(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6507863号
(P6507863)
(45)発行日　令和1年5月8日(2019.5.8)　(24)登録日　平成31年4月12日(2019.4.12)

(51)Int.Cl.　F I
G06F 21/31 (2013.01)　G06F 21/31
G06F 21/62 (2013.01)　G06F 21/62

請求項の数 4　(全 25 頁)

(21)出願番号　特願2015-113041(P2015-113041)
(22)出願日　平成27年6月3日(2015.6.3)
(65)公開番号　特開2016-224849(P2016-224849A)
(43)公開日　平成28年12月28日(2016.12.28)
審査請求日　平成30年2月28日(2018.2.28)

(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　110001210
特許業務法人ＹＫＩ国際特許事務所
(72)発明者　鈴木　善晴
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】情報処理装置及びプログラム

(57)【特許請求の範囲】
【請求項１】
利用のリクエストを第１端末装置から受け、前記利用に必要な認証方式を特定する特定手段と、
前記第１端末装置が対応している認証方式が、前記特定された認証方式に適合していない場合に、前記特定された認証方式に対応している第２端末装置に関する情報を、前記第１端末装置に出力するよう制御する制御手段と、
前記利用のリクエスト時に前記第１端末装置にて表示されている画面に関する画面情報を記憶する画面情報記憶手段と、
を有し、
前記制御手段は、更に、前記第２端末装置において前記特定された認証方式に従った認証が成功した場合、前記画面情報記憶手段に記憶されている前記画面情報を前記第２端末装置に出力するよう制御する、
情報処理装置。
【請求項２】
前記利用のリクエストに応じて、前記第１端末装置から取得された認証方式を示す情報を記憶する記憶手段を更に有し、
前記制御手段は、前記記憶手段に記憶された情報に基づいて前記第２端末装置を特定する、
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】
前記第１端末装置及び前記第２端末装置の位置情報を取得する位置取得手段を更に有し、
前記制御手段は、前記第１端末装置の位置情報及び前記第２端末装置の位置情報に応じて、前記第２端末装置に関する情報を異ならせて出力するように制御する、
ことを特徴とする請求項１又は請求項２に記載の情報処理装置。
【請求項４】
コンピュータを、
利用のリクエストを第１端末装置から受け、前記利用に必要な認証方式を特定する特定手段と、
前記第１端末装置に対応している認証方式が、前記特定された認証方式に適合していない場合に、前記特定された認証方式に対応している第２端末装置に関する情報を、前記第１端末装置に出力するよう制御する制御手段と、
として機能させ、
前記制御手段は、更に、前記利用のリクエスト時に前記第１端末装置にて表示されている画面に関する画面情報を画面情報記憶手段に記憶させ、前記第２端末装置において前記特定された認証方式に従った認証が成功した場合、前記画面情報記憶手段に記憶されている前記画面情報を前記第２端末装置に出力するよう制御する、
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置及びプログラムに関する。
【背景技術】
【０００２】
データのセキュリティ上の重要度等に応じて、ユーザに対して要求する認証方式を切り替える技術が知られている。
【０００３】
例えば特許文献１には、ＩＤ及びパスワードのみの認証と生体認証とがユーザによって選択されるようにしたシステムが開示されている。
【０００４】
特許文献２には、複数の認証方式の組み合わせを認証レベルとして定義し、その認証レベルによってアクセス操作を制限する装置が開示されている。
【０００５】
特許文献３には、生体認証を利用することにより、文書データへのアクセスを許可又は制限するシステムが開示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００３－３０３１７５号公報
【特許文献２】特開２００７－１５６９５９号公報
【特許文献３】特開２００４－５２７３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ところで、ユーザが利用する装置が、サービスの利用に要求される認証方式に対応していない場合があり得る。
【０００８】
本発明の目的は、要求される認証方式に対応していない端末装置に対して、当該認証方式に対応している端末装置に関する情報を提供することである。

【課題を解決するための手段】
【０００９】
請求項１に係る発明は、利用のリクエストを第１端末装置から受け、前記利用に必要な認証方式を特定する特定手段と、前記第１端末装置が対応している認証方式が、前記特定された認証方式に適合していない場合に、前記特定された認証方式に対応している第２端末装置に関する情報を、前記第１端末装置に出力するよう制御する制御手段と、前記利用のリクエスト時に前記第１端末装置にて表示されている画面に関する画面情報を記憶する画面情報記憶手段と、を有し、前記制御手段は、更に、前記第２端末装置において前記特定された認証方式に従った認証が成功した場合、前記画面情報記憶手段に記憶されている前記画面情報を前記第２端末装置に出力するよう制御する、情報処理装置である。
【００１０】
請求項２に係る発明は、前記利用のリクエストに応じて、前記第１端末装置から取得された認証方式を示す情報を記憶する記憶手段を更に有し、前記制御手段は、前記記憶手段に記憶された情報に基づいて前記第２端末装置を特定する、ことを特徴とする請求項１に記載の情報処理装置である。
【００１１】
請求項３に係る発明は、前記第１端末装置及び前記第２端末装置の位置情報を取得する位置取得手段を更に有し、前記制御手段は、前記第１端末装置の位置情報及び前記第２端末装置の位置情報に応じて、前記第２端末装置に関する情報を異ならせて出力するように制御する、ことを特徴とする請求項１又は請求項２に記載の情報処理装置である。
【００１３】
請求項４に係る発明は、コンピュータを、利用のリクエストを第１端末装置から受け、前記利用に必要な認証方式を特定する特定手段と、前記第１端末装置に対応している認証方式が、前記特定された認証方式に適合していない場合に、前記特定された認証方式に対応している第２端末装置に関する情報を、前記第１端末装置に出力するよう制御する制御手段と、として機能させ、前記制御手段は、更に、前記利用のリクエスト時に前記第１端末装置にて表示されている画面に関する画面情報を画面情報記憶手段に記憶させ、前記第２端末装置において前記特定された認証方式に従った認証が成功した場合、前記画面情報記憶手段に記憶されている前記画面情報を前記第２端末装置に出力するよう制御する、プログラムである。
【発明の効果】
【００１４】
請求項１，４に係る発明によると、要求される認証方式に対応していない端末装置に対して、当該認証方式に対応している端末装置に関する情報が提供される。また、ユーザによる無駄な操作の発生が防止又は低減される。
【００１５】
請求項２に係る発明によると、端末装置から得られた情報によって、認証方式に対応している端末装置が特定される。
【００１６】
請求項３に係る発明によると、ユーザにとって利用しやすい端末装置に関する情報が優先的に提供され得る。
【図面の簡単な説明】
【００１８】
【図１】本発明の実施形態に係る文書管理システムの一例を示すブロック図である。
【図２】本実施形態に係る文書管理装置の一例を示すブロック図である。
【図３】画像形成装置の一例を示すブロック図である。
【図４】画像形成装置の一例を示すブロック図である。
【図５】携帯端末の一例を示すブロック図である。
【図６】オブジェクト権限テーブルの一例を示す図である。
【図７】認証方式テーブルの一例を示す図である。

【図８】データ形式テーブルの一例を示す図である。
【図９】代替認証方式テーブルの一例を示す図である。
【図１０】認証端末テーブルの一例を示す図である。
【図１１】文書管理システムにて実行される処理の一例を示すフローチャートである。
【図１２】文書管理装置にて実行される処理の一例を示すフローチャートである。
【図１３】代替顔認証処理の一例を示すフローチャートである。
【図１４】追加認証処理の一例を示すフローチャートである。
【図１５】画像形成装置の画面の一例を示す図である。
【図１６】画像形成装置の画面の一例を示す図である。
【図１７】画像形成装置の画面の一例を示す図である。
【図１８】画像形成装置の画面の一例を示す図である。
【発明を実施するための形態】
【００１９】
図１には、本発明の実施形態に係る文書管理システムの一例が示されている。文書管理システムは、例えば、情報処理装置としての文書管理装置１０と、端末装置としての複数の画像形成装置（一例として、画像形成装置１２Ａ，１２Ｂ）と、を含む。文書管理装置１０及び画像形成装置１２Ａ，１２Ｂは、ネットワーク等の通信経路Ｎに接続されている。また、携帯端末１４が通信経路Ｎに接続されている。なお、図１に示す例では、２台の画像形成装置が文書管理システムに含まれているが、これは一例に過ぎず、３台以上の画像形成装置が文書管理システムに含まれていてもよい。また、携帯端末１４は文書管理システムに含まれていなくてもよい。
【００２０】
文書管理装置１０は文書データを格納する装置であり、他の装置との間でデータを送受信する機能を備えている。文書データは、例えば、画像形成装置１２Ａ，１２Ｂ等の装置から文書管理装置１０に対して提供されるデータである。文書データは、文字によって表されるテキストデータであってもよいし、画像データであってもよいし、文字や画像によって表されるデータであってもよい。
【００２１】
画像形成装置１２Ａ，１２Ｂは、スキャン機能、プリンタ機能、コピー機能及びファクシミリ機能の中の少なくとも１つの機能を備えた装置である。また、画像形成装置１２Ａ，１２Ｂは、他の装置との間でデータを送受信する機能を備えている。本実施形態では一例として、画像形成装置１２Ａにカメラ等の撮像部が設けられており、画像形成装置１２Ｂには撮像部が設けられていないものとする。その撮像部は、例えば、顔認証に用いられるものである。
【００２２】
携帯端末１４は、カメラ等の撮像部を備えた装置であり、例えば、スマートフォン、携帯電話、タブレットＰＣ（パーソナルコンピュータ）又はＰＣ等の装置である。また、携帯端末１４は、他の装置との間でデータを送受信する機能を備えている。
【００２３】
例えば、画像形成装置１２Ａ，１２Ｂ等の装置を利用して文書管理装置１０にログインし、画像形成装置１２Ａ，１２Ｂ等の装置において、文書管理装置１０に格納されている文書データが利用されることが想定される。別の例として、画像形成装置１２Ａ，１２Ｂ等の装置によって文書データが作成され、その文書データが文書管理装置１０に送信されて格納されてもよい。本実施形態では、そのログインや利用等に際して、認証が要求される場合がある。
【００２４】
以下、文書管理装置１０、画像形成装置１２Ａ，１２Ｂ、及び、携帯端末１４の構成について詳しく説明する。
【００２５】
図２には、文書管理装置１０の構成が示されている。

