

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年11月28日(28.11.2019)



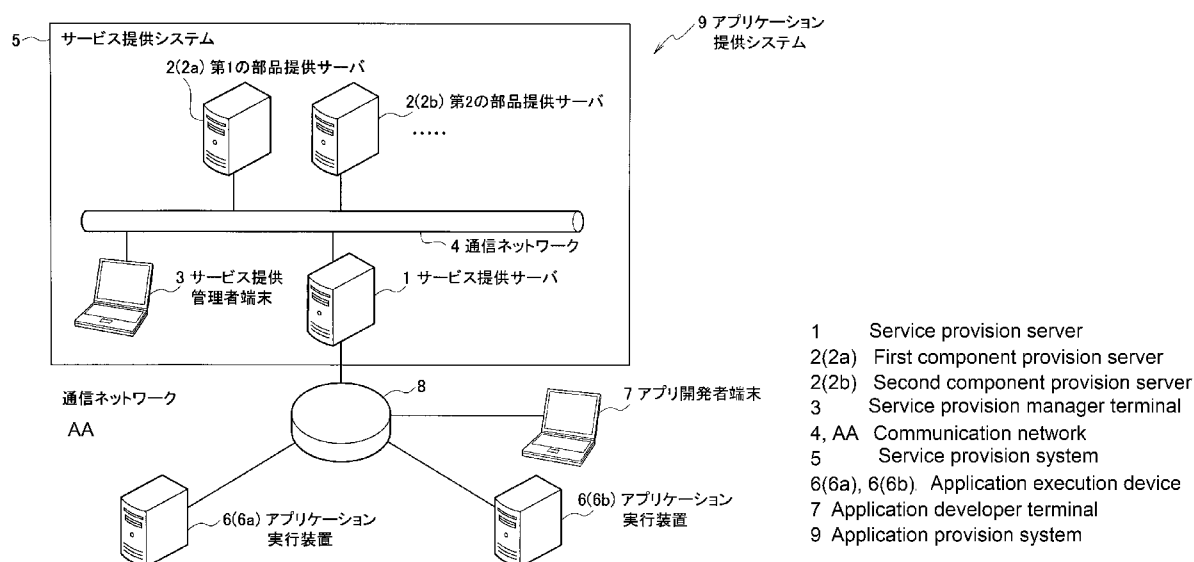
(10) 国際公開番号

WO 2019/225474 A1

- (51) 国際特許分類:
H04L 9/14 (2006.01) *G06F 21/60* (2013.01)
G06F 9/445 (2018.01)
- (21) 国際出願番号: PCT/JP2019/019516
- (22) 国際出願日: 2019年5月16日(16.05.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2018-096765 2018年5月21日(21.05.2018) JP
- (71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).
- (72) 発明者: 木村 昌史 (KIMURA Masashi); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT知的財産センタ内 Tokyo (JP).
- (74) 代理人: 三好 秀和, 外 (MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門1丁目2番8号 虎ノ門琴平タワー Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

(54) Title: SERVICE PROVISION SYSTEM, SERVICE PROVISION SERVER, SERVICE PROVISION METHOD, AND SERVICE PROVISION PROGRAM

(54) 発明の名称: サービス提供システム、サービス提供サーバ、サービス提供方法およびサービス提供プログラム



(57) Abstract: A service provision server 1 is provided with; an encryption object API designation unit 36 which receives an instruction to encrypt a mashup API; an encryption object item notification unit 37 which generates encryption object item data E and notifies a component provision server 2 thereof; and an API processing unit 38 which receives a processing request for the mashup API from an application execution device 6, and causes the component provision server 2 to execute a plurality of APIs specified by the mashup API in a predetermined processing order. The component provision server 2

QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第21条(3))

is provided with an API processing unit 123 which receives a processing request for an API from the service provision server 1, processes the API, and generates a processing response by encrypting, among output items of the processed API, an output item designated as an encryption object by the encryption object item data E.

(57) 要約: サービス提供サーバ1は、マッシュアップAPIについて暗号化するとの指示を受信する暗号対象API指定部36と、暗号対象項目データEを生成して、部品提供サーバ2に通知する暗号対象項目通知部37と、アプリケーション実行装置6からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIを所定の処理順序で、部品提供サーバ2に実行させるAPI処理部38を備える、部品提供サーバ2は、サービス提供サーバ1からAPIの処理リクエストを受信して、APIを処理し、処理したAPIの出力項目のうち、暗号対象項目データEで暗号化対象として指定された出力項目を暗号化して処理レスポンスを生成するAPI処理部123を備える。

明 細 書

発明の名称：

サービス提供システム、サービス提供サーバ、サービス提供方法およびサービス提供プログラム

技術分野

[0001] 本発明は、アプリケーションを実行するアプリケーション実行装置から、複数のAPIとAPIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システム、サービス提供サーバ、サービス提供方法およびサービス提供プログラムに関する。

背景技術

[0002] 一般的に、アプリケーションの処理の一部を、部品提供サーバが担うシステムが普及している。部品提供サーバは、イネーブラとも呼ばれ、少なくとも一つのアプリケーションに、特定の機能を提供する。

[0003] このようなシステムにおいて、アプリケーションは、複数の部品提供サーバを収容するサービス提供サーバに、必要な引数（パラメータ）を指定したAPIの処理リクエストを送信する。サービス提供サーバは、送信された処理リクエストに従って、APIを実行する部品提供サーバに、アプリケーションから送信された必要な引数を送信し、その処理結果を、部品提供サーバから受信して、アプリケーションに返す。

[0004] またアプリケーションの一つの処理リクエストに従って、複数のAPIを処理する場合もある。このようにマッシュアップされたAPIは、マッシュアップAPIと称される。マッシュアップAPIは、実行されるAPIの種類および順序などが、予めアプリケーション開発者とサービス提供サーバとの間で定義される。

[0005] またアプリケーションが送信または受信するデータの秘匿化が必要になる場合がある。例えば特許文献1に記載のシステムにおいて、アプリケーションは、予め指定された暗号化キーを用いてAPIのパラメータを暗号化して

部品提供サーバに送信する。さらに部品提供サーバは、予め指定された暗号化キーを用いて処理結果を暗号化して、アプリケーションに送信する。なお特許文献１は、マッシュアップＡＰＩではなく、アプリケーションが、単一のＡＰＩを呼び出す場合の処理を開示する。

先行技術文献

特許文献

[0006] 特許文献１：特開２０１８－２９２４１号公報

発明の概要

発明が解決しようとする課題

[0007] しかしながら、複数のＡＰＩ処理するマッシュアップＡＰＩについて秘匿化するに際し、特許文献１に記載の方法を用いることができない場合がある。

[0008] 例えば、マッシュアップＡＰＩにおいて複数のＡＰＩを所定の処理順序で実行するに際し、先に処理されるＡＰＩの出力項目が、後に処理されるＡＰＩの入力項目となる場合がある。各ＡＰＩの出力項目を一律に暗号化すると、マッシュアップＡＰＩを適切に処理できない場合がある。

[0009] 従って本発明の目的は、複数のＡＰＩ処理するマッシュアップＡＰＩについて適切に秘匿化するサービス提供システム、サービス提供サーバ、サービス提供方法およびサービス提供プログラムを提供することである。

課題を解決するための手段

[0010] 上記課題を解決するために、本発明の第１の特徴は、アプリケーションを実行するアプリケーション実行装置から、複数のＡＰＩとＡＰＩの処理順序を特定するマッシュアップＡＰＩの処理リクエストを受信して処理するサービス提供システムに関する。本発明の第１の特徴に係るサービス提供システムは、アプリケーション実行装置からマッシュアップＡＰＩの処理リクエストを受信し、マッシュアップＡＰＩで特定される複数のＡＰＩを処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、

[0011] サービス提供サーバからAPIの処理リクエストを受信して、APIを処理し、サービス提供サーバに処理レスポンスを返す部品提供サーバを備える。サービス提供サーバは、マッシュアップAPIについて暗号化するとの指示を受信する暗号対象API指定部と、マッシュアップAPIが特定する複数のAPIとAPIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定する暗号対象項目データを生成して、部品提供サーバに通知する暗号対象項目通知部と、アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIを処理順序で、部品提供サーバに実行させ、部品提供サーバからの処理レスポンスに基づいて、アプリケーション実行装置に送信する処理レスポンスを作成して送信するAPI処理部を備える。部品提供サーバは、サービス提供サーバから暗号対象項目データを取得する暗号対象項目取得部と、サービス提供サーバからAPIの処理リクエストを受信して、APIを処理し、処理したAPIの出力項目のうち、暗号対象項目データで暗号化対象として指定された出力項目を暗号化して処理レスポンスを生成して、サービス提供サーバに処理レスポンスを返すAPI処理部を備える。

[0012] サービス提供サーバは、アプリケーション実行装置が復号可能な暗号データを生成する暗号鍵データを取得する暗号鍵取得部と、暗号鍵データを部品提供サーバに提供する暗号鍵提供部をさらに備え、部品提供サーバのAPI処理部は、暗号鍵データで、暗号化対象として指定された出力項目を暗号化しても良い。

[0013] 本発明の第2の特徴は、アプリケーションを実行するアプリケーション実行装置から、複数のAPIとAPIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システムに用いられるサービス提供サーバに関する。本発明の第2の特徴においてサービス提供システムは、アプリケーション実行装置からマッシュアップAPIの処理リ

クエストを受信し、マッシュアップAPIで特定される複数のAPIを処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、サービス提供サーバからAPIの処理リクエストを受信して、APIを処理し、サービス提供サーバに処理レスポンスを返す部品提供サーバを備える。サービス提供サーバは、マッシュアップAPIについて暗号化するとの指示を受信する暗号対象API指定部と、マッシュアップAPIが特定する複数のAPIとAPIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定する暗号対象項目データを生成して、部品提供サーバに通知する暗号対象項目通知部と、アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIを処理順序で、部品提供サーバに実行させ、部品提供サーバからの処理レスポンスに基づいて、アプリケーション実行装置に送信する処理レスポンスを作成して送信するAPI処理部を備える。

