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

特許第4927583号
(P4927583)

(45)発行日　平成24年5月9日(2012.5.9)　(24)登録日　平成24年2月17日(2012.2.17)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	21/24	165C
G06F 13/00	(2006.01)	G06F	13/00	510A
G06F 12/00	(2006.01)	G06F	12/00	537D

請求項の数 14　(全 21 頁)

(21)出願番号　特願2007-29681(P2007-29681)
(22)出願日　平成19年2月8日(2007.2.8)
(65)公開番号　特開2008-197746(P2008-197746A)
(43)公開日　平成20年8月28日(2008.8.28)
審査請求日　平成22年2月8日(2010.2.8)

(73)特許権者　000104652
キヤノン電子株式会社
埼玉県秩父市下影森１２４８番地
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　中山　いずみ
埼玉県秩父市下影森１２４８番地

審査官　児玉　崇晶

最終頁に続く

(54)【発明の名称】ファイル共有システム、ファイル共有方法、サーバ及びコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
複数のコンピュータ間でサーバを介してファイルを共有するファイル共有システムであって、
第１コンピュータに備えられる手段であって、共有の対象となるファイルを指定する指定手段と、
前記サーバに備えられる手段であって、指定された前記ファイルにアクセスするために必要となるアクセスプログラムを生成するプログラム生成手段と、
前記第１コンピュータに備えられる手段であって、生成された前記アクセスプログラムを、前記ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスプログラムが起動されることで実現される手段であって、前記受信コンピュータに付与された固有の識別情報を取得する取得手段と、取得した前記識別情報を伴うアクセス要求をサーバへ送信するアクセス要求送信手段と、前記アクセス要求が正当なアクセス要求である場合に前記サーバから送信される前記ファイルを受信するファイル受信手段と、
前記サーバに備えられる手段であって、前記受信コンピュータから送信された前記識別情報から認証用のパスワードを生成するパスワード生成手段と、予め前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、前記生成されたパスワードと前記保持手段に保持さ

れているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を含むことを特徴とするファイル共有システム。
【請求項２】
前記サーバは、前記アクセスプログラムによる前記アクセス要求が前記ファイルに対する初回のアクセス要求であるか否かを判定する判定手段をさらに備え、
前記保持手段は、前記判定手段により前記アクセス要求が初回のアクセス要求であると判定されると、前記パスワード生成手段により生成された前記パスワードを、前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードとして保持する
ことを特徴とする請求項１に記載のファイル共有システム。
【請求項３】
前記識別情報は、前記受信コンピュータのＭＡＣアドレス、ドメイン名、前記受信コンピュータ上で稼働しているＯＳのビルドナンバー、該ＯＳのライセンスナンバー、前記受信コンピュータにログオンしているユーザのユーザＩＤのうち少なくとも１つを含むことを特徴とする請求項１又は２に記載のファイル共有システム。
【請求項４】
前記サーバは、前記パスワードが生成されると、前記受信コンピュータから受信した前記識別情報を消去する消去手段をさらに含むことを特徴とする請求項１乃至３のいずれか１項に記載のファイル共有システム。
【請求項５】
前記転送手段は、電子メールに前記アクセスプログラムを添付して送信する電子メール送信手段を含むことを特徴とする請求項１乃至４のいずれか１項に記載のファイル共有システム。
【請求項６】
前記プログラム生成手段は、
前記アクセスプログラムを他のアクセスプログラムと区別するためのアクセスプログラムＩＤを発行する発行手段と、該アクセスプログラムＩＤと前記ファイルとを対応付けて管理する管理テーブルと
を備え、
前記アクセス要求送信手段は、前記アクセスプログラムから前記アクセスプログラムＩＤを抽出して、前記アクセス要求とともに前記サーバへ送信し、
前記保持手段は、前記アクセス要求とともに受信した前記アクセスプログラムＩＤに基づいて前記管理テーブルを検索することで、前記アクセスプログラムＩＤに対応するファイルを特定し、特定された該ファイルのファイルＩＤとともに前記パスワードを保持することを特徴とする請求項１乃至５のいずれか１項に記載のファイル共有システム。
【請求項７】
前記アクセス要求送信手段は、
前記アクセスプログラムに含まれる、前記ファイルに対する初回のアクセスか否か判定するためのフラグを前記アクセス要求とともに送信し、
前記サーバは、
前記アクセス要求と共に受信した前記フラグに基づいて前記判定手段により前記アクセス要求が初回のアクセス要求と判定されると、前記アクセスプログラムを実行している前記受信コンピュータへ前記フラグを書き換えるよう指示する指示手段をさらに含み、
前記受信コンピュータは、
前記フラグを書き換えるよう指示されると、前記フラグの内容を初回のアクセスではないことを表すように書き換える書き換え手段を
含むこと特徴とする請求項２乃至６のいずれか１項に記載のファイル共有システム。
【請求項８】

複数のコンピュータ間でサーバを介してファイルを共有するファイル共有方法であって、
第１コンピュータが、共有の対象となるファイルを指定する指定工程と、
前記サーバが、指定された前記ファイルに第２コンピュータがアクセスするために必要となるアクセスプログラムを生成するプログラム生成工程と、
前記第１コンピュータが、生成された前記アクセスプログラムを、前記ファイルを共有することになる前記第２コンピュータへ転送する転送工程と、
前記第２コンピュータが、前記アクセスプログラムを起動する起動工程と、
前記第２コンピュータが、該第２コンピュータに付与された固有の識別情報を取得する取得工程と、
前記第２コンピュータが、取得した前記識別情報を伴うアクセス要求を前記サーバへ送信するアクセス要求送信工程と、
前記サーバが、前記第２コンピュータから送信された前記識別情報から認証用のパスワードを生成するパスワード生成工程と、
前記サーバが、予め前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードを保持する保持工程と、
前記サーバが、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致するか否かに応じて認証処理を実行する認証工程と、
前記サーバが、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致しなければ前記ファイルに対する前記第２コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致すれば前記ファイルに対する前記第２コンピュータからのアクセスを許可する許可工程と
を含むことを特徴とするファイル共有方法。
【請求項９】
複数のコンピュータ間でファイルを共有させるためのサーバであって、
共有対象となるファイルにアクセスするために必要となるアクセスプログラムを生成するプログラム生成手段と、
生成された前記アクセスプログラムを、前記共有対象となるファイルを指定した第１コンピュータを介して、該ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスプログラムが実行されると、前記受信コンピュータに付与された固有の識別情報を伴うアクセス要求を受信するアクセス要求受信手段と、
前記受信コンピュータから送信された識別情報から認証用のパスワードを生成するパスワード生成手段と、
予め前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を含むことを特徴とするサーバ。
【請求項１０】
複数のコンピュータ間でファイルを共有させるためのサーバで実行されるコンピュータプログラムであって、
共有対象となるファイルにアクセスするために必要となるアクセスプログラムを生成するプログラム生成手段と、
生成された前記アクセスプログラムを、前記共有対象となるファイルを指定した第１コ

ンピュータを介して、該ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスプログラムが実行されると、前記受信コンピュータに付与された固有の識別情報を伴うアクセス要求を受信するアクセス要求受信手段と、
前記受信コンピュータから送信された識別情報から認証用のパスワードを生成するパスワード生成手段と、
予め前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を前記サーバに機能させることを特徴とするコンピュータプログラム。
【請求項１１】
複数のコンピュータ間でサーバを介してファイルを共有するファイル共有システムであって、
第１コンピュータに備えられる手段であって、共有の対象となるファイルを指定する指定手段と、
前記サーバに備えられる手段であって、指定された前記ファイルにアクセスするために必要となるアクセスするための情報を生成する情報生成手段と、
前記第１コンピュータに備えられる手段であって、生成された前記アクセスするための情報を、前記ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスするための情報が起動されることで実現される手段であって、前記受信コンピュータに付与された固有の識別情報を取得する取得手段と、取得した前記識別情報を伴うアクセス要求をサーバへ送信するアクセス要求送信手段と、前記アクセス要求が正当なアクセス要求である場合に前記サーバから送信される前記ファイルを受信するファイル受信手段と、
前記サーバに備えられる手段であって、前記受信コンピュータから送信された前記識別情報から認証用のパスワードを生成するパスワード生成手段と、予め前記アクセスするための情報を通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を含むことを特徴とするファイル共有システム。
【請求項１２】
複数のコンピュータ間でサーバを介してファイルを共有するファイル共有方法であって、
第１コンピュータが、共有の対象となるファイルを指定する指定工程と、
前記サーバが、指定された前記ファイルに第２コンピュータがアクセスするために必要となるアクセスするための情報を生成する情報生成工程と、
前記第１コンピュータが、生成された前記アクセスするための情報を、前記ファイルを共有することになる前記第２コンピュータへ転送する転送工程と、
前記第２コンピュータが、前記アクセスするための情報にしたがって、該第２コンピュータに付与された固有の識別情報を取得する取得工程と、

