(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4280036号
(P4280036)

(45)発行日　平成21年6月17日(2009.6.17)　(24)登録日　平成21年3月19日(2009.3.19)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560B
G06F 12/00	(2006.01)	G06F	12/00	537A
G06F 21/20	(2006.01)	G06F	15/00	330C

請求項の数 12　(全 28 頁)

(21)出願番号	特願2002-221630 (P2002-221630)
(22)出願日	平成14年7月30日 (2002.7.30)
(65)公開番号	特開2003-122635 (P2003-122635A)
(43)公開日	平成15年4月25日 (2003.4.25)
審査請求日	平成17年5月23日 (2005.5.23)
(31)優先権主張番号	特願2001-236030 (P2001-236030)
(32)優先日	平成13年8月3日 (2001.8.3)
(33)優先権主張国	日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100098291
弁理士　小笠原　史朗
(72)発明者　山本　雅哉
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　岡本　隆一
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　大穂　雅博
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】アクセス権制御システム

(57)【特許請求の範囲】

【請求項１】

エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、

前記クライアント機器と通信可能に接続され、前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、

前記サーバは、前記アクセス権の問い合わせに対して前記アクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、

前記クライアント機器は、

他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、

前記アクセス可否問い合わせ部によって問い合わせた結果、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを他の機器に対して直接的に送信するデータ送信部とを含み、

前記アクセス可否問い合わせ部は、他の機器からデータ送信を要求され、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるときに、前記クライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書とを付加して前記アクセス可否判定部に問い合わせ、

前記アクセス可否判定部は、前記第１および第２の証明書を用いて前記アクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し判断結果を返信する、アクセス権管理システム。

【請求項２】

前記サーバが管理するアクセス権管理リストには、それぞれの前記クライアント機器が管理するデータ毎にアクセス可能な機器を示す前記アクセス権が記述され、

前記アクセス可否問い合わせ部は、前記データ送信を要求されたデータ毎に、前記アクセス可否判定部に問い合わせを行い、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する、請求項１に記載のアクセス権管理システム。

【請求項３】

さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた現在時刻に応じて前記時間条件を参照して、前記データ毎にそのアクセス権を判断する、請求項２に記載のアクセス権管理システム。

【請求項４】

さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた回数に応じて前記回数条件を参照して、前記データ毎にそのアクセス権を判断する、請求項２に記載のアクセス権管理システム。

【請求項５】

さらに、前記サーバが管理するアクセス権管理リストには、前記データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に前記複製条件を返信し、

前記データ送信部は、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを前記複製条件を付加して他の機器に対して直接的に送信する、請求項２に記載のアクセス権管理システム。

【請求項６】

前記サーバは、他のプロキシを介して前記クライアント機器と通信可能に接続されていることを特徴とする、請求項１に記載のアクセス権管理システム。

【請求項７】

前記証明書にはＸ．５０９を使用することを特徴とする、請求項１に記載のアクセス権管理システム。

【請求項８】

エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するサーバであって、

前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理部と、

前記クライアント機器から送信される前記アクセス権の問い合わせに対して、前記アクセス権管理部において前記アクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を問い合わせたクライアント機器に対して返信するアクセス可否判定部を含み、

前記アクセス可否判定部は、前記クライアント機器からの問い合わせに付加される、当該クライアント機器であることを証明するための第１の証明書と前記他の機器を証明するための第２の証明書を用いて前記アクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し、当該判断結果をアクセス権を問い合わせた前記クライアン

ト機器に対して返信する、サーバ。
【請求項９】
他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンドユーザが所有するクライアント機器であって、
他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせ部と、
前記アクセス可否問い合わせ部によって問い合わせた結果、前記サーバから返信された判断結果がアクセス可の場合、他の機器の要求に応じて直接的に前記データ送信を行うデータ送信部とを含み、
前記アクセス可否問い合わせ部は、前記要求に対する前記アクセス権を、前記クライアント機器であることを証明するための第１の証明書と前記他の機器を証明するための第２の証明書を付加して前記サーバに問い合わせることにより、当該サーバに前記第１の証明書と前記第２の証明書とを用いて当該アクセス権の問い合わせの認証を行わせる、クライアント機器。
【請求項１０】
エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、
前記サーバにおいて、前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、
前記クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記クライアント機器から前記サーバに問い合わせるアクセス可否問い合わせステップと、
前記アクセス可否問い合わせステップによる問い合わせに対して、前記アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を前記サーバで判断し判断結果を前記クライアント機器に返信するアクセス可否判定ステップと、
前記アクセス可否判定ステップによって返信された判断結果がアクセス可の場合、要求されたデータを前記クライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含み、
前記アクセス可否問い合わせステップでは、前記クライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書とを付加して前記アクセス権が前記サーバに問い合わせられ、
前記アクセス可否判定ステップでは、前記第１および第２の証明書を用いて前記クライアント機器からの問い合わせが認証された後、前記アクセス権が判断され、当該判断結果が前記クライアント機器に返信される、アクセス権制御方法。
【請求項１１】
エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断させるためのアクセス権制御プログラムを記録した当該サーバが読み取り可能な記録媒体であって、
前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、
前記クライアント機器がデータの直接的な送受信を行う際に、当該クライアント機器から前記サーバに対して行われるその送受信に対する前記アクセス権の問い合わせに応じて、前記アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を当該クライアント機器に返信するアクセス可否判定ステップとを含み、
前記アクセス可否判定ステップにおいて、前記クライアント機器からの問い合わせに付

加される当該クライアント機器であることを証明するための第１の証明書と前記他の機器を証明するための第２の証明書を用いて前記アクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し、当該判断結果を前記クライアント機器に対して返信する、アクセス権制御プログラムを記録した記録媒体。

【請求項１２】

他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、

前記クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせステップと、

前記アクセス可否問い合わせステップによって問い合わせた結果、前記サーバから返信された判断結果がアクセス可の場合、要求されたデータを前記クライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含み、

前記アクセス可否問い合わせステップにおいて、他の機器からデータ送信を要求され、その要求に対する前記アクセス権を、前記クライアント機器であることを証明するための第１の証明書と前記他の機器を証明するための第２の証明書を用いて認証する前記サーバに問い合わせるときに、前記第１の証明書と第２の証明書とを付加して前記アクセス可否判定部に問い合わせる、アクセス権制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークにおいてピアツーピア形式でデータ交換を行う際のアクセス権制御システムに関する。

【０００２】

【従来の技術】

近年、ピアツーピアコンピューティングが注目を集めている。ピアツーピアコンピューティングとは、ネットワークで接続された機器同士で直接やり取りしあうことにより、コンピュータリソース（ＣＰＵパワーやハードディスクのスペース）や各種サービス（メッセージやファイル交換システムなど）を共有することができ、機器同士の共同作業さえも可能となる技術である。このピアツーピア型のファイル交換システムでは、エンドユーザが所有する機器（クライアント機器）同士で直接的な通信を行い、当該機器が管理しているファイルを交換することが可能である。

【０００３】

上記ピアツーピア型のファイル交換システムにおけるクライアント機器が管理するファイルに対する他からのアクセスの可否（以下、アクセス権と記載する）は、当該クライアント機器自身によって行われる。例えば、アクセス先（データの提供元）のクライアント機器では、アクセス元（データの提供先）のクライアント機器に対してパスワードを要求し、正しいパスワードがアクセス元のクライアント機器から送信された場合にのみ、アクセス先のクライアント機器が管理するファイルに対するアクセスを許可するといったアクセス権の制御が行われる。さらに、アクセス先のクライアント機器が行う複雑なアクセス権制御としては、アクセス日時やアクセス元のクライアント機器を識別する識別子によるアクセス権制御があり、さらにアクセス先のクライアント機器が管理する各ファイル毎に、それぞれ固有の制御情報を設定するものなどが考えられる。

【０００４】

【発明が解決しようとする課題】

このような複雑なアクセス権制御は、アクセス先のクライアント機器が処理能力の高いパーソナルコンピュータ等で構成されている場合、実現することは容易である。しかしながら、アクセス先のクライアント機器が処理能力の限られた民生機器で構成されている場合

、上述したような複雑なアクセス権制御を実現することは非常に困難である。また、パーソナルコンピュータとは異なり、処理能力の限られた民生機器においては、購入後にその内部に格納されたソフトウェアを交換することは非常に困難であり、上述したアクセス権制御の方法を後から追加あるいは改変することは不可能である。

【０００５】

一方、上記ピアツーピア型のファイル交換システムと通信可能に接続されたサーバに、当該システム内に設けられたクライアント機器がそれぞれ管理するファイルを、リストとして管理することも行われている。このサーバで管理されているリストは、上記クライアント機器が管理しているファイル名称とそのクライアント機器が記述されており、同じシステム内に設けられたクライアント機器が当該リストを参照することによって、所望のファイルの有無およびそれを管理しているクライアント機器が判明するようになっている。しかしながら、上記サーバにおいては、上述したアクセス権制御を行う機能は有しておらず、最終的には、所望のファイルを管理しているアクセス先のクライアント機器自身によって上述と同様のアクセス権制御が行われている。

【０００６】

それ故に、本発明の目的は、ピアツーピア型のファイル交換システムにおけるクライアント機器において、所望のアクセス権制御が実行可能なアクセス権制御システムを提供することである。

【０００７】

上記目的を達成するために、本発明は、以下に述べるような特徴を有している。

第１の発明は、エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、クライアント機器と通信可能に接続され、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、サーバは、アクセス権の問い合わせに対してアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、クライアント機器は、他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をアクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを他の機器に対して直接的に送信するデータ送信部とを含み、アクセス可否問い合わせ部は、他の機器からデータ送信を要求され、その要求に対するアクセス権をアクセス可否判定部に問い合わせるときに、クライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書とを付加してアクセス可否判定部に問い合わせ、アクセス可否判定部は、第１および第２の証明書を用いてアクセス可否問い合わせ部からの問い合わせを認証した後、アクセス権を判断し判断結果を返信する。

【０００８】

第１の発明によれば、データの提供元となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【０００９】

第２の発明は、第１の発明に従属する発明であって、サーバが管理するアクセス権管理リ

ストには、それぞれのクライアント機器が管理するデータ毎にアクセス可能な機器を示すアクセス権が記述され、アクセス可否問い合わせ部は、データ送信を要求されたデータ毎に、アクセス可否判定部に問い合わせを行い、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する。

【００１０】

第２の発明によれば、それぞれのクライアント機器が管理するデータ毎にアクセス権を設定することが可能となる。

【００１１】

第３の発明は、第２の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件がデータ毎に記述され、アクセス可否判定部は、アクセス可否問い合わせ部から問い合わせされた現在時刻に応じて時間条件を参照して、データ毎にそのアクセス権を判断する。

【００１２】

第３の発明によれば、それぞれのクライアント機器が管理するデータ毎に、そのアクセス可能時間を条件としたアクセス権を設定することが可能となる。

【００１３】

第４の発明は、第２の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件がデータ毎に記述され、アクセス可否判定部は、アクセス可否問い合わせ部から問い合わせされた回数に応じて回数条件を参照して、データ毎にそのアクセス権を判断する。

