように提供される。ＢＴ端末であるプリントサービス提供装置（以下、「ＢＴアクセスポイント」とも呼ぶ。）を、ファミリーレストラン、観光スポット、遊園地、駅の構内等の多くの人が集まるような場所（以下、「公共の場所」と呼ぶ。）に設置する。写真プリントサービスの提供を受けたいユーザは、携帯電話やデジタルカメラ等の自分のＢＴ端末から、ＢＴアクセスポイントであるプリントサービス提供装置に、プリントしたい写真の電子データをＢＴ規格の無線通信（以下、「ＢＴ通信」とも呼ぶ。）を利用して伝送する。プリントサービス提供装置は、伝送された電子データの表す画像（写真）をプリントする。
【０００４】
ここで、ＢＴアクセスポイントとＢＴ端末との間でＢＴ通信を可能とするためには、ＢＴアクセスポイントとＢＴ端末との間で、ＢＴ通信回線の接続を確立させるために必要なＩＤ情報（ＢＴアドレス）を交換する必要がある。ＢＴ端末をＢＴアクセスポイントに接続させる場合、通常は、ＢＴ規格で規定されている「Ｉｎｑｕｉｒｙ」と呼ばれるモード（以下、「問い合わせモード」と呼ぶ。）を利用して、ＢＴ端末から電波の到達可能な範囲に存在するＢＴアクセスポイントを問い合わせし、応答の有ったＢＴアクセスポイントとの間でＢＴ通信回線の接続に必要なＩＤ情報を交換する。そして、交換したＩＤ情報を利用してＢＴ端末とＢＴアクセスポイントとの間でＢＴ通信回線の接続が確立される。
【０００５】
しかしながら、問い合わせモードを利用した場合、ＢＴアクセスポイントは、問い合わせの有ったＢＴ端末の全てに対して同等に応答を返して、ＢＴ通信の接続を確立させることになる。このため、ＢＴアクセスポイントから電波の到達範囲内にあるＢＴ端末のうち、本来サービス提供を受けるつもりのないユーザ、例えば、いたずら目的のユーザや、誤って接続指示してしまうような不用意なユーザなどのＢＴ端末と、ＢＴアクセスポイントとの間で、ＢＴ通信回線の接続が容易に確立されてしまうことになる。特に、公共の場所に設置されるようなＢＴアクセスポイントに対しては、不特定多数のユーザによって上記のようにサービスの提供を妨げるような接続がなされる可能性が高くなる。なお、以下では、上記のようにサービスの提供を妨げるような接続を、「不用意な接続」と呼ぶこととする。
【０００６】
また、ＢＴ端末は、上記のように、問い合わせに対して応答の有ったＢＴアクセスポイントとの間でＢＴ通信回線の接続に必要なＩＤ情報を交換してＢＴ通信回線の接続を確立する。このため、仮に、正しいＢＴアクセスポイントに偽装したＢＴアクセスポイント（以下、「偽装ＢＴアクセスポイント」と呼ぶ。）が存在した場合にも、この偽装ＢＴアクセスポイントとの間でＩＤ情報を交換してしまい、偽装ＢＴアクセスポイントとの間でＢＴ通信回線の接続を確立してしまう可能性がある。この結果、偽装ＢＴアクセスポイント

に接続したＢＴ端末から重要な個人情報が盗まれる可能性もある。

【０００７】

以上のことから、ＢＴ通信を利用したサービスの提供では、そのサービスを本当に受けようとするユーザのみが、自分の受けたいサービスを提供するＢＴアクセスポイントを指定でき、不用意な接続を防止すること、かつ、その接続しようとするＢＴアクセスポイントが、本当に接続を望む正規のＢＴアクセスポイントであることをユーザが確認できることが好ましい。すなわち、接続したいＢＴアクセスポイントをユーザが明示的に指定して、指定したＢＴアクセスポイントとユーザのＢＴ端末との間の通信回線の接続が確立されることが好ましい。

【０００８】

上記問題を解決する先行技術として、特許文献１には、赤外線（IR:Infrared）通信により、ＢＴ通信回線の接続に必要なＩＤ情報をＢＴ端末からＢＴアクセスポイントに対して送信する技術が開示されている。赤外線は指向性が高く、到達距離も数ｍ以下であるので、自分のＢＴ端末をＢＴアクセスポイントに接続したいユーザは、接続したいＢＴアクセスポイントの前まで行って、接続したいＢＴアクセスポイントであることを確認の上、ＢＴ通信回線の接続に必要なＩＤ情報を自分のＢＴ端末からＢＴアクセスポイントに対してＩＲ通信により送信することになる。これにより、ユーザは、接続したいＢＴアクセスポイントを明示的に指定して、指定したＢＴアクセスポイントとユーザのＢＴ端末との間のＢＴ通信回線の接続を確立させることができるので、上記問題点を解消することができる。

【０００９】

【特許文献１】特開２００１－１５６７２３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

ところで、一般に、無線通信では通信情報の漏洩が問題となるため、安全に無線通信を実行するために、通信情報を暗号化して送信することが好ましい。ＢＴ規格では通信情報の暗号化について規定されており、通信情報を暗号化して送信することができる。ＢＴ通信において通信情報を暗号化するためには、ＢＴ端末とＢＴアクセスポイントのそれぞれに、同じＰＩＮコード（個人認証番号：Personal Identification Number）を入力し、両者の間で互いに接続認証を行っておく必要がある。

【００１１】

しかしながら、上記従来技術は、ＢＴ通信回線の接続確立に関する技術のみを開示したものであり、接続認証に関して何ら考慮がなされていない。

【００１２】

ここで、ＢＴ端末へのＰＩＮコードの入力方法としては、例えば、ユーザが、ＢＴアクセスポイントとしてのＢＴ端末の表示画面を介して提供されるＰＩＮコードを読み取って、自分のＢＴ端末に入力する方法が考えられる。しかしながら、この入力方法の場合、ユーザが自分でＰＩＮコードを入力しなければならず、操作が煩雑である。また、ＰＩＮコードの入力を誤る恐れもある。また、表示されたＰＩＮコードを他人に盗み見される恐れもある。他人にＰＩＮコードが知られた場合、その他人は自分のＢＴ端末にそのＰＩＮコードを入力して接続認証を行うことが可能となり、情報が漏洩してしま可能性がある。

【００１３】

また、ＢＴアクセスポイントが提供するＰＩＮコードを、上記ＩＲ通信やＢＴ通信によってＢＴ端末に送信することにより、ＢＴアクセスポイントとＢＴ端末との間で同じＰＩＮコードを交換する方法が考えられる。この方法によれば、ユーザによるＰＩＮコードの入力処理をなくして、操作の煩雑さを解消することができる。しかしながら、ＩＲ通信もＢＴ通信も無線通信であるため、無線通信を傍受する他人によってＰＩＮコードが容易に盗まれる恐れがある。

【００１４】

なお、上記課題は、ＢＴ端末がＢＴアクセスポイントに接続されて構成される無線通信ネットワークシステムの場合に限らず、ＢＴ以外の無線通信規格を利用してデータ伝送を行う無線通信ネットワークシステムにおいても共通するものと考えられる。

【００１５】

この発明は、上記課題を解決するためになされたものであり、無線通信のアクセスポイント（無線局）に無線通信端末が接続される無線通信ネットワークシステムにおいて、接続したいアクセスポイントを、ユーザが明示的に指定することにより、指定したアクセスポイントとユーザの無線通信端末との間の通信回線の接続を確立することを可能とするとともに、無線通信端末とアクセスポイントとの間の接続認証を、簡便でかつ安全に実行することを可能とする技術を提供することを目的とする。

【課題を解決するための手段】

【００１６】

上述の課題の少なくとも一部を解決するため、本発明の第１の態様は、

無線局と、該無線局との間で特定の無線通信回線を介して接続される１以上の無線通信端末とを備える無線通信ネットワークシステムであって、

前記無線局は、

前記無線通信端末との間で指向性を有する通信媒体を利用した指向性無線通信を行う第１の指向性無線通信部と、

前記無線通信端末との間で前記特定の無線通信回線による特定の無線通信を行う第１の無線通信部と、

前記第１の指向性無線通信部および前記第１の無線通信部を制御し、前記無線通信端末との間で前記特定の無線通信回線の接続認証を行う第１の認証処理制御部と、を備え、

前記無線通信端末は、

前記無線局との間で前記指向性無線通信を行う第２の指向性無線通信部と、

前記無線局との間で前記特定の無線通信を行う第２の無線通信部と、

前記第２の指向性無線通信部および前記第２の無線通信部を制御し、前記無線局との間で前記特定の無線通信回線の接続認証を行う第２の認証処理制御部と、を備え、

前記第１の認証処理制御部は、

前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための第１の暗証コード生成情報であって、前記無線通信端末の前記第２の指向性無線通信部から送信された情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信するとともに、前記暗証コードを生成するための第２の暗証コード生成情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信し、

前記第１の暗証コード生成情報または第２の暗証コード生成情報のいずれか一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成し、

前記第２の認証処理制御部は、

前記第１の暗証コード生成情報を、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信した後、前記第１の指向性無線通信部から送信された前記無線局ＩＤ情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信するとともに、前記第１の指向性無線通信部から送信された前記第２の暗証コード生成情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信した場合に、前記一方の暗証コード生成情報を暗号化キーとして、前記他方の暗証コード生成情報を暗号化することにより前記暗証コードを生成する、

ことを特徴とする。

【００１７】

この構成によれば、無線通信端末は、指向性無線通信によって無線通信端末から無線局に第１の暗証コード生成情報が送信された場合に、はじめて、特定の無線通信に利用され

る無線局ＩＤ情報を、無線通信端末と無線局との間の指向性無線通信によって得ることになる。指向性無線通信は、一般に、指向性が高く信号到達距離も短いため、ユーザは自分の無線通信端末と無線局との間で指向性無線通信を行うために、信号到達距離内にある位置、一般に、無線局が視認できる位置まで近づく必要がある。これにより、ユーザは、自分の無線通信端末を接続させたい無線局を、明示的に指定することが可能である。

【００１８】

また、無線局および無線通信端末では、それぞれ無線通信端末から無線局に指向性通信により送信された第１の暗証コード生成情報および無線局から無線通信端末に指向性通信により送信され第２の暗証コード生成情報のうち、一方の暗証コード生成情報を暗号化キーとして、他方の暗証コード生成情報を暗号化することにより暗証コードを生成している。これにより、無線局と無線通信端末との接続認証を、簡便でかつ安全に実行することが可能である。

【００１９】

ここで、前記第１の暗証コード生成情報は、前記第２の認証処理制御部において、所定のマスク情報と排他的論理和することにより生成された第１の秘匿化暗証コード生成情報として、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信されることが好ましい。

【００２０】

こうすれば、第１の暗証コード生成情報を、無線通信端末から無線局に対して比較的安全に送信することが可能である。

【００２１】

なお、前記所定のマスク情報は、少なくとも、前記特定の無線通信回線の接続に利用される無線端末ＩＤ情報に基づいて生成されたデータを暗号化することにより生成されることが好ましい。

【００２２】

こうすれば、第１の暗証コード生成情報の秘匿性をさらに高めることが可能である。

【００２３】

また、前記第２の暗証コード生成情報は、前記第１の認証処理制御部において、前記第１の秘匿化暗証コード生成情報と排他的論理和することにより生成された第２の秘匿化暗証コード生成情報として、前記無線局の前記第１の指向性無線通信部から前記無線端末の前記第２の指向性無線通信部に対して送信されることが好ましい。

【００２４】

こうすれば、第２の暗証コード生成情報を、無線局から無線通信端末に対して比較的安全に送信することが可能である。

【００２５】

上記無線通信ネットワークシステムにいおいて、

前記第１の無線通信部は、前記無線局ＩＤ情報の異なった複数の無線通信ユニットを備えており、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記複数の無線通信ユニットの中から、第１の条件に基づいて１つの前記無線通信ユニットを前記第１の無線通信部として選択するようにしてもよい。

【００２６】

こうすれば、第１の無線通信部として、第１の条件に応じて種々の無線通信ユニットの選択が可能となる。例えば、複数の無線通信ユニットのうち、最も通信負荷の低い無線通信ユニットを選択することを第１の条件とすれば、使用される無線通信ユニットの平準化を図ることが可能である。また、前回選択された無線通信ユニットを除く他の無線通信ユニットのうちいずれか一つを選択することを第１の条件とすれば、同じ無線通信ユニットが連続して選択されることがないので、無線通信の安全性を向上させることができる。さらに、他の無線通信ユニットを選択する場合において、最も通信負荷の低い無線通信ユニ

