(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5072314号
(P5072314)
(45)発行日　平成24年11月14日(2012.11.14)　(24)登録日　平成24年8月31日(2012.8.31)

(51)Int.Cl.　　F I
G06F 12/00 (2006.01)　　G06F 12/00 537A
G06F 17/21 (2006.01)　　G06F 17/21 570M

請求項の数 16　(全 25 頁)

(21)出願番号　特願2006-286886 (P2006-286886)
(22)出願日　平成18年10月20日 (2006.10.20)
(65)公開番号　特開2008-102871 (P2008-102871A)
(43)公開日　平成20年5月1日 (2008.5.1)
審査請求日　平成21年10月20日 (2009.10.20)

(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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　平原　晶子
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

最終頁に続く

(54)【発明の名称】文書管理システム、文書管理方法、文書管理プログラム、記憶媒体

(57)【特許請求の範囲】
【請求項１】
ファイルに対するアクセスを管理する文書管理システムであって、
前記ファイルに設定する、デバイス毎に準備された仮想セキュリティポリシーを選択する選択手段と、
前記選択手段により選択された仮想セキュリティポリシーと、当該仮想セキュリティポリシーを設定した設定者の認証情報とにより、前記ファイルに対するアクセスが可能な権限を定めるアクセス権限情報を取得する取得手段と、
前記取得手段により取得された前記アクセス権限情報により、前記仮想セキュリティポリシーを、前記文書管理システムで共通に解釈可能であり、前記仮想セキュリティポリシーを設定した設定者の権限と前記設定者以外に適用されるべき権限とが含まれる実セキュリティポリシーに変換する変換手段と、
前記変換手段により変換された前記実セキュリティポリシーを前記ファイルに設定し、当該ファイルへのアクセスを管理する管理手段と、
を備えることを特徴とする文書管理システム。
【請求項２】
前記実セキュリティポリシーが設定された前記ファイルに対するアクセス権限の有無を、前記ファイルにアクセスする者の認証情報により判定するアクセス権限判定手段を更に備えることを特徴とする請求項１に記載の文書管理システム。
【請求項３】

前記管理手段は、前記アクセス権限判定手段の判定結果により、前記ファイルへのアクセスを制限することを特徴とする請求項２に記載の文書管理システム。
【請求項４】
前記取得手段が取得する前記アクセス権限情報には、前記ファイルに対するアクセスの種類を定める情報と、前記ファイルに対するアクセスが制限されるユーザグループの情報が含まれることを特徴とする請求項１に記載の文書管理システム。
【請求項５】
前記ユーザグループの情報を保存するユーザグループ情報保存手段を更に備え、
前記取得手段は前記仮想セキュリティポリシーを設定した設定者の認証情報により、前記ユーザグループ情報保存手段から前記ユーザグループの情報を取得し、
前記変換手段は、前記取得手段により取得された前記ユーザグループの情報により、前記仮想セキュリティポリシーを前記実セキュリティポリシーに変換することを特徴とする請求項４に記載の文書管理システム。
【請求項６】
前記選択手段により選択された前記仮想セキュリティポリシーを前記ファイルに設定して保存するファイル保存手段と、
前記ファイル保存手段に保存されている前記ファイルに対してアクセスが要求されたか判定するアクセス要求判定手段と、
前記アクセス要求判定手段の判定により、前記ファイルに対してアクセスが要求された場合、前記取得手段に対してポリシー変換要求を送信する送信手段を更に備え、
前記取得手段は、前記送信手段から送信された前記ポリシー変換要求により、前記アクセス権限情報を取得し、
前記変換手段は、前記ポリシー変換要求により取得された前記アクセス権限情報に基づいて前記仮想セキュリティポリシーを前記実セキュリティポリシーに変換することを特徴とする請求項１に記載の文書管理システム。
【請求項７】
前記選択手段と、前記取得手段と、前記変換手段とは、前記文書管理システムを構成する同一のデバイス上に構成されることを特徴とする請求項１に記載の文書管理システム。
【請求項８】
ファイルに対するアクセスを管理する文書管理システムにおける文書管理方法であって、
選択手段が、前記ファイルに設定する、デバイス毎に準備された仮想セキュリティポリシーを選択する選択工程と、
取得手段が、前記選択工程により選択された仮想セキュリティポリシーと、当該仮想セキュリティポリシーを設定した設定者の認証情報とにより、前記ファイルに対するアクセスが可能な権限を定めるアクセス権限情報を取得する取得工程と、
変換手段が、前記取得工程により取得された前記アクセス権限情報により、前記仮想セキュリティポリシーを、前記文書管理システムで共通に解釈可能であり、前記仮想セキュリティポリシーを設定した設定者の権限と前記設定者以外に適用されるべき権限とが含まれる実セキュリティポリシーに変換する変換工程と、
管理手段が、前記変換工程により変換された前記実セキュリティポリシーを前記ファイルに設定し、当該ファイルへのアクセスを管理する管理工程と、
を有することを特徴とする文書管理方法。
【請求項９】
アクセス権限判定手段が、前記実セキュリティポリシーが設定された前記ファイルに対するアクセス権限の有無を、前記ファイルにアクセスする者の認証情報により判定するアクセス権限判定工程を更に有することを特徴とする請求項８に記載の文書管理方法。
【請求項１０】
前記管理工程では、前記アクセス権限判定工程の判定結果により、前記ファイルへのアクセスを制限することを特徴とする請求項９に記載の文書管理方法。

【請求項１１】
前記取得工程が取得する前記アクセス権限情報には、前記ファイルに対するアクセスの種類を定める情報と、前記ファイルに対するアクセスが制限されるユーザグループの情報が含まれることを特徴とする請求項８に記載の文書管理方法。
【請求項１２】
ユーザグループ情報保存手段が、前記ユーザグループの情報をユーザグループ情報保存手段に保存するユーザグループ情報保存工程を更に有し、
前記取得工程では前記仮想セキュリティポリシーを設定した設定者の認証情報により、前記ユーザグループ情報保存手段から前記ユーザグループの情報を取得し、
前記変換工程では、前記取得工程により取得された前記ユーザグループの情報により、前記仮想セキュリティポリシーを前記実セキュリティポリシーに変換することを特徴とする請求項１１に記載の文書管理方法。
【請求項１３】
ファイル保存手段が、前記選択工程により選択された前記仮想セキュリティポリシーを前記ファイルに設定してファイル保存手段に保存するファイル保存工程と、
アクセス要求判定手段が、前記ファイル保存手段に保存されている前記ファイルに対してアクセスが要求されたか判定するアクセス要求判定工程と、
送信手段が、前記アクセス要求判定工程の判定により、前記ファイルに対してアクセスが要求された場合、前記取得工程に対してポリシー変換要求を送信する送信工程を更に有し、
前記取得工程では、前記送信工程から送信された前記ポリシー変換要求により、前記アクセス権限情報を取得し、
前記変換工程では、前記ポリシー変換要求により取得された前記アクセス権限情報に基づいて前記仮想セキュリティポリシーを前記実セキュリティポリシーに変換することを特徴とする請求項８に記載の文書管理方法。
【請求項１４】
前記選択工程の処理と、前記取得工程の処理と、前記変換工程の処理とは、前記文書管理システムを構成する同一のデバイス上において実行されることを特徴とする請求項８に記載の文書管理方法。
【請求項１５】
請求項８乃至１４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文書管理プログラム。
【請求項１６】
請求項１５に記載の文書管理プログラムを格納したことを特徴とするコンピュータ可読の記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はファイルに対するアクセスを管理する文書管理技術に関するものである。
【背景技術】
【０００２】
近年、情報セキュリティに関する意識の高まりと共に、企業などにおいては、個人情報保護法や知的財産の保護の観点により、情報漏洩の防止対策が求められている。そのため、電子文書に特定のユーザに対するアクセス権限や使用権限のコントロールをセキュリティポリシー(以下、「ポリシー」と記す)として、設定することによって、情報漏洩を防止することができるシステムが提供されている。
【０００３】
一例として、近年、アクセス制御管理サーバが市場に登場しており、個々のユーザに対する各種アクセス制御を、アクセス制御管理サーバを介して、ファイルに設定することができる。また、ファイル作成者は配布ファイルに対して、ユーザ個々に対し、詳細レベル

を指定してアクセス制御が可能となっている。
【０００４】
具体的なアクセス制御管理サーバの例としては、Ａｄｏｂｅ社がＬｉｖｅ Ｃｙｃｌｅ Ｐｏｌｉｃｙ Ｓｅｒｖｅｒを発表し、ＰＤＦファイルに対して前述したようなアクセス制御を可能にしている。また、Ｍｉｃｒｏｓｏｆｔ社はＲｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ Ｓｅｒｖｉｃｅｓを発表し、Ｍｉｃｒｏｓｏｆｔ製のＯｆｆｉｃｅアプリケーションに対して前述したようなアクセス制御を可能にしている。
【０００５】
アクセス制御管理サーバに登録されるポリシーのアクセス権限は、ユーザまたはグループ単位、時間単位、ネットワーク/ドメイン単位で設定が可能である。使用権限としては、印刷、転記の可否が設定可能になっている。また、文書配信後にも権限の剥奪・変更などがアクセス制御管理サーバ側で容易に実行することも可能である。
【０００６】
アクセス制御管理サーバに登録されるポリシーは、管理者が登録を行い、一般ユーザは自分が設定可能な一覧を取得し、利用するだけであるのが一般的である。一般ユーザが文書に対してポリシーを適用する場合は、アクセス制御管理サーバから設定可能なポリシーの一覧を取得し、一覧表示から指定する方法も行われている。
【０００７】
また、ネットワークに接続されたスキャナや、スキャナ機能を備えた複合機から読み取った画像データは電子メールに添付して、クライアントコンピュータに送信することが多く行われている。しかし、この送信データ形式は一般的なものであり、上記の電子文書同様、セキュリティ面で問題がある。
【０００８】
このため、上記のスキャナや、スキャナ機能を備えた複合機等のデバイスから読み込んだ画像データについてもセキュリティを適用する方法が提案されており、上記同様、アクセス制御管理サーバを利用する方法も提案されている。
【０００９】
特許文献１は、画像データをネットワーク上に出力する際にセキュリティ情報をデータに関連付ける方法を開示しており、電子文書作成と同時にセキュリティ情報を付加することができる。
【００１０】
特許文献２は、原稿画像を読み込む際に所定のフォーマットのアクセス制限情報入力シートを同時に読み込ませ、読み込んだシートの解析を行うことによりアクセス制限情報の生成を行う方法を開示している。この方法によると、操作パネルにより設定を行う必要がない。しかし、所定のフォーマットへ所望の設定を記入したりシートを読み込ませたりする必要がある。
【特許文献１】特開２００３－３０４３５２号公報
【特許文献２】特開２００３－２８１１４８号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
しかしながら、従来のアクセス制御管理サーバからポリシー一覧を取得し、選択する方法では、ポリシー設定項目が固定的で、一般ユーザは管理者が登録したポリシーしか利用できず、カスタマイズすることが不能である。
【００１２】
また、特に、デバイスに関しては、アクセス制御情報を指定するにあたり、デバイスの操作パネルを用いて設定する必要がある。ここでデバイスの操作パネルは一般的に小さく、アクセス制御に関し、詳細な設定を行わせるのは困難であり、操作性に問題がある。
【００１３】
ここで、上述のように、ユーザ毎にアクセス制御管理サーバから設定可能なポリシーの

