

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-182122
(P2017-182122A)

(43) 公開日 平成29年10月5日(2017.10.5)

(51) Int.Cl.		F I		テーマコード (参考)
G06F 21/62	(2013.01)	G06F 21/62	309	
G06F 12/00	(2006.01)	G06F 12/00	537A	

審査請求 未請求 請求項の数 12 O L (全 20 頁)

(21) 出願番号 特願2016-63304 (P2016-63304)
(22) 出願日 平成28年3月28日 (2016. 3. 28)

(71) 出願人 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 100086933
弁理士 久保 幸雄
(74) 代理人 100125117
弁理士 坂田 泰弘
(72) 発明者 岡 鉄也
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

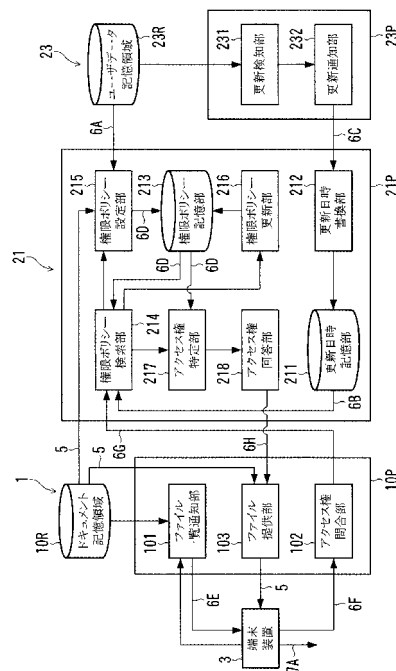
(54) 【発明の名称】 データ提供システム、アクセス権管理装置、データ提供方法、およびコンピュータプログラム

(57) 【要約】

【課題】ポリシーに基づくファイルのアクセス権の管理を従来よりも容易に行う。

【解決手段】権限ポリシー設定部215は、ドキュメント記憶領域10Rに保存されているファイル5をユーザから要求された際にこのファイル5のアクセス権が未だ設定されていなければ、このファイル5によって再現されるドキュメントの内容または属性を解析し、解析結果に基づいて設定する。そして、ファイル提供部103は、このアクセス権に従ってこのファイル5をユーザへ提供する。

【選択図】図5



【特許請求の範囲】**【請求項 1】**

保存手段に保存されている、ドキュメントのデータを提供する、データ提供システムであって、

前記データをユーザから要求された際に当該データのアクセス権が未だ設定されていない場合に、当該データに係る前記ドキュメントの内容または属性を解析する解析手段と、

前記データのアクセス権を、前記解析手段によって解析された前記内容または属性に基づいて設定する、設定手段と、

前記データをユーザから要求された後、前記アクセス権が前記設定手段によって設定された場合に、当該アクセス権に従って当該データを当該ユーザへ提供する、提供手段と、
を有することを特徴とするデータ提供システム。

10

【請求項 2】

前記データは、複数のユーザによって共有され得るものであり、

前記設定手段は、前記複数のユーザのそれぞれに対して前記アクセス権を設定する、

請求項 1 に記載のデータ提供システム。

【請求項 3】

前記データを前記ユーザから要求された際に前記アクセス権が既に設定されていれば、当該アクセス権を所定の規則に基づいて更新する、更新手段、

を有し、

前記提供手段は、前記データを前記ユーザから要求された後、前記アクセス権が更新手段によって更新された場合は、当該更新されたアクセス権に従って当該データを当該ユーザへ提供する、

請求項 1 に記載のデータ提供システム。

20

【請求項 4】

前記データは、複数のユーザによって共有され得るものであり、

前記設定手段は、前記複数のユーザのうちの一部のユーザに対してのみ前記データを使用することが認められるように、前記アクセス権を設定し、

前記更新手段は、更新する回数が増えるにつれて制限が緩くなるように前記アクセス権を更新する、

請求項 3 に記載のデータ提供システム。

30

【請求項 5】

前記更新手段は、前記回数が増えるにつれて前記複数のユーザのうちの前記データを使用することが認められるものが増えるように、前記アクセス権を更新する、

請求項 4 に記載のデータ提供システム。

【請求項 6】

前記データは、ドキュメントを再現するためのものであって、

前記設定手段は、前記複数のユーザのうちの前記ドキュメントの作成者に対して前記データを使用することが認められるように、前記アクセス権を設定する、

請求項 4 または請求項 5 に記載のデータ提供システム。

【請求項 7】

前記更新手段は、前記複数のユーザのうちの前記ドキュメントの作成者と同じ部署に所属するユーザに対して前記データを使用することが認められるように、前記アクセス権を更新する、

請求項 6 に記載のデータ提供システム。

40

【請求項 8】

前記更新手段は、前記複数のユーザのうちの前記ドキュメントに関連するユーザに対して前記データを使用することが認められるように、前記アクセス権を更新する、

請求項 6 または請求項 7 に記載のデータ提供システム。

【請求項 9】

前記更新手段は、前記複数のユーザのうち、前記データを使用することが以前に認め

50

られたが現在まで所定の期間以上、当該データを使用したことがないユーザに対しては、当該データを使用することが認められないように、前記アクセス権を更新する、請求項 4 ないし請求項 8 のいずれかに記載のデータ提供システム。

【請求項 10】

保存手段に保存されているドキュメントのデータのアクセス権を管理するアクセス権管理装置であって、

ユーザが前記データを要求した際に前記アクセス権が未だ設定されていない場合に、当該データに係る前記ドキュメントの内容または属性を解析する解析手段と、

前記データのアクセス権を、前記解析手段によって解析された前記内容または属性に基づいて設定する、設定手段と、

を有することを特徴とするアクセス権管理装置。

10

【請求項 11】

保存手段に保存されている、ドキュメントのデータを提供する、データ提供方法であって、

前記データをユーザから要求された際に当該データのアクセス権が未だ設定されていない場合に、当該データに係る前記ドキュメントの内容または属性を解析し、

前記データのアクセス権を、解析した前記内容または属性に基づいて設定し、

前記データをユーザから要求された後、前記アクセス権が設定された場合に、当該アクセス権に従って当該データを当該ユーザへ提供する、

ことを特徴とするデータ提供方法。

20

【請求項 12】

保存手段に保存されているドキュメントのデータのアクセス権を管理するコンピュータに用いられるコンピュータプログラムであって、

前記コンピュータに、

ユーザが前記データを要求した際に前記アクセス権が未だ設定されていない場合に、当該データに係る前記ドキュメントの内容または属性を解析する解析処理を実行させ、

前記データのアクセス権を、前記解析処理によって解析された前記内容または属性に基づいて設定する、設定処理を実行させる、

ことを特徴とするコンピュータプログラム。

30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データのアクセス権の管理の技術に関する。

【背景技術】

【0002】

従来、ドキュメントを表示または印刷するためのデータが不正にアクセスされるのを防止するために、特定のユーザに対してのみデータへアクセスするのを許可する技術が提案されている。具体的には、データを管理する装置（例えば、ファイルサーバ）は、特定のユーザに対してのみ、データのアクセス権を付与する。そして、アクセス権の範囲内で特定のユーザによるデータの使用を許可する。

40

【0003】

さらに、セキュリティの保護に鑑みたデータの提供の技術として、次のような技術が提案されている。情報処理端末であるクライアントは、PCに搭載されているデータ通信処理装置と、機密情報転送装置とを備えており、さらに、通信管理装置、AP、送信結果提示装置を備えている。また、機密情報転送装置は、複数の通信路の機密経路レベルを判定する機密経路判定部と、最適経路判定部と、機密キーワード定義DB及び形態素解析手段を有し、送信すべきデータの機密データレベルを判定する機密データ判定部と、機密経路レベル及び機密データレベルに基づいて最適な通信路を選択する最適経路判定部とを備えて構成される（特許文献1）。

