(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-66001
(P2013-66001A)
(43)公開日　平成25年4月11日(2013.4.11)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 40/22	(2009.01)	H04Q	7/00	354	5K067
H04W 84/20	(2009.01)	H04Q	7/00	635	
H04W 12/06	(2009.01)	H04Q	7/00	183	
H04W 84/12	(2009.01)	H04Q	7/00	630	

審査請求 未請求　請求項の数 5　ＯＬ　（全 14 頁）

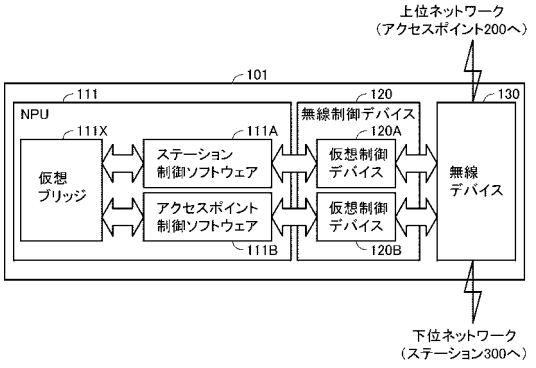
(21)出願番号　特願2011-202712 (P2011-202712)
(22)出願日　平成23年9月16日 (2011.9.16)

(71)出願人　591275481
株式会社アイ・オー・データ機器
石川県金沢市桜田町３丁目１０番地
(74)代理人　110000844
特許業務法人　クレイア特許事務所
(72)発明者　田畑　敬司
石川県金沢市桜田町３丁目１０番地
株式会社アイ・オー・データ機器内

Ｆターム(参考)　5K067 AA30　EE02　EE06　EE10

(54)【発明の名称】無線通信装置

(57)【要約】　（修正有）
【課題】無線通信におけるアクセスポイント間のセキュリティを低下させることなくアクセスポイント同士の接続を容易にする。
【解決手段】無線通信装置１０１は、少なくとも１つの無線通信デバイス１３０と、少なくとも１つの無線通信デバイスを利用することによって、アクセスポイント２００に対しては自身がステーションとして無線通信を行い、ステーション３００に対しては自身がアクセスポイントとして無線通信を行うためのプロセッサ（ＮＰＵ）１１１とを備える。
【選択図】図３



【特許請求の範囲】
【請求項１】
ネットワークの上位のアクセスポイントと下位のステーションと通信するための無線通信装置であって、
少なくとも１つの無線通信デバイスと、
前記少なくとも１つの無線通信デバイスを利用することによって、前記アクセスポイントに対しては自身がステーションとして無線通信を行い、前記ステーションに対しては自身がアクセスポイントとして無線通信を行うためのプロセッサとを備える、無線通信装置。
【請求項２】
前記プロセッサは、
前記アクセスポイントに対して、前記少なくとも１つの無線通信デバイスを介して、自身がステーションとして無線通信を行うためのステーション部と、
前記ステーションに対して、前記少なくとも１つの無線通信デバイスを介して、自身がアクセスポイントとして無線通信を行うためのアクセスポイント部と、
前記ステーション部と前記アクセスポイント部との間でデータを転送するための仮想ブリッジ部とを含む、請求項１に記載の無線通信装置。
【請求項３】
前記仮想ブリッジ部は、
前記ステーション部を介して前記アクセスポイントから受信したデータを前記アクセスポイント部を介して前記ステーションへと転送し、
前記アクセスポイント部を介して前記ステーションから受信したデータを前記ステーション部を介して前記アクセスポイントへと転送する、請求項２に記載の無線通信装置。
【請求項４】
前記仮想ブリッジ部は、前記アクセスポイントが認証サーバに接続されている場合に、前記アクセスポイント部および前記少なくとも１つの無線通信デバイスを介して前記認証サーバに対して前記ステーションからの認証の代理送信を実行する、請求項２または３に記載の無線通信装置。
【請求項５】
前記少なくとも１つの無線通信デバイスは、第１の無線通信デバイスと第２の無線通信デバイスとを含み、
前記ステーション部は、前記第１の無線通信デバイスを介して前記アクセスポイントと無線通信を行い、
前記アクセスポイント部は、前記第２の無線通信デバイスを介して前記ステーションと無線通信を行う、請求項２から４のいずれか１項に記載の無線通信装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線ＬＡＮ（Local Area Network）を構成する無線通信装置に関し、特に他のアクセスポイントやステーションとの間でデータを送受信する無線通信装置に関する。
【背景技術】
【０００２】
無線通信を利用して機器同士がデータの送受信を行う無線ＬＡＮシステムが知られている。そして、無線ＬＡＮシステムで使用されるモードとしては、たとえば、インフラストラクチャモードと、ＷＤＳ（Wireless Distribution System）モードなどが挙げられる。
【０００３】
特開２００９－３０３１７０号公報（特許文献１）には、無線通信システム、無線ＬＡＮ接続装置、無線ＬＡＮ中継装置が開示されている。特開２００９－３０３１７０号公報

（特許文献１）によると、無線通信システムは接続装置と中継装置とを備える。無線通信システムは、中継装置からの要求に基づくインフラモードの認証を経て中継装置を接続装置に接続し、端末装置と接続装置との間でやり取りされるデータを、ＷＤＳモードのデータフレームを用いて転送する。

【０００４】

また、特表２００７－５２７１５６号公報（特許文献２）には、通信装置用汎用クライアントが開示されている。特表２００７－５２７１５６号公報（特許文献２）によると、汎用クライアント（ＧＣ）は、異なるネットワークに同時に通信する多数の仮想ネットワークインタフェイスを動作させる。各仮想インタフェイスは、同一の物理インタフェイスを介して関連ネットワークを通して独立して通信を行うことができる。一実施例においては、ＧＣは、ＩＥＥＥ８０２．１１プロトコルに準拠してインフラストラクチャおよびアドホックネットワークの双方との同時通信を提供する。ＧＣは、異なるインフラストラクチャおよびアドホック仮想インタフェイスをインスタンス化することにより、これら２つの動作モードを提供する。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００９－３０３１７０号公報

