(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2007-201937
(P2007-201937A)
(43)公開日　平成19年8月9日(2007.8.9)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675D	5J104
G09C	1/00	(2006.01)	G09C	1/00	640E	

審査請求 有　請求項の数 5　OL　（全 12 頁）

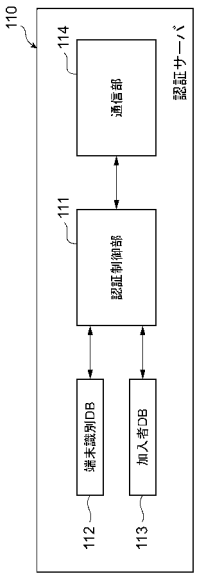
(21)出願番号　特願2006-19526(P2006-19526)
(22)出願日　平成18年1月27日(2006.1.27)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100092657
弁理士　寺崎　史朗
(74)代理人　100114270
弁理士　黒川　朋也
(74)代理人　100124800
弁理士　諏澤　勇司
(74)代理人　100121980
弁理士　沖山　隆

最終頁に続く

(54)【発明の名称】認証サーバ、認証システム及び認証方法

(57)【要約】
【課題】通信端末の機種を考慮した認証を可能とする。
【解決手段】通信端末の認証を行う認証サーバにおいて、通信を許可する通信端末の機種についての該機種固有の通信端末識別情報を格納した格納手段（端末識別ＤＢ１１２）と、通信端末にて網認証が許可された場合に設定される該通信端末の機種固有の通信端末識別情報を受信する受信手段（通信部１１４）と、受信された通信端末識別情報と格納された通信端末識別情報とを照合することで、通信端末識別情報に基づいた認証可否を決定する決定手段（認証制御部１１１）と、認証可否の決定に基づいて通信端末との接続制御を行う制御手段（認証制御部１１１）とを備えた。
【選択図】図４



【特許請求の範囲】
【請求項１】
通信端末の認証を行う認証サーバであって、
通信を許可する通信端末の機種についての該機種固有の通信端末識別情報を格納した格納手段と、
前記通信端末にて網認証が許可された場合に設定される該通信端末の機種固有の通信端末識別情報を、該通信端末から受信する受信手段と、
前記受信手段により受信された通信端末識別情報と、前記格納手段に格納された通信端末識別情報とを照合することで、通信端末識別情報に基づいた認証可否を決定する決定手段と、
前記決定手段による認証可否の決定に基づいて、前記通信端末との接続制御を行う制御手段と、
を備えた認証サーバ。
【請求項２】
前記決定手段は、
前記受信された通信端末識別情報が、前記格納された通信端末識別情報の中に存在する場合に、認証許可と決定し、前記受信された通信端末識別情報が、前記格納された通信端末識別情報の中に存在しない場合に、認証拒否と決定する
ことを特徴とする請求項１に記載の認証サーバ。
【請求項３】
前記認証サーバは、標準で規定された加入者認証情報に基づく認証処理と前記通信端末識別情報に基づく認証処理のうち、実行すべき認証処理を、接続先に応じて予め定めた接続先テーブルをさらに備え、
前記受信手段は、通信端末識別情報とともに加入者認証情報及び接続先情報を、前記通信端末から受信し、
前記決定手段は、前記受信された接続先情報をキーとして前記接続先テーブルを参照することで該接続先情報に応じた認証処理を決定し、
前記制御手段は、前記決定手段による決定内容に基づいて、該接続先情報に応じた認証処理を実行する、
ことを特徴とする請求項１又は２に記載の認証サーバ。
【請求項４】
１つ以上の通信端末と、
請求項１～３の何れか１項に記載の認証サーバと、
を含んで構成された認証システム。
【請求項５】
１つ以上の通信端末と、通信を許可する通信端末の機種についての該機種固有の通信端末識別情報を格納した格納手段を備え通信端末の認証を行う認証サーバと、を含んで構成された認証システムにおける認証方法であって、
前記通信端末が、網認証を許可した場合のみ、該通信端末の機種固有の通信端末識別情報を設定し、該通信端末識別情報を前記認証サーバへ送信する送信ステップと、
前記認証サーバが、前記通信端末からの通信端末識別情報を受信し、受信された通信端末識別情報と前記格納手段に格納された通信端末識別情報とを照合することで、通信端末識別情報に基づいた認証可否を決定する決定ステップと、
前記決定ステップでの認証可否の決定に基づいて、前記通信端末との接続制御を行う制御ステップと、
を備えた認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信端末の認証を行う認証サーバ、認証システム及び認証方法に関するもの

