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

特許第4441238号
(P4441238)

(45)発行日　平成22年3月31日(2010.3.31)　(24)登録日　平成22年1月15日(2010.1.15)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330B
G06F 3/12	(2006.01)	G06F	3/12	D
H04N 1/00	(2006.01)	H04N	1/00	107Z

請求項の数 4　(全 20 頁)

(21)出願番号　特願2003-387489 (P2003-387489)
(22)出願日　平成15年11月18日 (2003.11.18)
(65)公開番号　特開2005-149256 (P2005-149256A)
(43)公開日　平成17年6月9日 (2005.6.9)
審査請求日　平成18年1月25日 (2006.1.25)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100080931
弁理士　大澤　敬
(74)代理人　100123881
弁理士　大澤　豊
(72)発明者　寺尾　雄一
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　鳥居　稔

最終頁に続く

(54)【発明の名称】ネットワーク対応周辺装置およびその制御方法

(57)【特許請求の範囲】

【請求項１】

少なくとも１つの周辺装置機能と、ネットワークへ接続しネットワークを介して他の端末装置より前記周辺装置機能の利用を受け付けて該周辺装置機能を実行するネットワーク通信機能とを備えたネットワーク対応周辺装置において、

ローカルにユーザを認証するローカル認証機能を実現するローカル認証手段と、

前記ネットワークに設けた複数のネットワーク認証機能であって、ユーザが入力したアカウント情報を前記ローカル認証機能と共通に利用するネットワーク認証機能を利用してユーザを認証するネットワーク認証手段と、

前記ローカル認証機能と前記複数のネットワーク認証機能のおのおのの種別に優先順位を設定した認証種別優先順位テーブルと、前記ローカル認証機能と前記複数のネットワーク認証機能のおのおのの種別に対応してユーザに使用を許可する周辺装置機能の登録情報を設定した認証別登録情報テーブルとを記憶した記憶手段と、

（ａ）ユーザ認証を行う際、ユーザのアカウント情報の入力を受け付け、（ｂ）前記認証種別優先順位テーブルに従って前記ローカル認証機能又はいずれかの前記ネットワーク認証機能を選択し、（ｃ）前記ローカル認証機能を選択した場合は前記ローカル認証手段に、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｄ）いずれかの前記ネットワーク認証機能を選択した場合は前記ネットワーク認証手段に、該ネットワーク認証機能を利用して、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｅ）前記ローカル認証手段がユーザを認証したときには、前記

認証別登録情報テーブルに設定したローカル認証機能に対応した周辺装置機能の使用をユーザに許可し、前記ネットワーク認証手段がユーザを認証したときには、前記認証別登録情報テーブルに設定した、該ユーザを認証したネットワーク認証機能の種別に対応した周辺装置機能の使用をユーザに許可する制御手段とを備えたことを特徴とするネットワーク対応周辺装置。

【請求項２】

前記制御手段は、前記ローカル認証機能及び前記複数のネットワーク認証機能のうち、前記認証種別優先順位テーブルに設定した上位の優先順位のものを利用可能ではない状態では、該ローカル認証機能又はネットワーク認証機能の優先順位を一時的に最下位に設定することを特徴とする請求項１記載のネットワーク対応周辺装置。

【請求項３】

少なくとも１つの周辺装置機能と、ネットワークへ接続しネットワークを介して他の端末装置より前記周辺装置機能の利用を受け付けて該周辺装置機能を実行するネットワーク通信機能とを備えたネットワーク対応周辺装置の制御方法であって、

前記ネットワーク対応周辺装置は、ローカルにユーザを認証するローカル認証機能と前記ネットワークに設けた複数のネットワーク認証機能であって、ユーザが入力したアカウント情報を前記ローカル認証機能と共通に利用するネットワーク認証機能のおのおのの種別に優先順位を設定した認証種別優先順位テーブルと、前記ローカル認証機能と前記複数のネットワーク認証機能のおのおのの種別に対応してユーザに使用を許可する周辺装置機能の登録情報を設定した認証別登録情報テーブルとを記憶した記憶手段を備えるものであり、

前記ネットワーク対応周辺装置に、

前記ローカル認証機能を実現するローカル認証ステップと、

前記複数のネットワーク認証機能を利用してユーザを認証するネットワーク認証ステップと、

（ａ）ユーザ認証を行う際、ユーザのアカウント情報の入力を受け付け、（ｂ）前記認証種別優先順位テーブルに従って前記ローカル認証機能又はいずれかの前記ネットワーク認証機能を選択し、（ｃ）前記ローカル認証機能を選択した場合は前記ローカル認証手段に、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｄ）いずれかの前記ネットワーク認証機能を選択した場合は前記ネットワーク認証手段に、該ネットワーク認証機能を利用して、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｅ）前記ローカル認証手段がユーザを認証したときには、前記認証別登録情報テーブルに設定したローカル認証機能に対応した周辺装置機能の使用をユーザに許可し、前記ネットワーク認証手段がユーザを認証したときには、前記認証別登録情報テーブルに設定した、該ユーザを認証したネットワーク認証機能の種別に対応した周辺装置機能の使用をユーザに許可する制御ステップとを実行させることを特徴とするネットワーク対応周辺装置の制御方法。

【請求項４】

前記制御ステップは、前記ローカル認証機能及び前記複数のネットワーク認証機能のうち、前記認証種別優先順位テーブルに設定した上位の優先順位のものを利用可能ではない状態では、該ローカル認証機能又はネットワーク認証機能の優先順位を一時的に最下位に設定することを特徴とする請求項３記載のネットワーク対応周辺装置の制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、少なくとも１つの周辺装置機能と、ネットワークへ接続しネットワークを介して他の端末装置より前記周辺装置機能の利用を受け付けて該周辺装置機能を実行するネットワーク通信機能とを備えたネットワーク対応周辺装置およびその制御方法に関する。

【背景技術】

【０００２】

従来、ネットワークプリンタ装置／ネットワークスキャナ装置／インターネットファクシミリ装置に代表されるような、ＬＡＮ回線に接続するためのＩ／Ｆを備えたネットワーク対応周辺機器としては、例えば、操作パネルからユーザコードを入力したりＩＤカードを用いることでユーザや部門ごとに利用者制限を行う技術などがある（特許文献１，２参照）。

【０００３】

これによりユーザごとにコピーの色の制限やファクス送信、印刷、スキャナーなどの利用制限をかけることや、部門ごとの使用量集計や利用上の上限を設定し過度の使用を防ぐことができた。

【０００４】

また、機器利用ユーザをネットワーク上で管理されているものと統合することが可能にする技術などがある（特許文献３参照）。

【特許文献１】特開２００２－１７８５６７号公報

【特許文献２】特開２００２－２４０３９８号公報

【特許文献３】特開２００２－２０２９４５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、いずれの場合においても、利用者を特定するための認証システム（認証手段）が一つしかなく、その認証システムが正しく動作していない場合に代替手段を選択することができないという不具合を生じていた。

【０００６】

また、認証システムが一つしかないため、ある認証システムにリソース上の制約が発生したとき（例えば、メモリ制約による登録可能アカウント上限など）、その後の拡張が難しいという問題もあった。

【０００７】

本発明は、かかる実情に鑑みてなされたものであり、適切に利用者を認証することができるネットワーク対応周辺装置およびその制御方法を提供すること目的とする。

【課題を解決するための手段】

【０００８】

本発明のネットワーク対応周辺装置は、少なくとも１つの周辺装置機能と、ネットワークへ接続しネットワークを介して他の端末装置より上記周辺装置機能の利用を受け付けて該周辺装置機能を実行するネットワーク通信機能とを備えたネットワーク対応周辺装置において、ローカルにユーザを認証するローカル認証機能を実現するローカル認証手段と、上記ネットワークに設けた複数のネットワーク認証機能であって、ユーザが入力したアカウント情報を前記ローカル認証機能と共通に利用するネットワーク認証機能を利用してユーザを認証するネットワーク認証手段と、上記ローカル認証機能と上記複数のネットワーク認証機能のおのおのの種別に優先順位を設定した認証種別優先順位テーブルと、上記ローカル認証機能と上記複数のネットワーク認証機能のおのおのの種別に対応してユーザに使用を許可する周辺装置機能の登録情報を設定した認証別登録情報テーブルとを記憶した記憶手段と、（ａ）ユーザ認証を行う際、ユーザのアカウント情報の入力を受け付け、（ｂ）上記認証種別優先順位テーブルに従って上記ローカル認証機能又はいずれかの上記ネットワーク認証機能を選択し、（ｃ）上記ローカル認証機能を選択した場合は上記ローカル認証手段に、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｄ）いずれかの上記ネットワーク認証機能を選択した場合は上記ネットワーク認証手段に、該ネットワーク認証機能を利用して、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｅ）上記ローカル認証手段がユーザを認証したときには、上記認証別登録情報テーブルに設定したローカル認証機能に対応した周辺装置機能の使用をユーザに許可し、上記ネットワーク認証手段がユーザを認証したときには、上記認証別登録情報テーブルに設定した、該ユーザを認証したネットワーク認証機能の種別に

