(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3937475号
(P3937475)
(45)発行日　平成19年6月27日(2007.6.27)　(24)登録日　平成19年4月6日(2007.4.6)

(51)Int.Cl.		F I		
G06F 12/00	(2006.01)	G06F	12/00	537A
G06F 21/24	(2006.01)	G06F	12/00	545F
G06F 13/00	(2006.01)	G06F	12/14	530B
		G06F	12/14	530C
		G06F	12/14	520A

請求項の数 7　(全 12 頁)　最終頁に続く

(21)出願番号　特願平8-154118
(22)出願日　平成8年6月14日(1996.6.14)
(65)公開番号　特開平10-3420
(43)公開日　平成10年1月6日(1998.1.6)
審査請求日　平成15年5月20日(2003.5.20)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100093908
弁理士　松本　研一
(72)発明者　吉本　雅彦
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】アクセス制御システムおよびその方法

(57)【特許請求の範囲】

【請求項１】

ネットワーク上のサイトの資源を共有する分散システムのアクセス制御方法であって、

クライアント端末上で同時に起動される複数のクライアントからのサービス要求の代行および受信したメッセージの配布を行う中継手段が、サービスを要求する利用者の識別子を取得し、前記取得した利用者識別子を付加したサービス要求メッセージをサービス提供手段へ送信するステップと、

前記サービス提供手段が、前記中継手段から受信したサービス要求メッセージに付加された識別子を利用者識別子として取得するとともに、前記中継手段の識別子を端末識別子として取得し、前記取得した端末識別子および利用者識別子から、そのサービス要求に対する権限を一意に決定し、前記決定した権限を用いて前記サービス要求を受理するか否かを判定するステップとを有することを特徴とするアクセス制御方法。

【請求項２】

前記中継手段は、前記利用者識別子の取得を、サービス要求メッセージごとに行うことを特徴とする請求項1に記載されたアクセス制御方法。

【請求項３】

前記中継手段は、前記利用者識別子の取得を、コネクションが要求された際に行うことを特徴とする請求項1に記載されたアクセス制御方法。

【請求項４】

前記サービス提供手段は、前記中継手段の端末識別子の取得を、前記中継手段から受信

したサービス代行要求メッセージごとに行うことを特徴とする請求項1に記載されたアクセス制御方法。
【請求項５】
前記サービス提供手段は、前記中継手段の端末識別子の取得を、前記中継手段からコネクションが要求された際に行うことを特徴とする請求項1に記載されたアクセス制御方法。
【請求項６】
前記サービス提供手段は、前記中継手段が稼動する端末装置における特権的資源を用いてサービス代行要求が行われた場合、そのサービス代行要求を受理することを特徴とする請求項1に記載されたアクセス制御方法。
【請求項７】
ネットワーク上のサイトの資源を共有する分散システムのアクセス制御システムであって、
クライアント端末上で同時に起動される複数のクライアントからのサービス要求を代行するとともに、受信したメッセージの配布を行う中継手段、および、サービス提供手段を備え、
前記中継手段は、サービスを要求する利用者の識別子を取得し、取得した利用者識別子を付加したサービス要求メッセージを前記サービス提供手段に送信し、
前記サービス提供手段は、前記中継手段から受信したサービス要求メッセージに付加された識別子を利用者識別子として取得するとともに、前記中継手段の識別子を端末識別子として取得し、前記取得した端末識別子および利用者識別子から、そのサービス要求に対する権限を一意に決定し、前記決定した権限を用いて前記サービス要求を受理するか否かを判定することを特徴とするアクセス制御システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はアクセス制御システムおよびその方法に関し、例えば、ネットワーク上のサイトの資源を共有する分散システムに関する。
【０００２】
【従来の技術】
分散システムにおけるアクセス制御は、分散システムにおける認証機構と、各サイトにおける資源保護機構とを組み合わせたものが一般的である。
【０００３】
例えば、ローカルエリアネットワーク(LAN)による比較的小規模なネットワーク環境では、ネットワークを介したファイル共有手段である分散ファイルシステムが用いられる。この場合、ユーザ管理形態を統一することで、サイトレベルの利用者認証手段をネットワーク環境においても流用し、認証された利用者の権限に基づく資源保護が行われている。これらを実現するファイルアクセス制御手段は、一般に、オペレーティングシステム(OS)により提供される。
【０００４】
一方、ワイドエリアネットワーク(WAN)による比較的大規模なネットワーク環境では、ユーザ管理形態を統一することは困難であるから、認証システムによる認証が用いられることになる。大規模ネットワーク環境においては、小規模ネットワーク環境に比べて資源自体を共有する機会は少ないが、資源保護機構として最終的に用いられる機構がOSによって提供される点については、小規模ネットワーク環境の場合と同様である。
【０００５】
【発明が解決しようとする課題】
しかし、上述した技術においては、次のような問題点がある。
【０００６】
第一の問題は、サイトレベルの利用者認証機構を分散システムに適用しただけでは、充分

