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

特許第5927846号
(P5927846)

(45)発行日　平成28年6月1日(2016.6.1)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.		F I		
G06F 21/34	(2013.01)	G06F	21/34	
H04L 9/32	(2006.01)	H04L	9/00	673B
B41J 29/38	(2006.01)	B41J	29/38	Z
B41J 29/00	(2006.01)	B41J	29/00	Z
H04N 1/00	(2006.01)	H04N	1/00	C

請求項の数 12　(全 31 頁)　最終頁に続く

(21)出願番号　特願2011-241015(P2011-241015)
(22)出願日　平成23年11月2日(2011.11.2)
(65)公開番号　特開2013-97653(P2013-97653A)
(43)公開日　平成25年5月20日(2013.5.20)
審査請求日　平成26年10月20日(2014.10.20)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　滝澤　和行
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】情報処理装置、認証システム、及び認証プログラム

(57)【特許請求の範囲】
【請求項１】
認証情報を有する媒体から当該認証情報を取得する認証デバイスを識別する認証デバイス識別情報に、電子機器が有する機能の利用を制御するときの利用権限を示す利用権限情報と、当該認証デバイスから取得した認証情報に基づく認証の結果に応じて利用が制御される電子機器を識別する接続先識別情報と、が対応付けられたデバイス管理情報を保持する第１の保持手段と、
前記電子機器から、前記認証デバイス識別情報と前記接続先識別情報を受信する通信手段と、
前記デバイス管理情報のデータ操作を行い、前記認証デバイスと前記電子機器との接続関係を管理する管理手段と、
を有し、
前記管理手段は、前記通信手段が受信した前記認証デバイス識別情報及び前記接続先識別情報に基づいて、前記デバイス管理情報において、前記認証デバイスと前記電子機器との接続関係を管理することを特徴とする情報処理装置。
【請求項２】
前記管理手段は、
前記デバイス管理情報において、前記通信手段が受信した認証デバイス識別情報に対応付けて、前記通信手段が受信した接続先識別情報を登録す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】
前記管理手段は、
前記デバイス管理情報において、前記通信手段が受信した接続先識別情報と異なる接続先識別情報が、前記通信手段が受信した認証デバイス識別情報に対応付いて登録されている場合に、登録済みの接続先識別情報を、前記通信手段が受信した接続先識別情報で更新することを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記管理手段は、
前記デバイス管理情報において、前記通信手段が受信した接続先識別情報と一致する接続先識別情報が、前記通信手段が受信した認証デバイス識別情報と異なる認証デバイス識別情報に対応付いて登録されている場合に、登録済みの前記受信した接続先識別情報と前記異なる認証デバイス識別情報との接続関係を削除することを特徴とする請求項１乃至３のいずれか一項に記載の情報処理装置。
【請求項５】
前記管理手段は、前記デバイス管理情報において対応付いている前記受信した接続先識別情報及び前記異なる認証デバイス識別情報のうち、少なくともいずれかを削除することにより接続関係を削除する請求項４に記載の情報処理装置。
【請求項６】
前記通信手段が受信した前記認証デバイス識別情報及び前記接続先識別情報に基づく認証を行い、認証された場合に、前記デバイス管理情報において、受信した認証デバイス識別情報に対応付けられた利用権限情報に基づき、前記電子機器に適用する利用権限を決定する認証手段を備えることを特徴とする請求項１乃至５のいずれか一項に記載の情報処理装置。
【請求項７】
前記認証手段は、前記通信手段が受信した認証デバイス識別情報を含む前記デバイス管理情報を特定し、
前記管理手段は、前記認証手段が特定したデバイス管理情報に、前記通信手段が受信した接続先識別情報を登録することを特徴とする請求項６に記載の情報処理装置。
【請求項８】
利用者を識別する利用者識別情報と前記電子機器が有する機能の利用権限を示す利用権限情報が対応付けられた利用者管理情報を保持する第２の保持手段を有し、
前記通信手段は、前記電子機器から、前記認証デバイスから取得した認証デバイス情報と、当該電子機器を利用する利用者の利用者関連情報とを受信し、利用認証要求を受け付け、
前記認証手段は、前記通信手段が受信した認証デバイス情報と利用者関連情報に基づく認証を行い、認証された場合に、前記デバイス管理情報及び前記利用者管理情報とに基づき、認証された前記認証デバイス及び前記利用者に応じて前記電子機器に適用する利用権限を決定することを特徴とする請求項６に記載の情報処理装置。
【請求項９】
前記情報処理装置は、前記電子機器、あるいは、１台以上の前記電子機器と所定のデータ伝送路を介して接続されるサーバ装置であることを特徴とする請求項１乃至８のいずれか一項に記載の情報処理装置。
【請求項１０】
前記認証手段は、前記利用権限の適用を制御する制御設定に従って、前記デバイス管理情報から特定した利用権限情報及び前記利用者管理情報から特定した利用者権限情報のうち、優先順位の高い利用権限情報を特定し、特定した利用権限情報に基づき、前記電子機器に適用する利用権限を決定することを特徴とする請求項８に記載の情報処理装置。
【請求項１１】
コンピュータが電子機器の利用認証を行う認証システムであって、
前記コンピュータを、

認証情報を有する媒体から当該認証情報を取得する認証デバイスを識別する認証デバイス識別情報に、電子機器が有する機能の利用を制御するときの利用権限を示す利用権限情報と、当該認証デバイスから取得した認証情報に基づく認証の結果に応じて利用が制御される電子機器を識別する接続先識別情報と、が対応付けられたデバイス管理情報を保持する第１の保持手段、

前記電子機器から、前記認証デバイス識別情報と前記接続先識別情報を受信する通信手段、及び

前記デバイス管理情報のデータ操作を行い、前記認証デバイスと前記電子機器との接続関係を管理する管理手段、

として機能させ、

前記管理手段は、前記通信手段が受信した前記認証デバイス識別情報及び前記接続先識別情報に基づいて、前記デバイス管理情報において、前記認証デバイスと前記電子機器との接続関係を管理することを特徴とする認証プログラムと、

前記コンピュータと通信を行う第１の通信手段、及び

自機に接続される前記認証デバイスから、前記認証デバイス識別情報を取得する取得手段、

を有し、

前記第１の通信手段が、前記コンピュータに、前記取得手段で取得した前記認証デバイス識別情報、及び自機を識別する前記接続先識別情報を送信する前記電子機器と、

を備えることを特徴とする認証システム。

【請求項１２】

認証情報を有する媒体から当該認証情報を取得する認証デバイスを識別する認証デバイス識別情報に、電子機器が有する機能の利用を制御するときの利用権限を示す利用権限情報と、当該認証デバイスから取得した認証情報に基づく認証の結果に応じて利用が制御される電子機器を識別する接続先識別情報と、が対応付けられたデバイス管理情報を保持する第１の保持手段と、

前記電子機器から、前記認証デバイス識別情報と前記接続先識別情報を受信する通信手段と、

前記デバイス管理情報のデータ操作を行い、前記認証デバイスと前記電子機器との接続関係を管理する管理手段と、

としてコンピュータを機能させ、

前記管理手段は、前記通信手段が受信した前記認証デバイス識別情報及び前記接続先識別情報に基づいて、前記デバイス管理情報において、前記認証デバイスと前記電子機器との接続関係を管理することを特徴とする認証プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子機器の利用認証を行う技術に関するものである。

【背景技術】

【０００２】

例えば、特許文献１には、認証サーバが、カードに記憶された利用者情報と画像処理装置の機器情報とを用いて、利用認証を行う技術が開示されている。このような技術により、画像処理装置では、機能利用が制御される。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

しかしながら、従来の方法では、利用認証に用いる情報の管理作業が煩雑である。

例えば、同一利用者に対して、画像処理装置ごとに異なる利用権限を適用したい場合、利用者、画像処理装置、及び適用する利用権限を紐付けて管理する必要があり、その作業は煩雑である。また、特許文献１に開示されるように、利用者と画像処理装置を紐付けて

管理している場合、新規導入、入れ替え、又は撤去などにより、機器構成が変更されると、利用者と画像処理装置を紐付け直す必要があり、その作業は煩雑である。このように、機器情報を用いる利用認証では、用いる情報の管理に手間がかかる。

【０００４】

本発明は上記従来技術の問題点を鑑み提案されたものであり、機器利用認証に用いる情報管理の手間を軽減できる情報処理装置、認証システム、及び認証プログラムを提供することにある。

【課題を解決するための手段】

【０００５】

上記目的を達成するため、本発明に係る情報処理装置は、認証情報を有する媒体から当該認証情報を取得する認証デバイスを識別する認証デバイス識別情報に、電子機器が有する機能の利用を制御するときの利用権限を示す利用権限情報と、当該認証デバイスから取得した認証情報に基づく認証の結果に応じて利用が制御される電子機器を識別する接続先識別情報と、が対応付けられたデバイス管理情報を保持する第１の保持手段と、前記電子機器から、前記認証デバイス識別情報と前記接続先識別情報を受信する通信手段と、前記デバイス管理情報のデータ操作を行い、前記認証デバイスと前記電子機器との接続関係を管理する管理手段と、を有し、前記管理手段は、前記通信手段が受信した前記認証デバイス識別情報及び前記接続先識別情報に基づいて、前記デバイス管理情報において、前記認証デバイスと前記電子機器との接続関係を管理することを特徴とする。

【発明の効果】

【０００６】

本発明によれば、機器利用認証に用いる情報管理の手間を軽減可能な情報処理装置、認証システム、及び認証プログラムを提供することができる。

【図面の簡単な説明】

【０００７】

【図１】本発明の第１の実施形態に係る認証システムの構成例を示す図である。

【図２】本発明の第１の実施形態に係る認証サーバのハードウェア構成例を示す図である。

【図３】本発明の第１の実施形態に係る画像処理装置のハードウェア構成例を示す図である。

【図４】本発明の第１の実施形態に係る認証機能の構成例を示す図である。

【図５】本発明の第１の実施形態に係るデバイス管理情報のデータ例を示す図である。

【図６】本発明の第１の実施形態に係る認証の処理手順例を示すフローチャートである。

【図７】本発明の変形例に係るデバイス管理情報のデータ例を示す図である。

【図８】本発明の変形例に係る認証サーバにおける処理手順例（その１）を示すフローチャートである。

【図９】本発明の変形例に係るデバイス管理情報のデータ遷移例（その１）を示す図である。

【図１０】本発明の変形例に係るデバイス管理情報のデータ遷移例（その２）を示す図である。

【図１１】本発明の変形例に係るデバイス管理情報のデータ遷移例（その３）を示す図である。

【図１２】本発明の変形例に係る認証サーバにおける処理手順例（その２）を示すフローチャートである。

【図１３】本発明の変形例に係るデバイス管理情報のデータ遷移例（その４）を示す図である。

【図１４】本発明の変形例に係るデバイス管理情報のデータ遷移例（その５）を示す図である。

【図１５】本発明の変形例に係るデバイス管理情報のデータ遷移例（その６）を示す図である。

【図１６】本発明の第２の実施形態に係る認証機能の構成例を示す図である。
【図１７】本発明の第２の実施形態に係る利用者管理情報のデータ例を示す図である。
【図１８】本発明の第２の実施形態に係る制御設定の画面例を示す図である。
【図１９】本発明の第２の実施形態に係る認証サーバにおける処理手順例を示すフローチャートである。
【図２０】本発明の第２の実施形態に係る利用権限の適用処理手順例を示すフローチャートである。
【図２１】本発明の変形例に係る認証機能の構成例（その１）を示す図である。
【図２２】本発明の変形例に係る認証機能の構成例（その２）を示す図である。
【発明を実施するための形態】
【０００８】
以下、本発明の好適な実施の形態（以下「実施形態」という）について、図面を用いて詳細に説明する。
【０００９】
［第１の実施形態］
＜システム構成＞
図１は、本実施形態に係る認証システム１の構成例を示す図である。
図１には、１又は複数の画像処理装置２００$_1$～２００$_n$（以下総称する場合「画像処理装置２００」という）と認証サーバ１００が、所定のデータ伝送路Ｎ（例えば「ＬＡＮ：Local Area Network」）に接続されるシステム構成例が示されている。
【００１０】
画像処理装置２００は、印刷を含む画像処理機能を有する電子機器であり、プリンタやＭＦＰ（Multifunction Peripheral）などである。認証サーバ１００は、画像処理装置２００が有する機能の利用権限を管理し、画像処理装置２００の利用認証を行う認証機能を有する情報処理装置である。
【００１１】
画像処理装置２００は、自機に接続される認証デバイスを介して、利用者からの利用認証の指示を受け付けると、認証デバイス情報を含む認証情報を認証サーバ１００に送信し、利用認証を要求する。これを受けて認証サーバ１００は、受信した認証情報に基づき、画像処理装置２００の利用認証を行い、画像処理装置２００が有する機能の利用権限を認証結果として応答する。その結果、画像処理装置２００では、応答された利用権限に従って、自機が有する機能の機能利用（許可／不許可）を制御し、制御結果に基づき、操作画面を表示する。
【００１２】
以上のように、本実施形態に係る認証システム１は、画像処理装置２００の利用認証を行う認証サービスを提供することができる。
【００１３】
＜ハードウェア構成＞
《認証サーバ》
図２は、本実施形態に係る認証サーバ１００のハードウェア構成例を示す図である。
図２に示すように、認証サーバ１００は、入力装置１０１、表示装置１０２、外部Ｉ／Ｆ１０３、ＲＡＭ（Random Access Memory）１０４、ＲＯＭ（Read Only Memory）１０５、ＣＰＵ（Central Processing Unit）１０６、通信Ｉ／Ｆ１０７、及びＨＤＤ（Hard Disk Drive）１０８などを備え、それぞれがバスＢで相互に接続されている。
【００１４】
入力装置１０１は、キーボードやマウスなどを含み、認証サーバ１００に各操作信号を入力するのに用いられる。表示装置１０２は、ディスプレイなどを含み、認証サーバ１００による処理結果を表示する。
【００１５】
通信Ｉ／Ｆ１０７は、認証サーバ１００をネットワークに接続するインタフェースであ