対応した周辺装置機能の使用をユーザに許可する制御手段とを備えたものである。

【０００９】

上記制御手段は、上記ローカル認証機能及び上記複数のネットワーク認証機能のうち、上記認証種別優先順位テーブルに設定した上位の優先順位のものを利用可能ではない状態では、該ローカル認証機能又はネットワーク認証機能の優先順位を一時的に最下位に設定するとよい。

【００１０】

また、本発明のネットワーク対応周辺装置の制御方法は、少なくとも１つの周辺装置機能と、ネットワークへ接続しネットワークを介して他の端末装置より上記周辺装置機能の利用を受け付けて該周辺装置機能を実行するネットワーク通信機能とを備えたネットワーク対応周辺装置の制御方法であって、上記ネットワーク対応周辺装置は、ローカルにユーザを認証するローカル認証機能と上記ネットワークに設けた複数のネットワーク認証機能であって、ユーザが入力したアカウント情報を前記ローカル認証機能と共通に利用するネットワーク認証機能のおのおのの種別に優先順位を設定した認証種別優先順位テーブルと、上記ローカル認証機能と上記複数のネットワーク認証機能のおのおのの種別に対応してユーザに使用を許可する周辺装置機能の登録情報を設定した認証別登録情報テーブルとを記憶した記憶手段を備えるものであり、上記ネットワーク対応周辺装置に、上記ローカル認証機能を実現するローカル認証ステップと、上記複数のネットワーク認証機能を利用してユーザを認証するネットワーク認証ステップと、（ａ）ユーザ認証を行う際、ユーザのアカウント情報の入力を受け付け、（ｂ）上記認証種別優先順位テーブルに従って上記ローカル認証機能又はいずれかの上記ネットワーク認証機能を選択し、（ｃ）上記ローカル認証機能を選択した場合は上記ローカル認証手段に、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｄ）いずれかの上記ネットワーク認証機能を選択した場合は上記ネットワーク認証手段に、該ネットワーク認証機能を利用して、ユーザから受け付けた前記アカウント情報に基づいてユーザの認証を行わせ、（ｅ）上記ローカル認証手段がユーザを認証したときには、上記認証別登録情報テーブルに設定したローカル認証機能に対応した周辺装置機能の使用をユーザに許可し、上記ネットワーク認証手段がユーザを認証したときには、上記認証別登録情報テーブルに設定した、該ユーザを認証したネットワーク認証機能の種別に対応した周辺装置機能の使用をユーザに許可する制御ステップとを実行させるようにしたものである。

【００１１】

上記制御ステップは、上記ローカル認証機能及び上記複数のネットワーク認証機能のうち、上記認証種別優先順位テーブルに設定した上位の優先順位のものを利用可能ではない状態では、該ローカル認証機能又はネットワーク認証機能の優先順位を一時的に最下位に設定するとよい。

【発明の効果】

【００１５】

以上のようなこの発明のネットワーク対応周辺装置およびその制御方法によれば、ローカル認証機能と複数のネットワーク認証機能を用いてユーザ認証を行える場合におけるユーザ認証のパフォーマンスを向上できると共に、運用形態の自由度が増すという効果を得る。

【発明を実施するための最良の形態】

【００１９】

以下、添付図面を参照しながら、本発明の実施の形態を詳細に説明する。

【００２０】

図１は、本発明の一実施例にかかるネットワークシステムを示している。

【００２１】

同図において、ローカルエリアネットワークＬＡＮには、複数のワークステーション装置ＷＳ１～ＷＳｎ、サーバ装置ＳＭ、ネットワーク複合機ＭＦＰ、および、ネットワークスキャナ装置ＳＣが接続されているとともに、ルータ装置ＲＴを介してインターネットへ

接続されている。したがって、ワークステーション装置ＷＳ１～ＷＳｎ、サーバ装置ＳＭ、ネットワーク複合機ＭＦＰ、およびネットワークスキャナ装置ＳＣは、インターネットを介し、他の適宜な端末装置との間でデータをやりとりすることができる。

【００２２】

ここで、サーバ装置ＳＭは、ローカルエリアネットワークＬＡＮに接続されているワークステーション装置ＷＳ１～ＷＳｎを利用するユーザ、および、ネットワークネットワーク複合機ＭＦＰに対して、ネットワーク認証（リモート認証）や電子メールの収集および配布のサービスの種々のネットワークサービスを提供するものである。また、サーバ装置ＳＭは、ユーザアカウント情報およびグループ情報を記憶したＳＡＭ（セキュリティ・アカウント・マネージャ）データベースＳＭｄを備えており、ネットワーク上の各端末（ワークステーション装置ＷＳ１～ＷＳｎ、ネットワーク複合機ＭＦＰ、および、ネットワークスキャナ装置ＳＣ）に対して、リモート認証機能を提供する外部認証サーバ機能も備えている。

【００２３】

ここで、例えば、サーバ装置ＳＭにインストールされているオペレーティングシステムが、マイクロソフト社のＷｉｎｄｏｗｓＮＴ系のサーバー向けＯＳである場合、このサーバ装置ＳＭが提供する（外部）認証サーバ機能としては、例えば、いわゆるＮＴ認証機能を適用することができる。また、これ以外の認証サーバ機能としては、例えば、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）等、ディレクトリサーバ機能が備えるユーザ認証機能を適用することができる。また、この認証サーバ機能を利用して、ネットワーク上の各端末からこのサーバ装置ＳＭにログインすることで、どの端末でも同じユーザ・アカウントとして認識されるように運用することができる。

【００２４】

また、ワークステーション装置ＷＳ１～ＷＳｎには、文書作成および文書印刷の機能を備えた文書処理ソフトウェア、電子メールを作成および送受信する機能を備えた電子メール処理ソフトウェア、および、ローカルエリアネットワークＬＡＮを介してネットワーク複合機ＭＦＰを適宜に使用するためのドライバソフトウェアなどの種々のプログラムが導入されており、特定のユーザにより使用されるものである。ここで、特定のユーザは、一人または複数人のユーザであってよい。

【００２５】

また、ネットワーク複合機ＭＦＰは、画情報や各種レポートなどを電子メールとしてやりとりするための電子メール処理機能、アナログ公衆回線網ＰＳＴＮに接続し、この公衆網を伝送路として用いてグループ３ファクシミリ伝送手順による画情報伝送を行うファクシミリ通信機能、ローカルエリアネットワークＬＡＮを介して、ワークステーション装置ＷＳ１～ＷＳｎから要求される文書印刷ジョブを処理するネットワークプリンタ機能、読み取った原稿画像データを電子メール（イーメール（＝Ｅ－ｍａｉｌ））を用いて指定された宛先へ送信するスキャン・ツー・イーメール機能等の種々の機能を備えている。

【００２６】

すなわち、このネットワーク複合機ＭＦＰは、電子メール処理機能、ファクシミリ通信機能、ネットワークプリンタ機能、および、スキャン・ツー・イーメール機能という３つの周辺装置機能をネットワーク対応の周辺装置機能として備えている。

【００２７】

また、このネットワーク複合機ＭＦＰは、ローカル認証機能も備えており、そのためのユーザアカウント情報を記憶したＳＡＭデータベースＭＦＰｄも備えている。

【００２８】

また、ネットワークスキャナ装置ＳＣは、読み取った原稿画像データを電子メールを用いて指定された宛先へ送信するスキャン・ツー・イーメール機能を、その周辺装置機能として備えている。すなわち、このネットワークスキャナ装置ＳＣは、１つの周辺装置機能をネットワーク周辺装置機能として備えている。