【００２６】
通信部１６は通信インターフェースであり、他の装置にデータを送信する機能、及び、他の装置からデータを受信する機能を備えている。例えば、通信部１６によって、文書データの送受信や認証情報の受信等が行われる。
【００２７】
認証部１８は、認証情報を利用して認証処理を行う機能を備えている。認証処理としては、例えば、パスワードやユーザＩＤ等の情報を認証情報として利用するパスワード認証処理、ＩＣカードに格納された情報（例えばＩＤやパスワード）を認証情報として利用するＩＣカード認証、ユーザの生体情報を認証情報として利用する生体認証処理、等が利用される。生体認証処理としては、ユーザの顔を表す顔画像データを利用する顔認証処理、ユーザの声を示す音声データを利用する音声認証処理、ユーザの指紋情報を利用する指紋認証処理、ユーザの静脈パターンを利用する静脈認証処理、等が利用される。もちろん、これら以外の認証処理が行われてもよい。認証情報は記憶部２２に記憶されている。例えば、文書管理装置１０へのログイン時や特定の文書データへのアクセス時等に、画像形成装置１２Ａ，１２Ｂ等の装置から認証情報が送信されると、認証部１８は、記憶部２２に記憶されている認証情報と送信された認証情報とを用いて認証処理を行う。両認証情報が適合して認証が成功した場合（例えば両認証情報が一致した場合）、ログインやアクセスが許可される。認証が失敗した場合（例えば両認証情報が一致しない場合）、ログインやアクセスが禁止される。
【００２８】
オブジェクト管理部２０は、オブジェクトを管理する機能を備えている。オブジェクトは、例えば、文書データや文書データが格納されているフォルダ、等である。例えば、オブジェクト管理部２０は、文書管理装置１０に格納されている文書データ、文書データが格納されているフォルダ等の格納場所、及び、文書データやフォルダに対する操作権限（アクセス権限）、等を管理する。一例として、オブジェクト管理部２０は、画像形成装置１２Ａ，１２Ｂ等の装置から送信された文書データを記憶部２２に格納する。
【００２９】
記憶部２２はハードディスク等の記憶装置である。記憶部２２には、文書データや認証情報等が格納される。
【００３０】
制御部２４は、文書管理装置１０の各部の動作を制御する機能を備えている。また、制御部２４には、代替認証情報生成部２６が含まれている。
【００３１】
代替認証情報生成部２６は、文書管理装置１０を利用しようとする装置がその利用に際して要求される認証方式に対応していない場合に、当該認証方式に対応している装置に関する情報を生成する機能を備えている。例えば、文書管理装置１０へのログインに使用される装置が、そのログインに要求される認証方式に対応していない場合、代替認証情報生成部２６は、その認証方式に対応している装置に関する情報を生成する。また、代替認証情報生成部２６は、その認証方式に替わる代替認証方式に関する情報を生成してもよい。これらの情報は当該装置に送信される。代替認証情報生成部２６による処理については、図１１以降の図面を参照して詳しく説明する。
【００３２】
図３には、画像形成装置１２Ａの構成が示されている。
【００３３】
通信部２８は通信インターフェースであり、他の装置にデータを送信する機能、及び、他の装置からデータを受信する機能を備えている。例えば、通信部２８によって、文書データの送受信や認証情報の送信等が行われる。
【００３４】
画像形成部３０は、スキャン機能、プリンタ機能、コピー機能及びファクシミリ機能の中の少なくとも１つの機能を備えている。例えば、スキャン機能が実行されることにより

文書データが生成され、その文書データが文書管理装置１０に送信されて格納されてもよい。別の例として、プリンタ機能が実行されることにより、文書管理装置１０に格納されている文書データが印刷されてもよい。

【００３５】

記憶部３２はハードディスク等の記憶装置である。記憶部３２には、例えば文書データ等が格納される。

【００３６】

ＵＩ部３４はユーザインターフェースであり、表示部と操作部とを含む。表示部は、例えば液晶ディスプレイ等の表示装置である。操作部は、例えば操作パネル等の入力装置である。

【００３７】

撮像部３６はカメラである。例えば顔認証処理が適用される場合に、撮像部３６が利用される。画像形成装置１２Ａに撮像部３６が設けられていることにより、画像形成装置１２Ａは、顔認証の方式に対応している装置に相当する。

【００３８】

制御部３８は、画像形成装置１２Ａの各部の動作を制御する。

【００３９】

図４には、画像形成装置１２Ｂの構成が示されている。画像形成装置１２Ｂは、画像形成装置１２Ａと同様に、通信部２８、画像形成部３０、記憶部３２、ＵＩ部３４及び制御部３８を備えている。画像形成装置１２Ａと異なり、画像形成装置１２Ｂには、撮像部３６が設けられていない。つまり、画像形成装置１２Ｂは、顔認証の方式に対応していない装置に相当する。

【００４０】

図５には、携帯端末１４の構成が示されている。携帯端末１４は、例えば、代替認証方式に従った認証処理が適用される場合に利用される装置である。通信部４０は通信インターフェースであり、他の装置にデータを送信する機能、及び、他の装置からデータを受信する機能を備えている。撮像部４２はカメラである。例えば、代替認証方式として顔認証方式が適用される場合に、撮像部４２が利用される。ＵＩ部４４はユーザインターフェースであり、表示部と操作部とを含む。表示部は、例えば液晶ディスプレイ等の表示装置である。操作部は、例えばタッチパネルやキーボード等の入力装置である。制御部４６は、携帯端末１４の各部の動作を制御する。

【００４１】

以下、文書管理装置１０について詳しく説明する。

【００４２】

図６には、オブジェクト権限テーブルの一例が示されている。このオブジェクト権限テーブルは、文書データやフォルダ等に対する操作に要求される認証の方式を示す情報である。このオブジェクト権限テーブルは、文書管理装置１０のオブジェクト管理部２０によって作成され、記憶部２２に記憶される。例えば、文書データが文書管理装置１０に格納される度に、オブジェクト権限テーブルの内容が更新される。

【００４３】

具体的には、オブジェクト権限テーブルには、オブジェクトＩＤ、対象操作、及び、要求認証方式ＩＤの対応関係が示されている。オブジェクトＩＤは、文書管理装置１０の記憶部２２に格納されている文書データを識別するための文書識別情報（例えば「文書－１」等）、又は、記憶部２２において文書データが格納されているフォルダを識別するためのフォルダ識別情報（例えば「フォルダ－１」等）、等である。対象操作は、対応する文書データやフォルダに対する操作の内容である。要求認証方式ＩＤは、その対象操作に対して要求される認証の方式を示す情報である。例えば、「文書－１」の文書データについては、更新以外の操作には認証が要求されていない。つまり、「文書－１」の文書データに対して、更新以外の操作を行うときには認証が要求されないことになる。一方、「文書－２」の文書データについては、更新操作に、認証方式３による認証が要求されている。

つまり、「文書－２」の文書データに対して更新操作を行うときには、認証方式３に従った認証が要求されることになる。他のオブジェクトについても同様に、当該オブジェクトに対する操作の際に要求される認証方式を示す情報が対応付けられている。このオブジェクト権限テーブルを参照することにより、特定の文書データやフォルダに対する操作に要求される認証の方式が特定されることになる。各オブジェクトに要求される認証方式は、例えば、各オブジェクトの管理者によって設定されてもよいし、文書データ等のユーザによって設定されてもよい。もちろん、その認証方式は別の基準によって設定されてもよい。

【００４４】

図７には、認証方式テーブルの一例が示されている。この認証方式テーブルは、認証方式を示す情報である。認証方式テーブルは、例えば予め作成されて文書管理装置１０の記憶部２２に記憶されている。

【００４５】

具体的には、認証方式テーブルには、認証方式ＩＤ、認証方式名称、及び、データ形式ＩＤの対応関係が示されている。認証方式ＩＤは、認証方式を識別するための認証方式識別情報である。認証方式名称は、認証方式の名称である。データ形式ＩＤは、対応する認証方式に用いられるデータの形式を示す情報である。例えば、認証方式１はＩＤ・パスワード認証であり、その認証においてはデータ形式ＩＤ「０」のデータが用いられる。また、認証方式３は顔認証であり、その認証においてはデータ形式ＩＤ「２」のデータが用いられる。

【００４６】

図８には、データ形式テーブルの一例が示されている。このデータ形式テーブルは、データ形式の名称を示す情報である。データ形式テーブルは、例えば予め作成されて、文書管理装置１０の記憶部２２と画像形成装置１２Ａ，１２Ｂの記憶部３２に記憶されている。

【００４７】

具体的には、データ形式テーブルには、データ形式ＩＤとデータ形式名称との対応関係が示されている。このデータ形式ＩＤは、文書管理装置１０と画像形成装置１２Ａ，１２Ｂとで共通のＩＤである。例えば、データ形式ＩＤ「０」は文字列を示しており、データ形式ＩＤ「２」は「写真画像」を示している。

【００４８】

例えば図６及び図７に示されているテーブルを例に挙げて説明すると、「フォルダ－１」に対する操作には、認証方式３による認証が要求されており、その認証方式３には、データ形式ＩＤ「２」のデータが用いられる。つまり、この操作には、「写真画像」を利用した「顔認証」が要求されることになる。

【００４９】

図９には、代替認証方式テーブルの一例が示されている。この代替認証方式テーブルは、要求されている認証方式に替わる代替認証方式を示す情報である。代替認証方式テーブルは、例えば予め作成されて文書管理装置１０の記憶部２２に記憶されている。

【００５０】

具体的には、代替認証方式テーブルには、代替方式ＩＤ、代替方式名称、及び、認証方式ＩＤの対応関係が示されている。代替方式ＩＤは、要求されている認証方式に替わる代替認証方式を示す情報である。代替方式名称は、その代替認証方式の名称である。認証方式ＩＤは、要求されている認証方式を示す情報である。例えば、認証方式３は顔認証を示しており、その顔認証の代替認証方式として、代替方式１が用意されている。この代替方式１による認証は、携帯端末でのカメラ認証である。顔認証に対応していない装置が利用される場合、携帯端末を利用したカメラ認証が、顔認証の替わりとして利用されることが想定される。