一覧を取得し、この一覧表示から指定する方法を考察する。この場合、アクセス制御管理サーバに保存されているポリシーの粒度により詳細なアクセス制御の指定が可能である。

【００１４】

しかし、この一覧表示するデータ量が多くなると操作性が低下する。また、デバイスに限らず、ユーザのＰＣ上でも、同様の問題がある。ここで、ユーザ毎にアクセス制御管理サーバから選択可能なポリシーの一覧を取得し、ポリシー選択メニューを可変的（動的）に生成する場合について考察する。この場合、ネットワーク環境によっては、ユーザ毎に選択可能なポリシーのリストを生成するのに時間がかかり、ＵＩ表示に時間がかかる。ユーザ毎に動的に生成せず、全ポリシーのリストを取得し、表示するという方法もあるが、登録ポリシー数が多い場合には、ユーザが指定したいポリシーを見つけるのが困難である。

【００１５】

更に、従来のアクセス制御管理サーバに接続して、ポリシー一覧を取得する方法について考察する。この場合、アクセス制御管理サーバと接続できない環境では、文書にアクセス制御管理サーバに登録されたポリシーを設定することが不可能である。また、通信エラー等の場合は、ユーザは通信が回復してから、再度、ポリシー選択を行う必要があった。

【００１６】

本発明は上記の問題点を解消するためになされたもので、ポリシー選択メニューのカスタマイズを可能にし、ユーザの使用環境に応じたポリシーの設定で文書管理を行うことを一つの目的とする。

【００１７】

あるいは、ポリシー選択メニューを簡明にすることで、ユーザの選択を容易にし、ユーザの利便性を向上させることを一つの目的とする。

【００１８】

あるいは、ポリシー選択メニューを共通化することにより、メニュー表示の高速化を図ることを一つの目的とする。

【００１９】

あるいは、アクセス制御管理サーバと通信不能の場合にも、ポリシーを選択することを可能にして、ユーザによるポリシーの再選択の手間を省略することを一つの目的とする。

【課題を解決するための手段】

【００２０】

上記のいずれかの目的を達成する、本発明に係る文書管理システムは、ファイルに対するアクセスを管理する文書管理システムであって、

前記ファイルに設定する、デバイス毎に準備された仮想セキュリティポリシーを選択する選択手段と、

前記選択手段により選択された仮想セキュリティポリシーと、当該仮想セキュリティポリシーを設定した設定者の認証情報とにより、前記ファイルに対するアクセスが可能な権限を定めるアクセス権限情報を取得する取得手段と、

前記取得手段により取得された前記アクセス権限情報により、前記仮想セキュリティポリシーを、前記文書管理システムで共通に解釈可能であり、前記仮想セキュリティポリシーを設定した設定者の権限と前記設定者以外に適用されるべき権限とが含まれる実セキュリティポリシーに変換する変換手段と、

前記変換手段により変換された前記実セキュリティポリシーを前記ファイルに設定し、当該ファイルへのアクセスを管理する管理手段と、

を備えることを特徴とする。

【００２１】

上記のいずれかの目的を達成する、本発明に係る文書管理方法は、ファイルに対するアクセスを管理する文書管理システムにおける文書管理方法であって、

選択手段が、前記ファイルに設定する、デバイス毎に準備された仮想セキュリティポリシーを選択する選択工程と、

取得手段が、前記選択工程により選択された仮想セキュリティポリシーと、当該仮想セキュリティポリシーを設定した設定者の認証情報とにより、前記ファイルに対するアクセスが可能な権限を定めるアクセス権限情報を取得する取得工程と、

変換手段が、前記取得工程により取得された前記アクセス権限情報により、前記仮想セキュリティポリシーを、前記文書管理システムで共通に解釈可能であり、前記仮想セキュリティポリシーを設定した設定者の権限と前記設定者以外に適用されるべき権限とが含まれる実セキュリティポリシーに変換する変換工程と、

管理手段が、前記変換工程により変換された前記実セキュリティポリシーを前記ファイルに設定し、当該ファイルへのアクセスを管理する管理工程と、

を有することを特徴とする。

【発明の効果】

【００２２】

本発明によれば、ポリシー選択メニューのカスタマイズが可能になり、ユーザの使用環境に応じたポリシーの設定で文書管理をすることができる。

【００２３】

あるいは、本発明に拠れば、ポリシー選択メニューが簡明になることで、ユーザの選択が容易になり、ユーザの利便性を向上することができる。

【００２４】

あるいは、本発明に拠れば、ポリシー選択メニューを共通化することにより、メニュー表示が高速化するという効果が得ることができる。

【００２５】

あるいは、本発明に拠れば、アクセス制御管理サーバと通信不能の場合にも、ポリシー選択が可能であるため、ユーザによるポリシーの再選択を省略できるという効果が得られる。

【発明を実施するための最良の形態】

【００２６】

以下に、図面を参照して、本発明の好適な実施形態を例示的に詳しく説明する。ただし、この実施の形態に記載されている構成要素はあくまで例示であり、この発明の範囲をそれらのみに限定する趣旨のものではない。

【００２７】

（第１実施形態）

（文書管理システムの構成）

図１は、本発明の実施形態に係る文書管理システムの構成を説明するブロック図である。１０１、１０２はコンピュータ（情報処理装置）であり、１０７のイーサネット（登録商標）などのネットワークケーブルやネットワーク或いは公衆回線などによって、LAN/WAN/インターネット等のネットワークに接続されている。コンピュータ１０１、１０２はアプリケーションプログラム等の各種のプログラムを実行することが可能である。コンピュータ１０１、１０２は文書にアクセス制御情報（＝セキュリティポリシー）を設定及びアクセス制御情報が設定されている文書を参照するプログラムを搭載している。また、図１では複数台のコンピュータを記載してあるが、１台でも複数台でもよい。

【００２８】

１０３は本実施形態のアクセス制御管理サーバとしての情報処理装置であり、アクセス制御管理サーバ１０３はネットワーク１０７に接続されている。

【００２９】

１０４は印刷制御装置、スキャナ、コピー機能等を持った複合機（ＭＦＰ）として機能する画像形成装置である。画像形成装置１０４はネットワーク１０７に接続されており、操作部、表示部等を持つものは、本発明の実施形態に係るアクセス制御情報の設定が可能である。

【００３０】

尚、本発明の趣旨は、文書管理システムを構成する画像形成装置１０４を、複合機（M

ＦＰ）に限定するものではなく、スキャナなどのデバイスが単体でネットワーク１０７に接続されていても良いことは言うまでもない。

【００３１】

１０５は本実施形態のアクセス制御情報を生成するにあたり、ポリシー設定者のユーザ情報検索用ディレクトリサービスを提供するディレクトリサーバとして機能する情報処理装置である。ディレクトリサーバ１０５はネットワーク１０７に接続されている。尚、ディレクトリサーバ１０５は本実施形態のユーザ情報検索用サービスを提供するサーバとして記載しているが、文書管理システムの機能を実現するために必須のものではない。ディレクトリサーバ１０５がない場合は、本発明の実施形態に係るユーザ情報はアクセス制御管理サーバ１０３、ネットワーク１０７上の保存装置、デバイスのハードディスク等に保存される。

【００３２】

１０６は本実施形態の文書を格納するドキュメントサーバとしての情報処理装置であり、ネットワーク１０７に接続されている。尚、ドキュメントサーバ１０６は本実施形態の文書を保存するドキュメントサーバとして記載しているが、文書管理システムの機能を実現するために必須のものではない。ドキュメントサーバ１０６がない場合は、本発明の実施形態に係る文書はユーザ所有のコンピュータ１０１、１０２やファイルサーバ、ネットワーク１０７上の保存装置、デバイスのハードディスク等に保存される。

【００３３】

文書管理システムを構成するコンピュータ１０１、１０２とアクセス制御管理サーバ１０３、ディレクトリサーバ１０５、ドキュメントサーバ１０６は、一般的な情報処理装置により構成することが可能である。コンピュータ１０１、１０２、アクセス制御管理サーバ１０３、ディレクトリサーバ１０５、ドキュメントサーバ１０６、ＭＦＰ１０４にアクセス制御情報設定処理を行うプログラムを実行可能にインストールすることが可能である。

【００３４】

（情報処理装置の構成）

図２は、本発明の実施形態に係るコンピュータ（情報処理装置）の構成を説明するブロック図である。情報処理装置であるコンピュータ１０１、１０２、アクセス制御管理サーバ１０３、ディレクトリサーバ１０５、ドキュメントサーバ１０６は同様あるいは同等のハードウエア構成を有する。従ってイ、コンピュータ、アクセス制御管理サーバ、ディレクトリサーバ、ドキュメントサーバの構成を説明するブロック図として説明する。

