(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5067866号
(P5067866)
(45)発行日　平成24年11月7日(2012.11.7)　(24)登録日　平成24年8月24日(2012.8.24)

(51)Int.Cl.　F I
H04L 9/14 (2006.01)　H04L 9/00 641

請求項の数 9 (全 22 頁)

(21)出願番号　特願2008-1645(P2008-1645)
(22)出願日　平成20年1月8日(2008.1.8)
(65)公開番号　特開2009-164971(P2009-164971A)
(43)公開日　平成21年7月23日(2009.7.23)
審査請求日　平成22年12月14日(2010.12.14)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】通信装置及び制御方法

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
前記通信装置への接続を要求する第２の通信装置が要求する暗号化方式を確認する確認手段と、
前記確認手段により確認した前記第２の通信装置が要求する暗号化方式が、前記通信装置が形成する第１のネットワークで使用している第１の暗号化方式とは異なる第２の暗号化方式である場合に、前記第２の暗号化方式を用いる第２のネットワークを形成するための処理を行う形成手段と、
を有することを特徴とする通信装置。
【請求項２】
前記形成手段は、前記第２の暗号化方式を用いる第２のネットワークを形成し、該第２のネットワークを介して前記第２の通信装置と接続することを特徴とする請求項１に記載の通信装置。
【請求項３】
前記形成手段は、前記第２のネットワークを形成できるか否かを判断し、形成できると判断した場合に、前記第２のネットワークを形成するための処理を行うことを特徴とする請求項２に記載の通信装置。
【請求項４】
前記形成手段は、前記第２のネットワークを形成し、前記第２の暗号化方式に関する情

報を送信することを特徴とする請求項２に記載の通信装置。
【請求項５】
前記形成手段は、第３の通信装置に前記第２のネットワークを形成させるための処理を行うことを特徴とする請求項１に記載の通信装置。
【請求項６】
前記形成手段は、前記第２のネットワークを形成できる前記第３の通信装置の有無を判断し、前記第３の通信装置がある場合に、前記第３の通信装置に前記第２のネットワークの形成を要求することを特徴とする請求項５に記載の通信装置。
【請求項７】
前記第１のネットワークを介して通信されるデータと、前記第２のネットワークを介して通信されるデータとの中継を制限する制限手段を有することを特徴とする請求項１乃至請求項６の何れか１項に記載の通信装置。
【請求項８】
通信装置における制御方法であって、
確認手段が、前記通信装置への接続を要求する第２の通信装置が要求する暗号化方式を確認する確認工程と、
形成手段が、前記確認工程において確認した前記第２の通信装置が要求する暗号化方式が、前記通信装置が形成する第１のネットワークで使用している第１の暗号化方式とは異なる第２の暗号化方式である場合に、前記第２の暗号化方式を用いる第２のネットワークを形成するための処理を行う形成工程と、
を有することを特徴とする制御方法。
【請求項９】
通信装置のコンピュータに、
前記通信装置への接続を要求する第２の通信装置が要求する暗号化方式を確認する確認工程と、
前記確認工程において確認した前記第２の通信装置が要求する暗号化方式が、前記通信装置が形成する第１のネットワークで使用している第１の暗号化方式とは異なる第２の暗号化方式である場合に、前記第２の暗号化方式を用いる第２のネットワークを形成するための処理を行う形成工程と
を実行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、セキュリティレベルの異なる通信装置をネットワークに接続するための通信制御技術に関するものである。
【背景技術】
【０００２】
近年、無線通信の規格であるＩＥＥＥ８０２．１１規格（下記非特許文献１参照）に準拠した製品が広く普及し、通信装置による無線ＬＡＮの構築が一般的に行われるようになってきている。無線ＬＡＮにおける通信装置間の接続形態は、通常、以下の二つに大別することができる。
【０００３】
第一は、複数のステーション（ＳＴＡ）とアクセスポイント（ＡＰ）とにより構成されるインフラストラクチャ・モードである。また、第二は複数のステーションのみで構成され、アクセスポイントを介さずにステーション間で直接通信を行うアドホック・モードである。
【０００４】
このうちインフラストラクチャ・モードのように、中継器として機能するアクセスポイントを介して無線ＬＡＮを構築する場合、セキュリティ面において十分な注意を払う必要がある。アクセスポイントを介して無線ＬＡＮに不正侵入されたり、通信データが第三者

へ漏洩するといった事態が考えられるからである。
【０００５】
このため、インフラストラクチャ・モードの場合、データ伝送に暗号化方式が採用されなど、無線ＬＡＮの構築にあたっては、高度なセキュリティの確保が要求される。
【０００６】
暗号化方式の代表的なものとしては、例えばＷＥＰ（Wired Equivalent Privacy）が挙げられる。また、更に高度な暗号化方式としてＡＥＳ（Advanced Encryption Standard）等が挙げられる。これらの暗号化方式は、無線ＬＡＮを管理する管理者やユーザにより設定さる。
【０００７】
最近では、無線ＬＡＮに接続する際の無線パラメータの設定や暗号化方式の選択によるセキュリティレベルの設定を、アクセスポイント及びステーションに配されたボタンを押下することで自動的に実現する製品も登場してきている。
【０００８】
この無線パラメータの設定とセキュリティレベルの設定を簡易化するための規格として、ＷＰＳ（Wi-Fi Protected Setup）という規格が挙げられる。
【非特許文献１】ＩＥＥＥ　Ｓｔｄ　８０２．１１－１９９９（Ｒ２００３）
【発明の開示】
【発明が解決しようとする課題】
【０００９】
しかしながら、自動的に無線パラメータの設定やセキュリティレベルの設定ができるように構成すると、無線ＬＡＮ内にセキュリティレベルの低い通信装置が存在した場合に、全体のセキュリティレベルが低下してしまうという問題がある。
【００１０】
あるいは、ＷＥＰ等のセキュリティレベルの低い通信装置が、ＡＥＳ等が設定されたセキュリティレベルの高い無線ＬＡＮへ接続要求した場合に、接続が拒絶されてしまうという問題がある。
【００１１】
このため、設定の簡易化を図る一方で、セキュリティレベルの低い通信装置をネットワークに接続しようとした場合であっても、ネットワーク全体のセキュリティレベルを低下させることなく、接続できるようにすることが望まれている。
【００１２】
本発明は上記課題に鑑みてなされたものであり、セキュリティレベルの低い装置をネットワークに接続する場合であっても、ネットワーク全体のセキュリティレベルを低下させることなく、接続できるようにすることを目的とする。
【課題を解決するための手段】
【００１３】
上記の目的を達成するために本発明に係る通信装置は以下のような構成を備える。即ち、
通信装置であって、前記通信装置への接続を要求する第２の通信装置が要求する暗号化方式を確認する確認手段と、前記確認手段により確認した前記第２の通信装置が要求する暗号化方式が、前記通信装置が形成する第１のネットワークで使用している第１の暗号化方式とは異なる第２の暗号化方式である場合に、前記第２の暗号化方式を用いる第２のネットワークを形成するための処理を行う形成手段と、を有することを特徴とする。
【発明の効果】
【００１４】
本発明によれば、セキュリティレベルの低い装置をネットワークに接続する場合であっても、ネットワーク全体のセキュリティレベルを低下させることなく、接続できるようになる。
【発明を実施するための最良の形態】

