

NEC Cloud System ポータル 機能概要

第 4.0.0 版

2017 年 7 月

日本電気株式会社

免責事項

本書の内容はすべて日本電気株式会社が所有する著作権に保護されています。

本書の内容の一部または全部を無断で転載および複製することは禁止されています。

本書の内容は将来予告なしに変更することがあります。

日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任を負いません。

日本電気株式会社は、本書の内容に関し、その正確性、有用性、確実性その他いかなる保証もいたしません。

商標

- LINUX は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
- Red Hat、Red Hat Enterprise Linux は米国およびその他の国において登録された Red Hat, Inc.の商標です。
- OpenStack は、OpenStack Foundation の登録商標または商標です。
- Elasticsearch, Logstash, Kibana は、Elasticsearch BV の米国およびその他の国における登録 商標または商標です。
- Drupal の名称およびそのロゴは、Drupal Association が所有する登録商標または商標です。
- Cloudify は、GigaSpaces Technologies の登録商標または商標です。
- その他、本書に記載されているソフトウェア製品およびハードウェア製品の名称は、関係各社の登録商標または商標です。

その他、本書に記載のシステム名、会社名、製品名は、各社の登録商標もしくは商標です。

なお、本書内では、®、TM、©の記号は省略しています。

はじめに

本書は、『NEC Cloud System ポータル v4.0』の機能概要について説明させていただきます。

目 次

1. NEC Cloud System ポータルとは 6

1.1 概要 6

2. NEC Cloud System ポータルが提供する機能 7

2.1 概要 7

2.2 業務ワークフロー 8

2.2.1 概要 8

2.2.2 アプリケーション構造 9

2.2.3 用語 9

2.3 ワークフローエンジン 10

2.3.1 概要 10

2.3.2 申請書種別 10

2.3.3 ワークフローパターン 10

2.3.4 申請書 10

2.4 商品管理 11

2.4.1 概要 11

2.4.2 商材 11

2.4.3 商品・商品内容 11

2.4.4 価格表 12

2.4.5 商品テナント関連 12

2.5 契約管理 13

2.5.1 概要 13

2.5.2 契約 13

2.6 業務ワークフローに含まれるサンプル 14

2.6.1 概要 14

2.6.2 お問合せ 15

2.6.3 商品契約申請 15

2.6.4 入会・退会申請 17

2.6.5 お知らせ登録(メンテナンス情報) 18

2.6.6 Quota 購入変更 18

2.6.7 従量課金契約変更 19

2.6.8 オブジェクトストレージ契約 20

2.7 キャパシティ管理	21
2.7.1 概要	21
2.8 証跡管理	21
2.8.1 概要	21
2.9 ログ管理	21
2.9.1 概要	21
2.10 設定管理	22
2.10.1 概要	22
2.11 オブジェクトストレージ管理	22
2.11.1 概要	22
2.12 お知らせ機能	23
2.12.1 概要	23
2.12.2 機能ブロック構造	24
2.12.3 お知らせ機能 (Drupal)	24
2.12.4 OpenStack 標準画面 (Horizon)	25
2.12.5 Keystone 連携、SSO オプション	26
2.12.6 業務ワークフローエンジン	26
2.13 TOSCA テンプレートプロビジョニング機能	27
2.13.1 概要	27
2.13.2 機能ブロック構造	27
2.13.3 AP 自動構築操作画面	28
2.13.4 AP 自動構築基盤構築 Heat テンプレート	28
2.13.5 AP 自動構築基盤構築モジュール	28
2.13.6 サンプル TOSCA テンプレート	28
2.13.7 AP 自動構築基盤	28
2.14 ポリシー制御機能	29
2.14.1 概要	29
2.14.2 事業者権限の分離	29
2.14.3 事業者ユーザのセルフ管理	29
2.14.4 テナントユーザのサービス利用権限の分離	29
2.14.5 テナントソースの分割	29

1. NEC Cloud System ポータルとは

1.1 概要

OpenStack を基盤としたクラウドソリューションのための、カスタマイズ性・拡張性に優れたポータル機能であり、OpenStack Horizon をベースに開発されています。

2. NEC Cloud System ポータルが提供する機能

2.1 概要

OpenStack Horizon に対し、以下の機能拡張を標準機能として提供します。

本項では、それぞれの機能についての概要を説明します。

- ・ 業務ワークフロー
ワークフローエンジン
商品管理
契約管理
- ・ キャパシティ管理
- ・ 証跡管理
- ・ ログ管理
- ・ 設定管理
- ・ オブジェクトストレージ管理
- ・ ポリシー管理
- ・ お知らせ機能
- ・ TOSCA テンプレートプロビジョニング機能
- ・ ポリシー制御機能