【００１４】

第４の発明によれば、それぞれのクライアント機器が管理するデータ毎に、そのアクセス可能回数を条件としたアクセス権を設定することが可能となる。

【００１５】

第５の発明は、第２の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に複製条件を返信し、データ送信部は、アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを複製条件を付加して他の機器に対して直接的に送信する。

【００１６】

第５の発明によれば、それぞれのクライアント機器が管理するデータ毎に、データ取得後の複製に関する制限を付加することが可能となる。

【００１７】

第６の発明は、第１の発明に従属する発明であって、サーバは、他のプロキシを介してクライアント機器と通信可能に接続されていることを特徴とする。

【００１８】

第６の発明によれば、アクセス権を問い合わせる提供元のクライアント機器がサーバと直接通信が不可能であっても、他のプロキシを介してアクセス権の問い合わせが可能となり、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことができる。

【００２１】

第７の発明は、第１の発明に従属する発明であって、証明書にはＸ．５０９を使用することを特徴とする。

【００２２】

第７の発明によれば、サーバは、Ｘ．５０９方式の証明書を用いて、容易かつ確実に正しいクライアント機器からの通信であることを確認することができる。

【００３７】

第８の発明は、エンドユーザが所有するクライアント機器に対して他の機器から直接的

なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するサーバであって、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理部と、クライアント機器から送信されるアクセス権の問い合わせに対して、アクセス権管理部においてアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を問い合わせたクライアント機器に対して返信するアクセス可否判定部を含み、アクセス可否判定部は、クライアント機器の問い合わせに付加されるクライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書を用いてアクセス可否問い合わせ部からの問い合わせを認証した後、アクセス権を判断し、当該判断結果をアクセス権を問い合わせたクライアント機器に対して返信する。

【００３８】

第８の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ交換を行うクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能なサーバを構成できる。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【００３９】

第９の発明は、他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンドユーザが所有するクライアント機器であって、他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、他の機器の要求に応じて直接的にデータ送信を行うデータ送信部とを含み、アクセス可否問い合わせ部は、要求に対するアクセス権を、クライアント機器であることを証明するための第１の証明書と他の機器を証明するための第２の証明書を付加してサーバに問い合わせることにより、当該サーバに第１の証明書と第２の証明書とを用いて当該アクセス権の問い合わせの認証を行わせる。

【００４０】

第９の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ送信を要求されたクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能なクライアント機器を構成できる。また、提供元のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【００４７】

第１０の発明は、エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、サーバにおいて、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をクライアント機器からサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによる問い合わせに対して、アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権をサーバで判断し判断結果をクライアント機器に返信するアクセス可否判定ステップと、アクセス可否判定ステップによって返信された判断結果がアクセス可の場合、要求されたデータをクライアント機器から他の機器に対して直接

的に送信するデータ送信ステップとを含み、アクセス可否問い合わせステップにおいて、クライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書とを付加してアクセス権が前記サーバに問い合わせられ、アクセス可否判定ステップでは、第１および第２の証明書を用いてクライアント機器からの問い合わせが認証された後、アクセス権が判断され、当該判断結果がクライアント機器に返信される。

【００４８】

第１０の発明によれば、データの提供元となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【００５１】

第１１の発明は、エンドユーザが所有するクライアントに対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断させるためのアクセス権制御プログラムを記録した当該サーバが読み取り可能な記録媒体であって、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、クライアント機器がデータの直接的な送受信を行う際に、当該クライアント機器からサーバに対して行われるその送受信に対するアクセス権の問い合わせに応じて、アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を当該クライアント機器に返信するアクセス可否判定ステップとを含み、アクセス可否判定ステップにおいて、クライアント機器の問い合わせに付加されるクライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の証明書を用いてアクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し、当該判断結果を前記クライアント機器に対して返信する。

【００５２】

第１１の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ交換を行うクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能となる。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【００５３】

第１２の発明は、他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、要求されたデータをクライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含み、アクセス可否問い合わせステップにおいて、他の機器からデータ送信を要求され、その要求に対するアクセス権をアクセス可否判定部に問い合わせるときに、クライアント機器であることを証明するための第１の証明書と当該他の機器を証明するための第２の

証明書とを付加してアクセス可否判定部に問い合わせる。

【００５４】

第１２の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ送信を要求されたクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能となる。また、提供元のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。また、サーバは、第１および第２の証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。

【００５７】

【発明の実施の形態】

（第１の実施形態）

図１を参照して、本発明の第１の実施形態に係るアクセス権制御システムの全体の構成について説明する。図１において、当該アクセス権制御システムは、サーバ１１、アクセス権管理データベース１２、第１のクライアント機器１３、データ記憶装置１４、第２のクライアント機器１５、およびデータ記憶装置１６を備えている。第１および第２のクライアント機器１３および１５は、エンドユーザが所有するＣＰＵを備えた機器であり、互いに直接的に通信するピアツーピアコンピューティングを形成し、ピアツーピア型のファイル交換システムを形成するものである。また、サーバ１１は、上記ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されており、少なくとも第１のクライアント機器１３は、サーバ１１に対してアクセス可能に構成されている。データ記憶装置１４および１６は、それぞれ第１および第２のクライアント機器１３および１５によって管理されるファイル等を格納する記憶装置である。アクセス権管理データベース１２は、サーバ１１によって管理される後述するアクセス権管理リスト等を格納する記憶装置である。

【００５８】

なお、当該実施形態の説明では、説明を単純化するために第２のクライアント機器１５が、第１のクライアント機器１３が管理するデータ記憶装置１４に格納された所望のファイルの提供を受けるためにアクセスする場合を想定し、第１のクライアント機器１３がアクセス先（以下、提供元と記載する）のクライアント機器、第２のクライアント機器１５がアクセス元（以下、提供先と記載する）のクライアント機器として説明を行う。また、当該アクセス権制御システムにおいては、２つ以上のクライアント機器を配置することが可能であるが、ここでは、上記ファイルのアクセスに関連するクライアント機器のみを説明する。

【００５９】

次に、図２を参照して、サーバ１１の内部構成を説明する。なお、図２は、サーバ１１の内部構成を示す機能ブロック図である。図２において、サーバ１１は、アクセス可否判定部１１１、データベース制御部１１２、およびクライアント間通信部１１３を備えている。クライアント間通信部１１３は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器１３とサーバ１１との間の通信を行う。データベース制御部１１２は、アクセス権管理データベース１２に格納されているデータを制御している。例えば、データベース制御部１１２は、アクセス可否判定部１１１からアクセス権管理データベース１２に格納されているデータを要求された場合、その要求に応じてアクセス権管理データベース１２のデータを検索したり、検索後のデータの更新を行ったりする。また、データベース制御部１１２は、クライアント間通信部１１３を介して指示されるクライアント機器からの要求に応じて、アクセス権管理データベース１２のデータを追加したり削除したりする。アクセス可否判定部１１１は、後述する第１のクライアント機器１３からクライアント間通信部１１３を介してアクセス権判定を求められた場合、その内容からアクセス権管理データベース１２のアクセス権管理リストを参照し、そのアクセス権判定結果をクライアン

ト間通信部１１３に返す。また、その判定によって、当該アクセス権管理リストの更新が必要な場合、その更新をデータベース制御部１１２に指示する。

【００６０】

次に、図３を参照して、第１のクライアント機器１３の内部構成について説明する。なお、図３は、第１のクライアント機器１３の内部構成を示す機能ブロック図である。図３において、第１のクライアント機器１３は、サーバ間通信部１３１、アクセス可否問い合わせ部１３２、データ送信部１３３、クライアント間通信部１３４、および記憶装置制御部１３５を備えている。サーバ間通信部１３１は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器１３とサーバ１１との間の通信を行う。また、クライアント間通信部１３４は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器１３と第２のクライアント機器１５の間の通信を行う。データ送信部１３３は、クライアント間通信部１３４を介して第２のクライアント機器１５からデータ記憶装置１４に格納されたデータの一覧を要求された場合、記憶装置制御部１３５を介して、データ記憶装置１４に記憶されたデータの一覧を生成し、第２のクライアント機器１５に当該データ一覧を提供する。また、データ送信部１３３は、サーバ１１からアクセスが可能であることを通知された場合、記憶装置制御部１３５を介してデータ記憶装置１４から要求のあったデータを取得し、このデータをクライアント間通信部１３４を制御して第２のクライアント機器１５に送信する。アクセス可否問い合わせ部１３２は、第２のクライアント機器１５からデータの要求を受け付けた場合、当該データの提供可否を判定するために、サーバ１１へサーバ間通信部１３１を介して問い合わせを行う。また、第１のクライアント機器１３は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第１のクライアント機器１３に設けられたＣＰＵ固有の情報でもよいし、ＩＰアドレスでもかまわない。

【００６１】

次に、図４を参照して、第２のクライアント機器１５の内部構成について説明する。なお、図４は、第２のクライアント機器１５の内部構成を示す機能ブロック図である。図４において、第２のクライアント機器１５は、クライアント間通信部１５１、データ要求部１５２、データ受信部１５３、記憶装置制御部１５４、表示装置１５５、および入力装置１５６を備えている。クライアント間通信部１５１は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器１３と第２のクライアント機器１５の間の通信を行う。表示装置１５５は、例えば第１のクライアント機器１３からクライアント間通信部１５１を介して受け取った上記データ一覧を表示することによって、第２のクライアント機器１５の利用者にデータ一覧からの選択を促す。入力装置１５６は、利用者の操作によって所望のデータを上記データ一覧から選択する。データ要求部１５２は、利用者によって選択されたデータを取得すべく、第１のクライアント機器１３にデータ要求のための通信をクライアント間通信部１５１を介して行う。データ受信部１５３は、上記データ要求が許可された場合、第１のクライアント機器１３からクライアント間通信部１５１を介して当該データを受け取り、記憶装置制御部１５４がデータ記憶装置１６を制御して当該データをデータ記憶装置１６に格納する。また、第２のクライアント機器１５は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第２のクライアント機器１５に設けられたＣＰＵ固有の情報でもよいし、ＩＰアドレスでもかまわない。

【００６２】

なお、当該実施形態では、第１および第２のクライアント機器１３および１５において、それぞれ内部構成が異なる場合を記述した。このような相違は、上述したように第１のクライアント機器１３がデータの提供元であり、第２のクライアント機器１５がデータの提供先と想定していることに起因する。したがって、第１および第２のクライアント機器１３および１５が提供元にも提供先にもなり得る方が都合が良い場合には、それぞれのクライアント機器に両方のクライアント機器が備える機能を備えれば良い。

【００６３】

次に、図５を参照して、アクセス権制御システムの全体処理について説明する。なお、図５は、アクセス権制御システムを構成するサーバ１１、第１および第２のクライアント機器１３および１５が処理する動作を示すフローチャートである。ここで説明するアクセス権制御システムの全体処理についても、第１のクライアント機器１３がデータの提供元であり、第２のクライアント機器１５がデータの提供先と想定し、第２のクライアント機器１５が第１のクライアント機器１３に管理されているデータ記憶装置１４に格納された所望のデータを取得する場合について説明する。なお、このアクセス権制御システムの処理動作は、サーバ１１、第１および第２のクライアント機器１３および１５において、各機器に対応するアクセス権制御プログラムが各機器に備えられている記憶領域に格納され実行されることによって行われる。しかしながら、これらのアクセス権制御プログラムは、サーバ１１、第１および第２のクライアント機器１３および１５が、各機器に対応するそれらを読み出して実行可能である限りにおいて、各機器に備えられている記憶領域以外の他の記憶媒体に格納されていてもかまわない。

