(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7200776号
(P7200776)

(45)発行日　令和5年1月10日(2023.1.10)

(24)登録日　令和4年12月26日(2022.12.26)

(51)国際特許分類

Ｇ０６Ｆ　21/33　(2013.01)	Ｇ０６Ｆ	21/33	３５０
Ｇ０６Ｆ　21/31　(2013.01)	Ｇ０６Ｆ	21/31	
Ｇ０６Ｆ　21/45　(2013.01)	Ｇ０６Ｆ	21/45	

ＦＩ

請求項の数　14　（全24頁）

(21)出願番号　特願2019-50169(P2019-50169)
(22)出願日　平成31年3月18日(2019.3.18)
(65)公開番号　特開2020-154447(P2020-154447A)
(43)公開日　令和2年9月24日(2020.9.24)
審査請求日　令和4年2月28日(2022.2.28)

(73)特許権者　000005496
富士フイルムビジネスイノベーション株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110001519
弁理士法人太陽国際特許事務所
(72)発明者　新中 庸介
神奈川県横浜市西区みなとみらい六丁目１番 富士ゼロックス株式会社内
審査官　小林 秀和

最終頁に続く

(54)【発明の名称】　情報処理システム及びプログラム

(57)【特許請求の範囲】

【請求項１】

複数の情報処理装置を含み、利用者毎に付与された前記複数の情報処理装置間で共通の第１認証情報により各情報処理装置に対するアクセスが可能であり、且つ、アクセスされた情報処理装置から、特定のサービスに対して利用者毎に付与された第２認証情報により、前記サービスへのアクセスを許可する情報処理システムであって、

情報処理装置へのアクセスに用いた第１認証情報に対応し且つ前記サービスに対するアクセスを許可するための第１アクセス許可情報が記憶部に記憶されていない場合は、前記サービスにアクセスするための第２認証情報を入力する入力画面を表示する制御を行う表示制御部と、

前記第１アクセス許可情報が記憶部に記憶されている場合、及び、前記入力画面から入力された認証情報が予め定めた第２認証情報と一致する場合は、前記サービスに対するアクセスを許可すると共に、前記サービスに対する新たな第１アクセス許可情報を前記情報処理装置へのアクセスに用いた前記第１認証情報に対応付けて前記記憶部に記憶させる制御を行う記憶制御部と、

を備える情報処理システム。

【請求項２】

前記記憶制御部は、

取得された前記第１アクセス許可情報が正しい場合に、前記サービスに対するアクセスを許可する、

請求項１に記載の情報処理システム。
【請求項３】
前記記憶制御部は、
取得された前記第１アクセス許可情報から得られた有効期限付きの第２アクセス許可情報が正しい場合に、前記サービスに対するアクセスを許可する、
請求項１に記載の情報処理システム。
【請求項４】
前記情報処理システムは、
特定のサービスに対して特定の組織に所属する利用者に付与された第３認証情報により、前記記憶部に対するアクセスを許可する、
請求項１から請求項３までのいずれか１項に記載の情報処理システム。
【請求項５】
前記情報処理システムは、
前記第３認証情報から得られた有効期限付きの第３アクセス許可情報が正しい場合に、前記記憶部に対するアクセスを許可する、
請求項４に記載の情報処理システム。
【請求項６】
前記情報処理システムは、
前記複数の情報処理装置の外部に配置された第１記憶装置、及び前記複数の情報処理装置の各々に配置された第２記憶装置を含む複数の記憶装置を、前記記憶部として備える、
請求項１から請求項５までのいずれか１項に記載の情報処理システム。
【請求項７】
前記記憶制御部は、
前記特定のサービスが複数の機能を有する場合は、機能毎に異なる前記第１アクセス許可情報を記憶する、
請求項６に記載の情報処理システム。
【請求項８】
前記記憶制御部は、
前記特定のサービスが複数の機能を有する場合は、機能毎に前記第１アクセス許可情報を記憶する記憶装置を変更する、
請求項６または請求項７に記載の情報処理システム。
【請求項９】
前記記憶制御部は、
前記第１認証情報から生成した文字列に対応する値として前記第１アクセス許可情報を記憶する、
請求項１から請求項８までのいずれか１項に記載の情報処理システム。
【請求項１０】
前記文字列は、
前記第１認証情報に含まれる第１文字列、前記第１文字列のハッシュ値、前記第１認証情報に含まれる前記第１文字列とは異なる第２文字列、前記第２文字列のハッシュ値、前記第１文字列と前記第２文字列とを組み合わせた第３文字列、及び、前記第３文字列のハッシュ値のいずれか１つである、
請求項９に記載の情報処理システム。
【請求項１１】
前記記憶制御部は、
前記第１認証情報及び前記第３認証情報から生成した文字列に対応する値として前記第１アクセス許可情報を記憶する、
請求項４に記載の情報処理システム。
【請求項１２】
前記文字列は、

前記第１認証情報に含まれる文字列と前記第３認証情報に含まれる文字列とを組み合わせた第４文字列、及び、前記第４文字列のハッシュ値のいずれか１つである、
請求項１１に記載の情報処理システム。
【請求項１３】
前記表示制御部と前記記憶制御部とが、前記複数の情報処理装置の外部に配置される、
請求項１から請求項１２までのいずれか１項に記載の情報処理システム。
【請求項１４】
コンピュータを、請求項１から請求項１３までのいずれか１項に記載の情報処理システムの各部として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、情報処理システム及びプログラムに関する。
【背景技術】
【０００２】
特許文献１には、ユーザ端末を特定するための端末識別情報を記憶する手段と、セッションＩＤを生成し、ユーザ端末に対して、前記セッションＩＤを含んだＵＲＬ（Uniform Resource Locator）を送信する手段と、ユーザ端末から前記セッションＩＤを含んだＵＲＬによるリクエストを受け付ける度に、前記ユーザ端末から受信した端末識別情報を確認し、前記記憶しておいた端末識別情報と一致する場合に前記ユーザ端末の前記リクエストに応じ、前記記憶しておいた端末識別情報と一致しなかった場合は、前記リクエストを拒否する手段と、を備えるセッション管理装置が開示されている。
【０００３】
特許文献２には、画像形成装置と通信可能に配置されて利用者の識別情報である利用者情報による前記画像形成装置へのログインを許可するための画像形成装置用ログイン管理サーバであって、前記利用者情報による前記画像形成装置への前記ログインの依頼を受け付ける依頼受け付け手段と、前記依頼受け付け手段によって受け付けられた前記依頼に基づいて認証を実行する認証手段と、前記認証手段による認証が成功した前記依頼の対象の前記ログインを許可するか否かを決定するログイン手段と、前記ログイン手段によって許可されている前記ログインを記録する許可ログイン記録手段と、同一の前記利用者情報による前記画像形成装置への多重の前記ログインである同一情報多重ログインが許可されるための前記同一情報多重ログインのそれぞれの前記依頼の種類の組み合わせを設定する許可組み合わせ設定手段とを備えており、前記ログイン手段は、前記同一情報多重ログインのうち先の前記ログインである同一情報先ログインが前記許可ログイン記録手段によって記録されている場合に、前記同一情報先ログインの前記依頼の種類と、前記同一情報多重ログインのうち後の前記ログインである同一情報後ログインの前記依頼の種類との組み合わせが前記許可組み合わせ設定手段によって設定されているとき、前記同一情報後ログインを前記同一情報先ログインと多重に許可することを特徴とする画像形成装置用ログイン管理サーバが開示されている。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０１０-１３４６０２号公報
特開２０１３－０２９９０７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
情報処理システムは、複数の情報処理装置を含む。複数の情報処理装置の各々は、利用者毎に付与された複数の情報処理装置間で共通の認証情報により、各情報処理装置に対するアクセスが可能である。また、情報処理システムは、アクセスされた情報処理装置から

、特定のサービスに対して利用者毎に付与された第２認証情報により、特定のサービスに対するアクセスを許可する。

【０００６】

本発明の目的は、共通の第１認証情報でアクセスできる複数の情報処理装置のうちの１つの情報処理装置からの特定のサービスに対するアクセスが許可された場合には、他の情報処理装置から同じサービスにアクセスする際に、特定のサービスにアクセスするための第２認証情報の入力を省略することができる、情報処理システム及びプログラムを提供することにある。

【課題を解決するための手段】

【０００７】

第１態様に係る情報処理システムは、複数の情報処理装置を含み、利用者毎に付与された前記複数の情報処理装置間で共通の第１認証情報により各情報処理装置に対するアクセスが可能であり、且つ、アクセスされた情報処理装置から、特定のサービスに対して利用者毎に付与された第２認証情報により、前記サービスへのアクセスを許可する情報処理システムであって、情報処理装置へのアクセスに用いた第１認証情報に対応し且つ前記サービスに対するアクセスを許可するための第１アクセス許可情報が記憶部に記憶されていない場合は、前記サービスにアクセスするための第２認証情報を入力する入力画面を表示する制御を行う表示制御部と、前記第１アクセス許可情報が記憶部に記憶されている場合、及び、前記入力画面から入力された認証情報が予め定めた第２認証情報と一致する場合は、前記サービスに対するアクセスを許可すると共に、前記サービスに対する新たな第１アクセス許可情報を前記情報処理装置へのアクセスに用いた前記第１認証情報に対応付けて前記記憶部に記憶させる制御を行う記憶制御部と、を備える情報処理システムである。

