(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5002259号
(P5002259)
(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
G06F 21/20 (2006.01)　　G06F 21/20　144C
H04L 9/32 (2006.01)　　H04L 9/00　675D

請求項の数 3　(全 31 頁)

(21)出願番号　特願2006-348535 (P2006-348535)
(22)出願日　平成18年12月25日 (2006.12.25)
(65)公開番号　特開2008-158903 (P2008-158903A)
(43)公開日　平成20年7月10日 (2008.7.10)
審査請求日　平成21年12月8日 (2009.12.8)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　110000899
特許業務法人　松田国際特許事務所
(74)代理人　100092794
弁理士　松田　正道
(72)発明者　荒新　伸彦
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　田中　　治
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】認証システム

(57)【特許請求の範囲】
【請求項１】
主端末と、
前記主端末に接続された１台以上の副端末と、
前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、
前記副端末は、
前記認証サーバから受信した認証応答データに含まれる認証結果が不許可の場合には、前記認証応答データ受信後、所定の不許可受信タイムアウト期間内に前記主端末とのリンクを切断するものであり、
通信に使用する動作周波数を制御する周波数制御ユニットを有しており、
前記認証結果が不許可の前記認証応答データを受信すると、異なる動作周波数で動作している他の主端末と接続するためにそれまで確立していた前記主端末とのリンクを切断し、
前記主端末は、
前記副端末との接続状態を検知する接続検知ユニットと、
前記副端末との物理層の接続を制御する接続制御ユニットと、
前記副端末が認証を要求する際に前記認証サーバ宛に送信してくる認証要求データに含まれる少なくとも前記副端末のＩＤ情報を格納しておく認証状態テーブルと、

前記認証サーバに転送した前記認証要求データに対応して前記認証サーバが前記副端末宛に送信してくる前記認証応答データに含まれる認証結果が、前記認証状態テーブルに格納した前記ＩＤ情報に対応する前記副端末が不許可の端末であることを示す場合には、前記認証応答データを前記副端末宛に転送した後、前記副端末が前記不許可受信タイムアウト期間内にリンクの切断をしない場合、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットとを有する、認証システム。

【請求項２】

主端末と、

前記主端末に接続された１台以上の副端末と、

前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、

前記副端末は、

認証を要求するために前記認証サーバ宛に認証要求データを送信した後、前記認証要求データに対応する前記認証サーバからの認証応答データを所定のリトライ要求期間内に受信しなかった場合には、前記リトライ要求期間毎に、所定のリトライ回数、前記認証要求データを再送し、それでも前記認証応答データを受信しなかった場合、最初の前記認証要求データを送信した時点から所定の認証応答タイムアウト期間内に前記主端末とのリンクを切断するものであり、

通信に使用する動作周波数を制御する周波数制御ユニットを有しており、

前記所定のリトライ回数の前記認証要求データを再送しても前記認証応答データを受信しなかったときには、異なる動作周波数で動作している他の主端末と接続するためにそれまで確立していた前記主端末とのリンクを切断し、

前記主端末は、

前記副端末との接続状態を検知する接続検知ユニットと、

前記副端末との物理層の接続を制御する接続制御ユニットと、

前記副端末からの前記最初の前記認証要求データを前記認証サーバに転送した後、前記認証応答タイムアウト期間内に前記認証サーバから前記副端末宛の前記認証応答データが送信されてこないのに、前記副端末とのリンクが切断されない場合には、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットとを有する、認証システム。

【請求項３】

主端末と、

前記主端末に接続された１台以上の副端末と、

前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、

前記主端末は、

前記副端末との接続状態を検知する接続検知ユニットと、

前記副端末との物理層の接続を制御する接続制御ユニットと、

前記副端末が認証を要求する際に前記認証サーバ宛に送信してくる認証要求データに含まれる少なくとも前記副端末のＩＤ情報を格納しておく認証状態テーブルと、

前記認証サーバに転送した前記認証要求データに対応して前記認証サーバが前記副端末宛に送信してくる認証応答データに含まれる認証結果が、前記認証状態テーブルに格納した前記ＩＤ情報に対応する前記副端末が不許可の端末であることを示す場合には、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットと、

前記副端末間との通信速度が遅くなるように制限できる速度制限ユニットとを有しており、

前記認証状態制御ユニットは、前記副端末とのリンクが新たに確立されたことが前記接続検知ユニットによって検知された後、前記副端末が前記認証サーバによって認証されるまでの期間は、前記主端末と前記副端末間の通信速度が遅くなるように前記速度制限ユニットを制御する、認証システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク機器がネットワークに接続される認証システムに関する。

【背景技術】

【０００２】

通信システムにおいて通信機器の認証を行うことは、不正使用防止を目的とする上で非常に重要な事である。しかしシステム上に接続される全ての通信機器の認証をサーバで実現しようとする場合、認証を実施するサーバにかかる負荷が集中するという課題があった。

【０００３】

この課題に対して例えば、通信システムにおける認証処理などにかかる負荷の集中を回避する方法が提案されている（例えば、特許文献１参照）。

【０００４】

図１３は、特許文献１に開示されている従来の通信システムの接続構成図を示している。

【０００５】

ＤＨＣＰサーバ１０２は、ネットワーク１０１にアクセスしようとする端末に対して、ＩＰアドレスの割り当てを行う。ＨＰサーバ１０３は、ネットワーク１０１に接続される端末に対して、Ｗｅｂ閲覧およびデータベースアクセス等のサービスを提供する。ＨＰサーバ１０３は、ＤＨＣＰサーバ１０２によって認証が成立したクライアント端末だけが利用できるサーバである。

【０００６】

一方、無線クライアント端末１０６～１０８は、アクセスポイント１０５を介して、ネットワーク１０１に接続される。各無線クライアント端末１０６～１０８は、ＰＣなどのユーザ端末と無線ＬＡＮアダプタで構成されており、ユーザ端末１１３～１１５は、それぞれ無線ＬＡＮアダプタ１１０～１１２を利用して、無線でアクセスポイント１０５に接続し、アクセスポイント１０５を介してネットワーク１０１に接続する。

【０００７】

ここで、アクセスポイント１０５には、ネットワーク１０１にアクセス許可がされ得る無線クライアント端末のＭＡＣアドレスが予め登録されている登録アドレスリスト１０４が設けられている。

【０００８】

例えば、無線クライアント端末１０６がアドレス割り当てを要求する際に、まず、無線クライアント端末１０６は、アクセスポイント１０５からの物理層での接続の許可を受けてアクセスポイント１０５との間のリンクを確立する。リンク確立後、無線クライアント端末１０６は、自身のＭＡＣアドレスを含んだアドレス割り当て要求メッセージを送信すると、そのメッセージは、一旦アクセスポイント１０５で受信される。アクセスポイント１０５は、受信したアドレス割り当て要求メッセージからＭＡＣアドレスを抽出し、そのＭＡＣアドレスが登録アドレスリスト１０４に登録されているかどうかを解析する。

【０００９】

そして、ＭＡＣアドレスが未登録の場合には、アクセスポイント１０５は、ＩＰアドレスの割り当て処理を中断し終了する。つまり、この場合には、無線クライアント端末１０６からのアドレス割り当て要求メッセージはＤＨＣＰサーバ１０２へは送信されず、ＤＨＣＰサーバ１０２における無線クライアント端末１０６に対するＩＰアドレス割り当ての処理は発生しない。一方、ＭＡＣアドレスが登録されている場合には、アクセスポイント

１０５は、無線クライアント端末１０６からのアドレス割り当て要求メッセージをＤＨＣＰサーバ１０２に送信する。したがって、アクセスポイント１０５に無線で接続される無線クライアント端末１０６～１０８についてのＭＡＣアドレスによる端末認証処理は、ＤＨＣＰサーバ１０２ではなく、アクセスポイント１０５において行われることになる。

【００１０】

なお、図１３には記載していないが、ネットワーク１０１に有線で接続されるクライアント端末については、ＤＨＣＰサーバ１０２が端末認証処理を行い、ＩＰアドレスを割り当てる。

【００１１】

このようにして、従来はＤＨＣＰサーバ１０２で行われていた無線クライアント端末１０６～１０８の収容可否の判断処理をアクセスポイント１０５で行わせるようにしたことにより、不正アクセスを防止するとともに、ＤＨＣＰサーバ１０２に集中していたアドレス割り当ておよび認証処理に要する負荷を分散していた。

【特許文献１】特開２００３－３１８９３９号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

しかしながら、図１３に示す従来の通信システムでは、不正なクライアント端末からのアドレス割り当て要求に対してアクセスポイント１０５で拒否する場合でも、そのアクセスポイント１０５による判断処理のために帯域を割り当てているため、正規のクライアント端末が使用する帯域を占拠してしまっていた。

【００１３】

すなわち、不正な無線クライアント端末からのアドレス割り当て要求に対しても、アクセスポイント１０５は、物理層での接続を許可し、帯域を割り当てた上で、その無線クライアント端末からのアドレス割り当て要求を一旦受信し、そのメッセージの内容を解析している。このように不正な無線クライアント端末に対する収容可否の判断処理のために帯域を割り当てているために、正規の無線クライアント端末が本来割り当てられるはずの帯域を占拠してしまい、その判断処理の期間に伝送速度が遅くなってしまう等、正規の無線クライアント端末を使用するユーザにとって不利益が発生していた。

【００１４】

本発明は、上記従来の課題を解決するもので、正規のクライアント端末が使用する帯域を圧迫することなく認証サーバの負荷を低減できる認証システム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】

【００１７】

上述した課題を解決するために、第１の本発明は、

主端末と、

前記主端末に接続された１台以上の副端末と、

前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、

前記副端末は、

前記認証サーバから受信した認証応答データに含まれる認証結果が不許可の場合には、前記認証応答データ受信後、所定の不許可受信タイムアウト期間内に前記主端末とのリンクを切断するものであり、

通信に使用する動作周波数を制御する周波数制御ユニットを有しており、

前記認証結果が不許可の前記認証応答データを受信すると、異なる動作周波数で動作している他の主端末と接続するためにそれまで確立していた前記主端末とのリンクを切断し、

前記主端末は、

前記副端末との接続状態を検知する接続検知ユニットと、
前記副端末との物理層の接続を制御する接続制御ユニットと、
前記副端末が認証を要求する際に前記認証サーバ宛に送信してくる認証要求データに含まれる少なくとも前記副端末のＩＤ情報を格納しておく認証状態テーブルと、
前記認証サーバに転送した前記認証要求データに対応して前記認証サーバが前記副端末宛に送信してくる前記認証応答データに含まれる認証結果が、前記認証状態テーブルに格納した前記ＩＤ情報に対応する前記副端末が不許可の端末であることを示す場合には、前記認証応答データを前記副端末宛に転送した後、前記副端末が前記不許可受信タイムアウト期間内にリンクの切断をしない場合、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットとを有する、認証システムである。

【００１９】

また、第２の本発明は、
主端末と、
前記主端末に接続された１台以上の副端末と、
前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、
前記副端末は、
認証を要求するために前記認証サーバ宛に認証要求データを送信した後、前記認証要求データに対応する前記認証サーバからの認証応答データを所定のリトライ要求期間内に受信しなかった場合には、前記リトライ要求期間毎に、所定のリトライ回数、前記認証要求データを再送し、それでも前記認証応答データを受信しなかった場合、最初の前記認証要求データを送信した時点から所定の認証応答タイムアウト期間内に前記主端末とのリンクを切断するものであり、
通信に使用する動作周波数を制御する周波数制御ユニットを有しており、
前記所定のリトライ回数の前記認証要求データを再送しても前記認証応答データを受信しなかったときには、異なる動作周波数で動作している他の主端末と接続するためにそれまで確立していた前記主端末とのリンクを切断し、
前記主端末は、
前記副端末との接続状態を検知する接続検知ユニットと、
前記副端末との物理層の接続を制御する接続制御ユニットと、
前記副端末からの前記最初の前記認証要求データを前記認証サーバに転送した後、前記認証応答タイムアウト期間内に前記認証サーバから前記副端末宛の前記認証応答データが送信されてこないのに、前記副端末とのリンクが切断されない場合には、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットとを有する、認証システムである。

