目次

- 改訂情報
- システム管理者について
- システム管理者画面
  - システム管理者としてログインする
  - システム管理者の画面について
- システム環境構築
  - ライセンス管理
  - データソース設定
  - テナント管理
  - テナント環境セットアップ
  - Solr接続設定
- システム管理
  - モジュール参照
  - サービス設定
  - アプリケーションロック一覧
  - ファイル操作
  - データベース操作
  - 非同期-タスクキュー一覧
  - シェアードデータベース設定
  - ログインセッション一覧
  - 一般ユーザ管理
  - ポートレット管理
  - ポータル設定
  - クロスオリジンリソース共有設定
- システム管理者設定
  - パスワードを変更する
  - ロケールを変更する
  - 多要素認証を設定する
- 多要素認証を行う
  - 確認コードを利用してログインする
  - バックアップコードを利用してログインする
  - ログインできなくなってしまった場合

改訂情報

変更年月日	変更内容
2012-10-01	初版
2013-04-01	第2版 下記を追加・変更しました ▪ 「*モジュール参照*」を追加 ▪ 「*パスワードを変更する*」を追加
2014-08-01	第3版 下記を追加・変更しました ▪ 「*ロケールを変更する*」を追加 ▪ 「*テナント管理*」を追加 ▪ 「*データソース設定*」を変更 ▪ 「*Solr接続設定*」を追加 ▪ 「*システム管理者の画面について*」を追加 ▪ 「*ログインセッション一覧*」を追加 ▪ 「*システム管理者としてログインする*」を追加
2014-12-01	第4版 下記を追加・変更しました ▪ 「*ログインセッション管理*」を追加 ▪ 「*テナント環境情報*」に「グローバルナビ最大表示数」を追加 ▪ 「*テナント環境情報*」に「グローバルナビ最大表示数」を追加 ▪ 「*システム管理者用ホームウィジェット*」のシステム情報にダウンロードリンクを追加 ▪ 他のドキュメントへの参照をリンクに変更
2015-04-01	第5版 下記を追加・変更しました ▪ 「*ライセンス設定*」にテナントごとのライセンス数初期値の説明を追加 ▪ 「*ライセンス管理*」に注意を追加 ▪ 「*Solr接続設定*」の「*Solr接続設定 入力項目*」にポート番号についてのノートを追加 ▪ 「*システム管理者の画面について*」の画像を最新バージョンに変更 ▪ 「*サービス設定*」の画像を最新バージョンに変更
2015-08-01	第6版 下記を追加・変更しました ▪ 「*LDAP連携・設定*」に 2014 Spring(Granada) 以降のバージョンでLDAP認証モジュールを追加する場合の記載を追加 ▪ 「*Apache Cassandra接続情報*」に 2014 Spring(Granada) 以降のバージョンでIMBoxモジュールを追加する場合の記載を追加 ▪ 「*Solr接続設定*」の「*Solr接続設定 入力項目*」に「分散検索」を追加
2015-12-01	第7版 下記を追加・変更しました ▪ 「*ライセンス管理*」の説明を追加
2016-04-01	第8版 下記を追加・変更しました。 ▪ 「*テナント環境情報*」に日付・時刻の入力形式の変更を追加 ▪ 「*パスワード保存方式設定*」を追加
2016-12-01	第9版 下記を追加・変更しました。 ▪ ブックマークウィジェットのリンク先名称の変更に伴い、「*システム管理者の画面について*」内の画像を修正。

変更年月日	変更内容
2018-04-01	第10版 下記を追加・変更しました ▪ 「*多要素認証*」を追加
2018-08-01	第11版 下記を追加・変更しました ▪ 「*多要素認証を設定する*」を追加 ▪ 「*多要素認証を行う*」を追加
2018-12-01	第12版 下記を追加・変更しました ▪ 「*非同期-タスクキュー一覧*」の画像を最新バージョンに変更 ▪ 「*非同期-タスクキュー一覧*」に「タスクの実行詳細を確認する」を追加 ▪ 「*テナント環境情報*」のリソース参照名に関する注意の説明を変更 ▪ 「*ファイル操作*」の画像を最新バージョンに変更 ▪ 「*データベース操作*」の説明を変更
2019-08-01	第13版 下記を追加・変更しました ▪ 「*クロスオリジンリソース共有設定*」を追加
2019-12-01	第14版 下記を追加・変更しました ▪ 「*データソース設定*」に selectMethod の指定に関する説明を追加
2020-04-01	第15版 下記を追加・変更しました ▪ 「*サービスを停止する*」を追加 ▪ 「*サービスを再開する*」を追加 ▪ 「*クロスオリジンリソース共有設定*」の「*クロスオリジンリソース共有設定を登録する*」のパスに関する説明を変更

システム管理者について

intra-mart Accel Platform では、ひとつの intra-mart Accel Platform システムを独立した複数の会社などのグループで共同利用するような場合には WARファイルによる複数テナント や バーチャルテナントによる複数テナント として構築することができます。

同じハードウェアやアプリケーションを利用していながら、ロール、ユーザ、メニューそしてデータベースなどはテナントごとに異なる設定で利用できます。
そのため、各テナントが個別の intra-mart Accel Platform システム利用している感覚で使用することができます。

intra-mart Accel Platform では、共同で利用するそれぞれのグループを「テナント」、その管理者を「テナント管理者」と呼んでいます。
そして、これら「テナント」や「テナント管理者」を統括管理するのが「システム管理者」です。

システム管理者は、 intra-mart Accel Platform のデータベース設定など共通の設定管理と各テナントとその管理者に関する管理を行います。

システム管理者画面

ここではシステム管理者の画面について説明します。

システム管理者としてログインする

- Webブラウザより 以下のURLへアクセスします。

  システム管理者ログイン画面： *http://<HOST>:<PORT>/<CONTEXT_PATH>/system/login*

  > **コラム**
  >
  > 下記構築例の場合、システム管理者へのログイン画面へのURLは次の通りです。
  > システム管理者ログイン画面： *http://localhost:8080/imart/system/login*
  >
  > | 項目 | 例 |
  > |---|---|
  > | <HOST> | 「ローカル環境（localhost）」 |
  > | <PORT> | 「8080」ポート |
  > | <CONTEXT_PATH> | 「imart」 |

  構築された環境によってログイン画面へのURLは異なります。詳細については、環境を構築した管理者にお問合せください。

  > **コラム**
  >
  > 多要素認証を利用する場合、以下の設定を行ってください。
  > 「*多要素認証を有効化する*」

  > **コラム**
  >
  > 多要素認証を利用したログイン手順は以下を参照してください。
  > 「*多要素認証を行う*」

システム管理者の画面について

システム管理者のホーム画面から intra-mart Accel Platform の各種システム情報にアクセスできます。

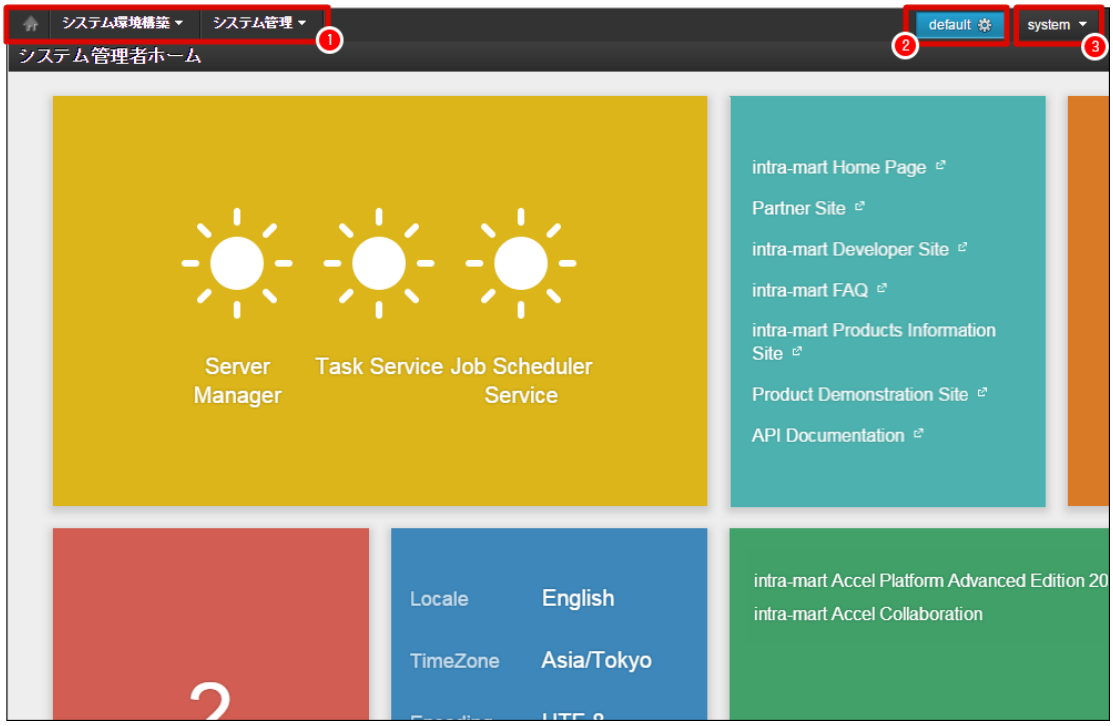
目次

- システム管理者のホーム画面
  - システム管理者のメニュー
  - テナントの切り替え
  - システム管理者用ホームウィジェット
    - ウィジェットを移動する

システム管理者のホーム画面

システム管理者のメニュー

ここではシステム管理者が標準で操作できるメニューについて説明します。



1. グローバルナビ
   システム環境構築やシステム管理の各種メニューにアクセスできます。

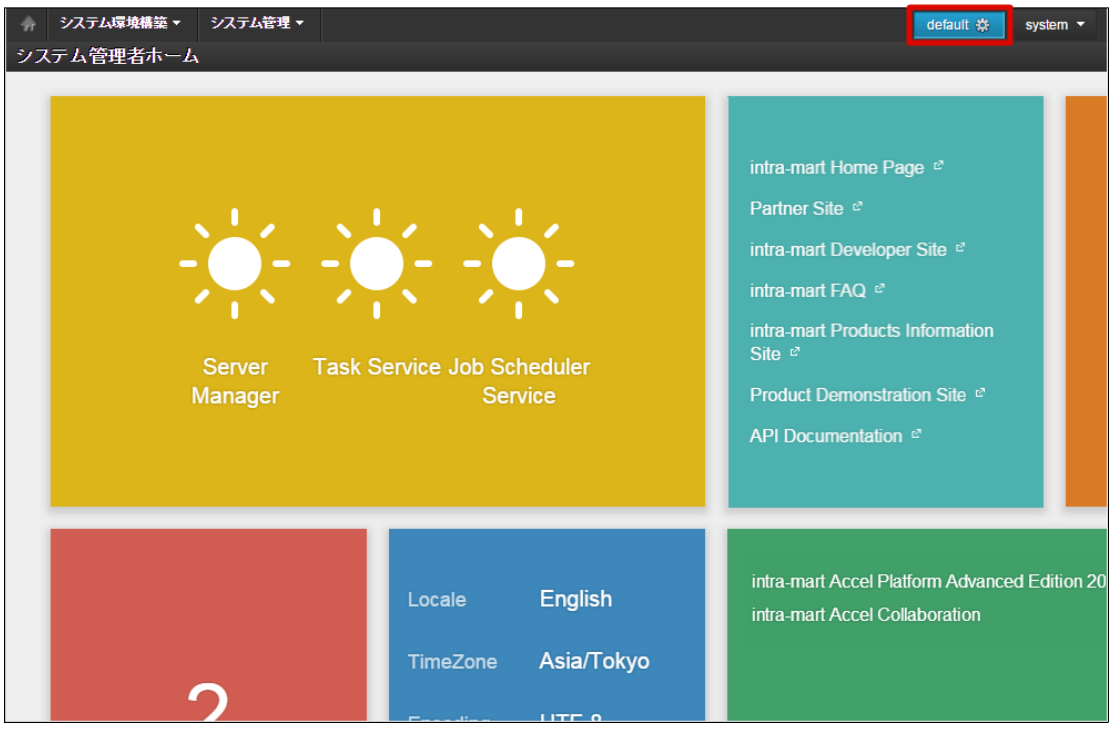
2. 操作中のテナントID
   現在操作中のテナントIDを確認できます。

3. ユーティリティメニュー
   メニューから各種機能を利用するためには、メニューグループカテゴリにメニューアイテムを登録する必要があります。
   メニューアイテムのリンク先のURLにアクセス権が設定されている場合のみ、画面上（グローバルナビ、サイトマップ等）に表示されます。

