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

特許第5002149号
(P5002149)

(45)発行日　平成24年8月15日(2012.8.15)　(24)登録日　平成24年5月25日(2012.5.25)

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

請求項の数 10　(全 17 頁)

(21)出願番号	特願2005-342224 (P2005-342224)
(22)出願日	平成17年11月28日 (2005.11.28)
(65)公開番号	特開2006-246433 (P2006-246433A)
(43)公開日	平成18年9月14日 (2006.9.14)
審査請求日	平成20年11月25日 (2008.11.25)
(31)優先権主張番号	特願2005-27224 (P2005-27224)
(32)優先日	平成17年2月3日 (2005.2.3)
(33)優先権主張国	日本国(JP)

(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　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(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　中木　努

最終頁に続く

(54)【発明の名称】通信装置及び通信方法

(57)【特許請求の範囲】
【請求項１】
報知信号と、他の通信装置から送信される探索信号に対する応答信号と、を送信する通信装置であって、
グループ識別情報を前記報知信号に含めずに送信する隠蔽機能のオン／オフを切り替える切替手段と、
前記切替手段により前記隠蔽機能をオンにしている際に他の通信装置から探索信号を受信した場合、前記探索信号に含まれる暗号化された第１のグループ識別情報を復号する復号手段と、
前記復号手段により復号した前記第１のグループ識別情報に予め定められた情報が含まれているか否かを判別する判別手段と、
前記第１のグループ識別情報とは異なる前記隠蔽機能により隠蔽している第２のグループ識別情報を暗号化する暗号化手段と、
前記判別手段による判別に応じて、前記探索信号に対する応答信号に前記暗号化手段により暗号化した前記第２のグループ識別情報を含めて送信する送信手段と、
を有することを特徴とする通信装置。
【請求項２】
請求項１において、
前記第２のグループ識別情報は、前記通信装置が形成するネットワークを特定するための情報であることを特徴とする通信装置。

【請求項３】
請求項１又は２において、
前記送信手段は、前記予め定められた情報が含まれている場合に、前記探索信号に対する応答信号に前記第２のグループ識別情報を含めて送信し、前記予め定められた情報が含まれていない場合には、前記探索信号に対する応答信号に前記第２のグループ識別情報を含めずに送信することを特徴とする通信装置。
【請求項４】
請求項１乃至３の何れかにおいて、
前記予め定められた情報は、前記他の通信装置から前記通信装置への登録を要求するための情報、前記他の通信装置の識別情報に基づく情報、前記通信装置の識別情報に基づく情報の少なくとも何れかを含むことを特徴とする通信装置。
【請求項５】
請求項１乃至４の何れかにおいて、
前記予め定められた情報は、前記通信装置が形成するネットワークを特定するための情報を含むことを特徴とする通信装置。
【請求項６】
請求項１乃至５の何れかにおいて、
前記判別手段が前記他の通信装置からの前記探索信号に前記予め定められた情報が含まれていないと判別した回数を記憶する記憶手段と、
前記回数に応じて、前記他の通信装置からのアクセスを制限する制限手段と、
を有することを特徴とする通信装置。
【請求項７】
請求項１乃至６の何れかにおいて、
前記第１のグループ識別情報に含まれている情報と前記探索信号に含まれる他の情報とを比較する第１の比較手段を更に有し、
前記判別手段は、前記第１の比較手段による比較結果に応じて、前記予め定められた情報が含まれているか否かを判別することを特徴とする通信装置。
【請求項８】
請求項１乃至７の何れかにおいて、
前記第１のグループ識別情報に含まれている情報と前記通信装置に設定されている情報とを比較する第２の比較手段を更に有し、
前記判別手段は、前記第２の比較手段による比較結果に応じて、前記予め定められた情報が含まれているか否かを判別することを特徴とする通信装置。
【請求項９】
報知信号と、他の通信装置から送信される探索信号に対する応答信号と、を送信する通信装置の通信方法であって、
第２のグループ識別情報を含めず隠蔽して報知信号を送信している際に、他の通信装置から探索信号を受信した場合に、前記探索信号に含まれる暗号化された第１のグループ識別情報を復号する復号工程と、
前記復号工程により復号した第１のグループ識別情報に予め定められた情報が含まれているか否かを判別する判別工程と、
前記第１のグループ識別情報とは異なる前記隠蔽機能により隠蔽している第２のグループ識別情報を暗号化する暗号化工程と、
前記判別工程における判別に応じて、前記探索信号に対する応答信号に前記暗号化手段により暗号化した前記第２のグループ識別情報を含めて送信する送信工程と、
を有することを特徴とする通信方法。
【請求項１０】
請求項９記載の通信方法の各工程をコンピュータに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、グループ識別情報を隠蔽して報知信号を送信する機能を備えた通信装置及び通信方法に関する。
【背景技術】
【０００２】
従来の無線ＬＡＮシステムではアクセスポイントと端末それぞれにおいて、同じグループ識別子（ＳＳＩＤ）の設定を手動で行わなければならなかった。これはアドホックモードやインフラストラクチャモードなどトポロジの違いなどを意識して設定する必要があるために、ある程度ＰＣに慣れたユーザー向けには良いが、初心者には向かないとされてきた。
【０００３】
しかし、最近では、端末側のアプリケーションにおいて、近隣の複数のグループ識別子（ＳＳＩＤ）を自動的に検出することにより、接続可能なアクセスポイントの一覧を生成し、この中から接続するアクセスポイントをユーザーに選択させるものもある。このような無線ＬＡＮサポートでは、暗号化によるセキュリティを無視すれば、ユーザーによる複雑な操作無しに、ほとんど自動的にネットワークへの接続を完了することができる。このような理由から、近年ホームユースへの浸透が進んでいる。
【０００４】
特に無線ＬＡＮシステムにおいては、セキュリティの観点から公開されているグループ識別子（ＳＳＩＤ）に対しては、使用者とは無関係な無線端末（悪意のある第三者）が不要なアクセスを行うことも考えられる。従って、所望の無線端末の接続が確認された後に、自動検出のために公開しているグループ識別子（ＳＳＩＤ）を意図的に隠蔽するといった、ステルス機能を備えたアクセスポイント装置が近年増加している。
【０００５】
又、別の従来例としては、例えば特許文献１をあげることが出来る。
【特許文献１】特開２００３－２３３９１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、意図的にグループ識別子（ＳＳＩＤ）を隠蔽したステルス機能を備えたアクセスポイント装置に、新たな無線端末を接続収容するためには、無線端末ユーザーが、予めグループ識別子（ＳＳＩＤ）を知りおき、個別に設定する方法がある。これは、グループ識別子（ＳＳＩＤ）をユーザーに通知するため、セキュリティの観点から情報（グループ識別子（ＳＳＩＤ））の漏洩が問題とされている。
【０００７】
また、アクセスポイント装置の管理者により一旦、ステルス機能を解除し、接続可能なアクセスポイントの一覧から接続するアクセスポイントをユーザーに選択させる方法がある。これは、従来のアクセスポイント管理者および無線端末ユーザーにおいては操作が煩雑なものとなり、更には利便性が著しく損なわれ、使い勝手の悪いものとなっている。
【課題を解決するための手段】
【０００８】
本発明は、上記問題点を解決することを目的とし、グループ識別情報を報知信号に含めずに送信する隠蔽機能をオンにして前記報知信号を送信している際に、他の通信装置から探索信号を受信した場合に、前記探索信号に含まれる暗号化された第１のグループ識別情報を復号し、該第１のグループ識別情報に予め定められた情報が含まれているか否かを判別し、該判別に応じて、前記探索信号に対する応答信号に前記第１のグループ識別情報とは異なる第２のグループ識別情報を暗号化し、暗号化した第２のグループ情報を含めて前記探索信号を送信した他の通信装置に送信することを特徴とする。
【発明の効果】
【０００９】