【００１５】
以下、図面を参照しながら、本発明の好適な実施形態について詳説する。なお、以下の説明では、通信装置を、アクセスポイントとして機能する装置とステーションとして機能する装置の両方を含む概念として用いることとする。さらに、通信装置には、アクセスポイントとしての機能またはステーションとしての機能の一方または両方を備える装置が含まれるものとする。
【００１６】
［第１の実施形態］
＜１．セキュリティレベルの低いステーションが接続する前の無線ＬＡＮの構成＞
図１は、本発明の第１の実施形態に係るアクセスポイントを備える無線ＬＡＮの構成を示す図である。
【００１７】
図１において、１００は、暗号化方式としてＡＥＳ（第１の暗号化方式）を用いた通信装置により形成される無線ＬＡＮの無線エリアを示したものであり、１０１～１０３は、無線エリア１００にアソシエート中の第２の通信装置であるステーションである。
【００１８】
１０４は、ルータ機能を備えた通信装置であるアクセスポイントであり、ＡＥＳ用ＢＳＳ制御部（第１の制御部）が、無線エリア１００にアソシエート中のステーション１０１～１０３を制御する。なお、ＢＳＳ（Basic Service Set）とは、アクセスポイントが生成するグループの単位であり、ＡＥＳ用ＢＳＳ制御部は、ＡＥＳを用いたＢＳＳ（グループ）を制御する制御部である。
【００１９】
１１０は、アクセスポイント１０４が接続されるＩＳＰ（Internet Service Provider）である。
【００２０】
１１２～１１４は、暗号化方式としてＷＥＰのみ使用可能な通信装置であるステーションであり（使用可能なセキュリティレベルがステーション１０１～１０３よりも低いステーションであり）、図１では無線ＬＡＮに接続されていない状態にある。
【００２１】
１２１は、無線ＬＡＮに接続するためにステーション１１２～１１４から送信されるプローブ要求メッセージを示している。
【００２２】
＜２．セキュリティレベルの低いステーションが無線ＬＡＮに接続するまでの全体処理の流れ＞
図２は、セキュリティレベルの低いステーション１１２～１１４が、本実施形態にかかるアクセスポイント１０４とステーション１０１～１０３とにより形成された無線ＬＡＮに接続するまでの処理の流れを示す図である。
【００２３】
ステーション１０１～１０３は起動中であり、暗号化方式としてＡＥＳを使用し、アクセスポイント１０４へのアソシエートと認証とが既に完了した状態（Ｍ２０１）にある。
【００２４】
この状態で、ステーション１１２～１１４の電源が操作され、ステーション１１２～１１４が起動したとする（あるいは起動済みのステーション１１２～１１４が無線エリア１００内に移動したとする）。
【００２５】
ステーション１１２～１１４では、無線ＬＡＮへの接続を要求するために、アクセスポイント１０４に対して暗号化方式としてＷＥＰを使用することを示す情報を含むプローブ要求メッセージ（Ｍ２０２）を送信する。
【００２６】
アクセスポイント１０４では、プローブ要求メッセージ（Ｍ２０２）を受信すると、ス

テーション１０１～１０３との間で形成した無線ＬＡＮにおいて用いられている暗号化方式（ＡＥＳ）を示す情報を含むプローブ応答メッセージ（Ｍ２０３）を送信する。

【００２７】

ステーション１１２～１１４では、アクセスポイント１０４より送信されたプローブ応答メッセージ（Ｍ２０３）を受信し、プローブ応答メッセージ（Ｍ２０３）に含まれる暗号化方式（ＡＥＳ）を示す情報を確認する。

【００２８】

確認の結果、ステーション１１２～１１４の暗号化方式（ＷＥＰ）と、プローブ応答メッセージに含まれる情報が示す暗号化方式（ＡＥＳ）とが異なっていると判断した場合には、プローブ要求メッセージ（Ｍ２０４）を再送信する。これにより、ステーション１１２～１１４はセキュリティレベルの等しい他のアクセスポイントを検索する。

【００２９】

ここで、アクセスポイント１０４では、プローブ要求メッセージに含まれる暗号化方式（ＷＥＰ）を示す情報に対応すべく、新たに、当該暗号化方式（ＷＥＰ）によりステーションとの無線通信を行う制御部（ＷＥＰ用ＢＳＳ制御部）を起動する（２００）。

【００３０】

そしてＷＥＰ用ＢＳＳ制御部（第２の制御部）では、暗号化方式としてＷＥＰ（第２の暗号化方式）を使用することを示す情報を含むプローブ応答メッセージ（Ｍ２０５）を送信する。この結果、ステーション１１２～１１４の暗号化方式（ＷＥＰ）とプローブ応答メッセージ（Ｍ２０５）に含まれる情報が示す暗号化方式（ＷＥＰ）とが一致することとなる。

【００３１】

プローブ応答メッセージ（Ｍ２０５）を確認の結果、暗号化方式が一致すると判断した場合、ステーション１１２～１１４では、アクセスポイント１０４に対してアソシエート処理を起動する（Ｍ２０６）。

【００３２】

以上の処理により、ステーション１１２～１１４が、アクセスポイント１０４により形成される無線ＬＡＮに接続することが可能となる。

【００３３】

＜３．セキュリティレベルの低いステーションが接続した後の無線ＬＡＮの構成＞

図３は、セキュリティレベルの低いステーション１１２～１１４が、アクセスポイント１０４が形成する無線ＬＡＮに接続した後の構成を示す図である。図３において、３０１は、暗号化方式としてＷＥＰを使用した無線ＬＡＮの無線エリアを示している。

【００３４】

図３に示すように、本実施形態にかかるアクセスポイント１０４では、セキュリティレベルの異なるステーション群ごとに、異なる無線ＬＡＮ（第１のネットワーク１００と第２のネットワーク３０１）を形成する構成としている。これにより、セキュリティレベルの異なるステーションが混在していた場合でも、全体のセキュリティレベルを低下させることなく無線通信を行うことが可能となる。

【００３５】

＜４．アクセスポイントにおける処理の詳細＞

次に、図２に示す接続処理を実現するにあたってのアクセスポイント１０４における処理の詳細について説明する。

【００３６】

図４は、ステーション１１２～１１４が無線ＬＡＮに接続する際のアクセスポイント１０４における処理の流れを詳細に示すフローチャートである。

【００３７】

ステップＳ４０１では、ステーション１１２～１１４からのプローブ要求メッセージ（Ｍ２０２）を受信したか否かを確認する。

【００３８】

ステップＳ４０１において、ステーション１１２～１１４からのプローブ要求メッセージ（Ｍ２０２）を受信したと判断した場合には、ステップＳ４０２に進み、該プローブ要求メッセージに含まれる暗号化方式を示す情報を確認する。これにより、各ステーション１１２～１１４が使用可能な暗号化方式を確認することができる。

【００３９】

ステップＳ４０３では、ステップＳ４０２において確認した暗号化方式が、アクセスポイント１０４が形成する無線ＬＡＮにおいて用いられている暗号化方式と一致するか否かを確認する。

【００４０】

確認の結果、一致すると判断された場合（すなわち、暗号化方式としてＡＥＳを使用することを示す情報がプローブ要求メッセージ（Ｍ２０２）に含まれていると判断した場合）には、ステップＳ４０４に進み、通常のアソシエート処理を実行する。

【００４１】

一方、確認の結果、一致していないと判断した場合には、ステーション１１２～１１４に対して、アクセスポイント１０４は、以下の処理を実行する。

【００４２】

すなわち、ステップＳ４０５では、暗号化方式としてＡＥＳを用いた既存のＢＳＳ以外に、ステーション１１２～１１４が使用可能な暗号化方式を用いたＢＳＳを生成できるか否かを判断する。ここでは、ステーション１１２～１１４が使用可能な暗号化方式を用いたＢＳＳを生成するＢＳＳ制御部を起動して新たなＢＳＳを生成するか否かを判断する。

【００４３】

ステップＳ４０５において、ステーション１１２～１１４が使用可能な暗号化方式を用いたＢＳＳを生成できないと判断し、新たなＢＳＳ制御部を起動しないと判断した場合には、処理を終了する。

【００４４】

一方、ステップＳ４０５において、ステーション１１２～１１４が使用可能な暗号化方式を用いたＢＳＳを生成するために、新たにＢＳＳ制御部を起動させると判断した場合には、ステップＳ４０６に進む。ステップＳ４０６では、暗号化方式としてＷＥＰを使用する新たな無線ＬＡＮを形成するために、ＷＥＰ用ＢＳＳ制御部を起動する。ＷＥＰ用ＢＳＳ制御部は、ＡＥＳ用ＢＳＳ制御部と異なる無線ＬＡＮを形成するために、ＡＥＳ用ＢＳＳ制御部とは異なる暗号方式、ＥＳＳＩＤ（グループ識別情報：ネットワーク識別情報）、使用チャネル（周波数チャネル）を用いる。

【００４５】

ステップＳ４０７では、ステーション１１２～１１４が使用可能な暗号化方式（ＷＥＰ）を、アクセスポイント１０４においても使用可能であることを示す情報を含むプローブ応答メッセージ（Ｍ２０５）を返信する。

【００４６】

プローブ応答メッセージ（Ｍ２０５）の受信に応じてステーション１１２～１１４では、暗号化方式としてＷＥＰを使用した新たなＢＳＳ制御部に対するアソシエート処理（Ｍ２０６）を開始する。このため、ステップＳ４０８では、アソシエート要求があったか否かを判断する。ステップＳ４０８においてアソシエート要求があったと判断した場合には、ステップＳ４０９に進む。

【００４７】

ステップＳ４０９では、ステーション１１２～１１４それぞれとの間の無線通信において使用する暗号化方式（セキュリティレベル）を確認する。

【００４８】

確認の結果、ステーション１１２～１１４とのセキュリティレベルが等しいと判断した場合には、ステップＳ４１０からステップＳ４１１に進み、同じセキュリティレベルで無線通信が可能なステーションについてグループ識別情報を格納する。