【0004】

50

複合装置は、画像入出力部が取り込んだ電子文書から特徴量解析部が、その特徴量を抽出して、配信先決定部が、該特徴量に基づいて電子文書の配信先を決定し、文書管理部が、文書提供元情報を取得して、該電子文書の文書提供元情報、該特徴量及び該配信先に関連する配信先関連情報を文書関連情報として該電子文書に関連付けて配信情報記憶部に記憶させるとともに、送受信部から該電子文書を該配信先へ配信する。電子文書の出力要求が出力要求元機器からあると、文書管理部が、該出力要求元機器の出力要求元情報を取得し、該出力要求元情報と文書関連データ記憶部の出力要求のあった電子文書の文書関連情報及び要求において入力された文書関連情報に基づいて電子文書の出力許可/不許可を制御する(特許文献2)。

【0005】

そのほか、ドキュメントのファイルを新たに保存する際に、予め決められたポリシーに基づいてそのファイルのアクセス権を付与する技術が知られている。

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2002-135351号公報

【特許文献2】特開2014-115748号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかし、ポリシーがない時期に保存されたデータには、管理者またはドキュメントの作成者がアクセス権を設定する作業を行っていない限り、アクセス権が設定されていないことが多い。

【0008】

したがって、ポリシーが決められた後、これらのデータについてポリシーを遵守するには、管理者または作成者がアクセス権を設定する作業を行わなければならない。

【0009】

また、ポリシーが変更された場合は、既存のデータのアクセス権を見直し、変更後のポリシーに合わせてアクセス権を設定し直す作業を行わなければならないことがある。

【0010】

しかし、従来技術によると、データのアクセス権に関するこれらの作業の煩わしさを解消することができない。

【0011】

本発明は、このような問題点に鑑み、ポリシーに基づくデータのアクセス権の管理を従来よりも容易に行うことを目的とする。

【課題を解決するための手段】

【0012】

本発明の一形態に係るデータ提供システムは、保存手段に保存されている、ドキュメントのデータを提供する、データ提供システムであって、前記データをユーザから要求された際に当該データのアクセス権が未だ設定されていない場合に、当該データに係る前記ドキュメントの内容または属性を解析する解析手段と、前記データのアクセス権を、前記解析手段によって解析された前記内容または属性に基づいて設定する、設定手段と、前記データをユーザから要求された後、前記アクセス権が前記設定手段によって設定された場合に、当該アクセス権に従って当該データを当該ユーザへ提供する、提供手段と、を有する。

【0013】

好ましくは、前記データは、複数のユーザによって共有され得るものであり、前記設定手段は、前記複数のユーザのそれぞれに対して前記アクセス権を設定する。

【0014】

または、前記データを前記ユーザから要求された際に前記アクセス権が既に設定されて

10

20

30

40

50

いれば、当該アクセス権を所定の規則に基づいて更新する、更新手段、を有し、前記提供手段は、前記データを前記ユーザから要求された後、前記アクセス権が更新手段によって更新された場合は、当該更新されたアクセス権に従って当該データを当該ユーザへ提供する。

【0015】

または、前記データは、複数のユーザによって共有され得るものであり、前記設定手段は、前記複数のユーザのうちの一部のユーザに対してのみ前記データを使用することが認められるように、前記アクセス権を設定し、前記更新手段は、更新する回数が増えるにつれて制限が緩くなるように前記アクセス権を更新する。

【発明の効果】

10

【0016】

本発明によると、ポリシーに基づくデータのアクセス権の管理を従来よりも容易に行うことができる。

【図面の簡単な説明】

【0017】

【図1】ドキュメント共有システムの全体的な構成の例を示す図である。

【図2】ドキュメント管理サーバのハードウェア構成の例を示す図である。

【図3】ユーザデータの例を示す図である。

【図4】端末装置のハードウェア構成の例を示す図である。

【図5】ドキュメント管理サーバ、権限ポリシー管理サーバ、およびユーザ管理サーバそれぞれの機能的構成の例を示す図である。

20

【図6】権限ポリシーデータの例を示す図である。

【図7】ドキュメント管理サーバにおける全体的な処理の流れの例を説明するフローチャートである。

【図8】権限ポリシー管理サーバにおける全体的な処理の流れの例を説明するフローチャートである。

【図9】ドキュメント管理サーバにおける全体的な処理の流れの変形例を説明するフローチャートである。

【図10】ドキュメント管理サーバにおける全体的な処理の流れの変形例を説明するフローチャートである。

30

【発明を実施するための形態】

【0018】

図1は、ドキュメント共有システム100の全体的な構成の例を示す図である。図2は、ドキュメント管理サーバ1のハードウェア構成の例を示す図である。図3は、ユーザデータ6Aの例を示す図である。図4は、端末装置3のハードウェア構成の例を示す図である。

【0019】

図1に示すように、ドキュメント共有システム100は、ドキュメント管理サーバ1、権限ポリシー管理サーバ21、ユーザ管理サーバ23、端末装置3、および通信回線4などによって構成される。

40

【0020】

ドキュメント管理サーバ1、権限ポリシー管理サーバ21、ユーザ管理サーバ23、および端末装置3は、通信回線4を介して通信することができる。通信回線4として、インターネット、LAN (Local Area Network)、公衆回線、または専用線などが用いられる。

【0021】

ドキュメント共有システム100は、文書、図表、写真、またはイラストなどによって構成されるドキュメント(書類)を複数のユーザによって使用するためのシステムである。

【0022】

50

以下、ある企業においてドキュメント共有システム 100 が使用される場合を説明する。したがって、この企業の従業員がドキュメント共有システム 100 のユーザである。各ユーザには、ユーザアカウントが 1 つずつ与えられている。ユーザアカウントには、ユニークなユーザコードが付されている。

【0023】

ドキュメント管理サーバ 1 は、ドキュメントをファイル単位で管理する。そして、端末装置 3 からの要求に基づいて、ファイルを端末装置 3 へ提供する。ドキュメント管理サーバ 1 として、いわゆるサーバ機または N A S (Network Attached Storage) などが用いられる。

【0024】

ドキュメント管理サーバ 1 は、図 2 に示すように、C P U (Central Processing Unit) 10 a、R A M (Random Access Memory) 10 b、R O M (Read Only Memory) 10 c、大容量記憶装置 10 d、および N I C (Network Interface Card) 10 e などによって構成される。

【0025】

N I C 10 e は、T C P / I P (Transmission Control Protocol/Internet Protocol) などのプロトコルによって通信回線 4 を介して権限ポリシー管理サーバ 2 1、ユーザ管理サーバ 2 3、および端末装置 3 などと通信を行う。

【0026】

大容量記憶装置 10 d には、各ドキュメントのファイル 5 を記憶するためのドキュメント記憶領域 10 R (図 5 参照) が設けられている。ファイル 5 は、ドキュメントを再現するためのファイルであって、P D F (Portable Document Format) ファイル、テキストファイル、または種々のアプリケーション (例えば、マイクロソフト社のワード、エクセル、またはパワーポイントなど) 用のフォーマットのファイルである。

【0027】

さらに、R O M 10 c または大容量記憶装置 10 d には、ファイル 5 を管理するためのファイル管理プログラム 10 P (図 5 参照) が記憶されている。

【0028】

ファイル管理プログラム 10 P は、R A M 10 b にロードされ、C P U 10 a によって実行される。大容量記憶装置 10 d として、ハードディスクまたは S S D (Solid State Drive) などが用いられる。

【0029】

権限ポリシー管理サーバ 2 1 は、各ファイル 5 の権限ポリシーを管理する。「権限ポリシー」は、ファイル 5 への各ユーザのアクセスに関するポリシー (規則) である。具体的には、権限ポリシーは、ユーザごとの、ファイル 5 のアクセス権を定める。

