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

特許第4838610号
(P4838610)

(45)発行日　平成23年12月14日(2011.12.14)　(24)登録日　平成23年10月7日(2011.10.7)

(51)Int.Cl.		F I		
G06F 17/30	(2006.01)	G06F	17/30	120B
G06F 12/00	(2006.01)	G06F	17/30	110F
G06F 21/24	(2006.01)	G06F	12/00	537A
		G06F	12/14	520A

請求項の数 11　(全 23 頁)

(21)出願番号　特願2006-82138(P2006-82138)
(22)出願日　平成18年3月24日(2006.3.24)
(65)公開番号　特開2007-257405(P2007-257405A)
(43)公開日　平成19年10月4日(2007.10.4)
審査請求日　平成20年10月16日(2008.10.16)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100145827
弁理士　水垣　親房
(72)発明者　斎藤　茂実
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　岩間　直純

最終頁に続く

(54)【発明の名称】文書管理装置、文書管理方法、プログラム

(57)【特許請求の範囲】
【請求項１】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を記憶可能な文書情報記憶手段と、
前記文書情報記憶手段に記憶された文書情報のインデクスを生成する処理を行うインデクス生成手段と、
ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成手段によるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信手段と、
前記送信手段が送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答して前記アクセス権管理装置から送信される前記文書情報に対する前記ユーザのアクセス権情報を受信する受信手段と、
前記受信手段が受信した前記アクセス権情報に基づいて前記文書情報に対するインデクス生成処理の実行の可否を判定する判定手段と、
前記判定手段の判定結果に基づいて、前記インデクス生成手段による前記文書情報のインデクス生成の処理を制御する制御手段と、を有することを特徴とする文書管理装置。
【請求項２】
前記判定手段は、前記アクセス権情報に基づいて、前記ユーザが前記文書情報に対する参照権限がある場合にはインデクス生成処理の実行を可と判定することを特徴とする、請

求項１に記載の文書管理装置。
【請求項３】
前記判定手段は、前記アクセス権情報に基づいて、前記ユーザが前記文書情報に対するインデクス生成のために必要な権限が無い場合にはインデクス生成処理の実行を不可と判定することを特徴とする、請求項１または２のいずれか１項に記載の文書管理装置。
【請求項４】
更に、前記インデクス生成手段が生成したインデクスを記憶するインデクス記憶手段と、
前記文書情報記憶手段に記憶されている１つ以上の文書情報の各々のインデクスが前記インデクス記憶手段に記憶されているか否かの状態を示すインデクス記憶状態を記憶するインデクス記憶状態記憶手段と、を有し、
前記送信手段は、前記インデクス記憶状態記憶手段を参照して、前記インデクス生成手段によるインデクス生成が行われていない文書情報を特定する情報を前記アクセス権管理装置へ送信し、
前記インデクス記憶状態記憶手段は、前記インデクス生成手段がインデクスを生成した文書情報に関するインデクス記憶状態をインデクス記憶済みとして記憶することを特徴とする請求項１乃至３のいずれか１項に記載の文書管理装置。
【請求項５】
前記文書情報記憶手段は更に、前記文書管理装置自身がアクセス管理する文書情報を記憶可能であり、前記送信手段は、前記インデクス記憶状態記憶手段を参照して、前記インデクス生成手段によるインデクス生成が行われていない文書情報が前記アクセス権管理装置によってアクセス権を管理されている場合、当該文書情報を特定する情報を前記アクセス権管理装置へ送信し、前記文書管理装置によってアクセス権を管理されている場合、当該文書情報を特定する情報を前記アクセス権管理装置へ送信しないことを特徴とする、請求項４に記載の文書管理装置。
【請求項６】
前記文書情報記憶手段は、前記アクセス権管理装置によってアクセス権を管理されている文書情報を暗号化した状態で記憶しており、
前記受信手段は更に、前記アクセス権管理装置から送信される前記文書情報に対する復号鍵を受信し、
前記インデクス生成手段は、前記文書情報記憶手段に記憶されている前記文書情報を前記復号鍵を用いて復号化し、当該復号化された文書情報に対してインデクス生成を行うことを特徴とする、請求項１乃至５のいずれか１項に記載の文書管理装置。
【請求項７】
更に、前記文書情報記憶手段が記憶する文書情報を処理する文書情報処理手段と、前記文書情報記憶手段が記憶する１つ以上の文書情報のうち、前記文書情報処理手段に処理させる文書の指定を受け付ける文書指定受付手段と、を有し、
前記インデクス生成手段は、前記文書指定受付手段が受け付けた前記文書情報処理手段による処理対象の文書情報以外の前記文書情報記憶手段に記憶されている文書情報に対するインデクス生成を行うことを特徴とする、請求項１乃至６のいずれか１項に記載の文書管理装置。
【請求項８】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を各々暗号化して記憶可能な文書情報記憶手段と、
文書情報のインデクスを生成する処理を行うインデクス生成手段と、
ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成手段によるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信手段と、
前記送信手段が送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答し

て前記アクセス権管理装置から送信される前記文書情報に対する復号鍵を受信した場合、受信した前記復号鍵に基づいて前記暗号化された文書情報を復号化する復号手段と、
前記送信手段による前記ユーザ特定情報と前記文書情報を特定する情報の送信に対して、前記アクセス権管理装置が前記文書情報に対する復号鍵を送信しなかった場合、前記インデクス生成手段による当該文書に対するインデクス生成処理を実行しないよう制御する制御手段と、を有することを特徴とする文書管理装置。
【請求項９】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を記憶可能な文書情報記憶手段を有する文書管理装置における文書管理方法であって、
前記文書情報記憶手段に記憶された文書情報のインデクスを生成する処理を行うインデクス生成ステップと、
ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成ステップによるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信ステップと、
前記送信ステップが送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答して前記アクセス権管理装置から送信される前記文書情報に対する前記ユーザのアクセス権情報を受信する受信ステップと、
前記受信ステップが受信した前記アクセス権情報に基づいて前記文書情報に対するインデクス生成処理の実行の可否を判定する判定ステップと、
前記判定ステップの判定結果に基づいて、前記インデクス生成ステップによる前記文書情報のインデクス生成の処理を制御する制御ステップと、
を有することを特徴とする文書管理方法。
【請求項１０】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を各々暗号化して記憶可能な文書情報記憶手段を有する文書管理装置における文書管理方法であって、
文書情報のインデクスを生成する処理を行うインデクス生成ステップと、
ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成ステップによるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信ステップと、
前記送信ステップが送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答して前記アクセス権管理装置から送信される前記文書情報に対する復号鍵を受信した場合、受信した前記復号鍵に基づいて前記暗号化された文書情報を復号化する復号ステップと、
前記送信ステップによる前記ユーザ特定情報と前記文書情報を特定する情報の送信に対して、前記アクセス権管理装置が前記文書情報に対する復号鍵を送信しなかった場合、前記インデクス生成ステップによる当該文書に対するインデクス生成処理を実行しないよう制御する制御ステップと、
を有することを特徴とする文書管理方法。
【請求項１１】
請求項９または１０のいずれか１項に記載の文書管理方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アクセス権限を管理するいずれかのサーバ装置と通信して、クライアント装置から要求される文書処理要求を制御する文書管理装置の文書管理処理に関するものである。

