(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2017-211769
(P2017-211769A)
(43)公開日　平成29年11月30日(2017.11.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 13/00	(2006.01)	G06F	13/00	510A	5B084
H04L 12/70	(2013.01)	H04L	12/70	A	5K030

審査請求 未請求　請求項の数 10　ＯＬ　（全 25 頁）

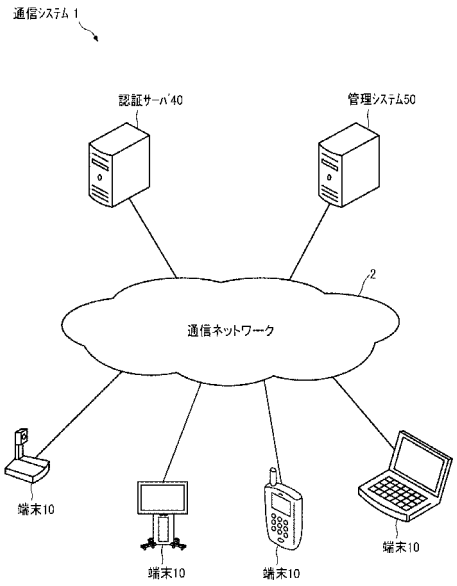
(21)出願番号　特願2016-103489 (P2016-103489)
(22)出願日　平成28年5月24日 (2016.5.24)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　日野原　寛
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　梅原　直樹
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　宮本　篤
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　堀内　岳志
東京都大田区中馬込１丁目３番６号　株式会社リコー内

最終頁に続く

(54)【発明の名称】管理システム、通信システム、認可方法、及びプログラム

(57)【要約】
【課題】　同じユーザの異なる通信端末を識別するために、通信端末ごとに認証用の情報を生成して認証することとした場合には、認証用の情報の生成に伴う通信システムの負荷が大きくなる。
【解決手段】　管理システム５０の送受信部５１は、自管理システムの利用が認可されたユーザのユーザ名を含む認可トークン、及び、ユーザ名に端末名が付加されているアカウント名を受信する。送受信部５１によるアカウント名の受信に応じて、管理システム５０のトークン確認部５２は、認可トークンに含まれるユーザ名、及びアカウント名から抽出されるユーザ名が一致するかにより認証する。トークン確認部５２によって認証されると、sub処理部５４は、上記のアカウント名に対応するアカウントに対して、端末１０間で送信されるメッセージのsubを認可する。
【選択図】図１



【特許請求の範囲】
【請求項１】
自管理システムの利用が認可された対象の識別情報を含む認可情報、及び、認証の対象の識別情報に通信端末の識別情報が付加されている付加情報を受信する受信手段と、
前記受信手段で受信した前記認可された対象の識別情報、及び前記受信手段で受信した前記付加情報のうち前記認証の対象の識別情報が一致するかにより認証する認証手段と、
前記認証手段によって認証されると、前記付加情報に対応するアカウントに対して、通信端末間で送信される情報の受信を認可する認可手段と、
を有する管理システム。
【請求項２】
同じ前記認証の対象の識別情報を含む異なるアカウントによる自管理システムへの接続数が所定数に達すると、前記認証の対象の識別情報を含むアカウントが接続要求するときに、自管理システムへの接続を制限する制限手段を有する請求項１に記載の管理システム。
【請求項３】
前記受信手段は、前記認証の対象の識別情報、前記通信端末の識別情報、及び、前記認証の対象の識別情報を抽出するための抽出情報を含む付加情報を受信する請求項１又は２に記載の管理システム。
【請求項４】
前記認可情報を出力する出力システムと、
請求項１乃至３のいずれか一項に記載の管理システムと、を有し、
前記管理システムの前記認証手段は、前記出力システムによって出力される前記認可情報、及び前記通信端末によって送信される前記認証の対象の識別情報が一致するかにより認証する通信システム。
【請求項５】
更に、前記付加情報を送信する通信端末を有する請求項４に記載の通信システム。
【請求項６】
請求項１乃至３のいずれか一項に記載の管理システムと、
前記通信端末と、
を有する通信システム。
【請求項７】
前記通信端末は、
入力される前記認証の対象の識別情報に、当該通信端末の識別情報を付加した付加情報を前記管理システムへ送信する請求項６に記載の通信システム。
【請求項８】
管理システムに、
自管理システムの利用が認可された対象の識別情報を含む認可情報、及び、認証の対象の識別情報に通信端末の識別情報が付加されている付加情報を受信する処理と、
前記処理で受信した前記認可された対象の識別情報、及び前記処理で受信した前記付加情報のうち前記認証の対象の識別情報が一致するかにより認証する処理と、
前記処理によって認証されると、前記付加情報に対応するアカウントに対して、通信端末間で送信される情報の受信を認可する処理と、
を実行させる認可方法。
【請求項９】
前記通信端末に、
入力される前記対象の識別情報に、当該通信端末の識別情報を付した付加情報を前記管理システムへ送信する処理を実行させる請求項８に記載の認可方法。
【請求項１０】
管理システムに、
自管理システムの利用が認可された対象の識別情報を含む認可情報、及び、認証の対象

の識別情報に通信端末の識別情報が付加された付加情報を受信する処理と、
前記処理で受信した前記認可された対象の識別情報、及び前記処理で受信した前記付加情報のうち前記認証の対象の識別情報が一致するかにより認証する処理と、
前記処理によって認証されると、前記付加情報に対応するアカウントに対して、通信端末間で送信される情報の受信を認可する処理と、
を実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、管理システム、通信システム、認可方法、及びプログラムに関する。
【背景技術】
【０００２】
近年、当事者の移動の経費や時間を削減する要請等に伴い、インターネットや専用線等の通信ネットワークを介して通信する通信システムが普及している。このような通信システムでは、認証システムを設けて、通信端末ごとのユーザ認証を行う。これにより、通信端末ごとのユーザを識別できるようになるので、通信端末による指定されたユーザ間のコミュニケーションが可能になる。
【０００３】
特許文献１には、ユーザアカウント名の自動割当システムにおいて、端末がネットワークに接続後、前記端末がＡＰサーバのサーバ・ソフトウェアへアクセスする前に、前記端末がＤＨＣＰサーバによって割り当てられる前記ネットワークのホストアドレスを取得し、前記端末が当該ホストアドレスを接尾語とするユーザアカウント名を生成することでユーザアカウント名の自動割り当てを行うことが開示されている。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
例えば、IoT(Internet of Things)などの分野では、異なるユーザの通信端末間の通信に限らず、同じユーザの異なる通信端末間の通信が確立される。しかしながら、同じユーザの異なる通信端末を識別するために、通信端末ごとに認証用の情報を生成して認証することとした場合には、認証用の情報の生成に伴う通信システムの負荷が大きくなるという課題が生じる。
【課題を解決するための手段】
【０００５】
請求項１に係る発明の管理システムは、自管理システムの利用が認可された対象の識別情報を含む認可情報、及び、認証の対象の識別情報に通信端末の識別情報が付加されている付加情報を受信する受信手段で受信した前記認可された対象の識別情報、及び前記受信手段で受信した前記付加情報のうち前記認証の対象の識別情報が一致するかにより認証する認証手段と、前記認証手段によって認証されると、前記付加情報に対応するアカウントに対して、通信端末間で送信される情報の受信を認可する認可手段と、を有する。
【発明の効果】
【０００６】
以上説明したように本発明によれば、同じユーザの異なる通信端末間の通信を行うときに、認証用の情報の生成に伴う通信システムの負荷を軽減できるという効果を奏する。
【図面の簡単な説明】
【０００７】
【図１】本発明の一実施形態に係る通信システムの概略図である。
【図２】一実施形態に係る端末のハードウェア構成図である。
【図３】一実施形態に係る管理システムのハードウェア構成図である。
【図４】一実施形態に係る端末のソフトウェア構成図である。
【図５】一実施形態に係る端末、認証サーバ、及び管理システムの各機能ブロック図であ

る。
【図６】認証サーバが管理する各管理テーブルを示す概念図である。
【図７】管理システムが管理する各管理テーブルを示す概念図である。
【図８】一実施形態における認証処理を示すシーケンス図である。
【図９】ログイン要求を許可するか判断する処理を示すフロー図である。
【図１０】端末間でメッセージを送信する処理の一例を示すシーケンス図である。
【図１１】メッセージをsubする権限を有するかを判断する処理の一例を示したフロー図である。
【図１２】メッセージをpubする権限を有するかを判断する処理の一例を示したフロー図である。
【図１３】端末間でメッセージを送信する処理の一例を示すシーケンス図である。
【図１４】一実施形態における認証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】
【０００８】
以下、本発明の実施形態について説明する。
【０００９】
＜＜通信システムの概略＞＞
図１は、本発明の一実施形態に係る通信システムの概略図である。図１に示されているように、通信システム１は、通信端末１０、認証サーバ４０、管理システム５０によって構築されている。以下、通信端末１０を単に端末１０と記載する。
【００１０】
管理システム５０は、出版－購読（Publish-Subscribe、以下PubSubと記載する）モデルにおいて、クライアント間でメッセージを交換するために、クライアントから、メッセージの出版（Publish、以下pubと記載する）やメッセージの購読（Subscribe、以下subと記載する）の要求を受け付けるサーバである。管理システム５０は、PubSubモデルに対応するプロトコルとして、例えば、MQTT（MQ Telemetry Transport）や、XMPP（eXtensible Messaging and Presence Protocol）のPubSub拡張（XEP-0060）等を実装しても良い。
【００１１】
端末１０は、例えば、汎用端末であって、任意のクライアントアプリケーションがインストールされている。以下、クライアントアプリケーションをクライアントアプリと表す。また、端末１０は、例えば、専用端末であって、クライアントとして稼働する特定のクライアントアプリが組み込まれている。端末１０が通信ネットワーク２を介して管理システム５０と通信可能に接続することで、各クライアントは、管理システム５０にメッセージのpubやメッセージのsubを要求することができる。端末１０は、例えば、テレビ会議端末、電子黒板、電子看板、電話、タブレット、スマートフォン、カメラ、ＰＣ（personal computer）等であっても良い。
【００１２】
認証サーバ４０は、端末１０上で動作するクライアントアプリである「クライアント」と、そのクライアントを利用する「ユーザ」とをそれぞれ認証し、管理システム５０の利用を認可するサーバである。管理システム５０は、上記の認証及び認可を実現するため、例えば、OAuth 2.0やOpenID Connectといった認証、認可のプロトコルを実装する。
【００１３】
図１では、説明を簡単にするために、管理システム５０、及び認証サーバ４０がそれぞれ一つの装置である場合について説明したが、本発明はこのような実施形態に限定されない。管理システム５０、及び認証サーバ４０の少なくとも一方は、複数の装置により構築されていても良い。また、管理システム５０、及び認証サーバ４０が、一つのシステム又は装置によって構築されていても良い。また、図１では、説明を簡単にするために、通信システム１において、４つの端末１０が設けられている場合について説明したが、本発明はこのような実施形態に限定されない。通信システム１に設けられる端末１０は、２つであっても、３つであっても、５つ以上であっても良い。また、各端末１０は、それぞれ同

