

(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2006-85641

(P2006-85641A)

(43) 公開日 平成18年3月30日(2006.3.30)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/20 (2006.01)	G06F 15/00 330D	2C061
B41J 5/30 (2006.01)	B41J 5/30 Z	2C187
B41J 29/38 (2006.01)	B41J 29/38 Z	2H027
G03G 21/00 (2006.01)	G03G 21/00 396	5B021
G06F 3/12 (2006.01)	G06F 3/12 K	5B085

審査請求 未請求 請求項の数 9 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願2004-272465 (P2004-272465)
 (22) 出願日 平成16年9月17日 (2004.9.17)

(71) 出願人 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
 (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
 Fターム(参考) 2C061 AP01 AP03 AP04 AP07 HJ06
 HQ17
 2C187 AD03 AD04 AD14 AE07 AE13
 AF03 BF26 CC04 CC08 FA01
 FA04 GD02

最終頁に続く

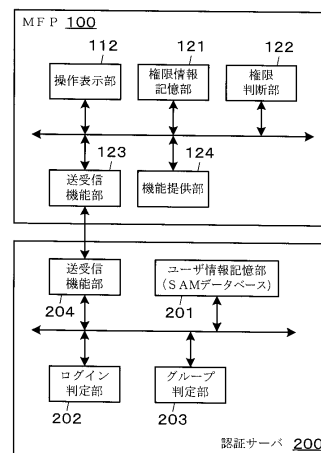
(54) 【発明の名称】 ネットワークシステム、利用権限判定方法、ネットワーク機器、プログラム及び記録媒体

(57) 【要約】

【課題】 ネットワーク機器と認証装置を備えるネットワークシステムにおいて、多数のネットワーク機器を使用する場合でも容易に各ユーザの利用権限を設定できるようにする。

【解決手段】 認証サーバ200に、ユーザの識別情報及び、そのユーザが属するグループの情報を記憶するユーザ情報記憶部201と、MFP100からユーザの識別情報を受信した場合に、その識別情報に係るユーザが属するグループを示す情報をMFP100に送信するグループ判定部203とを設け、MFP100に、自身の機能の利用権限を示す情報をグループ毎に記憶する権限情報記憶部121と、自身を使用しようとしたユーザの識別情報を認証サーバ200に送信し、認証サーバ200からそのユーザが属するグループの情報を受信し、その情報に基づいて自身を使用しようとしたユーザの利用権限有無を判断する権限判断部122とを設けた。

【選択図】 図3



【特許請求の範囲】**【請求項 1】**

ネットワーク機器と認証装置とを備えるネットワークシステムであって、
前記認証装置に、
前記ネットワーク機器を使用するユーザの識別情報及び、該ユーザが属するグループを示すグループ情報を記憶する記憶手段と、
前記ネットワーク機器からユーザの識別情報を受信した場合に、該識別情報に係るユーザが属するグループを示すグループ情報を前記ネットワーク機器に送信する送信手段とを設け、
前記ネットワーク機器に、
自身の機能の利用権限を示す利用権限情報を前記グループ毎に記憶する記憶手段と、
自身を使用しようとしたユーザの識別情報を前記認証装置に送信する送信手段と、
前記認証装置から受信したグループ情報に基づいて、自身を使用しようとしたユーザの利用権限有無を判断する判断手段とを設けたことを特徴とするネットワークシステム。

10

【請求項 2】

請求項 1 記載のネットワークシステムであって、
前記ネットワーク機器の判断手段が、前記認証装置からあるユーザが複数のグループに属することを示すグループ情報を受信した場合に、その複数のグループ中の少なくとも 1 つのグループについて利用権限のある機能については、そのユーザに利用権限を認めるようにしたことを特徴とするネットワークシステム。

20

【請求項 3】

請求項 1 記載のネットワークシステムであって、
前記ネットワーク機器の判断手段が、前記認証装置からあるユーザが複数のグループに属することを示すグループ情報を受信した場合に、その複数のグループ全てについて利用権限のある機能についてのみ、そのユーザに利用権限を認めるようにしたことを特徴とするネットワークシステム。

【請求項 4】

請求項 1 記載のネットワークシステムであって、
前記ネットワーク機器の記憶手段に、デフォルトグループに関する利用権限情報を記憶させておき、
前記ネットワーク機器の判断手段が、前記認証装置からあるユーザが属するグループがないことを示すグループ情報を受信した場合でも、そのユーザに前記デフォルトグループに係る利用権限を認めるようにしたことを特徴とするネットワークシステム。

30

【請求項 5】

請求項 1 乃至 4 のいずれか一項記載のネットワークシステムであって、
前記認証装置において、
前記記憶手段が前記各グループについて ID を記憶すると共に、
前記送信手段が前記グループ情報としてグループの ID を送信するようにし、
前記ネットワーク機器において、
前記記憶手段が前記利用権限情報を前記グループの ID 毎に記憶すると共に、
前記判断手段が前記認証装置から受信したグループの ID に基づいてユーザの利用権限有無を判断するようにしたことを特徴とするネットワークシステム。

40

【請求項 6】

ネットワーク機器における利用権限判定方法であって、
前記ネットワーク機器とネットワークを介して通信可能な前記認証装置に、
前記ネットワーク機器を使用するユーザの識別情報及び、該ユーザが属するグループを示すグループ情報を記憶させておき、
前記ネットワーク機器からユーザの識別情報を受信した場合に、該識別情報に係るユーザが属するグループを示すグループ情報を前記ネットワーク機器に送信させ、
前記ネットワーク機器に、

50

自身の機能の利用権限を示す利用権限情報を前記グループ毎に記憶させておき、自身を使用しようとしたユーザの識別情報を前記認証装置に送信させ、前記認証装置から受信したグループ情報に基づいて、自身を使用しようとしたユーザの利用権限有無を判定させるようにしたことを特徴とする利用権限判定方法。

【請求項 7】

自身の機能の利用権限を示す利用権限情報をユーザが属するグループ毎に記憶する記憶手段と、

自身を使用しようとしたユーザの識別情報を、ネットワークを介して通信可能な認証装置に送信する送信手段と、

該手段による送信に応じて前記認証装置から受信した、自身を使用しようとしたユーザが属するグループを示すグループ情報に基づいて、そのユーザの利用権限有無を判断する判断手段とを設けたことを特徴とするネットワーク機器。

10

【請求項 8】

コンピュータにネットワーク機器を制御させるためのプログラムであって、

前記コンピュータを、

前記ネットワーク機器の機能の利用権限を示す利用権限情報をユーザが属するグループ毎に記憶する記憶手段と、

前記ネットワーク機器を使用しようとしたユーザの識別情報を、ネットワークを介して通信可能な認証装置に送信する送信手段と、

該手段による送信に応じて前記認証装置から受信した、前記ネットワーク機器を使用しようとしたユーザが属するグループを示すグループ情報に基づいて、そのユーザの利用権限有無を判断する判断手段として機能させるためのプログラムを含むことを特徴とするプログラム。

20

【請求項 9】

請求項 8 記載のプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、ユーザに権限に応じた機能の利用を許可するネットワーク機器と、そのネットワーク機器と通信可能な認証装置とを備えたネットワークシステム、上記のようなネットワーク機器における利用権限判定方法、上記のようなネットワーク機器、コンピュータに上記のようなネットワーク機器を制御させるためのプログラム、およびこのようなプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

30

【背景技術】

【0002】

従来から、デジタル複合機（MFP）のようなネットワーク機器において、ユーザやグループごとに利用できる機能を制限できるようにすることが行われている。そして、このような装置においては、ユーザに操作パネルからユーザコードを入力させたり、IDカードを使用させたりして個人を識別し、各ユーザに、許可された権限の範囲内でのみ装置を使用させるようにすることが可能である。

40

このような装置によれば、ユーザごとにコピーの色の制限やファクス送信、印刷、スキャナなどの利用制限をかけたり、部門ごとに使用量を集計してその上限を設定し過度の使用を防ぐといったことが可能である。

このような装置については、例えば特許文献 1 乃至 3 に記載されている。

【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】特開平 10 - 58796 号公報

【0003】

なお、これらの上記の特許文献 1 乃至 3 に記載の装置は、ユーザの識別（認証）を機器自身が行うものであるが、ユーザ情報や各ユーザが有する各機器の利用権限の情報を一元

50

管理するディレクトリサーバを設け、複数のネットワーク機器がこのディレクトリサーバにおける認証機能を利用してユーザの利用権限有無を判定できるようにするシステムも提案されている。

