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

特許第4587164号
(P4587164)

(45)発行日　平成22年11月24日(2010.11.24)　(24)登録日　平成22年9月17日(2010.9.17)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	530D
G06F 3/12	(2006.01)	G06F	3/12	K
G06F 12/00	(2006.01)	G06F	12/00	537D

請求項の数 8　(全 20 頁)

(21)出願番号　特願2004-220684 (P2004-220684)
(22)出願日　平成16年7月28日 (2004.7.28)
(65)公開番号　特開2006-40060 (P2006-40060A)
(43)公開日　平成18年2月9日 (2006.2.9)
審査請求日　平成19年7月26日 (2007.7.26)

(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
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】印刷システム、印刷制御方法、並びにプログラム

(57)【特許請求の範囲】

【請求項１】

印刷装置による印刷処理の対象となる電子データが投入されるフォルダであるホットフォルダを登録する登録手段と、

前記登録手段により登録されたホットフォルダを使用して印刷が可能なユーザのユーザ情報を設定する設定手段と、

前記ホットフォルダに対する前記印刷装置による印刷処理の対象となる電子データの投入を監視する監視手段と、

前記ホットフォルダに対する前記電子データの投入が前記監視手段によって確認されたことに応じて、ユーザインターフェースにユーザ情報の入力を促すユーザ認証画面を表示させる表示制御手段と、

前記ユーザ認証画面を介して入力されたユーザ情報と、前記設定手段により前記ホットフォルダに対して設定されているユーザ情報とに基づいて、該ホットフォルダに投入された電子データの前記印刷装置による印刷処理を許可するか否かを判定する判定手段と、

前記判定手段により、前記電子データの前記印刷装置による印刷処理を許可すると判定された場合に、該電子データを前記印刷装置に印刷させる印刷制御手段と、

を備えることを特徴とする印刷システム。

【請求項２】

前記設定手段は、前記ホットフォルダを使用して印刷が可能な複数のユーザ毎にユーザ情報を設定することが可能であり、

前記ホットフォルダを使用して印刷が可能とされているユーザのうち少なくとも一人に対して印刷機能の制限情報を設定する制限手段と、
を更に備え、
前記印刷制御手段は、前記ユーザ認証画面を介して入力されたユーザ情報に対応するユーザに対して前記制限手段によって設定されている制限情報に従って、前記電子データを前記印刷装置に印刷させる
ことを特徴とする請求項１に記載の印刷システム。
【請求項３】
前記印刷システムには、印刷機能の異なる複数の印刷装置が含まれ、
前記制限手段によって制限されている印刷機能に応じて、前記電子データの印刷を行わせる印刷装置を切り替える切替手段を更に備える
ことを特徴とする請求項２に記載の印刷システム。
【請求項４】
前記表示制御手段は、前記ユーザ認証画面を介して入力されたユーザ情報に対応するユーザに対して前記制限手段によって設定されている制限情報により前記印刷装置による印刷機能が使用できない場合に、ユーザインターフェースに前記ユーザ情報とは異なるユーザ情報の入力を促すユーザ再認証画面を表示させ、
前記印刷制御手段は、当該制限情報により当該印刷機能が使用できる場合に、該印刷機能を使用して、前記電子データを前記印刷装置に印刷させる
ことを特徴とする請求項２又は３に記載の印刷システム。
【請求項５】
前記ホットフォルダの使用履歴を保存する保存手段と、
前記保存手段によって保存された使用履歴をユーザインターフェースに表示させる履歴表示手段と、
を更に備え、
前記履歴表示手段は、前記ホットフォルダが前記設定手段によって使用可能なユーザのユーザ情報が設定されているホットフォルダであるか否かを識別可能に表示させる
ことを特徴とする請求項１乃至４のいずれか１項に記載の印刷システム。
【請求項６】
前記監視手段は、印刷業務の受注、納期管理、消耗品管理、印刷デバイス管理機能を併せ持つことを特徴とする請求項１乃至５の何れか１項に記載の印刷システム。
【請求項７】
印刷システムにおける印刷制御方法であって、
登録手段が、印刷装置による印刷処理の対象となる電子データが投入されるフォルダであるホットフォルダを登録する登録工程と、
設定手段が、前記登録工程で登録されたホットフォルダを使用して印刷が可能なユーザのユーザ情報を設定する設定工程と、
監視手段が、前記ホットフォルダに対する前記印刷装置による印刷処理の対象となる電子データの投入を監視する監視工程と、
表示制御手段が、前記ホットフォルダに対する前記電子データの投入が前記監視工程で確認されたことに応じて、ユーザインターフェースにユーザ情報の入力を促すユーザ認証画面を表示させる表示制御工程と、
判定手段が、前記ユーザ認証画面を介して入力されたユーザ情報と、前記設定工程により前記ホットフォルダに対して設定されているユーザ情報とに基づいて、該ホットフォルダに投入された電子データの前記印刷装置による印刷処理を許可するか否かを判定する判定工程と、
印刷制御手段が、前記判定工程で前記電子データの前記印刷装置による印刷処理を許可すると判定された場合に、該電子データを前記印刷装置に印刷させる印刷制御工程と、
を有することを特徴とする印刷制御方法。
【請求項８】

コンピュータを、請求項１乃至６のいずれか１項に記載の印刷システムが有する各手段として機能させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、いわゆるホットフォルダに格納した電子データをホットフォルダの印刷設定に従って画像処理装置で印刷する印刷システムに関するものである。
【背景技術】
【０００２】
従来より、ＰＣ上で作成された電子データを所定の印刷設定で簡単に印刷するための方法としてホットフォルダが用いられている。
【０００３】
例えば、特許文献１には、印刷物の印刷出力を制御するためにホットフォルダを用いている。より具体的には、予め複数個のホットホルダーをサーバーに作成しておき、各ホットホルダーのそれぞれに対してサブ監視プログラムを起動し、所定時間ごとにホットホルダーを監視する。そのホットホルダーにドキュメントデータが入稿すれば、予めホットホルダーに設定されたルールをチェックし、そのデータを自動的にジョブ登録する。
【０００４】
このようなホットフォルダを用いることによって、ユーザは電子データをホットフォルダに投入（ドラッグ＆ドロップ）するだけで面倒な印刷設定を行う必要がなくなり、簡単に印刷を行うことが可能となる。
【特許文献１】特開２０００－１１８０９５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した従来の技術では、ホットフォルダに対してのユーザ管理を行っておらず、誰でもがホットフォルダを使用可能であったため、セキュリティ上の問題があった。
【０００６】
また、同様にホットフォルダに対してのユーザ管理が行われていなかったために、特定のユーザにしか高機能な印刷（カラー印刷等）を行わせないように制限をかけることもできなかった。
【０００７】
さらに、同様にホットフォルダに対してのユーザ管理が行われていなかったために、管理者側でどのユーザがホットフォルダを使用したかという情報を得ることもできなかった。
【０００８】
本発明は、このような問題点に鑑みてなされたものであり、共有フォルダたるホットフォルダにアクセスするユーザを制限することが可能で、ユーザ管理だけのために別サーバーを用意する必要のない印刷システムを提供するものである。
【０００９】
また、本発明は、管理サーバーを一つにすることができ、管理が行い易く、さらには、ユーザの操作性とセキュリティレベルを上げることが可能な印刷システムを提供するものである。
【００１０】
さらに、本発明は、管理者がホットフォルダを使用したユーザのログをウェブ・ブラウザを用いて容易に閲覧することが可能で、ホットフォルダにアクセスするユーザを制限できると共に、ユーザ毎に使用可能なホットフォルダの機能を制限することができる印刷システムを提供するものである。
【００１１】

また、本発明は、サーバーを立てることなく、ローカルＰＣ上だけでホットフォルダにアクセスできるユーザを制限することが可能な印刷システムを提供するものである。

【課題を解決するための手段】

【００１２】

上記課題を解決するために、本発明による印刷システムは、印刷装置による印刷処理の対象となる電子データが投入されるフォルダであるホットフォルダを登録する登録手段と、前記登録手段により登録されたホットフォルダを使用して印刷が可能なユーザのユーザ情報を設定する設定手段と、前記ホットフォルダに対する前記印刷装置による印刷処理の対象となる電子データの投入を監視する監視手段と、前記ホットフォルダに対する前記電子データの投入が前記監視手段によって確認されたことに応じて、ユーザインターフェースにユーザ情報の入力を促すユーザ認証画面を表示させる表示制御手段と、前記ユーザ認証画面を介して入力されたユーザ情報と、前記設定手段により前記ホットフォルダに対して設定されているユーザ情報とに基づいて、該ホットフォルダに投入された電子データの前記印刷装置による印刷処理を許可するか否かを判定する判定手段と、前記判定手段により、前記電子データの前記印刷装置による印刷処理を許可すると判定された場合に、該電子データを前記印刷装置に印刷させる印刷制御手段とを備えることを特徴とする。