【００３５】

図２において、２００は情報処理装置の制御手段であるＣＰＵである。ＣＰＵではハードディスク（ＨＤ）２０５に格納されているアプリケーションプログラム、ＯＳや本発明の文書管理プログラム等を実行する。更に、ＲＡＭ２０２にプログラムの実行に必要な情報、ファイル等を一時的に格納する制御を行う。

【００３６】

２０１は記憶手段であるＲＯＭであり、内部には、基本Ｉ／Ｏプログラム等のプログラムを記憶する。２０２は一時記憶手段であるＲＡＭであり、ＣＰＵ２００の主メモリ、ワークエリア等として機能する。

【００３７】

２０３は記憶媒体読み込み手段としてのフレキシブルディスク（ＦＤ）ドライブである。後述する図６に示すようにＦＤドライブ２０３を通じて記憶媒体としてのＦＤ２０４に記憶されたプログラム等をコンピュータシステムにロードすることができる。なお、記憶媒体は、ＦＤに限らず、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＰＣカード、ＤＶＤ、ＩＣメモリカード、ＭＯ、メモリスティック等を利用することができる。

【００３８】

２０４は記憶媒体であるフレキシブルディスク（ＦＤ）であり、コンピュータが読み取り可能なプログラムが格納された記憶媒体である。

【００３９】
２０５は外部記憶手段の一つであり、大容量メモリとして機能するハードディスク（ＨＤ）であり、アプリケーションプログラム、ＯＳ、文書管理プログラム、関連プログラム等を格納している。
【００４０】
２０６は指示入力手段であるキーボードであり、ユーザがコンピュータに対して、ポリシー選択指示など、ユーザ操作の各種指示を入力することが可能である。
【００４１】
２０７は表示手段であるディスプレイであり、設定画面、取得情報等を表示することが可能である。
【００４２】
２０８はシステムバスであり、コンピュータ、サーバ内のデータの流れを司るものである。
【００４３】
２０９は入出力手段であるインタフェースであり、インタフェース２０９を介してコンピュータ（情報処理装置）は外部装置とのデータのやり取りを行うことが可能である。
【００４４】
（画像形成装置の構成）
図３は、本発明の実施形態に係る画像形成装置であるＭＦＰ１０４の構成を説明するブロック図である。
【００４５】
図３において、３００は画像形成装置の制御手段であるＣＰＵである。ＣＰＵ３００はハードディスク（ＨＤ）３０５に格納されている各種制御プログラム、アプリケーションプログラム、ＯＳや本発明の文書管理プログラム等を実行する。更に、ＣＰＵ３００はＲＡＭ３０２にプログラムの実行に必要な情報、ファイル等を一時的に格納する制御を行う。
【００４６】
３０１は記憶手段であるＲＯＭであり、内部には、機器制御プログラム、基本Ｉ／Ｏプログラム等のプログラムを記憶する。３０２は一時記憶手段であるＲＡＭであり、ＣＰＵ３００の主メモリ、ワークエリア等として機能する。
【００４７】
３０３は記憶媒体読み込み手段としてのカードスロットであり、カードスロット３０３を通じて記憶媒体としてのメモリカード３０４に記憶されたプログラム等を画像形成装置上にロードすることや、文書ファイル（データ）を取得することができる。尚、記憶媒体は、メモリカードに限らず、ＦＤ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＰＣカード、ＤＶＤ、ＩＣメモリカード、ＭＯ、メモリスティック等、を利用することができる。
【００４８】
３０４は記憶媒体であるメモリカードであり、コンピュータが読み取り可能なプログラムが格納された記憶媒体である。
【００４９】
３０５は外部記憶手段の一つであり、大容量メモリとして機能するハードディスク（ＨＤ）であり、アプリケーションプログラム、ＯＳ、文書管理プログラム、関連プログラム等を格納している。
【００５０】
３０６は指示入力手段であるキーボードであり、ユーザが画像形成装置に対して、ポリシー選択指示など、ユーザ操作の各種指示を入力することが可能である。
【００５１】
３０７は表示手段であるディスプレイであり、設定画面、取得情報等を表示することが可能である。
【００５２】

３０８はシステムバスであり、画像形成装置内のデータの流れを司るものである。
【００５３】
３０９は入出力手段であるインタフェースであり、インタフェース３０９を介して画像形成装置は外部装置とのデータのやり取りを行うことが可能である。
【００５４】
３１０はスキャン部であり、スキャン部２１０を介して、紙文書からデータをスキャン、即ち、原稿に照射した光の画像に応じた反射光を光電変換して画像データを読み取ることができる。画像形成装置はＲＡＭ３０２をワークエリアとして画像を形成し、ＨＤ３０５に形成した画像を文書として保存することができる。
【００５５】
（メモリマップの説明)
図４は、図２、図３で示したコンピュータ（情報処理装置）、画像形成装置におけるメモリマップメモリマップ４００の一例を示す図である。４０１は基本Ｉ／Ｏプログラムであり、コンピュータ、画像形成装置の電源がＯＮされたときに、ＨＤ２０５、３０５からＯＳがＲＡＭ２０２、３０２に読み込まれる。ＯＳの動作を開始させるＩＰＬ（イニシャルプログラムローデイング）機能などを有しているプログラムが入っている領域である。
【００５６】
４０２はオペレーティングシステム（ＯＳ）であり、４０３は文書管理プログラムであり、ＲＡＭ２０２、３０２上に確保される領域に記憶される。４０４は関連データであり、ＲＡＭ２０２、３０２上に確保される領域に記憶される。４０５はワークエリアであり、ＣＰＵ２００、３００が文書管理プログラムを実行する領域が確保されている。
【００５７】
図５は、図２に示したＦＤ２０４のメモリマップの一例を示す図である。図５において、５００はＦＤ２０４のデータ内容であり、５０１はデータの情報を示すボリューム情報であり、５０２はディレクトリ情報、５０３は本実施形態で説明する文書管理プログラム、５０４はその関連データである。
【００５８】
図６は、図２に示したＦＤドライブ２０３に対して挿入されるＦＤ２０４との関係を示す図であり、図２と同一のものには同一の符号を付してある。図６において、ＦＤ２０４には、本実施形態で説明する文書管理プログラムおよび関連データが格納されている。
【００５９】
（文書管理処理）
図７は、本実施形態に係る文書管理システムの処理の流れを概略的に示す図である。図７では、特に、ＭＦＰ１０４で原稿をスキャンし、読み込んだデータ（ファイル）にアクセス制御情報を適用し、ＭＦＰ１０４のハードディスク（ＨＤ）３０５に保存する例を図示している。また、図７においては図１で説明した文書管理システムと同様の記号を使用している。
【００６０】
ＭＦＰ１０４において、文書管理プログラムが作動しており、ユーザはＭＦＰ１０４の表示部３０７に表示されたＵＩ(ユーザインターフェース)画面で、認証、仮想ポリシー選択などの各種操作を行うことが可能である。ここで、「仮想ポリシー」とは、コンピュータ、あるいはＭＦＰ等のデバイス毎に共通に準備されている仮のセキュリティポリシーである。仮想ポリシーは、コンピュータ、あるいはＭＦＰ等のユーザ毎にカスタマイズされたセキュリティポリシーである。
【００６１】
また、「実ポリシー」とは、本発明の実施形態に係る文書管理システムまたは文書管理プログラムで共通に解釈可能なセキュリティポリシーをいう。文書管理システムまたは文書管理プログラムで管理されているアクセス権の情報（ファイルに対するアクセスを制限する情報）に基づいて、仮想ポリシーは文書管理システム等で共通に解釈可能な実ポリシーに変換される。アクセス権の情報には、例えば、編集、閲覧等を制限する情報の他、仮

想ポリシーを設定した設定者の認証情報に基づいて、アクセス可能な範囲（アクセスが認められる（あるいは制限される）グループや部署、会社等）の情報が含まれる。

【００６２】

また、画像形成装置（ＭＦＰ）１０４のスキャン部３１０は原稿を読み取り、ＣＰＵ３００はユーザにより選択された仮想ポリシーをスキャン部３１０が読み取った原稿の画像データ（ファイル）に設定する。

【００６３】

ＭＦＰ１０４のＣＰＵ３００は、ポリシー変換要求をアクセス制御管理サーバ１０３に送信する。アクセス制御管理サーバ１０３はＭＦＰ１０４からのポリシー変換要求を受けて、仮想ポリシーを実ポリシーに変換し、変換した実ポリシーをＭＦＰ１０４に返信する。ディレクトリサーバ１０５にはユーザ情報が格納され、アクセス制御管理サーバ１０３からのユーザ情報及びグループ情報の問い合わせに対し、適宜情報を返信することが可能である。

【００６４】

閲覧者（編集を行う編集者でもよい）がコンピュータ１０１を介して、ＭＦＰ１０４に保存されたファイルに対し閲覧要求を行う場合、閲覧(或いは編集)に際しては、アクセス制御管理サーバ１０３に問い合わせが実施される。アクセス制御管理サーバ１０３は、問合せに対してＭＦＰ１０４に保存されたファイルに対する閲覧に関してアクセスの認証を行う。

【００６５】

データの保存先として、図７の例ではＭＦＰ１０４のハードディスク３０５を示したが、ネットワーク１０７の共有フォルダ、ドキュメントサーバ１０６、ファイルサーバ等、任意のストレージ装置に保存することが可能である。

【００６６】

原稿をスキャンして任意のストレージ装置（記憶領域）に保存する機能は、以降、「スキャン保存機能」と記載する。また、ＭＦＰ１０４上でアクセス制御情報を適用する例としては、スキャン送信機能、ＢＯＸ送信機能、ＢＯＸファイル設定機能等がある。スキャン送信機能は、原稿をスキャンしたデータファイルをメールで任意のメールアドレスに送信する機能である。ＢＯＸ送信はＭＦＰ１０４のハードディスク（ＢＯＸ）３０５に保存されたデータファイルをスキャン送信同様、任意のメールアドレスに送信する機能である。ＢＯＸファイル設定機能はＭＦＰ１０４のハードディスク（ＢＯＸ）に保存されたデータファイルに対し、アクセス制御情報等を設定する機能である。