【００４９】

＜５．ステーションにおける処理の詳細＞
次に、図２に示す接続処理を実現するにあたってのステーション１１２～１１４における処理の詳細について説明する。
【００５０】
図５は、ステーション１１２～１１４における無線ＬＡＮへの接続処理の流れを示すフローチャートである。
【００５１】
電源操作により起動すると、ステップＳ５０１では、接続要求を行う旨の指示があったか否かを確認し、接続要求を行う旨の指示があったと判断した場合には、ステップＳ５０２に進む。
【００５２】
ステップＳ５０２では、無線ＬＡＮへの接続を要求するために、アクセスポイント１０４に対して暗号化方式としてＷＥＰを使用することを示す情報を含んだプローブ要求メッセージ（Ｍ２０２）を送信する。
【００５３】
ステップＳ５０３では、アクセスポイント１０４からのプローブ応答メッセージ（Ｍ２０３）を受信したか否かを確認し、プローブ応答メッセージ（Ｍ２０３）を受信したと判断した場合には、ステップＳ５０４に進む。
【００５４】
ステップＳ５０４では、プローブ応答メッセージ（Ｍ２０３）に含まれる暗号化方式を示す情報を確認する。ステップＳ５０４における確認の結果、プローブ応答メッセージ（Ｍ２０３）に含まれる情報が示す暗号化方式と、ステーション１１２～１１４が使用可能な暗号化方式とが異なると判断した場合には、ステップＳ５０２に戻る。この場合、セキュリティレベルの等しい他のアクセスポイントを検索するため、プローブ要求メッセージ（Ｍ２０４）を再送信する。
【００５５】
一方、ステップＳ５０４における確認の結果、暗号化方式が一致すると判断した場合には、ステーション１１２～１１４は以下の処理を実行する。
【００５６】
すなわち、ステップＳ５０６では、アクセスポイント１０４において起動されたＢＳＳ制御部（ステーション１１２～１１４が使用可能な暗号化方式と一致する暗号化方式を用いるＢＳＳ制御部）を検索する。具体的には、検索タイマーを起動し、スキャン処理を開始する。
【００５７】
続いて、ステップＳ５０７において、アクセスポイント１０４において起動された新たなＢＳＳ制御部の検索に成功するまで、ステップＳ５０７～Ｓ５０８を繰り返す。
【００５８】
このとき、検索タイマーによるカウントアップが満了した場合には（ステップＳ５０７においてＹＥＳ）、ステップＳ５０２に戻り、再度セキュリティレベルが等しいＢＳＳ制御部を検索するため、プローブ要求メッセージ（Ｍ２０４）を再送信する。
【００５９】
一方、検索タイマーのカウントアップが満了する前に、暗号化方式としてＷＥＰを使用する新たなＢＳＳ制御部を検索した場合には（ステップＳ５０８：ＹＥＳ）、ステップＳ５０９に進み、アクセスポイント１０４に対してアソシエート処理を起動する。
【００６０】
ステップＳ５１０では、アクセスポイント１０４との間でアソシエーション処理（Ｍ２０６）を完了したか否かを確認し、完了したと判断された場合には、接続処理を終了する。
【００６１】
＜６．接続処理後の無線ＬＡＮにおける無線通信＞

図６は、本実施形態にかかるアクセスポイント１０４により形成される無線ＬＡＮ（ステーション１１２～１１４が接続された後の無線ＬＡＮ）における無線通信について説明するための図である。つまり、セキュリティレベルの異なるステーションと無線通信を行うＢＳＳ制御部が複数起動された状態におけるデータ伝送について説明するための図である。

【００６２】

図６において、６００は、ＢＳＳ制御部を備える制御部である。６０１は、アクセスポイント１０４の制御部６００が備えるＢＳＳ制御部のうち、暗号化方式としてＷＥＰを使用したＷＥＰ用ＢＳＳ制御部である。また、６０２は、暗号化方式としてＡＥＳを使用したＡＥＳ用ＢＳＳ制御部である。

【００６３】

また、６０３は、ＡＥＳ用ＢＳＳ制御部６０２からＷＥＰ用ＢＳＳ制御部６０１に伝送される伝送データを示したものであり、６０４は、ＷＥＰ用ＢＳＳ制御部６０１からＡＥＳ用ＢＳＳ制御部６０２に伝送される伝送データを示したものである。

【００６４】

図６において、ステーション１１２～１１４は、暗号化方式としてＷＥＰを使用したＷＥＰ用ＢＳＳ制御部６０１により形成される無線エリア３０１において、ＷＥＰ用ＢＳＳ制御部６０１の制御の下で無線通信を行う。

【００６５】

同様に、ステーション１０１～１０３は、暗号化方式としてＡＥＳを使用したＡＥＳ用ＢＳＳ制御部６０２により形成される無線エリア１００において、ＡＥＳ用ＢＳＳ制御部６０２の制御の下で無線通信を行う。

【００６６】

ＡＥＳ用ＢＳＳ制御部６０２からＷＥＰ用ＢＳＳ制御部６０１に伝送される伝送データ６０３については、ＷＥＰ用ＢＳＳ制御部６０１が、送信元のステーション１０１～１０３のアドレスを記憶する。

【００６７】

そして、ＷＥＰ用ＢＳＳ制御部６０１からＡＥＳ用ＢＳＳ制御部６０２に対しては、該記憶した送信元のステーション１０１～１０３のアドレスに対する伝送データのみを伝送する。つまり、セキュリティレベルの低いＢＳＳ制御部から、セキュリティレベルの高いＢＳＳ制御部への伝送データの伝送は、応答データのみに制限される。

【００６８】

以上の説明から明らかなように、本実施形態にかかるアクセスポイントを用いることにより、セキュリティレベルの低いステーションが接続要求を行った場合でもセキュリティレベルの異なるステーション毎に、無線ＬＡＮを分離することが可能となる。

【００６９】

また、アクセスポイント内部において、異なるセキュリティレベル間の伝送データを中継させる構成とすることで、伝送データを制限することが可能となる。この結果、以下のような効果を享受することが可能となる。

（１）セキュリティレベルの高い無線ＬＡＮと低い無線ＬＡＮとの混在が可能となる。

（２）それぞれのセキュリティレベルを保持することが可能となる。

（３）ＷＥＰ等のセキュリティレベルの低いステーションがセキュリティレベルの高い無線ＬＡＮのサービスを利用することが可能となる。

【００７０】

［第２の実施形態］

上記第１の実施形態では、セキュリティレベルの異なるステーションが接続要求を行った場合に、アクセスポイントが、新たにＢＳＳ制御部を起動させることにより（すなわち、２種類のＢＳＳ制御部を動作させることにより）対応することとした。

【００７１】

しかしながら、本発明はこれに限られず、例えば、既にアクセスポイントに接続してい

るステーションのうち、アクセスポイントとしての機能を有するステーションが、ＷＥＰ用ＢＳＳ制御部を起動させることで対応するようにしてもよい。以下、本実施形態の詳細について説明する。

【００７２】

＜１．セキュリティレベルの低いステーションが接続する前の無線ＬＡＮの構成＞

図７は、本発明の第２の実施形態に係るアクセスポイントを備える無線ＬＡＮの構成を示す図である。

【００７３】

図７において、７０１は、暗号化方式としてＡＥＳを使用した通信装置により形成される無線ＬＡＮの無線エリアを示したものであり、１０１～１０３は、無線エリア７０１にアソシエート中の第２の通信装置であるステーションである。また、７１１は、無線エリア７０１にアソシエート中の第３の通信装置であるディスプレイ装置である。ディスプレイ装置７１１は、ステーションモードとアクセスポイントモードの両方の機能を備える。

【００７４】

７１２は、無線エリア７０１にアソシエート中のステーション１０１～１０３およびディスプレイ装置７１１を制御するアクセスポイントである。アクセスポイント７１２が備えるＡＥＳ用ＢＳＳ制御部は、無線エリア７０１にアソシエート中のステーション１０１～１０３を制御する。

【００７５】

１１０は、アクセスポイント７１２が接続されるＩＳＰである。

【００７６】

７００はネットワーク制御装置であり、無線エリア７０１において接続中のステーション１０１～１０３、ディスプレイ装置７１１、アクセスポイント７１２それぞれにおいて使用可能な暗号化方式に関する情報を格納する。

【００７７】

７０２は、アクセスポイント７１２からネットワーク制御装置７００に対して伝送される伝送データである。７０３は、ネットワーク制御装置７００からアクセスポイント７１２に対して伝送される伝送データである。

【００７８】

７０４は、アクセスポイント７１２からディスプレイ装置７１１に対して伝送される伝送データである。７０５はディスプレイ装置７１１からアクセスポイント７１２に対して伝送される伝送データである。

【００７９】

１１２～１１４は、暗号化方式としてＷＥＰのみ使用可能な通信装置であるステーションであり（使用可能なセキュリティレベルがステーション１０１～１０３よりも低いステーションであり）、図７では、無線ＬＡＮに接続されていない状態にある。

