(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-142574
(P2007-142574A)
(43)公開日　平成19年6月7日(2007.6.7)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04N 1/00 | (2006.01) | H04N | 1/00 | 107Z | 2C061 |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 640E | 5B021 |
| B41J 29/38 | (2006.01) | B41J | 29/38 | Z | 5C062 |
| B41J 29/00 | (2006.01) | B41J | 29/00 | Z | 5J104 |
| G06F 3/12 | (2006.01) | G06F | 3/12 | K | |

審査請求 未請求　請求項の数 5　ＯＬ　（全 12 頁）

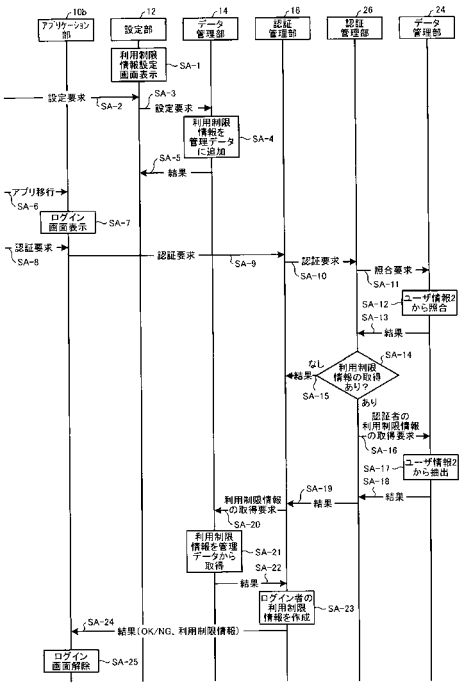
(21)出願番号　特願2005-330568 (P2005-330568)
(22)出願日　平成17年11月15日 (2005.11.15)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　大谷　葉子
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　2C061 AP01 CL08 HK11 HN04 HN15
5B021 EE04 NN00
5C062 AA05 AA29 AB22 AB38 AB40
AC04 AC34 AC58 AF12 AF14
5J104 KA01 PA07

(54)【発明の名称】画像形成装置および利用制限方法

(57)【要約】
【課題】管理者や利用者などへの作業負担を軽減すると共に、一定の権限を持つ者以外の者に対しても外部の認証情報に基づく認証を実施することができる画像形成装置、および当該画像形成装置で行われる利用制限方法を提供することを目的とする。
【解決手段】画像形成装置１の認証管理部１６は、画像形成装置２の認証管理部２６に対し、ネットワーク３を介して認証要求を行う。一方、画像形成装置２の認証管理部２６は、画像形成装置１の認証管理部１６からの認証要求に対して、データ管理部２４と連携して、管理データベース２４１に予め記憶したユーザ情報２に基づいて個人の認証を行う。
【選択図】　図２



【特許請求の範囲】
【請求項１】
パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置であって、
ネットワークを介して接続された他の画像形成装置からの認証要求に対して、前記認証手段を実行させることが可能であること
を特徴とする画像形成装置。
【請求項２】
パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置であって、
ネットワークを介して接続された請求項１に記載の画像形成装置へ認証要求を行うことが可能であること
を特徴とする画像形成装置。
【請求項３】
ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報および当該画像形成装置で予め設定した利用制限情報のうち少なくとも１つを、前記制限手段で用いる利用制限情報として決定する決定手段をさらに備え、
前記制御手段は、前記決定手段で決定した利用制限情報に基づいて機能の利用を制限すること
を特徴とする請求項１または２に記載の画像形成装置。
【請求項４】
パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置で行われる利用制限方法であって、
前記認証手段で個人の認証が行われた際またはネットワークを介して接続された他の画像形成装置の認証手段で個人の認証が行われた際、前記制限手段で、他の画像形成装置から予め取得した利用制限情報に基づいて機能の利用を制限すること
を特徴とする利用制限方法。
【請求項５】
パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置で行われる利用制限方法であって、
前記認証手段で個人の認証が行われた際またはネットワークを介して接続された他の画像形成装置の認証手段で個人の認証が行われた際、前記制限手段で、当該画像形成装置で予め設定した利用制限情報に基づいて機能の利用を制限すること
を特徴とする利用制限方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証情報に基づく個人の認証と、利用制限情報に基づく機能の利用の制限とを行うことができる画像形成装置、および当該画像形成装置で行われる利用制限方法に関する。
【背景技術】
【０００２】
セキュリティ対策として、画像形成装置でも、個人認証による各種機能の利用許可・利用不許可といったアクセス制限を実施している。そして、現状では、認証の種類には、画像形成装置内の認証情報に基づく個人認証と、画像形成装置外部の個人認証管理サーバーで一元的に管理する認証情報に基づく外部認証とがある。

