

(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
2011年4月7日(07.04.2011)



PCT



(10) 国際公開番号
WO 2011/040192 A1

- (51) 国際特許分類:
G06F 21/20 (2006.01) G06Q 50/00 (2006.01)
G06F 9/46 (2006.01)
- (21) 国際出願番号: PCT/JP2010/065375
- (22) 国際出願日: 2010年9月8日(08.09.2010)
- (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 2009-229104 2009年9月30日(30.09.2009) JP
- (71) 出願人 (米国を除く全ての指定国について): ブラザー工業株式会社 (BROTHER KOGYO KABUSHIKI KAISHA) [JP/JP]; 〒4678561 愛知県名古屋市中瑞穂区苗代町15番1号 Aichi (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 佐々木建太 (SASAKI Kenta) [JP/JP]; 〒4678561 愛知県名古屋市中瑞穂区苗代町15番1号 ブラザー工業株式会社内 Aichi (JP).

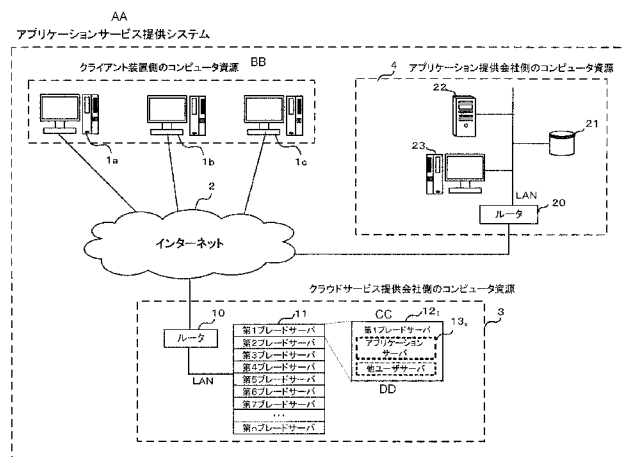
- (74) 代理人: 武藤勝典(MUTO Katsunori); 〒4910901 愛知県一宮市北浦町28番地5 Aichi (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: VIRTUAL MACHINE, VIRTUAL MACHINE PROGRAM, APPLICATION SERVICE PROVISION SYSTEM AND METHOD FOR PROVIDING APPLICATION SERVICE

(54) 発明の名称: 仮想マシン、仮想マシンのプログラム、アプリケーションサービス提供システム及びアプリケーションサービス提供方法

[図1]



- 2 Internet
3 Cloud service provision company computer resources
4 Application provision company computer resources
10, 20 Router
11 First blade server
Second blade server
Third blade server
Fourth blade server
Fifth blade server
Sixth blade server
Seventh blade server
nth blade server
13_x Application server
AA Application service provider system
BB Client device computer resources
CC First blade server
DD Other user servers

(57) Abstract: Provided is a virtual machine intended to promote the use of cloud services while an application provision company carries out security countermeasures for confidential corporate information. When the virtual machine (13_x) receives a request from a client device (1a-1c) via the internet (2), the virtual machine (13_x) determines whether or not processing is required on the basis of confidential corporate information, including information about the user using the client device (1a-1c). If the virtual machine (13_x) determines, on the basis of confidential corporate information, that processing is required, the virtual machine (13_x) securely communicates with a corporate database server connected to the corporate network and, on the basis of confidential corporate information, performs processing on the request from the client device (1a-1c). However, if the virtual machine (13_x) determines, on the basis of confidential corporate information, that processing is not required, the virtual machine (13_x) carries out the process stipulated in the request from the client device (1a-1c).

(57) 要約:

[続葉有]

WO 2011/040192 A1



添付公開書類:

— 国際調査報告（条約第 21 条(3)）

企業内秘匿情報のセキュリティ対策をアプリケーション提供会社側で行わせつつ、クラウドサービスの利用の促進を図ることができる仮想マシン等を提供すること。仮想マシン 13_xは、インターネット 2 を介してクライアント装置 1 a ~ 1 c からの要求を受け付けると、クライアント装置 1 a ~ 1 c を使用するユーザの情報を含む企業内秘匿情報に基づく処理が必要か否かを判定する。仮想マシン 13_xは、企業内秘匿情報に基づく処理が必要であると判定すると、企業内ネットワークに接続された企業内データベースサーバとの間でセキュアな通信を行って、企業内秘匿情報に基づきクライアント装置 1 a ~ 1 c からの要求に対する処理を行う。一方、企業内秘匿情報に基づく処理が必要ではないと判定すると、仮想マシン 13_xは、クライアント装置 1 a ~ 1 c からの要求に対する処理を実行する。

明 細 書

発明の名称：

仮想マシン、仮想マシンのプログラム、アプリケーションサービス提供システム及びアプリケーションサービス提供方法

技術分野

[0001] 本発明は、インターネットを介して接続されたサーバ上で動作する仮想マシン、その仮想マシンのプログラム、その仮想マシンを備えたアプリケーションサービス提供システム、及びそのアプリケーションサービス提供方法に関する。

背景技術

[0002] 従来、サーバコンピュータやデータベースなどのコンピュータ資源は、それらを使用する企業がそれぞれ自社で保有していた。しかし、ハードウェアやアプリケーションが複雑で高コストであり、また、コンピュータ資源を運用する専門の部門も必要となる。

[0003] そこで、インターネットを基本にした新しいコンピュータ資源の利用形態として、クラウド・コンピューティングというサービス形態（以下、「クラウドサービス」という）が注目されている。かかるクラウドサービスとしては、アマゾンが提供する「Elastic Compute Cloud (EC2)」が一例として挙げられる。

[0004] クラウドサービスでは、その利用者はコンピュータ資源の保有や管理を行う必要がない。クラウドサービスでは、利用料金を払うことでコンピュータ資源を利用することが可能となる。一方、クラウドサービス提供会社側では、1又は複数のサーバ上で利用者毎に仮想マシンを配置することで、サーバの利用効率や拡張性を向上させている。そのため、クラウドサービス提供会社は、比較的安価にコンピュータ資源をその利用者に提供することができる（例えば、特許文献1参照）。

[0005] このようにクラウドサービスでは、その利用者がコンピュータ資源を導入

する必要がないことから、導入コストや運用コストが軽減される。また、拡張性などにも優れているため、今後、ますます利用者が増加していくものと考えられる。

[0006] 特に、クラウドサービス提供会社から仮想マシンをレンタルして、クライアントにアプリケーションを提供するといった利用形態が増えるものと予測される。

[0007] インターネット経由でアプリケーションをクライアントに提供しようとする企業（以下、「アプリケーション提供会社」とする）は、クラウドサービスの利用者として、クラウドサービス提供会社からアプリケーションのプラットフォームとなる仮想マシンをレンタルする。そして、アプリケーション提供会社は、この仮想マシン上でアプリケーションを実行させる。アプリケーション提供会社は、アプリケーションのプラットフォームを保有及び管理する必要がないため、導入コスト及び運用コストが低減され、コスト的なハードルが下がる。そのため、アプリケーション提供会社は、アプリケーションサービスをクライアントに提供しやすくなる。

先行技術文献

特許文献

[0008] 特許文献1：特表2004-503011号公報

発明の概要

発明が解決しようとする課題

[0009] アプリケーション提供会社が提供するアプリケーションで使用するデータには、アプリケーション提供会社の内の機密情報やクライアント（すなわち、アプリケーション提供会社が提供するアプリケーションサービスのクライアント）の個人情報などの重要な情報（以下、「企業内秘匿情報」という）が含まれる。

[0010] しかし、上記クラウドサービスでは、アプリケーション提供会社は、提供するアプリケーションで使用するデータをクラウドサービス提供会社に預

けることになる。すなわち、アプリケーション提供会社は、提供するアプリケーションで使用されるデータのセキュリティ対策をクラウドサービス提供会社側に行わせることになる。

[0011] しかしながら、同一のサーバ上でアプリケーション提供会社の仮想マシンのみならず他の利用者の仮想マシンが配置された場合、サーバプログラムの不具合をついたハッキングなどにより、他の利用者等により企業内秘匿情報が盗まれるリスクがある。また、サーバの運用はクラウドサービス提供会社に任せてしまうため、クラウドサービス提供会社の内部からの不正アクセスにより不正コピーやディスクの盗難などが発生するリスクがある。このように企業内秘匿情報をクラウドサービス提供会社に預けた場合には、アプリケーション提供会社側で企業内秘匿情報を管理できないというセキュリティ上の問題がある。

[0012] このように、アプリケーション提供会社は、クライアントの情報等の企業内秘匿情報の管理をクラウドサービス提供会社に委ねることになり、情報流出に対する管理ができない。そのため、企業内秘匿情報をクラウドサービス提供会社に預けることに不安を抱き、クラウドサービスの利用を躊躇してしまう場合が多い。クラウドサービスは、多数の利点を有しながらもその利用が十分に図られていないのが現状である。

[0013] 本発明は、上述したような課題に鑑みてなされたものであり、企業内秘匿情報のセキュリティ対策をアプリケーション提供会社側で行わせつつ、クラウドサービスの利用の促進を図ることできる仮想マシン、仮想マシンのプログラム、アプリケーションサービス提供システム及びアプリケーションサービス提供方法を提供することを目的とする。

課題を解決するための手段

[0014] 上記目的を解決するために、請求項 1 に係る発明は、インターネットに接続されたサーバ上で動作し、クライアント装置からの要求を処理する仮想マシンと、企業内ネットワークに接続され、前記クライアント装置を使用するユーザに関する情報を含む企業内の秘匿情報を記憶する企業内データベース

サーバとを備えたアプリケーションサービス提供システムにおける前記仮想マシンであって、前記インターネットを介してクライアント装置からの要求を受け付ける受付手段と、前記クライアント装置からの要求に対して、前記企業内秘匿情報に基づく処理が必要か否かを判定する判定手段と、前記判定手段により前記企業内秘匿情報に基づく処理が必要であると判定されると、企業内ネットワークに接続され、かつ前記企業内秘匿情報の記憶処理を行う企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第 1 処理手段と、前記判定手段により前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第 2 処理手段と、を備えるものとした。

[0015] また、請求項 2 に係る発明は、請求項 1 に記載の仮想マシンであって、前記企業内データベースサーバは、前記クライアント装置のユーザの認証情報を記憶しており、前記判定手段は、前記クライアント装置から認証情報を取得したとき、前記企業内秘匿情報に基づく処理が必要であると判定し、前記第 1 処理手段は、前記取得された認証情報と一致する認証情報が前記企業内データベースサーバに記憶されているかどうかを前記企業内データベースサーバに問い合わせ、前記クライアント装置の認証処理を行うこととした。

[0016] また、請求項 3 に係る発明は、請求項 1 に記載の仮想マシンであって、前記クライアント装置から前記企業内秘匿情報を受信したとき、前記企業内データベースサーバとの間でセキュアな通信を行って、前記企業内データベースサーバに前記企業内秘匿情報を記憶する第 3 処理手段を備えたこととした。

[0017] また、請求項 4 に係る発明は、請求項 1 ～ 3 のいずれか 1 項に記載の仮想マシンであって、前記第 1 処理手段は、前記クライアント装置から取得した情報を前記企業内秘匿情報に基づき加工して前記クライアント装置へ送信することとした。

[0018] また、請求項 5 に係る発明は、インターネットに接続されたサーバ上で動作する仮想マシンのプログラムであって、前記インターネットを介してクラ

クライアント装置からの要求を受け付ける受付ステップと、前記クライアント装置からの要求に対して、前記クライアント装置のユーザ情報を含む企業内秘匿情報に基づく処理が必要か否かを判定する判定ステップと、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要であると判定されると、企業内ネットワークに接続され、かつ前記企業内秘匿情報を記憶した企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第1処理ステップと、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第2処理ステップと、を実行させるものとした。

[0019] また、請求項6に係る発明は、インターネットに接続されたサーバ上で動作し、クライアント装置からの要求に応じた処理を行う仮想マシンと、企業内ネットワークに接続された企業内データベースサーバと、を備えたアプリケーションサービス提供システムにおいて、前記企業内データベースサーバは、前記クライアント装置のユーザ情報を含む企業内秘匿情報を記憶する記憶手段と、前記仮想マシンからの要求に応じて、前記記憶手段に記憶した企業内秘匿情報の検索、変更又は削除、又は前記記憶手段への企業内秘匿情報の追加を行う記憶処理手段と、を備え、前記仮想マシンは、前記インターネットを介してクライアント装置からの要求を受け付ける受付手段と、前記クライアント装置からの要求に対して、前記企業内秘匿情報に基づく処理が必要か否かを判定する判定手段と、前記判定手段により前記企業内秘匿情報に基づく処理が必要であると判定されると、前記企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第1処理手段と、前記判定手段により前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第2処理手段と、を備えたこととした。

[0020] また、請求項7に係る発明は、インターネットに接続されたサーバ上で動作し、クライアント装置からの要求に応じた処理を行う仮想マシンと、企業

内ネットワークに接続された企業内データベースサーバとによるアプリケーションサービス提供方法であって、前記仮想マシンが、前記インターネットを介してクライアント装置からの要求を受け付ける受付ステップと、前記仮想マシンが、前記クライアント装置からの要求に対して、当該クライアント装置のユーザ情報を含む企業内秘匿情報に基づく処理が必要か否かを判定する判定ステップと、前記仮想マシンが、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要であると判定されると、前記企業内データベースサーバとの間でセキュアな通信を行って、前記企業内データベースサーバに対して、前記クライアント装置からの要求に応じた処理を行う要求ステップと、前記企業内データベースサーバが、前記仮想マシンからの要求に応じて、前記企業内秘匿情報を記憶した記憶手段から前記企業内秘匿情報の検索、変更又は削除、又は前記記憶手段への企業内秘匿情報の追加を行う記憶処理ステップと、前記仮想マシンが、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要ではない判定されると、前記クライアント装置からの要求に応じた処理を行う処理ステップと、有することとした。

発明の効果

- [0021] 本発明によれば、クラウドサービスの利用者であるアプリケーション提供会社は、インターネットを介して接続されたサーバ上で動作する仮想マシンを利用してコンピュータ資源の導入コストや運用コストを低減しつつ、企業内秘匿情報を含む情報をクラウドサービス提供会社に預けることなく、自社内でセキュリティ対策を行うことが可能となる。

図面の簡単な説明

- [0022] [図1]本発明の一実施形態に係るアプリケーションサービス提供システムの構成を示す図である。
- [図2]アプリケーションサービス提供システムの概略動作を示す図である。
- [図3]図1に示すクライアント装置の構成を示す図である。
- [図4]図1に示すクライアント装置の処理の流れを示す図である。
- [図5]図1に示すサーバシステムの構成を示す図である。