また、SI カスタマイズサンプルについてもご紹介します。

特に記載のない限り、global_portal および region_portal それぞれのサーバに提供される機能となります。

2.2 業務ワークフロー

region_portal のみに提供される機能です。

2.2.1 概要

業務ワークフローとは、以下の機能の総称です。

- ・ ワークフローエンジン
- ・ 商品管理
- ・ 契約管理

また、NEC Cloud System ポータルを用いて SI カスタマイズを行うことを想定したサンプル機能を含んでいます。

2.2.2 アプリケーション構造

業務ワークフローのアプリケーション構成図は、以下の通りです。

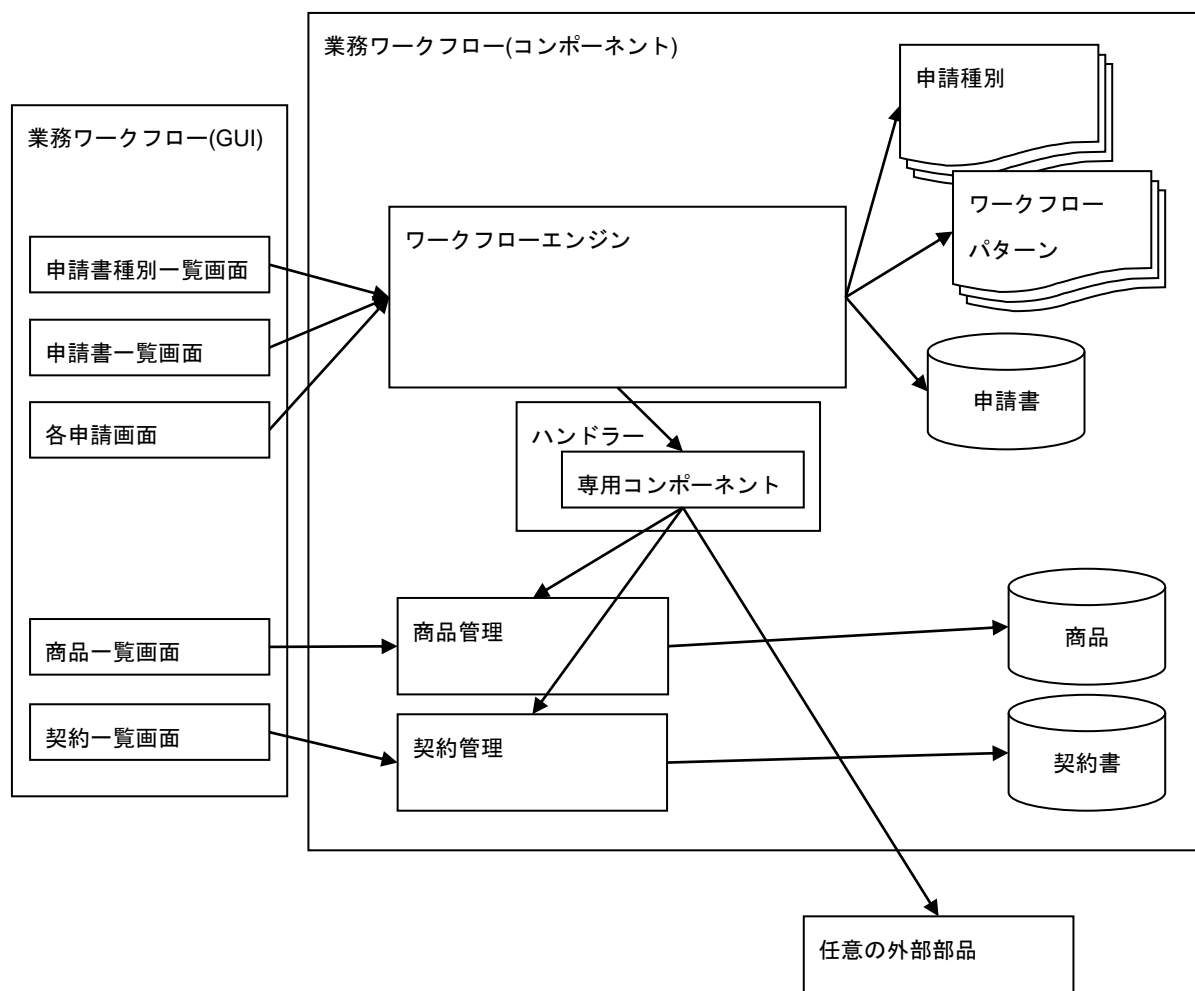


図 1 アプリケーション構造

2.2.3 用語

・ハンドラー

申請内容に応じた様々な処理をおこなうための固有のコンポーネントです。

業務に応じて、専用に作りこみを行う必要があります。

2.3 ワークフローエンジン

region_portal のみに提供される機能です。

2.3.1 概要

ポータル画面から、商品契約や作業依頼・お問合せなど、各種申請手続き処理を実装するためのフレームワークを提供します。

ワークフローエンジンを利用することで、ポータル画面に新たな申請ワークフロー機能を追加することができます。

ワークフローエンジンは、以下に説明する、申請書種別、ワークフローパターン、申請書の機能を持っており、これらとハンドラーを組み合わせ、申請ワークフロー処理を実現します。

2.3.2 申請書種別

申請書のフォーマットを管理する機能です。

申請書種別の登録・削除することができます。

新たに申請ワークフローを追加する場合、申請書に記載する内容を取り決めたうえで、そのフォーマットを本機能に登録してください。

申請書種別は、後述する商品管理と連携させて、商品契約申請書を作成することも可能です。

また、登録された申請書フォーマットを参照する GUI を標準機能として提供します。

2.3.3 ワークフローパターン

申請ワークフローにおけるワークフローパターンを管理する機能です。

ワークフローパターンを登録・削除することができます。

パターンフォーマットに沿ってフロー定義をしていただくことで、例えば、申請→中間承認→最終承認 or 否認といったワークフローを、実現することができます。

承認に至るルートや、チェックポイントの数は任意に設定することができます。

また、申請書種別とワークフローパターンを組み合わせ、申請書種別ごとに、個別のワークフローを定義することも可能です。

さらに、ポータル画面のユーザ権限(OpenStack におけるロール)と組み合わせ、承認や否認の実行権限を定義したり、独自に作成した SI 部品を、任意のタイミングで実行させたりといったアクションの定義もできます。

ワークフローエンジンは、これら定義をもとに、申請書のステータス遷移を管理します。またハンドラーなど、申請に伴って必要となる処理の実行トリガーとして動作します。

2.3.4 申請書

申請された申請書を管理する機能です。

申請書の参照・登録・更新・削除機能を提供します。

また、申請済みの申請書を参照する GUI を標準機能として提供します。

2.4 商品管理

region_portal のみに提供される機能です。

2.4.1 概要

商品やその内容、あるいは、価格情報を管理する機能です。

商品管理は、それ単独では、商品を契約するための機能を持っていませんが、ワークフローエンジン、契約管理と組み合わせて使用することで、商品契約機能を実現することができます。