な信頼性を確保できない点である。サイト間でユーザ管理形態を統一する場合であっても、それが強制力をもたず、あるサイトが一部の管理情報を個別に変更できる場合など、サイトの管理者はユーザになりすますことが可能であり、資源提供者はそれを検知することが困難である。

【０００７】

第二の問題は、OSによって提供される資源保護機構を分散資源に適用する場合、通常、資源保護機構が稼動するサイトにおいてのみ効力をもつため、外部からの資源操作要求は当該サイトにおける然るべき権限によって処理されなければならない。しかし、一旦認証された利用者が同一の権限をもつ限り、同一ユーザであってもサイトによって信頼性や権限レベルが異なるような状況には対処することができない。

【０００８】

本発明は、クライアント端末上で同時に起動される複数のクライアントのサービス要求を効率的に処理するとともに、ネットワーク上のサイトの共有資源を安全かつ柔軟に保護すること目的とする。

【０００９】

【課題を解決するための手段】

本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１１】

本発明にかかるネットワーク上のサイトの資源を共有する分散システムのアクセス制御方法は、クライアント端末上で同時に起動される複数のクライアントからのサービス要求の代行および受信したメッセージの配布を行う中継手段が、サービスを要求する利用者の識別子を取得し、前記取得した利用者識別子を付加したサービス要求メッセージをサービス提供手段へ送信するステップと、前記サービス提供手段が、前記中継手段から受信したサービス要求メッセージに付加された識別子を利用者識別子として取得するとともに、前記中継手段の識別子を端末識別子として取得し、前記取得した端末識別子および利用者識別子から、そのサービス要求に対する権限を一意に決定し、前記決定した権限を用いて前記サービス要求を受理するか否かを判定するステップとを有することを特徴とする。

【００１３】

本発明にかかるネットワーク上のサイトの資源を共有する分散システムのアクセス制御システムは、クライアント端末上で同時に起動される複数のクライアントからのサービス要求を代行するとともに、受信したメッセージの配布を行う中継手段、および、サービス提供手段を備え、前記中継手段は、サービスを要求する利用者の識別子を取得し、取得した利用者識別子を付加したサービス要求メッセージを前記サービス提供手段に送信し、前記サービス提供手段は、前記中継手段から受信したサービス要求メッセージに付加された識別子を利用者識別子として取得するとともに、前記中継手段の識別子を端末識別子として取得し、前記取得した端末識別子および利用者識別子から、そのサービス要求に対する権限を一意に決定し、前記決定した権限を用いて前記サービス要求を受理するか否かを判定することを特徴とする。

【００１４】

【発明の実施の形態】

以下、本発明にかかる一実施形態のアクセス制御システムを図面を参照して詳細に説明する。

【００１５】

以下で説明する実施形態は、複数のユーザが共存する分散システムに関するもので、とくに、サイトごとに利用者の管理形態が異なるような分散環境においても、個々のユーザの権限を一元的に管理する機構を備えた分散システムに関するものである。

【００１６】

【第１実施形態】

図1は本実施形態におけるネットワーク環境の構成例を示す図である。

【００１７】

同図において、ネットワークケーブル101には、後述する端末群が接続され、コンピュータネットワークが構成されている。なお、ここで説明するコンピュータネットワークには、例えば、EthernetやFDDIを用いたLANや、公衆回線や専用線によってネットワーク間を相互接続したWANなどが含まれる。