本発明によれば、意図的にグループ識別情報を隠蔽している通信装置から容易にグループ識別情報を取得でき、情報の漏洩を軽減でき、セキュリティが向上する。

【発明を実施するための最良の形態】

【００１０】

以下、本発明における無線通信システムの実施形態について、添付の図面を用いて説明する。図１は、本発明の第１の実施形態に係る無線通信システム構成図である。

【００１１】

図１において、無線アクセスポイント装置（以下、ＡＰ）１０３は、ネットワーク１０４に有線接続され、ネットワークにおけるデータ搬送制御／経路選択機能を提供する。また、無線端末１０１、１０２等の無線端末と無線通信リンクを確立する。

【００１２】

図２は、実施形態におけるＡＰ１０３の内部構成を表すブロック図であり、中央制御部２０１は、ＡＰ１０３のシステム制御を行う。有線インタフェース部２０２は、ＬＡＮケーブルを用いてネットワーク１０４に接続される。無線インタフェース部２０３は、アンテナ２０４を介して無線端末１０１、１０２と無線通信を行う。記憶領域部２０５は、システム内のそれぞれが使用するワーク領域およびテンポラリ領域で構成される揮発メモリと、装置の制御プログラムや、設定データ等を格納した不揮発メモリにより構成される。表示部２０６は、装置の初期化、データ設定およびメンテナンス等、システムの状態をＬＥＤ、ＬＣＤなどにより外部に通知する。なお、図２は、ＡＰ１０３の構成として説明したが、後述する無線端末７０２、１１０２、１１０３の構成も同様である。但し、無線端末７０２、１１０２、１１０３の場合は、スキャナ機能部、プリンタ機能部等、図示していない様々な構成も有することになる。

【００１３】

図３は、第１の実施形態の無線通信システムにおける処理のシーケンスチャートである。

【００１４】

図４は、ＩＥＥＥ８０２．１１ＭＡＣフレームのデータフォーマット４０１を説明したものである。

【００１５】

図４において、フレームデータ４１１は、ビーコン・フレームフォーマット４０２、プローブ応答フレームフォーマット４０３、およびプローブ要求フレームフォーマット４０４を示す。また、ＳＳＩＤ４１２は、ビーコン・フレーム構造４０２に含まれるＳＳＩＤ情報要素のフレーム４１０を示したものである。特に、ＳＳＩＤ４１２は、グループ識別子に関する情報を設定するエリアであり、ＥｌｅｍｅｎｔＩＤ４１３は、情報要素識別子示し、Ｌｅｎｇｔｈ４１４は、最大３２バイトのＳＳＩＤ４１５領域に設定されるＳＳＩＤデータの長さを表す。また、ＳＳＩＤ４１６は、プローブ応答フレーム構造４０３に含まれるＳＳＩＤ情報要素のフレーム４１０を示したものであり、ＳＳＩＤ４１７は、プローブ要求フレーム構造４０４に含まれるＳＳＩＤ情報要素のフレーム４１０を示したものである。

【００１６】

図５は、第１の実施形態の無線端末１０１、１０２における処理フローチャートである。

【００１７】

図６は、第１～第３の実施形態の無線アクセスポイント装置（ＡＰ）１０３、無線端末７０２、１１０２、１１０３における処理フローチャートである。

【００１８】

図７は、本発明の第２の実施形態に係る無線通信システム構成図である。

図７において、７０１は、無線機能を内蔵した無線端末である無線通信可能なデジタルカメラである。無線端末７０２は、無線端末７０１と、無線端末１０２等の無線端末とグループ識別子がＡＢＣ１２３であるアドホックネットワークを構成する。また、無線端末

７０２は、ＩＢＳＳクリエータとしてアドホックネットワーク固有のビーコン・フレーム情報を当該エリア内に報知する。

【００１９】

図８は、第２の実施形態の無線通信システムにおける処理のシーケンスチャートである。

【００２０】

図９は、第２の実施形態における無線端末７０１、１０２の処理フローチャートである。

【００２１】

図１０は、それぞれの実施形態におけるＡＰ１０３、無線端末７０２、１１０２、１１０３の記憶領域部２０５にある端末アクセス情報のテーブルである。

【００２２】

図１１は、第３の実施形態の無線通信システムにおける無線通信システムの構成図である。

図１１において、１１０１は、無線機能を内蔵した無線端末であり、無線通信可能なデジタルカメラである。

【００２３】

無線端末Ａ１１０２は、無線端末１１０１と同一の無線エリア内で使用される無線端末であり、ネットワークの構成については、アドホック、インフラストラクチャモードの何れも形成可能である。無線端末Ｂ１１０３は、無線デジタルカメラ１１０１と無線端末Ａ１１０２が使用される無線エリア内で起動され、無線端末Ａ１１０２と同等の機能を有する無線端末である。

【００２４】

図１２は、第３の実施形態の無線通信システムにおける処理のシーケンスチャートである。

また、上記各シーケンス図、フローチャート内のメッセージは、実施形態の説明に関する主なもののみを明記してあり、その他基本的なメッセージについては、一部省略してある。

【００２５】

（第１の実施形態）

以下、本発明の第１の実施形態における無線通信システムについて図１～図６、および図１０を用いて説明する。

【００２６】

図３の無線通信システムのシーケンスチャートにおいて、ＡＰ１０３が起動され、ビーコン信号（Ｍ３０１）が送信開始される。このとき、ビーコン信号（Ｍ３０１）のデータフレームにおけるＳＳＩＤ情報要素は、データレングス４１４が“０”でグループ識別子（ＳＳＩＤ）４１５にデータが未設定となっており、所謂、ステルス機能ＯＮの状態である。

【００２７】

このような状況下において、無線端末１０１が、ビーコン信号（Ｍ３０１）を検出すると（ステップＳ５０１：ＹＥＳ）、ビーコン信号内のグループ識別子を判別する（ステップＳ５０２）。グループ識別子（ＳＳＩＤ）４１５が存在しない場合（ステップＳ５０２：ＮＯ）、ステップＳ５０３に進む。ステップＳ５０３では、周辺の無線セルの有無を問い合わせ、接続収容可能なＡＰを発見し、無線端末１０１自身の登録を行うために、プローブ要求メッセージ（Ｍ３０２）をブロードキャストする。

【００２８】

このプローブ要求メッセージ（Ｍ３０２）には、予めＡＰ１０３との間で決められている登録要求の意味を示す特別な文字列等（例：ＳＳＩＤ＝‘ＲＥＧＲＥＱ’）を暗号化して含められている。詳細には、登録要求の意味を示す特別な文字列をグループ識別子（ＳＳＩＤ）４１５にコーディングする。そして、グループ識別子（ＳＳＩＤ）４１５のレン

