(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2005-149337
(P2005-149337A)
(43)公開日　平成17年6月9日(2005.6.9)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330D	5B085
G09C 1/00	G09C	1/00	640E	5J104
H04L 9/32	H04L	12/66	B	5K030
H04L 12/66	H04L	9/00	675A	
	H04L	9/00	675D	

審査請求 未請求　請求項の数 11　ＯＬ　（全 34 頁）　最終頁に続く

(21)出願番号　特願2003-388709 (P2003-388709)
(22)出願日　平成15年11月19日 (2003.11.19)

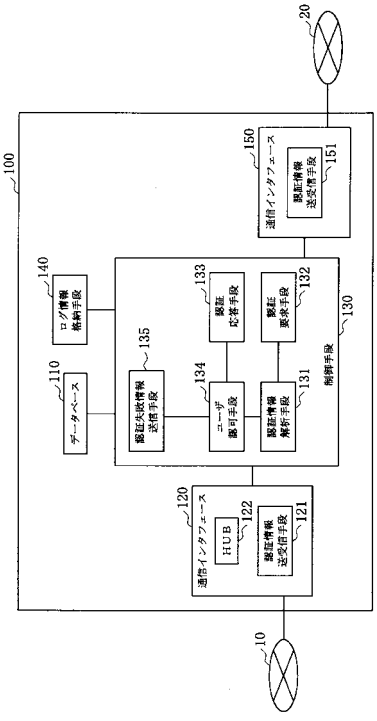
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100077274
弁理士　磯村　雅俊
(74)代理人　100102587
弁理士　渡邊　昌幸
(72)発明者　鍛冶　武志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山下　高生
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE02　AE03　AE04

最終頁に続く

(54)【発明の名称】ゲートウエイ装置

(57)【要約】
【課題】　ユーザの認証結果に応じて特定の仮想ネットワークとユーザが利用する通信端末とを接続させるための制御ができるゲートウエイ装置を提供すること。
【解決手段】　社内ネットワーク１０を構成する複数のＶＬＡＮのうち何れか１つとユーザが利用する通信端末とを接続させるユーザ認可手段１３４と、ユーザを認証するための認証情報を通信端末１１から受信する認証情報送受信手段１２１と、受信された認証情報に応じて認証ネットワーク２０にある認証サーバに認証の要求を行う認証要求手段１３２と、認証サーバから認証の要求に対する応答を表す認証応答情報を受信する認証応答手段１３３とを備え、認証応答情報が認証の成功を示していたとき、ユーザ認可手段１３４は、ユーザと対応する仮想ネットワークを識別するための仮想ネットワーク識別情報に従って仮想ネットワークとユーザが利用する通信端末とを接続させるように構成する。
【選択図】　図２



【特許請求の範囲】
【請求項１】
ユーザが利用する通信端末と第１のネットワークを介して通信可能に接続され、かつ前記ユーザを認証する認証サーバと第２のネットワークを介して通信可能に接続されたゲートウエイ装置において、
前記第１のネットワークを構成する複数の仮想ネットワークのうち何れか１つと前記ユーザが利用する通信端末とを接続させる仮想ネットワーク接続手段と、
前記ユーザを認証するための認証情報を前記通信端末から受信する認証情報受信手段と、
前記認証情報受信手段によって受信された認証情報に応じて前記認証サーバに認証の要求を行う認証要求手段と、
前記認証サーバから前記認証の要求に対する応答を表す認証応答情報を受信する認証応答手段とを備え、
前記認証応答手段によって受信された認証応答情報が前記認証の成功を示していたとき、
前記仮想ネットワーク接続手段は、前記ユーザと対応する仮想ネットワークを識別するための仮想ネットワーク識別情報に従って前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とするゲートウエイ装置。
【請求項２】
前記ゲートウエイ装置は、前記通信端末の仲介を行う仲介装置および前記通信端末と前記第１のネットワークを介して通信可能に接続され、
前記認証情報受信手段は、前記第１のネットワークを構成する前記複数の仮想ネットワークのうち何れか１つと前記ユーザが利用する通信端末とを接続する前記仲介装置から前記認証情報を受信し、
前記認証応答手段によって受信された認証応答情報が前記認証の成功を示していたとき、前記仮想ネットワーク接続手段は、前記ユーザと対応する仮想ネットワークと前記ユーザが利用する通信端末とを前記仲介装置に接続させることを特徴とする請求項１に記載のゲートウエイ装置。
【請求項３】
前記ゲートウエイ装置は、前記ユーザが利用可能な前記仲介装置を表す利用可能装置情報を格納する利用可能装置情報格納手段を備え、
前記仮想ネットワーク接続手段は、前記ユーザが前記仲介装置を利用可能か否かを前記利用可能装置情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを前記仲介装置に接続させることを特徴とする請求項２に記載のゲートウエイ装置。
【請求項４】
前記ゲートウエイ装置は、前記ユーザが利用可能な利用時間を表す利用時間情報を格納する利用時間情報格納手段を備え、
前記仮想ネットワーク接続手段は、前記ユーザが前記仮想ネットワークに接続可能か否かを前記利用時間情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とする請求項１から３のいずれか１項に記載のゲートウエイ装置。
【請求項５】
前記ゲートウエイ装置は、前記仮想ネットワーク識別情報を格納する仮想ネットワーク識別情報格納手段を備え、
前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とする請求項１から４のいずれか１項に記載のゲートウエイ装置。
【請求項６】
前記認証情報には、前記仮想ネットワークを識別するための仮想ネットワーク識別情報

が含まれ、
前記仮想ネットワーク接続手段は、前記認証情報に含まれる仮想ネットワーク識別情報が示す仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とする請求項１から４のいずれか１項に記載のゲートウエイ装置。
【請求項７】
前記ゲートウエイ装置は、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報を格納する許可情報格納手段を備え、
前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークに前記ユーザが接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とする請求項６に記載のゲートウエイ装置。
【請求項８】
前記認証情報には、前記ユーザを証明するための証明書が含まれ、
前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークと前記証明書に示されるユーザが利用する通信端末とを接続させることを特徴とする請求項１から５のいずれか１項に記載のゲートウエイ装置。
【請求項９】
前記証明書には、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報が含まれ、
前記仮想ネットワーク接続手段は、前記証明書に示されるユーザが前記仮想ネットワーク識別情報が示す仮想ネットワークに接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記証明書に示されるユーザが利用する通信端末とを接続させることを特徴とする請求項８に記載のゲートウエイ装置。
【請求項１０】
前記ゲートウエイ装置は、前記ユーザの利用可能な前記仮想ネットワークを問い合わせるための問い合わせ情報を前記通信端末から受信する問い合わせ情報受信手段と、
前記問い合わせ情報受信手段によって受信された問い合わせ情報に応じて前記許可情報格納手段から前記ユーザと対応するための仮想ネットワーク識別情報を前記ユーザが利用する通信端末に返答する仮想ネットワーク識別情報返答手段とを備えたことを特徴とする請求項７に記載のゲートウエイ装置。
【請求項１１】
前記ゲートウエイ装置は、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報を格納する許可情報格納手段を備え、
前記仲介装置は、前記第１のネットワークによって構成される全ての仮想ネットワークを表す情報を前記ユーザの利用する通信端末に通知し、
前記ユーザの利用する通信端末は、通知された情報に基づいて前記仮想ネットワークの優先度を与えた仮想ネットワークリストを作成し、
前記認証情報受信手段が前記仮想ネットワークリストを含む認証情報を受信したとき、
前記仮想ネットワーク接続手段は、前記仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順に前記ユーザが接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させることを特徴とする請求項２から４のいずれか１項に記載のゲートウエイ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、利用者が利用する端末とネットワークを介して通信可能に接続され、かつ他のネットワークとも通信可能に接続されたゲートウエイ装置に関するものである。
【背景技術】

【０００２】
近年、企業内で使用する企業ネットワークにおいては、企業ネットワークの管理コストを軽減するために、ユーザなどを認証するための認証サーバを企業ネットワークと接続せずに、ゲートウエイ装置を介して外部のネットワークと接続して、ユーザ認証を外部の企業に委託するような認証システムの研究開発が進められている。
【０００３】
例えば、図２４に示すように、企業ネットワークと外部のネットワークとを接続する従来の認証システムは、ネットワーク９２３およびネットワーク９１３を接続するＮＡＴ（Network Adress Translator）を搭載したゲートウエイ装置９２０と、ネットワーク９２３に接続された通信端末９２１ａおよび通信端末９２１ｂと、ネットワーク９１３に接続された認証代行サーバ９１２およびサーバ９１０とを備えた構成を有している。
【０００４】
上述の従来の認証システムとしては、ユーザが通信端末９２１ａを介してサーバ９１０ａへログインするとき、ユーザＩＤおよびパスワードを含む接続情報をゲートウエイ装置９２０を介して認証代行サーバ９１２に送信し、認証代行サーバ９１２が、送信された接続情報を認証し、認証が成功だったとき、ユーザに認証が成功したことを通信端末９２１ａに通知して、サーバ９１０ａまたはサーバ９１０ｂのログインが可能になるものが知られている（例えば特許文献１参照）。
【特許文献１】特開２００２－１２３４９１号公報（段落〔００３３〕、第２図）
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述のシステムでは、ユーザの認証結果に応じてサーバ９１０のログインが可能にすることができるが、ネットワーク９２３が複数の仮想ネットワークによって構成されていたとき、ユーザの認証結果に応じて仮想ネットワークと通信端末とを接続させるための制御ができないという課題が残されていた。
本発明は、従来の課題を解決するためになされたもので、ユーザの認証結果に応じて特定の仮想ネットワークとユーザが利用する通信端末とを接続させるための制御ができるゲートウエイ装置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】
【０００６】
請求項１に記載のゲートウエイ装置は、ユーザが利用する通信端末と第１のネットワークを介して通信可能に接続され、かつ前記ユーザを認証する認証サーバと第２のネットワークを介して通信可能に接続されたゲートウエイ装置において、前記第１のネットワークを構成する複数の仮想ネットワークのうち何れか１つと前記ユーザが利用する通信端末とを接続させる仮想ネットワーク接続手段と、前記ユーザを認証するための認証情報を前記通信端末から受信する認証情報受信手段と、前記認証情報受信手段によって受信された認証情報に応じて前記認証サーバに認証の要求を行う認証要求手段と、前記認証サーバから前記認証の要求に対する応答を表す認証応答情報を受信する認証応答手段とを備え、前記認証応答手段によって受信された認証応答情報が前記認証の成功を示していたとき、前記仮想ネットワーク接続手段は、前記ユーザと対応する仮想ネットワークを識別するための仮想ネットワーク識別情報に従って前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。
この構成により、認証応答情報が認証の成功を示していたとき、ユーザと対応する仮想ネットワークを識別するための仮想ネットワーク識別情報に従って、仮想ネットワークとユーザが利用する通信端末とを接続させるため、ユーザの認証結果に応じて特定の仮想ネットワークとユーザが利用する通信端末とを接続させるための制御ができる。
【０００７】
請求項２に記載のゲートウエイ装置は、前記通信端末の仲介を行う仲介装置および前記通信端末と前記第１のネットワークを介して通信可能に接続され、前記認証情報受信手段

は、前記第１のネットワークを構成する前記複数の仮想ネットワークのうち何れか１つと前記ユーザが利用する通信端末とを接続する前記仲介装置から前記認証情報を受信し、前記認証応答手段によって受信された認証応答情報が前記認証の成功を示していたとき、前記仮想ネットワーク接続手段は、前記ユーザと対応する仮想ネットワークと前記ユーザが利用する通信端末とを前記仲介装置に接続させる構成を有している。

この構成により、仲介装置が第１のネットワークを構築するためのロケーション毎に設置可能となるため、ユーザがネットワークに接続するための利便性を高めることができる。

【０００８】

請求項３に記載のゲートウエイ装置は、前記ユーザが利用可能な前記仲介装置を表す利用可能装置情報を格納する利用可能装置情報格納手段を備え、前記仮想ネットワーク接続手段は、前記ユーザが前記仲介装置を利用可能か否かを前記利用可能装置情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを前記仲介装置に接続させる構成を有している。

この構成により、ユーザが仲介装置を利用可能か否かを利用可能装置情報に従って判断し、接続可能と判断したとき仮想ネットワークとユーザが利用する通信端末とを仲介装置に接続させるため、ユーザに対して仲介装置の利用を制限することができる。

【０００９】

請求項４に記載のゲートウエイ装置は、前記ユーザが利用可能な利用時間を表す利用時間情報を格納する利用時間情報格納手段を備え、前記仮想ネットワーク接続手段は、前記ユーザが前記仮想ネットワークに接続可能か否かを前記利用時間情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。

この構成により、ユーザが仮想ネットワークに接続可能か否かを利用時間情報に従って判断し、接続可能と判断したとき仮想ネットワークとユーザが利用する通信端末とを接続させるため、ユーザに対して仮想ネットワークを利用する利用時間を制限することができる。

【００１０】

請求項５に記載のゲートウエイ装置は、前記仮想ネットワーク識別情報を格納する仮想ネットワーク識別情報格納手段を備え、前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。

この構成により、仮想ネットワーク識別情報が示す仮想ネットワークとユーザが利用する通信端末とを接続させるため、ゲートウエイ装置が、ユーザと対応する仮想ネットワークを選択して接続させることができる。

【００１１】

請求項６に記載のゲートウエイ装置は、前記認証情報には、前記仮想ネットワークを識別するための仮想ネットワーク識別情報が含まれ、前記仮想ネットワーク接続手段は、前記認証情報に含まれる仮想ネットワーク識別情報が示す仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。

この構成により、認証情報に含まれる仮想ネットワーク識別情報が示す仮想ネットワークとユーザが利用する通信端末とを接続させるため、ユーザが、ユーザと対応する仮想ネットワークを選択して接続させることができる。

【００１２】

請求項７に記載のゲートウエイ装置は、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報を格納する許可情報格納手段を備え、前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークに前記ユーザが接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。

この構成により、仮想ネットワーク識別情報が示す仮想ネットワークにユーザが接続可能か否かを許可情報に従って判断し、接続可能と判断したとき仮想ネットワークとユーザが利用する通信端末とを接続させるため、ユーザが利用できる仮想ネットワークを制限することができる。