【特許文献２】特表２００７－５２７１５６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、ＷＤＳは国際標準化されていないため、異なるメーカの無線ＬＡＮ親機（アクセスポイント）同士に互換性がない可能性が高い。すなわち、異なるメーカのアクセスポイント同士を接続することができない可能性が高い。また、ＷＤＳを利用する場合には、アクセスポイント同士を接続するために、セキュリティーを低下させなければならない場合がある。

【０００７】

本発明の目的は、無線通信におけるアクセスポイント間のセキュリティを低下させることなくアクセスポイント同士の接続を容易にすることである。

【課題を解決するための手段】

【０００８】

（１）

この発明のある局面に従うと、ネットワークの上位のアクセスポイントと下位のステーションと通信するための無線通信装置が提供される。無線通信装置は、少なくとも１つの無線通信デバイスと、少なくとも１つの無線通信デバイスを利用することによって、アクセスポイントに対しては自身がステーションとして無線通信を行い、ステーションに対しては自身がアクセスポイントとして無線通信を行うためのプロセッサとを備える。

【０００９】

（２）

好ましくは、プロセッサは、アクセスポイントに対して、少なくとも１つの無線通信デバイスを介して、自身がステーションとして無線通信を行うためのステーション部と、ステーションに対して、少なくとも１つの無線通信デバイスを介して、自身がアクセスポイントとして無線通信を行うためのアクセスポイント部と、ステーション部とアクセスポイント部との間でデータを転送するための仮想ブリッジ部とを含む。

【００１０】

（３）

好ましくは、仮想ブリッジ部は、ステーション部を介してアクセスポイントから受信したデータをアクセスポイント部を介してステーションへと転送し、アクセスポイント部を介してステーションから受信したデータをステーション部を介してアクセスポイントへと

転送する。
【００１１】
（４）
好ましくは、仮想ブリッジ部は、アクセスポイントが認証サーバに接続されている場合に、アクセスポイント部および少なくとも１つの無線通信デバイスを介して認証サーバに対してステーションからの認証の代理送信を実行する。
【００１２】
（５）
好ましくは、少なくとも１つの無線通信デバイスは、第１の無線通信デバイスと第２の無線通信デバイスとを含む。ステーション部は、第１の無線通信デバイスを介してアクセスポイントと無線通信を行う。アクセスポイント部は、第２の無線通信デバイスを介してステーションと無線通信を行う。
【発明の効果】
【００１３】
以上のように、本発明によって、無線通信におけるアクセスポイント間のセキュリティを低下させることなくアクセスポイント同士の接続を容易にすることができる。
【図面の簡単な説明】
【００１４】
【図１】本実施の形態に係るネットワークシステム１の全体構成を示すイメージ図である。
【図２】実施の形態１に係る無線通信装置１０１のハードウェア構成を示すブロック図である。
【図３】実施の形態１に係る無線通信装置１０１のソフトウェア構成を示すブロック図である。
【図４】ステーション制御ソフトウェア１１１Ａによる処理を示すフローチャートである。
【図５】ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの接続処理を示すイメージ図である。
【図６】ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの認証処理を示すイメージ図である。
【図７】ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの暗号化処理を示すイメージ図である。
【図８】ステーション制御ソフトウェア１１１Ａによる上位ネットワークとのＩＰプロトコルのデータ通信処理を示すイメージ図である。
【図９】アクセスポイント制御ソフトウェア１１１Ｂによる処理を示すフローチャートである。
【図１０】アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの接続処理を示すイメージ図である。
【図１１】アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの認証処理を示すイメージ図である。
【図１２】アクセスポイント制御ソフトウェア１１１Ｂと仮想ブリッジ１１１Ｘによる代理認証処理を示すイメージ図である。
【図１３】アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの暗号化処理を示すイメージ図である。
【図１４】アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとのＩＰプロトコルのデータ通信処理を示すイメージ図である。
【図１５】実施の形態２に係る無線通信装置１０２のハードウェア構成を示すブロック図である。
【図１６】実施の形態２に係る無線通信装置１０２のソフトウェア構成を示すブロック図である。

