(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2009-237662
(P2009-237662A)
(43)公開日　平成21年10月15日(2009.10.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530D	5B017
G06F 12/00	(2006.01)	G06F	12/00	537D	5B082

審査請求 有　請求項の数 16　ＯＬ　（全 22 頁）

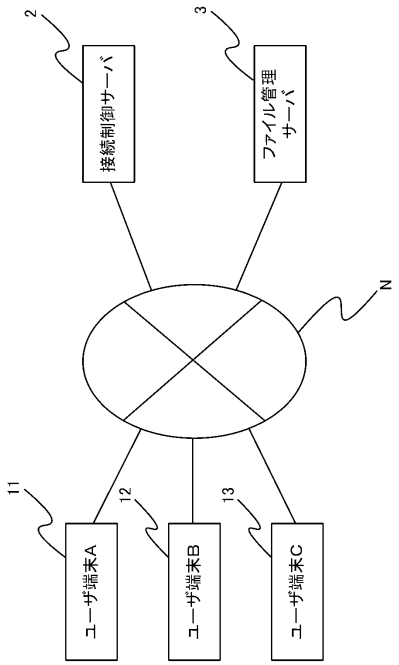
(21)出願番号　特願2008-79685(P2008-79685)
(22)出願日　平成20年3月26日(2008.3.26)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100124811
弁理士　馬場　資博
(72)発明者　平野　久美子
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　丸山　俊一
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA03　BA05　CA16
5B082 EA12

(54)【発明の名称】ファイル管理システム

(57)【要約】
【課題】ファイルへの不正なアクセスを制限し、セキュリティの向上を図る。
【解決手段】通信端末間の接続制御を行う接続制御装置と、通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備え、上記接続制御装置は、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知手段を備え、上記ファイル管理装置は、共有ファイルを共有する通信端末を特定する共有メンバ情報を記憶すると共に、共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証手段を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムであって、
前記接続制御装置は、前記通信端末間で確立されたセッションを特定するセッション情報を前記ファイル管理装置に通知するセッション情報通知手段を備え、
前記ファイル管理装置は、
前記共有ファイルを共有する前記通信端末を特定する共有メンバ情報を記憶すると共に、
前記共有メンバ情報に基づいて前記共有ファイルの共有メンバである全ての前記通信端末にて、前記接続制御装置から通知された前記セッション情報にて特定されるセッションが確立されているか否かを前記通信端末に対して問い合わせて判断し、全ての前記通信端末にてセッションが確立されていると判断した場合に当該通信端末による前記共有ファイルへのアクセスを許可する通信端末認証手段を備えた、
ことを特徴とするファイル管理システム。
【請求項２】
前記ファイル管理装置が有する前記通信端末認証手段は、前記セッションが確立している通信端末から当該通信端末を特定する情報及び当該セッションを特定する情報を含む通信端末認証情報を取得し、当該通信端末認証情報と、前記共有メンバ情報と、前記接続制御装置から通知された前記セッション情報と、に基づいて全ての前記通信端末にてセッションが確立されているか否かを判断する、
ことを特徴とする請求項１記載のファイル管理システム。
【請求項３】
前記ファイル管理装置が有する前記通信端末認証手段は、前記共有メンバ情報に前記接続制御装置から通知された前記セッション情報を付加して通信端末認証基準情報を生成し、この通信端末認証基準情報と、前記通信端末から取得した前記通信端末認証情報と、に基づいて、全ての前記通信端末にてセッションが確立されているか否かを判断する、
ことを特徴とする請求項２記載のファイル管理システム。
【請求項４】
前記ファイル管理装置は、前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段を備えた、
ことを特徴とする請求項１，２又は３記載のファイル管理システム。
【請求項５】
前記接続制御装置が有する前記セッション情報通知手段は、前記通信端末間で確立しているセッションが終了したときに、その旨を前記ファイル管理装置に通知し、
前記ファイル管理装置は、前記接続制御装置からセッション終了の通知を受けたときに、前記パスワード設定手段にて前記共有ファイルに設定した前記パスワードを無効にするパスワード解除手段を備えた、
ことを特徴とする請求項４記載のファイル管理システム。
【請求項６】
前記セッション情報は、前記セッションを確立するときにおける前記通信端末の接続順序を表す接続順序情報及び当該セッションの接続日時情報のうち、少なくとも１つの情報を含む、
ことを特徴とする請求項４又は５記載のファイル管理システム。
【請求項７】
通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装

置と、を備えたファイル管理システムであって、
前記接続制御装置は、前記通信端末間で確立されたセッションを特定するセッション情報を前記ファイル管理装置に通知するセッション情報通知手段を備え、
前記ファイル管理装置は、前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段を備えた、
ことを特徴とするファイル管理システム。
【請求項８】
通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置であって、
前記共有ファイルを共有する前記通信端末を特定する共有メンバ情報を記憶すると共に、
前記共有メンバ情報に基づいて前記共有ファイルの共有メンバである全ての前記通信端末にて、前記接続制御装置から通知されたセッションを特定するセッション情報にて特定されるセッションが確立されているか否かを前記通信端末に対して問い合わせて判断し、全ての前記通信端末にてセッションが確立されていると判断した場合に当該通信端末による前記共有ファイルへのアクセスを許可する通信端末認証手段を備えた、
ことを特徴とするファイル管理装置。
【請求項９】
前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段を備えた、
ことを特徴とする請求項８記載のファイル管理装置。
【請求項１０】
通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置であって、
前記接続制御装置から取得した前記通信端末間で確立されたセッションを特定するセッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段を備えた、
ことを特徴とするファイル管理装置。
【請求項１１】
通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置に、
前記共有ファイルを共有する前記通信端末を特定する共有メンバ情報に基づいて前記共有ファイルの共有メンバである全ての前記通信端末にて、前記接続制御装置から通知されたセッションを特定するセッション情報にて特定されるセッションが確立されているか否かを前記通信端末に対して問い合わせて判断し、全ての前記通信端末にてセッションが確立されていると判断した場合に当該通信端末による前記共有ファイルへのアクセスを許可する通信端末認証手段、を実現させるためのプログラム。
【請求項１２】
前記ファイル管理装置に、前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段、を実現させるための請求項１１記載のプログラム。
【請求項１３】
通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され前記通信端

末にて共有される共有ファイルを記憶して管理するファイル管理装置に、
前記接続制御装置から取得した前記通信端末間で確立されたセッションを特定するセッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定手段、を実現させるためのプログラム。
【請求項１４】
通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムによるファイル管理方法であって、
前記接続制御装置が、前記通信端末間で確立されたセッションを特定するセッション情報を前記ファイル管理装置に通知するセッション情報通知工程と、
前記ファイル管理装置が、前記共有ファイルを共有する前記通信端末を特定する共有メンバ情報に基づいて前記共有ファイルの共有メンバである全ての前記通信端末にて、前記接続制御装置から通知された前記セッション情報にて特定されるセッションが確立されているか否かを前記通信端末に対して問い合わせて判断し、全ての前記通信端末にてセッションが確立されていると判断した場合に当該通信端末による前記共有ファイルへのアクセスを許可する通信端末認証工程と、
を有することを特徴とするファイル管理方法。
【請求項１５】
前記ファイル管理装置が、前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定工程を有する、
ことを特徴とする請求項１４記載のファイル管理方法。
【請求項１６】
通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され前記通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムによるファイル管理方法であって、
前記接続制御装置が、前記通信端末間で確立されたセッションを特定するセッション情報を前記ファイル管理装置に通知するセッション情報通知工程と、
前記ファイル管理装置が、前記接続制御装置から取得した前記セッション情報に基づいてパスワードを生成し、当該パスワードを前記共有ファイルの操作を制限するパスワードとして設定し、当該パスワードを前記セッション情報にて特定されるセッションにて接続されている前記通信端末に通知するパスワード設定工程と、
を有することを特徴とするファイル管理方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ファイル管理システムにかかり、特に、ネットワークを介してセッションを確立している通信端末によってファイルを共有可能なよう管理するファイル管理システムに関する。
【背景技術】
【０００２】
近年、情報の電子化が進み、所定の情報が記録された電子データであるファイルをコンピュータで管理することが行われている。そして、ファイルを複数人で共有する場合には、データ内容の漏洩を抑制すべく、限られたメンバのみがアクセス可能なようパスワードやＩＤを事前に設定して、メンバに付与することが行われている。これにより、メンバは、パスワードやＩＤを用いることで、他のメンバの許可無くファイルにアクセス可能であ

り、ファイルの追記、変更、ファイル転送など、ファイル操作を行うことができる。
【０００３】
なお、ファイルへのアクセスを制限する技術として、特許文献１では、ファイルにアクセス可能なグループを設定し、当該グループに属するユーザのみがファイルにアクセス可能としている。また、関連する技術として、特許文献２では、１のグループに属する複数のユーザが接続している場合に、特定のサーバにアクセス可能とする技術が開示されている。
【０００４】
【特許文献１】特開２００１－３３１３７３号公報
【特許文献２】特開２００７－１９９９９５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述したように、ファイルへのアクセスにパスワードやＩＤを用いたとしても、当該パスワードが固定的なものである場合には、一度、そのパスワードやＩＤがメンバ以外の人に漏洩してしまうと、第三者によるファイルへのアクセスが可能となってしまう。すると、ファイルの内容が外部に漏洩してしまい、信頼性が低下する、という問題があった。
【０００６】
このため、本発明の目的は、上述した課題である、ファイルへの不正なアクセスを制限し、セキュリティの向上を図る、ことにある。
【課題を解決するための手段】
【０００７】
そこで、本発明の一形態であるファイル管理システムは、通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えている。そして、上記接続制御装置は、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知手段を備えている。さらに、上記ファイル管理装置は、共有ファイルを共有する通信端末を特定する共有メンバ情報を記憶すると共に、共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証手段を備えている。
【０００８】
また、本発明の他の形態であるファイル管理システムは、通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えている。そして、上記接続制御装置は、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知手段を備えている。さらに、上記ファイル管理装置は、接続制御装置から取得したセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末に通知するパスワード設定手段を備えている。
【０００９】
また、本発明の他の形態であるファイル管理装置は、通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置であって、共有ファイルを共有する前記通信端末を特定する共有メンバ情報を記憶すると共に、共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッションを特定するセッショ