[0014] 本発明の第3の特徴は、アプリケーションを実行するアプリケーション実行装置から、複数のAPIとAPIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システムに用いられるサービス提供方法に関する。本発明の第3の特徴に係るサービス提供方法においてサービス提供システムは、アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIを処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、サービス提供サーバからAPIの処理リクエストを受信して、APIを処理し、サービス提供サーバに処理レスポンスを返す部品提供サーバを備える。サービス提供方法は、サービス提供サーバが、マッシュアップAPIについて暗号化するとの指示を受信するステップと、サービス提供サーバが、マッシュアップAPIが特定する複数のAPIとAPIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化

対象として指定する暗号対象項目データを生成して、部品提供サーバに通知するステップと、部品提供サーバが、サービス提供サーバから暗号対象項目データを取得するステップと、サービス提供サーバが、アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIを処理順序で、部品提供サーバに実行させるステップと、部品提供サーバが、サービス提供サーバからAPIの処理リクエストを受信して、APIを処理し、処理したAPIの出力項目のうち、暗号対象項目データで暗号化対象として指定された出力項目を暗号化して処理レスポンスを生成して、サービス提供サーバに処理レスポンスを返すステップと、サービス提供サーバが、部品提供サーバからの処理レスポンスに基づいて、アプリケーション実行装置に送信する処理レスポンスを作成して送信するステップを備える。

[0015] 本発明の第4の特徴は、コンピュータに、本発明の第2の特徴に記載のサービス提供サーバとして機能させるためのサービス提供プログラムに関する。

発明の効果

[0016] 本発明によれば、複数のAPI処理するマッシュアップAPIについて適切に秘匿化するサービス提供システム、サービス提供サーバ、サービス提供方法およびサービス提供プログラムを提供することができる。

図面の簡単な説明

[0017] [図1]本発明の実施の形態に係るアプリケーション提供システムのシステム構成図である。

[図2]本発明の実施の形態に係るアプリケーション提供システムにおけるサービス提供方法を説明するシーケンス図である。

[図3]本発明の実施の形態に係るサービス提供方法において、アプリケーション開発者が、アプリケーションで用いるマッシュアップAPIと暗号化の有無を指定する画面の一例である。

[図4]本発明の実施の形態に係るサービス提供システムにおいて、マッシュア

ップAPIを構成する各APIによる出力項目の暗号化の有無の一例を説明する図である。

[図5]図4に示す例において用いられるマッシュアップAPIの仕様を説明する図である。

[図6]本発明の実施の形態に係るサービス提供システムにおいて、マッシュアップAPIを実行する際に送受信されるデータの一例を説明する図である（その1）。

[図7]本発明の実施の形態に係るサービス提供システムにおいて、マッシュアップAPIを実行する際に送受信されるデータの一例を説明する図である（その2）。

[図8]本発明の実施の形態に係るサービス提供サーバのハードウェアおよび機能ブロックを説明する図である。

[図9]本発明の実施の形態に係るサービス提供サーバの暗号対象APIデータのデータ構造とデータの一例を説明する図である。

[図10]本発明の実施の形態に係るサービス提供サーバの暗号対象項目データのデータ構造とデータの一例を説明する図である。

[図11]本発明の実施の形態に係るサービス提供サーバの暗号対象項目データをJSON形式で記載した場合のデータの一例を説明する図である。

[図12]本発明の実施の形態に係る部品提供サーバのハードウェアおよび機能ブロックを説明する図である。

発明を実施するための形態

[0018] 次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

[0019] （アプリケーション提供システム）

図1を参照して、本発明の実施の形態に係るサービス提供サーバ1が用いられるアプリケーション提供システム9を説明する。

[0020] アプリケーション提供システム9は、サービス提供サーバ1を備えるサー

ビス提供システム5、第1のアプリケーション実行装置6a、第2のアプリケーション実行装置6bおよびアプリ開発者端末7を備える。サービス提供システム5、第1のアプリケーション実行装置6a、第2のアプリケーション実行装置6bおよびアプリ開発者端末7は、インターネット等の通信ネットワーク8により相互に通信可能に接続される。

[0021] 本発明の実施の形態において第1のアプリケーション実行装置6aおよび第2のアプリケーション実行装置6bを区別しない場合、単にアプリケーション実行装置6と記載する場合がある。図1には2つのアプリケーション実行装置6を記載するが、アプリケーション提供システム9は、1つ以上のアプリケーション実行装置6を備えれば良い。

[0022] アプリケーション実行装置6は、マッシュアップAPIを含むAPIの処理をサービス提供システム5にリクエストして、その処理結果を受信するアプリケーションを実行する端末である。アプリケーション実行装置6の処理結果は、さらに他の端末（図示せず）に提供される場合もある。

[0023] アプリ開発者端末7は、アプリケーション実行装置6で実行されるアプリケーションを開発する開発者が用いる端末である。アプリ開発者端末7は、アプリケーション実行装置6に実行させるアプリケーションの開発時に、マッシュアップAPIの定義を、サービス提供システム5との間で決定する。その際、アプリ開発者端末7は、サービス提供システム5がこれらのAPIを用いるアプリケーションを識別するための識別子（APLキーまたはAPL_ID）を、サービス提供システム5から取得する。アプリケーションがAPIをサービス提供システム5に送信する際、アプリケーションを識別するための識別子が設定される。

[0024] サービス提供システム5は、アプリケーションを実行するアプリケーション実行装置6から、複数のAPIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理する。サービス提供システム5は、サービス提供サーバ1、第1の部品提供サーバ2a、第2の部品提供サーバ2bおよびサービス提供管理者端末3を備える。サービス提供サーバ1、第1の

部品提供サーバ2 a、第2の部品提供サーバ2 bおよびサービス提供管理者端末3は、LAN (Local Area Network) などの通信ネットワーク4により相互に通信可能に接続される。

[0025] 本発明の実施の形態において第1の部品提供サーバ2 aおよび第2の部品提供サーバ2 bを区別しない場合、単に部品提供サーバ2と記載する場合がある。図1には2つの部品提供サーバ2を記載するが、本発明の実施の形態において、サービス提供システム5が一つのマッシュアップAPIを構成する複数のAPIを実行できればよく、部品提供サーバ2の数は問わない。

[0026] サービス提供サーバ1は、アプリケーション実行装置6から処理リクエストを受信し、処理リクエストに従って、サービス提供サーバ1が収容する部品提供サーバ2に、所定のAPIの処理を実行させる。サービス提供サーバ1は、部品提供サーバ2による処理結果を、アプリケーション実行装置6に返す。本発明の実施の形態に係るサービス提供サーバ1は特に、アプリケーション実行装置6からマッシュアップAPIの処理リクエストを受信し、マッシュアップAPIで特定される複数のAPIをこの処理順序で、部品提供サーバ2に実行させる。

[0027] サービス提供サーバ1はさらに、サービス提供管理者端末3およびアプリ開発者端末7からの指示に従って、アプリケーションで用いるAPIシナリオに従って、APIを作成し、マッシュアップAPIの識別子(APIキー)を定義する。サービス提供サーバ1は、アプリ開発者端末7に、サービス提供サーバ1がアプリケーションを識別するためのAPLキーを払い出す。また本発明の実施の形態においてサービス提供サーバ1は、アプリケーションの実行に先だって、アプリケーションで実行されるマッシュアップAPIについて、各部品提供サーバ2の出力項目のうち、暗号化すべき出力項目とその暗号化キーを、各部品提供サーバ2に通知する。

[0028] 部品提供サーバ2は、サービス提供サーバ1からAPIの処理リクエストを受信して、APIを処理し、サービス提供サーバ1に処理レスポンスを返す。本発明の実施の形態において部品提供サーバ2は、処理結果をサービス

提供サーバ1に送信する際、予めサービス提供サーバ1によって指定された出力項目を暗号化する。部品提供サーバ2は、1つのサーバで複数のAPIを実行しても良い。

[0029] サービス提供管理者端末3は、サービス提供システム5を管理する管理者の端末である。サービス提供管理者端末3は、マッシュアップAPIにおいて部品提供サーバ2が実行するAPIの組み合わせおよび処理順序等を記載したシナリオを準備し、サービス提供サーバ1に読み込ませる。

[0030] 図2を参照して、図1に示すサービス提供システム5におけるサービス提供方法を説明する。図2に示す処理は、所定のアプリケーション（Aアプリ）に関する処理を示す。ステップS1ないしステップS8は、アプリケーション実行装置6がこのアプリケーションを実行する前に行う前処理である。ステップS11ないしステップS16は、アプリケーション実行装置6がこのアプリケーションを実行する際の処理である。

[0031] まずステップS1においてサービス提供管理者端末3は、シナリオをサービス提供サーバ1に読み込ませる。このシナリオは、マッシュアップAPIについて、APIを特定するデータと、そのAPIの処理順序を指定する。またシナリオにおいて、マッシュアップAPIの識別子（マッシュアップAPIキー）が特定される。

[0032] ステップS2においてサービス提供サーバ1は、ステップS1で送信されたシナリオに従って、APIとAPIの呼出順序を解析し、マッシュアップAPIを定義する。

[0033] ステップS3においてアプリ開発者端末7は、サービス提供サーバ1に対して、アプリケーションで用いるAPIと、アプリケーションで用いるAPIのうち出力を暗号化するAPIを指定する。例えばサービス提供サーバ1は、アプリ開発者端末7に図3に示す開発者ポータル画面を表示する。開発者ポータル画面は、アプリ開発者に、Aアプリにおいて用いるマッシュアップAPIの種別と、そのマッシュアップAPIの出力を暗号するか否かを指定させる。図3に示す例では、Aアプリでは、apiMashupAと、apiMashupCの

