

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4821292号  
(P4821292)

(45) 発行日 平成23年11月24日(2011.11.24)

(24) 登録日 平成23年9月16日(2011.9.16)

(51) Int. Cl.	F I		
<b>G06F 21/20</b> (2006.01)	G06F 15/00	330D	
<b>G09C 1/00</b> (2006.01)	G09C 1/00	640E	
<b>G06F 3/12</b> (2006.01)	G06F 3/12	K	
<b>B41J 29/38</b> (2006.01)	B41J 29/38	Z	
<b>B41J 29/00</b> (2006.01)	B41J 29/00	Z	
請求項の数 7 (全 32 頁) 最終頁に続く			

(21) 出願番号 特願2005-349265 (P2005-349265)  
 (22) 出願日 平成17年12月2日(2005.12.2)  
 (65) 公開番号 特開2007-156698 (P2007-156698A)  
 (43) 公開日 平成19年6月21日(2007.6.21)  
 審査請求日 平成20年11月20日(2008.11.20)

(73) 特許権者 000005496  
 富士ゼロックス株式会社  
 東京都港区赤坂九丁目7番3号  
 (74) 代理人 100137752  
 弁理士 亀井 岳行  
 (72) 発明者 上野 高史  
 神奈川県横浜市保土ヶ谷区神戸町134番  
 地 横浜ビジネスパークイーストタワー富  
 士ゼロックス株式会社内  
 審査官 小林 秀和

最終頁に続く

(54) 【発明の名称】 認証システム、認証装置および認証プログラム

(57) 【特許請求の範囲】

【請求項1】

画像形成装置の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段と、

前記利用者の認証を行う認証手段と、

利用者が利用できる前記画像形成装置の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段と、

認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する追加権限機能入力判別手段と、

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像を情報表示画面に表示する権限変更認証画像表示手段と、

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段と、

前記権限変更画像に入力された入力情報と前記権限変更認証情報記憶手段に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段と、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段と、

を備えたことを特徴とする認証システム。

【請求項 2】

前記認証を行うための認証画像を表示する認証画像表示手段と、前記認証画像で入力された入力認証情報を送信する入力認証情報送信手段と、認証の可否の結果を通知する認証可否情報を受信する認証可否情報受信手段とを有する画像形成装置と、

利用者が機能を利用する複数の前記画像形成装置に対してネットワークで接続された情報処理装置であって、前記入力認証情報送信手段により送信された入力認証情報を受信する入力認証情報受信手段と、前記認証情報記憶手段と、前記認証手段と、前記認証手段による認証の可否の結果を通知する認証可否情報を前記画像形成装置に送信する認証可否情報送信手段と、を有する前記情報処理装置と、

を備えたことを特徴とする請求項 1 に記載の認証システム。

【請求項 3】

利用者の利用を終了したことを通知する利用終了情報を前記情報処理装置に送信する利用終了情報送信手段、を有する前記画像形成装置と、

前記画像形成装置を利用中の利用者を記憶する利用者記憶手段と、前記入力認証情報に基づいて前記画像形成装置を利用中の利用者として前記利用者記憶手段に登録すると共に、受信した利用終了情報に基づいて前記利用者記憶手段に記憶された利用者を削除する利用者登録変更手段と、を有する前記情報処理装置と、

を備えたことを特徴とする請求項 2 に記載の認証システム。

【請求項 4】

前記入力認証情報により特定される利用者が、前記利用者記憶手段に記憶されているか否かを判別する利用者重複判別手段と、

前記入力認証情報により特定される利用者が前記利用者記憶手段に記憶されている場合に、利用中と記憶されている画像形成装置における認証を強制的に解除する強制認証解除情報を前記画像形成装置に送信する強制認証解除情報送信手段と、

を備えたことを特徴とする請求項 3 に記載の認証システム。

【請求項 5】

複数のサブネットワークを含むネットワークに接続された前記画像形成装置及び前記情報処理装置であって、

前記入力認証情報により特定される利用者が前記利用者記憶手段に記憶されている場合に、前記利用中と記憶されている画像形成装置が接続されているサブネットワークと、前記入力認証情報により認証を行おうとしている画像形成装置が接続されているサブネットワークとが一致するか否かを判別するサブネットワーク一致判別手段と、

前記サブネットワークが一致しない場合に、利用中と記憶されている画像形成装置における認証を強制的に解除する強制認証解除情報を前記画像形成装置に送信する前記強制認証解除情報送信手段と、

を備えたことを特徴とする請求項 4 に記載の認証システム。

【請求項 6】

画像形成装置の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段と、

前記利用者の認証を行う認証手段と、

利用者が利用できる前記画像形成装置の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置の画像形成の機能を特定する標準権限

10

20

30

40

50

と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段と、

認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する追加権限機能入力判別手段と、

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像を情報表示画面に表示する権限変更認証画像表示手段と、

10

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段と、

前記権限変更画像に入力された入力情報と前記権限変更認証情報記憶手段に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段と、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段と、

20

を備えたことを特徴とする認証装置。

【請求項 7】

コンピュータを、

画像形成装置の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段、

前記利用者の認証を行う認証手段、

利用者が利用できる前記画像形成装置の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段 認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する追加権限機能入力判別手段、

30

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像を情報表示画面に表示する権限変更認証画像表示手段、

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段、

40

前記権限変更画像に入力された入力情報と前記権限変更認証情報記憶手段に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段

として機能させるための認証プログラム。

【発明の詳細な説明】

【技術分野】

50

## 【 0 0 0 1 】

本発明は、複数の利用者が利用する際に利用者の認証を行う認証装置、認証システムおよび認証プログラムに関し、特に、複数の利用者が利用する際に利用者毎に利用権限が設定される認証システム、認証装置および認証プログラムに関する。

前記本発明の認証装置は、プリンタ、FAX、複写機等の画像形成装置や、パーソナルコンピュータやワークステーション、サーバ等の情報処理装置等の電子機器に好適に適用可能である。

## 【背景技術】

## 【 0 0 0 2 】

複数の利用者（ユーザ）が利用する画像形成装置やワークステーション等では、機器の動作設定等を各利用者が勝手に変更することを防止したり、特定の機能の使用を制限したりするために、認証（ログイン）時に、管理者や一般ユーザ、ゲストユーザ等に異なる利用権限を付与して、利用できる機能を制限することが行われている。

他にも、各機能の動作を制御する制御プログラム（いわゆる、ドライバ）について、利用者が利用可能な機能に応じて組み込む制御プログラムを変更する技術（例えば、特許文献1等参照）もある。

## 【 0 0 0 3 】

【特許文献1】特開2004-220532号公報

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【 0 0 0 4 】

（従来技術の問題点）

前記従来技術では、認証が行われた状態で、利用者が中座等して機器から離れた場合、利用権限のない第三者が、中座等した利用者の利用権限の範囲で自由に使用することが可能になってしまう。特に、利用権限の大きな管理者として認証がされた状態で第三者が自由に操作すると、機器が悪用され、機器が動作しなくなったり、機密情報が漏洩する恐れもある。

## 【 0 0 0 5 】

本発明は、前述の事情に鑑み、次の記載内容（001）を技術的課題とする。

（001）認証された状態で利用権限のない人物による使用を制限すること。

## 【課題を解決するための手段】

## 【 0 0 0 6 】

（本発明）

次に、前記課題を解決した本発明を説明するが、本発明の要素には、後述の実施の形態の具体例（実施例）の要素との対応を容易にするため、実施例の要素の符号をカッコで囲んだものを付記する。また、本発明を後述の実施例の符号と対応させて説明する理由は、本発明の理解を容易にするためであり、本発明の範囲を実施例に限定するためではない。

## 【 0 0 0 7 】

（第1発明）

前記技術的課題を解決するために、第1発明の認証システム（S）は、  
画像形成装置（Pr1）の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段（C4D，C31B）と、

前記利用者の認証を行う認証手段（C4，C31）と、

利用者が利用できる画像形成装置（Pr1）の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置（Pr1）の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置（Pr1）の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段（C7）と、

認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否か

10

20

30

40

50

を判別する追加権限機能入力判別手段（C 8 B）と、

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像（6 1）を情報表示画面（U I 1）に表示する権限変更認証画像表示手段（C 9 B）と、

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段（C 9 C）と、

前記権限変更画像（6 1）に入力された入力情報と前記権限変更認証情報記憶手段（C 9 C）に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段（C 9）と、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段（C 9）と、

を備えたことを特徴とする。

【0008】

（第1発明の作用）

前記構成要件を備えた第1発明の認証システム（S）では、認証情報記憶手段（C 4 D , C 3 1 B）は、画像形成装置（P r 1）の利用者の認証を行うための認証情報を利用者毎に記憶する。認証手段（C 4 , C 3 1）は、前記利用者の認証を行う。利用権限情報記憶手段（C 7）は、利用者が利用できる画像形成装置（P r 1）の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置（P r 1）の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置（P r 1）の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する。追加権限機能入力判別手段（C 8 B）は、認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する。

【0009】

権限変更認証画像表示手段（C 9 B）は、前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像（6 1）を情報表示画面（U I 1）に表示する。権限変更認証情報記憶手段（C 9 C）は、前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する。権限変更認証手段（C 9）は、前記権限変更画像（6 1）に入力された入力情報と前記権限変更認証情報記憶手段（C 9 C）に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う。

【0010】

したがって、第1発明の認証システム（S）では、追加権限機能に含まれる機能を利用する場合に権限変更認証が必要になるので、認証された利用者が中座等した場合に、利用権限のない第三者が使用しようとしても、標準権限機能に含まれる機能しか利用できず、追加権限機能に含まれる機能の利用が制限される。この結果、利用権限のない第三者が利用できる機能の範囲を制限することができ、追加権限機能に含まれる機能を悪用されることを抑制できる。したがって、第三者の悪用により、正常に動作しなくなったり、機密情報が漏洩することを減らすことができる。

【0011】

また、前記構成要件を備えた第1発明では、前記権限変更認証手段（C 9）は、追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の

10

20

30

40

50

機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力  
がされた場合に、標準権限に自動的に権限変更を行う。したがって、標準権限への権限変  
更は権限変更認証が必要ないので、権限変更時に必ず権限変更認証を行う場合に比べ入力  
操作を減らすことができ、操作性を高めることができる。

【 0 0 1 2 】

( 第 1 発明の形態 1 )

第 1 発明の形態 1 は、前記第 1 発明において、

前記認証を行うための認証画像 ( 1 1 ) を表示する認証画像表示手段 ( C 4 A ) と、前  
記認証画像 ( 1 1 ) で入力された入力認証情報を送信する入力認証情報送信手段 ( C 4 E  
) と、認証の可否の結果を通知する認証可否情報を受信する認証可否情報受信手段 ( C 4  
F ) とを有する画像形成装置 ( P r 1 ) と、

利用者が機能を利用する複数の前記画像形成装置 ( P r 1 ) に対してネットワーク ( N  
) で接続された情報処理装置 ( S b ) であって、前記入力認証情報送信手段 ( C 4 E ) に  
より送信された入力認証情報を受信する入力認証情報受信手段 ( C 3 1 A ) と、前記認証  
情報記憶手段 ( 3 1 B ) と、前記認証手段 ( C 3 1 ) と、前記認証手段 ( C 3 1 ) による  
認証の可否の結果を通知する認証可否情報を前記画像形成装置 ( P r 1 ) に送信する認証  
可否情報送信手段 ( C 3 1 F ) と、を有する前記情報処理装置 ( S b ) と、

を備えたことを特徴とする。

【 0 0 1 3 】

( 第 1 発明の形態 1 の作用 )

前記構成要件を備えた第 1 発明の形態 1 の認証システム ( S ) は、利用者が機能を利用  
する複数の前記画像形成装置 ( P r 1 ) に対してネットワーク ( N ) で接続された情報処  
理装置 ( S b ) を有する。画像形成装置 ( P r 1 ) の入力認証情報送信手段 ( C 4 E ) は  
、前記認証を行うための認証画像 ( 1 1 ) を表示する認証画像表示手段 ( C 4 A ) と、前  
記認証画像 ( 1 1 ) で入力された入力認証情報を送信する。情報処理装置 ( S b ) の入力  
認証情報受信手段 ( C 3 1 A ) は、前記入力認証情報送信手段 ( C 4 E ) により送信され  
た入力認証情報を受信する。前記認証情報記憶手段 ( C 3 1 B ) と、前記認証手段 ( C 3  
1 ) とを有する情報処理装置 ( S b ) の認証可否情報送信手段 ( C 3 1 F ) は、前記認証  
手段 ( C 3 1 ) による認証の可否の結果を通知する認証可否情報を前記画像形成装置 ( P  
r 1 ) に送信する。画像形成装置 ( P r 1 ) の認証可否情報受信手段 ( C 4 F ) は、認証  
の可否の結果を通知する認証可否情報を受信する。したがって、画像形成装置 ( P r 1 )  
の利用者の認証を情報処理装置 ( S b ) で行うことができ、画像形成装置 ( P r 1 ) の認  
証情報を情報処理装置 ( S b ) で管理することができる。