このような技術については、特許文献4に記載されている。

【特許文献4】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】

【0004】

しかしながら、上記の特許文献1乃至3に記載のような、ユーザに機能を提供するネットワーク機器自身が認証処理を行う構成では、ユーザ環境において複数のネットワーク機器を使用する場合、新規にユーザを追加したりユーザを削除したりする場合に、機器毎に個別にユーザIDやパスワード等を登録や削除する必要があり、設定が煩わしいという問題があった。

10

【0005】

一方、特許文献4に記載のように、ユーザ情報や利用権限の情報を一元管理するサーバを設け、各機器における権限や、ネットワークへのログインに使用する情報等を一括して管理するようにすれば、このような問題は解決には有効である。しかし、このようなサーバを利用可能とするためには、サーバに各ユーザについて各ネットワーク機器についてのアクセス制限の情報を記載したデータベースを作成する必要があった。そして、このようなデータベースの作成には深いネットワーク知識が必要である上、煩雑な作業が必要であるという問題があった。

20

この発明は、このような問題を解決し、多数のネットワーク機器を使用する場合でも、容易に各ユーザの利用権限を設定できるようにすることを目的とする。

【課題を解決するための手段】

【0006】

この発明は、上記の目的を達成するため、ネットワーク機器と認証装置とを備えるネットワークシステムにおいて、上記認証装置に、上記ネットワーク機器を使用するユーザの識別情報及び、そのユーザが属するグループを示すグループ情報を記憶する記憶手段と、上記ネットワーク機器からユーザの識別情報を受信した場合に、その識別情報に係るユーザが属するグループを示すグループ情報を上記ネットワーク機器に送信する送信手段とを設け、上記ネットワーク機器に、自身の機能の利用権限を示す利用権限情報を上記グループ毎に記憶する記憶手段と、自身を使用しようとしたユーザの識別情報を上記認証装置に送信する送信手段と、上記認証装置から受信したグループ情報に基づいて、自身を使用しようとしたユーザの利用権限有無を判断する判断手段とを設けたものである。

30

【0007】

このようなネットワークシステムにおいて、上記ネットワーク機器の判断手段が、上記認証装置からあるユーザが複数のグループに属することを示すグループ情報を受信した場合に、その複数のグループ中の少なくとも1つのグループについて利用権限のある機能については、そのユーザに利用権限を認めるようにするとよい。

あるいは、上記ネットワーク機器の判断手段が、上記認証装置からあるユーザが複数のグループに属することを示すグループ情報を受信した場合に、その複数のグループ全てについて利用権限のある機能についてのみ、そのユーザに利用権限を認めるようにしてもよい。

40

【0008】

あるいは、上記ネットワーク機器の記憶手段に、デフォルトグループに関する利用権限情報を記憶させておき、上記ネットワーク機器の判断手段が、上記認証装置からあるユーザが属するグループがないことを示すグループ情報を受信した場合でも、そのユーザに上記デフォルトグループに係る利用権限を認めるようにしてもよい。

また、上記の各ネットワークシステムについて、上記認証装置において、上記記憶手段に上記各グループについてIDを記憶させると共に、上記送信手段が上記グループ情報と

50

してグループのIDを送信するようにし、上記ネットワーク機器において、上記記憶手段が上記利用権限情報を上記グループのID毎に記憶すると共に、上記判断手段が上記認証装置から受信したグループのIDに基づいてユーザの利用権限有無を判断するようにするとよい。

【0009】

また、この発明のネットワーク機器における利用権限判定方法は、ネットワーク機器における利用権限判定方法において、上記ネットワーク機器とネットワークを介して通信可能な認証装置に、上記ネットワーク機器を使用するユーザの識別情報及び、そのユーザが属するグループを示すグループ情報を記憶させておき、上記ネットワーク機器からユーザの識別情報を受信した場合に、その識別情報に係るユーザが属するグループを示すグループ情報を上記ネットワーク機器に送信させ、上記ネットワーク機器に、自身の機能の利用権限を示す利用権限情報を上記グループ毎に記憶させておき、自身を使用しようとしたユーザの識別情報を上記認証装置に送信させ、上記認証装置から受信したグループ情報に基づいて、自身を使用しようとしたユーザの利用権限有無を判定させるようにしたものである。

10

【0010】

また、この発明のネットワーク機器は、自身の機能の利用権限を示す利用権限情報をユーザが属するグループ毎に記憶する記憶手段と、自身を使用しようとしたユーザの識別情報を、ネットワークを介して通信可能な認証装置に送信する送信手段と、その手段による送信に応じて上記認証装置から受信した、自身を使用しようとしたユーザが属するグループを示すグループ情報に基づいて、そのユーザの利用権限有無を判断する判断手段とを設けたネットワーク機器である。

20

【0011】

また、この発明のプログラムは、コンピュータにネットワーク機器を制御させるためのプログラムであって、上記コンピュータを、上記ネットワーク機器の機能の利用権限を示す利用権限情報をユーザが属するグループ毎に記憶する記憶手段と、上記ネットワーク機器を使用しようとしたユーザの識別情報を、ネットワークを介して通信可能な認証装置に送信する送信手段と、その手段による送信に応じて上記認証装置から受信した、上記ネットワーク機器を使用しようとしたユーザが属するグループを示すグループ情報に基づいて、そのユーザの利用権限有無を判断する判断手段として機能させるためのプログラムを含むものである。

30

また、この発明の記録媒体は、上記のプログラムを記録したコンピュータ読取可能な記録媒体である。

【発明の効果】

【0012】

以上のようなこの発明のネットワークシステム、利用権限判定方法又はネットワーク機器によれば、多数のネットワーク機器を使用する場合でも、容易に各ユーザの利用権限を設定することができる。

また、この発明のプログラムによれば、コンピュータを上記のネットワーク機器として機能させてその特徴を実現し、同様な効果を得ることができる。

40

この発明の記録媒体によれば、上記のプログラムを記憶していないコンピュータにそのプログラムを読み出させて実行させ、上記の効果を得ることができる。

【発明を実施するための最良の形態】

【0013】

以下、この発明を実施するための最良の形態について、図面を参照して説明する。

〔実施形態：図1乃至図8〕

まず、この発明のネットワーク機器の実施形態であるデジタル複合機(MFP)及び、そのデジタル複合機を備えたネットワークシステムについて説明する。

まず図1に、上記のMFPの構成を示す。

この図に示すとおり、MFP100は、CPU101、ROM102、RAM103、

50

画像蓄積メモリ104, 記憶装置105, LAN(ローカル・エリア・ネットワーク)コントローラ106, FAX(ファクシミリ)通信部107, スキャナ部108, プロッタ部109, パネルI/F(インタフェース)110を備え、これらがシステムバス111によって接続されている。また、パネルI/F110には操作表示部112が接続されている。

【0014】

そして、CPU101は、MFP100全体を統括制御する制御手段であり、ROM102や記憶装置105に記憶している種々の制御プログラムを実行することにより、後述するように、送信手段や判断手段等の各手段として機能し、この実施形態の特徴に係る種々の機能を実現する。

ROM102は、不揮発性の記憶手段であり、CPU101が実行する制御プログラムや、固定的なパラメータ等を記憶する。ROM102を書き換え可能な記憶手段として構成し、これらのデータをアップデートできるようにしてもよい。

RAM103は、一時的に使用するデータを記憶したり、CPU101のワークメモリとして使用したりする揮発性の記憶手段である。このRAM103は、電源が遮断されても記憶内容を保持できるようにバッテリーによってバックアップしておくともよい。

【0015】

画像蓄積メモリ104は、RAM等によって構成され、FAX通信部107で受信した画像や、スキャナ部108で読み取った画像のデータを記憶する記憶手段である。

記憶装置105は、NVRAM(不揮発RAM)やHDD(ハードディスクドライブ)等によって構成される書き換え可能な不揮発性記憶手段であり、CPU101に実行させる制御プログラムや、装置の電源がOFFされた後も保持しておく必要があるデータあるいはパラメータの値などを記憶する。後述する権限情報も、この記憶装置105に記憶させておくようにするとよい。

【0016】

LANコントローラ106は、MFP100をネットワークに接続するためのインタフェース及び通信制御に必要な回路等を含むユニットであり、例えばイーサネット(登録商標)方式の通信を行うためのインタフェースである。そして、ネットワークを介して他の装置と通信を行う場合、このLANコントローラ106とCPU101とが通信手段として機能する。なお、ネットワークは、イーサネット、無線LAN、IEEE(Institute of Electrical and Electronic Engineers)1394等、有線、無線を問わず種々の方式のものが使用可能である。

