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

特許第5759243号
(P5759243)

(45)発行日　平成27年8月5日(2015.8.5)　(24)登録日　平成27年6月12日(2015.6.12)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/32	(2013.01)	G06F	21/32	
G06F 21/34	(2013.01)	G06F	21/34	
H04L 9/32	(2006.01)	H04L	9/00	673A
G06T 7/00	(2006.01)	G06T	7/00	530

請求項の数 14　(全 19 頁)　最終頁に続く

(21)出願番号　特願2011-94369(P2011-94369)
(22)出願日　平成23年4月20日(2011.4.20)
(65)公開番号　特開2012-226606(P2012-226606A)
(43)公開日　平成24年11月15日(2012.11.15)
審査請求日　平成26年4月18日(2014.4.18)

(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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】情報処理システム、画像処理装置、情報処理装置、それらの制御方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
画像処理装置と、情報処理装置とを含む情報処理システムであって、
前記画像処理装置は、
ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求手段と、
前記画面情報取得要求の応答として前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御手段と
を備え、
前記情報処理装置は、
前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を生成する画面情報生成手段と、
前記画面情報生成手段によって生成された画面情報を、前記要求手段によって通知される画面情報取得要求の応答として前記画像処理装置に通知する画面情報通知手段と
を備え、
前記要求手段は、前記表示制御手段によって前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知し、
前記表示制御手段は、前記通知した新たな画面情報取得要求に従って前記画面情報生成手段によって生成された画面情報に従って表示している認証画面を更新することを特徴と

する情報処理システム。
【請求項２】
前記画像処理装置は、
前記表示制御手段によって表示された前記認証画面に従ってユーザによって入力された、該ユーザの情報を示す認証情報を受け付ける受付手段と
前記受付手段によって受け付けられた前記認証情報を前記情報処理装置に通知する認証情報通知手段と
をさらに備え、
前記情報処理装置は、
前記認証情報通知手段によって通知された前記認証情報と、前記情報処理装置の記憶手段に予め記憶されている情報とを用いて当該ユーザの認証を実行する認証手段と、
前記認証手段による認証結果を前記画像処理装置に通知する認証結果通知手段と
をさらに備え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】
前記認証画面は、前記画像処理装置に接続された認証機器が複数存在する場合、前記複数の認証機器のうち１つの認証機器に対応する認証画面であって、かつ、他の認証機器に対応する認証画面へ遷移するためのボタンを含む認証画面であることを特徴とする請求項１又は２に記載の情報処理システム。
【請求項４】
前記認証画面は、前記画像処理装置に接続された認証機器が複数存在する場合、前記複数の認証機器のそれぞれに対応する複数の認証画面がタブ形式で表示される画面であることを特徴とする請求項１又は２に記載の情報処理システム。
【請求項５】
前記画像処理装置に接続されている認証機器を示す認証機器情報を当該認証機器から取得する取得手段をさらに備え、
前記要求手段は、前記取得手段によって取得された認証機器情報を含む前記画面情報取得要求を生成して、前記情報処理装置に通知することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理システム。
【請求項６】
前記認証機器は、キー入力によって認証情報を取得する操作部、ＩＤカードから認証情報を取得するカード認証機器、及び指紋から認証情報を取得する指紋認証機器の少なくとも１つであることを特徴とする請求項１乃至５の何れか１項に記載の情報処理システム。
【請求項７】
情報処理装置と通信可能な画像処理装置であって、
ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求手段と、
前記画面情報取得要求の応答として前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御手段と
を備え、
前記要求手段は、前記表示制御手段によって前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知し、
前記表示制御手段は、前記通知した新たな画面情報取得要求に従って前記情報処理装置から通知される画面情報に従って表示している認証画面を更新することを特徴とする画像処理装置。
【請求項８】
画像処理装置と通信可能な情報処理装置であって、
前記画像処理装置から、ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を受信する受信手段と、
前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を

生成する画面情報生成手段と、
前記画面情報生成手段によって生成された画面情報を、前記画面情報取得要求の応答として前記画像処理装置に通知する画面情報通知手段と
を備え、
前記受信手段は、前記画像処理装置で前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を該画像処理装置から受信し、
前記画面情報生成手段は、前記受信した新たな画面情報取得要求に従って、前記画像処理装置で表示されている前記認証画面を更新するための新たな画面情報を生成し、
前記画面情報通知手段は、生成した前記新たな画面情報を前記画像処理装置に通知することを特徴とする情報処理装置。
【請求項９】
画像処理装置と、情報処理装置とを含む情報処理システムの制御方法であって、
前記画像処理装置において、
ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求ステップと、
前記画面情報取得要求の応答として、前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御ステップと
を実行し、
前記情報処理装置において、
前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を生成する画面情報生成ステップと、
前記画面情報生成ステップにおいて生成された画面情報を、前記画面情報取得要求の応答として前記画像処理装置に通知する画面情報通知ステップと
を実行し、
前記画像処理装置において、さらに、
前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知するステップと、
前記通知した新たな画面情報取得要求に従って前記情報処理装置で生成された画面情報に従って表示している認証画面を更新するステップとを実行することを特徴とする情報処理システムの制御方法。
【請求項１０】
情報処理装置と通信可能な画像処理装置の制御方法であって、
ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求ステップと、
前記画面情報取得要求の応答として、前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御ステップと
を実行し、
さらに、
前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知するステップと、
前記通知した新たな画面情報取得要求に従って前記情報処理装置で生成された画面情報に従って表示している認証画面を更新するステップとを実行することを特徴とする画像処理装置の制御方法。
【請求項１１】
画像処理装置と通信可能な情報処理装置の制御方法であって、
前記画像処理装置から、ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を受信する受信ステップと、

前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を生成する画面情報生成ステップと、
前記画面情報生成ステップにおいて生成された画面情報を、前記画面情報取得要求の応答として前記画像処理装置に通知する画面情報通知ステップと
を実行し、
さらに、
前記画像処理装置で前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を該画像処理装置から受信するステップと、
前記受信した新たな画面情報取得要求に従って、前記画像処理装置で表示されている前記認証画面を更新するための新たな画面情報を生成するステップと、
生成した前記新たな画面情報を前記画像処理装置に通知するステップとを実行することを特徴とする情報処理装置の制御方法。
【請求項１２】
請求項９に記載の情報処理システムの制御方法における各ステップをコンピュータに実行させるためのプログラム。
【請求項１３】
請求項１０に記載の画像処理装置の制御方法における各ステップをコンピュータに実行させるためのプログラム。
【請求項１４】
請求項１１に記載の情報処理装置の制御方法における各ステップをコンピュータに実行させるためのプログラム。
【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、画像処理装置、情報処理装置、それらの制御方法及びプログラムに関するものである。
【背景技術】
【０００２】
ＷＷＷ(World Wide Web)のコンテンツを閲覧するためのＷｅｂブラウザは、コンテンツとともに、コンテンツのＵＲＬ(uniform resource locator)やファイルのパス名などのリソースの格納位置が識別できる情報をアドレスバーなどの表示領域に表示する。近年、画像処理装置の高機能化に伴い、同装置に上記のようなＷｅｂブラウザが搭載され、ユーザは画像処理装置上からネットワークに接続することが可能となった。また、特許文献１には、画像処理装置が備える各機能を利用するための指示を入力する操作画面を、Ｗｅｂサーバが提供することが提案されている。
【０００３】
このような技術を応用して、画像処理装置におけるユーザ認証処理及び認証画面の提供をＷｅｂサーバが行い、認証画面を画像処理装置のＷｅｂブラウザに描画することで、認証操作をＷｅｂ化する技術が考えられる。これによって、認証に関わるリソースを画像処理装置内に保持する必要がなくなり、認証管理もＷｅｂサーバ上で容易に行うことが可能となる。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００５－２４２９９４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来技術には以下に記載する問題がある。ここで、画像処理装置の認証

方法が１つではなく、カードによる認証、キー入力による認証、指紋による認証等、複数の認証方法が存在する場合を考える。その場合、Ｗｅｂアプリケーションは各認証方法についての画面情報を作成する必要がある。そして、例え画像処理装置に１つの認証機器しか接続されていない場合でも、Ｗｅｂアプリケーションは画像処理装置にどの認証機器が接続されているか把握できないため、すべての認証機器に対応した画面を提供しなくてはならない。これによって、ユーザは接続されていない認証機器の認証情報を含んだ画面が表示されるため、画像処理装置の認証操作に手間取ってしまう可能性がある。