【００６４】

図５において、第２のクライアント機器１５のデータ要求部１５２は、第１のクライアント機器１３が管理するデータの一覧を要求するために、その内容が記述されたデータ一覧を第１のクライアント機器１３に要求する（ステップＳ１）。ステップＳ１では、第２のクライアント機器１５の利用者が入力装置１５６を操作することによって、データ要求部１５２にデータ一覧の要求が伝達される。そして、データ要求部１５２によって、クライアント間通信部１５１を介して、第１のクライアント機器１３に上記データ一覧が要求される。

【００６５】

次に、第１のクライアント機器１３のクライアント間通信部１３４は、第２のクライアント機器１５からデータ一覧が要求され、当該データ一覧の要求をデータ送信部１３３に伝える（ステップＳ２）。次に、データ送信部１３３は、記憶装置制御部１３５を制御することによってデータ記憶装置１４で管理されているデータを検索し、データ記憶装置１４で管理されているデータ一覧を作成する（ステップＳ３）。そして、データ送信部１３３は、上記ステップＳ３で作成したデータ一覧を、クライアント間通信部１３４を介して第２のクライアント機器１５に送信する（ステップＳ４）。

【００６６】

次に、第２のクライアント機器１５のクライアント間通信部１５１は、上記ステップＳ４で第１のクライアント機器１３から送信されたデータ一覧を受信し、第２のクライアント機器１５の表示装置１５５によって受信したデータ一覧が表示される（ステップＳ５）。次に、第２のクライアント機器１５の利用者は、表示装置１５５に表示されたデータ一覧から所望のデータを選択し、入力装置１５６を操作することによって選択結果をデータ要求部１５２に伝達する（ステップＳ６）。そして、データ要求部１５２は、ステップＳ６で選択されたデータを識別する提供対象ファイル名および自身を判別するための提供先識別子（つまり、第２のクライアント機器１５の識別子）を、クライアント間通信部１５１を介して送信することによって、第１のクライアント機器１３にデータを要求する（ステップＳ７）。

【００６７】

次に、第１のクライアント機器１３のクライアント間通信部１３４は、第２のクライアント機器１５から要求された上記提供対象ファイル名および上記提供先識別子を受信し、当該要求をアクセス可否問い合わせ部１３２に送る（ステップＳ８）。次に、アクセス可否問い合わせ部１３２は、第２のクライアント機器１５から要求されたデータに対するアクセスの可否を判定するために、当該要求に対するアクセス権問い合わせとして、上記提供対象ファイル名、上記提供先識別子、および自身を判別するための提供元識別子（つまり、第１のクライアント機器１３の識別子）を、サーバ間通信部１３１を介してサーバ１１に送信する（ステップＳ９）。

【００６８】

次に、サーバ１１のクライアント間通信部１１３は、第１のクライアント機器１３からアクセス権問い合わせとして送信された、上記提供対象ファイル名、上記提供先識別子、および上記提供元識別子を、アクセス可否判定部１１１に送る（ステップＳ１０）。次に、アクセス可否判定部１１１は、上記アクセス権問い合わせに対して、データベース制御部１１２を制御してアクセス権管理データベース１２に格納されているアクセス権管理リストを参照して、要求されているデータのアクセス権を判定する（ステップＳ１１）。なお、ステップＳ１１におけるアクセス権判定処理についての詳細な動作は、後述する。そして、アクセス可否判定部１１１は、ステップＳ１１で要求されたデータに対するアクセス権を判定した結果を、クライアント間通信部１１３を介して第１のクライアント機器１３に送信する（ステップＳ１２）。また、上記ステップＳ１１でアクセス権管理リストから参照した登録データにおいて、後述する「複製条件」の制限が記述されている場合、上記ステップＳ１２でその複製条件を示す情報（以下、複製条件情報と記載する）も同時に第１のクライアント機器１３に送信される。

【００６９】

次に、第１のクライアント機器１３のサーバ間通信部１３１は、サーバ１１から送信されたアクセス権判定結果を受信し、データ送信部１３３に送る（ステップＳ１３）。次に、データ送信部１３３は、上記ステップＳ８で第２のクライアント機器１５から要求されたデータのアクセス可否を上記アクセス権判定結果から判断する（ステップＳ１４）。データ送信部１３３は、上記アクセス権判定結果がアクセス可であった場合、上記ステップＳ８で第２のクライアント機器１５から要求されたデータを、記憶装置制御部１３５を制御することによってデータ記憶装置１４から検索し、当該データをクライアント間通信部１３４を介して第２のクライアント機器１５に送信する（ステップＳ１５）。また、上記ステップＳ１２で複製条件情報も同時に送信されている場合、要求されたデータは、その複製条件情報と共に第２のクライアント機器１５に送信される。一方、上記アクセス権判定結果がアクセス不可であった場合、第２のクライアント機器１５に対するデータ送信を拒否する。

【００７０】

次に、第２のクライアント機器１５のクライアント間通信部１５１は、上記ステップＳ１５で送信されたデータを受信し、データ受信部１５３に送る（ステップＳ１６）。そして、データ受信部１５３は、記憶装置制御部１５４を制御することによって、上記ステップＳ１６で受信したデータをデータ記憶装置１６に格納したり、表示装置１５５に当該データを表示したりする。また、上記ステップＳ１６で受信したデータが上記複製条件情報と共に受信された場合、当該データは以後の複製に関して、当該複製条件情報に制限される。なお、この複製の制限については、後述する。

【００７１】

次に、図６を参照して、アクセス権管理データベース１２に格納されているアクセス権管理リストのデータ構造について説明する。なお、図６は、アクセス権管理データベース１２に格納されているアクセス権管理リストの一例である。図６において、アクセス権管理データベース１２に格納されているアクセス権管理リストに登録されるデータは、「番号」、「提供元識別子」、「ファイル名」、「提供先識別子」、「時間条件」、「回数条件」、および「複製条件」の７つの項目から構成されている。

【００７２】

上記アクセス権管理リストの「番号」は、アクセス権管理データベース１２において、各登録データを管理するために使用する重複を避けた自然数の番号である。

【００７３】

上記アクセス権管理リストの「提供元識別子」は、データの提供元である端末（つまり、提供元のクライアント機器）を特定するための、各クライアント機器固有の識別子である。

【００７４】

上記アクセス権管理リストの「ファイル名」は、アクセス対象となるデータのファイル名

である。なお、このファイル名は、コンテンツに固有の識別情報であるコンテンツＩＤを記載してもかまわない。

【００７５】

上記アクセス権管理リストの「提供先識別子」は、データの提供先である端末（つまり、提供先のクライアント機器）を特定するための、各クライアント機器固有の識別子である。なお、この「提供先識別子」には、特定のクライアント機器が指定されるのみではなく、任意のクライアント機器に対してアクセスが許可される場合、「任意」と記述される。また、全てのクライアント機器に対してアクセスの許可をしない場合、「不可」と記述あるいは未記述とされる。

【００７６】

上記アクセス権管理リストの「時間条件」は、データの提供が許可される期日を指定したり、データの提供が許可される期間を指定したりするアクセス許可を行う時間的な制限である。なお、そのデータのアクセスに時間的な制限を設けない場合、「任意」と記述される。

【００７７】

上記アクセス権管理リストの「回数条件」は、データの提供元である端末から、データの提供が許可される回数に関する条件である。この「回数条件」に、上記回数が設定されるデータでは、サーバ１１がそのデータに対するアクセス権を付与すると「回数条件」が更新され、「回数条件」が「０回」に更新された時点で、以降のアクセスが許可されなくなる。なお、アクセス権管理リストのデータに回数に関する条件を設けない場合、「任意」と記述される。

【００７８】

上記アクセス権管理リストの「複製条件」は、提供されたデータを提供先の端末において更に複製することが許可されるか否かを示す条件である。この「複製条件」には、登録データに対して提供後の複製が許可されていない場合、「不可」と記述され、特に複製に関する条件を設けない場合、「任意」と記述され、複製世代数を制限する場合、その世代数（例えば、「番号」「４」に記述された「１世代のみ可」）が記述される。

【００７９】

上述した項目毎に、登録データがアクセス権管理リストに記述される。例えば、「番号」が「１」の登録データは、「提供元識別子」が「１１１１」に端末に記憶されている「ファイル名」「産声．ｗａｖ」という音声ファイルに関するアクセス権を管理するための登録データである。この音声ファイルには、「提供先識別子」が「２２２２」の端末のみがアクセスすることが可能である。そして、上記「２２２２」の端末がアクセスの日時や回数に関する制約は設けられていない。ただし、提供先の「２２２２」の端末では、提供されたファイル「産声．ｗａｖ」を更に複製することは禁止されている。

【００８０】

また、例えば、「番号」が「４」の登録データは、「提供元識別子」が「１１１１」の端末に記憶されている「ファイル名」「子供．ｊｐｇ」という画像ファイルに関するアクセス権を管理するための登録データである。この画像ファイルには、「提供先識別子」が「２２２２」および「３３３３」の端末のみがアクセスすることが可能である。そして、上記「２２２２」および「３３３３」の端末がアクセス可能な日時は、「２００１／０７／３１まで」に限定、つまり、２００１年7月３１日までアクセス可能であり、それ以降はアクセス不可能である。なお、上記「２２２２」および「３３３３」の端末がアクセスする回数に関する制約はない。また、提供先の「２２２２」および「３３３３」端末では、提供されたファイル「子供．ｊｐｇ」を更に１世代のみ複製することが許可されている。

【００８１】

さらに、「番号」が「９」の登録データは、特殊なアクセス権を管理するための登録データである。この登録データでは、「提供元識別子」が「４４４４」の端末が、「提供先識別子」が「１１１１」の端末に対するアクセス権管理用のデータであるが、「ファイル名」に関しては「任意」となっている。つまり、当該「４４４４」の端末に格納された全て

のファイルに対して、「１１１１」の端末がアクセス可能ということを意味している。このような利用形態は、「番号」が「１１１１」および「４４４４」の端末の所有者が同一人物であり、相互にファイルアクセスを無条件に許可する場合などに利用される。

【００８２】

なお、上述したアクセス権管理データベース１２に格納されているアクセス権管理リストに記述される登録データは、以下の条件によって記述することができる。

条件１：サーバ１１がアクセス権を管理する全てのクライアント機器が管理しているデータの内、他のクライアント機器に提供可能あるいは何らかの条件を付与して提供可能なデータを、アクセス権管理リストに記述する。（つまり、アクセス権管理リストに記述されていないデータはアクセス不可）

条件２：サーバ１１がアクセス権を管理する全てのクライアント機器が管理しているデータの内、他のクライアント機器に提供不可能あるいは何らかの条件を付与して提供可能なデータを、アクセス権管理リストに記述する。（つまり、アクセス権管理リストに記述されていないデータはアクセス可）