【発明を実施するための形態】
【００１５】
以下、図面を参照しつつ、本発明の実施の形態について説明する。以下の説明では、同一の部品には同一の符号を付してある。それらの名称および機能も同じである。したがって、それらについての詳細な説明は繰り返さない。
［実施の形態１］
【００１６】
＜ネットワークシステムの全体構成＞
【００１７】
まず、本実施の形態に係るネットワークシステムの全体構成について説明する。図１は、本実施の形態に係るネットワークシステム１の全体構成を示すイメージ図である。
【００１８】
図１を参照して、本実施の形態に係るネットワークシステム１は、無線通信装置１０１と、無線通信装置１０１と無線通信が可能なアクセスポイント２００とを含む。ネットワークシステム１は、無線通信装置１０１と無線通信が可能なステーション３００Ａ，３００Ｂと、アクセスポイント２００と無線通信が可能なステーション３００Ｃ，３００Ｄとを含む。なお、以下では、ステーション３００Ａ，３００Ｂ，３００Ｃ，３００Ｄを総称して、ステーション３００ともいう。
【００１９】
アクセスポイント２００は、アクセスポイント２００と有線通信が可能なハブ４００と接続されている。また、アクセスポイント２００は、ハブ４００を介して、認証サーバ５００とデータ通信が可能である。また、アクセスポイント２００は、ハブ４００およびルータ７００を介して、インターネットなどの外部のネットワークに接続可能である。
【００２０】
以下では、無線通信装置１０１と、ステーション３００Ａ，３００Ｂと、の間に構成されるネットワークを下位ネットワークという。無線通信装置１０１と、アクセスポイント２００、ハブ４００、ルータ７００と、の間に構成されるネットワークを上位ネットワークと言う。
＜無線通信装置１０１のハードウェア構成＞
【００２１】
次に、本実施の形態に係る無線通信装置１０１のハードウェア構成について説明する。図２は、本実施の形態に係る無線通信装置１０１のハードウェア構成を示すブロック図である。
【００２２】
図２を参照して、無線通信装置１０１は、ＮＰＵ（Network Processing Unit）１１１と、無線制御デバイス（ＭＡＣ）１２０と、無線デバイス（ＲＦ）１３０とを含む。
【００２３】
より詳細には、ＮＰＵ１１１は、無線制御デバイス１２０を介して無線デバイス１３０を制御することによって、アクセスポイント２００などの上位ネットワークとネットワークパケットの送受信を行う。同様に、ＮＰＵ１１１は、無線制御デバイス１２０を介して無線デバイス１３０を制御することによって、ステーション３００Ａ，３００Ｂなどの下位ネットワークとネットワークパケットの送受信を行う。
【００２４】
無線制御デバイス１２０と無線デバイス１３０とは、ＩＥＥＥ８０２．１１シリーズに準拠している。無線制御デバイス１２０は、ＮＰＵ１１１からの指示に基づいて、無線デバイス１３０を制御する。たとえば、無線デバイス１３０は、無線制御デバイス１２０に制御されることによって、ＮＰＵ１１１からのデータを外部のアクセスポイント２００やステーション３００Ａ，３００Ｂに送信する。また、無線デバイス１３０は、無線制御デバイス１２０に制御されることによって、外部のアクセスポイント２００やステーション３００Ａ，３００ＢからのデータをＮＰＵ１１１に受け渡す。

＜無線通信装置１０１のソフトウェア構成＞

【００２５】

次に、本実施の形態に係る無線通信装置１０１のソフトウェア構成について説明する。図３は、本実施の形態に係る無線通信装置１０１のソフトウェア構成を示すブロック図である。

【００２６】

図３を参照して、無線通信装置１０１は、仮想ブリッジ１１１Ｘと、ステーション制御ソフトウェア１１１Ａと、アクセスポイント制御ソフトウェア１１１Ｂと、第１の仮想制御デバイス１２０Ａと、第２の仮想制御デバイス１２０Ｂとを有する。

【００２７】

より詳細には、ＮＰＵ１１１は、図示しないメモリに格納されている制御プログラム（組み込みソフトウェア）を実行することによって、仮想ブリッジ１１１Ｘと、ステーション制御ソフトウェア１１１Ａと、アクセスポイント制御ソフトウェア１１１Ｂとを実現する。また、無線制御デバイス１２０は、無線デバイス１３０を制御するための第１の仮想制御デバイス１２０Ａと無線デバイス１３０を制御するための第２の仮想制御デバイス１２０Ｂとを実現する。

【００２８】

ステーション制御ソフトウェア１１１Ａについて説明する。ステーション制御ソフトウェア１１１Ａは、ＩＥＥＥ８０２．１１に準拠する。また、ステーション制御ソフトウェア１１１Ａは、ＩＥＥＥ８０２．１１ｉ、ＩＥＥＥ８０２．１ｘに準拠する認証処理を実行可能である。ステーション制御ソフトウェア１１１Ａは、無線ＬＡＮのセキュリティ機能に関して、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅが定めるＷＰＡ(Wi-Fi Protected Access)に準拠する。

【００２９】

このように構成されたステーション制御ソフトウェア１１１Ａは、第１の仮想制御デバイス１２０Ａを介して、無線デバイス１３０に外部のアクセスポイント２００と無線通信させる。すなわち、ステーション制御ソフトウェア１１１Ａは、無線デバイス１３０を介してアクセスポイント２００から受信したデータを仮想ブリッジ１１１Ｘへと受け渡す。逆に、ステーション制御ソフトウェア１１１Ａは、仮想ブリッジ１１１Ｘからのデータを、第１の仮想制御デバイス１２０Ａを介して、無線デバイス１３０に外部のアクセスポイント２００へと送信させる。

【００３０】

アクセスポイント制御ソフトウェア１１１Ｂについて説明する。アクセスポイント制御ソフトウェア１１１Ｂは、ＩＥＥＥ８０２．１１に準拠する。アクセスポイント制御ソフトウェア１１１Ｂは、ＩＥＥＥ８０２．１ｘに準拠した認証処理に関して、上位ネットワークの認証サーバ５００を代理することができる。アクセスポイント制御ソフトウェア１１１Ｂは、無線ＬＡＮのセキュリティ機能に関して、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅが定めるＷＰＡに準拠する。

【００３１】

このように構成されたアクセスポイント制御ソフトウェア１１１Ｂは、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０に外部のステーション３００Ａ，３００Ｂと無線通信させる。すなわち、アクセスポイント制御ソフトウェア１１１Ｂは、無線デバイス１３０を介してステーション３００Ａ，３００Ｂから受信したデータを仮想ブリッジ１１１Ｘへと受け渡す。逆に、ステーション制御ソフトウェア１１１Ａは、仮想ブリッジ１１１Ｘからのデータを、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０に外部のステーション３００Ａ，３００Ｂへと送信させる。

【００３２】

なお、本実施の形態においては、ステーション制御ソフトウェア１１１Ａとアクセスポイント制御ソフトウェア１１１Ｂのセキュリティは、別々に設定可能である。ただし、上位ネットワークと下位ネットワークとを共通なセキュリティとするために、同じ設定とす

