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

特許第4835111号
(P4835111)

(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 21/24	(2006.01)	G06F	12/14	520A
H04L 9/10	(2006.01)	G06F	12/14	540B
H04L 9/08	(2006.01)	H04L	9/00	621A
H04N 1/00	(2006.01)	H04L	9/00	601F
H04N 1/44	(2006.01)	H04N	1/00	107Z

請求項の数 2　(全 16 頁)　最終頁に続く

(21)出願番号　特願2005-319180 (P2005-319180)
(22)出願日　平成17年11月2日 (2005.11.2)
(65)公開番号　特開2007-128207 (P2007-128207A)
(43)公開日　平成19年5月24日 (2007.5.24)
審査請求日　平成20年10月22日 (2008.10.22)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　益井　隆徳
神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内

審査官　戸島　弘詩

最終頁に続く

(54)【発明の名称】ジョブ処理システム及び画像読取装置

(57)【特許請求の範囲】
【請求項１】
指示書提供装置と、画像読取装置とを有するジョブ処理システムであって、
指示書提供装置は、
読取指示と、該読取指示によって読み取られた画像を示す電子文書ファイルに対する操作制限を示すデータと、１以上の前記操作制限を解除できるフルアクセス権限者の公開鍵証明書のデータとを含んだ指示書データを記憶する記憶手段と、
記憶手段に記憶された指示書データの中から選択された指示書データを画像読取装置に提供する提供手段と、
を備え、
画像読取装置は、
指示書提供装置の提供手段から提供された指示書データから操作制限を示すデータとフルアクセス権限者の公開鍵証明書を示すデータとを検出する手段と、
前記提供された指示書データの読取指示に応じて原稿を読み取って得た画像を示す電子文書ファイルに対し、指示書データから操作制限のデータが検出された場合はそのデータに応じて操作制限を設定し、指示書データからフルアクセス権限者の公開鍵証明書のデータが検出された場合は、検出された公開鍵証明書のリストを作成し、作成したリストの中から選択された公開鍵証明書に応じてフルアクセス権限者を設定する手段と、
を備える、ことを特徴とするジョブ処理システム。
【請求項２】

指示書提供装置の提供手段から提供された指示書データから操作制限を示すデータとフルアクセス権限者の公開鍵証明書を示すデータとを検出する手段と、
前記提供された指示書データの読取指示に応じて原稿を読み取って得た画像を示す電子文書ファイルに対し、指示書データから操作制限のデータが検出された場合はそのデータに応じて操作制限を設定し、指示書データからフルアクセス権限者の公開鍵証明書のデータが検出された場合は、検出された公開鍵証明書のリストを作成し、作成したリストの中から選択された公開鍵証明書に応じてフルアクセス権限者を設定する手段と、
を備える画像読取装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル複合機やデジタル複写機、ネットワークスキャナなどの画像読取装置に関し、特に読み取った画像のファイルに対し操作制限の情報を設定できる画像読取装置に関する。
【背景技術】
【０００２】
特許文献１には、複合機等のクライアントからサーバに指示書データを送り、サーバに対しその指示書データに記述された処理を実行させるシステムが示される。また、この文献には、サーバ同士の間で指示書データを受け渡すことで、クライアントが要求する処理を複数のサーバで連携して処理する仕組みも示され、更に指示書データをその宛先となるサーバの公開鍵で暗号化する点が示される。
【０００３】
また特許文献２に示される原稿読取端末装置は、スキャンした原稿が指示書であるか、その指示書の示す処理の対象である文書であるかを判定し、指示書である場合は、指示書の後に続いて読み取った文書のスキャンデータを指示書中に指定された格納先に格納する。
【０００４】
一方、近年、米国アドビ・システムズ社が開発したのPDF(Portable Document Format)や富士ゼロックス株式会社が開発したXDWフォーマットのように、印刷禁止や編集禁止などといった操作制限の情報をファイル中に持たせることができるファイルフォーマットが普及している。例えば、アドビ社のアプリケーションソフトウエアAcrobat（登録商標）は、ＵＩ（ユーザインタフェース）画面から、PDFファイルに対して操作制限を指定することができる。編集ソフトウエアは、操作制限が加えられた電子文書ファイルを開いた場合、その操作制限の範囲内でしかユーザからの操作を認めない。したがって、例えば配布文書のフォーマットとしてPDFやXDW等を採用すれば、配布者の意図した範囲内でしか利用できない電子文書を作成し、配布することができる。
【０００５】
またPDFやXDW等のフォーマットでは、操作制限の例外として、ファイルに対するフルアクセス権限者を指定することができる。フルアクセス権限者は、当該ファイルの操作権限の設定を変更することができる。このフルアクセス権限者を識別するために、PKI（公開鍵基盤）技術が利用されている。すなわち、PDFやXDW等のファイルには、ファイル作成者から指定されたフルアクセス権限者の主体者DN(Distinguished Name: 識別名）がその権限者の公開鍵で暗号化された状態で組み込まれる。フルアクセス権限者は、自らの秘密鍵を用いてファイル中のフルアクセス権限者の主体者DNを正しく復号することができ、その主体者DNがその権限者自身のDNの一致しているので、編集アプリケーションからそのファイルのフルアクセス権限者として正しく認識される。このような仕組みにおいて、PDF等の電子文書ファイルに対してフルアクセス権限者を設定する場合、そのフルアクセス権限者の主体者DNや公開鍵を示した公開鍵証明書が必要となる。
【０００６】
近年の複合機等の画像読取装置には、スキャンした原稿のスキャン画像データをPDF等

の電子文書ファイルにし、指定された配布先に電子メール等で配布したり、ネットワーク経由で配布サーバに登録したりする機能を持つものが増えている。この種の画像読取装置においてスキャン画像の電子文書ファイルに対して操作制限を設定するには、コントロールパネルにある数字キーや、液晶タッチパネル上に表示されるソフトキーボードやＧＵＩ（グラフィカルユーザインタフェース）ボタンなど、パーソナルコンピュータよりも貧弱な入力装置から入力する必要があり、ユーザにとって作業が煩雑になるという問題がある。

【０００７】

また、スキャン画像の電子文書ファイルに対するフルアクセス権限者を画像読取装置上で設定する場合、画像読取装置がそのフルアクセス権限者の公開鍵証明書を持っているか、或いはネットワークを介してその公開鍵証明書を入手できる必要がある。

【０００８】

ところが、スキャンしたユーザが指定しようとするフルアクセス権限者の公開鍵証明書が画像読取装置内に必ず存在するようにメンテナンスすることは現実問題として困難である。特に、コンビニエンスストアなどに設置された画像読取装置のように、不特定多数の人が利用する画像読取装置の場合、ユーザが必要とする公開鍵証明書がその装置内にあることは一般に期待できない。