FAX通信部107は、画像の符号化や復号化を行う符号化復号化部、公衆通信網を介した通信を制御する網制御部等によって構成され、外部装置との間でファクシミリ通信により画情報の送受信を行う通信手段である。

【0017】

スキャナ部108は、原稿の画像を画像データとして読み取る画像読取手段である。

プロッタ部109は、画像データに基づいて用紙に画像を形成する画像形成手段である。

操作部I/F110は、表示操作部112をシステムバス111と接続するためのインタフェースである。そして、表示操作部112は、液晶ディスプレイにタッチパネルを積層した操作パネルや、各種キー等を備え、画面にメッセージやGUIを表示したり、ユーザからによる動作指示や情報入力等の操作を受け付ける機能を有する。

このMFP100は、以上のような構成を有し、CPU101が所要の制御プログラムを実行して各部を制御することにより、プリント、スキャン、コピー、ファクシミリ通信等の種々の機能を実現することができる画像処理装置である。

【0018】

次に、図2にこのMFPを備えるネットワークシステムの構成例を示す。

図2に示すネットワークシステムは、この発明のネットワークシステムの実施形態であり、図1に示したMFP100と、認証装置である認証サーバ200とをLAN400に

10

20

30

40

50

よって接続して構成している。また、LAN 400には、それぞれネットワーク通信手段を備えたネットワーク機器である複写機301，プリンタ302，FAX装置303，スキャナ304，PC（パーソナルコンピュータ）305も接続している。

【0019】

ここで、認証サーバ200は、ハードウェアとしては、CPU，ROM，RAM，HDD，ネットワークI/F等を備えた公知のコンピュータでよい。しかし、ROMやHDDに記憶させた所要の制御プログラムをCPUに実行させることにより、SAM（セキュリティ・アカウント・マネージャ）データベースを用いてLAN 400内で使用するユーザアカウント情報を管理するサーバ装置として機能させるようにしている。そして、SAMデータベースにおいては、ユーザアカウントとそのユーザが属するグループとを対応させて管理しており、ユーザ名とパスワードのようなユーザの識別情報によってユーザを認証し、そのユーザが属するグループを特定する機能を有する。

10

【0020】

また、認証サーバ200は、LAN 400上の各ネットワーク機器からの要求に応じてユーザを認証すると共に、そのユーザが属するグループ名をその要求元に通知する機能も有する。従って、MFP 100やPC 305を始めとする各ネットワーク機器は、自身でユーザ個々のユーザ名やパスワードを管理しなくても、認証サーバ200が管理しているユーザアカウントを利用してユーザを認証し、そのユーザの属するグループの情報を取得することができる。従って、認証サーバ200におけるユーザアカウントを変更するだけで、そのユーザアカウントを利用している全てのネットワーク機器についてユーザアカウントを変更した場合と同等な効果を得ることができる。

20

【0021】

次に、図3に、上記のようなMFP 100及び認証サーバ200の機能構成のうち、この実施形態の特徴に関連する部分を示す。なお、この図においては、この実施形態の特徴とあまり関係ない部分については図示を省略している。また、図中の各部を結ぶ矢印は、それらの各部の間で情報の授受があることを示すものであり、物理的な構成を意味するものではない。

【0022】

図3に示すように、認証サーバ200には、この実施形態の特徴に関連する機能部として、ユーザ情報記憶部201，ログイン判定部202，グループ判定部203，送受信機能部204を備えている。

30

そして、ユーザ情報記憶部201は、上述したようなSAMデータベースとして、ユーザの識別情報及び、そのユーザが属するグループを示すグループ情報を記憶する機能を有する。このユーザ情報記憶部201は、ハードウェアとしては、内部のHDD等の記憶手段に設けてもよいし、外部の記憶手段に設けてもよい。

【0023】

ログイン判定部202は、LAN 400を介して外部のネットワーク機器からユーザの認証を要求された場合に、そのネットワーク機器から認証に使用する識別情報（ここではユーザ名とパスワード）を取得し、これをユーザ情報記憶部201に記憶している情報と比較することによりユーザを認証する認証手段の機能を有する。そして、そのユーザが認証サーバ200にアクセスする権限を有すると判断した場合、認証サーバ200へのログインを許可する機能も有する。

40

【0024】

また、グループ判定部203は、ログイン判定部202における認証が成功したユーザについて、そのユーザが属するグループの情報の取得を要求された場合、ユーザ情報記憶部201からそのユーザが属するグループの情報を取得し、要求元に通知する機能を有する。なお、この場合において、情報を通知する前に、情報を要求してきた相手にこれを取得する権限があることを確認するようすとよい。

送受信機能部204は、外部のネットワーク機器との間で情報を送受信する機能を有する通信手段であり、上述した各部が行う要求の取得や通知の送信は、この送受信機能部2

50

04を介して行う。

【0025】

一方、MFP100には、この実施形態の特徴に関連する機能部として、操作表示部112、権限情報記憶部121、権限判断部122、送受信機能部123、機能提供部124を備えている。

操作表示部112については上述した通りであるが、MFP100の機能を使用する指示や、ユーザ名及びパスワードの入力等、種々の操作を受け付けたり、その受付を行うための画面を表示したりする機能を有する。

【0026】

権限情報記憶部121は、自身の機能のうちユーザに利用権限を与える機能の種類を示す利用権限情報を記憶する記憶手段である。そして、この利用権限情報は、認証サーバ200がSAMデータベースにおいてユーザのグループ分けに用いているグループの種類毎に、そのグループに属するユーザに与える利用権限を示す情報として記憶するようにしている。なお、この権限情報記憶部121に記憶させる利用権限情報は、操作表示部112から入力できるようにしたり、認証サーバ200等の外部装置からテンプレートをダウンロードして編集できるようにしたり、同じく外部装置からグループ名一覧のみダウンロードして各グループについて利用権限を設定できるようにしたりと、種々の方法で設定できるようにすることが考えられる。

10

【0027】

また、権限判断部122は、ユーザがMFP100の機能を利用しようとした場合に、そのユーザが有する利用権限の範囲を判断する判断手段の機能を有する。そしてここでは、この判断は、ユーザがMFP100の機能を利用しようとした場合に、表示操作部112を利用してユーザ名及びパスワードの入力を受け付け、これをMFP200に送信してそのユーザを認証させると共にそのユーザが属するグループの情報を取得し、この情報をもとに、権限情報記憶部121に記憶しているグループ毎の利用権限情報を参照して行うようにしている。

20

これらの権限情報記憶部121及び権限判断部122の機能がこの実施形態の主要な特徴である。

【0028】

また、送受信機能部123は、認証サーバ200等の外部装置との間で情報を送受信する機能を有する通信手段であり、権限判断部122は、この送受信機能部123を介してログイン要求の送信やグループ情報の受信等を行う。

30

機能提供部124は、スキャナ部108、プロッタ部109等を制御することにより、権限判断部122がユーザに利用を許可できると判断した範囲でコピー、プリント、スキャン等の種々の機能を提供する機能を有する。

【0029】

ここで、図4に、MFP100において表示操作部112から利用権限情報の入力を受け付けて権限情報記憶部121に記憶させる場合に使用する画面及びその操作手順の例を示す。

MFP100は、権限情報設定の権限を有するユーザに権限情報の設定を要求されると、図4(a)に示すような権限設定画面20を操作表示部112に表示させ、権限情報の設定を受け付けるようにしている。この受け付けも、機能提供部124が提供する機能の1つである

40

【0030】

そして、権限設定画面20においては、グループ名入力欄21において、利用権限情報を設定しようとするグループのグループ名の入力を受け付けるようにしている。また、変更キー22が押下された場合には、認証サーバ200にアクセスして認証サーバ200がユーザの管理に使用しているグループの情報を取得して一覧表示し、ユーザがその中から利用権限情報を設定するグループを選択してグループ名入力欄21に入力できるようにしている。

50

【0031】

そして、機能選択部23には、MFP100が備える機能と対応するキーを設け、ユーザがグループ名入力欄21で指定したグループにユーザに利用権限を与えたい機能のキーを押下すると、その機能に関する権限をより詳細に設定するための、(b)に示すような画面に移行するようにしている。なお、「初期設定」は、権限設定画面20で行うような権限の設定や、ネットワーク通信の設定等、MFP100の基本的な設定を行う機能を示すものである。

【0032】

また、設定キー25が押下された場合には、権限設定画面20で指定された内容を権限情報記憶部121に記憶させて設定し、取消キー24が押下された場合には権限設定画面20で指定された内容を記憶せずに権限情報の設定を終了するようにしている。