る事が好ましい。

【００３３】

また、無線通信装置１０１は、ステーション制御ソフトウェア１１１Ａとアクセスポイント制御ソフトウェア１１１Ｂのいずれかまたは両方を複数含んでもよい。

【００３４】

仮想ブリッジ１１１Ｘについて説明する。仮想ブリッジ１１１Ｘは、ステーション制御ソフトウェア１１１Ａとアクセスポイント制御ソフトウェア１１１Ｂと間で、ＩＰｖ４およびＩＰｖ６のネットワークパケットを転送する。具体的には、仮想ブリッジ１１１Ｘは、アクセスポイント制御ソフトウェア１１１Ｂからのデータをステーション制御ソフトウェア１１１Ａに受け渡す。逆に、仮想ブリッジ１１１Ｘは、ステーション制御ソフトウェア１１１Ａからのデータをアクセスポイント制御ソフトウェア１１１Ｂに受け渡す。

【００３５】

また、仮想ブリッジ１１１Ｘは、外部のハブ４００がＥＡＰ（Extensible Authentication Protocol）認証サーバ５００に接続されている場合、認証サーバ５００の代わりにアクセスポイント制御ソフトウェア１１１Ｂを介してＥＡＰ認証処理を実行する。仮想ブリッジ１１１Ｘは、アクセスポイント制御ソフトウェア１１１ＢからのＩＥＥＥ８０２．１ｘ準拠したＥＡＰＯＬ（Extensible Authentication Protocol over LAN）パケットを、ステーション制御ソフトウェア１１１Ａを介して上位ネットワークに存在する認証サーバ５００へ転送することができる。

【００３６】

より詳細には、仮想ブリッジ１１１Ｘまたはステーション制御ソフトウェア１１１Ａは、ＩＥＥＥ８０２．１ｘの認証サプリカントを有する。仮想ブリッジ１１１Ｘまたはステーション制御ソフトウェア１１１Ａは、当該サプリカントを利用して上位のネットワークと接続する。認証が成功した場合、仮想ブリッジ１１１Ｘは、ステーション制御ソフトウェア１１１Ａとアクセスポイント制御ソフトウェア１１１Ｂとを接続し、両者の間でインターネットプロトコルのデータをパススルーする。また、仮想ブリッジ１１１Ｘは、アクセスポイント制御ソフトウェア１１１ＢからのＩＥＥＥ８０２．１ｘの認証フレームもステーション制御ソフトウェア１１１Ａへと転送する。

＜ステーション制御ソフトウェア１１１Ａの処理＞

【００３７】

次に、ステーション制御ソフトウェア１１１Ａの処理について説明する。図４は、ステーション制御ソフトウェア１１１Ａによる処理を示すフローチャートである。

【００３８】

図４を参照して、ステーション制御ソフトウェア１１１Ａは、アクセスポイント２００などの上位ネットワークと通信を開始する（ステップＳ１０２）。ここで、図５は、ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの接続処理を示すイメージ図である。図５を参照して、ステーション制御ソフトウェア１１１Ａは、第１の仮想制御デバイス１２０Ａを介して、無線デバイス１３０に上位ネットワークと接続用のデータを送受信させる。

【００３９】

図４に戻って、ステーション制御ソフトウェア１１１Ａは、上位ネットワークとの認証処理を実行する（ステップＳ１０４）。ここで、図６は、ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの認証処理を示すイメージ図である。図６を参照して、ステーション制御ソフトウェア１１１Ａは、第１の仮想制御デバイス１２０Ａを介して、無線デバイス１３０に上位ネットワークと認証用のデータを送受信させる。

【００４０】

図４に戻って、ステーション制御ソフトウェア１１１Ａは、上位ネットワークと送受信するデータの暗号化・復号化処理を実行する（ステップＳ１０６）。ここで、図７は、ステーション制御ソフトウェア１１１Ａによる上位ネットワークとの暗号化処理を示すイメージ図である。図７を参照して、ステーション制御ソフトウェア１１１Ａは、第１の仮想

制御デバイス１２０Ａを介して、無線デバイス１３０に上位ネットワークと暗号化処理用のデータを送受信させる。

【００４１】

図４に戻って、認証および暗号化を完了したステーション制御ソフトウェア１１１Ａは、上位ネットワークとの間でデータを送受信する（ステップＳ１０８）。ここで、図８は、ステーション制御ソフトウェア１１１Ａによる上位ネットワークとのＩＰプロトコルのデータ通信処理を示すイメージ図である。図８を参照して、ステーション制御ソフトウェア１１１Ａは、第１の仮想制御デバイス１２０Ａを介して、無線デバイス１３０にＩＰプロトコルに従ってＩＰｖ４およびＩＰｖ６のパケットを上位ネットワークと送受信させる。なお、ステーション制御ソフトウェア１１１Ａは、上位ネットワークとのデータの送受信中、ステップＳ１０６とステップＳ１０８とを繰り返し実行する。

【００４２】

このように、本実施の形態においては、ステーション制御ソフトウェア１１１Ａは、適切なセキュリティを設定し、セキュアな上位ネットワークを構築する。ステーション制御ソフトウェア１１１Ａは、セキュリティを設定する場合、上位ネットワークと間で、ＩＥＥＥ８０２．１１シリーズに準拠したセキュリティを利用できるように認証、暗号化を行う。より詳細には、ＩＥＥＥ８０２．１ｘに準拠した認証が必要な場合、無線通信装置１０１は認証子機として、上位ネットワークに存在する認証サーバ５００と認証処理を行う。

