(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4701670号
(P4701670)
(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 5　(全 17 頁)

(21)出願番号　特願2004-297122(P2004-297122)
(22)出願日　平成16年10月12日(2004.10.12)
(65)公開番号　特開2006-113624(P2006-113624A)
(43)公開日　平成18年4月27日(2006.4.27)
審査請求日　平成19年2月14日(2007.2.14)

前置審査

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　竹内　敬亮
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　瀬野尾　修二
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内

審査官　田中　慎太郎

最終頁に続く

(54)【発明の名称】アクセス制御システム、認証サーバ、アプリケーションサーバ、およびパケット転送装置

(57)【特許請求の範囲】
【請求項１】
端末に接続されるアクセス制御システムであって、
認証サーバと、
ネットワークを介して前記端末に接続されるアプリケーションサーバと、を備え、
上記認証サーバは、
上記端末から送信された、上記アプリケーションサーバが接続するネットワークへ接続するための認証に用いられる第１の識別情報を受信する受信部と、
上記第１の識別情報による認証が成功した場合に、上記端末に対して割り当てられ、上記ネットワークで識別される第２の識別情報を上記端末に送信する送信部と、
上記第１の識別情報と上記第２の識別情報とを対応付けて記憶する第１のメモリを有し、
上記アプリケーションサーバは、
上記端末から送信された上記第２の識別情報と上記アプリケーションサーバからサービスを受けるための第３の識別情報とを含む接続要求を受信する受信部と、
上記第１の識別情報と上記第３の識別情報との対応付けを記憶する第２のメモリを有し、
上記受信した接続要求に含まれる第２の識別情報を上記認証サーバに送信する送信部と、を有し、
上記認証サーバは、

上記第１のメモリから、上記アプリケーションサーバから受信した第２の識別情報に対応する第１の識別情報を読み出して、上記アプリケーションサーバに送信し、
上記アプリケーションサーバは、
上記第２のメモリの対応付けに基づいて取得する上記認証サーバから受信した第１の識別情報に対応する第３の識別情報と、上記接続要求に含まれる第３の識別情報が一致した場合に、上記端末に、前記接続要求に対する認証成功を通知するパケットを送信する、ことを特徴とするアクセス制御システム。
【請求項２】
端末に接続された、アプリケーションサーバ、および認証サーバを備えたアクセス制御システムであって、
上記認証サーバは、上記アプリケーションサーバが接続されたネットワークへのアクセスを上記端末に対して認可するための第１の認証を行う第１の認証手段を有し、
上記アプリケーションサーバは、上記第１の認証で上記ネットワークへのアクセスが許可された上記端末に対してサービスの利用を認可するための第２の認証を行う第２の認証手段を有し、
上記アプリケーションサーバは、上記端末が上記第１の認証に用いる第１の識別情報と、上記第２の認証に用いる第２の識別情報との対応関係に関する情報を保持する第１の情報保持手段を有し、
上記認証サーバーは、上記第１の認証によって上記ネットワークへのアクセスが許可された端末に対して付与され、上記端末から送信されるパケットに付加される第３の識別情報と、上記端末が用いる第１の識別情報との対応関係に関する情報を保持する第２の情報保持手段を有し、
上記アプリケーションサーバは、上記第２の情報保持手段に対して問い合わせを行い、上記第２の認証のためのパケットに含まれる第３の識別情報と対応関係を有する第１の識別情報を取得する第１の情報取得手段と、
上記第１の情報保持手段に対して問い合わせを行い、上記第１の情報取得手段が取得した第１の識別情報と対応関係を有する第２の識別情報を取得する第２の情報取得手段と、
上記第２の認証のためのパケットに含まれる第２の識別情報と、上記第２の情報取得手段が取得した第２の識別情報とを比較する情報比較手段と、を有する、ことを特徴とするアクセス制御システム。
【請求項３】
アプリケーションサーバとネットワークを介して接続され、端末から上記ネットワークへの認証を行う認証サーバであって、
上記端末から送信された上記ネットワークに接続するための認証に用いられる第１の識別情報を受信する受信部と、
上記第１の識別情報による認証が成功した場合に、上記端末に対して割り当てられる上記ネットワークにおける識別情報である第２の識別情報を送信する送信部と、
上記第１の識別情報と上記第２の識別情報とを対応付けて記憶するメモリを有し、
さらに、上記受信部は、上記端末から上記アプリケーションサーバに上記ネットワークを介して送信された接続要求に含まれ第２の識別情報を上記アプリケーションサーバから受信し、
上記送信部は、上記アプリケーションサーバから受信した第２の識別情報に対応する上記第１の識別情報を上記メモリから読み出して上記アプリケーションサーバに送信することを特徴とする認証サーバ。
【請求項４】
端末および認証サーバとネットワークを介して接続されたアプリケーションサーバであって、
上記端末が、上記ネットワークに接続するための認証に用いられる第１の識別情報を上記認証サーバに送信したのちに、上記端末から、上記認証に応じて上記端末に割り当てられる上記ネットワークにおける識別情報である第２の識別情報と、上記アプリケーション

サーバからサービスを受けるための第３の識別情報と、を受信する受信部と、
上記第１の識別情報と上記第３の識別情報を対応付けて記憶するメモリと、
上記接続要求に含まれる第２の識別情報を上記認証サーバに送信する送信部を有し、
上記認証サーバで管理される上記第２の情報に対応する第１の識別情報を取得した場合、上記取得した第１の識別情報に対応づけられる第３の識別情報を上記メモリから取得し、
上記メモリから取得した第３の識別情報と、上記端末から受信した第３の識別情報が一致した場合に、上記端末に対して認証成功を通知するパケットを送信する、ことを特徴とするアプリケーションサーバ。
【請求項５】
アプリケーションサーバ、および認証サーバに接続され、端末からのパケットをネットワークを介して転送するパケット転送装置であって、
上記端末が上記認証サーバに上記ネットワークに接続するための認証に用いられる第１の識別情報を送信したのちに、上記認証に応じて上記端末に対して割り当てられる上記ネットワークで識別される第２の識別情報と上記アプリケーションサーバからサービスを受けるための第３の識別情報を上記端末から受信する受信部と、
第１の識別情報と第３の識別情報を対応づけて記憶するメモリと、
上記受信した第３の情報に対応する上記メモリに記憶された上記第１の識別情報を上記認証サーバに送信する送信部を有し、
上記認証サーバから受信した上記第１の識別情報に対応する第２の識別情報と、上記端末受信した上記第２の識別情報が一致した場合に、上記端末から受信した上記第２の識別情報および上記第３の識別情報を上記アプリケーションサーバに送信するパケット転送装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アクセス制御方式、システム、装置、プログラム、ならびに記録媒体に関し、特に、ネットワークを介して提供されるサービスに対するアクセス制御を行うための方式、システム、装置、プログラム、ならびに記録媒体に関する。
【背景技術】
【０００２】
現在、インターネットや企業網（イントラネット）などのネットワークにおいて、様々なサービスが提供されている。ネットワーク上のサービスを利用するとき、利用者は、まず端末装置をネットワークに接続するが、その際にネットワークの運用主体による接続の許可が必要になる場合がある。このとき、ネットワークの運用主体は、接続の可否の判定のために、利用者の認証を行う。例えば、インターネットに接続するためには、ＩＳＰ(Internet Service Provider)による接続の許可を受ける必要がある。このときの認証は、例えばＰＰＰ(Point-to-Point Protocol)を用いて、ＩＳＰの利用者を特定するための識別情報と、それによって特定される利用者が本人に相違ないことを確認するためのパスワードを入力することで行われる（ＰＰＰについては、非特許文献１参照）。
【０００３】
別の例として、企業内でイントラネットに接続する際に、接続の許可を受けることが必要になる場合がある。このときの認証には、例えばIEEE 802.1x を用いて、イントラネットの利用者を特定するための識別情報と、パスワードを入力することで行われる。一方、ネットワーク上で提供されるサービスの中には、サービスを提供する対象を特定の利用者に限定するものや、個々の利用者に異なる内容のサービスを提供するものが存在する。このようなサービスにおいては、利用者を特定して利用権限を付与するため、利用者はサービス提供者による認証を受ける必要がある。このときの認証は、ネットワーク接続が確立された後に、例えばＨＴＴＰ(Hyper Text Transfer Protocol)のような、ＯＳＩ参照モデルの上位レイヤに位置するプロトコルを用いて、サービス利用者を特定するための識別