ットを選択することを第１の条件とすれば、使用される無線通信ユニットの平準化を図ることが可能であるとともに、無線通信の安全性を向上させることが可能である。

【００２７】

また、上記無線通信ネットワークシステムにおいて、

前記第１の無線通信部は、複数の無線通信ユニットを備えており、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記複数の無線通信ユニットの中から、第１の条件に基づいて１つの前記無線通信ユニットを前記第１の無線通信部として選択し、

前記第１の無線通信部として選択した前記無線通信ユニットに対して、あらかじめ用意されている複数の前記無線局ＩＤ情報の中から、第２の条件に基づいて１つの前記無線局ＩＤ情報を選択して前記第１の無線通信部に設定するようにしてもよい。

【００２８】

こうすれば、第１の無線通信部として選択した無線通信ユニットに設定される無線局ＩＤ情報として、複数の無線局ＩＤ情報の中から、第２の条件に応じた種々の選択が可能となる。例えば、使用されていない期間の最も長い無線局ＩＤ情報を選択することを第２の条件とすれば、同じ無線局ＩＤ情報が連続して選択されることがないので、無線通信の安全性を向上させることができる。

【００２９】

また、上記通信ネットワークシステムにおいて、

前記第１の認証処理制御部は、

第１の暗証コード生成情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、あらかじめ用意されている複数の前記無線局ＩＤ情報の中から、所定の条件に基づいて１つの前記無線局ＩＤ情報を選択して前記無線通信部に設定するようにしてもよい。

【００３０】

こうすれば、第１の無線通信部に設定される無線局ＩＤ情報として、複数の無線局ＩＤ情報の中から、第２の条件に応じた種々の選択が可能となる。例えば、使用されていない期間の最も長い無線局ＩＤ情報を選択することを第２の条件とすれば、同じ無線局ＩＤ情報が連続して選択されることがないので、無線通信の安全性を向上させることができる。

【００３１】

また、上記無線通信ネットワークシステムにおいて、

前記第１の指向性無線通信部は、複数の前記無線通信端末との間で前記指向性無線通信を行うための複数の指向性無線通信ユニットを備えるようにしてもよい。

【００３２】

こうすれば、複数の指向性無線通信ユニットを分散して配置することができる。

【００３３】

本発明の第２の態様は、

無線局と、該無線局との間で特定の無線通信回線を介して接続される１以上の無線通信端末とを備える無線通信ネットワークシステムであって、

前記無線局は、

前記無線通信端末との間で指向性を有する通信媒体を利用した指向性無線通信を行う第１の指向性無線通信部と、

前記無線通信端末との間で前記特定の無線通信回線による特定の無線通信を行う第１の無線通信部と、

前記第１の指向性無線通信部および前記第１の無線通信部を制御し、前記無線通信端末との間で前記特定の無線通信回線の接続認証を行う第１の認証処理制御部と、を備え、

前記無線通信端末は、

前記無線局との間で前記指向性無線通信を行う第２の指向性無線通信部と、

前記無線局との間で前記特定の無線通信を行う第２の無線通信部と、

前記第２の指向性無線通信部および前記第２の無線通信部を制御し、前記無線局との間で前記特定の無線通信回線の接続認証を行う第２の認証処理制御部と、を備え、
前記第１の認証処理制御部は、
前記特定の無線通信回線の接続認証に用いられる暗証コードを生成するための暗号化キーを示す情報であって、前記無線通信端末の前記第２の指向性無線通信部から送信された情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記暗号化キーに基づいて前記暗証コードを暗号化した暗号化暗証コード情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信するとともに、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信し、
前記第２の認証処理制御部は、
前記暗号化キーを示す情報を、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信した後、前記第１の指向性無線通信部から送信された前記暗号化暗証コード情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信した場合に、前記暗号化キーに対応する複合化キーに基づいて前記暗号化暗証コード情報から前記暗証コードを復号するとともに、前記第１の指向性無線通信部から送信された前記無線局ＩＤ情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信する、
ことを特徴とする。

【００３４】

この構成においても、第１の態様の無線通信ネットワークシステムと同様に、ユーザは、自分の無線通信端末を接続させたい無線局を、明示的に指定することが可能である。また、無線局と無線通信端末との接続認証を、簡便かつ安全に実行することが可能である。

【００３５】

本発明の第３の態様は、
無線局と、該無線局との間で特定の無線通信回線を介して接続される１以上の無線通信端末とを備える無線通信ネットワークシステムであって、
前記無線局は、
前記無線通信端末との間で指向性を有する通信媒体を利用した指向性無線通信を行う第１の指向性無線通信部と、
前記無線通信端末との間で前記特定の無線通信回線による特定の無線通信を行う第１の無線通信部と、
前記第１の指向性無線通信部および前記第１の無線通信部を制御し、前記無線通信端末との間で前記特定の無線通信回線の接続認証を行う第１の認証処理制御部と、を備え、
前記無線通信端末は、
前記無線局との間で前記指向性無線通信を行う第２の指向性無線通信部と、
前記無線局との間で前記特定の無線通信を行う第２の無線通信部と、
前記第２の指向性無線通信部および前記第２の無線通信部を制御し、前記無線局との間で前記特定の無線通信回線の接続認証を行う第２の認証処理制御部と、を備え、
前記第１の認証処理制御部は、
前記特定の無線通信回線の接続認証に用いられる暗証コードを暗号化するための暗号化キーの送信を要求する送信要求情報であって、前記無線通信端末の前記第２の指向性無線通信部から送信された情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記暗号化キーを示す情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信し、
前記第２の認証処理制御部は、
前記送信要求情報を、前記無線通信端末の前記第２の指向性無線通信部から前記無線局の前記第１の指向性無線通信部に対して送信した後、前記第１の指向性無線通信部から送信された前記暗号化キー情報を、前記無線通信端末の前記第２の指向性無線通信部によって受信した場合に、前記暗号化キーに基づいて前記暗証コードを暗号化した暗号化暗証コ

ード情報を、前記第２の指向性無線通信部から前記第１の指向性無線通信部に対して送信し、
前記第１の認証処理制御部は、さらに、
前記無線通信端末の前記第２の指向性無線通信部から送信された前記暗号化暗証コード情報を、前記無線局の前記第１の指向性無線通信部によって受信した場合に、前記暗号化キーに対応する複合化キーに基づいて前記暗号化暗証コード情報から前記暗証コードを復号するとともに、前記特定の無線通信回線の接続に利用される無線局ＩＤ情報を、前記第１の指向性無線通信部から前記第２の指向性無線通信部に対して送信する、
ことを特徴とする。
【００３６】
この構成においても、第１の態様の無線通信ネットワークシステムと同様に、ユーザは、自分の無線通信端末を接続させたい無線局を、明示的に指定することが可能である。また、無線局と無線通信端末との接続認証を、簡便かつ安全に実行することが可能である。
【００３７】
なお、本発明は、種々の形態で実現することが可能であり、いずれの形態においても、上述した各態様を適宜、適用可能である。例えば、無線通信ネットワーク、その無線局、無線局に接続される無線通信端末、接続認証方法、それらの方法または装置の機能を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記録媒体等の種々の形態で実現することができる。
【００３８】
コンピュータが読み取り可能な記録媒体としては、例えば、フレキシブルディスクやＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、光磁気ディスク、ＩＣカード、ハードディスク等種々の媒体を利用することが可能である。
【発明を実施するための最良の形態】
【００３９】
次に、本発明の実施の形態を実施例に基づいて以下の順序で説明する。
Ａ．第１実施例：
Ａ．１．プリントサービス提供システムの構成：
Ａ．２．接続認証処理：
Ａ．３．効果：
Ｂ．第２実施例：
Ｃ．第３実施例：
Ｄ．第４実施例：
Ｅ．第５実施例：
Ｆ．第６実施例：
Ｇ．変形例：
【００４０】
Ａ．第１実施例：
Ａ．１．プリントサービス提供システムの構成：
図１は、本発明を適用した通信ネットワークシステムの第１実施例としてのプリントサービス提供システムを示す概略構成図である。このプリントサービス提供システム１００は、プリントサービスを提供するプリントサービス提供装置ＰＳＶと、プリントサービス提供装置ＰＳＶにＢＴ通信回線を介して接続される携帯電話ＰＴとを備えている。ユーザは、自分の携帯電話ＰＴとプリントサービス提供装置ＰＳＶとの間を、後述する手順でＩＲ通信回線およびＢＴ通信回線を介して接続する。そして、ユーザは、プリントしたい写真（画像）の電子データを、ＢＴ通信回線を介して自分の携帯電話ＰＴからプリントサービス提供装置ＰＳＶに送信し、プリントサービス提供装置ＰＳＶでプリントすることができる。
【００４１】
プリントサービス提供装置ＰＳＶは、本発明に関係する無線通信通信機能部として、Ｉ

Ｒ通信部１０と、ＢＴ通信部２０と、認証処理制御部３０と、を備えており、ＢＴアクセスポイント（無線局）として機能する。また、携帯電話ＰＴも、同様に、本発明に関係する無線通信機能部として、ＩＲ通信部４０と、ＢＴ通信部５０と、認証処理制御部６０と、を備えており、ＢＴ端末（無線通信端末）として機能する。なお、プリントサービス提供装置ＰＳＶはコンピュータであり、内部記憶装置、外部記憶装置や有線の通信装置などの種々の周辺装置、ディスプレイインタフェースや入力インタフェースフェースなどの種々のインタフェース等、コンピュータに一般的に備えられている種々の周辺装置、制御装置、およびインタフェースを備えているが、本発明の説明上特に必要ないので、図示および説明を省略する。また、携帯電話ＰＴも同様であり、本発明の説明上特に必要のない構成要素の図示および説明を省略する。

【００４２】

ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶには、ＢＴ規格に従って最大７台のＢＴ端末（無線通信端末）がＢＴ通信回線を介して接続可能である。なお、本例では、説明を容易にするため、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶに１台の携帯電話ＰＴがＢＴ端末として接続される場合を示している。

【００４３】

プリントサービス提供装置ＰＳＶのＩＲ通信部１０と、携帯電話ＰＴのＩＲ通信部４０とは、例えば、ＩｒＤＡ（Infrared Data Association）規格に従った赤外線無線通信（ＩＲ通信）を実行する。

【００４４】

プリントサービス提供装置ＰＳＶのＢＴ通信部２０と携帯電話ＰＴのＢＴ通信部５０とは、ＢＴ規格に従った無線通信（ＢＴ通信）を実行する。

【００４５】

プリントサービス提供装置ＰＳＶの認証処理制御部３０は、プリントサービス提供装置ＰＳＶのＩＲ通信部１０およびＢＴ通信部２０の動作を制御する。携帯電話ＰＴの認証処理制御部６０は、携帯電話ＰＴのＩＲ通信部４０およびＢＴ通信部５０の動作を制御する。

【００４６】

上記プリントサービス提供システム１００では、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶと、ＢＴ端末としての携帯電話ＰＴとの間で、プリントサービス提供装置ＰＳＶの認証処理制御部３０および携帯電話ＰＴの認証処理制御部６０による制御動作に基づいて、以下で説明するように、接続認証処理が実行される。

【００４７】

Ａ．２．接続認証処理：

図２および図３は、プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される接続認証処理の手順について示す説明図である。

【００４８】

携帯電話ＰＴのユーザが、携帯電話ＰＴのＩＲ通信部４０に含まれるＩＲトランシーバ４２（図１参照）を、プリントサービス提供装置ＰＳＶのＩＲ通信部１０に含まれるＩＲトランシーバ１２（図１参照）に向けて、接続認証の開始ボタン（図示しない）を押すと、図２に示す手順でＩＲ通信が実行される。そして、携帯電話ＰＴのＢＴ通信部５０に含まれるＢＴトランシーバ５２（図１参照）と、プリントサービス提供装置ＰＳＶのＢＴ通信部２０に含まれるＢＴトランシーバ２２（図１参照）とを介して、図３に示す手順でＢＴ通信が実行され、ＢＴ通信回線の接続認証処理が行われる。

