

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6298285号
(P6298285)

(45) 発行日 平成30年3月20日 (2018. 3. 20)

(24) 登録日 平成30年3月2日 (2018. 3. 2)

(51) Int. Cl.

F I

G 0 6 F 21/31 (2013. 01)

G 0 6 F 21/31

G 0 6 F 21/12 (2013. 01)

G 0 6 F 21/12 3 1 0

G 0 6 F 3/12 (2006. 01)

G 0 6 F 3/12 3 3 8

B 4 1 J 29/00 (2006. 01)

B 4 1 J 29/00 Z

B 4 1 J 29/38 (2006. 01)

B 4 1 J 29/38 Z

請求項の数 10 (全 18 頁)

(21) 出願番号 特願2013-260663 (P2013-260663)
 (22) 出願日 平成25年12月17日 (2013. 12. 17)
 (65) 公開番号 特開2015-118486 (P2015-118486A)
 (43) 公開日 平成27年6月25日 (2015. 6. 25)
 審査請求日 平成28年12月16日 (2016. 12. 16)

(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
 (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】 情報処理装置及びその制御方法、並びにプログラム

(57) 【特許請求の範囲】

【請求項 1】

ユーザ認証を必要とせずに情報処理装置を使用可能な第1のユーザとしてユーザが前記情報処理装置にログインした状態において、前記第1のユーザ以外の第2のユーザとしてユーザが前記情報処理装置にログインするためのユーザ認証を行う認証手段と、

前記認証手段によって前記ユーザ認証が行われると、前記情報処理装置が有する複数の機能のそれぞれについて、前記第1のユーザの使用権限と前記第2のユーザの使用権限とを比較して、前記第1のユーザに使用が許可されている機能のうちで前記第2のユーザに使用が許可されていない機能が存在するか否かを判定する判定手段と、

前記判定手段によって、前記第1のユーザに使用が許可されている機能のうちで前記第2のユーザに使用が許可されていない機能が存在すると判定されると、使用が許可されていない当該機能の使用を前記第2のユーザに許可するよう、当該機能についての前記第2のユーザの使用権限を修正する修正手段と、を備え、

前記情報処理装置には、前記情報処理装置を使用可能なユーザをそれぞれが含む複数のユーザグループが登録され、登録された各ユーザグループに対して、前記複数の機能のそれぞれについての使用権限が設定されており、

前記第1及び第2のユーザは、前記複数のユーザグループのうちの第1及び第2のユーザグループにそれぞれ属するように設定され、

前記修正手段は、前記第1のユーザグループに使用が許可されている機能のうちで前記第2のユーザグループに使用が許可されていない機能の使用を、前記第2のユーザグループ

10

20

に許可するよう、当該機能についての前記第 2 のユーザグループの使用権限を修正することを特徴とする情報処理装置。

【請求項 2】

前記修正手段によって前記第 2 のユーザの使用権限が修正されると、修正後の使用権限に従って、前記第 2 のユーザに使用が許可されている機能を使用可能にする制御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】

前記第 1 のユーザとしてユーザが前記情報処理装置にログインした状態において、前記複数の機能のうちのいずれかの機能を使用するためのユーザの指示を受け付ける指示手段を更に備え、

10

前記認証手段は、前記指示が示す機能の使用が前記第 1 のユーザに許可されている場合には前記ユーザ認証を行わず、前記指示が示す機能の使用が前記第 1 のユーザに許可されていない場合に前記第 2 のユーザとしてユーザが前記情報処理装置にログインするための前記ユーザ認証を行う

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】

前記情報処理装置に設定されている、前記複数の機能についての各ユーザの使用権限を、ユーザの指示に従って変更する変更手段を更に備え、

前記修正手段は、更に、

前記変更手段によっていずれかのユーザについての使用権限の変更が行われると、前記第 1 のユーザに使用が許可されている機能のうちで、前記第 2 のユーザに使用が許可されていない機能の使用を前記第 2 のユーザに許可するよう、当該機能についての前記第 2 のユーザの使用権限を修正する

20

ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載の情報処理装置。

【請求項 5】

前記情報処理装置に設定されている、前記複数の機能についての各ユーザの使用権限を、ユーザの指示に従って変更する変更手段と、

前記変更手段によっていずれかのユーザについての使用権限の変更が行われ、かつ、前記第 1 のユーザに使用が許可されている機能のうちで、前記第 2 のユーザに使用が許可されていない機能が存在する場合、前記第 2 のユーザの使用権限を修正するか否かをユーザに確認する確認手段と、を更に備え、

30

前記修正手段は、更に、

前記確認手段によって前記第 2 のユーザの使用権限を修正することが確認されると、前記第 1 のユーザに使用が許可されている機能のうちで、前記第 2 のユーザに使用が許可されていない機能の使用を前記第 2 のユーザに許可するよう、当該機能についての前記第 2 のユーザの使用権限を修正する

ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載の情報処理装置。

【請求項 6】

前記第 2 のユーザは、前記情報処理装置に登録されている、前記第 1 のユーザ以外の前記ユーザ認証を必要とする全てのユーザを含むことを特徴とする請求項 4 または 5 に記載の情報処理装置。

40

【請求項 7】

前記情報処理装置は、電源オフ状態から起動する際に、前記第 1 のユーザとして自動的にユーザがログインした状態で起動することを特徴とする請求項 1 から 6 のいずれか 1 項に記載の情報処理装置。

【請求項 8】

前記第 1 のユーザは、前記情報処理装置の工場出荷時に、前記情報処理装置に予め登録されるユーザであり、

前記第 2 のユーザは、前記情報処理装置の工場出荷後に登録される、前記ユーザ認証を必要とするユーザである

50

ことを特徴とする請求項 1 から 7 のいずれか 1 項に記載の情報処理装置。

【請求項 9】

ユーザ認証を必要とせずに情報処理装置を使用可能な第 1 のユーザとしてユーザが前記情報処理装置にログインした状態において、前記第 1 のユーザ以外の第 2 のユーザとしてユーザが前記情報処理装置にログインするためのユーザ認証を行う認証工程と、

前記認証工程で前記ユーザ認証が行われると、前記情報処理装置が有する複数の機能のそれぞれについて、前記第 1 のユーザの使用権限と前記第 2 のユーザの使用権限とを比較して、前記第 1 のユーザに使用が許可されている機能のうちで前記第 2 のユーザに使用が許可されていない機能が存在するか否かを判定する判定工程と、

前記判定工程で、前記第 1 のユーザに使用が許可されている機能のうちで前記第 2 のユーザに使用が許可されていない機能が存在すると判定されると、使用が許可されていない当該機能の使用を前記第 2 のユーザに許可するよう、当該機能についての前記第 2 のユーザの使用権限を修正する修正工程と、を含み、

前記情報処理装置には、前記情報処理装置を使用可能なユーザをそれぞれが含む複数のユーザグループが登録され、登録された各ユーザグループに対して、前記複数の機能のそれぞれについての使用権限が設定されており、

前記第 1 及び第 2 のユーザは、前記複数のユーザグループのうちの第 1 及び第 2 のユーザグループにそれぞれ属するように設定され、

前記修正工程では、前記第 1 のユーザグループに使用が許可されている機能のうちで前記第 2 のユーザグループに使用が許可されていない機能の使用を、前記第 2 のユーザグループに許可するよう、当該機能についての前記第 2 のユーザグループの使用権限を修正する

ことを特徴とする情報処理装置の制御方法。

【請求項 10】

コンピュータを請求項 1 から 8 のいずれか 1 項に記載の情報処理装置の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、情報処理装置及びその制御方法、並びにプログラムに関するものである。