【０００６】

このような問題に対して、特許文献１には、画像処理装置が提供するサービスに関わる情報の１つであるＵＲＬ（サービスへの接続情報）を、画像処理装置からＷｅｂサーバに通知することが提案されている。しかし、特許文献１は、画像処理装置の情報を常にＷｅｂサーバに通知してしまう。これによって、送信データ量が増加するだけでなく、機密性の高い情報が漏えいしてしまう危険性もある。また、ユーザがログイン後、Ｗｅｂブラウザを使ってＷｅｂアプリケーションのログイン画面を再び開いてしまうことも考えられ、複数回ログインを招く可能性もある。

【０００７】

本発明は、上述の問題に鑑みて成されたものであり、画像処理装置に接続されている認証機器に適した認証画面をユーザに提供する情報処理システム、画像処理装置、情報処理装置、それらの制御方法及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【０００８】

本発明は、画像処理装置と、情報処理装置とを含む情報処理システムであって、前記画像処理装置は、ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求手段と、前記画面情報取得要求の応答として前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御手段とを備え、前記情報処理装置は、前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を生成する画面情報生成手段と、前記画面情報生成手段によって生成された画面情報を、前記要求手段によって通知される画面情報取得要求の応答として前記画像処理装置に通知する画面情報通知手段とを備え、前記要求手段は、前記表示制御手段によって前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知し、前記表示制御手段は、前記通知した新たな画面情報取得要求に従って前記画面情報生成手段によって生成された画面情報に従って表示している認証画面を更新することを特徴とする。

【０００９】

また、本発明は、情報処理装置と通信可能な画像処理装置であって、ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を生成して、前記情報処理装置に通知する要求手段と、前記画面情報取得要求の応答として前記情報処理装置から通知される画面情報を用いて認証画面を表示部に表示する表示制御手段とを備え、前記要求手段は、前記表示制御手段によって前記表示部に前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を生成して、前記情報処理装置に通知し、前記表示制御手段は、前記通知した新たな画面情報取得要求に従って前記情報処理装置から通知される画面情報に従って表示している認証画面を更新することを特徴とする。

【００１０】

また、本発明は、画像処理装置と通信可能な情報処理装置であって、前記画像処理装置から、ユーザを認証するための認証機器を示す認証機器情報を含む画面情報取得要求を受信する受信手段と、前記認証機器情報が示す認証機器を用いた認証を実行するための認証画面の画面情報を生成する画面情報生成手段と、前記画面情報生成手段によって生成された画面情報を、前記画面情報取得要求の応答として前記画像処理装置に通知する画面情報

通知手段とを備え、前記受信手段は、前記画像処理装置で前記認証画面が表示されている間に、新たな認証機器が前記画像処理装置へ接続されると、最新の状態を示す前記認証機器情報を含む新たな画面情報取得要求を該画像処理装置から受信し、前記画面情報生成手段は、前記受信した新たな画面情報取得要求に従って、前記画像処理装置で表示されている前記認証画面を更新するための新たな画面情報を生成し、前記画面情報通知手段は、生成した前記新たな画面情報を前記画像処理装置に通知することを特徴とする。

【発明の効果】

【００１１】

本発明は、画像処理装置に接続されている認証機器に適した認証画面をユーザに提供する情報処理システム、画像処理装置、情報処理装置、それらの制御方法及びプログラムを提供できる。

【図面の簡単な説明】

【００１２】

【図１】第１の実施形態における情報処理システムの構成例を示す図である。

【図２】第１の実施形態におけるＭＦＰ１０１の構成例を示すブロック図である。

【図３】第１の実施形態におけるＷｅｂサーバ１０２の構成例を示すブロック図である。

【図４】第１の実施形態における情報処理システムのソフトウェア構成例を示す図である。

【図５】第１の実施形態における認証画面の一例を示す図である。

【図６】第１の実施形態における認証画面の一例を示す図である。

【図７】第１の実施形態におけるエラー画面の一例を示す図である。

【図８】第１の実施形態における情報処理システムの一連の処理を示すシーケンス図である。

【図９】第１の実施形態におけるＷｅｂアプリケーション４１０のキー認証画面作成処理を示すフローチャートである。

【図１０】第１の実施形態におけるＷｅｂアプリケーション４１０のカード認証画面作成処理を示すフローチャートである。

【図１１】第１の実施形態におけるＷｅｂアプリケーション４１０の指紋画面作成処理を示すフローチャートである。

【図１２】第１の実施形態におけるＷｅｂアプリケーション４１０の認証操作の動作を示すフローチャートである。

【図１３】第２の実施形態におけるＷｅｂアプリケーション４１０の認証画面作成処理を示すフローチャートである。

【図１４】第１の実施形態におけるＵＳＢ認証機器の抜き差しが起こったときの情報処理システムの一連の処理を示すシーケンス図である。

【発明を実施するための形態】

【００１３】

以下、本発明を実施するための形態について図面を用いて説明する。尚、以下の実施形態は特許請求の範囲に係る発明を限定するものでなく、また実施形態で説明されている特徴の組み合わせの全てが発明の解決手段に必須のものとは限らない。

【００１４】

＜第１の実施形態＞

＜情報処理システムの構成＞

まず、図１を参照して、本発明の第１の実施形態における情報処理システムの構成について説明する。ＬＡＮ１１０にはＭＦＰ１０１及びＷｅｂサーバ１０２が互いに通信可能に接続されている。なお、ＬＡＮ１１０は説明のためＬＡＮ（ローカル・エリア・ネットワーク）と記載しているが、インターネットなどの他のネットワークでもよい。

【００１５】

＜画像処理装置の構成＞

次に、図２を参照して、画像処理装置であるＭＦＰ１０１の構成について説明する。Ｍ

ＦＰ１０１は、制御部２１０、操作部２１９、プリンタ２２０、及びスキャナ２２１を備える。また、制御部２１０は、ＣＰＵ２１１、ＲＯＭ２１２、ＲＡＭ２１３、ＨＤＤ２１４、操作部Ｉ／Ｆ２１５、プリンタＩ／Ｆ２１６、スキャナＩ／Ｆ２１７、及びネットワークＩ／Ｆ２１８を備える。ＣＰＵ２１１を含む制御部２１０は、ＭＦＰ１０１全体の動作を統括的に制御する。ＣＰＵ２１１は、ＲＯＭ２１２に記憶された制御プログラムを読み出して読取制御や送信制御などの各種制御を行う。ＲＡＭ２１３は、ＣＰＵ２１１の主メモリ、ワークエリア等の一時記憶領域として用いられる。

【００１６】

ＨＤＤ２１４は、画像データや各種プログラム、或いは各種情報テーブルを記憶する。操作部Ｉ／Ｆ２１５は、操作部２１９と制御部２１０と接続する。操作部２１９には、タッチパネル機能を有する液晶表示部やキーボードなどが備えられ、ユーザからの入力を受け付ける。即ち、操作部２１９は、受付手段として機能する。また、ＭＦＰ１０１には後述するＷｅｂブラウザ４３０が備えられる。ＭＦＰ１０１のＷｅｂブラウザ４３０は、表示制御手段として機能し、Ｗｅｂサーバ１０２から受信したＨＴＭＬファイルを解析し、受信したＨＴＭＬファイルの記述に基づく操作画面を操作部２１９の液晶表示部に表示する。ここで、ＭＦＰ１０１のＷｅｂブラウザ４３０が受信するＨＴＭＬファイル（画面情報）は必ずしもＷｅｂサーバ１０２から受信したものでなくてもよい。即ち、後述のＭＦＰ１０１内部のサーブレットアプリケーションから受信したＨＴＭＬファイルでもよい。

【００１７】

プリンタＩ／Ｆ２１６は、プリンタ２２０と制御部２１０とを接続する。プリンタ２２０で印刷すべき画像データは、プリンタＩ／Ｆ２１６を介して制御部２１０から転送され、プリンタ２２０において記憶媒体上に印刷される。スキャナＩ／Ｆ２１７は、スキャナ２２１と制御部２１０とを接続する。スキャナ２２１は、原稿上の画像を読み取って画像データを生成し、スキャナＩ／Ｆ２１７を介して制御部２１０に画像データを入力する。ネットワークＩ／Ｆ２１８は、制御部２１０（ＭＦＰ１０１）をＬＡＮ１１０に接続する。ネットワークＩ／Ｆ２１８は、ＬＡＮ１１０上の外部装置（例えば、Ｗｅｂサーバ１０２）に画像データや情報を送信したり、ＬＡＮ１１０上の外部装置から各種情報を受信したりする。