各マッシュアップAPIを使うことと、apiMashupAの出力を暗号化し、apiMashupCの出力を暗号化しないことが指定されている。サービス提供サーバ1は、ステップS3で指定された内容を保持する。なお図3に示す例では、マッシュアップAPIのみ記載しているが、マッシュアップされていない単一のAPIも表示しても良い。

[0034] ステップS4においてアプリ開発者端末7は、ステップS3で指定されたアプリケーションで復号可能な暗号鍵を、サービス提供サーバ1に送信する。サービス提供サーバ1は、アプリケーションの識別子と、暗号鍵を対応づけて保持する。さらにステップS5においてサービス提供サーバ1は、ステップS3で指定されたアプリケーションをサービス提供サーバ1が識別するためのAPLキーを払い出し、アプリ開発者端末7に送信する。

[0035] ステップS6においてサービス提供サーバ1は、アプリケーションで用いられるマッシュアップAPIの識別子について、ステップS3における指定に従って、暗号対象APIデータ12と、暗号対象項目データEを生成する。暗号対象APIデータ12は、サービス提供サーバ1が扱うマッシュアップAPIのうち、暗号化が必要となるマッシュアップAPIの識別子（マッシュアップAPIキー）と、そのAPIを呼び出すアプリケーションの識別子（APLキー）を対応づけるデータである。暗号対象項目データEは、マッシュアップAPIを構成する各APIを実行する部品提供サーバ2において、APIの処理結果において、暗号化すべき出力項目を特定するデータである。暗号対象項目データEは、部品提供サーバ2毎に生成される。

[0036] ステップS7およびステップS8においてサービス提供サーバ1は、ステップS4で受信した暗号鍵と、ステップS6で生成した暗号対象項目データEを、各部品提供サーバ2に送信する。

[0037] ステップS11においてアプリケーション実行装置6は、アプリケーション実行中に、マッシュアップAPIの処理リクエストをサービス提供サーバ1に送信する。この処理リクエストには、マッシュアップAPIの識別子（マッシュアップAPIキー）と、このアプリケーションの識別子（APLキ

一)を含む。またここでリクエストされるマッシュアップAPIは、暗号化対象であるとする。

[0038] サービス提供サーバ1は、アプリケーション実行装置6から処理リクエストを受信すると、マッシュアップAPIキーで特定されるマッシュアップAPIを構成する各APIを、部品提供サーバ2に実行させる。マッシュアップAPIを、第1の部品提供サーバ2aおよび第2の部品提供サーバ2bの順で、それぞれAPIを実行させる場合、ステップS12においてサービス提供サーバ1は、第1の部品提供サーバ2aに処理リクエストを送信して、ステップS13において処理レスポンスを受信する。ステップS14においてサービス提供サーバ1は、第2の部品提供サーバ2bに処理リクエストを送信して、ステップS15において処理レスポンスを受信する。

[0039] 本発明の実施の形態において処理レスポンスは、複数の出力項目により構成される。複数の出力項目のうち、後続の処理の入力になる出力項目については平文で出力され、後続の処理の入力にならない出力項目については、ステップS4で受信した暗号鍵で暗号化されて出力される。例えばステップS13でサービス提供サーバ1が受信する処理レスポンスを構成する出力項目のうち、ステップS14で送信する処理リクエストに含まれる出力項目について、第1の部品提供サーバ2aは、暗号化せずに平文で処理レスポンスに含ませる。一方、ステップS13でサービス提供サーバ1が受信する処理レスポンスを構成する出力項目のうち、ステップS14で送信する処理リクエストに含まれない出力項目について、第1の部品提供サーバ2aは、暗号化して処理レスポンスに含ませる。また、最後のAPIを実行する第2の部品提供サーバ2bは、APIの各出力項目を暗号化して処理レスポンスに含ませる。

[0040] サービス提供サーバ1は、ステップS13およびステップS15で受信した処理レスポンスに基づいて、ステップS16において、ステップS11で受信した処理リクエストに対する処理レスポンスを送信する。この処理レスポンスに含まれる各出力項目は、部品提供サーバ2によって暗号化される。

[0041] このように本発明の実施の形態に係るサービス提供システム5は、マッシュアップAPIにおいて複数のAPIを実行する場合でも、各出力項目について適切に暗号化した処理レスポンスを生成し、アプリケーション実行装置6に返すことができる。

[0042] 図4ないし図7を参照して、サービス提供サーバ1と部品提供サーバ2とのデータ送受信を詳述する。ここでは、所定のアプリケーションで呼び出された、暗号化対象のマッシュアップAPI（APIキー：“apiMashupA”）について説明する。

[0043] APIキー“apiMashupA”のマッシュアップAPIの引数は、図4に示すように、key_aおよびkey_bの各項目であり、戻り値は、attr_a、attr_b、attr_cおよびattr_dの各項目である。アプリケーション実行装置6は、key_aおよびkey_bには、それぞれvalue_aおよびvalue_bの値を設定して、マッシュアップAPIの実行をリクエストする。

[0044] このマッシュアップAPIは、図4および図5に示すように、3つのAPIにより構成される。（1）のAPIは、“GET /api/v1/enabler1APIa”で、（2）のAPIは、“POST /api/v1/enabler1APIb”で、（3）のAPIは、“POST /api/v1/enabler2APIa”である。apiMashupAは、（1）、（2）および（3）の順にAPIを実行する。（1）および（2）のAPIは、第1の部品提供サーバ2aが提供するAPIで、（3）のAPIは、第2の部品提供サーバ2bが提供するAPIである。

[0045] まず、APIキー“apiMashupA”のマッシュアップAPIについて、引数key_aに値value_aが設定され、引数key_bに値value_bが設定されてリクエストされた場合に、各APIが処理する場合を説明する。

[0046] （1）のAPIは、GET関数である。（1）のAPIの引数として設定される値はない。第1の部品提供サーバ2aが（1）のAPIを実行すると、（1）のAPIの戻り値として、attr_cの値value_cと、attr_dの値value_dが設定される。

[0047] （2）のAPIは、POST関数である。（2）のAPIの引数として、key_a

の値value_aと、key_cの値value_cが設定される。key_aの値value_aは、apiMashupAPIの引数である。key_cの値value_cは、(1)のAPIの戻り値のattr_cの値value_cである。第1の部品提供サーバ2aが(2)のAPIを実行すると、(2)のAPIの戻り値として、attr_aの値value_a' と、attr_cの値value_c' が設定される。

[0048] (3)のAPIは、POST関数である。(3)のAPIの引数として、key_aの値value_a' と、key_bの値value_bと、key_dの値value_dが設定される。key_aの値value_a' は、(2)の戻り値であるattr_aの値value_a' である。key_bの値value_bは、apiMashupAPIの引数である。key_dの値value_dは、(1)のAPIの戻り値であるattr_dの値value_dである。第2の部品提供サーバ2bが(3)のAPIを実行すると、(3)のAPIの戻り値として、attr_aの値value_a' '、attr_bの値value_b' およびattr_dの値value_d' が設定される。

[0049] APIキー”apiMashupA”のマッシュアップAPIの戻り値は、図4に示すように、attr_a、attr_b、attr_cおよびattr_dの各項目である。サービス提供サーバ1は、(1)ないし(3)の各APIの処理の結果、attr_a、attr_b、attr_cおよびattr_dの各項目に、それぞれ値value_a' '、value_b'、value_c' およびvalue_d' を設定して、アプリケーション実行装置6に返す。

[0050] このようなマッシュアップAPIについて本発明の実施の形態に係るサービス提供サーバ1は、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外とするとともに、後続のAPIで参照される出力項目は暗号化対象とする。なお、図4等において、下線が付された値は、暗号化されていることを示し、下線が付されていない値は、暗号化されていないことを示す。

[0051] 図4に示す例において、(1)のAPIの戻り値value_cは、後続の(2)のAPIの引数となるので、(1)のAPIは、value_cを暗号化しないで平文のまま出力する。同様に(1)のAPIの戻り値value_dは、後続の(3)

のAPIの引数となるので、(1)のAPIは、value_dを暗号化しないで平文のまま出力する。

[0052] (2)のAPIの返り値value_a'は、後続の(3)のAPIの引数となるので、(2)のAPIは、value_a'を暗号化しないで平文のまま出力する。

(2)のAPIの返り値value_c'は、後続のAPIで用いられないので、(2)のAPIは、value_c'を暗号化して出力する。

[0053] (3)のAPIの返り値value_a'、value_b'およびvalue_d'はそれぞれ、後続のAPIがなく後続のAPIで用いられないので、(3)のAPIは、value_a'、value_b'およびvalue_d'をそれぞれ暗号化して出力する。

[0054] 図6および図7を参照して、図4に示すデータ例におけるデータのシーケンス図の一例を示す。図6および図7において、下線が付された値は、暗号化されていることを示し、下線が付されていない値は、暗号化されていないことを示す。

[0055] まずステップS51においてアプリケーション実行装置6は、データD1を送信する。このデータD1は、リクエストラインに示すように、APIキー”apiMashupA”のマッシュアップAPIの実行をリクエストするもので、ボディに示すように、引数key_aに値value_aが設定され、引数key_bに値value_bが設定される。またデータD1のリクエストヘッダには、このマッシュアップAPIの送信元のアプリケーションを識別するAPLキー(APL_ID)が設定される。なおサービス提供サーバ1が送受信する各データの各レスポンスヘッダにおいて、APLキー(APL_ID)が設定される。

[0056] サービス提供サーバ1は、データD1を受信すると、APIキー”apiMashupA”のマッシュアップAPIに従って、各部品提供サーバ2に処理をさせる。

[0057] まずステップS52においてサービス提供サーバ1は、GET /api/v1/enabler1APIaの処理を要求するデータD2を、第1の部品提供サーバ2aに送信する。データD2において、引数として設定される値はない。