【００１３】

請求項８に記載のゲートウエイ装置は、前記認証情報には、前記ユーザを証明するための証明書が含まれ、前記仮想ネットワーク接続手段は、前記仮想ネットワーク識別情報が示す仮想ネットワークと前記証明書に示されるユーザが利用する通信端末とを接続させる構成を有している。

この構成により、仮想ネットワーク識別情報が示す仮想ネットワークと証明書に示されるユーザが利用する通信端末とを接続させるため、ユーザを識別するための情報などを偽って仮想ネットワークを不正に利用することを防止できる。

【００１４】

請求項９に記載のゲートウエイ装置は、前記証明書には、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報が含まれ、前記仮想ネットワーク接続手段は、前記証明書に示されるユーザが前記仮想ネットワーク識別情報が示す仮想ネットワークに接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記証明書に示されるユーザが利用する通信端末とを接続させる構成を有している。

この構成により、証明書に示されるユーザが仮想ネットワーク識別情報が示す仮想ネットワークに接続可能か否かを許可情報に従って判断し、接続可能と判断したとき仮想ネットワークと証明書に示されるユーザが利用する通信端末とを接続させるため、証明書に従ってユーザが利用できる仮想ネットワークを制限することができる。

【００１５】

請求項１０に記載のゲートウエイ装置は、前記ユーザの利用可能な前記仮想ネットワークを問い合わせるための問い合わせ情報を前記通信端末から受信する問い合わせ情報受信手段と、前記問い合わせ情報受信手段によって受信された問い合わせ情報に応じて前記許可情報格納手段から前記ユーザと対応するための仮想ネットワーク識別情報を前記ユーザが利用する通信端末に返答する仮想ネットワーク識別情報返答手段とを備えた構成を有している。

この構成により、ユーザからの問い合わせに応じて仮想ネットワーク識別情報を返答するため、予めユーザが仮想ネットワーク識別情報を知らなくても、接続可能な仮想ネットワーク識別情報をユーザに通知でき、接続可能な仮想ネットワーク識別情報が複数あるときには、ユーザが望む仮想ネットワークと接続することができる。

【００１６】

請求項１１に記載のゲートウエイ装置は、前記複数の仮想ネットワークのうち前記ユーザが利用可能な前記仮想ネットワークだけに接続することを許可するための許可情報を格納する許可情報格納手段を備え、前記仲介装置は、前記第１のネットワークによって構成される全ての仮想ネットワークを表す情報を前記ユーザの利用する通信端末に通知し、前記ユーザの利用する通信端末は、通知された情報に基づいて前記仮想ネットワークの優先度を与えた仮想ネットワークリストを作成し、前記認証情報受信手段が前記仮想ネットワークリストを含む認証情報を受信したとき、前記仮想ネットワーク接続手段は、前記仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順に前記ユーザが接続可能か否かを前記許可情報に従って判断し、接続可能と判断したとき前記仮想ネットワークと前記ユーザが利用する通信端末とを接続させる構成を有している。

この構成により、仮想ネットワークの優先度が与えられた仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順にユーザが接続可能か否かを許可情報に従って判断するため、ユーザが望む優先度の高い順に仮想ネットワークと接続することができる

【発明の効果】

【００１７】
本発明は、ユーザの認証結果に応じて特定の仮想ネットワークとユーザが利用する通信端末とを接続させるための制御ができるゲートウエイ装置を提供するものである。
【発明を実施するための最良の形態】
【００１８】
以下、図面を参照して本発明の実施の形態について詳細に説明する。
図１は、本発明の第１の実施の形態に係る認証システムのシステム構成図である。
図１に示すように、認証システム１０００は、ユーザが利用する通信端末１１ａから通信端末１１ｄと、情報を中継するゲートウエイ装置１００とが、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置１００と、ユーザを認証する認証サーバ２１とが認証ネットワーク２０を介して通信可能に接続された構成を有している。
【００１９】
なお、通信端末１１ａ～１１ｄは、無線の通信が可能な携帯端末、若しくは、パソコンなどでもよい。図１には、通信端末１１を４つ図示しているが個数は限定されない。社内ネットワーク１０または認証ネットワーク２０は、有線、無線を問わない。社内ネットワーク１０は、ＬＡＮなどであり、会社内で用いられるネットワークに限定されるものではない。また、社内ネットワーク１０は、複数の仮想ネットワークによって構成され、仮想ネットワークは、例えば、ＶＬＡＮ（Virtual Local Area Network）３１、およびＶＬＡＮ３２を含む。以下、仮想ネットワークをＶＬＡＮとして説明する。
【００２０】
また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末１１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通信端末１１ａを利用し、ユーザｂが通信端末１１ｂを利用し、ユーザｃが通信端末１１ｃを利用し、ユーザｄが通信端末１１ｄを利用するものとする。
【００２１】
通信端末１１を利用するユーザがＶＬＡＮにログインするとき、通信端末１１は、ユーザを認証するための認証情報をゲートウエイ装置１００に送信するようになっている。ゲートウエイ装置１００は、通信端末１１から送信された認証情報を受信し、受信した認証情報に応じて認証サーバ２１に認証の要求を行うようになっている。
【００２２】
ゲートウエイ装置１００が認証の要求を行ったとき、認証サーバ２１は、認証情報に基づいてユーザの認証を行い、この認証の結果を表す情報であって認証の要求に対する応答を表す認証応答情報をゲートウエイ装置１００に送信するようになっている。
【００２３】
ゲートウエイ装置１００は、認証サーバ２１から送信された認証応答情報を受信し、受信した認証応答情報が認証の成功を示していたとき、ＶＬＡＮ３１およびＶＬＡＮ３２のうち１つとユーザが利用する通信端末１１とを接続するようになっている。管理端末１２は、認証失敗情報などを表示する。
【００２４】
図２は、本発明の第１の実施の形態に係るゲートウエイ装置のブロック構成図である。図２に示すように、ゲートウエイ装置１００は、データベース１１０、通信インタフェース１２０、制御手段１３０、ログ情報格納手段１４０、通信インタフェース１５０を含むように構成される。
【００２５】
データベース１１０（利用時間情報格納手段、仮想ネットワーク識別情報格納手段）は、ユーザが接続するＶＬＡＮを識別するための仮想ネットワーク識別情報、およびユーザが利用可能な利用時間を表す利用時間情報を格納するようになっている。ここで、データベース１１０が格納する情報の一例を表１に示す。以下、仮想ネットワーク識別情報をＶＬＡＮ番号として説明する。
【００２６】

【表１】

ユーザ識別子	内容			備考
	ＶＬＡＮ番号	曜日	時間	
ユーザａ	３１	制限なし	制限なし	社員（管理職）
ユーザｂ	３２	月曜～金曜	９時～１８時	派遣社員
ユーザｃ	３１	月曜～金曜	９時～２２時	社員（組合員）
ユーザｄ	３２	月曜～金曜	９時～１８時	来訪者

【００２７】
表１に示したように、例えば、ユーザａは、管理職の社員であり、ＶＬＡＮ３１を利用可能であり、利用時間には制限がない。また、ユーザｂは、派遣社員であり、ＶＬＡＮ３２を利用可能であり、９時から１８時まで利用可能である。ユーザｃは、組合員の社員であり、ＶＬＡＮ３１を利用可能であり、９時から２２時まで利用可能である。また、ユーザｄは、来訪者であり、ＶＬＡＮ３２を利用可能であり、９時から１８時まで利用可能である。

【００２８】
通信インタフェース１２０は、社内ネットワーク１０と通信するようになっており、認証情報送受信手段１２１および仮想ネットワーク接続手段（ＨＵＢ）１２２を含むように構成される。

【００２９】
認証情報送受信手段１２１は、例えば、ＥＡＰ－ＴＬＳ（PPP Extensible Authentication Protocol－Transport Layer Security）などの認証に関する認証プロトコルに準拠して通信端末１１と通信するようになっている。また、認証情報送受信手段１２１は、ＥＡＰ－ＴＬＳに準拠したパケットを用いて、ユーザを認証するための認証情報を通信端末１１から受信するようになっている。仮想ネットワーク接続手段（ＨＵＢ）１２２は、ＶＬＡＮ用のＨＵＢで構成されていてもよく、複数のＶＬＡＮのうち１つのＶＬＡＮと通信端末１１とを接続するようになっている。

【００３０】
制御手段１３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段１３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段１３４、および認証失敗情報送信手段１３５を有している。なお、これらの手段はプログラムのモジュールでもよい。

【００３１】
認証情報解析手段１３１は、認証情報送受信手段１２１が受信した認証プロトコルに準拠した認証情報を含む情報を解析するようになっている。例えば、認証情報解析手段１３１は、ＥＡＰ－ＴＬＳに準拠したパケットに含まれるユーザ識別子などの認証情報を解析するようになっている。

【００３２】
認証要求手段１３２は、認証情報解析手段１３１が解析した認証情報に応じて認証サーバ２１に認証の要求を行うようになっている。例えば、認証要求手段１３２は、認証情報を含むパケットを認証サーバ２１に送信することにより、認証の要求を行うようになっている。

【００３３】
認証応答手段１３３は、認証の結果を表す情報であって、認証の要求に対する応答を表す認証応答情報を認証サーバ２１から通信インタフェース１５０を介して受信するように

なっている。例えば、認証応答手段１３３は、Ｒａｄｉｕｓ（Remote Authentication Dial-In User Service）に準拠したAccess-Acceptパケット、Access-Challengeパケット、またはAccess-Rejectパケットを受信するようにしてもよい。なお、認証要求となるAccess-Requestパケットに対応するパケットは認証応答となるAccess-Challegeパケットであり、Access-AcceptパケットおよびAccess-Rejectパケットは認証結果を知らせるためのパケットである。

【００３４】

ユーザ認可手段１３４は、認証応答手段１３３によって受信された認証応答情報が認証の成功を示していたとき、認証情報に含まれていたユーザ識別子と対応するＶＬＡＮ番号をデータベース１１０から取得し、取得したＶＬＡＮ番号と対応するＶＬＡＮと通信端末１１とをＨＵＢ１２２に接続させるようになっている。

【００３５】

また、ユーザ認可手段１３４は、ユーザ識別子と対応する利用時間情報をデータベース１１０から取得し、取得した利用時間情報に従ってＶＬＡＮに接続可能か判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段１３４が、ＶＬＡＮ番号と対応するＶＬＡＮと通信端末１１とをＨＵＢ１２２に接続させるようになっている。

【００３６】

例えば、ユーザａを認証する場合、ユーザ認可手段１３４は、ユーザａと対応する「３１」を表すＶＬＡＮ番号、および利用時間情報をデータベース１１０から取得し、取得した利用時間情報が無制限を表しているため接続可能と判断し、ＶＬＡＮ３１と通信端末１１ａとをＨＵＢ１２２に接続させるようになっている。

【００３７】

また、ユーザ認可手段１３４は、認証応答情報が認証の失敗を示していたとき、認証失敗の旨を表す認証失敗情報をログ情報格納手段１４０に出力するようになっている。認証失敗情報送信手段１３５は、ユーザ認可手段１３４によって出力された認証失敗情報を管理端末１２に表示するようになっている。

【００３８】

ログ情報格納手段１４０は、社内ネットワーク１０および認証ネットワーク２０から通信インタフェース１２０および通信インタフェース１５０を介して送受信された情報を格納し、格納した情報を不図示のディスプレイなどに表示するようになっている。また、ログ情報格納手段１４０は、ユーザ認可手段１３４によって出力された認証失敗情報を格納するようにしてもよい。

【００３９】

通信インタフェース１５０は、認証ネットワーク２０と通信するようになっており、認証情報送受信手段１５１を含むように構成される。認証情報送受信手段１５１は、例えば、Ｒａｄｉｕｓを含む認証に関するプロトコルに準拠して認証サーバ２１と通信するようになっている。

【００４０】

認証情報送受信手段１５１は、認証情報送受信手段１２１によって受信された認証情報を含むAccess-Requestパケットに応じて認証サーバ２１に認証の要求を行うようになっている。また、認証情報送受信手段１５１は、認証の要求に対する応答を表す認証応答情報を認証サーバ２１から受信し、受信した認証応答情報を認証応答手段１３３に出力するようになっている。例えば、認証情報送受信手段１５１は、Ｒａｄｉｕｓに準拠したAccess-AcceptパケットまたはAccess-Rejectパケットを受信するようになっている。

【００４１】

以下、本発明の第１の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図３は、本発明の第１の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。

【００４２】

まず、通信端末１１から送信された認証情報は、認証情報送受信手段１２１によって受

信される（Ｓ１０１）。次に、利用時間情報は、認証情報解析手段１３１が認証情報を解析した後に、データベース１１０から取得され、取得された利用時間情報に基づいてＶＬＡＮに接続可能か否かが、ユーザ認可手段１３４によって判断される（Ｓ１０２）。

【００４３】

接続可能と判断されたとき、認証情報解析手段１３１が解析した認証情報に応じて認証サーバ２１に対する認証の要求が、認証要求手段１３２によって行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。

【００４４】

認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、ユーザと対応するＶＬＡＮ番号が、ユーザ認可手段１３４によってデータベース１１０から取得され、通信端末１１は、取得されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ１０６）。

【００４５】

以上説明したように、本発明の第１の実施の形態に係るゲートウエイ装置は、認証応答情報が認証の成功を示していたとき、ユーザと対応するＶＬＡＮを識別するための仮想ネットワーク識別情報に従って、ＶＬＡＮ３１またはＶＬＡＮ３２とユーザが利用する通信端末１１とを接続させるため、ユーザの認証結果に応じて特定のＶＬＡＮとユーザが利用する通信端末１１とを接続させるための制御ができる。

また、ユーザがＶＬＡＮに接続可能か否かを利用時間情報に従って判断し、接続可能と判断したときＶＬＡＮ３１またはＶＬＡＮ３２とユーザが利用する通信端末１１とを接続させるため、ユーザに対してＶＬＡＮを利用する利用時間を制限することができる。

