

明 細 書

発明の名称：クラウドセキュリティ管理システム

技術分野

[0001] 本発明は、クラウドコンピューティング等の情報処理の技術に関する。特に、利用者のプログラムをクラウド環境で実行させる場合のセキュリティ管理に関する。

背景技術

[0002] クラウドコンピューティングシステムとして、各種のパブリッククラウドが存在する。例えばWindows Azure（登録商標）、Amazon EC2（登録商標）、等がある。不特定の一般の利用者は、パブリッククラウド（そのリソース・サービス処理等）を利用する場合、利用者の端末等からパブリッククラウドのサーバ等にアクセスし、仮想サーバにより提供されるサービス処理やストレージのデータ等を利用して、利用者の所望のソフトウェアプログラム処理（Webアプリケーション処理やバッチ処理など）を実現する。利用者は、パブリッククラウド（そのサービス）との契約に基づき、利用者のプログラムをパブリッククラウドのサーバ（仮想サーバ）で実行させることができる。各種のパブリッククラウド及びその各種のサービスに応じて、利用方法や課金方式は様々である。

[0003] 上記のように利用者のプログラムをパブリッククラウド等のクラウド環境で実行させる場合、利用者のプログラムの実行の正当性を確認して成りすまし等を防止しセキュリティを確保することが必要である。

[0004] プログラム（ソフトウェア）の認証・セキュリティ管理などに係わる先行技術例として、特開2004-46606号公報（特許文献1）などがある。特許文献1などでは、プログラム（ソフトウェア）のライセンスをチェックしてマシン（利用者の端末）でのプログラムの実行を許可するか判断する旨の技術が記載されている。

先行技術文献

特許文献

[0005] 特許文献1：特開2004-46606号公報

発明の概要

発明が解決しようとする課題

[0006] 前記特許文献1などの先行技術例では、利用者の端末でのプログラムの実行の権限を確認することができるが、クラウド環境に対応した技術（例えば利用者プログラムの処理を実行するサーバ（仮想サーバ）等まで含めた認証や認可などを行う技術）ではないため、クラウド環境でのセキュリティの確保のためには不十分である。

[0007] また、パブリッククラウド等のクラウド環境において利用者プログラム（その処理）をサーバ（仮想サーバ）で実行させるサービスを提供する従来システムは、サーバでの利用者プログラムの実行の正当性を確認する手段（機能）が不十分である。即ち、従来のパブリッククラウド等では、仮想サーバのレベルでみると、1つの仮想サーバでは特定の利用者のプログラムのみ実行されるように占有利用する形態であり、1つの仮想サーバで複数の利用者のプログラムを実行させようとした場合には、セキュリティの確保が不十分となる（図8）。言い換えると、ある利用者のプログラム（例えばWebアプリケーション処理用のプログラムやバッチ処理用のプログラム）を、あるパブリッククラウドのサーバ（仮想サーバ）を利用して実行させる場合、セキュリティを確保するために、その利用者のプログラムをそのパブリッククラウドのサーバで本当に実行してもよいかどうか、実行の正当性を確認することが必要である。しかしその手段（機能）が不十分であり、クラウド環境でのセキュリティ確保などに関して検討余地がある。より詳しくは以下に例示する問題（課題）がある。

[0008] 例えばクライアントからサーバへのアクセスやサーバ間でのアクセスが発生する場合、一般的にはWebサービスなどのAPI呼び出しの形式であり、その際にID及びパスワードをベースとした認証ないし認可が行われることでセキュリティが向上できる。

[0009] 例えば従来システムのパブリッククラウド（例えばWindows Azure）では、仮想サーバ（例えばWebロールやWorkerロール）を利用者に対して公開して当該仮想サーバで利用者プログラムを実行させることができる。このような従来システムでは、利用者プログラムを利用者端末からクラウド環境（サーバ）へアップロード（登録）する際に、当該利用者プログラムの認証（ID及びパスワードをベースとした認証（権限確認など））を行っている。しかしながらそのアップロード（及び認証）以降では、その利用者プログラムをクラウド環境内にある各サーバで実行してもよいかどうかに関する認証・認可は行われぬか、あるいは行われてもそのための処理及び作業に手間がかかっている。即ちクラウド環境での効果的な制御・セキュリティ管理が実現できていない。

[0010] 上記従来システム例で、アップロード以降、パブリッククラウド内で利用者プログラムの処理を実行させる第1のサーバから更に他の機能やリソースを持つ第2のサーバにアクセスして処理を行う場合、その際のアクセスごとに及び第2のサーバの種類ごとに、上記ID及びパスワードによる認証・認可を要している。例えば利用者は、利用者プログラムのコード内に、上記各サーバへのアクセスごとのID及びパスワード等を記述する煩雑な作業を要し、管理コストが高い。

[0011] また特に、インターネット上、複数の利用者の複数のプログラム（利用者プログラム）、複数のパブリッククラウドの複数のサーバ（仮想サーバ）等が存在し、パブリッククラウドのサーバを共用して複数の利用者のプログラムを実行させる形態が考えられる。その場合、どの利用者のプログラムをどのパブリッククラウドのサーバ（共用サーバ）で実行させるかを制御・管理することになるが、この場合にも上記同様に、各サーバへのアクセス時などに本当にその利用者プログラムをそのサーバで実行してもよいかどうか、実行の正当性を確認してセキュリティを確保することが必要になってくると考えられる。

[0012] なお本発明者による関連する出願として、PCT/JP2012/056

039（クラウド共用型リソース提供システム）がある。この出願では、複数の利用者（端末）と複数のパブリッククラウドとの間に、利用者に対しパブリッククラウドのサーバによる共用リソース（共用サーバ）を提供する事業者（リソースプロバイダ）を設け、当該共用サーバで複数の利用者プログラムを実行可能とする技術について記載している。このシステムでも上記のように、どの利用者のプログラムをどのパブリッククラウドの共用サーバで実行するかに関するセキュリティ管理の問題が生じる。

[0013] 以上を鑑み、本発明の主な目的は、上記クラウド環境（仮想サーバ等）で利用者のプログラムを実行させる場合（１つの仮想サーバで複数の利用者のプログラムを実行させる場合）のセキュリティ確保などの問題を解決できる技術を提供することである。特に複数の利用者と複数のパブリッククラウド等を含むクラウド環境で、どの利用者のプログラムをどのパブリッククラウドのサーバ（共用サーバ等）で実行するかに関する認証・認可（正当性、権限の確認など）を行うことでセキュリティ確保や効果的な制御・管理が実現できる技術を提供することである。

課題を解決するための手段

[0014] 上記目的を達成するため、本発明のうち代表的な形態は、インターネット上、パブリッククラウド等のクラウド環境（仮想サーバ等）で利用者のプログラムを実行させ、その際のセキュリティ管理を行うコンピュータシステム（「クラウドセキュリティ管理システム」）であって、以下に示す構成を有することを特徴とする。