る。これにより、認証サーバ１００は、通信Ｉ／Ｆ１０７を介して、他の機器（画像処理装置）とデータ通信を行うことができる。

【００１６】

ＨＤＤ１０８は、プログラムやデータを格納している不揮発性の記憶装置である。格納されるプログラムやデータには、装置全体を制御する基本ソフトウェアであるＯＳ（Operating System）、及びＯＳ上において各種機能を提供するアプリケーションソフトウェアなどがある。また、ＨＤＤ１０８は、格納しているプログラムやデータを、所定のファイルシステム及び／又はＤＢ（Data Base）により管理している。

【００１７】

外部Ｉ／Ｆ１０３は、外部装置とのインタフェースである。外部装置には、記録媒体１０３ａなどがある。これにより、認証サーバ１００は、外部Ｉ／Ｆ１０３を介して、記録媒体１０３ａの読み取り及び／又は書き込みを行うことができる。記録媒体１０３ａには、フロッピー（商標又は登録商標）ディスク、ＣＤ（Compact Disk）、及びＤＶＤ（Digital Versatile Disk）、ならびに、ＳＤメモリカード（SD Memory card）やＵＳＢメモリ（Universal Serial Bus memory）などがある。

【００１８】

ＲＯＭ１０５は、電源を切っても内部データを保持することができる不揮発性の半導体メモリ（記憶装置）である。ＲＯＭ１０５には、認証サーバ１００の起動時に実行されるＢＩＯＳ（Basic Input/Output System）、ＯＳ設定、及びネットワーク設定などのプログラムやデータが格納されている。ＲＡＭ１０４は、プログラムやデータを一時保持する揮発性の半導体メモリ（記憶装置）である。ＣＰＵ１０６は、上記記憶装置（例えば「ＨＤＤ」や「ＲＯＭ」など）から、プログラムやデータをＲＡＭ上に読み出し、処理を実行することで、装置全体の制御や搭載機能を実現する演算装置である。

【００１９】

以上のように、本実施形態に係る認証サーバ１００は、上記ハードウェア構成により、機器利用認証を含む各種情報処理サービスを提供することができる。

【００２０】

《画像処理装置》

図３は、本実施形態に係る画像処理装置２００のハードウェア構成例を示す図である。

図３に示すように、画像処理装置２００は、コントローラ２１０、操作パネル２２０、プロッタ２３０、及びスキャナ２４０などを備え、それぞれが相互にバスＢで接続されている。

【００２１】

操作パネル２２０は、表示部及び入力部を備えており、機器情報などの各種情報をユーザに提供したり、動作設定や動作指示などの各種利用者操作を受け付けたりする。プロッタ２３０は、画像形成部を備えており、用紙に出力画像を形成する。出力画像を形成する方式には、例えば、電子写真プロセスやインクジェット方式などがある。スキャナ２４０は、原稿を光学的に読み取り、読み取り画像を生成する。

【００２２】

コントローラ２１０は、ＣＰＵ２１１、記憶装置２１２、通信Ｉ／Ｆ２１３、及び外部Ｉ／Ｆ２１４などを備えており、それぞれが相互にバスＢで接続されている。

【００２３】

ＣＰＵ２１１、通信Ｉ／Ｆ２１３、及び外部Ｉ／Ｆ２１４は、上記認証サーバ１００が備えるＣＰＵ１０６、通信Ｉ／Ｆ１０７、及び外部Ｉ／Ｆ１０３と同様である。また、記憶装置２１２は、プログラムや各種データ（例えば「画像データ」）を格納し保持する。記憶装置２１２には、ＲＡＭ１０４、ＲＯＭ１０５、及びＨＤＤ１０８などがある。

【００２４】

以上のように、本実施形態に係る画像処理装置２００では、上記ハードウェア構成により、印刷を含む画像処理サービスを提供することができる。

【００２５】

なお、本実施形態に係る画像処理装置２００は、外部Ｉ／Ｆ２１４を介して、認証デバイス２１４ｂの読み取りを行うことができる。認証デバイス２１４ｂには、所定の記憶領域に情報（認証情報）を保持する電子記録媒体（例えば「ＩＣカード（Integrated Circuit card）」）を接触／非接触で読み取り可能な装置などがある。よって、本実施形態に係る画像処理装置２００では、機器利用認証に必要な情報を取得することができる。

【００２６】

＜認証機能＞

本実施形態に係る認証機能について説明する。

本実施形態に係る認証システム１では、画像処理装置２００が、自機に接続された（接続検知した）認証デバイス２１４ｂから認証デバイス情報を取得し、取得した認証デバイス情報を認証サーバ１００に送信し、利用認証を要求する。認証サーバ１００は、受信した認証デバイス情報に基づき、該認証デバイス情報に対応付けて管理している画像処理装置２００の利用権限情報を取得する。認証サーバ１００は、取得した利用権限情報に基づき、画像処理装置２００に適用する利用権限を決定する。認証サーバ１００は、決定した利用権限を含む認証結果を送信し、利用認証要求に応答する。画像処理装置２００は、受信した認証結果に含まれる利用権限に従って、機能利用を制御する。本実施形態に係る認証システム１は、このような認証機能を有している。

【００２７】

従来のように、画像処理装置２００の機器情報を用いる利用認証では、例えば、機器ごとに利用権限を制御したい場合や機器構成が変更された場合、利用認証に用いる情報の管理が煩雑であった。

【００２８】

そこで、本実施形態に係る認証サーバ１００では、画像処理装置２００に接続される認証デバイス２１４ｂと画像処理装置２００が有する機能の利用権限を対応付けて管理する仕組みとした。

【００２９】

これにより、本実施形態に係る認証システム１は、画像処理装置２００に依存しない情報を用いて、画像処理装置２００の利用認証が可能な環境を提供する。その結果、本実施形態に係る認証システム１では、機器利用認証に用いる情報管理の手間を軽減できる。

【００３０】

以下に、本実施形態に係る認証機能の構成とその動作について説明する。

図４は、本実施形態に係る認証機能の構成例を示す図である。

図４に示すように、本実施形態に係る認証機能は、ＵＩ（User Interface）制御部１１、情報管理部１２、機器通信部１３、認証部１４、認証デバイス通信部２１、認証サーバ通信部２２、及びＵＩ制御部２３などを有している。

【００３１】

ＵＩ制御部１１、情報管理部１２、機器通信部１３、及び認証部１４は、認証サーバ１００が有する機能部である。認証デバイス通信部２１、認証サーバ通信部２２、及びＵＩ制御部２３は、画像処理装置２００が有する機能部である。

【００３２】

このように、本実施形態に係る認証機能は、各機器が有する上記機能部が連携動作することで実現される。

【００３３】

《画像処理装置》

認証デバイス通信部２１は、認証デバイス２１４ｂと通信を行う機能部である。認証デバイス通信部２１は、外部Ｉ／Ｆ２１４を介して、画像処理装置２００に接続される認証デバイス２１４ｂを検知する。認証デバイス通信部２１は、検知した認証デバイス２１４ｂを介して、利用者からの利用認証の指示を受け付けると（認証用のＩＣカードを読み取ると）、認証デバイス２１４ｂから認証デバイス情報（認証デバイスの識別子を含む固有情報）を取得する。

【００３４】
認証サーバ通信部２２は、認証サーバ１００と通信を行う機能部である。認証サーバ通信部２２は、通信Ｉ／Ｆ２１３を介して、認証サーバ１００と通信を行う。認証サーバ通信部２２は、認証デバイス通信部２１が取得した認証デバイス情報を含む認証情報を認証サーバ１００に送信し、利用認証を要求する。その結果、認証サーバ通信部２２は、認証サーバ１００から応答された認証結果を受信する。具体的には、認証サーバ１００が機能利用を認証した場合には、画像処理装置２００に適用する利用権限（機能利用の許可／不許可を示す利用権限値）を受信する。一方、認証サーバ１００が機能利用を認証しなかった場合には、認証されなかった旨のエラー通知を受信する。
【００３５】
ＵＩ制御部２３は、操作画面を含むＵＩを制御する機能部である。ＵＩ制御部２３は、認証サーバ通信部２２が受信した認証結果に基づき、自機が有する機能の利用許可／不許可を制御し、制御結果に基づき、操作画面を表示する。具体的には、認証サーバ１００から受信した利用権限に従って、利用許可機能のＧＵＩ（Graphical UI）を表示し、利用不許可機能（利用禁止機能）のＧＵＩを非表示とする。また、認証サーバ１００から受信したエラー通知に基づき、エラー内容（認証エラー）を表示する。
【００３６】
このように、画像処理装置２００では、利用認証要求に対して、認証サーバ１００から応答された認証結果に含まれる利用権限に従って、自機が有する機能利用を制御する。
【００３７】
《認証サーバ》
ＵＩ制御部１１は、操作画面を含むＵＩを制御する機能部である。ＵＩ制御部１１は、画像処理装置２００に接続される認証デバイス２１４ｂと画像処理装置２００が有する機能の利用権限を対応付ける入力値を受け付けるＧＵＩを操作画面として表示する。
【００３８】
情報管理部１２は、画像処理装置２００に接続される認証デバイス２１４ｂと画像処理装置２００が有する機能の利用権限を対応付けて管理する機能部である。情報管理部１２は、所定のデータ操作により、デバイス管理情報保持部９０にアクセスし、認証デバイス２１４ｂと利用権限とが対応付けられたデバイス管理情報を管理する。なお、デバイス管理情報保持部９０は、認証サーバ１００が備える記憶装置の所定の記憶領域にあたる。
【００３９】
ここで、デバイス管理情報について説明する。
図５は、本実施形態に係るデバイス管理情報９０Ｄのデータ例を示す図である。
図５に示すように、デバイス管理情報９０Ｄは、認証デバイス識別及び利用権限などの各情報項目が対応付けられた１又は複数の情報セットを含み、該情報セットが認証デバイス単位で管理される。
【００４０】
［認証デバイス識別］項目は、画像処理装置２００に接続される認証デバイス２１４ｂを識別する認証デバイス識別情報を保持する項目であり、項目値には、認証デバイス２１４ｂにユニークに割り当てられた識別子（認証デバイスＩＤ）などがある。［利用権限］項目は、画像処理装置２００が有する機能の利用権限が設定された利用権限情報を保持する項目であり、項目値には、機能ごとの利用許可／不許可を示す利用権限値（許可："○"／不許可："×"）などがある。
【００４１】
図４の説明に戻る。情報管理部１２は、上記デバイス管理情報９０Ｄの各情報項目値を、次のようにして設定・登録する。情報管理部１２は、ＵＩ制御部１１から設定・登録指示を受け付けると、デバイス管理情報保持部９０にアクセスし、設定・登録指示時に受け取った入力値を、参照したデバイス管理情報９０Ｄの該当情報項目値に設定・登録する。具体的には、認証デバイス２１４ｂに対応する入力値を［認証デバイス識別］項目値に設定・登録する。また、画像処理装置２００が有する機能の利用権限に対応する入力値を［

利用権限］項目値に設定・登録する。

【００４２】

また、情報管理部１２は、上記デバイス管理情報９０Ｄの各情報項目値を、次のようにして更新する。情報管理部１２は、ＵＩ制御部１１から更新指示を受け付けると、デバイス管理情報保持部９０にアクセスし、更新指示時に受け取った入力値で、参照したデバイス管理情報９０Ｄの該当情報項目値を更新する。具体的には、認証デバイス２１４ｂに対応する入力値で［認証デバイス識別］項目値を更新する。また、画像処理装置２００が有する機能の利用権限に対応する入力値で［利用権限］項目値を更新する。