さらに、仮想ネットワーク識別情報が示すＶＬＡＮとユーザが利用する通信端末１１とを接続させるため、ゲートウエイ装置１００が、ユーザと対応するＶＬＡＮを選択して接続させることができる。

【００４６】

図４は、本発明の第２の実施の形態に係る認証システムのシステム構成図である。

図４に示すように、認証システム２０００は、ユーザが利用する通信端末４１ａから通信端末４１ｄと、情報を中継するゲートウエイ装置２００と、通信端末４１ａ～４１ｄの仲介を行う認証クライアント１３ａ、ｂ（仲介装置）が、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置２００と、ユーザを認証する認証サーバ２１とが認証ネットワーク２０を介して通信可能に接続された構成を有している。

【００４７】

なお、本発明の第２の実施の形態に係る認証システムを構成する要素のうち、本発明の第１の実施の形態に係る認証システムを構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【００４８】

また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末４１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通信端末４１ａを利用し、ユーザｂが通信端末４１ｂを利用し、ユーザｃが通信端末４１ｃを利用し、ユーザｄが通信端末４１ｄを利用するものとする。

【００４９】

例えば、通信端末４１を利用するユーザがＶＬＡＮにログインするとき、通信端末４１は、ユーザを認証するための認証情報を認証クライアント１３を介してゲートウエイ装置２００に送信するようになっている。

【００５０】

認証クライアント１３は、通信端末４１から送信された認証情報をゲートウエイ装置２００に中継するようになっており、社内ネットワーク１０を構成するＶＬＡＮ３１およびＶＬＡＮ３２のうち、ゲートウエイ装置２００から送信されたＶＬＡＮ番号と対応するＶＬＡＮと通信端末４１とを接続するようになっている。また、認証クライアント１３は、

社内ネットワーク１０を構築するためのロケーション毎に設置されるものであり、例えば、ビルの各階に設置されるようにしてもよい。

【００５１】

図５は、本発明の第２の実施の形態に係る認証システムのシーケンスのイメージ図である。通信端末４１と認証クライアント１３との間は、ＥＡＰ－ＴＬＳ（PPP Extensible Authentication Protocol－Transport Layer Security）に準拠した認証が行われる。また、認証クライアント１３から認証サーバ２１までの間は、Ｒａｄｉｕｓに準拠した認証が行われる。認証クライアント１３は、ＥＡＰ－ＴＬＳに準拠したパケットとＲａｄｉｕｓに準拠したパケットとの変換を相互に行うようになっている。

【００５２】

ゲートウエイ装置２００は、認証クライアント１３から送信された認証情報を含むAccess-Requestパケットを認証サーバ２１に中継し、認証サーバ２１から送信された認証応答情報を含むAccess-Acceptパケットを、認証クライアント１３に中継するようになっている。

【００５３】

なお、認証サーバ２１からAccess-Acceptパケットを受信したとき、ゲートウエイ装置２００は、認証情報に含まれていたユーザ識別子と対応するＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを、Access-Requestパケットを送信した認証クライアント１３に送信することにより、ＶＬＡＮと通信端末４１とを接続させるようになっている。

【００５４】

図６は、本発明の第２の実施の形態に係るゲートウエイ装置のブロック構成図である。図６に示すように、ゲートウエイ装置２００は、データベース２１０、通信インタフェース２２０、制御手段２３０、ログ情報格納手段１４０、および通信インタフェース１５０を含むように構成される。なお、本シーケンスのイメージは一例であり、本発明は他の認証に関するプロトコルを用いてもよい。

【００５５】

なお、本発明の第２の実施の形態に係るゲートウエイ装置を構成する要素のうち、本発明の第１の実施の形態に係るゲートウエイ装置を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【００５６】

データベース２１０（利用可能装置情報格納手段、利用時間情報格納手段、仮想ネットワーク識別情報格納手段）は、ユーザが接続するＶＬＡＮを識別するためのＶＬＡＮ番号、ユーザが利用可能な利用時間を表す利用時間情報、およびユーザが利用可能な認証クライアント１３を表す利用可能装置情報を格納するようになっている。ここで、データベース２１０が格納する情報の一例を表２に示す。

【００５７】

【表２】

ユーザ識別子	内容			備考
	ＶＬＡＮ番号	時間	認証クライアント	
ユーザａ	３１	制限なし	ａ、ｂ	社員（管理職）
ユーザｂ	３２	９時～１８時	ａ、ｂ	派遣社員
		１８時～２２時	ｂ	
ユーザｃ	３１	９時～２２時	ａ、ｂ	社員（組合員）
ユーザｄ	３２	９時～１８時	ｂ	来訪者

【００５８】
表２に示したように、例えば、ユーザａは、管理職の社員であり、ＶＬＡＮ３１を利用可能であり、利用時間には制限がなく、認証クライアント１３ａおよび認証クライアント１３ｂを利用可能である。また、ユーザｂは、派遣社員であり、ＶＬＡＮ３２を利用可能であり、９時から２２時まで利用可能であり、９時から１８時まで認証クライアント１３ａおよび認証クライアント１３ｂを利用可能であり、１８時から２２時まで認証クライアント１３ｂのみ利用可能である。ユーザｃは、組合員の社員であり、ＶＬＡＮ３１を利用可能であり、9時から２２時まで利用可能であり、認証クライアント１３ａおよび認証クライアント１３ｂを利用可能である。また、ユーザｄは、来訪者であり、ＶＬＡＮ３２を利用可能であり、９時から１８時まで利用可能であり、認証クライアント１３ｂのみ利用可能である。

【００５９】
通信インタフェース２２０は、社内ネットワーク１０と通信するようになっており、認証情報送受信手段１２１を含むように構成される。

【００６０】
制御手段２３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段２３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段２３４、および認証失敗情報送信手段１３５を有している。なお、これらの手段はプログラムのモジュールでもよい。

【００６１】
ユーザ認可手段２３４（仮想ネットワーク接続手段）は、認証応答手段１３３によって受信された認証応答情報が認証の成功を示していたとき、認証情報に含まれていたユーザ識別子と対応するＶＬＡＮ番号をデータベース２１０から取得し、取得したＶＬＡＮ番号に従ってＶＬＡＮと通信端末４１とを認証クライアント１３に接続させるようになっている。例えば、ユーザ認可手段２３４は、取得したＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを認証クライアント１３に送信することにより、ＶＬＡＮと通信端末４１とを接続させるようになっている。

【００６２】
例えば、ユーザａから認証クライアント１３ａを経由してAccess-Requestパケットが送信された後、認証サーバ２１からAccess-Acceptパケットが受信されたとき、ユーザ認可手段２３４は、ユーザａと対応する「３１」を表すＶＬＡＮ番号および認証クライアント１３ａ並びに認証クライアント１３ｂを表す利用可能装置情報をデータベース２１０から取得し、取得した利用可能装置情報に従って認証クライアント１３ａが利用できるため、取得した「３１」を表すＶＬＡＮ番号をAccess-Acceptパケットに含め、Access-Requestパケットを認証クライアント１３ａに送信するようになっている。

【００６３】
また、ユーザ認可手段２３４は、ユーザ識別子と対応する利用時間情報をデータベース２１０から取得し、取得した利用時間情報に従ってＶＬＡＮに接続可能か否かを判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段２３４が、ＶＬＡＮ番号と対応するＶＬＡＮと通信端末４１とを認証クライアント１３に接続させるようになっている。
【００６４】
例えば、時刻１９時にユーザｂから認証クライアント１３ａを経由してAccess-Requestパケットが送信された後、認証サーバ２１からAccess-Acceptパケットが受信されたとき、ユーザ認可手段２３４は、ユーザｂと対応する「３２」を表すＶＬＡＮ番号、「１８時～２２時」を表す利用時間情報、および認証クライアント１３ｂを表す利用可能装置情報をデータベース２１０から取得し、取得した利用可能装置情報に従って認証クライアント１３ｂが利用できるため、接続を許可しないようになっている。
【００６５】
また、ユーザ認可手段２３４は、認証応答情報が認証の失敗を示していたとき、認証失敗の旨を表す認証失敗情報をログ情報格納手段１４０に出力するようになっている。
【００６６】
以下、本発明の第２の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図７は、本発明の第２の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。
【００６７】
なお、本発明の第２の実施の形態に係るゲートウエイ装置の動作のうち、本発明の第１の実施の形態に係るゲートウエイ装置の動作と同一のものについては、同一の符号を付す。
【００６８】
まず、通信端末４１から送信された認証情報は、認証情報送受信手段１２１によって受信される（Ｓ１０１）。次に、利用時間情報は、認証情報解析手段１３１が認証情報を解析した後に、ユーザ認可手段２３４によってデータベース２１０から取得され、取得された利用時間情報に従ってＶＬＡＮに接続可能か否かが、ユーザ認可手段２３４によって判断される（Ｓ１０２）。
【００６９】
接続可能と判断されたとき、さらに、データベース２１０から取得され、取得された利用可能装置情報に従って、ユーザがAccess-Requestパケットを送信した認証クライアント１３を利用可能か否かが、ユーザ認可手段２３４によって判断される（Ｓ２０１）。
【００７０】
認証クライアント１３を利用可能と判断されたとき、認証情報解析手段１３１が解析した認証情報に応じて認証サーバ２１に対する認証の要求が、認証要求手段１３２によって行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。
【００７１】
認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、ユーザと対応するＶＬＡＮ番号が、ユーザ認可手段２３４によってデータベース２１０から取得され、通信端末４１は、取得されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ１０６）。
【００７２】
以上説明したように、本発明の第２の実施の形態に係るゲートウエイ装置は、認証クライアント１３が社内ネットワーク１０を構築するためのロケーション毎に設置可能となるため、ユーザがネットワークに接続するための利便性を高めることができる。
また、ユーザが認証クライアント１３を利用可能か否かを利用可能装置情報に従って判断し、接続可能と判断したときＶＬＡＮ３１またはＶＬＡＮ３２とユーザが利用する通信

端末４１とを認証クライアント１３に接続させるため、ユーザに対して認証クライアント１３の利用を制限することができる。

【００７３】

図８は、本発明の第３の実施の形態に係る認証システムのシステム構成図である。図８に示すように、認証システム３０００は、ユーザが利用する通信端末５１ａから通信端末５１ｄと、情報を中継するゲートウエイ装置３００と、通信端末５１の仲介を行う認証クライアント５３ａ、ｂ（仲介装置）が、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置３００とユーザを認証する認証サーバ２１とが認証ネットワーク２０を介して通信可能に接続された構成を有している。

【００７４】

なお、本発明の第３の実施の形態に係る認証システムを構成する要素のうち、本発明の第２の実施の形態に係る認証システムを構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【００７５】

また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末５１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通信端末５１ａを利用し、ユーザｂが通信端末５１ｂを利用し、ユーザｃが通信端末５１ｃを利用し、ユーザｄが通信端末５１ｄを利用するものとする。

【００７６】

例えば、通信端末５１を利用するユーザがＶＬＡＮにログインするとき、通信端末５１は、ユーザを認証するための認証情報を認証クライアント５３を介してゲートウエイ装置３００に送信するようになっている。なお、認証情報には、ＶＬＡＮ（Virtual Local Area Network）３１およびＶＬＡＮ３２のうち何れか１つのＶＬＡＮを識別するためのＶＬＡＮ番号が含まれる。

【００７７】

認証クライアント５３は、通信端末５１から送信された認証情報をゲートウエイ装置３００に中継するようになっており、社内ネットワーク１０を構成するＶＬＡＮ３１およびＶＬＡＮ３２のうち、ゲートウエイ装置３００から送信されたＶＬＡＮ番号と対応するＶＬＡＮと通信端末５１とを接続するようになっている。また、認証クライアント５３は、社内ネットワーク１０を構築するためのロケーション毎に設置されるものであり、例えば、ビルの各階に設置されるようにしてもよい。

【００７８】

図９は、本発明の第３の実施の形態に係る認証システムのシーケンスのイメージ図である。通信端末５１と認証クライアント５３との間は、ＥＡＰ－ＴＬＳ（PPP Extensible Authentication Protocol－Transport Layer Security）に準拠した認証が行われる。

また、認証クライアント５３から認証サーバ２１までの間は、ＥＡＰ－ＴＬＳをサポートするＲａｄｉｕｓに準拠した認証が行われる。認証クライアント５３は、ＥＡＰ－ＴＬＳに準拠したパケットとＲａｄｉｕｓに準拠したパケットとの変換を相互に行うようになっている。

【００７９】

さらに、認証クライアント５３は、ＶＬＡＮ番号を含む認証情報であって、この認証情報を含むＥＡＰ－Ｒｅｓｐｏｎｓｅパケットを通信端末５１から受信し、受信したＥＡＰ－ＲｅｓｐｏｎｓｅパケットをＲａｄｉｕｓに準拠したAccess-Requestパケットに変換し、変換したAccess-Requestパケットをゲートウエイ装置３００に送信するようになっている。なお、認証クライアント５３は、ＥＡＰ－Ｒｅｓｐｏｎｓｅパケットに含まれるＶＬＡＮ番号をAccess-Requestパケットに引き継いでゲートウエイ装置３００に送信するようになっている。

【００８０】

ゲートウエイ装置３００は、認証クライアント５３から送信されたAccess-Requestパケットを認証サーバ２１に中継し、認証サーバ２１から送信された認証応答情報を含むAcce

ss-Acceptパケットを認証クライアント５３に中継するようになっている。

なお、ゲートウエイ装置３００は、認証クライアント５３から送信されたAccess-Requestパケットを受信し、受信したAccess-Requestパケットに含まれるＶＬＡＮ番号を取り除いて、認証サーバ２１に中継するようになっている。

【００８１】

なお、ゲートウエイ装置３００は、Access-Acceptパケットを受信したとき、Access-Requestパケットに含まれていたＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを、Access-Requestパケットを送信した認証クライアント５３に送信することにより、ＶＬＡＮと通信端末５１とを接続させるようになっている。

【００８２】

図１０は、本発明の第３の実施の形態に係るゲートウエイ装置のブロック構成図である。図１０に示すように、ゲートウエイ装置３００は、データベース３１０、通信インタフェース２２０、制御手段３３０、ログ情報格納手段１４０、および通信インタフェース１５０を含むように構成される。