【０００３】
ここで、画像形成装置内の認証情報に基づく個人認証の場合、他の画像形成装置の認証情報を直接使用することができない。そのため、現状では、画像形成装置は、認証情報を多数の画像形成装置同士で一元管理するために予め設定された管理サーバーから認証情報を取得して当該装置内に保持したり、ＷＥＢやツールや持ち運び可能なメディアを用いてバックアップリストアで他の画像形成装置の認証情報をコピーして当該装置内に保持したりすることで、他の画像形成装置と共通の認証情報に基づく個人認証を可能としている。なお、他の画像形成装置が保持しているユーザ情報を或る画像形成装置で使用可能にする技術については特許文献１で開示されている。これにより、或る画像形成装置は、ネットワークを介して接続された他の画像形成装置が保持しているユーザ情報を取得し、取得したユーザ情報を用いて所定の処理を行うことができる。
【０００４】
【特許文献１】特開２００５－０９４３５８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来の技術では、外部の認証情報を取得するにあたって管理サーバーを予め設定したりツールを用いたりしなければならないので、管理者や利用者などに多くの作業負担を掛けていたという問題点があった。また、従来の技術では、管理サーバーや他の画像形成装置から認証情報を取得するので、認証対象者のうち一定の権限を持つ者（例えば認証情報の取得が許された者）に対してしか外部の認証情報に基づく認証を実施することができないという問題点があった。
【０００６】
本発明は、上記問題点に鑑みてなされたものであって、管理者や利用者などへの作業負担を軽減すると共に、一定の権限を持つ者以外の者に対しても外部の認証情報に基づく認証を実施することができる画像形成装置、および当該画像形成装置で行われる利用制限方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上述した課題を解決し、目的を達成するために、本発明は、パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置であって、ネットワークを介して接続された他の画像形成装置からの認証要求に対して、前記認証手段を実行させることが可能であることを特徴とする。
【０００８】
また、本発明は、パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置であって、ネットワークを介して接続された請求項１に記載の画像形成装置へ認証要求を行うことが可能であることを特徴とする。
【０００９】
また、本発明は、請求項１または２に記載の画像形成装置であって、ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報および当該画像形成装置で予め設定した利用制限情報のうち少なくとも１つを、前記制限手段で用いる利用制限情報として決定する決定手段をさらに備え、前記制御手段は、前記決定手段で決定した利用制限情報に基づいて機能の利用を制限することを特徴とする。
【００１０】
また、本発明は、パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置で行われる利用制限方法であって、前記認証手段で個人の認証が行われた際またはネットワークを介して接続された他の画像形成装置の認証手段で個

人の認証が行われた際、前記制限手段で、他の画像形成装置から予め取得した利用制限情報に基づいて機能の利用を制限することを特徴とする。

【００１１】

また、本発明は、パスワードなどを含む予め記憶した認証情報に基づいて個人の認証を行う認証手段と機能の利用についての利用制限情報に基づいて機能の利用を制限する制限手段とを備えた画像形成装置で行われる利用制限方法であって、前記認証手段で個人の認証が行われた際またはネットワークを介して接続された他の画像形成装置の認証手段で個人の認証が行われた際、前記制限手段で、当該画像形成装置で予め設定した利用制限情報に基づいて機能の利用を制限することを特徴とする。

【発明の効果】

【００１２】

本発明によれば、ネットワークを介して接続された他の画像形成装置からの認証要求に対して、予め記憶した認証情報に基づいて個人の認証を行うことが可能である。また、本発明によれば、ネットワークを介して接続された他の画像形成装置へ認証要求を行うことが可能である。これにより、管理者や利用者などへの作業負担を軽減すると共に、一定の権限を持つ者以外の者に対しても外部の認証情報に基づく認証を実施することができるという効果を奏する。つまり、本発明によれば、他の画像形成装置の認証情報を直接使用することで、利便性の向上、認証情報の有効活用を実現することができるという効果を奏する。

【００１３】

また、本発明によれば、ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報および予め設定した利用制限情報のうち少なくとも１つを、機能の利用を制限する際に用いる利用制限情報として決定し、決定した利用制限情報に基づいて機能の利用を制限する。これにより、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合には、当該他の画像形成装置が保持する利用制限情報をそのまま用いることができ、その結果、リソース使用量の削減と、新たな利用制限情報の設定に要する手間を省くことでの利便性の向上とを実現することができるという効果を奏する。また、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合であっても、予め設定した利用制限情報をそのまま用いることができ、その結果、セキュリティの向上を実現することができるという効果を奏する。また、他の画像形成装置から予め取得した利用制限情報と予め設定した利用制限情報とを組み合わせることで、細かな利用制限情報の設定が可能となるという効果を奏する。