[図6] 図5に示すブレードサーバ上のアーキテクチャを示す図である。

[図7] 図5に示すブレードサーバの機能ブロック図である。

[図8] 仮想A Pサーバの処理の流れを示す図である。

[図9] D Bサーバの機能ブロック図である。

[図10] D Bサーバの処理の流れを示す図である。

[図11] W e b会議サービスのシステムの登録処理の流れを示す図である。

[図12] 第1テーブルのデータ構造の一例を示す図である。

[図13] 第2テーブルのデータ構造の一例を示す図である。

[図14] 第3テーブルのデータ構造の一例を示す図である。

[図15] W e b会議サービスのシステムの参加準備処理の流れを示す図である。

[図16] W e b会議サービスのシステムの会議処理の流れを示す図である。

[図17] クライアント装置の処理の流れを示す図である。

[図18] S I Pサーバの処理の流れ（その1）を示す図である。

[図19] S I Pサーバの処理の流れ（その2）を示す図である。

[図20] D Bサーバの処理の流れを示す図である。

発明を実施するための形態

[0023] [1. アプリケーションサービス提供システムの概要]

本実施形態のアプリケーションサービス提供システムは、インターネット経由でアプリケーションをクライアントに提供しようとする企業であるアプリケーション提供会社が、クラウドサービスを利用して、アプリケーションサービスをクライアントに提供することができるアプリケーションサービス提供システムである。

[0024] このようにアプリケーション提供会社がクラウドサービスを利用して提供するアプリケーションサービスにおいては、このアプリケーションサービスを利用するクライアントは、クラウドサービスであることを意識することはない。クライアントは、通常のアプリケーションサービスと同様に、アプリケーション提供会社からのアプリケーションサービスを受けることとなる。な

お、アプリケーションサービスとしては、例えば、後述するWeb会議サービス、データベースサービス、eラーニングサービス、画像配信サービスなどがある。

[0025] クラウドサービスを提供する企業であるクラウドサービス提供会社は、アプリケーションのプラットフォームとなる仮想マシンをアプリケーション提供会社にレンタルする。アプリケーション提供会社は、仮想マシン上でアプリケーションプログラムを実行させ、クライアントにアプリケーションサービスを提供する。なお、以下においては、アプリケーション提供会社からアプリケーションサービスの提供を受けるクライアントの装置をクライアント装置と呼ぶ。

[0026] 図1に示すように、クラウドサービス提供会社側のコンピュータシステム3は、インターネット2にLAN側入出力ポートを接続したルータ10と、ルータ10のLAN側入出力ポートに接続されたサーバシステム11とを有している。

[0027] このサーバシステム11は、後述するようにインターネットに接続された複数のブレードサーバで構成され、これらのブレードサーバ上で多数の仮想マシンを動作させることができるようにしている。ここでは、多数の仮想マシンのうち、アプリケーション提供会社は一つの仮想マシンでアプリケーションプログラムを実行して、クライアントにアプリケーションサービスを提供するものとする。アプリケーション提供会社は複数の仮想マシンを用いてアプリケーションサービスを用いてアプリケーションサービスを提供することもできる。以下、このようにアプリケーションプログラムを実行する仮想マシンを仮想APサーバ13_xと呼ぶ。図1に示す例では、第1ブレードサーバ12₁上で動作する仮想マシンを仮想APサーバ13_xとして用いている。

[0028] アプリケーション提供会社のアプリケーションサービスには、クライアント装置1a, 1b, 1c, …の利用者が加入している。各利用者は、各クライアント装置1a, 1b, 1c, …から仮想APサーバ13_xにアクセスしてアプリケーション提供会社のアプリケーションサービスを受ける。なお、ク

クライアント装置 1 a, 1 b, 1 c, …のうち何れかのクライアント装置又は全てのクライアント装置を示す場合には、便宜上、クライアント装置 1 という。

[0029] サーバシステム 1 1 はクラウドサービス提供会社の企業内ネットワークのクラウドサービス用のネットワーク領域に配置される。サーバシステム 1 1 上で動作する仮想 A P サーバ 1 3_x宛てに、クライアント装置 1 からインターネット経由での通信パケットが送信されたとき、ルータ 1 0 は、クライアント装置 1 からの通信パケットを仮想 A P サーバ 1 3_xに中継する。また、仮想 A P サーバ 1 3_xからクライアント装置 1 への通信パケットもルータ 1 0 によりクライアント装置 1 へ中継される。クライアント装置 1 は、仮想 A P サーバ 1 3_xとの間で、提供を受けるサービスに応じた通信パケットを送受信することで、アプリケーションサービスの提供を受ける。

[0030] アプリケーション提供会社のコンピュータシステム 4 は、VPN ルータ 2 0 と、ストレージ 2 1 と、このストレージ 2 1 のデータを管理するデータベースサーバ 2 2 と、ストレージ 2 1 を管理するための管理装置 2 3 とを有している。管理装置 2 3 は、データベースサーバ 2 2 を介してストレージ 2 1 へのデータの追加やデータの更新を行うことができる。なお、以下においては、データベースサーバを DB サーバとも呼ぶ。

[0031] DB サーバ 2 2 は、VPN ルータ 2 0 を介して、仮想 A P サーバ 1 3_xからアクセスされるようになっている。仮想 A P サーバ 1 3_xとコンピュータシステム 4 内のネットワークとの間は、VPN (Virtual Private Network) 接続によりセキュアな通信が確立される。ここで、セキュアな通信を行うとは、周知の方式により暗号化されたデータで通信を行うことである。すなわち、仮想 A P サーバ 1 3_xは、VPN 接続用のプログラムを記憶しており、VPN ルータ 2 0 と VPN 接続を行うようにしている。なお、VPN ルータ 2 0 を経由した通信パケットのみが DB サーバ 2 2 で受信可能となるように VPN ルータ 2 0 内のファイアウォールが設定されている。このように、仮想 A P サーバ 1 3_xのみが DB サーバ 2 2 に対するインターネット経由のアクセスを

行うことが可能である。

- [0032] 本実施形態に係るアプリケーションサービス提供システムでは、クライアント装置 1 からアクセスされた仮想 A P サーバ 1 3_xは、必要に応じて D B サーバ 2 2 と通信して、クライアント装置 1 からの要求に応じた処理を行うようにしている。
- [0033] D B サーバ 2 2 及びストレージ 2 1 は、共にアプリケーション提供会社の企業内ネットワークに配置されている。ストレージ 2 1 に、企業秘匿情報を含むアプリケーション用の情報が記憶される。企業秘匿情報には、クライアントの個人情報やアプリケーション提供会社の社内の機密情報などの重要な情報が含まれる。
- [0034] 本実施形態に係るアプリケーションサービス提供システムでは、企業秘匿情報をアプリケーション提供会社側の企業内ネットワーク内で管理することができるので、クラウドサービス提供会社に預けることなく、アプリケーション提供会社側で企業秘匿情報を管理することができる。
- [0035] 従って、アプリケーション提供会社は、社内のセキュリティ管理を厳密に行うことができる。このため、クラウドサービス提供会社側のセキュリティ対策を気にすることなく、クラウドサービスを利用することが可能となる。そのため、アプリケーション提供会社は、セキュリティ管理を厳密に行いつつも、コンピュータ資源の一部にクラウドサービスを利用して、比較的低コストで、アプリケーションサービスを運用することができる。
- [0036] 以上のように構成されるアプリケーションサービス提供システムの概略動作について図 2 を参照して説明する。
- [0037] 図 2 に示すように、まず、アプリケーションサービスを受けるクライアントは、クライアント装置 1 を用いてアプリケーションサービスを受けるための所定の操作を行う。この操作を受けてクライアント装置 1 は、インターネット 2 を介して、仮想 A P サーバ 1 3_xに対し、操作に応じた要求を行う（ステップ S 1 1）。
- [0038] クライアント装置 1 から要求を受け付けると、仮想 A P サーバ 1 3_xは、企

業内データベースサーバと通信が必要か否かを判定する（ステップS 1 2）。

仮想A Pサーバ1 3_xには、企業内データベースサーバとしてアプリケーション提供会社の企業内ネットワークに接続されたD Bサーバ2 2が登録されている。仮想A Pサーバ1 3_xは、このD Bサーバ2 2との通信が必要であるか否かを判定する。仮想A Pサーバ1 3_xは、例えば、クライアント装置1からの要求が、アプリケーションサービスへの登録要求や接続要求であり、クライアントのパスワード、I D、氏名、住所、職業などの個人情報を含むものであるとき、企業内データベースサーバと通信が必要であると判定する。

すなわち、仮想A Pサーバ1 3_xは、企業内秘匿情報を受信したとき、D Bサーバ2 2との通信が必要であると判定する。一方、仮想A Pサーバ1 3_xは、クライアントの個人情報を含まないときには、企業内データベースサーバと通信が必要ないと判定する。ここで、アプリケーションサービスへの登録要求とは、クライアントがクライアント装置1を用いてアプリケーションサービスを利用するために事前に行う要求であり、クライアントのパスワード、I D、氏名、住所、職業などの個人情報を登録するための要求である。また、アプリケーションサービスへの接続要求とは、クライアントがクライアント装置1を用いてアプリケーションサービスを利用する際に行う要求である。

アプリケーションサービスへの接続要求は、クライアントのパスワード及びI Dを含む。仮想A Pサーバ1 3_xは、この接続要求に含まれるクライアントのパスワード及びI D（認証情報）によりクライアントの認証を行う。このように、アプリケーション提供会社のクライアントの個人情報は、アプリケーション提供会社内で保持される。このため、クライアントの個人情報は、アプリケーション提供会社側で管理することができる。従って、アプリケーション提供会社は、極めて重要なクライアントの個人情報に対するセキュリティ対策を自社で行いつつも、仮想マシンを利用してコンピュータ資源の導入コストや運用コストを低減させて、アプリケーションサービスの提供を行うことができる。

[0039] このステップS 1 2の処理において、企業内データベースサーバと通信が

必要ではないと判定すると（ステップS 1 2 : N O）、仮想A Pサーバ1 3_xは、内部処理を行う（ステップS 1 3）。この内部処理として、仮想A Pサーバ1 3_xは、クライアント装置1からの要求に応じて必要な処理を行う。

[0040] 一方、企業内データベースサーバと通信が必要であると判定すると（ステップS 1 2 : Y E S）、仮想A Pサーバ1 3_xは、DBサーバ2 2に、受信した要求に対応するリクエストを送信する（ステップS 1 4）。このとき、仮想A Pサーバ1 3_xとDBサーバ2 2との間の通信経路のうちインターネットにおける通信経路は、V P N接続されていることから、仮想A Pサーバ1 3_xは、DBサーバ2 2との間でセキュアな通信を行うことができる。なお、ここでは、仮想A Pサーバ1 3_xとDBサーバ2 2との間でセキュアな通信を行うために、V P N接続を行うようにしているが、H T T P S (Hypertext Transfer Protocol over Secure Socket Layer) プロトコルを用いて、セキュアな通信を行うようにしてもよい。

[0041] DBサーバ2 2は、仮想A Pサーバ1 3_xからインターネット2を介して送信されるリクエストを受信し、このリクエストに基づいた処理を行う（ステップS 1 5）。例えば、受信したリクエストがアプリケーションサービスへの登録要求に応じたリクエストである場合、DBサーバ2 2は、受信したリクエストに含まれるクライアントのI D、パスワード、住所、氏名等の個人情報をストレージ2 1に記憶して、クライアントの個人情報を登録する。また、受信したリクエストがアプリケーションサービスへの接続要求に応じたリクエストである場合、DBサーバ2 2は、受信したリクエストに含まれるクライアントのI Dやパスワードなどの個人情報がストレージ2 1に記憶している個人情報と一致するかを判定する。

[0042] DBサーバ2 2は、ステップS 1 5で行った処理の結果をインターネット2を介して仮想A Pサーバ1 3_xへ送信する（ステップS 1 6）。例えば、DBサーバ2 2は、アプリケーションサービスへの登録要求に応じたリクエストに対しては、クライアントの個人情報をストレージ2 1に登録することが終了したことを示す情報を処理の結果として仮想A Pサーバ1 3_xへ送信する

。また、DBサーバ22は、アプリケーションサービスへの接続要求に応じたリクエストに対しては、クライアントの個人情報がストレージ21に登録されていれば、認証OKを示す情報を処理の結果として仮想APサーバ13_xへ送信する。一方、DBサーバ22は、クライアントの個人情報がストレージ21に登録されていなければ、認証NGを示す情報を処理の結果として仮想APサーバ13_xへ送信する。

[0043] 仮想APサーバ13_xは、DBサーバ22からインターネット2を介して送信される処理の結果を受信する（ステップS17）。仮想APサーバ13_xは、ステップS13で行った内部処理の結果、又は、ステップS17で受信した処理の結果を、クライアント装置1へ送信する（ステップS18）。

[0044] クライアント装置1は、仮想APサーバ13_xからインターネット2を介して送信される処理の結果を受信し（ステップS19）、その後、その結果に基づいて所定の処理を行う（ステップS20）。

[0045] [2. 各構成要素の具体的構成]

次に、アプリケーションサービス提供システムを構成する各要素の構成及び動作についてそれぞれ説明する。

[0046] [2. 1. クライアント装置1の構成及び動作]

まず、クライアント装置1の具体的構成について説明する。このクライアント装置1は、専用のコンピュータの他、一般のパーソナルコンピュータを適用可能である。クライアント装置1は、このクライアント装置1のユーザ、すなわちクライアントが所有するものである。図3に示すように、クライアント装置1は、制御部41と、記憶部42と、通信部43と、操作部44と、情報取得部45と、提示部46とを備えており、これらは、システムバス47を介して相互に接続されている。

[0047] 制御部41は、クライアント装置1全体を制御するものであり、CPU（Central Processing Unit）、内部メモリなどから構成される。記憶部42は、各種情報を記憶する記憶領域を有する書き換え可能な記憶装置であり、例えば、フラッシュメモリから構成される。通信部43は、他の装置とインタ

ーネット2を介して通信するための通信インターフェイスである。操作部44は、各種設定入力を行うための操作部である。情報取得部45は、カメラやマイクから構成され、カメラから撮像した映像情報を出し、マイクから取得した音声情報を出しする。提示部46は、液晶表示装置（LCD）やスピーカーから構成されており、映像情報や音声情報を再生する。

[0048] 以上のように構成されたクライアント装置1の動作について、図4のフローチャートに基づいて説明する。クライアント装置1での処理は、クライアント装置1において電源スイッチ（図示せず）がONされたときやリセットスイッチ（図示せず）が操作されたときに開始され、繰り返し行われる。このとき、制御部41のCPUは、内部メモリに記憶したプログラムを実行状態として、制御部41としての機能を動作状態にする。

