(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4490463号
(P4490463)
(45)発行日　平成22年6月23日(2010.6.23)　(24)登録日　平成22年4月9日(2010.4.9)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
G06F 15/00 (2006.01)　　G06F 15/00 390

請求項の数 10　(全 17 頁)

(21)出願番号　特願2007-217454(P2007-217454)
(22)出願日　平成19年8月23日(2007.8.23)
(65)公開番号　特開2009-53762(P2009-53762A)
(43)公開日　平成21年3月12日(2009.3.12)
審査請求日　平成20年10月9日(2008.10.9)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(74)復代理人　100115624
弁理士　濱中　淳宏
(74)復代理人　100128015
弁理士　堀田　誠
(72)発明者　猪瀬　康二
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置、および情報処理方法

(57)【特許請求の範囲】
【請求項１】
認証サーバと第１の装置と第２の装置とを含む情報処理システムであって、
前記認証サーバは、ユーザの識別情報及びパスワードを管理し、前記第１及び第２の装置のユーザ認証を行う認証管理部を有し、
前記第１の装置は、
第１の操作手段と、
前記第１の装置に対する前記第１の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受けるための第１の入力手段とを有し、
前記第２の装置は、
前記第１の操作手段とは異なる第２の操作手段と、
前記第２の装置に対する前記第２の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受けるための第２の入力手段とを有し、
前記第１の入力手段を介して入力された識別情報と該識別情報を認証するためのパスワードとが前記認証サーバにより認証され前記第１の装置に対するユーザからの操作が許可された場合、前記第２の装置は、該認証されたユーザの識別情報が前記第２の入力手段に入力されたときに当該ユーザからの操作を許可することを特徴とする情報処理システム。
【請求項２】

前記認証サーバは、前記第１の装置に対するユーザからの操作を許可した際に、当該操作を許可したユーザの識別情報を格納することを特徴とする請求項１に記載の情報処理システム。

【請求項３】

前記認証サーバは、前記第１の装置に対するユーザからの操作を許可した際に、当該操作を許可したユーザの識別情報を格納し、

前記第２の装置は、前記格納された識別情報に係るユーザに対して前記第２の装置での操作を許可するために、前記第２の入力手段を介しての前記識別情報及び前記パスワードの入力の要求を行う状態から、前記第２の入力手段を介しての前記パスワードの入力の要求を行わず、前記第２の入力手段を介しての前記識別情報の入力の要求を行う状態へと遷移することを特徴とする請求項２に記載の情報処理システム。

【請求項４】

前記入力手段は、カードからカード入力を取得するカード入力手段を含み、

前記識別情報は、前記カード入力から得られた情報であることを特徴とする請求項１乃至３の何れか１項に記載の情報処理システム。

【請求項５】

ユーザ認証を行う認証サーバと通信可能な通信手段と、ユーザからの操作を許可するためにユーザの識別情報及び該識別情報を認証するためのパスワードの入力を受けるための入力手段とを備える情報処理装置であって、

別の情報処理装置の操作手段から入力されたユーザの識別情報及びパスワードが前記認証サーバにより認証され、当該識別情報を有するユーザに対して、当該別の情報処理装置に対する操作が許可された場合に、

前記入力が行われた識別情報と同じ識別情報の入力が前記情報処理装置の入力手段を介してユーザから行われると、当該情報処理装置の操作が可能となることを特徴とする情報処理装置。

【請求項６】

複数の装置に接続された情報処理装置であって、

前記複数の装置の１つから、ユーザの識別情報及び装置の識別情報を取得する手段と、

前記取得したユーザの識別情報に基づき、ユーザの識別情報と特定の業務を達成するために必要な作業群と該作業群を処理するのに用いられる装置群とを関連付けたテーブルを参照して、運用途中の作業群が存在するか否かを判断する手段と、

前記複数の装置のうち、前記取得した装置の識別情報に係る装置に対して、前記ユーザの識別情報を認証するためのパスワードをユーザに対して要求するように指示する手段とを備え、

前記指示する手段は、前記判断する手段にて、運用途中の作業群が存在すると判断される場合に、前記指示を行わないことを特徴とする情報処理装置。

【請求項７】

前記作業群を取得する手段と、

前記複数の装置のうち、前記作業群を処理するのに用いられる装置群と前記作業群とを関連付けて管理する手段と、

前記取得したユーザの識別情報と、前記作業群と、前記装置群とを関連付けて、前記テーブルを作成する手段とをさらに備え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】

前記テーブルにおいて、前記装置群が、順序付けられて管理されてい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】

認証サーバと第１の装置と第２の装置とを含む情報処理システムにおける情報処理方法であって、

前記認証サーバが、ユーザの識別情報及びパスワードを管理し、前記第１及び第２の装

置のユーザ認証を行う工程と、
前記第１の装置が、前記第１の装置の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受ける第１の入力工程と、
前記第２の装置が、前記第２の装置の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受ける第２の入力工程とを有し、
前記第１の入力工程にて入力された識別情報とパスワードとが前記認証サーバにより認証され前記第１の装置に対するユーザからの操作が許可された場合、前記第２の入力工程にて、該操作が許可されたユーザの識別情報が入力されたときに前記第２の装置に対するユーザからの操作を許可すること
を特徴とする情報処理方法。
【請求項１０】
認証サーバと第１の装置と第２の装置とを含む情報処理システムにおいて情報処理方法を実行させるためのプログラムであって、前記情報処理方法は、
前記認証サーバが、ユーザの識別情報及びパスワードを管理し、前記第１及び第２の装置のユーザ認証を行う工程と、
前記第１の装置が、前記第１の装置の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受ける第１の入力工程と、
前記第２の装置が、前記第２の装置の操作手段を介したユーザからの操作を許可するために、ユーザの識別情報及び該識別情報を認証するためのパスワードの入力をユーザから受ける第２の入力工程とを有し、
前記第１の入力工程にて入力された識別情報とパスワードとが前記認証サーバにより認証され前記第１の装置に対するユーザからの操作が許可された場合、前記第２の入力工程にて、該操作が許可されたユーザの識別情報が入力されたときに前記第２の装置に対するユーザからの操作を許可すること
を特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理装置、および情報処理方法に関する。より詳細には、印刷やデータ入出力のフロントエンド装置として多機能デバイスを操作するシステムの構成、業務の形態において、取り扱う情報の機密性やユーザの操作状況に応じて動作が変化する情報処理システム、情報処理装置、および情報処理方法に関する。
【背景技術】
【０００２】
近年複合デバイスは高機能・多機能・高性能化、あるいはユーザインタフェースを含めた操作性の向上が進み、コピー作業やPCからの印刷に留まらず、以下に示すような処理、動作が行われるようになってきている。例えば、デバイス上でスキャンした画像をスキャン情報に従ってサーバに登録する、汎用的なフォーマットに変換し指定した宛先にネットワークを介して送信する、あるいは操作画面上にリストされたジョブを操作する等である。このように、複合デバイスにおいては、従来PC上で行っていた作業の一部代替を含めて、業務端末としての役割を果たす機会が多くなってきている。
【０００３】
ところで、一般に業務とは、関連性のある複数の作業を遂行する（ワークフロー；特定の業務を達成するために必要な作業群）ことでその目的を達成する。ここで個々の作業がデバイスの操作を伴うことも想定される。例えば、カタログ作成業務において、掲載予定の画像を撮影した人が、校正を目的として仕上がりをイメージできる程度の品質でカタログサンプルを印刷する、という業務を想定する。