【００５１】

図１０には、認証端末テーブルの一例が示されている。この認証端末テーブルは、文書

管理装置１０に対して利用リクエスト情報を送信したリクエスト装置に関する情報である。利用リクエスト情報は、文書管理装置１０へのログイン要求や、文書データやフォルダに対する操作要求、等を示す情報である。文書管理装置１０が文書管理装置１０以外の装置から利用リクエスト情報を受ける度に、認証端末テーブルが代替認証情報生成部２６によって更新される。

【００５２】

具体的には、認証端末テーブルには、端末ＩＤ、最終ネゴシエーション日時、ＩＰアドレス、位置情報、設置位置の説明、及び、送信対応データ形式ＩＤの対応関係が示されている。端末ＩＤは、文書管理装置１０に対して利用リクエスト情報を送信したリクエスト装置（例えば画像形成装置１２Ａ，１２Ｂ等）を識別するための装置識別情報である。最終ネゴシエーション日時は、当該利用リクエスト情報が送信された最新の日時である。ＩＰアドレスは、当該リクエスト装置のＩＰアドレスである。位置情報は、当該リクエスト装置の位置を示す座標であり、例えば、緯度と経度を示す情報である。設置位置の説明は、当該リクエスト装置が設置されている場所についての説明である。送信対応データ形式ＩＤは、当該リクエスト装置が対応しているデータの形式を示す情報であり、図８に示されているデータ形式テーブル中のデータ形式ＩＤに対応する情報である。図７に示すように、認証方式テーブルにおいて、データ形式ＩＤは認証方式ＩＤに対応しているため、送信対応データ形式ＩＤは、当該リクエスト装置がどのような認証方式に対応しているかを示す情報であるとも言える。

【００５３】

例えば、端末ＩＤが「１」の装置について説明すると、最終ネゴシエーション日時は「２０１５年1月1日１０時１０分１０秒」であり、ＩＰアドレスは「１２３．４５６．１１１．２２２」であり、位置（座標）は「ＸＸＸ，ＹＹＹ」である。また、その装置は、１０階の南側に設置されている。その装置が対応しているデータ形式のＩＤは「０」と「２」であるため、その装置は、文字列（ＩＤ＝０）と写真画像（ＩＤ＝２）に対応していることになる。つまり、その装置は、ＩＤ・パスワード認証（認証方式１）と顔認証（認証方式３）に対応していることになる。

【００５４】

例えば、利用リクエスト情報とともに、当該利用リクエスト情報を送信したリクエスト装置を示す端末ＩＤ、ＩＰアドレス、位置情報、設置場所の説明情報、及び、送信対応データ形式ＩＤが、当該リクエスト装置から文書管理装置１０へ送信される。代替認証情報生成部２６は、それらの情報によって認証端末テーブルを更新する。つまり、認証端末テーブルは、リクエスト装置からのアクセスの履歴を示す履歴情報に相当する。後述するように、認証端末テーブルを利用することにより、リクエスト装置が対応していない認証方式に対応している代替装置が検索される。

【００５５】

以下、本実施形態に係る文書管理システムにて実行される処理（認証ネゴシエーション処理）について説明する。図１１には、その処理の一例が示されている。一例として、ユーザが撮像部３６（カメラ）を備えていない画像形成装置１２Ｂを用いて、文書管理装置１０にログインする場合における処理について説明する。この場合、画像形成装置１２Ｂがリクエスト装置に相当する。

【００５６】

まず、画像形成装置１２Ｂにおいて、ユーザがＵＩ部３４を利用することにより、文書管理装置１０へのログインを指示する（Ｓ０１）。画像形成装置１２Ｂにおいては、制御部３８が、その指示に応じて利用リクエスト情報（認証ネゴシエーションリクエスト情報）を作成する（Ｓ０２）。この利用リクエスト情報には、ログインを要求するログイン要求情報、画像形成装置１２Ｂを識別するための端末ＩＤ、画像形成装置１２Ｂに割り当てられているＩＰアドレス、画像形成装置１２Ｂの位置情報（例えば緯度と経度を示す情報）、画像形成装置１２Ｂの設置場所の説明情報、及び、画像形成装置１２Ｂが対応しているデータの形式ＩＤ（送信対応データ形式ＩＤ）、が含まれる。なお、送信対応データ形

式ＩＤに替えて、又は、それとともに、画像形成装置１２Ｂが対応している認証方式のＩＤが、利用リクエスト情報に含まれてもよい。これらの情報は、予め画像形成装置１２Ｂの記憶部３２に記憶されている。そして、利用リクエスト情報は、通信部２８によって、画像形成装置１２Ｂから文書管理装置１０に送信される（Ｓ０２）。

【００５７】

文書管理装置１０においては、画像形成装置１２Ｂから送信された利用リクエスト情報が、通信部１６によって受信される（Ｓ０３）。

【００５８】

次に、代替認証情報生成部２６は、利用リクエスト情報に含まれる情報を記憶部２２に保存する（Ｓ０４）。例えば、代替認証情報生成部２６は、利用リクエスト情報に含まれる情報を、図１０に示されている認証端末テーブルに追加する。認証端末テーブルに画像形成装置１２Ｂに関する情報が既に登録されている場合、代替認証情報生成部２６は、当該情報を、新たに受けた利用リクエスト情報に含まれる情報に更新する。一例として、画像形成装置１２Ｂの端末ＩＤが「３」であるとすると、その端末ＩＤ３に対応する情報が認証端末テーブルに登録される。

【００５９】

次に、代替認証情報生成部２６は、利用リクエスト情報から送信対応データ形式ＩＤを抽出する（Ｓ０５）。また、代替認証情報生成部２６は、認証方式要件セットを取得する（Ｓ０６）。この認証方式要件セットには、文書管理装置１０へのログインに要求されるログイン認証方式のＩＤと、図６に示されているオブジェクト権限テーブルに示されている各オブジェクトの操作毎の要求認証方式ＩＤと、が含まれる。例えば、ログイン認証方式ＩＤは、文書管理装置１０の記憶部２２に記憶されていてもよいし、オブジェクト権限テーブルに登録されていてもよい。代替認証情報生成部２６は、記憶部２２又はオブジェクト権限テーブルからログイン認証方式ＩＤを取得し、オブジェクト権限テーブルから各オブジェクトの操作毎の要求認証方式ＩＤを取得する。これにより、認証方式要件セットが作成される。例えば、代替認証情報生成部２６は、オブジェクト権限テーブルから、全オブジェクトの操作毎の要求認証方式ＩＤを取得する。この場合、認証方式要件セットには、全オブジェクトの操作毎の要求認証方式ＩＤが含まれる。

【００６０】

そして、代替認証情報生成部２６は、図７に示されている認証方式テーブルを参照し、認証方式要件セットと送信対応データ形式ＩＤとに基づいて、認証対応方式セットと認証未対応方式セットとを作成する（Ｓ０７）。認証対応方式セットは、認証方式要件セットに含まれる認証方式ＩＤ群（ログイン認証方式ＩＤと要求認証方式ＩＤ群）の中で、画像形成装置１２Ｂが対応している認証方式ＩＤのセット（集合）を示す情報である。例えば、画像形成装置１２Ｂがログイン認証方式に対応している場合、認証対応方式セットには、そのログイン認証方式ＩＤが含まれる。また、認証対応方式セットには、画像形成装置１２Ｂが対応している各オブジェクトの操作毎の要求認証方式ＩＤが含まれる。認証未対応方式セットは、認証方式要件セットに含まれる認証方式ＩＤ群の中で、画像形成装置１２Ｂが対応していない認証方式ＩＤのセット（集合）を示す情報である。例えば、画像形成装置１２Ｂがログイン認証方式に対応していない場合、認証未対応方式セットには、そのログイン認証方式ＩＤが含まれる。また、認証未対応方式セットには、画像形成装置１２Ｂが対応していない各オブジェクトの操作毎の要求認証方式ＩＤが含まれる。認証方式テーブルには、データ形式ＩＤと認証方式ＩＤとが対応付けられているため、認証方式テーブルを参照することにより、送信対応データ形式ＩＤに対応する認証方式ＩＤが特定される。これにより、画像形成装置１２Ｂが対応している認証方式のＩＤが特定される。そして、画像形成装置１２Ｂが対応している認証方式のＩＤと、認証方式要件セットに含まれる認証方式ＩＤ群（ログイン認証方式ＩＤと要求認証方式ＩＤ群）と、を対比することにより、認証対応方式セットと認証未対応方式セットとが作成される。

【００６１】

一例として、画像形成装置１２Ｂの端末ＩＤが「３」であるとする。図１０に示されて

いる認証端末テーブルを参照すると、送信対応データ形式ＩＤは「０」、「１」である。また、図７に示されている認証方式テーブルを参照すると、そのデータ形式ＩＤ１、２に対応する認証方式ＩＤは、認証方式１，２である。従って、画像形成装置１２Ｂは、ＩＤ・パスワード認証処理とＩＣカード認証処理とに対応していることになる。また、図６に示されているオブジェクト権限テーブルを参照すると、認証なし及び認証方式２，３が登録されている。また、ログイン認証方式のＩＤは、認証方式１（ＩＤ・パスワード認証処理）であるとする。この場合、認証方式要件セットには、ログイン認証方式に対応する認証方式１、及び、各オブジェクトの各操作に対応する認証方式２，３が含まれることになる。画像形成装置１２Ｂは、認証方式１，２に対応しているので、認証対応方式セットには認証方式１，２が含まれ、認証未対応方式セットには認証方式３が含まれることになる。

【００６２】

代替認証情報生成部２６は、上記の認証対応方式セットと認証未対応方式セットとに基づいて、画像形成装置１２Ｂに送信されるレスポンス情報を作成する（Ｓ０８）。

【００６３】

ここで、図１２を参照して、レスポンス作成処理について説明する。

【００６４】

認証未対応の方式数が０（ゼロ）の場合（Ｓ０９，未対応方式数＝０）、代替認証情報生成部２６は、認証対応方式セットに基づいてレスポンス情報を作成する（Ｓ１０）。そして、処理は、図１１に示されているステップＳ１９に移行する。詳しく説明すると、認証方式要件セットに含まれる認証方式ＩＤ群の中で、画像形成装置１２Ｂが対応していない認証方式ＩＤがない場合、つまり、認証未対応方式セットに認証方式ＩＤが含まれていない場合、認証未対応の方式数が０（ゼロ）であると判定される。この場合、画像形成装置１２Ｂは、ログインに要求されるログイン認証方式と全オブジェクトの全操作に要求される認証方式とを含む全ての認証方式に対応していることになる。ここで作成されたレスポンス情報には、認証対応方式セットの内容（例えば、各認証方式を示す各対応認証情報（例えば認証方式名称））が含まれる。つまり、当該レスポンス情報には、画像形成装置１２Ｂが対応している認証方式を示す情報が含まれる。

