(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5921460号
(P5921460)
(45)発行日　平成28年5月24日(2016.5.24)　(24)登録日　平成28年4月22日(2016.4.22)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B

請求項の数 6　(全 27 頁)

(21)出願番号　特願2013-30649(P2013-30649)
(22)出願日　平成25年2月20日(2013.2.20)
(65)公開番号　特開2014-160942(P2014-160942A)
(43)公開日　平成26年9月4日(2014.9.4)
審査請求日　平成27年3月3日(2015.3.3)

(73)特許権者　504411166
アラクサラネットワークス株式会社
神奈川県川崎市幸区鹿島田一丁目１番２号
(74)代理人　110001678
特許業務法人藤央特許事務所
(72)発明者　樋口　秀光
神奈川県川崎市幸区鹿島田一丁目１番２号
アラクサラネットワークス株式会社内
(72)発明者　角南　浩隆
神奈川県川崎市幸区鹿島田一丁目１番２号
アラクサラネットワークス株式会社内
(72)発明者　能見　元英
神奈川県川崎市幸区鹿島田一丁目１番２号
アラクサラネットワークス株式会社内

最終頁に続く

(54)【発明の名称】認証方法、転送装置及び認証サーバ

(57)【特許請求の範囲】
【請求項１】
ユーザが使用する端末を認証する認証サーバと、前記端末と前記認証サーバとの間の認証シーケンスを仲介するスイッチとを有する認証システムがネットワーク認証機能を提供するための認証方法であって、
前記スイッチは、前記端末からのアクセスの応答として送信されるリダイレクト通知に含めて、前記スイッチの識別情報を前記端末に送信し、
前記端末は、前記スイッチの識別情報を含めて、前記認証サーバへのリクエストを送信し、
前記認証サーバは、前記端末から送信された認証要求を認証し、
前記認証サーバは、前記提供されたスイッチの識別情報に基づいて、前記認証の結果を前記スイッチに送信し、
前記スイッチは、前記認証サーバから受信した認証結果に基づいて、前記端末からのアクセスを認証することを特徴とする認証方法。
【請求項２】
ユーザが使用する端末を認証する認証サーバと、前記端末と前記認証サーバとの間の認証シーケンスを仲介するスイッチとを有する認証システムがネットワーク認証機能を提供するための認証方法であって、
前記スイッチは、前記認証シーケンスにおいて、前記スイッチを識別するための識別情報を前記認証サーバに提供し、

前記認証サーバは、前記端末から送信された認証要求を認証し、
前記認証サーバは、前記提供されたスイッチの識別情報に基づいて、前記認証の結果を前記スイッチに送信し、
前記スイッチは、前記認証サーバから受信した認証結果に基づいて、前記端末からのアクセスを認証することを特徴とする認証方法。
前記認証サーバは、前記スイッチへの前記認証結果の通知と別に、前記端末への前記認証結果の通知を送信することを特徴とする認証方法。
【請求項３】
請求項１又は２に記載の認証方法であって、
前記認証サーバは、ＲＡＤＩＵＳ認証及びシボレス認証のいずれか一つの認証シーケンスを用いて、前記端末を認証することを特徴とする認証方法。
【請求項４】
ネットワーク認証機能を提供する転送装置であって、
ネットワークに接続される通信インタフェースと、
前記通信インタフェースに接続されるデータ転送制御部と、
前記データ転送制御部に接続されるプロセッサと、を備え、
前記転送装置は、ユーザが使用する端末と前記端末を認証する認証サーバとの間の認証シーケンスを、前記ネットワークを介して仲介し、
前記プロセッサは、
前記端末からのアクセスの応答として送信されるリダイレクト通知に含めて、前記転送装置の識別情報を、前記通信インタフェースを介して前記端末に送信し、
前記転送装置の識別情報を含む前記認証サーバへのリクエストを、前記端末から前記通信インタフェースを介して受信し、
前記提供された転送装置の識別情報に基づいて前記認証サーバが送信した、前記端末を認証した結果を、前記通信インタフェースを介して受信し、
前記認証サーバから前記通信インタフェースを介して受信した認証結果に基づいて、前記端末からのアクセスを認証することを特徴とする転送装置。
【請求項５】
ユーザが使用する端末を認証する認証サーバであって、
プログラムを実行するプロセッサと、前記プログラムを格納するメモリと、ネットワークと接続するインタフェースとを備え、
前記端末と前記認証サーバとの間の認証シーケンスを仲介するスイッチと接続されており、
前記認証シーケンスにおいて、前記スイッチを識別するための識別情報を受信し、
前記端末から送信された認証要求を認証し、
前記受信したスイッチの識別情報に基づいて、前記認証の結果を前記スイッチに送信し、
前記スイッチに送信した認証結果は、前記スイッチが前記端末からのアクセスを認証するために用いられ、
前記認証サーバが前記端末から受信するスイッチの識別情報は、前記スイッチが前記端末からのアクセスの応答として送信されるリダイレクト通知に含めて前記端末に送信されることを特徴とする認証サーバ。
【請求項６】
ユーザが使用する端末を認証する認証サーバであって、
プログラムを実行するプロセッサと、前記プログラムを格納するメモリと、ネットワークと接続するインタフェースとを備え、
前記端末と前記認証サーバとの間の認証シーケンスを仲介するスイッチと接続されており、
前記認証シーケンスにおいて、前記スイッチを識別するための識別情報を受信し、
前記端末から送信された認証要求を認証し、

前記受信したスイッチの識別情報に基づいて、前記認証の結果を前記スイッチに送信し、

前記スイッチに送信した認証結果は、前記スイッチが前記端末からのアクセスを認証するために用いられ、

前記スイッチへの前記認証結果の通知と別に、前記端末への前記認証結果の通知を送信することを特徴とする認証サーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク認証システムに関する。

【背景技術】

【０００２】

通信ネットワークがインフラとして重要になるのに伴って、セキュリティを強化する様々な機能が提案されている。その一つがネットワーク認証である。ネットワーク認証システムは、主に端末接続される認証スイッチ及び端末を認証する認証サーバで構成される。従来のネットワーク認証システムでは、端末が認証スイッチに認証リクエストパケットを送信する。認証スイッチは、受信した認証リクエストパケットに含まれる認証情報を用いて、受信した認証情報が登録されているかを認証サーバに問い合わせる。認証スイッチは、認証サーバから当該認証情報が登録済みのものであることが通知されると、当該認証リクエストパケットのソースＭＡＣアドレスを通信可能にする。

【０００３】

本技術分野の背景技術として、特開２００６－３３２０６号公報（特許文献１）、特開２０１０－６２６６７号公報（特許文献２）がある。

【０００４】

特許文献１は、ＤＨＣＰサーバは端末装置からのリクエストに対してＩＰアドレスの払い出しを行う。認証サーバは端末装置から送信される認証フレームを受信し、端末装置の認証を行い、その認証が完了すると、認証用ハブの登録情報データベースに対して端末装置の通信許可を通知する。認証用ハブは端末装置が送信したフレームをフレーム受信回路部において受信し、その送信元情報を基に登録情報データベースを参照することによって、フレームの送信、書換え送信、破棄を決定し、送信または書換え送信が許可された送信フレームについては送信バッファに送る認証システムを開示する。

【０００５】

また、特許文献２は、ユーザ端末の認証を行う認証機能を備えたスイッチングハブにおいて、ユーザ端末からの認証要求のパケットを認証サーバへ転送し、認証サーバからの認証応答のパケットをユーザ端末へ転送するとともに、認証応答のパケットを参照し、認証成功の情報を読み取ったとき、上記ユーザ端末を認証済みとする認証手段を有するネットワークシステムを開示する。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２００６－３３２０６号公報

【特許文献２】特開２０１０－６２６６７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

従来の認証スイッチにおけるＷｅｂ認証方式では、認証スイッチでＷｅｂサーバを動作させ、認証スイッチがユーザから入力された認証情報を認証サーバに中継すると、認証スイッチの処理負荷が高くなる。このため、スイッチが制御可能な認証済み端末の数の上限が小さくなる。

【０００８】

また、従来の認証スイッチでは、複数のネットワーク認証方式をサポートする必要があり、新しい認証方式の認証サーバに対応するためには、認証方式毎のモジュールを追加する必要がある。

【０００９】

また、端末と認証サーバとが、直接、認証シーケンスを行う場合、認証サーバは、認証端末が接続されているスイッチの情報を持たない。このため、複数の認証スイッチがある場合、認証端末が接続している認証スイッチを認証サーバが知ることが困難である。

【００１０】

前述した従来技術のように、端末と認証サーバとが、直接、認証シーケンスを行う場合、認証スイッチが認証結果を使ってＩＰアドレスやＭＡＣアドレスのフィルタや端末のＱｏＳを設定すればよいので、認証スイッチの負荷は軽減する。しかし、この方法では、認証済み端末のネットワークからの離脱を管理できない。このため、不要な認証情報やフィルタ情報やＱｏＳ設定が認証スイッチ内に残り、認証スイッチの記憶容量を無駄に消費する。また、認証済みＭＡＣアドレスを詐称した端末が接続する可能性があり、セキュリティが低下する。

【課題を解決するための手段】

【００１１】

上述した課題の少なくとも一つを解決するため、本願において開示される発明の代表的な一例を示せば以下の通りである。すなわち、ユーザが使用する端末を認証する認証サーバと、前記端末と前記認証サーバとの間の認証シーケンスを仲介するスイッチとを有する認証システムがネットワーク認証機能を提供するための認証方法であって、前記スイッチは、前記端末からのアクセスの応答として送信されるリダイレクト通知に含めて、前記スイッチの識別情報を前記端末に送信し、前記端末は、前記スイッチの識別情報を含めて、前記認証サーバへのリクエストを送信し、前記認証サーバは、前記端末から送信された認証要求を認証し、前記認証サーバは、前記提供されたスイッチの識別情報に基づいて、前記認証の結果を前記スイッチに送信し、前記スイッチは、前記認証サーバから受信した認証結果に基づいて、前記端末からのアクセスを認証する。

【発明の効果】

【００１２】

本発明の代表的な実施の形態によれば、認証スイッチに認証結果を登録することができる。前述した以外の課題、構成及び効果は、以下の実施例の説明により明らかにされる。

【図面の簡単な説明】

【００１３】

【図１】第１の実施例の認証システムの構成を示すブロック図である。
【図２】第１の実施例の認証スイッチのハードウェア構成を示すブロック図である。
【図３】第１の実施例の認証済み端末登録テーブルの構成を説明する図である。
【図４】第１の実施例のシーケンス図である。
【図５】第１の実施例のパケット転送処理のフローチャートである。
【図６】第１の実施例の認証処理のフローチャートである。
【図７】第２の実施例の認証スイッチの構成を示すブロック図である。
【図８】第２の実施例の認証サーバの構成を示すブロック図である。
【図９】第２の実施例のシーケンス図である。
【図１０】第２の実施例のパケット転送処理のフローチャートである。
【図１１Ａ】第２の実施例の認証処理のフローチャートである。
【図１１Ｂ】第２の実施例の認証処理のフローチャートである。
【図１２】第３の実施例のシーケンス図である。
【図１３】第４の実施例の認証サーバの構成を示すブロック図である。
【図１４】第４の実施例のシーケンス図である。
【図１５】第４の実施例の認証処理のフローチャートである。