【００４９】

まず、携帯電話ＰＴの認証処理制御部６０（以下では、「端末側認証処理制御部６０」とも呼ぶ。）では、１６バイト（１２８ビット）の端末側乱数Ａｒｎを発生させる。そして、この端末側乱数Ａｒｎと、後述する１６バイトのマスクデータＭＤとの排他的論理和（ＸＯＲ）を下式（１）に従って求めることにより、端末側乱数Ａｒｎの秘匿性を高めた秘匿化端末側乱数Ａｅｎｃを生成する（ステップＳ１１０）。そして、生成した秘匿化端

末側乱数Ａｅｎｃを携帯電話ＰＴのＩＲ通信部４０（以下、「端末側ＩＲ通信部４０」とも呼ぶ。）を介してプリントサービス提供装置ＰＳＶのＩＲ通信部１０（以下では、「アクセスポイント側ＩＲ通信部１０」とも呼ぶ。）に送信する（ステップＳ１２０）。

Aenc=(Arn) XOR (MD) ...(1)

【００５０】

ここで、マスクデータＭＤは、以下のようにして生成される。図４は、マスクデータＭＤを示す説明図である。図４（ａ）は、マスクデータＭＤを生成するために生成される元データＯＤを示しており、図４（ｂ）は、元データＯＤからマスクデータＭＤを生成する手段について示している。

【００５１】

ところで、端末側乱数Ａｒｎは、後述するように、ＰＩＮコードを生成するための重要なデータであるため、秘匿性を持たせる必要がある。このため、（１）式に従って端末側乱数Ａｒｎとマスクデータ ＭＤとを排他的論理和（ＸＯＲ）することにより秘匿化端末側乱数Ａｅｎｃを生成している。

【００５２】

また、プリントサービス提供装置ＰＳＶ側において秘匿化端末側乱数Ａｅｎｃから元の端末側乱数Ａｒｎを取り出すためには、プリントサービス提供装置ＰＳＶにおいて、秘匿化端末側乱数Ａｅｎｃの生成に用いられたマスクデータＭＤと同じマスクデータを生成する必要がある。

【００５３】

そこで、マスクデータＭＤを生成するための元データＯＤとして、携帯電話ＰＴの４８ビットのＢＴアドレスＢＴ＿ＡＤＤＲ＿Ｋと、２８ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ｋのうちの１０ビットとを、図４（ａ）に示すよう交互に配置した、第０ビット（ＬＳＢ）から第１２７ビット（ＭＳＢ）の１２８ビット（１６バイト）のデータを生成することとした。なお、第１２６ビットおよび第１２７ビットの上位２ビットについては、２８ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ｋの最下位ビット（ＬＳＢ）の値に応じた値を設定することとした。具体的には、ＬＳＢの値が"０"の場合には、第１２６ビットを"１"、第１２７ビットを"０"とする。また、ＬＳＢの値の値が"１"の場合には、第１２６ビットを"１"、第１２７ビットを"０"とする。なお、上位２ビットをどちらも"０"あるいは"１"とするようにしてもよい。

【００５４】

そして、図４（ｂ）に示すように、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤＲ＿Ｋを暗号化キーとして元データＯＤを暗号化することにより、１２８ビットのマスクデータＭＤを生成する。なお、生成したマスクデータＭＤ自体も、暗号化により秘匿性が高められているので、秘匿化欄末側乱数Ａｅｎｃに含まれている端末側乱数Ａｒｎの秘匿性をさらに高めることができる。

【００５５】

なお、暗号化ルーチンとしては、例えば、ＢＴ規格で規定されているＥ２１アルゴリズム等の種々の暗号化ルーチンを利用することが可能である。ただし、Ｅ２１アルゴリズム等のＢＴ規格で規定されている暗号化ルーチンを利用することとすれば、ＢＴ通信部の暗号化回路あるいはファームウェアを共用することができるため効率的である。

【００５６】

以上のようにしてマスクデータＭＤを生成することとすれば、プリントサービス提供装置ＰＳＶにおいても、マスクデータＭＤと同じマスクデータを生成することができる。すなわち、後述する「Ｐａｇｅ」と呼ばれるモード（以下、「呼び出しモード」とも呼ぶ。）および「Ｐａｇｅ　Ｒｅｓｐｏｎｓｅ」と呼ばれるモード（以下、呼び出し応答モード）とも呼ばれる。）によって実行されるＢＴ通信回線の接続処理(以下、単に「ＢＴ通信回線接続処理」とも呼ぶ。)の過程で、携帯電話ＰＴからプリントサービス提供装置ＰＳＶにはＦＨＳパケットと呼ばれる制御コマンドが送信される。このＦＨＳパケットには、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋが

含まれている。従って、プリントサービス提供装置ＰＳＶでは、ＢＴ通信回線接続処理によって携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋを取得することができる。これにより、プリントサービス提供装置ＰＳＶにおいても、上記したマスクデータＭＤと同じマスクデータを生成することができるので、生成したマスクデータを用いて、後述するように、秘匿化端末側乱数Ａｅｎｃから端末側乱数Ａｒｎを取り出すことが可能となる。

【００５７】

なお、携帯電話ＰＴで生成される２８ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ｋのうち、以下で説明する１０ビットが、マスクデータＭＤの生成に利用される。図５は、マスクデータ生成用のＢＴクロックについて示す説明図である。

【００５８】

ＢＴ規格において、ＢＴクロックは２８ビットのカウンタとして規定されており、３１２．５μｓごとに１ずつインクリメントされて値が変化する。上記のように、プリントサービス提供装置ＰＳＶ側では、ＢＴ通信回線接処理によって取得する携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋに基づいて、マスクデータＭＤと同じマスクデータを生成し、生成したマスクデータに基づいて、秘匿化端末側乱数Ａｅｎｃから端末側乱数Ａｒｎを取得する。このため、携帯電話ＰＴにおいてマスクデータＭＤを生成する時に利用されたＢＴクロックの値に対して、プリントサービス提供装置ＰＳＶでマスクデータＭＤと同じマスクデータを生成する時に利用されるＢＴクロックの値が、変化することは許されない。なぜならば、マスクデータ生成用のＢＴクロックの値が変化した場合、マスクデータＭＤと同じマスクデータを生成することができず、秘匿化端末側乱数Ａｅｎｃから端末側乱数Ａｒｎを正しく取り出すことができないからである。

【００５９】

そこで、２７ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ｋのうち、マスクデータ生成用のＢＴクロックとして上位１０ビットのクロックを利用することとした。ただし、第１７ビットの値に応じて第１８ビット～第２７ビットの値を繰り上げ処理することとした。具体的には、第１７ビットの値が"０"の場合には、そのまま第１８ビット～第２７ビットのデータをマスクデータ生成用のＢＴクロックとする。また、第１７ビットの値が"０"の場合には、第１８ビットに"１"を足し込み繰り上げ計算を行って、繰り上げ計算後の第１８ビット～第２７ビットのデータをマスクデータ生成用のＢＴクロックとする。これにより、マスクデータ生成用のＢＴクロックＢＴ＿ＣＬＫ＿Ｋを少なくとも４０．９６ｓｅｃの間は変化しないように設定することができる。ただし、こうして設定されたマスクデータ生成用のＢＴクロックＢＴ＿ＣＬＫ＿Ｋも、多くとも８１．９２ｓｅｃ後には変化する。これによってもマスクデータＭＤの秘匿性を高めることができ、結果として携帯電話ＰＴから送信される端末側乱数Ａｒｎの秘匿性を高めることができる。なお、上記実施例では、４０秒程度ＢＴクロックが変化しないようにするために、上位１０ビットをマスクデータ生成用のＢＴクロックとして利用することとしている。しかしながら、これに限定されるものではない。もっと長い時間ＢＴクロックが変化しないようにするために、上位９ビット、上位８ビット等のように、マスクデータ生成用のＢＴクロックとして利用する上位ビット数を少なく設定するようにしてもよい。また、もっと短い時間でＢＴクロックが変化するように、上位１１ビット、上位１２ビット等のように、マスクデータ生成用のＢＴクロックとして利用する上位ビット数を多くするようにしてもよい。

【００６０】

次に、アクセスポイント側ＩＲ通信部１０では、端末側ＩＲ通信部４０から送信された秘匿化端末側乱数Ａｅｎｃを受信すると、受信した秘匿化端末側乱数Ａｅｎｃを認証処理制御部３０（以下、「アクセスポイント側認証処理制御部３０」とも呼ぶ。）に受け渡す。アクセスポイント側認証処理制御部３０では、１６バイト（１２８ビット）の返信データＰｉｆを生成させる。そして、この返信データＰｉｆと秘匿化端末側乱数Ａｅｎｃとの排他的論理和（ＸＯＲ）を下式（２）に従って求めることにより、返信データＰｉｆの秘

匿性を高めた秘匿化返信データＰｉｆｅｎｃを生成する（ステップＳ１３０）。そして、生成した秘匿化返信データＰｉｆｅｎｃをアクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する（ステップＳ１４０）。

Pifenc=(Pif) XOR (Aenc) ...(2)

【００６１】

ここで、返信データＰｉｆは、以下のようにして生成される。図６は、返信データＰｉｆを示す説明図である。返信データＰｉｆは、ＢＴ通信におけるＦＨＳパケットのペイロードデータに対応した１６バイト（１２８ビット）のデータであり、ＦＨＳパケットのペイロードデータのうち、「Ｐａｒｉｔｙ　ｂｉｔｓ」および「ＡＭ＿ＡＤＤＲ」を除いた１１７ビットのデータに、２１ビットの"０"が並ぶ「ａｌｌ　ｚｅｒｏ」領域を加えた構成を有している。なお、プリントサービス提供装置ＰＳＶの４８ビットのＢＴアドレスＢＴ＿ＡＤＤＲ＿Ａは、下位２４ビットを示す「ＬＡＰ」と、上位８ビットを示す「ＵＡＰ」と、ＬＡＰとＵＡＰを除く１６ビットを示す「ＮＡＰ」とに分けて配置される。また、２８ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ａは、下位２ビットを除く２６ビットが「CLK_{27-2}」に配置される。

【００６２】

次に、端末側ＩＲ通信部４０では、アクセスポイント側ＩＲ通信部１０から送信された秘匿化返信データＰｉｆｅｎｃを受信すると、受信した秘匿化返信データＰｉｆｅｎｃを端末側認証処理制御部６０に受け渡す。端末側認証処理制御部６０では、受け取った秘匿化返信データＰｉｆｅｎｃと、秘匿化端末側乱数Ａｅｎｃとの排他的論理和（ＸＯＲ）を下式（３）に従って求めることにより、返信データＰｉｆを取り出す（ステップＳ１５０）。

Pif=(Pifenc) XOR (Aenc) ...(3)

【００６３】

返信データＰｉｆには、上述したように、プリントサービス提供装置ＰＳＶの６バイト（４８ビット）のＢＴアドレスＢＴ＿ＡＤＤＲ＿Ａおよび２８ビットのＢＴクロックＢＴ＿ＣＬＫ＿Ｋのうち、下位２ビットを除く２６ビットのＢＴクロックが含まれているので、返信データＰｉｆに基づいて、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋを取得することができる。

【００６４】

一方、アクセスポイント側認証処理制御部３０では、１６バイト（１２８ビット）のアクセスポイント側乱数Ｃｒｎを発生させる。そして、このアクセスポイント側乱数Ｃｒｎと、秘匿化端末側乱数Ａｅｎｃとの排他的論理和（ＸＯＲ）を下式（４）に従って求めることにより、携帯電話ＰＴに送信する１６バイトの秘匿化アクセスポイント側乱数Ｃｅｎｃを生成する（ステップＳ１６０）。そして、生成した秘匿化アクセスポイント側乱数Ｃｅｎｃをアクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する（ステップＳ１７０）。

Cenc=(Crn) XOR (Aenc) ...(4)

【００６５】

秘匿化アクセスポイント側乱数Ｃｅｎｃを受信した端末側ＩＲ通信部４０では、受信した秘匿化アクセスポイント側乱数Ｃｅｎｃを端末側認証処理制御部６０に受け渡す。端末側認証処理制御部６０では、受け取った秘匿化アクセスポイント側乱数Ｃｅｎｃと、秘匿化端末側乱数Ａｅｎｃとの排他的論理和（ＸＯＲ）を下式（５）に従って求めることにより、アクセスポイント側乱数Ｃｒｎを取り出す（ステップＳ１８０）。

Crn=(Cenc) XOR (Aenc)=((Crn) XOR (Aenc)) XOR (Aenc) ...(5)