【００６５】

一方、認証未対応の方式数が０（ゼロ）ではない場合（Ｓ０９，未対応方式数＞０）、ステップＳ１１，Ｓ１２の処理が実行される。

【００６６】

ステップＳ１１では、代替認証情報生成部２６は、図１０に示されている認証端末テーブルから代替装置を検索する。つまり、代替認証情報生成部２６は、認証端末テーブルを参照することにより、画像形成装置１２Ｂが対応していない認証方式に対応している代替装置を特定する。例えば、画像形成装置１２Ｂが対応していない認証方式が、認証方式３「顔認証」である場合において、認証端末テーブルから、その「顔認証」に対応している代替装置が検索される。図７に示されている認証方式テーブルを参照すると、認証方式３に対応するデータ形式ＩＤは「２」であるため、認証端末テーブルにおいて、データ形式ＩＤ２に対応する端末ＩＤが特定される。例えば、認証端末テーブルを参照すると、端末ＩＤが「１」、「２」の装置が、代替装置として特定される。

【００６７】

ステップＳ１２では、代替認証情報生成部２６は、図９に示されている代替認証方式テーブルから代替認証方式を検索する。つまり、代替認証情報生成部２６は、代替認証方式テーブルを参照することにより、画像形成装置１２Ｂが対応していない認証方式に替わる代替認証方式を特定する。例えば、画像形成装置１２Ｂが対応していない認証方式が、認証方式３「顔認証」である場合において、代替認証方式テーブルから、その「顔認証」に対応している代替認証方式が検索される。図９に示されている代替認証方式テーブルを参照すると、認証方式３に替わる代替認証方式のＩＤは「１」であるため、携帯端末でのカメラ認証が代替認証方式として特定される。

【００６８】
なお、ステップＳ１１，Ｓ１２の処理の中の少なくとも１つの処理が実行されてもよい。つまり、ステップＳ１１の処理のみが実行されてもよいし、ステップＳ１２の処理のみが実行されてもよいし、ステップＳ１１，Ｓ１２の両方の処理が実行されてもよい。
【００６９】
そして、ステップＳ１１，Ｓ１２の検索結果に応じて、異なる処理が実行される。代替装置の数が０（ゼロ）ではないか、代替認証方式の数が０（ゼロ）ではない場合（Ｓ１３，代替装置数＞０、又は、代替認証方式数＞０）、処理はステップＳ１４に移行する。つまり、代替装置が存在するか、代替認証方式が存在する場合、処理はステップＳ１４に移行する。この場合、代替認証情報生成部２６は、代替認証リストを作成する（Ｓ１４）。代替装置が存在する場合、その代替認証リストには、代替装置に関する情報が含まれ、代替認証方式が存在する場合、その代替認証リストには、代替認証方式に関する情報が含まれる。また、代替装置及び代替認証方式が存在する場合、代替認証リストには、代替装置に関する情報と代替認証方式に関する情報が含まれる。例えば、代替装置に関する情報として、認証端末テーブルに含まれる情報が用いられる。具体的には、代替装置に関する情報として、例えば、その代替装置のＩＰアドレスや設置場所を示す情報等が用いられる。また、代替認証方式に関する情報として、代替認証方式テーブルに含まれる情報が用いられる。具体的には、代替認証方式に関する情報として、例えば、代替方式名称や、その代替認証方式の実行方法を説明するための情報、等が用いられる。
【００７０】
次に、代替認証情報生成部２６は、認証対応方式セット、認証未対応方式セット、及び、代替認証リストに基づいて、レスポンス情報を作成する（Ｓ１５）。そして、処理は、図１１に示されているステップＳ１９に移行する。ここで作成されたレスポンス情報には、認証対応方式セット、認証未対応方式セット、及び、代替認証リストの内容が含まれる。
【００７１】
一方、代替装置の数が０（ゼロ）であり、かつ、代替認証方式の数が０（ゼロ）の場合（Ｓ１３，代替装置数＝０、かつ、代替認証方式数＝０）、処理はステップＳ１６に移行する。つまり、代替装置及び代替認証方式のいずれも存在しない場合、処理はステップＳ１６に移行する。この場合、認証対応数に応じて異なる処理が実行される。認証対応数は、文書管理装置１０において要求される認証方式群の中で、画像形成装置１２Ｂが対応している認証方式の数である。つまり、認証対応数は、認証対応方式セットに含まれる認証方式ＩＤの数に相当する。認証対応数が０（ゼロ）ではない場合（Ｓ１６，認証対応数＞０）、つまり、認証対応方式セットに認証方式ＩＤが含まれている場合、処理はステップＳ１７に移行する。一方、認証対応数が０（ゼロ）である場合（Ｓ１６，認証対応数＝０）、つまり、認証対応方式セットに認証方式ＩＤが含まれていない場合、処理はステップＳ１８に移行する。
【００７２】
ステップＳ１７においては、代替認証情報生成部２６は、認証対応方式セットと認証未対応方式セットとに基づいて、レスポンス情報を作成する。そして、処理は、図１１に示されているステップＳ１９に移行する。ここで作成されたレスポンス情報には、認証対応方式セットと認証未対応方式セットの内容が含まれる。
【００７３】
ステップＳ１８においては、代替認証情報生成部２６は、エラーレスポンス情報を作成する。画像形成装置１２Ｂは、ログイン認証方式にも対応していないことになるため、画像形成装置１２Ｂから文書管理装置１０へのログインが不許可とされ、その旨の情報がエラーレスポンス情報に含まれる。そして、処理は、図１１に示されているステップＳ１９に移行する。
【００７４】
以下、図１１を参照して、ステップＳ１９以降の処理について説明する。上記のように

レスポンス情報又はエラーレスポンス情報が作成されると、その情報は、通信部１６によって、文書管理装置１０から画像形成装置１２Ｂに送信される（Ｓ１９）。

【００７５】

画像形成装置１２Ｂにおいては、文書管理装置１０から送信されたレスポンス情報又はエラーレスポンス情報が、通信部２８によって受信される（Ｓ２０）。

【００７６】

そして、画像形成装置１２Ｂにおいて、制御部３８が、レスポンス情報又はエラーレスポンス情報に従った処理を実行する。

【００７７】

画像形成装置１２Ｂがログイン認証方式に対応している場合、又は、画像形成装置１２Ｂはログイン認証方式に対応していないが、代替装置又は代替認証方式が存在する場合（Ｓ２１，Ｙｅｓ）、制御部３８は、ログイン用画面情報を作成し（Ｓ２２）、ログイン用画面をＵＩ部３４に表示させる（Ｓ２３）。

【００７８】

ログイン用画面には、画像形成装置１２Ｂが対応している認証方式を示す情報、未対応の認証方式を示す情報、代替装置に関する情報、代替認証方式に関する情報、等が表示される。

【００７９】

例えば、レスポンス情報に含まれる認証対応方式セットにログイン認証方式ＩＤが含まれている場合、画像形成装置１２Ｂはログイン認証方式に対応していることになる。この場合、そのログイン認証方式に関する情報がログイン用画面に表示される。例えば、ログイン操作するためのログインボタン等がログイン用画面に表示される。レスポンス情報に代替認証リストが含まれる場合において、その代替認証リストに、ログイン認証方式に対応する代替装置又は代替認証方式に関する情報が含まれる場合、代替装置又は代替認証方式が存在することになる。この場合、代替装置や代替認証方式に関する情報がログイン用画面に表示される。

【００８０】

一方、画像形成装置１２Ｂがログイン認証方式に対応していない場合、及び、代替装置と代替認証方式が存在しない場合（Ｓ２１，Ｎｏ）、制御部３８は、ログインエラー画面情報を作成し（Ｓ２３）、ログインエラー画面をＵＩ部３４に表示させる（Ｓ２４）。エラーレスポンス情報が受信された場合、画像形成装置１２Ｂが対応している認証方式が存在しないので、画像形成装置１２Ｂがログイン認証方式に対応していないことになる。また、レスポンス情報に含まれる認証対応方式セット及び代替認証リストに、ログイン認証方式ＩＤ、代替装置に関する情報、及び、代替認証方式に関する情報が含まれていない場合、画像形成装置１２Ｂがログイン認証方式に対応していないとともに、代替装置及び代替認証方式が存在しないことになる。この場合、ログイン操作が実行されないことになる。

【００８１】

画像形成装置１２ＢのＵＩ部３４に表示されている画面がユーザによって確認され（Ｓ２５）、以降の操作が行われる。ログインエラー画面が表示されている場合、ログインが禁止され、以降の操作が禁止される。ログイン用画面が表示されている場合、ユーザは、そのログイン用画面に従って操作することが想定される。

【００８２】

画像形成装置１２Ｂがログイン認証方式に対応している場合、ログイン用画面に表示されている情報に従って、ユーザが画像形成装置１２ＢのＵＩ部３４を利用してログイン操作を行うことになる（Ｓ２６）。例えば、ログインに要求される認証方式がＩＤ・パスワード認証であり、画像形成装置１２Ｂがその認証方式に対応している場合、ユーザが画像形成装置１２ＢのＵＩ部３４を操作することにより、ＩＤとパスワードが入力されることになる。ここで入力された認証情報（ＩＤとパスワード）が、画像形成装置１２Ｂから文書管理装置１０に送信され、文書管理装置１０の認証部１８によって認証処理が行われる

。認証が成功した場合、画像形成装置１２Ｂから文書管理装置１０へのログインが許可され、認証が失敗した場合、画像形成装置１２Ｂから文書管理装置１０へのログインが禁止される。

