(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4291213号
(P4291213)
(45)発行日　平成21年7月8日(2009.7.8)　(24)登録日　平成21年4月10日(2009.4.10)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
H04L 9/32 (2006.01)　　G06F 15/00 330A
　　H04L 9/00 673A
　　H04L 9/00 673B

請求項の数 15　(全 27 頁)

(21)出願番号　特願2004-155673 (P2004-155673)
(22)出願日　平成16年5月26日 (2004.5.26)
(65)公開番号　特開2005-339093 (P2005-339093A)
(43)公開日　平成17年12月8日 (2005.12.8)
審査請求日　平成17年6月30日 (2005.6.30)

(73)特許権者　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　100083552
弁理士　秋田　収喜
(74)代理人　100103746
弁理士　近野　恵一
(72)発明者　沖野　修
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　尾尻　健
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

最終頁に続く

(54)【発明の名称】認証方法、認証システム、認証代行サーバ、ネットワークアクセス認証サーバ、プログラム、及び記録媒体

(57)【特許請求の範囲】
【請求項１】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、
前記認証代行サーバが、前記サービスサーバから前記ユーザ端末を経由して認証要求を受けるステップと、
前記認証代行サーバが、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、
前記ネットワークアクセス認証サーバが、前記認証代行サーバからの依頼を受けて、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と、前記認証代行サーバからの依頼におけるキーであるＩＰアドレスに対応するネットワークユーザＩＤまたは前記認証代行サーバからの依頼におけるキーであるネットワークユーザＩＤに対応するＩＰアドレスを、前記認証代行サーバに対して送るステップと、
前記認証代行サーバが、前記ネットワークアクセス認証サーバから受けた認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記

ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送るステップと、
を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする認証方法。
【請求項２】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、
ユーザによる前記ユーザ端末からのサービス要求に対して前記サービスサーバが前記ユーザの認証を確認できた場合には前記ユーザに対してサービスを提供するステップと、
前記ユーザの認証が確認できない場合には前記サービスサーバから前記ユーザ端末にリダイレクト先アドレスを含んだ認証要求を送るステップと、
前記ユーザ端末から前記認証代行サーバに発ＩＰアドレスを含んだ認証要求を送るステップと、
前記認証代行サーバが前記ユーザを確認したときには認証結果情報を生成して前記ユーザ端末へ該認証結果情報とリダイヤル先アドレスを含んだ認証応答を送るステップと、
前記ユーザ端末から前記サービスサーバへ該認証結果情報を含んだ認証応答を送るステップと、
前記サービスサーバで該認証結果情報を検証するステップと、
該認証結果情報が無効の場合には前記ユーザへサービス提供不可を通知するステップと、
該認証結果情報が有効の場合には前記サービスサーバが前記ユーザに対してサービスを提供するステップと、
前記認証代行サーバが前記ユーザを未確認のときに前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、ネットワークアクセス認証サーバに対して、該ＩＰアドレスをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、
前記ネットワークアクセス認証サーバが該ＩＰアドレスに対応する、前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをネットワークアクセスセッション情報管理テーブルより検索するステップと、
対応するネットワークユーザＩＤを取得できたときに、前記ネットワークアクセス認証サーバから前記認証代行サーバへ、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と該ネットワークユーザＩＤとを送るステップと、
前記認証代行サーバが、取得した該ネットワークユーザＩＤに対応する、前記認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤをユーザ管理テーブルより検索するステップと、
取得した該ＩＤＰユーザＩＤと前記ユーザ端末と前記認証代行サーバ間での認証時に取得した該ＩＤＰユーザＩＤを比較するステップと、
前記比較により、両者が一致したときに、前記ユーザ端末に対して、認証結果情報を含んだ認証応答を送るステップと、
前記ユーザ端末から前記サービスサーバに該認証結果情報を含んだ認証応答を送るステップと、
を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする認証方法。
【請求項３】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提

供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、
ユーザによる前記ユーザ端末からのサービス要求に対して前記サービスサーバが前記ユーザの認証を確認できた場合には前記ユーザに対してサービスを提供するステップと、
前記ユーザの認証が確認できない場合には前記サービスサーバから前記ユーザ端末にリダイレクト先アドレスを含んだ認証要求を送るステップと、
前記ユーザ端末から前記認証代行サーバに発ＩＰアドレスを含んだ認証要求を送るステップと、
前記認証代行サーバが前記ユーザを確認したときには認証結果情報を生成して前記ユーザ端末へ該認証結果情報とリダイヤル先アドレスを含んだ認証応答を送るステップと、
前記ユーザ端末から前記サービスサーバへ該認証結果情報を含んだ認証応答を送るステップと、
前記サービスサーバで該認証結果情報を検証するステップと、
該認証結果情報が無効の場合には前記ユーザへサービス提供不可を通知するステップと、
該認証結果情報が有効の場合には前記サービスサーバが前記ユーザに対してサービスを提供するステップと、
前記認証代行サーバが前記ユーザを未確認のときに、前記認証代行サーバが認証時に取得したＩＤＰユーザＩＤに対応するネットワークユーザＩＤをＩＤＰユーザ管理テーブルより検索するステップと、
該ネットワークユーザＩＤを取得したときに、前記ネットワークアクセス認証サーバへ該ネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、
前記ネットワークアクセス認証サーバが該ネットワークユーザＩＤに対応するＩＰアドレスをネットワークアクセスセッション情報管理テーブルより検索するステップと、
対応するＩＰアドレスを取得したときに、前記ネットワークアクセス認証サーバから前記認証代行サーバへ、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と該ＩＰアドレスを送るステップと、
前記認証代行サーバが、取得したＩＰアドレスと、認証要求での発ＩＰアドレスを比較するステップと、
前記比較により、両者が一致したときに、前記ユーザ端末に対して、認証結果情報を含んだ認証応答を送るステップと、
前記ユーザ端末から前記サービスサーバに該認証結果情報を含んだ認証応答を送るステップと、
を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする認証方法。

【請求項４】
請求項１ないし３のうちいずれか１項に記載の認証方法において、
１つの認証代行サーバの配下に複数のネットワークアクセス認証サーバが接続される認証システムにおける認証方法であって、
前記認証代行サーバが、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記認証代行サーバから前記ネットワークアクセス認証サーバへネットワークアクセス認証状態を確認するときに、前記認証代行サーバが保有する前記ユーザが属するネットワークアクセス認証サーバを識別する識別子により該当するネットワークアクセス認証サーバを特定するステップと、
前記認証代行サーバから前記ネットワークアクセス認証サーバに、ネットワークアクセス認証状態の確認を依頼するステップと、
を有することを特徴とする認証方法。

【請求項５】
請求項４に記載の認証方法において、

前記認証代行サーバから前記ネットワークアクセス認証サーバへアクセスするとき、前記認証代行サーバが前記ユーザ端末のＩＰアドレスから該当する認証サーバを引くテーブルを用意するステップと、

該テーブルを用いてそのＩＰアドレスから該当するネットワークアクセス認証サーバを特定するステップと、

認証処理において、ネットワークアクセスサーバによる認証と認証代行サーバにおける認証とを連携して行う、または、ネットワークアクセスサーバによる認証と認証代行サーバにおける認証とを連携して行う代わりにネットワークアクセス認証単独の認証のみを行うステップと、

を有することを特徴とする認証方法。

【請求項６】

ＩＰアドレスを回線毎に固定的に割り当てるエッジルータと、ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、

前記認証代行サーバが、前記サービスサーバから前記ユーザ端末を経由して認証要求を受けるステップと、

前記認証代行サーバが、前記ユーザ端末と認証代行サーバ間でのＩＤＰ認証において、前記ユーザ端末に対して認証を行うと共に、ＩＤＰユーザＩＤのエントリーごとにユーザアカウント情報として前記認証代行サーバ内に格納してある前記エッジルータが回線毎に固定的に割り当てたＩＰアドレスを利用して発ＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送るステップと、

を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする認証方法。

【請求項７】

ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムであって、

前記認証代行サーバが、

前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、

前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼する手段と、

前記ネットワークアクセス認証サーバから受けた前記認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、

を備え、

前記ネットワークアクセス認証サーバが、前記認証代行サーバからの依頼を受けて、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と、前記認証代行サーバからの依頼におけるキーであるＩＰアドレスに対応するネットワークユーザＩＤまたは前記前記認証代行サーバからの依頼におけるキーであるネットワークユーザＩＤに対応するＩＰアドレスを、前記認証代行サーバに対して送る手段を、

備え、前記サービスサーバでの前記認証応答の検証終了後にサービスが開始されることを特徴とする認証システム。

【請求項８】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、
前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、
前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼する手段と、
前記ネットワークアクセス認証サーバから受けた前記認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、
を備えることを特徴とする認証代行サーバ。
【請求項９】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、
認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤ、ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤを含むユーザアカウントを持つ手段と、
前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバへ、前記ユーザ端末からの認証要求パケットの中の発ＩＰアドレスをキーとして、該ネットワークアクセス認証状態の確認を依頼する手段と、
前記ネットワークアクセス認証サーバより、ネットワークアクセス認証状態を含み認証済みの場合はネットワークユーザＩＤも含むネットワークアクセス認証状態確認結果を受信する手段と、
ネットワークアクセス認証状態が確認できないときにはユーザへサービス提供不可を通知する手段と、
受信により取得したネットワークユーザＩＤに対応するＩＤＰユーザＩＤを前記ユーザアカウントを持つ手段より検索する手段と、
ＩＤＰユーザＩＤが取得できたか否かの判断を行う手段と、
取得できないときは前記ユーザへサービス提供不可を通知する手段と、
取得したＩＤＰユーザＩＤと、前記ユーザ端末と前記認証代行サーバ間での認証時に取得したＩＤＰユーザＩＤとを比較する手段と、
該ＩＤＰユーザＩＤの比較で一致するか否かの判断を行う手段と、
一致しなければユーザへサービス提供不可を通知する手段と、
一致すれば認証結果情報を生成する手段と、
を備えることを特徴とする認証代行サーバ。
【請求項１０】
ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、
認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤ、ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤを含むユーザアカウントを持

つ手段と、
前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記認証時に取得したＩＤＰユーザＩＤに対応するネットワークユーザＩＤを前記ユーザアカウントを持つ手段より検索する手段と、
ネットワークユーザＩＤが取得できたか否かを判断する手段と、
取得できなかった場合にはユーザへサービス提供不可を通知する手段と、
取得できたときには前記認証代行サーバは、前記ネットワークアクセス認証サーバへ、該ネットワークユーザＩＤをキーとして該ネットワークアクセス認証状態の確認を依頼する手段と、
前記認証代行サーバは前記ネットワークアクセス認証サーバより、ネットワーク認証状態を含み認証済みの場合にはＩＰアドレスも含むネットワークアクセス認証状態確認結果を受信する手段と、
ネットワーク認証状態が済みか否かを判断する手段と、
未認証の場合にはユーザへサービス提供不可を通知する手段と、
認証済みの場合には、ネットワークアクセス認証サーバより取得したＩＰアドレスと、認証要求パケットの発ＩＰアドレスとを比較する手段と、
ＩＰアドレスの比較で一致するか否かの判断を行う手段と、
一致しなければユーザへサービス提供不可を通知する手段と、
一致すれば認証結果情報を生成する手段と、
を備えることを特徴とする認証代行サーバ。
【請求項１１】
請求項８ないし１０のうちいずれか１項に記載の認証代行サーバにおいて、
ユーザが属するネットワークアクセス認証サーバを識別する識別子を保有する手段と、
前記識別子により、確認を依頼するネットワークアクセス認証サーバを決定する手段と、
を備えることを特徴とする認証代行サーバ。
【請求項１２】
ＩＰアドレスを回線毎に固定的に割り当てるエッジルータと、ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、
前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、
前記ユーザ端末とのＩＤＰ認証において、前記ユーザ端末に対して認証を行うと共に、ＩＤＰユーザＩＤのエントリーごとにユーザアカウント情報として前記認証代行サーバ内に格納してある前記エッジルータが回線毎に固定的に割り当てたＩＰアドレスを利用して発ＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、
を備えることを特徴とする認証代行サーバ。
【請求項１３】
請求項１ないし６のうちいずれか１項に記載の各ステップをコンピュータに実行させるためのプログラム。
【請求項１４】
請求項７ないし１２のうちのいずれか１項に記載の各手段としてコンピュータを機能させるためのプログラム。
【請求項１５】
請求項１３または１４に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明はユーザ端末がネットワークを介してサービスサーバからサービス提供を受けるネットワーク構成でのシングルサインオン認証技術に関し、特にセキュリティの強化を目的とした認証技術に関するものである。