【0030】

権限ポリシー管理サーバ 2 1 のハードウェアの構成は、ドキュメント管理サーバ 1 と基本的に同様であり、図 2 に示した通りである。

【0031】

ただし、R O M または大容量記憶装置には、権限ポリシーを管理するための権限ポリシー管理プログラム 2 1 P (図 5 参照) が記憶されている。権限ポリシー管理プログラム 2 1 P は、R A M にロードされ、C P U によって実行される。

【0032】

ユーザ管理サーバ 2 3 は、各ユーザのユーザアカウント、部署、職級 (例えば、部長、課長、一般社員など)、および連絡先など情報を管理する。

【0033】

ユーザ管理サーバ 2 3 のハードウェアの構成は、ドキュメント管理サーバ 1 と基本的に同様であり、図 2 に示した通りである。

【0034】

ただし、大容量記憶装置には、ユーザデータ記憶領域 2 3 R が設けられている。ユーザ

10

20

30

40

50

データ記憶領域 2 3 R には、図 3 に示すように、ユーザごとのユーザデータ 6 A が記憶されている。ユーザデータ 6 A には、ユーザのユーザコード、所属部署（現在、所属している部署）、職級、および連絡先などが示される。

【 0 0 3 5 】

ユーザデータ 6 A は、この企業にユーザ（従業員）が入社した際に、管理者によって作成され、ユーザデータ記憶領域 2 3 R に記憶される。

【 0 0 3 6 】

さらに、ユーザが異動するごとに、異動先の部署が示されるように、そのユーザのユーザデータ 6 A が管理者によって更新される。また、ユーザの職級または連絡先が代わるごとに、新たな職級または連絡先が示されるように、そのユーザのユーザデータ 6 A が管理者によって更新される。

10

【 0 0 3 7 】

さらに、ROM または大容量記憶装置には、変更通知プログラム 2 3 P（図 5 参照）が記憶されている。変更通知プログラム 2 3 P は、RAM にロードされ、CPU によって実行される。

【 0 0 3 8 】

端末装置 3 は、ユーザがファイル 5 へアクセスしドキュメントを閲覧したり編集したりするための装置である。端末装置 3 として、スマートフォン、タブレットコンピュータ、携帯電話端末、パーソナルコンピュータなどが用いられる。以下、パーソナルコンピュータが端末装置 3 として用いられる場合を例に説明する。

20

【 0 0 3 9 】

端末装置 3 は、図 4 に示すように、CPU 3 0 a、RAM 3 0 b、ROM 3 0 c、補助記憶装置 3 0 d、液晶ディスプレイ 3 0 e、NIC 3 0 f、キーボード 3 0 g、およびポインティングデバイス 3 0 h などによって構成される。

【 0 0 4 0 】

液晶ディスプレイ 3 0 e には、ドキュメントのほか、端末装置 3 へ指令を与えるための画面などが表示される。

【 0 0 4 1 】

NIC 3 0 f は、TCP / IP などのプロトコルによってドキュメント管理サーバ 1 などと通信回線 4 を介して通信を行う。

30

【 0 0 4 2 】

キーボード 3 0 g およびポインティングデバイス 3 0 h は、ユーザが情報およびコマンドを入力するために用いられる。

【 0 0 4 3 】

ROM 3 0 c または補助記憶装置 3 0 d には、オペレーティングシステム、ウェブブラウザ、およびドキュメント管理サーバ 1 のドライバなどが記憶されている。これらのプログラムは、必要に応じて RAM 3 0 b にロードされ、CPU 3 0 a によって実行される。補助記憶装置 3 0 d として、ハードディスクまたは SSD などが用いられる。

【 0 0 4 4 】

ところで、少なくとも一部のファイル 5 は、ファイル管理プログラム 1 0 P および権限ポリシー管理サーバ 2 1 の運用が開始される前に、ドキュメント記憶領域 1 0 R に記憶されている。このようなファイル 5 には、運用が開始された時点では、権限ポリシーが設定されていない。

40

【 0 0 4 5 】

従来、ファイル 5 に権限ポリシーが設定されていない場合は、管理者またはファイル 5 の作成者が権限ポリシーを設定する作業を行わなければならない。

【 0 0 4 6 】

しかし、ファイル管理プログラム 1 0 P、権限ポリシー管理プログラム 2 1 P、および変更通知プログラム 2 3 P によると、作業を行うことなく、権限ポリシーを設定することができる。以下、この仕組みについて、説明する。

50

【 0 0 4 7 】

図 5 は、ドキュメント管理サーバ 1、権限ポリシー管理サーバ 2 1、およびユーザ管理サーバ 2 3 それぞれの機能的構成の例を示す図である。

【 0 0 4 8 】

ファイル管理プログラム 1 0 P によると、図 5 に示すファイル一覧通知部 1 0 1、アクセス権問合せ部 1 0 2、およびファイル提供部 1 0 3 などの機能がドキュメント管理サーバ 1 に実現される。

【 0 0 4 9 】

権限ポリシー管理プログラム 2 1 P によると、更新日時記憶部 2 1 1、更新日時書換部 2 1 2、権限ポリシー記憶部 2 1 3、権限ポリシー検索部 2 1 4、権限ポリシー設定部 2 1 5、権限ポリシー更新部 2 1 6、アクセス権特定部 2 1 7、およびアクセス権回答部 2 1 8 などの機能がドキュメント管理サーバ 1 に実現される。

10

【 0 0 5 0 】

変更通知プログラム 2 3 P によると、更新検知部 2 3 1 および更新通知部 2 3 2 などの機能がドキュメント管理サーバ 1 に実現される。

【 0 0 5 1 】

〔人事に関する処理〕

更新日時記憶部 2 1 1 には、更新日時データ 6 B が記憶されている。更新日時データ 6 B は、最近にユーザの情報に関する更新があった日時を示す。デフォルトの値は、「N U L L」である。更新日時データ 6 B は、次のように書き換えられる。

20

【 0 0 5 2 】

ユーザ管理サーバ 2 3 において、ユーザが異動したり職級が変わったりすると、上述の通り、そのユーザのユーザデータ 6 A (図 3 参照) が管理者によって更新される。

【 0 0 5 3 】

更新検知部 2 3 1 は、ユーザデータ記憶領域 2 3 R を常時、監視し、ユーザデータ 6 A が更新されたことを検知する。

【 0 0 5 4 】

すると、更新通知部 2 3 2 は、ユーザデータ 6 A が更新された日時を示す更新通知データ 6 C を権限ポリシー管理サーバ 2 1 へ送信する。

【 0 0 5 5 】

なお、複数のユーザのユーザデータ 6 A が同じ時期 (例えば、同じ日) に更新されることがある。このような場合は、これらのユーザデータ 6 A のうちの最後が更新された後、当該最後のユーザデータ 6 A が更新された日時を示すデータを 1 つだけ、更新通知データ 6 C として送信すればよい。最後が更新されたことは、管理者が所定のコマンドを入力することによってユーザ管理サーバ 2 3 へ知らせればよい。

30

【 0 0 5 6 】

そして、権限ポリシー管理サーバ 2 1 において、更新日時書換部 2 1 2 は、更新通知データ 6 C を受信すると、更新日時データ 6 B に示される日時を、更新通知データ 6 C に示される日時に書き換える。これにより、更新日時データ 6 B は、最近にユーザの情報に関する更新があった日時を示すようになる。

40

【 0 0 5 7 】

〔ファイル 5 に関する処理〕

図 6 は、権限ポリシーデータ 6 D の例を示す図である。

【 0 0 5 8 】

権限ポリシー管理サーバ 2 1 において、権限ポリシー記憶部 2 1 3 には、図 6 に示すように、ファイル 5 ごとの権限ポリシーデータ 6 D が記憶されている。権限ポリシーデータ 6 D には、ファイル 5 のファイル名、R / W 権を有するユーザのユーザコード、および R 権を有するユーザのユーザコード、有効期限、および更新日時が示される。