【００８３】

また、画像形成装置１２Ｂがログイン認証方式に対応していない場合において、代替装置が存在する場合、その代替装置を利用してログイン操作が行われることになる（Ｓ２７）。例えば、ログイン用画面には代替装置に関する情報が表示される。その情報を参考にして、ユーザが代替装置に移動し、その代替装置にてログイン操作を行うことが想定される。例えば、ログインに要求される認証方式が顔認証であり、画像形成装置１２Ｂがその認証方式に対応していない場合、代替装置に関する情報がログイン用画面に表示される。画像形成装置１２Ａが顔認証方式に対応している場合、画像形成装置１２Ａに関する情報が、画像形成装置１２ＢのＵＩ部３４（ログイン用画面）に表示される。この場合、ユーザは画像形成装置１２Ａに移動し、その画像形成装置１２Ａを用いてログイン操作を行うことになる。

【００８４】

また、画像形成装置１２Ｂがログイン認証方式に対応していない場合において、代替認証方式が存在する場合、その代替認証方式を利用してログイン操作が行われることになる（Ｓ２８）。例えば、ログイン用画面には代替認証方式に関する情報が表示される。例えば、ログインに要求される認証方式が顔認証であり、画像形成装置１２Ｂがその認証方式に対応していない場合、代替認証方式に関する情報が、画像形成装置１２ＢのＵＩ部３４（ログイン用画面）に表示される。この場合、ユーザはその代替認証方式に応じた操作を行うことにより、ログイン操作を実行する。

【００８５】

以上のように、画像形成装置１２Ｂがログイン認証方式に対応している場合、画像形成装置１２Ｂにおいてログイン操作が行われることになる。一方、画像形成装置１２Ｂがログイン認証方式に対応しておらず、代替装置や代替認証方式が存在する場合には、その代替装置や代替認証方式に関する情報が、画像形成装置１２Ｂに表示されることになる。これにより、要求されている認証方式に対応する代替装置や代替認証方式に関する情報がユーザに提供されることになる。それ故、ユーザによって使用されている画像形成装置１２Ｂが、ログイン認証方式に対応していない場合であっても、代替装置や代替認証方式を利用することにより、ログイン操作が実現されることになる。

【００８６】

次に、図１３を参照して、代替認証方式に従った認証処理について説明する。例えば、撮像部３６を備えていない画像形成装置１２Ｂが用いられ、対象操作（例えばログインや文書データの操作）に要求される認証方式が顔認証であるとする。図９に示されている代替認証方式テーブルによると、顔認証の代替認証方式として、携帯端末でのカメラ認証が用意されている。ここでは、携帯端末１４を利用して代替認証方式に従った認証処理が実行される。

【００８７】

カメラ認証を実行する前提として、文書管理装置１０に、携帯端末１４の端末ＩＤとユーザの顔を表す顔画像データとを事前に登録しておく。例えば、携帯端末１４の撮像部４２や別の撮像装置によって得られた顔画像データと携帯端末１４の端末ＩＤが、携帯端末１４等の装置から文書管理装置１０に送信され、それらが対応付けられて文書管理装置１０の記憶部２２に格納される。これにより、事前登録が完了する。

【００８８】

代替認証処理を実行する場合、ユーザは、登録済みの携帯端末１４の撮像部４２によって自身の顔を撮影する（Ｓ３０）。これにより、顔画像データが生成される。次に、携帯端末１４の端末ＩＤと顔画像データとを含む認証情報が、携帯端末１４から文書管理装置１０に送信される（Ｓ３１）。

【００８９】

文書管理装置１０においては、携帯端末１４から送信された認証情報が受信される（Ｓ３２）。次に、文書管理装置１０の認証部１８によって認証処理が実行される（Ｓ３３）。その認証処理においては、その認証情報に含まれる端末ＩＤ及び顔画像データと、文書管理装置１０の記憶部２２に格納されている事前登録情報（端末ＩＤ及び顔画像データ）と、が対比される。認証情報に適合する事前登録情報が記憶部２２に格納されている場合（例えば、認証情報に一致する事前登録情報が記憶部２２に格納されている場合）、認証部１８は、ワンタイムＩＤとワンタイムパスワードとを含む一時認証情報を作成する（Ｓ３４）。この一時認証情報は、認証部１８において一時的に保存される。一時認証情報は、文書管理装置１０から携帯端末１４に送信される（Ｓ３５）。一方、認証情報に適合する事前登録情報が記憶部２２に格納されていない場合、一時認証情報は作成されない。

【００９０】

文書管理装置１０から送信された一時認証情報は携帯端末１４によって受信され（Ｓ３６）、携帯端末１４のＵＩ部４４に表示される。ユーザは、画像形成装置１２ＢのＵＩ部３４を利用して、ワンタイムＩＤとワンタイムパスワードを入力する。画像形成装置１２Ｂは、ワンタイムＩＤとワンタイムパスワードを受け付けると（Ｓ３７）、それらを文書管理装置１０に送信する（Ｓ３８）。

【００９１】

文書管理装置１０の認証部１８は、保存されている一時認証情報と携帯端末１４から送信された一時認証情報とを用いて認証処理を行う（Ｓ３９）。両一時認証情報が適合して認証が成功した場合（例えば両一時認証情報が一致した場合）、文書管理装置１０にてレスポンス情報が作成され、そのレスポンス情報が画像形成装置１２Ｂに送信される（Ｓ４０）。文書管理装置１０から送信されたレスポンス情報は画像形成装置１２Ｂによって受信される（Ｓ４１）。これにより、対象操作（例えばログインや文書データの操作）が許可される。一方、両一時認証情報が適合せずに認証が失敗した場合（例えば両一時認証情報が一致しない場合）、対象操作が禁止される。

【００９２】

上記の処理によると、画像形成装置１２Ｂが顔認証方式に対応していない場合であっても、それに替わる認証方式によって認証処理が行われる。

【００９３】

また、ステップＳ３１において送信される認証情報には、顔画像データの撮影日時を示す撮影日時情報が含まれていてもよい。この場合、文書管理装置１０の認証部１８は、その顔画像データを含む認証情報を受け付けた受付日時と、その認証情報に含まれる撮影日時情報が示す撮影日時と、を比較する。そして、携帯端末１４から送信された認証情報に含まれる端末ＩＤと顔画像データが文書管理装置１０に登録されており、かつ、受付日時を基準として撮影日時が予め設定された時間以内（例えば５分以内）に含まれる場合、ワンタイムＩＤとワンタイムパスワードが作成されて携帯端末１４に送信される。一方、受付日時を基準として撮影日時が予め設定された時間以内に含まれていない場合、ワンタイムＩＤとワンタイムパスワードは作成されない。このように、撮影日時をも考慮して認証を行うことにより、文書管理装置１０のセキュリティが向上し得る。

【００９４】

別の例として、ステップＳ３３における認証処理において、携帯端末１４の位置情報が利用されてもよい。この場合、携帯端末１４から送信される認証情報には、携帯端末１４の位置情報が含まれる。例えば、ＧＰＳ（Global Positioning System）機能を備えた携帯端末１４が用いられ、そのＧＰＳ機能によって携帯端末１４の位置情報が取得される。文書管理装置１０の認証部１８は、認証端末テーブルから画像形成装置１２Ｂの位置情報を取得し、画像形成装置１２Ｂの位置情報と認証情報に含まれる携帯端末１４の位置情報とを比較する。認証情報に含まれる端末ＩＤと顔画像データが文書管理装置１０に登録されており、かつ、画像形成装置１２Ｂと携帯端末１４との位置関係が予め設定された基準を満たす場合、ワンタイムＩＤとワンタイムパスワードが作成されて携帯端末１４に送信される。例えば、画像形成装置１２Ｂと携帯端末１４との距離が閾値（例えば数ｍ）以内

の場合、ワンタイムＩＤとワンタイムパスワードが作成されて携帯端末１４に送信される。一方、位置関係が基準を満たさない場合（例えば距離が閾値を超える場合）、ワンタイムＩＤとワンタイムパスワードは作成されない。このように、携帯端末１４の位置をも考慮して認証を行うことにより、文書管理装置１０のセキュリティが向上し得る。つまり、画像形成装置１２Ｂに近い位置にある携帯端末１４のユーザほど、画像形成装置１２Ｂの真のユーザであると想定される。それ故、携帯端末１４の位置を考慮することにより、真のユーザによる利用が許可され、文書管理装置１０のセキュリティが向上し得る。なお、撮影日時情報と位置情報とを組み合わせて認証処理を行ってもよい。

【００９５】

次に、ログイン後の操作について説明する。文書管理装置１０へのログイン後においても、オブジェクト（文書データやフォルダ）によっては、操作のために認証が要求される場合がある。例えば、図６に示されているように、「フォルダ－１」に対する操作には認証方式３に従った認証が要求される。図１４には、その認証（追加認証）のための処理の一例が示されている。以下、図１４を参照してその追加認証について説明する。一例として、撮像部３６を備えていない画像形成装置１２Ｂが用いられるものとする。

【００９６】

まず、画像形成装置１２Ｂにおいて、ユーザがＵＩ部３４を利用することにより、特定の操作を実行する（Ｓ５０）。例えば、文書管理装置１０に格納されている文書データやフォルダに対する操作（例えばアクセス）が行われる。ユーザによって操作が実行されると、画像形成装置１２Ｂの通信部２８によって、その操作内容を示す操作要求情報が文書管理装置１０に送信される（Ｓ５１）。

【００９７】

文書管理装置１０においては、画像形成装置１２Ｂから送信された操作要求情報が、通信部１６によって受信される（Ｓ５２）。

【００９８】

次に、文書管理装置１０の認証部１８が、その操作要求情報を参照し、現時点における画像形成装置１２Ｂの認証状態が、その操作に要求される認証条件を満たすか否かを確認する（Ｓ５３）。図６に示されているオブジェクト権限テーブルには、各オブジェクトの操作毎に要求される認証方式が示されているため、そのオブジェクト権限テーブルを参照することにより、その操作に要求される認証方式が特定される。また、現時点における画像形成装置１２Ｂの認証状態が特定される。

