(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2015-170117
(P2015-170117A)
(43)公開日　平成27年9月28日(2015.9.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/20	131A	2C061
G06F 3/12	(2006.01)	G06F	3/12	K	
G06F 1/00	(2006.01)	G06F	1/00	370E	
B41J 29/38	(2006.01)	B41J	29/38	Z	
B41J 29/00	(2006.01)	B41J	29/00	Z	

審査請求 未請求　請求項の数 11　ＯＬ　（全 16 頁）

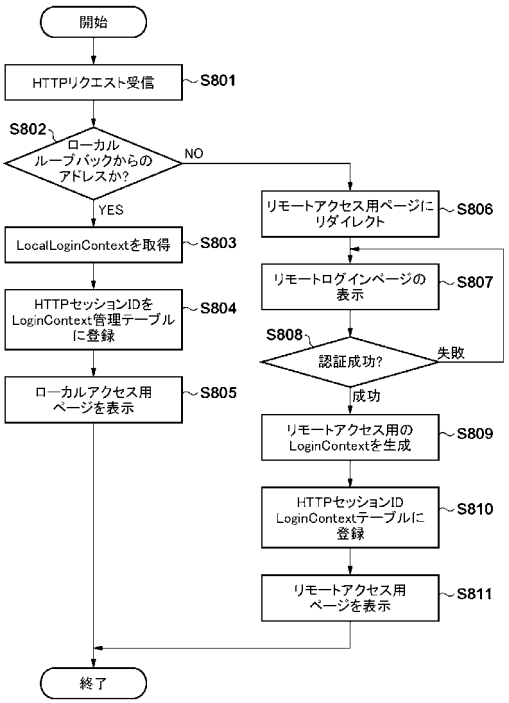
(21)出願番号　特願2014-44262(P2014-44262)
(22)出願日　平成26年3月6日(2014.3.6)

(71)出願人　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】情報処理装置、制御方法およびプログラム

(57)【要約】
【課題】認証を必要とするアプリケーションへのアクセスの際に、そのアクセス元に応じて認証画面の表示を適切に制御する情報処理装置を提供する。
【解決手段】ユーザ認証を要するアプリケーションを実行可能なサーバ機能を有する情報処理装置は、アプリケーションの実行要求の要求元が当該情報処理装置であるか否かを判定する。要求元が情報処理装置でないと判定された場合、要求元に、アプリケーションのユーザ認証を行うための認証情報の入力画面データを、実行要求に対する応答として送信する。一方、要求元が情報処理装置であると判定された場合、要求元に、認証情報の入力画面データを送信しない。
【選択図】図８



【特許請求の範囲】
【請求項１】
ユーザ認証を要するアプリケーションを実行可能なサーバ機能を有する情報処理装置であって、
前記アプリケーションの実行要求を受信する受信手段と、
前記受信手段により受信した実行要求の要求元が当該情報処理装置であるか否かを判定する判定手段と、
前記判定手段により当該要求元が当該情報処理装置でないと判定された場合、当該要求元に、前記アプリケーションのユーザ認証を行うための認証情報の入力画面データを、前記受信手段により受信した実行要求に対する応答として送信し、一方、前記判定手段により当該要求元が当該情報処理装置であると判定された場合、当該要求元に、前記認証情報の入力画面データを送信しない制御手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
前記判定手段により当該要求元が当該情報処理装置であると判定された場合、ユーザの当該情報処理装置へのログイン情報を用いて前記アプリケーションのユーザ認証を行う認証手段、をさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記制御手段は、前記判定手段により当該要求元が当該情報処理装置であると判定され、前記認証手段による認証が成功した場合、当該要求元に、前記アプリケーションの実行画面データを、前記受信手段により受信した実行要求に対応する応答として送信する、ことを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記判定手段により当該要求元が当該情報処理装置であると判定され、前記認証手段による認証が成功した場合、当該ユーザが当該情報処理装置にログインしている間、前記アプリケーションのセッションを維持するセッション制御手段、をさらに備える請求項２又は３に記載の情報処理装置。
【請求項５】
前記セッション制御手段は、前記アプリケーションのセッションのタイムアウトの実行を制限することにより、当該ユーザが当該情報処理装置にログインしている間、前記アプリケーションのセッションを維持する、ことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記セッション制御手段は、前記アプリケーションのセッションのタイムアウト時間を、当該ユーザの当該情報処理装置へのログイン状態に同期させることにより、当該ユーザが当該情報処理装置にログインしている間、前記アプリケーションのセッションを維持する、ことを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記判定手段は、前記受信手段により受信した実行要求に含まれる要求元のアドレスを参照することにより、当該要求元が当該情報処理装置であるか否かを判定する、ことを特徴とする請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記サーバ機能はＷｅｂサーバ機能であることを特徴とする請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
前記情報処理装置は、画像形成装置であり、
前記アプリケーションは、前記画像形成装置の設定を行うためのアプリケーションである、ことを特徴とする請求項１乃至８のいずれか１項に記載の情報処理装置。
【請求項１０】
ユーザ認証を要するアプリケーションを実行可能なサーバ機能を有する情報処理装置に

おいて実行される制御方法であって、
前記アプリケーションの実行要求を受信する受信工程と、
前記受信工程において受信した実行要求の要求元が当該情報処理装置であるか否かを判定する判定工程と、
前記判定工程において当該要求元が当該情報処理装置でないと判定された場合、当該要求元に、前記アプリケーションのユーザ認証を行うための認証情報の入力画面データを、前記受信工程において受信した実行要求に対する応答として送信し、一方、前記判定工程において当該要求元が当該情報処理装置であると判定された場合、当該要求元に、前記認証情報の入力画面データを送信しない制御工程と、
を有することを特徴とする制御方法。

【請求項１１】
請求項１乃至９のいずれか１項の情報処理装置の各手段としてコンピュータを機能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、サーバ機能を有する情報処理装置、制御方法およびプログラムに関する。

【背景技術】
【０００２】
ＰＣなどの情報処理装置がネットワーク上のＷｅｂサーバに接続され、Ｗｅｂサーバにより提供される操作画面を、情報処理装置が備えるＷｅｂブラウザ上に表示することが知られている。その場合、まず、情報処理装置のＷｅｂブラウザが、Ｗｅｂサーバに対して操作画面を要求（リクエスト）する。そして、Ｗｅｂサーバ上のＷｅｂアプリケーションが情報処理装置からの要求に応じて、Ｗｅｂブラウザに操作画面を表示させるためのＨＴＭＬデータを情報処理装置に応答（レスポンス）する。情報処理装置のＷｅｂブラウザは、受信したＨＴＭＬデータを解析し、ＨＴＭＬデータの記述に基づいた操作画面を表示する。更に、Ｗｅｂブラウザに表示された操作画面を介してユーザが指示を入力すると、Ｗｅｂブラウザは、その入力された指示をＷｅｂサーバに対して通知する。そして、Ｗｅｂアプリケーションは、その通知を受けると、入力された指示に従って処理を実行する。