【００８３】

なお、本発明の第３の実施の形態に係るゲートウエイ装置を構成する要素のうち、本発明の第２の実施の形態に係るゲートウエイ装置を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【００８４】

データベース３１０（利用可能装置情報格納手段、利用時間情報格納手段、許可情報格納手段）は、ユーザが接続するＶＬＡＮを識別するためのＶＬＡＮ番号であって、複数のＶＬＡＮのうち利用可能なＶＬＡＮだけに、ＶＬＡＮの接続を許可する許可情報、ユーザが利用可能な利用時間を表す利用時間情報、およびユーザが利用可能な認証クライアント５３を表す利用可能装置情報を格納するようになっている。ここで、データベース３１０が格納する情報の一例を表３に示す。

【００８５】

【表３】

ユーザ識別子	内容			備考
	ＶＬＡＮ番号（許可情報）	時間	認証クライアント	
ユーザａ	３１、３２	制限なし	ａ、ｂ	社員（管理職）
ユーザｂ	３２	９時～１８時	ａ、ｂ	派遣社員
		１８時～２２時	ｂ	
ユーザｃ	３１、３２	９時～２２時	ａ、ｂ	社員（組合員）
ユーザｄ	３２	９時～１８時	ｂ	来訪者

【００８６】

表３に示したように、例えば、ユーザａは、管理職の社員であり、ＶＬＡＮ３１およびＶＬＡＮ３２だけを利用可能であり、利用時間には制限がなく、認証クライアント５３ａおよび認証クライアント５３ｂを利用可能である。また、ユーザｂは、派遣社員であり、ＶＬＡＮ３２だけを利用可能であり、９時から２２時まで利用可能であり、９時から１８時まで認証クライアント５３ａおよび認証クライアント５３ｂを利用可能であり、１８時から２２時まで認証クライアント５３ｂのみ利用可能である。ユーザｃは、組合員の社員であり、ＶＬＡＮ３１およびＶＬＡＮ３２だけを利用可能であり、9時から２２時まで利用可能であり、認証クライアント５３ａおよび認証クライアント５３ｂを利用可能である。また、ユーザｄは、来訪者であり、ＶＬＡＮ３２だけを利用可能であり、９時から１８

時まで利用可能であり、認証クライアント５３ｂのみが利用可能である。

【００８７】

制御手段３３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段３３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段３３４、および認証失敗情報送信手段１３５を有している。なお、これらの手段はプログラムのモジュールでもよい。

【００８８】

ユーザ認可手段３３４は、ＶＬＡＮ番号を含む認証情報が認証クライアント５３を介して送信されたとき、認証情報に含まれるＶＬＡＮ番号を記憶し、記憶したＶＬＡＮ番号を認証情報から取り除き、ＶＬＡＮ番号が取り除かれた認証情報を認証情報送受信手段１５１に出力するようになっている。その後、ユーザ認可手段３３４は、認証応答手段１３３によって受信された認証応答情報が認証の成功を示していたとき、記憶したＶＬＡＮ番号と対応するＶＬＡＮと通信端末５１とを認証クライアント５３に接続させるようになっている。

【００８９】

例えば、ＶＬＡＮ番号「３２」を含むAccess-Requestパケットが、ユーザｂから認証クライアント５３ａを介して送信されたとき、ユーザ認可手段３３４は、Access-Requestパケットに含まれるＶＬＡＮ番号「３２」を記憶し、Access-RequestパケットからＶＬＡＮ番号「３２」を取り除くようになっている。その後、ユーザ認可手段３３４は、認証応答手段１３３がAccess-Acceptパケットを受信したとき、ＶＬＡＮ番号「３２」をAccess-Acceptパケットに含め、このAccess-Acceptパケットを認証クライアント５３ｂに送信することにより、通信端末５１ｂとを認証クライアント５３ａに接続させるようになっている。

【００９０】

また、ユーザ認可手段３３４は、認証情報が認証クライアント５３を介して送信されたとき、認証情報に含まれていたユーザ識別子と対応する許可情報をデータベース３１０から取得し、取得した許可情報に従って、認証情報に含まれるＶＬＡＮ番号と対応するＶＬＡＮに接続可能か否かを判断するようにしてもよい。接続可能と判断したとき、ユーザ認可手段３３４は、認証情報に含まれるＶＬＡＮ番号に従ってＶＬＡＮと通信端末５１とを認証クライアント５３に接続させるようになっている。

【００９１】

例えば、ＶＬＡＮ番号「３１」を含むAccess-Requestパケットが、ユーザｂから認証クライアント５３ａを介して送信されたとき、ユーザ認可手段３３４は、ＶＬＡＮ３２だけ利用可能を表す許可情報をデータベース３１０から取得し、取得した許可情報がＶＬＡＮ３２を表しているため、接続を許可しないようになっている。

【００９２】

また、ユーザ認可手段３３４は、ユーザ識別子と対応する利用時間情報をデータベース３１０から取得し、取得した利用時間情報に従ってＶＬＡＮに接続可能か否かを判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段３３４が、ＶＬＡＮ番号に従ってＶＬＡＮと通信端末５１とを認証クライアント５３に接続させるようになっている。

【００９３】

さらに、ユーザ認可手段３３４は、ユーザ識別子と対応する利用可能装置情報をデータベース３１０から取得し、取得した利用可能装置情報に従って、ユーザがAccess-Requestパケットを送信した認証クライアント５３を利用可能か否かを判断するようにしてもよい。利用可能と判断したときには、ユーザ認可手段３３４が、ＶＬＡＮ番号に従ってＶＬＡＮと通信端末５１とを認証クライアント５３に接続させるようになっている。

【００９４】

また、ユーザ認可手段３３４は、認証応答情報が認証の失敗を示していたとき、認証失

敗の旨を表す認証失敗情報をログ情報格納手段１４０に出力するようになっている。

【００９５】

以下、本発明の第３の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図１１は、本発明の第３の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。

【００９６】

なお、本発明の第３の実施の形態に係るゲートウエイ装置の動作のうち、本発明の第２の実施の形態に係るゲートウエイ装置の動作と同一のものについては、同一の符号を付す。

【００９７】

まず、通信端末５１から送信されたＶＬＡＮ番号を含む認証情報は、認証情報送受信手段１２１によって受信される（Ｓ１０１）。次に、ユーザ識別子と対応する利用時間情報は、ユーザ認可手段３３４によってデータベース３１０から取得され、取得された利用時間情報に従ってＶＬＡＮに接続可能か否かが、ユーザ認可手段３３４によって判断される（Ｓ３０１）。

【００９８】

接続可能と判断されたとき、さらに、ユーザ識別子と対応する利用可能装置情報がデータベース３１０から取得され、取得された利用可能装置情報に従って、ユーザが認証情報を送信した認証クライアント５３を利用可能か否かが、ユーザ認可手段３３４によって判断され、認証クライアント５３を利用可能と判断されたとき、認証情報に含まれるＶＬＡＮ番号が、ユーザ認可手段３３４によって記憶され、認証情報に含まれるＶＬＡＮ番号が取り除かれる（Ｓ３０２）。

【００９９】

認証クライアント５３を利用可能と判断されたとき、認証サーバ２１に対する認証の要求が、認証要求手段１３２によって認証情報解析手段１３１が解析した認証情報に応じて行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。

【０１００】

認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、通信端末５１は、ユーザ認可手段３３４によって記憶されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ３０３）。

【０１０１】

以上説明したように、本発明の第３の実施の形態に係るゲートウエイ装置は、認証情報に含まれる仮想ネットワーク識別情報が示すＶＬＡＮとユーザが利用する通信端末５１とを接続させるため、ユーザが、ユーザと対応するＶＬＡＮを選択して接続させることができる。

また、仮想ネットワーク識別情報が示すＶＬＡＮにユーザが接続可能か否かを許可情報に従って判断し、接続可能と判断したときＶＬＡＮ３１またはＶＬＡＮ３２とユーザが利用する通信端末５３とを接続させるため、ユーザが利用できるＶＬＡＮを制限することができる。

【０１０２】

図１２は、本発明の第４の実施の形態に係る認証システムのシステム構成図である。図１２に示すように、認証システム４０００は、ユーザが利用する通信端末６１ａから通信端末６１ｄと、情報を中継するゲートウエイ装置４００と、通信端末６１の仲介を行う認証クライアント６３ａ、ｂ（仲介装置）が、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置４００と、ユーザを認証する認証サーバ２１と、ユーザを証明するための証明書を発行する証明書発行サーバ２２が認証ネットワーク２０を介して接続された構成を有している。

【０１０３】

なお、本発明の第４の実施の形態に係る認証システムを構成する要素のうち、本発明の

第２の実施の形態に係る認証システムを構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１０４】

また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末６１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通信端末６１ａを利用し、ユーザｂが通信端末６１ｂを利用し、ユーザｃが通信端末６１ｃを利用し、ユーザｄが通信端末６１ｄを利用するものとする。

【０１０５】

証明書発行サーバ２２は、各ユーザと対応する証明書を予め発行し、各ユーザは、証明書発行サーバ２２によって発行された証明書を自己が利用する通信端末６１に予め格納するようにしてもよい。しかし、ユーザは、証明書を自己で管理するのが望ましい。なお、証明書は、Ｘ．５０９証明書などの電子証明書を含み、ユーザ識別子に代えて用いられる。

【０１０６】

例えば、通信端末６１を利用するユーザがＶＬＡＮにログインするとき、通信端末６１は、ユーザを認証するための認証情報を認証クライアント６３を介してゲートウエイ装置４００に送信するようになっている。

【０１０７】

認証クライアント６３は、社内ネットワーク１０を構成するＶＬＡＮ３１およびＶＬＡＮ３２のうち、ゲートウエイ装置４００から送信されたＶＬＡＮ番号と対応するＶＬＡＮと通信端末６１とを接続するようになっている。また、認証クライアント６３は、社内ネットワーク１０を構築するためのロケーション毎に設置されるものであり、例えば、ビルの各階に設置されるようにしてもよい。

【０１０８】

図１３は、本発明の第４の実施の形態に係る認証システムのシーケンスのイメージ図である。通信端末６１と認証クライアント６３との間は、ＥＡＰ－ＴＬＳ（PPP Extensible Authentication Protocol－Transport Layer Security）に準拠した認証が行われる。また、認証クライアント６３から認証サーバ２１までの間は、ＥＡＰ－ＴＬＳをサポートするＲａｄｉｕｓに準拠した認証が行われる。

【０１０９】

また、認証クライアント６３は、ＥＡＰ－ＴＬＳに準拠したパケットとＲａｄｉｕｓに準拠したパケットとの変換を相互に行うようになっている。なお、認証クライアント６３は、証明書を含む認証情報であって、この認証情報を含むEAP-Requestパケットを通信端末６１から受信し、受信したＥＡＰ－ＲｅｓｐｏｎｓｅパケットをＲａｄｉｕｓに準拠したAccess-Requestパケットに変換し、変換したAccess-Requestパケットをゲートウエイ装置４００に送信するようになっている。また、認証クライアント６３は、ＥＡＰ－Ｒｅｓｐｏｎｓｅパケットに含まれる証明書をAccess-Requestパケットに引き継いでゲートウエイ装置４００に送信するようになっている。

【０１１０】

ゲートウエイ装置４００は、認証クライアント６３から送信されたAccess-Requestパケットを認証サーバ２１に中継し、認証サーバ２１から送信された認証応答情報を含むAccess-Acceptパケットを認証クライアント６３に中継するようになっている。

【０１１１】

なお、Access-Acceptパケットを受信したとき、ゲートウエイ装置４００は、Access-Requestパケットに含まれていた証明書を有するユーザと対応するＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを認証クライアント６３に送信することにより、ＶＬＡＮと通信端末６１とを接続させるようになっている。

【０１１２】

図１４は、本発明の第４の実施の形態に係るゲートウエイ装置のブロック構成図である。図１４に示すように、ゲートウエイ装置４００は、データベース２１０、通信インタフ

ェース２２０、制御手段４３０、ログ情報格納手段１４０、および通信インタフェース１５０を含むように構成される。

【０１１３】

なお、本発明の第４の実施の形態に係るゲートウエイ装置を構成する要素のうち、本発明の第２の実施の形態に係るゲートウエイ装置を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１１４】

制御手段４３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段４３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段４３４、および認証失敗情報送信手段１３５を有している。なお、これらの手段はプログラムのモジュールでもよい。

【０１１５】

ユーザ認可手段４３４は、証明書を含む認証情報が認証クライアント６３を介して送信されたとき、認証情報に含まれる証明書をユーザ識別子に変換するなどして記憶するようになっている。その後、ユーザ認可手段４３４は、認証応答手段１３３によって受信された認証応答情報が認証の成功を示していたとき、記憶したユーザ識別子と対応するＶＬＡＮ番号をデータベース２１０から取得し、取得したＶＬＡＮ番号と対応するＶＬＡＮと通信端末６１とを認証クライアント６３に接続させるようになっている。

【０１１６】

例えば、ユーザ認可手段４３４は、取得したＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを認証クライアント６３に送信することにより、ＶＬＡＮと通信端末６１とを接続させるようになっている。

【０１１７】

また、ユーザ認可手段４３４は、記憶したユーザ識別子と対応する利用時間情報をデータベース２１０から取得し、取得した利用時間情報に従ってＶＬＡＮに接続可能か否かを判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段４３４が、ＶＬＡＮ番号と対応するＶＬＡＮと通信端末６１とを認証クライアント６３に接続させるようになっている。

【０１１８】

さらに、ユーザ認可手段４３４は、記憶したユーザ識別子と対応する利用可能装置情報をデータベース２１０から取得し、取得した利用可能装置情報に従って、ユーザがAccess-Requestパケットを送信した認証クライアント６３を利用可能か否かを判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段４３４が、ＶＬＡＮ番号に従ってＶＬＡＮと通信端末６１とを認証クライアント６３に接続させるようになっている。