テナントの切り替え

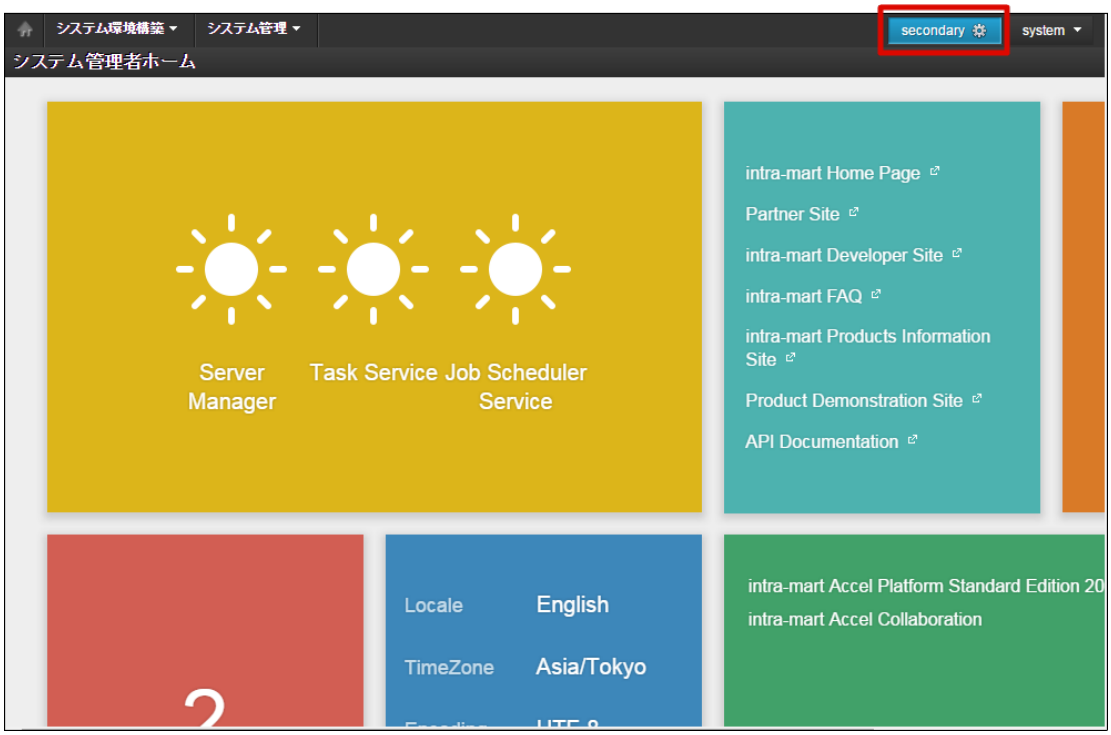
ここでは操作対象のテナントを切り替える方法を説明します。

1. 現在操作中のテナントIDの表示箇所をクリックします。



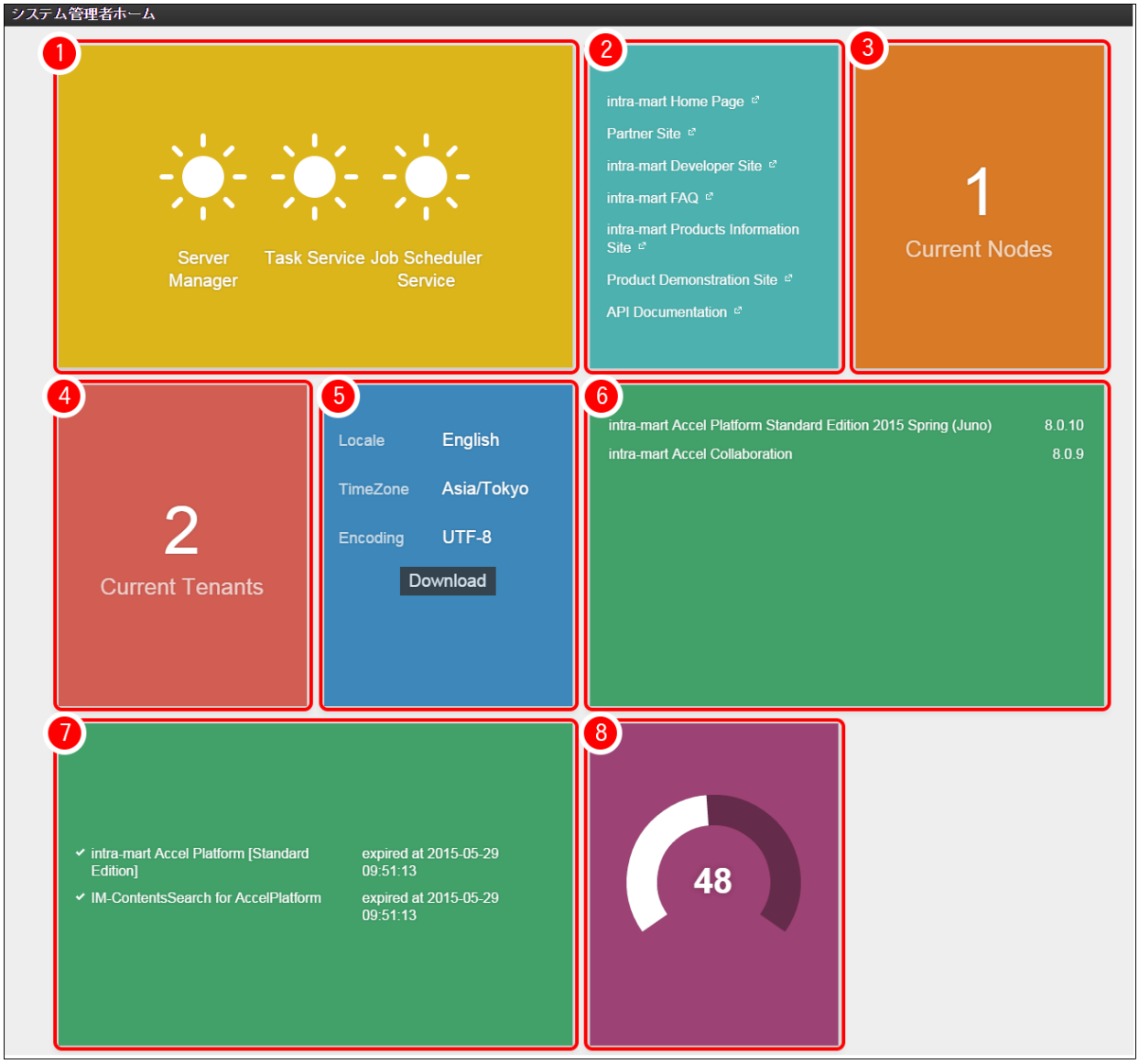
2. 切り替えたいテナントIDの行を選択し、「テナントを切り替える」ボタンをクリックしてください。

3. 操作対象のテナントを切り替えることができました。

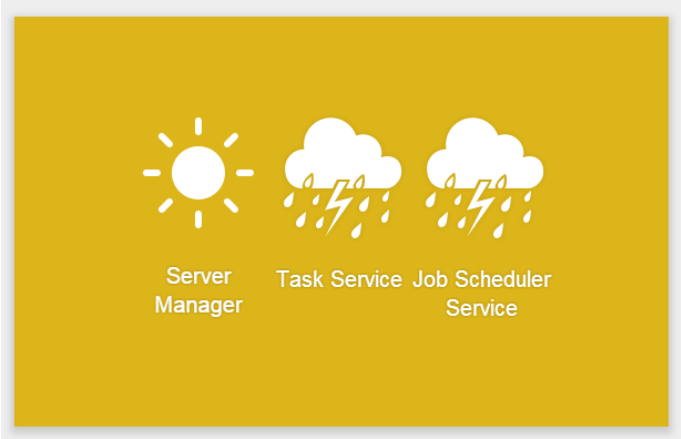


システム管理者用ホームウィジェット

システム管理者のホーム画面ではシステムの各種情報を確認できます。



1. システムサービスステータス
   システムサービスの稼働状況を示します。
   ウィジェットをクリックすると、「*サービス設定*」画面に遷移し、詳細を確認できます。



   晴れマークはシステムサービスが動作していることを示しています。
   雨マークはシステムサービスが停止していることを示しています。

2. ブックマーク
   ブックマークを表示します。

3. ノード
   現在システムを構築しているノードの数を表示します。
   ウィジェットをクリックすると「*サービス設定*」画面が表示されます。

4. テナント数
   現在システムに登録されているテナントの数を表示します。
   ウィジェットをクリックすると、「 *テナント管理* 」画面が表示されます。

5. システム情報
   以下のシステム情報を表示します。
   - ロケール
   - タイムゾーン
   - エンコーディング

   ダウンロードをクリックすると、「status.zip」がダウンロードできます。status.zipは弊社サポートへお問い合わせの際に問いあわせ内容とあわせて送付してください。
   （status.zipのダウンロードは2014 Winter(Iceberg)版以降で利用できます。）

6. プロダクト
   インストールされているプロダクトの一覧を表示します。
   ウィジェットをクリックすると「 *モジュール参照* 」画面が表示されます。

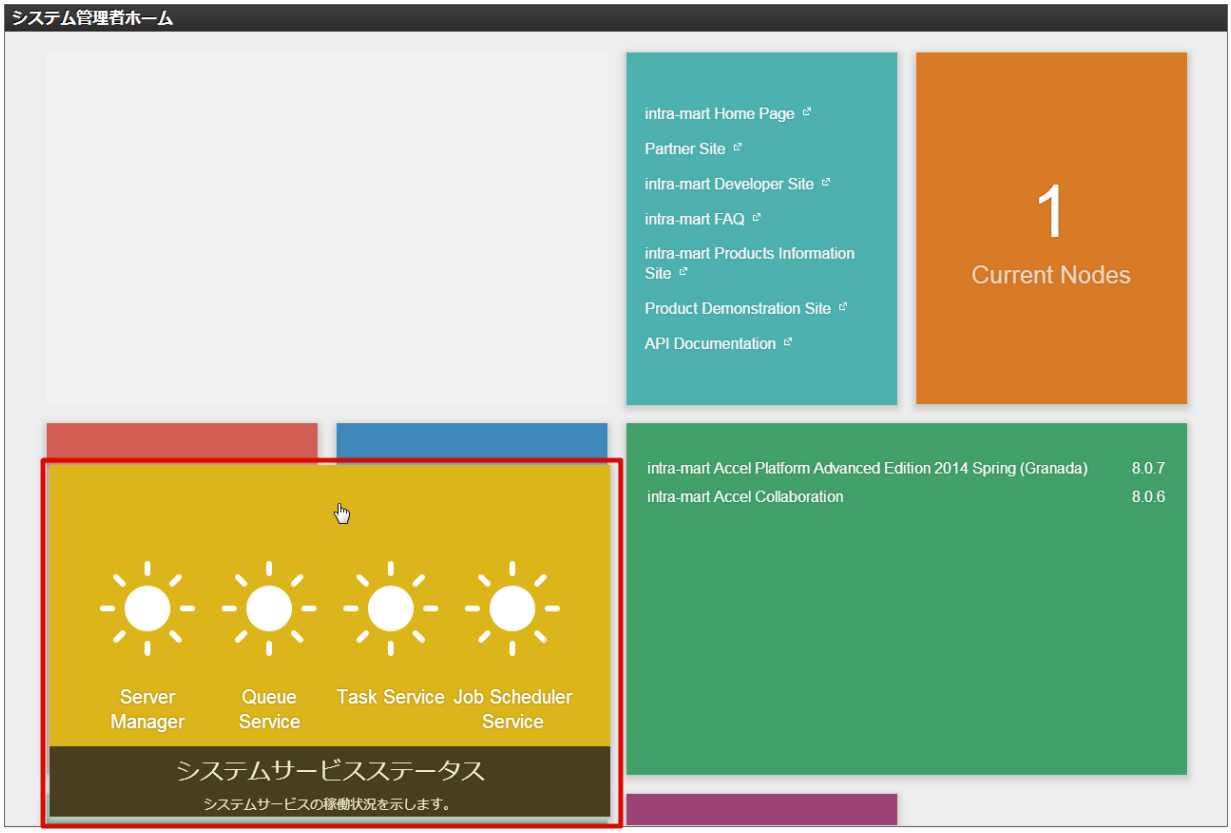
7. ライセンス
   インストールされているライセンスの一覧を表示します。
   ウィジェットをクリックすると「 *ライセンス管理* 」画面に遷移します。