【００１８】

＜Ｗｅｂサーバの構成＞

次に、図３を参照して、情報処理システムに含まれるＷｅｂサーバ１０２の構成について説明する。Ｗｅｂサーバ１０２は、制御部３１０を備える。また、制御部３１０は、ＣＰＵ３１１、ＲＯＭ３１２、ＲＡＭ３１３、ＨＤＤ３１４及びネットワークＩ／Ｆ３１５を備える。ＣＰＵ３１１を含む制御部３１０は、Ｗｅｂサーバ１０２全体の動作を統括的に制御する。ＣＰＵ３１１は、ＲＯＭ３１２に記憶された制御プログラムを読み出して各種制御処理を実行する。ＲＡＭ３１３は、ＣＰＵ３１１の主メモリ、ワークエリア等の一時記憶領域として用いられる。ＨＤＤ３１４は、画像データや各種プログラム、或いは各種情報テーブルを記憶する。ネットワークＩ／Ｆ３１５は、制御部３１０（Ｗｅｂサーバ１０２）をＬＡＮ１１０に接続する。ネットワークＩ／Ｆ３１５は、ＬＡＮ１１０上の他の装置との間で各種情報を送受信する。

【００１９】

＜情報処理システムのソフトウェア構成＞

次に、図４を参照して、情報処理システム全体のソフトウェア構成について説明する。図４に示す各機能部（ソフトウェア）は、ＭＦＰ１０１／Ｗｅｂサーバ１０２のそれぞれに備えられているＣＰＵが制御プログラムを実行することにより実現される。ＭＦＰ１０１は、Ｗｅｂブラウザ４３０、ログインアプリケーション部４４０、アクセス制御情報記憶部４５０、プリファレンス情報記憶部４６０、及びログインフレームワーク４７０を備える。また、ＵＳＢ（Universal Serial Bus：ユニバーサル・シリアル・バス）認証機器４８０と接続されている。

【００２０】

Ｗｅｂブラウザ４３０は、通信部４３１、解析部４３２、及び画面表示部４３３を含む。通信部４３１は、ＨＴＴＰプロトコルに従ってＷｅｂアプリケーション４１０のプレゼンテーション部４１１と通信する。より具体的には、通信部４３１は、ＵＲＩによって特定されるＷｅｂサーバ１０２のＷｅｂアプリケーション４１０のリソースに対してＧＥＴまたはＰＯＳＴのＨＴＴＰ要求を送信する。つまり、指定されたＵＲＩをアクセス先としてＷｅｂブラウザ４３０がアクセスを行う。そして、ＨＴＴＰ要求に対するＨＴＴＰ応答として、Ｗｅｂブラウザ４３０で表示するＨＴＭＬ等で記述された操作画面をＷｅｂアプリケーション４１０から取得する。また、Ｗｅｂブラウザ４３０で表示したＨＴＭＬフォーム等に入力されたユーザからの指示を、ＨＴＴＰ要求によってＷｅｂアプリケーション４１０に通知する。

【００２１】

解析部４３２は、Ｗｅｂアプリケーション４１０から受信するＨＴＭＬファイル（画面情報）を解析する。このＨＴＭＬファイルには、Ｗｅｂブラウザに表示すべき操作画面の内容を示す記述が含まれている。画面表示部４３３は、解析部４３２による解析の結果に基づいて、操作部２１９上に操作画面を表示する。このように、Ｗｅｂサーバ１０２から受信した画面情報（ＨＴＭＬファイル）に基づいて表示される画面をＷｅｂブラウザ画面と称する。

【００２２】

ログインアプリケーション部４４０は、ＵＳＢ認証機器情報取得部４４１、ＨＴＴＰリクエスト生成部４４２、及びログインコンテキスト生成部４４３を含む。ＵＳＢ認証機器情報取得部４４１は、ＭＦＰ１０１に接続されているＵＳＢ認証機器４８０を検知し、その情報を取得する。また、ＵＳＢ認証機器４８０の接続を新しく検知したり、接続が絶たれたことを検知した場合、ＵＳＢ認証機器情報をリクエスト生成部４４２に送信する。リクエスト生成部４４２は、Ｗｅｂブラウザ４３０がＷｅｂアプリケーション４１０と通信を行うために必要なＨＴＴＰリクエストを生成する。さらに、リクエスト生成部４４２は、ＵＳＢ認証機器情報取得部４４１からＵＳＢ認証機器情報を受け取り、それをＨＴＴＰリクエストヘッダに追記したうえで、Ｗｅｂブラウザ４３０の通信部４３１にＨＴＴＰリクエストをＰＯＳＴさせる。ログインコンテキスト生成部４４３は、Ｗｅｂアプリケーション４１０のログイン通知部４１３から通知されたログインユーザに関するセッション情報を生成する。ＭＦＰ１０１の各種機能は、そのセッション情報に応じて動作がパーソナライズされる。即ち、プリファレンス情報記憶部４６０の内容に応じてユーザが好む動作パラメータを優先する。また、アクセス制御情報記憶部４５０内に記憶された、ユーザに付与された権限に応じて、動作を禁止したり、続行したりする。

【００２３】

アクセス制御情報記憶部４５０は、ＭＦＰ１０１を使用する複数のユーザのそれぞれについて、ＭＦＰ１０１が提供する各種機能や資源に対する、実行や読み出し、書き込み等のアクセスを制御するためのアクセス制御情報を記憶する。アクセス制御情報とは、カラー処理を禁止し白黒処理を許可する、片面印字を禁止し図面プリントを許可する、文書の送信を禁止しコピーを許可する、管理者用設定パラメータの変更を禁止し一般ユーザ用設定パラメータの変更を許可する、等の情報である。アクセス制御情報は、システム管理者がアクセス制御情報記憶部４５０に予め設定できる。また、外部サーバに記憶管理されているアクセス・コントロール・リスト（ＡＣＬ）等をネットワーク経由で利用するように構成することもできる。

【００２４】

プリファレンス情報記憶部４６０は、ＭＦＰ１０１を使用する複数のユーザのそれぞれについて、ＭＦＰ１０１の動作に関する各種の好みを示すプリファレンス情報を記憶する。例えば、プリファレンス情報とは、カラーよりも白黒の処理を好む、用紙サイズはＡ４よりもレターサイズを好む、読み取り画像のプレビューを確認してから送信するよりも確認ステップを省き短手番で送信することを好む、等の情報である。プリファレンス情報は、ユーザや管理者がプリファレンス情報記憶部４６０に予め設定できる。また、ユーザに

よる過去の操作履歴から好みを自動判定しプリファレンス情報記憶部４６０に自動設定することもできる。ログインフレームワーク４７０は、ログインアプリケーション部４４０を管理し、ログイン要求をログインアプリケーション部４４０に対して行う。

【００２５】

ＵＳＢ認証機器４８０は、ＭＦＰ１０１と接続されており、カード認証機器４８１及び指紋認証機器４８２を含む。カード認証機器４８１はユーザからＩＤカードによる入力を受け付け、カードに含まれる認証情報をＵＳＢ認証機器情報取得部４４１に伝える。指紋認証機器４８２は、ユーザの指紋情報を受け付け、それをＵＳＢ認証機器情報取得部４４１に伝える。

【００２６】

Ｗｅｂサーバ１０２は、Ｗｅｂアプリケーション４１０及び認証情報記憶部４２０を含む。さらに、Ｗｅｂアプリケーション４１０は、プレゼンテーション部４１１、認証処理部４１２、及びログイン通知部４１３を含む。プレゼンテーション部４１１は、通信部４３１と通信し、ＭＦＰ１０１からの要求に応じて、ＭＦＰ１０１のＷｅｂブラウザ４３０で表示すべき操作画面をＭＦＰ１０１に送信する。また、ＭＦＰ１０１のＷｅｂブラウザ４３０に表示された操作画面を介して入力されたユーザからの指示をＭＦＰ１０１からＨＴＴＰ要求として受け取る。この際、プレゼンテーション部４１１は、通信部４３１からのＨＴＴＰリクエストヘッダを解析する。解析した結果、ＵＳＢ認証機器情報がリクエストヘッダに含まれていた場合は、プレゼンテーション部４１１は、ＵＳＢ認証機器４８０に対応した認証画面を通信部４３１に送信する。例えば、リクエストヘッダにカード認証機器情報が含まれていた場合はカード認証画面を、指紋認証機器情報が含まれていた場合は指紋認証画面をそれぞれ送信する。また、Ｗｅｂブラウザ４３０に表示されている認証画面を通じて、認証情報が通信部４３１から送信された場合は、認証処理部４１２に認証情報を送信して、認証処理を行わせる。即ち、プレゼンテーション部４１１は、ＭＦＰ１０１からのログイン要求に応答して認証画面の画面情報を生成する画面情報生成手段と、当該画面情報をＭＦＰ１０１に通知する画面情報通知手段として機能する。