【００１８】

サーバ端末102は、分散システムにおいて資源を提供するアプリケーションが稼動するワークステーションやパーソナルコンピュータなどのコンピュータシステムである。クライアント端末103は、分散システムにおいて資源を利用するアプリケーションが稼動する、サーバ端末102と同様のコンピュータシステムである。認証サーバ端末104は、ネットワーク環境において認証機構を提供する認証サーバが稼動する、サーバ端末102と同様のコンピュータシステムである。認証サーバは、例えば、Kerberosシステムによって提供されるものである。

【００１９】

これらコンピュータシステムには、固有の識別子が割当てられていて、その識別子は任意の端末間通信により取得される。また、上記のサーバアプリケーション、クライアントアプリケーションおよび認証サーバは、フロッピディスク、ハードディスク、光磁気ディスク(MO)、CD-ROM、CD-R、磁気テープなど外部記憶媒体、あるいは、ROMやフラッシュメモリなど任意の不揮発性記憶デバイスに記憶されたソフトウェアであって、必要に応じて、上記の端末装置が備えるメモリに読込まれた後、同端末装置が備えるCPUにより実行されるものである。なお、実行されるアプリケーションソフトウェアに対して専用の端末装置が割当てられる必要はなく、ある端末装置においてサーバやクライアントなどが同時に稼動していてもよい。またサーバやクライアントなどは、所定のサービスに関わるアプリケーションの役割に関する総称的な呼称であって、アプリケーションにおいて必ずしも固定的なものではない。実際に、あるアプリケーションは、あるサービスに関してはサーバであり、別のサービスに関してはクライアントであるような状況もある。

【００２０】

図2はクライアントからの要求をサーバが処理する手順の一例を示すフローチャートで、初めに、クライアントから送られてきたサービス要求から、ステップS201で端末識別子の取得し、ステップS202で利用者識別子の取得を行う。ここで、利用者識別子の取得処理は、認証サーバによって提供される認証手段を用いるが、ネットワーク環境に応じて提供される手段、例えば、TCP/IP(Transmission Control Protocol/Internet Protocol)ネットワーク環境におけるRFC1413に準拠した身元照会手段を用いて識別子を取得してもよい。

【００２１】

次に、ステップS203において、端末識別子および利用者識別子からサーバ端末上の対応する権限を決定する。ここで、サーバ端末上の権限とは、要求されたサービスが、OSによって保護された資源（例えばファイルやデバイスなど）へのアクセスを行うものであれば、そのOSによって定義された権限であり、サーバによって保護された資源（例えばデータベース管理システムにおける共有データなど）であれば、そのサーバによって独自に定義された権限である。

【００２２】

続いて、ステップS204でサービス要求に対して権限が有効（権限の範囲内）か否かを判定し、有効であればステップS205においてそのサービス要求を処理する。勿論、サービス要求に対して権限が無効（権限の範囲外）であれば、そのサービス要求は処理されない。

【００２３】

ステップS203およびS204における処理の詳細は次のようになる。

【００２４】

端末識別子と利用者識別子のそれぞれに対応する集合束の直積束において、ある同値関係によって定まる商束の部分集合をとると、その部分集合には商束における順序関係が成り立ち、その順序関係に関して極大の元すべてからなる集合Mが定まる。一方、ステップS201およびS202において得られた端末識別子と利用者識別子とに対応する商束の元rをとる。

ここで、Mの元mであって、m⊇rになるものが存在するとき、要求に対する権限は有効であるとする。

【００２５】

すなわち、各サービスに対して上記の同値関係と極大元の集合、ならびに、その極大元からサーバ端末上の権限への一意な対応関係が予め求められているものとして、ステップS203において、端末識別子および利用者識別子に対する同値類を決定し、ステップS204においては、その同値類と一連の極大元との間の順序関係の有無を判定する。

【００２６】

以上において、すべての集合は有限集合であることから、例えば、ビット列など公知の手段によって表現される。一方、同値関係は、例えば、上記のビット列を、宣言的または手続的に与えられた規則に従って、別の短いビット列に変換する手段である。

【００２７】

なお、ステップS201およびS202においては各種の障害による異常が発生し得る。その場合、ステップS203における同値類として、ステップS201の異常に対しては端末識別子に関する直積束の上限に対応する商束の元を代用し、ステップS202の異常に対しては利用者識別子に関する直積束の上限に対応する商束の元を代用し、両方の異常に対しては商束の上限を代用する。