【０００４】
まず撮影者は複合デバイスに足を運び、デジタルカメラに保存された画像データを入力して、カタログを作成するためのサーバに登録する（第一の工程とする）。一定の処理の後に印刷用のデータが準備され、デバイス上に表示された印刷用データのリストから、登録した画像がレイアウトされたカタログのサンプルを選択し、印刷する（第二の工程とする）。
【０００５】
ただし、第一の工程で使用するデバイスと第二の工程で使用するそれは、業務の都合上、あるいはデバイスの機能または性能上同一のものであることが許容されず、異なるものとする。一方、取り扱う画像は版権上機密性が高いため、第一の工程、第二の工程においてICカード等によるユーザ特定（個人特定）に加えてユーザ認証（パスワード入力）を必要となる。
【０００６】
さて、複数のデバイスを操作する際に必要なユーザ認証（個人認証）を行う従来技術が特許文献１に記載されている。これによれば、個人を特定するICカードの番号と、操作者の所持品に装備される無線タグの情報を予め関連付けして登録している。ここで、特許文献１においては、上記無線タグを所持品として衣服やアクセサリ等に搭載することによりユーザが身に着けたり、ユーザの周囲に配置することが前提となっている。特許文献１では、デバイス操作時にICカード番号と無線タグ情報を取得、照合し、一定の一致を見れば本人であると認める（認証成功とする）、つまり無線タグの情報の読み取りがパスワード入力の代わりを果たす、という特徴を有する。
【０００７】
【特許文献１】特開２００５－３５２７１０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
複数のデバイスを操作する際に、その都度パスワード入力することはユーザの負担である。デバイスの数が増えれば、その手間も比例して増す。特許文献１ではこの課題を解決している。しかしながら、特許文献１でのユーザ認証は、ユーザが身に着けたり、周囲に配置した無線タグの組合せとの一致に応じて行っているので、無線タグを１つでも紛失すると上記ユーザ認証が行えなくなってしまう。また、ICカードと無線タグが装備された所持品とを同時に紛失した場合、拾得した人による“なりすまし”が可能となること、また所持品が追加、変更になる度に登録が必要であり、セキュリティ面、使い勝手の面で課題が残る。
【０００９】
また、機密性の高い画像処理等のワークフローを遂行する際、例えば、上述の第１の工程と第２の工程とを異なるデバイスで行う場合、上記高い機密性のために、それぞれのデバイスにおいて、パスワード入力等のユーザ認証を行う必要がある。すなわち、第１の工程を行う際に第１の装置にてパスワード入力を行い、第２の工程を行う際には第２の装置にて再びパスワード入力を行う必要がある。
【００１０】
ここに特許文献１を適用しても、各デバイスへのログインの際に無線タグによるユーザ認証をその都度行っており、例えば第２の工程を行う際に無線タグを１つでも所持していないと、第２の装置へのログインが行えない。
【００１１】
また、従来では、シングルサインオン（Single Sign-On）という技術がある。この技術を用いれば、ある装置の操作部において１回のユーザ認証が行われると、該操作部を用いている限り、他のアプリケーションにユーザ認証無しでアクセスすることができる。これは、一つの操作部は、通常、唯一無二のユーザによって独占排他的に用いられることが多いという前提に立っている。この前提のもと、ある装置の操作部において１回のユーザ認

証が行われると、その操作部を用いて操作をする唯一無二のユーザは信頼できる人であるという仮定が成立し、従って、その後のアクセスは、ユーザ認証を必要としないのである。

【００１２】

しかしながら、こうしたシングルサインオンを用いる場合では、装置を変え操作部を変えると、もう一度パスワード入力等のユーザ認証を行う必要がある。なぜなら、別の装置を別の操作部から利用するユーザは、既にユーザ認証が済んだユーザとは異なる蓋然性が高いからである。そのため、上述のように、複数のデバイスで所定のワークフローを遂行する場合、処理を行うデバイスを変える度にパスワード入力が必要となり、手間がかかってしまう。

【００１３】

本発明は、このような課題に鑑みてなされたもので、その目的とするところは、複数の装置を用いて特定の作業を行う際、ユーザにかかるユーザ認証の負担を軽減可能な情報処理システム、情報処理装置、および情報処理方法を提供することにある。

【課題を解決するための手段】

【００１４】

このような目的を達成するために、本発明は、第１の装置と第２の装置とを含む情報処理システムであって、前記第１の装置は、前記第１の装置に対するユーザからの操作を許可するために、前記第１の装置の操作部を介してユーザからの、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する第１の要求手段を有し、前記第２の装置は、前記第２の装置に対するユーザからの操作を許可するために、前記第２の装置の操作部を介してユーザからの、ユーザ特定情報及びユーザ認証情報の入力を要求する第２の要求手段を有し、前記第１の装置に対するユーザからの操作が許可された場合に、前記第２の要求手段は、前記第２の装置に対するユーザからの操作を許可するための前記ユーザ認証情報の入力の要求を行わないことを特徴とする。

【００１５】

また、本発明は、操作部と、ユーザからの操作を許可するために、前記操作部を介してユーザから、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する要求手段とを備える情報処理装置であって、別の情報処理装置の操作部から、ユーザ特定情報及びユーザ認証情報の入力が行われ、前記ユーザ特定情報を有するユーザに対して、別の情報処理装置に対する操作が許可された場合に、前記要求手段は、前記入力が行われたユーザ特定情報と同じユーザ特定情報の入力が前記情報処理装置の操作部を介してユーザから行われると、前記情報処理装置の操作部を介しての前記ユーザ認証情報の入力を要求しないことを特徴とする。