【００１５】

さらなる本発明の特徴は、以下本発明を実施するための最良の形態および添付図面によって明らかになるものである。

【発明の効果】

【００１６】

本発明によれば、ＭＩＳサーバーによってネットワーク上に公開されているホットフォルダを使用できるユーザを限定させることができ、ホットフォルダを用いた印刷のセキュリティを向上させることが可能となる。

【００１７】

また、ホットフォルダを使用したユーザの履歴をＭＩＳサーバーがログとして残し、ウェブ・ブラウザを用いて閲覧することが可能となるため、ホットフォルダを使用しているユーザの作業状況を確認することが可能となる。

【００１８】

さらに、ホットフォルダを使用可能なユーザを制限可能なだけでなく、ホットフォルダを使用可能なユーザの中でも特定のユーザにしか付加価値の高い印刷（カラー印刷等）を行えなくさせることが可能となるため、セキュリティの向上だけでなく、ユーザ毎に対しての細かなセキュリティ設定を行うことが可能となる。

また、ＭＩＳサーバーを設けなくともユーザ管理プログラムをユーザＰＣ内に動作させておくことによって、ホットフォルダを使用可能なユーザを制限することが可能となる。

【発明を実施するための最良の形態】

【００１９】

以下、図面を参照しながら本発明に係る実施形態について詳細に説明する。

【００２０】

＜第１の実施形態＞

図１は第１の実施形態の全体構成図を表したものであり、図中の各装置はネットワーク１１１を介して接続されている。

【００２１】

１０１はユーザが作業を行うＰＣである。まず、ユーザはこのＰＣ上で作成した電子データ（ジョブデータやアプリケーションデータ等）を１１１のネットワーク上に公開されている任意のホットフォルダ１０４又は１０６に格納（ドラッグ＆ドロップ）する。すると、印刷装置や消耗品の管理等の機能を持つ管理情報システムサーバー（以下、ＭＩＳサーバーという）１０７が後述のユーザ認証手続を実行する。認証が得られれば、ホットフォルダに格納された電子データに対して、ネットワーク１１１上に接続している印刷装置１１０において印刷処理を実行することが可能になる。

【００２２】
ここで、ネットワーク１１１上のホットフォルダ１０４、１０６はそれぞれコンピュータ１０３、１０５において、ネットワーク上に共有されている。また、管理情報システムサーバー１０７は、ホットフォルダ１０４、１０６を使用できるユーザを制限する管理情報システムサーバーであり、ホットフォルダ１０４、１０６に電子データが投入されてくるのを常時監視しアクセスしたログをデータベース１０８に保存することが可能である。
【００２３】
なお、本実施形態において、ホットフォルダとは、ネットワーク上に接続されたユーザ共用のフォルダであり、そこに所定のジョブやデータを格納すると所定の処理を自動的に実行するよう構成されたフォルダである。
【００２４】
また、１０９は管理者ＰＣである。管理者ＰＣ１０９からホットフォルダ１０４、１０６にアクセスしたユーザのアクセスしたログをデータベース１０８から取得してウェブ・ブラウザで閲覧するのに用いられる。
【００２５】
図２は第１の実施形態にかかる動作を説明するためのフローチャートである。図２において、ステップＳ２０１乃至Ｓ２０４はユーザＰＣ １０１から電子データをホットフォルダ１０４、１０６に投入した際のユーザＰＣ１０１側の動作であり、ステップＳ３０１乃至Ｓ３０７はホットフォルダ１０４、１０６に電子データが投入された際のＭＩＳサーバー１０７側の動作である。
【００２６】
図２おいて、まずステップＳ２０１では、ユーザがＰＣ１０１上で作成した電子データを任意のホットフォルダ１０４又は１０６にドラッグ＆ドロップによって投入する。
【００２７】
ＭＩＳサーバー１０７は、ステップＳ３０１で示されるように常時ホットフォルダ１０４及び１０６を監視している。そして、ホットフォルダ１０４又は１０６に電子データが投入されたことを検知すると、ステップＳ３０２においてユーザＰＣに対してユーザ認証画面表示をするように指示をする。つまり、ＭＩＳサーバー１０７はホットフォルダ１０４及び１０６に電子データが投入されたのを検知すると、どこ（どのＰＣ）から投入されたのかについて情報（例えば、ＰＣのＩＰアドレス等）をコンピュータ１０３又は１０５から取得し、その対応するユーザＰＣに認証画面を表示するよう指示を送信するのである。
【００２８】
すると、ユーザＰＣ側では、ステップＳ２０２において、ＰＣ１０１の表示画面上に図３又は図４で示されるようなユーザ認証画面が表示される。図３はユーザ名及びパスワードを直接入力するタイプの認証画面を示し、図４はユーザ名とパスワードを記憶したＩＣカードの挿入を促すタイプの認証画面を示している。この認証画面の表示動作は次のように実現される。
【００２９】
ステップＳ２０３では、ユーザによってユーザ名やパスワードが入力され、それらがＭＩＳサーバー１０７に送信される。
【００３０】
ＭＩＳサーバー１０７はそのユーザデータを受信し、ステップＳ３０３において、ユーザ管理データベース内に登録され地得るユーザデータと等しいか否かが判断される。等しければ処理はステップＳ３０４に移行し、等しくなければ処理はステップＳ３０６に移行する。
【００３１】
ステップＳ３０６では、不正なユーザの投入した電子データであるとして印刷処理を実行しないように印刷装置１１０を制御する。また、ホットフォルダに投入された電子データはそこから削除するようにする。

【００３２】
一方、ステップＳ３０４では、認証に成功した正当なユーザのデータであるとして印刷処理を実行するように印刷装置１１０を制御する。そして、ステップＳ３０５に移行し、図５（ユーザのログをウェブ・ブラウザの表示例１）に示すようにユーザのホットフォルダへのアクセス日時６０２とユーザ名６０３とジョブ名６０４がデータベース１０８に保存されるとともに、ＰＣ１０９のウェブ・ブラウザからの閲覧が可能となるようにされる。
【００３３】
ここで、ＭＩＳサーバーは複数のホットフォルダを同時に監視することができるため、図６（ユーザのログをウェブ・ブラウザの表示例２）に示すようにどのユーザがどのホットフォルダを使用したかという情報をホットフォルダ名７０１として保存することも可能である。
【００３４】
また、ホットフォルダにはユーザ管理されているホットフォルダとユーザ管理されていないホットフォルダが存在するため、ユーザ管理されていないホットフォルダへのアクセスログに残す際には、図７（ユーザのログをウェブ・ブラウザの表示例３）に示すようにユーザ名欄６０３は空欄にしておき、ホットフォルダ名欄７０１にはユーザ管理していないホットフォルダであることを一目で分かるようにしてログに残すようにしている。
最後に、ステップＳ３０７では、処理の結果をＰＣ１０１上に表示するようにするための指示をＰＣ１０１に送信し、ＰＣ１０１ではステップＳ２０４で処理結果が表示画面上に表示されるようにしている。。
【００３５】
なお、図２では印刷処理を例に説明しているが、本実施形態ではこれに限らず、メール送信、ＰＤＦ化処理、特殊の画像処理等、どのような処理であっても良い。また、複数のホットフォルダを用意しておき、フォルダごとに処理を異ならしめるようにしてもよい。
【００３６】
また、図２のフローチャートの処理では、処理結果を表示するようにしているが、ユーザ認証の結果を表示画面上に表示するようにしても良い。
【００３７】
図８は、ユーザＰＣ１０１上のデスクトップ９０１を表示しており、ネットワーク１１１上のホットフォルダ１０４、１０５がユーザＰＣ１０１上で表示されている図の表示例である。
【００３８】
ユーザは作成した電子データ９０２をデスクトップ上に表示されている任意のホットフォルダ９０４、９０５、９０６のどれかにドラッグ＆ドロップすることで印刷装置１１０に印刷を行うことができるようになる。
【００３９】
次に、図９及び図１０を用いてホットフォルダに対してのユーザ認証を行うための、ユーザ管理方法について説明する。
【００４０】
図９及び図１０のそれぞれは、ホットフォルダを使用できるユーザを登録するための操作部の表示例を示している。
【００４１】
ＭＩＳサーバー１０７側において、まず図９のようなホットフォルダ操作画面１００１を開く。この画面上にはＭＩＳサーバー １０７に接続されている全てのホットフォルダ名１００２と、そのホットフォルダの更新日時１００３とそのホットフォルダはユーザ認証の設定がなされているかどうかを示す表示１００４が表示されている。
【００４２】
この画面内には、さらにホットフォルダの追加ボタン１００５とホットフォルダの削除ボタン１００６があり、ホットフォルダの追加と削除を行うことが可能となっている。