【０００９】

かといって、フルアクセス権限者の公開鍵証明書をネットワーク上のディレクトリサーバから画像読取装置にダウンロードするアプローチをとったとしても、次のような問題が生じる。すなわち、ディレクトリサーバで必要な公開鍵証明書を検索してダウンロードする場合、ディレクトリサーバのアクセス認証を受ける必要があるが、そのためのユーザＩＤや認証情報を画像読取装置のコントロールパネルから入力するのでは操作が煩雑である。また、アクセス認証に合格した場合でも、必要な公開鍵証明書を特定するための検索条件を更に入力する必要があり、画像読取装置からそのような情報を入力するのはユーザにとって負担が大きい。

【００１０】

特許文献１及び２は、画像読取装置でスキャンした文書のファイルを配布することを想定しているが、このような文書ファイルへの操作制限についての設定を画像読取装置のＵＩ機構から行うときのユーザの操作負担については考察していない。

【００１１】

【特許文献１】特開２００４－１５３４７２号公報

【特許文献２】特開２００５－２１７６６３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

本発明は、複合機等の画像読取装置でスキャンしたスキャン画像のファイルに対し操作制限の設定を行う際の、ユーザの入力操作負担を軽減する仕組みを提供する。

【課題を解決するための手段】

【００１３】

本発明の一つの側面では、指示書提供装置と、画像読取装置とを有するジョブ処理システムであって、指示書提供装置は、読取指示と、該読取指示によって読み取られた画像を示す電子文書ファイルに対する操作制限を示すデータと、１以上の前記操作制限を解除できるフルアクセス権限者の公開鍵証明書のデータとを含んだ指示書データを記憶する記憶手段と、記憶手段に記憶された指示書データの中から選択された指示書データを画像読取装置に提供する提供手段と、を備え、画像読取装置は、指示書提供装置の提供手段から提供された指示書データから操作制限を示すデータとフルアクセス権限者の公開鍵証明書を示すデータとを検出する手段と、前記提供された指示書データの読取指示に応じて原稿を読み取って得た画像を示す電子文書ファイルに対し、指示書データから操作制限のデータが検出された場合はそのデータに応じて操作制限を設定し、指示書データからフルアクセ

ス権限者の公開鍵証明書のデータが検出された場合は、検出された公開鍵証明書のリストを作成し、作成したリストの中から選択された公開鍵証明書に応じてフルアクセス権限者を設定する手段と、を備えるシステムを提供する。

【００１４】

参考例では、指示書提供装置と、画像読取装置とを有するジョブ処理システムであって、指示書提供装置は、指示書データを記憶する記憶手段であって、一以上の公開鍵証明書のデータを含んだ証明書リポジトリ指示書データを少なくとも記憶する記憶手段と、記憶手段に記憶された指示書データの中から選択された指示書データを画像読取装置に提供する提供手段と、を備え、画像読取装置は、指示書提供装置の提供手段から提供された証明書リポジトリ指示書データに含まれる公開鍵証明書のリストを該画像読取装置の表示画面に表示し、該リストの中からユーザの使用する公開鍵証明書の選択を受け付ける手段と、原稿を読み取って得た画像を示す電子文書ファイルに対し、選択された公開鍵証明書を用いて暗号化又はフルアクセス権限者の設定を行う手段と、を備えるシステムを提供する。

【発明を実施するための最良の形態】

【００１５】

以下、図面を参照して、本発明の実施の形態について説明する。

【００１６】

図１は、本発明に係るジョブ処理システムの概略構成を示す図である。図に示すように、このシステムでは、複合機１０，ＰＣ（パーソナルコンピュータ）２０，指示書プールサーバ３０，及びファイルサーバ４０が、インターネットやＬＡＮ（ローカルエリアネットワーク）などのネットワーク５０に接続されている。

【００１７】

複合機１０は、スキャナ、プリンタ、コピー機等の機能を兼ね備えた装置であり、与えられた指示書データに示される処理を実行するための機能を備える。複合機１０において、画像読取部１２は、自動原稿送り装置やプラテンなどにセットされた紙原稿を読み取るための機構である。ファイル作成部１４は、画像読取部１２が読み取った原稿の画像を含んだ、PDFやXDW等の所定の電子文書ファイル形式のファイルを作成する手段である。指示書実行部１６は、与えられた指示書データを解釈して、そこに示された指示内容を実行するための手段であり、典型的にはソフトウエアにより実現される。指示書データの解釈とそれに基づく処理の実行については、特許文献１に詳しく説明されているので、ここでは詳細な説明は省略する。

【００１８】

ＰＣ２０は、ユーザが使用するコンピュータであり、指示書データを作成するための指示書エディタ２２がインストールされている。

【００１９】

指示書プールサーバ３０は、各ユーザが作成した指示書データが登録されるサーバである。複合機１０は、指示書プールサーバ３０に登録された指示書データをダウンロードして実行することができる。

【００２０】

また、図１には、複合機１０がスキャンした画像から作成した電子文書ファイルの登録先の一例としてファイルサーバ４０を例示した。

【００２１】

複合機１０のファイル作成部１４は、スキャンした画像を示すPDF等の電子文書ファイルを作成する際に、そのファイルに対する操作制限を設定する機能を備える。例えば、そのファイルの印刷を禁止したり、編集を禁止したりするなどの操作制限である。また、ファイル作成部１４は、ファイルに対して設定された操作制限を解除できるフルアクセス権限者を設定する機能を備える。

【００２２】

この実施の形態では、このような操作制限やフルアクセス権限者の設定のために、指示

書データを利用することで、そのような設定を行うユーザの操作負担を軽減する。

【００２３】

この実施の形態における、ファイルへの操作制限やフルアクセス権限者の設定指示を含んだ指示書データ６０の一例を図２に示す。

【００２４】

図２の指示書データ６０は、指示書名称６２と、ジョブ内容記述６４を含んでいる。指示書名称６２は、"<NAME>"というタグの後に続いて記述された文字列であり、ユーザが各指示書を識別するために用いられる。ジョブ内容記述６４は、その指示書により指定される処理すなわち「ジョブ」の内容を示す記述であり、そのジョブのタイプを示す"JobType"の記述を含む。この例でのジョブタイプ"ScanToServer"は、画像読取部１２でスキャンした画像を電子文書ファイルとしてサーバに登録するジョブを示す。ジョブタイプの記述の後には、そのジョブのパラメータが記述される。パラメータ"Server"は、作成した電子文書ファイルを登録するサーバ（例えばファイルサーバ４０）のネットワーク５０上での識別情報である。パラメータ"Account"は、そのサーバに対してファイルを登録するためのアカウントを示す情報であり、例えばユーザ名とパスワードの組がその一例である。パラメータ"Scan File Format"は、作成する電子文書ファイルのファイル形式であり、XDWやPDF形式が選択肢となる。