【 0 0 5 9 】

「R / W 権」は、ファイル 5 の読取権および書込権の両方を含む権限であり、「R 権」

50

は、ファイル 5 の読取権および書込権のうちの読取権のみを含む権限である。読取権によると、ファイル 5 をアプリケーションなどで開いてドキュメントを閲覧することができるが、編集することはできない。一方、書込権によると、ドキュメント編集することができる。

【 0 0 6 0 】

「有効期限」は、これらの R / W 権および R 権が有効である期限である。つまり、有効期限を過ぎると、これらの R / W 権および R 権は、無効になる。「更新日時」は、この権限ポリシーデータ 6 D が最後に更新された日時である。ただし、この権限ポリシーデータ 6 D が作成される時点では、作成された日時が更新日時として示される。

【 0 0 6 1 】

一部のファイル 5 の権限ポリシーデータ 6 D は、未だ権限ポリシー記憶部 2 1 3 に記憶されておらず、後述する権限ポリシー設定部 2 1 5 によって生成され、権限ポリシー記憶部 2 1 3 に記憶される。

【 0 0 6 2 】

ユーザは、次のように、端末装置 3 を使用してファイル 5 へアクセスし、ドキュメントを閲覧しまたは編集することができる。

【 0 0 6 3 】

ユーザは、自分のユーザアカウントで端末装置 3 へ予めログインしておく。端末装置 3 のウェブブラウザを起動し、ドキュメント管理サーバ 1 のドキュメント記憶領域 1 0 R の URL (Uniform Resource Locator) をウェブブラウザへ入力する。

【 0 0 6 4 】

すると、ウェブブラウザは、入力された URL に基づいてウェブページをドキュメント管理サーバ 1 へ要求する。

【 0 0 6 5 】

ドキュメント管理サーバ 1 において、ファイル一覧通知部 1 0 1 は、端末装置 3 からの要求に従って、一覧データ 6 E を端末装置 3 へ送信する。一覧データ 6 E には、ドキュメント記憶領域 1 0 R に記憶されているすべてのファイル 5 それぞれのファイル名が示されている。

【 0 0 6 6 】

ウェブブラウザは、一覧データ 6 E を受信すると、一覧データ 6 E に基づいて一覧画面 7 A を表示する。一覧画面 7 A には、一覧データ 6 E に示されるファイル名が並んでいる。

【 0 0 6 7 】

ユーザは、閲覧しまたは編集したいドキュメントのファイル 5 のファイル名を一覧画面 7 A の中から選択する。

【 0 0 6 8 】

すると、ウェブブラウザは、リクエストデータ 6 F をドキュメント管理サーバ 1 へ送信する。リクエストデータ 6 F には、選択されたファイル名、そのユーザのユーザコード、およびファイル 5 の要求が示される。

【 0 0 6 9 】

ドキュメント管理サーバ 1 において、アクセス権問合せ部 1 0 2 は、リクエストデータ 6 F を受信すると、権限ポリシー管理サーバ 2 1 へ問合せデータ 6 G を送信することによって、そのユーザへ与えられているそのファイル 5 のアクセス権を問い合わせる。問合せデータ 6 G には、リクエストデータ 6 F に示されるファイル名およびユーザコードとアクセス権の回答の要求とが示される。

【 0 0 7 0 】

権限ポリシー管理サーバ 2 1 において、問合せデータ 6 G が送信されてきたら、そのユーザのアクセス権を特定し回答するための処理が権限ポリシー検索部 2 1 4 ないしアクセス権回答部 2 1 8 によって次のように行われる。

【 0 0 7 1 】

10

20

30

40

50

権限ポリシー検索部 2 1 4 は、問合せデータ 6 G に示されるファイル名を示す権限ポリシーデータ 6 D を権限ポリシー記憶部 2 1 3 から検索する。

【 0 0 7 2 】

そのような権限ポリシーデータ 6 D が権限ポリシー記憶部 2 1 3 に記憶されていない場合、つまり、権限ポリシー検索部 2 1 4 によって検索されなかった場合は、権限ポリシー設定部 2 1 5 は、権限ポリシーの設定のための処理を次のように実行する。

【 0 0 7 3 】

権限ポリシー設定部 2 1 5 は、問合せデータ 6 G に示されるファイル名のファイル 5 をドキュメント管理サーバ 1 からダウンロードする。なお、権限ポリシー管理サーバ 2 1 には、ドキュメント管理サーバ 1 のドキュメント記憶領域 1 0 R に記憶されているファイルへのアクセス権が予め与えられている。

10

【 0 0 7 4 】

権限ポリシー設定部 2 1 5 は、ユーザへの、そのファイル 5 の R / W 権および R 権の与え方（アクセス権付与方法）を、次のレベル__1、レベル__2、およびレベル__3 のうちのいずれかのレベルの方法に決定する。

【 0 0 7 5 】

（レベル__1） そのファイル 5 によって再現されるドキュメント（対象ドキュメント）を作成したユーザ（作成者）へそのファイル 5 の R / W 権を与えると決定する。

【 0 0 7 6 】

（レベル__2） 作成者へそのファイル 5 の R / W 権を与えると決定し、作成者と同じ部署に所属するユーザへそのファイル 5 の R 権を与えると決定する。

20

【 0 0 7 7 】

（レベル__3） 作成者へそのファイル 5 の R / W 権を与えると決定し、作成者と同じ部署に所属しまたは対象ドキュメントに類似するドキュメント（類似ドキュメント）の R / W 権もしくは R 権を有するユーザへそのファイル 5 の R 権を与えると決定する。

【 0 0 7 8 】

このように、レベルが高くなるほど、アクセス権を与える対象となるユーザの種類が増加する。

【 0 0 7 9 】

なお、権限ポリシー設定部 2 1 5 は、作成者を、そのファイル 5 のプロパティに基づいて特定する。または、そのファイル 5 に示される文書（文字列）の中から「作成者」、「著者」、「筆者」、または「作者」などの所定の単語を検索し、その所定の単語の直後に示される人が作成者であると、特定してもよい。または、そのファイル 5 に示されるドキュメントが所定のフォーマットのものである場合は、所定の位置に示される人が作成者であると、特定してもよい。

30

【 0 0 8 0 】

また、権限ポリシー設定部 2 1 5 は、作成者の所属する部署のユーザを、次のように特定する。作成者のユーザデータ 6 A（作成者のユーザコードを示すユーザデータ 6 A）に基づいて、作成者の部署を判別する。そして、その部署を示すユーザデータ 6 A を検索し、検索されたユーザデータ 6 A それぞれに示されるユーザコードのユーザが作成者の所属する部署のユーザであると、特定する。

40

【 0 0 8 1 】

また、権限ポリシー設定部 2 1 5 は、類似ドキュメントと、その R / W 権または R 権を有するユーザとを、次のように特定する。

【 0 0 8 2 】

権限ポリシー設定部 2 1 5 は、所定の規則に基づいて、対象ドキュメントの中からキーワードを抽出する。例えば、最も多く表われる単語をキーワードとして抽出してもよい。または、そのファイル 5 のファイル名に含まれる単語をキーワードとして抽出してもよい。または、対象ドキュメントが所定のフォーマットのものである場合は、対象ドキュメントの所定の位置（例えば、所定のフィールド）に示される単語をキーワードとして抽出し

50

てもよい。

【0083】

次に、権限ポリシー設定部215は、抽出したキーワードを、ドキュメント記憶領域10Rに記憶されている各ファイル5に示されるドキュメントの中から検索する。または、各ファイル5のファイル名の中から検索してもよい。そして、抽出したキーワードがヒットしたファイル5のドキュメントを類似ドキュメントとして特定する。

