(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6907491号
(P6907491)
(45)発行日　令和3年7月21日(2021.7.21)　(24)登録日　令和3年7月5日(2021.7.5)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601A
G06F 21/62 (2013.01)　　H04L 9/00 601E
　　G06F 21/62 318

請求項の数 21　(全 34 頁)

(21)出願番号　特願2016-182831(P2016-182831)
(22)出願日　平成28年9月20日(2016.9.20)
(65)公開番号　特開2018-50107(P2018-50107A)
(43)公開日　平成30年3月29日(2018.3.29)
審査請求日　令和1年5月23日(2019.5.23)

(73)特許権者　000001270
コニカミノルタ株式会社
東京都千代田区丸の内二丁目７番２号
(74)代理人　100117651
弁理士　高垣　泰志
(72)発明者　山口　敏伸
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内

審査官　大桃　由紀雄

最終頁に続く

(54)【発明の名称】情報共有サーバー、情報共有システム及びプログラム

(57)【特許請求の範囲】
【請求項１】
文書データを共有する複数のユーザーを一のグループに登録する登録手段と、
前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する取得手段と、
前記暗号化された文書データと、前記パスワードとを関連付けて記憶する記憶手段と、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記記憶手段から前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する復号手段と、
前記復号手段によって復号された文書データを提供する閲覧情報提供手段と、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、該ユーザーによって指定された印刷装置に対応するプリンタドライバがインストールされているか否かを判定し、前記プリンタドライバがインストールされていれば、前記プリンタドライバを起動して印刷ジョブを生成し、該印刷ジョブを前記印刷装置へ送信する印刷制御手段と、
を備え、
前記閲覧情報提供手段は、前記復号された文書データに基づいてＷｅｂブラウザで閲覧可能な閲覧用画像を生成し、前記閲覧要求の送信元に対して前記Ｗｅｂブラウザの保存機能を無効に設定して前記閲覧用画像を送信することを特徴とする情報共有サーバー。

【請求項２】
前記閲覧情報提供手段は、更に前記Ｗｅｂブラウザの印刷機能を無効に設定して前記閲覧用画像を送信することを特徴とする請求項１に記載の情報共有サーバー。
【請求項３】
前記登録手段は、前記一のグループに対して一対の暗号鍵と復号鍵を登録し、
前記記憶手段は、前記パスワードが前記暗号鍵によって暗号化された暗号化パスワードを記憶し、
前記復号手段は、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする請求項１又は２に記載の情報共有サーバー。
【請求項４】
前記取得手段は、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする請求項３に記載の情報共有サーバー。
【請求項５】
前記取得手段は、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする請求項３に記載の情報共有サーバー。
【請求項６】
前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記記憶手段には、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第１の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第２の暗号化パスワードとが記憶されることを特徴とする請求項３乃至５のいずれかに記載の情報共有サーバー。
【請求項７】
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する文書データ送信手段、
を更に備えることを特徴とする請求項１乃至６のいずれかに記載の情報共有サーバー。
【請求項８】
前記文書データ送信手段により前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する通知手段、
を更に備えることを特徴とする請求項７に記載の情報共有サーバー。
【請求項９】
前記印刷制御手段は、前記プリンタドライバがインストールされていないと判定した場合、前記暗号化された文書データと前記パスワードとを前記印刷装置へ送信することを特徴とする請求項１乃至８のいずれかに記載の情報共有サーバー。
【請求項１０】
請求項１乃至９のいずれかに記載の情報共有サーバーと、
前記情報共有サーバーに対して文書データをアップロードする情報処理装置と、
を有する情報共有システムであって、
前記情報処理装置は、
文書データをユーザーによって指定されたパスワードで暗号化する暗号化手段と、
前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、
を備えることを特徴とする情報共有システム。
【請求項１１】

請求項１乃至９のいずれかに記載の情報共有サーバーと、
前記情報共有サーバーに対して文書データをアップロードする画像処理装置と、
を有する情報共有システムであって、
前記画像処理装置は、
原稿を読み取ることによって文書データを生成する原稿読取手段と、
前記原稿読取手段によって生成された文書データを、ユーザーによって指定されたパスワードで暗号化する暗号化手段と、
前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、
を備えることを特徴とする情報共有システム。

【請求項１２】
前記アップロード手段は、前記暗号化された文書データを前記情報共有サーバーへアップロードすることに伴い、前記情報共有サーバーから暗号鍵を受信した場合、前記暗号鍵を用いて前記パスワードを暗号化した暗号化パスワードを生成し、前記暗号化パスワードを前記情報共有サーバーへアップロードすることを特徴とする請求項１０又は１１に記載の情報共有システム。

【請求項１３】
コンピュータに、
文書データを共有する複数のユーザーを一のグループに登録する第１ステップと、
前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する第２ステップと、
前記暗号化された文書データと、前記パスワードとを関連付けて記憶する第３ステップと、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する第４ステップと、
前記第４ステップによって復号された文書データを提供する第５ステップと、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、該ユーザーによって指定された印刷装置に対応するプリンタドライバがインストールされているか否かを判定し、前記プリンタドライバがインストールされていれば、前記プリンタドライバを起動して印刷ジョブを生成し、該印刷ジョブを前記印刷装置へ送信する第８ステップと、
を実行させ、
前記第５ステップは、前記復号された文書データに基づいてＷｅｂブラウザで閲覧可能な閲覧用画像を生成し、前記閲覧要求の送信元に対して前記Ｗｅｂブラウザの保存機能を無効に設定して前記閲覧用画像を送信することを特徴とするプログラム。

【請求項１４】
前記第５ステップは、更に前記Ｗｅｂブラウザの印刷機能を無効に設定して前記閲覧用画像を送信することを特徴とする請求項１３に記載のプログラム。

【請求項１５】
前記第１ステップは、前記一のグループに対して一対の暗号鍵と復号鍵を登録するステップを含み、
前記第３ステップは、前記暗号鍵によって前記パスワードが暗号化された暗号化パスワードを記憶し、
前記第４ステップは、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする請求項１３又は１４に記載のプログラム。

【請求項１６】
前記第２ステップは、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする請求項１５に記載

のプログラム。
【請求項１７】
前記第２ステップは、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする請求項１５に記載のプログラム。
【請求項１８】
前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記第３ステップは、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第１の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第２の暗号化パスワードとを記憶することを特徴とする請求項１５乃至１７のいずれかに記載のプログラム。
【請求項１９】
前記コンピュータに、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する第６ステップ、
を更に実行させることを特徴とする請求項１３乃至１８のいずれかに記載のプログラム。
【請求項２０】
前記コンピュータに、
前記第６ステップにより前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する第７ステップ、
を更に実行させることを特徴とする請求項１９に記載のプログラム。
【請求項２１】
前記第８ステップは、前記プリンタドライバがインストールされていないと判定した場合、前記暗号化された文書データと前記パスワードとを前記印刷装置へ送信することを特徴とする請求項１３乃至２０のいずれかに記載のプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報共有サーバー、情報共有システム及びプログラムに関し、特に複数のユーザーで文書データを共有するための技術に関する。
【背景技術】
【０００２】
従来、インターネットに接続されたクラウド上にＷｅｂサーバーとして機能する情報共有サーバーを設置し、複数のユーザーがそれぞれ異なる拠点から情報共有サーバーへアクセスしてログインすることにより、複数のユーザーが情報を共有しながら会議などを行えるようにした情報共有サービスが提供されている。この種の情報共有サービスでは、各ユーザーが作成した文書データを情報共有サーバーへアップロードすることにより、複数のユーザーがその文書データを共有することも可能である。
【０００３】
また情報共有サーバーは、アップロードされる文書データを、予め登録された複数のユーザー以外には公開しない機能を有している。そのため、情報共有サーバーには、パスワードによって暗号化された機密性の高い文書データがアップロードされることもある（例えば特許文献１）。この場合、情報共有サーバーは、パスワードによって暗号化された文書データを共有情報として保存することとなる。
【先行技術文献】

【特許文献】
【０００４】
【特許文献１】特開２０１４－１７４７２１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、情報共有サーバーにおいて保存される文書データに設定されたパスワードが文書データ毎に異なる場合、各ユーザーは個々の文書データに設定されているパスワードを自身で入力しなれば文書データの中身を閲覧することができない。そのため、文書データをアップロードするユーザーは、文書データに設定したパスワードを他のユーザーに通知する必要があり、煩わしい。
【０００６】
一方、文書データをアップロードしたユーザーがその文書データを閲覧する際の画面情報を他のユーザーにも提供できるように構成すれば、他のユーザーは文書データのパスワードを知らなくても、文書データの中身を閲覧することができる。しかし、このような構成では、他のユーザーは、文書データをアップロードしたユーザーがその文書データを閲覧しているときにしか閲覧できないため、利便性に欠けるという問題がある。
【０００７】
また文書データをアップロードするユーザーによって任意のパスワードが設定されると、情報共有サーバーは、そのパスワードを把握することができないため、他のユーザーに対し、パスワードによって暗号化された文書データのプレビュー機能を提供することができないという問題もある。
【０００８】
これに対し、文書データをアップロードするユーザーが、パスワードを設定することなく、文書データを文書共有サーバーへアップロードすれば、上記のような問題は解消される。しかし、この場合、他のユーザーによって文書データがダウンロードされてしまうと、文書データの閲覧に関する制限を課すことができなくなるため、情報漏洩のリスクが高くなるという新たな問題が発生する。
【０００９】
そこで本発明は、上記問題点を解決するためになされたものであり、パスワードによって暗号化された文書データがアップロードされた場合に、他のユーザーがパスワードを知らなくても文書データを閲覧できるようにして利便性を向上させた情報共有サーバー、情報共有システム及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
上記目的を達成するため、請求項１に係る発明は、情報共有サーバーであって、文書データを共有する複数のユーザーを一のグループに登録する登録手段と、前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する取得手段と、前記暗号化された文書データと、前記パスワードとを関連付けて記憶する記憶手段と、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記記憶手段から前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する復号手段と、前記復号手段によって復号された文書データを提供する閲覧情報提供手段と、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、該ユーザーによって指定された印刷装置に対応するプリンタドライバがインストールされているか否かを判定し、前記プリンタドライバがインストールされていれば、前記プリンタドライバを起動して印刷ジョブを生成し、該印刷ジョブを前記印刷装置へ送信する印刷制御手段と、を備え、前記閲覧情報提供手段は、前記復号された文書データに基づいてＷｅｂブラウザで閲覧可能な閲覧用画像を生成し、前記閲覧要求の送信元に対して前記Ｗｅｂブラウザ

の保存機能を無効に設定して前記閲覧用画像を送信することを特徴とする構成である。

【００１１】
請求項２に係る発明は、請求項１に記載の情報共有サーバーにおいて、前記閲覧情報提供手段は、更に前記Ｗｅｂブラウザの印刷機能を無効に設定して前記閲覧用画像を送信することを特徴とする構成である。
【００１２】
請求項３に係る発明は、請求項１又は２に記載の情報共有サーバーにおいて、前記登録手段は、前記一のグループに対して一対の暗号鍵と復号鍵を登録し、前記記憶手段は、前記パスワードが前記暗号鍵によって暗号化された暗号化パスワードを記憶し、前記復号手段は、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする構成である。
【００１３】
請求項４に係る発明は、請求項３に記載の情報共有サーバーにおいて、前記取得手段は、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする構成である。
【００１４】
請求項５に係る発明は、請求項３に記載の情報共有サーバーにおいて、前記取得手段は、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする構成である。
【００１５】
請求項６に係る発明は、請求項３乃至５のいずれかに記載の情報共有サーバーにおいて、前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記記憶手段には、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第１の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第２の暗号化パスワードとが記憶されることを特徴とする構成である。
【００１６】
請求項７に係る発明は、請求項１乃至６のいずれかに記載の情報共有サーバーにおいて、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する文書データ送信手段、を更に備えることを特徴とする構成である。
【００１７】
請求項８に係る発明は、請求項７に記載の情報共有サーバーにおいて、前記文書データ送信手段により前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する通知手段、を更に備えることを特徴とする構成である。
【００１８】
請求項９に係る発明は、請求項１乃至８のいずれかに記載の情報共有サーバーにおいて、前記印刷制御手段は、前記プリンタドライバがインストールされていないと判定した場合、前記暗号化された文書データと前記パスワードとを前記印刷装置へ送信することを特徴とする構成である。

【００１９】
請求項１０に係る発明は、請求項１乃至９のいずれかに記載の情報共有サーバーと、前記情報共有サーバーに対して文書データをアップロードする情報処理装置と、を有する情

報共有システムであって、前記情報処理装置は、文書データをユーザーによって指定されたパスワードで暗号化する暗号化手段と、前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、を備えることを特徴とする構成である。

【００２０】
請求項１１に係る発明は、請求項１乃至９のいずれかに記載の情報共有サーバーと、前記情報共有サーバーに対して文書データをアップロードする画像処理装置と、を有する情報共有システムであって、前記画像処理装置は、原稿を読み取ることによって文書データを生成する原稿読取手段と、前記原稿読取手段によって生成された文書データを、ユーザーによって指定されたパスワードで暗号化する暗号化手段と、前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、を備えることを特徴とする構成である。

【００２１】
請求項１２に係る発明は、請求項１０又は１１に記載の情報共有システムにおいて、前記アップロード手段は、前記暗号化された文書データを前記情報共有サーバーへアップロードすることに伴い、前記情報共有サーバーから暗号鍵を受信した場合、前記暗号鍵を用いて前記パスワードを暗号化した暗号化パスワードを生成し、前記暗号化パスワードを前記情報共有サーバーへアップロードすることを特徴とする構成である。

【００２２】
請求項１３に係る発明は、プログラムであって、コンピュータに、文書データを共有する複数のユーザーを一のグループに登録する第１ステップと、前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する第２ステップと、前記暗号化された文書データと、前記パスワードとを関連付けて記憶する第３ステップと、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する第４ステップと、前記第４ステップによって復号された文書データを提供する第５ステップと、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、該ユーザーによって指定された印刷装置に対応するプリンタドライバがインストールされているか否かを判定し、前記プリンタドライバがインストールされていれば、前記プリンタドライバを起動して印刷ジョブを生成し、該印刷ジョブを前記印刷装置へ送信する第８ステップと、を実行させ、前記第５ステップは、前記復号された文書データに基づいてＷｅｂブラウザで閲覧可能な閲覧用画像を生成し、前記閲覧要求の送信元に対して前記Ｗｅｂブラウザの保存機能を無効に設定して前記閲覧用画像を送信することを特徴とする構成である。