【００２９】
また、このネットワークスキャナ装置ＳＣは、ローカル認証機能も備えており、そのためのユーザアカウント情報を記憶したＳＡＭデータベースＳＣｄも備えている。
【００３０】
ここで、ユーザアカウント情報とは、通常は、ユーザ名と、パスワードを組にして登録したものであり、登録されたユーザ毎に作成され、ＳＡＭデータベースＭＦＰｄ，ＳＣｄには、複数ユーザについてのユーザアカウント情報が登録される。
【００３１】
図２は、ネットワーク複合機ＭＦＰの構成例を示している。
【００３２】
同図において、システム制御部１は、このネットワーク複合機ＭＦＰの各部の制御処理、ファクシミリ通信機能制御処理、複写機能制御処理、スキャン・ツー・イーメール機能制御処理、ネットワークプリンタ機能などの各種制御処理を行うものであり、システムメモリ２は、システム制御部１が実行する制御処理プログラム、および、処理プログラムを実行するときに必要な各種データなどを記憶するとともに、システム制御部１のワークエリアを構成するものであり、パラメータメモリ３は、このネットワーク複合機ＭＦＰに固有な各種の情報を記憶するためのものであり、時計回路４は、現在時刻情報を出力するものである。
【００３３】
スキャナ５は、所定の解像度で原稿画像を読み取るためのものであり、プロッタ６は、所定の解像度で画像を記録出力するためのものであり、操作表示部７は、このネットワーク複合機ＭＦＰを操作するためのもので、各種の操作キー、および、各種の表示器からなる。
【００３４】
符号化復号化部８は、画信号を符号化圧縮するとともに、符号化圧縮されている画情報を元の画信号に復号化するためのものであり、画像蓄積装置９は、符号化圧縮された状態の画情報を多数記憶するためのものである。
【００３５】
グループ３ファクシミリモデム１０は、グループ３ファクシミリのモデム機能を実現するためのものであり、伝送手順信号をやりとりするための低速モデム機能（Ｖ．２１モデム）、および、おもに画情報をやりとりするための高速モデム機能（Ｖ．１７モデム、Ｖ．３４モデム、Ｖ．２９モデム、Ｖ．２７ｔｅｒモデムなど）を備えている。
【００３６】
網制御装置１１は、このネットワーク複合機ＭＦＰをアナログ公衆回線網ＰＳＴＮに接続するためのものであり、自動発着信機能を備えている。
【００３７】
ローカルエリアネットワークインターフェース回路１２は、このネットワーク複合機ＭＦＰをローカルエリアネットワークＬＡＮに接続するためのものであり、ローカルエリアネットワーク伝送制御部１３は、ローカルエリアネットワークＬＡＮを介して、他のデータ端末装置との間で種々のデータをやりとりするための各種所定のプロトコルスイートの通信制御処理を実行するためのものである。
【００３８】
認証サービス処理部１４は、このネットワーク複合機ＭＦＰを操作するユーザについて認証する認証機能を実現するものであり、ＳＡＭデータベースＭＦＰｄを参照して行うローカル認証機能およびリモート認証機能を備えている。また、認証サービス処理部１４は、必要に応じて、ローカルエリアネットワークＬＡＮを介して、サーバ装置ＳＭに対し、リモート認証を要求する。
【００３９】
これらの、システム制御部１、システムメモリ２、パラメータメモリ３、時計回路４、スキャナ５、プロッタ６、操作表示部７、符号化復号化部８、画像蓄積装置９、グループ

３ファクシミリモデム１０、網制御装置１１、ローカルエリアネットワーク伝送制御部１３、認証サービス処理部１４、および、ＳＡＭデータベースＭＦＰｄは、内部バス１５に接続されており、これらの各要素間でのデータのやりとりは、主としてこの内部バス１５を介して行われている。

【００４０】

また、網制御装置１１とグループ３ファクシミリモデム１０との間のデータのやりとりは、直接行なわれている。

【００４１】

図３は、ネットワークスキャナ装置ＳＣの構成例を示している。

【００４２】

同図において、システム制御部２１は、このネットワークスキャナ装置ＳＣの各部の制御処理、および、スキャン・ツー・イーメール機能制御処理などの各種制御処理を行うものであり、システムメモリ２２は、システム制御部２１が実行する制御処理プログラム、および、処理プログラムを実行するときに必要な各種データなどを記憶するとともに、システム制御部２１のワークエリアを構成するものであり、パラメータメモリ２３は、このネットワークスキャナ装置ＳＣに固有な各種の情報を記憶するためのものであり、時計回路２４は、現在時刻情報を出力するものである。

【００４３】

スキャナ２５は、所定の解像度で原稿画像を読み取るためのものであり、操作表示部２６は、このネットワークスキャナ装置ＳＣを操作するためのもので、各種の操作キー、および、各種の表示器からなる。

【００４４】

符号化復号化部２７は、画信号を符号化圧縮するとともに、符号化圧縮されている画情報を元の画信号に復号化するためのものであり、画像蓄積装置２８は、符号化圧縮された状態の画情報を多数記憶するためのものである。

【００４５】

ローカルエリアネットワークインターフェース回路２９は、このネットワークスキャナ装置ＳＣをローカルエリアネットワークＬＡＮに接続するためのものであり、ローカルエリアネットワーク伝送制御部３０は、ローカルエリアネットワークＬＡＮを介して、他のデータ端末装置との間で種々のデータをやりとりするための各種所定のプロトコルスイートの通信制御処理を実行するためのものである。

【００４６】

認証サービス処理部３１は、このネットワークスキャナ装置ＳＣを操作するユーザについて認証する認証機能を実現するものであり、ＳＡＭデータベースＭＦＰｄを参照して行うローカル認証機能およびリモート認証機能を備えている。また、認証サービス処理部３１は、必要に応じて、ローカルエリアネットワークＬＡＮを介して、サーバ装置ＳＭに対し、リモート認証を要求する。

【００４７】

これらの、システム制御部２１、システムメモリ２２、パラメータメモリ２３、時計回路２４、スキャナ２５、操作表示部２６、符号化復号化部２７、画像蓄積装置２８、ローカルエリアネットワーク伝送制御部３０、認証サービス処理部３１、および、ＳＡＭデータベースＳＣｄは、内部バス３２に接続されており、これらの各要素間でのデータのやりとりは、主としてこの内部バス３２を介して行われている。

【００４８】

ここで、本実施例において、基本的には、ローカルエリアネットワークＬＡＮに接続されている端末相互間でのデータのやりとりは、いわゆるＴＣＰ／ＩＰと呼ばれるトランスポートレイヤまでの伝送プロトコルと、それ以上の上位レイヤの通信プロトコルとの組み合わせ（いわゆるプロトコルスイート）が適用して行われる。例えば、電子メールのデータのやりとりでは上位レイヤの通信プロトコルとしてＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）という通信プロトコルが適用される。

【００４９】
また、各端末がメールサーバ装置ＳＭに対して、ユーザ宛の電子メールの受信確認や取得要求などのために適用するプロトコルとしては、いわゆるＰＯＰ（Ｐｏｓｔ　Ｏｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ）などを適用することができる。
【００５０】
また、ＴＣＰ／ＩＰ，ＳＭＴＰ，ＰＯＰなどの通信プロトコル、および、電子メールのデータ形式やデータ構造などについては、それぞれＩＥＴＦから発行されているＲＦＣ文書により規定されている。例えば、ＴＣＰはＲＦＣ７９３、ＩＰはＲＦＣ７９３、ＳＭＴＰはＲＦＣ８２１、電子メールの形式は、ＲＦＣ８２２，ＲＦＣ１５２１，ＲＦＣ１５２２（ＭＩＭＥ（Ｍｕｌｔｉ　Ｐｕｒｐｏｓｅ　Ｍａｉｌ　Ｅｘｔｅｎｓｉｏｎ）形式）などでそれぞれ規定されている。
【００５１】
さて、本実施例では、まず、このネットワークを利用するユーザには、ユーザ名が登録されるとともに、認証用のパスワードが登録されている。そして、ネットワーク複合機ＭＦＰおよびネットワークスキャナ装置ＳＣでは、ユーザが操作表示部７，２６のいずれかの操作キーをオン操作すると、図４に示したような認証画面を表示し、ユーザに対してユーザ名とパスワードの入力を要求し、所定の認証動作を行い、その認証を突破したユーザのみ、自端末の操作を許可するようにしている。
【００５２】
なお、ネットワーク複合機ＭＦＰおよびネットワークスキャナ装置ＳＣの認証機能は、システム設定により使用するか否かの設定登録がなされる。
【００５３】
図５は、ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理の一例を示している。なお、ネットワークスキャナ装置ＳＣのシステム制御部２１も、同様の処理を行う。
【００５４】
まず、操作表示部７のいずれかの操作キーがオン操作されるまで、通常の状態表示画面を表示する（処理１０１、判断１０２のＮＯループ）。
【００５５】
ユーザが、操作表示部７のいずれかの操作キーをオン操作して、判断１０２の結果がＹＥＳになると、システム的に、認証機能を利用する旨が設定されているかどうかを調べる（判断１０３）。
【００５６】
判断１０３の結果がＹＥＳになるときには、図４に示したような認証画面を表示して、ユーザに対してユーザ名とパスワードの入力を要求して、ユーザにユーザ名とパスワードを入力させる（処理１０４）。
【００５７】
次いで、処理１０４で入力されたユーザ名とパスワードを用いて、認証サービス処理部１４に、ローカル認証を行わせる（処理１０５）。このローカル認証では、認証サービス処理部１４は、ＳＡＭデータベースＭＦＰｄの記憶内容を参照し、入力されたユーザ名のユーザアカウント情報が登録されているかどうかを調べ、登録されている場合には、当該ユーザアカウント情報からパスワードを読み出し、入力されたパスワードと比較する。そして、パスワードの比較が一致すると、認証結果がＯＫ（すなわち、ログイン成功）であると判断する。
【００５８】
ここで、認証サービス処理部１４が認証結果をＯＫと判断したかどうかを調べ（判断１０６）、判断１０６の結果がＹＥＳになるときには、通常の操作画面（図示略）を表示して（処理１０７）、次の処理へと移行する。
【００５９】
また、ローカル認証の結果がＯＫではなく、判断１０６の結果がＮＯになるときには、