【００２５】

パラメータ"Scan File Security"６６は、スキャン画像の電子文書ファイルに対するセキュリティ設定内容を示すパラメータであり、"Restriction"及び"FullAccessUser"という詳細パラメータを含む。"Restriction"は、当該ファイルに対する操作制限の内容を示すパラメータであり、"NO-Print"は「印刷禁止」、"NO-Edit"は「編集禁止」を示す。

【００２６】

また"FullAccessUser"は、その操作制限が解除できる特別の権限者であるフルアクセス権限者の識別情報である。この例では、フルアクセス権限者の識別情報として、X.509証明書などで用いられるDN(Distinguished Name: 識別名）を用いている（DNは比較的長い記述となり、図にそのまま示すと煩雑なので、図では簡略化して表現している）。また、フルアクセス権限者の記述に続き、その権限者の公開鍵証明書データ６８が付加されている。この公開鍵証明書データ６８は、複合機１０でフルアクセス権限者の設定をする際に用いられる。

【００２７】

図２に例示した指示書データは、スキャンした画像のファイルを指定されたサーバへ登録する処理を示したものであったが、スキャンを伴う処理としては、この他に、スキャン画像のファイルを指定された宛先に電子メールで送信する場合がある。この場合、指示書データには、パラメータとして、サーバのアドレスやアカウントに代えて、宛先の電子メールアドレスが記述される。また、宛先の公開鍵でそのファイルを暗号化する場合は、その宛先の公開鍵証明書が指示書データに組み込まれる。

【００２８】

ユーザは、ＰＣ２０にインストールされた指示書エディタ２２を用いて、このような指示書データを編集する。図３に、指示書エディタ２２のユーザインタフェース画面の表示例を示す。この画面は、ＰＣ２０のディスプレイ装置に表示される。

【００２９】

このユーザインタフェース画面は、部品ウインドウ１００と組み立てウインドウ１１０を有する。部品ウインドウ１００には、ジョブの構成要素となる単位処理を示すアイコン１０２，１０４，１０６が示される。図示例では、スキャン関連のジョブの要素アイコンのみを示している。組み立てウインドウ１１０には、必要な要素アイコン１０２，１０４，又は１０６を部品ウインドウ１００から例えばドラッグ・アンド・ドロップ操作で配置する。組み立てウインドウ１１０内に複数の要素アイコンに配置し、それらを矢印で結ぶなどの操作でその実行順序を規定することで、複数の単位処理の系列としてのジョブを定義できる。図示例では、「スキャン」アイコン１１２の後に「サーバへ登録」アイコン１

１４を繋げることで、原稿をスキャンしてサーバに登録するというジョブを定義している。

【００３０】

そして、組み立てウインドウ１１０に配置したアイコン１１２又は１１４をクリック操作などで選択することで、それら各アイコンに対応する個々の単位処理についての処理パラメータを設定する設定画面が呼び出される。図示例では、スキャン処理のパラメータ設定画面１２０を例示している。

【００３１】

この画面１２０には、スキャン画像を格納する電子文書のファイル形式の指定欄１２２と、そのファイルに対するセキュリティ設定の欄１３０が含まれる。ファイル形式の指定欄１２２は、XDW形式またはPDF形式のいずれか一方がラジオボタンで指定できるようになっている。

【００３２】

図示例では、セキュリティ設定の欄１３０には、ファイル暗号化要否の指定欄１３２，操作制限の指定欄１３４及びフルアクセス権限者の設定欄１３６が含まれる。ファイル暗号化要否の指定欄１３２には、暗号化を「する」又は「しない」ことを指示するためのＧＵＩボタンが示される。暗号化は、公開鍵暗号方式を想定している。すなわち、そのファイルの提供先であるユーザの公開鍵による暗号化である。クリック操作などで「しない」ボタンが選択されると、指示書はファイルの暗号化の指示を含まないものとなる。「する」ボタンが選択されると、ファイルの提供先となるユーザの公開鍵証明書の指定を受け付けるための画面（図示省略）が表示される。この画面には、ＰＣ２０内にインストールされた公開鍵証明書のリストや、ディレクトリサーバにアクセスして公開鍵証明書を検索するための検索条件入力欄が示される。そして、指示書の作成者は、インストールされている公開鍵証明書のリスト、又はディレクトリサーバで検索された公開鍵証明書のリストのなかから、ファイルの提供先とするユーザの公開鍵証明書を一以上選択すると、それら選択された公開鍵証明書が暗号化のための鍵を含む情報として指示書データに組み込まれる。なお、図２は、ファイルの暗号化を行わない場合を示した。

【００３３】

操作制限の指定欄１３４には、図示例では、「印刷許可」と「編集許可」の２つの項目についてのチェックボックスが示される。すなわち、この例は、デフォルトでは印刷も編集も禁止の場合を想定したものである。指示書作成者は、ファイルの印刷を認める場合は「印刷許可」のチェックボックスに、編集を認める場合は「編集許可」のチェックボックスに、マウスのクリック操作等でチェックマークを入れればよい。操作に対応するチェックボックスにマーキングがされなければ、その操作は禁止状態のままとなる。

【００３４】

フルアクセス権限者の設定欄１３６には、フルアクセス権限者の設定を「する」又は「しない」ことを指示するためのＧＵＩボタンが示される。「しない」ボタンが選択されると、指示書にはフルアクセス権限者は設定されない。「する」ボタンが選択されると、フルアクセス権限者とするユーザの公開鍵証明書の指定を受け付けるための画面（図示省略）が表示される。この画面には、暗号化のための公開鍵証明書の指定画面と同様、ＰＣ２０にインストールされている公開鍵証明書のリストや、ディレクトリサーバからの公開鍵証明書を検索するための画面が示される。そのリストや検索結果から指示書作成者がフルアクセス権限者とする一人以上の人の公開鍵証明書を選択すると、その公開鍵証明書が指示書データの中に組み込まれる。

【００３５】

以上、「スキャン」ボタン１１２がクリックされた場合を例に取ったが、「サーバへ登録」ボタン１１４がクリックされた場合も、同様にパラメータ（例えば登録先サーバのアドレスや、それに登録するユーザのアカウント情報など）の設定画面が表示され、その画面に対して設定された内容をもとに指示書データが作成される。

【００３６】

指示書エディタ２２は、以上のような指示書作成者からの指示に応じて指示書データを作成する。この手順を、図４を参照して説明する。

【００３７】

この手順では、まず指示書エディタ２２は、指示書作成者から操作制限の指示があるかどうかを判定する（Ｓ１）。図３に例示したパラメータ設定画面１２０の例では、デフォルトは印刷及び編集の全ての操作が禁止されており、指示書作成者が特に許可する操作をチェックボックスで指示する方式だった。したがって、「印刷許可」又は「編集許可」の両方が共にチェックされた場合だけは、操作に対する制限がない状態となるのでステップＳ１の判定結果は否定（ＮＯ）となり、それ以外の場合はいずれか操作に対し制限が残った状態となるので、この判定の結果は肯定（ＹＥＳ）となる。