【００２７】

認証処理部４１２は、プレゼンテーション部４１１から受け取った認証情報と、認証情報記憶部４２０の情報を照らし合わせることで認証を行う。ここで、認証情報記憶部４２０には、予め登録されたユーザ名と対応するパスワードが記憶されている。照らし合わせた結果、プレゼンテーション部４１１から受け取った認証情報が正しいものであれば、ログイン通知部４１３にログインが成功したことを伝えさせる。一方、認証情報が間違ったものであれば、プレゼンテーション部４１１にログインエラーの表示を行わせる。ログイン通知部４１３は、認証処理部４１２の認証照合の結果、ユーザがＷｅｂブラウザ４３０で入力した認証情報が認証情報記憶部４２０に存在した場合、ログインアプリケーション部４４０に、ログインが成功したことを通知する。これにより、ユーザのＭＦＰ１０１の使用が許可される。即ち、認証処理部４１２は、ＭＦＰ１０１から通知される認証情報と、認証情報記憶部４２０に予め記憶されている情報とを用いて当該ユーザの認証を実行する認証手段と、認証結果をＭＦＰ１０１へ通知する認証結果通知手段として機能する。

【００２８】

＜画面例＞

次に、図５乃至図７を参照して、Ｗｅｂブラウザ４３０が表示する画面について説明する。図５の５００は、Ｗｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼンテーション部４１１と通信を行って、キー認証画面を描画したＷｅｂブラウザ４３０の外観である。５０１はＷｅｂブラウザ４３０のコンテンツ表示領域である。この領域にＷｅｂサーバ１０２から受信したレスポンスに基づいてコンテンツを表示する。キー認証画面５００では、当該画面の画面情報をプレゼンテーション部４１１が送信し、通信部４３１が受信した後、解析部４３２が解析し、その後画面表示部４３３がコンテンツ表示領域５０１上に描画している。

【００２９】

５０２はツールバーである。ツールバーには、表示コンテンツに対する制御やＷｅｂブラウザに対する制御を実施するための操作ボタンを表示している。選択されると、対応する機能が実行される。５０３はカード認証画面６００への切り替えを行うボタンである。ボタン５０３は、Ｗｅｂブラウザ４３０の通信部４３１から、Ｗｅｂアプリケーション４１０のプレゼンテーション部４１１に送信したＨＴＴＰリクエストヘッダ内に、カード認証機器の情報が含まれている場合のみ表示される。５０４は指紋認証画面７００への切り替えを行うボタンである。ボタン５０４もカード認証ボタン切り替えボタン５０３同様、プレゼンテーション部４１１が受信したＨＴＴＰリクエストヘッダ内に、指紋認証機器の情報が含まれている場合のみ表示される。

【００３０】

５０５は、キー認証におけるユーザ名入力フィールドである。ＭＦＰ１０１のユーザはこのフィールドにユーザ名を入力することでキー認証を行うことができる。５０６は、キー認証におけるパスワード入力フィールドである。ＭＦＰ１０１のユーザはこのフィールドにパスワードを入力することでキー認証を行うことができる。５０７は、キー認証におけるログインボタンである。このボタンが押下されると、ユーザ名入力フィールド５０５、パスワード入力フィールド５０６に入力された値が取得され、Ｗｅｂサーバ１０２のプレゼンテーション部４１１に送信される。

【００３１】

図５の６００はＷｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼンテーション部４１１と通信を行って、カード認証画面を描画したＷｅｂブラウザ４３０の外観である。６０１はＷｅｂブラウザ４３０のコンテンツ表示領域である。この領域にＷｅｂサーバ１０２から受信したレスポンスに基づいてコンテンツが表示される。カード認証画面６００では、当該画面の画面情報をプレゼンテーション部４１１が送信し、通信部４３１が受信した後、解析部４３２が解析し、その後画面表示部４３３がコンテンツ表示領域６０１上に描画している。６０３はキー認証画面５００への切り替えを行うボタンである。このボタンはカード認証画面６００には必ず表示される。６０３は指紋認証画面７００への切り替えを行うボタンである。

【００３２】

図６の７００はＷｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼンテーション部４１１と通信を行って、指紋認証画面を描画したＷｅｂブラウザ４３０の外観である。７０１はＷｅｂブラウザ４３０のコンテンツ表示領域である。この領域にＷｅｂサーバ１０２から受信したレスポンスに基づいてコンテンツを表示する。指紋認証画面７００では、当該画面の画面情報をプレゼンテーション部４１１が送信し、通信部４３１が受信した後、解析部４３２が解析し、その後画面表示部４３３がコンテンツ表示領域７０１上に描画している。７０３はキー認証画面５００への切り替えを行うボタンである。このボタンは指紋認証画面７００には必ず表示される。７０３はカード認証画面６００への切り替えを行うボタンである。このように、認証画面５００、６００、７００には、１つの認証機器に対応する認証画面であり、他の複数の認証機器がＭＦＰ１０１に対して接続されている場合には、当該認証機器に対応する認証画面へのリンクボタンを含んで構成される。

【００３３】

図６の８００はＷｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼンテーション部４１１と通信を行って、タブ形式でキー認証画面５００、カード認証画面６００、指紋認証画面７００を描画したＷｅｂブラウザ４３０の外観である。８０１はＷｅｂブラウザ４３０のコンテンツ表示領域である。８０２はＷｅｂブラウザのタブ表示領域である。ここでは指紋認証画面７００が選択されているため、コンテンツ表示領域８０１には指紋認証画面７００が表示されている。なお、画面８００の詳細については、第２の実施形態において後述する。

【００３４】

図７の９００はＷｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼン

テーション部４１１と通信を行って、ログイン失敗時の画面を描画したＷｅｂブラウザ４３０の外観である。９０１はＷｅｂブラウザ４３０のコンテンツ表示領域である。また、図７の１０００はＷｅｂブラウザ４３０の通信部４３１がＷｅｂサーバ１０２のプレゼンテーション部４１１と通信を行って、排他処理時のエラー画面を描画したＷｅｂブラウザ４３０の外観である。ログインが完了しているにも関わらず、ログインサービスにアクセスされた時に表示される。１００１はＷｅｂブラウザ４３０のコンテンツ表示領域である。

【００３５】

＜認証処理＞

次に、図８を参照して、本実施形態における、ログインフレームワーク４７０が認証処理をログインアプリケーション部４４０に要求してから、認証成功の応答が返ってくるまでの処理について説明する。なお、以下で説明する処理は、ＭＦＰ１０１のＣＰＵ２１１又はＷｅｂサーバ１０２のＣＰＵ３１１がＲＯＭ２１２、３１２等に格納されている制御プログラムを読み出して実行することにより実現される。

【００３６】

Ｓ１１０１において、ログインフレームワーク４７０は、ログインアプリケーション部４４０に対して認証処理要求を行う。続いて、Ｓ１１０２において、ログインアプリケーション部４４０は、ＵＳＢ認証機器情報取得部４４１によって、ＭＦＰ１０１に接続されているＵＳＢ認証機器４８０の情報を取得する。Ｓ１１０３において、ログインアプリケーション部４４０は、Ｗｅｂブラウザ４３０がＷｅｂアプリケーション４１０と接続を行うためのＨＴＴＰリクエストを作成する。その際、リクエストヘッダにＳ１１０２で取得したＵＳＢ認証機器情報を記載して作成する。さらに、Ｓ１１０４において、ログインアプリケーション部４４０は、Ｗｅｂブラウザ４３０に対して、認証画面の表示を要求し、Ｓ１１０５において、Ｗｅｂブラウザ４３０に対して、Ｓ１１０３で作成したＨＴＴＰリクエストを送信する。

【００３７】

次に、Ｓ１１０６において、Ｗｅｂブラウザ４３０は、Ｓ１１０５で送信されたＨＴＴＰリクエストに従ってＷｅｂアプリケーション４１０に対して、認証画面を描画するためのｈｔｍｌ取得要求を行う。ｈｔｍｌ取得要求を受信したＷｅｂアプリケーション４１０は、Ｓ１１０７でｈｔｍｌを作成し、Ｓ１１０８で作成したｈｔｍｌの情報をＷｅｂブラウザ４３０に返信する。