認証サービス処理部１４は、ユーザ名とパスワードをサーバ装置ＳＭの外部認証サーバへ送信し、認証要求する（処理１０８）。

【００６０】

これにより、ローカルエリアネットワークＬＡＮを介して、認証要求がサーバ装置ＳＭの認証サーバ機能に発行され、それによって、サーバ装置ＳＭでは、ＳＡＭデータベースＳＭｄを参照して、ユーザ認証を行い、その結果を、認証要求元のネットワーク複合機ＭＦＰへと送信する。

【００６１】

これにより、ネットワーク複合機ＭＦＰは、サーバ装置ＳＭより認証結果を受信するので、その受信結果が認証ＯＫであるかどうかを調べ（判断１０９）、判断１０９の結果がＹＥＳになるときには、処理１０７へ進み、通常の操作画面（図示略）を表示して、次の処理へと移行する。

【００６２】

また、判断１０９の結果がＮＯになるときには、自端末のローカル認証でも、サーバ装置ＳＭのリモート認証によっても、ユーザアカウントを確認できなかった場合であり、このローカルエリアネットワークＬＡＮへログインできない場合であるので、例えば、「ログインできません」等のエラーメッセージを表示するエラー画面を表示し（処理１１０）、処理１０１へ戻って、初期画面を表示する。

【００６３】

また、システム的に認証機能を利用しない旨が設定されている場合で、判断１０３の結果がＮＯになるときには、処理１１０へ移行し、エラー画面を表示し、処理１０１へ戻って、初期画面を表示する。

【００６４】

このようにして、本実施例では、ローカル認証システム（ローカル認証手段）にアカウント情報がないときに別のリモート認証システムを利用するので、認証システムが停電やハードウェア故障など諸事情により機能しなくなったときでも使用することが可能となる。

【００６５】

また、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣにローカル認証システムを持つ場合、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣのユーザ認証については、認証サーバ機能を利用することができるので、このローカル認証システム側に持たせるアカウント情報の数を削減することができ、その結果、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣのコストを低減することができる。また、この場合、例えば、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣの設定管理等を行える管理者のアカウント情報のみをローカルアカウントとして登録し、それ以外の一般ユーザのアカウント情報はサーバ装置ＳＭの認証システムを利用するなどの運用が可能となる。

【００６６】

ところで、認証システム（認証手段）が、ローカルエリアネットワークＬＡＮに複数設けられている場合、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣで利用する認証システムに優先順位を設けることが可能となる。

【００６７】

例えば、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣで、ローカル認証と、ＮＴ認証と、ＬＤＡＰ認証を利用することができる場合、図６（ａ），（ｂ）に示したような優先順位選択画面を表示して、それらの認証の優先順位を適宜に設定操作することができる。

【００６８】

例えば、図６（ａ）では、「ローカル認証」、「ＮＴ認証」、「ＬＤＡＰ認証」の順に並んでおり、この順に優先順位が高い設定となっている。すなわち、この場合、ローカル認証が優先順位第１位、ＮＴ認証が優先順位第２位、ＬＤＡＰ認証が優先順位第３位に、

それぞれ設定されている。

【００６９】

この画面で、ローカル認証を選択し（選択した項目は、斜体で強調表示している）、鍵付き下矢印のシンボルを操作すると、同図（ｂ）に示したように、ローカル認証の優先順位が１つ下がり、２番目であったＮＴ認証の優先順位が１つ上がる態様に表示が変化する。そして、この状態で、「設定」ボタンを操作すると、変更操作内容が確定し、ＮＴ認証が優先順位第１位、ローカル認証が優先順位第２位、ＬＤＡＰ認証が優先順位第３位にそれぞれ設定される。

【００７０】

また、同図（ｂ）の状態で、鍵付き上矢印のシンボルを操作すると、同図（ａ）の状態へと変化し、この状態で、「設定」ボタンを操作すると、変更操作内容が確定し、ローカル認証が優先順位第１位、ＮＴ認証が優先順位第２位、ＬＤＡＰ認証が優先順位第３位にそれぞれ（再）設定される。

【００７１】

そして、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣは、このような認証種別についての優先順位の設定情報は、図７に示すような認証種別優先順位テーブルに保存される。この認証種別優先順位テーブルは、優先順位に従って３つの認証種別情報が配置されるものである。

【００７２】

図８は、この場合に、ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理の一例を示している。なお、ネットワークスキャナ装置ＳＣのシステム制御部２１も、同様の処理を行う。

【００７３】

まず、操作表示部７のいずれかの操作キーがオン操作されるまで、通常の状態表示画面を表示する（処理２０１、判断２０２のＮＯループ）。

【００７４】

ユーザが、操作表示部７のいずれかの操作キーをオン操作して、判断２０２の結果がＹＥＳになると、システム的に、認証機能を利用する旨が設定されているかどうかを調べる（判断２０３）。

【００７５】

判断２０３の結果がＹＥＳになるときには、図４に示したような認証画面を表示して、ユーザに対してユーザ名とパスワードの入力を要求して、ユーザにユーザ名とパスワードを入力させる（処理２０４）。

【００７６】

次に、カウンタｎの値を１に初期設定し（処理２０５）、認証種別優先順位テーブルからｎ番目の認証種別を判断して（処理２０６）、処理２０６で判断した認証種別に対応した認証処理を行う（処理２０７）。ローカル認証の場合には、処理２０４で入力されたユーザ名とパスワードを用いて、認証サービス処理部１４に、ローカル認証を行わせる。ＮＴ認証またはＬＤＡＰ認証の場合には、リモート認証であり、ＮＴ認証サーバまたはＬＤＡＰ認証サーバに対して、処理２０４で入力されたユーザ名とパスワードを通知して認証要求し、そのＮＴ認証サーバまたはＬＤＡＰ認証サーバから認証結果を受信する。

【００７７】

処理２０７で行った認証処理の結果、認証ＯＫ（ログイン成功）となったかどうかを調べ（判断２０８）、

【００７８】

そして、判断２０８の結果がＹＥＳになるときには、通常の操作画面（図示略）を表示して（処理２０９）、次の処理へと移行する。

【００７９】

また、処理２０７で行った認証結果が認証ＯＫではなく、判断２０８の結果がＮＯになるときには、試行できる他の認証種別があるかどうかを調べ（判断２１０）、判断２１０

の結果がＹＥＳになるときには、カウンタｎの値を１つ増やして（処理２１１）、処理２０６へ戻り、次の認証種別についての認証動作を行う。

【００８０】

また、全ての認証種別について認証ＮＧとなった場合、すなわち、いずれの認証種別を試行しても、認証ＯＫ（ログイン成功）とはならなかった場合で、判断２１０の結果がＮＯになるときには、例えば、「ログインできません」等のエラーメッセージを表示するエラー画面を表示し（処理２１２）、処理２０１へ戻って、初期画面を表示する。

【００８１】

また、システム的に認証機能を利用しない旨が設定されている場合で、判断２０３の結果がＮＯになるときには、処理２１２へ移行し、エラー画面を表示し、処理２０１へ戻って、初期画面を表示する。

