(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6859195号
(P6859195)
(45)発行日　令和3年4月14日(2021.4.14)　(24)登録日　令和3年3月29日(2021.3.29)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
G06F 13/00 (2006.01)　　G06F 13/00　３５７Ａ

請求項の数 9　(全 31 頁)

(21)出願番号　特願2017-98378(P2017-98378)
(22)出願日　平成29年5月17日(2017.5.17)
(65)公開番号　特開2018-195080(P2018-195080A)
(43)公開日　平成30年12月6日(2018.12.6)
審査請求日　令和2年5月15日(2020.5.15)

(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　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　菅原　彬
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　宮司　卓佳

最終頁に続く

(54)【発明の名称】情報処理システム、制御方法及びそのプログラム

(57)【特許請求の範囲】
【請求項１】
クラウドサービスを利用するクラウドユーザーを一意に識別するためのクラウドユーザー認証情報と、デバイスの機能を利用するローカルユーザーを一意に識別するためのローカルユーザー認証情報と、を管理するクラウドシステムと、
前記クラウドユーザー認証情報と前記ローカルユーザー認証情報とを管理する前記デバイスと、
リクエストを前記クラウドシステムに送信するクライアントデバイスと、
を含む情報処理システムであって、
前記クラウドシステムは、
前記クライアントデバイスからリクエストを受信したことに応じて、前記デバイスの機能を利用するための実行要求、および前記リクエストを送信したユーザーの前記ローカルユーザー認証情報を前記デバイスに送信し、
前記デバイスは、
前記実行要求に基づく処理の実行結果、および前記ローカルユーザー認証情報に対応する前記クラウドユーザー認証情報を前記クラウドシステムに送信することを特徴とする情報処理システム。
【請求項２】
前記クラウドユーザー認証情報は、
前記クラウドユーザーを一意に識別し、他のクラウドユーザー認証情報と重複すること

のないクラウドユーザーＵＵＩＤであり、
前記ローカルユーザー認証情報は、
前記ローカルユーザーを一意に識別し、他のローカルユーザー認証情報と重複することのないローカルユーザーＵＵＩＤであることを特徴とする請求項１記載の情報処理システム。
【請求項３】
前記クラウドシステムは、
前記クラウドユーザー認証情報と前記クラウドユーザー認証情報とを紐付けるための認証連携情報を介して前記クラウドユーザー認証情報と前記ローカルユーザー認証情報とを紐付けたクラウド紐付け情報を管理し、
前記デバイスは、
前記認証連携情報を介して前記クラウドユーザー認証情報と前記ローカルユーザー認証情報とを紐付けたデバイス紐付け情報を管理することを特徴とする請求項１から請求項２のいずれか一つに記載の情報処理システム。
【請求項４】
前記認証連携情報は、
ユーザーが前記クライアントデバイスにログインし、前記認証連携情報を発行するための発行要求が前記クラウドシステムに送信されたことで、前記クラウドシステムが前記認証連携情報を発行することを特徴とする請求項３に記載の情報処理システム。
【請求項５】
前記認証連携情報は、
前記ユーザーが前記デバイスにログインし、前記認証連携情報を発行するための発行要求が前記クラウドシステムに送信されたことで、前記クラウドシステムが前記認証連携情報を発行されることを特徴とする請求項３に記載の情報処理システム。
【請求項６】
前記クラウドシステムは、
前記クラウド紐付け情報に対して紐付けられた暗号鍵を用いて、前記デバイスの機能を実行するための実行要求に署名情報を付与して前記デバイスに送信し、前記デバイスにおいて該署名情報が検証されることを特徴とする請求項３から請求項５のいずれか一つに記載の情報処理システム。
【請求項７】
前記デバイスは、
前記デバイス紐付け情報に対して紐付けられた暗号鍵を用いて、前記実行結果に前記署名情報を付与して前記クラウドシステムに送信し、前記クラウドシステムにおいて該署名情報が検証されることを特徴とする請求項６に記載の情報処理システム。
【請求項８】
前記情報処理システムは、
前記デバイスが、前記ユーザーによるログイン操作を必要とするマルチユーザーデバイスか、前記ログイン操作を必要としないシングルユーザーデバイスであるかを判定する判定手段をさらに有し、
前記判定手段によって前記デバイスが前記シングルユーザーデバイスと判定された場合、
前記クラウドシステムは、
前記クラウドユーザー認証情報と前記実行要求とを前記デバイスに送信し、
前記デバイスは、
前記実行要求を実行したことで得られた前記実行結果と、前記実行要求とともに受信したクラウドユーザー認証情報とを前記クラウドシステムに送信することを特徴とする請求項１から請求項７のいずれか一つに記載の情報処理システム。
【請求項９】
クラウドサービスを利用するクラウドユーザーを一意に識別するためのクラウドユーザ

ー認証情報と、デバイスの機能を利用するローカルユーザーを一意に識別するためのローカルユーザー認証情報と、を管理するクラウドシステムと、
前記クラウドユーザー認証情報と前記ローカルユーザー認証情報とを管理する前記デバイスと、
リクエストを前記クラウドシステムに送信するクライアントデバイスと、
を含む情報処理システムの制御方法であって、
前記クラウドシステムは、
前記クライアントデバイスからリクエストを受信したことに応じて、前記デバイスの機能を利用するための実行要求、および前記リクエストを送信したユーザーの前記ローカルユーザー認証情報を前記デバイスに送信し、
前記デバイスは、
前記実行要求に基づく処理の実行結果、および前記ローカルユーザー認証情報に対応する前記クラウドユーザー認証情報を前記クラウドシステムに送信することを特徴とする情報処理システムの制御方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クラウドシステムを介してデバイスの機能を実行する情報処理システム、制御方法及びそのプログラムに関するものである。
【背景技術】
【０００２】
クライアントデバイスからクラウドシステムを介して他のデバイスにデータを送信するようなサービスが出てきている。また、デバイスの機能を利用するユーザー（以下、ローカルユーザー）を識別し、そのユーザーが利用できるデバイスの機能を制限するために、ローカルユーザーアカウントを設けるデバイスがある。このようなデバイスにおいてデバイスの機能を実行するためには、ローカルユーザーアカウントが必要となる。一方、クラウドシステムにおいてクラウドサービスを利用するユーザー（以下、クラウドユーザー）を識別し、そのユーザーが利用できるクラウドサービスを制限するために、クラウドユーザーアカウントを設けるクラウドシステムがある。このようなクラウドシステムにおいてクラウドサービスを実行するためには、クラウドユーザーアカウントが必要となる。
【０００３】
特許文献１には、ユーザーアカウント情報によってユーザーが認証された場合に、印刷ジョブの印刷を実行する印刷システムについて開示している。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１６－１８３３１
【発明の概要】
【発明が解決しようとする課題】
【０００５】
一人のユーザーが、デバイスにおいてデバイスの機能を利用するためにローカルユーザーアカウントを登録し、クラウドシステムにおいてクラウドサービスを利用するためにクラウドユーザーアカウントを登録しているものとする。両方のユーザーアカウントを用いて、クラウドサービスの一つであるＭＦＰ等のマルチユーザーデバイスの機能の実行を要求し、要求された機能がマルチユーザーデバイスにおいて実行され、その実行結果がマルチユーザーデバイスからクラウドシステムに送信される形態が考えられる。ここでマルチユーザーデバイスとは、複数のローカルユーザーを管理する機能を有し、デバイスの機能を用いる際にログイン操作を必要とするデバイスのことである。
【０００６】
ローカルユーザーアカウントとクラウドユーザーアカウントとを用いて、マルチユーザ

ーデバイスの機能の実行を要求し、その実行要求に対する実行結果がクラウドシステムに送信される形態において、マルチユーザーデバイスがクラウドシステムから実行要求をｐｕｌｌ型通信によって取得し、その実行要求に対する実行結果をマルチユーザーデバイスがクラウドシステムに対し送信する場合がある。ｐｕｌｌ型通信は、マルチユーザーデバイスがクラウドシステムに対して実行要求の取得をリクエストし、そのレスポンスとしてマルチユーザーデバイスが実行要求をクラウドシステムから受信することで通信が終了する。そのため、その実行結果をマルチユーザーデバイスからクラウドシステムに送信しても、実行要求を取得したｐｕｌｌ型通信と実行結果を送信する通信は互いに独立した非同期通信であるため、どの実行要求に対してどのような実行結果が得られたのかをクラウドシステムでは判断できない。つまり、どのリクエスト（実行要求）に対するレスポンス（実行結果）なのかを知るために、リクエストとレスポンスとを紐付ける手段が必要となる。

【０００７】

本発明では、クラウドシステムを介してマルチユーザーデバイスの機能を実行する際に、その機能を実行するために必要なローカルユーザーアカウントをマルチユーザーデバイスで特定し、その実行結果がどのクラウドユーザーアカウントに対するものなのかをクラウドシステムで特定し、リクエストとレスポンスとを紐付けることを目的とする。

【課題を解決するための手段】

【０００８】

クラウドサービスを利用するクラウドユーザーを一意に識別するためのクラウドユーザー認証情報と、デバイスの機能を利用するローカルユーザーを一意に識別するためのローカルユーザー認証情報と、を管理するクラウドシステムと、前記クラウドユーザー認証情報と前記ローカルユーザー認証情報とを管理する前記デバイスと、リクエストを前記クラウドシステムに送信するクライアントデバイスと、を含む情報処理システムであって、前記クラウドシステムは、前記クライアントデバイスからリクエストを受信したことに応じて、前記デバイスの機能を利用するための実行要求、および前記リクエストを送信したユーザーの前記ローカルユーザー認証情報を前記デバイスに送信し、前記デバイスは、前記実行要求に基づく処理の実行結果、および前記ローカルユーザー認証情報に対応する前記クラウドユーザー認証情報を前記クラウドシステムに送信することを特徴とする。

【発明の効果】

【０００９】

本発明により、クラウドシステムを介してマルチユーザーデバイスの機能を実行する際に、その機能を実行するために必要なローカルユーザーアカウントをマルチユーザーデバイスで特定し、その実行結果がどのクラウドユーザーアカウントに対するものなのかをクラウドシステムで特定し、リクエストとレスポンスとを紐付けることができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の情報処理システムの全体図である。

【図２】情報処理装置２００の内部構成図である。

【図３】情報処理システム１０７を構成する各装置とクライアントデバイス１０２の機能ブロック図である。

【図４】認証サーバー１０３がデバイス１０５を認証する過程を示すシーケンス図である。

【図５】認証連携情報を発行する過程を示すシーケンス図である。

【図６】認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理を示すシーケンス図である。

【図７】デバイス１０５におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理を示すシーケンス図である。

【図８】デバイス１０５における機能呼び出し処理を示すシーケンス図である。

【図９】Ｗｅｂブラウザ３００の設定画面の図である。

【図１０】Ｗｅｂブラウザ３００の実行結果画面の図である。
【図１１】Ｗｅｂブラウザ３００の実行結果選択画面の図である。
【図１２】結果取得処理のフロー図である。
【図１３】共通鍵を用いた場合の、デバイス１０５におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理を示すシーケンス図である。
【図１４】共通鍵を用いた場合の、デバイス１０５における機能呼び出し処理を示すシーケンス図である。
【図１５】シングルユーザーデバイスの場合の、認証連携情報を発行する過程を示すシーケンス図である。
【図１６】シングルユーザーデバイスの場合の、デバイス１０５における機能呼び出し処理を示すシーケンス図である。
【図１７】クライアントデバイス１０２における認証連携情報を発行する過程を示すシーケンス図である。
【図１８】デバイス１０５におけるローカルユーザーＵＵＩＤと認証連携情報とを紐付けるユーザー紐付け処理を示すシーケンス図である。
【図１９】認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け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】
【００１１】
以下、本発明を実施するための最良の形態について実施例を用いて説明する。
【００１２】
図１を用いて、本発明の実施形態に係る情報処理システム１０７を構成するデバイス１０５とクラウドシステム１０６、さらに情報処理システム１０７に接続するクライアントデバイス１０２について説明する。図１では、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１００を経由してクライアントデバイス１０２が、情報処理システム１０７を構築するサーバーコンピューター群とデバイス１０５とを接続している状態が示されている。ＷＡＮ　１００はＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１０１によって各デバイスと接続されている。
【００１３】
クライアントデバイス１０２はＰＣやスマードフォン、タブレット、画像形成装置等の情報処理装置である。認証サーバー１０３は、クラウドユーザーやローカルユーザー等のユーザーや、ＭＦＰ等のデバイス１０５を認証し、その認証情報を登録する。
【００１４】
サービスサーバー１０４は、ＷＡＮ１００を経由してクライアントデバイス１０２とデバイス１０５と通信可能であり、Ｍｅｓｓａｇｅ　Ｑｕｅｕｉｎｇ　Ｔｅｌｅｍｅｔｒｙ　Ｔｒａｎｓｐｏｒｔ　（ＭＱＴＴ）　Ｂｒｏｋｅｒによるメッセージ通信を行うサーバー等が挙げられる。ＭＱＴＴとはｐｕｂｌｉｓｈ／ｓｕｂｓｃｒｉｂｅモデルのメッセージ通信プロトコルである。ｐｕｂｌｉｓｈ／ｓｕｂｓｃｒｉｂｅモデルは、メッセージ送信者（以下、ｐｕｂｌｉｓｈｅｒ）からメッセージ受信者（以下、ｓｕｂｓｃｒｉｂｅｒ）に対して、メッセージ仲介者であるＭＱＴＴ　ｂｒｏｋｅｒを介してメッセージを配信する。実施例では、サービスサーバー１０４がＭＱＴＴ　ｂｒｏｋｅｒの機能を有するものとして説明する。ｓｕｂｓｃｒｉｂｅｒは、メッセージの送信先（以下、トピック）としてｓｕｂｓｃｒｉｂｅｒ自身を指定してメッセージをサービスサーバー１０４に送信し、そのトピックと一致したメッセージをサービスサーバー１０４から受信できるように予約する（以下、ｓｕｂｓｃｒｉｂｅ）。ｓｕｂｓｃｒｉｂｅするためにｓｕｂｓｃｒｉｂｅｒがサービスサーバー１０４に送信するメッセージをｓｕｂｓｃｒｉｂｅメッセージと呼ぶ。
【００１５】
ｐｕｂｌｉｓｈｅｒは、サービスサーバー１０４に対してトピックを指定したメッセージを送信する。サービスサーバー１０４は、そのトピックと同じトピックをｓｕｂｓｃｒ