【００６７】

（文書管理処理の流れ）

図８は、ＭＦＰ１０４におけるアクセス制御情報の設定処理の流れを説明するフローチャートである。ＭＦＰ１０４における本処理は、ＣＰＵ３００の全体的な制御の下に実行される。以下，フローチャートに従い、処理を説明する。

【００６８】

まず、ステップＳ８０１において、デバイス及び文書管理プログラムの起動に際し、必要な初期化処理を行う。

【００６９】

ステップＳ８０２において、認証画面を表示する。

【００７０】

ステップＳ８０３において、認証画面でログインされたか判定し、ログインされていないと判定されると（Ｓ８０３－Ｎｏ）、認証画面を表示したログイン待ちの状態で待機する。ステップＳ８０３で、ログインされたと判定された場合（Ｓ８０３－Ｙｅｓ）、処理はステップＳ８０４に進められる。

【００７１】

ステップＳ８０４において、ＣＰＵ３００は、表示部３０７に機能メニューを表示する。ユーザは機能メニューの表示画面で、自分の欲する要求を指定することができる。

【００７２】
ステップＳ８０５において、ＣＰＵ３００は、機能メニューの中からスキャン保存機能が選択されたか判定する。スキャン保存機能が選択された場合は（Ｓ８０５－Ｙｅｓ）、原稿をスキャンし、スキャンした画像をハードディスク（ＨＤ）３０５に一時保存する（Ｓ８０６）。
【００７３】
次に、ステップＳ８０７において、ＣＰＵ３００は、アクセス制御設定に関する指定があるかを判定し、指定がある場合は（Ｓ８０７－Ｙｅｓ）、処理をステップＳ８０８に進め、アクセス制御情報設定処理を行う。アクセス制御情報設定処理の詳細については、図９のフローチャートを参照して詳細に説明する。
【００７４】
アクセス制御情報設定処理（Ｓ８０８）の後、処理はステップＳ８０９に進められ、ステップＳ８０９において、ＣＰＵ３００は、指定されたストレージ装置（記憶領域）にファイルの保存処理を行い、処理をステップＳ８０４に戻す。ファイルの格納場所としては、アクセス可能な場所であればよく、ハードディスク（ＨＤ）、ファイルサーバ、ドキュメントサーバ等にファイルを格納しておくことが可能である。
【００７５】
本ステップにおいて、アクセス制御情報設定処理により仮想ポリシーから変換された実ポリシーが設定されたファイルが指定されたストレージ装置（記憶領域）等に格納される。
【００７６】
一方、ステップＳ８０５の判定で、スキャン保存機能が選択されていない場合（Ｓ８０５－Ｎｏ）、処理はステップＳ８１０に進められる。
【００７７】
ステップＳ８１０において、ＣＰＵ３００は、機能メニューの中で、スキャン送信機能が選択されたか判定する。スキャン送信機能が選択された場合（Ｓ８１０－Ｙｅｓ）、処理はステップＳ８１１に進められ、原稿をスキャンし、スキャンした画像をハードディスク（ＨＤ）３０５に一時保存する（Ｓ８１１）。
【００７８】
次に、ステップＳ８１２において、ＣＰＵ３００は、アクセス制御設定に関する指定があるかを判定し、指定がある場合（Ｓ８１２－Ｙｅｓ）、処理をステップＳ８１３に進め、アクセス制御情報設定処理を行う。
【００７９】
アクセス制御情報設定処理（Ｓ８１３）の後、処理はステップＳ８１４に進められ、ステップＳ８１４において、ＣＰＵ３００は、指定された送信先にファイルの送信処理を行い（Ｓ８１４）、処理をステップＳ８０４に戻す。
【００８０】
ステップＳ８１４において、アクセス制御情報設定処理により仮想ポリシーから変換された実ポリシーが設定されたファイルが指定された送信先に送信される。
【００８１】
一方、ステップＳ８１０の判定で、スキャン送信機能が選択されていない場合（Ｓ８１０－Ｎｏ）、処理はステップＳ８１５に進められる。
【００８２】
ステップＳ８１５において、ＣＰＵ３００は、機能メニューの中で、ＢＯＸ送信機能が選択されたか判定する。ＢＯＸ送信機能が選択された場合（Ｓ８１５－Ｙｅｓ）、処理はステップＳ８１６に進められ、ＣＰＵ３００は、表示部３０７にファイル選択画面を表示する。そして、ファイル選択画面からＢＯＸ送信の対象となるファイルが選択されたか判定する。ファイルが選択されない場合（Ｓ８１６－Ｎｏ）、ファイル選択画面の表示を継続した待機状態とする。ステップＳ８１６において、ファイルが選択された場合（Ｓ８１６－Ｙｅｓ）、処理はステップＳ８１２に進められる。

【００８３】
選択されたファイルに対して、アクセス制御設定処理の指定がある場合（Ｓ８１２－Ｙｅｓ）、処理はステップＳ８１３に進められる。ステップＳ８１３において、選択されたファイルに対してアクセス制御情報設定処理を行った後、ＣＰＵ３００は指定されたあて先に対してファイルを送信し（Ｓ８１４）、処理をステップＳ８０４に戻す。
【００８４】
一方、ステップＳ８１５の判定で、ＢＯＸ送信機能が選択されていない場合（Ｓ８１５－Ｎｏ）、処理はステップＳ８１７に進められる。
【００８５】
ステップＳ８１７において、ＣＰＵ３００は、機能メニューの中で、ＢＯＸデータ閲覧が要求されているか判定する。ＢＯＸデータ閲覧が選択された場合（Ｓ８１７－Ｙｅｓ）、処理はステップＳ８１８に進められ、ＣＰＵ３００は、ハードディスク（ボックス）３０５内のファイルを表示部３０７に表示する。
【００８６】
Ｓ８１９において、ＣＰＵ３００は、指定ファイルへのアクセス制御設定が要求されたか判定し、アクセス制御設定が指定されていない場合（Ｓ８１９－Ｎｏ）、処理はステップＳ８２１に進められる。
【００８７】
一方、ステップＳ８１９の判定で、アクセス制御設定が指定された場合（Ｓ８１９－Ｙｅｓ）、ＣＰＵ３００は処理をステップＳ８２０に進め、アクセス制御情報設定処理を行う。本処理により、仮想ポリシーから変換された実ポリシーがファイルに設定される。
【００８８】
アクセス制御情報設定処理（Ｓ８２０）の後、処理はステップＳ８２１に進められ、ＣＰＵ３００はＢＯＸ内ファイル閲覧要求の終了が指定されたか判定する。
【００８９】
ステップＳ８２１の判定でＢＯＸ内ファイル閲覧要求の終了が指定された場合（Ｓ８２１－Ｙｅｓ）、処理はステップＳ８０４に戻される。一方、ＢＯＸ内ファイル閲覧要求の終了が指定されていない場合（Ｓ８２１－Ｎｏ）、処理はステップＳ８１８に戻され、ＢＯＸ内の他のファイルの表示に関し同様の処理を行う。
【００９０】
一方、ステップＳ８１７の判定で、ＣＰＵ３００は、機能メニューの中で、ＢＯＸデータ閲覧が要求されていないと判定する場合（Ｓ８１７－Ｎｏ）、処理をステップＳ８２３に進める。
【００９１】
ステップＳ８２３において、ＣＰＵ３００は機能メニューの中で、ログアウトが選択されたか判定し、ログアウトが選択された場合（Ｓ８２３－Ｙｅｓ）、処理をステップＳ８２４に進め、ログアウト処理を行う（Ｓ８２４）。一方、ステップＳ８２３の判定で、ログアウトが選択されていない場合（Ｓ８２３－Ｎｏ）、処理はステップＳ８０４に戻され、ステップＳ８０４以降同様の処理を繰り返す。
【００９２】
（アクセス制御情報設定処理の流れ）
次に、アクセス制御情報設定処理について説明する。図９はアクセス制御情報設定処理の流れを説明するフローチャートである。
【００９３】
ステップＳ９０１において、アクセス制御管理サーバにログインを行い、ログインされたか判定する（Ｓ９０２）。図８のステップＳ８０３での認証とアクセス制御管理サーバでの認証が同じ場合、ステップＳ９０１、Ｓ９０２の処理は省略可能である。
【００９４】
ステップＳ９０２でログインが確認された場合（Ｓ９０２－Ｙｅｓ）、処理はステップＳ９０３に進められ、ＣＰＵ３００は、仮想ポリシーを列挙したポリシー選択画面を表示

部３０７に表示する。ステップＳ９０３で表示される仮想ポリシーは予めデバイス（ここでは画像形成装置）に設定された仮想ポリシーのリストである。

【００９５】

図１３は、仮想ポリシーを列挙した仮想ポリシー選択画面を例示する図である。ここでは、課外秘、部外秘、社外秘などの仮想ポリシーが表示されている。このリストから設定者は一つ選択し、ＯＫボタン１３０１を押下することで表示された何れかの仮想ポリシーを選択することが可能である。

【００９６】

説明を図９のステップＳ９０３に戻し、仮想ポリシー選択画面で仮想ポリシーが選択されたか確認し（Ｓ９０４）、仮想ポリシーが選択されていない場合（Ｓ９０４－Ｎｏ）、仮想ポリシーを選択待ちとする待機状態とする。

【００９７】

一方、ステップＳ９０４の判定で仮想ポリシーが選択されたと、ＣＰＵ３００が判定する場合（Ｓ９０４－Ｙｅｓ）、処理はステップＳ９０５に進められ、アクセス制御管理サーバ１０３にポリシー変換要求を送信する（Ｓ９０５）。

【００９８】

ここで、仮想ポリシーの選択において、ＣＰＵ３００は付随した仮想ポリシーの設定情報（例えば、アクセス可能な仮想グループ情報）をハードディスク（ＨＤ）３０５から読み出すことが可能である。ＣＰＵ３００は、選択された仮想ポリシーが仮想ポリシーの設定情報を必要とする場合、仮想ポリシーと共に仮想ポリシーの設定情報をアクセス制御管理サーバ１０３に送信する。