【００２３】
請求項１４に係る発明は、請求項１３に記載のプログラムにおいて、前記第５ステップは、更に前記Ｗｅｂブラウザの印刷機能を無効に設定して前記閲覧用画像を送信することを特徴とする構成である。

【００２４】
請求項１５に係る発明は、請求項１３又は１４に記載のプログラムにおいて、前記第１ステップは、前記一のグループに対して一対の暗号鍵と復号鍵を登録するステップを含み、前記第３ステップは、前記暗号鍵によって前記パスワードが暗号化された暗号化パスワードを記憶し、前記第４ステップは、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする構成

である。

【００２５】
請求項１６に係る発明は、請求項１５に記載のプログラムにおいて、前記第２ステップは、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする構成である。

【００２６】
請求項１７に係る発明は、請求項１５に記載のプログラムにおいて、前記第２ステップは、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする構成である。

【００２７】
請求項１８に係る発明は、請求項１５乃至１７のいずれかに記載のプログラムにおいて、前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記第３ステップは、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第１の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第２の暗号化パスワードとを記憶することを特徴とする構成である。

【００２８】
請求項１９に係る発明は、請求項１３乃至１８のいずれかに記載のプログラムにおいて、前記コンピュータに、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する第６ステップ、を更に実行させることを特徴とする構成である。

【００２９】
請求項２０に係る発明は、請求項１９に記載のプログラムにおいて、前記コンピュータに、前記第６ステップにより前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する第７ステップ、を更に実行させることを特徴とする構成である。

【００３０】
請求項２１に係る発明は、請求項１３乃至２０のいずれかに記載のプログラムにおいて、前記第８ステップは、前記プリンタドライバがインストールされていないと判定した場合、前記暗号化された文書データと前記パスワードとを前記印刷装置へ送信することを特徴とする構成である。

【発明の効果】
【００３１】
本発明によれば、パスワードによって暗号化された文書データがアップロードされた場合において、他のユーザーがパスワードを知らなくても文書データを閲覧することが可能になるため、暗号化された文書データを利用する際の利便性が向上する。
【図面の簡単な説明】
【００３２】
【図１】情報共有システムの概念的構成例を示す図である。

【図２】情報処理装置のハードウェア構成及び機能構成の一例を示すブロック図である。
【図３】画像処理装置のハードウェア構成及び機能構成の一例を示すブロック図である。
【図４】情報共有サーバーのハードウェア構成及び機能構成の一例を示すブロック図である。
【図５】共有情報の一例を示す図である。
【図６】アップロードデータ取得部による暗号化処理の概念を示す図である。
【図７】管理情報の一例を示す図である。
【図８】復号部の詳細な機能構成の一例を示す図である。
【図９】閲覧情報生成部の詳細な機能構成の一例を示す図である。
【図１０】情報処理装置において表示される閲覧画面の一例を示す図である。
【図１１】文書データを情報共有サーバーへアップロードして閲覧する場合の動作シーケンスを示す図である。
【図１２】文書データをダウンロードする場合の動作シーケンスを示す図である。
【図１３】文書データを印刷する場合の動作シーケンスを示す図である。
【図１４】情報共有サーバーによって行われる主たる処理手順の一例を示すフローチャートである。
【図１５】文書データ登録処理の詳細な処理手順の一例を示すフローチャートである。
【図１６】閲覧情報提供処理の詳細な処理手順の一例を示すフローチャートである。
【図１７】文書データ提供処理の詳細な処理手順の一例を示すフローチャートである。
【図１８】印刷制御処理の詳細な処理手順の一例を示すフローチャートである。
【図１９】文書データを情報共有サーバーへアップロードする際の動作シーケンスを示す図である。
【発明を実施するための形態】
【００３３】
以下、本発明に関する好ましい実施形態について図面を参照しつつ詳細に説明する。尚、以下に説明する実施形態において互いに共通する部材には同一符号を付しており、それらについての重複する説明は省略する。
【００３４】
（第１実施形態）
図１は、本発明における情報共有システム１の概念的構成例を示す図である。情報共有システム１は、インターネットに接続されたクラウド３上に設けられる情報共有サーバー２と、複数の情報処理装置４と、スキャン機能及びプリント機能を備えたＭＦＰ（Multifunction Peripherals）などで構成される画像処理装置５とが、インターネットなどのネットワークを介して相互にデータ通信を行うことができる構成である。複数の情報処理装置４のそれぞれは、例えば一般的なパーソナルコンピュータ（ＰＣ）によって構成される。各情報処理装置４は、それぞれ異なるユーザーＡ，Ｂ，Ｃ，Ｄによって使用される。またユーザーＡ，Ｂ，Ｃ，Ｄは、例えばそれぞれ異なる拠点に位置している。画像処理装置５は、例えばユーザーＡと同じ拠点に設置されており、ユーザーＡが使用可能である。
【００３５】
情報共有サーバー２は、Ｗｅｂサーバー機能、情報共有機能、ＴＶ会議機能などの様々な機能を備えており、予め登録された複数のユーザーＡ，Ｂ，Ｃ，Ｄが同じ情報を共有することができる情報共有サービスを提供する。例えば、情報共有サーバー２は、ユーザーＡが操作する情報処理装置４から文書データＤ１がアップロードされると、その文書データＤ１を保存して管理する。そして他のユーザーＢ，Ｃ，Ｄからその文書データＤ１の閲覧要求を受信すると、情報共有サーバー２は、ユーザーＡによってアップロードされた文書データＤ１を他のユーザーＢ，Ｃ，Ｄに公開する。
【００３６】
文書データＤ１をアップロードするとき、文書データＤ１が機密性の高い文書であれば、ユーザーＡは、情報処理装置４を操作することにより、文書データＤ１に対して任意のパスワードを設定し、文書データＤ１を暗号化する。そしてユーザーＡは、自身が設定し

たパスワードで暗号化された文書データＤ１を情報共有サーバー２へアップロードする。このとき、情報処理装置４は、暗号された文書データＤ１と共に、文書データＤ１を復号するためのパスワード（ユーザーＡによって設定されたパスワード）を情報共有サーバー２へ送信する。

【００３７】

この他にも、ユーザーＡは、画像処理装置５のスキャン機能を利用して原稿９を読み取って生成された文書データＤ１を情報共有サーバー２へアップロードすることもできる。この場合、画像処理装置５で生成される文書データＤ１を、ユーザーＡの情報処理装置４へ一旦転送した後、ユーザーＡの情報処理装置４から情報共有サーバー２へアップロードする第１の手法と、画像処理装置５で生成される文書データＤ１を、画像処理装置５から情報共有サーバー２へ直接アップロードする第２の手法とがある。第１の手法の場合、ユーザーＡがパスワードを設定して文書データＤ１を暗号化する処理は、画像処理装置５と情報処理装置４のいずれで行っても良い。これに対し、第２の手法の場合、画像処理装置５は、ユーザーＡによるパスワードの設定操作を受け付け、原稿９を読み取って生成した文書データＤ１を暗号化し、暗号化された文書データＤ１と共に、ユーザーＡによって設定されたパスワードを情報共有サーバー２へ送信する。

【００３８】

情報共有サーバー２は、ユーザーＡの情報処理装置４又は画像処理装置５から、暗号化された文書データＤ１と、パスワードと、を受信すると、それらを相互に関連付けた状態で記憶する。そして情報共有サーバー２は、ユーザーＡによってアップロードされた文書データＤ１を、予め登録された複数のユーザーＡ，Ｂ，Ｃ，Ｄによる共有対象の文書データとして管理する。

【００３９】

他のユーザーＢ，Ｃ，ＤがユーザーＡによってアップロードされた文書データＤ１を閲覧するとき、各ユーザーＢ，Ｃ，Ｄは、自身の情報処理装置４を操作することによって情報共有サーバー２にアクセスし、情報共有サーバー２にログインする。そして各ユーザーＢ，Ｃ，Ｄは、ユーザーＡによってアップロードされた文書データＤ１の閲覧要求を情報共有サーバー２へ送信する。

【００４０】

情報共有サーバー２は、他のユーザーＢ，Ｃ，Ｄからの閲覧要求を受信すると、ユーザーＡによってアップロードされた暗号化された文書データＤ１とパスワードとを読み出す。そしてユーザーＡによって設定されたパスワードを用いて暗号化された文書データＤ１を復号し、他のユーザーＢ，Ｃ，Ｄが閲覧可能な文書データＤ２を生成する。その後、情報共有サーバー２は、復号した文書データＤ２に基づく閲覧画面を生成し、他のユーザーＢ，Ｃ，Ｄの情報処理装置４へ送信する。これにより、他のユーザーＢ，Ｃ，Ｄは、ユーザーＡによって文書データＤ１に設定されたパスワードを知らなくても、文書データＤ１の中身を閲覧することができるようになる。以下、このような情報共有システム１について更に詳しく説明する。

【００４１】

まず情報処理装置４について説明する。図２は、情報処理装置４のハードウェア構成及び機能構成の一例を示すブロック図である。情報処理装置４は、ハードウェア構成として、ＣＰＵやメモリなどを備えて構成される制御部４０と、各種情報を記憶する記憶部４１と、カラー液晶ディスプレイなどで構成される表示部４２と、キーボードやマウス、タッチパネルなどで構成される操作部４３と、情報共有サーバー２などの他の装置と通信を行うための通信インタフェース４４とを備えている。

【００４２】

記憶部４１は、ハードディスクドライブ（ＨＤＤ）やソリッドステートドライブ（ＳＳＤ）などで構成される不揮発性の記憶手段である。この記憶部４１には、制御部４０のＣＰＵによって実行されるアプリケーションプログラム４５やブラウザプログラム４６が記憶されている。アプリケーションプログラムは、情報処理装置４において文書データＤ１

を作成する文書作成アプリケーション４７を起動させるためのプログラムである。ブラウザプログラム４６は、情報処理装置４においてＷｅｂページなどの閲覧画面を取得し、その閲覧画面を表示部４２に表示するＷｅｂブラウザ４８を起動させるためのプログラムである。また記憶部４１には、情報共有サーバー２へのアップロード対象となる文書データＤ１を記憶することが可能である。

【００４３】

文書作成アプリケーション４７は、操作部４３に対するユーザーの操作に基づいて文書の作成及び編集を行い、文書データＤ１を生成する処理部である。この文書作成アプリケーション４７は、パスワード設定部５１、文書データ暗号化部５２及び文書データ保存部５３を備えている。

【００４４】

パスワード設定部５１は、ユーザーの操作に基づいて作成した文書データＤ１を暗号化する際に機能し、パスワード設定画面を表示部４２に表示し、ユーザーによって操作部４３に入力されるパスワードを受け付ける。パスワード設定部５１は、ユーザーによって指定されたパスワードを文書データＤ１の暗号化用のパスワードに設定し、そのパスワードを文書データ暗号化部５２へ出力する。

【００４５】

文書データ暗号化部５２は、パスワード設定部５１によって設定されたパスワードを用いて文書データＤ１を暗号化する。これにより、文書データＤ１は、パスワードを入力しない限り、その内容を閲覧することができない暗号データに変換される。そして文書データ暗号化部５２は、暗号化された文書データＤ１を文書データ保存部５３へ出力する。

【００４６】

文書データ保存部５３は、暗号化された文書データＤ１を記憶部４１に保存する。尚、ユーザーによって文書データＤ１の暗号化が指定されていない場合、文書データ保存部５３は、暗号化されていない文書データＤ１を記憶部４１へ保存することもできる。

【００４７】

Ｗｅｂブラウザ４８は、通信インタフェース４４を介して、ユーザーによって指定されたＵＲＬのアドレスにアクセスし、そのアドレスにあるサーバーと通信を行い、サーバーから閲覧画面を取得して表示部４２に表示したり、閲覧画面に対するユーザーの操作に基づく操作情報をサーバーへ送信したりする。Ｗｅｂブラウザ４８は、閲覧表示部５５と、アップロード部５６とを備えている。閲覧表示部５５は、サーバーから閲覧画面を取得して表示部４２に表示させると共に、操作情報をサーバーへ送信するためのものであり、Ｗｅｂブラウザ４８に標準搭載されている機能である。アップロード部５６は、例えばサーバーから取得した閲覧画面に含まれるスクリプトプログラムなどをＷｅｂブラウザ４８が実行することによって実現される機能であり、ユーザーによって指定された文書データＤ１をサーバーへアップロードする処理部である。

【００４８】

例えばＷｅｂブラウザ４８が情報共有サーバー２にアクセスし、情報共有サーバー２から取得した閲覧画面に含まれるスクリプトプログラムを実行することによってアップロード部５６が機能した場合、アップロード部５６は、ユーザーによって指定された文書データＤ１を情報共有サーバー２へアップロードする。またアップロード部５６は、パスワードによって暗号化された文書データＤ１を情報共有サーバー２へアップロードするときには、暗号化された文書データＤ１と共に、文書データＤ１を復号するためのパスワードを情報共有サーバー２へアップロードする。そのため、アップロード部５６は、暗号化された文書データＤ１を情報共有サーバー２へアップロードするとき、表示部４２にパスワード入力画面を表示してユーザーによるパスワード入力操作を受け付ける。そしてユーザーによるパスワード入力操作が完了すると、アップロード部５６は、ユーザーによって入力されたパスワードを、暗号化された文書データＤ１と共に情報共有サーバー２へアップロードする。

【００４９】

したがって、情報処理装置４は、情報共有サーバー２に対して暗号化された文書データＤ１を送信するときには、暗号化された文書データＤ１だけでなく、その暗号化された文書データＤ１を復号するためのパスワードも同時に情報共有サーバー２へアップロードすることができる。