【０００３】
近年、スキャナやプリンタを備えたＭＦＰ（Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）にも、上述したようなＷｅｂブラウザが備えられている。そして、ＭＦＰは、上述の手順により、Ｗｅｂサーバにより提供される操作画面をＭＦＰのＷｅｂブラウザに表示し、ユーザからの各種指示を受け付ける。また、ＭＦＰがＷｅｂサーバの機能を備えている場合もある。そのような場合では、ユーザは、ＭＦＰ上のＷｅｂサーバで動作するＷｅｂアプリケーションを、ユーザが同じＭＦＰ上のブラウザを介して操作し、ＭＦＰの機能を利用するユースケースも知られている。

【０００４】
近年、ＭＦＰが認証機能を有し、ＭＦＰへのリソースアクセスに対して認証を求めるケースが多い。認証は、ＭＦＰの操作部上で実施される場合や、ＭＦＰ上のＷｅｂアプリケーションに対してＷｅｂブラウザからアクセスする際に実施される場合など、その形態は様々である。例えば、管理者がＭＦＰの設定情報を変更する場合、管理者は、ＭＦＰ上のＷｅｂアプリケーションに対して、ＰＣ等の情報処理装置上のＷｅｂブラウザを介してアクセスする。ＭＦＰは、アクセスしているユーザが管理者であるか否かを判定するために、Ｗｅｂブラウザに認証画面を表示して認証操作を要求する。また、他に、管理者がＭＦＰの操作部から設定情報を変更する場合、ＭＦＰは、操作部上に認証画面を表示し、ユーザに認証操作を要求する。いずれの場合においても、ユーザは設定情報を変更するために、認証操作を実行する必要がある。

【先行技術文献】
【特許文献】

【０００５】
【特許文献１】特開２００９－１１０５４２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
例えば、ＭＦＰの操作部からのログイン操作が行われた後に、Ｗｅｂブラウザは、そのＭＦＰ上で動作するＷｅｂアプリケーションへアクセスする場合を考える。その際、Ｗｅｂアプリケーションは、どこからアクセスされたかを考慮せずに新しいセッションを作成するので、ユーザに対して認証画面を表示し、認証操作を要求する。つまり、ユーザは、既にログイン操作を行っているにも関わらず、認証情報を入力するという認証操作を再び行わなくてはならない。
【０００７】
特許文献１には、組み込みＷｅｂブラウザであるか否か、若しくは、Ｗｅｂブラウザの種別に応じて、表示内容を動的に変更することが記載されている。しかしながら、特許文献１では、表示内容のみの変更が行われるに過ぎず、上記のようなユーザ操作に係るユーザビリティの低下を解決することができない。
【０００８】
本発明の目的は、このような従来の問題点を解決することにある。上記の点に鑑み、本発明は、認証を必要とするアプリケーションへのアクセスの際に、そのアクセス元に応じて認証画面の表示を適切に制御する情報処理装置、制御方法およ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】
【０００９】
上記課題を解決するため、本発明に係る情報処理装置は、ユーザ認証を要するアプリケーションを実行可能なサーバ機能を有する情報処理装置であって、前記アプリケーションの実行要求を受信する受信手段と、前記受信手段により受信した実行要求の要求元が当該情報処理装置であるか否かを判定する判定手段と、前記判定手段により当該要求元が当該情報処理装置でないと判定された場合、当該要求元に、前記アプリケーションのユーザ認証を行うための認証情報の入力画面データを、前記受信手段により受信した実行要求に対する応答として送信し、一方、前記判定手段により当該要求元が当該情報処理装置であると判定された場合、当該要求元に、前記認証情報の入力画面データを送信しない制御手段と、を備えることを特徴とする。
【発明の効果】
【００１０】
本発明によれば、認証を必要とするアプリケーションへのアクセスの際に、そのアクセス元に応じて認証画面の表示を適切に制御することができる。
【図面の簡単な説明】
【００１１】
【図１】情報処理装置と他装置とを含む情報通信システムの構成を示す図である。
【図２】ＭＦＰのハードウェア構成を示すブロック図である。
【図３】ＭＦＰのソフトウェア構成を示すブロック図である。
【図４】操作部に表示されるログイン画面を示す図である。
【図５】リモートログイン画面を示す図である。
【図６】ＬｏｇｉｎＣｏｎｔｅｘｔの管理テーブルとデータ構造を示す図である。
【図７】ＭＦＰのログイン処理を示すフローチャートである。
【図８】認証画面の表示制御処理を示すフローチャートである。
【図９】ローカルログイン部のログアウト処理を示すフローチャートである。
【図１０】リモートログイン部のログアウト処理を示すフローチャートである。
【発明を実施するための形態】
【００１２】

以下、添付図面を参照して本発明の好適な実施形態を詳しく説明する。尚、以下の実施形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。なお、同一の構成要素には同一の参照番号を付して、説明を省略する。

【００１３】

図１は、本実施形態における情報処理装置と他装置とを含む情報通信システムの構成を示す図である。情報処理システム１は、情報処理装置の一例であるＭＦＰ（ＭｕｌｔｉＦｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）１０１及び１０３、クライアントＰＣ１０２を含む。ＭＦＰとは、スキャン機能、印刷機能、ＦＡＸ機能等、複数機能が一体化された多機能周辺装置（画像形成装置）である。システム１に含まれるＭＦＰ１０１、クライアントＰＣ１０２、ＭＦＰ１０３は、ＬＡＮ等のネットワーク１１０を介して相互に通信可能に接続されている。なお、不図示の装置以外の装置がネットワーク１１０に接続されていても良い。また、ネットワーク１１０は、有線通信ネットワークでも良いし、無線通信ネットワークでも良い。システム１において、ＭＦＰ１０１若しくは１０３は、Ｗｅｂサーバ機能を有している。クライアントＰＣ１０２のユーザは、ネットワーク１１０を介して、Ｗｅｂサーバ機能により実行可能な各種アプリケーションを利用することができる。また、ＭＦＰ１０１又は１０３のユーザが、自身のＭＦＰのＷｅｂサーバ機能により実行可能な各種アプリケーションを利用することもできる。本実施形態において、各種アプリケーションは、例えば、ＭＦＰが実行可能なコピー機能等の設定情報の編集アプリケーションを含んでいる。

【００１４】

図２は、ＭＦＰ１０１及び１０３のハードウェア構成を示すブロック図である。本実施形態においては、以下、ＭＦＰ１０１をＭＦＰ１０１及び１０３の代表例として説明する。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実行することにより、例えば、読取制御や送信制御など各機能に対応したエンジン制御を行う。その結果、ＭＦＰ１０１は、コピー／スキャン（送信）／プリント等の各機能を実現することができる。ＲＡＭ２１３は、ＣＰＵ２１１の主メモリ、又は、ワークエリア等の一時記憶領域として用いられる。ハードディスク（ＨＤＤ）２１４は、画像データや機能設定情報、各種プログラムを記憶する。本実施形態の動作は、例えば、ＣＰＵ２１１がＲＯＭ２１２から制御プログラムをＲＡＭ２１３に読み出して実行することにより実現される。

