(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4606055号
(P4606055)
(45)発行日　平成23年1月5日(2011.1.5)　(24)登録日　平成22年10月15日(2010.10.15)

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

請求項の数 10　(全 25 頁)

(21)出願番号　特願2004-125150(P2004-125150)
(22)出願日　平成16年4月21日(2004.4.21)
(65)公開番号　特開2005-311653(P2005-311653A)
(43)公開日　平成17年11月4日(2005.11.4)
審査請求日　平成19年4月11日(2007.4.11)

(73)特許権者　390040187
株式会社バッファロー
愛知県名古屋市中区大須三丁目３０番２０号
(74)代理人　100096703
弁理士　横井　俊之
(72)発明者　田村　佳照
名古屋市南区柴田本通四丁目１５番　株式会社バッファロー内

審査官　速水　雄太

最終頁に続く

(54)【発明の名称】暗号鍵設定システム、アクセスポイントおよび暗号鍵設定方法

(57)【特許請求の範囲】
【請求項１】
無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で、無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定する暗号鍵設定システムであって、
上記端末は、
上記アクセスポイントに対して、当該端末が対応可能な暗号化方式を無線で伝える端末側暗号化方式伝達手段と、
上記アクセスポイントが採用した暗号化方式を検知し、同検知した暗号化方式を選択する端末側暗号化方式選択手段とを備え、
上記アクセスポイントは、
同アクセスポイントを介した無線ＬＡＮに参加している端末を特定し同参加している端末が変化したか否かを検知する接続端末検知手段と、
上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から、暗号化方式を選択して採用するアクセスポイント側暗号化方式選択手段とを備え、
上記アクセスポイント側暗号化方式選択手段は、上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共

通して対応可能である場合に、当該セキュリティレベルの高い暗号化方式を選択することを特徴とする暗号鍵設定システム。

【請求項２】

上記接続端末検知手段は、所定時間毎に繰り返し、上記無線ＬＡＮに参加している端末を各端末固有の識別情報に基づいて特定するとともに、同特定した各端末固有の識別情報と前回の端末の特定作業において取得した各端末固有の識別情報とを比較することによって、同無線ＬＡＮに参加している端末数の減少を検知することを特徴とする請求項１に記載の暗号鍵設定システム。

【請求項３】

上記接続端末検知手段は、所定時間毎に繰り返し、上記無線ＬＡＮに参加している端末を各端末固有の識別情報に基づいて特定するとともに、同特定した各端末固有の識別情報と前回の端末の特定作業において取得した各端末固有の識別情報とを比較することによって、同無線ＬＡＮに参加している端末に入替わりがあったことを検知することを特徴とする請求項１または請求項２のいずれかに記載の暗号鍵設定システム。

【請求項４】

上記アクセスポイントは、同アクセスポイントが対応可能な暗号化方式のうち、上記端末側暗号化方式伝達手段によって伝えられた暗号化方式によって絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とを端末に無線で伝えるアクセスポイント側暗号鍵伝達手段を備え、

上記端末は、上記アクセスポイントから伝えられた夫々の暗号化方式ごとの暗号鍵を所定の記憶領域に保存する端末側暗号鍵保存手段を備えることを特徴とする請求項１～請求項３のいずれかに記載の暗号鍵設定システム。

【請求項５】

上記アクセスポイント側暗号鍵伝達手段は、上記絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とを端末に伝える処理を、当該端末の端末側暗号化方式伝達手段によって暗号化方式を伝えられた際に一度だけ行うことを特徴とする請求項４に記載の暗号鍵設定システム。

【請求項６】

上記アクセスポイント側暗号化方式選択手段は、上記無線ＬＡＮに参加している端末の変化に伴い採用する暗号化方式を変更した際に、同暗号化方式の変更に対応してステーションＩＤを変更することを特徴とする請求項４または請求項５のいずれかに記載の暗号鍵設定システム。

【請求項７】

上記アクセスポイント側暗号鍵伝達手段は、同アクセスポイントが対応可能な暗号化方式の夫々に異なったステーションＩＤを特定し、上記絞り込んだ暗号化方式の夫々ごとに上記特定したステーションＩＤを上記暗号鍵とともに端末に無線で伝え、

上記端末側暗号化方式選択手段は、接続可能なアクセスポイントからステーションＩＤを取得し、予め上記端末側暗号鍵保存手段によって保存しておいたステーションＩＤと一致するものがあるときに同ステーションＩＤに対応した暗号化方式と暗号鍵とを採用することを特徴とする請求項４～請求項６のいずれかに記載の暗号鍵設定システム。

【請求項８】

上記端末側暗号化方式選択手段は、特定したステーションＩＤに基づくアクセスポイントとの無線通信が維持できなくなったときに、あらためて接続可能なアクセスポイントからステーションＩＤを取得し、保存しておいたステーションＩＤと一致するものがあるときに同ステーションＩＤに対応した暗号化方式と暗号鍵とを採用することを特徴とする請求項７に記載の暗号鍵設定システム。

【請求項９】

無線ＬＡＮ通信における複数の暗号化方式に対応した無線ＬＡＮ用の中継器であるアクセスポイントであって、

無線ＬＡＮ接続用デバイスを備えた端末との無線通信データを通信に先立って暗号化す

る際に用いられる暗号化方式と暗号鍵とを設定するにあたり、
同アクセスポイントを介した無線ＬＡＮに参加している端末を特定し同参加している端末が変化したか否かを検知する接続端末検知手段と、
上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、予め複数の端末から無線で伝えられた各端末が対応可能な暗号化方式にかかるデータに基づいて、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から暗号化方式を選択して採用するアクセスポイント側暗号化方式選択手段とを備え、
上記アクセスポイント側暗号化方式選択手段は、上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、当該セキュリティレベルの高い暗号化方式を選択することを特徴とするアクセスポイント。
【請求項１０】
無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で、無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定する暗号鍵設定方法であって、
上記端末は、上記アクセスポイントに対して、当該端末が対応可能な暗号化方式を無線で伝え、
上記アクセスポイントは、同アクセスポイントを介した無線ＬＡＮに参加している端末を特定するとともに同参加している端末が変化したか否かを検知し、同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から暗号化方式を選択して採用するにあたり、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、当該セキュリティレベルの高い暗号化方式を選択し、
上記端末は、上記アクセスポイントが採用した暗号化方式を検知し、同検知した暗号化方式を選択することを特徴とする暗号鍵設定方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号鍵設定システム、アクセスポイントおよび暗号鍵設定方法に関する。
【背景技術】
【０００２】
無線ＬＡＮ用の中継器であるアクセスポイントを介しての無線通信ネットワークを構築する場合には、ネットワークへの不正侵入や通信データの第三者への漏洩などを防ぐため、同ネットワークのセキュリティを高度に確保する必要がある。そのため、無線ＬＡＮに関しては、種々のセキュリティ技術が提案されていた。
【０００３】
例えば、端末に装着される無線ＬＡＮ接続用デバイス（例えば、無線ＬＡＮアダプタ）に予め割り当てられた固有の識別番号であるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを利用し、このＭＡＣアドレスをアクセスポイントに登録しておき、端末からのアクセスに伴ってアクセスポイントがＭＡＣアドレスの認証を行ない、登録されたＭＡＣアドレス以外のＭＡＣアドレスであれば、該端末からのネットワークへの接続要求を拒否する技術が提案されていた（例えば、特許文献１を参照）。また、端末およびアクセスポイントに、共通の暗号鍵としてＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）キーを設定しておき、端末とアクセスポイントとの間でやりとりされるデータの内容をＷＥＰキーを用いて暗号化し、データが漏洩した場合であっても、データの内容を解析しにくくし、データの内容がわからないようにする技術も提案されていた（例えば、特許文献２を参照）。

【０００４】
また、かかるＭＡＣアドレスの登録やＷＥＰキーに代表される暗号鍵の設定を簡易かつ安全に行うための発明について、本願出願人は既に出願を行っている（特願２００３‐４０８０１１）。すなわち、同出願によれば、アクセスポイントへのＭＡＣアドレスの登録や端末への暗号鍵の設定に際して煩雑な入力操作が不要であり、無線ＬＡＮを利用する端末を新たに追加しようとする場合にも、利用者は暗号鍵を表わすデータの漏洩を防ぎながら容易に必要なセキュリティ設定を行うことができる。
【特許文献１】特開２００１－３２０３７３号公報
【特許文献２】特開２００１－３４５８１９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、同出願に記載の発明においては、次の技術的課題が残されていた。つまり、新たな端末がネットワークに追加された場合には、所定のセキュリティポリシーに基づいて同ネットワークにおいて使用する暗号化方式及び暗号鍵が設定され、同設定された暗号化方式と暗号鍵は、次に他の端末がネットワークに追加されるまでは維持されていた。そして、ネットワークに参加する端末が減少した場合にも、同暗号化方式と暗号鍵との設定は維持されていた。その結果、ある端末がネットワークから離脱した後において、同ネットワークに参加する無線ＬＡＮ用機器間で設定し得る最適なセキュリティ環境が必ずしも構築されていない場合があった。
【０００６】
本発明は、上記課題にかんがみてなされたもので、無線ＬＡＮを構築する機器の変化に柔軟に対応し、各無線ＬＡＮ用機器に対して、その時点において最適なセキュリティ環境を設定可能な暗号鍵設定システム、アクセスポイントおよび暗号鍵設定方法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】
【０００７】
上記目的を達成するために本発明は、無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で、無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定する暗号鍵設定システムであって、上記端末は、上記アクセスポイントに対して、当該端末が対応可能な暗号化方式を無線で伝える端末側暗号化方式伝達手段と、上記アクセスポイントが採用した暗号化方式を検知し、同検知した暗号化方式を選択する端末側暗号化方式選択手段とを備え、上記アクセスポイントは、同アクセスポイントを介した無線ＬＡＮに参加している端末を特定し同参加している端末が変化したか否かを検知する接続端末検知手段と、上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から、所定の判断基準に従って所定の暗号化方式を選択して採用するアクセスポイント側暗号化方式選択手段とを備える構成としてある。
【０００８】
上記構成においては、無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定する。
ここで、端末は、端末側暗号化方式伝達手段によって、アクセスポイントに対して当該端末が対応可能な暗号化方式を無線で伝える。アクセスポイントは各端末が夫々対応可能な暗号化方式を認識する一方で、接続端末検知手段によって、同アクセスポイントを介した無線ＬＡＮに参加している端末を特定し、同参加している端末が変化したか否かを検知している。そして、同無線ＬＡＮに参加している端末が変化したことを検知した場合、アクセスポイント側暗号化方式選択手段は、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から、所定

の判断基準に従って所定の暗号化方式を選択して採用する。

【０００９】

一方、端末は、端末側暗号化方式選択手段において、上記アクセスポイントが採用した暗号化方式を検知し、同検知した暗号化方式を選択する。以後、上記無線ＬＡＮに参加する端末とアクセスポイントは、さらに同無線ＬＡＮに参加する端末が変化しない限り、基本的に上記採用した暗号化方式において利用する暗号鍵を用いて無線通信を行う。