【００８２】

このようにして、本実施例では、試行する認証種別（認証手段）の優先順位を設定できるので、利用環境に合わせてよりパフォーマンスの高い操作性を実現できる。たとえば、ほとんどの利用者はネットワーク上のサーバ装置ＳＭにアカウント情報を持ち、ある特定のユーザ（たとえば機器の管理者）のみ、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣのローカルにアカウント情報を持たせるようにした場合、このような環境下では、通常ネットワーク上のサーバに認証を先に取得しにいったほうが処理のオーバーヘッドが少なく、レスポンスに優れている。複数のリモート認証を行うような場合であっても同様である。通常、周辺機器利用者の環境はさまざまであり、本実施例のようにすることで、その環境に最適なパフォーマンスを得ることが可能となる。

【００８３】

ところで、認証システムに障害が発生して利用することができなくなっている場合、別の認証システムを利用することが好ましい。上述したように、認証種別に優先順位を設けている場合、障害が発生している認証種別の優先順位を一時的に下げることで、次に認証作業を行うときに要する時間を短縮することができる。また、その発生していた障害が解消し、認証システムが回復した場合には、元の優先順位に戻すことで、本来の認証システムの運用態様へ復帰することができる。

【００８４】

そこで、この場合には、まず、図９（ａ），（ｂ）に示すように、設定されている認証種別の優先順位を保存した基準認証種別優先順位テーブルと、現在の認証種別の優先順位を保存した参照認証種別優先順位テーブルを設ける。

【００８５】

そして、初期状態では、基準認証種別優先順位テーブルの内容を参照認証種別優先順位テーブルの内容へコピーし、その後は、認証システムの障害が発生すると、参照認証種別優先順位テーブルの内容を、適宜に変更する。

【００８６】

この後、例えば、一定の時間周期で、それぞれの認証システムの状態を調べ、障害が回復している場合には、当該認証システムの認証種別について、基準認証種別優先順位テーブルに保存されている優先順位に、参照認証種別優先順位テーブルの内容を復帰させる。

【００８７】

図１０は、この場合に、ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理の一例を示している。なお、ネットワークスキャナ装置ＳＣのシステム制御部２１も、同様の処理を行う。

【００８８】

まず、操作表示部７のいずれかの操作キーがオン操作されるまで、通常の状態表示画面を表示する（処理３０１、判断３０２のＮＯループ）。

【００８９】

ユーザが、操作表示部７のいずれかの操作キーをオン操作して、判断３０２の結果がＹＥＳになると、システム的に、認証機能を利用する旨が設定されているかどうかを調べる

（判断３０３）。

【００９０】

判断３０３の結果がＹＥＳになるときには、図４に示したような認証画面を表示して、ユーザに対してユーザ名とパスワードの入力を要求して、ユーザにユーザ名とパスワードを入力させる（処理３０４）。

【００９１】

次に、カウンタｎの値を１に初期設定し（処理３０５）、参照認証種別優先順位テーブルからｎ番目の認証種別を判断して（処理３０６）、処理３０６で判断した認証種別に対応した認証処理を行う（処理３０７）。すなわち、ローカル認証の場合には、処理３０４で入力されたユーザ名とパスワードを用いて、認証サービス処理部１４に、ローカル認証を行わせる。ＮＴ認証またはＬＤＡＰ認証の場合には、リモート認証であり、ＮＴ認証サーバまたはＬＤＡＰ認証サーバに対して、処理３０４で入力されたユーザ名とパスワードを通知して認証要求し、そのＮＴ認証サーバまたはＬＤＡＰ認証サーバから認証結果を受信する。

【００９２】

処理３０７で行った認証処理の結果、認証ＯＫ（ログイン成功）となったかどうかを調べ（判断３０８）、

【００９３】

そして、判断３０８の結果がＹＥＳになるときには、通常の操作画面（図示略）を表示して（処理３０９）、次の処理へと移行する。

【００９４】

また、処理３０７で行った認証結果が認証ＯＫではなく、判断３０８の結果がＮＯになるときには、そのときに試行した認証システムに障害が発生しているかどうかを調べる（判断３１０）。この認証システムに障害が発生しているか否かの判定は、当該認証システムに固有な適宜な周知方法で行うことができるので、ここでは説明を省略する。

【００９５】

判断３１０の結果がＹＥＳになるときには、参照認証種別優先順位テーブルにおける当該認証種別の優先順位を、最下位に変更する（処理３１１）。また、判断３１０の結果がＮＯになるときには、処理３１１を行わない。

【００９６】

次に、試行できる他の認証種別があるかどうかを調べ（判断３１２）、判断３１２の結果がＹＥＳになるときには、カウンタｎの値を１つ増やして（処理３１３）、処理３０６へ戻り、次の認証種別についての認証動作を行う。

【００９７】

また、全ての認証種別について認証ＮＧとなった場合、すなわち、いずれの認証種別を試行しても、認証ＯＫ（ログイン成功）とはならなかった場合で、判断３１２の結果がＮＯになるときには、例えば、「ログインできません」等のエラーメッセージを表示するエラー画面を表示し（処理３１４）、処理３０１へ戻って、初期画面を表示する。

【００９８】

また、システム的に認証機能を利用しない旨が設定されている場合で、判断３０３の結果がＮＯになるときには、処理３１４へ移行し、エラー画面を表示し、処理３０１へ戻って、初期画面を表示する。

【００９９】

図１１は、認証システムに発生した障害が回復した際に、変更した参照認証種別優先順位テーブルの内容を復帰する場合の処理の一例を示している。この処理は、例えば、一定時間間隔（一日、一時間等）で周期的に行われるものである。

【０１００】

まず、基準認証種別優先順位テーブルの内容と、参照認証種別優先順位テーブルの内容とを比較し（処理４０１）、それらが一致しているかどうかを調べる（判断４０２）。判断４０２の結果がＹＥＳになるときには、この処理を終了する。

【０１０１】
また、判断４０２の結果がＮＯになるときには、カウンタｎの値を１に設定し（処理４０３）、参照認証種別優先順位テーブルでのｎ番目の認証種別を判断し（処理４０４）、当該認証種別の認証システムを検査する（処理４０５）。この認証システムの検査方法は、当該認証システムに固有な適宜な周知方法で行うことができるので、ここでは説明を省略する。
【０１０２】
そして、そのときの検査結果を保存し（処理４０６）、次の認証種別があるかどうかを調べ（判断４０７）、判断４０７の結果がＹＥＳになるときには、カウンタｎの値を１つ増やし（処理４０８）、処理４０４へ戻って、次の認証種別の認証システムについて検査を行う。
【０１０３】
全ての認証種別について、認証システムの検査が終了した場合で、判断４０７の結果がＮＯになるときには、処理４０６で保存している確認証システムについての検査結果に基づいて、参照認証種別優先順位テーブルの内容を変更する（処理４０９）。この場合、例えば、検査結果で正常となっている認証種別については、基準認証種別優先順位テーブルでの優先順位に、参照認証種別優先順位テーブルでの優先順位を設定する。
【０１０４】
このようにして、本実施例では、故障した認証システムの優先順位を、一時的に最下位に変更しているので、より効率的な認証レスポンスを得ることができる。
【０１０５】
なお、通常時に使用する認証システム、異常時に使用する認証システムを分けることで、認証システムのバックアップ機能を実現することもできる。
【０１０６】
ところで、上述したように複数の認証システムを使い分ける場合、ユーザが認証ＯＫとなった認証システム別に、当該ユーザの使用可能な機能を制限あるいは設定することができる。
【０１０７】
例えば、ローカル認証で使用するＳＡＭデータベースＭＦＰｄ，ＳＣｄには、管理者ユーザのアカウント情報のみを登録し、一般ユーザのアカウント情報はサーバ装置ＳＭのＳＡＭデータベースＳＭｄに登録している場合には、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣの管理者ユーザが認証ＯＫとなるのは、ローカル認証であり、一般ユーザが認証ＯＫとなるのは、リモート認証である。
【０１０８】
そこで、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣに、認証システム別に使用を許可する機能の登録情報を作成して保存しておき、そのときの操作ユーザがローカル認証で認証ＯＫとなった場合には、ローカル認証に登録されている登録情報に基づいて操作を許可し、そのときの操作ユーザがリモート認証で認証ＯＫとなった場合には、リモート認証に登録されている登録情報に基づいて操作を許可する。
【０１０９】
このときに参照する認証別登録情報テーブルの一例を図１２（ａ）に示す。なお、この認証別登録情報テーブルは、ネットワーク複合機ＭＦＰの場合である。ネットワークスキャナ装置ＳＣの場合には、初期設定と、スキャナ関連の情報のみが登録される。
【０１１０】
この認証別登録情報テーブルは、ネットワーク複合機ＭＦＰの初期設定操作を許すか否かを示す「初期設定権限情報」、ネットワーク複合機ＭＦＰの複写機能の利用を許すか否かを示す「コピー利用権限情報」、複写機能を利用する際に利用可能な種々の機能を設定するための「コピー利用登録情報」、ネットワーク複合機ＭＦＰのスキャン・ツー・イーメール機能の利用を許すか否かを示す「スキャナ利用権限情報」、スキャン・ツー・イーメール機能を利用する際に利用可能な種々の機能を設定するための「スキャナ利用登録情