【０１１９】

さらに、証明書には、複数のＶＬＡＮのうちユーザが利用可能なＶＬＡＮだけに接続することを許可するための許可情報が含まれ、ユーザ認可手段４３４は、証明書に含まれる許可情報に従って、データベース２１０から取得したＶＬＡＮ番号と対応するＶＬＡＮに接続可能か否かを許可情報に従って判断するようにしてもよい。接続可能と判断したときには、ユーザ認可手段４３４が、ＶＬＡＮ番号と対応するＶＬＡＮと通信端末６１とを認証クライアント６３に接続させるようになっている。

【０１２０】

例えば、ＶＬＡＮ３１だけを許可する許可情報が含まれる証明書が、ユーザｂから認証クライアント６３ａを介して送信されたとき、ユーザ認可手段４３４は、データベース２１０から取得したＶＬＡＮ番号がＶＬＡＮ３２を表しているため、接続を許可しないようになっている。

【０１２１】

以下、本発明の第４の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図１５は、本発明の第４の実施の形態に係るゲートウエイ装置の動作の流

れを示すフローチャートである。

【０１２２】

なお、本発明の第４の実施の形態に係るゲートウエイ装置の動作のうち、本発明の第２の実施の形態に係るゲートウエイ装置の動作と同一のものについては、同一の符号を付す。

【０１２３】

まず、通信端末６１から送信された認証情報は、認証情報送受信手段１２１によって受信される（Ｓ１０１）。次に、利用時間情報は、認証情報解析手段１３１が認証情報を解析した後に、ユーザ認可手段４３４によってデータベース２１０から取得され、取得された利用時間情報に従ってＶＬＡＮに接続可能か否かが、ユーザ認可手段４３４によって判断される（Ｓ１０２）。

【０１２４】

接続可能と判断されたとき、さらに、利用可能装置情報がデータベース２１０から取得され、取得された利用可能装置情報に従って、ユーザがAccess-Requestパケットを送信した認証クライアント１３を利用可能か否かが、ユーザ認可手段４３４によって判断される（Ｓ２０１）。

【０１２５】

認証クライアント６３が利用可能と判断されたとき、ユーザ認可手段４３４によって証明書と対応するユーザ識別子が記憶され、認証情報解析手段１３１が解析した認証情報に応じて認証サーバ２１に対する認証の要求が、認証要求手段１３２によって行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。

【０１２６】

認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、記憶されたユーザ識別子と対応するＶＬＡＮ番号が、ユーザ認可手段４３４によってデータベース２１０から取得され、通信端末６１は、取得されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ１０６）。

【０１２７】

以上説明したように、本発明の第４の実施の形態に係るゲートウエイ装置は、仮想ネットワーク識別情報が示すＶＬＡＮと証明書に示されるユーザが利用する通信端末６１とを接続させるため、ユーザを識別するための情報などを偽ってＶＬＡＮを不正に利用することを防止できる。

また、証明書に示されるユーザが仮想ネットワーク識別情報が示すＶＬＡＮに接続可能か否かを許可情報に従って判断し、接続可能と判断したときＶＬＡＮと、証明書に示されるユーザが利用する通信端末６１とを接続させるため、証明書に従ってユーザが利用できるＶＬＡＮを制限することができる。

【０１２８】

図１６は、本発明の第５の実施の形態に係る認証システムのシステム構成図である。図１６に示すように、認証システム５０００は、ユーザが利用する通信端末７１ａから通信端末７１ｄと、情報を中継するゲートウエイ装置５００と、通信端末７１の仲介を行う認証クライアント５３ａ、ｂ（仲介装置）が、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置５００と、ユーザを認証する認証サーバ２１とが認証ネットワーク２０を介して通信可能に接続された構成を有している。

【０１２９】

なお、本発明の第５の実施の形態に係る認証システムを構成する要素のうち、本発明の第３の実施の形態に係る認証システムを構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１３０】

また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末７１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通

信端末７１ａを利用し、ユーザｂが通信端末７１ｂを利用し、ユーザｃが通信端末７１ｃを利用し、ユーザｄが通信端末７１ｄを利用するものとする。

【０１３１】

例えば、通信端末７１を利用するユーザがＶＬＡＮにログインするとき、通信端末７１は、ユーザを認証するための認証情報を認証クライアント５３を介してゲートウエイ装置５００に送信するようになっている。なお、認証情報には、ＶＬＡＮ（Virtual Local Area Network）３１およびＶＬＡＮ３２うち何れか１つのＶＬＡＮを識別するためのＶＬＡＮ番号が含まれる。

【０１３２】

図１７は、本発明の第５の実施の形態に係る認証システムのシーケンスのイメージ図である。ユーザが利用する通信端末７１は、自分が利用可能なＶＬＡＮを問い合わせるための問い合わせ情報を含むＥＡＰ－Ｒｅｓｐｏｎｓｅパケットを認証クライアント５３を介してゲートウエイ装置５００に送信するようになっている。

【０１３３】

ゲートウエイ装置５００は、問い合わせ情報を受信したとき、ユーザと対応するＶＬＡＮ番号が含まれるAccess-Challengeパケットを、認証クライアント５３を介して通信端末７１に返答するようになっている。通信端末７１は、返答されたＶＬＡＮ番号を認証情報に追加し、追加された認証情報を含むＥＡＰ－Ｒｅｓｐｏｎｓｅパケットを認証クライアント５３を介してゲートウエイ装置５００に送信するようになっている。なお、返答されたＶＬＡＮ番号が複数存在する場合、通信端末７１は、複数のＶＬＡＮ番号のうち１つを選択し、選択したＶＬＡＮ番号を認証情報に追加するようになっている。

【０１３４】

ゲートウエイ装置５００は、認証クライアント５３から送信されたAccess-Requestパケットを認証サーバ２１に中継し、認証サーバ２１から送信された認証応答情報を含むAccess-Acceptパケットを認証クライアント５３に中継するようになっている。また、ゲートウエイ装置５００は、Access-Acceptパケットを受信したとき、Access-Requestパケットに含まれていたＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを、Access-Requestパケットを送信した認証クライアント５３に送信することにより、ＶＬＡＮと通信端末７１とを接続させるようになっている。

【０１３５】

図１８は、本発明の第５の実施の形態に係るゲートウエイ装置のブロック構成図である。図１８に示すように、ゲートウエイ装置５００は、データベース３１０、通信インタフェース２２０、制御手段５３０、ログ情報格納手段１４０、および通信インタフェース１５０を含むように構成される。

【０１３６】

なお、本発明の第５の実施の形態に係るゲートウエイ装置を構成する要素のうち、本発明の第３の実施の形態に係るゲートウエイ装置を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１３７】

制御手段５３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段３３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段３３４、認証失敗情報送信手段１３５、問い合わせ情報受信手段５３６、および仮想ネットワーク識別情報返答手段５３７を有している。なお、これらの手段はプログラムのモジュールでもよい。

【０１３８】

問い合わせ情報受信手段５３６は、ユーザの利用可能なＶＬＡＮを問い合わせるための問い合わせ情報を通信端末７１から受信するようになっている。例えば、問い合わせ情報受信手段５３６は、認証情報解析手段１３１がＲａｄｉｕｓなどに準拠したパケットを解析した後、パケットに含まれる問い合わせ情報を受信するようにしてもよい。

【０１３９】
仮想ネットワーク識別情報返答手段５３７は、問い合わせ情報受信手段５３６によって受信された問い合わせ情報に応じてデータベース３１０からユーザと対応するためのＶＬＡＮ番号を、ユーザが利用する通信端末７１に返答するようになっている。
【０１４０】
例えば、問い合わせ情報受信手段５３６がユーザｃから送信された問い合わせ情報を受信したとき、仮想ネットワーク識別情報返答手段５３７は、データベース３１０が格納する表３に示した情報からＶＬＡＮ３１、ＶＬＡＮ３２を示す許可情報を取得し、取得した情報を通信端末７１ｃに返答するようになっている。ＶＬＡＮ３１、ＶＬＡＮ３２を示す許可情報を受信した通信端末７１ｃは、複数のＶＬＡＮ番号のうち１つを選択し、選択したＶＬＡＮ番号を認証情報に追加して、認証情報をゲートウエイ装置５００に送信するようになっている。
【０１４１】
以下、本発明の第５の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図１９は、本発明の第５の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。
【０１４２】
なお、本発明の第５の実施の形態に係るゲートウエイ装置の動作のうち、本発明の第３の実施の形態に係るゲートウエイ装置の動作と同一のものについては、同一の符号を付す。
【０１４３】
まず、ユーザの利用可能なＶＬＡＮを問い合わせるための問い合わせ情報であって、通信端末７１から送信された問い合わせ情報は、問い合わせ情報受信手段５３６によって受信される（Ｓ５０１）。次に、ユーザと対応する許可情報が、仮想ネットワーク識別情報返答手段５３７によってデータベース３１０から取得され（Ｓ５０２）、ユーザが利用する通信端末７１に返答される（Ｓ５０３）。なお、Ｓ５０２の後に、Ｓ３０１およびＳ３０２の動作を実行してもよい。
【０１４４】
その後、通信端末７１から送信されたＶＬＡＮ番号を含む認証情報は、認証情報送受信手段１２１によって受信される（Ｓ１０１）。次に、ユーザ識別子と対応する利用時間情報は、ユーザ認可手段３３４によってデータベース３１０から取得され、取得された利用時間情報に従ってＶＬＡＮに接続可能か否かが、ユーザ認可手段３３４によって判断される（Ｓ３０１）。
【０１４５】
接続可能と判断されたとき、さらに、ユーザ識別子と対応する利用可能装置情報がデータベース３１０から取得され、取得された利用可能装置情報に従って、ユーザが認証情報を送信した認証クライアント５３を利用可能か否かが、ユーザ認可手段３３４によって判断され、認証クライアント５３を利用可能と判断されたとき、認証情報に含まれるＶＬＡＮ番号が、ユーザ認可手段３３４によって記憶され、認証情報に含まれるＶＬＡＮ番号が取り除かれる（Ｓ３０２）。
【０１４６】
認証クライアント５３を利用可能と判断されたとき、認証サーバ２１に対する認証の要求が、認証要求手段１３２によって認証情報解析手段１３１が解析した認証情報に応じて行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。
【０１４７】
認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、通信端末７１は、ユーザ認可手段３３４によって記憶されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ３０３）。
【０１４８】

以上説明したように、本発明の第５の実施の形態に係るゲートウエイ装置は、ユーザからの問い合わせに応じてＶＬＡＮ番号を返答するため、予めユーザがＶＬＡＮ番号を知らなくても、接続可能なＶＬＡＮ番号をユーザに通知でき、接続可能なＶＬＡＮ番号が複数あるときには、ユーザが望むＶＬＡＮと接続することができる。

【０１４９】

図２０は、本発明の第６の実施の形態に係る認証システムのシステム構成図である。図２０に示すように、認証システム６０００は、ユーザが利用する通信端末８１ａから通信端末８１ｄと、情報を中継するゲートウエイ装置６００と、通信端末８１の仲介を行う認証クライアント７３ａ、ｂ（仲介装置）が、社内ネットワーク１０を介して通信可能に接続され、かつゲートウエイ装置６００と、ユーザを認証する認証サーバ２１とが認証ネットワーク２０を介して通信可能に接続された構成を有している。

【０１５０】

なお、本発明の第６の実施の形態に係る認証システムを構成する要素のうち、本発明の第３の実施の形態に係る認証システムを構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１５１】

また、ユーザａ、ユーザｂ、ユーザｃ、またはユーザｄは、如何なる通信端末８１を利用してもよい。しかし、本実施の形態においては、説明の便宜を図るため、ユーザａが通信端末８１ａを利用し、ユーザｂが通信端末８１ｂを利用し、ユーザｃが通信端末８１ｃを利用し、ユーザｄが通信端末８１ｄを利用するものとする。

【０１５２】

例えば、通信端末８１を利用するユーザがＶＬＡＮにログインするとき、通信端末８１は、ユーザを認証するための認証情報を認証クライアント７３を介してゲートウエイ装置６００に送信するようになっている。なお、認証情報には、ＶＬＡＮ（Virtual Local Area Network）３１、ＶＬＡＮ３２、およびＶＬＡＮ３３うち何れか１つのＶＬＡＮを識別するためのＶＬＡＮ番号が含まれる。

【０１５３】

図２１は、本発明の第６の実施の形態に係る認証システムのシーケンスのイメージ図である。認証クライアント７３には、社内ネットワーク１０によって構成される全てのＶＬＡＮを表す情報が予め登録され、認証クライアント７３は、全てのＶＬＡＮを表す情報を含むＥＡＰ－Ｒｅｑｕｅｓｔパケットを、ユーザの利用する通信端末８１に通知するようになっている。

【０１５４】

ユーザの利用する通信端末８１は、通知された情報に基づいてＶＬＡＮの優先度を与えた仮想ネットワークリストを作成し、作成した仮想ネットワークリストを認証情報に追加し、追加した認証情報を含むＥＡＰ－Ｒｅｓｐｏｎｓｅパケットを認証クライアント７３を介してゲートウエイ装置６００に送信するようになっている。例えば、仮想ネットワークリストは、ユーザが利用したい順番にＶＬＡＮ番号が記述されている。

【０１５５】

ゲートウエイ装置６００は、認証情報を含むAccess-Requestパケットを受信したとき、仮想ネットワークリストに基づいて優先度の高いＶＬＡＮから順にユーザが接続可能か否かを許可情報に従って判断し、接続可能と判断したとき認証クライアント７３から送信されたAccess-Requestパケットを認証サーバ２１に中継し、認証サーバ２１から送信された認証応答情報を含むAccess-Acceptパケットを認証クライアント７３に中継するようになっている。

【０１５６】

また、ゲートウエイ装置６００は、Access-Acceptパケットを受信したとき、Access-Requestパケットに含まれていたＶＬＡＮ番号をAccess-Acceptパケットに含め、このAccess-Acceptパケットを、Access-Requestパケットを送信した認証クライアント７３に送信することにより、接続可能と判断したＶＬＡＮと通信端末８１とを接続させるようになって

いる。

【０１５７】

図２２は、本発明の第６の実施の形態に係るゲートウエイ装置のブロック構成図である。図２２に示すように、ゲートウエイ装置６００は、データベース３１０、通信インタフェース２２０、制御手段６３０、ログ情報格納手段１４０、および通信インタフェース１５０を含むように構成される。