【発明を実施するための形態】

【００１４】
＜実施例１＞
本発明の第１の実施例では、認証機能を有する認証スイッチ４００が、認証スイッチ４００の情報と端末６００の情報とを端末６００を介して認証サーバ１００に通知し、認証サーバ１００は、認証結果を認証スイッチ４００に登録する。
【００１５】
図１は、第１の実施例の認証システムの構成を示すブロック図である。
【００１６】
第１の実施例の認証システムは、認証サーバ１００、サーバ２００、Ｌ３スイッチ３００、少なくとも一つの認証スイッチ４００及び少なくとも一つのＨＵＢ５００を含む。ＨＵＢ５００は、少なくとも一つの端末６００を接続する。
【００１７】
認証サーバ１００、サーバ２００及び認証スイッチ４００は、Ｌ３スイッチ３００に接続されている。また、ＨＵＢ５００は、認証スイッチ４００に接続されており、端末６００は、ＨＵＢ５００に接続されている。
【００１８】
認証サーバ１００は、プロセッサ及びメモリを有する計算機で、端末６００のユーザを認証し（例えば、ＲＡＤＩＵＳ認証、シボレス認証など）、認証結果を認証スイッチ４００に設定する機能を提供する。
【００１９】
認証サーバ１００は、プログラムを実行するプロセッサ、プロセッサで実行されるプログラムを格納するメモリ、プログラム実行時に使用されるデータを格納する記憶装置及びネットワークと接続する通信インタフェース１０８を有する計算機である。すなわち、プロセッサが実行するプログラムは、記憶装置から読み出されて、メモリにロードされて、プロセッサによって実行される。プロセッサが所定のプログラムを実行することによって、各部の機能が実装される。
【００２０】
認証サーバ１００は、認証機能部１０１、認証データベース１０５、認証端末登録テーブル１０６、認証画面データ１０７及び通信インタフェース１０８を有する。
【００２１】
認証機能部１０１は、認証サーバ１００に認証を要求した端末６００を認証する。認証機能部１０１は、認証機能本体部１０２、認証スイッチ連携部１０３及び認証登録インタフェース１０４を有する。
【００２２】
認証機能本体部１０２は、認証データベース１０５を参照して、端末６００から送信された認証要求を認証する。また、認証機能本体部１０２は、認証を要求した端末６００の情報及び端末６００が接続する認証スイッチ４００の情報を、受信した認証要求から取得し、取得した情報を認証端末登録テーブル１０６へ登録する。また、認証機能本体部１０２は、ユーザ認証の結果を、認証を要求した端末６００及び認証スイッチ連携部１０３へ通知する。
【００２３】
認証スイッチ連携部１０３は、認証機能本体部１０２から認証結果が通知されると、認証された端末６００から送信されたユーザＩＤを用いて認証端末登録テーブル１０６を検索し、検索された情報を用いて、認証登録インタフェース１０４及び通信インタフェース１０８を介して、認証されたユーザ及び端末６００を認証スイッチ４００へ登録する。
【００２４】
認証登録インタフェース１０４は、認証スイッチ連携部１０３からの要求に従って、認証されたユーザ及び端末６００の情報を認証スイッチ４００へ送信する。
【００２５】
認証データベース１０５は、記憶装置に格納され、端末６００を認証するための情報が

登録されたデータベースであり、例えば、パスワードによる認証の場合、ユーザＩＤ及びパスワードを含む。また、認証データベース１０５は、認証成功時のアクセスポリシ（例えば、ＶＬＡＮ、ＱｏＳ、フィルタの情報など）を含んでもよい。

【００２６】

認証端末登録テーブル１０６は、記憶装置に格納され、認証されたユーザの情報、認証された端末６００の情報、及び認証された端末６００が接続する認証スイッチの情報が登録されるテーブルである。認証端末登録テーブル１０６は、例えば、ユーザＩＤ、パスワード、端末６００の情報（ＩＰアドレス、ＭＡＣアドレス）、端末６００が接続している認証スイッチ４００の情報（ＩＰアドレス）、認証結果などを含む。

【００２７】

認証画面データ１０７は、記憶装置に格納され、ユーザ認証に用いられる情報を入力させるために、端末６００に表示させる画面データである。

【００２８】

通信インタフェース１０８は、パケットを送受信する機能を有する、例えばイーサネット規格（イーサネットは登録商標、以下同じ）に準じたネットワークインタフェースである。

【００２９】

プロセッサが実行するプログラムは、リムーバブルメディア（ＣＤ－ＲＯＭ、フラッシュメモリなど）又はネットワークを介して認証サーバ１００に提供され、非一時的記憶媒体である記憶装置に格納される。このため、認証サーバ１００は、リムーバブルメディアを読み込むインタフェース（例えば、光ディスク装置、ＵＳＢポートなど）を有するとよい。

【００３０】

サーバ２００は、プログラムを実行するプロセッサ、前記プロセッサで実行されるプログラムを格納するメモリ及びネットワークインタフェースを有する計算機で、例えば、端末６００からのアクセスを受け付け、Ｗｅｂサーバ機能やＦＴＰ機能を端末６００に提供する。

【００３１】

Ｌ３スイッチ３００は、接続された認証サーバ１００、サーバ２００及び認証スイッチ４００間でパケットを転送するパケット転送装置である。

【００３２】

認証スイッチ４００は、接続されたＬ３スイッチ３００及びＨＵＢ５００間でパケットを転送するパケット転送装置である。また、認証スイッチ４００は、認証済み端末登録テーブル４０４を用いて、認証サーバ１００よって認証された端末６００を管理する。

【００３３】

認証スイッチ４００は、認証機能部４０１、認証済み端末登録テーブル４０４、ＵＲＬリダイレクト処理部４０５、認証端末登録インタフェース部４０６、パケット送受信部４０７及び通信インタフェース４１１を有する。

【００３４】

認証機能部４０１は、端末６００から送信された認証要求を処理する。認証機能部４０１は、認証処理部４０２及び認証登録部４０３を有する。認証処理部４０２は、端末６００から送信された認証要求を処理するネットワーク認証機能を提供する。認証登録部４０３は、認証サーバ１００が認証した認証済み端末の情報を認証済み端末登録テーブル４０４に登録する。

【００３５】

認証済み端末登録テーブル４０４は、認証済み端末のＭＡＣアドレス、ＩＰアドレス、ユーザＩＤ、所属ＶＬＡＮ　ＩＤ、アクセス制御情報などを管理する。認証済み端末登録テーブル４０４の構成は、図３を用いて後述する。

【００３６】

ＵＲＬリダイレクト処理部４０５は、端末６００からＨＴＴＰアクセスを受信すると、

端末６００をサーバ２００に直接リダイレクトするコマンドを含むリダイレクト通知を出力する。出力されるリダイレクト通知は、認証スイッチ４００のＩＰアドレス、認証される端末６００のＩＰアドレス、認証される端末６００のＭＡＣアドレス、認証される端末６００が所属すべきＶＬＡＮの識別情報、認証される端末６００が接続する認証スイッチ４００の物理ポート情報等を含む。これらの情報が端末６００から認証サーバ１００に送られる。

【００３７】

認証端末登録インタフェース部４０６は、外部からの入力によって、認証済みの端末６００の情報を登録するためのインタフェースである。認証スイッチ４００が認証プロトコルをサポートしない場合でも、認証端末登録インタフェース部４０６が認証サーバ１００による端末６００の認証結果を認証スイッチ４００に登録し、認証スイッチ４００によるネットワーク認証を可能にする。

【００３８】

パケット送受信部４０７は、パケットを受信し、受信したパケットを送信するパケットの送受信機能を提供する。パケット送受信部４０７は、転送制御部４０８、パケット転送テーブル４０９及び認証前転送制御部４１０を有する。

【００３９】

転送制御部４０８は、パケット転送テーブル４０９を参照して、受信したパケットを出力するポートを決定する転送エンジンを含む。パケット転送テーブル４０９は、パケットを転送するために用いられる、パケットの宛先とポートとの関係、及び、認証済み端末登録テーブル４０４を参照するための情報（例えば、端末６００のＩＰアドレスやＭＡＣアドレス）を保持する。認証前転送制御部４１０は、接続してきた認証前の端末６００を認証前のＶＬＡＮに所属させる。

【００４０】

具体的には、認証前転送制御部４１０は、受信パケットの送信元ＭＡＣアドレスを用いてパケット転送テーブル４０９を検索する。そして、当該送信元ＭＡＣアドレスが認証済み端末に付与されたアドレスである場合、認証前転送制御部４１０は、パケット転送テーブル４０９に登録された転送ポリシに従ってパケットを転送する。一方、当該送信元ＭＡＣアドレスが認証済み端末に付与されたアドレスでなく、かつ、当該パケットがＨＴＴＰパケットである場合、認証前転送制御部４１０は、当該パケットをＵＲＬリダイレクト処理部４０５へ転送する。また、当該送信元ＭＡＣアドレスが認証済み端末に付与されたアドレスでなく、かつ、当該パケットがＨＴＴＰパケットでない場合、認証前転送制御部４１０は、パケット転送テーブルの転送ポリシ（認証前転送ポリシ）に従って、パケットを転送する。

【００４１】

このため、認証前の端末６００が送信したＨＴＴＰパケットは、所定の宛先（例えば、認証サーバ１００）にのみアクセスでき、他のネットワークにアクセスすることができない。

【００４２】

通信インタフェース４１１は、例えばイーサネット規格に準じたネットワークインタフェースであり、パケットを入出力するポートを提供する。

【００４３】

ＨＵＢ５００は、認証スイッチ４００と端末６００との間を接続し、端末６００が送受信するパケットを転送するパケット転送装置である。

【００４４】

端末６００は、プログラムを実行するプロセッサ、前記プロセッサで実行されるプログラムを格納するメモリ、ネットワークインタフェース及びユーザインタフェース（例えば、表示画面、入力装置）を有する計算機である。

【００４５】

図２は、第１の実施例の認証スイッチ４００のハードウェア構成を示すブロック図であ

る。
【００４６】
認証スイッチ４００は、プロセッサ４１５、記憶部４１６、制御部４１７及び通信インタフェース４１１を有する。
【００４７】
プロセッサ４１５は、メモリ（図示省略）に格納されたプログラムを実行する。プロセッサ４１５が所定のプログラムを実行することによって、認証機能部４０１、ＵＲＬリダイレクト処理部４０５及び認証端末登録インタフェース部４０６の機能が実装される。
【００４８】
記憶部４１６は、例えば、フラッシュメモリ、磁気記憶装置等の不揮発性の記憶装置であり、プロセッサ４１５によって実行されるプログラム及びプログラム実行時に使用されるデータ（例えば、認証済み端末登録テーブル４０４）を格納する。すなわち、プロセッサ４１５が実行するプログラムは、記憶部４１６から読み出されて、メモリにロードされて、プロセッサ４１５によって実行される。
【００４９】
なお、認証機能部４０１、ＵＲＬリダイレクト処理部４０５及び認証端末登録インタフェース部４０６の一部又は全部の機能を、ハードウェアのロジック回路によって構成してもよい。
【００５０】
制御部４１７は、パケットを転送するための制御を行うパケット送受信部４０７の機能を有する。例えば、制御部４１７は、パケット転送テーブル４０９を参照して、パケットのヘッダに含まれる宛先アドレスに従って、受信したパケットを出力するポートを決定する。制御部４１７は、例えば、ロジック回路による専用のＬＳＩで構成することができるが、プロセッサが実行する制御プログラムによって実装してもよい。
【００５１】
プロセッサ４１５が実行するプログラムは、リムーバブルメディア（フラッシュメモリ、ＣＤ－ＲＯＭなど）又はネットワークを介して認証スイッチ４００に提供され、非一時的記憶媒体である記憶装置に格納される。このため、認証スイッチ４００は、リムーバブルメディアを読み込むインタフェース（例えば、ＵＳＢポート、光ディスク装置など）を有するとよい。
【００５２】
図３は、第１の実施例の認証済み端末登録テーブル４０４の構成を説明する図である。
【００５３】
認証済み端末登録テーブル４０４は、ユーザ情報４０１０、認証端末情報４０２０及び認証スイッチ情報４０３０を含む。
【００５４】
ユーザ情報４０１０は、認証されたユーザの情報であり、ユーザＩＤ４０１１、パスワード４０１２及びＶＬＡＮ４０１３を含む。ユーザＩＤ４０１１は、認証されたユーザを一意に識別するための識別情報である。パスワード４０１２は、当該ユーザが認証のために使用するパスワードである。ＶＬＡＮ４０１３は、当該ユーザが使用するＶＬＡＮを一意に識別するための識別情報である。
【００５５】
認証端末情報４０２０は、認証された端末６００の情報であり、ＩＰアドレス４０２１、ＭＡＣアドレス４０２２及びアクセスポリシ４０２３を含む。ＩＰアドレス４０２１は、当該ユーザが使用している端末６００に付与されたＩＰアドレスである。ＭＡＣアドレス４０２２は、当該端末６００に付与されたＭＡＣアドレスである。アクセスポリシ４０２３は、当該端末６００に設定されたアクセスポリシであり、例えば、特定の宛先宛のパケットを廃棄するなどである。
【００５６】
認証スイッチ情報４０３０は、認証スイッチ４００の情報であり、ＩＰアドレス４０３

