

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-334741

(P2004-334741A)

(43) 公開日 平成16年11月25日(2004.11.25)

(51) Int.Cl.⁷

G06F 15/00

H04L 9/32

F I

G06F 15/00 330B

G06F 15/00 310B

G06F 15/00 330E

H04L 9/00 673A

テーマコード (参考)

5B085

5J104

審査請求 未請求 請求項の数 8 O L (全 10 頁)

(21) 出願番号 特願2003-132678 (P2003-132678)

(22) 出願日 平成15年5月12日 (2003.5.12)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(74) 代理人 100058479

弁理士 鈴江 武彦

(74) 代理人 100084618

弁理士 村松 貞男

(74) 代理人 100087963

弁理士 石川 義雄

(72) 発明者 岡本 学

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

Fターム(参考) 5B085 AA01 AE02 AE03 AE08 BA06

BG02 BG03 BG07

最終頁に続く

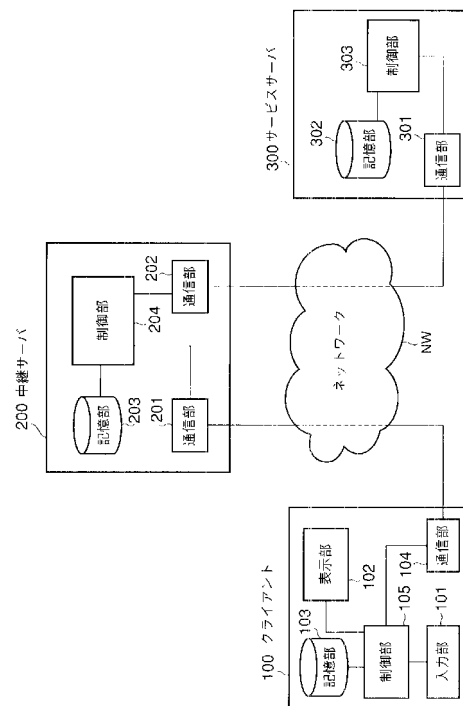
(54) 【発明の名称】 中継装置およびそのプログラム

(57) 【要約】

【課題】 サービスサーバ側でユーザ毎のサービス利用内容が判別されることを防止する中継装置およびそのプログラムを提供する。

【解決手段】 中継サーバ200がクライアント100から送信された中継サーバアカウントIDとパスワードによりクライアント100の認証を行い、クライアント100が正当なユーザの場合には、中継サーバ200がクライアント100から受信した中継サーバアカウントIDとパスワードに代わって、サービスサーバ300から予め割り当てられたサービスサーバアカウントIDとパスワードを用いてサービスサーバ300に認証を求め、サービスサーバ300から提供されるサービスをクライアント100に中継するようにしたものである。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

ネットワークを通じてサービスを提供するサーバと、前記サービスを利用可能なクライアントとの間を中継する中継装置において、
前記クライアントから受信した第 1 の認証情報に基づいて、前記クライアントが正当なユーザであるか否かを判定する認証手段と、
前記サーバに対して第 2 の認証情報を送信して、前記サービスの利用許可を要求する認証要求手段と、
前記認証手段が正当なユーザであると判定した場合に、前記認証要求手段の要求により前記サーバから許可されたサービスを中継して前記クライアントに提供する中継手段とを具備することを特徴とする中継装置。 10

【請求項 2】

さらに、前記第 2 の認証情報として、予め前記サーバから割り当てられた複数の認証情報を記憶する記憶手段を備え、
前記認証要求手段は、前記記憶手段が記憶する認証情報をランダムに選択し、この選択した認証情報を前記第 2 の認証情報として前記サーバに送信し、前記サービスの利用許可を要求することを特徴とする請求項 1 に記載の中継装置。

【請求項 3】

前記認証要求手段は、前記認証手段が正当なユーザであると判定した場合に、前記サーバに対して第 2 の認証情報を送信して、前記サービスの利用許可を要求することを特徴とする請求項 1 または請求項 2 に記載の中継装置。 20