【背景技術】
【０００２】
文書情報を記憶する記憶手段を備え、ネットワークを介してクライアント装置からの文書検索や文書登録処理を行う文書管理システムが実用化されている。
【０００３】
文書管理システムにおいては、各文書に関するアクセス権をユーザごとに設定し、アクセス時にユーザのアクセス権を判定し、操作の許可または拒否を行う。ここで言うアクセス権の例としては、参照権、読み込み権、書き込み権、削除権などがある。
【０００４】
また、ユーザとアクセス権の組み合わせを１つ以上束ねたものをポリシーと呼び、文書に対してポリシーを付与することで、アクセス権設定の労力を削減する手法がある。
【０００５】
また、複数の文書サーバの文書について、アクセス権と共に一覧表示する手法がある（例えば、特許文献１を参照）。
【０００６】
この特許文献１は、複数の文書サーバにまたがった検索結果を、アクセス権と共に一覧表示するものである。また、検索結果に含まれる文書について、そのアクセス権を該文書を管理する文書サーバに問い合わせて確認する検索プログラムについても言及している。
【０００７】
文書管理システムによるアクセス権管理は、文書管理システム内部の文書にのみ有効であり、文書管理システム外部の文書については以下のような手法が取られている。
【０００８】
すなわち、文書を暗号化し、アクセス時に認証を行い、アクセス権を確認してから復号化する手法である。
【０００９】
このような認証・認可（アクセス権管理）は、文書管理システム外の専用のサーバに対して行うことが多い。この専用サーバにおけるアクセス権管理は前述したポリシーを以って行われることが多いため、以下ではこのような専用サーバをポリシー管理サーバと呼ぶ。
【００１０】
このようなポリシー管理サーバを用いた、アクセス権管理を実現したシステムをＲｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ（ＲＭＳ）と呼ぶ。
【００１１】
ＲＭＳを用いてアクセス権管理されている文書を、文書管理システムに格納することは可能である。
【特許文献１】特開２００５-０８５１１３号公報
【発明の開示】
【発明が解決しようとする課題】
【００１２】
しかし、従来の文書管理システム（特許文献１で述べられている複数のサーバから構成される文書管理システムを含む）においては、ＲＭＳを用いてアクセス権管理されている文書は暗号化されている。このため、全文検索用情報を取得することができず、全文検索の対象外となっていた。
【００１３】
また、全文検索または属性検索を問わず、検索結果に含まれる文書において、ＲＭＳのアクセス権を判定することなく、ユーザに提示していた。
【００１４】
そのため、ユーザは自分がアクセスできる文書を簡単には確認することができず、１つ１つ文書にアクセスして、ポリシー管理サーバにアクセスの可否を問い合わせることで、アクセス権を確認する必要があり、利便性が悪かった。

【００１５】
さらに、全文検索結果においては、本来はアクセス制限によって秘匿されるべき文書の内容が、検索に用いたキーワードのみとはいえユーザが知ることとなり、セキュリティの面でも問題があった。
【００１６】
本発明は、上記の課題を解決するためになされたもので、本発明の目的は、アクセス権が設定され、かつ、暗号化して格納された文書情報であっても、ユーザ権限に従い、復号化して全文検索を利便性よく行える仕組みを提供することである。
【課題を解決するための手段】
【００１７】
上記目的を達成する本発明の文書管理装置は以下に示す構成を備える。
【００１８】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を記憶可能な文書情報記憶手段と、前記文書情報記憶手段に記憶された文書情報のインデクスを生成する処理を行うインデクス生成手段と、ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成手段によるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信手段と、前記送信手段が送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答して前記アクセス権管理装置から送信される前記文書情報に対する前記ユーザのアクセス権情報を受信する受信手段と、前記受信手段が受信した前記アクセス権情報に基づいて前記文書情報に対するインデクス生成処理の実行の可否を判定する判定手段と、前記判定手段の判定結果に基づいて、前記インデクス生成手段による前記文書情報のインデクス生成の処理を制御する制御手段とを有することを特徴とする。
【００１９】
上記目的を達成する本発明の文書管理方法は以下に示す構成を備える。
【００２０】
アクセス権管理装置によってアクセス権を管理されている１つ以上の文書情報を記憶可能な文書情報記憶手段を有する文書管理装置における文書管理方法であって、前記文書情報記憶手段に記憶された文書情報のインデクスを生成する処理を行うインデクス生成ステップと、ユーザを特定するためのユーザ特定情報を受け付け、該ユーザ特定情報と、前記文書情報記憶手段に記憶されている文書情報のうち、前記インデクス生成ステップによるインデクス生成処理が行われていない文書情報を特定する情報とを前記アクセス権管理装置へ送信する送信ステップと、前記送信ステップが送信した前記ユーザ特定情報と前記文書情報を特定する情報とに応答して前記アクセス権管理装置から送信される前記文書情報に対する前記ユーザのアクセス権情報を受信する受信ステップと、前記受信ステップが受信した前記アクセス権情報に基づいて前記文書情報に対するインデクス生成処理の実行の可否を判定する判定ステップと、前記判定ステップの判定結果に基づいて、前記インデクス生成ステップによる前記文書情報のインデクス生成の処理を制御する制御ステップとを有することを特徴とする。
【発明の効果】
【００２１】
本発明によれば、暗号化されて格納された文書情報をユーザ権限を管理サーバで管理可能な文書管理装置において、アクセス権が管理されている文書については復号化して全文検索が可能となる。
【００２２】
また、検索結果として検索したユーザがアクセス可能な文書のみが表示されるようになり、セキュリティとユーザの利便性を向上させることができる。
【発明を実施するための最良の形態】
【００２３】

次に本発明を実施するための最良の形態について図面を参照して説明する。

【００２４】

＜システム構成の説明＞

〔第１実施形態〕

図１は、本発明の第１実施形態を示す文書管理装置を適用可能な文書管理システムの構成を説明するブロック図である。本例はクライアント１０００と、文書管理装置として機能する文書サーバ１１００と、ポリシー管理サーバ１２００から構成される文書管理システム例である。

【００２５】

ここで、ポリシー管理サーバ１２００は、文書管理システムとは別に、文書（文書情報とも言う）に対してのアクセス制御を行う「ポリシー」という制御データを管理、発行する処理を行うサーバ装置として機能する。ここで、ポリシーとは、ユーザとアクセス権の組み合わせを１つ以上束ねたものである。

【００２６】

本実施形態における文書管理システムは、パーソナルコンピュータのＯＳ上で動作するクライアント１０００と文書サーバ１１００から構成されるアプリケーションである。そして、文書管理システムは、不図示のスキャナなどの画像入力デバイスや、ＯＳ上のファイルから文書を取り込み、文書を複数のユーザで管理する処理を実行する。

【００２７】

＜文書入出力処理部＞

まず、クライアント１０００内に配置される文書入出力や操作を行う処理部について説明する。

【００２８】

なお、クライアント１０００は、ＣＰＵ、ＲＯＭ、ＲＡＭを含むコントロールユニットをベースとして、入出力デバイスとして、キーボード、ポインティングデバイス、表示装置を備え、さらにハードディスク等の外部記憶装置を備える。

【００２９】

ＣＰＵは、外部記憶装置に記憶されたＯＳをＲＡＭにロードして、デバイス処理と、ソフトウエアの起動、終了等の処理を行う。なお、文書サーバ１１００も同様のハードウエア資源を備える。

【００３０】

また、クライアント１０００，文書サーバ１１００は、ネットワークを介して通信するためのネットワークコントローラを備え、複数のプロトコルで通信可能に構成されている。

【００３１】

図１において、１００１はユーザインターフェース部である。ユーザはユーザインターフェース部１００１を介して文書サーバ１１００に対して文書の登録や、文書サーバ１１００からの文書の獲得、あるいは文書の検索といった操作を行う。

【００３２】

ユーザインターフェース部１００１から操作された情報はコマンド制御部１００２で解析され、適切な処理が行われる。また、必要であれば文書サーバ１１００との通信を行うためのコマンドはここで作成される。

【００３３】

デバイス制御部１００３は、不図示のスキャナ等のデバイスの制御を行う。ここでは、デバイス側から文書データを吸い上げたり、デバイス側から送信されるデータを受け取ったりする処理がなされる。

【００３４】

ファイルサーバ等のＯＳ上に保存された文書ファイルは、文書データをインポートする形態で、ファイル制御部１００４において入力処理させることができるよう構成されている。また、ファイル制御部１００４は、文書サーバ１１００上で管理するファイルをＯＳ