[0015] 本形態のシステムは、例えば、利用者の端末と、複数のサーバを含むパブリッククラウドと、認証サーバとを含む要素がネットワークで接続される。前記パブリッククラウド内には、前記利用者のプログラムを実行させる対象となるサーバと、当該サーバを管理するための制御処理を行うコントローラとが設けられる。前記認証サーバは、認証制御部と、記憶部とを有する。前記記憶部は、前記利用者のＩＤを含む情報と、前記利用者のプログラムのＩＤを含む情報と、前記パブリッククラウドのＩＤを含む情報と、前記サーバ

のIDを含む情報と、前記利用者のプログラムと前記パブリッククラウドのサーバとの実行の関連付けを管理するための許可情報と、を格納する。前記認証制御部は、前記利用者のプログラムを認証するための第1の認証情報を作成し、前記利用者のプログラムに前記第1の認証情報を同梱させる、第1の処理部と、前記パブリッククラウドのサーバを認証するための第2の認証情報を作成し、対象のパブリッククラウドのサーバに提供する、第2の処理部と、前記利用者の端末からの入力に応じて前記許可情報の内容を設定する第3の処理部と、前記利用者のプログラムを前記パブリッククラウドのサーバで実行させる際に、前記コントローラと連携して、前記第1の認証情報、前記第2の認証情報、及び前記許可情報を参照し、当該利用者のプログラムを当該パブリッククラウドのサーバで実行許可するか判定して許可の場合は実行させる、第4の処理部と、を有する。

発明の効果

[0016] 本発明のうち代表的な形態によれば、上記クラウド環境（仮想サーバ等）で利用者のプログラムを実行させる場合（1つの仮想サーバで複数の利用者のプログラムを実行させる場合）のセキュリティ確保などの問題を解決できる。特に複数の利用者と複数のパブリッククラウド等を含むクラウド環境で、どの利用者のプログラムをどのパブリッククラウドのサーバ（共用サーバ等）で実行するかに関する認証・認可（正当性、権限の確認など）を行うことでセキュリティ確保や効果的な制御・管理が実現できる。結果、利用者はパブリッククラウド等のリソースを容易・安価に利用することができる。

図面の簡単な説明

[0017] [図1]本発明の一実施の形態のシステム（クラウドセキュリティ管理システム）の全体の構成を示す図である。

[図2]本システムでの要素間の処理シーケンス例を示す図である。

[図3]本システムでのパブリッククラウド側の登録時の構成例を示す図である。

[図4]本システムでの利用者側の登録時の構成例を示す図である。

[図5]本システムでの実行制御時及び認証時の構成例を示す図である。

[図6]本システムでの管理情報の構成例を示す図である。

[図7]本システムでの共用例を示す図である。

[図8] (a) 従来の仮想サーバの利用の形態、(b) 本システムでの仮想サーバ（共用サーバ）の利用の形態を示す図である。

発明を実施するための形態

[0018] 以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一部には原則として同一符号を付し、その繰り返しの説明は省略する。

[0019] [概要等]

本実施の形態のシステム（クラウドセキュリティ管理システム）は、図1のシステム構成において、図2（図3～図5）のような処理を行い、図6のようなデータ情報を管理し、図7のようにクラウド環境でのリソース共用を可能とする。

[0020] 前提として、図8で、(a)は、従来のパブリッククラウド例での仮想サーバの利用の形態を示し、(b)は、本実施の形態のシステムでの仮想サーバ（共用サーバ）の利用の形態を示す。(a)で、物理サーバ及びそのOS上に、複数の仮想サーバ（#1～#M）が構成されている。仮想サーバのレベルでみると、1つの仮想サーバでは、特定の利用者（U）の1つ以上のプログラム（UP）のみが実行されるように、一対一の関係付けで占有利用する形態である。一方、(b)で、本システムでは、パブリッククラウドにおける物理サーバ（33）及びそのOS（32）上に構成される複数の仮想サーバ（31）において、共用サーバとなる1つの仮想サーバ（31）では、複数の利用者（U）のプログラム（UP）が実行（許可）されるように、共同利用する形態である。本システムではこの利用の形態におけるセキュリティを確保する機能を備える。

[0021] 図1等のように、本システムでは、特に、複数の利用者U2（端末2）と複数のパブリッククラウド3との間に介在する事業者のシステム（認証局1

）を設ける。認証局（認証サーバ）１では、利用者のプログラムをパブリッククラウド３のサーバ（仮想サーバ）で実行させる際の認証・認可など（実行の正当性の確認、権限確認など）の処理を行う機能（認証制御部１３）を備える。これにより、クラウド環境でのセキュリティ確保／向上や、複数の利用者Ｕ２と複数のパブリッククラウド３との間での効果的な関連付けの制御・管理などを実現する。特に、本システムは、パブリッククラウド３のサーバを共用して複数の利用者のプログラムを実行させる機能（共用リソース提供サービス）を提供する。本機能では、利用者の要求・契約や、パブリッククラウド３の要求・契約や、特有の制御方式・課金方式や、通信・負荷の状況などに応じて、認証局（認証サーバ）１は、どの利用者Ｕ２のプログラム（ＵＰ）をどのパブリッククラウド３の仮想サーバ（共用サーバ３１）で実行させるかその関連付けを制御・管理する。本システムは、上記パブリッククラウド３のサーバ（共用サーバ３１）で利用者のプログラム（ＵＰ）を実行させる際、認証サーバ１の認証制御部１３を用いて認証処理を行う（当該サーバで当該利用者プログラムの処理を実行してもよいか、実行の正当性、権限を確認する）。

[0022] 本システムでは、第１の認証情報（Ｆ１）を用いて利用者のプログラム（ＵＰ）の認証を行って成りすまし等を防止しセキュリティを高め、第２の認証情報（Ｆ２）を用いてパブリッククラウド３の共用サーバ３１の認証を行って成りすまし等を防止しセキュリティを高め、そして第１、第２の認証情報、及び許可情報（ｄ１）を用いて、利用者プログラム（ＵＰ）と共用サーバ３１との関係付けでの実行に関する認証（確認）を行ってセキュリティを確保する。

[0023] [（１）システム構成]

図１において、本実施の形態のシステム（クラウドセキュリティ管理システム）の全体の構成を示している。なお図１に示す本システムは、基本（前提）となるシステムとしてクラウド共用リソース提供システムを含んでおり、その上にクラウドセキュリティ管理システムを統合的に実装した形態であ

る。言い換えると、本システムは、クラウド共用リソース提供機能（サービス）と、その機能に関するクラウドセキュリティ管理機能（サービス）とを有する構成である。

[0024] 本システムの全体は、認証局（認証サーバ）１と、複数の利用者Ｕ２の端末（利用者端末）２と、複数の各種のパブリッククラウド（ＣＬと略す）３とを有し、これらは通信網（インターネット）で接続される。図１ではＣＬ３の例として、ＣＬ－Ａ，Ｂ，Ｃを有する。なおＣＬ３は、認証局１の事業者が運営するＣＬと、他の各社が運営するＣＬとを含んでもよい。