報」、ネットワーク複合機ＭＦＰのファクス送信機能の利用を許すか否かを示す「ファクス送信権限情報」、ファクス送信機能を利用する際に利用可能な種々の機能を設定するための「ファクス送信利用登録情報」、ネットワーク複合機ＭＦＰのネットワークプリンタ機能の利用を許すか否かを示す「プリンタ利用権限情報」、および、ネットワークプリンタ機能を利用する際に利用可能な種々の機能を設定するための「プリンタ利用登録情報」からなる。

【０１１１】

また、この認証別登録情報テーブルは、ネットワーク複合機ＭＦＰの操作表示部７を操作して登録される。

【０１１２】

例えば、認証種別Ａ（ローカル認証）について、利用可能な機能を登録する場合、登録画面の初期画面は、図１３（ａ）に示すようなものとなり、使用できる機能として「初期設定」を設定するために、ボタン「初期設定」をオン操作すると、同図（ｂ）に示すように、ボタン「初期設定」の表示が登録状態（図では、太字斜体で表示）となり、認証種別Ａには、「初期設定」が機能登録される。

【０１１３】

なお、通常、「初期設定」については、管理者権限を有するグループのみが使用可能に登録される。

【０１１４】

また、認証種別Ｂ（リモート認証）について、利用可能な機能を登録する場合、登録画面の初期画面は、同図（ｃ）に示すようなものとなり、使用できる機能として「コピー（複写）」機能を設定するために、ボタン「コピー」をオン操作すると、図１４（ａ）に示すように、複写機能でさらに利用可能な設定条件等を登録するための画面が表示され、この登録画面の操作項目を適宜に操作することで、コピー利用登録情報への登録内容が指定される。登録を終了して、ボタン「設定」を操作すると、コピー利用登録情報への登録内容が決定されて、同図（ｂ）に示すような画面へ戻る。この画面では、既に登録が完了しているボタン「コピー」が登録状態となる。

【０１１５】

これにより、当該認証別登録情報テーブルのコピー利用権限情報に「コピー利用許可」をあらわす情報が登録されるとともに、コピー利用登録情報に、決定されたコピー機能使用時に適用可能な種々の情報が登録される。

【０１１６】

同様にして、スキャン・ツー・イーメール機能を登録する場合には、ボタン「スキャナ」を操作し、それに続く登録画面で所定の利用可能な機能等の登録を行い、ネットワークプリンタ機能を登録する場合には、ボタン「プリンタ」を操作し、それに続く登録画面で所定の利用可能な機能等の登録を行う。

【０１１７】

これらの３つの機能を登録した後の画面では、同図（ｃ）に示したように、ボタン「コピー」、ボタン「スキャナ」、および、ボタン「プリンター」の表示形態が登録状態となる。

【０１１８】

なお、同様にして、ボタン「ファクス送信」が操作された場合には、ファクス送信に関する情報が保存されるとともに、その後の登録画面では、ボタン「ファクス送信」の表示形態が登録状態となる。

【０１１９】

また、利用登録情報としては、例えば、コピー利用登録情報の場合には、上述したように、印刷色、印刷枚数、給紙トレイ等が登録される。プリンター利用登録情報の場合も、印刷色、印刷枚数、給紙トレイ等が登録される。また、スキャナ利用登録情報やファクシミリ送信利用登録情報の場合には、出力宛先を制限する情報や、使用可能な用紙サイズや、符号化方式指定情報等が登録される。出力宛先を制限する情報としては、例えば、「無

制限」等である。

【０１２０】

なお、認証別登録情報テーブルとして、例えば、図１２（ｂ）に示すように、ユーザが利用可能な時間帯を指定する利用可能時間帯情報を追加することもできる。この場合、ネットワーク複合機ＭＦＰは、ユーザが適用される認証種別に設定されている利用可能時間帯に限って、当該ユーザの利用を許可するように利用制限することができる。

【０１２１】

図１５は、この場合、通常操作画面からユーザ操作が入力された場合の処理の一例を示している。

【０１２２】

ユーザ操作入力がされると（処理５０１）、そのときに操作入力された機能と、当該ユーザの認証種別を判定し（処理５０２）、当該認証種別に対応した認証別登録情報テーブルから、当該機能に対応した利用権限情報と利用登録情報を読み出し（処理５０３）、当該機能をユーザが利用可能であるかを調べ（判断５０４）、判断５０４の結果がＹＥＳになるときには、利用登録情報の内容に従って、操作画面を編集し（処理５０５）、選択された機能処理（周辺機器機能処理）を実行する（処理５０６）。

【０１２３】

また、判断５０４の結果がＮＯになるときには、例えば、「利用権限がありません」等のエラーメッセージを表示して（処理５０７）、この処理を終了する。

【０１２４】

このようにして、本実施例では、認証が得られたシステムごとに利用者に制限を持たせられるので、たとえば外部からの訪問者と社内利用者とで認証システムを分け、それぞれに利用制限をかけることも可能となり、運用形態の自由度が増す。

また、認証システムの優先順位を設定できるので、利用環境に合わせてよりパフォーマンスの高い操作性を実現できる。

また、障害が発生していると判断される認証手段の優先順位を一時的により下位に設定することにより、障害が発生してレスポンスタイムが大幅に遅れる認証手段を利用する事態を回避でき、より効率的な認証レスポンスを得ることができる。

【０１２５】

なお、上述した各実施例は、ネットワーク複合機ＭＦＰあるいはネットワークスキャナ装置ＳＣに適用しているが、本発明は、それ以外のネットワーク対応周辺装置、例えば、ネットワークプリンタ装置や、ネットワーク対応コピー装置等についても、同様にして適用することができる。

【０１２６】

また、本発明が適用されるネットワークシステムは、上述した実施例のものに限ることはない。また、ネットワーク上に存在する認証サーバの種別や導入される基本ソフトウェア（オペレーティングシステム）の種類等も、上述した実施例のものに限ることはない。

【図面の簡単な説明】

【０１２７】

【図１】本発明の一実施例にかかるネットワークシステムを示したブロック図。

【図２】ネットワーク複合機ＭＦＰの構成例を示したブロック図。

【図３】ネットワークスキャナ装置ＳＣの構成例を示したブロック図。

【図４】認証画面の一例を示した概略図。

【図５】ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理の一例を示したフローチャート。

【図６】優先順位選択画面の一例を示した概略図。

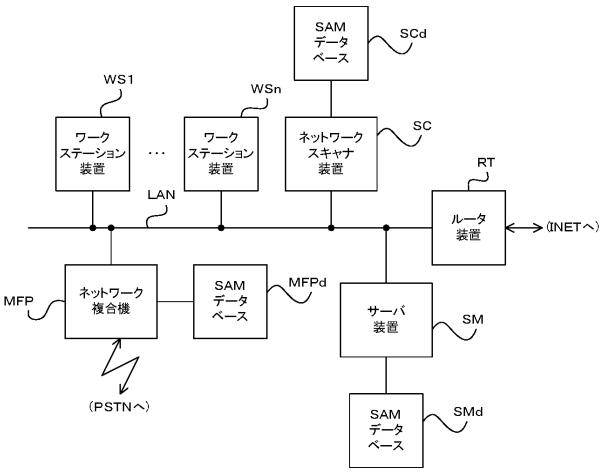
【図７】認証種別優先順位テーブルの一例を示した概略図。

【図８】ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理の他の例を示したフローチャート。

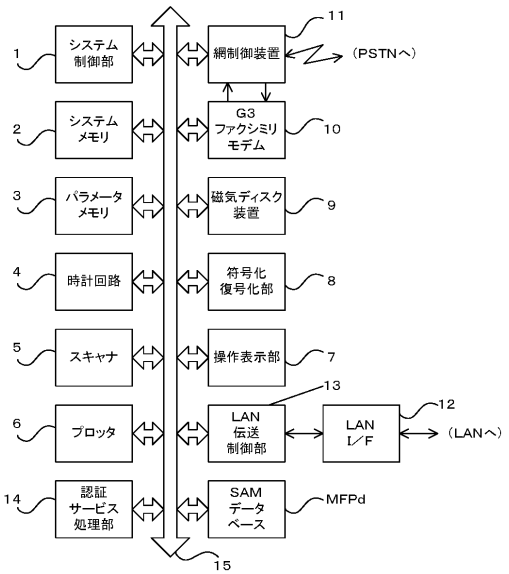
【図９】基準認証種別優先順位テーブルおよび参照認証種別優先順位テーブルの一例を示