【００８３】

次に、上記ステップＳ１１（図５を参照）でアクセス可否判定部１１１が行うアクセス権判定処理について、詳細な動作を説明する。なお、図７は、アクセス可否判定部１１１が行うアクセス権判定処理の詳細動作の一例を示す上記ステップＳ１１のサブルーチンである。また、上述したアクセス権管理データベース１２に格納されているアクセス権管理リストに記述される登録データは、上記条件１（つまり、アクセス権管理リストに記述されていないデータは、アクセス不可）に基づいて記述されているとして説明を行う。

【００８４】

図７において、アクセス可否判定部１１１は、提供元のクライアント機器を判別するための提供元識別子、提供先のクライアント機器を判別するための提供先識別子、および提供対象となるデータを識別するための提供対象ファイル名が記述されたアクセス権問い合わせを取得する（ステップＳ１１１）。次に、アクセス可否判定部１１１は、当該サブルーチンで利用する一時変数であるｎを初期化するために、１にセットする（ステップＳ１１２）。

【００８５】

次に、アクセス可否判定部１１１は、上記ステップＳ１１１で取得した提供元識別子と、アクセス権管理データベース１２に格納されている上記アクセス権管理リストに記述されている「番号」が「ｎ」の登録データの「提供元識別子」とが一致しているか否かを判定する（ステップＳ１１３）。そして、アクセス可否判定部１１１は、上記ステップＳ１１３で一致している場合、次のステップＳ１１４に処理を進める。一方、アクセス可否判定部１１１は、上記ステップＳ１１３で一致していない場合、次のステップＳ１１９に処理を進める。

【００８６】

ステップＳ１１４では、アクセス可否判定部１１１は、上記ステップＳ１１１で取得した提供対象ファイル名と、上記アクセス権管理リストに記述されている「番号」が「ｎ」の登録データの「ファイル名」とが一致しているか否かを判定する。なお、上述したようにアクセス権管理リストの「ファイル名」には、「任意」と設定されていることもある。この場合、アクセス可否判定部１１１は、上記ステップＳ１１１で取得した提供対象ファイル名が、アクセス権管理リストの「ファイル名」と一致していると判断する。そして、アクセス可否判定部１１１は、上記ステップＳ１１４で一致している場合、次のステップＳ１１５に処理を進める。一方、アクセス可否判定部１１１は、上記ステップＳ１１４で一致していない場合、次のステップＳ１１９に処理を進める。

【００８７】

ステップＳ１１５では、アクセス可否判定部１１１は、上記ステップＳ１１１で取得した提供先識別子と、上記アクセス権管理リストに記述されている「番号」が「ｎ」の登録データの「提供先識別子」とが一致しているか否かを判定する。なお、上述したようにアク

セス権管理リストの「提供先識別子」には、「任意」と設定されていることもある。この場合、アクセス可否判定部１１１は、上記ステップＳ１１１で取得した提供先識別子が、アクセス権管理リストの「提供先識別子」と一致していると判断する。そして、アクセス可否判定部１１１は、上記ステップＳ１１５で一致している場合、次のステップＳ１１６に処理を進める。一方、アクセス可否判定部１１１は、上記ステップＳ１１５で一致していない場合、次のステップＳ１１９に処理を進める。

【００８８】

ステップＳ１１６では、アクセス可否判定部１１１は、現在時刻と上記アクセス権管理リストに記述されている「番号」が「ｎ」の登録データの「時間条件」とを比較し、アクセス可否を判定する。このアクセス可否判定部１１１が行う上記比較は、「時間条件」に「任意」と記述されている場合、アクセス可と判定され、「時間条件」に時間的な制約が記述されている場合、現在時刻がその制約を満足するか否かで判定される。そして、アクセス可否判定部１１１は、上記ステップＳ１１６でアクセス可と判断した場合、次のステップＳ１１７に処理を進める。一方、アクセス可否判定部１１１は、上記ステップＳ１１６でアクセス不可と判断した場合、次のステップＳ１１９に処理を進める。

【００８９】

ステップＳ１１７では、アクセス可否判定部１１１は、上記アクセス権管理リストに記述されている「番号」が「ｎ」の登録データの「回数条件」を参照してアクセス可否を判定する。このアクセス可否判定部１１１が行う上記判定は、「回数条件」に「任意」あるいは「１回以上の回数」が記述されている場合、アクセス可と判定され、「回数条件」に「０回」が記述されている場合、アクセス不可と判定される。また、アクセス可否判定部１１１は、「回数条件」に「１回以上の回数」が記述され、アクセス可と判定した後、当該「回数条件」に記述されている回数を１だけ減らしてアクセス権管理リストを更新する。そして、アクセス可否判定部１１１は、上記ステップＳ１１７でアクセス可と判断した場合、次のステップＳ１１８に処理を進める。一方、アクセス可否判定部１１１は、上記ステップＳ１１７でアクセス不可と判断した場合、次のステップＳ１１９に処理を進める。

【００９０】

なお、上記ステップＳ１１７では、上記アクセス権管理リストの「回数条件」の更新として、アクセス可と判定された場合にどのクライアント機器からのアクセスにおいても必ず回数を１回減らす方法を説明した。しかしながら、複数の「提供先識別子」が設定されている場合、それらのクライアント機器が１つの「回数条件」を共有するのではなく、データの提供先の各クライアント機器毎に「回数条件」を持たせてもかまわない。

【００９１】

ステップＳ１１８では、アクセス可否判定部１１１は、上記ステップＳ１１１で取得したアクセス権問い合わせに対して、アクセス可と判断し、当該サブルーチンを終了する。なお、このステップＳ１１８の処理には、上述したステップＳ１１３～Ｓ１１７でアクセス可否判定部１１１が上記ステップＳ１１１で取得したアクセス権問い合わせの内容に一致し、かつアクセス条件を全て満たす場合のみ進むことができるため、アクセス可否判定部１１１は、上記アクセス権管理リストの登録データ記述に一致し、それぞれの条件を満たすクライアント機器にのみアクセス可の判定を行うことになる。

【００９２】

一方、上述したように、アクセス可否判定部１１１は、上記ステップＳ１１１で取得したアクセス権問い合わせが、上記ステップＳ１１３～Ｓ１１７で判定したいずれかの結果を満たさない場合、ステップＳ１１９に処理を進める。ステップＳ１１９では、アクセス可否判定部１１１は、当該サブルーチンで利用する一時変数であるｎを１だけ増やしてｎ＋１として、ステップＳ１２０に処理を進める。

【００９３】

ステップＳ１２０では、アクセス可否判定部１１１は、現在の一時変数であるｎが上記アクセス権管理リストのデータ登録数であるＮより大きいか否かを判断する。そして、アクセス可否判定部１１１は、ｎ＞Ｎの場合、上記アクセス権管理リストの登録データを全て

探索したと判断して、次のステップＳ１２１に処理を進める。一方、アクセス可否判定部１１１は、ｎ≦Ｎの場合、上記アクセス権管理リストに探索されていない登録データがあると判断して、上記ステップＳ１１３に戻り、上記ステップＳ１１９で設定した新たな「番号」に対して同様の探索を行う。

【００９４】

ステップＳ１２１では、アクセス可否判定部１１１は、上記ステップＳ１１１で取得したアクセス権問い合わせに対して、アクセス不可と判断し、当該サブルーチンを終了する。なお、このステップＳ１２１の処理には、上述したステップＳ１１３～Ｓ１１７でアクセス可否判定部１１１が上記ステップＳ１１１で取得したアクセス権問い合わせの内容が一致しない、あるいはアクセス条件のいずれかが満たさない場合に処理される。つまり、アクセス可否判定部１１１は、アクセス権問い合わせの内容が、上記アクセス権管理リストの登録データ記述のいずれかに一致しない、あるいは、それぞれの条件のいずれかを満たさないクライアント機器に対しては、アクセス不可の判定を行うことになる。

【００９５】

なお、上述した図７で示したアクセス可否判定部１１１が行うアクセス権判定処理は、アクセス権管理データベース１２に格納されているアクセス権管理リストに記述される登録データが、上記条件１に基づいて記述されているとして説明したが、上記登録データが、上記条件２（つまり、アクセス権管理リストに記述されていないデータはアクセス可）に基づいて記述されていてもかまわない。その場合、上述した図７で示したアクセス可否判定部１１１が行うアクセス権判定処理の動作手順を、以下に述べるステップのみ変更することによって対応可能である。つまり、図８を参照して、アクセス可否判定部１１１は、上記ステップＳ１１５～Ｓ１１７で「ｎｏ」と判定した場合、上記ステップＳ１２１に処理を進め、上記ステップＳ１１１で取得したアクセス権問い合わせに対して、アクセス不可と判断し、当該サブルーチンを終了する。また、アクセス可否判定部１１１は、上記ステップＳ１２０でｎ＞Ｎの場合、上記ステップＳ１１８に処理を進め、上記ステップＳ１１１で取得したアクセス権問い合わせに対して、アクセス可と判断し、当該サブルーチンを終了する。このように、アクセス可否判定部１１１は、複数の記述条件で記述されたアクセス権管理リストに対して、その記述条件に応じた動作手順を用いることによって、適切にアクセス可否の判定が可能である。

【００９６】

なお、第１の実施形態の説明では、第１および第２のクライアント機器１３および１５の認証に関する手法を記述していないが、サーバ１１と第１および第２のクライアント機器１３および１５との間で、認証によって正しいクライアント機器からの通信であることを確認してもかまわない。つまり、第２のクライアント機器１５から第１のクライアント機器１３への通信の際には、第２のクライアント機器１５であることを証明するための第２のクライアント証明書を送信し、第１のクライアント機器１３からサーバ１１への通信の際には、上記第２のクライアント証明書および第１のクライアント機器１３であることを証明する第１のクライアント証明書を、サーバ１１に送信することによって、サーバ１１は、これらの証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。このときに用いられる証明書としては、例えば、電子鍵証明書および証明書失効リストの標準仕様であるＸ．５０９等を用いることができる。

【００９７】

また、サーバ１１から第１のクライアント機器１３に対して、アクセス権の判定結果と共に複製条件情報が送信される場合、サーバ１１は、この複製条件情報に対して所定の暗号化を行う。例えば、サーバ１１が所有する秘密鍵で上記複製条件情報に署名して送信することによって、この複製条件が適用されるデータが提供される第２のクライアント機器１５に対して正当性が保証される。また、この複製条件が適用されるデータは、ＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）方式で暗号化される。例えば、データの提供元である第１のクライアント機器１３では、サーバ１１からアクセス権の判定結果と共に複製条件情報が送信された場合、その複製条件情報が適用されるデータに対し