【００５０】

次に画像処理装置５について説明する。図３は、画像処理装置５のハードウェア構成及び機能構成の一例を示すブロック図である。画像処理装置５は、ハードウェア構成として、ＣＰＵやメモリなどを備えて構成される制御部６０と、各種情報を記憶する記憶部６１と、ユーザーが画像処理装置５を使用する際のユーザーインタフェースとなる操作パネル６２と、情報共有サーバー２などの他の装置と通信を行うための通信インタフェース６３と、原稿の画像を光学的に読み取るスキャナ部６４と、印刷出力を行うプリンタ部６５とを備えている。また操作パネル６２は、各種情報を表示する表示部６２ａと、ユーザーによる操作を受け付ける操作部６２ｂとを備えている。記憶部６１は、例えばハードディスクドライブ（ＨＤＤ）によって構成される不揮発性の記憶手段である。この記憶部６１には、制御部４０のＣＰＵによって実行されるプログラム６６や、画像処理装置５を使用するユーザーに関する情報が登録されたユーザー情報６７などが記憶される。

【００５１】

制御部６０のＣＰＵは、画像処理装置５の起動時に記憶部６１からプログラム６６を自動的に読み出して実行する。これにより、制御部６０は、ユーザー認証部７０、スキャンアプリケーション７１及び印刷ジョブ実行部７２として機能する。

【００５２】

ユーザー認証部７０は、画像処理装置５を使用するユーザーの認証処理を行う。例えばユーザー認証部７０は、ユーザーが操作パネル６２を操作することによって入力した情報がユーザー情報６７に登録されているか否かを判別することにより、ユーザー認証を行う。ユーザーによって入力された情報がユーザー情報に登録されていれば、認証成功となるため、ユーザー認証部７０は、画像処理装置５をユーザーが利用可能なログイン状態へ移行させる。これに対し、ユーザーによって入力された情報がユーザー情報に登録されていない場合、認証失敗となるため、ユーザーは画像処理装置５を利用することができない。

【００５３】

スキャンアプリケーション７１は、ユーザー認証に成功したログインユーザーがスキャン機能の利用を選択した場合に機能する。このスキャンアプリケーション７１は、例えばユーザー情報６７を参照し、画像処理装置５にログインしたユーザーが情報共有サーバー２を利用可能なユーザーであるか否かを判断する。その結果、ログインユーザーが情報共有サーバー２を利用可能なユーザーであれば、スキャン機能によって生成した文書データＤ１を情報共有サーバー２へアップロード可能な機能を動作させる。この場合、スキャンアプリケーション７１は、原稿読取制御部７５、文書データ生成部７６、パスワード受付部７７、暗号化部７８及びアップロード部７９として機能する。

【００５４】

原稿読取制御部７５は、スキャナ部６４に動作命令を出力することにより、ユーザーによってセットされた原稿９の読み取り動作を制御し、原稿９を読み取って生成されたデータを取得する。文書データ生成部７６は、原稿読取制御部７５が取得したデータを例えばＰＤＦ（Portable Document Format）などの所定のデータ形式に変換し、文書データＤ１を生成する。パスワード受付部７７は、ユーザーによって文書データＤ１の暗号化が指定された場合に機能し、ユーザーによるパスワードの入力操作を受け付ける。暗号化部７８は、文書データ生成部７６で生成された文書データＤ１を、ユーザーによって指定されたパスワードを用いて暗号化することにより暗号データに変換する。そしてアップロード部７９は、暗号化された文書データＤ１と、ユーザーによって指定されたパスワードとを情報共有サーバー２へアップロードする。尚、アップロード部７９は、文書データＤ１をアップロードするとき、ユーザー情報６７からログインユーザーに関する情報を抽出し、ログインユーザーに関する情報を情報共有サーバー２へ送信する。これにより、情報共有サ

ーバー２は、文書データＤ１をアップロードしたユーザーを特定することができるようになる。

【００５５】

印刷ジョブ実行部７２は、通信インタフェース６３を介して印刷ジョブや文書データＤ１を受信した場合に機能し、印刷ジョブや文書データＤ１に基づいてプリンタ部６５を駆動することにより、画像処理装置５において印刷出力を行わせるものである。

【００５６】

次に情報共有サーバー２について説明する。図４は、情報共有サーバー２のハードウェア構成及び機能構成の一例を示すブロック図である。図４に示すように、情報共有サーバー２は、ＣＰＵやメモリなどを備えて構成される制御部１０と、各種情報を記憶する記憶部１１と、情報処理装置４や画像処理装置５と通信を行うための通信インタフェース１２とを備えており、一般的なコンピュータと同様のハードウェア構成を有している。記憶部１１は、例えばハードディスクドライブ（ＨＤＤ）などによって構成される不揮発性の記憶手段である。この記憶部１１には、制御部１０のＣＰＵによって実行されるプログラム１３が予め記憶される。また記憶部１１には、文書データＤ１を共有する複数のユーザーに関する情報が登録される共有情報１４、複数のユーザーで共有される文書データＤ１、文書データＤ１に設定されるパスワード３１などが記憶される。

【００５７】

制御部１０のＣＰＵは、情報共有サーバー２が起動すると、記憶部１１からプログラム１３を読み出して実行する。これにより、制御部１０は、共有情報登録部２０、ユーザー認証部２１、アップロードデータ取得部２２、文書データ管理部２３、パスワード管理部２４、閲覧情報提供部２５、文書データ提供部２６及び印刷制御部２７として機能する。

【００５８】

共有情報登録部２０は、管理者などの設定操作に基づき、情報を共有する複数のユーザーに関する情報などを共有情報１４に登録する処理部である。例えば、共有情報登録部２０は、情報共有サーバー２に管理者がログインした場合に機能し、管理者による設定操作に基づき、情報を共有するグループや、そのグループにおいて他のユーザーと情報を共有することが可能なユーザーに関する情報を共有情報１４に登録する。

【００５９】

図５は、共有情報１４の一例を示す図である。図５に示すように、共有情報１４は、グループ情報１４ａと、共有ユーザー情報１４ｂと、認証情報１４ｃと、暗号鍵１４ｄと、復号鍵１４ｅと、識別情報１４ｆとを含む情報である。図５では、情報を共有するグループとして、グループＸとグループＹの２つのグループが登録された例を示している。グループＸでは、情報を共有するユーザーとして、４人のユーザーＡ，Ｂ，Ｃ，Ｄが登録されている。そのため、グループＸに属する４人のユーザーＡ，Ｂ，Ｃ，Ｄは、グループＸに対してアップロードされる文書データＤ１を共有することができる。またグループＹでは、情報を共有するユーザーとして、別の４人のユーザーＥ，Ｆ，Ｇ，Ｈが登録されている。そのため、グループＹに属する４人のユーザーＥ，Ｆ，Ｇ，Ｈは、グループＹに対してアップロードされる文書データＤ１を共有することができる。このようなグループ管理により、情報共有サーバー２は、ユーザーがログインするときに、そのログインユーザーが所属するグループを特定することができるようになり、ログインユーザーが所属するグループにアップロードされた文書データＤ１だけをログインユーザーに公開することができると共に、ログインユーザーが所属していないグループにアップロードされた文書データＤ１をログインユーザーに公開しないように制限することができる。

【００６０】

認証情報１４ｃは、個々のユーザーを識別するための情報であり、例えば各ユーザーに対して個別に付与されるランダムな文字列などによって構成される。尚、認証情報１４ｃは、ユーザーＩＤとパスワードとの組み合わせによって構成される情報であっても構わない。この認証情報１４ｃは、ユーザーからのログイン要求を受け付けた場合に、そのユーザーを認証するために用いられる。

【００６１】
暗号鍵１４ｄは、例えば管理者によってグループ毎に設定される鍵情報であり、暗号化された文書データＤ１を復号する際に用いるパスワードを暗号化する鍵情報である。復号鍵１４ｅは、暗号鍵１４ｄと対をなす復号用の鍵情報であり、例えば管理者によってグループ毎に設定され、暗号化されたパスワードを復号するために用いられる。
【００６２】
識別情報１４ｆは、例えば管理者によってグループ毎に設定されるユニークな情報である。この識別情報１４ｆは、例えば４～８桁程度の暗証番号（ＰＩＮコード）などで構成される。
【００６３】
ただし、識別情報１４ｆは、図５に示すように復号鍵１４ｅと別に管理されるものではなく、復号鍵１４ｅを利用するために予め復号鍵１４ｅに設定される情報であっても構わない。例えば、復号鍵１４ｅを生成するときのオプション機能として、復号鍵１４ｅに識別情報１４ｆを設定する機能がある。そのようなオプション機能を用いて、復号鍵１４ｅに識別情報１４ｆが設定されたものであれば、共有情報１４において、復号鍵１４ｅとは別に識別情報１４ｆを記憶しておく必要はない。この場合、例えば復号鍵１４ｅは、識別情報１４ｆによって暗号化された情報となる。
【００６４】
共有情報登録部２０は、共有情報１４に対して新規グループを登録すると、その新規グループに対して登録された複数のユーザーのそれぞれに対し、認証情報１４ｃ及び識別情報１４ｆを個別に通知する。また共有情報登録部２０は、共有情報１４に登録されている既存のグループに対して新規ユーザーを登録した場合、その新規ユーザーに認証情報１４ｃ及び識別情報１４ｆを通知する。また共有情報登録部２０は、各ユーザーに対して認証情報１４ｃ及び識別情報１４ｆを通知するとき、情報共有サーバー２へアクセスするためのアドレス情報などを添付して通知する。したがって、このような通知を受けたユーザーは、自身の情報処理装置４を操作することにより情報共有サーバー２へアクセスすることが可能になると共に、情報共有サーバー２へログインするための認証情報１４ｃ、及び、自身が属するグループに付与されている固有の識別情報１４ｆを把握することができる。尚、共有情報登録部２０による通知は例えば電子メールなどによって行われる。
【００６５】
ユーザー認証部２１は、通信インタフェース１２が情報処理装置４からのログイン要求を受け付けた場合に機能し、ユーザー認証処理を行う。ユーザー認証部２１は、ログイン要求に含まれる情報が、共有情報１４においてユーザー毎に登録されている認証情報１４ｃに一致するか否かを判断することによりユーザー認証処理を行う。ログイン要求に含まれる情報が認証情報１４ｃに一致する場合、認証成功となり、ユーザー認証部２１は、その認証情報１４ｃに対応するユーザーと、そのユーザーが属するグループとを特定する。そしてユーザー認証部２１は、そのグループに対してアップロードされている文書データＤ１をユーザーが利用可能なログイン状態へ移行させる。これに対し、ログイン要求に含まれる情報が認証情報１４ｃに一致しない場合、認証失敗となるため、ユーザー認証部２１は、ログイン状態へは移行させない。
【００６６】
アップロードデータ取得部２２は、通信インタフェース１２がアップロードデータを受信した場合に機能し、情報処理装置４又は画像処理装置５からのアップロードデータを取得する処理部である。アップロードデータ取得部２２は、アップロードデータを取得すると、そのアップロードデータに含まれる情報からアップロードユーザーを特定し、共有情報１４を参照することにより、そのアップロードユーザーが属するグループを特定する。
【００６７】
またアップロードデータ取得部２２は、アップロードデータに暗号化された文書データＤ１と、パスワードとが含まれる場合、アップロードデータから文書データＤ１とパスワードとを分類する。そして暗号化された文書データＤ１を文書データ管理部２３へ出力し

、パスワードをパスワード管理部２４へ出力する。またアップロードデータ取得部２２は、アップロードデータに含まれるパスワードを暗号化してパスワード管理部２４へ出力するように構成される。

【００６８】

図６は、アップロードデータ取得部２２による暗号化処理の概念を示す図である。図６に示すようにアップロードデータ取得部２２は、暗号化部２２ａを備えている。この暗号化部２２ａは、情報処理装置４又は画像処理装置５から受信したアップロードデータにパスワードが含まれる場合に機能する。そして暗号化部２２ａは、アップロードデータを送信したユーザーが属するグループに登録されている暗号鍵１４ｄを共有情報１４から読み出し、情報処理装置４又は画像処理装置５から受信したパスワード３０をその暗号鍵１４ｄで暗号化する。すなわち、暗号化部２２ａは、文書データＤ１が共有されるグループに対して予め設定されている暗号鍵１４ｄを用いてパスワード３０を暗号化することにより、暗号化パスワード３１を生成するのである。そしてアップロードデータ取得部２２は、その暗号化パスワード３１をパスワード管理部２４へ出力する。

【００６９】

文書データ管理部２３は、アップロードデータ取得部２２から出力される文書データＤ１を記憶部１１に保存して管理する。またパスワード管理部２４は、アップロードデータ取得部２２から出力される暗号化パスワード３１を記憶部１１に保存して管理する。これらの文書データ管理部２３とパスワード管理部２４は、暗号化された文書データＤ１と、暗号化パスワード３１とを相互に関連付けた管理情報３５を生成し、その管理情報３５を共有することで、暗号化された文書データＤ１と暗号化パスワード３１とを１対１で関連付けて管理する。

【００７０】

図７は、管理情報３５の一例を示す図である。管理情報３５には、グループ情報３５ａと、共有文書ファイル名情報３５ｂと、アップロードユーザー情報３５ｃと、パスワード情報３５ｄとが含まれる。グループ情報３５ａは、文書データＤ１が共有されるグループを示す情報である。共有文書ファイル名情報３５ｂは、共有される文書データＤ１のファイル名を示す情報である。アップロードユーザー情報３５ｃは、文書データＤ１をアップロードしたユーザーを示す情報である。パスワード情報３５ｄは、文書データＤ１を復号するパスワード３０が暗号化された暗号化パスワード３１を特定するための情報である。したがって、図７に示す管理情報３５を参照すれば、記憶部１１に記憶される文書データＤ１がどのグループに共有されるデータであるかを特定することができると共に、個々の文書データＤ１に対応する暗号化パスワード３１を特定することも可能である。また管理情報３５を参照すれば、文書データＤ１のアップロードユーザーも特定することができる。文書データ管理部２３及びパスワード管理部２４によってこのような管理情報３５が共有して管理されることにより、暗号化された文書データＤ１は、共有対象となるグループ、アップロードユーザー及び暗号化パスワード３１を特定することが可能な状態で記憶部１１に保存されることになる。