情報と、パスワードを入力することで行われる（ＨＴＴＰについては、非特許文献２参照）。なお、上記の認証において、本人に相違ないことを確認するための情報としては、パスワード以外に、公開鍵証明書や生体情報が用いられる場合もある。

【０００４】

ところで、サービスの利用のための認証を行うにあたり、他人の識別情報とパスワードなど本人性を確認するための情報を盗用し、それらの本来の所有者になりすましてサービスの利用を不正に行うことが問題となる。このようななりすましによって、覚えのない利用に対する課金や、機密情報の漏洩といった問題が発生する。本人性を確認する手段として生体情報を用いれば、他人による盗用は困難になる。しかし、生体情報を用いた認証は、特殊な装置やソフトウェアを必要とするため、現在のところ、利用範囲は、入退室管理など厳格な認証を必要とする用途に限られており、ネットワーク上で広く利用されるには至っていない。

【０００５】

ネットワーク接続のための認証および認可と、サービス利用のための認証および認可は、一般的には異なる運用主体が行っている。このため、各々の認証に用いる識別情報は異なっており、かつ、それらの異なる識別情報が同一人物のものであるか否かの検査は行われていない。したがって、例えばインターネットへの接続は自身が正当に所持する識別情報とパスワードで行い、サービスを利用するための識別情報とパスワードは他人のものを盗用した場合でも、当該サービスの利用は可能になる。これに対して、異なる識別情報の対応関係を検査することで、ネットワーク接続を許可された利用者とサービスを受けようとする利用者が同一人物であるか否かを判定し、なりすましへの対策を強化することが考えられる。どの段階の認証においても、認証・認可を受けると、利用者からそれ以降送信されるパケットには認証に使用する識別情報は含まれず、代わりに、認可された利用に対してのみ有効な一時的な識別情報が付与され、この識別情報がパケットに含まれることが多い。例えば、インターネットなど、ＩＰ(Internet Protocol)を使用するネットワークでは、この一時的な識別情報として、ネットワーク上の位置を表すＩＰアドレスがしばしば用いられる。そのため、ＩＰを使用するネットワーク上で提供されるサービスを利用するための認証を行う際、利用者から提供者に対しては、ネットワークへの接続を許可された結果として付与されたＩＰアドレスを送信元とするパケットによって、サービスを利用するための認証に用いる識別情報が送信される。

【０００６】

したがって、各々の利用者に対して、上記パケットの送信元のＩＰアドレスと、サービスを利用するための認証に使用する識別情報とを照合すれば、ネットワークへの接続を許可された利用者とサービスを受けようとする利用者が同一人物であるか否かを検査することができる。例えば、ネットワークサービスの利用者が使用する機器に、サービスを利用するための識別情報を下位６４ビットに含むＩＰｖ６(Internet Protocol version 6)アドレスを付与する決まりとし、サービスを利用する際には、利用者から提示されたサービス利用のための識別情報とＩＰｖ６アドレスとを比較し、ＩＰｖ６アドレスに利用者の識別情報が含まれるか否かを検査するという技術がある（例えば、特許文献１参照）。

【０００７】

【特許文献１】特開２００３－１３２０３０号公報

【０００８】

【非特許文献１】"The Point-to-Point Protocol (PPP)", RFC1661, IETF

【非特許文献２】"Hypertext Transfer Protocol -- HTTP/1.1", RFC2616, IETF

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかし、現状のネットワークでは、ＩＰアドレスとサービス利用のための識別情報との対応関係は、動的に変化するのが一般的である。

例えば、現在のインターネットや企業内のネットワークでは、ＩＰアドレスとしてＩＰｖ

４(Internet Protocol version 4)アドレスが用いられているが、世界的なアドレス不足が問題となっていることから、一度ある利用者に割り当てたアドレスを、不要になった後に別の利用者に割り当てるといったことが広く行われている。

そのため、特許文献１のような、ＩＰアドレスとサービス利用のための識別情報との対応関係が不変であることを前提とする方式は、ネットワーク上での同一人物性の検査には不十分である。

【課題を解決するための手段】

【００１０】

本発明は、上記の課題に鑑みてなされたものであり、

ネットワーク上で提供されるサービスの利用者が、ネットワークへの接続を許可するための第１の認証に使用する第１の識別情報と、サービスの利用を許可するための第２の認証に使用する第２の識別情報との対応関係を保持する手段と、

ネットワークへの接続を許可された利用者に付与される第３の識別情報と、当該利用者の第１の識別情報との対応関係を保持する手段と、

第２の認証のためのパケットに含まれる第２の識別情報と第３の識別情報との対応関係を検査する手段とを有する。

第２の識別情報と第３の識別情報との対応関係の検査を行う手段は、詳しくは２通りの実現方法があり、第１の実現方法によれば、

第１の識別情報と第３の識別情報との対応関係を保持する手段に対して問合せを行い、第２の認証のためのパケットに含まれる第３の識別情報と対応関係を有する第１の識別情報を取得する手段と、

第１の識別情報と第２の識別情報との対応関係を保持する手段に対して問合せを行い、上記によって取得した第１の識別情報と対応関係を有する第２の識別情報を取得する手段と、

上記によって取得した第２の識別情報と、第２の認証のためのパケットに含まれる第２の識別情報とを比較する手段により構成される。

また、第２の実現方法によれば、第２の識別情報と第３の識別情報との対応関係を検査する手段は、

第１の識別情報と第２の識別情報との対応関係を保持する手段に対して問合せを行い、第２の認証のためのパケットに含まれる第２の識別情報と対応関係を有する第１の識別情報を取得する手段と、

第１の識別情報と第３の識別情報との対応関係を保持する手段に対して問合せを行い、上記によって取得した第１の識別情報と対応関係を有する第３の識別情報を取得する手段と、

上記によって取得した第３の識別情報と、第２の認証のためのパケットに含まれる第３の識別情報とを比較する手段により構成される。

【発明の効果】

【００１１】

本発明では、ネットワークへの接続が認可されたときに一時的に付与される識別情報と、サービス利用の認可を受けるための認証に使用する識別情報との対応関係の検査を行うため、インターネットのように発信者のアドレスが一定でないネットワークにおいても、他人になりすますことによるサービスの不正利用を低減することができる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明の実施の形態を図面を用いて説明する。

【実施例１】

【００１３】

図１は、本発明の第１の実施形態におけるシステム構成を示した図である。ユーザ端末１は、ＣＰＵ、メモリおよびユーザインタフェースからなる計算機である。ゲートウェイ装置２ａは、パケット送受信部２１ａ、認証クライアント部２２により構成される。パケ

ット送受信部２１ａは、論理回路およびメモリを有し、ネットワークから受信したパケットのヘッダを解析し、その結果に応じて、パケットの転送や、認証クライアント部２２への処理の振り分けを行う。また、認証クライアント部２２から処理を終えて返送されたパケットを、ネットワークに送出する。認証クライアント部２２は、ＣＰＵおよびメモリを有し、ネットワーク１００に接続するためのＩＤとパスワードを含むパケットをパケット送受信部２１ａから受信し、ＩＤとパスワードを抽出して認証サーバ３に送信する。また、認証サーバ３から処理結果を受信し、その内容に基づいた応答メッセージを生成して、パケット送受信部２１ａを介して利用者に送信する。認証サーバ３は、ＣＰＵ，メモリ、磁気ディスク装置およびインタフェースを有し、各種ソフトウェアが動作することによって、認証・認可処理部３１、ＩＰアドレス・ＩＤデータベース３２、ＩＤ・パスワードデータベース３３を構成している。認証・認可処理部３１は、ゲートウェイ装置の認証クライアント部から、ネットワーク１００に接続しようとする利用者が入力したユーザＩＤとパスワードを受信し、ＩＤ・パスワードデータベース３３を参照して対照表３３１に記録されている内容と比較して、その結果を認証クライアント部に通知する機能を有する。さらに、認証・認可処理部３１は、認証クライアント部から受信した内容と、対照表３３１に記録されている内容とが一致していれば、ネットワーク１００への接続を許可し、当該利用者のユーザ端末に対して、ＩＰアドレスを割り当てて、そのＩＰアドレスをＩＰアドレス・ＩＤデータベース３２に登録する機能を有する。ＩＰアドレス・ＩＤデータベース３２は、ネットワーク１００の利用者を識別するユーザＩＤと、各々の利用者にネットワーク１００への接続を許可したときに付与したＩＰアドレスとの対照表３２２と、対照表３２２の情報の読み出しや書き換えを行うソフトウェアにより構成されている。