【背景技術】

【0002】

従来の複合機（MFP）には、例えば特許文献 1 に示されるように、起動時にはユーザ認証を要求せずに誰でも使用可能な状態にし、特定の機能を使用する場合にユーザ認証を要求するものが存在する。このような MFP は、ユーザ認証に成功した場合にのみ、その機能の使用を許可するユーザ認証機能を備えている。

【0003】

このようなユーザ認証機能では、通常、MFP が有する複数の機能のうちでユーザ認証を要求する機能を、MFP の利用状況、ユーザ等に応じて、MFP の管理者が自由に設定できるようにしている。例えば、コピー機能、送信機能、保存機能等を有する MFP において、コピー機能を任意のユーザが使用でき、送信機能をユーザ A のみ、保存機能をユーザ B のみが使用できるように設定できる。

【0004】

また、MFP には、MFP が有する複数の機能のそれぞれについて使用する権限を、複数のユーザについて一括して管理するための、ユーザグループに相当する「ロール」と称される概念が導入されたものがある。例えば、送信機能の使用が許可され、保存機能の使用が禁止されたロール 1 と、送信機能の使用が禁止され、保存機能の使用が許可されたロール 2 とを登録し、ユーザ A 及び B にはロール 1 を、ユーザ C にはロール 2 を割り当てたとする。この場合、送信機能をユーザ A 及び B のみに使用させ、保存機能をユーザ C のみに使用させるという機能制御を実現できる。また、ロール 1 の権限を変更するだけで、ユーザ A 及び B の権限を一括して変更できるため、各ユーザの権限の管理が容易になる。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特許第4745657号

【発明の概要】

【発明が解決しようとする課題】

【0006】

上述のように、起動時にはユーザ認証なしで限定された機能のみ使用可能な状態で起動し、特定の機能をユーザが使用する場合にユーザ認証を要求するMFPでは、以下のような課題がある。このようなMFPでは、例えば、起動時には特定のユーザ（ここでは「自動ログインユーザ」と称する。）が自動的にログインした状態とする。また、ユーザが特定の機能を使用する場合には、別のユーザ（ここでは「ログインユーザ」と称する。）としてユーザにログインさせる。このような機能制御を行うMFPで、自動ログインユーザの権限を変更可能とするために自動ログインユーザにロールを割り当てた場合、ロールの権限の設定に依存して、ログインユーザの権限が自動ログインユーザの権限よりも限定されてることが起こりうる。

10

【0007】

例えば、ロール1については、送信機能の使用を許可し、保存機能の使用を禁止し、ロール2については、送信機能の使用を禁止し、保存機能の使用を許可するよう設定し、自動ログインユーザにロール1を、ログインユーザにロール2を割り当てたとする。この場合、MFPのユーザは、ユーザ認証前の自動ログイン状態では送信機能を使用可能であり、保存機能を使用するためにはユーザ認証が必要となる。ユーザ認証によりユーザがログインユーザとしてMFPにログインすると、保存機能が使用可能になる一方、認証前に自動ログインユーザとして使用できていた送信機能が使用不可能になる。また、ログインユーザとしてログインしたユーザが送信機能を使用するためには、一旦ログアウトして、自動ログイン状態に戻る必要がある。

20

【0008】

このように、ユーザ認証によってMFPの各機能の使用可否を個別に制御する場合、認証前のユーザについての機能の使用権限の設定と、認証後のユーザについての機能の使用権限の設定とに依存して、認証後に特定の機能が使用不可能になる可能性がある。

30

【0009】

本発明は、上述の問題に鑑みてなされたものである。本発明は、ユーザ認証によって各機能の使用可否を個別に制御する情報処理装置で、使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなることを防ぐ技術を提供することを目的としている。

【課題を解決するための手段】

【0010】

本発明は、例えば、情報処理装置として実現できる。本発明の一態様に係る情報処理装置は、ユーザ認証を必要とせずに情報処理装置を使用可能な第1のユーザとしてユーザが前記情報処理装置にログインした状態において、前記第1のユーザ以外の第2のユーザとしてユーザが前記情報処理装置にログインするためのユーザ認証を行う認証手段と、前記認証手段によって前記ユーザ認証が行われると、前記情報処理装置が有する複数の機能のそれぞれについて、前記第1のユーザの使用権限と前記第2のユーザの使用権限とを比較して、前記第1のユーザに使用が許可されている機能のうちで前記第2のユーザに使用が許可されていない機能が存在するか否かを判定する判定手段と、前記判定手段によって、前記第1のユーザに使用が許可されている機能のうちで前記第2のユーザに使用が許可されていない機能が存在すると判定されると、使用が許可されていない当該機能の使用を前記第2のユーザに許可するよう、当該機能についての前記第2のユーザの使用権限を修正する修正手段と、を備え、前記情報処理装置には、前記情報処理装置を使用可能なユーザをそれぞれが含む複数のユーザグループが登録され、登録された各ユーザグループに対して、前

40

50

記複数の機能のそれぞれについての使用権限が設定されており、前記第１及び第２のユーザは、前記複数のユーザグループのうちの第１及び第２のユーザグループにそれぞれ属するように設定され、前記修正手段は、前記第１のユーザグループに使用が許可されている機能のうちで前記第２のユーザグループに使用が許可されていない機能の使用を、前記第２のユーザグループに許可するよう、当該機能についての前記第２のユーザグループの使用権限を修正することを特徴とする。

【発明の効果】

【００１１】

本発明によれば、ユーザ認証によって各機能の使用可否を個別に制御する情報処理装置で、使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなることを防ぐことができる。これにより、ユーザにとっての利便性を向上させることができる。

10

【図面の簡単な説明】

【００１２】

【図１】MFP１０１に関連するシステム構成図。

【図２】MFP１０１のハードウェアの構成を示すブロック図。

【図３】MFP１０１のソフトウェアの構成を示すブロック図。

【図４】メインメニュー画面の例を示す図。

【図５】コピー画面の例を示す図。

【図６】送信画面の例を示す図。

20

【図７】認証画面の例を示す図。

【図８】設定画面の例を示す図。

【図９】ユーザ情報設定画面の例を示す図。

【図１０】ルール設定画面の例を示す図。

【図１１】権限修正確認画面の例を示す図。

【図１２】ユーザDB３０６に格納されているユーザ情報の例を示す図。

【図１３】ユーザDB３０６に格納されているルール情報の例を示す図。

【図１４】ユーザのログイン時の、権限情報の修正処理の手順を示すフローチャート。

【図１５】ユーザまたはルール情報の設定時の、権限情報の修正処理の手順を示すフローチャート。

30

【発明を実施するための形態】

【００１３】

以下、本発明を実施するための形態について図面を用いて説明する。なお、以下の実施形態は特許請求の範囲に係る発明を限定するものでなく、また実施形態で説明されている特徴の組み合わせの全てが発明の解決手段に必須のものとは限らない。

【００１４】

<システム構成>

図１は、MFP１０１を含むシステムの構成例を示すブロック図である。図１に示すシステムにおいて、MFP１０１、認証サーバ１０２及びメールサーバ１０３は、LAN１００に接続されており、LAN１００を介して相互に通信可能である。LAN１００は、インターネット１１０に接続されている。このため、MFP１０１、認証サーバ１０２及びメールサーバ１０３は、それぞれ、LAN１００を介してインターネット１１０に接続可能である。