【００３８】

操作制限がある場合、指示書エディタ２２は指示書データ中にその操作制限の記述を加える（Ｓ２）。図２の指示書データ例で言えば、例えば印刷禁止及び編集禁止の両方の制限が残っていれば、指示書データの"Scan File Security"の欄に、"Restriction: NO-Print, NO-Edit"の記述が追加される。

【００３９】

なお、操作制限の指定がない場合は、指示書エディタ２２は、セキュリティ関連以外のジョブ関連の指示内容についてのデータを指示書データに設定する（Ｓ７）。例えば、組み立てウインドウ１１０上で「スキャン」アイコン１１２と「サーバへ登録」アイコン１１４がこの順に順序づけられた場合、指示書エディタ２２は、指示書データに対し、ジョブタイプを示すタグ"<JobType>"に続き"ScanToServer"の文字列を追加する。また、指示書エディタ２２は、登録先のサーバのアドレスや、そのサーバにログインするためのアカウント情報の記述も追加する。また、図示は省略したが、指示書名の入力欄に対して作成者から名称の文字列が入力されると、その文字列を"<NAME>"タグの右側に続いて記述する。また、指示書エディタ２２はスキャン画像のファイル形式の記述を指示書データに追加する。

【００４０】

さて、ステップＳ２で操作制限のデータを指示所内に設定すると、次に指示書エディタ２２は、指示書作成者からフルアクセス権限者の指定があるかどうかを判定する（Ｓ３）。

【００４１】

フルアクセス権限者の指定がなければ、ステップＳ７に進み、ジョブ関連の指示内容を指示書に追加する。

【００４２】

フルアクセス権限者が指定されている場合、そのフルアクセス権限者の公開鍵証明書を取得し、検証する（Ｓ４）。この検証は、その証明書が信用できるものか、現在も有効であるかを確かめるために行う。すなわち、証明書の認証パス検証や、証明書に示された有効期間のチェック、失効リストに載っているか否かのチェックなどを行う。もちろん、これらの全てを行う必要は必ずしもなく、システムに要求されるセキュリティの程度と処理負荷とのバランスに応じて適切な検証処理を行えばよい。フルアクセス権限者が複数指定されている場合は、各フルアクセス権限者についてその検証を実行する。

【００４３】

ステップＳ５では、その検証の結果を判定する。指定されたフルアクセス権限者の公開鍵証明書が全て有効と判定した場合、指示書エディタ２２は、各フルアクセス権限者の識別名(DN)と公開鍵証明書データとを指示書データ内に組み込む（Ｓ６）。そして、ステップＳ７に進み、ジョブ関連の指示内容を指示書に追加する。

【００４４】

なお、ステップＳ５で、指定されたフルアクセス権限者のうちのいずれかの公開鍵証明書が有効でないと判定した場合、指示書エディタ２２は、所定のエラー表示を行う（Ｓ８）。エラー表示は、例えば、有効でない公開鍵証明書が指定されたことを示すメッセージ

を表示したものでよい。

【００４５】

なお、以上の例では、指定されたフルアクセス権限者のうちの一人でも公開鍵証明書が無効であればエラーとしたが、この代わりに、公開鍵証明書が有効であるフルアクセス権限者のみの識別名及び公開鍵証明書を指示書データ中に組み込む処理としてもよい。

【００４６】

また、以上の例では暗号化について言及しなかったが、仮にパラメータ設定画面１２０（図３参照）の暗号化要否の指定欄１３２で暗号化が選択され、ファイルの提供先ユーザの公開鍵証明書が指定された場合、指示書エディタ２２は、そのファイルを暗号化の設定情報（例えば暗号アルゴリズムの指定など）と、その公開鍵証明書とを指示書データ中に組み込む。

【００４７】

以上のようにして指示書エディタ２２で作成された指示書データは、例えばネットワーク５０を介して所定の指示書プールサーバ３０に登録される。

【００４８】

指示書プールサーバ３０は、登録された各指示書データをユーザからの要求に応じて提供する。この提供において、指示書プールサーバ３０は、ユーザのアクセス権管理を行う。すなわち、指示書作成者や指示書を利用するユーザは、指示書プールサーバ３０に対しアカウントが登録され、指示書作成者は自らが作成し登録した指示書データに対するアクセス権を指示書プールサーバ３０に対して設定できる。アクセス権は、ユーザ単位で付与したり、グループ単位で付与したりすることができる。各指示書データに対するアクセス権の情報は周知のアクセス制御リスト（ＡＣＬ）などとして指示書プールサーバ３０で管理される。指示書プールサーバ３０は、ユーザからアクセスを受けた場合、そのユーザを認証し、認証が成功するとそのユーザがアクセス権を持つ指示書のリストをＡＣＬに基づき作成し、そのリストをユーザに提供する。リストには、例えば、該当する各指示書の名称が列挙され、ユーザはこの名称のリストから所望の指示書を判別する。なお、指示書の名称に加え、作成者名や作成日時、その指示書のジョブタイプなどといった属性情報を併せて表示し、ユーザの判断に供するようにしてもよい。ユーザはそのリストの中から、自分が使いたい指示書を選択することができる。

【００４９】

この実施の形態では、ユーザが、原稿のスキャンのための指示書データを指示書プールサーバ３０から複合機１０にダウンロードし、使用する場合を考える。この場合の処理手順を図５に示す。

【００５０】

複合機１０の指示書実行部１６は、スキャンを含む処理を示した指示書データを取得し、ユーザからジョブ実行の指示を受けた場合、原稿自動送り装置又はプラテンにセットされた原稿のスキャンを画像読取部１２に実行させる（Ｓ１２）。スキャンの結果得られた画像は、ファイル作成部１４が、指示書データ中で指定されたファイル形式のファイル（スキャンファイルと呼ぶ）として作成する（Ｓ１３）。そして、指示書実行部１６は、指示書に操作制限の記述があるか否かを判定し（Ｓ１４）、なければ作成したスキャンファイルを指示書中に指定された宛先（サーバ、又は電子メールアドレス）に転送する（Ｓ２１）。

【００５１】

操作制限の記述があれば、指示書実行部１６は、スキャンファイルにその操作制限を設定するようファイル作成部１４に指示する（Ｓ１５）。ファイル作成部１４は、指定されたファイル形式のファイルに対する属性設定の機能を持っており、その機能を用いて操作制限（印刷禁止又は編集禁止又はその両方）の設定を行う。