【０００８】

第２態様に係る情報処理システムは、第１態様に係る情報処理システムにおいて、前記記憶制御部は、取得された前記第１アクセス許可情報が正しい場合に、前記サービスに対するアクセスを許可する。

【０００９】

第３態様に係る情報処理システムは、第１態様に係る情報処理システムにおいて、前記記憶制御部は、取得された前記第１アクセス許可情報から得られた有効期限付きの第２アクセス許可情報が正しい場合に、前記サービスに対するアクセスを許可する。

【００１０】

第４態様に係る情報処理システムは、第１態様から第３態様までのいずれか１つの情報処理システムにおいて、前記情報処理システムは、特定のサービスに対して特定の組織に所属する利用者に付与された第３認証情報により、前記記憶部に対するアクセスを許可する。

【００１１】

第５態様に係る情報処理システムは、第４態様に係る情報処理システムにおいて、前記情報処理システムは、前記第３認証情報から得られた有効期限付きの第３アクセス許可情報が正しい場合に、前記記憶部に対するアクセスを許可する。

【００１２】

第６態様に係る情報処理システムは、第１態様から第５態様までのいずれか１つの情報処理システムにおいて、前記情報処理システムは、前記複数の情報処理装置の外部に配置された第１記憶装置、及び前記複数の情報処理装置の各々に配置された第２記憶装置を含む複数の記憶装置を、前記記憶部として備える。

【００１３】

第７態様に係る情報処理システムは、第６態様に係る情報処理システムにおいて、前記記憶制御部は、前記特定のサービスが複数の機能を有する場合は、機能毎に異なる前記第１アクセス許可情報を記憶する。

【００１４】

第８態様に係る情報処理システムは、第６態様または第７態様に係る情報処理システム

において、前記記憶制御部は、前記特定のサービスが複数の機能を有する場合は、機能毎に前記第１アクセス許可情報を記憶する記憶装置を変更する。

【００１５】

第９態様に係る情報処理システムは、第１態様から第８態様までのいずれか１つの情報処理システムにおいて、前記記憶制御部は、前記第１認証情報から生成した文字列に対応する値として前記第１アクセス許可情報を記憶する。

【００１６】

第１０態様に係る情報処理システムは、第９態様に係る情報処理システムにおいて、前記文字列は、前記第１認証情報に含まれる第１文字列、前記第１文字列のハッシュ値、前記第１認証情報に含まれる前記第１文字列とは異なる第２文字列、前記第２文字列のハッシュ値、前記第１文字列と前記第２文字列とを組み合わせた第３文字列、及び、前記第３文字列のハッシュ値のいずれか１つである。

【００１７】

第１１態様に係る情報処理システムは、第４態様に係る情報処理システムにおいて、前記記憶制御部は、前記第１認証情報及び前記第３認証情報から生成した文字列に対応する値として前記第１アクセス許可情報を記憶する。

【００１８】

第１２態様に係る情報処理システムは、第１１態様に係る情報処理システムにおいて、前記文字列は、前記第１認証情報に含まれる文字列と前記第３認証情報に含まれる文字列とを組み合わせた第４文字列、及び、前記第４文字列のハッシュ値のいずれか１つである。

【００１９】

第１３態様に係る情報処理システムは、第１態様から第１２態様までのいずれか１つの情報処理システムにおいて、前記表示制御部と前記記憶制御部とが、前記複数の情報処理装置の外部に配置される。

【００２０】

第１４態様に係るプログラムは、コンピュータを、第１態様から第１３態様までのいずれか１つの情報処理システムの各部として機能させるためのプログラムである。

【発明の効果】

【００２１】

第１態様、第２態様、第１３態様、第１４態様に係る発明によれば、共通の第１認証情報でアクセスできる複数の情報処理装置のうちの１つの情報処理装置からの特定のサービスに対するアクセスが許可された場合には、他の情報処理装置から同じサービスにアクセスする際に、特定のサービスにアクセスするための第２認証情報の入力を省略することができる。

【００２２】

第３態様に係る発明によれば、サービスに対するアクセスを許可するための第２アクセス許可情報が有効期限付きで保存できない場合でも、有効期限のない第１アクセス許可情報を用いて新しい有効期限付きの第２アクセス許可情報を取得することができる。

【００２３】

第４態様に係る発明によれば、記憶部に対するアクセスを制限しない場合に比べて、第１アクセス許可情報に対するアクセスをセキュアに行うことができる。

【００２４】

第５態様に係る発明によれば、記憶部にアクセスすることができる利用者を、特定の組織に所属する利用者に制限することができる。

【００２５】

第６態様に係る発明によれば、記憶部を配置する場所によって記憶部に対するアクセスを制限することができる。

【００２６】

第７態様、第８態様に係る発明によれば、サービスの機能毎に、機能のセキュリティレベルに応じて、記憶部に対するアクセスを制限することができる。

【００２７】
第９態様、第１１態様に係る発明によれば、同じ第１アクセス許可情報が、複数の第１認証情報に対して重複して記憶されないようにすることができる。
【００２８】
第１０態様、第１２態様に係る発明によれば、認証情報を表す文字列にそのものに対応付けて第１アクセス許可情報を記憶する場合に比べて、第１アクセス許可情報に対するアクセスをセキュアに行うことができる。
【図面の簡単な説明】
【００２９】
【図１】本発明の実施の形態に係る情報処理システムの構成の一例を示す概略図である。
【図２】デバイスの電気的構成の一例を示すブロック図である。
【図３】要求受付部の電気的構成の一例を示すブロック図である。
【図４】第１実施の形態に係る情報処理システムの画面遷移図である。
【図５】第１実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【図６】第１実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【図７】第２実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【図８】第２実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【図９】第３実施の形態に係る情報処理システムの画面遷移図である。
【図１０】第３実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【図１１】機能毎にトークンの保存場所を記憶するテーブルの一例を示す図表である。
【図１２】トークンの保存場所のセキュリティレベルの違いを説明する図である。
【図１３】第３実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。
【発明を実施するための形態】
【００３０】
以下、図面を参照して本発明の実施の形態の一例を詳細に説明する。
【００３１】
＜第１実施の形態＞
本実施の形態に係る情報処理システムは、利用者が使用する複数の情報処理装置を含む。利用者には、複数の情報処理装置間で共通の第１認証情報が付与されている。第１認証情報は、複数の情報処理装置が利用者を識別するために利用者に付与する識別情報でもある。複数の情報処理装置の各々は、第１認証情報が取得された場合に、各情報処理装置へのアクセスを可能にする。
【００３２】
また、利用者は、アクセスされた情報処理装置から特定のサービスを利用可能である。利用者には、特定のサービスに対して第２認証情報が付与されている。第２認証情報は、特定のサービスについて利用者を識別するために利用者に付与する識別情報でもある。情報処理システムは、第２認証情報が取得された場合に、特定のサービスへのアクセスを許可する。
【００３３】
本実施の形態では、利用者は、アプリを利用して特定のサービスにアクセスする。アプリは、Ｗｅｂアプリケーションの略称である。アプリは、ネットワークを介してＷｅｂブラウザ上で動作するアプリケーション・ソフトウェアである。アプリは、Ｗｅｂブラウザ側のプログラムと、Ｗｅｂシステム側のプログラムとが協調することによって動作する。利用者は、Ｗｅｂブラウザが搭載された情報処理装置に、Ｗｅｂブラウザ側のプログラムをインストールして、アプリを利用する。
【００３４】
（情報処理システムの構成）
情報処理システムの構成の一例について説明する。

図１は本発明の実施の形態に係る情報処理システムの構成の一例を示す概略図である。本実施の形態では、情報処理システム１は、利用者が使用する複数の情報処理装置として、デバイス１０Ａとデバイス１０Ｂとを含む。デバイス１０Ａ及びデバイス１０Ｂの各々は、Ｗｅｂブラウザ２２を搭載している（図２参照）。デバイス１０Ａ及びデバイス１０Ｂの各々には、同じアプリ２４がインストールされている（図２参照）。アプリ２４のサービスを提供するＷｅｂシステムは、クラウド上に配置されている。

【００３５】

本実施の形態では、情報処理システム１は、アプリ２４のサービスを提供するＷｅｂシステムを含む。Ｗｅｂシステムは、アプリ２４に対してＡＰＩ（Application Programming Interface）を提供する。Ｗｅｂシステムは、例えば、要求受付部３０、トークン発行部４０、サービス部５０、及びトークン保存部６０を含む。Ｗｅｂシステムの各部は、各部のサービスを提供するサーバである。

【００３６】

要求受付部３０は、Ｗｅｂクライアントであるアプリ２４からの要求を受け付け、Ｗｅｂシステムの各部に処理を依頼する。各部は、依頼された処理を実行し、処理の結果をアプリ２４に返す。サービス部５０は、アプリ２４のサービスを提供する。トークン発行部４０は、サービス部５０へのアクセスに使用するトークンを発行する。トークン保存部６０は、トークン発行部４０で発行されたトークンを保存する。

【００３７】

デバイス１０Ａ及びデバイス１０Ｂの各々は、Ｗｅｂシステムの各部と通信回線７０を介して接続されている。デバイス１０Ａ及びデバイス１０Ｂの各々区別する必要がない場合は、デバイス１０と総称する。

【００３８】

本実施の形態では、情報処理システム１は、サービス部５０へのアクセスを、トークン発行部４０で発行されたトークンによりコントロールする。この点で、情報処理システム１による権限認可の仕組みは、RFC6749で定義されるOAuth2.0による権限認可の仕組みと類似する。