8. メモリ使用量
   ヒープメモリの使用量をパーセント表示で確認できます。

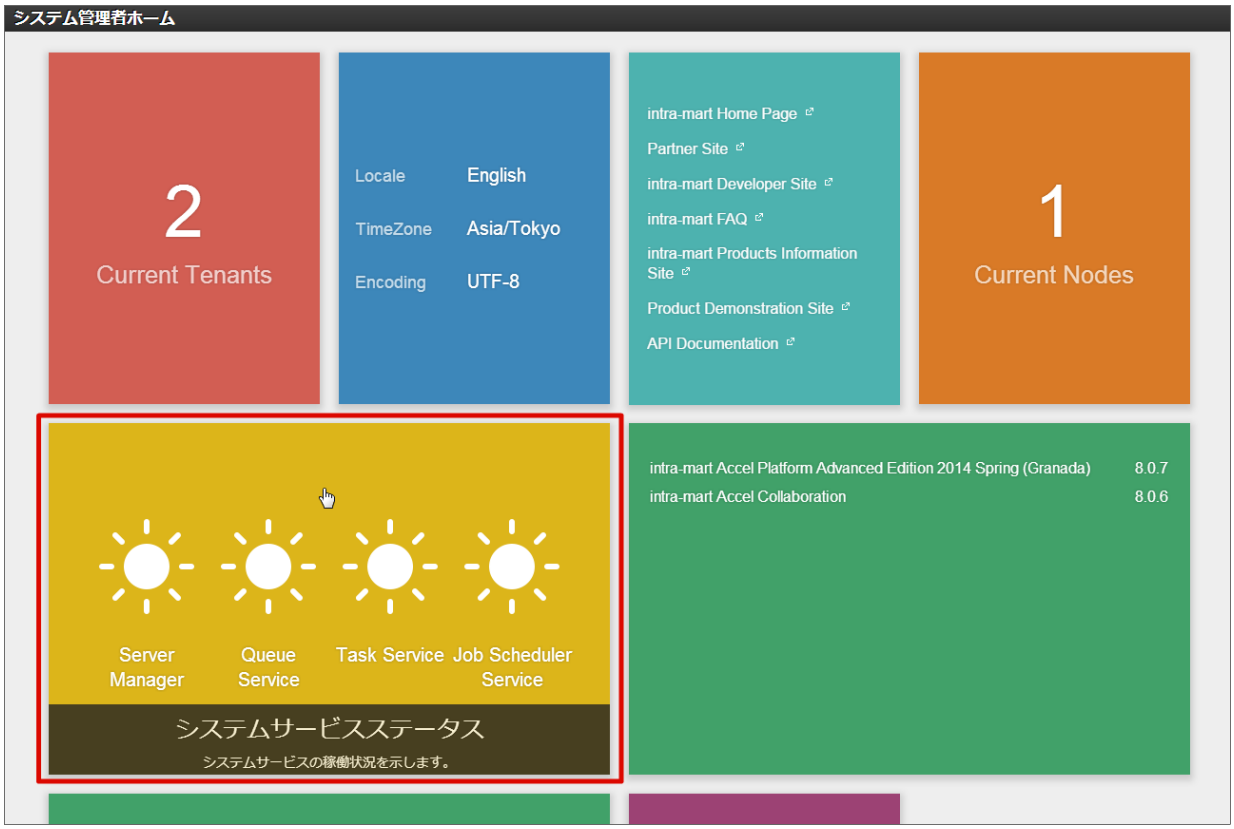
ウィジェットを移動する

1. 表示位置を変更したいウィジェットの任意の場所をドラッグします。

2. ウィジェットを移動する場所にドロップします。



3. 表示位置の変更が完了しました。
   変更した表示位置は保存されますので、再表示をおこなっても変更した表示位置で表示されます。



システム環境構築

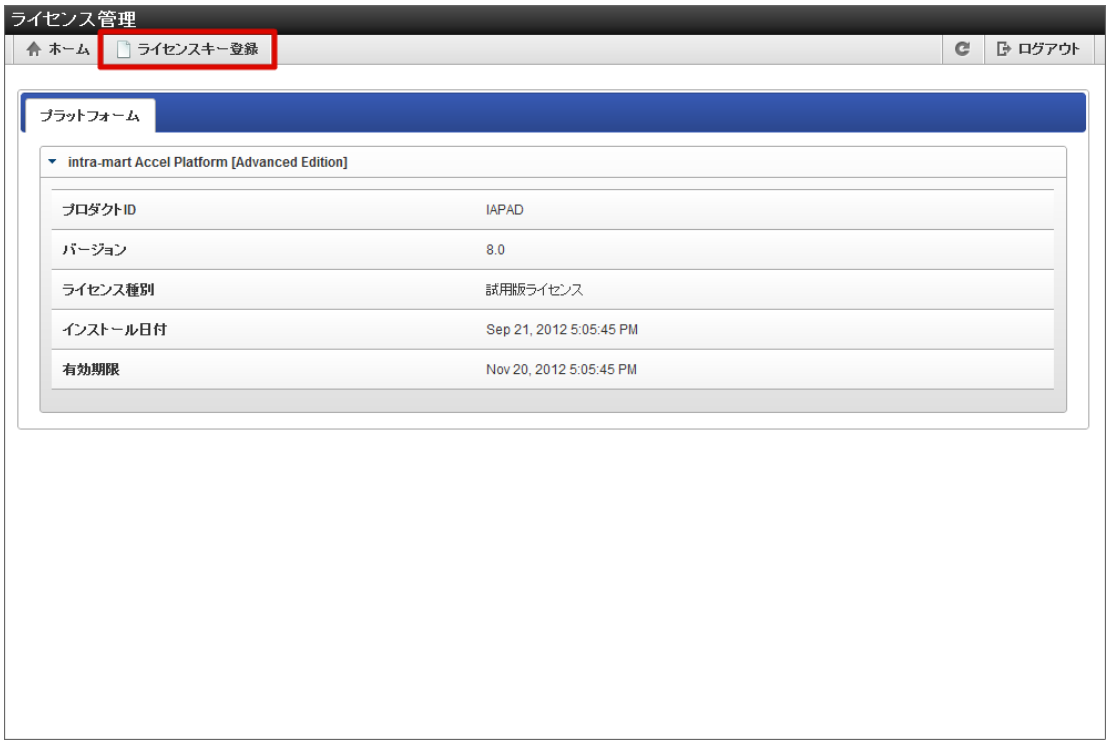
ここではシステム環境構築の操作を説明します。

ライセンス管理

intra-mart Accel Platform のライセンス情報を表示、登録します。

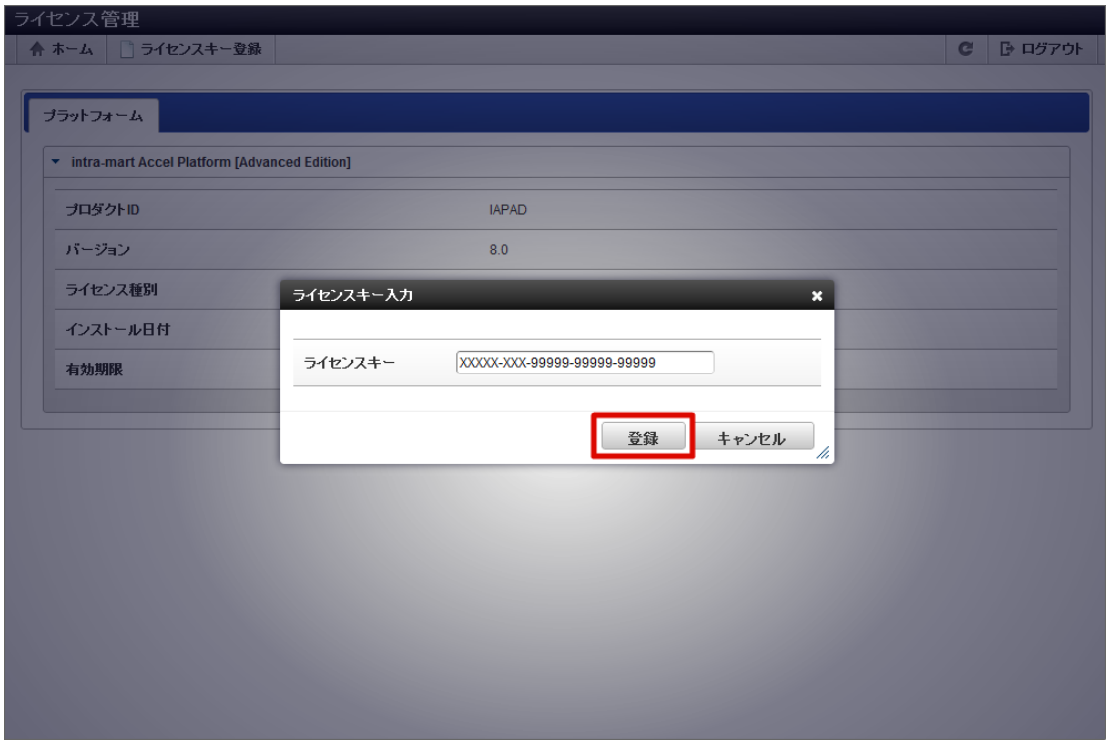
ライセンスを登録する

1. 「 システム環境構築 」→「ライセンス管理」をクリックします。
2. 「ライセンスキー登録」をクリックします。

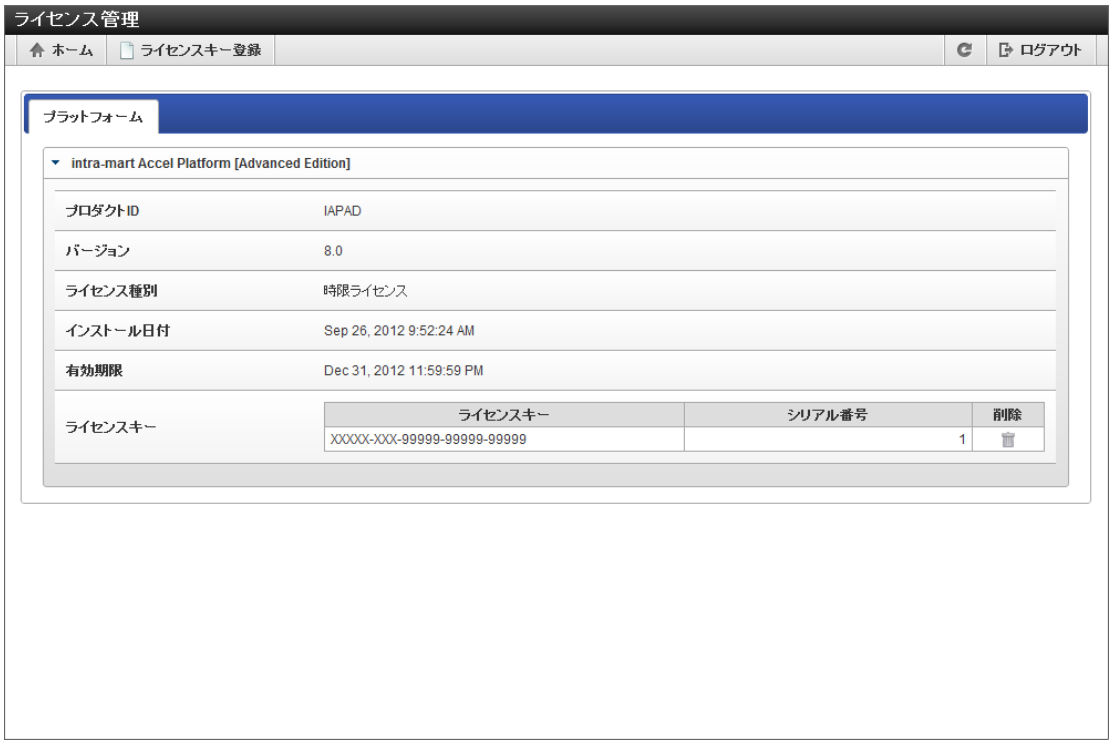


3. 「ライセンスキー入力」画面が表示されます。

4. 「登録」をクリックします。



5. ライセンスの登録が完了しました。



コラム

ライセンスを削除する場合

ライセンスキーの アイコンをクリックします。

注意

ライセンスを追加、変更する場合

既存のライセンスキーを削除せず、新規のライセンスキーを登録してください。

新規のライセンスキーを登録後、既存のライセンスキーを削除してください。（削除しなくても動作上問題はありません）

同じ製品のライセンスが複数登録されている場合、ユーザ数が多いライセンスが有効なライセンスとして扱われます。

注意

ライセンスの有効期限が切れた場合

一般利用者が利用する画面は表示できなくなり、システム管理者画面のみ表示可能です。
システム管理者画面よりライセンスキーを登録してください。
アプリケーションやエクステンションの一部のライセンスのみ有効期限が切れた場合も同様に、システム管理者画面のみ表示可能です。

注意

ライセンスキーを登録したアプリケーション製品を利用するためには
「テナント管理」-「ライセンス設定」からテナントごとの有効ライセンス数を設定する必要があります。
この手順を行わない場合、有効なアプリケーションライセンス数の上限は「0」となりアプリケーションを利用することはできません。
アプリケーションが利用できない場合にアプリケーションのページへアクセスした場合、403のエラーページが表示されます。

分散環境でのライセンスの登録

分散環境の場合、任意の Web Application Server 1台に、ライセンスをサーバ台数分登録します。

1. 任意の Web Application Server にシステム管理者としてログインします。
2. 「 システム環境構築 」→「ライセンス管理」をクリックします。
3. サーバ台数分のライセンスを登録します。ライセンスの登録方法は「*ライセンスを登録する*」を参照してください。

データソース設定

intra-mart Accel Platform で利用するテナントのデータソース情報を登録、参照します。

注意

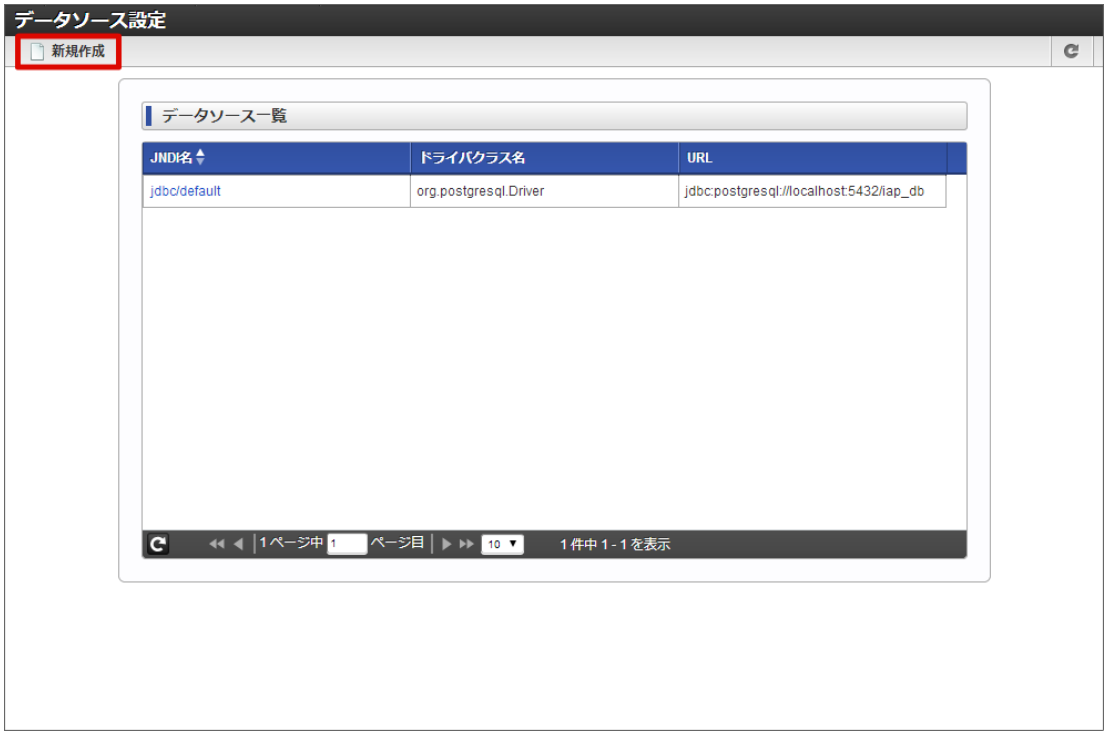
Resin または Payara 以外の Web Application Server の場合、データソース設定は行えません。