【００２８】

例えば、所定のネットワークに接続された端末において、所定の利用者から構成される利用者グループに提供するサービスを制限する場合、同値関係として「指定のネットワークに接続されている端末の識別子の集合と、指定の利用者グループに属する利用者の識別子の集合とで定められる直積束の部分束に含まれるかどうか」、換言すれば「指定のネットワークに接続されているかどうか」および「指定の利用者グループに属しているかどうか」の組を与える。

【００２９】

これによって、端末識別子の集合および利用者識別子の集合は、それぞれ互いに重なり合わない二つの部分集合に分割され、これに伴って、16個の要素からなる直積集合の商束が得られる。この商束は、明らかに端末識別子および利用者識別子それぞれに関する商束の直積束に同型である。従って、上記の商束には、サービス要求が受入れられるような端末識別子および利用者識別子のすべての組に対応する同値類がただ一つ定まり、その同値類を一つの元とする極大元の集合を定めて、サービスに対する権限と対応させる。以上によって、サービスに対する同値関係と極大元の集合、および、権限との対応関係が指定される。この設定において、クライアントのサービス要求から得られる端末識別子および利用者識別子の組は、商束の何れかの同値類に対応するが、要求が受理されるのは、極大元として採用した同値類に対応する場合に限られる。

【００３０】

すなわち、本実施形態によれば、集合における同値関係は、集合束における同値関係と自然に対応することから、端末や利用者に対するグループ化を行うことは、元の大きな集合束をより小さな商束に縮めることにほかならない。これにより、サーバが用いるすべての商束に対して普遍性をもつ商束が存在して、任意の商束が、普遍性をもつ商束に対して別の同値関係を定めて得られる商束になる。

【００３１】

上述した、指定のネットワークに接続された端末における指定の利用者グループに提供するサービスを制限する例で定めた極大元は、普遍性をもつ商束の部分束に対応している。従って、上記の例における設定に代わって、普遍性をもつ商束を定める同値関係と、商束の部分束の上限からなる極大元の集合を用いた場合の効果とは等価である。

【００３２】

このように、本実施形態によれば、権限を与えるかどうかを判定する対象を任意の単位で集約することができるので、アクセス制御の設定を極めて柔軟に行うことが可能である。

【００３３】

さらに、以下で説明する実施形態によれば、従来は実現が困難であった利用者の管理形態が異なる分散環境への対応に関しても、本発明が有効であることが示される。すなわち、同一の利用者に対するすべての端末識別子および利用者識別子の組を一つの同値とみなすものとし、すべての利用者についてこれを行えば、一つの同値関係が得られる。この同値関係によって得られる商束の元は、個々の利用者に対して利用者管理形態の差異と無関係に定まるものである。従って、例えば、その商束を普遍性をもつ商束とみなして極大元の集合を定めてもよく、別の同値関係を用いてより単純な商束を定めてもよい。また、安全性の乏しい端末からの不正なアクセスを禁止するためには、上記の同一利用者に対する同値類を安全性の水準に応じて二分割し、水準の低い同値類に対して弱い権限を与えるようにすることも可能である。

【００３４】

【第２実施形態】

以下、本発明にかかる第2実施形態のアクセス制御システムを説明する。なお、第2実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００３５】

図2に示した手順は、同一の利用者であっても、その利用者が利用する端末に応じて権限のレベルを任意に設定することが可能である。ところで、上記の手順は、利用者に対する認証処理をすべてのサービス要求について行うことになり、サービス要求が繰返し発行されるような場合は、効率上の問題がある。そこで、第2実施形態は、所謂トランスポートレベル以下の安全性が保証されていればよいという観点から、トランスポートレベルのコネクションを設定する際に認証処理を行うものである。

【００３６】

図3はトランスポートレベルのコネクションを設定する際の処理手順の一例を示すフローチャートである。

【００３７】

ステップS301からS303において、図2に示したステップS201とS203と同様に、コネクション要求から端末識別子および利用者識別子を取得し、サーバ端末上の対応する権限を決定する。そして、ステップS304において、決定した権限がサーバにおいて有効であるかどうかを判定し、有効であればステップS305でコネクション要求を受理する。勿論、決定した権限がサーバにおいて無効である場合は、コネクション要求は受理されない。