40

【００１５】

認証サーバ１０２は、MFP１０１の利用者（ユーザ）の認証（ユーザ認証）に利用される。メールサーバ１０３は、MFP１０１から電子メールを送信する際に利用される。MFP１０１は、コピー、スキャン、プリント、送信等の機能を備える。例えば、MFP１０１は、スキャンした原稿の画像を電子ファイルに変換し、その電子ファイルを電子メールに添付して、指定された送信先に送信することができる。

【００１６】

50

< MFPのハードウェア構成 >

図2は、MFP101のハードウェア構成例を示すブロック図である。MFP101は、MFP101全体の動作を制御する制御部200と、操作部209と、プリンタ210と、スキャナ211といったデバイスを備える。なお、MFP101は、本発明の情報処理装置の一例である。

【0017】

制御部200は、CPU201、ROM202、RAM203、HDD204、操作部インタフェース(I/F)205、プリンタI/F206、スキャナI/F207及びネットワークI/F208を備える。制御部200は、これらのデバイスによってMFP101全体の動作を制御する。操作部I/F205、プリンタI/F206及びスキャナI/F207には、それぞれ操作部209、プリンタ210及びスキャナ211が接続されている。

【0018】

CPU201は、ROM202に格納されている制御プログラムをRAM203に読み出して実行することで、読取制御や送信制御等の各種制御を行う。RAM203は、CPU201の主メモリ、ワークエリア等の一時記憶領域として用いられる。HDD204は、画像データや各種プログラム等を格納する。

【0019】

操作部I/F205は、操作部209と制御部200とを接続するためのインタフェースである。操作部209は、タッチパネル機能を有する液晶表示部、キーボード等を備え、表示デバイス及び入力デバイスとして機能する。液晶表示部は、各種の情報を表示する表示部として機能する。また、操作部209は、ユーザがMFP101に各種の情報及び指示を入力するためのユーザインタフェース(UI)として機能する。

【0020】

プリンタI/F206は、プリンタ210と制御部200とを接続するためのインタフェースである。CPU201は、プリンタ210によって記録媒体上に印刷すべき画像に対応する画像データを、プリンタI/F206を介してプリンタ210に転送する。プリンタ210は、制御部200から受信した画像データに基づく画像を記録媒体上に印刷する。

【0021】

スキャナI/F207は、スキャナ211と制御部200とを接続するためのインタフェースである。スキャナ211は、原稿上の画像を読み取って画像データを生成し、生成した画像データをスキャナI/F207を介して制御部200に送信する。

【0022】

ネットワークI/F208は、制御部200(MFP101)をLAN100に接続するためのインタフェースである。ネットワークI/F208は、LAN100に接続されている、認証サーバ102、メールサーバ103等の外部装置と通信を行うことで、外部装置との間で、各種の情報(データ)の送受信を行う。

【0023】

< MFPのソフトウェア構成 >

図3は、MFP101のソフトウェア構成例を示すブロック図である。図3に示す各機能ブロックに対応するソフトウェア(制御プログラム)は、MFP101のROM202またはHDD204に格納されている。図3に示す各機能ブロックの、以下で説明する機能は、CPU201が、ROM202またはHDD204に格納されているソフトウェアを実行することによって、MFP101上で実現される。ただし、各機能ブロックの機能は、専用のハードウェアによって実現されてもよい。なお、図3では、本実施形態の説明に特に関連するソフトウェア構成を示している。

【0024】

図3に示すように、MFP101は、ソフトウェア構成として、UI制御部300、メニュー処理部301、コピー処理部302、送信処理部303、認証処理部304、設定

10

20

30

40

50

処理部 305、及びユーザデータベース（ユーザDB）306を備える。

【0025】

UI制御部300は、操作部I/F205を介して操作部209を制御する機能を提供する。UI制御部300は、ユーザが操作部209で操作した内容を、各処理部301～305に通知し、また、各処理部301～305から画面表示リクエストを受けると、当該リクエストに応じた画面を表示するよう、操作部209を制御する。このように、各処理部301～305は、通常、UI制御部300を介して操作部209に画面を表示する。

【0026】

メニュー処理部301は、MFP101に搭載されている各種機能（アプリケーション）へアクセスするためのメニュー画面を提供する。メニュー処理部301は、MFP101に搭載されている機能を検出し、それらの機能の一覧であるメインメニュー画面400（図4）を操作部209に表示する。メインメニュー画面400上で、いずれかの機能に対応するボタンがユーザによって押下された場合、メニュー処理部301は、ボタンに対応する機能を実行する処理部に、画面表示に関する通知を送信する。更に、メニュー処理部301は、必要に応じて認証処理部304に認証リクエストを送信する。

10

【0027】

コピー処理部302は、コピーに関する機能を提供する。コピー処理部302は、プリンタI/F206を介してプリンタ210を制御するとともに、スキャナI/F207を介してスキャナ211を制御することによって、コピー機能を実現する。また、コピー処理部302は、コピー画面500（図5）を操作部209に表示する。

20

【0028】

送信処理部303は、送信に関する機能を提供する。例えば、送信処理部303は、スキャナI/F207を介してスキャナ211を制御し、スキャナ211によって得られたスキャンデータを、ネットワークI/F208を介してLAN100へ送信することで、外部装置へスキャンデータの送信を行う。また、送信処理部303は、送信画面600（図6）を操作部209に表示する。

【0029】

認証処理部304は、MFP101を使用するユーザを認証する機能を提供する。認証処理部304は、認証画面700（図7）を操作部209に表示する。認証処理部304は、ユーザによって認証画面700を介して入力された情報と、ユーザDB306に格納されている情報とを照合することで、ユーザ認証を行う。なお、本実施形態では、認証処理部304はMFP101内に設けられているが、認証サーバ102内に設けられてもよい。その場合には、ユーザDB306も認証サーバ102内に設けられてもよい。

30

【0030】

設定処理部305は、ユーザに関する情報を設定する機能を提供する。設定処理部305は、ユーザの指示を受け付けるための操作画面として、設定画面800（図8）、ユーザ情報設定画面900（図9）、ルール設定画面1000（図10）、及び権限修正確認画面1100（図11）を操作部209に表示する。設定処理部305は、ユーザによって各設定画面を介して入力された情報を、ユーザDB306へ保存するとともに、ユーザDB306に保存されている情報を、各設定画面に表示する。また、設定処理部305は、権限修正確認画面1100（図11）を介して入力されたユーザの指示に従って、ルール情報テーブル1300（図13）内の情報を修正する。

40

【0031】

ユーザDB306は、ユーザに関する情報であるユーザ情報と、ルールに関する情報であるルール情報とが格納されるデータベースである。本実施形態では、ユーザDB306は、HDD204内に構築される。このため、ユーザDB306に格納される情報は、HDD204に記憶される。

【0032】

本実施形態で、「ルール」は、MFP101が有する複数の機能のそれぞれについて使

50

用する権限を、複数のユーザについて一括して管理するためのユーザグループに相当する。MFP101には、MFPを使用可能なユーザをそれぞれが含む複数のロールを登録可能であり、登録された各ロールに対して、MFP101が有する機能ごとの使用権限を設定可能である。各ロールに属するユーザには、当該ロールに対して設定された使用権限が適用され、MFP101が有する機能ごとに、ユーザ間で共通する使用権限が設定される。各ロールに属するユーザは、当該ロールに対して使用が許可された機能を使用できる一方、当該ロールに対して使用が許可されていない機能を使用することはできない。

【0033】

<ユーザ情報の例>

図12は、ユーザDB306に格納（保存）されているユーザ情報の例を示す図である。ユーザDB306には、図12に示す、ユーザ情報が格納されたテーブルであるユーザ情報テーブル1200のように、ユーザ情報がテーブル形式のデータとして格納されている。ユーザ情報テーブル1200に格納されている情報は、ユーザ情報設定画面900（図9）を用いてユーザによって設定された情報であり、設定処理部305によって当該テーブルに格納される。