【００１４】

また、本発明によれば、個人の認証が行われた際、ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報に基づいて機能の利用を制限する。これにより、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合には、当該他の画像形成装置が保持する利用制限情報をそのまま用いることができ、その結果、リソース使用量の削減と、新たな利用制限情報の設定に要する手間を省くことでの利便性の向上とを実現することができるという効果を奏する。

【００１５】

また、本発明によれば、個人の認証が行われた際、予め設定した利用制限情報に基づいて機能の利用を制限する。これにより、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合であっても、予め設定した利用制限情報をそのまま用いることができ、その結果、セキュリティの向上を実現することができるという効果を奏する。

【発明を実施するための最良の形態】

【００１６】

以下に、添付図面を参照して、本発明に係る画像形成装置および利用制限方法の最良な実施の形態を詳細に説明する。なお、本発明は当該実施の形態により限定されるものではない。

【００１７】

まず、本実施の形態に係る画像形成装置の構成について図１を参照して詳細に説明する。図１は、本実施の形態に係る画像形成装置の構成を示す図である。本実施の形態に係る画像形成装置は、ネットワークを介して他の画像形成装置と通信可能に接続されている。具体的には、図１に示すように、本実施の形態に係る画像形成装置１と画像形成装置２とは、インターネットやＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などのネットワーク３を介して通信可能に接続されている。なお、本実施の形態では、画像形成装置２の構成の説明は、画像形成装置１のそれと同様であるため、省略する。

【００１８】

画像形成装置１は、図１に示すように、主に、アプリケーション部１０と設定部１２とデータ管理部１４と管理データベース１４１と認証管理部１６と制限部１８とで構成されている。

【００１９】

アプリケーション部１０は、コピーやスキャナーやファックスなどの画像形成にかかる固有の処理を行うプログラムとして、図示の如く、コピーアプリ１０ａとスキャナアプリ１０ｂとファックスアプリ１０ｃとを含んで構成されている。

【００２０】

設定部１２は、画像形成装置１が備える各種の機能の利用についての利用制限情報を、データ管理部１４を介して管理データベース１４１に設定（登録）する処理を主に行う。具体的には、設定部１２は、以下の（１－１）から（１－５）などの処理を行う。

（１－１）利用制限情報を操作者に設定させるための利用制限情報設定画面を、当該画像形成装置１が備える表示部（図示せず）に表示する。

（１－２）操作者が利用制限情報設定画面を介して指示した利用制限情報の設定要求に対して、当該利用制限情報設定画面から利用制限情報を取得する。

（１－３）（１－２）で取得した利用制限情報を管理データベース１４１に設定（登録）するために、データ管理部１４に対して利用制限情報の設定要求を行う。

（１－４）データ管理部１４から転送された、（１－３）で行った設定要求に対する設定結果（登録結果）を受ける。

（１－５）（１－４）で受けた設定結果を利用制限情報設定画面に表示する。

【００２１】

データ管理部１４は、管理データベース１４１の管理に関する処理を主に行う。具体的には、データ管理部１４は、以下の（２－１）から（２－６）などの処理を行う。

（２－１）設定部１２からの利用制限情報の設定要求に対して、利用制限情報を管理データベース１４１に設定（登録）する。

（２－２）（２－１）での設定結果（登録結果）を設定部１２へ転送する。

（２－３）認証管理部１６からの認証情報の照合要求に対して、管理データベース１４１に予め記憶したユーザ情報１（具体的にはユーザ情報１に含まれる認証情報）から照合を行う。

（２－４）（２－３）での照合結果（具体的には「照合成功（ＯＫ）」／「照合失敗（ＮＧ）」の情報）を認証管理部１６へ転送する。

（２－５）認証管理部１６からの利用制限情報の取得要求に対して、管理データベース１４１に予め記憶した利用制限情報から所望の利用制限情報を取得したり、管理データベース１４１に予め記憶したユーザ情報１から所望の利用制限情報を抽出することで所望の利用制限情報を取得したりする。

（２－６）（２－５）での取得結果（具体的には取得した利用制限情報）を認証管理部１６へ転送する。

【００２２】

管理データベース１４１は、データ管理部１４の管理下に置かれており、画像形成装置１に関するユーザ情報（名前やメールアドレスやＦＡＸ番号や認証情報（パスワードなどを含む）などを含む）であるユーザ情報１、画像形成装置１が備える各種機能の利用についての認証者ごとの利用制限情報などを記憶する。