ｉｂｅしているｓｕｂｓｃｒｉｂｅｒに対してメッセージを配信する（以下、ｐｕｂｌｉｓｈ）。ｐｕｂｌｉｓｈｅｒがｐｕｂｌｉｓｈするためにトピックを指定してサービスサーバー１０４に送信するメッセージ、およびｓｕｂｓｃｒｉｂｅｒに送信されるメッセージを、ｐｕｂｌｉｓｈメッセージを呼ぶ。

【００１６】

トピックは「／」で区切られた階層構造（例：／Ａ／ＢＣ／Ｄ／Ｅ）になっており、トピックの完全一致または一部一致をｓｕｂｓｃｒｉｂｅｒ側で指定することで、指定した条件に合ったトピックのメッセージをｓｕｂｓｃｒｉｂｅｒが受信できる。ＭＱＴＴ　ｂｒｏｋｅｒは、受信したｐｕｂｌｉｓｈメッセージのトピックとｓｕｂｓｃｒｉｂｅメッセージのトピックとの一致不一致を確認しており、一致した場合はｐｕｂｌｉｓｈメッセージをｓｕｂｓｃｒｉｂｅｒに送信する。これにより、ファイヤーウォールでサービスサーバー１０４からデバイス１０５への通信が遮断されていても、ＭＱＴＴを用いることでデバイス１０５への通信が可能となる。

【００１７】

後述の実施例は、サービスサーバー１０４がＭＱＴＴ　ｂｒｏｋｅｒの機能を有するものとして説明するが、デバイス１０５がサービスサーバー１０４からリクエストを取得できれば、他のプロトコルを用いた形態でもよい。例えば、デバイス１０５がサービスサーバー１０４に対して定期的に情報取得のためのリクエストを行い、そのレスポンスでサービスサーバー１０４からのリクエストを受信する形態も考えられる。

【００１８】

さらに、サービスサーバー１０４はクライアントデバイス１０２に対して、設定変更サービス等のサービスを提供する。設定変更サービスでは、デバイス１０５における設定変更を受け付けるための画面やクラウドユーザーが要求した設定変更結果を確認する画面をクライアントデバイス１０２に提供する。クライアントデバイス１０２上でのユーザー操作に従って発行される設定変更のリクエストは、サービスサーバー１０４を経由してデバイス１０５に届く。また、サービスサーバー１０４は、設定変更サービスを提供するための機能呼び出し制御サービスも提供する。機能呼び出し制御サービスでは、設定変更サービスを提供するためにクライアントデバイス１０２から要求されたリクエストの受付やデバイス１０５から受信した実行結果を、指示したクラウドユーザーにのみ表示させるための制御を行う。後述の実施例では、サービスサーバー１０４がデバイス１０５の設定変更サービスを提供する例で説明するが、印刷サービスなどの他のサービスでも良く、また印刷サービスと設定変更サービスなどの複数のサービスを提供する形態であっても良い。

【００１９】

デバイス１０５は、画像形成装置、ＰＣ、スマートフォン等の情報処理装置であり、複数のローカルユーザーに関する情報を管理する機能を有するデバイスである。デバイス１０５は、ＭＱＴＴ　Ｂｒｏｋｅｒであるサービスサーバー１０４に対してトピックを指定したｓｕｂｓｃｒｉｂｅメッセージを送信することで、そのトピックと一致したｐｕｂｌｉｓｈメッセージを受信することができる。

【００２０】

また、本発明の認証サーバー１０３やサービスサーバー１０４等の各サーバーコンピューターは複数台で構成されていてもよく、または、ひとつのコンピューターサーバーが認証サーバー１０３やサービスサーバー１０４の機能を兼ね備えていても良い。例えば、サービスサーバー１０４は、ＭＱＴＴ　Ｂｒｏｋｅｒと機能呼び出し制御サービスを提供する機能呼び出し制御サーバーとに分割することもできる。

【００２１】

図２は、図１に示したクラウドシステム１０６を構成するサーバーコンピューターである情報処理装置２００の内部構成について示したブロック図である。なお、図２に示されるブロック図は、クライアントデバイス１０２およびデバイス１０５も情報処理装置２００と同様の内部構造を有しているものとする。

【００２２】

情報処理装置２００において、ＣＰＵ２０２、ＲＯＭ２０３、ＲＡＭ２０４、ＨＤＤ２０５が内部バス２０１を介して接続されている。ＣＰＵ２０２は、ＲＯＭ２０３のブートプログラムを実行してＨＤＤ２０５に記憶されているＯＳや制御プログラムをＲＡＭ２０４に展開し、そのプログラムに基づいて、情報処理装置２００の制御を行うユニットである。

【００２３】

ＲＯＭ２０３は、情報処理装置２００のブートプログラムや各種データ等が格納されている記憶装置である。

【００２４】

ＲＡＭ２０４は、ＣＰＵ２０２が命令を実行する際に使用するワークメモリである。ＲＯＭ２０３に保存されていたプログラムがＲＡＭ２０４へとロードされ、そのプログラムの命令をＣＰＵ２０２が順次読みだし命令を実行する。

【００２５】

ＨＤＤ２０５は外部記憶装置であり、ＯＳや各種プログラムを格納している。

【００２６】

ネットワークＩ／Ｆ２０６は、内部バス２０１を介してＣＰＵ２０２、ＲＯＭ２０３、ＲＡＭ２０４、ＨＤＤ２０５と接続されており、ＬＡＮ１００等のネットワークを介して情報処理装置２００への情報の入出力を行う。

【００２７】

尚、後述の全ての説明においては、特に断りのない限りコンピューターサーバーやデバイス等のハード上の主体はＣＰＵ２０２であり、ソフトウェア上の主体はＨＤＤ２０５にインストールされたアプリケーションプログラムである。

【００２８】

図３を用いて、クライアントデバイス１０２と認証サーバー１０３、サービスサーバー１０４、デバイス１０５が有する機能について説明する。クライアントデバイス１０２が有するＷｅｂブラウザ３００を含め、本実施例における情報処理システム１０７内の装置が有する機能は、各装置のＣＰＵ２０２がＲＡＭ２０４にロードされたアプリケーションプログラムを実行することで実現される。機能の中でも特に、認証サーバー１０３やサービスサーバー１０４等のサーバーコンピューター上で実現される機能または機能群のことをクラウドサービスという。

【００２９】

クライアントデバイス１０２はＷｅｂブラウザ３００を備え、Ｗｅｂブラウザ３００は認証サーバー１０３やサービスサーバー１０４との通信を行う。Ｗｅｂブラウザ３００は、ＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）を利用するためのユーザーエージェントによって実現する機能であり、後述のＷｅｂブラウザ３０５も同様の機能である。

【００３０】

認証サーバー１０３は通信部３０１と認証部３０２とを備える。認証部３０２は、通信部３０１を介してクライアントデバイス１０２やサービスサーバー１０４、デバイス１０５との通信を行う機能である。

【００３１】

サービスサーバー１０４は通信制御部３０３と設定管理部３０４とを備える。通信制御部３０３は、ＭＱＴＴにおけるｓｕｂｓｃｒｉｂｅメッセージの受信やｐｕｂｌｉｓｈメッセージの送信を行う機能である。また、設定管理部３０４は通信制御部３０３を介して、クライアントデバイス１０２の設定画面を介した要求の受付や、クライアントデバイス１０２で実行結果画面を表示するための設定情報を管理する機能である。

【００３２】

デバイス１０５は、Ｗｅｂブラウザ３０５とローカルログイン部３０６、認証サーバー連携部３０７、機能呼び出し制御部３０８とを備える。Ｗｅｂブラウザ３０５は、認証サーバー１０３やサービスサーバー１０４と通信を行う機能である。ローカルログイン部３０６は、デバイス１０５の利用者であるローカルユーザーを認証するための機能である。

なお、このローカルログイン部３０６は、不図示の認証サーバーと通信することでローカルユーザーを認証するように構成することもできる。

【００３３】

認証サーバー連携部３０７は認証連携情報の発行要求を行う。また、クラウドシステム１０６の利用者であるクラウドユーザーを一意に識別するための情報であるクラウドユーザー認証情報と、ローカルユーザーを一意に識別するための情報であるローカルユーザー認証情報とを紐付ける機能でもある。

【００３４】

認証連携情報とはクラウドユーザー認証情報とローカルユーザー認証情報とを紐付けるために用いられる認証情報である。認証連携情報の一例として、パスコード等が挙げられる。クラウドユーザー認証情報は、クラウドユーザーがクラウドシステム１０６にログインした時に生成される認証情報の総称であり、クラウドユーザーＩＤやクラウドユーザーＵＵＩＤ（Ｕｎｉｖｅｒｓａｌｌｙ Ｕｎｉｑｕｅ Ｉｄｅｎｔｉｆｉｅｒ）等のクラウドユーザーを一意に識別するための情報が含まれる。ＵＵＩＤとはユーザーを一意に識別するための識別子であり、ＩＤとは違って他のユーザーと重複しないことを前提に作られているものである。つまり、クラウドユーザーＵＵＩＤを用いることで、マルチテナントシステムにおいてテナントごとに設定されたユーザー情報も全て識別できるものとする。後述の例ではクラウドユーザー認証情報としてトークンの形態を用いて説明しているが、クラウドユーザーを識別できる情報であればどのような形態でもよい。一方、ローカルユーザー認証情報とは、ローカルユーザーがデバイス１０５にログインした時に生成される認証情報の総称であり、ローカルユーザーＩＤやローカルユーザーＵＵＩＤ等のローカルユーザーを一意に識別するための情報が含まれる。後述の例では、ローカルユーザー認証情報としてトークンの形態を用いて説明しているが、ローカルユーザーを識別できる情報であればどのような形態でもよい。後述では、認証連携情報を用いてクラウドユーザーＵＵＩＤとローカルユーザーＵＵＩＤとを紐付けた紐付け情報を例に説明する。

【００３５】

機能呼び出し制御部３０８は、クラウドユーザーＵＵＩＤとローカルユーザーＵＵＩＤとを紐付けるユーザー紐付け処理において、ｓｕｂｓｃｒｉｂｅメッセージをサービスサーバー１０４に送信し、サービスサーバー１０４からの処理要求を待つ。

【００３６】

図４を用いて、認証サーバー１０３がデバイス１０５を認証する過程を説明する。この過程は、デバイス１０５において認証サーバー連携部３０７がインストールされ、初めて認証サーバー連携部３０７が起動したタイミングで開始されるものとする。認証サーバー１０３の通信部３０１はデバイス１０５の認証が必要になるように構成されている。

【００３７】

Ｓ１．１にて、認証サーバー連携部３０７が通信部３０１に対してデバイス登録要求を送信する。認証サーバー連携部３０７からデバイス登録要求を受信した通信部３０１は、ＳＳＬ／ＴＬＳ通信のネゴシエーションを開始する。その際、通信部３０１は認証サーバー連携部３０７に対してデバイス認証情報を要求して受信する。デバイス認証情報とは、デバイス１０５を特定するためにＳＳＬ／ＴＬＳ通信に用いられる証明書である。Ｓ１．２において、通信部３０１は不図示の証明書ストアにて設定されている証明書を用いて、Ｓ１．１で取得したデバイス認証情報を検証し、認証サーバー連携部３０７をデバイス１０５の登録要求元として認証する。Ｓ１．３にて、通信部３０１が認証部３０２に対して、認証サーバー連携部３０７から受信したデバイス登録要求とデバイス認証情報とを送信する。Ｓ１．４において認証部３０２は、Ｓ１．３で取得したデバイス認証情報を基に、デバイス１０５を一意に識別するためのデバイス識別情報を発行する。以降の実施例では、デバイス識別情報は証明書の形態を持つものとして説明するが、認証部３０２がデバイス１０５を一意に識別できさえすれば、デバイス識別情報は証明書の形態や数値文字列の形態などでも良い。Ｓ１．５にて、認証部３０２は通信部３０１を介して認証サーバー連携部３０７に対して、デバイス登録要求に対する応答としてデバイス識別情報を送信する

。

【００３８】

以上が、認証サーバー１０３がデバイス１０５を認証する過程である。この過程により、認証部３０２が発行したデバイス識別情報を用いることで、認証サーバー連携部３０７はデバイス１０５を特定することが可能となる。また、本実施例の事前設定は、認証サーバー連携部３０７を認証部３０２への登録する登録処理としているが、その処理には必ずしも限定されない。例えば、認証部３０２が発行したデバイス識別情報を認証サーバー連携部３０７へ手動で登録しても良い。また、出荷時に認証サーバー連携部３０７へ埋め込まれているデバイス認証情報をそのまま利用しても良い。また、以降の実施例では、「外部から通信部３０１を介して認証部３０２への通信」を、「外部から認証部３０２への通信」と記載する。

【００３９】

［実施例１］

デバイス１０５がマルチユーザーデバイスである場合、ローカルユーザーＵＵＩＤに対して複数のクラウドユーザーＵＵＩＤの紐付けを許容する。実行結果がどのクラウドユーザーＵＵＩＤに対するものなのかをクラウドシステム１０６で特定し、リクエストとレスポンスとを紐付ける形態を実施例１で説明する。デバイス１０５の登録処理が成された状態（図４）で、認証部３０２が管理するクラウドユーザーＵＵＩＤとローカルログイン部３０６が管理するローカルユーザーＵＵＩＤとを紐付けるための認証連携情報を発行する過程を図５で説明する。

【００４０】

Ｓ２．１においてローカルログイン部３０６は、ローカルログイン部３０６において定められている認証方法によってユーザーのログイン処理を受信する。認証方法としては例えば、ユーザーＩＤとパスワードとの組み合わせを検証する方法、指紋等の生体情報を検証する方法、非接触型のＩＣカードを利用する方法、更には複数の認証方法を組み合わせる多要素認証方法等が考えられる。また、不図示の認証サーバーと通信することでユーザーを認証するように構成することもできる。実施例１では、ローカルユーザーＩＤとパスワードとの組み合わせを検証する認証方法を用いた場合を例として説明する。表１は、ローカルログイン部３０６が管理するユーザー情報の一例である。

【００４１】

【表１】

表１

| ローカルユーザーID | ローカルユーザーUUID | パスワード | 権限情報 |
|---|---|---|---|
| admin | AAA1 | admin | 管理者 |
| user | AAA2 | user | 一般 |