【００８０】

１２１は、無線ＬＡＮに接続するためにステーション１１２～１１４から送信されるプローブ要求メッセージを示している。

【００８１】

＜２．セキュリティレベルの低いステーションが無線ＬＡＮに接続するまでの全体処理の流れ＞

図８は、セキュリティレベルの低いステーション１１２～１１４が本実施形態にかかるアクセスポイント７１２とステーション１０１～１０３、ディスプレイ装置７１１とにより形成された無線ＬＡＮに接続するまでの処理の流れを示す図である。

【００８２】

上述したように、ステーション１０１～１０３、およびディスプレイ装置７１１は、暗号化方式としてＡＥＳを使用し、アクセスポイント７１２へのアソシエートと認証とが既に完了した状態（Ｍ８０１）にある。

【００８３】

この状態で、ステーション１１２～１１４の電源が操作され、ステーション１１２～１１４が起動したとする（あるいは起動済みのステーション１１２～１１４が無線エリア７０１内に移動したとする）。

【００８４】

ステーション１１２～１１４では、無線ＬＡＮへの接続を要求するために、アクセスポイント７１２に対して暗号化方式としてＷＥＰを使用することを示す情報を含むプローブ要求メッセージ（Ｍ８０２）を送信する。

【００８５】

プローブ要求メッセージ（Ｍ８０２）を受信したアクセスポイント７１２では、ネットワーク制御装置７００に対して、ＡＰ問合せ要求メッセージ（Ｍ８０３）を送信する。ＡＰ問合せ要求メッセージ（Ｍ８０３）は、アクセスポイント７１２にアソシエート中の通信装置のうち、アクセスポイント機能を有する通信装置であって、暗号化方式としてＷＥＰを使用可能な通信装置の有無を問い合わせるメッセージである。

【００８６】

ＡＰ問合せ要求メッセージ（Ｍ８０３）を受信したネットワーク制御装置７００では、格納した情報を検索し、検索結果をＡＰ問合せ確認メッセージ（Ｍ８０４）としてアクセスポイント７１２に送信する。

【００８７】

また、アクセスポイント７１２では、プローブ要求メッセージ（Ｍ８０２）の応答として、プローブ応答メッセージ（Ｍ８０５）を送信する。プローブ応答メッセージ（Ｍ８０５）には、ステーション１０１～１０３、ディスプレイ装置７１１との間で形成した無線ＬＡＮにおいて用いられている暗号化方式（ＡＥＳ）を示す情報が含まれる。

【００８８】

ステーション１１２～１１４では、アクセスポイント７１２より送信されたプローブ応答メッセージ（Ｍ８０５）を受信し、プローブ応答メッセージ（Ｍ８０５）に含まれる暗号化方式（ＡＥＳ）を示す情報を確認する。

【００８９】

確認の結果、ステーション１１２～１１４の暗号化方式（ＷＥＰ）と、プローブ応答メッセージに含まれる情報が示す暗号化方式（ＡＥＳ）とが異なっていると判断した場合には、プローブ要求メッセージ（Ｍ８０７）を再送信する。これにより、ステーション１１２～１１４はセキュリティレベルの等しい他のアクセスポイントを検索する。

【００９０】

ここで、アクセスポイント７１２では、ＡＰ問合せ確認メッセージ（Ｍ８０４）を受信することにより、アクセスポイントとして機能し、かつステーション１１２～１１４の暗号化方式（ＷＥＰ）を使用可能な通信装置の有無を認識する。

【００９１】

本実施形態では、アクセスポイントとして機能し、ステーション１１２～１１４の暗号化方式（ＷＥＰ）を使用可能な通信装置として、ディスプレイ装置７１１を認識するものとする。この場合、アクセスポイント７１２からディスプレイ装置７１１に対して、グループ設定要求メッセージ（Ｍ８０６）を送信する。このグループ設定要求メッセージは、アクセスポイントとして起動し、指定する暗号化方式により新たな無線ＬＡＮの形成し、新たなグループの形成を要求するメッセージである。なお、グループ設定要求メッセージにより、グループを形成する通信装置、グループ識別情報、使用する周波数チャネルを指定してもよい。グループ設定要求メッセージ（Ｍ８０６）を受信したディスプレイ装置７１１では、該メッセージにより指定された暗号化方式（ＷＥＰ）による無線ＬＡＮを形成するために、ＷＥＰ用ＢＳＳ制御部を起動する（８００）。

【００９２】

ディスプレイ装置７１１のＷＥＰ用ＢＳＳ制御部では、暗号化方式としてＷＥＰを使用することを示す情報を含むプローブ応答メッセージ（Ｍ８０８）を送信する。この結果、ステーション１１２～１１４の暗号化方式とプローブ応答メッセージ（Ｍ８０８）に含ま

れる情報が示す暗号化方式とが一致することとなる。

【００９３】

プローブ応答メッセージ（Ｍ８０８）を確認の結果、暗号化方式が一致すると判断した場合、ステーション１１２～１１４では、ディスプレイ装置７１１のＷＥＰ用ＢＳＳ制御部に対してアソシエート処理を起動する（Ｍ８０９）。

【００９４】

以上の処理により、ステーション１１２～１１４が、ディスプレイ装置７１１により形成される無線ＬＡＮに接続することが可能となる。

【００９５】

アソシエート処理が完了すると、ディスプレイ装置７１１は、新たなグループを形成したことをアクセスポイント７１２に通知するために、グループ設定確認メッセージ（Ｍ８１０）をアクセスポイント７１２に送信する。グループ設定確認メッセージ（Ｍ８１０）を受信したアクセスポイント７１２では、ネットワーク制御装置７００に対して、グループ設定通知メッセージ（Ｍ８１１）を送信する。グループ設定通知メッセージ（Ｍ８１１）を受信したネットワーク制御装置７００では、これを格納する。

【００９６】

＜３．セキュリティレベルの低いステーションが接続した後の無線ＬＡＮの構成＞

図９は、セキュリティレベルの低いステーション１１２～１１４が接続した後の無線ＬＡＮの構成を示す図である。図９に示すように、ステーション１０１～１０３は、アクセスポイント７１２が生成する第１のネットワークに接続し、ステーション１１２～１１４は、ディスプレイ装置７１１が生成する２のネットワークに接続している。

【００９７】

また、ネットワーク制御装置７００には、暗号化方式としてＡＥＳを用いたステーション１０１～１０３に関する情報に加え、ＷＥＰを用いたステーション１１２～１１４に関する情報が格納される。

【００９８】

＜４．アクセスポイントにおける処理の詳細＞

次に、図８に示す接続処理を実現するにあたってのアクセスポイント７１２における処理の詳細について説明する。

【００９９】

図１０は、アクセスポイント７１２における接続処理の流れを詳細に示すフローチャートである。

【０１００】

ステップＳ１００１では、ステーション１１２～１１４からのプローブ要求メッセージ（Ｍ８０２）を受信したか否かを確認する。

【０１０１】

ステップＳ１００１において、ステーション１１２～１１４からのプローブ要求メッセージ（Ｍ８０２）を受信したと判断した場合には、ステップＳ１００２に進み、該プローブ要求メッセージに含まれる暗号化方式を示す情報を確認する。これにより、各ステーション１１２～１１４が使用可能な暗号化方式を確認することができる。

【０１０２】

ステップＳ１００３では、ステップＳ１００３において確認した暗号化方式が、アクセスポイント７１２が形成する無線ＬＡＮにおいて用いられている暗号化方式と一致するか否かを確認する。

【０１０３】

確認の結果、一致すると判断された場合（すなわち、暗号化方式としてＡＥＳを使用することを示す情報がプローブ要求メッセージ（Ｍ８０２）に含まれていると判断した場合）には、ステップＳ１００４に進み、通常のアソシエート処理を実行する。

【０１０４】

一方、確認の結果、一致していないと判断した場合には、無線エリア７０１に存在する

通信装置の中からアクセスポイントの機能を有し、かつプローブ要求メッセージに含まれる情報が示す暗号化方式を使用する通信装置を特定する処理を実行する。

【０１０５】

具体的には、ステップＳ１００５において、ネットワーク制御装置７００に対してＡＰ問合せ要求メッセージ（Ｍ８０３）を送信する。更にステップＳ１００６において、ＡＰ問合せ確認メッセージ（Ｍ８０４）待ち状態に遷移する。

【０１０６】

ステップＳ１００７では、ネットワーク制御装置７００より、ＡＰ問合せ確認メッセージ（Ｍ８０４）を受信すると、該メッセージを解析し、該当する通信装置が存在するか否かを判断する。ステップＳ１００７において該当する通信装置が存在しないと判断した場合には、処理を終了する。