【請求項 4】

さらに、前記サーバから受信した入力フォームを前記クライアントに送信する入力フォーム送信手段を備え、
前記認証手段は、前記クライアントから受信した入力フォームに含まれる前記第 1 の認証情報に基づいて、前記クライアントが正当なユーザであるか否かを判定し、
前記認証要求手段は、前記第 1 の認証情報に代わって前記第 2 の認証情報を前記クライアントから受信した入力フォームに含め、これを前記サーバに送信して前記サービスの利用許可を要求することを特徴とする請求項 1 乃至請求項 3 のいずれかに記載の中継装置。 30

【請求項 5】

ネットワークを通じてサービスを提供するサーバと、前記サービスを利用可能なクライアントとの間を中継する中継装置のプログラムであって、
前記クライアントから受信した第 1 の認証情報に基づいて、前記クライアントが正当なユーザであるか否かを判定する認証手段と、
前記サーバに対して第 2 の認証情報を送信して、前記サービスの利用許可を要求する認証要求手段と、
前記認証手段が正当なユーザであると判定した場合に、前記認証要求手段の要求により前記サーバから許可されたサービスを中継して前記クライアントに提供する中継手段として、前記中継装置を機能させるためのプログラム。 40

【請求項 6】

さらに、前記第 2 の認証情報として、予め前記サーバから割り当てられた複数の認証情報を記憶する記憶手段として機能させ、
前記認証要求手段は、前記記憶手段が記憶する認証情報をランダムに選択し、この選択した認証情報を前記第 2 の認証情報として前記サーバに送信し、前記サービスの利用許可を要求することを特徴とする請求項 5 に記載のプログラム。 40

【請求項 7】

前記認証要求手段は、前記認証手段が正当なユーザであると判定した場合に、前記サーバに対して第 2 の認証情報を送信して、前記サービスの利用許可を要求することを特徴とする請求項 5 または請求項 6 に記載のプログラム。

【請求項 8】

さらに、前記サーバから受信した入力フォームを前記クライアントに送信する入力フォーム送信手段を備え、

前記認証手段は、前記クライアントから受信した入力フォームに含まれる前記第1の認証情報に基づいて、前記クライアントが正当なユーザであるか否かを判定し、

前記認証要求手段は、前記第1の認証情報に代わって前記第2の認証情報を前記クライアントから受信した入力フォームに含め、これを前記サーバに送信して前記サービスの利用許可を要求することを特徴とする請求項5乃至請求項7のいずれかに記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

10

この発明は、コンピュータネットワークを通じてサービスサーバが特定のユーザにサービスを提供するためのユーザ認証技術に関する。

【0002】

【従来の技術】

周知のように、コンピュータネットワークを通じてサービスサーバが特定のユーザにサービスを提供する従来のサービスシステムでは、サービスサーバがユーザを認証して利用許可すると、サービスを利用させるためのアカウントIDを発行し、これをユーザが利用することでサービス利用を開始することができる。

【0003】

しかしながら、ユーザとアカウントIDが一対一で対応し、ユーザがサービスを利用して 20
いる中で、上記アカウントIDをキーとして様々なユーザ情報を記憶できる。このため、プライバシー保護の観点から、特に匿名性の高いサービスなどにあっては、アカウントIDと個人とを結びつける情報をサービスサーバ運営者が知ることのないようなシステム構造が望ましい。

【0004】

これに対して従来のシステムでは、ユーザ側に特別なアプリケーションを組み込む必要があったり、サービスサーバ側にもそれ相応の設備が必要であったりして、ユーザおよびサービス提供者に負担がかかる方式であった。

この他に、従来のシステムとしては、単純プロキシサーバを用いたシステムがある（例えば、特許文献1参照）。しかしながら、このシステムでは、ユーザ網へアクセスポイント 30
を特定する情報が流出することは防止できるものの、サービスサーバにはアカウントIDと個人とを結びつける情報が伝達されることは防止できない。