【００３９】

トークンは、サービスに対するアクセスを許可するためのアクセス許可情報の一例である。アクセス許可情報は、文字列で表される。本実施の形態では、アクセストークンとリフレッシュトークンという２種類のトークンを用いる例について説明する。以下では、アクセストークンを「Ａトークン」と略称し、リフレッシュトークンを「Ｒトークン」と略称する。

【００４０】

アクセストークン及びリフレッシュトークンの各々は、OAuth2.0で定義されている。本実施の形態に則して説明すると、Ａトークンは、サービス部５０に直接アクセスするために使用されるトークンである。Ｒトークンは、トークン発行部４０にＡトークンを発行してもらうために使用されるトークンである。

【００４１】

Ａトークンには、サービスへのアクセス権限（スコープ）が含まれる。例えば、デバイス上の複数のアプリについて、共通のアクセス権限を付与する。Ａトークンには、例えば約１５分等、短い有効期限が設定される。Ｒトークンには、有効期限が設定されていないか、または、Ａトークンの有効期限に比べて長い有効期限が設定されている。

【００４２】

トークン発行部４０で、Ａトークンを発行する際に、Ｒトークンも発行する。Ｒトークンは、トークン保存部６０に保存しておく。Ａトークンの有効期限が切れた場合には、Ｒトークンを用いて新しいＡトークンを取得する。

【００４３】

－デバイスの構成－

図２はデバイスの電気的構成の一例を示すブロック図である。

デバイス１０は、装置全体の制御及び各種演算を行うコンピュータである情報処理部１２を備えている。情報処理部１２は、ＣＰＵ１２Ａ、各種プログラムを記憶したＲＯＭ１２Ｂ、プログラムの実行時にワークエリアとして使用されるＲＡＭ１２Ｃ、不揮発性のメモリ１２Ｄ、及び入出力部１２Ｅを備えている。ＣＰＵ１２Ａ、ＲＯＭ１２Ｂ、ＲＡＭ１２Ｃ、メモリ１２Ｄ、及び入出力部１２Ｅの各々は、バス１２Ｆを介して接続されている。

【００４４】

デバイス１０は、マウス、キーボード等の入力部１４、ディスプレイ等の出力部１６、外部装置と通信を行うためのインターフェースである通信部１８、及びハードディスク等の外部記憶装置である記憶部２０を備えている。入力部１４、出力部１６、通信部１８、及び記憶部２０の各部は、入出力部１２Ｅに接続されている。情報処理部１２は、各部との間で情報の授受を行って、各部を制御する。

【００４５】

記憶部２０には、Ｗｅｂブラウザ２２、アプリ２４、テナントアカウント情報２６等が記憶されている。アプリ２４は、Ｗｅｂブラウザ側のプログラムである。なお、各種プログラムや各種データは、装置内外の他の記憶装置に記憶されていてもよく、ＣＤ－ＲＯＭ等の記録媒体に記録されていてもよい。また、各種プログラムや各種データは、通信を介して取得されてもよい。

【００４６】

－サーバの構成－

Ｗｅｂシステムに含まれる、要求受付部３０、トークン発行部４０、サービス部５０、及びトークン保存部６０の各々は、サービスを提供するサーバである。ここでは、要求受付部３０の電気的構成について説明する。サーバの電気的構成はどれも同じであるため、トークン発行部４０、サービス部５０、及びトークン保存部６０の各々については説明を省略する。

【００４７】

図３は要求受付部の電気的構成の一例を示すブロック図である。

要求受付部３０は、装置全体の制御及び各種演算を行うコンピュータである情報処理部３２を備えている。情報処理部３２は、ＣＰＵ３２Ａ、各種プログラムを記憶したＲＯＭ３２Ｂ、プログラムの実行時にワークエリアとして使用されるＲＡＭ３２Ｃ、不揮発性のメモリ３２Ｄ、及び入出力部３２Ｅを備えている。ＣＰＵ３２Ａ、ＲＯＭ３２Ｂ、ＲＡＭ３２Ｃ、メモリ３２Ｄ、及び入出力部３２Ｅの各々は、バス３２Ｆを介して接続されている。

【００４８】

要求受付部３０は、外部装置と通信を行うためのインターフェースである通信部３４、及びハードディスク等の外部記憶装置である記憶部３６を備えている。通信部３４及び記憶部３６の各部は、入出力部３２Ｅに接続されている。情報処理部３２は、各部との間で情報の授受を行って、各部を制御する。

【００４９】

（画面遷移）

次に、本実施の形態の概要を画面遷移図で説明する。

図４は第１実施の形態に係る情報処理システムの画面遷移図である。

－デバイスログイン－

まず、利用者はデバイスを利用可能にする。

利用者には、第１認証情報としてデバイスログイン情報が予め付与されている。デバイスログイン情報は、複数のデバイスの間で共通の情報である。デバイスログイン情報は、複数のデバイスの各々が利用者を識別するための情報である。デバイスは、利用者にデバイスログイン画面１００を表示して、利用者からのデバイスログイン情報の入力を受け付ける。デバイスログイン情報は、デバイスログイン用のユーザＩＤとパスワードである。デバイスがカード認証部を備える場合には、利用者が所持するＩＣカード等から、デバイスログイン情報を読み取るカード認証を行ってもよい。

【００５０】
図示した例では、デバイスログイン画面１００は、入力部１０２、入力部１０４、指示部１０６を備える。入力部１０２は、デバイスログイン用のユーザＩＤを入力する領域である。入力部１０４は、デバイスログイン用のパスワードを入力する領域である。指示部１０６は、実行を指示するボタンである。デバイスは、ユーザＩＤ及びパスワードが入力されて、実行が指示されると、認証処理を開始する。
【００５１】
デバイスは、利用者から取得された情報が、予め定めたデバイスログイン情報と一致する場合には、利用者のデバイスに対するアクセスを許可する。デバイスログイン情報は、デバイスの記憶装置に記憶される。デバイスは、機能を選択するためのデバイスメニュー画面２００を利用者に表示して、利用者からの機能の選択を受け付ける。
【００５２】
図示した例では、デバイスメニュー画面２００は、選択部２０２、アプリ選択部２０４、指示部２０６を備える。選択部２０２は、デバイスの機能を選択するボタンである。アプリ選択部２０４は、アプリを選択するボタンである。指示部２０６は、実行を指示するボタンである。アプリが選択されて実行が指示されると、アプリが起動される。ここで、起動されるアプリを「アプリＡ」とする。
【００５３】
－サービスログイン－
次に、利用者はアプリＡが提供するサービスを利用可能にする。
利用者には、アプリＡに固有の第２認証情報としてアカウント情報が予め付与されている。アカウント情報は、アプリが利用者を識別するための識別情報である。アカウント情報は、利用者が事前に登録したものでもよい。情報処理システムは、利用者にサービスログイン画面３００を表示して、利用者からのアカウント情報の入力を受け付ける。アカウント情報は、サービス用のユーザＩＤとパスワードである。
【００５４】
図示した例では、サービスログイン画面３００は、入力部３０２、入力部３０４、指示部３０６を備える。入力部３０２は、サービス用のユーザＩＤを入力する領域である。入力部３０４は、サービス用のパスワードを入力する領域である。指示部３０６は、実行を指示するボタンである。情報処理システムは、ユーザＩＤ及びパスワードが入力されて、実行が指示されると、認証処理を開始する。
【００５５】
情報処理システムは、利用者から取得された情報が、予め定めたアカウント情報と一致する場合には、利用者のサービスに対するアクセスを許可する。情報処理システムは、サービスの機能を選択するためのサービスメニュー画面４００を利用者に表示して、利用者からの機能の選択を受け付ける。
【００５６】
図示した例では、サービスメニュー画面４００は、選択部４０２、指示部４０４を備える。選択部４０２は、サービスの機能を選択するボタンである。指示部４０４は、実行を指示するボタンである。サービスの機能が選択されて実行が指示されると、情報処理システムは、サービスの機能に対するアクセスを許可する。
【００５７】
本実施の形態では、情報処理システムは、アプリＡが起動された際に、まずデバイスログイン情報を取得する。情報処理システムは、デバイスログイン情報に紐づくＲトークンがあるか否かを確認する。後述する通り、サービスにアクセスする度に、クラウド上のトークン保存部６０にＲトークンが保存される。利用者が複数のデバイスで同じアプリＡを利用する場合、いずれかのデバイスでアプリＡにログインしていれば、デバイスログイン情報に紐づくＲトークンが取得される。
【００５８】
Ｒトークンが取得できた場合は、情報処理システムは、サービスメニュー画面４００を

利用者に表示して、サービスに対するアクセスを許可する。Ｒトークンが取得できた場合は、サービスログイン画面３００の表示、アカウント情報の入力等、アプリＡが提供するサービスへのログインの手順が省略される。

【００５９】

（情報処理システムの動作）

次に、アプリ起動後の情報処理システムの動作について説明する。

アプリ２４の動作は、Ｗｅｂブラウザ側のプログラムの処理手順を表し、要求受付部３０、トークン発行部４０、サービス部５０、及びトークン保存部６０の動作は、Ｗｅｂシステム側のプログラムの処理手順を表す（図１参照）。

【００６０】

トークン発行部４０は、アカウント情報を記憶している。トークン保存部６０は、後述する通り、デバイスログイン情報に紐付けてＲトークンを記憶している。また、上記の通り、デバイスログイン情報は、デバイスの記憶装置に記憶されている。