このように、本発明によれば、無線ＬＡＮを構築する機器の構成に変化が生じたことを検知する度に、採用する暗号化方式の設定を見直す。そのため、無線ＬＡＮに参加している機器に変化が生じても、同無線ＬＡＮに参加している機器間で採用し得る暗号化方式から最適な暗号化方式を自動的に選択でき、常にセキュリティ環境を最適なものとすることができる。

【００１０】

本発明は、上記アクセスポイント側暗号化方式選択手段は、上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、同セキュリティレベルの高い暗号化方式を選択する構成としてある。

【００１１】

上記構成においては、接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合、アクセスポイント側暗号化方式選択手段は、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、同セキュリティレベルの高い暗号化方式を選択する。つまり、アクセスポイントは、無線ＬＡＮによる通信を継続しようとする機器の構成に変化が生じたことを検知する度に、同通信を継続しようとする機器間において、それまで採用していた方式よりも安全性の高い暗号化方式を採用できないか見直しを図る。かかる見直しを図ることで、例えば、アクセスポイントが対応可能な暗号化方式のうち無線ＬＡＮに参加している端末が共通して対応可能な方式であって最もセキュリティレベルの高い暗号化方式を常に選択するようにすることもできる。

【００１２】

本発明は、上記接続端末検知手段は、所定時間毎に繰り返し、上記無線ＬＡＮに参加している端末を各端末固有の識別情報に基づいて特定するとともに、同特定した各端末固有の識別情報と前回の端末の特定作業において取得した各端末固有の識別情報とを比較することによって、同無線ＬＡＮに参加している端末数の減少を検知する構成としてある。

【００１３】

すなわち、無線ＬＡＮに参加している端末の変化を検知する際の具体的構成として、接続端末検知手段は、所定時間毎に繰り返し、無線ＬＡＮに参加している端末数が減少したか否かを検知するとした。接続端末検知手段は、無線ＬＡＮに参加している端末を定期的に各端末固有の識別情報に基づいて特定するとともに、同特定した各端末固有の識別情報と前回の端末の特定作業において取得した各端末固有の識別情報とを比較して端末数の減少を検知する。従って、アクセスポイントは、無線ＬＡＮに参加している端末を特定する度に、同特定した端末にかかるリストデータを、少なくとも次に無線ＬＡＮに参加している端末を特定するまでの間は保存しておく必要がある。

このように、所定期間毎に絶えず無線ＬＡＮに参加している端末数の変化を監視することで、確実に無線ＬＡＮに参加する機器数が減る度に暗号化方式の設定を見直すことができる。

【００１４】

また、上記接続端末検知手段は、所定時間毎に繰り返し、上記無線ＬＡＮに参加している端末を各端末固有の識別情報に基づいて特定するとともに、同特定した各端末固有の識別情報と前回の端末の特定作業において取得した各端末固有の識別情報とを比較することによって、同無線ＬＡＮに参加している端末に入替わりがあったことを検知するとしても

よい。
つまり、無線ＬＡＮに参加する端末の幾つかが入替わった場合にも、無線ＬＡＮに参加する機器間で採用可能な暗号化方式を見直す余地はある。そして、かかる見直し行えば、端末が入替わる前に採用していた暗号化方式よりもセキュリティレベルの高い暗号化方式を採用できる場合がある。
【００１５】
本発明は、上記アクセスポイントは、同アクセスポイントが対応可能な暗号化方式のうち、上記端末側暗号化方式伝達手段によって伝えられた暗号化方式によって絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とを端末に無線で伝えるアクセスポイント側暗号鍵伝達手段を備え、上記端末は、上記アクセスポイントから伝えられた夫々の暗号化方式ごとの暗号鍵を所定の記憶領域に保存する端末側暗号鍵保存手段を備える構成としてある。
【００１６】
上記構成においては、アクセスポイント側暗号鍵伝達手段は、アクセスポイントが対応可能な暗号化方式のうち、上記端末側暗号化方式伝達手段によって伝えられた暗号化方式によって絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とを端末に無線で伝える。また、端末側暗号鍵保存手段は、アクセスポイントから伝えられた夫々の暗号化方式ごとの暗号鍵を所定の記憶領域に保存する。その結果、各端末は、自己とアクセスポイントの間で共通して採用可能な暗号化方式と各方式において利用する暗号鍵を取得することができる。また、予め上記絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とをアクセスポイントから端末の側に伝えておくことにより、後にアクセスポイントが暗号化方式を変更したとしても、暗号鍵を通知し直す必要はなくなる。これにより、通知の煩雑さを解消し、また、同時に暗号鍵の通知に伴うセキュリティの低下を防止することが可能となる。
【００１７】
ここで、上記アクセスポイント側暗号鍵伝達手段は、上記絞り込んだ暗号化方式と同絞り込んだ暗号化方式の夫々において利用する暗号鍵とを端末に伝える処理を、当該端末の端末側暗号化方式伝達手段によって暗号化方式を伝えられた際に一度だけ行うとしてもよい。つまり、アクセスポイントから端末に対して、一度だけ、上記絞り込んだ暗号化方式及び暗号鍵とを伝えておけば、後にアクセスポイントが暗号化方式を変更したとしても、暗号鍵を再度通知し直す必要はなくなる。
これにより、暗号化方式及び暗号鍵の通知の煩雑さを大幅に解消し、また、同時に暗号鍵の通知に伴うセキュリティの低下を極力防止することが可能となる。
【００１８】
端末の側では幾つかの暗号化方式とそれに対応する暗号鍵を通知されることにより、暗号化方式の特定が必要になることがある。
この場合の好適な一例として、本発明は、上記アクセスポイント側暗号化方式選択手段は、上記無線ＬＡＮに参加している端末の変化に伴い採用する暗号化方式を変更した際に、同暗号化方式の変更に対応してステーションＩＤを変更する構成としてある。
【００１９】
上記構成においては、無線ＬＡＮに参加している端末の変化に伴い、上記アクセスポイント側暗号化方式選択手段が暗号化方式を変更した際に同変更に対応してステーションＩＤを変更する。端末側では、同変更されたステーションＩＤを検知することで、暗号化方式が変更されたことを容易に検知することができるため、アクセスポイント側の暗号化方式の選択に容易に追従できる。
【００２０】
より具体的な構成例として、本発明は、上記アクセスポイント側暗号鍵伝達手段は、同アクセスポイントが対応可能な暗号化方式の夫々に異なったステーションＩＤを特定し、上記絞り込んだ暗号化方式の夫々ごとに上記特定したステーションＩＤを上記暗号鍵とともに端末に無線で伝え、上記端末側暗号化方式選択手段は、接続可能なアクセスポイント

からステーションＩＤを取得し、予め上記端末側暗号鍵保存手段によって保存しておいたステーションＩＤと一致するものがあるときに同ステーションＩＤに対応した暗号化方式と暗号鍵とを採用する構成としてある。

【００２１】

上記構成においては、アクセスポイント側暗号鍵伝達手段が、同アクセスポイントが対応可能な複数の暗号化方式のそれぞれに異なったステーションＩＤを特定するとともに、上記絞り込んだ暗号化方式のそれぞれごとに上記特定されているステーションＩＤを上記暗号鍵とともに上記端末に無線で伝える。そして、アクセスポイント側暗号化方式選択手段は、そのとき無線ＬＡＮを構成する機器間で採用する暗号化方式に対応したステーションＩＤを採用することになる。

【００２２】

一方、端末側暗号化方式選択手段は、接続可能なアクセスポイントからステーションＩＤを取得し、予め上記アクセスポイントから無線で伝えられて保存しておいたステーションＩＤと一致するものがないか判断する。一致するものがあるときは、アクセスポイントが同ステーションＩＤに対応した暗号化方式と暗号鍵を採用していると判断できるので、端末においても同暗号化方式と暗号鍵を採用する。このように、アクセスポイントと端末との間で敢えて暗号化方式の特定のための通知を行う必要が無くなるので手続の煩雑さを解消しつつセキュリティの低下を防止できる。

【００２３】

アクセスポイントと端末との間で暗号化方式の特定のための通知を行う必要が無いのは、採用する暗号化方式が変更になった場合も同じである。

そこで、本発明は、上記端末側暗号化方式選択手段は、特定したステーションＩＤに基づくアクセスポイントとの無線通信が維持できなくなったときに、あらためて接続可能なアクセスポイントからステーションＩＤを取得し、保存しておいたステーションＩＤと一致するものがあるときに同ステーションＩＤに対応した暗号化方式と暗号鍵とを採用する構成としてある。

【００２４】

上記構成においては、上記端末側暗号化方式選択手段は、特定したステーションＩＤに基づくアクセスポイントとの無線通信が維持できなくなったときに、あらためて接続可能なアクセスポイントからステーションＩＤを取得する。そして、保存しておいたステーションＩＤと一致するものがあるときに同ステーションＩＤに対応した暗号化方式と暗号鍵とを採用する。つまり、無線ＬＡＮに参加している端末の減少や入替えによって採用する暗号化方式を変更した場合でも、アクセスポイントは、継続して無線通信を行おうとする端末に新たに採用した暗号化方式などを通知する必要が無い。各端末の側で自動的に暗号化方式の変更に追尾することができるため、メインテナンスの煩雑さを解消し、また、セキュリティの低下を防止できる。

【００２５】

上述した暗号鍵設定システムは、アクセスポイントと端末とからなるシステム全体として把握するだけでなく、その構成要素であるアクセスポイントの発明として把握することができる。

そこで、本発明は、無線ＬＡＮ通信における複数の暗号化方式に対応した無線ＬＡＮ用の中継器であるアクセスポイントであって、無線ＬＡＮ接続用デバイスを備えた端末との無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定するにあたり、同アクセスポイントを介した無線ＬＡＮに参加している端末を特定し同参加している端末が変化したか否かを検知する接続端末検知手段と、上記接続端末検知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、予め複数の端末から無線で伝えられた各端末が対応可能な暗号化方式にかかるデータに基づいて、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から暗号化方式を選択して採用するアクセスポイント側暗号化方式選択手段とを備え、当該アクセスポイント側暗号化方式選択手段は、上記接続端末検

知手段が同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、当該セキュリティレベルの高い暗号化方式を選択する構成としてある。