て第２のクライアント機器１５が公開する公開鍵で暗号化し、上記複製条件情報と共に第２のクライアント機器１５に送信する。そして、第２のクライアント機器１５では、秘密鍵を耐タンパ領域に格納し、当該機器の利用者に対しても秘密になるように保持しておく。これによって、第２のクライアント機器１５以外に上記データを不正にコピーした場合でもデータの復号化は不可能であり、実質的に複製が制限される。また、上記複製条件にしたがってコピーを行う場合には、暗号化されたデータを第２のクライアント機器１５の秘密鍵で一度復号化し、再度複製先機器が公開する公開鍵を用いて暗号化することによって、複製を制限することが可能である。なお、ここではデータを直接公開鍵で暗号化するとしたが、データを共通鍵方式の暗号鍵で暗号化し、さらにここで使用した暗号鍵を第２のクライアント機器１５が公開する公開鍵を用いて第１のクライアント機器１３が暗号化し、暗号化したデータと共に暗号鍵を送信してもかまわない。なお、上記複製条件情報の署名が改竄されている（つまり、サーバ１１からの情報ではない）場合、その複製条件情報が適用されるデータに対する複製は不可とされる。

【００９８】

また、サーバ１１と第１および第２のクライアント機器１３および１５との間で行われる通信の経路に関する秘匿性・耐改竄性については、第１の実施形態では特に手法を記述していないが、秘密鍵方式とセッション鍵とを組み合わせた暗号化方式による暗号化通信を行ってもかまわない。このような暗号化通信としては、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）等を用いることができる。

【００９９】

また、第１の実施形態では、第１のクライアント機器１３は、上記ステップＳ３において、自身が管理しているデータ記憶装置１４に格納されたデータをデータ一覧として作成したが、第２のクライアント機器１５がアクセス可能なデータのみを上記データ一覧として作成してもかまわない。これは、第１のクライアント機器１３が、上記ステップＳ２で第２のクライアント機器１５からデータ一覧要求を受信することによって、サーバ１１に対して第２のクライアント機器１５がアクセス可能なデータ返信するように、アクセス権問い合わせを行う。そのアクセス権問い合わせの結果、送信される第２のクライアント機器１５に提供可能と判断されたデータに基づいて、上記データ一覧を作成することによって、アクセス可能なデータのみを上記データ一覧として作成することができる。なお、上記アクセス可能なデータのみが記載されたデータ一覧を用いて、第２のクライアント機器１５がデータの要求を行った後も、第１のクライアント機器１３は、再度サーバ１１に対してアクセス権問い合わせを行ってもかまわない。

【０１００】

このように、第１の実施形態に係るアクセス権制御システムによれば、データの提供元となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【０１０１】

（第２の実施形態）

図９を参照して、本発明の第２の実施形態に係るアクセス権制御システムの全体の構成について説明する。なお、上述した第１の実施形態では、データの提供元であるクライアント機器（つまり、アクセス先の第１のクライアント機器１３）がアクセス権の問い合わせをサーバ１１に対して行ったが、第２の実施形態では、データの提供先であるクライアント機器（つまり、アクセス元のクライアント機器）がアクセス権の問い合わせをサーバに

対して行うアクセス権制御システムである。

【０１０２】

図９において、当該アクセス権制御システムは、サーバ２１、アクセス権管理データベース２２、第１のクライアント機器２３、データ記憶装置２４、第２のクライアント機器２５、およびデータ記憶装置２６を備えている。第１および第２のクライアント機器２３および２５は、エンドユーザが所有するＣＰＵを備えた機器であり、互いに直接的に通信するピアツーピアコンピューティングを形成し、ピアツーピア型のファイル交換システムを形成するものである。また、サーバ２１は、上記ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されており、少なくとも第２のクライアント機器２５は、サーバ２１に対してアクセス可能に構成されている。データ記憶装置２４および２６は、それぞれ第１および第２のクライアント機器２３および２５によって管理されるファイル等を格納する記憶装置である。アクセス権管理データベース２２は、サーバ２１によって管理される後述するアクセス権管理リスト等を格納する記憶装置である。

【０１０３】

なお、当該実施形態の説明では、説明を単純化するために第２のクライアント機器２５が、第１のクライアント機器２３が管理するデータ記憶装置２４に格納された所望のファイルの提供を受けるためにアクセスする場合を想定し、第１のクライアント機器２３がアクセス先（以下、提供元と記載する）のクライアント機器、第２のクライアント機器２５がアクセス元（以下、提供先と記載する）のクライアント機器として説明を行う。また、当該アクセス権制御システムにおいては、２つ以上のクライアント機器を配置することが可能であるが、ここでは、上記ファイルのアクセスに関連するクライアント機器のみを説明する。

【０１０４】

次に、図１０を参照して、サーバ２１の内部構成を説明する。なお、図１０は、サーバ２１の内部構成を示す機能ブロック図である。図１０において、サーバ２１は、アクセス可否判定部２１１、データベース制御部２１２、およびクライアント間通信部２１３を備えている。クライアント間通信部２１３は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第２のクライアント機器２５とサーバ２１との間の通信を行う。データベース制御部２１２は、アクセス権管理データベース２２に格納されているデータを制御している。例えば、データベース制御部２１２は、アクセス可否判定部２１１からアクセス権管理データベース２２に格納されているデータを要求された場合、その要求に応じてアクセス権管理データベース２２のデータを検索したり、検索後のデータの更新を行ったりする。また、データベース制御部２１２は、クライアント間通信部２１３を介して指示されるクライアント機器からの要求に応じて、アクセス権管理データベース２２のデータを追加したり削除したりする。アクセス可否判定部２１１は、後述する第２のクライアント機器２５からクライアント間通信部２１３を介してアクセス権判定を求められた場合、その内容からアクセス権管理データベース２２のアクセス権管理リストを参照し、そのアクセス権判定結果をクライアント間通信部２１３に返す。また、その判定によって、当該アクセス権管理リストの更新が必要な場合、その更新をデータベース制御部２１２に指示する。

【０１０５】

次に、図１１を参照して、第１のクライアント機器２３の内部構成について説明する。なお、図１１は、第１のクライアント機器２３の内部構成を示す機能ブロック図である。図１１において、第１のクライアント機器２３は、クライアント間通信部２３１、データ送信部２３２、および記憶装置制御部２３３を備えている。クライアント間通信部２３１は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器２３と第２のクライアント機器２５の間の通信を行う。データ送信部２３２は、クライアント間通信部２３１を介して第２のクライアント機器２５からデータ記憶装置２４に格納されたデータの一覧を要求された場合、記憶装置制御部２３３を介して、データ記憶装置２４に記憶されたデータの一覧を生成し、第２のクライアント機器２５に当該データ一覧を提供する。また、デ

ータ送信部２３２は、第２のクライアント機器２５からサーバ２１がアクセスが可能であることを判定した結果が送信された場合、記憶装置制御部２３３を介してデータ記憶装置２４から要求のあったデータを取得し、このデータをクライアント間通信部２３１を制御して第２のクライアント機器２５に送信する。また、第１のクライアント機器２３は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第１のクライアント機器２３に設けられたＣＰＵ固有の情報でもよいし、ＩＰアドレスでもかまわない。

【０１０６】

次に、図１２を参照して、第２のクライアント機器２５の内部構成について説明する。なお、図１２は、第２のクライアント機器２５の内部構成を示す機能ブロック図である。図１２において、第２のクライアント機器２５は、サーバ間通信部２５１、アクセス可否問い合わせ部２５２、データ要求部２５３、クライアント間通信部２５４、記憶装置制御部２５５、およびデータ受信部２５６、表示装置２５７および入力装置２５８を備えている。サーバ間通信部２５１は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第２のクライアント機器２５とサーバ２１との間の通信を行う。また、クライアント間通信部２５４は、ＴＣＰ／ＩＰ等のプロトコルを使用し、第１のクライアント機器２３と第２のクライアント機器２５の間の通信を行う。表示装置２５７は、例えば第１のクライアント機器２３からクライアント間通信部２５４を介して受け取った上記データ一覧を表示することによって、第２のクライアント機器２５の利用者にデータ一覧からの選択を促す。入力装置２５８は、利用者の操作によって所望のデータを上記データ一覧から選択する。データ要求部２５３は、アクセス可否問い合わせ部２５２に利用者によって選択されたデータに対するアクセス権の判定の問い合わせを指示し、その判定結果に基づいて上記選択されたデータを取得すべく、第１のクライアント機器２３にデータ要求のための通信をクライアント間通信部２５４を介して行う。アクセス可否問い合わせ部２５２は、データ要求部２５３からデータの要求を受け付けた場合、当該データのアクセス可否を判定するために、サーバ２１へサーバ間通信部２５１を介して問い合わせを行う。データ受信部２５６は、上記アクセスが許可された場合、第１のクライアント機器２３からクライアント間通信部２５４を介して当該データを受け取り、記憶装置制御部２５５がデータ記憶装置２６を制御して当該データをデータ記憶装置２６に格納する。また、第２のクライアント機器２５は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第２のクライアント機器２５に設けられたＣＰＵ固有の情報でもよいし、ＩＰアドレスでもかまわない。

【０１０７】

なお、当該実施形態では、第１および第２のクライアント機器２３および２５において、それぞれ内部構成が異なる場合を記述した。このような相違は、上述したように第１のクライアント機器２３がデータの提供元であり、第２のクライアント機器２５がデータの提供先と想定していることに起因する。したがって、第１および第２のクライアント機器２３および２５が提供元にも提供先にもなり得る方が都合が良い場合には、それぞれのクライアント機器に両方のクライアント機器が備える機能を備えれば良い。

【０１０８】

次に、図１３を参照して、第２の実施形態に係るアクセス権制御システムの全体処理について説明する。なお、図１３は、アクセス権制御システムを構成するサーバ２１、第１および第２のクライアント機器２３および２５が処理する動作を示すフローチャートである。ここで説明するアクセス権制御システムの全体処理についても、第１のクライアント機器２３がデータの提供元であり、第２のクライアント機器２５がデータの提供先と想定し、第２のクライアント機器２５が第１のクライアント機器２３に管理されているデータ記憶装置２４に格納された所望のデータを取得する場合について説明する。なお、このアクセス権制御システムの処理動作は、サーバ２１、第１および第２のクライアント機器２３および２５において、各機器に対応するアクセス権制御プログラムが各機器に備えられている記憶領域に格納され実行されることによって行われる。しかしながら、これらのア

クセス権制御プログラムは、サーバ２１、第１および第２のクライアント機器２３および２５が、各機器に対応するそれらを読み出して実行可能である限りにおいて、各機器に備えられている記憶領域以外の他の記憶媒体に格納されていてもかまわない。

【０１０９】

図１３において、第２のクライアント機器２５のデータ要求部２５３は、第１のクライアント機器２３が管理するデータの一覧を要求するために、その内容が記述されたデータ一覧を第１のクライアント機器２３に要求する（ステップＳ２１）。ステップＳ２１では、第２のクライアント機器２５の利用者が入力装置２５８を操作することによって、データ要求部２５３にデータ一覧の要求が伝達される。そして、データ要求部２５３によって、クライアント間通信部２５４を介して、第１のクライアント機器２３に上記データ一覧が要求される。

【０１１０】

次に、第１のクライアント機器２３のクライアント間通信部２３１は、第２のクライアント機器２５からデータ一覧が要求され、当該データ一覧の要求をデータ送信部２３２に伝える（ステップＳ２２）。次に、データ送信部２３２は、記憶装置制御部２３３を制御することによってデータ記憶装置２４で管理されているデータを検索し、データ記憶装置２４で管理されているデータ一覧を作成する（ステップＳ２３）。そして、データ送信部２３２は、上記ステップＳ２３で作成したデータ一覧を、クライアント間通信部２３１を介して第２のクライアント機器２５に送信する（ステップＳ２４）。

