(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5000457号
(P5000457)
(45)発行日　平成24年8月15日(2012.8.15)　(24)登録日　平成24年5月25日(2012.5.25)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 21/24　160C

請求項の数 18　(全 56 頁)

(21)出願番号　特願2007-283688(P2007-283688)
(22)出願日　平成19年10月31日(2007.10.31)
(65)公開番号　特開2009-110401(P2009-110401A)
(43)公開日　平成21年5月21日(2009.5.21)
審査請求日　平成22年1月22日(2010.1.22)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100093861
弁理士　大賀　眞司
(72)発明者　児玉　昇司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　熊沢　清健
神奈川県小田原市中里３２２番２号　株式会社日立製作所ＲＡＩＤシステム事業部内
(72)発明者　岩見　直子
神奈川県小田原市中里３２２番２号　株式会社日立製作所ＲＡＩＤシステム事業部内
最終頁に続く

(54)【発明の名称】ファイル共有システム及びファイル共有方法

(57)【特許請求の範囲】
【請求項１】
第１の情報処理装置及び第２の情報処理装置と、前記情報処理装置とインターネットを介して接続される第1及び第２のストレージ装置とを含み、前記情報処理装置から前記ストレージ装置にファイルを格納し、その格納したファイルを前記情報処理装置で共有するファイル共有システムであって、
前記第１の情報処理装置は、
前記第１の情報処理装置で管理される情報であって、ファイルを作成するユーザを特定する第１のアカウント及び第１のパスを含むプライバシ情報と、前記第１のアカウントと異なる第２のアカウントと、前記第２のアカウントと異なる第３のアカウント及び前記第１のパスと異なる第２のパスと、第３のパスとを含む格納用管理情報とを少なくとも管理する第１の管理テーブルと、
前記第１のストレージ装置に新規ファイルを作成するときに、前記第１のアカウント及び前記第１のパスから前記第２のアカウント及び前記第２のパスを作成し、前記作成した前記第２のアカウント及び前記第２のパスを前記管理テーブルに前記第１のアカウント及び前記第１のパスに対応付けて登録する登録部と、
前記管理テーブルに登録された前記第２のアカウント及び前記第２のパスを用いて前記第１のストレージ装置に前記新規ファイルを作成するファイル作成部と、
前記第1のアカウント及び前記第１のパスで指定されたファイルを共有ファイルとして作成するときに、前記第1のアカウント及び前記第１のパスから、前記第２のアカウント

及び前記第２のパスを作成し、前記作成した前記第２のアカウント及び前記第２のパスを基に前記第３のアカウント及び前記第３のパスを作成し、前記作成した前記第２のアカウント及び前記第２のパスと、前記作成した前記第３のアカウント及び前記第３のパスを前記管理テーブルに前記第１のアカウント及び前記第１のパスに対応付けて登録して管理する共有処理部と、

前記共有処理部で作成された前記第２のアカウント及び前記第２のパスを用いて前記第１のストレージ装置から、前記共有ファイルとなる共有元ファイルをリードするリード部と、

前記リード部でリードされた前記共有元ファイルを、前記共有処理部で作成された前記第３のアカウント及び前記第３のパスを用いて前記第２のストレージ装置に共有先ファイルとして保存すると共に、前記共有先ファイルの説明情報を前記共有先ファイルに関連づけて保存する保存部と、

前記第２の情報処理装置は、

前記第２の情報処理装置で管理される情報であって、検索対象のファイルを割り当てるユーザを特定する第４のアカウント及び第４のパスを含むプライバシ情報と、前記第４のアカウントと異なる第５のアカウント及び前記第４のパスと異なる第５のパスとを含む格納用管理情報とを少なくとも管理する第２の管理テーブルと、

前記第１のストレージ装置または前記第２のストレージ装置からファイルを検索するときに、前記第４のアカウントから前記第５のアカウントを作成し、前記作成した第５のアカウントに対応したストレージ装置を検索対象のストレージ装置として、前記前記第１のストレージ装置または前記第２のストレージ装置の中から選択し、前記選択した検索対象のストレージ装置に対して、検索キーワードを指定して検索要求を行う要求処理部と、

前記検索対象のストレージ装置から、前記検索キーワードに対応するファイルの前記第５のパスと、当該第５のパスに対応する説明情報を検索結果として受信した場合、前記受信した検索結果を前記第４のパスに対応づけて前記第２の管理テーブルに登録する第２の登録部と、を備えること、

を特徴とするファイル共有システム。

【請求項２】

前記プライバシ情報は、さらに、前記第１のアカウントが属するグループ、ファイルの種別、ファイルのアクセス権限、前記情報処理装置から前記ストレージ装置にアクセスした時刻の少なくともいずれかの情報を含み、

前記管理テーブルは、前記プライバシ情報にさらに含まれる前記第１のアカウントが属するグループ、ファイルの種別、ファイルのアクセス権限、前記情報処理装置から前記ストレージ装置にアクセスした時刻の少なくともいずれかの情報を前記第１のアカウント及び前記第１のパスに対応付けて管理すること、

を特徴とする請求項１記載のファイル共有システム。

【請求項３】

前記情報処理装置は、さらに、

前記新規ファイルを暗号化する暗号化部を備え、

前記ファイル作成部は、前記暗号化部で暗号化された新規ファイルを前記ストレージ装置に作成し、

前記管理テーブルは、前記第１のアカウント及び前記第１のパスと対応付けて前記暗号化された新規ファイルを複合する暗号鍵を管理すること、

を特徴とする請求項１記載のファイル共有システム。

【請求項４】

前記第１の情報処理装置のファイル作成部は、

第１の新規ファイルを作成する際に、第１の暗号鍵を用いて前記暗号化部で暗号化された前記第１の新規ファイルを前記第２のアカウントを用いて前記ストレージ装置に作成し、

前記第２の情報処理装置のファイル作成部は、

第２の新規ファイルを作成する際に、第２の暗号鍵を用いて前記暗号化部で暗号化された前記第２の新規ファイルを前記第２のアカウントを用いて前記ストレージ装置に作成すること、
を特徴とする請求項３記載のファイル共有システム。
【請求項５】
前記登録部は、前記第１のアカウントから前記第２のアカウントを生成するときに、前記第１のアカウントを用いて作成されるファイル群に対して、ファイル毎に異なる前記第２のアカウントを割り当て、
前記ファイル作成部は、前記ファイル毎に異なる第２のアカウントを用いて各ファイルを前記ストレージ装置に作成すること、
を特徴とする請求項１記載のファイル共有システム。
【請求項６】
前記登録部は、前記新規ファイルを作成するときに、前記ファイル毎に異なる第２のアカウントから、ファイル数が一番少ない第２のアカウントを選択し、
前記ファイル作成部は、前記選択された第２のアカウントを用いて前記ストレージ装置にファイルを作成すること、
を特徴とする請求項５記載のファイル共有システム。
【請求項７】
前記情報処理装置は、
前記第１のアカウント及び前記第１のパスを用いて指定されるファイルのリード要求を受けると、前記リード要求されたファイルに対するアクセス権限があるか否かを、前記管理テーブルを参照して判定するアクセス権限判定部と、
前記アクセス権限判定部でアクセス権限があると判定した場合に、前記管理テーブルを参照し、前記リート要求されたファイルに対応付けられた第２のアカウント及び第２のパスを用いて、前記ストレージ装置に対してリード要求し、前記リード要求されたファイルをリードするリード処理部と、
を備えることを特徴とする請求項２記載のファイル共有システム。
【請求項８】
前記情報処理装置は、
前記第１のアカウント及び前記第１のパスを用いて指定されるファイルのライト要求を受けると、前記ライト要求されたファイルに対するアクセス権限があるか否かを、前記管理テーブルを参照して判定するアクセス権限判定部と、
前記アクセス権限判定部でアクセス権限があると判定した場合に、前記管理テーブルを参照し、前記ライト要求されたファイルに対応付けられた第２のアカウント及び第２のパスを用いて、前記ストレージ装置に対してライト要求をし、前記ライト要求のライト結果を更新する更新処理部と、
を備えることを特徴とする請求項２記載のファイル共有システム。
【請求項９】
前記管理テーブルは、さらに、登録されるファイル毎に時刻情報を管理し、
前記情報処理装置は、
ランダムに決定された時刻に、前記管理テーブルからランダムに決定したファイルに対して、前記管理テーブル内の時刻情報は更新せず、前記ストレージ装置内の前記ランダムに決定されたファイルにアクセスするアクセス部を更に備えること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１０】
前記情報処理装置は、
前記ストレージ装置にランダムな内容を有する新規ファイルを作成するダミーファイル作成部を備えること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１１】

前記ストレージ装置は、
前記第２のアカウントと対応づけたパスワードを管理するアカウント管理テーブルを備え、
前記情報処理装置は、
定期的に前記ストレージ装置に対して、前記第２のアカウントと対応するパスワードを変更するパスワード変更部を備えること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１２】
前記情報処理装置は、前記第３のアカウント及び前記第３のパスで指定されるファイルを前記異なるストレージ装置から削除するファイル削除部を備えること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１３】
前記異なるストレージ装置にアクセス可能な情報処理装置は、
ファイルを検索するユーザを特定する第４のアカウントを含むプライバシ情報とともに検索に用いられる検索情報の入力を受け付け、前記第４のアカウントと対応する第５のアカウントを用いて前記異なるストレージ装置にアクセスし、前記検索情報を用いて前記異なるストレージ装置内の説明情報を検索する要求をする検索要求部と、
この検索要求部の要求に基づいて検索された説明情報及びその説明情報に関連付けられたファイルのパスを検索結果として受け取る検索結果受信部とを備えること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１４】
前記ファイル作成部は、前記新規ファイルを作成するときに、その作成する新規ファイルを所定のサブ・ファイルに分割し、その分割されたサブ・ファイル毎に前記第２のパスを決定し、その第２のパスを用いて前記複数のストレージ装置に前記ファイルを前記サブ・ファイル毎に分割して作成する処理を含み、
前記管理テーブルは、前記サブ・ファイル毎に決定した第２のパスと前記サブ・ファイルを作成したストレージ装置との対応関係の管理を含むこと、
を特徴とする請求項１記載のファイル共有システム。
【請求項１５】
前記少なくとも１以上の情報処理装置と、前記ストレージ装置との間に前記インターネット上のアドレスを変換するサーバを備え、
前記情報処理装置は、前記サーバを経由して前記ストレージ装置へアクセスすること、
を特徴とする請求項１記載のファイル共有システム。
【請求項１６】
前記第１のパスと、前記第２のパスと、前記第３のパスと、前記第４のパス及び前記第５のパスは、異なる名前空間で管理されること
を特徴とする請求項１記載のファイル共有システム。
【請求項１７】
第１の情報処理装置及び第２の情報処理装置と、前記情報処理装置とインターネットを介して接続される第1及び第２のストレージ装置とを含み、前記情報処理装置から前記ストレージ装置にファイルを格納し、その格納したファイルを前記情報処理装置で共有するファイル共有システムのファイル共有方法であって、
前記第１の情報処理装置は、
前記第１の情報処理装置で管理される情報であって、ファイルを作成するユーザを特定する第１のアカウント及び第１のパスを含むプライバシ情報と、前記第１のアカウントと異なる第２のアカウントと、前記第２のアカウントと異なる第３のアカウント及び前記第１のパスと異なる第２のパスと、第３のパスとを含む格納用管理情報とを少なくとも管理する第１の管理テーブルを含み、
前記第１のストレージ装置に新規ファイルを作成するときに、前記第１のアカウント及び前記第１のパスから前記第２のアカウント及び前記第２のパスを作成し、前記作成した

前記第２のアカウント及び前記第２のパスを前記管理テーブルに前記第１のアカウント及び前記第１のパスに対応付けて登録するステップと、
前記管理テーブルに登録された前記第２のアカウント及び前記第２のパスを用いて前記第１のストレージ装置に前記新規ファイルを作成するステップと、
前記第1のアカウント及び前記第１のパスで指定されたファイルを共有ファイルとして作成するときに、前記第1のアカウント及び前記第１のパスから、前記第２のアカウント及び前記第２のパスを作成し、前記作成した前記第２のアカウント及び前記第２のパスを基に前記第３のアカウント及び前記第３のパスを作成し、前記作成した前記第２のアカウント及び前記第２のパスと、前記作成した前記第３のアカウント及び前記第３のパスを前記管理テーブルに前記第１のアカウント及び前記第１のパスに対応付けて登録して管理するステップと、
前記作成された前記第２のアカウント及び前記第２のパスを用いて前記第１のストレージ装置から、前記共有ファイルとなる共有元ファイルをリードするステップと、
前記リードされた前記共有元ファイルを、前記作成された前記第３のアカウント及び前記第３のパスを用いて前記第２のストレージ装置に共有先ファイルとして保存すると共に、前記共有先ファイルの説明情報を前記共有先ファイルに関連づけて保存するステップとを備え、
前記第２の情報処理装置は、
前記第２の情報処理装置で管理される情報であって、検索対象のファイルを割り当てるユーザを特定する第４のアカウント及び第４のパスを含むプライバシ情報と、前記第４のアカウントと異なる第５のアカウント及び前記第４のパスと異なる第５のパスとを含む格納用管理情報とを少なくとも管理する第２の管理テーブルを含み、
前記第１のストレージ装置または前記第２のストレージ装置からファイルを検索するときに、前記第４のアカウントから前記第５のアカウントを作成し、前記作成した第５のアカウントに対応したストレージ装置を検索対象のストレージ装置として、前記前記第１のストレージ装置または前記第２のストレージ装置の中から選択し、前記選択した検索対象のストレージ装置に対して、検索キーワードを指定して検索要求を行うステップと、
前記検索対象のストレージ装置から、前記検索キーワードに対応するファイルの前記第５のパスと、当該第５のパスに対応する説明情報を検索結果として受信した場合、前記受信した検索結果を前記第４のパスに対応づけて前記第２の管理テーブルに登録するステップとを備えること、
を特徴とするファイル共有方法。
【請求項１８】
前記第１のパスと、前記第２のパスと、前記第３のパスと、前記第４のパス及び前記第５のパスは、異なる名前空間で管理されること
を特徴とする請求項１７記載のファイル共有方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ファイル共有システム及びファイル共有方法に関し、例えば、不特定多数の情報処理装置がアクセスするオンライン・ファイル・ストレージに格納したファイルを、第三者と共有する際に、そのファイルを使用するユーザのプライバシを保護するファイル共有システム及びファイル共有方法に適用しても好適なものである。
【背景技術】
【０００２】
ユーザはＰＣ（Personal Computer）内のファイルをインターネット経由で“Amazon S3 (Simple Storage Service)”を代表とするオンライン・ファイル・ストレージやファイル・サーバに格納することが出来る。これらネットワーク接続型のストレージ装置では、ファイルをオンライン・ファイル・ストレージに格納する際に、ＮＦＳ（Network File System）やＨＴＴＰ（Hyper Text Transfer Protocol）などが利用されている。

【０００３】
ＮＦＳやＨＴＴＰは、ストレージ装置側がファイル・システム機能を有し、ファイル・システムがアカウント情報データベースとファイルのパス名、ディスク・ドライブ上のファイルの物理レイアウトを集中管理している。
【０００４】
オンライン・ファイル・ストレージは、クライアントが指定したアカウント名とパスワードをアカウント情報データベースと照合することによってクライアントを認証する。そして、オンライン・ファイル・ストレージはファイル毎にアクセス権情報を管理し、アクセス権を有するアカウントのみ、そのファイルへのアクセスを許可することで、不正アクセスを防止している。
【０００５】
ファイルには、オンライン・ファイル・ストレージ内でファイルを一意に識別するパス名が付与される。パス名はファイルが格納されているディレクトリの階層とファイル名から構成される。ディレクトリの階層やファイル名には任意の文字列を利用できるが、通常はファイル作成者本人がファイルの内容を理解できるような固有名詞や数字を利用する。ファイルのパス名はそのファイルを格納するオンライン・ファイル・ストレージが管理している（例えば、非特許文献１参照）。
【０００６】
また、ネットワークに接続する複数のオンライン・ファイル・ストレージを仮想的な一つのストレージ装置として利用できる“CleverSafe”や“pNFS”という技術がある。これら技術は、ファイルを格納するオンライン・ファイル・ストレージと、ファイルにアクセスするクライアントと、ファイルの所在を管理するメタ・データ・サーバから構成される。
【０００７】
メタ・データ・サーバは、クライアントが指定したアカウント名とパスワードをアカウント情報データベースと照合することによってクライアントを認証する。オンライン・ファイル・ストレージも、クライアントが指定したアカウント名とパスワードをアカウント情報データベースと照合することによってクライアントを認証する。“CleverSafe”の場合、メタ・データ・サーバ、オンライン・ファイル・ストレージ、及び、クライアント間で一つのアカウント情報データベースを利用する。ユーザやアプリケーションは、クライアントに一回ログインするだけで、メタ・データ・サーバや複数のオンライン・ファイル・ストレージ毎にアカウント情報を覚えておく必要はない。クライアントは、ファイル作成時に、作成するファイルのパス名を指定してメタ・データ・サーバに対してファイル作成要求を出す。それに対して、メタ・データ・サーバが、該ファイルをどのオンライン・ファイル・ストレージに格納するのか位置を決定し、その位置情報をクライアントに返す。クライアントはファイルを指定されたオンライン・ファイル・ストレージに格納する。ファイルのパス名はメタ・データ・サーバが管理する。メタ・データ・サーバは複数存在でき、それぞれ独立した名前空間を持つ事ができる（例えば、非特許文献２参照）。
【非特許文献１】http://aws.amazon.com/s3
【非特許文献２】http://www.cleversafe.org/wiki/Login_authentication
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、従来技術では、ファイル利用や共有の利便性を追求してきたため、個人のプライバシ情報をいかに保護するか、という点で欠点があった。特にオンライン・ファイル・ストレージは信用度が低いサービスもあるため、ユーザが、自身のプライバシ情報が漏洩するのを嫌い使用に躊躇することもあり上記サービスの普及が遅れている。
【０００９】
例えば、“Amazon（登録商標）”のようなサービスの場合、ファイルをオンライン・ファイル・ストレージに格納する際にファイルに付属する情報として個人を特定する情報も

合わせて格納していた。これをプライバシ情報と呼ぶ。プライバシ情報の例として、ファイルの所有者名、その所有者が属するグループ名、ファイルのパス名、ファイル種別、ファイルへのアクセス時刻、ファイルのアクセス権限情報などがある。

【００１０】

アカウント名をオンライン・ファイル・ストレージ側で管理する場合のプライバシ上の問題点を説明する。オンライン・ファイル・ストレージ側で、そのアカウントで作成した全ファイルをリストアップ可能であるため、アカウント名やファイルのパス名、アクセス履歴を関連付けて分析することで、そのアカウントを開設したユーザやユーザの行動を特定することが可能になる。そのためユーザのプライバシを保護できないという問題があった。

【００１１】

ファイルのパス名にランダムな文字列を使うことで、個人の特定を困難する解決策も考えられるが、ランダムな文字列の場合、ファイル名からではファイルの内容を推測することができず、利用者にとって不便になるという問題がある。また、ファイル毎にそのファイルを所有するアカウント名情報をオンライン・ファイル・ストレージ側が管理しているため、いつどのアカウントがどのファイルにアクセスしたかを分析することで、ユーザやユーザの行動を特定することが可能になる。

【００１２】

“CleverSafe”のようなアーキテクチャを利用する場合、メタ・データ・サーバがファイルのパス名を管理するため、オンライン・ファイル・ストレージ側からだけではファイルに付属する情報を参照しても、ファイルのパス名を得ることは出来ない。そのため、ユーザを特定しにくくなる。ユーザはパス名を使ってファイルにアクセスできるため、ユーザの利便性は損なわれない。

【００１３】

しかしながら、アカウント情報はメタ・データ・サーバ、オンライン・ファイル・ストレージ、クライアント間で共有するため、どのアカウント利用者がどのファイルへアクセスしたかのアクセス履歴情報はオンライン・ファイル・ストレージ側で収集できる。そのため、その情報を解析することでユーザやユーザの行動を特定できてしまうという問題があった。

【００１４】

本発明は、以上の点を考慮してなされたもので、ユーザがファイルをオンライン・ファイル・ストレージに対して処理する場合に、利便性を損なわずにユーザのプライバシ情報を保護するファイル共有システム及びファイル共有方法を提案しようとするものである。

【００１５】

また、本発明のもう一つの目的は、ユーザのプライバシ情報を保護したまま、オンライン・ファイル・ストレージを介して複数のユーザ間でデータ共有を行えるファイル共有システム及びファイル共有方法を提案しようとするものである。

【課題を解決するための手段】

【００１６】

本発明は、少なくとも１以上の情報処理装置と、これら少なくとも１以上の情報処理装置とインターネットを介して接続されるストレージ装置とを含み、少なくとも１以上の情報処理装置からストレージ装置にファイルを格納し、その格納したファイルを少なくとも１以上の情報処理装置で共有するファイル共有システムであって、情報処理装置は、ストレージ装置にファイルを作成するときに、ファイルを作成するユーザを特定するプライバシ情報をストレージ装置にファイルを作成するために必要な情報から分離し、その分離されたプライバシ情報を変換した情報を用いてファイルをストレージ装置に作成するファイル作成部を備えるのである。

【００１７】

また、本発明は、少なくとも１以上の情報処理装置と、これら少なくとも１以上の情報処理装置とインターネットを介して接続されるストレージ装置とを含み、少なくとも１以

上の情報処理装置からストレージ装置にファイルを格納し、その格納したファイルを少なくとも１以上の情報処理装置で共有するファイル共有システムであって、情報処理装置は、ファイルを作成するユーザを特定する第１のアカウント及び第１のパスを含むプライバシ情報と、第１のアカウントと異なる第２のアカウント及び第１のパスと異なる第２のパスを含む格納用管理情報とを少なくとも管理する管理テーブルと、ストレージ装置に新規ファイルを作成するときに、第１のアカウント及び第１のパスから２のアカウント及び第２のパスを作成し、管理テーブルに第１のアカウント及び第１のパスに対応付けて登録する登録部と、管理テーブルに登録された第２のアカウント及び第２のパスを用いてストレージ装置に新規ファイルを作成するファイル作成部とを備えるものである。

【発明の効果】

【００１８】

本発明によれば、ユーザがファイルをオンライン・ファイル・ストレージに対して処理する場合に、利便性を損なわずにユーザのプライバシ情報を保護するファイル共有システム及びファイル共有方法を提案できる。

【００１９】

また、本発明によれば、ユーザのプライバシ情報を保護したまま、オンライン・ファイル・ストレージを介して複数のユーザ間でデータ共有を行えるファイル共有システム及びファイル共有方法を提案できる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の各実施の形態について図面を参照して説明する。

【００２１】

（第１の実施形態）

先ず、第１の実施形態について説明する。図１は、プライバシ保護ファイル共有システムの構成を示す図である。図１に示すように、プライバシ保護ファイル共有システム１は、ＰＣ（Personal Computer）１００、携帯型端末２００、オンライン・ファイル・ストレージ３００及び４００を有している。ＰＣ１００、携帯型端末２００、オンライン・ファイル・ストレージ３００及び４００は、インターネット１０を介して接続されている。なお、プライバシ保護ファイル共有システム１に含まれるＰＣ１００、携帯型端末２００、オンライン・ファイル・ストレージ３００，４００は、図１に示すものに限られず、ＰＣ又は携帯型端末が少なくとも１台以上、オンライン・ファイル・ストレージが１台以上であればよい。