【０１０７】

一方、ステップＳ１００７において、該当する通信装置が存在すると判断した場合には、接続要求をしているステーション１１２～１１４に対して、以下の処理を実施する。なお、ここでは、ディスプレイ装置７１１が、該当する通信装置であるとする。

【０１０８】

ステップＳ１００７では、接続要求をしているステーション１１２～１１４に対して、プローブ応答メッセージ（Ｍ８０５）を返信する。なお、アクセスポイント７１２より返信されるプローブ応答メッセージ（Ｍ８０５）には、暗号化方式としてＡＥＳを使用することを示す情報が含まれる。

【０１０９】

ステップＳ１００８では、アクセスポイント７１２が、ディスプレイ装置７１１に対して、ステーション１１２～１１４のグループ識別情報を含むグループ設定要求メッセージ（Ｍ８０６）を送信する。これにより、ディスプレイ装置７１１では、ＷＥＰ用ＢＳＳ制御部が起動されることとなる。

【０１１０】

ステップＳ１００９では、アクセスポイント７１２が、ディスプレイ装置７１１からのグループ設定確認メッセージ（Ｍ８１０）待ちの状態に遷移する。

【０１１１】

グループ設定確認メッセージ（Ｍ８１０）待ち状態において、ディスプレイ装置７１１からのグループ設定確認メッセージ（Ｍ８１０）を受信した場合には、ステップＳ１００９からステップＳ１０１０に進む。

【０１１２】

ステップＳ１０１０では、グループ設定確認メッセージ（Ｍ８１０）を解析する。そして新たな無線エリア９００を形成するディスプレイ装置７１１、ステーション１１２～１１４、これらの装置により形成されるグループを識別するグループ識別情報を含むグループ設定通知メッセージ（Ｍ８１１）をネットワーク制御装置７００に送信する。

【０１１３】

＜５．ディスプレイ装置における処理の詳細＞

次に、図８に示す接続処理を実現するにあたってのディスプレイ装置７１１における処理の詳細について説明する。

【０１１４】

図１１は、ディスプレイ装置７１１における処理の流れを示すフローチャートである。

【０１１５】

なお、ディスプレイ装置７１１は、アクセスポイント７１２に対してアソシエートと認証とが完了した状態（Ｍ８０１）にあるものとする。

【０１１６】

ステップＳ１１０１では、アクセスポイント７１２からイベントを受信したか否かを判定する。ステップＳ１１０１においてイベントを受信したと判定した場合には、ステップＳ１１０２に進み、当該イベントが、グループ設定要求メッセージ（Ｍ８０６）であるか

否かを判定する。
【０１１７】
ステップＳ１１０２において、当該イベントがグループ設定要求メッセージ（Ｍ８０６）でないと判断された場合には、ステップＳ１１０３に進み、当該イベントに従った処理を行う。
【０１１８】
一方、ステップＳ１１０２において、当該イベントがグループ設定要求メッセージ（Ｍ８０６）であると判断された場合には、ステップＳ１１０４に進む。
【０１１９】
ステップＳ１１０４では、ＢＳＳ制御部を起動し、該要求により指定される暗号化方式を使用した無線ＬＡＮ（ＢＳＳ）を生成可能か否かを判断する。ここでは、ステーション１１２～１１４が使用可能な暗号化方式（ＷＥＰ）を使用したＢＳＳ制御部を起動し、無線ＬＡＮを生成可能か否かを判断する。ステップＳ１１０４において、当該暗号化方式（ＷＥＰ）を使用したＢＳＳ制御部（ＷＥＰ用ＢＳＳ制御部）を起動しないと判断した場合には、処理を終了する。
【０１２０】
一方、ステップＳ１１０４において、当該暗号化方式（ＷＥＰ）を使用したＢＳＳを生成するために、ＢＳＳ制御部（ＷＥＰ用ＢＳＳ制御部）を起動すると判断された場合には、ステップＳ１１０５に進む。ステップＳ１１０５では、暗号化方式としてＷＥＰを使用する新たな無線ＬＡＮを形成するために、ＷＥＰ用制御部を起動する。ＷＥＰ用制御部は、グループ設定要求メッセージにより指定された暗号化方式を用いてＢＳＳを生成する。なお、グループ設定要求メッセージによりＥＳＳＩＤ（グループ識別情報：ネットワーク識別情報）、使用チャネル（周波数チャネル）も指定される場合は、指定されたＥＳＳＩＤ，仕様チャネルを用いてＢＳＳを生成する。　ステップＳ１１０６では、ディスプレイ装置７１１が、暗号化方式としてＷＥＰを使用した新たなＢＳＳ制御部を起動後、ステーション１１２～１１４それぞれとの間でアソシエート処理（Ｍ８０９）を実施する。
【０１２１】
ステップＳ１１０７では、ディスプレイ装置７１１が、ステーション１１２～１１４との無線通信において使用する暗号化方式と接続台数とを確認する。ディスプレイ装置７１１では、暗号化方式が一致し、かつセキュリティレベルが等しいステーションについての情報をグループ設定確認メッセージの情報要素として格納する。
【０１２２】
これらの処理を、接続要求のあった全てのステーション１１２～１１４について行い、ステーション１１２～１１４全てに対する処理が完了すると、ステップＳ１１０９に進み、グループ設定確認メッセージ（Ｍ８１０）をアクセスポイント７１２に送信する。
【０１２３】
＜６．ステーションにおける処理の詳細＞
次に、図８に示す接続処理を実現するにあたってのステーション１１２～１１４における処理の詳細について説明する。
【０１２４】
図１２は、ステーション１１２～１１４における無線ＬＡＮへの接続処理の流れを示すフローチャートである。
【０１２５】
電源操作により起動すると、ステップＳ１２０１では、接続要求を行う旨の指示があったか否かを確認し、接続要求を行う旨の指示があったと判断した場合には、ステップＳ１２０２に進む。
【０１２６】
ステップＳ１２０２では、無線ＬＡＮへの接続を要求するために、アクセスポイント７１２に対して暗号化方式としてＷＥＰを使用することを示す情報を含んだプローブ要求メッセージ（Ｍ８０２）を送信する。

【０１２７】
ステップＳ１２０３では、アクセスポイント７１２からのプローブ応答メッセージ（Ｍ８０５）を受信したか否かを確認し、プローブ応答メッセージ（Ｍ８０５）を受信したと判断した場合には、ステップＳ１２０４に進む。
【０１２８】
ステップＳ１２０４では、プローブ応答メッセージ（Ｍ８０５）に含まれる暗号化方式を確認する。ステップＳ１２０４における確認の結果、プローブ応答メッセージ（Ｍ８０５）に含まれる暗号化方式とステーション１１２～１１４が使用可能な暗号化方式とが異なると判断した場合には（ステップＳ１２０５においてＮｏ）、ステップＳ１２０２に戻る。この場合、セキュリティレベルの等しい他のアクセスポイントを検索するため、プローブ要求メッセージ（Ｍ８０７）を再送信する。
【０１２９】
一方、ステップＳ１２０４における確認の結果、暗号化方式が一致すると判断した場合（ステップＳ１２０５においてＹＥＳ）、ステーション１１２～１１４は以下の処理を実行する。
【０１３０】
すなわち、ステップＳ１２０６において、ディスプレイ装置７１１において起動されたＢＳＳ制御部（ステーション１１２～１１４が使用可能な暗号化方式と一致する暗号化方式を用いるＢＳＳ制御部）を検索する。具体的には、検索タイマーを起動し、スキャン処理を開始する。
【０１３１】
続いて、ステップＳ１２０７において、ディスプレイ装置７１１において起動された新たなＢＳＳ制御部の検索に成功するまで、ステップＳ１２０７～Ｓ１２０８を繰り返す。
【０１３２】
このとき、検索タイマーによるカウントアップが満了した場合には（ステップＳ１２０７においてＹＥＳ）、ステップＳ１２０２に戻り、再度セキュリティレベルが等しいＢＳＳ制御部を検索するため、プローブ要求メッセージ（Ｍ８０７）を再送信する。
【０１３３】
一方、検索タイマーのカウントアップが満了する前に、暗号化方式としてＷＥＰを使用する新たなＢＳＳ制御部を検索した場合には（ステップＳ１２０８：ＹＥＳ）、ステップＳ１２０９に進む。ステップＳ１２０９では、当該ＢＳＳ制御部を備えるディスプレイ装置７１１に対してアソシエート処理を起動する。
【０１３４】
ステップＳ１２１０では、アクセスポイント７１２との間でアソシエーション処理（Ｍ８０９）を完了したか否かを確認し、完了したと判断された場合には、接続処理を終了する。
【０１３５】
＜７．接続処理後の無線ＬＡＮにおける無線通信＞
図１３は、本実施形態にかかるアクセスポイント７１２及びディスプレイ装置７１１により形成される無線ＬＡＮ（ステーション１１２～１１４が接続された後の無線ＬＡＮ）における無線通信について説明するための図である。つまり、セキュリティレベルの異なるステーションと無線通信を行うディスプレイ装置７１１のＢＳＳ制御部が起動された状態におけるデータ伝送について説明するための図である。
【０１３６】
図１３において、ステーション１０１～１０３は、暗号化方式としてＡＥＳを使用した無線エリア７０１において、アクセスポイント７１２の制御の下で無線接続された状態にある。同様に、ステーション１１２～１１４は、暗号化方式としてＷＥＰを使用した無線エリア９００において、ディスプレイ装置７１１の制御の下で無線接続された状態にある。更に、ディスプレイ装置７１１は、アクセスポイント７１２の制御の下で、無線接続された状態にある。