【００３８】

ｈｔｍｌの情報を取得すると、Ｓ１１０９において、Ｗｅｂブラウザ４３０は、キー認証画面５００を表示部に表示する。また、この際カード認証画面６００への切り替えボタン５０３が押された場合、Ｗｅｂアプリケーション４１０は後述する図１０の処理を行う。同様に指紋認証画面７００への切り替えボタン５０４が押下された場合、Ｗｅｂアプリケーション４１０は後述する図１１の処理を行う。それぞれの場合において、Ｗｅｂアプリケーション４１０の処理フローは図９と同様であり、各認証方法への切り替えボタンは作成せず、キー認証への切り替えボタンを代わりに作成する。また、認証画面の表示中にＵＳＢ認証機器４８０の抜き差しが行われた場合、ログインアプリケーション部４４０は新しいＵＳＢ認証機器情報をＷｅｂブラウザ４３０に通知し、認証画面の更新を行う。図１４はこのフローを示している。図１４のＳ１７０１からＳ１７０９までのフローは図８のＳ１１０２からＳ１１０９までのフローと同一であり、この処理によって、常に最新のＵＳＢ認証機器４８０状態に対応した認証画面をＷｅｂブラウザ４３０が描画する。

【００３９】

次に、Ｓ１１１０において、Ｗｅｂブラウザ４３０は、ユーザから入力された認証情報を取得する。認証情報を取得すると、Ｓ１１１１において、Ｗｅｂブラウザ４３０は、認証情報通知手段として機能し、Ｓ１１１０で取得した認証情報をＷｅｂアプリケーション４１０に送信する。Ｓ１１１２において、Ｗｅｂアプリケーション４１０は、Ｓ１１１１でＷｅｂブラウザ４３０から送信された認証情報の認証操作を行う。Ｓ１１２の認証操作

が成功すると、Ｓ１１１３において、Ｗｅｂアプリケーション４１０は、ユーザのログインを許可するログイン通知をログインアプリケーション部４４０に通知する。

【００４０】

Ｓ１１１４において、ログインアプリケーション部４４０は、ログインコンテキスト生成部４４３によってユーザのセッション情報を含むログインコンテキストを生成する。Ｓ１１１５において、ログインアプリケーション部４４０は、ログインフレームワーク４７０に対して認証成功通知を通知する。

【００４１】

以上説明した処理がログインフレームワーク４７０が認証処理をログインアプリケーション部に要求してから、認証成功の応答が返ってくるまでの処理である。これによって、ＭＦＰ１０１に接続されているＵＳＢ認証機器情報に基づいて、Ｗｅｂブラウザ４３０が最適な認証画面をユーザに提供したのち、認証を行うフローを実現している。

【００４２】

＜画面情報の作成＞

次に、図９乃至図１１を参照して、Ｗｅｂアプリケーション４１０において、画面情報となるｈｔｍｌを作成する作成処理について説明する。なお、以下で説明する処理は、Ｗｅｂサーバ１０２のＣＰＵ３１１がＲＯＭ３１２等に格納されている制御プログラムを読み出して実行することにより実現される。まず、図９を参照して、Ｗｅｂアプリケーション４１０がＷｅｂブラウザ４３０から上記Ｓ１１０６のｈｔｍｌ取得要求を受信した際の処理について説明する。

【００４３】

Ｓ１２０１において、Ｗｅｂアプリケーション４１０は、Ｓ１１０６でＷｅｂブラウザ４３０が送信したＨＴＴＰリクエストを取得する。続いて、Ｓ１２０２において、Ｗｅｂアプリケーション４１０は、Ｗｅｂブラウザ４３０に表示させるキー認証画面５００のｈｔｍｌ（画面情報）を作成する。Ｓ１２０３において、Ｗｅｂアプリケーション４１０は、Ｓ１２０１で受信したＨＴＴＰリクエストのヘッダを解析する。Ｓ１２０４において、Ｗｅｂアプリケーション４１０は、Ｓ１２０３で解析した結果、リクエストヘッダ内にキー認証機器情報が含まれているかを判定する。ここで、ヘッダ内にキー認証機器情報が含まれていればＳ１２０５に進み、含まれていなければＳ１２１０に進む。Ｓ１２１０において、Ｗｅｂアプリケーション４１０は、Ｓ１２０２で作成したｈｔｍｌを認証エラー用のｈｔｍｌに作り変え、Ｓ１２０９に進む。リクエストヘッダ内にキー認証機器情報が入っていないということは、ユーザがログイン後にＷｅｂブラウザ４３０を通して、アクセスを行ったことを意味する。よって、複数回のログインを防止するため、エラーページ（エラー画面１０００）へ飛ばす処理をここで行っている。

【００４４】

Ｓ１２０５において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内にカード認証機器情報が含まれているかを判定する。判断を行う。ここで、ヘッダ内にカード認証機器情報が含まれていればＳ１２０６に進み、含まれていなければＳ１２０７に進む。Ｓ１２０６において、Ｗｅｂアプリケーション４１０は、Ｓ１２０２で作成したキー認証画面用のｈｔｍｌにカード認証サービス（カード認証画面６００）へのリンクボタンを追加し、Ｓ１２０７に進む。

【００４５】

Ｓ１２０７において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内に指紋認証機器情報が含まれているかを判定する。ここで、ヘッダ内に指紋認証機器情報が含まれていればＳ１２０８に進み、含まれていなければＳ１２０９に進む。Ｓ１２０８において、Ｗｅｂアプリケーション４１０は、Ｓ１２０２で作成したキー認証画面用のｈｔｍｌに指紋認証サービス（指紋認証画面７００）へのリンクボタンを追加し、Ｓ１２０９に進む。Ｓ１２０９において、Ｗｅｂアプリケーション４１０は、作成されたキー認証画面用のｈｔｍｌをＷｅｂブラウザ４３０に送信し、処理を終了する。

【００４６】

次に、図１０及び図１１を参照して、カード認証画面６００のｈｔｍｌの作成、指紋認証画面７００のｈｔｍｌの作成について説明する。なお、図１０及び図１１のｈｔｍｌ作成処理は、図９のｈｔｍｌ作成処理とほぼ同様であるため、図９のフローチャートとの差異についてのみ説明する。

【００４７】

図１０は、カード認証画面６００のｈｔｍｌを作成する処理であり、Ｓ１３０２においてカード認証画面用のｈｔｍｌを作成する。さらに、Ｓ１３０４乃至Ｓ１３０７の処理において、キー認証ボタンと、指紋認証ボタンとを当該ｈｔｍｌに追加する必要があるかを判定し、必要が有れば追加する処理を行っている。また、図１１は、指紋認証画面７００のｈｔｍｌを作成する処理であり、Ｓ１４０２において指紋認証画面用のｈｔｍｌを作成する。さらに、Ｓ１４０４乃至Ｓ１４０７の処理において、キー認証ボタンと、カード認証ボタンとを当該ｈｔｍｌに追加する必要があるかを判定し、必要が有れば追加する処理を行っている。

【００４８】

＜認証操作＞

次に、図１２を参照して、Ｗｅｂアプリケーション４１０における認証操作（Ｓ１１１２）について説明する。なお、以下で説明する処理は、Ｗｅｂサーバ１０２のＣＰＵ３１１がＲＯＭ３１２等に格納されている制御プログラムを読み出して実行することにより実現される。

【００４９】

Ｓ１５０１において、Ｗｅｂアプリケーション４１０は、Ｓ１１１１でＷｅｂブラウザ４３０から送信された認証情報を取得する。続いて、Ｓ１５０２において、Ｗｅｂアプリケーション４１０は、Ｓ１５０１で取得した認証情報と認証情報記憶部４２０に格納されているデータとの照合を行う。Ｓ１５０３において、Ｗｅｂアプリケーション４１０は、Ｓ１５０２で照合を行った結果、完全に一致するデータが見つかったかどうかを判定する。ここで、完全に一致するデータが見つかればＳ１５０４に進み、見つからなければＳ１５０５に進む。

【００５０】

Ｓ１５０４において、Ｗｅｂアプリケーション４１０は、ログイン成功通知をログインアプリケーション部４４０に対して送信し、処理を終了する。一方、Ｓ１５０５において、Ｗｅｂアプリケーション４１０は、ログインエラーを通知するｈｔｍｌを作成し、Ｗｅｂブラウザ４３０に送信し、処理を終了する。Ｗｅｂブラウザ４３０は当該エラー通知を受けて、ログインエラー画面９００を表示する。

【００５１】

＜第２の実施形態＞

次に、図１３を参照して、本発明の第２の実施形態について説明する。本実施形態は、ＭＦＰ１０１に接続されている認証機器が複数存在する場合に、各認証機器に対応した認証画面をタブ形式で一覧表示する形態を提供する。なお、ユーザの認証情報入力に必要な手間を考え、キー入力認証よりもカード認証を優先して表示し、カード認証よりも指紋認証を優先して表示することとする。図１３は、本実施形態における画面取得処理におけるＷｅｂアプリケーション４１０の処理フローである。なお、以下で説明する処理は、Ｗｅｂサーバ１０２のＣＰＵ３１１がＲＯＭ３１２等に格納されている制御プログラムを読み出して実行することにより実現される。