【００７１】

閲覧情報提供部２５は、情報共有サーバー２がログインユーザーによるログイン状態へ移行することにより機能し、ログインユーザーが共有可能な文書データＤ１の閲覧情報を提供する処理部である。例えば、閲覧情報提供部２５は、ログインユーザーによるログイン状態となると、共有情報１４を参照することによってそのログインユーザーが属するグループを特定する。そして閲覧情報提供部２５は、文書データ管理部２３に対して特定したグループを通知し、文書データ管理部２３からログインユーザーが属するグループにおいて共有されている文書データＤ１の一覧情報を取得する。閲覧情報提供部２５は、その一覧情報に基づき、ログインユーザーが操作する情報処理装置４に対して一覧情報を提供する。これにより、ログインユーザーは、自身が閲覧可能な文書データＤ１の一覧を把握することができ、その一覧の中から所望の文書データＤ１を選択して情報共有サーバー２に閲覧要求を送信することができる。

【００７２】
閲覧情報提供部２５は、ログインユーザーの情報処理装置４から文書データＤ１を指定した閲覧要求を受信すると、復号部２５ａ、閲覧情報生成部２５ｂ及び閲覧情報送信部２５ｃを順次機能させる。
【００７３】
復号部２５ａは、ログインユーザーによって指定された文書データＤ１であって、暗号化された文書データＤ１を復号する処理部である。図８は、この復号部２５ａの詳細な機能構成の一例を示す図である。復号部２５ａは、図８に示すように、識別情報受付部８１と、識別情報判定部８２と、復号鍵取得部８３と、パスワード復号部８４と、文書データ復号部８５とを備えている。
【００７４】
識別情報受付部８１は、ログインユーザーによる識別情報の入力操作を受け付ける処理部である。この識別情報受付部８１は、ログインユーザーの情報処理装置４に対して識別情報の入力操作を促す識別情報入力画面を送信する。その後、識別情報受付部８１は、ログインユーザーが識別情報入力画面に対して入力した識別情報を受信すると、その識別情報を識別情報判定部８２へ出力する。
【００７５】
識別情報判定部８２は、ログインユーザーによって入力された識別情報が共有情報１４に登録されている識別情報１４ｆに一致するか否かを判定する処理部である。すなわち、識別情報判定部８２は、識別情報受付部８１からログインユーザーによって入力された識別情報を取得すると、共有情報１４を参照し、その識別情報がログインユーザーの属するグループに登録されている識別情報１４ｆと一致するか否かを判定する。このようにユーザーが情報共有サーバー２にログインしている状態であっても、さらにログインユーザーに識別情報の入力を促して共有情報１４に予め登録されている識別情報１４ｆと一致するか否かを判定することにより、ログインユーザーのなりすましによって文書データＤ１が閲覧されてしまうことを未然に防止することができ、セキュリティの高いシステムが実現される。
【００７６】
復号鍵取得部８３は、識別情報判定部８２によってログインユーザーの入力した識別情報が共有情報１４に登録されている識別情報１４ｆと一致した場合に機能する。そして復号鍵取得部８３は、共有情報１４を参照し、ログインユーザーの属するグループに登録されている復号鍵１４ｅを取得する。復号鍵取得部８３が復号鍵１４ｅを取得すると、その復号鍵１４ｅをパスワード復号部８４へ出力する。
【００７７】
尚、上述したように、復号鍵１４ｅに識別情報１４ｆが設定されている場合には、上述した識別情報判定部８２は特に必要ではない。すなわち、この場合は、復号鍵取得部８３がログインユーザーによって入力された識別情報１４ｆを用いて復号鍵１４ｅを取得するようにすれば良い。例えばログインユーザーによって入力された識別情報１４ｆを用いて暗号化された復号鍵１４ｅを復号するのである。そして復号鍵取得部８３は、識別情報１４ｆを用いて取得した復号鍵１４ｅをパスワード復号部８４へ出力する。ただし、ログインユーザーによって入力された識別情報１４ｆを用いても、ログインユーザーの属するグループに登録されている復号鍵１４ｅを正常に取得することができないこともある。例えば、ログインユーザーによって入力された識別情報１４ｆでは、復号鍵１４ｅを正常に復号することができない場合などである。そのような場合、これ以後の処理は行われないので、ログインユーザーのなりすましによって文書データＤ１が不正に閲覧されてしまうことを未然に防止することができる。
【００７８】
パスワード復号部８４は、復号鍵１４ｅを取得すると、パスワード管理部２４に対し、ログインユーザーが指定した暗号化された文書データＤ１を復号するための暗号化パスワード３１を問い合わせる。その後、パスワード復号部８４は、パスワード管理部２４から

の回答に基づき、記憶部１１から暗号化パスワード３１を読み出して取得する。そしてパスワード復号部８４は、復号鍵取得部８３から取得した復号鍵１４ｅを用いて暗号化パスワード３１を復号する。これにより、暗号化パスワード３１は、ログインユーザーが指定した暗号化された文書データＤ１を復号する際に用いられるパスワード３０に復元される。

【００７９】

続いて文書データ復号部８５が機能する。文書データ復号部８５は、パスワード復号部８４から復号されたパスワード３０を取得すると、文書データ管理部２３に対し、ログインユーザーが指定した暗号化された文書データＤ１を問い合わせる。その後、文書データ復号部８５は、文書データ管理部２３からの回答に基づき、記憶部１１から閲覧対象として指定された暗号化された文書データＤ１を読み出して取得する。そして文書データ復号部８５は、復号されたパスワード３０を用いて暗号化された文書データＤ１を復号する。これにより、暗号化された文書データＤ１は、その中身を閲覧することが可能な文書データＤ２に変換される。

【００８０】

図４に戻り、上記のようにして復号された文書データＤ２が生成されると、次に閲覧情報提供部２５において閲覧情報生成部２５ｂが機能する。閲覧情報生成部２５ｂは、復号された文書データＤ２に基づいて閲覧用画像を生成し、その閲覧用画像を含む閲覧画面を生成する処理部である。図９は、閲覧情報生成部２５ｂの詳細な機能構成の一例を示す図である。閲覧情報生成部２５ｂは、図９に示すように、閲覧用画像生成部９１と、閲覧画面生成部９２とを備えている。また閲覧画面生成部９２は、保存禁止設定部９２ａと、印刷禁止設定部９２ｂとを備えている。

【００８１】

閲覧用画像生成部９１は、復号された文書データＤ２に基づいて閲覧用画像を生成するものである。この閲覧用画像は、例えばビットマップなどの画像データであり、文書データＤ２に含まれるテキストなどのコンテンツをそのまま画像化したプレビュー用の画像データである。そのため、ログインユーザーが情報処理装置４に表示される閲覧用画像を閲覧しているときに、文書データＤ２に含まれるテキストなどのコンテンツデータがオリジナルデータのままでコピーされてしまうことを未然に防止することができる。

【００８２】

閲覧画面生成部９２は、閲覧用画像生成部９１によって文書データＤ２に基づく閲覧用画像が生成されると、その閲覧用画像を含む閲覧画面を生成する。この閲覧画面は、例えばＨＴＴＰ（Hypertext Transfer Protocol）などで記述されたＷｅｂページとして生成される。また閲覧情報送信部２５ｃは、閲覧画面を生成するとき、保存禁止設定部９２ａ及び印刷禁止設定部９２ｂを機能させる。

【００８３】

保存禁止設定部９２ａは、情報処理装置４において起動されているＷｅｂブラウザ４８の閲覧画面の保存機能を無効にする処理部である。例えば保存禁止設定部９２ａは、Ｗｅｂページとして生成される閲覧画面に、Ｗｅｂブラウザ４８の保存機能を無効にするコマンドを組み込むことにより、閲覧画面の保存禁止設定を行う。そのため、ログインユーザーが情報処理装置４に表示される閲覧画面を閲覧しているときに、Ｗｅｂブラウザ４８の保存機能により、情報共有サーバー２が関与できない状態で閲覧用画像が保存されてしまうことを防止することができる。

【００８４】

また印刷禁止設定部９２ｂは、情報処理装置４において起動されているＷｅｂブラウザ４８の閲覧画面の印刷機能を無効にする処理部である。例えば印刷禁止設定部９２ｂは、上記と同様、Ｗｅｂページとして生成される閲覧画面に、Ｗｅｂブラウザ４８の印刷機能を無効にするコマンドを組み込むことにより、閲覧画面の印刷禁止設定を行う。そのため、ログインユーザーが情報処理装置４に表示される閲覧画面を閲覧しているときに、Ｗｅｂブラウザ４８の印刷機能により、情報共有サーバー２が関与できない状態で閲覧用画像

が印刷出力されてしまうことを防止することができる。

【００８５】

再び図４に戻り、上記のようにして閲覧画面が生成されると、次に閲覧情報提供部２５において閲覧情報送信部２５ｃが機能する。閲覧情報送信部２５ｃは、閲覧情報生成部２５ｂによって生成された閲覧用画像を含む閲覧画面を、閲覧要求の送信元であるログインユーザーの情報処理装置４へ送信する。これにより、ログインユーザーの情報処理装置４は、Ｗｅｂブラウザ４８の機能によって情報共有サーバー２から取得した閲覧画面を表示部４２に表示する。

【００８６】

図１０は、情報処理装置４において表示される閲覧画面Ｇ１の一例を示す図である。この閲覧画面Ｇ１は、情報処理装置４において起動されているＷｅｂブラウザ４８によって表示される画面である。例えば閲覧画面Ｇ１の中央の表示領域Ｒ１には、図１０に示すように復号された文書データＤ２に基づく閲覧用画像が表示される。ただし、この閲覧画面Ｇ１には上述した保存禁止設定や印刷禁止設定が施されているため、ログインユーザーは、Ｗｅｂブラウザ４８の機能を利用した閲覧画面Ｇ１の保存や印刷を行うことはできない。

【００８７】

また図１０に示すように、閲覧画面Ｇ１の下部には、文書一覧ボタンＢ１と、ダウンロードボタンＢ２と、印刷ボタンＢ３と、終了ボタンＢ４とが含まれている。文書一覧ボタンＢ１は、ログインユーザーが閲覧可能な文書一覧を情報共有サーバー２へ要求するボタンである。ダウンロードボタンＢ２は、現在閲覧中である文書データＤ１のダウンロードを情報共有サーバー２へ要求するボタンである。印刷ボタンＢ３は、現在閲覧中である文書データＤ１の印刷を情報共有サーバー２へ要求するボタンである。さらに終了ボタンＢ４は、文書データＤ１の閲覧を終了することを情報共有サーバー２へ通知するボタンである。

【００８８】

ログインユーザーは、現在閲覧中である文書データＤ１を入手したい場合、ダウンロードボタンＢ２を操作する。これにより、Ｗｅｂブラウザ４８は、情報共有サーバー２へダウンロード要求を送信する。またログインユーザーは、現在閲覧中である文書データＤ１を印刷したい場合、印刷ボタンＢ３を操作する。これにより、Ｗｅｂブラウザ４８は、情報共有サーバー２へ印刷要求を送信する。

【００８９】

図４に戻り、文書データ提供部２６は、情報共有サーバー２が情報処理装置４からダウンロード要求を受信した場合に機能し、ログインユーザーによって指定された文書データＤ１をダウンロード要求の送信元である情報処理装置４へ提供する処理部である。この文書データ提供部２６は、データ送信部２６ａと、通知部２６ｂとを備えている。

【００９０】

データ送信部２６ａは、ダウンロード対象である暗号化された文書データＤ１を記憶部１１から取得すると共に、その暗号化された文書データＤ１を復号するためのパスワード３０を閲覧情報提供部２５から取得する。尚、データ送信部２６ａは、記憶部１１から暗号化パスワード３１を読み出し、復号鍵１４ｅを用いて暗号化パスワード３１を復号することにより、パスワード３０を取得するようにしても良い。そしてデータ送信部２６ａは、暗号化された文書データＤ１と、パスワード３０とを、ダウンロード要求の送信元であるログインユーザーの情報処理装置４へ送信する。これにより、ログインユーザーは、暗号化された文書データＤ１及びパスワード３０をダウンロード取得することができるため、パスワード３０を用いて暗号化された文書データＤ１を復号することにより、文書データＤ１を利用することができるようになる。

【００９１】

またデータ送信部２６ａは、暗号化された文書データＤ１とパスワード３０とをそれぞれ異なる通信経路で送信するようにしても良い。例えば、データ送信部２６ａは、暗号化

された文書データＤ１を情報処理装置４のＷｅｂブラウザ４８に対して送信し、パスワード３０を電子メールなどによってログインユーザーへ送信するようにしても良い。このように暗号化された文書データＤ１とパスワード３０とをそれぞれ異なる通信経路で送信することにより、セキュリティのより一層高いシステムが実現される。

【００９２】

通知部２６ｂは、データ送信部２６ａによって暗号化された文書データＤ１とパスワード３０の送信が行われることに伴い、文書データＤ１をアップロードしたユーザーに対して文書データＤ１がダウンロードされたことを通知する処理部である。通知部２６ｂがアップロードユーザーに対して通知を行う際には、文書データＤ１をダウンロードしたユーザーや、ダウンロード日時なども通知することが好ましい。また通知部２６ｂは、文書データＤ１のアップロードユーザーだけではなく、同じグループに属する全てのユーザーに通知を行うようにしても良いし、また管理者にも通知を行うようにしても良い。

【００９３】

印刷制御部２７は、情報共有サーバー２が情報処理装置４から印刷要求を受信した場合に機能するものである。印刷制御部２７は、ログインユーザーによって指定された文書データＤ１を、ログインユーザーによって指定された印刷装置へ送信する。印刷制御部２７は、印刷要求を受信すると、印刷要求の送信元である情報処理装置４と同じローカルネットワークに存在する印刷装置を検索する。その結果、情報処理装置４と同じローカルネットワーク内に印刷装置が存在する場合、印刷制御部２７は、その印刷装置をログインユーザーに提示し、ログインユーザーによる印刷装置の指定操作を受け付ける。尚、検索によって印刷装置が見付からなかった場合、印刷制御部２７は、ログインユーザーによる印刷装置の手動設定操作を受け付け、その手動設定操作に基づいて印刷データの送信先となる印刷装置を特定する。このような印刷制御部２７は、印刷データ送信部２７ａと、通知部２７ｂとを備えている。