【００１５】

操作部Ｉ／Ｆ２１５は、操作部２１９と制御部２１０との間の通信接続を可能にする。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ており、ユーザからのＭＦＰ１０１の各機能の実行指示や設定操作を受け付けることができる。また、操作部２１９は、ＭＦＰ１０１のＷｅｂサーバ機能により実行可能なアプリケーションの利用の指示（アクセス指示）を受け付けることもできる。

【００１６】

プリンタＩ／Ｆ２１６は、プリンタ２２０と制御部２１０との間の通信接続を可能にする。プリンタ２２０で印刷対象の画像データは、プリンタＩ／Ｆ２１６を介して制御部２１０からプリンタ２２０に転送される。プリンタ２２０は、画像データを、インクジェット方式や電子写真方式等の各記録方式に従った印刷用データに変換し、記録媒体上に印刷対象の画像を印刷する。スキャナＩ／Ｆ２１７は、スキャナ２２１と制御部２１０との間の通信接続を可能にする。スキャナ２２１は、不図示のＡＤＦ（自動原稿フィーダ）や原稿台上に置かれた原稿上の画像を光学的に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に入力する。

【００１７】

ネットワークＩ／Ｆ２１８は、制御部２１０とネットワーク１１０との間の通信接続を可能にする。ネットワークＩ／Ｆ２１８は、ネットワーク１１０上の装置（例えば、クライアントＰＣ１０２や他のＭＦＰ）との間の通信を可能にする。

【００１８】
図３は、ＭＦＰ１０１及び１０３のソフトウェア構成を示すブロック図である。図１と同様に、ＭＦＰ１０１をＭＦＰ１０１及び１０３の代表例として説明する。図３に示す各ブロックは、例えば、ＨＤＤ２１４に記憶されたプログラムを、ＣＰＵ２１１が実行することによって実現される。なお、ＭＦＰ１０１には、図３に示すブロック以外のブロックが含まれても良い。
【００１９】
メニュー管理部３０１は、ＭＦＰ１０１の各ソフトウェアモジュール（ブロック）を起動するためのメニュー画面を操作部２１９に表示するためのモジュールである。メニュー管理部３０１は、コピー画面や後述のＷｅｂブラウザによる設定画面等の表示を指示するためのＧＵＩ（Ｇｒａｐｈｉｃａｌ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）ボタンを操作部２１９に一覧表示する。また、それらの画面上でコピーやスキャン等に対応する各ボタンのユーザ押下に応じて、ＣＰＵ２１１は、各対応するソフトウェアモジュールを起動する。
【００２０】
ＨＴＴＰ通信部３０２は、ＨＴＴＰに準拠する通信を可能にする。Ｗｅｂブラウザ３０３は、ＨＴＴＰ通信部３０２を介してＷｅｂサーバ３１３とＨＴＴＰ通信を行う。また、Ｗｅｂブラウザ３０３は、ＨＴＴＰ通信部３０２及びネットワークＩ／Ｆ２１８を介して、他の装置のＷｅｂサーバとＨＴＴＰ通信を行うこともできる。Ｗｅｂサーバ３１３は、Ｗｅｂアプリケーション３０９を動作させるためのプラットホームであり、Ｗｅｂアプリケーション３０９は、Ｗｅｂサーバ３１３上で動作する。本実施形態では、Ｗｅｂアプリケーション３０９は、ＭＦＰ１０１の各機能の設定変更を実行可能なＷｅｂアプリケーションである。つまり、ユーザは、Ｗｅｂアプリケーション３０９をＷｅｂブラウザ３０３を介して利用し、後述する図５の設定変更画面５０５若しくは５０８により、Ｗｅｂアプリケーション３０９が動作しているＭＦＰ１０１の設定情報を変更（編集）することができる。
【００２１】
ＷｅｂクライアントとなるＷｅｂブラウザ３０３からＷｅｂアプリケーション３０９に対してアクセス（要求）があった場合、Ｗｅｂアプリケーション３０９はＷｅｂサーバ３１３及びＨＴＴＰ通信部３０２を介しＷｅｂクライアントとＨＴＴＰ通信を実行する。ここで、Ｗｅｂクライアントは、ＭＦＰ１０１のＷｅｂブラウザ３０３に限られず、例えば、クライアントＰＣ１０２のＷｅｂブラウザ３０３の場合もある。
【００２２】
Ｗｅｂブラウザ３０３は、操作部２１９を介してユーザからＵＲＬを指定されると、そのＵＲＬに対応するＨＴＭＬデータを、Ｗｅｂサーバ３１３を介してＷｅｂアプリケーション３０９に要求する。また、Ｗｅｂブラウザ３０３は、その要求に対する応答としてＷｅｂアプリケーション３０９から送信されたＨＴＭＬデータをＷｅｂサーバ３１３及びＨＴＴＰ通信部３０２を介して受信する。そして、Ｗｅｂブラウザ３１３は、受信したＨＴＭＬデータに基づく画面を操作部２１９に表示する。ここで、Ｗｅｂサーバは、ＭＦＰ１０１のＷｅｂサーバ３１３に限られず、例えば、ネットワーク１１０に接続されＷｅｂアプリケーションを有する別装置として構成されたＷｅｂサーバの場合もある。Ｗｅｂアプリケーション３０９は、ＭＦＰ１０１への操作を行うためのユーザインタフェース（ＵＩ）画面をＨＴＭＬデータとしてＷｅｂクライアントに提供する。ユーザは、そのＵＩ画面上で、ＭＦＰ１０１の設定情報の変更や、画像データの印刷等の指示を行うことができる。
【００２３】
ローカルアクセス用ページ３１０は、同じＭＦＰ１０１内のＷｅｂブラウザ３０３からＷｅｂアプリケーション３０９にアクセスされた場合に、Ｗｅｂクライアントに提供するＷｅｂページである。また、リモートアクセス用ページ３１１は、外部装置のＷｅｂブラウザからアクセスされた場合に、Ｗｅｂクライアントに提供するＷｅｂページである。
【００２４】

ロケーション判定部３１２は、Ｗｅｂアプリケーション３０９に対してアクセスがあった場合、同じＭＦＰ１０１のＷｅｂブラウザ３０３からのアクセスであるか否かを判定する。ロケーション判定部３１２は、Ｗｅｂアプリケーション３０９に対するアクセスが、同じＭＦＰ１０１のＷｅｂブラウザ３０３からのアクセスであると判定した場合、ローカルアクセス用ページ３１０をＷｅｂクライアントに提供するＷｅｂページとして指定する。一方、同じＭＦＰ１０１のＷｅｂブラウザ３０３からのアクセスでない（即ち、外部装置のＷｅｂブラウザからのアクセス等）と判定した場合、リモートアクセス用ページ３１１をＷｅｂクライアントに提供するＷｅｂページとして指定する。