【００１６】

また、本発明は、操作部と、ユーザからの操作を許可するために、前記操作部を介してユーザから、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する要求手段とを備える情報処理装置であって、別の情報処理装置の操作部からユーザ特定情報及びユーザ認証情報の入力が行われ、前記ユーザ特定情報を有するユーザに対して、別の情報処理装置に対する操作が許可された場合に、前記要求手段は、前記入力が行われたユーザ特定情報と同じユーザ特定情報の入力が前記情報処理装置の操作部を介してユーザから行われると、前記情報処理装置の操作部を介しての前記ユーザ認証情報の入力なしに、前記ユーザ特定情報を有するユーザからの前記情報処理装置に対する操作を許可することを特徴とする。

【００１７】

また、本発明は、複数の装置に接続された情報処理装置であって、前記複数の装置の１つから、ユーザを特定するためのユーザ特定情報を取得する手段と、前記ユーザ特定情報に基づき、ユーザ特定情報と特定の業務を達成するために必要な作業群と該作業群を処理するのに用いられる装置としてグループ化された装置群とを関連付けたテーブルを参照して、運用途中の作業群が存在するか否かを判断する手段と、前記複数の装置のうち、前記

ユーザ特定情報の取得先の装置に対して、ユーザを認証するためのユーザ認証情報の入力をユーザに対して要求するように指示する手段とを備え、前記指示する手段は、前記判断する手段にて、運用途中の作業群が存在すると判断される場合に、前記指示を行わないことを特徴とする。

【００１８】

また、本発明は、第１の装置と第２の装置とを含む情報処理システムにおける情報処理方法であって、前記第１の装置に対するユーザからの操作を許可するために、前記第１の装置の操作部を介してユーザからの、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する第１の要求工程と、前記第２の装置に対するユーザからの操作を許可するために、前記第２の装置の操作部を介してユーザからの、ユーザ特定情報及びユーザ認証情報の入力を要求する第２の要求工程とを有し、前記第１の装置に対するユーザからの操作が許可された場合に、前記第２の要求工程は、前記第２の装置に対するユーザからの操作を許可するための前記ユーザ認証情報の入力の要求を行わないことを特徴とする。

【００１９】

また、本発明は、操作部を有する情報処理装置における情報処理方法であって、ユーザからの操作を許可するために、前記操作部を介してユーザから、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する要求工程を有し、別の情報処理装置の操作部から、ユーザ特定情報及びユーザ認証情報の入力が行われ、前記ユーザ特定情報を有するユーザに対して、別の情報処理装置に対する操作が許可された場合に、前記要求工程は、前記入力が行われたユーザ特定情報と同じユーザ特定情報の入力が前記情報処理装置の操作部を介してユーザから行われると、前記情報処理装置の操作部を介しての前記ユーザ認証情報の入力を要求しないことを特徴とする。

【００２０】

また、本発明は、操作部を有する情報処理装置における情報処理方法であって、ユーザからの操作を許可するために、前記操作部を介してユーザから、ユーザを特定するためのユーザ特定情報及びユーザを認証するためのユーザ認証情報の入力を要求する要求工程を有し、別の情報処理装置の操作部からユーザ特定情報及びユーザ認証情報の入力が行われ、前記ユーザ特定情報を有するユーザに対して、別の情報処理装置に対する操作が許可された場合に、前記要求工程は、前記入力が行われたユーザ特定情報と同じユーザ特定情報の入力が前記情報処理装置の操作部を介してユーザから行われると、前記情報処理装置の操作部を介しての前記ユーザ認証情報の入力なしに、前記ユーザ特定情報を有するユーザからの前記情報処理装置に対する操作を許可することを特徴とする。

【００２１】

また、本発明は、複数の装置に接続された情報処理装置における情報処理方法であって、前記複数の装置の１つから、ユーザを特定するためのユーザ特定情報を取得する手段と、前記ユーザ特定情報に基づき、ユーザ特定情報と特定の業務を達成するために必要な作業群と該作業群を処理するのに用いられる装置としてグループ化された装置群とを関連付けたテーブルを参照して、運用途中の作業群が存在するか否かを判断する工程と、前記複数の装置のうち、前記ユーザ特定情報の取得先の装置に対して、ユーザを認証するためのユーザ認証情報の入力をユーザに対して要求するように指示する工程とを有し、前記指示する工程は、前記判断する工程にて、運用途中の作業群が存在すると判断される場合に、前記指示を行わないことを特徴とする。

【発明の効果】

【００２２】

特定のワークフローを遂行する過程で使用することが計画されている装置群に対して、実際にそれらを使用するフェーズで個々の装置でのユーザ認証情報（例えば、パスワード）入力を必要としない。よって、任意の装置において、上記入力を１回のみで済ますことができ、ユーザの負担軽減とユーザ認証情報入力によるセキュリティ確保を両立させることができる。

【発明を実施するための最良の形態】
【００２３】
以下、図面を参照して本発明の実施形態を詳細に説明する。なお、以下で説明する図面で、同一機能を有するものは同一符号を付け、その繰り返しの説明は省略する。
図１を用いて、本発明の一実施形態を実施する代表的なシステム構成について説明する。
符号101は、画像の入力や印刷データのリスト等を行う、ユーザが直接操作する第１のデバイス（第１の装置）を表す。符号102は、認証サーバ109との間でICカードから読み取ったユーザID（ユーザ特定情報；ユーザを特定するための情報）、ユーザが入力するパスワード（ユーザ認証情報；ユーザを認証するための情報）をやりとりするための通信部である。通信部102は、例えば、デバイスを特定する情報（デバイス特定情報）など、上述以外の情報についても認証サーバ111とやり取りすることができる。符号103は、ユーザがICカードをかざした際にユーザを特定するICカードの番号を読み取り、ユーザ特定情報としてのユーザIDを取得するICカード読取部を表す。
【００２４】
符号104は、ユーザ特定とユーザ認証の処理の後に利用可能なデバイスの機能を提供する情報処理部を表す。この情報処理部104は、種々の演算、制御、判別などの処理動作を実行するCPUを備えている。また、情報処理部104は、該CPUによって実行される、図２等にて後述される本発明に係る処理などの制御プログラムなどを格納するROMを備えている。さらに、情報処理部104は、上記CPUの処理動作中のデータや入力データなどを一時的に格納するRAMなどを備えている。
【００２５】
符号105は、所定の指令あるいはデータなどを入力するキーボードあるいは各種スイッチなどを含む入力操作部である。第１のデバイス101は、装置の入力・設定状態などをはじめとする種々の表示を行う表示部（不図示）を備えることができる。さらに、第1のデバイスは、プリンタ等の画像形成機能、スキャナ等の画像読取機能等を適宜、備えることができる。
【００２６】
本発明の一実施形態では、上記情報処理部104は、上記各構成を統合して制御する。
【００２７】
本発明の一実施形態では、ユーザがICカードをICカード読取部103にかざすことによって、ICカード読取部103がICカードからユーザ特定情報としてのユーザIDを取得することになる。そして、ユーザが入力操作部105を操作してパスワードを入力することにより、第1のデバイスはユーザ認証情報としてのパスワードを取得することになる。
【００２８】
なお、本発明の一実施形態においては、ユーザ特定情報を取得するためにICカードによる読取を行っているが、これに限定されない。例えば、入力操作部105にてユーザがIDを入力するなど、第１のデバイス101がユーザ特定情報を取得できればいずれの手段を用いても良い。
【００２９】
符号106は、第１のデバイス101と同等の機能を有する第２のデバイス（第２の装置）である。通信部107は通信部102と、ICカード読取部108はICカード読取部103と、情報処理部109は情報処理部104と、入力操作部110は入力操作部105それぞれ同等の機能を有する。なお、第２のデバイスも上記表示部、画像形成機能、画像読取機能等を備えることができる。
【００３０】
符号111は、ユーザによる第１のデバイス101、第２のデバイス105の利用を管理する認証サーバを表す。符号112は、本発明の特徴である、パスワード入力を必要とするか否かを検証するパスワード管理部である。符号113は、デバイスを用いようとしているユーザが許可されたユーザか否かを判断するユーザ情報管理部である。符号114は、パスワード