である。
【背景技術】
【０００２】
通信端末（例えば無線ＬＡＮ対応可能な携帯電話など）からのアクセスを正当なユーザからのみに限定するために、加入者情報に基づく認証を行う加入者認証サーバのような加入者認証装置が知られている。
【非特許文献１】3GPP TS33.234、URL:http://www.3gpp.org
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、上記従来技術に係る加入者認証装置は、以下に示すような問題点があった。即ち、上記従来技術に係る加入者認証装置は、通信端末の機種を考慮した認証を行うことができない。したがって、認証対象の通信端末が、想定外の機能を持った通信端末（例えばパーソナル・コンピュータのような高機能の端末）であっても、正当な加入者情報を持っていれば、認証が許可されてしまう。この場合、想定外の機能を持った通信端末から、想定を越えるトラヒック量のデータがネットワークに流入する危険性や、ネットワーク上の装置を意図的に誤作動させる通信が行われる危険性が想定される。
【０００４】
そこで、本発明は、上記問題点を解決し、通信端末の機種を考慮した認証を可能とする認証サーバ、認証システム及び認証方法を提供することを目的とする。
【課題を解決するための手段】
【０００５】
上記目的を達成するために、本発明に係る認証サーバは、通信端末の認証を行う認証サーバであって、通信を許可する通信端末の機種についての該機種固有の通信端末識別情報を格納した格納手段と、通信端末にて網認証が許可された場合に設定される該通信端末の機種固有の通信端末識別情報を、該通信端末から受信する受信手段と、受信手段により受信された通信端末識別情報と、格納手段に格納された通信端末識別情報とを照合することで、通信端末識別情報に基づいた認証可否を決定する決定手段と、決定手段による認証可否の決定に基づいて、通信端末との接続制御を行う制御手段とを備えたことを特徴とする。
【０００６】
これにより、通信端末の機種を考慮した認証を実行することができるため、従来の認証では許可されてしまう通信端末（例えば正当な加入者情報が設定された想定外の機種の通信端末）については、機種を考慮した認証によって拒否することができ、自網を確実に守ることができる。
【０００７】
上記の認証サーバでは、決定手段は、受信された通信端末識別情報が、格納された通信端末識別情報の中に存在する場合に、認証許可と決定し、受信された通信端末識別情報が、格納された通信端末識別情報の中に存在しない場合に、認証拒否と決定する構成とすることが望ましい。これにより、存在する全ての通信端末に関する通信端末識別情報を格納しておく必要はなく、通信を許可する通信端末の機種についての通信端末識別情報のみを格納しておけば済むという利点がある。
【０００８】
また、上記の認証サーバは、標準で規定された加入者認証情報に基づく認証処理と通信端末識別情報に基づく認証処理のうち、実行すべき認証処理を、接続先に応じて予め定めた接続先テーブルをさらに備え、受信手段は、通信端末識別情報とともに加入者認証情報及び接続先情報を、通信端末から受信し、決定手段は、受信された接続先情報をキーとして接続先テーブルを参照することで該接続先情報に応じた認証処理を決定し、制御手段は、決定手段による決定内容に基づいて、該接続先情報に応じた認証処理を実行する構成とすることが望ましい。これにより、接続先情報に応じた認証処理を実行することができる

。即ち、接続先の目的・用途によっては、標準で規定された加入者認証情報に基づく認証機能のみを実装した想定外の通信端末の接続を許容することや、通信端末識別情報に基づく認証機能のみを実装した通信端末の接続のみを許容することや、加入者認証情報に基づく認証機能と通信端末識別情報に基づく認証機能の両方を実装した通信端末の接続のみを許容することを、自在に実現することができる。

【０００９】

本発明に係る認証システムは、１つ以上の通信端末と、上述したような認証サーバと、を含んで構成することを特徴とする。

【００１０】

また、本発明に係る認証方法は、１つ以上の通信端末と、通信を許可する通信端末の機種についての該機種固有の通信端末識別情報を格納した格納手段を備え通信端末の認証を行う認証サーバと、を含んで構成された認証システムにおける認証方法であって、通信端末が、網認証を許可した場合のみ、該通信端末の機種固有の通信端末識別情報を設定し、該通信端末識別情報を認証サーバへ送信する送信ステップと、認証サーバが、通信端末からの通信端末識別情報を受信し、受信された通信端末識別情報と格納手段に格納された通信端末識別情報とを照合することで、通信端末識別情報に基づいた認証可否を決定する決定ステップと、決定ステップでの認証可否の決定に基づいて、通信端末との接続制御を行う制御ステップとを備えたことを特徴とする。