前記第２コンピュータが、取得した前記識別情報を伴うアクセス要求を前記サーバへ送信するアクセス要求送信工程と、
前記サーバが、前記第２コンピュータから送信された前記識別情報から認証用のパスワードを生成するパスワード生成工程と、
前記サーバが、予め前記アクセスするための情報を通じて前記ファイルにアクセスする際のパスワードを保持する保持工程と、
前記サーバが、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致するか否かに応じて認証処理を実行する認証工程と、
前記サーバが、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致しなければ前記ファイルに対する前記第２コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持工程により保持されたパスワードとが一致すれば前記ファイルに対する前記第２コンピュータからのアクセスを許可する許可工程と
を含むことを特徴とするファイル共有方法。

【請求項１３】
複数のコンピュータ間でファイルを共有させるためのサーバであって、
共有対象となるファイルにアクセスするために必要となるアクセスするための情報を生成する情報生成手段と、
生成された前記アクセスするための情報を、前記共有対象となるファイルを指定した第１コンピュータを介して、該ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスするための情報にしたがって、前記受信コンピュータに付与された固有の識別情報を伴うアクセス要求を受信するアクセス要求受信手段と、
前記受信コンピュータから送信された識別情報から認証用のパスワードを生成するパスワード生成手段と、
予め前記アクセスするための情報を通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を含むことを特徴とするサーバ。

【請求項１４】
複数のコンピュータ間でファイルを共有させるためのサーバで実行されるコンピュータプログラムであって、
共有対象となるファイルにアクセスするために必要となるアクセスするための情報を生成する情報生成手段と、
生成された前記アクセスするための情報を、前記共有対象となるファイルを指定した第１コンピュータを介して、該ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスするための情報にしたがって、前記受信コンピュータに付与された固有の識別情報を伴うアクセス要求を受信するアクセス要求受信手段と、
前記受信コンピュータから送信された識別情報から認証用のパスワードを生成するパスワード生成手段と、
予め前記アクセスするための情報を通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか

否かに応じて認証処理を実行する認証手段と、
前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を前記サーバに機能させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数のコンピュータ間でサーバを介してファイルを共有するファイル共有技術に関する。
【背景技術】
【０００２】
社内あるいは企業間で情報を共有する手段として従来から用いられているツールとして電子メールがある。電子メールは、ファイルを電子メールに添付し、共有したい相手のメールアドレス宛てに送信することで情報を共有することのできる便利なツールである。しかし電子メール送受信による情報共有には数々の問題点が存在する。セキュリティ上の問題としては、送信時に第三者に傍受される可能性、ファイル受信者による第三者への漏洩の可能性がある。また、複数ユーザにファイルを送信する際に、メールサーバで宛先数の分だけファイルのコピーを作成することによるメールサーバ負荷の問題がある。さらに、送信したファイルが受信者により改変された状態又は情報が古いままの状態で別のユーザにファイルが送信されてしまうことによる情報の完全性喪失の問題もある。
【０００３】
非特許文献１のサービスは、メールの送受信経路及びデータ自体を暗号化することにより送信者と受信者間の安全なファイル交換を実現するものである。特許文献１に記載の発明は、ファイル本体をユーザに提供せずに、ファイルにアクセスするためのラベル情報のみを電子メールで送信し、認証されたユーザのみ閲覧ツールを用いてファイルを閲覧させる、というものである。
【非特許文献１】ＮＲＩセキュアテクノロジーズ株式会社「クリプト便」＜ＵＲＬ　ｈｔｔｐ：／／ｗｗｗ．ｎｒｉ－ｓｅｃｕｒｅ．ｃｏ．ｊｐ／ｓｅｒｖｉｃｅ／ｃｒｙｐｔｏ／ｉｎｄｅｘ．ｈｔｍｌ＞
【特許文献１】特開２００５－２６７３７９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
非特許文献１の技術によれば、暗号化通信によりメールが傍受されて第三者に漏洩する可能性は回避できるであろう。しかし、受信者が復号したファイルを送信者の意図しない第三者に送信すれば、情報が漏洩してしまう。また特許文献１に記載の発明は、悪意のない利用者による漏洩は防止できるであろう。しかし、悪意のある利用者がファイル閲覧用のプログラムを第三者に転送し、パスワードを教えてしまえば、情報が漏洩してしまう。
【０００５】
また、非特許文献１及び特許文献１によるファイル共有技術には、送信者によるメールシステムの変更、送信相手のパスワード設定とその配布、という作業が伴う。また、受信者はパスワードの記憶、閲覧用プログラムのインストール、パスワードの入力、など非常に厄介な作業が伴う。そのため、送信者、受信者ともに作業負担が重かった。
【０００６】
そこで、本発明は、これらの課題又は他の課題のうち少なくとも１つを解決することを目的とする。例えば、本発明の１つは、送信者及び受信者の負荷が少なく、かつ、情報漏洩の可能性を低減したファイル共有方法を提供することを目的とする。なお、他の課題や目的については、明細書及び図面の全体から理解できるであろう。

【課題を解決するための手段】
【０００７】
上記目的を達成するために、本発明は、例えば、複数のコンピュータ間でサーバを介してファイルを共有するファイル共有システム、ファイル共有方法、サーバ及びコンピュータとして実現されうる。
【０００８】
例えば、ファイル共有システムは、
複数のコンピュータ間でサーバを介してファイルを共有するファイル共有システムであって、
第１コンピュータに備えられる手段であって、共有の対象となるファイルを指定する指定手段と、
前記サーバに備えられる手段であって、指定された前記ファイルにアクセスするために必要となるアクセスプログラムを生成するプログラム生成手段と、
前記第１コンピュータに備えられる手段であって、生成された前記アクセスプログラムを、前記ファイルを共有することになる受信コンピュータへ転送する転送手段と、
前記受信コンピュータにおいて前記アクセスプログラムが起動されることで実現される手段であって、前記受信コンピュータに付与された固有の識別情報を取得する取得手段と、取得した前記識別情報を伴うアクセス要求をサーバへ送信するアクセス要求送信手段と、前記アクセス要求が正当なアクセス要求である場合に前記サーバから送信される前記ファイルを受信するファイル受信手段と、
前記サーバに備えられる手段であって、前記受信コンピュータから送信された前記識別情報から認証用のパスワードを生成するパスワード生成手段と、予め前記アクセスプログラムを通じて前記ファイルにアクセスする際のパスワードを保持する保持手段と、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致するか否かに応じて認証処理を実行する認証手段と、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致しなければ前記ファイルに対する前記受信コンピュータからのアクセスを拒否し、前記生成されたパスワードと前記保持手段に保持されているパスワードとが一致すれば前記ファイルに対する前記受信コンピュータからのアクセスを許可する許可手段と
を含むことを特徴とする。
【０００９】
また、上記ファイル共有システムは、
前記識別情報は、前記受信コンピュータのＭＡＣアドレス、ドメイン名、前記受信コンピュータ上で稼働しているＯＳのビルドナンバー、該ＯＳのライセンスナンバー、前記受信コンピュータにログオンしているユーザのユーザＩＤのうち少なくとも１つを含むように構成されてもよい。
【００１０】
また、上記ファイル共有システムは、
前記パスワードが生成されると、前記受信コンピュータから受信した前記識別情報を消去する消去手段をさらに含むように構成されてもよい。
【００１１】
また、上記ファイル共有システムは、
前記転送手段は、電子メールに前記アクセスプログラムを添付して送信する電子メール送信手段を含むことを特徴とする請求項１乃至３のいずれか１項に記載のファイル共有システム。
【００１２】
また、上記ファイル共有システムは、
前記プログラム生成手段が、前記アクセスプログラムを他のアクセスプログラムと区別するためのアクセスプログラムＩＤを付与し、該アクセスプログラムＩＤと前記ファイルとを対応付けて管理する管理テーブルを備え、