管理部112によって利用され、所定のワークフローと該ワークフローの処理に関するデバイス群とを関係付けておくデバイスグループ管理部である。

【００３１】

また、認証サーバ111は、種々の演算、制御、判別などの処理動作を実行するCPU（不図示）を有する制御部（不図示）を備えている。該制御部は、該CPUによって実行される、図２等にて後述される本発明に係る処理などの制御プログラムなどを格納するROM（不図示）を有している。さらに、制御部は、上記CPUの処理動作中のデータや入力データなどを一時的に格納するRAM（不図示）などを有する。

【００３２】

さらに、認証サーバ111は、所定の指令あるいはデータなどを入力するキーボードあるいは各種スイッチなどを含む入力操作部、および装置の入力・設定状態などをはじめとする種々の表示を行う表示部（不図示）を備えることができる。

【００３３】

本発明の一実施形態では、上記制御部は、認証サーバ111が備える上記各構成を統合して制御する。

【００３４】

図１において、認証サーバ111と第１のデバイス101および第２のデバイス106との間で情報のやりとりが行えるように、認証サーバ111と第１のデバイス101および第２のデバイス106とはネットワークなどを介して接続されている。

【００３５】

なお、図１においては、認証サーバ111に、第１のデバイス101および第２のデバイス106が接続される形態を示しているが、他のデバイスを接続するようにしても良い。

【００３６】

さて、本発明の一実施形態では、あるワークフローを処理するために用いられるデバイスを、上記あるワークフローに関連付けて管理することが重要である。すなわち、あるワークフローの処理に関するデバイスをグループ化して認証サーバ111にて管理し、該グループに属する複数のデバイスについて、ユーザ認証情報の入力を最初の一回のみとすることが本発明の特徴である。

【００３７】

上記グループ化は、ユーザが認証サーバ111の入力操作部を操作して、ワークフローと該ワークフローに関するデバイスとの関連付けを行うようにすれば良い。

例えば、ワークフローがカタログ作成に関するものである場合、ユーザが認証サーバ111の入力操作部を操作して、認証サーバ111に接続されたデバイス群（装置群）の中から、上記カタログ作成に必要なデバイスを選択する。認証サーバ111は、該選択に基づいて、選択されたデバイス群をグループ化し、上記カタログ作成というワークフローと関連付ける。

【００３８】

この関連付けとしては、例えば、認証サーバ111が、各ワークフローに対してワークフローを識別するためのワークフローID（作業群識別子）を付与し、さらにグループ化されたデバイス群に対してデバイスグループID（装置群識別子）を付与する。そして、図３に示すように、ワークフローID301と、デバイスグループID302とを関連付けたテーブルを作成する。さらに、上記デバイスグループIDと、該デバイスグループIDにて識別されるデバイス群に含まれる各デバイスとを関連付けるために、図４に示すようなテーブルを作成する。このようにして、上記関連付けを行うことができる。なお、図３や図４に示すテーブルは、認証サーバ111のRAMに格納される。

【００３９】

ここで、あるワークフロー（例として、カタログ作成とする）に関する装置群として、第１のデバイス101と第２のデバイス106とを用いる場合について説明する。以下の説明では、上記カタログ作成について、第１のデバイス101にて第1の処理を行い、第2のデバイスにて第２の処理を行うものとする。

まずは、認証サーバ111は、カタログ作成について用いるデバイス群（装置群）のグループ化を行い、カタログ作成と第１のデバイス101および第２のデバイス102との関連付けを行う。このようにして、図３、４のようなテーブルが作成される。この例で言えば、図３のようなテーブルにおいて、カタログ作成を識別するためのワークフローIDと、第１のデバイス101と第２のデバイス106とを含むデバイス群を識別するためのデバイスグループIDとを関連付ける。また、図４のようなテーブルにおいて、上記デバイスグループIDと、該デバイスグループIDによって識別されるデバイス群に含まれる第１のデバイス101および第２のデバイス106とを関連付ける。

【００４０】

次いで、第１のデバイス101は、該第１のデバイス101に対するユーザからの操作を許可するために、ICカード読取部103を介してユーザからのユーザID、および入力操作部105を介してユーザからのパスワードの入力を要求する（第１の要求）。該要求によりユーザからのユーザIDおよびパスワードの入力があると、第１のデバイス101は、操作部（ICカード読取部や入力操作部等）を介して、ユーザ特定情報としてのユーザIDとユーザ認証情報としてのパスワードとを取得する。第1のデバイス101は、該ユーザIDおよびパスワードによって、該情報を提供したユーザに対して第１のデバイスにて上記カタログ作成に関する所定の処理の実行を許可する。よって、ユーザは、第１のデバイスにて第1の処理（デバイス処理）を行う。

【００４１】

ユーザが第２のデバイス106にて第２の処理を行う場合、第２のデバイス106は、該第１のデバイス106に対するユーザからの操作を許可するために、ユーザからの、ユーザIDおよびユーザからのパスワードの入力を要求する（第２の要求）。ただし、本発明の一実施形態では、カタログ作成の処理について同グループにグループ化された第１のデバイス101に対するユーザからの操作が許可された場合、第２の要求において、第２のデバイス106に対するパスワード入力の要求を行わない。