【0034】

ユーザID1201は、ユーザIDフィールド901に入力された情報に相当する。パスワード1202は、パスワードフィールド902に入力された情報に相当する。ロール1203は、ロールフィールド903で選択されたロール名（図13に示すロール名1301）に相当する。

【0035】

ユーザID1201が「自動ログイン」であるユーザは、自動ログインユーザに相当する。自動ログインユーザのユーザ情報は、MFP101の工場出荷時に予め登録される。自動ログインユーザのユーザ情報のうち、ユーザID1201及びパスワード1202は、出荷時には未設定の状態であり、出荷後にも設定されることはない。本実施形態で、自動ログインユーザは、ユーザ認証を必要とせずにMFP101を使用可能なユーザ（第1のユーザ）である。ユーザがMFP101を使用する場合、ユーザ認証を行う前には、自動ログインユーザとしてMFP101にログインした状態である。このため、自動ログインユーザに使用が許可されている機能については、ユーザ認証を必要とすることなく任意のユーザが使用できる。

【0036】

ユーザID1201が「ユーザ1」及び「ユーザ2」であるユーザは、ユーザ認証を必要とするユーザ（以下では「ログインユーザ」とも称する。）である。ログインユーザのユーザ情報は、MFP101の工場出荷後に任意に登録可能である。ログインユーザのユーザ情報には、ユーザ認証用にパスワード1202が設定される。図12に示すように、自動ログインユーザ及びログインユーザは、MFP101に登録された複数のロール（ユーザグループ）のうちで、いずれかのロールに属するように設定される。

【0037】

<ロール情報の例>

図13は、ユーザDB306に格納（保存）されているロール情報の例を示す図である。ユーザDB306には、図13に示す、ロール情報が格納されたテーブルであるロール情報テーブル1300のように、ロール情報がテーブル形式のデータとして格納されている。ロール情報テーブル1300に格納されている情報は、ユーザがロール設定画面1000（図10）を用いて設定した情報であり、設定処理部305によって当該テーブルに格納される。

【0038】

ロール名1301は、ロール名フィールド1001に入力された情報に相当する。列1302～1304は、それぞれ、MFP101が有するコピー機能、送信機能及び設定機能についての、各ロールの使用権限に相当し、選択フィールド1002を使用して、「許可」または「禁止」が設定される。なお、本実施形態では、MFP101が有する機能（

10

20

30

40

50

アプリケーション)として、コピー機能、送信機能及び設定機能を例として説明するが、MFP101が他の機能を有していてもよい。例えば、MFP101は、これらの機能の他に、MFP101内にスキャンデータを保存するための保存機能を有していてもよい。

【0039】

<画面例>

次に、図4乃至図10を参照して、本実施形態における上述の各処理部301～305の動作に関連する、操作部209に表示される操作画面の例について説明する。

【0040】

(メインメニュー画面400)

図4は、メニュー処理部301によって操作部209に表示されるメインメニュー画面の一例を示す図である。図4に示すメインメニュー画面400は、本実施形態ではMFP101が起動した直後に操作部209に表示される。メインメニュー画面400は、MFP101に搭載されている機能の一覧を表示する。MFP101のユーザは、この画面に表示されているボタン401～403を押下することで、MFP101に搭載されている各機能を使用することができる。

【0041】

コピーボタン401は、コピー機能を使用するために用いられ、当該ボタンが押下されると、コピー画面500が操作部209に表示される。送信ボタン402は、送信機能を使用するために用いられ、当該ボタンが押下されると、送信画面600が操作部209に表示される。設定ボタン403は、設定機能を使用するために用いられ、当該ボタンが押下されると、設定画面800が操作部209に表示される。なお、ボタン401～403のうち、ユーザが押下したボタンに対応する機能の使用が禁止されている場合、UI制御部300は、操作部209に認証画面700を表示する。

【0042】

ログインボタン404は、ユーザ認証の実行をMFP101に指示するために用いられ、当該ボタンが押下されると、認証画面700が操作部209に表示される。ユーザ認証を行う前は、ユーザは、ユーザ認証なしで自動ログインユーザとしてMFP101にログインした状態にある。ログインボタン404は、自動ログインユーザ以外の別のユーザ(例えば、図12に示すユーザ1またはユーザ2)としてユーザがMFP101にログインするためのユーザ認証の実行を指示する場合に用いられる。自動ログインユーザ以外の別のユーザとしてユーザがMFP101にログインした状態である場合、ログインボタン404に代えて、MFP101からログアウトする(即ち、自動ログインユーザに戻る)ためのボタンがメインメニュー画面400に表示される。

【0043】

(コピー画面500)

図5は、コピー画面の一例を示す図である。図5に示すコピー画面500は、コピー処理部302によって操作部209に表示される。MFP101のユーザは、コピー画面500を使用することで、MFP101のコピー機能を使用することができる。コピー設定表示フィールド501には、現在設定されている値が表示される。コピー設定フィールド502には、コピー機能に関する各種設定を行うためのボタンが表示される。

【0044】

(送信画面600)

図6は、送信画面の一例を示す図である。図6に示す送信画面600は、送信処理部303によって操作部209に表示される。MFP101のユーザは、送信画面600を使用することで、MFP101の送信機能を使用することができる。宛先設定フィールド601には、スキャンデータの送信先となる宛先を設定するためのボタンが表示される。スキャン設定フィールド602には、スキャンに関する各種の設定が表示される。

【0045】

(認証画面700)

図7は、認証画面の一例を示す図である。図7に示す認証画面700は、認証処理部3

10

20

30

40

50

04によって操作部209に表示される。MFP101のユーザは、認証画面700を使用することで、MFP101の各機能を使用するためのユーザ認証をMFP101に実行させることができる。

【0046】

ユーザ名入力フィールド701は、ユーザ名を入力するために用いられる。パスワード入力フィールド702は、パスワードを入力するために用いられる。キャンセルボタン703は、認証画面700を用いたユーザ認証をキャンセルするために用いられる。ユーザがキャンセルボタン703を押下した場合、UI制御部300は、認証画面700を表示する前に表示していた画面を操作部209に表示する。ログインボタン704は、ユーザ認証の実行を指示するために用いられる。ユーザがログインボタン704を押下した場合、認証処理部304は、ユーザ名入力フィールド701及びパスワード入力フィールド702に入力された情報に基づいてユーザ認証を実行する。

10

【0047】

(設定画面800)

図8は、各種の詳細な設定項目を表示するための設定画面の一例を示す図である。図8に示す設定画面800は、設定処理部305によって操作部209に表示される。設定画面800においてユーザがボタン801を押下した場合、UI制御部300は、ユーザ情報設定画面900を操作部209に表示する。設定画面800においてユーザがボタン802を押下した場合、UI制御部300は、ロール設定画面1000を操作部209に表示する。

20

【0048】

(ユーザ情報設定画面900)

図9は、ユーザに関する情報を設定するための設定画面の一例を示す図である。図9に示すユーザ情報設定画面900は、設定処理部305によって操作部209に表示される。ユーザIDフィールド901は、ユーザを一意に識別するための識別子であるユーザIDを入力するためのテキストフィールドである。パスワードフィールド902は、ユーザIDフィールド901で設定されたユーザの認証に用いるパスワードを入力するためのテキストフィールドである。ロールフィールド903は、ユーザIDフィールド901で設定されたユーザのロールを選択するために用いられる。ロールフィールド903には、ロール情報テーブル1300に含まれるロール(ロール名1301)を選択項目として含む、ロールを選択するためのプルダウンメニューが表示される。