【００５２】

Ｓ１４０１において、Ｗｅｂアプリケーション４１０は、ＨＴＴＰリクエストを取得する。続いて、Ｓ１４０２において、Ｗｅｂアプリケーション４１０は、取得したＨＴＴＰリクエストのリクエストヘッダを解析する。Ｓ１４０３において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内にキー認証機器情報が含まれる否かを判定する。ここで、ヘッダ内にキー認証機器情報が含まれていればＳ１４０４に進み、含まれていなければＳ１４０６に進む。Ｓ１４０４において、Ｗｅｂアプリケーション４１０は、キー認証画

面５００のｈｔｍｌを作成し、Ｓ１４０５に進む。

【００５３】

一方、Ｓ１４０６において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内にカード認証機器情報が含まれているかを判定する。ここで、ヘッダ内にカード認証機器情報が含まれていればＳ１４０７に進み、含まれていなければＳ１４０８に進む。Ｓ１４０７において、Ｗｅｂアプリケーション４１０は、カード認証画面６００のＨｔｍｌを作成し、Ｓ１４０５に進む。

【００５４】

一方、Ｓ１４０８において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内に指紋認証機器情報が含まれているかを判定する。ここで、ヘッダ内に指紋認証機器情報が含まれていればＳ１４０９に進み、含まれていなければＳ１４１０に進む。Ｓ１４０９において、Ｗｅｂアプリケーション４１０は、指紋認証画面７００のＨｔｍｌを作成し、Ｓ１４０５に進む。

【００５５】

一方、Ｓ１４１０において、Ｗｅｂアプリケーション４１０は、リクエストヘッダ内にいずれの認証機器情報も含まれていないことを意味するため、認証エラー用のｈｔｍｌを作成し、Ｓ１４０５に進む。Ｓ１４０５において、Ｗｅｂアプリケーション４１０は、作成した認証画面のｈｔｍｌをＷｅｂブラウザ４３０に送信する。この後、Ｗｅｂブラウザ４３０は受信したｈｔｍｌ情報に基づき認証画面を描画する。この際、新たな認証機器用の認証画面情報が送信された場合、新しく受信した認証画面を前面に表示することが望ましい。これによって、キー認証画面５００よりカード認証画面６００の方が、カード認証画面６００より指紋認証画面７００の方が優先して前面に表示されることとなる。

【００５６】

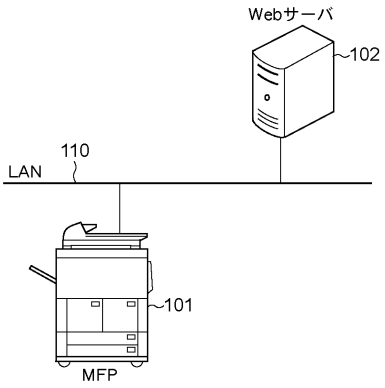
以上説明した処理が、本実施形態におけるＷｅｂアプリケーション４１０の画面情報作成処理であり、ＭＦＰ１０１が利用可能な認証機器の分だけこの処理を繰り返すことで画面８００のような、タブ形式での認証画面を表示することができる。このように、本実施形態によれば、タブで認証画面を切り替えることにより、認証画面切り替え時のＷｅｂアプリケーションとの通信による画面遷移時間を省略できる。また、入力時間の短い認証画面を前面に出すことにより、ユーザの認証所要時間を短縮できる。

【００５７】

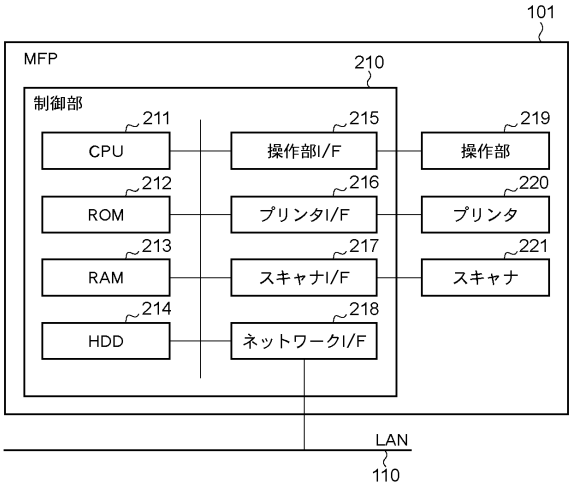
＜その他の実施形態＞

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

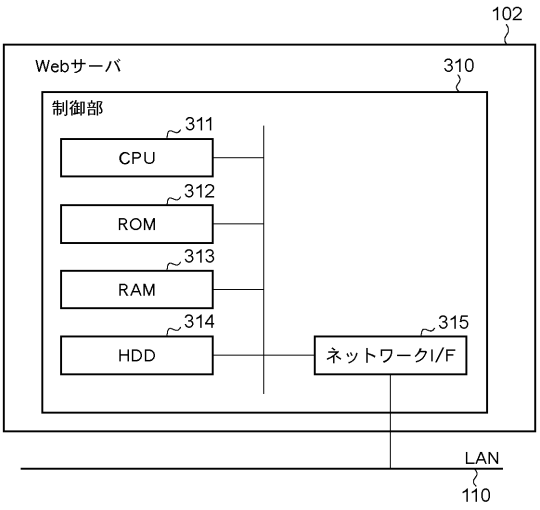
【図１】


Webサーバ
102
110
LAN
101
MFP

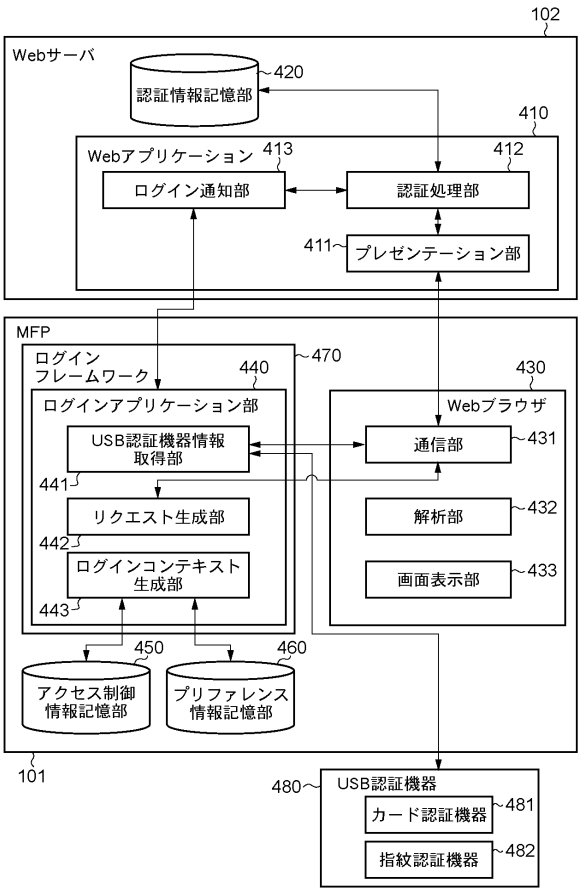
【図２】


101
MFP
210
制御部
211
CPU
212
ROM
213
RAM
214
HDD
215
操作部I/F
216
プリンタI/F
217
スキャナI/F
218
ネットワークI/F
219
操作部
220
プリンタ
221
スキャナ
LAN
110