- [0058] 第1の部品提供サーバ2 aは、データD 2に従ってGET /api/v1/enabler1APIaの処理を行い、ステップS 5 3においてその結果のデータD 3をサービス提供サーバ1に返す。データD 3において、戻り値として、attr_cの値value_cが設定され、attr_dの値value_dが設定される。この戻り値の値value_cおよびvalue_dは、後続のAPIの入力になるためいずれも暗号化されない。
- [0059] ステップS 5 4においてサービス提供サーバ1は、POST /api/v1/enabler1APIbの処理を要求するデータD 4を、第1の部品提供サーバ2 aに送信する。データD 4において、key_aの値value_aと、key_cの値value_cが設定される。
- [0060] 第1の部品提供サーバ2 aは、データD 4に従ってPOST /api/v1/enabler1APIbの処理を行い、ステップS 5 5においてその結果のデータD 5をサービス提供サーバ1に返す。データD 5において、戻り値として、attr_aの値value_a' およびattr_cの値value_c' が設定される。ここでvalue_a' は、後続のAPIで用いられるので暗号化されないが、value_c' は、後続のAPIで用いられないので暗号化される。
- [0061] ステップS 5 6においてサービス提供サーバ1は、POST /api/v1/enabler2APIaの処理を要求するデータD 6を、第2の部品提供サーバ2 bに送信する。データD 6において、key_aの値value_a' と、key_bの値value_bと、key_dの値value_dが設定される。
- [0062] 第2の部品提供サーバ2 bは、データD 6に従ってPOST /api/v1/enabler2APIaの処理を行い、ステップS 5 7においてその結果のデータD 7をサービス提供サーバ1に返す。データD 7において、戻り値として、attr_aの値value_a' '、attr_bの値value_b' およびattr_dの値value_d' が設定される。ここでvalue_a' '、value_b' およびvalue_d' は、後続のAPIで用いられないので暗号化される。
- [0063] サービス提供サーバ1が、ステップS 5 2ないしステップS 5 7において、マッシュアップAPIを実行した結果、ステップS 5 8においてデータD 8をアプリケーション実行装置6に送信する。データD 8において、戻り値

としてattr_aの値value_a'、attr_bの値value_b'、attr_cの値value_c'およびattr_dの値value_d'の各項目が設定される。また各value_a'、value_b'、value_c'およびvalue_d'は、それぞれ暗号化される。

[0064] (サービス提供サーバ)

図8を参照して、本発明の実施の形態に係るサービス提供サーバ1を説明する。サービス提供サーバ1は、一般的な機能とともに、図4ないし図7を参照して説明したように、各部品提供サーバ2が所与の出力項目を暗号化できるように制御する機能を実装する。

[0065] サービス提供サーバ1は、記憶装置10、処理装置30および通信制御装置50を備える一般的なコンピュータである。一般的なコンピュータがサービス提供プログラムを実行することにより、図8に示す機能を実現する。

[0066] 記憶装置10は、ROM (Read Only Memory)、RAM (Random access memory)、ハードディスク等であって、処理装置30が処理を実行するための入力データ、出力データおよび中間データなどの各種データを記憶する。処理装置30は、CPU (Central Processing Unit) であって、記憶装置10に記憶されたデータを読み書きしたり、通信制御装置50とデータを入出力したりして、サービス提供サーバ1における処理を実行する。通信制御装置50は、部品提供サーバ2、サービス提供管理者端末3、アプリケーション実行装置6およびアプリ開発者端末7等と接続するためのインタフェースである。

[0067] 記憶装置10は、暗号鍵データP、API定義データ11、暗号対象APIデータ12および暗号対象項目データEを記憶する。

[0068] 暗号鍵データPは、アプリケーション実行装置6が復号可能な暗号データを生成するための暗号鍵のデータである。暗号鍵データPは、公開鍵暗号の場合、アプリケーション実行装置6が有する秘密鍵とペアの暗号鍵であり、共通鍵暗号の場合、アプリケーション実行装置6が有する暗号鍵と同じ暗号鍵である。暗号鍵データPは、アプリケーション実行装置6が復号可能な暗号データを生成するものであれば、どのようなものでも良い。

- [0069] API定義データ11は、サービス提供サーバ1が、マッシュアップAPIを処理するために用いられるデータである。例えば、マッシュアップAPIで処理されるAPIの識別子、引数、戻り値、そのAPIを収容する部品提供サーバ2の識別子等の情報、処理順序等を含む。
- [0070] 暗号対象APIデータ12は、アプリケーションの識別子と、そのアプリケーションが呼び出すマッシュアップAPIについて、暗号化するか否かを示すデータである。暗号対象APIデータ12は、図9に示すように、マッシュアップAPI識別子、マッシュアップAPI名、アプリ識別子、暗号化フラグおよびシナリオ等を対応づけたデータである。暗号化フラグがTrueに設定されたマッシュアップAPI識別子およびアプリ識別子について、そのアプリから、そのマッシュアップAPIが呼び出された際に、サービス提供サーバ1は、そのマッシュアップAPIの出力項目について暗号化されたデータを設定してアプリケーション実行装置6に返す。
- [0071] 暗号対象項目データEは、マッシュアップAPIが特定する複数のAPIとAPIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定するデータである。暗号対象項目データEは、部品提供サーバ2毎に生成され、その部品提供サーバ2が実行するAPIの出力項目について、暗号化するか否かを指定する。暗号化対象項目データEは、アプリケーションから呼び出されるマッシュアップAPIの各出力項目が暗号化されてアプリケーションに返されるように設定される。
- [0072] 暗号対象項目データEは、例えば図10に示すデータであって、アプリ識別子、マッシュアップAPI識別子、APIおよび出力項目の暗号化を対応づける。図10(a)は、第1の部品提供サーバ2a向けの暗号対象項目データEaであって、図10(b)は、第2の部品提供サーバ2b向けの暗号対象項目データEbである。
- [0073] 第1の部品提供サーバ2a向けの暗号対象項目データEaの1行目は、アプリ識別子APL_Aから、マッシュアップAPI識別子apiMashupAが呼び出され、e

nablerAPIaを実行した際、その出力項目のattr_cおよびattr_dはともに暗号化せずに出力することを示す。2行目は、アプリ識別子APL_Aから、マッシュアップAPI識別子apiMashupAが呼び出され、enablerAPIbを実行した際、その出力項目のattr_aは暗号化せずに出力し、attr_cは暗号化して出力することを示す。一つのマッシュアップAPIにおいて、同一のAPIが複数回呼び出される場合、さらに、呼び出される回数を指定するカラムを設けて、回数ごとに出力項目の暗号化の可否を指定しても良い。

[0074] 暗号対象項目データEは、例えば図11に示すようにJSON形式で記載されたデータであっても良い。図11(a)は、第1の部品提供サーバ2a向けの暗号対象項目データEaであって、図11(b)は、第2の部品提供サーバ2b向けの暗号対象項目データEbである。暗号対象項目データEは、部品提供サーバ2が読み取り可能なデータ形式で生成される。

[0075] 処理装置30は、暗号鍵処理部31、シナリオ処理部34、API処理部38を備える。

[0076] 暗号鍵処理部31は、暗号鍵取得部32と暗号鍵提供部33を備える。暗号鍵取得部32は、アプリ開発者端末7から、アプリケーション実行装置6が復号可能な暗号データを生成する暗号鍵データPを取得する。取得した暗号鍵データPは、記憶装置10に記憶される。暗号鍵提供部33は、暗号鍵データPを部品提供サーバ2に提供する。暗号鍵提供部33は、少なくとも、暗号化が必要なAPIを実行する部品提供サーバ2に、暗号鍵データPを提供する。

[0077] シナリオ処理部34は、シナリオ解析部35、暗号対象API指定部36および暗号対象項目通知部37を備える。

[0078] シナリオ解析部35は、サービス提供管理者端末3から入力されたシナリオを解析して、API定義データ11を生成する。

[0079] 暗号対象API指定部36は、アプリ開発者端末7からマッシュアップAPIについて暗号化するとの指示を受信する。暗号対象API指定部36は、例えば図3に示す画面をアプリ開発者端末7に表示して、マッシュアップ

A P I で用いる A P I と、その A P I の出力項目を暗号化するか否かの指示を受信する。暗号対象 A P I 指定部 3 6 は、アプリ開発者端末 7 からの指示に従って、暗号対象 A P I データ 1 2 を生成し、記憶装置 1 0 に記憶する。

[0080] 暗号対象項目通知部 3 7 は、マッシュアップ A P I が特定する複数の A P I と A P I の処理順序に従って、各 A P I の出力項目のうち、後続の A P I で参照される出力項目は暗号化対象外として指定し、後続の A P I で参照される出力項目は暗号化対象として指定する暗号対象項目データ E を生成する。暗号対象項目通知部 3 7 はさらに、生成した暗号対象項目データ E を、部品提供サーバ 2 に通知する。暗号対象項目通知部 3 7 は、図 4 等を参照して説明したように、マッシュアップ A P I で特定される複数の A P I を所定の順序で各部品提供サーバ 2 に処理させる際、各部品提供サーバ 2 で暗号化する出力項目を指定して、暗号対象項目データ E を生成する。

[0081] A P I 処理部 3 8 は、アプリケーション実行装置 6 からマッシュアップ A P I の処理リクエストを受信し、マッシュアップ A P I で特定される複数の A P I を所定の処理順序で、部品提供サーバ 2 に実行させ、部品提供サーバ 2 からの処理レスポンスに基づいて、アプリケーション実行装置 6 に送信する処理レスポンスを作成して送信する。A P I 処理部 3 8 は、マッシュアップ A P I の A P I を部品提供サーバ 2 に実行させる際、A P I 定義データ 1 1 を参照して、その A P I を収容する部品提供サーバ、処理順序、引数等の情報を特定する。

[0082] 暗号対象のマッシュアップ A P I の処理レスポンスに含まれる出力項目は、それぞれ部品提供サーバ 2 によって暗号化されるので、A P I 処理部 3 8 は、暗号化された出力項目を含む処理レスポンスを、アプリケーション実行装置 6 に送信することができる。

[0083] (部品提供サーバ)