【0084】

そして、権限ポリシー設定部215は、類似ドキュメントのR/W権またはR権を有するユーザを、類似ドキュメントの権限ポリシーデータ6Dに基づいて特定する。

【0085】

アクセス権付与方法を決定すると、権限ポリシー設定部215は、それに従って権限ポリシーデータ6Dを生成する。

【0086】

アクセス権付与方法に関わらず、その権限ポリシーデータ6Dの各フィールドには、次の情報が示される。「ファイル名」のフィールドには、対象ドキュメントのファイル5のファイル名が示される。「R/W権」のフィールドには、作成者のユーザコードが示される。「有効期限」のフィールドには、現在から所定の時間後（例えば、4ヶ月後）の日時が示される。「更新日時」のフィールドには、現在の日時が示される。

【0087】

アクセス権付与方法をレベル__2に決定した場合は、その権限ポリシーデータ6Dの「R権」のフィールドに作成者の所属する部署のユーザ（ただし、作成者を除く）それぞれのユーザコードが、さらに示される。

【0088】

また、アクセス権付与方法をレベル__3に決定した場合は、その権限ポリシーデータ6Dの「R権」のフィールドに類似ドキュメントのR/W権またはR権を有するユーザそれぞれのユーザコードが、さらに示される。

【0089】

そして、権限ポリシー設定部215は、生成した権限ポリシーデータ6Dを権限ポリシー記憶部213に記憶させる。

【0090】

問合せデータ6Gに示されるファイル名を示す権限ポリシーデータ6Dが権限ポリシー検索部214によって検索されたが、その権限ポリシーデータ6Dが無効である場合に、権限ポリシー更新部216は、その権限ポリシーデータ6Dを更新する処理を次のように実行する。

【0091】

なお、権限ポリシー更新部216は、現在の日時が、その権限ポリシーデータ6Dに示される有効期限を過ぎており、または、その権限ポリシーデータ6Dに示される更新日時が更新日時データ6Bに示される日時よりも前である場合に、その権限ポリシーデータ6Dが無効であると、判別する。そうでない場合は、有効であると、判別する。

【0092】

権限ポリシー更新部216は、前に挙げたレベル__1、レベル__2、およびレベル__3のうちのいずれかのレベルのアクセス権付与方法によって、R/W権またはR権を与えるユーザを決定する。

【0093】

そして、権限ポリシー更新部216は、その権限ポリシーデータ6Dの各フィールドを次のように更新する。「R/W権」のフィールドを、R/W権を与えると決定したユーザのユーザコードを示すように更新し、「R権」のフィールドを、R権を与えると決定したユーザのユーザコードを示すように更新する。さらに、「有効期限」のフィールドを、現在から所定の時間後（例えば、4ヶ月後）の日時が示されるように更新し、「更新日時」のフィールドを、現在の日時を示すように更新する。

10

20

30

40

50

【 0 0 9 4 】

アクセス権特定部 2 1 7 は、問合せデータ 6 G に示されるユーザコードを有するユーザの、問合せデータ 6 G に示されるファイル名のファイル 5 のアクセス権を、次のように特定する。

【 0 0 9 5 】

アクセス権特定部 2 1 7 は、そのユーザコードが、そのファイル 5 の権限ポリシーデータ 6 D の「R / W 権」に示される場合は、そのユーザのアクセス権を R / W 権であると、特定する。「R 権」に示される場合は、そのユーザのアクセス権を R 権であると、特定する。「R / W 権」および「R 権」のいずれにも示されない場合は、そのユーザのアクセス権がないと、特定する。

10

【 0 0 9 6 】

アクセス権回答部 2 1 8 は、アクセス権特定部 2 1 7 によって特定されたアクセス権を示す回答データ 6 H をドキュメント管理サーバ 1 へ送信する。

【 0 0 9 7 】

ドキュメント管理サーバ 1 において、ファイル提供部 1 0 3 は、回答データ 6 H を受信すると、回答データ 6 H に基づいて、端末装置 3 から要求されたファイル 5 (リクエストデータ 6 F に示されるファイル名のファイル 5) を、例えば次のように端末装置 3 へ提供する。

【 0 0 9 8 】

R / W 権が回答データ 6 H に示される場合は、ファイル提供部 1 0 3 は、そのファイル 5 を、編集が可能なモードで送信する。

20

【 0 0 9 9 】

端末装置 3 において、ウェブブラウザは、そのファイル 5 に基づいてドキュメントを液晶ディスプレイ 3 0 e に表示させる。そして、ユーザがドキュメントを編集する操作を行ったら、操作の内容をドキュメント管理サーバ 1 へ送信する。すると、ファイル提供部 1 0 3 は、操作の内容に応じてそのファイル 5 を更新する。

【 0 1 0 0 】

または、R 権が回答データ 6 H に示される場合は、ファイル提供部 1 0 3 は、そのファイル 5 を、編集が不能なモード (読取専用モード) で送信する。

【 0 1 0 1 】

30

端末装置 3 において、ウェブブラウザは、そのファイル 5 に基づいてドキュメントを配置した画面を、液晶ディスプレイ 3 0 e に表示させる。ドキュメントを編集するためのユーザインタフェースは提供されない。

【 0 1 0 2 】

または、アクセス権がないことが回答データ 6 H に示される場合は、ファイル提供部 1 0 3 は、そのファイル 5 へアクセスできない旨のメッセージを端末装置 3 へ送信する。

【 0 1 0 3 】

端末装置 3 において、ウェブブラウザは、そのメッセージを受信すると、液晶ディスプレイ 3 0 e に表示させる。

【 0 1 0 4 】

40

ところで、上述の通り、権限ポリシー設定部 2 1 5 は、レベル__ 1、レベル__ 2、およびレベル__ 3 のうちのいずれかに従って、R / W 権または R 権を与えるユーザを決定する。権限ポリシー更新部 2 1 6 も、同様に決定する。ここで、決定の仕方の例を、あるファイル 5 の権限ポリシーデータ 6 D を生成し、その後、その権限ポリシーデータ 6 D を更新する場合を例に、説明する。

【 0 1 0 5 】

権限ポリシー設定部 2 1 5 は、そのファイル 5 について、アクセス権付与方法のレベルを、そのファイル 5 の重要度に応じて決定する。重要度は、そのファイル 5 に示されるドキュメントに基づいて求めることができる。例えば、そのドキュメントに含まれる特定の語句 (「社内秘」、 「機密」、 「取扱い注意」、 または 「重要」 など) の個数または割合

50

に応じて重要度を求めればよい。または、特定の語句ごとに予め重要度を定義しておき、ファイル名に含まれる特定の語句に応じて重要度を求めてもよい。

【0106】

または、権限ポリシー設定部215は、そのファイル5の重要度に関わらず、所定のレベル（例えば、レベル_1）に決定してもよい。

【0107】

そのファイル5の権限ポリシーデータ6Dが生成された後、その権限ポリシーデータ6Dを更新するタイミングが訪れると、権限ポリシー更新部216は、そのファイル5のアクセス権付与方法のレベルを、前回に決定されたレベルよりも1つ進んだレベルに決定する。例えば、前回、権限ポリシー設定部215によってレベル_1に決定された場合は、権限ポリシー更新部216は、レベル_2に決定する。

10

【0108】

さらにその後、その権限ポリシーデータ6Dを更新するタイミングが訪れると、権限ポリシー更新部216は、同様に、そのファイル5のアクセス権付与方法のレベルを、前回に決定されたレベルよりも1つ進んだレベルに決定する。例えば、前回、レベル_2に決定した場合は、レベル_3に決定する。ただし、前回、最も高いレベルに決定した場合は、今回も同じレベルに決定する。