【００２２】

また、図１に示すプライバシ保護ファイル共有システム１では、ファイルを格納する記憶装置として、インターネット１０に接続されるオンライン・ファイル・ストレージ３００，４００を用いている構成となっているが、プライバシ保護ファイル共有システムは例えば、データセンター内のローカル環境にも適用することができる。このようにローカル環境にプライバシ保護ファイル共有システム１を適用した場合には、オンライン・ファイル・ストレージに代えて、ファイル・サーバやＮＡＳ（Network Attached Storage）などを利用することができる。また、ＰＣとファイル・サーバなどとの接続には、イーサネット（登録商標）を利用することができる。

【００２３】

ＰＣ１００は、アプリケーション１１０、個人ファイル管理システム１２０を有している。アプリケーション１１０は、各種業務を行なうためのアプリケーションを実現する制御部であり、個人ファイル管理システム１２０を介して、オンライン・ファイル・ストレージ３００又は４００内にファイルを作成し、その作成されたファイルの参照、更新を行なう。個人ファイル管理システム１２０は、ファイルを管理するために必要な管理情報のうち、アプリケーションを利用しているユーザ個人を特定する管理情報（以下、プライバシ情報と称する。）を分離し、プライバシ情報を個人ファイル管理システム１２０内で管理することで、オンライン・ファイル・ストレージ３００，４００からプライバシ情報を

保護する処理を行う。この処理の詳細については後述する。

【００２４】

個人ファイル管理システム１２０は、初期化部１３０、要求処理部１４０、匿名化支援機能部１５０、個人アカウント管理テーブル１６０、ストレージ管理テーブル１７０、ファイル管理テーブル１８０及び匿名化契機テーブル１９０を有している。初期化部１３０は、ユーザが個人ファイル管理システム１２０に対して新しくファイル・システムを作成する要求を出した場合に実行する処理部である。要求処理部１４０は、ファイルの作成・参照・更新・削除、ファイル検索、ファイル共有、アカウント管理などアプリケーション１１０からの要求を処理する処理部である。匿名化支援機能部１５０は、アプリケーション１１０からのファイル・アクセス要求とは無関係にオンライン・ファイル・ストレージ３００，４００内のファイルにアクセスしたりランダムなファイルを作成することで、アクセス履歴に関する匿名性を維持するとともに、ストレージ・アカウントのパスワードを定期的に変更することでパスワードのクラッキングを防止する処理を行う処理部である。なお、初期化部１３０、要求処理部１４０、匿名化支援機能部１５０の処理の内容及び個人アカウント管理テーブル１６０、ストレージ管理テーブル１７０、ファイル管理テーブル１８０、匿名化契機テーブル１９０に保存される内容についての詳細は後述する。

【００２５】

携帯型端末２００は、例えば、ＰＤＡ（Personal Digital Assistant）である。携帯型端末２００は、アプリケーション２１０、個人ファイル管理システム２２０を有している。これらの説明については、符号が異なるもののＰＣ１００と同じ説明になるため詳細な説明は省略する。なお、図１においては、個人ファイル管理システム２２０内の各処理部及びテーブルについては図示を省略している。

【００２６】

オンライン・ファイル・ストレージ３００は、ＰＣ１００、携帯型端末２００からのファイルを格納するストレージである。オンライン・ファイル・ストレージ３００は、ファイル・サーバ部３１０、ストレージ・アカウント管理テーブル３２０、ファイル・システム管理情報テーブル３３０、ボリューム３４０を有している。ファイル・サーバ部３１０は、ファイル・サーバとしての機能を実現する処理を実行する。ストレージ・アカウント管理テーブル３２０及びファイル・システム管理情報テーブル３３０に保存される内容については後述する。ボリューム３４０は、複数の物理ディスクから論理的に構成されている。なお、オンライン・ファイル・ストレージ４００は、オンライン・ファイル・ストレージ３００と符号が異なるものの同様な構成であるため、説明を省略する。

【００２７】

図２は、ＰＣ１００の物理的な構成を示す図である。ＰＣ１００は、ＣＰＵ（Central Processing Unit）１０１、メモリ１０２、ＨＤＤ（Hard Disk Drive）、ネットワーク・インタフェース１０５を構成要素として持ち、これらが内部バス１０４を介して接続されている。さらに、内部バス１０４には、ディスプレイ１０６、キーボード１０７、マウス１０８が接続される。

【００２８】

ＣＰＵ１０１は、メモリ１０２に格納された各種プログラムを実行して、上記アプリケーション１１０、個人ファイル管理システム１２０で行なわれる初期化部１３０の処理、要求処理部１４０の処理、匿名化支援機能部１５０の処理などの各種処理を実現する。メモリ１０２は、ＣＰＵ１０１が実行する各種プログラムを保存するとともに個人アカウント管理テーブル１６０、ストレージ管理テーブル１７０、ファイル管理テーブル１８０、匿名化契機テーブル１９０を保持する。ネットワーク・インタフェース１０５は、インターネット１０を介したオンライン・ファイル・ストレージ３００，４００との通信を制御する。ディスプレイ１０６は、ユーザがＰＣ１００を用いて操作を行なう際にユーザに必要な情報を表示する。キーボード１０７、マウス１０８は、ユーザがＰＣ１００で各種操作を行なう際に、ＰＣ１００に指示入力するために用いられる。

【００２９】

図３は、オンライン・ファイル・ストレージ３００の物理的な構成を示す図である。オンライン・ファイル・ストレージ３００は、ネットワーク・インタフェース３０１、コントローラ３０２、キャッシュメモリ３０３、内部バス３０４、ディスク・インタフェース３０５、ハードディスクドライブ３０６～３０８を有している。

【００３０】

ネットワーク・インタフェース３０１は、インターネット１０を介したＰＣ１００，携帯型端末２００との通信を制御する。コントローラ３０２は、メモリ等を内蔵しており、メモリに格納されたプログラムを実行することにより、ファイル・サーバ部３１０の処理を実行する。キャッシュメモリ３０３は、ネットワーク・インタフェース３０１を介して受信したデータを一時的に保存する。内部バス３０４は、ネットワーク・インタフェース３０１、コントローラ３０２、キャッシュメモリ３０３、ディスク・インタフェース３０５を接続する。ディスク・インタフェース３０５は、ハードディスクドライブ３０６～３０８へのデータのライトや、ハードディスクドライブ３０６～３０８からのデータのリードを制御する。ハードディスクドライブ３０６～３０８は、ボリューム３４０を構成するとともに各種ファイルを保存する。

【００３１】

次に、ＰＣ１００内の個人ファイル管理システム１２０に記憶される個人アカウント管理テーブル１６０、ストレージ管理テーブル１７０及びファイル管理テーブル１８０について図４から図８を参照して説明する。

【００３２】

図４は、個人アカウント管理テーブル１６０の一例を示す図である。個人アカウント管理テーブル１６０は、個人ファイル管理システム１２０がユーザを認証するために利用するアカウント名とパスワードを管理するためのテーブルである。この個人アカウント管理テーブル１６０は、個人ファイル管理システム１２０毎に存在する。

【００３３】

個人アカウント管理テーブル１６０は、個人アカウント名欄１６１、パスワード欄１６２、パスワード期限欄１６３、所属グループ名欄１６４を有している。個人アカウント名欄１６１は、この個人アカウントテーブル１６０を管理する個人ファイル管理システム１２０内でユニークな、ユーザを識別するためのアカウント名を保存する欄である。パスワード欄１６２は、アカウント名に対応するパスワードを保存する欄である。このパスワードは、パスワードが一致することで正しいユーザであるか否かの認証を行うために用いられる。パスワード期限欄１６３は、パスワードが有効な期限を保存する欄である。所属グループ名欄１６４は、アカウントが所属するグループ名を保存する欄である。なお、グループ名は個人ファイル管理システム１２０内でユニークな情報である。

【００３４】

個人アカウント管理テーブル１６０には、例えば、個人アカウント名欄１６１に“ＵＳＥＲ１”、パスワード欄１６２に“ＰＷＡ”、パスワード期限欄１６３に“０７／０７／０７”、所属グループ名欄１６４に“Ｇｒｏｕｐ１”が保存される。

【００３５】

図５は、ストレージ管理テーブル１７０の一例を示す図である。ストレージ管理テーブル１７０は、個人ファイル管理システム１２０がファイルを格納するオンライン・ファイル・ストレージ群と、ファイルを格納する際に利用可能なオンライン・ファイル・ストレージ側のアカウント情報を管理するためのテーブルである。一つのオンライン・ファイル・ストレージに複数のアカウントが利用可能なため、アカウント数分テーブルのエントリが存在する。ストレージ管理テーブル１７０は、ストレージ識別子欄１７１、ストレージ・アカウント名欄１７２、パスワード欄１７３、パスワード期限欄１７４、利用ファイル数欄１７５を有する。

【００３６】

ストレージ識別子欄１７１は、オンライン・ファイル・ストレージを一意に識別する為のストレージ識別子を保存する欄である。例えば、オンライン・ファイル・ストレージの

ＩＰ（Internet Protocol）アドレスやＵＲＬ（Uniform Resource Locator）などを使う。ストレージ・アカウント名欄１７２は、オンライン・ファイル・ストレージが管理しているアカウント名を保存する欄である。このストレージ・アカウント欄１７２に保存されるアカウント名は、個人ファイル管理システム１２０が管理する個人アカウント名とは異なるものである。パスワード欄１７３は、ストレージ・アカウントに対応するパスワードを保存する欄である。このパスワードは、オンライン・ファイル・ストレージがアカウントを認証する際に利用される。パスワード期限欄１７４は、パスワードの有効期限を保存する欄である。利用ファイル数欄１７５は、オンライン・ファイル・ストレージ内で該アカウントが所有する利用ファイルを保存する欄である。一つの個人アカウントが複数のストレージ・アカウントを利用している場合に、ストレージ・アカウント間で作成したファイル数に偏りが発生することで個人が特定されないよう、ストレージ・アカウント毎に所有するファイル数が均等になるよう、ファイル作成時に利用するストレージ・アカウントを決定する。

【００３７】

ストレージ管理テーブル１７０には、例えば、ストレージ識別子欄１７１に“ＳＴＲ１”、ストレージ・アカウント名欄１７２に“ＡＣＮＴ１”、パスワード欄１７３に“ＰＷ１”、パスワード期限欄１７４に“０７／０７／０７”、利用ファイル数欄１７５に“１００”が保存される。

【００３８】

図６は、ファイル管理テーブル１８０の一例を示す図である。ファイル管理テーブル１８０は、エントリ番号欄１８１、プライバシ情報欄１８２、格納用管理情報欄１８３、共有管理情報欄１８４を有している。このようにファイル管理テーブル１８０で管理される情報は、目的に応じて大きく３つの情報、すなわち、プライバシ情報、格納用管理情報、共有管理情報に分けられる。

【００３９】

エントリ番号欄１８１に保存されるエントリ番号は、個人ファイル管理システム１２０が管理するファイル個々に割り当てられるユニークな識別子である。プライバシ情報欄１８２に保存されるプライバシ情報はファイルの管理情報のうちプライバシに関する情報である。格納用管理情報欄１８３に保存される格納用管理情報は、ファイルをどのオンライン・ファイル・ストレージに格納したかを管理する。共有管理情報欄１８４に保存される共有管理情報は、ファイル共有に必要な情報を管理する。以下、プライバシ情報、格納用管理情報及び共有管理情報について詳細に説明する。

【００４０】

先ず、プライバシ情報について説明する。プライバシ情報が保存されるプライバシ情報欄１８２は、個人パス名欄１８２１、個人アカウント名欄１８２、個人用アクセス権限情報欄１８２３、個人用時刻情報欄１８２４を有している。

【００４１】

個人パス名欄１８２１は、個人ファイル管理システム１２０が管理するファイルの名前空間で該ファイルを識別するための情報であり、ディレクトリ階層とファイル名から成る個人パス名を保存する。個人アカウント名欄１８２は、該ファイルの所有者を示す個人アカウント名を保存する。

【００４２】

個人用アクセス権限情報欄１８２３は、個人ファイル管理システム１２０上で複数のアカウントが該ファイルにアクセスする場合に、アカウント毎にファイルへのアクセス権限を示す個人用アクセス権限情報を保存する。個人用アクセス権限情報欄１８２３は、図７に示すように、アカウント名欄１８２３Ａと権限情報欄１８２３Ｂを有している。アカウント名欄１８２３Ａに保存されるアカウント名毎に、ファイルへの参照権限があるか、更新権限があるかを示す情報が権限情報欄１８２３Ｂ保存される。権限情報欄１８２３Ｂには、例えば、図７に示すように、“リード／ライト”、“リード・オンリー”などが保存される。“リード／ライト”は、参照・更新権限があることを示し、“リード・オンリー

”の場合、参照権限のみあることを示している。

【００４３】

個人用時刻情報欄１８２４は、ファイルを作成した時刻、更新した時刻等の個人用時刻情報を保存する。個人用時刻情報欄１８２４は、図８に示すように、作成時刻欄１８２４Ａ、アクセス時刻欄１８２４Ｂ及び更新時刻欄１８２４Ｃを有している。作成時刻欄１８２４Ａは、ファイルを作成した時刻を保存する欄である。アクセス時刻欄１８２４Ｂは、作成したファイルに最後にアクセスのあった時刻を保存する欄である。更新時刻欄１８２４Ｃは、作成したファイルを更新した時刻を保存する欄である。

【００４４】

なお、例えば、オンライン・ファイル・ストレージがインターネット１０上で１台しかない場合のような個人用時刻情報をプライバシ情報として管理する必要がない場合は、ファイル管理テーブル１８０で個人用時刻情報を管理せず、そのオンライン・ファイル・ストレージがファイル毎に管理する時刻情報を使用するようにしても良い。しかし、オンライン・ファイル・ストレージが複数存在し、オンライン・ファイル・ストレージ毎にタイムゾーンが異なる場合や時刻がずれている場合など、オンライン・ファイル・ストレージ間で時刻を一致させることが困難な場合は、個人ファイル管理システム１２０側のファイル管理テーブル１８０でファイル毎の時刻情報を管理する。

【００４５】

次に、格納用管理情報について説明する。格納用管理情報を保存する格納用管理情報欄１８３は、ストレージ識別子欄１８３１、ストレージ・パス名欄１８３２、ストレージ・アカウント名欄１８３３、ストレージ用アクセス権限情報欄１８３４、暗号鍵欄１８３５を有している。

【００４６】

ストレージ識別子欄１８３１は、ファイルを格納したオンライン・ファイル・ストレージのストレージ識別子を保存する。ストレージ・パス名欄１８３２は、オンライン・ファイル・ストレージ内にファイルを格納する際に、オンライン・ファイル・ストレージが管理するファイルの名前空間で該ファイルを識別するためのストレージ・パス名を保存する。この情報は、ディレクトリ階層とファイル名から成る。なお、パス名ではなく、ＩＤでファイルを格納するようなオンライン・ファイル・ストレージの場合は、ＩＤを利用する。ストレージ・アカウント名欄１８３３は、ファイルをオンライン・ファイル・ストレージに格納する際に利用したアカウント名を保存する。このアカウント名は、オンライン・ファイル・ストレージ内では該ファイルの作成者に対応する。ストレージ用アクセス権限情報欄１８３４は、格納ファイル毎に関するアクセス権限情報を保存する。個人ファイル管理システム１２０は、ファイル共有時に、該ファイルに対してどのストレージ・アカウントがアクセス可能かを決定し、そのアクセス権限情報をオンライン・ファイル・ストレージに設定する。その際、設定情報を個人ファイル管理システム１２０側で記憶する目的で、ストレージ用アクセス権限情報を管理する。そのため、記憶する必要がなければ、この情報は必要ない。暗号鍵欄１８３５は、ファイルを暗号化してオンライン・ファイル・ストレージに格納する際に利用する暗号鍵を保存する。

【００４７】

次に、共有管理情報について説明する。共有管理情報を管理する共有管理情報欄１８４は、共有フラグ欄１８４１、共有先エントリ番号欄１８４２、ファイル種別欄１８４３を有している。

【００４８】

共有フラグ欄１８４１は、該ファイルが共有中か否かを示す共有フラグを保存する。例えば、共有フラグが“ＯＮ”の場合は共有中であることを示し、“ＯＦＦ”の場合は非共有であることを示す。共有先エントリ番号欄１８４２は、オリジナル・ファイルのコピーを管理するファイル管理テーブル１８０内のエントリ番号を保存する。本実施形態では、ファイルを共有する場合、オリジナル・ファイルのコピーを、オリジナル・ファイルが格納されているオンライン・ファイル・ストレージとは別のオンライン・ファイル・ストレ

ージに、オリジナル・ファイル作成時のアカウントとは別のアカウントで作成する。そしてコピー・ファイルの所在を他者に教えることで、オリジナル・ファイルの所有者に関する情報を他者から隠蔽し、プライバシを保護する。ファイル種別欄１８４３は、オリジナル・ファイルかコピー・ファイルかの違いを示すファイル種別を保存する。ファイル種別として例えば、“ＯＲＩＧ”，“ＣＯＰＹ”が保存される。“ＯＲＩＧ”が保存されている場合は、当該ファイルがオリジナル・ファイルであることを示している。また、“ＣＯＰＹ”が場合されている場合は、当該ファイルがコピー・ファイルであることを示している。コピー・ファイルの場合、ファイル管理テーブル１８０内のプライバシ情報はオリジナル・ファイルの情報と共有するため、エントリの内容は無効（Ｎ／Ａ）になる。

【００４９】

ファイル管理テーブル１８０には、例えば図６から図８に示すように、エントリ番号欄１８１に“００１”、個人パス名欄１８２１に“／ＤＩＲ１／ＦＩＬＥＡ”、個人アカウント名欄１８２２に“ＵＳＥＲ１”、個人用アクセス権限情報欄１８２３に“ＵＳＥＲ１：Ｒｅａｄ／Ｗｒｉｔｅ”、個人用時刻情報欄１８２４に“２００７／０７／０７”等、ストレージ識別子欄１８３１に“ＳＴＲ１”、ストレージ・パス名欄１８３２に“／ＡＢＣ／ＦＩＬＥ＿Ｘ”、ストレージ・アカウント名欄に“ＡＣＮ１”ストレージ用アクセス権限情報欄１８３４に、“データなし”、暗号鍵欄１８３５３に“Ｋｅｙ１”、共有フラグ欄１８４１に“ＯＮ”、共有先エントリ番号欄１８４２に“００３”、ファイル種別欄１８４３に“ＯＲＩＧ”が保存される。

【００５０】

図９は、匿名化契機テーブル１９０の一例を示す図である。匿名化契機テーブル１９０は、匿名化支援機能部１５０を実行させる契機が設定されるテーブルである。匿名化契機テーブル１９０は、契機種別欄１９１、次回契機欄１９２、時間間隔欄１９３を有している。契機種別欄１９１は、匿名化支援機能部１５０を実行させる契機の種別が保存される。この契機種別として、アクセス履歴匿名化契機欄１９４、ごみファイル作成契機欄１９５、パスワード変更契機欄１９６を有している。アクセス履歴匿名化契機欄１９４、ごみファイル作成契機欄１９５、パスワード変更契機欄１９６にはそれぞれ、アクセス履歴を匿名化する契機、ダミーファイルを作成する契機、パスワードを変更する契機を設定する。このようにアクセス履歴の匿名化、ダミーファイルの作成、パスワードの変更を匿名化契機テーブル１９０に設定された契機に実行することによりプライバシ保護ファイル共有システム１において匿名性を高める処理を行うことができる。次回契機欄１９２は、契機種別毎に匿名化処理を行う次回時刻を保存する。時間間隔欄１９３は、匿名化処理の頻度を示す。時間間隔がランダムの場合、匿名化契機をランダムに決定する。時間間隔が一日毎の場合、一日に一回、匿名化処理を行う。

【００５１】

匿名化契機テーブル１９０には、例えば、図９に示すように、契機種別欄１９１に“アクセス履歴匿名化契機”、次回契機欄１９２に“２００７／７／１７　１０：００ＡＭ”、時間間隔欄１９３に“ランダム”が保存される。

【００５２】

次に、オンライン・ファイル・ストレージ３００に保存されるストレージ・アカウント管理テーブル３２０及びファイル・システム管理情報テーブル３３０について説明する。

【００５３】

図１０は、ストレージ・アカウント管理テーブル３２０の一例を示す図である。ストレージ・アカウント管理テーブル３２０は、アカウント名欄３２１、パスワード欄３２２、パスワード期限欄３２３を有している。アカウント名欄３２１、パスワード欄３２２、パスワード期限欄３２３に保存される内容は、個人アカウント管理テーブル１６０と同様であるため、説明を省略する。

【００５４】

図１１は、ファイル・システム管理情報テーブル３３０の一例を示す図である。ファイル・システム管理情報テーブル３３０は、ファイルをボリューム３４０内に格納する際に

必要な管理情報と、ファイルを検索する際に利用するファイルの内容について説明した説明情報を有する。

【００５５】

ファイル・システム管理情報テーブル３３０は、ストレージ・パス名欄３３１、ストレージ・アカウント名欄３３２、ストレージ側アクセス権限情報欄３３３、ストレージ側時刻情報欄３３４、アイノード情報欄３３５、説明情報へのポインタ欄３３６を有している。これら管理情報は、格納しているファイル毎にファイル・システム管理情報テーブル３３０のエントリが存在する。

【００５６】

ストレージ・パス名欄３３１は、オンライン・ファイル・ストレージ内に格納したファイルのストレージ・パス名を保存する。ストレージ・アカウント名欄３３２は、そのファイルを作成したときに使ったストレージ・アカウント名を保存する。そのストレージ・アカウント名は、そのファイルの所有者に対応する。ストレージ側時刻情報欄３３３は、ファイルの作成時刻、ファイルのアクセス時刻、及びファイルの更新時刻を保存する。この保存される時刻は、オンライン・ファイル・ストレージが管理するタイマー（図示しない。）に基づいている。ストレージ側時刻情報欄３３４には、上記個人用時刻情報欄１８２４と同様の内容が保存されるため、説明は省略する。アイノード情報欄３３５は、ファイルがボリューム３４０上のどこに物理的に配置したか位置情報を管理するためのアイノード情報を保存する。説明情報へのポインタ欄３３６は、該ファイルの内容について記述した説明情報のパス名を示すポイントを保存する。なお、説明情報は、例えばテキストデータにより構成される。

【００５７】

次に、図１２から図２４を参照して、初期化部１３０、要求処理部１４０に要求をする際の要求フォーマット、及び要求処理部１４０からオンライン・ファイル・ストレージへ要求をする際の要求フォーマットについて説明する。

【００５８】

図１２は、アプリケーション１１０もしくはユーザが個人ファイル管理システム１２０に対して、ファイル・システムを作成する指示を行う場合の初期化要求情報の一例を示す図である。

【００５９】

図１２に示すように、初期化要求情報１３１は、要求種別１３２、オンライン・ファイル・ストレージ・リスト１３３、ストレージ・アカウント数１３４を有する。要求種別１３２が“初期化”の場合に、初期化部１３０の処理が実行される。オンライン・ファイル・ストレージ・リスト１３３は、作成するファイル・システムが利用するオンライン・ファイル・ストレージ群を指示する。利用するオンライン・ファイル・ストレージは、ストレージ識別子のリスト（例えば、ＳＴＲ１～ＳＴＲ３）で指示する。個人ファイル管理システム１２０は、ファイル作成時に、ファイルが指定されたオンライン・ファイル・ストレージ間で分散するよう格納先を決定する。ストレージ・アカウント数１３４は、各オンライン・ファイル・ストレージ３００，４００で作成するアカウント数を指示する。ストレージ・アカウント数が１０の場合、新規ファイル作成時に利用するストレージ・アカウントは、作成した１０個のストレージ・アカウントの中から決定する。