【０１５８】

なお、本発明の第６の実施の形態に係るゲートウエイ装置を構成する要素のうち、本発明の第３の実施の形態に係るゲートウエイ装置を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

【０１５９】

制御手段６３０は、プログラムを処理するＣＰＵ（Central Processing Unit）、およびプログラムを記憶するメモリなどを含むように構成される。また、制御手段６３０は、認証情報解析手段１３１、認証要求手段１３２、認証応答手段１３３、ユーザ認可手段６３４、および認証失敗情報送信手段１３５を有している。なお、これらの手段はプログラムのモジュールでもよい。

【０１６０】

ユーザ認可手段６３４は、ＶＬＡＮ番号を含む認証情報が認証クライアント７３を介して送信されたとき、認証情報に含まれる仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順にユーザが接続可能か否かを許可情報に従って判断するようになっている。

【０１６１】

例えば、ユーザ認可手段６３４は、仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順にＶＬＡＮ番号を抽出するようになっている。さらに、ユーザ認可手段６３４は、データベース３１０が格納する表３に示した情報からＶＬＡＮ３１、ＶＬＡＮ３２を示す許可情報を取得し、取得した許可情報に従って、抽出したＶＬＡＮ番号が接続可能か否かを判断するようになっている。接続不能であった場合、仮想ネットワークリストに基づいて次の優先度の高い仮想ネットワークから順にＶＬＡＮ番号を抽出し、抽出したＶＬＡＮ番号が接続可能か否かを判断することを繰り返すようになっている。

【０１６２】

より詳細には、仮想ネットワークリストがユーザが利用したい順番にＶＬＡＮ番号が記述され、ユーザｃから送信された「ＶＬＡＮ３３」、「ＶＬＡＮ３２」、「ＶＬＡＮ３１」の順に記述された仮想ネットワークリストであった場合、ユーザ認可手段６３４は、接続が許可されていないＶＬＡＮ３３の次に優先度の高いＶＬＡＮ３２を抽出し、抽出したＶＬＡＮ番号を記憶し、仮想ネットワークリストを認証情報から取り除き、仮想ネットワークリストが取り除かれた認証情報を認証情報送受信手段１５１に出力するようになっている。

【０１６３】

その後、ユーザ認可手段６３４は、認証応答手段１３３によって受信された認証応答情報が認証の成功を示していたとき、記憶したＶＬＡＮ番号と対応するＶＬＡＮと通信端末８１とを認証クライアント７３に接続させるようになっている。

【０１６４】

以下、本発明の第６の実施の形態に係るゲートウエイ装置の動作について、図面を参照して説明する。図２３は、本発明の第６の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。

【０１６５】

なお、本発明の第６の実施の形態に係るゲートウエイ装置の動作のうち、本発明の第３の実施の形態に係るゲートウエイ装置の動作と同一のものについては、同一の符号を付す。

【０１６６】

まず、通信端末８１から送信された仮想ネットワークリストを含む認証情報は、認証情報送受信手段１２１によって受信される（Ｓ６０１）。次に、ユーザ識別子と対応する利用時間情報は、ユーザ認可手段６３４によってデータベース３１０から取得され、取得された利用時間情報に従ってＶＬＡＮに接続可能か否かが、ユーザ認可手段６３４によって判断される（Ｓ３０１）。

【０１６７】

接続可能と判断されたとき、さらに、ユーザ識別子と対応する利用可能装置情報がデータベース３１０から取得され、取得された利用可能装置情報に従って、ユーザが認証情報を送信した認証クライアント７３を利用可能か否かが、ユーザ認可手段６３４によって判断される（Ｓ３０２）。

【０１６８】

認証クライアント７３を利用可能と判断されたとき、認証情報に含まれる仮想ネットワークリストに基づいて優先度の高い仮想ネットワークから順にＶＬＡＮ番号が、ユーザ認可手段６３４によって抽出され（Ｓ６０２）、抽出されたＶＬＡＮ番号が接続可能か否かが、ユーザ認可手段６３４によって判断され、抽出されたＶＬＡＮ番号が接続可能と判断された場合、ユーザ認可手段６３４によって記憶され、認証情報に含まれる仮想ネットワークリストが取り除かれる（Ｓ６０３）。なお、仮想ネットワークリストに記述されているＶＬＡＮ番号が全て接続不能であった場合、動作は終了する。

【０１６９】

ＶＬＡＮ番号が接続可能と判断された場合、認証サーバ２１に対する認証の要求が、認証要求手段１３２によって認証情報解析手段１３１が解析した認証情報に応じて行われる（Ｓ１０３）。その後、認証応答情報は、認証応答手段１３３によって認証サーバ２１から受信される（Ｓ１０４）。

【０１７０】

認証が成功したか否かが、認証応答手段１３３によって受信された認証応答情報に基づいて判断される（Ｓ１０５）。認証が成功したとき、通信端末８１は、ユーザ認可手段６３４によって記憶されたＶＬＡＮ番号と対応するＶＬＡＮに接続される（Ｓ３０３）。

【０１７１】

以上説明したように、本発明の第６の実施の形態に係るゲートウエイ装置は、ＶＬＡＮの優先度が与えられた仮想ネットワークリストに基づいて優先度の高いＶＬＡＮから順にユーザが接続可能か否かを許可情報に従って判断するため、ユーザが望む優先度の高い順にＶＬＡＮと接続することができる。また、ユーザは、予めユーザがＶＬＡＮ番号を知らなくても、接続可能なＶＬＡＮに接続できる。

【図面の簡単な説明】

【０１７２】

【図１】本発明の第１の実施の形態に係る認証システムのシステム構成図である。

【図２】本発明の第１の実施の形態に係るゲートウエイ装置のブロック構成図である。

【図３】本発明の第１の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。

【図４】本発明の第２の実施の形態に係る認証システムのシステム構成図である。

【図５】本発明の第２の実施の形態に係る認証システムのシーケンスのイメージ図である。

【図６】本発明の第２の実施の形態に係るゲートウエイ装置のブロック構成図である。

【図７】本発明の第２の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。

【図８】本発明の第３の実施の形態に係る認証システムのシステム構成図である。

【図９】本発明の第３の実施の形態に係る認証システムのシーケンスのイメージ図である。

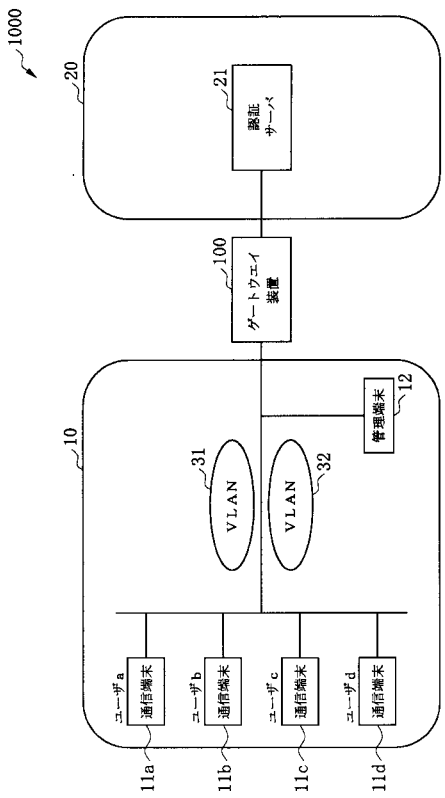
【図１０】本発明の第３の実施の形態に係るゲートウエイ装置のブロック構成図である。

【図１１】本発明の第３の実施の形態に係るゲートウエイ装置の動作の流れを示すフロー

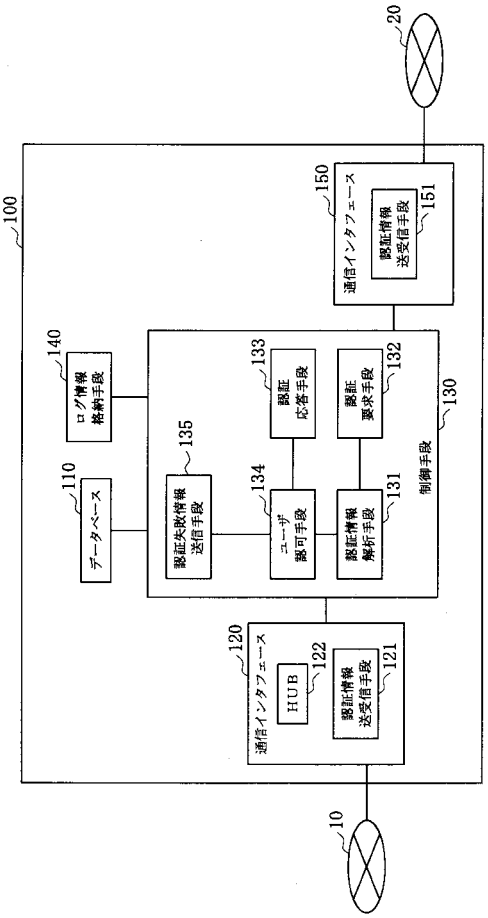
チャートである。
【図１２】本発明の第４の実施の形態に係る認証システムのシステム構成図である。
【図１３】本発明の第４の実施の形態に係る認証システムのシーケンスのイメージ図である。
【図１４】本発明の第４の実施の形態に係るゲートウエイ装置のブロック構成図である。
【図１５】本発明の第４の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。
【図１６】本発明の第５の実施の形態に係る認証システムのシステム構成図である。
【図１７】本発明の第５の実施の形態に係る認証システムのシーケンスのイメージ図である。
【図１８】本発明の第５の実施の形態に係るゲートウエイ装置のブロック構成図である。
【図１９】本発明の第５の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。
【図２０】本発明の第６の実施の形態に係る認証システムのシステム構成図である。
【図２１】本発明の第６の実施の形態に係る認証システムのシーケンスのイメージ図である。
【図２２】本発明の第６の実施の形態に係るゲートウエイ装置のブロック構成図である。
【図２３】本発明の第６の実施の形態に係るゲートウエイ装置の動作の流れを示すフローチャートである。
【図２４】従来の認証システムを示すブロック図である。
【符号の説明】
【０１７３】
１０：社内ネットワーク
１１（１１ａ～１１ｄ），４１（４１ａ～４１ｄ），５１（５１ａ～５１ｄ），６１（６１ａ～６１ｄ），７１（７１ａ～７１ｄ），８１（８１ａ～８１ｄ），９２１（９２１ａ，９２１ｂ）：通信端末
１２：管理端末
１３，５３，６３，７３：認証クライアント
２０：認証ネットワーク
２１：認証サーバ
２２：証明書発行サーバ
３１，３２，３３：ＶＬＡＮ
１００，２００，３００，４００，９２０：ゲートウエイ装置
１１０，２１０，３１０：データベース
１２０，１５０，２２０：通信インタフェース
１２１，１５１：認証情報送受信手段
１２２：仮想ネットワーク接続手段（ＨＵＢ）
１３０，２３０，３３０，４３０，５３０，６３０：制御手段
１３１：認証情報解析手段
１３２：認証要求手段
１３３：認証応答手段
１３４，２３４，３３４，４３４，６３４：ユーザ認可手段
１３５：認証失敗情報送信手段
１４０：ログ情報格納手段
５３６：問い合わせ情報受信手段
５３７：仮想ネットワーク識別情報返答手段
９１０ａ，９１０ｂ：サーバ
９１２：認証代行サーバ
９１３，９２３：ネットワーク
１０００，２０００，３０００，４０００，５０００，６０００：認証システム

ａ～ｄ：ユーザ

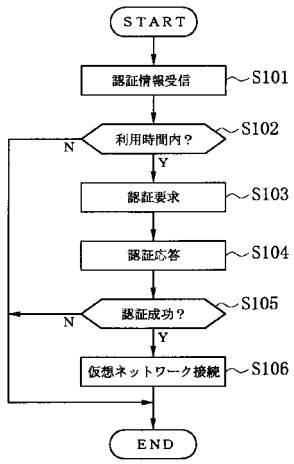
【図１】


1000
20
21
認証サーバ
100
ゲートウェイ装置
10
31
VLAN
32
VLAN
管理端末
12
ユーザａ
通信端末
ユーザｂ
通信端末
ユーザｃ
通信端末
ユーザｄ
通信端末
11a
11b
11c
11d

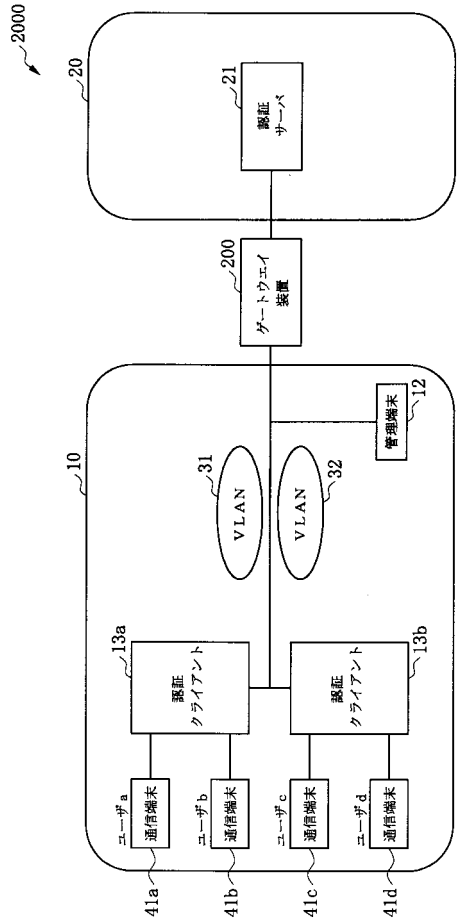
【図２】


20
100
150
通信インタフェース
認証情報送受信手段
151
140
ログ情報格納手段
133
認証応答手段
132
認証要求手段
130
制御手段
135
認証失敗情報送信手段
134
ユーザ認可手段
131
認証情報解析手段
110
データベース
120
通信インタフェース
HUB
122
認証情報送受信手段
121
10