上にエクスポートする処理も行う。

【００３５】

１００５は外部モジュール通信部で、外部アプリケーションとの通信を行い、文書サーバ１１００内の文書を外部アプリケーションに渡したり、外部アプリケーションから文書を受け取とる等の処理を行う。外部アプリケーションは、クライアント１０００にインストールされている他のアプリケーションである。外部モジュール通信部１００５は、例えばＭＡＰＩ（Messaging Application Programming Interface)に対応した電子メールアプリケーションに文書サーバ１１００で管理している文書を渡したりする処理を行う。

【００３６】

＜クライアント１０００の内部処理部＞

次に、クライアント１０００内に配置される各種処理部について説明する。

【００３７】

１００６は文書管理制御部で、クライアント１０００で文書管理処理を司る機能処理部である。ここでは、入出力処理部より渡されたファイルやコマンドに応じて処理を行う。

【００３８】

１００７は内部データ保存部で、テンポラリデータを保存する。内部データ保存部１００７は、画像処理を行う過程で作成されるデータや、サーバとの通信の過程で作成されるデータ等を一時的に保存する。内部データ保存部１００７は、実体的には、ハードディスクや、ＲＡＭ等のメモリ装置で構成され、そのメモリ装置へのアクセスは、ＯＳを介してＣＰＵが制御する構成である。

【００３９】

１００８は通信制御部で、所定のプロトコルで文書サーバ１１００やポリシー管理サーバ１２００と通信するための制御を行う。

【００４０】

本実施形態に示す通信制御部１００８は、文書サーバ１１００やポリシー管理サーバ１２００の処理に特化した制御のみを行っており、プロトコルであるＴＣＰ／ＩＰ等の通信そのものの制御はＯＳに用意されたものを使用している。

【００４１】

＜文書サーバ１１００の内部処理部＞

次に、文書サーバ１１００内に配置される各種処理部について説明する。

【００４２】

１１０１は通信制御部で、クライアント１０００の通信制御部１００８と通信のための制御を行う。

【００４３】

ただし、文書サーバ１１００のサーバの通信制御部１１０１は多数のクライアントの通信制御部１００８と同時に通信を行うことが可能に構成されている。本実施形態では、図１において、１台のクライアント１０００が文書サーバ１１００と通信可能な例を示すが、図示しない複数のクライアントと通信可能にシステムを構築できる。

【００４４】

１１０２は文書管理制御部であり、クライアント１０００からの指示に応じた文書サーバ１１００側での処理を総括的に制御している。

【００４５】

文書管理制御部１１０２は、ポリシー管理サーバ１２００に対する認証の結果、クライアント１０００から取得される文書情報を暗号化して後述するボリュームデータベース１１０７に登録し管理する

【００４６】

また、アクセス権限が後述する処理で判定された場合に、文書管理制御部１１０２は、ボリュームデータベース１１０７に暗号化されて登録された文書情報を保持される認証情報に基づいて復号処理する。あるいは、文書管理制御部１１０２は、ポリシー管理サーバ１２００から取得される認証情報に基づいて、暗号化された文書を復号処理する。

【００４７】
１１０３は内部データ保存部で、テンポラリデータを保存する。テンポラリデータ１１０３は、クライアント１０００との通信の過程で作成されるデータなどを一時的に保存する。
【００４８】
１１０４は検索制御部で、クライアント１０００から依頼された文書の検索のための処理を行ったり、登録された文書の検索情報登録処理を行ったりする。
【００４９】
１１０５はポリシーデータ処理部である。ポリシーデータ処理部１１０５は、文書に付与されているポリシーデータの有無を判定したり、ポリシーデータをポリシー管理サーバ１２００に対して送信してポリシーの内容を確認するための処理を行う。
【００５０】
クライアント１０００に要求して取得されるユーザ認証情報を取得して、当該ユーザの認証を行い、認証されたユーザの文書情報に対する権限情報（権限リストを含む）をポリシー管理サーバ１２００から取得する。
【００５１】
また、ポリシーデータ処理部で１１０５は、ポリシー管理サーバ１２００から受け取った利用可能な権限リストなどを処理し、文書管理制御部１１０２へポリシーの確認結果などを返す。なお、権限リスト等は、テンポラリデータ１１０３に保持されて、文書管理制御部１１０２により保持されているユーザ認証情報等が認証結果や、権限判定処理に基づいて削除する。
【００５２】
ポリシーデータ処理部１１０５は、ポリシー管理サーバ１２００の仕様に依存して構成される。
【００５３】
＜データベース処理部＞
次に、文書サーバ１１００内に配置されるデータベース処理部について説明する。
【００５４】
１１０６はデータベース制御部で、データベースに保存するデータを作成し、ボリュームデータベース１１０７、属性データベース１１０８、全文検索データベース１１０９に対応する文書を保存する処理を行う。
【００５５】
また、データベース制御部１１０６は、クライアント１０００からの要求に応じてそれぞれの上記各データベースからデータを取り出し、クライアント１０００に渡す文書を作成する処理を行う。
【００５６】
１１０７はボリュームデータベースで、文書の実体が保存されるデータベースである。ボリュームデータベース１１０７は概念的なものであって、実体がＯＳのファイルシステムであっても問題はない。
【００５７】
１１０８は属性データベースで、文書の名前や作成日付、コメントなどの属性に関する情報が保存されるデータベースである。また、属性データベース１１０８には、文書毎のアクセス権管理者、アクセス権ＩＤ、ポリシー管理サーバ情報、ポリシーＩＤ、およびＲＭＳのアクセス権情報のキャッシュも保存している。
【００５８】
１１０９は全文検索データベースで、ボリュームデータベース１１０７に登録された文書からテキストデータを抽出し、インデクス情報にしたデータが登録される。
【００５９】
クライアント１０００から全文検索の要求があると、文書管理制御部１１０２は、クライアント１０００から受け取る検索条件に基づいて、全文検索データベース１１０９内を

検索する。ここで、検索条件とは、キーワード、日時、タイトル、イメージ名等の各種のデータが検索条件として指定可能である。

【００６０】

＜ポリシー管理サーバ１２００の処理部＞

次に、ポリシー管理サーバ１２００に配置されるポリシー管理処理部について説明する。

【００６１】

１２０１は通信制御部で、サーバシステムの通信制御部１１０１と通信のための制御を行う。ポリシー管理サーバ１２００の通信制御部１２０１は、ネットワークに接続される多数の情報処理装置と同時に通信を行うことが可能に構成されている。

【００６２】

１２０２はポリシー管理制御部であり、ポリシー管理サーバ１２００の総括的な処理を行う。ポリシー管理制御部１２０２は、通信制御部１２０１より渡されたコマンドに応じて処理を行う。

【００６３】

１２０３はポリシー発行部で、ポリシーの作成を行う。ここで、ポリシーとは、ユーザとアクセス権の組み合わせを１つ以上束ねたものである。

【００６４】

１２０４はデータベース制御部で、ポリシー管理用データベース１２０５に保存するデータを作成し、ポリシー管理用データベース１２０５に保存する処理を行う。

【００６５】

また、データベース制御部１２０４は、外部からの要求に応じてポリシー管理用データベース１２０５から対応するデータを取り出し、クライアント１０００または文書サーバ１１００に渡す処理を行う。

【００６６】

１２０５はポリシー管理用データベースで、ポリシー、ポリシー管理サーバで管理するユーザ情報が保存されるデータベースである。

【００６７】

このように構成された文書管理システムにおいて文書管理装置（文書サーバ１１００）は、文書データベース（ボリュームデータベース１１０７）を備える。そして、ボリュームデータベース１１０７に対して暗号化されて登録された文書情報に対するユーザのアクセス権を管理するサーバ装置のいずれかと通信して、クライアント１０００から要求される文書処理要求を制御する。サーバ装置とは、ポリシー管理サーバ１２００や、図示しないアクセス権限取得先が登録されている他のポリシー管理サーバを含む。

【００６８】

文書サーバ１１００は、文書情報を全文検索するためのインデクスを作成するために、ユーザ認証情報、アクセス権限、等を特定する属性情報を記憶可能な属性データベース１１０８を備える。なお、属性情報は、アクセス権限管理先を特定する特定先情報（図３に示すようなポリシー管理サーバ情報３６）を含むものとする。

