(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7159136号
(P7159136)

(45)発行日　令和4年10月24日(2022.10.24)

(24)登録日　令和4年10月14日(2022.10.14)

(51)国際特許分類		FI		
G06F 11/34 (2006.01)		G06F	11/34	176
G06F 11/30 (2006.01)		G06F	11/30	140A
G06F 21/33 (2013.01)		G06F	11/30	140G
G06F 21/10 (2013.01)		G06F	21/33	
		G06F	21/10	

請求項の数　12　（全28頁）

(21)出願番号　特願2019-173122(P2019-173122)
(22)出願日　令和1年9月24日(2019.9.24)
(65)公開番号　特開2021-51461(P2021-51461A)
(43)公開日　令和3年4月1日(2021.4.1)
審査請求日　令和3年11月11日(2021.11.11)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110002365
特許業務法人サンネクスト国際特許事務所
(72)発明者　市川 雄二郎
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　柿田 将幸
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
審査官　多賀 実

最終頁に続く

(54)【発明の名称】　システム実行支援方法および装置

(57)【特許請求の範囲】

【請求項１】

（Ａ）一または複数の開発者により開発された複数のサービスモジュールのうちの一つ以上のサービスモジュールにより構成されたサービスシステムにおける対象のサービスモジュールについて、認証および認可の少なくとも一つのためのデータである認証認可データを持つ要求を受け、

前記複数のサービスモジュールの各々は、当該サービスモジュールについての要求を実行した場合に当該要求の実行における使用量を含む実行内容と当該要求のメタ情報とを含んだログである実行ログを第１のログ情報に書き込むようになっており、

（Ｂ）前記受けた要求に対し当該要求の通過ＩＤを付与し、

（Ｃ）当該要求のメタ情報に当該要求の認証認可データに代えて当該付与した通過ＩＤを設定し、

（Ｄ）当該通過ＩＤを含んだメタ情報を持つ要求を、前記対象のサービスモジュールに転送し、

（Ｅ）当該通過ＩＤと前記認証認可データとを含んだログである通過ログを第２のログ情報に書き込む、

システム実行支援方法。

【請求項２】

前記サービスシステムについて、第１のゲートウェイにより、クライアントから、当該クライアントの認証認可データを持つ要求を受け、

前記第１のゲートウェイにより、当該要求に対し通過ＩＤを付与し、
前記第１のゲートウェイにより、当該要求のメタ情報に当該要求の認証認可データに代えて当該付与した通過ＩＤを設定し、
前記第１のゲートウェイにより、当該通過ＩＤを含んだメタ情報を持つ要求を転送し、
前記第１のゲートウェイにより、当該要求ＩＤと当該要求が持つ認証認可データとを含んだ通過ログを前記第２のログ情報に書き込み、
前記第１のゲートウェイにより転送された要求を、（Ａ）において、前記一つ以上のサービスモジュールについてそれぞれ用意された一つ以上の第２のゲートウェイのうちの前記対象のサービスモジュールの第２のゲートウェイにより受け、
（Ｂ）～（Ｅ）は、前記対象のサービスモジュールの第２のゲートウェイにより実行される、
請求項１に記載のシステム実行支援方法。
【請求項３】
前記通過ログは、当該通過ログに対応し要求を転送したゲートウェイより付与された通過ＩＤと、当該要求から抽出された認証認可データと、当該要求の転送元のゲートウェイにより付与された通過ＩＤである親通過ＩＤとを含む、
請求項２に記載のシステム実行支援方法。
【請求項４】
親通過ＩＤの無い認証認可データについて、
当該認証認可データに対応した通過ＩＤに関連付いている一つ以上の通過ＩＤの集合である通過ＩＤ集合を前記第２のログ情報から特定し、
当該通過ＩＤ集合を構成する通過ＩＤ毎に、当該通過ＩＤを含んだメタ情報に対応する実行内容を特定し、
当該通過ＩＤ集合について特定された実行内容に従う使用量を表す情報である利用情報を生成する、
請求項３に記載のシステム実行支援方法。
【請求項５】
親通過ＩＤの無い認証認可データについて、さらに、
前記生成した利用情報を基に、当該利用情報が表す使用量に応じた課金額を決定し、
前記決定した課金額を出力する、
請求項４に記載のシステム実行支援方法。
【請求項６】
親通過ＩＤの無い認証認可データについて、さらに、
当該認証認可データに対応した契約内容を特定し、
前記決定した課金額に前記特定した契約内容を関連付けて出力する、
請求項５に記載のシステム実行支援方法。
【請求項７】
前記サービスシステムを構成する一つ以上のサービスモジュールの各々を、複数種類の計算資源に基づく実行基盤サービスにデプロイし、
前記サービスシステムについて前記第１のゲートウェイを前記実行基盤サービスにデプロイし、前記一つ以上のサービスモジュールについてそれぞれ前記一つ以上の第２のゲートウェイを前記実行基盤サービスにデプロイする、
請求項２に記載のシステム実行支援方法。
【請求項８】
要求を受けた場合、当該要求が持つ認証認可データを、前記サービスシステムの外部に設けられ認証認可を行う機能である認証認可サービス群に送信することで、当該認証認可サービス群に認証認可を実行させる、
請求項１に記載のシステム実行支援方法。
【請求項９】
前記要求のメタ情報は、当該要求のヘッダが持つヘッダ情報である、

請求項１に記載のシステム実行支援方法。
【請求項１０】
前記認証認可データは、アクセストークンである、
請求項１に記載のシステム実行支援方法。
【請求項１１】
（Ａ）一または複数の開発者により開発された複数のサービスモジュールのうちの一つ以上のサービスモジュールにより構成されたサービスシステムにおける対象のサービスモジュールについて、認証および認可の少なくとも一つのためのデータである認証認可データを持つ要求を受け、
前記複数のサービスモジュールの各々は、当該サービスモジュールについての要求を実行した場合に当該要求の実行における使用量を含む実行内容と当該要求のメタ情報とを含んだログである実行ログを第１のログ情報に書き込むようになっており、
（Ｂ）前記受けた要求に対し当該要求の通過ＩＤを付与し、
（Ｃ）当該要求のメタ情報に当該要求の認証認可データに代えて当該付与した通過ＩＤを設定し、
（Ｄ）当該通過ＩＤを含んだメタ情報を持つ要求を、前記対象のサービスモジュールに転送し、
（Ｅ）当該通過ＩＤと前記認証認可データとを含んだログである通過ログを第２のログ情報に書き込む、
ことをコンピュータに実行させるコンピュータプログラム。
【請求項１２】
複数種類の計算資源に基づく実行基盤サービスにデプロイされたサービスシステムに対して一つ以上のゲートウェイをデプロイするゲートウェイ制御部と、
第１のログ情報と第２のログ情報とを管理するログ管理部と
を備え、
前記サービスシステムは、一または複数の開発者により開発された複数のサービスモジュールのうちの一つ以上のサービスモジュールにより構成され、
前記複数のサービスモジュールの各々は、当該サービスモジュールについての要求を実行した場合に当該要求の実行における使用量を含む実行内容と当該要求のメタ情報とを含んだログである実行ログを第１のログ情報に書き込むようになっており、
前記一つ以上のゲートウェイのうちのいずれかのゲートウェイが、
認証および認可の少なくとも一つのためのデータである認証認可データを持つ要求を受け、
前記受けた要求に対し当該要求の通過ＩＤを付与し、
当該要求のメタ情報に当該要求の認証認可データに代えて当該付与した通過ＩＤを設定し、
当該通過ＩＤを含んだメタ情報を持つ要求を、対象のサービスモジュールに転送し、
当該通過ＩＤと前記認証認可データとを含んだログである通過ログを第２のログ情報に書き込む、
システム実行支援装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、情報通信に関し、特に、一または複数の開発者により開発された複数のサービスモジュールのうちの一つ以上のサービスモジュールをマッシュアップさせたサービスシステムの実行支援に関する。
【背景技術】
【０００２】
近年、マーケットプレイスなどを通じて調達可能な機能部品といったサービスモジュール（例えば音声解析）を、バックエンドサービスとして活用したサービスシステム（例え

ば、文書解析と機械学習を連携および活用した自動応対サービス）の開発が浸透している。サービス提供者は、例えば音声解析のバックエンドサービスと機械学習のバックエンドサービスを調達し、それらを連携させるための制御ルールを準備し、自動応対サービスを開発する。サービスシステムのパッケージ化（例えば、テンプレート化）およびデプロイメント自動化を通じて迅速な展開（例えば、同一企業内の複数の部署への展開）を実現することができることが望ましい。

【０００３】

サービス提供者によっては、サービスシステムの価値（効果）に基づいたマネタイズを実現するために、機能部品毎の使用量（例えば、解析時間、機械学習のための入力データ量）に基づいた従量課金を行いたい者がいると考えられる。

【０００４】

特許文献１に開示の方法は、複数のユーザがストレージサービスに対しアクセス要求を出す状況下で、ストレージの状態情報とアクセスの履歴情報とを突き合わせて、実際にアクセスしたアカウントを特定し、当該アカウントの課金額などとして計上する方法である。

【先行技術文献】

【特許文献】

【０００５】

【文献】特開２０１６－９２２４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかし、マーケットプレイスなどを通じて提供される各サービスモジュール（機能部品）はマルチユーザを想定した機能（典型的には、認証認可（認証および認可のうちの少なくとも一つ）、および、ユーザ情報を含むログ出力、のうちの少なくとも一つ）を備えるとは限らない。その理由の一つとして、サービスモジュールの開発者は、通常、価値向上に繋がると利用者から評価される可能性の高い機能／非機能要件（例えば、多言語対応、応答時間短縮）に対して集中投資をし、マルチユーザを想定した機能（例えば、あるサービス提供者が定めたログ出力仕様への対応）に対する投資を回避する傾向にあると考えられる。

【０００７】

このため、マルチユーザを想定した機能を備えていないサービスモジュールを含んだサービスシステムについて従量課金を行うことが困難であるという技術的課題が存在する。

【０００８】

予めサービス要件（例えば、利用規模またはサービスレベル）が決まっていればそのサービス要件を満たすサービスシステムを構築して提供することが可能であると考えられる。しかし、予めサービス要件が確定しているとは限らない。この場合、サービスシステムを使用しながら課題や要件を定め、必要に応じてサービスシステムをスケールすることが好ましい。故に、この場合、いわゆるスモールスタートでサービスシステムを使用することが好ましく、そのためには、サービスシステムの従量課金の実現が望まれる。従量課金の実現は、ユーザ情報を含んだログ出力や認証認可といった機能（つまり、マルチユーザを想定した機能）を備えていないサービスモジュールを含んだサービスシステムをマルチユーザ仕様とすることの一例と考えることができる。

【課題を解決するための手段】

【０００９】

サービスシステムにおける各サービスモジュールは、当該サービスモジュールについての要求を実行した場合に当該要求の実行における使用量を含む実行内容と当該要求のメタ情報とを含んだログである実行ログを第１のログ情報に書き込むようになっている。対象のサービスモジュールについて、ゲートウェイが、認証および認可の少なくとも一つのためのデータである認証認可データを持つ要求を受けた場合、当該要求に対し当該要求の通過ＩＤを付与し、当該要求のメタ情報に当該要求の認証認可データに代えて当該付与した

通過ＩＤを設定する。ゲートウェイが、当該通過ＩＤを含んだメタ情報を持つ要求を、対象のサービスモジュールに転送し、当該通過ＩＤと上記認証認可データとを含んだログである通過ログを第２のログ情報に書き込む。