以下に、商品管理のデータモデルを示します。

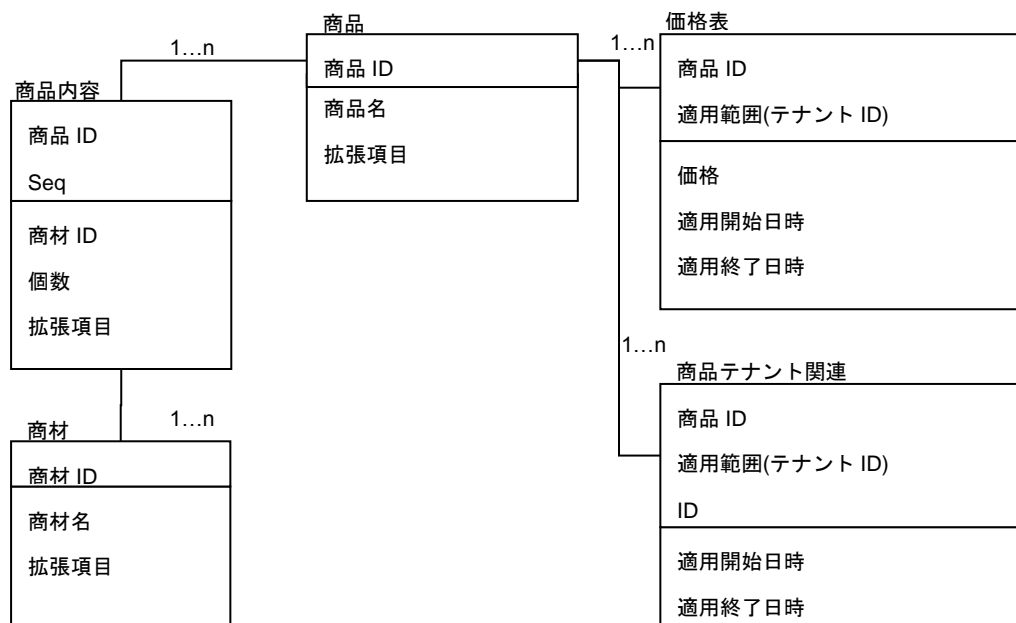


図 2 商品管理のデータモデル

2.4.2 商材

商材を管理する機能です。

商材情報の参照・登録・変更・削除機能を提供します。

NEC Cloud System ポータルでは、1 つ以上の商材を組み合わせ、様々な商品を定義することが可能です。

2.4.3 商品・商品内容

商品を管理する機能です。

商品、あるいは、その明細情報について、参照・登録・変更・削除機能を提供します。

あらかじめ定義された商材を、1 つ以上組み合わせ、商品として定義することができます。

汎用的なデータモデルを採用しており、商品には S I の内容に応じた、さまざまな種別を持たせることが可能です。商品を参照する GUI を標準機能として提供します。

2.4.4 価格表

商品の価格を管理する機能です。

商品に対する価格情報の参照・登録・変更・削除機能を提供します。

NEC Cloud System ポータルでは、価格は、商品に対して定義します。

価格情報には、全テナント共通となるパブリック価格以外に、お客様が利用するテナントごとに、個別のプライベート価格を設定することが可能です。

また、価格の設定には、有効期限を指定することができます。

パブリック価格、および、プライベート価格を設定するための GUI を標準機能として提供します。

なお、GUI からの操作において価格を新規登録した場合、有効期限の開始日時にはシステム日時が、終了日時には 9999/12/31 23:59:59.999 が設定されます。

価格を変更した場合は、既存の価格情報の終了日時をシステム日付－1 秒に設定し、システム日時～9999/12/31 23:59:59.999 を有効期限とした価格情報を新規作成する仕様となっています。