【００６０】

図１３は、アプリケーション１１０が個人ファイル管理システム１２０に対してファイル作成を要求する場合の要求フォーマット１４１の一例を示す図である。

【００６１】

図１３に示すように、要求フォーマット１４１は、要求種別１４２、個人パス名１４３、個人アカウント名１４４、データ・サイズ１４５、データへのポインタ１４６を有している。要求種別１４２は、“ファイル作成”となっている。個人パス名１４３は、個人ファイル管理システム１２０が管理する名前空間内で作成するファイルのパス名を指定する。個人アカウント名１４４は、どの個人アカウントでファイルを作成するかを指定する。

データ・サイズ１４５は、データのサイズである。データへのポインタ１４６は、作成するファイル内のデータを格納しているＰＣ１００のメモリ１０２内のアドレスを示す。

【００６２】

図１４は、個人ファイル管理システム１２０からオンライン・ファイル・ストレージに対してファイル作成を要求する場合の要求フォーマット５００の一例を示す図である。

【００６３】

図１４に示すように、要求フォーマット５００は、要求種別５０１、ストレージ・パス名５０２、ストレージ・アカウント名５０３、データ・サイズ５０４、データ５０５を有している。要求種別５０１は、“ファイル作成”となっている。また、データ・サイズ５０４、データ５０５は、個人ファイル管理システム１２０に対するファイル作成要求で指示されたものが指定される。なお、ストレージ・パス名５０２、ストレージ・アカウント名５０３については上記の説明と同様であるため、説明を省略する。

【００６４】

図１５は、アプリケーション１１０が個人ファイル管理システム１２０に対してファイル参照を要求する場合の要求フォーマット５１０の一例を示す図である。

【００６５】

要求フォーマット５１０は、要求種別５１１、個人パス名５１２、個人アカウント名５１３を有している。要求種別５１１は、“ファイル参照”となっている。個人パス名５１２は、個人ファイル管理システム１２０が管理する名前空間内のパス名を指定する。個人アカウント名５１３は、どの個人アカウントでファイルを参照するかを指定する。

【００６６】

図１６は、個人ファイル管理システム１２０からオンライン・ファイル・ストレージに対してファイル参照の要求をする場合の要求フォーマット５２０の一例を示す図である。

【００６７】

要求フォーマット５０２は、要求種別５２１、ストレージ・パス名５２２、ストレージ・アカウント名５２３を有している。要求種別５２１は、“ファイル参照”となっている。なお、ストレージ・パス名５２２、ストレージ・アカウント名５２３については上記の説明と同様であるため、説明を省略する。

【００６８】

図１７は、アプリケーション１１０が個人ファイル管理システム１２０に対してファイル更新を要求する場合の要求フォーマット５３０の一例を示す図である。

【００６９】

要求フォーマット５３０は、要求種別５３１、個人パス名５３２、個人アカウント名５３３、オフセット５３４、サイズ５３５、データへのポインタ５３６を有している。要求種別５３１は、“ファイル更新”となっている。個人パス名５３２は、個人ファイル管理システム１２０が管理する名前空間内のパス名を指定する。個人アカウント名５３３は、どの個人アカウントでファイルを参照するかを指定する。オフセット５３４とサイズ５３５は、ファイルの先頭からどの位置のデータを更新するかを指定する。データへのポインタ５３６は、作成するファイル内のデータを格納しているＰＣ１００のメモリ１０２内のアドレスを示す。

【００７０】

図１８は、個人ファイル管理システム１２０からオンライン・ファイル・ストレージに対してファイル更新を要求する場合の要求フォーマット５４０の一例を示す図である。

【００７１】

図１８に示すように、更新フォーマット５４０は、要求種別５４１、ストレージ・パス名５４２、ストレージ・アカウント名５４３、オフセット５４４、サイズ５４５、データ５４６を有している。要求種別５４１は、“ファイル更新”となっている。なお、ストレージ・パス名５４２、ストレージ・アカウント名５４３、オフセット５４４、サイズ５４５については上記の説明と同様であるため、説明を省略する。データ５４５は、ファイルの内容である。

【００７２】
図１９は、アプリケーション１１０が個人ファイル管理システム１２０に対してファイル削除を要求する場合の要求フォーマット５５０の一例を示す図である。
【００７３】
図１９に示すように、要求フォーマット５５０は、要求種別５５１、個人パス名５５２、個人アカウント名５５３を有している。要求種別５５１は“ファイル削除”となっている。個人パス名５５２は、個人ファイル管理システム１２０が管理する名前空間内のパス名を指定する。個人アカウント名５５３は、どの個人アカウントでファイルを参照するかを指定する。
【００７４】
図２０は、個人ファイル管理システム１２０からオンライン・ファイル・ストレージに対してファイル削除を要求する場合の要求フォーマット５６０の一例を示す図である。
【００７５】
図２０に示すように、要求フォーマット５６０、要求種別５６１、ストレージ・パス名５６２、ストレージ・アカウント名５６３を有している。要求種別５６１は“ファイル削除”となっている。ストレージ・パス名５６２、ストレージ・アカウント名５６３については上記の説明と同様であるため、説明を省略する。
【００７６】
次に、要求処理部１４０にファイルの共有及び検索を要求したときの処理の概要について説明する。図２１は、この処理の概要を説明するための図である。この図２１においては、ファイルを共有するためのオンライン・ファイル・ストレージをオンライン・ファイル・ストレージ０１，０２、アプリケーション、個人ファイル管理システムをそれぞれアプリケーション１，２、個人ファイル管理システムＰ１，Ｐ２とした場合で説明する。なお、例えば図１に示す構成と対応させれば、アプリケーション０１はアプリケーション１１０、アプリケーション０２はアプリケーション２１０、個人ファイル管理システムＰ１は個人ファイル管理システム１２０、個人ファイル管理システムＰ２は個人ファイル管理システム２２０に対応する。
【００７７】
先ず、アプリケーション１から個人ファイル管理システムＰ１へ共有要求をする場合を説明する。この共有要求には、例えば、個人パス名Ｎ１、個人アカウントＵ１、ストレージ識別子０２、説明情報Ｄ１が含まれる。次に個人ファイル管理システムＰ１は、オンライン・ファイル・ストレージ０１からストレージ・パス名Ｎ２、ストレージ・アカウントＵ２、ファイルをリードする。次に個人ファイル管理システムＰ１は、オンライン・ファイル・ストレージ０２に、ストレージ・パス名Ｎ３、ストレージ・アカウントＵ３を用いて共有ファイルを作成する。次に個人ファイル管理システムＰ１は、ストレージ・パス名Ｎ３を用いて説明情報Ｄ１をオンライン・ファイル・ストレージ０２に追加する。この４つの処理（図２１において丸数字１から４に対応）により、オンライン・ファイル・ストレージ０１内の共有元ファイル（ストレージ・パス名Ｎ２）をオンライン・ファイル・ストレージ０２内の共有先ファイル（ストレージ・パス名Ｎ３）と共有させることができる。
【００７８】
次に、アプリケーション２から個人ファイル管理システムＰ２へファイルの検索を要求する場合を説明する。この検索要求には、例えば、検索キーワード、個人アカウントＵ４が含まれる。次に個人ファイル管理システムＰ２は、ストレージ・アカウントＵ５、検索キーワードを用いてオンライン・ファイル・ストレージ０２内を検索する。次に個人ファイル管理システムＰ２は、オンライン・ファイル・ストレージ０２から検索結果、ストレージ・パス名Ｎ３、説明情報Ｄ１を受け取る。そして、個人ファイル管理システムＰ２は、検索結果、個人パス名Ｎ４、説明情報Ｄ１をアプリケーション２へ出力する。この４つの処理（図２１において丸数字５から８に対応）により、検索結果がアプリケーション２に出力される。

【００７９】
図２２は、アプリケーション１１０から個人ファイル管理システム１２０にファイル共有を要求する場合の要求フォーマット５７０の一例を示す図である。
【００８０】
図２２に示すように、要求フォーマット５７０は、要求種別５７１、個人パス名５７２、個人アカウント名５７３、共有ストレージ識別子５７４、説明情報５７５を有している。要求種別５７１は“ファイル共有要求”となっている。個人パス名５７２は、個人ファイル管理システム１２０が管理する名前空間内のパス名を指定する。個人アカウント名５７３は、どの個人アカウントでファイル共有要求を行うかを指定する。共有ストレージ識別子５７４は、共有するファイルのコピーをどのオンライン・ファイル・ストレージ（共有先オンライン・ファイル・ストレージと称する。一方、オリジナル・ファイルを格納する方を共有元オンライン・ファイル・ストレージ３００と称する。）に作成するかを決定する。説明情報５７５は、共有するファイルの内容を説明する情報を指定する情報である。
【００８１】
図２３は、アプリケーション２１０が個人ファイル管理システム２２０に対してファイル検索を要求する場合の要求フォーマット５８０の一例を示す図である。
【００８２】
図２３に示すように、要求フォーマット５８０は、要求種別５８１、個人アカウント名５８２、検索キーワード５８３を有している。要求種別５８１は“ファイル検索”となっている。個人アカウント名５８２は、検索結果のファイルに対してファイル管理テーブル１８０内で新規エントリを割り当てるときに設定する個人アカウント名である。検索キーワード５８３は、任意の文字列であり、その文字列を含む説明情報に対応するファイルを検索するために用いられる。
【００８３】
図２４は、アプリケーション１１０が個人ファイル管理システム１２０に対してアカウント管理を要求する場合の要求フォーマット５９０の一例を示す図である。
【００８４】
図２４に示すように、要求フォーマット５９０は、要求種別５９１、個人アカウント名５９２、新パスワード５９３、ストレージ・アカウント連携５９４を有している。要求種別５９１は“アカウント作成ｏｒアカウント削除ｏｒパスワード変更”となっている。すなわち、アカウント作成、アカウント削除、パスワード変更のいずれかが要求種別となる。アカウント作成は、新しい個人アカウントを作成する要求であり、アカウント削除は既存の個人アカウントを削除する要求であり、パスワード変更は既存の個人アカウントのパスワードを変更する要求である。個人アカウント名５９２は、処理対象の個人アカウント名を示す。新パスワード５９３はアカウント作成時とパスワード変更時のみに利用する。ストレージ・アカウント連携５９４は、アカウント作成時には、個人アカウント作成と合わせてストレージ・アカウントも作成し、パスワード変更時には、個人アカウントのパスワード変更と合わせてストレージ・アカウントのパスワードも変更する際に利用するフラグである。
【００８５】
次に、個人ファイル管理システム１２０の初期化部１３０の実行する処理について説明する。図２５は、初期化部１３０で実行される処理を示すフローチャートである。
【００８６】
初期化部１３０は、図１２を参照して説明した初期化要求１３１をアプリケーション１１０から受領すると（Ｓ１０１）、ファイル管理テーブル１８０の初期化を行なう（Ｓ１０２）。この初期化は、具体的には、ファイル管理テーブル１８０の全エントリをクリアする。続いて、初期化部１３０は、個人アカウント管理テーブル１６０を初期化し（Ｓ１０３）、ストレージ管理テーブル１７０を初期化する（Ｓ１０４）。そして、初期化部１３０は、初期化要求のオンライン・ファイル・ストレージ・リスト１３３で指示された各

オンライン・ファイル・ストレージに対して、初期化要求のストレージ・アカウント数１３４分のストレージ・アカウント名をランダムに作成する（Ｓ１０５）。作成後、初期化部１３０は、ストレージ管理テーブル１７０に作成したストレージ・アカウントの情報を登録する（Ｓ１０６）。以上で、初期化部１３０の処理が完了する。

【００８７】

なお、図２５には図示していないが、ファイル・システムを削除する場合、ファイル管理テーブル１８０で管理する全ファイルについて、オンライン・ファイル・ストレージから対応ファイルを削除し、次にストレージ管理テーブル１７０を参照し、全ストレージ・アカウントの削除を行い、最後にファイル管理テーブル１８０、個人アカウント管理テーブル１６０及び、ストレージ管理テーブル１７０の内容をクリアする。以上により、ファイル・システムの削除が完了する。

【００８８】

次に、個人ファイル管理システム１２０の要求処理部１４０の実行する処理について説明する。図２６は、要求処理部１４０で実行される処理を示すフローチャートである。

【００８９】

要求処理部１４０は、図１３で説明したファイルの作成要求、図１５で説明したファイルの参照要求、図１７で説明したファイルの更新要求、図１９で説明したファイル削除の要求、図２２で説明したファイルの共有要求、図２３で説明したファイルの検索要求、図２４で説明したアカウント管理要求などの要求をアプリケーション１１０から受領すると（Ｓ２０１）、要求種別について判定する（Ｓ２０２）。この判定は、受領した要求の要求フォーマットの要求種別の設定に基づいて判定される。

【００９０】

ステップＳ２０２で要求種別がファイル作成であると判定すれば、要求処理部１４０は、ファイル作成処理を実行する（Ｓ２０３）。ステップＳ２０２で要求種別がファイル参照であると判定すれば、要求処理部１４０は、ファイル参照処理を実行する（Ｓ２０４）。ステップＳ２０２で要求種別がファイル更新であると判定すれば、要求処理部１４０は、ファイル更新処理を実行する（Ｓ２０５）。ステップＳ２０２で要求種別がファイル削除であると判定すれば、要求処理部１４０は、ファイル削除処理を実行する（Ｓ２０６）。ステップＳ２０２で要求種別がファイル共有であると判定すれば、要求処理部１４０は、ファイル共有処理を実行する（Ｓ２０７）。ステップＳ２０２で要求種別がファイル非共有であると判定すれば、要求処理部１４０は、ファイル非共有処理を実行する（Ｓ２０８）。ステップＳ２０２で要求種別がファイル検索であると判定すれば、要求処理部１４０は、ファイル検索処理を実行する（Ｓ２０９）。ステップＳ２０２で要求種別がアカウント管理であると判定すれば、要求処理部１４０は、アカウント管理処理を実行する（Ｓ２１０）。

【００９１】

このようにステップＳ２０２の判定に応じたいずれかの処理が終了すると、この処理が完了する。なお、ファイル作成処理（Ｓ２０３）、ファイル参照処理（Ｓ２０４）、ファイル更新処理（Ｓ２０５）、ファイル削除処理（Ｓ２０６）、ファイル共有処理（Ｓ２０７）、ファイル検索処理（Ｓ２０９）、アカウント管理処理（Ｓ２１０）の各処理については、詳細を図２７から図３３を参照しながら詳細に説明する。

【００９２】

先ず、要求処理部１４０の実行するファイル作成処理について説明する。図２７は、ファイル作成処理を示すフローチャートである。このファイル作成処理では、要求処理部１４０は、ファイル管理テーブル１８０に新規エントリを作成し、新規エントリでプライバシ情報を管理し、オンライン・ファイル・ストレージ３００にファイルを作成する。

【００９３】

要求処理部１４０は、ファイル管理テーブル１８０に新規エントリを作成する（Ｓ３０１）。そして、要求処理部１４０はファイル管理テーブル１８０に情報を設定する。詳細には、要求処理部１４０はファイル管理テーブル１８０の個人パス名欄１８２１と個人ア

カウント名欄１８２２には、ファイル作成要求に指示された情報を設定する。要求処理部１４０は個人用アクセス権限情報欄１８２３には、ファイルが属するディレクトリ毎に設定されたアクセス権限の設定ポリシーに従って設定する。例えば所有者のみリード／ライト可能であり、他のアカウントではリード・オンリーに設定するなどである。要求処理部１４０は個人用時刻情報欄１８２４には、個人ファイル管理システム１２０のタイマー（図示しない。）を参照し、現在の時刻を設定する。ファイル作成時においては、ファイル共有はしないため、共有フラグ欄１８４１は“ＯＦＦ”、共有先エントリ番号欄１８４２は“Ｎ／Ａ”、ファイル種別欄１８４３は“ＯＲＩＧ”に設定する。また、要求処理部１４０はデータを暗号化して格納する場合は、暗号鍵を決定し、ファイル管理テーブル１８０のエントリの暗号鍵欄１８３５にその決定した暗号鍵を設定する（Ｓ３０２）。

【００９４】

次に、要求処理部１４０は、ストレージ管理テーブル１７０の利用ファイル数欄１７５を参照し、一番数が小さいエントリを見つける。これにより、ファイルを作成するオンライン・ファイル・ストレージのストレージ識別子とファイル作成時に利用するストレージ・アカウント名が決定する（Ｓ３０３）。なお、複数の異なる個人アカウントが、同一のストレージ・アカウントを使ってそれぞれファイルを作成する実施形態もあり得る。

【００９５】

次に、要求処理部１４０は、ランダムにストレージ・パス名を決定する。その際、オンライン・ファイル・ストレージ３００内に同一のストレージ・パス名が存在するかどうかをチェックし、ユニークなストレージ・パス名を決定する（Ｓ３０４）。

【００９６】

次に、要求処理部１４０は、ファイル管理テーブル１８０に、決定したストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を設定する（Ｓ３０５）。なお、ストレージ用アクセス権限情報は、必要があれば、ファイル共有時に設定する。

【００９７】

次に、要求処理部１４０は、オンライン・ファイル・ストレージに決定したストレージ・アカウント名と対応するパスワードを使ってログインし、決定したパス名のファイルを作成する（Ｓ３０６）。なお、オンライン・ファイル・ストレージに対するファイル作成要求の要求フォーマット５００の一例は、図１４を用いて既述している。そして、要求処理部１４０は、要求元のアプリケーション１１０に、ファイル作成が完了したことを応答する（Ｓ３０７）。これにより、ファイル作成処理が完了する。

【００９８】

次に要求処理部１４０の実行するファイル参照処理について説明する。図２８は、ファイル参照処理を示すフローチャートである。このファイル参照処理では、要求処理部１４０は、ファイル管理テーブル１８０から要求があった個人パス名に対応するオンライン・ファイル・ストレージ内のファイルを特定し、該ファイルをオンライン・ファイル・ストレージから読み出した後に、リードしたファイルをアプリケーション１１０に返すことを行う。

【００９９】

先ず、要求処理部１４０は、ファイル管理テーブル１８０の各エントリを検索し、指定された個人パス名と一致するエントリを見つける（Ｓ４０１）。そして、要求処理部１４０は、ファイル管理テーブル１８０の個人用アクセス権限情報欄１８２３を参照し、指定されたアカウントが該ファイルの参照をする権限があるか否かを判定する（Ｓ４０２）。ステップＳ４０２で参照する権限がないと判定した場合は、要求処理部１４０は、要求元のアプリケーション１１０にアクセス権エラーを返して処理を完了する（Ｓ４０３）。

【０１００】

一方、ステップＳ４０２で参照する権限があると判定した場合は、要求処理部１４０は、ファイル管理テーブル１８０のエントリから、該個人パス名に対応するストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を決定する（Ｓ４０４）。そして、要求処理部１４０は、決定したストレージ識別子に対応するオンライン・ファイル・スト

レージに対して、決定したストレージ・アカウント名と対応するパスワードを使ってログインし、決定したストレージ・パス名に対応するファイルをリードする（Ｓ４０５）。なお、オンライン・ファイル・ストレージに対するファイル参照要求の要求フォーマット５２０の一例は、図１６を用いて既述している。

【０１０１】

次に、要求処理部１４０は、ファイル管理テーブル１８０の個人用時刻情報欄１８２４のアクセス時刻を更新し（Ｓ４０６）、リードしたファイルをアプリケーション１１０に返して処理を完了する（Ｓ４０７）。これにより、ファイル参照処理が完了する。

【０１０２】

次に要求処理部１４０の実行するファイル更新処理について説明する。図２９は、ファイル更新処理を示すフローチャートである。このファイル更新処理では、要求処理部１４０は、ファイル管理テーブル１８０から要求があった個人パス名に対応するオンライン・ファイル・ストレージ内のファイルを特定し、更新データでオンライン・ファイル・ストレージ内の該ファイルを更新する処理を行う。

【０１０３】

先ず、要求処理部１４０は、ファイル管理テーブル１８０の各エントリを検索し、指定された個人パス名と一致するエントリを見つける（Ｓ５０１）。そして、要求処理部１４０は、ファイル管理テーブル１８０の個人用アクセス権限情報欄１８２３を参照し、指定されたアカウントが該ファイルを更新する権限を有するか否かを判定する（Ｓ５０２）。ステップＳ５０２で権限がないと判定した場合は、要求処理部１４０は、要求元のアプリケーション１１０にアクセス権エラーを返して処理を完了する（Ｓ５０３）。

【０１０４】

一方、ステップＳ５０２で権限があると判定した場合は、要求処理部１４０は、ファイル管理テーブル１８０のエントリから、該個人パス名に対応するストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を決定する（Ｓ５０４）。

【０１０５】

そして、要求処理部１４０は、決定したストレージ識別子に対応するオンライン・ファイル・ストレージに対して、決定したストレージ・アカウント名と対応するパスワードを使ってログインし、決定したストレージ・パス名に対応するファイルを指定されたデータで更新する（Ｓ５０５）。なお、オンライン・ファイル・ストレージに対するファイル更新要求の要求フォーマット５４０の一例は、図１８を用いて既述している。

【０１０６】

次に、要求処理部１４０は、ファイル管理テーブル１８０の個人用時刻情報欄１８２４のアクセス時刻と更新時刻を更新し（Ｓ５０６）、要求元のアプリケーション１１０に応答する（Ｓ５０７）。これにより、ファイルの更新処理が完了する。

【０１０７】

次に、要求処理部１４０の実行するファイル削除処理について説明する。図３０は、ファイル削除処理を示すフローチャートである。このファイル削除処理では、要求処理部１４０は、ファイル管理テーブル１８０から要求があった個人パス名に対応するオンライン・ファイル・ストレージ内のファイルを特定し、該ファイルをオンライン・ファイル・ストレージから削除した後に、ファイル管理テーブル１８０のエントリも削除する。なお、ファイル共有中の場合、削除するオリジナル・ファイルのコピー・ファイルも合わせて削除するため、本処理を再帰的に呼び出すこととする。

【０１０８】

先ず、要求処理部１４０は、ファイル管理テーブル１８０の各エントリを検索し、指定された個人パス名と一致するエントリを見つける（Ｓ６０１）。そして、要求処理部１４０は、ファイル管理テーブル１８０の個人アカウント名欄１８２２を参照し、指定されたアカウントが削除対象の所有者かどうかを判定する（Ｓ６０２）。ステップＳ６０２で所有者でないと判定した場合は、要求処理部１４０は、要求元のアプリケーション１１０にアクセス権エラーを返して処理を完了する（Ｓ６０３）。