目次

- データソースを登録する
- データソースを参照する

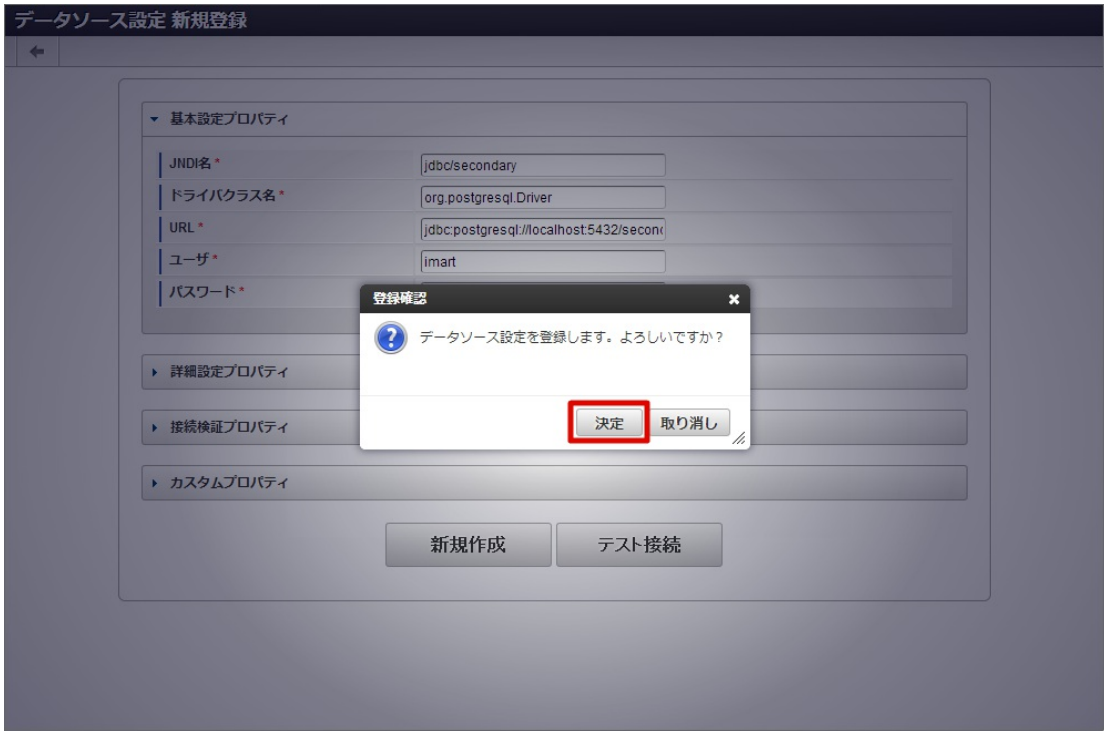
データソースを登録する

1. 「 システム環境構築 」→「データソース設定」をクリックします。
2. 「新規作成」をクリックします。



3. 内容を入力し、「新規作成」をクリックします。

4. 「決定」をクリックします。



5. データソースを登録できました。

コラム

テスト接続する場合

「テスト接続」をクリックします。

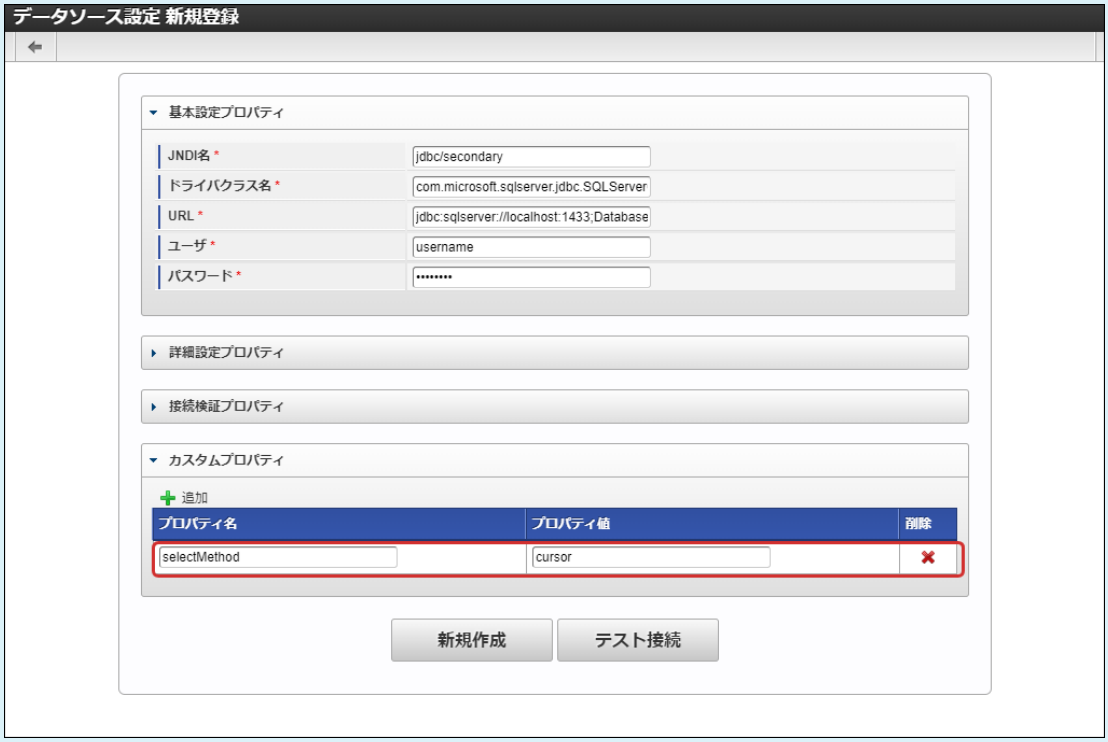
コラム

Microsoft SQL Server の場合に selectMethod を設定する

selectMethod はカスタムプロパティに指定してください。
利用するドライバクラスによって指定するキーが異なります。

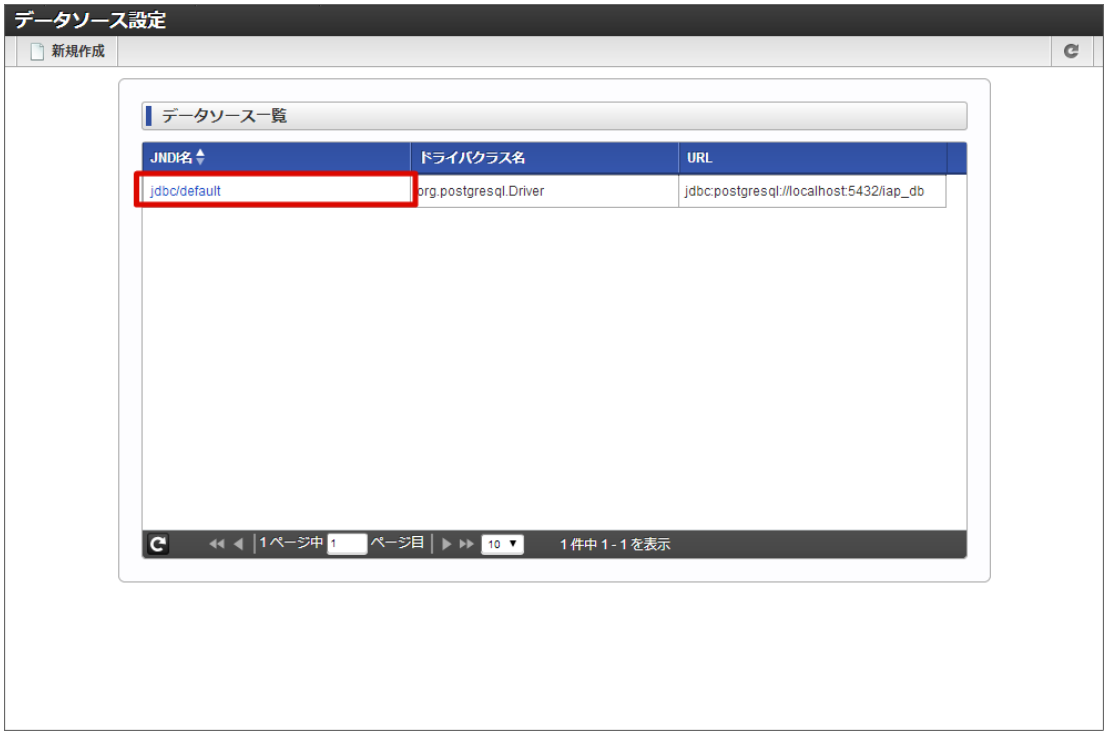
- com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource を利用する場合はキーに「selectMethod」を指定してください。
- com.microsoft.sqlserver.jdbc.SQLServerDriver を利用する場合はキーに「SelectMethod」を指定してください。

以下は com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource を利用する場合の設定例です。

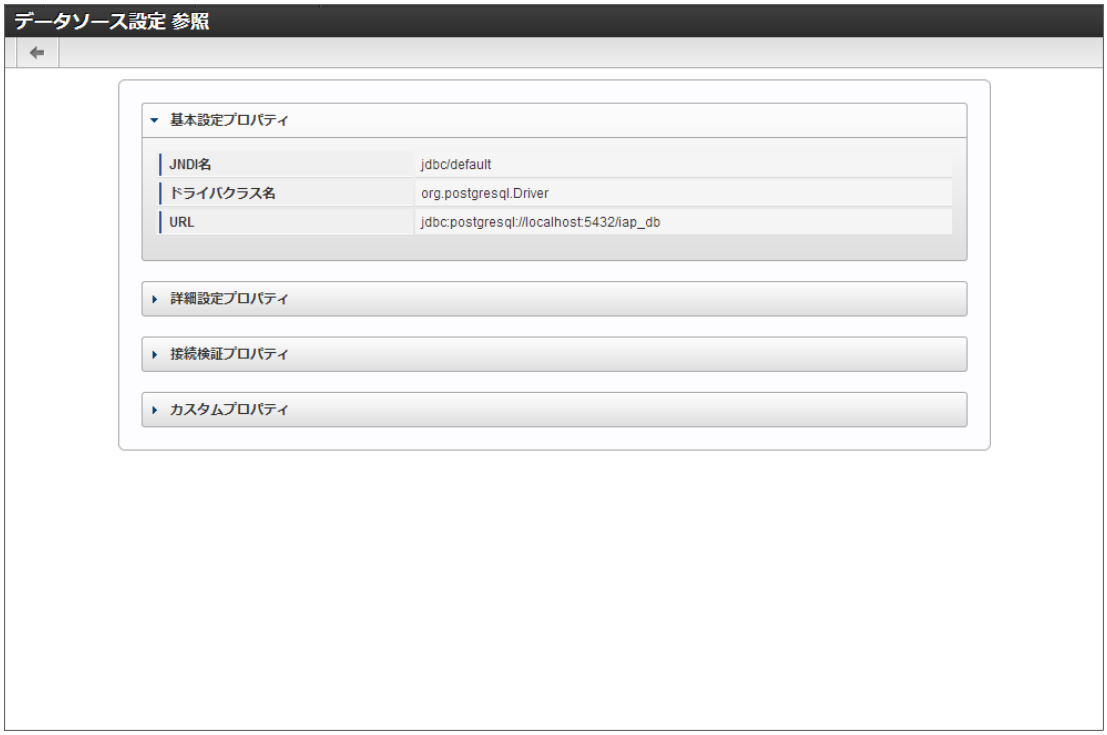


データソースを参照する

1. 「 システム環境構築 」→「データソース設定」をクリックします。
2. 参照したいデータソースのJNDI名をクリックします。



3. データソースの詳細が表示されます。



テナント管理

ここではテナント管理の操作の説明を行います。

テナント管理

システム管理者はテナント管理画面から intra-mart Accel Platform の作成済みのテナント情報の更新やテナントの削除を行うことができます。

目次

- テナント情報を更新する
- テナントを削除する

テナント情報を更新する

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 操作中のテナントの情報が表示されます。

各ウィザードの詳細については下記を参照してください。

テナント情報

1. **テナントの基本的な情報** を設定します。

項目	必須/任意	説明
テナントID	変更不可	テナントのIDが表示されます。
デフォルトロケール	変更不可	テナントのデフォルトロケールが表示されます。

項目	必須/任意	説明
タイムゾーン	必須	テナントのタイムゾーンを選択します。
デフォルトテナント	任意	デフォルトテナントかどうかを選択します。既にデフォルトテナントの場合は変更できません。
アカウントライセンス数	必須	テナントのアカウントライセンス数を入力します。 **テナント管理者を登録するため「1」以上を入力してください。**

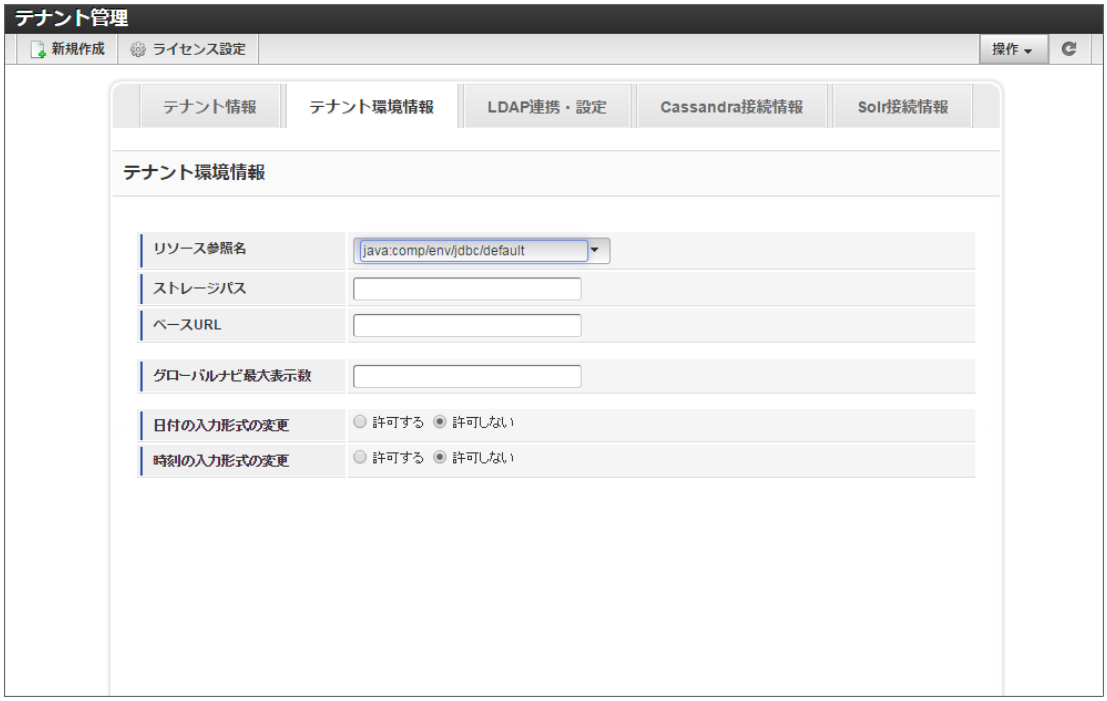
注意

TRY版利用などにおいてサンプルデータセットアップを行う場合は、「アカウントライセンス数」は **無制限** を選択する事を推奨します。

テナント環境情報

注意

「Resinデータソース設定」モジュールまたは「Payaraデータソース設定」モジュールを適用している場合、リソース参照名にセレクトボックスが表示されます。
モジュールが適用されていない場合はリソース参照名は表示されません。



項目	必須/任意	説明
リソース参照名	任意	リソース参照名を選択します。
ストレージパス	任意	ストレージパスを入力します。
ベースURL	任意	ベースURLを入力します。
グローバルナビ最大表示数	任意	グローバルナビの最大表示件数を入力します。
日付の入力形式の変更	必須	「許可する」を選択した場合、「日付と時刻の形式」にて日付の入力形式の変更が可能です。 未指定の場合の初期値は「許可しない」です。

項目	必須/任意	説明
時刻の入力形式の変更	必須	「許可する」を選択した場合、「日付と時刻の形式」にて時刻の入力形式の変更が可能です。 未指定の場合の初期値は「許可しない」です。

コラム

ストレージパスに storage-config.xml の <storage-directory-name>を付加したパスが
パブリックストレージパス %PUBLIC_STORAGE_PATH% に設定されます。
（例）
ストレージパスに /var/imart と入力し
設定ファイル storage-config.xml の <storage-directory-name> に storage と設定した場合、
%PUBLIC_STORAGE_PATH% は /var/imart/storage に設定されます。

コラム

未指定の場合は、それぞれの設定ファイルの内容が有効です。

パスワード保存方式設定

アカウントパスワードの保存方式 を設定します。

コラム

パスワード保存方式設定は 2016 Spring(Maxima) から利用可能です。
2016 Spring(Maxima) より前のバージョンでの保存方式は「暗号化」です。

設定画面

項目	必須/任意	説明

項目	必須/任意	説明
パスワード保存方式	必須 / 変更不可	データベース内で保持するアカウントパスワードの保存方式です。 以下の２つの方式を選択可能です。 ■ 暗号化：アカウントパスワードを暗号化して保存します。キーを用いる事でパスワードの復号化（平文パスワードの取得）が可能です。 ■ ハッシュ化：アカウントパスワードのハッシュ値を保存します。復号化（平文パスワードの取得）はできません。

注意

「ハッシュ化」を選択し更新した場合、以下の制限があります。

- 設定値を基にアカウントパスワードのハッシュ化を行うため一度設定した「ハッシュ化」の設定値を変更することはできません
- 平文パスワードを復元する方法が失われるため「暗号化」に戻すことはできません
- 平文パスワードを復元する方法が失われるため一部の機能がご利用いただけません
  - 詳細は 要件情報公開サイトを参照してください
- 既存のアカウントパスワードを変換するために「アカウントパスワードハッシュ化移行処理」ジョブを実行する必要があります。
  - 詳細は 「*アカウントパスワードハッシュ化移行処理*」 を参照してください。

以下の項目はパスワード保存方式で「ハッシュ化」を選択した場合のみ入力必須です。
パスワード保存方式が「ハッシュ化」で登録済みの場合は変更不可です。

項目	必須/任意	説明
ハッシュアルゴリズム	必須 / 変更不可	ハッシュ文字列を生成する計算式（関数）です。 intra-mart Accel Platform では以下の値が利用可能です。 ■ SHA-256 ■ SHA-384 ■ SHA-512
ソルト値	必須 / 変更不可	ハッシュ文字列を生成するためのパラメータの1つです。 パスワードのハッシュ化において、パスワード値にソルト値を付与した値に対してハッシュアルゴリズムによる計算を行った値がハッシュ文字列（パスワードとして保存される値）です。 ソルト値はユーザ毎に異なる値を利用するため、異なるユーザが同じパスワードを利用していた場合も保存されている値は異なります。 ソルト値の生成式は以下の通りです。 対象ユーザのユーザコード + "|" + テナントID + "|" + テナント属性で永続化されているソルトサフィックス
ストレッチング回数	必須 / 変更不可	ハッシュ文字列を生成するためのパラメータの1つです。 パスワードのハッシュ化において、ハッシュアルゴリズムによる計算をストレッチング数の回数繰り返して生成された値がハッシュ文字列（パスワードとして保存される値）です。 ストレッチング回数が多いほどパスワードの特定が難しくなりますが、ハッシュ化するための負荷が高くなります。

アカウントパスワードハッシュ化移行処理

アカウントパスワード、および、パスワード履歴管理で保存しているパスワード履歴の値を暗号化された値からハッシュ化された値に変更するためのジョブです。
パスワード保存方式を「暗号化」にて構築済みのテナントに対して「ハッシュ化」に変更した場合、一般ユーザによるログイン時にパスワードの照合に失敗してしまいます。
そのため、上述の環境においては「アカウントパスワードハッシュ化移行処理」ジョブを実行する必要があります。