従って、ユーザは、グループ名入力欄21にグループ名を入力し、機能選択部23の各キーを押下してそのグループのユーザに利用を許可する権限の種類を選択し、設定キー25を押下することにより、入力したグループに関する利用権限情報を権限情報記憶部121に記憶させて設定することができる。

【0033】

一方、(b)には、コピー機能が選択された場合に表示させるコピー権限設定画面30を示している。

そして、このコピー権限設定画面30においては、色指定部32の各キーにより、コピー時に使用を許可する色を指定することができる。図には、「白黒」「単色カラー」「2色カラー」「フルカラー」の各機能に対応させて許可/不許可を独立してトグルで選択可能なキーを用意し、このうち前2者を許可するようにした例を示している。

【0034】

また、枚数指定部33においては、コピー枚数の「制限なし」と「制限あり」の一方を指定可能であり、「制限あり」を指定した場合には、その右側の入力欄に使用を許可する枚数を入力できるようにしている。図には、コピー枚数を100枚に制限した例を示している。

また、トレイ指定部34では、各キーにより、コピー時に使用できる給紙トレイを指定できるようにしている。図には、「第1給紙トレイ」、「第2給紙トレイ」、「手差しトレイ」の各トレイに対応させて許可/不許可を独立してトグルで選択可能なキーを用意し、このうち前2者の使用を許可するようにした例を示している。

【0035】

そして、ユーザが設定キー36を押下すると、コピーについて使用を許可する機能の情報を一時的に記憶し、もとの権限設定画面20に戻る。このとき、コピーについて機能の指定がなされていることを示すため、コピー機能を選択するキーは網掛けして表示している。

そして、この後設定キー25を押下することにより、それまでに指定した内容を権限情報記憶部121に記憶させて設定することができる。また、機能選択部23において再度機能を選択すれば、その機能に関する権限の設定を追加や削除することもできる。

【0036】

また、コピー権限設定画面30において取消キー35が押下された場合には、コピー権限設定画面30で指定した内容を記憶せずにもとの権限設定画面20に戻る。この場合には、コピー機能に関する指定はなされていないので、(a)の状態に戻ることになる。

MFP100においては、権限情報設定の権限を有するユーザは、以上のような手順により、各グループについて利用権限情報を設定することができる。そしてここでは、この設定は、MFP100内のみで有効とし、他のネットワーク機器とは無関係に設定できるようにしている。

【0037】

なお、図4(a)に示した権限設定画面20や、機能選択部23での選択に従って表示する各画面において、どのような項目について許可/不許可の指定を受け付けるかについ

10

20

30

40

50

ては、機能提供部 124 が、MFP10 がどのような機能をユーザに提供可能かを把握し、その内容に基づいて定めるようにしてもよい。また、コピー権限設定画面 30 のような詳細な設定を行うための画面を設けず、コピー、プリンタ等のおおまかな括りで権限を設定できるようにしてもよい。

【0038】

次に、ユーザが MFP100 を使用しようとした場合に MFP100 が実行する処理及び、この処理に関連して認証サーバ 200 が実行する処理について説明する。

まず、図 5 及び図 6 に MFP100 側の処理を示す。

MFP100 の CPU101 は、ユーザが操作表示部 112 等の操作により MFP100 の利用を要求したことを検知した場合に、所要の制御プログラムを実行することにより図 5 のフローチャートに示す処理を開始する。 10

【0039】

そして、まずステップ S101 で、利用権限情報を用いて MFP100 の利用を制限する利用制限機能が有効となっているか否か判断する。そして、有効であれば、ステップ S102 に進み、認証サーバ 200 を用いてユーザを認証するネットワーク認証機能が有効となっているか否か判断する。そして、こちらも有効であれば、ステップ S103 以降の、認証サーバ 200 を利用した認証及び権限管理処理に進む。

そして、ステップ S103 では、操作表示部 112 にログイン画面を表示させ、ユーザ名とパスワードの入力を要求する。

【0040】

20

図 7 に、このログイン画面の表示例を示す。

このログイン画面 40 においては、ユーザ名入力部 41 においてユーザ名、パスワード入力部 42 においてパスワードの入力をそれぞれ受け付けるようにしており、ユーザがこれらを入力して設定キー 43 を押下すると、入力されたパスワードを確定して図 5 の処理をステップ S104 以降に進める。ユーザが取消キー 44 を押下した場合には、図示は省略したが、MFP100 の使用は許可できないので図 5 の処理をステップ S116 に進める。

図 5 の説明に戻ると、ステップ S103 の後、次のステップ S104 では、ステップ S103 で入力されたユーザ名とパスワードを認証サーバ 200 に送信してログインを要求する。そして、ステップ S105 でログインの成否を判断する。ここで成功していれば、図 6 のステップ S106 に進んで、認証サーバ 200 に認証されたユーザが属するグループの情報を要求し、これを取得する。 30

【0041】

そして、ステップ S107 で、ステップ S106 で取得したグループが、MFP100 に利用権限情報が登録されているいずれかのグループと一致するか否か判断する。この判断は、権限情報記憶部 121 に記憶している情報を基に行うことができる。そして、ここで一致するものがなければ、利用を要求してきたユーザには MFP100 の利用を許可できないため、図 5 のステップ S115 に進んで認証サーバ 200 からログアウトし、ステップ S116 でエラー画面を表示して処理を終了する。もちろん、処理の終了後に再度 MFP100 の利用の要求を受け付けることは可能である。 40

【0042】

一方、ステップ S107 で一致するものがあれば、ステップ S108 で、該当するグループについて設定されている利用権限情報により、MFP100 の利用を要求したユーザに利用を許可できる機能を把握する。この場合において、ユーザが複数のグループに属しており、そのそれぞれについて利用権限情報があるような場合の処理については、いくつかの方法が考えられるが、これについては後の変形例において述べる。ここでは一例としていずれか 1 つのグループをユーザに選択させるものとする。

【0043】

そして、次のステップ S109 では、ユーザに利用を許可できる機能についての操作を受け付けるための画面を、操作表示部 112 に表示させる。この画面においては、利用を 50

許可できる機能に係るキーのみを表示させたり、利用を許可できる機能に係るキー以外のキーを薄く表示させて操作できないことを示したりすることが考えられる。

そして、ステップS 1 1 0でその画面における操作に従ってユーザに機能を提供し、これが終了するとステップS 1 1 1で認証サーバ2 0 0からログアウトして処理を終了する。

【0 0 4 4】

また、ステップS 1 0 2でNOの場合には、認証サーバ2 0 0を利用せずに認証処理を行うことになる。そこでこの場合、ステップS 1 1 2に進み、ユーザ名とパスワードの入力を受け付け、入力されたユーザ名及びパスワードを用いてM F P 1 0 0自身でローカルの認証処理を行う。この場合の入力受付画面は、図7に示した画面と同様なものでよい。

10

そして、ステップS 1 1 3で認証の成否を判断し、成功であれば、ステップS 1 1 4に進み、ユーザ毎に設定されている利用権限情報に基づいて、利用を要求してきたユーザに利用を許可できる機能を把握する。その後、図6のステップS 1 0 9に進んで以降の処理を行う。

【0 0 4 5】

ステップS 1 1 3で認証失敗であれば、利用を要求してきたユーザにはM F P 1 0 0の利用を許可できないため、ステップS 1 1 6でエラー画面を表示して処理を終了する。

また、ステップS 1 0 1で利用制限機能が無効であった場合には、利用を要求してきたユーザに全ての機能の利用を許可してよいので、ステップS 1 1 7で全ての機能の利用を許可できると判断し、図6のステップS 1 0 9に進んで以降の処理を行う。

20

以上の処理において、ステップS 1 0 4乃至S 1 0 8がこの発明の利用権限判定方法の実施形態に係る処理であり、C P U 1 0 1は、ステップS 1 0 4の処理においては送信手段として、ステップS 1 0 7乃至S 1 0 9の処理においては判断手段として機能する。

【0 0 4 6】

次に、図8に、図5及び図6に示した処理と対応する認証サーバ2 0 0側の処理を示す。なお、この図には、図5及び図6に示した処理と関連する部分の処理のみを示し、それ以外の一般的な処理については図示を省略している。

認証サーバ2 0 0のC P Uは、M F P 1 0 0等の外部装置からログインの要求を受けた場合に、所要の制御プログラムを実行することにより、図8のフローチャートに示す処理を開始する。