30

【0049】

キャンセルボタン904は、ユーザ情報設定画面900を用いたユーザ情報の設定をキャンセルするために用いられる。ユーザがキャンセルボタン904を押下した場合、UI制御部300は、設定画面800を操作部209に表示する。OKボタン905は、ユーザ情報設定画面900に対して入力された内容に基づく設定の実行を指示するために用いられる。ユーザがOKボタン905を押下した場合、設定処理部305は、ユーザ情報設定画面900に対して入力された内容を、ユーザ情報テーブル1200に保存する。

【0050】

なお、ユーザ情報設定画面900では、自動ログインユーザのユーザ情報のうち、ユーザID及びパスワードを設定することはできず、ロールの選択のみを行うことが可能である。

40

【0051】

(ロール設定画面1000)

図10は、ロールに関する情報を設定するための設定画面の一例を示す図である。図10に示すロール設定画面1000は、設定処理部305によって操作部209に表示される。ロール名フィールド1001は、ロールを一意に識別するための識別子を入力するためのテキストフィールドである。選択フィールド1002には、ロール名フィールド1001に入力された識別子に対応するロールについての、各機能の使用権限(使用の許可または禁止)を選択するためのラジオボタンが表示される。

50

【 0 0 5 2 】

キャンセルボタン 1 0 0 3 は、ロール設定画面 1 0 0 0 を用いたロール情報の設定をキャンセルするために用いられる。ユーザがキャンセルボタン 1 0 0 3 を押下した場合、UI 制御部 3 0 0 は、設定画面 8 0 0 を操作部 2 0 9 に表示する。OK ボタン 1 0 0 4 は、ロール設定画面 1 0 0 0 に対して入力された内容に基づく設定の実行を指示するために用いられる。ユーザが OK ボタン 1 0 0 4 を押下した場合、設定処理部 3 0 5 は、ロール設定画面 1 0 0 0 に対して入力された内容を、ロール情報テーブル 1 3 0 0 に保存する。

【 0 0 5 3 】

< 権限情報の修正処理 (ログイン時) >

本実施形態では、上述のようにユーザ認証によって各機能の使用可否を個別に制御する M F P 1 0 1 で、使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなることを防ぐために、以下の処理を実行する。

【 0 0 5 4 】

ユーザが自動ログインユーザとして M F P 1 0 1 にログインした状態で、いずれかのログインユーザとしてログインするためのユーザ認証を行うと、C P U 2 0 1 は、機能ごとに自動ログインユーザの使用権限とログインユーザの使用権限とを比較する。比較の結果、自動ログインユーザに使用が許可されている機能のうちでログインユーザに使用が許可されていない機能が存在すると、C P U 2 0 1 は、当該機能の使用をログインユーザに許可するよう、当該機能についてのログインユーザの使用権限を修正する。

【 0 0 5 5 】

本実施形態では、各機能についての自動ログインユーザ及びログインユーザの使用権限は、上述のロールによって管理されている。このため、M F P 1 0 1 は、機能の使用権限を修正する際には、各ロールに対して設定されている使用権限を修正すればよい。C P U 2 0 1 は、M F P 1 0 1 が有する機能についてログインユーザの使用権限を修正した場合、修正後の使用権限に従って、ログインユーザに使用が許可されている (即ち、ログインユーザが属するロールに使用が許可されている) 機能を使用可能にする。

【 0 0 5 6 】

次に、図 1 4 を参照して、このような処理の具体例について説明する。図 1 4 は、M F P 1 0 1 において C P U 2 0 1 によって実行される、ユーザのログイン時の、権限情報の修正処理の手順を示すフローチャートである。図 1 4 の各ステップの処理は、C P U 2 0 1 が、R O M 2 0 2 または H D D 2 0 4 に格納されたソフトウェア (図 3 に示す各機能ブロックに対応するソフトウェア) を R A M 2 0 3 に読み出して実行することによって、M F P 1 0 1 において実現される。即ち、各ステップの処理は、C P U 2 0 1 によって実行される。

【 0 0 5 7 】

M F P 1 0 1 が電源オフ状態から起動すると、C P U 2 0 1 (メニュー処理部 3 0 1) は、S 1 0 0 で、メインメニュー画面 4 0 0 を操作部 2 0 9 に表示する。次に、S 1 0 1 で、C P U 2 0 1 (メニュー処理部 3 0 1) は、操作部 2 0 9 を介して、表示したメインメニュー画面 4 0 0 上のボタン 4 0 1、4 0 2、4 0 3 のいずれかがユーザによって押下されるまで待機する。C P U 2 0 1 は、ボタン 4 0 1、4 0 2、4 0 3 のいずれかが押下されたか否かを判定し、押下されたと判定すると、処理を S 1 0 2 に進める。

【 0 0 5 8 】

S 1 0 2 で、C P U 2 0 1 (メニュー処理部 3 0 1) は、ユーザ D B 3 0 6 から、自動ログインユーザの、M F P 1 0 1 が有する機能ごとの使用権限を示す情報 (権限情報) を取得し、その後、S 1 0 3 に処理を進める。上述のように、ユーザ D B 3 0 6 には、図 1 2 及び図 1 3 に示すユーザ情報テーブル 1 2 0 0 及びロール情報テーブル 1 3 0 0 が格納されている。C P U 2 0 1 は、ユーザ情報テーブル 1 2 0 0 を参照して、ユーザ I D 1 2 0 1 が「自動ログイン」に対応するロール 1 2 0 3 を参照し、「ロール 1」を取得する。更に、C P U 2 0 1 は、ロール情報テーブル 1 3 0 0 を参照して、ロール名 1 3 0 1 が「ロール 1」であるロールについての権限情報を取得する。

【 0 0 5 9 】

次に、S 1 0 3 で、C P U 2 0 1 (メニュー処理部 3 0 1) は、S 1 0 1 で押下されたボタンに対応する機能 (アプリケーション) を使用するためにユーザ認証が必要か否かを判定する。ここで、C P U 2 0 1 は、S 1 0 2 で取得した権限情報に基づいて、自動ログインユーザに対して設定されている、当該機能の使用権限を確認することで、当該機能の使用が許可されているか否かを確認する。C P U 2 0 1 は、当該機能の使用が許可されおらず、当該機能をユーザが使用するためにユーザ認証が必要な場合には、処理を S 1 0 4 に進め、ユーザ認証が必要ない場合には、処理を S 1 1 1 に進める。これにより、C P U 2 0 1 は、ユーザ認証を行うことなく当該機能を使用可能にする。

【 0 0 6 0 】

例えば、S 1 0 1 で送信ボタン 4 0 2 がユーザによって押下された場合、C P U 2 0 1 は、S 1 0 2 で取得した、自動ログインユーザが属する「ロール 1」についての権限情報のうちで、送信機能の使用権限を確認する。図 1 3 に示すように、「ロール 1」についての送信機能の使用権限は「禁止」であるため、C P U 2 0 1 は、当該機能をユーザが使用するためにはユーザ認証が必要であると判断する。また、S 1 0 1 でコピーボタン 4 0 1 がユーザによって押下された場合、C P U 2 0 1 は、S 1 0 2 で取得した、自動ログインユーザが属する「ロール 1」についての権限情報のうちで、コピー機能の使用権限を確認する。図 1 3 に示すように、「ロール 1」についてのコピー機能の使用権限は「許可」であるため、C P U 2 0 1 は、当該機能をユーザが使用するためにはユーザ認証は不要であると判断する。