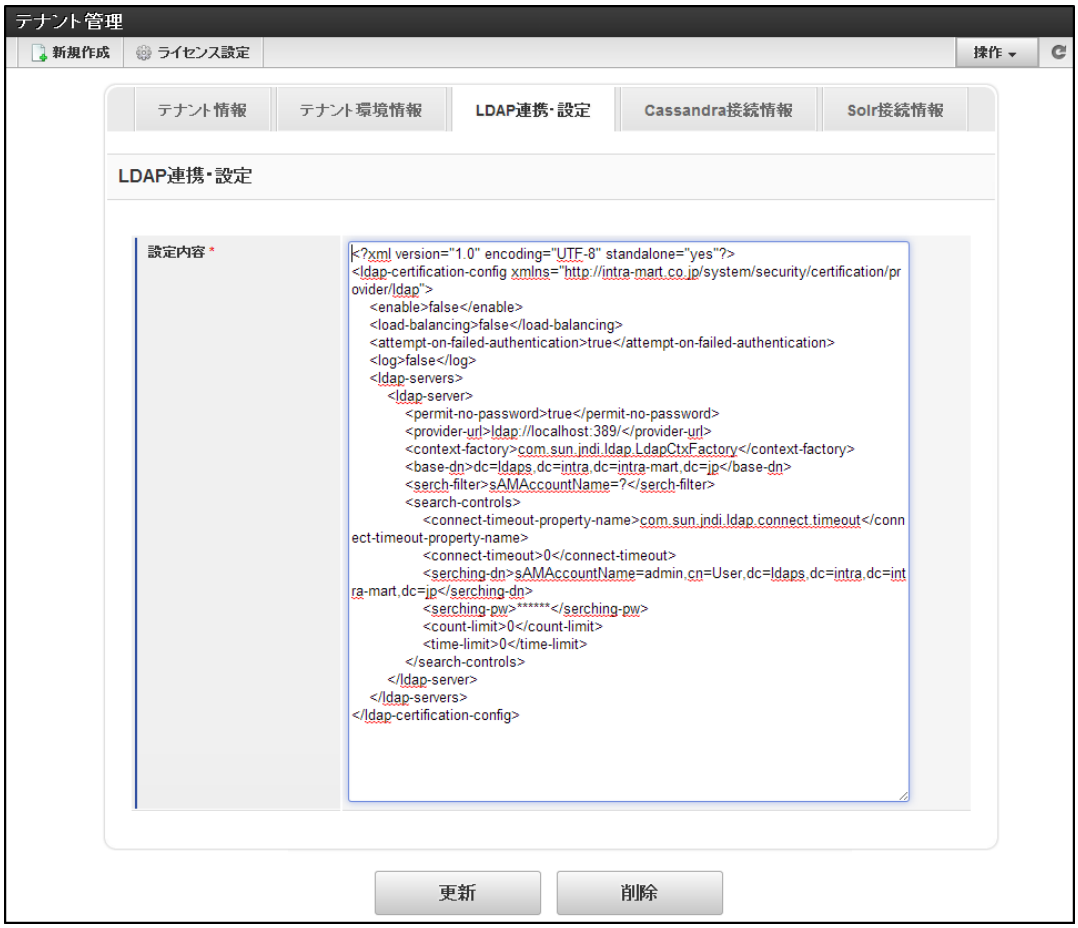
システム管理画面にログインした状態でジョブネット管理画面を開き「アカウントパスワードハッシュ化移行処理」ジョブを実行してください。
なお、ジョブネット管理画面はシステム管理画面のメニューには表示されません。
以下に示すURLをWebブラウザに直接入力してジョブネット管理画面を開いてください。
http://<HOST>:<PORT>/<CONTEXT_PATH>/tenant/job_scheduler/jobnet_maintenance

「アカウントパスワードハッシュ化移行処理」ジョブに関する詳細は 「 ジョブ・ジョブネットリファレンス 」の「 アカウントパスワードハッシュ化移行処理 」 を参照してください。

> **注意**
>
> ジョブを実行する前に 「 intra-mart Accel Platform セットアップガイド 」の「 バックアップ・リストア（復元） 」を参考にバックアップを行ってください。

LDAP連携・設定

1. **LDAP連携・設定** 情報を設定します。



> **注意**
>
> - <enable>タグの内容がtrueである場合のみLDAP認証が有効です。
> LDAP認証を有効とする場合、認証先であるLDAPの設定を正しく行ってください。
> - 2014 Spring(Granada) 以降のバージョンでLDAP認証モジュールを**追加**する場合は、テナント環境セットアップを実行する前にLDAP連携・設定情報を更新する必要があります。

項目	必須/任意	説明
設定内容	必須	LDAP認証の有効/無効、および、認証先であるLDAPの情報を入力します。 入力内容については「intra-mart Accel Platform セットアップガイド」-「LDAP認証設定ファイル」の説明を参照してください。

ログインセッション管理

> **注意**
>
> IM-Jugglingにおいて、 **ログインセッション管理モジュール** を選択した場合のみ、この画面が表示されます。

1. 一般ユーザのログイン時に二重ログインを検出した場合の動作を設定します。

ログインセッション管理の設定内容は以下のとおりです。

- 標準の認証エラーページを表示する

  標準の認証エラーページを表示します。

- 二重ログインの検出を表示する

  二重ログインを検出したことを一般ユーザに通知します。
  一般ユーザは通知された画面からログインを再試行することができます。

- ログインユーザによるセッションの無効化を許可する

  二重ログインを検出したことを一般ユーザに通知します。
  一般ユーザは通知された画面からログイン中のセッションを強制的に無効化しログインをすることができます。

Apache Cassandra接続情報

1. Apache Cassandra接続情報を更新します。

注意

- Apache Cassandra接続情報はIMBox利用時のみ表示されます。
- Apache Cassandra接続情報の更新時には、IMテナント拡張テーブル（im_tenant_attr）のみ更新が行われ、キースペースの作成などのApache Cassandraへの処理は行われません。
- Apache Cassandra接続情報の削除時には、IMテナント拡張テーブル（im_tenant_attr）のみ削除が行われ、キースペースの削除などのApache Cassandraへの処理は行われません。
- **接続先** に指定するすべてのCassandraサーバは、同一クラスタとして構築されている必要があります。
- テナント情報の更新時には、接続できないCassandra接続情報への更新が可能となるため設定内容の変更には注意してください。
- 2014 Spring(Granada) 以降のバージョンでIMBoxモジュールを**追加**する場合は、テナント環境セットアップを実行する前にCassandra接続情報を更新する必要があります。

項目	必須/任意	説明
クラスタ名	必須	Cassandraサーバのクラスタ名を入力します。
キースペース	必須	Cassandraサーバのキースペースを入力します。
接続先	必須	Cassandraが稼働しているサーバのIPアドレスとポート番号を入力します。 接続先は「IPアドレス」または、「IPアドレス:ポート番号」の形式で入力します。（ポート番号を省略した場合、9160を利用します。） 9160以外のポート番号を指定した場合、新規ノードの検出機能にてエラーが発生します。 分散構成で複数のCassandraが稼働している場合、すべての接続先を1行ずつ入力してください。
レプリケーションファクタ	必須	クラスタ内部のデータのレプリカ数を入力します。 レプリケーションファクタは、キースペース作成時のみ使用されます。 レプリケーションファクタの値を変更する場合は、Cassandra自体に変更を行う必要があります。 レプリケーションファクタ数の設定は、「Cassandra管理者ガイド」の「Cassandraのクラスタ構築」を参照してください。
認証情報設定	任意	Cassandraへの接続における認証の利用を選択します。

項目	必須/任意	説明
認証ユーザ名	認証設定利用時のみ必須	Cassandraへの認証接続における接続ユーザ名を入力します。 認証設定利用時のみ表示されます。
認証パスワード	認証設定利用時のみ必須	Cassandraへの認証接続におけるパスワードを入力します。 認証設定利用時のみ表示されます。
テスト接続		入力した内容でCassandraが接続可能であるかのテストが行えます。 テナント作成時には、必ず行うことを推奨します。

Apache Solr接続情報

1. Apache Solr接続情報を入力します。

> **注意**
>
> Apache Solr接続情報は、IM-ContentsSearch for Accel Platform利用時のみ表示されます。
> IM-ContentsSearch for Accel Platformを利用する場合は、Apache Solrのセットアップが必要です。
> Apache Solrのセットアップに関しての詳細は「Apache Solr」を参照してください。

標準接続先 入力項目

項目	必須/任意	説明
グループID（標準接続先）	固定（”default”）	標準接続先のグループIDは”default”から変更することはできません。
標準接続先	必須（「Solr接続情報」ボタンが有効になっている場合のみ）	接続先を選択します。Solr接続設定に登録されている接続先がセレクトボックスに表示されます。 他のテナントの標準接続先に設定されている接続先は表示されません。 Solr接続設定が1件も登録されていない場合、Solrサーバ接続設定ファイル（solr-config.xml）に定義されているSolr接続設定（”default”）が選択項目に表示されます。

追加接続先 入力項目

項目	必須/任意	説明
接続先を追加する		追加接続先の入力項目を追加します。 追加接続先は２０個まで追加可能です。

項目	必須/任意	説明
削除	任意	選択した行の追加接続先を更新時に削除します。
グループID（追加接続先）	任意	追加接続先のグループIDを入力します。 テキストボックスが空の場合は、右の接続先を選択していても更新されません。
追加接続先	任意	追加接続先を選択します。Solr接続設定に登録されている接続先がセレクトボックスに表示されます。 Solr接続設定に登録されているすべての接続先がセレクトボックスに表示されます。

コラム

追加接続先について

追加接続先はテナント管理画面で設定可能な項目です。
IM-ContentsSearch の全文検索機能では標準接続先のSolr接続先を利用します。
intra-mart Accel Platform 上の別のアプリケーションで、標準接続先とは別のSolr接続先を利用する場合に設定することを想定しています。

コラム

登録可能なSolr接続設定が存在しない場合、標準接続先・追加接続先の入力項目が表示されません。
Solr接続設定画面でSolr接続設定を登録してからSolr接続情報を編集してください。
Solr接続設定については *Solr接続設定* を参照してください。

多要素認証

注意

IM-Juggling において、**多要素認証機能モジュール**を選択した場合のみ、この画面が表示されます。

1. **多要素認証設定**情報を設定します。

項目	必須/任意	説明
多要素認証適用ポリシー	必須	多要素認証機能の運用に関するポリシーを以下から選択できます。 適用しない　多要素による認証を行いません。 ユーザが任意で適用　ユーザが個人設定の多要素認証設定を行うことにより、ログイン時にユーザコード・パスワードと多要素による認証が行われます。 強制的に適用　多要素による認証を行うことをユーザに強制します。 多要素認証の設定が行われていないユーザに対して、ログイン時に設定を要求します。
バックアップコードの生成数	必須	バックアップコードを生成する数を設定できます。
ブラウザ情報管理機能	必須	ブラウザ情報管理を有効にすることで、ユーザが多要素による認証時に認証を行うブラウザ情報を信頼済みのブラウザとして記憶できます。 信頼済みのブラウザからログインを行う場合、次回のログインから多要素による認証を省略できます。
ブラウザ情報の信頼期間(日)	必須	ブラウザ情報管理機能を有効にした場合にブラウザ情報を信頼する期間を日数で設定します。 設定されている日数を過ぎたブラウザでは、再び多要素による認証を要求します。
認証アプリ発行者情報	必須	認証アプリにアカウントを登録する際に付与する発行者情報を設定します。

3. 各ウィザードの詳細を参考に変更内容を入力し、「更新」をクリックします。

4. 「決定」をクリックします。

5. テナント情報が更新されました。

注意

テナント情報の更新では、テナントに紐づく情報が更新されます。
テナント環境セットアップが行われるわけではありません。

テナントを削除する

注意

テナントの削除をする前には、必ず事前に必要なバックアップを行ってください。

対象のテナントが動作していない時に削除を行ってください。
例えば以下の様な処理が行われていないように注意してください。

- ジョブが実行中
- 非同期のキューがある状態
- アプリケーションロックのかかる処理が実行中
- ユーザがログイン中

テナント削除では以下の内容は削除されません。

- テナントデータベース
- 削除するテナントのパブリックストレージ
- Apache Cassandra の削除するテナントのキースペース
- Apache Solr に保存されているデータ

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 操作中のテナントの情報が表示されます。

3. 「削除」をクリックします。

4. 「決定」をクリックします。

5. テナントが削除されました。

テナントの新規作成

システム管理者はテナント管理画面から intra-mart Accel Platform のテナントを新たに作成することができます。

テナントを新規作成する

テナント管理からテナントの新規作成を行うことができます。

> **注意**
>
> テナントの新規作成は Web Application Server が Resin の場合を対象としています。
> Resin 以外の Web Application Server は、動作保証対象外です。

> **注意**
>
> テナントの新規作成の際は、あらかじめ新しいデータソース設定の登録が必要です。
>
> 詳しくは、「*データソース設定*」を参照してください。

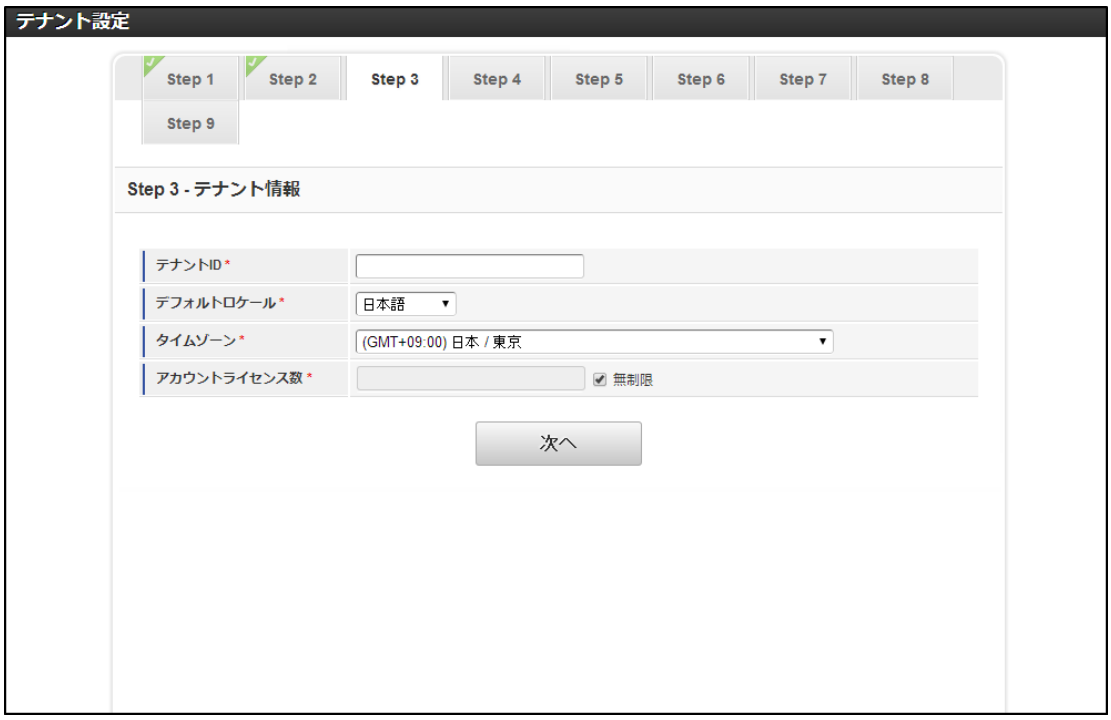
1. 「システム環境構築」→「テナント管理」をクリックします。
2. 「新規作成」をクリックします。

3. テナントの新規作成に必要なステップが表示されます。

各ウィザードの詳細については下記を参照してください。

テナント情報

1. **テナントの基本的な情報** を設定します。



項目	必須/任意	説明
テナントID	必須	テナントのIDを入力します。 「DataSourceマッピングの設定 」の <tenant-id> で設定した値を入力します。 DataSourceマッピングの設定を行っていない場合は、「 **default** 」を入力します。
デフォルトロケール	必須	テナントのデフォルトロケールを選択します。 初期表示されているロケールは、アクセスしているブラウザのロケール設定です。 **このロケールは運用中に変更することは推奨していません。** **運用に応じたロケールを設定してください。**
タイムゾーン	必須	テナントのタイムゾーンを選択します。
アカウントライセンス数	必須	テナントのアカウントライセンス数を入力します。 **テナント管理者を登録するため「1」以上を入力してください。**