【００４２】

Ｓ２．２にて、ローカルログイン部３０６はローカルユーザーＩＤとパスワードの組を用いてローカルユーザー認証を行う。具体的には、ローカルログイン部３０６は表１のユーザー情報を参照してローカルユーザー認証を行う。例えば、ユーザーがローカルユーザーＩＤ「ａｄｍｉｎ」とパスワード「ａｄｍｉｎ」を入力した場合、ローカルログイン部３０６はローカルユーザーＩＤ「ａｄｍｉｎ」のローカルユーザーとしてユーザーを認証する。

【００４３】

Ｓ２．３でローカルログイン部３０６は、Ｓ２．２で認証されたユーザーのローカルユーザー認証情報を生成し保存する。このローカルユーザー認証情報は、ユーザーが不図示のログアウト操作を実施するか、設定された時刻が経過するまで有力な状態で保存される。ローカルユーザー認証情報には、認証したユーザーのローカルユーザーＩＤ、ローカル

ユーザーＵＵＩＤ及び権限情報等が格納されている。つまり、表１で示したユーザー情報とほとんど同じ情報をローカルユーザー認証情報は含む。なお、ローカルログイン部３０６がローカルユーザー認証情報を直接格納する形態に限らない。ローカルユーザー認証情報と紐付けられたトークンをローカルログイン部３０６が格納し、そのトークンを参照することでローカルログイン部３０６とは別の場所に格納されたローカルユーザー認証情報を用いる形態でもよい。

【００４４】

Ｓ２．４において、Ｗｅｂブラウザ３０５はユーザーの操作により認証連携情報の発行要求を受け付ける。受信した発行要求に応じて、Ｗｅｂブラウザ３０５は認証サーバー連携部３０７に対して認証連携情報の発行要求を送信する（Ｓ２．５）。Ｓ２．６で認証サーバー連携部３０７はローカルログイン部３０６に対してローカルユーザーＵＵＩＤの取得要求を行う。Ｓ２．６の要求に対して、ローカルログイン部３０６は認証サーバー連携部３０７にローカルユーザーＵＵＩＤを応答する（Ｓ２．７）。Ｓ２．８にて、認証サーバー連携部３０７は認証部３０２に認証連携情報の発行要求を送信する。その際、Ｓ２．７で受信したローカルユーザーＵＵＩＤとＳ１．５で受信したデバイス識別情報とを認証部３０２に送信する。

【００４５】

Ｓ２．９で認証部３０２は認証連携情報を発行する。発行した認証連携情報とその有効期限の一例を表２に示す。実施例１では認証連携情報を文字列としているが、後述するようにＱＲコード（登録商標）などの形態の情報であっても構わない。また、実施例１では認証連携情報に有効期限が定められているが、無期限の認証連携情報でも良い。

【００４６】

【表２】

表２

| 認証連携情報 | 有効期限 |
|---|---|
| XXX-YYY-ZZZ | 2016/12/06 08:00:00 |
| AAA-BBB-CCC | 2016/11/06 07:00:00 |

【００４７】

Ｓ２．１０において、認証部３０２はＳ２．９で発行された認証連携情報とＳ２．８で受信したローカルユーザーＵＵＩＤ及びデバイス識別情報とを紐付けた紐付け情報を管理する。紐付け情報の例を表３に示す。

【００４８】

【表３】

表３

| デバイス識別情報 | ローカルユーザーUUID | 認証連携情報 |
|---|---|---|
| 00001 | AAA1 | XXX－YYY－ZZZ |

【００４９】

Ｓ２．１１にて、認証部３０２が認証サーバー連携部３０７に対して認証連携情報を応答する。認証サーバー連携部３０７は、ローカルユーザーＵＵＩＤとＳ２．１１で受信した認証連携情報とを紐付ける（Ｓ２．１２）。その際に生成されるマッピングテーブルの例を表４に示す。

【００５０】

【表４】

表４

| ローカルユーザーUUID | 認証連携情報 |
|---|---|
| AAA1 | XXX－YYY－ZZZ |

【００５１】

Ｓ２．１３において、Ｓ２．５における認証連携情報の発行要求に対して応答する。具体的には、Ｓ２．１１で応答された認証連携情報をＷｅｂブラウザ３０５に送信し、Ｗｅｂブラウザ３０５は認証連携情報を表示する。これにより、ユーザーは認証連携情報を入手できる。Ｓ２．１４で、ｓｕｂｓｃｒｉｂｅメッセージの送信を依頼する。具体的には、後述するユーザー紐付け処理のために、認証サーバー連携部３０７は機能呼び出し制御部３０８に対して、通信制御部３０３へのｓｕｂｓｃｒｉｂｅメッセージの送信を依頼する。Ｓ２．１５にて、機能呼び出し制御部３０８が通信制御部３０３に対してｓｕｂｓｃｒｉｂｅメッセージを送信する。ｓｕｂｓｃｒｉｂｅメッセージのトピックは、デバイス識別情報で指定する。具体的には、トピックは「／」で区切られた階層構造（例：／Ａ／ＢＣ／Ｄ／Ｅ）となっており、ｓｕｂｓｃｒｉｂｅｒが受信したい情報の分類を定義できるので、「（デバイス１０５が設置されている場所）／（デバイス識別情報）」というように、メッセージの送信先を指定する。これによりデバイス１０５のデバイス識別情報をトピックとするｐｕｂｌｉｓｈメッセージを、機能呼び出し制御部３０８が受信することができる。また、機能呼び出し制御部３０８は通信制御部３０３との通信を維持するために、通信の切断を検知する度に通信制御部３０３対してｓｕｂｓｃｒｉｂｅメッセージを送信する。

【００５２】

以上が認証連携情報を発行する過程である。これにより、認証サーバー１０３とデバイス１０５は、認証連携情報を用いたマッピングテーブル（表３、表４）を所有できる。また、ユーザーも認証連携情報を入手できる。

【００５３】

次に、認証サーバー１０３においてローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理について、図６を用いて説明する。Ｓ３．１でＷｅｂブラウザ３００はユーザーからログイン操作を受け付け、Ｓ３．２でＷｅｂブラウザ３００は認証部３０２に対してログイン処理を要求する。このログイン処理は認証部３０２において定められている認証方法によって行われる。認証方法としては例えば、ユーザーＩＤとパスワードの組み合わせを検証する方法を利用する方法等がある。実施例１では、クラウドユーザーＩＤとパスワードの組み合わせを例として説明する。表５に認証部３０２が管理するユーザー情報の一例を示す。

【００５４】

【表５】

表５

| クラウドユーザーID | クラウドユーザーUUID | パスワード |
|---|---|---|
| se001 | CCC1 | se001 |
| se002 | CCC2 | se002 |

【００５５】

Ｓ３．３において認証部３０２はクラウドユーザー認証を行い、Ｓ３．４で認証したクラウドユーザーのクラウドユーザー認証情報を生成し保存する。クラウドユーザー認証情報は、ユーザーが不図示のログアウト操作を実施するか、設定された時刻が経過するまで有力な状態で保存される。クラウドユーザー認証情報には、認証したクラウドユーザーの

クラウドユーザーＩＤ、クラウドユーザーＵＵＩＤが格納されている。つまり、表５で示したユーザー情報とほとんど同じ情報をクラウドユーザー認証情報は含む。なお、認証部３０２が各認証情報を直接格納する形態のみならず、各認証情報が参照可能に紐付けられたトークンを認証部３０２が格納し、そのトークンを参照することで認証部３０２とは別の場所に格納された認証情報を用いるようにした形態でもよい。

【００５６】

Ｓ３．５において、認証部３０２がＷｅｂブラウザ３００にログイン処理に対する応答を行う。その際、Ｓ３．４において生成されたクラウドユーザーＵＵＩＤと紐付くセッションＩＤがＷｅｂブラウザ３００に送信される。セッションＩＤとは、ログインしたユーザーを識別するための識別子であり、本実施例ではＳ３．４において生成されたクラウドユーザーＵＵＩＤと紐付いて認証部３０２で管理されている。Ｓ３．５においてセッションＩＤをＷｅｂブラウザ３００が受信することで、Ｗｅｂブラウザ３００のＣｏｏｋｉｅ（不図示）にセッションＩＤが管理される。後述の実施例では特に断りがない限り、Ｗｅｂブラウザ３００と認証部３０２における通信では、このセッションＩＤの受送信が行われる。

【００５７】

Ｓ３．６で、Ｗｅｂブラウザ３００は認証連携情報の入力要求をユーザーから受信し、Ｓ３．７でＷｅｂブラウザ３００は認証部３０２に対して認証連携情報の入力要求を行う。認証部３０２はＷｅｂブラウザ３００からの認証連携情報入力要求に対して入力画面を応答する（Ｓ３．８）。Ｓ３．９にてＷｅｂブラウザ３００はユーザーによる認証連携情報の入力操作を受け付け、Ｓ３．１０において、受け付けた認証連携情報を認証部３０２に送信し、認証連携情報を用いた紐付け処理を要求する。Ｓ３．１１において、Ｓ３．１０で受信した認証連携情報と認証部３０２が管理しているクラウドユーザーＵＵＩＤとを紐付ける。具体的には、認証部３０２が管理しているクラウドユーザーＵＵＩＤと、Ｓ３．１０で受信したセッションＩＤとを照合し、そのセッションＩＤを介してクラウドユーザーＵＵＩＤと認証連携情報とを紐付ける。その際に生成される紐付け情報の例を表６に示す。

【００５８】

【表６】

表６

| クラウドユーザーUUID | 認証連携情報 |
|---|---|
| CCC1 | XXX-YYY-ZZZ |

【００５９】

Ｓ３．１２において認証部３０２は、Ｓ２．１０で作成したマッピングテーブル（表３）とＳ３．１１で作成したマッピングテーブル（表６）とを一つのマッピングテーブルにまとめ、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付ける。具体的には、表３と表６とが共通の認証連携情報を有するのでその認証連携情報を介して、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付ける。その際のマッピングテーブルの例を表７に示す。表７の紐付け情報には、Ｓ３．１０で受信したセッションＩＤも紐付いているものとする。

【００６０】

【表７】

表７

| デバイス識別情報 | ローカルユーザーUUID | クラウドユーザーUUID |
|---|---|---|
| 00001 | AAA1 | CCC1 |

【００６１】
以上が、認証サーバー１０３においてローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとが紐付けるユーザー紐付け処理である。また、表７のようなマッピングテーブルを作成する際に認証連携情報が有効期限を迎え無効化されていれば、マッピングテーブル作成に失敗し、このユーザー紐付け処理を終了する。この際、マッピングテーブル作成に失敗した旨をＷｅｂブラウザ３００に通知しても良い。
【００６２】
次に、デバイス１０５においてローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理について、図７を用いて説明する。Ｓ４．１において、クラウドユーザーＵＵＩＤの紐付け依頼を送信する。具体的には、認証部３０２は通信制御部３０３に対して、Ｓ３．９で入力された認証連携情報とともにｐｕｂｌｉｓｈメッセージを送信する。ｐｕｂｌｉｓｈメッセージを送信する際のトピックはデバイス識別情報とする。これにより、Ｓ２．１５で機能呼び出し制御部３０８が送信したｓｕｂｓｃｒｉｂｅメッセージ（トピックはデバイス１０５のデバイス識別情報）と同じトピックのｐｕｂｌｉｓｈメッセージを送信することができる。認証部３０２が送るメッセージは、通信制御部３０３がＭＱＴＴと他のプロトコルとの変換機能を備えていれば、ＭＱＴＴのｐｕｂｌｉｓｈメッセージでなくても構わない。
【００６３】
Ｓ４．２において、クラウドユーザーＵＵＩＤの紐付け依頼を送信する。具体的には、ｓｕｂｓｃｒｉｂｅメッセージを送信した機能呼び出し制御部３０８に対して、クラウドユーザーＵＵＩＤの紐付け依頼としてｐｕｂｌｉｓｈメッセージを送る。その際、クラウドユーザーＵＵＩＤと認証連携情報も送信される。ｓｕｂｓｃｒｉｂｅメッセージは、Ｓ４．１で受信したｐｕｂｌｉｓｈメッセージと同じトピックなので、機能呼び出し制御部３０８にｐｕｂｌｉｓｈ　メッセージが送信される。Ｓ４．３にて、機能呼び出し制御部３０８が認証サーバー連携部３０７に対して、クラウドユーザーＵＵＩＤの紐付け要求を行う。その際、Ｓ４．２で受信した認証連携情報とクラウドユーザーＵＵＩＤも同時に通知する。Ｓ４．４では、認証サーバー連携部３０７が、Ｓ４．３で受信したクラウドユーザーＵＵＩＤと認証連携情報とを用いて、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとの紐付け処理を行う。認証サーバー連携部３０７では、Ｓ２．１２においてローカルユーザーＵＵＩＤと認証連携情報とが紐付けているため、認証連携情報を介してローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けることができる。Ｓ４．４において生成されるマッピングテーブルの例を表８に示す。
【００６４】
【表８】
表８

| ローカルユーザーUUID | クラウドユーザーUUID |
|---|---|
| AAA1 | CCC1 |

【００６５】
以上が、デバイス１０５におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理である。図６のユーザー紐付け処理により認証サーバー１０３ではローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとが紐づき、図７のユーザー紐付け処理によりデバイス１０５ではローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとが紐付いた。
【００６６】
次にデバイス１０５における機能呼び出し処理を、図８を用いて説明する。今回は、デバイス１０５の設定を例に機能呼び出し処理を説明するが、設定要求以外にもデバイス１０５の機能を利用するための実行要求なども考えられる。実施例１において、既に説明し

ているステップと同じステップには同じ符番をふり、詳細な説明は省略する。他の実施例の場合も同様である。

【００６７】

Ｓ５．１において、Ｗｅｂブラウザ３００はユーザーから設定画面の要求を受信する。このとき、デバイス識別情報も同時に受信する。Ｓ５．２でＷｅｂブラウザ３００は設定管理部３０４に設定画面を要求し、Ｓ５．３で設定管理部３０４はそれに対して応答する。今回、Ｗｅｂブラウザ３００とサービスサーバー１０４間のメッセージ通信プロトコルがＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）だとすると、Ｓ５．２でＷｅｂブラウザ３００から送信される設定要求は、ＨＴＴＰの方式に従ったリクエストメッセージである。以降のＷｅｂブラウザ３００とサービスサーバー１０４間のやり取りも同様である。設定管理部３０４が応答した設定画面の例を図９に示す。図９の設定画面はデバイス識別情報と、設定項目テーブル、入力完了ボタンを保有する。設定項目テーブルにおいて、設定値列に新しく設定したい設定値を入力する。さらに、ユーザーの操作により設定画面上の入力完了ボタンが押下されると、後述のＳ５．５のステップが開始される。