【００２５】

ログイン部３０８は、ＭＦＰ１０１に対するユーザ認証を実行する。ログイン部３０８は、ローカルログイン部３０４、リモートログイン部３０６、ユーザデータベース（ＤＢ）３０５、セッション管理部３０７を含む。

【００２６】

ユーザＤＢ３０５は、ＭＦＰ１０１を利用可能なユーザのユーザＩＤやパスワード、その他、権限情報を記憶する。ローカルログイン部３０４は、ＭＦＰ１０１の起動後等、ユーザによるＭＦＰ１０１の利用開始時にログイン画面を操作部２１９に表示し、ユーザから認証情報（ユーザ情報）を受け付けて認証処理を実行する。認証情報の受け付けについては、ユーザが操作部２１９に表示されたソフトウェアキーをタイプすることにより受け付ける場合や、不図示のメモリインタフェースに装着されたＩＣカード（メモリ）に記憶されたユーザ情報を読み出す場合がある。ローカルログイン部３０４は、受け付けたユーザ情報をユーザＤＢ３０５と照合する。その際、受け付けた認証情報がユーザＤＢ３０５に登録されているものと一致する場合には認証成功とし、そのユーザのＭＦＰ１０１の利用、つまりメニュー管理部３０１により表示されるメニュー画面の使用を許可する。なお、本実施形態では、認証に利用するユーザＤＢ３０５はＭＦＰ１０１内に構成されているが、ユーザ情報を管理する管理サーバを外部装置として構成し、上記のユーザ情報の照合を管理サーバ側で行うようにしても良い。

【００２７】

リモートログイン部３０６は、例えばクライアントＰＣ１０２上のＷｅｂブラウザからＭＦＰ１０１のＷｅｂアプリケーション３０９に対してアクセスがあった場合に、ユーザ認証を実行する。リモートログイン部３０６は、クライアントＰＣ１０２からＨＴＴＰ通信部３０２及びＷｅｂサーバ３１３を介してＷｅｂアプリケーション３０９に対してアクセスがあった場合、セッション管理部３０７に問い合わせを行う。その問い合わせとして、リモートログイン部３０６は、そのクライアントＰＣ１０２に対するセッションが存在するか否かをセッション管理部３０７に問い合わせる。セッションが存在しない場合には、予め定められた認証用画面をクライアントＰＣ１０２に送信（応答）する。そして、リモートログイン部３０６は、クライアントＰＣ１０２から認証情報をＨＴＴＰ通信部３０２を介して受信し、認証処理を実行する。ここで、認証の方法は、ローカルログイン部３０４の場合と同じであり、認証が成功した場合には、クライアントＰＣ１０２からＭＦＰ１０１のＷｅｂアプリケーション３０９に対するアクセスを許可する。

【００２８】

セッション管理部３０７は、ローカルログイン部３０４及びリモートログイン部３０６により制御され、認証が成功した場合には、それぞれのログイン部によりセッションが生成される。セッション管理部３０７では、それぞれのログイン部により設定されているタイムアウト時間に従って各セッションを監視する。例えば、一定時間、ユーザ操作が行われない場合や、ユーザが明示的に操作部２１９若しくはＷｅｂサーバ３１３に対してログアウトを指示した場合には、そのセッションを終了（破棄）する。

【００２９】

図４は、ＭＦＰ１０１の操作部２１９に表示されるログイン画面の一例を示す図である。ユーザは、ＭＦＰ１０１の起動後等にログインするために、ログイン画面４０１上のユーザ名入力部４０２及びパスワード入力部４０３にユーザ名及びパスワード（ログイン情

報）を入力してログインボタン４０４を押下する。ローカルログイン部３０４は、ログインボタン４０４の押下を検出すると認証処理を実行し、ユーザ名及びパスワードがユーザＤＢ３０５に登録されているものと一致するか否かを判定する。ユーザＤＢ３０５に登録されているものと一致すると判定された場合、メニュー管理部３０１は、メインメニュー画面４０５を操作部２１９に表示する。その結果、ユーザによるＭＦＰ１０１の操作が可能となる。

【００３０】

メインメニュー画面４０５には複数のボタンが表示され、例えば、コピーボタン４０６、スキャンボタン４０７、Ｗｅｂブラウザーボタン４０８が表示されている。ユーザは、各ボタンを選択して押下することにより、各機能の実行を指示することができる。メインメニュー画面４０５には、図４のボタン以外のボタンが構成されても良い。また、ユーザによりログアウトボタン４０９が押下されると、ローカルログイン部３０４は、ＭＦＰ１０１からのログアウト処理を実行する。ローカルログイン部３０４は、ログアウト処理の終了後、再び、操作部２１９にログイン画面４０１を表示する。

【００３１】

図５は、他の装置のＷｅｂブラウザから、ＭＦＰ１０１のＷｅｂアプリケーション３０９にアクセスした場合に、他の装置で表示されるリモートログイン画面の一例を示す図である。ここでは、ＭＦＰ１０３のＷｅｂブラウザ３０３から、ＭＦＰ１０１のＷｅｂアプリケーション３０９にアクセスしたとする。その場合には、ＭＦＰ１０３の操作部２１９には、図５に示すリモートログイン画面５０１を表示するためのＷｅｂページ（入力画面データ）が送信され、ＭＦＰ１０３のＷｅｂブラウザ３０３によりリモートログイン画面５０１が表示される。ユーザは、ＭＦＰ１０３の操作部２１９上のユーザ名入力部５０２及びパスワード入力部５０３にユーザ名及びパスワードを入力してログインボタン５０４を押下する。

【００３２】

ＭＦＰ１０１のリモートログイン部３０６は、ログインボタン５０４の押下を検出すると、入力されたユーザ名及びパスワード（認証情報）に基づいて認証処理を実行する。ここで、ユーザ名及びパスワードがユーザＤＢ３０５に登録されているものと一致した場合、ＭＦＰ１０１のＷｅｂサーバ３１３は、Ｗｅｂアプリケーション３０９の設定変更画面５０５を表示するためのＷｅｂページ（実行画面データ）にリダイレクトする。さらに、リモートログイン部３０６は、ＭＦＰ１０３のＷｅｂブラウザ３０３との間のセッションを作成する。作成されたセッションは、ＭＦＰ１０１のセッション管理部３０７により管理される。例えば、ユーザから一定時間アクセスがない場合や、設定変更画面５０５上のログアウトボタン５０７が押下された場合には、ＭＦＰ１０１のセッション管理部３０７は、そのセッションを終了する。ここで、セッションが終了された後（セッションが存在しない状態）で、ＭＦＰ１０３のＷｅｂブラウザ３０３が再びＭＦＰ１０１のＷｅｂアプリケーション３０９の設定変更画面５０５をリクエストした場合は、リモートログイン画面５０１が再び表示される。