【００２６】

また、上記暗号鍵設定システムの構成要素である端末についても発明として把握可能であることは言うまでも無い。

さらに、本願発明を無線通信システムとして装置の面から把握できるのと同時に、そのシステムの実行手順としても発明を把握できる。

そこで、本発明は、無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で、無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号化方式と暗号鍵とを設定する暗号鍵設定方法であって、上記端末は、上記アクセスポイントに対して、当該端末が対応可能な暗号化方式を無線で伝え、上記アクセスポイントは、同アクセスポイントを介した無線ＬＡＮに参加している端末を特定するとともに同参加している端末が変化したか否かを検知し、同無線ＬＡＮに参加している端末が変化したことを検知した場合に、同アクセスポイントが対応可能な暗号化方式であって同無線ＬＡＮに参加している端末が共通して対応可能な暗号化方式の中から暗号化方式を選択して採用するにあたり、同無線ＬＡＮに参加している端末が、それまで採用されていた暗号化方式よりもセキュリティレベルの高い暗号化方式に共通して対応可能である場合に、当該セキュリティレベルの高い暗号化方式を選択し、上記端末は、上記アクセスポイントが採用した暗号化方式を同アクセスポイントの発信行為に基づいて検知して採用する構成としてある。

【００２７】

むろん、独立形式の暗号鍵設定システムの発明に従属する各請求項にかかる発明と同様の態様を適用して、アクセスポイントや暗号鍵設定方法の各発明に従属する発明を夫々捉えることも可能である。

【発明の効果】

【００２８】

以上説明したように、本願発明によれば、無線ＬＡＮに参加する機器が変化する度に暗号化方式の設定を見直し、無線ＬＡＮに参加している機器間で採用可能な暗号化方式のうち最も安全性の高い暗号化方式など最適な暗号化方式を自動的に選択できるため、無線ＬＡＮに参加する機器間において、常に最適なセキュリティ環境を構築できる。

【発明を実施するための最良の形態】

【００２９】

下記の順序に従って本願発明の実施形態について説明する。

１．暗号鍵設定システムを実現するための概略構成

２．暗号鍵設定システムの具体的内容

２‐１．端末数を増加させる場合について

２‐２．端末数を減少させる場合について

３．変形例

４．まとめ

【００３０】

１．暗号鍵設定システムを実現するための概略構成

図１は本願にかかる暗号鍵設定システムを実現するハードウェア構成を示す説明図であり、図２はアクセスポイント２０の構成を示す説明図である。

暗号鍵設定システムでは、無線ＬＡＮの無線通信エリアＡＲ１内において、所定の端末とアクセスポイント２０との間で、暗号鍵の内容を表わす暗号鍵データを電波に乗せて無線通信することにより、所定の端末にアクセスポイント２０との無線通信において使用する暗号鍵を設定する。

【００３１】

図１に示すように、無線通信エリアＡＲ１には、無線ＬＡＮ用の中継器であるアクセスポイント（無線基地局）２０が設置されている。アクセスポイント２０は、図２に示すように、ＣＰＵ１１と、このＣＰＵ１１とバスにより相互に接続されたＲＯＭ１２，ＲＡＭ１３，ハードディスク等の不揮発的な記憶装置１４，ネットワークインタフェースとしてのＷＡＮポート１７，有線ＬＡＮとの接続用のＬＡＮポート２２，無線通信インタフェース１８，ディスプレイコントローラ１５，入出力コントローラ１６等の各部を備える。

【００３２】

ＲＯＭ１２には、無線通信エリアＡＲ１内の端末５０，６０，７０との通信やインターネットＩＮへの接続に関する各種のプログラムとこのプログラムの実行に必要なデータが格納されている。入出力コントローラ１６にはプッシュ式の登録ボタン１２７が接続されている。登録ボタン１２７は、その押圧部がアクセスポイント２０の筐体表面に露出した状態で設けられている。ディスプレイコントローラ１５には、無線ＬＡＮの接続状態や通信状態を点灯・点滅等によって表示する各種の表示ランプ１９が接続されている。

【００３３】

無線通信インタフェース１８には、電波を送信する送信機２５，電波を受信する受信機２６が接続されている。この送信機２５，受信機２６は、外部への電波の送信や外部からの電波の受信が可能な状態で、アクセスポイント２０に内蔵されている。図１では、送信機２５の出力や受信機２６の受信感度を標準設定値とした場合に、送信機２５から送信された電波が届き、かつ、受信機２６が端末５０，６０，７０からの電波を受け取れる範囲を、無線通信エリアＡＲ１として表わしている。こうしたアクセスポイント２０の設置により、無線通信エリアＡＲ１内を通常の通信範囲とした無線ＬＡＮが組まれる。

【００３４】

なお、ＲＯＭ１２には、端末５０，６０，７０との通信に関するプログラムとして、送信機２５の出力の標準設定値を一時的に変更する処理の内容が記述された出力値変更プログラムや受信機２６の受信感度の標準設定値を一時的に変更する処理の内容が記述された受信感度値変更プログラムが予め格納されている。この設定値を変更する処理は、具体的には、標準設定値を１／ｎ（ｎは予め定められた定数）倍する演算処理によって実現される。ＣＰＵ１１は、この出力値変更プログラム，受信感度値変更プログラムを実行することにより、変更後の出力値や受信感度値を、無線通信インタフェース１８を介して送信機２５，受信機２６に出力する。これにより、送信機２５から送信される電波の出力や受信機２６における電波の受信感度が変更される。

【００３５】

端末５０，６０，７０は、周知のノート型のパーソナルコンピュータであり、ＣＰＵ，ＲＯＭ，ＲＡＭ等からなる制御装置をはじめ、記憶装置としてのハードディスクやＣＤ－ＲＯＭドライブ等を備える。勿論、携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の他の端末であっても差し支えない。

【００３６】

また、端末５０，６０，７０には、アクセスポイント２０との間での電波の送受信を行なえるようにする無線ＬＡＮ接続用デバイスとして、無線ＬＡＮアダプタ５２，６２，７２が装着されている。この無線ＬＡＮアダプタ５２，６２，７２のデバイスドライバが端末５０に組み込まれることにより、端末５０，６０，７０は、装着された無線ＬＡＮアダプタ５２，６２，７２を認識し、無線ＬＡＮアダプタ５２，６２，７２を制御することが可能となる。なお、無線ＬＡＮアダプタ５２，６２，７２には、アダプタに固有の識別番号であるＭＡＣアドレスが付与されている。なお、以下において表現上、端末のＭＡＣアドレスと言った場合も、同端末に装着された無線ＬＡＮアダプタのＭＡＣアドレスを示すものとする。

【００３７】

無線通信エリアＡＲ１内に入ったコンピュータとしての端末５０，６０，７０は、装着された無線ＬＡＮアダプタ５２，６２，７２とアクセスポイント２０との間で電波が送受信されることにより、アクセスポイント２０との通信を無線で行なう。アクセスポイント

２０および無線ＬＡＮアダプタ５２，６２，７２は、やり取りするデータを通信に適した形式、いわゆるパケットに変換することが可能であり、これにより、端末５０，６０，７０とアクセスポイント２０との間において、オフライン（インターネットに接続されていない状態）でデータのやり取りをすることが理論上可能となる。

【００３８】

次に、アクセスポイント２０をインターネットＩＮに接続するための構成について説明する。図１に示すように、アクセスポイント２０のＷＡＮポート１７には、モデムを内蔵したルータ２８がケーブルを介して接続されている。ルータ２８は、無線ＬＡＮアダプタ５２，６２，７２それぞれのＭＡＣアドレスに基づいて、無線ＬＡＮ内の複数の各端末５０，６０，７０を特定し、これらを区別することができる。ルータ２８内のモデムは、ＣＡＴＶ回線，ｘＤＳＬ回線等のブロードバンドな通信回線ＣＬ、プロバイダＰＶの専用回線を介してインターネットＩＮに接続されている。即ち、ルータ２８は、無線ＬＡＮをインターネットＩＮに接続するゲートウェイとして機能する。

【００３９】

なお、本実施形態では、無線通信エリアＡＲ１内にある無線ＬＡＮアダプタを備えた端末のうち、そのＭＡＣアドレスがアクセスポイント２０に登録されている端末（以下、登録端末という）に、無線ＬＡＮへの接続を許容する。登録端末の所有者は、自己の端末をアクセスポイント２０を通じてインターネットＩＮに接続し、インターネットＩＮ上のサーバＳＶに格納されたウェブコンテンツ等の種々の情報を取得することができる。一方、ＭＡＣアドレスがアクセスポイント２０に登録されていない端末（非登録端末という）は、たとえ無線通信エリアＡＲ１内にいても無線ＬＡＮに接続することができない。即ち、無線通信エリアＡＲ１は、登録端末の所有者のみにインターネットＩＮへの接続サービスを提供するフリースポットとされている。なお、図１では、端末５０，６０が登録端末に該当し、端末７０が非登録端末に該当するものとする。

【００４０】

こうした登録端末とアクセスポイント２０との間では、契約やサービス等の種々の内容を有するデータ（以下、内容付きデータという）が電波に乗せて送受信される。本実施例では、内容付きデータを送信する側の装置（登録端末，アクセスポイント２０）が、送信に先立って、所定の暗号鍵を用いて内容付きデータを暗号化し、暗号化後の内容付きデータ（以下、暗号化データという）を受信側の装置（アクセスポイント２０，登録端末）に送信することとしている。受信側の装置は、受信した暗号化データを所定の暗号鍵を用いて復号化し、内容付きデータを得る。

【００４１】

ここで、暗号鍵としてはＷＥＰキーを用いることができる。ＷＥＰキーは、ＩＥＥＥ８０２．１１で使用される、秘密鍵暗号方式（データの暗号化と暗号化されたデータの復号化の双方で同じ暗号鍵を使用する方式）の暗号化技術である。暗号鍵として６４ビットのＷＥＰキーを用いる方式（ＷＥＰ６４）または１２８ビットのＷＥＰキーを用いる方式（ＷＥＰ１２８）がある。かかるＷＥＰキーを用いた暗号化により、無線通信エリアＡＲ１内において内容付きデータを乗せた電波が傍受された場合に同データの解析がしにくくなり、通信内容の第三者への漏洩が防止される。また、かかるＷＥＰキーを用いる暗号化方式以外にも、よりセキュリティレベルの高い、ＴＫＩＰ（Ｔｅｍｐｏｒａｌ Ｋｅｙ Ｉｎｔｅｇｒｉｔｙ Ｐｒｏｔｏｃｏｌ）や、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）といった暗号化方式を用いてもよい。これら、ＷＥＰ６４、ＷＥＰ１２８、ＴＫＩＰ、ＡＥＳは、後者に従うにつれてセキュリティレベルが高くなる。

【００４２】

２．暗号鍵設定システムの具体的内容

端末５０，６０に暗号鍵を順に設定する手法および、端末５０，６０のうち端末６０が無線ＬＡＮから離脱した場合の暗号鍵の再設定の手法について説明する。

【００４３】

２‐１．端末数を増加させる場合について

ここで、一般の無線ＬＡＮ機器が全ての暗号化方式に対応しているわけではない。本実施形態においては、アクセスポイント２０は、ＷＥＰ６４と、ＷＥＰ１２８と、ＴＫＩＰと、ＡＥＳとを採用可能であり、無線ＬＡＮアダプタ５２は、ＷＥＰ６４と、ＷＥＰ１２８と、ＴＫＩＰとに対応しており、無線ＬＡＮアダプタ６２はＷＥＰ６４と、ＷＥＰ１２８とに対応しているものとする。以下においては、最初にアクセスポイント２０に端末５０のＭＡＣアドレスを登録するとともに端末５０に暗号鍵を設定して無線ＬＡＮを構築し、その後、端末６０を無線ＬＡＮに追加する場合について説明する。