【００９９】

また、ＣＰＵ３００は、選択された仮想ポリシーがポリシー選択者（あるいは原稿をスキャン入力した入稿者）の情報を必要とする場合、同時にポリシー選択者の情報（ポリシー選択者情報）もアクセス制御管理サーバ１０３に送信する。

【０１００】

ポリシー変換要求を受信したアクセス制御管理サーバ１０３は、仮想ポリシーをアクセス制御管理サーバ１０３で解釈可能な実ポリシーに変換する。アクセス制御管理サーバ１０３による仮想ポリシーから実ポリシーへの変換処理の具体的な処理の流れは図１０のフローチャートを参照して説明する。

【０１０１】

ステップＳ９０６において、ＣＰＵ３００は、アクセス制御管理サーバ１０３から実ポリシーを受信したか判定し、受信していないと判定する場合は（Ｓ９０６－Ｎｏ）、実ポリシーの受信待ち状態で待機する。

【０１０２】

ステップＳ９０６の判定で、ＣＰＵ３００が実ポリシーを受信したと判定した場合（Ｓ９０６－Ｙｅｓ）、処理はステップＳ９０７に進められ、受信した実ポリシー（アクセス制御情報）をスキャンした画像データのファイルに設定する。ＣＰＵ３００は、変換された実ポリシーをファイルに設定し、例えば、ハードディスク（ＨＤ）３０５に格納する。格納されたファイルに対するアクセス権限は、アクセス制御管理サーバ１０３により管理される。

【０１０３】

（アクセス制御管理サーバの処理）

次にアクセス制御管理サーバ１０３の処理の流れを説明する。図１０は、アクセス制御管理サーバ１０３の処理の流れを説明するフローチャートである。本処理は、アクセス制御管理サーバ１０３のＣＰＵ２００による全体的な制御の下に実行される。

【０１０４】

まず、ステップＳ１００１において、文書管理プログラムの起動にあたり、必要な初期化処理を行う。

【０１０５】

ステップＳ１００２において、ＣＰＵ２００は、ログイン要求を検出したか判定する。リグイン要求を判定した場合（Ｓ１００２－Ｙｅｓ）、処理はステップＳ１００３に進められる。

【０１０６】

ステップＳ１００３において、ＣＰＵ２００は、ディレクトリサーバに問い合わせてユーザ（ポリシー選択者、あるいは原稿をスキャン入力した入稿者）のアクセス権を確認する。ここでは、一般的な検索サービスを持つディレクトリサーバがユーザのアクセス権に関する情報を持つこととしているが、ユーザ認証が可能な認証サーバ等、他の手段を利用することも可能である。

【０１０７】

次に、ステップＳ１００４において、ＣＰＵ２００は認証の結果を確認し、認証ＯＫの場合（Ｓ１００４－Ｙｅｓ）、ステップＳ１００６において、ＣＰＵ２００はログインに必要な処理を行う。ステップＳ１００６の後、処理はステップＳ１００２に戻される。

【０１０８】

ステップＳ１００４の判定で、認証ＮＧの場合（Ｓ１００４－Ｎｏ）、ステップＳ１００５において、ポリシーの変換を要求する要求元に認証エラーを返信し、処理をステップＳ１００２に戻す。

【０１０９】

ステップＳ１００２の判定で、ログイン要求が検出されない場合（Ｓ１００２－Ｎｏ）、処理はステップＳ１００７に進められる。

【０１１０】

ステップＳ１００７において、ＣＰＵ２００は、ポリシー変換要求を検出したか判定する。ポリシー変換要求を検出した場合（Ｓ１００７－Ｙｅｓ）、処理はステップＳ１００８に進められる。

【０１１１】

ステップＳ１００８において、ＣＰＵ２００は、ポリシー変換要求内に指定された仮想ポリシーと、かかる仮想ポリシーを選択（設定）したポリシー選択者の情報（ポリシー選択者情報）とを取得する。

【０１１２】

アクセス制御管理サーバ１０３は、例えば、ハードディスク（ＨＤ）２０５内のデータベース等に仮想ポリシーごとに設定されたアクセス権のリストを有する（例えば、図１５（ａ））。このリストは、ファイルへのアクセスが可能な権限を定めるアクセス権限情報となる。アクセス権限情報には、ファイルに対するアクセスの種類を定める情報と、ファイルに対するアクセスが制限されるユーザグループの情報が含まれる。

【０１１３】

ステップＳ１００９において、アクセス制御管理サーバ１０３のＣＰＵ２００は、そのリストから指定された仮想ポリシーに関する情報を読み込んで、変換が必要な仮想ユーザかつ/またはグループ情報を取得する。仮想ユーザ/グループ情報としては、例えば、図１５（ａ）の場合、「ポリシー設定者」、「ポリシー設定者所属部の部員」に関する情報が対応する。

【０１１４】

ステップＳ１０１０において、ＣＰＵ２００は変換に必要な仮想ユーザかつ/または仮想グループのポリシー設定者に関する情報をディレクトリサーバより取得し、実際に存在する実ユーザかつ/また実グループ情報を特定する。

【０１１５】

ステップＳ１０１１において、ＣＰＵ２００は、アクセス可能な実ユーザ名/グループ名より実ポリシーを特定する。

【０１１６】

ステップＳ１０１２において、ＣＰＵ２００は、先のステップＳ１０１１で特定された実ポリシーをポリシー変換要求者へ送信し、処理をステップＳ１００２に戻す。

【０１１７】
ここで、ディレクトリサーバ１０５には図１４で示されるように、ユーザ及びグループ情報について、ツリー構造の情報が格納されている。ツリー構造のリンクを辿っていくことで、例えば、課員、課、部と、上位の属性に関する情報を取得することが可能である。
【０１１８】
図１５（ａ）は仮想ポリシー「部外秘」に設定されたアクセス権（閲覧、編集、印刷、送信(デバイス用途のみ)）を示すリストを例示する図である。ポリシー設定者に関しては全アクセス権が付与（図中「○」印で示す）されている。ポリシー設定者の所属部の部員には編集以外のアクセス権が付与されている。それ以外のユーザはアクセス権が付与されていない。ここでは、変換が必要な情報（可変の情報としてリストに登録されている情報）は、「ポリシー設定者」と、「ポリシー設定者所属部の部員」である。
【０１１９】
例えば、図１４の例で「SUZUKI」がポリシー変換を要求する場合について説明すると、図１４より「SUZUKI」の所属部は「営業１部」であることが特定される。営業一部の部員である「SUZUKI」が仮想ポリシー「部外秘」を選択した場合の実ポリシーへの変換は図１５（ｂ）のように変換される。図１５（ｂ）では、「ポリシー設定者」が「SUZUKI」に変換され、「ポリシー設定者所属部の部員」が「営業１部　部員」と変換される。
【０１２０】
説明を図１０のステップＳ１００７に戻し、ポリシー変換要求を検出しない場合（Ｓ１００７－Ｎｏ）、処理はステップＳ１０１３に進められる。
【０１２１】
ＣＰＵ２００は、実セキュリティポリシーが設定されたファイルに対するアクセス権の有無をファイルにアクセスする者の認証情報に基づいて判定する。
【０１２２】
ステップＳ１０１３において、ＣＰＵ２００は、指定された仮想ポリシーに対するアクセス権確認要求か判定する。アクセス権確認要求の場合（Ｓ１０１３－Ｙｅｓ）、処理はステップＳ１０１４に進められる。ステップＳ１０１４において、ＣＰＵ２００は、データベース等に格納されているリストを参照して、指定された仮想ポリシーに対して設定されている、ユーザ、グループに関するアクセス権を取得する。
【０１２３】
ステップＳ１０１５において、ＣＰＵ２００は、要求されたアクセス権がアクセス確認者に付与されているか確認する。
【０１２４】
ステップＳ１０１６において、ＣＰＵ２００は、アクセス権の確認結果をアクセス権確認者へ送信し、処理をステップＳ１００２に戻す。
【０１２５】
ステップＳ１０１３の判定で、アクセス権確認要求でない場合（Ｓ１０１３－Ｎｏ）、処理はステップＳ１００２に戻され、同様の処理が繰り返される。
【０１２６】
（アクセス制御情報が設定されたファイルに対してアクセス要求を行うユーザコンピュータの処理）
次にアクセス制御情報が設定されたファイルに対してアクセス要求を行うユーザコンピュータ（例えば、図１のコンピュータ１０１、１０２）の処理を図１１のフローチャートを参照して説明する。本処理は、コンピュータ１０１、１０２におけるＣＰＵ２００の全体的な制御の下に実行される。
【０１２７】
まず、ステップＳ１１０１において、文書処理プログラムを起動し、初期化する。
【０１２８】
次に、ステップＳ１１０２において、文書ファイル（以下、「ファイル」ともいう）のオープン要求か判定する。ファイルのオープン（ＯＰＥＮ）要求の場合は（Ｓ１１０２－

Ｙｅｓ）、処理をステップＳ１１０３に進め、指定されたファイルを取得する。一方、ステップＳ１１０２の判定で、ファイルのオープン要求でない場合（Ｓ１１０２－Ｎｏ）、ファイルオープン要求の受信待ちの状態で待機する。ファイルの格納場所としては、アクセス可能な場所であればよく、ハードディスク（ＨＤ）、ファイルサーバ、ドキュメントサーバ等にファイルを格納しておくことが可能である。

【０１２９】

ステップＳ１１０４において、ファイルにアクセス制御管理サーバ１０３で管理されているアクセス制御情報（実ポリシー）が設定されているかを判定する。ステップＳ１１０４の判定で、ファイルにアクセス制御情報が設定されている場合は（Ｓ１１０４－Ｙｅｓ）、処理をステップＳ１１０５に進める。一方、ステップＳ１１０４の判定で、アクセス制御情報がファイルに設定されていない場合（Ｓ１１０４－Ｎｏ）、処理はステップＳ１１０２に戻される。

