

(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2016-224849

(P2016-224849A)

(43) 公開日 平成28年12月28日(2016.12.28)

(51) Int.Cl. F I テーマコード (参考)
G06F 21/31 (2013.01) G O 6 F 21/31
G06F 21/62 (2013.01) G O 6 F 21/62

審査請求 未請求 請求項の数 5 O L (全 24 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)

(71) 出願人 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Y K I 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

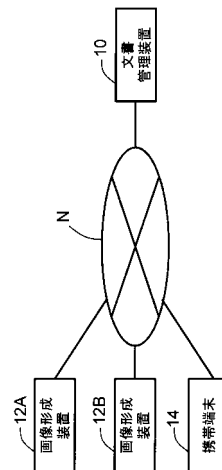
(54) 【発明の名称】 情報処理装置及びプログラム

(57) 【要約】

【課題】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。

【解決手段】文書管理装置10に対する利用のリクエストが第1端末装置から与えられると、その利用に必要な認証方式が特定される。また、第1端末装置に対応している認証方式を示す情報が取得される。そして、第1端末装置に対応している認証方式が、上記の利用に必要な認証方式に適合していない場合、その利用に必要な認証方式に対応している第2端末装置に関する情報が、第1端末装置に送信される。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

文書データを管理する文書管理装置に対する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を示す情報を取得する第 1 取得手段と、
前記取得された情報が示す認証方式が、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、
を有する情報処理装置。

【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第 2 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】

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を更に有し、
前記制御手段は、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、
ことを特徴とする請求項 1 から請求項 3 のいずれか一項に記載の情報処理装置。

【請求項 5】

コンピュータを、
文書データを管理する文書管理装置に対する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を示す情報を取得する取得手段と、
前記取得された情報が示す認証方式が、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

10

20

30

40

50

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、文書データを管理する文書管理装置に対する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を示す情報を取得する第1取得手段と、前記取得された情報が示す認証方式が、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、を有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第2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。

【0012】

請求項4に係る発明は、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を更に有し、前記制御手段は、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、ことを特徴とする請求項1から請求項3のいずれか一項に記載の情報処理装置である。

【0013】

請求項5に係る発明は、コンピュータを、文書データを管理する文書管理装置に対する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を示す情報を取得する取得手段と、前記取得された情報が示す認証方式が、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、として機能させるプログラムである。

【発明の効果】

10

20

30

40

50

【 0 0 1 4 】

請求項 1 , 5 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。

【 0 0 1 5 】

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。

【 0 0 1 6 】

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。

【 0 0 1 7 】

請求項 4 に係る発明によると、ユーザによる無駄な操作の発生が防止又は低減される。

【 図面の簡単な説明 】

【 0 0 1 8 】

【 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 1 0 】 認証端末テーブルの一例を示す図である。

【 図 1 1 】 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 1 2 】 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 1 3 】 代替顔認証処理の一例を示すフローチャートである。

【 図 1 4 】 追加認証処理の一例を示すフローチャートである。

【 図 1 5 】 画像形成装置の画面の一例を示す図である。

【 図 1 6 】 画像形成装置の画面の一例を示す図である。

【 図 1 7 】 画像形成装置の画面の一例を示す図である。

【 図 1 8 】 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 】

【 0 0 1 9 】

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 1 0 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 1 2 A , 1 2 B ）と、を含む。文書管理装置 1 0 及び画像形成装置 1 2 A , 1 2 B 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 1 4 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 1 4 は文書管理システムに含まれていなくてもよい。

【 0 0 2 0 】

文書管理装置 1 0 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 1 2 A , 1 2 B 等の装置から文書管理装置 1 0 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。

【 0 0 2 1 】

画像形成装置 1 2 A , 1 2 B 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 1 2 A

10

20

30

40

50

、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。

10

【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。

20

【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。

30

【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。

40

【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】

50

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、
10 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
20 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。
30

【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。
40

【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、
50

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。

10

20

30

40

50

【 0 0 4 8 】

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。

【 0 0 4 9 】

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。

【 0 0 5 0 】

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。

【 0 0 5 1 】

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度、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。