【００６８】

Ｓ５．４においてＷｅｂブラウザ３００はユーザーから設定情報入力操作を受信する。具体的には、Ｗｅｂブラウザ３００は表示している設定画面（図９）において設定情報の入力操作を受信し、「入力完了」ボタンが押下される。その際、「オートスリープ移行時間」の「設定値」欄に「５分」とユーザーが入力し、その設定情報をＷｅｂブラウザ３００が受信したものとする。オートスリープ移行時間とは、オートスリープ（起動中のデバイス１０５が消費電力を抑えるために一定時間ユーザーによる操作がなければ停止する）が起こるまでの時間のことをいう。Ｓ５．５で、Ｗｅｂブラウザ３００は設定管理部３０４に設定要求を送信する。その際Ｗｅｂブラウザ３００は、Ｓ３．５で受信したセッションＩＤを設定管理部３０４に対して送信する。具体的には、オートスリープ移行時間を５分にするための設定要求が設定管理部３０４に送信される。

【００６９】

Ｓ５．６において設定管理部３０４が通信制御部３０３に対して、Ｗｅｂブラウザ３００から受信した設定要求を送信する。その際、Ｓ５．１においてユーザーによって指定されたデバイス識別情報も送信される。Ｓ５．７において、通信制御部３０３は認証部３０２に対してローカルユーザーＵＵＩＤの取得要求を行う。その際、ローカルユーザーＵＵＩＤの取得要求とともにセッションＩＤが認証部３０２に送信される。認証部３０２において紐付いているローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとセッションＩＤとの紐付け情報（表７）を用いて、通信制御部３０３から受信したセッションＩＤと紐付くローカルユーザーＵＵＩＤを特定し、通信制御部３０３からの取得要求に対して送信すべきローカルユーザーＵＵＩＤを特定することができる。Ｓ５．８において、認証部３０２が通信制御部３０３に対してローカルユーザーＵＵＩＤを送信することで、ローカルユーザーＵＵＩＤの取得応答を行う。

【００７０】

Ｓ５．９において、通信制御部３０３が、Ｓ５．８で取得したローカルユーザーＵＵＩＤとＳ５．６で受信した設定要求とを機能呼び出し制御部３０８に対して送信する。具体的には、オートスリープ移行時間を５分にするための設定要求が機能呼び出し制御部３０８に送信される。実施例１では、サービスサーバー１０４がＭＱＴＴによるメッセージ通信を行うサーバーである場合を例に説明しているので、設定要求を機能呼び出し制御部３０８にｐｕｂｌｉｓｈメッセージを送信する。その際のトピックはデバイス識別情報である。これにより、Ｓ２．１５で機能呼び出し制御部３０８が送信したｓｕｂｓｃｒｉｂｅメッセージ（トピックはデバイス１０５のデバイス識別情報）と同じトピックのｐｕｂｌｉｓｈメッセージを送信することができる。

【００７１】

Ｓ５．１０において機能呼び出し制御部３０８は、Ｓ５．９で受信したｐｕｂｌｉｓｈ

メッセージの内容に応じて設定要求を実行する。その際、設定要求とともに受信したローカルユーザーＵＵＩＤで特定されるローカルユーザーとして設定要求を実行する。具体的には、機能呼び出し制御部３０８がローカルユーザーＵＵＩＤ「ＡＡＡ１」を受信した場合、デバイス１０５が保有するユーザー情報（表１）より、ローカルユーザーＩＤ「ａｄｍｉｎ」としてオートスリープ移行時間が５分に設定される。

【００７２】

Ｓ５．１１において、通信制御部３０３から受信したローカルユーザーＵＵＩＤと紐づくクラウドユーザーＵＵＩＤの取得要求を、機能呼び出し制御部３０８が認証サーバー連携部３０７に対して行う。Ｓ５．１２において、認証サーバー連携部３０７が管理しているマッピングテーブル（表８）を用いて、ローカルユーザーＵＵＩＤと紐づくクラウドユーザーＵＵＩＤを機能呼び出し制御部３０８に応答する。Ｓ５．１３において機能呼び出し制御部３０８は、Ｓ５．１２で取得したクラウドユーザーＵＵＩＤとともに実行結果を通信制御部３０３に対して応答する。ここで、実行結果とともにクラウドユーザーＵＵＩＤを送信する理由は、通信制御部３０３において１つのローカルユーザーＵＵＩＤに対し複数のクラウドユーザーＵＵＩＤが紐付いている場合があるため、通信制御部３０３において一意に特定されるクラウドユーザーＵＵＩＤを送信する必要がある。

【００７３】

実施例１では設定要求として、「オートスリープ移行時間を５分」にするデバイス１０５の設定変更をＷｅｂブラウザ３００から受信した例として説明しているため、Ｓ５．１３における実行結果の応答には設定変更後の値が含まれる。デバイス１０５がＭＦＰ等の印刷機能を有している場合、設定要求としては印刷機能の利用なども考えられる。その場合は結果応答としてステータス情報を通信制御部３０３に送信するなど、設定要求の内容に応じて実行結果の応答に含まれる情報は変わる。また、デバイス１０５の設定が失敗したときや機能の実行が失敗したときは、応答される実行結果にはエラーに関する情報が含まれる。

【００７４】

Ｓ５．１４において、通信制御部３０３は設定管理部３０４に対してクラウドユーザーＵＵＩＤとともに設定要求の実行結果を送信する。設定管理部３０４はＳ５．１４で受信したクラウドユーザーＵＵＩＤを用いることで、どのクラウドユーザーによる設定要求に対して結果が応答されたのかを特定することができる。また、設定管理部３０４が認証部３０２から、クラウドユーザーＵＵＩＤと紐付くローカルユーザーＵＵＩＤを取得することで、どのローカルユーザーによる設定要求に対して結果が応答されたのかも特定することができる。実行結果とそれを実行した際に用いたローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤは、最終的には設定管理部３０４で管理される。

【００７５】

以上が、デバイス１０５における機能呼び出し処理である。これにより、ユーザーはクライアントデバイス１０２のＷｅｂブラウザ３００を介して、デバイス１０５が公開している機能を利用することができ、その機能を利用したことによる実行結果を確認することができる。

【００７６】

デバイス１０５の機能を実行した後、クライアントデバイス１０２のＷｅｂブラウザ３００は不図示の実行結果画面の要求をユーザーから受信し、実行結果画面を表示することができる。その実行結果画面の例を図１０に示す。図１０には、設定変更を行ったデバイス１０５のデバイス識別情報とその設定変更の前後の値が格納されている。また、各設定項目に対して設定変更ステータスを格納することも可能である。

【００７７】

また、その実行結果画面を表示するための、結果取得処理のフローの一例を図１２に示す。本フローの起動は、ユーザーが実行結果画面を要求したときである。その際、実行結果を要求するデバイス１０５のデバイス識別情報とレスポンス識別情報とが、Ｗｅｂブラウザ３００において選択される。選択する際にＷｅｂブラウザ３００に表示される実行結

果選択画面の一例を図１１に示す。図１１では「内容概要」の欄内の各項目に対してリンクがあり、そのリンクが選択されることでレスポンス識別情報が選択され、実行結果画面が要求される。また、実施例１ではリクエストとレスポンスが直接紐付くわけではないため、図１１ではリクエストとレスポンスを分割して記載しているが、この形態に限定されるわけではない。実行結果選択画面上でクラウドユーザーの実行履歴を管理することも可能である。図１１の画面でデバイス識別情報とレスポンス識別情報が選択された後、Ｓ６．１で設定管理部３０４が認証部３０２から、ログインしているクラウドユーザーのクラウドユーザーＵＵＩＤを取得する。Ｓ６．２にて、設定管理部３０４はＳ６．１で取得したクラウドユーザーＵＵＩＤと、選択されたデバイス識別情報とレスポンス識別情報を用いて、デバイス１０５の実行結果に関する情報を格納する不図示のデータベースから取得する。

【００７８】

以上が、実行結果画面を表示するための結果取得処理のフローである。これにより、ユーザーは自身が要求したリクエストに対するデバイス１０５の実行結果を参照することが可能となる。結果取得処理のフローは、図１１や図１２の形態に限らない。例えば、ユーザーは結果画面要求時にリクエストの選択を行わず、これまでの実行結果から最新の情報のみを閲覧するような形態等も考えられる。また、ユーザーの実行結果画面要求に応じて実行結果を取得するのではなく、Ｓ５．１４で設定管理部３０４が実行結果を取得した際に実行結果画面を作成しておくことも考えられる。

【００７９】

［実施例２］

デバイス１０５が保有するローカルユーザーＵＵＩＤと認証サーバー１０３で保有するクラウドユーザーＵＵＩＤが漏洩することで、ユーザーのなりすましが行われる可能性がある。そのため、ユーザー紐付け処理において共通鍵を発行し、機能呼び出し処理において署名情報を付与することでデバイス１０５への設定要求の改竄を検知することができる。設定要求の改竄で例えば、デバイス１０５への設定要求が「オートスリープ移行時間を５分にする」ための設定要求だとすると、この設定要求が改竄されて「オートスリープ移行時間を１分にする」など、ユーザーが意図していない設定要求がデバイス１０５で実行されてしまう。実施例２では、共通鍵を利用した場合のユーザー紐付け処理と機能呼び出し処理について説明する。実施例１のユーザー紐付け処理（図６、図７）と、機能呼び出し処理（図８）とで同様のステップについては詳細な説明は省略する。

【００８０】

まず、共通鍵を用いた場合の、認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとのユーザー紐付け処理について図６を用いて説明する。Ｓ３．１１を後述のＳ７．１、Ｓ３．１２を後述のＳ７．２に置き換えることで、共通鍵を用いた場合のユーザー紐付け処理が実現する。

【００８１】

Ｗｅｂブラウザ３００はユーザーから認証連携情報の入力要求を受信し（Ｓ３．６）、認証部３０２に対して認証連携情報の入力要求を行う（Ｓ３．７）。Ｓ３．７の入力要求に対して、認証部３０２は認証連携情報の入力画面を応答する（Ｓ３．８）。Ｗｅｂブラウザ３００は、応答された入力画面を用いて認証連携情報の入力操作をユーザーから受け付け（Ｓ３．９）、認証部３０２に対して紐付け処理を要求する（Ｓ３．１０）。Ｓ７．１において、認証部３０２でクラウドユーザーＵＵＩＤと認証連携情報との紐付け処理を行い、その紐付け情報に対して共通鍵を発行する。Ｓ７．１で発行された共通鍵を用いて、認証部３０２はクラウドユーザーＵＵＩＤとローカルユーザーＵＵＩＤとデバイス識別情報との紐付け情報（表７）と共通鍵とを紐付ける（Ｓ７．２）。

【００８２】

以上が、共通鍵を用いた場合の、認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとのユーザー紐付け処理である。これにより認証部３０２は、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤと紐づいた共通鍵を保持でき

る。
【００８３】
次に、共通鍵を用いた場合の、デバイス１０５におけるローカルユーザーＵＵＩＤとクラウドＵＵＩＤとのユーザー紐付け処理について図１３を用いて説明する。Ｓ７．３において、認証連携情報とクラウドユーザーＵＵＩＤと共通鍵の紐付け依頼を送信する。具体的には、認証部３０２がＳ３．９において入力された認証連携情報とＳ７．１において発行された共通鍵ともに通信制御部３０３に対してｐｕｂｌｉｓｈメッセージを送信する。ｐｕｂｌｉｓｈメッセージを送信する際のトピックはデバイス識別情報とする。これにより、Ｓ２．１５において機能呼び出し制御部３０８が送信したｓｕｂｓｃｒｉｂｅメッセージ（トピックはデバイス１０５のデバイス識別情報）と同じトピックのｐｕｂｌｉｓｈメッセージを送信することができる。この際に認証部３０２が送るメッセージは、通信制御部３０３がＭＱＴＴと他のプロトコルとの変換機能を備えていれば、ＭＱＴＴのｐｕｂｌｉｓｈメッセージでなくても構わない。
【００８４】
Ｓ７．４において、クラウドユーザーＵＵＩＤと共通鍵の紐付け依頼を送信する。今回は、ｓｕｂｓｃｒｉｂｅメッセージを送信した機能呼び出し制御部３０８に対して、クラウドユーザーＵＵＩＤの紐付け依頼としてｐｕｂｌｉｓｈメッセージを送る。そのメッセージとともに、クラウドユーザーＵＵＩＤと認証連携情報と共通鍵が送信される。ｓｕｂｓｃｒｉｂｅメッセージには、Ｓ７．３で受信したｐｕｂｌｉｓｈメッセージと同じトピックなので、機能呼び出し制御部３０８にｐｕｂｌｉｓｈメッセージが送信される。Ｓ７．５にて、機能呼び出し制御部３０８は認証サーバー連携部３０７に対して、クラウドユーザーＵＵＩＤの紐付け要求を行う。その際、Ｓ７．４で受信した認証連携情報とクラウドユーザーＵＵＩＤ、共通鍵も同時に通知する。Ｓ７．６では、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤと共通鍵とを紐付ける紐付け処理を行う。具体的には認証サーバー連携部３０７が、Ｓ４．３で受信したクラウドユーザーＵＵＩＤと認証連携情報と共通鍵とを用いて、紐付け処理を行う。
【００８５】
以上が、共通鍵を用いた場合の、デバイス１０５におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとのユーザー紐付け処理である。これにより認証サーバー連携部３０７は、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤと紐づいた共通鍵を保持できる。
【００８６】
上記した内容では、対称鍵暗号の共通鍵基盤を前提として鍵交換を行った。しかしこれに限定されることはなく、例えば非対称鍵暗号の公開鍵基盤を用いても良い。その場合、Ｓ７．１において認証部３０２で非対称鍵ペア（公開鍵、秘密鍵）を発行し、Ｓ７．４において公開鍵を機能呼び出し制御部３０８に送信する。その後さらに、認証サーバー連携部３０７で非対称鍵ペアを発行し、その公開鍵を認証部３０２に送信することが考えられる。デバイス１０５が鍵発行機能を備えていない場合は、認証部３０２が代行して非対称鍵ペアを２ペア発行しても良い。
【００８７】
次に、共通鍵を用いた場合の機能呼び出し処理を図１４で説明する。図８の機能呼び出し処理のときと同じステップには同じ符番をふり、詳細な説明は省略する。Ｓ５．１において、Ｗｅｂブラウザ３００はユーザーからデバイス識別情報とともに設定画面要求操作を受信する。受信した設定画面要求操作に応じてＷｅｂブラウザ３００は、設定管理部３０４に対して設定画面を要求し（Ｓ５．２）、設定管理部３０４は設定画面をＷｅｂブラウザ３００に応答する（Ｓ５．３）。応答された設定画面の例は図９に示した通りである。Ｗｅｂブラウザ３００はユーザーから設定情報入力操作を受信し（Ｓ５．４）、受信した設定要求を設定管理部３０４に送信する（Ｓ５．５）。今回も実施例１のときと同様に、「オートスリープ移行時間」の「設定値」欄に「５分」とユーザーが入力し、Ｓ５．４においてその設定要求をＷｅｂブラウザ３００が受信したものとする。オートスリープ移