グス４１４と共に、ＡＰ１０３との共有鍵で暗号化し、ＳＳＩＤ情報要素４１７として含められている。そして無線端末１０１は、プローブ要求メッセージ（Ｍ３０２）を送信すると、プローブ応答タイマーを起動する（ステップＳ５０３）。

【００２９】

ＡＰ１０３がプローブ要求メッセージ（Ｍ３０２）を受信すると（ステップＳ６０１）、当該メッセージ内のＳＳＩＤ情報要素４１７にあるグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を共に秘密鍵を用いて復号化する（ステップＳ６０２）。復号化されたグループ識別子（ＳＳＩＤ）４１５が、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧ－ＲＥＱ’）であることが確認された場合（ステップＳ６０３：ＹＥＳ）、ステップＳ６０７に進む。

【００３０】

そして、ＳＳＩＤ情報要素４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”以外の所定の値で、またグループ識別子情報４１５の領域に、所定のＳＳＩＤ情報（ＳＳＩＤ＝‘ＡＢＣ１２３’）を設定する。さらに、レングス４１４とグループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）情報４１５の領域を共有鍵で暗号化したＳＳＩＤ情報要素４１６を含めたプローブ応答メッセージ（Ｍ３０３）をユニキャスト形式で無線端末１０１に対して送信する（ステップＳ６０７）。引き続き、無線端末１０１の端末識別情報（ＭＡＣアドレス等）をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照し、対応する端末識別情報のアクセス回数１００２を更新する。また、接続チェック１００３をＯＫに設定する。

【００３１】

プローブ応答メッセージ（Ｍ３０３）を受信した（ステップＳ５０４：ＹＥＳ）無線端末１０１は、グループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５を確認し、グループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５をリスト表示する。つまり、ＡＰ１０３を接続可能な無線アクセスポイント装置としてリストアップする。

【００３２】

また、プローブ応答メッセージ（Ｍ３０３）を受信できない場合（ステップＳ５０４：ＮＯ）、無線端末１０１は、タイマー満了か否かを確認する。タイマー満了以前であれば、（ステップＳ５０５：ＮＯ）、再度、ＡＰ１０３からのプローブ応答メッセージ（Ｍ３０３）待ちの状態に遷移する（ステップＳ５０４）。タイマーが満了した場合（ステップＳ５０５：ＹＥＳ）、無線端末１０１は、新たなビーコン信号の検出状態に遷移する（ステップＳ５０１）。

【００３３】

グループ識別子をリスト表示した無線端末１０１は、ユーザーの選択操作（ステップＳ５０６：ＹＥＳ）によりＡＰ１０３への接続が選択されると、ＡＰ１０３に対して無線認証要求送信し、認証シーケンス処理（Ｍ３０４）を実施する（ステップＳ５０７）。無線認証要求を受信したＡＰ１０３は（ステップＳ６０８：ＹＥＳ）、無線端末１０１との間で認証シーケンス処理（Ｍ３０４）を実施し、引き続きアソシエーション処理を起動する（ステップＳ６０９）。

【００３４】

無線端末１０１は、認証シーケンス処理（Ｍ３０４）が完了すると（ステップＳ５０８：ＹＥＳ）、ＡＰ１０３との間でアソシエーション処理（Ｍ３０５）を実施する（ステップＳ５０９）。アソシエーション処理（Ｍ３０５）が完了すると（ステップＳ６１０：ＹＥＳ）、無線端末１０１とＡＰ１０３は、通信中状態へ遷移する。

【００３５】

また、ＡＰ装置１０３が、無線端末１０２より前記プローブ要求メッセージ（Ｍ３０６）を受信した場合（ステップＳ６０１：ＹＥＳ）、ステップＳ６０２に進む。ステップＳ６０２では、プローブ要求メッセージ（Ｍ３０２）内のＳＳＩＤ情報要素４１７にあるグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を検出する。また、それらを共に共有鍵を用いて復号化する（ステップＳ６０２）。復号化されたグループ識別子（ＳＳＩ

Ｄ）４１５が、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧ－ＲＥＱ’）がどうかを判定する（ステップＳ６０３）。登録要求の意味を示す文字列であることが確認されない場合（ステップＳ６０３：ＮＯ）、無線端末１０２の端末識別情報（ＭＡＣアドレス等）１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照し、アクセス回数１００２を更新する。また、接続チェック１００３をＮＧに設定する。また、ＳＳＩＤ４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”でグループ識別子情報４１５にデータが未設定のプローブ応答メッセージ（Ｍ３０７）をユニキャスト形式で無線端末１０２に対して送信する（ステップＳ６０４）。

【００３６】

プローブ応答メッセージ（Ｍ３０７）を受信した無線端末１０２は、グループ識別子情報４１５を確認し、存在しない場合、グループ識別子情報４１５をリスト表示する。この場合、グループ識別子情報４１５は未設定なので、図３に示すように「？？？？」とリスト表示する。従って、無線端末１０２では、ＡＰ１０３は、接続不可のためユーザーは選択できない。

【００３７】

ＡＰ１０３は、無線端末１０２に対してプローブ応答メッセージ（Ｍ３０７）を送信した後、無線端末１０２からのアクセス回数１００２を確認する（ステップＳ６０５）。その結果、規定回数（例：１６回）を超えない場合（ステップＳ６０５：ＮＯ）には、無線端末からのプローブ要求メッセージ受信状態（ステップＳ６０１）に遷移する。

【００３８】

一方、規定回数（例：１６回）を超えた場合（ステップＳ６０５：ＹＥＳ）には、記憶領域部２０５にある端末アクセス情報テーブルを参照する。そして、無線端末１０２の端末識別情報（ＭＡＣアドレス等）１００１をＭＡＣアドレスフィルターに登録し、ＭＡＣレベルでの端末アクセス制御処理を実施する（ステップＳ６０６）。

【００３９】

（第２の実施形態）

以下、本発明の第２の実施形態における無線通信システムについて図６～図１０を用いて説明する。

【００４０】

図８において、当該エリア内においては、複数のＡＰ１０３が起動しており、これらは、起動と同時にビーコン信号（Ｍ８００）を報知している。このビーコン信号（Ｍ８００）は、データフレームにおけるＳＳＩＤ４１２であるＳＳＩＤ情報要素フレーム４０４のデータレングス４１４が“０”以外で情報４１５の領域であるグループ識別子に所定のＳＳＩＤ情報（ＳＳＩＤ＝ＤＥＦ５６８）が設定されている。即ち、所謂、ステルス機能ＯＦＦの状態である。