【００４４】

アクセスポイント２０のＲＯＭ１２には、端末５０，６０との通信に関するプログラムとして、無線ＬＡＮアダプタ５２，６２のＭＡＣアドレスの登録に関するプログラム（ＭＡＣ登録プログラム）と暗号化方式選択プログラムが予め格納されている。一方、無線ＬＡＮの使用に際して端末５０，６０にインストールされたユーティリティプログラムには、暗号化方式および暗号鍵の設定に関するプログラム（暗号鍵設定プログラム）が含まれている。

【００４５】

また、上記アクセスポイント２０の登録ボタン１２７と同様に、無線ＬＡＮアダプタ５２，６２にもハードウェアのスイッチで実現された図示しない所定の登録ボタンが備えられている。同登録ボタンの押し下げ状態はインターフェイスを介してソフトウェアにて判別可能となっている。

図３および図４は、アクセスポイント２０の側と端末５０，６０とが実施するＭＡＣ登録プログラムと暗号化方式選択プログラムと暗号鍵設定プログラムとに対応したフローチャートである。アクセスポイント２０の側においては、暗号化方式選択処理とＭＡＣアドレス登録処理とを並行して実施する。以下のフローチャートにおいては、端末５０，６０の側をＳＴＡと表示し、アクセスポイント２０の側をＡＰと表示している。

【００４６】

アクセスポイント２０および端末５０，６０においては、各登録ボタンの押し下げによってそれぞれワンタッチ登録モードとなり、対応する処理を開始する。すなわち、端末５０の側においては、図３に示すステップＳ３１０にて登録ボタンの押し下げを検知すると、ステップＳ３１２以下の処理の実行を開始し、アクセスポイント２０の側においては、ステップＳ４１０にて登録ボタン１２７の押し下げを検知すると、ステップＳ４１２以下のワンタッチ登録モードを開始する。

【００４７】

端末５０は、ワンタッチ登録モードに入ると、ステップＳ３１６にてワンタッチ登録モードに入っているアクセスポイント２０を探す。具体的には、アクセスポイント２０の側においてワンタッチ登録モードに入るとステーションＩＤ（ＥＳＳＩＤ）を予め決められている特定のステーションＩＤに変更してビーコンを送出するので、端末５０の側ではこの特定されたＥＳＳＩＤのアクセスポイントに対して接続を試みる。また、接続可能なアクセスポイントを探し、接続可能なそれぞれのアクセスポイントにおけるステータスを取得し、同ステータスに基づいてワンタッチ登録モードであるか否かを判断するようにしてもよい。

【００４８】

ワンタッチ登録モードにあるアクセスポイント２０の探索はステップＳ３１４の処理により所定時間内に限定され、所定時間を経過したときはステップＳ３３４に移行してワンタッチ登録モードの実行を終了する。

一方、所定時間内にワンタッチ登録モードにあるアクセスポイント２０を発見した場合は、ステップＳ３１８にて同発見したアクセスポイント２０に対して接続を試みる。具体的には、端末５０は、無線ＬＡＮアダプタ５２のＭＡＣアドレスを特定し、無線ＬＡＮに加入する旨の指示を表わすデータに同ＭＡＣアドレスをヘッダ情報として付加したパケットをアクセスポイント２０に対して送信する。ステップＳ３２０ではこのような接続の試

み回数が不要に多くなることを防止するものであり、所定回数を超えていればリトライオーバーとしてステップＳ３３４に移行してワンタッチ登録モードの実行を終了する。

【００４９】

端末５０は、リトライオーバーとなることなくアクセスポイント２０に接続できると、ステップＳ３２２にてアクセスポイント２０とセキュリティ情報パケットの交換処理を実施する。

一方、アクセスポイント２０は、ステップＳ４１６において、受信したパケットのヘッダ情報からＭＡＣアドレスを読取り、読取ったＭＡＣアドレスをＲＡＭ１３のバッファ領域に一時的に記憶する。また、ステップＳ４１８においては、上記端末５０の処理に対応してセキュリティ情報を作成しつつパケットの交換処理を実行する。このセキュリティ情報パケットの交換処理を図４のステップＳ３５０，Ｓ４５０以下に示している。

【００５０】

まず、パケットの交換処理の具体的内容は次のとおりである。

サブ１．端末５０から、アクセスポイント２０に対して、セキュリティ情報の作成リクエストを送出する。

サブ２．アクセスポイント２０から、端末５０に対して、リクエストの要求を表すリプライを送出する。なお、アクセスポイント２０は、初めてセキュリティ情報の作成リクエストを受領した時点で、当該アクセスポイント２０が対応している暗号化方式毎に、ＥＳＳＩＤと、暗号鍵の値を決定する。例えば、暗号化方式ＷＥＰ６４に対して「ＥＳＳＩＤ１」と「ＤＡＴＡ１」を設定し、暗号化方式ＷＥＰ１２８に対して「ＥＳＳＩＤ２」と「ＤＡＴＡ２」を設定し、暗号化方式ＴＫＩＰに対して「ＥＳＳＩＤ３」と「ＤＡＴＡ３」を設定し、暗号化方式ＡＥＳに対して「ＥＳＳＩＤ４」と「ＤＡＴＡ４」を設定する。「ＥＳＳＩＤ１」～「ＥＳＳＩＤ４］は乱数などに基づいてランダムに決定したステーションＩＤであり、「ＤＡＴＡ１」～「ＤＡＴＡ４」は各暗号方式に対応しつつランダムに決定した値となっている。

【００５１】

サブ３．端末５０から、アクセスポイント２０に対して、端末５０で対応する暗号化方式を示すデータを送出する。この場合、端末５０に装着されている無線ＬＡＮアダプタ５２は、ＷＥＰ６４と、ＷＥＰ１２８と、ＴＫＩＰとに対応しており、これら三つの暗号化方式をデータに表して送出する。

【００５２】

サブ４．アクセスポイント２０は、受信したデータに基づいて端末５０が対応可能な暗号化方式を検知できるので、同暗号化方式により自己の対応可能な暗号化方式を絞り込む。具体的には、端末５０の場合は、ＷＥＰ６４とＷＥＰ１２８とＴＫＩＰとに絞り込まれる。そして、これらの暗号化方式毎に、アクセスポイント２０から、端末５０に対して、既に決めておいたＥＳＳＩＤと暗号鍵の値を示すデータを送出する。具体的には、暗号化方式ＷＥＰ６４に対応させた「ＥＳＳＩＤ１」と「ＤＡＴＡ１」と、暗号化方式ＷＥＰ１２８に対応させた「ＥＳＳＩＤ２」と「ＤＡＴＡ２」と、暗号化方式ＴＫＩＰに対応させた「ＥＳＳＩＤ３」と「ＤＡＴＡ３」とを送出する。

このようにして、アクセスポイント２０から同アクセスポイント２０と自己で共通して対応可能な暗号化方式に対応するＥＳＳＩＤと暗号鍵の値を表わすデータを受信した端末５０は、かかるデータを所定の記憶領域に保存する。

【００５３】

以上が、端末５０におけるステップＳ３５０とアクセスポイント２０におけるステップＳ４５０でのセキュリティ情報パケットの交換処理である。かかるパケット交換処理は、一つの端末とアクセスポイント２０との間では一度行えば十分である。すなわち、以降は、アクセスポイント２０と当該端末との間では、暗号化方式や暗号鍵自体を表わすデータをやり取りする必要が無くなり、後述するように、端末はアクセスポイント２０が発信するビーコン信号に基づいて、採用すべき暗号化方式を特定することができる。なお、上記パケット交換処理は相手側ＭＡＣアドレスを特定した上で暗号化を行って通信している。

具体的には、端末５０の側で暗号化のための種（ＩｎｉｔＩＤ）を生成して上記リクエストとともに送信しており、以後、このＩｎｉｔＩＤに基づくＶＰＮ関数を用いた暗号化と復号化とをアクセスポイント２０と端末５０の双方で実施して通信を行なう。

【００５４】

セキュリティ情報パケットの交換処理後、アクセスポイント２０の側では、ステップＳ４５２において、端末５０から通知された暗号化方式の中からセキュリティレベルの最高のものを選択する。端末５０からは、暗号化方式としてＷＥＰ６４とＷＥＰ１２８とＴＫＩＰとが通知され、セキュリティレベルの最も高いものはＴＫＩＰであり、これを一応の候補（今回の最高レベル）として選択する。ステップＳ４５４では、アクセスポイント２０は、ステップＳ４５２で選択した候補と、現在の最高レベルとを比較する。ここで現在の最高レベルとは、アクセスポイント２０が対応している暗号化方式の中から上述したようにして端末が対応可能な暗号化方式で絞り込んだ暗号化方式の中のセキュリティレベルが最も高いものという意味である。

【００５５】

初めて端末５０とセキュリティ情報パケットの交換処理を行った時点では、この端末５０から通知された暗号化方式の中のセキュリティレベルが最高のものであるから、両者は一致する。しかし、以降、端末を追加する際には、過去に登録した端末が対応可能な暗号化方式で絞り込まれたものとなっていくので、必ずしも一致することにはならない。

【００５６】

このステップＳ４５４の判断に対応し、ＹＥＳ（現在の最高レベルよりも高い）のときには、現在の最高レベルを維持し、ＮＯ（現在の最高レベルよりも低いか、等しい）のときには、今回の最高レベルであるステップＳ４５２で選択した暗号化方式を採用する。従って、端末５０とのパケット交換の結果では、上述したように「等しい」の判断となり、ステップＳ４５８にて「今回の最高レベルを採用」となるから、暗号化方式はＴＫＩＰとなる。

以上の分岐は、ユーザーによるセキュリティポリシーを表している。ここで、セキュリティポリシーとは、アクセスポイント２０で対応可能な暗号化方式と端末で対応可能な暗号化方式とを対比したときに、いずれの暗号化方式を採用するかを特定する指針を意味している。

【００５７】

先の分岐の例では、新たに加わった端末が対応可能なセキュリティレベルの最高のものがそれまでのセキュリティレベルよりも高くないものであるとき、「セキュリティレベルを下げても、同端末がネットワークに参加できるようにする」というセキュリティポリシー（以下、ポリシー１という）を示している。なお、等しいと判断されたときも処理上は「高くない」場合の処理を実行するが、結果的にはステップＳ４５６での「現在の最高レベルを採用」と同じことになる。