【 0 0 1 4 】

( 第 1 発明の形態 2 )

第 1 発明の形態 2 は、前記第 1 発明の形態 1 において、

利用者の利用を終了したことを通知する利用終了情報を前記情報処理装置 ( S b ) に送  
信する利用終了情報送信手段 ( C 2 2 ) 、を有する前記画像形成装置 ( P r 1 ) と、

前記画像形成装置 ( P r 1 ) を利用中の利用者を記憶する利用者記憶手段 ( C 3 2 A )  
と、前記入力認証情報に基づいて前記画像形成装置 ( P r 1 ) を利用中の利用者として前  
記利用者記憶手段 ( C 3 2 A ) に登録すると共に、受信した利用終了情報に基づいて前記  
利用者記憶手段 ( C 3 2 A ) に記憶された利用者を削除する利用者登録変更手段 ( C 3 2  
D ) と、を有する前記情報処理装置 ( S b ) と、

を備えたことを特徴とする。

【 0 0 1 5 】

( 第 1 発明の形態 2 の作用 )

前記構成要件を備えた第 1 発明の形態 2 では、情報処理装置 ( S b ) の利用者記憶手段  
( C 3 2 A ) は、前記画像形成装置 ( P r 1 ) を利用中の利用者を記憶する。前記画像形  
成装置 ( P r 1 ) の利用終了情報送信手段 ( C 2 2 ) は、利用者の利用を終了したことを  
通知する利用終了情報を前記情報処理装置 ( S b ) に送信する。利用者登録変更手段 ( C

10

20

30

40

50

32D)は、前記入力認証情報に基づいて前記画像形成装置(P r 1)を利用中の利用者として前記利用者記憶手段(C 3 2 A)に登録すると共に、受信した利用終了情報に基づいて前記利用者記憶手段(C 3 2 A)に記憶された利用者を削除する。したがって、第1発明の形態2では、画像形成装置(P r 1)毎に利用中の利用者を管理することができる。

【0016】

(第1発明の形態3)

第1発明の形態3は、前記第1発明の形態2において、

前記入力認証情報により特定される利用者が、前記利用者記憶手段(C 3 2 A)に記憶されているか否かを判別する利用者重複判別手段(C 3 2 B)と、

10

前記入力認証情報により特定される利用者が前記利用者記憶手段(C 3 2 A)に記憶されている場合に、利用中と記憶されている画像形成装置(P r 1)における認証を強制的に解除する強制認証解除情報を前記画像形成装置(P r 1)に送信する強制認証解除情報送信手段(C 2 1)と、

を備えたことを特徴とする。

【0017】

(第1発明の形態3の作用)

前記構成要件を備えた第1発明の形態3では、利用者重複判別手段(C 3 2 B)は、前記入力認証情報により特定される利用者が、前記利用者記憶手段(C 3 2 A)に記憶されているか否かを判別する。強制認証解除情報送信手段(C 2 1)は、前記入力認証情報により特定される利用者が前記利用者記憶手段(C 3 2 A)に記憶されている場合に、利用中と記憶されている画像形成装置(P r 1)における認証を強制的に解除する強制認証解除情報を前記画像形成装置(P r 1)に送信する。したがって、第1発明の形態3では、複数の画像形成装置(P r 1)を同じ利用者が重複して利用することを防止でき、利用者が一方の画像形成装置(P r 1)の利用を終了する処理を忘れた状態で、他方の画像形成装置(P r 1)を利用しようとした場合に、終了し忘れた一方の画像形成装置(P r 1)の認証を解除することができる。この結果、終了し忘れた一方の画像形成装置(P r 1)を利用権限のない第三者が利用することを防止できる。

20

【0018】

(第1発明の形態4)

第1発明の形態4は、前記第1発明の形態3において、

複数のサブネットワーク(3, 4)を含むネットワーク(N)に接続された前記画像形成装置(P r 1)及び前記情報処理装置(S b)であって、

30

前記入力認証情報により特定される利用者が前記利用者記憶手段(C 3 2 A)に記憶されている場合に、前記利用中と記憶されている画像形成装置(P r 1)が接続されているサブネットワーク(3, 4)と、前記入力認証情報により認証を行おうとしている画像形成装置(P r 1)が接続されているサブネットワーク(3, 4)とが一致するか否かを判別するサブネットワーク一致判別手段(C 3 2 B 1)と、

前記サブネットワーク(3, 4)が一致しない場合に、利用中と記憶されている画像形成装置(P r 1)における認証を強制的に解除する強制認証解除情報を前記画像形成装置(P r 1)に送信する前記強制認証解除情報送信手段(C 2 1)と、

40

を備えたことを特徴とする。

【0019】

(第1発明の形態4の作用)

前記構成要件を備えた第1発明の形態4では、前記画像形成装置(P r 1)及び前記情報処理装置(S b)は、複数のサブネットワーク(3, 4)を含むネットワーク(N)に接続されている。サブネットワーク一致判別手段(C 3 2 B 1)は、入力認証情報により特定される利用者が前記利用者記憶手段(C 3 2 A)に記憶されている場合に、前記利用中と記憶されている画像形成装置(P r 1)が接続されているサブネットワーク(3, 4)と、前記入力認証情報により認証を行おうとしている画像形成装置(P r 1)が接続さ

50

れているサブネットワーク(3,4)とが一致するか否かを判別する。前記強制認証解除情報送信手段(C21)は、前記サブネットワーク(3,4)が一致しない場合に、利用中と記憶されている画像形成装置(Pr1)における認証を強制的に解除する強制認証解除情報を前記画像形成装置(Pr1)に送信する。したがって、第1発明の形態4では、サブネットワーク(3,4)が一致する場合には、複数の画像形成装置(Pr1)を同一の利用者が利用することができるので、1台の画像形成装置(Pr1)しか利用できない場合に比べ、柔軟な運用ができる。

【0021】

(第2発明)

前記技術的課題を解決するために、第2発明の認証装置(Pr1)は、  
画像形成装置(Pr1)の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段(C4D, C31B)と、

前記利用者の認証を行う認証手段(C4, C31)と、

利用者が利用できる画像形成装置(Pr1)の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置(Pr1)の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置(Pr1)の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段(C7)と、

認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する追加権限機能入力判別手段(C8B)と、

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像(61)を情報表示画面(UI1)に表示する権限変更認証画像表示手段(C9B)と、

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段(C9C)と、

前記権限変更画像(61)に入力された入力情報と前記権限変更認証情報記憶手段(C9C)に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段(C9)と、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段(C9)と、

を備えたことを特徴とする。

【0022】

(第2発明の作用)

前記構成要件を備えた第2発明の認証装置(Pr1)では、認証情報記憶手段(C4D, C31B)は、画像形成装置(Pr1)の利用者の認証を行うための認証情報を利用者毎に記憶する。認証手段(C4, C31)は、前記利用者の認証を行う。利用権限情報記憶手段(C7)は、利用者が利用できる画像形成装置(Pr1)の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置(Pr1)の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置(Pr1)の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する。追加権限機能入力判別手段(C8B)は、認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する。

【0023】

10

20

30

40

50

権限変更認証画像表示手段（C9B）は、前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像（61）を情報表示画面（UI1）に表示する。権限変更認証情報記憶手段（C9C）は、前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する。権限変更認証手段（C9）は、前記権限変更画像（61）に入力された入力情報と前記権限変更認証情報記憶手段（C9C）に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う。

【0024】

したがって、第2発明の認証装置（Pr1）では、追加権限機能に含まれる機能を利用する場合に権限変更認証が必要になるので、認証された利用者が中座等した場合に、利用権限のない第三者が使用しようとしても、標準権限機能に含まれる機能しか利用できず、追加権限機能に含まれる機能の利用が制限される。この結果、利用権限のない第三者が利用できる機能の範囲を制限することができ、追加権限機能に含まれる機能を悪用されることを抑制できる。したがって、第三者の悪用により、正常に動作しなくなったり、機密情報が漏洩することを減らすことができる。

また、前記構成要件を備えた第2発明では、前記権限変更認証手段（C9）は、追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う。したがって、標準権限への権限変更は権限変更認証が必要ないので、権限変更時に必ず権限変更認証を行う場合に比べ入力操作を減らすことができ、操作性を高めることができる。

【0025】

（第3発明）

前記技術的課題を解決するために、第3発明の認証プログラム（P1）は、コンピュータ（Pr1）を、画像形成装置（Pr1）の利用者の認証を行うための認証情報を利用者毎に記憶する認証情報記憶手段（C4D、C31B）、

前記利用者の認証を行う認証手段（C4、C31）、

利用者が利用できる画像形成装置（Pr1）の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置（Pr1）の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置（Pr1）の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する利用権限情報記憶手段（C7）、

認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する追加権限機能入力判別手段（C8B）、

前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像（61）を情報表示画面（UI1）に表示する権限変更認証画像表示手段（C9B）、

前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する権限変更認証情報記憶手段（C9C）、

前記権限変更画像（61）に入力された入力情報と前記権限変更認証情報記憶手段（C9C）に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う権限変更認証手段（C9）、

前記追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を

10

20

30

40

50

利用する入力がされた場合に、標準権限に自動的に権限変更を行う前記権限変更認証手段 (C 9)、

として機能させることを特徴とする。

【0026】

(第3発明の作用)

前記構成要件を備えた第3発明の認証プログラム(P1)により、認証情報記憶手段(C4D, C31B)は、画像形成装置(Pr1)の利用者の認証を行うための認証情報を利用者毎に記憶する。認証手段(C4, C31)は、前記利用者の認証を行う。利用権限情報記憶手段(C7)は、利用者が利用できる画像形成装置(Pr1)の機能を特定する利用権限であって、認証時に標準的に利用できる機能であり且つ前記画像形成装置(Pr1)の画像形成の機能を特定する標準権限と、追加的に利用できる機能であり且つ前記画像形成の機能を有さず前記画像形成装置(Pr1)の仕様を登録または変更する機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する。追加権限機能入力判別手段(C8B)は、認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する。

10

【0027】

権限変更認証画像表示手段(C9B)は、前記認証された利用者が前記標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた場合に、前記利用者の権限を変更するための権限変更画像(61)を情報表示画面(UI1)に表示する。権限変更認証情報記憶手段(C9C)は、前記追加権限で特定される機能を使用する際に、前記標準権限から前記追加権限に権限を変更する前記利用者の権限変更認証を行うための権限変更認証情報を記憶する。権限変更認証手段(C9)は、前記権限変更画像(61)に入力された入力情報と前記権限変更認証情報記憶手段(C9C)に記憶された権限変更認証情報とに基づいて、権限変更を行う前記利用者の権限変更認証を行う。

20

【0028】

したがって、第3発明の認証プログラム(P1)により、追加権限機能に含まれる機能を利用する場合に権限変更認証が必要になるので、認証された利用者が中座等した場合に、利用権限のない第三者が使用しようとしても、標準権限機能に含まれる機能しか利用できず、追加権限機能に含まれる機能の利用が制限される。この結果、利用権限のない第三者が利用できる機能の範囲を制限することができ、追加権限機能に含まれる機能を悪用されることを抑制できる。したがって、第三者の悪用により、正常に動作しなくなったり、機密情報が漏洩することを減らすことができる。

30

また、前記構成要件を備えた第2発明では、前記権限変更認証手段(C9)は、追加認証がされた利用者が前記追加権限で特定される追加権限機能に含まれない前記画像形成の機能であり、且つ前記標準権限で特定される標準権限機能に含まれる機能を利用する入力がされた場合に、標準権限に自動的に権限変更を行う。したがって、標準権限への権限変更は権限変更認証が必要ないので、権限変更時に必ず権限変更認証を行う場合に比べ入力操作を減らすことができ、操作性を高めることができる。

40

【発明の効果】

【0029】

前述の本発明は、下記の効果(E01)を奏する。

(E01) 認証された状態で利用権限のない人物による使用を制限することができる。

【発明を実施するための最良の形態】

【0030】

次に図面を参照しながら、本発明の実施の形態の具体例(実施例)を説明するが、本発明は以下の実施例に限定されるものではない。

【実施例1】

【0031】

50

図1は本発明の実施例1の認証システムの全体説明図である。

図1において、本発明の実施例1のプリントシステム（認証システム）Sは、インターネット回線（公衆通信回線）1やローカルエリアネットワーク（LAN）2を含むネットワークNを有する。前記ローカルエリアネットワーク2は、ルーターRを介してインターネット回線1に接続されている。実施例1では、前記ローカルエリアネットワーク2は、第1事業部門用の第1サブネットワーク3と、第2事業部門用の第2サブネットワーク4とを有し、第1サブネットワーク3と第2サブネットワーク4はルーターRを介して接続されている。

前記各サブネットワーク3, 4には、それぞれ、複数のクライアントパソコンPC（電子マニュアル閲覧装置）やネットワーク接続型の複合機（コピー、FAX、プリンタ、スキャナ機能を有する画像形成装置、電子機器、認証装置、コンピュータ）Pr1~Pr4、ネットワーク管理者の管理者サーバSb（情報処理装置、電子機器）、その他、図示しないワークステーションやデータベースサーバ等が接続されている。また、インターネット回線1を介して複合機Pr5が接続されている。