【００６１】

ＷｅｂブラウザとＷｅｂシステムとはＨＴＴＰプロトコルを使用して通信を行う。Ｗｅｂブラウザは、要求内容を記述したＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。Ｗｅｂシステムは、要求を処理して、処理結果を記述したＨＴＴＰレスポンスを、Ｗｅｂブラウザに送信する。

【００６２】

ＨＴＴＰリクエスト及びＨＴＴＰレスポンスの各々は、ヘッダとボディとを有している。ヘッダは、通信に使用するソフトウェアの種類、データ形式、言語等の情報を含む。ボディは、送信されるメッセージ等を含む。トークンや認証情報は、ＨＴＴＰリクエストのヘッダ部に含まれる。

【００６３】

以下、Ｒトークンが取得できない場合と、Ｒトークンが取得できる場合とに分けて、アプリ起動後の情報処理システムの動作を説明する。

【００６４】

－Ｒトークンが取得できない場合－

図５は第１実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。アプリＡをはじめて利用する場合等、トークン保存部６０にＲトークンが保存されていなければ、Ｒトークンは取得できない。

【００６５】

ステップ１００で、アプリ２４は、利用者からアプリ起動の指示を受けてアプリを起動する。次にステップ１０２で、アプリ２４は、デバイスの記憶装置からデバイスログイン情報を取得する。次にステップ１０４で、アプリ２４は、Ｒトークンの取得を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにデバイスログイン情報を含む。

【００６６】

次にステップ１０６で、要求受付部３０は、トークン取得要求を受け付け、トークン保存部６０にトークン取得を依頼する。次にステップ１０８で、トークン保存部６０は、Ｒトークン取得処理を実行する。トークン保存部６０は、デバイスログイン情報に基づいてＲトークンを抽出する。ここでは、Ｒトークンが取得できない場合について説明する。トークン保存部６０は、Ｒトークンが抽出されない場合に、ＨＴＴＰレスポンスを送信して、抽出に失敗したことをアプリ２４に通知する。

【００６７】

トークン保存部６０は、デバイスログイン情報またはデバイスログイン情報から生成した情報をキーワードとして、キーとバリューとを対応付けるキーバリュー方式でトークンを記憶している。キーバリュー方式では、キーとバリューとが１対１で対応付けられ、キーワードとトークンとの組合せに重複がない。トークン保存部６０は、デバイスログイン情報からキーワードを生成し、生成したキーワードに対応するＲトークンをキーバリュー

方式で抽出する。

【００６８】

キーワードは、例えば、デバイスログイン用のユーザＩＤを表す第１文字列、デバイスログイン用のパスワードを表す第２文字列、第１文字列と第２文字列とを結合した第３文字列、ハッシュ関数を用いて各文字列から得られたハッシュ値などである。

【００６９】

次にステップ１１０で、アプリ２４は、サービスへのアクセスを要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。次にステップ１１２で、要求受付部３０は、サービスアクセス要求を受け付け、リダイレクトでトークン発行部４０に処理を依頼する。即ち、サービス部５０ではなく、まずトークン発行部４０に処理を依頼する。

【００７０】

次にステップ１１４で、トークン発行部４０は、サービスログイン画面（図４参照）を取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。次にステップ１１６で、アプリ２４は、サービスログイン画面を表示して、利用者からアカウント情報の入力を受け付ける。アカウント情報が入力されて、実行が指示されると、ステップ１１８に進む。

【００７１】

次にステップ１１８で、アプリ２４は、利用者からの指示に応じて、サービスへのアクセスに必要なＡトークンの発行を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにアカウント情報を含む。

【００７２】

次にステップ１２０で、要求受付部３０は、トークン発行要求を受け付け、トークン発行部４０に処理を依頼する。次にステップ１２２で、トークン発行部４０は、トークン発行処理を実行する。トークン発行部４０は、アカウント情報による認証を行い、利用者から取得された情報が予め記憶されたアカウント情報と一致する場合には、Ａトークンと新しいＲトークンとを発行する。トークン発行部４０は、処理結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。

【００７３】

Ａトークンを発行できる場合、即ち、認証に成功した場合は、処理結果に、トークン発行部４０により発行されたＡトークン及びＲトークンが含まれる。Ａトークンを発行できない場合、即ち、認証に失敗した場合は、処理結果に、認証に失敗した旨を表示する画面の画面データが含まれる。

【００７４】

認証に失敗した場合は、次にステップ１２４に進む。ステップ１２４では、アプリ２４は、認証に失敗した旨を表示する画面を処理結果として表示して、利用者にアカウント情報の再入力を促す。認証に成功した場合は、ステップ１２４を飛ばしてステップ１２６に進む。

【００７５】

次にステップ１２６で、アプリ２４は、新しいＲトークンの保存を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、デバイスログイン情報と新しいＲトークンとを含む。

【００７６】

次にステップ１２８で、要求受付部３０は、Ｒトークン保存要求を受け付け、トークン保存部６０に処理を依頼する。次にステップ１３０で、トークン保存部６０は、新しいＲトークンを、デバイスログイン情報に紐付けて記憶する。

【００７７】

次にステップ１３２で、アプリ２４は、サービスへのアクセスを要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにＡトークンを含む。次にステップ１３４で、要求受付部３０は、サービスアクセス要求を受け付け、サービス部５０に処理を依頼する。

【００７８】
次にステップ１３６で、サービス部５０は、まず、受信したＡトークンが正しいか否かを判定する。サービス部５０は、例えば、ＨＴＴＰリクエストのヘッダに含まれる他の文字列をキーとして受信したＡトークンを復号して、予め定めた文字列が得られる場合には、受信したＡトークンが正しいと判定する。
【００７９】
サービス部５０は、受信したＡトークンが正しいと判定した場合には、サービスへのアクセスを許可し、サービス用の画面を生成する処理を実行する。サービス部５０は、サービスメニュー画面（図４参照）を取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。
【００８０】
次にステップ１３８で、アプリ２４は、サービスメニュー画面を表示して、利用者からのサービス機能の選択を受け付ける。
【００８１】
なお、サービス部５０は、受信したＡトークンが正しくない場合は、サービスへのアクセスに失敗した旨を表示する画面の画面データを取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。アプリ２４は、サービスへのアクセスに失敗した旨を表示する画面を処理結果として表示して、利用者にアクセスのやり直しを促す。
【００８２】
－Ｒトークンが取得できた場合－
図６は第１実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。同じデバイスまたは異なるデバイスからアプリＡを使用したことがある場合は、トークン保存部６０にＲトークンが保存されおり、Ｒトークンを取得できる。
【００８３】
図６に示す動作は、ステップ１１０からステップ１１６までを含んでいない点以外は、図５に示す動作と同じであるため、相違点のみ説明する。
【００８４】
図５に示す動作では、ステップ１０８で、トークン保存部６０はＲトークンを抽出できなかったが、図６に示す動作では、ステップ１０８で、トークン保存部６０はＲトークンを抽出できる。トークン保存部６０は、Ｒトークンを含むＨＴＴＰレスポンスをアプリ２４に送信する。
【００８５】
図６に示すように、Ｒトークンを取得できた場合は、ステップ１１０からステップ１１６までの手順、即ち、サービスログイン画面を表示して、利用者からのアカウント情報の入力を受け付ける手順が省略される。
【００８６】
次にステップ１１８で、アプリ２４は、利用者からの指示に応じて、サービスへのアクセスに必要なＡトークンの発行を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにＲトークンを含む。
【００８７】
次にステップ１２０で、要求受付部３０は、トークン発行要求を受け付け、トークン発行部４０に処理を依頼する。次にステップ１２２で、トークン発行部４０は、トークン発行処理を実行する。
【００８８】
トークン発行部４０は、受信したＲトークンが正しいか否かを判定する。トークン発行部４０は、受信したＲトークンが正しいと判定した場合には、Ａトークン及び新しいＲトークンを発行する。トークン発行部４０は、処理結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。
【００８９】
本実施の形態では、トークン保存部６０にＲトークンを保存しておく例について説明し

たが、Ａトークンの有効期間が長い場合は、トークン保存部６０にＡトークンを保存しておいてもよい。

【００９０】

この場合は、図５及び図６のステップ１１０からステップ１１６までの処理でＡトークンが取得される。図５及び図６のステップ１１８からステップ１２４までの処理が省略される。ステップ１１６からステップ１２６に進む。図５及び図６のステップ１２６からステップ１３０までで、Ａトークンが保存される。

【００９１】

＜第２実施の形態＞

第２実施の形態では、事前にアプリにテナントアカウント情報を登録しておく。テナントアカウントは、企業等の組織単位でアプリを利用する場合等に、組織に属する利用者に付与される組織用のアカウントである。テナントアカウント情報は、組織用のアカウントのＩＤ及びパスワードを含む。

【００９２】

利用者には、アプリをインストールしたときに、第３認証情報としてテナントアカウント情報が予め付与されている。テナントアカウント情報は、利用者が使用するデバイスの記憶装置に記憶されると共に、クラウド上のトークン発行部４０の記憶装置にも記憶されている。

【００９３】

本実施の形態では、トークン保存部へのアクセスには、テナントアカウント用のトークン（以下、「テナント用トークン」という。）が必要である。アプリは、テナント用トークンを取得し、取得したテナント用トークンでトークン保存部にアクセスする。テナント用トークンを用いてアクセスすることで、トークン保存部へのアクセスがセキュアに行われる。