前記アクセス要求送信手段が、前記アクセスプログラムから前記アクセスプログラムＩＤを抽出して、前記アクセス要求とともに前記サーバへ送信し、
前記保持手段は、前記アクセス要求とともに受信した前記アクセスプログラムＩＤに基づいて前記管理テーブルを検索することで、前記アクセスプログラムＩＤに対応するファイルを特定し、特定された該ファイルのファイルＩＤとともに前記パスワードを保持するように構成されてもよい。

【００１３】

また、上記ファイル共有システムは、
前記アクセス要求送信手段が、
前記アクセスプログラムに含まれる、前記ファイルに対する初回のアクセスか否かを認識するためのフラグを前記アクセス要求とともに送信し、
前記サーバが、
前記アクセス要求と共に受信した前記フラグに基づいて前記判定手段により前記アクセス要求が初回のアクセス要求と判定されると、前記アクセスプログラムを実行している前記受信コンピュータへ前記フラグを書き換えるよう指示する指示手段をさらに含み、
前記受信コンピュータが、
前記フラグを書き換えるよう指示されると、前記フラグの内容を初回のアクセスではないことを表すように書き換える書き換え手段を
含むように構成されてもよい。

【発明の効果】

【００１４】

本発明によれば、例えば、送信者及び受信者の負荷が少なく、かつ、情報漏洩の可能性を低減したファイル共有方法等を実現可能となる。すなわち、送信者はアクセスプログラムを受信者に送信するだけで済む利点がある。また、受信者は、アクセスプログラムを実行することで、送信者の指定したファイルにアクセスできるため、従来よりも作業負担が緩和される。また、送信者から受信者へファイルが直接送信されることはないため、漏洩の可能性も低減される。

【００１５】

また、本発明によれば、受信者のコンピュータに付与された固有の情報からパスワードが作成される。よって、仮に、アクセスプログラムが第三者に転送されたとしても、第三者によるアクセス要求により作成されるパスワードは正当なパスワードとは異なることになり、情報漏洩が抑制される。また、パスワードはサーバ内で作成され保持されているため、パスワード自体が流出することもない。

【００１６】

さらに、本発明によれば、パスワードの作成に使用された識別情報は、パスワードの作成後にサーバから消去されるため、この識別情報がサーバから流出する可能性も低減される。

【００１７】

また、本発明によれば、アクセスプログラムを転送するために、広く普及した電子メールを利用できるため、送信者や受信者の負担が軽減される。

【００１８】

また、本発明によれば、各受信者に提供されるアクセスプログラムに区別のためのアクセスプログラムＩＤを付与することで、単一のファイルを同時に複数の受信者に共有させることも可能となる。

【００１９】

また、本発明によれば、ファイルに対するアクセスが初回か否かを管理するためのフラグを導入することで、初回のアクセスを行った受信者について生成されたパスワードを正当なパスワードとして保持できる利点がある。これは、一般に、ファイルに対して初回にアクセスしてくる受信者は正当な受信者であり、正当な受信者よりも先に不正な第三者がアクセスしてくることは極めて稀であるという事実に則している。

【発明を実施するための最良の形態】
【００２０】
以下、添付図面を参照して、本発明の好適な実施の形態を詳細に説明する。図１は、実施形態に係るファイル共有システムの概要を示す図である。サーバ１０１は、複数のコンピュータ（送信コンピュータ１０２、受信コンピュータ１０３）間でファイルを共有させるためのコンピュータ（情報処理装置）である。ここでは、サーバ１０１の管理下にあるファイルのうち、送信コンピュータ１０２により指定されたファイルについてアクセスプログラムが作成される。アクセスプログラムは、送信コンピュータ１０２を介して受信コンピュータ１０３へ送信される。そして、受信コンピュータ１０３は起動したアクセスプログラムにしたがってファイルにアクセスする。よって、アクセスプログラムを有しない非所望コンピュータ１０４は、ファイルに対してアクセスすることはできない。
【００２１】
図２は、実施形態に係るファイル共有についてのシーケンス図である。ステップＳ２０１で、送信コンピュータは、共有の対象となるファイルを指定する。この際に、ファイルの開示期限が送信コンピュータ１０２からサーバ１０１へ通知されてもよい。ステップＳ２０２で、サーバ１０１は、指定されたファイルにアクセスするために必要となるアクセスプログラムを生成し、送信コンピュータ１０２へ送信する。
【００２２】
ステップＳ２０３で、送信コンピュータ１０２は、サーバ１０１から受信したアクセスプログラムを、ファイルを共有することになる受信コンピュータ１０３へ転送する。ステップＳ２０４で、受信コンピュータ１０３は、送信コンピュータ１０２から受信したアクセスプログラムを起動する。
【００２３】
ステップＳ２０５で、受信コンピュータ１０３は、自己に付与された固有の識別情報を取得する。識別情報は、例えば、受信コンピュータのＭＡＣアドレス、ドメイン名、受信コンピュータ上で稼働しているＯＳのビルドナンバー、ＯＳのライセンスナンバー、受信コンピュータにログオンしているユーザのユーザＩＤなどである。そして、受信コンピュータ１０３は、取得した識別情報を伴うアクセス要求をサーバ１０１へ送信する。
【００２４】
ステップＳ２０６で、サーバ１０１は、受信コンピュータ１０３から送信された識別情報から認証用のパスワードを生成する。受信コンピュータ１０３からのアクセスが初回のアクセスであれば、このとき作成されたパスワードがこれ以降のアクセスの際におけるパスワードとしてサーバ１０１に保持されることになる。初回のアクセスでなければ、今回のアクセスにより生成されたパスワードと、初回のアクセスにより生成されたパスワードとを比較することで、認証処理が実行される。
【００２５】
認証が成功した場合、ステップＳ２０７で、サーバ１０１は、受信コンピュータ１０３に対して共有対象ファイルへのアクセスを許可する。ステップＳ２０８で、受信コンピュータ１０３は、ファイルにアクセスして当該ファイルを受信し、ファイルの内容を表示する。なお、受信コンピュータ１０３においてファイルを保存する行為はアクセスプログラムによって禁止される。すなわち、ファイルは、キャッシュなどに一時的に記憶され、アクセスプログラムが終了する際には消去されることになる。
【００２６】
ところで、非所望コンピュータ１０４にアクセスプログラムが転送されたとしても、ファイルへのアクセスは拒否される。ステップＳ２１３で、受信コンピュータ１０３がアクセスプログラムを非所望コンピュータ１０４へ転送する。ステップＳ２１４で、非所望コンピュータ１０４がアクセスプログラムを起動する。ステップＳ２１５で、非所望コンピュータ１０４はアクセスプログラムにしたがって、非所望コンピュータ１０４の識別情報を伴うアクセス要求をサーバ１０１へ送信する。
【００２７】

ステップＳ２１６で、サーバ１０１は、非所望コンピュータ１０４の識別情報からパスワードを生成し、あらかじめ保持されているパスワードと比較する。ここで、双方のパスワードは一致しないため、ステップＳ２１７で、サーバ１０１は、非所望コンピュータ１０４からのファイルへのアクセスを拒否する。ステップＳ２１８で、非所望コンピュータ１０４はアクセスプログラムにしたがって、エラーメッセージを出力する。

【００２８】

図３は、本発明の一実施の形態に係るファイル共有システムを示すブロック図である。なお、各部は、ＣＰＵ、ＲＡＭ、ＡＳＩＣなどのハードウエア、コンピュータプログラムなどのソフトウエアによって実現可能である。