【0005】

【特許文献1】

特開2001-273257公報（第4-6頁、図1）。

【0006】

【発明が解決しようとする課題】

従来では、サービスサーバ運営者がサービス提供にあたってアカウントIDをユーザに与えてサービスを利用させるが、ユーザとアカウントIDが一対一で対応してしまうため、サービス利用内容が個人情報として利用されてしまう虞があるという問題があった。 40

【0007】

この発明は上記の問題を解決すべくなされたもので、サービスサーバに特別な設備投資を行うことなく、かつユーザ側の機器においても特別に新しい機能を加えることなく、サービスサーバ側でユーザ毎のサービス利用内容が判別されることを防止する中継装置およびそのプログラムを提供することを目的とする。

【0008】

【課題を解決するための手段】

上記の目的を達成するために、請求項1に係わる本発明は、ネットワークを通じてサービスを提供するサーバと、サービスを利用可能なクライアントとの間を中継する中継装置において、クライアントから受信した第1の認証情報に基づいて、クライアントが正当なユ 50

ーザであるか否かを判定する認証手段と、サーバに対して第2の認証情報を送信して、サービスの利用許可を要求する認証要求手段と、認証手段が正当なユーザであると判定した場合に、認証要求手段の要求によりサーバから許可されたサービスを中継してクライアントに提供する中継手段とを具備して構成するようにした。

【0009】

また、請求項5に係わる本発明は、ネットワークを通じてサービスを提供するサーバと、サービスを利用可能なクライアントとの間を中継する中継装置のプログラムであって、クライアントから受信した第1の認証情報に基づいて、クライアントが正当なユーザであるか否かを判定する認証手段と、サーバに対して第2の認証情報を送信して、サービスの利用許可を要求する認証要求手段と、認証手段が正当なユーザであると判定した場合に、認証要求手段の要求によりサーバから許可されたサービスを中継してクライアントに提供する中継手段として、中継装置を機能させるようにプログラムを構成するようにした。

10

【0010】

上記構成の中継装置およびプログラムでは、クライアントから送信された第1の認証情報に基づいてクライアントの認証を行い、クライアントから受信した第1の認証情報に代わって第2の認証情報を用いてサーバに利用許可を求め、クライアントが正当なユーザの場合に、サーバから提供されるサービスをクライアントに中継するようにしている。

【0011】

したがって、上記構成の中継装置およびプログラムによれば、クライアントが正当なユーザの場合には、クライアントから送られた第1の認証情報に代わって第2の認証情報でサービスサーバに認証を受けてサービスが提供されることになるため、サーバに特別な設備投資を行ったり、クライアントに特別に新しい機能を加えなくても、サーバ側でユーザ毎のサービス利用内容が判別されることを防止できる。

20

【0012】

【発明の実施の形態】

以下、図面を参照して、この発明の一実施形態について説明する。

図1は、この発明の一実施形態に係わるネットワークサービスシステムの構成を示すもので、ユーザが利用するパーソナルコンピュータなどのクライアント100と、このクライアント100に対してサービスを提供するサービスサーバ300と、クライアント100とサービスサーバ300とをネットワークNWを通じて中継接続する中継サーバ200とを備える。なお、図1では、説明を簡略にするために、1つのクライアント100のみを示しているが、実際のシステムでは複数のクライアントがこのネットワークに接続可能である。

30

【0013】

クライアント100は、パーソナルコンピュータなどの端末装置であって、キーボードやマウスなどの入力部101と、液晶ディスプレイなどの表示部102と、ハードディスクや、RAMやROMなどの半導体記録媒体からなる記憶部103と、ネットワークNWを通じて通信するモデムなどの通信部104と、CPU（Central Processing Unit）、RAMやROMなどからなり、当該クライアント100の各部を統括して制御する制御部105とを備える。