【００６９】

また、文書サーバ１１００は、ポリシー管理サーバ１２００からアクセス権限情報を取得する取得機能を備える。

【００７０】

具体的には、後述するフローチャートに手順を示すように、クライアント１０００から全文検索の要求があると、以下の処理を行う。つまり、クライアント１０００から取得されるユーザ認証情報に基づいて属性データベースから特定されるポリシー管理サーバ情報３６に従ってポリシー管理サーバ１２００からアクセス権限情報を取得する取得機能を備える。

【００７１】

そして、ポリシー管理サーバ１２００から取得される、文書に対するユーザ毎のアクセ

ス権限情報を属性データベース１１０８に設定する設定機能を備える。

【００７２】

さらに、文書サーバ１１００は、属性データベース１１０８に記憶されるユーザ認証情報に基づいて、暗号化されて登録されている文書のうちアクセスが許可されている文書復号化する文書復号化機能を備える。なお、文書の暗号化アルゴリズムとしては、種々のアルゴリズムに対応しているものとする。

【００７３】

また、文書サーバ１１００は、復号化された文書情報から全文検索用情報（インデクス）を取得する取得機能と、取得した全文検索情報を全文検索データベース１１０９へ登録する登録機能を備える。

【００７４】

また、文書サーバ１１００は、ポリシー管理サーバ１２００から取得したポリシーに基づいて、全文検索要求を行うユーザ毎のアクセス権限の有効性を判定する判定機能を備える。そして、その判定結果に基づいて、属性データベース１１０８に記憶されているアクセス権限のない文書情報に対するアクセス要求を制限する制限機能を備える。これにより、暗号化されている文書に対して、ポリシーに基づくアクセス権管理をしながら、全文検索をアクセス権限に従って実行させることができる。

【００７５】

また、文書サーバ１１００は、は、判定機能による判定結果に基づいて、属性データベース１１０８に記憶されている、検索要求元のユーザのアクセス権限のある文書情報の一覧を表示部に表示させるための検索結果表示情報をクライアント１０００に通知する通知機能を備える。

【００７６】

ここで、アクセス権限は、複数の階層構造で、例えば削除権、書き込み権、読み込み権、参照権のように各権限を設定可能に構成されている。

【００７７】

また、属性データベース１１０８に記憶されている属性情報は、全文検索データベース１１０９に対する全文検索情報の登録状態を管理する状態情報（図３に示す全文検索情報登録状態３８参照）を設定可能に構成されている。

【００７８】

さらに、属性情報は、全文検索データベース１１０９に対する全文検索情報の登録と、登録された全文検索情報の取得とを非同期で行うように構成されている。

【００７９】

図２は、図１に示した属性データベース１１０８に登録されている文書に関する情報のデータ構造を説明する概念図である。

【００８０】

図２において、２００１はルートで、属性データベース１１０８で管理されるデータを特定する指標として機能する。この属性データベース１１０８内に登録される全ての登録されるデータは、ルート２００１の子データである。

【００８１】

２００２はフォルダデータであり、ユーザがデータを文書サーバ１１００に格納するためのフォルダのデータである。フォルダ２００２はフォルダＩＤとフォルダ属性情報、親フォルダＩＤから成る。

【００８２】

なお、本実施形態において、フォルダは複数存在することができるので、最上位に存在するフォルダはその数だけ、フォルダ２００３のようにルート２００１の直下に接続される子データとして登録される。したがって、フォルダ２００２、２００３の親フォルダはルート２００１になる。

【００８３】

２００４は文書データで、格納されるフォルダ２００２の子データとして存在する。

【００８４】
文書データ２００４は文書ＩＤと文書属性情報、検索インデクスＩＤ、ボリュームデータＩＤ、親フォルダＩＤからなり、文書属性情報として文書名や更新日時、コメントデータなどのデータを保存している。
【００８５】
文書ＩＤは、文書に付けられたＩＤであり、文書管理システム全体でユニークな値である。検索インデクスＩＤは全文検索データベースが文書を区別するために用いるＩＤで、データベース制御部１１０６にキーワードを指定して検索させると該当する文書の検索インデクスＩＤが返される。
【００８６】
ボリュームデータＩＤはボリュームデータベースに登録されたＩＤで、ＩＤを利用して文書に関連した情報を各データベースから引き出すことが可能である。文書データもフォルダの下に複数存在することができるので、その数分だけ文書データ２００５のように登録される。親フォルダＩＤは当該文書が格納されるフォルダのＩＤを示す情報である。例えば、文書データ２００４の親フォルダＩＤはフォルダ２００２のフォルダＩＤになる。
【００８７】
図３は、図１に示した属性データベース１１０８に保持する文書属性情報の一部を説明する図である。属性データベース１１０８には、文書毎のアクセス権管理者、アクセス権ＩＤ、ポリシー管理サーバ情報、ポリシーＩＤ、およびＲＭＳのアクセス権情報のキャッシュも保存される。したがって、以下のデータ構造で各種の情報を管理する。
【００８８】
図３において、３１は文書ＩＤである。３２は親フォルダで、上位のフォルダのＩＤが設定される。文書名３３は、文書の文書名である。アクセス権管理者３４は、文書に対するアクセス権を制御する主体となる情報であり、ここでは「文書管理システム」または「ポリシー管理サーバ」のいずれかの値を取る。
【００８９】
アクセス権ＩＤ３５は、文書に対するアクセス権が、文書管理システムにて制御される場合における、文書管理システム内で管理設定される、アクセス権を特定する情報である。
【００９０】
ポリシー管理サーバ情報３６は、文書に対するアクセス権が外部のポリシー管理サーバ１２００を用いて制御される場合に、該ポリシー管理サーバ１２００のネットワークに対するＩＰアドレスである。
【００９１】
ポリシーＩＤ３７は、該文書に対するアクセス権がポリシー管理サーバ情報３６で特定されるポリシー管理サーバを用いて制御される場合の、当該ポリシー管理サーバおけるポリシーを特定するユニークなＩＤである。
【００９２】
全文検索情報登録状態３８は、文書管理制御部１１０２により復号化された文書情報に対して生成された全文検索情報が全文検索データベース１１０９に登録されているか否かを示す情報、例えば「登録済み」あるいは「未登録」のいずれかが設定される。ここで、全文検索情報とは、検索のためのインデクス情報であり、文書管理制御部１１０２によりボリュームデータベース１１０７に暗号化されて登録される。全文検索情報は、ユーザ認証と、認証されたユーザのアクセス権限に従い復号化された後、該復号化された文書情報に対して生成される。
【００９３】
図４は、図１に示した属性データベース１１０８に保持されるアクセス権情報の一例を示す図である。
【００９４】
図４において、４１はアクセス権ＩＤである。４２はユーザＩＤである。文書に対する

アクセス権４３は、文書管理システムにて制御される場合、文書管理システムはこの情報を参照する。

【００９５】

本実施形態において、アクセス権４３は、削除権、書き込み権、読み込み権、参照権の４種類とし、この順にアクセス権が強いものとする。すなわち、削除権は、書き込み権、読み込み権、参照権を包含するものとする。

【００９６】

なお、本実施形態では、アクセス権ＩＤ４１とユーザＩＤ４２の組み合わせがアクセス権情報に存在しない場合、該ユーザは該アクセス権ＩＤの付与された文書について、一切のアクセス権を保持していないものとして管理される。

【００９７】

図５は、図１に示した属性データベース１１０８に保持されるポリシー管理サーバ１２００のポリシーのキャッシュの一例を示す図である。

【００９８】

図５において、本キャッシュは、ユーザＩＤ５１、ポリシー管理サーバ情報５２、ポリシーＩＤ５３、アクセス権５４から構成される。

【００９９】

本キャッシュは、ポリシー管理サーバ１２００（や、他の不図示のポリシー管理サーバ）が保持するポリシーの部分的なコピーであり、ポリシーデータ処理部１１０５がポリシー管理サーバからポリシーを取得する毎にデータベース制御部１１０６が追加して管理する。また、ポリシー管理サーバ１２００から、ポリシーの変更が通知された場合、ポリシーデータ処理部１１０５が属性データベース１１０８上で保持される該当するポリシーのキャッシュを削除する。ポリシー管理サーバ１２００から変更されたポリシーの内容も通知された場合は、変更後のポリシーをキャッシュするようにしても良い。