【 0 0 5 2 】

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。

【 0 0 5 3 】

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。

【 0 0 5 4 】

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

10

20

30

40

50

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。

10

【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）。

20

【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」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。

30

【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。

40

【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、

50

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。

10

【0061】

一例として、画像形成装置12Bの端末IDが「3」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。

20

30

【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。

40

【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)、

50

ステップ S 1 1 , S 1 2 の処理が実行される。

【 0 0 6 6 】

ステップ S 1 1 では、代替認証情報生成部 2 6 は、図 1 0 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 2 6 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 1 2 B 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 1 2 B 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 ID 2 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。

10

【 0 0 6 7 】

ステップ S 1 2 では、代替認証情報生成部 2 6 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 2 6 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 1 2 B 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 1 2 B 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。

20

【 0 0 6 8 】

なお、ステップ S 1 1 , S 1 2 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 S 1 1 の処理のみが実行されてもよいし、ステップ S 1 2 の処理のみが実行されてもよいし、ステップ S 1 1 , S 1 2 の両方の処理が実行されてもよい。

【 0 0 6 9 】

そして、ステップ S 1 1 , S 1 2 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 (S 1 3 , 代替装置数 > 0、又は、代替認証方式数 > 0)、処理はステップ S 1 4 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 S 1 4 に移行する。この場合、代替認証情報生成部 2 6 は、代替認証リストを作成する (S 1 4)。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。

30

【 0 0 7 0 】

次に、代替認証情報生成部 2 6 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 (S 1 5)。そして、処理は、図 1 1 に示されているステップ S 1 9 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。

40

【 0 0 7 1 】

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 (S 1 3 , 代替装置数 = 0、かつ、代替認証方式数 = 0)、処理はステップ S 1 6 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 S 1 6 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

50

、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 12 B 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 (S 16, 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 S 17 に移行する。一方、認証対応数が 0 (ゼロ) である場合 (S 16, 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 S 18 に移行する。

【0072】

ステップ S 17 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 S 19 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。

10

【0073】

ステップ S 18 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 12 B 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 12 B 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 S 19 に移行する。

【0074】

以下、図 11 を参照して、ステップ S 19 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 12 B に送信される (S 19)。

20

【0075】

画像形成装置 12 B 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 (S 20)。

【0076】

そして、画像形成装置 12 B 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 12 B 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 12 B 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 (S 21, Yes)、制御部 38 は、ログイン用画面情報を作成し (S 22)、ログイン用画面を UI 部 34 に表示させる (S 23)。

30

【0078】

ログイン用画面には、画像形成装置 12 B 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 12 B 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。

40

【0080】

一方、画像形成装置 12 B 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 (S 21, No)、制御部 38 は、ログインエラー画面情報を作成し (S 23)、ログインエラー画面を UI 部 34 に表示させる (S 24)。エ

50

レスポンス情報が受信された場合、画像形成装置 1 2 B 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 1 2 B 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 1 2 B 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。

【 0 0 8 1 】

画像形成装置 1 2 B の UI 部 3 4 に表示されている画面がユーザによって確認され (S 2 5)、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。

10

【 0 0 8 2 】

画像形成装置 1 2 B 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 1 2 B の UI 部 3 4 を利用してログイン操作を行うことになる (S 2 6)。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 1 2 B 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 1 2 B の UI 部 3 4 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 1 2 B から文書管理装置 1 0 に送信され、文書管理装置 1 0 の認証部 1 8 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 1 2 B から文書管理装置 1 0 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 1 2 B から文書管理装置 1 0 へのログインが禁止される。

20

【 0 0 8 3 】

また、画像形成装置 1 2 B 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 (S 2 7)。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 1 2 B 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 1 2 A が顔認証方式に対応している場合、画像形成装置 1 2 A に関する情報が、画像形成装置 1 2 B の UI 部 3 4 (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 1 2 A に移動し、その画像形成装置 1 2 A を用いてログイン操作を行うことになる。

30

【 0 0 8 4 】

また、画像形成装置 1 2 B 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 (S 2 8)。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 1 2 B 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 1 2 B の UI 部 3 4 (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。