40

【0014】

記憶部103には、オペレーティングシステム（OS）やクライアントソフトウェア、種々の制御データの他に、サービスサーバ300が提供するサービスを受けるためのアプリケーションソフトウェアが記憶されており、これらを制御部105が読み込んで各部を制御し、例えば通信部104を制御して中継サーバ200を通じてサービスサーバ300と通信し、サービスサーバ300からサービスが提供される。

【0015】

中継サーバ200は、ネットワークNWを通じて通信するモデムなどの通信部201、202と、ハードディスクや、RAMやROMなどの半導体記録媒体からなる記憶部203と、CPU、RAMやROMなどからなり、当該中継サーバ200の各部を統括して制御

50

する制御部 204 とを備える。

【0016】

記憶部 203 には、オペレーティングシステム、認証や中継を行うためのプログラム、種々の制御データ、アプリケーションソフトウェアが記憶されており、これを制御部 204 が読み込んで各部を制御し、クライアント 100 とサービスサーバ 300 とをネットワーク NW を通じて中継接続し、サービスサーバ 300 がクライアント 100 に提供するサービスを実現させる。この他、記憶部 203 には、クライアント 100 が当該中継サーバ 200 を利用するために予め割り当てた中継サーバアカウント ID とパスワード、およびサービスサーバ 300 から予め割り当てられた複数のサービスサーバアカウント ID とパスワードなどの認証情報が記憶される。

10

【0017】

サービスサーバ 300 は、ネットワーク NW を通じて通信するモデムなどの通信部 301 と、ハードディスクや、RAM や ROM などの半導体記録媒体からなる記憶部 302 と、CPU、RAM や ROM などからなり、当該サービスサーバ 300 の各部を統括して制御する制御部 303 とを備える。

【0018】

記憶部 302 には、オペレーティングシステム、認証やサービスを提供するためのアプリケーションソフトウェア、種々の制御データ、予め中継サーバ 200 に割り当てたサービスサーバアカウント ID とパスワードなどの認証情報が記憶されており、これを制御部 303 が読み込んで各部を制御し、ネットワーク NW および中継サーバ 200 を通じてクライアント 100 にサービスを提供する。

20

【0019】

次に、上記構成のネットワークサービスシステムの動作について説明する。図 2 は、この動作を説明するためのシーケンス図である。

クライアント 100 では、入力部 101 を通じてユーザからサービスの利用を求める要求が与えられると、制御部 105 は通信部 104 を制御して中継サーバ 200 に対して、サービスサーバ 300 に宛てた接続要求を行う（ステップ S1）。これに対して、中継サーバ 200 では、制御部 204 が通信部 201 を制御して、クライアント 100 から上記接続要求を受け付けると、制御部 204 が通信部 202 を制御して、サービスサーバ 300 に対して接続要求を行う。

30

【0020】

これに対して、サービスサーバ 300 では、通信部 301 が中継サーバ 200 から接続要求を受信したことを制御部 303 が検出すると、制御部 303 は入力フォームの情報を記憶部 302 から読み出し、通信部 301 を制御して上記入力フォームを送信する（ステップ S2）。これに対して、中継サーバ 200 では、制御部 204 が通信部 202 を制御して、サービスサーバ 300 から上記入力フォームを受け付けると、制御部 204 が通信部 201 を制御して、クライアント 100 に対して上記入力フォームを送信する。

【0021】

これに対して、クライアント 100 では、通信部 104 が入力フォームを受信すると、制御部 105 は表示部 102 に上記入力フォームを表示して、ユーザに対しその入力欄にアカウント ID とパスワードの入力を促し、入力部 101 を通じてアカウント ID とパスワードの入力を受け付ける（ステップ S3）。ここでユーザは、認証情報として、予め中継サーバ 200 から割り当てられた中継サーバアカウント ID とパスワードを入力する。そして入力が完了すると、クライアント 100 では、制御部 105 が通信部 104 を制御して、ユーザから入力された認証情報が含まれた入力フォームを送信する（ステップ S4）。

