

(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2007-72605

(P2007-72605A)

(43) 公開日 平成19年3月22日(2007.3.22)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/20 (2006.01)	G06F 15/00 330D	5B017
G06F 12/00 (2006.01)	G06F 12/00 537D	5B082
G06F 21/24 (2006.01)	G06F 12/14 520B	5B285

審査請求 未請求 請求項の数 10 O L (全 13 頁)

(21) 出願番号	特願2005-256858 (P2005-256858)	(71) 出願人	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
(22) 出願日	平成17年9月5日(2005.9.5)	(74) 代理人	100076428 弁理士 大塚 康德
		(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	阿武 純 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
		Fターム(参考)	5B017 AA01 BA06 BB06 CA16
			最終頁に続く

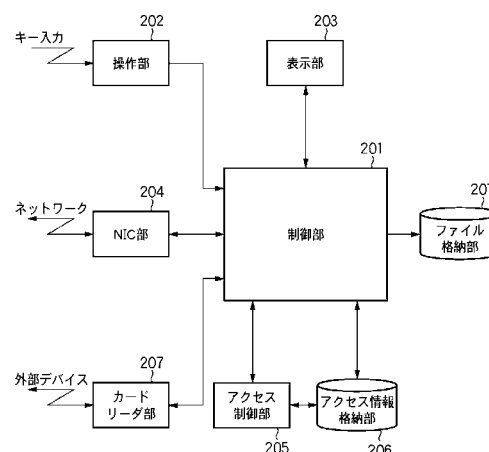
(54) 【発明の名称】 情報処理装置および情報処理方法

(57) 【要約】

【課題】 個人認証により各種オブジェクトへのアクセスを制御する情報処理装置において、当該オブジェクトのセキュリティを維持しつつ、当該オブジェクト使用時の利便性を向上させる。

【解決手段】 オブジェクトへのアクセスを制御する情報処理装置であって、複数のユーザが重複してログイン可能なログイン手段(207)と、前記ログイン手段(207)を介してログインした各ログインユーザがアクセス可能なオブジェクトを、該ログインユーザごとに表示領域をわけて表示する表示手段(203)と、前記表示手段(203)に表示された表示領域内のオブジェクトが、ユーザにより選択された場合に、該オブジェクトへのアクセスを行うアクセス手段(205)とを備える。

。 【選択図】 図2



【特許請求の範囲】**【請求項 1】**

オブジェクトへのアクセスを制御する情報処理装置であって、

複数のユーザが重複してログイン可能なログイン手段と、

前記ログイン手段を介してログインした各ログインユーザがアクセス可能なオブジェクトを、該ログインユーザごとに表示領域をわけて表示する表示手段と、

前記表示手段に表示された表示領域内のオブジェクトが、ユーザにより選択された場合に、該オブジェクトにアクセスするアクセス手段と
を備えることを特徴とする情報処理装置。

【請求項 2】

前記ログイン手段を介してログインした各ログインユーザがアクセス可能なオブジェクトと、該ログインユーザを特定するための識別子と対応付けたアクセス制御リストを保持する保持手段を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記表示手段は、

前記アクセス制御リストに基づいて、前記ログイン手段を介してログインした各ログインユーザがアクセス可能なオブジェクトを認識し、ログインユーザごとに表示領域をわけて表示することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

前記アクセス手段は、

前記表示手段により表示された表示領域内のオブジェクトが、ユーザにより選択された場合において、該選択されたオブジェクトが、該選択されたオブジェクトの属する表示領域のログインユーザによってアクセス可能なオブジェクトであるか否かを、前記アクセス制御リストに基づいて判断することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

オブジェクトへのアクセスを制御するための情報処理方法であって、

複数のユーザが重複してログイン可能なログイン工程と、

前記ログイン工程を介してログインした各ログインユーザがアクセス可能なオブジェクトを、該ログインユーザごとに表示領域をわけて表示する表示工程と、

前記表示工程に表示された表示領域内のオブジェクトが、ユーザにより選択された場合に、該オブジェクトへのアクセスを行うアクセス工程と
を備えることを特徴とする情報処理方法。