【背景技術】

【０００２】

仮想閉域網（ＶＰＮ）内において複数のＷｅｂサーバに対して、一度の認証手続きでアクセスを可能とするシングルサインオン技術が存在する。

【０００３】

（１）このシングルサインオン技術には、リバース・プロキシ型とエージェント・モジュール型があり、前者はＷｅｂサーバ宛のアクセストラヒックを全て専用のシングルサインオンサーバで受け、ユーザ毎に規定されたアクセスリストに照らし合わせて、パケット転送の可否を取捨選択する方法であり、シングルサインオンサーバへの処理負荷の集中の点で、大規模な網への適用には不向きである。後者は各Ｗｅｂサーバでユーザ認証の認証状態を判断して、未認証の場合にはユーザからのアクセス要求をシングルサインオンサーバへ転送して、認証を受けさせるものである。認証が成功すると証明書が発行され、各Ｗｅｂサーバは受信したアクセス要求の中の証明書が添付されていることをもって、そのユーザが認証済みであることを判断してアクセスが許可される。以上述べた動作は、Ｗｅｂサーバが設備されているネットワークにユーザ端末が既に接続されていることを前提にしており、ＶＰＮに遠隔から接続するときの様に、ＶＰＮへの接続自体に認証が求められる場合には、ユーザは２度の手続きが必要となり、パケット管理が複雑化する問題がある。

【０００４】

（２）リモートアクセスユーザの端末から、電話網、インターネット経由でＶＰＮに接続してＶＰＮ内のＷｅｂサーバにアクセスする場合のシングルサインオン技術の実施例は、非特許文献１にあるので、それを図１３により説明する。リモートアクセスユーザの端末からの認証に必要な情報、例えばＩＤとパスワードは、リモートアクセスサーバ（ＲＡＳ）あるいはＩＰｓｅｃ（Security Architecture for the Internet Protocol）ゲートウェイを経由して、ネットワークアクセス認証サーバに送られる。該ネットワークアクセス認証サーバでは内部に保持するユーザ認証用情報に照らして、ユーザ認証を行い、接続要求を行った端末に対してはＶＰＮ接続用のＩＰアドレスを払い出し、ネットワーク認証状態テーブルで管理する。次に該ユーザがＶＰＮ内のあるＷｅｂサーバ（サービスサーバ）にアクセスを試みると、その時点では該端末が証明書を保持していないため、該端末からのアクセス要求はＷｅｂサーバ（サービスサーバ）により認証代行サーバにリダイレクトされる。該認証代行サーバでは、端末から送信された認証要求パケットから送信元ＩＰアドレスを抽出し、ネットワークアクセス認証サーバに送信する。ネットワークアクセス認証サーバではネットワーク認証状態テーブルを参照し、受信したＩＰアドレスが先にＶＰＮ接続の認証時に払い出したＩＰアドレスであるかを検索し、結果を認証代行サーバに送る。認証代行サーバでは、先に送ったＩＰアドレスが払い出し済のＩＰアドレスに該当していた場合には、証明書を発行する。以上によりユーザは、ＶＰＮ接続時の一度の認証手続きにより、ＶＰＮ接続とＶＰＮ内Ｗｅｂサーバへのシングルサインオンを実現している。

【０００５】

（３）リモートアクセス拠点にＬＡＮを構成してそれに接続されている端末からＶＰＮにリモートアクセスする場合のシングルサインオン技術を以下に説明する。この場合はユーザルータを介して同時に複数の端末での接続が可能であり、（２）で述べた接続形態を当てはめると、ネットワークアクセス認証サーバから付与されるのはユーザルータの公衆網側アドレスのみとなり、認証代行サーバに届くアクセス要求パケットの送信元アドレスとなる端末のアドレスは、端末毎に１対１に対応されていないため、（２）と同様の手順では認証状態が判別できない。このための実施例は非特許文献１にあるので、それを図１４により以下に説明する。具体的にはリモートアクセス拠点内にユーザルータとローカル認証サーバを配置し、リモートアクセス拠点内の端末に対するユーザ認証とアドレスの払

い出し結果を、ネットワークアクセス認証サーバに通知することで認証状態を管理する。ここでユーザルータはＬＡＮ内端末へのアドレス払い出しとともに、払い出したアドレスをネットワークアクセス認証サーバに通知する機能を持つ。またローカル認証サーバはユーザルータからの依頼によりＩＤとパスワードでユーザを認証する。以上により、ＬＡＮ内の端末に対してもアドレス情報がネットワークアクセス認証サーバに蓄積されることになり、端末からのＶＰＮ内Ｗｅｂサーバにアクセス要求が行われた場合には、（２）で示したリモートアクセスユーザの端末から、電話網、インターネット経由でＶＰＮに接続してＶＰＮ内のＷｅｂサーバにアクセスする場合と同様の処理により、Ｗｅｂサーバにシングルサインオンが可能となる。

【０００６】

いずれも本発明の目的とする認証連携を記載したものではない。

【０００７】

【非特許文献１】三好潤、石川啓之、「ＩＰ－ＶＰＮにおけるネットワーク連動型シングルサインオン実現方式の検討」、電子情報通信学会、情報ネットワーク研究会、信学技報、ＮＳ２００２－３１３、ＩＮ２００２－２８６、２００２年3月、２７９頁～　２８４頁

【発明の開示】

【発明が解決しようとする課題】

【０００８】

従来の技術では、ネットワークアクセス認証サーバでの認証（ＮＷアクセス認証）が完了していれば、ユーザの端末からサービスサーバにアクセスを試みたとき、サービスサーバで該当ユーザの認証が済んでいればサービスを開始する。反対にサービスサーバで認証が未認証の場合には、認証代行サーバがユーザ端末経由での認証要求を受信し、認証代行サーバでの認証（ＩＤＰ認証）が既に成功あるいは認証が成功すれば、認証代行サーバは認証結果情報（アサーション）を生成してサービスサーバへ認証結果情報の検証を依頼し、サービスサーバでの認証結果情報の検証が済めば、ＮＷアクセス認証の状況に関わらず、サービス提供可能となる。いずれの場合でも、ＮＷアクセス認証、ＩＤＰ認証のいずれかの認証が成功していれば、サービス提供を可能としている。なお、ＮＷはネットワークを意味する。

【０００９】

本発明では、インターネット等のオープンなネットワークを対象に、以下の課題の解決並びにセキュリティをより強固にしたシングルサインオンを実現することを目的とする。

（１）課題：ＮＷユーザＩＤとＩＤＰユーザＩＤが１：１であるため、ホームゲートウェイ内の個人（端末）まで識別した認証（１：ｎ）ができない。

（２）課題：ＮＷユーザＩＤとＩＤＰユーザＩＤが１：１であるため、１ユーザが複数のＮＷユーザＩＤをもつ形態（ｎ：１）に対応できない。

（３）機能向上：ＩＤＰ認証とＮＷアクセス認証を併用して、双方の認証を確認した場合のみ証明書を発行することによりセキュリティをより強固にする。

【課題を解決するための手段】

【００１０】

本発明は上記課題を解決するため、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、

前記認証代行サーバが、前記サービスサーバから前記ユーザ端末を経由して認証要求を受けるステップと、前記認証代行サーバが、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、前記ネットワークアクセス認証サーバが、前記認証代行サ

ーバからの依頼を受けて、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と、前記認証代行サーバからの依頼におけるキーであるＩＰアドレスに対応するネットワークユーザＩＤまたは前記認証代行サーバからの依頼におけるキーであるネットワークユーザＩＤに対応するＩＰアドレスを、前記認証代行サーバに対して送るステップと、前記認証代行サーバが、前記ネットワークアクセス認証サーバから受けた認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送るステップと、を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする。

【００１１】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、ユーザによる前記ユーザ端末からのサービス要求に対して前記サービスサーバが前記ユーザの認証を確認できた場合には前記ユーザに対してサービスを提供するステップと、前記ユーザの認証が確認できない場合には前記サービスサーバから前記ユーザ端末にリダイレクト先アドレスを含んだ認証要求を送るステップと、前記ユーザ端末から前記認証代行サーバに発ＩＰアドレスを含んだ認証要求を送るステップと、前記認証代行サーバが前記ユーザを確認したときには認証結果情報を生成して前記ユーザ端末へ該認証結果情報とリダイヤル先アドレスを含んだ認証応答を送るステップと、前記ユーザ端末から前記サービスサーバへ該認証結果情報を含んだ認証応答を送るステップと、前記サービスサーバで該認証結果情報を検証するステップと、該認証結果情報が無効の場合には前記ユーザへサービス提供不可を通知するステップと、該認証結果情報が有効の場合には前記サービスサーバが前記ユーザに対してサービスを提供するステップと、前記認証代行サーバが前記ユーザを未確認のときに前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、ネットワークアクセス認証サーバに対して、該ＩＰアドレスをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、前記ネットワークアクセス認証サーバが該ＩＰアドレスに対応する、前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをネットワークアクセスセッション情報管理テーブルより検索するステップと、対応するネットワークユーザＩＤを取得できたときに、前記ネットワークアクセス認証サーバから前記認証代行サーバへ、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と該ネットワークユーザＩＤとを送るステップと、前記認証代行サーバが、取得した該ネットワークユーザＩＤに対応する、前記認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤをユーザ管理テーブルより検索するステップと、取得した該ＩＤＰユーザＩＤと前記ユーザ端末と前記認証代行サーバ間での認証時に取得した該ＩＤＰユーザＩＤを比較するステップと、前記比較により、両者が一致したときに、前記ユーザ端末に対して、認証結果情報を含んだ認証応答を送るステップと、前記ユーザ端末から前記サービスサーバに該認証結果情報を含んだ認証応答を送るステップと、を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする。

【００１２】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、ユーザによる前記ユーザ端末からのサービス要求に対して前記サービスサーバが前記ユーザの認証を確認できた場合には前記ユーザに対してサービスを提供するステップと、前記ユーザの認証が確認できない場

合には前記サービスサーバから前記ユーザ端末にリダイレクト先アドレスを含んだ認証要求を送るステップと、前記ユーザ端末から前記認証代行サーバに発ＩＰアドレスを含んだ認証要求を送るステップと、前記認証代行サーバが前記ユーザを確認したときには認証結果情報を生成して前記ユーザ端末へ該認証結果情報とリダイヤル先アドレスを含んだ認証応答を送るステップと、前記ユーザ端末から前記サービスサーバへ該認証結果情報を含んだ認証応答を送るステップと、前記サービスサーバで該認証結果情報を検証するステップと、該認証結果情報が無効の場合には前記ユーザへサービス提供不可を通知するステップと、該認証結果情報が有効の場合には前記サービスサーバが前記ユーザに対してサービスを提供するステップと、前記認証代行サーバが前記ユーザを未確認のときに、前記認証代行サーバが認証時に取得したＩＤＰユーザＩＤに対応するネットワークユーザＩＤをＩＤＰユーザ管理テーブルより検索するステップと、該ネットワークユーザＩＤを取得したときに、前記ネットワークアクセス認証サーバへ該ネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼するステップと、前記ネットワークアクセス認証サーバが該ネットワークユーザＩＤに対応するＩＰアドレスをネットワークアクセスセッション情報管理テーブルより検索するステップと、対応するＩＰアドレスを取得したときに、前記ネットワークアクセス認証サーバから前記認証代行サーバへ、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と該ＩＰアドレスを送るステップと、前記認証代行サーバが、取得したＩＰアドレスと、認証要求での発ＩＰアドレスを比較するステップと、前記比較により、両者が一致したときに、前記ユーザ端末に対して、認証結果情報を含んだ認証応答を送るステップと、前記ユーザ端末から前記サービスサーバに該認証結果情報を含んだ認証応答を送るステップと、有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする。