40

【 0 0 8 5 】

以上のように、画像形成装置 1 2 B がログイン認証方式に対応している場合、画像形成装置 1 2 B 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 1 2 B 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 1 2 B 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 1 2 B 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

50

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、それらに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。

10

【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нтаムIDとワнта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。

20

30

【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нтаムIDとワнтаムパスワードを入力する。画像形成装置12Bは、ワнтаムIDとワнта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。

40

【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

50

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нтаム ID とワнта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нтаム ID とワнта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нтаム ID とワнта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нтаム ID とワнта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нтаム ID とワнта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るとし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

10

20

30

40

50

像形成装置 1 2 B の認証状態が特定される。

【 0 0 9 9 】

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 (S 5 4 , Y e s)、その操作が許可される。この場合、制御部 2 4 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 1 6 によって画像形成装置 1 2 B に送信される (S 5 5)。そのレスポンス情報は画像形成装置 1 2 B によって受信され (S 5 6)、画像形成装置 1 2 B 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。

【 0 1 0 0 】

例えば、画像形成装置 1 2 B を利用して、 I D ・パスワード認証によって文書管理装置 1 0 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、 I D ・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 1 2 B において「文書 - 2 」に対する操作が許可される。

【 0 1 0 1 】

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 (S 5 4 , N o)、追加認証処理が実行される。この場合、制御部 2 4 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 1 6 によって画像形成装置 1 2 B に送信される (S 5 6)。その追加認証要求情報は画像形成装置 1 2 B によって受信され (S 5 7)、画像形成装置 1 2 B と文書管理装置 1 0 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 (S 5 8)。つまり、図 1 1 及び図 1 2 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 1 0 において、画像形成装置 1 2 B 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 1 0 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 1 2 B に送信される。画像形成装置 1 2 B 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 1 2 B に表示される。

【 0 1 0 2 】

例えば、画像形成装置 1 2 B を利用して、 I D ・パスワード認証によって文書管理装置 1 0 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 - 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 - 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 S 5 8 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 1 2 B に表示される。

【 0 1 0 3 】

画像形成装置 1 2 B 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 1 2 B 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。

【 0 1 0 4 】

10

20

30

40

50

ステップ S 5 9 では、上記の追加認証要求画面に従った処理が行われる (S 5 9)。画像形成装置 1 2 B 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 1 2 B 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。

【 0 1 0 5 】

以上のように、画像形成装置 1 2 B 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 1 2 B 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 1 2 B 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 1 2 B 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 1 2 B 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。

10

【 0 1 0 6 】

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 1 0 の制御部 2 4 は、その時点において画像形成装置 1 2 B 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 2 2 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 1 2 A) を用いた認証処理が成功した場合、制御部 2 4 は、記憶部 2 2 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 1 2 A) に送信する。この場合、代替装置としての画像形成装置 1 2 A の UI 部 3 4 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 1 2 A 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 1 2 A において、文書管理装置 1 0 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。

20

30

【 0 1 0 7 】

次に、上記の処理によって画像形成装置 1 2 B に表示される画面について説明する。

【 0 1 0 8 】

図 1 5 には、初期画面の一例が示されている。初期画面 4 8 は、ログイン時に画像形成装置 1 2 B の UI 部 3 4 に表示される画面である。初期画面 4 8 には、通信経路 N に接続されている文書管理装置 1 0 の一覧が表示されている。例えば、2 つの文書管理装置 1 0 (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 1 0 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 1 2 B は、装置 A (文書管理装置 1 0) に対して、利用リクエスト情報を送信する。そして、図 1 1 及び図 1 2 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 1 2 B の UI 部 3 4 に表示される。

40

【 0 1 0 9 】

図 1 6 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 5 0 は、図 1 1 中のステップ S 2 4 において、画像形成装置 1 2 B の UI 部 3 4 に表示される画面である。このログイン用画面 5 0 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。

【 0 1 1 0 】

50

「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 12 B 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 12 B 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 12 B 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 12 B から文書管理装置 10 にログインすることが想定される。