[0025] （１） 認証局１は、複数の利用者Ｕ２（端末２）と複数のＣＬ３との間に介在して、クラウド共用リソース提供機能及びそれに関連するクラウドセキュリティ管理機能を提供する事業者によるコンピュータシステムであり、認証サーバを含んで構成される。

[0026] 認証局（認証サーバ）１は、ＵＩ部１０と、登録部１１と、実行制御部１２と、認証制御部１３と、ライブラリ５０（記憶部）とを有し、これら各部は例えばＬＡＮ等で接続される。認証制御部１３は、ＵＰ（利用者プログラム）認証情報作成処理１３１と、サーバ認証情報作成処理１３２と、許可情報設定処理１３３と、認証処理１３４（権限確認、許可判定処理）と、を含む各処理を行う処理部を有する。ライブラリ５０は、利用者端末２から登録されるＵＰ（利用者プログラム）データ１０２と、管理情報６０とを有する。管理情報６０として、許可情報ｄ１、利用者情報ｄ２、ＵＰ（利用者プログラム）情報ｄ３、ＣＬ（パブリッククラウド）情報ｄ４、及びサーバ情報ｄ５を有する（図６）。登録されるＵＰデータ１０２は、ＵＰ認証情報ファイルＦ１が含まれている（同梱されている）。なおライブラリ５０のデータ情報は認証局１によりセキュアに管理される。

[0027] 認証サーバ１の各処理部（１０～１３）は、例えば認証サーバ１に備える図示しないプロセッサ、メモリ、通信インタフェース、ＯＳ、入力装置、出力装置、等の公知の要素を用いたソフトウェアプログラム処理で実現される。ライブラリ５０（記憶部）は、例えば認証サーバ１によりアクセス可能な

メモリ、ストレージ、DB及びその入出力制御処理を用いて実現される。

[0028] 認証局1は、クラウド共用リソース提供機能として、登録部11及び実行制御部12等を用いて、複数の利用者U2に対し、利用契約に基づき、複数のCL3によるリソース（共用リソース）を提供する。このリソースとして、各CL3内に設置（設定）される共同利用型の仮想サーバである共用サーバ31を含む。利用者U2は、認証局1（ライブラリ50）に利用者プログラム101（102）を登録することができる。そして共用サーバ31上で複数の利用者U2のプログラム（UP103）を実行させることができる。なお本明細書では、「リソース」とは、利用者（利用者プログラム）から見て利用可能（候補）となる、すべてのCL3と共用サーバ（仮想サーバ）31を含む全体を指すこととする。複数の利用者U2が共用リソース（共用サーバ31）を利用する仕組みにより安価で利用できる。

[0029] UI部10は、利用者U2、CL3の事業者（管理者など）、及び認証局1の事業者（管理者など）の各者に対して、本システムのユーザインタフェース（UI）を提供する処理部であり、例えばWebサーバで実装される。1, 2, 3の各者は、端末などから認証サーバ1のUI部10の提供するWebページにアクセスしてログインし、その画面で各種の設定（登録）や、データ情報の参照や、指示入力などに関する操作が可能である。なお各者は上記ログインのためにWebユーザとしての専用の氏名、ID等（後述の認証情報のID及びパスワード等とは別）を登録し、認証サーバ1は当該Webユーザ情報を管理する。

[0030] 登録部11は、利用者U2によりライブラリ50に各種情報（d2, d3）やUPデータ102を登録する処理や、CL3の事業者（または認証局1の事業者）によりライブラリ50に各種情報（d4, d5）を登録する処理などを行う。

[0031] 実行制御部12は、利用者U2からの指示に基づき、ライブラリ50に登録済みのUPデータ102を、対象のCL3の共用サーバ31で実行させる制御処理を行う。

[0032] 認証制御部 13 は、クラウド共用リソース提供機能に関連したクラウドセ

キュリタイ管理機能を実現する。UP 認証情報作成処理 131 では、利用者 U2 側による登録時 (図 3) に、UP 認証情報 F1 を作成し、利用者 U2 (132 では、CL3 側による登録時 (図 2) に、サーバ認証情報 F2 を作成し、CL3 の事業者 (共用サーバ 31) に対して提供する処理などを行う。

許可情報設定処理 133 では、利用者 U2 側による登録時 (図 3) に、許可情報 d1 などを設定する処理を行う。認証処理 134 では、UP 102 (103) を共用サーバ 31 で実行しようとする際 (実行制御時及び認証時 (図 4)) に、上記の F1, F2, d1 等を参照して認証処理 (実行の正当性、権限を確認する処理) を行う。

[0033] (2) 利用者端末 2 は、不特定の一般の利用者 U2 が使用するコンピュータシステムないし PC 等の端末である。例えば利用者 U2 は企業のプログラマ開発者などである。利用者端末 2 に、利用者 U2 により作成・用意される利用者プログラム (UP) 101 を有する。利用者端末 2 は、図示しないプロセッサ、メモリ、通信インタフェース、OS, Web ブラウザ、入力装置、出力装置、等の公知の要素を用いて実現され、ソフトウェアプログラム処理により、認証局 1 とのやりとりの処理 (図 4) などを行う。

[0034] UP 101 は、対象の CL3 の共用サーバ 31 に対して実行させる所定の処理 (例えば Web アプリケーション処理やバッチ処理など) のためのプログラム (コード) のデータ (ファイル群) である。なお UP 101 は構成設定情報 (configuration) ファイルなどを含む。なお 101, 102, 103 は対応した内容である。

[0035] 利用者 U2 は利用者端末 2 から、認証局 1 (そのサーバ) を介して、CL3 のリソース (共用サーバ 31) を利用し、UP 101 (102, 103) を共用サーバ 31 上で実行させる。

[0036] (3) パブリッククラウド (CL) 3 は、当該 CL3 全体を制御する制御部 35 と、複数の物理サーバ等の HW (ハードウェア) 33 と、その他図

示しない公知要素（ストレージ・DBやネットワーク機器など）とを有し、これらはネットワークで接続される。HW 33で稼動するOS 32を有し、OS 32上で稼動する1つ以上の共用サーバ（仮想サーバ）31を有する。OS 32は仮想化ソフトウェアやミドルウェア等を含む。共用サーバ31上で1つ以上の利用者プログラム（UP）103が実行される。また共用サーバ31上（又はOS 33上）で稼動するコントローラ30を有する。共用サーバ31（又は対応するコントローラ30）は、サーバ認証情報ファイルF2を有する。

[0037] 制御部35は、CL 3ごとに元々備える制御部（公知技術）であり、CL 3内のHW 33を含むリソース等を管理・制御する。例えば、35は、HW 33や仮想サーバ31等の起動や停止を制御し、複数の物理サーバや仮想サーバから成るサーバグループを管理する。なお一般的には複数（多数）の物理サーバ及び仮想サーバを有し、それらがサーバグループの単位で管理される場合が多いので、図示する1つの共用サーバ31を1つのサーバグループと捉えてもよい（そのサーバグループの単位内ではどのサーバが使用されてもよい）。