【００１３】

また、前記認証方法において、１つの認証代行サーバの配下に複数のネットワークアクセス認証サーバが接続される認証システムにおける認証方法であって、前記認証代行サーバが、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記認証代行サーバから前記ネットワークアクセス認証サーバへネットワークアクセス認証状態を確認するときに、前記認証代行サーバが保有する前記ユーザが属するネットワークアクセス認証サーバを識別する識別子により該当するネットワークアクセス認証サーバを特定するステップと、前記認証代行サーバから前記ネットワークアクセス認証サーバに、ネットワークアクセス認証状態の確認を依頼するステップと、を有することを特徴とする。

【００１４】

また、前記認証方法において、前記認証代行サーバから前記ネットワークアクセス認証サーバへアクセスするとき、前記認証代行サーバが前記ユーザ端末のＩＰアドレスから該当する認証サーバを引くテーブルを用意するステップと、該テーブルを用いてそのＩＰアドレスから該当するネットワークアクセス認証サーバを特定するステップと、認証処理において、ネットワークアクセスサーバによる認証と認証代行サーバにおける認証とを連携して行う、または、ネットワークアクセスサーバによる認証と認証代行サーバにおける認証とを連携して行う代わりにネットワークアクセス認証単独の認証のみを行うステップと、を有することを特徴とする。

【００１５】

また、ＩＰアドレスを回線毎に固定的に割り当てるエッジルータと、ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証方法であって、前記認証代行サーバが、前記サービスサーバから前記ユーザ端末を経由して認証要求を受けるステップと、前記認証代行サーバが、前記ユーザ端末と認証代行サーバ間でのＩＤＰ認証において、前記ユーザ端末に対して認証を行うと共に、ＩＤＰユーザＩＤのエントリーごとにユーザアカウント情報として前記認証代行サーバ内に格納してある前記エッジルータが回線毎に固定的に割り当てたＩＰアドレスを利用して発ＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユ

ーザ端末を経由して前記サービスサーバに送るステップと、を有し、前記サービスサーバでの該認証応答の検証終了後にサービスが開始されることを特徴とする。

【００１６】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムであって、前記認証代行サーバが、前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼する手段と、前記ネットワークアクセス認証サーバから受けた前記認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、を備え、前記ネットワークアクセス認証サーバが、前記認証代行サーバからの依頼を受けて、ネットワークアクセス認証サーバにおける認証状態を示す認証状態情報と、前記認証代行サーバからの依頼におけるキーであるＩＰアドレスに対応するネットワークユーザＩＤまたは前記前記認証代行サーバからの依頼におけるキーであるネットワークユーザＩＤに対応するＩＰアドレスを、前記認証代行サーバに対して送る手段を、備え、前記サービスサーバでの前記認証応答の検証終了後にサービスが開始されることを特徴とする。

【００１７】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバに対して、前記ユーザ端末のＩＰアドレスまたは前記ユーザ端末のユーザの前記ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤをキーとしてネットワークアクセス認証状態の確認を依頼する手段と、前記ネットワークアクセス認証サーバから受けた前記認証状態情報と前記ネットワークアクセス認証サーバにＩＰアドレスをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたネットワークユーザＩＤまたは前記ネットワークアクセス認証サーバにネットワークユーザＩＤをキーとして確認を依頼して前記ネットワークアクセス認証サーバから受けたＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、を備えることを特徴とする。

【００１８】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤ、ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤを含むユーザアカウントを持つ手段と、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記ネットワークアクセス認証サーバへ、前記ユーザ端末からの認証要求パケットの中の発ＩＰアドレスをキーとして、該ネットワークアクセス認証状態の確認を依頼する手段と、前記ネットワークアクセス認証サーバ

より、ネットワークアクセス認証状態を含み認証済みの場合はネットワークユーザＩＤも含むネットワークアクセス認証状態確認結果を受信する手段と、ネットワークアクセス認証状態が確認できないときにはユーザへサービス提供不可を通知する手段と、受信により取得したネットワークユーザＩＤに対応するＩＤＰユーザＩＤを前記ユーザアカウントを持つ手段より検索する手段と、ＩＤＰユーザＩＤが取得できたか否かの判断を行う手段と、取得できないときは前記ユーザへサービス提供不可を通知する手段と、取得したＩＤＰユーザＩＤと、前記ユーザ端末と前記認証代行サーバ間での認証時に取得したＩＤＰユーザＩＤとを比較する手段と、該ＩＤＰユーザＩＤの比較で一致するか否かの判断を行う手段と、一致しなければユーザへサービス提供不可を通知する手段と、一致すれば認証結果情報を生成する手段と、を備えることを特徴とする。

【００１９】

また、ユーザ端末のネットワークアクセスを認証するネットワークアクセス認証サーバと、前記ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤ、ネットワークアクセス認証サーバにおけるユーザＩＤであるネットワークユーザＩＤを含むユーザアカウントを持つ手段と、前記ユーザ端末と前記認証代行サーバ間での認証処理終了後に、前記認証時に取得したＩＤＰユーザＩＤに対応するネットワークユーザＩＤを前記ユーザアカウントを持つ手段より検索する手段と、ネットワークユーザＩＤが取得できたか否かを判断する手段と、取得できなかった場合にはユーザへサービス提供不可を通知する手段と、取得できたときには前記認証代行サーバは、前記ネットワークアクセス認証サーバへ、該ネットワークユーザＩＤをキーとして該ネットワークアクセス認証状態の確認を依頼する手段と、前記認証代行サーバは前記ネットワークアクセス認証サーバより、ネットワーク認証状態を含み認証済みの場合にはＩＰアドレスも含むネットワークアクセス認証状態確認結果を受信する手段と、ネットワーク認証状態が済みか否かを判断する手段と、未認証の場合にはユーザへサービス提供不可を通知する手段と、認証済みの場合には、ネットワークアクセス認証サーバより取得したＩＰアドレスと、認証要求パケットの発ＩＰアドレスとを比較する手段と、ＩＰアドレスの比較で一致するか否かの判断を行う手段と、一致しなければユーザへサービス提供不可を通知する手段と、一致すれば認証結果情報を生成する手段と、を備えることを特徴とする。

【００２０】

また、前記認証代行サーバにおいて、ユーザが属するネットワークアクセス認証サーバを識別する識別子を保有する手段と、前記識別子により、確認を依頼するネットワークアクセス認証サーバを決定する手段と、を備えることを特徴とする。

【００２１】

また、ＩＰアドレスを回線毎に固定的に割り当てるエッジルータと、ユーザ端末にサービスを提供するサービスサーバと、前記サービスサーバのサービス提供のために前記ユーザ端末の認証を代行する認証代行サーバをネットワークを介して接続してなる認証システムにおける認証代行サーバであって、前記サービスサーバから前記ユーザ端末を経由して認証要求を受ける手段と、前記ユーザ端末とのＩＤＰ認証において、前記ユーザ端末に対して認証を行うと共に、ＩＤＰユーザＩＤのエントリーごとにユーザアカウント情報として前記認証代行サーバ内に格納してある前記エッジルータが回線毎に固定的に割り当てたＩＰアドレスを利用して発ＩＰアドレスの検証を行い、有効ならば、認証結果情報を含んだ認証応答を、前記ユーザ端末を経由して前記サービスサーバに送る手段と、を備えることを特徴とする。

【００２２】

また、前記認証代行サーバからＩＰアドレスまたはネットワークユーザＩＤをキーとして、ネットワークアクセス認証状態の確認の依頼を受けるネットワークアクセス認証サーバであって、前記認証代行サーバからの依頼を受けて、ネットワークアクセス認証サーバ

における認証状態情報と、前記ＩＰアドレスまたは前記ネットワークユーザＩＤに対応するネットワークユーザＩＤまたはＩＰアドレスを、前記認証代行サーバに対して送る手段と、を備えることを特徴とする。

【００２３】

また、前記認証代行サーバからＩＰアドレスをキーとして、ネットワークアクセス認証状態の確認の依頼を受けるネットワークアクセス認証サーバであって、ＩＰアドレスをキーとしたネットワークアクセス認証状態の確認依頼を受信する手段と、該ＩＰアドレスに対応するネットワークユーザＩＤをネットワークアクセスセッション情報管理テーブルから検索する手段と、対応するネットワークユーザＩＤが取得できたか否かを判断する手段と、取得できなかった場合には前記認証代行サーバへネットワークアクセス認証状態結果（認証不成功）を返信する手段と、取得できた場合には前記ネットワークアクセス認証サーバから認証代行サーバへ、ネットワークアクセス認証状態確認結果（認証状態が認証済み、ネットワークユーザＩＤ）を送る手段と、を備えることを特徴とする。

【００２４】

また、前記認証代行サーバからネットワークユーザＩＤをキーとして、ネットワークアクセス認証状態の確認の依頼を受けるネットワークアクセス認証サーバであって、ネットワークユーザＩＤをキーとしたネットワークアクセス認証状態の確認依頼を受信する手段と、ネットワークユーザＩＤに対応するＩＰアドレスをネットワークアクセスセッション情報管理テーブルから検索する手段と、対応するＩＰアドレスが取得できたか否かを判断する手段と、取得できなかった場合には前記認証代行サーバへ前記ネットワークアクセス認証状態結果（認証不成功）を返信する手段と、取得できた場合には前記ネットワークアクセス認証サーバから前記認証代行サーバへ、ネットワークアクセス認証状態確認結果（認証状態が認証済み、ＩＰアドレス）を送る手段と、を備えることを特徴とする。

【００２５】

また、前記各ステップをコンピュータに実行させるためのプログラムであり、前記各手段としてコンピュータを機能させるためのプログラムであり、前記プログラムを記録したコンピュータ読取可能な記録媒体である。

【発明の効果】

【００２６】

（１）ユーザ端末からの認証要求によりネットワークアクセス認証サーバで認証を行うだけで、サービスサーバへのサービス要求時は、ユーザはそれ以降のＩＤＰ認証あるいはサービスサーバでの認証処理を意識する必要がなく、一度の認証手続きでサービスを享受可能となる。

（２）ＩＤＰ認証とＮＷアクセス認証との併用により、セキュリティの向上と個人まで認識した認証が可能となる。すなわち、ホームゲートウェイ内の個々のユーザ（ユーザ端末）まで識別した認証が可能となる。また１ユーザが複数のＮＷユーザＩＤを持つことが可能となる。

（３）サービスサーバに対しては然るべきネットワークからアクセスしていることを保証し、特定のネットワークのみに特別なサービスを提供可能となる。

（４）サービスプロバイダにおいて課金情報の取得を不要とすることを目的として、認証代行サーバからの認証結果情報の発行履歴を、発行先サービス（ＵＲＬ）と発行ユーザのＩＤとを対応付けて、それを課金情報として利用することも可能となる。

（５）１つの認証代行サーバの配下に複数のネットワークアクセス認証サーバが接続される場合でも、認証代行サーバにおいて、認証サーバの識別子、あるいはＩＰアドレスから認証サーバを引くテーブルにより、該当ネットワークアクセス認証サーバを特定することが可能である。