【発明の効果】

【００１０】

認証認可とユーザ情報を含んだログの出力といった機能を持たないサービスモジュールを含んだサービスシステムをマルチユーザ仕様にできる。

【図面の簡単な説明】

【００１１】

【図１】実施形態１に係るシステム全体の構成と当該システム全体における関係の一部とを示す図である。

【図２】実施形態１に係るシステム全体の構成と当該システム全体における関係の一部とを示す図である。

【図３】システム実行基盤サービスおよびログ管理部の構成の例を示す図である。

【図４】コーディネーションサービスの構成の例を示す図である。

【図５】実行ログテーブルおよび通過ログテーブルの構成の例と、要求の転送とログの出力との関係の例とを示す図である。

【図６】ゲートウェイ制御部が持つテーブルの構成の例を示す図である。

【図７】ロググルーピング部が持つテーブルの構成の例を示す図である。

【図８】認証認可ゲートウェイの動作の流れの例を示す図である。

【図９】ロググルーピング部の動作の流れの例を示す図である。

【図１０】ゲートウェイデプロイメント部の処理フローチャートの例を示す図である。

【図１１】転送設定部および認証認可ゲートウェイの処理フローチャートの例を示す図である。

【図１２】認可設定部および認証認可ゲートウェイの処理フローチャートの例を示す図である。

【図１３】ヘッダ設定部の処理フローチャートの例を示す図である。

【図１４】認証検知部の処理フローチャートの例を示す図である。

【図１５】ユーザアクセストークン特定の処理フローチャートの例を示す図である。

【図１６】ロググループ出力部の処理フローチャートの例を示す図である。

【図１７】実施形態２におけるコーディネーションサービスの構成の例を示す図である。

【図１８】実施形態２における課金用データ出力の処理フローチャートの例を示す図である。

【図１９】実施形態３におけるコーディネーションサービスの構成の例を示す図である。

【図２０】契約マッピングテーブルの構成の例を示す図である。

【図２１】実施形態３における課金用データ出力の処理フローチャートの例を示す図である。

【発明を実施するための形態】

【００１２】

以下の説明では、「インターフェース装置」は、一つ以上のインターフェースデバイスでよい。当該一つ以上のインターフェースデバイスは、下記のうちの少なくとも一つでよい。

・一つ以上のＩ／Ｏ（Input/Output）インターフェースデバイス。Ｉ／Ｏ（Input/Output）インターフェースデバイスは、Ｉ／Ｏデバイスと遠隔の表示用計算機とのうちの少なくとも一つに対するインターフェースデバイスである。表示用計算機に対するＩ／Ｏインターフェースデバイスは、通信インターフェースデバイスでよい。少なくとも一つのＩ／Ｏデバイスは、ユーザインターフェースデバイス、例えば、キーボードおよびポインティングデバイスのような入力デバイスと、表示デバイスのような出力デバイスとのうちのいずれでもよい。

・一つ以上の通信インターフェースデバイス。一つ以上の通信インターフェースデバイス

は、一つ以上の同種の通信インターフェースデバイス（例えば一つ以上のＮＩＣ（Network Interface Card））であってもよいし二つ以上の異種の通信インターフェースデバイス（例えばＮＩＣとＨＢＡ（Host Bus Adapter））であってもよい。

【００１３】

また、以下の説明では、「メモリ」は、一つ以上のメモリデバイスであり、典型的には主記憶デバイスでよい。メモリにおける少なくとも一つのメモリデバイスは、揮発性メモリデバイスであってもよいし不揮発性メモリデバイスであってもよい。

【００１４】

また、以下の説明では、「永続記憶装置」は、一つ以上の永続記憶デバイスである。永続記憶デバイスは、典型的には、不揮発性の記憶デバイス（例えば補助記憶デバイス）であり、具体的には、例えば、ＨＤＤ（Hard Disk Drive）またはＳＳＤ（Solid State Drive）である。

【００１５】

また、以下の説明では、「記憶装置」は、メモリと永続記憶装置の少なくともメモリでよい。

【００１６】

また、以下の説明では、「プロセッサ」は、一つ以上のプロセッサデバイスである。少なくとも一つのプロセッサデバイスは、典型的には、ＣＰＵ（Central Processing Unit）のようなマイクロプロセッサデバイスであるが、ＧＰＵ（Graphics Processing Unit）のような他種のプロセッサデバイスでもよい。少なくとも一つのプロセッサデバイスは、シングルコアでもよいしマルチコアでもよい。少なくとも一つのプロセッサデバイスは、プロセッサコアでもよい。少なくとも一つのプロセッサデバイスは、処理の一部または全部を行うハードウェア回路（例えばＦＰＧＡ（Field-Programmable Gate Array）またはＡＳＩＣ（Application Specific Integrated Circuit））といった広義のプロセッサデバイスでもよい。

【００１７】

また、以下の説明では、「ｘｘｘテーブル」といった表現にて、入力に対して出力が得られる情報を説明することがあるが、当該情報は、どのような構造のデータでもよいし、入力に対する出力を発生するニューラルネットワークのような学習モデルでもよい。従って、「ｘｘｘテーブル」を「ｘｘｘ情報」と言うことができる。また、以下の説明において、各テーブルの構成は一例であり、一つのテーブルは、二つ以上のテーブルに分割されてもよいし、二つ以上のテーブルの全部または一部が一つのテーブルであってもよい。

【００１８】

また、以下の説明では、「プログラム」を主語として処理を説明する場合があるが、プログラムは、プロセッサによって実行されることで、定められた処理を、適宜に記憶装置及び／又はインターフェース装置等を用いながら行うため、処理の主語が、プロセッサ（或いは、そのプロセッサを有するコントローラのようなデバイス）とされてもよい。プログラムは、プログラムソースから計算機のような装置にインストールされてもよい。プログラムソースは、例えば、プログラム配布サーバ又は計算機が読み取り可能な（例えば非一時的な）記録媒体であってもよい。また、以下の説明において、二つ以上のプログラムが一つのプログラムとして実現されてもよいし、一つのプログラムが二つ以上のプログラムとして実現されてもよい。

【００１９】

また、以下の説明では、「ｋｋｋ部」の表現にて機能を説明することがあるが、機能は、一つ以上のコンピュータプログラムがプロセッサによって実行されることで実現されてもよいし、一つ以上のハードウェア回路（例えばＦＰＧＡまたはＡＳＩＣ）によって実現されてもよい。プログラムがプロセッサによって実行されることで機能が実現される場合、定められた処理が、適宜に記憶装置および／またはインターフェース装置等を用いながら行われるため、機能はプロセッサの少なくとも一部とされてもよい。機能を主語として説明された処理は、プロセッサあるいはそのプロセッサを有する装置が行う処理としても

よい。プログラムは、プログラムソースからインストールされてもよい。プログラムソースは、例えば、プログラム配布計算機または計算機が読み取り可能な記録媒体（例えば非一時的な記録媒体）であってもよい。各機能の説明は一例であり、複数の機能が一つの機能にまとめられたり、一つの機能が複数の機能に分割されたりしてもよい。

【００２０】

また、以下の説明では、同種の要素を区別しないで説明する場合には、参照符号のうちの共通部分を使用し、同種の要素を区別する場合は、参照符号を使用することがある。例えば、認証認可ゲートウェイを区別しない場合には、「認証認可ゲートウェイ３１２」と言い、認証認可ゲートウェイを区別する場合には、「認証認可ゲートウェイ３１２Ａ」、「認証認可ゲートウェイ３１２Ｂ」のように言うことがある。

【００２１】

以下、本発明の実施の形態を添付図面に基づいて説明する。

［実施形態１］

【００２２】

図１および図２は、本発明の実施形態１に係るシステム全体の構成と当該システム全体における関係とを示す。

【００２３】

コーディネータ１１０と、システム実行基盤提供者（以下、提供者）１２０と、バックエンドサービス開発者（以下、開発者）１３０と、テナント１００とが存在する。テナント１００内にテナント管理者（以下、管理者）１０１およびシステム利用者（以下、利用者）１０２が存在する。

【００２４】

テナント１００は、企業または企業内の部門でよい。管理者１０１は、テナント用システム１０４を管理する一従業員でよい。利用者１０２は、テナント用システム１０４を利用する一従業員でよい。

【００２５】

コーディネータ１１０は、提供者１２０および開発者１３０とテナント１００と間をコーディネートする。例えば、コーディネータ１１０は、コーディネーションサービス１１３を操作して、一または複数の開発者１３０により開発された複数のサービスモジュールのうちの二つ以上のサービスモジュールを組み合わせたテナント用システム１０４（サービスシステムの一例）を設計し、テナント用システム１０４をテナント１００に提供する。また、コーディネータ１１０は、テナント用システム１０４の従量課金によりテナント１００から利用料を取得する。また、コーディネータ１１０は、テナント用システム１０４の実行に関し計算資源の使用量に応じた料金を提供者１２０に支払う。また、コーディネータ１１０は、当該テナント用システム１０４の構成要素である一つ以上のバックエンドサービスの各々について、当該バックエンドサービスの使用量に応じた料金を開発者１３０に支払う。

【００２６】

提供者１２０が提供するシステム実行基盤サービス１２２は、例えば、クラウドコンピューティングサービスでよい。コーディネーションサービス１１３およびシステム実行基盤サービス１２２の少なくとも一つは、複数の計算資源（例えば、インターフェース装置、記憶装置およびプロセッサ）を有する物理的な計算機システム（例えば、一つ以上の物理計算機）でもよいし、当該複数の計算資源上に構築された論理的な計算機システム（例えば、一つ以上の仮想計算機）でもよい。

【００２７】

矢印Ａ１３１によれば、一または複数の開発者１３０が、複数のバックエンドサービスのイメージをイメージリポジトリ１２４に登録する。

【００２８】

矢印Ａ１１２によれば、コーディネータ１１０は、テナント１００との契約に基づいて、テナント１００に対し、サービス一式の提供を行う。「サービス一式」とは、少なくと

もテナント１００用のシステム１０４を含む。
【００２９】
矢印Ａ１１７によれば、コーディネータ１１０は、前述のサービス一式を具現化するために、一または複数の開発者１３０からは一つ以上のバックエンドサービスを調達し（例えば、マーケットプレイス経由で調達し）、提供者１２０からはそれらのバックエンドサービスを稼動させるためのシステム実行基盤サービス１２２を調達する。調達されたバックエンドサービスをテナント用システム１０４が含み、テナント用システム１０４が、調査津されたシステム実行基盤サービス１２２のうちのシステム実行領域１２６で実行される。
【００３０】
矢印Ａ１１１によれば、コーディネータ１１０は、テナント用システム１０４をシステム実行領域１２６へ配備（デプロイメント）するための操作をコーディネーションサービス１１３に対して行う。
【００３１】
矢印Ａ１１８によれば、コーディネーションサービス１１３は、矢印Ａ１１１が示す操作に対しシステム実行基盤サービス１２２を制御する。
【００３２】
矢印Ａ１０５によれば、テナント用システム１０４は、ＣＰＵやメモリなどの計算資源を持つシステム実行領域１２６上で稼働する。
【００３３】
矢印Ａ１０３によれば、管理者１０１や利用者１０２はテナント用システム１０４が提供するインターフェース（例えば、ＧＵＩ（Graphical User Interface）、ＲＥＳＴ（Representational State Transfer）など）を通じてテナント用システム１０４を利用する。コーディネーションサービス１１３は、テンプレート部１１４と、デプロイメント要求部１１５と、ログ分類部１１７と、ログ管理部１１６とを含む。
【００３４】
矢印Ａ１２１によれば、提供者１２０は、システム実行基盤サービス１２２を所有および運営する。システム実行基盤サービス１２２は、システム実行領域１２６と、デプロイメント実行部１２３と、イメージリポジトリ１２４と、認証認可サービス群１２５とを含む。システム実行領域１２６は、複数の計算資源（例えば、インターフェース装置、記憶装置およびプロセッサ）に基づく論理的な領域であり、テナント用システム１０４が実行される領域である。
【００３５】
図２によれば、テナント用システム１０４（具体的には、当該システム１０４が実行されるシステム実行領域１２６）と、コーディネーションサービス１１３とは、ネットワーク２００にて接続されている。
【００３６】
矢印Ａ２０１によれば、デプロイメント要求部１１５は、デプロイメント実行部１２３に対し、テナント用システム１０４のデプロイメント要求を送信する。矢印Ａ２０２によれば、デプロイメント実行部１２３は、システム実行領域１２６へ、デプロイメント要求に従ってテナント用システム１０４のデプロイメントを実行する。矢印Ａ２０３によれば、テナント用システム１０４のデプロイメント実行の際に、テナント用システムを構成するバックエンドサービスのイメージ（例えば、コンテナイメージ）がイメージリポジトリ１２４からロードされ、起動される。矢印Ａ２０４によれば、デプロイメントされたテナント用システム１０４は、必要に応じて認証および認可を行うために認証認可サービス群１２５にアクセスする。
【００３７】
図３は、システム実行基盤サービス１２２およびログ管理部１１６の構成の例を示す図である。
【００３８】