2.4.5 商品テナント関連

どの商品をどのテナントに公開するのか、といった、テナントと商品の紐付け情報を管理する機能です。

テナントと商品の紐付け情報の参照・登録・変更・削除機能を提供します。

商品の公開範囲として、特定のテナント以外に、全テナントを指定することも可能です。

また、価格情報と同様に、有効期限を設定することができます。

商品の公開範囲を設定するための GUI を標準機能として提供します。

GUI を使用した場合の有効期限の設定方法は、価格表と同じです。

2.5 契約管理

region_portal のみに提供される機能です。

2.5.1 概要

契約情報を管理する機能です。

ワークフロー、商品管理と組み合わせて、商品契約機能を実現することができます。

2.5.2 契約

契約情報を管理する機能です。

契約情報の参照・登録・更新・削除機能を提供します。

ワークフローエンジン上で実装される申請処理から、任意のタイミングで、契約管理機能が呼び出されて利用されることを想定しています。

なお、NEC Cloud System ポータルでは、1つの申請に対して、1つの契約情報を作成するように想定されています。

また、契約情報を参照するための GUI を標準機能として提供します。

2.6 業務ワークフローに含まれるサンプル

region_portal のみに提供される機能です。

2.6.1 概要

以下に説明する機能は、SI サンプルとして提供する機能です。
SI によるカスタマイズのベースとしてご利用ください。

大まかには、先のアプリケーション構成図の内、以下に該当する部分を、想定する業務に沿って、定義、あるいは、作成していただくことになります。

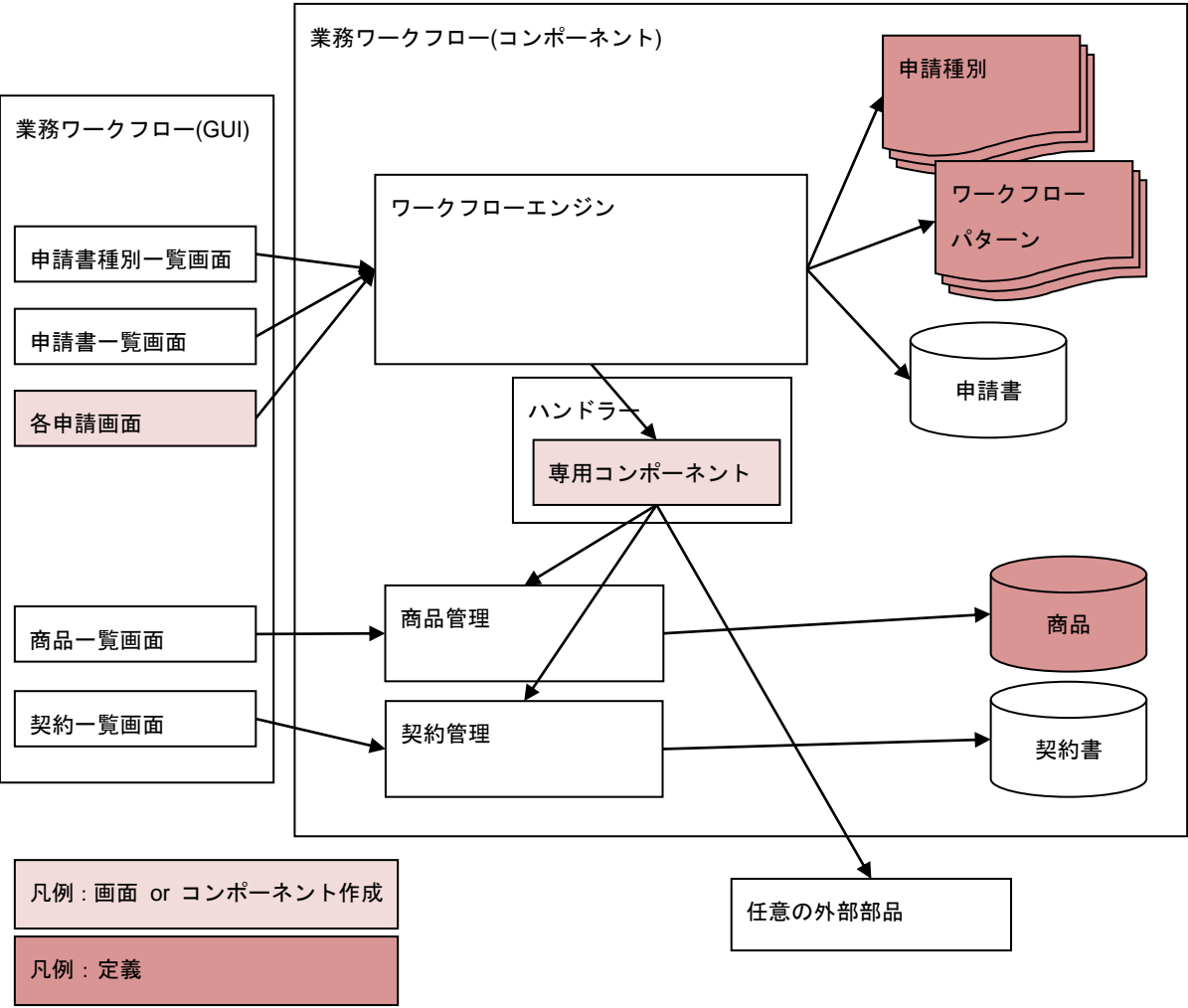


図 3 アプリケーション構成図

2.6.2 お問い合わせ

2.6.2.1 概要

ポータル内でテナントをご利用中のお客様と、ポータルの運用者様との間での、Q&A 等のやりとりに利用する機能です。

ポータル画面上で、お問い合わせの申請やその回答を行うことができます。

ワークフローは以下のように定義されています。

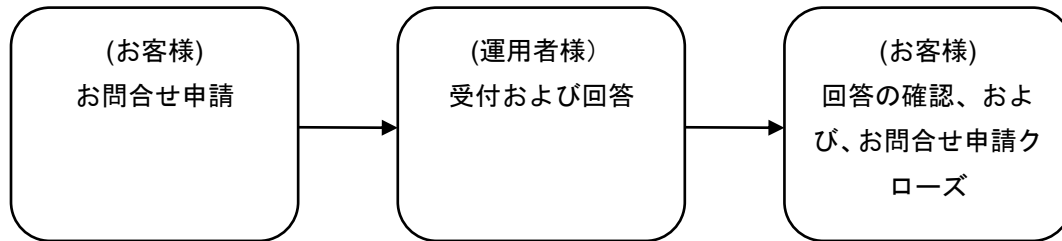


図 4 お問い合わせのワークフロー

2.6.3 商品契約申請

2.6.3.1 概要

商品契約・解約のための申請機能です。

本機能は、OpenStack 上のリソースに対し、利用契約・解約を行う機能です。

商品として、CPU、メモリ、ディスクのセット商品が定義されており、申請により、商品契約、あるいは解約をすることができます。

商品は、定額制で、月額での課金を想定しています。

申請が行われ、承認されて契約が成立すると、OpenStack 上で利用可能なリソースを、申込みいただいたテナントに対し割り当てる仕様となっています。

また、契約情報は、契約管理上に記録され、履歴を参照することが可能です。

なお、NEC Cloud System ポータルでは課金機能を提供していません。

ただし、商品・契約管理上で管理されるデータを利用して、定額制の課金計算を行っていただく、あるいは、商品・契約管理と、OpenStack 標準サービスである Ceilometer を組み合わせて、従量制の課金計算を行っていただくことなどが可能です。

お客様のご利用環境に応じて、別途、課金機能をご用意ください。

2.6.3.2 新規申請

ワークフローは以下のように定義されています。

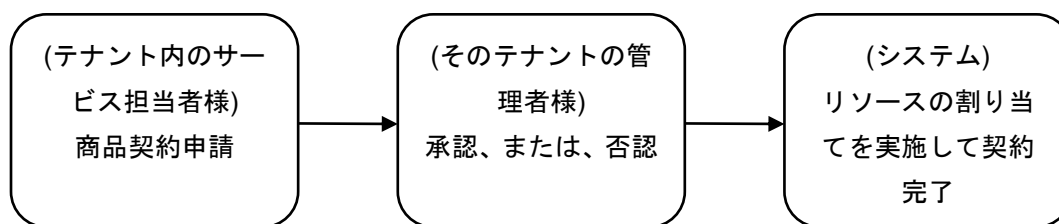


図 5 新規申請のワークフロー

2.6.3.3 解約申請

ワークフローは以下のように定義されています。

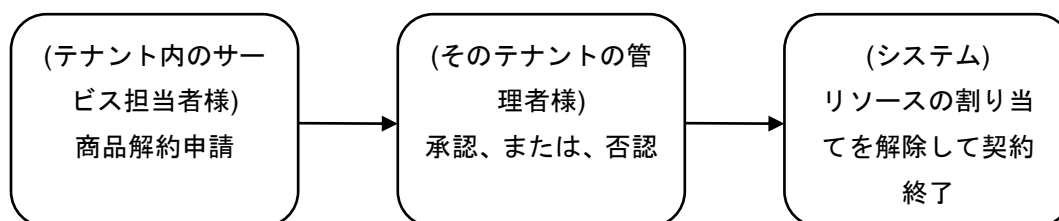


図 6 解約申請のワークフロー

2.6.4 入会・退会申請

2.6.4.1 概要

テナント未契約者様が NEC Cloud System ポータルを初めて利用するために入会をするワークフローです。テナント未契約者様が Drupal から申請を出し、契約管理者様が承認をすることで基本契約が締結されます。

契約管理者様は申請を受け付けると、テナント作成、ユーザ作成、グループ作成、権限付与等の入会準備作業を手動で行い入会準備ができたことをテナント未契約者様に手動メール送信を行います。