#### 【0032】

前記各クライアントパソコンPCや管理者サーバSbは、コンピュータ装置により構成されており、それぞれ、コンピュータ本体H1と、ディスプレイ（情報表示画面）H2と、キーボードH3やマウスH4等の入力装置、図示しないHDドライブ（ハードディスクドライブ）、CDドライブ（コンパクトディスクドライブ）等により構成されている。

前記複合機Pr1~Pr5は、ユーザインタフェースUIと、印刷用紙を給紙するための複数の給紙トレイTRと、排紙トレイTRhとを有している。なお、前記複合機Pr1~Pr5は、マイクロコンピュータを内蔵し、コピー、プリンタ、FAX、ネットワークスキャナの全ての機能を備えた電子写真方式の複合機である。

#### 【0033】

図1において、実施例1のプリントシステムSは、現在一般的に普及しているTCP/IP（Transmission Control Protocol / Internet Protocol）環境で運用されており、ネットワークNに接続された各機器PC, Pr1~Pr5には、それぞれ、固有のネットワーク識別情報（IPアドレス）が割り当てられている（設定されている）。実施例1では、第1サブネットワーク3に接続された各機器PC, Pr1, Pr2には、IPアドレスとして「192.168.0.\*」（\*は、0~255で機器毎に異なる値）が割り当てられており、第2サブネットワーク4に接続された各機器PC, Pr3, Pr4には、IPアドレスとして「192.168.1.\*」が割り当てられている。

#### 【0034】

ここで、IPアドレスについて説明すると、IPv4（Internet Protocol Version 4）では、IPアドレスに32bitの番号（実際には、8bitずつの10進数に分けて「123.123.123.123」等と表現する）を使用している。標準では、32bitのうち、上位16bit分をネットワークアドレス番号とし、下位16bit分をホストアドレス番号としている。ホストアドレス番号は、16bit分（すなわち、0~65535）であるため、65536台の機器を管理することとなり、全てを管理することは困難である。したがって、現在、ホストアドレス番号を、例えば、上位8bitと下位8bitに分割して（サブネット化して）、下位8bit分の256台で管理することが行われている。このとき、IPアドレスからサブネットのネットワークアドレスを求めるために使用されるのがサブネットマスクであり、IPアドレスにサブネットマスクでANDをとるとサブネットのネットワークアドレスを求めることができる。前記サブネットマスクは、前記下位8bitの場合では、「255.255.255.0」となり、上位24bit分がサブネットのネットワークアドレスとなる。なお、実施例1では、このサブネットマスクが各機器に設定、記憶されている。したがって、第1サブネットワーク3のサブネットのネットワークアドレスは「192.168.0.0」となり、第2サブネットワーク4のサブネットのネットワークアドレスは「192.168.1.0」となる

#### 【0035】

10

20

30

40

50

(実施例1の制御部の説明)

次に実施例1の制御部の説明を行うが、ユーザの入力に応じて印刷用の画像情報をネットワークNを介して複合機Pr1~Pr5に送信したり、複合機Pr1~Pr5でスキャンした読取画像情報をネットワークNを介して取り込むクライアントパソコンPCや管理者サーバSbの制御部の説明は、従来公知であるので省略する。

(画像形成装置の制御部の説明)

図2は、実施例1の画像形成装置としての複合機の制御部分が備えている各機能をブロック図(機能ブロック図)で示した図である。

図2において、実施例1の複合機Pr1のコントローラCは、外部との信号の入出力および入出力信号レベルの調節等を行うI/O(入出力インターフェース)、必要な処理を行うためのプログラムおよびデータ等が記憶されたROM(リードオンリーメモリ)やハードディスク、必要なデータを一時的に記憶するためのRAM(ランダムアクセスメモリ)、前記ROM等に記憶されたプログラムに応じた処理を行うCPU(中央演算処理装置)、ならびにクロック発振器等を有するマイクロコンピュータにより構成されており、前記ROM等に記憶されたプログラムを実行することにより種々の機能を実現することができる。

なお、各複合機Pr1~Pr5のコントローラCは、同様に構成されているので、以下の説明では、複合機Pr1について説明し、その他の複合機Pr2~Pr5についての詳細な説明は省略する。

【0036】

(前記コントローラCに接続された信号入力要素)

前記コントローラCは、UI(ユーザインタフェース)や図示しない各種センサ等の信号入力要素からの信号が入力されている。

前記UIは、表示器UI1や、コピースタートキーUI2、テンキーUI3等の入力キーを備えており、それらが入力されたことを検出して、その検出信号をコントローラCに入力する。

【0037】

(前記コントローラCに接続された制御要素)

前記コントローラCは、画像情報に応じて画像を形成し、原稿画像を読取る画像読取り部材(スキャナ部)PrAや、給紙トレイTRから給紙された用紙に画像を記録して排出トレイTRhに排出する画像記録部材(プリンタ部)PrB、その他の制御要素に接続されており、それらの作動制御信号を出力している。

【0038】

(前記コントローラCの機能)

前記コントローラCは、前記各信号出力要素からの出力信号やネットワークNを介して受信した情報、信号に応じた処理を実行して、前記各制御要素に制御信号を出力する機能(制御手段)を有している。前記コントローラCの機能(制御手段)を次に説明する。

C1:画像情報受信手段

画像情報受信手段C1は、ネットワークNを介してクライアントパソコンPC等から送信された印刷画像情報や、FAX画像情報等の画像情報を受信する。

C2:画像情報記憶手段

画像情報記憶手段C2は、受信した画像情報や、コピー動作時やスキャナ動作時、FAX送信動作時の読取り画像情報等の作業(ジョブ、すなわち、プリント動作やスキャナ動作、FAX動作、コピー動作等)を実行するための情報(データ)を記憶する。

【0039】

C3:画像形成手段

画像形成手段C3は、実行するジョブ(コピー動作、プリント動作等)に応じて、前記画像読取り部材PrAや画像記録部材PrBの動作を制御して、ジョブを実行する。

P1:認証プログラム

認証プログラムP1は、認証手段C4と、機能選択画像表示手段C5と、認証ユーザ記

10

20

30

40

50

憶手段 C 6 と、利用権限情報記憶手段 C 7 と、利用権限判別手段 C 8 と、権限変更認証手段 C 9 とを有し、利用者の認証や利用権限の設定、変更等を行う。

#### C 4 : 認証手段

認証手段 C 4 は、認証画像表示手段 C 4 A と、認証不可告知画像表示手段 C 4 B と、キーボード用画像表示手段 C 4 C と、認証情報記憶手段 C 4 D とを有し、複合機 P r 1 を使用しようとしているユーザ（利用者や管理者）が登録されたユーザであるか否かの認証を行う。

##### 【 0 0 4 0 】

図 3 は実施例 1 の認証画像の説明図である。

#### C 4 A : 認証画像表示手段

認証画像表示手段 C 4 A は、ユーザの認証情報を入力するための認証画像 1 1（図 3 参照）を表示部（情報表示画面）U I 1 に表示する。図 3 において、実施例 1 の認証画像 1 1 は、認証情報としてのユーザ I D を入力するためユーザ I D 入力欄 1 2 と、認証情報としてのパスワードを入力するためのパスワード入力欄 1 3 と、ユーザ I D やパスワードを入力するためのキーボード画像を表示するためのキーボード入力開始画像 1 4（図 3 の「キーボード」のアイコン参照）と、認証情報（ユーザ I D およびパスワード）の入力を終了して認証（ログイン）するための認証実行画像 1 6（図 3 の「ログイン」アイコン参照）とを有する。なお、実施例 1 の表示部 U I 1 は、ユーザが指先で画像部分を触れることで入力可能な接触入力型（いわゆる、タッチパネル）の表示部 U I 1 により構成されている。

##### 【 0 0 4 1 】

図 4 は実施例 1 の認証不可告知画像の説明図である。

#### C 4 B : 認証不可告知画像表示手段

認証不可告知画像表示手段 C 4 B は、ユーザ I D やパスワードが一致せず、認証（ログイン）ができなかった場合に、そのことをユーザに告知する認証不可告知画像 2 1（図 4 参照）を表示部 U I 1 に表示する。図 4 において、実施例 1 の認証不可告知画像 2 1 は、認証ができなかったことをユーザが確認する確認画像 2 2（図 4 の「OK」アイコン参照）を有する。

##### 【 0 0 4 2 】

図 5 は実施例 1 のキーボード画像の説明図であり、図 5 A はひらがなを入力するためのキーボード画像の説明図、図 5 B は英数字を入力するためのキーボード画像の説明図である。

#### C 4 C : キーボード用画像表示手段

キーボード用画像表示手段 C 4 C は、前記認証画像 1 1 において、キーボード入力開始画像 1 4 の入力がされた場合に、ユーザ I D またはパスワードの入力を行うためのキーボード画像 3 1（図 5 参照）を表示部 U I 1 に表示する。図 5 において、実施例 1 のキーボード画像 3 1 は、入力項目を表示する入力項目表示欄 3 2（図 3 ではユーザ I D 表示欄）と、画像部分を指で触れて入力を行うキーボード入力部 3 3 と、入力項目表示欄 3 2 に入力された内容を認証画像 1 1 の該当する入力欄 1 2, 2 3 に反映するための入力決定画像 3 4（図 5 の「決定」アイコン参照）と、入力項目表示欄 3 2 に表示された内容を破棄して前記認証画像 1 1 に戻る入力取り消し画像 3 6（図 5 の「取り消し」アイコン参照）と、ひらがな、カタカナ、英数、記号の中で入力モードを切り替えるための入力モード切替画像 3 7（図 5 の「ひらがな」、「カタカナ」、「英数」、「記号」のアイコン参照）とを有する。

##### 【 0 0 4 3 】

#### C 4 D : 認証情報記憶手段

認証情報記憶手段 C 4 D は、前記認証手段 C 6 が認証を行う際に参照する、複合機 P r 1 を利用可能な利用者の認証情報（ユーザ I D およびパスワード）を記憶する。前記認証情報は、図示しない従来公知の認証情報登録手段（プログラム）によって、管理者により予め登録（記憶）されている。

10

20

30

40

50

## 【 0 0 4 4 】

図 6 は実施例 1 の機能選択画像の説明図である。

## C 5 : 機能選択画像表示手段

機能選択画像表示手段 C 5 は、複合機 P r 1 の各機能を選択するための機能選択画像 4 1 (メニュー画像、図 6 参照) を表示部 U I 1 に表示する。図 6 において、実施例 1 の機能選択画像 4 1 は、各機能を選択するための機能選択アイコン 4 2 (図 6 の「コピー」アイコン 4 2 a、「F A X」アイコン 4 2 b、「スキャナ」アイコン 4 2 c 参照) と、複合機 P r 1 の各種設定や仕様を登録、変更するための仕様変更アイコン 4 3 (図 6 の「仕様変更」アイコン参照) と、複合機 P r 1 の操作を終了するためのログアウト画像 4 7 (「ログアウト」アイコン参照) とを有する。

10

## 【 0 0 4 5 】

## C 6 : 認証ユーザ記憶手段 ( 認証利用者記憶手段 )

認証ユーザ記憶手段 C 6 は、前記認証手段 C 4 で認証されたユーザ (利用者) を記憶する。すなわち、現在複合機 P r 1 を利用中のユーザを記憶する。

## C 7 : 利用権限情報記憶手段

利用権限情報記憶手段 C 7 は、ユーザ権限グループ管理テーブル記憶手段 C 7 A と、権限機能管理テーブル記憶手段 C 7 B とを有し、ユーザ (利用者) が利用できる機能を特定する利用権限であって、認証時に標準的に利用できる機能を特定する標準権限と、追加的に利用できる機能を特定する追加権限とを含む利用権限の情報である利用権限情報を記憶する。

20

## 【 0 0 4 6 】

図 7 は実施例 1 の利用権限情報の説明図であり、図 7 A はユーザ権限グループ管理テーブルの説明図、図 7 B は権限機能管理テーブルの説明図である。

## C 7 A : ユーザ権限グループ管理テーブル記憶手段

ユーザ権限グループ管理テーブル記憶手段 C 7 A は、特定の範囲の利用権限が認められた利用権限グループと、各ユーザ (利用者) がどのグループ (利用権限) に所属するかをテーブル化したユーザ権限グループ管理テーブル (図 7 A 参照) を記憶する。図 7 A において、実施例 1 では、前記利用権限グループとして、「一般ユーザ 1」、「一般ユーザ 2」および「管理者」を有し、各ユーザ (ユーザ A ~ ユーザ C) の所属するグループ (各ユーザに認められている利用権限) と、最初の認証時に付与される標準権限グループと、