10

【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 12 B 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 12 B 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 12 B 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 12 B 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。

20

【0113】

画像形成装置 12 B 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 12 B と代替装置との位置関係を特定し、画像形成装置 12 B 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 12 B 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 12 B 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。

30

【0114】

別の例として、代替装置が画像形成装置 12 B 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 12 B 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 12 B 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 12 B 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。

40

【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 12 B が対応していない認証方式に替わる代替

50

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。

10

【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)ということを示している。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に対応している認証方式が存在することになる。また、代替装置及び代替認証方式が存在することになる。これらの情報が表示されることにより、画像形成装置12Bに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。

20

【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。

30

【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。

40

【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

50

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 1 2 B 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。

【 0 1 2 3 】

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 1 2 B の U I 部 3 4 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。

【 0 1 2 4 】

画像形成装置 1 2 B 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 5 4 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 1 2 B 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 1 2 B の U I 部 3 4 に表示される。

10

【 0 1 2 5 】

また、追加認証処理が実行される場合、図 1 7 に示されている画面 5 2 の情報（例えば URL）が、文書管理装置 1 0 の記憶部 2 2 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 U I 部 3 4 に画面 5 2 が表示される。これにより、文書管理装置 1 0 へのログイン操作が省かれ、ユーザの手間が軽減される。

【 0 1 2 6 】

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。

20

【 0 1 2 7 】

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。

【 0 1 2 8 】

また、認証部 1 8 は、文書管理装置 1 0 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 1 0 に送信されることになる。文書管理装置 1 0 は、その認証結果に応じた処理を実行する。

30

【 0 1 2 9 】

上記の文書管理装置 1 0、画像形成装置 1 2 A、1 2 B 及び携帯端末 1 4 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。