【００２１】

また、第３の本発明は、
主端末と、
前記主端末に接続された１台以上の副端末と、
前記主端末に接続され、前記主端末を介して前記副端末との間で認証用データを交換することにより、前記副端末が通信を許可された端末であるかを認証する認証サーバとを備えた認証システムであって、
前記主端末は、
前記副端末との接続状態を検知する接続検知ユニットと、
前記副端末との物理層の接続を制御する接続制御ユニットと、
前記副端末が認証を要求する際に前記認証サーバ宛に送信してくる認証要求データに含まれる少なくとも前記副端末のＩＤ情報を格納しておく認証状態テーブルと、
前記認証サーバに転送した前記認証要求データに対応して前記認証サーバが前記副端末

宛に送信してくる認証応答データに含まれる認証結果が、前記認証状態テーブルに格納した前記ＩＤ情報に対応する前記副端末が不許可の端末であることを示す場合には、その副端末からのリンクの確立をできなくするために、前記接続制御ユニットによってその副端末との物理層の接続を切断させる認証状態制御ユニットと、

前記副端末間との通信速度が遅くなるように制限できる速度制限ユニットとを有しており、

前記認証状態制御ユニットは、前記副端末とのリンクが新たに確立されたことが前記接続検知ユニットによって検知された後、前記副端末が前記認証サーバによって認証されるまでの期間は、前記主端末と前記副端末間の通信速度が遅くなるように前記速度制限ユニットを制御する、認証システムである。

【発明の効果】

【００２８】

本発明により、従来よりも容易な管理で、認証サーバの負荷を低減できる認証システムを提供できる。

【発明を実施するための最良の形態】

【００２９】

以下、本発明および本発明に関連する発明を実施するための最良の形態について図面を参照しながら説明する。

【００３０】

（実施の形態１）

図１は、本発明の実施の形態１における認証システムの構成を概略的に示す構成図である。

【００３１】

本実施の形態１の認証システムは、主端末７１の配下に複数の副端末７２～７４が同軸ケーブルで接続されている。主端末７１と副端末７２～７４との接続には、宅内に既設のＴＶ用の同軸ケーブルを利用しており、分配器７８を介して同軸ケーブル８５～８８によって接続される。副端末７２～７４は、それぞれ、同軸ケーブルモデム７９～８１およびＰＣなどのユーザ端末８２～８４で構成されている。主端末７１は、例えば、宅内のＴＶ用に設置された同軸ケーブルを利用した同軸ホームネットワークを構成する際に、クライアント用の同軸ケーブルモデム７９～８１と共に利用されるマスタ用の同軸ケーブル用モデムである。

【００３２】

図１では、主端末７１の配下に３つの副端末７２～７４が接続される構成を示しているが、接続される副端末の数はこれに限る物でない。また、本実施の形態１の認証システムにおける主端末７１の数も複数存在しても良い。

【００３３】

また、主端末７１の上位には、主端末７１および各副端末７２～７４の機器認証を行う認証サーバ７５と、主端末７１および各副端末７２～７４の端末管理を行う端末管理装置７６が接続される。認証サーバ７５および端末管理装置７６は、それぞれ、図１３に示した従来の通信システムにおける、ＤＨＣＰサーバ１０２およびＨＰサーバ１０３に相当するものである。また、主端末７１、認証サーバ７５および端末管理装置７６は、光ファイバケーブル８９によりインターネット７７に接続されている。

【００３４】

次に、主端末７１および同軸ケーブルモデム７９～８１の各構成について説明する。

【００３５】

図２は、図１に示した主端末７１の内部構成図を示している。

【００３６】

主端末７１は、通信Ｉ／Ｆ１０と同軸Ｉ／Ｆ１１とを備えており、双方のＩ／Ｆから受信したデータを所望のＩ／Ｆに転送する通信機器である。通信Ｉ／Ｆ１０は、例えばイーサネット（登録商標）などの、同軸Ｉ／Ｆとは異なる通信Ｉ／Ｆである。また、主端末７

１は、自身のデータを処理したりする制御を行う転送制御部１７を備えている。
【００３７】
主端末７１は更に、通信Ｉ／Ｆ１０におけるデータの送受信を処理する通信送受信処理部１６と、同軸Ｉ／Ｆ１１におけるデータの送受信を処理する同軸送受信処理部１９を備えている。また、転送制御部１７は、転送制御部１７で処理するデータをスヌープする通信データスヌープ部１８を有している。また、通信データスヌープ部１８でスヌープしたデータが配下に接続される副端末７２～７４、または認証サーバ７５からの認証データであった場合に、その認証データを解析する認証データ解析部１２と、解析した認証データを基に配下に接続される副端末７２～７４の認証状態を記憶する認証状態記憶部１３と、配下に接続される副端末７２～７４の同軸接続を制御する同軸制御部１４と、同軸Ｉ／Ｆ１１に接続される副端末７２～７４の接続を検知する接続検知部１５を備えている。認証状態記憶部１３は、配下に接続された副端末の状態を、状態管理テーブル２９を用いて管理する。また、同軸制御部１４は、同軸Ｉ／Ｆ１１に接続される装置との間で使用する速度を設定できる機能を有している。
【００３８】
なお、認証状態記憶部１３、同軸制御部１４、接続検知部１５、および状態管理テーブル２９が、それぞれ、本発明の、認証状態制御ユニット、接続制御ユニット、接続検知ユニット、および認証状態テーブルの一例にあたる。
【００３９】
図３は、図１に示した副端末７２～７４を構成している同軸ケーブルモデム７９～８１の内部構成図を示している。
【００４０】
同軸ケーブルモデム７９～８１は、通信Ｉ／Ｆ２１と同軸Ｉ／Ｆ２０とを備えており、双方のＩ／Ｆから受信したデータを所望のＩ／Ｆに転送する通信機器である。通信Ｉ／Ｆ２１は、例えばイーサネットなどの、同軸Ｉ／Ｆとは異なる通信Ｉ／Ｆである。また、同軸ケーブルモデム７９～８１は、自身が処理する制御を行う転送制御部２５を備えている。
【００４１】
同軸ケーブルモデム７９～８１は更に、通信Ｉ／Ｆ２１におけるデータの送受信を処理する通信送受信処理部２６と、同軸Ｉ／Ｆ２０におけるデータの送受信を処理する同軸送受信処理部２３を備えている。また、同軸ケーブルモデム７９～８１自身の機器認証を要求する際に必要な認証ＩＤを記憶する認証ＩＤ記憶部２８と、認証ＩＤを使用して認証要求データを作成する認証データ作成部２７と、認証サーバ７５からの認証応答データを解析する認証データ解析部２４と、同軸接続における動作周波数を制御する同軸周波数制御部２２を備えている。
【００４２】
次に、本実施の形態１の主端末７１における、主端末７１の配下に接続される副端末７２～７４の管理方法について説明する。
【００４３】
図４は、主端末７１が管理する、配下に接続される副端末７２～７４の認証時の状態遷移図を示している。図５（ａ）～（ｄ）は、主端末７１が認証状態記憶部１３で管理している、配下に接続された副端末７２の状態管理テーブル２９を示している。
【００４４】
以下に、主端末７１が動作している動作周波数に、副端末７２が新たに接続される場合を例に説明する。ここでは、副端末７２を構成している同軸ケーブルモデム７９のモデムＩＤ（ここではＭＡＣアドレスとする）を、００：９９：８８：７７：６６：５５とする。
【００４５】
まず、主端末７１の動作について説明する。
【００４６】

主端末７１は、図２に示す接続検知部１５が、同軸Ｉ／Ｆ１１に新たに副端末７２が接続されたことを検知すると、その接続情報を同軸制御部１４を介して認証状態記憶部１３に通知する。認証状態記憶部１３は、図５（ａ）に示すように、状態管理テーブル２９に同軸ケーブルモデム７９のモデムＩＤを登録し、図４に示すように、副端末７２の遷移状態を「認証要求待ち状態」３２にする。

【００４７】

なお、ここで状態管理テーブル２９に登録する同軸ケーブルモデム７９のモデムＩＤが、本発明の、副端末のＩＤ情報の一例にあたる。

【００４８】

更に認証状態記憶部１３は、認証サーバ７５がそのモデムＩＤ（００：９９：８８：７７：６６：５５）から作成する、許可および不許可のそれぞれを示す認証応答データと同じデータを算出し、状態管理テーブル２９の「応答値」にそれらの算出結果を登録する。ここでは、許可および不許可を示す認証応答データの値を、それぞれ、０ｘ２００６および０ｘ１０２９とする。これらの応答値の算出方法は、認証サーバ７５と主端末７１と同軸ケーブルモデム７９で共有されていれば良いため、ここでは特に記載しない。

【００４９】

この「認証要求待ち状態」３２で同軸ケーブルモデム７９のリンク接続が切れると、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図４の「未接続状態」３１とする。

【００５０】

次に、主端末７１に接続した副端末７２の動作について説明する。

【００５１】

主端末７１に接続した同軸ケーブルモデム７９は、自身の機器認証を行うために、認証データ作成部２７が、認証ＩＤ記憶部２８から認証ＩＤを取得して認証要求データを作成する。認証データ作成部２７が、作成した認証要求データの処理を同軸送受信処理部２３に依頼すると、同軸送受信処理部２３は、同軸ケーブル８５、分配器７８、同軸ケーブル８８および主端末７１を介して、その認証要求データを認証サーバ７５に対して送信する。同軸ケーブルモデム７９は、認証サーバ７５からの認証応答データを受信するまで認証要求データを再送する。

【００５２】

次に、同軸ケーブルモデム７９が認証要求データを送信した後の、主端末７１の動作について説明する。

【００５３】

主端末７１は、同軸送受信処理部１９が、同軸ケーブルモデム７９から送信されてきた認証要求データを同軸Ｉ／Ｆ１１を介して受信すると、転送制御部１７にその認証要求データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証要求データ）をスヌープして、認証データ解析部１２へ渡す。そして、通信送受信処理部１６によって、認証要求データは、そのまま通信Ｉ／Ｆ１０へ転送される。

【００５４】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。この場合の認証用データとは、認証要求データまたは認証応答データのことを言う。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【００５５】

新たに接続された同軸ケーブルモデム７９からの認証要求データだった場合は、認証状態記憶部１３は、状態管理テーブル２９の副端末７２の状態を、図５（ｂ）に示すように「認証応答待ち状態」３３に遷移させる。

【００５６】

更に認証状態記憶部１３は、同軸ケーブルモデム７９から受信した認証要求データから

、認証サーバ７５のアドレスと認証応答データのキーワードも抽出して、状態管理テーブル２９に同時に登録する。ここでは、認証サーバ７５のアドレスを「１９２．１６８．０．１０」、認証応答データのキーワードを「ｒｏｏｔｃｅｒｔ」とする。

【００５７】

もし、この「認証応答待ち状態」３３で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図４の「未接続状態」３１とする。