30

【0 0 4 7】

そして、まずステップS 2 0 1において、ログインの要求とともに受け取ったユーザ名とパスワードが適切なものであるか否かを判断する。この判断は、ユーザ情報記憶部2 0 1に記憶している情報を基に行うことができる。

そして、適切であると判断した場合には、ログインを許可できると判断し、ステップS 2 0 2に進んでログイン処理を行い、ステップS 2 0 3でログイン要求元にログイン許可を通知する。

【0 0 4 8】

その後、ステップS 2 0 4でグループ情報を要求されたか否かを判断し、要求されていればステップS 2 0 5でログインを許可したユーザが属するグループの情報を送信し、ステップS 2 0 6に進む。このグループの情報も、ユーザ情報記憶部2 0 1から取得することができる。また、ステップS 2 0 4で要求がなければ、そのままステップS 2 0 6に進む。

40

【0 0 4 9】

そして、ステップS 2 0 6でログアウト要求があれば、ステップS 2 0 7に進んでログアウト処理を行い、処理を終了する。ログアウト要求がなければ、ステップS 2 0 4に戻って処理を繰り返す。

一方、ステップS 2 0 1でユーザ名とパスワードが適切でなければ、ステップS 2 0 8に進み、ログイン要求元にログイン拒否を通知して処理を終了する。

以上の処理も、この発明の利用権限判定方法の実施形態に係る処理であり、この処理に

50

おいては、認証サーバ200のCPUが送信手段として機能する。

【0050】

MFP100及び認証サーバ200に、以上説明した各処理を実行させることにより、図3を用いて説明したような、グループの情報を用いた権限管理を行うことができる。そして、このようなネットワークシステムによれば、各ユーザがどのグループに属するかという情報を認証サーバ200において一括して管理し、多数のネットワーク機器からでも共通にこの情報を利用することができる一方、各グループのユーザにどのような権限を与えるかという情報は、機器毎に設定することができる。

【0051】

従って、認証サーバ200の管理者は、個々の機器における詳細な設定について関知する必要がない。また、個々の機器の管理者は、権限を与えたいユーザがどのグループに所属しているかさえ把握していれば、認証サーバ200におけるデータ管理の詳細を把握していなくても、個々の機器における利用権限を設定することができる。そして、この場合において、グループ毎の設定が可能であるので、ユーザが多数いる場合でも設定すべき項目を低減できるから、機器毎に設定を行ったとしても、負担はさほど大きくない。また、設定に際してネットワークに関する高度な知識は不要である。従って、全体として、上述のような権限管理を行うようにしたことにより、多数のネットワーク機器を使用する場合でも、容易に各ユーザの利用権限を設定できるようにすることができると言える。

【0052】

また、このような機能を備えたネットワークシステムによれば、機器を部門間で移動させたことにより使用を許可するグループを変更する必要が生じたり、機器を新たに導入して権限情報を設定する必要が生じたりした場合に、認証サーバ200における権限情報は変更せずに設定を行うことができる。従って、このような事態が頻繁に発生するような環境では、上述のネットワークシステムによる効果が特に大きい。

なお、上述したMFP100において、図5のステップS112乃至S114に示したようなローカル認証の機能を設けることは、必須ではない。

【0053】

〔第1の変形例：図9〕

次に、上述した実施形態の第1の変形例について説明する。この変形例は、ユーザが複数のグループに属する場合の取り扱いが上述の実施形態と異なるのみである。そして、この点に伴い、ユーザがMFP100を使用しようとした場合にMFP100のCPU101が実行する処理において図6に示した部分が上述の実施形態と異なるのみであるので、この相違点についてのみ説明する。

【0054】

図9に、この変形例における図6と対応する処理のフローチャートを示す。

この第1の変形例のMFP100においては、図5のステップS105においてログイン成功であった場合、処理は図9のステップS301に進み、ここで認証サーバにユーザが属するグループのリストを要求し、これを取得する。

【0055】

そして、そのリストに含まれる各グループを順次対象として、ステップS302及びS303の処理を繰り返す。これらの処理は、ステップS302で、対象グループがMFP100に利用権限情報の登録されているいずれかのグループと一致するか否か判断し、いずれかと一致した場合に、ステップS303で、該当するグループについて設定されている利用権限を、認証サーバ200に認証された(MFP100の利用を要求している)ユーザの利用権限に追加するというものである。

【0056】

なお、ステップS302の判断は、権限情報記憶部121に記憶している情報を基に行うことができる。また、ステップS301を行う時点では、認証されたユーザの利用権限は何もないものとする。

従って、ステップS302及びS303のループにより、ユーザが複数のグループに属

10

20

30

40

50

する場合、その複数のグループ中の少なくとも1つのグループについて利用権限のある機能については、そのユーザに利用権限を認めるようにすることになる。

【0057】

そして、その後ステップS304で、認証されたユーザに利用権限があるか否か判断し、あればステップS109以降の処理を行ってユーザに機能を提供する。なければ、図5のステップS115以降の処理に進み、ユーザにMFP100の利用を許可せずに終了する。

ステップS109以降又はステップS115以降の処理については、上述した実施形態の場合と同様であるので、説明は省略する。

以上のような処理を行うことにより、ユーザが複数のグループに属する場合でも、各グループにおける権限の内容を反映した処理が可能となり、より柔軟に利用権限を設定することができる。

【0058】

〔第2の変形例：図10〕

次に、上述した実施形態の第2の変形例について説明する。この変形例も、ユーザが複数のグループに属する場合の取り扱いが上述の実施形態と異なるのみである。そして、この点に伴い、ユーザがMFP100を使用しようとした場合にMFP100のCPU101が実行する処理において図6に示した部分が上述の実施形態と異なるのみであるので、この相違点についてのみ説明する。

【0059】

図10に、この変形例における図6と対応する処理のフローチャートを示す。

この第2の変形例のMFP100においては、図5のステップS105においてログイン成功であった場合、処理は図10のステップS401に進み、ここで認証サーバにユーザが属するグループのリストを要求し、これを取得する。

そして、そのリストに含まれる各グループを順次対象として、ステップS402及びS403の処理を繰り返す。これらの処理は、ステップS402で対象グループが、MFP100に利用権限情報の登録されているいずれかのグループと一致するか否か判断し、いずれかと一致した場合に、ステップS403で該当するグループについて設定されている利用権限を、認証サーバ200に認証された(MFP100の利用を要求している)ユーザの利用権限から削除するというものである。

【0060】

なお、ステップS402の判断は、権限情報記憶部121に記憶している情報を基に行うことができる。また、ステップS401を行う時点では、認証されたユーザは全ての利用権限を有するものとする。

従って、ステップS402及びS403のループにより、ユーザが複数のグループに属する場合、その複数のグループ全てについて利用権限のある機能についてのみ、そのユーザに利用権限を認めるようにすることになる。

【0061】

そして、その後ステップS404で、認証されたユーザが、MFP100に利用権限情報の登録されているいずれかのグループに属していたか否か判断する。そして、属していなければ、MFP100の使用は許可できないので、図5のステップS115以降の処理に進み、ユーザにMFP100の利用を許可せずに終了する。図9の処理の場合、ユーザがいずれのグループにも属していない場合、ステップS402とS403のループの後、全ての機能の利用権限を有する状態になってしまうので、このような処理を設けたものである。

【0062】

そして、ステップS404でYESであれば、ステップS405に進み、認証されたユーザに利用権限があるか否か判断し、あればステップS109以降の処理を行ってユーザに機能を提供する。なければ、図5のステップS115以降の処理に進み、ユーザにMFP100の利用を許可せずに終了する。

10

20

30

40

50

ステップ S 1 0 9 以降又はステップ S 1 1 5 以降の処理については、上述した実施形態の場合と同様であるので、説明は省略する。

以上のような処理を行うことによって、ユーザが複数のグループに属する場合でも、各グループにおける権限の内容を反映した処理が可能となり、より柔軟に利用権限を設定することができる。なお、この変形例の方式の場合、複数のグループに属するユーザに認める利用権限の範囲は、上述した第 1 の変形例の場合よりも総じて狭くなる。

【 0 0 6 3 】

〔 第 3 の変形例：図 1 1 ， 図 1 2 〕

次に、上述した実施形態の第 3 の変形例について説明する。この変形例は、デフォルトグループを設けてこのグループについての利用権限情報を権限情報記憶部 1 2 1 に設定しておき、ユーザに M F P 1 0 0 の利用権限がなかった場合でもデフォルトグループについて設定されている利用権限を与えるようにした点が、上述の第 1 の変形例と異なるのみである。そして、この点に伴い、ユーザが M F P 1 0 0 を使用しようとした場合に M F P 1 0 0 の C P U 1 0 1 が実行する処理において図 9 に示した部分が上述の第 1 の変形例と異なるのみであるので、この相違点についてのみ説明する。