[0049] まず、制御部41は、操作部44を介して処理の実行指示を受け付けたかどうかを判定する（ステップS21）。実行指示を受け付けていないと判定すると（ステップS21：NO）、制御部41は、実行指示を受け付けるまで、ステップS21の判定を繰り返す。一方、実行指示を受け付けたと判定すると（ステップS21：YES）、制御部41は、受け付けた指示に基づいた要求を、仮想APサーバ13_xに送信する（ステップS22）。その後、制御部41は、ステップS22で送信した要求に対する処理結果を受信し（ステップS23）、この処理結果に基づいて所定の処理を行う（ステップS24）。

[0050] [2. 2. 仮想APサーバ13_xの構成及び動作]

仮想APサーバ13_xは、上述したようにサーバシステム11上に形成される仮想マシンである。

[0051] サーバシステム11は、図5に示すように、複数のブレードサーバ12₁～12_nと、ストレージ14₁～14_nと、サーバ管理装置15とから構成される。なお、ブレードサーバ12₁～12_nのうち何れかのブレードサーバ又は全てのブレードサーバを示す場合には、便宜上、ブレードサーバ12という。また、ストレージ14₁～14_nのうち何れかのストレージ又は全てのストレージを

示す場合には、便宜上、ストレージ 14 という。

- [0052] 各ブレードサーバ 12 は、CPU 401 と、ROM 402 と、RAM 403 と、入出力部 404 と、通信部 405 と、ハードディスク（HDD）406 とを有しており、これらはシステムバス 407 を介して相互に接続されている。入出力部 404 は、サーバ管理装置 15 とのデータの送受信を行うための通信インターフェイスである。通信部 405 は、クラウドサービス提供会社内の企業内ネットワークである LAN に接続するための通信インターフェイスである。
- [0053] このように構成されたブレードサーバ 12₁ ~ 12_n 上で、複数の仮想マシン 13₁ ~ 13_n が動作する。なお、複数の仮想マシン 13₁ ~ 13_n のうち何れかの仮想マシン又は全ての仮想マシンを示す場合には、便宜上、仮想マシン 13 という。
- [0054] 図 6 にブレードサーバ 12 上のアーキテクチャを示す。同図に示すように、ブレードサーバ 12 では、そのベースプログラムであるメイン OS が動作する。そしてメイン OS 上で仮想マシンを動作させるためのプログラムである仮想マシンプログラムが動作する。そして、この仮想マシンプログラム上で複数のゲスト OS が動作する。各ゲスト OS 上では、1 以上のアプリケーションプログラムを動作させることができる。
- [0055] サーバ管理装置 15 は、各ブレードサーバ 12 を制御及び管理する装置である。サーバ管理装置 15 は、ゲスト OS に割り当てるリソース（CPU 401, ROM 402, RAM 403, HDD 406 など）を管理する。例えば、サーバ管理装置 15 は、仮想マシン 13 によるリソースの利用率に応じて、仮想マシン 13 に割り当てるリソースを変更することができる。また、サーバ管理装置 15 は、アプリケーションプログラムの実行開始や実行停止などを制御することができる。さらに、サーバ管理装置 15 は、各ブレードサーバ 12 と通信を行って、ゲスト OS やアプリケーションプログラムの追加、削除又は更新を行うことができる。
- [0056] 本実施形態では、ブレードサーバ 12 上で動作する仮想マシン 13 のうち

、第1ブレードサーバ12_i上で動作する仮想マシンを仮想APサーバ13_xとして用いる（図1参照）。

[0057] ブレードサーバ12上で動作する仮想APサーバ13_{x1}は、図7に示すように、ブレードサーバ12のリソースを利用することで、制御部411、記憶部412、通信部413などとして機能し、アプリケーション用プログラムを実行する。制御部411は、受付手段、判定手段、第1処理手段、第2処理手段、第3処理手段等として機能する。

[0058] 次に、仮想APサーバ13_xでの処理について、図8のフローチャートに基づいて具体的に説明する。仮想APサーバ13_xでの処理は、サーバ管理装置15によりブレードサーバ上での仮想APサーバ13_xの動作が許可されたときに開始する。

[0059] まず、制御部411は、クライアント装置1から要求を受信したか否かを判定する（ステップS31）。この処理において、要求を受信していないと判定すると（ステップS31：NO）、制御部411は、クライアント装置1から要求を受信するまで、ステップS31の判定を繰り返す。一方、要求を受信したと判定した場合は（ステップS31：YES）、制御部411は、DBサーバ22との通信が必要か否かを判定する（ステップS32）。

[0060] この処理において、DBサーバ22との通信が必要ではないと判定すると（ステップS32：NO）、制御部411は、受信した要求に応じた処理を、仮想APサーバ13_x内部で実行する（ステップS33）。一方、DBサーバ22との通信が必要であると判定すると（ステップS32：YES）、制御部411は、クライアント装置1からの要求に応じてDBサーバ22に対するリクエストを生成し、生成したリクエストをDBサーバ22に送信する（ステップS34）。その後、制御部411は、ステップS34で送信したリクエストに対する処理結果を受信する（ステップS35）。この処理が終了したとき、又はステップS33の処理が終了すると、制御部411は、ステップS31で受信した要求を送信したクライアント装置1に対して、処理の結果（ステップS33における内部処理の結果、または、ステップS35

で受信した処理結果）を送信する（ステップS 3 6）。

[0061] [2. 3. DBサーバ2 2の構成及び動作]

次に、DBサーバ2 2の具体的構成について説明する。DBサーバ2 2は、一般のサーバコンピュータを適用可能である。DBサーバ2 2は、ユーザの企業（アプリケーション提供会社）によって管理される。図9に示すように、DBサーバ2 2は、制御部6 1と、記憶部6 2と、通信部6 3と、操作部とを備えており、これらはシステムバス6 4を介して相互に接続されている。制御部6 1は、ストレージ2 1を制御する。記憶部6 2は、各種情報を記憶する記憶領域を有する書き換え可能な記憶装置である。通信部6 3は、管理装置2 3等と通信するための通信インターフェイスである。

[0062] 制御部6 1は、CPU（Central Processing Unit）、内部メモリなどから構成される。CPUは内部メモリに記憶されているプログラムを読み出して実行することによって、記憶処理手段等として機能する。

[0063] 次に、DBサーバ2 2での処理について、図10のフローチャートに基づいて具体的に説明する。DBサーバ2 2での処理は、DBサーバ2 2において電源スイッチ（図示せず）がONされたときやリセットスイッチ（図示せず）が操作されたときに開始され、繰り返し行われる。このとき、制御部6 1のCPUは、内部メモリに記憶したプログラムを実行状態として、制御部6 1としての機能を動作状態とする。

[0064] まず、制御部6 1は、仮想APサーバ1 3_xからリクエストを受信したか否かを判定する（ステップS 4 1）。リクエストを受信していないと判定すると（ステップS 4 1：NO）、制御部6 1は、リクエストを受信するまで、ステップS 4 1の判定を繰り返す。一方、リクエストを受信したと判定した場合は（ステップS 4 1：YES）、制御部6 1は、ステップS 4 2において、リクエストの内容に基づいた処理を行う。このとき、必要に応じて、ストレージ2 1に記憶されている企業内秘匿情報が用いられる。その後、ステップS 4 3において、制御部6 1は、ステップS 4 1で受信したリクエストを送信した仮想APサーバ1 3_xに対して、処理の結果を送信する。

[0065] 以上説明したとおり、クライアント装置 1、仮想 AP サーバ 13_x、DB サーバ 22 のそれぞれが上述した処理を繰り返すことにより、アプリケーションサービス提供システムが動作する。

[0066] [4. 本実施形態を適用した Web 会議システム]

[0067] 次に、上述した構成を有するアプリケーションサービス提供システムを用いた Web 会議サービスのシステム（以下、「Web 会議システム」）について具体的に説明する。この Web 会議システムは、ブレードサーバ 12 上で設定した仮想マシン 13 で Web 会議用のアプリケーションソフトウェアを動作させることにより実行されるものである。ここでは、一例として、アプリケーション提供会社が、第 2 ブレードサーバ 12₂ 上で動作する仮想マシンをレンタルして、SIP (Session Initiation Protocol) サーバ 13_{x2} として用いて、Web 会議サービスを提供するものとして説明する。

[0068] 以下の説明において、この Web 会議システムは、SIP サーバ 13_{x2} を介してクライアント装置 1 間で映像情報や音声情報の送受信を行うことによって、遠隔地間での会議を可能とするものである。以下においては、音声情報の処理については省略するが、映像情報の処理と同様の処理である。

[0069] 図 1 に示す構成において、クライアント装置 1a ~ 1c を使用するクライアント A ~ C の 3 者が Web 会議を行う場合、クライアント A が使用するクライアント装置 1a の提示部 46 には、クライアント装置 1b 及び 1c から取得した映像情報が提示される。また、クライアント B が使用するクライアント装置 1b の提示部 46 には、クライアント装置 1a 及び 1c から取得した映像情報が提示される。また、クライアント C が使用するクライアント装置 1c の提示部 46 には、クライアント装置 1a 及び 1b から取得した映像情報が提示される。また、SIP サーバ 13_{x2} は、各クライアント装置 1 から取得した映像情報に基づいて、各クライアント装置 1 に送信するための映像情報を加工して送信する。

[0070] また、ストレージ 21 には、クライアント装置 1 毎の情報が登録される第 1 テーブル（図 12 参照）と、開催される会議の開始時刻や終了時刻などの

情報が登録される第2テーブル（図13参照）と、会議に参加するクライアント装置1の情報が登録される第3テーブル（図14参照）とが記憶される。Web会議を行うには、事前に主催者のクライアント装置1から後述の会議情報をストレージ21に登録する必要がある。また、Web会議に参加するためには、参加する各クライアント装置1において、参加準備の操作を行う必要がある。

[0071] このWeb会議システムにおいては、以下の3つの処理が行われる。

- （1）主催する会議をDBサーバ22に登録するための「登録処理」
- （2）会議への参加手続きを行うための「参加準備処理」
- （3）Web会議を行うための「会議処理」

以下、それぞれの処理について、具体的に説明する。

[0072] [4. 1. 登録処理]

まず、登録処理について、図11を参照しつつ説明する。この処理は、会議を主催するクライアントのクライアント装置1と、SIPサーバ13_{x2}と、DBサーバ22とで実行される。

[0073] まず、クライアント装置1は、会議の主催者から操作部44を介して拠点ID及びパスワードの入力、及び、認証処理の実行指示を受け付ける。なお、拠点ID及びパスワードは予め記憶部42に記憶している場合には、操作部44を介しての入力は不要となる。そして、クライアント装置1は、受け付けた情報に基づいた認証処理の要求を、SIPサーバ13_{x2}に送信する（ステップS51）。この要求には、認証処理の実行要求を示す情報と、拠点ID及びパスワードとが含まれる。なお、この際、拠点IDやパスワードに対して所定の暗号化処理を施してもよい。

[0074] SIPサーバ13_{x2}は、認証処理の要求を受け付けると、DBサーバ22に対し、認証処理の要求に応じた認証処理リクエストを送信する（ステップS52）。この認証処理リクエストには、クライアント装置1から送信された情報に加え、SIPサーバ13_{x2}を識別するための識別情報が含まれている。

[0075] DBサーバ22は、認証処理リクエストを受け付けると、認証処理を行う

(ステップS 5 3)。DBサーバ2 2は、ストレージ2 1に記憶している第1テーブル(図1 2)を参照して認証処理を行う。すなわち、この認証処理において、DBサーバ2 2は、受信した認証処理リクエストに含まれる拠点IDとパスワードとの組み合わせがストレージ2 1の第1テーブルに登録されているかどうかの照合を行う。拠点IDとパスワードとの組み合わせが第1テーブルに登録されているとき、DBサーバ2 2は、認証が成功したと判定する。それ以外の場合には認証が失敗したと判定する。なお、ストレージ2 1に記憶される拠点IDやパスワードについても、クライアント装置1での処理と同様に、暗号化処理を施してもよい。この場合には照合の際に復号化することになる。

[0076] ここで、ストレージ2 1に記憶されている第1テーブルのデータ構造について説明する。図1 2に示すように、第1テーブルには、クライアント装置1毎の設定として、「拠点ID」、「IPアドレス」、「パスワード」、「担当者名」、「電話番号」、「会社名」、「サービス内容」、「メールアドレス」が記憶されている。

[0077] 認証処理の後、SIPサーバ1 3_{x2}は、認証処理リクエストを送信したSIPサーバ1 3_{x2}に対し、認証結果を送信する(ステップS 5 4)。認証結果には、認証が成功したか否かを示す情報、すなわち認証OKを示す情報または認証NGを示す情報が含まれる。

[0078] SIPサーバ1 3_{x2}は、DBサーバ2 2から認証結果を受信すると、ステップS 5 2で受け付けた要求を送信したクライアント装置1に対し、その認証結果を送信する(ステップS 5 5)。

[0079] クライアント装置1は、認証OKを示す情報を含む認証結果を受信すると、会議の主催者から操作部4 4を介して主催する会議の情報(以下、「会議情報」という)の入力を受け付け、また、会議情報登録処理の実行処理を受け付ける。そして、クライアント装置1は、受け付けた情報に基づいた会議情報登録処理の要求を、SIPサーバ1 3_{x2}に送信する(ステップS 5 6)。ここで、会議情報には、会議に参加するクライアントが使用するクライアン

ト装置 1 の識別番号（以下、「会議参加拠点番号」という）、及び、会議の予定開始時間／予定終了時間が含まれている。また、会議に参加する各クライアント装置 1 上の表示レイアウトの設定情報（後述）もこの要求に含まれる。

[0080] SIPサーバ 13_{x2}は、会議情報登録処理の要求を受け付けると、DBサーバ 22 に対し、SIPサーバ 13_{x2}の識別情報を含む登録処理リクエストを送信する（ステップ S 57）。DBサーバ 22 は、登録処理リクエストを受け付けると、会議情報登録処理を行う（ステップ S 58）。会議情報登録処理では、受信した登録処理リクエストに基づいて、会議情報をストレージ 21 の第 2 テーブル及び第 3 テーブルに登録する。すなわち、DBサーバ 22 は、登録処理リクエストに含まれる会議情報のうち、会議の予定開始時間と、予定終了時間と、会議情報登録処理の要求を行ったクライアント装置 1 の拠点 ID（開催拠点 ID）と、SIPサーバ 13_{x2}の識別情報とを、新たに発行した会議 ID に関連づけて第 2 テーブルに登録する。また、DBサーバ 22 は、登録処理リクエストに含まれる会議情報のうち、会議参加拠点番号と設定情報とを新たに発行した会議 ID に関連づけて第 3 テーブルに登録する。