【００１１】

上記の認証システム、認証方法においても、通信端末の機種を考慮した認証を実行することができるため、従来の認証では許可されてしまう通信端末（例えば正当な加入者情報が設定された想定外の機種の通信端末）については、機種を考慮した認証によって拒否することができ、自網を確実に守ることができる。

【発明の効果】

【００１２】

本発明に係る認証サーバ、認証システム及び認証方法によれば、通信端末の機種を考慮した認証を実行することができるため、従来の認証では許可されてしまう通信端末（例えば正当な加入者情報が設定された想定外の機種の通信端末）については、機種を考慮した認証によって拒否することができ、自網を確実に守ることができる。

【発明を実施するための最良の形態】

【００１３】

以下、図面を用いて本発明の実施形態に係る認証サーバ、認証システム及び認証方法について説明する。まず、本実施形態に係る認証システムの構成について説明する。図１は本実施形態に係る認証システム１の構成図を示す。この図１に示すように、認証システム１は、ネットワーク５０内に設けられた認証サーバ１１０と、ネットワーク５０と外部との複数の接続点の各々に設置された接続装置３１０Ａ、３１０Ｂ、３１０Ｃ（以下「接続装置３１０」と総称する）と、複数の通信端末２１０Ａ、２１０Ｂ、２１０Ｃ（以下「通信端末２１０」と総称する）とを含んで構成される。このような認証システム１において通信端末２１０は、接続装置３１０を介して認証サーバ１１０と通信し認証を行う。認証サーバ１１０により認証が許可された場合、接続装置３１０は通信端末２１０との間で仮想的な通信路を設定し所望のネットワークへ安全に接続することができる。

【００１４】

続いて、図２を用いて本実施形態に係るプロトコルについて説明する。図２において最上位に示す認証プロトコルのレイヤーは、通信端末２１０と認証サーバ１１０間で終端し、接続装置３１０は関与しないものとして、認証処理を認証サーバ１１０に集約する。認証プロトコルでは、加入者の認証に用いられる加入者認証情報、及び、通信端末が網認証で許可された場合のみ設定される該通信端末の機種に固有の識別情報（以下「通信端末識別情報」という）を、Type/Length/Value形式（いわゆるＴＬＶ形式）で設定する。通信端末識別情報としては、例えば、ＩＭＥＩＳＶ（International Mobile Equipment Identity Software Version number）を設定する。

【００１５】
また、図２において中位に示すノード間プロトコルは、接続装置３１０と認証サーバ１１０間で終端する信号を制御するプロトコルであり、接続プロトコルは、通信端末２１０と接続装置３１０間で終端する信号を制御するプロトコルである。図２において最下位に示す通信プロトコルは、各装置間の通信路を提供するＯＳＩ参照モデルのトランスポート層以下のレイヤーを表している。
【００１６】
次に、本実施形態に係る認証サーバ１１０のハードウェア構成と機能ブロック構成を順に説明する。図３は認証サーバ１１０のハードウェア構成を示し、この図３に示すように認証サーバ１１０は、ＣＰＵ１０１、ＲＡＭ１０２、ＲＯＭ１０３、外部との通信処理を行うネットワーク制御部１０４、及び、大容量の不揮発性記憶装置としてのハードディスク（Hard disk（以下「ＨＤ」という）１０５を含んで構成される。
【００１７】
図４は認証サーバ１１０の機能ブロック構成を示し、この図４に示すように認証サーバ１１０は、加入者認証情報を格納するための加入者データベース（加入者ＤＢ）１１３と、ネットワークへの接続を許可する通信端末の機種に関する通信端末識別情報のリストを格納するための端末識別データベース（端末識別ＤＢ）１１２と、後述する認証処理を実行する認証制御部１１１と、外部との通信処理を行う通信部１１４とを含んで構成される。このうち認証制御部１１１は、図３のＣＰＵ１０１、ＲＡＭ１０２及びＲＯＭ１０３から構成され、通信部１１４は図３のネットワーク制御部１０４から構成される。端末識別ＤＢ１１２及び加入者ＤＢ１１３はＨＤ１０５内に形成されている。
【００１８】
通信部１１４は、図１の接続装置３１０からの信号を受信し、認証制御部１１１へ加入者認証情報と通信端末識別情報を転送する。また、通信部１１４は、認証制御部１１１からの網認証情報や認証結果を受信し、接続装置３１０を介して通信端末２１０に網認証情報や認証結果を送信する。
【００１９】
認証制御部１１１は、受信した加入者認証情報に基づいて加入者ＤＢ１１３を検索することで、加入者認証可否を判断する。また、認証制御部１１１は、受信した通信端末識別情報をもって端末識別ＤＢ１１２を検索し、該通信端末識別情報が格納されていれば認証可と判断し、該通信端末識別情報が格納されていなければ認証否と判断することで、通信端末識別情報に基づく認証を行う。
【００２０】
なお、本発明に係る認証サーバにおける格納手段は図４の端末識別ＤＢ１１２に相当し、受信手段は通信部１１４に相当し、決定手段及び制御手段は認証制御部１１１に相当する。
【００２１】
次に、本実施形態に係る通信端末識別情報について説明する。通信端末識別情報は、十分なビット長で構成される、通信端末の機種に固有の値が設定される。その値の付与は、当該値の推測が容易でないようにするため、未使用の値からランダムに設定される。
【００２２】
続いて、図５、図６を用いて認証サーバ１１０の動作について説明する。図５は認証サーバ１１０の認証許可の動作を示すシーケンスであり、図６は認証サーバ１１０の認証拒否の動作を示すシーケンスである。本実施形態に係る認証サーバ１１０を動作させるにあたっては、まず、通信端末２１０が認証要求信号を接続装置３１０へ送信し、認証要求信号を受信した接続装置３１０は、認証サーバ１１０へ該認証要求信号を転送する（図５と図６で共通のＳ１０１）。認証サーバ１１０は、通信部１１４により認証要求信号を受信し、認証制御部１１１によって、加入者ＤＢ１１３に格納される網認証情報を取得し、通信部１１４により通信端末２１０へ返送する（Ｓ１０２）。
【００２３】