部品提供サーバ 2 は、記憶装置 1 1 0、処理装置 1 2 0 および通信制御装置 1 3 0 を備える一般的なコンピュータである。一般的なコンピュータが部品提供プログラムを実行することにより、図 1 2 に示す機能を実現する。

- [0084] 記憶装置 110 は、ROM (Read Only Memory)、RAM (Random access memory)、ハードディスク等であって、処理装置 120 が処理を実行するための入力データ、出力データおよび中間データなどの各種データを記憶する。処理装置 120 は、CPU (Central Processing Unit) であって、記憶装置 110 に記憶されたデータを読み書きしたり、通信制御装置 130 とデータを入出力したりして、サービス提供サーバ 1 における処理を実行する。通信制御装置 130 は、サービス提供サーバ 1 等と接続するためのインターフェースである。
- [0085] 記憶装置 110 は、暗号対象項目データ E および暗号鍵データ P を記憶する。暗号対象項目データ E および暗号鍵データ P は、サービス提供サーバ 1 から提供されるデータであって、図 8 等を参照して説明した通りである。
- [0086] 処理装置 120 は、暗号対象項目取得部 121、暗号鍵取得部 122 および API 処理部 123 を備える。
- [0087] 暗号対象項目取得部 121 は、サービス提供サーバ 1 から暗号対象項目データ E を取得して、記憶装置 110 に記憶する。暗号対象項目データ E は、部品提供サーバ 2 が処理する API、この API に紐付くマッシュアップ API およびアプリケーションに対して、API の出力項目のうち、暗号化の必要な出力項目を特定するものである。
- [0088] 暗号鍵取得部 122 は、サービス提供サーバ 1 から暗号鍵データ P を取得して、記憶装置 110 に記憶する。暗号鍵データ P は、部品提供サーバ 2 が処理する API に紐付くアプリケーション毎に用意される。
- [0089] API 処理部 123 は、サービス提供サーバ 1 から API の処理リクエストを受信して、API を処理し、処理レスポンスを生成して、サービス提供サーバ 1 に処理レスポンスを返す。
- [0090] 本発明の実施の形態において API 処理部 123 は、暗号化処理部 124 を備える。暗号化処理部 124 は、API 処理部 123 が処理した API の出力項目のうち、暗号対象項目データ E で暗号化対象として指定された出力項目を、暗号鍵データ P で暗号化する。API 処理部 123 は、暗号対象項

目データEで暗号化対象として指定された項目のデータを暗号化し、それ以外の項目のデータを暗号化することなく平文のまま、処理レスポンスを生成する。

[0091] このような本発明の実施の形態に係るサービス提供システム5によれば、複数のAPIを紐づけたマッシュアップAPIについても、その出力を適切に暗号化して、秘匿化することが可能になる。またマッシュアップAPIについて適切に暗号化することが可能であるので、アプリケーションから、秘匿化が必要なマッシュアップAPIを呼び出すことが可能になり、APIの呼出回数を削減することができる。

[0092] (その他の実施の形態)

上記のように、本発明の実施の形態によって記載したが、この開示の一部をなす論述および図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例および運用技術が明らかとなる。

[0093] 例えば、本発明の実施の形態に記載したサービス提供サーバは、図8に示すように一つのハードウェア上に構成されても良いし、その機能や処理数に応じて複数のハードウェア上に構成されても良い。

[0094] 本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。従って、本発明の技術的範囲は上記の説明から妥当な請求の範囲に係る発明特定事項によってのみ定められるものである。

符号の説明

- [0095]
- 1 サービス提供サーバ
 - 2 部品提供サーバ
 - 3 サービス提供管理者端末
 - 4、8 通信ネットワーク
 - 5 サービス提供システム
 - 6 アプリケーション実行装置
 - 7 アプリ開発者端末

9 アプリケーション提供システム

10、110 記憶装置

11 API定義データ

12 暗号対象APIデータ

30、120 処理装置

31 暗号鍵処理部

32、122 暗号鍵取得部

33 暗号鍵提供部

34 シナリオ処理部

35 シナリオ解析部

36 暗号対象API指定部

37 暗号対象項目通知部

38 API処理部

50、130 通信制御装置

121 暗号対象項目取得部

124 暗号化処理部

E 暗号対象項目データ

P 暗号鍵データ

請求の範囲

[請求項1]

アプリケーションを実行するアプリケーション実行装置から、複数のAPIと前記APIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システムであって、

前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、

前記サービス提供サーバからAPIの処理リクエストを受信して、前記APIを処理し、前記サービス提供サーバに処理レスポンスを返す部品提供サーバを備え、

前記サービス提供サーバは、

前記マッシュアップAPIについて暗号化すると の指示を受信する暗号対象API指定部と、

前記マッシュアップAPIが特定する複数のAPIと前記APIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定する暗号対象項目データを生成して、前記部品提供サーバに通知する暗号対象項目通知部と、

前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、前記部品提供サーバに実行させ、前記部品提供サーバからの処理レスポンスに基づいて、前記アプリケーション実行装置に送信する処理レスポンスを作成して送信するAPI処理部を備え、

前記部品提供サーバは、

前記サービス提供サーバから暗号対象項目データを取得する暗号対象項目取得部と、

前記サービス提供サーバからAPIの処理リクエストを受信して、前記APIを処理し、処理した前記APIの出力項目のうち、前記暗号対象項目データで暗号化対象として指定された出力項目を暗号化して前記処理レスポンスを生成して、前記サービス提供サーバに前記処理レスポンスを返すAPI処理部を備える

ことを特徴とするサービス提供システム。

[請求項2]

前記サービス提供サーバは、

前記アプリケーション実行装置が復号可能な暗号データを生成する暗号鍵データを取得する暗号鍵取得部と、

前記暗号鍵データを前記部品提供サーバに提供する暗号鍵提供部をさらに備え、

前記部品提供サーバのAPI処理部は、前記暗号鍵データで、暗号化対象として指定された出力項目を暗号化する

ことを特徴とする請求項1に記載のサービス提供システム。

[請求項3]

アプリケーションを実行するアプリケーション実行装置から、複数のAPIと前記APIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システムに用いられるサービス提供サーバであって、

前記サービス提供システムは、

前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、

前記サービス提供サーバからAPIの処理リクエストを受信して、前記APIを処理し、前記サービス提供サーバに処理レスポンスを返す部品提供サーバを備え、

前記サービス提供サーバは、

前記マッシュアップAPIについて暗号化するとの指示を受信する

暗号対象API指定部と、

前記マッシュアップAPIが特定する複数のAPIと前記APIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定する暗号対象項目データを生成して、前記部品提供サーバに通知する暗号対象項目通知部と、

前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、前記部品提供サーバに実行させ、前記部品提供サーバからの処理レスポンスに基づいて、前記アプリケーション実行装置に送信する処理レスポンスを作成して送信するAPI処理部を備える

ことを特徴とするサービス提供サーバ。

[請求項4]

アプリケーションを実行するアプリケーション実行装置から、複数のAPIと前記APIの処理順序を特定するマッシュアップAPIの処理リクエストを受信して処理するサービス提供システムに用いられるサービス提供方法であって、

前記サービス提供システムは、

前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、後記部品提供サーバに実行させるサービス提供サーバと、

前記サービス提供サーバからAPIの処理リクエストを受信して、前記APIを処理し、前記サービス提供サーバに処理レスポンスを返す部品提供サーバを備え、

前記サービス提供方法は、

前記サービス提供サーバが、前記マッシュアップAPIについて暗号化するとの指示を受信するステップと、

前記サービス提供サーバが、前記マッシュアップAPIが特定する複数のAPIと前記APIの処理順序に従って、各APIの出力項目のうち、後続のAPIで参照される出力項目は暗号化対象外として指定し、後続のAPIで参照される出力項目は暗号化対象として指定する暗号対象項目データを生成して、前記部品提供サーバに通知するステップと、

前記部品提供サーバが、前記サービス提供サーバから暗号対象項目データを取得するステップと、

前記サービス提供サーバが、前記アプリケーション実行装置からマッシュアップAPIの処理リクエストを受信し、前記マッシュアップAPIで特定される複数のAPIを前記処理順序で、前記部品提供サーバに実行させるステップと、