【００２９】

送信コンピュータ１０２は、共有対象となるファイルを指定する指定部３００と、アクセスプログラムを受信コンピュータ１０３へ転送する転送部３０１を備えている。

【００３０】

サーバ１０１は、ファイルを格納するファイル格納部３０２と、ファイル情報を格納するファイル情報データベース３０３と、アクセスプログラム生成部３０５と、パスワード生成部３０６とを備えている。さらに、サーバ１０１は、認証制御部３０７と、ファイル情報の要求があった場合に該当するファイル情報を返すファイル情報管理部３０４とを備えている。また、サーバ１０１は、認証制御部３０７の結果により、受信コンピュータ１０３からのファイルアクセスを許可するアクセス制御部３０８を備えている。

【００３１】

受信コンピュータ１０３は、送信コンピュータ１０２から電子メールで受信したアクセスプログラム３１１を保持している。アクセスプログラムは、受信コンピュータ１０３上で各種の手段を実現するためのプログラムモジュールを備えている。実現される手段としては、例えば、ＩＤ取得部３１２、ファイル閲覧部３１３及びアクセス記憶部３１４などがある。ＩＤ取得部３１２は、受信コンピュータ１０３のＩＤを取得する。ファイル閲覧部３１３は、ファイルにアクセスしてファイル内容を表示する。アクセス記憶部３１４は、受信者が初回アクセスを実行した事実をフラグに記憶する。なお、アクセスプログラムは、ファイルを表示するためのコンピュータプログラムであり、ファイルを表示するのみで保存機能（上書き保存、別名保存など）を持たないようすることが好ましい。これは、ファイルのコピーが漏洩するのを防止するためである。

【００３２】

ファイルを共有する場合、送信コンピュータ１０２は、ファイル格納部３０２に格納されているファイルのうち、共有化したいファイルを１つ以上指定する。例えば、送信コンピュータ１０２がサーバ１０１にアクセスすると、サーバ１０１はメニューダイアログ（例：Ｗｅｂページ）を提供する。メニューダイアログからは、ファイルのアップロード（格納処理）、共有対象ファイルの指定などを選択できるようになっている。共有対象ファイルの指定が選択されると、サーバ１０１は、ファイルの選択画面を送信コンピュータ１０２に提供し、送信コンピュータ１０２はポインティングデバイスなどから入力される情報にしたがって共有対象ファイルを指定する。

【００３３】

ファイル情報管理部３０４は、ファイル情報データベース３０３から、指定されたファイルのファイルＩＤを取得する。さらに、ファイル情報管理部３０４は、取得したファイルＩＤを伴うアクセスプログラム生成要求をアクセスプログラム生成部３０５に対して送出する。

【００３４】

図４は、実施形態に係るアクセスプログラム生成要求の一例を示す図である。アクセスプログラム生成要求４０１は、例えば、ファイルＩＤを備えている。

【００３５】

アクセスプログラム生成部３０５は、アクセスプログラム生成要求を受信すると、アクセスプログラムＩＤを発行する。アクセスプログラム生成部３０５は、アクセスプログラ

ムＩＤを内包したアクセスプログラムを生成する。なお、アクセスプログラム生成部３０５は、送信コンピュータ１０２に対して開示期限を問い合せてもよい。送信コンピュータ１０２は、送信者がキーボードなどから入力した開示期限のデータをアクセスプログラム生成部３０５へ送信する。開示期限は、後述するように、アクセスプログラム生成部３０５によってファイル情報管理テーブルに登録される。

【００３６】

図５は、実施形態に係るアクセスプログラムに搭載される情報の一例を示す図である。今回生成したアクセスプログラムを他のアクセスプログラムと区別するためのアクセスプログラムＩＤ、アクセス管理フラグを含む。アクセス管理フラグは、受信コンピュータ１０３がアクセスプログラムを用いてサーバ１０１へアクセス済みかどうかを示す情報である。受信コンピュータからアクセスがまだ行われていない場合、フラグの値はＦＡＬＳＥである。これはサーバ１０１にパスワードがまだ登録されていない状態であることを示す。既に受信コンピュータ１０３が共有対象ファイルにアクセスをしたことがある場合、フラグの値はＴＲＵＥとなる。すなわち、アクセスプログラム３１１は、初回のアクセスの際に、初回のアクセスではないことを表すよう、ＦＡＬＳＥからＴＲＵＥへとフラグの内容を書き換える。なお、ＴＲＵＥは、サーバ１０１にパスワードが既に登録済みであることを示す。もちろん、アクセスプログラム生成部３０５で生成された直後のアクセスプログラムは、アクセス管理フラグの値がＦＡＬＳＥに設定されている。

【００３７】

なお、送信コンピュータ１０２が複数のファイルを指定した場合、アクセスプログラム生成部３０５は、指定されたファイル数の分だけアクセスプログラムを生成する。アクセスプログラムのアイコンはファイル本体のそれと同じ名前及び絵柄を含むことが望ましいだろう。これは、共有対象ファイルの種類を視覚的に把握しやすくするためである。

【００３８】

図６は、実施形態に係るファイル情報管理テーブルの一例を示す図である。アクセスプログラム生成部３０５は、生成したアクセスプログラムの情報をファイル情報管理部３０４のファイル情報管理テーブルに記録する。図６が示すように、ファイル情報管理テーブルは、ファイルＩＤ、ファイルアドレス（パス名）、アクセスプログラムＩＤ、開示期限、パスワード、で構成されている。ファイルアドレスもファイル情報データベース３０３から取得されたものである。アクセスプログラムの生成時にはパスワードが設定されていないため、パスワード欄は空欄となる。パスワード欄を空欄とする代わりに、パスワードが未設定であることを表す特定の情報が格納されていてもよい。

【００３９】

送信コンピュータ１０２の転送部３０１は、生成されたアクセスプログラムをサーバ１０１から受信し、それを電子メールに添付して、ファイルを共有したいユーザに送信する。送信者は、キーボード又はポインティングデバイスを操作して、受信者の電子メールアドレスを入力することになる。なお、アクセスプログラムをサーバ１０１から送信コンピュータ１０２へ送信するためのプロトコルは、ＨＴＴＰ、ＦＴＰ及びその他など、アクセスプログラムを転送できるものであればよい。

【００４０】

受信コンピュータ１０３は、受信したアクセスプログラム３１１を起動すると、ＩＤ取得部３１２が自動的に受信コンピュータ１０３の固有の識別情報（以下、コンピュータＩＤ）を取得する。コンピュータＩＤは、例えば、ＭＡＣアドレス、ドメイン名、稼働しているＯＳのビルドナンバー、ＯＳのライセンスナンバー、受信コンピュータにログオンしているユーザのユーザＩＤのうち少なくとも１つである。これらコンピュータＩＤを取得すると、ファイル閲覧部３１３は、サーバ１０１に対しアクセス要求を出す。

【００４１】

図７は、実施形態に係るアクセス要求の一例を示す図である。図７が示すように、アクセス要求には、アクセスプログラムＩＤ、コンピュータＩＤ（ログオンユーザーＩＤ、ドメイン名、ＭＡＣアドレス）、アクセス管理フラグが含まれている。なお、コンピュータ

ＩＤの固有性を高めるためには、複数の識別情報を組み合わせることが好ましいだろう。例えば、ＭＡＣアドレスだけをコンピュータＩＤとすれば、受信コンピュータ１０３にログオンできるすべてのユーザが、アクセスプログラム３１１を通じて共有対象ファイルにアクセスできてしまう。よって、受信者に関しても厳密に管理するためには、ＭＡＣアドレスだけでなく、ログオンＩＤなどもコンピュータＩＤとして必要となろう。

【００４２】

サーバ１０１のアクセス制御部３０８は、アクセス要求を受信すると、アクセス要求に含まれるコンピュータＩＤなどをパスワード生成部３０６に転送する。パスワード生成部３０６は、コンピュータＩＤを用いて認証用のパスワードを生成する。パスワード生成部３０６は生成した時点で、アクセス要求に含まれるコンピュータＩＤを消去する。これは、サーバで個人情報を保持しないための設計配慮である。また、情報の漏洩を防止する観点からも好ましいであろう。