【００４３】

このように、認証サーバ１００には、管理者などが、認証システム１の運用方針などに基づき、利用認証の対象機器である画像処理装置２００に接続される認証デバイス２１４ｂと画像処理装置２００が有する機能の利用権限を、予め対応付けて設定しておく。

【００４４】

機器通信部１３は、画像処理装置２００と通信を行う機能部である。機器通信部１３は、通信Ｉ／Ｆ１０７を介して、画像処理装置２００と通信を行う。機器通信部１３は、画像処理装置２００（認証サーバ通信部）から認証デバイス情報を含む認証情報を受信し、利用認証の要求を受け付けると、後述する認証部１４に利用認証の実行を指示する。このとき、機器通信部１３は、受信した認証デバイス情報を含む認証情報を認証部１４に渡す。その結果、機器通信部１３は、後述する認証部１４から受け取った認証結果を画像処理装置２００（認証サーバ通信部）に送信する。具体的には、認証部１４が機能利用を認証した場合には、画像処理装置２００に適用する利用権限を受け取り、送信する。一方、認証部１４が機能利用を認証しなかった場合には、認証されなかった旨のエラー内容を受け取り、送信する。

【００４５】

認証部１４は、画像処理装置２００の利用認証を行う機能部である。認証部１４は、機器通信部１３から利用認証の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った認証デバイス情報を含む認証情報に基づき、デバイス管理情報９０Ｄを参照し、画像処理装置２００が有する機能の利用認証を行う。認証部１４は、受け取った認証デバイス情報の認証デバイス識別情報に基づき、参照したデバイス管理情報９０Ｄの該当情報セットを特定する。認証部１４は、特定した情報セットの利用権限情報に基づき、画像処理装置２００に適用する利用権限を決定する。具体的には、認証部１４は、画像処理装置２００が有する機能に対して、利用を許可する機能／利用を許可しない機能を決定する。認証部１４は、決定結果に基づき、適用する利用権限を含む認証結果を生成し、機器通信部１３に生成した認証結果を渡し、利用認証要求元への応答を指示する。

【００４６】

なおこのとき、認証部１４は、特定した情報セットの［利用権限］項目値に、１つ以上の利用許可値が設定されている場合に、機能利用を認証し、機能利用の許可／不許可を制御する利用権限値を含む認証結果を生成する。一方、認証部１４は、特定した情報セットの［利用権限］項目値の全てに、利用不許可値が設定されている場合に、機能利用を認証せず、エラー内容を示すエラー値を含む認証結果を生成する。また、認証部１４は、受け取った認証デバイス情報の認証デバイス識別情報に基づき、参照したデバイス管理情報９０Ｄの該当情報セットを特定できなかった場合も、機能利用を認証しない。

【００４７】

このように、認証サーバ１００では、画像処理装置２００からの利用認証要求に対して、機能利用の許可／不許可を制御する利用権限値を含む認証結果を応答する。

【００４８】

以上のように、本実施形態に係る認証機能は、上記各機能部が連携動作することにより実現される。なお、上記各機能部は、システム１を構成する各機器に搭載（インストール）されるプログラム（認証機能を実現するソフトウェア）が、演算装置（ＣＰＵ）により、記憶装置（「ＨＤＤ」や「ＲＯＭ」）からメモリ（ＲＡＭ）上に読み出され、各機器に

おいて、以下の処理が実行されることで実現される。

【００４９】

本実施形態に係る認証機能の詳細な動作（機能部群の連携動作）について、処理手順を示すフローチャートを用いて説明する。

【００５０】

図６は、本実施形態に係る認証の処理手順例を示すフローチャートである。（Ａ）には、画像処理装置２００で実行される処理、（Ｂ）には、認証サーバ１００で実行される処理が示されている。

【００５１】

《画像処理装置の主な処理》

図６（Ａ）に示すように、画像処理装置２００は、認証デバイス通信部２１が、画像処理装置２００に接続される認証デバイス２１４ｂを介して、利用者からの利用認証の指示を受け付けると（ステップＳ１０１：ＹＥＳ）、認証デバイス２１４ｂから認証デバイス識別情報を含む認証デバイス情報を取得する（ステップＳ１０２）。

【００５２】

画像処理装置２００は、認証デバイス情報の取得を受けて、認証サーバ通信部２２が、通信Ｉ／Ｆ２１３を介して、認証デバイス通信部２１が取得した認証デバイス情報を含む認証情報を認証サーバ１００に送信し、利用認証を要求する（ステップＳ１０３）。

【００５３】

その結果、画像処理装置２００は、認証サーバ１００から、利用権限（機能利用の許可／不許可を制御する利用権限値）を含む認証結果を受信するまで待つ（ステップＳ１０４：ＮＯ）。

【００５４】

画像処理装置２００は、認証サーバ通信部２２が、認証サーバ１００から認証結果を受信すると（ステップＳ１０４：ＹＥＳ）、受信した認証結果をＵＩ制御部２３に渡し、操作画面の制御を指示する。

【００５５】

画像処理装置２００は、ＵＩ制御部２３が、操作画面の制御指示を受け付けると、受け取った認証結果に基づき、利用認証されたか否かを判定する（ステップＳ１０５）。

【００５６】

画像処理装置２００は、ＵＩ制御部２３が、利用認証されたと判定した場合（ステップＳ１０５：ＹＥＳ）、制御指示時に受け取った利用権限に従って、自機が有する機能の利用許可／不許可を制御する（ステップＳ１０６）。

【００５７】

その結果、画像処理装置２００は、ＵＩ制御部２３が、制御結果に基づき、操作画面を表示する（表示内容を更新する：ステップＳ１０７）。このとき、ＵＩ制御部２３は、利用許可機能のＧＵＩを表示し、利用不許可機能のＧＵＩを非表示とする。

【００５８】

また、画像処理装置２００は、ＵＩ制御部２３が、利用認証されなかった判定した場合（ステップＳ１０５：ＮＯ）、エラー内容（認証エラー）を表示する。

【００５９】

《認証サーバの主な処理》

図６（Ｂ）に示すように、認証サーバ１００は、機器通信部１３が、通信Ｉ／Ｆ１０７を介して、画像処理装置２００（認証サーバ通信部）から認証デバイス情報を含む認証情報を受信し、利用認証の要求を受け付けると（ステップＳ２０１：ＹＥＳ）、受信した認証情報を認証部１４に渡し、利用認証の実行を指示する。

【００６０】

認証サーバ１００は、認証部１４が、利用認証の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし（ステップＳ２０２）、受け取った認証情報を含まれる認証デバイス情報の認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参照する（

ステップＳ２０３）。
【００６１】
認証サーバ１００は、認証部１４が、参照したデバイス管理情報９０Ｄの中に該当デバイス管理情報９０Ｄが存在する（該当情報セットが特定できた）か否かを判定し（ステップＳ２０４）、画像処理装置２００が有する機能の利用認証を行う。
【００６２】
その結果、認証サーバ１００は、認証部１４が、該当デバイス管理情報９０Ｄが存在すると判定した場合（ステップＳ２０４：ＹＥＳ）、該当デバイス管理情報９０Ｄ（特定した情報セット）の利用権限情報に基づき、画像処理装置２００が有する機能に対して、利用を許可する機能／利用を許可しない機能を決定する（ステップＳ２０５）。
【００６３】
認証サーバ１００は、認証部１４が、決定した利用権限に従って、認証結果（適用する利用権限を含む認証結果）を生成する（ステップＳ２０６）。このとき、認証部１４は、特定した情報セットの［利用権限］項目値に、１つ以上の利用許可値が設定されている場合に、機能利用を認証し、機能利用の許可／不許可を制御する利用権限値を含む認証結果を生成する。
【００６４】
例えば、認証部１４が、機器通信部１３から受け取った認証デバイス情報の認証デバイス識別情報"１２３"に基づき、図５に示すデバイス管理情報９０Ｄを参照した場合には、次のように認証結果を生成する。認証部１４は、特定した情報セットの［利用権限］項目値に、１つ以上の利用権限値"○"が設定されていることから、機能利用を認証する。認証部１４は、プリント及びコピー機能を、利用を許可する機能に決定し、スキャン及びファックス機能を、利用を許可しない機能に決定する。認証部１４は、決定結果に基づき、プリント及びコピー機能利用の許可／スキャン及びファックス機能利用の不許可を制御する利用権限値（プリント："○"，コピー："○"，スキャン："×"，ファックス："×"）を含む認証結果を生成する。なお、認証部１４は、特定した情報セットの［利用権限］項目値の全てに、利用不許可値"×"が設定されている場合に、機能利用を認証せず、エラー内容を示すエラー値を含む認証結果を生成する。認証部１４は、このようにして生成した認証結果を機器通信部１３に渡し、利用認証要求元への応答を指示する。
【００６５】
認証サーバ１００は、機器通信部１３が、応答指示を受け付けると、受け取った認証結果（機能利用の許可／不許可を制御する利用権限値）を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ２０７）。
【００６６】
また、認証サーバ１００は、認証部１４が、該当デバイス管理情報９０Ｄが存在しないと判定した場合（ステップＳ２０４：ＮＯ）、機能利用を認証しなかった旨（認証エラー）を示すエラー値を含む認証結果を生成し、機器通信部１３に渡し、利用認証要求元へのエラー通知を指示する。
【００６７】
認証サーバ１００は、機器通信部１３が、通知指示を受け付けると、受け取った認証結果（認証エラー）を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ２０８）。
【００６８】
＜まとめ＞
以上のように、本実施形態に係る認証システム１によれば、画像処理装置２００は、認証デバイス通信部２１により、自機に接続された（接続検知した）認証デバイス２１４ｂから認証デバイス情報を取得する。画像処理装置２００は、認証サーバ通信部２２により、取得された認証デバイス情報を認証サーバ１００に送信し、利用認証を要求する。
【００６９】
これを受けて認証サーバ１００は、機器通信部１３により、認証デバイス情報を受信し

、認証部１４により、受信した認証デバイス情報に基づき、該認証デバイス情報に対応付けて管理している画像処理装置２００の利用権限情報を取得する。認証部１４は、取得した利用権限情報に基づき、画像処理装置２００に適用する利用権限を決定する。認証サーバ１００は、機器通信部１３により、決定した利用権限を含む認証結果を送信し、利用認証要求に応答する。

【００７０】

その結果、画像処理装置２００は、認証サーバ通信部２２により、認証結果を受信し、ＵＩ制御部２３により、認証結果に含まれる利用権限に従って、機能利用を制御する。

【００７１】

これによって、本実施形態に係る認証システム１は、画像処理装置２００に依存しない情報を用いて、画像処理装置２００の利用認証が可能な環境を提供できる。そのため、機器ごとに利用権限を制御したい場合や機器構成が変更された場合であっても、機器利用認証に用いる情報管理の手間を軽減できる。具体的には、機器ごとに利用権限を制御したい場合には、認証サーバ１００で利用権限を設定した認証デバイス２１４ｂを、利用権限を適用する画像処理装置ごとに接続するだけでよい。また、機器構成が変更された場合には、新規導入された画像処理装置２００又は入れ替えられた画像処理装置２００に認証デバイス２１４ｂを接続するだけでよい。

【００７２】

［変形例］

例えば、認証システム１では、システム運用や保守作業において、認証デバイス２１４ｂと画像処理装置２００の接続関係（利用権限の適用関係）を管理したい場合が考えられる。このような場合、例えば、機器構成の変更により認証デバイス２１４ｂの接続先を変更する場合や１台の機器に複数の認証デバイス２１４ｂを接続する場合など、管理者が、両装置の接続関係を手作業により管理するのは煩雑である。

【００７３】

そこで、本変形例では、認証デバイス２１４ｂの接続先にあたる画像処理装置２００（利用権限の適用機器）に関する情報を含むデバイス管理情報９０Ｄを管理し、利用認証を行う技術を提案する。

【００７４】

これにより、本変形例では、認証デバイス２１４ｂと画像処理装置２００の接続関係（利用権限の適用関係）を自動的に管理し、画像処理装置２００の利用認証が可能な環境を提供することができる。

【００７５】

なお、以降には、上記実施形態と異なる事項についてのみを説明し、同一事項については、同一参照符号を付し、その説明を省略する。

【００７６】

まず、本変形例に係るデバイス管理情報９０Ｄについて説明する。

図７は、本変形例に係るデバイス管理情報９０Ｄのデータ例を示す図である。

図７に示すように、本変形例に係るデバイス管理情報９０Ｄは、認証デバイス識別及び利用権限の他に、接続先識別を含む各情報項目が対応付けられている。

【００７７】

［接続先識別］項目は、認証デバイス２１４ｂの接続先を識別する接続先識別情報を保持する項目であり、項目値には、接続先にあたる画像処理装置２００の識別子（機器ＩＤ）などがある。