【００３８】

図3に示す手順に従ってコネクション要求を処理する場合のサービス要求に対する処理手順は、図2に示した手順からステップS201からS203を削除し、代わりにサービス要求からステップS303において決定された権限を検索するように変更したものである。この手順の変更は容易である。すなわち、ステップS305においてコネクション識別子と権限の組を記録し、サービス要求を処理する時点でコネクション識別子から権限を検索すればよい。なお、記録された組は、コネクションが切断された場合に、サーバにおいて自律的に破棄される。

【００３９】

ステップS303およびS304の処理は、図2に示したステップS203およびS204の処理と同様である。ただし、図3においては、サービスに関する諸設定に代わってコネクションに関する諸設定、すなわち同値関係と極大元の集合、ならびに、極大元からサーバ端末上の権限への一意的な対応関係を用いるものとする。ここで、コネクションに関する諸設定と一連のサービスに関する諸設定とは、通常は前者における判定基準を満たすものは、後者における判定基準を満たすように選ばれるが、一般には独立でよい。

【００４０】

【第３実施形態】

以下、本発明にかかる第3実施形態のアクセス制御システムを説明する。なお、第3実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明

を省略する。

【００４１】

ある種の分散システムでは、クライアント端末上で同時に起動される複数のクライアントからのサービス要求を一括してサーバに送付するとともに、サーバから送られてくるメッセージをクライアントに配布する、一種のサーバ（以下では「中継サーバ」と呼ぶ）を設けることがある。こうした形態は、共有資源のレプリカをクライアント端末上に保持する場合や、サーバからのメッセージを一連のクライアントに向けて同報的に送付するような場合、とくに有効である。このような形態においては、以下で説明するように、図2あるいは図3に示した手順を簡略化することが可能である。

【００４２】

まず、サーバと中継サーバの間では、図2または図3に示した手順に従って権限の確認処理が行われるものとする。ただし、サーバが中継サーバに対して直接提供するサービスは、クライアントに対して提供されるものとは異なり、クライアントからの要求を代行する機構を提供するためのものである。従って、図2に示したステップS203とS204は、サービスに関する諸設定に基づいて行われる。また、ステップS205は、サービス要求を処理するのではなく、サービス代行要求を処理することになる。なお、サービス代行要求処理自体は、後述する手順から得られる利用者識別子と中継サーバの端末識別子を用いて、第1実施形態におけるステップS203以降の手順に従って行われる。

【００４３】

図4は、上記の形態の分散システムにおいて、中継サーバが各クライアントに対して行う図2に相当する手順の一例を示すフローチャートである。

【００４４】

まず、ステップS401でサービス要求から利用者識別子を取得する。ここで、中継サーバとクライアントは同一端末装置において稼動していることから、利用者識別子の取得処理は、認証サーバなどを用いることなく、安全かつ効率的に行うことができる。

【００４５】

次に、サーバから一連のサービスに関する諸設定が与えられている場合は、ステップS402およびS403において、権限の決定およびサービス要求に対する有効性の判定を行う。ただし、ステップS402とS403は、無駄なサービス要求の中継を抑制するためのものであり、手順から省略してもよい。

【００４６】

最後に、ステップS404において、サービス要求の代行処理を行う。この代行処理は、クライアントの要求メッセージに、ステップS401で取得した利用者識別子を付加したメッセージを、サーバに転送するものである。付加される利用者識別子は、中継サーバにおけるサービス代行要求処理において必要になる利用者識別子にほかならない。

【００４７】

図5は中継サーバが各クライアントに対して行う図3に相当する手順の一例を示すフローチャートである。

【００４８】

同図において、ステップS501において、図4に示すステップS401と同様に、コネクション要求から利用者識別子を取得する。

【００４９】

次に、サーバからコネクション要求に関する諸設定が与えられている場合は、ステップS502およびS503において、権限の決定および有効性の判定を行う。ただし、ステップS502およびS503は、無駄なコネクション要求を抑制するためのものであり、実際に行うことが望ましいが、手順から省略することも可能である。