【００２３】
認証管理部１６は、データ管理部１４を介して、管理データベース１４１に予め記憶したユーザ情報１（具体的にはユーザ情報１に含まれる認証情報）に基づいて個人を認証する処理（本発明の認証手段が行う処理に対応）を主に行う。具体的には、認証管理部１６は、以下の（３－１）から（３－８）などの処理を行う。
（３－１）ネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）からの認証情報の認証要求やアプリケーション部１０からの認証情報の認証要求に対して、データ管理部１４を介して、管理データベース１４１に予め記憶したユーザ情報１（具体的にはユーザ情報１に含まれる認証情報）に基づいて個人の認証を行う。具体的には、ネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）からの認証情報の認証要求やアプリケーション部１０からの認証情報の認証要求を受けると、データ管理部１４に対して認証情報の照合要求を行ったり、データ管理部１４から転送された照合結果を受けたりする。
（３－２）アプリケーション部１０からの認証情報の認証要求に対して、ネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）へ認証情報の認証要求を行う。
（３－３）利用制限情報を既に取得したか否かを確認する。
（３－４）データ管理部１４に対して利用制限情報の取得要求を行う。例えば、（３－３）での確認結果が「取得あり」であった場合に、データ管理部１４に対して利用制限情報の取得要求を行う。
（３－５）データ管理部１４から転送された利用制限情報の取得結果（具体的には取得した利用制限情報）を受ける。
（３－６）（３－１）での照合結果や（３－３）での確認結果や（３－５）での取得結果を、ネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）へ転送する。
（３－７）利用制限情報を作成する。具体的には、データ管理部１４を介して管理データベース１４１から取得した利用制限情報や、ネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）から転送された利用制限情報に基づいて利用制限情報を作成する。なお、データ管理部１４を介して管理データベース１４１から取得した利用制限情報およびネットワーク３を介して接続された他の画像形成装置（図１では画像形成装置２の認証管理部２６）から転送された利用制限情報のうち少なくとも１つを、制限部１８で用いる利用制限情報として決定してもよい（本発明の決定手段が行う処理に対応）。
（３－８）既に取得したり作成したりした利用制限情報や上述した各種結果（具体的には、照合結果、確認結果、取得結果）をアプリケーション部１０へ転送する。
【００２４】
制限部１８は、利用制限情報に基づいて、当該画像形成装置１が備える各種機能の利用を制限する（本発明の制限手段が行う処理に対応）。
【００２５】
以上、本実施の形態に係る画像形成装置の構成について説明したが、画像形成装置１の認証管理部１６と画像形成装置２の認証管理部２６とは、要求情報などの送受信（受け渡し）を行うため、ＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）のサーバー／クライアントの関係になっている。換言すると、画像形成装置１と画像形成装置２との間で行われる要求情報などの受け渡しはＦＴＰで実施するため、画像形成装置１と画像形成装置２とはＦＴＰのサーバー・クライアントの関係になっている。また、本実施の形態では、２台の画像形成装置がネットワーク３を介して接続されている場合を一例として示したが、画像形成装置の台数はこれに限定するものではない。
【００２６】
以上の構成において、本実施の形態に係る画像形成装置が行う処理である、“利用制限情報の設定に関する処理”および“個人の認証から利用制限情報の取得・作成、そして利

用の制限までの一連の処理”について、図２を参照して詳細に説明する。図２は、本実施の形態に係る画像形成装置が行う処理の一例を示すシーケンス図である。

【００２７】

最初に、本実施の形態に係る画像形成装置が行う、利用制限情報の設定に関する処理について説明する。なお、本処理の説明は、図１に示す画像形成装置１を用いて行う。

【００２８】

まず、画像形成装置１の設定部１２は、当該画像形成装置１が備える表示部に利用制限情報設定画面を表示する（ステップＳＡ－１）。

【００２９】

つぎに、画像形成装置１の設定部１２は、操作者がステップＳＡ－１で表示した利用制限情報設定画面を介して指示した利用制限情報の設定要求を受ける（ステップＳＡ－２）と、当該利用制限情報設定画面から利用制限情報を取得し、データ管理部１４に対して、取得した利用制限情報を転送すると共に利用制限情報の設定要求を行う（ステップＳＡ－３）。

【００３０】

つぎに、画像形成装置１のデータ管理部１４は、ステップＳＡ－３で行った設定要求およびステップＳＡ－３で転送した利用制限情報を受けると、当該利用制限情報を管理データベース１４１に追加する（ステップＳＡ－４）。これにより、自機内で利用制限情報を保持することができた。

【００３１】

つぎに、画像形成装置１のデータ管理部１４は、ステップＳＡ－４で行った処理の結果（具体的には利用制限情報の設定結果）を設定部１２へ転送する（ステップＳＡ－５）。そして、画像形成装置１の設定部１２は、ステップＳＡ－５で転送した結果を受けると、当該結果を利用制限情報設定画面に表示する。