【0109】

このように、権限ポリシー更新部216は、権限ポリシーデータ6Dを更新することにより、アクセス権を与える対象となるユーザの種類を増加させる。

20

【0110】

図7は、ドキュメント管理サーバ1における全体的な処理の流れの例を説明するフローチャートである。図8は、権限ポリシー管理サーバ21における全体的な処理の流れの例を説明するフローチャートである。

【0111】

次に、ドキュメント管理サーバ1および権限ポリシー管理サーバ21それぞれの全体的な処理の流れを、フローチャートを参照しながら説明する。

【0112】

ドキュメント管理サーバ1は、ファイル管理プログラム10Pに基づいて、図7に示す手順で処理を実行する。

30

【0113】

ドキュメント管理サーバ1は、ドキュメント記憶領域10Rのウェブページを端末装置3から要求されると（図7の#11でYes）、一覧データ6Eを端末装置3へ送信する（#12）。

【0114】

または、端末装置3からリクエストデータ6Fを受信すると、つまり、ファイル5を要求されると（#13でYes）、ドキュメント管理サーバ1は、権限ポリシー管理サーバ21へ問合せデータ6Gを送信することによって、要求元であるユーザに対して与えられている、そのファイル5のアクセス権を問い合わせる（#14）。そして、問合せに対する応答として回答データ6Hを受信する（#15）。

40

【0115】

R/W権がアクセス権として与えられていることが回答データ6Hに示される場合は（#16でYes）、ドキュメント管理サーバ1は、要求されたファイル5を編集モードで端末装置3へ提供する（#17）。

【0116】

または、R権がアクセス権として与えられていることが回答データ6Hに示される場合は（#16でNo、#18でYes）、ドキュメント管理サーバ1は、そのファイル5を読取専用モードで端末装置3へ提供する（#19）。

【0117】

または、アクセス権がない旨が回答データ6Hに示される場合は（#16でNo、#1

50

8でNo)、ドキュメント管理サーバ1は、そのファイル5へアクセスできない旨のメッセージを端末装置3へ送信する(#20)。

【0118】

ドキュメント管理サーバ1は、ファイル5の共有のサービスを提供している間、適宜、上述の処理を実行する。

【0119】

権限ポリシー管理サーバ21は、権限ポリシー管理プログラム21Pに基づいて、図8に示す手順で処理を実行する。

【0120】

ドキュメント管理サーバ1から問合せデータ6Gを受信すると(#31でYes)、その問合せデータ6Gに示されるファイル名を示す権限ポリシーデータ6Dを検索する(#32)。つまり、そのファイル名のファイル5の権限ポリシーを検索する。

10

【0121】

権限ポリシーデータ6Dが見つからない場合は(#33でNo)、権限ポリシー管理サーバ21は、そのファイル5の権限ポリシーデータ6Dを生成し記憶する(#34)。

【0122】

権限ポリシーデータ6Dが見つかった場合は(#33でYes)、権限ポリシー管理サーバ21は、その権限ポリシーデータ6Dが有効であるか無効であるかを判別する(#35)。

【0123】

その権限ポリシーデータ6Dが無効である場合は(#36でNo)、権限ポリシー管理サーバ21は、その権限ポリシーデータ6Dを更新する(#37)。

20

【0124】

権限ポリシー管理サーバ21は、問合せデータ6Gに示されるユーザコードのユーザの、そのファイル5のアクセス権を特定する(#38)。なお、ステップ#34において権限ポリシーデータ6Dを生成した場合は、この権限ポリシーデータ6Dに基づいて特定する。ステップ#37において権限ポリシーデータ6Dを更新した場合は、更新後の権限ポリシーデータ6Dに基づいて特定する。ステップ#32において権限ポリシーデータ6Dの検索に成功しかつそれが有効である場合は、この権限ポリシーデータ6Dに基づいて特定する。

30

【0125】

そして、権限ポリシー管理サーバ21は、特定したアクセス権を示すデータを回答データ6Hとしてドキュメント管理サーバ1へ送信する(#39)。

【0126】

または、ユーザ管理サーバ23から更新通知データ6Cを受信した場合は(#40でYes)、権限ポリシー管理サーバ21は、更新通知データ6Cに示される日時が示されるように、更新日時データ6Bを書き換える(#41)。

【0127】

権限ポリシー管理サーバ21は、アクセス権の問合せに対する応答のサービスを提供している間、適宜、上述の処理を実行する。

40

【0128】

本実施形態によると、ファイル5のアクセス権の、ポリシーに基づいた管理を、従来よりも容易に行うことができる。すなわち、ファイル5へのアクセスが要求された際に、そのファイル5の権限ポリシー(ユーザごとのアクセス権)を新たに設定しまたは更新する。よって、セキュリティなどに関するポリシーが新たに決められまたは変更されてたとしても、必要が生じたタイミングで、ファイル5の権限ポリシーを新たに設定しまたは、更新すればよい。

【0129】

図9~図10は、ドキュメント管理サーバ1における全体的な処理の流れの変形例を説明するフローチャートである。

50

【0130】

本実施形態では、権限ポリシー管理サーバ21は、レベル__1、レベル__2、およびレベル__3の3つのレベルの中から1つを選択したが、4つ以上のレベルのアクセス権付与方法の中から1つを選択するようにしてもよい。この場合、例えば、次のようなレベルのアクセス権付与方法を用意しておく。

【0131】

(レベル__1) 作成者へそのファイル5のR/W権を与えると決定する。

【0132】

(レベル__2) 作成者へそのファイル5のR/W権および印刷権を与えると決定し、作成者と同じ部署に所属するユーザへそのファイル5のR権を与えると決定する。

10

【0133】

(レベル__3) 作成者へそのファイル5のR/W権、印刷権、およびコピー権を与えると決定し、作成者と同じ部署に所属するユーザへそのファイル5のR/W権を与えると決定し、類似ドキュメントのR/W権またはR権を有するユーザへそのファイル5のR権を与えると決定する。

【0134】

(レベル__4) 作成者へそのファイル5のR/W権、印刷権、およびコピー権を与えると決定し、作成者と同じ部署に所属するユーザへそのファイル5のR/W権および印刷権を与えると決定し、類似ドキュメントのR/W権またはR権を有するユーザへそのファイル5のR/W権を与えると決定する。

20

【0135】

なお、「印刷権」は、そのファイル5を使用してドキュメントを印刷する権限である。「コピー権」は、そのファイル5をコピーする権限である。

【0136】

そして、権限ポリシー管理サーバ21は、4つのレベルの中から選択したレベルのアクセス権付与方法を使用して権限ポリシーデータ6Dを生成しまたは更新する。

【0137】

本実施形態では、権限ポリシー管理サーバ21は、作成者と同じ部署に所属するユーザなどへファイル5のアクセス権を付与したが、他の種類のユーザへも付与してもよい。

【0138】

例えば、権限ポリシー管理サーバ21は、作成者よりも職級が高いユーザへアクセス権を付与してもよい。または、ユーザごとに、携わっている業務に関連するキーワードを示す辞書を予め用意しておき、そのファイル5のドキュメントにキーワードが含まれるユーザへアクセス権を付与してもよい。

30

【0139】

本実施形態では、権限ポリシー管理サーバ21は、いずれのレベルにおいても作成者へアクセス権を付与したが、作成者の部署が変わった場合は、作成者へアクセス権を付与するのを中止してもよい。作成者の部署が変わったことは、ユーザ管理サーバ23が作成者のユーザデータ6Aを監視することによって、検知することができる。

【0140】

本実施形態では、権限ポリシー管理サーバ21は、あるドキュメントに類似する他のドキュメント(類似ドキュメント)をキーワードに基づいて判別したが、レイアウトに基づいて判別してもよい。例えば、そのドキュメントのレイアウトが2段組である場合は、2段組のレイアウトを有する他のドキュメントを類似ドキュメントであると判別してもよい。