【００５０】

最後に、ステップS504においては、コネクション要求を受理し、得られたコネクション識別子と利用者識別子の組を記録する。

【００５１】

以後、中継サーバは受理したコネクションに対して、クライアントからのサービス要求の代行処理を行う。この代行処理は、クライアントの要求メッセージに、ステップS504において記録した利用者識別子を付加したメッセージを、サーバに転送するものである。なお、記録した組は、コネクションが切断された場合に、中継サーバにおいて自律的に破棄される。

【００５２】

【第４実施形態】

以下、本発明にかかる第4実施形態のアクセス制御システムを説明する。なお、第4実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００５３】

上述した第3実施形態において、中継サーバが稼動する端末装置の安全性が保証され、かつ、その端末装置において中継サーバがOSにおける特権的なプロセスである場合は、認証サーバなど第三者による中継サーバの認証処理を省略してもよい。例えば、TCP/IPネットワーク環境では、端末装置のOSによっては1023番以下のポート番号によるアドレス設定に特権が必要である。

【００５４】

これによれば、中継サーバが特権的なポート番号によるアドレス設定を行い、サーバは、そのアドレスが中継サーバによって設定されたものであるかどうかを確認することで、第三者の認証手段によらずに中継サーバの身元照会が可能である。ここで確認手段は、上記の特権ポートを用いた通信によってランダムに選ばれた任意のビットパターンの折返し転送を行うなど、単純な手段で充分である。端末装置の安全性が保証される限り、上記ビットパターンを返送する不正な特権プロセスは存在し得ないからである。勿論、当該手段は、WAN環境においては、中間経路の信頼性が一般に保証されないことから危険であるが、オフィスなどの多くのLAN環境では充分に実用的である。

【００５５】

【他の実施形態】

なお、本発明は、複数の機器（例えばホストコンピュータ，インタフェイス機器，リーダ，プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機，ファクシミリ装置など）に適用してもよい。

【００５６】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，CD-ROM，CD-R，磁気テープ，不揮発性のメモリカード，ROMなどを用いることができる。

【００５７】

また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５８】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わる

CPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５９】

本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するプログラムコードを格納することになるが、簡単に説明すると、図6または図７のメモリマップ例に示す各モジュールを記憶媒体に格納することになる。すなわち、少なくとも「識別子取得」「権限決定」および「有効判定」の各モジュール、または、中継手段用に少なくとも「識別子取得A」「識別子付加」および「送信」の各モジュールと、サービス提供手段用に少なくとも「受信」「識別子取得B」「権限決定」および「有効判定」の各モジュールとのプログラムコードを記憶媒体に格納すればよい。

【００６０】

【発明の効果】

以上説明したように、本発明によれば、クライアント端末上で同時に起動される複数のクライアントのサービス要求を効率的に処理するとともに、ネットワーク上のサイトの共有資源を安全かつ柔軟に保護することができる。

【図面の簡単な説明】

【図１】本発明にかかる一実施形態におけるネットワーク環境の構成例を示す図、

【図２】クライアントからのサービス要求をサーバが処理する手順の一例を示すフローチャート、

【図３】クライアントからのコネクション要求をサーバが処理する手順の一例を示すフローチャート、

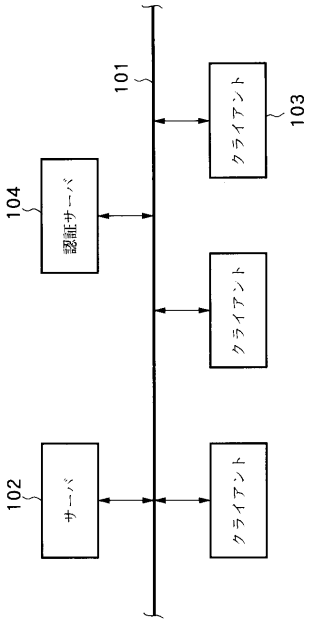
【図４】クライアントからのサービス要求を中継サーバが処理する手順の一例を示すフローチャート、