テナント管理者様が申請を出し、契約管理者様が承認をすることで契約の解約が締結されます。

契約管理者様は申請があると、テナント無効化、ユーザ無効化、サービスアクセス制御のためのネットワークリソース削除を行いテナント管理者様へ退会日が決まったことを手動でメール送信を行います。システム管理者様は後日、実リソースを手動で削除します。

子テナントがあるテナントの場合は、解約失敗となります。

2.6.4.2 入会申請

ワークフローは以下のように定義されています。

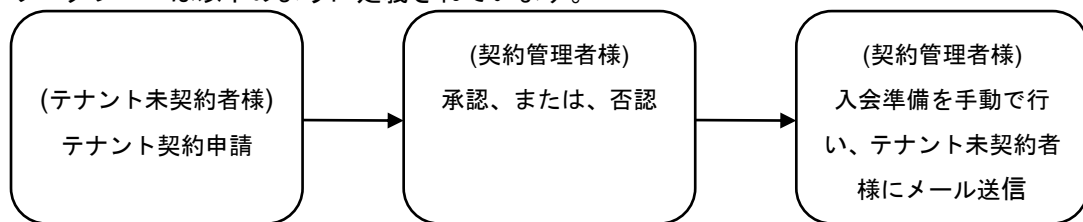


図 7 テナント契約申請のワークフロー

2.6.4.3 退会申請

ワークフローは以下のように定義されています。

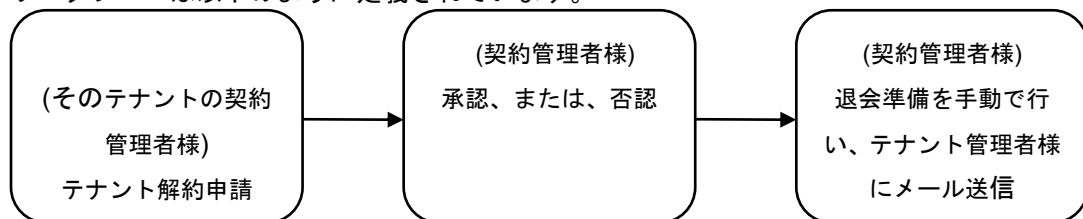


図 8 テナント解約申請のワークフロー

2.6.5 お知らせ登録(メンテナンス情報)

2.6.5.1 概要

事業者内で、お知らせシステムへのメンテナンス情報の登録業務ワークフローです。

事業者はお知らせシステムへ登録する内容を申請し、サービス管理者様は申請内容を承認することができます。

お知らせシステムへメンテナンス情報の自動登録ができます。

ワークフローは以下のように定義されています。

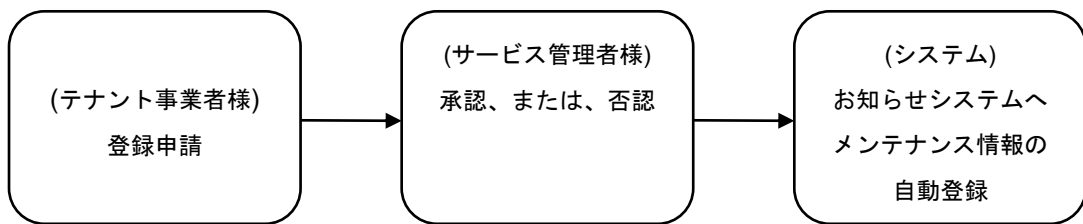


図 9 お知らせ登録のワークフロー

2.6.6 Quota 購入変更

2.6.6.1 概要

従量課金契約から Quota 購入契約への変更申請機能です。

テナント利用者様は契約変更時にリソースの使用量を事前に計測し、Quota 購入契約へ変更依頼時に Quota 購入数を指定し申請します。契約管理者様が契約承認することで、自動的に従量課金契約が解約され、Quota 購入契約が締結されます。