１及び接続ポート４０３２を含む。ＩＰアドレス４０３１は、当該端末６００が接続する認証スイッチ４００に付与されたＩＰアドレスである。接続ポート４０３２は、当該端末６００が接続する認証スイッチ４００のポートの識別情報である。

【００５７】

図４は、第１の実施例の端末６００、認証スイッチ４００及び認証サーバ１００の間のシーケンス図である。

【００５８】

まず、端末６００は、ＨＵＢ５００に接続すると、端末６００に付与されたＭＡＣアドレス及びＩＰアドレスをＨＵＢ５００に送信する。ＨＵＢ５００は、端末６００から受信したＭＡＣアドレス及びＩＰアドレスを認証スイッチ４００に送信する。認証スイッチ４００は、接続した端末６００のアドレス（ＭＡＣアドレス、ＩＰアドレス）を記憶し、当該端末６００を認証前ＶＬＡＮに所属させる。このとき、端末６００は、認証前ＶＬＡＮで許可された宛先（本実施例では、認証サーバ１００）を除き、認証スイッチ４００より先のネットワークへアクセスできない。

【００５９】

その後、端末６００が、サーバ２００にアクセスをするために、ＨＴＴＰリクエストを送信する（１１０１）。認証スイッチ４００は、端末６００から送信されたＨＴＴＰアクセスを受信すると、ＨＴＴＰアクセスを送信した端末６００が認証済かを判定する。そして、ＨＴＴＰアクセスを送信した端末６００が未認証端末であれば、当該ＨＴＴＰアクセスを認証サーバ１００に再送信するためのリダイレクト通知を、ＨＴＴＰアクセスの送信元の端末６００に送信する（１１０２）。このリダイレクト通知は、認証スイッチ４００の情報（ＩＰアドレス、端末６００が接続されるポートの識別情報）を含む。

【００６０】

端末６００は、リダイレクト通知を受信すると、受信したリダイレクト通知に含まれるアクセス先の認証サーバ１００にＨＴＴＰリクエストを送信し、認証サーバ１００の認証ページにアクセスする（１１０３）。このとき、端末６００は、認証前ＶＬＡＮを用いて、認証サーバ１００にアクセスすることができる。認証サーバ１００は、認証ページにアクセスしてきた端末６００に、認証情報入力画面のデータを含むＨＴＴＰレスポンスを送信する（１１０４）。

【００６１】

ユーザは、端末６００に表示された認証情報入力画面に、認証情報（例えば、ユーザＩＤ及びパスワード）を入力する。端末６００は、入力された認証情報を、認証スイッチ４００を介して認証サーバ１００に送信する（１１０５）。端末６００は、受信したリダイレクト通知に含まれる認証スイッチ４００の情報を、認証情報と共に認証サーバ１００に送信する。なお、端末６００は、ＨＴＴＰリクエスト（１１０３）に含めて、認証スイッチ４００の情報を認証サーバ１００に送信してもよい。

【００６２】

認証サーバ１００は、受信した認証情報を用いて認証データベース１０５を検索する。受信した認証情報が認証データベース１０５に登録されている場合（１１０６）、認証サーバ１００は、認証の成功（ＲＡＤＩＵＳ認証によるアクセス許可）を認証スイッチ４００に通知する（１１０７）。

【００６３】

認証スイッチ４００宛の認証登録通知は、認証成功の情報及びアクセス制御情報（例えば、認証された端末６００を所属させるＶＬＡＮ情報）を含む。認証スイッチ４００は、認証された端末６００のＭＡＣアドレスについて認証許可処理を行い、認証結果を認証済み端末登録テーブル４０４に登録する（１１０８）。認証済み端末登録テーブル４０４への登録によって、認証サーバ１００に指定されたＶＬＡＮに、認証された端末６００が所属する。

【００６４】

また、認証サーバ１００は、認証の成功を端末６００に通知する（１１０９）。端末６

００は、認証の成功の通知を受けると、認証成功画面を表示する。
【００６５】
一方、認証サーバ１００は、受信した認証情報が認証データベース１０５に登録されていない場合（１１１０）、認証の失敗（ＲＡＤＩＵＳ認証によるアクセス拒否）を認証スイッチ４００に通知する（１１１１）。認証スイッチ４００は、認証失敗の情報を認証済み端末登録テーブル４０４に登録しなくてよい。
【００６６】
また、認証サーバ１００は、認証の失敗を端末６００に返信する（１１１２）。端末６００は、認証の失敗の通知を受けると、認証失敗画面を表示する。
【００６７】
図５は、第１の実施例の認証スイッチ４００が実行するパケット転送処理のフローチャートである。
【００６８】
まず、パケット送受信部４０７は、パケットを受信すると（１１２１）、受信したパケットの送信元のＭＡＣアドレス又はＩＰアドレスを用いて認証済み端末登録テーブル４０４を検索し、受信したパケットを送信した端末６００が認証済み端末であるかを判定する（１１２２）。
【００６９】
パケットを送信した端末６００が認証済み端末である場合、認証済み端末登録テーブル４０４に登録された転送ポリシ（例えば、ＶＬＡＮ）に従って、受信したパケットを転送する（１１２３）。一方、パケットを送信した端末６００が認証済み端末ではない場合、受信したパケットの種別を判定する（１１２４）。
【００７０】
その結果、受信したパケットがＨＴＴＰアクセスではない場合、認証前転送制御部４１０は、パケット転送テーブル４０９に登録された認証前転送ポリシに従ってパケットを転送する（１１２５）。一方、受信したパケットがＨＴＴＰアクセスである場合、パケット送受信部４０７は、当該パケットをＵＲＬリダイレクト処理部４０５へ転送する（１１２６）。
【００７１】
その後、パケット送受信部４０７は、認証サーバの生死を確認する（１１２７）。その結果、認証サーバから応答がある場合、ＵＲＬリダイレクト処理部４０５は、認証サーバ１００へリダイレクトさせるためのリダイレクトパケットを生成し、パケットを送信した端末６００へ送信する（１１２８）。
【００７２】
一方、認証サーバから応答がない場合、ＵＲＬリダイレクト処理部４０５は、自装置宛へリダイレクトさせるためのリダイレクトパケットを生成し、パケットを送信した端末６００へ送信する（１１２９）。
【００７３】
ステップ１１２８、１１２９で生成されるリダイレクトパケットは、認証スイッチ４００のＩＰアドレス、端末６００が接続している物理ポートの情報、及び、端末６００のＭＡＣアドレス及びＩＰアドレス等を格納する。
【００７４】
図６は、第１の実施例の認証処理のフローチャートである。図６に示す認証処理は、認証サーバ１００のプロセッサが実行する。
【００７５】
まず、認証機能本体部１０２は、通信インタフェース１０８が認証要求のＨＴＴＰリクエストを受信するまで待機する（１１３１）。認証機能本体部１０２は、受信したＨＴＴＰリクエストから認証情報（ユーザＩＤ、パスワード）を抽出し、認証データベース１０５を用いて、抽出した認証情報の認証を試みる（１１３２）。
【００７６】

その結果、認証が成功した場合、認証機能本体部１０２は、ＨＴＴＰリクエストから端末情報を抽出し、抽出した端末情報を認証端末登録テーブル１０６へ書き込む（１１３３）。その後、認証機能本体部１０２は、認証結果及び該当ユーザＩＤを認証スイッチ連携部１０３へ通知する（１１３４）。

【００７７】

認証スイッチ連携部１０３は、認証機能本体部１０２から受信した認証結果及びユーザＩＤを用いて認証データベース１０５を検索し、当該ユーザのアクセス制御の情報を取得し、取得したアクセス制御の情報を認証端末登録テーブル１０６に書き込む（１１３５）。そして、認証スイッチ連携部１０３は、受信したユーザＩＤを用いて認証端末登録テーブル１０６を検索し、当該ユーザの情報を取得する（１１３６）。

【００７８】

さらに、認証スイッチ連携部１０３は、取得したユーザの情報から認証登録情報を作成し、作成した認証登録情報を認証登録インタフェース１０４に送る。認証登録インタフェース１０４は、受信した認証登録情報を認証スイッチ４００に送信する（１１３７）。

【００７９】

なお、以上に説明した認証方法は、従来の、認証スイッチ４００がプロキシとなるＷｅｂ認証機能と併用することができる。例えば、認証スイッチ４００において、Ｗｅｂ認証機能を使うモードと認証サーバ１００を使うモードとを切り替えてもよい。また、認証サーバ１００の状態によって、認証スイッチ４００のＷｅｂ認証機能の有効／無効を制御してもよい。

【００８０】

具体的には、前述した転送処理のステップ１１２７において、ＵＲＬリダイレクト処理部４０５が、認証サーバ１００の状態を確認する。認証サーバ１００からの応答がない場合、ＵＲＬリダイレクト処理部４０５は、自装置のＷｅｂ認証機能を有効にし、リダイレクト先を自宛にして、アクセスしてきた端末６００に応答する（１１２９）。

【００８１】

以上に説明したように、第１の実施例では、認証スイッチ４００が送信するリダイレクト通知１１０２によって、端末６００と認証スイッチ４００との間の認証シーケンスから、端末６００と認証サーバ１００との間の認証シーケンスに切り替える。このため、認証サーバ１００は、端末６００が接続している認証スイッチ４００を知ることができ、認証端末登録インタフェース部４０６を介して、認証結果を認証スイッチ４００に登録することができる。特に、前述した特許文献１のように端末と認証サーバとの間の認証シーケンスをスヌーピングしなくても、認証結果を認証スイッチ４００に登録することができる。さらに、認証スイッチ４００は、登録された端末６００をネットワーク認証された端末として管理することができる。

【００８２】

また、認証スイッチでＷｅｂサーバを動作させ認証情報を認証サーバに中継する必要がないので、認証スイッチ４００の認証処理による負荷を減らしつつ、認証済み端末を検出でき、認証済み端末の離脱をチェックすることができる。このため、不要な認証情報やフィルタ情報やＱｏＳ設定を認証スイッチから消去することができ、認証スイッチの記憶領域を有効に利用することができる。また、認証済みＭＡＣアドレスを詐称した端末の接続を排除して、セキュリティを向上することができる。

【００８３】

また、認証スイッチが認証プロキシ機能を有する場合、ネットワーク認証方式毎のモジュールを設ける必要があるが第１の実施例では、ネットワーク認証方式に依存しないネットワーク認証システムを構築することができる。

【００８４】

＜実施例２＞

次に、本発明の第２の実施例について説明する。第２の実施例では、端末６００から送信されたＨＴＴＰアクセスを認証サーバ１００へトンネリングすることによって、端末６

００及び認証スイッチ４００の情報を認証サーバ１００通知する。このため、第２の実施例では、第１の実施例における図１の認証スイッチ４００及び認証サーバ１００の構成が異なる。なお、第２の実施例において、前述した第１の実施例と異なる構成、機能及び処理のみを説明し、同一の部分の説明は省略する。

【００８５】

図７は、第２の実施例の認証スイッチ４００の構成を示すブロック図である。

【００８６】

第２の実施例の認証スイッチ４００は、認証機能部４０１、認証済み端末登録テーブル４０４、ＵＲＬリダイレクト処理部４０５、認証端末登録インタフェース部４０６、パケット送受信部４０７、通信インタフェース４１１及びトンネリング処理部４２１を有する。