【００１４】

図２に対照表３２１の内容を示す。対照表３２１は、ネットワーク１００の利用者のユーザＩＤを記録する領域３２２と、ＩＰアドレスを記録する領域３２３を有する。領域３２３の内容は、利用者がネットワーク１００への接続を開始するたびに変化する。また、ネットワーク１００への接続を行っていない利用者については、領域３２３は空欄となる。ＩＤ・パスワードデータベース３３は、ネットワーク１００の利用者を識別するユーザＩＤと、各々の利用者が本人に相違ないことを確認するためのパスワードとの対照表３３１と、対照表３３１の情報の読み出しや書き換えを行うソフトウェアにより構成されている。この対照表３２１を参照することによって、ネットワーク１００へアクセスしようとするユーザが用いているＩＰアドレスがどのユーザに割当てられたものかを検出することができる。

【００１５】

図３に対照表３３１の内容を示す。対照表３３１は、ネットワーク１００の利用者のユーザＩＤを記録する領域３３２と、パスワードを記録する領域３３３を有する。領域３３３の内容は、他人に知られることを防止するために、暗号化されている。Ｗｅｂサーバ４ａは、ＣＰＵ、メモリ、磁気ディスク装置およびインタフェースを有する計算機であり、各種ソフトウェアが動作することによって、Ｗｅｂサーバプログラム４１ａ、認証・認可処理部４２ａ、ＩＤ検査部４３、ＩＤデータベース４４、ＩＤ・パスワードデータベース４５を構成している。Ｗｅｂサーバプログラム４１ａは、受信したＨＴＴＰのパケットを解析し、必要な応答メッセージを生成して送信元に返送する。受信したＨＴＴＰのパケットが、Ｗｅｂサーバ４ａに接続するためのＩＤとパスワードを含む場合には、Ｗｅｂサーバ４ａはそのパケットを認証・認可処理部４２ａならびにＩＤ検査部４３に渡し、これらの機能部から通知された処理結果に基づいて応答メッセージを生成する。ＩＤ検査部４３は、パケット解析部４３１、ネットワーク接続用ＩＤ問合せ部４３２、Ｗｅｂサーバ接続用ＩＤ問合せ部４３３、ＩＤ比較部４３４により構成されている。パケット解析部４３１は、利用者が認証を受けるために送信したパケットの内容を解析してＷｅｂサーバ４ａへの接続のために使用するＩＤを抽出し、ＩＤ比較部４３４に渡す。また、同じパケットから送信元のＩＰアドレスを抽出し、ネットワーク接続用ＩＤ問合せ部４３２に渡す。ネットワーク接続用ＩＤ問合せ部４３２は、パケット解析部４３１によって抽出されたＩＰア

ドレスを付与された利用者がネットワーク１００への接続のために使用するＩＤを、ＩＰアドレス・ＩＤデータベース３２に対して問い合わせ、その結果として取得したＩＤをＷｅｂサーバ接続用ＩＤ問合せ部４３３に渡す。Ｗｅｂサーバ接続用ＩＤ問合せ部４３３は、ネットワーク接続用ＩＤ問合せ部４３２が取得したネットワーク１００への接続のためのＩＤを使用する利用者がＷｅｂサーバ４ａへの接続のために使用するＩＤを、ＩＤデータベース４４に対して問い合わせ、その結果として取得したＩＤをＷｅｂサーバ接続用ＩＤ比較部４３４に渡す。Ｗｅｂサーバ接続用ＩＤ比較部４３４は、パケット解析部４３１から通知されたＩＤと、Ｗｅｂサーバ接続用ＩＤ問合せ部４３３から通知されたＩＤとを比較して、両者が一致しているか否かを検査し、その結果を認証・認可処理部４２ａに渡す。この構成により、ネットワーク１００にアクセスを許されたユーザからのアクセスか否かを判定することができる。認証・認可処理部４２ａは、Ｗｅｂサーバ接続用ＩＤ比較部４３４におけるＩＤの比較の結果の通知を受信し、ＩＤが一致していれば、Ｗｅｂサーバプログラム４１ａから受信した認証のためのＨＴＴＰパケットに含まれるＩＤとパスワードを抽出して、それらがＩＤ・パスワードデータベース４５に登録されている内容と一致しているか否かを検査し、その結果をＷｅｂサーバプログラム４１ａに通知する。また、ＩＤが一致していなければ、認証に失敗したことを示す通知をＷｅｂサーバプログラム４１ａに対して行う。この構成により、ネットワーク１００にアクセスを許されたユーザが、当該サーバの提供するサービスを受けられるユーザか否かを判定することができる。

【００１６】

ＩＤデータベース４４は、ネットワーク１００への接続の利用者を識別するユーザＩＤと、Ｗｅｂサーバ４ａの利用者を識別するユーザＩＤの対照表４４１と、対照表４４１の情報の読み出しや書き換えを行うソフトウェアにより構成されている。

図４に対照表４４１の内容を示す。対照表４４１は、ネットワーク１００の利用者のユーザＩＤを記録する領域４４２と、Ｗｅｂサーバ４ａの利用者のユーザＩＤを記録する領域４４３とを有する。

ＩＤ・パスワードデータベース４５は、Ｗｅｂサーバ４ａの利用者のユーザＩＤと、各々の利用者が本人に相違ないことを確認するためのパスワードとの対照表４５１と、対照表４５１の情報の読み出しや書き換えを行うソフトウェアにより構成されている。

【００１７】

図５に対照表４５１の内容を示す。対照表４５１は、Ｗｅｂサーバ４ａの利用者のユーザＩＤを記録する領域４５２と、パスワードを記録する領域４５３を有する。領域４５３の内容は、他人に知られることを防止するために、暗号化されている。

なお、Ｗｅｂサーバ４ａは、図６のフローチャートに示す手順で処理を行うプログラムを計算機上で動作させることによっても実現可能であり、必ずしも図１に示す構成をとらなくても良い。

【００１８】

以下、図６のフローチャートについて説明する。Ｗｅｂサーバ４ａは、自身に宛てたＨＴＴＰパケットを受信すると（ステップ１０１Ａ）、まず受信パケットの内容を解析し、受信したパケットが、Ｗｅｂサーバ４ａに接続するために用いるＩＤおよびパスワードを含むものであるか否かを判定する（ステップ１０２Ａ）。もしＷｅｂサーバ４ａへの接続に用いるＩＤおよびパスワードを含むパケットでない場合には、ＨＴＴＰによる要求に対する応答処理を行い（ステップ１０８Ａ）、その結果をＨＴＴＰパケットの送信元に返送する（ステップ１１１Ａ）。一方、ＩＤおよびパスワードを含むパケットである場合には、受信したパケットから、送信元のＩＰアドレス、およびＷｅｂサーバ４ａへの接続に用いるＩＤの抽出を行う（ステップ１０３Ａ）。次に、抽出されたＩＰアドレスを用いて、このアドレスを割り当てられた利用者がネットワーク１００への接続のために用いるＩＤを取得する（ステップ１０４Ａ）。ネットワーク１００への接続のためのＩＤの取得に失敗した場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１１０Ａ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１１Ａ）。ネットワーク１００への接続のためのＩＤの取得に成功した場合には、取得したＩＤを使用する利用

者がＷｅｂサーバ４ａに接続するために用いるＩＤを取得する（ステップ１０５Ａ）。Ｗｅｂサーバ４ａへの接続のためのＩＤの取得に失敗した場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１１０Ａ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１１Ａ）。Ｗｅｂサーバ４ａへの接続のためのＩＤの取得に成功した場合には、取得したＩＤと、先にＨＴＴＰパケットから抽出されたＩＤとを比較する（ステップ１０６Ａ）。比較の結果、両者のＩＤが一致しない場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１１０Ａ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１１Ａ）。両者のＩＤが一致した場合には、ＨＴＴＰパケットに含まれるＩＤとパスワードを用いて認証を行い（ステップ１０７Ａ）、その結果に基づいて認証に成功または失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１０９Ａ、１１０Ａ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１１Ａ）。