30

## 【 0 0 4 7 】

## C 7 B : 権限機能管理テーブル記憶手段

権限機能管理テーブル記憶手段 C 7 B は、各利用権限グループで使用可能な機能をテーブル化した権限機能管理テーブル (図 7 B 参照) を記憶する。図 7 B において、実施例 1 では、前記「一般ユーザ 1」には「コピー」機能のみ利用権限が設定されており、「一般ユーザ 2」には「コピー」機能、「F A X」機能、「スキャン」機能の利用権限が設定され、「管理者」には「仕様変更」機能の利用権限が設定されている。そして、「一般ユーザ 1」、「一般ユーザ 2」、「管理者」の順に権限が大きくなることが記憶されている。したがって、図 7 A、図 7 B において、「ユーザ A」では、認証時の標準権限である「一般ユーザ 2」に設定されている「コピー」機能、「F A X」機能および「スキャン」機能が標準権限機能となり、標準で付与されない追加権限である「管理者」に設定されている「仕様設定」が追加権限機能となる。また、実施例 1 では、「ユーザ B」および「ユーザ C」には、標準権限 (「一般ユーザ 2」または「一般ユーザ 1」) のみが設定され、追加権限が設定されていない。

40

## 【 0 0 4 8 】

## C 8 : 利用権限判別手段

利用権限判別手段 C 8 は、付与利用権限記憶手段 C 8 A と、追加権限機能入力判別手段 C 8 B と、権限大小判別手段 C 8 C と、権限無し告知画像表示手段 C 8 D とを有し、ユーザの利用権限を判別する。

50

#### C 8 A : 付与利用権限記憶手段

付与利用権限記憶手段 C 8 A は、認証されたユーザに現在付与されている利用権限を記憶する。実施例 1 の付与利用権限記憶手段 C 8 A は、現在、ユーザが属している利用権限グループと、利用権限グループに設定されている利用権限機能とを記憶することにより、ユーザに現在付与されている利用権限を記憶する。

【 0 0 4 9 】

#### C 8 B : 追加権限機能入力判別手段

追加権限機能入力判別手段 C 8 B は、認証されたユーザ（利用者）が標準権限で特定される標準権限機能に含まれない機能であり、且つ前記追加権限で特定される追加権限機能に含まれる機能を利用する入力がされた否かを判別する。実施例 1 の追加権限機能入力判別手段 C 8 B は、前記利用権限記憶手段に記憶されている現在の利用権限の機能に含まれない機能であって、利用中のユーザの他の利用権限の機能に含まれる機能を利用する入力がされたか否かを判別することにより、標準権限機能に含まれない機能であり且つ追加権限機能に含まれる機能を利用する入力がされたについても判別している。

10

#### C 8 C : 権限大小判別手段

権限大小判別手段 C 8 C は、追加権限機能入力判別手段 C 8 B により、現在の利用権限の機能に含まれない機能であって、ユーザの他の利用権限の機能に含まれる機能を利用する入力がされた場合に、権限機能管理テーブル記憶手段 C 7 B に記憶された権限の順序に基づいて、現在の利用権限と他の利用権限のどちらの権限が大きいかを判別する。

【 0 0 5 0 】

20

図 8 は実施例 1 の権限無し告知画像の説明図である。

#### C 8 D : 権限無し告知画像表示手段

権限無し告知画像表示手段 C 8 D は、認証されたユーザにより利用する入力がされた機能が、標準権限機能にも追加権限機能にも含まれていない場合に、利用権限がないことをユーザに告知する権限無し告知画像 5 1（図 8 参照）を表示する。図 8 において、実施例 1 の権限無し告知画像 5 1 は、利用者が告知内容を確認したことを指示する確認画像 5 2（図 8 の「OK」アイコン参照）を有する。

#### C 9 : 権限変更認証手段

権限変更認証手段 C 9 は、権限変更認証情報記憶手段 C 9 A と、権限変更認証画像表示手段 C 9 B と、権限変更認証不可告知画像表示手段 C 9 C とを有し、権限変更画像（後述する図 9 参照）に入力された入力情報と、権限変更認証情報記憶手段 C 9 B に記憶された権限変更認証情報とに基づいて、権限変更を行うユーザの権限変更認証を行う。

30

【 0 0 5 1 】

#### C 9 A : 権限変更認証情報記憶手段

権限変更認証情報記憶手段 C 9 A は、追加権限で特定される機能を使用する際に、標準権限から追加権限に権限を変更するユーザの権限変更認証を行うための権限変更認証情報を記憶する。実施例 1 の権限変更認証情報記憶手段 C 9 A は、権限変更認証情報として、前記認証情報記憶手段 C 4 D に記憶された認証用のパスワードとは異なる、予め設定された権限変更用パスワードを記憶する。なお、前記認証用のパスワードと権限変更用パスワードとは異なることが望ましいが、共通化することも可能である。

40

【 0 0 5 2 】

図 9 は実施例 1 の再認証必要告知画像の説明図である。

#### C 9 B : 権限変更認証画像表示手段

権限変更認証画像表示手段 C 9 B は、認証されたユーザが前記標準権限機能に含まれない機能であり且つ追加権限機能に含まれる機能を利用する入力がされた場合に、ユーザの利用権限を変更するための権限変更画像 6 1（図 9 参照）を表示部 UI 1（情報表示画面）に表示する。図 9 において、実施例 1 の権限変更画像 6 1 は、権限変更認証情報としての権限変更用パスワードを入力するためのパスワード入力欄 6 2 と、権限変更用パスワードを入力するためのキーボード画像（前記図 5 参照）を表示するためのキーボード入力開始画像 6 3（図 9 の「キーボード」のアイコン参照）と、権限変更認証情報（権限変更用

50

パスワード)の入力を終了して権限変更認証を行うための権限変更認証実行画像64(図9の「OK」アイコン参照)と、権限変更認証を行わないことを指示する不実行指示画像66(図9の「キャンセル」アイコン参照)と、を有する。

#### 【0053】

図10は実施例1の権限変更認証不可告知画像の説明図である。

C9C：権限変更認証不可告知画像表示手段

権限変更認証不可告知画像表示手段C9Cは、前記権限変更認証画像61のパスワード入力欄62に入力された入力情報と、権限変更認証情報記憶手段に記憶された権限変更認証情報とが一致せず、権限変更認証ができなかった場合に、権限変更認証ができなかったことを告知する権限変更認証不可告知画像71(図10参照)を表示部UI1に表示する。図10において、実施例1の権限変更認証不可告知画像71は、ユーザが告知内容を確認したことを指示する確認画像72(図10の「OK」アイコン参照)を有する。

10

C10：ネットワーク情報記憶手段

ネットワーク情報記憶手段C10は、複合機(画像形成装置)Pr1のIPアドレスを記憶するIPアドレス記憶手段C10Aと、複合機Pr1のサブネットマスクを記憶するサブネットマスク記憶手段C10Bとを有し、複合機Pr1のIPアドレスおよびサブネットマスクからなるネットワーク情報を記憶する。

#### 【0054】

(実施例1のフローチャートの説明)

次に、実施例1の複合機Pr1の処理の流れをフローチャートを使用して説明するが、ユーザの入力に応じて複合機Pr1に対してプリントアウト用の画像情報を送信するクライアントパソコンPC等の処理は、従来公知であるため、図示及び詳細な説明を省略する。

20

#### 【0055】

(メインフローチャートの説明)

図11は実施例1の画像形成装置のメインフローチャートである。

図11のフローチャートの各ST(ステップ)の処理は、複合機Pr1のROMやハードディスク等に記憶されたプログラムに従って行われる。また、この処理は複合機Pr1の他の各種処理と並行してマルチタスクで実行される。

図11に示すフローチャートは複合機Pr1の電源オンにより開始される。

30

#### 【0056】

図11のST1において、認証画像11(ログイン画像)を表示部UI1に表示し、ST2に進む。

ST2において、認証画像11の認証実行画像16(図3の「ログイン」アイコン参照)を選択する入力がされたか否かを判別する。ノー(N)の場合はST3に進み、イエス(Y)の場合はST7に進む。

ST3において、認証画像11のキーボード入力開始画像14(図3の「キーボード」のアイコン参照)を選択する入力がされたか否かを判別する。イエス(Y)の場合はST4に進み、ノー(N)の場合はST5に進む。

ST4において、キーボード画像31を表示部UI1に表示し、キーボード入力部33によりユーザIDまたはパスワードの入力を行い、入力決定画像34(図5の「決定」アイコン参照)の入力に応じて、認証画像11のユーザID入力欄12またはパスワード入力欄13に入力内容を反映させるキーボード用入力処理(図示省略)を実行して、ST1に戻る。

40

#### 【0057】

ST5において、ユーザインタフェースUIのテンキーUI3による入力がされたか否かを判別する。イエス(Y)の場合はST6に進み、ノー(N)の場合はST2に戻る。

ST6において、入力に応じて認証画像11(ユーザID入力欄12またはパスワード入力欄13の選択されている一方の欄)の画像を更新して、ST2に戻る。

ST7において、認証画像11のユーザID入力欄12に入力された情報に基づいて、

50

入力されたユーザIDは認証情報記憶手段C4Dに登録(記憶)されているか否かを判別する。イエス(Y)の場合はST8に進み、ノー(N)の場合はST9に進む。

ST8において、認証画像11のパスワード入力欄13に入力された情報に基づいて、入力されたパスワードが、認証情報記憶手段C4Dに登録(記憶)されているユーザIDのパスワード(認証情報)に一致するか否かを判別する。ノー(N)の場合はST9に進み、イエス(Y)の場合はST11に進む。

【0058】

ST9において、認証不可告知画像21(図4参照)を表示部UI1に表示する。そして、ST10に進む。

ST10において、認証不可告知画像21の確認画像22(図4の「OK」アイコン参照)を選択する入力がされたか否かを判別する。イエス(Y)の場合はST1に戻り、ノー(N)の場合はST10を繰り返す。

ST11において、ユーザ権限グループ管理テーブル(図7A参照)に基づいて、ログインしたユーザ(認証された利用者)に設定されている標準権限グループを読み取り、付与利用権限記憶手段C8Aに記憶する(取得する)。そして、ST12に進む。

ST12において、権限機能管理テーブル(図7B参照)に基づいて、取得した標準の利用権限グループに設定されている標準権限機能を読み取り、付与利用権限記憶手段C8Aに記憶する(取得する)。そして、ST13に進む。

【0059】

ST13において、機能選択画像41(図6参照)を表示部UI1に表示する。そして、ST14に進む。

ST14において、「コピー」アイコン42aを選択する入力がされたか否かを判別する。イエス(Y)の場合はST15に進み、ノー(N)の場合はST17に進む。

ST15において、選択された機能が、認証されたユーザが現在属する利用権限グループの利用権限機能に含まれているか否かを判別し、必要に応じて権限変更認証を実行する権限判別認証処理(後述する図11のサブルーチン参照)を実行して、ST16に進む。

ST16において、コピー枚数等を設定してジョブとしてのコピー動作を実行する従来公知のコピー機能選択時の処理を行い、ST13に戻る。

【0060】

ST17において、「FAX」アイコン42bを選択する入力がされたか否かを判別する。イエス(Y)の場合はST18に進み、ノー(N)の場合はST20に進む。

ST18において、前記ST15と同様の権限判別認証処理(後述する図11のサブルーチン参照)を実行して、ST19に進む。

ST19において、宛先を入力し、原稿画像を読み取って送信する従来公知のFAX動作(ジョブ)を実行するFAX機能選択時の処理を行い、ST13に戻る。

ST20において、「スキャナ」アイコン42cを選択する入力がされたか否かを判別する。イエス(Y)の場合はST21に進み、ノー(N)の場合はST23に進む。

ST21において、前記ST15と同様の権限判別認証処理(後述する図11のサブルーチン参照)を実行して、ST22に進む。

ST22において、原稿画像を読み取るスキャナ動作(ジョブ)を実行する従来公知のスキャナ機能選択時の処理を行い、ST13に戻る。

【0061】

ST23において、仕様変更アイコン43を選択する入力がされたか否かを判別する。イエス(Y)の場合はST24に進み、ノー(N)の場合はST26に進む。

ST24において、前記ST15と同様の権限判別認証処理(後述する図11のサブルーチン参照)を実行して、ST25に進む。

ST25において、複合機Pr1の動作設定を登録、変更したり、FAXの宛先を編集したりする従来公知の仕様変更選択時の処理を実行して、ST13に戻る。

ST26において、機能選択画像41の「ログアウト」アイコン47を選択する入力がされたか否かを判別する。イエス(Y)の場合はST27に進み、ノー(N)の場合はS

10

20

30

40

50

T 1 4 に戻る。

S T 2 7 において、ログインしたユーザのログアウト（認証解除）処理を実行する。そして、S T 1 に戻る。

【 0 0 6 2 】

（権限判別認証処理（S T 1 5 , S T 1 8 , S T 2 1 , S T 2 4 のサブルーチン）の説明）

図 1 2 は実施例 1 の権限判別認証処理のフローチャートであり、図 1 1 の S T 1 5 , S T 1 8 , S T 2 1 , S T 2 4 のサブルーチンである。