【００８７】

認証機能部４０１、認証済み端末登録テーブル４０４、ＵＲＬリダイレクト処理部４０５及び認証端末登録インタフェース部４０６の構成及び機能は、前述した第１の実施例のこれらの構成及び機能と同じである。

【００８８】

トンネリング処理部４２１は、認証スイッチ４００と認証サーバ１００との間に設定されたトンネルを用いて、端末６００と認証サーバ１００との間のＨＴＴＰパケットを転送する。また、トンネリング処理部４２１は、カプセル化されたパケットのヘッダを外して、デカプセリング処理を行う。

【００８９】

パケット送受信部４０７は、パケットを受信し、受信したパケットを送信するパケットの送受信機能を提供する。パケット送受信部４０７は、転送制御部４０８、パケット転送テーブル４０９、認証前転送制御部４１０及びトンネル判定部４２２を有する。

【００９０】

転送制御部４０８、パケット転送テーブル４０９、認証前転送制御部４１０及び通信インタフェース４１１の構成及び機能は、前述した第１の実施例のこれらの構成及び機能と同じである。

【００９１】

トンネル判定部４２２は、カプセル化されてトンネルを経由して転送されたパケットを判定して、トンネリング処理部４２１に送る。

【００９２】

図８は、第２の実施例の認証サーバ１００の構成を示すブロック図である。

【００９３】

認証サーバ１００は、プログラムを実行するプロセッサ、プロセッサで実行されるプログラムを格納するメモリ、プログラム実行時に使用されるデータを格納する記憶装置及びネットワークと接続する通信インタフェースを有する計算機である。

【００９４】

第２の実施例の認証サーバ１００は、認証機能部１０１、認証データベース１０５、認証端末登録テーブル１０６、認証画面データ１０７、通信インタフェース１０８及びトンネリング処理部１２１を有する。

【００９５】

認証機能部１０１、認証データベース１０５、認証端末登録テーブル１０６、認証画面データ１０７及び通信インタフェース１０８の構成及び機能は、前述した第１の実施例のこれらの構成及び機能と同じである。

【００９６】

トンネリング処理部１２１は、認証スイッチ４００と認証サーバ１００との間に設定されたトンネルを用いて、端末６００と認証サーバ１００との間のＨＴＴＰパケットを転送する。また、トンネリング処理部１２１は、カプセル化されたパケットのヘッダを外して、デカプセリング処理を行う。

【００９７】
通信インタフェース１０８は、パケットを送受信する機能を有する、例えばイーサネット規格に準じたネットワークインタフェースである。また、通信インタフェース１０８は、トンネル判定部１２２を有する。トンネル判定部１２２は、カプセル化されてトンネルを経由して転送されたパケットを判定して、トンネリング処理部１２１に送る。
【００９８】
図９は、第２の実施例の端末６００、認証スイッチ４００及び認証サーバ１００の間のシーケンス図である。
【００９９】
まず、端末６００が、サーバ２００にアクセスをするために、ＨＴＴＰリクエストを送信する（１２０１）。認証スイッチ４００は、端末６００から送信されたＨＴＴＰアクセスを受信すると、ＨＴＴＰアクセスを送信した端末６００が認証済かを判定する。そして、認証スイッチ４００は、ＨＴＴＰアクセスを送信した端末６００が未認証端末であれば、接続した端末６００のアドレス（ＭＡＣアドレス、ＩＰアドレス）を記憶し、当該端末６００を認証前ＶＬＡＮに所属させる。このとき、端末６００は、認証前ＶＬＡＮで許可された宛先（本実施例では、認証サーバ１００）を除き、認証スイッチ４００より先のネットワークへアクセスできない。
【０１００】
また、認証スイッチ４００は、認証スイッチ４００のＩＰアドレスを送信元にし、認証サーバ１００のＩＰアドレスを宛先にしたヘッダで、受信したパケット（ＨＴＴＰアクセス）をカプセル化する（１２０２）。そして、認証スイッチ４００は、カプセル化されたＨＴＴＰアクセスを、認証サーバ１００との間に設定されたトンネルを経由して送信する（１２０３）。認証サーバ１００に送信されるＨＴＴＰアクセスは、認証スイッチ４００の情報（ＩＰアドレス、端末６００が接続されるポートの識別情報）を含む。
【０１０１】
認証サーバ１００は、カプセル化されたＨＴＴＰアクセスを受信すると、カプセル化されたパケットからカプセリングヘッダを外す処理を行い、当該ＨＴＴＰアクセスを認証サーバ１００に再送信するためのリダイレクト通知を作成する。そして、認証サーバ１００は、作成されたリダイレクト通知をカプセル化し、カプセル化されたリダイレクト通知を、認証スイッチ４００との間に設定されたトンネルを経由して、ＨＴＴＰアクセスの送信元の認証スイッチ４００に送信する（１２０４）。認証サーバ１００から送信されるリダイレクト通知は、リダイレクト先である認証サーバ１００の情報を含む。
【０１０２】
認証スイッチ４００は、カプセル化されたリダイレクト通知を受信すると、受信したリダイレクト通知からカプセリングヘッダを外してデカプセル化して（１２０５）、デカプセル化されたリダイレクト通知を、ＨＴＴＰアクセスの送信元の端末６００に送信する（１２０６）。
【０１０３】
端末６００は、リダイレクト通知を受信すると、リダイレクト通知に含まれるアクセス先の認証サーバ１００にＨＴＴＰリクエストを送信し、認証サーバ１００の認証ページにアクセスする（１２０７）。認証サーバ１００は、認証ページにアクセスしてきた端末６００に、認証情報入力画面のデータを含むＨＴＴＰレスポンスを送信する（１２０８）。
【０１０４】
１２０９から１２１６の処理は、第１の実施例の１１０５から１１１２の処理と同じである。
【０１０５】
図１０は、第２の実施例の認証スイッチ４００が実行するパケット転送処理のフローチャートである。
【０１０６】
まず、パケット送受信部４０７がパケットを受信すると（１２２１）、トンネル判定部

４２２は、受信したパケットのヘッダを参照して、受信したパケットの種別を判定する（１２２２）。

【０１０７】

その結果、受信したパケットがトンネルパケットであれば（１２２３でＹ）、トンネル判定部４２２は、受信したパケットをトンネリング処理部４２１に送る。トンネリング処理部４２１は、受信したパケットからカプセリングヘッダを外してデカプセル化する（１２２４）。パケット送受信部４０７は、デカプセル化されたパケットを、ヘッダに従って端末６００へ転送する（１２２５）。

【０１０８】

一方、受信したパケットがトンネルパケットでなければ（１２２３でＮ）、トンネル判定部４２２は、受信したパケットが認証情報登録パケットであるかを判定する（１２２６）。

【０１０９】

その結果、受信したパケットが認証情報登録パケットであれば（１２２６でＹ）、トンネル判定部４２２は、受信したパケットを認証端末登録インタフェース部４０６に送る。認証端末登録インタフェース部４０６は、受信パケットから認証登録情報を取得し、取得した認証情報を認証登録部４０３へ送る（１２２７）。認証登録部４０３は、受信した認証情報を認証済み端末登録テーブル４０４へ登録する（１２２８）。

【０１１０】

一方、受信したパケットが認証情報登録パケットでなければ（１２２６でＮ）、トンネル判定部４２２は、認証済み端末登録テーブル４０４を参照して、受信したパケットのＭＡＣアドレスが認証済み端末のアドレスであるかを判定する（１２２９）。

【０１１１】

その結果、受信したパケットのＭＡＣアドレスが認証済み端末のアドレスであれば、転送制御部４０８は、パケット転送テーブル４０９を参照して、パケットのヘッダに含まれる宛先アドレスに従って、受信したパケットを転送する（１２３０）。

【０１１２】

一方、受信したパケットのＭＡＣアドレスが認証済み端末のアドレスでなければ（１２２９でＮ）、トンネル判定部４２２は、受信したパケットのプロトコルを判定する（１２３１）。

【０１１３】

その結果、受信したパケットのプロトコルがＨＴＴＰプロトコルでなければ、パケット送受信部４０７は、受信したパケットの転送が不要であると判定して、パケットを破棄する（１２３２）。一方、受信したパケットのプロトコルがＨＴＴＰプロトコルであれば、トンネリング処理部４２１は、認証サーバ１００のＩＰアドレスを宛先にしたヘッダで、受信したパケットをカプセル化するカプセリング処理を実行する（１２３３）。そして、パケット送受信部４０７は、カプセル化されたパケットを認証サーバ１００に送信する（１２３４）。

【０１１４】

図１１Ａ及び図１１Ｂは、第２の実施例の認証処理のフローチャートである。図１１Ａ及び図１１Ｂに示す認証処理は、認証サーバ１００のプロセッサが実行する。

【０１１５】

まず、通信インタフェース１０８がパケットを受信すると（１２４１）、トンネル判定部１２２は、受信したパケットのヘッダを参照して、受信したパケットの種別を判定する（１２４２）。

【０１１６】

その結果、受信したパケットがトンネルパケットでなければ（１２４３でＮ）、認証機能本体部１０２は、受信したパケットから認証情報を抽出し、抽出した認証情報を用いて認証データベース１０５を検索する通常の認証処理を実行する（１２４４）。

【０１１７】

一方、受信したパケットがトンネルパケットであれば（１２４３でＹ）、トンネル判定部１２２は、受信したパケットをトンネリング処理部１２１に送る。トンネリング処理部１２１は、受信したパケットからカプセリングヘッダを外してデカプセル化するデカプセリング処理を実行し（１２４５）、デカプセル化したパケットの種別を判定する（１２４６）。

【０１１８】

その結果、デカプセル化されたパケットがＨＴＴＰアクセスであれば（１２４７でＹ）、トンネリング処理部１２１は、受信したパケットを認証機能本体部１０２に送る。認証機能本体部１０２は、当該ＨＴＴＰアクセスを認証サーバ１００に再送信するためのリダイレクト通知を生成し、生成したリダイレクト通知をトンネリング処理部１２１に送る（１２４８）。

【０１１９】

トンネリング処理部１２１は、認証スイッチ４００のＩＰアドレスを宛先にしたヘッダで、生成されたリダイレクト通知をカプセル化し、カプセル化したパケットを通信インタフェース１０８に送る（１２４９）。通信インタフェース１０８は、カプセル化したパケットを認証スイッチ４００に送信する（１２５０）。

【０１２０】

一方、デカプセル化されたパケットがＨＴＴＰアクセスでなければ（１２４７でＮ）、トンネリング処理部１２１は、デカプセル化されたパケットが認証受付のＨＴＴＰリクエストであるかを判定する（１２５１）。

【０１２１】

その結果、デカプセル化されたパケットが認証受付のＨＴＴＰリクエストであれば（１２５１でＹ）、トンネリング処理部１２１は、受信したパケットを認証機能本体部１０２に送る。認証機能本体部１０２は、認証画面データ１０７から取得した認証情報入力画面のデータを含むＨＴＴＰレスポンスを、当該ＨＴＴＰリクエストを送信した端末６００に送信する（１２５２）。一方、デカプセル化されたパケットが認証受付のＨＴＴＰリクエストでなければ（１２５１でＮ）、ステップ１２５３に進む。

【０１２２】

ステップ１２５３では、トンネリング処理部１２１は、デカプセル化されたパケットが認証要求のＨＴＴＰリクエストであるかを判定する（１２５３）。

【０１２３】

その結果、デカプセル化されたパケットが認証要求のＨＴＴＰリクエストでなければ（１２５３でＮ）、当該パケットを処理する必要がないため、認証機能本体部１０２は、受信したパケット（デカプセル化したパケット）を破棄する（１２５４）。

【０１２４】

一方、デカプセル化されたパケットが認証要求のＨＴＴＰリクエストであれば（１２５３でＹ）、認証機能本体部１０２は、認証データベース１０５を用いて、端末６００から送信された認証情報（ユーザＩＤ、パスワード）の認証を試みる（１２５５）。