商品の有効期限がすでに切れている場合は、契約失敗となります。

Quota 購入数より使用中のリソース量が多い場合、契約失敗となります。

従量課金契約が既に締結されている場合は、契約失敗となります。

ワークフローは以下のように定義されています。

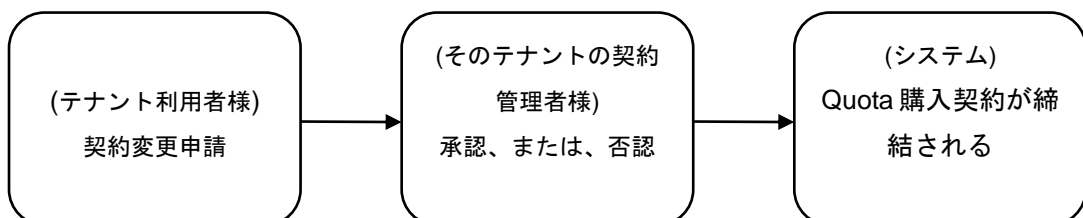


図 10 Quota 購入変更のワークフロー

2.6.7 従量課金契約変更

2.6.7.1 概要

CPU、メモリ、ストレージのリソース使い放題（一定の上限内）を購入申請する機能です。

テナント利用者が申請を出し、テナントの契約管理者様が承認することで契約が締結され、Quota 値はサービス管理者様が指定した上限に自動的に設定されます。

商品の有効期限がすでに切れている場合は、契約失敗となります。

Quota 購入契約が既に締結されている場合は、契約失敗となります。

量課金契約が既に締結されている場合は、契約失敗となります。

テナント利用者は申請した後、契約管理者様が契約承認することで、自動的に Quota 購入契約が解約され、従量課金契約が締結されます。

商品の有効期限がすでに切れている場合は、契約失敗となります。

2.6.7.2 契約変更申請

ワークフローは以下のように定義されています。

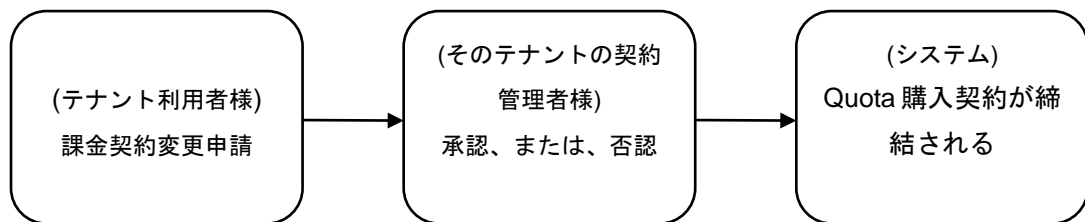


図 11 従量課金契約変更のワークフロー

2.6.7.3 解約申請

ワークフローは以下のように定義されています。

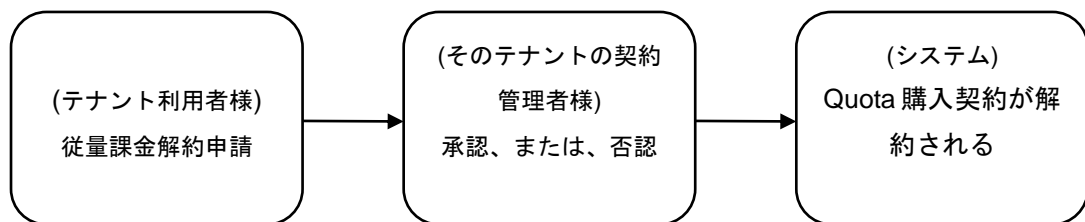


図 12 従量課金解約のワークフロー

2.6.8 オブジェクトストレージ契約

2.6.8.1 概要

従量課金契約の一種です。

オブジェクトストレージ管理機能を使用するための申請機能です。

テナント利用者が申請を出し、契約管理者様が承認することで契約が締結され、オブジェクトストレージ管理機能がすぐに使用可能になります。

商品の有効期限がすでに切れている場合は、契約失敗となります。

オブジェクトストレージ契約がすでに締結されている場合は、契約失敗となります。

テナント利用者が従量課金契約を解約申請した後、契約管理者様が解約承認をすることで、承認日時を解約日時として従量課金契約の解約が締結され、契約内容が自動反映されます。システム管理者は後日、実リソースを手動で削除します。

2.6.8.2 契約申請

ワークフローは以下のように定義されています。

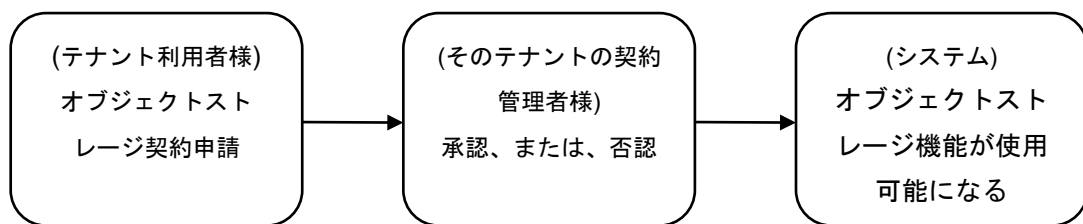


図 13 オブジェクトストレージ契約のワークフロー

2.6.8.3 解約申請

ワークフローは以下のように定義されています。

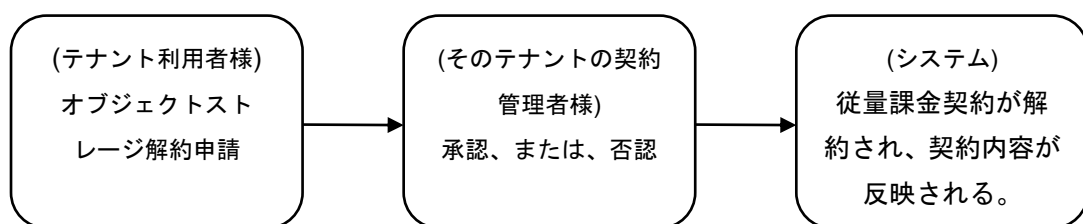


図 14 オブジェクトストレージ解約のワークフロー

2.7 キャパシティ管理

region_portal のみに提供される機能です。

2.7.1 概要

OpenStack 上で管理されるリソースの使用状況を監視するための機能です。

リソース使用状況を参考に、適切なタイミングで、リソースの増強や配分を行うための情報を提供します。

リソースの使用状況は、ポータル画面上にグラフで表示されます。

グラフは、システム全体、OpenStack が管理するアベイラビリティゾーンごと、OpenStack が管理するホストごと、といった単位で参照できます。

また、参照できるのは、CPU、メモリ、ディスクに関するリソースの使用状況です。

2.8 証跡管理

2.8.1 概要

ポータル画面の操作ログを確認できます。

操作ログは、ポータル画面に一覧表示され、いつ、だれが、どんな操作を行ったかを参照することができます。アクセス解析や、問題発生時の調査に活用することができます。

また、ログの絞り込み検索を行うことが可能です。

2.9 ログ管理

2.9.1 概要

ポータルの運用者様が、運用環境上の様々なログの解析を行うための機能です。

ログ情報の保存に当たっては、バックエンドに、オープンソースである Elasticsearch を利用しています。

ログ収集には、同じくオープンソースである、Logstash を利用します。

ログの解析と結果表示には、Elasticsearch のプラグインである Kibana を利用しています。

また、ポータル画面に、Kibana の GUI を埋め込んでおり、ポータルからシームレスに操作できます。

運用者様が Logstash を使用して、独自にログを収集して Elasticsearch に登録していただくことで、Kibana によるログ解析と、解析結果のグラフィカルな表示が可能となり、ログの収集や監視に活用いただけます。

2.10 設定管理

2.10.1 概要

ポータル運用者様がポータルを含めたシステム運用をするうえで、必要な資料の文書管理を行える機能です。

インフラストラクチャのパラメータシートなど、運用上必要な資料を GitLab に登録していただくことができ、文書の整理や、安全な管理が可能です。

バックエンドに、GitLab を利用しており、ポータル画面からの GitLab の GUI へのリンクを設けています。

2.11 オブジェクトストレージ管理

region_portal のみに提供される機能です。

2.11.1 概要

NEC Cloud System ポータルでは、コンテンツのバックアップ、アーカイブなど、大容量データの保存先として、オブジェクトストレージを利用可能です。

保存先ストレージには、NEC iStorage HS シリーズ（HYDRAstor）を利用しています。

オブジェクトの操作は、OpenStack Horizon 標準の GUI、もしくは、HS が提供するインターフェース（S3 互換 API）を用いて行うことができます。