【００５２】

そして、指示書実行部１６は、指示書の中にフルアクセス権限者の記述があるかどうかを確認し（Ｓ１６）、なければ、操作制限を設定したスキャンファイルを指定された宛先

に転送する（Ｓ２１）。指示書の中にフルアクセス権限者の記述がある場合は、その指示書に内包されたその権限者の公開鍵証明書データ６８を取得し（Ｓ１７）、その証明書データ６８が有効であるかを検証する（Ｓ１８）。このステップでは、認証パスの検証や有効期間の検証、失効リストのチェックなどのうち所定のものを実行すればよい。そして、その検証の結果、証明書データ６８が有効であるか否かを判定し（Ｓ１９）、有効と判定されれば、指示書実行部１６は、ファイル作成部１４に命じて、そのフルアクセス権限者をスキャンファイルに設定させる（Ｓ２０）。この命令を受けたファイル作成部１４は、そのフルアクセス権限者の公開鍵証明書に示される識別名(DN)を、その公開鍵証明書に含まれる公開鍵で暗号化し、その暗号化された識別名をスキャンファイルの属性情報の１つであるフルアクセス権限者リストに登録する。そして、このようにフルアクセス権限者が設定されたスキャンファイルを、指定された宛先に転送する（Ｓ２１）。

【００５３】

なお、ステップＳ１９で証明書データ６８が有効でないと判定されれば、指示書実行部１６は、公開鍵証明書が有効でない旨のメッセージなどを含んだエラー表示を、複合機１０の表示装置に対して行う（Ｓ２２）。

【００５４】

なお、１つの指示書データの中にフルアクセス権限者が複数指定されている場合は、指定されたフルアクセス権限者ごとにその公開鍵証明書が有効か否かを判定し（Ｓ１９）、有効であればその人をスキャンファイルのフルアクセス権限者リストに登録すればよい（Ｓ２０）。ここで、指示書データ中に指定されたフルアクセス権限者の中に公開鍵証明書が有効でなくなっている人がいれば、その人はスキャンファイルのフルアクセス権限者リストに登録しない。また、別の方法として、指示書データ中のフルアクセス権限者の中に一人でも公開鍵証明書が有効でなくなっている人がいれば、スキャンファイルの転送（Ｓ２１）は行わずにエラー表示（Ｓ２２）を行うようにしてもよい。

【００５５】

このようにして操作制限又はフルアクセス権限者又はその両方が設定されたスキャンファイルは、そのスキャンファイルを閲覧するための閲覧ソフトウエアや、編集のための編集ソフトウエアによって開くことができる。このとき、そのソフトウエアを使用するユーザが、そのファイルに設定されたフルアクセス権限者であれば、そのユーザのＰＣ内にあるそのユーザの秘密鍵によりフルアクセス権限者リスト中の当該ユーザの識別名が復号でき、復号された識別名が当該ユーザの識別名と一致する。そこで、そのソフトウエアは、そのユーザがフルアクセス権限者であると認識し、当該ファイルに設定されている操作制限の解除を許可する。

【００５６】

図５の手順では、指示書データにスキャンファイルの暗号化についての設定がある場合を考慮していなかった。これを考慮するとするならば、指示書実行部１６は、指示書中で暗号化が指示されていれば、ファイル作成部１４に命じてスキャンファイルの内容を暗号化させる。このときファイル作成部１４は、例えばセッション鍵を（例えばランダムに）生成し、そのセッション鍵により共通鍵暗号方式でスキャンファイルの内容を暗号化すると共に、指示書中に組み込まれた暗号化のための公開鍵証明書に示された公開鍵でそのセッション鍵を暗号化し、これを暗号化されたスキャンファイルに組み込む。暗号化のための公開鍵証明書が指示書データ中に複数指定されている場合は、個々の証明書の公開鍵でそれぞれセッション鍵を暗号化したものをリストとしてスキャンファイルに組み込めばよい。スキャンファイルを取得したユーザは、自分の秘密鍵でスキャンファイル中の暗号化されたセッション鍵のうちの１つが復号できれば、そのセッション鍵を用いてスキャンファイルの内容を復号できる。

【００５７】

以上に説明した実施の形態によれば、スキャンファイルの作成を指示する指示書データの中に、そのスキャンファイルに対する操作制限が記述されているので、ユーザは適切な指示書データを複合機１０に入力して実行させればよく、複合機１０のユーザインタフェ

ース画面から細かな操作制限の設定を行わずに済む。

【００５８】

また、指示書データ中にフルアクセス権限者の公開鍵証明書が含まれるので、複合機１０の中にフルアクセス権限者の公開鍵証明書がなくても、指示書データ中からそれを取得してスキャンファイルにフルアクセス権限者を設定できる。

【００５９】

また、この実施の形態では、指示書プールサーバ３０からダウンロードした指示書データにフルアクセス権限者の公開鍵証明書が含まれるので、フルアクセス権限者の公開鍵証明書をＬＤＡＰサーバ等のディレクトリサーバから検索して取得する場合より、操作が簡素化できる。すなわち、ディレクトリサーバから公開鍵証明書を検索する場合、ユーザは指示書を取得するために指示書プールサーバ３０の認証を受けるだけでなく、証明書検索のためにディレクトリサーバの認証も受ける必要がある。これら両者の認証のための認証情報は一般に異なるので、ユーザの操作負担は大きい。これに対し、この実施の形態によれば、ユーザは指示書プールサーバ３０の認証に合格するだけで、フルアクセス権限者の公開鍵証明書を含んだ指示書を取得できるので、認証のための操作負担は少ない。

【００６０】

以上の例では、スキャンファイルに対する操作制限として、印刷禁止及び編集禁止を例示したが、操作制限の内容はこれに限られるものではない。

【００６１】

また、以上の例では、スキャンファイルに「操作制限」を設定する場合を例示したが、この代わりに、当業者なら理解できるように、許可する操作項目を限定的に列挙した「操作権限」をスキャンファイルに設定する場合でも、上記実施の形態の処理は適用可能である。このようにファイルに対し操作制限を設定することも、操作権限を設定することも、技術的には等価である。ファイルに操作権限を設定した場合、フルアクセス権限者は、その操作権限の設定を変更できるユーザということになる。

【００６２】

以上に示した実施の形態は、スキャンファイルに対して操作制限やフルアクセス権限者の情報を組み込んだ指示書データについてのものであった。次に、指示書をユーザ固有の証明書リポジトリとして利用する場合の例について説明する。

【００６３】

証明書リポジトリとして用いられる指示書データの例を図６に示す。図示した指示書データ７０には、指示書名称７２と、証明書リポジトリ情報７４が含まれる。証明書リポジトリ情報７４には、その指示書に含まれる各公開鍵証明書７８と、それら各公開鍵証明書の主体者の識別名(DN)のリスト７６とが含まれる。