【０１０９】
一方、ステップＳ６０２で所有者であると判定した場合は、要求処理部１４０は、ファイル管理テーブル１８０の共有フラグ欄１８４１を参照し、該ファイルが共有中かどうかを判定する（Ｓ６０４）。ステップＳ６０４で共有中であると判定した場合、要求処理部１４０は、ファイル管理テーブル１８０から該ファイルのコピー・ファイルを特定し、そのファイルを削除するために、ファイル削除処理を再帰的に実行する（Ｓ６０５）。
【０１１０】
次に、ステップＳ６０２で共有中でないと判定した場合、又は、ステップＳ６０５で共有中のファイルを削除した場合、要求処理部１４０は、ファイル管理テーブル１８０から個人パス名に対応するストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を決定する（Ｓ６０６）。
【０１１１】
そして、要求処理部１４０は、決定したストレージ識別子に対応するオンライン・ファイル・ストレージに対して、決定したストレージ・アカウント名と対応するパスワードを使ってログインし、決定したストレージ・パス名に対応するファイルを削除する（Ｓ６０７）。なお、オンライン・ファイル・ストレージに対するファイル削除要求の要求フォーマット５６０の一例は、図２０を用いて既述している。
【０１１２】
そして、要求処理部１４０は、ファイル管理テーブル１８０から、削除ファイルに対応するエントリを削除し（Ｓ６０８）、要求元のアプリケーション１１０に応答する（Ｓ６０９）。これにより、ファイル削除処理が処理する。
【０１１３】
次に、要求処理部１４０の実行するファイル共有処理について説明する。図３１は、ファイル共有処理を示すフローチャートである。このファイル共有処理では、要求処理部１４０は、ファイル管理テーブル１８０から要求があった個人パス名に対応するオンライン・ファイル・ストレージ内のファイルを特定し、該ファイルのコピーを説明情報と共に指定されたオンライン・ファイル・ストレージ内に作成し、ファイル管理テーブル１８０でオリジナルとコピーの関係を管理する処理を行う。なお、図３１は、図２１を参照して概略的に説明したファイル共有処理の詳細を示すものである。
【０１１４】
先ず、要求処理部１４０は、ファイル管理テーブル１８０の各エントリを検索し、指定された個人パス名（図２１では“個人パス名Ｎ１”）と一致するエントリを見つける（Ｓ７０１）。そして、要求処理部１４０は、ファイル管理テーブル１８０の個人アカウント名欄１８２２を参照し、指定されたアカウント（図２１では“個人アカウントＵ１”）が共有対象の所有者かどうかを判定する（Ｓ７０２）。ステップＳ７０２で共有対象の所有者でないと判定した場合は、要求処理部１４０は、要求元のアプリケーション１１０にアクセス権エラーを返して処理を完了する（Ｓ７０３）。
【０１１５】
一方、ステップＳ７０２で共有対象の所有者であると判定した場合は、要求処理部１４０は、ファイル管理テーブル１８０にファイル種別欄１８４３が“ＣＯＰＹ”となる新規エントリを作成する。この際、個人パス名欄１８２１と個人アカウント名欄１８２２は“Ｎ／Ａ”を設定する（Ｓ７０４）。
【０１１６】
そして、要求処理部１４０は、共有するファイルに対応するファイル管理テーブル１８０のエントリに関し、共有フラグ欄１８４１を“ＯＮ”に設定し、共有先エントリ番号欄１８４２を新規エントリの番号に設定し、共有元ファイルの共有管理情報を更新する（Ｓ７０５）。
【０１１７】
次に、要求処理部１４０は、コピー・ファイル用のストレージ・パス名（図２１では“Ｎ２”）を共有先オンライン・ファイル・ストレージ（図２１では、“オンライン・ファ

イル・ストレージ０２”）内でユニークになるようランダムに決定する。また、要求処理部１４０は、ストレージ管理テーブル１７０から、共有先オンライン・ファイル・ストレージにコピー・ファイルを作成する際のストレージ・アカウント名（図２１では、“Ｕ２”）を決定する。そして、要求処理部１４０は、ファイル管理テーブル１８０の新規エントリに対して、共有元ファイルのストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を設定する。共有フラグは“ＯＦＦ”、共有先エントリ番号は“Ｎ／Ａ”に設定する（Ｓ７０６）。

【０１１８】

次に、要求処理部１４０はファイル管理テーブル１８０から、共有するファイル（共有元ファイルと呼ぶ）に対応するストレージ識別子、ストレージ・パス名、ストレージ・アカウント名（図２１では、ストレージ識別子０１、ストレージ・パス名Ｎ２、ストレージ・アカウント名Ｕ２）を決定する（Ｓ７０７）。

【０１１９】

次に、要求処理部１４０は、共有元オンライン・ファイル・ストレージ（図２１では、“オンライン・ファイル・ストレージ０１）から共有元ファイルをリードし（Ｓ７０８）、共有先オンライン・ファイル・ストレージにストレージ・アカウント名（図２１では、“Ｕ３”）を使って共有元オンライン・ファイル・ストレージからリードしたファイルをストレージ・パス名（図２１では、“Ｎ３”）で指定される新規ファイルとして作成する（Ｓ７０９）。

【０１２０】

次に、要求処理部１４０は、共有先オンライン・ファイル・ストレージ内のストレージ・パス名（図２１では“N３”）で指定するファイルのストレージ側アクセス権限を、どのストレージ・アカウントからでもアクセス可能になるよう変更する（Ｓ７１０）。ただし、別の実施形態として、特定のストレージ・アカウント群からのみアクセス可能になるよう設定することも考えられる。必要があれば、個人ファイル管理システム１２０のファイル管理テーブル１８０のストレージ用アクセス権限情報欄１８３４に、共有先オンライン・ファイル・ストレージ３００に対して設定した内容を保持する。

【０１２１】

次に、要求処理部１４０は、共有先オンライン・ファイル・ストレージ内の共有先ファイルに対してストレージ・パス名（図２１では、“Ｎ３”）を用いて説明情報Ｄ１を追加する。共有先オンライン・ファイル・ストレージは、説明情報Ｄ１を自身のファイル・システム内に格納し、自身のファイル・システム管理情報でファイルに対応するエントリに説明情報Ｄ１へのポインタを設定する（Ｓ７１１）。これにより、ファイル共有処理が完了する。

【０１２２】

次に、要求処理部１４０の実行するファイル非共有処理について説明する。ファイル非共有処理では、要求処理部１４０は、ファイル管理テーブル１８０から非共有にするファイルの共有管理情報を削除し、また、対応するコピー・ファイルのエントリを削除し、コピーが存在するオンライン・ファイル・ストレージからコピー・ファイルと説明情報を削除することで実現する。

【０１２３】

次に、要求処理部１４０の実行するファイル検索処理について説明する。図３２は、ファイル検索処理を示すフローチャートである。このファイル検索処理では、要求処理部１４０は、個人アカウント名（図２１では“Ｕ４”）及び検索キーワード（例えば、Ｗ１）をアプリケーション２１０から受け付けると、オンライン・ファイル・ストレージから検索キーワードを含むファイルを検索し、検索結果のファイルをファイル管理テーブル１８０に新規ファイルとして登録する処理を行う。

【０１２４】

先ず、要求処理部１４０（図２１では、個人ファイル管理システムＰ２内の要求処理部）は、ストレージ管理テーブル１７０から、検索対象のオンライン・ファイル・ストレー

ジ（図２１では、オンライン・ファイル・ストレージ０２）に対応する任意のストレージ・アカウント名（図２１では“Ｕ５”）を選択する。なお、検索対象のオンライン・ファイル・ストレージが複数ある場合は、各オンライン・ファイル・ストレージに対して以下の処理を繰り返す（Ｓ８０１）。

【０１２５】

次に、要求処理部１４０は、オンライン・ファイル・ストレージに対して、選択したストレージ・アカウント名がアクセス可能なファイル群を対象に、検索キーワード（例えば、“Ｗ１”）を指定して検索要求を行う（Ｓ８０２）。オンライン・ファイル・ストレージ側は、指定されたストレージ・アカウントがアクセス可能なファイル群を対象にそれらに対応する説明情報（図２１では、“Ｄ１”）を検索し、検索キーワードにマッチするファイル群のパス名と対応する説明情報（図２１では、“Ｎ３”と“Ｄ１”）をセットにしてリストとして要求処理部１４０に応答する。

【０１２６】

次に、要求処理部１４０は、検索結果として、ストレージ・パス名と説明情報（図２１では“Ｎ３”と“Ｄ１”）のセットのリストを得る（Ｓ８０３）。

【０１２７】

次に、要求処理部１４０は、得られたストレージ・パス名（Ｎ３）毎に、ファイル管理テーブル１８０に新規エントリを作成し、任意のユニークな個人パス名（Ｎ４）を割り当て設定する。個人アカウント名は、アプリケーション１１０が検索要求で指定した個人アカウント名（図２１では“Ｕ４”）を設定する。個人アクセス情報権限は、ファイル作成時と同様に設定ポリシーに従う。ストレージ識別子欄１８３１、ストレージ・パス名欄１８３２、ストレージ・アカウント名欄１８３３はステップＳ８０１，Ｓ８０３の情報（図２１では、“０２”，“Ｎ３”、“Ｕ５”）を設定する。共有管理情報欄１８４はクリアする。

【０１２８】

次に、要求処理部１４０は、検索結果としてアプリケーション１１０に対して新規に作成した個人パス名と対応する説明情報（“Ｎ４”と“Ｄ１”）をセットにしてリストとして返す（Ｓ８０５）。これにより、ファイル検索処理が完了する。なお、アプリケーション１１０は個人パス名（“Ｎ４”）を指定することで、検索結果のファイルにアクセスできるようになる。

【０１２９】

次に、要求処理部１４０の実行するアカウント管理処理について説明する。図３３は、アカウント管理処理を示すフローチャートである。このアカウント管理処理では、要求処理部１４０は、個人ファイル管理システム１２０に対してアカウントの作成・削除、パスワード変更の要求を処理する。

【０１３０】

先ず、要求処理部１４０は、アカウント管理の要求種別を判定する。要求種別は、図２４で説明した要求フォーマット５９０の要求種別欄５９１に設定されている情報に基づいて判定される（Ｓ９０１）。要求種別が“アカウント作成”であればステップＳ９０２に、“アカウント削除”であればステップＳ９０５に、“パスワード変更”であればステップＳ９０６に進む。

【０１３１】

ステップＳ９０１で要求種別が“アカウント作成”であると判定した場合、要求処理部１４０は、個人アカウント管理テーブル１６０に新規エントリを追加し、アカウント管理要求に指定された個人アカウント名とパスワード、パスワード期限を設定する。パスワード期限は予めシステムで決めておいた期間を設定する（Ｓ９０２）。

【０１３２】

そして、要求処理部１４０は、ストレージ・アカウントも合わせて変更するか否かを判定する（Ｓ９０３）。アカウント管理要求のストレージ・アカウント連携のフラグが“ＯＮ”か“ＯＦＦ”かによって判定される。フラグが“ＯＦＦ”である場合は処理が完了と

なる。

【０１３３】

一方、フラグが“ＯＮ”である場合は、要求処理部１４０は、ストレージ管理テーブル１６０からランダムにオンライン・ファイル・ストレージを選択する。次にそのオンライン・ファイル・ストレージ内でユニークな新規ストレージ・アカウントと、そのアカウント用のパスワードをランダムに決定する。最後に、そのストレージ・アカウントをオンライン・ファイル・ストレージに作成し、ストレージ管理テーブル１６０に新規エントリを追加する（Ｓ９０４）。

【０１３４】

また、ステップＳ９０１で要求種別が“アカウント削除”であると判定した場合、要求処理部１４０は、個人アカウント管理テーブル１６０から指定された個人アカウントのエントリを削除し、処理を完了する。

【０１３５】

一方、ステップＳ９０１で要求種別が“パスワード変更”であると判定した場合、要求処理部１４０は、個人アカウント管理テーブル１６０からアカウント管理要求に指定された個人アカウント名に対応するエントリを検索し、そのパスワードを指定されたパスワードで更新する。また、パスワード期限を新しい値に設定しなおす（Ｓ９０６）。

【０１３６】

次に、要求処理部１４０は、ストレージ・アカウントも合わせて変更するか否かを判定する（Ｓ９０７）。アカウント管理要求のストレージ・アカウント連携のフラグが“ＯＮ”か“ＯＦＦ”かによって判定される。フラグが“ＯＦＦ”である場合は処理が完了となる。

【０１３７】

一方、フラグが“ＯＮ”である場合は、要求処理部１４０は、ファイル管理テーブル１８０を参照し、アカウント管理要求で指定された個人アカウント名で作成した全ファイルをリストアップする。そのリスト内の全ファイルについて、オンライン・ファイル・ストレージに格納する際に利用したストレージ・アカウントをリストアップする。そのリスト内の全ストレージ・アカウントについて、ランダムにパスワードを決定し、オンライン・ファイル・ストレージに対してストレージ・アカウントのパスワード変更を要求する。最後にストレージ管理テーブル１７０のパスワード欄とパスワード期限欄を更新する（Ｓ９０８）。

【０１３８】

次に、匿名化支援機能部１５０の処理について説明する。図３４は、匿名化支援機能部１５０で実行される処理を示すフローチャートである。匿名化支援機能部１５０は、アプリケーション１１０からのファイル・アクセス要求とは無関係にオンライン・ファイル・ストレージ内のファイルにアクセスしたり、ランダムなファイルを作成することで、アクセス履歴に関する匿名性を維持し、ストレージ・アカウントのパスワードを定期的に変更することでパスワードのクラッキングを防止する処理を行う。

【０１３９】

先ず、匿名化支援機能部１５０は、図９を用いて説明した匿名化契機テーブル１９０を参照し、タイマー（図示しない。）から得た現在時刻を比較し、アクセス履歴匿名化契機かどうかを判定する（Ｓ１００１）。アクセス履歴匿名化契機であると判定した場合は、匿名化支援機能部１５０は、ファイル管理テーブル１８０からランダムにファイルを選択し（Ｓ１００２）、オンライン・ファイル・ストレージ内の該ファイルにアクセスを行う。この際、個人ファイル管理システム１２０のファイル管理テーブル１８０で管理している時刻情報は更新しない。ファイル・アクセス時に、データをリードするか、ライトするかはランダムに決定する。ライトの場合、ファイルの内容が変わらないように、一度データをリードしたのちに、そのデータをファイルの同じ位置に書き込む（Ｓ１００３）。

【０１４０】

ステップＳ１００３の処理が終了した場合、又は、ステップＳ１００１でアクセス履歴

匿名化契機でないと判定した場合は、匿名化支援機能部１５０は、匿名化契機テーブル１９０を参照し、ごみファイル作成契機かどうかを判定する（Ｓ１００４）。ごみファイル作成契機であると判定した場合は、匿名化支援機能部１５０は、ストレージ管理テーブル１７０からランダムにオンライン・ファイル・ストレージとストレージ・アカウント名を選択する（Ｓ１００５）。そして、匿名化支援機能部１５０は、オンライン・ファイル・ストレージに存在しないストレージ・パス名とランダムに決定する。また、ファイルのサイズとデータの内容をランダムに決定する（Ｓ１００６）。次に、匿名化支援機能部１５０は、選択したオンライン・ファイル・ストレージに対して、選択したストレージ・アカウントを使って、決定したストレージ・パス名で、ダミーファイルを作成する。作成後、該ダミーファイルの管理情報をファイル管理テーブル１８０に追加する（Ｓ１００７）。

【０１４１】

ステップＳ１００７の処理が終了した場合、又は、ステップＳ１００４でごみファイル作成契機でないと判定した場合は、匿名化支援機能部１５０は、匿名化契機テーブル１９０を参照し、パスワード変更契機かどうかを判定する（Ｓ１００８）。パスワード変更契機であると判定した場合は、匿名化支援機能部１５０は、ストレージ管理テーブル１７０の全ストレージ・アカウントを対象に、ランダムな新パスワードを決定する（Ｓ１００９）。そして、匿名化支援機能部１５０は、オンライン・ファイル・ストレージに対して、ストレージ・アカウントのパスワードを新パスワードで更新する（Ｓ１０１０）。次に、匿名化支援機能部１５０は、ストレージ管理テーブル１７０のパスワード欄１７３を新パスワードで更新する（Ｓ１０１１）。ステップＳ１０１１の処理又はステップＳ１００８でパスワード変更契機でないと判定した場合は、処理が完了となる。

【０１４２】

この第１の実施形態によると、プライバシ保護ファイル共有システム１は、ユーザがファイルをオンライン・ファイル・ストレージに対してファイルの作成、更新等の処理をする場合に、個人を特定するためのプライバシ情報を、オンライン・ファイル・ストレージに対してそのファイルを処理するための情報から分離するように構成しているため、ユーザの利便性を損なわずにユーザのプライバシ情報を保護し、オンライン・ファイル・ストレージ側からではユーザのプライバシ情報を特定できないようにすることができる。

【０１４３】

また、プライバシ保護ファイル共有システム１は、ユーザのプライバシ情報を保護したまま、オンライン・ファイル・ストレージを介して複数の個人間でデータ共有を行うことができる。

【０１４４】

（第２の実施形態）

次に第２の実施形態について説明する。この第２の実施形態は、一つのファイルを複数のサブ・ファイルに分割し、各サブ・ファイルを別々のオンライン・ファイル・ストレージに格納することで、プライバシ情報を保護する構成である点が第１の実施形態と異なっている。このため、以下では、上記異なる点を中心述べることとし、詳細な説明は省略する。

【０１４５】

図３５は、この第２の実施形態におけるプライバシ保護ファイル共有システム２の構成を概略的に示す図である。図３５に示すように、このプライバシ保護ファイル共有システム２では、個人ファイル管理システム６２０が新規なファイルＸ６１０を作成する場合に、ファイルＸ６１０を、オフセットの０番目、１００番目、２５０番目で区切り、３つのサブ・ファイルＬ６３２、サブ・ファイルＭ６４２、サブ・ファイルＮ６５２に分割する。それらサブ・ファイルをオンライン・ファイル・ストレージ６３０，６４０，６５０にそれぞれ格納する。

【０１４６】

図３６は、システム２における個人ファイル管理システム６２０が管理するファイル管理テーブル１８０を示す図である。第１の実施形態とは、サブ・ファイル構成情報欄１８

５設けられている点が異なっている。他の要素については第１の実施形態と同様であるため、同様な符号を付すこととし、説明は省略する。

【０１４７】

サブ・ファイル構成情報欄１８５は、オフセット欄１８５１、サイズ欄１８５２、次エントリ欄１８５３を有している。サブ・ファイル構成情報欄１８５に保存されるサブ・ファイル構成情報は、ファイルがどのように分割され、サブ・ファイル間がどういう連続性にあるかを示している。

【０１４８】

図３６に示すように、オフセット欄１８５１では、ファイルＸ６１０の先頭から１００番地までをサブ・ファイルの一番目、ファイルＸ６１０の１００番地から２５０番地までをサブ・ファイルの二番目、ファイルＸ６１０の２５０番地から３００番地までをサブ・ファイルの三番目に区切っている。サイズ欄１８５２では、各サブ・ファイル（ファイルＬ，Ｍ，Ｎ）のサイズを示している。次エントリ欄１８５３では、サブ・ファイル間の順序を示している。エントリ番号００１のサブ・ファイルの次がエントリ番号００２のサブ・ファイルに続いている。エントリ番号００３のサブ・ファイルは、最後の部分であるため、次エントリ欄１８５３には、“Ｎ／Ａ”が保存されている。

【０１４９】

この第２の実施形態では、サブ・ファイルＬ６３２、サブ・ファイルＭ６４２、サブ・ファイルＮ６５２毎に、オンライン・ファイル・ストレージ６３０，６４０，６５０内のファイルを対応付けるため、ファイル管理テーブル１８０の格納用管理情報欄１８３のストレージ識別子欄１８３１に保存される情報でその対応を管理する。図３６では、エントリ番号００１のサブ・ファイルがストレージ識別子“ＳＴＲ１”で識別するオンライン・ファイル・ストレージ６３０のストレージ・パス名“／ＡＢＣ／ＦＩＬＥ＿Ｘ”で指定されるファイルに対応付けられている。

【０１５０】

この第２の実施形態によると、１つのファイルＸ６１０を３つのサブ・ファイルＬ，Ｍ，Ｎに分けて、それぞれオンライン・ファイル・ストレージ６３０，６４０，６５０に格納することができるため、第１の実施形態よりさらにプライバシ情報の保護のレベルを上げることができる。

【０１５１】

（第３の実施形態）

次に第３の実施形態について説明する。この第３の実施形態は、ＰＣ毎にユニークなＩＰ（Internet Protocol）アドレスが割り振られている場合にＩＰアドレスを匿名化する構成を有している点が第１の実施形態と異なっている。このため、以下では、上記異なる点を中心述べることとし、詳細な説明は省略する。

【０１５２】

図３７は、この第３の実施形態のプライバシ保護ファイル共有システム３の構成を概略的に示す図である。このプライバシ保護ファイル共有システム３では、複数のＰＣ７１０，７２０，７３０がプロキシサーバ７４０を経由して、オンライン・ファイル・ストレージ７５０に接続する構成となっている。各ＰＣ７１０，７２０，７３０は、それぞれユニークなＩＰアドレス７１２，７２２，７３２を有している。また、プロキシサーバ７４０もユニークなＩＰアドレス７４１を有している。

【０１５３】

各ＰＣ７１０，７２０，７３０に含まれる個人ファイル管理システム（図示しない。）が、オンライン・ファイル・ストレージ７５０にファイルの作成等の要求を発行する場合に、プロキシサーバ７４０が、送信元のＰＣのＩＰアドレスをプロキシサーバのＩＰアドレスに置き換えることで、オンライン・ファイル・ストレージ７５０からは、複数のＰＣ７１０，７２０，７３０のいずれからの要求であっても、プロキシサーバ７４０からの要求となるように認識させることができる。

【０１５４】

この第３の実施形態によると、複数のＰＣ７１０，７２０，７３０からのオンライン・ファイル・ストレージ７５０に関する要求を、全てプロキシサーバ７４０からの要求であるとオンライン・ファイル・ストレージ７５０は認識するため、各ＰＣ７１０，７２０，７３０のＩＰアドレスの匿名性の保護をより高いものとすることができる。

【０１５５】

（他の実施形態）

なお、上記第１の実施形態では本発明を、ＰＣ１００，携帯型端末２００と、これらＰＣ１００，携帯型端末２００とインターネットを介して接続されるオンライン・ファイル・ストレージ３００，４００とを含み、ＰＣ１００，携帯型端末２００との少なくともいずれかからオンライン・ファイル・ストレージ３００，４００にファイルを格納し、その格納したファイルをＰＣ１００，携帯型端末２００で共有するファイル共有システム１であって、ＰＣ１００は、オンライン・ファイル・ストレージ３００にファイルを作成するときに、ファイルを作成するユーザを特定するプライバシ情報をオンライン・ファイル・ストレージ３００にファイルを作成するために必要な情報から分離し、その分離されたプライバシ情報を変換した情報を用いてファイルをオンライン・ファイル・ストレージ３００に作成する（Ｓ２０３）場合で説明しているが、本発明はこれに限られるものではない。なお、このように個人を特定する情報をオンライン・ファイル・ストレージ３００から分離することができるのでインターネット１０上におけるユーザの匿名性を確保することができる。

【０１５６】

また、上記第１の実施形態では本発明を、ＰＣ１００，携帯型端末２００と、これらＰＣ１００，携帯型端末２００とインターネットを介して接続されるオンライン・ファイル・ストレージ３００，４００とを含み、ＰＣ１００，携帯型端末２００の少なくともいずれかからオンライン・ファイル・ストレージ３００，４００にファイルを格納し、その格納したファイルをＰＣ１００，携帯型端末２００で共有するファイル共有システム１であって、ＰＣ１００は、ファイルを作成するユーザを特定する個人アカウント名及び個人パスパスを含むプライバシ情報と、個人アカウントと異なるストレージ・アカウント名及び個人パス名と異なるストレージ・パス名を含む格納用管理情報とを少なくとも管理するファイル管理テーブル１８０と、オンライン・ファイル・ストレージ３００に新規ファイルを作成するときに、個人アカウント名及び個人パス名からストレージ・アカウント名及びストレージ・パス名を作成し、ファイル管理テーブル１８０に個人アカウント名及び個人パス名に対応付けて登録する登録部（Ｓ３０５）と、ファイル管理テーブル１８０に登録されたストレージ・アカウント名及びストレージ・パス名を用いてオンライン・ファイル・ストレージ３００に新規ファイルを作成するファイル作成部（Ｓ３０６）を備える場合で説明しているが、本発明は、この構成に限られるものではない。なお、このように個人を特定する情報をオンライン・ファイル・ストレージ３００から分離することができるのでインターネット１０上におけるユーザの匿名性を確保することができる。