【図５】クライアントからのコネクション要求を中継サーバが処理する手順の一例を示すフローチャート、

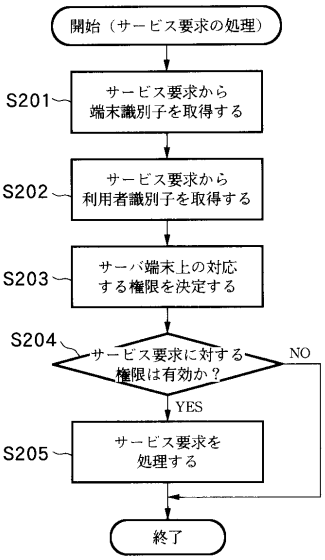
【図６】本発明のプログラムコードを格納した記憶媒体の一例を示す図、

【図７】本発明のプログラムコードを格納した記憶媒体の第二例を示す図である。

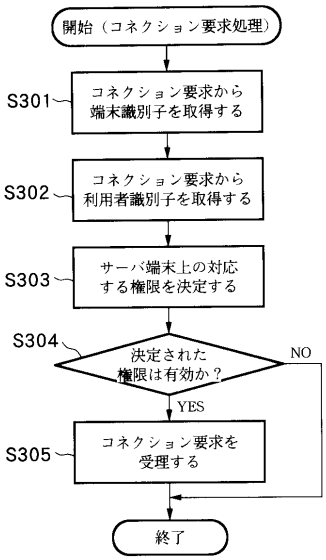
【図１】


101
クライアント
103
104
認証サーバ
クライアント
102
サーバ
クライアント

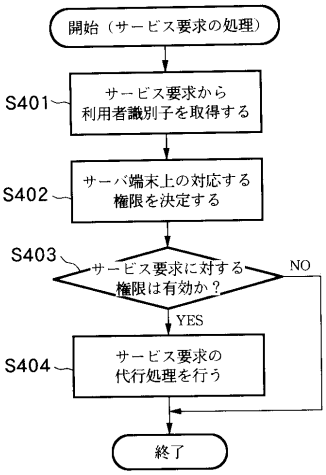
【図２】


開始（サービス要求の処理）
S201
サービス要求から
端末識別子を取得する
S202
サービス要求から
利用者識別子を取得する
S203
サーバ端末上の対応
する権限を決定する
S204
サービス要求に対する
権限は有効か？
NO
YES
S205
サービス要求を
処理する
終了

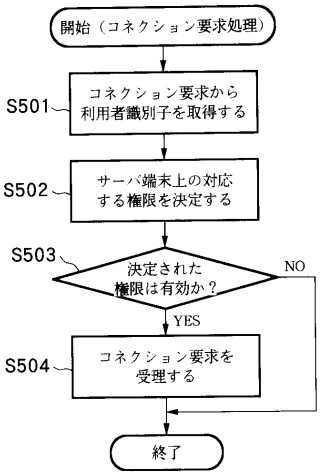
【図３】


開始（コネクション要求処理）
S301
コネクション要求から
端末識別子を取得する
S302
コネクション要求から
利用者識別子を取得する
S303
サーバ端末上の対応
する権限を決定する
S304
決定された
権限は有効か？
NO
YES
S305
コネクション要求を
受理する
終了

【図４】


開始（サービス要求の処理）
S401
サービス要求から
利用者識別子を取得する
S402
サーバ端末上の対応する
権限を決定する
S403
サービス要求に対する
権限は有効か？
NO
YES
S404
サービス要求の
代行処理を行う
終了

【図５】



【図６】

ディレクトリ情報
:
:
サービス要求受信モジュール
識別子取得モジュール
権限決定モジュール
サービス要求有効判定モジュール
サービス要求処理モジュール
:
:
:
:

【図７】

ディレクトリ情報
:
識別子取得モジュール
識別子付加モジュール
サービス要求送信モジュール
受信メッセージ配布モジュール
:
サービス要求受信モジュール
識別子取得モジュール
権限決定モジュール
サービス要求有効判定モジュール
サービス要求処理モジュール
:
:

フロントページの続き

(51)Int.Cl. FI
G06F 13/00 353M
G06F 13/00 355

(56)参考文献 特開平07－056795（JP，A）
特開平06－035859（JP，A）
特開平05－061834（JP，A）
特開平05－108451（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G06F 12/00
G06F 13/00
G06F 21/24