[0081] ここで、ストレージ 21 に記憶されている第 2 テーブル及び第 3 テーブルのデータ構造について説明する。図 13 に示すように、第 2 テーブルには、会議 ID をキーとして、主催者のクライアント装置 1 を示す「開催拠点 ID」、会議の開始時刻を示す「予定開始時間」、会議の終了時刻を示す「予定終了時間」が登録されている。また、第 2 テーブルには、会議 ID をキーとして、SIPサーバ 13_{x2}の識別情報も登録されるが、ここでは図示していない。また、図 14 に示すように、第 3 テーブルには、会議 ID をキーとして、会議に参加するクライアント装置 1 の識別番号を示す「会議参加拠点 ID」と「設定情報」とが登録されている。設定情報は、表示する映像情報の品質（映像情報の圧縮方式など）や表示レイアウトの情報が含まれている。なお、本実施形態では、この設定情報も企業内秘匿情報として扱われる。

[0082] ステップ S 58 における会議情報の登録が終了すると、DBサーバ 22 は

、S I Pサーバ13_{x2}に対し、会議情報の登録処理が完了したことを示す完了情報を送信する（ステップS59）。S I Pサーバ13_{x2}は、DBサーバ22から完了情報を受信すると、クライアント装置1に対し、その完了情報を送信する（ステップS60）。

[0083] [4. 2. 参加準備処理]

次に、参加準備処理について、図15を参照しつつ説明する。この処理は、Web会議に参加するクライアントが使用する各クライアント装置1に対し、Web会議が行われることを通知し、かつ、各クライアント装置1の認証を行うための処理である。

[0084] まず、S I Pサーバ13_{x2}は、DBサーバ22に対し、会議情報リクエストを送信する（ステップS61）。この会議情報リクエストには、S I Pサーバ13_{x2}の識別番号が含まれている。このステップS61の処理は、所定時間間隔ごとに、繰り返し行われる。

[0085] DBサーバ22は、受信した会議情報リクエストに含まれるS I Pサーバ13_{x2}の識別番号に基づき、ストレージ21に記憶されている第1～第3テーブルを参照して会議情報を抽出する（ステップS62）。具体的には、DBサーバ22は、第2テーブルを参照して、S I Pサーバ13_{x2}の識別番号と関連し、かつ現時刻から所定時間内に開始される会議IDを抽出する。DBサーバ22は、抽出した会議IDを検索キーとして、第3テーブルを参照して、会議参加拠点ID及び設定情報を抽出する。そして、DBサーバ22は、抽出した会議参加拠点IDを検索キーとして、第1テーブルを参照して、メールアドレスを抽出する。そして、DBサーバ22は、これら抽出した情報を会議情報とする。その後、DBサーバ22は、ステップS62で受信した会議情報リクエストを送信したS I Pサーバ13_{x2}に対し、抽出した会議情報を送信する（ステップS63）。

[0086] S I Pサーバ13_{x2}は、会議情報を受信すると（ステップS64）、受信した会議情報に含まれる会議参加拠点番号のクライアント装置1に対して、会議が行われることを示す会議通知情報を電子メールで送信する（ステップS

65)。

[0087] 会議通知情報を受信すると、クライアント装置1は、クライアントから操作部44を介して拠点ID及びパスワードの入力、及び、認証処理の実行指示を受け付ける。そして、クライアント装置1は、受け付けた情報に基づいた認証処理の要求を、SIPサーバ13_{x2}に送信する(ステップS66)。SIPサーバ13_{x2}は、認証処理の要求を受け付けると、DBサーバ22に対し、認証処理リクエストを送信する(ステップS67)。

[0088] DBサーバ22は、認証処理リクエストを受け付けると、認証処理を行う(ステップS68)。この認証処理は、ストレージ21に記憶している第1テーブルと第3テーブルとを参照して行われる。すなわち、DBサーバ22は、認証処理リクエストに含まれる拠点IDとパスワードとの組み合わせが、第1テーブルに登録されているかを判定し、第1テーブルに登録されていれば、さらに、第3テーブルに拠点IDが登録されているかを判定する。いずれにも登録されているとき、DBサーバ22は、認証が成功したと判定し、それ以外の場合は、認証が失敗したと判定する。その後、DBサーバ22は、認証処理リクエストを送信したSIPサーバ13_{x2}に対し、認証結果を送信する(ステップS69)。DBサーバ22は、認証が成功したときには、ストレージ21に記憶されている第3テーブルから認証処理リクエストに含まれる拠点IDに対応する設定情報を取得し、この設定情報を、認証OKを示す情報と共にSIPサーバ13_{x2}へ送信する。

[0089] SIPサーバ13_{x2}は、DBサーバ22から認証結果を受信する(ステップS70)と、受信した認証結果に含まれる各クライアント装置1の拠点IDと設定情報との組み合わせを、記憶部412又はストレージ14に記憶する(ステップS71)。さらに、SIPサーバ13_{x2}は、認証処理の要求を送信したクライアント装置1に対して、認証結果を送信する(ステップS72)。なお、クライアント装置1は、記憶部42に会議中フラグを有し、会議開始時刻になると、そのフラグがONとなるものとする。

[0090] [4. 3. 会議処理]

次に、会議処理について、図 16 を参照しつつ説明する。この処理は、Web 会議に参加する各クライアント装置 1 と SIP サーバ 13_{x2} との間で実行される処理である。なお、図 16 では、説明の便宜上、クライアント装置 1 a とクライアント装置 1 b の 2 つのクライアント装置を示しているが、実際は、会議に参加するクライアント装置 1 の数だけ同様の処理が、Web 会議中繰り返し行われる。

[0091] まず、クライアント装置 1 a は、情報取得部 45 を介して取得した映像情報を SIP サーバ 13_{x2} に送信する（ステップ S 75 a）。同様に、クライアント装置 1 b は、情報取得部 45 を介して取得した映像情報を SIP サーバ 13_{x2} に送信する（ステップ S 75 b）。

[0092] SIP サーバ 13_{x2} は、各クライアント装置 1 から映像情報を受信する（ステップ S 76）と、受信した映像情報に基づいて、各クライアント装置 1 に送信する映像情報を生成する（ステップ S 77）。このとき、記憶部 412 又はストレージ 14 に記憶しているクライアント装置 1 毎の設定情報が参照される。その後、SIP サーバ 13_{x2} は、各クライアント装置 1 に対し、生成した映像情報を送信する（ステップ S 78）。

[0093] SIP サーバ 13_{x2} から映像情報を受信したクライアント装置 1 a、1 b は、それぞれ、受信した映像情報に基づいて、提示部 46 に映像を表示する（ステップ S 79 a、S 79 b）。

[0094] 次に、以上のような動作を行う Web 会議システムにおける各要素ごとの具体的な処理について説明する。

[0095] [4. 4. クライアント装置 1 での処理]

まず、クライアント装置 1 での処理について、図 17 を参照しつつ具体的に説明する。

[0096] まず、制御部 41 は、クライアントから操作部 44 を介して認証処理の実行指示を受け付けたか否かを判定する（ステップ S 81）。認証処理の実行指示を受け付けたと判定すると（ステップ S 81：YES）、制御部 41 は、SIP サーバ 13_{x2} に対し、認証処理の要求を送信する（ステップ S 82）

。この登録処理の要求には、拠点ID及びパスワードが含まれる。その後、制御部41は、SIPサーバ13_{x2}から認証結果を受信する（ステップS83）。

[0097] 一方、ステップS81において、認証処理の実行指示を受け付けていないと判定すると（ステップS81：NO）、制御部41は、ステップS84において、会議情報登録処理の実行指示を受け付けたか否かを判定する。会議登録処理の実行指示を受け付けたと判定すると（ステップS84：YES）、制御部41は、ステップS85において、SIPサーバ13_{x2}に対し、受け付けた入力に基づいて会議情報登録処理の要求を送信する。その後、制御部41は、会議情報登録処理の要求に対し、SIPサーバ13_{x2}から送信される会議情報の登録を示す完了情報を受信する（ステップS86）。

[0098] 一方、ステップS84において、会議情報登録処理の実行指示を受け付けていないと判定すると（ステップS84：NO）、制御部41は、会議開始の時刻であるか否かを判定する（ステップS87）。この処理において、制御部41は、会議開始の時刻となったときに、会議指示があったと判定する。この判定は、記憶部42に記憶されている会議中フラグがONとなっているかに基づいて行われる。会議開始の時刻ではないと判定すると（ステップS87：NO）、制御部41は、処理をステップS81に移行させ、ステップS81以降の処理を繰り返す。一方、会議開始の時刻であると判定すると（ステップS87：YES）、制御部41は、処理をステップS88に移行させる。

[0099] ステップS88において、制御部41は、情報取得部45を介して取得した映像情報を、SIPサーバ13_{x2}に送信する。また、制御部41は、SIPサーバ13_{x2}から取得した映像情報を、提示部46に提示する（ステップS89）。その後、制御部41は、会議終了か否かを判定する（ステップS90）。この判定は、記憶部42に記憶されている会議中フラグがOFFとなったか否かに基づいて行われる。会議終了ではないと判定すると（ステップS90：NO）、制御部41は、処理をステップS88に移行させ、ステップ

S 8 8からの処理を繰り返す。一方、会議終了であると判定すると（ステップS 9 0 : Y E S）、制御部4 1は、処理をステップS 8 1に移行させ、ステップS 8 1からの処理を繰り返す。

[0100] [4. 5. S I Pサーバ1 3_{x2}における処理（その1）]

次に、S I Pサーバ1 3_{x2}における処理（その1）について、図1 8を参照しつつ具体的に説明する。この処理では、クライアント装置1から受信した要求に応じた処理を行う。

[0101] まず、制御部4 1 1は、いずれかのクライアント装置1から認証処理の要求を受信したか否かを判定する（ステップS 1 0 1）。認証処理の要求を受信したと判定すると（ステップS 1 0 1 : Y E S）、制御部4 1 1は、認証処理リクエストを、DBサーバ2 2に送信する（ステップS 1 0 2）。この認証処理リクエストに対して、DBサーバ2 2から認証結果を受信する（ステップS 1 0 3）と、制御部4 1 1は、その認証結果を、クライアント装置1に送信する（ステップS 1 0 4）。

[0102] 一方、ステップS 1 0 1において、認証処理の要求を受信していないと判定すると（ステップS 1 0 1 : N O）、制御部4 1 1は、会議情報登録処理の要求を受信したか否かを判定する（ステップS 1 0 5）。会議登録処理の要求を受信したと判定すると（S 1 0 5 : Y E S）、制御部4 1 1は、登録処理リクエストを、DBサーバ2 2に送信する（ステップS 1 0 6）。この登録処理リクエストに対して、DBサーバ2 2から処理結果を受信する（ステップS 1 0 7）と、クライアント装置1にその処理結果を送信する（ステップS 1 0 8）。

[0103] 一方、ステップS 1 0 5において、会議情報登録処理の要求を受信していないと判定すると（ステップS 1 0 5 : N O）、制御部4 1 1は、映像情報を受信したか否かを判定する（ステップS 1 0 9）。映像情報を受信していないと判定すると（ステップS 1 0 9 : N O）、制御部4 1 1は、処理をステップS 1 0 1に移行させ、ステップS 1 0 1以降の処理を繰り返す。一方、映像情報を受信したと判定すると（ステップS 1 0 9 : Y E S）、制御部

4 1 1 は、受信した映像情報を、記憶部 4 1 2 又はストレージ 1 4 に一時的に記憶する（ステップ S 1 1 0）。

[0104] その後、制御部 4 1 1 は、ステップ S 1 0 9 で受信した映像情報を送信したクライアント装置 1 に送信する映像情報を生成する（ステップ S 1 1 1）。この映像情報は、記憶部 4 1 2 又はストレージ 1 4 に記憶している他のクライアント装置 1 から受信した映像情報を加工して生成される。また、加工時には、記憶部 4 1 2 又はストレージ 1 4 に記憶している企業内秘匿情報の 1 つである設定情報が参照される。映像情報を生成すると、制御部 4 1 1 は、生成した映像情報を、クライアント装置 1 に送信する（ステップ S 1 1 2）。

[0105] [4. 6. SIPサーバ 1 3_{x2}における処理（その 2）]

次に、SIPサーバ 1 3_{x2}における処理（その 2）について、図 1 9 を参照しつつ具体的に説明する。この処理は、DBサーバ 2 2 に、現時刻から所定時間以内に開始される会議が存在するか否かを問い合わせる処理であり、所定時間間隔で繰り返し実行される。なお、処理（その 2）は、上述した「SIPサーバ 1 3_{x2}における処理（その 1）」と並列して実行される。

[0106] まず、制御部 4 1 1 は、DBサーバ 2 2 に対し会議情報リクエストを送信する（ステップ S 1 2 1）。この会議情報リクエストに対する応答を受信すると（ステップ S 1 2 2）、制御部 4 1 1 は、受信した応答に会議情報が含まれているか否かを判定する（ステップ S 1 2 3）。なお、ステップ S 1 2 1 で送信した会議情報リクエストに該当する会議情報が存在しない場合には、受信した応答には会議情報が含まれていない。

[0107] 会議情報が含まれていないと判定すると（S 1 2 3 : NO）、制御部 4 1 1 は、この処理を終了する。一方、会議情報が含まれていると判定すると（S 1 2 3 : YES）、制御部 4 1 1 は、会議情報に含まれる会議参加拠点番号のクライアント装置 1 に対して、会議が行われることを示す会議通知情報を電子メールで送信する（ステップ S 1 2 4）。

[0108] [4. 7. DBサーバ 2 2 における処理]

次に、DBサーバ22における処理について、図20を参照しつつ具体的に説明する。

- [0109] まず、DBサーバ22の制御部61は、SIPサーバ13_{x2}から認証処理リクエストを受信したか否かを判定する（ステップS131）。認証処理リクエストを受信したと判定すると（ステップS131：YES）、制御部61は、認証処理を実行する（ステップS132）。この認証処理は、上述のステップS68の処理で説明したように、ストレージ21に記憶されている第1テーブルと第3テーブルとを参照して行われる。この認証処理が終了すると、制御部61は、その認証結果をSIPサーバ13_{x2}に送信する（ステップS133）。
- [0110] 一方、ステップS131において、認証処理のリクエストを受信していないと判定すると（ステップS131：NO）、制御部61は、登録処理リクエストを受信したか否かを判定する（ステップS134）。登録処理リクエストを受信したと判定すると（ステップS134：YES）、制御部61は、上述のステップS58の処理で説明したように、会議情報をストレージ21の第2テーブル及び第3テーブルに登録する（ステップS135）。その後、制御部61は、会議情報の登録が完了したことを示す完了情報を、SIPサーバ13_{x2}に送信する（ステップS136）。
- [0111] 一方、ステップS134において、登録処理リクエストを受信していないと判定すると（ステップS134：NO）、制御部61は、会議情報リクエストを受信したか否かを判定する（ステップS137）。会議情報リクエストを受信していないと判定すると（ステップS137：NO）、制御部61は、処理をステップS131に移行させ、ステップS131以降の処理を繰り返す。一方、会議情報リクエストを受信したと判定すると（ステップS137：YES）、制御部61は、上述のステップS62で説明したように、ストレージ21に記憶されている第1～第3テーブルを参照して会議情報を抽出する（ステップS138）。その後、制御部61は、抽出した会議情報を、SIPサーバ13_{x2}に送信する（ステップS139）。