【００４１】

このとき、無線端末１０２や無線端末（デジタルカメラ）７０１は、複数のＡＰ１０３のビーコン信号（Ｍ８００）を検出する（ステップＳ９０１：ＹＥＳ）。そして、グループ識別子（ＳＳＩＤ）４１５が存在するかどうかを判定する（ステップＳ９０２）。グループ識別子（ＳＳＩＤ）４１５が存在する場合（ステップＳ９０２：ＹＥＳ）、複数のＡＰ１０３を、接続選択可能な無線アクセスポイント装置としてリストアップし表示する（ステップＳ９０６）。引き続き、エリア内で、グループ識別子（ＳＳＩＤ）４１５が存在するビーコン信号（Ｍ８００）を報知しているその他のＡＰを探索する。上記のごとく更にＳＳＩＤ情報を含む他のビーコンが検出された場合（ステップＳ９０７：ＮＯ）、ビーコン信号におけるＳＳＩＤ情報の確認処理（ステップＳ９０１、Ｓ９０２、Ｓ９０６、Ｓ９０７）を繰り返す。

【００４２】

このような状況下において、ＡＰ１０３とは異なる、無線端末７０２は、ＩＢＳＳクリエータとしてビーコンインターバルを決定し、複数の無線端末との間でデータを送受信す

るための同期を確立している。このビーコンインターバルの開始、すなわちビーコン送信タイミングから始まる一定の期間をＡＴＩＭウインドウと呼ぶ。ＩＢＳＳでは、ＰＳ（パワーセーブ：省電力）モードの端末にデータフレームを送信するためにＡＴＩＭ（Ａｎｎｏｕｎｃｅｍｅｎｔ Ｔｒａｆｆｉｃ Ｉｎｄｉｃａｔｉｏｎ Ｍｅｓｓａｇｅ）フレームを使用して、事前にデータ送信を予告する。ＡＴＩＭは、ＡＴＩＭ Ｗｉｎｄｏｗという特別な期間に送信される。ＡＴＩＭ Ｗｉｎｄｏｗ期間中は、ビーコンあるいは、ＡＴＩＭのみ送信が許されており、ＰＳモードの無線デジタルカメラ７０１は、送受信可能な（Ａｗａｋｅ）状態となっている。

【００４３】

ＩＢＳＳクリエータである無線端末７０２は、ビーコン信号（Ｍ８０１）送信中状態である。このビーコン信号（Ｍ８０１）のデータフレームにおけるＳＳＩＤ情報要素は、データレングス４１４が“０”でグループ識別子（ＳＳＩＤ）４１５にデータが未設定となっている。所謂、ステルス機能ＯＮの状態である。このとき、無線端末７０１が、ビーコン信号（Ｍ８０１）を検出し（ステップＳ９０１：ＹＥＳ）、グループ識別子（ＳＳＩＤ）４１５が存在しない場合（ステップＳ９０２：ＮＯ）、ステップＳ９０３に進む。

【００４４】

ステップＳ９０３では、周辺の無線セルの有無を問い合わせ、接続収容可能なＡＰまたは無線端末を発見し、無線端末７０１自身の登録を行うために、プローブ要求メッセージ（Ｍ８０２）をブロードキャストする。当該メッセージ（Ｍ８０２）には、予め無線端末装置７０２との間で決められている登録要求の意味を示す特別な文字列（ＲＥＧＲＥＱ）等と無線端末７０１の端末識別情報（１Ｅ－ＦＦ－ＥＥ：ＭＡＣアドレスの下３バイト等）を暗号化して含められている。詳細には、登録要求の意味を示す特別な文字列と無線端末７０１の端末識別情報をグループ識別子（例：ＳＳＩＤ＝‘ＲＥＧＲＥＱ １Ｅ－ＦＦ－ＥＥ’）４１５にコーディングする。そして、レングス４１４と共に無線端末７０２の所有する秘密鍵に対応した公開鍵で暗号化し、ＳＳＩＤ情報要素４１７として含められている。そして、無線端末７０１は、プローブ要求メッセージ（Ｍ８０２）をブロードキャストすると、プローブ応答タイマーを起動する（ステップＳ９０３）。

【００４５】

無線端末７０２が、プローブ要求メッセージ（Ｍ８０２）を受信すると（ステップＳ６０１：ＹＥ）、ステップＳ６０２に進む。ステップＳ６０２では、プローブ要求メッセージ（Ｍ８０２）内のＳＳＩＤ情報要素４１７にあるグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を共に秘密鍵を用いて復号化する（ステップＳ６０２）。

【００４６】

そして、復号化されたグループ識別子（ＳＳＩＤ）４１５が、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧＲＥＱ’）であるかどうかを確認する。登録要求の意味を示す文字列であることが確認された場合、付随する無線端末７０１の端末識別情報（１Ｅ－ＦＦ－ＥＥ：ＭＡＣアドレスの下３バイト等）とマネージメントフレーム４０１にあるＭＡＣアドレスを比較する。

【００４７】

一致した場合、無線端末７０１からの正しい登録要求を示すプローブ要求メッセージ（Ｍ８０２）と判断する（ステップＳ６０３）。ステップＳ６０７では、ＳＳＩＤ情報要素４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”以外の所定の値で、またグループ識別子情報４１５の領域に所定のＳＳＩＤ情報（ＳＳＩＤ＝‘ＡＢＣ１２３’）を設定する。そして、レングス４１４とグループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）情報４１５の領域を共有鍵で暗号化したＳＳＩＤ情報要素４１６を含めたプローブ応答メッセージ（Ｍ８０３）をユニキャスト形式で無線端末７０１に送信する（ステップＳ６０７）。

【００４８】

引き続き、無線端末７０１の端末識別情報（ＭＡＣアドレス等）１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照し、アクセス回数１００２を更新

する。また、接続チェック１００３をＯＫに設定する。

【００４９】

プローブ応答メッセージ（Ｍ８０３）を受信した無線端末７０１は（ステップＳ９０４：ＹＥＳ）、グループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５を確認する（ステップＳ９０２）。そして、無線端末７０２に対応するグループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５を他の無線アクセスポイント装置と異なる形でリスト表示する（図８参照）。

【００５０】

ここでは、ビーコン信号内のＳＳＩＤ情報の確認処理（ステップＳ９０１、Ｓ９０２、Ｓ９０７）により検出した無線アクセスポイント装置に対応するＳＳＩＤ情報（ＤＥＦ５６８等）とは異なる形で、グループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）を表示する。即ち、無線端末７０２を接続可能な無線端末としてリストアップする（ステップＳ９０６）。エリア内のすべてのビーコン信号に対する検出処理が終了するまでビーコン信号におけるＳＳＩＤ情報の確認処理（ステップＳ９０１、Ｓ９０２、Ｓ９０６、Ｓ９０７）を実施する。

【００５１】

一方、エリア内のすべてのビーコン信号に対する検出処理が終了した場合（ステップＳ９０７：ＹＥＳ）、ユーザーによる接続選択操作待ち状態に遷移する。

【００５２】

また、プローブ応答メッセージ（Ｍ８０３）を受信できない場合（ステップＳ９０４：ＮＯ）、無線端末７０１は、タイマー満了か否かを確認する（ステップＳ９０５）。タイマー満了以前であれば、（ステップＳ９０５：ＮＯ）、再度、無線端末７０２からのプローブ応答メッセージ（Ｍ８０３）待ちの状態に遷移する（ステップＳ９０４）。タイマーが満了した場合（ステップＳ９０５：ＹＥＳ）、無線端末７０１は、新たなビーコン信号の検出状態に遷移する（ステップＳ９０１）。