した概略図。
【図１０】ネットワーク複合機ＭＦＰのシステム制御部１がユーザ操作待機状態で実行する処理のさらに他の例を示したフローチャート。
【図１１】認証システムに発生した障害が回復した際に、変更した参照認証種別優先順位テーブルの内容を復帰する場合の処理の一例を示したフローチャート。
【図１２】認証別登録情報テーブルの一例を示した概略図。
【図１３】登録画面の一例を示した概略図。
【図１４】登録画面の他の例を示した概略図。
【図１５】通常操作画面からユーザ操作が入力された場合の処理の一例を示したフローチャート。
【符号の説明】
【０１２８】
ＭＦＰ　ネットワーク複合機
ＳＣ　ネットワークスキャナ装置
ＳＭ　サーバ装置
ＭＦＰｄ，ＳＣｄ，ＳＭｄ　ＳＡＭデータベース
ＬＡＮ　ローカルエリアネットワーク

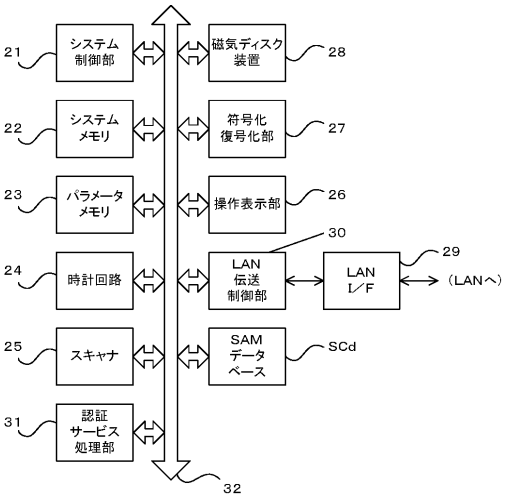
【図１】



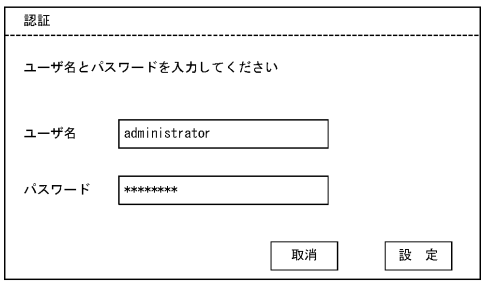
【図２】



【図３】

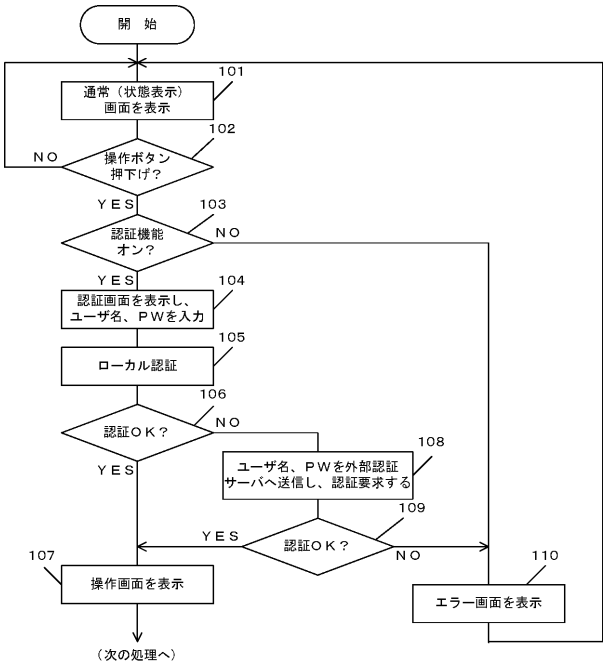


【図４】



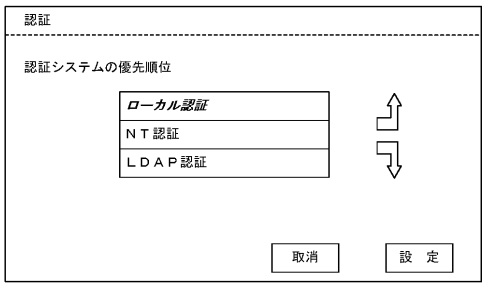
（認証画面）

【図５】



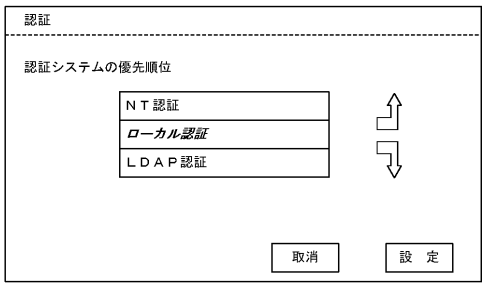
【図６】

(a)



（優先順位選択画面）

(b)



（優先順位選択画面）

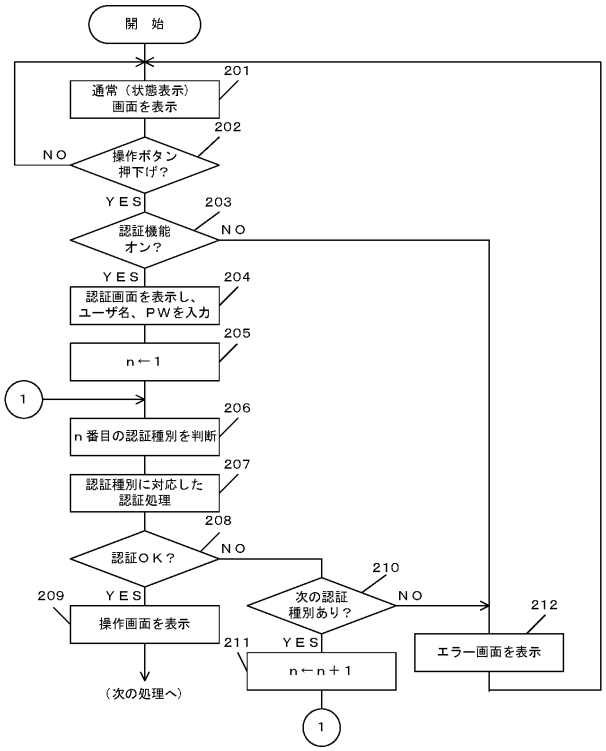
【図７】

（優先順位）

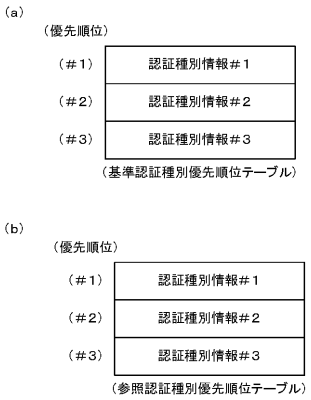
（＃１）	認証種別情報＃１
（＃２）	認証種別情報＃２
（＃３）	認証種別情報＃３

（認証種別優先順位テーブル）

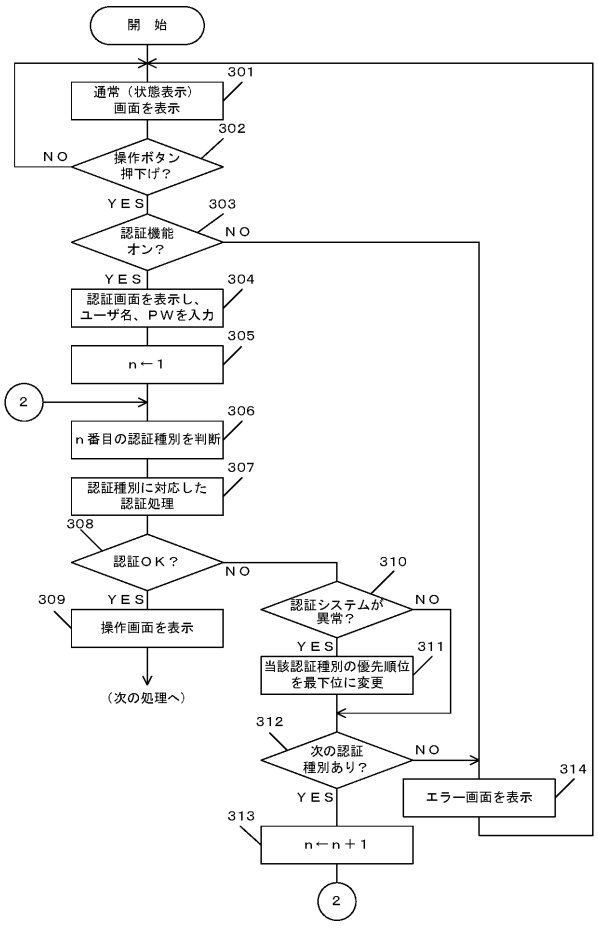
【図８】


開　始
通常（状態表示）画面を表示
201
操作ボタン押下げ？
202
NO
YES
認証機能オン？
203
NO
YES
認証画面を表示し、ユーザ名、ＰＷを入力
204
ｎ←１
205
1
ｎ番目の認証種別を判断
206
認証種別に対応した認証処理
207
認証ＯＫ？
208
NO
YES
209
操作画面を表示
（次の処理へ）
次の認証種別あり？
210
NO
YES
211
ｎ←ｎ＋１
1
エラー画面を表示
212