種であっても、図１のように異種であっても良い。
【００１４】
＜＜ハードウェア構成＞＞
次に、通信システム１を構成する各装置のハードウェア構成を説明する。
【００１５】
図２は、一実施形態に係る端末１０のハードウェア構成図である。なお、端末１０は、通信可能であれば、端末１０のハードウェア構成は図２の構成に限定されない。例えば、端末１０は、図２に記載されていない構成が含まれていても、図２に記載の構成の一部が含まれていなくても良い。また、図２に記載の構成の一部は端末１０に接続可能な外部装置等であっても良い。図２に示されているように、本実施形態の端末１０は、端末１０全体の動作を制御するＣＰＵ(Central Processing Unit)１０１、ＩＰＬ(Initial Program Loader)等のＣＰＵ１０１の駆動に用いられるプログラムを記憶したＲＯＭ(Read Only Memory)１０２、ＣＰＵ１０１のワークエリアとして使用されるＲＡＭ(Random Access Memory)１０３、端末１０の各種端末用のプログラム、画像データ、及び音データ等の各種データを記憶するフラッシュメモリ１０４、ＣＰＵ１０１の制御にしたがってフラッシュメモリ１０４に対する各種データの読み出し又は書き込みを制御するＳＳＤ（Solid State Drive）１０５、フラッシュメモリやＩＣカード（Integrated Circuit Card）等の記録メディア１０６に対するデータの読み出し又は書き込み（記憶）を制御するメディアＩ／Ｆ１０７、宛先を選択する場合などに操作される操作ボタン１０８、端末１０の電源のＯＮ／ＯＦＦを切り換えるための電源スイッチ１０９、通信ネットワーク２を利用してデータ伝送をするためのネットワークＩ／Ｆ(Interface)１１１を備えている。
【００１６】
また、端末１０は、ＣＰＵ１０１の制御に従って被写体を撮像して画像データを得る内蔵型のカメラ１１２、このカメラ１１２の駆動を制御する撮像素子Ｉ／Ｆ１１３、音を入力する内蔵型のマイク１１４、音を出力する内蔵型のスピーカ１１５、ＣＰＵ１０１の制御に従ってマイク１１４及びスピーカ１１５との間で音信号の入出力を処理する音入出力Ｉ／Ｆ１１６、ＣＰＵ１０１の制御に従って外付けのディスプレイ１２０に画像データを伝送するディスプレイＩ／Ｆ１１７、各種の外部機器を接続するための外部機器接続Ｉ／Ｆ１１８、端末１０の各種機能の異常を知らせるアラームランプ１１９、及び上記各構成要素を図２に示されているように電気的に接続するためのアドレスバスやデータバス等のバスライン１１０を備えている。
【００１７】
ディスプレイ１２０は、被写体の画像や操作等を表示する液晶や有機ＥＬ(Organic Electroluminescence)によって構成された表示部である。また、ディスプレイ１２０は、ケーブル１２０ｃによってディスプレイＩ／Ｆ１１７に接続される。このケーブル１２０ｃは、アナログＲＧＢ（ＶＧＡ）信号用のケーブルであってもよいし、コンポーネントビデオ用のケーブルであってもよいし、ＨＤＭＩ（登録商標）(High-Definition Multimedia Interface)やＤＶＩ(Digital Video Interactive)信号用のケーブルであってもよい。
【００１８】
カメラ１１２は、レンズや、光を電荷に変換して被写体の画像（映像）を電子化する固体撮像素子を含み、固体撮像素子として、ＣＭＯＳ(Complementary Metal Oxide Semiconductor)や、ＣＣＤ（Charge Coupled Device）等が用いられる。
【００１９】
外部機器接続Ｉ／Ｆ１１８には、筐体１１００の接続口１１３２に差し込まれたＵＳＢ(Universal Serial Bus)ケーブル等によって、外付けカメラ、外付けマイク、及び外付けスピーカ等の外部機器がそれぞれ電気的に接続可能である。外付けカメラが接続された場合には、ＣＰＵ１０１の制御に従って、内蔵型のカメラ１１２に優先して、外付けカメラが駆動する。同じく、外付けマイクが接続された場合や、外付けスピーカが接続された場合には、ＣＰＵ１０１の制御に従って、それぞれが内蔵型のマイク１１４や内蔵型のスピーカ１１５に優先して、外付けマイクや外付けスピーカが駆動する。

【００２０】
なお、記録メディア１０６は、端末１０に対して着脱自在な構成となっている。また、ＣＰＵ１０１の制御にしたがってデータの読み出し又は書き込みを行う不揮発性メモリであれば、フラッシュメモリ１０４に限らず、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）等を用いてもよい。
【００２１】
図３は、一実施形態に係る管理システム５０のハードウェア構成図である。管理システム５０は、管理システム５０全体の動作を制御するＣＰＵ５０１、ＩＰＬ等のＣＰＵ５０１の駆動に用いられるプログラムを記憶したＲＯＭ５０２、ＣＰＵ５０１のワークエリアとして使用されるＲＡＭ５０３、管理システム５０用のプログラム等の各種データを記憶するＨＤ５０４、ＣＰＵ５０１の制御にしたがってＨＤ５０４に対する各種データの読み出し又は書き込みを制御するＨＤＤ(Hard Disk Drive)５０５、フラッシュメモリ等の記録メディア５０６に対するデータの読み出し又は書き込み（記憶）を制御するメディアドライブ５０７、カーソル、メニュー、ウィンドウ、文字、又は画像などの各種情報を表示するディスプレイ５０８、通信ネットワーク２を利用してデータ通信するためのネットワークＩ／Ｆ５０９、文字、数値、各種指示などの入力のための複数のキーを備えたキーボード５１１、各種指示の選択や実行、処理対象の選択、カーソルの移動などを行うマウス５１２、着脱可能な記録媒体の一例としてのＣＤ－ＲＯＭ(Compact Disc Read Only Memory)５１３に対する各種データの読み出し又は書き込みを制御するＣＤ－ＲＯＭドライブ５１４、及び、上記各構成要素を図３に示されているように電気的に接続するためのアドレスバスやデータバス等のバスライン５１０を備えている。
認証サーバ４０は、管理システム５０と同様のハードウェア構成を有しているため、その説明を省略する。
【００２２】
＜＜ソフトウェア構成＞＞
図４は、一実施形態に係る端末１０のソフトウェア構成図である。図４に示されているように、ＯＳ１０２０、クライアントアプリ（１０３１，１０３２）は、端末１０のＲＡＭ１０３の作業領域１０１０上で動作する。ＯＳ１０２０、及び、クライアントアプリ（１０３１，１０３２）は、端末１０にインストールされている。
【００２３】
ＯＳ１０２０は、基本的な機能を端末１０に提供し、端末１０全体を管理する基本ソフトウェアである。クライアントアプリ（１０３１，１０３２）は、認証サーバ４０に認証を要求し、管理システム５０にpub要求及びsub要求の少なくとも一つを実行するためのアプリである。
【００２４】
なお、図４では少なくとも２つのクライアントアプリ（１０３１，１０３２）が端末１０にインストールされているが、１以上の任意の数のクライアントアプリが端末１０にインストールされていれば良い。また、ＯＳ１０２０上で任意のアプリケーションが動作しており、この任意のアプリケーション上でクライアントアプリが動作しても良い。
【００２５】
＜＜機能構成＞＞
次に、本実施形態の機能構成について説明する。図５は、一実施形態に係る通信システム１の一部を構成する端末１０、認証サーバ４０、及び管理システム５０の機能ブロック図である。図５では、端末１０、認証サーバ４０、及び管理システム５０が、通信ネットワーク２を介してデータ通信することができるように接続されている。
【００２６】
＜端末の機能構成＞
端末１０は、送受信部１１、操作入力受付部１２、表示制御部１３、認証要求部１４、pub要求部１５、sub要求部１６、及び記憶・読出部１９を有している。これら各部は、図２に示されている各構成要素のいずれかが、フラッシュメモリ１０４からＲＡＭ１０３上

に展開されたプログラムに従ったＣＰＵ１０１からの命令によって動作することで実現される機能である。また、端末１０は、図２に示されているＲＯＭ１０２、ＲＡＭ１０３、フラッシュメモリ１０４によって構築される記憶部１０００を有している。

【００２７】

（端末の各機能構成）

次に、図２及び図５を用いて、端末１０の各機能構成について詳細に説明する。なお、以下では、端末１０の各機能構成を説明するにあたって、図２に示されている各構成要素のうち、端末１０の各機能構成を実現させるための主な構成要素との関係も説明する。

【００２８】

送受信部１１は、ＣＰＵ１０１からの命令、及びネットワークＩ／Ｆ１１１によって実現され、通信ネットワーク２を介して、相手側の端末、各装置又はシステム等と各種データ（または情報）の送受信を行う。

【００２９】

操作入力受付部１２は、ＣＰＵ１０１からの命令、並びに操作ボタン１０８及び電源スイッチ１０９によって実現され、ユーザによる各種入力を受け付けたり、ユーザによる各種選択を受け付けたりする。

【００３０】

表示制御部１３は、ＣＰＵ１０１からの命令、及びディスプレイＩ／Ｆ１１７によって実現され、通話する際に相手側から送られてきた画像データをディスプレイ１２０に送信するための制御を行う。

【００３１】

認証要求部１４は、クライアントアプリに従ったＣＰＵ１０１からの命令によって実現され、認証サーバ４０に対して認証を要求する。なお、端末１０において複数のクライアントアプリがインストールされている場合、端末１０には、起動したクライアントアプリ毎に認証要求部１４が生成される。

【００３２】

pub要求部１５は、クライアントアプリに従ったＣＰＵ１０１からの命令によって実現され、管理システム５０に対してメッセージのpub要求をする。なお、クライアントアプリがsubに対応する一方でpubには対応していない場合、端末１０においてpub要求部１５は生成されない。また、端末１０においてpubに対応した複数のクライアントアプリがインストールされている場合、端末１０には、起動したクライアントアプリ毎にpub要求部１５が生成される。