【００５８】

これに対して、最低のセキュリティレベルを決めておき、そのセキュリティレベル以下にはしないというセキュリティポリシー（以下、ポリシー２という）とすることもできる。この場合、ステップＳ４５２の後で、「最低のセキュリティレベルよりも高いか等しい？」という判断のステップを加え、ＹＥＳの場合にステップＳ４５２以下へ進み、ＮＯの場合にステップＳ４５６へ進むようにすればよい。

【００５９】

また、特別な用途を考えた場合に新たな端末のセキュリティの最高レベルまでセキュリティレベルを上げるというセキュリティポリシー（以下、ポリシー３という）とするのであれば、ステップＳ４５６にて「現在の最高レベルを採用」する処理に代えて「今回の最高レベルを採用する」処理を実行すれば良い。このように、新たな端末の登録にあたり、予めユーザーが選択するセキュリティポリシーを反映させるように分岐処理を用意することにより、個々の暗号鍵の設定の煩雑さを解消するのみならず、常にユーザーが選択するセキュリティポリシーを反映させることが可能となる。

【００６０】
このような選択は、アクセスポイント２０の設定プログラムなどで、上記ポリシー１～ポリシー３を画面上に表示させ、ユーザーに対してマウスなどを利用して選択させ、選択結果を取得してレジスタなどに書き込んでおく。アクセスポイント２０は実際の処理時に同レジスタの内容を読み込み、同書き込み内容を反映した分岐処理を実行することになる。むろん、アクセスポイント２０にディップスイッチなどのハードウェアスイッチを設けておき、このスイッチ操作でセキュリティポリシーを選択できるようにしておいても良い。

【００６１】
以上でアクセスポイント２０の側におけるセキュリティ情報のパケット交換処理を終了する。

図３に戻ると、アクセスポイント２０はステップＳ４２０にてパケット交換が完了したか判断し、パケット交換が完了する前にステップＳ４１４にて所定時間が経過したと判断された場合を除き、ステップＳ４２２にて、上記決定したセキュリティ情報を設定する。すなわち、ステップＳ４５６，Ｓ４５８にて採用することとなった暗号化方式を採用することにしつつ、同暗号化方式に対応しているステーションＩＤと暗号鍵の値を以後の暗号化と復号化に採用することになる。また、同ステップＳ４２２では、端末５０のＭＡＣアドレスの登録も行う。すなわち、アクセスポイント２０は、端末５０のＭＡＣアドレスを、ＲＡＭ１３から記憶装置１４の管理領域に登録する処理を行う。

【００６２】
端末５０とのパケット交換の処理においては、ＴＫＩＰが採用されたので、ステーションＩＤは「ＥＳＳＩＤ３」を採用し、ＴＫＩＰの暗号鍵に「ＤＡＴＡ３」を採用することになる。

この後、アクセスポイント２０はステップＳ４２４にてワンタッチ登録モードを終えて通常の無線交信モードに切り替える。また、パケット交換中に所定時間が経過してしまったときもステップＳ４２６にてワンタッチ登録モードは終了するが、登録が完了していないので無線交信モードに切り替えることはしない。

【００６３】
このようにアクセスポイント２０は決定した暗号化方式を端末５０等に通知することはしない。

一方の端末５０の側では、パケット交換の完了後、ステップＳ３２８にて、アクセスポイント２０から受信して保存したセキュリティ情報から無線交信モードのアクセスポイント２０を探索する。上述したように、アクセスポイント２０から受信したセキュリティ情報というのは、暗号化方式ＷＥＰ６４に対応させた「ＥＳＳＩＤ１」と「ＤＡＴＡ１」と、暗号化方式ＷＥＰ１２８に対応させた「ＥＳＳＩＤ２」と「ＤＡＴＡ２」と、暗号化方式ＴＫＩＰに対応させた「ＥＳＳＩＤ３」と「ＤＡＴＡ３」である。

【００６４】
まず、端末５０は、アクセス可能なアクセスポイントのステーションＩＤを取得する。この手続はＩＥＥＥ８０２．１１の通信規格に基づいて実行されるものであり、端末５０においてはアクセスポイントからのビーコンを受信して現在アクセス可能なアクセスポイントのステーションＩＤが取得できる。上述したようにアクセスポイント２０は暗号化方式としてＴＫＩＰを採用したので、そのステーションＩＤは「ＥＳＳＩＤ３」である。従って、端末５０はアクセスポイント２０からのビーコンに基づいてそのステーションＩＤが「ＥＳＳＩＤ３」であることを取得し、先に受信して所定の記憶領域に保存したセキュリティ情報と対比する。対比結果として、ステーションＩＤが「ＥＳＳＩＤ３」であることは暗号化方式としてＴＫＩＰであることを特定するものであり、さらに暗号鍵として「ＤＡＴＡ３」を使用することによって暗号化と復号化が実現できることを検知できる。

【００６５】
ステップＳ３３０では発見したアクセスポイントの状態に合わせてアクセスポイントから受信したセキュリティ情報を設定する。すなわち、発見したステーションＩＤに対応す

る暗号化方式と暗号鍵を今後の暗号化と復号化に利用することになる。
このようにして、アクセスポイント２０への無線ＬＡＮアダプタ５２のＭＡＣアドレスの登録と、アクセスポイント２０及び端末５０への共通の暗号鍵の設定が完了する。そして、ステップＳ３３２では、端末５０は発見したアクセスポイント２０に接続するとともに、以後、後述する接続監視モードを開始する。

【００６６】

なお、ステップＳ３２８にてアクセスポイント２０を所定時間内に探索できなかったときには、ステップＳ３２６の判断を経て暗号化方式などを特定することなくステップＳ３３４に進み、ワンタッチ登録モードを中断する。
図５は、端末側における接続監視モードを示している。なお、図中の波線部分は他の処理が存在することを前提に関連の深い処理だけを示しているに過ぎない。
ステップＳ３２２にてパケット交換の処理を実施し、ステップＳ３３２にて発見したアクセスポイントに対して接続をしている状態で、ステップＳ３６０～Ｓ３６６の接続監視モードが実行される。すなわち、ステップＳ３６０では予め決定しておいた接続監視間隔が経過していないか判断し、経過したと判断したらステップＳ３６２にてアクセスポイント２０との接続状態が維持されているか否かを判断する。言い換えれば、一定時間間隔ごとにアクセスポイント２０との接続が維持されているかを判断することになる。維持されていれば再度ステップＳ３６０に戻るので、接続中は一定時間毎に同じ処理を繰り返すことになる。

【００６７】

一方、アクセスポイント２０との接続が維持されていない場合は、ステップＳ３６４にて受信できるアクセスポイントのビーコンからアクセス可能なアクセスポイントのステーションＩＤを取得し、同ステーションＩＤと、先にアクセスポイント２０から受信しているセキュリティ情報のステーションＩＤとを対比する。そして、一致するものがあればアクセスポイント２０はステーションＩＤを変化させて暗号化方式を変更しつつ無線交信モードとなっていることを検知することができる。ステップＳ３６６では発見したアクセスポイント２０の状態に合わせて予め受信していたセキュリティ情報を設定する。すなわち、以後は変化したステーションＩＤに対応している暗号化方式と暗号鍵を採用する。

【００６８】

次に、このような暗号化方式の変化が起こる状況を端末６０の登録の際に生じるアクセスポイント２０の側の処理に基づいて説明する。図６は図３に示すアクセスポイントにおける処理のなかで端末６０に対応して処理内容が変化するステップを特に示したものである。

【００６９】

端末６０を登録するにあたり、端末６０とアクセスポイント２０とがそれぞれステップＳ３５０，Ｓ４５０にてパケットの交換処理を行う。なお、端末６０が無線ＬＡＮに新たに参加する場合にも、アクセスポイント２０の側においては上述のＭＡＣ登録プログラムを実施するが、その内容は端末５０を登録する場合と同様であるため説明を省略する。
端末６０の無線ＬＡＮアダプタ６２が対応している暗号化方式はＷＥＰ６４とＷＥＰ１２８だけであるので、パケット交換の処理は、以下のようになる。

【００７０】

サブ１．端末６０から、アクセスポイント２０に対して、セキュリティ情報の作成リクエストを送出する。
サブ２．アクセスポイント２０から、端末６０に対して、リクエストの要求を表すリプライを送出する。なお、アクセスポイント２０は、既に端末５０からのリクエスト受信時に上述した暗号化方式毎のステーションＩＤと暗号鍵とを決定している。
サブ３．端末６０から、アクセスポイント２０に対して、端末６０で対応する暗号化方式を示すデータを送出する。この場合、端末６０に装着されている無線ＬＡＮアダプタ６２は、ＷＥＰ６４と、ＷＥＰ１２８とに対応しており、これら二つの暗号化方式をデータに表して送出する。

【００７１】
サブ４．アクセスポイント２０は、受信したデータに基づいて端末６０が対応可能な暗号化方式を検知し、同暗号化方式により自己の対応可能な暗号化方式を絞り込む。具体的には、端末６０の場合は、ＷＥＰ６４とＷＥＰ１２８に絞り込まれる。そして、これらの暗号化方式毎に、アクセスポイント２０から、端末６０に対して、暗号化方式ＷＥＰ６４に対応させた「ＥＳＳＩＤ１」と「ＤＡＴＡ１」と、暗号化方式ＷＥＰ１２８に対応させた「ＥＳＳＩＤ２」と「ＤＡＴＡ２」とを送出する。
【００７２】
すなわち、端末６０は、端末５０の場合と異なり、パケットの交換処理の結果、暗号化方式ＷＥＰ６４に対応させた「ＥＳＳＩＤ１」と「ＤＡＴＡ１」と、暗号化方式ＷＥＰ１２８に対応させた「ＥＳＳＩＤ２」と「ＤＡＴＡ２」だけを受信し、所定の記憶領域に保存することになる。
アクセスポイント２０は、端末６０が対応している暗号方式がＷＥＰ６４とＷＥＰ１２８だけであることを検知し、ステップＳ４５２にてその中での最高の暗号化（セキュリティ）レベルのＷＥＰ１２８を選択し、ステップＳ４５４にて現在採用している最高レベルのものと比較する。上述したように現在の最高レベルのものはＴＫＩＰであるから、ステップＳ４５４の判断では現在の最高レベルよりも低いと判断され、ステップＳ４５８にて今回の最高レベルであるＷＥＰ１２８を採用することになる。
【００７３】
ステップＳ４２２において、暗号化方式はＷＥＰ１２８を採用し、さらにステーションＩＤは「ＥＳＳＩＤ２」に変化させ、暗号鍵も「ＤＡＴＡ２」とする。また、ステップＳ４２４にて無線交信モードに切り替える。
端末６０は、上述した端末５０の場合と同様に、受信可能なアクセスポイントのビーコンからステーションＩＤを取得し、受信したセキュリティ情報に基づいて一致するステーションＩＤの暗号化方式と暗号鍵を採用し（ステップＳ３２８，３３０）、ステップＳ３３２にてアクセスポイント２０に接続する。
【００７４】
一方、端末５０は、ステップＳ３６０，Ｓ３６２にて一定時間毎にアクセスポイント２０との接続が維持されているか判断しているが、端末６０の登録によってステーションＩＤが「ＥＳＳＩＤ２」に変化したので、「ＥＳＳＩＤ３」をステーションＩＤとしていた接続状態は維持されていない。この結果、ステップＳ３６４にて受信できるアクセスポイントのビーコンからアクセスポイント２０のステーションＩＤが「ＥＳＳＩＤ２」に変化したことを検知する。そして、同ステーションＩＤによって、暗号化方式としてＷＥＰ１２８が採用されるとともに暗号鍵は「ＤＡＴＡ２」であることを検知し、これらの情報を設定する。その後、ステップＳ３３２にて同設定情報を利用してアクセスポイント２０に接続する。
【００７５】
このように、アクセスポイント２０は端末５０や端末６０に対して決定した暗号化方式を特に通知することはなかったにもかかわらず、端末５０や端末６０はステーションＩＤだけから暗号化方式と暗号鍵を特定できることになる。これは、端末が徐々に追加されていく状況では非常に有効である。なぜなら、従来の手法であれば、このようなアクセスポイントの設定情報に変化が有れば、各端末に対して通知するのが当然であったが、本発明の方式によればステーションＩＤを変更させるだけで、ＩＥＥＥ８０２．１１の通信規格に基づき、自ずから全端末が通信可能なアクセスポイントを発見しようと努めることになる。その結果、ステーションＩＤだけからその時点で有効な暗号化方式や暗号鍵に設定変更できる。従って、端末の追加に伴って暗号化方式を変化するときにも全端末に通知する必要がなくなり、セキュリティ上のメリットがある。
【００７６】
以上の処理を行うことにより、予め決めておいたセキュリティポリシーに基づくセキュリティレベルが維持される。