【００５３】

グループ識別子をリスト表示した無線端末７０１は、ユーザーの選択操作により無線端末７０２への接続が選択されると（ステップＳ９０８）、無線端末７０２に対して無線認証要求送信し、認証シーケンス処理（Ｍ８０４）を実施する（ステップＳ９０９）。無線認証要求を受信した無線端末７０２は（ステップＳ６０８：ＹＥＳ）、無線端末７０１との間で認証シーケンス処理（Ｍ８０４）を実施し、引き続きアソシエーション処理を起動する（ステップＳ６０９）。

【００５４】

無線端末７０１は、認証シーケンス処理（Ｍ８０４）が完了すると（ステップＳ９１０：ＹＥＳ）、無線端末７０２との間でアソシエーション処理（Ｍ８０５）を実施する（ステップＳ９１１）。アソシエーション処理（Ｍ８０５）が完了すると（ステップＳ６１０：ＹＥＳ）、無線端末７０１と無線端末装置７０２は、通信中状態へ遷移する。

【００５５】

また、無線端末７０２が、無線端末１０２よりプローブ要求メッセージ（Ｍ８０６）を受信した場合（ステップＳ６０１：ＹＥＳ）、ステップＳ６０２に進む。ステップＳ６０２では、プローブ要求メッセージ（Ｍ８０２）内のＳＳＩＤ情報要素４１７にあるグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を共に共有鍵を用いて復号化する（ステップＳ６０２）。そして、復号化されたグループ識別子（ＳＳＩＤ）４１５が、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧ－ＲＥＱ’）であるかどうかを確認する（ステップＳ６０３）。

【００５６】

特別な文字列であることが確認されない場合、または、端末識別情報が異なるなど成りすまし等の危険性が疑われる場合（ステップＳ６０３：ＮＯ）、ステップＳ６０４に進む。ステップＳ６０４では、無線端末１０２の端末識別情報（ＭＡＣアドレス等）１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照し、アクセス回数１００２を更新する。また、接続チェック１００３をＮＧに設定する。また、ＳＳＩＤ４１

６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”でグループ識別子（ＳＳＩＤ）情報４１５が未設定のプローブ応答メッセージ（Ｍ８０７）をユニキャスト形式で無線端末１０２に送信する（ステップＳ６０４）。

【００５７】

プローブ応答メッセージ（Ｍ８０７）を受信した無線端末１０２は、グループ識別子（ＳＳＩＤ）４１５を確認し、存在しない場合、グループ識別子情報４１５をリスト表示する。この場合、グループ識別子情報４１５は未設定なので、図８に示すように「？？？？」とリスト表示する。従って、無線端末１０２では無線端末７０２は、接続不可のためユーザーは選択できない。

【００５８】

また、無線端末７０２は、無線端末１０２に対してプローブ応答メッセージ（Ｍ８０７）を送信した後、無線端末１０２からのアクセス回数１００２を確認する（ステップＳ６０５）。その結果、規定回数（例：１６回）を超えない場合（ステップＳ６０５：ＮＯ）には、無線端末からのプローブ要求メッセージ受信状態に遷移する（ステップＳ６０１）。

【００５９】

一方、規定回数（例：１６回）を超えた場合（ステップＳ６０５：ＹＥＳ）には、記憶領域部２０５にある端末アクセス情報テーブルを参照する。そして、無線端末１０２の端末識別情報（ＭＡＣアドレス等）１００１をＭＡＣアドレスフィルターに登録し、ＭＡＣレベルでの端末アクセス制御処理を実施する。（ステップＳ６０６）

（第３の実施形態）

以下、本発明の第３の実施形態における無線通信システムについて図１０～図１２を用いて説明する。図１１において、無線端末１１０１の当該エリア内において、無線端末Ａ１１０２が自宅内で起動している。更に隣家では無線端末Ａ１１０２と同等の機能を有する無線端末Ｂ１１０３が起動している。これらは、起動と同時にビーコン信号（Ｍ１２００、Ｍ１２０１）を報知している（図１２）。

【００６０】

このビーコン信号（Ｍ１２００、Ｍ１２０１）は、データフレームにおけるＳＳＩＤ４１２であるＳＳＩＤ情報要素フレーム４０４のデータレングス４１４が“０”でグループ識別子（ＳＳＩＤ）４１５にデータが未設定となっている。所謂、ステルス機能ＯＮの状態である。このような状況のもと、無線端末１１０１を同一宅内の無線端末Ａ１１０２に登録する際、無線端末Ａ１１０２の製造番号下４桁（１２３４）を無線端末１１０１に登録する。

【００６１】

無線端末１１０１が、ビーコン信号（Ｍ１２００、１２０１）の何れかを検出した場合、グループ識別子（ＳＳＩＤ）４１５の存在を確認する。グループ識別子（ＳＳＩＤ）４１５が存在しない場合、無線端末Ａ１１０２に対して無線端末１１０１自身の登録を行うために、プローブ要求メッセージ（Ｍ１２０２）をブロードキャストする。当該メッセージ（Ｍ１２０２）には、予め無線端末Ａ１１０２との間で決められている登録要求の意味を示す特別な文字列等と無線端末１１０１の端末識別情報と予め登録しておいた無線端末Ａ１１０２の製造番号下４桁を暗号化して含められている。詳細には、文字列をＲＥＧＲＥＱ、端末識別情報を１Ｅ－ＦＦ－ＢＢ：ＭＡＣアドレスの下３バイト、製造番号の下４桁を１２３４とし、これらの情報をグループ識別子（例：ＳＳＩＤ＝‘ＲＥＧＲＥＱ　１Ｅ－ＦＦ－ＢＢ－１２３４’）４１５にコーディングする。そして、レングス４１４と共に無線端末Ａ１１０２の所有する秘密鍵に対応した公開鍵で暗号化し、ＳＳＩＤ情報要素４１７として含められている。そして、無線端末１１０１は、プローブ応答タイマーを起動する。

【００６２】

無線端末Ａ１１０２が、プローブ要求メッセージ（Ｍ１２０２）を受信すると（ステップＳ６０１）、ステップＳ６０２に進む。ステップＳ６０２では、プローブ要求メッセー

ジ（Ｍ１２０２）内のＳＳＩＤ情報要素４１７にあるグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を共に秘密鍵を用いて復号化する。

【００６３】

そして、復号化されたグループ識別子（ＳＳＩＤ）４１５が、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧＲＥＱ’）であるかどうかを判定する。登録要求の意味を示す特別な文字列であることが確認された場合、付随する無線端末１１０１の端末識別情報（１Ｅ－ＦＦ－ＢＢ：ＭＡＣアドレスの下３バイト等）とマネージメントフレーム４０１にあるＭＡＣアドレスを比較する。一致した場合には、付随している４桁の数字を無線端末Ａ１１０２の製造番号下４桁と比較し、合致しているかどうかも判定する。合致していた場合には、無線端末１１０１から無線端末Ａ１１０２に対する正しい登録要求を示すプローブ要求メッセージ（Ｍ１２０２）と判断する（ステップＳ６０３）。そして、ＳＳＩＤ情報要素４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”以外の所定の値で、またグループ識別子情報４１５の領域に所定のＳＳＩＤ情報（ＳＳＩＤ＝‘ＡＢＣ１２３’）を設定する。そして、レングス４１４と共に共有鍵で暗号化したＳＳＩＤ情報要素４１６を含めたプローブ応答メッセージ（Ｍ１２０３）をユニキャスト形式で無線端末１１０１に対して送信する（ステップＳ６０７）。