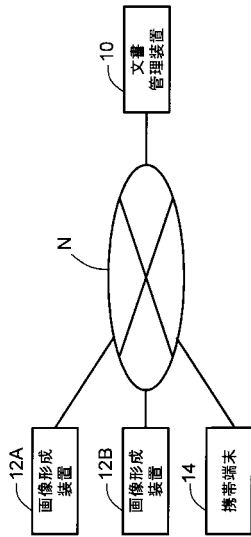
40

【 符号の説明 】

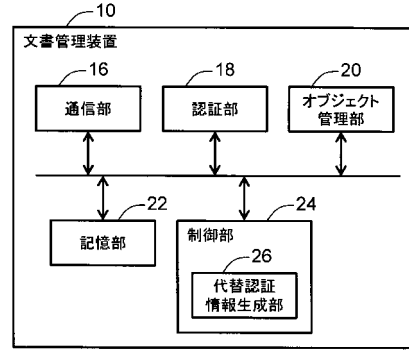
【 0 1 3 0 】

1 0 文書管理装置、1 2 A、1 2 B 画像形成装置、1 4 携帯端末、1 8 認証部、2 0 オブジェクト管理部、2 6 代替認証情報生成部。

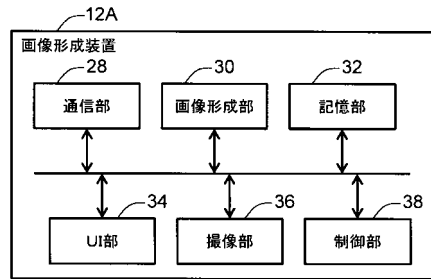
【 図 1 】



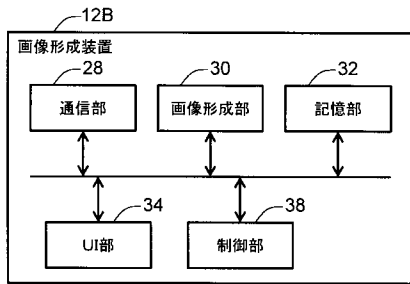
【 図 2 】



【 図 3 】



【 図 4 】

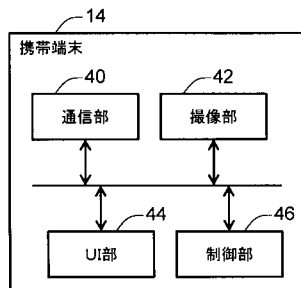


【 図 6 】

<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 5 】



【 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>

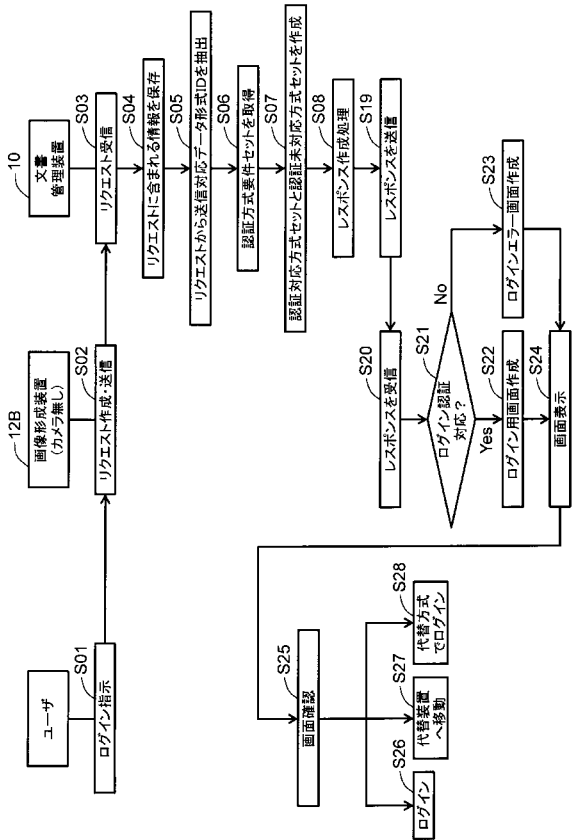
代替方式ID	代替方式名称	認証方式ID
代替方式1	携帯端末でのカメラ認証	認証方式3