【００７８】

機器通信部１３は、画像処理装置２００（認証サーバ通信部）から、認証デバイス識別情報と接続先識別情報を含む認証情報を受信し、利用認証の要求を受け付けると、認証部１４に利用認証の実行を指示する。このとき、機器通信部１３は、受信した認証デバイス識別情報と接続先識別情報を含む認証情報を認証部１４に渡す。

【００７９】

認証部１４は、受け取った認証情報に基づき、画像処理装置２００が有する機能の利用認証を行い、情報管理部１２に情報登録／更新／削除・更新の実行を指示する。このとき、認証部１４は、受け取った認証デバイス情報と接続先識別情報を情報管理部１２に渡す。

【００８０】

情報管理部１２は、情報登録／更新／削除・更新指示に従って、デバイス管理情報９０Ｄを登録／更新／削除・更新し、認証デバイス２１４ｂと画像処理装置２００の接続関係を管理する。なお、デバイス管理情報９０Ｄの管理方法（データ操作方法）には、主に２通りの方法が挙げられる。具体的には、認証デバイス識別情報に基づき、対応付ける接続先識別情報を管理する方法（認証デバイスを基準とした接続関係の管理方法）と、接続先識別情報に基づき、対応付ける認証デバイス識別情報を管理する方法（接続先を基準とした接続関係の管理方法）である。

【００８１】

以下に、利用認証要求受付時に認証サーバ１００で実行される処理例を用いて、情報管理部１２と認証部１４の連携動作について説明する。

【００８２】

《認証サーバの主な処理：その１》

図８は、本変形例に係る認証サーバ１００における処理手順例（その１）を示すフローチャートである。本処理には、認証デバイス２１４ｂを基準とした接続関係の管理方法の処理例が示されている。

【００８３】

図８に示すように、機器通信部１３は、通信Ｉ／Ｆ１０７を介して、画像処理装置２００（認証サーバ通信部）から認証デバイス識別情報と接続先識別情報を含む認証情報を受信し、利用認証の要求を受け付けると（ステップＳ３０１：ＹＥＳ）、受信した認証情報を認証部１４に渡し、利用認証の実行を指示する。

【００８４】

認証部１４は、利用認証の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし（ステップＳ３０２）、受け取った認証情報を含まれる認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参照する（ステップＳ３０３）。

【００８５】

認証部１４は、参照したデバイス管理情報９０Ｄの中に該当デバイス管理情報９０Ｄが存在するか否かを判定し（ステップＳ３０４）、画像処理装置２００が有する機能の利用認証を行う。

【００８６】

認証部１４は、該当デバイス管理情報９０Ｄが存在すると判定した場合（ステップＳ３０４：ＹＥＳ）、該当デバイス管理情報９０Ｄの中に、認証デバイス識別情報に対応付けて接続先識別情報が登録されている（［接続先識別］項目値に設定値が存在する）か否かを判定する（ステップＳ３０５）。

【００８７】

認証部１４は、認証デバイス識別情報に対応付けて接続先識別情報が登録されていない（［接続先識別］項目値がＮＵＬＬ）と判定した場合（ステップＳ３０５：ＮＯ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報登録の実行を指示する。

【００８８】

情報管理部１２は、情報登録の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参照し、受け取った接続先識別情報を、認証デバイス識別情報に対応付けて登録する（ステップＳ３０６）。

【００８９】

このときに行われる具体的なデータ操作については、図９を用いて説明する。

図９は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その１）を示す図である。図９には、情報管理部１２が、情報登録指示時に、認証部１４から、認証デバイス識別情報"４５６", 接続先識別情報"ＭＦＰ－Ｘ"を受け取った場合の例が示されている。

【００９０】

情報管理部１２は、まず、図９（Ａ）に示すように、受け取った認証デバイス識別情報"４５６"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲを特定する。次に、情報管理部１２は、図９（Ｂ）に示すように、特定した情報セットＲの［接続先識別］項目値に、受け取った接続先識別情報の値"ＭＦＰ－Ｘ"を登録する。

【００９１】

このように、本変形例では、新規導入された画像処理装置２００に登録済み認証デバイス２１４ｂが接続された場合の接続関係が自動登録される。

【００９２】

図８の説明に戻る。認証部１４は、情報管理部１２から情報登録完了の旨を受け付けると、該当デバイス管理情報９０Ｄの利用権限情報に基づき、画像処理装置２００が有する機能に対して、利用を許可する機能／利用を許可しない機能を決定する（ステップＳ３０７）。

【００９３】

認証部１４は、決定した利用権限に従って、認証結果を生成し（ステップＳ３０８）、生成した認証結果を機器通信部１３に渡し、利用認証要求元への応答を指示する。

【００９４】

認証サーバ１００は、機器通信部１３が、応答指示を受け付けると、受け取った認証結果を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ３０９）。

【００９５】

また、認証部１４は、該当デバイス管理情報９０Ｄが存在しないと判定した場合（ステップＳ３０４：ＮＯ）、機能利用を認証しなかった旨の認証結果を生成し、機器通信部１３に渡し、利用認証要求元へのエラー通知を指示する。

【００９６】

機器通信部１３は、通知指示を受け付けると、受け取った認証結果（認証エラー）を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ３１０）。

【００９７】

また、認証部１４は、認証デバイス識別情報に対応付けて接続先識別情報が登録されている（［接続先識別］項目値がＮＵＬＬでない）と判定した場合（ステップＳ３０５：ＹＥＳ）、該当デバイス管理情報９０Ｄの中で、登録済みの接続先識別情報が受け取った接続先識別情報と一致するか否かを判定する（ステップＳ３１１）。

【００９８】

認証部１４は、登録済みの接続先識別情報が受け取った接続先識別情報と一致すると判定した場合（ステップＳ３１１：ＹＥＳ）、ステップＳ３０７の処理に移行する。つまり、認証部１４は、情報管理部１２に情報登録の実行を指示せず、該当デバイス管理情報９０Ｄの利用権限情報に基づき、認証結果を生成する。

【００９９】

また、認証部１４は、登録済みの接続先識別情報が受け取った接続先識別情報と一致しない（不一致）と判定した場合（ステップＳ３１１：ＮＯ）、受け取った接続先識別情報がデバイス管理情報９０Ｄに登録されているか否かを判定する（ステップＳ３１２）。

【０１００】

認証部１４は、受け取った接続先識別情報がデバイス管理情報９０Ｄに登録されていないと判定した場合（ステップＳ３１２：ＮＯ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報更新の実行を指示する。

【０１０１】

情報管理部１２は、情報更新の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参

照し、受け取った接続先識別情報で、認証デバイス識別情報に対応付けて登録された接続先識別情報を更新（上書き）する（ステップＳ３１３）。

【０１０２】

このときに行われる具体的なデータ操作については、図１０を用いて説明する。

図１０は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その２）を示す図である。図１０には、情報管理部１２が、情報更新指示時に、認証部１４から、認証デバイス識別情報"１２３"，接続先識別情報"ＭＦＰ－Ｘ"を受け取った場合の例が示されている。

【０１０３】

情報管理部１２は、まず、図１０（Ａ）に示すように、受け取った認証デバイス識別情報"１２３"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲを特定する。次に、情報管理部１２は、図１０（Ｂ）に示すように、特定した情報セットＲの［接続先識別］項目値"ＭＦＰ－Ａ"を、受け取った接続先識別情報の値"ＭＦＰ－Ｘ"で上書きする。

【０１０４】

このように、本変形例では、機器入れ替え後の画像処理装置２００に入れ替え前の機器に接続していた登録済み認証デバイス２１４ｂが接続された場合の接続関係が自動更新される。

【０１０５】

図８の説明に戻る。認証部１４は、情報管理部１２から情報更新完了の旨を受け付けると、ステップＳ３０７の処理に移行する。

【０１０６】

また、認証部１４は、受け取った接続先識別情報がデバイス管理情報９０Ｄに登録されていると判定した場合（ステップＳ３１２：ＹＥＳ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報削除・更新の実行を指示する。

【０１０７】

情報管理部１２は、情報削除・更新の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った接続先識別情報に基づき、デバイス管理情報９０Ｄを参照し、受け取った接続先識別情報と一致する登録済みの接続先識別情報を削除する（ステップＳ３１４）。

【０１０８】

情報管理部１２は、情報削除が完了すると、ステップＳ３１３の処理に移行する。つまり、情報管理部１２は、受け取った接続先識別情報で、認証デバイス識別情報に対応付けて登録された接続先識別情報を更新（上書き）する。

【０１０９】

このときに行われる具体的なデータ操作については、図１１を用いて説明する。

図１１は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その３）を示す図である。図１１には、情報管理部１２が、情報削除・更新指示時に、認証部１４から、認証デバイス識別情報"２３４"，接続先識別情報"ＭＦＰ－Ｂ"を受け取った場合の例が示されている。

【０１１０】

情報管理部１２は、まず、図１１（Ａ）に示すように、受け取った接続先識別情報"ＭＦＰ－Ｂ"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲａを特定する。次に、情報管理部１２は、図１１（Ｂ）に示すように、特定した情報セットＲａの［接続先識別］項目値"ＭＦＰ－Ｂ"を削除する。

【０１１１】

情報管理部１２は、図１１（Ａ）に示すように、受け取った認証デバイス識別情報"２３４"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲｂを特定する。次に、情報管理部１２は、図１１（Ｂ）に示すように、特定した情報セットＲｂの［接続先

識別］項目値"ＭＦＰ－Ａ"を、受け取った接続先識別情報の値"ＭＦＰ－Ｂ"で上書きする。

【０１１２】

このように、本変形例では、機器入れ替え後の画像処理装置２００に他の機器に接続していた登録済み認証デバイス２１４ｂが接続された場合の接続関係が自動更新される。

【０１１３】

図８の説明に戻る。認証部１４は、情報管理部１２から情報削除・更新完了の旨を受け付けると、ステップＳ３０７の処理に移行する。

【０１１４】

以上のように、認証デバイス２１４ｂを基準とした接続関係の管理方法では、認証デバイス２１４ｂに割り当てられた利用権限を機器構成変更後の画像処理装置２００に適用することができる。

【０１１５】

《認証サーバの主な処理：その２》

図１２は、本変形例に係る認証サーバ１００における処理手順例（その２）を示すフローチャートである。本処理には、接続先（画像処理装置）を基準とした接続関係の管理方法の処理例が示されている。

【０１１６】

図１２に示すように、機器通信部１３は、通信Ｉ／Ｆ１０７を介して、画像処理装置２００（認証サーバ通信部）から認証デバイス識別情報と接続先識別情報を含む認証情報を受信し、利用認証の要求を受け付けると（ステップＳ４０１：ＹＥＳ）、受信した認証情報を認証部１４に渡し、利用認証の実行を指示する。

【０１１７】

認証部１４は、利用認証の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし（ステップＳ４０２）、受け取った認証情報を含まれる接続先識別情報に基づき、デバイス管理情報９０Ｄを参照する（ステップＳ４０３）。

【０１１８】

認証部１４は、参照したデバイス管理情報９０Ｄの中に該当デバイス管理情報９０Ｄが存在するか否かを判定し（ステップＳ４０４）、画像処理装置２００が有する機能の利用認証を行う。

【０１１９】

認証部１４は、該当デバイス管理情報９０Ｄが存在すると判定した場合（ステップＳ４０４：ＹＥＳ）、該当デバイス管理情報９０Ｄの中に接続先識別情報に対応付けて認証デバイス識別情報が登録されている（［認証デバイス識別］項目値に設定値が存在する）か否かを判定する（ステップＳ４０５）。

【０１２０】

認証部１４は、接続先識別情報に対応付けて認証デバイス識別情報が登録されていない（［認証デバイス識別］項目値がＮＵＬＬ）と判定した場合（ステップＳ４０５：ＮＯ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報登録の実行を指示する。

【０１２１】

情報管理部１２は、情報登録の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った接続先識別情報に基づき、デバイス管理情報９０Ｄを参照し、受け取った認証デバイス識別情報を、接続先識別情報に対応付けて登録する（ステップＳ４０６）。

【０１２２】

このときに行われる具体的なデータ操作については、図１３を用いて説明する。

図１３は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その４）を示す図である。図１３には、情報管理部１２が、情報登録指示時に、認証部１４から、認証デバイス識別情報"４５６"，接続先識別情報"ＭＦＰ－Ｘ"を受け取った場合の例が示されてい