ログ管理部１１６は、実行ログテーブル３００と、通過ログテーブル３０１とを格納する。実行ログテーブル３００は、矢印Ａ３４０が示すように、バックエンドサービス３１１（インスタンス）の実行ログが格納されるテーブルである。通過ログテーブル３０１は、矢印Ａ３４１が示すように、認証認可ゲートウェイ３１２（インスタンス）の通過ログが格納されるテーブルである。

【００３９】

テナントＡ用システム領域３１０は、テナントＡ１００Ａ用に、システム実行領域１２６が持つ計算資源や権限などが論理的に分割されたことにより得られた領域である。テナントＡ用システム領域３１０には、一つ以上のバックエンドサービス３１１のインスタンスと、バックエンドサービス制御プログラム３１３と、認証認可ゲートウェイ３１２のインスタンスとが展開される。

【００４０】

バックエンドサービス制御プログラム３１３は、利用者クライアント３５０およびバックエンドサービス３１１間の連携を行う。例えば、バックエンドサービス制御プログラム３１３は、事前に定義された制御ルール３１４（例えば、ロジック、処理フローまたはステップ）に従って、要求および応答データの相互通信を制御する。なお、利用者クライアント３５０は、利用者が使用する物理的または仮想的な情報処理端末でよい。

【００４１】

認証認可ゲートウェイ３１２は、矢印Ａ３４３が示すように、バックエンドサービス３１１およびバックエンドサービス制御プログラム３１３の代わりに認証認可サービス群１２５にアクセスする。

【００４２】

イメージリポジトリ１２４は、イメージの実態（例えばコンテナファイル）となるイメージファイル３２２と、イメージのメタ情報を管理するイメージ管理部３２３とを持つ。

【００４３】

デプロイメント実行部１２３は、デプロイ処理部３２０と、アンデプロイ処理３２１とを備える。デプロイ処理部３２０は、イメージファイル３２２を用いて、システム実行領域１２６に、テナント用システム１０４を構成する各バックエンドサービスなどのインスタンスを作成する。アンデプロイ処理３２１は、テナント用システム１０４の廃棄時に、システム実行領域１２６から、当該テナント用システム１０４のバックエンドサービスなどのインスタンスを削除する。

【００４４】

認証認可サービス群１２５は、認証部３６０と認可部３６１とを含む。認証部３６０は、要求（例えば、利用者クライアント３５０からバックエンドサービス３１１（または、当該サービス３１１を含むテナント用システム１０４）への要求）の認証を行う。認可部３６１は、要求の認可を行う。「認証認可」は、上述したように、認証および認可のうちの少なくとも一つを意味するが、本実施形態では両方を意味する。本実施形態では、要求の認証認可は、認証認可ゲートウェイ３１２が認証認可サービス群１２５（認証部３６０と認可部３６１）にアクセスすることにより行われる。

【００４５】

バックエンドサービス３１１は、矢印Ａ３４０が示すように、バックエンドサービス３１１の実行ログを実行ログテーブル３００に転送する。認証認可ゲートウェイ３１２は、図８で示すような内部処理による結果を表す通過ログを、矢印Ａ３４１が示すように、通過ログテーブル３０１に転送する。矢印Ａ３４０および矢印Ａ３４１は、直接転送（例えば、ＨＴＴＰ通信）を意味してもよいし、間接転送（例えば、転送用エージェントや、システム実行基盤サービス１２２に別途用意されるログ転送部による転送）を意味してもよい。

【００４６】

本実施形態では、例えば、テナントＡ用システム１０４Ａが、一つ以上のサービスモジュールを含むサービスシステムの一例である。テナントＡ用システム１０４Ａがテナント

Ａ用システム領域３１０にデプロイされ、かつ、認証認可ゲートウェイ３１２が当該領域３１０にデプロイされる。具体的には、例えば、バックエンドサービス３１１毎の認証認可ゲートウェイ３１２と、利用者クライアント３５０から要求を受け付ける認証認可ゲートウェイ３１２とがデプロイされる。また、一つのサービスモジュールが複数のテナント用システム１０４の部品とされることもある。具体的には、一つのサービスモジュールの複数の複製がそれぞれ複数のテナント用システム１０４の部品とされることもある。

【００４７】

図４は、コーディネーションサービス１１３の構成の例を示す図である。

【００４８】

コーディネーションサービス１１３は、ログ分類部１１７、テンプレート部１１４、デプロイメント要求部１１５、ログ管理部１１６、および、ロググルーピング部４０１を含む。コーディネーションサービス１１３には、ネットワーク２００などを通じて、コーディネータ１１０の情報処理端末の一例である作業用端末５３０から操作される。

【００４９】

テンプレート部１１４により用意されたテンプレート（例えば、テナント用システムのテンプレート）には、デプロイメントに必要な情報の一例として、テナント用システム１０４の構成要素となるバックエンドサービス３１１の情報（例えば、イメージ名称や稼働に必要な設定情報（環境変数、起動時引数、システム実行領域１２６に要求するリソース量など））の集合が含まれる。

【００５０】

ゲートウェイ制御部４００は、ゲートウェイデプロイメント部４１０、転送設定部４１１、認可設定部４１２、ヘッダ設定部４１３、認証認可要件テーブル４２０、追加ヘッダテーブル４２１、および、ゲートウェイインスタンステーブル４２２を含む。ロググルーピング部４０１は、認証検知部４３０、ユーザ判定部４３１、ロググループ出力部４３２、確認状態テーブル４４０、追加ヘッダテーブル４２１、および、ロググループテーブル４４２を含む。追加ヘッダテーブル４２１は、図示の例の通り、ゲートウェイ制御部４００とロググルーピング部４０１に共通でよい。ゲートウェイ制御部４００およびロググルーピング部４０１が有する機能およびテーブルの詳細は後述する。

【００５１】

図５は、実行ログテーブル３００および通過ログテーブル３０１の構成の例と、要求の転送とログの出力との関係の例とを示す図である。

【００５２】

実行ログテーブル３００は、実行ログ毎にエントリを有する。実行ログは、バックエンドサービス３１１のタスクの実行のログである。各レコードは、バックエンドサービスを識別するためのバックエンドサービスＩＤ５００と、実行ログの出力時刻を示す時刻５０１と、要求に従い実行されたタスクを識別するためのタスク名５０２と、バックエンドサービス３１１に送信された要求（ＨＴＴＰ要求）のヘッダを示す要求ヘッダ５０３と、タスクの実行内容（例えば、要求から抽出した引数、処理の概要、実行結果）を示すタスク内容５０４とを含む。図５では、複数のバックエンドサービスの実行ログを集約することとし、バックエンドサービスＩＤ５００を設けたが、実行ログテーブル３００は、バックエンドサービス毎に設けられてもよい。また、タスク名５０２やタスク内容５０４は統合および分割（例えば、タスク内容５０４から引数情報のみを別のカラムにするなど）されてもよい。

【００５３】

通過ログテーブル３０１は、通過ログ毎にエントリを有する。通過ログは、利用者クライアント３５０から認証認可ゲートウェイ３１２を経由してバックエンドサービス３１１に要求が送信される際の、認証認可ゲートウェイ３１２の要求受信履歴に関するログである。各レコードは、受信した要求の通過ＩＤ（言い換えれば、通過ログを識別するＩＤ）を示す通過ＩＤ５１０、要求を受信したゲートウェイのゲートウェイＩＤであるゲートウェイＩＤ５１１、要求から抽出したアクセストークンであるアクセストークン５１２、お

よび、要求から抽出した親の通過ＩＤ（１つ前の認証認可ゲートウェイ３１２が残した通過ログの通過ＩＤ）を示す親通過ＩＤ５１３を持つ。「通過ＩＤ」としての値は、認証認可ゲートウェイ３１２が要求受信時に発行したＵＵＩＤ（Universally Unique Identifier）としての値でよい。認証認可ゲートウェイ３１２が、要求受信時に事前に定めた要求ヘッダに、当該ゲートウェイ３１２が発行した通過ＩＤが埋め込まれる。この要求ヘッダを持つ要求を次の認証認可ゲートウェイ３１２が受けた場合、当該次の認証認可ゲートウェイ３１２が、当該要求の要求ヘッダから、１つ前の認証認可ゲートウェイ３１２により埋め込まれた通過ＩＤを抽出できる。この抽出された通過ＩＤが、親通過ＩＤである。アクセストークンや親通過ＩＤの埋め込み先となる要求ヘッダのヘッダ名は、図６に示すように、追加ヘッダテーブル４２１にて管理される。

【００５４】

図５によれば、一例として、以下の処理が行われる。なお、図５の説明では、ＩＤ“α”を持つ要素を、要素“α”と言うことがある。

・利用者クライアント３５０から要求０１を認証認可ゲートウェイ“gw-312a”３１２Ｃが受ける。認証認可ゲートウェイ“gw-312a”３１２Ｃが、当該要求からアクセストークン“3SUJBZl…”を取得し、かつ、通過ＩＤ“Da417013df”を付与する。認証認可ゲートウェイ“gw-312a”３１２Ｃが、アクセストークン“3SUJBZl…”および通過ＩＤ“Da417013df”を含んだ通過ログ＃１を通過ログテーブル３０１に格納する。認証認可ゲートウェイ“gw-312a”３１２Ｃが、要求０１のヘッダに通過ＩＤ“Da417013df”を設定し、当該要求０１をバックエンドサービス制御プログラム３１３へと転送する。

・バックエンドサービス制御プログラム３１３が、制御ルール３１４に従い、最初のバックエンドサービス３１１Ａに要求０１を転送する。転送した要求０１のアクセストークンは、例えば、利用者クライアント３５０からのアクセストークン“3SUJBZl…”（利用者のアクセストークン）に代えて、制御ルール３１４で指定されているアクセストークン“LS0u9tL…”（テナントＡのアクセストークン）が採用される。

・その要求０１を、バックエンドサービス３１１Ａについての認証認可ゲートウェイ“gw-312b”３１２Ａが受ける。認証認可ゲートウェイ“gw-312b”３１２Ａが、要求０１からアクセストークン“LS0u9tL…”を取得し、要求０１のヘッダから通過ＩＤ“Da417013df”を取得し、かつ、通過ＩＤ“60ed6bf4oPp”を付与する。認証認可ゲートウェイ“gw-312b”３１２Ａが、アクセストークン“LS0u9tL…”、親通過ＩＤ“Da417013df”および通過ＩＤ“60ed6bf4oPp”を含んだ通過ログ＃２を通過ログテーブル３０１に格納する。認証認可ゲートウェイ“gw-312b”３１２Ａが、要求０１のヘッダに通過ＩＤ“60ed6bf4oPp”を設定し（ヘッダにおける親通過ＩＤ“Da417013df”を通過ＩＤ“60ed6bf4oPp”に差し替え）、当該要求０１をバックエンドサービス３１１Ａへと転送する。