【００３２】

以上、利用制限情報の設定に関する処理の説明を終了する。

【００３３】

つぎに、本実施の形態に係る画像形成装置が行う、個人の認証から利用制限情報の取得・作成、そして利用の制限までの一連の処理について説明する。なお、本処理の説明は、図１に示す画像形成装置１および画像形成装置２を用いて行う。また、本処理の説明では、画像形成装置２の管理データベース２４１にはユーザ情報２のみが格納されているものとする。

【００３４】

まず、画像形成装置１のアプリケーション部１０（具体的には、コピーアプリ１０ａ、スキャナアプリ１０ｂ、ファックスアプリ１０ｃ）は、操作者（認証者、ログイン者）により指示されたアプリ移行の要求を受ける（ステップＳＡ－６）と、当該画像形成装置１が備える表示部にログイン画面を表示する（ステップＳＡ－７）。

【００３５】

つぎに、画像形成装置１のアプリケーション部１０は、操作者（認証者、ログイン者）がステップＳＡ－７で表示したログイン画面を介して指示した認証情報の認証要求を受ける（ステップＳＡ－８）と、当該ログイン画面から認証情報を取得し、認証管理部１６に対して、取得した認証情報を転送すると共に認証情報の認証要求を行う（ステップＳＡ－９）。

【００３６】

つぎに、画像形成装置１の認証管理部１６は、ステップＳＡ－９で行った認証要求およびステップＳＡ－９で転送した認証情報を受けると、ネットワーク３を介して、画像形成装置２の認証管理部２６に対して、当該認証情報を転送すると共に認証情報の認証要求を行う（ステップＳＡ－１０）。これにより、画像形成装置１は、ネットワーク３を介して接続された画像形成装置２に対して、認証要求を行うことができた。つまり、外部機器（ここでは画像形成装置２）へ認証要求を行うことができた。

【００３７】
つぎに、画像形成装置２の認証管理部２６は、ステップＳＡ－１０で行った認証要求およびステップＳＡ－１０で転送した認証情報を受けると、データ管理部２４に対して、当該認証情報を転送すると共に認証情報の照合要求を行う（ステップＳＡ－１１）。
【００３８】
つぎに、画像形成装置２のデータ管理部２４は、ステップＳＡ－１１で行った照合要求およびステップＳＡ－１１で転送した認証情報を受けると、当該認証情報に関し、管理データベース２４１に予め記憶したユーザ情報２（具体的には認証情報）から照合する（ステップＳＡ－１２）。
【００３９】
つぎに、画像形成装置２のデータ管理部２４は、ステップＳＡ－１２で行った処理の結果（具体的には認証情報の照合結果（照合成功（ＯＫ）／照合失敗（ＮＧ））））を認証管理部２６へ転送する（ステップＳＡ－１３）。
【００４０】
なお、上述したステップＳＡ－１１からステップＳＡ－１３までの処理は、本発明の認証手段が行う処理に対応する。これにより、外部機器（ここでは画像形成装置１）からの認証要求を処理することができた。
【００４１】
つぎに、画像形成装置２の認証管理部２６は、ステップＳＡ－１３で転送した結果（具体的には認証情報の照合結果）を受けると、利用制限情報を既に取得しているか否かを確認し、確認した結果が「取得なし」であった場合（ステップＳＡ－１４：「なし」）にはネットワーク３を介して画像形成装置１の認証管理部１６に対して当該受けた結果（具体的には認証情報の照合結果）を転送し（ステップＳＡ－１５）、確認した結果が「取得あり（取得済み）」であった場合（ステップＳＡ－１４：「あり」）にはデータ管理部２４に対して操作者（認証者、ログイン者）に関する利用制限情報の取得要求を行う（ステップＳＡ－１６）。
【００４２】
つぎに、画像形成装置２のデータ管理部２４は、ステップＳＡ－１６で行った取得要求を受けると、管理データベース２４１に予め記憶したユーザ情報２から操作者（認証者、ログイン者）に関する利用制限情報を抽出する（ステップＳＡ－１７）。
【００４３】
つぎに、画像形成装置２のデータ管理部２４は、ステップＳＡ－１７で行った処理の結果（具体的には利用制限情報の抽出結果（抽出成功（ＯＫ）／抽出失敗（ＮＧ）；抽出成功の場合には抽出した利用制限情報を含む））を認証管理部２６へ転送する（ステップＳＡ－１８）。
【００４４】
つぎに、画像形成装置２の認証管理部２６は、ステップＳＡ－１８で転送した結果（具体的には利用制限情報の抽出結果）を受けると、ネットワーク３を介して、画像形成装置１の認証管理部１６に対して、当該結果を、当該認証管理部２６が先に受けた結果（具体的には認証情報の照合結果）と共に転送する（ステップＳＡ－１９）。これにより、外部機器（ここでは画像形成装置１）に操作者（認証者、ログイン者）の利用制限情報を渡すことができた。
【００４５】
つぎに、画像形成装置１の認証管理部１６は、ステップＳＡ－１５で転送した結果（具体的には認証情報の照合結果）またはステップＳＡ－１９で転送した結果（具体的には認証情報の照合結果および利用制限情報の抽出結果）を受けると、データ管理部１４に対し、操作者（認証者、ログイン者）に関する利用制限情報の取得要求を行う（ステップＳＡ－２０）。
【００４６】
つぎに、画像形成装置１のデータ管理部１４は、ステップＳＡ－２０で行った取得要求