【００３３】

sub要求部１６は、クライアントアプリに従ったＣＰＵ１０１からの命令によって実現され、管理システム５０に対してメッセージのsub要求をする。なお、クライアントアプリがpubに対応する一方でsubには対応していない場合、端末１０においてsub要求部１６は生成されない。また、端末１０においてsubに対応した複数のクライアントアプリがインストールされている場合、端末１０には、起動したクライアントアプリ毎にsub要求部１６が生成される。

【００３４】

記憶・読出部１９は、ＣＰＵ１０１からの命令及びＳＳＤ１０５によって実行され、又はＣＰＵ１０１からの命令によって実現され、記憶部１０００に各種データを記憶したり、記憶部１０００に記憶された各種データを抽出したりする処理を行う。

【００３５】

＜認証サーバの機能構成＞

認証サーバ４０は、送受信部４１、ユーザ認証部４２、クライアント認証部４３、認可部４４、トークン発行部４５、及び記憶・読出部４９を有する。これら各部は、図３に示されている各構成要素のいずれかが、ＨＤ５０４からＲＡＭ５０３上に展開された認証サーバ４０用のプログラムに従ったＣＰＵ５０１からの命令によって動作することで実現される機能である。また、認証サーバ４０は、ＨＤ５０４により構築される記憶部４０００

を有している。

【００３６】

（ユーザ管理テーブル）

図６（Ａ）は、ユーザ管理テーブルを示す概念図である。記憶部４０００には、ユーザ管理テーブルによってユーザ管理ＤＢ４００１が構築される。ユーザ管理テーブルでは、ユーザＩＤ（identifier, identification）毎に、ユーザ名、及びパスワードが関連付けられて管理されている。

【００３７】

（クライアント管理テーブル）

図６（Ｂ）は、クライアント管理テーブルを示す概念図である。記憶部４０００には、クライアント管理テーブルによってクライアント管理ＤＢ４００２が構築される。クライアント管理テーブルでは、クライアントＩＤ毎に、クライアント名、及びパスワードが関連付けられて管理されている。

なお、監視カメラアプリは、端末１０が、管理システム５０に対して撮像画像の画像データをメッセージとしてpubすることを要求するためのクライアントアプリである。監視センターアプリは、管理システム５０に対して撮像画像の画像データをメッセージとしてsubすることを要求するためのクライアントアプリである。なお、監視センターアプリは、管理システム５０に対してsub要求するクライアントアプリであるが、監視カメラアプリから撮像画像の管理要求を受けるサーバアプリでもある。

【００３８】

（サービス管理テーブル）

図６（Ｃ）は、サービス管理テーブルを示す概念図である。記憶部４０００には、サービス管理テーブルによってサービス管理ＤＢ４００３が構築される。サービス管理テーブルでは、サービスＩＤ毎に、サービス名が関連付けられて管理されている。一実施形態において、サービスＩＤ「Ｓ０１」で識別されるサービス「伝送管理システム」は、管理システム５０である。なお、管理システム５０のPubSubの機能を利用する権利がリソースである。また、管理システム５０を使ったPubSubサービスは、OAuth 2.0のプロトコルにおいて認可の単位となるスコープである。また、管理システム５０はリソースサーバに相当する。

【００３９】

（サービス認可管理テーブル）

図６（Ｄ）は、サービス認可管理テーブルを示す概念図である。記憶部４０００には、サービス認可管理テーブルによってサービス認可管理ＤＢ４００４が構築される。サービス認可管理テーブルでは、クライアントＩＤ毎に、サービスＩＤが関連付けられて管理されている。これにより、サービス認可管理テーブルは、どのクライアントがどのサービスにアクセスして利用することができるかを管理することができる。図６（Ｄ）のサービス認可管理テーブルによれば、クライアントＩＤ「Ｃ０１」で識別されるchatアプリは、サービスＩＤ「Ｓ０１」で識別される伝送管理システム、すなわち、管理システム５０にアクセスして利用することができることを示す。

【００４０】

（認証サーバの各機能構成）

送受信部４１は、ＣＰＵ５０１からの命令、及びネットワークＩ／Ｆ５０９によって実現され、通信ネットワーク２を介して、相手側の端末、各装置又はシステム等と各種データ（または情報）の送受信を行う。

【００４１】

ユーザ認証部４２は、ＣＰＵ５０１からの命令によって実現され、クライアントからの要求に応じてユーザ認証を行う。

【００４２】

クライアント認証部４３は、ＣＰＵ５０１からの命令によって実現され、クライアントからの要求に応じてクライアント認証を行う。

【００４３】
認可部４４は、ＣＰＵ５０１からの命令によって実現され、サービスへのクライアントのアクセス権を指定することで認可する。
【００４４】
トークン発行部４５は、ＣＰＵ５０１からの命令によって実現され、クライアントがサービスへアクセスするときに、サービスで用いられる認可トークンを発行する。
【００４５】
記憶・読出部４９は、ＣＰＵ５０１からの命令及びＨＤＤ５０５によって実行され、又はＣＰＵ５０１からの命令によって実現され、記憶部４０００に各種データを記憶したり、記憶部４０００に記憶された各種データを抽出したりする処理を行う。
【００４６】
＜管理システムの機能構成＞
管理システム５０は、送受信部５１、トークン確認部５２、pub処理部５３、sub処理部５４、及び記憶・読出部５９を有している。これら各部は、図３に示されている各構成要素のいずれかが、ＨＤ５０４からＲＡＭ５０３上に展開された管理システム５０用のプログラムに従ったＣＰＵ５０１からの命令によって動作することで実現される機能である。また、管理システム５０は、ＨＤ５０４により構築される記憶部５０００を有している。
【００４７】
（トピック管理テーブル）
図７（Ａ）は、トピック管理テーブルを示す概念図である。記憶部５０００には、トピック管理テーブルによってトピック管理ＤＢ５００１が構築される。トピック管理テーブルでは、トピックＩＤ毎に、トピック名が関連付けられて管理されている。トピックとはメッセージに関連付けられる属性である。クライアントアプリがトピックを指定してsub要求すると、管理システム５０は、そのトピックに関連付けてpubされたメッセージを、要求元のクライアントアプリへ送信する。
【００４８】
（クライアント認可管理テーブル）
図７（Ｂ）は、クライアント認可管理テーブルを示す概念図である。記憶部５０００には、クライアント認可管理テーブルによってクライアント認可管理ＤＢ５００２が構築される。クライアント認可管理テーブルでは、トピックＩＤ毎に、クライアント名、及びpub又はsubする権限を有するか否かを示す権限情報が関連付けられて管理されている。
【００４９】
（ユーザ認可管理テーブル）
図７（Ｃ）は、ユーザ認可管理テーブルを示す概念図である。記憶部５０００には、ユーザ認可管理テーブルによってユーザ認可管理ＤＢ５００３が構築される。ユーザ認可管理テーブルでは、トピックＩＤ毎に、アカウント名、クライアント名、及びpub又はsubする権限を有するか否かを示す権限情報が関連付けられて管理されている。本実施形態において、アカウント名は、認可の単位になる情報であって、ユーザ名、若しくはユーザ名に端末名を付加した形式で表される。本実施形態において、ユーザ名は、IETF(Internet Engineering Task Force)のRFC(Request for Comments)で標準化されたメールアドレス形式で表される。また、アカウント名はユーザ名に対して、端末名を付加した形式で表される。
【００５０】
（セッション管理テーブル）
図７（Ｄ）は、セッション管理テーブルを示す概念図である。記憶部５０００には、セッション管理テーブルによってセッション管理ＤＢ５００４が構築される。セッション管理テーブルでは、トピックＩＤ、アカウント名、及びクライアント名が関連付けられて管理されている。セッション管理テーブルは、現在、セッションを実行中のアカウントが、どのトピックのメッセージをsubしているかを示す。これにより、管理システム５０は、トピックに対するメッセージのpub要求を受信したときに、どのアカウントにメッセージ

を送信すれば良いかを判断することができる。
【００５１】
（管理システムの各機能構成）
次に、管理システム５０の各機能構成について詳細に説明する。なお、以下では、管理システム５０の各機能構成を説明するにあたって、図３に示されている各構成要素のうち、管理システム５０の各機能構成を実現させるための主な構成要素との関係も説明する。
【００５２】
送受信部５１は、ＣＰＵ５０１からの命令、及びネットワークＩ／Ｆ５０９によって実現され、通信ネットワーク２を介して各端末、装置又はシステムと各種データ（または情報）の送受信を行う。
【００５３】
トークン確認部５２は、ＣＰＵ５０１からの命令によって実現され、端末１０のログイン要求に含まれている認可トークンを確認する。
【００５４】
pub処理部５３は、ＣＰＵ５０１からの命令によって実現され、クライアントによるpub要求を受け付ける。
【００５５】
sub処理部５４は、ＣＰＵ５０１からの命令によって実現され、クライアントによるsub要求を受け付ける。
【００５６】
記憶・読出部５９は、ＣＰＵ５０１からの命令及びＨＤＤ５０５によって実行され、又はＣＰＵ５０１からの命令によって実現され、記憶部５０００に各種データを記憶したり、記憶部５０００に記憶された各種データを抽出したりする処理を行う。
【００５７】
＜＜処理または動作＞＞
続いて、通信システム１を構成する端末１０、認証サーバ４０、及び管理システム５０の処理または動作について説明する。まずは、図８を用いて、一実施形態における認証処理について説明する。図８は、一実施形態における認証処理を示すシーケンス図である。
【００５８】
なお、以下の処理では、端末１０のユーザ認証に加えてクライアント認証が実行される処理の一例を示している。しかしながら、少なくともユーザ認証が実行されるものであれば、本発明は、以下の実施形態に限定されない。
【００５９】
端末１０にインストールされている任意のクライアントアプリが起動すると（ステップＳ２１）、起動したクライアントアプリにより、以下の各処理が実行される。端末１０のクライアントアプリは、ユーザのユーザＩＤ、ユーザ名、及びユーザパスワードを取得する（ステップＳ２２）。取得方法は、特に限定されないが、操作入力受付部１２が、ユーザによるユーザＩＤ及びユーザパスワードの入力を受け付ける方法や、記憶・読出部１９が、記憶部１０００に記憶されているユーザＩＤ、ユーザ名、及びユーザパスワードを読み出す方法等が挙げられる。
【００６０】
端末１０の認証要求部１４は、送受信部１１から認証サーバ４０へ、認証／認可要求を送信させる（ステップＳ２３）。認証／認可要求は、ユーザ認証要求、クライアント認証要求、及びサービス利用認可要求を含む。
【００６１】
ユーザ認証要求は、ステップＳ２２で取得されるユーザＩＤ、ユーザ名、及びユーザパスワードを含む。上記のとおり、ユーザ名は、IETFのRFCで標準化されたメールアドレス形式で表される。以下、端末１０ａ，１０ｂ，１０ｃの共通のユーザをユーザａ、ユーザａのユーザ名を、"a@example.com"と表す。
【００６２】