【００４３】
さらに、選択したホットフォルダに対して、ユーザ認証の設定を行うためのボタン１００７を押下することによって、そのホットフォルダにアクセス可能なユーザを追加／削除することが可能となっている。
【００４４】
ユーザ管理設定ボタン１００７を押下すると、図１０に示すようなユーザ管理設定画面１１０１が表示される。この画面内には、選択したホットフォルダのユーザ認証の「有り／無し」チェックボタン１１０２があり、このチェックボックスを「有り」にチェックすることでホットフォルダにアクセスする際には、ユーザ認証を行わなければアクセスできないようにすることが可能となる。
【００４５】
さらに、ユーザ管理設定画面１１０１にはユーザ追加ボタン１１０３とユーザ削除ボタン１１０４とユーザ編集ボタン１１０９があり、これらのボタンを押下することで、ホットフォルダにアクセス可能なユーザの追加／削除及び、ユーザ名やパスワードの編集を行うことが可能となる。
【００４６】
以上説明したように、本実施形態によればＭＩＳサーバー１０７によって、ネットワーク１１１上に公開されているホットフォルダを使用できるユーザを限定させることができ、ホットフォルダを用いた印刷のセキュリティを向上させることが可能となる。
【００４７】
また、ホットフォルダを使用したユーザの履歴をＭＩＳサーバーがログとして残し、ウェブ・ブラウザを用いて閲覧することが可能となるため、ホットフォルダを使用しているユーザの作業状況を確認することが可能となる。
【００４８】
＜第２の実施形態＞
図１１は第２の実施形態に係る全体構成図を表したものである。図１と共通の構成については同じ参照番号を用いている。
【００４９】
１０１はユーザが作業を行うＰＣであり、ユーザはこのＰＣ上で作成した電子データ（アプリケーションデータ等）を１１１のネットワーク上に公開されている任意のホットフォルダ１０４と１０６に格納（ドラッグ＆ドロップ）することによって、ホットフォルダに接続された白黒印刷装置１１０またはカラー印刷装置１１０１に印刷を実行することが可能である。ここで、ネットワーク１１１上のホットフォルダ１０４、１０６はそれぞれコンピュータ１０３、１０５において、ネットワーク上に共有されている。
【００５０】
また、管理情報システムサーバー（以下、ＭＩＳサーバーという）１０７は、ホットフォルダ１０４、１０６を使用できるユーザを制限すると共に、使用可能な印刷機能をユーザ毎に制限をかけることができる管理情報システムサーバーであり、ホットフォルダ１０４、１０６に電子データが投入されてくるのを常時監視しアクセスしたログをデータベース １０８に保存することが可能である。
【００５１】
また、１０９は管理者ＰＣであり、管理者ＰＣ １０９からホットフォルダ １０４、１０６にアクセスしたユーザのアクセスしたログをデータベース１０８から取得してウェブ・ブラウザで閲覧するのに用いられる。
【００５２】
次に、図１２を用いて本実施形態に係る動作について説明する。本実施形態ではカラー電子データがホットフォルダに投入された場合の処理に関するものであり、図１２おいて、ステップＳ１２０１乃至Ｓ１２０４はユーザＰＣ １０１から電子データをホットフォルダ１０４、１０６に投入した際のユーザＰＣ １０１側の動作あり、ステップＳ１３０１乃至Ｓ１３０９はホットフォルダ１０４、１０６に電子データが投入された際のＭＩＳ

サーバー１０７側の動作である。

【００５３】

まず図１２において、ステップＳ１２０１では、ユーザはユーザＰＣ １０１で作成したカラー電子データをネットワーク上に公開されているホットフォルダ１０４もしくは１０６に投入（ドラッグ＆ドロップ）する。

【００５４】

ＭＩＳサーバー１０７は、第１の実施形態同様、ホットフォルダ１０４及び１０６を常時監視しているため、カラー電子データの投入を検知する。

【００５５】

ステップＳ１３０２では、ユーザＰＣに対してユーザ認証画面表示をするように指示をする。つまり、ＭＩＳサーバー１０７はホットフォルダ１０４及び１０６に電子データが投入されたのを検知すると、どこ（どのＰＣ）から投入されたのかについて情報（例えばユーザＰＣのＩＰアドレス等）をコンピュータ１０３又は１０５から取得し、その対応するユーザＰＣに認証画面を表示するよう指示を送信するのである。

【００５６】

すると、ユーザＰＣ側では、ステップＳ１２０２において、ＰＣ１０１の表示画面上に図３又は図４で示されるようなユーザ認証画面が表示される。図３はユーザ名及びパスワードを直接入力するタイプの認証画面を示し、図４はユーザ名とパスワードを記憶したＩＣカードの挿入を促すタイプの認証画面を示している。この認証画面の表示動作は次のように実現される。

【００５７】

ステップＳ１２０３では、ユーザによってユーザ名やパスワードが入力され、ＯＫボタンを押下することによってそれらがＭＩＳサーバー１０７に送信される。

【００５８】

ＭＩＳサーバー１０７はそのユーザデータを受信し、ステップＳ１３０３において、ユーザ管理データベース内に登録され地得るユーザデータと等しいか否かが判断される。等しければ処理はステップＳ１３０４に移行し、等しくなければ処理はステップＳ１３０８に移行する。

【００５９】

ステップＳ３０８では、不正なユーザの投入した電子データであるとして印刷処理を実行しないように印刷装置１１０を制御する。また、ホットフォルダに投入された電子データはそこから削除するようにする。

【００６０】

ステップＳ１３０３で認証に成功した場合には、さらに、ユーザが投入したホットフォルダに対して電子データを投入したユーザに設定されている印刷制限を取得する。そして、ステップＳ１４０４において、ホットフォルダ１０４又は１０６に投入したカラー電子データについて、ホットフォルダを用いてカラー印刷を行えるように設定されているユーザかどうかを判断している。つまり、当該ユーザがホットフォルダ経由でカラー印刷する権限を有するか否かが判断される。なお、各ホットフォルダに対してユーザ毎に印刷制限の設定を行う際の設定方法ついては、図１３乃至図１６を用いて後述する。

【００６１】

カラー印刷権限を有しない場合には、処理はステップＳ１３０６に移行し、モノクロ印刷実行の指示が白黒印刷装置１１０に対してなされ、そこで印刷が実行される。一方カラー印刷権限がある場合には、処理はステップＳ１３０５に移行し、カラー印刷実行の指示がカラー印刷装置１１０１に対してなされ、そこでカラー印刷が実行される。

【００６２】

印刷が実行されると処理はステップＳ１３０７に移行し、ログ保存処理が実行される。つまり、図５（ユーザのログをウェブ・ブラウザの表示例１）に示すようにユーザのホットフォルダへのアクセス日時６０２とユーザ名６０３とジョブ名６０４がデータベース１０８に保存されるとともに、ＰＣ１０９のウェブ・ブラウザからの閲覧が可能となるよう

にされる。ここで、ＭＩＳサーバーは複数のホットフォルダを同時に監視することができるため、図６（ユーザのログをウェブ・ブラウザの表示例２）に示すようにどのユーザがどのホットフォルダを使用したかという情報をホットフォルダ名７０１として保存することも可能である。また、ホットフォルダにはユーザ管理されているホットフォルダとユーザ管理されていないホットフォルダが存在するため、ユーザ管理されていないホットフォルダへのアクセスログに残す際には、図７（ユーザのログをウェブ・ブラウザの表示例３）に示すようにユーザ名欄６０３は空欄にしておき、ホットフォルダ名欄７０１にはユーザ管理していないホットフォルダであることを一目で分かるようにしてログに残すようにしている。