・バックエンドサービス３１１Ａが、認証認可ゲートウェイ“gw-312b”３１２Ａから要求０１を受け、当該要求０１に従いタスクを実行する。バックエンドサービス３１１Ａが、要求０１の要求ヘッダとタスク内容とを含む実行ログ＃３を、実行ログテーブル３００に格納する。

・バックエンドサービス３１１Ａが、要求０１の実行結果に従う応答０２を返す。応答０２は、例えば、要求０１のヘッダ、つまり、通過ＩＤ“60ed6bf4oPp”を含む。応答０２は、バックエンドサービス制御プログラム３１３が受ける。

・バックエンドサービス制御プログラム３１３が、制御ルール３１４に従い、応答０２が持つ実行結果に基づく要求０３を、次のバックエンドサービス３１１Ｂに転送する。要求０３のヘッダは、応答０２が持つ通過ＩＤ“60ed6bf4oPp”を持つ。

・その要求０３を、バックエンドサービス３１１Ｂについての認証認可ゲートウェイ“gw-312c”３１２Ｂが受ける。以降、認証認可ゲートウェイ“gw-312c”３１２Ｂにより、要求０１を受けた認証認可ゲートウェイ“gw-312b”３１２Ａが行った処理と同様の処理が行われる。故に、要求０３から取得された親通過ＩＤ“60ed6bf4oPp”と、要求０３を受けたときに認証認可ゲートウェイ“gw-312c”３１２Ｂが付与した通過ＩＤとを含む通過ログが、通過ログテーブル３０１に格納される。そして、要求０３がバックエンドサービス３１

１Ｂに転送される。
【００５５】
図６は、ゲートウェイ制御部４００が持つテーブルの構成の例を示す図である。
【００５６】
認証認可要件テーブル４２０は、バックエンドサービス３１１およびバックエンドサービス制御プログラム３１３が認証認可およびその両方を必要とするかを示すテーブルである。認証認可要件テーブル４２０の各レコードは、バックエンドサービス３１１およびバックエンドサービス制御プログラム３１３のイメージを識別するサービスイメージ名６００、サービスイメージ名６００が示すイメージによって作成されたインスタンスが認証を必要または不要とするかを示す認証連携６０１、および、サービスイメージ名６００が示すイメージによって作成されたインスタンスが認可を必要または不要とするかを示す認可連携６０２を持つ。
【００５７】
追加ヘッダテーブル４２１は、要求ヘッダの役割を示すメタ情報である。追加ヘッダテーブル４２１の各レコードは、認証認可ゲートウェイ３１２のゲートウェイＩＤであるゲートウェイＩＤ６１０、要求ヘッダの役割を示す用途６１１、および、要求ヘッダの名称を示す要求ヘッダ名６１２を持つ。
【００５８】
ゲートウェイインスタンステーブル４２２は、バックエンドサービス３１１およびバックエンドサービス制御プログラム３１３と、認証認可ゲートウェイ３１２のインスタンスとの関連を管理するテーブルである。ゲートウェイインスタンステーブル４２２の各レコードは、認証認可ゲートウェイ３１２のゲートウェイＩＤであるゲートウェイＩＤ６２０、および、バックエンドサービス３１１およびバックエンドサービス制御プログラム３１３のインスタンスのＩＤであるサービスＩＤ６２１を持つ。
【００５９】
図７は、ロググルーピング部４０１が持つテーブルの構成の例を示す図である。なお、追加ヘッダテーブル４２１の図示は省略されている。
【００６０】
確認状態テーブル４４０は、実行ログテーブル３００に蓄積された各実行ログに関して、どの実行ログまでを確認したか、または次にどの実行ログを確認するかを特定するための情報を保持する。図７では、実行ログが時系列順に蓄積され、実行ログ間で時系列関係を示す情報（例えば、タイムスタンプのような時刻）は重複しないものとして説明する。キー７００は、実行ログの出力元（例えば、インスタンス名など）を識別する文字列である。位置関連７０１は、確認した最も新しい実行ログまたは次に確認すべき最も古い実行ログの時刻（タイムスタンプ）である。実行ログが時系列順に蓄積されない場合は、エントリ番号（行番号）またはそれに類する値が、位置関連７０１の値となる。
【００６１】
ロググループテーブル４４２は、実行ログテーブル３００の各実行ログを、利用者（ユーザ）観点でグループ化するための情報を保持する。ロググループテーブル４４２の各レコードにおいて、ラベル７１０は、ロググループを識別するための文字列である。ユーザ識別７１１は、アクセストークンなどユーザを識別できる情報である。通過ＩＤ７１２は、通過ログテーブル３０１と関連付けるための情報である。
【００６２】
図８は、認証認可ゲートウェイ３１２の動作の流れの例を示す図である。
【００６３】
認証認可ゲートウェイ３１２は、バックエンドサービス制御の要求元８００（利用者クライアント３５０またはバックエンドサービス制御プログラム３１３）と、認可部３６１と、認証部３６０と、ロール管理サービス８１０と連携する。認証認可ゲートウェイ３１２は、認証を行う役割を持つ（要求元８００の認証連携６０１が“Ｙ”である）場合は、要求元８００からの要求８０１について認証向け制御８０３を行う。また、認証認可ゲート

ウェイ３１２は、認可を行う役割を持つ（要求元８００の認可連携６０２が“Ｙ”である）場合は、要求８０１について認可向け制御８０４を実行する。図８は、認証認可ゲートウェイ３１２が認証と認可の両方の役割を持つ場合を例示する。また、本実施形態では、要求８０１は、ＨＴＴＰ要求である。

【００６４】

まず、認証認可ゲートウェイ３１２は、要求元８００より、バックエンドサービス３１１向けのＨＴＴＰ要求８０１を受信する（矢印Ａ８０２）。

【００６５】

次に、認証認可ゲートウェイ３１２は、認証結果取得処理８０５を行う。具体的には、例えば、認証認可ゲートウェイ３１２は、ＨＴＴＰ要求８０１から認証の入力情報（例えば、要求ヘッダ内のアクセストークンとユーザ識別情報）を取得する。認証認可ゲートウェイ３１２は、取得した認証入力情報を認証部３６０に送信し認証を要求する。認証部３６０は、入力情報と認証テーブル８０９（例えば、ユーザ識別情報とトークンの関係を表すテーブル）を照らし合わせて認証を行い、その結果を認証認可ゲートウェイ３１２に返す（矢印Ａ８０７）。

【００６６】

続いて、認証認可ゲートウェイ３１２は、認証結果取得処理８０５において認証成功であった場合（認証入力情報内のユーザの識別情報とアクセストークンとのペアの承認が得られた場合）に、認可引数取得処理８０６へ処理を移す（矢印Ａ８１３）。認可引数取得処理８０６では、認証認可ゲートウェイ３１２は、ユーザの識別情報を入力として、ロール管理サービス８１０に対し当該ユーザのロール情報取得を要求する。ロール管理サービス８１０は、入力をキーとしてロールテーブル８１１（例えば、ユーザの識別情報とロール名の関係を表すテーブル）よりロール名を取得し返す（矢印Ａ８１２）。その後、認証認可ゲートウェイ３１２は、ヘッダ付与処理８１６へ処理を移す（矢印Ａ８１４）。

【００６７】

認証認可ゲートウェイ３１２は、ヘッダ付与処理８１６において、ヘッダ設定部４１３を通じて事前に定められたルールに従って、ＨＴＴＰ要求８０１のヘッダに、前述のロール名を少なくとも含む追加ヘッダ情報を付与する（矢印Ａ８１７）。

【００６８】

その後、認証認可ゲートウェイ３１２は、要求送信処理８１９を行う。具体的には、例えば、認証認可ゲートウェイ３１２は、転送エントリ８２４の内容に従って、追加ヘッダ情報つきＨＴＴＰ要求８２１を認可部３６１へ送信する（矢印Ａ８２０）。また、認証認可ゲートウェイ３１２は、要求８０１から取得されたアクセストークンと追加ヘッダ情報に含まれる通過ＩＤ（認証認可ゲートウェイ３１２が付与したＩＤ）とを含む通過ログを通過ログテーブル３０１に格納する（矢印Ａ８１８）。

【００６９】

認可部３６１は、ロール名と認可ルール８２２を照らし合わせて認可を行い、認可成功（入力のロール名はバックエンドサービスのアクセス権限を持つ）の場合は、バックエンドサービス３１１へＨＴＴＰ要求８２１を送信する（矢印Ａ８２３）。

【００７０】

認可向け制御８０４が不要の場合、認証結果取得処理８０５の後、処理が、ヘッダ付与処理８１６に移動する（矢印Ａ８１５）。

【００７１】

図９は、ロググルーピング部４０１の動作の流れの例を示す図である。

【００７２】

認証検知部４３０は、確認状態テーブル４４０にアクセスし、次に確認すべき実行ログテーブル３００の位置を特定する。その後、認証検知部４３０は、特定した位置より実行ログテーブル３００から実行ログ（実行ログレコード）を取得する。認証検知部４３０は、新規に受けた要求について認証があった場合は、ユーザ判定部４３１を開始する。

【００７３】

ユーザ判定部４３１は、通過ログテーブル３０１を辿り、アクセストークン５１２がユーザ用である通過ログ（通過ログレコード）を特定し、特定された通過ログから通過ＩＤ５１０を抽出する。

【００７４】

ロググループ出力部４３２は、抽出された通過ＩＤと、当該通過ＩＤに対応したユーザ識別情報（当該通過ＩＤをキーに実行ログ中の要求ヘッダから取得されたユーザ識別情報）とを入力として起動する。ロググループ出力部４３２は、通過ＩＤとユーザ識別情報のセットに任意のラベル（例えば、ＵＵＩＤや連番などの一意性が保証できる文字列）を付与する。ロググループ出力部４３２は、ラベル、通過ＩＤおよびユーザ識別情報の組を、ロググループテーブル４４２に格納する。

【００７５】

図１０は、ゲートウェイデプロイメント部４１０の処理フローチャートの例を示す。

【００７６】

ゲートウェイデプロイメント部４１０は、情報Ａを引数として起動する。情報Ａは、イメージ名と、認証認可ゲートウェイ３１２からの転送先ＡＰＩエンドポイントと、外部公開用のＡＰＩエンドポイントと、領域名称（デプロイメント先となるシステム実行領域の名称）とを含む。

【００７７】

ゲートウェイデプロイメント部４１０は、認証実行要求のためのメタ情報を認証部３６０より取得する（ステップ１０００）。ゲートウェイデプロイメント部４１０は、認証認可ゲートウェイ３１２からの接続受付のためのメタ情報を認証部３６０に送信する（ステップ１００１）。

【００７８】

ゲートウェイデプロイメント部４１０は、情報Ａ内のイメージ名に対応した認証連携６０１および認可連携６０２を認証認可要件テーブル４２０から取得する（ステップ１００２）。

【００７９】

ゲートウェイデプロイメント部４１０は、情報Ａ内の領域名称をデプロイメントの第一引数とする（ステップ１００４）。

【００８０】

ゲートウェイデプロイメント部４１０は、ステップ１００２で取得した認証連携６０１の値が“Ｙ”か確認する（ステップ１００５）。認証連携６０１の値が“Ｙ”であれば、ゲートウェイデプロイメント部４１０は、ステップ１０００とステップ１００１で取得したメタ情報をデプロイメントの第２の引数（環境変数など）とする（ステップ１００６）。

【００８１】

ゲートウェイデプロイメント部４１０は、デプロイメントの引数を用いて、デプロイメント要求部１１５に対して、認証認可ゲートウェイ３１２のデプロイメントを依頼し完了を待つ（ステップ１００７）。

【００８２】

ゲートウェイデプロイメント部４１０は、情報Ａ内の転送先ＡＰＩエンドポイントと外部公開用ＡＰＩエンドポイントと領域名称とを引数として、転送設定部４１１を開始し完了を待つ（ステップ１００８）。