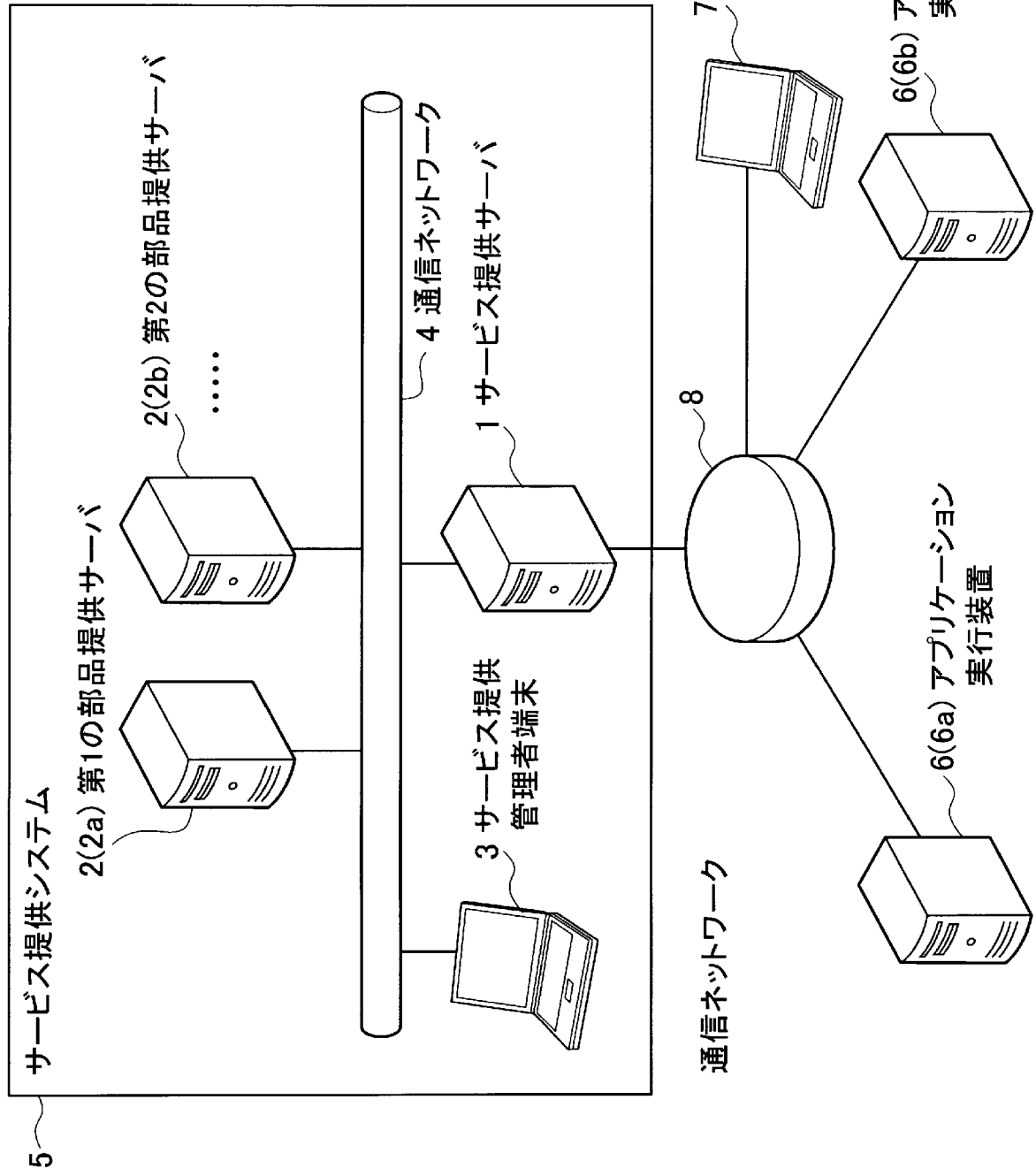
前記部品提供サーバが、前記サービス提供サーバからAPIの処理リクエストを受信して、前記APIを処理し、処理した前記APIの出力項目のうち、前記暗号対象項目データで暗号化対象として指定された出力項目を暗号化して前記処理レスポンスを生成して、前記サービス提供サーバに前記処理レスポンスを返すステップと、

前記サービス提供サーバが、前記部品提供サーバからの処理レスポンスに基づいて、前記アプリケーション実行装置に送信する処理レスポンスを作成して送信するステップ

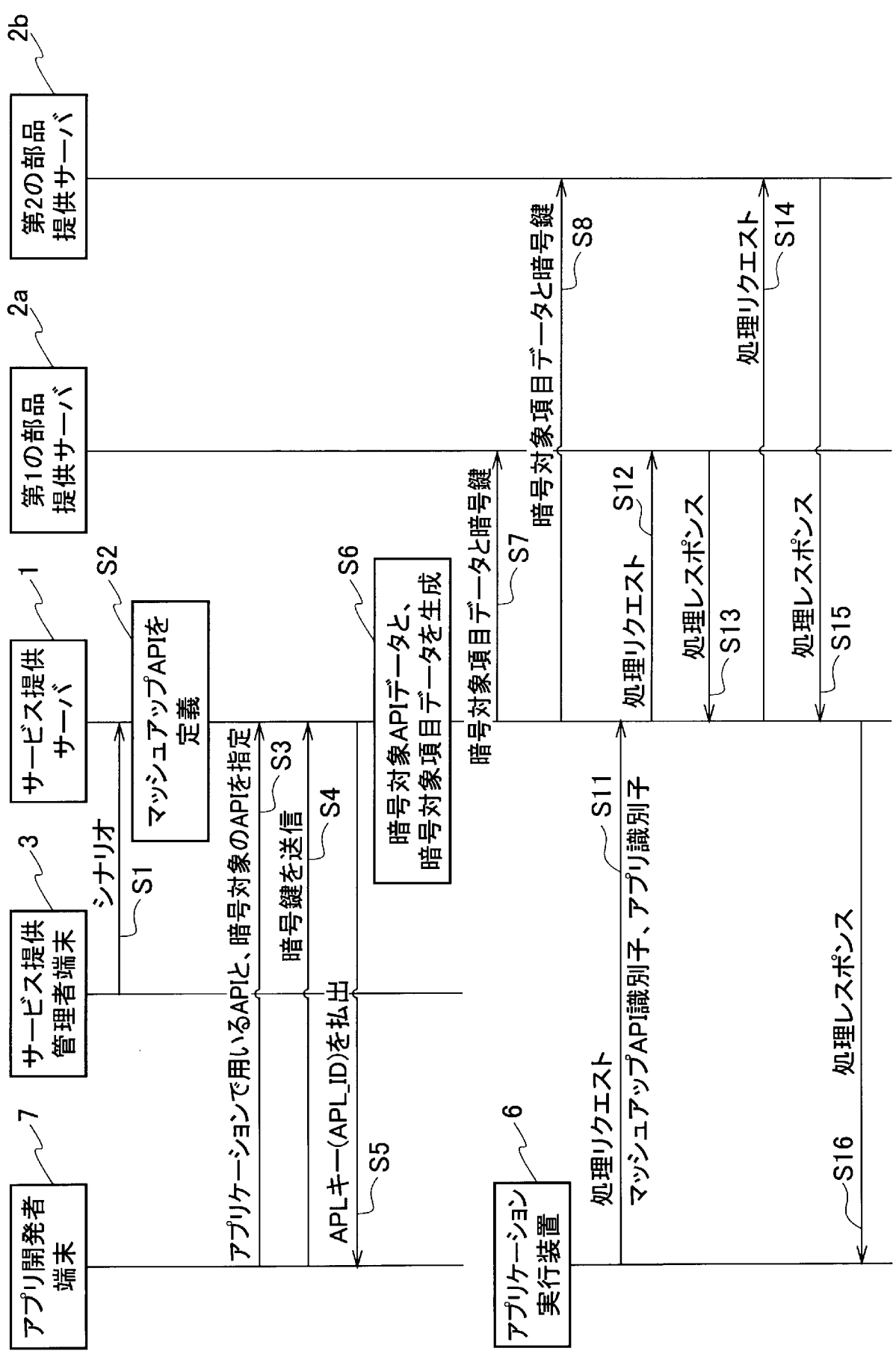
を備えることを特徴とするサービス提供方法。

[請求項5] コンピュータを、請求項3に記載のサービス提供サーバとして機能させるためのサービス提供プログラム。

[図1]

9 アプリケーション
提供システム

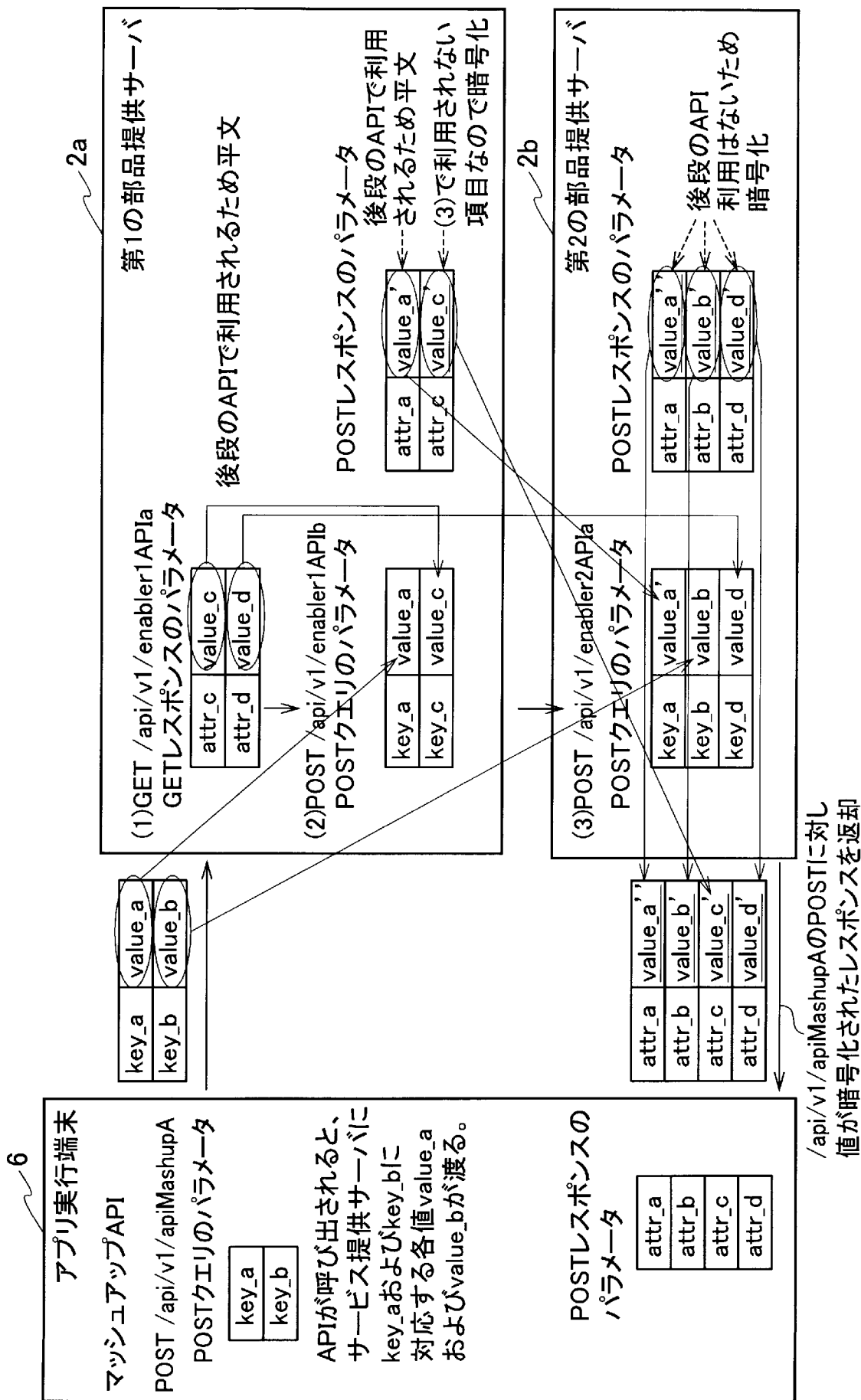
[図2]