【発明を実施するための最良の形態】

【００２７】

以下に本発明の実施の形態を、図面を参照して説明する。

【００２８】

図１によりユーザ端末１００、ホームゲートウェイ１１０、ネットワークアクセス認証サーバ１２０、認証代行サーバ１３０、サービスサーバ１４０、アクセスサーバ１５０で構成されるシステムの構成において、認証代行サーバ１３０によるＩＤＰ認証（認証代行サーバでの認証）とネットワークアクセス認証サーバ１２０によるＮＷアクセス認証（ネットワークアクセス認証サーバでの認証）とを併用する場合の処理手順を、以下に段階毎に分けて説明する。なお、ネットワークをＮＷと略記する場合がある。

【００２９】

図１に示すように、ホームゲートウェイ１１０には複数のユーザ端末（図１ではユーザＡとユーザＢの端末）を接続することができるが、ホームゲートウェイ１１０を設けずにユーザ端末１００が直接アクセスサーバ１５０に接続するようにしてもよい。また、ホームゲートウェイ１１０は家庭用に用いるものでなくてもよく、一般に、ユーザ端末１００とネットワークとを接続するためのゲートウェイであればよい。アクセスサーバ１５０はユーザ端末１００／ホームゲートウェイ１１０にＩＰアドレスを動的に割り当てる。ネットワークアクセス認証サーバ１２０は、ＲＡＤＩＵＳ（Remote Authentication Dial-In User Servce）サーバであり、ネットワークアクセス認証サーバにおけるユーザＩＤであるＮＷユーザＩＤ（図の例ではＮＷ　Ｘ）とそれに割り当てられた動的割当ＩＰアドレスを含むＮＷアクセスセッション情報をＮＷアクセスセッション情報管理テーブル１２１に格納する。また、認証代行サーバ１３０は認証代行サーバにおけるユーザＩＤであるＩＤＰユーザＩＤ（図の例ではユーザＡ、ユーザＢ）とそれに対応するパスワード（図の例ではＰＷＤ）とネットワークアクセス認証サーバにおけるユーザＩＤであるＮＷユーザＩＤ（図の例ではＮＷ　Ｘ）とを含むユーザアカウントをＩＤＰユーザ管理テーブル１３１に格納し、一つのＮＷユーザＩＤに対して複数のＩＤＰユーザＩＤを管理することができる。したがって、ネットワークアクセス認証サーバ１２０は同じホームゲートウェイ１１０に接続されたユーザＡとユーザＢの端末を識別することはできないが、認証代行サーバ１３０はユーザＡとユーザＢの端末を識別できる。

【００３０】

まず、図１を用いて、処理手順の概要を説明する。

（１）：［１］ユーザ端末１００はホームゲートウェイ１１０とアクセスサーバ１５０を介してネットワークアクセス認証サーバ１２０に接続し、ネットワークアクセス認証サーバ１２０はユーザ端末１００／ホームゲートウェイ１１０に対してＮＷユーザＩＤとパスワードでＮＷアクセス認証を行う。ネットワークアクセス認証サーバ１２０はＮＷユーザＩＤ（ＮＷ　Ｘ）とアクセスサーバ１５０が動的に割り当てたＩＰアドレス（動的割当ＩＰアドレス）をＮＷアクセスセッション情報管理テーブル１２１に格納する。

（２）：［２］ユーザ端末１００はサービスサーバ１４０に対してシングルサインオンによるサービスを要求する。

（３）：［３］サービスサーバ（ＳＰ）１４０はリダイレクト先ＵＲＬ（認証代行サーバ１３０のＵＲＬ）を含む認証要求をユーザ端末１００送り、ユーザ端末１００は認証代行サーバ（ＩＤＰ）１３０へ認証要求を返す。

（４）：［４］認証代行サーバ１３０はユーザ端末１００に対してＨＴＴＰＳによる認証（ＩＤＰユーザＩＤ／パスワードまたは電子証明書による認証）を行い、認証代行サーバ１３０はユーザ端末１００／ホームゲートウェイ１１０の発ＩＰアドレスも取得する（発ＩＰアドレスは［３］で取得してもよい）。

（５）：［５］認証代行サーバ１３０はネットワークアクセス認証サーバ１２０に対して、ユーザに対応するＮＷユーザＩＤをキーに割り当て中のＩＰアドレスを問い合わせ、ＩＰアドレスを取得する。なお、逆に、発ＩＰアドレスをキーにしてＮＷユーザＩＤを取得してもよい。

（６）：［６］認証代行サーバ１３０はＩＤＰ認証（パスワード認証等）だけでなく、［４］で取得した発ＩＰアドレスと［５］で取得したＩＰアドレスを比較し、発ＩＰアドレス検証を行う。

（７）：［７］サービスサーバ１４０は、認証代理サーバ１３０からの認証結果情報（ア

サーション）をユーザ端末１００／ホームゲートウェイ１１０経由で取得し、認証結果情報の検証を行い、有効ならば、ユーザ端末１００（図１の場合はユーザＢの端末）に対してサービスを提供する。

【００３１】

これにより、正当なルートでアクセスしていることが確認可能となり、より強固になりすましを防止することが可能となる。パスワード（ＰＷＤ）が漏洩しても発ＩＰアドレス検証でなりすましを検出することが可能である。また、認証代行サーバ１３０では個人を識別した認証が可能である。さらに、サービスプロバイダ１４０は特定のネットワークからアクセスするユーザにのみサービスを提供することが可能である。

【００３２】

以下、この処理手順を詳細に説明するが、最初にユーザ端末１００／ホームゲートウェイ１１０からサービスサーバ１４０にサービス要求を行って、サービスの提供を受けようとするとき、既にサービスサーバ１４０あるいは認証代行サーバ１３０で認証状態が確認されている場合の手順を図６によりステップに分けて詳細に説明する。なお、ステップ１等を図においてはＳ１等と略記する。また、図においてはホームゲートウェイをＨＧＷと略記することがある。

（１）：ステップ１：ユーザ端末１００／ホームゲートウェイ１１０からサービスサーバ１４０に対して、サービス提供ＵＲＬを含んだサービス要求を送る。

（２）：ステップ２：サービスサーバ１４０では該ユーザの認証状態を確認する。認証済みならば、ステップ９に遷移してユーザへのサービス提供が開始される。認証済みでないならば、ステップ３に遷移する。

（３）：ステップ３：サービスサーバ１４０からユーザ端末１００／ホームゲートウェイ１１０に対してリダイレクトＵＲＬを含んだ認証要求を送る。

（４）：ステップ４：ユーザ端末１００／ホームゲートウェイ１１０では認証代行サーバ１３０に対して発ＩＰアドレスを含んだ認証要求を返す。

（５）：ステップ５：認証代行サーバ１３０では、認証要求を受信し、該当ユーザの認証状態を確認する。該当ユーザの認証状態が認証済みであるので（ここでの説明の条件下において）、認証結果情報（アサーション）を生成して、ステップ６に進む。

（６）：ステップ６：認証代行サーバ１３０からユーザ端末１００／ホームゲートウェイ１１０に対して、認証応答（認証結果情報、リダイレクト先ＵＲＬ）を送る。

（７）：ステップ７：ユーザ端末１００／ホームゲートウェイ１１０はサービスサーバに対して、該認証応答（認証結果情報）を返す。

（８）：ステップ８：サービスサーバ１４０では認証結果情報の検証を行い、有効ならばステップ９へ、有効でないならばユーザへサービス提供不可の通知を行う。

（９）：ステップ９：サービスサーバはユーザ端末１００／ホームゲートウェイ１１０に対してサービス提供を開始する。

【００３３】

次に同図１によりユーザ端末１００、ホームゲートウェイ１１０、ネットワークアクセス認証サーバ１２０、認証代行サーバ１３０、サービスサーバ１４０、アクセスサーバ１５０で構成されるシステムの構成において、同図６により説明した前記処理ステップの中で下記の状況下の場合を詳細に説明する。すなわち、サービスサーバ１４０及び認証代行サーバ１３０での認証が未認証の場合であり、ステップ５において、認証代行サーバ１３０で認証代行サーバの認証が未認証である状況以降の手順を以下に説明する

（１）：ステップ１０：ユーザ端末１００／ホームゲートウェイ１１０と認証代行サーバ１３０間で、ＩＤ、パスワード（ＰＷＤ）等によるＩＤＰ認証が行われる。

（２）：ステップ１１：認証代行サーバ１３０において認証が成功の場合は、ネットワーク認証状態を検証するため、認証代行サーバ１３０からネットワークアクセス認証サーバ１２０へ、認証要求パケットの発ＩＰアドレス（ソースＩＰアドレス）をキーとしてネットワークアクセス認証状態の確認を依頼する。なお、逆に、ＮＷユーザＩＤをキーにＩＰアドレスを取得する方法もある。

（３）：ステップ１２：ネットワークアクセス認証サーバ１２０では、ＮＷアクセスセッション情報管理テーブル１２１よりＩＰアドレス（図１の動的割当ＩＰアドレス）に対応するＮＷユーザＩＤ（図１のＮＷ　Ｘ）を検索する。対応するＮＷユーザＩＤが取得できた場合には、ステップ１３に進む。
（４）：ステップ１３：ネットワークアクセス認証サーバ１２０は認証代行サーバ１３０に対してネットワーク認証状態の認証済みとＮＷユーザＩＤを含んだネットワークアクセス認証状態確認結果を送る。
（５）：ステップ１４：認証代行サーバ１３０においては、取得したＮＷユーザＩＤ（図１ではＮＷ　Ｘ）に対応するＩＤＰユーザＩＤをＩＤＰユーザ管理テーブル１３１より検索し、ＩＤＰユーザＩＤ（図１ではユーザＡ、ユーザＢ）を取得できた場合には、その取得したＩＤＰユーザＩＤと、ＩＤＰ認証時に取得したＩＤＰユーザＩＤを比較する。この比較で、一致するものが存在する場合には、認証結果情報（アサーション）を生成する。
（６）：ステップ６：認証代行サーバ１３０からユーザ端末１００／ホームゲートウェイ１１０に対して、認証応答（認証結果情報、リダイレクト先ＵＲＬ）を送る。
（７）：ステップ７：ユーザ端末１００／ホームゲートウェイ１１０はサービスサーバ１４０に対して、該認証応答（認証結果情報）を返す。
（８）：ステップ８：サービスサーバ１４０では認証結果情報の検証を行い、有効ならばステップ９へ、有効でないならばユーザへサービス提供不可の通知を行う。
（９）：ステップ９：サービスサーバ１４０はユーザ端末１００／ホームゲートウェイ１１０に対してサービス提供を開始する。
【００３４】
以上により、ＩＤＰ認証とＮＷアクセス認証とを連携させた認証処理が完了する。
【００３５】
前記において、図６のステップ５からステップ６に遷移するまでの認証代行サーバ１３０の処理内容を図７で詳細に説明する。
（１）：ステップ２１：認証代行サーバ１３０は、サービスサーバ１４０よりユーザ端末１００を経由してきた認証要求を受信する。
（２）：ステップ２２：認証要求の中から送信元ＩＰアドレス（発ＩＰアドレス）を取得する。
（３）：ステップ２３：セッション情報を参照して、該当ユーザの認証状態を確認する。セッション情報とはセッションを管理する情報であり、本実施形態ではサービスサーバ１４０がユーザが新規アクセスするごとに払い出したＣｏｏｋｉｅ情報をキーとして管理する情報であり、セッションＩＤや認証状態を含む。
（４）：ステップ２４：認証状態が確認済みか否かを判断する。認証済みの場合には、ステップ２８に進む。認証済みでない場合にはステップ２５に進む。以下ステップ２５へ進む場合を先に説明する。
（５）：ステップ２５：ＩＤ／パスワード、公開鍵証明書、バイオメトリクス、あるいはワンタイムパスワードなどによるＩＤＰ認証を実施する。
（６）：ステップ２６：ＩＤＰ認証が成功か否かを判断する。成功の場合はステップ２７へ、不成功の場合はステップ３０へ進む。
（７）：ステップ２７：ＮＷアクセス認証状態の検証を行う。この処理は図８により詳細に説明する。
（８）：ステップ２８：ＮＷアクセス認証状態の検証が正常を受けて、認証結果情報（アサーション）を生成する。
（９）：ステップ２９：認証代行サーバ１３０はユーザ端末１００へ、サービスサーバ１４０への認証結果情報（アサーション）の送出を依頼する。
（１０）：ステップ３０：本ステップはステップ２６での認証が不成功の場合に実施するステップで、ユーザへサービスサーバ提供不可を通知する。
【００３６】
さらに図７のステップ２７でのＮＷアクセス認証状態の検証に関する処理内容を図８（