図 1 2 の S T 3 1 において、選択された機能の利用権限がないか否かを判別する。すなわち、付与利用権限記憶手段 C 8 A に記憶された利用権限機能に、選択された機能が含まれているか否かを判別する。イエス（Y）の場合（利用権限がない場合）は S T 3 2 に進み、ノー（N）の場合（利用権限がある場合）は図 1 2 の権限判別認証処理を終了して、図 1 1 のメインフローチャートに戻る。

10

【 0 0 6 3 】

S T 3 2 において、ユーザ権限グループ管理テーブル（図 7 A 参照）に基づいて、ログインユーザ（認証された利用者）に、別の利用権限グループの設定があるか否かを判別する。イエス（Y）の場合は S T 3 3 に進み、ノー（N）の場合は S T 3 4 に進む。

S T 3 3 において、ユーザ権限グループ管理テーブル（図 7 A 参照）および権限機能管理テーブル（図 7 B 参照）に基づいて、選択された機能が利用権限機能として含まれる別の権限グループがあるか否かを判別する。ノー（N）の場合は S T 3 4 に進み、イエス（Y）の場合は S T 3 6 に進む。

20

S T 3 4 において、権限無し告知画像 5 1（図 8 参照）を表示する。そして、S T 3 5 に進む。

S T 3 5 において、権限無し告知画像 5 1 の確認画像 5 2（図 8 の「OK」アイコン参照）を選択する入力がされたか否かを判別する。ノー（N）の場合は S T 3 5 を繰り返し、イエス（Y）の場合は図 1 1 の S T 1 3 に戻る。

【 0 0 6 4 】

S T 3 6 において、権限機能管理テーブル（図 7 B 参照）に基づいて、権限のある別の利用権限グループは、現在の利用権限グループよりも権限が大きいか否かを判別する。イエス（Y）の場合は S T 3 7 に進み、ノー（N）の場合は S T 4 5 に進む。

30

S T 3 7 において、権限変更画像 6 1（図 9 参照）を表示部 U I 1（情報表示画面）に表示する。そして、S T 3 8 に進む。

S T 3 8 において、権限変更画像 6 1 の権限変更認証実行画像 6 4（図 9 の「OK」アイコン参照）を選択する入力がされたか否かを判別する。ノー（N）の場合は S T 3 9 に進み、イエス（Y）の場合は S T 4 2 に進む。

S T 3 9 において、権限変更画像 6 1 の不実行指示画像 6 6（図 9 の「キャンセル」アイコン参照）を選択する入力がされたか否かを判別する。ノー（N）の場合は S T 4 0 に進み、イエス（Y）の場合は図 1 1 の S T 1 3 に戻る。

【 0 0 6 5 】

S T 4 0 において、権限変更画像 6 1 のキーボード入力開始画像 6 3（図 9 の「キーボード」のアイコン参照）やテンキー U I 3 により、権限変更認証情報としての権限変更用パスワードの入力がされたか否かを判別する。イエス（Y）の場合は S T 4 1 に進み、ノー（N）の場合は S T 3 8 に戻る。

40

S T 4 1 において、入力に応じて権限変更画像 6 1 を更新する。そして、S T 3 8 に戻る。

S T 4 2 において、権限変更画像 6 1 のパスワード入力欄 6 2 に入力された権限変更用パスワードが権限変更認証情報記憶手段 C 9 A に記憶された権限変更用パスワードに一致するか否かを判別する。ノー（N）の場合は S T 4 3 に進み、イエス（Y）の場合は S T 4 5 に進む。

【 0 0 6 6 】

50

ST43において、権限変更認証不可告知画像71(図10参照)を表示部UI1に表示する。そして、ST44に進む。

ST44において、権限変更認証不可告知画像71の確認画像72(図10の「OK」アイコン参照)を選択する入力されたか否かを判別する。イエス(Y)の場合はST37に戻り、ノー(N)の場合はST44を繰り返す。

ST45において、ログインユーザの利用権限グループを、選択された機能を利用する権限のある別の利用権限グループに変更する。そして、図12の権限判別認証処理を終了して図11のメインフローチャートに戻る。

【0067】

(実施例1の作用)

前記構成を備えた実施例1の複合機Pr1では、図7Aに示すように、各利用者に少なくとも1つの標準権限グループが設定されており、標準権限グループで権限が付与されている機能とは別の機能の利用権限がある利用権限グループが追加設定されている利用者(実施例1ではユーザA)もいる。

図7Aにおいて、複数の利用権限グループに属するユーザAは、最初の認証時には、標準権限グループに属し、標準権限機能が使用でき、追加権限機能(実施例1では「仕様変更」)は利用できない。そして、追加権限機能を使用する場合、権限変更認証をすることにより、追加権限機能に含まれる機能が使用でき、標準権限機能は利用できなくなる。

【0068】

したがって、実施例1の複合機Pr1では、標準権限グループの状態ユーザが中座等して複合機Pr1から離れた場合に、利用権限のない第三者が使用しようとしても、標準権限グループ内の機能しか利用できず、権限変更認証がされなければ、追加権限グループの機能の利用が制限される。例えば、管理者としてユーザAがログインした状態では、管理者であっても標準権限機能では仕様変更ができないので、この状態で管理者が中座しても、第三者により仕様変更されることを防止できる。この結果、認証がされた状態で第三者が利用できる機能の範囲を制限することができ、機器が悪用されることを低減することができる。したがって、第三者の悪用により、機器が動作しなくなったり、機密情報が漏洩することを少なくすることができる。

【0069】

また、実施例1の複合機Pr1では、利用権限グループに権限の大きさの順序が設定されており、権限が小さい利用権限グループから権限が大きな利用権限グループに権限変更する場合は権限変更認証が必要になるが(ST36~ST44参照)、権限が大きいグループから権限の小さいグループへは権限変更認証を行わずに権限変更ができる(ST36およびST45参照)。したがって、悪用された場合に被害が大きくなる可能性がある権限の大きな利用権限グループへの権限変更には権限変更認証を必要とすることで、悪用されにくくすることができる(セキュリティを高めることができる)。また、権限の小さいグループへの権限変更は権限変更認証が必要ないので、権限変更時に必ず権限変更認証を行う場合に比べ入力操作を減らすことができ、操作性を高めることができる。

【実施例2】

【0070】

次に本発明の実施例2の説明を行うが、この実施例2の説明において、前記実施例1の構成要素に対応する構成要素には同一の符号を付して、その詳細な説明を省略する。この実施例2は、下記の点で前記実施例1と相違しているが、他の点では前記実施例1と同様に構成されている。

【0071】

(実施例2の制御部の説明)

(画像形成装置の制御部の説明)

(実施例2のコントローラCの機能)

図13は、実施例2の画像形成装置としての複合機の制御部分が備えている各機能をブロック図(機能ブロック図)で示した図であり、実施例1の図2に対応する図である。

10

20

30

40

50

図13において、実施例2の複合機Pr1~Pr5の認証プログラムP1では、認証手段C4は、認証情報記憶手段C4Dに換えて、認証画像11で入力された入力認証情報を管理者サーバSbに送信する入力情報送信手段C4Eと、送信した入力認証情報に応じて管理者サーバから送信される認証可否情報を受信する認証可否情報受信手段C4Fとを有する。そして、実施例2の認証手段C4は、受信した認証可否情報に基づいて、認証（ログイン可否の判別）を行う。なお、実施例2では、利用者の認証が管理者サーバSbで行われ、認証された利用者の標準権限グループおよび追加権限グループや、権限変更認証情報は管理者サーバSbから前記認証可否情報に含まれて送信され、ユーザ権限グループ管理テーブル記憶手段C7Aや権限変更認証情報記憶手段C9Aに記憶される。すなわち、ユーザ権限グループ管理テーブル記憶手段C7Aや権限変更認証情報記憶手段C9Aには、実施例1と異なり、利用中の利用者に関する情報のみが記憶されている。

10

【0072】

また、実施例2の認証プログラムP1では、実施例1の認証プログラムP1の各機能手段C4~C9に加え、下記の機能手段を有する。

C21：自動ログアウト情報受信手段（強制認証解除情報受信手段）

自動ログアウト情報受信手段C21は、管理者サーバ（情報処理装置）Sbから送信された、認証されている利用者の認証を強制的に解除する強制認証解除情報（自動ログアウト情報）を受信する。すなわち、実施例2の自動ログアウト情報受信手段C21は、ログイン状態のユーザを自動的にログアウトさせる自動ログアウト情報を受信する。

C22：利用終了情報送信手段

20

利用終了情報送信手段C22は、複合機Pr1で認証されていた利用者が利用を終了したことを通知する利用終了情報を管理者サーバSbに送信する。実施例2の利用終了情報送信手段C22は、機能選択画像41の「ログアウト」アイコン47を選択する入力された場合または自動ログアウト情報を受信した場合に、ユーザIDと複合機の識別情報（実施例2ではIPアドレス）とを含む利用終了情報を管理者サーバSbに送信する。

【0073】

（管理者サーバSbの制御部の説明）

図14は実施例2の管理者サーバの制御部分が備えている各機能をブロック図（機能ブロック図）で示した図である。

図14において、管理者サーバSbのコンピュータ本体H1は、外部との信号の入出力および入出力信号レベルの調節等を行うI/O（入出力インターフェース）、必要な処理を行うためのプログラムおよびデータ等が記憶されたROM（リードオンリーメモリ）、必要なデータを一時的に記憶するためのRAM（ランダムアクセスメモリ）、ハードディスクやROM等に記憶されたプログラムに応じた処理を行うCPU（中央演算処理装置）、ならびにクロック発振器等を有している。

30

前記構成の管理者サーバSbは、前記ハードディスクやROM等に記憶されたプログラムを実行することにより種々の機能を実現することができる。

【0074】

図14において、実施例2の管理者サーバSbのハードディスクドライブには、コンピュータ本体H1の基本動作を制御する基本ソフト（オペレーティングシステム）OSや、文書作成ソフトウェアや作図ソフトウェア等のアプリケーションプログラムAP、アプリケーションプログラムAP等からの印刷指示に応じて画像形成装置Pr1~Pr5に画像情報の送信を行う従来公知のプリンタドライバPDに加え、認証手段C31、利用者管理手段C32、自動ログアウト情報送信手段C33およびネットワーク情報記憶手段C34を有する。

40

以下、従来公知のオペレーティングシステムOSやアプリケーションプログラムAP、プリンタドライバPDを除く各機能（制御手段）を説明する。

【0075】

C31：認証手段

認証手段C31は、入力認証情報受信手段C31Aと、認証情報受信手段C31Bと、

50

ユーザ権限グループ管理テーブル記憶手段 C 3 1 C と、権限機能管理テーブル記憶手段 C 3 1 D と、権限変更認証情報記憶手段 C 3 1 E と、認証可否情報送信手段 C 3 1 F とを有し、複合機 P r 1 ~ P r 5 を利用としている利用者の認証を、ネットワーク N を介して行う。

#### C 3 1 A : 入力認証情報受信手段

入力認証情報受信手段 C 3 1 A は、複合機 P r 1 ~ P r 5 から送信された前記入力認証情報を受信する。

#### C 3 1 B : 認証情報記憶手段

認証情報記憶手段 C 3 1 B は、実施例 1 の認証情報記憶手段 C 4 D と同様に、前記認証手段 C 3 1 が認証を行う際に参照する、複合機 P r 1 ~ P r 5 を利用可能な利用者の認証情報（ユーザ ID およびパスワード）を記憶する。前記認証情報は、図示しない従来公知の認証情報登録手段（プログラム）によって、管理者により予め登録（記憶）されている。

10

#### 【 0 0 7 6 】

#### C 3 1 C : ユーザ権限グループ管理テーブル記憶手段

ユーザ権限グループ管理テーブル記憶手段 C 3 1 C は、実施例 1 のユーザ権限グループ管理テーブル記憶手段 C 7 A と同様に、ユーザ権限グループ管理テーブルを記憶する。

#### C 3 1 D : 権限機能管理テーブル記憶手段

権限機能管理テーブル記憶手段 C 3 1 D は、実施例 1 の権限機能管理テーブル記憶手段 C 7 B と同様に、権限機能管理テーブルを記憶する。

20

#### C 3 1 E : 権限変更認証情報記憶手段

権限変更認証情報記憶手段 C 3 1 E は、実施例 1 の権限変更認証情報記憶手段 C 9 A と同様に、権限変更認証情報を記憶する。

#### 【 0 0 7 7 】

#### C 3 1 F : 認証可否情報送信手段

認証可否情報送信手段 C 3 1 F は、前記認証手段 C 3 1 による認証結果を通知する認証可否情報を各複合機 P r 1 ~ P r 5 に送信する。実施例 2 の認証可否情報送信手段 C 3 1 F は、認証されなかった場合（ログイン不可の場合）には、ログイン不許可の認証可否情報を送信し、認証された場合（ログイン許可の場合）には、認証された利用者の標準権限グループ、追加権限グループ、権限変更認証情報およびログイン許可の認証可否情報を送信する。