[図3]

開発者ポータル	
Aアプリ	
apiMashupA	
☒	use
☒	encrypted
apiMashupB	
☐	use
☐	encrypted
apiMashupC	
☒	use
☐	encrypted

[図4]



[図5]

API仕様(apiMashupA)

(1) GET /api/v1/enabler1APIa

引数(json)

なし

返り値(json)

attr_c

attr_d

(2) POST /api/v1/enabler1APIb

引数(json)

key_a

key_c

返り値(json)

attr_a

attr_c

(3) POST /api/v1/enabler2APIa

引数(json)

key_a

key_b

key_d

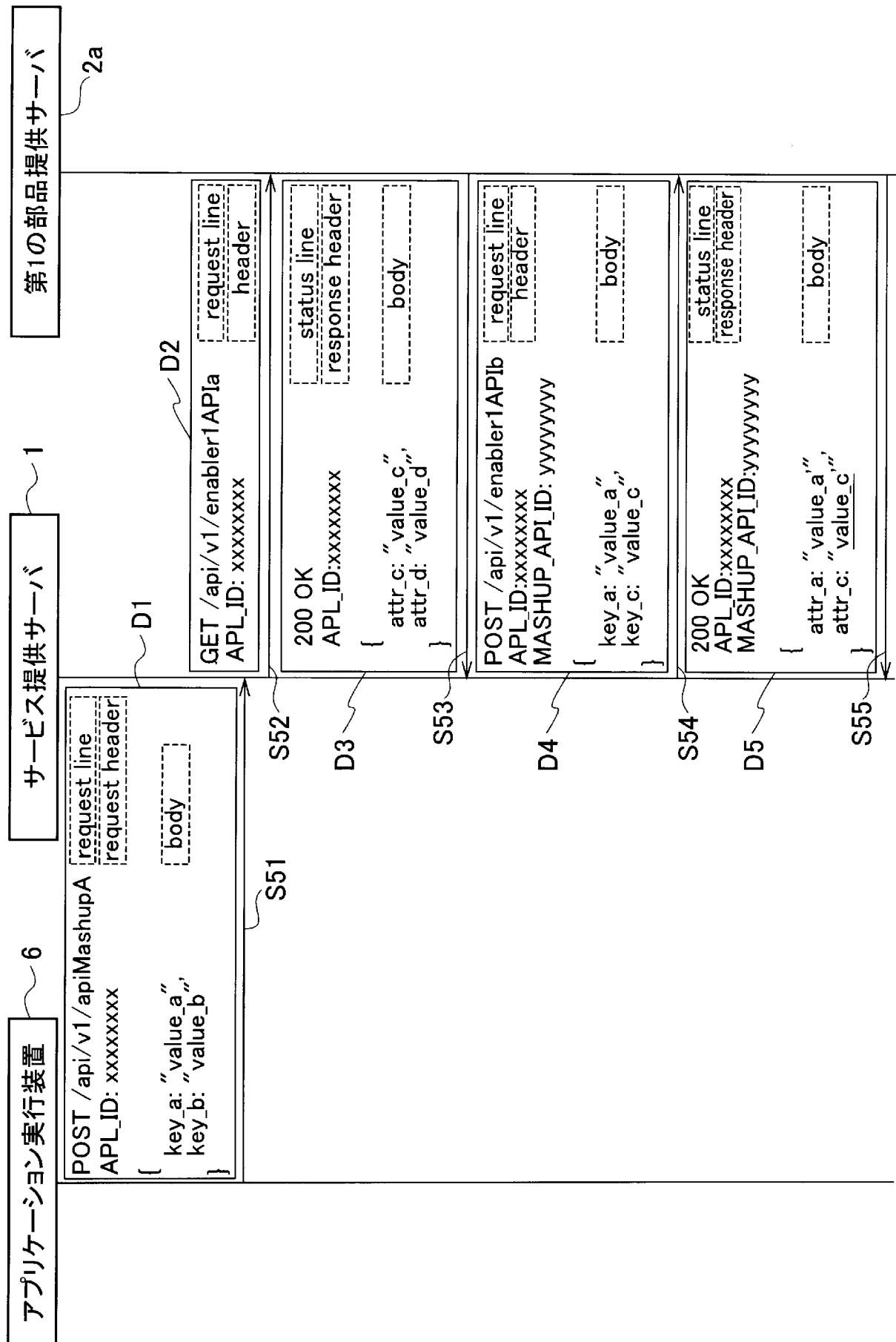
返り値(json)