【０１１１】

次に、第２のクライアント機器２５のクライアント間通信部２５４は、上記ステップＳ２４で第１のクライアント機器２３から送信されたデータ一覧を受信し、第２のクライアント機器２５の表示装置２５７によって受信したデータ一覧が表示される（ステップＳ２５）。次に、第２のクライアント機器２５の利用者は、表示装置２５７に表示されたデータ一覧から所望のデータを選択し、入力装置２５８を操作することによって選択結果をデータ要求部２５３に伝達する（ステップＳ２６）。そして、データ要求部２５３は、ステップＳ２６で選択されたデータを識別する提供対象ファイル名および提供元の端末を判別するための提供元識別子（つまり、第１のクライアント機器２３の識別子）を、アクセス可否問い合わせ部２５２に送る。次に、アクセス可否問い合わせ部２５２は、データ要求部２５３によって要求されたデータに対するアクセスの可否を判定するために、当該要求に対するアクセス権問い合わせとして、上記提供対象ファイル名、上記提供元識別子、および自身を判別するための提供先識別子（つまり、第２のクライアント機器２５の識別子）を、サーバ間通信部２５１を介してサーバ２１に送信する（ステップＳ２７）。

【０１１２】

次に、サーバ２１のクライアント間通信部２１３は、第２のクライアント機器２５からアクセス権問い合わせとして送信された、上記提供対象ファイル名、上記提供先識別子、および上記提供元識別子を、アクセス可否判定部２１１に送る（ステップＳ２８）。次に、アクセス可否判定部２１１は、上記アクセス権問い合わせに対して、データベース制御部２１２を制御してアクセス権管理データベース２２に格納されているアクセス権管理リストを参照して、要求されているデータのアクセス権を判定する（ステップＳ２９）。なお、ステップＳ２９におけるアクセス権判定処理については、後述する。そして、アクセス可否判定部２１１は、ステップＳ２９で要求されたデータに対するアクセス権を判定した結果に対して所定の暗号化を行った後、クライアント間通信部２１３を介して第２のクライアント機器２５に送信する（ステップＳ３０）。また、上記ステップＳ２９でアクセス権管理リストから参照した登録データにおいて、「複製条件」の制限が記述されている場合、上記ステップＳ３０でその複製条件情報も同時に第２のクライアント機器２５に送信される。

【０１１３】

なお、上記ステップＳ３０で行うアクセス権を判定した結果に対する暗号化は、サーバ２１でのアクセス権の判定結果に対する正当性を保証するためである。例えば、上記アクセ

ス権の判定結果を第１のクライアント機器２３が公開する公開鍵で暗号化する、あるいは、サーバ２１が所有する秘密鍵で署名したデータを付加して送信することによって、上記正当性が保証される。つまり、この暗号化によって、通信途上での改竄を防止することができ、後述する第１のクライアント機器２３の正当性評価では、確実にサーバ２１が判定した結果であることを判断することが可能である。

【０１１４】

次に、第２のクライアント機器２５のサーバ間通信部２５１は、サーバ２１から送信されたアクセス権判定結果を受信し、データ要求部２５３に送る（ステップＳ３１）。次に、データ要求部２５３は、上記アクセス権判定結果によって上記ステップＳ２６で選択したデータに対するアクセスが可能か否かを判断する（ステップＳ３２）。データ要求部２５３は、上記アクセス権判定結果がアクセス可であった場合、上記提供対象ファイル名をサーバ２１から送信された上記アクセス権判定結果と共に、クライアント間通信部２５４を介して送信することによって、第１のクライアント機器２３にデータを要求する（ステップＳ３３）。また、上記ステップＳ３０で複製条件情報も同時に送信されている場合、その複製条件情報と共に第１のクライアント機器２３に要求される。一方、上記アクセス権判定結果がアクセス不可であった場合、第２のクライアント機器２５は、第１のクライアント機器２３に対するデータ要求を中止する。

【０１１５】

次に、第１のクライアント機器２３のクライアント間通信部２３１は、第２のクライアント機器２５から要求された上記提供対象ファイル名および上記アクセス権判定結果を受信し、データ送信部２３２に送る（ステップＳ３４）。そして、データ送信部２３２は、上記アクセス権判定結果の正当性をサーバ２１によって判定された結果か否か等によって判断する（ステップＳ３５）。このステップＳ３５では、データ送信部２３２は、上記ステップＳ３０でサーバ２１によって暗号化されたアクセス権判定結果を解くことによって、その正当性を確認することができる。そして、データ送信部２３２は、上記アクセス権判定結果が正当であった場合、第２のクライアント機器２５から要求されたデータを、記憶装置制御部２３３を制御することによってデータ記憶装置２４から検索し、当該データをクライアント間通信部２３１を介して第２のクライアント機器２５に送信する（ステップＳ３６）。また、上記ステップＳ３３で複製条件情報も同時に送信されている場合、要求されたデータは、その複製条件情報と共に第２のクライアント機器２５に送信される。一方、上記アクセス権判定結果が不当であった場合、第２のクライアント機器２５に対するデータ送信を拒否する。

【０１１６】

次に、第２のクライアント機器２５のクライアント間通信部２５４は、上記ステップＳ３６で送信されたデータを受信し、データ受信部２５６に送る（ステップＳ３７）。そして、データ受信部２５６は、記憶装置制御部２５５を制御することによって、上記ステップＳ３７で受信したデータをデータ記憶装置２６に格納したり、表示装置２５７に当該データを表示したりする。また、上記ステップＳ３７で受信したデータが上記複製条件情報と共に受信された場合、当該データは以後の複製に関して、当該複製条件情報に制限される。なお、この複製の制限については、後述する。

【０１１７】

アクセス権管理データベース２２に格納されているアクセス権管理リストのデータ構造については、図６を用いて説明した第１の実施形態のデータ構造と同様である。また、上記ステップＳ２９（図１３を参照）でアクセス可否判定部２１１が行うアクセス権判定処理の詳細な動作についても、図７を用いて説明した第１の実施形態のサブルーチンと同様である。つまり、アクセス可否判定部２１１は、第２の実施形態においても、複数の記述条件で記述されたアクセス権管理リストに対して、その記述条件に応じた動作手順を用いることによって、適切にアクセス可否の判定が可能である。したがって、第２の実施形態において、アクセス権管理リストのデータ構造およびアクセス可否判定部２１１が行うアクセス権判定処理の詳細な動作についての詳細な説明は省略する。

【０１１８】
なお、第２の実施形態では、第１のクライアント機器２３は、上記ステップＳ２３において、自身が管理しているデータ記憶装置２４に格納されたデータをデータ一覧として作成したが、第２のクライアント機器２５が第１のクライアント機器２３からアクセス可能なデータのみを、サーバ２１に問い合わせることによって、サーバ２１から上記データ一覧を取得してもかまわない。これは、第２のクライアント機器２５が、上記ステップＳ２１でデータ一覧要求をサーバ２１に送信することによって、第２のクライアント機器２５がアクセス可能なデータ返信するように、アクセス権問い合わせを行う。そして、サーバ２１において第２のクライアント機器２５がアクセス可能なデータをアクセス権管理リストから検索して上記データ一覧を作成することによって、アクセス可能なデータのみを上記データ一覧として作成し、第２のクライアント機器２５に送信することができる。
【０１１９】
また、第２の実施形態の説明では、第２のクライアント機器２５の認証に関する手法を記述していないが、サーバ２１と第１および第２のクライアント機器２３および２５との間で、認証によって正しいクライアント機器からの通信であることを確認してもかまわない。つまり、第２のクライアント機器２５から第１のクライアント機器２３あるいはサーバ２１への通信の際には、第２のクライアント機器２５であることを証明するための第２のクライアント証明書を送信することによって、サーバ２１および第１のクライアント機器２３は、この証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。このときに用いられる証明書としては、例えば、電子鍵証明書および証明書失効リストの標準仕様であるＸ．５０９等を用いることができる。
【０１２０】
また、サーバ２１から第２のクライアント機器２５に対して、アクセス権の判定結果と共に複製条件情報が送信される場合、サーバ２１は、この複製条件情報に対して所定の暗号化を行う。例えば、サーバ２１が所有する秘密鍵で上記複製条件情報に署名して送信することによって、この複製条件が適用されるデータが提供される第２のクライアント機器２５に対して正当性が保証される。また、この複製条件が適用されるデータは、ＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）方式で暗号化される。例えば、データの提供元である第１のクライアント機器２３では、サーバ２１からアクセス権の判定結果と共に複製条件情報が送信された場合、その複製条件情報が適用されるデータに対して第２のクライアント機器２５が公開する公開鍵で暗号化し、上記複製条件情報と共に第２のクライアント機器２５に送信する。そして、第２のクライアント機器２５では、秘密鍵を耐タンパ領域に格納し、当該機器の利用者に対しても秘密になるように保持しておく。これによって、第２のクライアント機器２５以外に上記データを不正にコピーした場合でもデータの復号化は不可能であり、実質的に複製が制限される。また、上記複製条件にしたがってコピーを行う場合には、暗号化されたデータを第２のクライアント機器２５の秘密鍵で一度復号化し、再度複製先機器が公開する公開鍵を用いて暗号化することによって、複製を制限することが可能である。なお、ここではデータを直接公開鍵で暗号化するとしたが、データを共通鍵方式の暗号鍵で暗号化し、さらにここで使用した暗号鍵を第２のクライアント機器２５が公開する公開鍵を用いて第１のクライアント機器２３が暗号化し、暗号化したデータと共に暗号鍵を送信してもかまわない。なお、上記複製条件情報の署名が改竄されている（つまり、サーバ２１からの情報ではない）場合、その複製条件情報が適用されるデータに対する複製は不可とされる。
【０１２１】
また、サーバ２１と第１および第２のクライアント機器２３および２５との間で行われる通信の経路に関する秘匿性・耐改竄性については、第２の実施形態では特に手法を記述していないが、秘密鍵方式とセッション鍵とを組み合わせた暗号化方式による暗号化通信を行ってもかまわない。このような暗号化通信としては、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）等を用いることができる。
【０１２２】

このように、第２の実施形態に係るアクセス権制御システムによれば、データの提供先となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【０１２３】

なお、上述した第１および第２の実施形態に係るアクセス権制御システムでは、サーバと直接的に接続されたクライアント機器がサーバにアクセス権の判定を依頼し、その結果を相手のクライアント機器に送信することによって構成されているが、アクセス権の判定を依頼するクライアント機器とサーバとは、直接的に接続されていなくてもかまわない。上記サーバが、ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されていれば、サーバと直接的に通信可能な他のプロキシとしてのクライアント機器（第３のクライアント機器とする）を介して、アクセス権の判定を依頼するクライアント機器とサーバとが通信することによって、本発明は実現可能である。例えば、上述した第１の実施形態では、第１のクライアント機器１３がサーバ１１と直接的に通信できない場合、第１のクライアント機器１３が上記第３のクライアント機器を介してサーバ１１と通信することによって、同様のアクセス権制御システムを構成することが可能である。また、上述した第２の実施形態では、第２のクライアント機器２５がサーバ２１と直接的に通信できない場合、第２のクライアント機器２５が上記第３のクライアント機器を介してサーバ２１と通信することによって、同様のアクセス権制御システムを構成することが可能である。このように上記第３のクライアント機器を介してアクセス権制御システムを構成する場合、さらに第３のクライアント機器であることを証明するための第３のクライアント証明書を用いて、それぞれのクライアント機器およびサーバが互いに認証することによって、正しいクライアント機器からの通信であることを確認することができることは、言うまでもない。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るアクセス権制御システムの全体の構成について説明するための図である。