【００５８】

一方、この「認証応答待ち状態」３３で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証応答待ち状態」３３を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【００５９】

次に、認証サーバ７５の動作について説明する。

【００６０】

認証サーバ７５は、主端末７１によって転送されてきた同軸ケーブルモデム７９からの認証要求データを受信すると、同軸ケーブルモデム７９からの認証要求データに含まれる認証ＩＤが正しければ、モデムＩＤを基に認証許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。もし、認証ＩＤが正しくなければ、認証不許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。

【００６１】

このときに、認証サーバ７５で算出される認証許可および認証不許可を示す認証応答データは、主端末７１の認証状態記憶部１３が、同軸ケーブルモデム７９からの認証要求データを受信した際に算出して図５（ａ）の状態管理テーブル２９に登録したデータと同じデータである。

【００６２】

次に、認証サーバ７５が認証応答データを送信した後の、主端末７１の動作について説明する。

【００６３】

主端末７１は、通信送受信処理部１６が、認証サーバ７５から送信されてきた認証応答データを通信Ｉ／Ｆ１０を介して受信すると、転送制御部１７にその認証応答データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証応答データ）をスヌープして、認証データ解析部１２へ渡す。そして、同軸送受信処理部１９によって、認証応答データは、そのまま同軸Ｉ／Ｆ１１へ転送される。

【００６４】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【００６５】

認証応答データであった場合、認証状態記憶部１３は、どの副端末宛なのかを判断し、もし状態管理テーブル２９で管理している副端末７２に対する認証応答データであった場合、その認証応答データに含まれる送信元アドレス、認証データキーワードおよび応答値を、それぞれ、図５（ｂ）に示す状態管理テーブル２９に登録した認証サーバ７５のアドレス、キーワードおよび応答値と比較する。

【００６６】

もし、これらのうち一つでも一致しなかった場合は、何もしない。全てが一致して、応答値が「許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図５（ｃ）に示す「定常状態（認証完了状態）」３４に遷移させる。また、全てが

一致して、応答値が「不許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図５（ｄ）に示すように「不正／切断」３５に遷移させ、同軸制御部１４によって、対象となる同軸ケーブルモデム７９との接続を物理層で切断させる。

【００６７】

次に、主端末７１が認証サーバ７５からの認証応答データを転送した後の、同軸ケーブルモデム７９の動作について説明する。

【００６８】

同軸ケーブルモデム７９は、同軸送受信処理部２３が、主端末７１によって転送されてきた認証サーバ７５からの認証応答データを同軸Ｉ／Ｆ２０を介して受信すると、認証データ解析部２４へその認証応答データを渡す。

【００６９】

もし、認証応答データの応答値が「許可」の場合、認証データ解析部２４は、転送制御部２５へ転送開始を指示し、通信データの転送を開始し、同軸ケーブルモデム７９に接続されるユーザ端末８２の通信が可能になる。もし、認証応答データの応答値が「不許可」の場合、何もしない。すなわち、この場合、通信データの転送が不許可のままの状態となる。

【００７０】

次に、主端末７１における、「定常状態（認証完了状態）」３４に遷移した副端末７２の状態の管理方法について説明する。

【００７１】

もし、この「認証完了状態」３４で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図４の「未接続状態」３１とする。

【００７２】

一方、この「認証完了状態」３４で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証完了状態」３４を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【００７３】

なお、上記で説明した本実施の形態１では、主端末７１の接続検知部１５が同軸Ｉ／Ｆ１１に新たに副端末７２が接続されたことを検知し、副端末７２の遷移状態を「未接続状態」３１から「認証要求待ち状態」３２に遷移させる際に、認証状態記憶部１３が、認証サーバ７５が副端末７２に対して作成する許可および不許可のそれぞれを示す認証応答データを算出して状態管理テーブル２９の「応答値」に登録しておくこととしたが、これらの認証応答データをこのときに算出せずに、「認証応答待ち状態」３３で認証サーバ７５から副端末７２宛の認証応答データを受信した際に算出することとし、その算出した値とそのときに受信した認証応答データに含まれる応答値とを比較するようにしてもよい。

【００７４】

図１３に示す従来の通信システムでは、ＤＨＣＰサーバ１０２の認証処理の負荷を低減するために、登録アドレスリスト１０４に、予め正規のクライアント端末のＭＡＣアドレスを登録しておかなければならなかった。この方法では、例えばＤＨＣＰサーバ１０２の配下の無線クライアント端末が増加した場合など、その都度、アクセスポイント１０５内の登録アドレスリスト１０４を更新しなければならず、管理が煩雑となっていた。

【００７５】

本実施の形態１の認証システムでは、主端末７１が配下の副端末７２～７４および認証サーバ７５からの認証用データをスヌープして認証状態を管理することにより、もし副端末が不正であった場合、主端末７１が自動で不正端末として登録するため、予め正規端末などを登録する必要が無くなり、図１３に示すような従来の通信システムに比べて管理を簡素化できる。

【００７６】
また、正規の認証サーバ７５でなく不正なりすまし認証サーバが副端末７２の認証をしようとした場合には、そのなりすまし認証サーバからは、正規の認証サーバ７５から送信してくるはずの正しいキーワードおよび応答値を送信してこないと考えられる。本実施の形態１の認証システムでは、認証サーバ７５のアドレス、キーワードおよびシステムでユニークな応答値を比較することで、なりすまし認証サーバからの応答を防ぐことが可能になり、より強固なシステムを構築することが可能となる。本実施の形態１の認証システムの場合、認証応答データに含まれるキーワードや応答値が正しい値でない場合には、主端末７１も副端末７２も、その認証応答データが正規の認証サーバ７５からの認証応答データではないと判断し、その認証応答データを無視する。
【００７７】
また、本実施の形態１の認証システムでは、主端末７１が不正と判断し、「不正／切断」状態に遷移させるとその副端末のリンク確立は完全に不可能となるため、一度不許可になった副端末が認証サーバ７５に認証要求を送信することが無くなり、認証サーバ７５にかかる負荷を大幅に軽減することが可能になる。
【００７８】
（実施の形態２）
次に、本発明に関連する発明の実施の形態２の認証システムにおける主端末の、配下に接続される副端末の管理方法について説明する。
【００７９】
なお、本実施の形態２における認証システムの構成、主端末７１および副端末７２～７４の構成は、実施の形態１と同様で図１に示す通りである。
【００８０】
図６は、主端末７１が管理する、配下に接続される副端末７２～７４の認証時の状態遷移図を示している。図７（ａ）～（ｄ）は、主端末７１が認証状態記憶部１３で管理している、配下に接続された副端末７２～７４の状態管理テーブル２９を示している。
【００８１】
以下に、主端末７１が動作している動作周波数に、副端末７２が新たに接続される場合を例に説明する。ここでは、副端末７２を構成している同軸ケーブルモデム７９のモデムＩＤ（ここではＭＡＣアドレスとする）を、００：９９：８８：７７：６６：５５とする。
【００８２】
まず、主端末７１の動作について説明する。
【００８３】
主端末７１は、図２に示す接続検知部１５が、同軸Ｉ／Ｆ１１に新たに副端末７２が接続されたことを検知すると、その接続情報を同軸制御部１４を介して認証状態記憶部１３に通知する。認証状態記憶部１３は、図７（ａ）に示すように、状態管理テーブル２９に同軸ケーブルモデム７９のモデムＩＤを登録し、図４に示すように、副端末７２の遷移状態を「認証要求待ち状態」４２にする。
【００８４】
更に認証状態記憶部１３は、認証サーバ７５がそのモデムＩＤ（００：９９：８８：７７：６６：５５）から作成する、許可および不許可のそれぞれを示す認証応答データと同じデータを算出し、状態管理テーブル２９の「応答値」にそれらの算出結果を登録する。ここでは、許可および不許可を示す認証応答データの値を、それぞれ、０ｘ２００６および０ｘ１０２９とする。これらの応答値の算出方法は、認証サーバ７５と主端末７１と同軸ケーブルモデム７９で共有されていれば良いため、ここでは特に記載しない。
【００８５】
更に、主端末７１は、新たに配下に接続された同軸ケーブルモデム７９が認証要求データを送信してくるであろう最大の認証要求タイムアウト時間（１５０秒）も、図７（ａ）に示すように状態管理テーブル２９に登録する。この状態管理テーブル２９に登録した認

証要求タイムアウト時間は、カウントダウンされていき、配下の同軸ケーブルモデム７９が認証要求データを再送するたびに１５０秒に更新される。ここで、最大の認証要求タイムアウト時間を１５０秒としたが、この値はシステムによって最適な時間になることは言うまでもない。

【００８６】

主端末７１の認証状態記憶部１３は、新たに接続された同軸ケーブルモデム７９からの認証要求データを最大の認証要求タイムアウト時間（１５０秒）内に受信しなかった場合には、その副端末７２が正規の認証シーケンスに則っていない不正な端末と判断し、副端末７２の状態管理テーブル２９の状態を図７（ｄ）に示すように「不正／切断」４５に遷移させ、同軸制御部１４によって、対象となる同軸ケーブルモデム７９との接続を物理層で切断させる。

【００８７】

「認証要求待ち状態」４２で、同軸ケーブルモデム７９のリンク接続が最大の認証要求タイムアウト時間（１５０秒）内に切れた場合には、認証状態記憶部１３は状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図６の「未接続状態」４１とする。

【００８８】

次に、主端末７１に接続した副端末７２の動作について説明する。

【００８９】

主端末７１に接続した同軸ケーブルモデム７９は、自身の機器認証を行うために、認証データ作成部２７が、認証ＩＤ記憶部２８から認証ＩＤを取得して認証要求データを作成する。認証データ作成部２７が、作成した認証要求データの処理を同軸送受信処理部２３に依頼すると、同軸送受信処理部２３は、同軸ケーブル８５、分配器７８、同軸ケーブル８８および主端末７１を介して、その認証要求データを認証サーバ７５に対して送信する。同軸ケーブルモデム７９は、認証サーバ７５からの認証応答データを受信するまで認証要求データを再送する。

【００９０】

次に、同軸ケーブルモデム７９が認証要求データを送信した後の、主端末７１の動作について説明する。

【００９１】

主端末７１は、同軸送受信処理部１９が、同軸ケーブルモデム７９から送信されてきた認証要求データを同軸Ｉ／Ｆ１１を介して受信すると、転送制御部１７にその認証要求データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証要求データ）をスヌープして、認証データ解析部１２へ渡す。そして、通信送受信処理部１６によって、認証要求データは、そのまま通信Ｉ／Ｆ１０へ転送される。

【００９２】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【００９３】

新たに接続された同軸ケーブルモデム７９からの認証要求データだった場合は、認証状態記憶部１３は、状態管理テーブル２９の副端末７２の状態を、図７（ｂ）に示すように「認証応答待ち状態」４３に遷移させる。

【００９４】

更に認証状態記憶部１３は、同軸ケーブルモデム７９から受信した認証要求データから、認証サーバ７５のアドレスと認証応答データのキーワードも抽出して、状態管理テーブル２９に同時に登録する。ここでは、認証サーバ７５のアドレスを「１９２．１６８．０．１０」、認証応答データのキーワードを「ｒｏｏｔｃｅｒｔ」とする。

【００９５】

もし、この「認証応答待ち状態」４３で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図６の「未接続状態」４１とする。

【００９６】

一方、この「認証応答待ち状態」４３で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証応答待ち状態」４３を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【００９７】