通信端末２１０は、網認証情報を受信すると、該網認証情報に従い認証先のネットワークが正当であることを確認する（いわゆる網認証を実行する）（Ｓ１０３）。認証先のネットワークが正当であれば、通信端末２１０は、自端末の機種に固有の通信端末識別情報、及び加入者認証情報を接続装置３１０経由で認証サーバ１１０へ送信する（Ｓ１０４）。

【００２４】

一方、Ｓ１０３で認証先ネットワークが不正であれば、通信端末２１０において通信端末識別情報は設定しないことで、プロトコル上の通信端末識別情報の存在自体を隠蔽する。仮に、通信端末識別情報の設定方法と設定値が漏れた場合、想定しない通信端末が、漏れた正当な通信端末識別情報を詐称設定してくる危険性がある。そのため、通信端末２１０において通信端末識別情報は設定しないことで、上記危険性を回避することができる。

【００２５】

認証サーバ１１０は、通信部１１４により通信端末識別情報及び加入者認証情報を受信すると、認証制御部１１１によって、上記受信した通信端末識別情報が端末識別ＤＢ１１２に格納されているか否かを確認する（Ｓ１０５）。ここで、上記通信端末識別情報が格納されていれば、送信元の通信端末２１０は正当な通信端末であると判断し、上記通信端末識別情報が格納されていなければ、送信元の通信端末２１０は不正な通信端末であると判断する。

【００２６】

送信元の通信端末２１０が正当な通信端末であると判断された場合、認証サーバ１１０は、認証制御部１１１によって、上記受信した加入者認証情報に基づいて加入者ＤＢ１１３を検索することで、該加入者認証情報の正当性を判断する（Ｓ１０６）。このようにＳ１０５、Ｓ１０６において、通信端末識別情報と加入者認証情報のどちらも正当であれば認証許可と判断され、どちらかが不正であれば認証拒否と判断される。なお、図５、図６では、通信端末識別情報の認証、加入者認証情報の認証の順に実行する例を示したが、その実行順序に限定されるものではなく、加入者認証情報の認証を先に、通信端末識別情報の認証を後に実行してもよいし、通信端末識別情報の認証及び加入者認証情報の認証を同時並行で実行してもよい。

【００２７】

上述したＳ１０１～Ｓ１０６の動作は、図５と図６で共通であるが、認証許可の場合の動作を図５に、認証拒否の場合の動作を図６に、それぞれ示す。

【００２８】

認証制御部１１１により認証許可と判断された場合、図５に示すように認証サーバ１１０は、認証許可の認証結果を通信部１１４によって接続装置３１０経由で通信端末２１０へ送信する（Ｓ１０７Ａ）。ここでの認証結果は、認証プロトコルだけでなく、ノード間プロトコルにも設定するものとする。これにより、通信端末２１０と接続装置３１０との間の通信が確立される（Ｓ１０８Ａ）。