【請求項 6】

前記ログイン工程を介してログインした各ログインユーザがアクセス可能なオブジェクトと、該ログインユーザを特定するための識別子と対応付けたアクセス制御リストを保持する保持工程を更に備えることを特徴とする請求項 5 に記載の情報処理方法。

【請求項 7】

前記表示工程は、

前記アクセス制御リストに基づいて、前記ログイン工程を介してログインした各ログインユーザがアクセス可能なオブジェクトを認識し、ログインユーザごとに表示領域をわけて表示することを特徴とする請求項 6 に記載の情報処理方法。

【請求項 8】

前記アクセス工程は、

前記表示工程により表示された表示領域内のオブジェクトが、ユーザにより選択された場合において、該選択されたオブジェクトが、該選択されたオブジェクトの属する表示領域のログインユーザによってアクセス可能なオブジェクトであるか否かを、前記アクセス制御リストに基づいて判断することを特徴とする請求項 6 に記載の情報処理方法。

【請求項 9】

請求項 5 乃至 8 のいずれかに記載の情報処理方法をコンピュータによって実現させるための制御プログラムを格納した記憶媒体。

10

20

30

40

50

【請求項 10】

請求項 5 乃至 8 のいずれかに記載の情報処理方法をコンピュータによって実現させるための制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ファイルやフォルダ等の各種オブジェクトへのアクセスを制御する制御技術に関するものである。

【背景技術】

【0002】

近年、情報の安全性に対する関心の高まりに伴い、ファイルやフォルダ等の各種情報へのアクセスを制御するための制御技術が、様々な端末に取り込まれるようになってきている。

【0003】

MFP (Multi Function Peripheral) も例外ではなく、複写等の従来の基本機能に加え、原稿のスキャン、印刷、保存、表示等の各種機能が付加されたことに伴い、MFP が取得した各種情報へのアクセスの制御がますます重要になってきている。

【0004】

このため、最近の MFP には、例えば、MFP の操作を行う前に、個人の ID カードをリーダに読み込ませることで、個人認証を行う機能が備えられている。そして、個人認証に成功した場合にのみ、当該個人にアクセス権が付与されるよう構成されている。つまり、当該個人は当該アクセス権を用いることによってのみ、該 MFP が接続されるネットワーク上あるいは、MFP 内部のファイルやフォルダにアクセスし、該ファイルの閲覧・編集・送信などを行うことができる。

【0005】

このように、最近では MFP においてもパソコンのログインおよびアクセス制御と同様の仕組みが取り込まれるようになってきている。

【特許文献 1】特開 2004 - 110549 号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

一方、上述のように、MFP は原稿のスキャン、印刷、保存、表示等が可能であることから、今後は、パソコンを使わずにビジネス業務を遂行する際のツールとしての役割が求められている。

【0007】

例えば、MFP を会議室や打ち合わせスペース等のみんなが集まる場所に設置し、会議や打ち合わせの際に利用するツールとしての役割が考えられる。具体的には、当該 MFP から自由に文書やデータを取りだし、参加者に見えるように表示したり、当該表示結果について参加者が検討した結果をデータとして保存し、各参加者に配信するといった利用方法が考えられる。

【0008】

しかしながら、従来の MFP は、パソコンと同様、一人のみがログイン可能であり、当該ログインした個人のもつアクセス権の範囲内で、ネットワーク上あるいは MFP 内部のファイルやフォルダにアクセスができるにとどまっていた。

【0009】

このため、上述のような利用方法を実現しようとしても、参加者のうちの一人（ログインした人）以外の方は、自身のアクセス権が及ぶファイルやフォルダに、自由にアクセスすることができない。そのため、参加者全員が各々のファイルを持ち寄って検討したり、検討結果を各参加者の個人フォルダに保存したりといった処理を行うことができず、従来

10

20

30

40

50

のMF Pは、ビジネス業務を遂行するためのツールとして十分な役割を果たすことができなかった。そこで、このような利用方法にも対応できる、オブジェクトへのアクセス制御技術の実現が望まれている。

【0010】

本発明は上記課題に鑑みてなされたものであり、個人認証により各種オブジェクトへのアクセスを制御する情報処理装置において、当該オブジェクトのセキュリティを維持しつつ、当該オブジェクト使用時の利便性を向上させることを目的とする。