30

#### C 3 2 : 利用者管理手段

利用者管理手段 C 3 2 は、利用者記憶手段 C 3 2 A と、利用者重複判別手段 C 3 2 B と、利用終了情報受信手段 C 3 2 C と、利用者登録変更手段 C 3 2 D とを有し、複合機 P r 1 を利用している利用者（認証されてログイン状態のユーザ）の管理を行う。

#### 【 0 0 7 8 】

#### C 3 2 A : 利用者記憶手段

利用者記憶手段 C 3 2 A は、複合機 P r 1 ~ P r 5 を現在利用中の利用者を記憶する。実施例 2 では、利用者のユーザ ID と利用中の複合機 P r 1 の識別情報（実施例 2 では IP アドレス）と対応させて記憶する。

40

#### C 3 2 B : 利用者重複判別手段

利用者重複判別手段 C 3 2 B は、受信した入力認証情報により特定される利用者が、利用者記憶手段 C 3 2 A に記憶されているか否かを判別することにより、複数の複合機 P r 1 ~ P r 5 を同じ利用者が重複して利用しようとしていないか否かを判別する。

#### 【 0 0 7 9 】

#### C 3 2 C : 利用終了情報受信手段

利用終了情報受信手段 C 3 2 C は、複合機 P r 1 ~ P r 5 から送信された前記利用終了情報を受信する。

#### C 3 2 D : 利用者登録変更手段

利用者登録変更手段 C 3 2 D は、入力認証情報に基づいて認証手段 C 3 1 により認証さ

50

れた利用者を複合機 P r 1 ~ P r 5 (電子機器) を利用中の利用者として利用者記憶手段 C 3 2 A に登録する。また、実施例 2 の利用者登録変更手段 C 3 2 D は、受信した利用終了情報に基づいて利用者記憶手段 C 3 2 A に記憶された利用者を削除する。

【 0 0 8 0 】

C 3 3 : 自動ログアウト情報送信手段 (強制認証解除情報送信手段)

自動ログアウト情報送信手段 C 3 3 は、前記利用者重複判別手段 C 3 2 B で利用者が重複していると判別された場合に、利用者記憶手段 C 3 2 A に利用中と記憶されている複合機 P r 1 ~ P r 5 における認証を強制的に解除する自動ログアウト情報 (強制認証解除情報) を複合機 (電子機器) P r 1 ~ P r 5 に送信する。

C 3 4 : ネットワーク情報記憶手段

ネットワーク情報記憶手段 C 3 4 は、管理者サーバ (情報処理装置) S b の I P アドレスを記憶する I P アドレス記憶手段 C 3 4 A と、管理者サーバ S b のサブネットマスクを記憶するサブネットマスク記憶手段 C 3 4 B とを有し、管理者サーバ S b の I P アドレスおよびサブネットマスクからなるネットワーク情報を記憶する。

【 0 0 8 1 】

(実施例 2 のフローチャートの説明)

次に、実施例 2 のフローチャートの説明を行うが、実施例 1 のフローチャートと同様の処理には同一のステップ ( S T ) 番号を付し、詳細な説明は省略する。

(複合機のメインフローチャートの説明)

図 1 5 は実施例 2 の複合機のメインフローチャートであり、実施例 1 の図 1 1 に対応するフローチャートである。

【 0 0 8 2 】

図 1 5 において、実施例 2 のメインフローチャートでは、実施例 1 のメインフローチャートの S T 7 , S T 8 が省略され、 S T 2 においてイエス ( Y ) の場合は S T 5 1 に進む。

S T 5 1 において、管理者サーバ S b に入力認証情報を送信する。そして、 S T 5 2 に進む。

S T 5 2 において、管理者サーバ S b から送信された認証可否情報を受信したか否かを判別する。イエス ( Y ) の場合は S T 5 3 に進み、ノー ( N ) の場合は S T 5 2 を繰り返す。

S T 5 3 において、受信した認証可否情報はログイン許可 (認証された) であるか否かを判別する。ノー ( N ) の場合は S T 9 に進み、イエス ( Y ) の場合は S T 1 1 に進む。

【 0 0 8 3 】

次に、 S T 1 1 ~ S T 2 6 を実行し、 S T 2 6 でノー ( N ) の場合は S T 5 4 に進み、イエス ( Y ) の場合は S T 2 7 に進む。

S T 5 4 において、自動ログアウト情報を受信したか否かを判別する、イエス ( Y ) の場合は S T 2 7 に進み、ノー ( N ) の場合は S T 1 4 に戻る。

S T 2 7 において、次の処理 ( 1 )、( 2 ) を実行して、 S T 1 に戻る。

( 1 ) ログインしたユーザのログアウト (認証解除) 処理を実行する。

( 2 ) 利用終了情報を管理者サーバ S b に送信する。

【 0 0 8 4 】

(管理者サーバ S b の処理の説明)

(メインフローチャートの説明)

図 1 6 は実施例 2 の管理者サーバ S b のメインフローチャートである。

図 1 6 のフローチャートの各 S T (ステップ) の処理は、コンピュータ本体 H 1 のハードディスク等に記憶されたプログラムに従って行われる。また、この処理は管理者サーバ S b の他の各種処理と並行してマルチタスクで実行される。

図 1 6 に示すフローチャートは管理者サーバ S b の電源オンにより開始される。

【 0 0 8 5 】

図 1 6 の S T 6 1 において、複合機 P r 1 ~ P r 5 から送信された入力認証情報を受信

10

20

30

40

50

したか否かを判別する。ノー（N）の場合はST62に進み、イエス（Y）の場合はST64に進む。

ST62において、複合機Pr1～Pr5から送信された利用終了情報を受信したか否かを判別する。イエス（Y）の場合はST63に進み、ノー（N）の場合はST61に戻る。

ST63において、受信した利用終了情報に含まれるユーザIDと複合機Pr1～Pr5の識別情報を、利用者記憶手段C32Aから削除する。そして、ST61に戻る。

【0086】

ST64において、受信した入力認証情報のユーザIDは認証情報記憶手段C31Bに登録されているか否かを判別する。イエス（Y）の場合はST65に進み、ノー（N）の場合はST66に進む。

ST65において、受信した入力認証情報のパスワードが認証情報記憶手段C31Bに登録されているパスワードに一致するか否かを判別する。ノー（N）の場合はST66に進み、イエス（Y）の場合はST67に進む。

ST66において、ログイン不許可の情報を含む認証可否情報を、入力認証情報を送信した複合機Pr1～Pr5に送信する。

ST67において、受信した入力認証情報のユーザIDは、利用者記憶手段C32Aに未登録であるか否かを判別する。ノー（N）の場合はST68に進み、イエス（Y）の場合はST69に進む。

【0087】

ST68において、利用者記憶手段C32Aに登録されている機器（複合機）Pr1～Pr5に対して、自動ログアウト情報（強制認証解除情報）を送信する。そして、ST69に進む。

ST69において、認証されたユーザの利用権限グループ、権限変更認証情報およびログイン許可の情報を含む認証可否情報を、入力認証情報を送信した複合機Pr1～Pr5に送信する。そして、ST70に進む。

ST70において、ユーザIDとログインした（利用中の）複合機Pr1～Pr5の識別情報を利用者記憶手段C32Aに登録する。そして、ST61に戻る。

【0088】

（実施例2の作用）

前記構成を備えた実施例2の認証システムSでは、認証情報や各ユーザに設定されている利用権限グループが管理者サーバSbに記憶され、管理者により管理されている。したがって、管理しやすく、複合機Pr1～Pr5への不正アクセスにより認証情報等が漏洩することを減らすことができる。

また、管理者サーバSbにより、各複合機Pr1～Pr5で現在認証されている（ログインしている）ユーザが記憶されており、ある複合機Pr1～Pr5にログイン中のユーザが、他の複合機Pr1～Pr5からログインしようとする、元の複合機Pr1～Pr5が自動的に（強制的に）ログアウトされる。したがって、ユーザがログアウトし忘れて、別の複合機Pr1～Pr5を使用しようとした場合に、元の複合機Pr1～Pr5を自動でログアウトできるので、ログアウトし忘れた複合機Pr1～Pr5を他のユーザが操作することを減らすことができる。

その他、実施例2の認証システムSは、実施例1の認証システムSと同様の作用効果を有する。

【実施例3】

【0089】

次に本発明の実施例3の説明を行うが、この実施例3の説明において、前記実施例1、2の構成要素に対応する構成要素には同一の符号を付して、その詳細な説明を省略する。この実施例3は、下記の点で前記実施例1、2と相違しているが、他の点では前記実施例1、2と同様に構成されている。

【0090】

10

20

30

40

50

(実施例3の制御部の説明)

(画像形成装置の制御部の説明)

(実施例3のコントローラCの機能)

図17は、実施例3の管理者サーバの制御部分が備えている各機能をブロック図(機能ブロック図)で示した図であり、実施例2の図14に対応する図である。

図17において、実施例3の管理者サーバSbでは、利用者重複判別手段C32Bは、サブネットワーク一致判別手段C32B1を有する。

【0091】

C32B1:サブネットワーク一致判別手段

サブネットワーク一致判別手段C32B1は、入力認証情報により特定される利用者が利用者記憶手段C32Aに記憶されている場合に、前記利用中と記憶されている複合機Pr1~Pr5が接続されているサブネットワーク3,4と、前記入力認証情報により認証を行おうとしている電子機器が接続されているサブネットワークとが一致するか否かを判別する。実施例3サブネットワーク一致判別手段C32B1は、ログインしようとしている複合機Pr1~Pr5のIPアドレスをサブネットマスクでマスキングして得られるサブネットのネットワークアドレスが、利用者記憶手段C32Aに登録されているログイン中の複合機Pr1~Pr5のIPアドレスをサブネットマスクでマスキングして得られるサブネットのネットワークアドレスに一致するか否かを判別することにより、サブネットワークが一致するか否かを判別する。

また、これに応じて、実施例3の自動ログアウト情報送信手段C33は、前記利用者重複判別手段C32Bで利用者が重複し且つサブネットワークが一致しない場合に、利用者記憶手段C32Aに利用中と記憶されている複合機Pr1~Pr5における認証を強制的に解除する自動ログアウト情報(強制認証解除情報)を複合機(電子機器)Pr1~Pr5に送信する。

【0092】

(実施例3のフローチャートの説明)

次に、実施例3のフローチャートの説明を行うが、実施例1,2のフローチャートと同様の処理には同一のステップ(ST)番号を付し、詳細な説明は省略する。

なお、実施例3の複合機Pr1~Pr5のメインフローチャートは実施例2の図15と同様であるため詳細な説明は省略する。

(管理者サーバのメインフローチャートの説明)

図18は実施例3の管理者サーバのメインフローチャートであり、実施例2の図16に対応する図である。

図18において、実施例3のメインフローチャートは、実施例2のメインフローチャートのST67とST68の間に、下記のST71を実行する以外は実施例2のメインフローチャートと同様であるので異なる部分のみを説明し、その他の説明は省略する。

したがって、ST67でノー(N)の場合はST71に進む。

ST71において、入力認証情報を送信した複合機Pr1~Pr5のIPアドレス(識別情報)を管理者サーバSbのサブネットマスクでマスキングして得られるサブネットのネットワークアドレスと、利用者記憶手段C32Aに記憶されている利用中の複合機Pr1~Pr5のIPアドレス(識別情報)をサブネットマスクでマスキングして得られるサブネットのネットワークアドレスと、が一致するか否かを判別する。イエス(Y)の場合はST69に進み、ノー(N)の場合はST68に進む。

【0093】

(実施例3の作用)

前記構成を備えた実施例3の認証システムSでは、複数の複合機Pr1~Pr5が同一のサブネットワーク3,4に接続されている場合、複数の複合機Pr1~Pr5に同じ利用者が重複してログインすることが許可される。したがって、同一のサブネットワーク3,4に接続され、比較的近い場所に設置されていると推察される複数の複合機Pr1~Pr5を利用者が同時に使用したい場合に、これを許可することができる。例えば、一方の

複合機でコピーをしながら、他方の複合機でFAXの送信を行うといったことが許可される。この結果、1台しかログインできない場合に比べ柔軟な運用が可能となり、利便性が向上する。

その他、実施例3の認証システムSは、実施例1, 2と同様の作用効果を有する。

#### 【0094】

(変更例)

以上、本発明の実施例を詳述したが、本発明は、前記実施例に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内で、種々の変更を行うことが可能である。本発明の変更例(H01)~(H011)を下記に例示する。

(H01)前記実施例において、ネットワークN上に接続された機器の構成は、上記実施例に限定されず、ネットワークスキャナやデータベースサーバ、ワークステーション等を接続することも可能であり、各サブネットワーク3, 4に接続された画像形成装置が1台であっても問題はない。また、サブネットワークは1つとしたり、3つ以上とすることも可能である。さらに、ネットワークに接続された複合機Pr1に限定されず、プリンタサーバを介してネットワークに接続された画像形成装置、あるいは、ネットワークに接続されていない単独の画像形成装置に適用可能である。