【００９９】

現時点における認証状態が、操作に要求される認証条件を満たす場合（Ｓ５４，Ｙｅｓ）、その操作が許可される。この場合、制御部２４によってレスポンス情報が作成され、そのレスポンス情報が通信部１６によって画像形成装置１２Ｂに送信される（Ｓ５５）。そのレスポンス情報は画像形成装置１２Ｂによって受信され（Ｓ５６）、画像形成装置１２Ｂからの操作が許可される。例えば、特定の文書データやフォルダへのアクセスや更新等が許可される。

【０１００】

例えば、画像形成装置１２Ｂを利用して、ＩＤ・パスワード認証によって文書管理装置１０にログインしているものとする。つまり、現時点における認証状態は、ＩＤ・パスワードによる認証状態ということになる。また、操作に要求される認証方式が存在しないものとする。つまり、その操作には認証が要求されていないものとする。例えば、オブジェクト権限テーブルによると、「文書－２」に対する操作には対応する認証方式が存在しておらず、「文書－２」に対する操作には認証は要求されていない。ユーザによって実行される操作が、「文書－２」に対する操作である場合、現時点における認証状態は、操作に要求される認証条件を満たしていることになり、画像形成装置１２Ｂにおいて「文書－２」に対する操作が許可される。

【０１０１】

一方、現時点における認証状態が、操作に要求される認証条件を満たさない場合（Ｓ５

４，Ｎｏ）、追加認証処理が実行される。この場合、制御部２４によって追加認証要求情報が作成され、その追加認証要求情報が通信部１６によって画像形成装置１２Ｂに送信される（Ｓ５６）。その追加認証要求情報は画像形成装置１２Ｂによって受信され（Ｓ５７）、画像形成装置１２Ｂと文書管理装置１０との間で追加の認証ネゴシエーション処理が実行される（Ｓ５８）。つまり、図１１及び図１２を参照して説明した認証ネゴシエーション処理が実行される。これにより、文書管理装置１０において、画像形成装置１２Ｂが操作に要求される認証方式に対応しているか否かに応じて、認証対応方式セットと認証未対応方式セットが作成される。また、その認証方式に対応している代替装置が存在している場合や、その認証方式に替わる代替認証方式が存在している場合、代替装置や代替認証方式に関する情報を含む代替認証リストが作成される。そして、文書管理装置１０において、認証対応方式セット、認証未対応方式セット及び代替認証リストに基づいて、レスポンス情報が作成され、そのレスポンス情報が画像形成装置１２Ｂに送信される。画像形成装置１２Ｂにおいては、そのレスポンス情報に従って追加認証要求画面の情報が作成され、その追加認証要求画面が画像形成装置１２Ｂに表示される。

【０１０２】

例えば、画像形成装置１２Ｂを利用して、ＩＤ・パスワード認証によって文書管理装置１０にログインしているものとする。また、操作に要求される認証方式が顔認証であるとする。例えば、オブジェクト権限テーブルによると、「フォルダー１」に対する操作には認証方式３が対応付けられており、その操作には顔認証が要求されている。ユーザによって実行される操作が、「フォルダー１」に対する操作である場合、現時点における認証状態は、操作に要求される認証条件を満たしていないことになる。この場合、ステップＳ５８における認証ネゴシエーション処理が実行され、追加認証要求画面が画像形成装置１２Ｂに表示される。

【０１０３】

画像形成装置１２Ｂが、対象操作に要求される認証方式に対応していない場合、追加認証要求画面には、操作に要求される認証方式を示す情報、代替装置を示す情報、代替認証方式を示す情報、等が表示される。画像形成装置１２Ｂが、対象操作に要求される認証方式に対応している場合、追加認証要求画面には、その認証方式に従った認証処理を実行するための情報（例えば認証実行ボタン等）が表示される。

【０１０４】

ステップＳ５９では、上記の追加認証要求画面に従った処理が行われる（Ｓ５９）。画像形成装置１２Ｂが、操作に要求される認証方式に対応している場合、その認証方式に従った追加認証が実行される。認証が成功すると、その操作が許可される。また、代替装置が存在する場合、その代替装置によって追加認証が実行され、認証が成功すると、その操作が許可される。また、代替認証方式が存在する場合、その代替認証方式に従った認証処理が実行され、その認証が成功すると、その操作が許可される。一方、画像形成装置１２Ｂが、操作に要求される認証方式に対応しておらず、かつ、代替装置及び代替認証方式が存在しない場合、エラー処理となる。この場合、その操作が禁止される。

【０１０５】

以上のように、画像形成装置１２Ｂが対象操作に要求される認証方式に対応している場合、画像形成装置１２Ｂにおいてその認証方式に従った認証処理が行われることになる。一方、画像形成装置１２Ｂがその認証方式に対応していない場合において、その認証方式に対応している代替装置や代替認証方式が存在する場合には、その代替装置や代替認証方式に関する情報が、画像形成装置１２Ｂに表示されることになる。これにより、対象操作に要求される認証方式に対応している代替装置や代替認証方式に関する情報がユーザに提供されることになる。それ故、ユーザによって使用されている画像形成装置１２Ｂが、要求されている認証方式に対応していない場合であっても、代替装置や代替認証方式を利用することにより、対象操作が実行されることになる。

【０１０６】

また、追加認証処理が実行される場合、つまり、現時点における認証状態が、操作に要

求される認証条件を満たしていない場合、文書管理装置１０の制御部２４は、その時点において画像形成装置１２Ｂに表示されている最後の画面の情報（例えばＵＲＬ等）を、認証情報（例えばユーザＩＤ等）と関連付けて記憶部２２に記憶させておいてもよい。そして、代替装置（例えば画像形成装置１２Ａ）を用いた認証処理が成功した場合、制御部２４は、記憶部２２に記憶されている最後の画面の情報を代替装置（例えば画像形成装置１２Ａ）に送信する。この場合、代替装置としての画像形成装置１２ＡのＵＩ部３４には、その画面の情報に従って、上記の最後の画面が表示される。これにより、画像形成装置１２Ａにおいて、その最後の画面から操作が再開されることになり、ユーザの利便性が向上する。つまり、画像形成装置１２Ａにおいて、文書管理装置１０へのログイン操作から操作を開始せずに済む。なお、代替装置を用いた認証が成功した場合、その代替装置には、ユーザの選択に従って、初期画面又は最後の画面のいずれかが表示されるようにしてもよい。

【０１０７】

次に、上記の処理によって画像形成装置１２Ｂに表示される画面について説明する。

【０１０８】

図１５には、初期画面の一例が示されている。初期画面４８は、ログイン時に画像形成装置１２ＢのＵＩ部３４に表示される画面である。初期画面４８には、通信経路Ｎに接続されている文書管理装置１０の一覧が表示されている。例えば、２つの文書管理装置１０（装置Ａ，Ｂ）が通信経路Ｎに接続されている場合、それらの一覧が表示される。この一覧からユーザによって選択された文書管理装置１０に対してアクセスが実行される。例えば装置Ａが選択された場合、画像形成装置１２Ｂは、装置Ａ（文書管理装置１０）に対して、利用リクエスト情報を送信する。そして、図１１及び図１２を参照して説明した処理（認証ネゴシエーション処理）が実行され、ログイン用画面が画像形成装置１２ＢのＵＩ部３４に表示される。

【０１０９】

図１６には、ログイン用画面の一例が示されている。ログイン用画面５０は、図１１中のステップＳ２４において、画像形成装置１２ＢのＵＩ部３４に表示される画面である。このログイン用画面５０には、「対応認証」、「未対応認証」、「代替認証装置一覧」及び「代替認証方式一覧」が表示されている。

【０１１０】

「対応認証」は、文書管理装置１０に設定されている認証方式群の中で画像形成装置１２Ｂが対応している認証方式であり、認証対応方式セットに含まれる認証方式である。レスポンス情報に認証対応方式セットが含まれている場合、その認証対応方式セットに含まれる認証方式の一覧がログイン用画面５０に表示される。例えば、画像形成装置１２Ｂが「ＩＤ・パスワード認証」と「ＩＣカード認証」に対応している場合、「ＩＤ・パスワード認証」を示す情報と「ＩＣカード」を示す情報が、ログイン用画面５０に表示される。また、図１６に示す例では、「ＩＤ・パスワード認証」と「ＩＣカード認証」が、ログインに要求されるログイン認証方式である。この例では、画像形成装置１２Ｂは、ログイン認証方式に対応していることになる。この場合、図１１中のステップＳ２６の処理が実行され、画像形成装置１２Ｂから文書管理装置１０にログインすることが想定される。

【０１１１】

「未対応認証」は、文書管理装置１０に設定されている認証方式群の中で画像形成装置１２Ｂが対応していない認証方式であり、認証未対応方式セットに含まれる認証方式である。レスポンス情報に認証未対応方式セットが含まれている場合、その認証未対応方式セットに含まれる認証方式の一覧がログイン用画面５０に表示される。例えば、画像形成装置１２Ｂが「顔認証」に対応していない場合、「顔認証」を示す情報がログイン用画面５０に表示される。

【０１１２】

「代替認証装置一覧」は、画像形成装置１２Ｂが対応していない認証方式に対応している代替装置の一覧であり、代替認証リストに含まれる代替装置に関する情報の一覧である

。レスポンス情報に代替認証リストが含まれている場合、その代替認証リストに含まれる代替装置に関する情報がログイン用画面５０に表示される。例えば、画像形成装置１２Ｂが「顔認証」に対応していない場合、その「顔認証」に対応している代替装置に関する情報がログイン用画面５０に表示される。一例として、代替装置のＩＰアドレスや設置場所に関する情報が表示される。

【０１１３】

画像形成装置１２Ｂと代替装置との位置関係に応じて、代替装置の表示順が変更されてもよい。例えば、代替認証情報生成部２６は、図１０に示されている認証端末テーブルにて管理されている位置情報を用いることにより、リクエスト装置としての画像形成装置１２Ｂと代替装置との位置関係を特定し、画像形成装置１２Ｂとの距離が近い代替装置ほど高い表示順位を付与する。ログイン用画面５０には、画像形成装置１２Ｂとの距離が近い代替装置に関する情報ほど上位に表示される。これにより、画像形成装置１２Ｂとの距離が近い代替装置ほど、ユーザにとって見やすい位置に表示される。