ン情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証手段を備えた、という構成を採る。

【００１０】

また、本発明の他の形態であるファイル管理装置は、通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置であって、接続制御装置から取得した通信端末間で確立されたセッションを特定するセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末に通知するパスワード設定手段を備えた、という構成を採る。

【００１１】

また、本発明の他の形態であるプログラムは、通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置に、共有ファイルを共有する通信端末を特定する共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッションを特定するセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証手段、を実現させる、という構成を採る。

【００１２】

また、本発明の他の形態であるプログラムは、通信端末間の接続制御を行う接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置に、接続制御装置から取得した通信端末間で確立されたセッションを特定するセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末に通知するパスワード設定手段、を実現させる、という構成を採る。

【００１３】

さらに、本発明の他の形態であるファイル管理方法は、通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムによるファイル管理方法であって、上記接続制御装置が、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知工程と、上記ファイル管理装置が、共有ファイルを共有する通信端末を特定する共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証工程と、を有する、という構成を採る。

【００１４】

また、本発明の他の形態であるファイル管理方法は、通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムによるファイル管理方法であって、上記接続制御装置が、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知工程と、上記ファイル管理装置が、接続制御装置から取得したセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末

に通知するパスワード設定工程と、を有する、という構成を採る。
【発明の効果】
【００１５】
本発明は、以上のように構成されるため、共有ファイルを共有するよう予め設定された共有メンバ全員が、共通の通信状態を形成している間のみ、共有ファイルへのアクセスや操作が可能となる。つまり、通信状態が変更されると、共有ファイルへのアクセスや操作が不可能となる。その結果、第三者によるなりすましを有効に抑制でき、ファイルアクセスのセキュリティの向上を図ることができる、という優れた効果を有する。
【発明を実施するための最良の形態】
【００１６】
本発明は、高度のセキュリティが要求されるファイルアクセスシステムにおいて、限られたメンバのみにアクセスを許されるファイルを、当該メンバ全員が共通の通信状態を形成する間のみ、該共有ファイルのアクセスを許容する、ことに特徴を有する。
【００１７】
そして、本発明の一形態であるファイル管理システムは、
通信端末間の接続制御を行う接続制御装置と、この接続制御装置にネットワークを介して接続され通信端末にて共有される共有ファイルを記憶して管理するファイル管理装置と、を備えたファイル管理システムであって、
上記接続制御装置は、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知手段を備え、
上記ファイル管理装置は、
共有ファイルを共有する通信端末を特定する共有メンバ情報を記憶すると共に、
共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証手段を備えた、
という構成を採る。
【００１８】
また、上記ファイル管理システムでは、ファイル管理装置が有する通信端末認証手段は、セッションが確立している通信端末から当該通信端末を特定する情報及び当該セッションを特定する情報を含む通信端末認証情報を取得し、当該通信端末認証情報と、共有メンバ情報と、接続制御装置から通知されたセッション情報と、に基づいて全ての通信端末にてセッションが確立されているか否かを判断する、という構成を採る。
【００１９】
さらに、上記ファイル管理システムでは、ファイル管理装置が有する通信端末認証手段は、共有メンバ情報に接続制御装置から通知されたセッション情報を付加して通信端末認証基準情報を生成し、この通信端末認証基準情報と、通信端末から取得した通信端末認証情報と、に基づいて、全ての通信端末にてセッションが確立されているか否かを判断する、という構成を採る。
【００２０】
上記発明によると、ファイル管理装置は、まず、共有ファイルを共有する通信端末を特定する共有メンバ情報を記憶している。この共有メンバ情報は、例えば、事前にファイル管理装置に登録されていたり、あるいは、所定の通信端末から接続制御装置を介して登録される。そして、通信端末間でセッションが確立されると、接続制御装置からセッションを特定するセッション情報が通知され、これをファイル管理装置が受信する。すると、ファイル管理装置は、このセッション情報にて特定されるセッションにて、共有ファイルに設定された共有メンバの全員が接続されているか否かを判断する。例えば、共有メンバ情報にセッション情報を付加した情報を各メンバの認証基準情報とし、各通信端末から当該端末とセッションとを特定する情報が付加された通信端末認証情報を取得して、比較する

。そして、全ての通信端末について一致した場合には、共有ファイルへのアクセスを許容する。

【００２１】

従って、共有ファイルを共有するよう予め設定された共有メンバ全員が、共通の通信状態を有する場合にのみ、共有ファイルへのアクセスが可能となる。その結果、第三者によるなりすましを有効に抑制でき、ファイルアクセスのセキュリティの向上を図ることができる。

【００２２】

また、上記ファイル管理システムでは、上記ファイル管理装置は、接続制御装置から取得したセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末に通知するパスワード設定手段を備えた、という構成を採る。

【００２３】

また、上記ファイル管理システムでは、上記接続制御装置が有するセッション情報通知手段は、通信端末間で確立しているセッションが終了したときに、その旨をファイル管理装置に通知し、上記ファイル管理装置は、接続制御装置からセッション終了の通知を受けたときに、パスワード設定手段にて共有ファイルに設定したパスワードを無効にするパスワード解除手段を備えた、という構成を採る。

【００２４】

なお、上記セッション情報は、セッションを確立するときにおける通信端末の接続順序を表す接続順序情報及び当該セッションの接続日時情報のうち、少なくとも１つの情報を含む。

【００２５】

上記発明によると、ファイル管理装置は、接続制御装置にて確立されている通信端末間のセッションを特定するセッション情報に基づいてパスワードを生成し、このパスワードを共有ファイルの操作に必要なパスワードとして、共有ファイルに設定する。また、このパスワードを、セッションを確立している通信端末に通知する。そして、通信端末が、ファイル管理装置から通知を受けたパスワードを用いてファイルアクセスを実行すると、ファイル管理装置は、送信されたパスワードと共有ファイルに設定されているパスワードとが一致している場合に、当該共有ファイルの操作を許可する。

【００２６】

これにより、共通のセッションにて接続されている通信端末のみが、当該セッションの内容に対応して生成された動的なパスワードに基づいて共有ファイルにアクセス可能となるため、第三者の不正アクセスを有効に抑制することができる。特に、セッションが切断されるとパスワードが無効となるため、仮にパスワードが盗まれた場合であっても、セッションを切断することで共有ファイルへのアクセスを防止できる。また、パスワードをセッションの識別情報や接続日時情報などの情報に基づいて生成することで、よりセッションに対応したパスワードを設定でき、パスワードの解読や不正な生成を防止できる。その結果、ファイル共有のセキュリティの向上を図ることができる。

【００２７】

また、本発明の他の形態であるファイル管理方法は、上述したように、

上記接続制御装置が、通信端末間で確立されたセッションを特定するセッション情報をファイル管理装置に通知するセッション情報通知工程と、

上記ファイル管理装置が、共有ファイルを共有する前記通信端末を特定する共有メンバ情報に基づいて共有ファイルの共有メンバである全ての通信端末にて、接続制御装置から通知されたセッション情報にて特定されるセッションが確立されているか否かを通信端末に対して問い合わせて判断し、全ての通信端末にてセッションが確立されていると判断した場合に当該通信端末による共有ファイルへのアクセスを許可する通信端末認証工程と、

を有する、という構成を採る。

【００２８】
そして、さらに、上記ファイル管理方法は、上記ファイル管理装置が、接続制御装置から取得したセッション情報に基づいてパスワードを生成し、当該パスワードを共有ファイルの操作を制限するパスワードとして設定し、当該パスワードをセッション情報にて特定されるセッションにて接続されている通信端末に通知するパスワード設定工程を有する、という構成を採る。
【００２９】
以下、本発明の具体的な構成及び動作を説明する。なお、以下では、３つのユーザ端末（通信端末）にてファイルが共有される場合を例示するが、共有ファイルを共有するユーザ端末の数はこれに限定されない。
【００３０】
＜実施形態１＞
本発明の第１の実施形態を、図１乃至図１２を参照して説明する。図１は、ファイル管理システムの構成を示すブロック図である。図２は、接続制御サーバの構成を示す機能ブロック図である。図３は、ファイル管理サーバの構成を示す機能ブロック図である。図４は、共有ファイルの管理状況の一例を説明するための図である。図５乃至図６は、ファイル管理システムの動作の一例を示すシーケンス図である。図７は、共有ファイルの管理状況の一例を説明するための図である。図８乃至図９は、ファイル管理システムの動作の一例を示すシーケンス図である。図１０は、共有ファイルの管理状況の一例を説明するための図である。図１１乃至図１２は、ファイル管理システムの動作の一例を示すシーケンス図である。図１３は、ファイル管理システムの動作の一例を示すシーケンス図である。
【００３１】
［構成］
図１に示すように、本実施形態におけるファイル管理システムは、共有ファイルを共有しうるユーザ端末Ａ１１と、ユーザ端末Ｂ１２と、ユーザ端末Ｃ１３と、を備えている。そして、上記ユーザ端末Ａ１１，Ｂ１２，Ｃ１３間のネットワークＮを介した接続制御を行い、これらのグループ通信状態を管理する接続制御サーバ２を備えている。さらに、接続制御サーバ２にネットワークＮを介して接続され、上記ユーザ端末Ａ１１，Ｂ１２，Ｃ１３からの共有ファイルへのアクセスを管理するファイル管理サーバ３を備えている。以下、各構成について詳述する。
【００３２】
上記ユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３は、１台あるは複数台の他のユーザ端末とセッションを確立して通信可能な通信端末である。例えば、各ユーザ端末Ａ１１等は、接続制御サーバ２にて接続制御されることで、ＰＯＣ（Ｐｕｓｈ－ｔｏ－Ｔａｌｋ ｏｖｅｒ Ｃｅｌｌｕｌａｒ）やＶＯＩＰ（Ｖｏｉｃｅ ｏｖｅｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）やチャットなど、他の通信端末とセッションを確立して通話やデータ通信を行う機能を有する情報処理端末である。
【００３３】
そして、ここでは、ユーザ端末Ａ１１は、ファイルＺを保有しており、ユーザ端末Ｂ１２とユーザ端末Ｃ１３とにアクセスを許容して、共有することを希望していることとする。この場合に、ユーザ端末Ａ１１は、上記ユーザ端末Ｂ１２，Ｃ１３に予め付与されたユーザ識別子を含めたグループ共有指示を、接続制御サーバ２に対して送信する。すると、接続制御サーバ２から、ユーザ端末Ｂ１２とユーザ端末Ｃ１３とに対して、グループセッションを確立する要求が通知される。これに応じて、ユーザ端末Ｂ１２とユーザ端末Ｃとは、接続制御サーバ２にグループ共有応答を送信することで、グループセッションに参加することを通知する。これにより、ユーザ端末Ａ１１，Ｂ１２、Ｃ１３間で、接続制御サーバ２によりグループセッションが確立され、相互に通話や通信が可能となる。
【００３４】
また、ユーザ端末Ａ１１は、グループセッションが確立された他のユーザ端末Ｂ１２，Ｃ１３が、共有ファイルＺを共有したい正しいユーザであるか否かの本人確認（声や映像