次に、認証サーバ７５の動作について説明する。

【００９８】

認証サーバ７５は、主端末７１によって転送されてきた同軸ケーブルモデム７９からの認証要求データを受信すると、同軸ケーブルモデム７９からの認証要求データに含まれる認証ＩＤが正しければ、モデムＩＤを基に認証許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。もし、認証ＩＤが正しくなければ、認証不許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。

【００９９】

このときに、認証サーバ７５で算出される認証許可および認証不許可を示す認証応答データは、主端末７１の認証状態記憶部１３が、同軸ケーブルモデム７９からの認証要求データを受信した際に算出して図７（ａ）の状態管理テーブル２９に登録したデータと同じデータである。

【０１００】

次に、認証サーバ７５が認証応答データを送信した後の、主端末７１の動作について説明する。

【０１０１】

主端末７１は、通信送受信処理部１６が、認証サーバ７５から送信されてきた認証応答データを通信Ｉ／Ｆ１０を介して受信すると、転送制御部１７にその認証応答データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証応答データ）をスヌープして、認証データ解析部１２へ渡す。そして、同軸送受信処理部１９によって、認証応答データは、そのまま同軸Ｉ／Ｆ１１へ転送される。

【０１０２】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【０１０３】

認証応答データであった場合、認証状態記憶部１３は、どの副端末宛なのかを判断し、もし状態管理テーブル２９で管理している副端末７２に対する認証応答データであった場合、その認証応答データに含まれる送信元アドレス、認証データキーワードおよび応答値を、それぞれ、図７（ｂ）に示す状態管理テーブル２９に登録した認証サーバ７５のアドレス、キーワードおよび応答値と比較する。

【０１０４】

もし、これらのうち一つでも一致しなかった場合は、何もしない。全てが一致して、応答値が「許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図７（ｃ）に示す「定常状態（認証完了状態）」４４に遷移させる。また、全てが一致して、応答値が「不許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図７（ｄ）に示すように「不正／切断」４５に遷移させ、同軸制御部１４によって、対象となる同軸ケーブルモデム７９との接続を物理層で切断させる。

【０１０５】

次に、主端末７１が認証サーバ７５からの認証応答データを転送した後の、同軸ケーブルモデム７９の動作について説明する。

【０１０６】

同軸ケーブルモデム７９は、同軸送受信処理部２３が、主端末７１によって転送されてきた認証サーバ７５からの認証応答データを同軸Ｉ／Ｆ２０を介して受信すると、認証データ解析部２４へその認証応答データを渡す。

【０１０７】

もし、認証応答データの応答値が「許可」の場合、認証データ解析部２４は、転送制御部２５へ転送開始を指示し、通信データの転送を開始し、同軸ケーブルモデム７９に接続されるユーザ端末８２の通信が可能になる。もし、認証応答データの応答値が「不許可」の場合、何もしない。すなわち、この場合、通信データの転送が不許可のままの状態となる。

【０１０８】

次に、主端末７１における、「定常状態（認証完了状態）」４４に遷移した副端末７２の状態の管理方法について説明する。

【０１０９】

もし、この「認証完了状態」４４で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図６の「未接続状態」４１とする。

【０１１０】

一方、この「認証完了状態」４４で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証完了状態」４４を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【０１１１】

本実施の形態２の認証システムは、主端末７１が配下の副端末７２～７４および認証サーバ７５からの認証用データをスヌープして認証状態を管理することにより、もし副端末が不正であった場合や、副端末が認証を行わない等の正規の認証シーケンスを取らないような、海賊版の副端末が接続された場合に対しても主端末７１が自動で不正端末を登録するため、予め正規端末などを登録する必要が無くなり、管理を簡素化できる。

【０１１２】

また、認証サーバ７５のアドレス、キーワードおよびシステムでユニークな応答値を比較することで、なりすまし認証サーバからの応答を防ぐことが可能になり、より強固なシステムを構築することが可能となる。

【０１１３】

また、主端末７１が不正と判断し、「不正／切断」状態に遷移させるとその副端末のリンク確立は完全に不可能となるため、一度不許可になった副端末が認証サーバ７５に認証要求を送信することが無くなり、認証サーバ７５にかかる負荷を大幅に軽減することが可能になる。

【０１１４】

（実施の形態３）

次に、本発明の実施の形態３の認証システムにおける主端末の、配下に接続される副端末の管理方法について説明する。

【０１１５】

なお、本実施の形態３における認証システムの構成、主端末７１および副端末７２～７４の構成は、実施の形態１と同様で図１に示す通りである。

【０１１６】

図８は、主端末７１が管理する、配下に接続される副端末７２～７４の認証時の状態遷移図を示している。図９（ａ）～（ｅ）は、主端末７１が認証状態記憶部１３で管理して

いる、配下に接続された副端末７２～７４の状態管理テーブル２９を示している。

【０１１７】

以下に、主端末７１が動作している動作周波数に、副端末７２が新たに接続される場合を例に説明する。ここでは、副端末７２を構成している同軸ケーブルモデム７９のモデムＩＤ（ここではＭＡＣアドレスとする）を、００：９９：８８：７７：６６：５５とする。

【０１１８】

まず、主端末７１の動作について説明する。

【０１１９】

主端末７１は、図２に示す接続検知部１５が、同軸Ｉ／Ｆ１１に新たに副端末７２が接続されたことを検知すると、その接続情報を同軸制御部１４を介して認証状態記憶部１３に通知する。認証状態記憶部１３は、図９（ａ）に示すように、状態管理テーブル２９に同軸ケーブルモデム７９のモデムＩＤを登録し、図８に示すように、副端末７２の遷移状態を「認証要求待ち状態」５２にする。

【０１２０】

更に認証状態記憶部１３は、認証サーバ７５がそのモデムＩＤ（００：９９：８８：７７：６６：５５）から作成する、許可および不許可のそれぞれを示す認証応答データと同じデータを算出し、状態管理テーブル２９の「応答値」にそれらの算出結果を登録する。ここでは、許可および不許可を示す認証応答データの値を、それぞれ、０ｘ２００６および０ｘ１０２９とする。これらの応答値の算出方法は、認証サーバ７５と主端末７１と同軸ケーブルモデム７９で共有されていれば良いため、ここでは特に記載しない。

【０１２１】

更に、認証状態記憶部１３は、新たに配下に接続された同軸ケーブルモデム７９が認証要求データを送信してくるであろう最大の認証要求タイムアウト時間（１５０秒）も、図９（ａ）に示すように状態管理テーブル２９に登録する。この状態管理テーブル２９に登録した認証要求タイムアウト時間は、カウントダウンされていき、配下の同軸ケーブルモデム７９が認証要求データを再送するたびに１５０秒に更新される。ここで、最大の認証要求タイムアウト時間を１５０秒としたが、この値はシステムによって最適な時間になることは言うまでもない。

【０１２２】

主端末７１の認証状態記憶部１３は、新たに接続された同軸ケーブルモデム７９からの認証要求データを最大の認証要求タイムアウト時間（１５０秒）内に受信しなかった場合には、その副端末７２が正規の認証シーケンスに則っていない不正な端末と判断し、副端末７２の状態管理テーブル２９の状態を図９（ｅ）に示すように「不正／切断」５５に遷移させ、同軸制御部１４によって、対象となる同軸ケーブルモデム７９との接続を物理層で切断させる。

【０１２３】

「認証要求待ち状態」５２で、同軸ケーブルモデム７９のリンク接続が最大の認証要求タイムアウト時間（１５０秒）内に切れた場合には、認証状態記憶部１３は状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図８の「未接続状態」５１とする。

【０１２４】

次に、主端末７１に接続した副端末７２の動作について説明する。

【０１２５】

主端末７１に接続した同軸ケーブルモデム７９は、自身の機器認証を行うために、認証データ作成部２７が、認証ＩＤ記憶部２８から認証ＩＤを取得して認証要求データを作成する。認証データ作成部２７が、作成した認証要求データの処理を同軸送受信処理部２３に依頼すると、同軸送受信処理部２３は、同軸ケーブル８５、分配器７８、同軸ケーブル８８および主端末７１を介して、その認証要求データを認証サーバ７５に対して送信する。

【０１２６】
同軸ケーブルモデム７９の転送制御部２５は、同軸送受信処理部２３が認証サーバ７５からの認証応答データを規定時間（例えば５秒間）内に受信しなかった場合には、認証要求データを同軸送受信処理部２３によって認証サーバ７５に再送させる。さらに、転送制御部２５は、認証応答データの再送が規定回数（例えば５回）を超えると、同軸周波数制御部２２に周波数サーチを行わせて、主端末７１が使用する動作周波数と異なる動作周波数を使用している他の主端末の配下に接続に行かせる。
【０１２７】
なお、同軸周波数制御部２２が、本発明の周波数制御ユニットの一例にあたる。
【０１２８】
次に、同軸ケーブルモデム７９が認証要求データを送信した後の、主端末７１の動作について説明する。
【０１２９】
主端末７１は、同軸送受信処理部１９が、同軸ケーブルモデム７９から送信されてきた認証要求データを同軸Ｉ／Ｆ１１を介して受信すると、転送制御部１７にその認証要求データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証要求データ）をスヌープして、認証データ解析部１２へ渡す。そして、通信送受信処理部１６によって、認証要求データは、そのまま通信Ｉ／Ｆ１０へ転送される。
【０１３０】
認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。
【０１３１】
新たに接続された同軸ケーブルモデム７９からの認証要求データだった場合は、認証状態記憶部１３は、状態管理テーブル２９の副端末７２の状態を、図９（ｂ）に示すように「認証応答待ち状態」５３に遷移させる。
【０１３２】
更に、認証状態記憶部１３は、新たに配下に接続された同軸ケーブルモデム７９が認証要求データを送信してから認証サーバ７５からの認証応答データが来なかった場合に、同軸ケーブルモデム７９が認証応答タイムアウトするであろう時間（認証応答タイムアウト５秒×再送５回＋マージン＝３０秒）を図９（ｂ）に示すように登録する。ここでは、認証応答タイムアウト時間を３０秒間としたが、認証応答タイムアウト時間はシステムに最適な値であれば良いことは言うまでもない。
【０１３３】
なお、認証応答タイムアウト時間が、本発明の認証応答タイムアウト期間の一例にあたる。
【０１３４】
もし、この「認証応答待ち状態」５３で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図８の「未接続状態」５１とする。
【０１３５】
一方、この「認証応答待ち状態」５３で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証応答待ち状態」５３を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。
【０１３６】
次に、認証サーバ７５の動作について説明する。
【０１３７】

認証サーバ７５は、主端末７１によって転送されてきた同軸ケーブルモデム７９からの認証要求データを受信すると、同軸ケーブルモデム７９からの認証要求データに含まれる認証ＩＤが正しければ、モデムＩＤを基に認証許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。もし、認証ＩＤが正しくなければ、認証不許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。

【０１３８】

このときに、認証サーバ７５で算出される認証許可および認証不許可を示す認証応答データは、主端末７１の認証状態記憶部１３が、同軸ケーブルモデム７９からの認証要求データを受信した際に算出して図９（ａ）の状態管理テーブル２９に登録したデータと同じデータである。

【０１３９】

次に、認証サーバ７５が認証応答データを送信した後の、主端末７１の動作について説明する。

【０１４０】

主端末７１は、通信送受信処理部１６が、認証サーバ７５から送信されてきた認証応答データを通信Ｉ／Ｆ１０を介して受信すると、転送制御部１７にその認証応答データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証応答データ）をスヌープして、認証データ解析部１２へ渡す。そして、同軸送受信処理部１９によって、認証応答データは、そのまま同軸Ｉ／Ｆ１１へ転送される。