【００８３】

ゲートウェイデプロイメント部４１０は、ステップ１００２で取得した認可連携６０２の値が“Ｙ”か確認する（ステップ１００９）。認可連携６０２の値が“Ｙ”であれば、ゲートウェイデプロイメント部４１０は、認可部３６１のＡＰＩエンドポイントを引数として認可設定部４１２を開始し完了を待つ（ステップ１０１０）。

【００８４】

図１１は、転送設定部４１１および認証認可ゲートウェイ３１１の処理フローチャートの例を示す図である。

【００８５】
転送設定部４１１は、情報Ｂを引数として起動する。情報Ｂは、図１０のステップ１００８について説明した通り、転送先ＡＰＩエンドポイント、外部公開用ＡＰＩエンドポイント、および、領域名称（システム実行領域の名称）を含む。
【００８６】
転送設定部４１１は、情報Ｂ内の転送先ＡＰＩエンドポイント、外部公開用ＡＰＩエンドポイントおよび領域名称のセットを転送エントリとする（ステップ１１００）。
【００８７】
転送設定部４１１は、転送エントリを引数に認証認可ゲートウェイの転送エントリ追加ＡＰＩにアクセスする（ステップ１１０１）。
【００８８】
認証認可ゲートウェイ３１１は、環境変数などより、認証部３６０に接続するためのメタ情報を取得する（ステップ１１１０）。認証認可ゲートウェイ３１１は、当該取得したメタ情報を認証結果取得処理８０５（図８参照）に設定する（ステップ１１１１）。
【００８９】
認証認可ゲートウェイ３１１は、ＡＰＩサービスを開始し要求受信を待つ（ステップ１１１２）。認証認可ゲートウェイ３１１は、転送エントリ追加ＡＰＩが呼ばれた（要求を受信した）場合（ステップ１１１３：Ｙ）、当該ＡＰＩの呼び出しの引数とされ受信した転送エントリを転送エントリ８２４（例えば、メモリ上の変数、外部ＤＢ、設定ファイルなど）に追加し、再び要求受信を待つ（ステップ１１１２）。
【００９０】
図１２は、認可設定部４１２および認証認可ゲートウェイの処理フローチャートの例を示す図である。
【００９１】
認可設定部４１２は、情報Ｃを引数として起動する。情報Ｃは、領域名称（システム実行領域の名称）、転送先ＡＰＩエンドポイント、ロール名、およびユーザ名を含む。ここで言う転送先ＡＰＩエンドポイントは、図１０のステップ１０１０において引数とされた、認可部３６１のＡＰＩエンドポイントである。領域名称は、ゲートウェイデプロイメント部４１０に入力された情報Ａ内の領域名称である。ロール名およびユーザ名は、ロール管理サービス８１０から取得された情報である。
【００９２】
認可設定部４１２は、情報Ｃを認可エントリとする（ステップ１２００）。認可設定部４１２は、認可エントリを引数に認証認可ゲートウェイ３１１の認可エントリ追加ＡＰＩにアクセスする（ステップ１２０１）。
【００９３】
認証認可ゲートウェイ３１２のステップ１２１０～１２１２は、図１１のステップ１１１０～１１１２と同じである。認証認可ゲートウェイ３１２は、認可エントリ追加ＡＰＩが呼ばれた（要求を受信した）場合（ステップ１２１３：Ｙ）、認可エントリを引数に認可部３６１の認可ルール追加ＡＰＩにアクセス（要求を送信）する（ステップ１２１４）。
【００９４】
認可部３６１の認可ルール追加ＡＰＩ１２２０は、認証認可ゲートウェイ３１２から受けた要求より認可エントリを取得し、取得した認可エントリを認可ルール８２２に追加する（ステップ１２２１）。
【００９５】
図１３は、ヘッダ設定部４１３の処理フローチャートの例を示す図である。
【００９６】
ヘッダ設定部４１３は、通過ＩＤ用のヘッダ名“auth_id”を引数に起働する。ヘッダ設定部４１３は、ヘッダ付与処理８１６に対して、入力のヘッダ名で通過ＩＤをＨＴＴＰ要求のヘッダに付与するための設定を行う（ステップ１３００）。
【００９７】

図１４は、認証検知部４３０の処理フローチャートの例を示す図である。
【００９８】
認証検知部４３０は、タスク実行ログキー（バックエンドサービス３１１のインスタンス名など）を入力に起動する。
【００９９】
認証検知部４３０は、追加ヘッダテーブル４２１より、用途６１１が“ゲートウェイ通過識別”のレコードのヘッダ名６１２を取得する（ステップ１４００）。認証検知部４３０は、タスク実行ログキーを用いて、確認状態テーブル４４０より位置関連７０１を取得する（ステップ１４０１）。認証検知部４３０は、タスク実行ログキーと取得された位置関連７０１より、実行ログテーブル３００の読み取り開始点を決定する（ステップ１４０２）。
【０１００】
認証検知部４３０は、実行ログテーブル３００の次の実行ログレコード（開始点に属するレコードの次のレコード）を取得する（ステップ１４０３）。認証検知部４３０は、当該取得した実行ログレコードの要求ヘッダ５０３より、ステップ１４００で取得したヘッダ名に関するヘッダ値を取得する（ステップ１４０４）。認証検知部４３０は、ロググループテーブル４４２の通過ＩＤ７１２内に、ステップ１４０４で取得したヘッダ値が存在するか確認する（ステップ１４０５）。
【０１０１】
当該ヘッダ値が存在する場合（ステップ１４０６：Ｙ）、認証検知部４３０は、当該ヘッダ値（通過ＩＤ）を引数に図１５のユーザアクセストークン特定を開始する（ステップ１４０７）。
【０１０２】
当該ヘッダ値が存在しない場合（ステップ１４０６：Ｎ）、または、ステップ１４０７の後、認証検知部４３０は、ステップ１４０３で取得した実行ログレコードがタスク実行ログキーに関して実行ログテーブル３００の最後のレコードか確認する（ステップ１４０８）。確認結果が真であれば、処理が終了する。確認結果が偽であれば、処理がステップ１４０３へ移動する。
【０１０３】
図１５は、ユーザアクセストークン特定の処理フローチャートの例を示す。
【０１０４】
認証検知部４３０は、引数とされた通過ＩＤを持つ通過ログレコードを通過ログテーブル３３１から取得する（ステップ１５００）。認証検知部４３０は、ステップ１５００で取得した通過ログレコードよりゲートウェイＩＤを取得する（ステップ１５０１）。認証検知部４３０は、ステップ１５０１で取得したゲートウェイＩＤと同じゲートウェイＩＤ６２０を持つレコードを、ゲートウェイインスタンステーブル４２２から取得する（ステップ１５０２）。認証検知部４３０は、ステップ１５０２で取得したレコードのサービスＩＤ６２１に属するサービスイメージ名６００を持つレコードを認証認可要件テーブル４２０から取得する（ステップ１５０３）。ステップ１５０３で取得したレコードの認証連携６０１が“Ｙ”の場合（ステップ１５０４：Ｙ）、処理がステップ１５０８へ移動する。当該認証連携６０１が“Ｎ”であるが当該レコードの認可連携６０２が“Ｙ”の場合（ステップ１５０４：Ｎ、ステップ１５０５：Ｙ）、処理がステップ１５０６へ移動する。認証連携６０１と認可連携６０２のいずれも“Ｎ”の場合は（ステップ１５０４：Ｎ、ステップ１５０５：Ｎ）、処理が終了する。
【０１０５】
ステップ１５０５：Ｙの場合、認証検知部４３０は、ステップ１５０１で取得した通過ログレコードより親通過ＩＤ５１３を取得する（ステップ１５０６）。認証検知部４３０は、ステップ１５０６で取得した親通過ＩＤを通過ＩＤとし（ステップ１５０７）、ステップ１５００以降を実施する。
【０１０６】
ステップ１５０４：Ｙの場合、認証検知部４３０は、ステップ１５００で取得した通過

ログレコードのアクセストークン５１２をユーザ識別情報とする（ステップ１５０８）。認証検知部４３０は、通過ＩＤとユーザ識別情報を引数としてロググループ出力部４３２を開始する（ステップ１５０９）。認証検知部４３０は、ゲートウェイインスタンステーブル４２２に次のレコードがあるか確認する（ステップ１５１０）。確認結果が真であれば、処理がステップ１５０１に移動する。確認結果が偽であれば、処理が終了する。

【０１０７】

図１６は、ロググループ出力部４３２の処理フローチャートの例を示す図である。

【０１０８】

ロググループ出力部４３２は、通過ＩＤと、ユーザ識別情報を入力として起動する。ロググループ出力部４３２は、通過ＩＤとユーザ識別情報のセットに任意のラベル（ＵＵＩＤや連番などの一意性が保証できる文字列）を付与する（ステップ１６００）。ロググループ出力部４３２は、通過ＩＤ、ユーザ識別情報およびラベルをロググループテーブル４４２のレコードとして出力する（ステップ１６０１）。

【０１０９】

本実施形態によれば、バックエンドサービス３１１は認証認可機能を持たず、かつ複数のユーザで共用する場合でも、ユーザ（利用者）毎の利用明細を出力できる。

［実施形態２］

【０１１０】

実施形態２を説明する。その際、実施形態１との相違点を主に説明し、実施形態１との共通点については説明を省略または簡略する。

【０１１１】

実施形態１では、バックエンドサービス３１１への要求にあるアクセストークンと、各要求が認証認可ゲートウェイ３１２（インスタンス）を通過する際に当該要求のヘッダに自動的に埋め込まれた要求ＩＤと、要求ＩＤ間の親子関係を用いて、バックエンドサービス３１１が出力する実行ログをユーザ（利用者）毎に分類するためのグループ情報が生成される。本実施形態では、前述の実行ログとグループ情報を用いて、業務（例えば、ユーザ毎の課金や利用状況の可視化など）に向けたデータが出力される。

【０１１２】

図１７は、本実施形態におけるコーディネーションサービス１７０１の構成の例を示す図である。

【０１１３】

コーディネーションサービス１７０１は、課金用データ出力部１７００を備える。課金用データ出力部１７００は、前述の実行ログとグループ情報を用いて業務に向けたデータを出力するデータ出力部１７１０を持つ。

【０１１４】

図１８は、データ出力部１７１０の処理フローチャートの例を示す図である。

【０１１５】

データ出力部１７１０は、ユーザ識別情報と追加のフィルタ情報（時刻範囲など）を入力として起動する。追加のフィルタ情報は必須ではない。

【０１１６】

データ出力部１７１０は、入力のユーザ識別情報を用いてロググループテーブル４４２から通過ＩＤの集合を取得する（ステップ１８００）。データ出力部１７１０は、ステップ１８００で取得した通過ＩＤ集合のいずれかの通過ＩＤを要求ヘッダ５０３に持つ実行ログを実行ログテーブル３００から取得する（ステップ１８０１）。