10

【 0 0 6 4 】

図 1 1 に、この変形例における図 9 と対応する処理のフローチャートを示す。また、このフローチャートは、上述した実施形態における図 6 とも対応するものである。

この第 3 の変形例の M F P 1 0 0 においては、ステップ S 3 0 4 より前の処理は図 9 に示した第 1 の変形例の場合と同様であるが、ステップ S 3 0 4 でユーザに利用権限がなかった場合、ステップ S A で、デフォルトグループについて設定されている利用権限を、認証されたユーザの利用権限に追加し、ステップ S 1 0 9 以下の処理に進むようにしている。

20

【 0 0 6 5 】

そして、このような処理により、ユーザが属するグループがないことを示すグループ情報を受信した場合でも、そのユーザにデフォルトグループに係る利用権限を認めるようにしたものである。

なお、ステップ S 1 0 9 以降の処理については、上述した実施形態の場合と同様であるので、説明は省略する。

【 0 0 6 6 】

以上のような処理を行うことにより、特に設定を行わなくても全てのユーザについて一定の機能の利用を許可することができるので、それ以上の機能の使用を許可したいグループについてのみ利用権限を設定するのみでよく、設定の労力を低減することができる。

30

なお、同様な効果を得るためには、図 1 1 に示した処理に代えて、図 1 2 に示した処理を行うようにしてもよい。この処理においては、ステップ S A の処理をステップ S 3 0 1 の直後に行うようにしている。そして、このようにした場合、全てのユーザが少なくともデフォルトグループについて設定されている利用権限を有することになるため、図 1 1 のステップ S 3 0 4 の処理は省略している。

【 0 0 6 7 】

〔 第 4 の変形例：図 1 3 乃至図 1 5 〕

40

次に、上述した実施形態の第 4 の変形例について説明する。この変形例は、ユーザが属するグループの情報と、利用権限情報を定義したグループの情報とを比較する際に、グループ名ではなくグループの ID を用いるようにした点が、上述の第 1 の変形例と異なるのみである。なお、この ID としては、例えばウィンドウズ（登録商標）を使用する場合には、G U I D（Global Unique Identifier）や S I D（Security Identifier）を用いることができる。

この変形例の説明においても、この点に伴う第 1 の変形例からの変更点についてのみ説明する。

この変形例においては、上述した実施形態において図 4 等を用いて説明したように各グループについての利用権限情報を設定しようとする場合、権限情報記憶部 1 2 1 に、グル

50

ープ名と共にそのグループのIDも登録するようにしている。

【0068】

図13に、このための処理のフローチャートを示す。

この変形例においては、MFP100のCPU101は、ユーザがグループに関する利用権限情報を設定する指示を行った場合（例えば図4に示した権限設定画面20で設定キー25を押下した場合）、図13のフローチャートに示す処理を開始する。

そして、まずステップS501で、認証サーバ200にログインする。この際に使用するアカウントは、利用権限情報を設定しようとしたユーザのアカウントでも、MFP100自体のアカウントでもよい。そして、ステップS502でログインが成功したか否か判断し、成功していればステップS503で利用権限情報を設定しようとしているグループのIDを認証サーバに要求して送信させ、取得する。

【0069】

ここで、認証サーバ200において各グループにIDを付して管理するようにしておけば、認証サーバ200において定義されているグループについてはIDが取得できるはずであるが、ユーザが入力した名前のグループが必ずしも認証サーバ200において定義されているとは限らないので、グループのIDが取得できない場合も考えられる。

そこで、ステップS504で取得が成功したか否か判断する。そして、成功であれば、ステップS505で取得したIDをグループ名及び利用権限情報と共に権限情報記憶部121に登録し、ステップS506で登録成功のメッセージを操作表示部112に表示させて処理を終了する。

また、ステップS502でログインが失敗であったり、ステップS504でグループIDの取得に失敗した場合には、IDを登録できないため、利用権限情報の登録自体を取り止め、ステップS507で登録失敗のメッセージを操作表示部112に表示させて処理を終了する。

【0070】

以上のような処理を行うことにより、権限情報記憶部121に、グループ名や利用権限情報と対応させて、認証サーバ200でグループの管理に使用しているIDを登録することができる。すなわち、このID毎に利用権限情報を登録することができる。従って、認証サーバ200から受信するグループ情報に基づいてユーザの利用権限を判断する場合、グループのIDの情報を受信し、これを用いて判断するようにすることができる。

【0071】

また、MFP100においてグループの利用権限を設定しようとするに当たって、予め認証サーバ200からグループリスト及び各グループのIDを受信しておき、認証サーバ200で定義されているグループについて利用権限を設定させるようにしてもよい。

図14に、このようにする場合に、グループの利用権限を設定しようとするに当たってMFP100と認証サーバ200との間で実行する通信シーケンスを示す。

このように、予めMFP100が認証サーバ200で定義されているグループのリスト及び各グループのIDを取得しておくようにすれば、ユーザが利用権限を登録しようとした場合に認証サーバ200にアクセスする必要はないし、IDが取得できないために利用権限情報の登録自体ができなくなるといった事態を防止することができる。

【0072】

なお、このようなグループIDを利用する場合、第1の変形例の図9と対応する処理は、この変形例では以下のようにすることができる。

図15にこの処理のフローチャートを示す。

すなわち、この第4の変形例のMFP100においては、図5のステップS105においてログイン成功であった場合、処理は図15のステップS601に進み、ここで認証サーバ200にユーザが属するグループのIDのリストを要求して送信させ、これを取得する。

【0073】

10

20

30

40

50

そして、そのリストに含まれる各IDを順次対象として、ステップS602及びS603の処理を繰り返す。これらの処理は、ステップS602で、対象IDがMFP100に利用権限情報の登録されているいずれかのグループのIDと一致するか否か判断し、いずれかと一致した場合に、ステップS603で該当するグループについて設定されている利用権限を、認証サーバ200に認証された(MFP100の利用を要求している)ユーザの利用権限に追加するというものである。

なお、ステップS602の判断は、権限情報記憶部121に記憶している情報を基に行うことができる。また、ステップS601を行う時点では、認証されたユーザの利用権限は何もないものとする。

【0074】

そして、その後ステップS604で、認証されたユーザに利用権限があるか否か判断し、あればステップS109以降の処理を行ってユーザに機能を提供する。なければ、図5のステップS115以降の処理に進み、ユーザにMFP100の利用を許可せずに終了する。

ステップS109以降又はステップS115以降の処理については、上述した実施形態の場合と同様であるので、説明は省略する。

【0075】

以上のような処理を行い、グループをIDに基づいて比較するようにしたことにより、組織変更等により認証サーバ200側でグループの名称を変更する必要が生じた場合でも、グループIDが変わらなければ、MFP100側の設定内容を変更せずに権限管理を行うことができる。従って、設定の手間を省き、利用権限の管理をより省力化することができる。

【0076】

以上で実施形態及び変形例の説明を終了するが、以上説明した実施形態の及び変形例の構成は、互いに矛盾しない範囲で適宜組み合わせ適用することができる。

また、ネットワークシステムを構成する装置、各ネットワーク機器のハードウェア構成や機能構成、データの形式や処理の内容等が、上述の実施形態及び変形例で説明したものに限られないことも、もちろんである。

【0077】

例えば、ネットワークシステムは、最低限1つのネットワーク機器と1つの認証装置とによって構成することができる。また、通信に使用するネットワークも、LANに限られず、インターネットを介すものであってもよいし、有線、無線を問わずに、任意の通信経路を用いることができる。

さらに、各ネットワーク機器における利用権限情報の設定は、機器の操作表示部からだけでなく、ネットワークを介して通信可能なPC等の端末装置からウェブブラウザ等を用いてネットワーク機器にアクセスして行うことができるようにしてもよい。ネットワーク機器の機能の利用についても同様であり、外部の端末装置から機能の利用を要求される場合にも、上述したような権限管理は有効である。

【0078】

また、この発明が、認証装置からユーザが属するグループの情報を取得可能なネットワーク機器であれば、どのようなネットワーク機器にも適用可能であることはもちろんである。適用対象としては、例えば、プリンタ、FAX装置、デジタル複写機、スキャナ装置、デジタル複合機等の画像処理装置のほか、汎用コンピュータ、ネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム、自動車、航空機等にネットワーク通信機能を持たせたネットワーク機器が考えられる。