行時間を５分にするための設定要求がＷｅｂブラウザ３００から設定管理部３０４に送信される（Ｓ５．５）。設定管理部３０４は受信した設定要求を送信する（Ｓ５．６）。

【００８８】

Ｓ７．７において、通信制御部３０３は認証部３０２にローカルユーザーＵＵＩＤと共通鍵の取得要求を行う。Ｓ７．１でクラウドユーザーＵＵＩＤと認証連携情報との紐付け情報に対して共通鍵が発行されているので、Ｓ７．７で通信制御部３０３が認証部３０２にセッションＩＤを送信することで、要求されている共通鍵を特定できる。具体的には、Ｓ７．２においてローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとセッションＩＤとの紐付け情報と共通鍵とが紐付いているので、通信制御部３０３から受信したセッションＩＤを用いて、要求されている共通鍵を特定する。Ｓ７．８において、認証部３０２が通信制御部３０３に対してローカルユーザーＵＵＩＤと共通鍵を送信する。その結果、サービスサーバー１０４において共通鍵とローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとが紐付く。Ｓ７．９において、共通鍵を用いて設定要求に対して署名情報を付与する。送信されるリクエストはＪＷＴ（ＪＳＯＮ Ｗｅｂ Ｔｏｋｅｎ）形式の文字列として生成され、更にＪＷＳ（ＪＳＯＮ Ｗｅｂ Ｓｉｇｎａｔｕｒｅ）で定義される署名情報が付与される。署名情報の形式は、必ずしもＪＷＴ、ＪＷＡに限定されるわけではない。後述の署名情報についても同様である。

【００８９】

Ｓ７．１０において通信制御部３０３は機能呼び出し制御部３０８に、Ｓ７．８で取得したローカルユーザーＵＵＩＤとともにＳ７．９において署名情報を付与した設定要求をｐｕｂｌｉｓｈメッセージとして送信する。その際のトピックはデバイス１０５のデバイス識別情報である。これにより、Ｓ２．１５で機能呼び出し制御部３０８が送信したｓｕｂｓｃｒｉｂｅメッセージ（トピックはデバイス１０５のデバイス識別情報）と同じトピックのｐｕｂｌｉｓｈメッセージを送信することができる。設定要求の具体例として今回は、オートスリープ移行時間を５分にするための設定要求が機能呼び出し制御部３０８に送信される。

【００９０】

Ｓ７．１１において、機能呼び出し制御部３０８は認証サーバー連携部３０７にクラウドユーザーＵＵＩＤと共通鍵の取得要求を行う。Ｓ７．１１の取得要求に対して、認証サーバー連携部３０７はクラウドユーザーＵＵＩＤと共通鍵とを応答する（Ｓ７．１２）。Ｓ７．６で、認証サーバー連携部３０７においてローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤと共通鍵とが紐付けた。そのため、認証サーバー連携部３０７は、Ｓ７．１２で機能呼び出し制御部３０８に応答すべきクラウドユーザーＵＵＩＤと共通鍵を特定することができる。

【００９１】

Ｓ７．１３において、機能呼び出し制御部３０８がＳ７．１２において受信した共通鍵を用いて、設定要求に付与された署名情報を検証した後、Ｓ７．１０で受信したｐｕｂｌｉｓｈメッセージの内容に応じて、オートスリープ移行時間を５分にするための設定機能を実行する。Ｓ７．１４において、機能呼び出し制御部３０８は通信制御部３０３に設定要求の実行結果を応答すると同時に、送信するメッセージに対して署名情報を付与する。Ｓ７．１４において、機能呼び出し制御部３０８はＳ７．８において受信した共通鍵を用いて、実行結果に付与された署名情報を検証する。署名情報の検証後、通信制御部３０３は設定管理部３０４に対して、クラウドユーザーＵＵＩＤとともに設定要求の実行結果を送信する（Ｓ５．１４）。

【００９２】

以上が、共通鍵を用いた場合の機能呼び出し処理である。これにより、Ｗｅｂブラウザ３００を介してデバイス１０５が公開している機能を利用でき、さらにデバイス１０５への設定要求の改竄検知を行うことができる。

【００９３】

［実施例３］

実施例１、２では、デバイス１０５がマルチユーザーデバイスである形態を説明した。実施例３では、デバイス１０５がシングルユーザーデバイスである形態を図１５、図１６を用いて説明する。ただし、マルチユーザーデバイスである場合と同じ過程については、同じステップの番号を用いて詳細の説明を省略する。ここで、シングルユーザーデバイスとは、デバイスの機能を用いる際にログイン操作を必要とせず、複数のローカルユーザーを管理する機能を有さないデバイスのことである。そのため、実施例１や実施例２とは異なり、実施例３でのデバイス１０５はローカルログイン部３０６を備えていない。

【００９４】

図１５を用いて、デバイス１０５がシングルユーザーデバイスの場合の認証連携情報を発行する過程を説明する。マルチユーザーデバイスの場合（図５）との相違点はデバイス１０５がローカルログイン部３０６を備えていないため、ログイン処理によりローカルユーザーを認証する過程（Ｓ２．１～Ｓ２．３）が図１５には存在しない。まず、Ｓ２．４においてＷｅｂブラウザ３０５が認証連携情報の発行要求を受信した後、Ｓ２．５で認証サーバー連携部３０７に認証連携情報の発行要求を送信する。

【００９５】

Ｓ８．１にて、認証サーバー連携部３０７が認証部３０２に対して認証連携情報の発行要求とともに、デバイス識別情報を送信する。Ｓ２．９で、認証部３０２は認証連携情報を発行する。発行された認証連携情報の一例は表２に示した通りである。Ｓ８．２において、認証部３０２が認証連携情報とデバイス識別情報との紐付け情報を管理する。Ｓ２．１１にて、認証部３０２は認証サーバー連携部３０７に対して認証連携情報の応答を行う。Ｓ８．３において、認証サーバー連携部３０７はＳ２．１１において受信した認証連携情報とデバイス識別情報とを紐づけて保存する。Ｓ２．１３で、その認証連携情報をＷｅｂブラウザ３０５に応答し、ユーザーはＷｅｂブラウザ３０５を介して認証連携情報を入手する。Ｓ２．１４で、後述のユーザー情報紐付け処理のために、認証サーバー連携部３０７が機能呼び出し制御部３０８に対して、通信制御部３０３へのｓｕｂｓｃｒｉｂｅメッセージの送信を依頼する。Ｓ２．１５で、機能呼び出し制御部３０８は通信制御部３０３に対して、ｓｕｂｓｃｒｉｂｅメッセージを送信する。ｓｕｂｓｃｒｉｂｅメッセージを送信する際のトピックはデバイス識別情報である。

【００９６】

以上が、デバイス１０５がシングルユーザーデバイスの場合の認証連携情報を発行する過程となる。これにより、認証連携情報とデバイス識別情報とが紐づいた紐付け情報を認証部３０２と認証サーバー連携部３０７とで管理することができ、ユーザーは認証連携情報を入手することができる。

【００９７】

デバイス１０５がシングルユーザーデバイスの場合の、認証サーバー１０３におけるユーザー情報紐付け処理について図６を用いて説明する。図６におけるＳ３．１２を後述のＳ９．１に置き換えることで本処理は実現する。それ以外のステップについてはマルチユーザーデバイスの場合と同じなので、詳細な説明は省略する。

【００９８】

Ｗｅｂブラウザ３００はユーザーから認証連携情報の入力要求を受信し（Ｓ３．６）、認証連携情報の入力要求を認証部３０２に対して送信する（Ｓ３．７）。認証部３０２は受信した入力要求に対して、認証連携情報の入力画面をＷｅｂブラウザ３００に応答する（Ｓ３．８）。Ｗｅｂブラウザ３００はその入力画面を介して認証連携情報の入力操作をユーザーから受け付け（Ｓ３．９）、認証部３０２に対して紐付け処理の要求とともに、受け付けた認証連携情報を送信する（Ｓ３．１０）。認証部３０２は受信した認証連携情報を用いてクラウドユーザーＵＵＩＤと認証連携情報との紐付け処理を行う（Ｓ３．１１）。紐付け処理によって得られた紐付け情報の例は表６に示した通りである。

【００９９】

Ｓ９．１では、認証部３０２はクラウドユーザーＵＵＩＤとデバイス識別情報とが紐づいたマッピングテーブルを生成する。具体的には、Ｓ３．１１で作成した紐付け情報と、

Ｓ８．２で作成した紐付け情報とを用いて、認証連携情報を介してクラウドユーザーＵＵＩＤとデバイス識別情報とを紐付ける。以上がシングルユーザーデバイスの場合の、認証サーバー１０３におけるユーザー紐付け処理である。これにより、認証部３０２はクラウドユーザーＵＵＩＤとデバイス識別情報との紐付け情報を管理することができる。

【０１００】

次に、デバイス１０５がシングルユーザーデバイスの場合の、デバイス１０５におけるユーザー紐付け処理について図７を用いて説明する。図７のＳ４．４を後述のＳ９．２に置きかえることで本処理は実現する。それ以外のマルチユーザーデバイスの場合と同じステップに関しては、同じ符番をふり詳細な説明は省略する。

【０１０１】

認証部３０２は通信制御部３０３に対してクラウドユーザーＵＵＩＤの紐付け依頼を送信する（Ｓ４．１）。通信制御部３０３は機能呼び出し制御部３０８に対してクラウドユーザーＵＵＩＤの紐付け依頼を送信する（Ｓ４．２）。機能呼び出し制御部３０８は認証サーバー連携部３０７に対して、クラウドユーザーＵＵＩＤの紐付け要求を送信する（Ｓ４．３）。その際、Ｓ４．２で受信した認証連携情報とクラウドユーザーＵＵＩＤも同時に通知する。Ｓ９．２において、クラウドユーザーＵＵＩＤとデバイス識別情報とを紐付けた紐付け情報を管理する。認証サーバー連携部３０７はデバイス識別情報と認証連携情報との紐付け情報を管理している（Ｓ８．３）ので、Ｓ９．２ではその紐付け情報とＳ４．３で受信した情報を用いて、クラウドユーザーＵＵＩＤとデバイス識別情報とを紐付けることができる。

【０１０２】

以上が、シングルユーザーデバイスの場合の、デバイス１０５におけるユーザー紐付け処理である。これにより、認証サーバー連携部３０７において、デバイス識別情報とクラウドユーザーＵＵＩＤとの紐付け情報を管理することができる。また、本処理においても、デバイス１０５がマルチユーザーデバイスの場合と同様に、暗号鍵を用いることが可能である。この際、Ｓ９．２にて共通鍵を発行し、クラウドユーザーＵＵＩＤとデバイス識別情報との紐付け情報に対して紐付ける。

【０１０３】

次にシングルユーザーデバイスの場合の機能呼び出し処理について、図１６を用いて説明する。マルチユーザーデバイスの場合と同じステップに関しては、同じ符番をふり詳細な説明は省略する。まず、Ｗｅｂブラウザ３００はユーザーからデバイス識別情報とともに設定画面要求操作を受信する（Ｓ５．１）。Ｗｅｂブラウザ３００は設定管理部３０４に設定画面を要求し（Ｓ５．２）、設定管理部３０４はＷｅｂブラウザ３００に対して応答する（Ｓ５．３）。その際の設定画面の例は図９に示した通りである。Ｗｅｂブラウザ３００は設定情報入力操作をユーザーから受信し（Ｓ５．４）、設定要求を設定管理部３０４に送信する（Ｓ５．５）。設定管理部３０４は通信制御部３０３に対して設定要求を送信する（Ｓ５．６）。

【０１０４】

Ｓ９．３において、通信制御部３０３は認証部３０２に対してクラウドユーザーＵＵＩＤの取得要求を行う。具体的には、Ｓ５．５においてＷｅｂブラウザ３００が設定管理部３０４に送信したセッションＩＤを、設定管理部３０４が通信管理部３０３に送信することで、Ｓ９．３においてクラウドユーザーＵＵＩＤの取得要求とともにセッションＩＤが送信される。認証部３０２は、受信したセッションＩＤと紐付くクラウドユーザーＵＵＩＤを特定し、Ｓ９．４において通信制御部３０３にクラウドユーザーＵＵＩＤの取得応答を行う。

【０１０５】

Ｓ９．５にて通信制御部３０３は機能呼び出し制御部３０８に対し、設定要求としてｐｕｂｌｉｓｈメッセージを送信し、それと同時にクラウドユーザーＵＵＩＤを送信する。これにより、Ｓ２．１５で機能呼び出し制御部３０８が送信したｓｕｂｓｃｒｉｂｅメッセージ（トピックはデバイス識別情報）と同じトピックのｐｕｂｌｉｓｈメッセージを送

信することができる。Ｓ５．４において、オートスリープ移行時間を５分にするための設定要求をＷｅｂブラウザ３００が受け付けたものとすると、Ｓ９．５で送信した設定要求は、オートスリープ移行時間を５分にするための設定要求である。

【０１０６】

Ｓ９．６において、機能呼び出し制御部３０８はＳ５．９で受信したｐｕｂｌｉｓｈメッセージの内容に応じて設定要求を実行する。その際、設定要求とともに受信したクラウドユーザーＵＵＩＤで特定されるクラウドユーザーとして設定要求を実行する。具体的には、機能呼び出し制御部３０８がクラウドユーザーＵＵＩＤ「ＣＣＣ１」を受信した場合、クラウドユーザーＩＤ「ｓｅ００１」としてオートスリープ移行時間を５分にするための設定が実行される。