【００３３】

上記のように、ユーザによるＭＦＰ１０１へのログイン後、ＭＦＰ１０１のＷｅｂアプリケーション３０９により設定変更画面５０５を表示するためのＷｅｂページがＭＦＰ１０３に提供され、ＭＦＰ１０３の操作部２１９に表示される。ユーザは、設定変更画面５０５上で、ＭＦＰ１０１の設定を設定項目５０６から選択することができる。図５では、設定項目５０６として、設定Ａ、設定Ｂ、設定Ｃが表示されている。設定Ａ～Ｃは、例えば、ＭＦＰ１０１が実行可能な各機能に対応している。ユーザにより設定項目が選択されると、不図示の詳細設定画面を表示するためのＷｅｂページがＭＦＰ１０３に提供され、ＭＦＰ１０３の操作部２１９上に詳細設定画面が表示される。その結果、ＭＦＰ１０３のユーザは、ＭＦＰ１０１の各機能に係る設定情報を変更（編集）することができる。

【００３４】

次に、ユーザがＭＦＰ１０１の操作部２１９上でログイン画面４０１によりＭＦＰ１０

１にログインした後、ＭＦＰ１０１のＷｅｂアプリケーションにアクセス（設定変更画面のリクエスト）した場合を説明する。つまり、ＭＦＰ１０１のＷｅｂブラウザ３０３がＭＦＰ１０１のＷｅｂアプリケーション３０９にアクセスした場合には、Ｗｅｂアプリケーション３０９により設定変更画面５０８を表示するためのＷｅｂページがＷｅｂブラウザ３０３に提供される。

【００３５】

設定変更画面５０８は、ログアウトボタン５０７がない点で設定変更画面５０５と異なる。本実施形態では、設定変更画面５０８が表示される場合には、Ｗｅｂブラウザ３０３のセッションの維持は、ローカルログイン部３０４のセッション（ログイン状態）と同期して管理される。つまり、ローカルログイン部３０４によりログアウト処理が実行されると、その実行に同期して、Ｗｅｂブラウザ３０３のセッションをクローズする。そのような構成により、ローカルログイン部３０４とＷｅｂブラウザ３０３の両方がログイン処理を実行している場合に、Ｗｅｂブラウザ３０３のセッションがログアウトされ、再度のログインのために認証処理が必要となってしまうことを防ぐ。

【００３６】

または、設定変更画面５０８にもログアウトボタン５０７と同様のログアウトボタンを構成し、ユーザからの明示的なログアウトを可能にしても良い。本実施形態においては、Ｗｅｂブラウザ３０３のセッションのタイムアウトの実行は制限される。例えば、Ｗｅｂブラウザ３０３のセッションのタイムアウト時間は、ローカルログイン部３０４のセッションのタイムアウト時間に同期するように制御される。そのような構成により、ローカルログイン部３０４とＷｅｂブラウザ３０３の両方がログイン処理を実行している場合に、Ｗｅｂブラウザ３０３のセッションがタイムアウトしてしまい、再度のログインのために認証処理が必要となってしまうことを防ぐ。

【００３７】

若しくは、ローカルログイン部３０４とＷｅｂブラウザ３０３の両方がログイン処理を実行している場合に、Ｗｅｂブラウザ３０３のセッションがタイムアウト等でログアウトした場合に、認証処理を行うものの認証画面の表示を抑制するようにしても良い。例えば、その場合、Ｗｅｂアプリケーション３０９は、図７のＳ７０２で受け付けたユーザＩＤ及びパスワードを用いて認証処理を行う。

【００３８】

図６は、ＭＦＰ１０１の、セッション管理部３０７により管理されるＬｏｇｉｎＣｏｎｔｅｘｔの管理テーブルとそのデータ構造の一例を示す図である。ＬｏｇｉｎＣｏｎｔｅｘｔは、ユーザのログインからログアウトまでのログイン状態と、ログインしているユーザに関する情報とを保持するオブジェクトである。ＭＦＰ１０１内のＷｅｂアプリケーション３０９は、ＬｏｇｉｎＣｏｎｔｅｘｔからユーザに関する情報を取得し、本実施形態の処理を実行する。

【００３９】

図６の項目６０１は、各ＬｏｇｉｎＣｏｎｔｅｘｔを識別するための識別子である。項目６０２は、ＬｏｇｉｎＣｏｎｔｅｘｔのタイプを示す。本実施形態では、項目６０２は、各ＬｏｇｉｎＣｏｎｔｅｘｔがローカルログイン部３０４で生成されたものであるか、若しくは、リモートログイン部３０６で生成されたものであるかを表す。「Ｌｏｃａｌ」と表示されたＬｏｇｉｎＣｏｎｔｅｘｔは、ローカルログイン部３０４で生成されたものを示す。また、「Ｒｅｍｏｔｅ」と表示されたＬｏｇｉｎＣｏｎｔｅｘｔは、リモートログイン部３０６で生成されたものを示す。項目６０３は、各ユーザを識別するための識別子である。項目６０４は、ＳｅｓｓｉｏｎＩＤを示し、関連するＨＴＴＰセッションが存在する場合には、そのＨＴＴＰセッションを識別するためのＳｅｓｓｉｏｎＩＤが格納される。

【００４０】

例えば、図６のＬｏｇｉｎＣｏｎｔｅｘｔＩＤが「１」のＬｏｇｉｎＣｏｎｔｅｘｔは、ローカルログイン部３０４で生成され、「Ｕｓｅｒ１」で識別されるユーザに関し、関

連するＨＴＴＰセッションのＳｅｓｓｉｏｎＩＤが「ｓ１」であることを示す。図６のテーブルで管理されるＬｏｇｉｎＣｏｎｔｅｘｔは、セッション管理部３０７により管理され、ユーザがＭＦＰ１０１からログアウトするタイミングで図６のテーブルから破棄される。このようにして、Ｗｅｂブラウザ３０３のセッションがローカルログイン部３０４のログイン状態と同期され、少なくとも、ユーザがＭＦＰ１０１にログインしている間は、Ｗｅｂブラウザ３０３のセッションは維持される（セッション制御）。

【００４１】

図７は、ＭＦＰ１０１の操作部２１９を介したログイン処理を示すフローチャートである。本処理は、ログイン部３０８のローカルログイン部３０４により実行される。例えばＭＦＰ１０１の電源投入等により、本処理が開始される。Ｓ７０１において、ローカルログイン部３０４は、操作部２１９にログイン画面４０１を表示する。

【００４２】

Ｓ７０２において、ローカルログイン部３０４は、ユーザから認証情報（ユーザＩＤ及びパスワード）をログイン画面４０１上のユーザＩＤ入力部４０２及びパスワード入力部４０３を介して受け付ける。そして、ローカルログイン部３０４は、ユーザによるログインボタン４０４の押下を検出する。