【課題を解決するための手段】

【0011】

上記の目的を達成するために本発明に係る情報処理装置は以下のような構成を備える。 10
即ち、

オブジェクトへのアクセスを制御する情報処理装置であって、

複数のユーザが重複してログイン可能なログイン手段と、

前記ログイン手段を介してログインした各ログインユーザがアクセス可能なオブジェクトを、該ログインユーザごとに表示領域をわけて表示する表示手段と、

前記表示手段に表示された表示領域内のオブジェクトが、ユーザにより選択された場合に、該オブジェクトへのアクセスを行うアクセス手段とを備える。

【発明の効果】

【0012】

本発明によれば、個人認証により各種オブジェクトへのアクセスを制御する情報処理装置において、当該オブジェクトのセキュリティを維持しつつ、当該オブジェクト使用時の利便性が向上する。 20

【発明を実施するための最良の形態】

【0013】

以下、必要に応じて添付図面を参照しながら本発明の各実施形態を詳細に説明する。なお、以下の実施形態では、本発明にかかる情報処理方法をMF P上で実現する場合について説明する（本発明にかかる情報処理装置を備えるMF Pを本発明の実施形態として説明する）。

【0014】

〔第1の実施形態〕 30

＜MF Pを備えるネットワークシステムの構成＞

図1は、本発明の第1の実施形態にかかるMF Pが接続されたネットワークシステムの構成例を示す図である。

【0015】

同図において、105～107はMF Pであり、102はファイルサーバである。また、108は認証サーバであり、103～104はクライアントPCである。MF P105～107、ファイルサーバ102、認証サーバ108、クライアントPC103～104はネットワーク101を介して相互に通信可能に接続されている。

【0016】

＜MF Pのハードウェア構成＞ 40

次に、図3を用いて、本発明の第1の実施形態にかかるMF P105の詳細なハードウェア構成を説明する。同図において、301は、印刷・スキャンなどの制御機能を持つ本体装置、302はタッチパネルのように操作入力とその結果の表示を同じ画面で実現する表示装置である。また、304はMF P内にデータを保存するデータ保存装置、305は、個人認証用のためにIDカードを読み込むカードリーダー装置305である。なお、表示装置302の画面面積が小さい場合を考慮し、本体装置301には外付けプロジェクタ303が接続できるようになっている。

【0017】

ただし、MF P105の構成は特にこれに限定されるものではない。例えば、表示装置302が、操作入力機能を有しない、表示専用機器として構成されていてもよいし、デー 50

タ保存装置 304 が、本体装置 301 の中に収納するよう構成されていてもよい。さらに、カードリーダー装置 305 に代えて、指紋認証や彩文認証などの個人認証方式を採用した装置が備えられていても良い。

【0018】

ここで、MF P 105 を会議室に載置し、複数の参加者による会議に利用した場合の、当該 MF P 105 の処理について説明する。

【0019】

MF P 105 の利用に先立ち、まず、最初の参加者 (user A) がカードリーダー装置 305 に個人の ID カードを読み込ませ、必要に応じてパスワードを入力し、個人認証を行うことで MF P 105 にログインする。

10

【0020】

続いて、次の参加者 (user B) が、当該 MF P 105 を利用すべく、同様にカードリーダー装置 305 に個人の ID カードを読み込ませる。

【0021】

この時、従来の MF P では、既に user A がログインしている状態にあるため、ログイン画面が表示されないか、あるいは、ログイン画面が表示されたとしてもログインが拒否されることとなる。

【0022】

これに対して、本実施形態にかかる MF P 105 では、user B のログイン画面が表示され、必要に応じてパスワードを入力し、個人認証を行うことで、user B も MF P 105 にログインすることができる。更に会議に参加する人数に応じて、必要な人数がログインできるようにログイン画面が表示される。

20

【0023】

つまり、MF P 105 では、複数の参加者がログインできるように構成されている。

【0024】

< MF P の機能構成 >

続いて、MF P 105 における上記ログイン機能について、図 2 を参照しながら説明する。図 2 は、MF P 105 の機能構成を示す図である。

【0025】

制御部 201 は MF P 105 全体の制御を行うが、その一つの機能としてログイン制御を行っている。

30

【0026】

ユーザはカードリーダー部 207 を介してログイン作業を行う。カードが挿入されるとその個人 ID を読み込み、必要に応じてカードの内部データを読み出すための PIN コードの入力を促す画面を表示部 203 に表示する。