40

【0141】

決定したアクセス権付与方法によってアクセス権を与えるべきユーザを特定することができない場合に、権限ポリシー管理サーバ21は、アクセス権を与えるべきユーザを管理者または作成者へ問い合わせてもよい。そして、管理者または作成者が指定したユーザへアクセス権を与えればよい。

50

【 0 1 4 2 】

権限ポリシー管理サーバ 2 1 は、あるファイル 5 のアクセス権をあるユーザへ付与した後、所定の期間、そのユーザがそのファイル 5 へアクセスしたことがない場合は、そのユーザへ与えたそのアクセス権を削除してもよい。アクセスの有無は、ログを参照して判別すればよい。

【 0 1 4 3 】

アクセス権の削除は、そのファイル 5 の要求があった際に行えばよい。具体的には、権限ポリシー管理サーバ 2 1 は、そのファイル 5 の権限ポリシーデータ 6 D を更新する際に、上述のいずれかのレベルのアクセス権付与方法によって、アクセス権を与えるユーザを決定する。決定したユーザの中から、以前にそのファイル 5 のアクセス権を与えたことがあるが、現在まで所定の期間以上、そのファイル 5 へアクセスしたことがないユーザを判別する。そして、判別してユーザを、決定したユーザから除外して、権限ポリシーデータ 6 D を更新する。

10

【 0 1 4 4 】

権限ポリシー管理サーバ 2 1 は、権限ポリシーデータ 6 D を生成しまたは更新する前に、アクセス権を与えるユーザを管理者または作成者へ通知してもよい。そして、管理者または作成者が許可した場合に、その権限ポリシーデータ 6 D を生成しまたは更新してもよい。

【 0 1 4 5 】

本実施形態では、ファイル 5 として、ドキュメントを再現するためのファイルを例に説明したが、音声または動画像を再生するためのファイルを用いる場合にも、本発明を適用することができる。

20

【 0 1 4 6 】

本実施形態では、図 5 に示す機能をドキュメント管理サーバ 1、権限ポリシー管理サーバ 2 1、およびユーザ管理サーバ 2 3 に分散して実現したが、ドキュメント管理サーバ 1 に集約してもよい。

【 0 1 4 7 】

この場合は、ファイル管理プログラム 1 0 P の代わりにファイル管理プログラム 1 0 Q をドキュメント管理サーバ 1 の ROM 1 0 c または大容量記憶装置 1 0 d に記憶させておく。

30

【 0 1 4 8 】

そして、ドキュメント管理サーバ 1 は、ファイル管理プログラム 1 0 Q に基づいて、図 9 ~ 図 1 0 に示す手順で処理を実行する。

【 0 1 4 9 】

ドキュメント管理サーバ 1 は、ドキュメント記憶領域 1 0 R のウェブページを端末装置 3 から要求されると (図 9 の # 5 1 で Y e s)、一覧データ 6 E を端末装置 3 へ送信する (# 5 2)。

【 0 1 5 0 】

または、端末装置 3 からリクエストデータ 6 F を受信すると (# 5 3 で Y e s)、ドキュメント管理サーバ 1 は、リクエストデータ 6 F に示されるファイル名を示す権限ポリシーデータ 6 D を検索する (# 5 4)。

40

【 0 1 5 1 】

権限ポリシーデータ 6 D が見つからない場合は (# 5 5 で N o)、ドキュメント管理サーバ 1 は、そのファイル 5 の権限ポリシーデータ 6 D を生成し記憶する (# 5 6)。

【 0 1 5 2 】

権限ポリシーデータ 6 D が見つかった場合は (# 5 5 で Y e s)、ドキュメント管理サーバ 1 は、その権限ポリシーデータ 6 D が有効であるか無効であるかを判別する (# 5 7)。

【 0 1 5 3 】

その権限ポリシーデータ 6 D が無効である場合は (# 5 8 で N o)、ドキュメント管理

50

サーバ 1 は、その権限ポリシーデータ 6 D を更新する (# 5 9) 。

【 0 1 5 4 】

ドキュメント管理サーバ 1 は、リクエストデータ 6 F に示されるユーザコードのユーザの、そのファイル 5 のアクセス権を特定する (# 6 0) 。特定に使用する権限ポリシーデータ 6 D は、図 8 のステップ # 3 8 で使用する権限ポリシーデータ 6 D と同様である。

【 0 1 5 5 】

特定したアクセス権が R / W 権である場合は (図 1 0 の # 6 1 で Y e s) 、ドキュメント管理サーバ 1 は、要求されたファイル 5 を編集モードで端末装置 3 へ提供する (# 6 2) 。

【 0 1 5 6 】

特定したアクセス権が R 権である場合は (# 6 1 で N o 、 # 6 3 で Y e s) 、ドキュメント管理サーバ 1 は、そのファイル 5 を読取専用モードで端末装置 3 へ提供する (# 6 4) 。

【 0 1 5 7 】

アクセス権がない場合は (# 6 1 で N o 、 # 6 3 で N o) 、ドキュメント管理サーバ 1 は、そのファイル 5 へアクセスできない旨のメッセージを端末装置 3 へ送信する (# 6 5) 。

【 0 1 5 8 】

または、ユーザデータ 6 A が更新されたことを検知した場合は (# 6 6 で Y e s) 、ドキュメント管理サーバ 1 は、更新された日時が示されるように、更新日時データ 6 B を書き換える (# 6 7) 。

【 0 1 5 9 】

ドキュメント管理サーバ 1 は、ファイル 5 の共有のサービスを提供している間、適宜、上述の処理を実行する。

【 0 1 6 0 】

その他、ドキュメント共有システム 1 0 0 、ドキュメント管理サーバ 1 。権限ポリシー管理サーバ 2 1 、ユーザ管理サーバ 2 3 の全体または各部の構成、処理の内容、処理の順序、データの構成などは、本発明の趣旨に沿って適宜変更することができる。

【 符号の説明 】

【 0 1 6 1 】

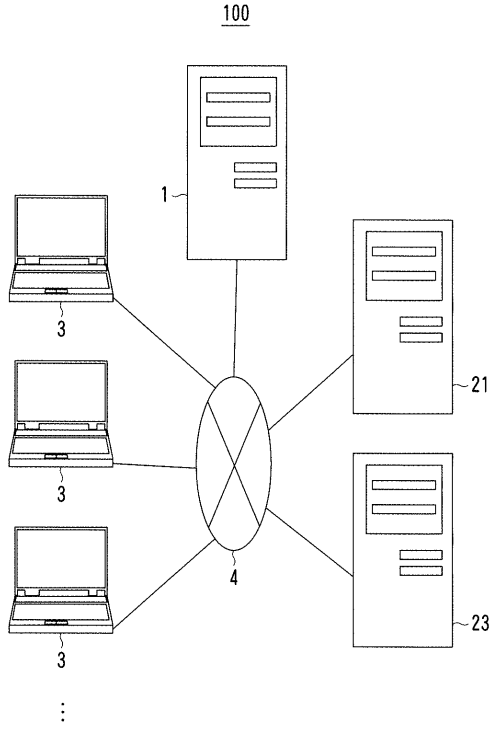
- 1 0 0 ドキュメント共有システム (データ提供システム)
- 1 0 3 ファイル提供部 (提供手段)
- 1 0 R ドキュメント記憶領域 (保存手段)
- 2 1 権限ポリシー管理サーバ (アクセス権管理装置)
- 2 1 5 権限ポリシー設定部 (解析手段、設定手段)
- 2 1 6 権限ポリシー更新部 (更新手段)
- 5 ファイル (データ)
- 6 D 権限ポリシーデータ