【０１１４】

別の例として、代替装置が画像形成装置１２Ｂと同一のサブネットに含まれるか否かに応じて、代替装置の表示順が変更されてもよい。例えば、代替認証情報生成部２６は、図１０に示されている認証端末テーブルにて管理されているＩＰアドレスを用いることにより、画像形成装置１２Ｂと同一サブネットに含まれる代替装置に高い表示順位を付与する。ログイン用画面５０には、画像形成装置１２Ｂと同一サブネットに含まれる代替装置が上位に表示される。これにより、画像形成装置１２Ｂと同一サブネットに含まれる代替装置ほど、ユーザにとって見やすい位置に表示される。

【０１１５】

更に別の例として、最終ネゴシエーション日時を基準にして代替装置の表示順が変更されてもよい。例えば、代替認証情報生成部２６は、図１０に示されている認証端末テーブルにて管理されている最終ネゴシエーション日時を参照することにより、最終ネゴシエーション日時が新しい代替装置ほど高い表示順位を付与する。ログイン用画面５０には、最終ネゴシエーション日時が新しい代替装置ほど上位に表示される。これにより、稼働していない、又は、破棄されたと疑われる代替装置が下位に表示されることになる。

【０１１６】

「代替認証方式一覧」は、画像形成装置１２Ｂが対応していない認証方式に替わる代替認証方式の一覧であり、代替認証リストに含まれる代替認証方式に関する情報の一覧である。レスポンス情報に代替認証リストが含まれている場合、その代替認証リストに含まれる代替認証方式に関する情報がログイン用画面５０に表示される。例えば、画像形成装置１２Ｂが「顔認証」に対応していない場合、その「顔認証」に替わる代替認証方式に関する情報がログイン用画面５０に表示される。一例として、「携帯端末でのカメラ認証」を示す情報が代替認証方式に関する情報として表示される。また、説明ページへのリンクボンタンが設定されてもよい。この説明ページは、代替認証方式の利用方法が記述されたページである。このリンクボタンには、例えばＵＲＬ等のリンク情報が対応付けられている。そのリンクボタンが押下されると、画像形成装置１２Ｂがリンク先にアクセスし、画像形成装置１２ＢのＵＩ部３４に説明ページが表示される。

【０１１７】

また、ログイン用画面５０には、画像形成装置１２Ｂ（デバイス）が一部の文書にて要求される認証方式に対応していない旨が表示されている。これは、認証未対応の方式数が０（ゼロ）ではない（未対応方式数＞０）ということを意味している。一方で、上記のように「対応認証」が表示されているため、文書管理装置１０に設定されている認証方式群の中で、画像形成装置１２Ｂが対応している認証方式が存在していることになる。また、代替装置及び代替認証方式が存在していることになる。これらの情報が表示されることにより、画像形成装置１２Ｂが対応している認証方式では利用（操作）が許可されない文書データやフォルダが文書管理装置１０に存在していることが、ユーザによって把握されることになる。また、それらの文書データやフォルダを利用（操作）するために必要な認証

方式、その認証方式に対応している代替装置、及び、代替認証方式が、ユーザに提供されることになる。

【０１１８】

次に、ログイン後の画面について説明する。図１７には、フォルダＡ内の内容を示す画面５２が示されている。一例として、ＩＤとパスワードを用いた認証処理（ログイン処理）によって、撮像部３６を備えていない画像形成装置１２Ｂから文書管理装置１０にログインしているものとする。そして、ログイン後において、文書管理装置１０に格納されているフォルダ群の中からフォルダＡが選択されたものとする。そのフォルダＡには、例えば、設計書フォルダ、人事フォルダ、仕様書フォルダ、文書Ａ及び文書Ｂが格納されている。

【０１１９】

ここで、ユーザによって人事フォルダが指定されたものとする。また、この人事フォルダに対する操作には、認証方式３による顔認証が必要であるとする。

【０１２０】

図１８には、追加認証要求画面の一例が示されている。追加認証要求画面５４は、上記の人事フォルダの指定に応じて画像形成装置１２ＢのＵＩ部３４に表示される画面であり、図１４中のステップＳ５８において作成されて表示される画面である。つまり、追加認証要求画面５４は、追加の認証ネゴシエーション処理の実行結果として表示される画面である。

【０１２１】

一例として、画像形成装置１２Ｂは顔認証に対応していないものとする。この場合、追加認証要求画面５４には、実行された操作が必要な認証に対応していない旨、実行された操作の内容を示す情報（例えば「人事フォルダの内容表示」）、及び、その操作に必要な認証を示す情報（例えば「顔認証」）が表示される。また、顔認証に対応している代替装置が存在する場合には「代替認証装置一覧」が表示され、顔認証に替わる代替認証方式が存在する場合には「代替認証方式一覧」が表示される。このように、人事フォルダを利用（操作）するために必要な認証方式、その認証方式に対応している代替装置、及び、代替認証方式が、ユーザに提供される。

【０１２２】

代替認証装置一覧においては、図１６を参照して説明したように、画像形成装置１２Ｂと代替装置との位置関係に応じて、代替装置の表示順が変更されてもよい。別の例として、代替装置が画像形成装置１２Ｂと同一サブネットに含まれるか否かに応じて、代替装置の表示順が変更されてもよいし、最終ネゴシエーション日時を基準にして代替装置の表示順が変更されてもよい。

【０１２３】

例えば、代替装置を利用して顔認証が実行され、その認証が成功すると、人事フォルダの内容が画像形成装置１２ＢのＵＩ部３４に表示される。また、代替認証方式に従った認証処理が実行され、その認証が成功すると、人事フォルダの内容が表示される。

【０１２４】

画像形成装置１２Ｂが、人事フォルダに対する操作に要求される認証方式に対応している場合、その認証方式に従った認証処理を実行するための情報が、追加認証要求画面５４に表示される。例えば、顔認証が要求される場合には、その顔認証の実行を促す内容の情報が表示される。そして、画像形成装置１２Ｂを用いて顔認証が実行され、その認証が成功すると、人事フォルダの内容が画像形成装置１２ＢのＵＩ部３４に表示される。

【０１２５】

また、追加認証処理が実行される場合、図１７に示されている画面５２の情報（例えばＵＲＬ）が、文書管理装置１０の記憶部２２に記憶されてもよい。この場合、代替装置を用いた認証処理が成功すると、その代替装置のＵＩ部３４に画面５２が表示される。これにより、文書管理装置１０へのログイン操作が省かれ、ユーザの手間が軽減される。

【０１２６】

上記の本実施形態では、生体認証として顔認証を例に挙げて説明したが、他の生体認証が用いられてもよい。例えば、音声認証処理、指紋認証処理、静脈認証処理等が利用されてもよい。例えば、これらの処理に用いられるデータを取得する機能を備えた画像形成装置が代替装置として利用されてもよいし、その機能を備えた携帯端末を利用した代替認証方式が適用されてもよい。

【０１２７】

なお、上記の実施形態では、画像形成装置が認証の対象となる端末装置として説明したが、画像形成装置以外の装置が認証の対象となってもよい。

【０１２８】

また、認証部１８は、文書管理装置１０以外の装置、例えば認証サーバ等に設けられていてもよい。この場合、認証処理は認証サーバ等の装置によって実行され、認証結果が認証サーバ等の装置から文書管理装置１０に送信されることになる。文書管理装置１０は、その認証結果に応じた処理を実行する。

【０１２９】

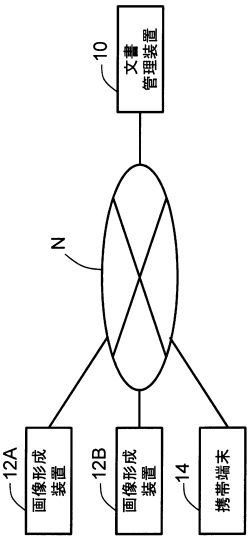
上記の文書管理装置１０、画像形成装置１２Ａ，１２Ｂ及び携帯端末１４は、一例としてハードウェア資源とソフトウェアとの協働により実現される。具体的には、これらの装置は、図示しないＣＰＵ等のプロセッサを備えている。当該プロセッサが、図示しない記憶装置に記憶されたプログラムを読み出して実行することにより、これらの装置の各部の機能が実現される。上記プログラムは、ＣＤやＤＶＤ等の記録媒体を経由して、又は、ネットワーク等の通信経路を経由して、記憶装置に記憶される。または、これらの装置の各部は、例えばプロセッサや電子回路等のハードウェア資源により実現されてもよい。その実現においてメモリ等のデバイスが利用されてもよい。別の例として、各部は、ＤＳＰ（Digital Signal Processor）やＦＰＧＡ（Field Programmable Gate Array）等によって実現されてもよい。

【符号の説明】

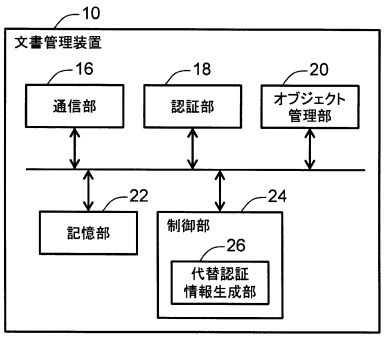
【０１３０】

１０　文書管理装置、１２Ａ，１２Ｂ　画像形成装置、１４　携帯端末、１８　認証部、２０　オブジェクト管理部、２６　代替認証情報生成部。

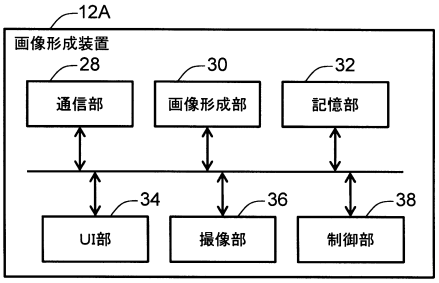
【図１】



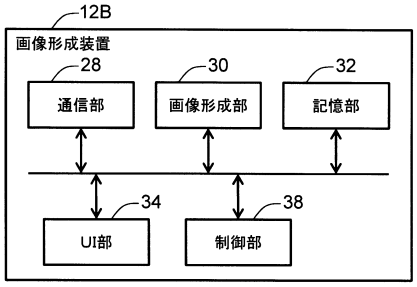
【図２】



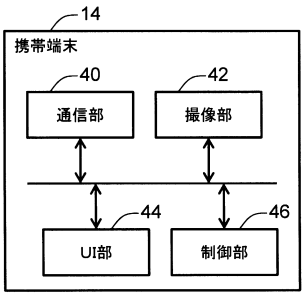
【図３】



【図４】



【図５】



【図６】

<オブジェクト権限テーブル>

オブジェクトID	対象操作	要求認証方式ID
文書－１	更新以外の操作	なし
文書－２	更新操作	認証方式３
文書－３	全操作	なし
フォルダ－１	全操作	認証方式３
フォルダ－２	全操作	認証方式２