【0027】

その後、PIN の入力を操作部 202 から受け付けると、制御部 201 ではカードの内部データを読み出し、個人認証を行う。個人認証を正しく行うことができた場合には、ユーザのアクセス制御リストを取得する。取得方法は、認証システムの構成に依存するので、ここではその一例を示す。

40

【0028】

NIC (Network Interface Card) 部 204 経由でネットワーク 101 上の認証サーバ 108 にアクセスし、そのユーザのアクセス制御リストを取得する。制御部 201 は取得したアクセス制御リストを、アクセス制御部 205 と連携してアクセス情報格納部 206 に保存する。

【0029】

MF P 105 は、内部にあるファイル格納部 207 やファイルサーバ 102 にアクセスして、それらが管理するファイルを読み書きする。この時、これらのファイルは認証サーバ 108 に登録されているユーザのアクセス制御リストに従ってアクセス権の範囲が決められており、アクセスが制御される。これらの動作は、個人認証とアクセス制御という技

50

術で実現されており、一般的に知られているものである。

【0030】

なお、上述のように、個人認証の方法は、IDカードを用いる以外に指紋認証や彩文認証などを利用することも可能であり、それらに従って認証方法も変わってくるが、アクセス制御の本質は同じである。

【0031】

<ユーザのログイン>

続いて、図4と図5を用いてログイン時のユーザインターフェースについて説明する。

【0032】

図4及び図5はMFP105の表示部203（タッチパネル式になっていて入力機能も備える）に表示される表示画面の一例を表している。図4は、ユーザが誰もログインしていない状態のときの表示画面を示す。表示画面401上にログインを行うためにIDカードをリーダに読み込ませることを促す表示ウィンドウ402が表示されている。なお、認証方法が非接触方式であったり、指紋認証であった場合には、表示文字はそれに合わせた表記に変わることは言うまでもない。

【0033】

ユーザが、IDカードをリーダに読み込ませると、図5の表示画面が表示される。ここでは、IDカードのユーザ名が表示欄501に表示されるため、ユーザはユーザ名を確認することができる。そして、ユーザに対して、IDカード内の認証情報を読み出すためのPINコード（パスワード）の入力を促し、表示欄502において入力を受け付ける。このようにして、MFP105へのユーザのログインが行われる。

【0034】

<ユーザのワーク領域>

ユーザによるログインが完了すると、表示部203には、図6に示すようにユーザごとにカスタマイズされたワーク領域601が表示される。ワーク領域601は複数のパーツから構成されている。具体的には、ユーザ名を表示する部分602、当該ユーザが利用可能なツール（コマンドアイコン）603、当該ユーザがアクセス権を持つフォルダやファイルを表示するオブジェクト表示領域604である。

【0035】

オブジェクト表示領域604は、フォルダとファイルを表示するが、それぞれの名称も表示しているので、簡単に識別して選択することができる。また、アクセス権として、書き込みと読み出しの両方をもつフォルダは、オブジェクト表示領域604のように実線で表示される。また、読み出しのアクセス権しか持たないフォルダは、オブジェクト表示領域605のように破線で表示される。このため、一目でアクセス権状態がわかる。なお、カスタマイズされたワーク領域の表示に関しては、一般的に知られているものである。

【0036】

このようにワーク領域が表示されるため、会議において、ユーザは目的のファイルを簡単に見つけ出し、当該ファイルを用いてプレゼンテーションを行ったり、当該ファイルにアイデアを書き込んだりすることが可能である。

【0037】

<複数ユーザのログイン>

続いて、一人以上のユーザがログインしている状態において、別のユーザがログインする場合のユーザインターフェースについて説明する。既にログインしているユーザについては、図6に示すワーク領域が表示部203上に表示されている。この時、別のユーザがIDカードをリーダに読み込ませると、再び図5に示す表示画面が表示される。このユーザは既に説明した方法でログインを行う。このようなユーザインターフェースにより、複数ユーザのIDカードの認証を行うことができ、ログインが実行される。