【０１４１】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【０１４２】

認証応答データであった場合、認証状態記憶部１３は、どの副端末宛なのかを判断し、もし状態管理テーブル２９で管理している副端末７２に対する認証応答データであった場合、その認証応答データに含まれる送信元アドレス、認証データキーワードおよび応答値を、それぞれ、図７（ｂ）に示す状態管理テーブル２９に登録した認証サーバ７５のアドレス、キーワードおよび応答値と比較する。

【０１４３】

もし、これらのうち一つでも一致しなかった場合は、何もしない。全てが一致して、応答値が「許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図９（ｄ）に示す「定常状態（認証完了状態）」５４に遷移させる。

【０１４４】

また、全てが一致して、応答値が「不許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図９（ｃ）に示すように「サーチ待ち状態」５６に遷移させる。それとともに、正規の副端末であれば「不許可」の認証応答データを受信した後に少なくともその時間内に周波数サーチに行くであろうサーチタイムアウト時間（ここでは５秒）も、状態管理テーブル２９に設定する。

【０１４５】

なお、この場合のサーチアウトタイム時間が、本発明の不許可受信タイムアウト期間の一例にあたる。

【０１４６】

また、図９（ｂ）に示すように「認証応答待ち状態」５３に遷移させた際に状態管理テーブル２９に設定した、同軸ケーブルモデム７９が認証応答タイムアウトするであろう時間（この例では、３０秒間に設定）を超えても、認証サーバ７５からの認証応答データが来ない場合には、認証状態記憶部１３は、副端末７２が認証応答タイムアウトしたと判断して、副端末７２の状態管理テーブル２９の状態を、図９（ｃ）に示すように「サーチ待ち状態（５６）」に遷移させる。それとともに、正規の副端末であれば認証応答タイムア

ウトした後に少なくともその時間内に周波数サーチに行くであろうサーチタイムアウト時間（ここでは５秒）も、状態管理テーブル２９に設定する。

【０１４７】

なお、ここでは、サーチタイムアウト時間を５秒間としたが、サーチタイムアウト時間はシステムに最適な値であれば良いことは言うまでもない。

【０１４８】

認証結果が「不許可」の認証応答データを受信した際に、周波数サーチに行かずサーチタイムアウト時間（５秒）以上主端末７１に接続し続けている副端末、および、認証応答データが来ずに認証応答タイムアウト時間（３０秒）を超えた際に、周波数サーチに行かずサーチタイムアウト時間（５秒）以上主端末７１に接続し続けている副端末を、認証状態記憶部１３は、正規の認証シーケンスに則っていない不正な端末と判断し、それらの副端末の状態管理テーブル２９の状態を、図９（ｅ）に示すように「不正／切断」５５に遷移させ、同軸制御部１４によって、対象となる副端末との接続を物理層で切断させる。

【０１４９】

「サーチ待ち状態」５６で、サーチタイムアウト時間（５秒）内に副端末が周波数サーチに行き、リンクが切断された場合には、認証状態記憶部１３は、その副端末を正規の端末と判断し、状態管理テーブル２９から副端末を削除する。すなわち、実際には管理しない状態である図８の「未接続状態」５１とする。

【０１５０】

このように、サーチタイムアウト時間を用いることにより、正規のシーケンスでリンクの切断をしない副端末は不正な端末として取り扱うとともに、異なる周波数を利用する他の主端末に属する正規の副端末が間違って接続してきたような場合のその副端末は不正な副端末としては取り扱わないようにできる。

【０１５１】

次に、主端末７１が認証サーバ７５からの認証応答データを転送した後の、同軸ケーブルモデム７９の動作について説明する。

【０１５２】

同軸ケーブルモデム７９は、同軸送受信処理部２３が、主端末７１によって転送されてきた認証サーバ７５からの認証応答データを同軸Ｉ／Ｆ２０を介して受信すると、認証データ解析部２４へその認証応答データを渡す。

【０１５３】

もし、認証応答データの応答値が「許可」の場合、認証データ解析部２４は、転送制御部２５へ転送開始を指示し、通信データの転送を開始し、同軸ケーブルモデム７９に接続されるユーザ端末８２の通信が可能になる。もし、認証応答データの応答値が「不許可」の場合、同軸周波数制御部２２が周波数サーチを行い、主端末７１が使用している動作周波数と異なる動作周波数を使用している他の主端末の配下に接続に行く。

【０１５４】

次に、主端末７１における、「定常状態（認証完了状態）」５４に遷移した副端末７２の状態の管理方法について説明する。

【０１５５】

もし、この「認証完了状態」５４で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図８の「未接続状態」５１とする。

【０１５６】

一方、この「認証完了状態」５４で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証完了状態」５４を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【０１５７】

本実施の形態３の認証システムは、主端末７１が配下の副端末７２～７４および認証サーバ７５からの認証用データをスヌープして認証状態を管理することにより、もし副端末が不正であった場合や、副端末が認証を行わない等の正規の認証シーケンスを取らないような、海賊版の副端末が接続された場合に対しても主端末７１が自動で不正端末を登録するため、予め正規端末などを登録する必要が無くなり、管理を簡素化できる。

【０１５８】

また、副端末が認証シーケンスにおいて認証応答タイムアウトや不許可応答などのエラー状態になった場合に自動で周波数サーチを行うことにより、副端末が別システムに入ってしまった場合の回避を自動で行うことができるため、主端末７１は、別システムの副端末を不正な端末として管理しなくとも良く、本当に不正な端末の管理で済むため、主端末７１の負荷も軽減することが可能になる。

【０１５９】

また、認証サーバ７５のアドレス、キーワードおよびシステムでユニークな応答値を比較することで、なりすまし認証サーバからの応答を防ぐことが可能になり、より強固なシステムを構築することが可能となる。

【０１６０】

また、主端末７１が不正と判断し、「不正／切断」状態に遷移させるとその副端末のリンク確立は完全に不可能となるため、一度不許可になった副端末が認証サーバ７５に認証要求を送信することが無くなり、認証サーバ７５にかかる負荷を大幅に軽減することが可能になる。

【０１６１】

（実施の形態４）

次に、本発明の実施の形態４の認証システムにおける主端末の、配下に接続される副端末の管理方法について説明する。

【０１６２】

なお、本実施の形態４における認証システムの構成、主端末７１および副端末７２～７４の構成は、実施の形態１と同様で図１に示す通りである。

【０１６３】

図１０は、主端末７１が管理する、配下に接続される副端末７２～７４の認証時の状態遷移図を示している。図１１（ａ）～（ｄ）は、主端末７１が認証状態記憶部１３で管理している、配下に接続された副端末７２～７４の状態管理テーブル２９を示している。

【０１６４】

以下に、主端末７１が動作している動作周波数に、副端末７２が新たに接続される場合を例に説明する。ここでは、副端末７２を構成している同軸ケーブルモデム７９のモデムＩＤ（ここではＭＡＣアドレスとする）を、００：９９：８８：７７：６６：５５とする。

【０１６５】

まず、主端末７１の動作について説明する。

【０１６６】

主端末７１は、図２に示す接続検知部１５が、同軸Ｉ／Ｆ１１に新たに副端末７２が接続されたことを検知すると、その接続情報を同軸制御部１４を介して認証状態記憶部１３に通知する。認証状態記憶部１３は、図１１（ａ）に示すように、状態管理テーブル２９に同軸ケーブルモデム７９のモデムＩＤを登録し、図１０に示すように、副端末７２の遷移状態を「認証要求待ち状態」６２にする。

【０１６７】

更に認証状態記憶部１３は、認証サーバ７５がそのモデムＩＤ（００：９９：８８：７７：６６：５５）から作成する、許可および不許可のそれぞれを示す認証応答データと同じデータを算出し、状態管理テーブル２９の「応答値」にそれらの算出結果を登録する。ここでは、許可および不許可を示す認証応答データの値を、それぞれ、０ｘ２００６および０ｘ１０２９とする。これらの応答値の算出方法は、認証サーバ７５と主端末７１と同

軸ケーブルモデム７９で共有されていれば良いため、ここでは特に記載しない。

【０１６８】

更に、主端末７１の認証状態記憶部１３は、新たに配下に接続された副端末７２に対して、認証用に通信速度を制限する。認証状態記憶部１３は、図１１（ａ）に示すように状態管理テーブル２９に認証用の速度制限（ここでは１Ｍｂｐｓ）を設定するとともに、同軸制御部１４に対して、同軸Ｉ／Ｆ１１に接続される副端末７２との通信速度を１Ｍｂｐｓとする設定をする。ここでは、認証用速度制限設定を１Ｍｂｐｓとしたが、認証用速度制限設定はシステムに最適な値であれば良いことは言うまでもない。

【０１６９】

なお、同軸制御部１４が、本発明の速度制限ユニットの一例にあたる。

【０１７０】

更に、認証状態記憶部１３は、新たに配下に接続された同軸ケーブルモデム７９が認証要求データを送信してくるであろう最大の認証要求タイムアウト時間（１５０秒）も、図１１（ａ）に示すように状態管理テーブル２９に登録する。この状態管理テーブル２９に登録した認証要求タイムアウト時間は、カウントダウンされていき、配下の同軸ケーブルモデム７９が認証要求データを再送するたびに１５０秒に更新される。ここで、最大の認証要求タイムアウト時間を１５０秒としたが、この値はシステムによって最適な時間になることは言うまでもない。

【０１７１】

主端末７１の認証状態記憶部１３は、新たに接続された同軸ケーブルモデム７９からの認証要求データを最大の認証要求タイムアウト時間（１５０秒）内に受信しなかった場合には、その副端末７２が正規の認証シーケンスに則っていない不正な端末と判断し、副端末７２の状態管理テーブル２９の状態を図１１（ｄ）に示すように「不正／切断」６５に遷移させ、同軸制御部１４によって、対象となる同軸ケーブルモデム７９との接続を物理層で切断させる。また、このとき、副端末７２に対する認証用速度制限設定も解除する。

【０１７２】

「認証要求待ち状態」６２で、同軸ケーブルモデム７９のリンク接続が最大の認証要求タイムアウト時間（１５０秒）内に切れた場合には、認証状態記憶部１３は状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図１０の「未接続状態」６１とする。また、このとき、副端末７２に対する認証用速度制限設定も解除する。

【０１７３】

次に、主端末７１に接続した副端末７２の動作について説明する。

【０１７４】

主端末７１に接続した同軸ケーブルモデム７９は、自身の機器認証を行うために、認証データ作成部２７が、認証ＩＤ記憶部２８から認証ＩＤを取得して認証要求データを作成する。認証データ作成部２７が、作成した認証要求データの処理を同軸送受信処理部２３に依頼すると、同軸送受信処理部２３は、同軸ケーブル８５、分配器７８、同軸ケーブル８８および主端末７１を介して、その認証要求データを認証サーバ７５に対して送信する。

【０１７５】

同軸ケーブルモデム７９の転送制御部２５は、同軸送受信処理部２３が認証サーバ７５からの認証応答データを規定時間（例えば５秒間）内に受信しなかった場合には、認証要求データを同軸送受信処理部２３によって認証サーバ７５に再送させる。さらに、転送制御部２５は、認証応答データの再送が規定回数（例えば５回）を超えると、同軸周波数制御部２２に周波数サーチを行わせて、主端末７１が使用する動作周波数と異なる動作周波数を使用している他の主端末の配下に接続に行かせる。