【００１９】

以下、図１に示した本発明の第１の実施形態におけるシステムの動作について、図７、図８、図９に示すシーケンス図を用いて説明する。ユーザ端末１からネットワーク１００を介してＷｅｂサーバ４ａに接続しようとする利用者は、まずゲートウェイ装置２に接続要求を行う（ステップ１Ａ）。ゲートウェイ装置２ａは、接続要求を受信すると、利用者に対して、ユーザＩＤとパスワードの入力を要求する（ステップ２Ａ）。これに対し、利用者は、ネットワーク１００への接続において有効なユーザＩＤとパスワードを入力する。入力されたユーザＩＤとパスワードはパケット化され、ユーザ端末１からゲートウェイ装置２に送信される（ステップ３Ａ）。ゲートウェイ装置２では、パケット送受信部２１がこのパケットを受信し、ユーザＩＤとパスワードを含むパケットであると判断して、認証クライアント部２２に渡す（ステップ４Ａ）。認証クライアント部２２は、渡されたパケットからユーザＩＤとパスワードを抽出し、認証サーバ３に渡す（ステップ５Ａ）。認証サーバ３は、認証・認可処理部３１において、ゲートウェイ装置２ａから渡されたユーザＩＤとパスワードを、ＩＤ・パスワードデータベース３３に登録されている内容と比較し、ともに一致していれば、利用者に対してゲートウェイ装置２ａを介したインターネット１００への接続を許可する。このとき、認証・認可処理部３１は、利用者に対して、ユーザ端末１が使用するＩＰアドレスを割り当てる（ステップ６Ａ）。さらに、割り当てたＩＰアドレスの値と、割り当てた先の利用者のＩＤとを対応付けて、ＩＰアドレス・ＩＤデータベース３２に登録する（ステップ７Ａ、８Ａ、９Ａ）。ネットワーク１００への接続を許可された利用者は、次に、Ｗｅｂサーバ４ａに対して接続要求を行う（ステップ１３Ａ、１４Ａ）。Ｗｅｂサーバ３は、接続要求を受信すると、利用者に対して、ユーザＩＤとパスワードの入力を要求するＷｅｂページを送信する（ステップ１５Ａ、１６Ａ）。これに対し、利用者は、Ｗｅｂサーバ４ａへの接続において有効なユーザＩＤとパスワードを入力する。このユーザＩＤおよびパスワードは、ＳＳＬ(Secure Socket Layer)を用いて暗号化されたＨＴＴＰパケットによって、ユーザ端末１からＷｅｂサーバ４ａに送信される（ステップ１７Ａ、１８Ａ）。Ｗｅｂサーバ４ａでは、Ｗｅｂサーバプログラム４１ａがこのパケットを受信し、内容を解析した結果（ステップ１９Ａ）、認証を受けるためのユーザＩＤとパスワードを含むパケットであると判断して、パケット解析部４３１に渡す（ステップ２０Ａ）。パケット解析部４３１は、前記パケットを解析して送信元のＩＰアドレスを抽出し（ステップ２１Ａ）、ネットワーク接続用ＩＤ問合せ部４３２に渡す（ステップ２２Ａ）。ネットワーク接続用ＩＤ問合せ部４３２は、ＩＰアドレス・ＩＤデータベース３２に対して問合せを行い（ステップ２３Ａ）、ステップ２２Ａにてパケット解析部４３１から渡されたＩＰアドレスに対応付けられたネットワーク１００への接続のためのユーザＩＤを取得する（ステップ２４Ａ）。取得したユーザＩＤは、Ｗｅｂサーバ接続用ＩＤ問合せ部４３３に渡される（ステップ２５Ａ）。Ｗｅｂサーバ接続用ＩＤ問合せ部４３３は、ＩＤデータベース４４に対して問合せを行い（ステップ２６Ａ）、ステップ２５Ａにてネットワーク接続用ＩＤ問合せ部４３２から渡されたネットワーク１００への接続のためのユーザＩＤに対応付けられた、Ｗｅｂサーバ４ａへの接続のためのユーザ

ＩＤを取得する（ステップ２７Ａ）。取得したユーザＩＤは、ＩＤ比較部４３４に渡される（ステップ２８Ａ）。ステップ２２Ａないし２８Ａと並行して、パケット解析部４３１は、ステップ２０ＡにてＷｅｂサーバプログラム４１から渡されたパケットを解析してユーザＩＤを抽出し（ステップ２９Ａ）、ＩＤ比較部４３４に渡す（ステップ３０Ａ）。ＩＤ比較部４３４は、ステップ２８ＡにてＷｅｂサーバ接続用ＩＤ問合せ部４３４から渡されたユーザＩＤと、ステップ３０Ａにてパケット解析部４３１から渡されたユーザＩＤとを比較し（ステップ３１Ａ）、両者の値が一致しているか否かを、認証・認可処理部４２ａに通知する（ステップ３２Ａ）。認証・認可処理部４２ａは、ステップ３２Ａにて、前記２つのユーザＩＤの値が一致している旨の通知を受信すると、ユーザ端末１から受信したユーザＩＤとパスワードを用いて、認証処理を行う。また、認証処理の結果に応じて、Ｗｅｂサーバ４ａによって提供されるサービスの利用認可を行い（ステップ３３Ａ）、その結果をＷｅｂサーバプログラム４１ａに通知する（ステップ３４Ａ）。Ｗｅｂサーバプログラム４１ａは、ステップ３４Ａにて認証・認可処理部４２ａから通知された利用認可の結果に従って、ステップ１３Ａ、１４Ａの接続要求に対する応答を、ユーザ端末１に返送する（ステップ３５Ａ、３６Ａ）。

【実施例２】

【００２０】

図１０は、本発明の第２の実施形態におけるシステム構成を示した図である。

なお、前述した第１の実施の形態と同一の構成には同一の符号を付し、その詳細な説明は省略する。ゲートウェイ装置２ｂは、パケット送受信部２１ｂ、認証クライアント部２２、ＩＤ検査部２３により構成される。パケット送受信部２１ｂは、論理回路あるいはＣＰＵを有し、ネットワークから受信したパケットのヘッダを解析し、その結果に応じて、パケットの転送や、認証クライアント部２２やＩＤ検査部２３への処理の振り分けを行う。また、認証クライアント部２２やＩＤ検査部２３から処理を終えて返送されたパケットを、ネットワークに送出する。

【００２１】

ＩＤ検査部２３は、ＣＰＵおよびメモリを有し、各種ソフトウェアが動作することによって、パケット解析部２３１、ネットワーク接続用ＩＤ問合せ部２３２、ＩＰアドレス問合せ部２３３、ＩＰアドレス比較部２３４、応答生成部２３５を構成している。パケット解析部２３１は、利用者から受信したＷｅｂサーバ４ｂへの接続の際の認証を受けるためのパケットの内容を解析して送信元のＩＰアドレスを抽出し、ＩＰアドレス比較部２６５ｂに渡す。また、同じパケットからＷｅｂサーバ４ｂへの接続のために使用するＩＤを抽出し、ネットワーク接続用ＩＤ問合せ部２３２に渡す。さらに、受信したパケットを応答生成部２３５に転送する。ネットワーク接続用ＩＤ問合せ部２３２は、パケット解析部２３１によって抽出されたＷｅｂサーバ４ｂへの接続のためのＩＤを使用する利用者が、ネットワーク１００への接続のために使用するＩＤを、ＩＤデータベース４４に対して問い合わせ、その結果として取得したＩＤをＩＰアドレス問合せ部２３３に渡す。ＩＰアドレス問合せ部２３３は、ネットワーク接続用ＩＤ問合せ部２３２が取得したネットワーク１００への接続のためのＩＤを使用する利用者に付与されたＩＰアドレスを、ＩＰアドレス・ＩＤデータベース３２に対して問い合わせ、その結果として取得したＩＰアドレスをＩＰアドレス比較部２３４に渡す。ＩＰアドレス比較部２３４は、パケット解析部２３１から通知されたＩＰアドレスと、ＩＰアドレス問合せ部２３３から通知されたＩＰアドレスとを比較して、両者が一致しているか否かを検査し、その結果をパケット転送部２３５に渡す。応答生成部２３５は、パケット解析部３１から転送されたパケットを保持しておく。また、ＩＰアドレス比較部２３４によるＩＰアドレスの比較の結果を受信し、一致している場合には、保持しているパケットをＷｅｂサーバ４ｂに転送する。一致していない場合には、保持しているパケットに対して認証に失敗したことを示す応答メッセージを生成し、パケットの送信元に返送する。Ｗｅｂサーバ４ｂは、ＣＰＵ、メモリ、磁気ディスク装置およびインタフェースを有し、各種ソフトウェアが動作することによって、Ｗｅｂサーバプログラム４１ｂ、認証・認可処理部４２ｂ、ＩＤ・パスワードデータベース４５を