【０１０７】

Ｓ５．１３において機能呼び出し制御部３０８は、Ｓ５．１２で取得したクラウドユーザーＵＵＩＤとともに実行結果を通信制御部３０３に対して応答する。Ｓ５．１４において、通信制御部３０３は設定管理部３０４に対してクラウドユーザーＵＵＩＤとともに実行結果を送信する。以上が、デバイス１０５がシングルユーザーデバイスである場合の機能呼び出し処理である。これにより、デバイス１０５がシングルユーザーデバイスの場合でも、ユーザーはクライアントデバイス１０２のＷｅｂブラウザ３００を介して、デバイス１０５が公開している機能を利用することができ、その機能を利用したことによる実行結果を確認することができる。

【０１０８】

また、ユーザー情報紐付け処理において暗号鍵を用いて紐付けを行う場合についても説明する。その場合、Ｓ９．４において認証部３０２はクラウドユーザーＵＵＩＤと同時に共通鍵を取得する。Ｓ９．５において、リクエストするメッセージに取得した共通鍵を用いて署名情報を付与する。機能呼び出し制御部３０８が共通鍵を用いて署名情報を検証した後、Ｓ９．６で設定要求を実行する。

【０１０９】

Ｓ５．１３で実行結果を送信する前に、認証サーバー連携部３０７にＳ９．５で受信したクラウドユーザーＵＵＩＤと紐付く共通鍵を取得し、実行結果に署名情報を付与する。実行結果を受信した通信制御部３０３は、共通鍵を用いて実行結果に付与されている署名情報を検証する。検証後、Ｓ５．１４において通信制御部３０３は設定管理部３０４に対してクラウドユーザーＵＵＩＤとともに実行結果を応答する。デバイス１０５がマルチユーザーデバイスである場合と同様に、共通鍵に限定されるわけではなく、例えば公開鍵でも同様に署名情報を付与できる。

【０１１０】

実施例３より、クラウドシステムを介してシングルユーザーデバイスの機能を実行する際に、その実行結果がどのクラウドユーザーＵＵＩＤに対するものなのかをクラウドシステム１０６で特定し、リクエストとレスポンスとを紐付けることができる。

【０１１１】

また、実施例１と実施例３より、デバイス１０５がシングルユーザーデバイスかマルチユーザーデバイスかによって、認証連携情報を発行する過程やユーザーＵＵＩＤの紐付け処理等のシーケンスが異なる。そのためには、デバイス１０５がマルチユーザーデバイスかシングルユーザーデバイスかを予め判定する必要がある。

【０１１２】

その判定方法の一つとして、デバイス１０５のデバイス識別情報を用いる方法がある。デバイス識別情報に予め、デバイス１０５を一意に識別する情報以外にも、デバイス１０５がシングルユーザーデバイスなのか、マルチユーザーデバイスなのかを示す情報が含まれている。その一例を表９に示す。

【０１１３】

【表９】

表９

| デバイス識別情報 |
|---|
| 00001-00 |
| 00002-01 |
| 00003-01 |

【０１１４】

表９では、デバイス識別情報の末尾の数字が「００」の場合はシングルユーザーデバイスであり、「０１」の場合はマルチユーザーデバイスである例を示している。ただし、デバイス識別情報に、デバイス１０５に関する情報を含める形態は表９の形態に限らない。

【０１１５】

Ｓ１．３において、通信部３０１は認証部３０２にデバイス登録要求を送信すると同時に、認証サーバー連携部３０７から受信したデバイス識別情報を通知する。このデバイス識別情報（表９）により、デバイス１０５がマルチユーザーデバイスであるか否かを判定することができる。

【０１１６】

判断方法の二つ目は、認証部３０２がテーブル（表１０）を予め保持している方法である。認証部３０２には予め、デバイス１０５がシングルユーザーデバイスなのかマルチユーザーデバイスなのかを示す情報を管理するテーブルがあり、そのテーブルを参考にしてデバイス１０５の判定を行うことができる。そのテーブルの一例を表１０に示す。

【０１１７】

【表１０】

表１０

| デバイス識別情報 | デバイスの種類 |
|---|---|
| 00001 | シングル |
| 00002 | マルチ |
| 00003 | マルチ |

【０１１８】

今回はデバイス識別情報として数字を例に説明したが、デバイス１０５を一意に識別する情報であれば何でもよい。また、デバイス１０５がマルチユーザーデバイスかシングルユーザーデバイスかの判定は、通信部３０１や認証部３０２、通信制御部３０３が実行してもよく、認証連携情報を発行する過程やユーザーＵＵＩＤの紐付け処理等のシーケンスが開始される前であれば、どのタイミングで行ってもよい。

【０１１９】

実施例３より、デバイス１０５がシングルユーザーデバイスの場合でも、ユーザーはクライアントデバイス１０２のクラウドシステム１０６を介して、デバイス１０５が公開している機能を利用することができ、その機能を利用したことによる実行結果を確認できる。さらに、デバイス１０５がマルチユーザーデバイスなのかどうかを判断することにより、実施例１と実施例３のどちらのシーケンスを実行すべきかを判断できる。

【０１２０】

［実施形４］

実施例１では、ユーザーがデバイス１０５において認証連携情報を取得し、取得した認証連携情報をクライアントデバイス１０２に入力し、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤを紐付けた。実施例４ではクライアントデバイス１０２で認証連携情報を取得し、取得した認証連携情報をデバイス１０５に入力し、ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付ける形態を説明する。

【０１２１】

まず、クライアントデバイス１０２における認証連携情報の発行処理を、図１７を用いて説明する。Ｓ１０．１において、Ｗｅｂブラウザ３００が認証連携情報の発行要求を受信し、Ｓ１０．２において、認証部３０２に対して認証連携情報の発行要求を行う。Ｓ１０．２の発行要求に対して、Ｓ１０．３において認証部３０２が認証連携情報を発行する。表２に示した通り、認証連携情報は文字列としているが、それに限定されるわけではない。Ｓ１０．４にて認証部３０２は、Ｓ１０．３で発行された認証連携情報と現在ログインしているクラウドユーザーのクラウドユーザーＵＵＩＤとを紐付ける。具体的には、Ｓ１０．２において認証部３０２は認証連携情報の発行要求とともにセッションＩＤを受信するため、そのセッションＩＤを介してＳ１０．３において発行された認証連携情報とクラウドユーザーＵＵＩＤとを紐付ける。その際に生成される紐付け情報の例は表１１のとおりである。

【０１２２】

【表１１】

表１１

| クラウドユーザーUUID | 認証連携情報 |
|---|---|
| CCC1 | XXX-YYY-ZZZ |

【０１２３】

Ｓ１０．５にて、認証部３０２はＷｅｂブラウザ３００に対して認証連携情報を応答する。受信した認証連携情報をＷｅｂブラウザ３００が表示することで、ユーザーは認証連携情報を入手することができる。以上が、クライアントデバイス１０２における認証連携情報の発行処理である。

【０１２４】

次に、図１８を用いて、デバイス１０５においてローカルユーザーＵＵＩＤと認証連携情報とを紐付けるユーザー紐付け処理を説明する。ただし、既に説明した過程と同じものについては、同じステップの番号を用いて詳細な説明を省略する。Ｓ２．１において、ローカルログイン部３０６はユーザーのログイン処理を受信する。ローカルログイン部３０６が管理するユーザー情報の一例は表１に示した通りである。Ｓ２．２にて、ローカルログイン部３０６は表１のユーザー情報を参照し、ローカルユーザーＩＤとパスワードの組を用いてローカルユーザー認証を行う。Ｓ２．３では、ローカルログイン部３０６は認証したユーザーのローカルユーザー認証情報を生成し保存する。

【０１２５】

Ｓ１１．１において、Ｗｅｂブラウザ３０５は認証連携情報の入力操作をユーザーから受け付け、認証連携情報の入力完了後にＳ１１．２で認証サーバー連携部３０７に対して認証連携情報の紐付け処理を要求する。Ｓ２．６とＳ２．７により、認証サーバー連携部３０７はローカルログイン部３０６からローカルユーザーＵＵＩＤを取得する。Ｓ１１．３にて、認証サーバー連携部３０７は認証サーバー連携部３０７においてローカルユーザーＵＵＩＤと認証連携情報とを紐付ける。この際にできる紐付け情報の例を表１２に示す。

【０１２６】

【表１２】

表１２

| ローカルユーザーUUID | 認証連携情報 |
|---|---|
| AAA1 | XXX-YYY-ZZZ |

【０１２７】

以上が、デバイス１０５におけるローカルユーザーＵＵＩＤと認証連携情報とを紐付けるユーザー紐付け処理である。

【０１２８】

次に、認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理について図１９を用いて説明する。Ｓ１２．１において、認証サーバー連携部３０７は認証部３０２に対して認証連携情報とローカルユーザーＵＵＩＤとデバイス識別情報とを同時に送り、認証連携情報の紐付け要求を行う。Ｓ１２．２にて認証部３０２は、Ｓ１２．１で受信した認証連携情報とローカルユーザー認証連携情報とデバイス識別情報とを紐付ける。その際にできるマッピングテーブルの例は表３に示した通りである。Ｓ１２．３で認証部３０２は、紐付け情報（表３、表１１）を用いて、クラウドユーザーＵＵＩＤとローカルユーザーＵＵＩＤとデバイス識別情報とを紐付ける。その際にできるマッピングテーブルの例は表７に示した通りである。Ｓ１２．４にて、認証部３０２は認証サーバー連携部３０７に対してクラウドユーザーＵＵＩＤと認証連携情報とを送信し、紐付け要求に対して応答する。Ｓ１２．５において、認証サーバー連携部３０７はＳ１２．４で受信した認証連携情報とクラウドユーザーＵＵＩＤとを紐付ける。Ｓ１２．６で、認証サーバー連携部３０７はＳ１２．５で紐付けた紐付け情報と、Ｓ１１．３で紐付けた紐付け情報とを用いて、クラウドユーザーＵＵＩＤとローカルユーザーＵＵＩＤとを紐付ける。この際にできるマッピングテーブルの例は、表８に示した通りである。Ｓ１２．７にて、Ｓ１１．２の紐付け処理の要求に対する応答として、認証サーバー連携部３０７はＷｅｂブラウザ３０５に対して紐付け処理が完了したことを応答する。これにより、ユーザーに紐付け処理が完了したことが通知される。

【０１２９】

以上が、認証サーバー１０３におけるローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとを紐付けるユーザー紐付け処理である。ローカルユーザーＵＵＩＤとクラウドユーザーＵＵＩＤとのユーザー紐付け処理後の機能呼び出し処理は実施例１（図８）と同様なので省略する。

【０１３０】

実施例４でも、デバイス１０５がシングルユーザーデバイスの場合が考えられる。マルチユーザーデバイスの場合との相違点は、認証部３０２と認証サーバー連携部３０７において、ユーザーマッピングテーブル生成時にローカルユーザー認証情報が存在しないことである。また、実施例４でも実施例２と同様に暗号鍵の交換も行える。

【０１３１】

実施例１と実施例４の過程の使い分けは、デバイス１０５やクライアントデバイス１０２のデバイス特性やユースケースに依存する。例えば実施例１の場合、デバイス１０５がＳＦＰなどのユーザー入力が不向きな装置であり、クライアントデバイス１０２がスマートフォンなどのカメラ搭載端末であれば、認証連携情報としてＱＲコード（登録商標）をデバイス１０５のＷｅｂブラウザ３０５に表示し、クライアントデバイス１０２が搭載するカメラでＱＲコード（登録商標）を読み取り、認証部３０２に対して紐付け要求を行うことができる。

【０１３２】

また、実施例４の場合、例えばデバイス１０５がＭＦＰなどのユーザー入力を受け付け可能のデバイスであり、クライアントデバイス１０２がＰＣなどのカメラ非搭載端末であれば、認証連携情報として文字列をＷｅｂブラウザ３００に表示することでユーザーはその認証連携情報を入手し、デバイス１０５にその認証連携情報を入力することで認証部３０２に対して紐付け要求を行うことができる。つまり、実施例１と実施例４の過程を使い分けることで、クライアントデバイス１０２やデバイス１０５の形態に応じて、ユーザー紐付け処理の手順を変えることができる。

【０１３３】

［他の実施例］

上記の実施例で示したステップにおいて受送信される情報は、上記で例として示した情

報のみならず、その情報を含みさえすればどのような情報を受送信しても良い。例えば、クラウドユーザーＩＤなどの他のクラウドユーザー認証情報とともにクラウドユーザーＵＵＩＤを送信する形態等も考えられる。ローカルユーザーＵＵＩＤの場合も同様である。

【０１３４】

また、本発明の目的は以下の処理を実行することによっても達成される。即ち、上述した実施例の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、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）が記憶媒体に格納されたプログラムコードを読み出す処理である。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施例の機能を実現することになり、そのプログラムコード及び該プログラムコードを記憶した記憶媒体は本発明を構成することになる。

【０１３５】

上述した各実施例によれば、クライアントデバイス１０２からクラウドシステム１０６経由でデバイス１０５の機能を実行する際に、クラウドユーザーＵＵＩＤと紐づくローカルユーザーＵＵＩＤを用いて実行することができる。さらには、クラウドシステム１０６及びデバイス１０５間の非同期処理において、リクエストとレスポンスを紐付けるための識別子を用いること無く、クラウドユーザーに対してデバイス１０５の機能の実行結果を通知することができる。

【０１３６】

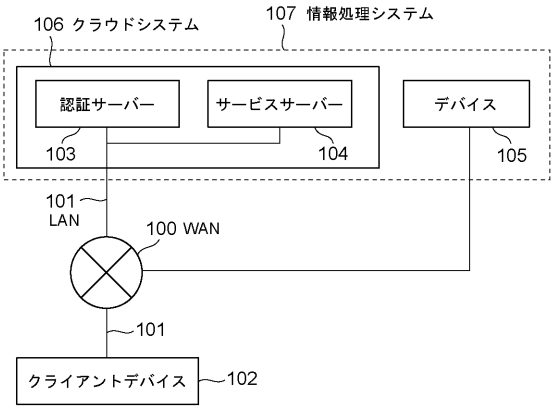
以上で本発明の好ましい形態について詳述したが、本実施例は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【符号の説明】