【００９４】

印刷データ送信部２７ａは、印刷データの送信先として特定された印刷装置に対して印刷データを送信する処理部である。この印刷データ送信部２７ａは、印刷データの送信先として特定された印刷装置に対応するプリンタドライバがインストールされているか否かを判断し、プリンタドライバがインストールされていれば、そのプリンタドライバを起動し、特定された印刷装置において実行可能な印刷ジョブを生成する。すなわち、印刷データ送信部２７ａは、プリンタドライバを起動して印刷ジョブを印刷装置へ送信する場合、復号された文書データＤ２に基づいて印刷ジョブを生成し、その印刷ジョブを印刷装置へ送信する。

【００９５】

これに対し、印刷データの送信先として特定された印刷装置に対応するプリンタドライバがインストールされていない場合、印刷データ送信部２７ａは、特定された印刷装置がダイレクトプリント対応機種であると判断し、文書データＤ１をそのまま印刷装置へ送信する。すなわち、印刷装置がダイレクトプリント対応機種である場合、印刷データ送信部２７ａは、暗号化された文書データＤ１と、その文書データＤ１を復号するためのパスワード３０とを印刷装置へ送信し、印刷装置において暗号化された文書データＤ１を復号させることによって印刷可能な文書データＤ２を生成させて印刷出力を行わせる。

【００９６】

例えば上述した画像処理装置５が印刷装置として特定された場合、画像処理装置５は、情報共有サーバー２から、暗号化された文書データＤ１とパスワード３０とを受信する。これに伴い、画像処理装置５において印刷ジョブ実行部７２が動作する。そして印刷ジョブ実行部７２は、パスワード３０を用いて暗号化された文書データＤ１を復号する。これにより、印刷ジョブ実行部７２は、印刷可能な文書データＤ２を取得することができる。そして印刷ジョブ実行部７２は、復号した文書データＤ２に基づいて印刷出力を行う。したがって、この場合、情報共有サーバー２は、画像処理装置５に対応するプリンタドライバをインストールしていなくても、画像処理装置５に印刷出力を行わせることができるた

め、情報共有サーバー２の負荷を軽減することができる。

【００９７】

通知部２７ｂは、印刷データ送信部２７ａによって印刷データが印刷装置へ送信されることに伴い、文書データＤ１をアップロードしたユーザーに対して印刷出力が行われたことを通知する処理部である。通知部２７ｂがアップロードユーザーに対して通知を行う際には、印刷出力を行ったユーザーや、印刷日時なども通知することが好ましい。また通知部２７ｂは、文書データＤ１のアップロードユーザーだけではなく、同じグループに属する全てのユーザーに通知を行うようにしても良いし、また管理者にも通知を行うようにしても良い。

【００９８】

このように情報共有サーバー２は、ログインユーザーによって文書データＤ１のダウンロードや印刷出力が行われると、それをログインユーザーとは異なる他のユーザーであって、少なくとも同一グループに属するユーザーに通知するため、万一、文書データＤ１が第三者に漏洩した場合には漏洩元を速やかに特定することができるという利点がある。

【００９９】

次に上記のような情報共有システム１において行われる動作の概要について説明する。図１１は、ユーザーＡが文書データＤ１を情報共有サーバー２へアップロードし、ユーザーＢがその文書データＤ１を閲覧する場合の動作シーケンスを示す図である。尚、図１１では、ユーザーＡが情報処理装置４ａを操作し、ユーザーＢが情報処理装置４ｂを操作する場合を例示している。

【０１００】

まずユーザーＡは、情報処理装置４ａを操作することにより、情報共有サーバー２へのアップロード対象となる文書データＤ１を作成する（プロセスＰ１０）。その文書データＤ１が機密情報を含んでいる場合、ユーザーＡは、情報処理装置４ａに対してパスワード３０を入力し（プロセスＰ１１）、文書データＤ１をそのパスワード３０で暗号化する（プロセスＰ１２）。その後、ユーザーＡは、情報処理装置４ａを操作することによって情報共有サーバー２へログインし、情報共有サーバー２へ暗号化された文書データＤ１をアップロードする。このとき、情報処理装置４ａは、暗号化された文書データＤ１を復号するためのパスワード３０を情報共有サーバー２へ送信する。

【０１０１】

情報共有サーバー２は、情報処理装置４ａから暗号化された文書データＤ１とパスワード３０とを受信すると、共有情報１４を参照することにより、ユーザーＡが属するグループを特定し、ユーザーＡが属するグループに設定されている暗号鍵１４ｄを取得する。そして情報共有サーバー２は、情報処理装置４ａから受信したパスワード３０を暗号鍵１４ｄで暗号化し、暗号化パスワード３１を生成する（プロセスＰ１３）。続いて情報共有サーバー２は、暗号化された文書データＤ１と、暗号化パスワード３１とを相互に関連付けて記憶部１１へ保存する（プロセスＰ１４）。このとき、情報処理装置４ａから受信したパスワード３０は、暗号化された暗号化パスワード３１として記憶部１１に保存されるため、仮に暗号化された文書データＤ１と暗号化パスワード３１とが不正に読み出されたとしても、暗号化された文書データＤ１を復号することはできず、情報漏洩を防止することができる。尚、情報共有サーバー２は、情報処理装置４ａから受信したパスワード３０を暗号鍵１４ｄで暗号化することに伴い、オリジナルのパスワード３０を削除しておくことが好ましい。そして情報共有サーバー２は、ユーザーＡによってアップロードされた文書データＤ１を、ユーザーＡと同じグループに属する他のユーザーに公開する。

【０１０２】

ユーザーＡと同一グループに属するユーザーＢは、文書データＤ１を閲覧するとき、情報処理装置４ｂを操作することによってＷｅｂブラウザ４８を起動し、情報共有サーバー２にアクセスする。これにより、情報処理装置４ｂには情報共有サーバー２にログインするための画面が表示される。ユーザーＢは、その画面に対して事前に通知されている自身の認証情報１４ｃを入力し、情報共有サーバー２に対してログイン要求Ｄ１０を送信する

。情報共有サーバー２は、ログイン要求Ｄ１０を受信すると、ユーザー認証を行い（プロセスＰ１５）、ユーザーＢが共有情報１４に登録された正規ユーザーであれば、ユーザーＢが閲覧可能な文書データＤ１の一覧を情報処理装置４ｂへ送信する。これにより、ユーザーＢは、自身が所属するグループにおいて公開されている文書データＤ１の一覧を入手することができ、その一覧の中から一の文書データＤ１を指定した閲覧要求Ｄ１１を情報共有サーバー２へ送信することができるようになる。

【０１０３】

情報共有サーバー２は、情報処理装置４ｂから閲覧要求Ｄ１１を受信すると、ユーザーＢが所属するグループに登録されている復号鍵１４ｅを読み出し、閲覧対象として指定された文書データＤ１に関連付けられている暗号化パスワード３１を復号する（プロセスＰ１６）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号するためのパスワード３０に変換される。そして情報共有サーバー２は、その復号されたパスワード３０を用いて、暗号化された文書データＤ１を復号する（プロセスＰ１７）。これにより、暗号化された文書データＤ１は、閲覧可能な文書データＤ２に復号される。その後、情報共有サーバー２は、復号された文書データＤ２に基づく閲覧用画像を含む閲覧画面Ｇ１を生成し（プロセスＰ１８）、その閲覧画面Ｇ１を情報処理装置４ｂへ送信する。情報処理装置４ｂは、情報共有サーバー２から閲覧画面Ｇ１を受信すると、その閲覧画面Ｇ１を表示部４２に表示する。これにより、ユーザーＢは、文書データＤ１の中身を閲覧することができるようになる。したがって、ユーザーＢは、ユーザーＡによって文書データＤ１に設定されたパスワードを知らなくても、文書データＤ１の中身を閲覧することができるのである。

【０１０４】

次に図１２は、ユーザーＢが文書データＤ１をダウンロードする場合の動作シーケンスを示す図である。ユーザーＢが文書データＤ１を閲覧しているときにダウンロードボタンＢ２を操作すると、情報処理装置４ｂは、情報共有サーバー２に対し、現在閲覧中の文書データＤ１のダウンロード要求Ｄ１２を送信する。情報共有サーバー２は、情報処理装置４ｂからダウンロード要求Ｄ１２を受信すると、ダウンロード対象として指定された文書データＤ１であって暗号化された文書データＤ１を記憶部１１から読み出す（プロセスＰ２０）。そして情報共有サーバー２は、ダウンロード対象の文書データＤ１に関連付けている暗号化パスワード３１を読み出し、復号鍵１４ｅを用いてその暗号化パスワード３１を復号する（プロセスＰ２１）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号するためのパスワード３０に変換される。そして情報共有サーバー２は、暗号化された文書データＤ１と、復号されたパスワード３０とを情報処理装置４ｂへ送信する。その結果、ユーザーは、情報処理装置４ｂにおいて暗号化された文書データＤ１を、パスワード３０を用いて復号することができるようになる。そして情報共有サーバー２は、文書データＤ１のアップロードユーザーであるユーザーＡに対して通知Ｄ１３を送信し、文書データＤ１がユーザーＢによってダウンロードされたことを通知する。これにより、ユーザーＡは、自身が作成した機密性のある文書がユーザーＢによって入手されたことをリアルタイムで把握することができる。

【０１０５】

次に図１３は、ユーザーＢが文書データＤ１を印刷する場合の動作シーケンスを示す図である。尚、図１３では、ユーザーＢが画像処理装置５を印刷装置として指定した場合を例示している。ユーザーＢが文書データＤ１を閲覧しているときに印刷ボタンＢ３を操作すると、情報処理装置４ｂは、情報共有サーバー２に対し、現在閲覧中の文書データＤ１の印刷要求Ｄ１４を送信する。情報共有サーバー２は、情報処理装置４ｂから印刷要求Ｄ１４を受信すると、画像処理装置５が印刷装置として指定されたことを検知する。そして画像処理装置５に対応するプリンタドライバがインストールされていない場合、情報共有サーバー２は、画像処理装置５に対して暗号化された文書データＤ１とパスワード３０とを送信することを決定する。この場合、情報共有サーバー２は、印刷対象として指定された文書データＤ１であって暗号化された文書データＤ１を記憶部１１から読み出す（プロ

セスＰ２５）。また情報共有サーバー２は、印刷対象の文書データＤ１に関連付けている暗号化パスワード３１を読み出し、復号鍵１４ｅを用いてその暗号化パスワード３１を復号する（プロセスＰ２６）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号するためのパスワード３０に変換される。そして情報共有サーバー２は、暗号化された文書データＤ１と、復号されたパスワード３０とを画像処理装置５へ送信する。

【０１０６】

画像処理装置５は、情報共有サーバー２から暗号化された文書データＤ１とパスワード３０とを受信すると、パスワード３０を用いて暗号化された文書データＤ１を復号する（プロセスＰ２７）。これにより、暗号化された文書データＤ１は、印刷可能な文書データＤ２に変換される。そして画像処理装置５は、復号した文書データＤ２に基づき印刷出力を行う（プロセスＰ２８）。一方、情報共有サーバー２は、暗号化された文書データＤ１とパスワード３０とを画像処理装置５へ送信することに伴い、文書データＤ１のアップロードユーザーであるユーザーＡに対する通知処理を行う（プロセスＰ２９）。これにより、ユーザーＡは、自身が作成した機密性のある文書がユーザーＢによって印刷出力されたことをリアルタイムで把握することができる。

【０１０７】

次に情報共有サーバー２によって行われる具体的な処理手順の一例について説明する。図１４乃至図１８は、情報共有サーバー２によって行われる処理手順の一例を示すフローチャートである。この処理は、情報共有サーバー２の制御部１０に設けられたＣＰＵがプログラム１３を読み出して実行することにより行われる処理である。

【０１０８】

情報共有サーバー２は、この処理を開始すると、図１４に示すようにまず登録処理を行うか否かを判断する（ステップＳ１）。ここでは、例えば管理者によって新規グループや新規ユーザーの登録が指示されたか否かが判断される。そして登録処理を行う場合（ステップＳ１でＹＥＳ）、情報共有サーバー２は、共有情報登録処理を実行する（ステップＳ２）。この共有情報登録処理（ステップＳ２）は、管理者による新規グループや新規ユーザーの登録操作に基づいて共有情報１４に新規な情報を登録処理である。尚、登録処理を行わない場合は（ステップＳ１でＮＯ）、ステップＳ２の処理はスキップする。

【０１０９】

続いて情報共有サーバー２は、情報処理装置４からのログイン要求Ｄ１０を受信したか否かを判断する（ステップＳ３）。ログイン要求Ｄ１０を受信した場合（ステップＳ３でＹＥＳ）、情報共有サーバー２は、ユーザー認証を行い（ステップＳ４）、認証成功となったか否かを判断する（ステップＳ５）。認証成功である場合（ステップＳ５でＹＥＳ）、情報共有サーバー２は、ログイン要求Ｄ１０を送信したユーザーをログインユーザーとしてログイン状態へ移行させる（ステップＳ６）。これにより、ログインユーザーは、自身が所属するグループで共有される文書データＤ１の閲覧などが可能となる。ログイン状態へ移行させると、情報共有サーバー２は、ログインユーザーからアップロードデータを受信したか否かを判断し（ステップＳ７）、アップロードデータを受信していれば（ステップＳ７でＹＥＳ）、文書データ登録処理を実行する（ステップＳ８）。尚、この文書データ登録処理の詳細は後述する。また情報共有サーバー２は、ログインユーザーから閲覧要求Ｄ１１を受信したか否かを判断し（ステップＳ９）、閲覧要求Ｄ１１を受信していれば（ステップＳ９でＹＥＳ）、閲覧情報提供処理を実行する（ステップＳ１０）。尚、この閲覧情報提供処理の詳細は後述する。続いて情報共有サーバー２は、ログインユーザーからダウンロード要求Ｄ１２を受信したか否かを判断し（ステップＳ１１）、ダウンロード要求Ｄ１２を受信していれば（ステップＳ１１でＹＥＳ）、文書データ提供処理を実行する（ステップＳ１２）。尚、この文書データ提供処理の詳細についても後述する。さらに情報共有サーバー２は、ログインユーザーから印刷要求Ｄ１４を受信したか否かを判断し（ステップＳ１３）、印刷要求Ｄ１４を受信していれば（ステップＳ１３でＹＥＳ）、印刷制御処理を実行する（ステップＳ１４）。尚、この印刷制御処理の詳細についても後