【００６３】

そして、最後に、ステップＳ１３０９において、処理結果をユーザＰＣ１０１の表示画面上に表示するための指示をユーザＰＣ１０１に対して送信する。ユーザＰＣ１０１側ではそれを受信し、処理結果に応じた表示を表示画面上になすようにしている。

【００６４】

前述の通り、図１３乃至図１６はホットフォルダを使用できるユーザの登録及び、ユーザ毎に使用可能なホットフォルダの印刷機能に制限をかけるための操作部の表示例である。これらを用いて各ホットフォルダに対してユーザ毎に印刷制限の設定を行う際の設定方法ついて説明する。

【００６５】

まず、ＭＩＳサーバー１０７側において、図１３にあるようなホットフォルダ操作画面１００１を開く。この画面上にはＭＩＳサーバー１０７に接続されている全てのホットフォルダ名１００２と、そのホットフォルダの更新日時１００３と、そのホットフォルダはユーザ認証の設定がなされているかどうかを示す表示１００４と、そのホットフォルダにおいて印刷制限設定がなされているかどうかを示し表示１５０１がある。

【００６６】

ホットフォルダ操作画面内には、さらにホットフォルダの追加ボタン１００５とホットフォルダの削除ボタン１００６があり、ホットフォルダの追加と削除を行うことが可能となっている。

【００６７】

さらに、選択したホットフォルダに対して、ユーザ認証の設定を行うためのボタン１００７を押下することによって、そのホットフォルダにアクセス可能なユーザを追加／削除することが可能である。

【００６８】

ホットフォルダ操作画面上の任意のホットフォルダを選択し、ユーザ管理設定１００７を押下することによって、図１４に示すようなユーザ管理設定画面１１０１が表示される。この画面内には、選択したホットフォルダのユーザ認証の「有り／無し」チェックボタン１１０２がある。このチェックボックスを「有り」にチェックすることでホットフォルダにアクセスする際には、ユーザ認証を行わなければアクセスできないようにすることが可能となる。

【００６９】

さらに、ユーザ管理設定画面１１０１にはユーザ追加ボタン１１０３とユーザ削除ボタン１１０４とユーザ編集ボタンがある。これらのボタンを押下することで、ホットフォルダにアクセス可能なユーザの追加／削除及びユーザ名、パスワードの編集を行うことが可能となる。

【００７０】

また、ユーザ管理設定画面内には印刷制限設定を行うか／行わないかを設定するチェックボックス１６０１が表示されている。この印刷制限設定はユーザ認証を「有り」にした場合にのみ設定することが可能となるようになっている。図１４においては、ユーザ認証設定１１０２を「無し」にしているため、印刷制限設定１６０１が選択できなくなっている状態を表している。また、同様にユーザ認証を行っていないので、ユーザ名、パスワー

ド、印刷制限を表示した表示項目１１０５、１１０６、１６０２も選択できなくなっている状態を表している。

【００７１】

次に、図１４のユーザ認証設定のチェックボックス １１０２を「有り」に設定すると、図１５に示すような画面になり、ユーザ名、パスワードを表示した表示項目１１０５、１１０６が表示され、ユーザの追加／削除、ユーザ名やパスワードの変更を行うことが可能となる。また、同時に印刷制限設定１６０１も選択することが可能となる。

【００７２】

図１５のユーザ管理設定画面において、印刷制限設定１６０１を「有り」に設定すると図１６に示すような画面となり、各印刷制限の項目に対して、各ユーザに権限を与える／与えないを１８０１のリストボックスで選択する。

【００７３】

図１６の印刷制限としては、カラー印刷、白黒印刷、文書結合印刷、全て許可の項目しか挙げられていないが、これ以外の印刷制限を設定することも可能である。

【００７４】

以上説明したように、第２の実施形態によればＭＩＳサーバー１０７によって、ネットワーク上に公開されているホットフォルダを使用できるユーザ及びユーザが使用可能な印刷設定を限定させることができるようになるため、高機能な印刷（カラー印刷）は特定のユーザにしか使うことができないようにすることが可能となり、セキュリティの向上だけでなく、ユーザ毎に対しての細かなセキュリティ設定を行うことが可能となる。

【００７５】

＜第３の実施形態＞

第１及び第２の実施形態では、ネットワーク上のホットフォルダを使用し、ＭＩＳサーバー１０７でネットワーク上のホットフォルダを監視しユーザ管理するというものであったが、第３の実施形態においては、ＭＩＳサーバー１０７を設けずにユーザＰＣ１０１内にホットフォルダを作成し、そのホットフォルダに対してのユーザ管理を行うために、ユーザＰＣ内にユーザ管理プログラムとユーザのアクセスを記録するデータベース１９０２をユーザＰＣ内に設けたことが特徴となっている。

【００７６】

図１９は第３の実施形態の全体構成図を示しており、第１及び第２の実施形態とは異なり、ＭＩＳサーバー１０７を必要とせず、代わりにユーザＰＣ内でユーザ管理プログラム１９０３が動作しており、ユーザＰＣ上のホットフォルダにアクセス可能なユーザを監視している。

【００７７】

本実施形態の動作はフローチャート図１８で示されており、ＭＩＳサーバーをユーザ管理プログラムに読み替えるだけで動作的には図２と変わりがないので説明は省略する。

【００７８】

以上説明したように、本実施形態によればユーザＰＣ内にユーザ管理プログラムとユーザ管理データベースを設けることによって、複数のユーザが同一のＰＣを使用するような作業環境においては、ＭＩＳサーバーを設置しなくとも簡単にホットフォルダに対するユーザ管理を行うことが可能となる。

【００７９】

＜第４の実施形態＞

図１９は第４の実施形態の動作を説明するためのフローチャートである。第４の実施形態は、第２の実施形態の処理に加えてユーザがカラー印刷権限を有しない場合に追認処理を行うものである。第２の実施形態と同じ処理を実行するステップは同じ参照番号が付されており、ここでは第４の実施形態に特有の動作を中心に説明する。

【００８０】

ステップＳ１３０４においてユーザにカラー印刷する権限がないと判断されると、処理はステップＳ１９０１に移行する。ステップＳ１９０１では、ＭＩＳサーバー１０７は、

追認を希望するか否かをユーザに判断させるための画面を表示する指示をユーザＰＣ１０１に送信する。

【００８１】

ステップＳ１９０２では、ＭＩＳサーバー１０７から送信された指示を受信し、それに対応して追認希望画面がユーザＰＣ１０１の表示画面上に表示される。そして、ユーザによって追認希望の有無及びどのユーザによる追認を希望するかについての情報が入力され、それがＭＩＳサーバー１０７に送信される。なお、追認希望の有無を入力する画面の例が図２０に示されている。図２０で「ＹＥＳ」をクリックすると、図２１の画面がＰＣ１０１の画面上に表示される。図２１は、ネットワーク１１１に接続された全部又は一部のユーザ（図２１では１０１及びＡ～Ｅの６人）を示している。ここでは、カラー印刷権限を有するユーザはＡ及びＥで、その他のユーザには網掛けが掛かっており、権限が無いことを即座に判断できるように表示されている。そして、ＰＣ１０１のユーザとしては、Ａ又はＥのどちらに追認してもらいたいかを選択すればよく、その際にはどちらかのＰＣのアイコンダブルクリックすればよい。ダブルクリックすると、追認希望の有無と追認希望先の情報がＭＩＳサーバー１０７に送信されるのである。追認を希望しない場合には図２０の「ＮＯ」をクリックすればよく、その情報がＭＩＳサーバー１０７に送信される。

【００８２】

続いて、ステップＳ１９０４において、ユーザＰＣ１０１から追認希望に関する情報を受信し、追認希望の有無が判断される。追認なしの場合には処理はステップＳ１３０６に移行し、カラー印刷は実行せずにモノクロ印刷を実行するように白黒印刷装置１１０を制御する。