【０１７６】

次に、同軸ケーブルモデム７９が認証要求データを送信した後の、主端末７１の動作について説明する。

【０１７７】
主端末７１は、同軸送受信処理部１９が、同軸ケーブルモデム７９から送信されてきた認証要求データを同軸Ｉ／Ｆ１１を介して受信すると、転送制御部１７にその認証要求データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証要求データ）をスヌープして、認証データ解析部１２へ渡す。そして、通信送受信処理部１６によって、認証要求データは、そのまま通信Ｉ／Ｆ１０へ転送される。
【０１７８】
認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。
【０１７９】
新たに接続された同軸ケーブルモデム７９からの認証要求データだった場合は、認証状態記憶部１３は、状態管理テーブル２９の副端末７２の状態を、図１１（ｂ）に示すように「認証応答待ち状態」６３に遷移させる。このとき、副端末７２に対する認証用速度制限設定はそのまま維持する。
【０１８０】
更に、認証状態記憶部１３は、新たに配下に接続された同軸ケーブルモデム７９が認証要求データを送信してから認証サーバ７５からの認証応答データが来なかった場合に、同軸ケーブルモデム７９が認証応答タイムアウトするであろう時間（認証応答タイムアウト５秒×再送５回＋マージン＝３０秒）を図１１（ｂ）に示すように登録する。ここでは、認証応答タイムアウト時間を３０秒間としたが、認証応答タイムアウト時間はシステムに最適な値であれば良いことは言うまでもない。
【０１８１】
もし、この「認証応答待ち状態」６３で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図１０の「未接続状態」６１とする。
【０１８２】
一方、この「認証応答待ち状態」６３で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証応答待ち状態」６３を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。
【０１８３】
次に、認証サーバ７５の動作について説明する。
【０１８４】
認証サーバ７５は、主端末７１によって転送されてきた同軸ケーブルモデム７９からの認証要求データを受信すると、同軸ケーブルモデム７９からの認証要求データに含まれる認証ＩＤが正しければ、モデムＩＤを基に認証許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。もし、認証ＩＤが正しくなければ、認証不許可の認証応答データを算出し、副端末７２に対してその認証応答データを送信する。
【０１８５】
このときに、認証サーバ７５で算出される認証許可および認証不許可を示す認証応答データは、主端末７１の認証状態記憶部１３が、同軸ケーブルモデム７９からの認証要求データを受信した際に算出して図１１（ａ）の状態管理テーブル２９に登録したデータと同じデータである。
【０１８６】
次に、認証サーバ７５が認証応答データを送信した後の、主端末７１の動作について説明する。
【０１８７】

主端末７１は、通信送受信処理部１６が、認証サーバ７５から送信されてきた認証応答データを通信Ｉ／Ｆ１０を介して受信すると、転送制御部１７にその認証応答データを渡す。転送制御部１７の通信データスヌープ部１８は、通信データ（この場合は、認証応答データ）をスヌープして、認証データ解析部１２へ渡す。そして、同軸送受信処理部１９によって、認証応答データは、そのまま同軸Ｉ／Ｆ１１へ転送される。

【０１８８】

認証データ解析部１２は、通信データスヌープ部１８から渡された通信データが、認証用データであるかどうかを判断する。もし、認証用データで無ければ何もしない。認証用データであった場合は、認証要求データであるか、認証応答データであるかどうかを判断する。

【０１８９】

認証応答データであった場合、認証状態記憶部１３は、どの副端末宛なのかを判断し、もし状態管理テーブル２９で管理している副端末７２に対する認証応答データであった場合、その認証応答データに含まれる送信元アドレス、認証データキーワードおよび応答値を、それぞれ、図７（ｂ）に示す状態管理テーブル２９に登録した認証サーバ７５のアドレス、キーワードおよび応答値と比較する。

【０１９０】

もし、これらのうち一つでも一致しなかった場合は、何もしない。全てが一致して、応答値が「許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図１１（ｄ）に示す「定常状態（認証完了状態）」６４に遷移させる。また、このとき、認証状態記憶部１３は、副端末７２に対する認証用速度制限設定を解除し、運用速度保証、運用速度制限の設定があれば、図１１（ｃ）に示されるようにその設定を副端末７２に対して行う。

【０１９１】

また、全てが一致して、応答値が「不許可」の場合、認証状態記憶部１３は、副端末７２の状態管理テーブル２９の状態を、図１１（ａ）に示すように再度「認証要求待ち状態」６２に遷移させる。それとともに、同軸ケーブルモデム７９が認証要求データを送信してくるであろう最大の認証要求タイムアウト時間（１５０秒）も、図１１（ａ）に示すように登録する。ここでは、最大の認証要求タイムアウト時間を１５０秒間としたが、この値はシステムに最適な値であれば良いことは言うまでもない。ここで再度、「認証要求待ち状態」６２に戻すのは、正規の副端末であれば、「不許可」の認証応答データを受信した際には周波数サーチに行く為、リンクが切れて「未接続状態」６１に遷移するので問題がなく、一方、不正な副端末であれば、周波数サーチに行かないので、認証要求データタイムアウトで「不正／切断状態」６５に陥り、結果的に不正な副端末を防ぐことが可能だからである。

【０１９２】

次に、主端末７１が認証サーバ７５からの認証応答データを転送した後の、同軸ケーブルモデム７９の動作について説明する。

【０１９３】

同軸ケーブルモデム７９は、同軸送受信処理部２３が、主端末７１によって転送されてきた認証サーバ７５からの認証応答データを同軸Ｉ／Ｆ２０を介して受信すると、認証データ解析部２４へその認証応答データを渡す。

【０１９４】

もし、認証応答データの応答値が「許可」の場合、認証データ解析部２４は、転送制御部２５へ転送開始を指示し、通信データの転送を開始し、同軸ケーブルモデム７９に接続されるユーザ端末８２の通信が可能になる。もし、認証応答データの応答値が「不許可」の場合、同軸周波数制御部２２が周波数サーチを行い、主端末７１が使用している動作周波数と異なる動作周波数を使用している他の主端末の配下に接続に行く。

【０１９５】

次に、主端末７１における、「定常状態（認証完了状態）」６４に遷移した副端末７２

の状態の管理方法について説明する。

【０１９６】

もし、この「認証完了状態」６４で同軸ケーブルモデム７９のリンク接続がＸ秒間連続して切れた場合、主端末７１の認証状態記憶部１３は、状態管理テーブル２９から副端末７２を削除する。すなわち、実際には管理しない状態である図１０の「未接続状態」６１とする。

【０１９７】

一方、この「認証完了状態」６４で同軸ケーブルモデム７９のリンク接続が切れても、一定時間（Ｘ秒）内で再接続した場合には、主端末７１の認証状態記憶部１３は、状態管理テーブル２９の「認証完了状態」６４を保つ。ここでの一定時間（Ｘ秒）とは、システムに最適な値であれば良いことは言うまでもない。

【０１９８】

本実施の形態４の認証システムは、主端末７１が配下の副端末７２～７４および認証サーバ７５からの認証用データをスヌープして認証状態を管理することにより、もし副端末が不正であった場合や、副端末が認証を行わない等の正規の認証シーケンスを取らないような、海賊版の副端末が接続された場合に対しても主端末７１が自動で不正端末を登録するため、予め正規端末などを登録する必要が無くなり、管理を簡素化できる。

【０１９９】

また、副端末が認証シーケンスにおいて認証応答タイムアウトや不許可応答などのエラー状態になった場合に自動で周波数サーチを行うことにより、副端末が別システムに入ってしまった場合の回避を自動で行うことができるため、主端末７１は、別システムの副端末を不正な端末として管理しなくとも良く、本当に不正な端末の管理で済むため、主端末７１の負荷も軽減することが可能になる。また、認証サーバ７５のアドレス、キーワードおよびシステムでユニークな応答値を比較することで、なりすまし認証サーバからの応答を防ぐことが可能になり、より強固なシステムを構築することが可能になる。

【０２００】

また、主端末７１が不正と判断し、「不正／切断」状態に遷移させると副端末のリンク確立は完全に不可能となるため、一度不許可になった副端末が認証サーバ７５に認証要求を送信することが無くなるため、認証サーバ７５にかかる負荷を大幅に軽減することが可能になる。

【０２０１】

また、認証中の副端末に対して認証用速度制限設定を行うことにより、認証するのに必要最低限の帯域を割り当てるだけで済むため、認証が完了した正規の副端末の帯域に対する影響が軽減される。

【０２０２】

（実施の形態５）

図１２は、本発明に関連する発明の実施の形態５の認証システムの主端末の内部構成図を示している。

【０２０３】

本実施の形態５の認証システムの構成は、実施の形態１～４と同様であり、図１に示す通りである。実施の形態１～４とは、主端末の構成のみが異なる。図１２において、図２と同じ構成部分には、同じ符号を用いている。以下には、図２の主端末７１と異なる構成部分およびそれらの動作について説明する。

【０２０４】

本実施の形態５の主端末９１は、図２の主端末７１の構成に加えて、認証データ作成部９２、認証ＩＤ記憶部９３、不正端末通知部９４、および認証管理実施要否設定部９５を備えている。

【０２０６】

認証管理実施要否設定部９５は、実施の形態１～４で主端末７１が行っていた認証管理の処理を、主端末９１が実施するか否かの設定を行う。認証管理実施要否設定部９５が「

認証管理実施」に設定されている場合には、主端末９１は認証管理の処理を行うが、「認証管理不実施」に設定されている場合には、主端末９１は認証管理の処理を行わず、転送制御の処理のみを行う。認証管理実施要否設定部９５は、予めユーザやシステム提供者などによって設定されるものであり、ハード的なスイッチなどであってもよいし、メモリ上に設定するソフト的なフラグなどであってもよい。

【０２０７】

認証管理実施要否設定部９５を設けたことにより、認証サーバが不要な小規模システムにおいても、認証管理実施要否設定部９５の設定を「認証管理不実施」に設定しておくことで、本実施の形態５の主端末９１を使用することができる。つまり、本実施の形態５の主端末９１は、認証サーバが必要なシステムでも、認証サーバが不要なシステムでも適用できるので、これらの異なるシステムで共用化できる。

【０２０８】

以下に説明する認証処理は、認証管理実施要否設定部９５を「認証管理実施」に設定している場合について説明している。認証管理実施要否設定部９５が「認証管理不実施」に設定されている場合には、以下の処理は行わない。

【０２０９】

不正端末通知部９４は、認証状態記憶部１３が状態管理テーブル２９を用いて管理している副端末７２～７４の認証状態を、端末管理装置７６に送信する。例えば、認証状態記憶部１３が不正な副端末を検出し、「不正／切断状態」に遷移した場合に、不正端末通知部９４によって端末管理装置７６にＳＮＭＰ－ＴＲＡＰや、ＳＹＳＬＯＧを送信させる。

【０２１０】

このように、実施の形態１～４で、主端末７１が配下に接続された副端末７２～７４の認証状態の管理を行っていたのに加えて、その管理状態を端末管理装置７６に送信するようにしたことにより、端末管理装置７６は、自動で不正な副端末を検出することが可能になり、端末管理の煩雑化を防ぐことができる。

【０２１１】

つまり、実施の形態１～４では、端末管理装置７６は主端末７１に対して定期的にポーリングする等により各副端末７２～７４の管理をしていたのに対し、本実施の形態５の認証システムでは、端末管理装置７６は主端末９１からの認証状態の通知を受信するだけでよく、しかも主端末９１が不正な副端末を検出した時点で、すぐに新たな不正な副端末を検出することができる。