[0038] 共用サーバ31は、HW 31、OS 32上に、仮想化ソフトウェアによるリソースの多重化により構成される仮想サーバないし仮想マシンであり、共用サーバとして設定され公開される。UP 103の処理は、適宜、CL 3の共用サーバ31等のリソースを使用（参照）しながら行われる。

[0039] コントローラ（エージェント）30は、認証サーバ1と連携して制御処理を行うプログラム処理モジュールであり、対応する共用サーバ31と共に設置（インストール）される。コントローラ30は、共用サーバ31でのUP 103の実行の際の認証などに関する処理を認証サーバ1（認証制御部13）との連携で行う。

[0040] また認証局1は、図示しないが、各CL 3の共用サーバ31等の状況（UP 103の実行状況など）をコントローラ30との連携に基づきモニタして課金計算処理などを行うサブシステムを有してもよい。これにより例えば共

用サーバ31でのUP103（例えばバッチ処理）の実行の実績に応じた課金などが可能である。

[0041] [(2) 処理シーケンス]

図2は、本システム（図1）での各要素（1, 2, 3）間の処理シーケンスを示す。S101等は処理ステップを表す。大きくは、CL3側登録時（図3）の処理と、利用者U2側登録時（図4）の処理と、実行制御・認証時（図5）の処理とを有する。

[0042] ○CL3側登録時（図3）：

(S301) まずCL3側の基本登録処理として、CL3事業者と認証局1との契約に基づき、CL3事業者の管理者等（または代わりの認証局1事業者の管理者等）は、端末から、認証サーバ1のUI部10及び登録部11を通じて、CL3及びその共用サーバ31に関する情報を登録する。認証サーバ1は、管理情報60に、対応するCL情報d4、サーバ情報d5を登録する（図6）。

[0043]

(S101) 認証制御部13は、サーバ認証情報作成処理132で、上記CL3及び共用サーバ31に関するサーバ認証情報F2（SV-1D等を含む）を作成し、対象のCL3の共用サーバ31（コントローラ30）へ提供（送信）する。

[0044]

(S302) 対象のCL3の共用サーバ31にはコントローラ30がインストールされると共に、共用サーバ31（コントローラ30）は、上記サーバ認証情報F2を受信して格納・管理する。

[0045]

○利用者U2側登録時（図4）：

(S201) 利用者U2（利用者端末2）側の基本登録（設定）処理として、利用者U2と認証局1との契約（利用者U2からの申請）に基づき、利用者U2（または代わりの認証局1事業者の管理者等）は、認証サーバ1のUI部10及び登録部11を通じて、利用者U2及びそのUP101に関する情報を登録する。認証サーバ1は、管理情報60に、対応する利用者情報d2、UP情報d3を登録する（図6）。なおUP情報d3の登録を後で行っ

てもよい。

[0046] (S202) また、利用者U2により、UI部10及び登録部11を通じて、許可情報d1を設定する。例えば画面で利用者U2が許可情報d1の設定のための情報（どのリソース（CL3、共用サーバ31、機能など）を利用するか、あるいは所望の性能や料金などの情報）を選択する。なお許可情報d1の設定を後で行ってもよい。例えばジョブ情報を作成・登録する際に許可情報を設定してもよい。

[0047] (S102) 認証サーバ1の認証制御部13の許可情報設定処理133では、S202の利用者U2による設定（選択）に基づき、管理情報60に、対応する許可情報d1の内容を設定する（図6）。UP101と共用サーバ31との関係付けを利用者U2が直接的に指定する形式も可能であるし、間接的な形式、即ち認証局1が利用者U2の所望の性能や料金体系などに応じて具体的な関係付けを決定することも可能である。

[0048] (S203) 利用者U2（利用者端末2）から、UI部10を介して登録部11に対し、UP101のデータ（セット101b）を事前登録するための指示（要求）を行う。なおUP101（102）の登録のためにUP認証情報F1を必要とする仕組みであるため、まずF1を要求して取得（ダウンロード）する流れになる。

[0049] (S103) 認証サーバ1は、S203に従い、認証制御部13に連携し、UP認証情報作成処理131では、該当の利用者情報d2、UP情報d3を用いて、UP認証情報F1（UP-IDを含む）を作成する。ここで例えば利用者U2に対し、F1の暗号化のためのID及びパスワード（PW）等を要求する。

[0050] (S204) 利用者U2は、S103に従い、F1を暗号化するためのID及びPW等を設定（指定入力）する。

[0051] (S104) 認証制御部13（131）は、S204のID及びPW等を用いてUP認証情報F1を暗号化し、暗号化したF1（ファイル）を、利用者U2（利用者端末2）へ提供（送信）する。

- [0052] (S205) 利用者U 2 (利用者端末 2) は、S104の F 1 (暗号化状態) を取得 (ダウンロード) すると、作成・用意したUP 1 0 1 に当該 F 1 を同梱してセット 1 0 1 b (PW付き) を構成し、当該セット 1 0 1 b を認証サーバ 1 へアップロードして登録する。
- [0053] (S105) 認証サーバ 1 (1 3 1) は、S205のセット 1 0 1 b を受信し、ライブラリ 5 0 内にUPデータ 1 0 2 として登録する。
- [0054] ○実行制御及び認証時 (図 5) :
- (S206) 上記登録後、適宜、利用者U 2 は、利用者端末 2 から、認証サーバ 1 のUI部 1 0 を通じて、登録済みのUP 1 0 2 の実行に関するジョブ情報を登録 (設定) することができる。
- [0055] (S106) 認証サーバ 1 の実行制御部 1 2 は、S206のジョブ情報をライブラリ 5 0 にジョブ情報 6 5 として格納する。
- [0056] (S207) 利用者U 2 は、利用者端末 2 から、適宜、UI部 1 0 を通じて実行制御部 1 2 に対し、登録済みのUP 1 0 2 の実行を指示する。また例えばS206で登録済みのジョブを指定してジョブ実行指示をすることができる。
- [0057] (S107) 認証サーバ 1 の実行制御部 1 2 は、S207のUP (ジョブ) の実行指示を受けると、ライブラリ 5 0 内の該当のUPデータ 1 0 2、UP情報 d 3、ジョブ情報 6 5 等を参照し、当該UP (ジョブ) を実行する対象となるCL 3 の共用サーバ 3 1 (対応するコントローラ 3 0) を判断し、当該CL 3 の共用サーバ 3 1 へ、UP実行指示 (実行ジョブ情報) を送信する。
- [0058] (S304) 対象のCL 3 の共用サーバ 3 1 (コントローラ 3 0) は、S107の認証サーバ 1 からの指示・情報を受け、キューに格納し、順に参照して処理する。
- [0059] (S108) また認証サーバ 1 の実行制御部 1 2 は、S207の該当UPデータ 1 0 2 (F 1 を含む) を、対象のCL 3 の共用サーバ 3 1 のコントローラ 3 0 へ送信する。
- [0060] (S305) 対象のCL 3 の共用サーバ 3 1 のコントローラ 3 0 は、S108の認証サーバ 1 からのUPデータ 1 0 2 を受信 (取得) する。