や文字入力など）を実施する。そして、他のユーザ端末Ｂ１２，Ｃ１３が正しいと判断した場合には、ユーザ端末Ａ１１は、接続制御サーバ２に対して共有ファイルＺを添付したファイル共有指示を送信する。このとき、ユーザ端末Ａ１１は、ファイル共有指示に、共有ファイルＺを共有する各ユーザ端末Ａ１１、Ｂ１２、Ｃ１３にそれぞれ付与された識別情報であるＩＤを付加して送信する。なお、ユーザ端末Ａ１１は、共有ファイルＺがすでにファイル管理サーバ３に記憶されている場合には、当該共有ファイルＺを指定する情報と、共有するユーザ端末のＩＤを送信してもよい。

【００３５】

また、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３は、後述するようにファイル管理サーバ３からＩＤ入力要求を受けると、自端末にそれぞれ固有の識別情報である固有ＩＤに、グループセッションに固有の識別情報であるセッションＩＤを付加した動的ＩＤを生成して、ファイル管理サーバ３に送信する機能を有する。

【００３６】

さらに、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３は、後述するようにファイル管理サーバ３からパスワードの配布を受けると、当該パスワードを受信して記憶する。そして、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３は、受信したパスワードを用いて、ファイル管理サーバ３が記憶している共有ファイルＺにアクセスして、閲覧、更新などの操作を実行することができる。

【００３７】

また、ユーザ端末Ａ１１は、上述したように確立されたグループセッションの終了を希望する場合には、かかる指示を接続制御サーバ２に通知する機能を有する。これに応じて、接続制御サーバ２は、ユーザ端末Ｂ１２，Ｃ１３に対してグループ共有終了要求を行うが、当該ユーザ端末Ｂ１２、Ｃ１３は、グループ共有終了応答を行う機能を有する。これにより、セッションが終了され、同時に共有ファイルの共有も終了される。

【００３８】

次に、接続制御サーバ２の構成について、図２を参照して説明する。接続制御サーバ２（接続制御装置）は、一般的なサーバコンピュータであり、図２に示すように、装備された演算装置（図示せず）に所定のプログラムが組み込まれることによって構築された、セッション制御部２１と、セッション情報通知部２２と、を備えている。

【００３９】

そして、上記セッション制御部２１は、上述したようにユーザ端末Ａ１１からのグループ共有指示を受けると、他のユーザ端末Ｂ１２，Ｃ１３に対してグループ共有要求を行い、これに対してグループ共有応答を受けると、上述したようにユーザ端末Ａ１１，Ｂ１２，Ｃ１３間のグループセッションを確立して、これら各端末の接続制御を行う機能を有している。また、セッション制御部２１は、ユーザ端末Ａ１１からグループ共有終了の指示を受けると、他のユーザ端末Ｂ１２，Ｃ１３に終了を要求し、これに対する応答を受けると、セッションを終了する。

【００４０】

また、上記セッション情報通知部２２（セッション情報通知手段）は、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１２間でセッションが確立されると、当該確立されたセッションの内容を表すセッション情報、具体的には、セッションを特定する識別情報であるセッションＩＤ、セッションを確立するときにおけるユーザ端末Ａ１１，Ｂ１２，Ｃ１３の接続順序を表す接続順序情報、当該セッションの接続日時情報、を含むセッション情報を、ファイル管理サーバ３に送信する機能を有する。なお、セッションＩＤは、接続制御サーバ２で生成された情報である。また、セッション情報には、少なくともセッションＩＤが含まれていればよく、他の情報は必ずしも含まれていなくてもよい。

【００４１】

また、セッション情報通知部２２は、上述したようにユーザ端末Ａ１１から通知された共有ファイルＺ自体（あるいは、共有ファイルＺを指定する情報）と、共有するユーザ端末を特定するＩＤとを、ファイル管理サーバ３に通知する機能を有する。

【００４２】
さらに、セッション情報通知部２２は、上述したようにセッション制御部２１にてセッションが終了されると、その旨をファイル管理サーバ３に通知する。具体的には、終了されたセッションを確立していたユーザ端末Ａ１１，Ｂ１２，Ｃ１３間で共有されていた共有ファイルＺの共有停止指示を、ファイル管理サーバ２に対して行う。
【００４３】
次に、ファイル管理サーバ３の構成について、図３乃至図４を参照して説明する。ファイル管理サーバ３（ファイル管理装置）は、ファイルを記憶して管理する一般的なサーバコンピュータである。そして、ファイル管理サーバ３は、図３に示すように、装備された演算装置（図示せず）に所定のプログラムが組み込まれることによって構築された、ファイル共有情報取得部３１と、ユーザ認証部３２と、パスワード設定部３３と、ファイルアクセス管理部３４と、共有解除部３５と、を備えている。また、装備された記憶装置には、ファイル記憶部３６と、共有ユーザ管理情報記憶部３７と、が形成されている。
【００４４】
上記ファイル共有情報取得部３１は、上述したようにユーザ端末Ａから共有ファイルＺ及び共有メンバとなるユーザ端末Ａ１１，Ｂ１２，Ｃ１３のＩＤを接続制御サーバ２を介して受信した場合に、まず、上記共有ファイルＺをファイル記憶部３６に記憶する。このとき、共有ファイルＺを共有不可に設定しておく。また、共有ファイルＺと共に受信した各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３の固定ＩＤを、図４（ａ）に示すように、共有ファイルＺに関連付けて共有ユーザ管理情報記憶部３７内に記憶し、当該共有ファイルを共有するユーザ端末を特定する共有メンバ情報とする。なお、この共有メンバ情報は、以後、共有ファイルＺに関連付けられたままとなる。
【００４５】
さらに、ファイル共有情報取得部３１は、上述したようにユーザ端末Ａ１１，Ｂ１２，Ｃ１３間でセッションが確立されたときに送信された、当該セッションを特定するセッションＩＤを、上記共有メンバ情報である各ユーザ端末の固定ＩＤに付加して、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３を特定する動的ＩＤとして設定し、各ユーザ端末を認証するときの基準となる認証基準情報（通信端末認証基準情報）として記憶する。例えば、図４（ｂ）に示すように、セッションＩＤが「ＸＹＺ」である場合に、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３に対応する動的ＩＤは、「ａａａＸＹＺ」、「ｂｂｂＸＹＺ」、「ｃｃｃＸＹＺ」とそれぞれ設定される。
【００４６】
また、上記ユーザ認証部３２（通信端末認証手段）は、上述したように各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３に対応して設定した動的ＩＤに基づいて、セッションを確立しているユーザ端末が共有ファイルＺにアクセス可能か否かの認証を行う。具体的には、上述した接続制御サーバ２からのユーザ端末の通知に応じて、ネットワークＮを介して各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３に動的ＩＤの入力要求を行う。そして、各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３から送信された動的ＩＤ（通信端末認証情報）の入力を受け付けて、共有ユーザ管理情報記憶部３７に記憶している動的ＩＤと一致するか否かを調べる。これにより、セッションＩＤ「ＸＹＺ」のセッションに、共有ファイルを共有する全ての通信端末が接続されているか否かを調べることができる。そして、全ての動的ＩＤが一致すると、共有ファイルへのアクセスを許可すべくパスワード設定部３３に通知する。一方、１つでも一致しない場合や受信しない場合には、共有ファイルへのアクセスは不許可とする。
【００４７】
また、上記パスワード設定部３３（パスワード設定手段）は、上記ユーザ認証部３２にて全てのユーザ端末の認証が成功した旨の通知を受けると、共有ファイルの操作を制限するためのパスワードを生成して、当該パスワードを共有ファイルに設定し、また、当該パスワードをセッションを確立している各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３に通知する。具体的には、上述したように接続制御サーバ２から通知されたセッションの接続日時情報（例えば、接続日時が１０月２２日１２時３１分の場合に、「１０２２１２３１」）、各

ユーザ端末の固定ＩＤ（ａａａ，ｂｂｂ，ｃｃｃ）を用いて当該ユーザ端末のセッションの接続順序を表す接続順序情報（例えば、「ａａａｂｂｂｃｃｃ」）、セッションＩＤ（例えば、「ＸＹＺ」）、を組み合わせた動的なパスワード（例えば、「１０２２１２３１ａａａｂｂｂｃｃｃＸＹＺ」）を生成する。これにより、セッション及び当該セッションに接続されているユーザ端末に固有のパスワードを生成する。そして、図４（ｃ）に示すように、ファイル記憶部３６に記憶されている共有ファイルに、上記パスワードを設定する。また、セッションを確立している各ユーザ端末Ａ１１，Ｂ１２，Ｃ１３に、生成したパスワードを通知して、共有ファイルＺの共有許可を通知する。なお、上述した動的パスワードの生成方法は一例であって、これに限定されない。つまり、上記では、セッションの接続日時情報と、接続順序情報と、セッションＩＤと、を組み合わせて動的パスワードを生成しているが、これらのうち少なくとも１つの情報を含めることによって、セッションに固有なパスワードを生成すればよい。