【０１００】

図６は、図１に示したテンポラリデータ１１０３に保存されるポリシー管理サーバ１２００への認証情報の一例を示す図である。なお、本認証情報は、全文検索情報取得処理時および検索処理時に参照される。

【０１０１】

図６において、認証情報は、クレデンシャル６４として持つ場合と、ユーザ名６５とパスワード６６の組で持つ場合がある。

【０１０２】

図６に示す例では、文書管理制御部１１０２がパスワード６６をクレデンシャル６４とは別の項目として管理しているが、パスワード６６もクレデンシャル６４の一つとして管理するようにしても良い。

【０１０３】

認証情報６３をクレデンシャル６４として持つ場合、認証情報６３の有効期限６７は、ポリシー管理サーバ１２００のポリシー管理制御部１２０２で制御される。

【０１０４】

一方、認証情報６３をユーザ名６５とパスワード６６の組で持つ場合、認証情報６３の有効期限６７は文書管理システムの文書管理制御部１１０２で制御される。

【０１０５】

本実施形態において、クレデンシャル６４とは、ユーザがポリシー管理サーバ１２００に対して認証を行う場合に用いられる何らかの情報である。

【０１０６】

クレデンシャルとして、例えば、当該ユーザを証明するための情報や、ポリシー管理サーバ１２００と認証のためのセッションを行う場合に用いられる暗号鍵や署名情報等が含まれる。

【０１０７】

なお、テンポラリデータ１１０３に保存される本情報には、ポリシー管理サーバ１２０

０への認証が成功した時点で文書管理制御部１１０２により情報が追加される。また、認証が無効になった時点で該当する情報を削除する。

【０１０８】

図７は、図１に示した属性データベース１１０８に保存されるユーザ毎の全文検索情報取得範囲を示す図である。本情報は、ユーザが意図しない文書が検索結果に含まれてしまうことを防止するために使われるもので、文書管理制御部１１０２により全文検索情報登録処理において参照される。

【０１０９】

図７において、全文検索情報取得許可範囲７２は、文書管理システムのユーザ毎に設定することができ、ユーザＩＤ７１と結びつけて保存管理される。

【０１１０】

全文検索情報取得許可範囲７２は、「全て許可」，「一部許可」，「全て拒否」のいずれかである。

【０１１１】

ここで、「全て許可」は、該ユーザが図４に示したアクセス権４３を持つ文書全てについて、全文検索情報の取得、登録を許可する場合に設定される。

【０１１２】

また、「一部許可」の場合、ユーザは許可する範囲を文書またはフォルダ単位で指定し、文書管理システムは、指定された範囲を文書ＩＤまたはフォルダＩＤの集合として許可範囲７３に記録する場合に設定される。

【０１１３】

さらに、「全て拒否」の場合、ユーザがアクセス権を持つ文書全てについて、全文検索情報の取得・登録を許可しない場合に設定される。

【０１１４】

図８は、本実施形態を示す文書管理装置における第１のデータ処理手順の一例を示すフローチャートである。本処理は、文書管理システムを介したポリシー管理サーバ１２００への認証処理手順に対応する。

【０１１５】

また、本処理は、文書管理システム上に格納されたＲＭＳを用いてアクセス権が管理されている文書を開く場合や、アクセス権を確認する場合に、その処理前に呼び出される。本処理の後、文書を開く、アクセス権情報を取得するなどの処理が実行される。なお、（８０１）～（８０７）は各ステップを示す。また、各ステップは、図８は、クライアント１０００、文書サーバ１１００が行う処理について説明し、文書管理システム以外で行う処理については後述する。

【０１１６】

まず、ステップ（８０１）で、文書管理制御部１１０２は、操作ユーザのポリシー管理サーバ１２００の認証情報が、テンポラリデータ１１０３上のポリシー管理サーバ１２００への一時的な認証情報に記憶されているかを判定する。ここで、文書管理制御部１１０２がテンポラリデータ１１０３上に認証情報が記憶されていると判定した場合、ステップ（８０４）に進む。

【０１１７】

一方、ステップ（８０１）で、文書管理制御部１１０２がテンポラリデータ１１０３上に認証情報が記憶されていないと判断した場合、ステップ（８０２）に進む。

【０１１８】

なお、本ステップ（８０１）および後述するステップ（８０６）、ステップ（８０７）は、ユーザへの認証情報要求の回数を削減し、利便性の向上を図るためのステップである。

【０１１９】

ステップ（８０２）で、文書管理制御部１１０２は、通信制御部１１０１を通じて、ポリシー管理サーバ１２００への認証情報をユーザに対して要求する。この要求は、最終的

にクライアント１０００のユーザインターフェース部１００１に伝わり、ユーザに対する問い合わせとなる。

【０１２０】

これに対して、ユーザは、クライアント１０００上の入力デバイスを操作して、表示されるＵＩ画面に対してポリシー管理サーバ１２００への認証情報を入力する。

【０１２１】

そして、ステップ（８０３）で、クライアント１０００のユーザインターフェース部１００１は、ユーザからポリシー管理サーバ１２００への認証情報を取得し、通信制御部１００８、１１０１を経て認証情報をポリシーデータ処理部１１０５に伝える。

【０１２２】

次に、ステップ（８０４）で、ポリシーデータ処理部１１０５は、該文書の操作ユーザに対するアクセス権をポリシー管理サーバ１２００に問い合わせる。これは、通信制御部１１０１を介してポリシー管理サーバ１２００に問い合わせを行うことで実行される。

【０１２３】

この時、ステップ（８０３）で、クライアント１０００から入力された認証情報、またはステップ（８０１）でテンポラリデータ１１０３から取得した認証情報を添えて問い合わせる。

【０１２４】

これに対して、ポリシー管理サーバ１２００は、上記認証情報を受信し、ポリシー管理用データベース１２０５を参照して認証処理を行い、その結果を文書サーバ１１００に返信する。

【０１２５】

そして、ステップ（８０５）において、文書管理制御部１１０２は、ステップ（８０４）の問い合わせに対して、認証が成功したかどうか判定する。そして、文書管理制御部１１０２が認証が成功したと判定した場合、ステップ（８０７）へ進み、認証が失敗したと判定した場合、ステップ（８０６）へ進む。

【０１２６】

そして、ステップ（８０６）において、操作ユーザのポリシー管理サーバ１２００の認証情報が、テンポラリデータ１１０３に登録されている場合、文書管理制御部１１０２は該認証情報を削除して、ステップ（８０２）へ戻る。

【０１２７】

これにより、既存の認証情報であって、ステップ（８０５）で誤っていると判定された認証情報による認証処理が回避されるので、処理効率が向上する。

【０１２８】

一方、ステップ（８０５）で、文書管理制御部１１０２は認証が成功したと判定した場合、ステップ（８０７）で、文書管理制御部１１０２は、ポリシー管理サーバ１２００の認証情報をテンポラリデータ１１０３に新たに記録して、本処理を終了する。

【０１２９】

なお、認証情報がすでに記録されている場合、この処理は省略しても良い。

【０１３０】

図９は、本実施形態を示す文書管理装置における第２のデータ処理手順の一例を示すフローチャートである。本処理は、全文検索情報登録処理の基本処理例である。また、本処理は、図８の認証処理の実行後に行われるが、図８の認証処理の後ユーザが本来実行を意図している文書処理（例えば、ユーザが指定するの文書情報を表示したり、新規に文書情報を登録したりする処理など）とは別に、当該ユーザが認証状態である期間に実行される。ポリシー管理サーバ１２００でアクセス権を管理されている文書情報は暗号化されているので、ユーザが文書サーバ１１００に認証している期間であれば、当該ユーザのクレデンシャル情報を用いてポリシー管理サーバからこのような暗号化された文書情報の復号鍵を取得することが出来る。（当然、当該文書に対するアクセスが可能なポリシーが適用されていることが前提である。）これにより、ユーザがインデクスの生成を指示することな