- [0061] (S306) 対象のCL3の共用サーバ31のコントローラ30は、取得したUPデータ102に含まれているID及びパスワード等の情報を用いて、UPデータ102に含まれているUP認証情報F1を復号化（解凍）し、そのF1に含まれているUP-ID等の情報を取り出して参照する。
- [0062] また、同コントローラ30は、予めS302で当該共用サーバ31に格納されているサーバ認証情報F2を参照する。そしてF1の処理と同様に、コントローラ30は、F2を復号化し、F2に含まれているSV-ID等の情報を取り出して参照する。
- [0063] (S307) 対象の共用サーバ31のコントローラ30は、S306でF1、F2から得たUP-ID、SV-ID等の情報を用いて、認証処理（当該共用サーバ31で当該UP102を実行してもよいかどうかの確認）のために、認証サーバ1（認証制御部13）へ、認証の要求を送信する。
- [0064] (S109) 認証サーバ1の認証制御部13（権限確認処理134）は、S307の要求を受けると、当該要求に含まれているUP-ID、SV-ID等の情報を参照して、ライブラリ50内の該当の許可情報d1を参照し（図6）、認証処理を行い、その結果情報を、対象のCL3の共用サーバ31（コントローラ30）へ応答送信する。
- [0065] (S308) 対象の共用サーバ31のコントローラ30は、S109の結果情報を受け、その情報が実行の許可を示している場合は、当該共用サーバ31上で当該UP102（103）の処理を実行し、不許可を示している場合は実行しない。
- [0066] なおUP103及び共用サーバ31がバッチ処理用である場合、そのバッチ処理は所定の日時で起動する。また必要に応じて、当該共用サーバ31でのUP103の処理から、他のリソース（CL3、共用サーバ31）へアクセスが発生する。その場合は、当該アクセスごとに、上記同様に認証処理などが行われる。
- [0067] [（3）CL側登録時の処理]

図3は、本システムでのCL3側の登録時の構成・処理例を示す。認証局

1 事業者とCL3事業者との契約に基づき、予め対象のCL3内に共用サー

バ31が設置（設定）される。認証サーバ1（認証制御部13）は、CL3事業者（管理者などのユーザU3）に対し、共用サーバ31の認証情報（SV-IDを含む）であるサーバ認証情報F2のファイルを作成・提供する。

特にF2は、対応するCL3の認証情報（CL-IDを含む）を含めた形としてもよい。なおサーバ認証情報F2の仕組みは基本的にUP認証情報F1

の仕組み（図4等）と同様であるため簡易説明とする。共用サーバ31は、

種別（Webアプリ/パッチ等）や機能（PDF/メール等）などに応じて複数設けることができ、それぞれにサーバ認証情報F2が格納される。各共

用サーバ31間では必要に応じてアクセスが発生し連携して処理が行われる。共用サーバ31として、例えば#A1はWebアプリケーションサーバ、

#A2はパッチサーバである。

[0068]

（a1）CL3事業者（U3）は、端末36などから認証サーバ1にアク

セスし、U1部10及び登録部11の処理を介して、前述のようにCL情報d4、サーバ情報d5を登録する。（a2）予め共用サーバ31のセットア

ップ時に、認証制御部13は、コントロール30となるプログラムを対象のCL3の共用サーバ31に提供しインストールさせる。各共用サーバ31の

稼動時に一緒にコントロール30を稼動させる。（a3）認証制御部13のサーバ認証情報作成処理132では、CL情報d4、サーバ情報d5を用い

て、SV-ID等を含むサーバ認証情報F2（U3のパスワードによる暗号化）を作成し、対象のCL3の共用サーバ31（コントロール30）へ提供

し格納させる。

[0069]

〔（4）利用者側登録時の処理〕

図4は、本システムでの利用者U2（端末2）側の登録時の構成・処理例

を示す。認証サーバ1は、利用者U2（端末2）に対し、UP認証情報F1

（UP-IDを含む）のファイルを作成・提供する。F1は利用者U2の認

証情報（U-IDを含む）を含めた形としてもよい。

[0070]

利用者U2の端末2では、認証サーバ1のU1部10及び登録部11等の

処理を通じて、UP登録処理201（UP101の登録に関する処理）を行う。例えばUI部10により提供されるWebページの画面でUP登録処理201を行う。UP登録処理201として、利用者情報（d2）の登録と、UP情報（d3）の登録と、UPデータ（102）の登録と、認証設定（パスワードの設定）と、許可情報（d1）の設定と、を有する。

[0071] （b1）利用者U2は、必要に応じて、画面で、利用者情報（d2）の登録と共にUP情報（d3）を登録する。利用者U2は、UP101を作成／用意し、UP情報（d3）の登録と共に、UP101に関するUP認証情報F1を認証サーバ1からダウンロード（取得）する。（b2）その際、利用者U2は、UP認証情報作成処理131に対し、認証設定（UP認証情報F1の暗号化のためのパスワードの設定）を行い、（b3）UP認証情報作成処理131により暗号化されたUP認証情報F1をダウンロード（取得）する。（b4）利用者U2は、UP101にUP認証情報F1を同梱（添付）してセット101bを構成し、（b5）認証サーバ1のライブラリ50へUPデータ102としてアップロード（登録）する。

[0072] なお上記で所定形式のセット101bにまとめて登録する作業・処理は、既存の汎用的なツール（例えば複数ファイルを1つのZIPファイルに圧縮・暗号化するソフトウェア）を使用してもよいし、本システムで専用ツールを用意してもよい。なお必要とするセキュリティレベルに応じたツール・形式を利用すればよい。

[0073] （b6）また利用者U2は、各情報（d2，d3）の登録と共に、UI部10及び認証制御部13の許可情報設定処理133を通じて、UP101（102）に関する許可情報（d1）を設定する。利用者U2は、例えば画面で、UP101ごとに、候補の中から利用対象となるリソース（CL3、共用サーバ31、その機能）、利用方式（料金体系）などを選択する。許可情報設定処理133は、利用者U2の選択に応じて、許可情報d1及び利用者情報d2などの内容（関連付け等）を設定する。料金体系は例えば性能としてCPU（プロセッサ）1秒あたりの単価などを提示して選択可能とする。