【０１３７】
１３０１は、アクセスポイント７１２からネットワーク制御装置７００に伝送される伝送データを示したものである。なお、ネットワーク制御装置７００では、無線エリア７０１と無線エリア９００のそれぞれの通信装置に関するセキュリティレベルの情報を無線エリア毎に分類して格納する。また、両方の無線エリアに属しているディスプレイ装置７１１は、それぞれの管理エリアに格納される。
【０１３８】
１３０２は、アクセスポイント７１２からディスプレイ装置７１１に伝送される伝送データを示したものである。１３０３は、ディスプレイ装置７１１からアクセスポイント７１２に伝送される伝送データを示したものである。
【０１３９】
アクセスポイント７１２からディスプレイ装置７１１に対して伝送される伝送データ１３０２について、ディスプレイ装置７１１では、送信元であるステーション１０１～１０３のアドレスを記憶する。
【０１４０】
そして、ディスプレイ装置７１１からアクセスポイント７１２に対しては、ディスプレイ装置７１１において、受信時に記憶したステーション１０１～１０３の送信元アドレスに応答する伝送データのみを伝送する。つまり、セキュリティレベルの低いＢＳＳ制御部から、セキュリティレベルの高いＢＳＳ制御部への伝送データの伝送は応答データのみに制限される。
【０１４１】
以上の説明から明らかなように、本実施形態にかかるアクセスポイントを用いることにより、セキュリティレベルの低いステーションが接続要求を行った場合でもセキュリティレベルの異なるステーション毎に、無線ＬＡＮを分離することが可能となる。
【０１４２】
また、アクセスポイントとディスプレイ装置との間の伝送データを制限することが可能となる。この結果、以下のような効果を享受することが可能となる。
（１）セキュリティレベルの高い無線ＬＡＮと低い無線ＬＡＮとの混在が可能となる。
（２）それぞれのセキュリティレベルを保持することが可能となる。
（３）ＷＥＰ等のセキュリティレベルの低いステーションがセキュリティレベルの高い無線ＬＡＮのサービスを利用することが可能となる。
【０１４３】
［第３の実施形態］
上記第１及び第２の実施形態では、ＷＥＰ用ＢＳＳ制御部とＡＥＳ用ＢＳＳ制御部との間において伝送データを伝送するにあたり、送信元アドレスに折り返す伝送データ以外を制限する構成とした。
【０１４４】
しかしながら、本発明はかかる構成に限られず、例えば、予め設定されたアドレスまたはそれ以外のアドレスに合致したアドレスに伝送する伝送データを、制限するように構成してもよい。
【０１４５】
あるいは、アドレスよりも上位のレイヤ、例えばＩＰアドレスとポート番号等のＴＣＰ／ＵＤＰセッションの一部の情報を記憶しておき、これを折り返す伝送データ以外の伝送データを制限するように構成してもよい。
【０１４６】
［第４の実施形態］
上記第２の実施形態では、ネットワーク制御装置７００が、無線エリア７０１と無線エリア９００それぞれの無線ＬＡＮ毎の通信装置に関するセキュリティレベルを管理することとした。
【０１４７】

しかしながら、本発明はこれに限定されず、無線ＬＡＮ毎の通信装置に関するセキュリティレベルを管理する機能を、ＷＰＳにおけるレジストラにおいて実現するように構成してもよい。

【０１４８】

［他の実施形態］

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【０１４９】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給するよう構成することによっても達成されることはいうまでもない。この場合、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することにより、上記機能が実現されることとなる。なお、この場合、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【０１５０】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピ（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【０１５１】

また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現される場合に限られない。例えば、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１５２】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、前述した実施形態の機能が実現される場合も含まれる。つまり、プログラムコードがメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって実現される場合も含まれる。

【図面の簡単な説明】

【０１５３】

【図１】本発明の第１の実施形態に係るアクセスポイントを備える無線ＬＡＮの構成を示す図である。

【図２】セキュリティレベルの低いステーション１１２～１１４が、アクセスポイント１０４とステーション１０１～１０３とにより形成された無線ＬＡＮに接続するまでの処理の流れを示す図である。

【図３】セキュリティレベルの低いステーション１１２～１１４が、アクセスポイント１０４が形成する無線ＬＡＮに接続した後の構成を示す図である。

【図４】ステーション１１２～１１４が無線ＬＡＮに接続する際のアクセスポイント１０４における処理の流れを詳細に示すフローチャートである。

【図５】ステーション１１２～１１４における無線ＬＡＮへの接続処理の流れを示すフローチャートである。

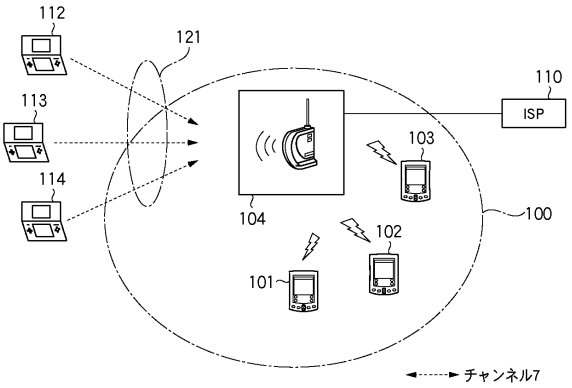
【図６】アクセスポイント１０４により形成される無線ＬＡＮ（ステーション１１２～１１４が接続された後の無線ＬＡＮ）における無線通信について説明するための図である。

【図７】本発明の第２の実施形態に係るアクセスポイントを備える無線ＬＡＮの構成を示す図である。

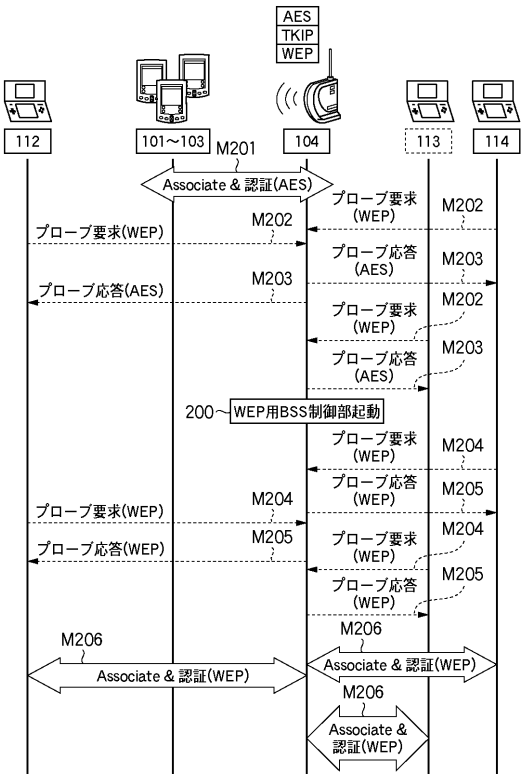
【図８】セキュリティレベルの低いステーション１１２～１１４がアクセスポイント７１

２とステーション１０１～１０３と、ディスプレイ装置７１１とにより形成された無線ＬＡＮに接続するまでの処理の流れを示す図である。
【図９】セキュリティレベルの低いステーション１１２～１１４が接続した後の無線ＬＡＮの構成を示す図である。
【図１０】アクセスポイント７１２における接続処理の流れを詳細に示すフローチャートである。
【図１１】ディスプレイ装置７１１における処理の流れを示すフローチャートである。
【図１２】ステーション１１２～１１４における無線ＬＡＮへの接続処理の流れを示すフローチャートである。
【図１３】アクセスポイント７１２及びディスプレイ装置７１１により形成される無線ＬＡＮ（ステーション１１２～１１４が接続された後の無線ＬＡＮ）における無線通信について説明するための図である。
【符号の説明】
【０１５４】
１００　無線エリア
１０１～１０３　ステーション
１０４　アクセスポイント
１１０　ＩＳＰ
１１２～１１４　ステーション
３０１　無線エリア
６０１　ＷＥＰ用ＢＳＳ制御部
６０２　ＡＥＳ用ＢＳＳ制御部
６０３　伝送データ
６０４　伝送データ
７００　ネットワーク制御装置
７０１　無線エリア
７１１　ディスプレイ装置
７１２　アクセスポイント
９００　無線エリア
１３０２　伝送データ
１３０３　伝送データ