次に、無線ＬＡＮに参加する端末数が減少する場合のセキュリティ設定について説明する。

【００７７】

２‐２．端末数を減少させる場合について

これまでの説明においては、無線ＬＡＮに参加する端末数が増えた場合に、アクセスポイント２０と各端末間において用いる暗号化方式と暗号鍵とが変更され得る。ここで、アクセスポイント２０を中心として構築される無線ＬＡＮでは、各端末の所有者の都合によって、ネットワークに参加する端末数が流動的に変化する。従って、無線ＬＡＮに参加する端末が減る場合に、暗号化方式のセキュリティレベルをより高レベルのものに変更できる場合がある。

図７は、無線ＬＡＮに参加する端末数が減少した場合にアクセスポイント２０が実施する暗号化方式選択プログラムに対応したフローチャートである。

【００７８】

以下の処理は、アクセスポイント２０が無線交信モードに切替わっている状態において継続的に行うものである。

アクセスポイント２０は、無線交信モードにおいては、ステップＳ４６０にて所定の接続端末確認間隔が経過していないか確認し、経過したと判断した場合は、そのとき自己に接続している端末にかかる接続端末リストを生成する（ステップＳ４６２）。すなわち、アクセスポイント２０は、所定期間毎に上記接続端末リストを生成し直す。そして、かかる接続端末リストは、少なくとも上記接続端末確認間隔以上の期間、一時的にＲＡＭ１３などに記憶しておく。

【００７９】

ここで、接続端末リストは上記ＭＡＣアドレスを利用して生成する。すなわち、アクセスポイント２０は、上記ワンタッチ登録モードにおいて各端末のＭＡＣアドレスを登録しているため、接続端末リストの生成時に自己への接続を維持している端末のＭＡＣアドレスを選択して接続端末リストを生成する。

【００８０】

アクセスポイント２０は、最新の接続端末リストを生成したら、同最新の接続端末リストと保存しておいた前回生成した接続端末リスとを比較し、無線ＬＡＮに参加している端末が減少したか否か判断する（ステップＳ４６４）。端末数が減少していなければ、以下に述べる暗号化方式の見直し作業は行わない。これは、端末数が変化していなかったり、増加している場合には、上記ワンタッチ登録モードにおいて最後にある端末の追加登録を行った際に、所定のセキュリティポリシーに基づいて適切な暗号化方式の設定が行われたと考えられるからである。

端末数が減少していると判断した場合、アクセスポイント２０は、同アクセスポイント２０が採用可能であって、かつ上記最新の接続端末リストによって特定した各端末が共通して対応可能な暗号化方式のうち、最もセキュリティレベルの高い暗号化方式を選択する（ステップＳ４６６）。

【００８１】

ステップＳ４６８では、現在採用している暗号化方式のセキュリティレベルとステップＳ４６６で選択した暗号化方式のセキュリティレベルとを比較する。

ここでは、端末５０，６０がアクセスポイント２０を介して無線ＬＡＮに参加していた状況において端末６０が同無線ＬＡＮから離脱し、同端末６０の離脱によって、ステップＳ４６４で端末の減少を検知した場合を例に説明を行う。端末５０の無線ＬＡＮアダプタ５２は、ＷＥＰ６４と、ＷＥＰ１２８と、ＴＫＩＰとに対応しており、端末６０の無線ＬＡＮアダプタ６２はＷＥＰ６４と、ＷＥＰ１２８とに対応している。かかる、各端末５０，６０が夫々対応する暗号化方式は、上記セキュリティ情報パケットの交換処理において、すでにアクセスポイント２０側で取得できている。上述のように、端末６０が無線ＬＡＮから離脱したのであるから、上記ステップＳ４６６でアクセスポイント２０が選択する暗号化方式はＴＫＩＰということになる。

【００８２】
一方、ワンタッチ登録モードで端末５０，６０を登録した際に上記セキュリティポリシーとしてポリシー１が選択されていた場合、現在の暗号化方式としては、端末５０よりも対応可能な暗号化方式の最高レベルが低い端末６０でもネットワークに参加可能とするためにＷＥＰ１２８が採用されている。
【００８３】
ステップＳ４７０では、上記選択した暗号化方式のセキュリティレベルが現在の暗号化方式のセキュリティレベルを上回る場合に、上記選択した暗号化方式を採用する。上記の例では、上記選択した暗号化方式のセキュリティレベルが現在の暗号化方式のセキュリティレベルを上回るため、上記選択した暗号化方式ＴＫＩＰを採用する。このとき、アクセスポイント２０は、ステーションＩＤを「ＥＳＳＩＤ３」に変化させ、暗号鍵を「ＤＡＤＡ３」とする。
一方、上記選択した暗号化方式のセキュリティレベルが現在のセキュリティレベルよりも高くない場合には、現在のセキュリティレベルを維持し暗号化方式の変更は行わない。
【００８４】
すなわち、本願構成を用いれば、端末５０，６０のうち端末６０が無線ＬＡＮから離脱した後の無線ＬＡＮにおいては、採用する暗号化方式のセキュリティレベルが自動的に上がる場合がある。
【００８５】
かかる暗号化方式の見直しは、無線ＬＡＮに参加する端末数が減少した場合だけでなく、同参加する端末が所定の期間内に入替わった場合にも行う余地がある。
図８は、無線ＬＡＮに参加する端末が一部において入替わった場合にアクセスポイント２０が実施する暗号化方式選択プログラムに対応したフローチャートである。ここでは、一回の接続端末確認間隔の間に、端末５０，６０がアクセスポイント２０を介して無線ＬＡＮに参加していた状況において、端末７０が新たに登録端末として無線ＬＡＮに参加し、さらに端末６０が同無線ＬＡＮから離脱した場合を例に説明を行う。
【００８６】
つまり、ワンタッチ登録モードにおいて無線ＬＡＮアダプタ７２のＭＡＣアドレスをアクセスポイント２０に登録し、かつ端末５０～７０が共通して対応可能な暗号化方式と同暗号化方式において利用する暗号鍵が端末５０～７０に設定されている状態において、端末６０が無線ＬＡＮから離脱した場合である。なお、端末７０の無線ＬＡＮアダプタ７２は、ＷＥＰ６４と、ＷＥＰ１２８と、ＴＫＩＰとに対応しているものとする。同図においては、図７と相違する部分を中心に説明する。
【００８７】
同図に示すように、ステップＳ４８４の分岐でＮＯである場合には、「無線ＬＡＮに参加する端末に入替えがあるか？」という判断を行う（ステップＳ４８６）。具体的には、ステップＳ４８２で生成した最新の接続端末リストと、保存しておいた前回生成した接続端末リストとを比較し、各リストを構成する端末のＭＡＣアドレスに基づいて、無線ＬＡＮに参加する端末に入替えがあるかを判断する。本実施形態では、前回生成した接続端末リストは端末５０，６０を示し、最新の接続端末リストは端末５０，７０を示すため、ステップＳ４８８以下の処理に進み、暗号化方式の見直しを行う。
【００８８】
ステップＳ４８６にてＮＯの判断がされたとき、つまり、無線ＬＡＮから離脱した端末が無く単に端末数が増加している場合または、同無線ＬＡＮに参加している端末に変化が無い場合には、暗号化方式の見直し作業は行わない。この場合には、上記ワンタッチ登録モードにおいて最後にある端末の追加登録を行った際に、所定のセキュリティポリシーに基づいて適切な暗号化方式の設定が行われたと考えられるからである。
【００８９】
ステップＳ４８８以下の処理は、図７のステップＳ４６６以下の処理と同じである。上述のように、接続端末確認間隔の間に端末７０が追加され端末６０が無線ＬＡＮから離脱

したのであるから、ステップＳ４８８でアクセスポイント２０が選択する暗号化方式はＴＫＩＰということになる。一方、ワンタッチ登録モードで端末５０，６０を登録した際に上記セキュリティポリシーとしてポリシー１が選択されていた場合、現在の暗号化方式としてはＷＥＰ１２８が採用されている。従って、ステップＳ４９０における暗号化方式の見直しを行った結果、上記の例では暗号化方式ＴＫＩＰが採用され、セキュリティレベルが向上する。このように、図８にかかる構成によっても、採用する暗号化方式のセキュリティレベルを自動的に上げることができる。

【００９０】

なお、ステップＳ４６６，４８８において暗号化方式を選択する際に、「アクセスポイント２０が採用可能であって、かつ最新の接続端末リストによって特定した各端末が共通して対応可能な暗号化方式のうち、最もセキュリティレベルの高い暗号化方式を選択する」という指針を必ずしも用いる必要は無い。例えば、高度なセキュリティ設定を行うあまり、通信速度を犠牲にし過ぎる場合等には、上記ステップＳ４６６，４８８で選択可能な暗号化方式のセキュリティレベルに上限を設けておき、前記通信速度の低下といった不都合を回避するようにしても良い。