く、ポリシー管理サーバ１２００でアクセス権を管理されている文書情報のインデクス生成を文書サーバ１１００が自動的に行うことが出来る。

【０１３１】

まず、ステップ（９０１）において、文書管理システムがテンポラリデータ１１０３に一時的に保持しているユーザのポリシー管理サーバ１２００への認証情報を取得する。そして、各ポリシー管理サーバ１２００への認証情報ごとに、以下のステップ（９０２）からステップ（９１１）の処理を繰り返す。

【０１３２】

まず、ステップ（９０２）で、文書サーバ１１００の文書管理制御部１１０２が図１に示した属性データベース１１０８に保存されるユーザのユーザＩＤ７１から全文検索情報取得許可範囲７２を取得する。そして、文書管理制御部１１０２は、全文検索情報取得許可範囲７２が「全て許可」もしくは「一部許可」であるかを判断する。

【０１３３】

文書管理制御部１１０２が全文検索情報取得許可範囲７２が「全て許可」もしくは「一部許可」であると判断した場合は、ステップ（９０３）へ進み、「全て拒否」であると判断した場合は、ステップ（９１１）へ進む。

【０１３４】

そして、ステップ（９０３）で、文書管理制御部１１０２は、ユーザの許可範囲７３に含まれる文書の文書ＩＤの集合を取得し、各文書についてステップ（９０４）からステップ（９１０）の処理を繰り返す。

【０１３５】

次に、ステップ（９０４）で、文書管理制御部１１０２が、取得した文書ＩＤが設定されているいずれかの文書の全文検索情報登録状態、ここでは、図３に示した属性データベース１１０８に保持する全文検索情報登録状態３８を取得する。そして、文書管理制御部１１０２は、その全文検索情報登録状態３８が「登録済」であるか否かを判断する。

【０１３６】

ここで、文書管理制御部１１０２が「登録済」であると判断した場合は、ステップ（９１０）へ進み、次の文書について処理を行い、「未登録」であると判断した場合はステップ（９０５）へ進む。

【０１３７】

次に、ステップ（９０５）で、ステップ（９０１）で取得したポリシー管理サーバ１２００への認証情報と、未登録と判断した文書の文書ＩＤとを、ポリシー管理サーバ１２００に送信し、文書の復号化のための復号鍵をポリシー管理サーバ１２００から受信する。

【０１３８】

そして、ステップ（９０６）で、文書管理制御部１１０２がポリシー管理サーバ１２００から受信した復号鍵を用いての文書情報の復号化が成功したか否かを判定する。当該ユーザがポリシー管理サーバ１２００へ送信した文書ＩＤで特定される文書情報に対する参照権限以上のアクセス権を有していない場合や、ポリシー管理サーバ１２００には当該文書情報のポリシーが無い場合には、ポリシーサーバからは復号鍵が送られてこない。このような場合には文書情報を復号化することが出来ないのでステップ（９０６）は復号化が成功しないものと判定する。言い換えれば、当該文書ＩＤで特定される文書情報に対して、当該ユーザが参照権限委譲のアクセス権を有するポリシーが適用されていれば、当該文書情報の復号化が可能であり、引き続くインデクス生成処理が可能であると判断することもできる。ここで、文書管理制御部１１０２が復号化に成功したと判定した場合はステップ（９０７）へ進み、失敗したと判定した場合は、ステップ（９１０）へ進み、次の文書について処理を行う。

【０１３９】

次に、ステップ（９０７）で文書管理システムの文書管理制御部１１０２が復号化した文書から全文検索情報（インデクス）を取得し、全文検索情報を全文検索データベース１１０９に登録する（９０８）。そして、当該文書ＩＤに対する属性データベース１１０８

で管理される全文検索情報登録状態３８を「登録済」に状態を変更する（９０９）。
【０１４０】
以上、ステップ（９０３）からステップ（９０９）までの処理を、ユーザの全文検索情報取得許可範囲７２に含まれる文書について繰り返す（９１０）。
【０１４１】
そして、ステップ（９０２）からステップ（９１０）までの処理を、文書管理システムのテンポラリデータ１１０３に対して一時的に保持しているユーザのポリシー管理サーバ１２００への認証情報について繰り返して（９１１）、本処理を終了する。
【０１４２】
図１０は、本実施形態を示す文書管理システムにおける第３のデータ処理手順の一例を示すフローチャートである。本処理は、本システムの文書検索処理例である。なお、（１００１）～（１０１４）は各ステップを示す。本フローチャートは、クライアント１０００からの検索要求に基づいて開始する。
【０１４３】
ステップ（１００１）で、文書管理システムはユーザに対し、検索条件を問い合わせる。ユーザは、クライアント１０００からユーザインターフェース部１００１を介して検索条件を入力する。文書管理システムの文書管理制御部１００６は、ユーザインターフェース部１００１を介してその応答を受信して、図示しないメモリあるいはテンポラリデータ１００３上に検索条件を保持する。
【０１４４】
次に、ステップ（１００２）で、文書管理システムの文書管理制御部１００６は、上記メモリ上に保持される検索条件にマッチする文書を文書サーバ１１００に問合せる。これは以下の処理を行うことである。
【０１４５】
例えばデータベース制御部１１０６は、全文検索データベース１１０９から、上記検索条件にマッチする文書を検索し、検索インデクスＩＤの集合を返す。ここで、文書管理制御部１１０２は、検索インデクスＩＤを対応する文書ＩＤに変換し、テンポラリデータ１１０３に記憶する。以後、テンポラリデータ１１０３に記憶した文書ＩＤの集合を検索結果と記述する。
【０１４６】
文書管理システムは、検索結果に含まれる各文書について、ステップ（１００４）から（１０１３）の処理を行う。
【０１４７】
具体的には、ステップ（１００４）で、文書のアクセス権管理者がポリシー管理サーバ１２００であるか、文書管理システムであるか文書管理制御部１１０２が判定する。
【０１４８】
ここで、文書管理制御部１１０２がポリシー管理サーバ１２００であると判断した場合、ステップ（１００６）へ進み、文書管理システムであると判断した場合、ステップ（１００５）へ進む。
【０１４９】
そして、ステップ（１００５）で、文書管理システムの文書管理制御部１１０２は属性データベース１１０８を検索し、文書に対する操作ユーザのアクセス権を取得する。
【０１５０】
なお、ステップ（１００６）からステップ（１０１１）は、文書に対するアクセス権がポリシー管理サーバ１２００で管理されている場合の処理である。
【０１５１】
まず、ステップ（１００６）において、文書管理システムの文書管理制御部１１０２は、図５に示した文書のアクセス権５４を管理しているポリシー管理サーバ情報５２とポリシーＩＤ５３を取得する。
【０１５２】

そして、ステップ（１００７）において、文書管理システムの文書管理制御部１１０２は、ポリシーＩＤ５３に対する操作ユーザのアクセス権情報をテンポラリデータ１１０３上にキャッシュしているかどうか判定する。ここで、文書管理制御部１１０２がアクセス権情報のキャッシュが存在すると判定した場合は、そのアクセス権情報を取得し、ステップ（１０１２）へ進み、キャッシュが存在しないと判定した場合は、ステップ（１００８）へ進む。

【０１５３】

そして、ステップ（１００８）で、文書管理システムにおいて、文書管理制御部１１０２がテンポラリデータ１１０３上に一時的に保存している操作ユーザのポリシー管理サーバ１２００への認証情報６３が有効であるかどうかを判定する。

【０１５４】

ここで、文書管理制御部１１０２が認証情報６３が有効であると判定した場合は、ステップ（１０１０）へ進む。

【０１５５】

一方、文書管理制御部１１０２が無効であると判定した場合は、図８で示したポリシー管理サーバ１２００への認証処理を行うため、ステップ（１００９）で、ポリシー管理サーバ１２００への認証情報を取得する。