【００８３】

一方、追認の希望ありの場合には、ステップＳ１９０５において追認処理が実行される。つまり、ＰＣ１０１のユーザによって指定された追認権者（Ａ又はＥ）に追認の許否を確認する処理を行う。より具体的には、指定された追認権者に対してＭＩＳサーバー１０７から図示しない追認フォームが送信され、それに対する応答（追認ＯＫ又はＮＧ）を受信する。追認ＯＫの場合には処理はステップＳ１３０５に移行し、カラー印刷を実行するようにカラー印刷装置１１０１が制御される。追認ＮＧの場合には、例えば、別の追認権者に追認の許否を再度確認したり、強制的にモノクロ印刷処理を行うようにする。

【００８４】

以上説明したように、第４の実施形態によれば、自己がカラー印刷権限を有しない場合であっても追認処理を行うことにより、カラー印刷を実行する途を確保できるという効果がある。

【００８５】

＜その他の実施形態＞

本発明では、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或は装置に提供し、そのシステム或は装置のコンピュータ（又は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。このような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、フロッピィ（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。

【００８６】

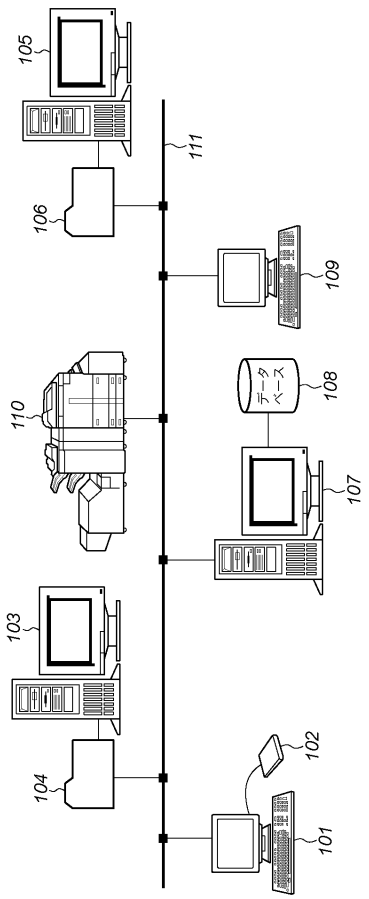
また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが実際の処理の一部又は全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれている。

【００８７】
さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書きこまれた後、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又は全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含む。
【００８８】
また、上記実施の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がネットワークを介して配信されることにより、システム又は装置のハードディスクやメモリ等の記憶手段又はＣＤ-ＲＷ、ＣＤ-Ｒ等の記憶媒体に格納され、そのシステム又は装置のコンピュータ(又はＣＰＵやＭＰＵ)が当該記憶手段や当該記憶媒体に格納されたプログラムコードを読み出して実行することによっても、達成されることは云うまでもない。
【００８９】
＜まとめ＞
本発明の実施形態によれば、管理サーバがホットフォルダに電子データが格納されるのを監視し、管理サーバーにおいてホットフォルダにアクセス可能なユーザを制限し、管理サーバーにおいてホットフォルダに印刷データが投入されてきた際には、印刷データ投入元のコンピュータ上にユーザ認証画面を表示し、ユーザ認証画面を表示することでユーザ認証を行い、ユーザ認証に成功した場合は、ホットフォルダに投入された電子データを印刷装置で印刷を行い、ユーザ認証に失敗した場合は、ホットフォルダに投入された電子データを印刷装置での印刷をキャンセルすることにより、ホットフォルダにアクセスするユーザを制限することが可能である。
【００９０】
また、管理サーバーは印刷業務の受注、納期管理、消耗品管理、印刷デバイス管理機能を併せ持つことにより、ユーザ管理だけのために別サーバーを用意する必要がなくなる。
また、管理サーバーは複数のホットフォルダに対してのユーザ管理を行えることにより、管理サーバーを一つにすることができ、管理が行い易くなる。
【００９１】
さらに、ユーザ名及びパスワード、ＩＣカードを用いることにより、ユーザ認証を行うことが可能となり、ユーザの操作性とセキュリティレベルを上げることが可能である。
【００９２】
また、ホットフォルダへのユーザ認証に成功し、印刷装置での印刷が実行された際にはユーザ名とアクセス日時をログとして記録することにより、ホットフォルダを使用したユーザの管理を行うことが可能である。
【００９３】
記録したログは管理者がウェブ・ブラウザを用いて閲覧可能としておくことにより、管理者がホットフォルダを使用したユーザのログをウェブ・ブラウザを用いて容易に閲覧することが可能である。
【００９４】
本発明の実施形態によれば、ホットフォルダを介して電子データを印刷する印刷システムであり、管理サーバーがホットフォルダに電子データが格納されるのを監視し、管理サーバーにおいてホットフォルダにアクセス可能なユーザを制限し、ユーザ毎に使用可能な印刷機能を制限し、管理サーバーにおいてホットフォルダに印刷データが投入されてきた際には、印刷データ投入元のコンピュータ上にユーザ認証画面を表示し、ユーザ認証画面を表示することでユーザ認証を行い、ユーザ認証に成功した場合は、ホットフォルダに投入された電子データを印刷制限機能でユーザに設定されている印刷機能に限定して印刷を行い、ユーザ認証に失敗した場合は、ホットフォルダに投入された電子データの印刷をキャンセルするように印刷装置を制御することにより、ホットフォルダにアクセスするユーザを制限できると共に、ユーザ毎に使用可能なホットフォルダの機能を制限することが可能である。

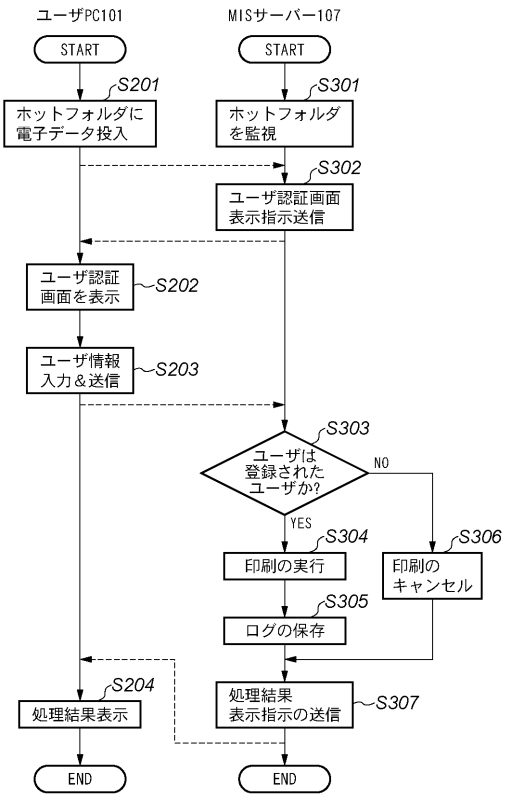
【００９５】
　また、管理サーバーは、印刷業務の受注、納期管理、消耗品管理、印刷デバイス管理機能を併せ持つことにより、ユーザ管理だけのために別サーバーを用意する必要がなくなる。
【００９６】
　前記管理サーバーは、複数のホットフォルダに対してのユーザ管理を行えることにより、管理サーバーを一つにすることができ、管理が行い易くなる。
【００９７】
　また、ユーザ認証には、ユーザ名及びパスワード、ＩＣカードを用いることにより、特に、ＩＣカードの使用によりユーザの操作性とセキュリティレベルを上げることが可能である。
【００９８】
　さらに、ホットフォルダへのユーザ認証に成功し、印刷装置での印刷が実行された際にはユーザ名とアクセス日時をログとして記録することにより、ホットフォルダを使用したユーザの管理を行うことが可能である。
【００９９】
　また、記録したログは管理者がウェブ・ブラウザを用いて閲覧可能としておくことにより、管理者がホットフォルダを使用したユーザのログをウェブ・ブラウザを用いて容易に閲覧することが可能である。
【０１００】
　さらに、印刷制限機能は、付加価値の高い印刷（カラー印刷等）の許可/不許可を設定することにより、ユーザ毎にホットフォルダで使用可能な印刷機能を細かく設定することが可能である。
【０１０１】
　本発明による実施形態によれば、ホットフォルダを介して電子データを印刷する印刷システムであり、監視プログラムがホットフォルダに電子データが格納されるのをローカルコンピュータ上で監視し、監視プログラムにおいてホットフォルダにアクセス可能なユーザを制限し、監視プログラムにおいてホットフォルダに印刷データが投入されてきた際には、ローカルコンピュータ上にユーザ認証画面を表示し、ユーザ認証画面を表示することでユーザ認証を行い、ユーザ認証に成功した場合は、ホットフォルダに投入された電子データを印刷し、ユーザ認証に失敗した場合は、ホットフォルダに投入された電子データの印刷をキャンセルするように印刷装置を制御することにより、サーバーを立てることなく、ローカルPC上だけでホットフォルダにアクセスできるユーザを制限することが可能となる。
【０１０２】
　監視プログラムは複数のホットフォルダに対してのユーザ管理を行えることにより、実行する監視プログラムは一つだけで起動しておけばよくなる。
【図面の簡単な説明】
【０１０３】
【図１】第１の実施形態の全体構成図である。
【図２】第１の実施形態の動作を説明するためのフローチャートである。
【図３】ユーザ認証画面の第１の具体例を示す図である。
【図４】ユーザ認証画面の第２の具体例を示す図である。
【図５】ウェブ・ブラウザを用いたユーザのアクセス履歴表示画面の第１具体例を示す図である。
【図６】ウェブ・ブラウザを用いたユーザのアクセス履歴表示画面の第２の具体例を示す図である。
【図７】ウェブ・ブラウザを用いたユーザのアクセス履歴表示画面の第３の具体例を示す図である。
【図８】ユーザＰＣからホットフォルダへの電子データ投入を示す図である。