クライアント認証要求は、起動したクライアントのクライアントＩＤ及びクライアントパスワードを含む。クライアントＩＤ及びクライアントパスワードは、記憶部１０００に予め記憶されている。送受信部１１は、記憶部１０００に記憶されているクライアントＩＤ及びクライアントパスワードを読み出して、送信用のクライアント認証要求に含める。

【００６３】

サービス利用認可要求は、これから利用するサービスを示すスコープとしてサービスＩＤを含む。以下、サービス利用認可要求に含まれるサービスＩＤは、管理システム５０を示す「Ｓ０１」であるものとする。

【００６４】

認証サーバ４０の送受信部４１は、端末１０によって送信された、ユーザ認証要求、クライアント認証要求、及びサービス利用認可要求を含む認証／認可要求を受信する。認証／認可要求の受信に応じて、ユーザ認証部４２は、ユーザ認証を行う。この場合、ユーザ認証部４２は、ユーザ認証要求に含まれるユーザＩＤ、ユーザ名、及びユーザパスワードの組が、ユーザ管理テーブル（図６（Ａ）参照）において管理されているか判断する。

【００６５】

ユーザＩＤ、ユーザ名、及びユーザパスワードの組がユーザ管理テーブルで管理されている場合には、ユーザ認証部４２はユーザ認証に成功する。例えば、ユーザ認証要求に含まれるユーザ名が"a@example.com"であり、ユーザＩＤが"U01"であり、ユーザパスワードが"abc"である場合には、これらの組がユーザ管理テーブルにおいて管理されているのでユーザ認証に成功する。ユーザＩＤ、ユーザ名、及びユーザパスワードの組がユーザ管理テーブルにおいて管理されていない場合には、ユーザ認証部４２はユーザ認証に失敗する。

【００６６】

ユーザ認証に成功した場合、認証サーバ４０のクライアント認証部４３は、クライアント認証要求に含まれるクライアントＩＤ及びクライアントパスワードの組が、クライアント管理テーブル（図６（Ｂ）参照）で管理されているか判断する。クライアント認証要求に含まれるクライアントＩＤ及びクライアントパスワードの組がクライアント管理テーブルで管理されている場合には、クライアント認証部４３はクライアント認証に成功する（ステップＳ２５）。クライアント認証要求に含まれるクライアントＩＤ及びクライアントパスワードの組がクライアント管理テーブルにおいて管理されていない場合には、クライアント認証部４３はクライアント認証に失敗する。

【００６７】

クライアント認証に成功すると、認証サーバ４０の認可部４４は、クライアント認証要求に含まれるクライアントＩＤ、及びサービス利用認可要求に含まれるサービスＩＤの組が、サービス認可管理テーブル（図６（Ｄ）参照）で管理されているか判断する。クライアントＩＤ及びサービスＩＤの組がサービス認可管理テーブルで管理されている場合には、認可部４４はサービス利用認可に成功する（ステップＳ２６）。クライアントＩＤ及びサービスＩＤの組がサービス認可管理テーブルで管理されていない場合には、認可部４４はサービス利用認可に失敗する。

【００６８】

ユーザ認証、クライアント認証、及びサービス利用認可の少なくとも一つに失敗した場合、送受信部４１は、認証又は認可に失敗した旨を示すエラーメッセージを要求元の端末１０へ送信する。

【００６９】

ユーザ認証、クライアント認証、及びサービス利用認可のすべてに成功した場合、認証サーバ４０のトークン発行部４５は、認証要求元の端末１０による管理システム５０へのアクセスが認可されたことを示す認可トークンを発行する。このとき、トークン発行部４５は、認可トークンに、ユーザ認証要求に含まれるユーザ名、クライアント認証要求に含まれるクライアントＩＤに対応するクライアント名、サービス利用認可要求に含まれるサービスＩＤに対応するサービス名、及び認可トークンの有効期限を含める。

【００７０】
なお、通信システム１において、認証及び認可は、OAuth 2.0及びOpenID Connect等のプロトコルを用いて実行することもできる。この場合、ユーザＩＤ／ユーザパスワードなどの認証情報の授受の方法、認可トークンに含まれる内容は、OAuth 2.0及びOpenID Connect等の仕様によって規定されることになる。その場合、トークン自体はJWT(JSON Web Token)であっても良い。また、認可トークンがその経路上で改竄されないことを保証するため、トークン発行部４５は、認可トークンに対して秘密鍵を用いて署名しても良い。秘密鍵は、ＲＳＡ（Rivest, Shamir, Adleman）暗号を用いたものでも良い。なお、署名に、ＨＭＡＣ(Hash-based Message Authentication Code)のような公開鍵を用いても良い。認可トークンを利用する管理システム５０では、認可トークンが秘密鍵で署名されているか共有鍵で署名されているかに応じて、公開鍵または共有鍵を用いて署名の確認をする。署名は例えばJWS(JSON Web Signature)といった公知の標準を用いることもできる。認可トークンは必要に応じて、例えば、JWE(JSON Web Encryption)で暗号化される。

【００７１】
送受信部４１は、発行された認可トークン、及び認証及び認可に成功した旨の結果情報を端末１０へ送信する（ステップＳ２７）。端末１０の送受信部１１は、認証サーバによって送信された認可トークン、及び結果情報を受信する。続いて、端末１０の送受信部１１は受信した認可トークンと、アカウント名と、を含むログイン要求を管理システム５０へ送信する（ステップＳ２８）。

【００７２】
本実施形態において、アカウント名は、ステップＳ２２で取得されるユーザ名に、端末１０の端末名が付加された形式で表される。以下、端末１０のうち端末１０ａの端末名は、"camera1"、端末１０ｂの端末名は、"camera2"、端末１０ｃの端末名は、"operator"であるものとする。なお、端末名は、端末１０の記憶部１０００に記憶されたものであっても、操作入力受付部１２で受け付けられたものであっても良い。

【００７３】
ユーザ名と端末名との間は、予め定められた区切り文字で区切られている。区切り文字は、事前の取り決めによってユーザ名と端末名を一意に分割できる文字とする。たとえば、ユーザ名がemailアドレスの形式であれば、@以降のドメイン部分には+は使えないので+を区切り文字として使用する。端末１０の送受信部１１は、ステップＳ２２で取得されるユーザ名に、区切り文字、及び端末名を付加することでアカウント名を生成する。例えば、ユーザａが端末１０ａを用いてログイン要求するときに生成されるアカウント名は、"a@example.com+camera1"である。

【００７４】
管理システム５０の送受信部５１は、端末１０によって送信されたログイン要求を受信する。管理システム５０のトークン確認部５２は、ログイン要求に含まれる認可トークンを確認する（ステップＳ２９）。この処理で、トークン確認部５２は、認可トークンが有効であるか検証する。認可トークンの検証方法は、例えば、共有鍵、及び公開鍵による署名検証であり、認証サーバ４０の提供するトークン検証ＡＰＩ(Application Programming Interface)におけるトークンの形式や署名の方式に応じて適宜選択される。本実施形態の認可トークンには、有効期限が含まれているので、トークン確認部５２は、有効期限により認可トークンが有効であるか検証しても良い。また、本実施形態の認可トークンには、サービスＩＤが含まれているので、トークン確認部５２は、サービスＩＤによって示されるサービスが、自管理システムを示すものであるか確認することで、認可トークンが有効であるか検証しても良い。

【００７５】
検証の結果、認可トークンが有効ではない場合、トークン確認部５２は、ログイン要求元による自管理システムへのログインを拒否する。
認可トークンが有効である場合、トークン確認部５２は、ログイン要求元のログイン要求を許可するか判断する。図９を用いて、ログイン要求を許可するか判断する処理を詳細

に説明する。図９は、ログイン要求を許可するか判断する処理を示すフロー図である。

【００７６】

トークン確認部５２は、ステップＳ２８で受信されたログイン要求に含まれるアカウント名からユーザ名を抽出する（ステップＳ２９－１）。例えば、トークン確認部５２は、ログイン要求に含まれるアカウント名"a@example.com+camera1"から、区切り文字"+"より前の部分をユーザ名"a@example.com"として抽出する。なお、アカウント名からユーザ名を抽出する方法は上記に限定されず、端末１０によるアカウント名の生成ルールに従うものであれば良い。例えば、先頭の３文字にユーザ名を含めるルールでアカウント名が生成される場合、ユーザ認証部４２は、アカウント名から先頭の３文字をユーザ名として抽出する。或いは、ユーザ名を大文字、端末名を小文字とするルールでアカウント名が生成される場合、ユーザ認証部４２は、アカウント名から大文字の部分をユーザ名として抽出する。

【００７７】

ログイン要求に含まれるアカウント名からユーザ名が抽出されると、トークン確認部５２は、認可トークンに含まれるユーザ名と、ログイン要求に含まれるアカウント名から抽出されるユーザ名と、が一致するか判断する（ステップＳ２９－２）。

【００７８】

判断の結果、ユーザ名が一致しない場合（ステップＳ２９－２のＮＯ）、トークン確認部５２は、ログイン要求元の認証に失敗し、ログイン要求元による自管理システムへのログインを拒否する（ステップＳ２９－４）。

ユーザ名が一致する場合（ステップＳ２９－２のＹＥＳ）、トークン確認部５２は、ログイン要求元の認証に成功し、ログイン要求元による自管理システムへのログインを許可する。これにより、管理システム５０の送受信部５１は、端末１０へ、ログインに成功した旨の結果情報をログイン要求元の端末へ送信する（ステップＳ３０）。そして、管理システム５０は、端末１０との間の通信セッションを確立する。

【００７９】

セッションが確立すると管理システム５０では、ログイン要求に含まれているアカウント名、認可トークンに含まれているクライアント名、及びログイン要求元の端末１０のＩＰアドレス等を関連付けて記憶部５０００において管理する。これにより、ログインした端末１０が管理システム５０へ情報を送信するたびに、アカウント名、及びクライアント名を通知しなくても、管理システム５０では、送信元のアカウント名、及びクライアント名を把握できる。