ただし、OpenStack Horizon 標準の GUI では、オブジェクトに対するアクセスコントロール設定を行う画面がありません。

このため、拡張機能として、アクセスコントロール設定画面を提供します。

この拡張機能を利用することで、GUI から、HS に対して、アクセスコントロール設定が可能になります。

2.12 お知らせ機能

2.12.1 概要

お知らせ機能は、OSS の Drupal を利用し、以下の 3 つの機能を提供します。

1. グローバルポータル画面に、テナントユーザに向けたサービス管理者からのお知らせを掲示します。お知らせ情報の掲載は、Drupal の WEB 画面上から「コンテンツ登録」として実施するか、業務ワークフローの 申請・承認 機能を利用して掲載することができます。

お知らせ情報のスコープは、下表の 3 種が存在します。

- ・ システム全体に関わる情報
- ・ 特定リージョンに関わる情報
- ・ 特定テナントに関わる情報

2. リージョンポータル画面に、申請/契約の未完了件数を表示することが出来ます。Keystone と業務ワークフローへの REST API 呼び出し結果を掲示します。カスタマイズすることで他のコンポーネン

トの REST API を呼び出した結果を掲示することが出来ます。

3. 未契約者向けの新規テナント申し込み画面を提供します。サービス管理者が統合ポータル画面で、未契約者からの契約申し込みを管理することが出来ます。

お知らせ機能は、Contents Management System (以降 CMS)として Drupal を使用して実現しています。

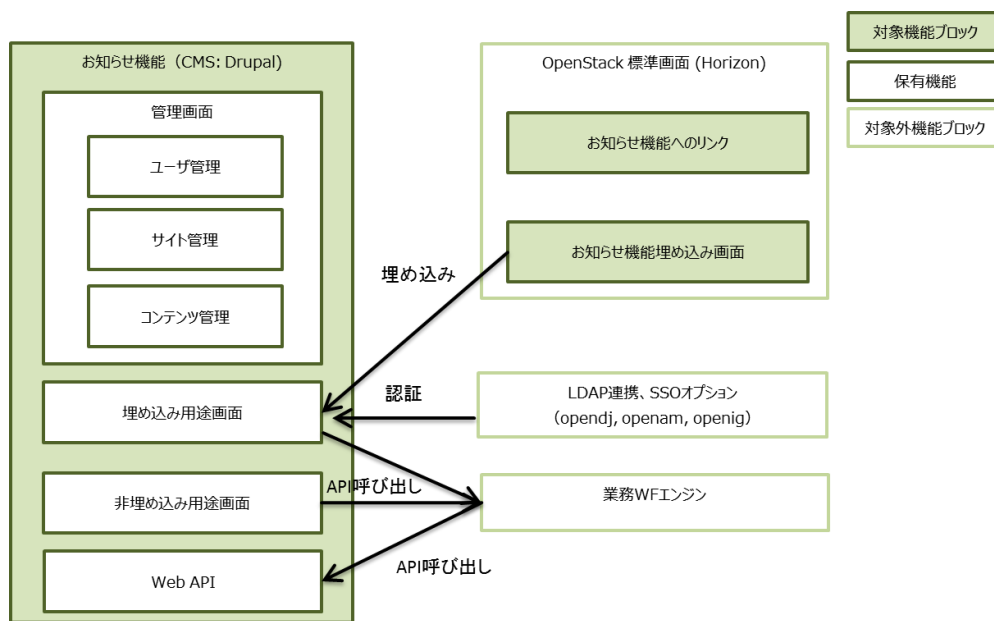
2.12.2 機能ブロック構造

お知らせ機能の機能ブロック構造を下図に示します。

「対象機能ブロック」が、お知らせ機能で実現する機能です。

「保有機能」とは、Drupal が持つ基本機能であり、これを利用することで、お知らせ画面のレイアウト、デザインを構築しています。

「対象外機能ブロック」は、ユーザ連携を実現するため、及び NEC Cloud System ポータルのコンポーネントです。



【お知らせ機能-機能ブロック構造】

2.12.3 お知らせ機能 (Drupal)