を受けると、管理データベース１４１に予め記憶した利用制限情報から操作者（認証者、ログイン者）に関する利用制限情報を取得する（ステップＳＡ－２１）。

【００４７】

つぎに、画像形成装置１のデータ管理部１４は、ステップＳＡ－２１で行った処理の結果（具体的には利用制限情報の取得結果（取得成功（ＯＫ）／取得失敗（ＮＧ）；取得成功の場合には取得した利用制限情報を含む））を認証管理部１６へ転送する（ステップＳＡ－２２）。

【００４８】

つぎに、画像形成装置１の認証管理部１６は、これまでの処理で取得した利用制限情報（具体的にはステップＳＡ－１７で抽出した利用制限情報および／またはステップＳＡ－２１で取得した利用制限情報）に基づいて、操作者（認証者、ログイン者）の利用制限情報を作成する（ステップＳＡ－２３）。これにより、制限部１８で用いる利用制限情報を決定することができた。なお、ステップＳＡ－２３において、ステップＳＡ－１７で抽出した利用制限情報およびステップＳＡ－２１で取得した利用制限情報のうち少なくとも１つを、そのまま、制限部１８で用いる利用制限情報として決定してもよい。

【００４９】

つぎに、画像形成装置１の認証管理部１６は、ステップＳＡ－２０で受けた結果（具体的には認証情報の照合結果）およびステップＳＡ－２３で作成した利用制限情報を、アプリケーション部１０へ転送する（ステップＳＡ－２４）。

【００５０】

つぎに、画像形成装置１のアプリケーション部１０は、ステップＳＡ－２４で転送した結果（具体的には認証情報の照合結果）および利用制限情報を受けると、ログイン画面の解除を行う（ステップＳＡ－２５）。そして、画像形成装置１の制限部１８は、ステップＳＡ－２５で受けた利用制限情報に基づいて、当該画像形成装置１が備える各種機能の利用を制限（許可）する。

【００５１】

以上、個人の認証から利用制限情報の取得・作成、そして利用の制限までの一連の処理の説明を終了する。

【００５２】

以上説明したように、画像形成装置１は、ネットワーク３を介して接続された画像形成装置２へ認証要求を行うことができる（図２のステップＳＡ－１０参照）。ゆえに、本実施の形態に係る画像形成装置は、ネットワークを介して接続された他の画像形成装置へ認証要求を行うことができる。また、画像形成装置２は、ネットワーク３を介して接続された画像形成装置１からの認証要求に対して、個人の認証に関する処理を行うことができる（図２のステップＳＡ－１１参照）。ゆえに、本実施の形態に係る画像形成装置は、ネットワークを介して接続された他の画像形成装置からの認証要求に対して、個人の認証に関する処理を行うことができる。これにより、管理者や利用者など操作者への作業負担を軽減すると共に、一定の権限を持つ者以外の者に対しても外部の認証情報に基づく認証を実施することができる。つまり、他の画像形成装置の認証情報を直接使用することで、利便性の向上、認証情報の有効活用を実現することができる。

【００５３】

ここで、これまで、セキュリティ対策として、画像形成装置でも個人認証による機器の利用許可、利用不許可とったアクセス制限を実施している。現状、認証の種類としては、自機内の認証データに基づいた個人認証と、機器外部の個人認証管理サーバーで一元的に管理されているデータに基づいた外部認証とがある。ここで、自機内の認証データに基づいた個人認証については、他機種の認証データを直接使用することができない。そのため、現状では、多数の機器同士でデータの一元管理をするためのサーバーを立てて、そこからデータを取得して自機内に保持したり、ＷＥＢやツール、持ち運び可能なメディアを用いて、バックアップリストアで他機種のデータを自機内にコピーしたりすることで、他機種と共通の認証データによる個人認証を可能としている。しかし、これらの方法を用いる

場合は、サーバーやツールといった手段を必要とするため、複数の手順を必要とし、一定の権限を持つ認証者しか実施できないといった制限がある。そこで、本実施の形態に係る画像形成装置では、他機種の認証データを直接使用することで、これら手順の簡略化や、制限を解消し、データを有効に活用することができる。つまり、本実施の形態に係る画像形成装置によれば、利便性の向上、データの有効活用を実現することができる。