40

【0022】

これに対して、中継サーバ 200 では、制御部 204 が通信部 201 を制御して、クライアント 100 から上記入力フォームを受信し、この受信した入力フォームに含まれる中継サーバアカウント ID とパスワードを、記憶部 203 に保存しておいた認証情報と比較し

50

て正当な利用者であるか否かを判定する（ステップS5）。そして、正当な利用者である場合には、制御部204が記憶部203から認証情報を検索し、サービスサーバ300から予め割り当てられたサービスサーバアカウントIDとパスワードの組を1つ選択する（ステップS6）。なお、この選択は、記憶部203に記憶される複数のサービスサーバアカウントIDとパスワードの組のうちから、ランダムに選択される。

【0023】

そして、中継サーバ200では、制御部204が、ステップS4で受信した入力フォームのアカウントIDとパスワードを、それぞれステップS6で選択したサービスサーバアカウントIDとパスワードに置換する（ステップS7）。そして、制御部204は、通信部202を制御して、上記置換が施された入力フォームをサービスサーバ300に送信する（ステップS8）。 10

【0024】

これに対して、サービスサーバ300では、制御部303が通信部301を制御して、中継サーバ200から上記入力フォームを受信し、この受信した入力フォームに含まれるサービスサーバアカウントIDとパスワードを、記憶部302に保存しておいた認証情報と比較して正当な利用者であるか否かを判定する（ステップS9）。そして、正当な利用者である場合には、制御部303は通信部301を制御して、サービスの提供を開始する（ステップS10）。

【0025】

以後、中継サーバ200は、制御部204が通信部201、202を制御してクライアント100とサービスサーバ300との間を中継し、クライアント100から受信したデータをそのままサービスサーバ300に転送し、一方、サービスサーバ300から受信したデータをそのままクライアント100に転送する。 20

【0026】

次に、入力フォームへの入力例を挙げて、上記構成のネットワークサービスシステムの動作について説明する。図3は、そのシーケンスを示すものである。

クライアント100は、ユーザからサービスの利用を求める要求が与えられると、サービスサーバ300に宛てた接続要求を行う（ステップS1）。これに対して、サービスサーバ300は、上記接続要求の受信を検出すると、入力フォームを送信する（ステップS2）。このようにして送信された入力フォームは、中継サーバ200では、制御部204が通信部202を制御して、サービスサーバ300から上記入力によりクライアント100に送信される。 30

【0027】

これに対して、クライアント100では、受信した入力フォームを表示して、ユーザにアカウントIDとパスワードの入力を促し、これらの入力を受け付ける（ステップS3）。ここでユーザは、予め中継サーバ200から割り当てられた中継サーバアカウントID「1234」とパスワード「abcd」を入力する。そして入力が完了すると、クライアント100は、ユーザから入力された中継サーバアカウントID「1234」とパスワード「abcd」が含まれる入力フォームを送信する（ステップS4）。 40

【0028】

これに対して、中継サーバ200は、クライアント100から受信した入力フォームに含まれる中継サーバアカウントIDとパスワードを、記憶部203に保存しておいた認証情報と比較して正当な利用者であるか否かを判定する（ステップS5）。そして、正当な利用者である場合には、記憶部203から認証情報を検索し、サービスサーバ300から予め割り当てられたサービスサーバアカウントID「5678」とパスワード「pqrs」の組を1つ選択する（ステップS6）。そして、ステップS4で受信した入力フォームのアカウントID「1234」とパスワード「abcd」を、それぞれステップS6で選択したサービスサーバアカウントID「5678」とパスワード「pqrs」に置換する（ステップS7）。そして、上記置換が施された入力フォームをサービスサーバ300に送信する（ステップS8）。 50

【0029】

これに対して、サービスサーバ300は、中継サーバ200から受信した入力フォームに含まれるサービスサーバアカウントID「5678」とパスワード「p q r s」を、記憶部302に保存しておいた認証情報と比較して正当な利用者であるか否かを判定する（ステップS9）。そして、正当な利用者である場合には、サービスの提供を開始する（ステップS10）。