[0074] (b 7) また利用者U 2 (端末2のジョブ登録処理204)は、適宜、ジョブ情報65を登録することができる。ジョブ情報65は、ジョブの名称、識別情報(一意のコード等)、当該ジョブで使用するUP102のID(UP-ID)及び許可情報d1の指定、実行日時、等の情報を含む。ジョブ情報を登録しておけば、利用者U2は、UP102を実行させる際に、UI部10からジョブを指定して実行することにより、対応するUP102を実行させることができる(図5)。なおジョブを登録せずに直接・個別的にUP102の実行指示をしてもよい。

[0075] なお他の構成例として、UP101とF1とのセット101b(UPデータ102)を認証サーバ1のライブラリ50に登録する構成については、セット101bの構成を認証サーバ1側で行うなど、利用者U2及びUP101の成りすまし等を防止できる方式であればよい。

[0076] [(5) 実行制御・認証時の処理]

図5は、本システムでの認証サーバ1及びCL3による実行制御時及び認証時の構成・処理例を示す。

[0077] (c1) 利用者U2の端末2では、認証サーバ1のUI部10及び実行制御部12に対して、UP実行処理202を行う。UP実行処理202として、ジョブ登録(図4の204と同様)や、個別のUP実行指示や、ジョブ実行指示などを有する。例えば利用者U2はジョブを登録してそのジョブの実行指示を与える。認証サーバ1の実行制御部12は、端末2(UP実行処理202)からの指示・要求(c1)を受け、ライブラリ50にジョブ情報65を登録したり、UP実行指示やジョブ実行指示に対応したUPデータ102を参照してその実行制御を行う。

[0078] (c2) 実行制御部12は、利用者U2からの指示(c1)に従い、該当のUPデータ102を対象のCL3の共用サーバ31で実行させるために、対象のCL3の共用サーバ31のコントローラ30と連携し、実行指示を送信する。例えばジョブ情報65による指示の場合は、認証サーバ1からCL3またはコントローラ30の管理するキューへ実行ジョブ情報を送信し格納

させる。(c 3) 上記指示と併せて、実行制御部 12 はライブラリ 50 の UP データ 102 を取り出して対象の共用サーバ 31 へ送信する。

[0079] 共用サーバ 31 (コントローラ 30) は、実行制御部 12 からの指示 (c 2) に従い、対象の UP 102 (103) の処理を対象の共用サーバ 31 上で稼働させる。その際、実行の正当性 (権限) を確認するために、認証サーバ 1 (認証制御部 13) と連携して認証処理を行う。例えば共用サーバ 31 は、キューを参照して自分が実行すべきジョブ情報がある場合は順に処理する。

[0080] (c 4) コントローラ 30 は、上記共用サーバ 31 での UP 103 の実行の前に、当該共用サーバ 31 のサーバ認証情報 F2 を参照すると共に、UP 103 に同梱されている UP 認証情報 F1 を参照する。その際、F1 は暗号化状態であるので、UP 103 に含まれている復号化のパスワード情報を取り出して当該パスワードで F1 を復号化 (解凍) して参照する。コントローラ 30 は、復号化した F1 に含まれている UP-ID 等の情報を参照し、復号化した F2 に含まれている SV-ID 等の情報を参照する。

[0081] (c 5) コントローラ 30 は、上記 F1, F2 から得た UP-ID, SV-ID 等の情報を用いて、認証サーバ 1 へ認証の要求を送信する。(c 6) 認証サーバ 1 の認証制御部 13 は、認証処理 134 において、コントローラ 30 からの要求を受け、その UP-ID, SV-ID 等の情報を用いて、該当する許可情報 d1 を参照する (図 6)。そして、134 は、該当の利用者 U2 (U-ID) の UP 103 (UP-ID) を該当の CL3 (CL-ID) の共用サーバ 31 (SV-ID) で実行してもよいかどうか権限確認 (許可判定) する。(c 7) 認証サーバ 1 (13) は、認証処理 134 の結果情報をコントローラ 30 へ応答送信する。コントローラ 30 は、結果情報から許可 / 不許可を確認し、許可である場合は、当該共用サーバ 31 で UP 103 の処理を実行する。

[0082] (c 8) また上記許可された共用サーバ 31 での UP 103 の処理において、更に当該 CL3 内の他の共用サーバ 31 (その機能 f1 等) へのアクセ

スが発生する場合には、上記同様に、UP 認証情報 F 1 と、アクセス先の共用サーバ 3 1 のサーバ認証情報 F 2 とを用いて認証処理が行われる。(c 9) また他の CL 3 へのアクセスが発生する場合にも上記同様に、UP 認証情報 F 1 と、アクセス先の CL 3 の共用サーバ 3 1 のサーバ認証情報 F 2 とを用いて認証処理が行われる。

[0083] 上記のように、各共用サーバ 3 1 へのアクセス時の自動的な認証処理で UP 1 0 3 と共用サーバ 3 1 の正当性及びその関連付けでの権限を確認した上で実行させることができるので、クラウド環境でのセキュリティを確保できる。

[0084] [(6) 管理情報]

図 6 は、本システムでの認証サーバ 1 のライブラリ 5 0 (記憶部) に格納・管理される管理情報 6 0 (d 1 ~ d 5) の構成例を示す。各情報 (d 1 ~ d 5) は図示の例のように相互にリンク・関連付けられる。リソース情報として CL 情報 d 4 とサーバ情報 d 5 を含む。

[0085] 許可情報 d 1 は、認証局 1 として、どの利用者 U 2 のどの UP 1 0 1 (1 0 2) をどの CL 3 のどの共用サーバ 3 1 (その種別や機能) で実行を許可するかについての関連付けを制御・管理するための設定情報であり、認証処理時に実行の許可／不許可 (権限) を判定 (確認) する際に参照される。

[0086] 利用者情報 d 2 は、複数の各々の利用者 U 2 の管理情報である。利用者情報 d 2 として、利用者 U 2 の名称、識別情報 (一意のコード等。U-ID とする)、各種の属性 (例えば会社名、連絡先、Web ユーザ情報など)、利用方式 (料金体系)、などの情報を有する。利用方式は例えば認証局 1 が提示するサービス項目や料金体系 (課金方式) などから利用者 U 2 が選択したものを示す。なお U-ID の例を「利用者 A」「U # 1」等以示す。

[0087] プログラム (UP) 情報 d 3 は、利用者 U 2 (U-ID) (d 2) に関連付けられる、複数の各々の UP 1 0 1 (1 0 2) の管理情報である。UP 情報 d 3 として、UP 1 0 1 の名称、識別情報 (一意のコード等。UP-ID とする)、プログラム種別 {例えば Web アプリ処理用／バッチ処理用など

、利用機能・リソース(種類) {例えばPDF／メール／DBなど}、等を有する。なおUP-IDの例を「UP # A1」等で示す。UP情報d3は、UP-IDによりUP認証情報F1と関連付けられる。