注意

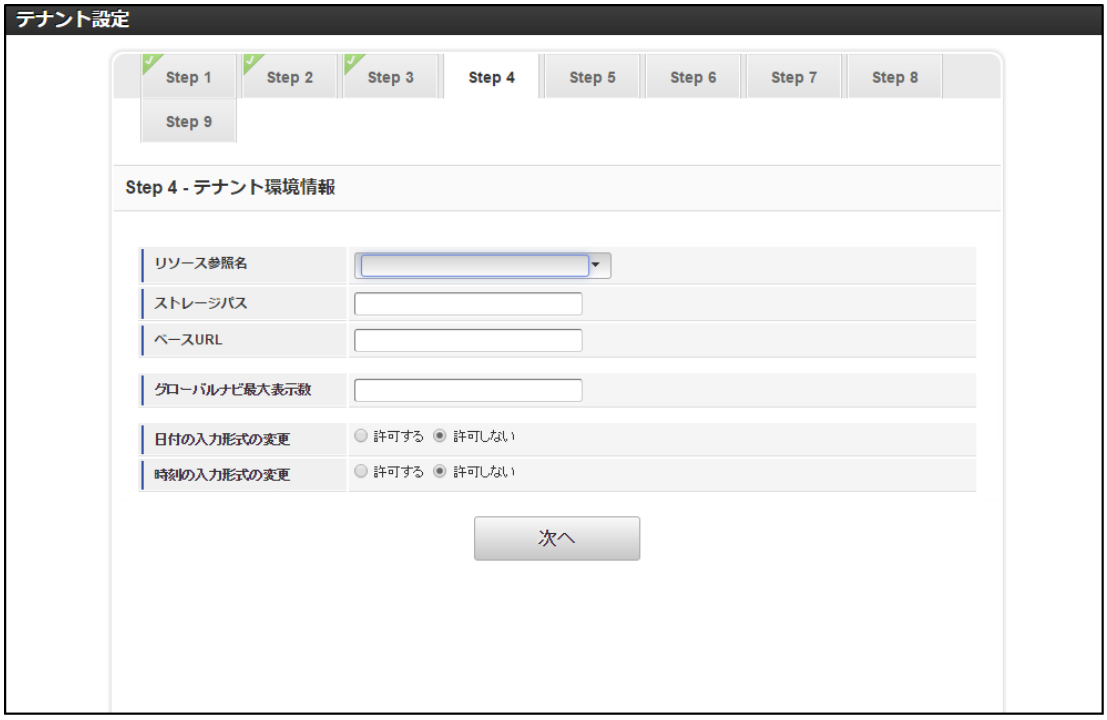
試用版利用などにおいてサンプルデータセットアップを行う場合は、「アカウントライセンス数」は **無制限** を選択する事を推奨します。

テナント環境情報

1. **テナントの環境情報** を設定します。

コラム

「Resinデータソース設定」モジュールまたは「Payaraデータソース設定」モジュールを適用している場合、リソース参照名にセレクトボックスが表示されます。
モジュールが適用されていない場合はリソース参照名は表示されません。



項目	必須/任意	説明
リソース参照名	任意	リソース参照名を選択します。
ストレージパス	任意	ストレージパスを入力します。
ベースURL	任意	ベースURLを入力します。
グローバルナビ最大表示数	任意	グローバルナビの最大表示件数を入力します。
日付の入力形式の変更	必須	「許可する」を選択した場合、「日付と時刻の形式」にて日付の入力形式の変更が可能です。 初期値は「許可しない」です。
時刻の入力形式の変更	必須	「許可する」を選択した場合、「日付と時刻の形式」にて時刻の入力形式の変更が可能です。 初期値は「許可しない」です。

コラム

ストレージパスに storage-config.xml の <public-directory-name> と <storage-directory-name> を付加したパスが、パブリックストレージパス %PUBLIC_STORAGE_PATH% です。
（例）
ストレージパスに /var/imart と入力し、設定ファイル storage-config.xml の <public-directory-name> に public、<storage-directory-name> に storage と設定した場合、%PUBLIC_STORAGE_PATH% は /var/imart/public/storage です。

コラム

未指定の場合は、それぞれの設定ファイルの内容が有効です。

テナント管理者情報

1. **テナントの管理者** を設定します。

項目	必須/任意	説明
ユーザコード	必須	テナント管理者のユーザコードを入力します。 （例：tenant）
パスワード	任意	テナント管理者のパスワードを入力します。
パスワード(確認)	任意	テナント管理者のパスワードを再入力します。

> **コラム**
>
> “任意”項目は、必要に応じて入力してください。必要がなければ入力の必要はありません。

> **コラム**
>
> テナント環境セットアップ中にエラーが発生してセットアップが中断してしまった場合、 再度セットアップを実施してもテナント管理者は登録されません。
> このように正常にテナント管理者を登録できなかった場合、テナント管理画面から改めてテナント管理者を登録することができます。
> 詳しくは「システム管理者操作ガイド」-「テナント管理」の「テナント管理者を新規に作成する」の項を参照してください。

パスワード保存方式設定

1. **アカウントパスワードの保存方式** を設定します。

> **コラム**
>
> パスワード保存方式設定は 2016 Spring(Maxima) から利用可能です。
> 2016 Spring(Maxima) より前のバージョンでの保存方式は「暗号化」です。

項目	必須/任意	説明
パスワード保存方式	必須	データベース内で保持するアカウントパスワードの保存方式です。 以下の２つの方式を選択可能です。 ▪ 暗号化：アカウントパスワードを暗号化して保存します。キーを用いる事でパスワードの復号化(平文パスワードの取得)が可能です。 ▪ ハッシュ化：アカウントパスワードのハッシュ値を保存します。復号化(平文パスワードの取得)はできません。

注意

「ハッシュ化」を選択し登録した場合、以下の制限があります。

- 設定値を基にアカウントパスワードのハッシュ化を行うため一度設定した「ハッシュ化」の設定値を変更することはできません
- 平文パスワードを復元する方法が失われるため「暗号化」に戻すことは出来ません
- **平文パスワードを復元する方法が失われるため一部の機能がご利用いただけなくなります**
  - 詳細は 要件情報公開サイト を参照してください

以下の項目はパスワード保存方式で「ハッシュ化」を選択した場合のみ入力必須です。

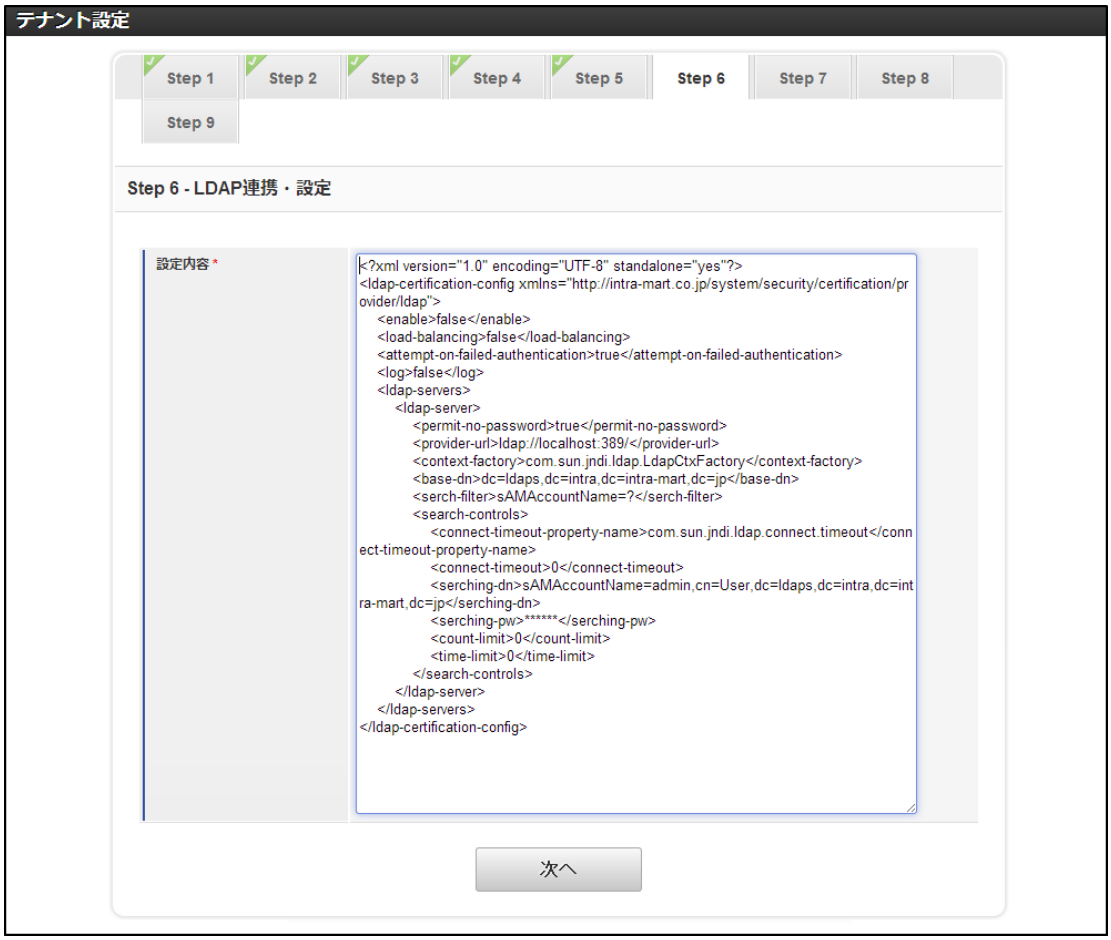
項目	必須/任意	説明
ハッシュアルゴリズム	必須	ハッシュ文字列を生成する計算式（関数）です。 intra-mart Accel Platform では以下の値が利用可能です。 ▪ SHA-256 ▪ SHA-384 ▪ SHA-512

項目	必須/任意	説明
ソルト値	必須	ハッシュ文字列を生成するためのパラメータの1つです。 パスワードのハッシュ化において、パスワード値にソルト値を付与した値に対してハッシュアルゴリズムによる計算を行った値がハッシュ文字列（パスワードとして保存される値）となります。 ソルト値はユーザ毎に異なる値を利用するため、異なるユーザが同じパスワードを利用していた場合も保存されている値は異なる値となります。 ソルト値の生成式は以下の通りです。 対象ユーザのユーザコード + "|" + テナントID + "|" + テナント属性で永続化されているソルトサフィックス
ストレッチング回数	必須	ハッシュ文字列を生成するためのパラメータの1つです。 パスワードのハッシュ化において、ハッシュアルゴリズムによる計算をストレッチング数の回数繰り返して生成された値がハッシュ文字列（パスワードとして保存される値）となります。 ストレッチング回数が多いほどパスワードの特定が難しくなりますが、ハッシュ化するための負荷が高くなります。

LDAP連携・設定

> **注意**
>
> IM-Juggling において、 **LDAP認証モジュール** を選択した場合のみ、この画面が表示されます。

1. **LDAP連携・設定** 情報を設定します。



> **コラム**
>
> 初期表示は IM-Juggling のプロジェクト/conf/ldap-certification-config.xmlの内容が表示されます。
> ただし、<enable>タグの値はfalseとなっています。

> **注意**
>
> <enable>タグの内容がtrueである場合のみLDAP認証が有効となります。
> LDAP認証を有効とする場合、認証先であるLDAPの設定を正しく行ってください。

項目	必須/任意	説明
設定内容	必須	LDAP認証の有効/無効、および、認証先であるLDAPの情報を入力します。 入力内容については「intra-mart Accel Platform セットアップガイド」-「LDAP認証設定ファイル」の説明を参照してください。

ログインセッション管理

> **注意**
>
> IM-Jugglingにおいて、 **ログインセッション管理モジュール** を選択した場合のみ、この画面が表示されます。

1. 一般ユーザのログイン時に二重ログインを検出した場合の動作を設定します。

ログインセッション管理の設定内容は以下のとおりです。

- 標準の認証エラーページを表示する

  標準の認証エラーページを表示します。

- 二重ログインの検出を表示する

  二重ログインを検出したことを一般ユーザに通知します。
  一般ユーザは通知された画面からログインを再試行することができます。

- ログインユーザによるセッションの無効化を許可する

  二重ログインを検出したことを一般ユーザに通知します。
  一般ユーザは通知された画面からログイン中のセッションを強制的に無効化しログインをすることができます。

Apache Cassandra接続情報

> **注意**
>
> IM-Jugglingにおいて、 **IMBoxモジュール** を選択した場合のみ、この画面が表示されます。

1. Apache Cassandra接続情報を入力します。

> **注意**
>
> Apache Cassandra接続情報はIMBox利用時のみ表示されます。
> テナント環境セットアップを実行する前にApache Cassandraの設定、起動が行われている必要があります。
> Apache Cassandraの設定に関しての詳細は「 IMBox Cassandra管理者ガイド 」を参照してください。

項目	必須/任意	説明
クラスタ名	必須	Cassandraサーバのクラスタ名を入力します。 （例：IMBox Cluster）
キースペース	必須	Cassandraサーバのキースペースを入力します。 （例：default）
接続先	必須	Cassandraが稼働しているサーバのIPアドレスとポート番号を入力します。 接続先は「IPアドレス」または、「IPアドレス:ポート番号」の形式で入力します。（ポート番号を省略した場合、9160を利用します。） 9160以外のポート番号を指定した場合、新規ノードの検出機能にてエラーが発生します。 分散構成で複数のCassandraが稼働している場合、すべての接続先を1行ずつ入力してください。 （例：127.0.0.1:9160）
レプリケーションファクタ	必須	クラスタ内部のデータのレプリカ数を入力します。 レプリケーションファクタは、キースペース作成時のみ使用されます。 （例：1）
認証情報設定	任意	Cassandraへの接続における認証の利用を選択します。 認証情報を設定する場合には書込み権限の確認を行うため、事前にキースペースを作成しておく必要があります。
認証ユーザ名	認証設定利用時のみ必須	Cassandraへの認証接続における接続ユーザ名を入力します。 認証設定利用時のみ表示されます。 （例：admin）

項目	必須/任意	説明
認証パスワード	認証設定利用時のみ必須	Cassandraへの認証接続におけるパスワードを入力します。 認証設定利用時のみ表示されます。 （例：admin）
テスト接続		入力した内容でCassandraが接続可能であるかのテストが行えます。 テナント作成時には、必ず行うことを推奨します。

コラム

“任意”項目は、必要に応じて入力してください。必要がなければ入力の必要はありません。

コラム

Cassandra接続情報の登録時の初期値は、Cassandraサーバ接続設定（cassandra-config.xml）の設定値となります。
cassandra-config.xmlに関する詳細は「intra-mart Accel Platform セットアップガイド」-「IMBox」を参照してください。

Apache Solr接続情報

注意

- IM-Jugglingにおいて、 **IM-ContentsSearchモジュール** を選択した場合のみ、この画面が表示されます。
- IM-ContentsSearch for Accel Platformを利用する場合は、Apache Solrのセットアップが必要となります。
  Apache Solrのセットアップに関しての詳細は「 Apache Solr 」の「セットアップ」を参照してください。

1. Apache Solr接続情報を入力します。

項目	必須/任意	説明
Solr接続情報を設定する	任意	テナント環境セットアップ時にApache Solr接続情報を設定するかどうかをこのボタンで切り替えることができます。 「Solr接続情報」ボタンを未選択状態にすることで、Apache Solr接続情報を設定せずにテナント環境セットアップを実行することができます。
グループID	固定(“default”)	標準接続先のグループIDは”default”から変更することはできません。

項目	必須/任意	説明
標準接続先	必須（「Solr接続情報」ボタンが有効になっている場合のみ）	接続先を選択します。 「Solr接続情報」ボタンが選択状態になっている場合のみ選択することができます。 他のテナントの標準接続先に設定されている接続先は表示されません。

Solr接続情報の設定方法

テナント環境セットアップ時に、システムデータベースへ登録するSolr接続情報を設定する方法は以下の通りです。

- **設定ファイルから変更する方法**

  初回のテナント環境セットアップ前にSolrサーバ接続設定ファイル（solr-config.xml）を設定しておくことで、solr-config.xmlの設定（<group name=”default”>）で定義されている設定値がSolr接続情報としてシステムデータベースへ登録されます。
  Solrサーバ接続設定ファイル（solr-config.xml）は初回のテナント環境セットアップ時、または、Solr接続設定が1件も登録されていない場合に標準接続先の項目として利用します。
  solr-config.xmlに関する詳細は「intra-mart Accel Platform セットアップガイド」-「IM-ContentsSearch」を参照してください。

- **画面から変更する方法**

  別のテナントを新規作成するときは「Solr接続設定」画面で登録したSolr接続情報が標準接続先の選択項目として表示されます。
  システム管理者メニューのテナント管理画面で、作成したテナントにApache Solr接続情報を設定することができます。
  「Solr接続設定」画面に関する詳細は「 システム管理者操作ガイド 」-「 Solr接続設定 」を参照してください。