【００２９】

一方、認証制御部１１１により認証拒否と判断された場合、図６に示すように認証サーバ１１０は、認証拒否の認証結果を通信部１１４によって接続装置３１０経由で通信端末２１０へ送信する（Ｓ１０７Ｂ）。ここでの認証結果は、認証プロトコルだけでなく、ノード間プロトコルにも設定するものとする。これにより、通信端末２１０と接続装置３１０との間の通信は確立しない（Ｓ１０８Ｂ）。

【００３０】

続いて、本実施形態の効果について説明する。本実施形態に係る認証サーバは、通信端末の機種を考慮した認証を行うことで、正当な加入者情報が設定された想定外の通信端末からの通信を拒否することができる。これにより、想定外の機能を持った通信端末により想定を越えるトラヒック量のデータがネットワークに流入する危険性、及びネットワーク上の装置を意図的に誤作動させる通信が行われる危険性を回避し、ネットワークを守ることができる。

【００３１】
続いて、本実施形態に係る認証サーバ１１０の変形例について説明する。すなわち、上記実施形態に係る認証サーバ１１０では、認証可否を常に加入者情報と通信端末識別情報の両方に基づいて決定していたが、本変形例では、接続先に応じて、「加入者情報のみに基づく認証」、「通信端末識別情報のみに基づく認証」、「加入者情報と通信端末識別情報の両方に基づく認証」の３つを切り替えて実行するというものである。なお、本変形例での認証サーバ１１０では、認証制御部１１１が、図９に示す接続先テーブル１１５を内蔵しており、この接続先テーブル１１５はＲＯＭ１０３内に記憶されている。接続先テーブル１１５には、接続先ごとに、どの認証方法を行うかがフラグ設定されている。図９では、フラグが立っている状態を「要」、フラグが立っていない状態を「不要」と記載している。その他、認証サーバ１１０および認証システム１の構成は、前述した実施形態と同様であるので、説明を省略する。

【００３２】
次に、図７、図８を用いて本変形例に係る認証サーバ１１０の動作について説明する。図７は認証サーバ１１０の認証許可の動作を示すシーケンスであり、図８は認証サーバ１１０の認証拒否の動作を示すシーケンスである。本変形例に係る認証サーバ１１０を動作させるにあたっては、まず、通信端末２１０が認証要求信号を接続装置３１０へ送信し、認証要求信号を受信した接続装置３１０は、認証サーバ１１０へ該認証要求信号を転送する（図７と図８で共通のＳ２０１）。認証サーバ１１０は、通信部１１４により認証要求信号を受信し、認証制御部１１１によって、加入者ＤＢ１１３に格納される網認証情報を取得し、通信部１１４により通信端末２１０へ返送する（Ｓ２０２）。

【００３３】
通信端末２１０は、網認証情報を受信すると、該網認証情報に従い認証先のネットワークが正当であることを確認する（いわゆる網認証を実行する）（Ｓ２０３）。認証先のネットワークが正当であれば、通信端末２１０は、自端末の機種に固有の通信端末識別情報、加入者認証情報、及び接続先情報を接続装置３１０経由で認証サーバ１１０へ送信する（Ｓ２０４）。たとえ接続先が加入者認証情報を参照しない接続先であったとしても、通信端末２１０は一定の動作をさせるものとする。

【００３４】
一方、Ｓ２０３で認証先ネットワークが不正であれば、通信端末２１０において通信端末識別情報は設定しないことで、プロトコル上の通信端末識別情報の存在自体を隠蔽する。仮に、通信端末識別情報の設定方法と設定値が漏れた場合、想定しない通信端末が、漏れた正当な通信端末識別情報を詐称設定してくる危険性がある。そのため、通信端末２１０において通信端末識別情報は設定しないことで、上記危険性を回避することができる。

【００３５】
認証サーバ１１０は、通信部１１４により通信端末識別情報、加入者認証情報及び接続先情報を受信すると、認証制御部１１１によって、該認証制御部１１１に内蔵された図９の接続先テーブル１１５を参照し、上記接続先情報に応じた認証方法を判別する（Ｓ２０５）。