【0038】

この時のMFP105の処理について図2を用いて説明する。2人目以降のログインが行われると、1人目と同様に、NIC（Network Interface Card

10

20

30

40

50

部 2 0 4 経由でネットワーク 1 0 1 上の認証サーバ 1 0 8 にアクセスし、そのユーザのアクセス制御リストを取得する。

【 0 0 3 9 】

制御部 2 0 1 では取得したアクセス制御リストを、アクセス制御部 2 0 5 と連携してアクセス情報格納部 2 0 6 に保存する。この時、複数ユーザ分のアクセス制御リストがアクセス情報格納部 2 0 6 に保存されるが、どのユーザのアクセス制御リストであるかは、ユーザの ID から識別できるので、混同されることなく保存することが出来る。

【 0 0 4 0 】

< 複数ユーザのワーク領域 >

複数ユーザのログインが完了すると、図 7 に示すようにユーザごとにカスタマイズされたワーク領域 7 0 1 と 7 1 1 が表示される。それぞれのワーク領域のユーザ名を表示する部分 7 0 1 と 7 1 1 にユーザ名が表示されるため、どちらのワーク領域がどのユーザのものであるかが簡単に判別できる。 10

【 0 0 4 1 】

なお、図 7 の表示画面の例では、各ユーザ間でワーク領域のデザインを同じように描画しているが (7 0 2 ~ 7 0 5 、 7 1 2 ~ 7 1 5 参照) 、ユーザごとにワーク領域のデザインをカスタマイズできる。このため、どのワーク領域がどのユーザのものであるかは、ワーク領域のデザインをみれば一目瞭然である。

【 0 0 4 2 】

このように、本実施形態にかかる M F P 1 0 5 では、複数ユーザがログインしている場合、複数のワーク領域が表示される。なお、図 7 の表示画面の例では、ワーク領域を 2 つしか表示していないが、スクロールや頁をめくるなど、ユーザインタフェースを工夫することにより、2 つ以上のワーク領域を表示することも可能である。 20

【 0 0 4 3 】

< 複数ユーザがログインした場合のアクセス制御方法 >

続いて、図 2 を参照しながら、ログインしているユーザが単数である場合のアクセス制御の方法について説明した後、複数ユーザがログインした場合のアクセス制御方法について説明する。

【 0 0 4 4 】

ログインしているユーザは図 7 に示す表示画面 4 0 1 のアイコンなどを指し示すことで、目的のファイルを開いて表示装置 3 0 2 上に表示させることができる。例えば、ユーザ「user A」のフォルダ 7 0 4 の中にあるファイル「File 1 0 1」を開く場合、ユーザはワーク領域 7 0 1 の中にある「File 1 0 1」のアイコンを指し示して、「ファイルを開く」と指示する。 30

【 0 0 4 5 】

この時、M F P 1 0 5 の内部では、次のような動作を行う。「ファイルを開く」と指示されたときに指し示しているのがワーク領域 7 0 1 であることを、操作部 2 0 2 が検知する。

【 0 0 4 6 】

制御部 2 0 1 ではアクセス制御部 2 0 5 に対し、ワーク領域 7 0 1 の「user A」のアクセス制御リストをアクセス情報格納部 2 0 6 から取得し、これを用いて、ファイル「File 1 0 1」にアクセスする。この時、ファイル「File 1 0 1」がネットワーク上のファイルサーバ 1 0 2 内にあれば、N I C 部 2 0 4 経由でアクセスし、M F P 1 0 5 内部のファイル格納部 2 0 7 内にあれば、直接アクセスする。 40

【 0 0 4 7 】

一方、「user B」のフォルダ 7 1 4 の中にあるファイル「File 5 0 1」を開く場合、ユーザはワーク領域 7 1 1 の中にある「File 5 0 1」のアイコンを指し示して、「ファイルを開く」と指示する。

【 0 0 4 8 】

この時、M F P 1 0 5 の内部では、指し示しているのがワーク領域 7 1 1 であることを 50

操作部 202 が検知する。アクセス制御部 205 では、ワーク領域 711 の「user B」のアクセス制御リストをアクセス情報格納部 206 から取得し、これを用いて、ファイル「File 501」にアクセスする。