【０１２５】

認証が成功した場合の処理（１２５６～１２６０）は、第１の実施例の１１３３から１１３７の処理と同じである。

【０１２６】

以上に説明したように、前述した第１の実施例の効果に加え、第２の実施例では、認証サーバ１００が送信するリダイレクト通知１２０４及び１２０６によって、端末６００と認証スイッチ４００との間の認証シーケンスから、端末６００と認証サーバ１００との間の認証シーケンスに切り替える。このため、認証サーバ１００は、端末６００が接続している認証スイッチ４００を知ることができ、認証端末登録インタフェース部４０６を介して、認証結果を認証スイッチ４００に登録することができる。さらに、認証スイッチ４００は、登録された端末６００をネットワーク認証された端末として管理することができる。

【０１２７】
＜実施例３＞
次に、本発明の第３の実施例について説明する。第３の実施例では、シボレス認証におけるサービスプロバイダ（ＳＰ）を認証サーバとし、サービスプロバイダがリダイレクト通知を送信することによって、端末とアイデンティティプロバイダ（ＩｄＰ）との間の認証を実現する。なお、第３の実施例において、前述した第１又は第２の実施例と異なる構成、機能及び処理のみ説明し、同一の部分の説明は省略する。
【０１２８】
シボレス（Ｓｈｉｂｂｏｌｅｔｈ）認証とは、アイデンティティプロバイダ（ＩｄＰ）２５０が利用者の情報を提供し、サービスプロバイダ（ＳＰ）１５０が、アイデンティティプロバイダから提供された情報を利用して、通信を許可し、ＳＳＯ（シングルサインオン）環境を実現する認証システムである。
【０１２９】
第３の実施例の認証システムは、サービスプロバイダ１５０、アイデンティティプロバイダ２５０、Ｌ３スイッチ３００、少なくとも一つの認証スイッチ４００及び少なくとも一つのＨＵＢ５００を含む。ＨＵＢ５００は、少なくとも一つの端末６００を接続する。すなわち、第３の実施例の認証システムは、図１に示す第１の実施例の認証システムのうち、認証サーバ１００がサービスプロバイダ１５０に置き換わり、サーバ２００がアイデンティティプロバイダ２５０に置き換わったものである。
【０１３０】
図１２は、第３の実施例の端末６００、認証スイッチ４００、サービスプロバイダ（ＳＰ）１５０及びアイデンティティプロバイダ（ＩｄＰ）２５０の間のシーケンス図である。
【０１３１】
まず、端末６００が、サーバ２００にアクセスをするのために、ＨＴＴＰリクエストを送信する（１３０１）。認証スイッチ４００は、端末６００から送信されたＨＴＴＰアクセスを受信すると、ＨＴＴＰアクセスを送信した端末６００が認証済かを判定する。そして、認証スイッチ４００は、ＨＴＴＰアクセスを送信した端末６００が未認証端末であれば、接続した端末６００のアドレス（ＭＡＣアドレス、ＩＰアドレス）を記憶し、当該端末６００を認証前ＶＬＡＮに所属させる。このとき、端末６００は、認証前ＶＬＡＮで許可された宛先（本実施例では、サービスプロバイダ１５０）を除き、認証スイッチ４００より先のネットワークへアクセスできない。
【０１３２】
また、認証スイッチ４００は、認証スイッチ４００のＩＰアドレスを送信元にし、認証サーバ１００のＩＰアドレスを宛先にしたヘッダで、受信したパケット（ＨＴＴＰアクセス）をカプセル化する（１３０２）。そして、認証スイッチ４００は、カプセル化されたＨＴＴＰアクセスを、サービスプロバイダ１５０との間に設定されたトンネルを経由して送信する（１３０３）。サービスプロバイダ１５０に送信されるＨＴＴＰアクセスは、認証スイッチ４００の情報を含む。
【０１３３】
サービスプロバイダ１５０は、カプセル化されたＨＴＴＰアクセスを受信すると、カプセル化されたパケットからカプセリングヘッダを外す処理を行い、当該ＨＴＴＰアクセスをサービスプロバイダ１５０に再送信するためのリダイレクト通知を作成する。そして、サービスプロバイダ１５０は、作成されたリダイレクト通知をカプセル化し、カプセル化されたリダイレクト通知を、認証スイッチ４００との間に設定されたトンネルを経由して送信する（１３０４）。サービスプロバイダ１５０から送信されるリダイレクト通知は、サービスプロバイダ１５０の情報を含む。
【０１３４】
認証スイッチ４００は、カプセル化されたリダイレクト通知を受信すると、受信したリダイレクト通知からカプセリングヘッダを外してデカプセル化して（１３０５）、デカプ

セル化されたリダイレクト通知を、ＨＴＴＰアクセスの送信元の端末６００に送信する（１３０６）。

【０１３５】

端末６００は、リダイレクト通知を受信すると、リダイレクト通知に含まれるアクセス先のサービスプロバイダ１５０に、認証ページにアクセスするためのＨＴＴＰリクエストを送信する（１３０７）。

【０１３６】

認証スイッチ４００は、認証スイッチ４００のＩＰアドレスを送信元にし、認証サーバ１００のＩＰアドレスを宛先にしたヘッダで、受信したパケット（ＨＴＴＰリクエスト）をカプセル化する（１３０８）。そして、認証スイッチ４００は、カプセル化されたＨＴＴＰリクエストを、サービスプロバイダ１５０との間に設定されたトンネルを経由して送信する（１３０９）。

【０１３７】

サービスプロバイダ１５０は、カプセル化されたＨＴＴＰリクエストを受信すると、カプセル化されたパケットからカプセリングヘッダを外すデカプセリング処理を行い、当該ＨＴＴＰリクエストをアイデンティティプロバイダ２５０に再送信するためのリダイレクト通知を作成する。そして、サービスプロバイダ１５０は、作成されたリダイレクト通知をカプセル化し、カプセル化されたリダイレクト通知を、認証スイッチ４００との間に設定されたトンネルを経由して送信する（１３１０）。サービスプロバイダ１５０から送信されるリダイレクト通知は、アイデンティティプロバイダ２５０の情報を含む。

【０１３８】

認証スイッチ４００は、カプセル化されたリダイレクト通知を受信すると、受信したリダイレクト通知からカプセリングヘッダを外してデカプセル化して（１３１１）、デカプセル化されたリダイレクト通知を、ＨＴＴＰリクエストの送信元の端末６００に送信する（１３１２）。

【０１３９】

端末６００は、リダイレクト通知を受信すると、リダイレクト通知に含まれるアクセス先のアイデンティティプロバイダ２５０に、認証ページにアクセスするためのＨＴＴＰリクエストを送信して、シボレス認証システムにアクセスする（１３１３）。

【０１４０】

なお、認証前の端末６００とアイデンティティプロバイダ２５０との間の通信は、パケットをフォワーディングするフィルタを認証スイッチ４００に設定することによって、認証スイッチ４００によるトンネリング処理を回避する。

【０１４１】

アイデンティティプロバイダ２５０は、認証ページにアクセスしてきた端末６００に、認証情報入力画面のデータを含むＨＴＴＰレスポンスを送信する（１３１４）。

【０１４２】

ユーザは、端末６００に表示された認証情報入力画面に、認証情報（例えば、ユーザＩＤ及びパスワード）を入力する。端末６００は、入力された認証情報を、認証スイッチ４００を介してアイデンティティプロバイダ２５０に送信する（１３１５）。

【０１４３】

アイデンティティプロバイダ２５０は、受信した認証情報を用いて認証データベースを検索し、受信した認証情報が認証データベースに登録されている場合、認証の成功を端末６００に通知する（１３１６）。端末６００宛の認証成功通知は、認証成功の情報及びサービスプロバイダ１５０へのリダイレクト情報を含む。

【０１４４】

端末６００は、受信した認証成功通知に含まれるリダイレクト情報に従って、サービスプロバイダ１５０へアクセスするためのパケットを送信する（１３１７）。端末６００が送信するパケットは、端末６００の認証成功の情報を含む。

【０１４５】

認証スイッチ４００は、認証スイッチ４００のＩＰアドレスを送信元にし、認証サーバ１００のＩＰアドレスを宛先にしたヘッダで、受信したパケットをカプセル化する（１３１８）。そして、認証スイッチ４００は、カプセル化されたパケットを、サービスプロバイダ１５０との間に設定されたトンネルを経由して送信する（１３１９）。

【０１４６】

サービスプロバイダ１５０は、受信した認証成功の情報を用いて認証データベースを検索し、受信した認証情報が認証データベースに登録されている場合、認証データベースから取得した認証が成功した端末６００の情報を認証スイッチ４００に通知する（１３２０）。認証スイッチ４００宛の認証登録通知は、認証成功の情報及びアクセス制御情報（例えば、認証された端末６００を所属させるＶＬＡＮ情報）を含む。認証スイッチ４００は、認証された端末６００のＭＡＣアドレスについて認証許可処理を行い、認証結果を認証済み端末登録テーブル４０４に登録する。認証済み端末登録テーブル４０４への登録によって、認証サーバ１００に指定されたＶＬＡＮに、認証された端末６００を所属させる。

【０１４７】

また、サービスプロバイダ１５０は、認証の成功を端末６００に送信する認証成功の画面を含むＨＴＴＰレスポンスを作成する。そして、サービスプロバイダ１５０は、作成されたＨＴＴＰレスポンスをカプセル化し、認証スイッチ４００との間に設定されたトンネルを経由して、カプセル化されたＨＴＴＰレスポンスを送信する（１３２１）。

【０１４８】

認証スイッチ４００は、カプセル化されたＨＴＴＰレスポンスを受信すると、受信したＨＴＴＰレスポンスからカプセリングヘッダを外してデカプセル化して（１３２２）、デカプセル化されたＨＴＴＰレスポンスを、ＨＴＴＰリクエストの送信元の端末６００に送信する（１３２３）。

【０１４９】

端末６００は、認証の成功の通知を受けると、認証成功画面を表示する。

【０１５０】

以上に説明したように、前述した第１の実施例の効果に加え、第３の実施例では、シボレス認証システムにおいても、認証サーバ１００による認証の結果を認証済み端末登録テーブル４０４に登録することができる。さらに、認証スイッチ４００は、登録された端末６００をネットワーク認証された端末として管理することができる。

【０１５１】

＜実施例４＞

次に、本発明の第４の実施例について説明する。第４の実施例では、認証サーバ１００が認証スイッチ４００からのＲＡＤＩＵＳプロトコルを使った認証リクエスト情報を保持し、端末６００と認証サーバ１００との間で認証した結果を使って、保持する認証リクエスト情報に対する返信を認証スイッチ４００に送信する。このため、第４の実施例では、第１の実施例における図１の認証サーバ１００の構成が異なる。なお、第４の実施例において、前述した第１の実施例と異なる構成、機能及び処理のみ説明し、同一の部分の説明は省略する。

【０１５２】

図１３は、第４の実施例の認証サーバ１００の構成を示すブロック図である。

【０１５３】

第４の実施例の認証サーバ１００は、プログラムを実行するプロセッサ（ＣＰＵ）１４１、プロセッサで実行されるプログラムを格納するメモリ（図示省略）、プログラム実行時に使用されるデータを格納する記憶装置１４５及びネットワークと接続する通信インタフェース１４８を有する計算機である。

【０１５４】

プロセッサ１４１は、メモリに格納されたプログラムを実行する。プロセッサ１４１が所定のプログラムを実行することによって、認証処理部１４２、ＨＴＴＰサーバ部１４３及びＲＡＤＩＵＳサーバ部１４４の機能が実装される。