述する。ユーザーが情報共有サーバー２にログインしている状態のときには（ステップＳ１５でＮＯ）、上記ステップＳ７～Ｓ１４の処理が繰り返し行われる。これに対し、ユーザーがログインしなかった場合には（ステップＳ３でＮＯ又はステップＳ５でＮＯ）、ステップＳ７～Ｓ１４の処理は行われずにスキップする。そして情報共有サーバー２は、上記ステップＳ１～Ｓ１５の処理を繰り返し実行する。

【０１１０】

図１５は、文書データ登録処理（ステップＳ８）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー２は、この処理を開始すると、アップロードデータとして取得した文書データＤ１を解析し（ステップＳ２０）、文書データＤ１が暗号化されているか否かを判断する（ステップＳ２１）。その結果、文書データＤ１が暗号化されている場合（ステップＳ２１でＹＥＳ）、情報共有サーバー２は、暗号化された文書データＤ１と共に、パスワード３０を受信したか否かを判断する（ステップＳ２２）。ここでパスワード３０を受信していないことが判明した場合（ステップＳ２２でＮＯ）、情報共有サーバー２は、アップロードを行った情報処理装置４においてパスワード要求画面を表示させる（ステップＳ２３）。これにより、アップロードユーザーは、暗号化された文書データＤ１を復号するためのパスワードを入力することが可能となり、情報共有サーバー２にパスワード３０が送信される。その結果、情報共有サーバー２は、情報処理装置４からパスワード３０を受信する（ステップＳ２４）。尚、受信したアップロードデータにパスワード３０が含まれていれば（ステップＳ２２でＹＥＳ）、ステップＳ２３，Ｓ２４の処理は不要である。

【０１１１】

続いて情報共有サーバー２は、アップロードユーザーが属するグループを特定し、そのグループに登録されている暗号鍵１４ｄを読み出し（ステップＳ２５）、情報処理装置４から受信したパスワード３０を暗号鍵１４ｄで暗号化する（ステップＳ２６）。これに伴い、情報共有サーバー２は、情報処理装置４から受信したパスワード３０を破棄するようにしても良い。そして情報共有サーバー２は、暗号化された文書データＤ１と、暗号化パスワード３１とを相互に関連付けて記憶部１１に保存する（ステップＳ２７）。

【０１１２】

一方、アップロードデータに含まれる文書データＤ１が暗号化されていない場合（ステップＳ２１でＮＯ）、情報共有サーバー２は、文書データＤ１の機密性が低いと判断し、受信した文書データＤ１をそのまま記憶部１１に保存して管理する（ステップＳ２８）。

【０１１３】

次に図１６は、閲覧情報提供処理（ステップＳ１０）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー２は、この処理を開始すると、まず閲覧対象の文書データＤ１を特定し（ステップＳ３０）。その文書データＤ１が暗号化されているか否かを判断する（ステップＳ３１）。その結果、閲覧対象が暗号化された文書データＤ１である場合（ステップＳ３１でＹＥＳ）、情報共有サーバー２は、その暗号化された文書データＤ１に関連付けられている暗号化パスワード３１を読み出し（ステップＳ３２）、その暗号化パスワード３１を復号するための復号鍵１４ｅを取得して（ステップＳ３３）、暗号化パスワード３１を復号する（ステップＳ３４）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号可能なパスワード３０に変換される。そして情報共有サーバー２は、復号したパスワード３０を用いて、暗号化された文書データＤ１を復号する（ステップＳ３５）。

【０１１４】

その後、情報共有サーバー２は、復号した文書データＤ２に基づいて閲覧用画像を生成すると共に（ステップＳ３６）、その閲覧用画像を含む閲覧画面Ｇ１を生成する（ステップＳ３７）。また情報共有サーバー２は、閲覧画面Ｇ１に対する保存禁止設定を付与すると共に（ステップＳ３８）、閲覧画面Ｇ１に対する印刷禁止設定を付与する（ステップＳ３９）。これにより、情報処理装置４のＷｅｂブラウザ４８の機能によって閲覧画面Ｇ１が保存されたり、印刷出力されることを防止することができる。

【０１１５】
これに対し、閲覧対象の文書データＤ１が暗号化されていない場合（ステップＳ３１でＮＯ）、情報共有サーバー２は、その文書データＤ１に基づいて閲覧用画像を生成すると共に（ステップＳ４１）、その閲覧用画像を含む閲覧画面Ｇ１を生成する（ステップＳ４２）。ただし、文書データＤ１が暗号化されていないときには、文書データＤ１に機密情報が含まれないと判断することができるため、情報処理装置４のＷｅｂブラウザ４８よる閲覧画面Ｇ１の保存機能や印刷機能を制限する必要はない。そのため、文書データＤ１が暗号化されていない場合、情報共有サーバー２は、閲覧画面Ｇ１に対する保存禁止設定や印刷禁止設定を付与しない。
【０１１６】
その後、情報共有サーバー２は、上記のようにして生成された閲覧画面Ｇ１を、閲覧要求Ｄ１１の送信元である情報処理装置４へ送信する（ステップＳ４０）。これにより、ログインユーザーは、自身の情報処理装置４において文書データＤ１の中身を閲覧することができるようになる。
【０１１７】
次に図１７は、文書データ提供処理（ステップＳ１２）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー２は、この処理を開始すると、まずダウンロード対象の文書データＤ１を特定し（ステップＳ５０）。その文書データＤ１が暗号化されているか否かを判断する（ステップＳ５１）。その結果、ダウンロード対象が暗号化された文書データＤ１である場合（ステップＳ５１でＹＥＳ）、情報共有サーバー２は、その暗号化された文書データＤ１に関連付けられている暗号化パスワード３１を読み出し（ステップＳ５２）、その暗号化パスワード３１を復号するための復号鍵１４ｅを取得して（ステップＳ５３）、暗号化パスワード３１を復号する（ステップＳ５４）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号可能なパスワード３０に変換される。そして情報共有サーバー２は、ダウンロード対象である暗号化された文書データＤ１を読み出し（ステップＳ５５）、その暗号化された文書データＤ１を、ダウンロード要求Ｄ１２の送信元である情報処理装置４へ送信すると共に（ステップＳ５６）、復号されたパスワード３０を情報処理装置４へ送信する（ステップＳ５７）。その後、情報共有サーバー２は、アップロードユーザーに対して文書データＤ１がダウンロードされたことを通知する通知処理を行う（ステップＳ５８）。
【０１１８】
これに対し、ダウンロード対象の文書データＤ１が暗号化されていない場合（ステップＳ５１でＮＯ）、情報共有サーバー２は、ダウンロード対象の文書データＤ１を読み出し（ステップＳ４１）、その文書データＤ１をそのまま情報処理装置４へ送信する（ステップＳ４２）。その後、情報共有サーバー２は、アップロードユーザーに対して文書データＤ１がダウンロードされたことを通知する通知処理を行う（ステップＳ５８）。
【０１１９】
次に図１８は、印刷制御処理（ステップＳ１４）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー２は、この処理を開始すると、まず印刷対象の文書データＤ１を特定し（ステップＳ７０）。その文書データＤ１が暗号化されているか否かを判断する（ステップＳ７１）。その結果、印刷対象が暗号化された文書データＤ１である場合（ステップＳ７１でＹＥＳ）、情報共有サーバー２は、その暗号化された文書データＤ１に関連付けられている暗号化パスワード３１を読み出し（ステップＳ７２）、その暗号化パスワード３１を復号するための復号鍵１４ｅを取得して（ステップＳ７３）、暗号化パスワード３１を復号する（ステップＳ７４）。これにより、暗号化パスワード３１は、暗号化された文書データＤ１を復号可能なパスワード３０に変換される。そして情報共有サーバー２は、印刷対象である暗号化された文書データＤ１を読み出す（ステップＳ７５）。
【０１２０】
続いて情報共有サーバー２は、印刷装置を特定し（ステップＳ７６）、その特定した印

刷装置に対応するプリンタドライバがインストールされているか否かを判断する（ステップＳ７７）。印刷装置に対応するプリンタドライバがインストールされている場合（ステップＳ７７でＹＥＳ）、情報共有サーバー２は、復号されたパスワード３０を用いて暗号化された文書データＤ１を復号する（ステップＳ７８）。そして情報共有サーバー２は、文書データＤ１を復号して生成された文書データＤ２に基づいて印刷装置で実行可能な印刷ジョブを生成し（ステップＳ７９）、その印刷ジョブを印刷装置へ送信する（ステップＳ８０）。

【０１２１】

これに対し、印刷装置に対応するプリンタドライバがインストールされていない場合（ステップＳ７７でＮＯ）、情報共有サーバー２は、暗号化された文書データＤ１を印刷装置へ送信すると共に（ステップＳ８１）、復号されたパスワード３０も印刷装置へ送信する（ステップＳ８２）。これにより、印刷装置において、暗号化された文書データＤ１を復号して印刷出力を行うことができるようになる。

【０１２２】

また印刷対象の文書データＤ１が暗号されていない場合（ステップＳ７１でＮＯ）、情報共有サーバー２は、印刷対象である文書データＤ１を読み出す（ステップＳ８４）。続いて情報共有サーバー２は、印刷装置を特定し（ステップＳ８５）、その特定した印刷装置に対応するプリンタドライバがインストールされているか否かを判断する（ステップＳ８６）。印刷装置に対応するプリンタドライバがインストールされている場合（ステップＳ８６でＹＥＳ）、情報共有サーバー２は、文書データＤ１に基づいて印刷装置で実行可能な印刷ジョブを生成し（ステップＳ８７）、その印刷ジョブを印刷装置へ送信する（ステップＳ８８）。また印刷装置に対応するプリンタドライバがインストールされていない場合（ステップＳ８６でＮＯ）、情報共有サーバー２は、文書データＤ１をそのまま印刷装置へ送信する（ステップＳ８９）。これにより、印刷装置において、文書データＤ１に基づく印刷出力を行うことができるようになる。

【０１２３】

その後、情報共有サーバー２は、アップロードユーザーに対して文書データＤ１が印刷出力されたことを通知する通知処理を行う（ステップＳ９０）。したがって、アップロードユーザーは、自身がアップロードした文書データＤ１がどのユーザーによって印刷出力されたかを把握することができる。

【０１２４】

以上のように、本実施形態の情報共有システム１は、情報共有サーバー２が情報処理装置４において暗号化された文書データＤ１を取得すると、その暗号化された文書データＤ１を復号するためのパスワード３０を取得することができ、暗号化された文書データＤ１とパスワード３０とを相互に関連付けて記憶する。そして暗号化された文書データＤ１の閲覧権限を有する他のユーザーから暗号化された文書データＤ１の閲覧要求Ｄ１１などを取得すると、情報共有サーバー２は、暗号化された文書データＤ１に関連付けて管理しているパスワード３０を用いて暗号化された文書データＤ１を復号し、他のユーザーが閲覧可能な態様で文書データＤ１に基づく閲覧情報を提供する。そのため、他のユーザーは、暗号化された文書データＤ１に設定されているパスワードを知らなくてもその文書データＤ１の中身を閲覧することが可能であり、特に機密文書を複数のユーザー間で共有して利用する際の利便性が向上する。

【０１２５】

また本実施形態の情報共有サーバー２は、閲覧権限を有するユーザーに対して暗号化された文書データＤ１の閲覧情報を提供する際、復号した文書データＤ２をそのまま提供するのではなく、復号した文書データＤ２に基づく閲覧用画像を生成し、その閲覧用画像を含む閲覧画面を提供するように構成される。そのため、復号された文書データＤ２に含まれるテキストなどのコンテンツデータがオリジナルデータのままでコピーされてしまうことを防止できるので、情報漏洩し難い態様で閲覧情報が提供されているのである。

【０１２６】

また本実施形態では、情報共有サーバー２が暗号化された文書データＤ１を復号するためのパスワード３０をそのまま保存して管理するのではなく、グループ毎に設定される暗号鍵１４ｄを用いてパスワード３０を暗号化することにより、暗号化パスワード３１に変換した状態で管理する構成である。そのため、仮に、暗号化された文書データＤ１と、それに関連付けられた暗号化パスワード３１とが外部に流出したとしても、それだけでは暗号化された文書データＤ１を復号することができないため、セキュリティの高い情報管理が実現されている。

【０１２７】

（第２実施形態）

次に本発明の第２実施形態について説明する。上述した第１実施形態では、暗号化された文書データＤ１を復号するパスワード３０を、情報共有サーバー２において暗号化する場合を例示した。これに対し、本実施形態では、情報処理装置４又は画像処理装置５が情報共有サーバー２に対して暗号化された文書データＤ１をアップロードする際に、情報処理装置４又は画像処理装置５において暗号化された文書データＤ１を復号するパスワード３０を暗号化する形態について説明する。

【０１２８】

図１９は、本実施形態においてユーザーＡが情報処理装置４ａを操作することにより文書データＤ１を情報共有サーバー２へアップロードする場合の動作シーケンスを示す図である。ユーザーＡは、情報処理装置４ａを操作することにより、情報共有サーバー２へのアップロード対象となる文書データＤ１を作成する（プロセスＰ３０）。その文書データＤ１が機密情報を含んでいる場合、ユーザーＡは、情報処理装置４ａに対してパスワード３０を入力し（プロセスＰ３１）、文書データＤ１をそのパスワード３０で暗号化する（プロセスＰ３２）。その後、ユーザーＡは、情報処理装置４ａを操作することによって情報共有サーバー２へログインし、情報共有サーバー２へ暗号化された文書データＤ１をアップロードする。