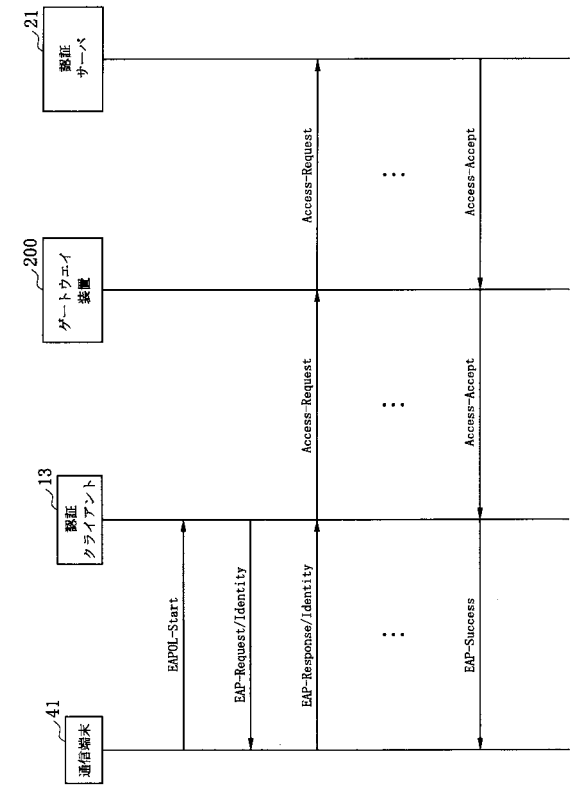
【図３】


START
認証情報受信
S101
利用時間内？
S102
N
Y
認証要求
S103
認証応答
S104
認証成功？
S105
N
Y
仮想ネットワーク接続
S106
END

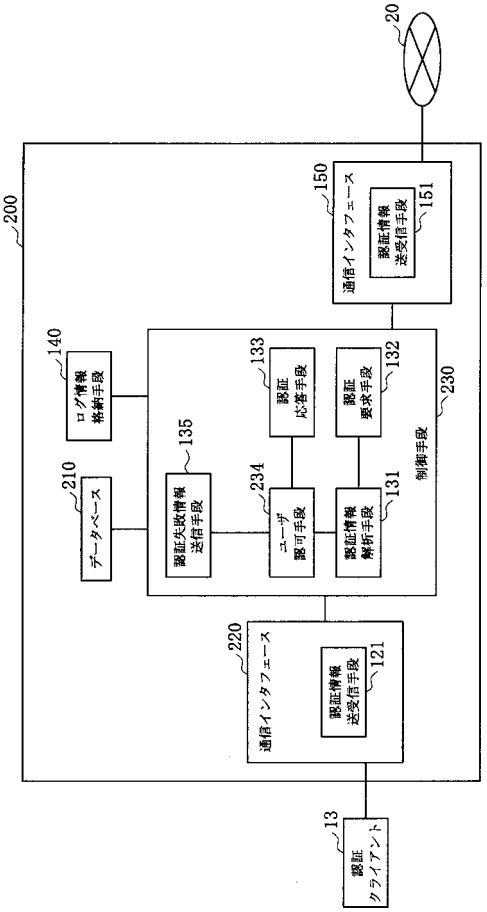
【図４】


2000
20
21
認証サーバ
200
ゲートウェイ装置
10
12
管理端末
31
VLAN
32
VLAN
13a
認証クライアント
13b
認証クライアント
ユーザ a
通信端末
ユーザ b
通信端末
ユーザ c
通信端末
ユーザ d
通信端末
41a
41b
41c
41d

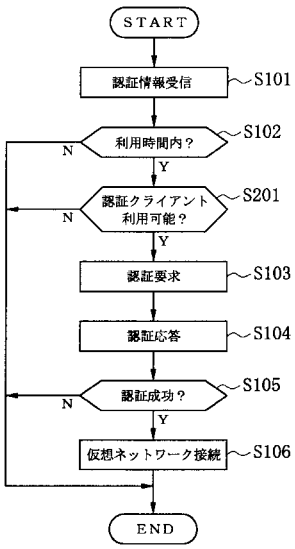
【図５】


21
認証サーバ
200
ゲートウェイ装置
13
認証クライアント
41
通信端末
Access-Request
Access-Accept
Access-Request
Access-Accept
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Success

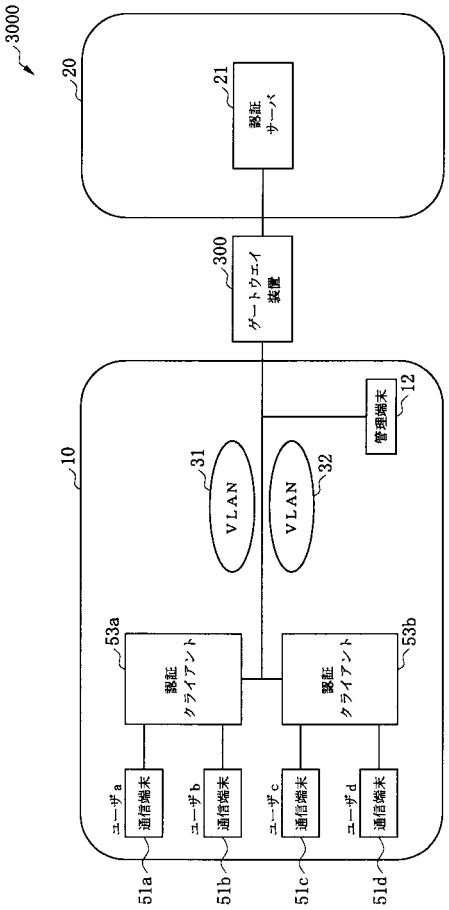
【図６】


20
200
150
通信インタフェース
151
認証情報送受信手段
140
ログ情報格納手段
133
認証応答手段
132
認証要求手段
230
制御手段
135
認証失敗情報送信手段
234
ユーザ認可手段
131
認証情報解析手段
210
データベース
220
通信インタフェース
121
認証情報送受信手段
13
認証クライアント

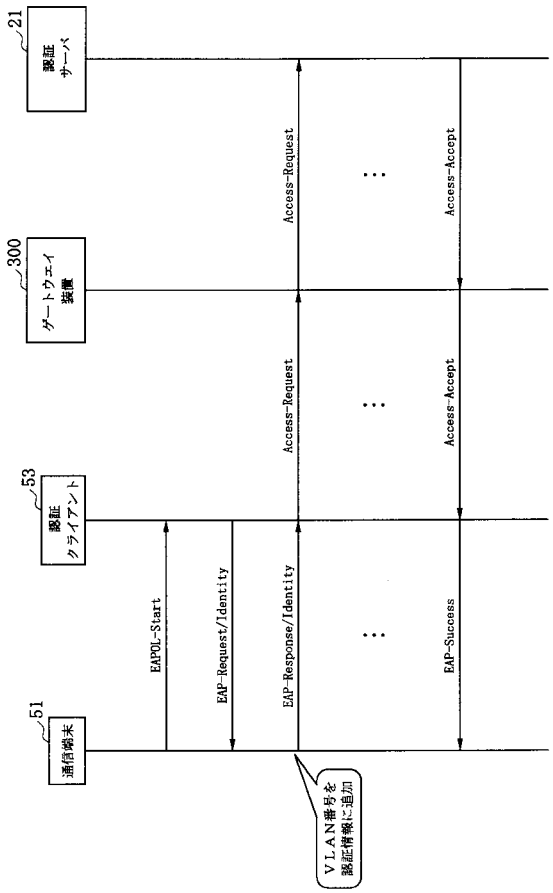
【図７】


START
認証情報受信
S101
利用時間内？
S102
N
Y
認証クライアント利用可能？
S201
N
Y
認証要求
S103
認証応答
S104
認証成功？
S105
N
Y
仮想ネットワーク接続
S106
END

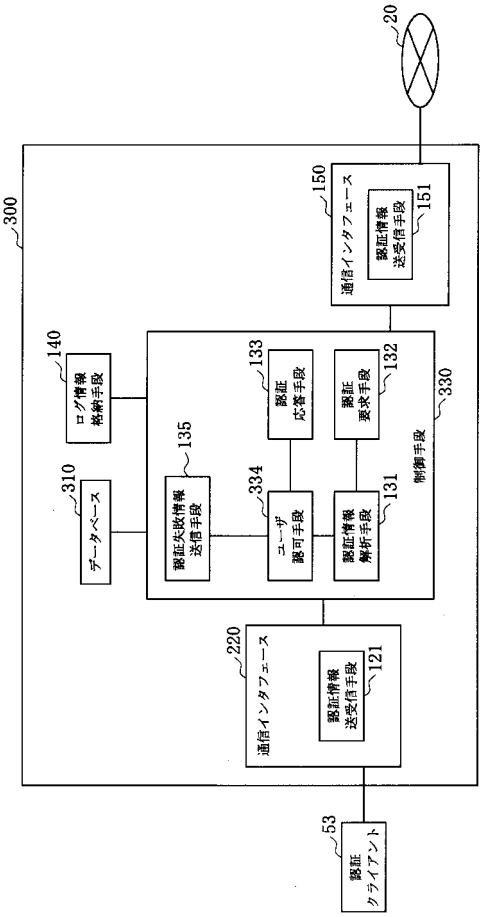
【図８】


3000
20
21
認証サーバ
300
ゲートウェイ装置
10
管理端末
12
31
VLAN
32
VLAN
53a
認証クライアント
53b
認証クライアント
ユーザa
通信端末
ユーザb
通信端末
ユーザc
通信端末
ユーザd
通信端末
51a
51b
51c
51d

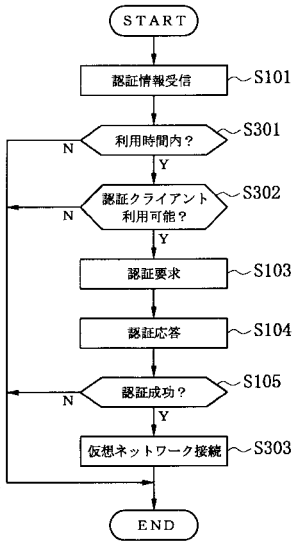
【図９】


21
認証サーバ
300
ゲートウェイ装置
53
認証クライアント
51
通信端末
Access-Request
Access-Request
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Access-Accept
Access-Accept
EAP-Success
VLAN番号を認証情報に追加

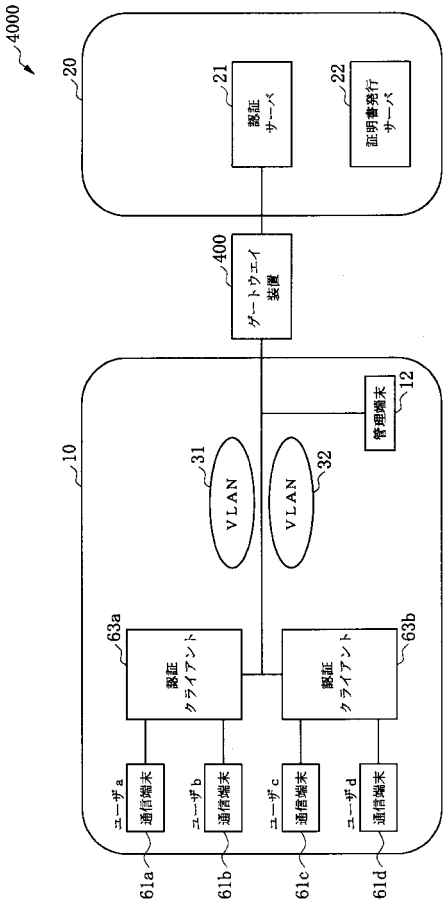
【図１０】


20
300
150
通信インタフェース
認証情報送受信手段
151
140
ログ情報格納手段
133
認証応答手段
132
認証要求手段
330
制御手段
135
認証失敗情報送信手段
334
ユーザ認可手段
131
認証情報解析手段
310
データベース
220
通信インタフェース
認証情報送受信手段
121
53
認証クライアント