【 0 0 6 1 】

S 1 0 3 から S 1 0 4 に処理を進めた場合、S 1 0 4 で、C P U 2 0 1 (認証処理部 3 0 4) は、認証画面 7 0 0 を操作部 2 0 9 に表示する。更に、S 1 0 5 で、C P U 2 0 1 (認証処理部 3 0 4) は、操作部 2 0 9 を介して、ユーザによってログインボタン 7 0 4 を押下されたか、キャンセルボタン 7 0 3 が押下されたかを判定する。ログインボタン 7 0 4 が押下された場合には、C P U 2 0 1 は処理を S 1 0 6 に進める。一方、キャンセルボタン 7 0 3 が押下された場合には、C P U 2 0 1 は処理を S 1 0 0 に戻し、再びメインメニュー画面 4 0 0 を操作部 2 0 9 に表示する。

【 0 0 6 2 】

S 1 0 6 で、C P U 2 0 1 (認証処理部 3 0 4) は、認証画面 7 0 0 を介して入力されたユーザ名及びパスワードに基づいてユーザ認証を実行し、認証が成功したか否かを判定する。ここで、C P U 2 0 1 は、操作部 2 0 9 に表示した認証画面 7 0 0 のユーザ名入力フィールド 7 0 1 及びパスワード入力フィールド 7 0 2 に入力された情報と、ユーザ情報テーブル 1 2 0 0 に含まれる情報とを照合することによって、ユーザ認証を実行する。認証が成功した場合には、処理を S 1 0 7 に進め、認証が失敗した場合には、処理を S 1 0 8 に進める。このようにして、C P U 2 0 1 は、自動ログインユーザ (第 1 のユーザ) としてユーザが M F P 1 0 1 にログインした状態において、別のユーザ (第 2 のユーザ) としてユーザが M F P 1 0 1 にログインするためのユーザ認証を実行する。

【 0 0 6 3 】

なお、S 1 0 6 で、C P U 2 0 1 は、ユーザ認証が成功したユーザが属するロールに、S 1 0 1 で押下されたボタンに対応する機能の使用が許可されていない (禁止されている) 場合には、ユーザ認証が失敗したものとみなして、処理を S 1 0 8 に進めてもよい。この場合、C P U 2 0 1 は、ユーザ情報テーブル 1 2 0 0 を参照して、ユーザ認証が成功したユーザのユーザ ID 1 2 0 1 に対応するロール 1 2 0 3 を確認すればよい。更に、C P U 2 0 1 は、ロール情報テーブル 1 3 0 0 を参照して、確認したロールについての権限情報を確認すればよい。

【 0 0 6 4 】

S 1 0 8 で、C P U 2 0 1 (認証処理部 3 0 4) は、ユーザ認証に失敗したことを示すエラー画面を操作部 2 0 9 に表示することで、認証が失敗したことをユーザに通知する。その後、C P U 2 0 1 (メニュー処理部 3 0 1) は処理を S 1 0 0 に戻し、再びにメイン

10

20

30

40

50

メニュー画面 4 0 0 を操作部 2 0 9 に表示する。

【 0 0 6 5 】

一方、S 1 0 7 で、C P U 2 0 1 (認証処理部 3 0 4) は、ユーザ認証が成功したユーザ (ログインユーザ) の権限情報を、ユーザ D B 3 0 6 から取得する。次に、S 1 0 9 で、C P U 2 0 1 は、M F P 1 0 1 が有する複数の機能のそれぞれについて、自動ログインユーザの使用権限とログインユーザの使用権限とを比較する。更に C P U 2 0 1 は、自動ログインユーザに使用が許可されている機能のうちで、ログインユーザに使用が許可されていない機能が存在するか否か (即ち、ログインユーザの使用権限に、自動ログインユーザの使用権限よりも低いものが存在するか否か) を判定する。

【 0 0 6 6 】

例えば、S 1 0 6 で、図 1 2 に示す「ユーザ 1」としてユーザ認証に成功した (即ち、ログインユーザが「ユーザ 1」である) 場合を想定する。この場合、ユーザ情報テーブル 1 2 0 0 及びロール情報テーブル 1 3 0 0 から、自動ログインユーザが属するロールは「ロール 1」であり、「ロール 1」についてはコピー機能の使用が許可されている。一方、「ユーザ 1」が属するロールは「ロール 2」であり、「ロール 2」についてはコピー機能の使用が禁止されている。このため、S 1 0 9 では、C P U 2 0 1 が、自動ログインユーザに使用が許可されている機能のうちでログインユーザ (「ユーザ 1」) に使用が許可されていない機能が存在すると判定する結果となる。即ち、ログインユーザの使用権限には、自動ログインユーザの使用権限よりも低いものが存在する。

【 0 0 6 7 】

S 1 0 9 における判定の結果、ログインユーザの使用権限に、自動ログインユーザの使用権限よりも低いものが存在しない場合には処理を S 1 1 1 に進め、存在する場合には処理を S 1 1 0 に進める。S 1 1 0 で、C P U 2 0 1 (認証処理部 3 0 4) は、自動ログインユーザに使用が許可されており、ログインユーザに使用が許可されていない機能の使用を、当該ログインユーザに使用が許可するよう、当該ログインユーザの使用権限を修正 (変更) する。例えば、上述の例の場合、C P U 2 0 1 は、ロール情報テーブル 1 3 0 0 に保存されている、「ロール 2」についてのコピー機能の使用権限を、「禁止」から「許可」に変更する。その後、C P U 2 0 1 は処理を S 1 1 1 に進める。

【 0 0 6 8 】

S 1 0 3、S 1 0 9 または S 1 1 0 から S 1 1 1 に処理を進めた場合、S 1 1 1 で、C P U 2 0 1 (メニュー処理部 3 0 1) は、S 1 0 1 で押下されたボタンに対応する機能を提供するための画面を操作部 2 0 9 に表示する。当該画面は、例えば、コピー画面 5 0 0、送信画面 6 0 0 または設定画面 8 0 0 である。このようにして、C P U 2 0 1 は、S 1 1 0 でログインユーザの使用権限を変更した場合には、変更後の使用権限に従って、ログインユーザに使用が許可されている機能を使用可能にする。以上により、C P U 2 0 1 は、図 1 4 に示す手順に従った処理を終了し、操作部 2 0 9 に表示した画面を介してユーザによって入力される指示に従った処理を行う。

【 0 0 6 9 】

以上のように、本実施形態では、M F P 1 0 1 は、ユーザがログインユーザとしてログインする際に、機能ごとに、自動ログインユーザよりも低い使用権限がログインユーザの使用権限に存在しなくなるよう、ログインユーザの使用権限の設定を修正する。これにより、使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなることを防ぐことが可能となり、ユーザにとっての利便性を向上させることが可能となる。

【 0 0 7 0 】

< 権限情報の修正処理 (ユーザまたはロール情報の設定時) >

使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなる状態が生じることを防ぐには、ユーザまたはロール情報の設定が行われた際に、未然にそのような状態が生じることを防ぐことも可能である。以下では、図 1 5 を参照して、そのような処理の具体例について説明する。図 1 5 は、M F P 1 0 1 において C P

10

20

30

40

50

U 2 0 1によって実行される、ユーザまたはロール情報の設定時の、権限情報の修正処理の手順を示すフローチャートである。図 1 5 の各ステップの処理は、C P U 2 0 1 が、R O M 2 0 2 または H D D 2 0 4 に格納されたソフトウェア（図 3 に示す各機能ブロックに対応するソフトウェア）を R A M 2 0 3 に読み出して実行することによって、M F P 1 0 1 において実現される。即ち、各ステップの処理は、C P U 2 0 1 によって実行される。