１）、図８（２）により詳細に説明する。前者の図では、ＩＰアドレスをキーとして、認証代行サーバからネットワークアクセス認証サーバへ認証要求する場合で、後者の図では、ＮＷユーザＩＤをキーにする場合である。

【００３７】

最初に図８（１）によりＩＰアドレスをキーとした場合の処理方法を詳細に説明する。

（１）：ステップ３１：認証代行サーバ１３０はネットワークアクセス認証サーバ１２０へ、認証要求パケットの中の発ＩＰアドレスをキーとして、ネットワークアクセス認証状態の確認を依頼する。

（２）：ステップ３２：ネットワークアクセス認証サーバ１２０より、ネットワークアクセス認証状態確認結果（ネットワーク認証状態と、認証済みの場合にはＮＷユーザＩＤが含まれる）を受信する。

（３）：ステップ３３：ネットワーク認証状態が認証済みの場合には、ステップ３４に進み、未認証の場合には、図７のステップ３０に進む。

（４）：ステップ３４：取得したＮＷユーザＩＤに対応するＩＤＰユーザＩＤをＩＤＰユーザ管理テーブル１３１より検索する。

（５）：ステップ３５：ＩＤＰユーザＩＤが取得できたか否かの判断を行う。取得できた場合には、ステップ３６に進み、取得出来なかった場合には図７のステップ３０に進む。

（６）：ステップ３６：これにより認証代行サーバ１３０が取得しＩＤＰユーザＩＤと、ＩＤＰ認証時に取得したＩＤＰユーザＩＤとを比較する。

（７）：ステップ３７：ＩＤＰユーザＩＤの比較で一致するものがあるか否かの判断を行う。一致するものがあれば図７のステップ２８に進む。一致しなければ、同図のステップ３０に進む。

【００３８】

次に、ＮＷアクセス認証状態の検証に関する処理方法でＮＷユーザＩＤをキーとする場合の処理を図８（２）により詳細に説明する。

（１）：ステップ４１：認証代行サーバは、ＩＤＰ認証時に取得したＩＤＰユーザＩＤに対応するＮＷユーザＩＤをＩＤＰユーザ管理テーブルより検索する。

（２）：ステップ４２：ＮＷユーザＩＤが取得できたか否かを判断する。取得できた場合には、ステップ４３に進み、取得できなかった場合には図７のステップ３０に進む。

（３）：ステップ４３：認証代行サーバ１３０は、ネットワークアクセス認証サーバ１２０へ、ＮＷユーザＩＤをキーとしてＮＷアクセス認証状態の確認を依頼する。

（４）：ステップ４４：認証代行サーバ１３０はネットワークアクセス認証サーバ１２０より、ＮＷアクセス認証状態確認結果（ＮＷ認証状態と、認証済みの場合にはＩＰアドレスが含まれる）を受信する。

（５）：ステップ４５：ＮＷ認証状態が済みか否かを判断する。済みの場合にはステップ４６に進み、未承認の場合には図７のステップ３０に進む。

（６）：ステップ４６：ネットワークアクセス認証サーバ１２０より取得したＩＰアドレスと、認証要求パケットの発ＩＰアドレスとを比較する。

（７）：ステップ４７：ＩＰアドレスの比較で一致するものがあるか否かの判断を行う。一致するものがあれば図７のステップ２８に遷移し、一致しなければ、同図のステップ３０に遷移する。

【００３９】

さらに、前記の図８（１）のＩＤＰ処理での、ＩＰアドレスをキーとしたＮＷアクセス認証状態の検証において、同図のステップ３２におけるネットワークアクセス認証サーバ１２０の処理を図９（１）により詳細に説明する。すなわち、

（１）：ステップ５１：ネットワークアクセス認証サーバ１２０は、ＩＰアドレスをキーとしたネットワークアクセス認証状態の確認依頼を受信する。

（２）：ステップ５２：ＩＰアドレスに対応するＮＷユーザＩＤをＮＷアクセスセッション情報管理テーブル１２１から検索する

（３）：ステップ５３：対応するＮＷユーザＩＤが取得できたか否かを判断する。取得で

きた場合にはステップ５５へ、取得できなかった場合にはステップ５４に進む。
（４）：ステップ５５：ネットワークアクセス認証サーバ１２０から認証代行サーバ１３０へ、ネットワークアクセス認証状態確認結果（認証状態が認証済み、ＮＷユーザＩＤ）を送る。
（５）：ステップ５４：ネットワークアクセス認証サーバ１２０から認証代行サーバ１３０へ、ネットワークアクセス認証状態確認結果（認証状態が未認証）を送る。
【００４０】
次に、前記の図８（２）のＩＤＰ処理での、ＮＷユーザＩＤをキーとしたＮＷアクセス認証状態の検証において、同図のステップ４４におけるネットワークアクセス認証サーバ１２０の処理を図９（２）により詳細に説明する。すなわち、
（１）：ステップ６１：ネットワークアクセス認証サーバ１２０は、ＮＷユーザＩＤをキーとしたネットワークアクセス認証状態の確認依頼を受信する。
（２）：ステップ６２：ＮＷユーザＩＤに対応するＩＰアドレスをＮＷアクセスセッション情報管理テーブル１２１から検索する。
（３）：ステップ６３：対応するＩＰアドレスが取得できたか否かを判断する。取得できた場合にはステップ６５へ、取得できなかった場合にはステップ６４に進む。
（４）：ステップ６５：ネットワークアクセス認証サーバ１２０から認証代行サーバ１３０へ、ネットワークアクセス認証状態確認結果（認証状態が認証済み、ＩＰアドレス）を送る。
（５）：ステップ６４：ネットワークアクセス認証サーバ１２０から認証代行サーバ１３０へ、ネットワークアクセス認証状態確認結果（認証状態が未認証）を送る。
【００４１】
ユーザ端末１００、ホームゲートウェイ１１０からの、ネットワーク接続並びに認証要求に対するＮＷアクセス認証の処理は図５により詳細に説明する。
（１）：ステップ７０：ユーザ端末１００／ホームゲートウェイ１１０はアクセスサーバ１５０に対して、認証情報としてＩＤ、パスワード等によりネットワークへの接続・認証要求を行う。
（２）：ステップ７１：アクセスサーバ１５０はネットワークアクセス認証サーバ１２０に対して認証要求を行う。
（３）：ステップ７２：ネットワークアクセス認証サーバ１２０では、ユーザ認証を行う。認証成功の場合はステップ７３に遷移し、不成功の場合には図１２によりアクセスサーバ１５０へ認証不可を返信して、ネットワークアクセス認証サーバ１２０の処理を終了する。
（４）：ステップ７３：ネットワークアクセス認証サーバ１２０はアクセスサーバ１５０へ認証応答（認証結果）を送る。
（５）：ステップ７４：アクセスサーバ１５０はユーザ端末１００／ホームゲートウェイ１１０に接続・認証応答（認証結果、ＩＰアドレス）を送る。
（６）：ステップ７５：アクセスサーバ１５０はネットワークアクセス認証サーバ１２０に対して払い出したＩＰアドレスを通知する。
（７）：ステップ７６：ネットワークアクセス認証サーバ１２０は、前記ＩＰアドレスを受信し、ＮＷアクセスセッション情報管理テーブル１２１の該当ＮＷユーザＩＤ（図１ではＮＷ　Ｘ）に対してＩＰアドレス（図１では動的割り当てＩＰアドレス）を登録する。
【００４２】
図２により１つの認証代行サーバの配下に複数のネットワークアクセス認証サーバが接続されているシステムの構成における認証の手順を説明する。図６で示したＩＤＰ認証とＮＷアクセス認証とを連携する処理手順と異なる部分のみを以下で詳細に説明する。
（１）：基本となる事前処理：ＩＤＰユーザＩＤをエントリーする毎に、ネットワークアクセス認証サーバ１２０Ｘ、１２０Ｙの識別子を付与する。
（２）：サービスサーバ（図示していない）からユーザ端末１００Ｘ、１００Ｙを経由して認証代行サーバ１３０に送られた認証要求を契機に、ユーザ端末１００Ｘ、１００Ｙと

認証代行サーバ１３０間で、ＩＤ、パスワードあるいは電子証明書等によるＩＤＰ認証が行われ、成功した場合にはＩＤＰユーザＩＤを取得する。
（３）：認証代行サーバ１３０は、前記の識別子により該当するネットワークアクセス認証サーバ１２０Ｘ、１２０Ｙに、認証要求パケットのソースＩＰアドレスをキーとしてネットワークアクセス認証状態の検証を依頼する。
（４）：以降の手順は、図８（１）もしくは図８（２）のステップ３１からステップ３７と同じとし、さらに図７により認証代行サーバ１３０が認証結果情報（アサーション）を生成し（ステップ２８）、ユーザ端末１００Ｘ、１００Ｙへサービスサーバへの認証結果情報（アサーション）の送出を依頼して（ステップ２９）、認証連携の処理を可能にする。

【００４３】
前記処理において、ＩＤＰ認証が成功した後に、図７により認証結果情報（アサーション）を生成して（ステップ２８）、認証代行サーバはユーザ端末へサービスサーバへの認証結果情報（アサーション）の送出を依頼して（ステップ２９）、認証処理を行う手順も可能になる。

【００４４】
図２に、１つの認証代行サーバ１３０の下に複数のネットワークアクセス認証サーバが存在する場合のシステムを示す。ユーザＡのユーザ端末１００Ｘ／ホームゲートウェイ１１０ＸはＩＳＰ　Ｘ経由でインターネット、ＶＰＮ等に接続する。ＩＳＰ　Ｘのネットワークアクセス認証サーバ１２０Ｘは、ＲＡＤＩＵＳサーバであり、ＮＷアクセスセッション情報をＮＷアクセスセッション情報管理テーブル１２１Ｘに格納し、ＮＷユーザＩＤ（図２ではＮＷ　Ｘ）とパスワード（図２ではＰＷＤ）を含むＮＷアクセスアカウントをＮＷアクセスアカウント管理テーブル１２２Ｘに格納する。ネットワークアクセス認証サーバ１２０Ｘはユーザ Ａのユーザ端末１００Ｘに対してパスワードベースでネットワークアクセス認証を行い、ＩＰアドレスを動的に割り当てる。また、ユーザＢのユーザ端末１００Ｙ／ホームゲートウェイ１１０ＹはＩＳＰ　Ｙ経由でインターネット、ＶＰＮ等に接続する。ＩＳＰ　Ｙのネットワークアクセス認証サーバ１２０Ｙは、ＲＡＤＩＵＳサーバであり、ＮＷアクセスセッション情報をＮＷアクセスセッション情報管理テーブル１２１Ｙに格納し、ＮＷユーザＩＤ（図２ではＮＷ　Ｙ）とパスワード（図２ではＰＷＤ）を含むＮＷアクセスアカウントをＮＷアクセスアカウント管理テーブル１２２Ｙに格納する。ネットワークアクセス認証サーバ１２０Ｙはユーザ Ｂのユーザ端末１００Ｙに対してパスワードベースでネットワークアクセス認証を行い、ＩＰアドレスを動的に割り当てる。認証代行サーバ１３０はポータルユーザアカウントをＩＤＰユーザ管理テーブル１３２に格納する。ポータルユーザアカウントには、各ユーザがどのネットワークアクセス認証サーバ（ＲＡＤＩＵＳサーバ）に属するかを識別する情報（図２ではＲＡＤＩＵＳ－Ｘ、ＲＡＤＩＵＳ－Ｙ）を含む。なお、その他の点については図１と同様であり、図２においてもサービスプロバイダ（図示していない）が存在する。