【0030】

以上のように、上記構成のネットワークサービスシステムでは、中継サーバ200がクライアント100から送信された中継サーバアカウントIDとパスワードによりクライアント100の認証を行い、クライアント100が正当なユーザの場合には、中継サーバ200がクライアント100から受信した中継サーバアカウントIDとパスワードに代わって、サービスサーバ300から予め割り当てられたサービスサーバアカウントIDとパスワードを用いてサービスサーバ300に認証を求め、提供されるサービスを中継するようにしている。 10

【0031】

したがって、上記構成のネットワークサービスシステムによれば、正当なユーザに対しては、中継サーバ200がサービスサーバ300から割り当てられたアカウントIDとパスワードでサービスサーバ300に認証を受けてサービスが提供される。このため、サービスサーバ300に特別な設備投資を行うことなく、かつクライアント100においても特別に新しい機能を加えることなく、サービスサーバ300側でユーザ毎のサービス利用内容が判別されることを防止できる。 20

【0032】

なお、この発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また上記実施形態に開示されている複数の構成要素を適宜組み合わせることによって種々の発明を形成できる。また例えば、実施形態に示される全構成要素からいくつかの構成要素を削除した構成も考えられる。さらに、異なる実施形態に記載した構成要素を適宜組み合わせてもよい。

【0033】

例えば、上記実施の形態では、クライアント100が正当なユーザであると中継サーバ200が判断した場合に、サービスサーバ300に対して認証を求めてサービスの提供を受け、これを中継するようにした。これに代わって例えば、中継サーバ200が予めサービスサーバ300からサービスの提供を受けることができるように認証を完了させておき、その後、クライアント100からの接続要求が発生した場合にクライアント100の認証を行って、正当なユーザであることが判明すると、サービスサーバ300から提供されるサービスをクライアント100に中継するようにしてもよい。 30

その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることはいうまでもない。

【0034】

【発明の効果】

以上述べたように、この発明では、クライアントから送信された第1の認証情報に基づいてクライアントの認証を行い、クライアントから受信した第1の認証情報に代わって第2の認証情報を用いてサーバに利用許可を求め、クライアントが正当なユーザの場合に、サーバから提供されるサービスをクライアントに中継するようにしている。 40

【0035】

したがって、この発明によれば、クライアントが正当なユーザの場合には、クライアントから送られた第1の認証情報に代わって第2の認証情報でサービスサーバに認証を受けてサービスが提供されることになるため、サーバに特別な設備投資を行ったり、クライアントに特別に新しい機能を加えなくても、サーバ側でユーザ毎のサービス利用内容が判別されることを防止可能な中継装置およびプログラムを提供できる。

【図面の簡単な説明】

【図 1】この発明に係わるネットワークサービスシステムの一実施形態の構成を示す回路ブロック図。

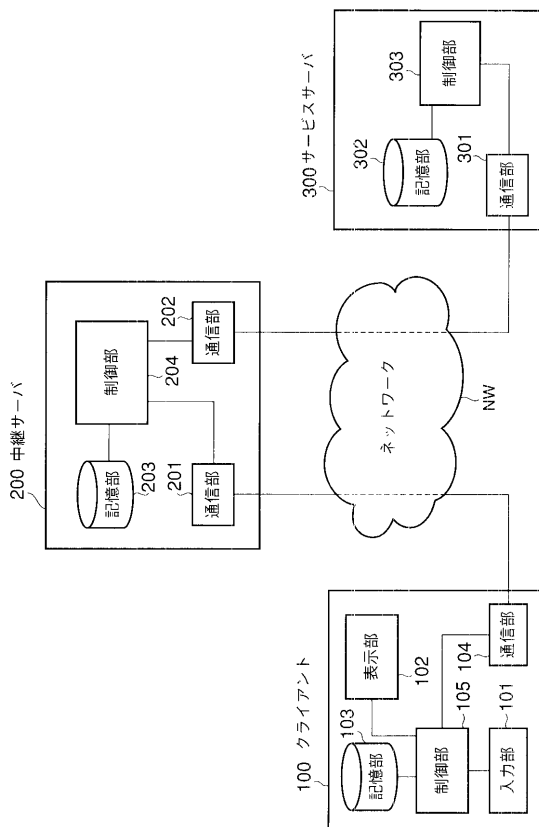
【図 2】図 1 に示したネットワークサービスシステムの動作シーケンスを示す図。