【００６６】

以上のようにして、携帯電話ＰＴとプリントサービス提供装置ＰＳＶとの間でＩＲ通信を実行することにより、携帯電話ＰＴでは、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを取得することができる。

【００６７】

ＩＲ通信が終了すると、携帯電話ＰＴとプリントサービス提供装置ＰＳＶとの間では、アクセスポイント側認証処理制御部３０がＢＴ通信部２０(以下、「アクセスポイント側ＢＴ通信部２０」とも呼ぶ。)を制御し、端末側認証処理制御部６０がＢＴ通信部５０(以下、「端末側ＢＴ通信部５０」とも呼ぶ。)を制御して、「Ｐａｇｅ(呼び出し)」および「Ｐａｇｅ　Ｒｅｓｐｏｎｓｅ(呼び出し応答)」によるＢＴ通信回線接続処理を実行して、ＢＴ通信回線の接続を確立する(ステップＳ１９０)。なお、このＢＴ通信回線接続処理は、ＢＴ通信における一般的な処理であるので詳細な説明を省略する。

【００６８】

ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶと、ＢＴ端末としての携帯電話ＰＴとの間で、ＢＴ通信回線の接続が確立されると、アクセスポイント側認証処理制御部３０は、アクセスポイント側ＢＴ通信部２０を介して受け取ったＦＨＳパケットのペイロードデータから、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋを取得する(ステップＳ２００)。

【００６９】

そして、取得した携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋに基づいて、秘匿化端末側乱数Ａｅｎｃを生成する際に利用したマスクデータＭＤと同じはずのマスクデータＭＤ'を、マスクデータＭＤと同じ手順で生成する。生成したマスクデータＭＤ'と秘匿化端末側乱数Ａｅｎｃとの排他的論理和（ＸＯＲ）を下式（６）に従って求めることにより、秘匿化端末側乱数Ａｅｎｃから端末側乱数Ａｒｎを取り出す（ステップＳ２１０）。

$$Arn=(Aenc)\ XOR\ (MD')=((Arn)\ XOR\ (MD))\ XOR\ (MD') \quad ...(6)$$

【００７０】

以上のようにして、プリントサービス提供装置ＰＳＶで発生したアクセスポイント側乱数Ｃｒｎと、携帯電話ＰＴで発生した端末側乱数Ａｒｎとが、ＩＲ通信およびＢＴ通信を介して交換される。

【００７１】

そして、アクセスポイント側認証処理制御部３０および端末側認証処理制御部６０のそれぞれにおいて、以下のようにＰＩＮコードが生成される。図７は、ＰＩＮコード生成手段を示す説明図である。アクセスポイント側認証処理制御部３０は、図７に示すように、アクセスポイント側乱数Ｃｒｎを暗号化キー（共通キー）として、端末側乱数Ａｒｎを暗号化することによりＰＩＮコードを生成することができる(ステップＳ２２０ａ)。また、端末側認証処理制御部６０でも、同様に、アクセスポイント側乱数Ｃｒｎを暗号化キー（共通キー）として、端末側乱数Ａｒｎを暗号化することで、ＰＩＮコードを生成することができる(ステップＳ２２０ｂ)。

【００７２】

なお暗号化ルーチンとしては、例えば、ＢＴ規格で規定されているＥ２２アルゴリズム等の種々の暗号化ルーチンを利用することが可能である。ただし、Ｅ２２アルゴリズムを利用すれば、ＢＴ通信部の暗号化回路あるいはファームウェアを共用することができるため効率的である。なお、端末側乱数Ａｒｎを暗号化キー（共通キー）としてアクセスポイント側乱数Ｃｒｎを暗号化してＰＩＮコードを生成するようにしてもよい。

【００７３】

以上のようにして、プリントサービス提供装置ＰＳＶおよび携帯電話ＰＴの両方でＰＩＮコードが求められると、次に、ＢＴ通信回線の接続認証処理を実行する(ステップＳ２３０)。なお、この処理は、ＢＴ通信における一般的な処理であるので説明を省略する。

【００７４】

以上のようにして、プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間のＢＴ通信回線の接続認証処理を実行することができる。

【００７５】

Ａ．３．効果：

以上のように、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶと、Ｂ

Ｔ端末としての携帯電話ＰＴとの間で、ＢＴ通信回線の接続認証を実行する場合において、携帯電話ＰＴは、接続先であるプリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを、ＩＲ通信を介して受け取る構成としている。ＩＲ通信は赤外線を伝送媒体としているため、指向性が高く信号の到達距離も短い。従って、携帯電話ＰＴとプリントサービス提供装置ＰＳＶとの間でＩＲ通信を実行するために、ユーザは、プリントサービス提供装置ＰＳＶの近くで、携帯電話ＰＴのＩＲトランシーバ４２をプリントサービス提供装置ＰＳＶのＩＲトランシーバ１２に向けてやる必要がある（図１参照）。このため、ユーザは、自分が接続したいプリントサービス提供装置の近くまで行って、自分の携帯電話とそのプリントサービス提供装置との間でＩＲ通信を実行することになる。これにより、ユーザは、自分が接続したいプリントサービス提供装置であることを確認の上で、自分の携帯電話をそのプリントサービス提供装置に対してＢＴ通信回線で接続させることができる。この結果、ＢＴ通信回線の接続を実行する場合に、従来のような、プリントサービス提供装置のモードを問い合わせモードではなく、問い合わせ不能モードとすることができるので、従来技術で説明したように、不用意な接続を抑制することが可能である。また、偽装アクセスポイントに接続して、個人情報等の重要な情報が盗まれる事態の発生を抑制することが可能である。

【００７６】

また、携帯電話ＰＴとプリントサービス提供装置ＰＳＶとの間の接続認証に用いられるＰＩＮコードを、ＩＲ通信を介して事前に交換した乱数Ａｒｎ，Ｃｒｎを用いて生成しているので、ユーザがＰＩＮコードを入力する煩雑さをなくすことができる。また、携帯電話ＰＴで発生した端末側乱数Ａｒｎ、および、プリントサービス提供装置ＰＳＶで発生したアクセスポイント側乱数Ｃｒｎを、秘匿性を高めた形式のデータに変換するとともに、指向性の高いＩＲ通信により交換し、交換した乱数の一方（実施例ではアクセスポイント側乱数Ｃｒｎ）を暗号化キー（共通キー）として、他方の乱数(実施例では端末側乱数Ａｒｎ)を暗号化してＰＩＮコードを生成している。ＰＩＮコード生成に利用されるデータおよび暗号化キーとして、乱数を利用し、これら乱数を秘匿性を高めた形式で送信することにより、ＰＩＮコード生成に利用されるデータおよび暗号化キーの秘匿性を高めることができる。また、暗号化ルーチンを用いてＰＩＮコードを生成することにより、ＰＩＮコードの秘匿性をさらに高めることができる。

【００７７】

ここで、プリントサービス提供装置ＰＳＶが取得した端末側乱数乱数Ａｒｎ、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋ、プリントサービス提供装置ＰＳＶが生成したマスクデータＭＤ'、携帯電話ＰＴが取得したアクセスポイント側乱数Ｃｒｎ、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａのうち、少なくとも１つが正しいものではなければ、プリントサービス提供装置ＰＳＶおよび携帯電話ＰＴそれぞれで生成したＰＩＮコードが一致しないことになる。この結果、ＢＴ端末としての携帯電話ＰＴの接続認証が失敗となるため、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶはＢＴ通信回線の接続を切断することができる。一方、接続認証が成功すれば、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶとＢＴ端末としての携帯電話ＰＴとの間で共有する秘密キー(リンクキー)が生成され、生成されたリンクキーを用いてＢＴ通信における通信情報の暗号化が可能となる。この結果、セキュアなＢＴ通信が可能となる。

【００７８】

なお、携帯電話ＰＴからプリントサービス提供装置ＰＳＶに送信される端末側乱数Ａｒｎ、プリントサービス提供装置ＰＳＶから携帯電話ＰＴに送信されるアクセスポイント側乱数Ｃｒｎは、ＩＲ通信で送信される際に、第３者にキャプチャされる可能性がある。そのため厳密には保護されているとは言えない。しかしながら、ＩＲ通信は指向性が高く第３者が勝手にキャプチャすることは比較的困難である。

【００７９】

また、実際にＩＲ通信で送信されているのは、端末側乱数Ａｒｎの秘匿性を高めた秘匿

化端末側乱数Ａｅｎｃであり、アクセスポイント側乱数Ｃｒｎの秘匿性を高めたアクセスポイント側送信乱数Ｃｅｎｃである。このため、仮に、秘匿化されたこれらの乱数が読み取られたとしても、秘匿化された乱数に含まれている乱数を取り出して利用することは容易ではない。

【００８０】

さらに、接続認証に利用されるＰＩＮコードは、サービス提供装置ＰＳＶと携帯電話との間で交換した端末側乱数Ａｒｎおよびアクセスポイント側乱数Ｃｒｎの一方を、暗号化キー（共通キー）として利用して、所定の暗号化ルーチンにより生成される。このため、仮に、秘匿化された乱数に含まれている乱数を取り出せたとしても、暗号化ルーチンがわからなければ、正しいＰＩＮコードを生成することはできず、接続認証を成功させることはできない。

【００８１】

また、悪意のある第３者が、乱数を取り出す手順や暗号化ルーチンを全て把握し、ＩＲ通信をキャプチャして乱数を取り出し、ＰＩＮコードを生成したとしても、この時点では、既にＢＴ通信回線の接続が確立され、接続認証も終了しているので、悪意のある第３者による接続確立および接続認証を成功させることは難しいと考えられる。

【００８２】

以上のことから、本実施例のプリントサービス提供システムでは、ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶとＢＴ端末である携帯電話ＰＴとの間で、簡便でかつ安全に接続認証を行うことが可能である。

【００８３】

以上説明したように、本実施例のプリントサービス提供システムでは、ユーザが接続したいＢＴアクセスポイントを明示的に指定することにより、指定したＢＴアクセスポイントとユーザのＢＴ端末との間の通信回線の接続を確立することを可能とするとともに、ＢＴ端末とＢＴアクセスポイントとの間の接続認証を、簡便でかつ安全に実行することが可能である。

【００８４】

なお、上記実施例における端末側乱数Ａｒｎが本発明の第１の暗証コード生成情報に相当し、アクセスポイント側乱数Ｃｒｎが本発明の第２の暗証コード生成情報に相当する。また、上記実施例におけるＰＩＮコードが本発明の暗証コードに相当する。

【００８５】

Ｂ．第２実施例：

図８は、通信ネットワークシステムの第２実施例としてのプリントサービス提供システムを示す概略構成図である。このプリントサービス提供システム２００は、第１実施例と同様に、プリントサービス提供装置ＰＳＶ２と、プリントサービス提供装置ＰＳＶ２にＢＴ通信回線を介して接続される携帯電話ＰＴとを備えている。第２実施例のプリントサービス提供装置ＰＳＶ２は、複数のＢＴ通信部、図の例では４つのＢＴ通信部２０ａ～２０ｄを備えており、携帯電話ＰＴとＢＴ通信を実行するＢＴ通信部が認証処理制御部３０Ａによって選択される構成としている点が第１実施例のプリントサービス提供装置ＰＳＶと異なっている。

【００８６】

本実施例のプリントサービス提供装置ＰＳＶ２と携帯電話ＰＴとの間では、下記に示す手順に従ってＢＴ通信が実行される。

【００８７】

（ａ）まず、第１実施例と同様に、図２に示した手順に従ってアクセスポイント側ＩＲ通信部１０と携帯電話ＰＴのＩＲ通信部４０（図１参照）との間でＩＲ通信が実行される。

（ｂ）このとき、アクセスポイント側認証処理制御部３０Ａは、所定の条件に従って複数のＢＴ通信部のなかから１つを選択する。ここでは、第３のＢＴ通信部２０ｃが選択されることとする。