[0112] なお、上述した各実施形態の説明は本発明の一例であり、本発明は上述の実施形態に限定されることはない。このため、上述した各実施形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

符号の説明

- [0113] 1 クライアント装置
- 1 1 サーバシステム
 - 1 2 ブレードサーバ
 - 1 3_x 仮想APサーバ
 - 1 3_{x2} SIPサーバ
 - 1 4, 2 1 ストレージ
 - 2 2 データベースサーバ
 - 2 3 管理装置

請求の範囲

[請求項1]

インターネットに接続されたサーバ上で動作し、クライアント装置からの要求を処理する仮想マシンと、企業内ネットワークに接続され、前記クライアント装置を使用するユーザに関する情報を含む企業内秘匿情報を記憶する企業内データベースサーバとを備えたアプリケーションサービス提供システムにおける前記仮想マシンであって、

前記インターネットを介してクライアント装置からの要求を受け付ける受付手段と、

前記クライアント装置からの要求に対して、前記企業内秘匿情報に基づく処理が必要か否かを判定する判定手段と、

前記判定手段により前記企業内秘匿情報に基づく処理が必要であると判定されると、企業内ネットワークに接続され、かつ前記企業内秘匿情報の記憶処理を行う企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第1処理手段と、

前記判定手段により前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第2処理手段と、を備えた仮想マシン。

[請求項2]

前記企業内データベースサーバは、前記クライアント装置のユーザの認証情報を記憶しており、

前記判定手段は、前記クライアント装置から認証情報を取得したとき、前記企業内秘匿情報に基づく処理が必要であると判定し、

前記第1処理手段は、前記取得された認証情報と一致する認証情報が前記企業内データベースサーバに記憶されているかどうかを前記企業内データベースサーバに問い合わせ、前記クライアント装置の認証処理を行うことを特徴とする請求項1に記載の仮想マシン。

[請求項3]

前記クライアント装置から前記企業内秘匿情報を受信したとき、前記企業内データベースサーバとの間でセキュアな通信を行って、前記

企業内データベースサーバに前記企業内秘匿情報を記憶する第 3 処理手段を備えたことを特徴とする請求項 1 に記載の仮想マシン。

[請求項4] 前記第 1 処理手段は、前記クライアント装置から取得した情報を前記企業内秘匿情報に基づき加工して前記クライアント装置へ送信することを特徴とする請求項 1 ～ 3 のいずれか 1 項に記載の仮想マシン。

[請求項5] インターネットに接続されたサーバ上で動作する仮想マシンに、
前記インターネットを介してクライアント装置からの要求を受け付ける受付ステップと、

前記クライアント装置からの要求に対して、前記クライアント装置のユーザ情報を含む企業内秘匿情報に基づく処理が必要か否かを判定する判定ステップと、

前記判定ステップにより前記企業内秘匿情報に基づく処理が必要であると判定されると、企業内ネットワークに接続され、かつ前記企業内秘匿情報を記憶した企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第 1 処理ステップと、

前記判定ステップにより前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第 2 処理ステップと、を実行させるプログラム。

[請求項6] インターネットに接続されたサーバ上で動作し、クライアント装置からの要求に応じた処理を行う仮想マシンと、

企業内ネットワークに接続された企業内データベースサーバと、を備えたアプリケーションサービス提供システムにおいて、

前記企業内データベースサーバは、

前記クライアント装置のユーザ情報を含む企業内秘匿情報を記憶する記憶手段と、

前記仮想マシンからの要求に応じて、前記記憶手段に記憶した企業内秘匿情報の検索、変更又は削除、又は前記記憶手段への企業内秘匿

情報の追加を行う記憶処理手段と、を備え、

前記仮想マシンは、

前記インターネットを介してクライアント装置からの要求を受け付ける受付手段と、

前記クライアント装置からの要求に対して、前記企業内秘匿情報に基づく処理が必要か否かを判定する判定手段と、

前記判定手段により前記企業内秘匿情報に基づく処理が必要であると判定されると、前記企業内データベースサーバとの間でセキュアな通信を行って、前記企業内秘匿情報に基づき前記要求に対する処理を行う第1処理手段と、

前記判定手段により前記企業内秘匿情報に基づく処理が必要ではないと判定されると、前記要求に対する処理を実行する第2処理手段と、を備えたアプリケーションサービス提供システム。

[請求項7]

インターネットに接続されたサーバ上で動作し、クライアント装置からの要求に応じた処理を行う仮想マシンと、企業内ネットワークに接続された企業内データベースサーバとによるアプリケーションサービス提供方法であって、

前記仮想マシンが、前記インターネットを介してクライアント装置からの要求を受け付ける受付ステップと、

前記仮想マシンが、前記クライアント装置からの要求に対して、当該クライアント装置のユーザ情報を含む企業内秘匿情報に基づく処理が必要か否かを判定する判定ステップと、

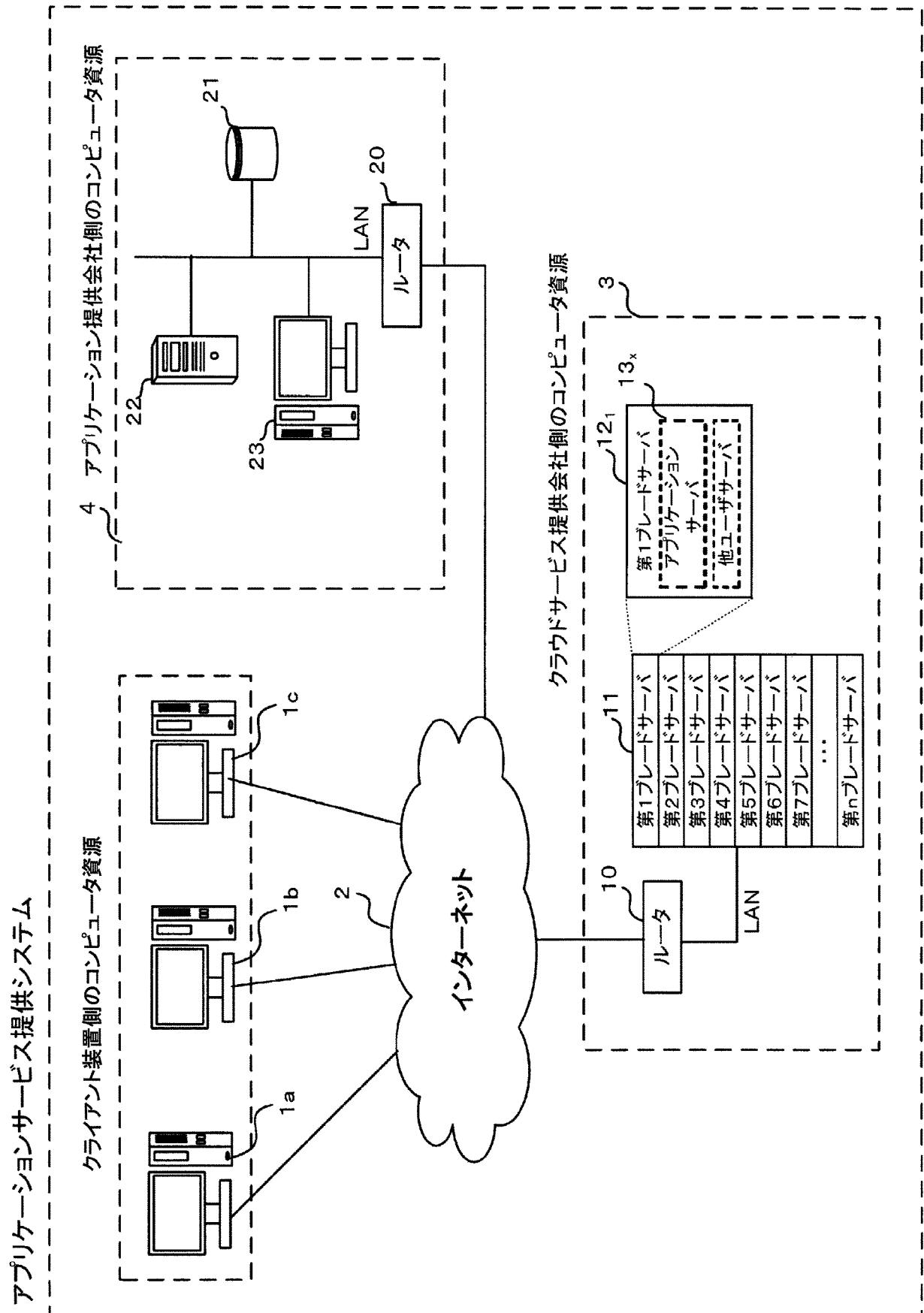
前記仮想マシンが、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要であると判定されると、前記企業内データベースサーバとの間でセキュアな通信を行って、前記企業内データベースサーバに対して、前記クライアント装置からの要求に応じた処理を行う要求ステップと、

前記企業内データベースサーバが、前記仮想マシンからの要求に応

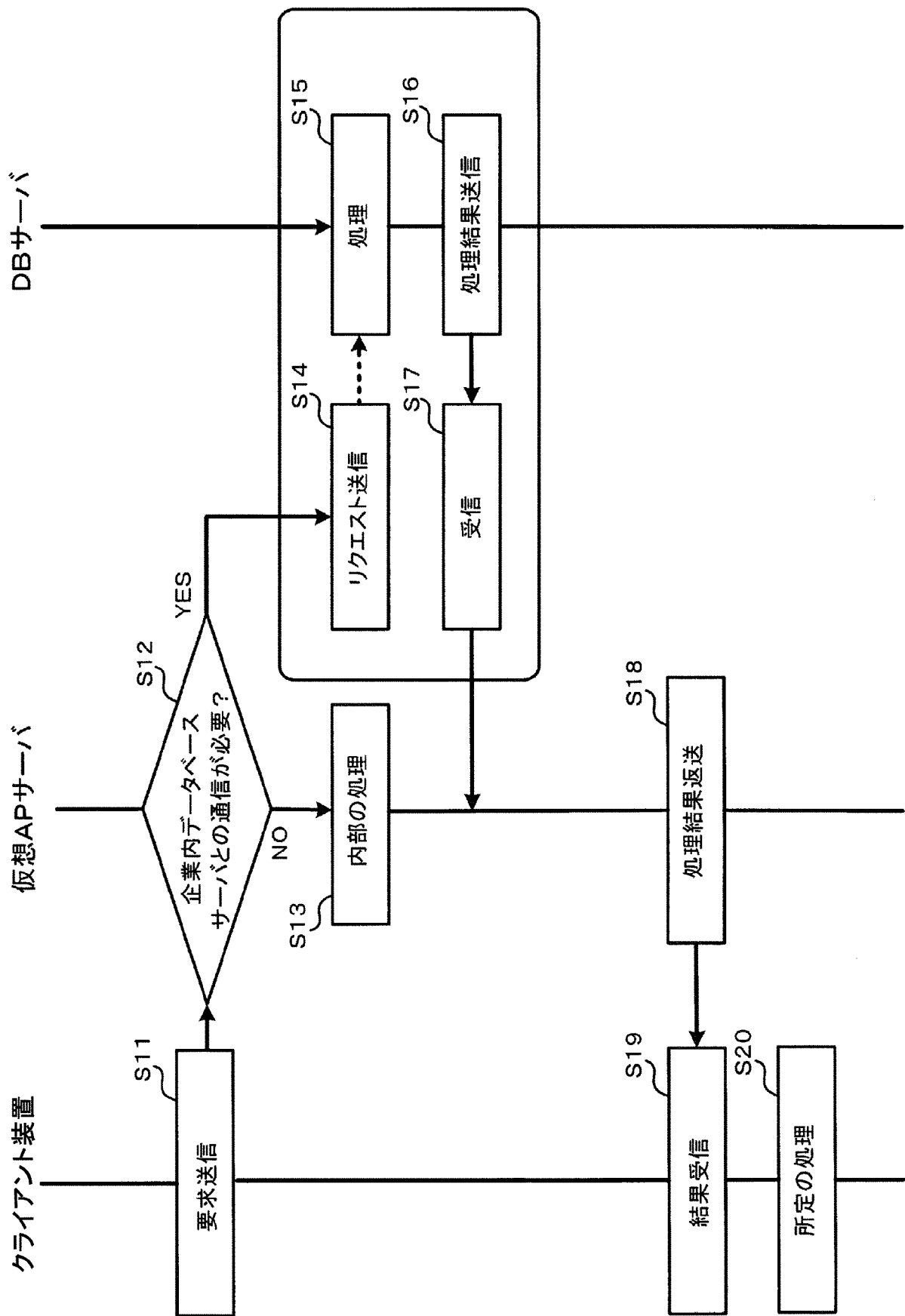
じて、前記企業内秘匿情報を記憶した記憶手段から前記企業内秘匿情報の検索、変更又は削除、又は前記記憶手段への企業内秘匿情報の追加を行う記憶処理ステップと、

前記仮想マシンが、前記判定ステップにより前記企業内秘匿情報に基づく処理が必要ではない判定されると、前記クライアント装置からの要求に応じた処理を行う処理ステップと、有することを特徴とするアプリケーションサービス提供方法。