【０１３０】

ステップＳ１１０５において、コンピュータ１０１または１０２のＣＰＵ２００は、アクセス制御管理サーバ１０３へログイン処理を行う。

【０１３１】

Ｓ１１０６で、アクセス制御管理サーバ１０３は、ログインユーザ即ちファイルアクセス要求者がアクセス制御情報（実ポリシー）が設定されているファイルに対して、アクセスする権限（アクセス権）を保持するか確認する。ここで、アクセス権には、例えば、アクセス制御情報（実ポリシー）が設定されているファイルに対する閲覧、編集、印刷、送信等が含まれる。

【０１３２】

アクセス制御管理サーバ１０３は、アクセス権の確認要求の処理として、図１０のステップＳ１０１４、Ｓ１０１５、Ｓ１０１６の処理を実行する。ステップＳ１０１６の処理により、コンピュータ１０１または１０２は、アクセス権の確認結果を取得することが可能である。

【０１３３】

ステップＳ１１０７において、先のステップＳ１１０６の確認結果に基づき、ログインユーザがファイルに対して編集アクセスが可能であるか判定する。

【０１３４】

ＣＰＵ２００は、先のステップＳ１１０６の確認結果に基づき、実ポリシーが設定されたファイルへのアクセスを制限する。編集アクセスが可能な場合（Ｓ１１０７－Ｙｅｓ）、ステップＳ１１０８において、ＣＰＵ２００の制御の下、文書処理プログラムはRead/Write権限でファイルをオープンし、処理をステップＳ１１０２に戻す。

【０１３５】

一方、ステップＳ１１０７の判定で、編集アクセスが不可の場合（Ｓ１１０７－Ｎｏ）、処理はステップＳ１１０９に進められ、先のステップＳ１１０６の確認結果に基づき、ログインユーザがファイルに対して閲覧アクセスが可能であるか判定する。閲覧アクセスが可能な場合（Ｓ１１０９－Ｙｅｓ）、ステップＳ１１１０において、ＣＰＵ２００の制御の下、文書処理プログラムはRead　Only権限でファイルをオープンし、その旨をユーザに通知する。そして、処理をステップＳ１１０２に戻す。

【０１３６】

ステップＳ１１０９の判定で、ファイルを閲覧するアクセス権限がない場合、ステップＳ１１１１において、エラー通知を行い、処理をステップＳ１１０２に戻す。

【０１３７】

以上説明したように、本発明の本実施形態によれば、ポリシー選択メニューのカスタマイズが可能になり、ユーザの使用環境に応じたポリシーの設定で文書管理をすることができる。

【０１３８】

あるいは、本発明の本実施形態によれば、ポリシー選択メニューが簡明になることで、

ユーザの選択が容易になり、ユーザの利便性を向上することができる。

【０１３９】

あるいは、本発明の本実施形態によれば、ポリシー選択メニューを共通化することにより、メニュー表示が高速化するという効果が得ることができる。

【０１４０】

（第２実施形態）

第１実施形態ではデバイス（たとえば、ＭＦＰ１０４で入稿された画像データのファイルに対してアクセス制御情報を設定する例を説明した。本実施形態では、例えば、ユーザコンピュータ側でアクセス制御情報を設定する例を説明する。尚、本実施形態では、ユーザコンピュータを例として、アクセス制御情報をファイルに設定する例を説明するが、他のサーバ等のコンピュータ上においても処理の流れは同様のものとなる。

【０１４１】

図１２は、本発明の第２実施形態に係る文書管理システムの構成を説明するブロック図である。図１２において、コンピュータ１０２からアクセス可能な文書ファイルに対して、アクセス制御情報を適用し、ドキュメントサーバ１０６に保存する例を図示している。また、図１の文書管理システムと同様の構成要素に関しては、同一の参照番号を付している。

【０１４２】

コンピュータ１０２において、本発明の実施形態にかかるアクセス制御情報の設定が可能な文書管理プログラムが作動している。仮想ポリシー設定者であり、かつ、ドキュメントサーバへの入稿者であるユーザはコンピュータ１０２に表示されたＵＩ(ユーザインターフェース)画面で、認証、ファイル選択、ポリシー選択などの各種操作を行うことが可能である。

【０１４３】

また、選択したファイルに対し、アクセス制御情報を設定し、ドキュメントサーバ１０６に保存することが可能である。

【０１４４】

アクセス制御管理サーバ１０３はコンピュータ１０２からのポリシー変換要求を受けて、先に説明したアクセス制御設定処理（図９）に従い仮想ポリシーを実ポリシーに変換してコンピュータ１０２に返信する。

【０１４５】

ディレクトリサーバ１０５にはユーザ情報が格納され、アクセス制御管理サーバ１０３からのユーザ情報及びグループ情報の問い合わせに対し、適宜情報を返信する。

【０１４６】

コンピュータ１０１のユーザは、ドキュメントサーバ１０６に保存されたファイルに対し、閲覧要求を行う閲覧者（編集を行う編集者でもよい）である。閲覧(或いは編集)に際しては、アクセス制御情報が設定されている場合、アクセス制御管理サーバ１０３に問い合わせが実施される。アクセス制御管理サーバ１０３は、アクセス権の確認を行い、閲覧或は編集に関して与えられている権限の確認結果に基づきファイルへのアクセスが許可される。

【０１４７】

ファイルの保存先として、図１２では、ドキュメントサーバ１０６を示したが、コンピュータ１０２のローカルハードディスク、ネットワークの共有フォルダ、ファイルサーバ等、任意のストレージ装置に保存することも可能である。

【０１４８】

アクセス制御管理サーバ１０３の処理、及びアクセス制御情報設定ファイルに対するアクセス要求者によるコンピュータ１０１側の処理は、第１実施形態の場合と同様である。

【０１４９】

第１実施形態における処理と異なるのは、ポリシー設定者がコンピュータ１０２でアクセス制御情報を指定する点であり、図１６に示す処理の流れとなる。尚、このフローチャ

ートの処理は、第１実施形態で説明した図１１の処理と合わせて閲覧者側のプログラムとして実装することが可能である。本処理は、コンピュータ１０２のＣＰＵ２００の全体的な制御の下に実行される。

【０１５０】

まず、ステップＳ１６０１において、文書処理プログラムを起動し、初期化する。次に、ステップＳ１６０２において、ファイルに対するオープン要求か判定し、ファイルのオープン要求の場合は（Ｓ１６０２－Ｙｅｓ）、ステップＳ１６０３において、指定されたファイルを表示する。

【０１５１】

一方、ステップＳ１６０２の判定で、ファイルのオープン要求でない場合（Ｓ１６０２－Ｎｏ）、処理はステップＳ１６０４に進められ、ファイルに対するアクセス制御設定要求か判定する。

【０１５２】

ステップＳ１６０４の判定で、ファイルに対するアクセス制御設定要求の場合（Ｓ１６０４－Ｙｅｓ）、処理はステップＳ１６０５に進められる。ステップＳ１６０５において、アクセス制御管理サーバ１０３はコンピュータ１０２からのポリシー変換要求を受けて、アクセス制御設定処理（図９）に従い仮想ポリシーを実ポリシーに変換してコンピュータ１０２に返信する。

【０１５３】

ステップＳ１６０４の判定で、ファイルに対するアクセス制御設定要求でない場合（Ｓ１６０４－Ｎｏ）、処理はステップＳ１６０２に戻される。

【０１５４】

以上説明したように、本発明の本実施形態によれば、ポリシー選択メニューのカスタマイズが可能になり、ユーザの使用環境に応じたポリシーの設定で文書管理をすることができる。

【０１５５】

あるいは、本発明の本実施形態によれば、ポリシー選択メニューが簡明になることで、ユーザの選択が容易になり、ユーザの利便性を向上することができる。

【０１５６】

あるいは、本発明の本実施形態によれば、ポリシー選択メニューを共通化することにより、メニュー表示が高速化するという効果が得ることができる。

【０１５７】

（第３実施形態）

第１及び第２実施形態で説明した構成では、ポリシー設定者の設定フローの中で、アクセス制御管理サーバ１０３によるポリシー変換を行い、ファイルにアクセス制御情報（実ポリシー）を設定している。アクセス制御情報（実ポリシー）を設定するタイミングとしては、第１及び第２実施形態の例に限定されず、例えば、閲覧者或いは編集者からファイルに対するアクセス要求があった時に、仮想ポリシーから実ポリシーへのポリシー変換を行うようにしてもよい。

【０１５８】

この場合、図９のステップＳ９０５～Ｓ９０７の処理は行わず、ステップＳ９０４で選択された仮想ポリシーをファイルに設定する。ファイルに対する編集、閲覧等のアクセスが指定された場合に、ファイルに設定されている仮想ポリシーの変換要求をアクセス制御管理サーバ１０３に送信して、図９のステップＳ９０５～Ｓ９０７の処理を実行するようにしてもよい。

【０１５９】

仮想ポリシーの変換要求とファイルに対するアクセス権の確認要求と同じタイミングで実行することも可能である。

【０１６０】

ポリシー変換のタイミングをポリシー設定者がファイルへのポリシー設定時に行うか、

閲覧者或いは編集者からファイルアクセス要求があった時に行うか、文書管理システムの環境設定として切り替え可能に構成することも可能である。

【０１６１】

本発明の本実施形態によれば、アクセス制御管理サーバと通信不能の場合にも、ポリシー選択が可能であるため、通信が回復したときにユーザによるポリシーの再選択を省略できるという効果が得られる。

【０１６２】

（第４実施形態）

第１実施形態において、仮想ポリシーを実ポリシーに変換する構成をアクセス制御管理サーバ１０３で行う構成として説明したが、本発明の趣旨はこの例に限定されるものでないことは言うまでもない。例えば、仮想ポリシーの選択を行う構成と、アクセス権限情報を取得する構成と、文書管理システムで共通に解釈可能な実セキュリティポリシーに変換する構成とを、同一のネットワークデバイスに設けることが可能である。ここで、同一のネットワークデバイスとは、第１実施形態の場合はＭＦＰ１０４上、第２実施形態の場合は図１２のコンピュータ１０２上、第３実施形態の場合は閲覧者のコンピュータ上である。