2.12.3.1 ユーザ管理

CMS のユーザを管理する機能です。

ユーザとテナントを紐付けるためのロール設定が行えます。

v

2.12.3.2 サイト管理

Drupal で構築するウェブサイト进行管理する機能です。

埋め込み画面、および非埋め込み用途画面のメンテナンスを行うことができます。

2.12.3.3 コンテンツ管理

Drupal で作成するコンテンツ进行管理する機能です。

埋め込み用途画面、および非埋め込み用途画面に掲載するコンテンツのメンテナンスを行うことができます。

2.12.3.4 埋め込み用途画面

Openstack 標準画面 (Horizon) に iframe で埋め込まれる画面です。

サービス管理者が CMS のサイト管理機能を用いて、お知らせ画面として作成します。この画面で、テナントユーザに向けたサービス管理者からのお知らせを掲示します。

2.12.3.5 非埋め込み用途画面

Openstack 標準画面 (Horizon) とは別の単独のサイトとして公開する画面です。

サービス管理者が CMS の画面メンテナンス機能を用いて、テナント新規申し込み画面として作成します。

この画面で、未契約者向けの新規テナント申し込み画面を表示します。

2.12.3.6 Web API

Drupa I が備えている REST API です。

業務ワークフローエンジンから呼び出されます。

2.12.4 OpenStack 標準画面(Horizon)

2.12.4.1 お知らせ機能へのリンク

NEC Cloud System ポータル v1 で実装済みの「他 SW 呼出し」機能です。

今回、CMS へのリンクを追加します。

2.12.4.2 お知らせ機能埋め込み画面

埋め込み用途画面を埋め込むための画面です。
Horizon の新規メニューとして表示します。

2.12.5 Keystone 連携、SSO オプション

NEC Cloud System ポータルユーザと Drupal ユーザの連携と認証を実現します。

2.12.6 業務ワークフローエンジン

NEC Cloud System ポータルにおいて機能強化を行うポータルのコンポーネントです。

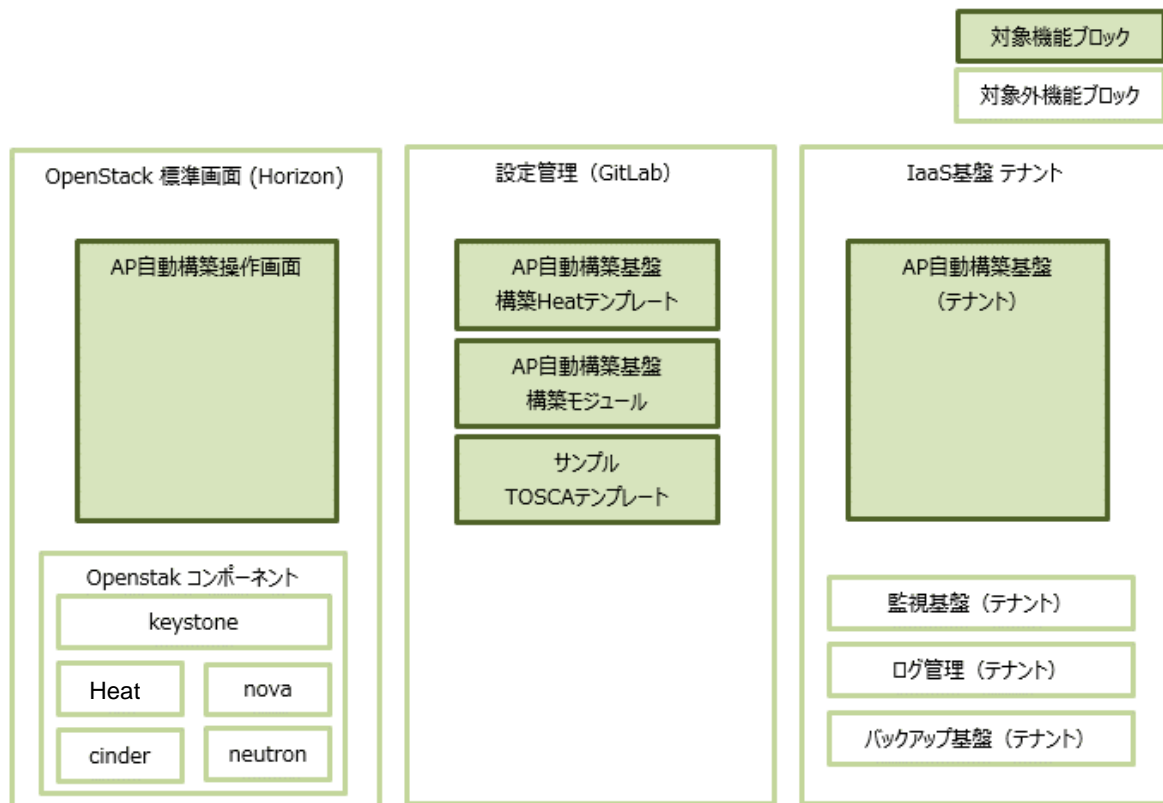
2.13 TOSCA テンプレートプロビジョニング機能

2.13.1 概要

テナントユーザが、ポータル上で TOSCA テンプレートプロビジョニングを実現する機能です。
本機能は大別して、プロビジョニングを操作する画面と、それを実現する基盤とに分かれます。
基盤には、OSS である Cloudify-Manager を利用しています。

2.13.2 機能ブロック構造

TOSCA テンプレートプロビジョニング機能の機能ブロック構造を下図に示します。
「対象機能ブロック」が、TOSCA テンプレートプロビジョニング機能で実現する機能です。



【TOSCA テンプレートプロビジョニング機能-機能ブロック構造】

2.13.3 AP 自動構築操作画面

Openstack 標準画面 (Horizon) に追加する、AP 自動構築基盤 (テナント) を操作するための画面です。

テナントユーザが利用します。

2.13.4 AP 自動構築基盤構築 Heat テンプレート

設定管理 (GitLab) にサービス管理者が配置する、Heat テンプレートです。

Openstack コンポーネントの Heat に投入することで、IaaS 基盤テナントの AP 自動構築基盤 (テナント) を構築できます。

2.13.5 AP 自動構築基盤構築モジュール

AP 自動構築基盤 (テナント) を構築する際に、必要とする構築モジュールです。

AP 自動構築 Heat テンプレートから参照します。設定管理 (GitLab) にサービス管理者が配置します。

2.13.6 サンプル TOSCA テンプレート

AP 自動構築基盤 (テナント) に投入する TOSCA テンプレートです。

AP 自動構築基盤操作画面で使用できます。テナントユーザが利用します。

2.13.7 AP 自動構築基盤

IaaS 基盤テナント上に、AP 自動構築 Heat テンプレートおよび AP 自動構築基盤構築モジュールで構築できる機能です。AP 自動構築操作画面から TOSCA テンプレートを投入することで、OpenStack コンポーネントの外部公開 API を利用し、自身のテナント上に vApp をプロビジョニングできます。

2.14 ポリシー制御機能

2.14.1 概要

ユーザごとに、利用可能な機能/リソースを制御するための機能です。

事業者ユーザ、階層化プロジェクト、テナントユーザの管理機能、各ユーザの権限管理の機能を有しており、「ポリシー制御画面」で設定が行えます。

2.14.2 事業者権限の分離

クラウドサービスを提供する事業者は一般的に、システム全体を統括する管理者と、各 DC やリージョンなどのシステム単位に管理する管理者に分けられます。また、その管理者も担当する役割に応じて、職責が分離されます。

そのため、あらかじめシステムとして、DC/リージョン/役割の単位でロールを定義します。

また、上位の管理者が下位の管理者を作り権限を委譲することで、権限の階層化を実現します。

2.14.3 事業者ユーザのセルフ管理

事業者ユーザのユーザ管理を各権限の上位であるスーパーアドミンが実施しては、スーパーアドミンの負荷が高くなります。通常、事業者内に置いては、システム管理者、契約管理者、サービス管理者で組織が分かれ、それぞれが独立して組織運営ができる必要があるため、それぞれにプロジェクトを用意し、スーパーアドミンからユーザ管理権限を委譲してもらい、各権限のプロジェクト内でユーザをセルフ管理します。

2.14.4 テナントユーザのサービス利用権限の分離

テナントユーザにおいては、プロジェクト内でのリソースの管理対象に応じて、利用可能なサービスを限定することで、プロジェクト内の職責分離や内部統制を実現できる必要があります。

テナントユーザに対するロールの定義も、事業者ユーザ同様に、最小の分割単位でロールを定義した後、階層に応じて、必要なロールをユーザに付与します。

2.14.5 テナントソースの分割

テナントユーザ自身がサブプロジェクトを用意し、そのサブプロジェクトごとに利用可能なリソース量を分配し、分配されたサブプロジェクトにユーザを紐で来ることで、リソース量の分割を行います。