【００４２】

すなわち、別の情報処理装置である第１のデバイス101の操作部からユーザIDとパスワードの入力が行われ、該ユーザIDを有するユーザに対して、第１のデバイス101に対する操作が許可された場合に、パスワード入力を要求しない。つまり、第２のデバイス106は、第２のデバイス106の操作部（ICカード読取部108.や入力操作部110）を介しての、第２のデバイスに対するユーザからの操作を許可するためのパスワードの入力を要求しないのである。言い換えると、第２のデバイス106は、第２のデバイス106の操作部を介してのパスワードの入力無しに、上記ユーザIDを有するユーザからの第２のデバイス106に対する操作を許可することになる。

【００４３】

本発明の一実施形態では、上述のような第２のデバイス106における、パスワード入力を要するか否かの判断を、パスワード管理部112が、ワークフローとそれに関るグループ化されたデバイス群とを関連付けたテーブルに基づいて行っている。そして、該判断に基づいて、あるデバイス群において、すでにパスワード入力がされている場合のパスワード入力を省くことができる。よって、複数のデバイスを用いてあるワークフローを行う際、ユーザにかかるユーザ認証の負担を軽減することができる。

【００４４】

（第１の実施形態）

図２、図３、図４、図７を用いて、本実施形態に係る情報処理システムにおける、ワークフローと関連付いたデバイス群を利用する際の、パスワード入力の要否に関する処理について説明する。

図２は、本実施形態に係る、ワークフローの運用状況を管理することでパスワード入力の要否を制御する手順を示すフローチャートである。図３は、ワークフローID301とデバイス群を識別するデバイスグループID302とを関連付けたテーブルを示す。図４は、デバイスグループID401とその要素となるデバイスを識別するデバイスID402とを関係付けたテ

ーブルであり、符号401は符号302と同等である。図７は、運用途中のワークフローのリスト（運用途中確認テーブル）を示す図である。図７において、符号701は、ワークフローを運用しているユーザを識別するためのユーザ識別子としてのICカード番号（ユーザ特定情報）である。符号702は、ユーザが運用途中のワークフローIDである。符号703は、ワークフローが完了するまでに操作されるデバイスのうち、上記ワークフローの処理においてまだ使用されていない未操作デバイスを示す。

本実施形態では、図７に示すような運用途中確認テーブルは、あるワークフローの処理において、該処理に関るグループに含まれるデバイスのログイン時にパスワード入力が必要と判断される場合に、デバイスグループ管理部114によって作成される。

【００４５】

本実施形態では、認証サーバ111に、第１のデバイス101を含むデバイスが複数接続されているとする。そして、以下の説明では、例として第１のデバイス101に焦点を当てて説明する。

【００４６】

なお、本実施形態では、認証サーバ111にて、上述のようにして、ワークフローと該ワークフローを処理するデバイスとの関連付けが行われ、認証サーバ111が図３、４に示すテーブルを保持しているものとする。

【００４７】

ステップ201で、本実施形態に係る処理を開始する。ステップ202にて、第１のデバイス101は、ICカードの読み取りを定期的に繰り返す。ユーザがICカードを、ICカード読取部103にかざすことで、ステップ203にて、第１のデバイス101は、ICカード番号を読み取り、ユーザ特定情報（ユーザID）を取得する。次いで、通信部102は、読み取ったICカード番号を示すユーザ特定情報とユーザが操作しているデバイスを識別するデバイス識別情報（デバイスID）とを認証サーバ111に送信する。認証サーバ111は、ユーザ特定情報とデバイス識別情報とを受信すると、RAMに各情報を格納する。さらに、認証サーバ111は、ユーザ情報管理部113にて、送信されたユーザ特定情報にて識別されるユーザが許可されたユーザであることを確認する。

【００４８】

ステップ204～208に示す処理について、運用途中のワークフローが存在しない場合は、以下に示す＜運用途中のワークフローが存在しない場合＞にて詳細に説明する。一方、運用途中のワークフローが存在する場合は、以下に示す＜運用途中のワークフローが存在する場合＞にて詳細を述べる。

＜運用途中のワークフローが存在しない場合＞

ステップ204では、パスワード管理部112は、認証サーバ111に送信されたデバイス識別情報にて特定されるデバイス群に対応するデバイスグループを検索する。すなわち、パスワード管理部112は、第１のデバイス101から受信したデバイス識別情報（デバイスID）に基づいて、該デバイスIDが含まれるデバイスグループを示すデバイスグループIDを抽出する。検索されれば、パスワード管理部112は、続いて図３のテーブルを用いて該当するデバイスグループに対応するワークフローを検索する。すなわち、抽出されたデバイスグループIDに対応するワークフローIDを抽出する。認証サーバ111は、該抽出されたワークフローIDをRAMに格納する。複数存在する場合はユーザ選択により、運用対象のワークフローとして確定させる。

【００４９】

ここで、操作したデバイス（第１のデバイス101）の識別子（デバイス識別情報）が“Dev011”であるとする。よって、図４より、“Dev011”を含むデバイスグループは“G011”と判定され、図３よりそのデバイスを使用して運用可能なワークフローは“W001”に確定する。また、ユーザ特定情報である、ICカード番号が“yamada”であるとする。

【００５０】

また、パスワード管理部111は、ステップ204において、運用途中のワークフローがあるか否かを検索する。すなわち、パスワード管理部111は、RAMから、ユーザ特定情報および

デバイス識別情報と、上記抽出されたワークフローIDとを読み出し、運用途中確認テーブルを参照して、現在処理しようとするワークフローが運用途中か否かを検索する。この検索では、受信したユーザ特定情報と抽出されたワークフローIDとが運用途中確認テーブルにて関連付けられているかを判断し、関連付けられていない場合は、運用途中のワークフローが無いと判断する。関連付けられている場合は、現在処理しようとしているワークフローは、すでに別のデバイスにて処理が行われていると判断し、後述する＜運用途中のワークフローが存在する場合＞の処理を行うことになる。

【００５１】

このような判断が行われるのは、運用途中確認テーブルが、あるワークフローの処理において、該処理に関るグループに含まれるデバイスのログインのうち、パスワード入力が行われる場合に作成されるからである。従って、すでに、運用途中確認テーブルにおいて、ユーザ特定情報と抽出されたワークフローIDとが関連付けられていれば、該ワークフローIDにて特定されるワークフローの処理は始まっていることになる。よって、運用途中のワークフローが存在することが分かるのである。