【００９４】

（情報処理システムの動作）

次に、情報処理システムの動作について説明する。

図７及び図８は第２実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。

【００９５】

－トークンの取得－

まず、トークンを取得する際に、テナント用トークンを使用する。図５及び図６のステップ１０４からステップ１０８までの手順が、図７に示すステップ２００からステップ２１２までの手順に置き換わる。その外の手順は図５及び図６と同じであるため、図示及び説明を省略する。

【００９６】

ステップ１００で、アプリ２４は、利用者からアプリ起動の指示を受けてアプリを起動する。次にステップ１０２で、アプリ２４は、デバイスの記憶装置に記憶されたデバイスログイン情報を読み出して、デバイスログイン情報を取得する。

【００９７】

次にステップ２００で、アプリ２４は、デバイスの記憶装置からテナントアカウント情報を取得する。次にステップ２０２で、アプリ２４は、テナント用のＡトークンの発行を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにテナントアカウント情報を含む。

【００９８】

次にステップ２０４で、要求受付部３０は、トークン発行要求を受け付け、トークン発行部４０にトークン発行を依頼する。次にステップ２０６で、トークン発行部４０は、トークン発行処理を実行する。トークン発行部４０は、テナントアカウント情報による認証を行い、利用者から取得された情報が予め記憶されたテナントアカウント情報と一致する場合には、テナント用Ａトークンを発行する。

【００９９】
トークン発行部４０は、処理結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。ＨＴＴＰレスポンスは、テナント用Ａトークンを含む。
【０１００】
次にステップ２０８で、アプリ２４は、Ｒトークンの取得を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにテナント用Ａトークンを含み、ボディにデバイスログイン情報を含む。
【０１０１】
次にステップ２１０で、要求受付部３０は、トークン取得要求を受け付け、トークン保存部６０にトークン取得を依頼する。次にステップ２１２で、トークン保存部６０は、Ｒトークン取得処理を実行する。まず、トークン保存部６０は、受信したテナント用Ａトークンが正しいか否かを判定する。
【０１０２】
受信したテナント用Ａトークンが正しいと判定した場合には、トークン保存部６０は、デバイスログイン情報に基づいてＲトークンを抽出する。Ｒトークンが抽出された場合は、トークン保存部６０は、Ｒトークンを含むＨＴＴＰレスポンスをアプリ２４に送信する。Ｒトークンが抽出されない場合は、トークン保存部６０は、ＨＴＴＰレスポンスを送信して、抽出に失敗したことをアプリ２４に通知する。
【０１０３】
－トークンの保存－
次に、トークンを保存する際に、テナント用トークンを使用する。
図５及び図６のステップ１２６からステップ１３０までの手順が、図８に示すステップ２２０からステップ２２４までの手順に置き換わる。その外の手順は図５及び図６と同じであるため、図示及び説明を省略する。
【０１０４】
ステップ２２０では、アプリ２４は、Ｒトークンの保存を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにテナント用Ａトークンを含み、ボディに、デバイスログイン情報、及びＲトークンを含む。
【０１０５】
次にステップ２２２で、要求受付部３０は、Ｒトークン保存要求を受け付け、トークン保存部６０に処理を依頼する。次にステップ２２４で、トークン保存部６０は、受信したテナント用Ａトークンが正しいか否かを判定する。トークン保存部６０は、受信したテナント用Ａトークンが正しいと判定した場合には、デバイスログイン情報に紐付けてＲトークンを記憶する。
【０１０６】
＜第３実施の形態＞
第３実施の形態では、サービスへのアクセスが許可された後も、サービスの機能毎に、各機能へのアクセスの許可が必要になる。また、サービスの機能のセキュリティレベルに応じて、トークンの保存場所を変更する。セキュリティレベルが高いほど、トークンの保存場所へのアクセスが制限される。第１実施の形態ではトークン保存部に保存していたが、第３実施の形態では、機能毎にトークンの保存場所を変更する。
【０１０７】
図１１は機能毎にトークンの保存場所を記憶するテーブルの一例を示す図表である。本実施の形態では、デバイスへのアクセスに用いたデバイスログイン情報に紐付けて、Ｒトークンを保存する。このテーブルは、クラウドの要求受付部３０の記憶装置に記憶されている。サービスの管理者は、このテーブルを書き換えて、機能毎のセキュリティレベルを変更してもよい。
【０１０８】
図１１に示す例では、サービスへのログイン用のＲトークンの保存場所は「クラウド」、機能Ａ用のＲトークンの保存場所は「デバイス」、機能Ｂ用のＲトークンは「保存しな

い」とされている。トークンを保存しない場合は、トークンを盗まれる可能性も無く最もセキュアである。

【０１０９】

図１２はトークンの保存場所のセキュリティレベルの違いを説明する図である。利用者１１が、デバイス１０Ａを使用してトークンを保存した後、別のデバイス１０Ｂを使用してトークンを取得する場合について説明する。

【０１１０】

保存場所が「クラウド」の場合、利用者１１は、クラウドのトークン保存部６０からトークンを取得する。保存場所が「クラウド」の場合、利用者１１が使用するどのデバイスからでも保存場所にアクセスできる。保存場所が「デバイス」の場合、利用者１１は、自装置のトークン保存部６２Ｂに保存されたトークンは取得できるが、他装置のトークン保存部６２Ａに保存されたトークンは取得できない。このため、保存場所を「デバイス」とした方が、保存場所を「クラウド」とするよりもセキュアである。

【０１１１】

（画面遷移）

次に、本実施の形態の概要を画面遷移図で説明する。

図９は第２実施の形態に係る情報処理システムの画面遷移図である。

【０１１２】

－サービスログイン－

サービスメニュー画面４００を表示するまでの手順は、第１実施の形態と同様である。

ログイン用のＲトークンは、第１実施の形態と同様のＲトークンである。本実施の形態では、情報処理システムは、アプリが起動されたときに、ログイン用のＲトークンが取得できた場合は、サービスメニュー画面４００を利用者に表示して、サービスに対するアクセスを許可する。この場合は、サービスログイン画面３００（図４参照）の表示、アカウント情報の入力等、アプリＡが提供するサービスへのログインの手順が省略される。

【０１１３】

－機能ログイン－

次に、利用者はサービス機能を利用可能にする。

情報処理システムは、サービスメニュー画面４００で機能Ａが選択されて実行が指示されると、機能Ａのサービスログイン画面５００を表示する。利用者には、機能Ａを利用するための第４認証情報が予め付与されている。ここでは、第４認証情報を、サービスログインのときと同じアカウント情報とする。情報処理システムは、利用者に機能Ａのサービスログイン画面５００を表示して、利用者からのアカウント情報の入力を受け付ける。

【０１１４】

図示した例では、機能Ａのサービスログイン画面５００は、入力部５０２、入力部５０４、指示部５０６を備える。入力部５０２は、サービス用のユーザＩＤを入力する領域である。入力部５０４は、サービス用のパスワードを入力する領域である。指示部５０６は、実行を指示するボタンである。情報処理システムは、ユーザＩＤ及びパスワードが入力されて、実行が指示されると、認証処理を開始する。

【０１１５】

情報処理システムは、利用者から取得された情報が、予め定めたアカウント情報と一致する場合には、利用者の機能Ａに対するアクセスを許可する。情報処理システムは、機能Ａの実行画面６００を利用者に表示する。機能Ａの実行画面６００は、機能Ａが実行中であることを示す画面等である。

【０１１６】

本実施の形態では、サービスの機能Ａが利用されたときに、機能Ａにアクセスするための機能Ａ用Ｒトークンが、クラウド上のトークン保存部６０に保存される。利用者が複数のデバイスで同じアプリＡを利用する場合、いずれかのデバイスでアプリＡの機能Ａを利用していれば、デバイスログイン情報に紐づく機能Ａ用Ｒトークンが取得される。

【０１１７】

Ｒトークンが取得できた場合は、情報処理システムは、サービスメニュー画面４００を利用者に表示して、サービスに対するアクセスを許可する。Ｒトークンが取得できた場合は、サービスログイン画面３００の表示、アカウント情報の入力等、アプリＡが提供するサービスへのログインの手順が省略される。利用者が複数のデバイスで同じアプリＡを利用する場合、いずれかのデバイスでアプリＡの機能Ａを利用していれば、デバイスログイン情報に紐づくＲトークンが取得される。

【０１１８】

Ｒトークンが取得できた場合は、情報処理システムは、サービスメニュー画面４００を利用者に表示して、サービスに対するアクセスを許可する。Ｒトークンが取得できた場合は、サービスログイン画面３００の表示、アカウント情報の入力等、アプリＡが提供するサービスへのログインの手順が省略される。

【０１１９】

本実施の形態では、情報処理システムは、サービスメニュー画面４００で機能Ａが選択された際に、機能Ａ用Ｒトークンが取得できた場合は、機能Ａの実行画面６００を利用者に表示して、利用者のサービスに対するアクセスを許可する。この場合は、情報処理システムは、機能Ａのサービスログイン画面５００の表示、アカウント情報の入力等、機能Ａへのログインの手順が省略される。

【０１２０】

（情報処理システムの動作）

次に、情報処理システムの動作について説明する。

－機能選択前の動作－

サービスメニュー画面４００（図９参照）で機能Ａを選択する前の動作について説明する。図１０は第３実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。図５及び図６のステップ１０６の手順が、図１０に示すステップ３００からステップ３０４までの手順に置き換わる。その以外の手順は図５及び図６と同じであるため、図示及び説明を省略する。