【０１５７】

上記第１の実施形態における、プライバシ情報は、個人アカウント名、個人パス名、個人アカウント名が属するグループ、ファイルの種別、ファイルのアクセス権限、情報処理装置からオンライン・ファイル・ストレージ３００にアクセスした時刻の情報を含むものであり、これらは、ファイル管理テーブル１８０で管理されることとしているが、本発明は、プライバシ情報をファイル管理テーブル１８０で管理する場合に限られるものではない。

【０１５８】

上記第１の実施形態における、ＰＣ１００は、新規ファイルを暗号化する暗号化部（Ｓ３０２）を備え、ファイル作成部（Ｓ３０６）は、暗号化部で暗号化された新規ファイルをオンライン・ファイル・ストレージ３００に作成し、ファイル管理テーブル１８０は、個人アカウント名及び個人パス名と対応付けて暗号化された新規ファイルを複合する暗号鍵を管理する場合説明しているが、本発明は、このような構成に限られるものではない。

なお、このように暗号鍵を用いることで、暗号鍵を管理する個人ファイル管理システム１２０のみがデータの参照を行なうことができるようにすることができる。

【０１５９】

上記第１の実施形態におけるＰＣ１００のファイル作成部（Ｓ３０６）は、第１の新規ファイルを作成する際に、第１の暗号鍵を用いて暗号化部で暗号化された第１の新規ファイルをストレージ・アカウント名を用いてオンライン・ファイル・ストレージ３００に作成し、携帯型端末２００のファイル作成部は、第２の新規ファイルを作成する際に、第２の暗号鍵を用いて暗号化部で暗号化された第２の新規ファイルを上記ストレージ・アカウント名を用いてオンライン・ファイル・ストレージ３００に作成する場合で説明しているが、本発明は、これに限られるものではない。なお、このよう同じアカウントを用いても異なる暗号鍵を使用することにより、オンライン・ファイル・ストレージに格納したファイル群とその所有者の対応関係を匿名化することができる。

【０１６０】

上記第１の実施形態における登録部（Ｓ３０５）は、個人アカウント名からストレージ・アカウント名を生成するときに、個人アカウント名を用いて作成されるファイル群に対して、ファイル毎に異なるストレージ・アカウント名を割り当て、ファイル作成部（Ｓ３０６）は、ファイル毎に異なるストレージ・アカウント名を用いて各ファイルをオンライン・ファイル・ストレージ３００に作成するようにしても良い場合で説明しているが、本発明はこれに限られるものではない。

【０１６１】

上記第１の実施形態における登録部（Ｓ３０５）は、新規ファイルを作成するときに、ファイル毎に異なるストレージ・アカウント名から、ファイル数が一番少ないストレージ・アカウント名を選択し、ファイル作成部（Ｓ３０６）は、選択されたストレージ・アカウント名を用いてオンライン・ファイル・ストレージ３００にファイルを作成する場合で説明をしているが、本発明はこの構成に限るものではない。なお、このようにファイル数が一番少ないストレージ・アカウント名を選択するようにすれば、ファイル数が平均化されるので、より、匿名性を高めることができる。

【０１６２】

上記第１の実施形態におけるＰＣ１００は、個人アカウント名及び個人パス名を用いて指定されるファイルのリード要求を受けると、リード要求されたファイルに対するアクセス権限があるか否かを、ファイル管理テーブル１８０を参照して判定するアクセス権限判定部（Ｓ４０２）と、アクセス権限判定部でアクセス権限があると判定した場合に、ファイル管理テーブル１８０を参照し、リート要求されたファイルに対応付けられたストレージ・アカウント名及びストレージ・パス名を用いて、オンライン・ファイル・ストレージ３００に対してリード要求し、リード要求部の要求に基づいてオンライン・ファイル・ストレージ３００から送信されるリード要求されたファイルをリードするリード処理部（Ｓ４０５）を備える場合で説明しているが、本発明はこれに限れられるものではない。

【０１６３】

上記第１の実施形態におけるＰＣ１００は、個人アカウント名及び個人パス名を用いて指定されるファイルのライト要求を受けると、ライト要求されたファイルに対するアクセス権限があるか否かを、ファイル管理テーブル１８０を参照して判定するアクセス権限判定部（Ｓ５０２）と、アクセス権限判定部でアクセス権限があると判定した場合に、ファイル管理テーブル１８０を参照し、ライト要求されたファイルに対応付けられたストレージ・アカウント名及びストレージ・パス名を用いて、オンライン・ファイル・ストレージ３００に対してライト要求をし、そのライト要求に基づいてオンライン・ファイル・ストレージ３００からライト要求されたファイルのライト結果を更新する更新処理部（Ｓ５０５）を備える場合で説明しているが、本発明はこの構成に限るものではない。

【０１６４】

上記第１の実施形態におけるファイル管理テーブル１８０は、登録されるファイル毎に時刻情報を管理し、ＰＣ１００は、ランダムに決定された時刻に、ファイル管理テーブル

１８０からランダムに決定したファイルに対して、ファイル管理テーブル１８０内の時刻情報は更新せず、オンライン・ファイル・ストレージ３００内のランダムに決定されたファイルにアクセスするアクセス部（Ｓ１００１～Ｓ１００３）を備える場合で説明しているが、本発明はこの構成に限るものではない。なお、オンライン・ファイル・ストレージ３００内の時刻情報のみを更新することにより、ユーザがアクセスしたアクセス履歴情報の匿名性を確保することができる。

【０１６５】

上記第１の実施形態におけるＰＣ１００は、オンライン・ファイル・ストレージ３００にランダムな内容を有する新規ファイルを作成するダミーファイル作成部（Ｓ１００４～Ｓ１００７）を備える場合で説明しているが、本発明はこの構成に限るものではない。なお、このようにダミーファイルを作成することで、第三者がオンライン・ストレージ・ファイルを参照しても、個人情報を特定するファイルを発見することを困難にすることができる。

【０１６６】

上記第１の実施形態におけるオンライン・ファイル・ストレージ３００は、ストレージ・アカウント名と対応づけたパスワードを管理するストレージ・アカウント管理テーブル３２０を備え、また、ＰＣ１００は、定期的にオンライン・ファイル・ストレージ３００に対して、ストレージ・アカウント名と対応するパスワードを変更するパスワード変更部（Ｓ１００８～Ｓ１０１１）を備える場合で説明しているが、本発明はこの構成に限るものではない。なお、このように、パスワードを変更することにより、パスワードが漏洩することを防止することができる。

【０１６７】

上記第１の実施形態におけるＰＣ１００は、個人アカウント名及び個人パス名で指定されたファイルを共有するためにファイルが作成されたオンライン・ファイル・ストレージ３００に対してファイルを共有する処理を行う共有処理部（Ｓ７０１～Ｓ７０７）と、共有処理部の処理に基づいてオンライン・ファイル・ストレージ３００からファイルのストレージ・アカウント名及びストレージ・パス名を用いてファイルをリードするリード部（Ｓ７０８）と、ストレージ・アカウント名及びストレージ・パス名とそれぞれ対応づけた新たなアカウント及び新たなパスを作成し、オンライン・ファイル・ストレージ３００とは異なるオンライン・ファイル・ストレージ４００にリードしたファイルとともに新たなアカウント及び新たなパスを保存する保存部（Ｓ７１１）と、を備える場合で説明しているが、本発明は、この構成に限るものではない。なお、このようにファイルを共有することにより、例えば、個人ファイル管理システムＰ１と個人ファイル管理システムＰ２とで、匿名性を維持しながら、ファイルを共有することが可能となる。

【０１６８】

上記第１の実施形態におけるＰＣ１００は、上記新たなアカウント及び上記新たなパスで指定されるファイルを異なるオンライン・ファイル・ストレージ４００から削除するファイル削除部（Ｓ２０６）を備える場合で説明しているが、本発明は、この構成に限るものではない。

【０１６９】

上記第１の実施形態における保存部は（Ｓ７１１）、ファイルの共有を要求するときにファイルの説明情報を、上記新たなアカウント及び上記新たなパスで指定されるファイルに関連づけて説明情報を付加する場合で説明しているが、本発明は、この構成に限るものではない。なお、このように説明情報を付加することにより、説明情報を検索することにより、ユーザが必要なファイルを発見することが可能となる。

【０１７０】

上記第１の実施形態における異なるオンライン・ファイル・ストレージ４００にアクセス可能な携帯型端末２００は、ファイルを検索するユーザを特定するアカウントを含むプライバシ情報とともに検索に用いられるキーワードの入力を受け付け、ユーザを特定するアカウントと対応するアカウントを用いて異なるオンライン・ファイル・ストレージ４０

０にアクセスし、キーワードを用いて異なるオンライン・ファイル・ストレージ４００内の説明情報Ｄ１を検索する要求をする検索要求部（Ｓ８０２）と、この検索要求部の要求に基づいて検索された説明情報及びその説明情報に関連付けられたファイルのパスを検索結果として受け取る検索結果受信部（Ｓ８０３）を備える場合で説明しているが、本発明は、この構成に限るものではない。なお、このようにファイルのパスを提示することにより、共有可能なファイル群を第三者が検索することが可能となる。

【０１７１】

上記第２の実施形態におけるプライバシ保護ファイル共有システム２は、オンライン・ファイル・ストレージ６３０，６４０，６５０を有し、ファイル作成部（Ｓ３０６）は、新規ファイルを作成するときに、その作成する新規ファイルを所定のサブ・ファイル（ファイルＬ，Ｍ，Ｎ）に分割し、その分割されたサブ・ファイル毎にストレージ・パス名を決定し、そのストレージ・パス名を用いて複数のオンライン・ファイル・ストレージ６３０、６４０，６５０にファイルをサブ・ファイル毎に分割して作成する処理を含み、ファイル管理テーブル１８０は、サブ・ファイル（ファイルＬ，Ｍ，Ｎ）毎に決定したストレージ・パス名とサブ・ファイルを作成したオンライン・ファイル・ストレージ３００との対応関係の管理（サブ・ファイル構成情報欄１８５）を含む場合で説明しているが、本発明は、この構成に限るものではない。なお、このようにファイルを複数のサブ・ファイルに分割することにより、サブ・ファイルの１つが漏洩しても全ての情報が漏洩することを防止することができる。

【０１７２】

上記第３の実施形態におけるプライバシ保護ファイル共有システム３は、ＰＣ７１０，２０，７３０と、オンライン・ファイル・ストレージ７５０との間にインターネット上のアドレスを変換するプロキシサーバ７４０を備え、ＰＣ７１０，２０，７３０は、プロキシサーバ７４０を経由してオンライン・ファイル・ストレージ７５０へアクセスする場合で説明しているが、本発明は、この構成に限るものではない。なお、このようにプロキシサーバ７４０でＩＰアドレスの変換を行なうことにより、ＰＣ７１０，２０，７３０のＩＰアドレスの匿名化を行なうことができる。

【産業上の利用可能性】

【０１７３】

本発明は、ブライバシ保護ファイル共有システム及びプライバシ保護ファイル共有方法に広く適用することができる。

【図面の簡単な説明】

【０１７４】

【図１】本発明の第１の実施形態に係わるプライバシ保護ファイル共有システムの構成を示す図である。

【図２】同実施形態に係わるＰＣの物理的な構成を示す図である。

【図３】同実施形態に係わるオンライン・ファイル・ストレージの物理的な構成を示す図である。

【図４】同実施形態に係わる個人アカウント管理テーブルの一例を示す図である。

【図５】同実施形態に係わるストレージ管理テーブルの一例を示す図である。

【図６】同実施形態に係わるファイル管理テーブルの一例を示す図である。

【図７】同実施形態に係わる個人用アクセス権限情報欄に含まれる情報の一例を示す図である。

【図８】同実施形態に係わる個人用時刻情報欄に含まれる情報の一例を示す図である。

【図９】同実施形態に係わる匿名化契機テーブルの一例を示す図である。

【図１０】同実施形態に係わるストレージ・アカウント管理テーブルの一例を示す図である。

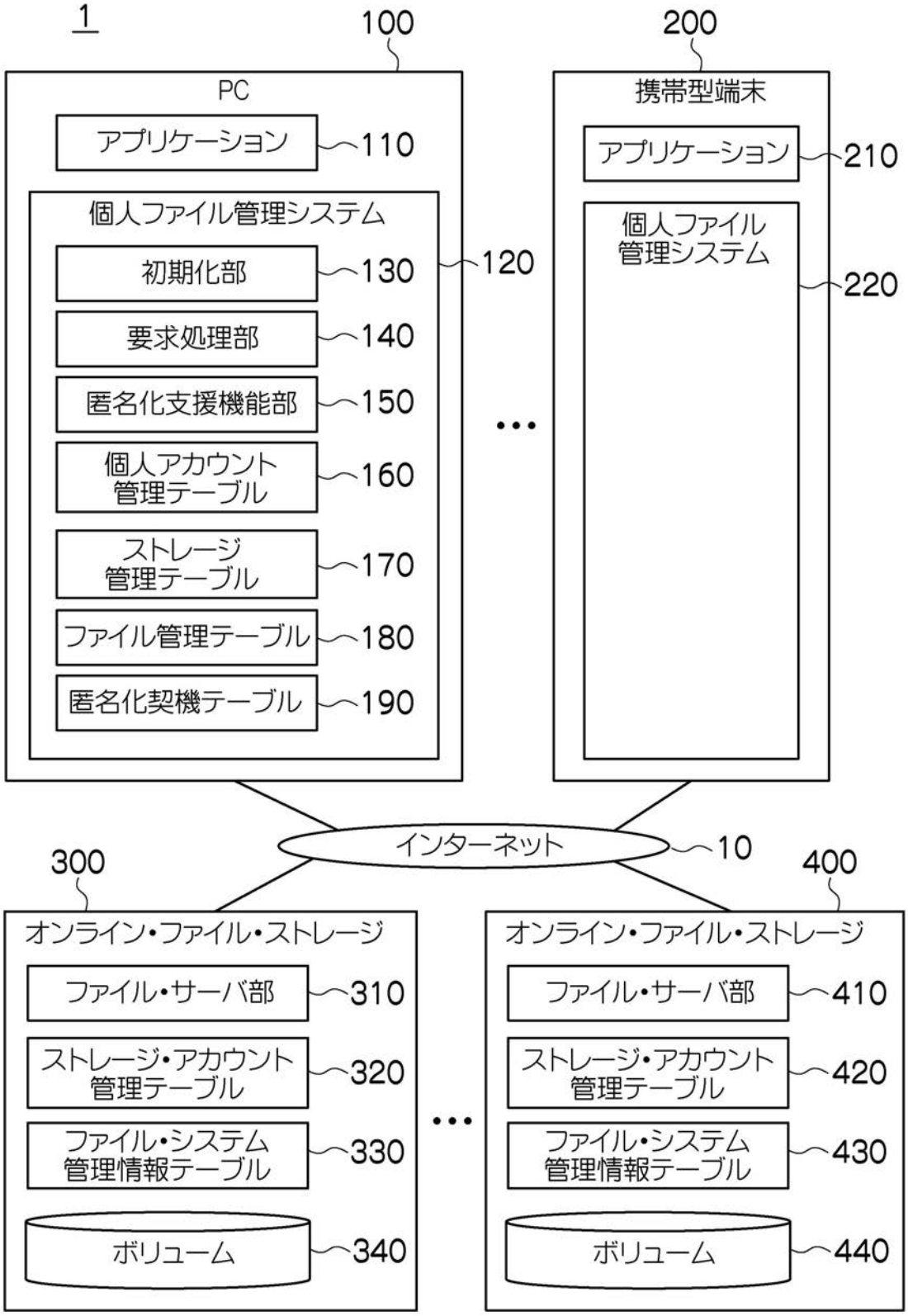
【図１１】同実施形態に係わるファイル・システム管理情報テーブルの一例を示す図である。

【図１２】同実施形態に係わる初期化要求情報の一例を示す図である。

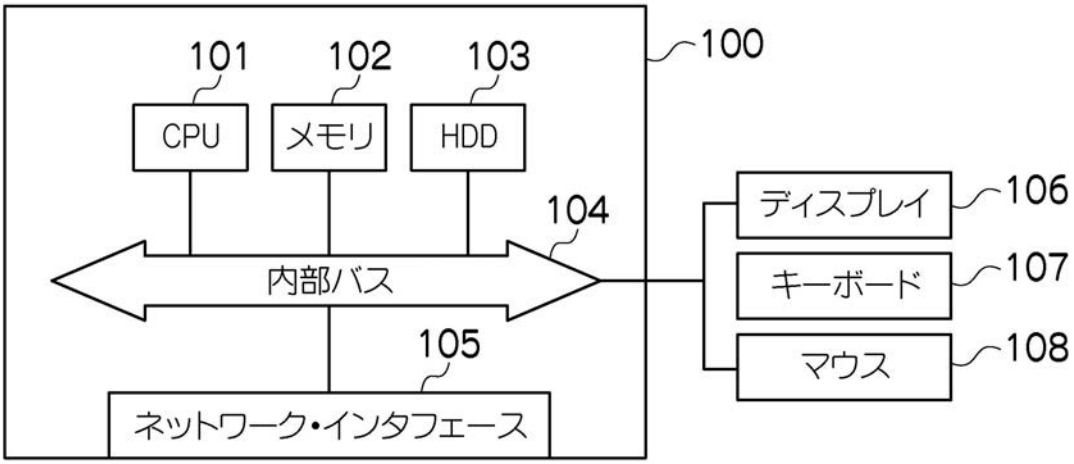
【図１３】同実施形態に係わる個人ファイル管理システムに対してファイル作成を要求する場合の要求フォーマットの一例を示す図である。
【図１４】同実施形態に係わるオンライン・ファイル・ストレージに対してファイル作成を要求する場合の要求フォーマットの一例を示す図である。
【図１５】同実施形態に係わる個人ファイル管理システムに対してファイル参照を要求する場合の要求フォーマットの一例を示す図である。
【図１６】同実施形態に係わるオンライン・ファイル・ストレージに対してファイル参照を要求する場合の要求フォーマットの一例を示す図である。
【図１７】同実施形態に係わる個人ファイル管理システムに対してファイル更新を要求する場合の要求フォーマットの一例を示す図である。
【図１８】同実施形態に係わるオンライン・ファイル・ストレージに対してファイル更新を要求する場合の要求フォーマットを示す図である。
【図１９】同実施形態に係わる個人ファイル管理システムに対してファイル削除を要求する場合の要求フォーマットを示す図である。
【図２０】同実施形態に係わるオンライン・ファイル・ストレージに対してファイル削除を要求する場合の要求フォーマットの一例を示す図である。
【図２１】同実施形態に係わる共有処理及び検索処理の概要を説明するための図である。
【図２２】同実施形態に係わる個人ファイル管理システムにファイル共有を要求する場合の要求フォーマット一例を示す図である
【図２３】同実施形態に係わる個人ファイル管理システムに対してファイル検索を要求する場合の要求フォーマットの一例を示す図である。
【図２４】同実施形態に係わる個人ファイル管理システムに対してアカウント管理を要求する場合の要求フォーマットの一例を示す図である。
【図２５】同実施形態に係わる初期化部で実行される処理を示すフローチャートである。
【図２６】同実施形態に係わる要求処理部で実行される処理を示すフローチャートである。
【図２７】同実施形態に係わるファイル作成処理を示すフローチャートである。
【図２８】同実施形態に係わるファイル参照処理を示すフローチャートである。
【図２９】同実施形態に係わるファイル更新処理を示すフローチャートである。
【図３０】同実施形態に係わるファイル削除処理を示すフローチャートである。
【図３１】同実施形態に係わるファイル共有処理を示すフローチャートである。
【図３２】同実施形態に係わるファイル検索処理を示すフローチャートである。
【図３３】同実施形態に係わるアカウント管理処理を示すフローチャートである。
【図３４】同実施形態に係わる匿名化支援機能部で実行される処理を示すフローチャートである。
【図３５】本発明の第２の実施形態に係わるシステムの構成を概略的に示す図である。
【図３６】同実施形態に係わるファイル管理テーブルを示す図である。
【図３７】本発明の第３の実施形態に係わるシステムの構成を概略的に示す図である。
【符号の説明】
【０１７５】
１，２，３…プライバシ保護ファイル共有システム、１０…インターネット、１００…ＰＣ、１１０…アプリケーション、１２０…個人ファイル管理システム、１３０…初期化部、１４０…要求処理部、１５０…匿名化支援機能部、１６０…個人アカウント管理テーブル、１７０…ストレージ管理テーブル、１８０…ファイル管理テーブル、１９０…匿名化契機テーブル、２００…携帯型端末、３００，４００…オンライン・ファイル・ストレージ、３２０，４２０…ストレージ・アカウント管理テーブル、３３０，４３０…ファイル・システム管理情報テーブル

【図１】

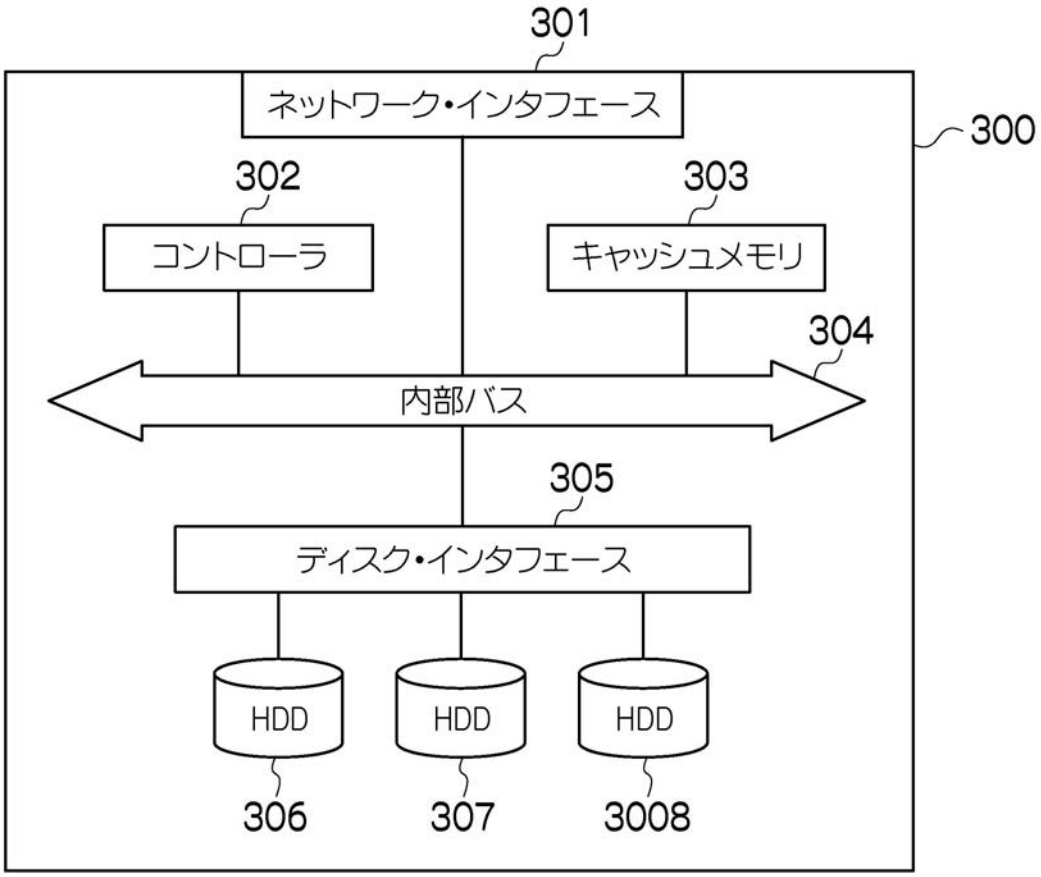
図1


1
100
PC
アプリケーション
110
個人ファイル管理システム
初期化部
130
120
要求処理部
140
匿名化支援機能部
150
個人アカウント管理テーブル
160
ストレージ管理テーブル
170
ファイル管理テーブル
180
匿名化契機テーブル
190
200
携帯型端末
アプリケーション
210
個人ファイル管理システム
220
インターネット
10
300
オンライン・ファイル・ストレージ
ファイル・サーバ部
310
ストレージ・アカウント管理テーブル
320
ファイル・システム管理情報テーブル
330
ボリューム
340
400
オンライン・ファイル・ストレージ
ファイル・サーバ部
410
ストレージ・アカウント管理テーブル
420
ファイル・システム管理情報テーブル
430
ボリューム
440