10

#### 【0095】

(H02)前記実施例3において、サブネットワークが一致するか否かをIPアドレスとサブネットマスクに基づいて判別したが、これに限定されず、AppleTalk(登録商標)のゾーン名や、ウィンドウズ(登録商標)で使用されているワークグループ等により構成されたサブネットワークで複数に区分されるネットワークにおいて、前記ゾーン名やワークグループ名が一致するか否かに基づいて、サブネットワークが一致するか否かの判別を行うように構成することも可能である。

20

(H03)前記実施例において、各画像11~71は設計等に応じて変更可能である。

(H04)前記実施例において、コピー、プリンタ、スキャナ、FAXの全ての機能を備えた複合機を例示したが、これに限定されず、各機能のいずれか1つまたは複数を用意した画像形成装置にも適用可能である。

#### 【0096】

(H05)前記実施例において、認証方法や権限変更認証方法はユーザIDとパスワードを使用したか、これに限定されず、パスワードのみとしたり、認証情報が記憶された磁気カードやICカードを読み取る(接触型または非接触型)認証を採用したり、指紋パターンや静脈パターン、網膜パターン等により認証を行う生体認証を採用する等、任意の認証方法を採用可能である。

30

(H06)前記実施例において、利用者が重複した場合に、元の複合機を自動ログアウトさせる構成を例示したが、これに限定されず、両方をログアウトさせたり、両方に警告表示を行い、両方に再認証の入力をさせて、真の利用者でなかった方(認証できなかった方)の複合機をログアウトさせることも可能である。

#### 【0097】

(H07)前記実施例において、権限が付与される機能として、コピー、FAX, スキャナ、仕様変更を例示したが、これに限定されず、更に詳細な機能の権限、例えば、両面印刷の可否やカラーコピーの可否、使用可能な給紙トレイの制限、FAX読取り解像度の変更の可否、スキャナ読取り解像度の可否等の機能の権限とすることが可能である。

40

(H08)前記実施例において、標準権限グループよりも追加権限グループの方が権限が大きい場合を例示したが、標準権限グループの方の権限を大きくすることも可能である。

(H09)前記実施例において、利用権限グループが1つまたは2つの場合を例示したが、3つ以上設定することも可能である。

#### 【0098】

(H010)前記実施例において、機能を選択する入力がされなければ追加権限グループから標準権限グループに変更されなかったが、これに限定されず、追加権限グループに変更された時にタイマーをセットし、所定時間が経過すると、自動的に追加権限グループから

50

標準権限グループに移行するように構成することも可能である。

(H011)前記実施例において、認証装置または電子機器として画像形成装置を例示したが、これに限定されず、例えば、クライアントパソコン(情報処理装置)PCのような、新たなソフトウェアのインストール機能、特定のファイルの閲覧機能、利用者登録機能、印刷機能等の複数の機能を有する電子機器に適用することも可能である。

【図面の簡単な説明】

【0099】

【図1】図1は本発明の実施例1の認証システムの全体説明図である。

【図2】図2は、実施例1の画像形成装置としての複合機の制御部分が備えている各機能をブロック図(機能ブロック図)で示した図である。

10

【図3】図3は実施例1の認証画像の説明図である。

【図4】図4は実施例1の認証不可告知画像の説明図である。

【図5】図5は実施例1のキーボード画像の説明図であり、図5Aはひらがなを入力するためのキーボード画像の説明図、図5Bは英数字を入力するためのキーボード画像の説明図である。

【図6】図6は実施例1の機能選択画像の説明図である。

【図7】図7は実施例1の利用権限情報の説明図であり、図7Aはユーザ権限グループ管理テーブルの説明図、図7Bは権限機能管理テーブルの説明図である。

【図8】図8は実施例1の権限無し告知画像の説明図である。

【図9】図9は実施例1の再認証必要告知画像の説明図である。

20

【図10】図10は実施例1の権限変更認証不可告知画像の説明図である。

【図11】図11は実施例1の画像形成装置のメインフローチャートである。

【図12】図12は実施例1の権限判別認証処理のフローチャートであり、図11のST15, ST18, ST21, ST24のサブルーチンである。

【図13】図13は、実施例2の画像形成装置としての複合機の制御部分が備えている各機能をブロック図(機能ブロック図)で示した図であり、実施例1の図2に対応する図である。

【図14】図14は実施例2の管理者サーバの制御部分が備えている各機能をブロック図(機能ブロック図)で示した図である。

【図15】図15は実施例2の複合機のメインフローチャートであり、実施例1の図11に対応するフローチャートである。

30

【図16】図16は実施例2の管理者サーバSbのメインフローチャートである。

【図17】図17は、実施例3の管理者サーバの制御部分が備えている各機能をブロック図(機能ブロック図)で示した図であり、実施例2の図14に対応する図である。

【図18】図18は実施例3の管理者サーバのメインフローチャートであり、実施例2の図16に対応する図である。

【符号の説明】

【0100】

11...認証画像、

61...権限変更画像、

40

C4, C31...認証手段、

C4A...認証画像表示手段、

C4D, C31B...認証情報記憶手段、

C4E...入力認証情報送信手段、

C4F...認証可否情報受信手段、

C7...利用権限情報記憶手段、

C8B...追加権限機能入力判別手段、

C9...権限変更認証手段、

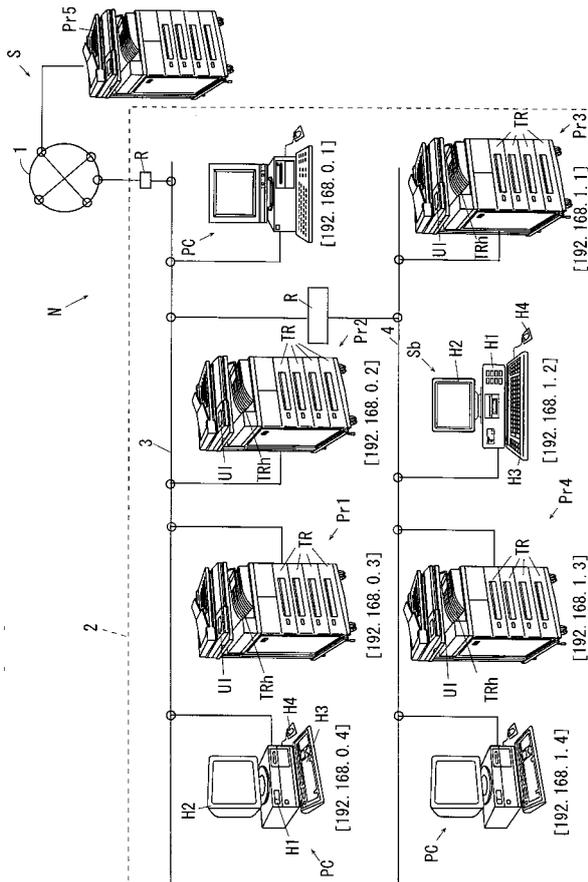
C9B...権限変更認証画像表示手段、

C9C...権限変更認証情報記憶手段、

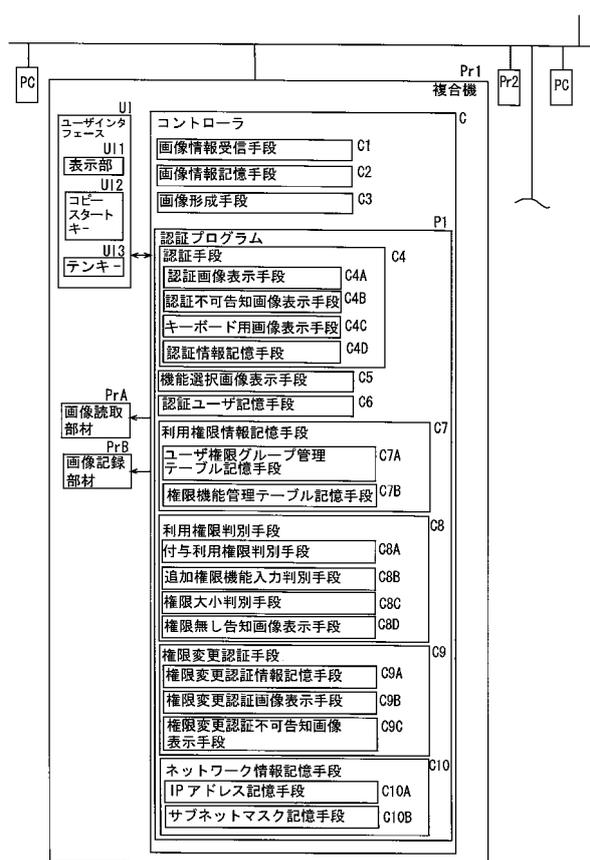
50

- C 2 1 ... 強制認証解除情報送信手段、
- C 2 2 ... 利用終了情報送信手段、
- C 3 1 A ... 入力認証情報受信手段、
- C 3 1 F ... 認証可否情報送信手段、
- C 3 2 A ... 利用者記憶手段、
- C 3 2 B ... 利用者重複判別手段、
- C 3 2 B 1 ... サブネットワーク一致判別手段、
- C 3 2 D ... 利用者登録変更手段、
- N ... ネットワーク、
- Pr 1 ... 電子機器, 画像形成装置, 認証装置, コンピュータ、
- P 1 ... 認証プログラム、
- S ... 認証システム、
- Sb ... 情報処理装置、
- UI 1 ... 情報表示画面。

【図 1】



【図 2】



【図3】

11 ユーザーIDを入力して下さい

16 ログイン

12 ユーザーID

14 キーボード

13 パスワード

キーボード

【図4】

21 ユーザーID又はパスワードが間違っています。

ユーザーIDとパスワードを確認して下さい。

22 OK

【図5】

(図5A)

32 ユーザーID ユーザーA

36 取消し

34 決定

31

37 ひらがな  
カタカナ  
英/数  
記号

33

あ	か	さ	た	な	は	ま	や	ら	わ	
い	き	し	ち	に	ひ	み	ゆ	り	を	後退
う	く	す	つ	ぬ	ふ	よ	る	ん	スペース	
え	け	せ	て	ね	へ	め	ー	れ	シフト	
お	こ	そ	と	の	ほ	も	ろ		半角変換	
入力文字	スペース									

(図5B)

(図5B)

32 ユーザーID ユーザーA

36 取消し

34 決定

31

37 ひらがな  
カタカナ  
英/数  
記号

33

1	2	3	4	5	6	7	8	9	0	~	¥	後退
q	w	e	r	t	y	u	i	o	p	@	[	スペース
caps	a	s	d	f	g	h	j	k	l	;	]	シフト
z	x	c	v	b	n	m	.	/	]			
スペース												

【図6】

47

41

メニュー

42a コピー

42b FAX

42c スキャナー

43 仕様変更

ログアウト

【図7】

(図7A) ユーザーとアクセス権限の管理テーブル

	グループ			最初の認証で付与されるアクセス権
	一般ユーザー1	一般ユーザー2	管理者	
ユーザーA	×	○	○	一般ユーザー2
ユーザーB	×	○	×	一般ユーザー2
ユーザーC	○	×	×	一般ユーザー1

(図7B)