【００８０】

同じユーザａが異なる端末１０を利用する場合、上記のステップＳ２１乃至Ｓ３０の処理は、端末１０ごとに実行される。例えば、ユーザａが利用する端末１０ａ，１０ｂの監視カメラアプリは、それぞれ、アカウント名"a@example.com+camera1, a@example.com+camera2"を管理システム５０へ送信してログイン要求する。また、ユーザａが利用する端末１０ｃの監視センターアプリは、アカウント名"a@example.com+operator"を管理システム５０へ送信してログイン要求する。この場合でも、認証サーバは、一つのユーザ名"a@example.com"を認証名として認証することができる。

【００８１】

続いて、図１０を用いて端末１０間でメッセージを送信する処理について説明する。図１０は、端末１０ａ，１０ｃ間でメッセージを送信する処理の一例を示すシーケンス図である。端末１０ａは通信機能を有するカメラであり、店舗に配置されている。端末１０ｃは、通信機能を有するPCであり、事務所に配置されている。端末１０ａ，１０ｃは同一の認証対象であるユーザａにより利用される。すなわち、上記のステップＳ２１乃至Ｓ３０の処理で、端末１０ａの監視カメラアプリ及び端末１０ｃの監視センターアプリは、管理システム５０へ、それぞれアカウント名"a@example.com+camera1, a@example.com+operator"を送信することで、それぞれ認証、及び認可される。

【００８２】

端末１０ｃのsub要求部１６は、監視カメラアプリが撮像した画像を受信するため、sub要求を管理システム５０へ送信する（ステップＳ４１）。sub要求には、監視カメラアプリが撮像する画像を示すトピック名"surveillance/shop_a"が含まれている。

【００８３】

管理システム５０の送受信部５１は、端末１０ｃによって送信されたsub要求を受信する。管理システム５０のsub処理部５４は、sub要求元のアカウントが、sub要求に係るトピック名"surveillance/shop_a"のトピックに対しsubする権限を有するかを判断する（ステップＳ４２）。ステップＳ４２の処理について、図１１を用いて詳細に説明する。図１１は、メッセージをsubする権限を有するかを判断する処理の一例を示したフロー図である。

【００８４】

まず、sub処理部５４は、sub要求に含まれるトピック名"surveillance/shop_a"が、トピック管理テーブル（図７（Ａ）参照）において管理されているかを判断する（ステップＳ４２－１）。sub要求に含まれるトピック名がトピック管理テーブルにおいて管理されていないと判断された場合（ステップＳ４２－１のＮＯ）、sub処理部５４は、sub要求元が、sub要求に係るトピックに対して、subする権限を有さない旨、判断する（ステップＳ４２－６）。

【００８５】

sub要求に含まれるトピック名がトピック管理テーブルにおいて管理されていると判断された場合（ステップＳ４２－１のＹＥＳ）、sub処理部５４は、sub要求に含まれるトピック名"surveillance/shop_a"に対応するトピックＩＤ"T01"、sub要求元のクライアント名「監視センターアプリ」、及びsub権限有りを示す権限情報"sub"の組が、クライアント認可管理テーブルにおいて管理されているかを判断する（ステップＳ４２－２）。

【００８６】

sub要求に係るトピックのトピックＩＤ、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、クライアント認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４２－２のＹＥＳ）、sub処理部５４は、sub要求元が、sub要求に係るトピックをsubする権限を有する旨、判断する（ステップＳ４２－５）。ステップＳ４２－２では、特定のクライアントによる要求であればアカウントによらずsub可能なトピックに対して、subする権限があるか判断する。

【００８７】

ステップＳ４２－２においてＮＯと判断された場合、sub処理部５４は、sub要求に係るトピックのトピックＩＤ"T01"、sub要求元のアカウント名"a@example.com+operator"、sub要求元のクライアント名「監視センターアプリ」、及びsub権限有りを示す権限情報"sub"の組が、ユーザ認可管理テーブルにおいて管理されているかを判断する（ステップＳ４２－３）。

【００８８】

sub要求に含まれるトピックのトピックＩＤ、sub要求元のアカウント名、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４２－３のＹＥＳ）、sub処理部５４は、sub要求元が、sub要求に係るトピックに対して、subする権限を有する旨、判断する（ステップＳ４２－５）。

【００８９】

sub要求に係るトピックのトピックＩＤ、sub要求元のアカウント名、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていないと判断された場合（ステップＳ４２－３のＮＯ）、sub処理部５４は、sub要求に係るトピックのトピックＩＤ、sub要求元のユーザ名、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されているか判断する（ステップＳ４２－４）。なお、sub処理部５４は、sub要求元のアカウント名から、区切り文字"+"以前の部分をユーザ名として抽出して上記の処理を行う。

【００９０】
sub要求に係るトピックのトピックＩＤ、sub要求元のユーザ名、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていないと判断された場合（ステップＳ４２－４のＮＯ）、sub処理部５４は、sub要求元が、sub要求に係るトピックに対して、subする権限を有さない旨、判断する（ステップＳ４２－６）。
【００９１】
sub要求に係るトピックのトピックＩＤ、sub要求元のユーザ名、sub要求元のクライアント名、及びsub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４２－４のＹＥＳ）、sub処理部５４は、sub要求元が、sub要求に係るトピックをsubする権限を有する旨、判断する（ステップＳ４２－５）。ステップＳ４２－４の処理では、特定のユーザによる要求であればアカウントによらずsub可能なトピックに対して、subする権限を有するか判断する。
【００９２】
ステップＳ４２－５で、sub要求元がsub権限を有する旨、判断された場合、sub処理部５４は、sub要求元のアカウント名"a@example.com+operator"、クライアント名「監視センターアプリ」、及びsub要求に係るトピックのトピックＩＤ"T01"をセッション管理テーブルに関連付けて登録する（図７（Ｄ）参照）（ステップＳ４３）。
【００９３】
一方、端末１０ａのpub要求部１５は、端末１０ｃの監視センターアプリにメッセージを送信するため、pub要求を管理システム５０へ送信する（ステップＳ４４）。pub要求には、監視カメラアプリが撮像する画像を示すトピック名"surveillance/shop_a"、及びメッセージとして自端末で撮像された画像の画像データが含まれている。
【００９４】
管理システム５０の送受信部５１は、端末１０ａによって送信されたpub要求を受信する。管理システム５０のpub処理部５３は、pub要求元のアカウントが、pub要求に係るトピック名"surveillance/shop_a"のトピックに対しpubする権限を有するかを判断する（ステップＳ４５）。ステップＳ４５の処理について、図１２を用いて詳細に説明する。図１２は、メッセージをpubする権限を有するかを判断する処理の一例を示したフロー図である。
【００９５】
まず、pub処理部５３は、pub要求に含まれるトピック名"surveillance/shop_a"が、トピック管理テーブル（図７（Ａ）参照）において管理されているかを判断する（ステップＳ４５－１）。pub要求に含まれるトピック名がトピック管理テーブルにおいて管理されていないと判断された場合（ステップＳ４５－１のＮＯ）、pub処理部５３は、pub要求元が、pub要求に係るトピックに対して、pubする権限を有さない旨、判断する（ステップＳ４５－６）。
【００９６】
pub要求に係るトピック名がトピック管理テーブルにおいて管理されていると判断された場合（ステップＳ４５－１のＹＥＳ）、pub処理部５３は、pub要求に含まれるトピック名"surveillance/shop_a"に対応するトピックＩＤ"T01"、pub要求元のクライアント名「監視カメラアプリ」、及びpub権限有りを示す権限情報"pub"の組が、クライアント認可管理テーブルにおいて管理されているかを判断する（ステップＳ４５－２）。
【００９７】
pub要求に係るトピックのトピックＩＤ、pub要求元のクライアント名、及びpub権限有りを示す権限情報の組が、クライアント認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４５－２のＹＥＳ）、pub処理部５３は、pub要求元が、pub要求に係るトピックをpubする権限を有する旨、判断する（ステップＳ４５－５）。ステップＳ４５－２では、特定のクライアントによる要求であればアカウントによらずpub可能なトピックに対して、pubする権限があるか判断する。

【００９８】
ステップＳ４５－２においてＮＯと判断された場合、pub処理部５３は、pub要求に係るトピックのトピックＩＤ"T01"、pub要求元のアカウント名"a@example.com+camera1"、pub要求元のクライアント名「監視カメラアプリ」、及びpub権限有りを示す権限情報"pub"の組が、ユーザ認可管理テーブルにおいて管理されているかを判断する（ステップＳ４５－３）。
【００９９】
pub要求に係るトピックのトピックＩＤ、pub要求元のアカウント名、pub要求元のクライアント名、及びpub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４５－３のＹＥＳ）、pub処理部５３は、pub要求元が、pub要求に係るトピックに対して、pubする権限を有する旨、判断する（ステップＳ４５－５）。
【０１００】
pub要求に係るトピックのトピックＩＤ、pub要求元のアカウント名、pub要求元のクライアント名、及びpub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていないと判断された場合（ステップＳ４５－３のＮＯ）、pub処理部５３は、pub要求に係るトピックのトピックＩＤ"T01"、pub要求元のユーザ名"a@example.com"、pub要求元のクライアント名「監視カメラアプリ」、及びpub権限有りを示す権限情報"pub"の組が、ユーザ認可管理テーブルにおいて管理されているか判断する（ステップＳ４５－４）。なお、pub処理部５３は、pub要求元のアカウント名から、区切り文字"+"以前の部分をユーザ名として抽出して上記の処理を行う。
【０１０１】
pub要求に係るトピックのトピックＩＤ、pub要求元のユーザ名、pub要求元のクライアント名、及びpub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていないと判断された場合（ステップＳ４５－４のＮＯ）、pub処理部５３は、pub要求元が、pub要求に係るトピックに対して、pubする権限を有さない旨、判断する（ステップＳ４５－６）。
【０１０２】
pub要求に係るトピックのトピックＩＤ、pub要求元のユーザ名、pub要求元のクライアント名、及びpub権限有りを示す権限情報の組が、ユーザ認可管理テーブルにおいて管理されていると判断された場合（ステップＳ４５－４のＹＥＳ）、pub処理部５３は、pub要求元が、pub要求に係るトピックをpubする権限を有する旨、判断する（ステップＳ４５－５）。ステップＳ４５－４の判断により、特定のユーザによる要求であればアカウントによらずpub可能なトピックに対して、pubする権限の有無を判断する。
【０１０３】
ステップＳ４５－５で、pub要求元がpub権限を有する旨、判断された場合、pub処理部５３は、pub要求に係るトピック名"surveillance/shop_a"のトピックのトピックＩＤ"T01"を検索キーとして、セッション管理テーブルを検索し、対応するアカウント名"a@example.com+operator"及びクライアント名「監視センターアプリ」を取得する（ステップＳ４６）。これにより、pub処理部５３は、メッセージの送信先として、アカウント名"a@example.com+operator"で管理システム５０へログインした端末１０ｃの監視センターアプリを特定する。
【０１０４】
送受信部５１は、pub要求に含まれるメッセージとしての画像データ、及びpub要求元のアカウント名"a@example.com+camera1"を、上記で特定された端末１０ｃの監視センターアプリへ送信する。これにより、端末１０ｃの送受信部１１は、メッセージとしての画像データ、及びpub要求元のアカウント名を受信する。
【０１０５】
管理システム５０は、pub要求に係るメッセージを記憶部５０００において管理しても良い。これにより、pub要求時には管理システム５０と接続していないクライアントが、