【０１５５】
認証処理部１４２は、認証データベース１４６を参照して、端末６００から送信された認証要求を認証する。ＨＴＴＰサーバ部１４３は、ユーザ認証のためのＨＴＴＰ応答パケットを生成する。
【０１５６】
ＲＡＤＩＵＳサーバ部１４４は、ＭＡＣ認証のためのＲＡＤＩＵＳ応答を生成するための処理を実行する。具体的には、ＲＡＤＩＵＳサーバ部１４４は、ＭＡＣ認証リクエストパケットを受信するまで待機し、ＭＡＣ認証リクエストパケットを受信した後、ＲＡＤＩＵＳアクセス要求パケットを受け付ける。そして、ＲＡＤＩＵＳサーバ部１４４は、受け付けたＲＡＤＩＵＳアクセス要求パケットから、認証すべき端末６００のＩＰアドレス及びＲＡＤＩＵＳアクセス要求パケットデータの組を抽出し、抽出した情報を認証待ち端末登録テーブル１４７に登録する。
【０１５７】
記憶装置１４５は、例えば、磁気記憶装置、フラッシュメモリ等の不揮発性の記憶装置であり、プロセッサ１４１によって実行されるプログラム及びプログラム実行時に使用されるデータを格納する。すなわち、プロセッサ１４１が実行するプログラムは、記憶装置１４５から読み出されて、メモリにロードされて、プロセッサ１４１によって実行される。記憶装置１４５は、認証データベース１４６及び認証待ち端末登録テーブル１４７を格納する。
【０１５８】
認証データベース１４６は、端末６００を認証するための情報が登録されたデータベースであり、例えば、パスワードによる認証の場合、ユーザＩＤ及びパスワードを含む。また、認証データベース１４６は、認証成功時のアクセスポリシ（例えば、ＶＬＡＮ、ＱｏＳ、フィルタの情報等）を含んでもよい。
【０１５９】
認証待ち端末登録テーブル１４７は、ＭＡＣ認証を行う際にＲＡＤＩＵＳのセッションを一時的に保持しておくための情報が登録されるテーブルであり、端末６００のＩＰアドレス及びＲＡＤＩＵＳアクセス要求パケットデータの組が保持される。
【０１６０】
通信インタフェース１４８は、パケットを送受信する機能を有する、例えばイーサネット規格に準じたネットワークインタフェースである。
【０１６１】
プロセッサ１４１が実行するプログラムは、リムーバブルメディア（ＣＤ－ＲＯＭ、フラッシュメモリなど）又はネットワークを介して認証サーバ１００に提供され、非一時的記憶媒体である記憶装置に格納される。このため、認証サーバ１００は、リムーバブルメディアを読み込むインタフェース（例えば、光ディスク装置、ＵＳＢポート）を有するとよい。
【０１６２】
図１４は、第４の実施例の端末６００、認証スイッチ４００及び認証サーバ１００の間のシーケンス図である。
【０１６３】
まず、端末６００は、ＨＵＢ５００に接続すると、端末６００に付与されたＭＡＣアドレス及びＩＰアドレスをＨＵＢ５００に送信する。ＨＵＢ５００は、端末６００から受信したＭＡＣアドレス及びＩＰアドレスを認証スイッチ４００に送信する（１４０１）。
【０１６４】
認証スイッチ４００は、接続した端末６００のアドレス（ＭＡＣアドレス、ＩＰアドレス）を記憶し、当該端末６００を認証前ＶＬＡＮに所属させる。このとき、端末６００は、認証前ＶＬＡＮで許可された宛先（本実施例では、認証サーバ１００）を除き、認証スイッチ４００より先のネットワークへアクセスできない。
【０１６５】

そして、認証スイッチ４００は、認証サーバへＭＡＣ認証リクエストパケットを送信する（１４０２）。このＭＡＣ認証リクエストパケットは、ＲＡＤＩＵＳ認証要求のパラメータとして、端末のＭＡＣアドレス及びＩＰアドレスを含む。また、ＭＡＣ認証レスポンス１４０７までに認証がタイムアウトしないように、ＲＡＤＩＵＳ認証のタイムアウト時間を十分に長い値に設定する。

【０１６６】

その後、端末６００は、ＨＴＴＰリクエストを認証サーバ１００に送信し、認証サーバ１００の認証ページにアクセスする（１４０３）。このとき、端末６００は、認証前ＶＬＡＮを用いて、認証サーバ１００にアクセスすることができる。認証サーバ１００は、認証ページにアクセスしてきた端末６００に、認証情報入力画面のデータを含むＨＴＴＰレスポンスを送信する（１４０４）。

【０１６７】

ユーザは、端末６００に表示された認証情報入力画面に、認証情報（例えば、ユーザＩＤ及びパスワード）を入力する。端末６００は、入力された認証情報を、認証スイッチ４００を介して認証サーバ１００に送信する（１４０５）。

【０１６８】

認証サーバ１００は、受信した認証情報を用いて認証データベース１０５を検索し、受信した認証情報が認証データベース１０５に登録されている場合（１４０６）、ＭＡＣ認証レスポンスを認証スイッチ４００に送信し、ＲＡＤＩＵＳ認証によるアクセス許可を通知する（１４０７）。認証スイッチ４００宛のＭＡＣ認証レスポンスは、認証成功の情報及びアクセス制御情報（例えば、認証された端末６００を所属させるＶＬＡＮ情報）を含む。認証スイッチ４００は、認証された端末６００のＭＡＣアドレスについて認証許可処理を行い、認証結果を認証済み端末登録テーブル４０４に登録する（１４０８）。認証済み端末登録テーブル４０４への登録によって、認証サーバ１００に指定されたＶＬＡＮに、認証された端末６００を所属させる。

【０１６９】

また、認証サーバ１００は、認証の成功を端末６００に通知する（１４０９）。端末６００は、認証の成功の通知を受けると、認証成功画面を表示する。

【０１７０】

一方、認証サーバ１００は、受信した認証情報が認証データベース１０５に登録されていない場合（１４１０）、ＭＡＣ認証レスポンスを認証スイッチ４００に送信し、ＲＡＤＩＵＳ認証によるアクセス拒否を通知する（１４１１）。認証スイッチ４００は、認証失敗の情報を認証済み端末登録テーブル４０４に登録しなくてもよい。また、認証サーバ１００は、認証の失敗を端末６００に通知する（１４１２）。端末６００は、認証の失敗の通知を受けると、認証失敗画面を表示する。

【０１７１】

図１５は、第４の実施例の認証処理のフローチャートである。図１５に示す認証処理は、認証サーバ１００のプロセッサが実行する。

【０１７２】

まず、ＨＴＴＰサーバ部１４３は、認証受付のＨＴＴＰリクエストを受信するまで待機する（１４２１）。ＨＴＴＰサーバ部１４３は、受信した認証受付のＨＴＴＰリクエストの応答として、認証情報入力画面を端末６００へ送信する（１４２２）。

【０１７３】

その後、認証処理部１４２は、端末６００から送信された認証要求のＨＴＴＰリクエストを受信するまで待機する（１４２３）。認証処理部１４２は、認証要求を受信すると、認証データベース１４６を参照してユーザ認証を行う。ＨＴＴＰサーバ部１４３は、受信した認証要求に含まれるユーザＩＤ及びパスワードが認証データベース１４６に登録されているユーザＩＤ及びパスワードと同一であれば認証成功と判定する（１４２４）。

【０１７４】

その後、ＲＡＤＩＵＳサーバ部１４４は、認証要求を送信した端末６００のＩＰアドレ

スを用いて認証待ち端末登録テーブル１４７を検索し、当該ＩＰアドレスに対応するＲＡＤＩＵＳアクセス要求パケットデータを認証待ち端末登録テーブル１４７から取得する（１４２５）。

【０１７５】

そして、ステップ１４２４で行われた認証が成功であれば（１４２６でＹ）、ＲＡＤＩＵＳサーバ部１４４は、取得したＲＡＤＩＵＳアクセス要求パケットデータに対応するＲＡＤＩＵＳアクセス許可を応答する（１４２７）。その後、ＨＴＴＰサーバ部１４３は、認証成功画面を含むＨＴＴＰレスポンスを端末６００に送信する（１４２８）。さらに、ＲＡＤＩＵＳサーバ部１４４は、認証待ち端末登録テーブル１４７から、認証済みの端末６００のエントリを削除する（１４２９）。

【０１７６】

一方、ステップ１４２４で行われた認証が失敗であれば（１４２６でＮ）、ＲＡＤＩＵＳサーバ部１４４は、取得したＲＡＤＩＵＳアクセス要求パケットデータに対応するＲＡＤＩＵＳアクセス拒否を応答する（１４３０）。その後、ＨＴＴＰサーバ部１４３は、認証失敗画面を含むＨＴＴＰレスポンスを端末６００に送信する（１４３１）。さらに、ＲＡＤＩＵＳサーバ部１４４は、認証待ち端末登録テーブル１４７から、認証が失敗した端末６００のエントリを削除する（１４２９）。

【０１７７】

その後、ステップ１４２１に戻り、ＨＴＴＰサーバ部１４３が、認証受付のＨＴＴＰリクエストを受信するまで待機する。

【０１７８】

以上に説明したように、第４の実施例では、ＭＡＣ認証を行うＲＡＤＩＵＳ認証システムにおいても、認証サーバ１００による認証の結果を認証済み端末登録テーブル４０４に登録することができる。さらに、認証スイッチ４００は、登録された端末６００をネットワーク認証された端末として管理することができる。

【０１７９】

以上、本発明を添付の図面を参照して詳細に説明したが、本発明はこのような具体的構成に限定されるものではなく、添付した請求の範囲の趣旨内における様々な変更及び同等の構成を含むものである。

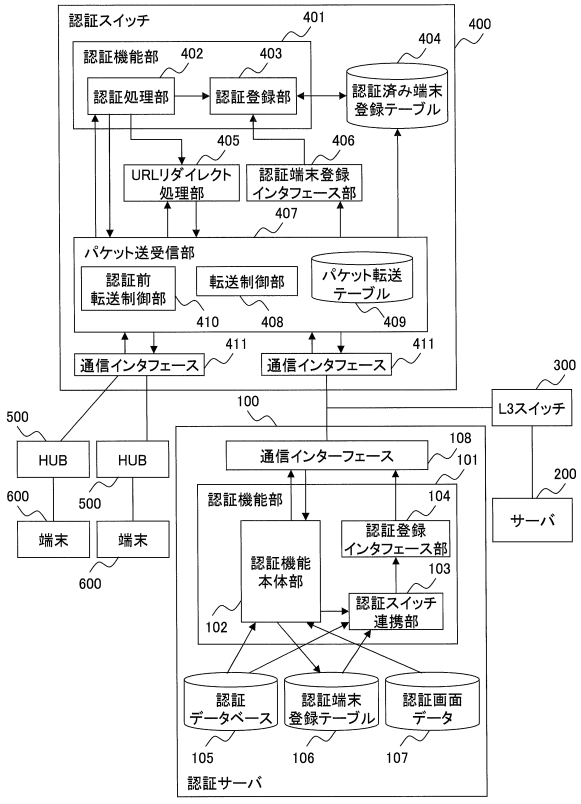
【符号の説明】

【０１８０】

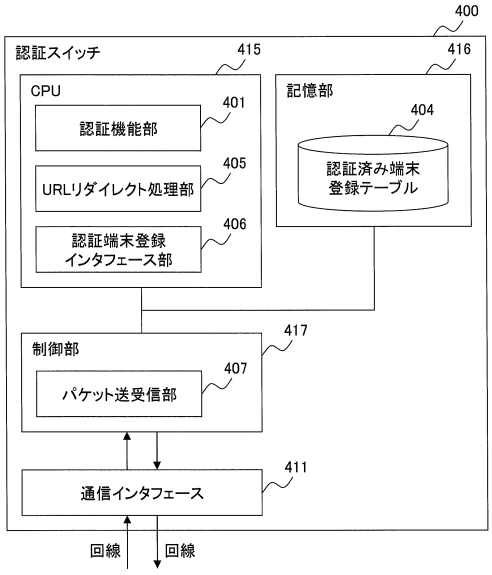
１００　認証サーバ
１０１　認証機能部
１０２　認証機能本体部
１０３　認証スイッチ連携部
１０４　認証登録インタフェース
１０５　認証データベース
１０６　認証端末登録テーブル
１０７　認証画面データ
１０８　通信インタフェース
１２１　トンネリング処理部
１２２　トンネル判定部
１４１　プロセッサ（ＣＰＵ）
１４５　記憶装置
１４８　通信インタフェース
１４２　認証処理部
１４３　ＨＴＴＰサーバ部
１４４　ＲＡＤＩＵＳサーバ部
１４６　認証データベース
１４７　認証待ち端末登録テーブル