attr_a

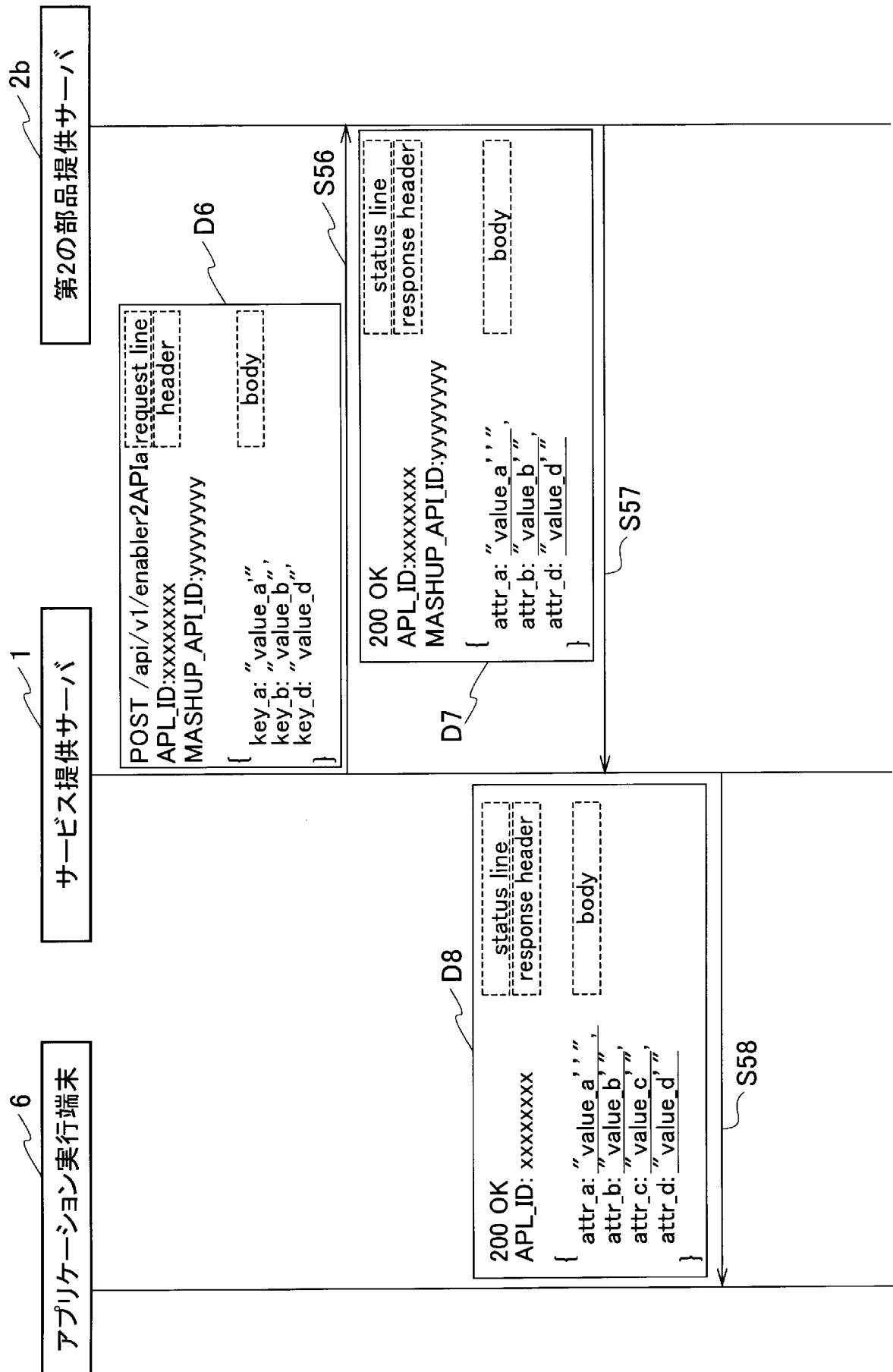
attr_b

attr_d

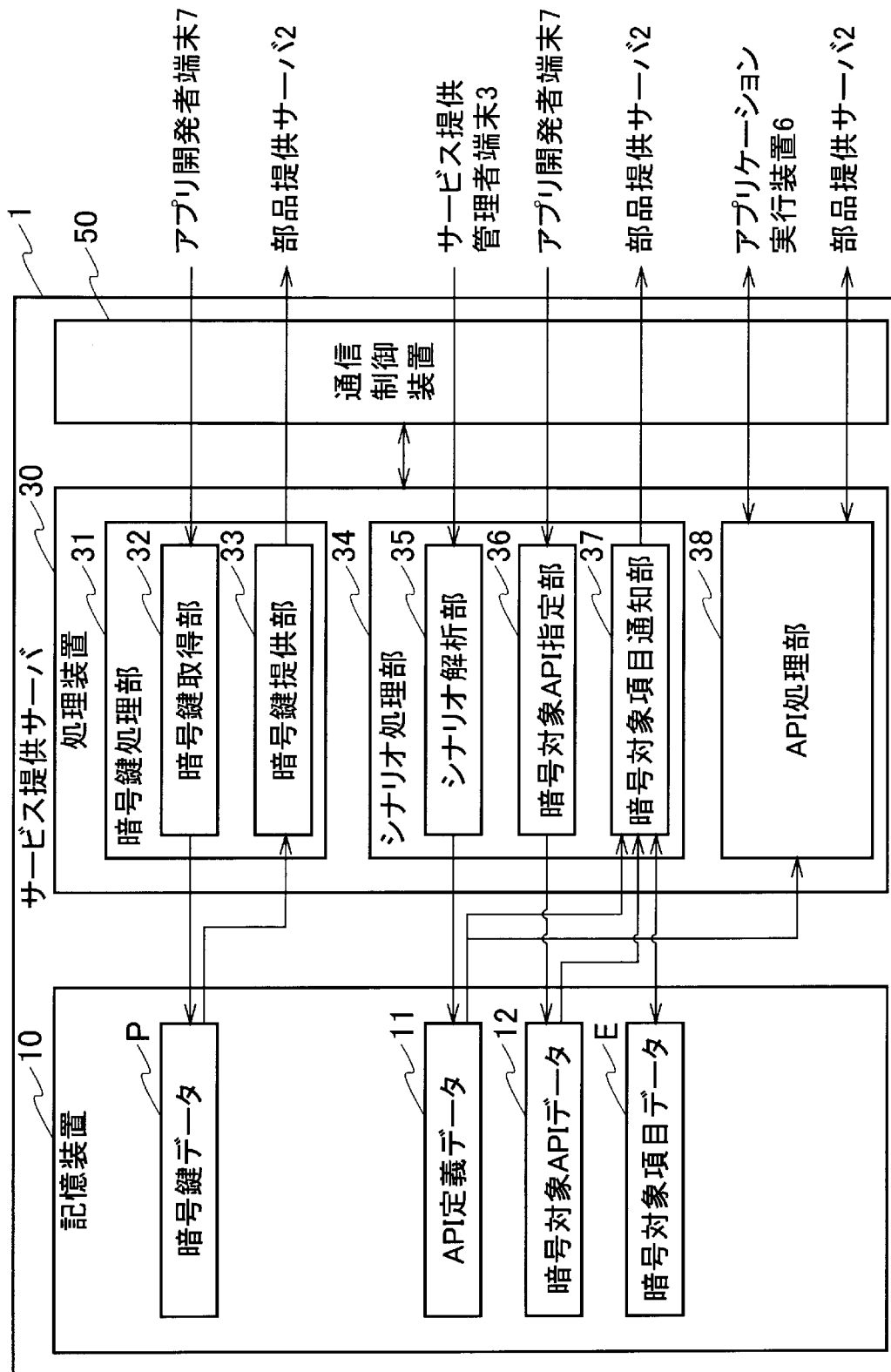
[図6]



[図7]



[図8]



[図9]

13 暗号対象APIデータ

マッシュアップAPI識別子 (MASHUP_API_ID)	マッシュアップAPI名 (MASHUP_API_NAME)	アプリ識別子 (APL_ID)	暗号化フラグ (encrypt)	シナリオ (scenario)
apiMashupA	...	APL_A	True	...
apiMashupC	...	APL_A	False	...
...	...	...	...	...

[図10]

(a)

E (Ea) 暗号対象項目データ(第1の部品提供サーバ)

アプリ識別子 (APL_ID)	マッシュアップAPI識別子 (MASHUP_API_ID)	API(targetAPI)	出力項目の暗号化 (encrypt)
APL_A	apiMashupA	enabler1APIa	"attr_c": false, "attr_d": false
APL_A	apiMashupA	enabler1APIb	"attr_a": false, "attr_c": true

(b)

E (Eb) 暗号対象項目データ(第2の部品提供サーバ)

アプリ識別子 (APL_ID)	マッシュアップAPI識別子 (MASHUP_API_ID)	API(targetAPI)	出力項目の暗号化 (encrypt)
APL_A	apiMashupA	enabler2APIa	"attr_a": true, "attr_b": true, "attr_d": true

[図11]

(a)

E(Ea) 暗号対象項目データ
(第1の部品提供サーバ)

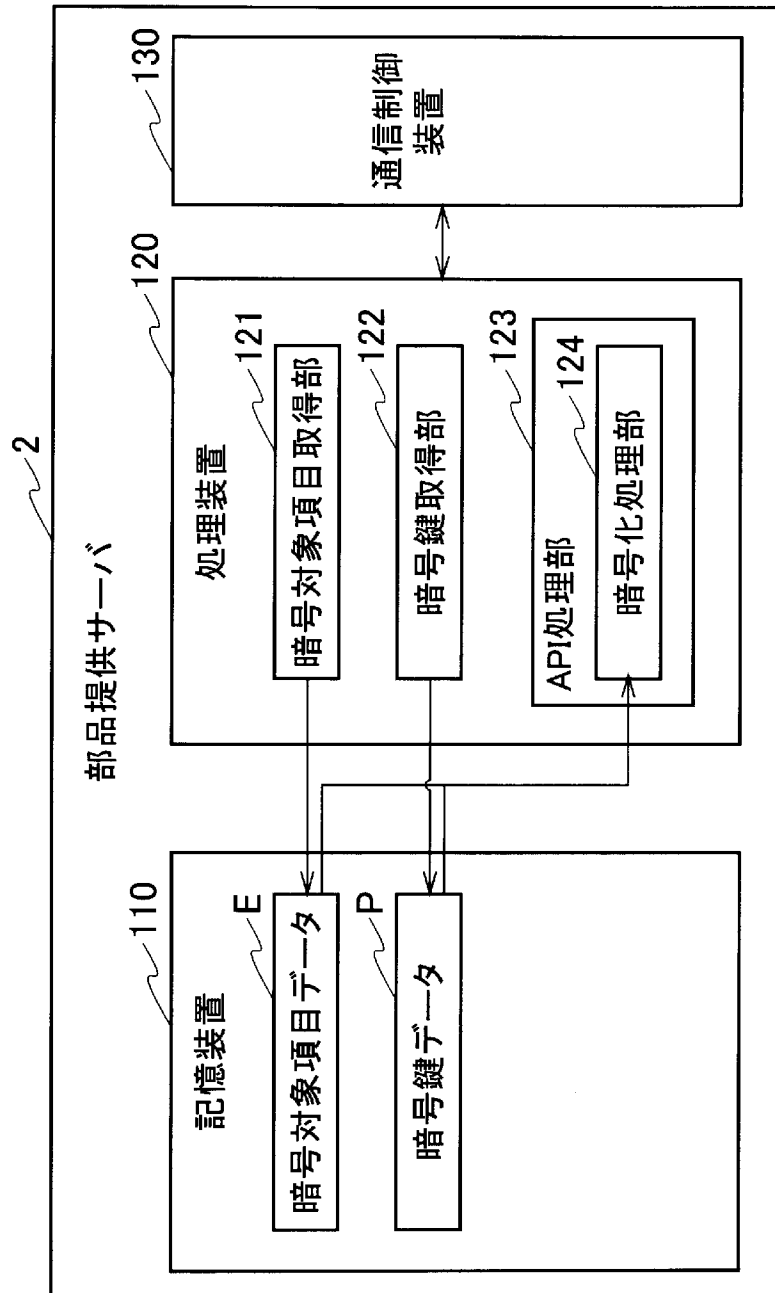
```
{
  "APL_ID": "xxxxxxx",
  "MASHUP_API_ID": "apiMashupA",
  {
    "targetAPI": "enabler1APIa",
    "encrypt": [
      {
        "attr_c": false,
        "attr_d": false
      }
    ],
    "targetAPI": "enabler1APIb",
    "encrypt": [
      {
        "attr_a": false,
        "attr_c": true
      }
    ]
  }
}
```

(b)

E(Eb) 暗号対象項目データ
(第2の部品提供サーバ)

```
{
  "APL_ID": "xxxxxxx",
  "MASHUP_API_ID": "apiMashupB",
  {
    "targetAPI": "enabler2APIa",
    "encrypt": [
      {
        "attr_a": true,
        "attr_b": true,
        "attr_d": true
      }
    ]
  }
}
```

[図12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/019516

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L9/14 (2006.01) i, G06F9/445 (2018.01) i, G06F21/60 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. H04L9/14, G06F9/445, G06F21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-145506 A (CANON INC.) 25 July 2013 & US 2013/0185809 A1	1-5
A	JP 2011-211382 A (HITACHI, LTD.) 20 October 2011 (Family: none)	1-5



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

04.07.2019

Date of mailing of the international search report

16.07.2019

Name and mailing address of the ISA/

Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/019516

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	AtsushiNakatsugawa, 複数サービスをマッシュアップする際に注意したいこと, NTT COMMUNICATIONS CORPORATION [online], 17 March 2017, [retrieved on 04 July 2019], Internet: <URL:https://developer.ntt.com/ja/blog/d2b60d5d-963e-4f98-b695-96e744c4e361>, 「データを疎結合にする」の項, non-official translation (Things to be aware of when mashing up multiple services, item of "making data loosely coupled")	1-5

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/14(2006.01)i, G06F9/445(2018.01)i, G06F21/60(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/14, G06F9/445, G06F21/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で利用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2013-145506 A（キヤノン株式会社）2013.07.25, & US 2013/0185809 A1	1-5
A	JP 2011-211382 A（株式会社日立製作所）2011.10.20,（ファミリーなし）	1-5

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

04.07.2019

国際調査報告の発送日

16.07.2019

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

吉田 歩

電話番号 03-3581-1101 内線 3546

5 S

1206

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	AtsushiNakatsugawa, 複数サービスをマッシュアップする際に注意 したいこと, NTT Communications Corporation [online], 2017.03.17 [検索日 2019.07.04], インターネット:<URL: https://developer.ntt.com/ja/blog/d2b60d5d-963e-4f98-b695-96 e744c4e361>, 「データを疎結合にする」の項	1-5