【００５２】

つまり、図７に示す運用途中のワークフローを管理するテーブルにおいて、ICカード番号“yamada”とワークフローID“W001”とが関連付けられて管理されていない場合に、運用途中のワークフローが無いと判断する。

【００５３】

ステップ205では、パスワード管理部112は、ステップ204にてワークフローが検索されれば、ステップ206に進む。一方、検索されない場合は、今回の操作を単独のデバイス操作とみなし、パスワード管理部112は、第１のデバイス101に対して、パスワード入力を要求せずにそのままデバイス処理を行うように指示する情報を送信する。ステップ210では、第１のデバイス101は、該情報に基づいて、ユーザに対してパスワード入力の要求を行わず、所定のデバイス処理（画像取り込みやスキャンなど）を行う。該デバイス処理が終了すると、ステップ214にて、第1のデバイス101は、ログアウトを行い、ステップ202に進み、待機状態に入る。

【００５４】

ステップ206では、パスワード管理部111は、運用途中のワークフローがあるか否かを判断する。すなわち、パスワード管理部111は、ステップ204にて運用途中のワークフローがあると判断されたか否かを確認し、運用途中のワークフローが無いと判断した場合は、ステップ207に進む。

【００５５】

ステップ207において、パスワード管理部112は、第１のデバイス101（ユーザIDの取得先）に対して、ユーザにパスワード入力を要求するパスワード入力要求情報を送信する。第１のデバイス101は、上記パスワード入力要求情報を受信すると、該情報に従って、表示部等によりユーザに対してパスワード入力を促す。そして、ユーザが入力操作部105にてパスワードを入力すると、第１のデバイス101は、ユーザ認証情報としてのパスワードを取得し、通信部102により、パスワードを取得した旨を示すパスワード取得情報を認証サーバ111に送信する。なお、パスワード取得情報ではなく、パスワード自体を送信するようにしても良い。

【００５６】

ステップ208では、認証サーバ111がパスワード取得情報（または、パスワード自体）を受信すると、デバイスグループ管理部114は、現在処理しようとするワークフローについて、運用途中確認テーブルを作成する。該作成されたテーブルは、認証サーバ111のRAMに格納される。具体的には、デバイスグループ管理部114は、RAMに格納されたユーザ特定情報と、ステップ204にて抽出された、ワークフローIDおよびデバイスグループIDに含まれるデバイスIDとを関連付けて、上記テーブルを作成する。

【００５７】

すなわち、デバイスグループ管理部114は、デバイスグループID　G001にて特定される

デバイス群（Dev011,Dev012,Dev021にて特定されるデバイス群）を、未操作デバイスとする。デバイスグループ管理部114は、こうして得られた未操作デバイスに関する識別情報Dev011,Dev012,Dev021を、ICカード番号“yamada”とワークフローID“W001”とに関連付けて、運用途中確認テーブルを作成する。

【００５８】

このように、本実施形態では、ユーザ特定情報であるICカード番号を、運用途中のワークフローの有無を判断するための運用途中確認テーブルに関連付けている。そして、認証サーバ111が、該テーブルを用いて、適切なユーザ特定情報を入力するユーザが正しいユーザであると決め込むように上記有無の判断を行っているので、適切なユーザ特定情報を入力されれば、２度目以降のパスワードの入力を省くことができる。

【００５９】

ステップ209では、認証サーバ111は、デバイス処理を行うように指示する情報を第１のデバイス101に送信する。第１のデバイス101は、該情報を受信すると、所定のデバイス処理（画像取り込みやスキャンなど）を行う。

【００６０】

＜運用途中のワークフローが存在する場合＞

上述のように、パスワード管理部111は、受信したユーザ特定情報と抽出されたワークフローIDとが運用途中確認テーブルにて関連付けられているかを判断し、関連付けられている場合は、運用途中のワークフローがあると判断する。この場合は、パスワード管理部111は、現在処理しようとしているワークフローに関るグループ化されたデバイス群において、すでにパスワード入力があったと判断し、パスワード入力を促さない。

【００６１】

ステップ209では、パスワード管理部111は、第１のデバイス101に対して、パスワード入力要求情報ではなく、パスワード入力を要求せずにそのままデバイス処理を行うように指示する情報を送信する。第１のデバイス101は、該情報を受信すると、所定のデバイス処理（画像取り込みやスキャンなど）を行う。

【００６２】

以上のように、ステップ206での判断に応じて、＜運用途中のワークフローが存在しない場合＞および＜運用途中のワークフローが存在する場合＞のいずれか一方の処理を行う。

【００６３】

次いで、ステップ211では、デバイスグループ管理部114は、運用途中確認テーブルの、未操作デバイスから、今回操作したデバイスを削除する。本例では、今回操作したデバイスは、デバイスID　Dev011にて特定される第１のデバイス101であるので、図７に示すように、未操作デバイスの欄には、Dev012,Dev021が残ることになる。

【００６４】

ステップ211では、デバイスグループ管理部114は、運用途中確認テーブルの、今回処理を行っているワークフローIDに関連付けられた未操作デバイスの欄に、デバイスIDがあるか否かを判断する。デバイスIDがある場合は、未操作デバイスがあると判断し、ステップ214に進む。一方、デバイスIDが無い場合は、該当するワークフローの処理に関するデバイスを全て使用したと判断し、ステップ213にて、デバイスグループ管理部214は、該当するワークフローを運用途中確認テーブルから削除する。

【００６５】

ステップ214では、第1のデバイス101は、ログアウトを行い、ステップ202に進み、待機状態に入る。

【００６６】

（第２の実施形態）

第１の実施形態に記載のパスワード要否制御はデバイス操作に順序性がない説明であったが、順序性を伴うケースも想定される。図２、図５、図６、図８を用いて、本実施形態に係る、デバイス操作の順序を考慮したパスワード要否制御について説明する。