【００４３】

パスワード生成部３０６は、パスワードを生成するとアクセス要求年月日をサーバ１０１のタイマー（不図示）から取得する。アクセス要求年月日は、アクセス要求の発生（受信）したときの年月日である。さらに、パスワード生成部３０６は、生成したパスワードとアクセス要求年月日のデータなどを伴う認証要求を認証制御部３０７に送出する。

【００４４】

図８は、実施形態に係る認証要求の一例を示す図である。図８が示すように、認証要求は、アクセス年月日、アクセスプログラムＩＤ、パスワード、アクセス管理フラグ、で構成されている。認証制御部３０７は、ファイル情報管理部３０４のファイル情報管理テーブル６０１を参照し、アクセス権があるかどうかの認証処理を実行する。認証制御部３０７は、認証結果を伴うアクセス制御要求をアクセス制御部３０８に送出する。

【００４５】

認証処理は、例えば次のように実行される。まず認証制御部３０７は、アクセスプログラムＩＤに対応する開示期限をファイル情報管理テーブル６０１から抽出し、抽出した開示期限と認証要求に含まれるアクセス年月日とを比較することで、アクセス年月日が開示期限内であるかどうかを判定する。開示期限外であればアクセス不許可とする。開示期限内である場合、認証制御部３０７は、アクセス管理フラグに応じてパスワード登録又はパスワードの照合のいずれかを実行する。

【００４６】

すなわち、アクセス管理フラグがＦＡＬＳＥの場合、認証制御部３０７は、ファイル情報管理テーブル６０１に、認証要求に含まれるパスワードをアクセスプログラムＩＤに対応づけて登録する。また、アクセス管理フラグが初回のアクセスであることを示しているため、認証制御部３０７は、アクセス許可と判断する。

【００４７】

一方、アクセス管理フラグがＴＲＵＥである場合、認証制御部３０７は、認証要求に含まれていたアクセスプログラムＩＤと関連づけられて登録されているパスワードをファイル情報管理テーブル６０１から抽出する。認証制御部３０７は、抽出したパスワードと、認証要求に含まれるパスワードとを比較する。認証要求に含まれるパスワードが登録済みパスワードの１つと一致すれば、認証制御部３０７は、アクセス許可と判断する。一方、認証制御部３０７は、一致するパスワードが存在しなければアクセス不許可と判断する。

【００４８】

認証制御部３０７は、アクセス許可と判断すると、アクセス判断の値（認証結果）としてＴＲＵＥを返すとともに、ファイル情報管理テーブル６０１から対象ファイルのファイルアドレスを取得して、アクセス制御部３０８に送出する。一方、アクセス不許可と判断したときは、認証制御部３０７が、アクセス判断の値としてＦＡＬＳＥをアクセス制御部３０８に返す。これらの情報はアクセス制御要求として認証制御部３０７からアクセス制御部３０８に送出される。

【００４９】

図９は、実施形態に係るアクセス制御要求の一例を示す図である。図９が示すように、アクセス制御要求は、例えば、アクセス判断の値、ファイルアドレス、パスワード新規登録フラグ、で構成されている。

【００５０】

アクセス制御要求を受信したアクセス制御部３０８は、アクセス判断の値がＴＲＵＥである場合、受信コンピュータ１０３のファイル閲覧部３１３にアクセス結果を送信する。また、アクセス制御部３０８は、ファイルアドレスにしたがってファイル格納部３０２に格納されている共有対象ファイルへのファイル閲覧部３１３によるアクセスを許可する。最終的に、アクセス制御部３０８は、受信コンピュータ１０３とファイル格納部３０２との通信を開始させる。このようにして、受信コンピュータ１０３は、サーバ１０１から送信されるファイルを受信して、ディスプレイなどに表示することが可能となる。

【００５１】

図１０は、実施形態に係るアクセス結果の一例を示す図である。図１０が示すように、アクセス結果は、アクセス判断の値とパスワード新規登録フラグで構成されている。アクセス判断の値がＴＲＵＥでない場合、ファイル閲覧部３１３は「アクセス不可」を意味するエラーメッセージを表示する。パスワード新規登録フラグの値がＴＲＵＥの場合、ファイル閲覧部３１３はアクセス記憶部３１４に対し、アクセス管理フラグを書き換えるための書き換え要求を送信する。なお、アクセス制御部３０８は、アクセスプログラムを実行している受信コンピュータ１０３へフラグを書き換えるよう指示する指示手段として機能することになる。すなわち、パスワード新規登録フラグの値をＴＲＵＥに設定して送信することは、アクセス管理フラグの書き換えを指示することに相当する。アクセス記憶部３１４は、書き換え要求を受信すると、アクセスプログラム３１１のアクセス管理フラグの値をＴＲＵＥに書き換える。

【００５２】

図１１は、実施形態に係るサーバ、送信コンピュータ及び受信コンピュータについての例示的なブロック図である。ここでは、図３に示した機能ブロックを実現するためのハードウエアユニットについて説明する。なお、説明の簡略化のため、サーバ１０１、送信コンピュータ１０２及び受信コンピュータ１０３の内部構成を同一のものとして説明するが、実際には一部が異なっていてもよい。

【００５３】

ＣＰＵ１１０１は、コンピュータプログラムに基づいて、コンピュータの各ユニットを統括的に制御する制御ユニットである。ＲＯＭ１１０２は、ファームウエア、ＯＳなどの制御プログラムを記憶する不揮発性の記憶ユニットである。ＲＡＭ１１０３は、ワークエリアとして機能する揮発性の記憶ユニットである。ハードディスクドライブ（ＨＤＤ）１１０４は、大容量の記憶ユニットである。例えば、サーバ１０１のハードディスクドライブ（ＨＤＤ）１１０４は、共有対象ファイル、ファイル情報データベース３０３及びファイル情報管理テーブル６０１などを記憶する。入力装置１１０５は、ポインティングデバイスやキーボードなどの入力ユニットである。例えば、送信コンピュータ１０２の入力装置１１０５は、共有対象ファイルを指定したり、受信者のメールアドレスを入力したりするために使用される。表示装置１１０６は、ユーザに対して各種情報を表示するための表示ユニットである。例えば、受信コンピュータ１０３の表示装置１１０６は、アクセスの許可された共有対象ファイルを表示する。通信装置１１０７は、ネットワーク通信カード（ＮＩＣ）などの通信ユニットである。例えば、通信装置１１０７は、電子メールの送受信、各種要求とそれに対する応答の送受信などに使用される。

【００５４】

図１２は、実施形態に係るアクセスプログラムの生成手順を示すフローチャートである。サーバ１０１は、このフローチャートにしたがってアクセスプログラムを生成することができる。

【００５５】

ステップＳ１２０１で、サーバ１０１のＣＰＵ１１０１は、送信コンピュータ１０２か

ら通信装置１１０７を通じて共有を希望するファイルの指定を受け付ける。この段階で、複数のファイルが指定されたり、受信者の数についても送信コンピュータ１０２から指定されたりしてもよい。ステップＳ１２０２で、ＣＰＵ１１０１は、指定されたファイルの名称などに基づいてファイル情報データベース３０３を検索し、対応するファイルＩＤを抽出する。この際に、ファイルアドレスも抽出されてもよい。

【００５６】

ステップＳ１２０３で、ＣＰＵ１１０１は、送信コンピュータ１０２から通信装置１１０７を通じてファイルの開示期限のデータを取得する。ステップＳ１２０４で、ＣＰＵ１１０１は、アクセスプログラムＩＤを発行する。アクセスプログラムＩＤは、アクセスプログラムごとに異なる識別情報であり、通常は、ファイル及び受信者の組ごとに異なる（図６）。例えば、同一のファイルであっても、受信者が異なれば、アクセスプログラムＩＤも異なる。また、同一の受信者であっても、ファイルが異なれば、アクセスプログラムＩＤも異なる。

【００５７】

ステップＳ１２０５で、ＣＰＵ１１０１は、発行したアクセスプログラムＩＤ及びＦＡＬＳＥに設定されたアクセス管理フラグを生成する。なお、アクセスプログラムの雛型は、あらかじめＨＤＤ１１０４などに保持されているものとする。このようにすれば、雛型にアクセスプログラムＩＤとアクセス管理フラグを搭載するだけで済むため、ＣＰＵ１１０１の処理負荷を軽減できる。