【 0 0 7 1 】

M F P 1 0 1 が電源オフ状態から起動した状態において、ユーザが、メインメニュー画面 4 0 0 のボタン 4 0 3 を押下し、設定画面 8 0 0 のボタン 8 0 2 を押下すると、C P U 2 0 1 は、S 2 0 0 の処理を実行する。S 2 0 0 で、C P U 2 0 1（設定処理部 3 0 5）は、ユーザ情報設定画面 9 0 0 を操作部 2 0 9 に表示する。次に、S 2 0 1 で、C P U 2 0 1（設定処理部 3 0 5）は、操作部 2 0 9 を介して、表示したユーザ情報設定画面 9 0 0 上の O K ボタン 9 0 5 がユーザによって押下されるまで待機する。C P U 2 0 1 は、O K ボタン 9 0 5 が押下されたか否かを判定することで、ユーザ（管理者）によって、ユーザ情報の設定が実行されたか否かを判定する。O K ボタン 9 0 5 が押下されると、C P U 2 0 1 は、処理を S 2 0 2 に進める。

10

【 0 0 7 2 】

S 2 0 2 で、C P U 2 0 1（設定処理部 3 0 5）は、M F P 1 0 1 の機能についての各ユーザの使用権限が、ユーザの指示に従って変更されたか否かを確認する。例えば、C P U 2 0 1 は、ユーザ情報設定画面 9 0 0 内のロールフィールド 9 0 3 の設定が変更されたか否かを確認する。なお、C P U 2 0 1 は、S 2 0 0 で、ロール設定画面 1 0 0 0 を表示するとともに、S 2 0 2 で、ロール設定画面 1 0 0 0 内でいずれかのロールについての機能の使用権限が変更されたか否かを確認してもよい。C P U 2 0 1 は、M F P 1 0 1 の機能についての各ユーザの使用権限が変更されたと判定した場合、処理を S 2 0 3 に進め、変更されていないと判定した場合、処理を S 2 0 9 に進める。

20

【 0 0 7 3 】

S 2 0 3 で、C P U 2 0 1（設定処理部 3 0 5）は、S 1 0 2 と同様、ユーザ D B 3 0 6 から、自動ログインユーザの、M F P 1 0 1 が有する機能ごとの使用権限を示す情報（権限情報）を取得する。更に、S 2 0 4 で、C P U 2 0 1（設定処理部 3 0 5）は、ユーザ D B 3 0 6 に登録されている、自動ログインユーザ以外の各ユーザの、M F P 1 0 1 が有する機能ごとの権限情報を、ユーザ D B 3 0 6 から取得する。なお、ここではユーザ D B 3 0 6 に登録されている、自動ログインユーザ以外の、ユーザ認証を必要とする全てのユーザの権限情報を取得すればよい。

30

【 0 0 7 4 】

次に、S 2 0 5 で、C P U 2 0 1（設定処理部 3 0 5）は、M F P 1 0 1 が有する複数の機能のそれぞれについて、自動ログインユーザの使用権限と、登録されている各ユーザの使用権限とを比較する。更に C P U 2 0 1 は、自動ログインユーザに使用が許可されている機能のうちで、登録されている各ユーザに使用が許可されていない機能が存在するか否か（即ち、登録されている各ユーザの使用権限に、自動ログインユーザの使用権限よりも低いものが存在するか否か）を判定する。S 2 0 5 における判定の結果、登録されている各ユーザの使用権限に、自動ログインユーザの使用権限よりも低いものが存在しない場合には処理を S 2 0 9 に進め、存在する場合には処理を S 2 0 6 に進める。

40

【 0 0 7 5 】

S 2 0 6 で、C P U 2 0 1（設定処理部 3 0 5）は、図 1 1 に示す、権限修正確認画面 1 1 0 0 を操作部 2 0 9 に表示する。これにより、C P U 2 0 1 は、M F P 1 0 1 のいずれかの機能について、自動ログインユーザよりも低い使用権限を有する、登録されたユーザの使用権限を修正するか否かを、M F P 1 0 1 を操作中のユーザに確認する。更に、S 2 0 7 で、C P U 2 0 1 は、ユーザによって権限修正確認画面 1 1 0 0 上の Y E S ボタン 1 1 0 3 が押下されたか、N O ボタン 1 1 0 2 が押下されたかを判定することで、登録されたユーザの使用権限を修正するか否かを判定する。C P U 2 0 1 は、Y E S ボタン 1 1 0 3 が押下されたと判定した場合、処理を S 2 0 8 に進め、N O ボタン 1 1 0 2 が押下さ

50

れたと判定した場合、処理をＳ２０９に進める。

【００７６】

Ｓ２０８で、ＣＰＵ２０１（設定処理部３０５）は、自動ログインユーザに使用が許可されており、登録されたユーザに使用が許可されていない機能の使用を、当該登録されたユーザに使用が許可するよう、当該登録されたユーザの使用権限を修正（変更）する。その後、処理をＳ２０９に進める。

【００７７】

Ｓ２０９で、ＣＰＵ２０１（設定処理部３０５）は、ユーザ情報設定画面９００（またはロール設定画面１０００）を用いて設定されたユーザ情報（またはロール情報）を、ユーザＤＢ３０６へ保存して、処理を終了する。

10

【００７８】

なお、ユーザまたはロール情報の設定が行われた際に、ユーザに対する確認を行うことなく必要に応じて自動的に権限情報を修正すべきことが予め設定されている場合には、Ｓ２０６及びＳ２０７の確認処理を省略してもよい。

【００７９】

以上のように、本実施形態では、ＭＦＰ１０１は、ユーザまたはロール情報の設定が行われた際に、自動ログインユーザよりも低い使用権限が、登録されているユーザの使用権限に存在しなくなるよう、登録されているユーザの使用権限の設定を修正する。これにより、ＭＦＰ１０１において、使用権限の設定によってユーザ認証前の状態で使用可能な機能がユーザ認証後に使用できなくなる状態が生じることを未然に防ぐことができる。

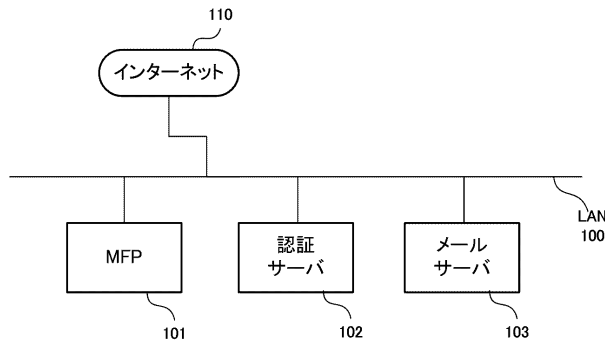
20

【００８０】

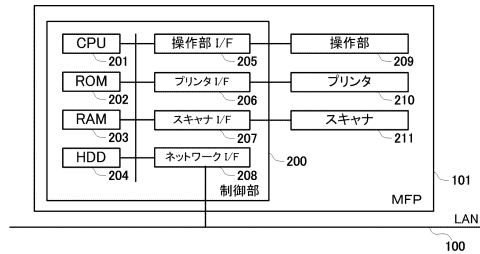
〔その他の実施形態〕

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワークまたは各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