（ｃ）そして、アクセスポイント側認証処理制御部３０Ａは、選択したＢＴ通信部２０ｃ

のＢＴアドレスを、第１実施例と同様に、図２に示し手順に従い、アクセスポイント側ＩＲ通信部１０を介して携帯電話ＰＴに通知する。
（ｄ）携帯電話ＰＴは、第１実施例と同様に、図３の手順に従って、選択されたＢＴ通信部２０ｃとの間で、ＢＴ通信回線の接続認証を実行し、ＢＴ通信を開始する。
【００８８】
ここで、例えば、各ＢＴ通信部の通信負荷を比較し、通信負荷が最も低いＢＴ通信部を携帯電話ＰＴの通信相手として選択することが、所定の条件として考えられる。この場合、ある携帯電話ＰＴからプリントサービス提供装置ＰＳＶ２にＢＴ通信回線の接続要求があると、複数のＢＴ通信部２０ａ～２０ｄのうち最も低い通信負荷のＢＴ通信部を選択し、選択されたＢＴ通信部を利用してＢＴ通信を実行することができるので、各ＢＴ通信部の通信負荷を平準化できる。
【００８９】
また、例えば、前回接続されたＢＴ通信部の選択および使用を禁止し、他のＢＴ通信部の中からいずれか一つを選択することや、サービス提供に利用されたＢＴ通信部の選択および使用を一定期間禁止し、他のＢＴ通信部の中からいずれか一つを選択することも所定の条件として考えられる。一度選択されたＢＴ通信部のＢＴアドレスは、プリントサービス提供装置ＰＳＶ２から送信される電波到達範囲内のＢＴ端末によって読み取られる可能性がある。上記のようにすれば、不正アクセスを防止し、セキュリティを向上させることが可能である。また、他のＢＴ通信部の中からいずれか一つを選択する場合に、上記のように最も低い通信負荷のＢＴ通信部を選択するようにしてもよい。こうすれば、不正アクセスを防止し、セキュリティを向上させるとともに、通信負荷の平準化を図ることができる。なお、選択および使用禁止となったＢＴ通信部は、外部から要求される「Ｐａｇｅ」処理に対して、「Ｐａｇｅ　Ｒｅｓｐｏｎｓｅ」処理を行わないように設定しておくことが望ましい。
【００９０】
Ｃ．第３実施例：
図９は、通信ネットワークシステムの第３実施例としてのプリントサービス提供システムを示す概略構成図である。このプリントサービス提供システム３００も、第１実施例と同様に、プリントサービス提供装置ＰＳＶ３と、プリントサービス提供装置ＰＳＶ３にＢＴ通信回線を介して接続される携帯電話ＰＴとを備えている。第３実施例のプリントサービス提供装置ＰＳＶ３は、ＩＲ通信部１０と、ＢＴ通信部２０Ｂと、認証処理制御部３０Ｂとを備えており、基本的に第１実施例のプリントサービス提供装置ＰＳＶと同様の構成を有している。ただし、認証処理制御部３０Ｂが、ＢＴ通信部２０Ｂに設定するための複数のＢＴアドレス、ここでは、４つのＢＴアドレスＢＴ＿ＡＤＤＲ＿Ａ１～ＢＴ＿ＡＤＤＲ＿Ａ４を図示しないメモリに有しており、いずれか一つのＢＴアドレスが選択されて、ＢＴ通信部２０Ｂに設定される構成としている点が異なっている。
【００９１】
本実施例のプリントサービス提供装置ＰＳＶ３と携帯電話ＰＴとの間では、下記に示す手順に従ってＢＴ通信が実行される。
【００９２】
（ａ）まず、第１実施例と同様に、図２に示した手順に従ってアクセスポイント側ＩＲ通信部１０と携帯電話ＰＴのＩＲ通信部４０（図１参照）との間でＩＲ通信が実行される。
（ｂ）このとき、アクセスポイント側認証処理制御部３０Ｂは、所定の条件に従って複数のＢＴアドレスの中から１つを選択し、ＢＴ通信部２０Ｂに設定する。ここでは、第３のＢＴアドレスＢＴ＿ＡＤＤＲ＿Ａ３が選択されていることとする。
（ｃ）そして、アクセスポイント側認証処理制御部３０Ｂは、選択したＢＴアドレスＢＴ＿ＡＤＤＲ＿Ａ３を、第１実施例と同様に、図２に示した手順に従い、アクセスポイント側ＩＲ通信部１０を介して携帯電話ＰＴに通知する。
（ｄ）携帯電話ＰＴは、第１実施例と同様に、図３の手順に従って、ＢＴ通信部２０Ｂととの間で、ＢＴ通信回線の接続認証を実行し、ＢＴ通信を開始する。

【００９３】
ここで、例えば、用意されている複数のＢＴアドレスそれぞれの使用状況を考慮し、使用されていない期間の最も長いＢＴアドレスを１つ選択することが所定の条件として考えられる。この場合、以下の効果を得ることができる。
【００９４】
一度選択されたＢＴ通信部のＢＴアドレスは、プリントサービス提供装置ＰＳＶ３から送信される電波到達範囲内のＢＴ端末によって読み取られる可能性がある。しかしながら、上記のように、一度使用されたＢＴアドレスの使用を、ある期間禁止にすることができれば、不正アクセスを防止し、セキュリティを向上させることが可能である。また、一度サービスの提供を受けた正規のユーザが、別の未登録のユーザにプリントサービス提供装置ＰＳＶ３のＢＴアドレスを教えることによって、不正アクセスが行われる可能性を抑制することもできる。なぜならば、上記のようにすれば、その未登録のユーザが、接続しようとしたときにＢＴ通信部２０Ｂに設定されるＢＴアドレスは異なったものになっている可能性が高くなるからである。
【００９５】
なお、本実施例においても、第２実施例のように複数のＢＴ通信部を備える構成として、各ＢＴ通信部の通信負荷を平準化しつつ、セキュリティの確保を柔軟に行うことができるようにしてもよい。
【００９６】
Ｄ．第４実施例：
図１０は、通信ネットワークシステムの第４実施例としてのプリントサービス提供システムを示す概略構成図である。このサービス提供システム４００は、第１実施例と同様に、プリントサービス提供装置ＰＳＶ４と、プリントサービス提供装置ＰＳＶ４にＢＴ通信回線を介して接続される携帯電話ＰＴとを備えている。第４実施例のプリントサービス提供装置ＰＳＶ４は、第２実施例のプリントサービス提供装置ＰＳＶ２と同様に、複数のＢＴ通信部、図の例では４つのＢＴ通信部２０ａ～２０ｄを備え、かつ、複数のＩＲ通信部、図の例では３つのＩＲ通信部１０ａ～１０ｃを備えており、認証処理制御部３０Ｃによって、携帯電話ＰＴとの間でＩＲ通信を実行するＩＲ通信部が制御され、携帯電話ＰＴとＢＴ通信を実行するＢＴ通信部が選択される構成としている点が第１実施例のプリントサービス提供装置ＰＳＶおよび第２実施例のプリントサービス提供装置ＰＳＶ２と異なっている。
【００９７】
本実施例のサービス提供システム４００としては、例えば、ファミリーレストランに設置するプリントサービス提供システムが考えられる。この場合、ファミリーレストランのテーブルごとにＩＲ通信部を配置することができる。ユーザは自分が着席したテーブル上に設けられたＩＲ通信部に、自分の携帯電話のＩＲ通信部を向けて、サービスの提供を指示する。プリントサービス提供装置ＰＳＶ４の認証処理制御部３０Ｃは、サービス提供の要求が有った携帯電話ＰＴとのＩＲ通信を実行するＩＲ通信部の配置位置から、どのテーブルに座ったユーザに対してサービスを提供すべきか確定できる。そして、下記に示す手順に従い、テーブルの位置に応じて、サービス提供に使用するＢＴ通信部が選択され、プリントサービス提供装置ＰＳＶ４と携帯電話ＰＴとの間でＢＴ通信が実行される。
【００９８】
（ａ）まず、第１実施例と同様に、図２に示した手順に従ってアクセスポイント側ＩＲ通信部と携帯電話ＰＴのＩＲ通信部４０（図１参照）との間でＩＲ通信が実行される。ここでは、第１のＩＲ通信部１０ａと携帯電話ＰＴのＩＲ通信部４０との間でＩＲ通信が実行されることとする。
（ｂ）このとき、アクセスポイント側認証処理制御部３０Ｃは、所定の条件に従って複数のＢＴ通信部の中から１つを選択する。ここでは、第３のＢＴ通信部２０ｃが選択されることとする。
（ｃ）そして、アクセスポイント側認証処理制御部３０Ｃは、選択したＢＴ通信部２０ｃ

のＢＴアドレスを、第１実施例と同様に、図２に示し手順に従い、第１のアクセスポイント側ＩＲ通信部１０ａを介して携帯電話ＰＴに通知する。
（ｄ）携帯電話ＰＴは、第１実施例と同様に、図３の手順に従って、選択されたＢＴ通信部２０ｃとの間で、ＢＴ通信回線の接続認証を実行し、ＢＴ通信を開始する。
【００９９】
ここで、例えば、ＩＲ通信を行っている第１のアクセスポイント側ＩＲ通信部に最も近く、かつ、通信負荷が最も低いＢＴ通信部を携帯電話ＰＴの通信相手として選択することが、所定の条件として考えられる。
【０１００】
この場合、複数のＢＴ通信部のうち最も低い通信負荷のＢＴ通信部を選択し、選択されたＢＴ通信部を利用してＢＴ通信を実行することができるので、各ＢＴ通信部の通信負荷を平準化できる。
【０１０１】
また、ＩＲ通信を実行しているＩＲ通信部の配置位置に最も近いＢＴ通信部を選択することとしているので、ファミリーレストランのように、サービスエリアが広い場合に、ユーザに最も近いＢＴ通信部を選択することにより、電波強度の強い安定した通信を行うことが可能である。
【０１０２】
なお、第４実施例においても、第３実施例のように設定可能な複数のＢＴアドレスを用意し、選択したＢＴアドレスを、使用するＢＴ通信部に設定する構成を加えるようにすれば、各ＢＴ通信部の通信負荷を平準化しつつ、ユーザに最も近いＢＴ通信部を選択して安定な通信を行うことができるとともに、セキュリティの確保を柔軟に行うことができる。
【０１０３】
Ｅ．第５実施例：
上記第１実施例では、暗号化キーとして共通キー(共通鍵)を利用し、ＢＴアクセスポイントとＢＴ端末との間で相互に交換した共通鍵を用いてＰＩＮコードを生成することにより、ＢＴ端末とＢＴアクセスポイントとの間の接続認証を、簡便でかつ安全に実行することを可能とする場合を例に説明している。これに対して、以下で説明するように、ＢＴアクセスポイントにおいて、ＢＴ端末から送信された公開鍵（公開キー）を用いてＰＩＮコードを暗号化し、暗号化したＰＩＮコードをＢＴ端末に送信し、ＢＴ端末において、暗号化したＰＩＮコードを受信し、秘密鍵（秘密キー）を用いて復号することにより、ＢＴ端末とＢＴアクセスポイントとの間の接続認証を、安全に実行することも可能である。
【０１０４】
図１１は、プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される、第５実施例としての接続認証処理の手順について示す説明図である。プリントサービス提供装置ＰＳＶおよび携帯電話ＰＴの構成は、各ブロックにおける処理が図１１の処理手順に従って実行される点を除いて、基本的に第１実施例(図１参照)と同じである。
【０１０５】
携帯電話ＰＴのユーザが、携帯電話ＰＴのＩＲ通信部４０に含まれるＩＲトランシーバ４２（図１参照）を、プリントサービス提供装置ＰＳＶのＩＲ通信部１０に含まれるＩＲトランシーバ１２（図１参照）に向けて、接続認証の開始ボタン（図示しない）を押すと、図１１に示す手順でＩＲ通信が実行される。そして、携帯電話ＰＴのＢＴ通信部５０に含まれるＢＴトランシーバ５２（図１参照）と、プリントサービス提供装置ＰＳＶのＢＴ通信部２０に含まれるＢＴトランシーバ２２（図１参照）とを介してＢＴ通信が実行され、ＢＴ通信回線の接続認証処理が行われる。
【０１０６】
まず、携帯電話ＰＴの端末側認証処理制御部６０は、公開鍵Ｋｅｎｃおよび秘密鍵Ｋｄｅｃを設定する(ステップＳ３１０)。ただし、公開鍵Ｋｅｎｃおよび秘密鍵Ｋｄｅｃは毎回同じものが設定されてもよい。そして、設定した公開鍵Ｋｅｎｃを、携帯電話ＰＴの端末側ＩＲ通信部４０を介してプリントサービス提供装置ＰＳＶのアクセスポイント側ＩＲ