【００４８】

また、上記ファイルアクセス管理部３４は、ファイル記憶部３６に記憶されている共有ファイルへのユーザ端末からのアクセスを管理する。具体的には、共有ファイルにパスワードが設定されている場合には、同一のパスワードを通知してアクセスしてきたユーザ端末に対してのみ、共有ファイルの操作（読み出し、追記など）を許可し、一方、パスワードを有しないユーザ端末からのアクセスは拒否する。

【００４９】

また、上記共有解除部（パスワード解除手段）は、接続制御サーバ２からセッション終了の通知を受けると、当該セッションを確立しているユーザ端末にて共有されている共有ファイルＺに設定されているパスワードを解除すると共に、共有ファイルＺを共有不可とする。つまり、ユーザ端末に配布したパスワードを無効とし、いかなる端末であっても共有ファイルＺへのアクセスを不可とする。

【００５０】

［動作］

次に、上記構成のファイル管理システム動作を説明する。はじめに、図５乃至図６のシーケンス図を参照して、共有ファイルをはじめて設定し、当該共有ファイルを共有するときの動作を説明する。

【００５１】

まず、ユーザ端末Ａ１１が保有するファイルＺをユーザ端末Ｂ１２とユーザ端末Ｃ１３とで共通にアクセスを行いたい場合、ユーザ端末Ａ１１は、ユーザ端末Ｂ１２，Ｃ１３に予め付与されたユーザ識別子を付与したグループ共有指示を、接続制御サーバ２に送信する。つまり、ユーザ端末Ａ１１は、接続制御サーバ２に対して、自身であるユーザ端末Ａ１１と、ユーザ端末Ｂ１２と、ユーザ端末Ｃ１３とのグループセッションを確立したいことを通知する（ステップＳ１）。

【００５２】

そして、ユーザ端末Ａ１１からグループ共有指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、それぞれグループセッションを構成するすべてのユーザ端末Ａ、Ｂ、Ｃの識別子を付与したグループ共有要求を送信する（ステップＳ２，Ｓ４）。すると、グループ共有要求を受信したユーザ端末Ｂ１２、Ｃ１３は、グループ共有応答を接続制御サーバ２に送信し（ステップＳ３，Ｓ５）、グループセッションに参加することを通知する。これにより、グループ共有応答を受信した接続制御サーバ２は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３との間で、グループセッションの確立を行う（ステップＳ６、点線参照）。本セッションは、ＰＯＣやＶＯＩＰやチャットなどのコミュニケーション手段のいずれでも可能とする。

【００５３】

続いて、グループセッションが確立したユーザ端末Ａ１１、Ｂ１２、Ｃ１３の間で、ユーザ端末Ａ１１が、ファイルＺを共通にアクセスしたいユーザが正しいか否かを、このグループセッションを通して本人確認（声や映像や文字入力など）を実施する（ステップＳ

６）。そして、コミュニケーションセッションが確立したら、接続制御サーバ２は、このセッションにおけるユーザ端末の接続順序「Ａ→Ｂ→Ｃ」、セッションを特定する識別情報である動的なセッションＩＤ「ＸＹＺ」、接続日時を表す情報を生成し、ファイル管理サーバ３に送信する（ステップＳ６、セッション情報通知工程）。これらセッションに関する情報を受信したファイル管理サーバ３は、コミュニケーションセッション管理として、セッションＩＤ：ＸＹＺ、接続時間、順序の通知／管理を行う。

【００５４】

続いて、共有ファイルＺを共有したいメンバが、同一のセッションに接続されていて正しいと判断したユーザ端末Ａ１１は、接続制御サーバ２に対して共有ファイルＺを添付したファイル共有指示を送信する（ステップＳ７）。そして、ファイル共有指示を受信した接続制御サーバ２は、ユーザ端末Ａ１１から送付された共有ファイルと、すでに管理されたグループセッションを構成するユーザ端末Ａ１１、Ｂ１２、Ｃ１３に付与されたＩＤを付加したファイル共有指示を、ファイル管理サーバ３に送信する（ステップＳ８）。

【００５５】

続いて、上記ファイル共有指示を受信したファイル管理サーバ３は、共有ファイルＺのアクセス管理を行うために、グループセッションを構成するユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３のみのアクセスを許可するための動的ＩＤを作成すると共に（ステップＳ９）、共有ファイルＺに対するアクセス許容状態を共有不可とする。このとき、図４（ｂ）に示すように、共有ファイルＺにアクセス可能なユーザ端末を特定する動的ＩＤとして、各ユーザ端末の固有ＩＤにセッションＩＤを付加したデータ（通信端末認証基準情報）を生成して、共有ファイルＺに関連付けて記憶しておく。

【００５６】

続いて、ファイル管理サーバ３は、ユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、ＩＤ入力指示を送信する（ステップＳ１０，Ｓ１２，Ｓ１４）。すると、ＩＤ入力指示をそれぞれ受信したユーザ端末Ａ１１、Ｂ１２、Ｃ１３は、各自の固定ＩＤと動的セッションＩＤ：ＸＹＺで生成された動的ＩＤ（通信端末認証情報）を付与したＩＤ入力応答を、ファイル管理サーバ３に送信する（ステップＳ１１，Ｓ１３，Ｓ１５）。これらＩＤ入力応答を受信したファイル管理サーバ３は、ユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３からそれぞれ入力された動的ＩＤと、上記共有ファイルＺに関連付けて設定した動的ＩＤとが、全て一致するか否か認証を行う（通信端末認証工程）。

【００５７】

全ての動的ＩＤが一致した場合は、接続時間、接続順序、ユーザ端末固有のＩＤ、セッションＩＤを用いて、動的パスワードを作成する（ステップＳ１６）。動的パスワードは、例えば、接続時間が、１０月２２日１２時３１分、接続順序が、Ａ→Ｂ→Ｃ順、セッションＩＤがＸＹＺの場合には、「１０２２１２３１ａａａｂｂｂｃｃｃＸＹＺ」とする。このように、生成されたパスワードは、セッションに関連した情報を用いているため、当該セッション中のみ有効となり、後述するように、セッション終了後はこのパスワードは無効となる。

【００５８】

続いて、ファイル管理サーバ３は、上記生成したパスワードを、図４（ｃ）に示すように、共有ファイルＺの操作を制限するパスワードとして当該共有ファイルＺに設定し、共有ファイルＺのアクセス許容状態を共有中とする（ステップＳ１７）。また、ファイル管理サーバ３は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３に対して、上記生成したパスワードと共に、共有ファイルＺの共有許可通知を送信し（ステップＳ１８，Ｓ１９，Ｓ２０）、共有ファイルＺへのアクセス及び操作が可能であることを通知する（パスワード設定工程）。

【００５９】

その後、ファイル管理サーバ３は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３から、上記共有ファイルＺへのアクセス要求時に、上記動的パスワード「１０２２１２３１ａａａｂｂｂ

ｃｃｃＸＹＺ」を受信すると、各ユーザ端末に共有ファイルＺの操作を許可する（ステップＳ２１）。

【００６０】

その後、グループセッションの終了をユーザ端末Ａ１１が希望する場合には、当該ユーザ端末Ａ１１は、接続制御サーバ２に対してグループ共有終了指示を送信する（ステップＳ２２）。このグループ共有終了指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、Ｃ１３に対してグループ共有終了要求を送信する（ステップＳ２３，Ｓ２５）。そして、グループ共有終了要求を受信したユーザ端末Ｂ１２、Ｃ１３は、グループセッションの終了を許諾し、接続制御サーバ２に対してグループ共有終了応答を送信する（ステップＳ２４，Ｓ２６）。このようにして、グループ共有終了応答をすべて受信した接続制御サーバ２は、グループセッション中の状態をクリア、つまり、セッションを終了する（ステップＳ２７）。

【００６１】

また、接続制御サーバ２は、一旦、共有ファイルＺのアクセスを未許可にするために、ファイル共有停止指示をファイル管理サーバ３に送信する（ステップＳ２８）。ファイル共有停止指示を受信したファイル管理サーバ３は、共有ファイルＺのすべてのユーザからのアクセスを未許可にし、また、共有ファイルＺに設定されているパスワードを無効にする（ステップＳ２９）。

【００６２】

次に、上述したように、すでに一度ファイル共有を実施し、その後グループセッションを終了後に（ステップＳ１００）、再度、共有ファイルＺへのアクセスを実施する場合の動作を、図７乃至図９を参照して説明する。

【００６３】

まず、ユーザ端末Ａ１１が、再度共有ファイルＺをユーザ端末Ｂ１２とユーザ端末Ｃ１３とで共通にアクセスを行いたい場合には、上述同様に、ユーザ端末Ａ１１は、ユーザ端末Ｂ１２，Ｃ１３に予め付与されたユーザ識別子を付与したグループ共有指示を、接続制御サーバ２に送信する。つまり、ユーザ端末Ａ１１は、接続制御サーバ２に対して、自身であるユーザ端末Ａ１１と、ユーザ端末Ｂ１２と、ユーザ端末Ｃ１３とのグループセッションを確立したいことを通知する（ステップＳ１０１）。

【００６４】

そして、ユーザ端末Ａ１１からグループ共有指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、それぞれグループセッションを構成するすべてのユーザ端末Ａ、Ｂ、Ｃの識別子を付与したグループ共有要求を送信する（ステップＳ１０２，Ｓ１０４）。すると、グループ共有要求を受信したユーザ端末Ｂ１２、Ｃ１３は、グループ共有応答を接続制御サーバ２に送信し（ステップＳ１０３，Ｓ１０５）、グループセッションに参加することを通知する。これにより、グループ共有応答を受信した接続制御サーバ２は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３との間で、グループセッションの確立を行う（ステップＳ１０６、点線参照）。