構成している。Ｗｅｂサーバプログラム４１ｂは、受信したＨＴＴＰのパケットを解析し、必要な応答メッセージを生成して送信元に返送する。受信したＨＴＴＰのパケットが、Ｗｅｂサーバ４ｂに接続するためのＩＤとパスワードを含む場合には、そのパケットを認証・認可処理部４２ｂに渡し、この機能部から通知された処理結果に基づいて応答メッセージを生成する。認証・認可処理部４２ｂは、Ｗｅｂサーバプログラム４１ｂから受信した認証のためのＨＴＴＰパケットに含まれるＩＤとパスワードを抽出して、それらがＩＤ・パスワードデータベース４５に登録されている内容と一致しているか否かを検査し、その結果をＷｅｂサーバプログラム４１ｂに通知する。ＩＤデータベースサーバ５は、ＣＰＵ、メモリ、磁気ディスク装置およびインタフェースを有し、各種ソフトウェアが動作することによって、ＩＤデータベース４４を構成している。なお、ゲートウェイ装置２ｂは、図１１のフローチャートに示す手順で処理を行うプログラムを計算機上で動作させることによっても実現可能であり、必ずしも図１０に示す構成をとらなくても良い。

【００２２】

以下、図１１のフローチャートについて説明する。ゲートウェイ装置２ｂは、パケットを受信すると（ステップ１０１Ｂ）、まず、受信パケットの内容を解析し、受信したパケットが、ネットワーク１００に接続するために用いるＩＤおよびパスワードを含むものであるか否かを判定する（ステップ１０２Ｂ）。もしネットワーク１００に接続するためのＩＤおよびパスワードを含むパケットである場合には、ネットワーク１００への接続のための認証を行い（ステップ１０４Ｂ）、その結果をパケットの送信元に返送する（ステップ１１０Ｂ）。一方、ネットワーク１００に接続するためのＩＤおよびパスワードを含むパケットでない場合には、次に、このパケットがＷｅｂサーバ４ｂに接続するためのＩＤおよびパスワードを含むものであるか否かを判定する（ステップ１０３Ｂ）。もしＷｅｂサーバ４ｂへの接続に用いるＩＤおよびパスワードを含むパケットでない場合には、そのパケットをそのままＷｅｂサーバ４ｂに転送する（ステップ１１１Ｂ）。一方、Ｗｅｂサーバ４ｂへの接続に用いるＩＤおよびパスワードを含むパケットである場合には、受信したパケットから、送信元のＩＰアドレス、およびＷｅｂサーバ４ｂへの接続に用いるＩＤの抽出を行う（ステップ１０５Ｂ）。次に、抽出されたＩＤを用いて、このＩＤを使用する利用者がネットワーク１００への接続のために用いるＩＤを取得する（ステップ１０６Ｂ）。ネットワーク１００への接続のためのＩＤの取得に失敗した場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１０９Ｂ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１２Ｂ）。ネットワーク１００への接続のためのＩＤの取得に成功した場合には、取得したＩＤを使用する利用者に割り当てられているＩＰアドレスを取得する（ステップ１０７Ｂ）。ＩＰアドレスの取得に失敗した場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１０９Ｂ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１２Ｂ）。ＩＰアドレスの取得に成功した場合には、取得したＩＰアドレスと、先にＨＴＴＰパケットから抽出されたＩＰアドレスとを比較する（ステップ１０８Ｂ）。比較の結果、両者のＩＰアドレスが一致しない場合には、認証に失敗したことを示すＨＴＴＰの応答メッセージを生成し（ステップ１０９Ｂ）、ＨＴＴＰパケットの送信元に返送する（ステップ１１２Ｂ）。両者のＩＰアドレスが一致した場合には、ＨＴＴＰパケットをＷｅｂサーバ４ｂに転送する（ステップ１１１Ｂ）。

【００２３】

以下、図１０に示した本発明の第２の実施形態におけるシステムの動作について、図１２、図１３、図１４に示すシーケンス図を用いて説明する。ユーザ端末１からネットワーク１００を介してＷｅｂサーバ４ｂに接続しようとする利用者は、まずゲートウェイ装置２ｂに接続要求を行う（ステップ１Ｂ）。ゲートウェイ装置２ｂは、接続要求を受信すると、利用者に対して、ユーザＩＤとパスワードの入力を要求する（ステップ２Ｂ）。これに対し、利用者は、ネットワーク１００への接続のみにおいて有効なユーザＩＤとパスワードを入力する。入力されたユーザＩＤとパスワードはパケット化され、ユーザ端末１からゲートウェイ装置２に送信される（ステップ３Ｂ）。ゲートウェイ装置２ｂでは、パケ

ット送受信部２１ｂがこのパケットを受信し、ユーザＩＤとパスワードを含むパケットであると判断して、認証クライアント部２２に渡す（ステップ４Ｂ）。認証クライアント部２２は、渡されたパケットからユーザＩＤとパスワードを抽出し、認証サーバ３に渡す（ステップ５Ｂ）。認証サーバ３の動作は、第１の実施形態における認証サーバ３と同一であるため、ここでは説明を省略する。インターネット１００への接続を許可された利用者は、次に、Ｗｅｂサーバ４ｂに対して接続要求を行う（ステップ１３Ｂ、１４Ｂ）。Ｗｅｂサーバ４ｂは、接続要求を受信すると、利用者に対して、ユーザＩＤとパスワードの入力を要求するＷｅｂページを送信する（ステップ１５Ｂ、１６Ｂ）。これに対し、利用者は、Ｗｅｂサーバ４ｂへの接続のみにおいて有効なユーザＩＤとパスワードを入力する。このユーザＩＤおよびパスワードは、ＨＴＴＰパケットによって、ユーザ端末１からゲートウェイ装置２ｂに送信される（ステップ１７Ｂ）。ゲートウェイ装置２ｂでは、パケット送受信部２１ｂがこのパケットを受信し、内容を解析した結果（ステップ１８Ｂ）、Ｗｅｂサーバ４ｂでの認証を受けるためのユーザＩＤとパスワードを含むパケットであると判断して、パケット解析部２３１に渡す（ステップ１９Ｂ）。パケット解析部２３１は、前記パケットに含まれるＷｅｂサーバ４ｂへの接続に用いるユーザＩＤを抽出し（ステップ２０Ｂ）、ネットワーク接続用ＩＤ問合せ部２３２に渡す（ステップ２１Ｂ）。ネットワーク接続用ＩＤ問合せ部２３２は、ＩＤデータベース４４に対して問合せを行い（ステップ２２Ｂ）、ステップ２１Ｂにてパケット解析部２３１から渡されたＷｅｂサーバ４ｂへの接続のためのユーザＩＤに対応付けられた、ネットワーク１００への接続のためのユーザＩＤを取得する（ステップ２３Ｂ）。取得したユーザＩＤは、ＩＰアドレス問合せ部２３３に渡される（ステップ２４Ｂ）。ＩＰアドレス問合せ部２３３は、ＩＰアドレス・ＩＤデータベース３２に対して問合せを行い（ステップ２５Ｂ）、ステップ２４Ｂにてネットワーク接続用ＩＤ問合せ部２３２から渡されたユーザＩＤに対応付けられたＩＰアドレスを取得する（ステップ２６Ｂ）。取得したＩＰアドレスは、ＩＰアドレス比較部２３４に渡される（ステップ２７Ｂ）。ステップ２１Ｂないし２７Ｂと並行して、パケット解析部２３１は、ステップ１６ｂにてパケット送受信部２２から渡されたパケットの送信元のＩＰアドレスを抽出し（ステップ２８Ｂ）、ＩＰアドレス比較部２３４に渡す（ステップ２９Ｂ）。パケット解析部２３１は、ステップ２１Ｂおよび２８Ｂにおける解析処理が終了すると、パケットを応答生成部２３５に転送する（ステップ３０Ｂ）。応答生成部２３５では、転送されたパケットを保持する。ＩＰアドレス比較部２３４は、ステップ２７ＢにてＩＰアドレス問合せ部２３３から渡されたＩＰアドレスと、ステップ２９Ｂにてパケット解析部２３１から渡されたＩＰアドレスとを比較し（ステップ３１Ｂ）、両者の値が一致しているか否かを、応答生成部２３５に渡す（ステップ３２Ｂ）。応答生成部２３５は、ステップ３２Ｂにて、前記２つのＩＰアドレスの値が一致している旨の通知を受信すると、ステップ３０Ｂにてパケット解析部２３１から受信したパケットを、パケット送受信部２１ｂを介してＷｅｂサーバ４ｂに転送する（ステップ３３Ｂ、３４Ｂ）。Ｗｅｂサーバ４ｂでは、Ｗｅｂサーバプログラム４１ｂがこのパケットを受信し、内容を解析した結果（ステップ３５Ｂ）、認証を受けるためのユーザＩＤとパスワードを含むパケットであると判断して、認証・認可処理部４２ｂに渡す（ステップ３６Ｂ）。認証・認可処理部４２ｂは、ステップ３６Ｂにて受信したパケットに含まれるユーザＩＤおよびパスワードを用いて認証処理を行い、その結果に応じて、Ｗｅｂサーバ４ｂによって提供されるサービスの利用認可を行う（ステップ３７Ｂ）。また、認証・認可処理の結果をＷｅｂサーバプログラム４１ｂに通知する（ステップ３８Ｂ）。Ｗｅｂサーバプログラム４１ｂは、ステップ３８Ｂにて認証・認可処理部４２ｂから通知された利用認可の結果に従って、ステップ１３Ｂ、１４Ｂの接続要求に対する応答を、ユーザ端末１に返送する（ステップ３９Ｂ、４０Ｂ）。本発明の第２の実施形態は、ゲートウェイ装置が２種類のＩＤの対応関係を検査するため、Ｗｅｂサーバは既存のものを変更することなくそのまま利用できることが利点として挙げられる。