＜アクセスポイント制御ソフトウェア１１１Ｂの処理＞

【００４３】

次に、アクセスポイント制御ソフトウェア１１１Ｂの処理について説明する。図９は、アクセスポイント制御ソフトウェア１１１Ｂによる処理を示すフローチャートである。

【００４４】

図９を参照して、アクセスポイント制御ソフトウェア１１１Ｂは、ステーション３００Ａ，３００Ｂなどの下位ネットワークと通信を開始する（ステップＳ２０２）。ここで、図１０は、アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの接続処理を示すイメージ図である。図１０を参照して、アクセスポイント制御ソフトウェア１１１Ｂは、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０に下位ネットワークと接続用のデータを送受信させる。

【００４５】

図９に戻って、アクセスポイント制御ソフトウェア１１１Ｂは、下位ネットワークとの認証処理を実行する（ステップＳ２０４）。ここで、図１１は、アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの認証処理を示すイメージ図である。図１１を参照して、アクセスポイント制御ソフトウェア１１１Ｂは、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０に下位ネットワークと認証用のデータを送受信させる。

【００４６】

なお、無線通信装置１０１は、ステーション３００Ａ，３００ＢからＥＡＰ認証の要求を受信した場合には、認証サーバ５００の代理認証を行う。ここで、図１２は、アクセスポイント制御ソフトウェア１１１Ｂと仮想ブリッジ１１１Ｘによる代理認証処理を示すイメージ図である。図１２を参照して、アクセスポイント制御ソフトウェア１１１Ｂは、第２の仮想制御デバイス１２０Ｂを介して、仮想ブリッジ１１１Ｘに認証パケットの送信を要求する。仮想ブリッジ１１１Ｘは、下位ネットワークのために認証サーバ５００とＥＡＰ認証のための情報のやり取りを行う。

【００４７】

図９に戻って、アクセスポイント制御ソフトウェア１１１Ｂは、下位ネットワークと送受信するデータの暗号化・復号化処理を実行する（ステップＳ２０６）。ここで、図１３は、アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとの暗号化処理を示すイメージ図である。図１３を参照して、アクセスポイント制御ソフトウェア１１１

Ｂは、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０に下位ネットワークと暗号化処理用のデータを送受信させる。

【００４８】

図９に戻って、認証および暗号化を完了したアクセスポイント制御ソフトウェア１１１Ｂは、下位ネットワークとの間でデータを送受信する（ステップＳ２０８）。ここで、図１４は、アクセスポイント制御ソフトウェア１１１Ｂによる下位ネットワークとのＩＰプロトコルのデータ通信処理を示すイメージ図である。図１４を参照して、無線通信装置１０１が下位ネットワークのステーション３００Ａ，３００ＢとＩＰプロトコルのデータ通信処理をする際、アクセスポイント制御ソフトウェア１１１Ｂは、第２の仮想制御デバイス１２０Ｂを介して、無線デバイス１３０にＩＰプロトコルに従ってＩＰｖ４およびＩＰｖ６のパケットを下位ネットワークと送受信させる。なお、アクセスポイント制御ソフトウェア１１１Ｂは、下位ネットワークとのデータの送受信中、ステップＳ２０６とステップＳ２０８とを繰り返し実行する。

【００４９】

このように、本実施の形態においては、アクセスポイント制御ソフトウェア１１１Ｂは、適切なセキュリティを設定し、セキュアな下位ネットワークを構築する。アクセスポイント制御ソフトウェア１１１Ｂは、セキュリティを設定する場合、下位ネットワークと間で、ＩＥＥＥ８０２．１１シリーズに準拠したセキュリティを利用できるように認証、暗号化を行う。

【００５０】

以上のように、本実施の形態においては、無線通信装置１０１が、アクセスポイント２００などの上位のネットワークに対しては自身がインフラストラクチャーモードの子機として振る舞い、ステーション３００Ａ，３００Ｂなどの下位のネットワークに対しては自身がインフラストラクチャーモードの親機として振る舞う。これによって、アクセスポイント間でＷＤＳ（Wireless Distribution System）を利用する必要が無くなり、両者の互換性を高めることができる。その結果、無線通信装置１０１とアクセスポイント２００との間のセキュリティを高めることも可能になる。

［実施の形態２］

【００５１】

次に、本発明の実施の形態２について説明する。上述した実施の形態１に係る無線通信装置１０１は、１つの無線デバイス１３０を利用して、アクセスポイント２００などの上位ネットワークとステーション３００Ａ，３００Ｂなどの下位ネットワークと通信するものであった。しかしながら、本実施の形態に係る無線通信装置１０２は、無線デバイス１３１を利用してアクセスポイント２００などの上位ネットワークと通信し、他の無線デバイス１３２を利用してステーション３００Ａ，３００Ｂなどの下位ネットワークと通信するものである。

＜ネットワークシステムの全体構成＞

【００５２】

本実施の形態に係るネットワークシステム１の全体構成は、図１に示す実施の形態１のそれと同様であるため、ここでは説明を繰り返さない。以下では、本実施の形態に係る無線通信装置１０２について説明する。

＜無線通信装置１０２のハードウェア構成＞

【００５３】

本実施の形態に係る無線通信装置１０２のハードウェア構成について説明する。図１５は、本実施の形態に係る無線通信装置１０２のハードウェア構成を示すブロック図である。

【００５４】

図２を参照して、無線通信装置１０１は、ＮＰＵ（Network Processing Unit）１１２と、第１の無線制御デバイス（ＭＡＣ）１２１と、第２の無線制御デバイス（ＭＡＣ）１２２と、第１の無線デバイス（ＲＦ）１３１と、第２の無線デバイス１３２（ＲＦ）とを