多要素認証

> **注意**
> IM-Juggling において、**多要素認証機能モジュール**を選択した場合のみ、この画面が表示されます。

1. 多要素認証機能の動作を設定します。

項目	必須/任意	説明

項目	必須/任意	説明
多要素認証適用ポリシー	必須	多要素認証機能の運用に関するポリシーを以下から選択できます。 適用しない：多要素による認証を行いません。 ユーザが任意で適用：ユーザが個人設定の多要素認証設定を行うことにより、ログイン時にユーザコード・パスワードと多要素による認証が行われます。 強制的に適用：多要素による認証を行うことをユーザに強制します。 多要素認証の設定が行われていないユーザに対して、ログイン時に設定を要求します。
バックアップコードの生成数	必須	バックアップコードを生成する数を設定できます。
ブラウザ情報管理機能	必須	ブラウザ情報管理を有効にすることで、ユーザが多要素による認証時に認証を行うブラウザ情報を信頼済みのブラウザとして記憶できます。 信頼済みのブラウザからログインを行う場合、次回のログインから多要素による認証を省略できます。
ブラウザ情報の信頼期間(日)	必須	ブラウザ情報管理機能を有効にした場合にブラウザ情報を信頼する期間を日数で設定します。 設定されている日数を過ぎたブラウザでは、再び多要素による認証を要求します。
認証アプリ発行者情報	必須	認証アプリにアカウントを登録する際に付与する発行者情報を設定します。

登録

1. 各ステップの設定が完了したら、「登録」をクリックします。

> **注意**
> セットアップでエラーが発生した場合、「 セットアップで困ったら・・・ 」を参照してください。

セットアップが完了すると、下記の画面が表示されます。

処理結果	モジュールID	インポート種別	インポート対象名	エラーメッセージ
	im_javamail	EXTENSION	jp.co.intra_mart.system.mail.template.migration.MailTemplateMigrator	-
	im_tenant	DDL	products/import/basic/im_tenant/im_tenant_common/im_tenant_common-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_calendar/im_calendar-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_admin/im_admin-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_authz/im_authz-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_menu/im_menu-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_password_history/im_password_history-ddl.sql	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_en.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_ja.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_zh_CN.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_en.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_ja.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_zh_CN.xml	-

4. テナント作成に成功すると、操作中のテナントが切り替わります。

処理結果	モジュールID	インポート種別		エラーメッセージ
	im_javamail	EXTENSION	jp.co.intra_mart.system.mail.template.migration.MailTemplateMigrator	-
	im_tenant	DDL	products/import/basic/im_tenant/im_tenant_common/im_tenant_common-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_calendar/im_calendar-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_admin/im_admin-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_authz/im_authz-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_menu/im_menu-ddl.sql	-
	im_tenant	DDL	products/import/basic/im_tenant/im_password_history/im_password_history-ddl.sql	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_en.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_ja.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_calendar/im_calendar-role_zh_CN.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_en.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_ja.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_admin/im_admin-role_zh_CN.xml	-
	im_tenant	DML	products/import/basic/im_tenant/im_authz/im_authz-role.xml	-

ライセンス設定

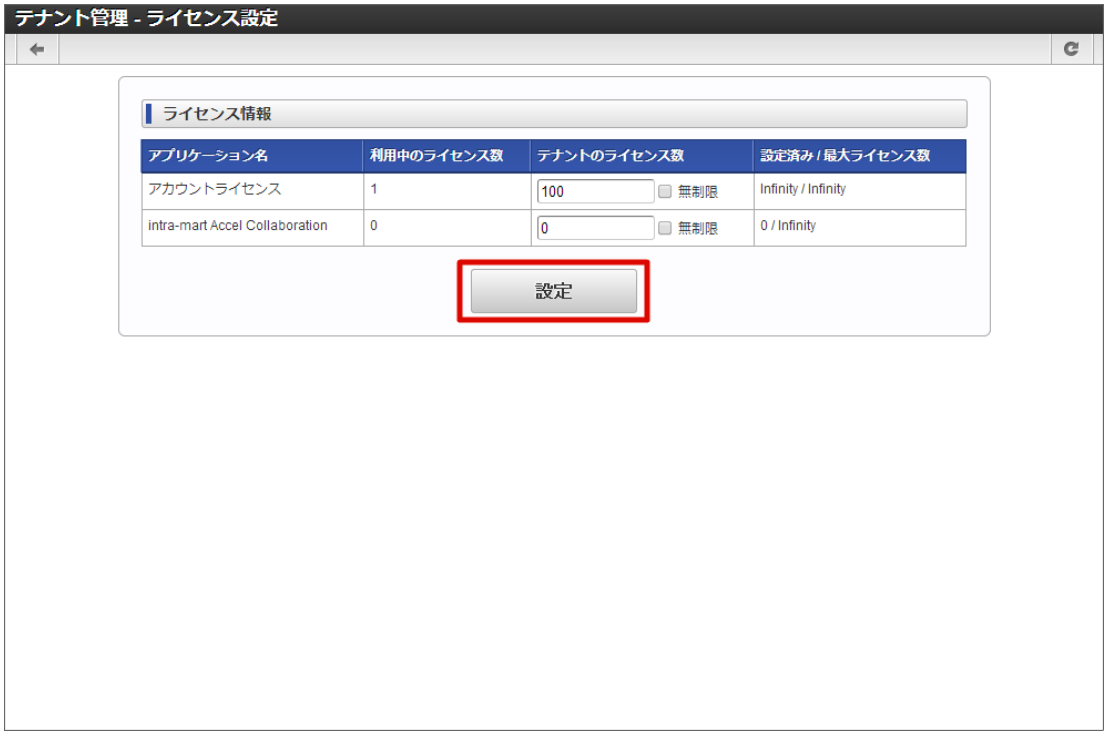
操作中のテナントに対してライセンスの管理を行うことができます。
利用中のライセンス数の確認とテナントに付与するライセンス数を設定をすることができます。
バーチャルテナントによる複数テナントが存在する場合には、システム管理者がそれぞれのテナントに対して、ライセンス数を割り当てる必要があります。

アカウントライセンスを除いた各アプリケーションのテナントに付与されるライセンスの初期値は0です。
そのためライセンスの付与数を設定しない場合はアプリケーションを利用できません。

テナントのライセンス数を設定する

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 「ライセンス設定」をクリックします。

3. テナントのライセンス数を入力し、「設定」クリックします。



4. 「決定」をクリックします。

5. テナントのライセンス数を設定することができました。

注意

最大ライセンス数は、バーチャルテナントによる複数テナントが存在する場合に、全てのテナントに割り当てることができる合計のライセンス数です。
存在するテナントのライセンス数の合計値が最大ライセンス数を超えることはできません。
すでにアカウントにライセンスが割り当てられている場合は、その割り当てられている数より小さい値に変更することはできません。

コラム

テナントに付与したライセンスはテナントの管理画面でユーザに付与することができます。
詳細は以下のドキュメントを参照してください。

- 「テナント管理者操作ガイド」
  - 「アカウントライセンス一覧を使用する」
  - 「アプリケーションライセンス一覧を使用する」

または、IM-共通マスタのユーザ管理画面で設定することもできます。
詳細は「 IM-共通マスタ 管理者操作ガイド」-「ユーザ」の「アカウント」タブ、「ロール」タブについてを参照してください。

テナントの操作を行う

テナントに対して行うことができる操作は、以下の通りです。

- *テナント管理者を新規に作成する*

  テナントに対して新しいテナント管理者権限を持つユーザを登録します。

  システム管理者がテナントのユーザとして一時的にログインする場合や、テナント環境セットアップでテナント管理者が作成されなかった場合に実行します。

- *管理者用認可リソースを復旧する*

  認可設定を行うための最低限の認可リソースを復旧します。

  認可設定に関する認可リソースが誤って削除されてしまい、認可設定が画面上から行えなくなってしまった場合に実行します。

- *特定のユーザに認可設定権限を付与する*

  テナントに登録されているユーザに対して認可設定権限を与えます。
  また、ユーザの有効期限設定、ロック状態を初期化し、アカウントライセンスが付与されていない場合は付与してログイン可能な状態にします。

  既存のテナント管理者が何らかの理由でログインできなくなった場合や、認可設定が可能なユーザが不在となった場合に実行します。

テナント管理者を新規に作成する

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 「操作」→「テナント管理者の作成」をクリックします。

3. 「ユーザコード」にテナント管理権限を与えるユーザコードを入力します。
   パスワードを設定する場合は、「パスワード」「パスワード（確認用）」を入力します。

4. 「実行」をクリックします。

5. テナント管理者を作成することができました。

コラム

作成するユーザのロール

この操作で作成するユーザには自動的に「テナント管理者」ロールが付与されます。
「テナント管理者」ロールが存在しない場合、ロールは付与されませんがユーザは作成されます。

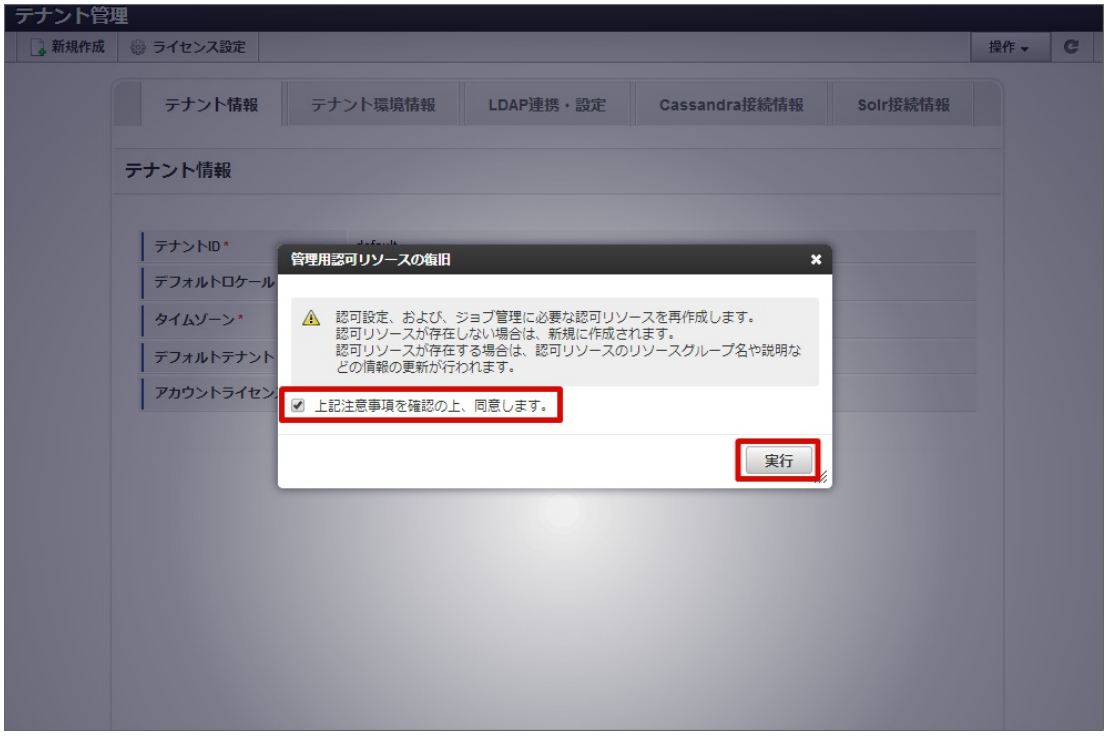
対象のユーザにアカウントライセンスを付与できない場合

この操作で作成するユーザには自動的にアカウントライセンスが付与されます。
アカウントライセンスの上限に達したなどの理由でアカウントライセンスを付与できない場合、アカウントライセンスは付与されませんがユーザは作成されます。
アカウントライセンスが必要な場合は、テナント管理画面でアカウントライセンス数を増やした後、「認可設定権限の付与」からアカウントライセンスを付与してください。

管理者用認可リソースを復旧する

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 「操作」→「管理用認可リソースの復旧」をクリックします。

3. 表示されている注意事項を読み、「上記注意事項を確認の上、同意します。」のチェックボックスをオンにして、「実行」をクリックします。



4. 管理者用認可リソースを復旧することができました。

コラム

復旧する認可リソース

復旧する認可リソースは、以下の通りです。

- 「画面・処理」→「認可」→「認可設定（Ajax）」
- 「画面・処理」→「認可」→「認可設定（基本画面）」
- 「画面・処理」→「認可」→「認可設定（ポップアップ）」
- 「画面・処理」→「ジョブ管理」→「ジョブ管理」
- 「画面・処理」→「ジョブ管理」→「ジョブネットモニター覧」

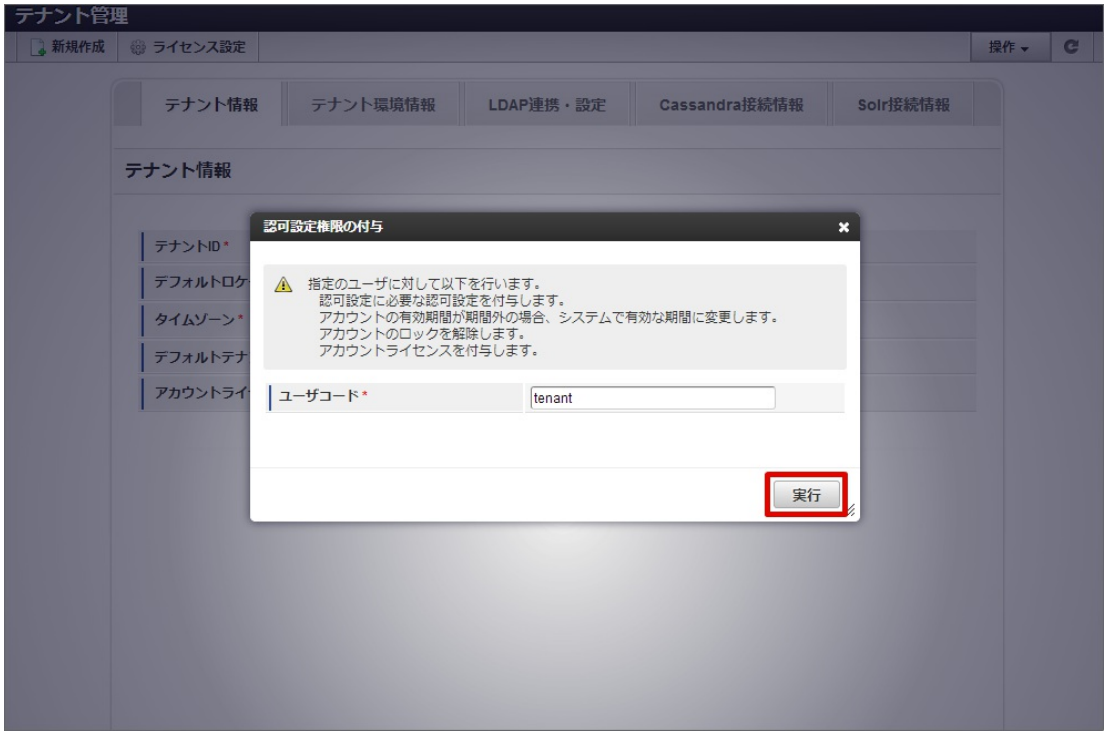
注意

- 復旧する認可リソースの一部がすでに登録済みの場合、対象の認可リソースの名称は初期値に戻ります。
- 権限設定（認可ポリシー）は設定されませんので、リソースを復旧後に認可設定画面を開くことができるユーザでログインし、認可設定画面から適宜権限を付与してください。