【産業上の利用可能性】

【００２４】

本発明は、ゲートウェイ装置やアプリケーションサーバ装置、およびこれらの装置からなる情報処理システムに適用することができ、ゲートウェイ装置とアプリケーションサーバの各々において認証が必要なシステムに適用すると好適である。

【図面の簡単な説明】

【００２５】

【図１】本発明の第１の実施形態における情報処理システムの構成を示すブロック図。

【図２】ネットワークへの接続のために用いるユーザＩＤと、ネットワークへの接続を許可された利用者に付与されるＩＰアドレスとの対照表。

【図３】ネットワークへの接続のために用いるユーザＩＤとパスワードの対照表。

【図４】ネットワークへの接続のために用いるユーザＩＤと、Ｗｅｂサーバへの接続のために用いるユーザＩＤとの対照表。

【図５】Ｗｅｂサーバへの接続のために用いるユーザＩＤとパスワードの対照表。

【図６】本発明の第１の実施形態におけるＷｅｂサーバの動作手順を示すフローチャート。

【図７】本発明の第１の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その１。

【図８】本発明の第１の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その２。

【図９】本発明の第１の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その３。

【図１０】本発明の第２の実施形態における情報処理システムの構成を示すブロック図。

【図１１】本発明の第２の実施形態におけるゲートウェイ装置の動作手順を示すフローチャート。

【図１２】本発明の第２の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その１。

【図１３】本発明の第２の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その２。

【図１４】本発明の第２の実施形態における情報処理システムの全体の動作手順を示すシーケンス図その３。

【符号の説明】

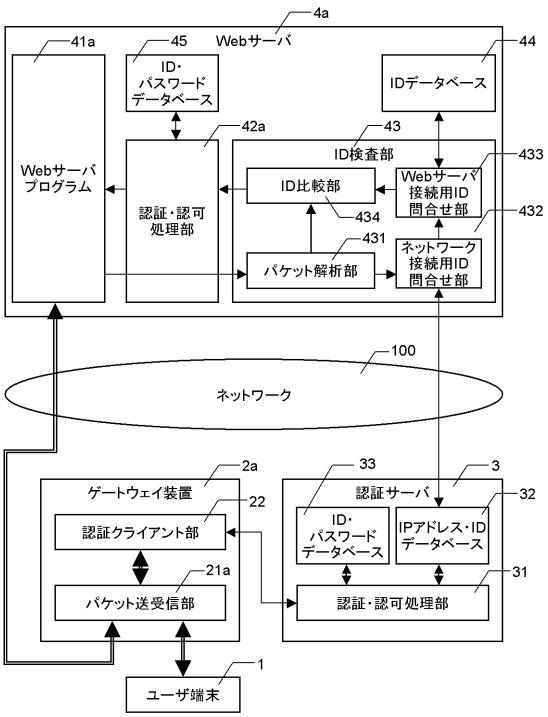
【００２６】

１…ユーザ端末
１００…ネットワーク
２ａ…ゲートウェイ装置
２１ａ…パケット送受信部
２２…認証クライアント部
３…認証サーバ
３１…認証・認可処理部
３２…ＩＰアドレス・ＩＤデータベース
３２１…ユーザＩＤとＩＰアドレスの対照表
３２２…ユーザＩＤを記録する領域
３２３…ＩＰアドレスを記録する領域
３３…ＩＤ・パスワードデータベース
３３１…ユーザＩＤとパスワードの対照表
３３２…ユーザＩＤを記録する領域
３３３…パスワードを記録する領域４ａ…Ｗｅｂサーバ
４１ａ…Ｗｅｂサーバプログラム
４２ａ…認証・認可処理部
４３…ＩＤ検査部
４３１…パケット解析部

４３２…ネットワーク接続用ＩＤ問合せ部
４３３…Ｗｅｂサーバ接続用ＩＤ問合せ部
４３４…ＩＤ比較部
４４…ＩＤデータベース
４４１…ネットワーク接続用ＩＤとＷｅｂサーバ接続用ＩＤの対照表
４４２…ネットワーク接続用ＩＤを記録する領域
４４３…Ｗｅｂサーバ接続用ＩＤを記録する領域
４５…ＩＤ・パスワードデータベース
４５１…ユーザＩＤとパスワードの対照表
４５２…ユーザＩＤを記録する領域
４５３…パスワードを記録する領域
２ｂ…ゲートウェイ装置
２１ｂ…パケット送受信部
２３…ＩＤ検査部
２３１…パケット解析部
２３２…ネットワーク接続用ＩＤ問合せ部
２３３…ＩＰアドレス問合せ部
２３４…ＩＰアドレス比較部
２３５…応答生成部
４ｂ…Ｗｅｂサーバ
４１ｂ…Ｗｅｂサーバプログラム
４２ｂ…認証・認可処理部
５…ＩＤデータベース。