通信部１０に送信する(ステップＳ３２０)。

【０１０７】

アクセスポイント側ＩＲ通信部１０は、端末側ＩＲ通信部４０から送信された公開鍵Ｋｅｎｃを受信すると、受信した公開鍵Ｋｅｎｃをアクセスポイント側認証処理制御部３０に受け渡す。

【０１０８】

アクセスポイント側認証処理制御部３０は、携帯電話ＰＴにＰＩＮコードを割り当て(ステップＳ３３０)、割り当てたＰＩＮコードを公開鍵Ｋｅｎｃを用いて暗号化する(ステップＳ３４０)。ＰＩＮコードは毎回違うものであることが好ましい。そして、暗号化したＰＩＮコードＰＩＮｅｎｃを、アクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する(ステップＳ３５０)。なお、公開鍵を用いた暗号としては、ＲＳＡ暗号を利用する。ＲＳＡ暗号は、非常に大きな数の素因数分解が困難であることを利用した暗号である。

【０１０９】

端末側ＩＲ通信部４０は、アクセスポイント側ＩＲ通信部１０から送信された、暗号化ＰＩＮコードＰＩＮｅｎｃを受信すると、受信した暗号化ＰＩＮコードＰＩＮｅｎｃを端末側認証処理制御部６０に受け渡す。

【０１１０】

端末側認証処理制御部６０は、秘密鍵Ｋｄｅｃを用いて、受け取った暗号化ＰＩＮコードＰＩＮｅｎｃからＰＩＮコードを復号する(ステップＳ３６０)。

【０１１１】

一方、アクセスポイント側認証処理制御部３０は、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを、アクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する(ステップＳ３７０)。

【０１１２】

端末側ＩＲ通信部４０は、受信したプリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを端末側認証処理制御部６０に受け渡す。これにより、端末側認証処理制御部６０は、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを取得する。

【０１１３】

ＩＲ通信を終了すると、ＢＴ端末としての携帯電話ＰＴとＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶとの間で、ＢＴ通信を開始する。

【０１１４】

まず、ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶのアクセスポイント側認証処理制御部３０がアクセスポイント側ＢＴ通信部２０を制御し、ＢＴ端末である携帯電話ＰＴの端末側認証処理制御部６０が端末側ＢＴ通信部５０を制御して、「Ｐａｇｅ(呼び出し)」および「Ｐａｇｅ　Ｒｅｓｐｏｎｓｅ(呼び出し応答)」によるＢＴ通信回線接続処理を実行して、ＢＴ通信回線の接続を確立する(ステップＳ３８０)。

【０１１５】

ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶと、ＢＴ端末である携帯電話ＰＴとの間で、ＢＴ通信回線の接続が確立されると、アクセスポイント側認証処理制御部３０は、アクセスポイント側ＢＴ通信部２０を介して受け取ったＦＨＳパケットのペイロードデータから、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋを取得する(ステップＳ３９０)。

【０１１６】

以上のようにして、携帯電話ＰＴにおいて、プリントサービス提供装置ＰＳＶで割り当てられたＰＩＮコードが求められ、携帯電話ＰＴおよびプリントサービス提供装置ＰＳＶとの間で、互いのＢＴアドレスおよびＢＴクロックが交換されると、さらに、これらの情報を利用してＢＴ通信回線の接続認証処理が実行される(ステップＳ２３０)。

【０１１７】

以上説明したように、本実施例においても、ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶと、ＢＴ端末である携帯電話ＰＴとの間で、ＢＴ通信回線の接続認証を実行する場合において、携帯電話ＰＴは、接続先であるプリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを、ＩＲ通信を介して受け取る構成としている。これにより、ユーザは、自分が接続したいプリントサービス提供装置であることを確認の上で、自分の携帯電話をそのプリントサービス提供装置に対してＢＴ通信回線で接続させることができる。この結果、ＢＴ通信回線の接続を実行する場合に、従来のような、プリントサービス提供装置のモードを問い合わせモードではなく、問い合わせ不能モードとすることができるので、従来技術で説明したように、不用意な接続を抑制することが可能である。また、偽装アクセスポイントに接続して、個人情報等の重要な情報が盗まれる事態の発生を抑制することが可能である。

【０１１８】

また、ＢＴ端末である携帯電話ＰＴとＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶとの間の接続認証に用いられるＰＩＮコードを、公開鍵を用いて暗号化し、暗号化したＰＩＮコードを示す情報をＩＲ通信によってプリントサービス提供装置ＰＳＶから携帯電話ＰＴに送信する構成としている。これにより、ＰＩＮコードの秘匿性を高めることができる。

【０１１９】

従って、本実施例のプリントサービス提供システムでは、ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶとＢＴ端末である携帯電話ＰＴとの間で、簡便でかつ安全に接続認証を行うことが可能である。ただし、公開鍵を用いた暗号方式の場合、暗号化および復号化のための演算処理が複雑であるため、ＣＰＵの処理能力が比較的低い装置では不向きである。一方、第１実施例のように共通鍵を用いた場合は、演算処理が比較的簡単であるため、ＣＰＵの処理能力が比較的低い装置に容易に適用することができるという利点がある。

【０１２０】

なお、本実施例は、第１実施例のプリントサービス提供システムにおいて、本実施例の接続認証の処理手順を適用した場合について説明したが、第２実施例のプリントサービス提供システムと同様に、複数のＢＴ通信部を備えて、所定の条件に従って１つのＢＴ通信部を選択する構成とするようにしてもよい。また、第３実施例のプリントサービス提供システムと同様に、複数のＢＴアドレスを有しており、所定の条件に従って１つのＢＴアドレスを選択する構成とするようにしてもよい。さらに、第４実施例のプリントサービス提供システムと同様に、複数のＢＴ通信部と、複数のＩＲ通信部とを備えて、所定の条件に従って１つのＢＴ通信部を選択する構成とするようにしてもよい。また、複数のＢＴ通信部を備え、第１の条件に従って１つのＢＴ通信部を選択し、第２の条件に従って１つのＢＴアドレスを選択する構成としてもよい。

【０１２１】

Ｆ．第６実施例：

また、以下で説明するように、ＢＴ端末において、ＢＴアクセスポイントから送信された公開鍵を用いてＰＩＮコードを暗号化し、暗号化したＰＩＮコードをＢＴアクセスポイントに送信し、ＢＴアクセスポイントにおいて、暗号化したＰＩＮコードを受信し、秘密鍵を用いて復号することにより、ＢＴ端末とＢＴアクセスポイントとの間の接続認証を、安全に実行することも可能である。

【０１２２】

図１２は、プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される、第６実施例としての接続認証処理の手順について示す説明図である。プリントサービス提供装置ＰＳＶおよび携帯電話ＰＴの構成は、各ブロックにおける処理が図１１の処理手順に従って実行される点を除いて、基本的に第１実施例(図１参照)と同じである。

【０１２３】

携帯電話ＰＴのユーザが、携帯電話ＰＴのＩＲ通信部４０に含まれるＩＲトランシーバ

４２（図１参照）を、プリントサービス提供装置ＰＳＶのＩＲ通信部１０に含まれるＩＲトランシーバ１２（図１参照）に向けて、接続認証の開始ボタン（図示しない）を押すと、図１２に示す手順でＩＲ通信が実行される。そして、携帯電話ＰＴのＢＴ通信部５０に含まれるＢＴトランシーバ５２（図１参照）と、プリントサービス提供装置ＰＳＶのＢＴ通信部２０に含まれるＢＴトランシーバ２２（図１参照）とを介してＢＴ通信が実行され、ＢＴ通信回線の接続認証処理が行われる。

【０１２４】

まず、携帯電話ＰＴの端末側認証処理制御部６０は、ＰＩＮコードを暗号化するための公開鍵の送信要求コマンドを、携帯電話ＰＴの端末側ＩＲ通信部４０を介してプリントサービス提供装置ＰＳＶのアクセスポイント側ＩＲ通信部１０に送信する(ステップＳ４１０)。

【０１２５】

アクセスポイント側ＩＲ通信部１０は、端末側ＩＲ通信部４０から送信された公開鍵送信要求コマンドを受信すると、受信した公開鍵送信要求をアクセスポイント側認証処理制御部３０に受け渡す。

【０１２６】

アクセスポイント側認証処理制御部３０は、公開鍵Ｋｅｎｃと秘密鍵Ｋｄｅｃとを設定し（ステップＳ４２０）、設定した公開鍵Ｋｅｎｃを、アクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する(ステップＳ４３０)。

【０１２７】

端末側ＩＲ通信部４０は、アクセスポイント側ＩＲ通信部１０から送信された、公開鍵Ｋｅｎｃを受信すると、受信した公開鍵Ｋｅｎｃを端末側認証処理制御部６０に受け渡す。

【０１２８】

携帯電話ＰＴの端末側認証処理制御部６０は、プリントサービス提供装置ＰＳＶにＰＩＮコードを割り当て(ステップＳ４４０)、割り当てたＰＩＮコードを公開鍵Ｋｅｎｃを用いて暗号化する(ステップＳ４５０)。ＰＩＮコードは毎回違うものであることが好ましい。そして、暗号化したＰＩＮコードＰＩＮｅｎｃを、端末側ＩＲ通信部４０を介してアクセスポイント側ＩＲ通信部１０に送信する(ステップＳ４６０)。なお、公開鍵を用いた暗号としては、第５実施例と同様にＲＳＡ暗号を利用する。

【０１２９】

アクセスポイント側ＩＲ通信部１０は、端末側ＩＲ通信部４０から送信された、暗号化ＰＩＮコードＰＩＮｅｎｃを受信すると、受信した暗号化ＰＩＮコードＰＩＮｅｎｃをアクセスポイント側証処理制御部３０に受け渡す。

【０１３０】

アクセスポイント側認証処理制御部３０は、秘密鍵Ｋｄｅｃを用いて、受け取った暗号化ＰＩＮコードＰＩＮｅｎｃからＰＩＮコードを復号する(ステップＳ４７０)。

【０１３１】

そして、アクセスポイント側認証処理制御部３０は、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを、アクセスポイント側ＩＲ通信部１０を介して端末側ＩＲ通信部４０に送信する(ステップＳ４８０)。

【０１３２】

端末側ＩＲ通信部４０は、受信したプリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを端末側認証処理制御部６０に受け渡す。これにより、端末側認証処理制御部６０は、プリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを取得する。

【０１３３】

ＩＲ通信を終了すると、ＢＴ端末としての携帯電話ＰＴとＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶとの間で、ＢＴ通信を開始する。

【０１３４】

まず、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶのアクセスポイント側認証処理制御部３０がアクセスポイント側ＢＴ通信部２０を制御し、ＢＴ端末としての携帯電話ＰＴの端末側認証処理制御部６０が端末側ＢＴ通信部５０を制御して、「Ｐａｇｅ(呼び出し)」および「Ｐａｇｅ　Ｒｅｓｐｏｎｓｅ(呼び出し応答)」によるＢＴ通信回線接続処理を実行して、ＢＴ通信回線の接続を確立する(ステップＳ４９０)。

【０１３５】

ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶと、ＢＴ端末としての携帯電話ＰＴとの間で、ＢＴ通信回線の接続が確立されると、アクセスポイント側認証処理制御部３０は、アクセスポイント側ＢＴ通信部２０を介して受け取ったＦＨＳパケットのペイロードデータから、携帯電話ＰＴのＢＴアドレスＢＴ＿ＡＤＤ＿ＫおよびＢＴクロックＢＴ＿ＣＬＫ＿Ｋを取得する(ステップＳ５００)。

【０１３６】

以上のようにして、プリントサービス提供装置ＰＳＶにおいて、携帯電話ＰＴで割り当てられたＰＩＮコードが求められ、携帯電話ＰＴおよびプリントサービス提供装置ＰＳＶにおいて、互いのＢＴアドレスおよびＢＴクロックが交換されると、さらに、これらを利用してＢＴ通信回線の接続認証処理が実行される(ステップＳ５１０)。