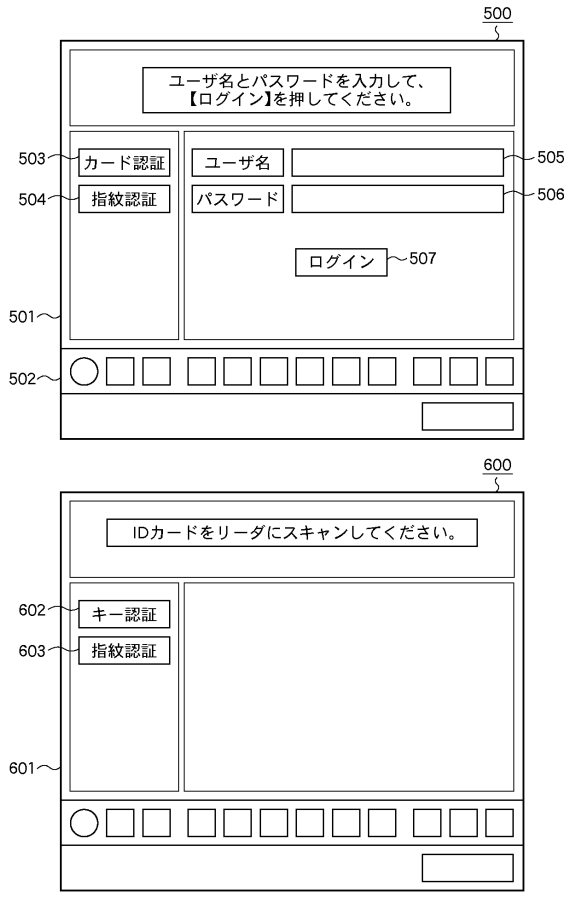
【図３】


102
Webサーバ
310
制御部
311
CPU
312
ROM
313
RAM
314
HDD
315
ネットワークI/F
LAN
110

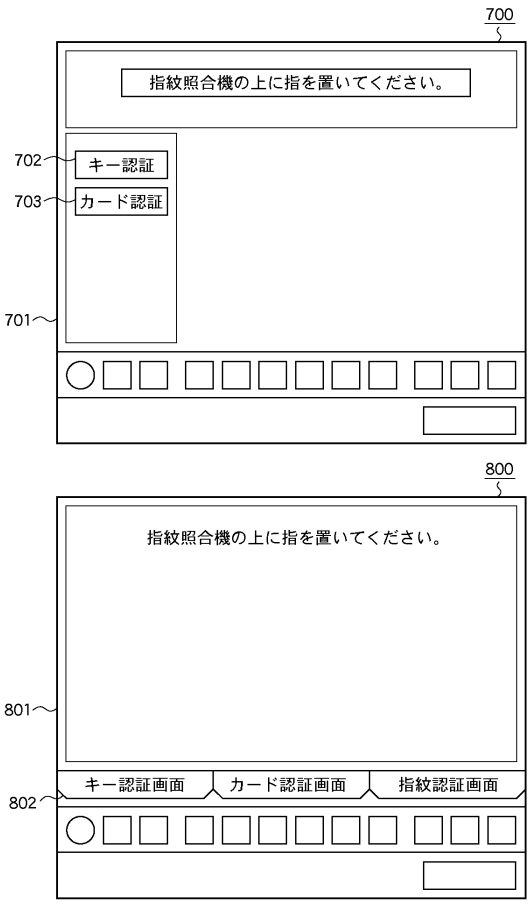
【図４】


102
Webサーバ
420
認証情報記憶部
410
Webアプリケーション
413
ログイン通知部
412
認証処理部
411
プレゼンテーション部
MFP
ログイン
フレームワーク
470
440
ログインアプリケーション部
USB認証機器情報
取得部
441
リクエスト生成部
442
ログインコンテキスト
生成部
443
430
Webブラウザ
通信部
431
解析部
432
画面表示部
433
450
アクセス制御
情報記憶部
460
プリファレンス
情報記憶部
101
480
USB認証機器
カード認証機器
481
指紋認証機器
482

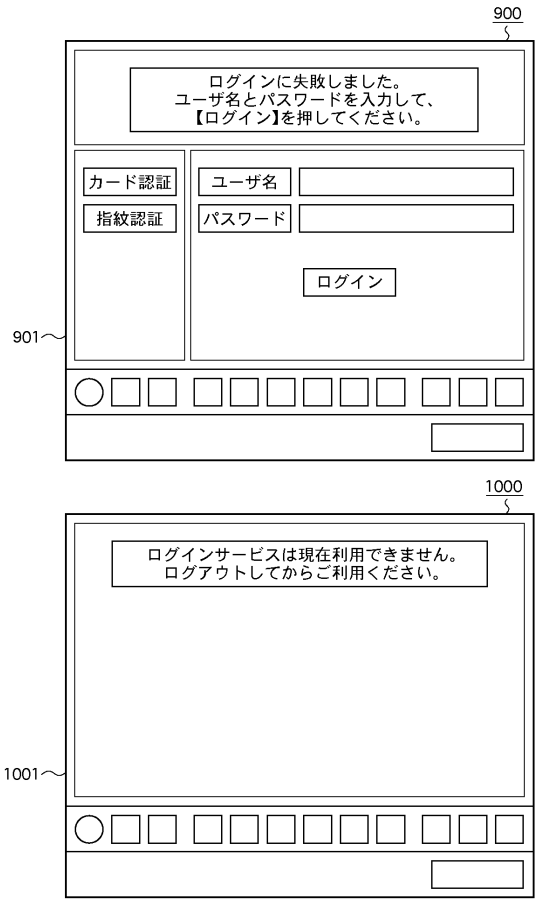
【図５】


500
ユーザ名とパスワードを入力して、
【ログイン】を押してください。
503
カード認証
504
指紋認証
ユーザ名
505
パスワード
506
ログイン
507
501
502
600
IDカードをリーダにスキャンしてください。
602
キー認証
603
指紋認証
601

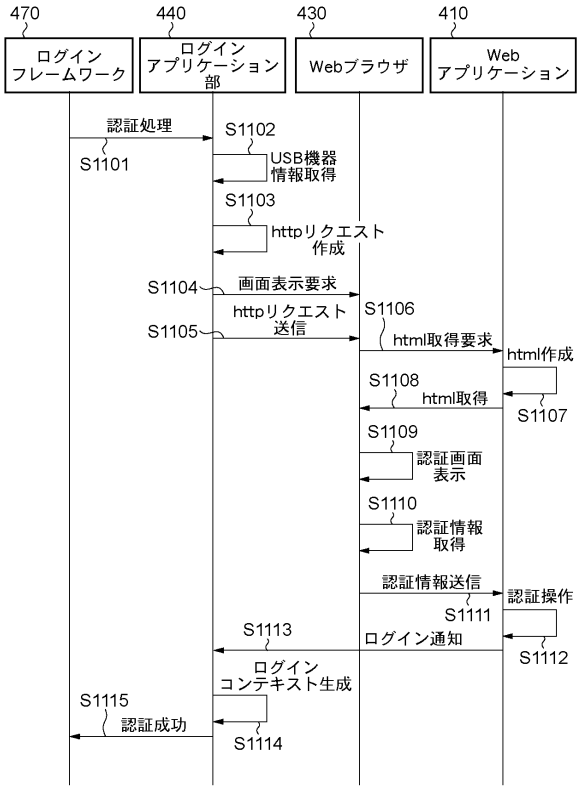
【図６】


700
指紋照合機の上に指を置いてください。
702
キー認証
703
カード認証
701
800
指紋照合機の上に指を置いてください。
801
キー認証画面
カード認証画面
指紋認証画面
802

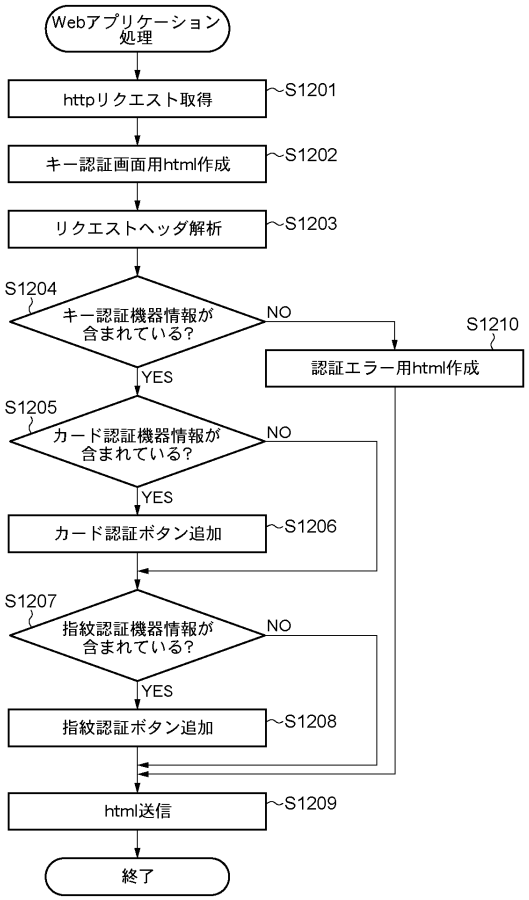
【図７】


900
ログインに失敗しました。
ユーザ名とパスワードを入力して、
【ログイン】を押してください。
カード認証
ユーザ名
指紋認証
パスワード
ログイン
901
1000
ログインサービスは現在利用できません。
ログアウトしてからご利用ください。
1001