１４８　通信インタフェース
２００　サーバ
３００　Ｌ３スイッチ
４００　認証スイッチ
４０１　認証機能部
４０２　認証処理部
４０３　認証登録部
４０４　認証済み端末登録テーブル
４０５　ＵＲＬリダイレクト処理部
４０６　認証端末登録インタフェース部
４０７　パケット送受信部
４０８　転送制御部
４０９　パケット転送テーブル
４１０　認証前転送制御部
４１１　通信インタフェース
４１５　プロセッサ
４１６　記憶部
４１７　制御部
４２１　トンネリング処理部
４２２　トンネル判定部
５００　ＨＵＢ
６００　端末

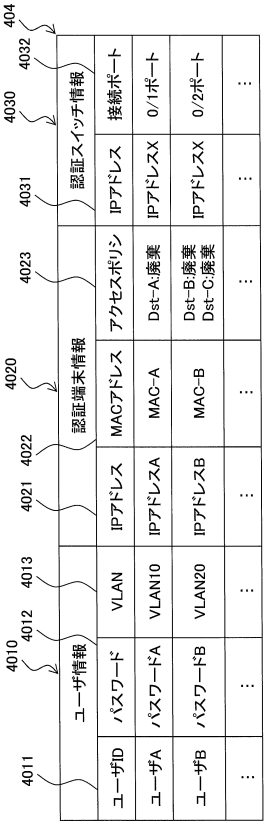
【図１】



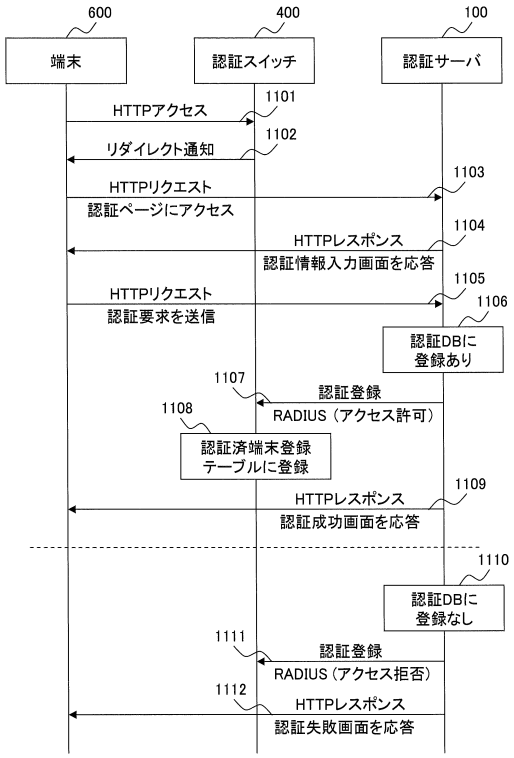
【図２】



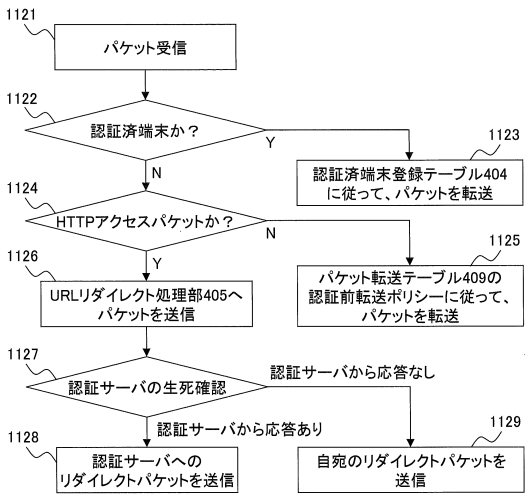
【図３】


404
4032
4030
4031
4023
4020
4022
4021
4013
4012
4010
4011
認証スイッチ情報
認証端末情報
ユーザ情報
接続ポート
IPアドレス
アクセスポリシ
MACアドレス
IPアドレス
VLAN
パスワード
ユーザID
0/1ポート
IPアドレスX
Dst-A:廃棄
MAC-A
IPアドレスA
VLAN10
パスワードA
ユーザA
0/2ポート
IPアドレスX
Dst-B:廃棄
Dst-C:廃棄
MAC-B
IPアドレスB
VLAN20
パスワードB
ユーザB
…

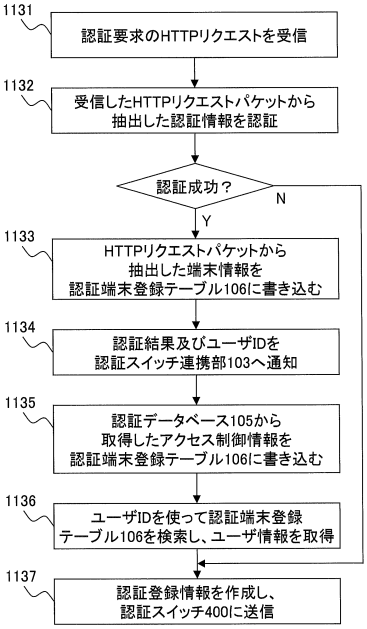
【図４】


600
端末
400
認証スイッチ
100
認証サーバ
1101
HTTPアクセス
1102
リダイレクト通知
1103
HTTPリクエスト
認証ページにアクセス
1104
HTTPレスポンス
認証情報入力画面を応答
1105
HTTPリクエスト
認証要求を送信
1106
認証DBに
登録あり
1107
認証登録
RADIUS（アクセス許可）
1108
認証済端末登録
テーブルに登録
1109
HTTPレスポンス
認証成功画面を応答
1110
認証DBに
登録なし
1111
認証登録
RADIUS（アクセス拒否）
1112
HTTPレスポンス
認証失敗画面を応答

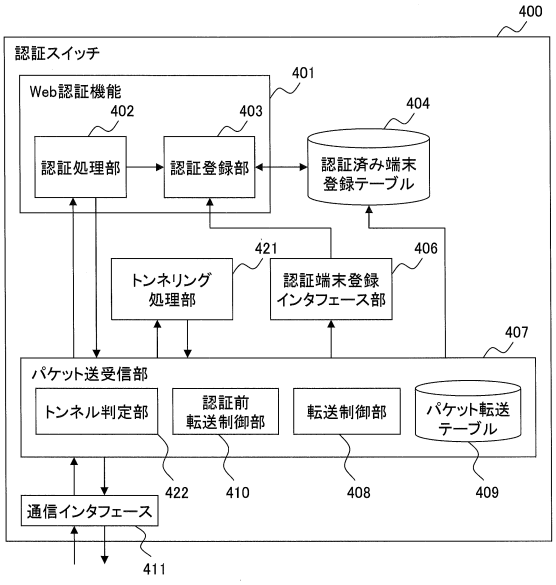
【図５】


1121
パケット受信
1122
認証済端末か？
Y
N
1123
認証済端末登録テーブル404
に従って、パケットを転送
1124
HTTPアクセスパケットか？
N
Y
1125
パケット転送テーブル409の
認証前転送ポリシーに従って、
パケットを転送
1126
URLリダイレクト処理部405へ
パケットを送信
1127
認証サーバの生死確認
認証サーバから応答なし
認証サーバから応答あり
1128
認証サーバへの
リダイレクトパケットを送信
1129
自宛のリダイレクトパケットを
送信

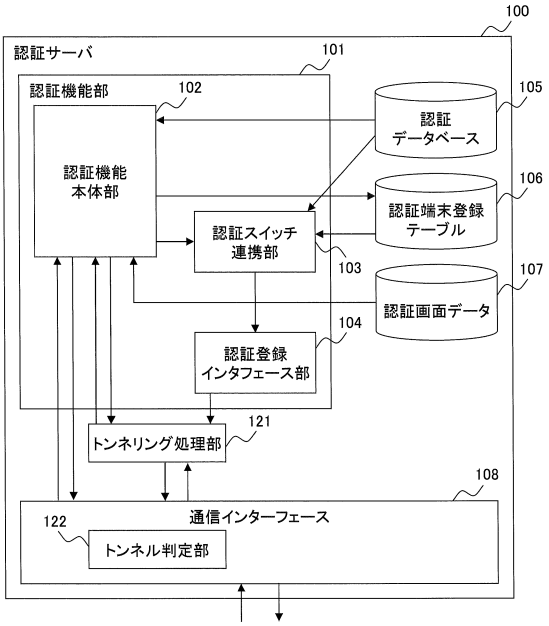
【図６】


1131
認証要求のHTTPリクエストを受信
1132
受信したHTTPリクエストパケットから
抽出した認証情報を認証
認証成功？
N
Y
1133
HTTPリクエストパケットから
抽出した端末情報を
認証端末登録テーブル106に書き込む
1134
認証結果及びユーザIDを
認証スイッチ連携部103へ通知
1135
認証データベース105から
取得したアクセス制御情報を
認証端末登録テーブル106に書き込む
1136
ユーザIDを使って認証端末登録
テーブル106を検索し、ユーザ情報を取得
1137
認証登録情報を作成し、
認証スイッチ400に送信

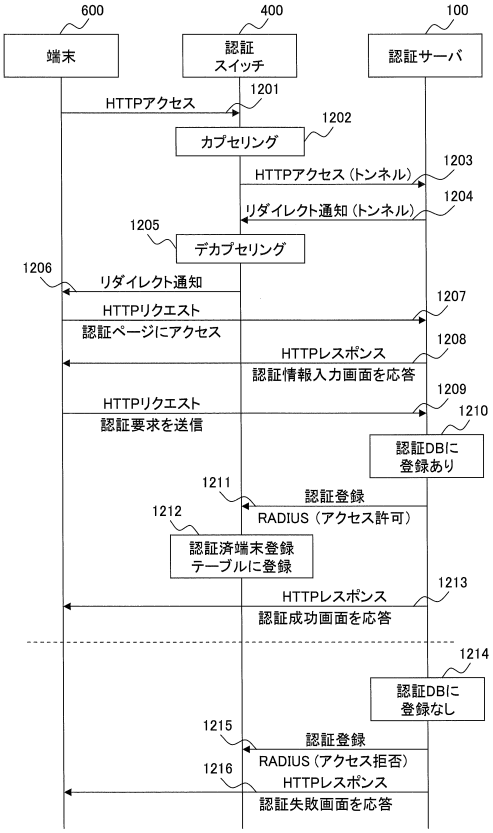
【図７】


400
認証スイッチ
Web認証機能
401
402
403
404
認証処理部
認証登録部
認証済み端末
登録テーブル
421
406
トンネリング
処理部
認証端末登録
インタフェース部
407
パケット送受信部
トンネル判定部
認証前
転送制御部
転送制御部
パケット転送
テーブル
422
410
408
409
通信インタフェース
411