【０１３７】

以上説明したように、本実施例においても、ＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶと、ＢＴ端末としての携帯電話ＰＴとの間で、ＢＴ通信回線の接続認証を実行する場合において、携帯電話ＰＴは、接続先であるプリントサービス提供装置ＰＳＶのＢＴアドレスＢＴ＿ＡＤＤＲ＿ＡおよびＢＴクロックＢＴ＿ＣＬＫ＿Ａを、ＩＲ通信を介して受け取る構成としている。これにより、ユーザは、自分が接続したいプリントサービス提供装置であることを確認の上で、自分の携帯電話をそのプリントサービス提供装置に対してＢＴ通信回線で接続させることができる。この結果、ＢＴ通信回線の接続を実行する場合に、従来のような、プリントサービス提供装置のモードを問い合わせモードではなく、問い合わせ不能モードとすることができるので、従来技術で説明したように、不用意な接続を抑制することが可能である。また、偽装アクセスポイントに接続して、個人情報等の重要な情報が盗まれる事態の発生を抑制することが可能である。

【０１３８】

また、ＢＴ端末としての携帯電話ＰＴとＢＴアクセスポイントとしてのプリントサービス提供装置ＰＳＶとの間の接続認証に用いられるＰＩＮコードを、公開鍵を用いて暗号化し、暗号化ＰＩＮコードをＩＲ通信によって携帯電話ＰＴからプリントサービス提供装置ＰＳＶに送信する構成としている。これにより、ＰＩＮコードの秘匿性を高めることができる。

【０１３９】

従って、本実施例のプリントサービス提供システムでは、ＢＴアクセスポイントであるプリントサービス提供装置ＰＳＶとＢＴ端末である携帯電話ＰＴとの間で、簡便でかつ安全に接続認証を行うことが可能である。

【０１４０】

なお、本実施例と第５実施例とは、ＰＩＮコードを公開鍵（暗号化キー）を用いて暗号化し、ＩＲ通信によって送信する構成としている点で同じである。しかしながら、第５実施例は、ＰＩＮコードを、プリントサービス提供装置ＰＳＶで公開鍵を用いて暗号化し、携帯電話ＰＴで秘密鍵（複合化キー）を用いて復号する構成であるのに対して、本実施例は、携帯電話ＰＴで公開鍵を用いて暗号化し、プリントサービス提供装置ＰＳＶで秘密鍵を用いて復号する構成としている点が異なっている。

【０１４１】

ここで、ＲＳＡ暗号は、暗号化よりも復号化の処理が非常に複雑であり、演算処理時間を多く要するものである。例えば、暗号化の処理時間を１とすると、復号化の処理時間は２６程度である。携帯電話ＰＴは比較的処理能力が低く低速なＣＰＵを備える可能性が高く、第５実施例のようにＰＩＮコードの復号化を携帯電話ＰＴで行う構成とした場合、復

号化の処理に要する時間が大きくなる可能性が高い。一方、本実施例は、ＰＩＮコードの暗号化を携帯電話ＰＴで行い、ＰＩＮコードの復号化をプリントサービス提供装置ＰＳＶで行う構成としており、比較的処理能力が高く高速なＣＰＵを備える可能性が高いプリントサービス提供装置ＰＳＶ側でＰＩＮコードを復号することができるという利点がある。

【０１４２】

なお、本実施例は、第１実施例のプリントサービス提供システムにおいて、本実施例の接続認証の処理手順を適用した場合について説明したが、第２実施例のプリントサービス提供システムと同様に、複数のＢＴ通信部を備えて、所定の条件に従って１つのＢＴ通信部を選択する構成とするようにしてもよい。また、第３実施例のプリントサービス提供システムと同様に、複数のＢＴアドレスを有しており、所定の条件に従って１つのＢＴアドレスを選択する構成とするようにしてもよい。さらに、第４実施例のプリントサービス提供システムと同様に、複数のＢＴ通信部と、複数のＩＲ通信部とを備えて、所定の条件に従って１つのＢＴ通信部を選択する構成とするようにしてもよい。また、複数のＢＴ通信部を備え、第１の条件に従って１つのＢＴ通信部を選択し、第２の条件に従って１つのＢＴアドレスを選択する構成としてもよい。

【０１４３】

Ｇ．変形例：

なお、この発明は上記の実施例や実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の態様において実施することが可能である。例えば、次のような変形も可能である。

【０１４４】

Ｇ１．変形例１：

上記各実施例では、ＢＴアクセスポイントとしてのプリントサービス提供装置と、ＢＴ端末としての携帯電話とで構成されるプリントサービス提供システムを、通信ネットワークシステムの例として説明しているが、これに限定されるものではない。ＢＴアクセスポイントとしての種々のサービス提供装置と、ＢＴ端末としての種々の無線通信端末とで構成されるサービス提供システム等、ＢＴ通信を利用した種々の通信ネットワークシステムに適用することができる。

【０１４５】

Ｇ２．変形例２：

上記実施例ではＢＴによる通信ネットワークシステムを例に示しているがこれに限定されるものではなく、種々の無線通信規格を利用した通信ネットワークシステムに適用することもできる。

【０１４６】

Ｇ３．変形例３：

上記実施例では、指向性を有する赤外線を通信媒体とするＩＲ通信を例に説明しているが、これに限定されるものではなく、種々の指向性を有する通信媒体を利用した指向性通信を利用することが可能である。例えば、通信媒体として、可視光線や超音波、レーザ等が利用できる。

【０１４７】

Ｇ４．変形例４：

なお、上記実施例の各構成要素は、ハードウェアによって構成されていてもよく、また、ハードウェアによる構成とソフトウェアによる構成の組合せによって構成されていてもよい。ソフトウェアによる構成は、図示しない記憶装置に格納されたコンピュータプログラムをコンピュータが実行することによって実現される。

【図面の簡単な説明】

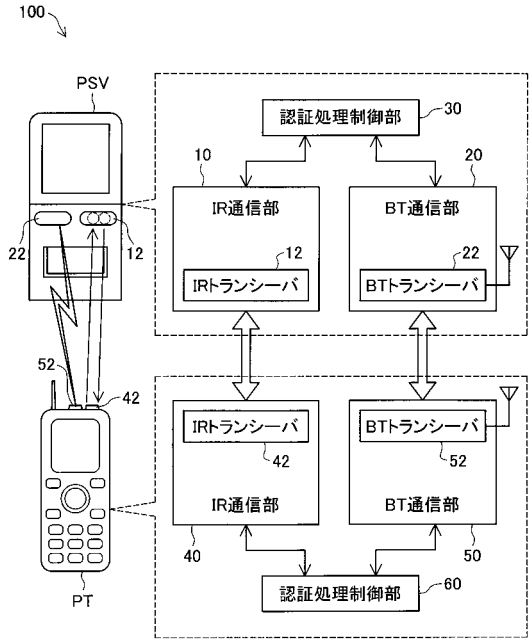
【０１４８】

【図１】本発明を適用した通信ネットワークシステムの第１実施例としてのプリントサービス提供システムを示す概略構成図である。

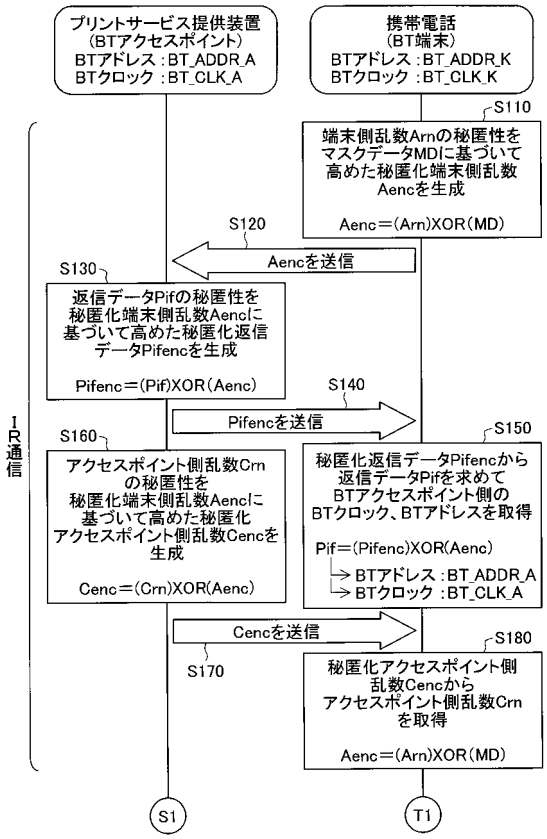
【図２】プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される接続認証処

理の手順について示す説明図である。
【図３】プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される接続認証処理の手順について示す説明図である。
【図４】マスクデータＭＤを示す説明図である。
【図５】マスクデータ生成用のＢＴクロックについて示す説明図である。
【図６】返信データＰｉｆを示す説明図である。
【図７】ＰＩＮコード生成手段を示す説明図である。
【図８】通信ネットワークシステムの第２実施例としてのプリントサービス提供システムを示す概略構成図である。
【図９】通信ネットワークシステムの第３実施例としてのプリントサービス提供システムを示す概略構成図である。
【図１０】通信ネットワークシステムの第４実施例としてのプリントサービス提供システムを示す概略構成図である。
【図１１】プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される、第５実施例としての接続認証処理の手順について示す説明図である。
【図１２】プリントサービス提供装置ＰＳＶと携帯電話ＰＴとの間で実行される、第６実施例としての接続認証処理の手順について示す説明図である。
【符号の説明】
【０１４９】
１００...プリントサービス提供システム
２００...プリントサービス提供システム
３００...プリントサービス提供システム
４００...プリントサービス提供システム
ＰＳＶ...プリントサービス提供装置
ＰＳＶ２...プリントサービス提供装置
ＰＳＶ３...プリントサービス提供装置
ＰＳＶ４...プリントサービス提供装置
ＰＴ...携帯電話
１０...ＩＲ通信部（アクセスポイント側ＩＲ通信部）
１２...ＩＲトランシーバ
１０ａ...ＩＲ通信部（アクセスポイント側ＩＲ通信部）
１０ｂ...ＩＲ通信部（アクセスポイント側ＩＲ通信部）
１０ｃ...ＩＲ通信部（アクセスポイント側ＩＲ通信部）
２０...ＢＴ通信部（アクセスポイント側ＢＴ通信部）
２２...ＢＴトランシーバ
２０ａ～２０ｄ...ＢＴ通信部（アクセスポイント側ＢＴ通信部）
３０...側認証処理制御部（アクセスポイント側認証処理制御部）
３０Ａ...認証処理制御部（アクセスポイント側認証処理制御部）
３０Ｂ...認証処理制御部（アクセスポイント側認証処理制御部）
３０Ｃ...認証処理制御部（アクセスポイント側認証処理制御部）
４０...ＩＲ通信部（端末側ＩＲ通信部）
４２...ＩＲトランシーバ
５０...ＢＴ通信部（端末側ＢＴ通信部）
５２...ＢＴトランシーバ
６０...側認証処理制御部（端末側側認証処理制御部）

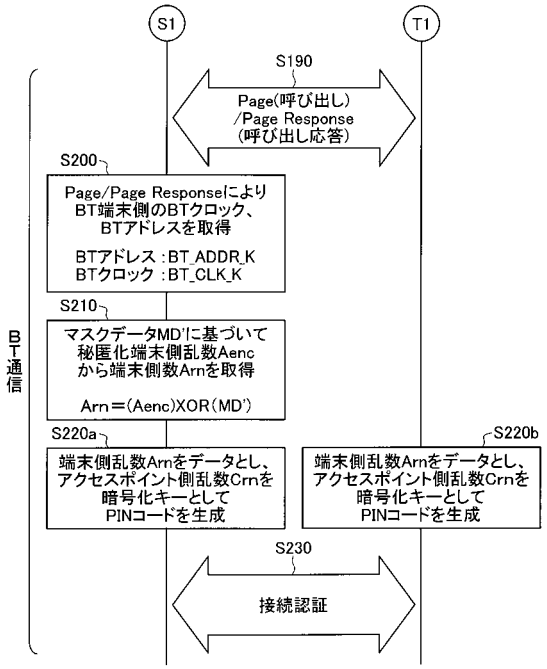
【図１】


100
PSV
認証処理制御部
30
10
20
IR通信部
BT通信部
12
22
IRトランシーバ
BTトランシーバ
52
42
40
50
60
PT

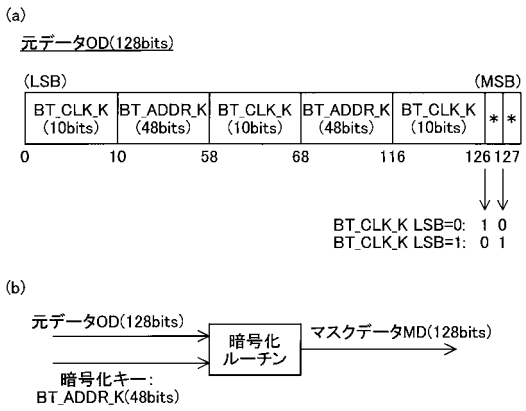
【図２】


プリントサービス提供装置
(BTアクセスポイント)
BTアドレス :BT_ADDR_A
BTクロック :BT_CLK_A
携帯電話
(BT端末)
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
S110
端末側乱数Arnの秘匿性を
マスクデータMDに基づいて
高めた秘匿化端末側乱数
Aencを生成
Aenc=(Arn)XOR(MD)
S120
Aencを送信
S130
返信データPifの秘匿性を
秘匿化端末側乱数Aencに
基づいて高めた秘匿化返信
データPifencを生成
Pifenc=(Pif)XOR(Aenc)
S140
Pifencを送信
IR通信
S160
アクセスポイント側乱数Crn
の秘匿性を
秘匿化端末側乱数Aencに
基づいて高めた秘匿化
アクセスポイント側乱数Cencを
生成
Cenc=(Crn)XOR(Aenc)
S150
秘匿化返信データPifencから
返信データPifを求めて
BTアクセスポイント側の
BTクロック、BTアドレスを取得
Pif=(Pifenc)XOR(Aenc)
BTアドレス :BT_ADDR_A
BTクロック :BT_CLK_A
Cencを送信
S170
S180
秘匿化アクセスポイント側
乱数Cencから
アクセスポイント側乱数Crn
を取得
Aenc=(Arn)XOR(MD)
S1
T1