【００９１】

ある端末のネットワークからの離脱や入替えを契機として、採用される暗号化方式及び暗号鍵が変更になった場合でも、ネットワークへの接続を維持し続けようとする他の端末は、かかる変更に容易に追従できる。すなわち、図５で説明したように、アクセスポイント２０が暗号化方式を変更させてステーションＩＤを変更しても、ネットワークへの接続を維持し続けようとする端末は接続監視モードにおいて、同変更されたステーションＩＤを検知する。そして、同端末は、上記の例では暗号化方式として新たにＴＫＩＰが採用されるとともに暗号鍵は「ＤＡＴＡ３」であることを検知し、これらの情報を利用して、その後もアクセスポイント２０との接続を維持することができる。

【００９２】

また、セキュリティレベルを向上させる余地がある場合に、図９に示す処理を実行してもよい。

まず、アクセスポイント２０の側からステップＳ５００にて既に暗号鍵（キー）を配信した全端末に対して対応可能な暗号化方式を確認する確認パケットを送信する。

これに対して各端末はステップＳ３８０にてその時点で対応可能な暗号化方式を表す応答パケットを返信する。この場合、暗号化方式を返信しても良いし、予め各暗号化方式に対応させておいたセキュリティレベルを返信しても良い。

アクセスポイント２０の側では、ステップＳ５０２にて、今回応答があった全ての端末で共通するセキュリティレベルの最も高い暗号化方式と現在アクセスポイント２０が採用している暗号化方式とを対比し、セキュリティレベルが無用に下がっていないかを判断する。そして、セキュリティレベルを上げる余地があるのであれば、ステップＳ５０４にてセキュリティレベルを上げた暗号化方式に変更し、ステップＳ５０６にてその設定情報に変更する。この場合も敢えて各端末に対して変更の通知はしないが、各端末毎に接続監視モードにおいてアクセスポイント２０のステーションＩＤの変化の有無に基づき、適切な暗号化方式と暗号鍵に切り替えることができる。

【００９３】

３．変形例

以上本発明の一実施形態を説明したが、本発明は上記態様以外にも、本発明の要旨を逸脱しない範囲内において種々なる様態で実施し得ることは勿論である。

【００９４】

例えば、上記では、端末とアクセスポイントとの間でやりとりされるデータの内容を暗号化する技術としてＷＥＰなどを用いたが、これら以外の他の暗号化技術を用いても差し支えない。例えば、公開鍵暗号方式（データの暗号化と暗号化されたデータの復号化とで異なる暗号鍵を使用する方式）の暗号化技術を用いてもよい。また、強度の高い暗号化技術であるＷＰＡ（Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ）を用いることも考え

ることができる。

【００９５】

上記実施形態では、設定を、端末５０に装着された無線ＬＡＮアダプタ５２とアクセスポイント２０の送信機２５，受信機２６との間の電波の送受信によって実現したが、こうした電波以外の他の無線を用いた通信によって設定を行なう構成としても差し支えない。こうした他の無線としては、赤外線、光、音声信号、超音波、微弱電波などを考えることができる。また、端末５０とアクセスポイント２０との間の無線通信を、Ｂｌｕｅｔｏｏｔｈ（商標）という近距離間での無線通信方式を用いて実現することも可能である。

【００９６】

また、上記実施形態の構成に、上記のような他の無線によるデータ伝送を併用しても差し支えない。一例として、赤外線によるデータ伝送を併用した構成について、以下に説明する。上記実施形態の構成と異なる点は、アクセスポイント２０に、ＣＰＵ１１とバスにより相互に接続された赤外線受信インタフェースと、赤外線受信インタフェースに接続された赤外線受信部とを設ける点、端末５０等に、ＣＰＵとバスにより相互に接続された赤外線送信インタフェースと、赤外線送信インタフェースに接続された赤外線発信部とを設ける点である。

【００９７】

アクセスポイント２０側の赤外線受信部は、赤外線領域に感度を持つフォトダイオードによって構成されており、端末５０の赤外線発信部は、赤外線領域の波長の光を出力するＬＥＤによって構成されている。端末５０側の赤外線送信インタフェースは、ＣＰＵからの指令信号を、この指令信号を重畳させた伝送波に変換する。変換された伝送波は、赤外線発信部から発信される。こうして端末５０から発信された伝送波は、端末５０がセキュリティ受信エリア（赤外線受信部によって伝送波を受信可能なエリア）内にある場合に、アクセスポイント２０側の赤外線受信部によって受信される。こうして受信された伝送波を受け取った赤外線受信インタフェースは、伝送波を二値化された指令信号に変換し、変換後の指令信号をＣＰＵ１１に送る。

【００９８】

なお、上記の赤外線送信インタフェースや赤外線発信部は、これらを予め端末５０に組み込むことによって実現してもよいし、端末５０の音声出力端子に赤外線発信機を接続することによって実現してもよい。

以上、電波を用いたデータ通信に赤外線によるデータ伝送を併用した構成を一例として説明したが、赤外線以外の他の無線（例えば、光、音声信号、超音波、微弱電波）によるデータ伝送を電波を用いたデータ通信に併用することとしても差し支えない。また、可視光によるデータ伝送を併用する場合には、パーソナルコンピュータや携帯情報端末等の液晶表示部を発光素子として用いてもよい。こうすれば、端末の液晶表示部から、ＭＡＣアドレスの情報が重畳された光信号を、アクセスポイント２０に発信することが可能となる。

【００９９】

また、上記実施形態では、設定中における無線通信範囲を限定したが、このような無線通信範囲の限定は、上述した設定のみならず、アクセスポイント２０と端末５０との間のやり取りによって設定される他の情報にも適用することができる。例えば、特定の人に対してのみ有料コンテンツを送信するフリースポットでは、アクセスした端末の所有者が特定の人であることを認証するための情報（例えば、端末所有者の氏名，ＩＤやパスワード等）をアクセスポイント２０や端末５０に予め登録する場合がある。こうした個人を認証する情報の登録を、アクセスポイント２０と端末５０との間の無線通信範囲を限定しつつ、無線通信によって行なう構成としてもよい。こうすれば、ＩＤやパスワード等の個人を認証する情報をマニュアルで設定する必要がない。

【０１００】

４．まとめ

このように、アクセスポイント２０は、所定期間毎に繰り返し、自己を介した無線ＬＡ

Ｎに接続している端末を検知し、無線ＬＡＮに参加している端末数が減少している場合や端末に入替えがある場合には、採用する暗号化方式の見直しを行う。かかる見直しにおいて、ネットワークを構築する機器間で共通して採用可能な暗号化方式のうち最もセキュリティレベルの高い暗号化方式を選択するという指針に沿って暗号化方式を採用することにより、ある端末がネットワークから離脱した後や上記入替えがあった後において、不必要に低いレベルのセキュリティ設定が維持されてしまうということが防がれる。また、端末数が増加する場合には上記セキュリティポリシーに基づくセキュリティ設定を、端末数が減少したりや上記入替えがあった場合には上述した指針に基づいてセキュリティ設定の見直しを行うことで、ネットワークを構築する端末構成の変化にかかわらず、常にその時点で最適なセキュリティ環境を得ることができる。

【図面の簡単な説明】

【０１０１】

【図１】本発明の一実施形態にかかる暗号鍵設定システムを実現するハードウェア構成を示す説明図である。

【図２】アクセスポイントの構成を示す説明図である。

【図３】暗号鍵設定システムでのワンタッチ登録手順を示すフローチャートである。

【図４】パケット交換の処理と暗号化方式の決定手順を示すフローチャートである。

【図５】接続監視モードの処理手順を示すフローチャートである。

【図６】端末の追加の処理を示すフローチャートである。

【図７】端末の減少に伴う暗号化方式の決定手順を示すフローチャートである。

【図８】端末の入替に伴う暗号化方式の決定手順を示すフローチャートである。

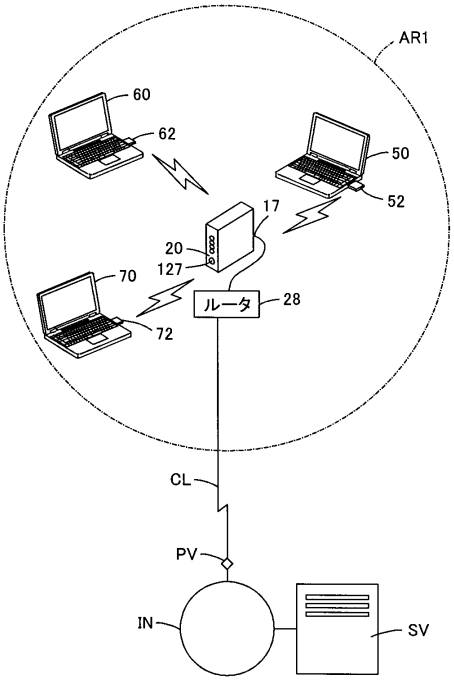
【図９】暗号化方式の変更を実行する手順を示すフローチャートである。

【符号の説明】

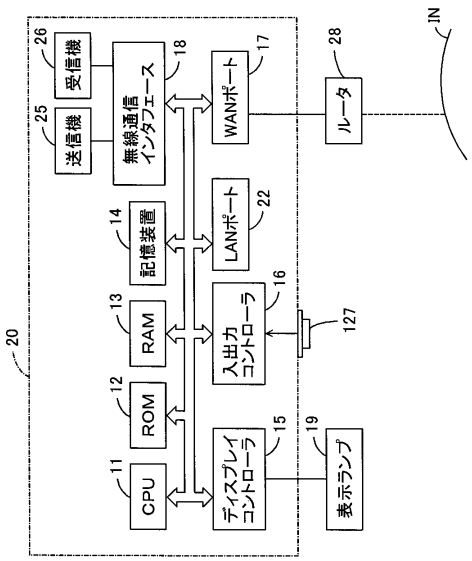
【０１０２】

１１…ＣＰＵ
１２…ＲＯＭ
１３…ＲＡＭ
１４…記憶装置
１５…ディスプレイコントローラ
１６…入出力コントローラ
１７…ＷＡＮポート
１８…無線通信インタフェース
２０…アクセスポイント
２２…ＬＡＮポート
２５…送信機
２６…受信機
２８…ルータ
５０，６０，７０…端末
５２，６２，７２…無線ＬＡＮアダプタ
１２７…登録ボタン
ＡＲ１…無線通信エリア