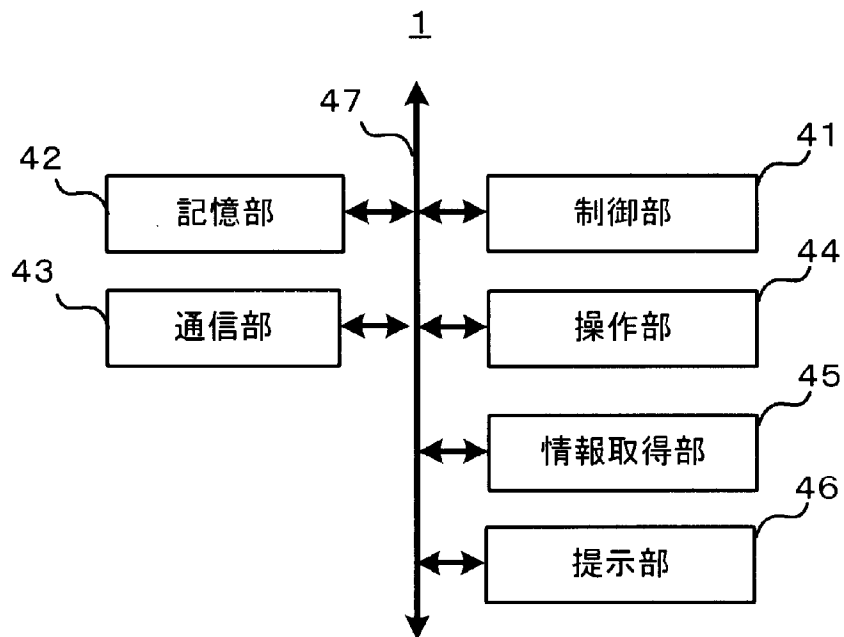
[図1]



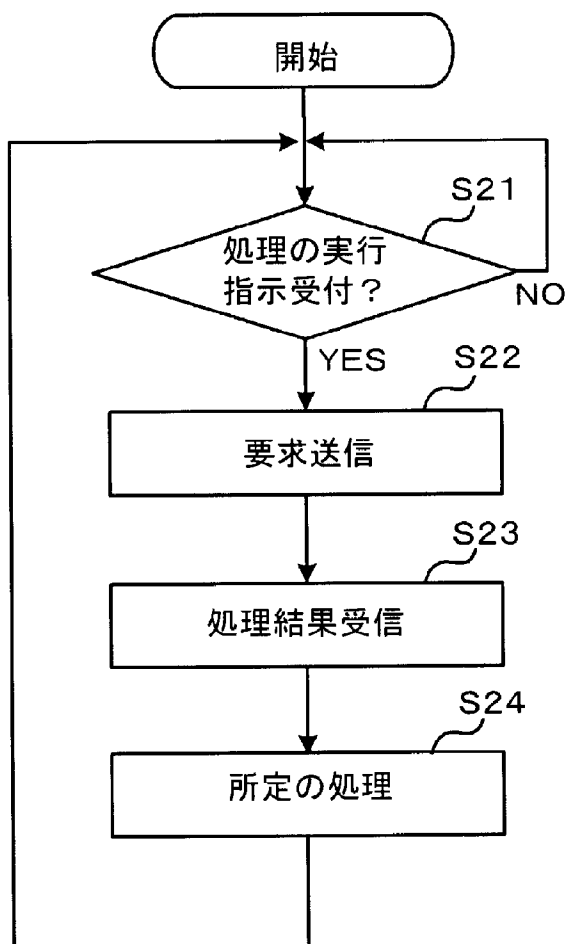
[図2]



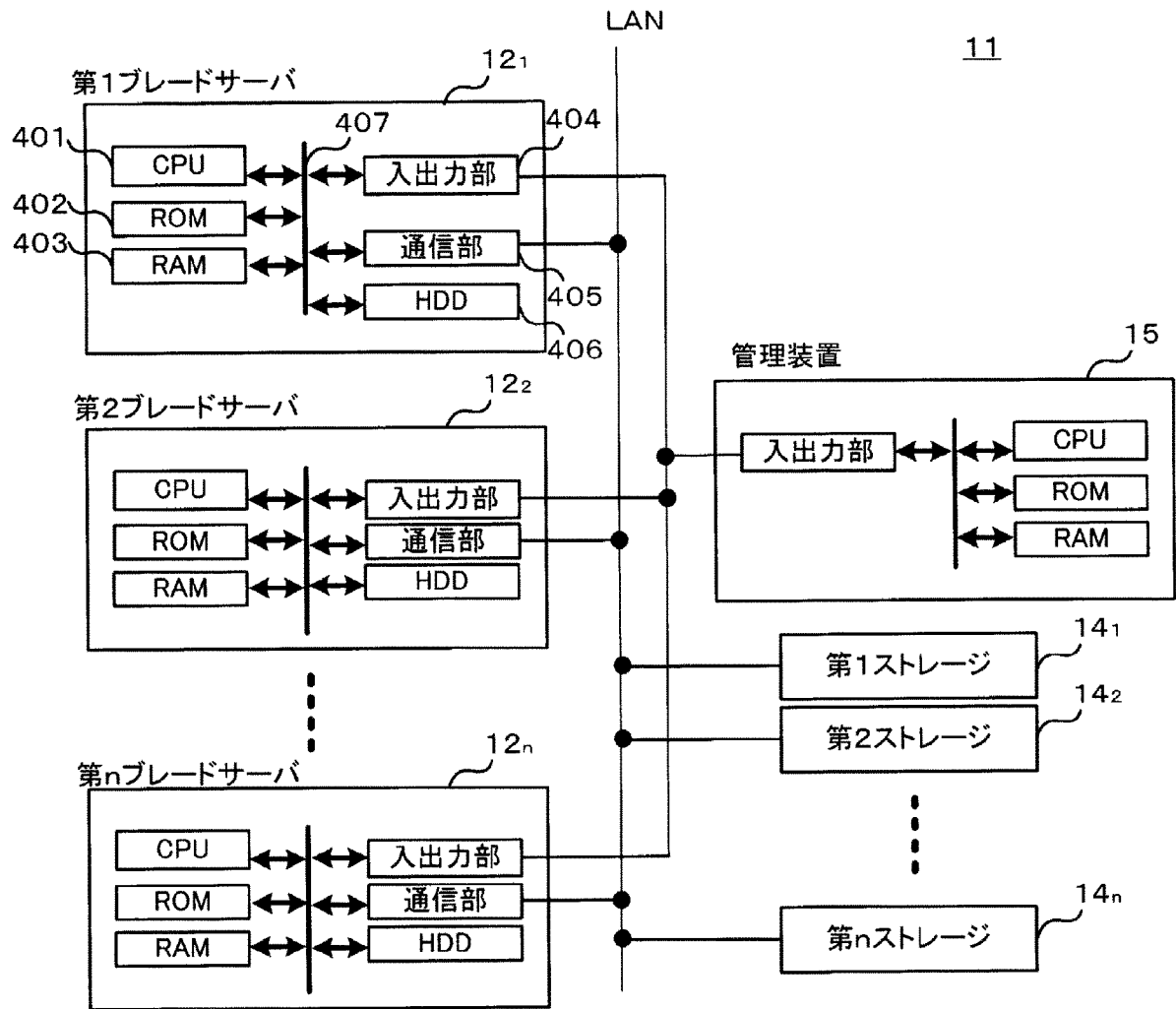
[図3]



[図4]

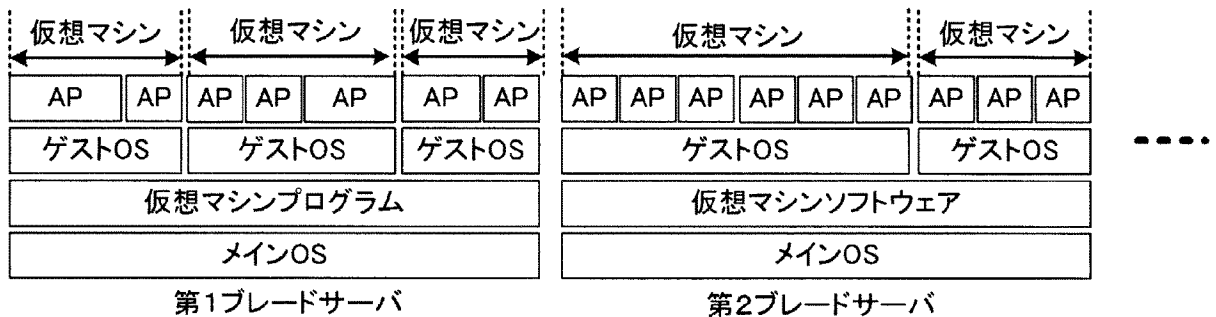


[図5]

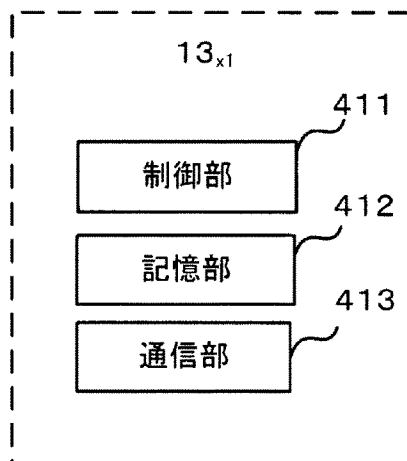


[図6]

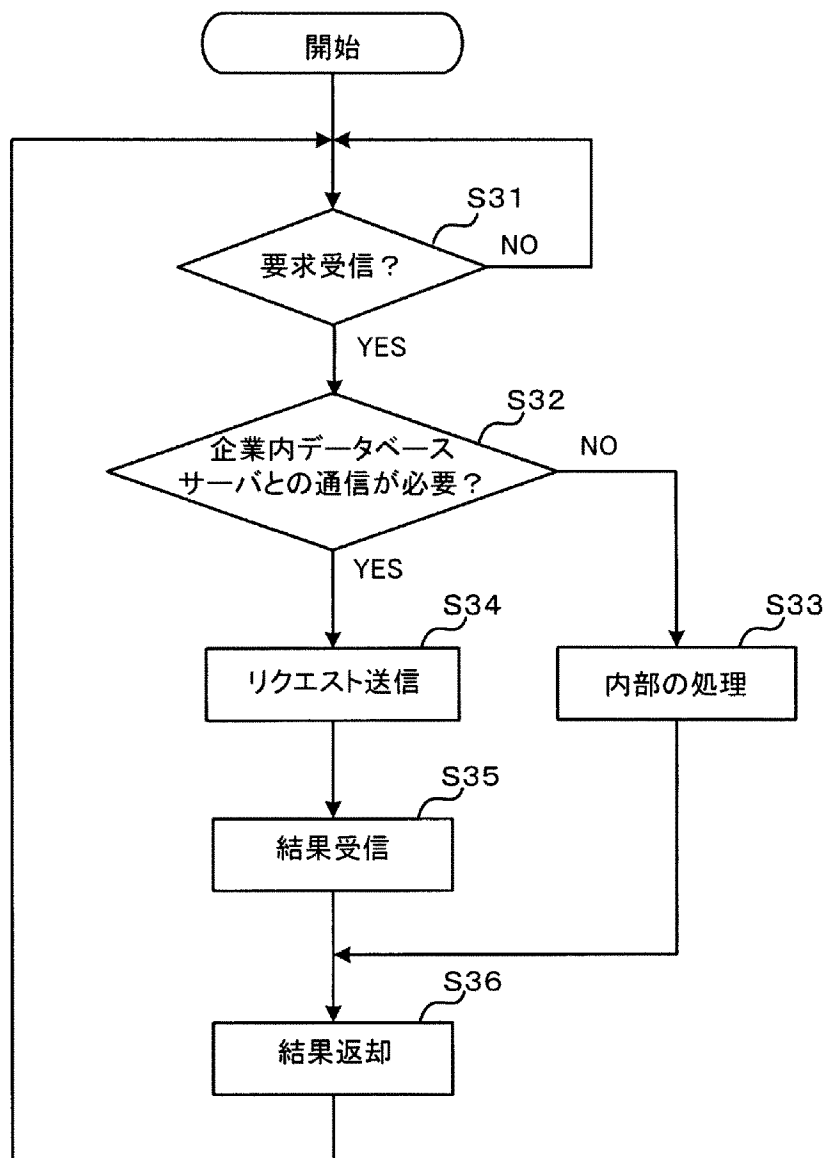
サーバシステムのアーキテクチャ



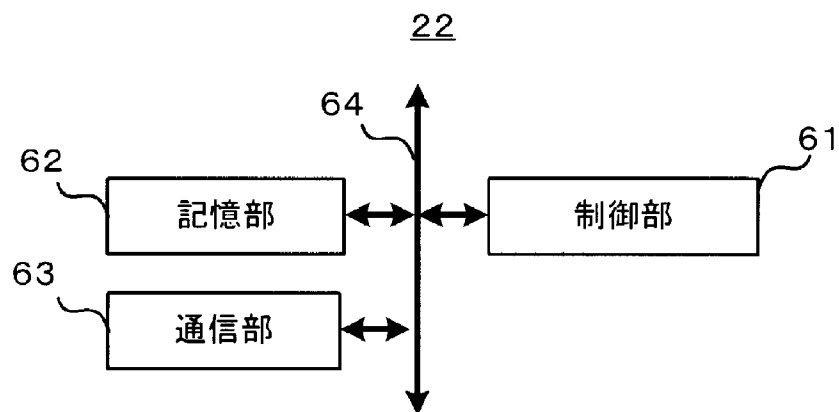
[図7]



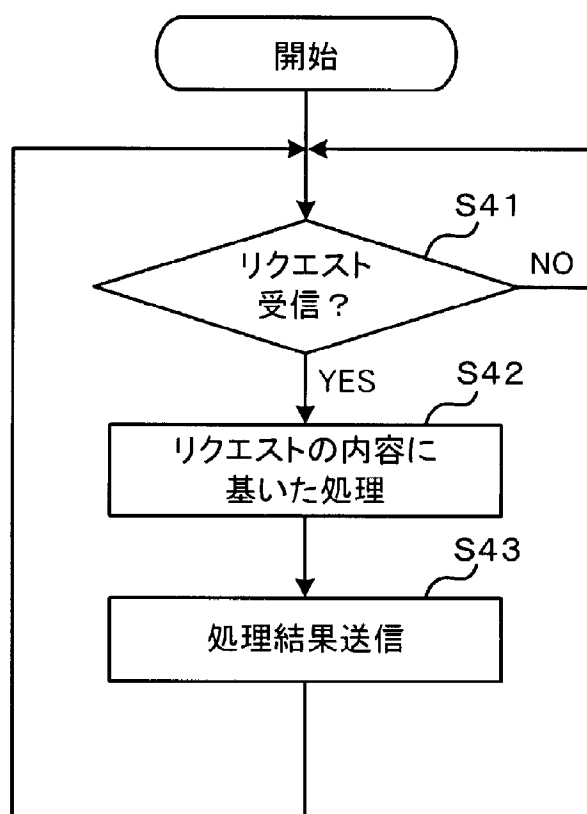
[図8]