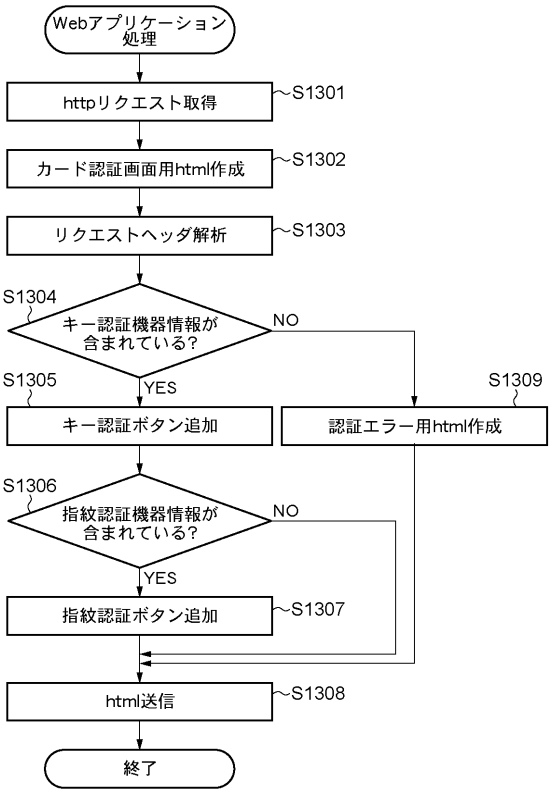
【図８】


470
ログイン
フレームワーク
440
ログイン
アプリケーション
部
430
Webブラウザ
410
Web
アプリケーション
認証処理
S1101
S1102
USB機器
情報取得
S1103
httpリクエスト
作成
S1104
画面表示要求
S1105
httpリクエスト
送信
S1106
html取得要求
html作成
S1108
html取得
S1107
S1109
認証画面
表示
S1110
認証情報
取得
認証情報送信
S1111
認証操作
S1113
ログイン通知
S1112
ログイン
コンテキスト生成
S1115
認証成功
S1114

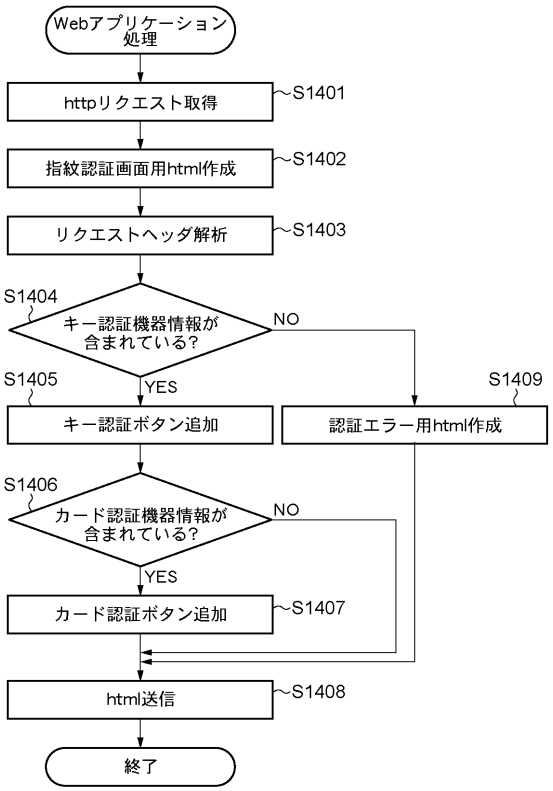
【図９】



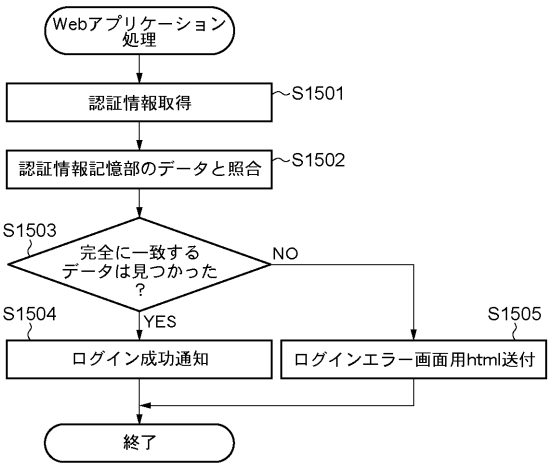
【図１０】



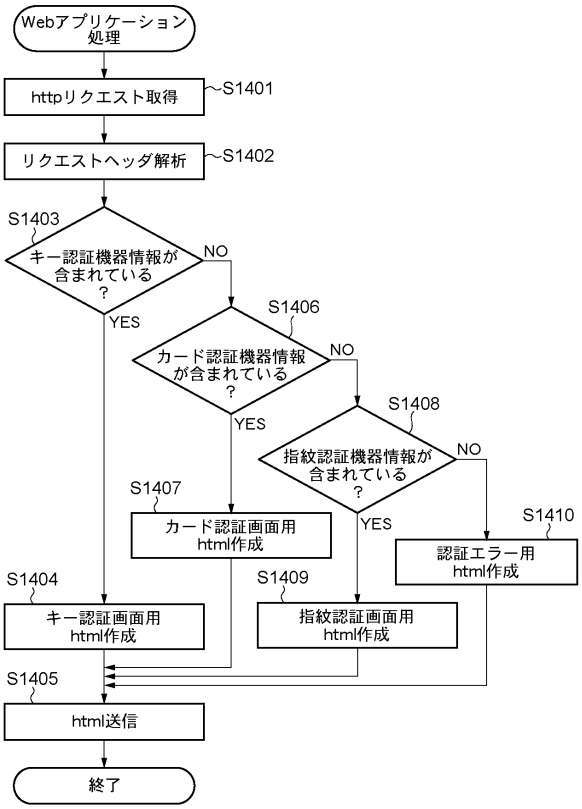
【図１１】



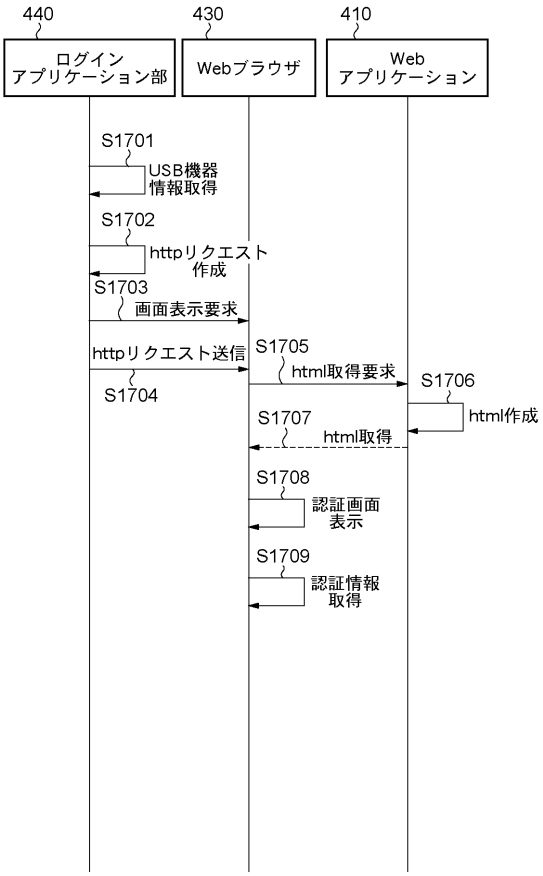
【図１２】



【図１３】


Webアプリケーション処理
httpリクエスト取得
S1401
リクエストヘッダ解析
S1402
S1403
キー認証機器情報が含まれている？
NO
YES
S1406
カード認証機器情報が含まれている？
NO
YES
S1408
指紋認証機器情報が含まれている？
NO
YES
S1407
カード認証画面用html作成
S1410
認証エラー用html作成
S1404
キー認証画面用html作成
S1409
指紋認証画面用html作成
S1405
html送信
終了

【図１４】


440
ログインアプリケーション部
430
Webブラウザ
410
Webアプリケーション
S1701
USB機器情報取得
S1702
httpリクエスト作成
S1703
画面表示要求
httpリクエスト送信
S1704
S1705
html取得要求
S1706
html作成
S1707
html取得
S1708
認証画面表示
S1709
認証情報取得

フロントページの続き

(51)Int.Cl.		FI		
B41J 29/00	***(2006.01)***	B41J	29/00	Z
B41J 29/42	***(2006.01)***	B41J	29/42	F
B41J 29/38	***(2006.01)***	B41J	29/38	Z

(72)発明者　池内　雄馬
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

審査官　岸野　徹

(56)参考文献　特開２００８－２６２３０９（ＪＰ，Ａ）
特開２００９－１９９２３５（ＪＰ，Ａ）
特開２００２－１３５４９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｂ４１Ｊ　２９／００
Ｂ４１Ｊ　２９／３８
Ｂ４１Ｊ　２９／４２
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｆ　２１／３４
Ｇ０６Ｔ　７／００
Ｈ０４Ｌ　９／３２