る。
【０１２３】
情報管理部１２は、まず、図１３（Ａ）に示すように、受け取った接続先識別情報"ＭＦＰ－Ｘ"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲを特定する。次に、情報管理部１２は、図１３（Ｂ）に示すように、特定した情報セットＲの［認証デバイス識別］項目値に、受け取った認証デバイス識別情報の値"４５６"を登録する。
【０１２４】
このように、本変形例では、認証デバイス２１４ｂが未接続の既存機器の画像処理装置２００に新規認証デバイス２１４ｂが接続された場合の接続関係が自動登録される。
【０１２５】
図１２の説明に戻る。認証部１４は、情報管理部１２から情報登録完了の旨を受け付けると、該当デバイス管理情報９０Ｄの利用権限情報に基づき、画像処理装置２００が有する機能に対して、利用を許可する機能／利用を許可しない機能を決定する（ステップＳ４０７）。
【０１２６】
認証部１４は、決定した利用権限に従って、認証結果を生成し（ステップＳ４０８）、生成した認証結果を機器通信部１３に渡し、利用認証要求元への応答を指示する。
【０１２７】
認証サーバ１００は、機器通信部１３が、応答指示を受け付けると、受け取った認証結果を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ４０９）。
【０１２８】
また、認証部１４は、該当デバイス管理情報９０Ｄが存在しないと判定した場合（ステップＳ４０４：ＮＯ）、機能利用を認証しなかった旨の認証結果を生成し、機器通信部１３に渡し、利用認証要求元へのエラー通知を指示する。
【０１２９】
機器通信部１３は、通知指示を受け付けると、受け取った認証結果（認証エラー）を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ４１０）。
【０１３０】
また、認証部１４は、接続先識別情報に対応付けて認証デバイス識別情報が登録されている（［認証デバイス識別］項目値がＮＵＬＬでない）と判定した場合（ステップＳ４０５：ＹＥＳ）、該当デバイス管理情報９０Ｄの中で、登録済みの認証デバイス識別情報が受け取った認証デバイス識別情報と一致するか否かを判定する（ステップＳ４１１）。
【０１３１】
認証部１４は、登録済みの認証デバイス識別情報が受け取った認証デバイス識別情報と一致すると判定した場合（ステップＳ４１１：ＹＥＳ）、ステップＳ４０７の処理に移行する。つまり、認証部１４は、情報管理部１２に情報登録の実行を指示せず、該当デバイス管理情報９０Ｄの利用権限情報に基づき、認証結果を生成する。
また、認証部１４は、登録済みの認証デバイス識別情報が受け取った認証デバイス識別情報と一致しないと判定した場合（ステップＳ４１１：ＮＯ）、受け取った認証デバイス識別情報がデバイス管理情報９０Ｄに登録されているか否かを判定する（ステップＳ４１２）。
【０１３２】
認証部１４は、受け取った認証デバイス識別情報がデバイス管理情報９０Ｄに登録されていないと判定した場合（ステップＳ４１２：ＮＯ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報更新の実行を指示する。
【０１３３】
情報管理部１２は、情報更新の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った接続先識別情報に基づき、デバイス管理情報９０Ｄを参照し、受け取った認証デバイス識別情報で、接続先識別情報に対応付けて登録された認証デバイ

ス識別情報を更新（上書き／追加）する（ステップＳ４１３）。
【０１３４】
このときに行われる具体的なデータ操作については、図１４を用いて説明する。
図１４は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その５）を示す図である。図１４には、情報管理部１２が、情報更新指示時に、認証部１４から、認証デバイス識別情報"６７８"，接続先識別情報"ＭＦＰ－Ａ"を受け取った場合の例が示されている。
【０１３５】
情報管理部１２は、まず、図１４（Ａ）に示すように、受け取った接続先識別情報"ＭＦＰ－Ａ"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲを特定する。次に、情報管理部１２は、図１４（Ｂ）に示すように、特定した情報セットＲの［認証デバイス識別］項目値"１２３"を、受け取った認証デバイス識別情報の値"６７８"で上書きする。
【０１３６】
このように、本変形例では、認証デバイス２１４ｂが接続済みの既存機器の画像処理装置２００に新規認証デバイス２１４ｂが接続された場合の接続関係が自動更新される。
【０１３７】
また、情報管理部１２は、図１４（Ｃ）に示すように、特定した情報セットＲの［認証デバイス識別］項目値に、受け取った認証デバイス識別情報の値"６７８"を追加してもよい。
【０１３８】
これは、１台の画像処理装置２００に対して、複数の認証デバイス２１４ｂが接続された場合を想定しており、このような場合でも、複数の認証デバイス２１４ｂと画像処理装置２００の接続関係が自動更新される。
【０１３９】
図１２の説明に戻る。認証部１４は、情報管理部１２から情報更新完了の旨を受け付けると、ステップＳ４０７の処理に移行する。
【０１４０】
また、認証部１４は、受け取った認証デバイス識別情報がデバイス管理情報９０Ｄに登録されていると判定した場合（ステップＳ４１２：ＹＥＳ）、認証要求受付時に受け取った認証デバイス識別情報と接続先識別情報を情報管理部１２に渡し、情報削除・更新の実行を指示する。
【０１４１】
情報管理部１２は、情報削除・更新の実行指示を受け付けると、デバイス管理情報保持部９０にアクセスし、受け取った認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参照し、受け取った認証デバイス識別情報と一致する登録済みの認証デバイス識別情報を削除する（ステップＳ４１４）。
【０１４２】
情報管理部１２は、情報削除が完了すると、ステップＳ４１３の処理に移行する。つまり、情報管理部１２は、受け取った認証デバイス識別情報で、接続先識別情報に対応付けて登録された認証デバイス識別情報を更新（上書き）する。
【０１４３】
このときに行われる具体的なデータ操作については、図１５を用いて説明する。
図１５は、本変形例に係るデバイス管理情報９０Ｄのデータ遷移例（その６）を示す図である。図１５には、情報管理部１２が、情報削除・更新指示時に、認証部１４から、認証デバイス識別情報"２３４"，接続先識別情報"ＭＦＰ－Ａ"を受け取った場合の例が示されている。
【０１４４】
情報管理部１２は、まず、図１５（Ａ）に示すように、受け取った認証デバイス識別情報"２３４"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲａを特定する

。次に、情報管理部１２は、図１５（Ｂ）に示すように、特定した情報セットＲａの［認証デバイス識別］項目値"２３４"を削除する。

【０１４５】

情報管理部１２は、図１５（Ａ）に示すように、受け取った接続先識別情報"ＭＦＰ－Ａ"に基づき、参照したデバイス管理情報９０Ｄの該当情報セットＲｂを特定する。次に、情報管理部１２は、図１５（Ｂ）に示すように、特定した情報セットＲｂの［認証デバイス識別］項目値"１２３"を、受け取った認証デバイス識別情報の値"２３４"で上書きする。

【０１４６】

このように、本変形例では、認証デバイス２１４ｂが接続済みの既存機器の画像処理装置２００に登録済み認証デバイス２１４ｂが接続された場合の接続関係が自動更新される。

【０１４７】

図１２の説明に戻る。認証部１４は、情報管理部１２から情報削除・更新完了の旨を受け付けると、ステップＳ４０７の処理に移行する。

【０１４８】

以上のように、接続先を基準とした接続関係の管理方法では、認証デバイス２１４ｂが接続切り替えされても、画像処理装置２００に割り当てられた利用権限を適用することができる。

【０１４９】

本変形例では、認証デバイス２１４ｂと画像処理装置２００の接続関係（利用権限の適用関係）を自動的に管理し、画像処理装置２００の利用認証が可能な環境を提供できる。

【０１５０】

［第２の実施形態］

上記実施形態では、認証デバイス２１４ｂに接続先の画像処理装置２００が有する機能の利用権限を対応付けて管理する構成について説明を行った。

【０１５１】

そこで、本実施形態では、利用者に対応付けられた利用権限と認証デバイス２１４ｂに対応付けられた利用権限に基づき、画像処理装置２００の利用認証を行う技術を提案する。

【０１５２】

これにより、本実施形態では、機器利用認証時に、認証デバイス単位により利用権限の適用の他に、利用者／利用者の所属単位による利用権限の適用が可能で、かつ、機器利用認証に用いる情報管理の手間を軽減できる。

【０１５３】

なお、以降には、上記実施形態と異なる事項についてのみを説明し、同一事項については、同一参照符号を付し、その説明を省略する。

【０１５４】

＜認証機能＞

図１６は、本実施形態に係る認証機能の構成例を示す図である。

図１６に示すように、本実施形態に係る認証機能は、デバイス管理情報保持部９０の他に、利用者管理情報保持部８０及び制御設定値保持部７０を有し、各保持部９０，８０，７０で保持される情報は、情報管理部１２により管理される。なお、利用者管理情報保持部８０及び制御設定値保持部７０は、デバイス管理情報保持部９０と同様に、認証サーバ１００が備える記憶装置の所定の記憶領域にあたる。

【０１５５】

情報管理部１２は、利用者／利用者の所属と画像処理装置２００が有する機能の利用権限を対応付けて管理する。情報管理部１２は、所定のデータ操作により、利用者管理情報保持部８０にアクセスし、利用者／利用者の所属と利用権限が対応付けられた利用者管理情報を管理する。

【０１５６】
ここで、利用者管理情報について説明する。なお、利用者管理情報は、利用者情報と所属情報に大別される。
図１７は、本実施形態に係る利用者管理情報８０Ｄのデータ例を示す図である。
図１７（Ａ）に示すように、利用者管理情報８０Ｄの利用者情報８０Ｄ$_1$は、利用者識別、所属識別、利用権限などの各情報項目が対応付けられた１又は複数の情報セットを含み、該情報セットが利用者単位で管理される。
【０１５７】
［利用者識別］項目は、利用者を識別する利用者識別情報を保持する項目であり、項目値には、利用者にユニークに割り当てられた識別子（利用者ＩＤ）などがある。［所属識別］項目は、利用者の所属を識別する所属識別情報を保持する項目であり、項目値には、所属にユニークに割り当てられた識別子（所属ＩＤ）などがある。［利用権限］項目は、画像処理装置２００が有する機能の利用権限が設定された利用権限情報を保持する項目である。
【０１５８】
図１６の説明に戻る。情報管理部１２は、上記利用者情報８０Ｄ$_1$の各情報項目値を、次のようにして設定・登録する。情報管理部１２は、ＵＩ制御部１１から設定・登録指示を受け付けると、利用者管理情報保持部８０にアクセスし、設定・登録指示時に受け取った入力値を、参照した利用者情報８０Ｄ$_1$の該当情報項目値に設定・登録する。具体的には、利用者／利用者の所属に対応する入力値を［利用者識別］／［所属識別］項目値に設定・登録する。また、画像処理装置２００が有する機能の利用権限に対応する入力値を［利用権限］項目値に設定・登録する。
【０１５９】
また、情報管理部１２は、上記利用者情報８０Ｄ$_1$の各情報項目値を、次のようにして更新する。情報管理部１２は、ＵＩ制御部１１から更新指示を受け付けると、利用者管理情報保持部８０にアクセスし、更新指示時に受け取った入力値で、参照した利用者情報８０Ｄ$_1$の該当情報項目値を更新する。具体的には、利用者／利用者の所属に対応する入力値で［利用者識別］／［所属識別］項目値を更新する。また、画像処理装置２００が有する機能の利用権限に対応する入力値で［利用権限］項目値を更新する。
【０１６０】
このように、認証サーバ１００には、管理者などが、認証システム１の運用方針などに基づき、利用認証の対象利用者と利用認証の対象機器が有する機能の利用権限を、予め対応付けて設定しておく。
【０１６１】
また、図１７（Ｂ）に示すように、利用者管理情報８０Ｄの所属情報８０Ｄ$_2$は、所属識別及び利用権限などの各情報項目が対応付けられた１又は複数の情報セットを含み、該情報セットが所属単位で管理される。
【０１６２】
［所属識別］項目は、利用者の所属を識別する所属識別情報を保持する項目である。［利用権限］項目は、画像処理装置２００が有する機能の利用権限が設定された利用権限情報を保持する項目である。
【０１６３】
図１６の説明に戻る。情報管理部１２は、上記所属情報８０Ｄ$_2$の各情報項目値を、次のようにして設定・登録する。情報管理部１２は、ＵＩ制御部１１から設定・登録指示を受け付けると、利用者管理情報保持部８０にアクセスし、設定・登録指示時に受け取った入力値を、参照した所属情報８０Ｄ$_2$の該当情報項目値に設定・登録する。具体的には、所属に対応する入力値を［所属識別］項目値に設定・登録する。また、画像処理装置２００が有する機能の利用権限に対応する入力値を［利用権限］項目値に設定・登録する。
【０１６４】
また、情報管理部１２は、上記所属情報８０Ｄ$_2$の各情報項目値を、次のようにして更

新する。情報管理部１２は、ＵＩ制御部１１から更新指示を受け付けると、利用者管理情報保持部８０にアクセスし、更新指示時に受け取った入力値で、参照した所属情報８０Ｄ$_2$の該当情報項目値を更新する。具体的には、所属に対応する入力値で［所属識別］項目値を更新する。また、画像処理装置２００が有する機能の利用権限に対応する入力値で［利用権限］項目値を更新する。