【０１２１】

ステップ１００で、アプリ２４は、利用者からアプリ起動の指示を受けてアプリを起動する。次にステップ１０２で、アプリ２４は、デバイスの記憶装置からデバイスログイン情報を取得する。次にステップ１０４で、アプリ２４は、ログイン用Ｒトークンの取得を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにデバイスログイン情報を含む。

【０１２２】

次にステップ３００で、要求受付部３０は、トークン取得要求を受け付ける。次にステップ３０２で、要求受付部３０は、図１１に示すテーブルを参照して、ログイン用トークンの保存場所を確認する。ログイン用トークンの保存場所は、トークン保存部６０である。次にステップ３０４で、要求受付部３０は、トークン保存部６０にトークン取得を依頼する。

【０１２３】

次にステップ１０８で、トークン保存部６０は、Ｒトークン取得処理を実行する。トークン保存部６０は、デバイスログイン情報に基づいてＲトークンを抽出する。トークン保存部６０は、抽出結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。

【０１２４】

－機能選択後の動作－

サービスメニュー画面４００（図９参照）で機能Ａを選択した後の動作について説明する。図１３は第３実施の形態に係る情報処理システムの動作の一例を示すシーケンス図である。ここでは、先ず、機能Ａ用Ｒトークンが取得できない場合の動作について説明する。

【０１２５】

－Ｒトークンが取得できない場合－

ステップ４００で、アプリ２４は、利用者による機能Ａの選択を受け付ける。次にステ

ップ４０２で、アプリ２４は、機能Ａ用Ｒトークンの取得を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにデバイスログイン情報を含む。なお、デバイスログイン情報は、ログインの際に既に取得されている。

【０１２６】

次にステップ４０４で、要求受付部３０は、トークン取得要求を受け付ける。次にステップ４０６で、要求受付部３０は、図１１に示すテーブルを参照して、機能Ａ用トークンの保存場所を確認する。機能Ａ用Ａトークンの保存場所は、自装置であるデバイスのトークン保存部６２とする。次にステップ４０８で、要求受付部３０は、アプリ２４にトークン取得を依頼する。要求受付部３０は、機能Ａ用トークンの保存場所を示す情報を含むＨＴＴＰレスポンスをアプリ２４に送信する。

【０１２７】

次にステップ４１０で、アプリ２４は、機能Ａ用Ｒトークン取得処理を実行する。アプリ２４は、デバイス内のトークン保存部６２にアクセスし、デバイスログイン情報に基づいて機能Ａ用Ｒトークンを抽出する。アプリ２４は、機能Ａ用Ｒトークンが取得できない場合には、ステップ４１２に進む。

【０１２８】

次にステップ４１２で、アプリ２４は、機能Ａへのアクセスを要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。次にステップ４１４で、要求受付部３０は、機能アクセス要求を受け付け、リダイレクトでトークン発行部４０に処理を依頼する。即ち、サービス部５０ではなく、まずトークン発行部４０に処理を依頼する。

【０１２９】

次にステップ４１６で、トークン発行部４０は、機能Ａのサービスログイン画面（図９参照）を取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。次にステップ４１８で、アプリ２４は、機能Ａのサービスログイン画面を表示して、利用者からアカウント情報の入力を受け付ける。アカウント情報が入力されて、実行が指示されると、ステップ４２０に進む。

【０１３０】

次にステップ４２０で、アプリ２４は、利用者からの指示に応じて、機能Ａへのアクセスに必要な、機能Ａ用Ａトークンの発行を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダにアカウント情報を含む。

【０１３１】

次にステップ４２２で、要求受付部３０は、トークン発行要求を受け付け、トークン発行部４０に処理を依頼する。次にステップ４２４で、トークン発行部４０は、機能Ａ用Ａトークンのトークン発行処理を実行する。

【０１３２】

トークン発行部４０は、アカウント情報による認証を行い、利用者から取得された情報が予め記憶されたアカウント情報と一致する場合には、機能Ａ用Ａトークンと新しい機能Ａ用Ｒトークンとを発行する。トークン発行部４０は、処理結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。なお、トークン発行部４０で発行された機能Ａ用Ａトークンは、サービス部５０の記憶装置に記憶される。

【０１３３】

認証に失敗した場合は、次にステップ４２６に進む。ステップ４２６では、アプリ２４は、認証に失敗した旨を表示する画面を処理結果として表示して、利用者にアカウント情報の再入力を促す。認証に成功した場合は、ステップ４２６を飛ばしてステップ４２８に進む。

【０１３４】

次にステップ４２８で、アプリ２４は、新しい機能Ａ用Ｒトークンを、デバイス内のトークン保存部６２に、デバイスログイン情報と紐付けて保存する。

【０１３５】

次にステップ４３０で、アプリ２４は、機能Ａへのアクセスを要求するＨＴＴＰリクエ

ストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダに機能Ａ用Ａトークンを含む。次にステップ４３２で、要求受付部３０は、機能アクセス要求を受け付け、サービス部５０に処理を依頼する。

【０１３６】

次にステップ４３４で、サービス部５０は、まず、受信した機能Ａ用Ａトークンが正しいか否かを判定する。サービス部５０は、受信した機能Ａ用Ａトークンが正しいと判定した場合には、機能Ａへのアクセスを許可し、機能Ａの実行画面を生成する処理を実行する。サービス部５０は、機能Ａの実行画面（図９参照）を取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。次にステップ４３６で、アプリ２４は、機能Ａの実行画面（図９参照）を表示する。

【０１３７】

なお、サービス部５０は、受信した機能Ａ用Ａトークンが正しくない場合は、機能Ａへのアクセスに失敗した旨を表示する画面の画面データを取得して、画面データを含むＨＴＴＰレスポンスをアプリ２４に送信する。アプリ２４は、機能Ａへのアクセスに失敗した旨を表示する画面を処理結果として表示して、利用者にアクセスのやり直しを促す。

【０１３８】

－Ｒトークンが取得できた場合－

図１３のステップ４１０で、機能Ａ用Ｒトークンが取得できた場合は、図１３に示すステップ４１２からステップ４１８までの手順（即ち、機能ログイン画面を表示して、利用者からのアカウント情報の入力を受け付ける手順）が省略される。トークン発行要求のＨＴＴＰリクエストのヘッダ部には、アカウント情報ではなく、機能Ａ用Ｒトークンが含まれる。

【０１３９】

次にステップ４２０で、アプリ２４は、利用者からの指示に応じて、機能Ａへのアクセスに必要な、機能Ａ用Ａトークンの発行を要求するＨＴＴＰリクエストを、Ｗｅｂシステムに送信する。ＨＴＴＰリクエストは、ヘッダに機能Ａ用Ｒトークンを含む。

【０１４０】

次にステップ４２２で、要求受付部３０は、トークン発行要求を受け付け、トークン発行部４０に処理を依頼する。次にステップ４２４で、トークン発行部４０は、トークン発行処理を実行する。

【０１４１】

トークン発行部４０は、受信した機能Ａ用Ｒトークンが正しいか否かを判定する。トークン発行部４０は、受信した機能Ａ用Ｒトークンが正しいと判定した場合には、機能Ａ用Ａトークン及び新しい機能Ａ用Ｒトークンを発行する。トークン発行部４０は、処理結果を含むＨＴＴＰレスポンスをアプリ２４に送信する。

【０１４２】

本実施の形態では、デバイスのトークン保存部６２に機能Ａ用Ｒトークンを保存しておく例について説明したが、第１実施の形態と同様に、Ａトークンの有効期間が長い場合は、トークン保存部６２に機能Ａ用Ａトークンを保存しておいてもよい。機能Ａ用Ａトークンを保存しておく場合には、図１３に示す手順のうち、機能Ａ用Ｒークンを用いて機能Ａ用Ａトークンを取得するための一部の手順が省略または変更される。

【０１４３】

＜変形例＞

なお、上記実施の形態で説明した情報処理装置、プログラム、及び情報処理システムの構成は一例であり、本発明の主旨を逸脱しない範囲内においてその構成を変更してもよいことは言うまでもない。

【０１４４】

上記実施の形態では、アプリケーションの処理をソフトウェアで実現する場合について説明したが、同等の処理をハードウェアで実現してもよい。

【０１４５】

上記の第３実施の形態では、機能毎にトークンの保存場所を記憶するテーブルが、クラウドの要求受付部の記憶装置に記憶されている例について説明したが、上記テーブルをデバイスの記憶装置に記憶しておいてもよい。この場合は、デバイスの管理者（例えば、利用者等）は、このテーブルを書き換えて、機能毎のセキュリティレベルを変更できる。

【０１４６】

上記の実施の形態では、クラウドのトークン保存部またはデバイスのトークン保存部にトークンを保存する例について説明したが、トークンの保存場所はこれ等に限定されない。トークンの保存場所は、複数のデバイスからアクセス可能なサーバの記憶装置であればよい。例えば、デバイスとイントラネットで接続されたサーバの記憶装置を、トークンの保存場所としてもよい。

【０１４７】

上記の実施の形態では、デバイスを、Ｗｅｂブラウザが搭載された画像形成装置としてもよい。アプリが提供するサービスの機能としては、クラウド上の記憶装置に記憶された文書を印刷する機能、画像形成装置のスキャナで読み取られた文書をクラウド上の記憶装置に格納する機能などがある。