【図２】図１に示すサーバ１１の内部構成を示す機能ブロック図である。

【図３】図１に示す第１のクライアント機器１３の内部構成を示す機能ブロック図である。

【図４】図１に示す第２のクライアント機器１５の内部構成を示す機能ブロック図である。

【図５】図１に示すサーバ１１、第１および第２のクライアント機器１３および１５が処理する全体動作を示すフローチャートである。

【図６】図１に示すアクセス権管理データベース１２に格納されているアクセス権管理リストのデータ構造について説明する図である。

【図７】図５に示すステップＳ１１において、アクセス可否判定部１１１が行うアクセス権判定処理の詳細動作の一例を示すサブルーチンである。

【図８】図５に示すステップＳ１１において、アクセス可否判定部１１１が行うアクセス権判定処理の詳細動作の他の例を示すサブルーチンである。

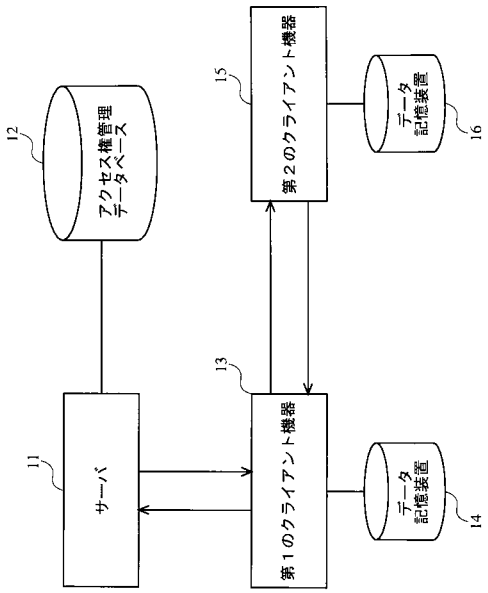
【図９】本発明の第２の実施形態に係るアクセス権制御システムの全体の構成について説明するための図である。

【図１０】図９に示すサーバ２１の内部構成を示す機能ブロック図である。

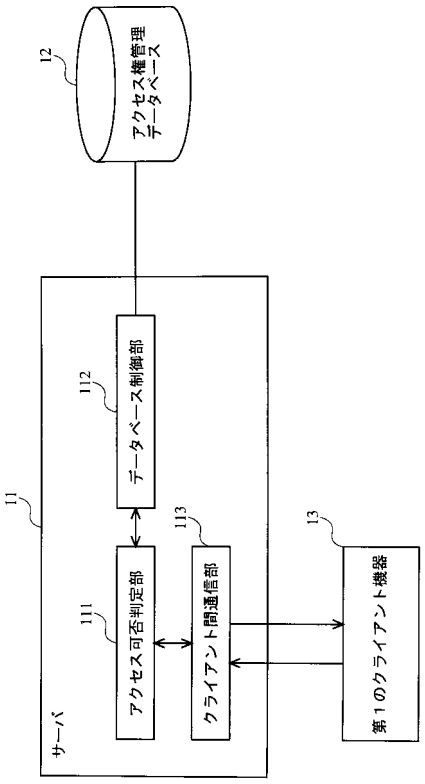
【図１１】図９に示す第１のクライアント機器２３の内部構成を示す機能ブロック図であ

る。
【図１２】図９に示す第２のクライアント機器２５の内部構成を示す機能ブロック図である。
【図１３】図９に示すサーバ２１、第１および第２のクライアント機器２３および２５が処理する全体動作を示すフローチャートである。
【符号の説明】
１１、２１…サーバ
１２、２２…アクセス権管理データベース
１３、２３…第１のクライアント機器
１４、１６、２４、２６…データ記憶装置
１５、２５…第２のクライアント機器
１１１、２１１…アクセス可否判定部
１１２、２１２…データベース制御部
１１３、１３４、１５１、２１３、２３１、２５４…クライアント間通信部
１３１、２５１…サーバ間通信部
１３２、２５２…アクセス可否問い合わせ部
１３３、１３２…データ送信部
１３５、１５４、２３３、２５５…記憶装置制御部
１５２、２５３…データ要求部
１５３、２５６…データ受信部
１５５、２５７…表示装置
１５６、２５８…入力装置