【００５８】

ステップＳ１２０６で、ＣＰＵ１１０１は、ＨＤＤ１１０４に記憶されているファイル管理テーブルに、ファイルＩＤ、ファイルアドレス、アクセスプログラムＩＤ、開示期限、パスワード（空欄又は特定の情報）を登録する。ステップＳ１２０７で、ＣＰＵ１１０１は、通信装置１１０７を通じて、生成したアクセスプログラムを送信コンピュータ１０２へ送信する。

【００５９】

上述したように、送信コンピュータ１０２のＣＰＵ１１０１は、受信したアクセスプログラムを、電子メールなどを用いて受信者へ転送する。送信コンピュータ１０２の入力装置１１０５から電子メールアドレスは入力される。もちろん、入力装置１１０５から入力された選択指示にしたがって、ＨＤＤ１１０４などに記憶されているアドレス帳から電子メールアドレスが選択されてもよい。

【００６０】

受信者は、任意のコンピュータを使用して電子メールを受信する。受信者は、任意のコンピュータを使用して電子メールに添付されていたアクセスプログラムを実行する。なお、電子メールを受信するコンピュータと、アクセスプログラムを実行するコンピュータは同一でなくてもよいが、初回アクセスを行ったコンピュータが、受信コンピュータ１０３として動作する。これは、初回アクセスを行ったコンピュータのコンピュータＩＤがパスワードに反映されるからである。

【００６１】

図１３は、実施形態に係る受信コンピュータがファイルにアクセスする処理の手順を示すフローチャートである。受信コンピュータ１０３は、このフローチャートにしたがってアクセスプログラムを起動して、ファイルにアクセスすることができる。

【００６２】

ステップＳ１３０１で、受信コンピュータ１０３のＣＰＵ１１０１は、送信コンピュータ１０２から送信されたアクセスプログラム３１１を受信して起動する。ステップＳ１３０２で、ＣＰＵ１１０１は、起動したアクセスプログラムにしたがって、受信コンピュータ１０３のコンピュータＩＤを取得する。

【００６３】

ステップＳ１３０３で、ＣＰＵ１１０１は、取得したコンピュータＩＤを伴うアクセス要求を、通信装置１１０７を通じてサーバ１０１へ送信する。ステップＳ１３０４で、Ｃ

ＰＵ１１０１は、アクセス要求に対する応答としてアクセス結果をサーバ１０１から受信する。

【００６４】

ステップＳ１３０５で、ＣＰＵ１１０１は、アクセス結果に含まれているアクセス判断の値がＴＲＵＥか否かに応じて、アクセスが許可されたか否かを判定する。ＴＲＵＥでなければ（ＦＡＬＳＥ）であれば、ステップＳ１３０７に進む。ステップＳ１３０７で、ＣＰＵ１１０１は、「アクセス不可」を意味するメッセージを表示装置１１０６に表示する。その後、ステップＳ１３１０に進む。

【００６５】

一方、アクセス判断の値ＴＲＵＥであれば、ステップＳ１３０６に進む。ステップＳ１３０６で、ＣＰＵ１１０１は、サーバ１０１を通じてファイルにアクセスし、ファイルの内容を表示装置１１０６に表示する。ステップＳ１３０８で、ＣＰＵ１１０１は、アクセス結果に含まれるパスワード新規登録フラグの値がＴＲＵＥか否かに応じて、アクセスプログラムのアクセス管理フラグを書き換えるか否かを判定する。パスワード新規登録フラグの値がＴＲＵＥであれば、ステップＳ１３０９に進み、ＣＰＵ１１０１は、アクセス管理フラグの値をＦＡＬＳＥからＴＲＵＥに書き換える。パスワード新規登録フラグの値がＦＡＬＳＥであれば、２回目以降のアクセスであるため、アクセス管理フラグを書き換えることなく、ステップＳ１３１０に進む。

【００６６】

ステップＳ１３１０で、ＣＰＵ１１０１は、ファイルの閲覧を終了するための（アクセスプログラムの終了）指示が入力装置１１０５から入力されると、アクセスプログラムを終了させる。

【００６７】

図１４は、実施形態に係るアクセス要求の処理手順を示すフローチャートである。サーバ１０１は、このフローチャートにしたがって受信コンピュータ１０３からのアクセス要求を処理することができる。

【００６８】

ステップＳ１４０１で、サーバ１０１のＣＰＵ１１０１は、受信コンピュータ１０３から通信装置１１０７を通じてアクセス要求を受信する。ステップＳ１４０２で、ＣＰＵ１１０１は、アクセス要求に含まれるコンピュータＩＤを用いてパスワードを生成する。ステップＳ１４０３で、ＣＰＵ１１０１は、コンピュータＩＤを消去する。

【００６９】

ステップＳ１４０４で、ＣＰＵ１１０１は、アクセス要求の発生した年月日の情報をＣＰＵ１１０１内部のタイマーから取得する。ステップＳ１４０５で、ＣＰＵ１１０１は、アクセス要求に含まれていたアクセスプログラムＩＤに対応する開示期限の情報をファイル情報管理テーブル６０１から取得し、アクセス要求の発生した年月日が開示期限内か否かを判定する。開示期限内でなければ、ステップＳ１４０６に進み、ＣＰＵ１１０１は、アクセス不許可（拒否）を意味するアクセス結果を受信コンピュータ１０３に送信する。

【００７０】

一方、開示期限内であれば、ステップＳ１４０７に進み、ＣＰＵ１１０１は、アクセス要求に含まれていたアクセス管理フラグの値がＦＡＬＳＥか否かに応じて、初回アクセスか否かを判定する。

【００７１】

初回アクセスであれば、ステップＳ１４０８に進み、ＣＰＵ１１０１は、ファイル情報管理テーブル６０１に、アクセスプログラムＩＤと対応づけてパスワードを登録する。ステップＳ１４０９で、ＣＰＵ１１０１は、受信コンピュータ１０３からファイルへのアクセスを許可する。ステップＳ１４１０で、ＣＰＵ１１０１は、受信コンピュータ１０３に対し、アクセス結果としてアクセス判断（ＴＲＵＥ）と、パスワード新規登録フラグ（ＴＲＵＥ）を送信する。

【００７２】

一方、２回目以降のアクセスであれば、ステップＳ１４１１に進み、ＣＰＵ１１０１は、認証処理を実行する。すなわち、ＣＰＵ１１０１は、アクセス要求に含まれていたアクセスプログラムＩＤと対応づけてファイル情報管理テーブル６０１に登録されているパスワードを抽出する。さらに、ＣＰＵ１１０１は、抽出したパスワードと生成したパスワードとを比較する。ステップＳ１４１２で、ＣＰＵ１１０１は、双方のパスワードが一致するか否かを判定する。パスワードが一致しなければ、認証に失敗したことになるので、ステップＳ１４０６に進む。

【００７３】

一方、パスワードが一致すれば、ステップＳ１４１３に進み、ＣＰＵ１１０１は、ファイルへのアクセスを許可する。ステップＳ１４１４で、ＣＰＵ１１０１は、受信コンピュータ１０３に対し、アクセス結果としてアクセス判断（ＴＲＵＥ）を送信する。

【００７４】

以上説明したように本実施形態によれば、送信者及び受信者の負荷が少なく、かつ、情報漏洩の可能性を低減したファイル共有システム等を実現できる。すなわち、送信者はアクセスプログラムを受信者に送信するだけで済む利点がある。また、受信者は、アクセスプログラムを実行することで、送信者の指定したファイルにアクセスできるため、従来よりも作業負担が緩和される。また、送信者から受信者へファイルが直接送信されることはないため、漏洩の可能性も低減される。

【００７５】

また、本実施形態によれば、受信者のコンピュータに付与された固有のコンピュータＩＤからパスワードが作成される。よって、仮に、アクセスプログラムが第三者に転送されたとしても、第三者によるアクセス要求により作成されるパスワードは正当なパスワードとは異なることになり、情報漏洩が抑制される。また、パスワードはサーバ内で作成され保持されているため、パスワード自体が流出する可能性は低い。