【００６５】

続いて、グループセッションが確立したユーザ端末Ａ１１、Ｂ１２、Ｃ１３の間で、ユーザ端末Ａ１１がファイルＺを共通にアクセスしたいユーザが正しいか否かを、このグループセッションを通して本人確認（声や映像や文字入力など）を実施する（ステップＳ１０６）。そして、コミュニケーションセッションが確立したら、接続制御サーバ２は、このセッションにおけるユーザ端末の接続順序「Ａ→Ｂ→Ｃ」、セッションを特定する識別情報である動的なセッションＩＤ「ＬＭＮ」、接続日時を表す情報を生成し、ファイル管理サーバ３に送信する（ステップＳ１０６、セッション情報通知工程）。このとき、セッションＩＤや接続日時を表す情報は、上述した図５及び図６の例とは異なる。

【００６６】

続いて、共有ファイルＺを共有したいメンバが、同一のセッションに接続されていて正しいと判断したユーザ端末Ａ１１は、接続制御サーバ２に対してすでにファイル管理サー

バ３に登録されている共有ファイルＺを指定したファイル共有指示を送信する（ステップＳ１０７）。そして、ファイル共有指示を受信した接続制御サーバ２は、ユーザ端末Ａ１１から送付された共有ファイルの指定と、すでに管理されたグループセッションを構成するユーザ端末Ａ１１、Ｂ１２、Ｃ１３に付与されたＩＤを付加したファイル共有指示を、ファイル管理サーバ３に送信する（ステップＳ１０８）。

【００６７】

続いて、上記ファイル共有指示を受信したファイル管理サーバ３は、共有ファイルＺのアクセス管理を行うために、グループセッションを構成するユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３のみのアクセスを許可するための動的ＩＤを作成すると共に（ステップＳ１０９）、共有ファイルＺに対するアクセス許容状態を共有不可とする。このとき、図７（ａ）に示すように、共有ファイルＺを共有することが可能なユーザ端末の固定ＩＤが当該共有ファイルＺに関連付けられて既に記憶されているが、これに対して上記とは異なるセッションＩＤ「ＬＭＮ」を付加した動的ＩＤを生成し、図７（ｂ）に示すように、共有ファイルＺに関連付けて記憶しておく。このように、本例における動的ＩＤは、上述した前回のセッション時のときとは異なる。

【００６８】

続いて、ファイル管理サーバ３は、ユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、ＩＤ入力指示を送信する（ステップＳ１１０，Ｓ１１２，Ｓ１１４）。すると、ＩＤ入力指示をそれぞれ受信したユーザ端末Ａ１１、Ｂ１２、Ｃ１３は、各自の固定ＩＤと動的セッションＩＤ：ＬＭＮで生成された動的ＩＤを付与したＩＤ入力応答を、ファイル管理サーバ３に送信する（ステップＳ１１１，Ｓ１１３，Ｓ１１５）。これらＩＤ入力応答を受信したファイル管理サーバ３は、ユーザ端末Ａ１１、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３からそれぞれ入力された動的ＩＤと、上記共有ファイルＺに関連付けて設定した動的ＩＤとが、全て一致するか否か認証を行う（通信端末認証工程）。

【００６９】

全ての動的ＩＤが一致した場合は、接続時間、接続順序、ユーザ端末固有のＩＤ、セッションＩＤを用いて、動的パスワードを作成する（ステップＳ１１６）。今回は、接続時間が、１０月２２日１４時２４分、接続順序が、Ａ→Ｂ→Ｃ順、セッションＩＤがＬＭＮであり、前回のセッション確立とは接続時間とセッションＩＤとが異なるため、「１０２２１４２４ａａａｂｂｂｃｃｃＬＭＮ」と、異なるパスワードが生成される。

【００７０】

続いて、ファイル管理サーバ３は、上記生成したパスワードを、図４（ｃ）に示すように、共有ファイルＺの操作を制限するパスワードとして当該共有ファイルＺに設定し、共有ファイルＺのアクセス許容状態を共有中とする（ステップＳ１１７）。また、ファイル管理サーバ３は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３に対して、上記生成したパスワードと共に、共有ファイルＺの共有許可通知を送信し（ステップＳ１１８，Ｓ１１９，Ｓ１２０）、共有ファイルＺへのアクセス及び操作が可能であることを通知する（パスワード設定工程）。

【００７１】

その後、ファイル管理サーバ３は、ユーザ端末Ａ１１、Ｂ１２、Ｃ１３から、上記共有ファイルＺへのアクセス要求時に、上記動的パスワード「１０２２１４２４ａａａｂｂｂｃｃｃＬＭＮを受信すると、各ユーザ端末に共有ファイルＺの操作を許可する（ステップＳ１２１）。

【００７２】

その後、グループセッションの終了をユーザ端末Ａ１１が希望する場合には、当該ユーザ端末Ａ１１は、接続制御サーバ２に対してグループ共有終了指示を送信する（ステップＳ１２２）。このグループ共有終了指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、Ｃ１３に対してグループ共有終了要求を送信する（ステップＳ１２３，Ｓ１２５）。そして、グループ共有終了要求を受信したユーザ端末Ｂ１２、Ｃ１３は、グループセッションの終了を許諾し、接続制御サーバ２に対してグループ共有終了応答を送信する（ステ

ップＳ１２４，Ｓ１２６）。このようにして、グループ共有終了応答をすべて受信した接続制御サーバ２は、グループセッション中の状態をクリア、つまり、セッションを終了する（ステップＳ１２７）。また、接続制御サーバ２は、一旦、共有ファイルＺのアクセスを未許可にするために、ファイル共有停止指示をファイル管理サーバ３に送信する（ステップＳ１２８）。ファイル共有停止指示を受信したファイル管理サーバ３は、共有ファイルＺのすべてのユーザからのアクセスを未許可にし、また、共有ファイルＺに設定されているパスワードを無効にする（ステップＳ１２９）。

【００７３】

次に、上述したように、すでに一度ファイル共有を実施し、その後グループセッションを終了後に（ステップＳ２００）、ユーザ端末Ｃ１３の許可なしに、再度、共有ファイルＺへのアクセスを実施する場合の動作を、図１０乃至図１２を参照して説明する。

【００７４】

まず、ユーザ端末Ａ１１が、再度共有ファイルＺをユーザ端末Ｂ１２とユーザ端末Ｃ１３とで共通にアクセスを行いたい場合には、上述同様に、ユーザ端末Ａ１１は、ユーザ端末Ｂ１２，Ｃ１３に予め付与されたユーザ識別子を付与したグループ共有指示を、接続制御サーバ２に送信する。つまり、ユーザ端末Ａ１１は、接続制御サーバ２に対して、自身であるユーザ端末Ａ１１と、ユーザ端末Ｂ１２と、ユーザ端末Ｃ１３とのグループセッションを確立したいことを通知する（ステップＳ２０１）。

【００７５】

そして、ユーザ端末Ａ１１からグループ共有指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、それぞれグループセッションを構成するすべてのユーザ端末Ａ、Ｂ、Ｃの識別子を付与したグループ共有要求を送信する（ステップＳ２０２，Ｓ２０４）。このとき、グループ共有要求を受信したユーザ端末Ｂ１２は、グループ共有応答を接続制御サーバ２に送信し（ステップＳ２０３）、グループセッションに参加することを通知する。一方、グループ共有要求を受信したユーザ端末Ｃ１３は、グループセッションの形成を拒否することから、グループ共有応答を送信しない（ステップＳ２０５）。すると、接続制御サーバ２は、ユーザ端末Ａ１１、Ｂ１２、との間のみでグループセッションの確立を行う（ステップＳ２０６、点線参照）。

【００７６】

続いて、グループセッションが確立したユーザ端末Ａ１１、Ｂ１２の間で、ユーザ端末Ａ１１がファイルＺを共通にアクセスしたいユーザが正しいか否かを、このグループセッションを通して本人確認（声や映像や文字入力など）を実施する（ステップＳ２０６）。そして、コミュニケーションセッションが確立したら、接続制御サーバ２は、このセッションにおけるユーザ端末の接続順序「Ａ→Ｂ」、セッションを特定する識別情報である動的なセッションＩＤ「ＯＰＱ」、接続日時を表す情報を生成し、ファイル管理サーバ３に送信する（ステップＳ２０６、セッション情報通知工程）。このとき、セッションＩＤや接続日時を表す情報は、上述した例とは異なる。

【００７７】

続いて、共有ファイルＺを共有したいメンバが、同一のセッションに接続されていて正しいと判断したユーザ端末Ａ１１は、接続制御サーバ２に対してすでにファイル管理サーバ３に登録されている共有ファイルＺを指定したファイル共有指示を送信する（ステップＳ２０７）。そして、ファイル共有指示を受信した接続制御サーバ２は、ユーザ端末Ａ１１から送付された共有ファイルの指定と、すでに管理されたグループセッションを構成するユーザ端末Ａ１１、Ｂ１２に付与されたＩＤを付加したファイル共有指示を、ファイル管理サーバ３に送信する（ステップＳ２０８）。

【００７８】

続いて、上記ファイル共有指示を受信したファイル管理サーバ３は、共有ファイルＺのアクセス管理を行うために、グループセッションを構成するユーザ端末Ａ１１、ユーザ端末Ｂ１２のみのアクセスを許可するための動的ＩＤを作成すると共に（ステップＳ２０９）、共有ファイルＺに対するアクセス許容状態を共有不可とする。このとき、図１０（ａ

）に示すように、共有ファイルＺを共有することが可能なユーザ端末の固定ＩＤが当該共有ファイルＺに関連付けられて既に記憶されているが、これに対して上記とは異なるセッションＩＤ「ＯＰＱ」を付加した動的ＩＤを生成し、図１０（ｂ）に示すように、共有ファイルＺに関連付けて記憶しておく。但し、この場合に、ユーザ端末Ｃ１３については、上述したようにグループセッションに接続されていないため、動的ＩＤは生成されず、記憶されない。