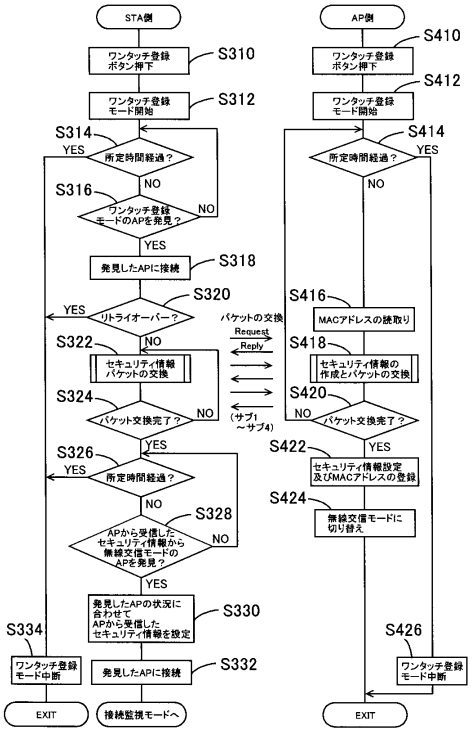
【図１】


AR1
60
62
50
52
17
20
127
70
72
ルータ
28
CL
PV
IN
SV

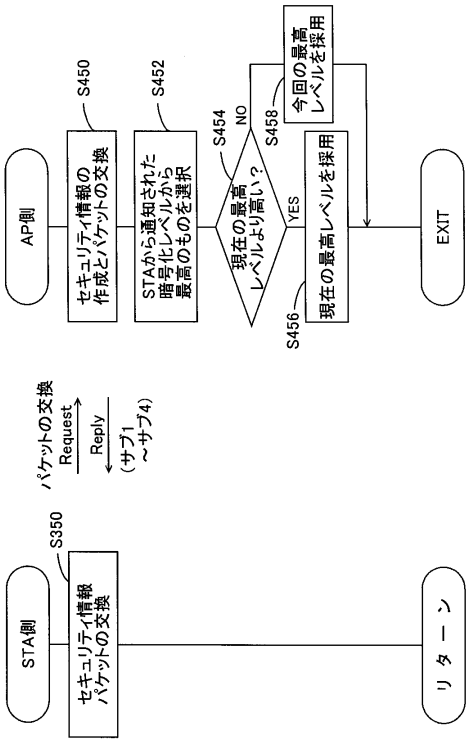
【図２】


IN
26
受信機
25
送信機
無線通信インタフェース
18
WANポート
17
ルータ
28
記憶装置
14
LANポート
22
RAM
13
入出力コントローラ
16
127
ROM
12
ディスプレイコントローラ
15
19
表示ランプ
CPU
11
20

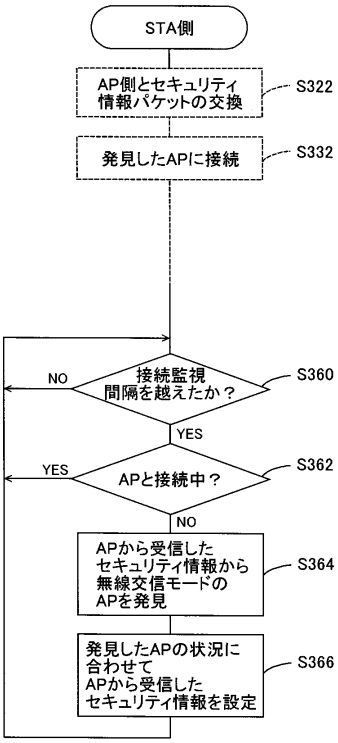
【図３】


STA側
AP側
ワンタッチ登録ボタン押下
S310
S410
ワンタッチ登録モード開始
S312
S412
S314
所定時間経過？
YES
NO
S414
S316
ワンタッチ登録モードのAPを発見？
NO
YES
発見したAPに接続
S318
S320
リトライオーバー？
YES
NO
パケットの交換
Request
Reply
（サブ1～サブ4）
S416
MACアドレスの読取り
S322
セキュリティ情報パケットの交換
S418
セキュリティ情報の作成とパケットの交換
S324
パケット交換完了？
NO
S420
S326
所定時間経過？
S422
セキュリティ情報設定及びMACアドレスの登録
S328
APから受信したセキュリティ情報から無線交信モードのAPを発見？
S424
無線交信モードに切り替え
発見したAPの状況に合わせてAPから受信したセキュリティ情報を設定
S330
S334
S426
ワンタッチ登録モード中断
発見したAPに接続
S332
EXIT
接続監視モードへ

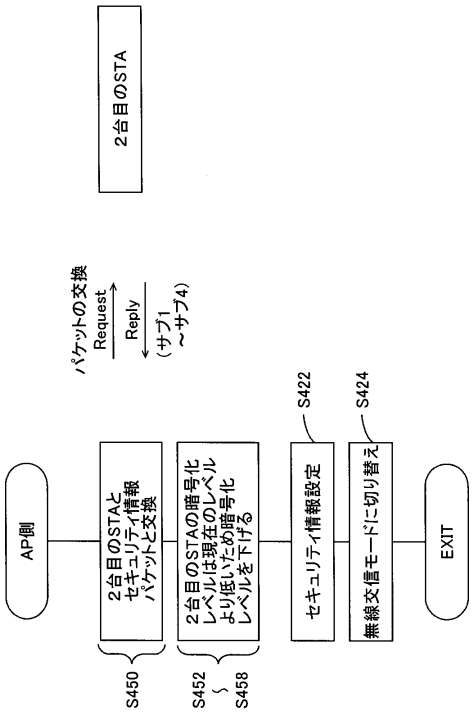
【図４】


AP側
S450
セキュリティ情報の作成とパケットの交換
S452
STAから通知された暗号化レベルから最高のものを選択
S454
現在の最高レベルより高い？
NO
YES
S458
今回の最高レベルを採用
S456
現在の最高レベルを採用
EXIT
パケットの交換
Request
Reply
（サブ1～サブ4）
S350
STA側
セキュリティ情報パケットの交換
リターン

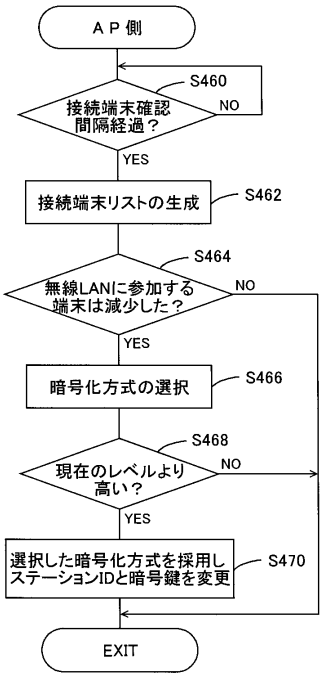
【図５】


STA側
AP側とセキュリティ情報パケットの交換
S322
発見したAPに接続
S332
接続監視間隔を越えたか？
S360
NO
YES
APと接続中？
S362
YES
NO
APから受信したセキュリティ情報から無線交信モードのAPを発見
S364
発見したAPの状況に合わせてAPから受信したセキュリティ情報を設定
S366

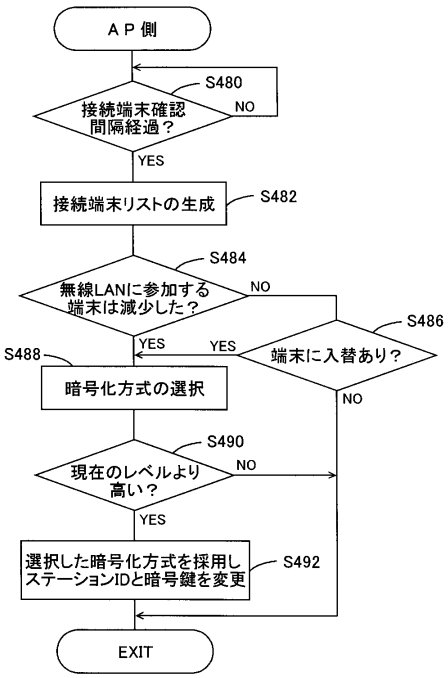
【図６】


2台目のSTA
パケットの交換
Request
Reply
（サブ1～サブ4）
AP側
2台目のSTAとセキュリティ情報パケットと交換
2台目のSTAの暗号化レベルは現在のレベルより低いため暗号化レベルを下げる
セキュリティ情報設定
無線交信モードに切り替え
EXIT
S422
S424
S450
S452
～
S458

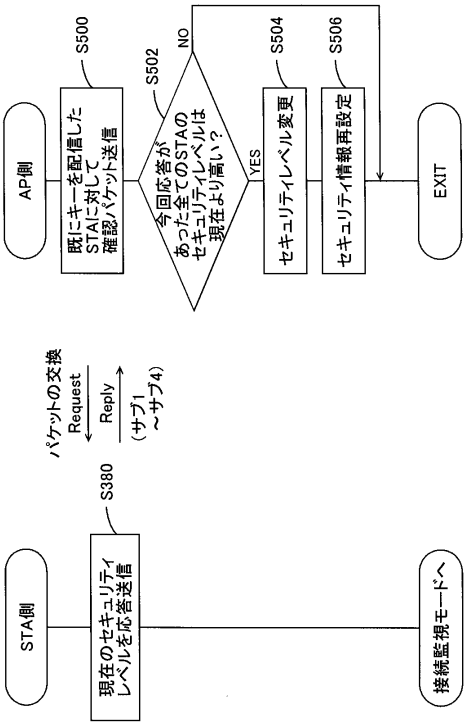
【図７】


ＡＰ側
接続端末確認間隔経過？
S460
NO
YES
接続端末リストの生成
S462
無線LANに参加する端末は減少した？
S464
NO
YES
暗号化方式の選択
S466
現在のレベルより高い？
S468
NO
YES
選択した暗号化方式を採用しステーションIDと暗号鍵を変更
S470
EXIT

【図８】


ＡＰ側
接続端末確認間隔経過？
S480
NO
YES
接続端末リストの生成
S482
無線LANに参加する端末は減少した？
S484
NO
YES
端末に入替あり？
S486
YES
NO
暗号化方式の選択
S488
現在のレベルより高い？
S490
NO
YES
選択した暗号化方式を採用しステーションIDと暗号鍵を変更
S492
EXIT

【図９】


AP側
S500
既にキーを配信した
STAに対して
確認パケット送信
S502
今回応答が
あった全てのSTAの
セキュリティレベルは
現在より高い？
NO
YES
S504
セキュリティレベル変更
S506
セキュリティ情報再設定
EXIT
パケットの交換
Request
Reply
（サブ1
～サブ4）
STA側
S380
現在のセキュリティ
レベルを応答送信
接続監視モードへ

フロントページの続き

(56)参考文献 特開２００４－０３２６６４（ＪＰ，Ａ）
坪山博貴，設定なんかでもう悩まない！ 達人たちの無線ＬＡＮスッキリ運用法 Ｐａｒｔ２ 絶対できるラクラク設定術，ＤＯＳ／Ｖ ｍａｇａｚｉｎｅ，ソフトバンクパブリッシング（株），２００３年 2月 4日，第１２巻，第４号，第１４４－１４８頁
清水理史，清水理史のイニシャルＢ 第87回：ワンタッチで設定できるバッファローの「AOSS」で変わる無線LANのセキュリティ対策，２００４年 1月２７日，[online]，２００４年1月２７日，[２０１０年6月１７日検索]，ＵＲＬ，http://bb.watch.impress.co.jp/cda/shimizu/4007.html