[0088] パブリッククラウド(CL)情報d4は、複数の各々のCL3の管理情報

である。CL情報d4として、CL3の名称、識別情報(一意のコード等。CL-IDとする)、各種の属性(例えば事業者情報、地域(位置)など)、サーバグループ情報、課金方式(単価)、等の情報を有する。サーバグループ情報は、当該CL3内に有するサーバグループ(共用サーバ31のグループを含む)の管理情報である。課金方式(単価)は、当該CL3(共用サーバ31)ごとにおける課金方式(単価)の情報である。なおCL-IDの例を「CL-A」等で示す。

[0089] サーバ情報d5は、CL3(CL-ID)(d4)に関連付けられる、複

数の各々の共用サーバ31の管理情報である。サーバ情報d5としては、サーバ(共用サーバ31)の名称、識別情報(一意のコード等。SV-IDとする)、サーバ種別 {例えばWebアプリケーション／パッチ用など}、提供機能・リソース(種類) {例えばPDF／メール／DB等}、等の情報を有する。なおSV-IDの例を「SV # A1」等で示す。

[0090] 許可情報d1は、例えば利用者U2ごとに1つ以上を設定することができ

、複数設定した場合は選択利用可能である。許可情報d1は、例えば、利用者U2を示すU-IDと、当該利用者U2による利用(アクセス)を許可するCL3を示すCL-IDと、当該CL3内で利用(アクセス)を許可する機能(例えばPDF等)と、の関連付けの情報を含む。あるいは、許可情報d1は、各ID(U-ID, UP-ID, CL-ID, SV-ID)の関連付け(許可を示す)の情報を含む。よって、許可情報d1を参照すれば、どの利用者U2(U-ID)のどのプログラム(UP-ID)をどのCL3(CL-ID)のどの共用サーバ31(SV-ID)で実行してよいかを確認(判定)できる。

[0091] なお関連付けの仕方として、U-IDとCL-IDとを関連付けることで

、その利用者U 2の全UP 1 0 2をそのCL 3内の全共用サーバ3 1で実行許可する形式としてもよいし、個々のUP-IDとSV-IDとを関連付けることで、その組合せのみ実行許可する形式としてもよい等、各種が可能である。

[0092] 〔（７）認証情報〕

UP認証情報F 1は、対象のUP 1 0 1及びその所有者（オーナー）である利用者U 2に関する認証用の情報である。UP認証情報F 1の構成例としては、少なくともUP-IDを含む形式であり、更にU-ID（当該UP 1 0 1を持つ利用者U 2を示す）等の情報を含ませてもよい。少なくともUP-IDがあれば、関連付けにより、UP情報d 3を参照し利用者情報d 2を参照し許可情報d 1を参照することができる。

[0093] サーバ認証情報F 2は、対象の共用サーバ3 1及びその所有者（オーナー）であるCL 3に関する認証用の情報である。サーバ認証情報F 2の構成例としては、少なくともSV-IDを含む形式であり、更にCL-ID（当該共用サーバ3 1を持つCL 3を示す）等の情報を含ませてもよい。少なくともSV-IDがあれば、関連付けにより、サーバ情報d 5を参照しCL情報d 4を参照し許可情報d 1を参照することができる。

[0094] なお図4のセット1 0 1 bの構成例としては、UP 1 0 1（UPデータファイル群）にUP認証情報F 1（暗号化状態）及びそのパスワード情報が同梱されたセットである。パスワード情報は例えばUPデータファイル群のうちの構成設定情報ファイルに記述される。

[0095] 〔（８）共用例〕

図7では、本システムでのリソースの共用の具体例を示している。例えば、第1の利用者Aは、端末2に2つのUP 1 0 1である# A 1、# A 2を有する。例えば# A 1はWebアプリ処理用のプログラム、# A 2はバッチ処理用のプログラムである。第2の利用者Bは、端末2に、1つのUP 1 0 1である# B 1を有する。例えば# B 1はWebアプリ処理用のプログラムである。それぞれのUP 1 0 1が認証局1のライブラリ5 0に登録され、対応

して図示の例のように許可情報 d 1 などが設定される。例えば利用者 A の U P # A 1 の処理は、C L - A (例えば東京) の第 1 の共用サーバ 3 1 である S V # A 1 (W e b アプリ処理用) で実行許可され、U P # A 2 の処理は、C L - B (例えば北米) の第 1 の共用サーバ 3 1 である S V # B 1 (バッチ処理用) で実行許可される。利用者 B の U P # B 1 の処理は、C L - A の第 1 の共用サーバ 3 1 である S V # A 1 (W e b アプリ処理用) で実行許可される。また U P # A 1 の処理では、機能 f 1 (例えば P D F 生成処理) が利用 (許可) され、S V # A 1 から機能 f 1 を持つ共用サーバ 3 1 である S V # A 3 へのアクセスが許可される。同様に U P # B 1 の処理では、機能 f 2 (例えばメール送信処理) が利用 (許可) され、S V # A 1 から機能 f 2 を持つ共用サーバ 3 1 である S V # A 4 へのアクセスが許可される。

[0096] このように各利用者 U 2 は所望のリソース (C L 3、共用サーバ 3 1) を利用して U P 1 0 1 の実行ができると共に、各共用サーバ 3 1 での処理時に前述の認証がされるのでセキュリティも確保される。

[0097] また、各 C L 3 (A, B, C) は、位置 (地域) 及び利用者 U 2 (端末 2) との距離が異なり、性能や機能が異なる。各種の C L 3、共用サーバ 3 1、及び機能 (f 1 等) ごとに、課金方式 (利用単価) などが異なる。認証局 1 でそれらの利用の組合せに応じて統合的なサービス項目・料金体系を設定して利用者 U 2 に提供することで、利用者 U 2 は容易・安価にクラウド環境を利用できる。例えば U 1 部 1 0 の画面で、性能あたりの単価や、機能ごとの料金などを提示し、利用者 U 2 により選択して利用契約が可能である。利用者 U 2 は特定の C L 3 等を指定して利用することもできるし、要求性能などを指定して特定の C L 3 等によらずに利用することもできる。

[0098] また例えば S V # B 1 での U P # A 2 のバッチ処理は所定の日時に実行されるので、コントローラ 3 0 によりそのバッチ処理の状況 (稼動時間など) をモニタすれば、そのモニタ情報に応じた課金計算処理が認証局 1 で可能である。

[0099] [効果等]

以上説明したように、本実施の形態によれば、利用者（UP101）とCL3（共用サーバ31）の双方の認証情報（F1、F2）、及び許可情報d1を用いた確認などにより、特に複数の利用者U2と複数のCL3を含むクラウド環境で、どの利用者U2のプログラム（UP）をどのCL3の共用サーバ31等で実行するかに関する認証・認可（実行の正当性の確認、権限確認など）を行うことで、1つの仮想サーバで複数の利用者のプログラムを実行させる場合におけるセキュリティ確保や効果的な制御・管理が実現できる。結果、利用者U2はCL3等のリソースを容易・安価に利用でき、Webアプリ処理やバッチ処理などを容易・安価に実現できる。