【０１２９】

情報共有サーバー２は、情報処理装置４ａから文書データＤ１を受信すると、その文書データＤ１が暗号化されたデータであるか否かを判断し、暗号化されたデータであれば、ユーザーＡの属するグループに設定されている暗号鍵１４ｄを読み出し、その暗号鍵１４ｄを情報処理装置４ａへ送信する。これにより、情報処理装置４ａは、情報共有サーバー２からユーザーＡが所属するグループに対して予め設定されている暗号鍵１４ｄを取得することができる。

【０１３０】

情報処理装置４ａは、情報共有サーバー２から暗号鍵１４ｄを取得すると、その暗号鍵１４ｄを用いて、ユーザーＡが文書データＤ１に設定したパスワード３０を暗号化する（プロセスＰ３３）。具体的には、図２に示したＷｅｂブラウザ４８のアップロード部５６が、ユーザーＡによって入力されるパスワード３０を、情報共有サーバー２から受信した暗号鍵１４ｄを用いて暗号化する。これにより、ユーザーＡが入力するパスワード３０は、情報処理装置４ａから情報共有サーバー２に送信されるときに情報処理装置４ａにおいて暗号化パスワード３１に変換される。そして情報処理装置４ａは、暗号化パスワード３１を情報共有サーバー２へ送信する。これにより、情報共有サーバー２は、情報処理装置４ａにおいて暗号化された暗号化パスワード３１を受信することができる。その後、情報共有サーバー２は、情報処理装置４ａから受信した暗号化された文書データＤ１と、暗号化パスワード３１とを相互に関連付けて保存する（プロセスＰ３４）。

【０１３１】

このように情報処理装置４ａにおいてパスワード３０を暗号化して暗号化パスワード３１を生成することにより、情報共有サーバー２においてパスワード３０を暗号化する必要がなくなるため、情報共有サーバー２の処理負担を軽減することができるようになる。

【０１３２】

また画像処理装置５が情報共有サーバー２に対して暗号化された文書データＤ１を直接

アップロードする場合も同様である。すなわち、図３に示したスキャンアプリケーション７１のアップロード部７９は、ユーザーＡによって入力されるパスワード３０を、情報共有サーバー２から受信した暗号鍵１４ｄを用いて暗号化するのである。これにより、ユーザーＡが入力するパスワード３０は、画像処理装置５から情報共有サーバー２に送信されるときに画像処理装置５において暗号化パスワード３１に変換される。そのため、情報共有サーバー２は、画像処理装置５から暗号化された文書データＤ１を受信した場合にその画像処理装置５に対して暗号鍵１４ｄを送信することにより、画像処理装置５において暗号化された暗号化パスワード３１を受信することができる。この場合においても、情報共有サーバー２においてパスワード３０を暗号化する必要がなくなるため、情報共有サーバー２の処理負担を軽減することが可能である。

【０１３３】

また本実施形態では、パスワード３０を暗号化する暗号鍵１４ｄは情報共有サーバー２から情報処理装置４ａなどの外部に流出することになるが、暗号化パスワード３１を復号するための復号鍵１４ｅを外部に流出させないため、セキュリティを低下させるものではない。

【０１３４】

尚、本実施形態におけるその他の点は、第１実施形態で説明したものと同様である。

【０１３５】

（第３実施形態）

次に本発明の第３実施形態について説明する。例えば情報共有サーバー２に暗号化された文書データＤ１をアップロードするユーザーＡが複数のグループに所属している場合、ユーザーＡは、それら複数のグループにおいて同じ文書データＤ１を共有したいことがある。そのような場合において、ユーザーＡは、一つのグループに対して暗号化された文書データＤ１をアップロードする操作を行った後、他のグループに対しても同様の操作を行わなければならないこととすると操作が煩雑になる。また情報共有サーバー２においては、同じ文書データＤ１であるにもかかわらず、グループが異なれば別の文書データとして管理しなければならないこととすると、重複した文書データＤ１が記憶部１１の記憶領域を圧迫してしまうという問題もある。そこで本実施形態では、暗号化された文書データＤ１をアップロードするユーザーＡが複数のグループで共有する文書データＤ１をアップロードする際の操作性を改善すると共に、情報共有サーバー２において重複した文書データＤ１が記憶部１１の記憶領域を圧迫してしまうことがない形態について説明する。

【０１３６】

本実施形態では、例えばユーザーＡが暗号化された文書データＤ１を情報共有サーバー２へアップロードするとき、情報共有サーバー２に対して文書データＤ１を共有するグループを指定する。このとき、ユーザーＡは、自身が所属する複数のグループを指定することもできる。そしてユーザーＡは、自身の情報処理装置４ａを操作することにより、パスワード３０で暗号化された文書データＤ１を情報共有サーバー２へアップロードする。このとき、情報処理装置４ａは、暗号化された文書データＤ１と共に、暗号化された文書データＤ１を復号するためのパスワード３０を情報共有サーバー２へ送信する。

【０１３７】

図４に示した情報共有サーバー２のアップロードデータ取得部２２は、ユーザーＡの情報処理装置４ａからアップロードデータを受信すると、そのアップロードデータから暗号化された文書データＤ１を抽出し、その文書データＤ１を文書データ管理部２３へ出力する。文書データ管理部２３は、その暗号化された文書データＤ１を記憶部１１に保存して管理する。

【０１３８】

またアップロードデータ取得部２２は、ユーザーＡによって暗号化された文書データＤ１を複数のグループで共有することが指定されている場合、ユーザーＡによって指定された複数のグループのそれぞれに登録されている暗号鍵１４ｄを取得する。そしてユーザーＡの情報処理装置４ａから受信したパスワード３０を、複数のグループのそれぞれに登録

されている暗号鍵１４ｄを用いて１つずつ暗号化していき、複数のグループのそれぞれに対応する複数の暗号化パスワード３１を生成する。そしてアップロードデータ取得部２２は、グループ毎に生成される複数の暗号化パスワード３１をパスワード管理部２４へ出力する。パスワード管理部２４は、それら複数の暗号化パスワード３１を記憶部１１へ保存し、それら複数の暗号化パスワード３１を文書データ管理部２３によって管理される１つの暗号化された文書データＤ１に関連付けて管理する。

【０１３９】

例えばユーザーＡがグループＸとグループＸとの２つのグループに属しており、それら２つのグループＸ，Ｚを文書データＤ１の共有グループとして指定した場合、アップロードデータ取得部２２は、グループＸに登録されている暗号鍵１４ｄを用いてパスワード３０を暗号化することにより第１の暗号化パスワード３１を生成すると共に、グループＺに登録されている暗号鍵１４ｄを用いてパスワード３０を暗号化することにより第２の暗号化パスワード３１を生成する。そして、これら２つの暗号化パスワード３１は、１つの暗号化された文書データＤ１と関連付けて管理される。そのため、グループＸに属する他のユーザーが文書データＤ１の閲覧要求Ｄ１１を送信してきた場合、閲覧情報提供部２５は、第１の暗号化パスワード３１を復号して暗号化された文書データＤ１を復号するためのパスワード３０を取得することができる。またグループＺに属する他のユーザーが文書データＤ１の閲覧要求Ｄ１１を送信してきた場合、閲覧情報提供部２５は、第２の暗号化パスワード３１を復号して暗号化された文書データＤ１を復号するためのパスワード３０を取得することができる。

【０１４０】

したがって、本実施形態では、ユーザーＡが文書データＤ１をアップロードする際に複数のグループで共有することを指定すれば良いため、同じアップロード操作を繰り返す必要がなく、操作性に優れている。また本実施形態では、１つの暗号化された文書データＤ１が、複数のグループで共有して利用されるため、重複した文書データＤ１が記憶部１１の記憶領域を圧迫してしまうという問題も解決することができるようになる。

【０１４１】

尚、上記においては、情報共有サーバー２のアップロードデータ取得部２２が、情報処理装置４ａから受信したパスワード３０をグループ毎に暗号鍵１４ｄで暗号化する場合を説明した。しかし、これに限られるものではなく、例えば第２実施形態のように、アップロードデータ取得部２２が、複数のグループのそれぞれに登録されている暗号鍵１４ｄを情報処理装置４ａへ送信し、情報処理装置４ａにおいて暗号化された複数の暗号化パスワード３１を取得するように構成しても良い。また本実施形態におけるその他の点は、第１実施形態又は第２実施形態で説明したものと同様である。

【０１４２】

（変形例）

以上、本発明に関する実施形態について説明したが、本発明は、上記実施形態において説明した内容のものに限られるものではなく、種々の変形例が適用可能である。

【０１４３】

例えば上記実施形態では、情報共有サーバー２がインターネットに接続されたクラウド３上に設けられる場合を例示したが、これに限られるものではない。すなわち、情報共有サーバー２は、ローカルネットワークに設けられるものであっても構わない。

【０１４４】

また上記実施形態では、パスワード３０を暗号化するための暗号鍵１４ｄと、復号するための復号鍵１４ｅとが互いに対となる別の鍵情報である場合を例示した。しかし、上述した第１実施形態においては、暗号鍵１４ｄと復号鍵１４ｅとが別の鍵情報である必要はなく、例えばパスワードなどのような同一の鍵情報であっても構わない。

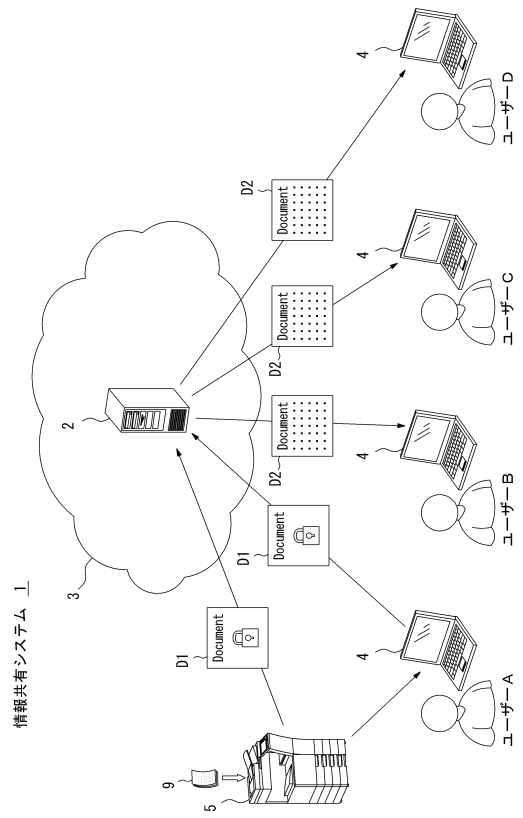
【符号の説明】

【０１４５】

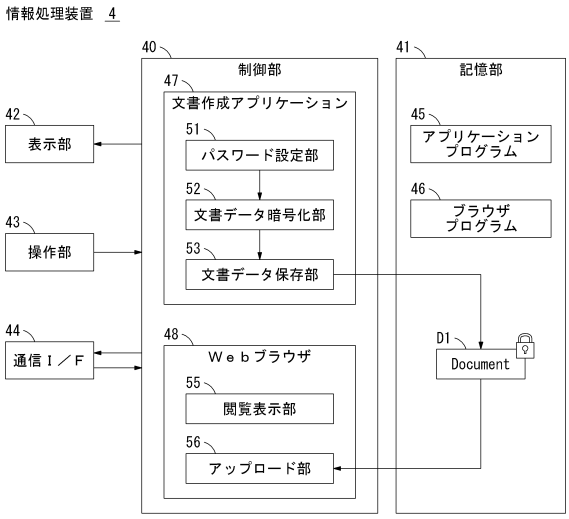
１　情報共有システム

２　情報共有サーバー
４　情報処理装置
５　画像処理装置
１１　記憶部（記憶手段）
２０　共有情報登録部（登録手段）
２２　アップロードデータ取得部（取得手段）
２５　閲覧情報提供部（閲覧情報提供手段）
２５ａ　復号部（復号手段）
２６　文書データ提供部（文書データ送信手段）
２６ｂ　通知部（通知手段）
２７　印刷制御部（印刷制御手段）
５２　文書データ暗号化部（暗号化手段）
５６　アップロード部（アップロード手段）
７８　暗号化部（暗号化手段）
７９　アップロード部（アップロード手段）

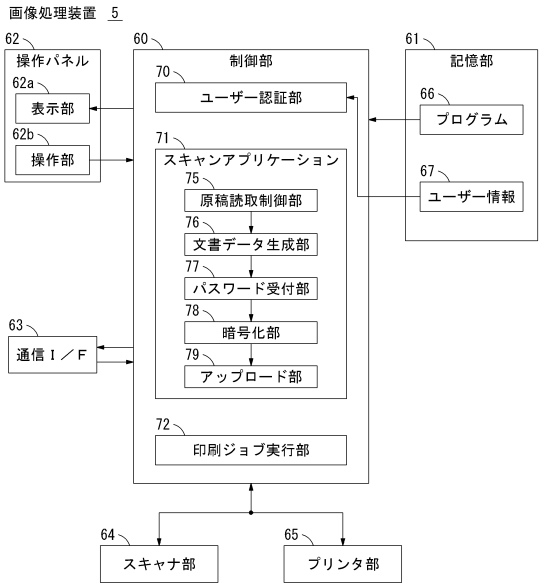
【図１】



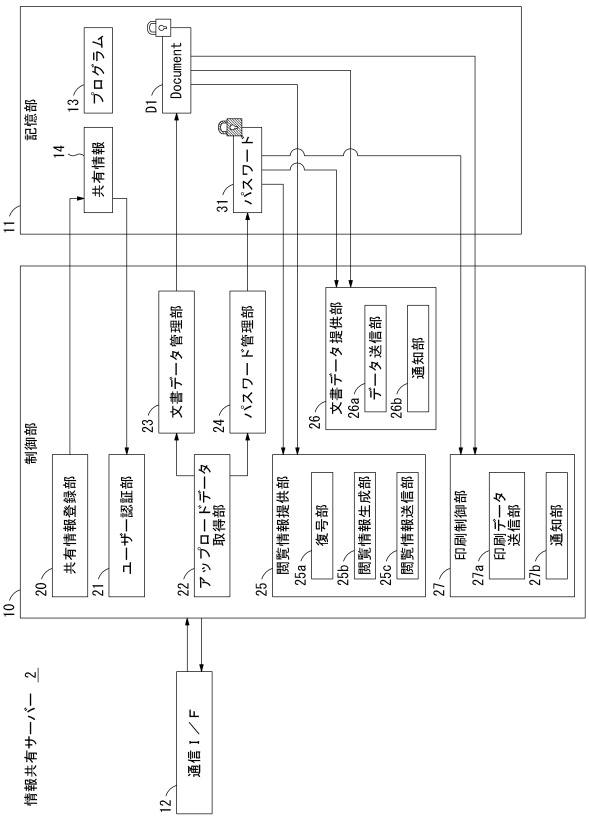
【図２】



【図３】



【図４】

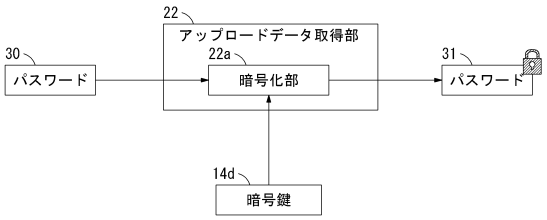


【図５】

共有情報 14

14a グループ	14b 共有ユーザー	14c 認証情報	14d 暗号鍵	14e 復号鍵	14f 識別情報
グループＸ	ユーザーＡ	*******	key01a	key01b	6219
	ユーザーＢ	*******			
	ユーザーＣ	*******			
	ユーザーＤ	*******			
グループＹ	ユーザーＥ	*******	key23a	key23b	4356
	ユーザーＦ	*******			
	ユーザーＧ	*******			
	ユーザーＨ	*******			