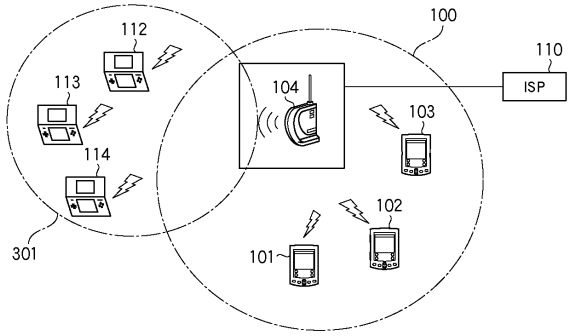
【図１】


112
121
113
114
110
ISP
103
104
102
100
101
チャンネル7

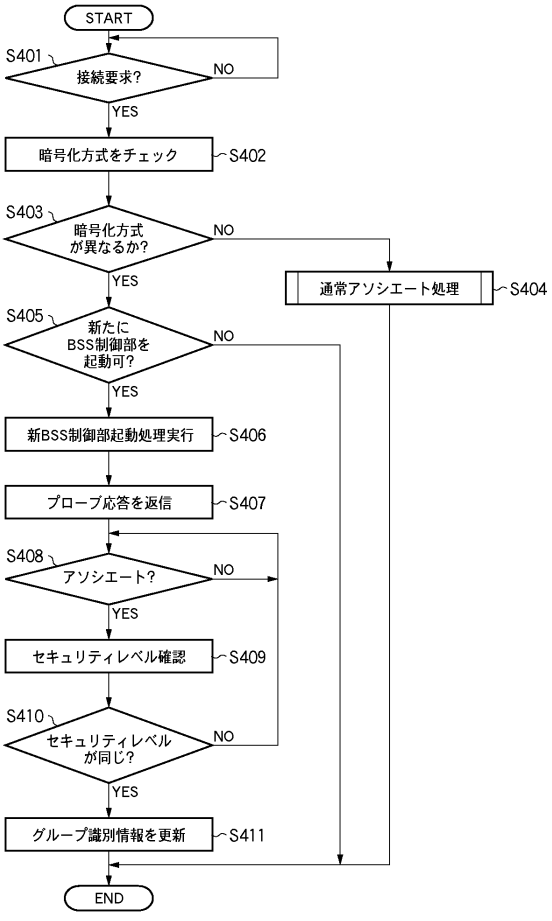
【図２】


AES
TKIP
WEP
112
101～103
104
113
114
M201
Associate & 認証(AES)
プローブ要求(WEP)
M202
プローブ応答(AES)
M203
200
WEP用BSS制御部起動
M204
プローブ応答(WEP)
M205
M206
Associate & 認証(WEP)

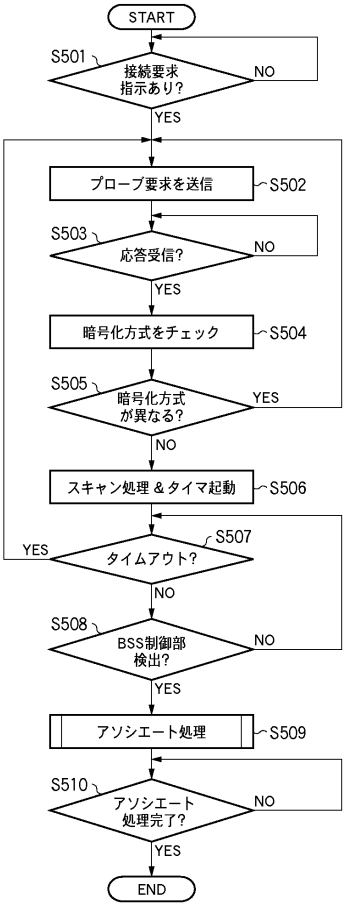
【図３】


100
112
110
ISP
113
104
103
114
102
301
101

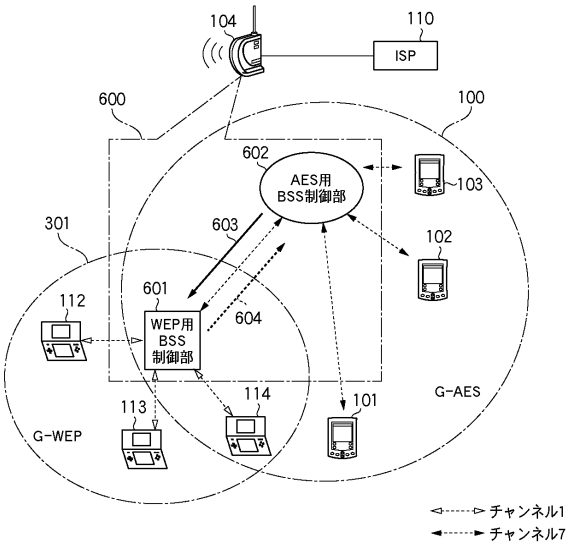
【図４】


START
S401
接続要求?
NO
YES
暗号化方式をチェック
S402
S403
暗号化方式が異なるか?
通常アソシエート処理
S404
S405
新たにBSS制御部を起動可?
新BSS制御部起動処理実行
S406
プローブ応答を返信
S407
S408
アソシエート?
セキュリティレベル確認
S409
S410
セキュリティレベルが同じ?
グループ識別情報を更新
S411
END

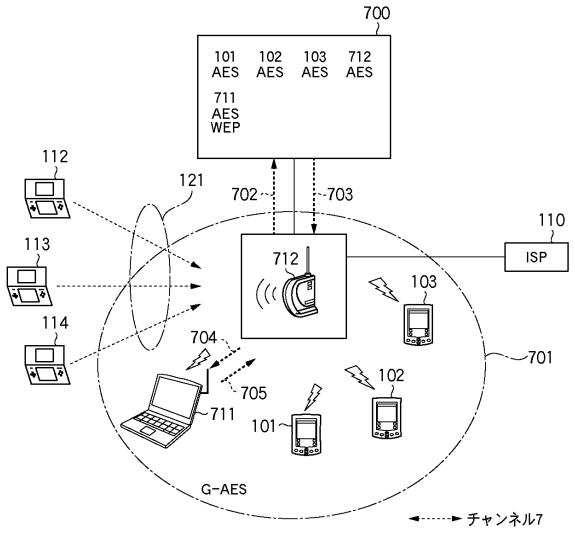
【図５】


START
S501
接続要求指示あり?
NO
YES
プローブ要求を送信
S502
S503
応答受信?
NO
YES
暗号化方式をチェック
S504
S505
暗号化方式が異なる?
YES
NO
スキャン処理＆タイマ起動
S506
S507
YES
タイムアウト?
NO
S508
BSS制御部検出?
NO
YES
アソシエート処理
S509
S510
アソシエート処理完了?
NO
YES
END

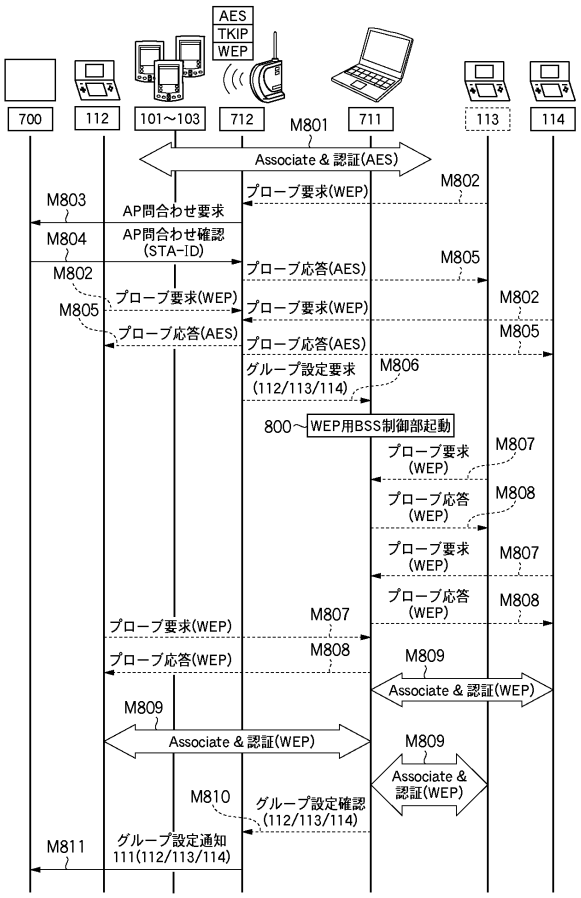
【図６】


104
110
ISP
600
100
602
AES用BSS制御部
103
301
603
102
601
112
WEP用BSS制御部
604
G-AES
114
113
101
G-WEP
チャンネル1
チャンネル7