【００６７】
本実施形態において、符号501は符号301と同等であり、符号502は符号302と同等であり、符号601は符号401と同等である。符号602は符号302と基本的には同等である。デバイスID602において、一番目に操作するデバイスは“Dev011”、二番目に操作するデバイスは“Dev012”または“Dev013”、三番目に操作するデバイスは“Dev021”または“Dev022”である、ことを意味する。このように、本実施形態では、あるワークフロー処理において用いるデバイスの順番も関連付けて管理（順序付けて管理）されている。
【００６８】
図８は、図７のような、運用途中確認テーブルを示す図であるが、未操作デバイスの欄においては、上記処理の順番も反映して管理されている。符号801は、ワークフローを運用しているユーザを識別するためのICカード番号である。符号802は、運用中のワークフローを識別するためのワークフローIDである。符号803は、ワークフローが完了するまでに操作されるデバイス（未操作デバイス）である。ここにリストされていることは即ち運用途中のワークフローが存在することを意味する。符号801は符号701と同等であり、符号802は符号702と同等である。符号803は、一番目に操作するデバイスは“Dev012”または“Dev013”、二番目に操作するデバイスは“Dev021”または“Dev022”、であることを意味する。
【００６９】
本実施形態において、ステップ201～214の処理は第１の実施形態に記載の各ステップと一部を除いて同等である。以下で、第１の実施形態と異なるステップについて説明する。
【００７０】
ステップ204において、パスワード管理部112は、ワークフローを検索する際、運用途中のワークフローが存在しない場合は、デバイスID602の先頭に、ステップ203にて受信したデバイスIDを含むか否かを判定する。また、運用途中のワークフローが存在する場合についても、デバイスID803の先頭に、ステップ203にて受信したデバイスIDを含むか否かを判定する。それぞれの判定において含まれれば運用可能なワークフローの候補とする。含まれていない場合は、ステップ205にて、パスワード管理部112は、ワークフローは検索されなかったと判断し、ステップ210に進む。
【００７１】
（第３の実施形態）
図７、図９、図１０を用いて、本実施形態に係る、操作するデバイスが複数のワークフローに関連する際のユーザインタフェース（UI）について説明する。図９において、符号903はデバイス上のUI（例えば、第１のデバイス、第２のデバイスの表示部に表示されるUI）、符号901は、ワークフロー名称であり、符号902は、パスワード入力が必要か否かを表すステータスである。図１０は、図９の画面操作の後、図７に示すテーブルが変化した後のテーブルを示す図である。
【００７２】
図３、図４の例示、および図７の例示を前提とし、“Dev021”という識別子のデバイスを操作したとする。すると図２の制御にしたがい、ワークフローID“W001”と“W002”とが検索される。ここで、“W001”に対しては「パスワード入力不要」、“W002”に対しては「パスワード入力が必要」であるとし、“W001”がワークフロー名称901の“カタログ画像登録”、“W002”がのワークフロー名称901の“PC購買発注”とする。ステータス902の文言がパスワード要否の状況を表している。ユーザは所望のワークフローを選択する。“PC購買発注”を選択した場合、図７のリストに“W002”が追加される（図１０）。
【００７３】
図９に示すUIは、ステップ203にてICカードの読み取りが終了した直後に、該当するデバイスが入力表示部に上記UIを表示し、ユーザに選択させるようにすれば良い。該選択によって、認証サーバ111は、パスワード入力が必要か否かの判断を行うことができる。
【００７４】
（その他の実施形態）

本発明は、複数の機器（例えばコンピュータ、インターフェース機器、リーダ、プリンタなど）から構成されるシステムに適用することも、１つの機器からなる装置（複合機、プリンタ、ファクシミリ装置など）に適用することも可能である。

【００７５】

前述した実施形態の機能を実現するように前述した実施形態の構成を動作させるプログラムを記憶媒体に記憶させ、該記憶媒体に記憶されたプログラムをコードとして読み出し、コンピュータにおいて実行する処理方法も上述の実施形態の範疇に含まれる。即ちコンピュータ読み取り可能な記憶媒体も実施例の範囲に含まれる。また、前述のコンピュータプログラムが記憶された記憶媒体はもちろんそのコンピュータプログラム自体も上述の実施形態に含まれる。

【００７６】

かかる記憶媒体としてはたとえばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性メモリカード、ＲＯＭを用いることができる。

【００７７】

また前述の記憶媒体に記憶されたプログラム単体で処理を実行しているものに限らず、他のソフトウエア、拡張ボードの機能と共同して、ＯＳ上で動作し前述の実施形態の動作を実行するものも前述した実施形態の範疇に含まれる。

【００７８】

以上の各実施例の説明から、シングルサインオンと各実施例とが異なることが明らかにわかる。

【００７９】

シングルサインオン（Single Sign-0n）では、上述のように、一つの操作部は、通常、唯一無二のユーザによって独占排他的に用いられることが多いという前提に立っている。この前提のもと、ある装置の操作部において１回のユーザ認証が行われると、その操作部を用いて操作をする唯一無二のユーザは信頼できる人であるという仮定が成立し、従って、その後のアクセスは、ユーザ認証を必要としない。

【００８０】

しかし、別の装置の操作部から別の装置が利用される場合には、もう一度パスワード入力等のユーザ認証を行う必要がある。なぜなら、別の装置を別の操作部から利用するユーザは、既にユーザ認証が済んだユーザとは異なる蓋然性が高いからである。

【００８１】

一方、各実施例では、一回のユーザ認証が行われると、別の装置の操作部から別の装置が利用される場合にも、再度のユーザ認証を必要としない。この実施例の前提は、例えば、あるＩＣカードが唯一無二のユーザによって所持されているという仮定がある。そして、そのあるＩＣカードを持っているユーザによりユーザ認証が行われると、（そのＩＣカードを落としてしまうということが無い限り）、そのＩＣカードは信頼できるユーザに持たれているという仮定が成立する。従って、その後のアクセスは、ユーザ認証を必要としないのである。

【図面の簡単な説明】

【００８２】

【図１】本発明の一実施形態に係る情報処理システムの構成を示す図である。

【図２】本発明の一実子形態に係るパスワード要否の制御を説明するフローチャートである。

【図３】本発明の一実施形態に係るワークフローとデバイス群識別子とを関係付けるテーブルを示す図である。

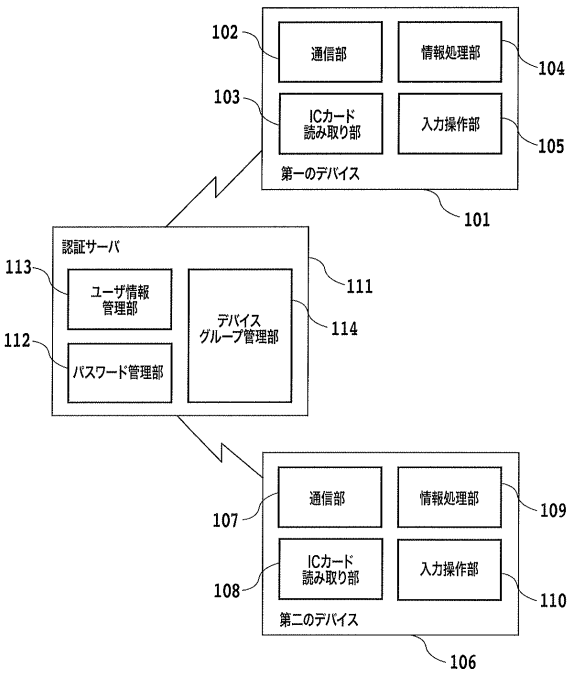
【図４】本発明の一実施形態に係る装置群識別子と装置とを関係付けるテーブルを示す図である。