【0049】

この時、ファイル「File 501」がネットワーク上のファイルサーバ 102 内にあれば、NIC 部 204 経由でアクセスし、MFP 105 内部のファイル格納部 207 内にあれば、直接アクセスする。

【0050】

以上のようにして、アクセス指示されたワーク領域のログインユーザのアクセス制御リストを用いてそのファイルにアクセスする。また、この方法はファイルに限らずアクセス制御リストでアクセス制御が行われているオブジェクトに対しても適用できることはいうまでもない。

【0051】

< MFP における処理の流れ >

以上の動作を、図 8 に示すフローチャートを用いて説明する。

【0052】

複数ユーザがログインした状態（ステップ S801）において、操作部 202 を介して、所定のオブジェクトへのアクセス指示を受け付ける（ステップ S802）。すると、制御部 201 ではどのワーク領域においてアクセス指示がなされたかを検知する（ステップ S803）。ワーク領域が特定されればそのユーザも特定されるので、アクセス指示がなされたワーク領域に該当するユーザのアクセス制御リストを取得する（ステップ S804）。制御部 201 は取得したアクセス制御リストを用いて指示されたオブジェクトへのアクセスを行う（ステップ S805）。

【0053】

このように、操作部 202 においてなされたアクセス指示は、そのワーク領域のユーザのアクセス制御リストを用いて、そのアクセス権の範囲内でアクセスを行うことができる。

【0054】

< 複数ユーザがログインした場合の有効活用例 >

続いて、MFP 105 の有効な活用例について図 7 を用いて説明する。例えば、「user A」が自分のファイル「File 101」を、「user B」のワーク領域 711 にあるフォルダ 714 にコピーしようとした時、フォルダ 714 は「user B」以外は書き込み権の無いフォルダであるとする。

【0055】

「user A」のアクセス制御リストを用いてコピー（つまり、ファイルの書き込み）をしようすると、アクセス権が無いのでコピーできない。しかし、「user B」のアクセス制御リストを用いてコピーしようすると、アクセス権があるので可能である。

【0056】

このため、ファイルのコピーは次のように行われる。ファイル「File 101」を読み出すのはワーク領域 701 において行うため、「user A」のアクセス制御リストを用いて行う。また、ファイル「File 101」をフォルダ 714 に書き込むのはワーク領域 711 において行うため、「user B」のアクセス制御リストを用いて行う。これによって、ファイル「File 101」をコピーすることが可能になる。このように MFP 105 では、操作部 202 においてコピーの指示を行う人が「user A」なのか「user B」なのかを判別しているのではなく、どのワーク領域でアクセスしているのかにより判別している。

【0057】

また、例えば、「user A」が自分のファイル「File 101」を、「user B」が自分のファイル「File 501」をともに開き、これらのファイルをマージし

10

20

30

40

50

て別のファイルを作成する場合を考える。さらにその後、作成されたファイルをそれぞれのユーザのフォルダに保存する場合を考える。

【0058】

マージして作成した新しいファイルを「user A」のワーク領域701のフォルダ704に保存する（書き込む）時は「user A」のアクセス制御リストを用いて行う。また、「user B」のワーク領域711のフォルダ714に保存する（書き込む）時は「user B」のアクセス制御リストを用いて行う。この場合も、それぞれのワーク領域に該当するユーザのアクセス制御リストを用いて、そのアクセス権の範囲内でアクセスをしているので任意のユーザが指示をすることができる。

【0059】

また、例えば、「user A」が自分のファイル「File101」を、「user B」しかアクセスできないアドレス帳の中に登録しているメールアドレスに送信する場合を考える。はじめに「user A」のアクセス制御リストを用いてファイル「File101」を選択する。続いて、「user B」のアクセス制御リストを用いて、例えばコマンドアイコン713の中にある「user B」のアドレス帳を開き、メールアドレスを選択して送信する。この場合も、それぞれのワーク領域に該当するユーザのアクセス制御リストを用いて操作を行う。これにより、他のユーザのアクセス権の範囲内での指示が可能である。