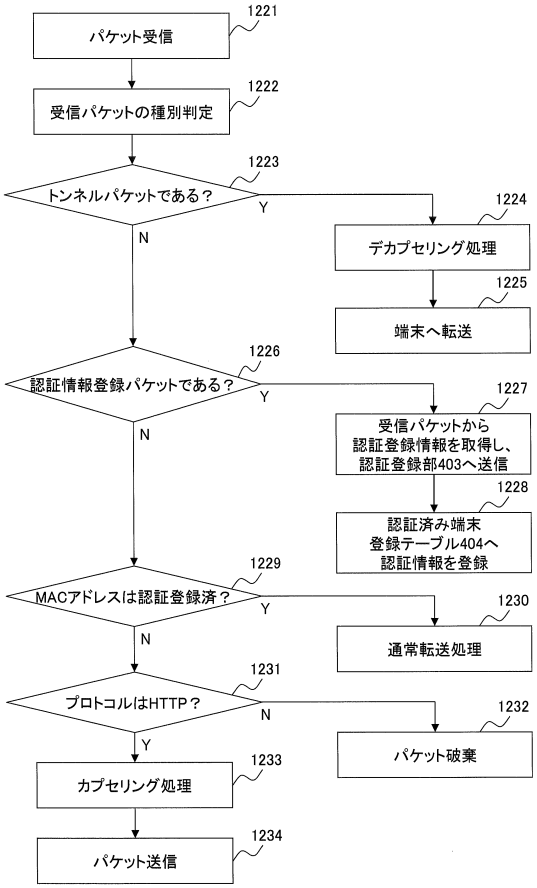
【図８】


100
認証サーバ
101
認証機能部
102
105
認証
データベース
認証機能
本体部
106
認証端末登録
テーブル
認証スイッチ
連携部
103
107
認証画面データ
104
認証登録
インタフェース部
121
トンネリング処理部
108
通信インターフェース
122
トンネル判定部

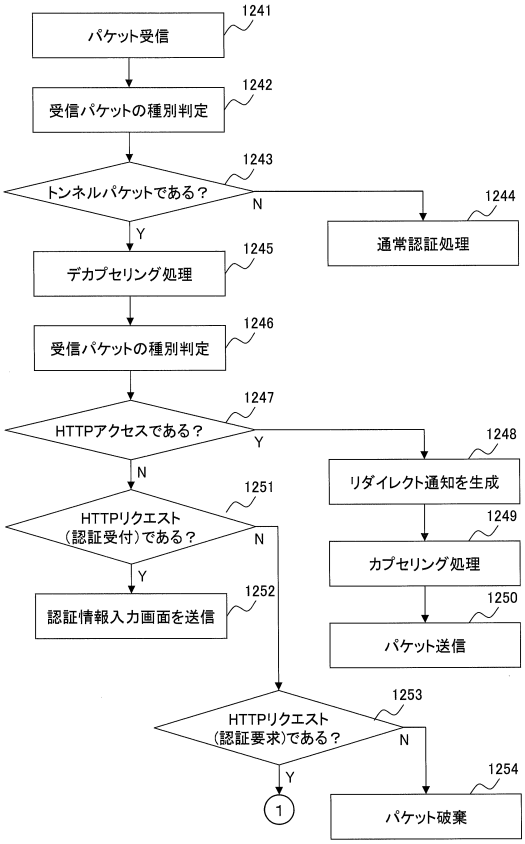
【図９】


600
400
100
端末
認証
スイッチ
認証サーバ
1201
HTTPアクセス
1202
カプセリング
1203
HTTPアクセス（トンネル）
1204
リダイレクト通知（トンネル）
1205
デカプセリング
1206
リダイレクト通知
1207
HTTPリクエスト
認証ページにアクセス
1208
HTTPレスポンス
認証情報入力画面を応答
1209
HTTPリクエスト
認証要求を送信
1210
認証DBに
登録あり
1211
認証登録
RADIUS（アクセス許可）
1212
認証済端末登録
テーブルに登録
1213
HTTPレスポンス
認証成功画面を応答
1214
認証DBに
登録なし
1215
認証登録
RADIUS（アクセス拒否）
1216
HTTPレスポンス
認証失敗画面を応答

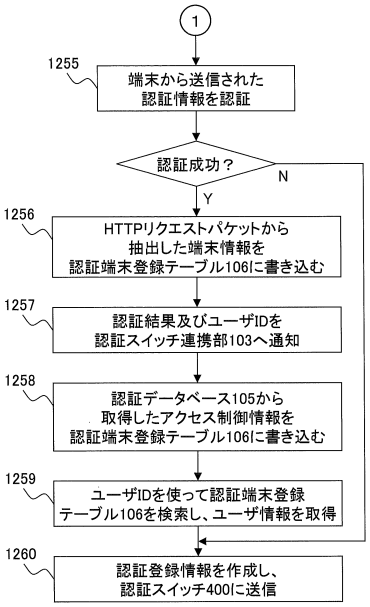
【図１０】


1221
パケット受信
1222
受信パケットの種別判定
1223
トンネルパケットである？
Y
N
1224
デカプセリング処理
1225
端末へ転送
1226
認証情報登録パケットである？
Y
N
1227
受信パケットから
認証登録情報を取得し、
認証登録部403へ送信
1228
認証済み端末
登録テーブル404へ
認証情報を登録
1229
MACアドレスは認証登録済？
Y
N
1230
通常転送処理
1231
プロトコルはHTTP？
N
Y
1232
パケット破棄
1233
カプセリング処理
1234
パケット送信

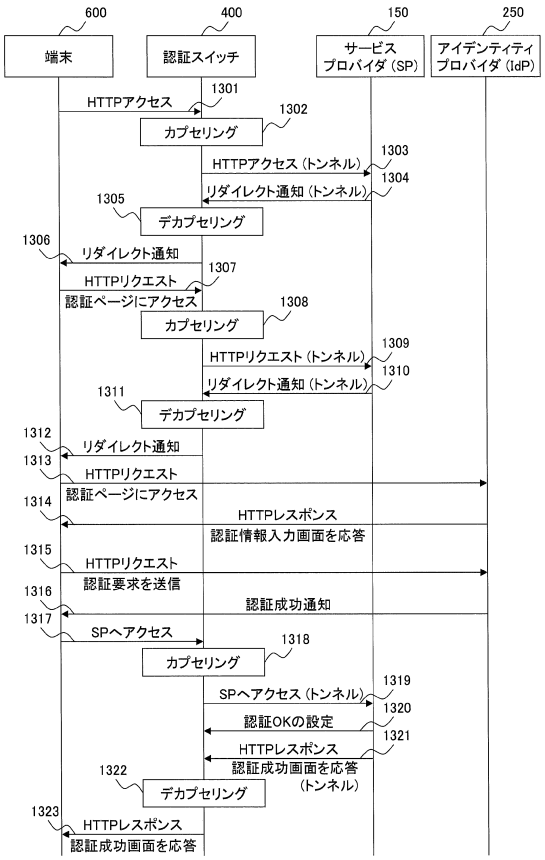
【図１１Ａ】



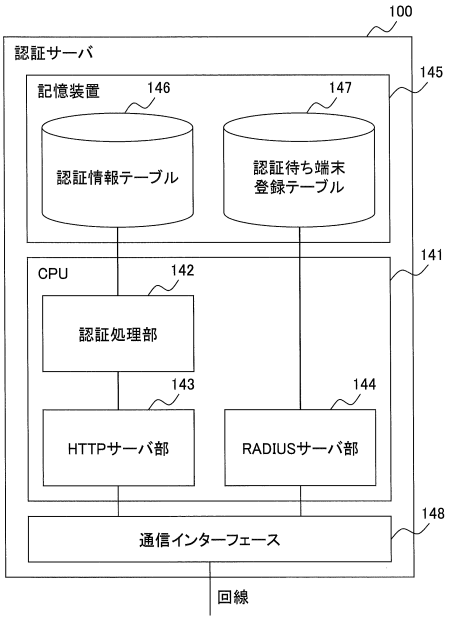
【図１１Ｂ】



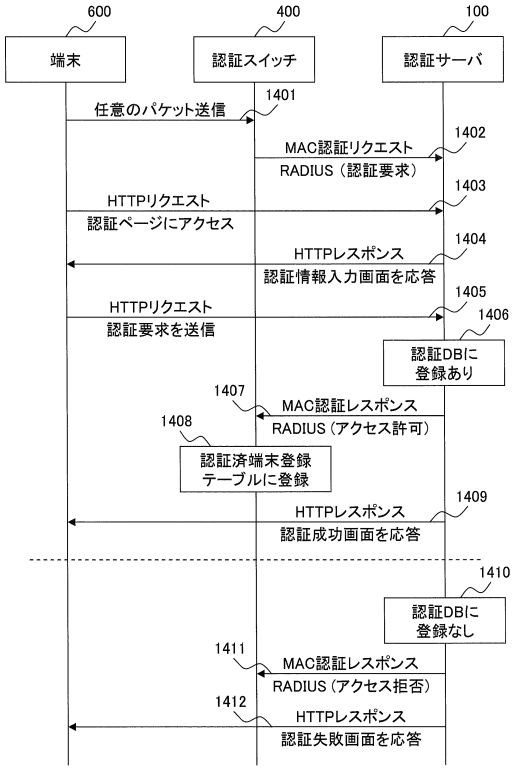
【図１２】



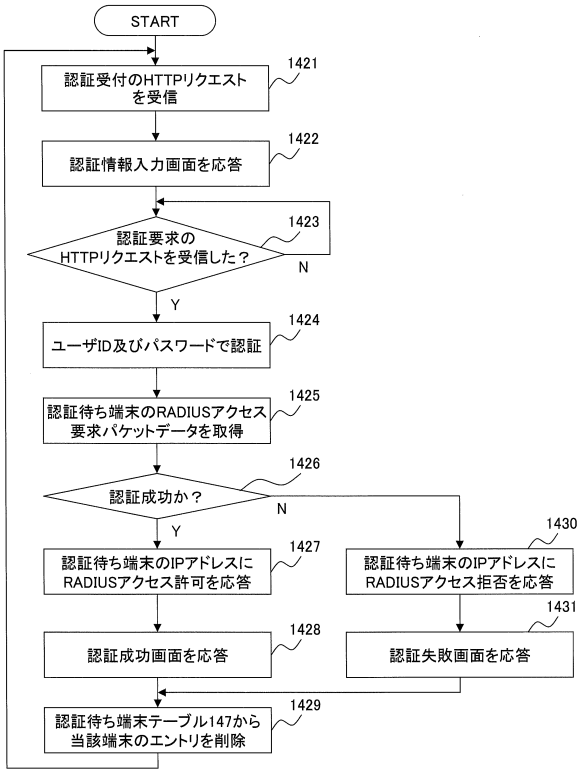
【図１３】



【図１４】


600
400
100
端末
認証スイッチ
認証サーバ
1401
任意のパケット送信
1402
MAC認証リクエスト
RADIUS（認証要求）
1403
HTTPリクエスト
認証ページにアクセス
1404
HTTPレスポンス
認証情報入力画面を応答
1405
HTTPリクエスト
認証要求を送信
1406
認証DBに
登録あり
1407
MAC認証レスポンス
RADIUS（アクセス許可）
1408
認証済端末登録
テーブルに登録
1409
HTTPレスポンス
認証成功画面を応答
1410
認証DBに
登録なし
1411
MAC認証レスポンス
RADIUS（アクセス拒否）
1412
HTTPレスポンス
認証失敗画面を応答

【図１５】


START
1421
認証受付のHTTPリクエスト
を受信
1422
認証情報入力画面を応答
1423
認証要求の
HTTPリクエストを受信した？
N
Y
1424
ユーザID及びパスワードで認証
1425
認証待ち端末のRADIUSアクセス
要求パケットデータを取得
1426
認証成功か？
N
Y
1427
認証待ち端末のIPアドレスに
RADIUSアクセス許可を応答
1428
認証成功画面を応答
1430
認証待ち端末のIPアドレスに
RADIUSアクセス拒否を応答
1431
認証失敗画面を応答
1429
認証待ち端末テーブル147から
当該端末のエントリを削除

フロントページの続き

審査官　宮島　郁美

(56)参考文献　特開２０１２－０８０４１８（ＪＰ，Ａ）
特開２０１１－１３０４０７（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１４５９０２（ＵＳ，Ａ１）
特開２０１０－０６２６６７（ＪＰ，Ａ）
特開２００６－０３３２０６（ＪＰ，Ａ）
特表２０１２－５０５４３６（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１８８５０８（ＵＳ，Ａ１）
特開２００４－１３４８５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２８，１２／４４－１２／９５５
Ｇ０６Ｆ２１／００，２１／３０－２１／４６