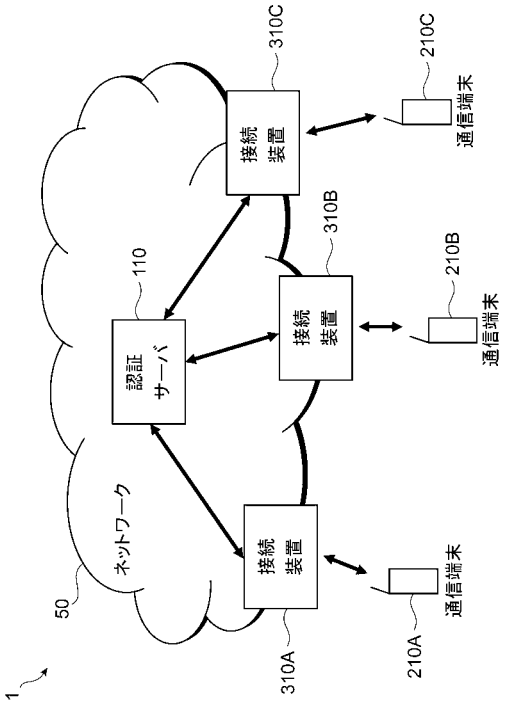
【００３６】
ここで、接続先が接続先１又は接続先２の場合は、通信端末識別情報に基づく認証を行うフラグが立っているため、認証サーバ１１０は、認証制御部１１１によって、上記受信した通信端末識別情報が端末識別ＤＢ１１２に格納されているか否かを確認する（Ｓ２０６）。ここで、上記通信端末識別情報が格納されていれば、送信元の通信端末２１０は正当な通信端末であると判断し、上記通信端末識別情報が格納されていなければ、送信元の通信端末２１０は不正な通信端末であると判断する。

【００３７】
また、接続先が接続先１又は接続先３の場合は、加入者認証情報に基づく認証を行うフラグが立っているため、認証サーバ１１０は、認証制御部１１１によって、上記受信した加入者認証情報に基づいて加入者ＤＢ１１３を検索することで、該加入者認証情報の正当

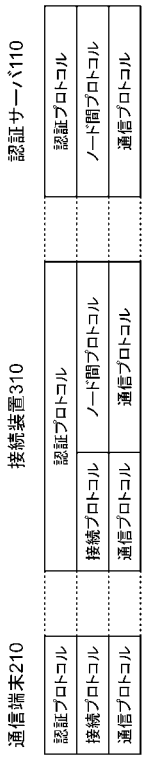
性を判断する（Ｓ２０７）。
【００３８】
このように接続先テーブル１１５のフラグに応じた認証処理を行い、すべての認証が許可であった場合に、認証許可と判断し、いずれかの認証が拒否であった場合は、認証拒否と判断する。なお、接続先が接続先４の場合は、Ｓ２０６、Ｓ２０７の認証処理は実行せずスキップする。
【００３９】
上述したＳ２０１～Ｓ２０７の動作は、図７と図８で共通であるが、認証許可の場合の動作を図７に、認証拒否の場合の動作を図８に、それぞれ示す。
【００４０】
認証制御部１１１により認証許可と判断された場合、図７に示すように認証サーバ１１０は、認証許可の認証結果を通信部１１４によって接続装置３１０経由で通信端末２１０へ送信する（Ｓ２０８Ａ）。ここでの認証結果は、認証プロトコルだけでなく、ノード間プロトコルにも設定するものとする。これにより、通信端末２１０と接続装置３１０との間の通信が確立される（Ｓ２０９Ａ）。
【００４１】
一方、認証制御部１１１により認証拒否と判断された場合、図８に示すように認証サーバ１１０は、認証拒否の認証結果を通信部１１４によって接続装置３１０経由で通信端末２１０へ送信する（Ｓ２０８Ｂ）。ここでの認証結果は、認証プロトコルだけでなく、ノード間プロトコルにも設定するものとする。これにより、通信端末２１０と接続装置３１０との間の通信は確立しない（Ｓ２０９Ｂ）。
【００４２】
最後に、本変形例の効果について説明する。本変形例に係る認証サーバ１１０は、接続先テーブル１１５に基づいた認証方法による認証を実行しネットワークへの接続可否を判断する。このような処理とすることで、接続先の特性に合わせた認証処理を実行することができるという効果が得られる。即ち、接続先の目的・用途によっては、加入者認証情報に基づく認証機能のみを実装した想定外の通信端末の接続を許容することや、通信端末識別情報に基づく認証機能のみを実装した通信端末の接続のみを許容することや、加入者認証情報に基づく認証機能と通信端末識別情報に基づく認証機能の両方を実装した通信端末の接続のみを許容することを、自在に実現することができる。
【図面の簡単な説明】
【００４３】
【図１】本発明の実施形態に係る認証システムの構成図である。
【図２】本発明の実施形態に係る認証システムで用いられるプロトコルスタックを示す図である。
【図３】本発明の実施形態に係る認証サーバのハードウェア構成図である。
【図４】本発明の実施形態に係る認証サーバの機能ブロック図である。
【図５】本発明の実施形態に係る認証方法（認証許可）の動作を示すシーケンス図である。
【図６】本発明の実施形態に係る認証方法（認証拒否）の動作を示すシーケンス図である。
【図７】本発明の変形例に係る認証方法（認証許可）の動作を示すシーケンス図である。
【図８】本発明の変形例に係る認証方法（認証拒否）の動作を示すシーケンス図である。
【図９】本発明の変形例に係る認証サーバの接続先テーブルを示す図である。
【符号の説明】
【００４４】
１…認証システム、５０…ネットワーク、１０１…ＣＰＵ、１０２…ＲＡＭ、１０３…ＲＯＭ、１０４…ネットワーク制御部、１０５…ＨＤ、１１０…認証サーバ、１１１…認証制御部、１１２…端末識別ＤＢ、１１３…加入者ＤＢ、１１４…通信部、１１５…接続先テーブル、２１０、２１０Ａ、２１０Ｂ、２１０Ｃ…通信端末、３１０、３１０Ａ、３