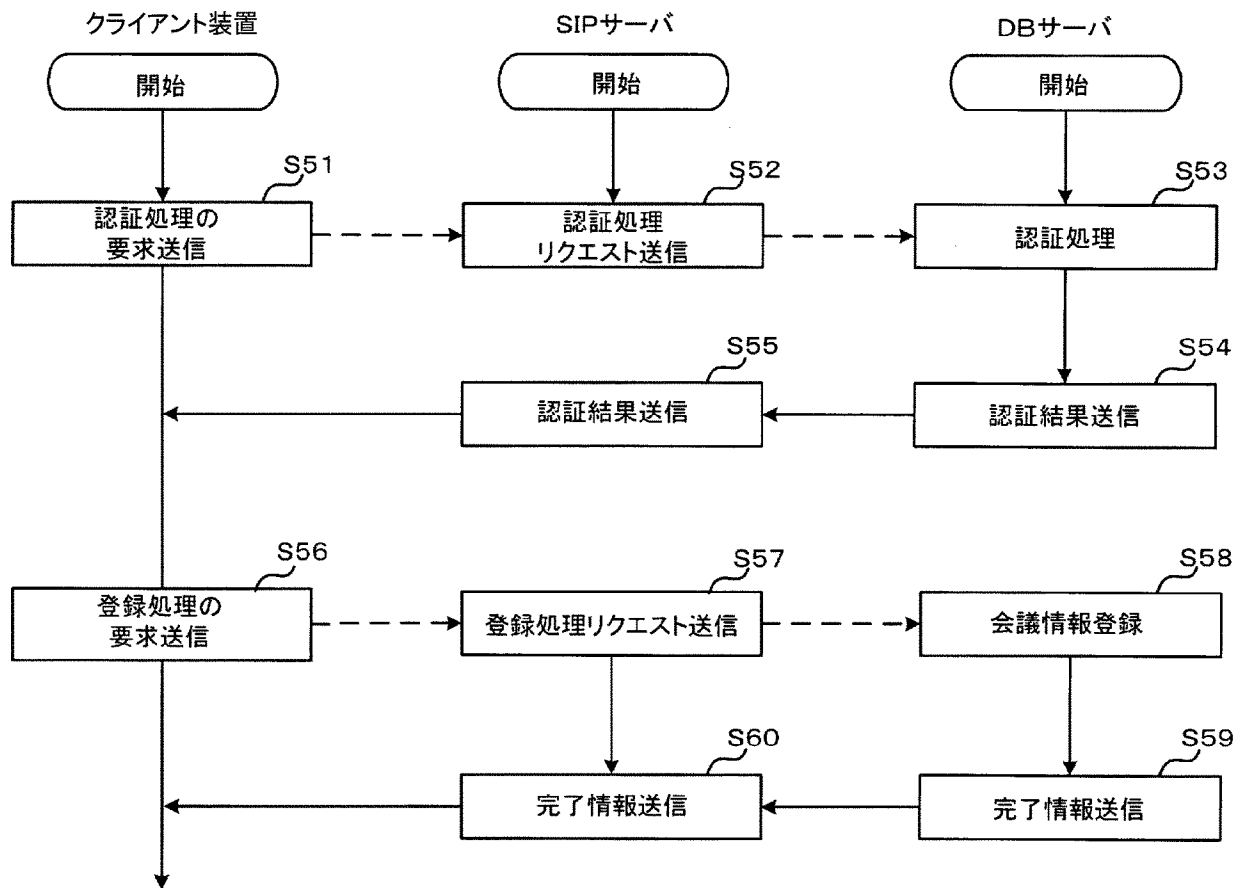
[図9]



[図10]



[図11]



[図12]

拠点ID	IPアドレス	Password	担当者名	電話番号	会社名	サービス内容	メールアドレス
0000001	111.111.111.111	pass1	兄弟 一郎	000-000-0000	A社	プランA	*****
0000002	222.222.222.222	pass2	兄弟 二郎	000-000-0001	B社	プランA	*****
0000003	-	pass3	兄弟 三郎	000-000-0002	C社	プランA	*****
0000004	-	pass4	兄弟 四郎	000-000-0003	D社	プランA	*****
0000005	-	pass5	兄弟 五郎	000-000-0004	E社	プランB	*****
0000006	111.111.111.112	pass6	兄弟 六郎	000-000-0005	F社	プランC	*****
0000007	111.111.111.113	pass7	兄弟 七郎	000-000-0006	F社	プランC	*****
0000008	-	pass8	兄弟 八郎	000-000-0007	F社	プランC	*****
0000009	-	pass9	兄弟 九郎	000-000-0008	G社	プランB	*****
0000010	-	pass10	兄弟 十郎	000-000-0009	H社	プランA	*****

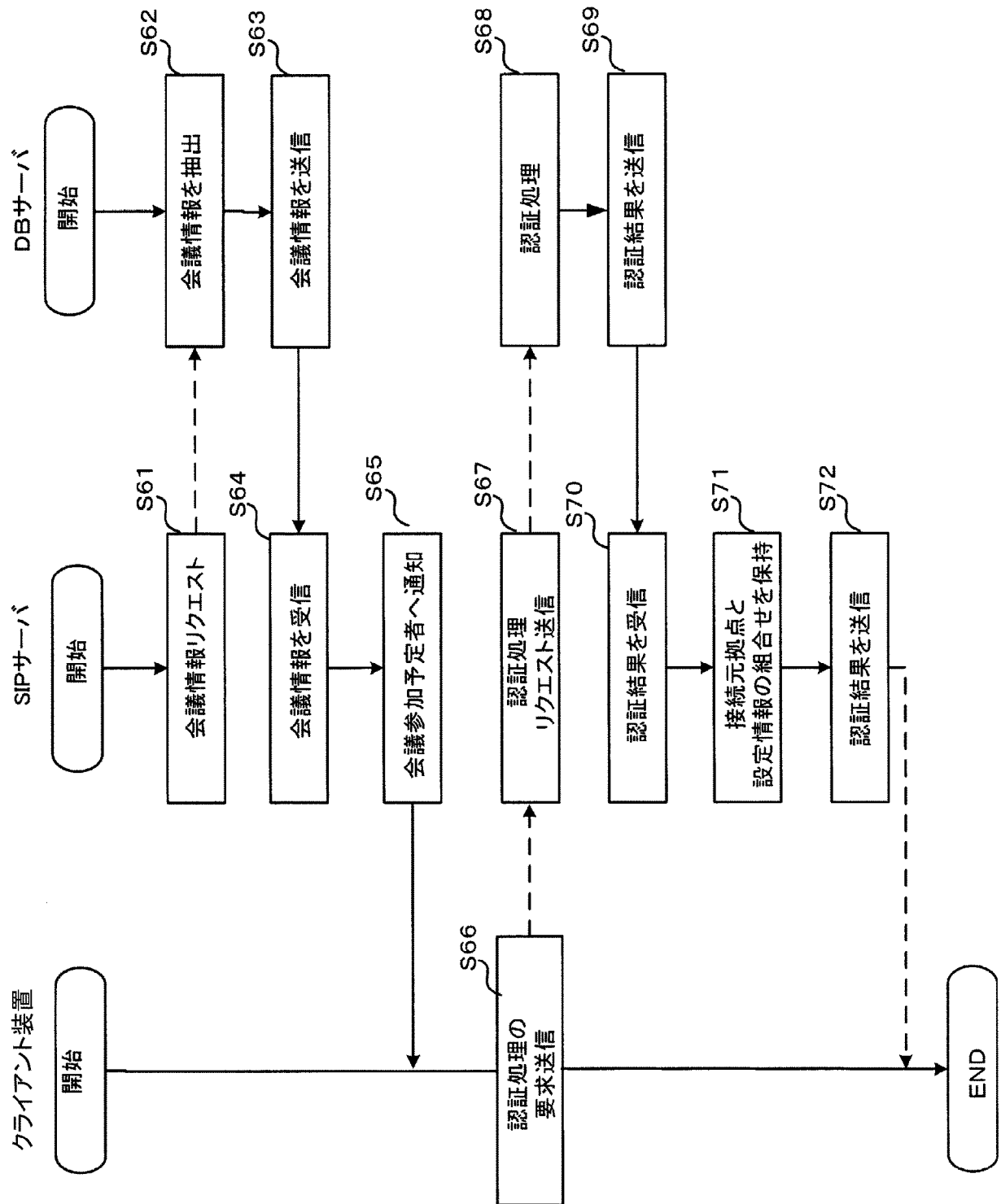
[図13]

会議ID	開催拠点ID	予定開始時間	予定終了時間
90000001	0000001	2009/1/1 0:00	2009/1/1 1:00
90000002	0000003	2009/1/2 0:00	2009/1/2 1:00
90000003	0000002	2009/1/3 0:00	2009/1/3 1:00
90000004	0000009	2009/1/4 0:00	2009/1/4 1:00

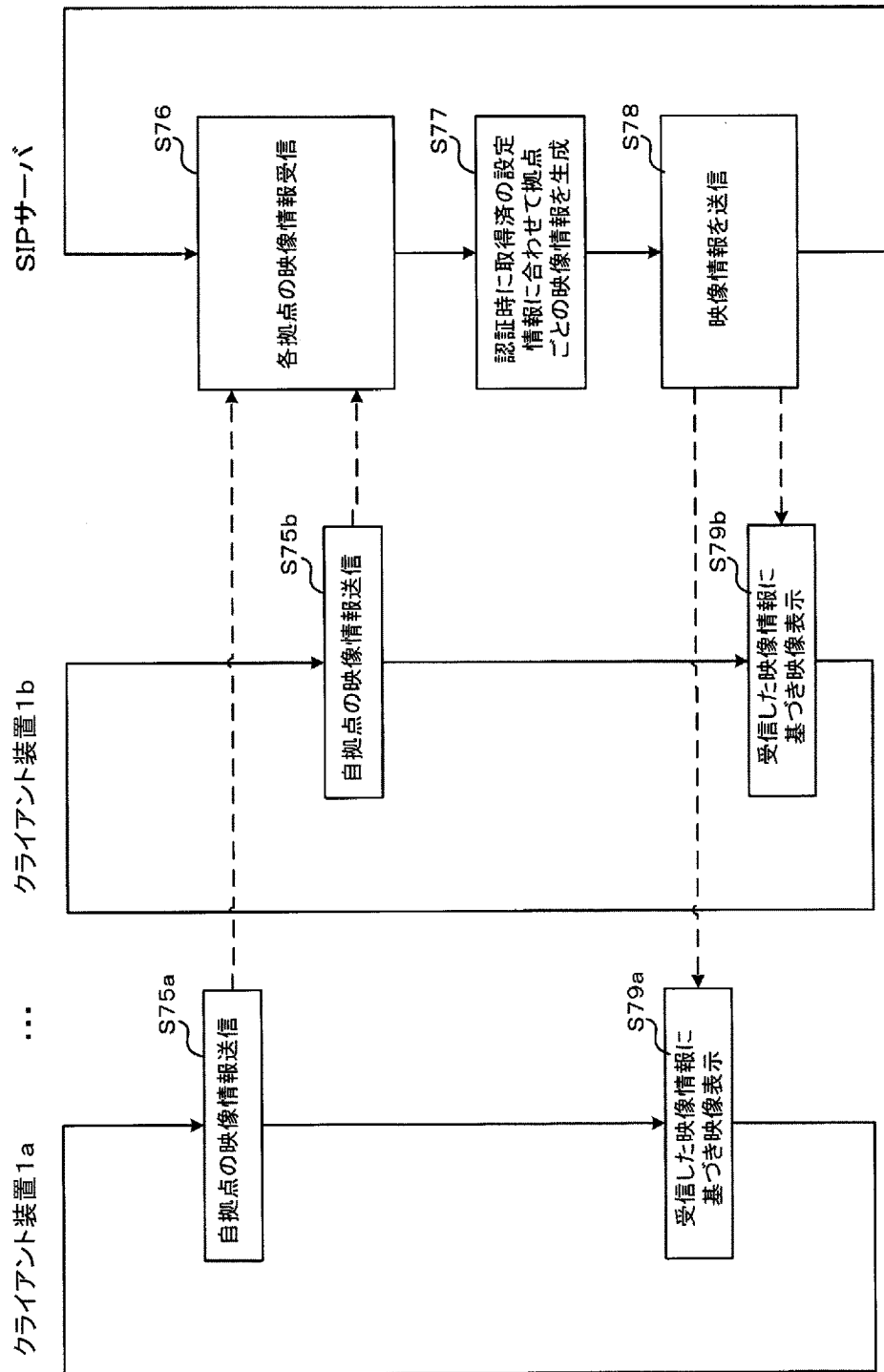
[図14]

会議ID	会議参加拠点ID	設定情報
90000001	0000001	1
90000001	0000002	6
90000001	0000003	4

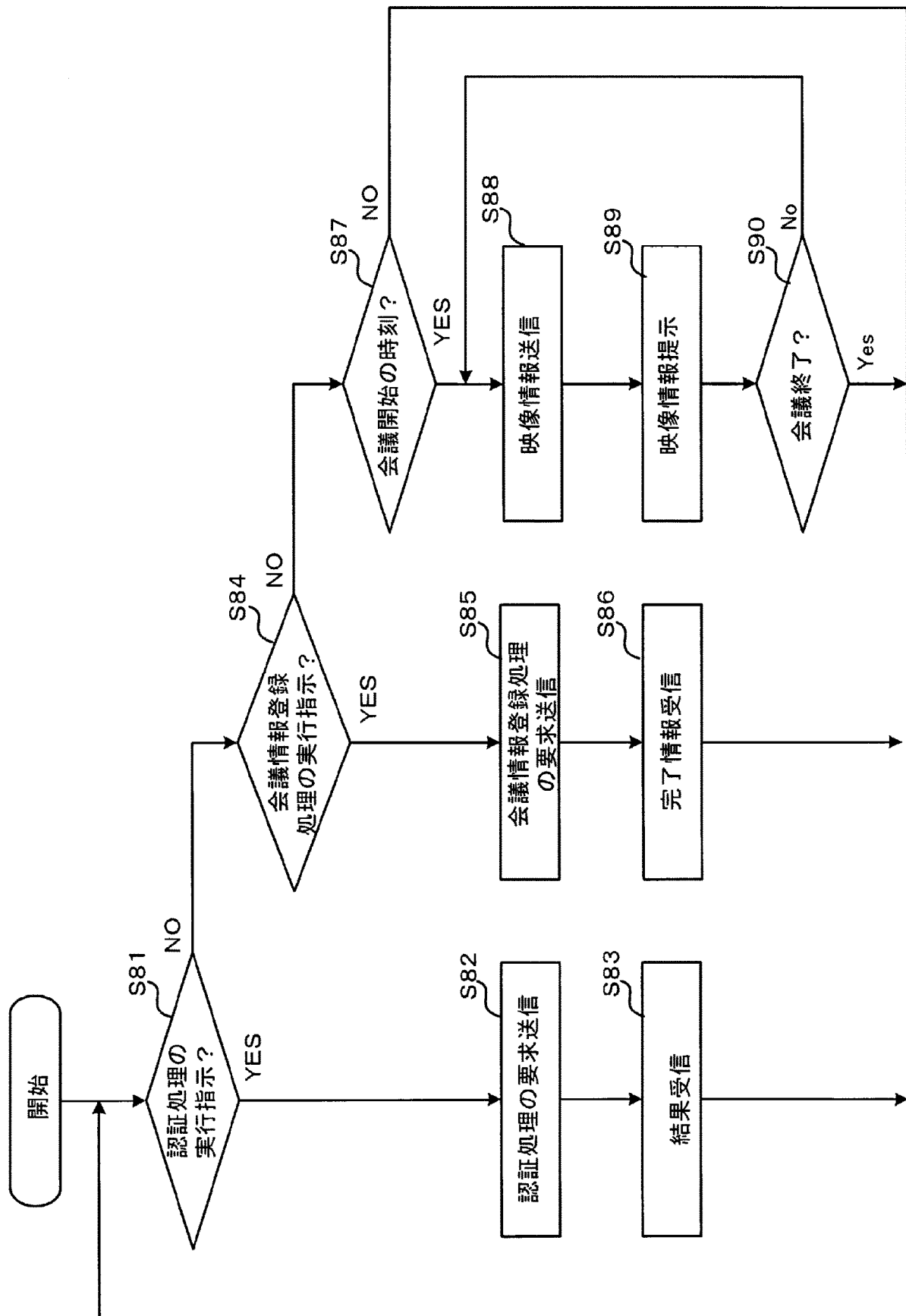
[図15]