【００６４】

引き続き、無線端末１１０１の端末識別情報（ＭＡＣアドレス等）１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照し、アクセス回数１００２を更新する。また、接続チェック１００３をＯＫに設定する。プローブ応答メッセージ（Ｍ１２０３）を受信した無線端末１１０１は、グループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５を確認し、無線端末Ａ１１０２に対応するグループ識別子（ＳＳＩＤ＝ＡＢＣ１２３）４１５をリスト表示する。即ち、無線端末Ａ１１０２を接続可能な無線端末としてリストアップする。

【００６５】

また、無線端末Ａ１１０２は、受信したプローブ要求メッセージ（Ｍ１２０２）において上記特定の文字列が確認されない場合は、誤った登録要求を示すプローブ要求メッセージ（Ｍ１２０２）と判断し、上述したステップＳ６０４以降の処理を行う。また、無線端末１１０１の端末識別情報とマネージメントフレーム４０１のＭＡＣアドレスと一致しない場合、無線端末Ａ１１０２の製造番号下４桁が合致しない場合にも、上述したステップＳ６０４以降の処理を行う。

【００６６】

その後、無線端末１１０１におけるユーザーの選択操作により、無線端末Ａ１１０２への接続が選択されると、無線端末１１０１は、無線端末Ａ１１０２に対して無線認証要求送信し、認証シーケンス処理（Ｍ１２０４）を実施する。無線認証要求を受信した無線端末Ａ１１０２は、無線端末１１０１との間で認証シーケンス処理（Ｍ１２０４）を実施し、引き続きアソシエーション処理を起動する（ステップＳ６０８、６０９）。

【００６７】

無線端末１１０１と無線端末Ａ１１０２は、認証シーケンス処理（Ｍ１２０４）が完了すると、無線端末Ａ１１０２との間でアソシエーション処理（Ｍ１２０５）を実施する。アソシエーション処理（Ｍ１２０５）が完了すると、無線端末１１０１と無線端末Ａ１１０２は、通信中状態へ遷移する（ステップＳ６１０）。

【００６８】

また、無線端末Ｂ１１０３が無線端末１１０１よりプローブ要求メッセージ（Ｍ１２０２）を受信すると（ステップＳ６０１）、ステップＳ６０２に進む。ステップＳ６０２では、当該メッセージ内のグループ識別子（ＳＳＩＤ）４１５とそのレングス４１４を共に共有鍵を用いて復号化する。

【００６９】

そして、復号化されたグループ識別子（ＳＳＩＤ）４１５が、正しい登録要求を示すプ

ローブ要求メッセージかどうかを判別する（ステップＳ６０３）。即ち、記憶領域部２０５にある登録要求の意味を示す特別な文字列等（例：‘ＲＥＧ－ＲＥＱ’）であるかどうか、端末識別情報が異なるかどうか、４桁の情報が自身の製造番号と異なるかどうかを判別する。上記特別な文字列であることが確認されない場合、無線端末１１０１の端末識別情報（ＭＡＣアドレス等）１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照する。同様に、端末識別情報が異なり成りすましの危険性がある場合、また、４桁の情報が自身の製造番号と異なる場合にも、無線端末１１０１の端末識別情報１００１をもとに、記憶領域部２０５にある端末アクセス情報テーブルを参照する。そして、アクセス回数１００２を更新する。また、接続チェック１００３をＮＧに設定する。更に、ＳＳＩＤ４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”でグループ識別子（ＳＳＩＤ）情報４１５が未設定のプローブ応答メッセージ（Ｍ１２０４）をユニキャストで無線端末１１０１に送信する（ステップＳ６０７）。

【００７０】

プローブ応答メッセージ（Ｍ１２０４）を受信した無線端末１１０１は、グループ識別子（ＳＳＩＤ）４１５を確認する。グループ識別子（ＳＳＩＤ）４１５が存在しない場合、グループ識別子（ＳＳＩＤ）４１５をリスト表示する。この場合、グループ識別子情報４１５は未設定なので、図１２に示すように「？？？？」とリスト表示する。

【００７１】

また、無線デジタルカメラ１１０１からのアクセス回数１００２を確認し（ステップＳ６０５）、規定回数（例：１６回）を超えない場合には、無線端末からのプローブ要求メッセージ受信状態に遷移する。一方、規定回数を超えた場合には、記憶領域部２０５にある端末アクセス情報テーブルを参照する。そして、無線デジタルカメラ１１０１の端末識別情報（ＭＡＣアドレス等）１００１をＭＡＣアドレスフィルターに登録し、ＭＡＣレベルでの端末アクセス制御処理を実施する（ステップＳ６０６）。

【００７２】

なお、上記各実施形態におけるプローブ要求メッセージ及び／あるいはプローブ応答メッセージは、公開鍵で暗号化し、秘密鍵で復号化しても、秘密鍵で暗号化し、公開鍵で復号化するようにしても、本発明は同様に実現される。

【００７３】

また、図６のステップＳ６０４において、ＳＳＩＤ４１６であるＳＳＩＤ情報要素フレーム４１０のデータレングス４１４が“０”でグループ識別子（ＳＳＩＤ）情報４１５が未設定のプローブ応答メッセージをユニキャスト形式で送信した。しかし、ステップＳ６０４では、プローブ応答メッセージを送信しないようにしてもよい。この場合、プローブ要求メッセージを送信した無線端末では、プローブ応答メッセージを受信しないことになる。その結果、無線端末では、プローブ応答メッセージを送信した機器のみを接続可能なＡＰまたは無線端末として表示するようにする。

【００７４】

また、無線端末は、データレングス４１４が“０”でグループ識別子（ＳＳＩＤ）情報４１５が未設定のプローブ応答メッセージを受信した場合には、プローブ応答メッセージの送信元の機器を表示しないようにしてもよい。

【００７５】

また、図６のステップＳ６０３の判断を、他の情報に基づいて行うようにしてもよい。例えば、運用中のグループ識別子（ＳＳＩＤ）と合致するか否かにより、正しい接続要求がどうかを判断してもよい。具体的には、図３のＡＰ１０３がプローブ要求メッセージを受信した場合には、当該メッセージに含まれているグループ識別子がＡＢＣ１２３の場合に正しい接続要求と判断する。それ以外のグループ識別子が含まれていた場合には、正しい接続要求ではないと判断する。

【００７６】

なお、上記実施の形態においてはＩＥＥＥ８０２．１１に準拠する無線ＬＡＮのネットワークを一例として説明したが、他の無線方式のネットワークにおいても本発明は実施す

ることができる。また、無線通信に限らず、有線ネットワークであってもよい。その他、本発明はその要旨を逸脱しない範囲内で種々変形して実施することが可能である。

【００７７】

以上のように上記説明によれば、無線端末を操作するユーザーに対して、予めグループ識別子（ＳＳＩＤ）を通知する手順が省略され、情報の漏洩という問題は解決され、セキュリティが向上する。