【００７９】

続いて、ファイル管理サーバ３は、グループセッションを確立しているユーザ端末Ａ１１、ユーザ端末Ｂ１２に対して、ＩＤ入力指示を送信する（ステップＳ２１０，Ｓ２１２）。すると、ＩＤ入力指示をそれぞれ受信したユーザ端末Ａ１１、Ｂ１２は、各自の固定ＩＤと動的セッションＩＤ：ＯＰＱで生成された動的ＩＤを付与したＩＤ入力応答を、ファイル管理サーバ３に送信する（ステップＳ２１１，Ｓ２１３）。これらＩＤ入力応答を受信したファイル管理サーバ３は、ユーザ端末Ａ１１、ユーザ端末Ｂ１２からそれぞれ入力された動的ＩＤと、上記共有ファイルＺに関連付けて設定した動的ＩＤとが、全て一致するか否か認証を行う（通信端末認証工程）。すると、この例の場合には、ユーザ端末Ｃ１３のＩＤ入力応答がないことから、設定された動的ＩＤと不一致と判断し、アクセス許容状態未許可のままとする。そして、ユーザ端末Ａ１２、Ｂ１２に対して、ファイル共有未許可通知を送付し（ステップＳ２１４，Ｓ２１５）、共有ファイルＺへのアクセスを許可しない。

【００８０】

その後は、ユーザ端末Ａ１１は、接続制御サーバ２に対してグループ共有終了指示を送信する（ステップＳ２１６）。このグループ共有終了指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２に対してグループ共有終了要求を送信する（ステップＳ２１７）。そして、グループ共有終了要求を受信したユーザ端末Ｂ１２は、グループセッションの終了を許諾し、接続制御サーバ２に対してグループ共有終了応答を送信する（ステップＳ２１８）。このようにして、グループ共有終了応答を受信した接続制御サーバ２は、グループセッション中の状態をクリア、つまり、セッションを終了する（ステップＳ２１９）。

【００８１】

次に、上述したように、すでに一度ファイル共有を実施し、その後グループセッションを終了後に（ステップＳ３００）、再度、共有ファイルＺへのアクセスを実施する場合に、ユーザ端末Ｃに成りすましたユーザ端末Ｄ１４がグループセッションに参加した場合の動作を、図１３を参照して説明する。

【００８２】

まず、ユーザ端末Ａ１１が、再度共有ファイルＺをユーザ端末Ｂ１２とユーザ端末Ｃ１３とで共通にアクセスを行いたい場合には、上述同様に、ユーザ端末Ａ１１は、ユーザ端末Ｂ１２，Ｃ１３に予め付与されたユーザ識別子を付与したグループ共有指示を、接続制御サーバ２に送信する。つまり、ユーザ端末Ａ１１は、接続制御サーバ２に対して、自身であるユーザ端末Ａ１１と、ユーザ端末Ｂ１２と、ユーザ端末Ｃ１３とのグループセッションを確立したいことを通知する（ステップＳ３０１）。

【００８３】

そして、ユーザ端末Ａ１１からグループ共有指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、ユーザ端末Ｃ１３に対して、それぞれグループセッションを構成するすべてのユーザ端末Ａ、Ｂ、Ｃの識別子を付与したグループ共有要求を送信する（ステップＳ３０２，Ｓ３０４）。ところが、本例では、ユーザ端末Ｃ１３に送信したはずのグループ共有要求は、当該ユーザ端末Ｃ１３に成りすましたユーザ端末Ｄ１４に送信されることとなる（ステップＳ３０４）。

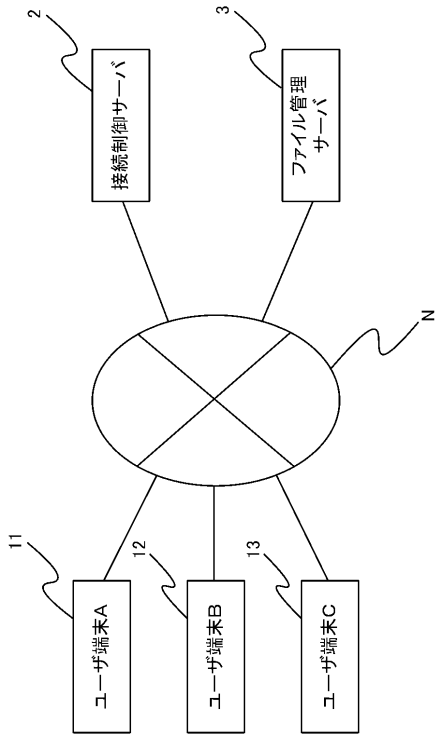
【００８４】

そして、グループ共有要求を受信したユーザ端末Ｂ１２，Ｄ１４は、グループ共有応答を接続制御サーバ２に送信し（ステップＳ３０３，Ｓ３０５）、グループセッションに参加することを通知する。すると、接続制御サーバ２は、ユーザ端末Ａ１１、Ｂ１２、Ｄ１

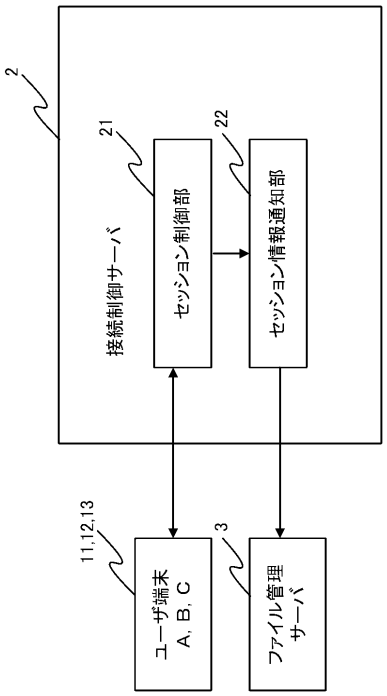
４との間で、グループセッションの確立を行う（ステップＳ３０６、点線参照）。
【００８５】
続いて、グループセッションが確立したユーザ端末Ａ１１、Ｂ１２、Ｄ１４の間で、ユーザ端末Ａ１１がファイルＺを共通にアクセスしたいユーザが正しいか否かを、このグループセッションを通して本人確認（声や映像や文字入力など）を実施する（ステップＳ３０６）。ところが、本例では、ユーザ端末Ｄ１４が共有を希望するユーザ端末Ｃ１３でないため、ユーザ端末Ａ１１は、直ちにグループセッションの終了を行うために、接続制御サーバ２に対してグループ共有終了指示を送信する（ステップＳ３０７）。このグループ共有終了指示を受信した接続制御サーバ２は、ユーザ端末Ｂ１２、Ｄ１４に対してグループ共有終了要求を送信する（ステップＳ３０８、Ｓ３１０）。そして、グループ共有終了要求を受信したユーザ端末Ｂ１２、Ｄ１４は、グループセッションの終了を許諾し、接続制御サーバ２に対してグループ共有終了応答を送信する（ステップＳ３０９、Ｓ３１１）。このようにして、グループ共有終了応答を受信した接続制御サーバ２は、グループセッション中の状態をクリア、つまり、セッションを終了する（ステップＳ３１２）。
【００８６】
以上のように、本発明では、共有ファイルを共有するよう予め設定された共有メンバ全員が、共通の通信状態を有する場合にのみ共有ファイルへのアクセスが可能となる。その結果、ファイルアクセスのセキュリティの向上を図ることができる。
【００８７】
また、共通のセッションにて接続されているユーザ端末のみが、当該セッションの内容に対応して生成された動的なパスワードに基づいて共有ファイルにアクセス可能となるため、第三者の不正アクセスを有効に抑制することができる。特に、セッションが切断されるとパスワードが無効となるため、仮にパスワードが盗まれた場合であっても、セッションを切断することで共有ファイルへのアクセスを防止できる。
【産業上の利用可能性】
【００８８】
本発明は、高度なセキュリティを要するファイル（映像や画像、文書ファイルなど）を、複数人でアクセス、閲覧、変更など共有することを可能とするシステムに適用可能であり、産業上の利用可能性を有する。
【図面の簡単な説明】
【００８９】
【図１】ファイル管理システムの構成を示すブロック図である。
【図２】接続制御サーバの構成を示す機能ブロック図である。
【図３】ファイル管理サーバの構成を示す機能ブロック図である。
【図４】共有ファイルの管理状況の一例を説明するための図である。
【図５】ファイル管理システムの動作の一例を示すシーケンス図である。
【図６】ファイル管理システムの動作の一例を示すシーケンス図であり、図５の続きを示す。
【図７】共有ファイルの管理状況の一例を説明するための図である。
【図８】ファイル管理システムの動作の一例を示すシーケンス図である。
【図９】ファイル管理システムの動作の一例を示すシーケンス図であり、図５の続きを示す。
【図１０】共有ファイルの管理状況の一例を説明するための図である。
【図１１】ファイル管理システムの動作の一例を示すシーケンス図である。
【図１２】ファイル管理システムの動作の一例を示すシーケンス図であり、図５の続きを示す。
【図１３】ファイル管理システムの動作の一例を示すシーケンス図である。
【符号の説明】
【００９０】
２　接続制御サーバ

３　ファイル管理サーバ
１１　ユーザ端末Ａ
１２　ユーザ端末Ｂ
１３　ユーザ端末Ｃ
１４　ユーザ端末Ｄ
２１　セッション制御部
２２　セッション情報通知部
３１　ファイル共有情報取得部
３２　ユーザ認証部
３３　パスワード設定部
３４　ファイルアクセス管理部
３５　共有解除部
３６　ファイル記憶部
３７　共有ユーザ管理情報記憶部