【図５】本発明の一実施形態に係る、ワークフローと装置群識別子を関係付けるテーブル（順序性あり）を示す図である。

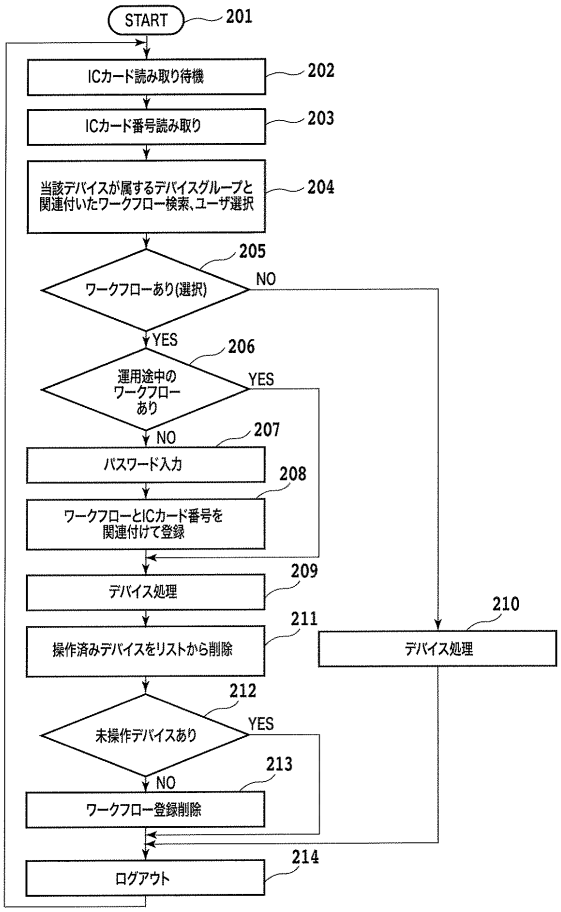
【図６】本発明の一実施形態に係る、装置群識別子と装置を関係付けるテーブル（順序性あり）を示す図である。
【図７】本発明の一実施形態に係る、運用途中のワークフローのリストを示す図である。
【図８】本発明の一実施形態に係る、運用途中のワークフローのリスト（順序性あり）を示す図である。
【図９】本発明の一実施形態に係る、ワークフローを選択するUIを示す図である。
【図１０】本発明の一実施形態に係る、運用途中のワークフローのリストを示す図である。

【符号の説明】
【００８３】
１０１、１０６　　第１のデバイス
１０２、１０７　　通信部
１０３、１０８　　ＩＣカード読取部
１０４、１０９　　情報処理部
１０５、１１０　　入力操作部
１１１　　認証サーバ
１１２　　パスワード管理部
１１３　　ユーザ情報管理部
１１４　　デバイスグループ管理部

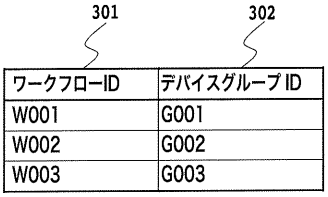
【図１】



【図２】

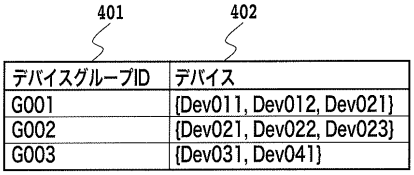


【図３】



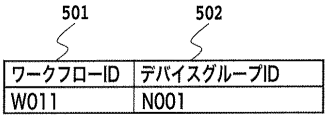
301	302
ワークフローID	デバイスグループ ID
W001	G001
W002	G002
W003	G003

【図４】



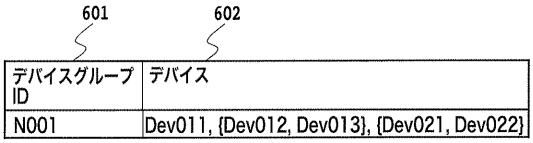
401	402
デバイスグループID	デバイス
G001	{Dev011, Dev012, Dev021}
G002	{Dev021, Dev022, Dev023}
G003	{Dev031, Dev041}

【図５】



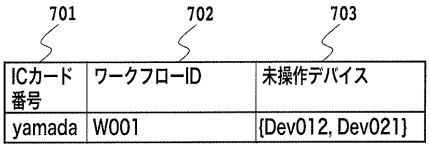
501	502
ワークフローID	デバイスグループID
W011	N001

【図６】



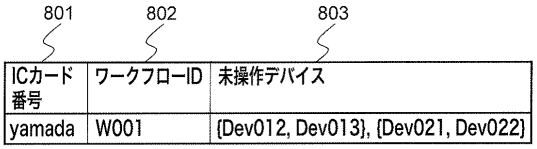
601	602
デバイスグループ ID	デバイス
N001	Dev011, {Dev012, Dev013}, {Dev021, Dev022}

【図７】



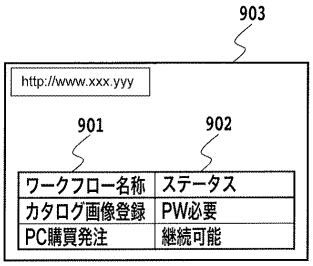
701	702	703
ICカード番号	ワークフローID	未操作デバイス
yamada	W001	{Dev012, Dev021}

【図８】

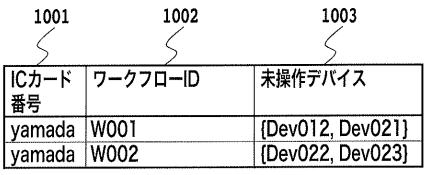


801	802	803
ICカード番号	ワークフローID	未操作デバイス
yamada	W001	{Dev012, Dev013}, {Dev021, Dev022}

【図９】



【図１０】



1001	1002	1003
ICカード番号	ワークフローID	未操作デバイス
yamada	W001	{Dev012, Dev021}
yamada	W002	{Dev022, Dev023}

フロントページの続き

審査官　鳥居　稔

(56)参考文献　特開２００６－１３４３０１（ＪＰ，Ａ）
特開２００７－１２５７７７（ＪＰ，Ａ）
特開平０９－２５９２３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２４
Ｇ０６Ｆ　１５／００