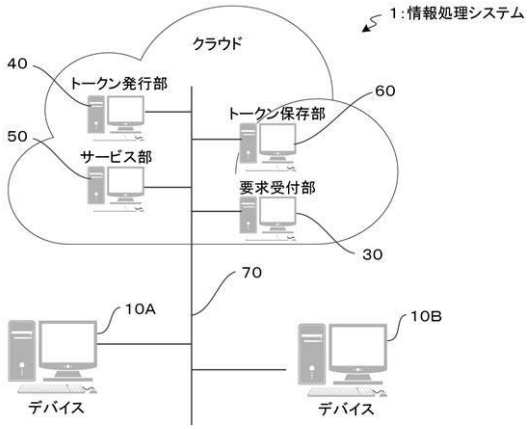
【符号の説明】

【０１４８】

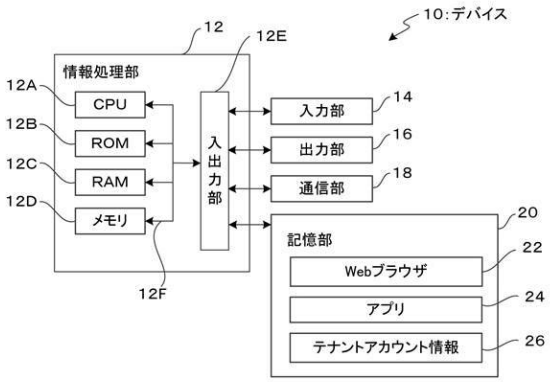
１　情報処理システム
１０　デバイス
１０Ａ デバイス
１０Ｂ デバイス
１１　利用者
１２　情報処理部
１４　入力部
１６　出力部
１８　通信部
２０　記憶部
２２　Ｗｅｂブラウザ
２４　アプリ
２６　テナントアカウント情報
３０　要求受付部
３２　情報処理部
３４　通信部
３６　記憶部
４０　トークン発行部
５０　サービス部
６０　トークン保存部
６２　トークン保存部
７０　通信回線
１００ デバイスログイン画面
２００ デバイスメニュー画面
３００ サービスログイン画面
４００ サービスメニュー画面
５００ サービスログイン画面
６００ 実行画面

【図面】

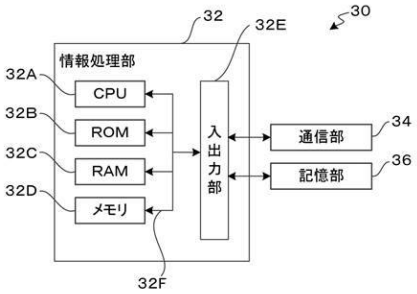
【図１】


1:情報処理システム
クラウド
40
トークン発行部
60
トークン保存部
50
サービス部
要求受付部
30
70
10A
10B
デバイス
デバイス

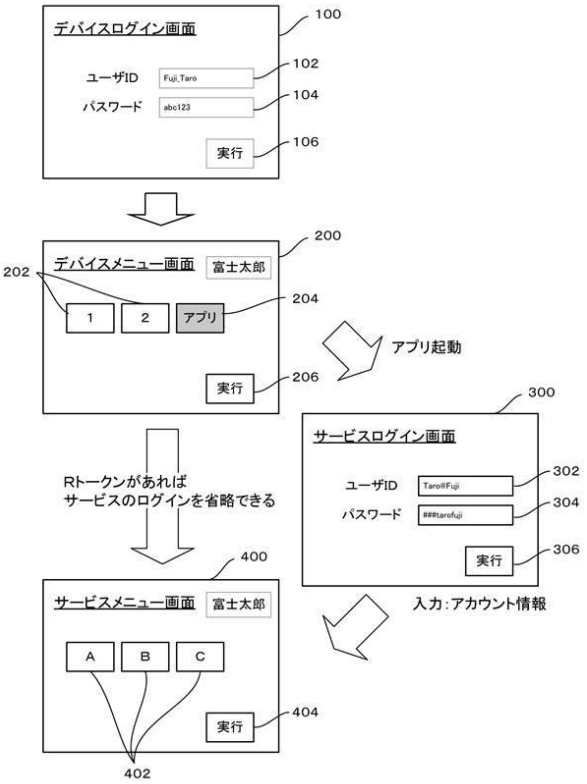
【図２】


10:デバイス
12
12E
情報処理部
12A
CPU
12B
ROM
12C
RAM
12D
メモリ
入出力部
12F
入力部
14
出力部
16
通信部
18
記憶部
20
Webブラウザ
22
アプリ
24
テナントアカウント情報
26

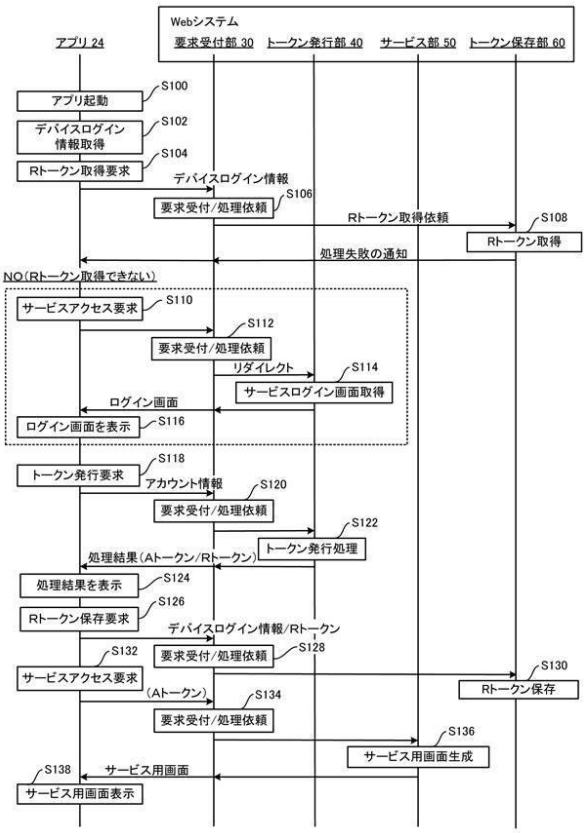
【図３】


32
32E
30
情報処理部
32A
CPU
32B
ROM
32C
RAM
32D
メモリ
入出力部
通信部
34
記憶部
36
32F

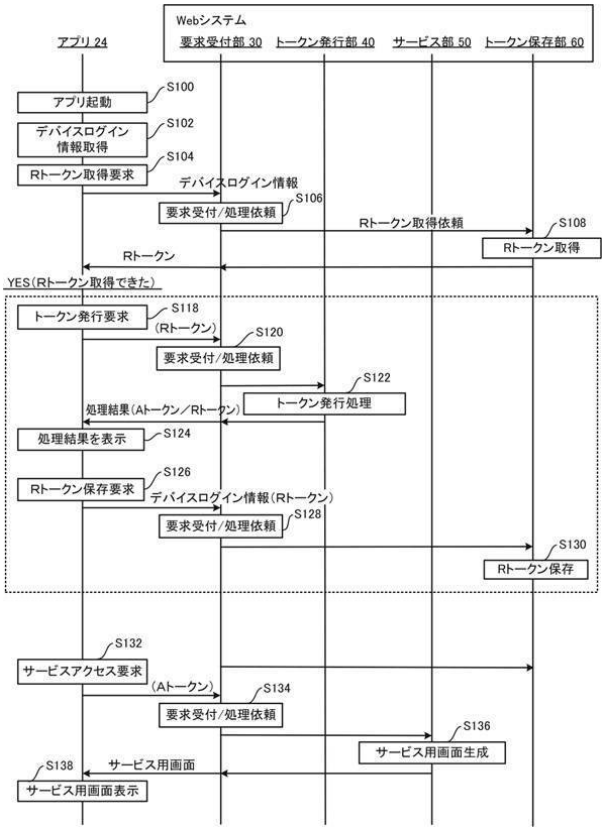
【図４】


デバイスログイン画面
100
ユーザID
Fuji_Taro
102
パスワード
abc123
104
実行
106
デバイスメニュー画面
富士太郎
200
202
1
2
アプリ
204
実行
206
アプリ起動
300
サービスログイン画面
ユーザID
Taro@Fuji
302
パスワード
###tarofuji
304
実行
306
入力:アカウント情報
Rトークンがあれば
サービスのログインを省略できる
400
サービスメニュー画面
富士太郎
A
B
C
実行
404
402

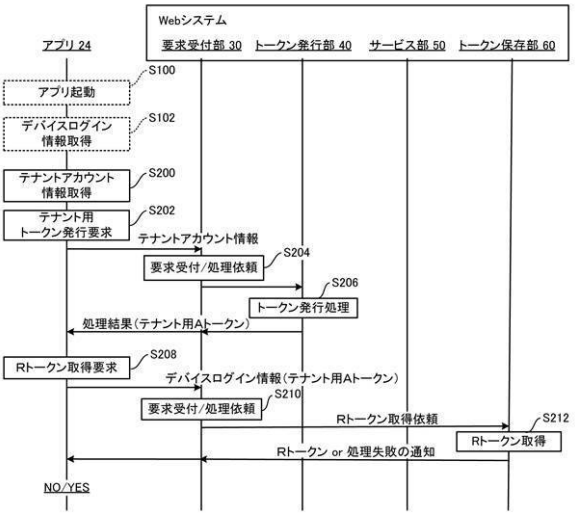
【図５】


Webシステム
アプリ 24
要求受付部 30
トークン発行部 40
サービス部 50
トークン保存部 60
アプリ起動
S100
デバイスログイン情報取得
S102
Rトークン取得要求
S104
デバイスログイン情報
要求受付/処理依頼
S106
Rトークン取得依頼
S108
Rトークン取得
処理失敗の通知
NO（Rトークン取得できない）
サービスアクセス要求
S110
要求受付/処理依頼
S112
リダイレクト
S114
サービスログイン画面取得
ログイン画面
ログイン画面を表示
S116
トークン発行要求
S118
アカウント情報
要求受付/処理依頼
S120
トークン発行処理
S122
処理結果（Aトークン/Rトークン）
処理結果を表示
S124
Rトークン保存要求
S126
デバイスログイン情報/Rトークン
要求受付/処理依頼
S128
サービスアクセス要求
S132
S130
Rトークン保存
（Aトークン）
要求受付/処理依頼
S134
S136
サービス用画面生成
S138
サービス用画面
サービス用画面表示