10

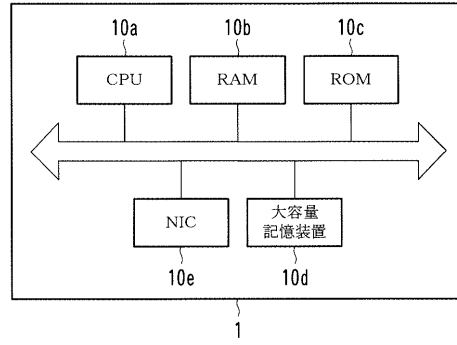
20

30

【 図 1 】



【 図 2 】



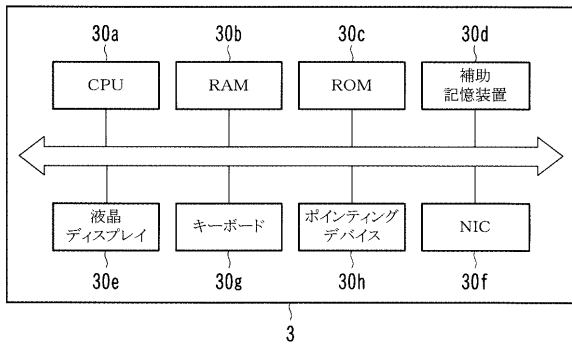
【 図 3 】

23R

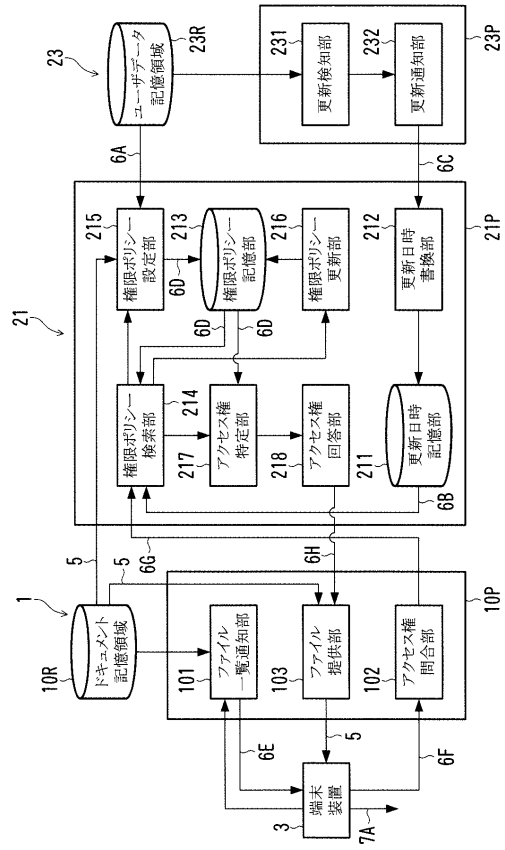
ユーザコード	部署	職級	連絡先	...
A001	営業部	部長	a001@example.com	...
A002	経理部	課長	a002@example.com	...
A003	人事部	一般社員	a003@example.com	...
A004	営業部	一般社員	a004@example.com	...
A005	人事部	部長	a005@example.com	...
...

6A
6A
6A
6A
6A

【 図 4 】



【 図 5 】

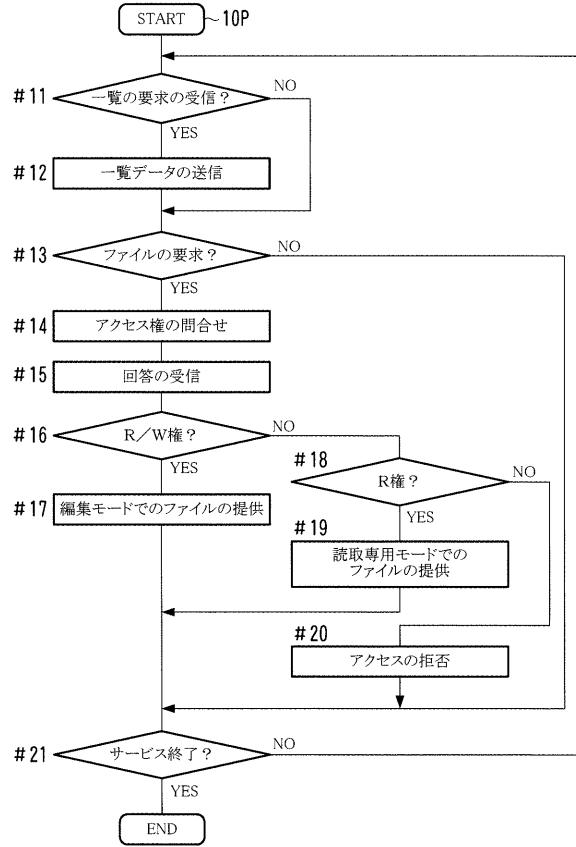


【 図 6 】

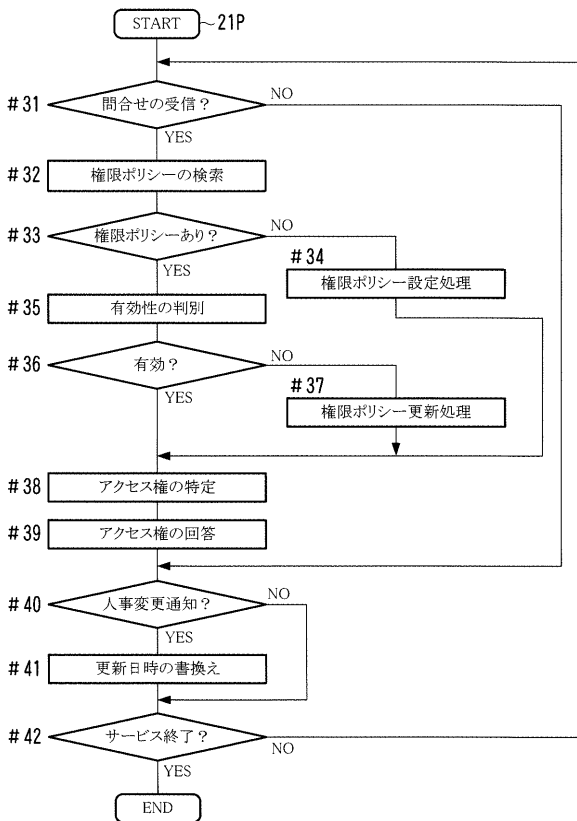
ファイル名	R/W権	更新日時	有効期限
001.pdf	A004	2016/3/4 11:00	2016/7/4 11:00
002.doc	A012,A015	2016/3/2 9:30	2016/3/2 9:30
005.pdf	A021,A025	2016/2/28 14:15	2016/6/28 14:15

213

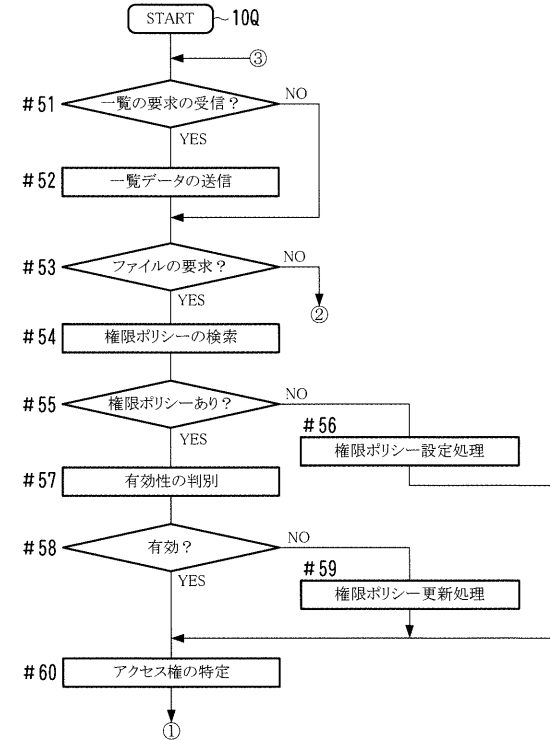
【 図 7 】



【 図 8 】



【 図 9 】



【図 10】