【０１６３】

この場合、アクセス制御情報設定処理（図９）のステップＳ９０５～Ｓ９０７のポリシー変換要求先をアクセス制御管理サーバ１０３ではなく、ポリシー変換を行う変換アプリケーションに変更すればよい。

【０１６４】

また、図１０のステップＳ１００７～Ｓ１０１２の処理を、ポリシー変換を行う変換アプリケーションとして実装すればよい。ポリシー変換を行う変換アプリケーションをポリシー設定者側で実行し、ポリシー変換要求の処理をポリシー設定者側で実行しても第１実施形態から第３実施形態と同様の効果を得ることができる。

【０１６５】

（他の実施形態）

なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェ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ことによっても、達成されることは言うまでもない。また、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、達成されることは言うまでもない。

【０１６６】

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。

【０１６７】

プログラムコード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、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【０１６８】

また、コンピュータが読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。また、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）など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が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

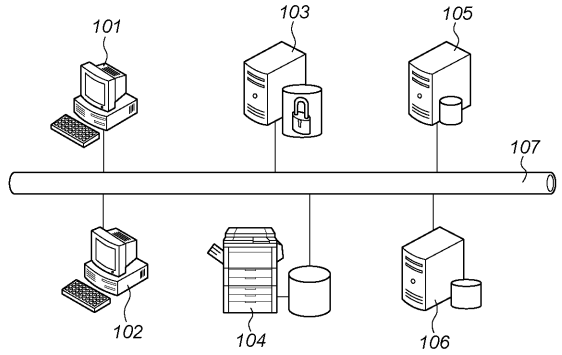
【０１６９】

【図１】本発明の実施形態に係る文書管理システムの構成を説明するブロック図である。

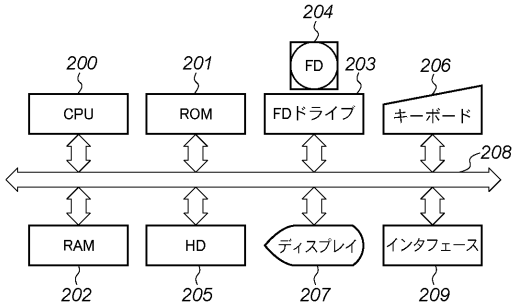
【図２】本発明の実施形態に係るコンピュータ（情報処理装置）の構成を説明するブロッ

ク図である。
【図３】本発明の実施形態に係る画像形成装置であるＭＦＰ１０４の構成を説明するブロック図である。
【図４】図２、図３で示したコンピュータ（情報処理装置）、画像形成装置におけるメモリマップメモリマップ一例を示す図である。
【図５】図２に示したＦＤ２０４のメモリマップの一例を示す図である。
【図６】図２に示したＦＤドライブ２０３に対して挿入されるＦＤ２０４との関係を示す図である。
【図７】第１実施形態に係る文書管理システムの処理の流れを概略的に示す図である。
【図８】第１実施形態に係るデバイスにおけるアクセス制御情報の設定処理の流れを説明するフローチャートである。
【図９】第１実施形態に係るアクセス制御情報設定処理の流れを説明するフローチャートである。
【図１０】第１実施形態に係るアクセス制御管理サーバの処理の流れを説明するフローチャートである。
【図１１】第１実施形態に係るアクセス制御情報が設定されたファイルに対してアクセス要求を行うユーザコンピュータの処理の流れを説明するフローチャートである。
【図１２】第２実施形態に係る文書管理システムの構成を説明するブロック図である。
【図１３】第１実施形態に係る仮想ポリシーを列挙した仮想ポリシー選択画面を例示する図である。
【図１４】ディレクトリサーバに格納されているユーザ及びグループ情報を例示する図である。
【図１５】（ａ）は仮想ポリシー「部外秘」に設定されたアクセス権（閲覧、編集、印刷、送信(デバイス用途のみ)）を示すリストを例示する図であり、（ｂ）は実ポリシーへの変換を例示する図である。
【図１６】第２実施形態に係る処理の流れを説明するフローチャートである。