【０１６５】

このように、認証サーバ１００には、管理者などが、認証システム１の運用方針などに基づき、利用認証の対象所属と利用認証の対象機器が有する機能の利用権限を、予め対応付けて設定しておく。

【０１６６】

また、ＵＩ制御部１１は、図１８に示すような設定画面Ｗを表示し、機器利用認証時に、デバイス管理情報９０Ｄと利用者管理情報８０Ｄに設定された各利用権限の適用を制御する入力値を受け付ける。

【０１６７】

図１８は、本実施形態に係る制御設定の画面例を示す図である。

図１８には、認証デバイス２１４ｂ、利用者、所属の各利用権限を適用する優先順位が設定可能なＧＵＩと利用権限重複時に適用する利用権限が設定可能なＧＵＩを有する画面例が示されている。設定画面Ｗを介して受け付けた各種設定の入力値は、情報管理部１２により管理される。

【０１６８】

図１６の説明に戻る。ＵＩ制御部１１は、上記設定画面Ｗを介して、各種設定を受け付けると、設定受付時に受け取った入力値を情報管理部１２に渡し、情報登録の実行を指示する。

【０１６９】

情報管理部１２は、情報登録指示を受け付けると、制御設定値保持部７０にアクセスし、受け取った入力値を設定制御値として保持する。

【０１７０】

機器通信部１３は、画像処理装置２００（認証サーバ通信部）から、認証デバイス情報と利用者関連情報を含む認証情報を受信し、利用認証の要求を受け付けると、認証部１４に利用認証の実行を指示する。このとき、機器通信部１３は、受信した認証デバイス識別情報と利用者関連情報を含む認証情報を認証部１４に渡す。

【０１７１】

認証部１４は、認証指示を受け付けると、各保持部９０，８０，７０にアクセスし、受け取った認証情報に基づき、デバイス管理情報９０Ｄ、利用者管理情報８０Ｄ、及び制御設定値を取得し、取得した情報／制御設定値に基づき、画像処理装置２００が有する機能の利用認証を行う。

【０１７２】

以下に、利用認証要求受付時に認証サーバ１００で実行される処理例を用いて、認証部１４の動作について説明する。

【０１７３】

《認証サーバの主な処理》

図１９は、本実施形態に係る認証サーバ１００における処理手順例を示すフローチャートである。

図１９に示すように、機器通信部１３は、通信Ｉ／Ｆ１０７を介して、画像処理装置２００（認証サーバ通信部）から認証デバイス情報と利用者関連情報を含む認証情報を受信し、利用認証の要求を受け付けると（ステップＳ５０１：ＹＥＳ）、受信した認証情報を認証部１４に渡し、利用認証の実行を指示する。

【０１７４】

認証部１４は、利用認証の実行指示を受け付けると、各保持部９０，８０，７０にアクセスする（ステップＳ５０２）。

【０１７５】
認証部１４は、制御設定値保持部７０から、利用権限の適用を制御する制御設定値（適用の優先順位設定及び重複時の適用設定）を取得する（ステップＳ５０３）。
【０１７６】
認証部１４は、受け取った認証情報を含まれる利用者関連情報の利用者識別情報に基づき、利用者管理情報８０Ｄの利用者情報$８０Ｄ_{1}$を参照し（ステップＳ５０４）、利用者の利用権限情報を取得する（ステップＳ５０５）。このとき、認証部１４は、利用者識別情報に基づき、参照した利用者情報$８０Ｄ_{1}$の該当情報セットを特定する。認証部１４は、特定した情報セットの利用権限情報を取得する。
【０１７７】
認証部１４は、同情報セットの所属識別情報に基づき、利用者管理情報８０Ｄの所属情報$８０Ｄ_{2}$を参照し（ステップＳ５０６）、所属の利用権限情報を取得する（ステップＳ５０７）。このとき、認証部１４は、所属識別情報に基づき、参照した所属情報$８０Ｄ_{2}$の該当情報セットを特定する。認証部１４は、特定した情報セットの利用権限情報を取得する。
【０１７８】
認証部１４は、受け取った認証情報を含まれる認証デバイス情報の認証デバイス識別情報に基づき、デバイス管理情報９０Ｄを参照し（ステップＳ５０８）、認証デバイス２１４ｂの利用権限情報を取得する（ステップＳ５０９）。このとき、認証部１４は、認証デバイス識別情報に基づき、参照したデバイス管理情報９０Ｄの該当情報セットを特定する。認証部１４は、特定した情報セットの利用権限情報を取得する。
【０１７９】
認証部１４は、取得した利用権限情報／制御設定値に基づき、画像処理装置２００が有する機能に対して、設定された利用権限を適用し、利用を許可する機能／利用を許可しない機能を決定する（ステップＳ５１０）。
【０１８０】
認証部１４は、決定した利用権限に従って、認証結果を生成し（ステップＳ５１１）、生成した認証結果を機器通信部１３に渡し、利用認証要求元への応答を指示する。
【０１８１】
機器通信部１３は、応答指示を受け付けると、受け取った認証結果を画像処理装置２００（認証サーバ通信部）に送信する（ステップＳ５１２）。
【０１８２】
以下に、ステップＳ５１０の詳細処理について説明する。
《利用権限の適用処理》
図２０は、本実施形態に係る利用権限の適用処理手順例を示すフローチャートである。
図２０に示すように、認証部１４は、優先順位の制御設定値に基づき、利用権限を適用する優先順位設定に従って、認証デバイス２１４ｂ、利用者、所属の各利用権限情報（取得した利用権限情報）の中から、優先順位の高い順に利用権限情報を特定する（ステップＳ６０１）。
【０１８３】
認証部１４は、優先順位に従って、利用権限情報を特定できたか否かを判定する（ステップＳ６０２）。
【０１８４】
認証部１４は、利用権限情報を特定できなかったと判定した場合（ステップＳ６０２：ＮＯ）、画像処理装置２００が有する全ての機能を、利用を許可しない機能に決定する（ステップＳ６０３）。
【０１８５】
一方、認証部１４は、利用権限情報を特定できた判定した場合（ステップＳ６０２：ＹＥＳ）、特定した利用権限情報が複数存在する（同一の優先順位が設定された利用権限が複数存在する）か否かを判定する（ステップＳ６０４）。

【０１８６】
認証部１４は、特定した利用権限情報が複数存在しないと判定した場合（ステップＳ６０４：ＮＯ）、特定した利用権限情報に基づき、画像処理装置２００が有する機能に対して、設定された利用権限を適用し、利用を許可する機能／利用を許可しない機能を決定する（ステップＳ６０５）。
【０１８７】
一方、認証部１４は、特定した利用権限情報が複数存在すると判定した場合（ステップＳ６０４：ＹＥＳ）、重複時の制御設定値に基づき、利用権限重複時の適用設定が「禁止（不許可）」か否かを判定する（ステップＳ６０６）。
【０１８８】
認証部１４は、利用権限重複時の適用設定が「禁止（不許可）」であると判定した場合（ステップＳ６０６：ＹＥＳ）、特定した複数の利用権限情報に基づき、機能ごとの利用権限値（"○"：許可／"×"：不許可）を比較し、１つでも「禁止（不許可）」が設定されている機能を、利用を許可しない機能に決定する（ステップＳ６０７）。
【０１８９】
一方、認証部１４は、利用権限重複時の適用設定が「許可」であると判定した場合（ステップＳ６０６：ＮＯ）、特定した複数の利用権限情報に基づき、機能ごとの利用権限値（"○"：許可／"×"：不許可）を比較し、１つでも「許可」が設定されている機能を、利用を許可する機能に決定する（ステップＳ６０８）。
【０１９０】
＜まとめ＞
以上のように、本実施形態に係る認証システム１によれば、画像処理装置２００は、認証デバイス通信部２１により、自機に接続された（接続検知した）認証デバイス２１４ｂから認証デバイス情報を取得する。画像処理装置２００は、認証サーバ通信部２２により、取得した認証デバイス情報と利用者関連情報を認証サーバ１００に送信し、利用認証を要求する。
【０１９１】
これを受けて認証サーバ１００は、機器通信部１３により、認証デバイス情報と利用者関連情報を受信する。認証サーバ１００は、認証部１４により、受信した認証デバイス情報と利用者関連情報に基づき、画像処理装置２００の利用権限情報を取得する。このとき、認証部１４は、該認証デバイス情報に対応付けて管理している画像処理装置２００の利用権限情報と利用者／利用者の所属に対応付けて管理している画像処理装置２００の利用権限情報を取得する。認証部１４は、取得した利用権限情報の中から、利用権限の適用を制御する制御設定に従って特定した利用権限情報に基づき、画像処理装置２００に適用する利用権限を決定する。認証サーバ１００は、機器通信部１３により、決定した利用権限を含む認証結果を送信し、利用認証要求に応答する。
【０１９２】
その結果、画像処理装置２００は、認証サーバ通信部２２により、認証結果を受信し、ＵＩ制御部２３により、認証結果に含まれる利用権限に従って、機能利用を制御する。
【０１９３】
これによって、本実施形態に係る認証システム１は、機器利用認証時に、認証デバイス単位により利用権限の適用の他に、利用者／利用者の所属単位による利用権限の適用が可能で、かつ、機器利用認証に用いる情報管理の手間を軽減できる。
【０１９４】
ここまで、上記実施形態の説明を行ってきたが、上記実施形態に係る「認証機能」は、図を用いて説明を行った各処理手順を、動作環境（プラットフォーム）にあったプログラミング言語でコード化したプログラムが、システム１を構成する各機器（「認証サーバ」や「画像処理装置」）が備える演算装置（ＣＰＵ）により実行されることで実現される。
【０１９５】
上記プログラムは、コンピュータが読み取り可能な記録媒体１０３ａに格納することが

できる。これにより、例えば、認証サーバ１００の場合、上記プログラムは、外部Ｉ／Ｆ１０３を介して、認証サーバ１００にインストールすることができる。また、認証サーバ１００は、通信Ｉ／Ｆ１０７を備えていることから、電気通信回線を用いて上記プログラムをダウンロードし、インストールすることもできる。画像処理装置２００の場合も同様である。

【０１９６】

［変形例］

なお、上記実施形態に係る認証機能は、次のような機能構成であってもよい。

図２１，２２は、本変形例に係る認証機能の構成例（その１，２）を示す図である。

図２１には、画像処理装置２００が単体で認証機能を有する構成例が示されている。この場合、画像処理装置２００は、情報管理部１２、認証部１４、認証デバイス通信部２１、ＵＩ制御部２３、デバイス管理情報保持部９０を有する。また、図２２には、利用者管理サーバ３００（利用者管理情報保持部）と認証サーバ１００（認証部）が連携動作する場合の認証機能の構成例が示されている。

【０１９７】

このように、本変形例に示す機能構成であっても、上記実施形態と同様の効果を奏することができる。

【０１９８】

最後に、上記実施形態に挙げた形状や構成に、その他の要素との組み合わせなど、ここで示した要件に、本発明が限定されるものではない。これらの点に関しては、本発明の主旨をそこなわない範囲で変更することが可能であり、その応用形態に応じて適切に定めることができる。

【符号の説明】

【０１９９】

１　　認証システム
１１，２３　ＵＩ制御部
１２　　情報管理部
１３　　機器通信部
１４　　認証部
２１　　認証デバイス通信部
２２　　認証サーバ通信部
７０　　制御設定値保持部
８０　　利用者管理情報保持部（D_1：利用者情報，D_2：所属情報）
９０　　デバイス管理情報保持部（Ｄ：デバイス管理情報）
１００　認証サーバ（情報処理装置）
２００　画像処理装置（電子機器）