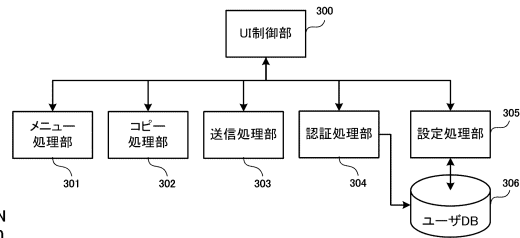
【図 1】



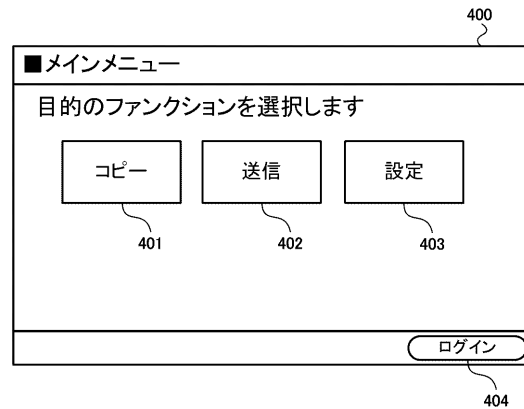
【図 2】



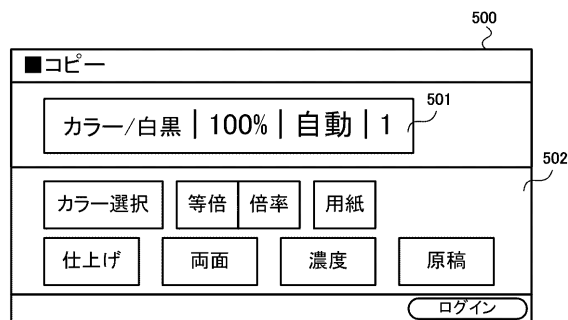
【図 3】



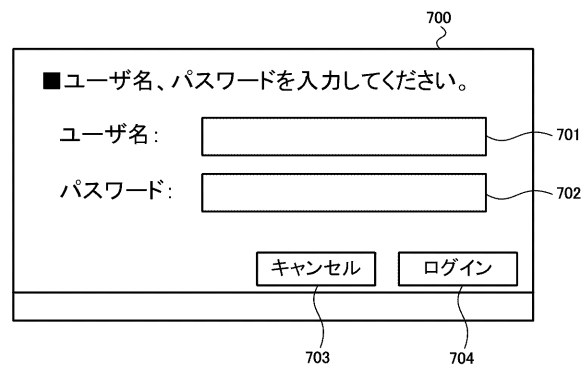
【図 4】



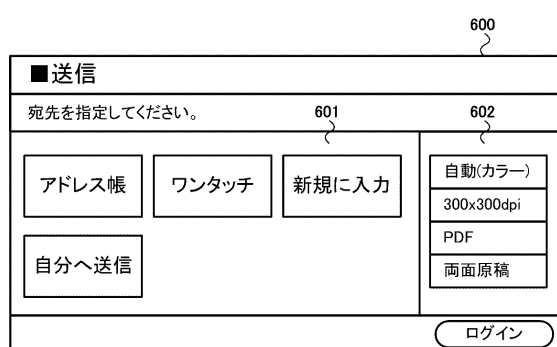
【図 5】



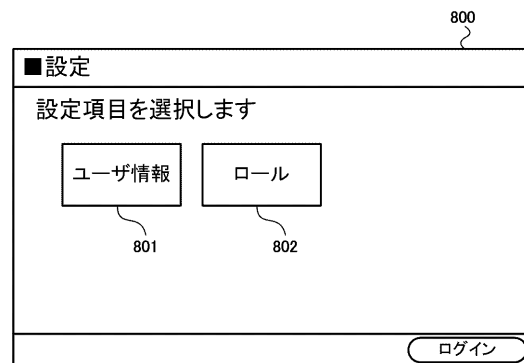
【図 7】



【図 6】



【図 8】



【図 9】

900

■設定 > ユーザ情報

901 ユーザ情報を設定します

902

903

ユーザID	パスワード	ロール
自動ログイン		ロール選択▼
ユーザ1	****	ロール1
ユーザ2	****	ロール2
		ロール3

904

905

キャンセル OK ログイン

【図 10】

1000

■設定 > ロール

1001

ロールを設定します

ロール名:

1002

コピー: ☒ 許可 ☐ 禁止

送信: ☐ 許可 ☒ 禁止

保存: ☒ 許可 ☐ 禁止

設定: ☒ 許可 ☐ 禁止

1003

キャンセル

1004

OK

ログイン

【図 11】

1100

■設定

1101

自動ログインユーザよりも
権限が低いユーザが存在します。

そのユーザの権限を修正しますか？

1102

1103

NO YES

【図 12】

1200

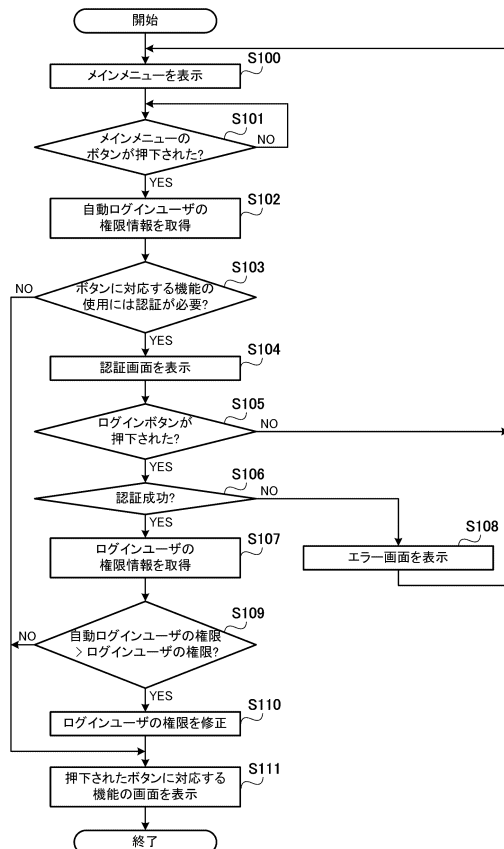
1201	1202	1203
ユーザID	パスワード	ロール
自動ログイン		ロール1
ユーザ1	****	ロール2
ユーザ2	****	ロール3

【図 13】

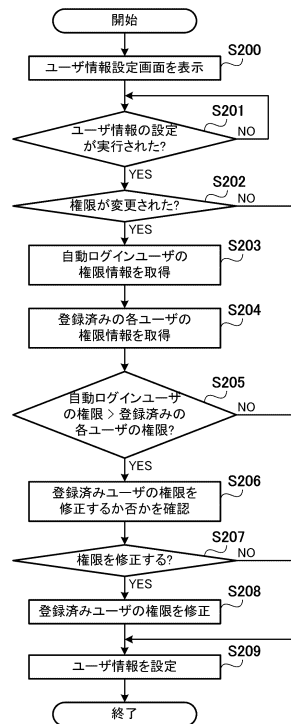
1300

1301	1302	1303	1304
ロール名	コピー	送信	設定
ロール1	許可	禁止	禁止
ロール2	禁止	許可	許可
ロール3	許可	許可	許可

【図 14】



【図 15】



フロントページの続き

(72)発明者 佐藤 圭
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 宮司 卓佳

(56)参考文献 特開2010-114504(JP,A)
特開2006-085641(JP,A)
特開2001-331451(JP,A)
米国特許出願公開第2005/0278546(US,A1)
米国特許出願公開第2012/0167201(US,A1)

(58)調査した分野(Int.Cl., DB名)
G06F 21/00 - 21/88
B41J 29/00
B41J 29/38
G06F 3/12