【００４３】

Ｓ７０３において、ローカルログイン部３０４は、Ｓ７０３で受け付けたユーザＩＤ及びパスワードがユーザＤＢ３０５に登録されているものと一致するか否かを判定する。ここで、一致すると判定された場合、即ち、認証成功の場合にはＳ７０４に進み、一致しないと判定された場合、即ち、認証失敗の場合にはＳ７０１からの処理を繰り返す。

【００４４】

Ｓ７０４において、ローカルログイン部３０４は、新しいＬｏｇｉｎＣｏｎｔｅｘｔＩＤを発行し、セッション管理部３０７により管理されるＬｏｇｉｎＣｏｎｔｅｘｔテーブルに登録する。ここで、登録される情報として、例えば、ＵｓｅｒＩＤや、ＬｏｇｉｎＣｏｎｔｅｘｔのタイプである。また、ユーザに関する他の情報を登録するようにしても良い。また、本処理の場合には、ユーザは操作部２１９からログインしたので、ＬｏｇｉｎＣｏｎｔｅｘｔのタイプは、ローカルログイン部３０４で生成されたことを示す「Ｌｏｃａｌ」となる。

【００４５】

Ｓ７０５において、ローカルログイン部３０４はメニュー管理部３０１にｌｏｇｉｎＣｏｎｔｅｘｔの登録を通知すると、メニュー管理部３０１は、メインメニュー画面４０５を操作部２１９に表示する。その結果、ユーザによるＭＦＰ１０１の操作が可能となり、図７の処理を終了する。

【００４６】

図８は、ＭＦＰ１０１のＷｅｂアプリケーション３０９の表示制御処理を示すフローチャートである。本処理が開始されると、Ｓ８０１において、Ｗｅｂアプリケーション３０９は、Ｗｅｂクライアントから送信されたＨＴＴＰリクエスト（実行要求）を受信する。なお、Ｗｅｂアプリケーション３０９は、ローカルアクセス用ページ３１０、リモートアクセス用ページ３１１の２つのページを各ＵＲＬとして有している。いずれのＵＲＬに対してＷｅｂクライアントからＨＴＴＰリクエストを受信した場合でも、本フローチャートの処理が開始される。

【００４７】

Ｓ８０２において、Ｗｅｂアプリケーション３０９のロケーション判定部３１２は、Ｓ８０１で受信したＨＴＴＰリクエストの情報を解析し、ＷｅｂクライアントのＩＰアドレスがローカルループバックからのアクセスであるか否かを判定する。ここで、ローカルループバックアドレス、若しくはＷｅｂクライアントのＩＰアドレスがＷｅｂアプリケーション３０９の動作するＭＦＰ１０１のＩＰアドレスと一致する場合には、ローカルループバックからのアクセスであると判定してＳ８０３に進む。一方、異なる場合にはローカルループバックからのアクセスでないと判定してＳ８０６に進む。

【００４８】
Ｓ８０３において、Ｗｅｂアプリケーション３０９は、ローカルログイン部３０４により生成された、即ち、タイプが「Ｌｏｃａｌ」であるＬｏｇｉｎＣｏｎｔｅｘｔを、セッション管理部３０７から取得する。Ｓ８０４において、Ｓ８０３で取得したＬｏｇｉｎＣｏｎｔｅｘｔに対して、Ｓ８０２で受信したＨＴＴＰリクエストに含まれるＨＴＴＰセッションのＳｅｓｓｉｏｎＩＤを、ＬｏｇｉｎＣｏｎｔｅｘｔ管理テーブルの項目６０４に格納する。Ｓ８０５において、Ｗｅｂアプリケーション３０９は、設定変更画面５０８を表示するためのＷｅｂページ（実行画面データ）をＨＴＴＰレスポンスとしてＷｅｂクライアントに送信する。ここで、Ｗｅｂクライアントとは、ＭＦＰ１０１のＷｅｂブラウザ３０３である。Ｓ８０５の処理後、本処理を終了する。ここで、Ｗｅｂブラウザ３０３のセッションに予め設定されているタイムアウト機能は制限される。例えば、Ｗｅｂブラウザ３０３のセッションのタイムアウト時間は、ローカルログイン部３０４のセッションのタイムアウト時間に同期するように設定される。

【００４９】
このように、本実施形態においては、ユーザが操作部２１９からＭＦＰ１０１にログインした後、Ｗｅｂアプリケーション３０９にアクセスした場合には、図５のリモートログイン画面５０１は表示されない。その結果、ユーザは、ＭＦＰ１０１へのログイン操作に加えて、Ｗｅｂアプリケーション３０９への認証情報の入力を行わなくて済むので、ユーザビリティが向上する。また、Ｗｅｂアプリケーション３０９は、Ｓ８０２においてローカルループバックからのアクセスであると判定された場合に、認証処理そのものをスキップして、Ｗｅｂブラウザ３０３に、設定変更画面５０８を表示するためのＷｅｂページを提供しても良い。若しくは、その際の認証処理やアクセス制限を、図７のＳ７０２で受け付けたユーザＩＤ及びパスワードを用いて行っても良い。

【００５０】
Ｓ８０２でＷｅｂクライアントのＩＰアドレスがローカルループバックからのアクセスでないと判定された場合、Ｓ８０６で、Ｗｅｂアプリケーション３０９は、Ｓ８０１で受信したＨＴＴＰリクエストをリモートアクセス用のページ３１１にリダイレクトする。

【００５１】
Ｓ８０７において、Ｗｅｂアプリケーション３０９は、リモートログイン画面５０１を表示するためのＷｅｂページ（入力画面データ）をＷｅｂクライアントに提供する。そして、リモートログイン部３０６は、アクセス元（要求元）でユーザ名入力部５０２及びパスワード入力部５０３を介して受け付けたユーザ名及びパスワードを取得する。Ｓ８０８において、リモートログイン部３０６は、Ｓ８０７で取得したユーザＩＤ及びパスワードが、ユーザＤＢ３０５に登録されているものと一致するか否かを判定する。ここで、一致すると判定された場合にはＳ８０９に進み、一致しないと判定された場合にはＳ８０７からの処理を繰り返す。

【００５２】
Ｓ８０９において、リモートログイン部３０６は、ＬｏｇｉｎＣｏｎｔｅｘｔを生成し、セッション管理部３０７により管理されるＬｏｇｉｎＣｏｎｔｅｘｔ管理テーブルに登録する。ここで、リモートログイン部３０６により生成されたＬｏｇｉｎＣｏｎｔｅｘｔのタイプは「Ｒｅｍｏｔｅ」となる。

【００５３】
Ｓ８１０で、リモートログイン部３０６は、Ｓ８０９で生成したＬｏｇｉｎＣｏｎｔｅｘｔに対し、Ｓ８０１で受信したＨＴＴＰリクエストに含まれるＨＴＴＰセッションのＳｅｓｓｉｏｎＩＤをＬｏｇｉｎＣｏｎｔｅｘｔ管理テーブルの項目６０４に格納する。ここで、Ｗｅｂアプリケーション用のセッションのタイムアウト時間は、予め本リモートアクセス用に設定されている時間のまま適用される。つまり、一定時間ＨＴＴＰ通信が実行されない場合には、セッション管理部３０７によりセッションが終了される。そして、新しくＨＴＴＰリクエストが送信された場合には、再び、Ｓ８０１の処理から実行される。