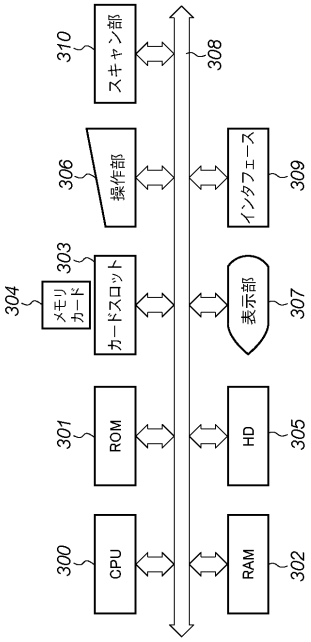
【図１】



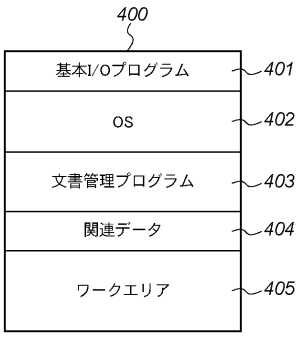
【図２】



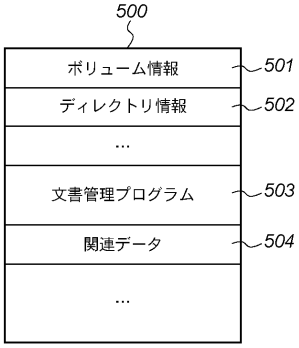
【図３】



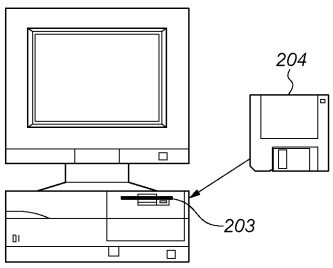
【図４】



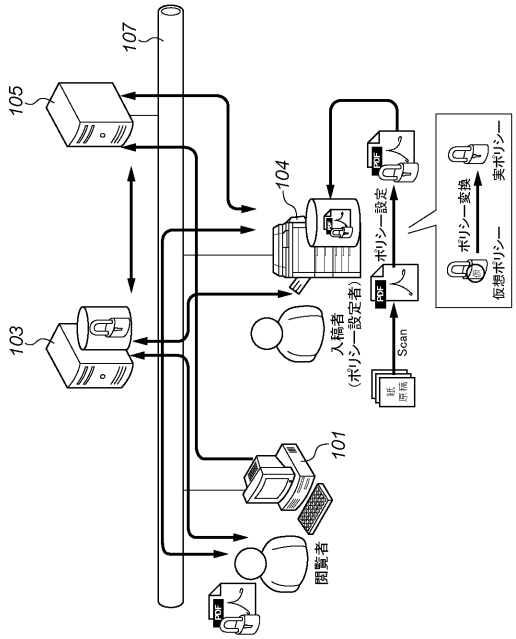
【図５】



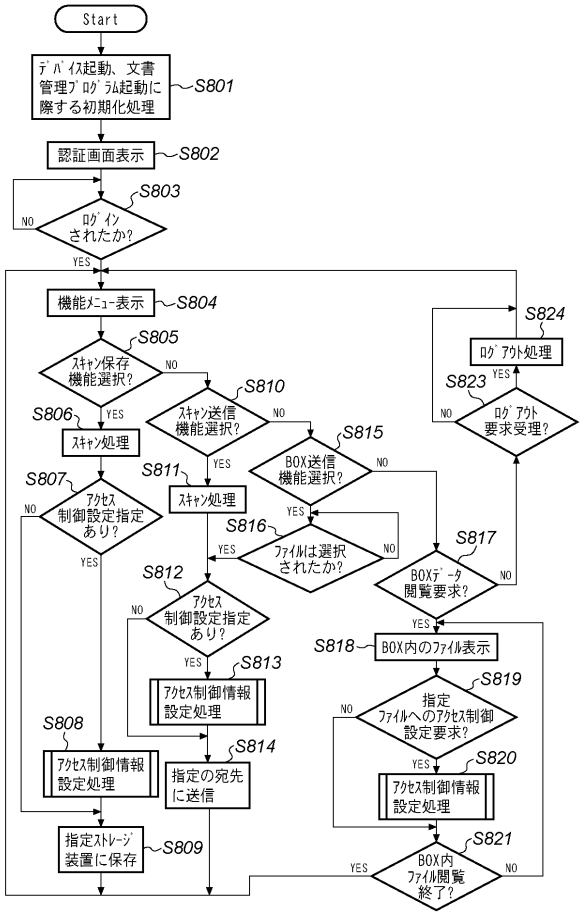
【図６】



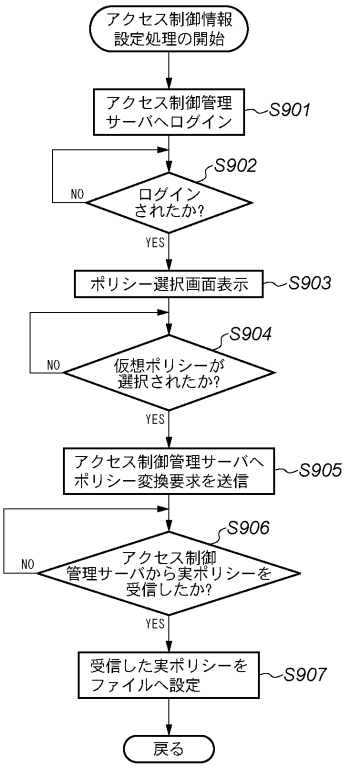
【図７】


107
105
104
103
101
ポリシー設定
ポリシー変換
実ポリシー
仮想ポリシー
入稿者
(ポリシー設定者)
Scan
閲覧者

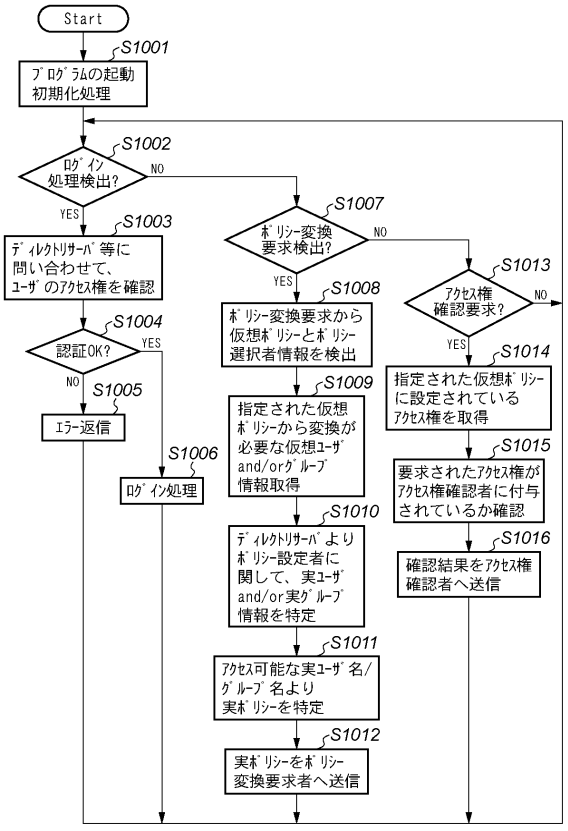
【図８】


Start
ﾃﾞﾊﾞｲｽ起動、文書管理ﾌﾟﾛｸﾞﾗﾑ起動に際する初期化処理
S801
認証画面表示
S802
ﾛｸﾞｲﾝされたか?
S803
機能ﾒﾆｭｰ表示
S804
ｽｷｬﾝ保存機能選択?
S805
ｽｷｬﾝ処理
S806
ｱｸｾｽ制御設定指定あり?
S807
ｽｷｬﾝ送信機能選択?
S810
ｽｷｬﾝ処理
S811
ﾌｧｲﾙは選択されたか?
S816
BOX送信機能選択?
S815
BOXﾃﾞｰﾀ閲覧要求?
S817
BOX内のﾌｧｲﾙ表示
S818
指定ﾌｧｲﾙへのｱｸｾｽ制御設定要求?
S819
ｱｸｾｽ制御情報設定処理
S820
BOX内ﾌｧｲﾙ閲覧終了?
S821
ﾛｸﾞｱｳﾄ要求受理?
S823
ﾛｸﾞｱｳﾄ処理
S824
ｱｸｾｽ制御設定指定あり?
S812
ｱｸｾｽ制御情報設定処理
S813
ｱｸｾｽ制御情報設定処理
S808
指定の宛先に送信
S814
指定ｽﾄﾚｰｼﾞ装置に保存
S809

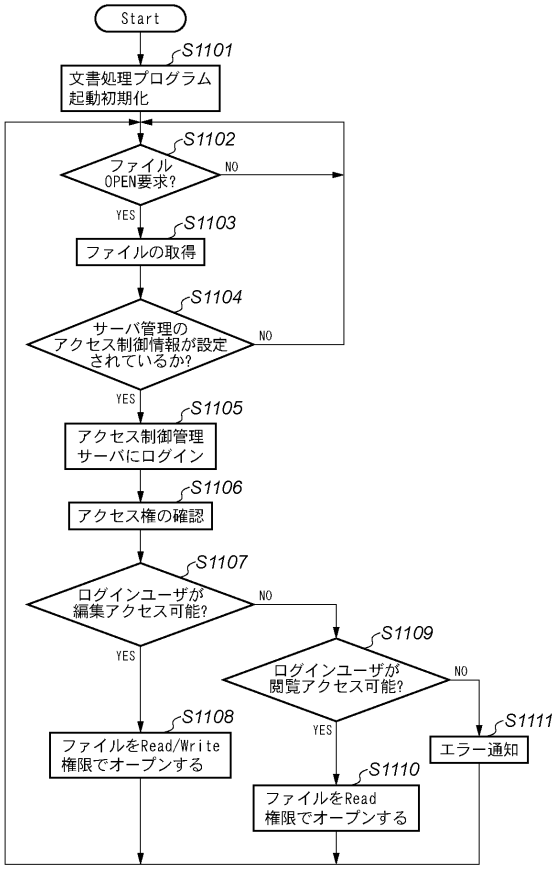
【図９】


アクセス制御情報設定処理の開始
アクセス制御管理サーバへログイン
S901
ログインされたか?
S902
ポリシー選択画面表示
S903
仮想ポリシーが選択されたか?
S904
アクセス制御管理サーバへポリシー変換要求を送信
S905
アクセス制御管理サーバから実ポリシーを受信したか?
S906
受信した実ポリシーをファイルへ設定
S907
戻る

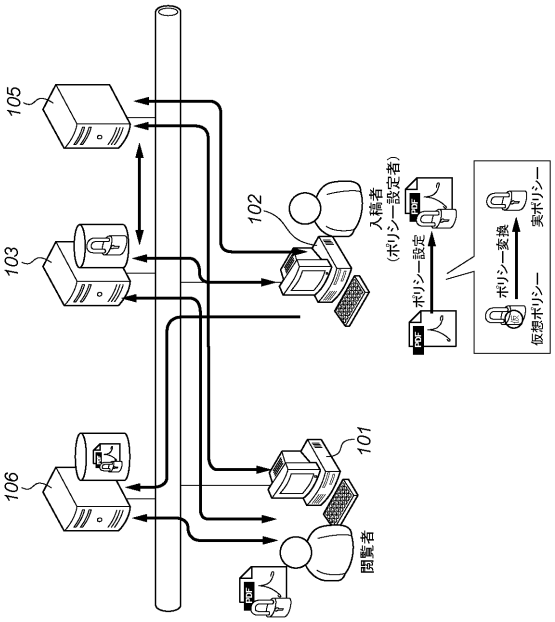
【図１０】


Start
ﾌﾟﾛｸﾞﾗﾑの起動初期化処理
S1001
ﾛｸﾞｲﾝ処理検出?
S1002
ﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ等に問い合わせて、ﾕｰｻﾞのｱｸｾｽ権を確認
S1003
認証OK?
S1004
ｴﾗｰ返信
S1005
ﾛｸﾞｲﾝ処理
S1006
ﾎﾟﾘｼｰ変換要求検出?
S1007
ﾎﾟﾘｼｰ変換要求から仮想ﾎﾟﾘｼｰとﾎﾟﾘｼｰ選択者情報を検出
S1008
指定された仮想ﾎﾟﾘｼｰから変換が必要な仮想ﾕｰｻﾞand/orｸﾞﾙｰﾌﾟ情報取得
S1009
ﾃﾞｨﾚｸﾄﾘｻｰﾊﾞよりﾎﾟﾘｼｰ設定者に関して、実ﾕｰｻﾞand/or実ｸﾞﾙｰﾌﾟ情報を特定
S1010
ｱｸｾｽ可能な実ﾕｰｻﾞ名/ｸﾞﾙｰﾌﾟ名より実ﾎﾟﾘｼｰを特定
S1011
実ﾎﾟﾘｼｰをﾎﾟﾘｼｰ変換要求者へ送信
S1012
ｱｸｾｽ権確認要求?
S1013
指定された仮想ﾎﾟﾘｼｰに設定されているｱｸｾｽ権を取得
S1014
要求されたｱｸｾｽ権がｱｸｾｽ権確認者に付与されているか確認
S1015
確認結果をｱｸｾｽ権確認者へ送信
S1016

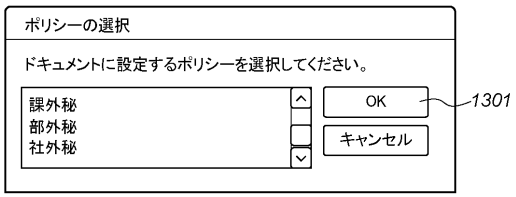
【図１１】



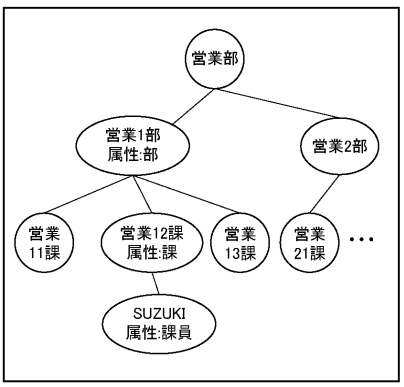
【図１２】



【図１３】



【図１４】



【図１５】

(a)

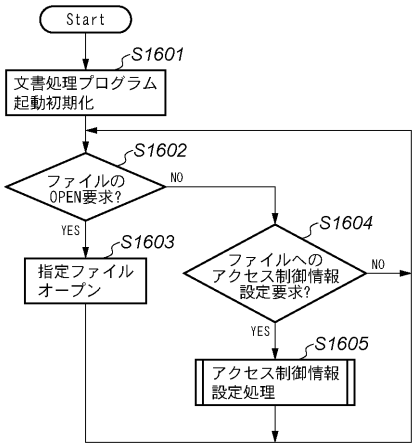
アクセスの種類＼ユーザ・グループ	ポリシー設定者《可変》	ポリシー設定者所属部の部員《可変》	その他
閲覧	○	○	×
編集	○	×	×
印刷	○	○	×
送信(デバイス用途のみ)	○	○	×

営業1部の部員であるSUZUKIが
仮想ポリシー「部外秘」を選択した
場合の実ポリシーへの変換

(b)

アクセスの種類＼ユーザ・グループ	SUZUKI (ポリシー設定者)	営業1部 部員 (部員)	その他
閲覧	○	○	×
編集	○	×	×
印刷	○	○	×
送信(デバイス用途のみ)	○	○	×

【図１６】


Start
S1601
文書処理プログラム
起動初期化
S1602
ファイルの
OPEN要求?
NO
YES
S1603
指定ファイル
オープン
S1604
ファイルへの
アクセス制御情報
設定要求?
NO
YES
S1605
アクセス制御情報
設定処理

フロントページの続き

審査官　池田　聡史

(56)参考文献　特開２００５－０３８３７１（ＪＰ，Ａ）
特開２００５－３３９５０６（ＪＰ，Ａ）
特開２００１－１１７８０３（ＪＰ，Ａ）

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