【図６】

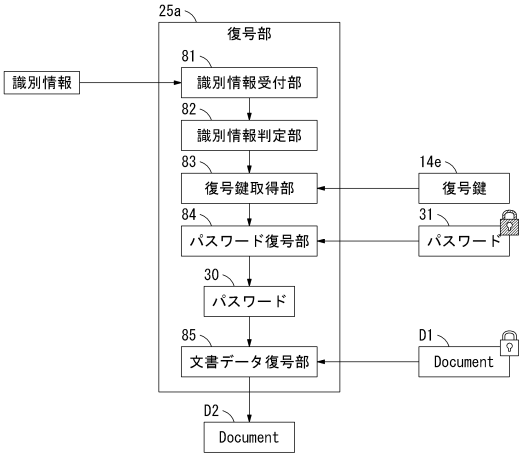


【図７】

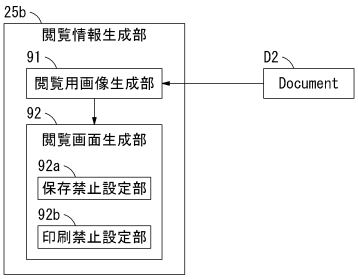
管理情報 35

35a グループ	35b 共有文書ファイル名	35c アップロードユーザー	35d パスワード情報
グループＸ	Document001.pdf	ユーザーＡ	*******
	Document002.pdf	ユーザーＡ	*******
	Document003.doc	ユーザーＢ	*******
グループＹ	Document111.pdf	ユーザーＦ	*******
	Document112.pdf	ユーザーＥ	*******
	Document113.doc	ユーザーＨ	*******

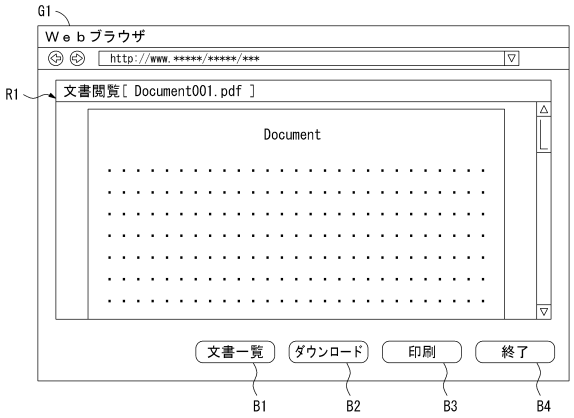
【図８】



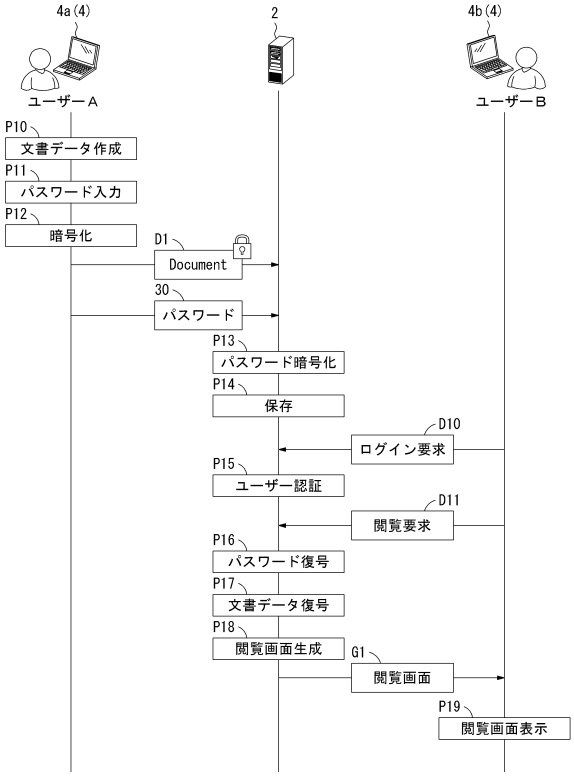
【図９】



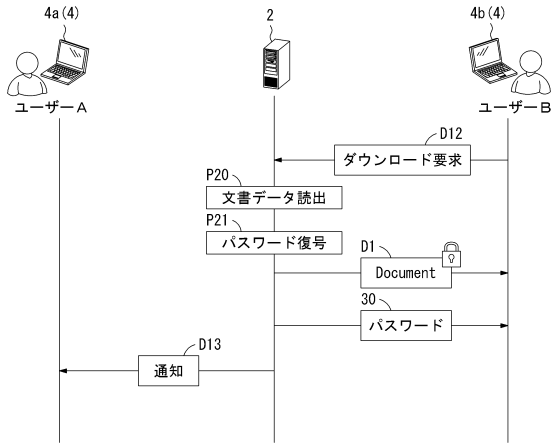
【図１０】



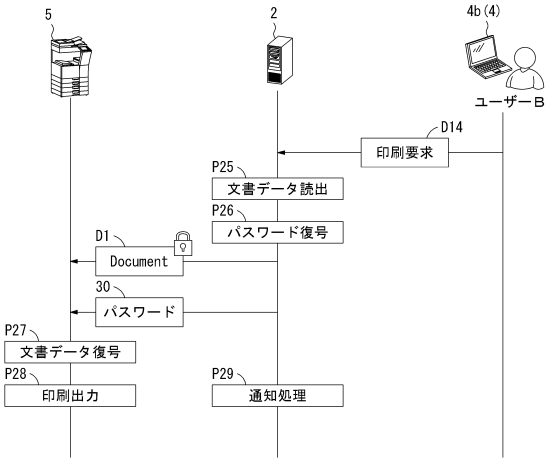
【図１１】



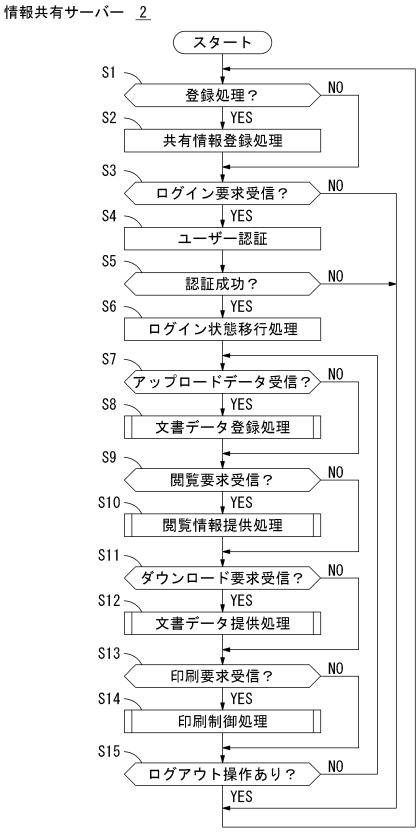
【図１２】



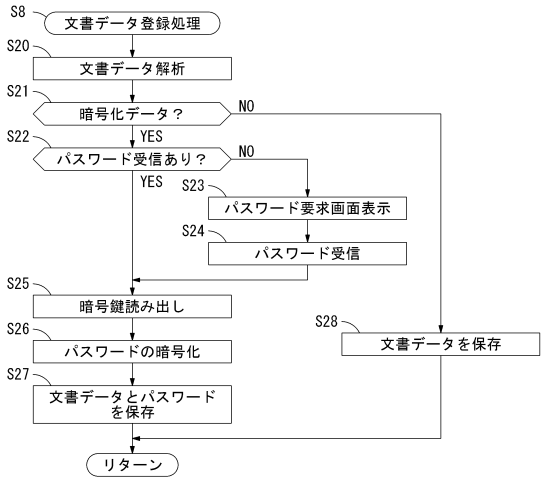
【図１３】



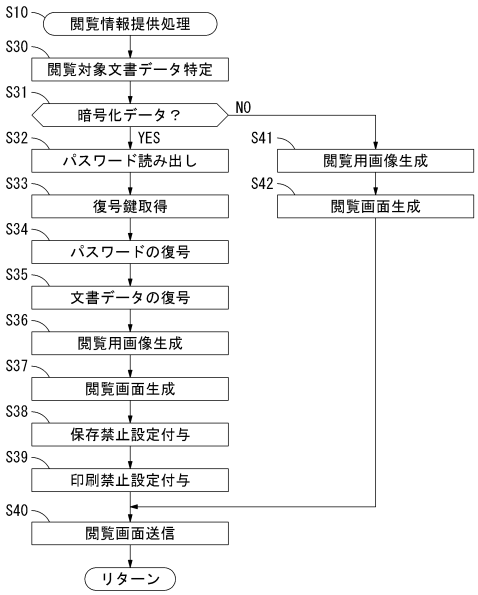
【図１４】



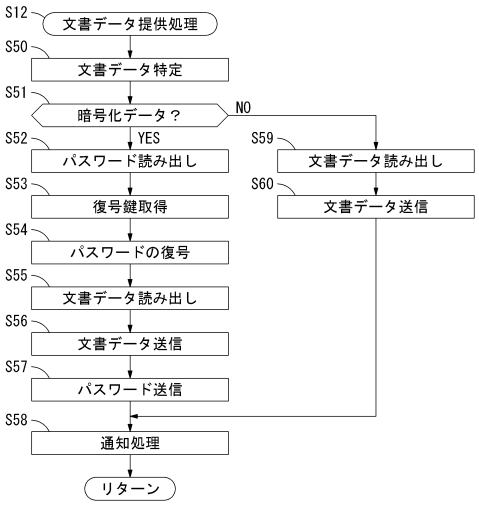
【図１５】



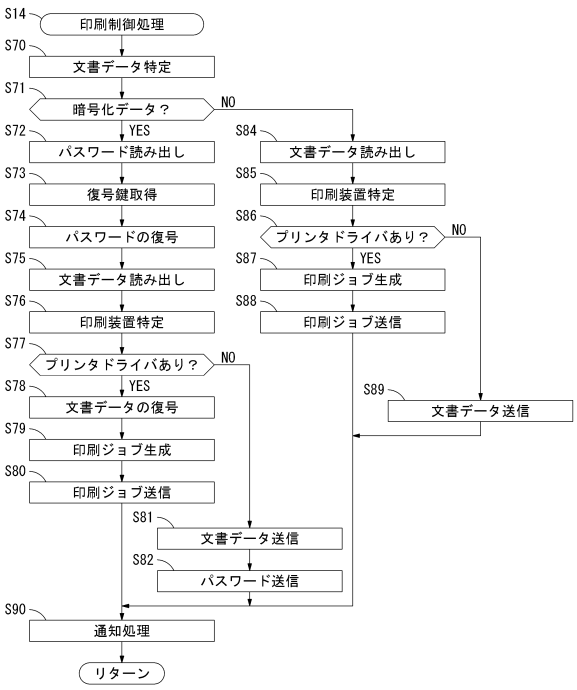
【図１６】



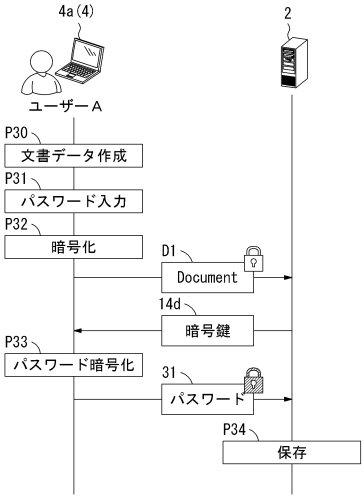
【図１７】



【図１８】


S14
印刷制御処理
S70
文書データ特定
S71
暗号化データ？
NO
YES
S72
パスワード読み出し
S73
復号鍵取得
S74
パスワードの復号
S75
文書データ読み出し
S76
印刷装置特定
S77
プリンタドライバあり？
NO
YES
S78
文書データの復号
S79
印刷ジョブ生成
S80
印刷ジョブ送信
S81
文書データ送信
S82
パスワード送信
S84
文書データ読み出し
S85
印刷装置特定
S86
プリンタドライバあり？
NO
YES
S87
印刷ジョブ生成
S88
印刷ジョブ送信
S89
文書データ送信
S90
通知処理
リターン

【図１９】


4a(4)
2
ユーザーA
P30
文書データ作成
P31
パスワード入力
P32
暗号化
D1
Document
14d
暗号鍵
P33
パスワード暗号化
31
パスワード
P34
保存

フロントページの続き

(56)参考文献 特開２０１０－０３３２６９（ＪＰ，Ａ）
特開２００５－２３４７１９（ＪＰ，Ａ）
特開２００３－０４４２９７（ＪＰ，Ａ）
特開平０９－２９４１２０（ＪＰ，Ａ）
特開２００３－１９６５４６（ＪＰ，Ａ）
特開２０１４－１７４７２１（ＪＰ，Ａ）
特開２００６－２１１３４９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／６２