【００５４】

Ｓ８１１において、Ｗｅｂアプリケーション３０９は、設定変更画面５０５を表示するＷｅｂページをＨＴＴＰレスポンスとしてＷｅｂクライアントに送信する。Ｓ８１１の処理後、本処理を終了する。

【００５５】

図９は、ＭＦＰ１０１のローカルログイン部３０４におけるログアウト処理を示すフローチャートである。本処理が開始されると、Ｓ９０１において、ローカルログイン部３０４は、操作部２１９に表示されるメインメニュー画面４０５上のログアウトボタン４０９の押下（ログアウトイベント）を検出する。若しくは、ユーザが操作部２１９に対して一定時間操作を実施しなかった場合や、予め設定されたローカルタイムアウト時間が経過した場合にも以降の処理が実行される。

【００５６】

Ｓ９０２にて、ローカルログイン部３０４は、セッション管理部３０７により管理されるＬｏｇｉｎＣｏｎｔｅｘｔであり項目６０２が「Ｌｏｃａｌ」であるＬｏｇｉｎＣｏｎｔｅｘｔの項目６０４に、ＳｅｓｓｉｏｎＩＤが登録されているか否かを判定する。以下、登録されていると判定されたＳｅｓｓｉｏｎＩＤを関連ＳｅｓｓｉｏｎＩＤと呼ぶ。ここで、関連ＳｅｓｓｉｏｎＩＤが登録されていると判定された場合にはＳ９０３に進み、関連ＳｅｓｓｉｏｎＩＤが登録されていないと判定された場合には、Ｓ９０４において「Ｌｏｃａｌ」であるＬｏｇｉｎＣｏｎｔｅｘｔを破棄する。

【００５７】

Ｓ９０３において、セッション管理部３０７は、Ｓ９０３で登録されていると判定された関連ＳｅｓｓｉｏｎＩＤのセッションをクローズする。そして、Ｓ９０４において、セッション管理部３０７は、ＬｏｇｉｎＣｏｎｔｅｘｔ管理テーブルからクローズ対象の関連ＳｅｓｓｉｏｎＩＤの情報を破棄するとともに、「Ｌｏｃａｌ」であるＬｏｇｉｎＣｏｎｔｅｘｔを破棄する。Ｓ９０４の処理後、本処理を終了する。

【００５８】

図９のような処理により、ＭＦＰ１０１にログイン後、Ｗｅｂアプリケーション３０９にアクセスしたユーザに係るＷｅｂブラウザ３０３のセッションの維持制御をローカルログイン部３０４によるログイン状態に同期させて行う。

【００５９】

図１０は、ＭＦＰ１０１のリモートログイン部３０６のログアウト処理を示すフローチャートである。本処理が開始されると、Ｓ１００１において、リモートログイン部３０６は、設定変更画面５０５のログアウトボタン５０７の押下（ログアウトイベント）を検出する。若しくは、Ｗｅｂアプリケーション３０９が一定時間ＨＴＴＰリクエストを受信しない場合や、予め設定されたリモートタイムアウト時間が経過した場合にも以降の処理が実行される。

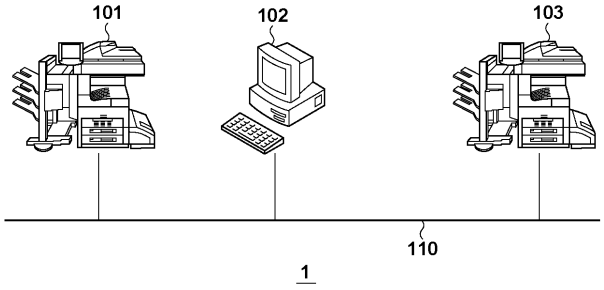
【００６０】

Ｓ１００２において、リモートログイン部３０６は、ＬｏｇｉｎＣｏｎｔｅｘｔ管理テーブルの項目６０２が「Ｒｅｍｏｔｅ」で、かつ項目６０４のＳｅｅｓｉｏｎＩＤがＨＴＴＰリクエストのＩＤと一致するＬｏｇｉｎＣｏｎｔｅｘｔを検索する。そして、セッション管理部３０７は、そのＳｅｓｓｉｏｎＩＤのセッションをクローズする。Ｓ１００３において、セッション管理部３０７は、検索されたＬｏｇｉｎＣｏｎｔｅｘｔの項目６０４からＳｅｓｓｉｏｎＩＤを破棄するとともに、「Ｒｅｍｏｔｅ」であるＬｏｇｉｎＣｏｎｔｅｘｔを破棄する。Ｓ１００３の処理後、本処理を終了する。