【図９】第１の実施形態のホットフォルダ操作画面を示す図である。
【図１０】第１の実施形態のユーザ管理設定画面を示す図である。
【図１１】第２の実施形態の全体構成図である。
【図１２】第２の実施形態の動作を説明するためのフローチャートである。
【図１３】第２の実施形態のホットフォルダ操作画面を示す図である。
【図１４】第２の実施形態のユーザ管理設定画面の第１の具体例を示す図である。
【図１５】第２の実施形態のユーザ管理設定画面の第２の具体例を示す図である。
【図１６】第２の実施形態のユーザ管理設定画面の第３の具体例を示す図である。
【図１７】第３の実施形態の全体構成図である。
【図１８】第３の実施形態の動作を説明するためのフローチャートである。
【図１９】第４の実施形態の動作を説明するためのフローチャートである。
【図２０】追認権者の追認画面を示す図である。
【図２１】ユーザが追認権者を選択するための画面表示を示す図である。

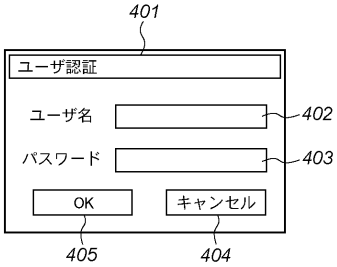
【図１】



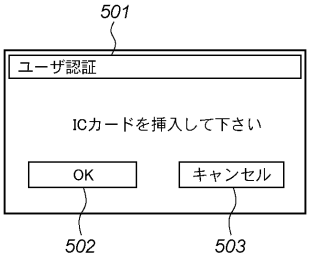
【図２】



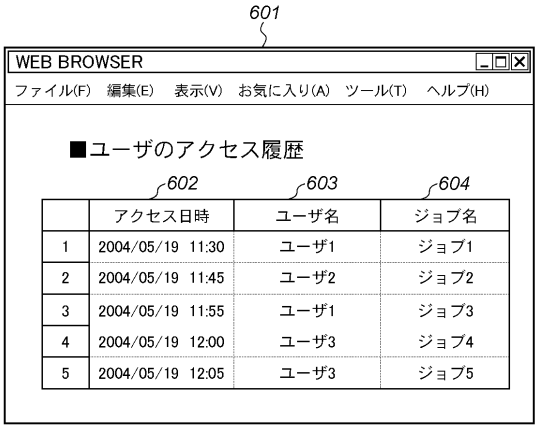
【図３】


401
ユーザ認証
ユーザ名
402
パスワード
403
OK
キャンセル
405
404

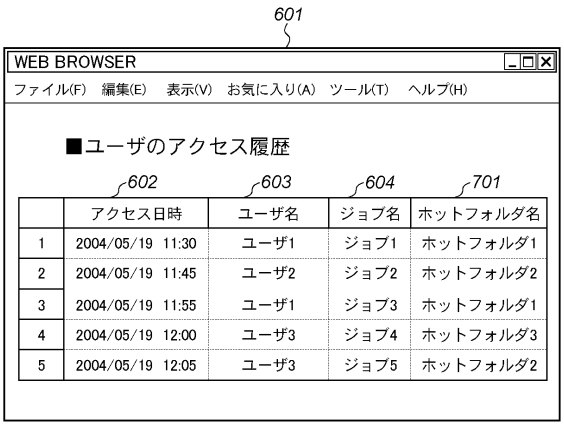
【図４】


501
ユーザ認証
ICカードを挿入して下さい
OK
キャンセル
502
503

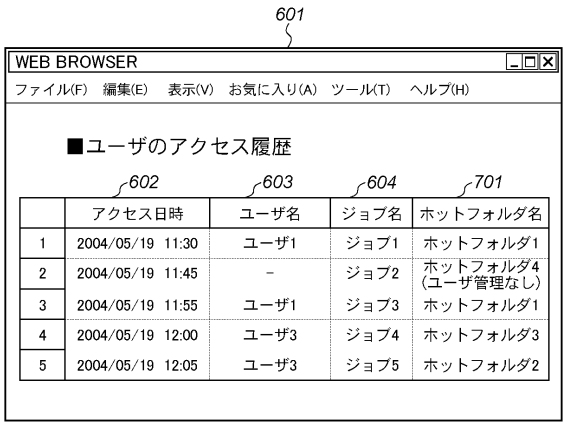
【図５】


601
WEB BROWSER
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
■ユーザのアクセス履歴
602
603
604
アクセス日時
ユーザ名
ジョブ名
1 2004/05/19 11:30 ユーザ1 ジョブ1
2 2004/05/19 11:45 ユーザ2 ジョブ2
3 2004/05/19 11:55 ユーザ1 ジョブ3
4 2004/05/19 12:00 ユーザ3 ジョブ4
5 2004/05/19 12:05 ユーザ3 ジョブ5

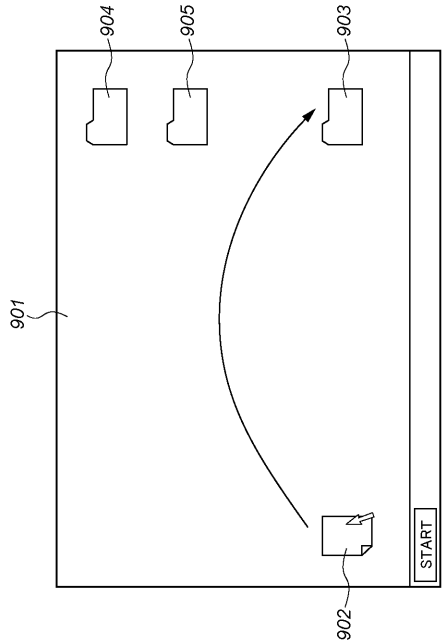
【図６】


601
WEB BROWSER
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
■ユーザのアクセス履歴
602
603
604
701
アクセス日時
ユーザ名
ジョブ名
ホットフォルダ名
1 2004/05/19 11:30 ユーザ1 ジョブ1 ホットフォルダ1
2 2004/05/19 11:45 ユーザ2 ジョブ2 ホットフォルダ2
3 2004/05/19 11:55 ユーザ1 ジョブ3 ホットフォルダ1
4 2004/05/19 12:00 ユーザ3 ジョブ4 ホットフォルダ3
5 2004/05/19 12:05 ユーザ3 ジョブ5 ホットフォルダ2