【 図 10 】

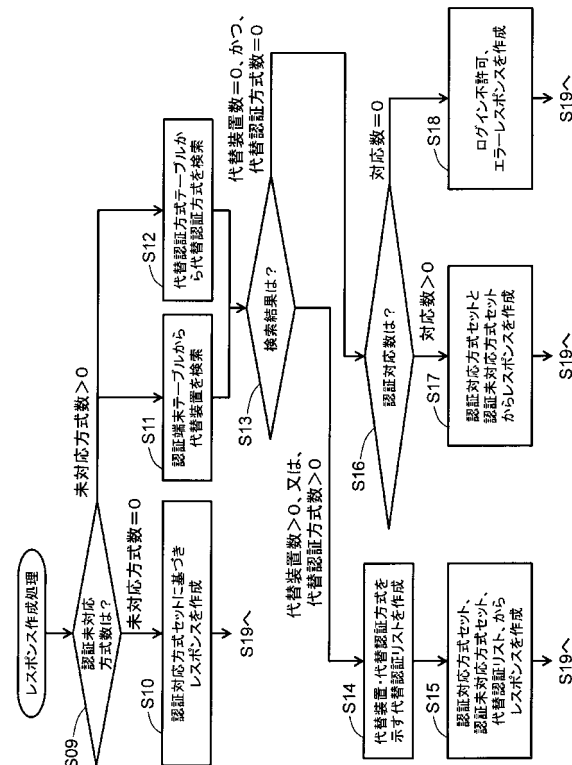
<認証端末テーブル>

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

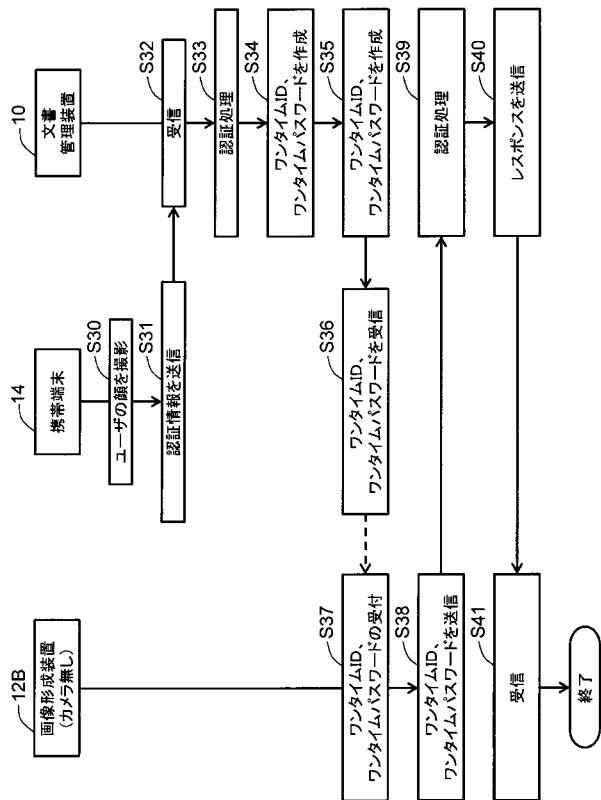
【図 1 1】



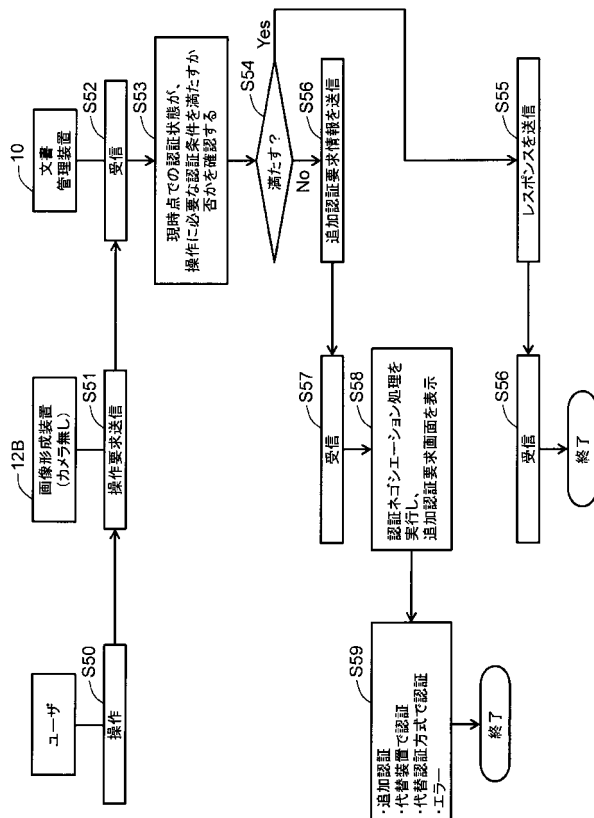
【図 1 2】



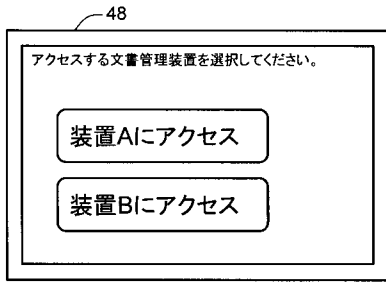
【図 1 3】



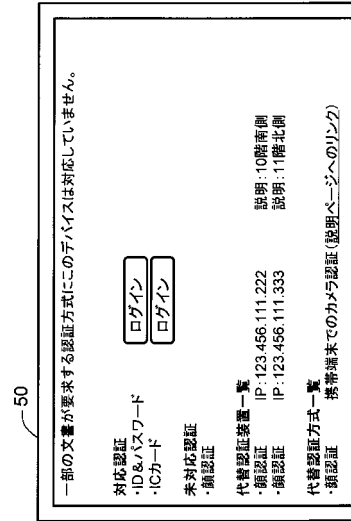
【図 1 4】



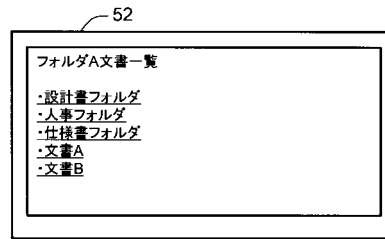
【 図 1 5 】



【 図 1 6 】



【 図 1 7 】



【 図 1 8 】