【００５４】

また、画像形成装置１は、ステップＳＡ－１７で抽出した利用制限情報および／またはステップＳＡ－２１で取得した利用制限情報に基づいて、操作者（認証者、ログイン者）の利用制限情報を作成することで、制限部１８で用いる利用制限情報を決定することができる（図２のステップＳＡ－２３参照）。ゆえに、本実施の形態に係る画像形成装置は、ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報および当該画像形成装置で予め設定した利用制限情報のうち少なくとも１つを、機能の利用を制限する際に用いる利用制限情報として決定することができる。具体的には、本実施の形態に係る画像形成装置は、個人の認証が行われた際、ネットワークを介して接続された他の画像形成装置から予め取得した利用制限情報に基づいて機能の利用を制限することができる。また、具体的には、本実施の形態に係る画像形成装置は、個人の認証が行われた際、予め設定した利用制限情報に基づいて機能の利用を制限することができる。

【００５５】

これにより、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合には、当該他の画像形成装置が保持する利用制限情報をそのまま用いることができ、その結果、リソース使用量の削減と、新たな利用制限情報の設定に要する手間を省くことでの利便性の向上とを実現することができる。また、例えば、他の画像形成装置の認証結果で機能の利用を制限（許可）する場合であっても、予め設定した利用制限情報をそのまま用いることができ、その結果、セキュリティの向上を実現することができる。また、他の画像形成装置から予め取得した利用制限情報と予め設定した利用制限情報とを組み合わせることで、細かな利用制限情報の設定が可能となる。換言すると、他機器の利用制限情報と自機の利用制限情報とを組み合わせることができる（例えば、機器内と機器外の利用制限情報を同時に使用することが可能である）ので、細かい利用制限の設定が可能となる。つまり、他機器の利用制限情報と自機の利用制限情報とを組み合わせることで、利用制限の設定時の利便性の向上とセキュリティの向上を実現することができる。

【００５６】

ここで、他機器の認証結果で自機の利用を許可する場合、セキュリティ的にも認証者にどの機能を許可するかについて制限する必要がある。しかし、自機内にそのための情報を持つには、手間もかかるし、設定数によってはリソースも多く使う。そこで、本実施の形態に係る画像形成装置では、外部から取得した利用制限情報を使用可能にすることで、リソース使用量の削減と、設定の手順を省くことでの利便性の向上を実現することができる。つまり、他機器の利用制限情報をそのまま使うことで、利用制限の設定を省略することが可能となる。ただし、他機器の利用制限情報を自機で使用すると、自機で制御することができなくなる場合がある。そして、この場合、他機器で管理者の権限を持っていると、セキュリティ的に問題が生じる可能性がある。そこで、本実施の形態に係る画像形成装置では、自機の利用制限情報も作成可能とすることで、セキュリティの向上も実現することができる。

【００５７】

（付記１）

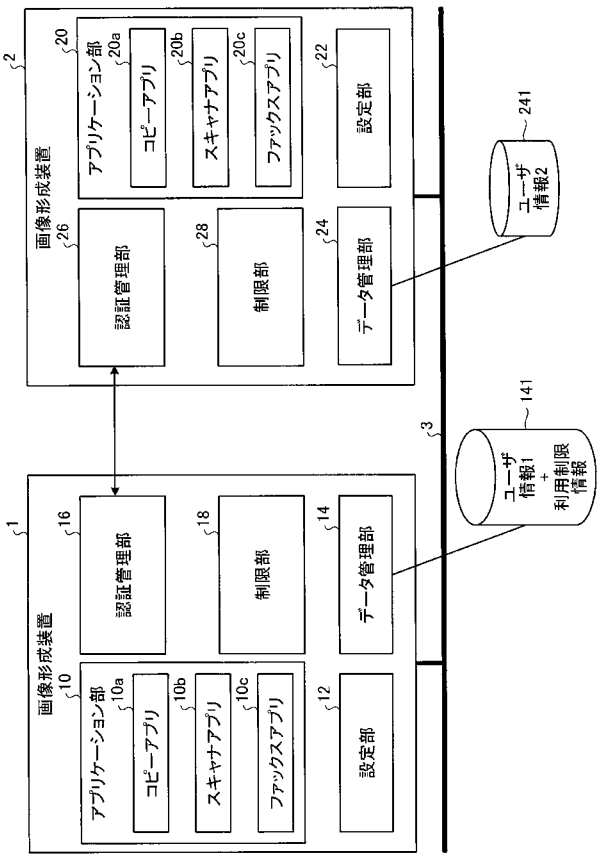
機器使用時に自機内の認証情報に基づいて個人を認証する手段を備え、認証者毎に機器の利用についての利用制限情報を管理する手段を備え、利用制限情報に基づいて機器の利用を制限することが可能な画像形成装置であって、