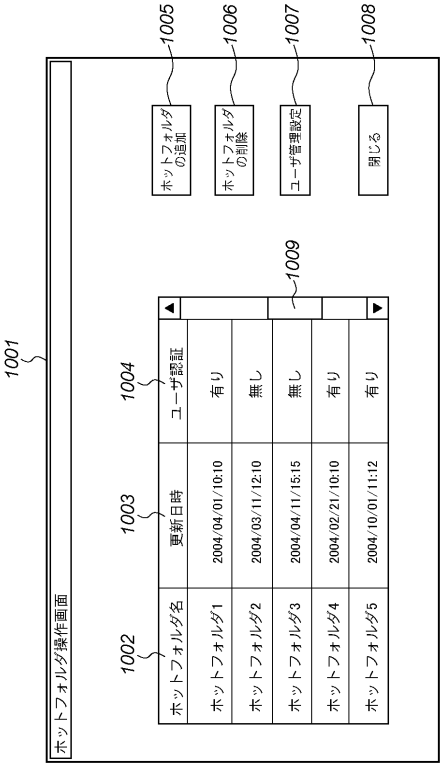
【図７】


601
WEB BROWSER
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
■ユーザのアクセス履歴
602
603
604
701
アクセス日時
ユーザ名
ジョブ名
ホットフォルダ名
1 2004/05/19 11:30 ユーザ1 ジョブ1 ホットフォルダ1
2 2004/05/19 11:45 - ジョブ2 ホットフォルダ4 (ユーザ管理なし)
3 2004/05/19 11:55 ユーザ1 ジョブ3 ホットフォルダ1
4 2004/05/19 12:00 ユーザ3 ジョブ4 ホットフォルダ3
5 2004/05/19 12:05 ユーザ3 ジョブ5 ホットフォルダ2

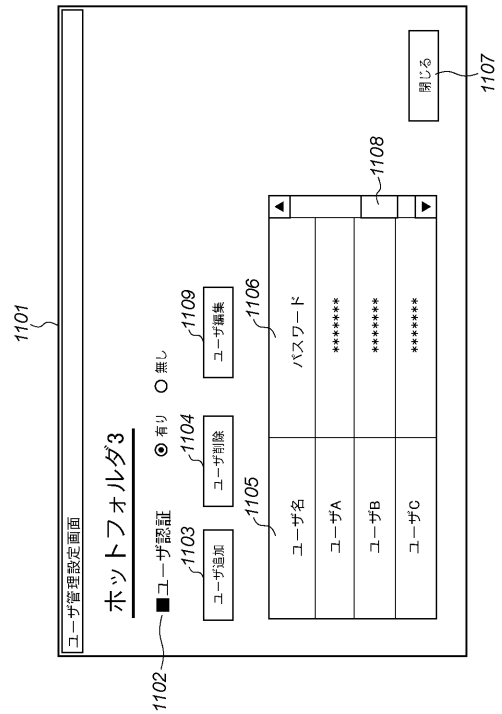
【図８】


904
905
903
901
START
902

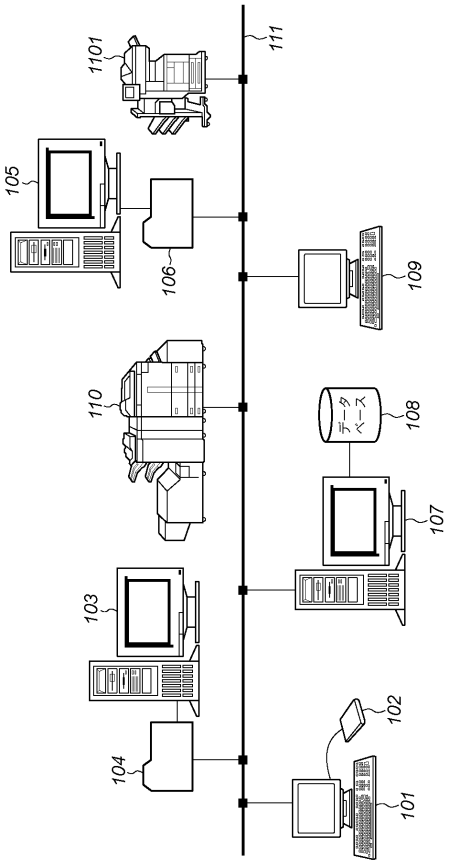
【図９】


1005
1006
1007
1008
ホットフォルダの追加
ホットフォルダの削除
ユーザ管理設定
閉じる
1001
ホットフォルダ操作画面
1009
1004
1003
1002
ホットフォルダ名
更新日時
ユーザ認証
ホットフォルダ1
2004/04/01/10:10
有り
ホットフォルダ2
2004/03/11/12:10
無し
ホットフォルダ3
2004/04/11/15:15
無し
ホットフォルダ4
2004/02/21/10:10
有り
ホットフォルダ5
2004/10/01/11:12
有り

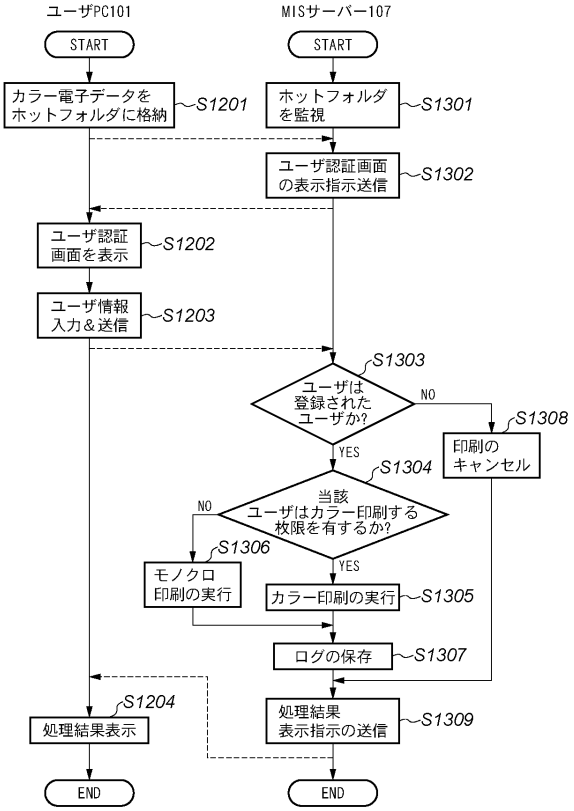
【図１０】


1101
ユーザ管理設定画面
ホットフォルダ3
■ユーザ認証
有り
無し
1102
1103
ユーザ追加
1104
ユーザ削除
1109
ユーザ編集
1105
1106
1108
1107
閉じる
ユーザ名
パスワード
ユーザA
ユーザB
ユーザC
****
****
****