【0079】

また、この発明によるプログラムは、コンピュータに、上述したMFP100のようなネットワーク機器を制御させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

このようなプログラムは、はじめからコンピュータに備えるROMあるいはHDD等の

10

20

30

40

50

記憶手段に格納しておいてもよいが、記録媒体であるCD-ROMあるいはフレキシブルディスク、SRAM、EEPROM、メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてCPUに実行させるか、CPUにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【産業上の利用可能性】

【0080】

10

以上説明してきたように、この発明のネットワークシステム、利用権限判定方法、ネットワーク機器、プログラム又は記録媒体によれば、多数のネットワーク機器を使用する場合でも、容易に各ユーザの利用権限を設定することができる。

従って、この発明を利用することにより、高いセキュリティと利便性を両立したネットワークシステムを構成することができる。

【図面の簡単な説明】

【0081】

【図1】この発明のネットワーク機器の実施形態であるMFPのハードウェア構成を示すブロック図である。

【図2】図1に示した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。

20

【図3】図2に示したMFP及び認証サーバの機能構成のうち、この実施形態の特徴に関連する部分を示す図である。

【図4】図3に示したMFPにおいて表示操作部から利用権限情報の入力を受け付けて権限情報記憶部に記憶させる場合に使用する画面及びその操作手順について説明するための図である。

【図5】ユーザが図3に示したMFPを使用しようとした場合にMFPが実行する処理の一部を示すフローチャートである。

【図6】図5の続きの部分を示すフローチャートである。

【図7】図5に示した処理において使用するログイン画面の表示例を示す図である。

【図8】図5及び図6に示した処理と対応する認証サーバ側の処理を示すフローチャートである。

30

【図9】この発明の実施形態の第1の変形例における図6と対応する処理を示すフローチャートである。

【図10】この発明の実施形態の第2の変形例における図6と対応する処理を示すフローチャートである。

【0082】

【図11】この発明の実施形態の第3の変形例における図6と対応する処理を示すフローチャートである。

【図12】そのさらに別の例を示すフローチャートである。

【図13】この発明の実施形態の第4の変形例において、ユーザがグループに関する利用権限情報を設定する指示を行った場合にMFPが行う処理を示すフローチャートである。

40

【図14】その変形例のバリエーションにおいて、グループの利用権限を設定しようとするに当たってMFPと認証サーバとの間で実行する通信のシーケンスを示す図である。

【図15】この発明の実施形態の第4の変形例における図6と対応する処理を示すフローチャートである。

【符号の説明】

【0083】

20：権限設定画面、30：コピー権限設定画面、40：ログイン画面、

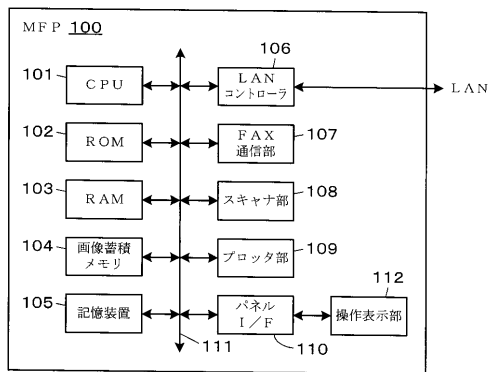
100：MFP、101：CPU、102：ROM、103：RAM、

104：画像蓄積メモリ、105：記憶装置、106：LANコントローラ、

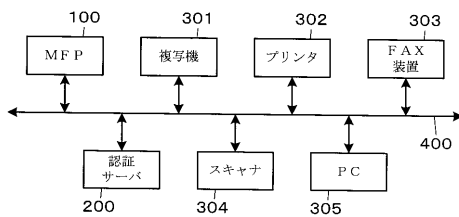
50

107 : FAX 通信部、108 : スキャナ部、109 : プロッタ部、
 110 : パネル I / F、111 : システムバス、112 : 操作表示部、
 121 : 権限情報記憶部、122 : 権限判断部、123 : 送受信機能部、
 124 : 機能提供部、200 : 認証サーバ、201 : ユーザ情報記憶部、
 202 : ログイン判定部、203 : グループ判定部、204 : 送受信機能部