【００６４】

証明書エディタ２２は、証明書リポジトリを示す指示書の作成指示を受けた場合、公開鍵証明書を選択するために、ＰＣ２０にインストールされている公開鍵証明書のリストや、ディレクトリサーバからの公開鍵証明書を検索するための画面を表示する。ユーザが、そのリストや検索結果から指示書作成者がフルアクセス権限者や暗号化宛先とする一人以上の人の公開鍵証明書を選択すると、指示書エディタ２２は、その公開鍵証明書と識別名を証明書リポジトリ情報７４の中に含んだ指示書データを作成する。

【００６５】

ユーザは、自分がよく利用する公開鍵証明書を含んだ指示書データを作成し、指示書プールサーバ３０に登録しておくことで、後で複合機１０にその指示書データをダウンロードして、自分専用の公開鍵証明書リストとして表示装置に表示させて利用することができる。

【００６６】

このような証明書リポジトリの指示書は、ジョブ内容を指示する他の指示書と組み合わせて利用される。例えば、スキャン画像のファイルを暗号化する処理を示した指示書と組み合わせて用いられた場合、証明書リポジトリの指示書に含まれる公開鍵証明書のリスト

が、暗号化に用いる公開鍵（すなわち暗号化したファイルの提供先となるユーザ）の選択肢として利用される。また、スキャン画像のファイルに対して操作制限とフルアクセス権限者を設定する処理を示した指示書と組み合わせて用いられた場合、証明書リポジトリに含まれる公開鍵証明書のリストが、フルアクセス権限者の選択肢として利用される。

【００６７】

いずれの場合も、証明書リポジトリ情報７４は、ユーザにとってのいわばアドレス帳の役割を果たす。

【００６８】

以上では、ジョブ内容を示す指示書と証明書リポジトリを示す指示書とを組み合わせて用いると説明したが、ジョブ内容を示す指示書の中に、証明書リポジトリ情報７４（７６及び７８）を組み込んでもよい。

【００６９】

証明書リポジトリ情報７４を含んだ指示書を処理する際の複合機１０の処理手順を図７に示す。この例では、複合機１０にダウンロードされるのは、スキャン指示と証明書リポジトリ情報７４を含んだ指示書（それら両者が別の指示書となっていても良い）であるとする。

【００７０】

この手順では、複合機１０はユーザの選択した指示書を指示書プールサーバ３０から取得すると（Ｓ３１）、その指示書の中に証明書リポジトリ情報７４が含まれているかどうかを判定する（Ｓ３２）。証明書リポジトリ情報７４が含まれていなければ、指示書実行部１６は、単に、その指示書に示されたジョブ（この場合は原稿のスキャン）を実行する（Ｓ４１）。指示書にスキャンファイルの登録先や送信先が指定されていれば、指示書実行部１６はその指定に従ってスキャンファイルを登録又は送信する。

【００７１】

ステップＳ３２で指示書に証明書リポジトリ情報７４が含まれていると判定された場合、指示書実行部１６は、証明書リポジトリ情報７４に含まれる公開鍵証明書のリストを作成し、複合機１０の表示装置に表示する（Ｓ３３）。このリスト表示は、ユーザの要求に応じて呼び出されるようにすることも好適である。すなわち、例えば、表示装置の初期画面には、他の操作のためのＧＵＩボタンと共に証明書リストを呼び出すボタンを表示し、証明書リストのボタンが押下されると、公開鍵証明書のリストが画面表示するなどである。

【００７２】

なお、複合機１０には、その複合機１０を利用する複数のユーザで共有する共有のアドレス帳が登録されている場合があり、そのアドレス帳に各宛先ユーザの公開鍵証明書が登録されている場合がある。このような場合には、指示書中に含まれる公開鍵証明書のリストと、共有アドレス帳との両方を表示するようにしてもよい。

【００７３】

公開鍵証明書のリスト表示では、各公開鍵証明書の主体者の識別名或いはメールアドレス（これも証明書に含まれる）の一覧を表示すればよい。

【００７４】

ユーザは、このリスト表示の中から、対象となる１以上の公開鍵証明書を選択する（Ｓ３４）。この選択結果を受けた複合機１０の指示書実行部１６は、選択された公開鍵証明書を証明書リポジトリ情報７４又は共有アドレス帳から取得し、それが有効か否かを上述と同様の方法で検証する（Ｓ３５）。そして、その検証の結果、その証明書が有効か否かを判定する（Ｓ３６）。有効であれば、更に指示書がスキャンファイルの暗号化を指示するものであるか否かを判定し（Ｓ３７）、暗号化指示であれば、ステップＳ３４で選択された公開鍵証明書を暗号化結果の宛先として、ファイル作成部１４に設定する（Ｓ３８）。暗号化指示でなければ、ステップＳ３８はスキップする。また、指示書実行部１６は、指示書にフルアクセス権限者の設定が指示されているかどうかを判定し（Ｓ３９）、指示されている場合は、ステップＳ３４で選択された公開鍵証明書をフルアクセス権限者の情

報としてファイル作成部１４に設定する（Ｓ４０）。フルアクセス権限者設定が指示されていない場合は、ステップＳ４０はスキップする。

【００７５】

そして、指示書実行部１６は、画像読取部１２に原稿をスキャンさせ、得られたスキャン画像を示すスキャンファイルをファイル作成部１４に作成させる（Ｓ４１）。このとき、ステップＳ３８で暗号化宛先が設定されていれば、ファイル作成部１４は、その宛先の公開鍵証明書を用いて、スキャンファイルの内容を上述と同様の処理で暗号化する。また、ステップＳ４０でフルアクセス権限者が設定されていれば、その権限者の公開鍵証明書を用いて、そのスキャンファイルにフルアクセス権限者を設定する。

【００７６】

ステップＳ３６で公開鍵証明書が有効でないと判定された場合は、指示書実行部１６は、有効でない証明書が選択された旨のメッセージ等を示すエラー表示を、複合機１０の表示装置に表示し（Ｓ４２）、スキャンを行わずに処理を終了する。

【００７７】

なお、以上の例では、指示書にてスキャンファイルの暗号化又はスキャンファイルに対するフルアクセス権限者の設定のいずれかが指示される場合を例に取ったが、それらの両方が指示書中で指示されてももちろんよい。両方が指示された場合、ステップＳ３４では、暗号化ファイルの宛先の公開鍵証明書と、フルアクセス権限者の公開鍵証明書とをそれぞれ個別にユーザに選択させればよい。

【００７８】

また、以上の例では、ジョブ内容の指示と証明書リポジトリ情報７４とを含んだ指示書を複合機１０で処理する場合を例にとったが、ジョブ内容の指示は複合機１０のメニュー画面から行い、証明書リポジトリ情報７４だけ指示書から利用する場合も、上記と同様の処理が適用できる。