含む。
【００５５】
より詳細には、ＮＰＵ１１２は、第１の無線制御デバイス１２１を介して無線デバイス１３１を制御することによって、アクセスポイント２００などの上位ネットワークとネットワークパケットの送受信を行う。同様に、ＮＰＵ１１２は、第２の無線制御デバイス１２２を介して無線デバイス１３２を制御することによって、ステーション３００Ａ，３００Ｂなどの下位ネットワークとネットワークパケットの送受信を行う。
【００５６】
無線制御デバイス１２１，１２２と無線デバイス１３１，１３２とは、ＩＥＥＥ８０２．１１シリーズに準拠している。無線制御デバイス１２１，１２２は、ＮＰＵ１１２からの指示に基づいて、無線デバイス１３１，１３２を制御する。たとえば、無線デバイス１３１，１３２は、それぞれ、無線制御デバイス１２１，１２２に制御されることによって、ＮＰＵ１１２からのデータを外部のアクセスポイント２００やステーション３００Ａ，３００Ｂに送信する。また、無線デバイス１３１，１３２は、無線制御デバイス１２１，１２２に制御されることによって、外部のアクセスポイント２００やステーション３００Ａ，３００ＢからのデータをＮＰＵ１１２に受け渡す。
＜無線通信装置１０２のソフトウェア構成＞
【００５７】
次に、本実施の形態に係る無線通信装置１０２のソフトウェア構成について説明する。図１６は、本実施の形態に係る無線通信装置１０２のソフトウェア構成を示すブロック図である。
【００５８】
図１６を参照して、無線通信装置１０２は、仮想ブリッジ１１２Ｘと、ステーション制御ソフトウェア１１２Ａと、アクセスポイント制御ソフトウェア１１２Ｂとを有する。より詳細には、ＮＰＵ１１２は、図示しないメモリに格納されている制御プログラム（組み込みソフトウェア）を実行することによって、仮想ブリッジ１１２Ｘと、ステーション制御ソフトウェア１１２Ａと、アクセスポイント制御ソフトウェア１１２Ｂとを実現する。
【００５９】
すなわち、本実施の形態においては、第１の無線制御デバイス１２１が実施の形態１の無線制御デバイス１２０の第１の仮想制御デバイス１２０Ａの役割を果たし、第２の無線制御デバイス１２２が実施の形態１の無線制御デバイス１２０の第２の仮想制御デバイス１２０Ｂの役割を果たす。そして、第１の無線デバイス１３１と第２の無線デバイス１３２とが実施の形態１の無線デバイス１３０の役割を果たす。
【００６０】
本実施の形態に係るステーション制御ソフトウェア１１２Ａ、アクセスポイント制御ソフトウェア１１２Ｂ、仮想ブリッジ１１２Ｘは、実施の形態１のステーション制御ソフトウェア１１１Ａ、アクセスポイント制御ソフトウェア１１１Ｂ、仮想ブリッジ１１１Ｘと同様に構成されるため、それらについての詳細な説明は繰り返さない。
＜その他の実施の形態＞
【００６１】
また、本発明は、無線通信装置１０１，１０２や他の無線通信装置などにプログラムを供給することによって達成される場合にも適用できることはいうまでもない。たとえば、本発明は、無線通信機能に加えて他の機能を有するコンピュータにも適用することができる。そして、本発明を達成するためのソフトウェアによって表されるプログラムを格納した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣＰＵ、ＭＰＵ、ＮＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、本発明の効果を享受することが可能となる。
【００６２】
この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施の形態の機能を実現することになり、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。

【００６３】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施の形態の機能が実現されるだけでなく、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動している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の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。

【００６４】

さらに、記憶媒体から読み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き込まれた後、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、その処理によって前述した実施の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。

【００６５】

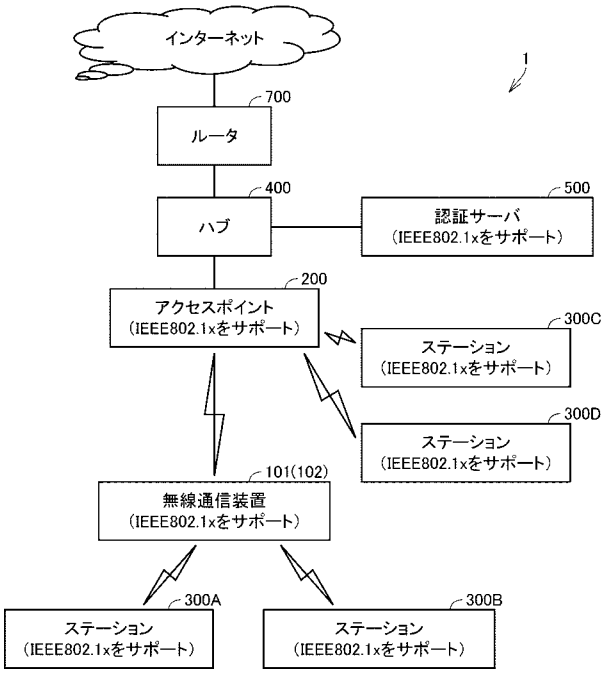
今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した説明ではなく、特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【符号の説明】

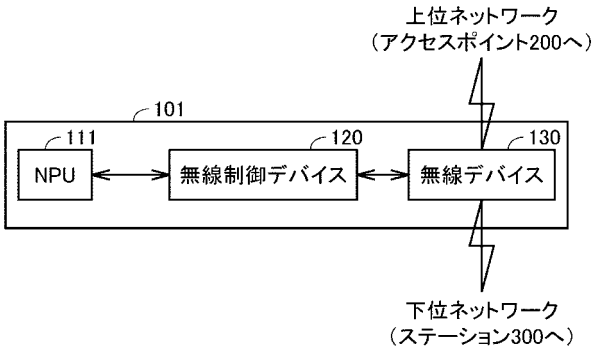
【００６６】

１０１，１０２　無線通信装置
１１１Ａ　ステーション制御ソフトウェア
１１１Ｂ　アクセスポイント制御ソフトウェア
１１１Ｘ　仮想ブリッジ
１１２Ａ　ステーション制御ソフトウェア
１１２Ｂ　アクセスポイント制御ソフトウェア
１１２Ｘ　仮想ブリッジ
１２０　無線制御デバイス
１２０Ａ　第１の仮想制御デバイス
１２０Ｂ　第２の仮想制御デバイス
１２１　第１の無線制御デバイス
１２２　第２の無線制御デバイス
１３０　無線デバイス
１３１　第１の無線デバイス
１３２　第２の無線デバイス
２００　アクセスポイント
３００Ａ，３００Ｂ，３００Ｃ，３００Ｄ　ステーション
４００　ハブ
５００　認証サーバ
７００　ルータ