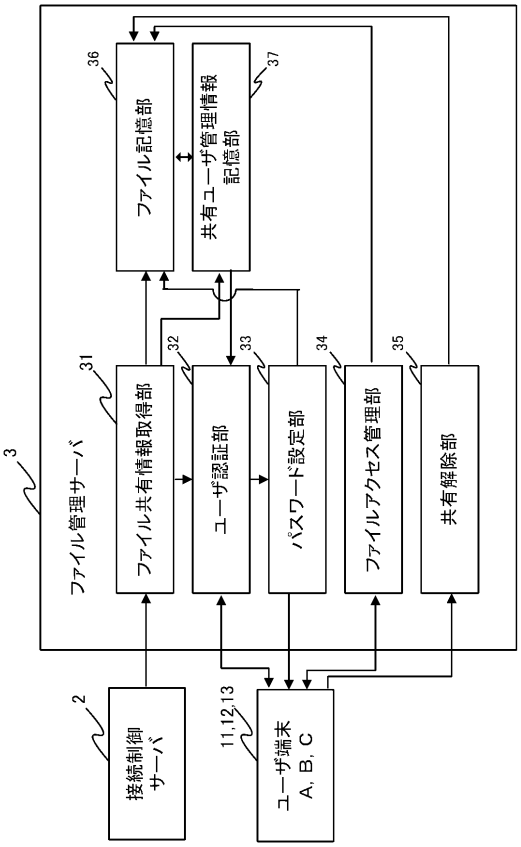
【図１】



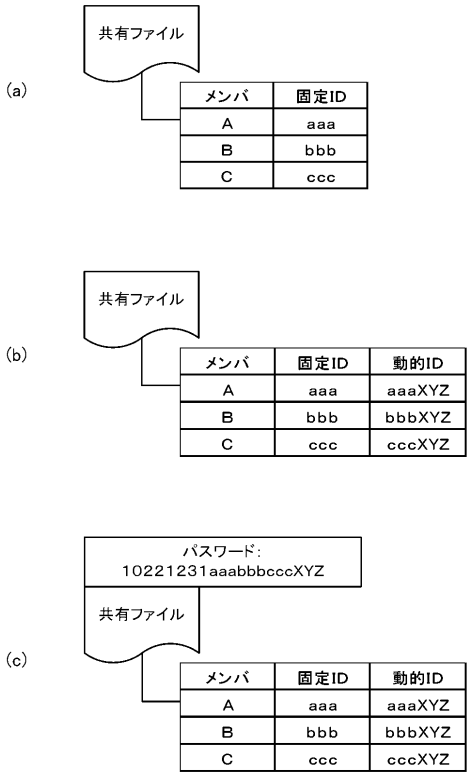
【図２】



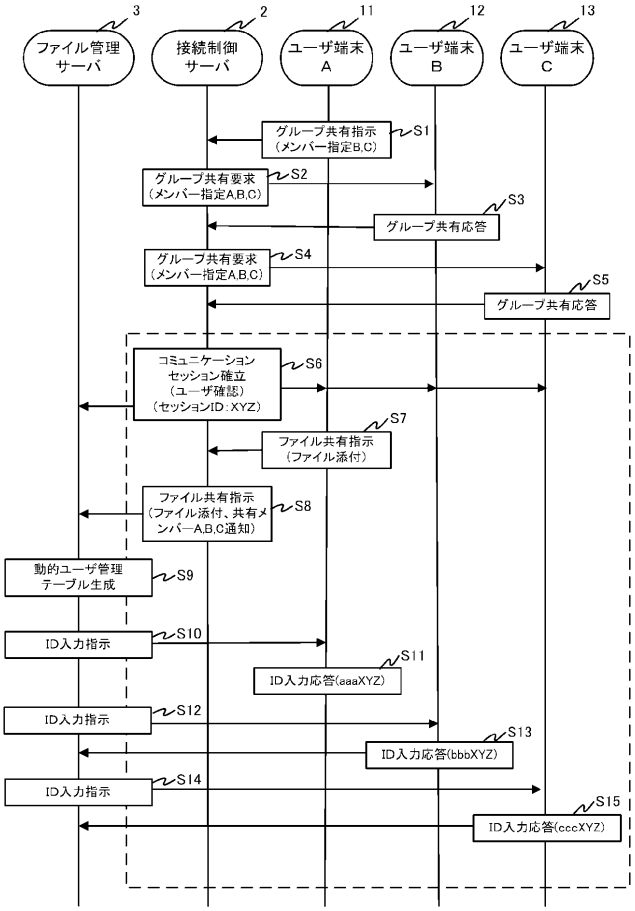
【図３】


ファイル管理サーバ
3
ファイル記憶部
36
共有ユーザ管理情報記憶部
37
ファイル共有情報取得部
31
ユーザ認証部
32
パスワード設定部
33
ファイルアクセス管理部
34
共有解除部
35
接続制御サーバ
2
ユーザ端末A, B, C
11,12,13

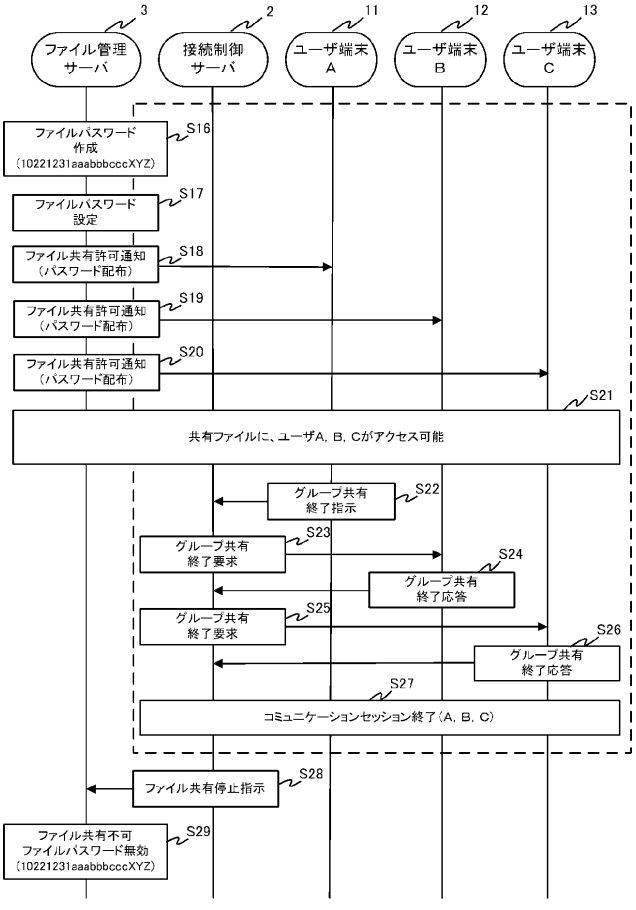
【図４】


(a)
共有ファイル
メンバ
固定ID
A
aaa
B
bbb
C
ccc
(b)
共有ファイル
メンバ
固定ID
動的ID
A
aaa
aaaXYZ
B
bbb
bbbXYZ
C
ccc
cccXYZ
(c)
パスワード:
10221231aaabbbcccXYZ
共有ファイル
メンバ
固定ID
動的ID
A
aaa
aaaXYZ
B
bbb
bbbXYZ
C
ccc
cccXYZ

【図５】


ファイル管理サーバ
3
接続制御サーバ
2
ユーザ端末A
11
ユーザ端末B
12
ユーザ端末C
13
グループ共有指示（メンバー指定B,C）
S1
グループ共有要求（メンバー指定A,B,C）
S2
グループ共有応答
S3
グループ共有要求（メンバー指定A,B,C）
S4
グループ共有応答
S5
コミュニケーションセッション確立（ユーザ確認）（セッションID：XYZ）
S6
ファイル共有指示（ファイル添付）
S7
ファイル共有指示（ファイル添付、共有メンバーA,B,C通知）
S8
動的ユーザ管理テーブル生成
S9
ID入力指示
S10
ID入力応答(aaaXYZ)
S11
ID入力指示
S12
ID入力応答(bbbXYZ)
S13
ID入力指示
S14
ID入力応答(cccXYZ)
S15

【図６】


ファイル管理サーバ
3
接続制御サーバ
2
ユーザ端末A
11
ユーザ端末B
12
ユーザ端末C
13
ファイルパスワード作成（10221231aaabbbcccXYZ）
S16
ファイルパスワード設定
S17
ファイル共有許可通知（パスワード配布）
S18
ファイル共有許可通知（パスワード配布）
S19
ファイル共有許可通知（パスワード配布）
S20
共有ファイルに、ユーザA, B, Cがアクセス可能
S21
グループ共有終了指示
S22
グループ共有終了要求
S23
グループ共有終了応答
S24
グループ共有終了要求
S25
グループ共有終了応答
S26
コミュニケーションセッション終了（A, B, C）
S27
ファイル共有停止指示
S28
ファイル共有不可ファイルパスワード無効（10221231aaabbbcccXYZ）
S29

【図７】

(a)

共有ファイル

メンバ	固定ID
A	aaa
B	bbb
C	ccc

(b)

共有ファイル

メンバ	固定ID	動的ID
A	aaa	aaaLMN
B	bbb	bbbLMN
C	ccc	cccLMN

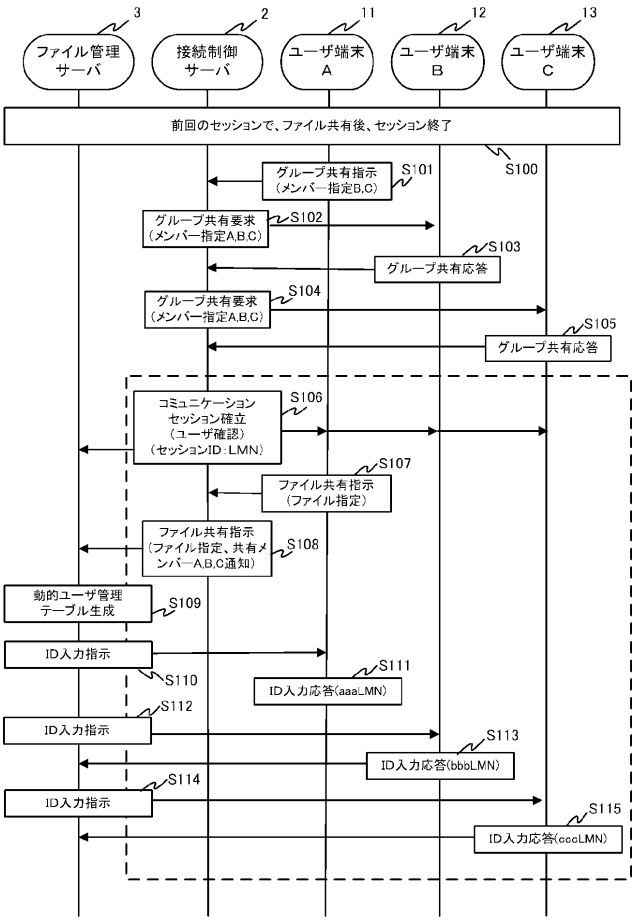
(c)