【００４５】
図２の実施形態の場合は、一つの認証代行サーバの配下に複数のネットワークアクセス認証サーバが存在する場合に、認証代行サーバにおいて対応するネットワークアクセス認証サーバ（ＲＡＤＩＵＳサーバ）を識別することができる。したがって、異なるネットワークアクセス認証サーバ上に同名のＮＷユーザＩＤの存在が可能とである。

【００４６】
図２により、１つの認証代行サーバ１３０の配下に複数のネットワークアクセス認証サーバ１２０Ｘ、１２０Ｙが接続されているシステムの構成における認証の手順で、サービスサーバからユーザ端末１００Ｘ、１００Ｙを経由して認証代行サーバ１３０に送られた認証要求を契機に、以下の手順によっても認証処理、並びにサービス提供が可能である。以下に手順を詳細に説明する。すなわち、
（１）：基本となる事前処理：認証代行サーバ１３０では、ユーザ端末１００Ｘ、１００Ｙの発ＩＰアドレスからネットワークアクセス認証サーバ１２０Ｘ、１２０Ｙを引くテー

ブルを用意する。図２では、ＩＤＰユーザ管理テーブル１３２のＲＡＤＩＵＳ－Ｘ、ＲＡＤＩＵＳ－ＹがユーザＡ、ユーザＢがどのネットワークアクセス認証サーバに属するのかを識別する情報である。
（２）：ユーザ端末からの発ＩＰアドレスにより前記テーブルを用いて、該当ネットワークアクセス認証サーバを特定し、認証代行サーバ１３０から該当ネットワークアクセス認証サーバへ認証要求を行う。
（３）：これを受けたステップは、図９（１）で説明したネットワークアクセス認証サーバ１２０でのステップ５１からステップ５４ないしは５５までと同じ処理となる。
（４）：認証代行サーバ１３０ではＮＷユーザＩＤを取得したことにより、認証結果情報（アサーション）を生成する。
（５）：これを受けたステップは、図７のステップ２９によりＩＤＰ認証処理が完結する。

【００４７】
また、前記処理において、認証代行サーバ１３０において、ユーザ端末１００Ｘ、１００Ｙの発ＩＰアドレスからネットワークアクセス認証サーバを引くテーブルを用意して、ユーザ端末からの発ＩＰアドレスにより該当するネットワークアクセス認証サーバへ認証要求を行う前記の処理手順において、（４）の処理の代わりに、以下のステップを実施してＩＤＰ認証と連携させることも可能である。すなわち、
（１）：認証代行サーバ１３０ではＮＷユーザＩＤを取得する。
（２）：認証代行サーバ１３０は、ユーザ端末１００Ｘ、１００ＹからのＩＤ、パスワードによりＩＤＰ認証を行い、それにより得られたＮＷユーザＩＤと、それぞれのユーザに対応するネットワークアクセス認証サーバ１２０Ｘ、１２０Ｙからの認証応答のＮＷユーザＩＤとを比較して、それが一致した時に、認証結果情報（アサーション）を生成して、図７のステップ２９により、ＮＷユーザ認証とＩＤＰ認証の連携が可能となる。本実施形態ではＮＷユーザ認証とＩＤＰ認証を連携して行っているが、ＮＷユーザ認証だけで十分なセキュリティを確保できる場合は、ＮＷユーザ認証単独の認証のみを行うようにしてもよい。

【００４８】
図３に、サービスオーダー時に投入されるＩＰアドレスを補助的に利用した認証を行う場合のシステムを示す。図３はユーザアカウント情報としてサービスオーダー時に投入されるＩＰアドレスを補助的に利用したパスワードベースのユーザ認証の例である。ホームゲートウェイ１１０には複数のユーザ端末（図３ではユーザＡ、ユーザＢの端末）が接続されることがある。ユーザ端末１００／ホームゲートウェイ１１０はエッジルータ１６０を介して認証代行サーバ１３０に接続する。図３の実施形態においてはＩＰアドレスは回線毎に固定的に割り当てられている。エッジルータ１６０に備えられたＩＰアドレス割当テーブルには、ＮＷユーザＩＤ（図３ではＮＷ　Ｘ）のＶＬＡＮＩＤと固定割当ＩＰアドレスが格納される。認証代行サーバ１３０に備えられたＩＤＰユーザ管理テーブル１３３には、割当済ＩＰアドレスが格納される。認証代行サーバ１３０は、ユーザ端末１００に対してＨＴＴＰ上でパスワード認証を行い、また、ＩＤＰユーザ管理テーブル１３３に格納された割当済ＩＰアドレスを用いて発ＩＰアドレスの検証も行う。なお、その他の点については図１と同様であり、図３の実施形態においてもサービスプロバイダ（図示していない）が存在する。

【００４９】
図３により、ユーザ端末１００がホームゲートウェイ１１０、エッジルータ１６０を介して認証代行サーバ１３０に接続されるシステムの構成における、シングルサインオンの処理を説明する。
（１）：サービスオーダー時に投入されるＩＰアドレスをユーザアカウント情報として登録する。
（２）：エッジルータ１６０においてＩＰアドレスは回線毎に固定的に割り当てられる。
（３）：ユーザ端末１００と認証代行サーバ１３０間での、ＩＤ、パスワード等によるＩ

ＤＰ認証においては、発ＩＰアドレスの検証にはユーザアカウント情報のＩＰアドレスを補助的に利用する。認証代行サーバ１３０がＩＤＰユーザＩＤのエントリー毎にＩＰアドレスを記憶しているので、ＩＤ／パスワード認証と発ＩＰアドレス検証の二重チェックが可能となる。

【００５０】

認証結果情報（アサーション）発行履歴を課金に利用する実施例を図４により説明する。

（１）：［１］：ユーザ端末１００とネットワークアクセス認証サーバ１２０間で、ネットワークアクセス認証が行われ、認証が成功すると、ネットワークアクセス認証サーバ１２０のＮＷアクセスセッション情報管理テーブル１２３の該当ＮＷユーザＩＤ（図４ではＮＷ　Ａ）に対してＩＰアドレス（図４では動的割当ＩＰアドレス）を登録する。

（２）：［２］ユーザ端末１００からサービスサーバ１４０へサービス要求が送られる。

（３）：［３］サービスサーバ１４０では、当該ユーザの認証状態を確認できた場合は［８］に遷移する（サービス提供開始）。認証確認ができない場合は、サービスサーバ１４０からユーザ端末１００を経由して認証代行サーバ１３０に認証要求を行う。

（４）：［４］認証代行サーバ１３０はネットワークアクセス認証サーバ１２０に対して、認証要求のＩＰアドレスをキーにＮＷアクセスユーザＩＤを問合せる。

（５）：［５］認証代行サーバ１３０は取得したＮＷアクセスユーザＩＤに対応するＩＤＰユーザＩＤが存在すれば、認証が済みとする。

（６）：［６］認証代行サーバ１３０では認証結果情報（アサーション）発行履歴を「発行先サービス（ＵＲＬ）」と「発行ユーザ（ＩＤＰユーザＩＤ）」とを対応付けて管理（サービスサーバ別かつユーザ別）する。これをサービス提供時の課金に利用すると、サービスプロバイダでは課金情報の取得が不要になる。

（７）：［７］認証代行サーバ１３０での認証結果情報（アサーション）をユーザ端末１００を経由してサービスサーバ１４０へ送る。

（８）：［８］サービスサーバ１４０は認証結果情報を受信することにより、ユーザ端末１００に対してサービス提供を行う。

【００５１】

図４の実施形態により、各サービスプロバイダ（ＳＰ）は通信回線業者のアクセス網を経由して正規のアクセス認証を経たユーザのアクセスであることを確認した上でサービスを認可することが可能である。したがって、サービスプロバイダにて課金情報の取得が不要となる。

【００５２】

以上の処理は図１０の処理フローでも説明でき、前記処理手順において、ＩＤＰ認証が不成功のとき、ＮＷアクセス認証状態を検証して認証済みでないときは、同図によりユーザへサービス提供不可を通知する処理となる。図１０において、ステップ７７～ステップ８５はこれまで説明してきたものと同様である。ステップ８６において、ユーザ端末へサービスサーバへの認証結果情報（アサーション）の送出を依頼する。ステップ８７において、アサーション発行履歴テーブルへ履歴を記録する。

【００５３】

さらに同図１０により認証結果情報（アサーション）発行履歴テーブルへ履歴を記録する処理に関わるテーブル内容は図１１により説明する。

（１）：認証結果情報（アサーション）発行毎に認証結果情報（アサーション）発行履歴管理テーブルにログを記録する。アサーション発行履歴テーブルには、ＩＤＰユーザＩＤ、サービスサーバ識別子、サービス識別子、日時が記録される。また、サービス料金管理テーブルには、サービスサーバ識別子、サービス識別子、サービス料金が格納されている。

（２）：各ユーザ毎に課金情報を集計する際には、サービス料金管理テーブルから各サービスの料金を取得し、認証結果情報（アサーション）発行履歴管理テーブルを元にユーザ毎のサービス利用料を算出する。

【００５４】
なお、アクセス終了に伴う切断処理は従来の動作と変わらないので図示しない。
【００５５】
また、各実施形態では、ＮＷアクセス認証の具体的方法として、ＩＤ・パスワード認証方法を用いたが、その他の後置の方法、例えば、電子証明書を用いた方法、発番号認証（ダイアルアップ接続時におけるユーザ端末の電話番号や、常時接続時におけるアクセスサーバのユーザ端末向け物理ポートなどに基づく認証）などの方法を用いてもよい。
【００５６】
以上のフローチャートに基づいて、コンピュータプログラムを作成することができ、また、そのプログラムを記録媒体に記録することも、ネットワークを通じて提供することも可能である。
【００５７】
以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。
【図面の簡単な説明】
【００５８】
【図１】ＩＤＰ認証とＮＷアクセス認証の併用による認証処理を示すネットワークの構成
【図２】１つの認証代行サーバの下に複数のネットワークアクセス認証サーバが存在する場合のシステムの構成
【図３】サービスオーダー時に投入されるＩＰアドレスを補助的に利用した認証を説明するネットワークの構成
【図４】認証結果情報（アサーション）発行履歴を課金に応用する例を説明するシステムの構成
【図５】ＮＷアクセス認証の認証処理シーケンス
【図６】認証処理においてサービス要求からサービス提供までの認証処理シーケンス
【図７】サービス要求時の認証代行サーバの処理フロー
【図８】サービス要求時の認証処理サーバの処理においてネットワークアクセス認証状態の検証の処理フロー
【図９】サービス要求時のネットワークアクセス認証サーバの認証処理フロー
【図１０】認証結果情報（アサーション）発行・履歴管理処理のフロー
【図１１】認証結果情報（アサーション）履歴管理とサービス課金への適用のための管理テーブル
【図１２】ＮＷアクセス認証時のネットワークアクセス認証サーバの処理フロー
【図１３】従来技術によるリモートアクセスユーザ端末からのシングルサインオンを実現するシステムの構成（リモートアクセス拠点が端末の場合）
【図１４】従来技術によるリモートアクセスユーザ端末からのシングルサインオンを実現するシステムの構成（リモートアクセス拠点がＬＡＮの場合）
【符号の説明】
【００５９】
１００…ユーザ端末、１１０…ホームゲートウェイ、１２０…ネットワークアクセス認証サーバ、１３０…認証代行サーバ、１４０…サービスサーバ、１５０…アクセスサーバ、１６０…エッジルータ