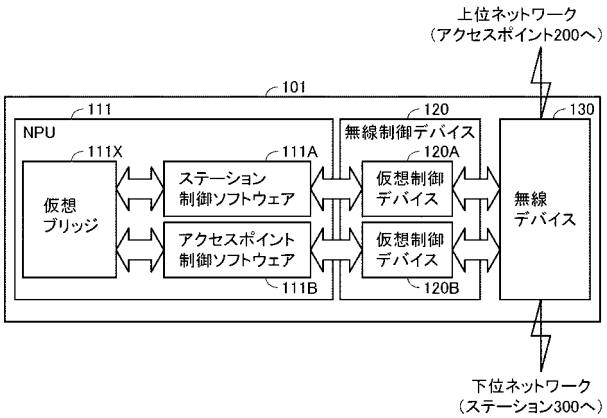
【図１】


インターネット
1
700
ルータ
400
ハブ
500
認証サーバ
（IEEE802.1xをサポート）
200
アクセスポイント
（IEEE802.1xをサポート）
300C
ステーション
（IEEE802.1xをサポート）
300D
ステーション
（IEEE802.1xをサポート）
101(102)
無線通信装置
（IEEE802.1xをサポート）
300A
ステーション
（IEEE802.1xをサポート）
300B
ステーション
（IEEE802.1xをサポート）

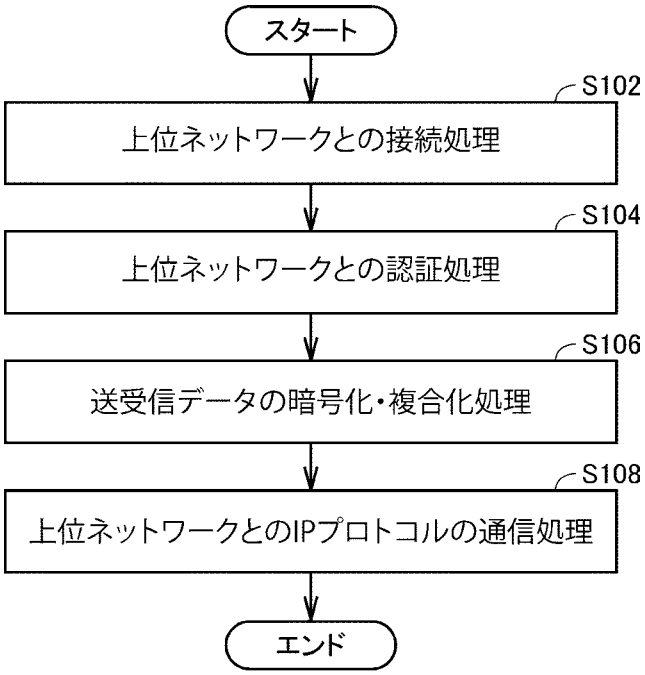
【図２】


上位ネットワーク
（アクセスポイント200へ）
101
111
NPU
120
無線制御デバイス
130
無線デバイス
下位ネットワーク
（ステーション300へ）

【図３】

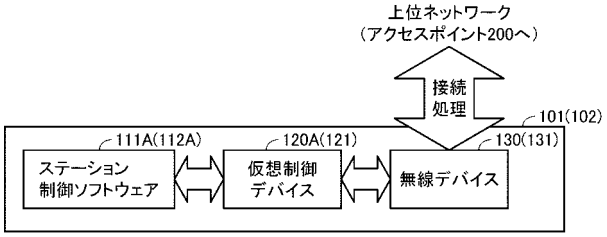

上位ネットワーク
（アクセスポイント200へ）
101
111
NPU
120
無線制御デバイス
130
111X
仮想
ブリッジ
111A
ステーション
制御ソフトウェア
120A
仮想制御
デバイス
無線
デバイス
アクセスポイント
制御ソフトウェア
仮想制御
デバイス
111B
120B
下位ネットワーク
（ステーション300へ）