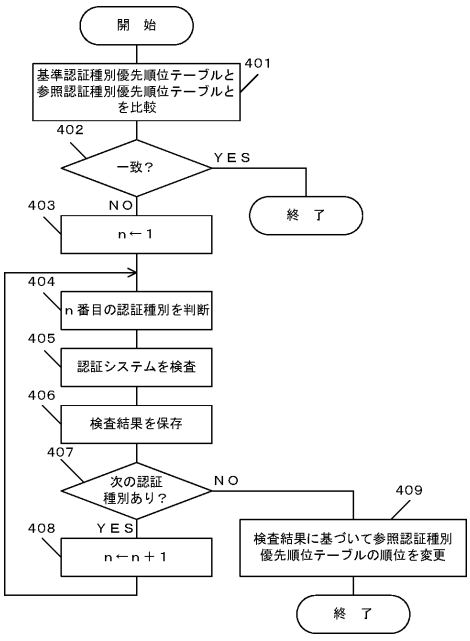
【図９】


(a)
（優先順位）
（＃１）
認証種別情報＃１
（＃２）
認証種別情報＃２
（＃３）
認証種別情報＃３
（基準認証種別優先順位テーブル）
(b)
（優先順位）
（＃１）
認証種別情報＃１
（＃２）
認証種別情報＃２
（＃３）
認証種別情報＃３
（参照認証種別優先順位テーブル）

【図１０】


開　始
通常（状態表示）画面を表示
301
操作ボタン押下げ？
302
NO
YES
認証機能オン？
303
NO
YES
認証画面を表示し、ユーザ名、ＰＷを入力
304
ｎ←１
305
2
ｎ番目の認証種別を判断
306
認証種別に対応した認証処理
307
認証ＯＫ？
308
NO
YES
309
操作画面を表示
（次の処理へ）
認証システムが異常？
310
NO
YES
当該認証種別の優先順位を最下位に変更
311
次の認証種別あり？
312
NO
YES
313
ｎ←ｎ＋１
2
エラー画面を表示
314

【図１１】


開　始
基準認証種別優先順位テーブルと参照認証種別優先順位テーブルとを比較
401
一致？
402
YES
終　了
NO
ｎ←１
403
ｎ番目の認証種別を判断
404
認証システムを検査
405
検査結果を保存
406
次の認証種別あり？
407
NO
YES
ｎ←ｎ＋１
408
検査結果に基づいて参照認証種別優先順位テーブルの順位を変更
409
終　了

【図１２】

(a)

認証種別（ローカル／リモート）	
初期設定権限情報	
コピー利用権限情報	コピー利用登録情報
スキャナ利用権限情報	スキャナ利用登録情報
ファクス送信利用権限情報	ファクス送信利用登録情報
プリンタ利用権限情報	プリンタ利用登録情報

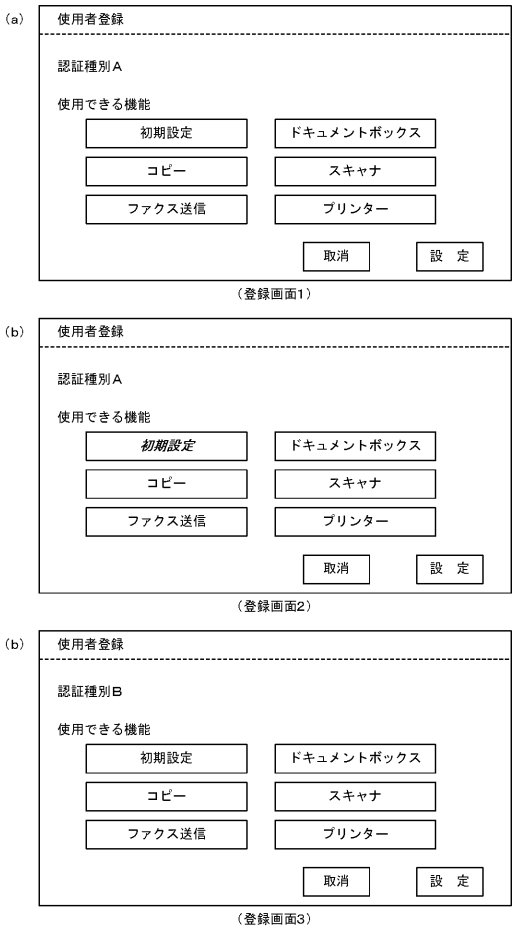
（認証別登録情報テーブル）

(b)

認証種別（ローカル／リモート）	
初期設定権限情報	
コピー利用権限情報	コピー利用登録情報
スキャナ利用権限情報	スキャナ利用登録情報
ファクス送信利用権限情報	ファクス送信利用登録情報
プリンタ利用権限情報	プリンタ利用登録情報
利用可能時間帯情報	

（認証別登録情報テーブル）

【図１３】

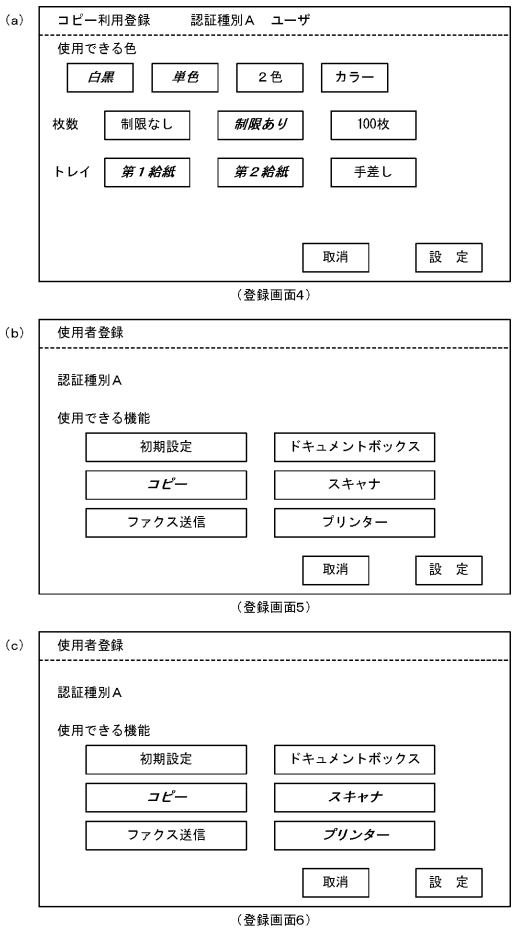


（登録画面1）

（登録画面2）

（登録画面3）

【図１４】

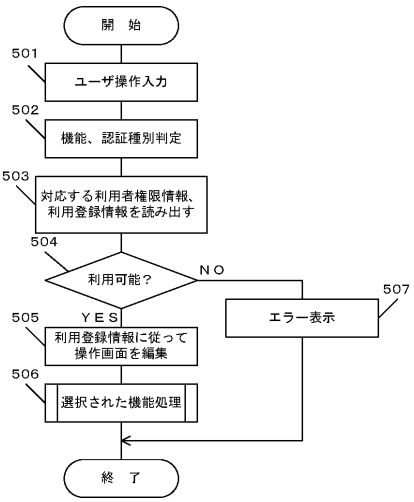


（登録画面4）

（登録画面5）

（登録画面6）

【図１５】



フロントページの続き

(56)参考文献 特開２００２－３５９７１８（ＪＰ，Ａ）
特開平０３－１３５２４１（ＪＰ，Ａ）
特開２００２－１８３０９３（ＪＰ，Ａ）
特開２００２－１５２４５８（ＪＰ，Ａ）
特開２００４－２７２４８６（ＪＰ，Ａ）
特開平０７－２９５９０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２０
Ｇ０６Ｆ　３／１２
Ｈ０４Ｎ　１／００