【０１５６】

文書管理システムのポリシーデータ処理部１１０５は、ポリシー管理サーバ１２００に対して、認証情報とポリシーＩＤを付してアクセス権を問い合わせる。ポリシー管理サーバ１２００は、ポリシーＩＤで管理されるポリシーのうち、当該ユーザに関連付けられたアクセス権情報を返す。文書管理システムのポリシーデータ処理部１１０５は、ポリシー管理サーバ１２００からアクセス権情報を受信する（１０１０）。そして、文書管理システムの文書管理制御部１１０２は、ポリシー管理サーバ１２００から受信したアクセス権をテンポラリデータ１１０３上のキャッシュに追加登録する（１０１１）。

【０１５７】

次に、ステップ（１０１２）で、文書管理システムにおいて、文書管理制御部１１０２がステップ（１００５）または（１００７）または（１０１０）で取得した、文書に対するアクセス権が図５に例示される、「読み込み権」以上であるか否かを判断する。

【０１５８】

ここで、文書管理制御部１１０２が文書に対するアクセス権が「読み込み権」以上でないと判断した場合は、検索結果から当該文書のＩＤを取り除く（１０１３）。以上の処理を、検索結果に含まれる各文書について繰り返す（１０１４）。そして、ステップ（１０１５）において、文書管理システムの文書管理制御部１１０２は、クライアント１０００に検索結果を通知する。これにより、クライアント１０００のユーザインターフェース部１００１を介して、クライアント１０００が備えるデバイス制御部１００３が表示装置に検索結果を表示して、ユーザに確認させて、本処理を終了する。

【０１５９】

これにより、文書管理装置において、アクセス権が外部のポリシー管理サーバで管理され、暗号化された状態で格納されている文書についても全文検索が可能となる。

【０１６０】

また、検索結果として検索したユーザがアクセス可能な文書のみが検索結果として表示されるようになり、セキュリティとユーザの利便性を向上させることができる。

【０１６１】

〔第２実施形態〕

上記実施形態では、ポリシー管理サーバ１２００で文書に対するポリシーを管理する場合に、その権限等が変更される場合がある。

【０１６２】

そこで、ポリシー管理サーバ１２００からポリシーの変更通知を文書管理制御部１１０２が受信した場合には、ポリシーデータ処理部１１０５が以下の処理を行う。

【０１６３】
ポリシーデータ処理部１１０５が受信したポリシーの変更通知によって対応するポリシーのアクセス権情報を削除する。具体的には、ユーザＩＤ等を参照して、属性データベース１１０８内のアクセス権限等を削除する。
【０１６４】
また、ポリシー管理サーバ１２００から変更後のポリシーの内容もあわせて通知された場合は、変更後のポリシーで規定してるアクセス権情報で変更前のアクセス権情報を上書きするようにしても良い。
【０１６５】
これにより、最新のアクセス権限に適応した文書検索処理を行える。
【０１６６】
〔第３実施形態〕
以下、図１１に示すメモリマップを参照して本発明に係る文書管理装置で読み取り可能なデータ処理プログラムの構成について説明する。
【０１６７】
図１１は、本発明に係る文書管理装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体のメモリマップを説明する図である。
【０１６８】
なお、特に図示しないが、記憶媒体に記憶されるプログラム群を管理する情報、例えばバージョン情報，作成者等も記憶され、かつ、プログラム読み出し側のＯＳ等に依存する情報、例えばプログラムを識別表示するアイコン等も記憶される場合もある。
【０１６９】
さらに、各種プログラムに従属するデータも上記ディレクトリに管理されている。また、各種プログラムをコンピュータにインストールするためのプログラムや、インストールするプログラムが圧縮されている場合に、解凍するプログラム等も記憶される場合もある。
【０１７０】
本実施形態における図８に示す機能が外部からインストールされるプログラムによって、ホストコンピュータにより遂行されていてもよい。そして、その場合、ＣＤ－ＲＯＭやフラッシュメモリやＦＤ等の記憶媒体により、あるいはネットワークを介して外部の記憶媒体から、プログラムを含む情報群を出力装置に供給される場合でも本発明は適用されるものである。
【０１７１】
以上のように、前述した実施形態の機能を実現するソフトウエアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給する。そして、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。
【０１７２】
この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１７３】
従って、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。
【０１７４】
プログラムを供給するための記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤなどを用いることができる。
【０１７５】

この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【０１７６】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続する。そして、該ホームページから本発明のコンピュータプログラムそのもの、もしくは、圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバやｆｔｐサーバ等も本発明の請求項に含まれるものである。

【０１７７】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせる。そして、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【０１７８】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけではない。例えばそのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行う。そして、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１７９】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込ませる。その後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１８０】

本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から排除するものではない。

【０１８１】

本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるのではない。

【図面の簡単な説明】

【０１８２】

【図１】本発明の第１実施形態を示す文書管理装置の構成を説明するブロック図である。

【図２】図１に示した属性データベースに登録されている文書に関する情報のデータ構造を説明する概念図である。

【図３】図１に示した属性データベースに保持する文書属性情報の一部を説明する図である。

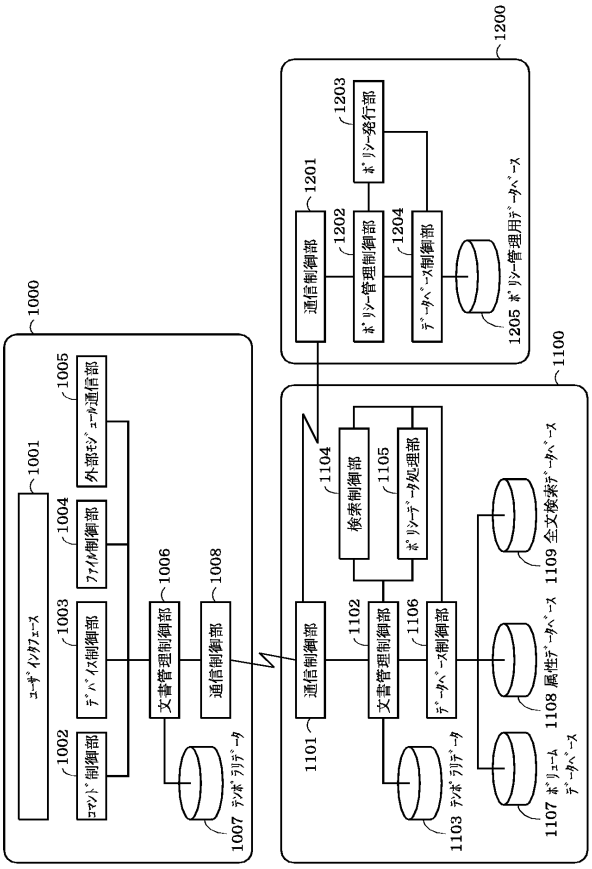
【図４】図１に示した属性データベースに保持されるアクセス権情報の一例を示す図である。

【図５】図１に示した属性データベースに保持されるポリシー管理サーバのポリシー情報のキャッシュの一例を示す図である。

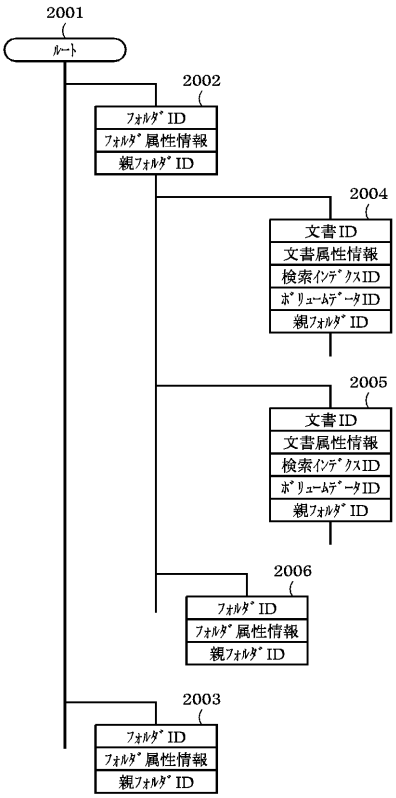
【図６】図１に示したテンポラリデータに保存されるポリシー管理サーバへの認証情報の