アクセス権限と機能の管理テーブル

権限	コピー	ファックス	スキャン	仕様設定
一般ユーザー1	○	×	×	×
一般ユーザー2	○	○	○	×
管理者	×	×	×	○

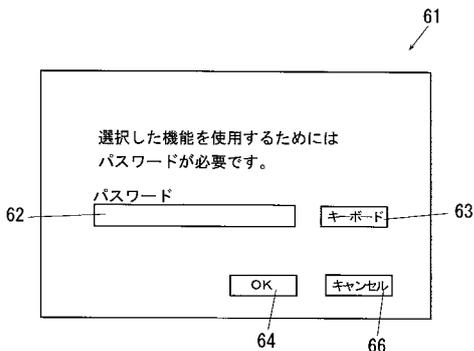
【図8】

51

ユーザーID: ユーザーA  
ではこの機能を使用する権限がありません。

52 OK

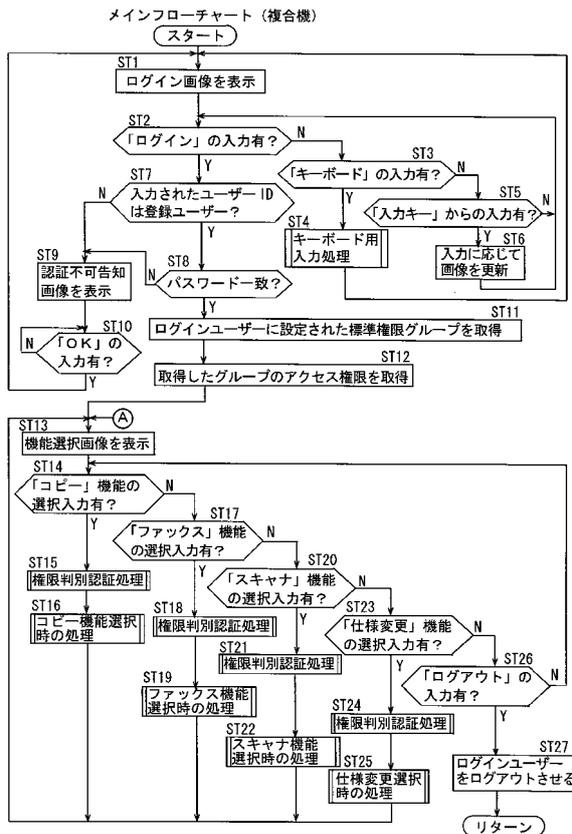
【図9】



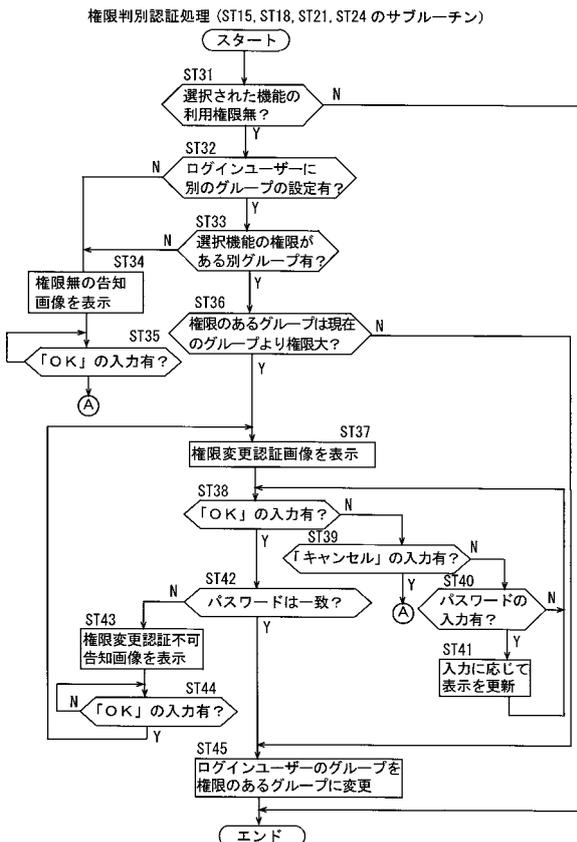
【図10】



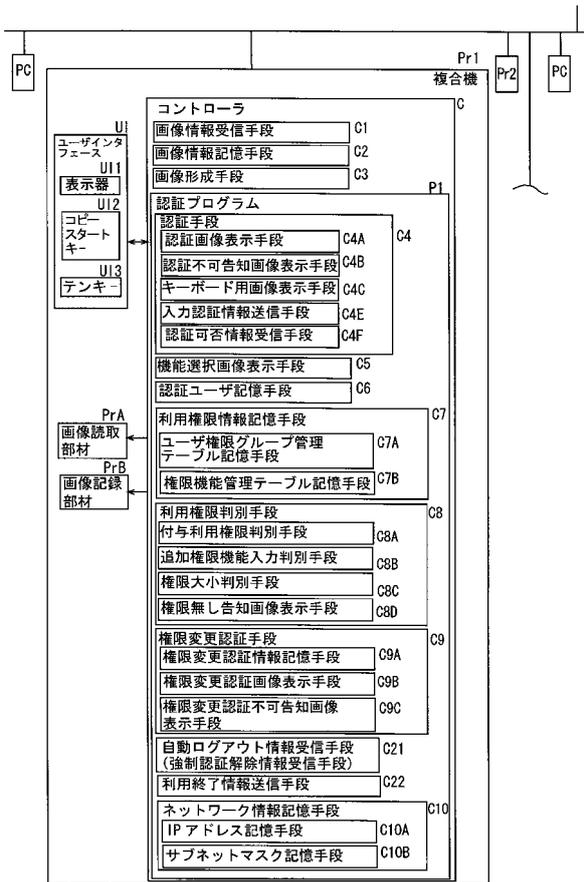
【図11】



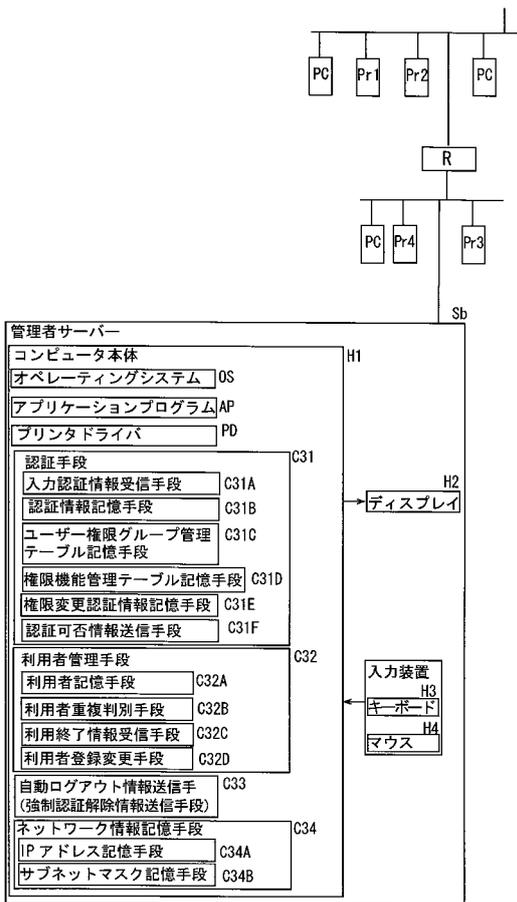
【図12】



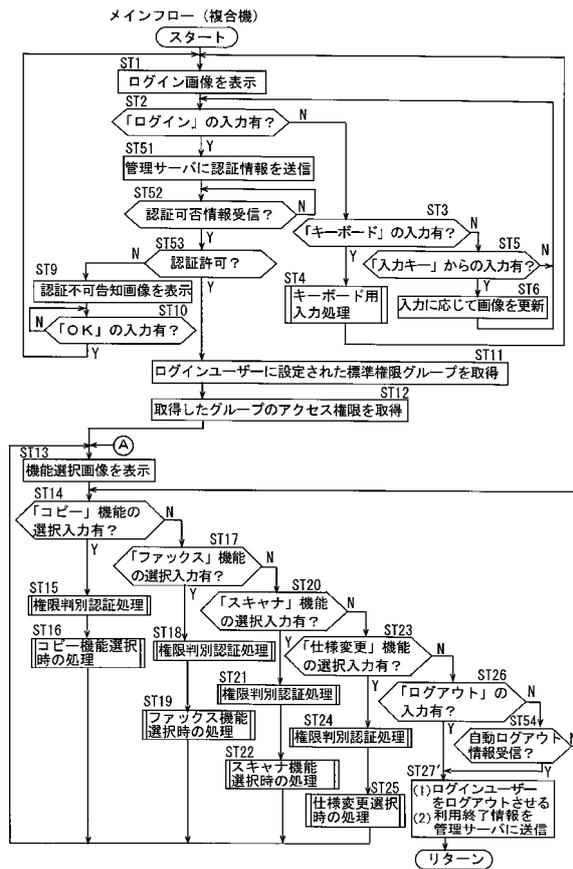
【図13】



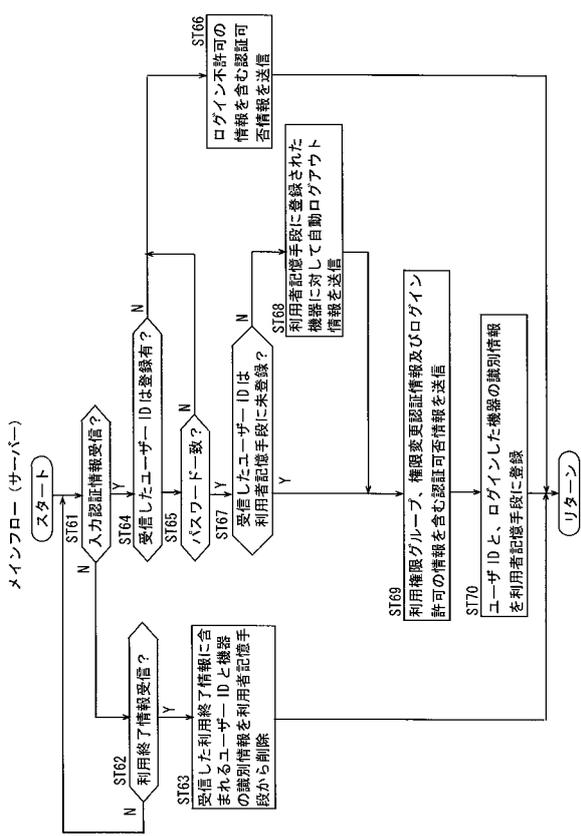
【図14】



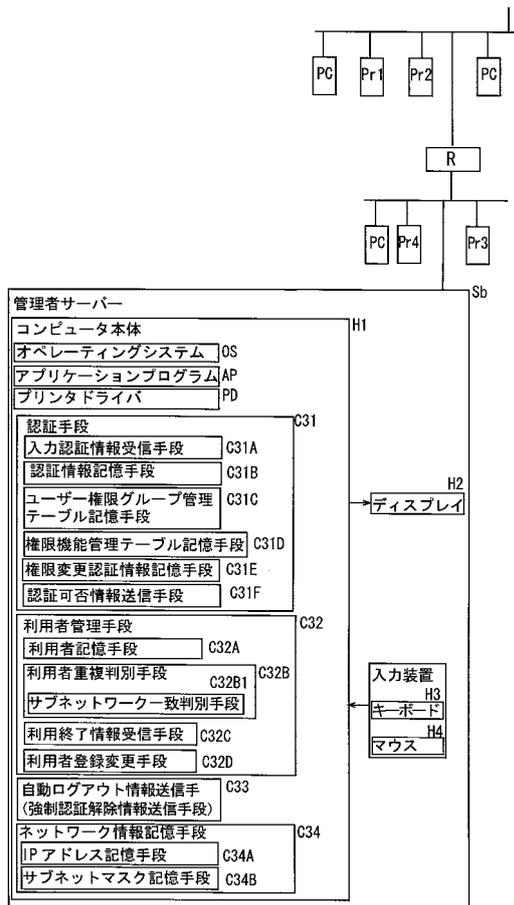
【図15】



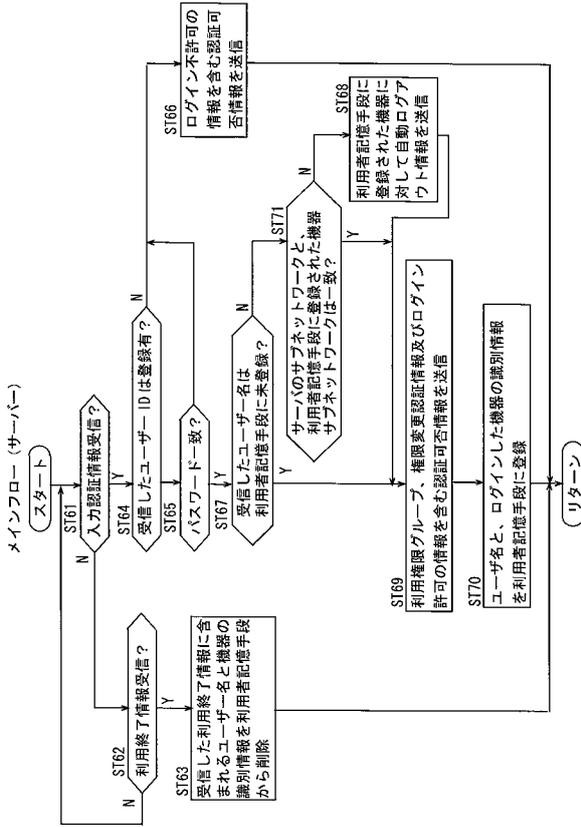
【図16】



【図17】



【 図 18 】



## フロントページの続き

(51) Int.Cl. F I  
H 0 4 N 1/44 (2006.01) H 0 4 N 1/44

(56) 参考文献 特開平 1 1 - 0 3 1 0 1 9 ( J P , A )  
特開 2 0 0 3 - 2 1 6 2 6 0 ( J P , A )  
国際公開第 2 0 0 2 / 0 0 3 2 1 5 ( W O , A 1 )  
特開平 1 0 - 2 4 0 6 9 0 ( J P , A )  
特開 2 0 0 5 - 3 1 8 5 0 3 ( J P , A )  
特開平 0 9 - 1 3 0 5 3 2 ( J P , A )  
特開平 1 0 - 1 9 8 6 2 2 ( J P , A )  
特開 2 0 0 2 - 3 5 1 8 3 1 ( J P , A )  
特開平 1 0 - 3 1 2 3 6 1 ( J P , A )

(58) 調査した分野(Int.Cl. , D B 名)

G 0 6 F 2 1 / 2 0  
B 4 1 J 2 9 / 0 0  
B 4 1 J 2 9 / 3 8  
G 0 6 F 3 / 1 2  
G 0 9 C 1 / 0 0  
H 0 4 N 1 / 4 4