【００７８】

また、管理者により一旦、ステルス機能を解除することも不要となる。また、接続可能な無線端末においては、接続許可された（応答を返信した）アクセスポイントの一覧から所望のアクセスポイントをユーザーが適宜選択して接続することが可能となり管理者および無線端末ユーザーにおける煩雑な操作が解消され、利便性が向上する。

【００７９】

また、異なる無線端末が、隣接した環境で同時に接続設定を実施しても、所望の無線端末からの接続要求を識別可能となり、誤接続の発生を軽減できる。

【００８０】

さらに、グループ識別子に関する情報の漏洩、無線端末の接続収容時のステルス機能の一時的な解除（ＯＦＦ）、登録モード等の特殊状態への遷移によるシステム運用の一時的な停止等を回避し、アクセス希望者への柔軟な接続制御を実現できる。

【００８１】

以上のことから、無線通信システムへのイージーアクセス（ユーザーによる接続操作等の軽減）とセキュリティの両立といった効果が期待できる。

【図面の簡単な説明】

【００８２】

【図１】第１の実施形態における無線通信システムの構成図

【図２】無線アクセスポイント及び無線端末の内部構成図

【図３】第１の実施形態の無線通信システムにおける処理のシーケンスチャート

【図４】ＩＥＥＥ８０２．１１ＭＡＣフレームのデータフォーマット

【図５】第１の実施形態の無線端末１０１、１０２における処理フローチャート

【図６】第１～第３の実施形態の無線アクセスポイント装置（ＡＰ）１０３、無線端末７０２、１１０２、１１０３における処理フローチャート

【図７】第２の実施形態に係る無線通信システム構成図

【図８】第２の実施形態の無線通信システムにおける処理のシーケンスチャート

【図９】第２の実施形態における無線端末７０１、１０２の処理フローチャート

【図１０】各実施形態におけるＡＰ１０３、無線端末７０２、１１０２、１１０３の記憶領域部２０５にある端末アクセス情報のテーブル

【図１１】第３の実施形態の無線通信システムにおける無線通信システムの構成図

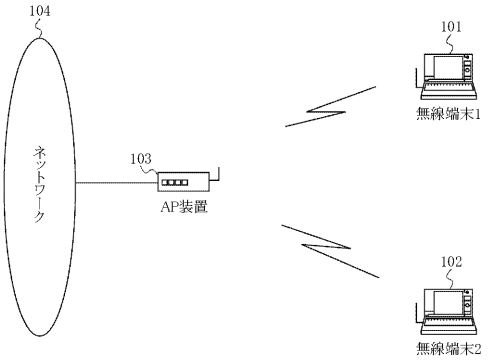
【図１２】第３の実施形態の無線通信システムにおける処理のシーケンスチャート

【符号の説明】

【００８３】

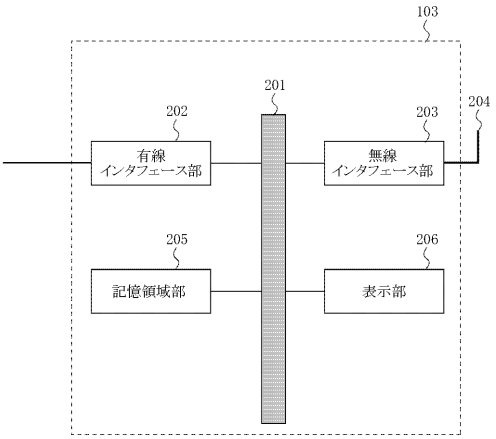
１０１　無線端末
１０２　無線端末
１０３　無線アクセスポイント装置
１０４　ネットワーク
Ｍ３０１　ビーコン
Ｍ３０２　プローブ要求メッセージ
Ｍ３０３　プローブ応答メッセージ
Ｍ３０４　無線認証手順
Ｍ３０５　アソシエーション手順
Ｍ３０６　プローブ要求メッセージ
Ｍ３０７　プローブ応答メッセージ