【図 3】図 1 に示したネットワークサービスシステムの動作シーケンスを示す図。

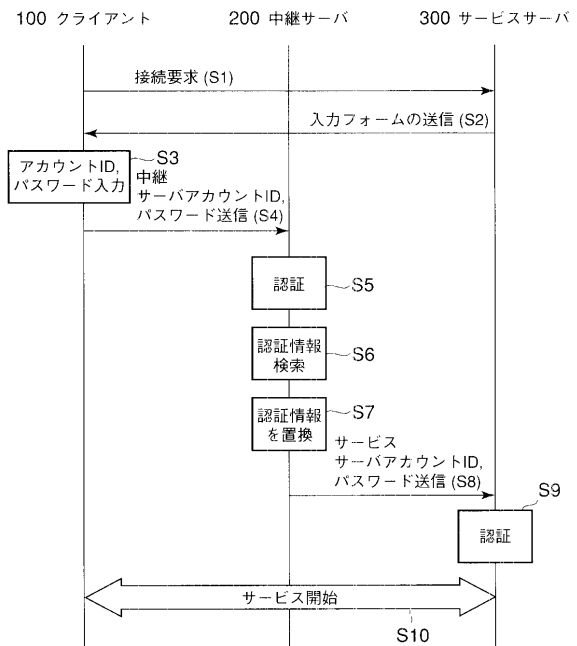
【符号の説明】

100…クライアント、101…入力部、102…表示部、103…記憶部、104…通信部、105…制御部、200…中継サーバ、201…通信部、202…通信部、203…記憶部、204…制御部、300…サービスサーバ、301…通信部、302…記憶部、303…制御部、NW…ネットワーク。

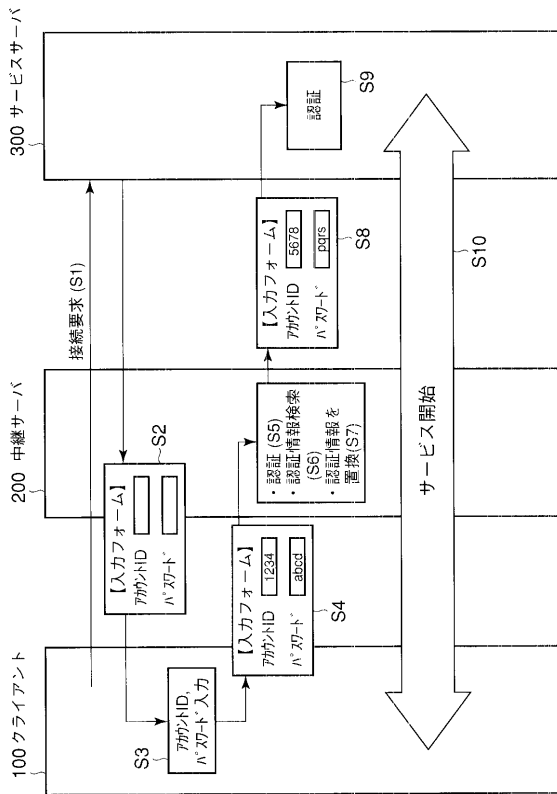
【図 1】



【図 2】



【図 3】



フロントページの続き

Fターム(参考) 5J104 AA01 AA02 AA07 BA02 KA01 KA04 MA01 NA05 NA27 NA38
PA07