【０１１７】

データ出力部１７１０は、追加のフィルタ情報が入力されているかを確認する（ステップ１８０２）。確認結果が偽であれば、処理がステップ１８０４に移動する。

【０１１８】

確認結果が真であれば、データ出力部１７１０は、ステップ１８０１で取得した実行ログに対して追加のフィルタ情報でフィルタする（ステップ１８０３）。

【０１１９】
データ出力部１７１０は、要求元に実行ログを返す（ステップ１８０４）。
【０１２０】
図１８では、実行ログの出力先として実行ログの要求元としたが、既定のディレクトリやテーブルなどへの実行ログが出力されてもよい。
［実施形態３］
【０１２１】
実施形態３を説明する。その際、実施形態２との相違点を主に説明し、実施形態２との共通点については説明を省略または簡略する。
【０１２２】
実施形態２では、ログとそのグループ情報を用いて、業務（例えば、ユーザ毎の課金や利用状況の可視化など）に向けたデータが出力される。本実施形態では、請求実行などに必要な契約関連情報が、前述のデータに付与される。
【０１２３】
図１９は、本実施形態におけるコーディネーションサービス１９１０の構成の例を示す図である。
【０１２４】
コーディネーションサービス１９１０において、課金用データ出力部１９２０が、データ出力部１９５０と、契約マッピングテーブル１９００とを備える。また、契約管理サービス１９０２が備えられる。契約管理サービス１９０２は、契約ＩＤ、および、契約内容（例えば、利用するバックエンドサービスとその利用単価などといった情報）を持つ。契約マッピングテーブル１９００は、前述の契約ＩＤと、課金用データ（例えば、実行ログレコードの集合）を関連付けるためのマッピングテーブルである。矢印Ａ１９０１が示すように、データ出力部１９５０は、契約マッピングテーブル１９００から、課金用データのラベルに対応した契約ＩＤを取得し、契約管理サービス１９０２から、当該契約ＩＤに対応した契約内容を取得し、取得した契約内容を基に課金用データを加工する（例えば、契約内容の情報を付与する）。
【０１２５】
図２０は、契約マッピングテーブル１９００の構成の例を示す図である。
【０１２６】
契約マッピングテーブル１９００は、契約ＩＤ２０００とラベル２００１の対応関係を管理する。
【０１２７】
図２１は、本実施形態におけるデータ出力部１９５０の処理フローチャートの例を示す図である。
【０１２８】
図１８との違いは、ステップ２１００、２１０１、２１０２の追加である。データ出力部１９５０は、ロググループテーブル４４２のラベル７１０をキーに、ラベル７１０に一致するラベル２００１に対応した契約ＩＤ２０００を契約マッピングテーブル１９００から取得する（ステップ２１００）。データ出力部１９５０は、契約管理サービス１９０２から、取得した契約ＩＤ２０００に一致する契約ＩＤに対応した契約内容を取得する（ステップ２１０１）。データ出力部１９５０は、ステップ２１０１で取得した契約内容を用いて課金用データを加工する（ステップ２１０２）。
【０１２９】
以上の実施形態１～３の説明を、例えば以下のように総括することができる。また、以下では、上述の説明が必要に応じて補足されてよい。
【０１３０】
一または複数の開発者１３０により開発された複数のバックエンドサービス３１１（複数のサービスモジュールの一例）うちの一つ以上のバックエンドサービス３１１により構成されたテナント用システム１０４（サービスシステムの一例）が、複数種類の計算資源

に基づく実行基盤サービス１２２にデプロイされる。実行基盤サービス１２２に、コーディネーションサービス１１３（システム実行支援装置の一例）のゲートウェイ制御部４００により、テナント用システム１０４について一つ以上のゲートウェイ３１２がデプロイされる。

【０１３１】

各バックエンドサービス３１１は、当該バックエンドサービス３１１についての要求を実行した場合に当該要求の実行における使用量を含む実行内容と当該要求のヘッダ情報（要求のヘッダが有する情報）とを含んだログである実行ログを実行ログテーブル３００（第１のログ情報の一例）に書き込むようになっている。「使用量」は、時間、計算資源量およびデータ量の少なくとも一種類の量を含んでよい。また、「使用量」は、バックエンドサービス３１１の実行により使用された物理的な計算資源の使用量でもよいし、バックエンドサービス３１１の使用量でもよい。

【０１３２】

テナント用システム１０４におけるバックエンドサービス３１１Ａ（対象のサービスモジュールの一例）について、ゲートウェイ３１２Ａが、アクセストークン（認証および認可の少なくとも一つのためのデータである認証認可データの一例）を持つ要求を受ける。すると、ゲートウェイ３１２Ａは、受けた要求に対し当該要求の通過ＩＤを付与し、当該要求のヘッダに、アクセストークンに代えて当該付与した通過ＩＤを設定する。ゲートウェイ３１２Ａは、当該通過ＩＤを含んだヘッダを持つ要求を、対象のバックエンドサービス３１１Ａに転送し、当該通過ＩＤと上記アクセストークンとを含んだログである通過ログを通過ログテーブル３０１（第２のログ情報の一例）に書き込む。

【０１３３】

各バックエンドサービス３１１が上述の実行ログを書き込むようになっていても、実行ログは、利用者の識別情報相当の情報を含んでいない。一方、ゲートウェイ３１２が、アクセストークンを含む上述の通過ログを書き込むようになっていても、通過ログは、バックエンドサービス３１１の実行に従う使用量を表す情報を含んでいない。実行ログと通過ログが、通過ＩＤを介して互いに関連付けられる。具体的には、実行ログ内のヘッダ情報に設定された通過ＩＤと、通過ログに設定された通過ＩＤとにより、実行ログと通過ログとが関連付けられる。結果として、通過ＩＤをキーに使用量の特定が可能となり、故に、使用量に応じた従量課金が可能となる。

【０１３４】

なお、アクセストークンは、認証認可に使用されるデータでありログに記録されることは避ける方が好ましい。バックエンドサービス３１１に転送される要求のヘッダ情報は、アクセストークンに代えて通過ＩＤを持つので、実行ログにヘッダ情報が含まれても、アクセストークンが実行ログに含まれずに済む。

【０１３５】

実行ログテーブル３００および通過ログテーブル３０１は、ログ管理部１１６により管理されてよい。ログ管理部１１６は、例えばファイルシステムでよい。

【０１３６】

また、要求のメタ情報として、ヘッダ情報以外の情報でもよいが、メタ情報がヘッダ情報であることで、要求としてＨＴＴＰ要求の採用が可能である。また、認証認可データは、アクセストークン以外のデータでもよいが、認証認可データがアクセストークンであることで、要求としてＨＴＴＰ要求の採用が可能である。

【０１３７】

テナント用システム１０４を構成するバックエンドサービス３１１Ａおよび３１１Ｂにそれぞれ用意されるゲートウェイ３１２Ａおよび３１２Ｂ（第２のゲートウェイの一例）の他に、テナント用システム１０４についてのゲートウェイ３１２Ｃ（第１のゲートウェイの一例）がある。ゲートウェイ３１２Ｃが、クライアント３５０から、利用者のアクセストークンを持つ要求を受ける。ゲートウェイ３１２Ｃが、当該要求に対し通過ＩＤを付与し、当該要求のヘッダに当該付与した通過ＩＤを設定する。ゲートウェイ３１２Ｃが、

当該通過ＩＤを含んだヘッダ情報を持つ要求を転送し、当該要求ＩＤと利用者のアクセストークンとを含んだ通過ログを通過ログテーブル３０１に書き込む。ゲートウェイ３１２Ｃにより転送された要求を、ゲートウェイ３１２Ａが受ける。

【０１３８】

このようにゲートウェイ３１２間で要求が転送され、個々のゲートウェイ３１２により通過ログが蓄積される。通過ログを辿ることで、利用者のアクセストークンについて実行ログ毎の使用量を算出することが期待できる。

【０１３９】

また、テナント用システム１０４に関し一連の要求の転送について、最初の通過ログには、クライアント３５０からの要求が持つアクセストークンが含まれる。この場合、仮に、バックエンドサービス制御プログラム３１３を通じてバックエンドサービス３１１が受ける要求のアクセストークンが、テナントのアクセストークンであるとしても、ゲートウェイ３１２Ｃがクライアント３５０から受ける要求が持つアクセストークンは、利用者のアクセストークンである可能性が高い。このため、テナント用システム１０４についてテナント単位のアクセストークンが発行されているケースでも、利用者単位で、テナント用システム１０４の実行に従う使用量の集計が可能であることが期待される。

【０１４０】

通過ログは、当該通過ログに対応し要求を転送したゲートウェイより付与された通過ＩＤと、当該要求から抽出された認証認可データと、当該要求の転送元のゲートウェイにより付与された通過ＩＤである親通過ＩＤとを含む。ゲートウェイ３１２Ｃが受けた要求のアクセストークンについて、通過ＩＤを用いて通過ログを辿ることができる。

【０１４１】

具体的には、例えば、親通過ＩＤの無いアクセストークンについて、ロググルーピング部４０１が、当該アクセストークンに対応した通過ＩＤに関連付いている一つ以上の通過ＩＤの集合である通過ＩＤ集合を通過ログテーブル３０１から特定してよい。ロググルーピング部４０１が、当該通過ＩＤ集合を構成する通過ＩＤ毎に、当該通過ＩＤを含んだヘッダ情報に対応する実行内容（タスク内容５０４）を特定してよい。ログテーブル３０１が、当該通過ＩＤ集合について特定された実行内容に従う使用量を表す情報である利用情報を生成してよい。このようにして、親通過ＩＤの無いアクセストークン毎に、使用量を表す利用情報の生成が可能である。

【０１４２】

また、例えば、親通過ＩＤの無いアクセストークンについて、さらに、課金用データ出力部１７００が、生成され利用情報を基に、当該利用情報が表す使用量に応じた課金額を決定し、決定した課金額を出力してよい。このようにして、親通過ＩＤの無いアクセストークン毎に、使用量に応じた従量課金が可能である。

【０１４３】

また、例えば、親通過ＩＤの無いアクセストークンについて、さらに、課金用データ出力部１９２０が、当該アクセストークンに対応した契約内容を特定し、上記決定した課金額に上記特定した契約内容を関連付けて出力してよい。このようにして、課金額の根拠の一例となる契約内容を表す情報も一緒に出力することが可能である。

【０１４４】

ゲートウェイ制御部４００が、テナント用システム１０４を構成する一つ以上のバックエンドサービス３１１の各々を、実行基盤サービス１２２にデプロイし、当該テナント用システム１０４についてゲートウェイ３１２Ｃを実行基盤サービス１２２にデプロイし、当該テナント用システム１０４を構成するバックエンドサービス３１１Ａおよび３１２Ｂ（一つ以上のサービスモジュールの一例）についてゲートウェイ３１２Ａおよび３１２Ｂ（一つ以上の第２のゲートウェイの一例）を実行基盤サービス１２２にデプロイする。このようにして、テナント用システム１０４の窓口としてゲートウェイ３１２Ｃと、テナント用システム１０４を構成するバックエンドサービス３１１Ａ（３１１Ｂ）のゲートウェイ３１２Ａ（３１２Ｂ）とを配備することができる。例えば、ゲートウェイ制御部４００

は、テナント用システム１０４のテンプレート情報またはイメージといった情報から、テナント用システム１０４を構成する個々のバックエンドサービス３１１を特定し、特定したバックエンドサービス３１１毎にゲートウェイ３１２をデプロイし、テナント用システム１０４についてゲートウェイ３１２Ｃをデプロイすることができる。

【０１４５】

各ゲートウェイ３１２は、要求を受けた場合、必要に応じて（例えば、転送先サービスモジュールのサービスイメージ名６００に対応した認証連携６０１と認可連携６０２の値に応じて）、当該要求が持つアクセストークンを、テナント用システム１０４の外部に設けられ認証認可を行う機能である認証認可サービス群１２５に送信することで、当該認証認可サービス群１２５に認証認可を実行させる。このため、いずれのバックエンドサービス３１１が認証認可機能を持たなくても、認証認可を行うことができる。

【０１４６】

以上の説明は、本発明の説明のための例示であって、本発明の範囲を上述の実施形態にのみ限定する趣旨ではない。本発明は、他の種々の形態でも実施することが可能である。

【０１４７】

例えば、テナント用システム１０４は、それぞれがアプリケーションサービスに関連付けられている複数のノードと当該複数のノードにおける各ノード間の結線とで表現されたアプリケーションソフトウェアフローでよい。ノードに関連付いたアプリケーションサービスは、サービスモジュールの一例でよい。アプリケーションソフトウェアフローは、ビジュアルプログラミングツールで記述されてよい。ビジュアルプログラミングツールは、「モデル開発環境」と呼ばれてもよい。ソフトウェアの構成要素や処理単位がノードであり、ノード同士の結線は「エッジ」と呼ばれてもよい。