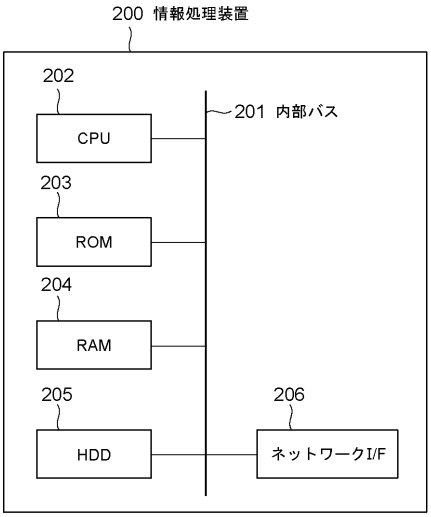
【０１３７】

１０２　クライアントデバイス
１０３　認証サーバー
１０４　サービスサーバー
１０５　デバイス
３００、３０５　Ｗｅｂブラウザ
３０１　通信部
３０２　認証部
３０３　通信制御部
３０４　設定管理部
３０６　ローカルログイン部
３０７　認証サーバー連携部
３０８　機能呼び出し制御部

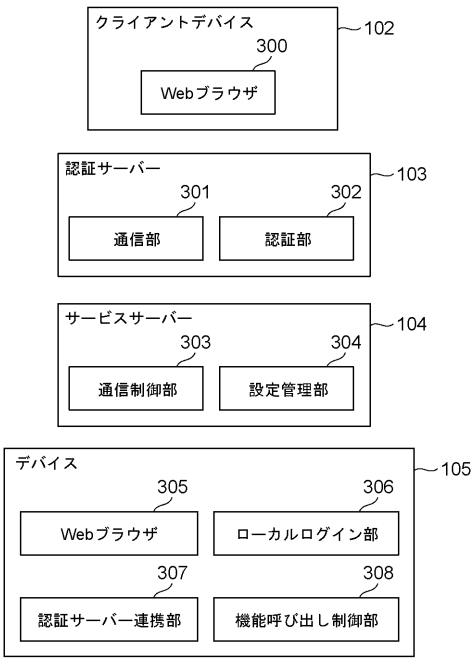
【図１】


106 クラウドシステム
107 情報処理システム
認証サーバー
サービスサーバー
デバイス
103
104
105
101
LAN
100 WAN
101
クライアントデバイス
102

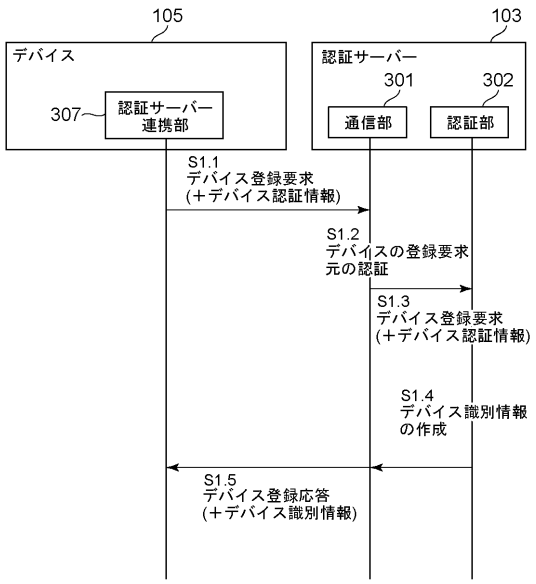
【図２】


200 情報処理装置
202
CPU
201 内部バス
203
ROM
204
RAM
205
HDD
206
ネットワークI/F

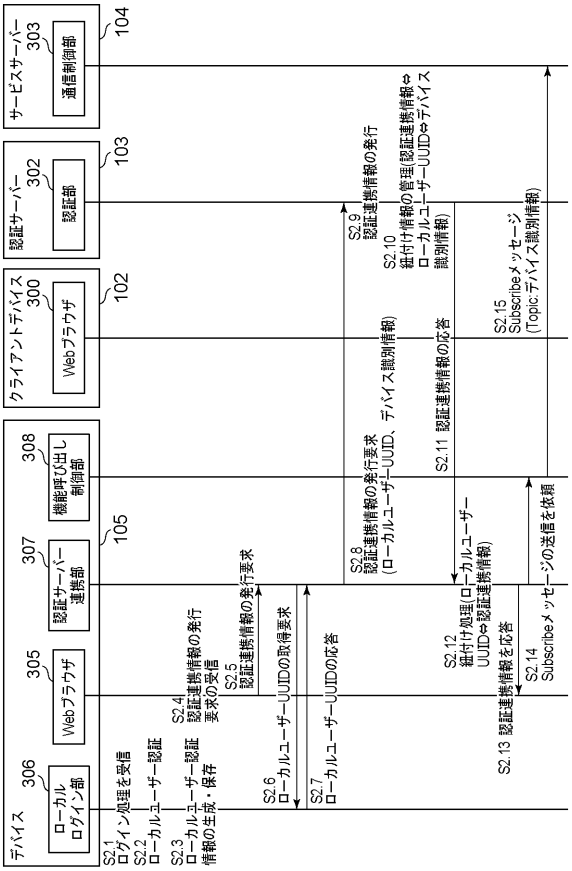
【図３】


クライアントデバイス
102
300
Webブラウザ
認証サーバー
103
301
302
通信部
認証部
サービスサーバー
104
303
304
通信制御部
設定管理部
デバイス
105
305
306
Webブラウザ
ローカルログイン部
307
308
認証サーバー連携部
機能呼び出し制御部

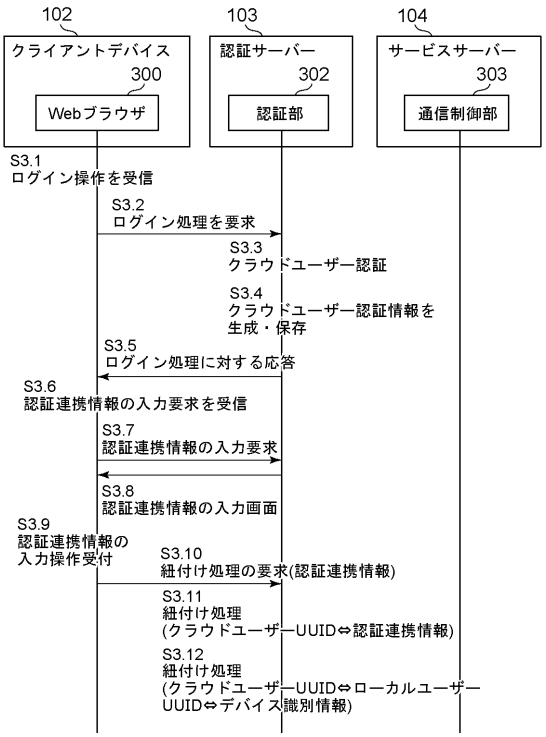
【図４】


105
103
デバイス
認証サーバー
307
認証サーバー連携部
301
302
通信部
認証部
S1.1
デバイス登録要求
(＋デバイス認証情報)
S1.2
デバイスの登録要求元の認証
S1.3
デバイス登録要求
(＋デバイス認証情報)
S1.4
デバイス識別情報の作成
S1.5
デバイス登録応答
(＋デバイス識別情報)

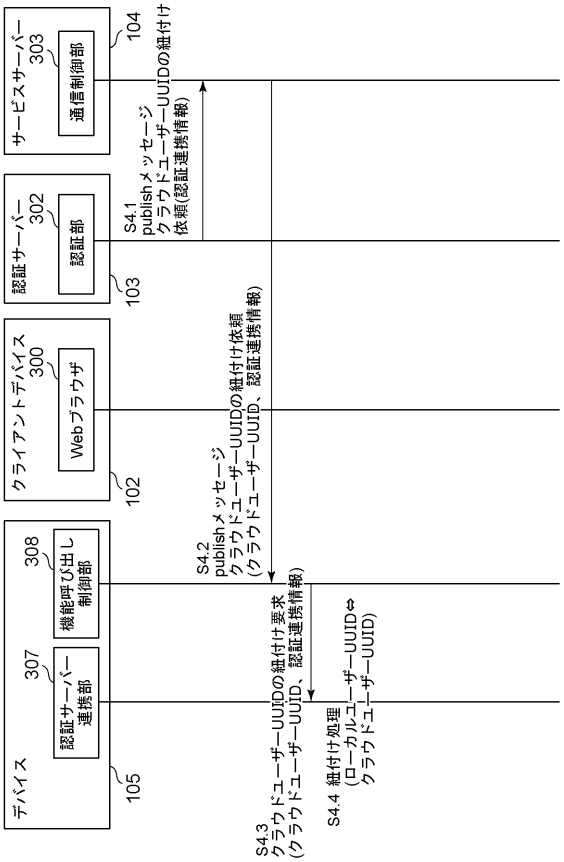
【図５】


サービスサーバー
303
通信制御部
104
認証サーバー
302
認証部
103
クライアントデバイス
300
Webブラウザ
102
デバイス
306
ローカルログイン部
Webブラウザ
305
認証サーバー連携部
307
機能呼び出し制御部
308
105
S2.1 ログイン処理を受信
S2.2 ローカルユーザー認証
S2.3 ローカルユーザー認証情報の生成・保存
S2.4 認証連携情報の発行要求
S2.5 認証連携情報の発行要求
S2.6 ローカルユーザーUUIDの取得要求
S2.7 ローカルユーザーUUIDの応答
S2.8 認証連携情報の発行要求 (ローカルユーザーUUID、デバイス識別情報)
S2.9 認証連携情報の発行
S2.10 紐付け情報の管理(認証連携情報⇔ローカルユーザーUUID⇔デバイス識別情報)
S2.11 認証連携情報の応答
S2.12 紐付け処理(ローカルユーザーUUID⇔認証連携情報)
S2.13 認証連携情報を応答
S2.14 Subscribeメッセージの送信を依頼
S2.15 Subscribeメッセージ (Topicデバイス識別情報)

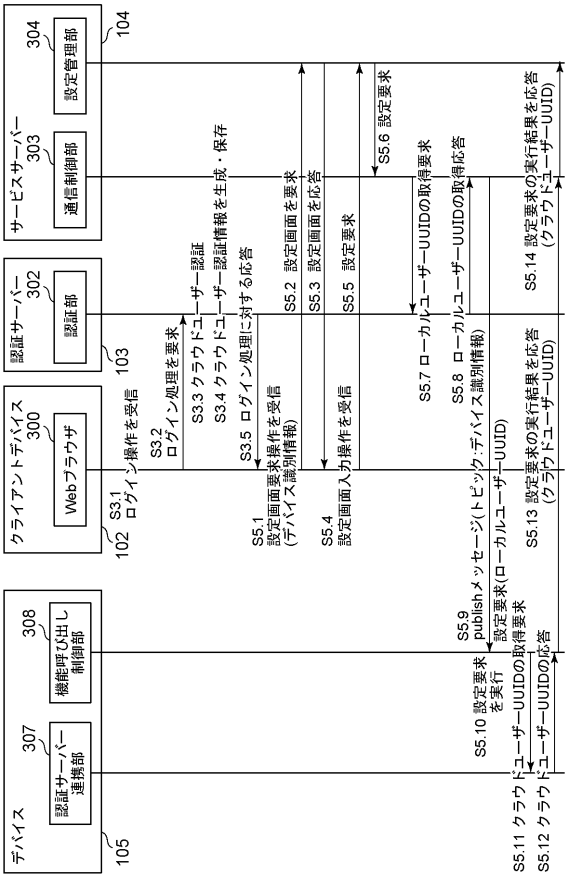
【図６】


102
クライアントデバイス
300
Webブラウザ
103
認証サーバー
302
認証部
104
サービスサーバー
303
通信制御部
S3.1 ログイン操作を受信
S3.2 ログイン処理を要求
S3.3 クラウドユーザー認証
S3.4 クラウドユーザー認証情報を生成・保存
S3.5 ログイン処理に対する応答
S3.6 認証連携情報の入力要求を受信
S3.7 認証連携情報の入力要求
S3.8 認証連携情報の入力画面
S3.9 認証連携情報の入力操作受付
S3.10 紐付け処理の要求(認証連携情報)
S3.11 紐付け処理 (クラウドユーザーUUID⇔認証連携情報)
S3.12 紐付け処理 (クラウドユーザーUUID⇔ローカルユーザーUUID⇔デバイス識別情報)

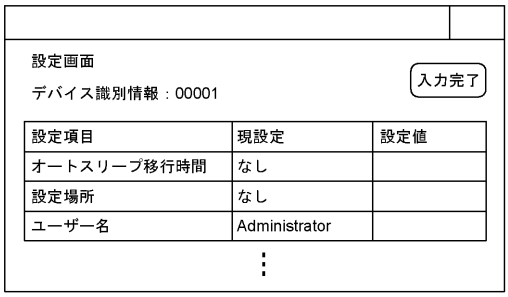
【図７】


サービスサーバー
303
通信制御部
104
認証サーバー
302
認証部
103
クライアントデバイス
300
Webブラウザ
102
デバイス
307
認証サーバー連携部
機能呼び出し制御部
308
105
S4.1 publishメッセージ クラウドユーザーUUIDの紐付け依頼(認証連携情報)
S4.2 publishメッセージ クラウドユーザーUUIDの紐付け依頼 (クラウドユーザーUUID、認証連携情報)
S4.3 クラウドユーザーUUIDの紐付け要求 (クラウドユーザーUUID、認証連携情報)
S4.4 紐付け処理 (ローカルユーザーUUID⇔クラウドユーザーUUID)

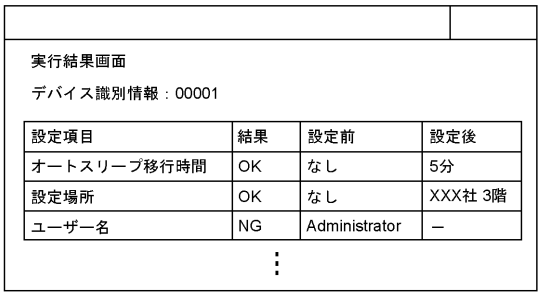
【図８】


サービスサーバー
303
通信制御部
304
設定管理部
104
認証サーバー
302
認証部
103
クライアントデバイス
300
Webブラウザ
102
デバイス
307
認証サーバー連携部
機能呼び出し制御部
308
105
S3.1 ログイン操作を受信
S3.2 ログイン処理を要求
S3.3 クラウドユーザー認証
S3.4 クラウドユーザー認証情報を生成・保存
S3.5 ログイン処理に対する応答
S5.1 設定画面要求操作を受信 (デバイス識別情報)
S5.2 設定画面を要求
S5.3 設定画面を応答
S5.4 設定画面入力操作を受信
S5.5 設定要求
S5.6 設定要求
S5.7 ローカルユーザーUUIDの取得要求
S5.8 ローカルユーザーUUIDの取得応答
S5.9 publishメッセージ(トピック:デバイス識別情報) 設定要求(ローカルユーザーUUID)
S5.10 設定要求を実行
S5.11 クラウドユーザーUUIDの取得要求
S5.12 クラウドユーザーUUIDの応答
S5.13 設定要求の実行結果を応答 (クラウドユーザーUUID)
S5.14 設定要求の実行結果を応答 (クラウドユーザーUUID)