【先行技術文献】

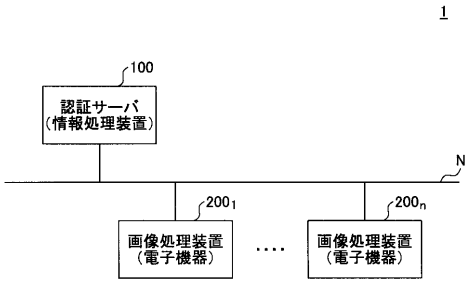
【特許文献】

【０２００】

【特許文献１】特開２００８－１６２１７１号公報

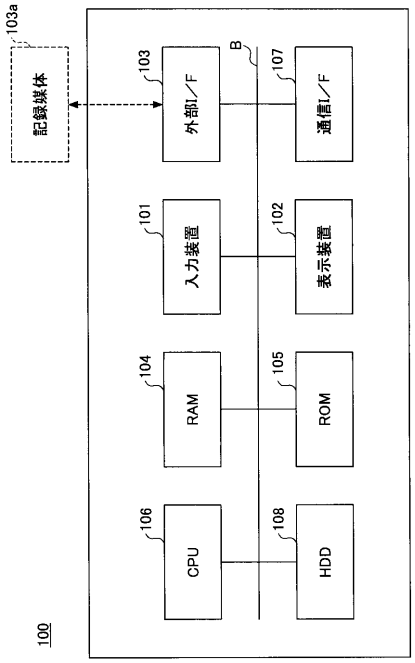
【図１】

本発明の第1の実施形態に係る認証システムの構成例を示す図



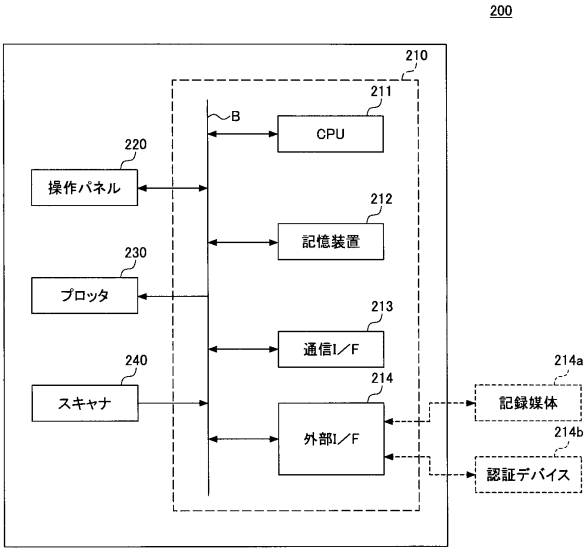
【図２】

本発明の第1の実施形態に係る認証サーバのハードウェア構成例を示す図



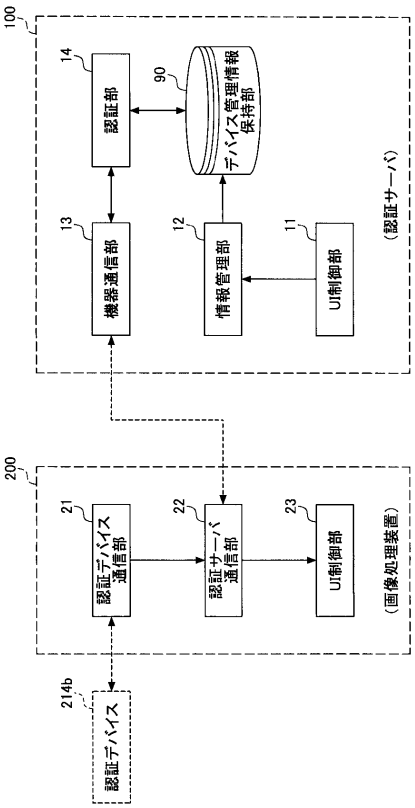
【図３】

本発明の第1の実施形態に係る画像処理装置のハードウェア構成例を示す図



【図４】

本発明の第1の実施形態に係る認証機能の構成例を示す図



【図５】

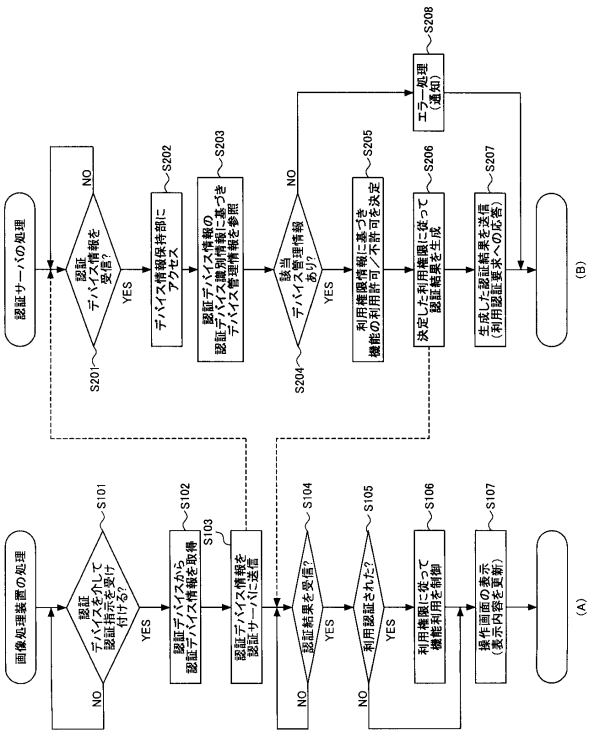
本発明の第1の実施形態に係るデバイス管理情報のデータ例を示す図

90D

認証デバイス識別	利用権限				
	プリント	コピー	スキャン	ファックス	……
123	○	○	×	×	……
234	○	○	○	○	……
456	×	○	○	×	……
678	○	×	×	×	……
……	……	……	……	……	……

【図６】

本発明の第1の実施形態に係る認証の処理手順例を示すフローチャート



【図７】

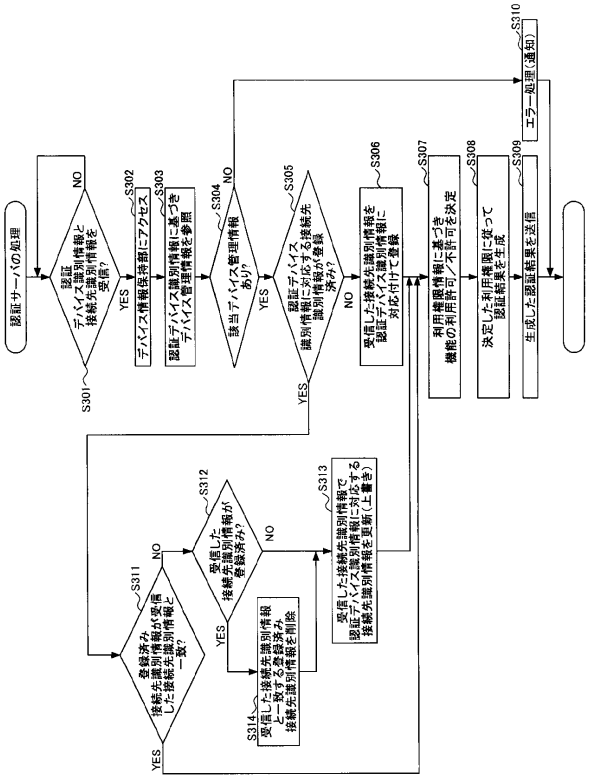
本発明の変形例に係るデバイス管理情報のデータ例を示す図

90D

認証デバイス識別	接続先識別	利用権限				
		プリント	コピー	スキャン	ファックス	……
123	MFP－A	○	○	×	×	……
234	MFP－B	○	○	○	○	……
456	MFP－C	×	○	○	×	……
678	MFP－D	○	×	×	×	……
……	……	……	……	……	……	……

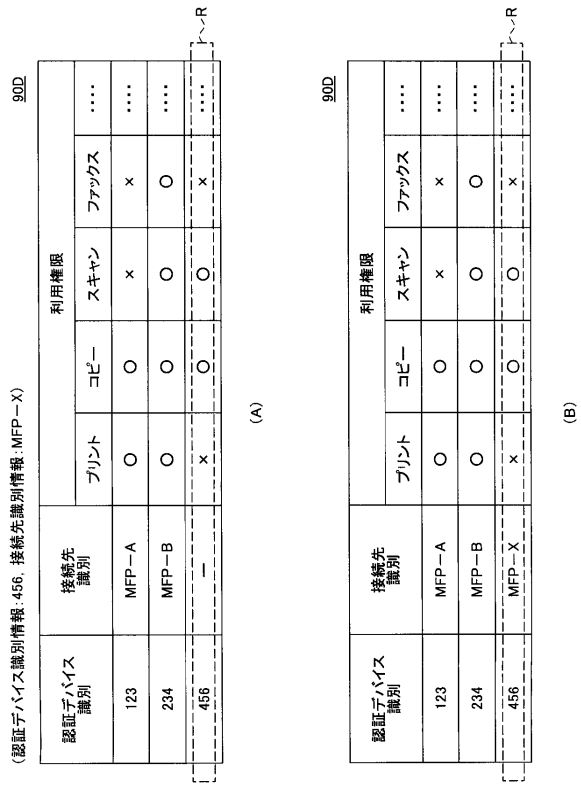
【図８】

本発明の変形例に係る認証サーバにおける処理手順例(その1)を示すフローチャート



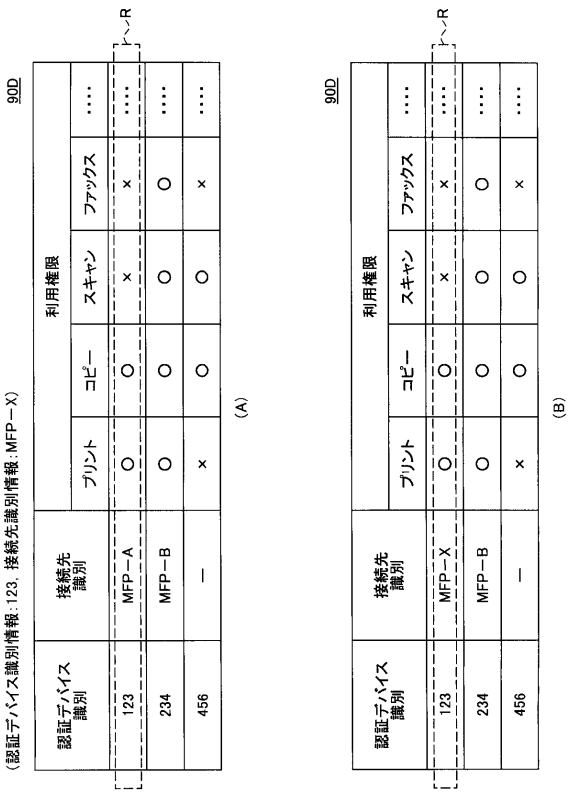
【図９】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その1)を示す図



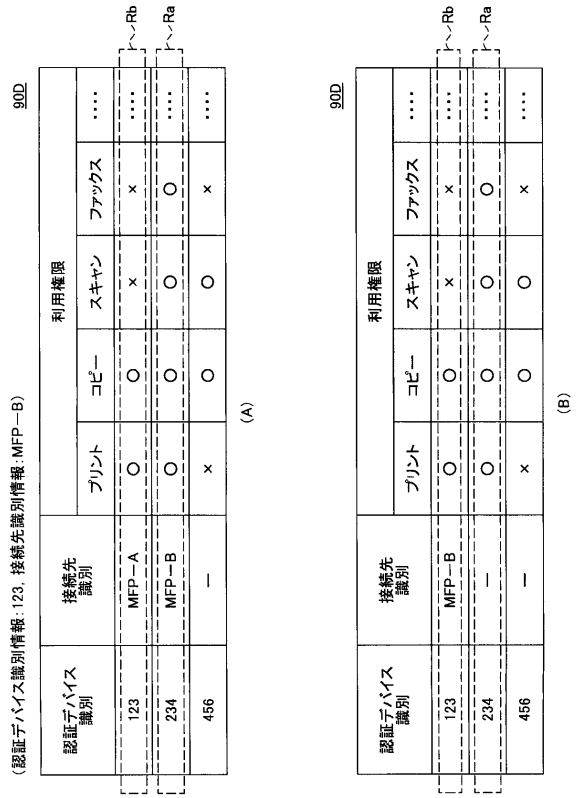
【図１０】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その2)を示す図



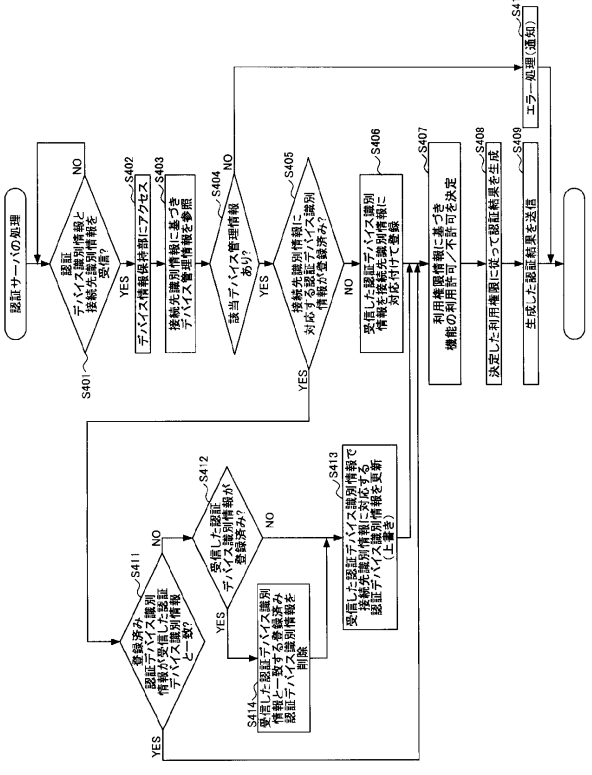
【図１１】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その3)を示す図