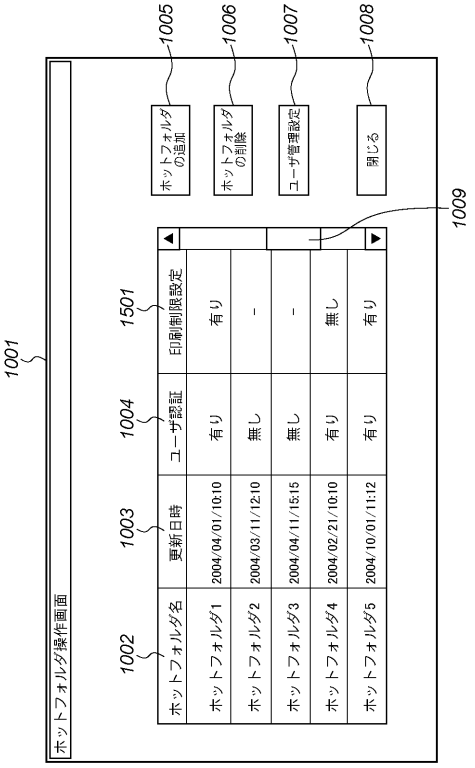
【図１１】


111
1101
105
106
109
110
108
データベース
107
103
104
102
101

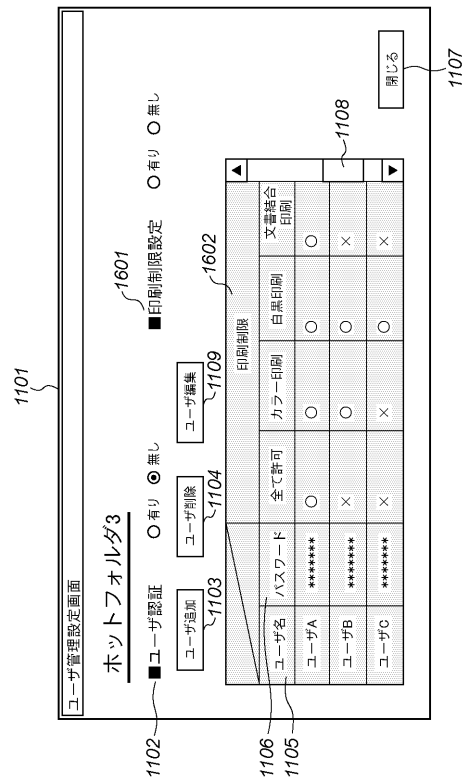
【図１２】



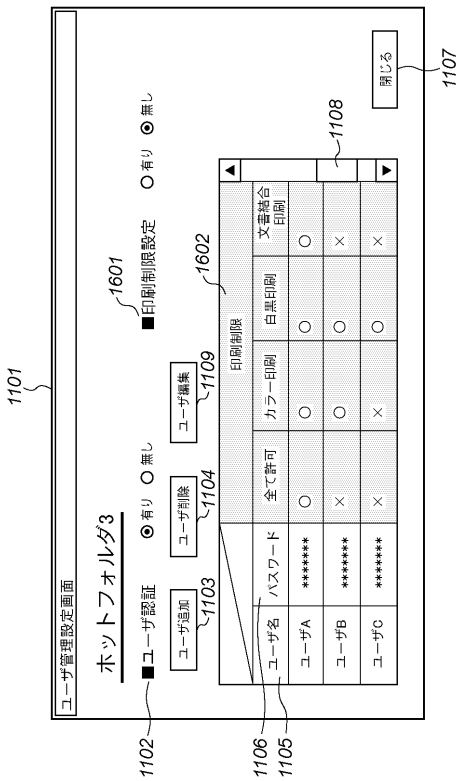
【図１３】



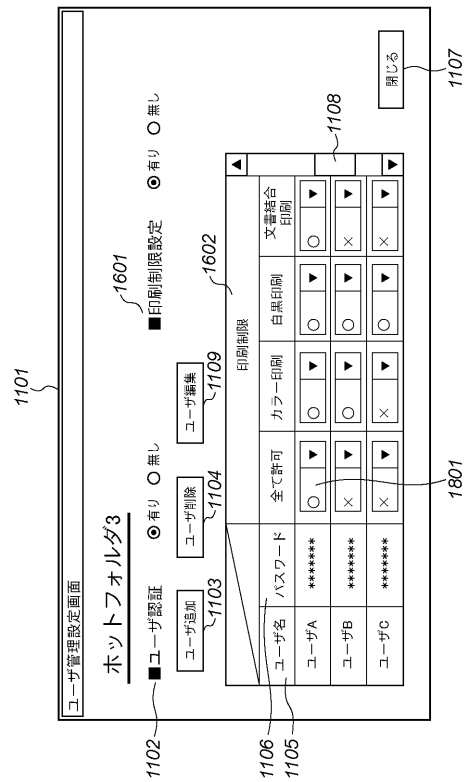
【図１４】



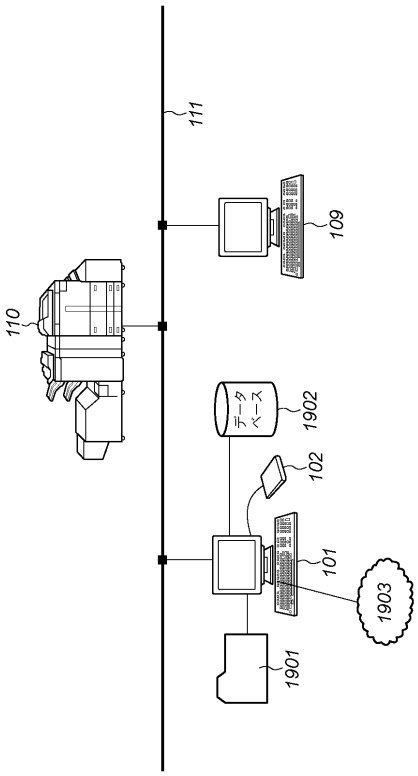
【図１５】



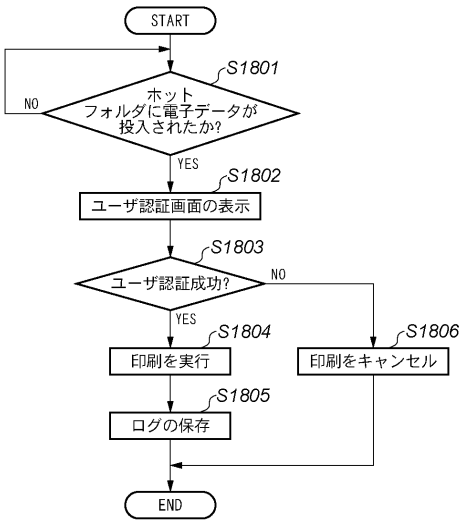
【図１６】



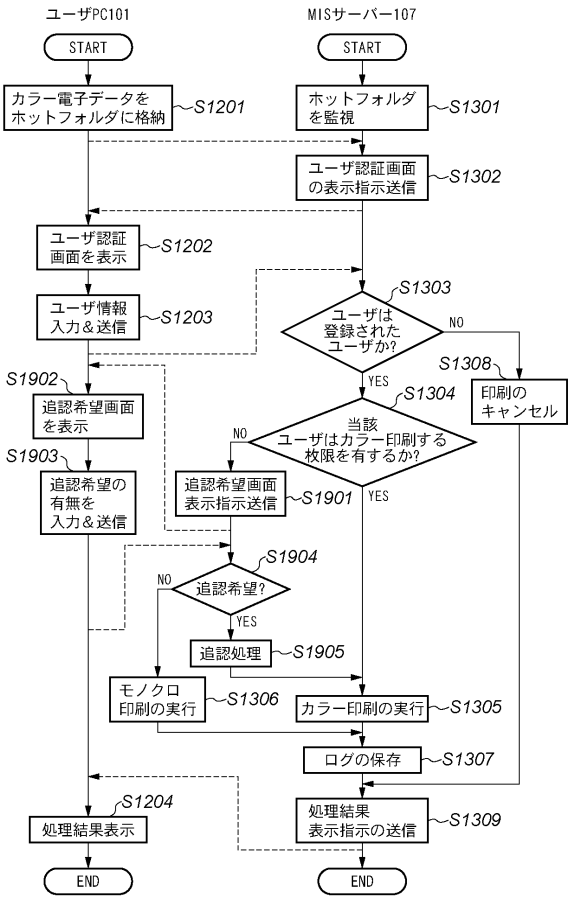
【図１７】



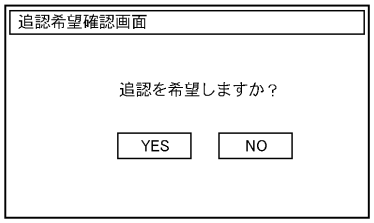
【図１８】



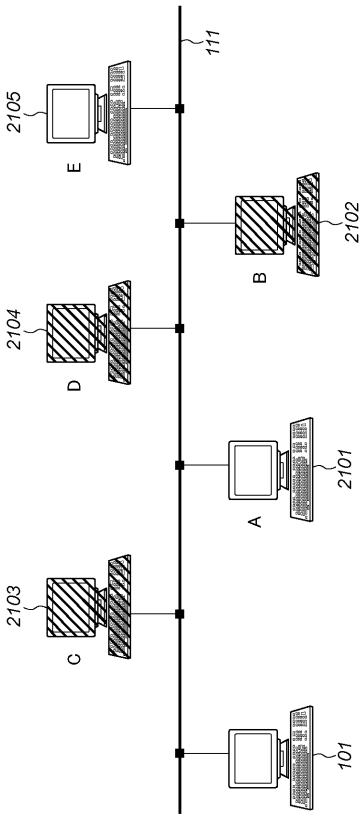
【図１９】



【図２０】


追認希望確認画面
追認を希望しますか？
YES
NO

【図２１】


111
2105
E
2102
B
2104
D
2101
A
2103
C
101

フロントページの続き

(72)発明者　寺尾　仁秀
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　岸野　徹

(56)参考文献　特開２０００－０２９６４４（ＪＰ，Ａ）
特開２００３－１９６０６９（ＪＰ，Ａ）
特開２００３－０７６５２５（ＪＰ，Ａ）
特開２００２－００７０７９（ＪＰ，Ａ）
特開２０００－１１８０９５（ＪＰ，Ａ）
特開２００３－２６０８５４（ＪＰ，Ａ）
特開２０００－２１６９３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　３／１２