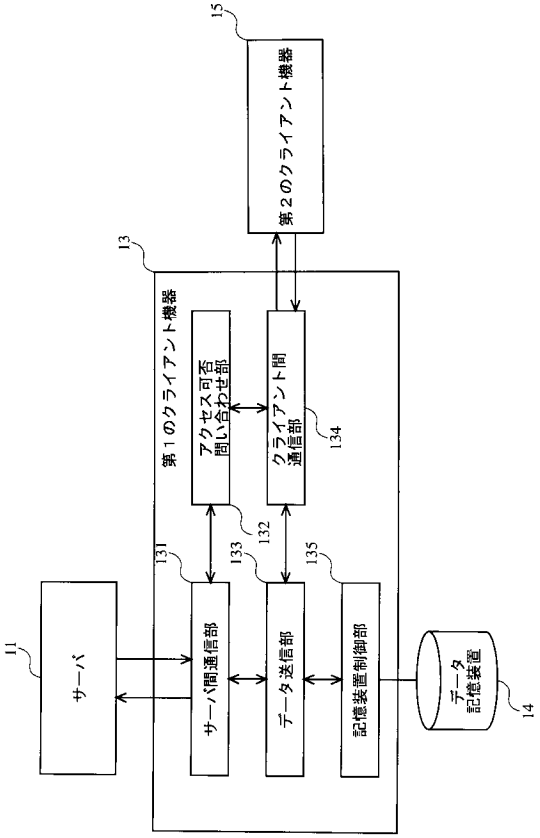
【図１】



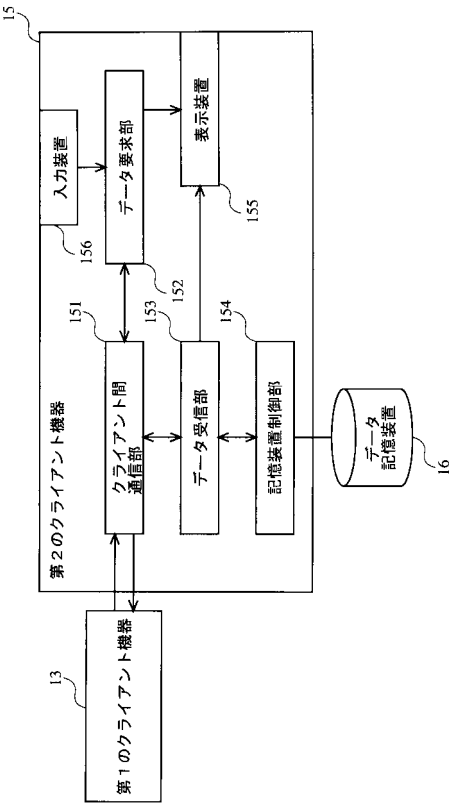
【図２】



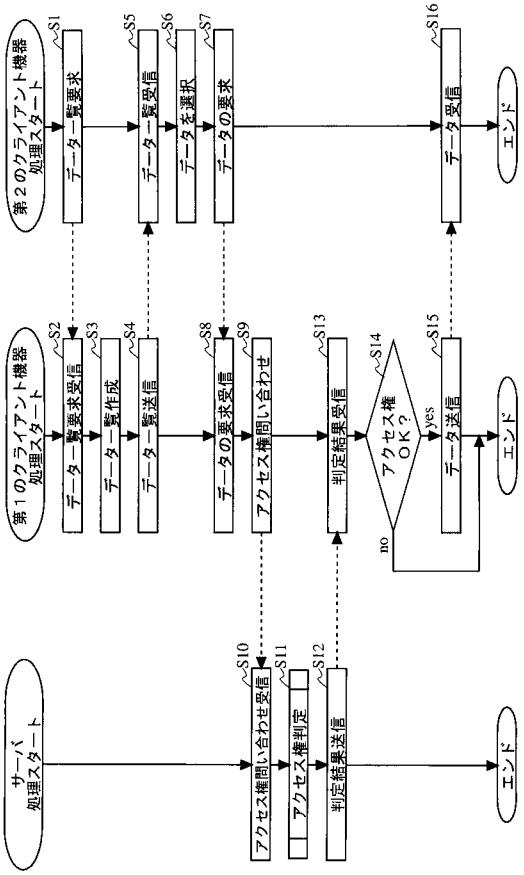
【図３】



【図４】



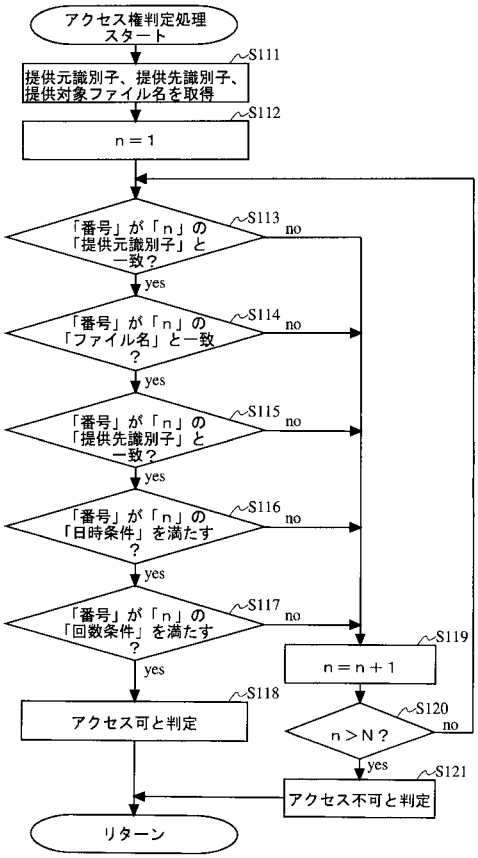
【図５】



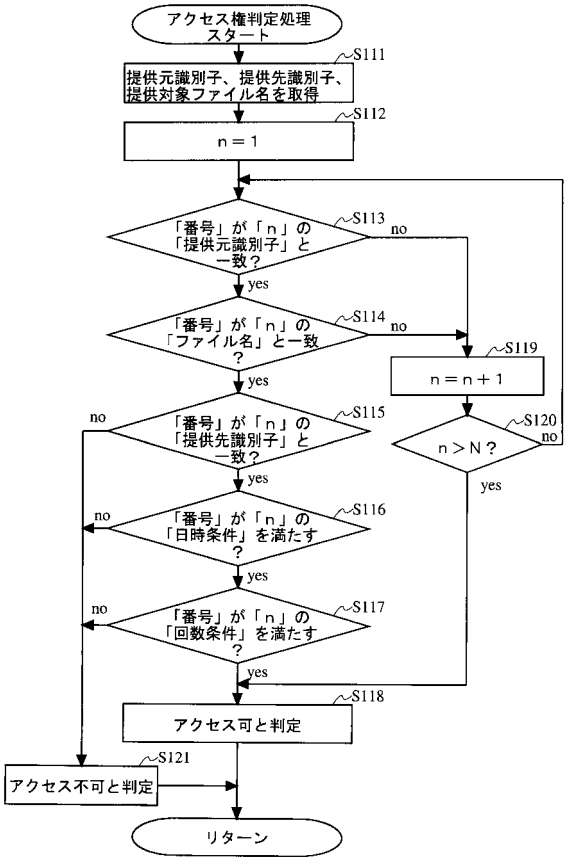
【図６】

番号	提供元識別子	ファイル名	提供先識別子	時間条件	回数条件	複製条件
1	1111	産声.wav	2222	任意	任意	不可
2	1111	誕生.jpg	任意	2001/03/31まで	任意	不可
3	1111	誕生会.mov	3333	任意	2回	任意
4	1111	子供.jpg	2222，3333	2001/07/31まで	任意	1世代のみ可
5	1111	お祝い金.txt	1111，4444	任意	任意	任意
6	2222	海外旅行.mov	1111	2001/06/01から1ヶ月	1回	任意
7	2222	連絡事項.text	1111，2222	任意	任意	不可
8	3333	結婚式.mov	任意	2001/07/31まで	任意	不可
9	4444	任意	1111	任意	任意	任意
10	：	：	：	：	：	：
11						
12						
13						

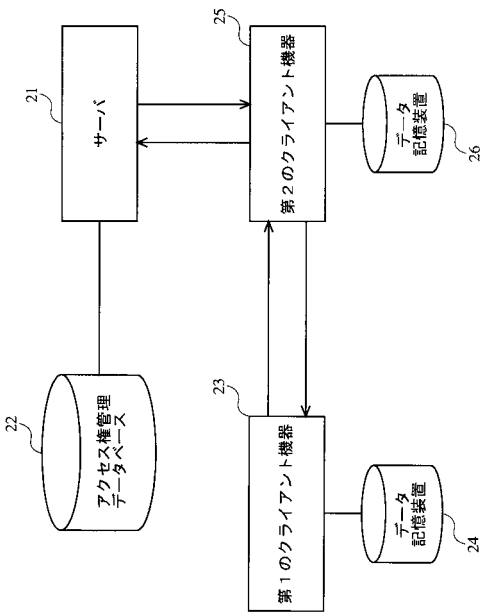
【図７】


アクセス権判定処理
スタート
S111
提供元識別子、提供先識別子、
提供対象ファイル名を取得
S112
n＝1
S113
「番号」が「n」の
「提供元識別子」と
一致？
no
yes
S114
「番号」が「n」の
「ファイル名」と一致
？
no
yes
S115
「番号」が「n」の
「提供先識別子」と
一致？
no
yes
S116
「番号」が「n」の
「日時条件」を満たす
？
no
yes
S117
「番号」が「n」の
「回数条件」を満たす
？
no
yes
S119
n＝n＋1
S120
n＞N？
no
yes
S118
アクセス可と判定
S121
アクセス不可と判定
リターン

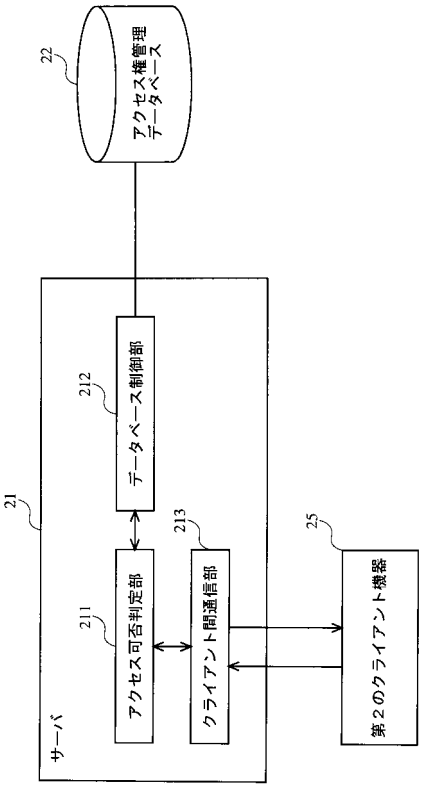
【図８】


アクセス権判定処理
スタート
S111
提供元識別子、提供先識別子、
提供対象ファイル名を取得
S112
n＝1
S113
「番号」が「n」の
「提供元識別子」と
一致？
no
yes
S114
「番号」が「n」の
「ファイル名」と一致
？
no
yes
S119
n＝n＋1
S120
n＞N？
no
yes
S115
「番号」が「n」の
「提供先識別子」と
一致？
no
yes
S116
「番号」が「n」の
「日時条件」を満たす
？
no
yes
S117
「番号」が「n」の
「回数条件」を満たす
？
no
yes
S118
アクセス可と判定
S121
アクセス不可と判定
リターン

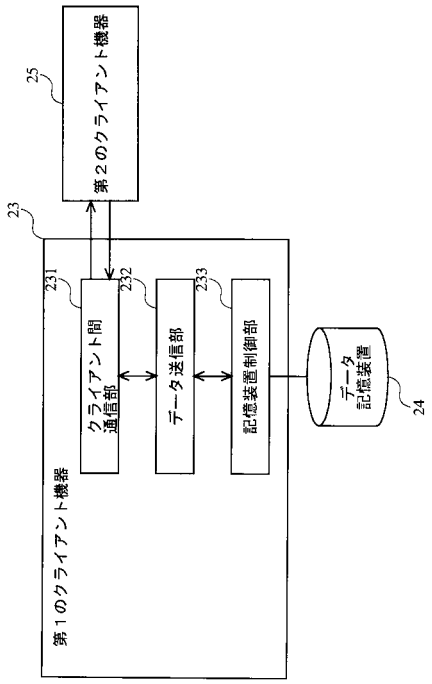
【図９】


21
サーバ
25
第２のクライアント機器
データ
記憶装置
26
22
アクセス権管理
データベース
23
第１のクライアント機器
データ
記憶装置
24

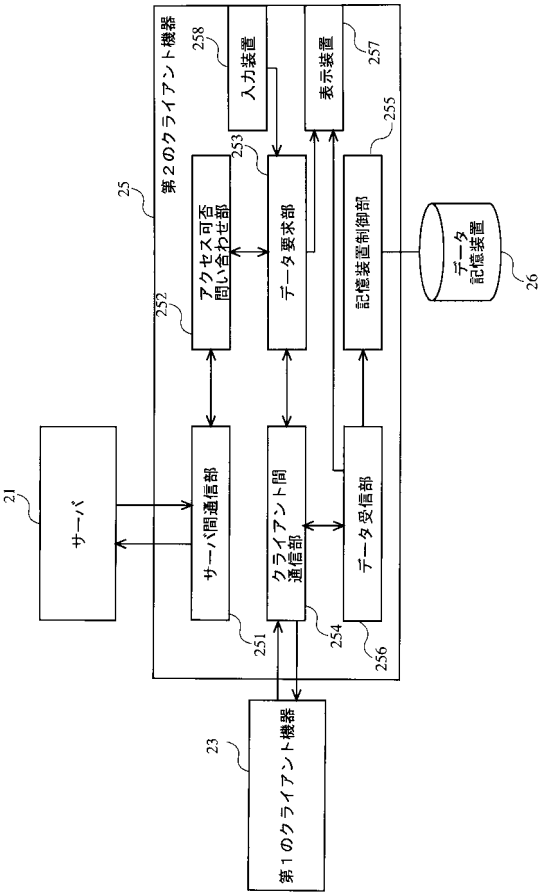
【図１０】


22
アクセス権管理
データベース
21
サーバ
212
データベース制御部
211
アクセス可否判定部
213
クライアント間通信部
25
第２のクライアント機器

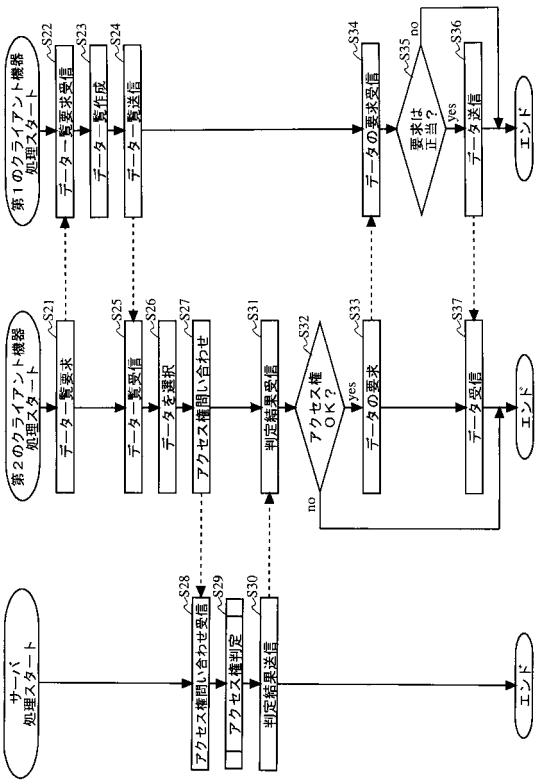
【図１１】


25
第２のクライアント機器
23
231
232
233
クライアント間通信部
データ送信部
記憶装置制御部
データ記憶装置
24
第１のクライアント機器

【図１２】


25
第２のクライアント機器
258
入力装置
257
表示装置
255
253
252
アクセス可否問い合わせ部
データ要求部
記憶装置制御部
データ記憶装置
26
21
サーバ
サーバ間通信部
クライアント間通信部
データ受信部
251
254
256
23
第１のクライアント機器

【図１３】


第１のクライアント機器 処理スタート
S22
データ一覧要求送信
S23
データ一覧作成
S24
データ一覧送信
S34
データの要求受信
S35
no
要求は正当？
yes
S36
データ送信
エンド
第２のクライアント機器 処理スタート
S21
データ一覧要求
S25
データ一覧受信
S26
データを選択
S27
アクセス権問い合わせ
S31
判定結果受信
S32
アクセス権 OK？
yes
S33
データの要求
S37
データ受信
エンド
no
サーバ 処理スタート
S28
アクセス権問い合わせ受信
S29
アクセス権判定
S30
判定結果送信
エンド

フロントページの続き

審査官　宮司　卓佳

(56)参考文献　特開平１１－０８８４３６（ＪＰ，Ａ）
特開２０００－２９３４３９（ＪＰ，Ａ）
特開２０００－２９８９４３（ＪＰ，Ａ）
特開２０００－０１０９３０（ＪＰ，Ａ）
特開２００１－１８６１２２（ＪＰ，Ａ）
特開２００２－３１２５２３（ＪＰ，Ａ）
特開２００１－２５７６６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
G06F 21/24