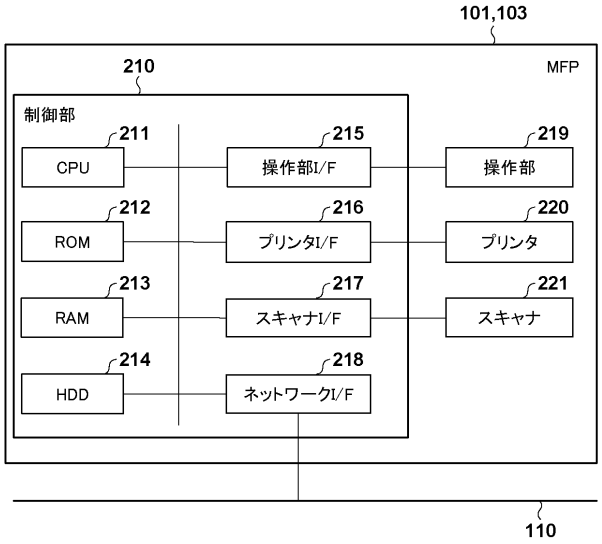
【００６１】

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。

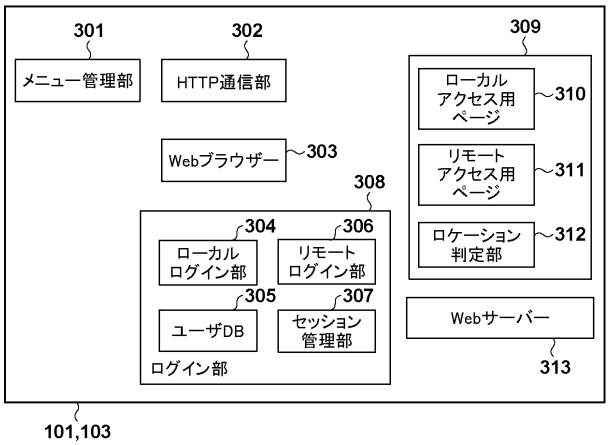
【図１】


101
102
103
110
1

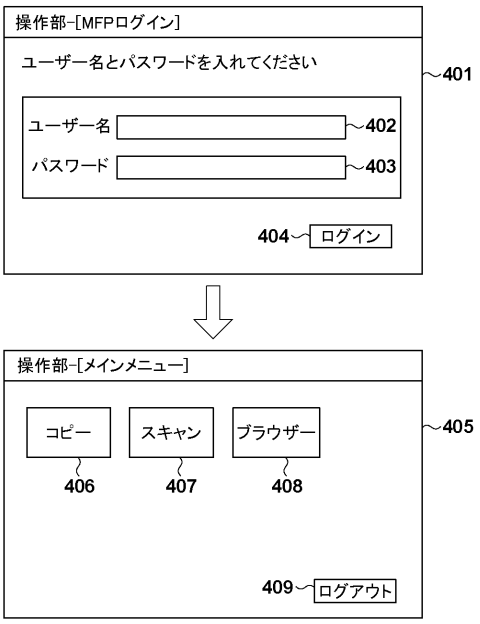
【図２】


101,103
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
110

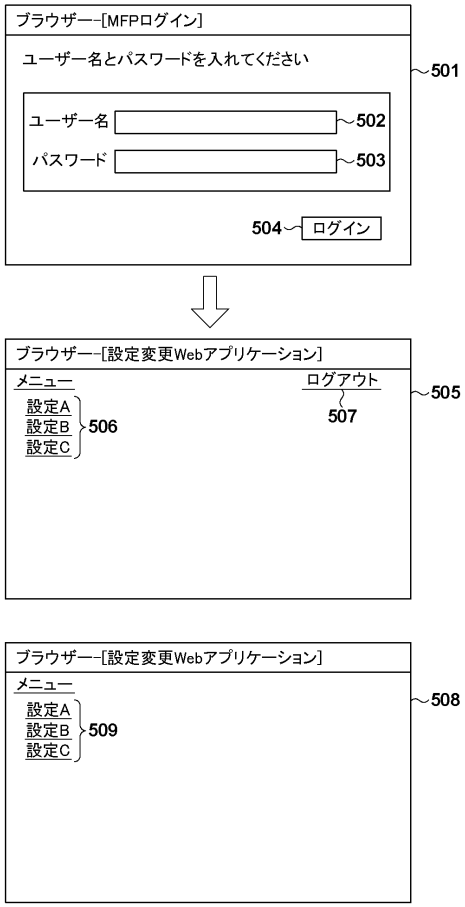
【図３】


301
メニュー管理部
302
HTTP通信部
303
Webブラウザー
304
ローカル
ログイン部
305
ユーザDB
306
リモート
ログイン部
307
セッション
管理部
308
ログイン部
309
ローカル
アクセス用
ページ
310
リモート
アクセス用
ページ
311
ロケーション
判定部
312
Webサーバー
313
101,103

【図４】


操作部-[MFPログイン]
ユーザー名とパスワードを入れてください
401
ユーザー名
402
パスワード
403
404
ログイン
操作部-[メインメニュー]
405
コピー
406
スキャン
407
ブラウザー
408
409
ログアウト

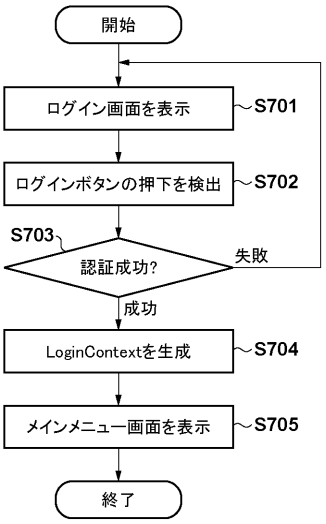
【図５】



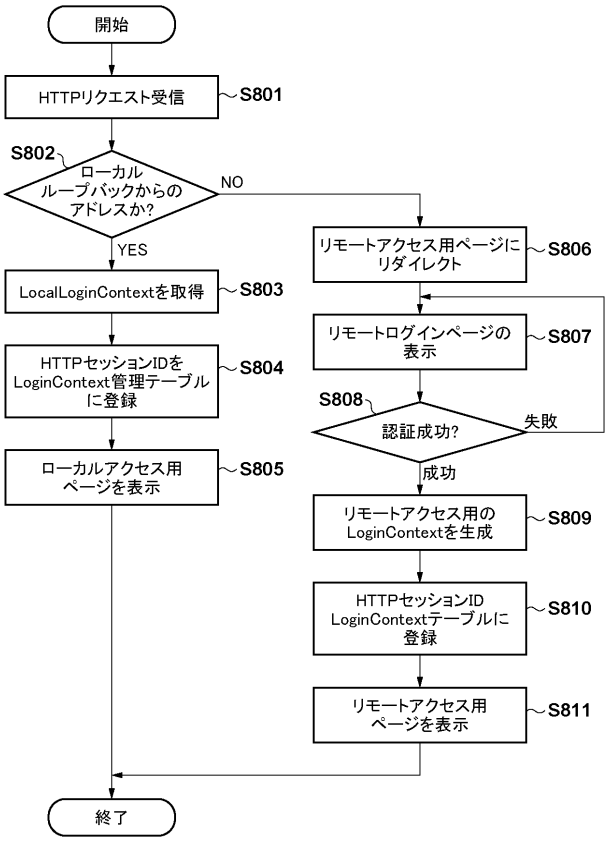
【図６】

601 LoginContextID	602 Type	603 UserID	604 SessionID
1	Local	User1	s1
2	Remote	User2	s2

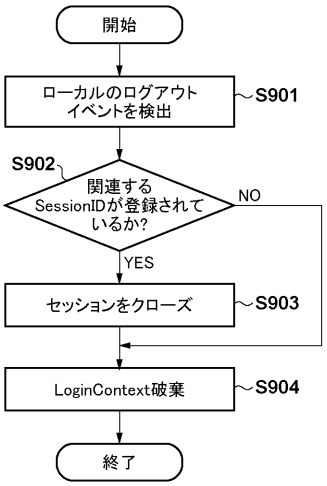
【図７】



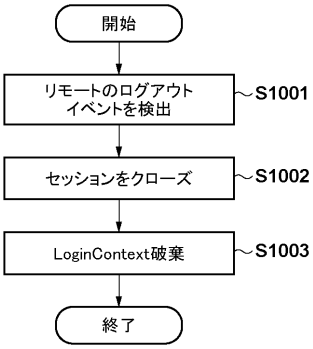
【図８】



【図９】



【図１０】


開始
リモートのログアウト
イベントを検出
S1001
セッションをクローズ
S1002
LoginContext破棄
S1003
終了

フロントページの続き

(72)発明者　安原　洋
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

Ｆターム(参考) 2C061 AP01　AP07　CL08　HK19　HN15　HP00　HQ01