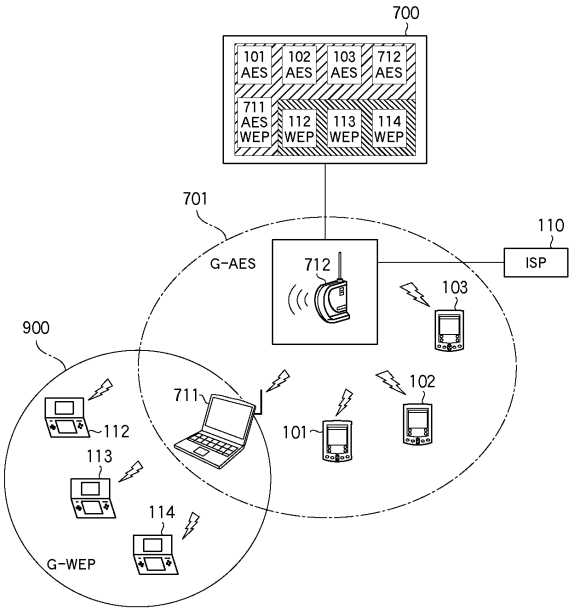
【図７】


700
101 AES
102 AES
103 AES
712 AES
711 AES WEP
112
121
702
703
110
ISP
113
712
103
114
704
701
705
102
711
101
G-AES
チャンネル7

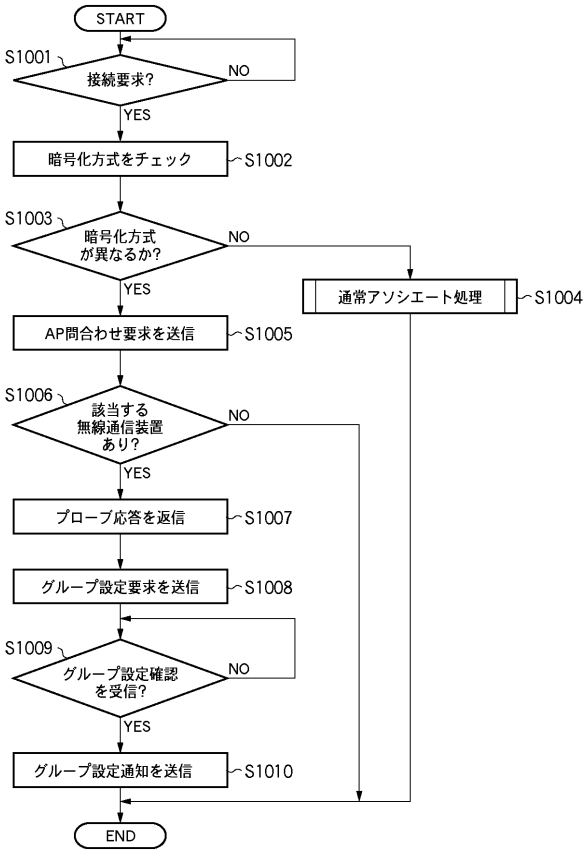
【図８】


AES
TKIP
WEP
700
112
101～103
712
711
113
114
M801
Associate & 認証(AES)
M802
プローブ要求(WEP)
M803
AP問合わせ要求
M804
AP問合わせ確認(STA-ID)
M805
プローブ応答(AES)
M806
グループ設定要求(112/113/114)
800
WEP用BSS制御部起動
M807
プローブ要求(WEP)
M808
プローブ応答(WEP)
M809
Associate & 認証(WEP)
M810
グループ設定確認(112/113/114)
M811
グループ設定通知111(112/113/114)

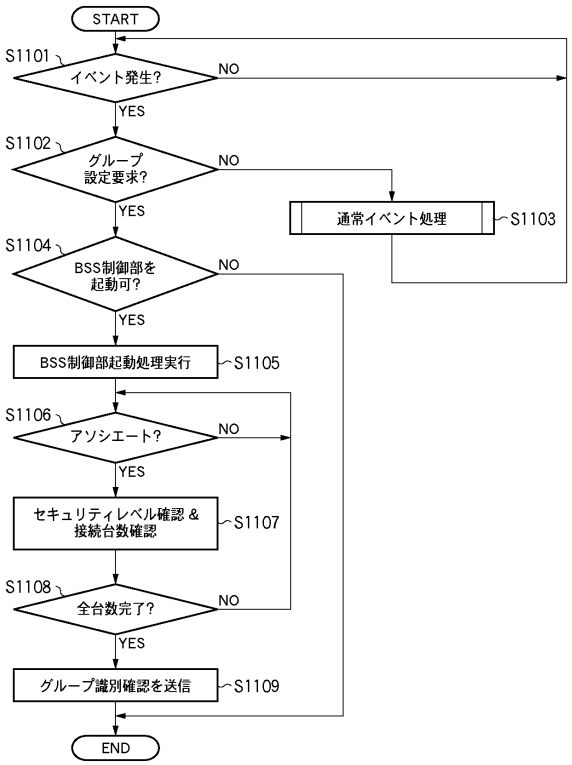
【図９】



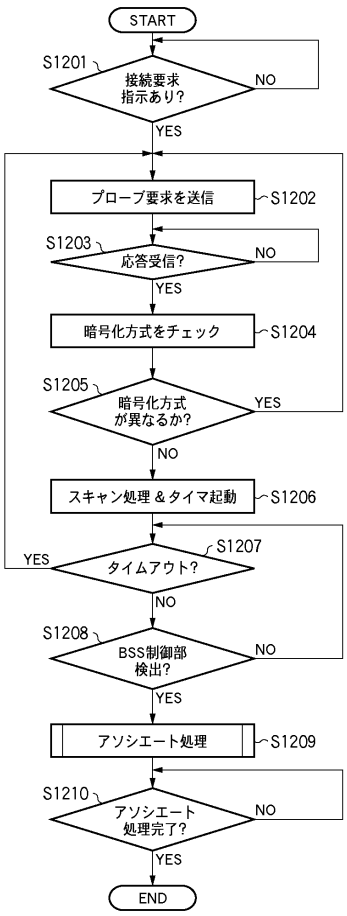
【図１０】



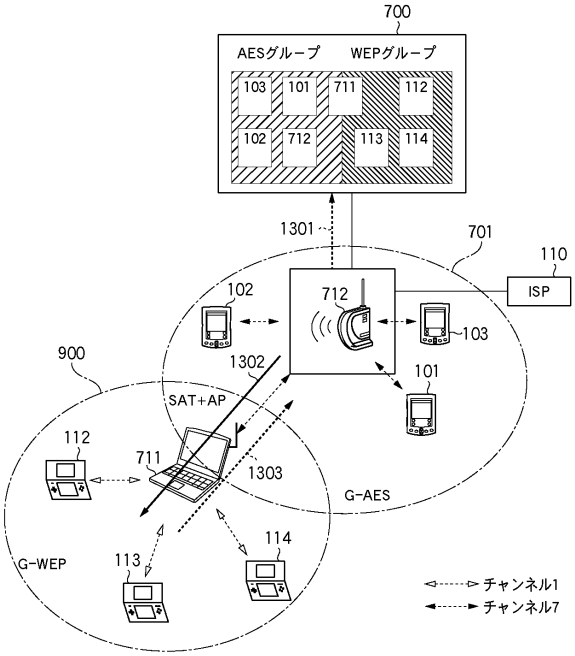
【図１１】



【図１２】



【図１３】


700
AESグループ
WEPグループ
103
101
711
112
102
712
113
114
1301
701
110
ISP
102
712
103
101
900
1302
SAT+AP
112
711
1303
G-AES
114
G-WEP
113
チャンネル1
チャンネル7

フロントページの続き

(72)発明者　池田　宣弘
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　中里　裕正

(56)参考文献　特開２００９－５５３８１（ＪＰ，Ａ）
特開２００６－１８６９４１（ＪＰ，Ａ）
特表２００５－５２４３４２（ＪＰ，Ａ）
特表２００５－１７５５２４（ＪＰ，Ａ）
特開２００４－３２６６４（ＪＰ，Ａ）
無線LANサービスを多様化させる仮想アクセスポイント技術，ホワイト・ペーパー，コルブリス・ネットワークス，２００５年　7月１０日，ＵＲＬ，http://japan.colubris.com/download/WP_VAP.pdf
簡単、高速、配線スッキリのワイヤレス　無線ＬＡＮ導入作戦，日経パソコン　Ｎｏ．５３９　NIKKEI PERSONAL COMPUTING，日本，日経ＢＰ社　Nikkei Business Publications,Inc.

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４