【００７９】

この例によれば、ユーザは、自分がよく使う公開鍵証明書からなる証明書リポジトリ情報７４を含んだ指示書データを作成し、指示書プールサーバ３０に登録しておくことで、どの複合機１０で原稿をスキャンしても、その指示書データをサーバ３０からダウンロードすれば、自分のよく使う公開鍵証明書をその指示書から取得して利用できる。

【００８０】

以上に説明した実施の形態及びその変形例では、指示書エディタ２２が作成した指示書データを指示書プールサーバ３０に登録し、ユーザが必要に応じそのサーバ３０から指示書をダウンロードして利用するという構成を例示した。しかしながら、ユーザが、指示書エディタ２２を用いて作成した指示書データをＵＳＢ(Universal Serial Bus)メモリ等の可搬型記録媒体に保存して携帯し、複合機１０がその媒体から指示書データを読み取って実行するシステム構成でも、上述と同様の仕組みが利用できる。

【００８１】

また、以上の例では、指示書エディタ２２は、ＰＣ２０にインストールされていたが、これに限らず、例えばアプリケーション・サービス・プロバイダがその指示書エディタ２２の機能をＰＣ２０にオンデマンドで提供するようにしてもよい。

【図面の簡単な説明】

【００８２】

【図１】実施の形態のシステム構成例を示す図である。

【図２】実施の形態の指示書データの例を示す図である。

【図３】指示書エディタのユーザインタフェース画面の一表示例を示す図である。

【図４】指示書エディタの処理手順を示すフローチャートである。

【図５】複合機がスキャン指示の指示書を処理する手順を示すフローチャートである。

【図６】証明書リポジトリ情報を含んだ指示書データの例を示す図である。

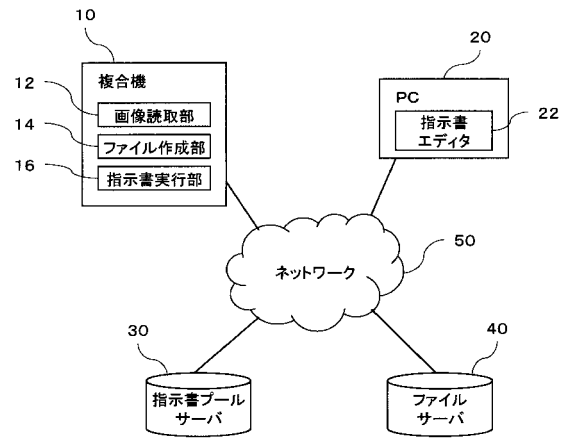
【図７】複合機が証明書リポジトリ情報を含んだ指示書データを処理する場合の処理手順を示すフローチャートである。

【符号の説明】

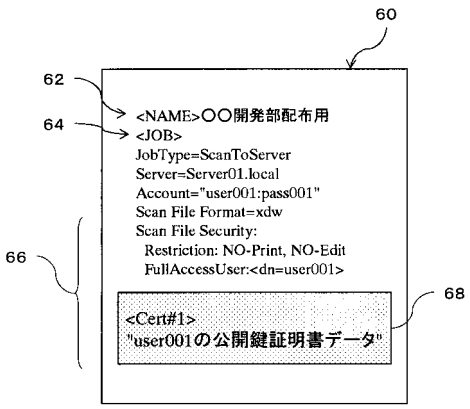
【００８３】

１０　複合機、１２　画像読取部、１４　ファイル作成部、１６　指示書実行部、２０　ＰＣ（パーソナルコンピュータ）、２２　指示書エディタ、３０　指示書プールサーバ、４０　ファイルサーバ、５０　ネットワーク。

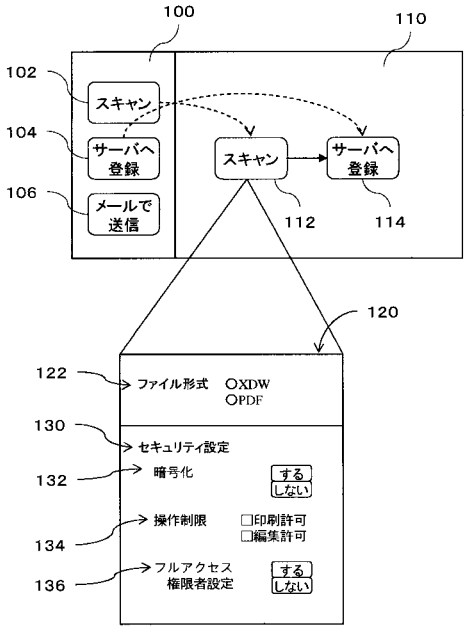
【図１】



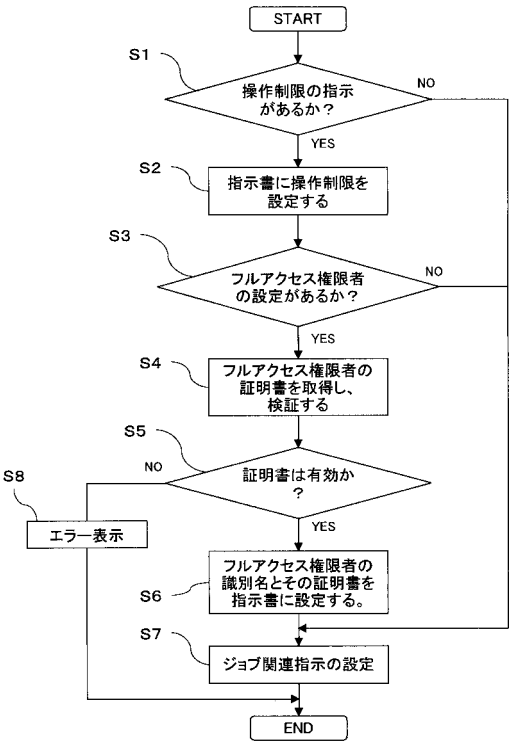
【図２】



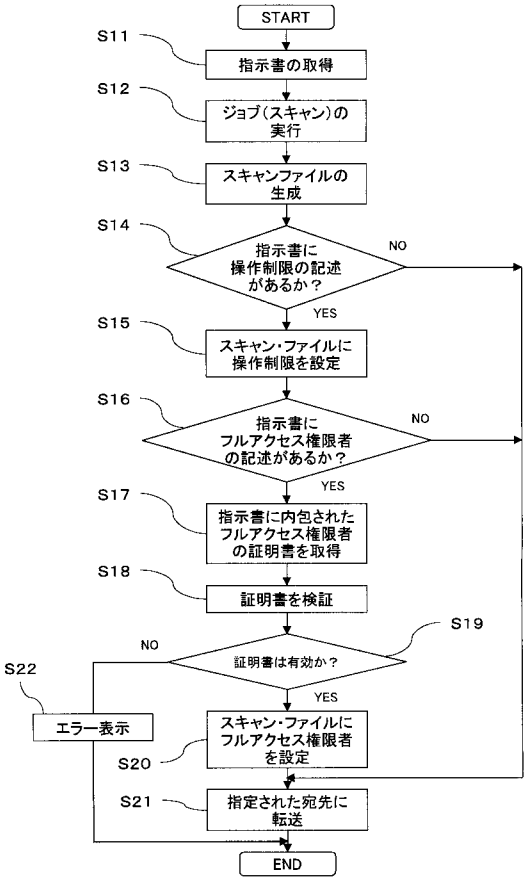
【図３】


100
110
102
スキャン
104
サーバへ登録
106
メールで送信
スキャン
サーバへ登録
112
114
120
122
ファイル形式 ○XDW ○PDF
130
セキュリティ設定
132
暗号化
する
しない
操作制限
□印刷許可
□編集許可
134
フルアクセス権限者設定
136
する
しない