後に管理システム５０と接続したときに、管理システム５０は、記憶部５０００において管理されているメッセージをクライアントに送信することもできる。

【０１０６】

＜＜実施形態の変形例Ａ＞＞

続いて、実施形態の変形例Ａについて、上記の実施例とは異なる点を説明する。

図１３は、端末１０ｃから端末１０ａへメッセージを送信する処理の一例を示すシーケンス図である。

【０１０７】

端末１０ａのsub要求部１６は、監視センターアプリによるコマンドを受信するため、sub要求を管理システム５０へ送信する（ステップＳ１４１）。sub要求には、アカウント名"a@example.com+camera1"のアカウント宛のメッセージを示すトピック名"message_to/a@example.com+camera1"が含まれている。

【０１０８】

管理システム５０の送受信部５１は、端末１０ａによって送信されたsub要求を受信する。管理システム５０のsub処理部５４は、sub要求元のアカウントが、sub要求に係るトピック名"message_to/a@example.com+camera1"のトピックに対しsubする権限を有するかを判断する（ステップＳ１４２）。

【０１０９】

ステップＳ１４２の処理は、sub要求に含まれるトピック名が"message_to/a@example.com+camera1"に、このトピック名に対応するトピックＩＤが"T02"に、sub要求元のクライアント名が「監視カメラアプリ」に、sub要求元のアカウント名が"a@example.com+camera1"に、変更される点を除き、ステップＳ４２と同様である。すなわち、ステップＳ１４２では、ステップＳ４２－３に対応する処理で、sub要求に含まれるトピックのトピックＩＤ"T02"、sub要求元のアカウント名"a@example.com+camera1"、sub要求元のクライアント名「監視カメラアプリ」、及びsub権限有りを示す権限情報"sub"の組が、ユーザ認可管理テーブルにおいて管理されていると判断される。そして、ステップＳ４２－５に対応する処理で、sub処理部５４は、sub要求元が、sub要求に係るトピックをsubする権限を有する旨、判断する。

【０１１０】

sub要求元がsub権限を有する旨、判断されると、sub処理部５４は、sub要求元のアカウント名"a@example.com+camera1"、クライアント名「監視カメラアプリ」、sub要求に係るトピックのトピックＩＤ"T02"をセッション管理テーブルに関連付けて登録する（図７（Ｄ）参照）（ステップＳ１４３）。

【０１１１】

一方、端末１０ｃのpub要求部１５は、ユーザａが利用中の端末１０ａの監視カメラアプリにメッセージとしてのコマンドを送信するため、pub要求を管理システム５０へ送信する（ステップＳ１４４）。pub要求には、アカウント名"a@example.com+camera1"のアカウント宛のメッセージを示すトピック名"message_to/a@example.com+camera1"、及びメッセージとしてカメラの向きを水平方向に時計回りで３０°回転させるためのコマンド"rotate(30,0,0)"が含まれている。なお、メッセージは上記のものに限定されず、例えば、ズームやフォーカスの変更、撮像を開始または終了するためのコマンドであっても良い。

【０１１２】

管理システム５０の送受信部５１は、端末１０ｃによって送信されたpub要求を受信する。管理システム５０のpub処理部５３は、pub要求元のアカウントが、pub要求に係るトピック名"message_to/a@example.com+camera1"のトピックに対して、pubする権限を有するかを判断する（ステップＳ１４５）。

【０１１３】

ステップＳ１４５の処理は、pub要求に含まれるトピック名が"message_to/a@example.com+camera1"に、このトピック名に対応するトピックＩＤが"T02"に、pub要求元のクライアント名「監視センターアプリ」に、pub要求元のアカウント名が"a@example.com+operat

or"に変更される点を除き、ステップＳ４５と同様である。すなわち、ステップＳ１４５では、ステップＳ４５－３に対応する処理で、pub要求に含まれるトピックのトピックＩＤ"T02"、pub要求元のアカウント名"a@example.com+operator"、pub要求元のクライアント名「監視センターアプリ」、及びpub権限有りを示す権限情報"pub"の組が、ユーザ認可管理テーブルにおいて管理されていると判断される。そして、ステップＳ４５－５に対応する処理で、pub処理部５３は、pub要求元が、pub要求に係るトピックに対して、pubする権限を有する旨、判断する。

【０１１４】

pub要求元がpub権限を有する旨、判断された場合、pub処理部５３は、pub要求に係るトピック名"message_to/a@example.com+camera1"のトピックのトピックＩＤ"T02"を検索キーとして、セッション管理テーブルを検索し、対応するアカウント名"a@example.com+camera1"及びクライアント名「監視カメラアプリ」を取得する。これにより、pub処理部５３は、メッセージの送信先として、アカウント名"a@example.com+camera1"で管理システム５０へログインした端末１０ａの監視カメラアプリを特定する（ステップＳ１４６）。

【０１１５】

送受信部５１は、pub要求に含まれるメッセージとしてのコマンド"rotate(30,0,0)"、及びpub要求元のアカウント名"a@example.com+operator"を、上記で特定された端末１０ａの監視カメラアプリへ送信する。端末１０ａの送受信部１１は、管理システム５０によって送信されるメッセージとしてのコマンド、及びpub要求元のアカウント名を受信する。これにより、端末１０ａは、受信したコマンドに従って、カメラ１１２を３０°回転させる。

【０１１６】

＜＜実施形態の変形例Ｂ＞＞

続いて、実施形態の変形例Ｂについて、上記の実施形態と異なる点を説明する。

図１４は、一実施形態における認証処理を示すシーケンス図である。管理システム５０の記憶・読出部５９は、現在、管理システム５０へログインしているアカウントのアカウント名を記憶部５０００へ記憶して管理する。

【０１１７】

管理システム５０において、ステップＳ２９の認証に成功すると、トークン確認部５２は、ログイン要求元のユーザ名を検索キーとして、記憶部５０００を検索し、ログイン要求元のユーザ名と同じユーザ名を含むアカウント名の数をカウントする（ステップＳＢ１）。例えば、ログイン要求元のユーザ名が"a@example.com"である場合、トークン確認部５２は、検索結果から"a@example.com"を含むアカウント名の数をカウントする。

【０１１８】

トークン確認部５２は、ログイン要求元のユーザ名と同じユーザ名を含むアカウント名の数が、所定の数（例えば、１００）内であるか判断する（ステップＳＢ１）。ログイン要求元のユーザ名と同じユーザ名を含むアカウント名の数が、所定の数を超える場合（ステップＳＢ１のＮＯ）、送受信部５１は、ログインに失敗した旨を示す結果情報をログイン要求元に送信する（ステップＳＢ２）。これにより、管理システム５０のトークン確認部５２は、同じユーザによるログインの回数が所定の数を超える場合に、ログイン要求元のログインを制限する。

【０１１９】

ログイン要求元のユーザ名と同じユーザ名を含むアカウント名の数が所定の数内である場合（ステップＳＢ１のＹＥＳ）、トークン確認部５２は、ログイン要求元によるログインを制限しない。これにより、ログイン要求元の端末１０と管理システム５０との間のセッションが確立される。

【０１２０】

＜＜本実施形態の主な効果＞＞

続いて、上記の実施形態の主な効果を説明する。上記実施形態の認可方法によると、管理システム５０の送受信部５１(受信手段の一例）は、自管理システムの利用が認可され

たユーザのユーザ名（認可された対象の識別情報の一例）を含む認可トークン（認可情報の一例）、及び、ユーザ名（認証の対象の識別情報の）に端末名（通信端末の識別情報の一例）が付加されているアカウント名（付加情報の一例）を受信する。送受信部５１によるアカウント名の受信に応じて、管理システム５０のトークン確認部５２（認証手段の一例）は、認可トークンに含まれるユーザ名、及びアカウント名から抽出されるユーザ名が一致するかにより認証する。トークン確認部５２によって認証されると、sub処理部５４（認可手段の一例）は、上記のアカウント名に対応するアカウントに対して、端末１０間で送信されるメッセージ（情報の一例）のsub（受信の一例）を認可する。上記実施形態によると、同じユーザの異なる端末１０間の通信を行うときに、一つのユーザ名で認証できるので、認証用の情報の生成に伴う通信システム１の負荷を軽減できる。

【０１２１】

管理システム５０のトークン確認部５２（制限手段の一例）は、同じユーザ名を含む異なるアカウントによるログイン数（接続数の一例）が所定数に達すると、このユーザ名を含むアカウントがログイン要求（接続要求の一例）するときに、自管理システム５０へのログインを拒否することでログインを制限する。これにより、サービスの設定の自由度が向上する。

【０１２２】

管理システム５０の送受信部４１は、ユーザ名、端末名、及び、ユーザ名を抽出するための区切り文字（抽出情報の一例）を含むアカウント名を受信する。これにより、管理システム５０では、アカウント名からユーザ名を抽出できるようになる。

【０１２３】

認証サーバ４０（出力システムの一例）は、自管理システムの利用が認可されたユーザのユーザ名を含む認可トークンを発行する（出力の一例）する。これにより、管理システム５０のトークン確認部５２は、認証サーバ４０によって発行された認可トークンに含まれるユーザ名と、端末１０から送信されるアカウント名から抽出されるユーザ名が一致するかにより、認証することができる。

【０１２４】

端末１０は、入力されるユーザ名に、自端末の端末名を付したアカウント名を管理システム５０へ送信する。これにより、端末１０は、自端末の端末名を管理するだけで、ユーザごとのアカウント名を生成できるようになる。

【０１２５】

＜＜実施形態の補足＞＞

端末１０、認証サーバ４０、及び管理システム５０用の各プログラムは、インストール可能な形式又は実行可能な形式のファイルによって、コンピュータで読み取り可能な記録媒体（記録メディア１０６等）に記録されて流通されるようにしてもよい。また、上記記録媒体の他の例として、ＣＤ－Ｒ(Compact Disc Recordable)、ＤＶＤ(Digital Versatile Disk)、ブルーレイディスク等が挙げられる。