【図７】

<認証方式テーブル>

認証方式ID	認証方式名称	データ形式ID
認証方式1	ID・パスワード認証	0
認証方式2	ICカード認証	1
認証方式3	顔認証	2
認証方式4	指紋認証	4

【図８】

<データ形式テーブル>

データ形式ID	データ形式名称
0	文字列
1	ICデータ
2	写真画像
3	音声
4	指紋

【図９】

<代替認証方式テーブル>

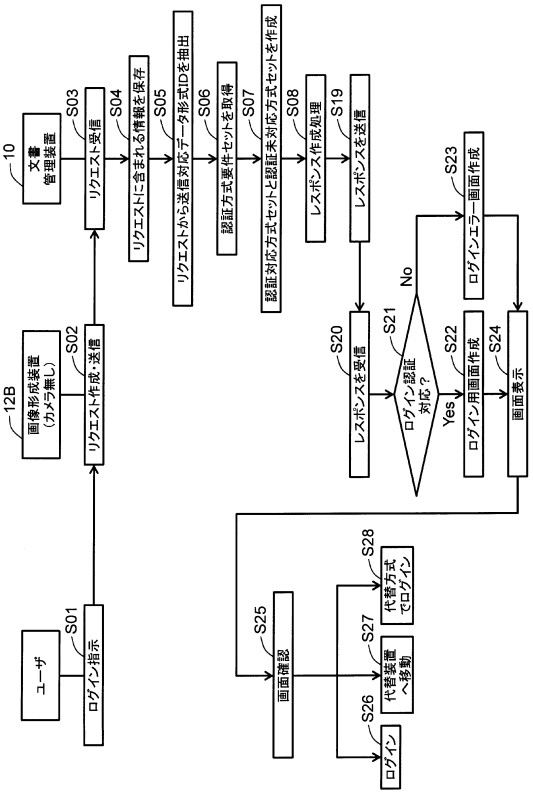
代替方式ID	代替方式名称	認証方式ID
代替方式1	携帯端末でのカメラ認証	認証方式3

【図１０】

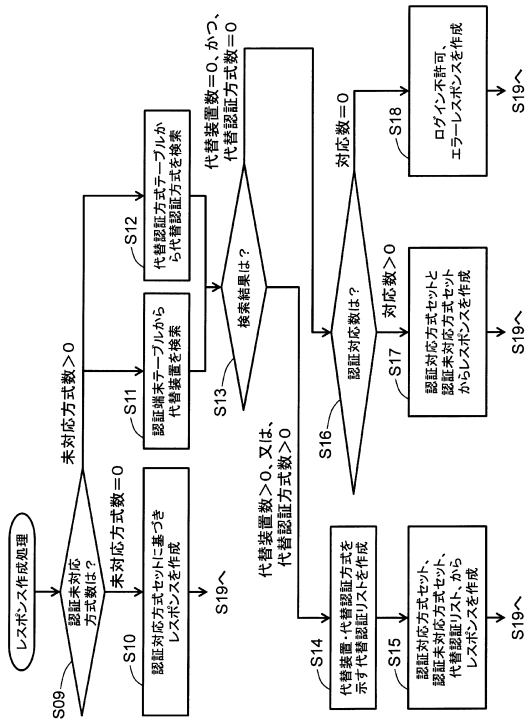
<認証端末テーブル>

端末ID	最終ネゴシエーション日時	IPアドレス	位置情報	設置場所の説明	送信対応データ形式ID
1	2015-01-01T10:10:10	123.456.111.222	XXX, YYY	10階南側	0,2
2	2015-01-02T11:10:10	123.456.111.333	AAA, BBB	11階北側	0,1,2
3	2015-01-03T12:10:10	123.456.111.444	CCC, DDD	12階中央	0,1

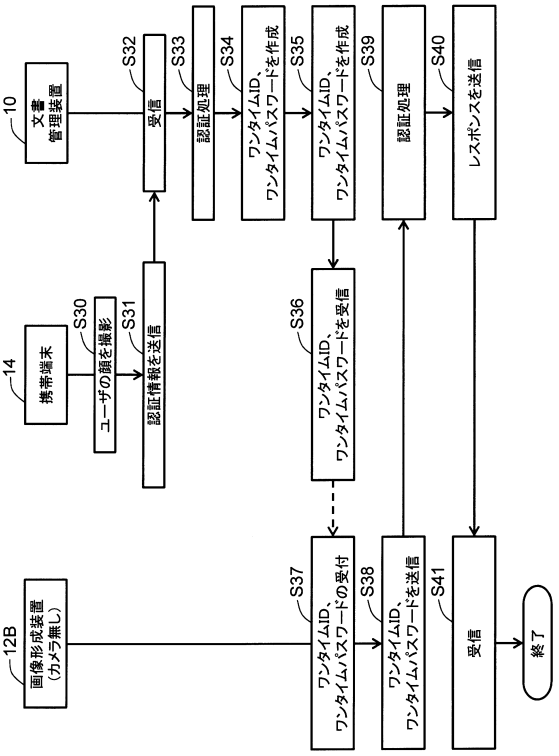
【図１１】



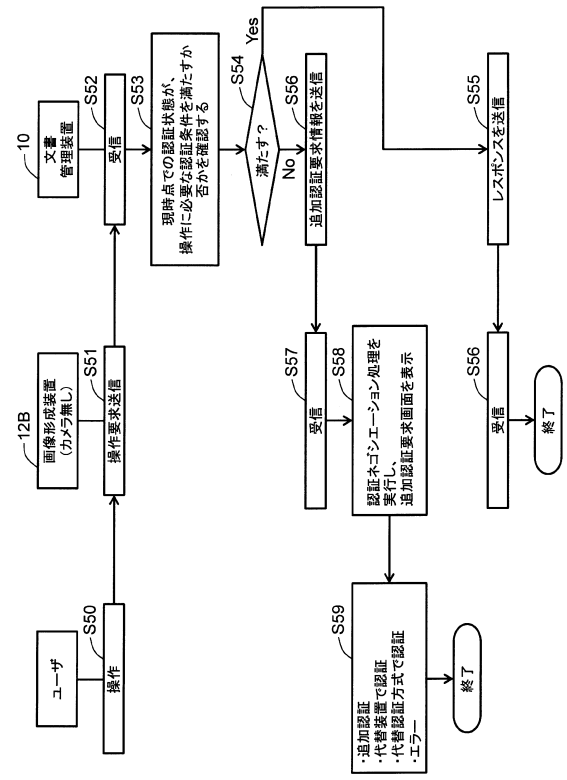
【図１２】



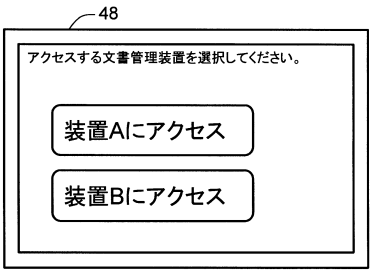
【図１３】



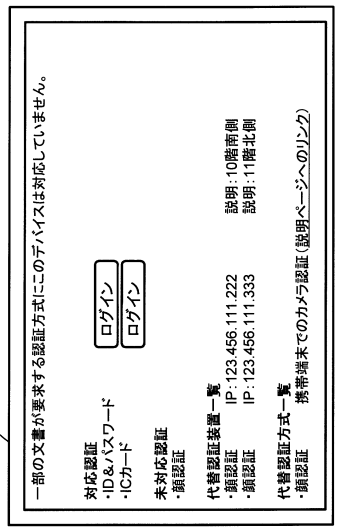
【図１４】



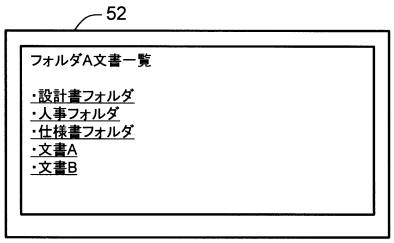
【図１５】



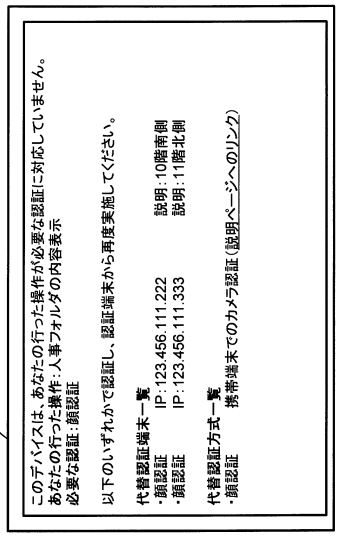
【図１６】


50
一部の文書が要求する認証方式にこのデバイスは対応していません。
対応認証
・ID＆パスワード
・ICカード
ログイン
ログイン
未対応認証
・顔認証
代替認証装置一覧
・顔認証 IP:123.456.111.222 説明:10階南側
・顔認証 IP:123.456.111.333 説明:11階北側
代替認証方式一覧
・顔認証 携帯端末でのカメラ認証（説明ページへのリンク）

【図１７】


52
フォルダA文書一覧
・設計書フォルダ
・人事フォルダ
・仕様書フォルダ
・文書A
・文書B

【図１８】


54
このデバイスは、あなたの行った操作が必要な認証に対応していません。
あなたの行った操作：人事フォルダの内容表示
必要な認証：顔認証
以下のいずれかで認証し、認証端末から再度実施してください。
代替認証端末一覧
・顔認証 IP:123.456.111.222 説明:10階南側
・顔認証 IP:123.456.111.333 説明:11階北側
代替認証方式一覧
・顔認証 携帯端末でのカメラ認証（説明ページへのリンク）

フロントページの続き

(56)参考文献 特開２００９－２１１５６６（ＪＰ，Ａ）
特開２００６－１９５８１１（ＪＰ，Ａ）
特開２０１０－０２０７１２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／６２