【００７６】

さらに、本実施形態によれば、パスワードの作成に使用された識別情報は、パスワードの作成後にサーバから消去されるため、この識別情報がサーバから流出する可能性も低減される。これは、個人情報の保護の観点からも好ましいだろう。

【００７７】

また、本実施形態によれば、アクセスプログラムを転送するために、広く普及した電子メールを利用できるため、送信者や受信者の負担が軽減される。使い慣れたツールを使用できることは、ユーザフレンドリーなインタフェースを提供する観点からも望ましいだろう。

【００７８】

また、本実施形態によれば、各受信者に提供されるアクセスプログラムに区別のためのアクセスプログラムＩＤを付与することで、単一のファイルを同時に複数の受信者に共有させることも可能となる。

【００７９】

また、本実施形態によれば、ファイルに対するアクセスが初回か否かを管理するためのフラグを導入することで、初回のアクセスを行った受信者について生成されたパスワードを正当なパスワードとして保持できる利点がある。これは、一般に、ファイルに対して初回にアクセスしてくる受信者は正当な受信者であり、正当な受信者よりも先に不正な第三者がアクセスしてくることは極めて稀であるという事実に則している。

【００８０】

また、アクセスプログラムはファイルごとに生成されるため、通常のファイルと同じように管理することができる。それゆえ、通常のファイルを開くのと同様の操作で認証が行われて所望のファイルにアクセスすることが可能となる。

【００８１】

さらに、ファイルの本体はあくまでファイルサーバに記憶されている。そのため、複数ユーザとファイルを共有する場合に、従来のようにメールサーバでファイルをコピーする

必要がないため負荷が軽減される。さらに、送信したファイルが受信者により改変された状態又は情報が古いままの状態で別のユーザにファイルが送信されてしまうことによる情報の完全性喪失の問題も合わせて解決されよう。

【００８２】

［他の実施形態］

図１５は、実施形態に係るファイル共有システムの変形例を示す図である。上述した実施形態におけるサーバ１０１又はサーバ１０１の一部機能を送信コンピュータ１０２に配置してもよい。例えば、サーバ１０１のファイル情報管理部３０４、アクセスプログラム生成部３０５、パスワード生成部３０６、認証制御部３０７、アクセス制御部３０８は、送信コンピュータに配置されてもよい。図１５によれば、ファイルサーバ１５０１には、ファイル情報データベース３０３とファイル格納部３０２が配置されている。

【００８３】

また、送信コンピュータ１０２はコンピュータ以外の情報処理装置でもよい。例えば、ネットワーク機能を有するスキャナ装置１５０２や、ネットワークファクシミリ装置であってもよい。図１５によれば、スキャナ装置１５０２にサーバ１０１の一部機能及び送信コンピュータ１０２の処理を具備させた場合の構成例が示されている。この場合、スキャナ装置１５０２の画像スキャン部１５０３で画像ファイルを生成する。この画像ファイルをファイル格納部３０２に保存する。さらに、アクセスプログラム生成部３０５は、この画像ファイルについてアクセスプログラムを生成する。メール送信部１５０４は、電子メールにアクセスプログラムを添付して送信する。これにより、アクセスプログラムの添付された電子メールの受信者のみが画像ファイルにアクセスすることができるようになる。

【図面の簡単な説明】

【００８４】

【図１】実施形態に係るファイル共有システムの概要を示す図である。

【図２】実施形態に係るファイル共有についてのシーケンス図である。

【図３】本発明の一実施の形態に係るファイル共有システムを示すブロック図である。

【図４】実施形態に係るアクセスプログラム生成要求の一例を示す図である。

【図５】実施形態に係るアクセスプログラムに搭載される情報の一例を示す図である。

【図６】実施形態に係るファイル情報管理テーブルの一例を示す図である。

【図７】実施形態に係るアクセス要求の一例を示す図である。

【図８】実施形態に係る認証要求の一例を示す図である。

【図９】実施形態に係るアクセス制御要求の一例を示す図である。

【図１０】実施形態に係るアクセス結果の一例を示す図である。

【図１１】実施形態に係るサーバ、送信コンピュータ及び受信コンピュータについての例示的なブロック図である。

【図１２】実施形態に係るアクセスプログラムの生成手順を示すフローチャートである。

【図１３】実施形態に係る受信コンピュータがファイルにアクセスする処理の手順を示すフローチャートである。

【図１４】実施形態に係るアクセス要求の処理手順を示すフローチャートである。

【図１５】実施形態に係るファイル共有システムの変形例を示す図である。

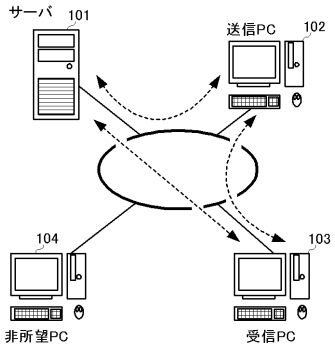
【符号の説明】

【００８５】

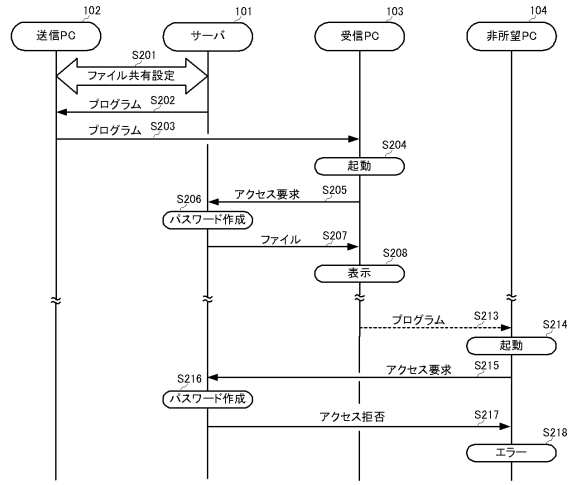
１０１…サーバ
１０２…送信コンピュータ
１０３…受信コンピュータ
３００…ファイル指定部
３０１…ファイル転送部
３０２…ファイル格納部
３０３…ファイル情報データベース
３０４…ファイル情報管理部

３０５…アクセスプログラム生成部
３０６…パスワード生成部
３０７…認証制御部
３０８…アクセス制御部
３１１…アクセスプログラム
３１２…ＩＤ取得部
３１３…ファイル閲覧部
３１４…アクセス記憶部

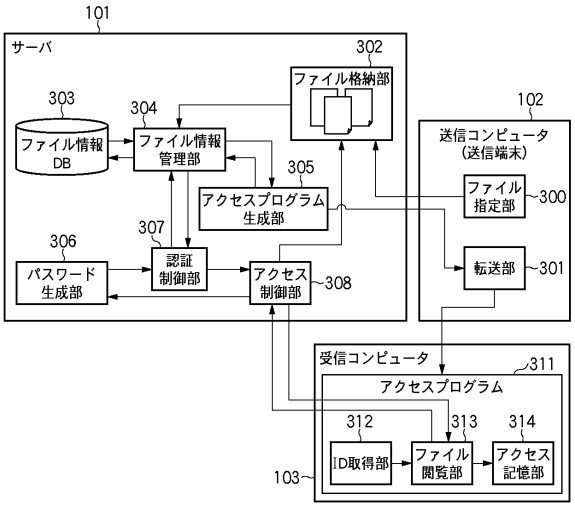
【図１】



【図２】



【図３】



【図４】

データ項目	内容
ファイルID	ACCOUNT019485-23

401

【図５】

データ項目	内容
アクセスプログラムID	ACCOUNT019485-23_002
アクセス管理フラグ	FALSE

【図６】

601

ファイルID	ファイルアドレス	アクセスプログラムID	開示期限	パスワード
ACCOUNT019485-23	￥￥CompanyB￥Account￥....	ACCOUNT019485-23_001	2006/2/1	KOJDLKALKJu3u
		ACCOUNT019485-23_002	2006/5/3	XSKOIUSDKdwuu
				IEOIUQRWKEIkjZ
				OWIUERkdiwu0eu
LEGAL1081091-14	￥￥CompanyB￥Legal￥....	LEGAL1081091-14_001	2005/4/2	KAJHFOiEKr0oiO
		LEGAL1081091-14_002	2006/1/23	UFEPOXKLwerlkJ
LEGAL3340234-34	￥￥CompanyD￥Legal￥....	LEGAL3340234-34_001	2007/3/12	OIUESALKDjowe