【0060】

以上の説明から明らかなように、本実施形態によれば、1台または複数台のMFPに複数のユーザが同時にログインできるようになる。このとき、それぞれのユーザのワーク領域をそれらのMFP上に表示して、ワーク領域ごとのアクセス権を守りながら自由にオブジェクトへのアクセスを行うよう構成することにより、オブジェクト使用時の利便性を向上させることが可能となる。この結果、当該MFPを用いれば、例えば、会議を効率的・効果的に進めることが可能となる。

【0061】

〔第2の実施形態〕

上記第1の実施形態では、単体のMFPにおける処理について説明したが、本発明は特にこれに限定されない。例えば、複数台のMFPがネットワークで繋がっている場合においても適用可能である。この場合、複数台のMFPの制御部201がNIC部204を介して、他のMFPと通信を行い、ログインしたユーザのアクセス制御リストを相互に交換し合い、あたかも1つのMFPでシームレスに作業が出来るように制御することとなる。この実現方法は一般的に知られているものであるので、ここでは詳細説明は割愛する。

【0062】

複数台のMFPがあたかも1つのMFPでシームレスに作業が出来るようになっていた場合、物理的には別のMFPの操作画面上から別のMFPの操作画面上にファイルをコピーすることも可能になる。つまり、複数台のMFPを用いて複数のユーザがログインして、ファイルのコピーや保存、送信などを行うことが可能となる。

【0063】

なお、以上の実施形態では、MFPを例に説明したが、これに限ることなく、ログイン処理によってユーザ毎のアクセス権を付与する装置であれば、その種類を問うものではない。

【0064】

〔他の実施形態〕

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【0065】

また、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、

10

20

30

40

50

システムあるいは装置に供給し、
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み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。

【0066】

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。

【0067】

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、フロッピー（登録商標）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、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

【0068】

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なく、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）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。

【0069】

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込まれた後、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。