ネットワークを介して接続された他の画像形成装置からの個人認証要求に対して、自機内の認証情報を元に認証することが可能であることを特徴とする画像形成装置。

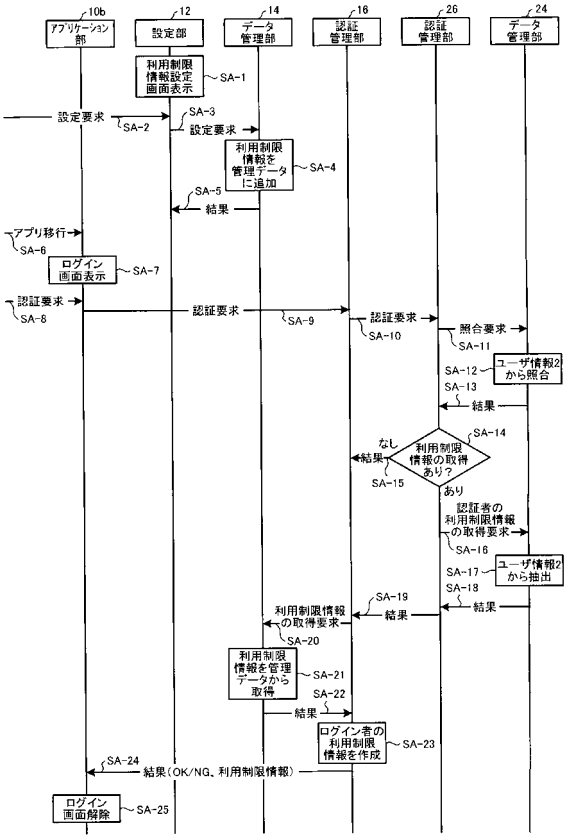
（付記２）

機器使用時に個人を認証するための手段を備え、認証者毎の利用制限情報に基づいて機器の利用を制限することが可能な画像形成装置であって、
ネットワークを介して接続された付記１記載の画像形成装置に対して個人認証要求を行うことが可能であることを特徴とする画像形成装置。
（付記３）
付記２で認証が実施された際、他機器から取得した利用制限情報に従って機器の利用を制限することを特徴とした利用制限方法。
（付記４）
付記２で認証が実施された際、自機で設定した利用制限情報に従って機器の利用を制限することを特徴とした利用制限方法。
（付記５）
付記３記載の他機器から取得した利用制限情報に従うか、付記４記載の自機内の利用制限情報に従うか、予め設定する手段を持つことを特徴とする付記１または付記２に記載の画像形成装置。
【図面の簡単な説明】
【００５８】
【図１】本実施の形態に係る画像形成装置の構成を示す図である。
【図２】本実施の形態に係る画像形成装置が行う処理の一例を示すシーケンス図である。
【符号の説明】
【００５９】
１，２　画像形成装置
　　１０，２０　アプリケーション部
　　　　１０ａ，２０ａ　コピーアプリ
　　　　１０ｂ，２０ｂ　スキャナアプリ
　　　　１０ｃ，２０ｃ　ファックスアプリ
　　１２，２２　設定部
　　１４，２４　データ管理部
　　　　１４１，２４１　管理データベース
　　１６，２６　認証管理部
　　１８，２８　制限部
３　　ネットワーク

【図１】


画像形成装置
2
アプリケーション部
20
コピーアプリ
20a
スキャナアプリ
20b
ファックスアプリ
20c
設定部
22
認証管理部
26
制限部
28
データ管理部
24
ユーザ情報2
241
3
ユーザ情報1＋利用制限情報
141
画像形成装置
1
認証管理部
16
制限部
18
データ管理部
14
アプリケーション部
10
コピーアプリ
10a
スキャナアプリ
10b
ファックスアプリ
10c
設定部
12

【図２】


アプリケーション部
10b
設定部
12
データ管理部
14
認証管理部
16
認証管理部
26
データ管理部
24
利用制限情報設定画面表示
SA-1
設定要求
SA-2
SA-3
設定要求
利用制限情報を管理データに追加
SA-4
SA-5
結果
アプリ移行
SA-6
ログイン画面表示
SA-7
認証要求
SA-8
認証要求
SA-9
認証要求
SA-10
照合要求
SA-11
SA-12
ユーザ情報2から照合
SA-13
結果
なし
結果
SA-15
利用制限情報の取得あり？
SA-14
あり
認証者の利用制限情報の取得要求
SA-16
SA-17
ユーザ情報2から抽出
SA-18
結果
SA-19
結果
利用制限情報の取得要求
SA-20
利用制限情報を管理データから取得
SA-21
SA-22
結果
ログイン者の利用制限情報を作成
SA-23
SA-24
結果（OK/NG、利用制限情報）
ログイン画面解除
SA-25