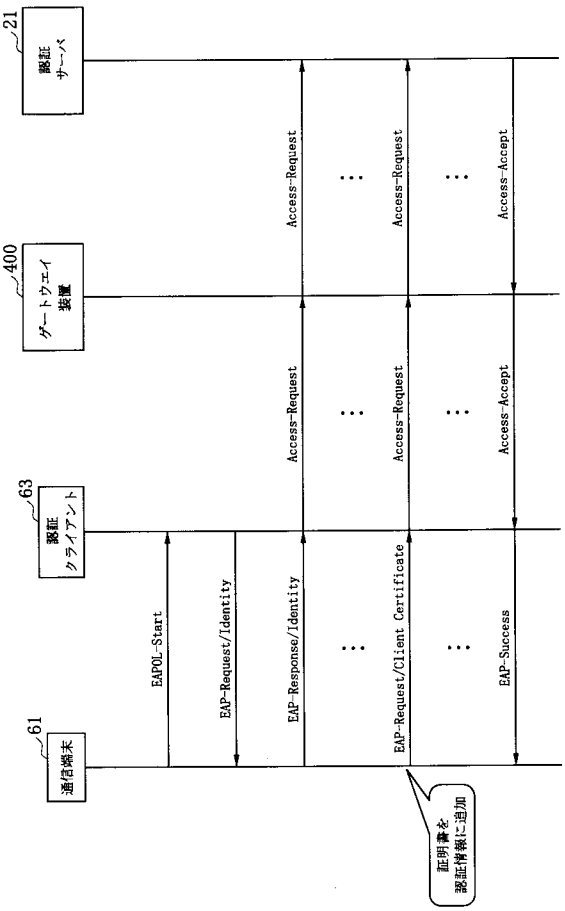
【図１１】



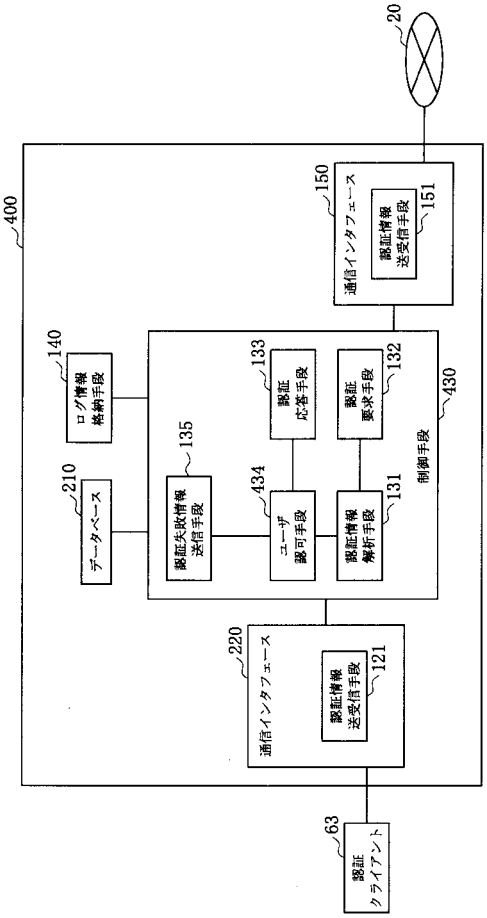
【図１２】



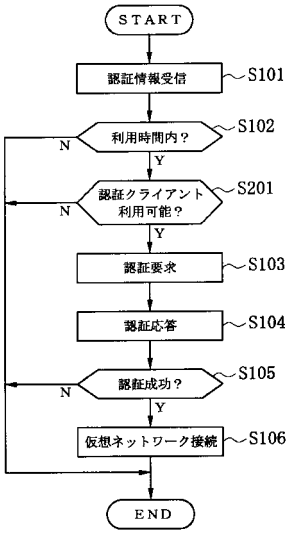
【図１３】



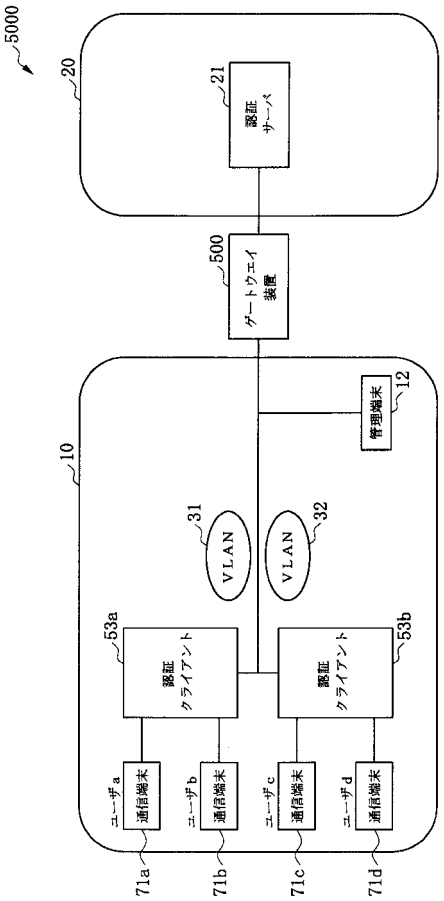
【図１４】



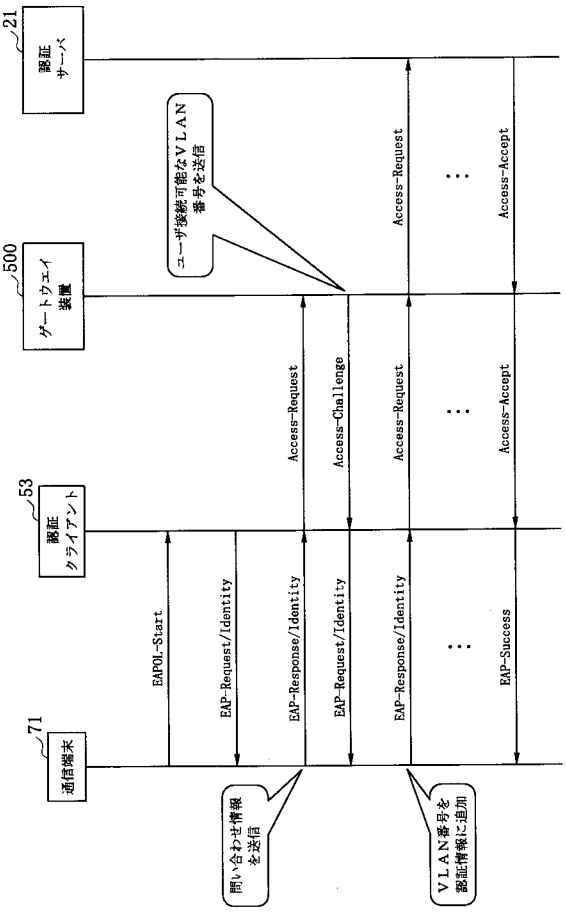
【図１５】



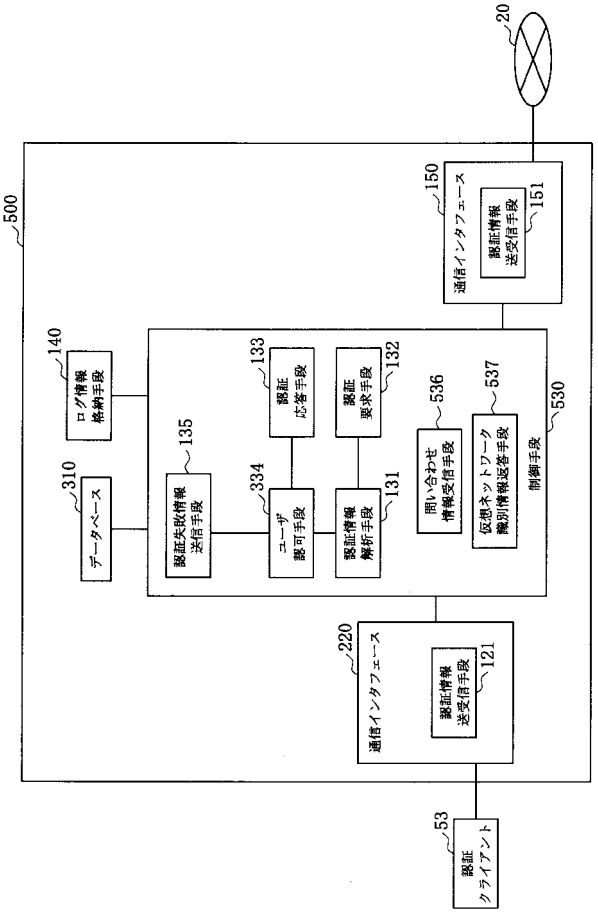
【図１６】



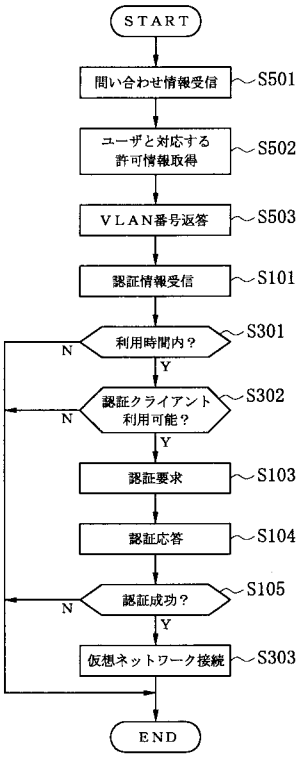
【図１７】



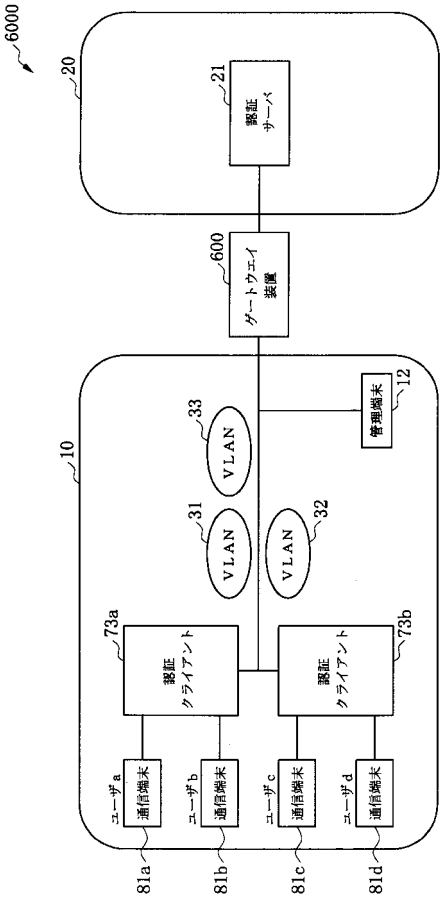
【図１８】



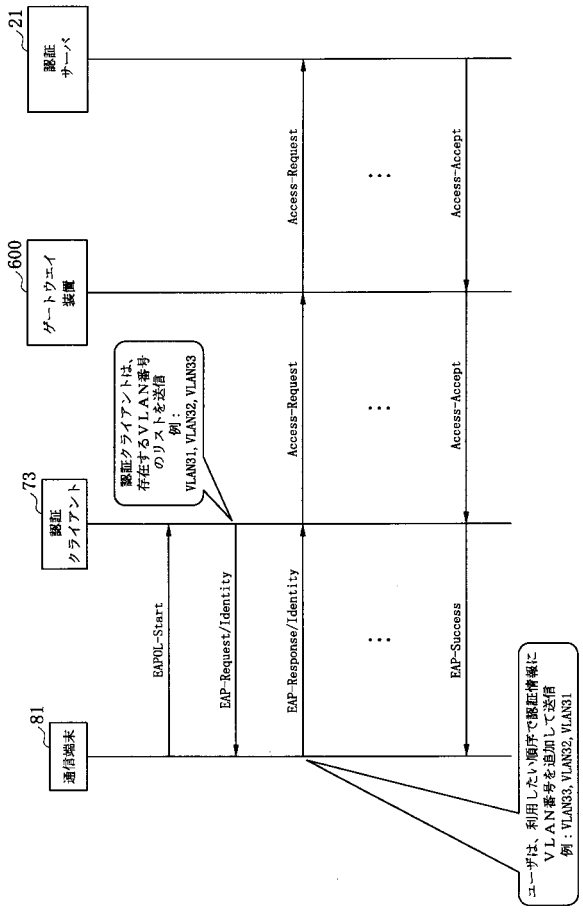
【図１９】



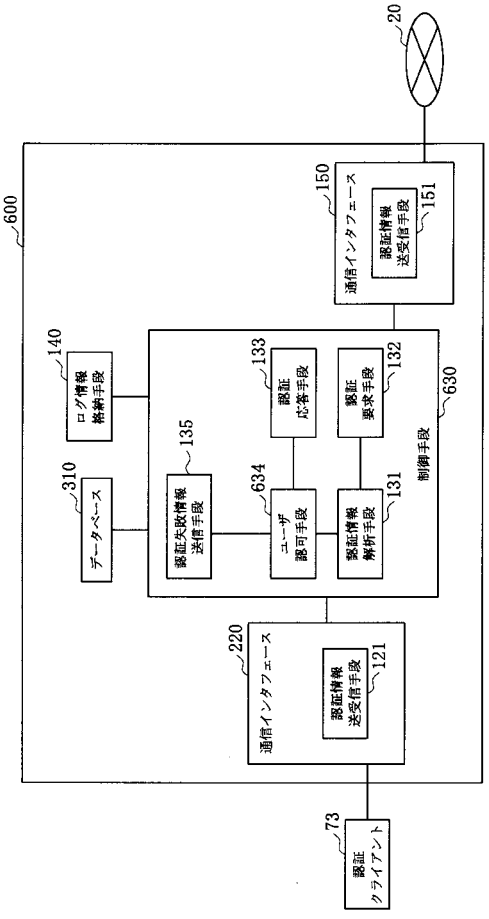
【図２０】



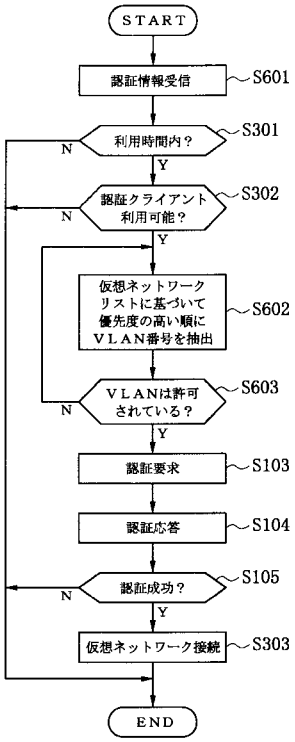
【図２１】



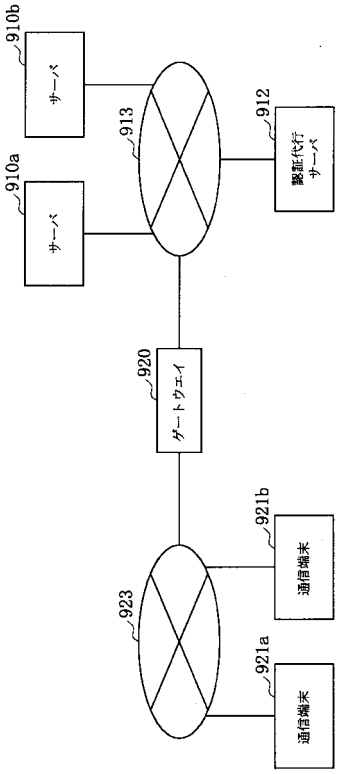
【図２２】



【図２３】


START
認証情報受信
S601
利用時間内？
S301
N
Y
認証クライアント
利用可能？
S302
N
Y
仮想ネットワーク
リストに基づいて
優先度の高い順に
ＶＬＡＮ番号を抽出
S602
ＶＬＡＮは許可
されている？
S603
N
Y
認証要求
S103
認証応答
S104
認証成功？
S105
N
Y
仮想ネットワーク接続
S303
END

【図２４】


910b
サーバ
910a
サーバ
913
912
認証代行
サーバ
920
ゲートウェイ
923
921b
通信端末
921a
通信端末

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	Ｈ０４Ｌ 9/00 ６７５Ｚ	

Ｆターム(参考) 5J104 AA07 BA02 KA01 KA02 KA04 KA15 MA01 NA05 NA38 PA07
5K030 GA15 HA08 HC13 HD03 HD06 KA04 LB05