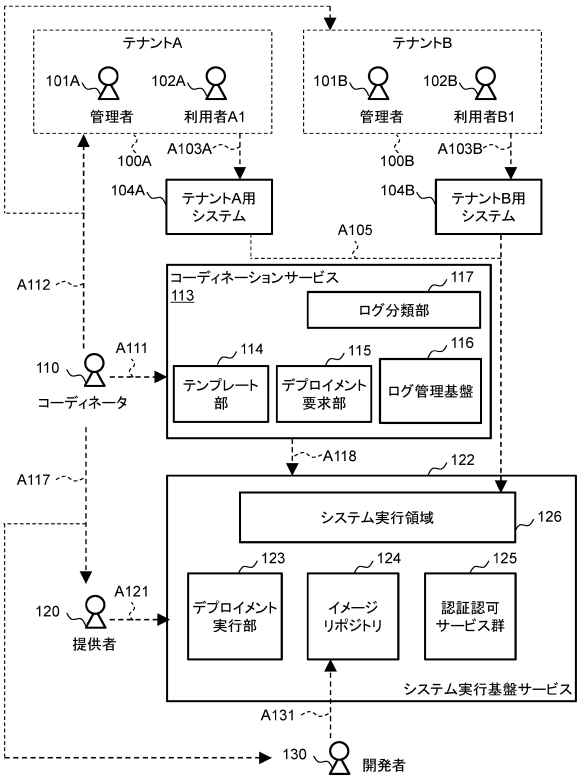
【０１４８】

また、本発明は、要求にメタ情報を付与できる環境全般に適用することが期待できる。例えば、ＷＥＢシステムに代えて、クライアントプログラムがライブラリにデータを記述する環境であって、関数の引数に独自の引数を追加することが許容されている環境にも、本発明を適用可能である。