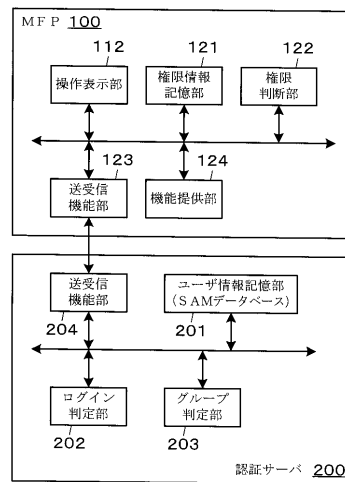
【図1】



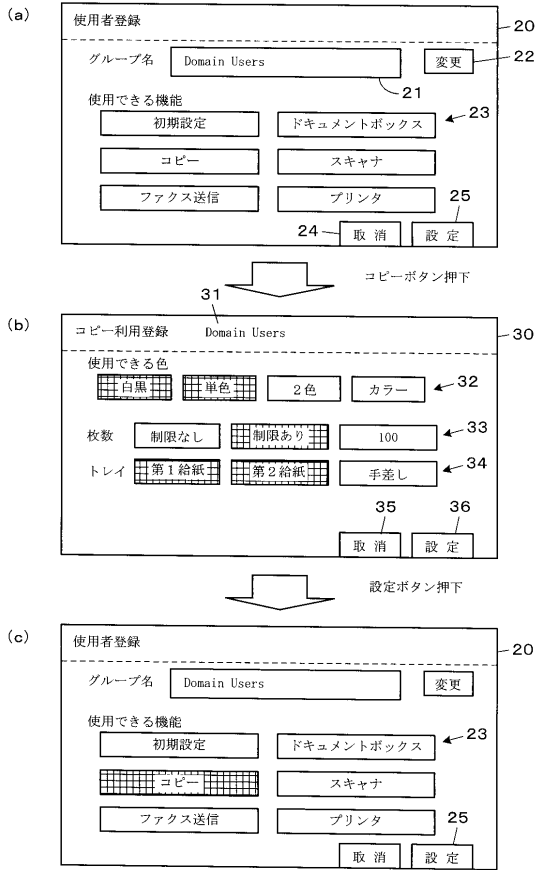
【図2】



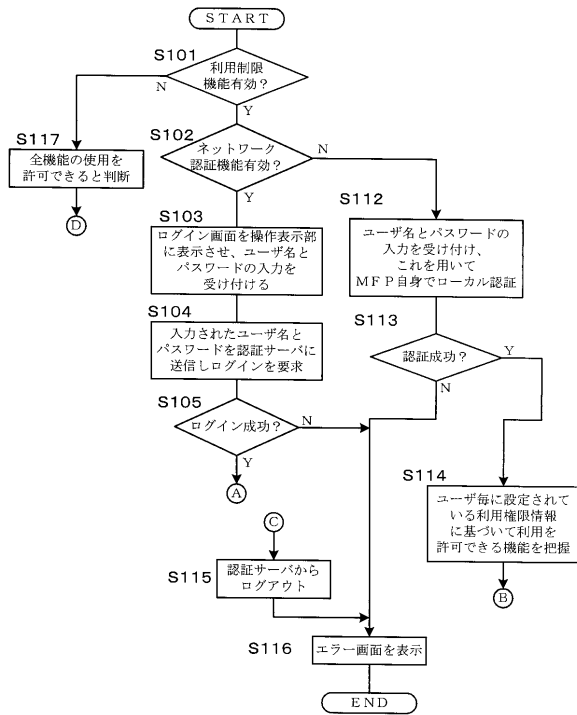
【図3】



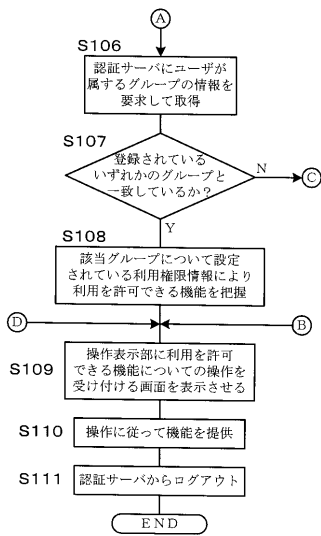
【 図 4 】



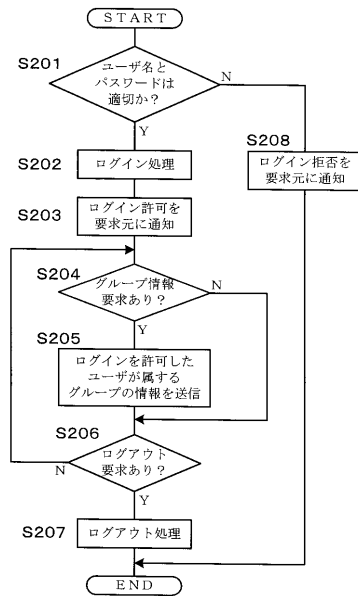
【 図 5 】



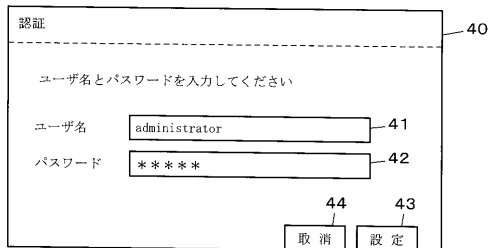
【 図 6 】



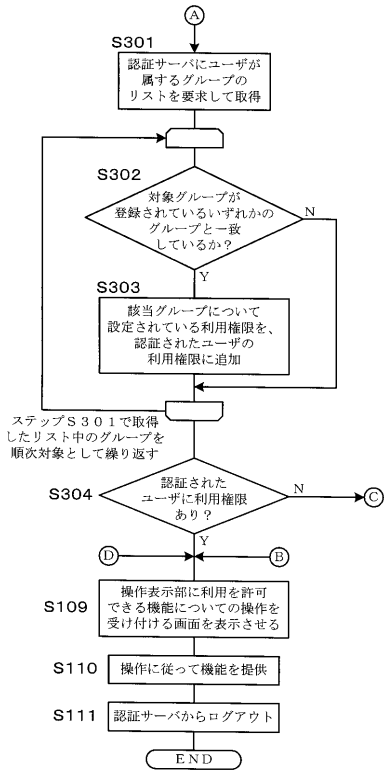
【 図 8 】



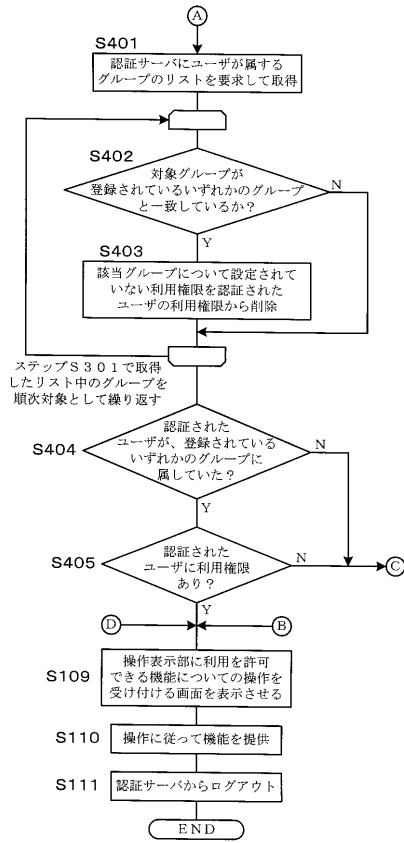
【 図 7 】



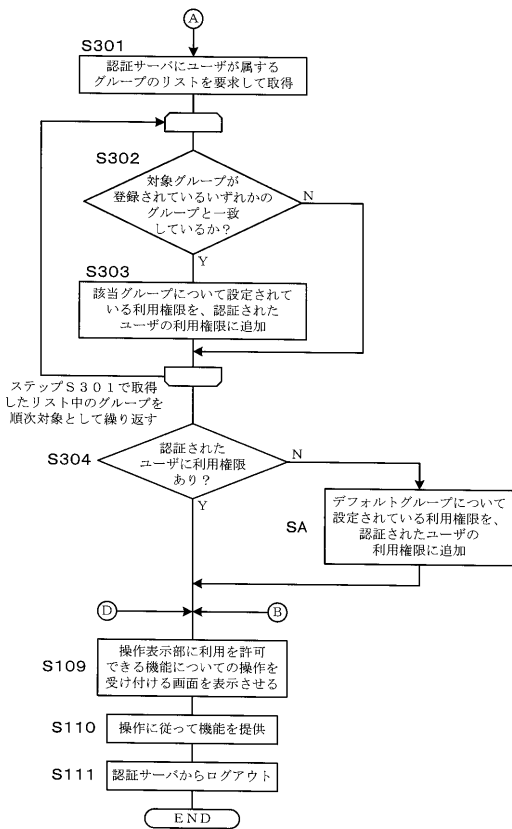
【 図 9 】



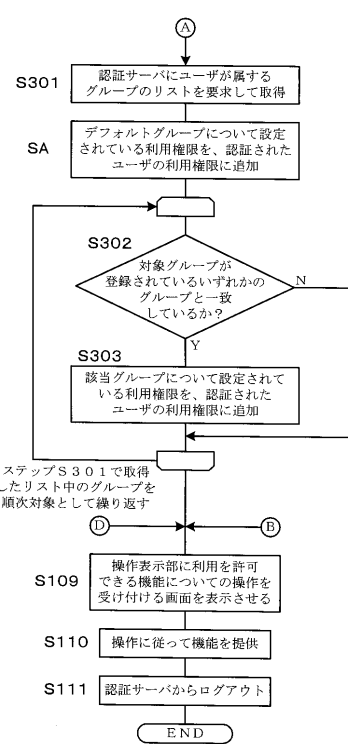
【 図 10 】



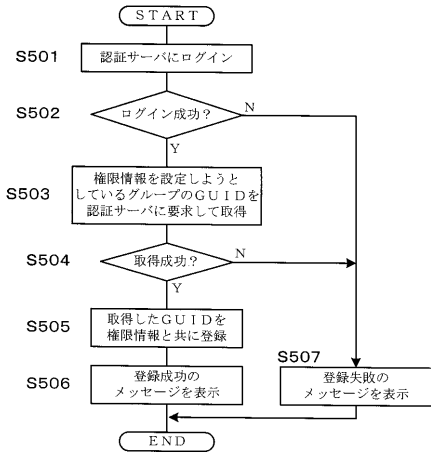
【 図 11 】



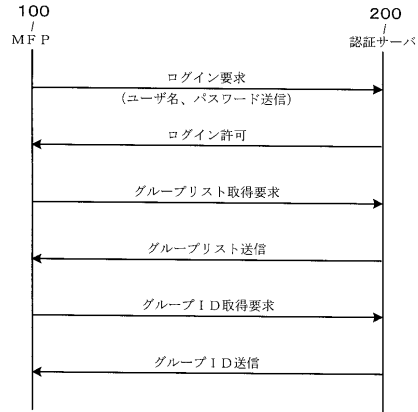
【 図 12 】



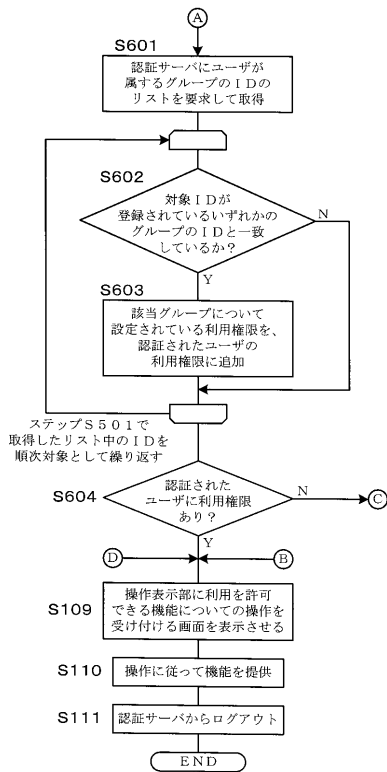
【 図 1 3 】



【 図 1 4 】



【 図 1 5 】



フロントページの続き

(51) Int.Cl.	F I	テーマコード(参考)
G 0 6 F 13/00 (2006.01)	G 0 6 F 13/00 3 5 7 A	5 B 0 8 9
G 0 3 G 21/04 (2006.01)	G 0 3 G 21/00 3 9 0	

Fターム(参考) 2H027 DA36 DE07 DE09 EB04 EC06 EC07 EE07 EE08 EE10 EH06
EJ03 EJ04 EJ08 EJ13 GA54 GB13 GB20 ZA07
5B021 AA01 AA02 BB01 CC05 DD12 NN18
5B085 AE02 AE03 AE06
5B089 GA13 GA14 GA15 GA16 JB15 KA13 KB13 KC58