【図面の簡単な説明】

【0070】

【図1】本発明の第1の実施形態にかかるMFPを備えるネットワークシステムの構成例を示す図である。

【図2】MFP（Multi Function Peripheral）の機能構成を示すブロック図である。

【図3】MFPのハードウェア構成を示す模式図である。

【図4】ログイン時の表示画面の一例を示す模式図である。

【図5】ログイン時の表示画面の一例を示す模式図である。

【図6】ログインした後、ユーザごとにカスタマイズされた表示画面を示す断面図である。

【図7】ログインした後、ユーザごとにカスタマイズされた表示画面を示す断面図である。

【図8】本発明の第1の実施形態にかかるMFPにおけるアクセス制御の流れを示すフローチャートである。

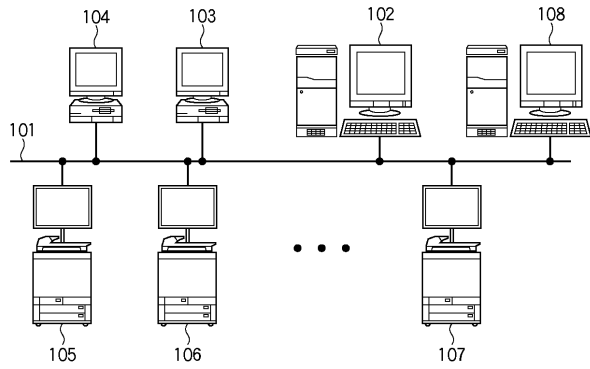
10

20

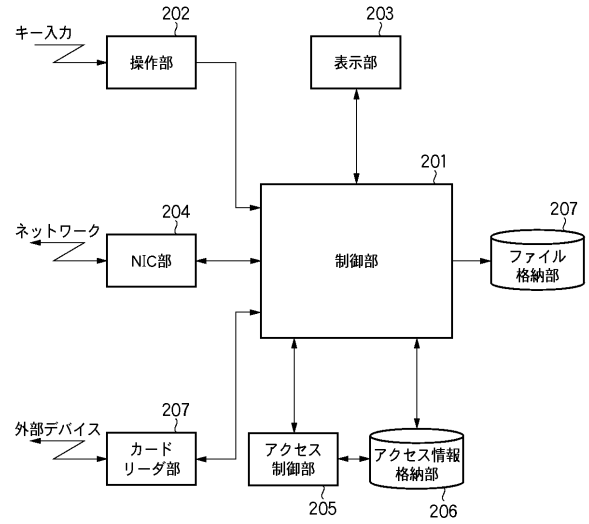
30

40

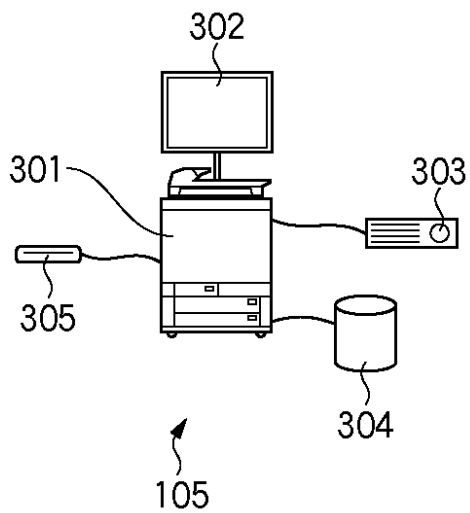
【 図 1 】



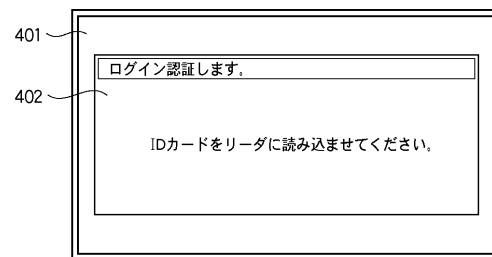
【 図 2 】



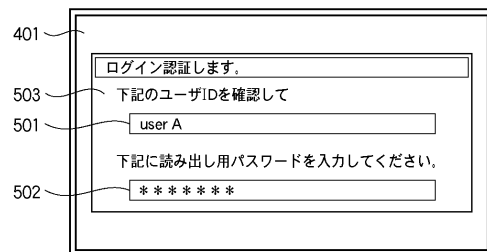
【 図 3 】



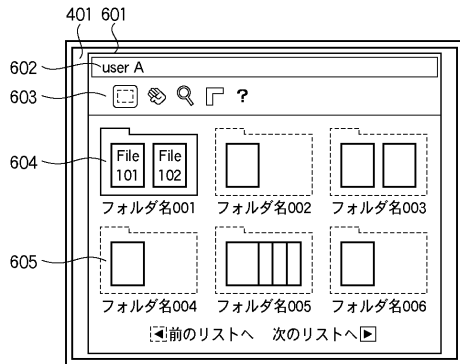
【 図 4 】



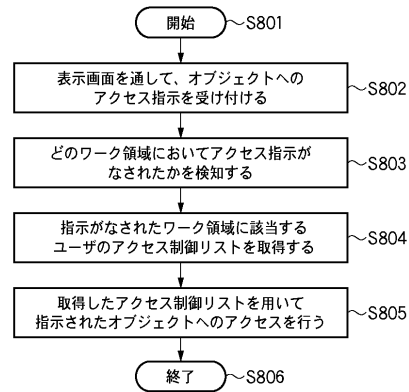
【 図 5 】



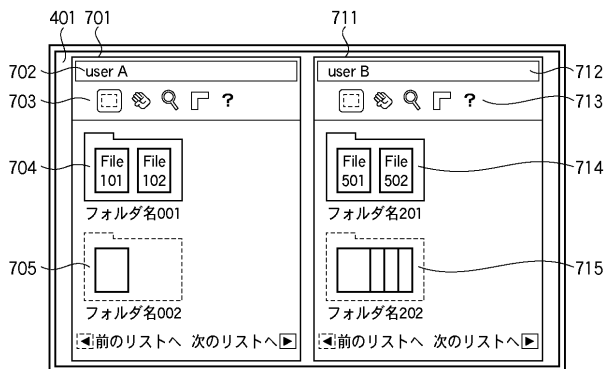
【図 6】



【図 8】



【図 7】



フロントページの続き

F ターム(参考) 5B082 EA12 GC01

5B285 AA01 BA07 CA02 CA12 CB63 CB74 CB85