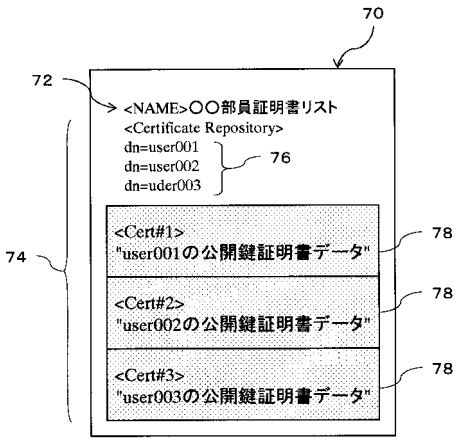
【図４】


START
S1
操作制限の指示があるか？
NO
YES
S2
指示書に操作制限を設定する
S3
フルアクセス権限者の設定があるか？
NO
YES
S4
フルアクセス権限者の証明書を取得し、検証する
S5
証明書は有効か？
NO
S8
エラー表示
YES
S6
フルアクセス権限者の識別名とその証明書を指示書に設定する。
S7
ジョブ関連指示の設定
END

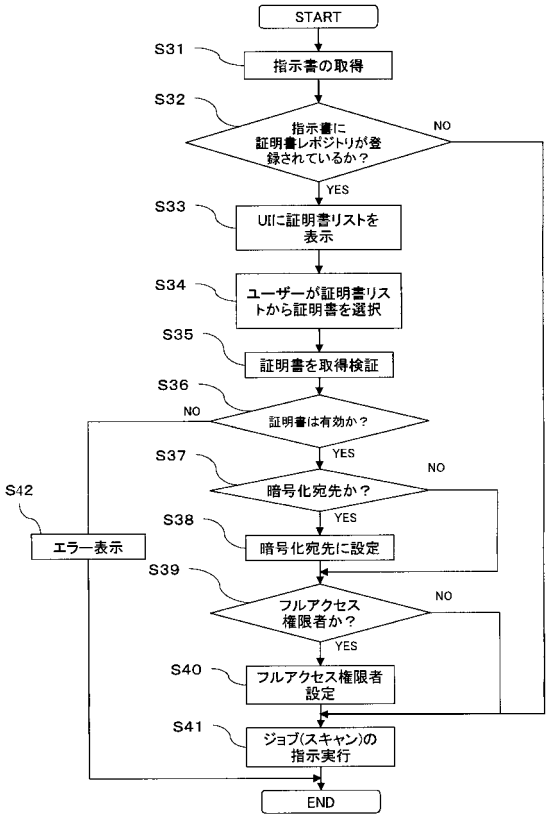
【図５】


START
S11
指示書の取得
S12
ジョブ(スキャン)の実行
S13
スキャンファイルの生成
S14
指示書に操作制限の記述があるか？
NO
YES
S15
スキャン・ファイルに操作制限を設定
S16
指示書にフルアクセス権限者の記述があるか？
NO
YES
S17
指示書に内包されたフルアクセス権限者の証明書を取得
S18
証明書を検証
S19
NO
証明書は有効か？
YES
S22
エラー表示
スキャン・ファイルにフルアクセス権限者を設定
S20
S21
指定された宛先に転送
END

【図６】


70
72
<NAME>○○部員証明書リスト
<Certificate Repository>
dn=user001
dn=user002
dn=uder003
76
74
<Cert#1>
"user001の公開鍵証明書データ"
78
<Cert#2>
"user002の公開鍵証明書データ"
78
<Cert#3>
"user003の公開鍵証明書データ"
78

【図７】


START
S31
指示書の取得
S32
指示書に
証明書レポジトリが登
録されているか？
NO
YES
S33
UIに証明書リストを
表示
S34
ユーザーが証明書リス
トから証明書を選択
S35
証明書を取得検証
S36
証明書は有効か？
NO
YES
S37
暗号化宛先か？
NO
YES
S42
エラー表示
S38
暗号化宛先に設定
S39
フルアクセス
権限者か？
NO
YES
S40
フルアクセス権限者
設定
S41
ジョブ(スキャン)の
指示実行
END

フロントページの続き

(51)Int.Cl.			FI		
G06F	*3/12*	*(2006.01)*	H04N	1/44	
G06F	*12/00*	*(2006.01)*	G06F	3/12	K
H04N	*1/21*	*(2006.01)*	G06F	12/00	537A
			H04N	1/21	

(56)参考文献 特開平11－110274（JP，A）
特開2005－275472（JP，A）
特開2004－289673（JP，A）
特開2004－289654（JP，A）
特開2004－287862（JP，A）
特開2005－011146（JP，A）
特開2003－179707（JP，A）
特許第4337698（JP，B2）
特開2002－041548（JP，A）
特開2005－092729（JP，A）
特開2004－032264（JP，A）
特開2004－247799（JP，A）
特開2005－149088（JP，A）
特開2004－310463（JP，A）
特開2002－269093（JP，A）
特開2004－288112（JP，A）
米国特許第06587129（US，B1）
米国特許第07516491（US，B1）
藤田 将幸，Ｗｉｎｄｏｗｓ Ｓｅｒｖｅｒでココまでできる！社内ＬＡＮセキュリティアップ講座，ＮＥＴＷＯＲＫ ＭＡＧＡＺＩＮＥ，株式会社アスキー，２００５年１０月２７日，第１０巻 第１２号，第１０５頁
山本 実香，企業内システムにおける電子証明書を用いたセキュリティ管理，第６１回（平成１２年後期）全国大会講演論文集（３）データベースとメディア ネットワーク，社団法人情報処理学会，２０００年１０月 3日，３－２０８頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／２４
Ｇ０６Ｆ３／１２，１２／００
Ｈ０４Ｎ１／００
Ｈ０４Ｎ１／２１