【図面】

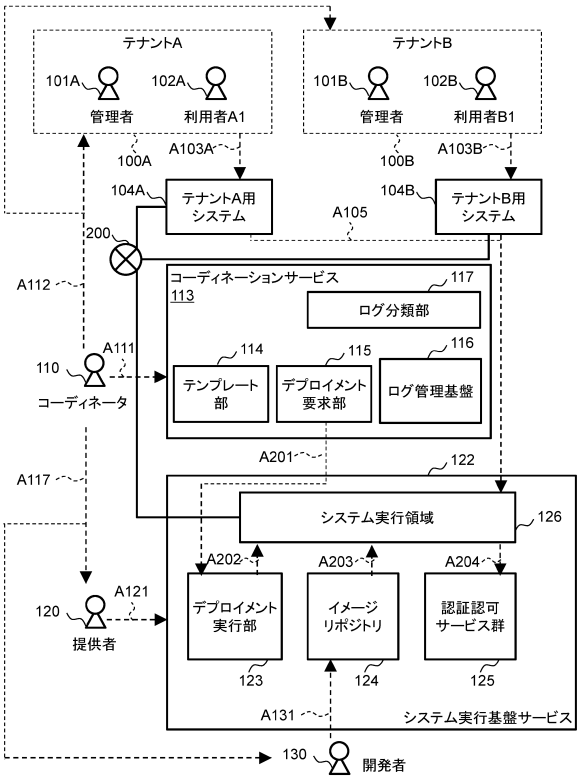
【図１】

図 1



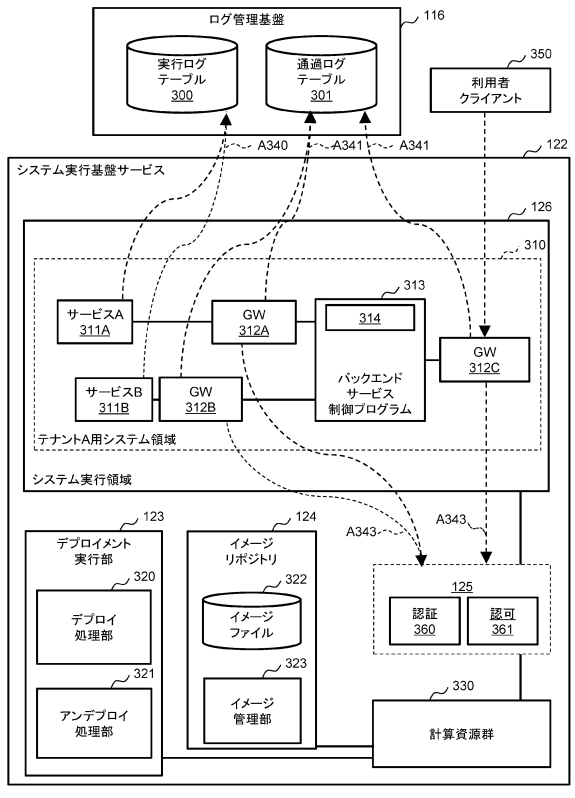
【図２】

図 2



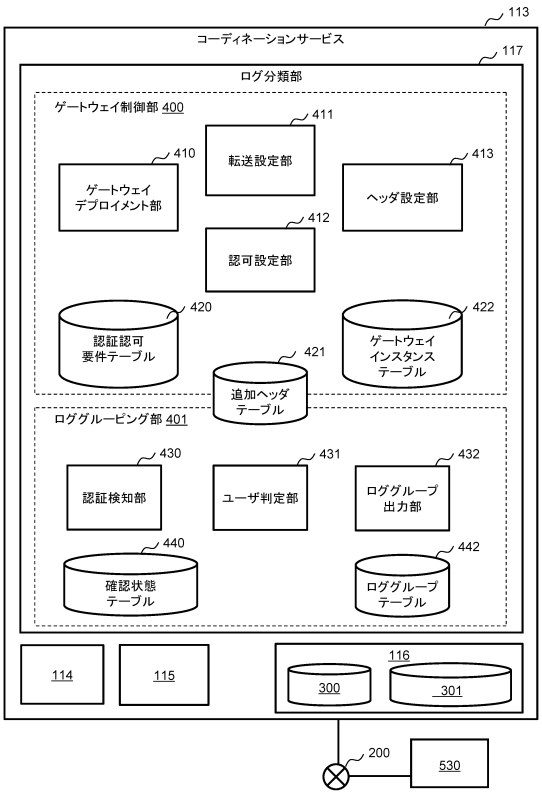
【図３】

図 3



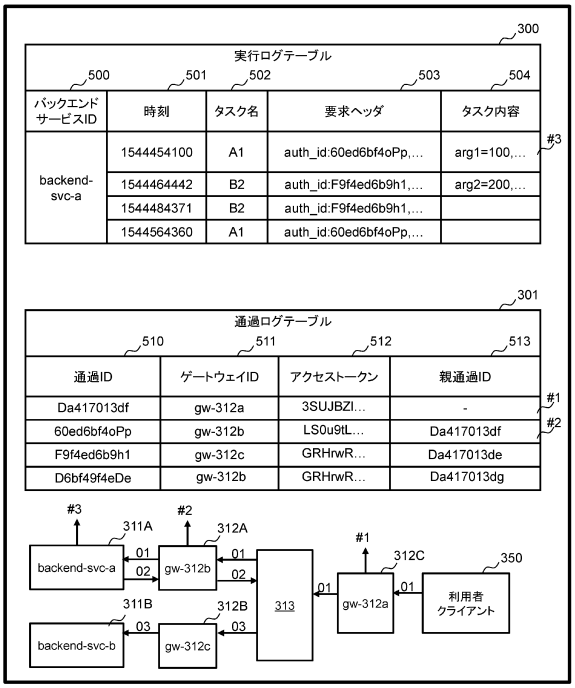
【図４】

図 4



【図５】

図 5

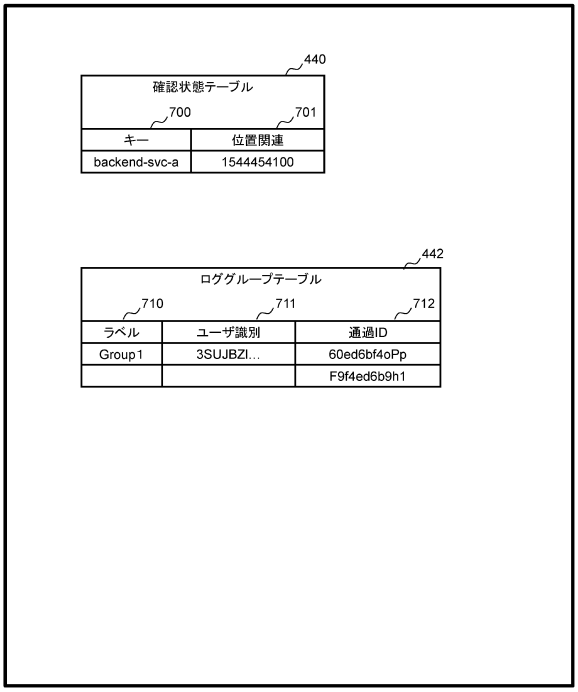


【図６】

図 6

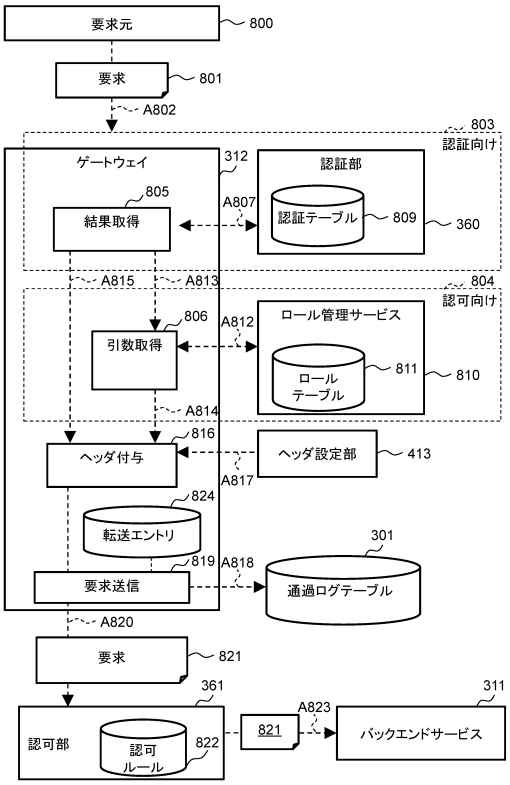
【図７】

図 7



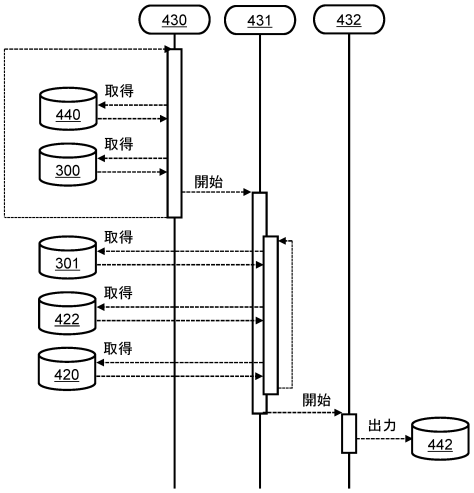
【図８】

図 8



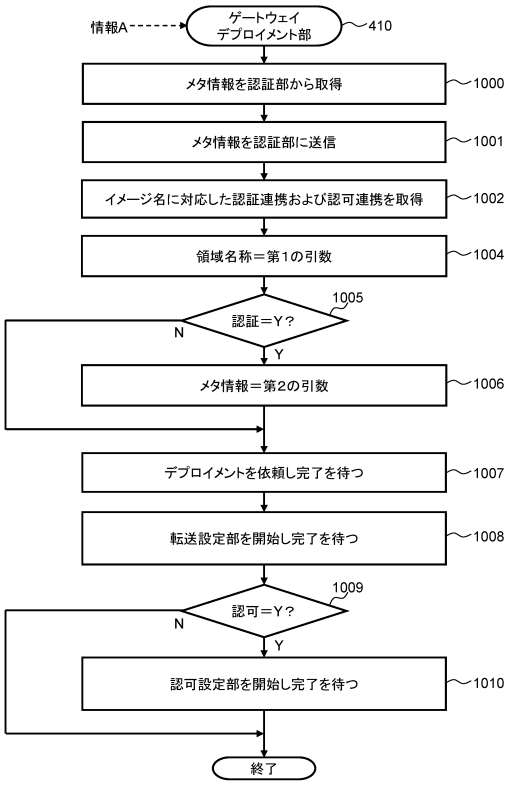
【図９】

図 9



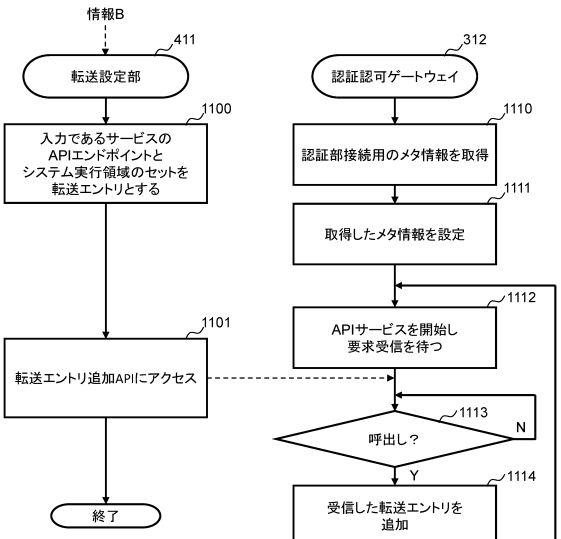
【図１０】

図 10



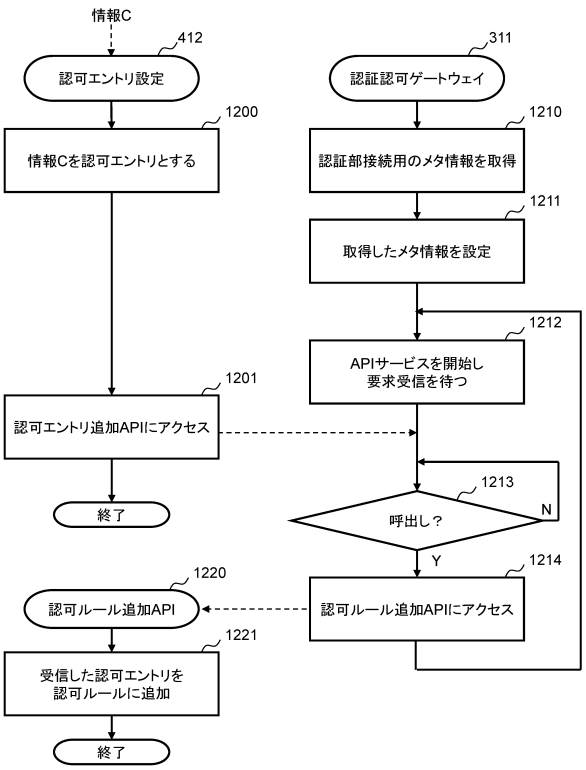
【図１１】

図 11



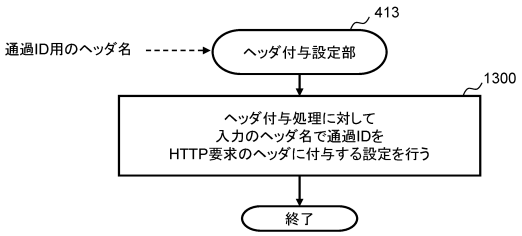
【図１２】

図 12



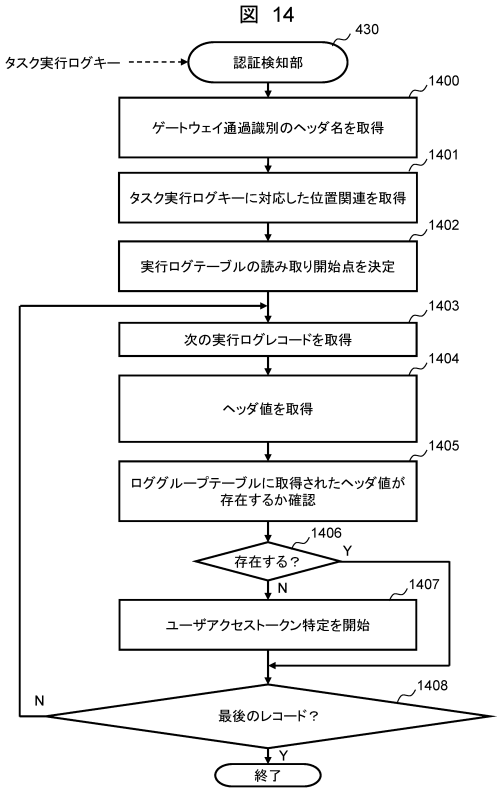
【図１３】

図 13



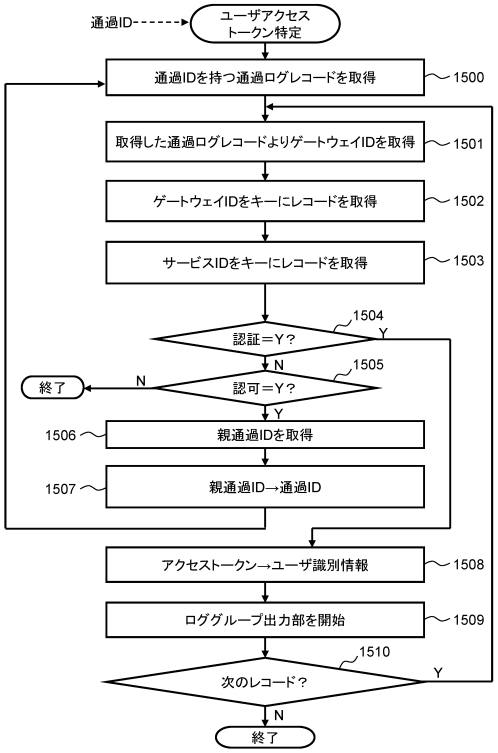
【図１４】

図 14



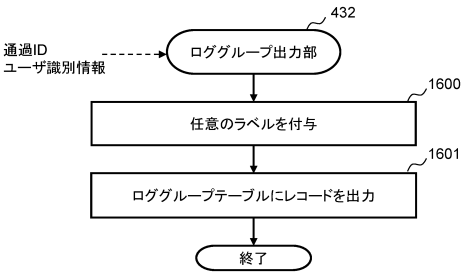
【図１５】

図 15



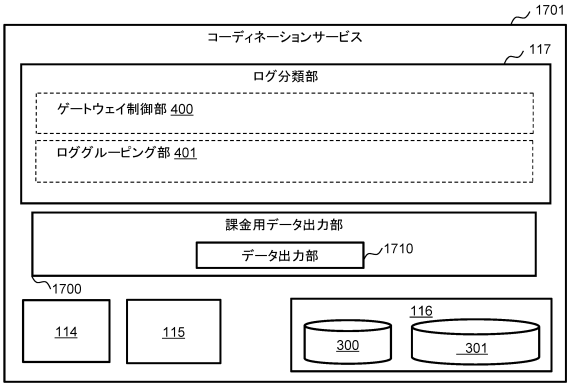
【図１６】

図 16



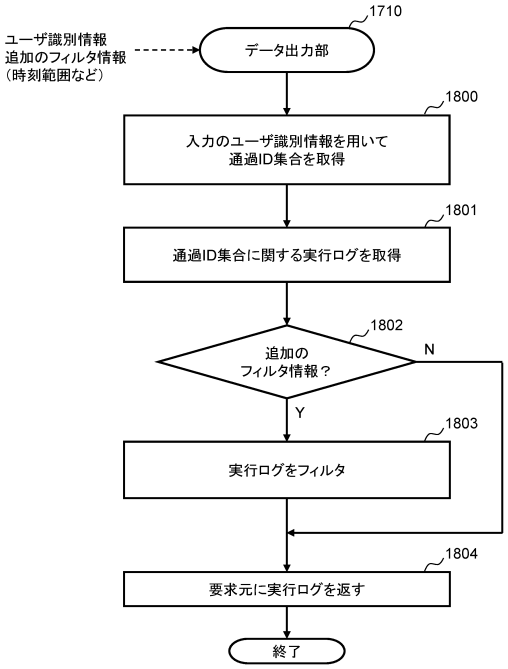
【図１７】

図 17



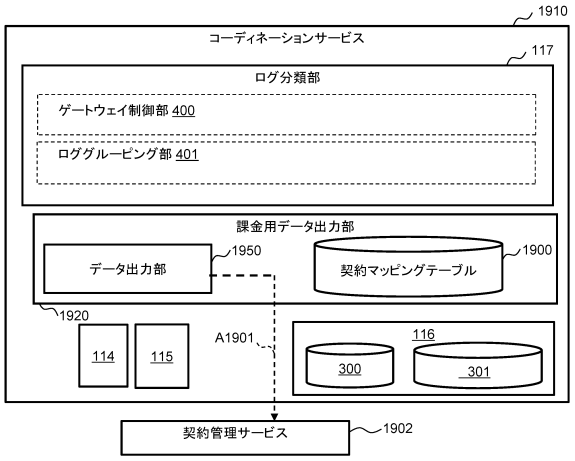
【図１８】

図 18



【図１９】

図 19



【図２０】

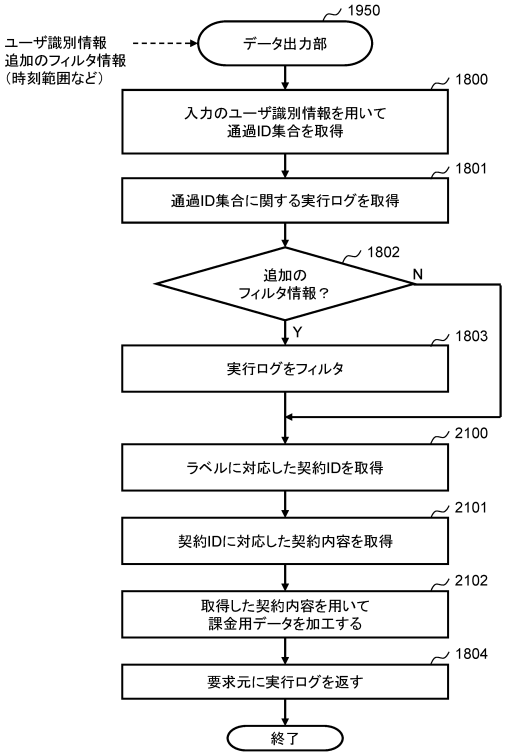
図 20

1900

契約関連マッピングテーブル	
2000	2001
契約ID	ラベル
backend-svc-a	Group1

【図２１】

図 21


1950
ユーザ識別情報
追加のフィルタ情報
（時刻範囲など）
データ出力部
1800
入力のユーザ識別情報を用いて
通過ID集合を取得
1801
通過ID集合に関する実行ログを取得
1802
追加の
フィルタ情報？
N
Y
1803
実行ログをフィルタ
2100
ラベルに対応した契約IDを取得
2101
契約IDに対応した契約内容を取得
2102
取得した契約内容を用いて
課金用データを加工する
1804
要求元に実行ログを返す
終了

フロントページの続き

(56)参考文献 特開２００２－１１６９２８（ＪＰ，Ａ）
特開２０１３－０１１９９５（ＪＰ，Ａ）
特開２０１４－０７５０８４（ＪＰ，Ａ）
特開２０１７－１９９１４５（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １１／０７
Ｇ０６Ｆ １１／２８－１１／３６
Ｇ０６Ｆ ２１／００－２１／８８
Ｇ０６Ｑ １０／００－９９／００