【０２１２】

認証データ作成部９２および認証ＩＤ記憶部９３は、それぞれ、図３に示す副端末７２～７４の、認証データ作成部２７および認証ＩＤ記憶部２８と同様の機能を有している。

【０２１３】

本実施の形態５の主端末９１は、主端末９１自身が起動した際に、認証データ作成部９２が、認証ＩＤ記憶部９３に記憶されている認証ＩＤを基に認証要求データを作成する。そして、通信送受信処理部１６が、通信Ｉ／Ｆ１０を介して、その作成した認証要求データを認証サーバ７５に対して送信する。

【０２１４】

通信送受信処理部１６が、その認証要求データに対応する認証応答データを認証サーバ７５から受信すると、認証データ解析部１２が、その認証応答データを解析する。

【０２１６】

その認証応答データの応答値が「許可」だった場合には、認証データ解析部１２は、転送制御部１７に対して転送開始を指示し、通信Ｉ／Ｆ１０と同軸Ｉ／Ｆ１１間の通信データの転送を開始させる。これで、配下の副端末７２～７４に接続されているユーザ端末８２～８４の通信が可能になる。

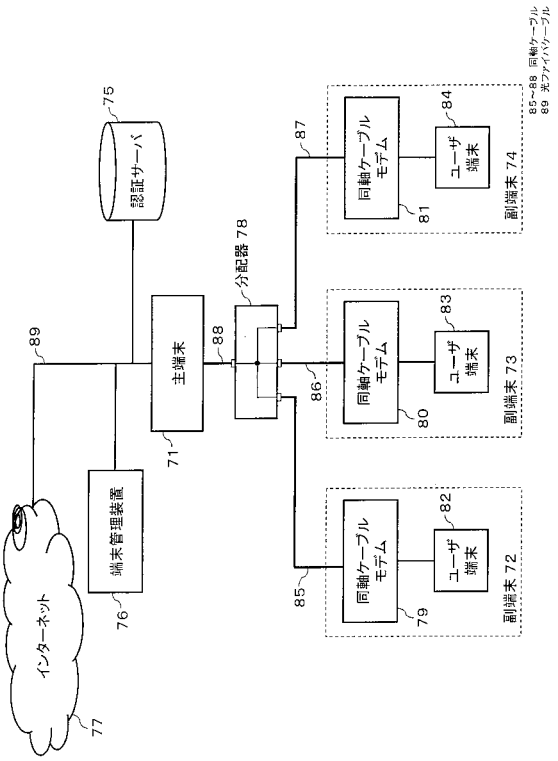
【０２１７】

そして、主端末９１自身が認証された場合には、主端末９１は、実施の形態１～４に記述した副端末７２～７４の認証管理を実施する。

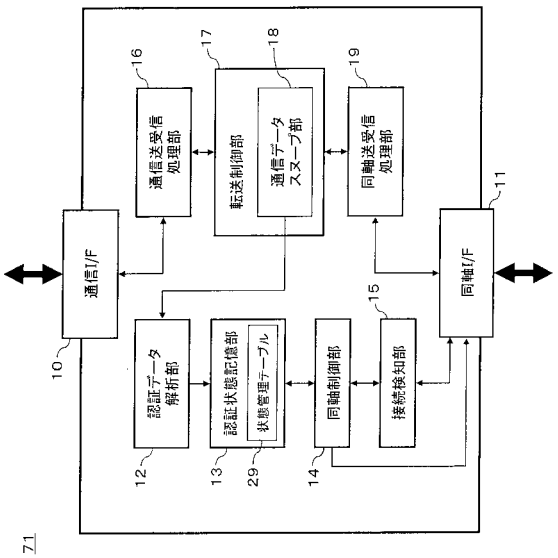
【０２１８】
なお、各実施の形態の、主端末および同軸ケーブルモデムは、宅内のＴＶ用に設置された同軸ケーブルを利用した同軸ホームネットワークを構成する際の、マスタ用の同軸ケーブル用モデムおよびクライアント用の同軸ケーブル用モデムとして説明したが、同軸ホームネットワークに限らず、各実施の形態に説明した主端末および同軸ケーブルモデムと同様の構成を設けることにより、他の通信システムでも適用できる。
【０２１９】
例えば、宅内の電灯線を利用してＰＬＣ通信用モデムで同様の構成とし、ＰＬＣ通信用モデムに、各実施の形態で説明した主端末および同軸ケーブルモデムの機能を備えさせることにより、同様の効果が得られる。
【０２２０】
また、主端末と副端末間の接続が同軸ケーブルのような有線で接続されるものに限らず、無線で接続される通信システムであっても適用できる。例えば、図１３に示す従来の無線を用いて通信システムの構成において、各実施の形態で説明した主端末および同軸ケーブルモデムの機能を、それぞれ、アクセスポイント１０５および無線ＬＡＮアダプタ１１０～１１２に備えさせるようにしてもよい。この場合、アクセスポイント１０５が不正な無線ＬＡＮアダプタであると判断した場合には、その無線ＬＡＮアダプタとの物理層を切断することにより、以降の、その不正と判断された無線ＬＡＮアダプタからのＳＳＩＤ認証を受け付けないようになる。
【０２２１】
以上に説明したように、本発明の認証システムは、不正な副端末に対しての物理層接続を不可にすることで、不正副端末に帯域を占拠させなくなるため、正規副端末のユーザに不利益を与えない。また、不正副端末の不正使用を完全に排除するため、通信システムのサーバにかかる負荷を軽減できる。また、認証中の副端末に速度制限を設定することによって、認証に必要なだけの帯域になることで、正規副端末の帯域を圧迫しない。また主端末は、配下に接続されている副端末不正クライアントの登録を自動で行うことが可能になるため、管理を簡素化することができる。
【０２２２】
すなわち、本発明の認証システムは、通信システムのサーバにかかる負荷を軽減し、また不正クライアント端末の排除を行い、不正クライアントの登録も自動で行うことができる認証システムである。
【０２２３】
本発明の認証システムを用いることにより、不正端末の検知と排除が容易になるため、例えばケーブルインターネットなどの同軸ケーブルを使用したアクセス系システムに有益であり、また主契約端末、副契約端末が宅内に設置されるようなホームネットワークにおける副契約端末の認証などにも応用が可能である。
【産業上の利用可能性】
【０２２４】
本発明にかかる、認証システムは、従来よりも容易な管理で、認証サーバの負荷を低減できる効果を有し、ネットワーク機器がネットワークに接続される認証システム等に有用である。
【図面の簡単な説明】
【０２２５】
【図１】本発明の実施の形態１の認証システムの概略構成図
【図２】本発明の実施の形態１の主端末の内部構成図
【図３】本発明の実施の形態１のケーブルモデムの内部構成図
【図４】本発明の実施の形態１の主端末が管理する、副端末の認証時の状態遷移図
【図５】（ａ）～（ｄ）本発明の実施の形態１の主端末が管理する、副端末の状態管理テーブルを示す図
【図６】本発明に関連する発明の実施の形態２の主端末が管理する、副端末の認証時の状

態遷移図
【図７】（ａ）～（ｄ）本発明に関連する発明の実施の形態２の主端末が管理する、副端末の状態管理テーブルを示す図
【図８】本発明の実施の形態３の主端末が管理する、副端末の認証時の状態遷移図
【図９】（ａ）～（ｅ）本発明の実施の形態３の主端末が管理する、副端末の状態管理テーブルを示す図
【図１０】本発明の実施の形態４の主端末が管理する、副端末の認証時の状態遷移図
【図１１】（ａ）～（ｄ）本発明の実施の形態４の主端末が管理する、副端末の状態管理テーブルを示す図
【図１２】本発明に関連する発明の実施の形態５の主端末の内部構成図
【図１３】従来の通信システムの接続構成図
【符号の説明】
【０２２６】
１０、２１　通信Ｉ／Ｆ
１１、２０　同軸Ｉ／Ｆ
１２、２４　認証データ解析部
１３　認証状態記憶部
１４　同軸制御部
１５　接続検知部
１６、２６　通信送受信処理部
１７、２５　転送制御部
１８　通信データスヌープ部
１９、２３　同軸送受信処理部
２２　同軸周波数制御部
２７　認証データ作成部
２８　認証ＩＤ記憶部
２９　状態管理テーブル
３１、４１、５１、６１　未接続状態
３２、４２、５２、６２　認証要求待ち状態
３３、４３、５３、６３　認証応答待ち状態
３４、４４、５４、６４　認証完了状態
３５、４５、５５、６５　不正／切断
５６　サーチ待ち状態
７１　主端末
７２、７３、７４　副端末
７５　認証サーバ
７６　端末管理装置
７７　インターネット
７８　分配器
７９、８０、８１　同軸ケーブルモデム
８２、８３、８４　ユーザ端末
８５、８６、８７、８８　同軸ケーブル
８９　光ファイバケーブル
９２　認証データ作成部
９３　認証ＩＤ記憶部
９４　不正端末通知部
９５　認証管理実施要否設定部

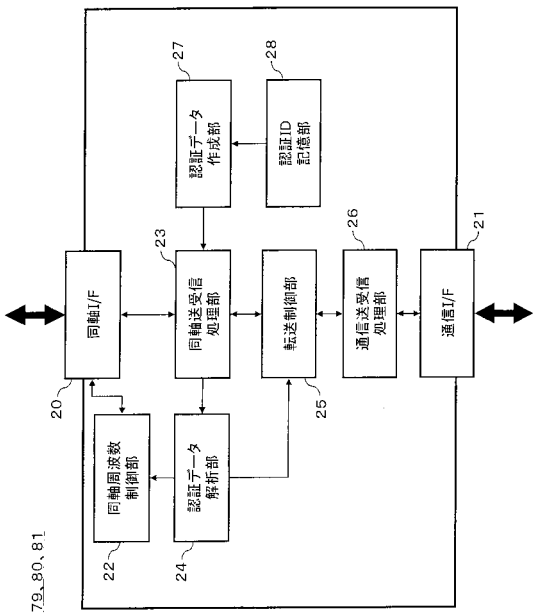
【図１】


認証サーバ
75
端末管理装置
76
インターネット
77
主端末
71
88
分配器 78
89
同軸ケーブル
モデム
80
ユーザ端末
83
副端末 73
同軸ケーブル
モデム
79
ユーザ端末
82
副端末 72
同軸ケーブル
モデム
81
ユーザ端末
84
副端末 74
85
86
87
85～88 同軸ケーブル
89 光ファイバケーブル

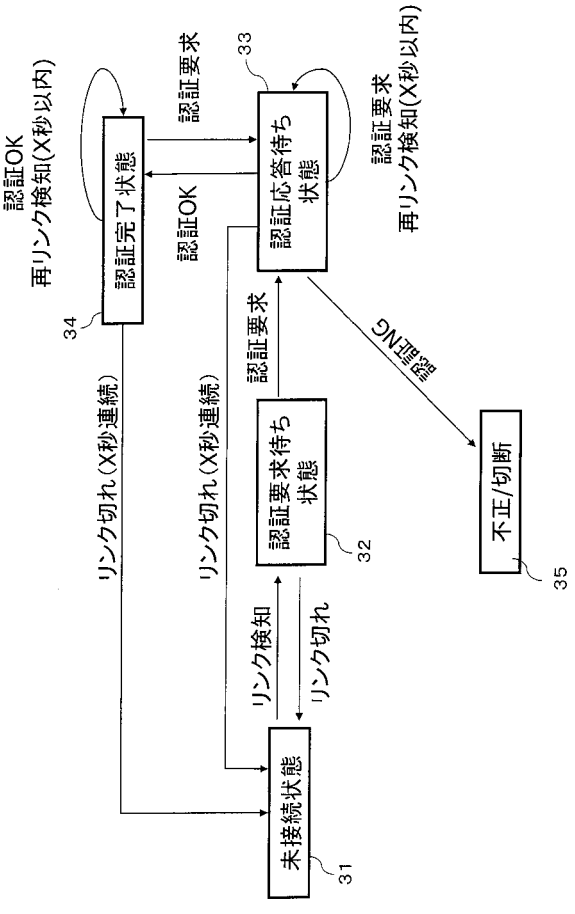
【図２】


71
通信I/F
10
認証データ解析部
12
認証状態記憶部
13
状態管理テーブル
29
同軸制御部
14
接続検知部
15
同軸I/F
11
通信送受信処理部
16
転送制御部
17
通信データスヌープ部
18
同軸送受信処理部
19