【図１】

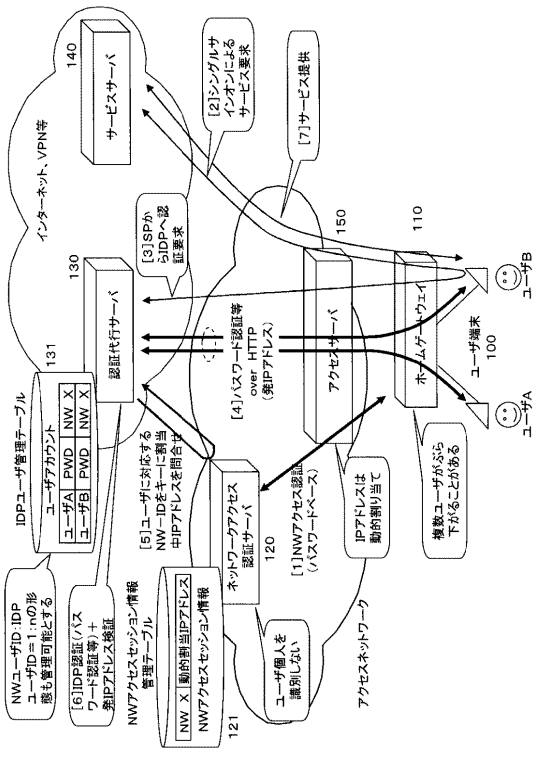


図1 IDP認証とNWアクセス認証の併用による認証処理
インターネット、VPN等
サービスサーバ
140
IDPユーザ管理テーブル
ユーザアカウント
ユーザA PWD NW X
ユーザB PWD NW X
131
認証代行サーバ
130
[3]SPからIDPへ認証要求
[2]シングルサインオンによるサービス要求
[7]サービス提供
[6]IDP認証（パスワード認証等）＋発IPアドレス検証
NWアクセスセッション情報管理テーブル
NW X 動的割当IPアドレス
NWアクセスセッション情報
[5]ユーザに対応するNW－IDをキーに割当中IPアドレスを問合せ
ネットワークアクセス認証サーバ
120
121
[4]パスワード認証等 over HTTP（発IPアドレス）
[1]NWアクセス認証（パスワードベース）
アクセスサーバ
150
IPアドレスは動的割り当て
ホームゲートウェイ
110
ユーザ端末
100
ユーザA
ユーザB
NWユーザID-IDP
ユーザID＝1：nの形態も管理可能とする
アクセスネットワーク
ユーザ個人を識別しない
複数ユーザがぶら下がることがある

【図２】

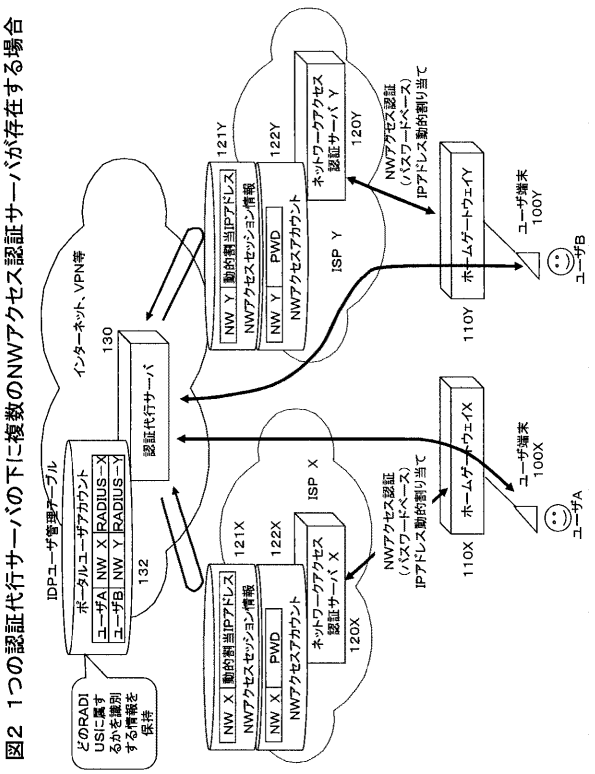


図2 1つの認証代行サーバの下に複数のNWアクセス認証サーバが存在する場合
インターネット、VPN等
IDPユーザ管理テーブル
ポータルユーザアカウント
ユーザA NW X RADIUS→X
ユーザB NW Y RADIUS→Y
132
どのRADIUSに基づるかを識別する情報を保持
認証代行サーバ
130
ISP X
ISP Y
121X
122X
NW X 動的割当IPアドレス
NWアクセスセッション情報
NW X PWD
NWアクセスアカウント
ネットワークアクセス認証サーバ X
120X
NWアクセス認証（パスワードベース）IPアドレス動的割り当て
ホームゲートウェイX
110X
ユーザ端末100X
ユーザA
121Y
122Y
NW Y 動的割当IPアドレス
NW Y PWD
ネットワークアクセス認証サーバ Y
120Y
NWアクセス認証（パスワードベース）IPアドレス動的割り当て
ホームゲートウェイY
110Y
ユーザ端末100Y
ユーザB

【図３】

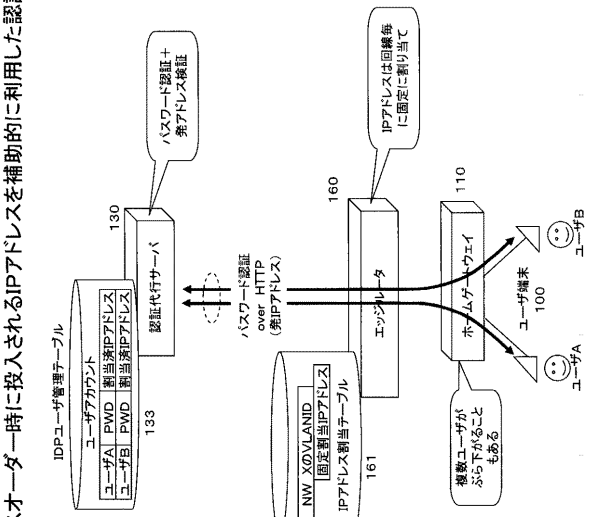


図3 サービスオーダー時に投入されるIPアドレスを補助的に利用した認証
IDPユーザ管理テーブル
ユーザアカウント
ユーザA PWD 割当済IPアドレス
ユーザB PWD 割当済IPアドレス
133
130
認証代行サーバ
パスワード認証＋発アドレス検証
パスワード認証 over HTTP（発IPアドレス）
160
エッジルータ
NW X のVLANID
固定割当IPアドレス
IPアドレス割当テーブル
161
IPアドレスは回線毎に固定に割り当て
ホームゲートウェイ
110
ユーザ端末
100
ユーザA
ユーザB
複数ユーザがぶら下がることもある

【図４】

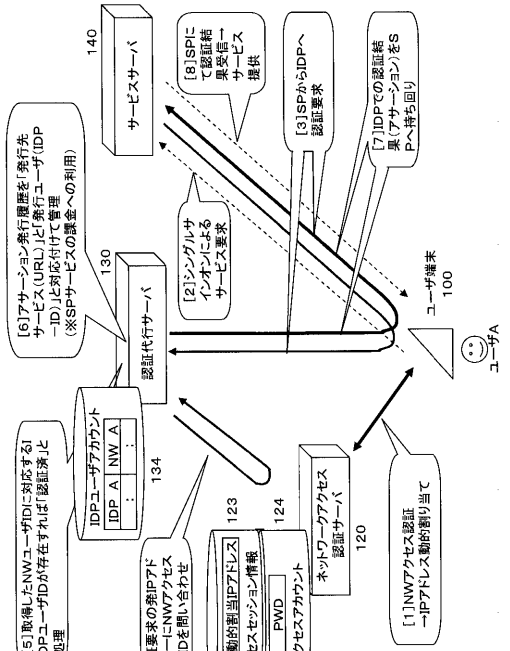


図4 認証結果情報（アサーション）発行履歴の課金への利用
[6]アサーション発行履歴を「発行先サービス（URL）」と「発行ユーザ（IDP－ID）」に対応付けて管理（※SPサービスの課金への利用）
サービスサーバ
140
[8]SPに下認証結果を伝達→サービス提供
[3]SPからIDPへ認証要求
[7]IDPでの認証結果（アサーション）をSPへ持ち回り
[2]シングルサインオンによるサービス要求
認証代行サーバ
130
[5]取得したNWユーザIDに対応するIDPユーザIDが存在すれば「認証済」と処理
IDPユーザアカウント
IDP A NW A
134
[4]認証要求の発IPアドレスをキーにNWアクセスユーザIDを問い合わせ
NW A 動的割当IPアドレス
NWアクセスセッション情報
123
NW A PWD
NWアクセスアカウント
124
ネットワークアクセス認証サーバ
120
[1]NWアクセス認証－IPアドレス動的割り当て
ユーザ端末
100
ユーザA

【図５】

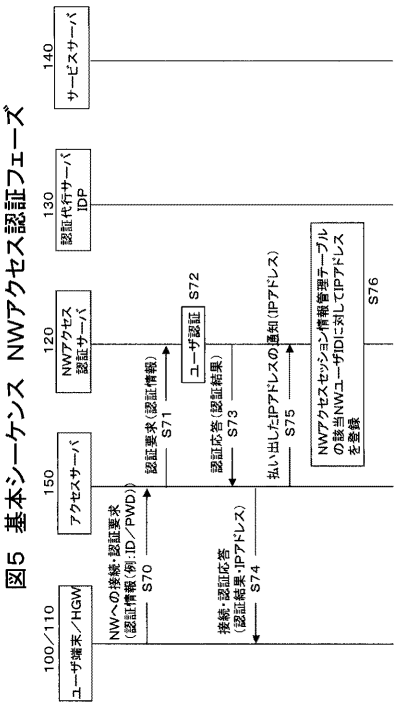


図5 基本シーケンス NWアクセス認証フェーズ
100／110 ユーザ端末／HGW
150 アクセスサーバ
120 NWアクセス認証サーバ
130 認証代行サーバ IDP
140 サービスサーバ
NWへの接続・認証要求（例：ID／PWD）
S70
認証要求（認証情報）
S71
ユーザ認証
S72
認証応答（認証結果）
S73
接続・認証応答（認証結果：IPアドレス）
S74
払い出したIPアドレスの通知（IPアドレス）
S75
NWアクセスセッション情報管理テーブルの該当NWユーザIDに対してIPアドレスを登録
S76

【図６】

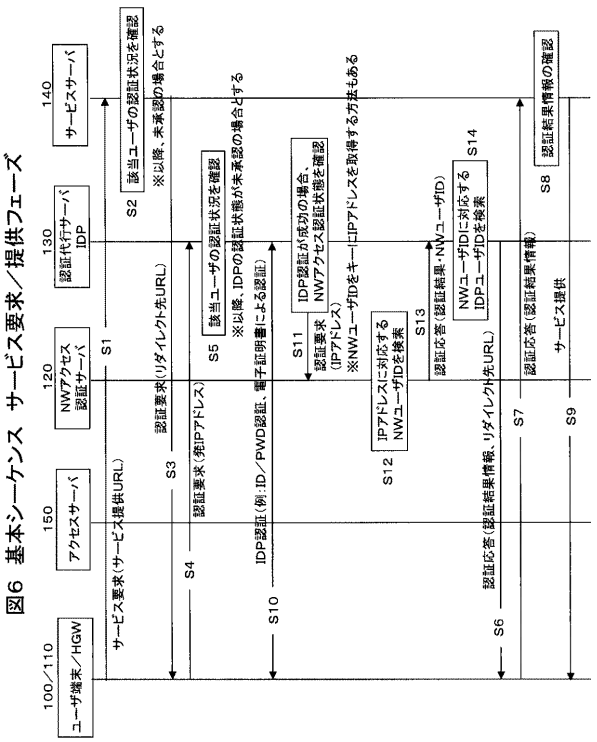


図6 基本シーケンス サービス要求／提供フェーズ
100／110 ユーザ端末／HGW
150 アクセスサーバ
120 NWアクセス認証サーバ
130 認証代行サーバ IDP
140 サービスサーバ
S1 サービス要求（サービス提供URL）
S2 該当ユーザの認証状況を確認
※以降、未承認の場合とする
S3 認証要求（宛IPアドレス）
S4 認証要求（リダイレクト先URL）
S5 該当ユーザの認証状況を確認
※以降、IDPの認証状態が未承認の場合とする
S10 IDP認証（例：ID／PWD認証、電子証明書による認証）
S11 IDP認証が成功の場合、NWアクセス認証状態を確認
認証要求（IPアドレス）
※NWユーザIDをキーにIPアドレスを取得する方法もある
S12 IPアドレスに対応するNWユーザIDを検索
S13
S14 NWユーザIDに対応するIDPユーザIDを検索
認証応答（認証結果：NWユーザID）
S6 認証応答（認証結果情報、リダイレクト先URL）
S7 認証応答（認証結果情報）
S8 認証結果情報の確認
S9 サービス提供