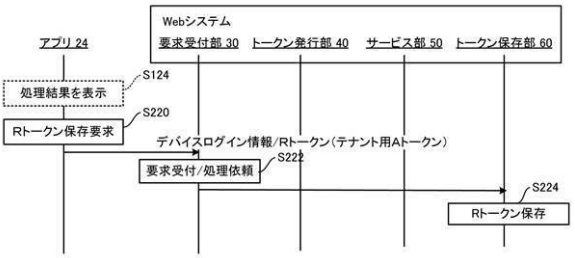
【図６】


Webシステム
アプリ 24
要求受付部 30
トークン発行部 40
サービス部 50
トークン保存部 60
アプリ起動
S100
デバイスログイン情報取得
S102
Rトークン取得要求
S104
デバイスログイン情報
要求受付/処理依頼
S106
Rトークン取得依頼
S108
Rトークン取得
Rトークン
YES（Rトークン取得できた）
トークン発行要求
S118
（Rトークン）
要求受付/処理依頼
S120
S122
トークン発行処理
処理結果（Aトークン/Rトークン）
処理結果を表示
S124
Rトークン保存要求
S126
デバイスログイン情報（Rトークン）
要求受付/処理依頼
S128
S130
Rトークン保存
S132
サービスアクセス要求
（Aトークン）
要求受付/処理依頼
S134
S136
サービス用画面生成
S138
サービス用画面
サービス用画面表示

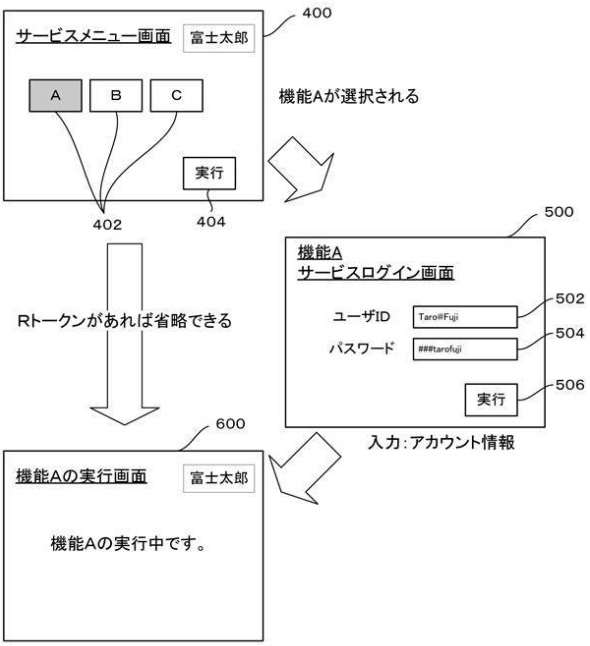
【図７】


Webシステム
アプリ 24
要求受付部 30
トークン発行部 40
サービス部 50
トークン保存部 60
アプリ起動
S100
デバイスログイン情報取得
S102
テナントアカウント情報取得
S200
テナント用トークン発行要求
S202
テナントアカウント情報
要求受付/処理依頼
S204
S206
トークン発行処理
処理結果（テナント用Aトークン）
Rトークン取得要求
S208
デバイスログイン情報（テナント用Aトークン）
要求受付/処理依頼
S210
Rトークン取得依頼
S212
Rトークン取得
Rトークン or 処理失敗の通知
NO/YES

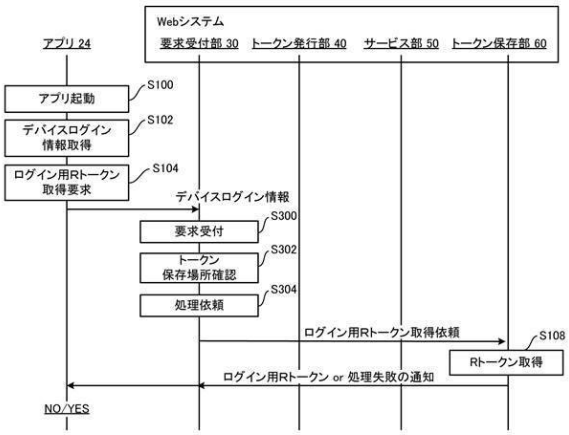
【図８】


Webシステム
アプリ 24
要求受付部 30
トークン発行部 40
サービス部 50
トークン保存部 60
処理結果を表示
S124
Rトークン保存要求
S220
デバイスログイン情報/Rトークン（テナント用Aトークン）
要求受付/処理依頼
S222
S224
Rトークン保存

【図９】



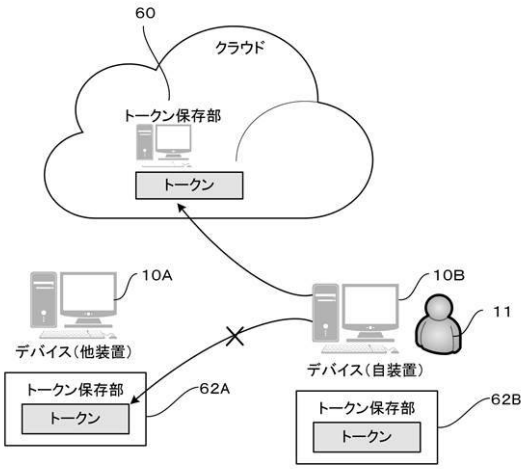
【図１０】



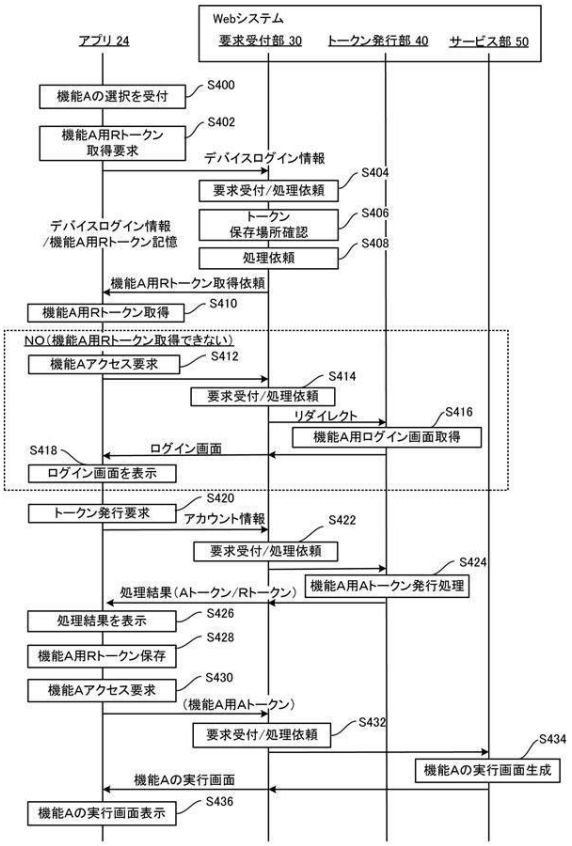
【図１１】

機能	保存場所
ログイン	クラウド
機能 A	デバイス
機能 B	保存しない

【図１２】



【図１３】


Webシステム
アプリ 24
要求受付部 30
トークン発行部 40
サービス部 50
機能Aの選択を受付
S400
機能A用Rトークン
取得要求
S402
デバイスログイン情報
S404
要求受付/処理依頼
トークン
保存場所確認
S406
デバイスログイン情報
/機能A用Rトークン記憶
S408
処理依頼
機能A用Rトークン取得依頼
機能A用Rトークン取得
S410
NO(機能A用Rトークン取得できない)
機能Aアクセス要求
S412
S414
要求受付/処理依頼
リダイレクト
S416
機能A用ログイン画面取得
S418
ログイン画面
ログイン画面を表示
トークン発行要求
S420
アカウント情報
S422
要求受付/処理依頼
S424
機能A用Aトークン発行処理
処理結果(Aトークン/Rトークン)
処理結果を表示
S426
機能A用Rトークン保存
S428
機能Aアクセス要求
S430
(機能A用Aトークン)
要求受付/処理依頼
S432
S434
機能Aの実行画面生成
機能Aの実行画面
機能Aの実行画面表示
S436

フロントページの続き

(56)参考文献　国際公開第２０１３／１４５５１７（WO，Ａ１）
特開２００７－１７９３９０（ＪＰ，Ａ）
特開２０１４－０９２８２３（ＪＰ，Ａ）
米国特許出願公開第２０１５／０１８０８５９（ＵＳ，Ａ１）
特開２０１０－１１３４６２（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／４５