【図４】



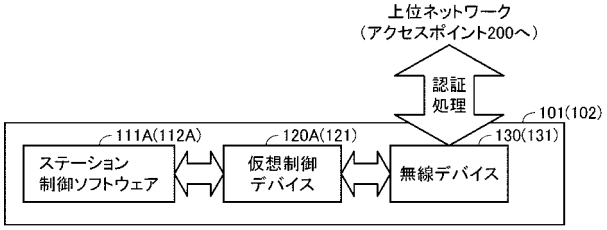
【図５】

上位ネットワークのアクセスポイントとの接続処理



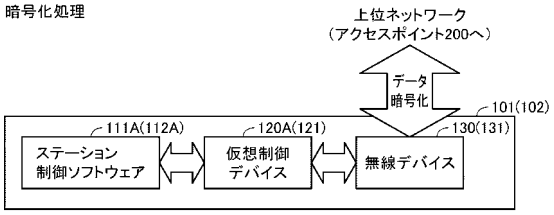
【図６】

上位ネットワークのアクセスポイントとの認証処理



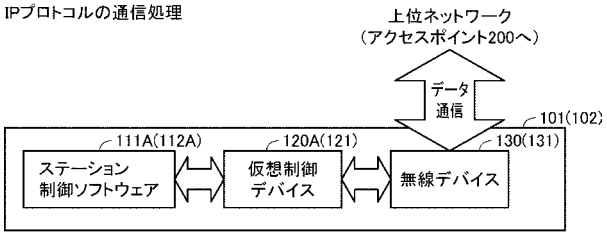
【図７】

上位ネットワークのアクセスポイントとの
暗号化処理

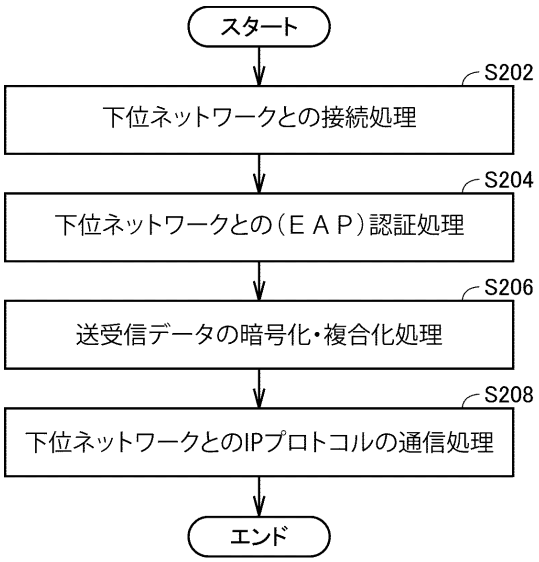


【図８】

上位ネットワークのアクセスポイントとの
IPプロトコルの通信処理

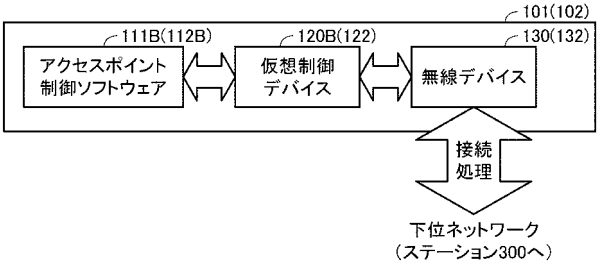


【図９】



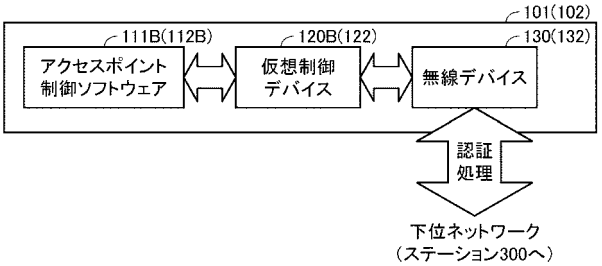
【図１０】

下位ネットワークのステーション300からの接続処理



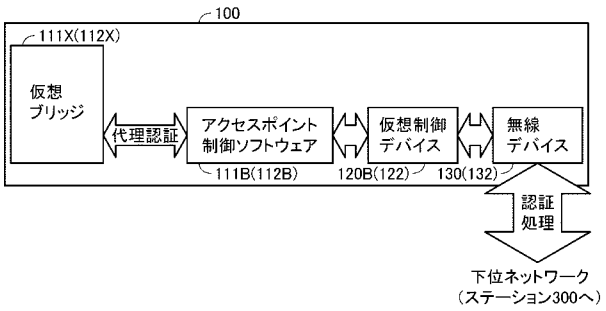
【図１１】

下位ネットワークのステーション300からの認証処理



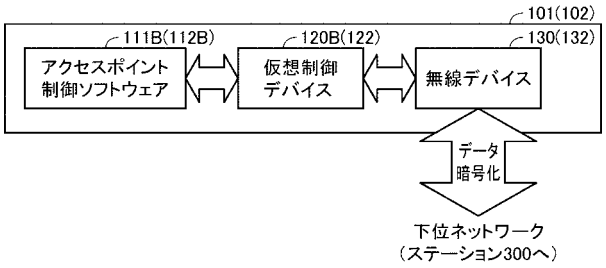
【図１２】

ステーションからのEAP認証



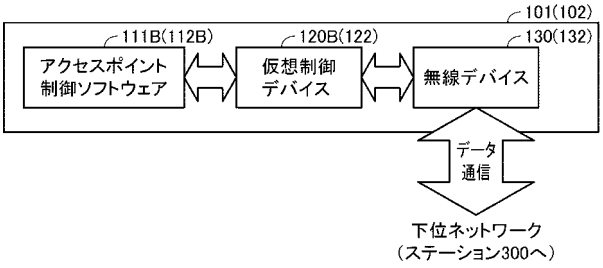
【図１３】

下位ネットワークのステーション300との暗号化処理

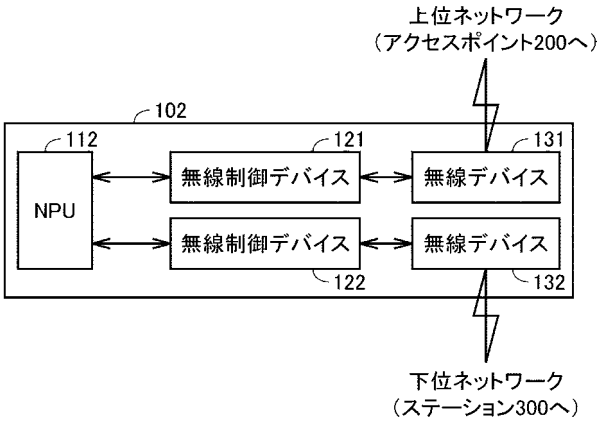


【図１４】

下位ネットワークのステーション300とのIPプロトコルの通信処理



【図１５】



【図１６】