【０１２６】

また、上記実施形態の各プログラムが記憶されたＣＤ－ＲＯＭ等の記録媒体、並びに、これらプログラムが記憶されたＨＤ５０４は、プログラム製品(Program Product)として、国内又は国外へ提供されることができる。

【０１２７】

また、上記実施形態における端末１０、認証サーバ４０、及び管理システム５０は、単一のコンピュータによって構築されてもよいし、各部（機能又は手段）を分割して任意に割り当てられた複数のコンピュータによって構築されていてもよい。また、認証サーバ４０及び管理システム５０は、単一のコンピュータによって構築されていても良い。

【０１２８】

上記で説明した実施形態の各機能は、一又は複数の処理回路によって実現することが可能である。ここで、本明細書における「処理回路」とは、電子回路を含むプロセッサのようにソフトウェアによって各機能を実行するようプログラミングされたプロセッサや、上

記で説明した各機能を実行するよう設計されたASIC(Application Specific Integrated Circuit)や従来の回路モジュール等のデバイスを含むものとする。

【符号の説明】

【０１２９】

１　通信システム
２　通信ネットワーク
１０　端末
１１　送受信部
１２　操作入力受付部
１３　表示制御部
１４　認証要求部
１５　pub要求部
１６　sub要求部
１９　記憶・読出部
４０　認証サーバ
４１　送受信部
４２　ユーザ認証部
４３　クライアント認証部
４４　認可部
４５　トークン発行部
４９　記憶・読出部
５０　管理システム
５１　送受信部
５２　トークン確認部
５３　pub処理部
５４　sub処理部
５９　記憶・読出部
１０００　記憶部
４０００　記憶部
４００１　ユーザ管理ＤＢ
４００２　クライアント管理ＤＢ
４００３　サービス管理ＤＢ
４００４　サービス認可管理ＤＢ
５０００　記憶部
５００１　トピック管理ＤＢ
５００２　クライアント認可管理ＤＢ
５００３　ユーザ認可管理ＤＢ
５００４　セッション管理ＤＢ

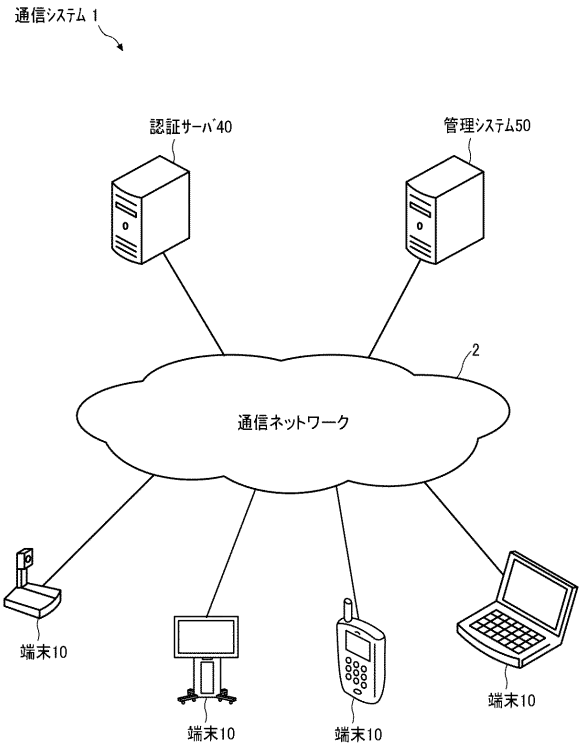
【先行技術文献】

【特許文献】

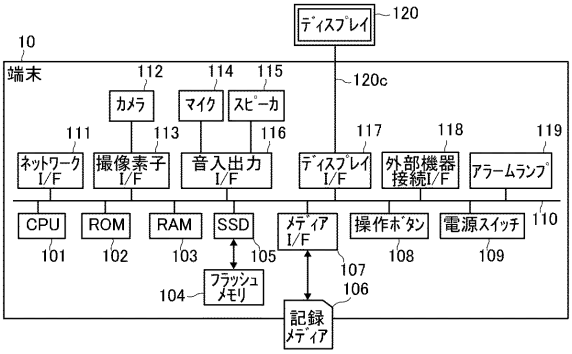
【０１３０】

【特許文献１】特開２００７－２３５６１８号公報

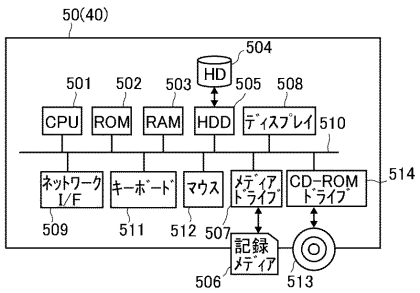
【図１】


通信ｼｽﾃﾑ 1
認証ｻｰﾊﾞ40
管理ｼｽﾃﾑ50
2
通信ネットワーク
端末10
端末10
端末10
端末10

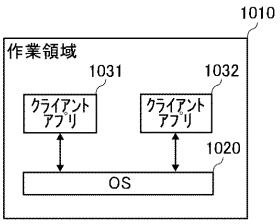
【図２】


ﾃﾞｨｽﾌﾟﾚｲ
120
10
端末
112
114
115
120c
カメラ
マイク
ｽﾋﾟｰｶ
111
113
116
117
118
119
ﾈｯﾄﾜｰｸ I/F
撮像素子 I/F
音入出力 I/F
ﾃﾞｨｽﾌﾟﾚｲ I/F
外部機器 接続I/F
ｱﾗｰﾑﾗﾝﾌﾟ
CPU
ROM
RAM
SSD
ﾒﾃﾞｨｱ I/F
操作ﾎﾞﾀﾝ
電源ｽｲｯﾁ
110
101
102
103
105
107
108
109
フラッシュ メモリ
104
106
記録 ﾒﾃﾞｨｱ

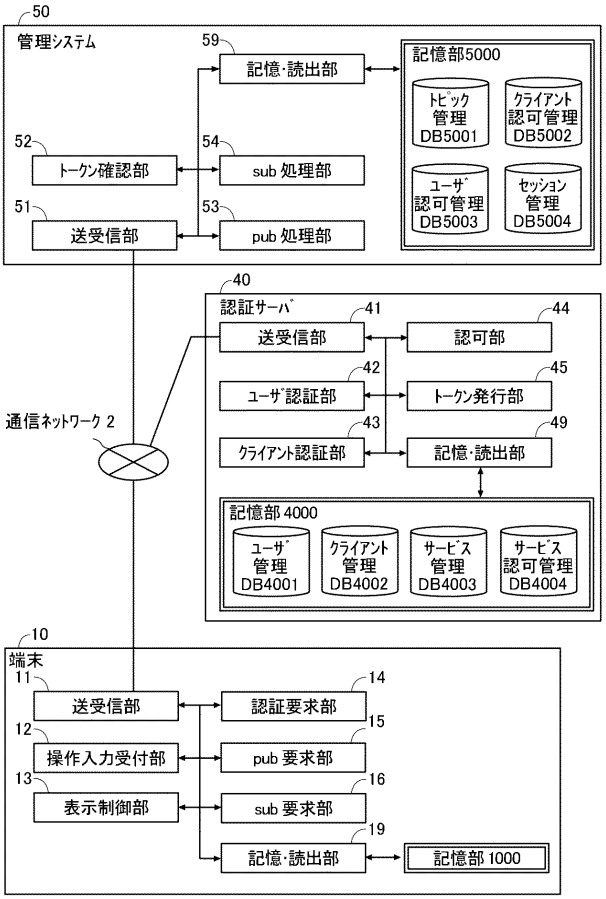
【図３】


50(40)
504
HD
501
502
503
505
508
CPU
ROM
RAM
HDD
ﾃﾞｨｽﾌﾟﾚｲ
510
ﾈｯﾄﾜｰｸ I/F
ｷｰﾎﾞｰﾄﾞ
ﾏｳｽ
ﾒﾃﾞｨｱ ﾄﾞﾗｲﾌﾞ
CD-ROM ﾄﾞﾗｲﾌﾞ
514
509
511
512
507
記録 ﾒﾃﾞｨｱ
506
513

【図４】


1010
作業領域
1031
1032
ｸﾗｲｱﾝﾄ ｱﾌﾟﾘ
ｸﾗｲｱﾝﾄ ｱﾌﾟﾘ
1020
OS

【図５】



【図６】

(A) ユーザ管理テーブル

ユーザID	ユーザ名	ユーザパスワード
U01	a@example.com	abc
U02	x@example.com	def
…	…	…

(B) クライアント管理テーブル

クライアントID	クライアント名	クライアントパスワード
C01	監視カメラアプリ	dddd
C02	監視センターアプリ	eeee
…	…	…

(C) サービス管理テーブル

サービスID	サービス名
S01	伝送管理システム
…	…

(D) サービス認可管理テーブル

クライアントID	サービスID
C01	S01
C02	S01

【図７】

(A) トピック管理テーブル

トピックID	トピック名
T01	surveillance/shop_a
T02	message_to/a@example.com+camera1
T03	message_to/a@example.com+camera2
T04	log

(B) クライアント認可管理テーブル

トピックID	クライアント名	権限情報
T04	ログ管理	pub

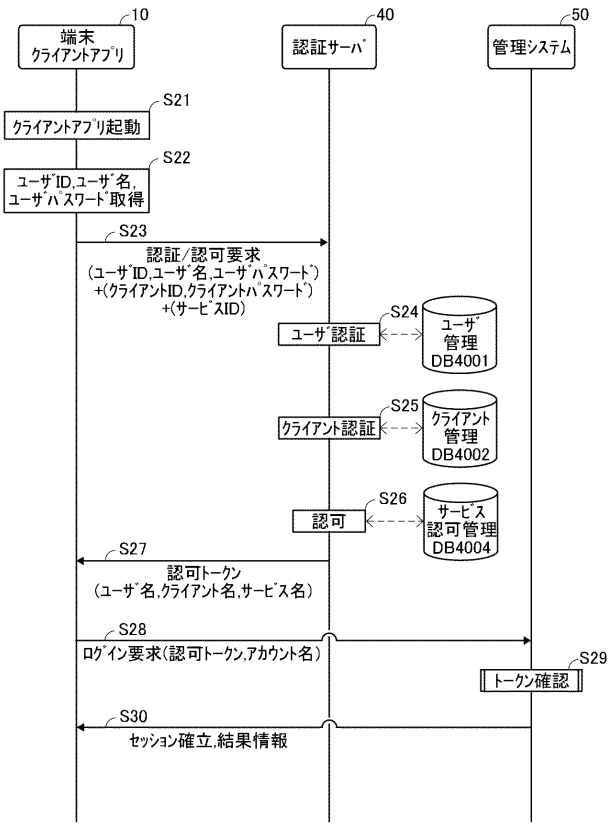
(C) ユーザ認可管理テーブル

トピックID	アカウント名	クライアント名	権限情報
T01	a@example.com	監視カメラアプリ	pub
T01	a@example.com+operator	監視センターアプリ	sub
T02,T03	a@example.com+operator	監視センターアプリ	pub
T02	a@example.com+camera1	監視カメラアプリ	sub
T03	a@example.com+camera2	監視カメラアプリ	sub
…	…	…	…