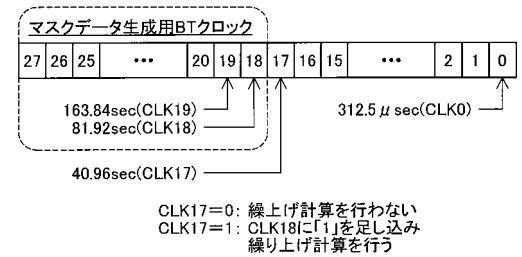
【図３】


S1
T1
S190
Page(呼び出し)
/Page Response
(呼び出し応答)
S200
Page/Page Responseにより
BT端末側のBTクロック、
BTアドレスを取得
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
S210
マスクデータMD'に基づいて
秘匿化端末側乱数Aenc
から端末側数Arnを取得
Arn=(Aenc)XOR(MD')
BT通信
S220a
端末側乱数Arnをデータとし、
アクセスポイント側乱数Crnを
暗号化キーとして
PINコードを生成
S220b
端末側乱数Arnをデータとし、
アクセスポイント側乱数Crnを
暗号化キーとして
PINコードを生成
S230
接続認証

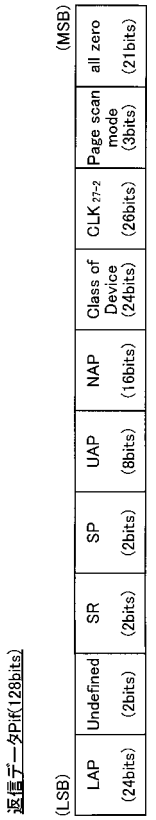
【図４】


(a)
元データOD(128bits)
(LSB)
(MSB)
BT_CLK_K
(10bits)
BT_ADDR_K
(48bits)
BT_CLK_K
(10bits)
BT_ADDR_K
(48bits)
BT_CLK_K
(10bits)
*
*
0
10
58
68
116
126
127
BT_CLK_K LSB=0: 1 0
BT_CLK_K LSB=1: 0 1
(b)
元データOD(128bits)
暗号化キー:
BT_ADDR_K(48bits)
暗号化
ルーチン
マスクデータMD(128bits)

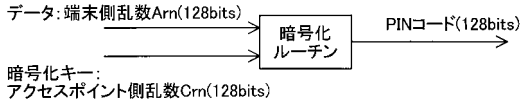
【図５】


BTクロック(28ビットのカウンタ)
マスクデータ生成用BTクロック
27
26
25
20
19
18
17
16
15
2
1
0
163.84sec(CLK19)
81.92sec(CLK18)
40.96sec(CLK17)
312.5 μ sec(CLK0)
CLK17=0: 繰上げ計算を行わない
CLK17=1: CLK18に「1」を足し込み
繰り上げ計算を行う

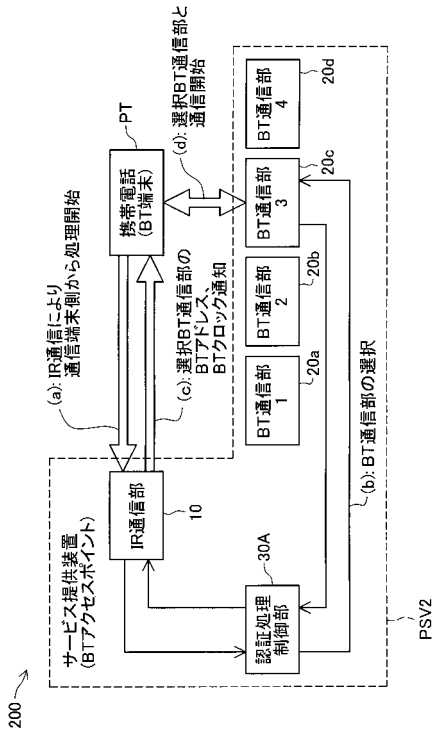
【図６】



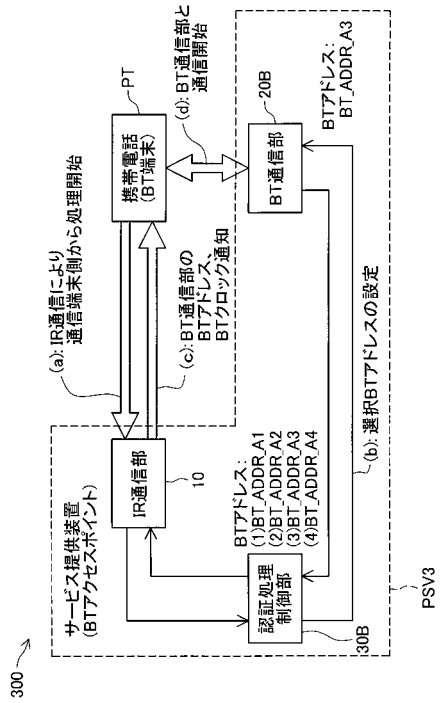
【図７】



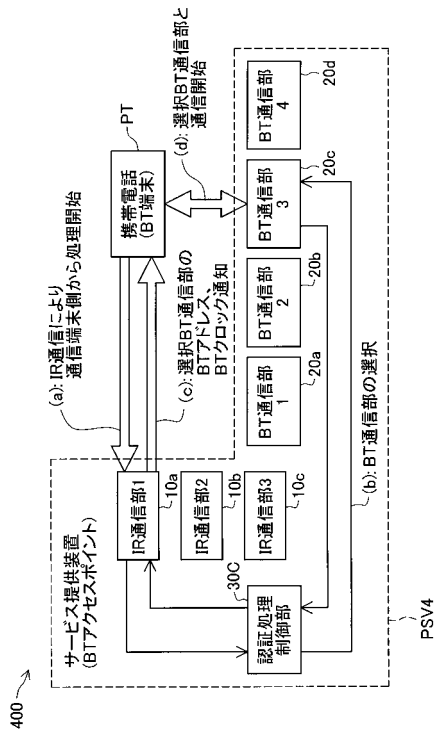
【図８】



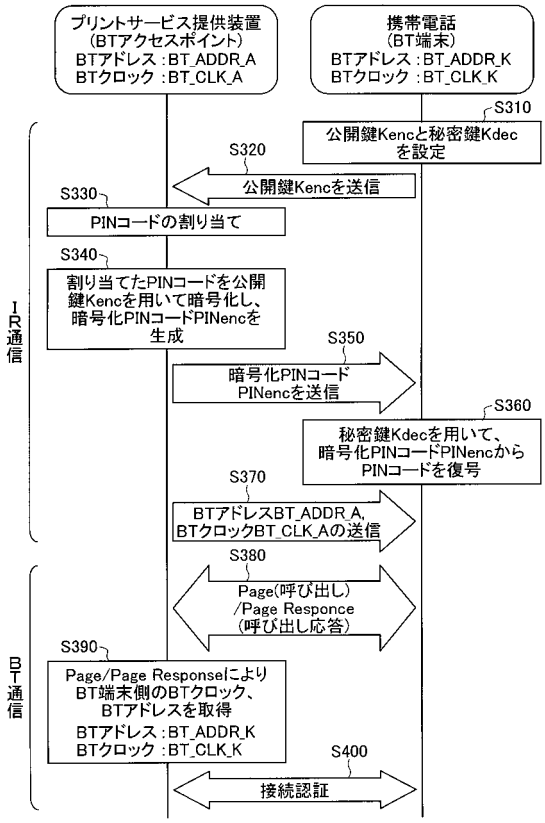
【図９】



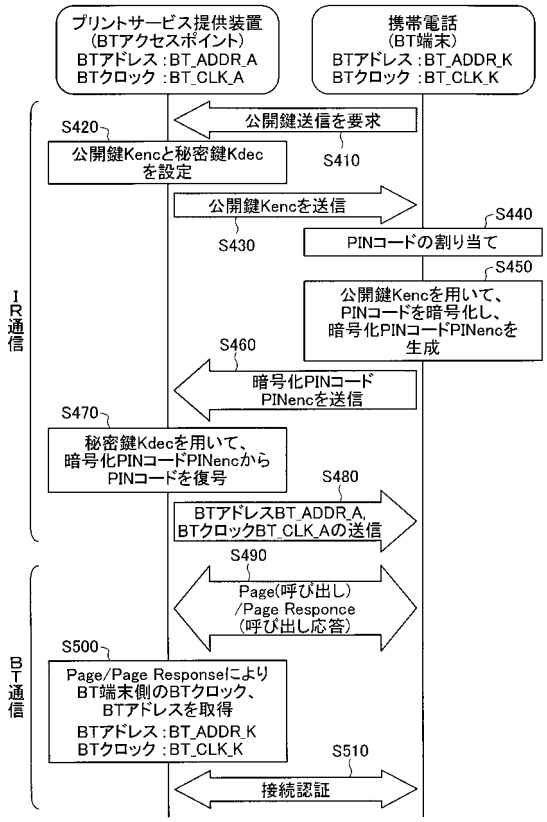
【図１０】



【図１１】


プリントサービス提供装置
(BTアクセスポイント)
BTアドレス :BT_ADDR_A
BTクロック :BT_CLK_A
携帯電話
(BT端末)
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
S310
公開鍵Kencと秘密鍵Kdec
を設定
S320
公開鍵Kencを送信
S330
PINコードの割り当て
S340
割り当てたPINコードを公開
鍵Kencを用いて暗号化し、
暗号化PINコードPINencを
生成
S350
暗号化PINコード
PINencを送信
S360
秘密鍵Kdecを用いて、
暗号化PINコードPINencから
PINコードを復号
S370
BTアドレスBT_ADDR_A,
BTクロックBT_CLK_Aの送信
S380
Page(呼び出し)
/Page Responce
(呼び出し応答)
S390
Page/Page Responseにより
BT端末側のBTクロック、
BTアドレスを取得
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
S400
接続認証
IR通信
BT通信

【図１２】


プリントサービス提供装置
(BTアクセスポイント)
BTアドレス :BT_ADDR_A
BTクロック :BT_CLK_A
携帯電話
(BT端末)
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
公開鍵送信を要求
S410
S420
公開鍵Kencと秘密鍵Kdec
を設定
公開鍵Kencを送信
S430
S440
PINコードの割り当て
S450
公開鍵Kencを用いて、
PINコードを暗号化し、
暗号化PINコードPINencを
生成
S460
暗号化PINコード
PINencを送信
S470
秘密鍵Kdecを用いて、
暗号化PINコードPINencから
PINコードを復号
S480
BTアドレスBT_ADDR_A,
BTクロックBT_CLK_Aの送信
S490
Page(呼び出し)
/Page Responce
(呼び出し応答)
S500
Page/Page Responseにより
BT端末側のBTクロック、
BTアドレスを取得
BTアドレス :BT_ADDR_K
BTクロック :BT_CLK_K
S510
接続認証
IR通信
BT通信

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｗ　８４／１２
Ｈ０４Ｗ　８８／０８