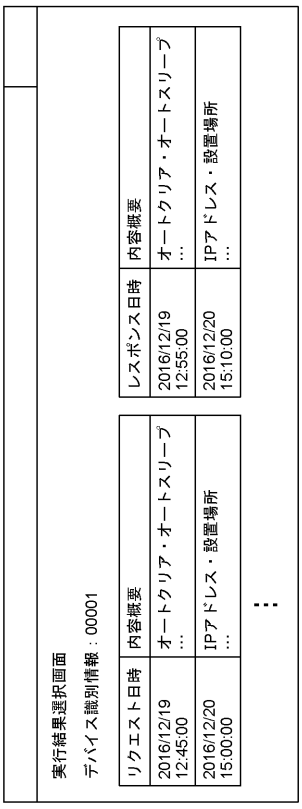
【図９】



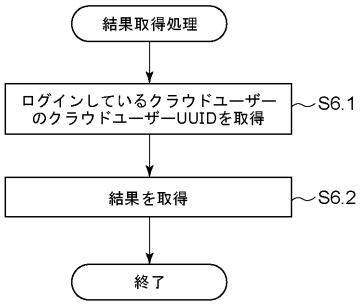

【図１０】



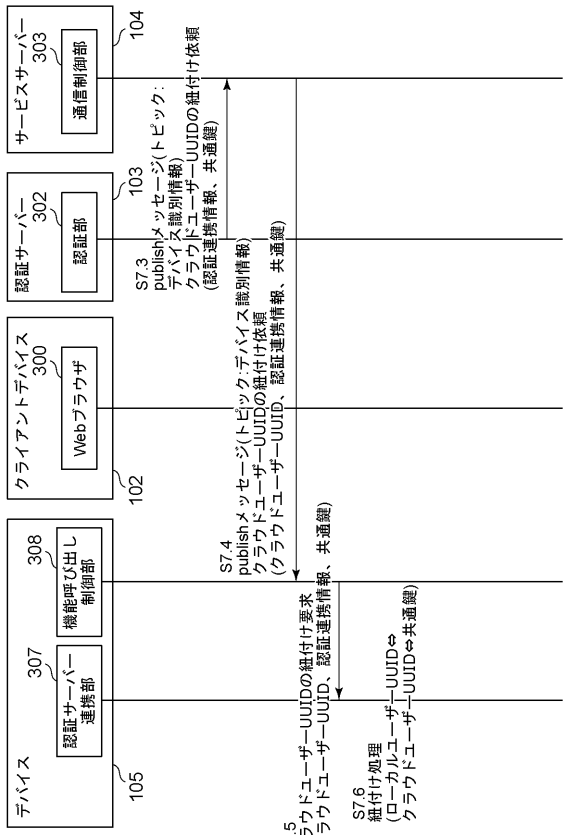

【図１１】



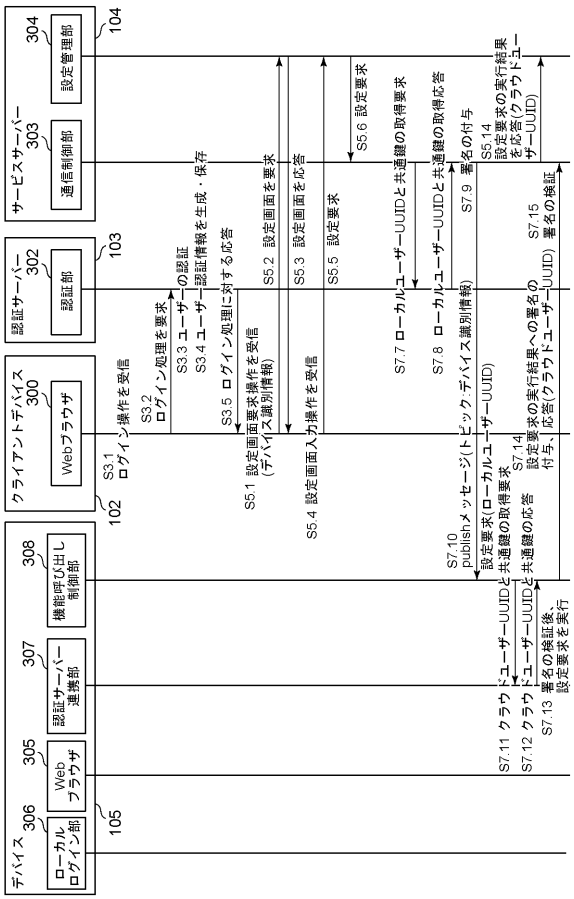

【図１２】



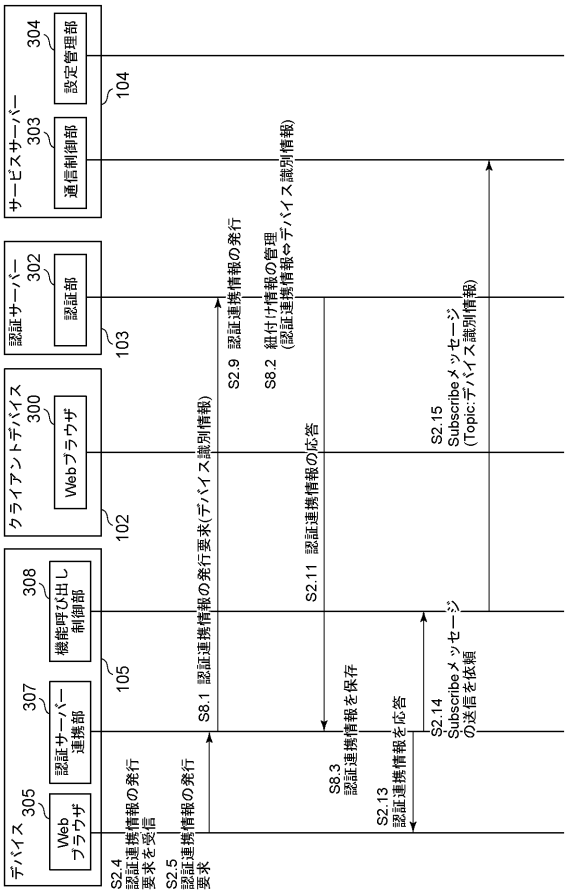
【図１３】



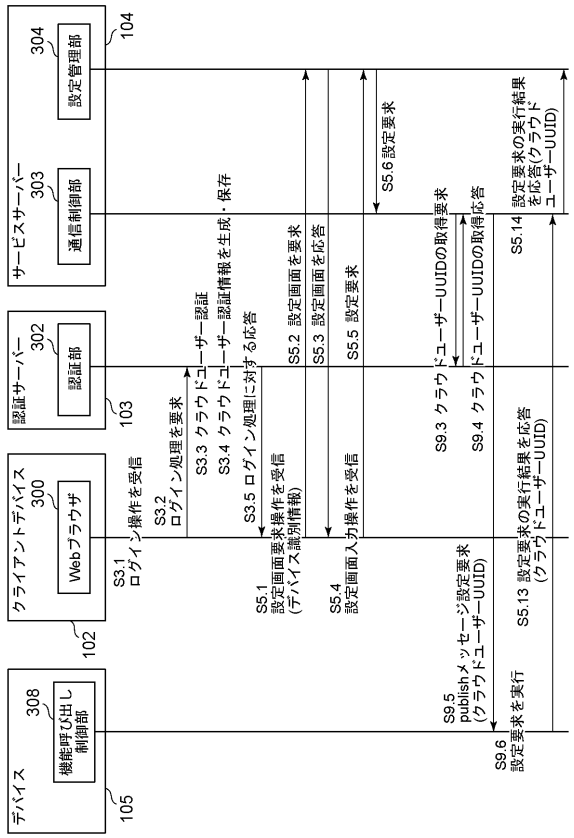

【図１４】



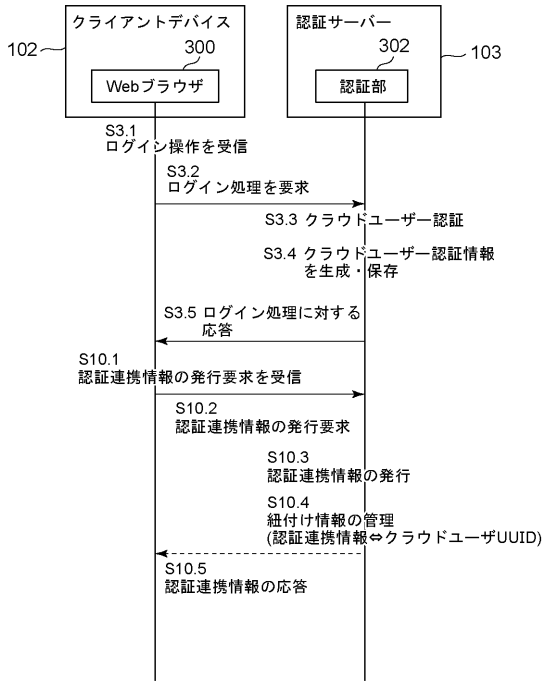

【図１５】



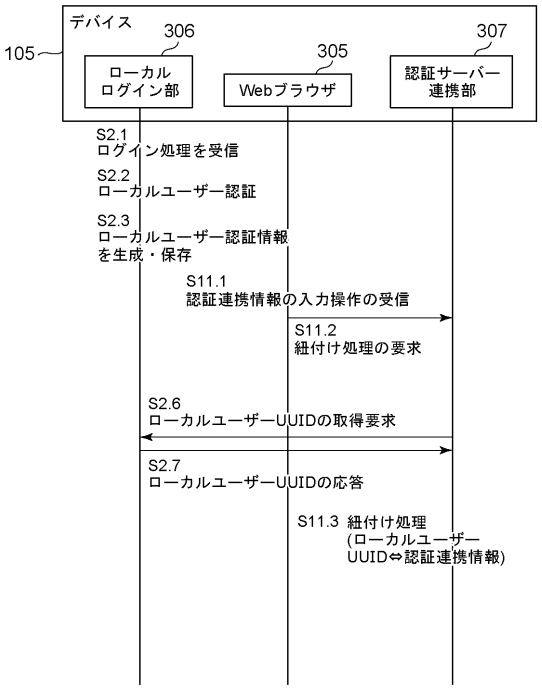

【図１６】



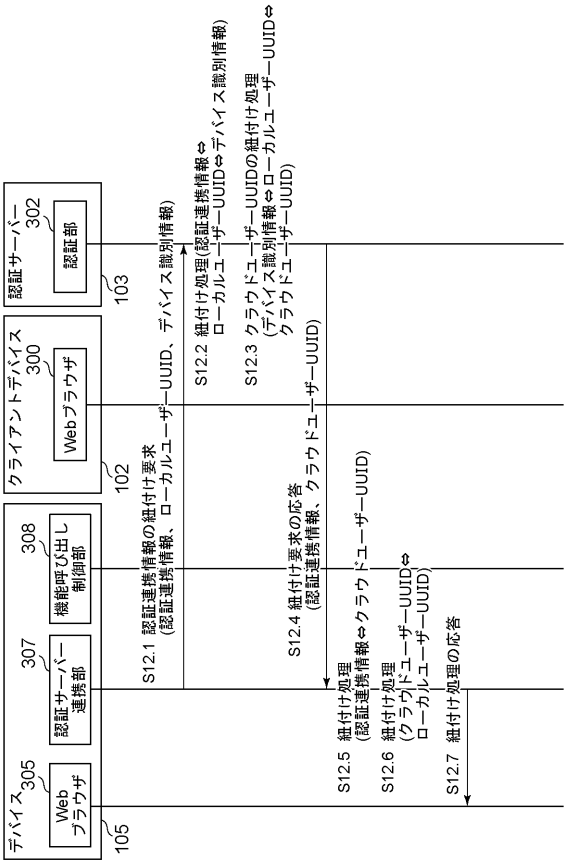
【図１７】


クライアントデバイス
102
300
Webブラウザ
認証サーバー
302
認証部
103
S3.1
ログイン操作を受信
S3.2
ログイン処理を要求
S3.3 クラウドユーザー認証
S3.4 クラウドユーザー認証情報
を生成・保存
S3.5 ログイン処理に対する
応答
S10.1
認証連携情報の発行要求を受信
S10.2
認証連携情報の発行要求
S10.3
認証連携情報の発行
S10.4
紐付け情報の管理
(認証連携情報⇔クラウドユーザUUID)
S10.5
認証連携情報の応答

【図１８】


デバイス
105
ローカル
ログイン部
306
Webブラウザ
305
認証サーバー
連携部
307
S2.1
ログイン処理を受信
S2.2
ローカルユーザー認証
S2.3
ローカルユーザー認証情報
を生成・保存
S11.1
認証連携情報の入力操作の受信
S11.2
紐付け処理の要求
S2.6
ローカルユーザーUUIDの取得要求
S2.7
ローカルユーザーUUIDの応答
S11.3 紐付け処理
(ローカルユーザー
UUID⇔認証連携情報)

【図１９】


認証サーバー
302
認証部
103
クライアントデバイス
300
Webブラウザ
102
デバイス
305
Web
ブラウザ
307
認証サーバー
連携部
308
機能呼び出し
制御部
105
S12.1 認証連携情報の紐付け要求
(認証連携情報、ローカルユーザーUUID、デバイス識別情報)
S12.2 紐付け処理(認証連携情報⇔
ローカルユーザーUUID⇔デバイス識別情報)
S12.3 クラウドユーザーUUIDの紐付け処理
(デバイス識別情報⇔ローカルユーザーUUID⇔
クラウドユーザーUUID)
S12.4 紐付け要求の応答
(認証連携情報、クラウドユーザーUUID)
S12.5 紐付け処理
(認証連携情報⇔クラウドユーザーUUID)
S12.6 紐付け処理
(クラウドユーザーUUID⇔
ローカルユーザーUUID)
S12.7 紐付け処理の応答

フロントページの続き

(56)参考文献 特開２０１７－００４４０３（ＪＰ，Ａ）
特開２０１４－２３５５０２（ＪＰ，Ａ）
特開２０１３－１８６６７４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　１３／００