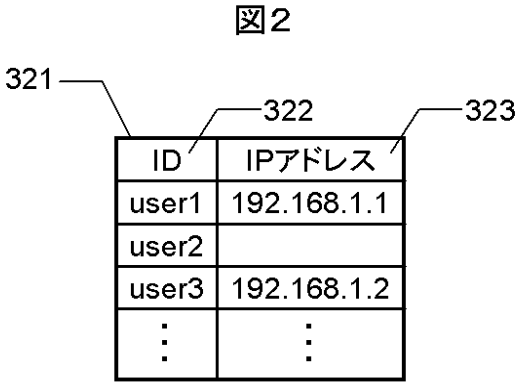
【図１】

図1



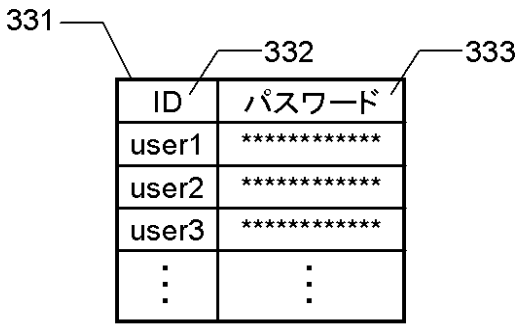
【図２】

図2



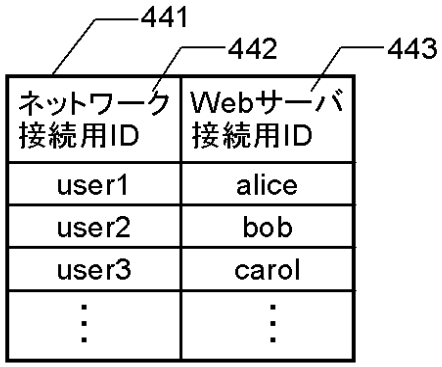
【図３】

図3



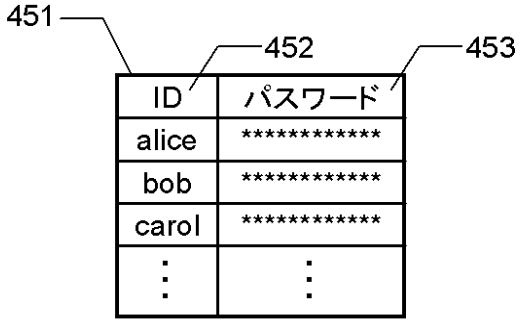
【図４】

図4



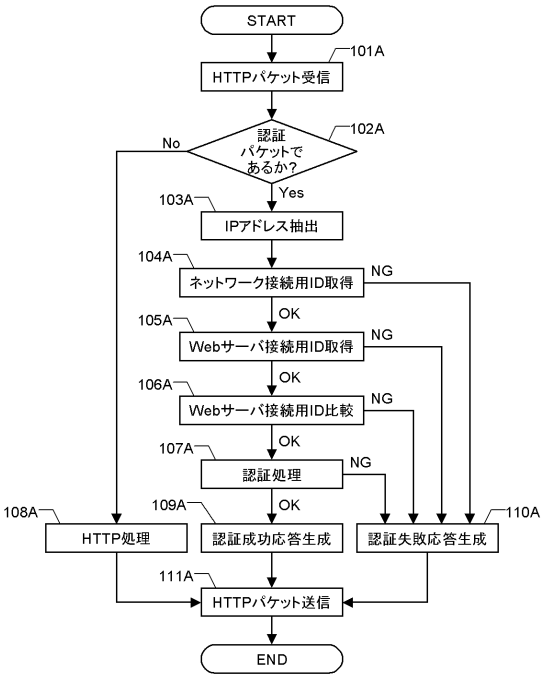
【図５】

図5



【図６】

図6



【図７】

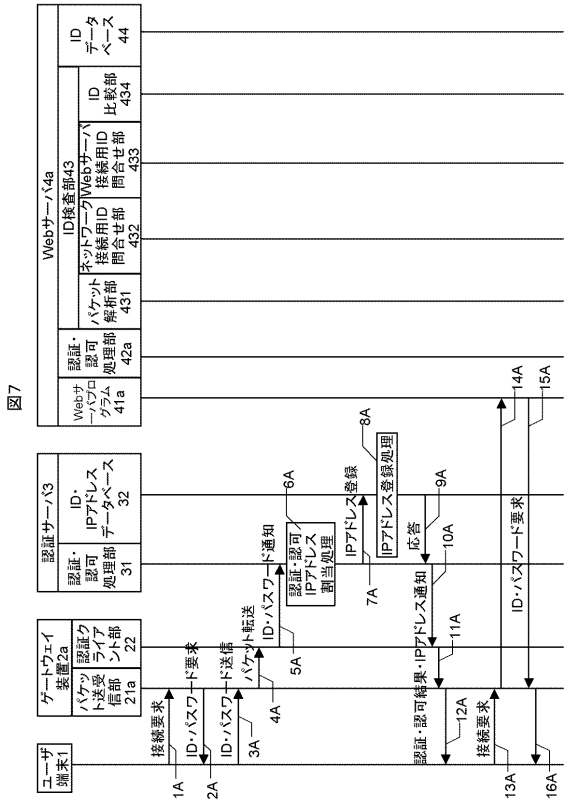


図7
Webサーバ4a
ID検査部43
ネットワーク接続用ID問合せ部 432
Webサーバ接続用ID問合せ部 433
IDデータベース 44
IDアドレスデータベース 32
認証・認可処理部 31
認証・認可処理部 42a
認証クライアント部 22
パケット送受信部 21a
ユーザ端末1
接続要求
ID・パスワード要求
ID・パスワード送信
パケット転送
ID・パスワード通知
認証・認可IPアドレス割当処理
IPアドレス登録
IPアドレス登録処理
応答
IPアドレス通知
認証・認可結果・IPアドレス通知
ID・パスワード要求
接続要求

【図８】

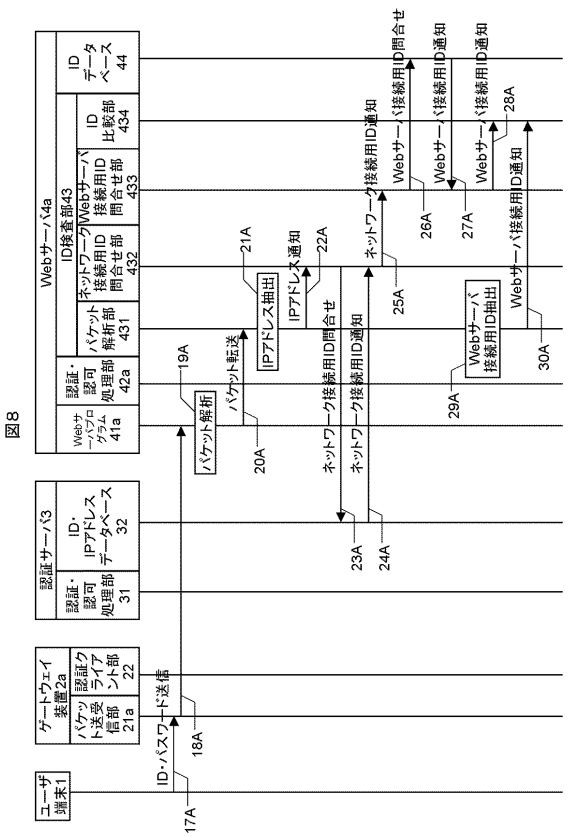


図8
Webサーバ4a
ID検査部43
ネットワーク接続用ID問合せ部 432
Webサーバ接続用ID問合せ部 433
IDデータベース 44
IDアドレスデータベース 32
認証・認可処理部 31
認証・認可処理部 42a
認証クライアント部 22
パケット送受信部 21a
ユーザ端末1
パケット解析
パケット転送
IPアドレス抽出
IPアドレス通知
ネットワーク接続用ID問合せ
ネットワーク接続用ID通知
Webサーバ接続用ID問合せ
Webサーバ接続用ID通知
Webサーバ接続用ID抽出
ID・パスワード送信

【図９】

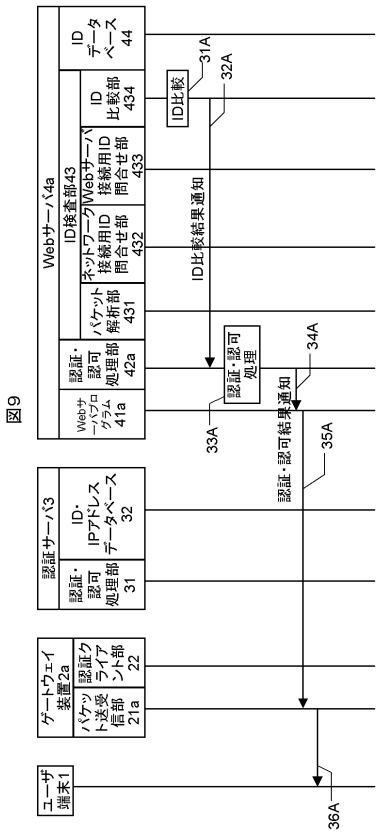


図9
Webサーバ4a
ID検査部43
ネットワーク接続用ID問合せ部 432
Webサーバ接続用ID問合せ部 433
IDデータベース 44
IDアドレスデータベース 32
認証・認可処理部 31
認証・認可処理部 42a
認証クライアント部 22
パケット送受信部 21a
ユーザ端末1
ID比較
ID比較結果通知
認証・認可処理
認証・認可結果通知