【図７】

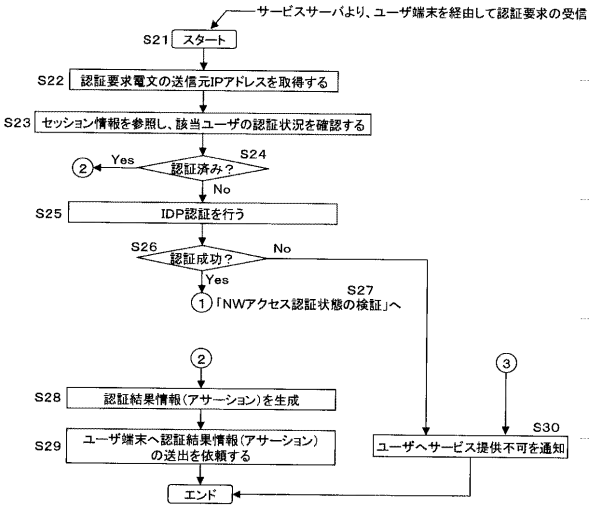


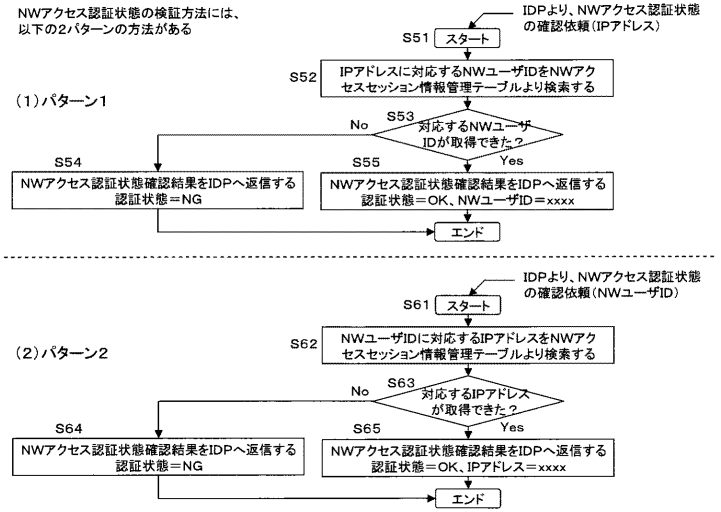
図7 サービス要求時のIDP処理
サービスサーバより、ユーザ端末を経由して認証要求の受信
S21 スタート
S22 認証要求電文の送信元IPアドレスを取得する
S23 セッション情報を参照し、該当ユーザの認証状況を確認する
S24 認証済み？
Yes
No
S25 IDP認証を行う
S26 認証成功？
No
Yes
S27 ①「NWアクセス認証状態の検証」へ
S28 認証結果情報（アサーション）を生成
S29 ユーザ端末へ認証結果情報（アサーション）の送出を依頼する
S30 ユーザへサービス提供不可を通知
エンド

【図８】

図8 サービス要求時のIDP処理（NWアクセス認証状態の検証）
以下の2パターンの方法がある
（1）パターン1
（2）パターン2
S31 NWアクセス認証サーバへ、認証要求パケットの発IPアドレスをキーとしてNWアクセス認証状態の確認を依頼する
S32 NWアクセス認証サーバより、NWアクセス認証状態確認結果を受信する（NW認証状態と、認証済みの場合はNWユーザIDが含まれる）
S33 NW認証状態＝OK？
No
Yes
S34 取得したNWユーザIDに対応するIDPユーザIDをIDPユーザ管理テーブルより検索する
S35 IDPユーザIDが取得できた？
No
Yes
S36 取得したIDPユーザIDと、IDP認証時に取得したIDPユーザIDを比較する
S37 一致するものが存在？
No
Yes
S41 IDP認証時に取得したIDPユーザIDに対応するNWユーザIDをIDPユーザ管理テーブルより検索する
S42 NWユーザIDが取得できた？
No
Yes
S43 NWアクセス認証サーバへNWユーザIDをキーとしてNWアクセス認証状態の確認を依頼する
S44 NWアクセス認証サーバより、NWアクセス認証状態確認結果を受信する（NW認証状態と、認証済みの場合はIPアドレスが含まれる）
S45 NW認証状態＝OK？
No
Yes
S46 NWアクセス認証サーバより取得したIPアドレスと、認証要求パケットの発IPアドレスを比較する
S47 一致するものが存在？
No
Yes

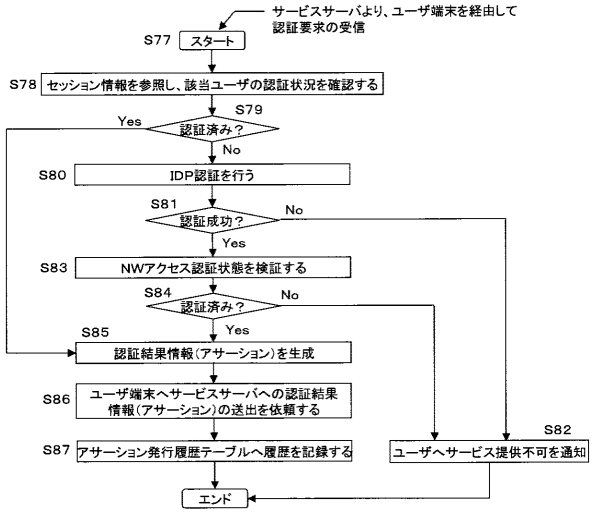
【図９】

図9　サービス要求時のNWアクセス認証サーバ処理



【図１０】

図10　認証結果情報（アサーション）発行・履歴管理処理のフローチャート



【図１１】

図11　アサーション履歴管理とサービス課金への適用

アサーション発行履歴管理テーブル

IDP-ユーザID	サービスサーバ識別子	サービス識別子（※1）	日時
Yamada@xxx.ne.jp	SP-1	http://www.xxx.co.jp/lerning/lesson1.avi	200402261921
kato@yyy.ne.jp	SP-3	http://www.yyy.ne.jp/contents/soccor.mpg	200402261923
Sasaki@xxx.ne.jp	SP-1	http://www.xxx.co.jp/lerning/lesson5.avi	200402261935
…	…	…	…

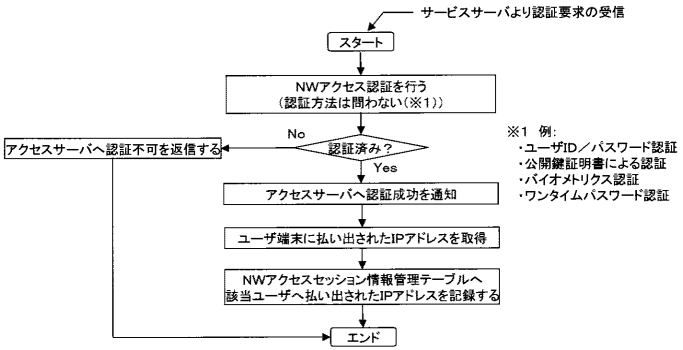
サービス料金管理テーブル

サービスサーバ識別子	サービス識別子（※1）	サービス料金
SP1	http://www.xxx.co.jp/lerning/lesson1.avi	200
…	…	…
SP1	http://www.xxx.co.jp/lerning/lesson5.avi	200
…	…	…
SP3	http://www.yyy.ne.jp/contents/soccor.mpg	100
…	…	…

※1：サービス識別子におけるサービス単位は任意．例としては，
・有料コンテンツをダウンロードする毎に認証・課金する．（コンテンツへのリンクをクリック時に認証を行い，正規ユーザだと確認した上で課金，サービス提供）
・有料サイトへログインする毎に認証・課金する．（ログイン時に認証を行い，正規ユーザだと確認した上で課金，サービス提供）
・通信（IM，VoIP等）する毎に認証・課金する．（通信開始時に認証を行い，正規ユーザだと確認した上で課金，サービス提供）
…

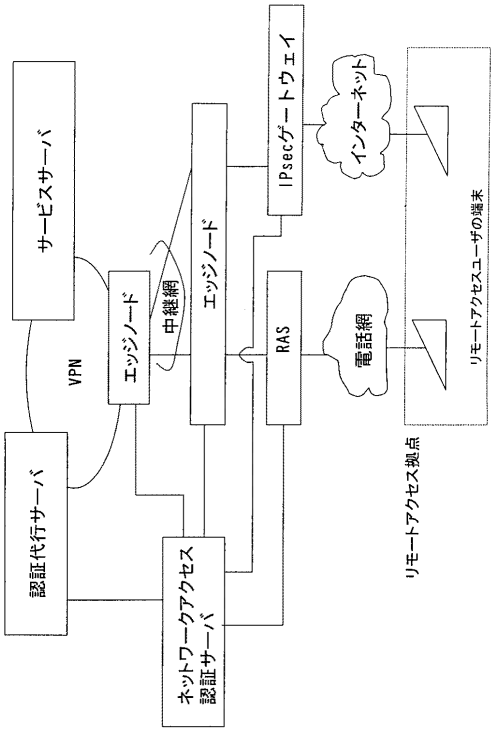
【図１２】

図12　NWアクセス認証時のNWアクセス認証サーバ処理のフローチャート



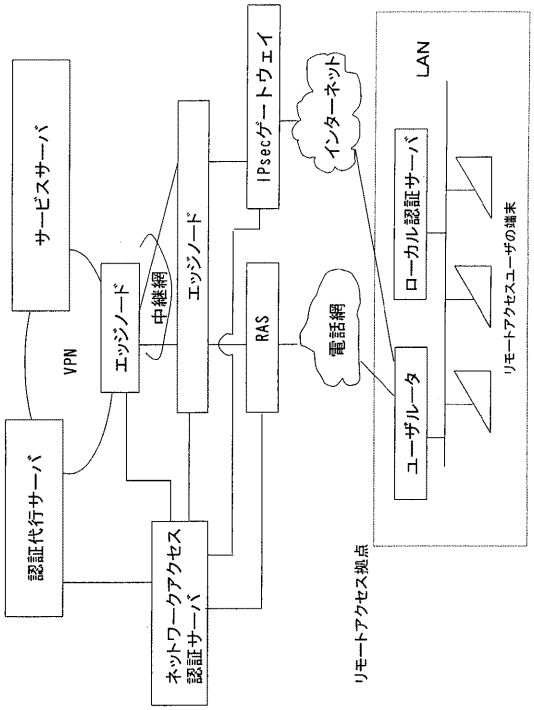
【図１３】

図13



【図１４】

図14



フロントページの続き

(72)発明者　鈴木　光
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

審査官　宮司　卓佳

(56)参考文献　特開２００１－２１７８６５（ＪＰ，Ａ）
特開２００４－１２６７８５（ＪＰ，Ａ）
特開２００４－０８０１３８（ＪＰ，Ａ）
特開２００３－２７１４７７（ＪＰ，Ａ）
特開２００４－１１０４３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２