【図７】

データ項目	内容
アクセスプログラムID	ACCOUNT019485-23_002
ログオンユーザ　ID	nakamura12345
ドメイン名	COMPANY
MACアドレス	00-08-03-0E-KP-93
アクセス管理フラグ	FALSE

【図８】

データ項目	内容
アクセス年月日	2006/02/03
アクセスプログラムID	ACCOUNT019485-23_002
パスワード	XSKOIUSDKdwuu
初回アクセス済みフラグ	FALSE

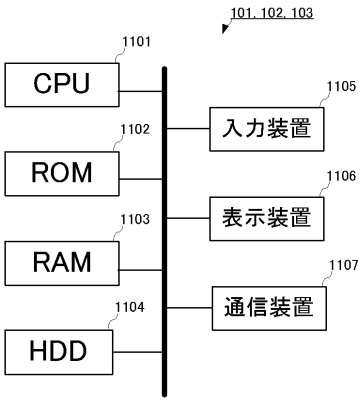
【図９】

データ項目	内容
アクセス判断	TRUE
ファイル場所アドレス	￥￥CompanyB￥Account￥....
パスワード新規登録フラグ	TRUE

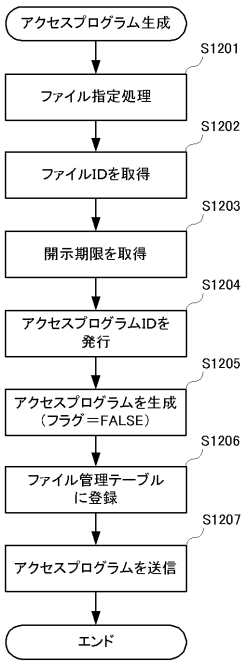
【図１０】

データ項目	内容
アクセス判断	TRUE
パスワード新規登録フラグ	TRUE

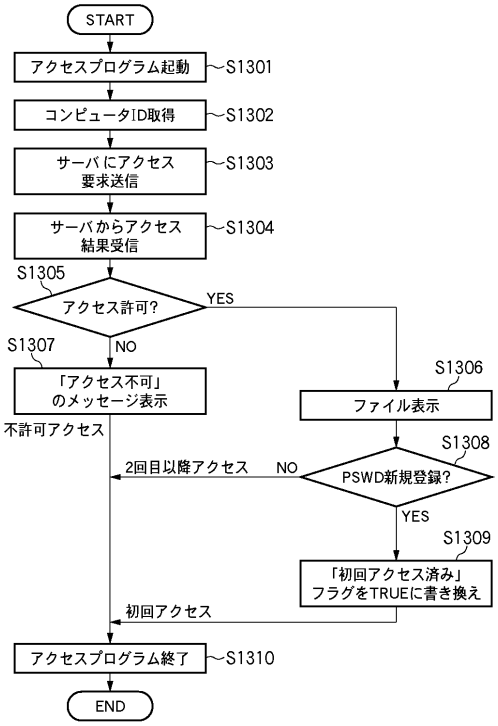
【図１１】



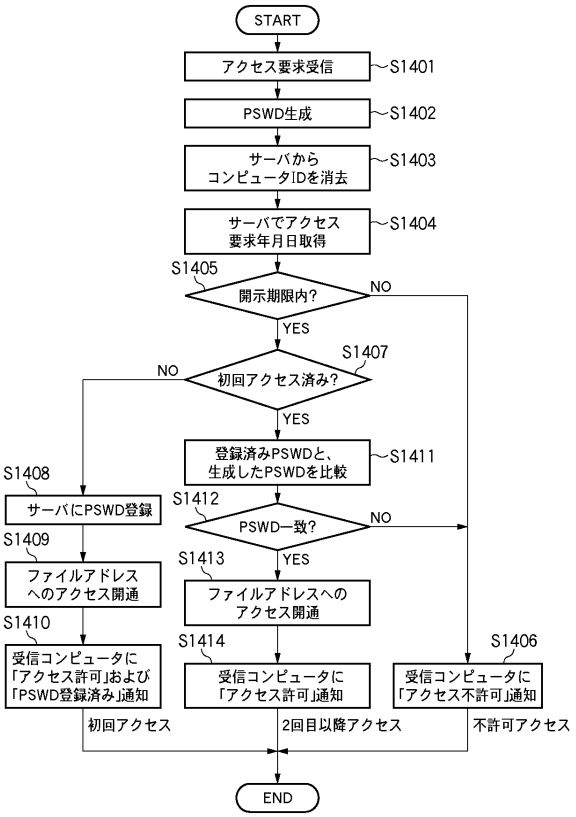
【図１２】



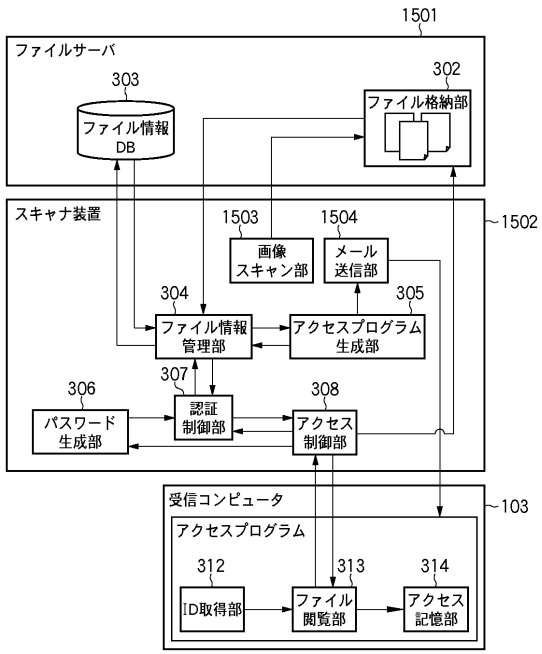
【図１３】


START
アクセスプログラム起動
S1301
コンピュータID取得
S1302
サーバにアクセス要求送信
S1303
サーバからアクセス結果受信
S1304
S1305
アクセス許可?
YES
S1307
NO
「アクセス不可」のメッセージ表示
S1306
ファイル表示
不許可アクセス
S1308
2回目以降アクセス
NO
PSWD新規登録?
YES
S1309
「初回アクセス済み」フラグをTRUEに書き換え
初回アクセス
アクセスプログラム終了
S1310
END

【図１４】


START
アクセス要求受信
S1401
PSWD生成
S1402
サーバからコンピュータIDを消去
S1403
サーバでアクセス要求年月日取得
S1404
S1405
開示期限内?
NO
YES
S1407
NO
初回アクセス済み?
YES
登録済みPSWDと、生成したPSWDを比較
S1411
S1408
サーバにPSWD登録
S1412
PSWD一致?
NO
S1409
YES
ファイルアドレスへのアクセス開通
S1413
ファイルアドレスへのアクセス開通
S1410
S1414
S1406
受信コンピュータに「アクセス許可」および「PSWD登録済み」通知
受信コンピュータに「アクセス許可」通知
受信コンピュータに「アクセス不許可」通知
初回アクセス
2回目以降アクセス
不許可アクセス
END

【図１５】


1501
ファイルサーバ
303
ファイル情報DB
302
ファイル格納部
スキャナ装置
1502
1503
画像スキャン部
1504
メール送信部
304
ファイル情報管理部
305
アクセスプログラム生成部
307
306
パスワード生成部
認証制御部
308
アクセス制御部
受信コンピュータ
103
アクセスプログラム
312
ID取得部
313
ファイル閲覧部
314
アクセス記憶部

フロントページの続き

(56)参考文献　国際公開第２００６／０２２０１１（WO，Ａ１）
特開２００３－２９５９６４（ＪＰ，Ａ）
特開２００１－２６５９３７（ＪＰ，Ａ）
特開２０００－０９９３２３（ＪＰ，Ａ）

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