パスワード：
10221424aaabbbcccLMN

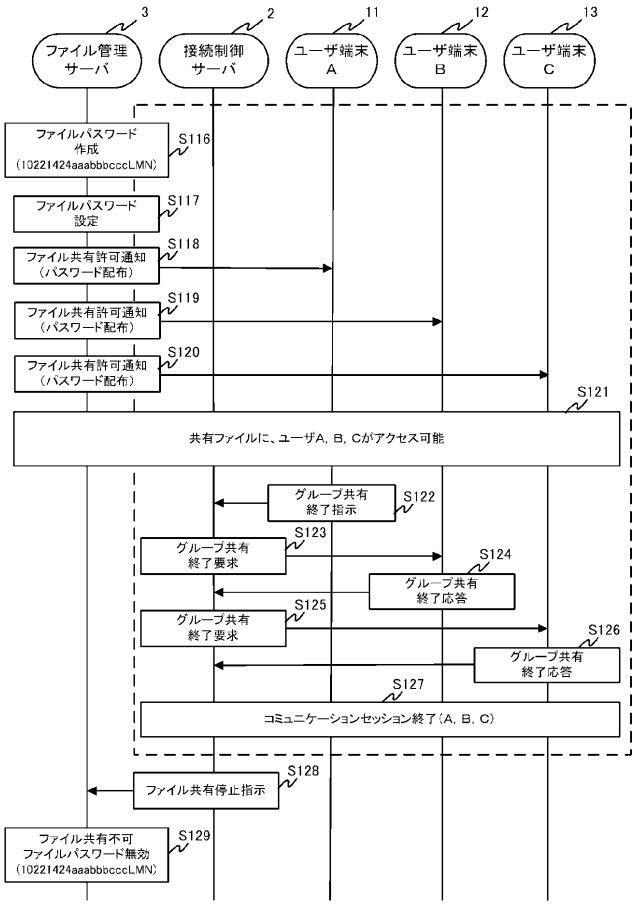
共有ファイル

メンバ	固定ID	動的ID
A	aaa	aaaLMN
B	bbb	bbbLMN
C	ccc	cccLMN

【図８】



【図９】



【図１０】

(a)

共有ファイル

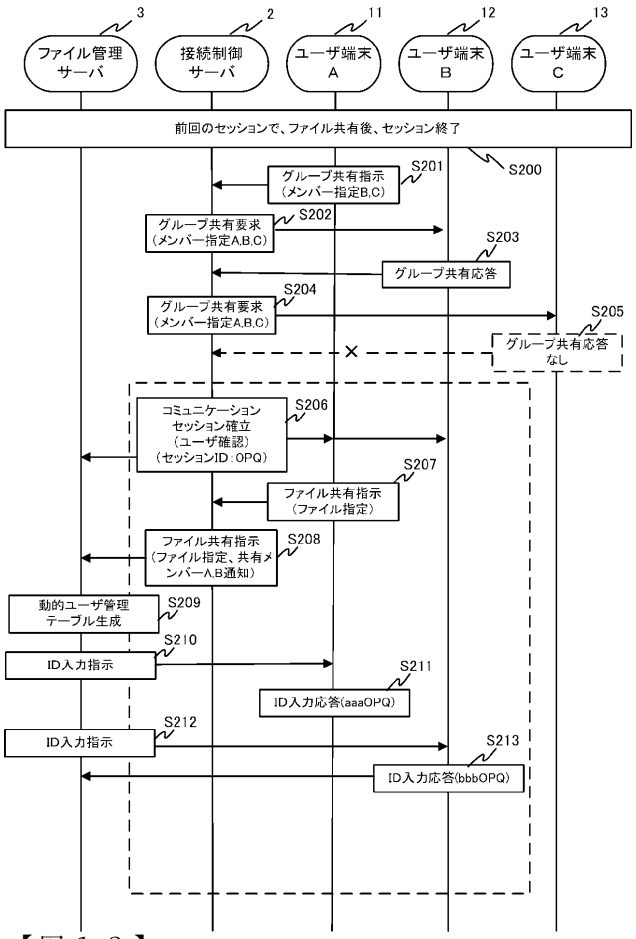
メンバ	固定ID
A	aaa
B	bbb
C	ccc

(b)

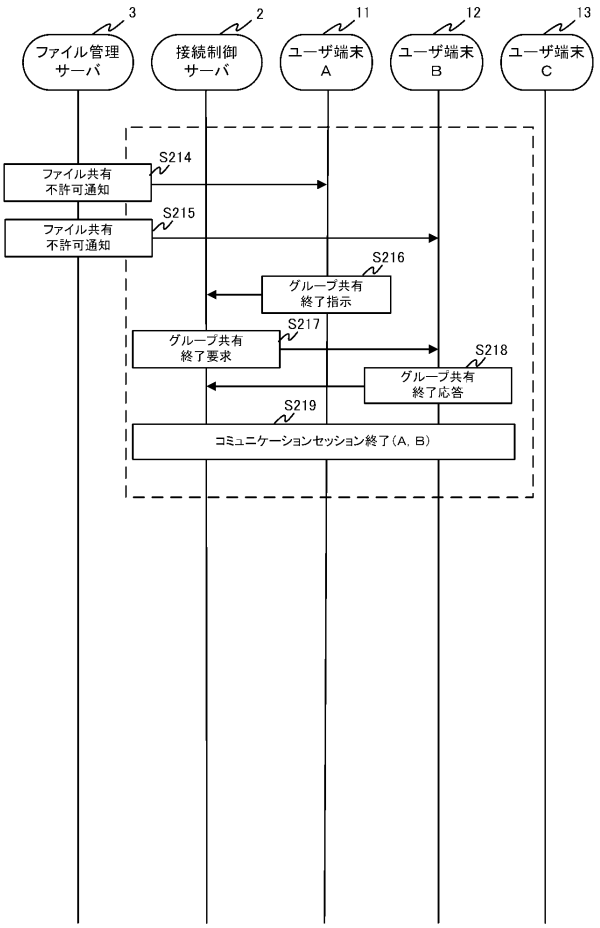
共有ファイル

メンバ	固定ID	動的ID
A	aaa	aaaOPQ
B	bbb	bbbOPQ
C	ccc	なし

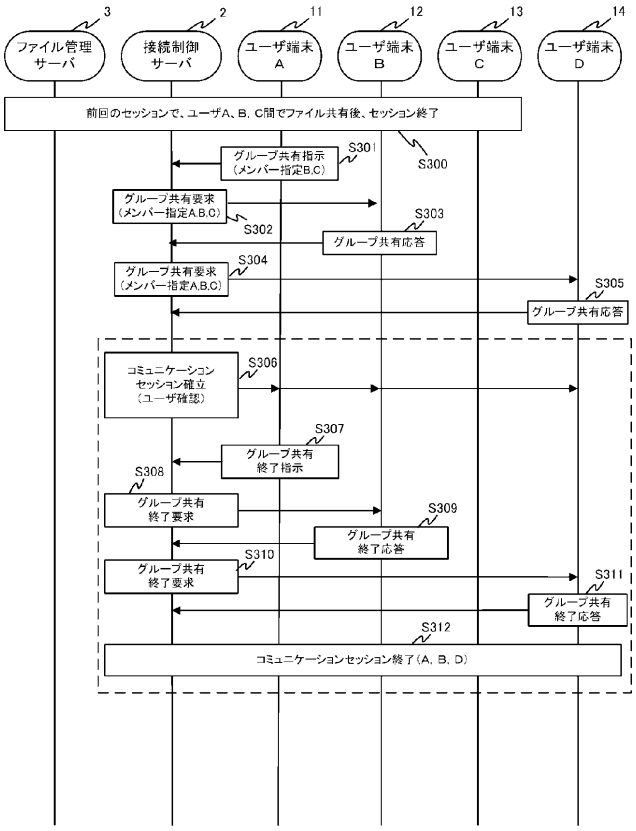
【図１１】


3
ファイル管理サーバ
2
接続制御サーバ
11
ユーザ端末A
12
ユーザ端末B
13
ユーザ端末C
前回のセッションで、ファイル共有後、セッション終了
S200
グループ共有指示（メンバー指定B,C）
S201
グループ共有要求（メンバー指定A,B,C）
S202
S203
グループ共有応答
S204
グループ共有要求（メンバー指定A,B,C）
S205
グループ共有応答なし
コミュニケーションセッション確立（ユーザ確認）（セッションID：OPQ）
S206
S207
ファイル共有指示（ファイル指定）
ファイル共有指示（ファイル指定、共有メンバーA,B通知）
S208
動的ユーザ管理テーブル生成
S209
ID入力指示
S210
S211
ID入力応答(aaaOPQ)
ID入力指示
S212
S213
ID入力応答(bbbOPQ)

【図１２】


3
ファイル管理サーバ
2
接続制御サーバ
11
ユーザ端末A
12
ユーザ端末B
13
ユーザ端末C
ファイル共有不許可通知
S214
ファイル共有不許可通知
S215
S216
グループ共有終了指示
グループ共有終了要求
S217
S218
グループ共有終了応答
S219
コミュニケーションセッション終了（A，B）

【図１３】


3
ファイル管理サーバ
2
接続制御サーバ
11
ユーザ端末A
12
ユーザ端末B
13
ユーザ端末C
14
ユーザ端末D
前回のセッションで、ユーザA、B、C間でファイル共有後、セッション終了
S300
グループ共有指示（メンバー指定B,C）
S301
グループ共有要求（メンバー指定A,B,C）
S302
S303
グループ共有応答
グループ共有要求（メンバー指定A,B,C）
S304
S305
グループ共有応答
コミュニケーションセッション確立（ユーザ確認）
S306
S307
グループ共有終了指示
S308
グループ共有終了要求
S309
グループ共有終了応答
S310
グループ共有終了要求
S311
グループ共有終了応答
S312
コミュニケーションセッション終了（A，B，D）