[0100] 特に、利用者U2側は、UP101にUP認証情報F1を同梱して認証サーバ1側にアップロード（登録）するだけで、それ以降のこと（認証サーバ1及び各CL3側での制御や認証等）を考える必要無く、セキュリティを確保できる。利用者U2は、UP101のコード内でセキュリティを意識して前述の各リソースへのアクセスなどのID及びパスワード等を記述する手間も必要無く、作業負担が小さく、コードも簡素化できる。

[0101] また特に、認証局（認証サーバ）1を提供する事業者は、各CL3に共用サーバ31を設置（設定）し、複数の利用者U2（UP101）と複数のCL3（共用サーバ31）とにおける実行の制御及びその際の認証（セキュリティ管理）を行うサービスが可能である。利用者U2の要求や契約、CL3の要求や契約、特有の課金方式や制御方式、通信状況などに応じて、効果的で柔軟な関係付けの制御を実現すると共に、その際のセキュリティを確保・向上できる。

[0102] 以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。

産業上の利用可能性

[0103] 本発明は、パブリッククラウド等に利用可能である。

請求の範囲

[請求項1] 利用者の端末と、複数のサーバを含むパブリッククラウドと、認証サーバとを含む要素がネットワークで接続され、

前記パブリッククラウド内には、前記利用者のプログラムを実行させる対象となるサーバと、当該実行に関する制御処理を行うコントローラとが設けられ、

前記認証サーバは、認証制御部と、記憶部とを有し、

前記記憶部は、前記利用者のIDを含む情報と、前記利用者のプログラムのIDを含む情報と、前記パブリッククラウドのIDを含む情報と、前記サーバのIDを含む情報と、前記利用者のプログラムと前記パブリッククラウドのサーバとの実行の関連付けを管理するための許可情報と、を格納し、

前記認証制御部は、

前記利用者のプログラムを認証するための第1の認証情報を作成し、前記利用者のプログラムに前記第1の認証情報を同梱させる、第1の処理部と、

前記パブリッククラウドのサーバを認証するための第2の認証情報を作成し、前記パブリッククラウドのサーバに提供する、第2の処理部と、

前記利用者の端末からの入力に応じて前記許可情報の内容を設定する第3の処理部と、

前記利用者のプログラムを前記パブリッククラウドのサーバで実行させる際に、前記コントローラと連携して、前記第1の認証情報、前記第2の認証情報、及び前記許可情報を参照し、当該利用者のプログラムを当該パブリッククラウドのサーバで実行許可するか判定して許可の場合は実行させる、第4の処理部と、を有すること、を特徴とするクラウドセキュリティ管理システム。

[請求項2] 請求項1記載のクラウドセキュリティ管理システムにおいて、

前記認証サーバの認証制御部の第1の処理部は、前記利用者の端末から指定される第1のパスワード情報を用いて前記第1の認証情報を暗号化し、前記利用者のプログラムに当該暗号化された第1の認証情報及び第1のパスワード情報を同梱させ、

前記パブリッククラウドのサーバで前記利用者のプログラムを実行させる際、前記コントローラは、前記サーバに格納されている前記第2の認証情報に含まれているサーバのIDを参照し、前記利用者のプログラムに同梱されている前記第1の認証情報及び第1のパスワード情報を参照し、当該第1の認証情報を第1のパスワード情報を用いて復号化し、当該第1の認証情報に含まれているプログラムのIDを参照し、当該サーバのID及びプログラムのIDを含む認証の要求を前記認証サーバへ送信し、

前記認証サーバの認証制御部の第4の処理部は、前記認証の要求に含まれているサーバのID及びプログラムのIDを用いて該当する許可情報を参照し、前記実行許可の判定をすること、を特徴とするクラウドセキュリティ管理システム。

[請求項3]

請求項1記載のクラウドセキュリティ管理システムにおいて、

前記パブリッククラウド内には、前記利用者のプログラムを実行させる対象となる複数の第1のサーバと、前記利用者のプログラムの処理のための各機能を提供する複数の第2のサーバとを有し、各々のサーバに第2の認証情報が格納され、

前記認証サーバの第4の処理部は、前記第1のサーバから前記第2のサーバへのアクセスごとに、前記コントローラと連携して、前記利用者のプログラムに対応した第1の認証情報、前記アクセス先の第2のサーバに対応した第2の認証情報、及び前記許可情報を参照し、当該第2のサーバの機能の利用許可の判定をすること、を特徴とするクラウドセキュリティ管理システム。

[請求項4]

請求項1記載のクラウドセキュリティ管理システムにおいて、

複数の利用者の端末を有し、複数のパブリッククラウドを有し、
前記パブリッククラウド内には、前記複数の利用者のプログラムを
共用で実行させる候補となる 1 つ以上の共用サーバと、当該共用サー
バを管理するための制御処理を行う前記コントローラとが設けられ、
前記許可情報は、前記利用者のプログラムと前記パブリッククラウド
の共用サーバとの実行の関連付けが設定されること、を特徴とする
クラウドセキュリティ管理システム。

[請求項5]

請求項 1 記載のクラウドセキュリティ管理システムにおいて、
前記認証サーバは、登録部と、実行制御部とを有し、
前記登録部は、前記利用者の端末からの指示に基づき、前記利用者
のプログラムのデータを前記記憶部に格納する処理を行い、
前記実行制御部は、前記利用者の端末からの指示に基づき、前記記
憶部に登録されている前記利用者のプログラムのデータを対象のパブ
リッククラウドのサーバで実行させる制御処理を前記コントローラと
連携して行い、
前記認証制御部の前記第 1 の処理部は、前記利用者のプログラムを
認証するための第 1 の認証情報を作成し、前記利用者のプログラムに
前記第 1 の認証情報を同梱して前記記憶部に登録すること、を特徴と
するクラウドセキュリティ管理システム。

[請求項6]

請求項 1 記載のクラウドセキュリティ管理システムにおいて、
前記認証サーバは、前記利用者の端末に対して画面を提供するユー
ザインターフェイス部を有し、
前記ユーザインターフェイス部による画面で前記利用者は前記利用
者のプログラムを実行させる対象となるパブリッククラウドのサーバ
及び機能を直接的に指定可能であり、
前記第 3 の処理部は、上記指定に応じて前記許可情報の内容を設定
すること、を特徴とするクラウドセキュリティ管理システム。

[請求項7]

請求項 1 記載のクラウドセキュリティ管理システムにおいて、

前記認証サーバは、前記利用者の端末に対して画面を提供するユーザインターフェイス部を有し、

前記ユーザインターフェイス部による画面で前記利用者は前記利用者のプログラムを実行させる対象となるパブリッククラウドのサーバ及び機能を、性能または料金体系の選択の形式で間接的に指定可能であり、

前記第3の処理部は、上記指定に応じて、前記利用者のプログラムを実行させる対象となるパブリッククラウドのサーバ及び機能の関連付けを決定し、前記許可情報の内容を設定すること、を特徴とするクラウドセキュリティ管理システム。