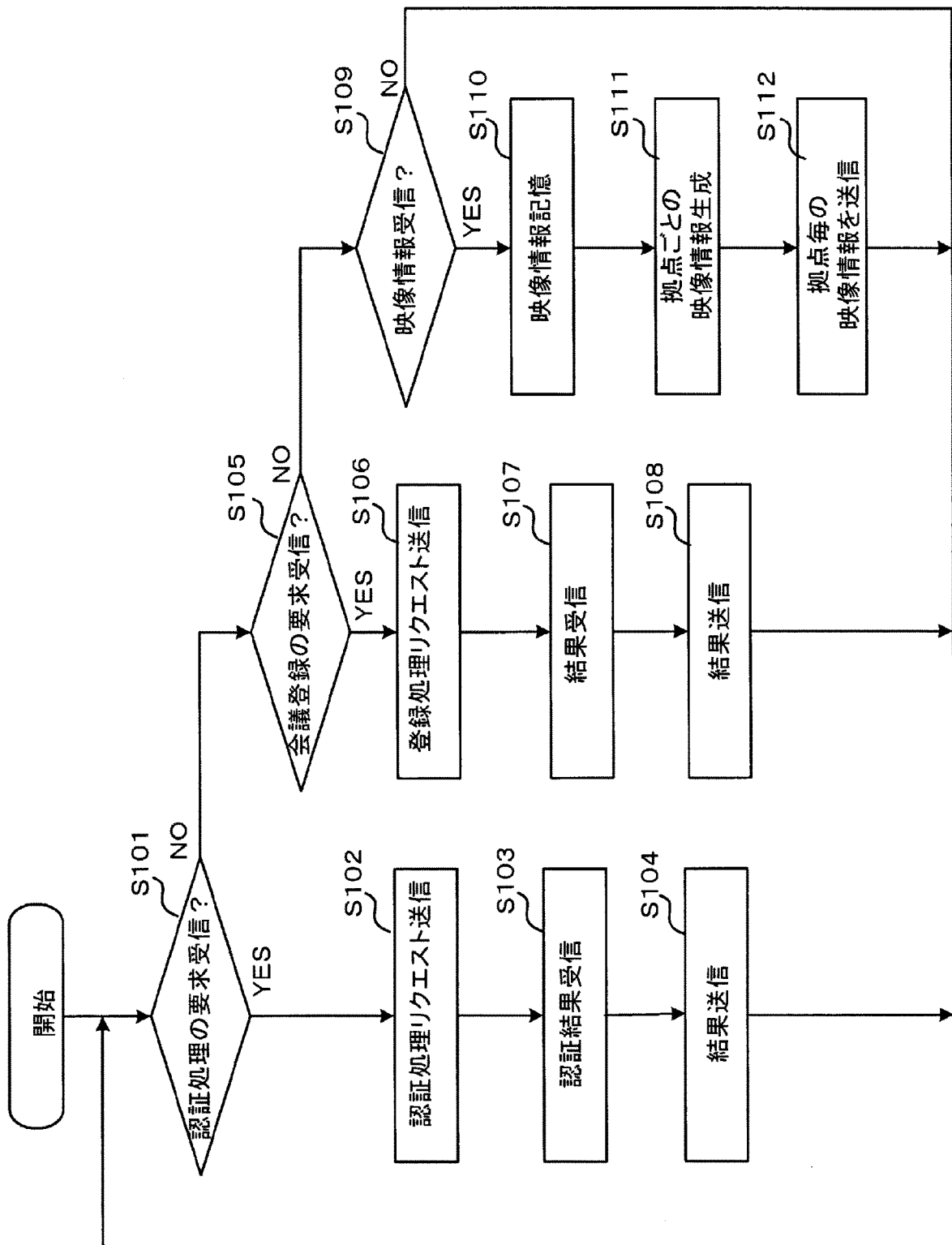
[図16]



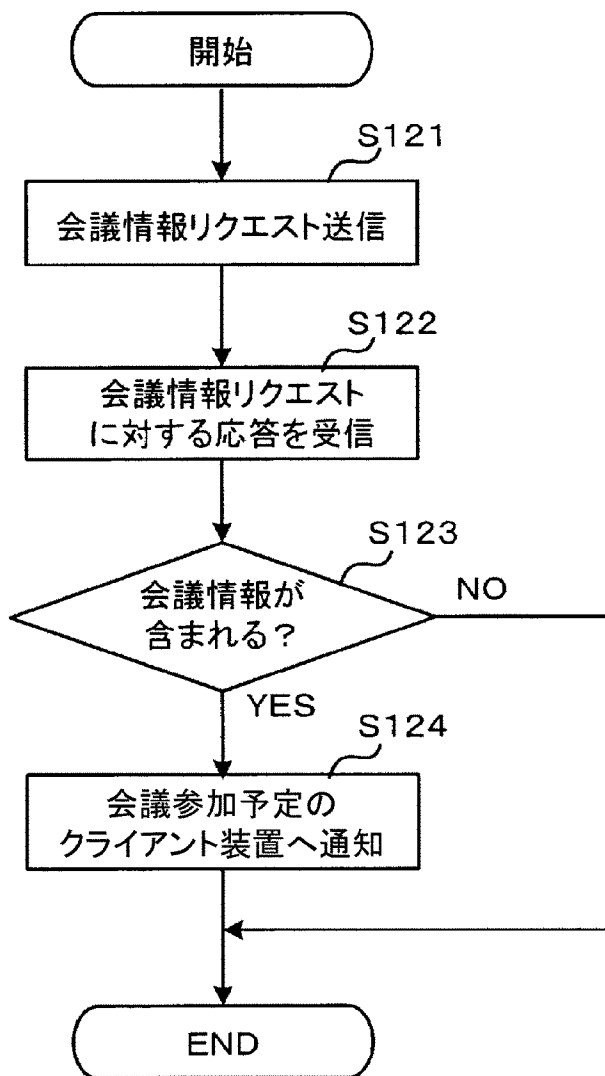
[図17]



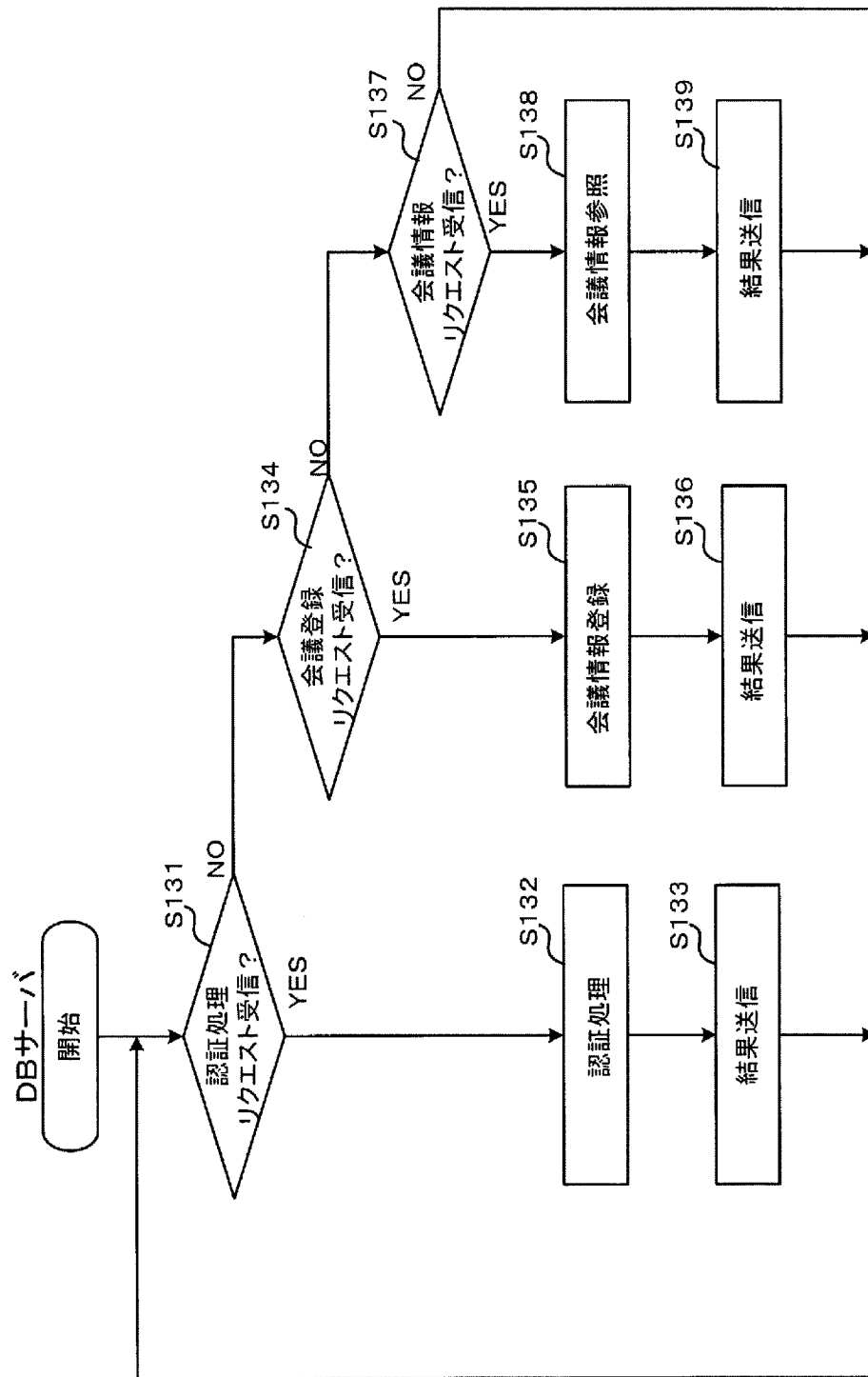
[図18]



[図19]



[図20]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/065375

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/20(2006.01)i, G06F9/46(2006.01)i, G06Q50/00(2006.01)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)

G06F21/20, G06F9/46, G06Q50/00

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2010

Kokai Jitsuyo Shinan Koho 1971-2010 Toroku Jitsuyo Shinan Koho 1994-2010

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.
Y	Tatsuji SHIMOE, 'The Progress and Transition of Identity Management Related Technologies (Web Identity and Artificial Intelligence)', Journal of Japanese Society for Artificial Intelligence, The Japanese Society for Artificial Intelligence, 01 July 2009 (01.07.2009), vol.24, no.4, pages 504 to 511, page 508, left column, line 31 to right column, line 7, fig. 5	1-7

☒ 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
05 October, 2010 (05.10.10)Date of mailing of the international search report
12 October, 2010 (12.10.10)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/065375

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-503011 A (Ernst & Young LLP), 29 January 2004 (29.01.2004), claim 1; paragraphs [0146] to [0151]; fig. 4 & EP 1297446 A2 & EP 1297446 B1 & WO 2002/003220 A2 & US 2002/0069369 A1 & US 7448079 B2 & MX PA02012728 A & ES 2249450 T3 & DK 1297446 T3 & DE 60113539 T2 & CN 1448017 A & CA 2414869 C & AU 6771901 B2 & AU 6771901 C1	1-7
Y	Noboru KURUMAI et al., 'Identity Management from SaaS Application Platform(Web Identity and Artificial Intelligence)', Journal of Japanese Society for Artificial Intelligence, The Japanese Society for Artificial Intelligence, 01 July 2009 (01.07.2009), vol.24, no.4, pages 552 to 558 page 557, right column, lines 5 to 12, fig. 8	3, 6, 7
A	page 557, left column, lines 1 to 13, fig. 7	1-7

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/20(2006.01)i, G06F9/46(2006.01)i, G06Q50/00(2006.01)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. G06F21/20, G06F9/46, G06Q50/00

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 年

国際調査で使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
Y	下江達二, 「WebアイデンティティとAI アイデンティティ管理関連技術の進展と変遷」, 人工知能学会誌, 社団法人人工知能学会, 2009.07.01, 第24巻, 第4号, 第504-511頁 第508頁左欄第31行-右欄第7行, 図5	1-7
Y	JP 2004-503011 A (アーンスト&ヤング エルエルビー) 2004.01.29 【請求項1】, 段落【0146】 - 【0151】 , 【図4】 & EP 1297446 A2 & EP 1297446 B1 & WO 2002/003220 A2	1-7

☒ 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

0 5 . 1 0 . 2 0 1 0

国際調査報告の発送日

1 2 . 1 0 . 2 0 1 0

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）

間野 裕一

5 S

9 7 4 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 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
	& US 2002/0069369 A1 & US 7448079 B2 & MX PA02012728 A & ES 2249450 T3 & DK 1297446 T3 & DE 60113539 T2 & CN 1448017 A & CA 2414869 C & AU 6771901 B2 & AU 6771901 C1	
Y	車井登他, 「WebアイデンティティとAI SaaSアプリケーションプラットフォームから見たアイデンティティ管理」, 人工知能学会誌, 社団法人人工知能学会, 2009.07.01, 第24巻, 第4号, 第552-558頁	3, 6, 7
A	第557頁右欄第5行-第12行, 図8 第557頁左欄第1行-第13行, 図7	1-7