一例を示す図である。
【図７】図１に示した属性データベースに保存されるユーザ毎の全文検索情報取得範囲を示す図である。
【図８】本実施形態を示す文書管理装置における第１のデータ処理手順の一例を示すフローチャートである。
【図９】本実施形態を示す文書管理装置における第２のデータ処理手順の一例を示すフローチャートである。
【図１０】本実施形態を示す文書管理装置における第３のデータ処理手順の一例を示すフローチャートである。
【図１１】本発明に係る文書管理装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体のメモリマップを説明する図である。
【符号の説明】
【０１８３】
１０００　クライアント
１００６　文書管理制御部
１１００　文書サーバ
１１０２　文書管理制御部
１１０３　テンポラリデータ
１１０４　検索制御部
１１０５　ポリシーデータ処理部
１１０６　データベース制御部
１２００　ポリシー管理サーバ

【図１】



【図２】



【図３】

1108

31 文書ID	32 親ﾌｫﾙﾀﾞID	33 文書名	34 ｱｸｾｽ権管理者	35 ｱｸｾｽ権ID	36 ﾎﾟﾘｼｰ管理ｻｰﾊﾞ情報	37 ﾎﾟﾘｼｰID	38 全文検索情報登録状態
1	1	文書1	文書管理ｼｽﾃﾑ	1	－	－	登録済
2	1	文書2	ﾎﾟﾘｼｰ管理ｻｰﾊﾞ	－	192.168.0.100	3	未登録
3	2	文書3	ﾎﾟﾘｼｰ管理ｻｰﾊﾞ	－	192.168.0.200	4	登録済

【図４】

1108

41 ｱｸｾｽ権ID	42 ﾕｰｻﾞID	43 ｱｸｾｽ権
1	1	削除権
1	2	読み込み権
1	3	書き込み権
2	1	書き込み権
3	2	読み込み権

【図５】

1108

51 ﾕｰｻﾞID	52 ﾎﾟﾘｼｰ管理ｻｰﾊﾞ情報	53 ﾎﾟﾘｼｰID	54 ｱｸｾｽ権
1	192.168.0.100	3	なし
1	192.168.0.100	7	参照権
1	192.168.0.200	11	読み込み権
2	192.168.0.100	3	書き込み権
3	192.168.0.100	3	削除権

【図６】

1108

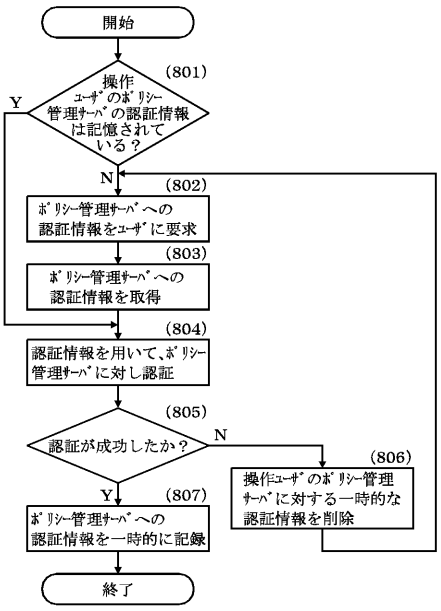
61 ﾕｰｻﾞID	62 ﾎﾟﾘｼｰ管理ｻｰﾊﾞ情報	63 認証情報	64 ｸﾚﾃﾞﾝｼｬﾙ	65 ﾕｰｻﾞ名	66 ﾊﾟｽﾜｰﾄﾞ	67 有効期限
1	192.168.0.100	未認証	－	－	－	－
1	192.168.0.200	ｸﾚﾃﾞﾝｼｬﾙ	fajdhfauh343fafd95	－	－	－
2	192.168.0.100	ﾊﾟｽﾜｰﾄﾞ	－	taro	taro1	6/20 18:00
2	192.168.0.200	未認証	－	－	－	－

【図７】

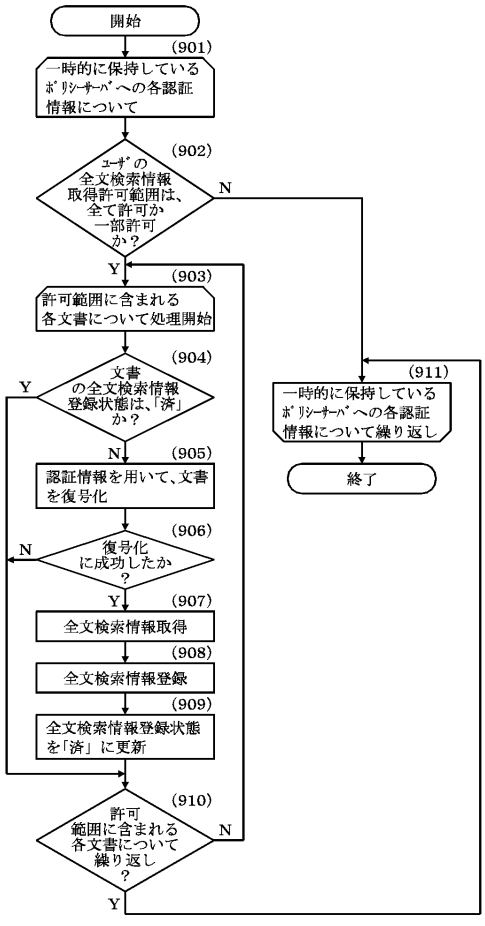
1108

71 ﾕｰｻﾞID	72 全文検索情報取得許可範囲	73 許可範囲
1	全て許可	－
2	一部許可	1,4,7,9
3	全て拒否	－

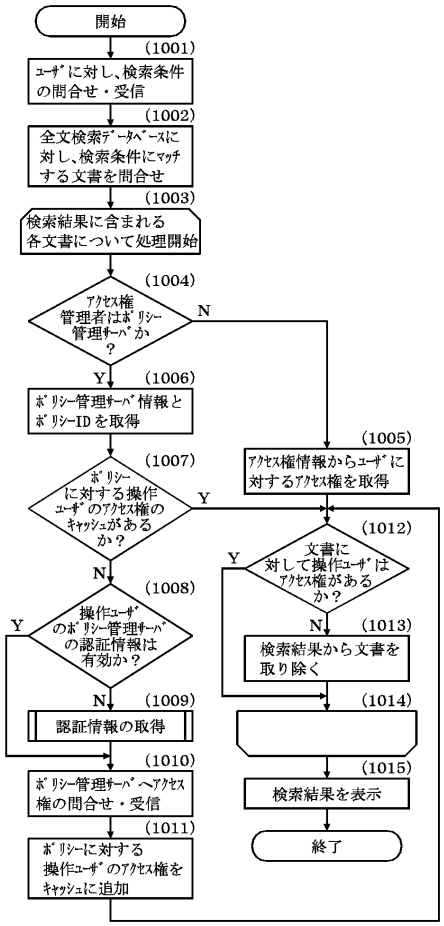
【図８】



【図９】



【図１０】



【図１１】

FD/CD-ROM等の記憶媒体

ディレクトリ情報
第１のデータ処理プログラム 図８に示すフローチャートのステップに対応するプログラムコード群
第２のデータ処理プログラム 図９に示すフローチャートのステップに対応するプログラムコード群
第３のデータ処理プログラム 図10に示すフローチャートのステップに対応するプログラムコード群

記憶媒体のメモリマップ

フロントページの続き

(56)参考文献 特開２００５－０８５１１３（ＪＰ，Ａ）
特開２００３－１６２４４９（ＪＰ，Ａ）
特開２００２－０７３４１９（ＪＰ，Ａ）
特開２００４－２５９２０２（ＪＰ，Ａ）
特開２００１－０７５８５４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１７／３０
Ｇ０６Ｆ　１２／００
Ｇ０６Ｆ　２１／２４