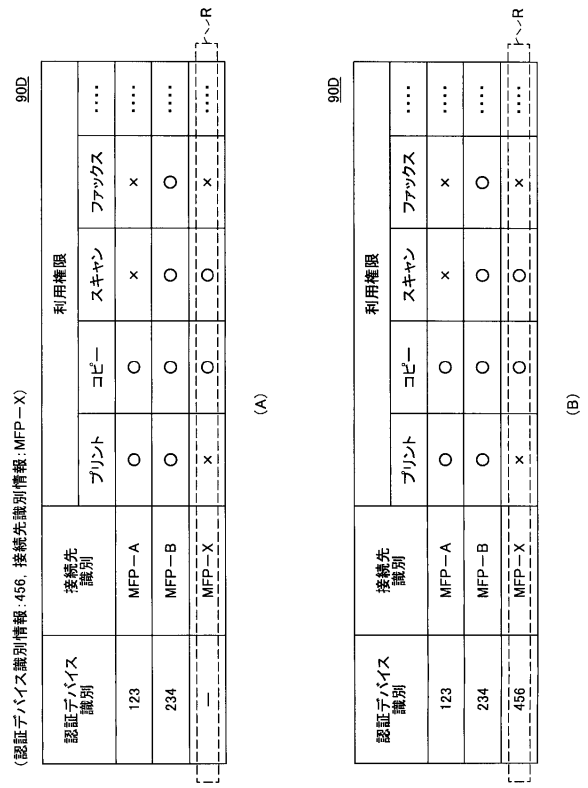
【図１２】

本発明の変形例に係る認証サーバにおける処理手順例(その2)を示すフローチャート



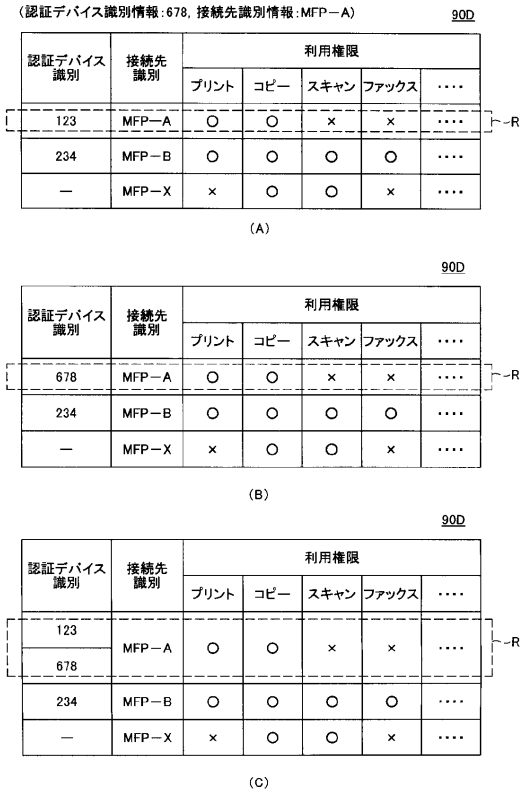
【図１３】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その4)を示す図



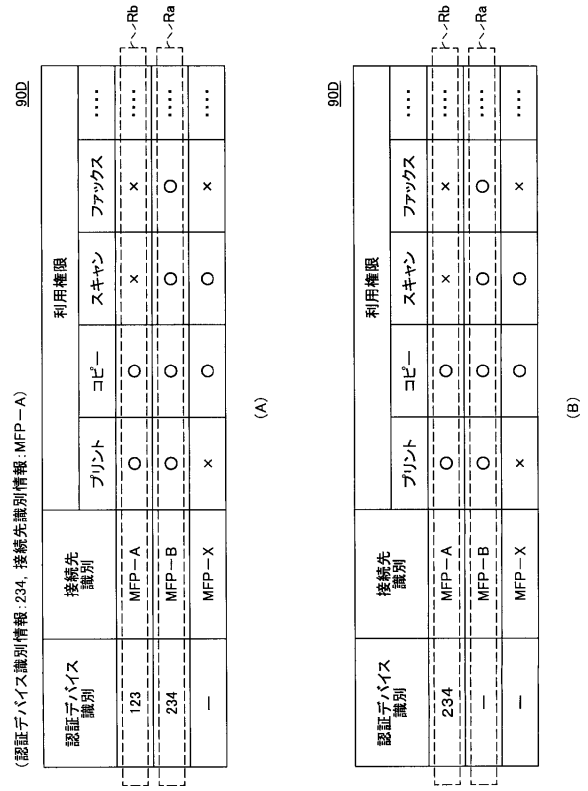
【図１４】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その5)を示す図



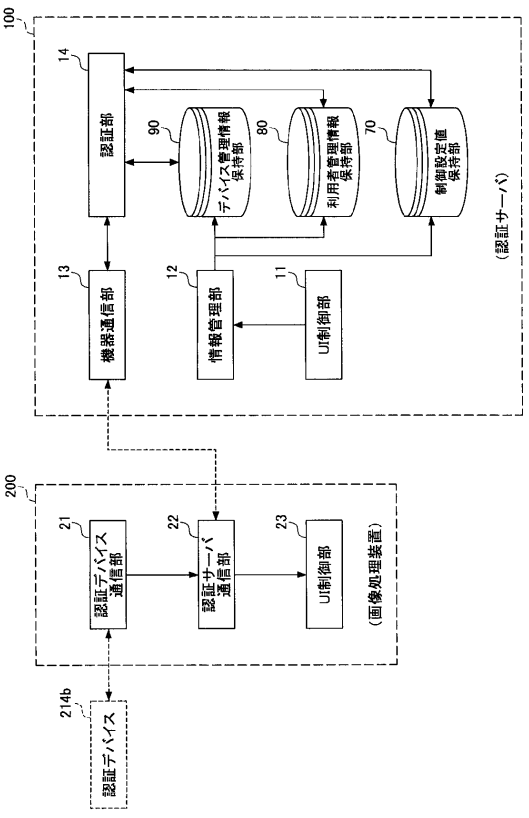
【図１５】

本発明の変形例に係るデバイス管理情報のデータ遷移例(その6)を示す図



【図１６】

本発明の第2の実施形態に係る認証機能の構成例を示す図



【図１７】

本発明の第2の実施形態に係る利用者管理情報のデータ例を示す図

80D1

利用者識別	所属識別	利用権限				
		プリント	コピー	スキャン	ファックス	....
UserA	GroupX,Y	○	○	○	○	....
UserB	GroupX	○	○	×	○	....
UserC	—	○	○	○	×	....
....	....	....	....	....	....	....

(A)

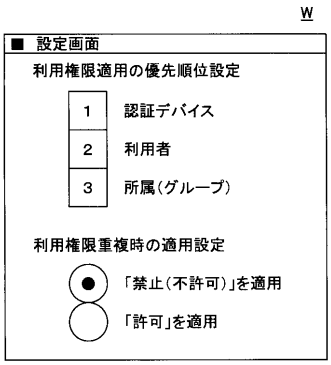
80D2

所属識別	利用権限				
	プリント	コピー	スキャン	ファックス	....
GroupX	○	×	○	×	....
GroupY	○	×	×	×	....
....	....	....	....	....	....

(B)

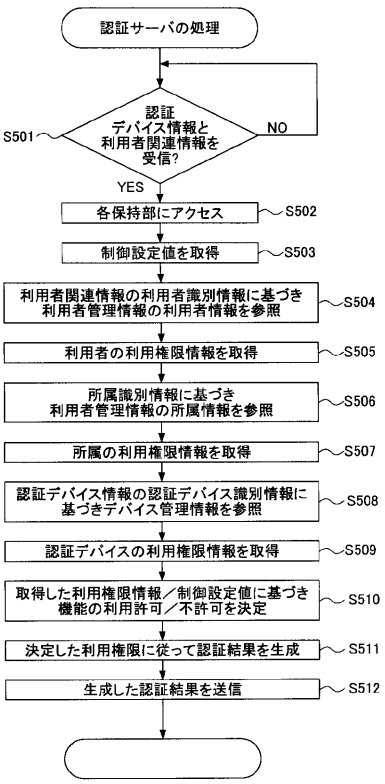
【図１８】

本発明の第2の実施形態に係る制御設定の画面例を示す図



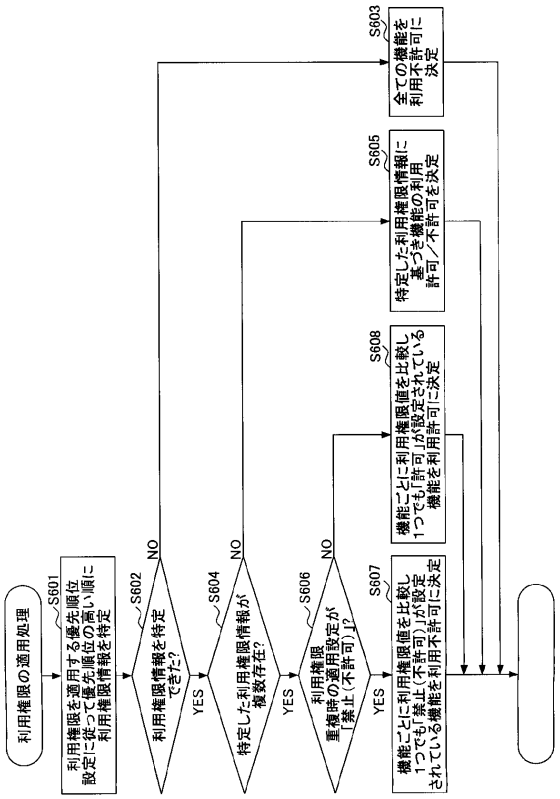
【図１９】

本発明の第2の実施形態に係る
認証サーバにおける処理手順例を示すフローチャート



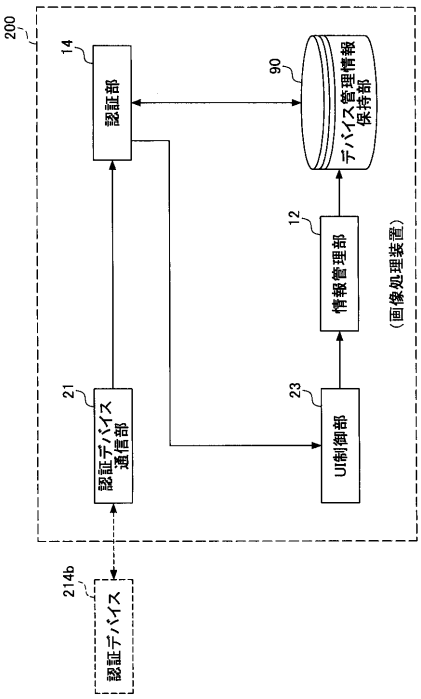
【図２０】

本発明の第2の実施形態に係る
利用権限の適用処理手順例を示すフローチャート



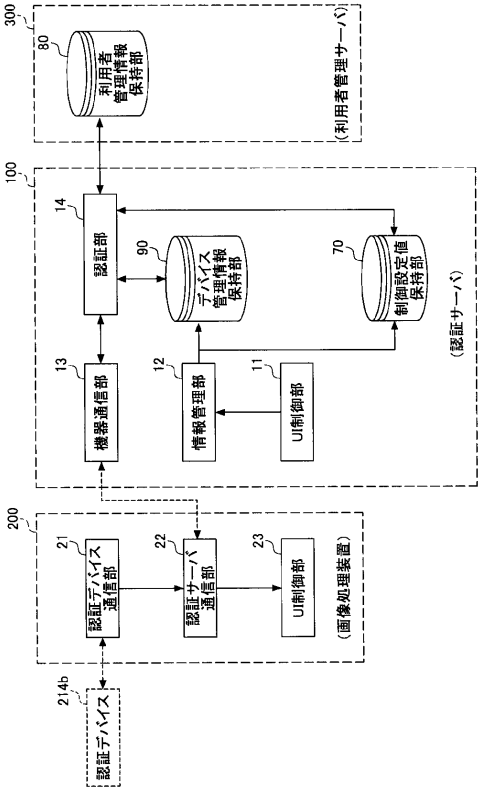
【図２１】

本発明の変形例に係る認証機能の構成例（その1）を示す図



【図２２】

本発明の変形例に係る認証機能の構成例（その2）を示す図



フロントページの続き

(51)Int.Cl. F I
H04N 1/00 107Z

(56)参考文献 特開２０１１－１２３８６５（ＪＰ，Ａ）
特開２００９－１５７４３５（ＪＰ，Ａ）
特開２０１０－２０６２５５（ＪＰ，Ａ）
特開２０１０－０９２４５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８
Ｂ４１Ｊ ２９／００
Ｂ４１Ｊ ２９／３８
Ｈ０４Ｌ ９／３２
Ｈ０４Ｎ １／００