【図２】
図2

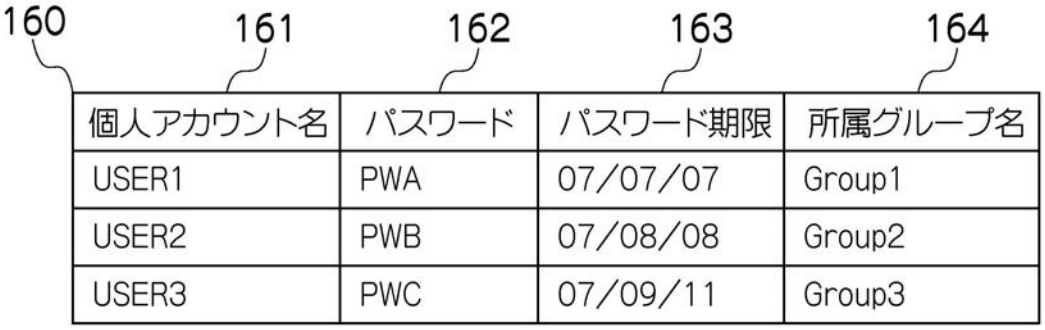

101
102
103
100
CPU
メモリ
HDD
104
ディスプレイ
106
内部バス
キーボード
107
105
マウス
108
ネットワーク・インタフェース

【図３】
図3


301
ネットワーク・インタフェース
300
302
303
コントローラ
キャッシュメモリ
304
内部バス
305
ディスク・インタフェース
HDD
HDD
HDD
306
307
3008

【図４】

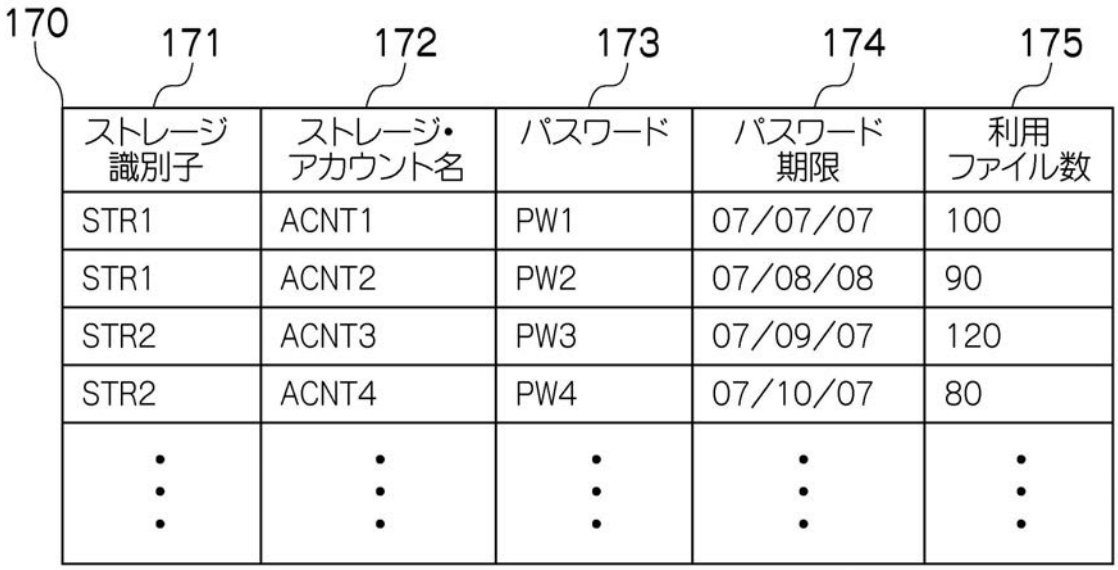
図4



個人アカウント名	パスワード	パスワード期限	所属グループ名
USER1	PWA	07/07/07	Group1
USER2	PWB	07/08/08	Group2
USER3	PWC	07/09/11	Group3

【図５】

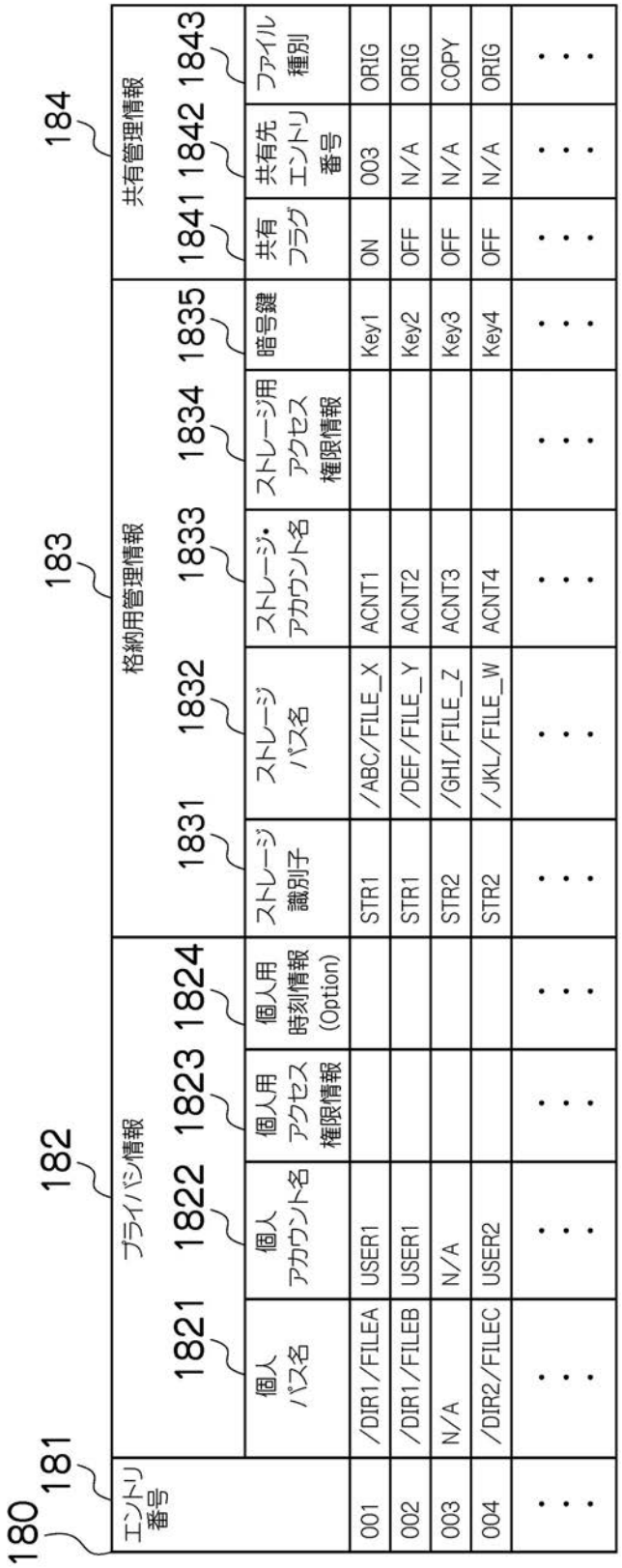
図5



ストレージ識別子	ストレージ・アカウント名	パスワード	パスワード期限	利用ファイル数
STR1	ACNT1	PW1	07/07/07	100
STR1	ACNT2	PW2	07/08/08	90
STR2	ACNT3	PW3	07/09/07	120
STR2	ACNT4	PW4	07/10/07	80
・・・	・・・	・・・	・・・	・・・

【図６】

図6


180
181
182
183
184
エントリ番号
プライバシ情報
格納用管理情報
共有管理情報
1821
1822
1823
1824
1831
1832
1833
1834
1835
1841
1842
1843
個人パス名
個人アカウント名
個人用アクセス権限情報
個人用時刻情報(Option)
ストレージ識別子
ストレージパス名
ストレージ・アカウント名
ストレージ用アクセス権限情報
暗号鍵
共有フラグ
共有先エントリ番号
ファイル種別
001 /DIR1/FILEA USER1 STR1 /ABC/FILE_X ACNT1 Key1 ON 003 ORIG
002 /DIR1/FILEB USER1 STR1 /DEF/FILE_Y ACNT2 Key2 OFF N/A ORIG
003 N/A N/A STR2 /GHI/FILE_Z ACNT3 Key3 OFF N/A COPY
004 /DIR2/FILEC USER2 STR2 /JKL/FILE_W ACNT4 Key4 OFF N/A ORIG

【図７】

図7

アカウント名	権限情報
USER1	Read／Write
USER2	Read Only
USER3	Read Only

【図８】

図8

1824

作成時刻	2007／7／10 10:10:10	1824A
アクセス時刻	2007／7／10 10:18:10	1824B
更新時刻	2007／7／10 10:12:10	1824C

【図９】

図9

190

契機種別	次回契機	時間間隔	
アクセス履歴匿名化契機	2007／7／17 10:00 AM	ランダム	194
ごみファイル作成契機	2007／7／18 9:00 AM	ランダム	195
パスワード変更契機	2007／7／19 10:00 PM	一日毎	196

191 192 193

【図１０】
図10

320

321 アカウント名	322 パスワード	323 パスワード期限
ACNT1	PW1	07/07/07
ACNT2	PW2	07/08/08
・ ・ ・	・ ・ ・	・ ・ ・

【図１１】
図11

330

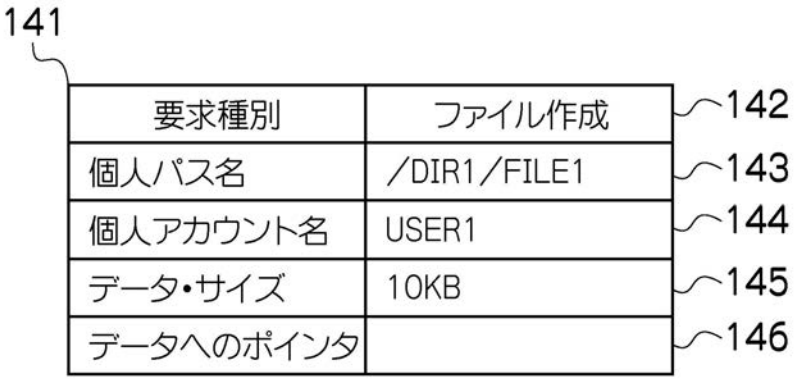
331 ストレージパス名	332 ストレージアカウント名	333 ストレージ側アクセス権限情報	334 ストレージ側時刻情報	335 inode情報	336 説明情報へのポインタ
/ABC/FILE_X	ACNT1				
/DEF/FILE_Y	ACNT2				
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図１２】

図12

【図１３】

図13



【図１４】

図14

【図１５】

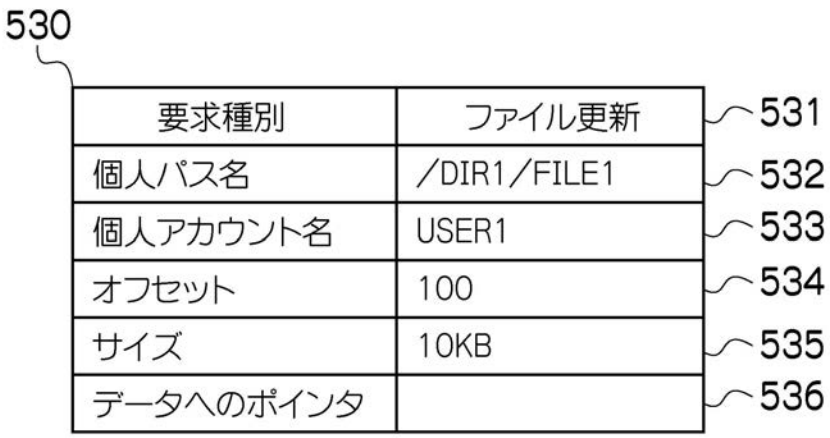
図15

【図１６】

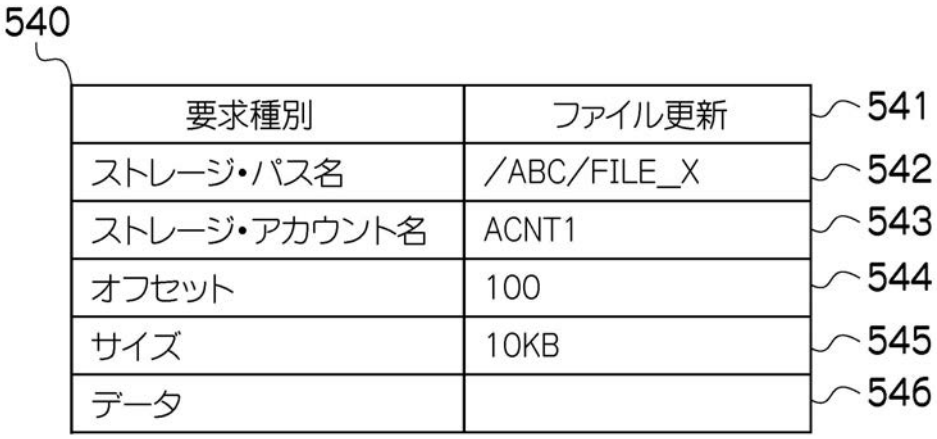
図16

【図１７】

図17



【図１８】
図18

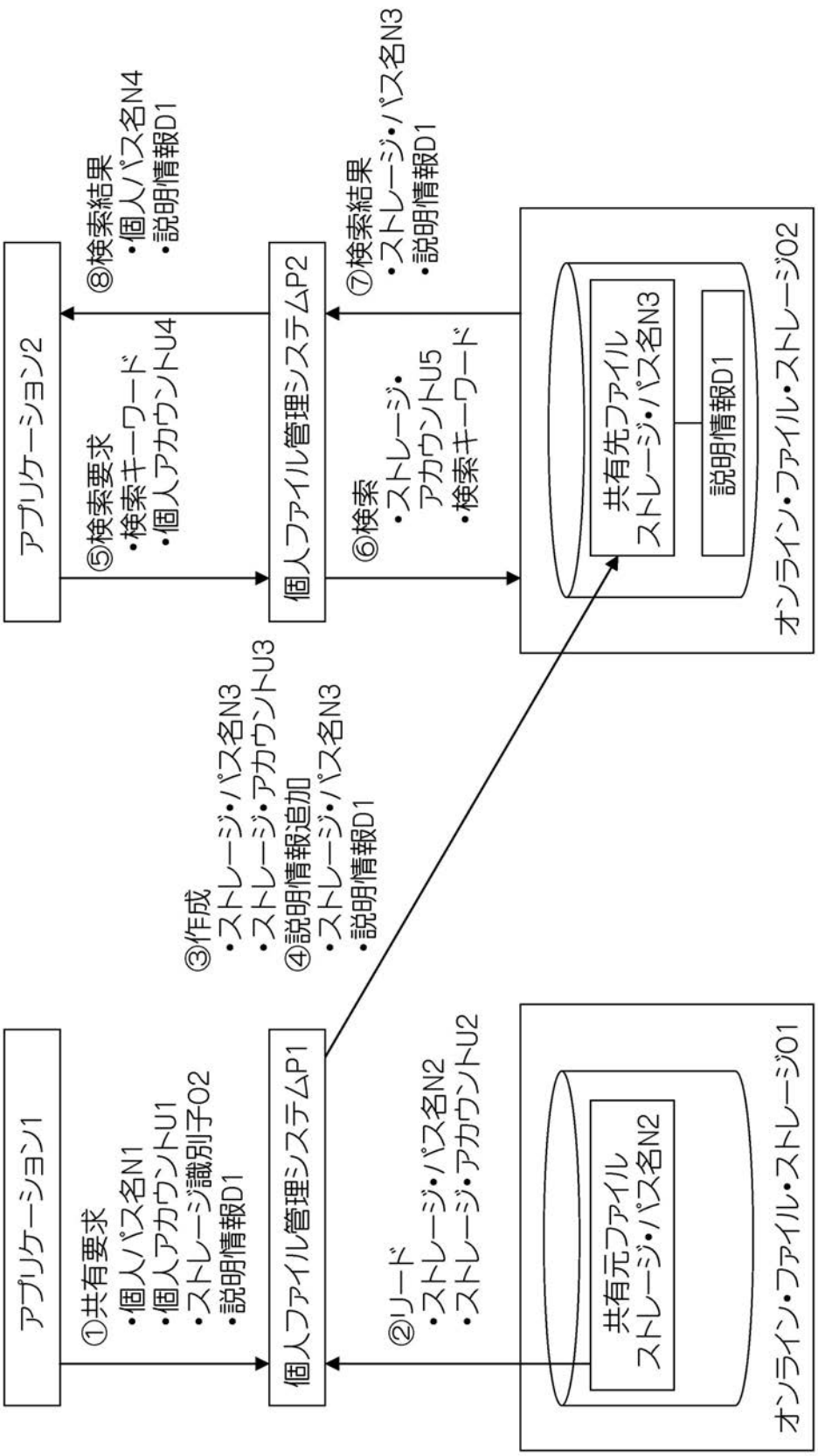


【図１９】
図19

【図２０】
図20

【図２１】

図21


アプリケーション1
①共有要求
・個人パス名N1
・個人アカウントU1
・ストレージ識別子O2
・説明情報D1
個人ファイル管理システムP1
②リード
・ストレージ・パス名N2
・ストレージ・アカウントU2
③作成
・ストレージ・パス名N3
・ストレージ・アカウントU3
④説明情報追加
・ストレージ・パス名N3
・説明情報D1
共有元ファイル
ストレージ・パス名N2
オンライン・ファイル・ストレージO1
アプリケーション2
⑤検索要求
・検索キーワード
・個人アカウントU4
個人ファイル管理システムP2
⑥検索
・ストレージ・
アカウントU5
・検索キーワード
⑦検索結果
・ストレージ・パス名N3
・説明情報D1
⑧検索結果
・個人パス名N4
・説明情報D1
共有先ファイル
ストレージ・パス名N3
説明情報D1
オンライン・ファイル・ストレージO2

【図２２】
図22

570

要求種別	ファイル共有要求	571
個人パス名	N1	572
個人アカウント名	U1	573
共有ストレージ識別子	O2	574
説明情報	D1	575

【図２３】
図23

580

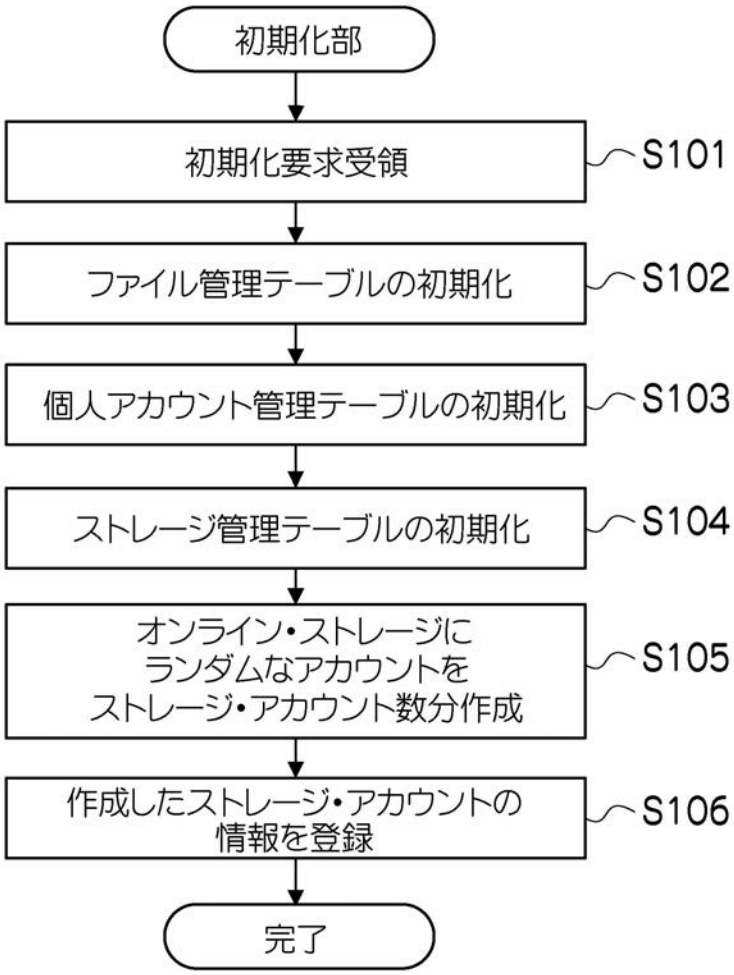
要求種別	ファイル検索	581
個人アカウント名	U3	582
検索キーワード	W 1	583

【図２４】
図24

590

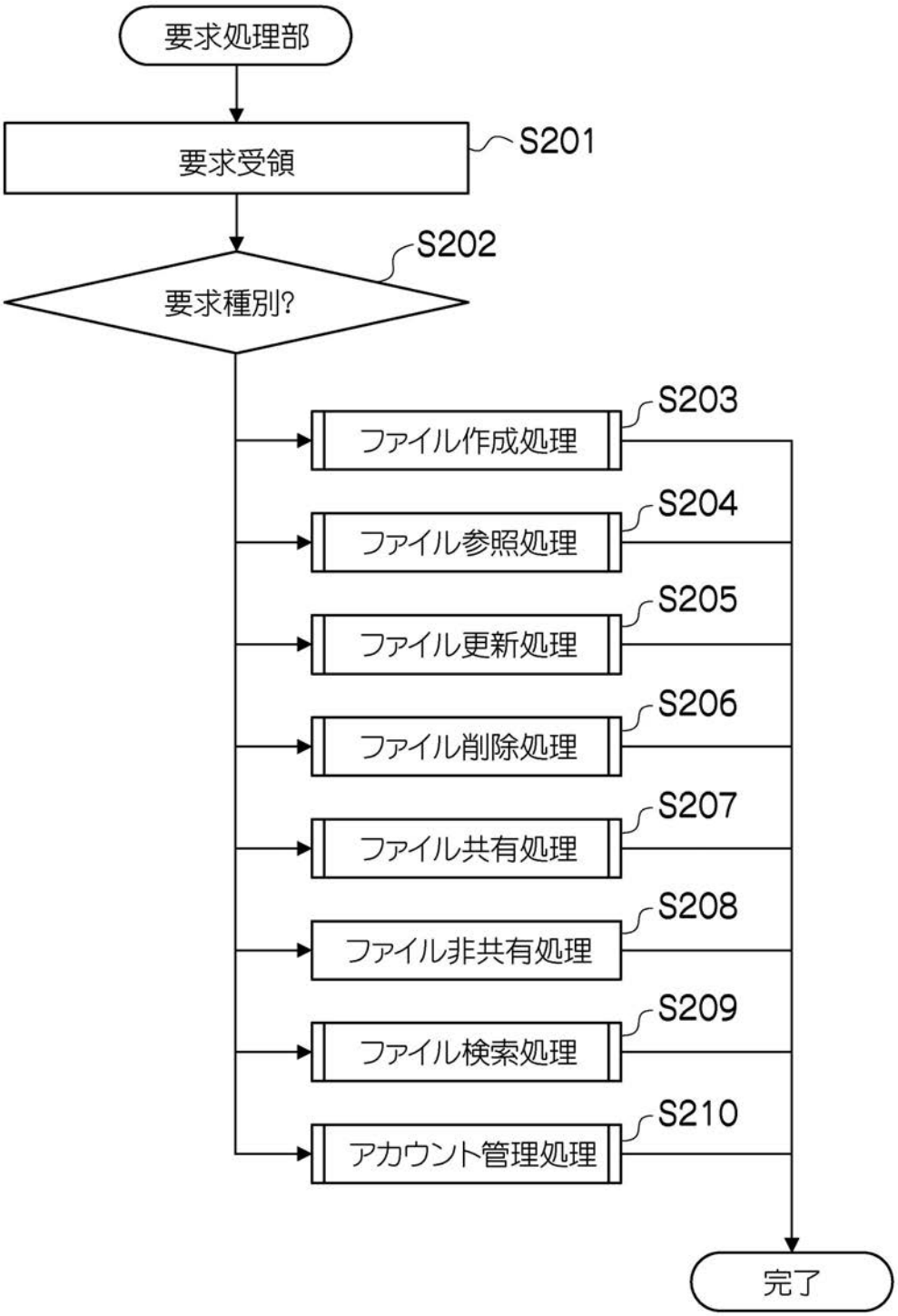
要求種別	アカウント作成 or アカウント削除 or パスワード変更	591
個人アカウント名	USER1	592
新パスワード	PW1	593
ストレージ・アカウント連携	要	594