【図１】

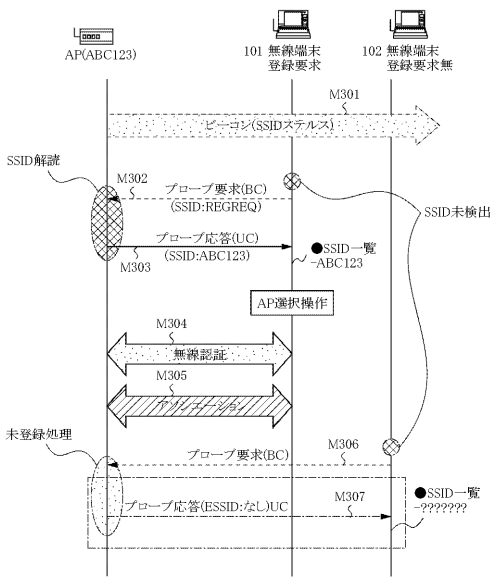


第1の実施の形態における無線通信システムの構成図

【図２】

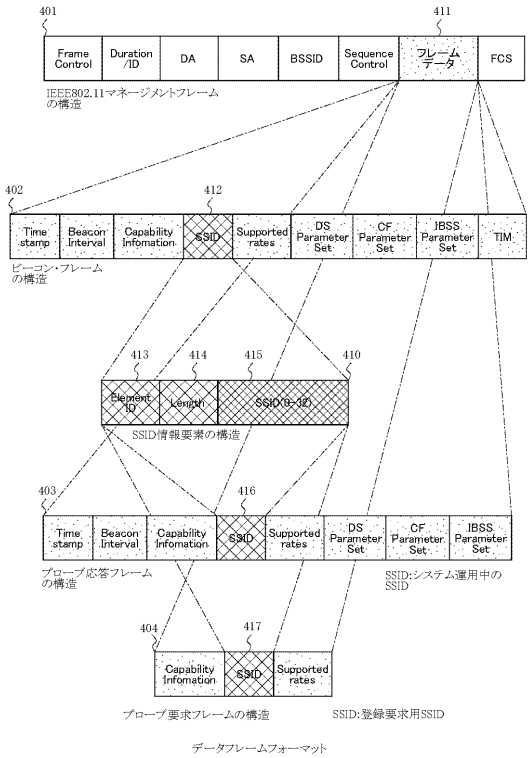


【図３】



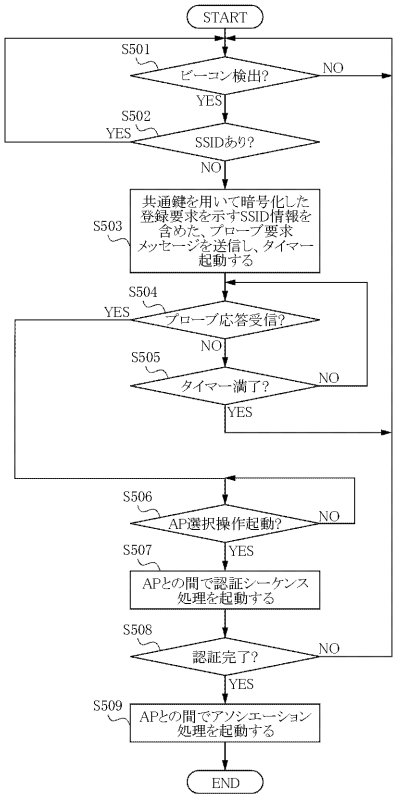
実施例1における処理のシーケンスチャート

【図４】

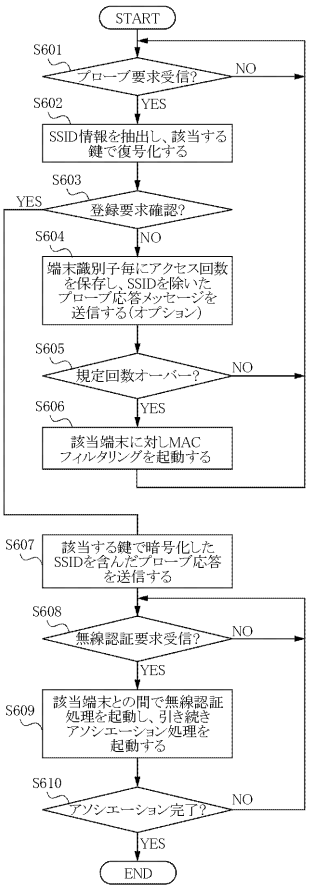


データフレームフォーマット

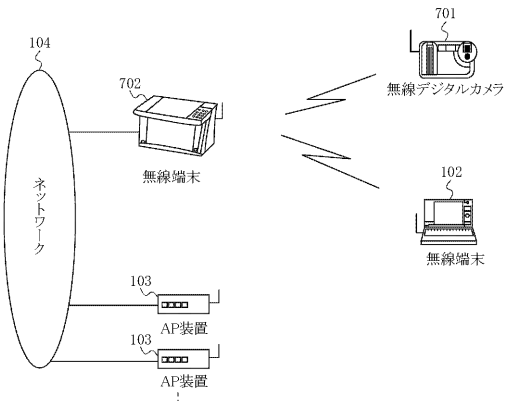
【図５】



【図６】

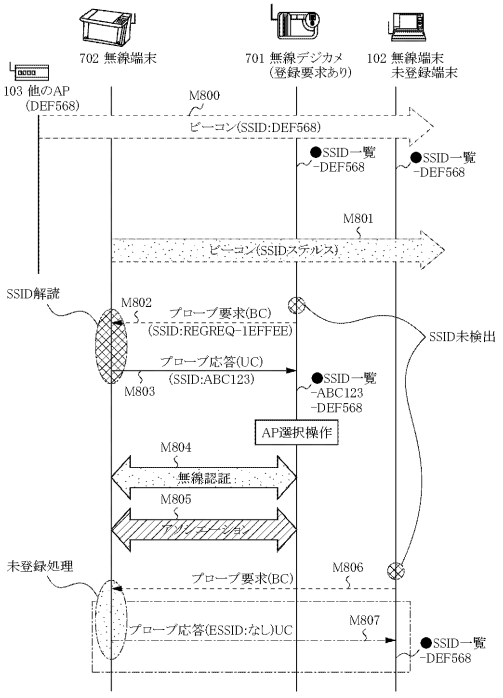


【図７】



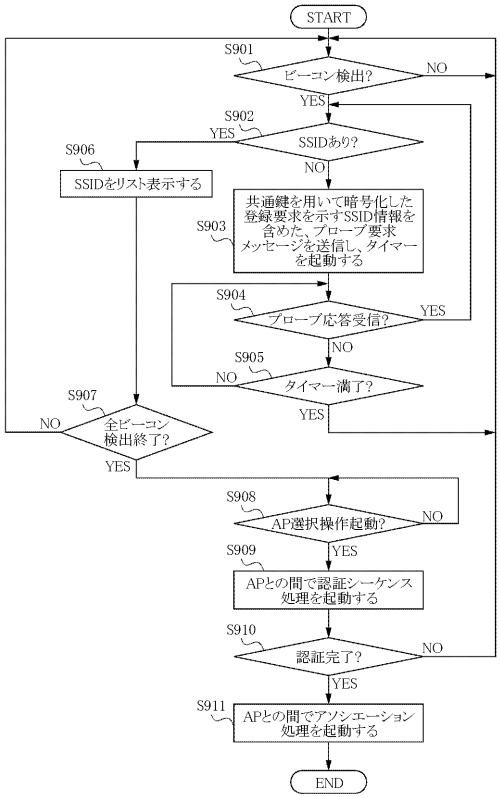
第2の実施の形態における無線通信システムの構成図

【図８】



実施例2における処理のシーケンスチャート

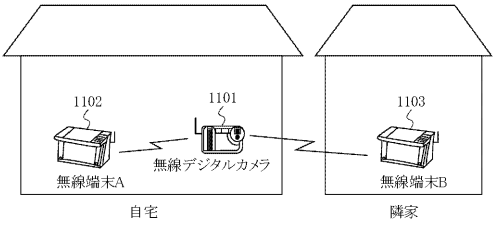
【図９】



【図１０】

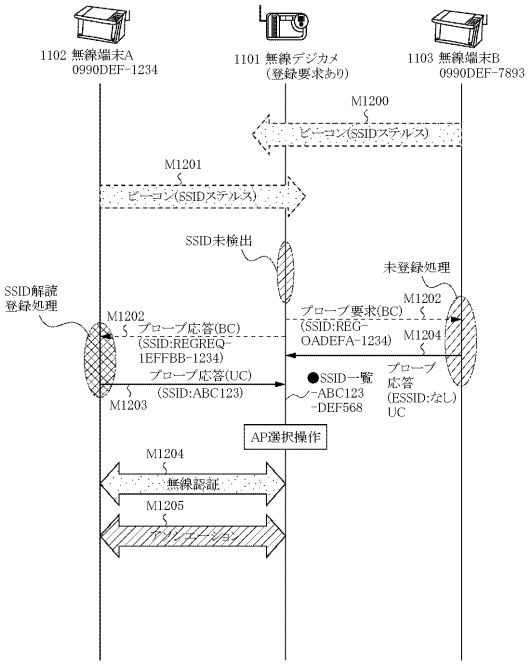
1001 アクセス端末MACアドレス	1002 回数	1003 接続チェック
00:02:2D:1E:FF:AA	4	■OK □NG
00:02:2D:1E:FF:BB	2	■OK □NG
00:02:2D:1E:FF:CC	16	□OK ■NG
00:02:2D:1E:FF:DD	16	□OK ■NG
00:02:2D:1E:FF:EE	1	■OK □NG
00:02:2D:1E:FF:FF	1	■OK □NG

【図１１】



第3の実施の形態における無線通信システムの構成図

【図１２】



実施例3における処理のシーケンスチャート

フロントページの続き

(56)参考文献 特開２００４－３６３８７８（ＪＰ，Ａ）
特開２００５－２５２８１２（ＪＰ，Ａ）
特開２００６－２２９７７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　８４／１２
Ｈ０４Ｗ　８８／０８
Ｈ０４Ｌ　１２／２８－４６