【図１０】

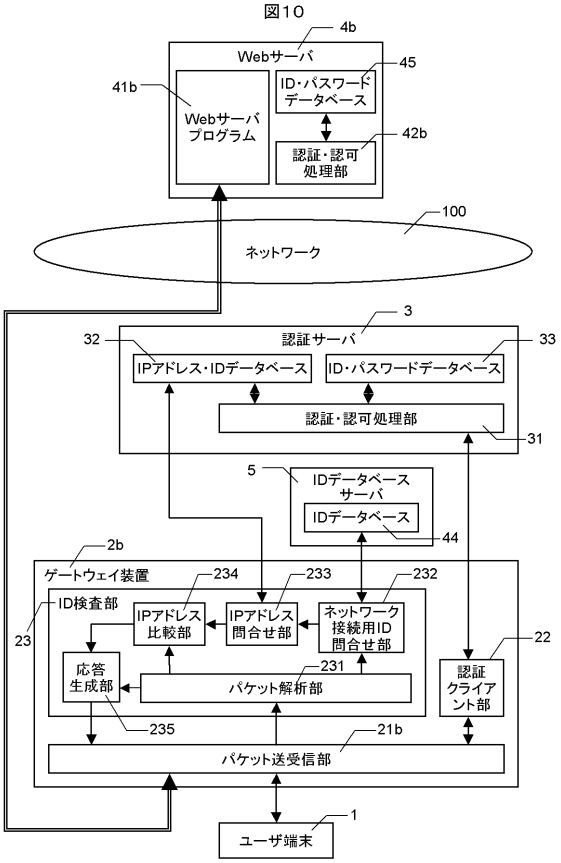
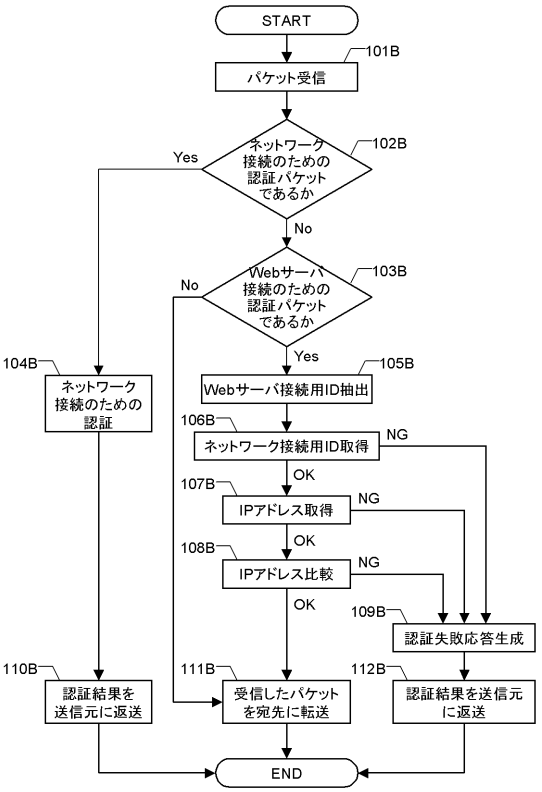


図10
Webサーバ
Webサーバプログラム
ID・パスワードデータベース
認証・認可処理部
ネットワーク
認証サーバ
IPアドレス・IDデータベース
ID・パスワードデータベース
認証・認可処理部
IDデータベースサーバ
IDデータベース
ゲートウェイ装置
ID検査部
IPアドレス比較部
IPアドレス問合せ部
ネットワーク接続用ID問合せ部
応答生成部
パケット解析部
認証クライアント部
パケット送受信部
ユーザ端末

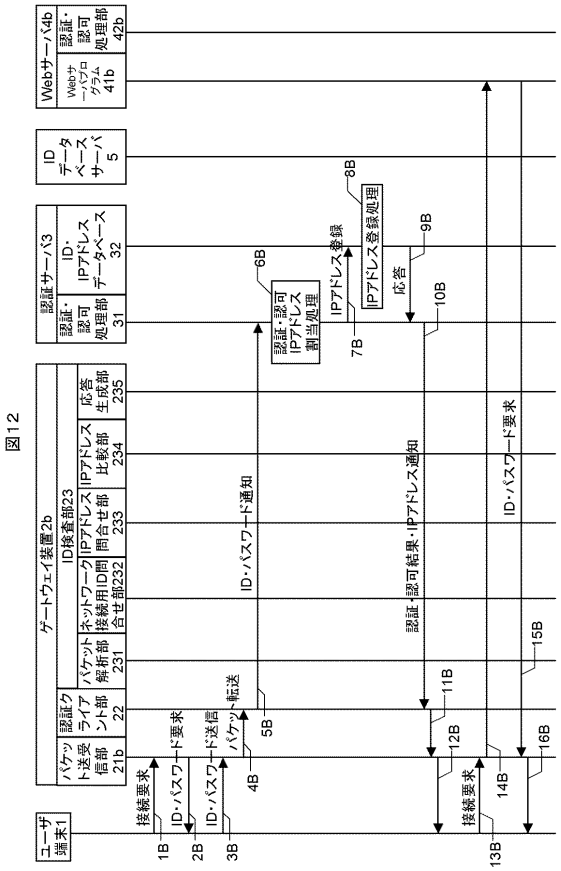
【図１１】

図11



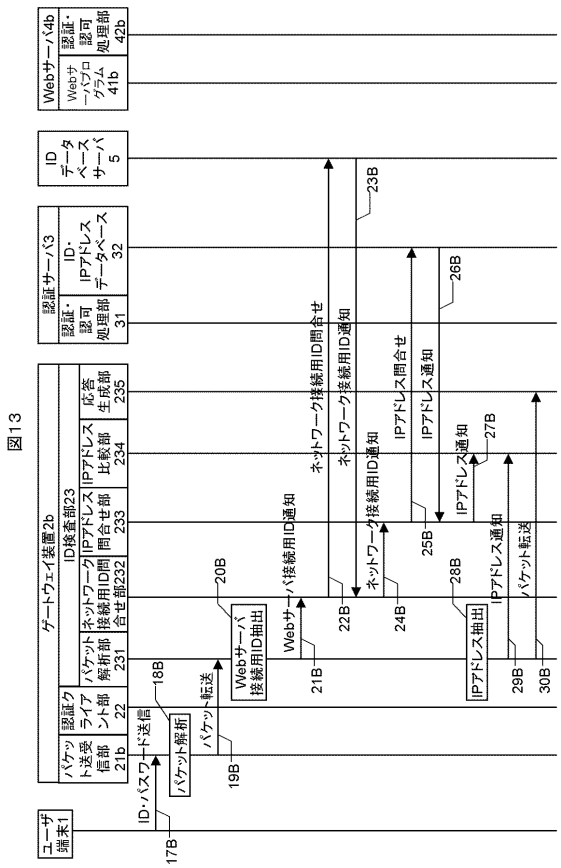
【図１２】

図12



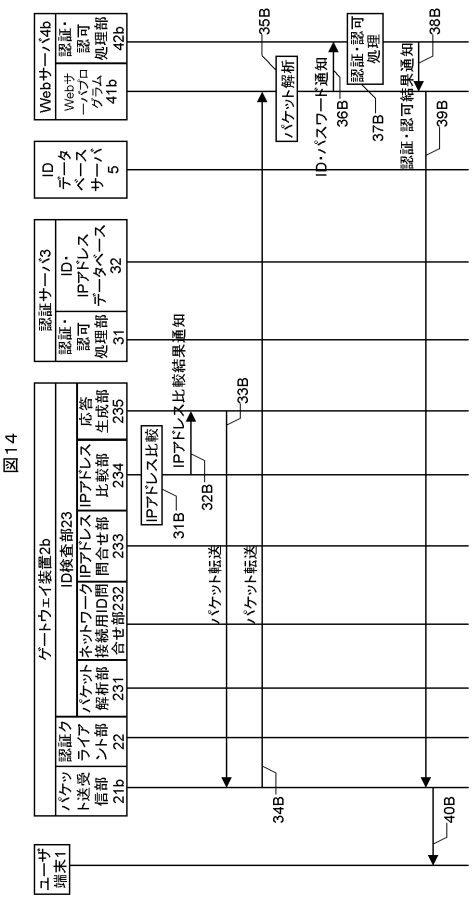
【図１３】

図13



【図１４】

図14



フロントページの続き

(56)参考文献 特開２００３－１３２０３０（ＪＰ，Ａ）
特開２００２－２５９２５４（ＪＰ，Ａ）
特開２００１－２０２４３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０９Ｃ　１／００