【図２５】
図25

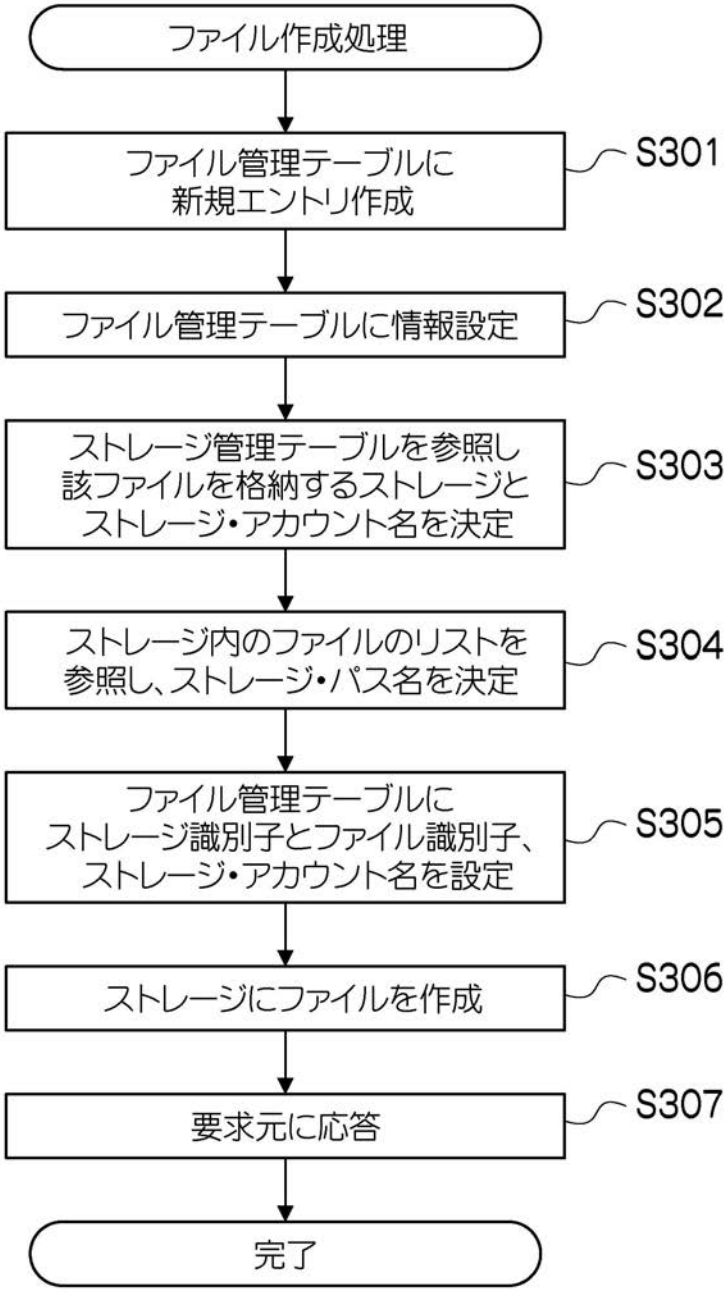

初期化部
初期化要求受領
S101
ファイル管理テーブルの初期化
S102
個人アカウント管理テーブルの初期化
S103
ストレージ管理テーブルの初期化
S104
オンライン・ストレージに
ランダムなアカウントを
ストレージ・アカウント数分作成
S105
作成したストレージ・アカウントの
情報を登録
S106
完了

【図２６】

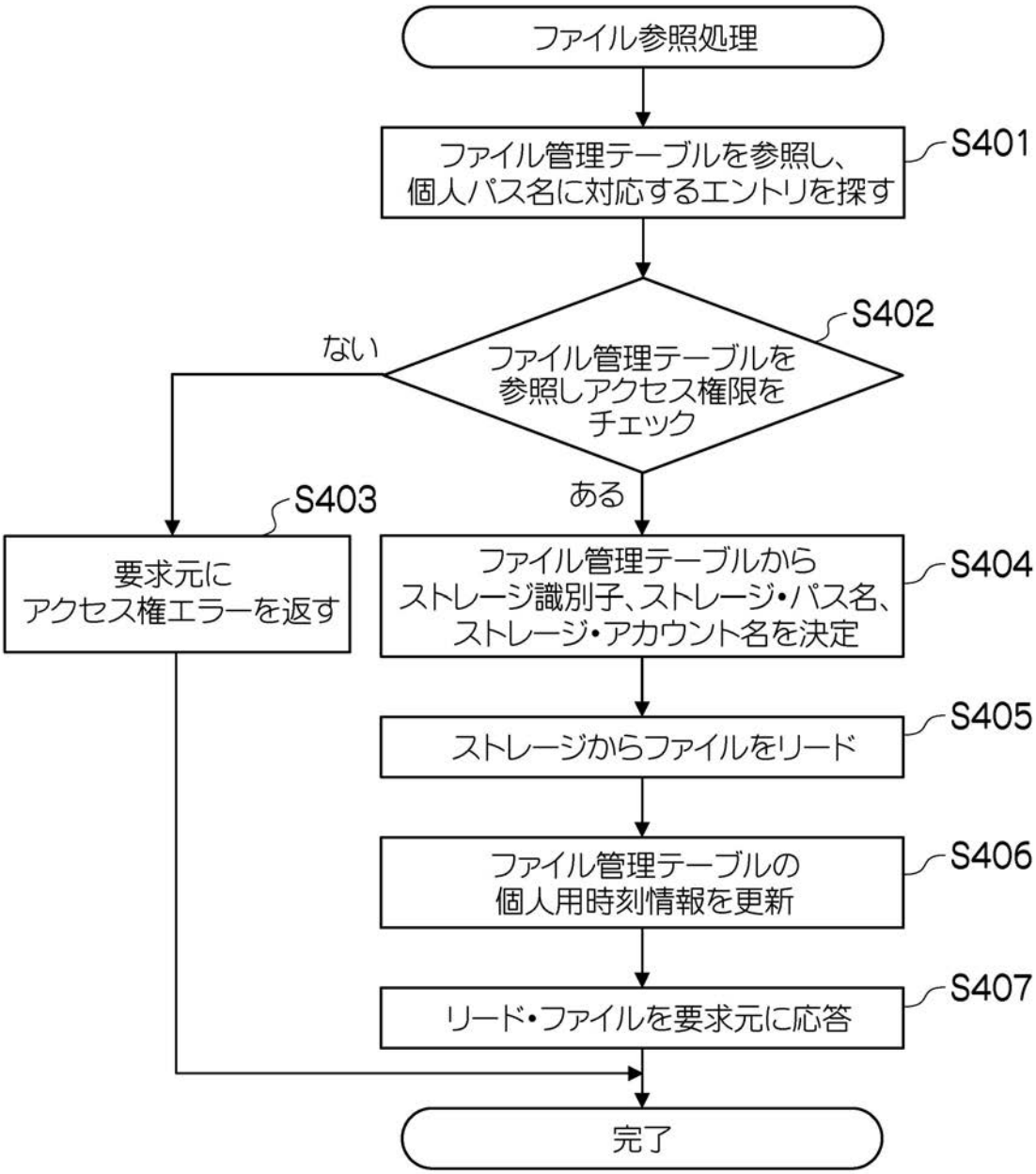
図26


要求処理部
要求受領
S201
S202
要求種別?
S203
ファイル作成処理
S204
ファイル参照処理
S205
ファイル更新処理
S206
ファイル削除処理
S207
ファイル共有処理
S208
ファイル非共有処理
S209
ファイル検索処理
S210
アカウント管理処理
完了

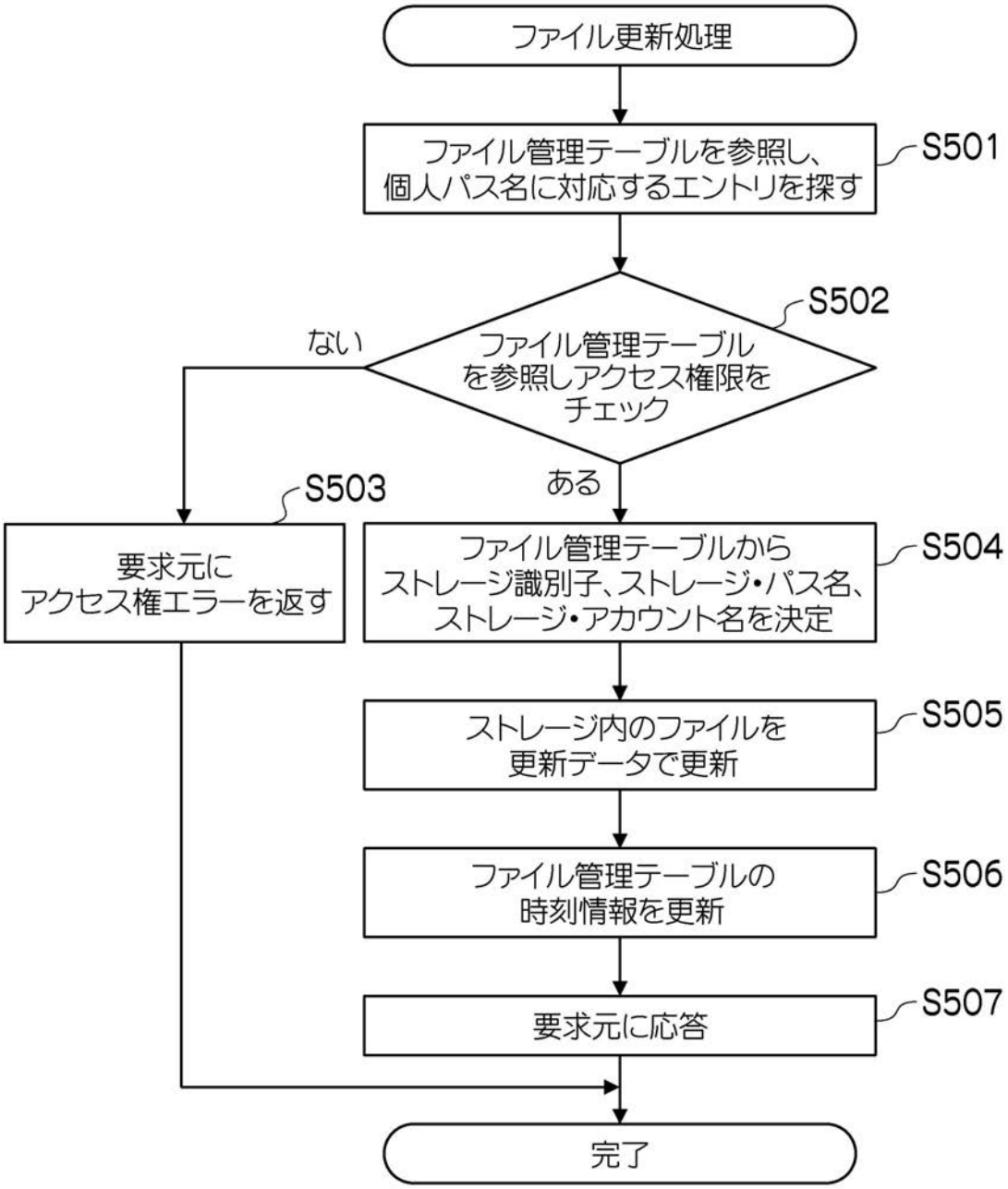
【図２７】
図27


ファイル作成処理
ファイル管理テーブルに
新規エントリ作成
S301
ファイル管理テーブルに情報設定
S302
ストレージ管理テーブルを参照し
該ファイルを格納するストレージと
ストレージ・アカウント名を決定
S303
ストレージ内のファイルのリストを
参照し、ストレージ・パス名を決定
S304
ファイル管理テーブルに
ストレージ識別子とファイル識別子、
ストレージ・アカウント名を設定
S305
ストレージにファイルを作成
S306
要求元に応答
S307
完了

【図２８】
図28

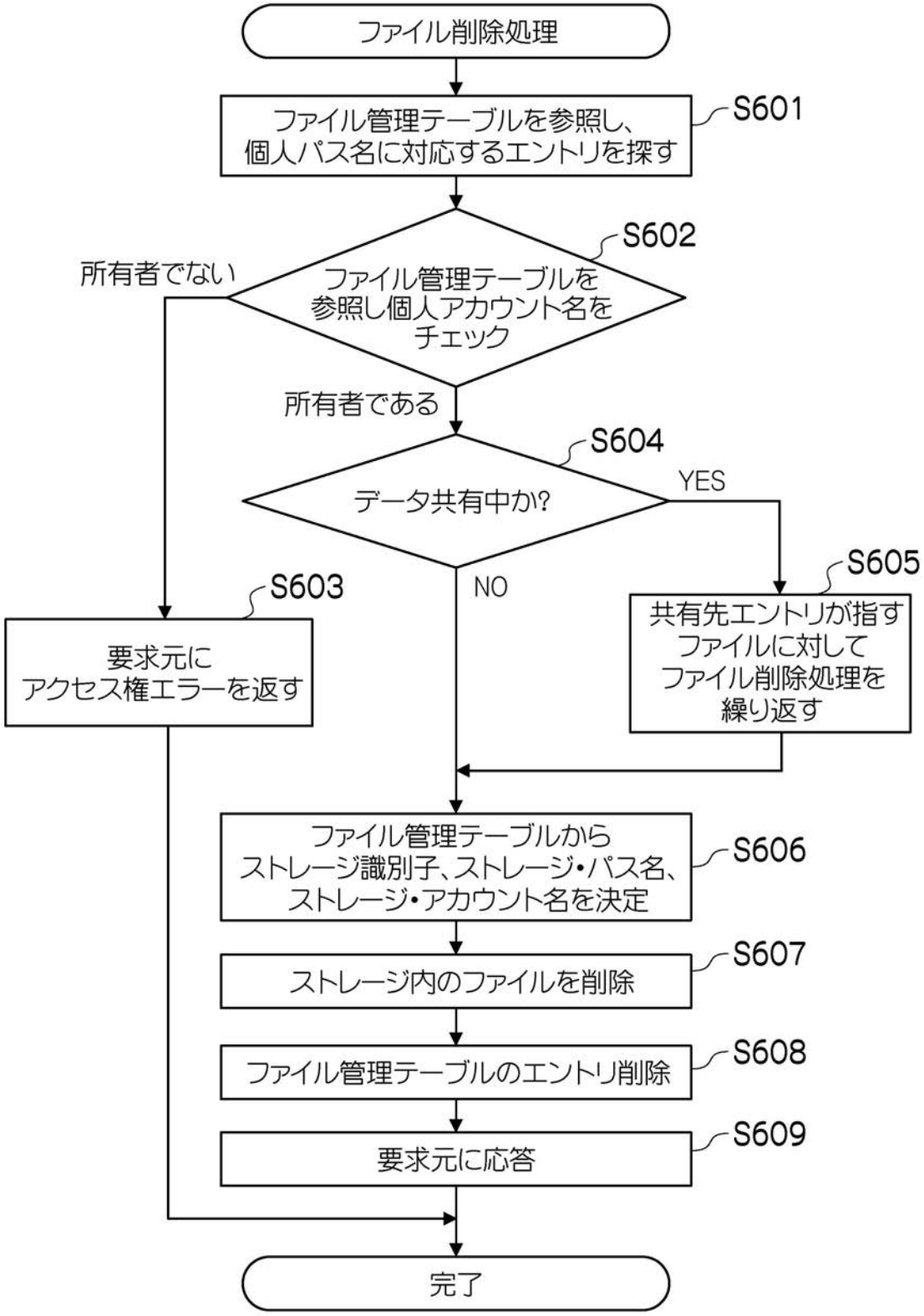

ファイル参照処理
ファイル管理テーブルを参照し、
個人パス名に対応するエントリを探す
S401
ファイル管理テーブルを
参照しアクセス権限を
チェック
S402
ない
ある
S403
要求元に
アクセス権エラーを返す
ファイル管理テーブルから
ストレージ識別子、ストレージ・パス名、
ストレージ・アカウント名を決定
S404
ストレージからファイルをリード
S405
ファイル管理テーブルの
個人用時刻情報を更新
S406
リード・ファイルを要求元に応答
S407
完了

【図２９】
図29


ファイル更新処理
ファイル管理テーブルを参照し、
個人パス名に対応するエントリを探す
S501
S502
ファイル管理テーブル
を参照しアクセス権限を
チェック
ない
ある
S503
要求元に
アクセス権エラーを返す
ファイル管理テーブルから
ストレージ識別子、ストレージ・パス名、
ストレージ・アカウント名を決定
S504
ストレージ内のファイルを
更新データで更新
S505
ファイル管理テーブルの
時刻情報を更新
S506
要求元に応答
S507
完了

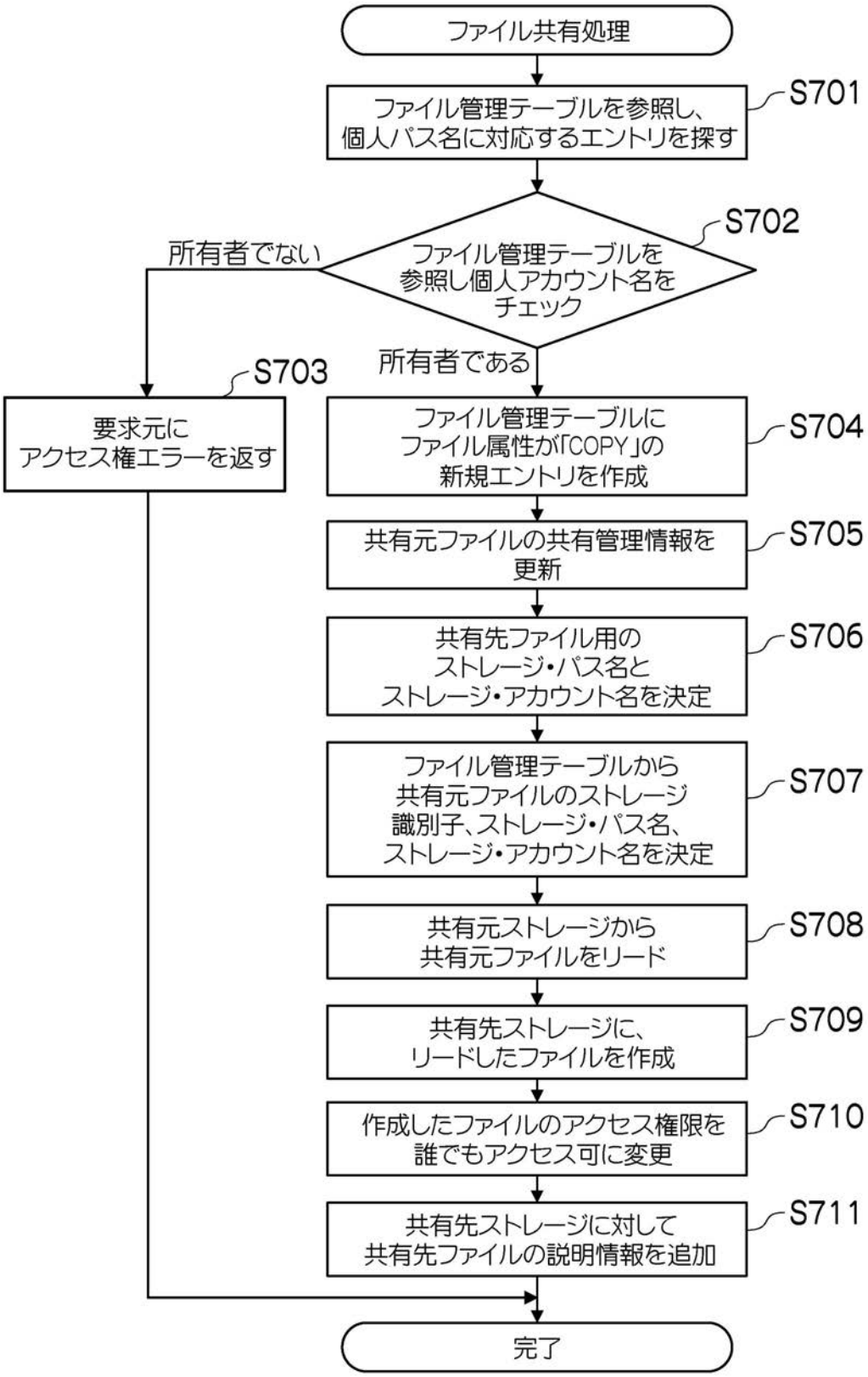
【図３０】

図30

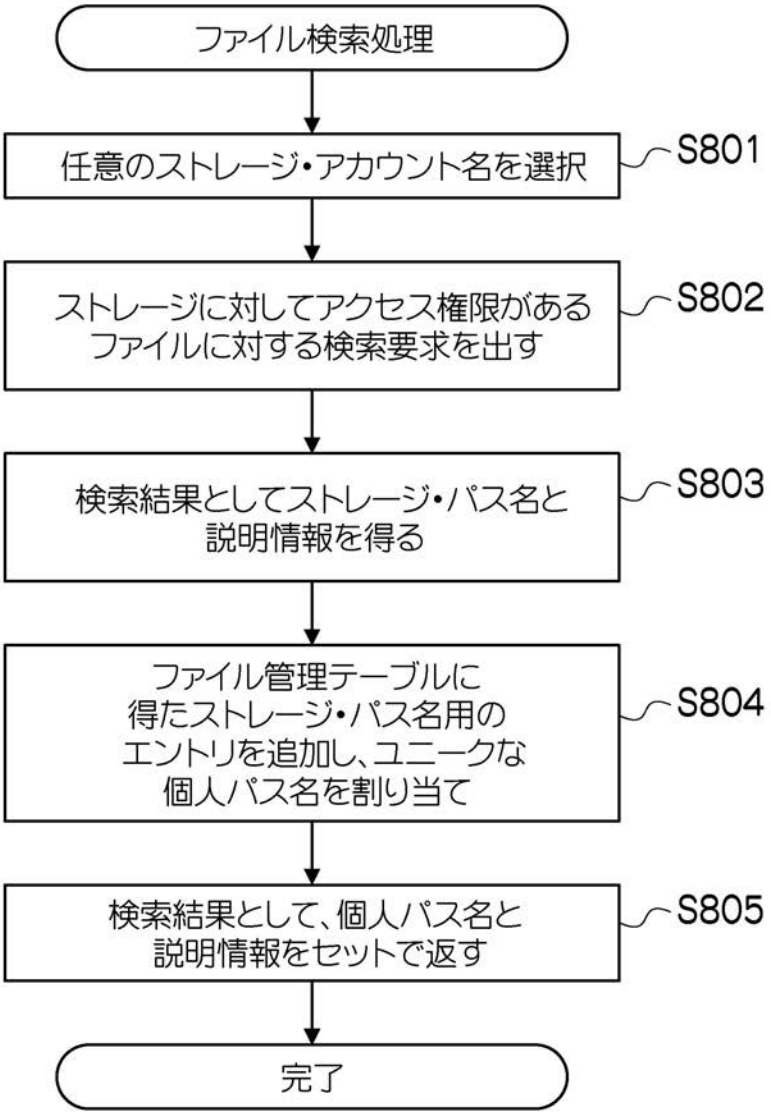

ファイル削除処理
ファイル管理テーブルを参照し、
個人パス名に対応するエントリを探す
S601
ファイル管理テーブルを
参照し個人アカウント名を
チェック
S602
所有者でない
所有者である
データ共有中か?
S604
YES
NO
要求元に
アクセス権エラーを返す
S603
共有先エントリが指す
ファイルに対して
ファイル削除処理を
繰り返す
S605
ファイル管理テーブルから
ストレージ識別子、ストレージ・パス名、
ストレージ・アカウント名を決定
S606
ストレージ内のファイルを削除
S607
ファイル管理テーブルのエントリ削除
S608
要求元に応答
S609
完了