【図３】


79、80、81
同軸I/F
20
同軸周波数制御部
22
認証データ解析部
24
同軸送受信処理部
23
認証データ作成部
27
認証ID記憶部
28
転送制御部
25
通信送受信処理部
26
通信I/F
21

【図４】


認証OK
再リンク検知(X秒以内)
認証要求
認証完了状態
34
認証応答待ち状態
33
認証OK
認証要求
再リンク検知(X秒以内)
リンク切れ(X秒連続)
リンク切れ(X秒連続)
認証要求
認証NG
リンク検知
リンク切れ
認証要求待ち状態
32
未接続状態
31
不正/切断
35

【図５】

(a)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	認証要求待ち	OK:0x2006 NG:0x1029	----	----

(b)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	認証応答待ち	OK:0x2006 NG:0x1029	192.168.0.10	rootcert

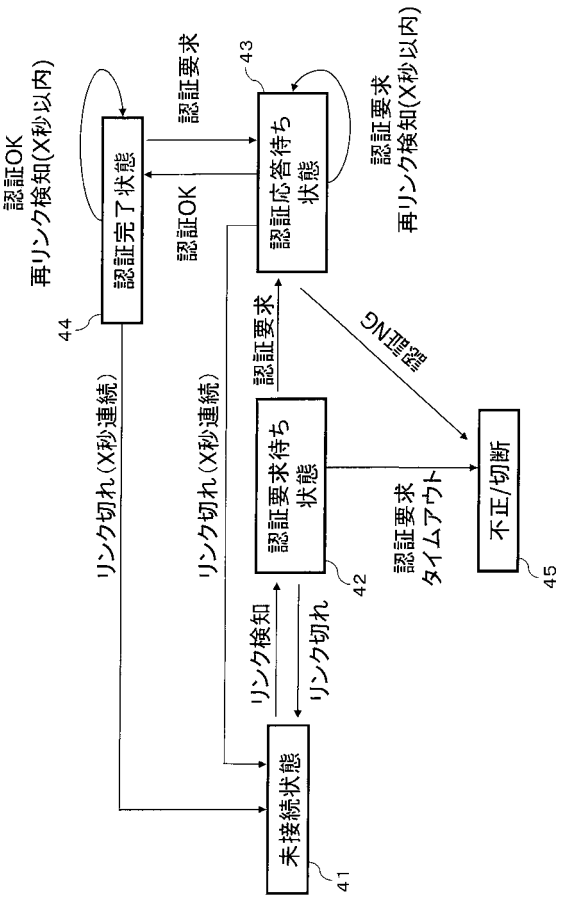
(c)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	定常状態	OK:0x2006 NG:0x1029	192.168.0.10	rootcert

(d)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	不正/切断	----	----	----

【図６】



【図７】

(a)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	認証要求待ち 150秒	OK:0x2006 NG:0x1029	----	----

(b)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	認証応答待ち	OK:0x2006 NG:0x1029	192.168.0.10	rootcert

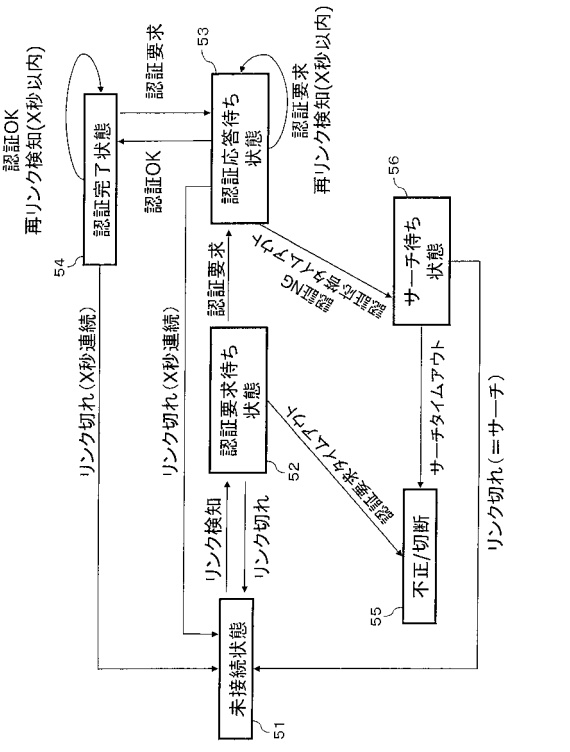
(c)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	定常状態	OK:0x2006 NG:0x1029	192.168.0.10	rootcert

(d)

No	モデムID	状態	応答値	サーバアドレス	キーワード
1	00:99:88:77:66:55	不正/切断	----	----	----

【図８】



【図９】

(a)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード	運用 保証速度	運用 制限速度
1	00:99:88:77:66:55	認証要求待ち 150秒 速度制限中(1Mbps)	OK:0x2006 NG:0x1029	----	----	5Mbps	10Mbps

(b)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード	運用 保証速度	運用 制限速度
1	00:99:88:77:66:55	認証応答待ち 30秒 速度制限中(1Mbps)	OK:0x2006 NG:0x1029	192.168.0.10	rootcert	5Mbps	10Mbps

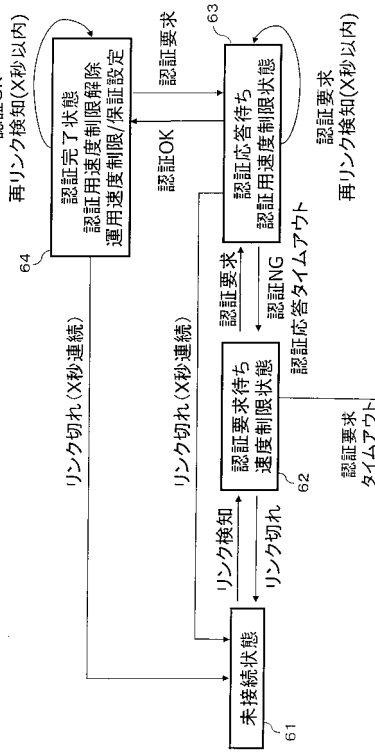
(c)

No	モデムID	状態	応答値	サーバアドレス	キーワード	運用保証速度	運用制限速度
1	00:99:88:77:66:55	定常状態 運用速度設定中 (制限3Mbps 保証1Mbps)	OK:0x2006 NG:0x1029	192.168.0.10	rootcert	5Mbps	10Mbps

(d)

No	モデムID	状態	応答値	サーバアドレス	キーワード	運用保証速度	運用制限速度
1	00:99:88:77:66:55	不正/切断	----	----	----	5Mbps	10Mbps

【図１０】



【図１１】

(a)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード	運用 保証速度	運用 制限速度
1	00:99:88:77:66:55	認証要求待ち 150秒 速度制限中(1Mbps)	OK:0x2006 NG:0x1029	----	----	5Mbps	10Mbps

(b)

No	モデムID	状態 残り時間	応答値	サーバアドレス	キーワード	運用 保証速度	運用 制限速度
1	00:99:88:77:66:55	認証応答待ち 30秒 速度制限中(1Mbps)	OK:0x2006 NG:0x1029	192.168.0.10	rootcert	5Mbps	10Mbps

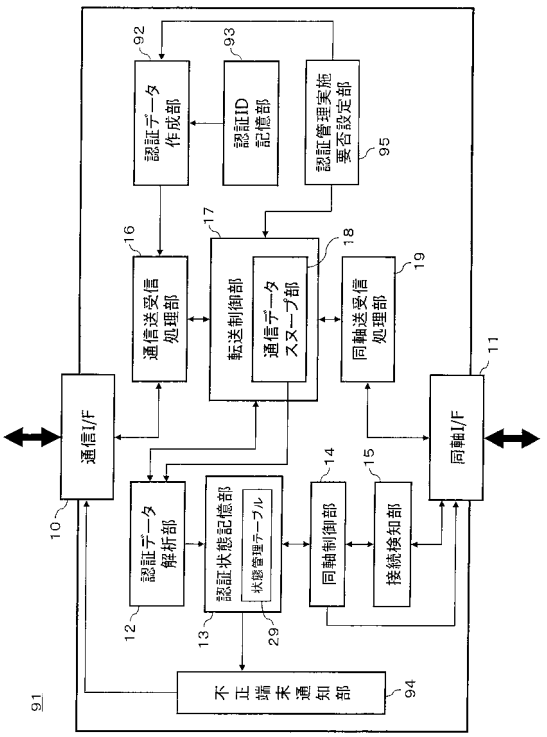
(c)

No	モデムID	状態	応答値	サーバアドレス	キーワード	運用保証速度	運用制限速度
1	00:99:88:77:66:55	定常状態 運用速度設定中 (制限3Mbps 保証1Mbps)	OK:0x2006 NG:0x1029	192.168.0.10	rootcert	5Mbps	10Mbps

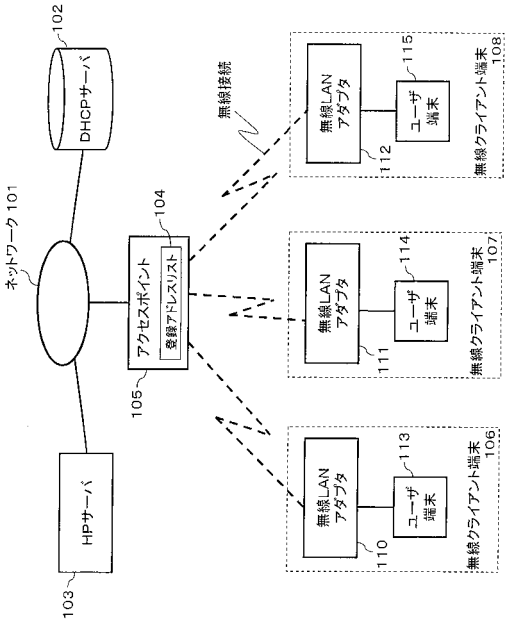
(d)

No	モデムID	状態	応答値	サーバアドレス	キーワード	運用保証速度	運用制限速度
1	00:99:88:77:66:55	不正/切断	----	----	----	5Mbps	10Mbps

【図１２】



【図１３】


ネットワーク101
DHCPサーバ
102
HPサーバ
103
アクセスポイント
104
登録アドレスリスト
105
無線接続
無線LANアダプタ
112
ユーザ端末
115
無線クライアント端末
108
無線LANアダプタ
111
ユーザ端末
114
無線クライアント端末
107
無線LANアダプタ
110
ユーザ端末
113
無線クライアント端末
106

フロントページの続き

(72)発明者　渡邊　寛如
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　山田　豊士
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　名越　方彦
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　平井　誠

(56)参考文献　特開２００３－０４６５３３（ＪＰ，Ａ）
特開２００３－１４３１２６（ＪＰ，Ａ）
特開２００２－２７１３１９（ＪＰ，Ａ）
特開２００３－１１０５７０（ＪＰ，Ａ）
特開２００４－００７３７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１