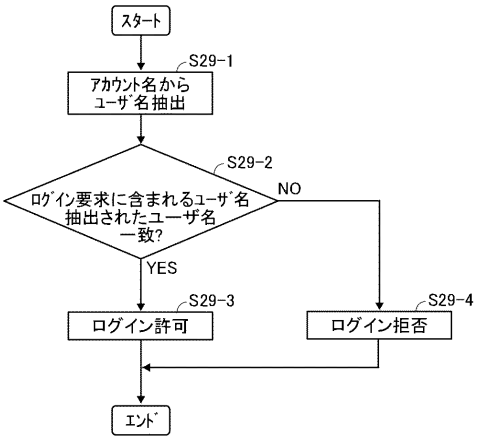
(D) セッション管理テーブル

トピックID	アカウント名	クライアント名
T01	a@example.com+operator	監視センターアプリ
T02	a@example.com+camera1	監視カメラアプリ
T03	a@example.com+camera2	監視カメラアプリ
…	…	…

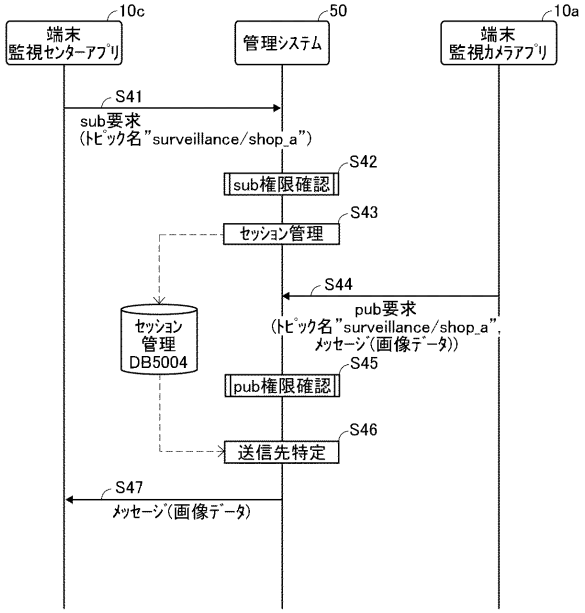
【図８】



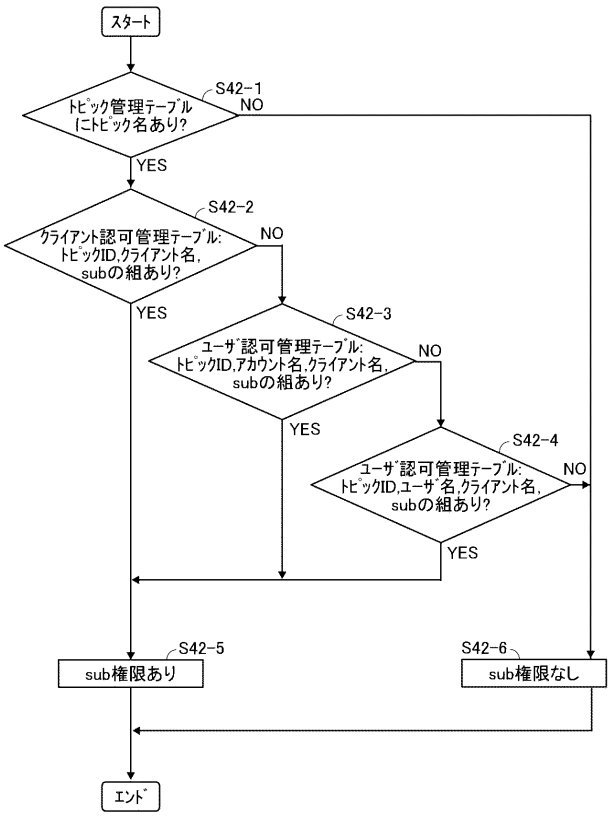
【図９】



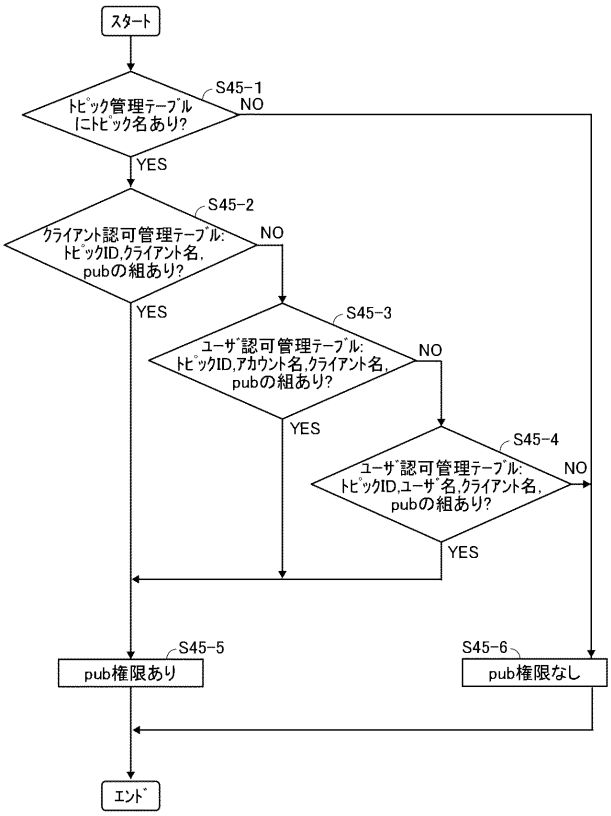
【図１０】



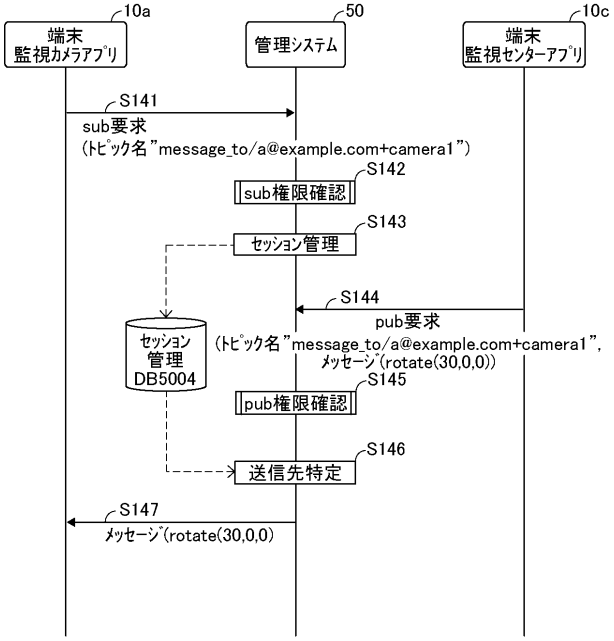
【図１１】



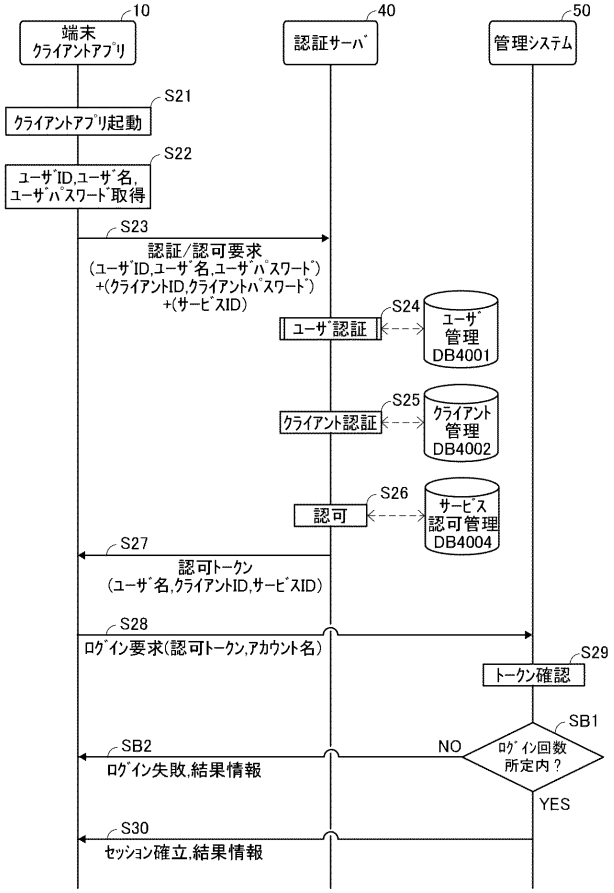
【図１２】



【図１３】


10a
端末
監視カメラアプリ
50
管理システム
10c
端末
監視センターアプリ
S141
sub要求
(トピック名"message_to/a@example.com+camera1")
S142
sub権限確認
S143
セッション管理
セッション
管理
DB5004
S144
pub要求
(トピック名"message_to/a@example.com+camera1",
メッセージ(rotate(30,0,0))
S145
pub権限確認
S146
送信先特定
S147
メッセージ(rotate(30,0,0)

【図１４】


10
端末
クライアントアプリ
40
認証サーバ
50
管理システム
S21
クライアントアプリ起動
S22
ユーザID,ユーザ名,
ユーザパスワード取得
S23
認証/認可要求
(ユーザID,ユーザ名,ユーザパスワード)
+(クライアントID,クライアントパスワード)
+(サービスID)
S24
ユーザ認証
ユーザ
管理
DB4001
S25
クライアント認証
クライアント
管理
DB4002
S26
認可
サービス
認可管理
DB4004
S27
認可トークン
(ユーザ名,クライアントID,サービスID)
S28
ログイン要求(認可トークン,アカウント名)
S29
トークン確認
SB1
ログイン回数
所定内？
NO
YES
SB2
ログイン失敗,結果情報
S30
セッション確立,結果情報

フロントページの続き

(72)発明者　曽根田　拓也
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考) 5B084 AA01 AA02 AA30 AB36 AB37 AB39 BB12 CB06 CB22 DC02
5K030 GA15 HB11 HD09 JA10 LB02 LD20