【図３１】

図31

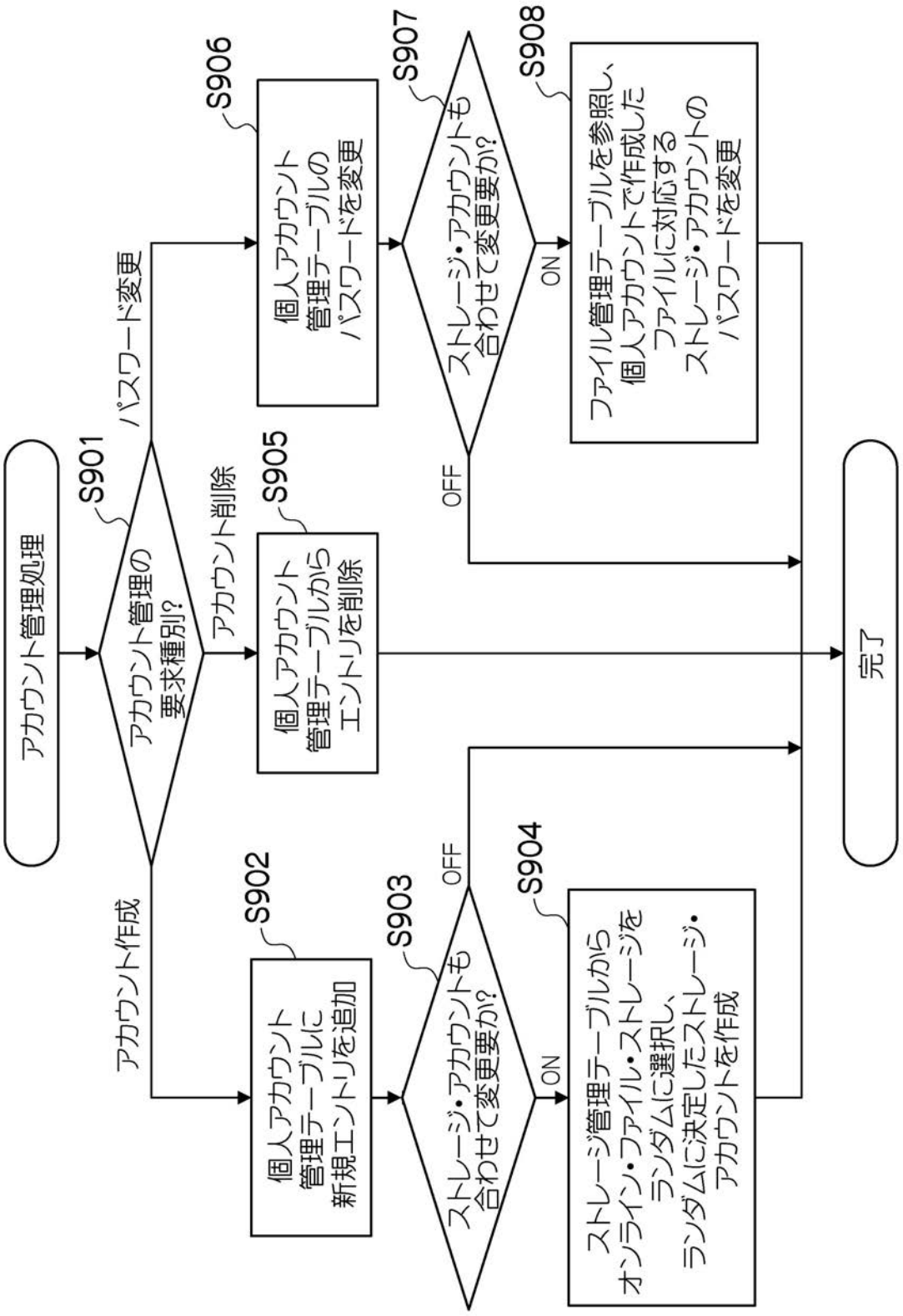

ファイル共有処理
ファイル管理テーブルを参照し、個人パス名に対応するエントリを探す
S701
ファイル管理テーブルを参照し個人アカウント名をチェック
S702
所有者でない
所有者である
S703
要求元にアクセス権エラーを返す
ファイル管理テーブルにファイル属性が「COPY」の新規エントリを作成
S704
共有元ファイルの共有管理情報を更新
S705
共有先ファイル用のストレージ・パス名とストレージ・アカウント名を決定
S706
ファイル管理テーブルから共有元ファイルのストレージ識別子、ストレージ・パス名、ストレージ・アカウント名を決定
S707
共有元ストレージから共有元ファイルをリード
S708
共有先ストレージに、リードしたファイルを作成
S709
作成したファイルのアクセス権限を誰でもアクセス可に変更
S710
共有先ストレージに対して共有先ファイルの説明情報を追加
S711
完了

【図３２】
図32


ファイル検索処理
任意のストレージ・アカウント名を選択
S801
ストレージに対してアクセス権限がある
ファイルに対する検索要求を出す
S802
検索結果としてストレージ・パス名と
説明情報を得る
S803
ファイル管理テーブルに
得たストレージ・パス名用の
エントリを追加し、ユニークな
個人パス名を割り当て
S804
検索結果として、個人パス名と
説明情報をセットで返す
S805
完了

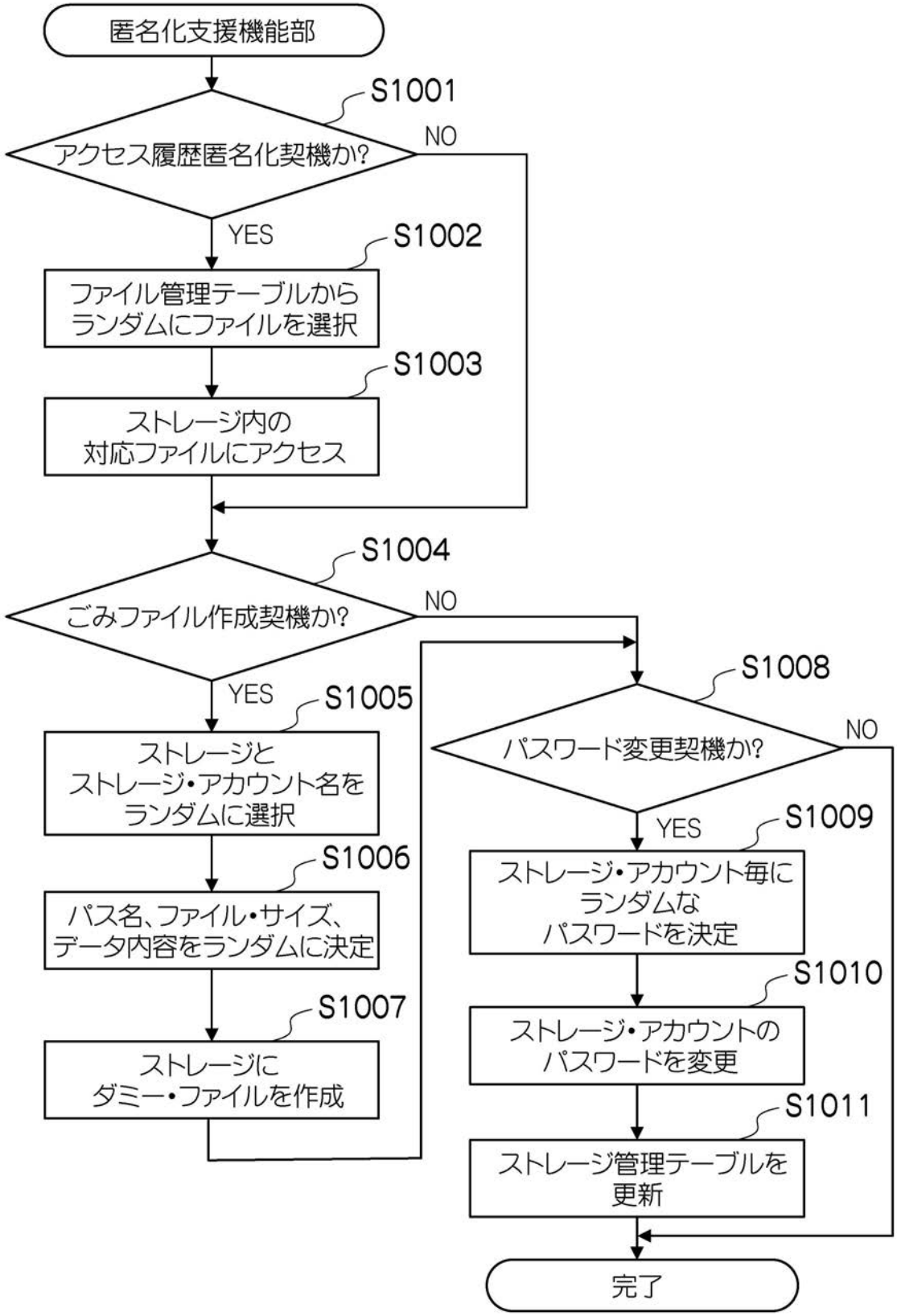
【図３３】

図33

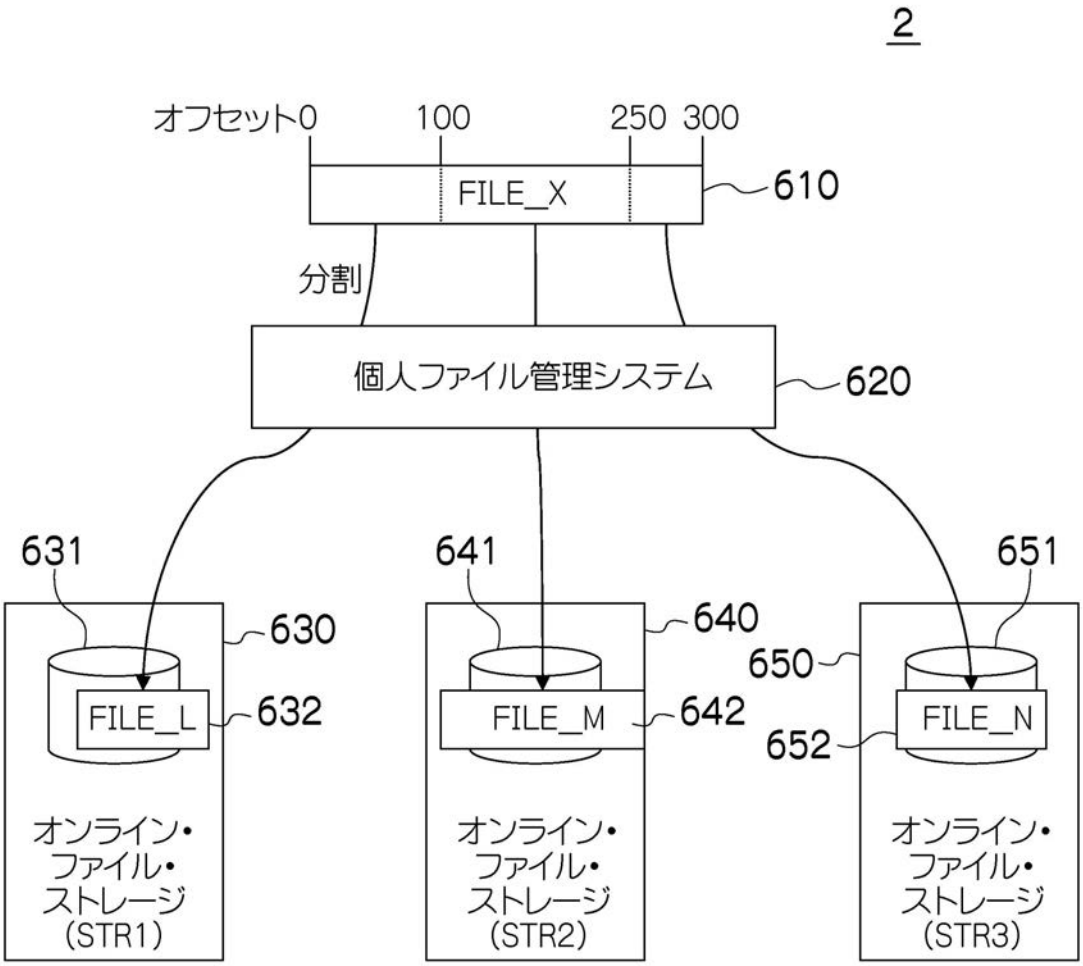

アカウント管理処理
S901
アカウント管理の要求種別?
アカウント作成
パスワード変更
アカウント削除
S902
個人アカウント管理テーブルに新規エントリを追加
S903
ストレージ・アカウントも合わせて変更要か?
OFF
ON
S904
ストレージ管理テーブルからオンライン・ファイル・ストレージをランダムに選択し、ランダムに決定したストレージ・アカウントを作成
S905
個人アカウント管理テーブルからエントリを削除
S906
個人アカウント管理テーブルのパスワードを変更
S907
ストレージ・アカウントも合わせて変更要か?
OFF
ON
S908
ファイル管理テーブルを参照し、個人アカウントで作成したファイルに対応するストレージ・アカウントのパスワードを変更
完了

【図３４】

図34

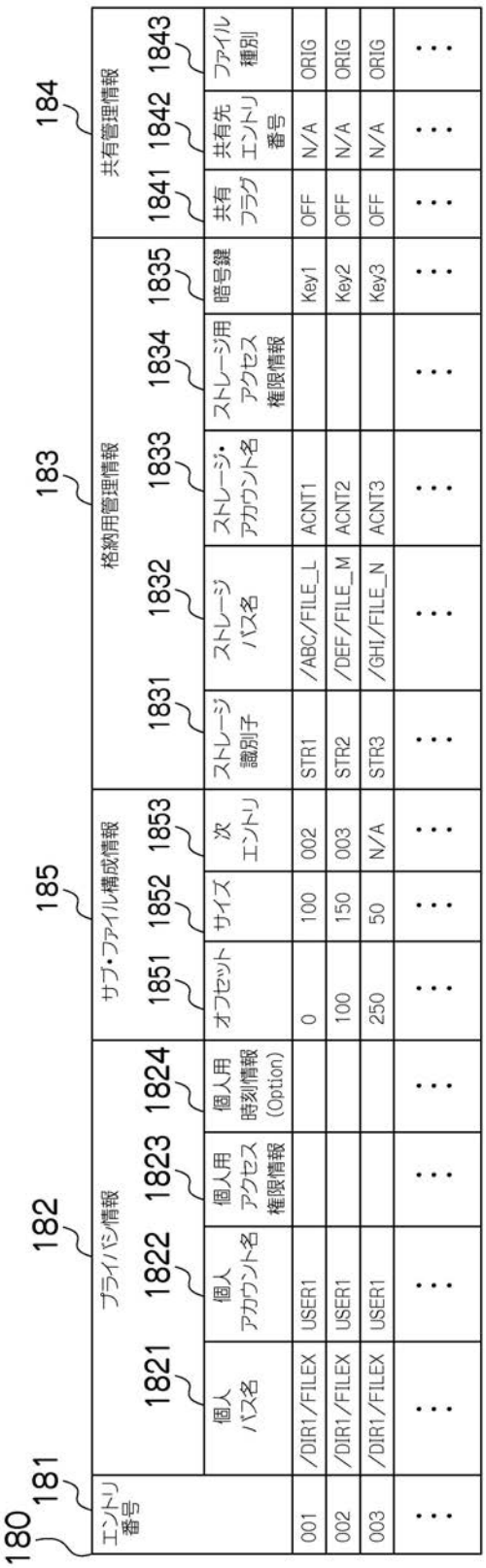

匿名化支援機能部
S1001
アクセス履歴匿名化契機か?
NO
YES
S1002
ファイル管理テーブルから
ランダムにファイルを選択
S1003
ストレージ内の
対応ファイルにアクセス
S1004
ごみファイル作成契機か?
NO
YES
S1005
ストレージと
ストレージ・アカウント名を
ランダムに選択
S1006
パス名、ファイル・サイズ、
データ内容をランダムに決定
S1007
ストレージに
ダミー・ファイルを作成
S1008
パスワード変更契機か?
NO
YES
S1009
ストレージ・アカウント毎に
ランダムな
パスワードを決定
S1010
ストレージ・アカウントの
パスワードを変更
S1011
ストレージ管理テーブルを
更新
完了

【図３５】
図35

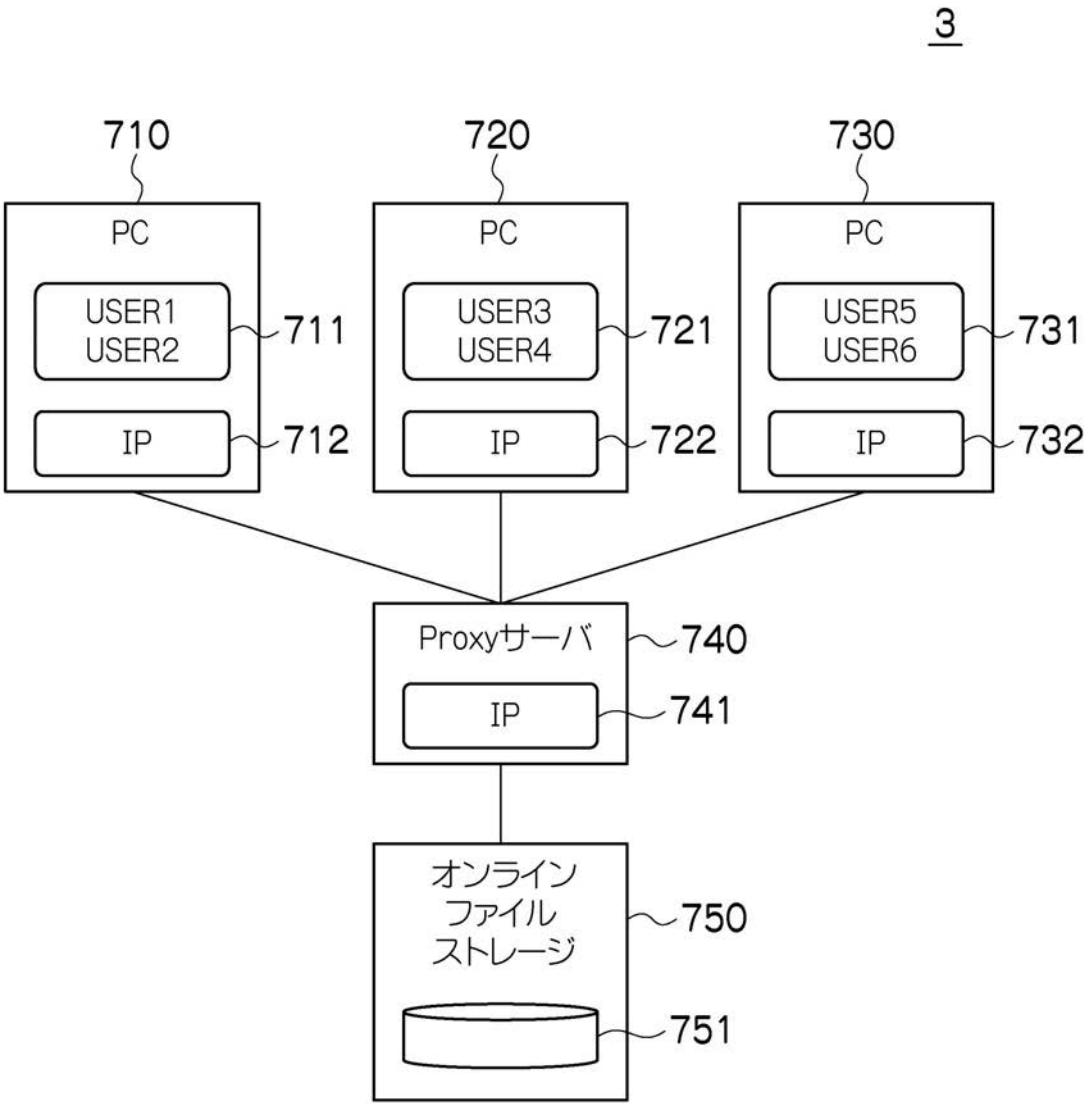

2
オフセット0
100
250
300
FILE_X
610
分割
個人ファイル管理システム
620
631
641
651
630
640
650
FILE_L
632
FILE_M
642
652
FILE_N
オンライン・ファイル・ストレージ (STR1)
オンライン・ファイル・ストレージ (STR2)
オンライン・ファイル・ストレージ (STR3)

【図３６】

図36


180
181
182
183
184
185
エントリ番号
プライバシ情報
格納用管理情報
共有管理情報
サブ・ファイル構成情報
1821 個人パス名
1822 個人アカウント名
1823 個人用アクセス権限情報
1824 個人用時刻情報(Option)
1831 ストレージ識別子
1832 ストレージパス名
1833 ストレージ・アカウント名
1834 ストレージ用アクセス権限情報
1835 暗号鍵
1841 共有フラグ
1842 共有先エントリ番号
1843 ファイル種別
1851 オフセット
1852 サイズ
1853 次エントリ
001 /DIR1/FILEX USER1 0 100 002 STR1 /ABC/FILE_L ACNT1 Key1 OFF N/A ORIG
002 /DIR1/FILEX USER1 100 150 003 STR2 /DEF/FILE_M ACNT2 Key2 OFF N/A ORIG
003 /DIR1/FILEX USER1 250 50 N/A STR3 /GHI/FILE_N ACNT3 Key3 OFF N/A ORIG

【図３７】
図37


3
710
720
730
PC
PC
PC
USER1
USER2
711
USER3
USER4
721
USER5
USER6
731
IP
712
IP
722
IP
732
Proxyサーバ
740
IP
741
オンライン
ファイル
ストレージ
750
751

フロントページの続き

(72)発明者　上村　哲也
東京都国分寺市東恋ヶ窪１丁目２８０番地　株式会社日立製作所中央研究所内

審査官　和田　財太

(56)参考文献　特開２００２－０３２３７２（ＪＰ，Ａ）
特開平０８－０８７４５４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４