１０Ｂ、３１０Ｃ…接続装置。

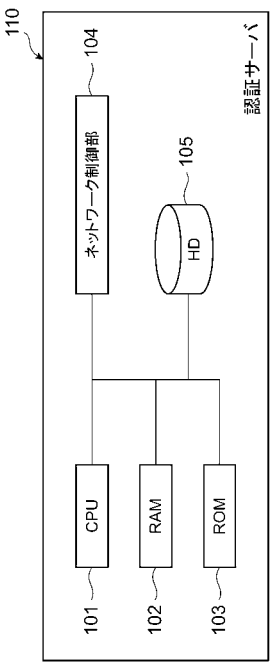
【図１】



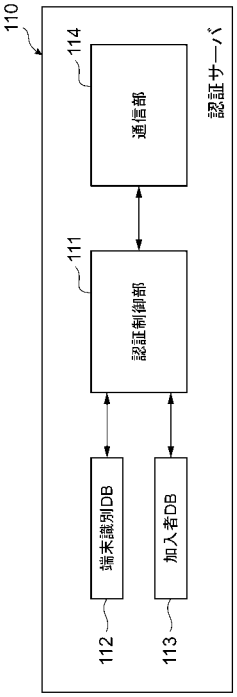
【図２】



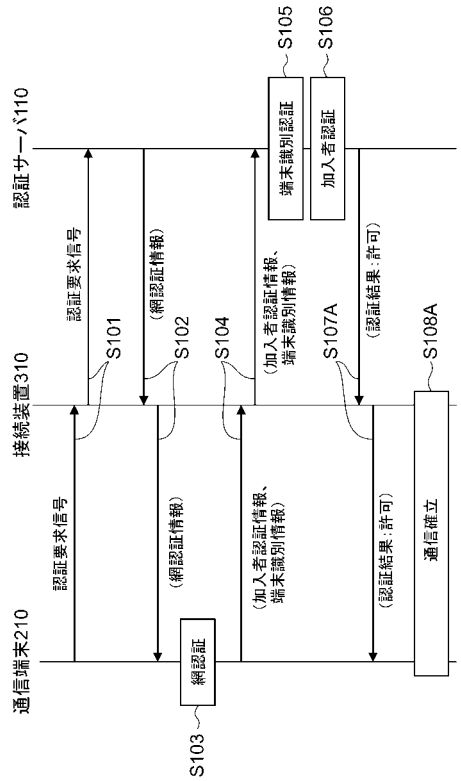
【図３】


110
認証サーバ
104
ネットワーク制御部
105
HD
CPU
RAM
ROM
101
102
103

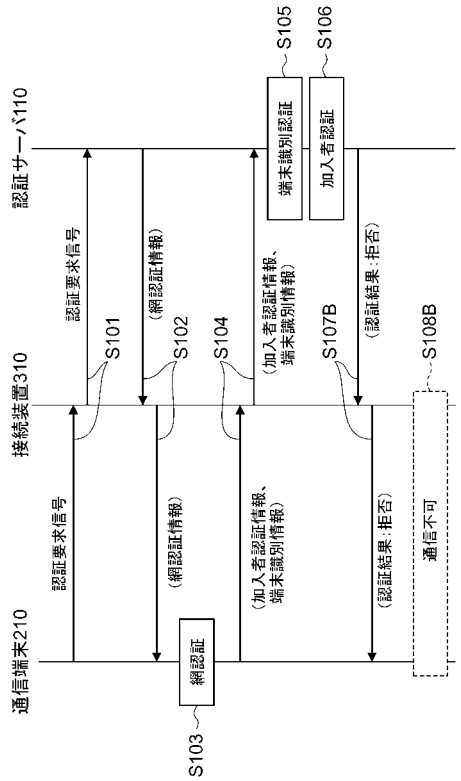
【図４】


110
認証サーバ
114
通信部
111
認証制御部
端末識別DB
加入者DB
112
113

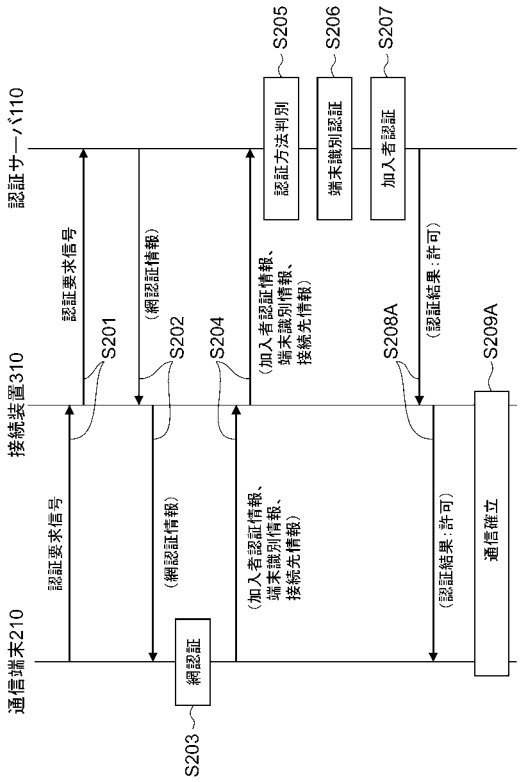
【図５】


通信端末210
接続装置310
認証サーバ110
認証要求信号
S101
(網認証情報)
S102
網認証
S103
(加入者認証情報、端末識別情報)
S104
端末識別認証
S105
加入者認証
S106
(認証結果:許可)
S107A
通信確立
S108A

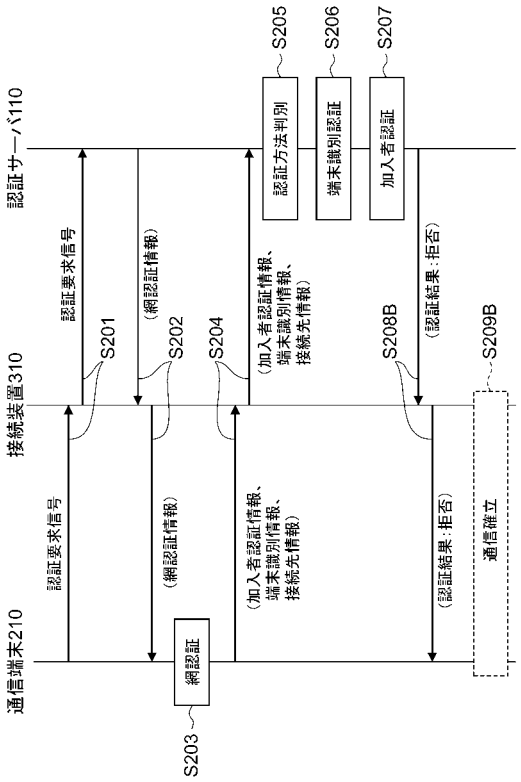
【図６】


通信端末210
接続装置310
認証サーバ110
認証要求信号
S101
(網認証情報)
S102
網認証
S103
(加入者認証情報、端末識別情報)
S104
端末識別認証
S105
加入者認証
S106
(認証結果:拒否)
S107B
通信不可
S108B

【図７】



【図８】



【図９】

115

接続先	認証方法	
	通信端末識別情報に基づく認証	加入者認証情報に基づく認証
接続先1	要	要
接続先2	要	不要
接続先3	不要	要
接続先4	不要	不要

フロントページの続き

(72)発明者　谷津　文平
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　池田　智彦
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　大谷　知行
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

Ｆターム(参考) 5J104 AA07　KA02　KA04　KA15　MA01　NA05　NA27　NA38