特定のユーザに認可設定権限を付与する

1. 「システム環境構築」→「テナント管理」をクリックします。
2. 「操作」→「認可設定権限の付与」をクリックします。

3. 付与対象のユーザの「ユーザコード」を入力し、「実行」をクリックします。



4. 認可設定権限を付与することができました。

コラム

設定する認可の権限設定（認可ポリシー）

権限設定を行う対象の認可リソースは、以下の通りです。

- 「画面・処理」→「認可」→「認可設定（Ajax）」
- 「画面・処理」→「認可」→「認可設定（基本画面）」

対象のユーザにアカウントライセンスを付与できない場合

この操作で権限を付与するユーザには自動的にアカウントライセンスが付与されます。
アカウントライセンスの上限に達したなどの理由でアカウントライセンスを付与できない場合、アカウントライセンスは付与されません。
アカウントライセンスが必要な場合は、以下のいずれかの操作を行ってください。

- テナント管理画面でアカウントライセンス数を増やした後、再実行してください。
- アカウントライセンスがすでに付与されているユーザに対して、再実行してください。

注意

- この操作では指定したユーザコードに対応する対象者条件（認可サブジェクトグループ）を作成します。
  テナントの状態を正常な状態に復旧した後は、認可設定画面から対象の対象者条件を削除してください。
  登録される対象者条件の名称は、以下の通りです。
  - 「テナント復旧用:＜ユーザコード＞」
- この操作では指定したユーザがログイン可能になるよう、有効期限、ロック状態、アカウントライセンスの付与状態を変更します。
  テナントの状態を正常な状態に復旧した後は、必要に応じてユーザの状態を再設定してください。

テナント環境セットアップ

モジュールやアプリケーションを新たに追加した場合、再度テナント環境セットアップをおこないます。
初期導入時のテナント環境セットアップ、サンプルデータセットアップは **「セットアップガイド」** を参照してください。

注意

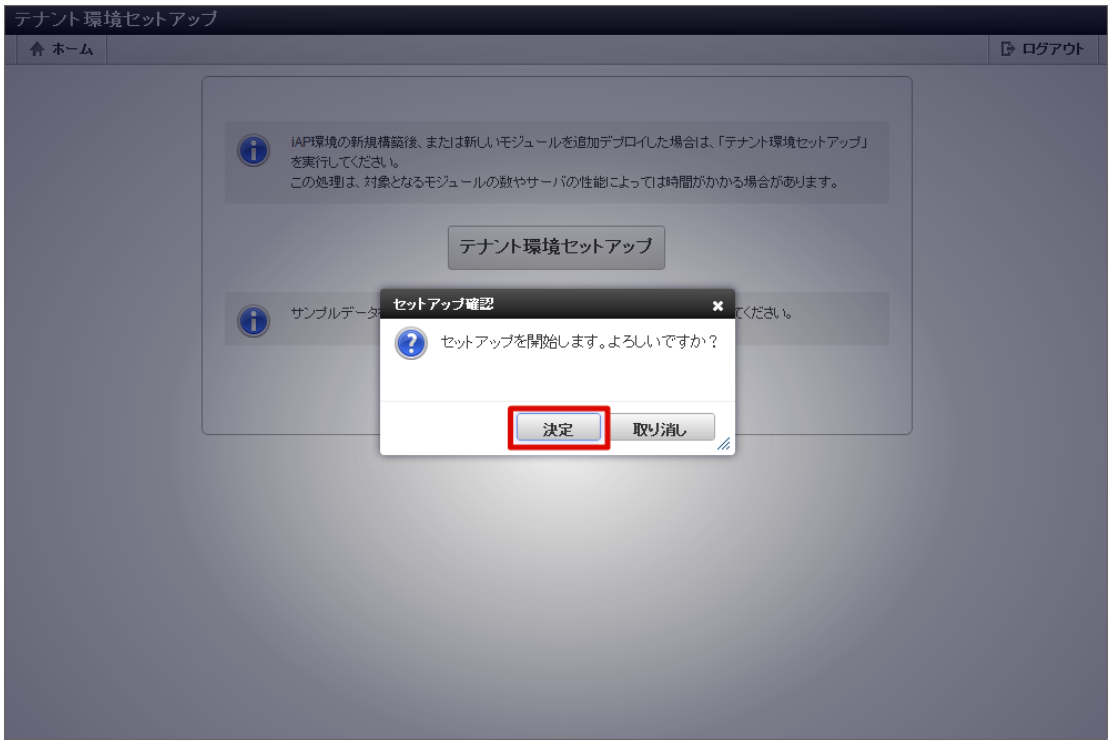
バーチャルテナントによる複数テナント が存在する場合には、すべてのテナントに対してテナント環境セットアップを行ってください。

> **注意**
>
> サンプルデータセットアップは更新情報を管理していません。
> その為、複数回実行するとデータベースエラーが発生する可能性があります。

追加モジュールの環境セットアップをおこなう

1. 「 システム環境構築 」→「テナント環境セットアップ」をクリックします。
2. 「テナント環境セットアップ」をクリックします。

3. 「決定」をクリックします。



4. テナント環境セットアップが完了し、追加モジュールの環境セットアップができました。

注意
テナント環境セットアップボタンは更新するデータが存在しない（システムが最新の状態になっている）場合、表示されません。

Solr接続設定

intra-mart Accel Platform のSolr接続設定の表示、登録、更新を行います。

注意
Solr接続設定は、IM-ContentsSearch for Accel Platform利用時のみの設定です。

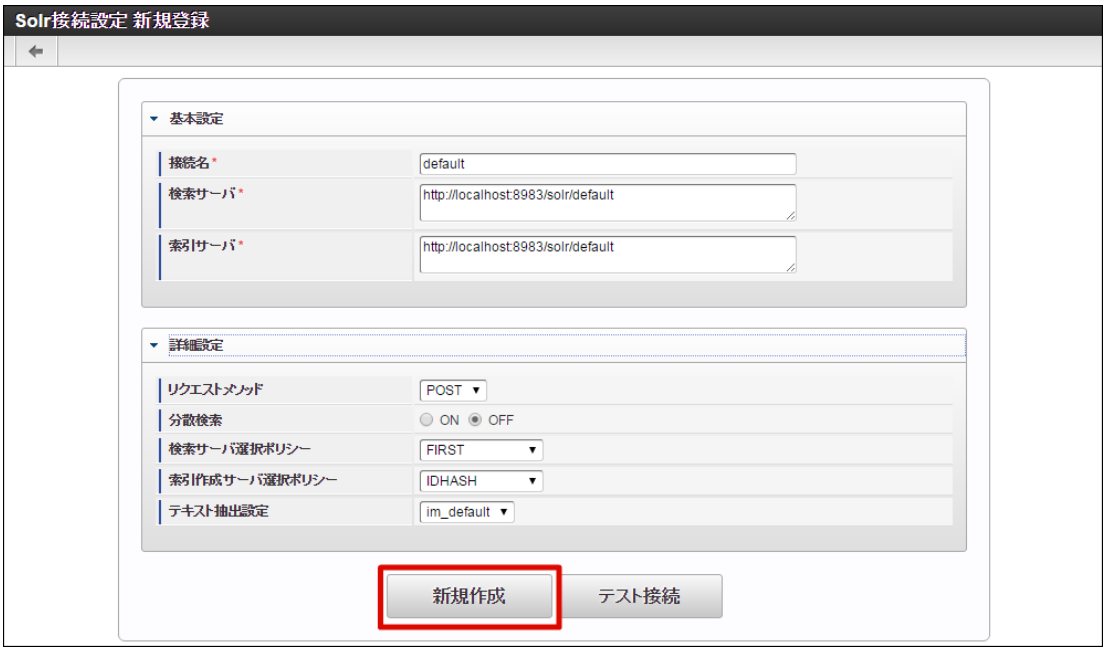
目次

- Solr接続設定を登録する
- Solr接続設定を参照する
- Solr接続設定を更新する
- Solr接続設定 入力項目

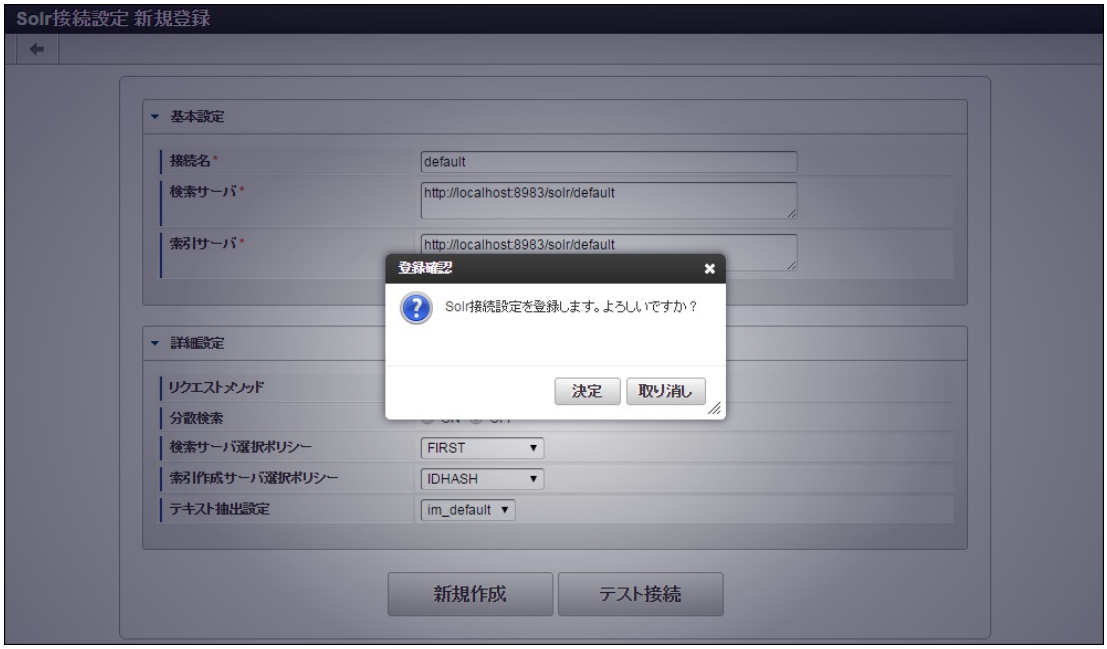
Solr接続設定を登録する

1. 「 システム環境構築 」→「Solr接続設定」をクリックします。
2. 「新規作成」をクリックします。

3. 内容を入力し、「新規作成」をクリックします。



4. 「決定」をクリックします。



5. Solr接続設定を登録することができました。

> **コラム**
> **テスト接続する場合**
> 「テスト接続」をクリックします。

Solr接続設定を参照する

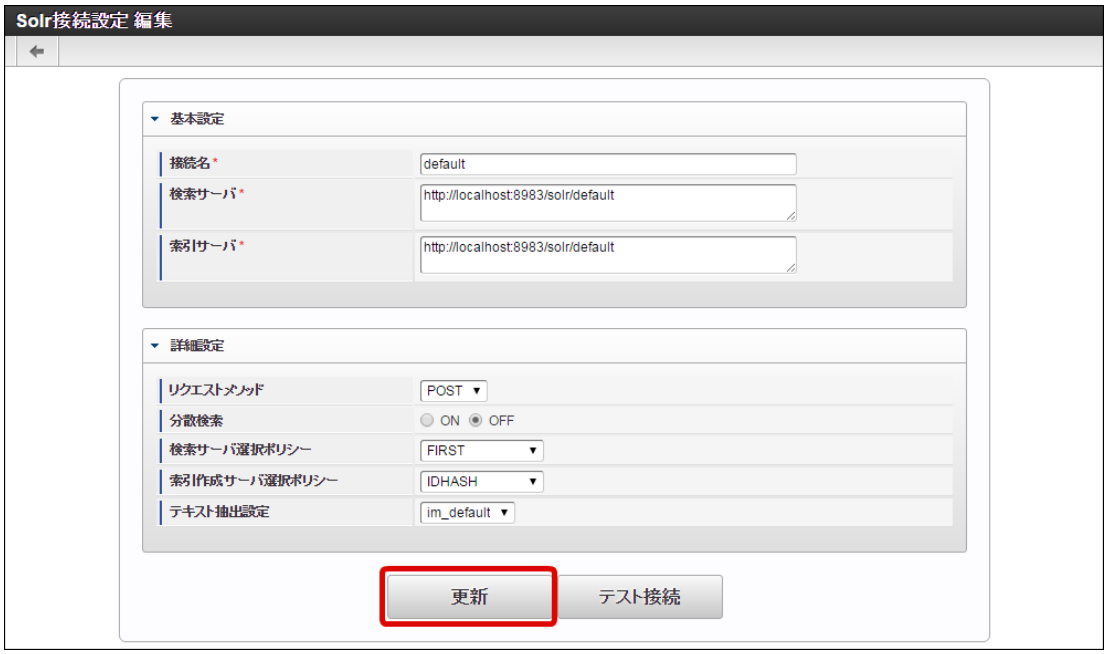
1. 「 システム環境構築 」→「Solr接続設定」をクリックします。
2. 参照したいSolr接続設定の接続名をクリックします。

3. Solr接続設定の詳細が表示されます。

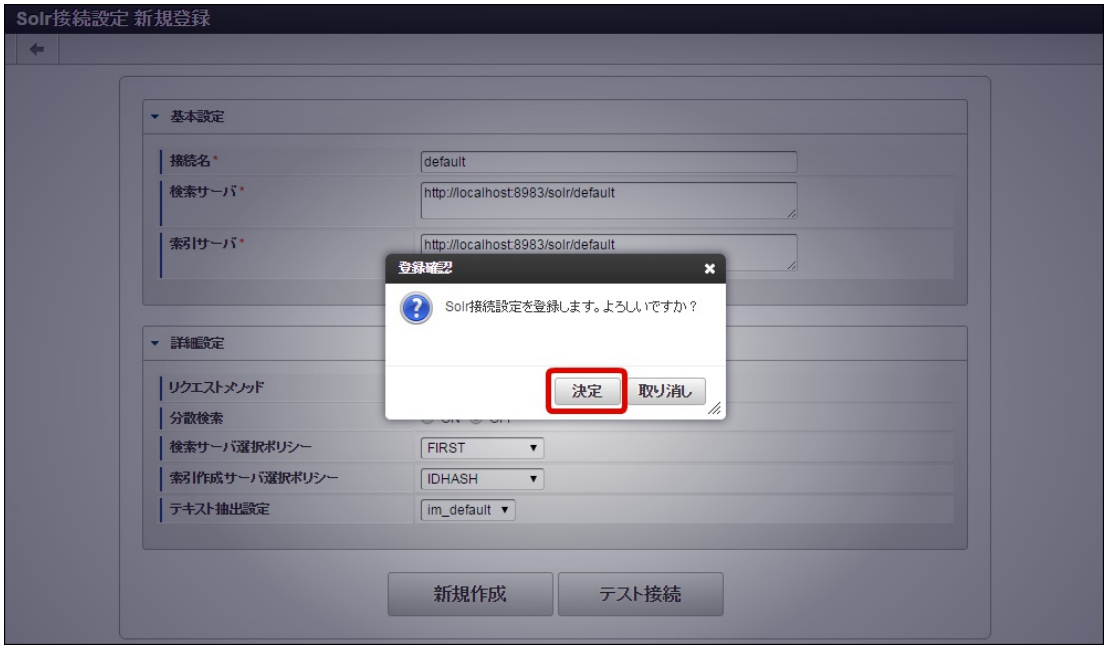
Solr接続設定を更新する

1. 「 システム環境構築 」→「Solr接続設定」をクリックします。
2. 更新したいSolr接続設定の接続名をクリックします。

3. 内容を入力し、「更新」をクリックします。



4. 「決定」をクリックします。



5. Solr接続設定を更新することができました。

Solr接続設定 入力項目

- 基本設定

項目	必須/任意	説明
接続名	必須	Solr接続設定の名称を入力します。
検索サーバ	必須	検索時に接続するSolrサーバのURLを設定します。 Solrサーバを構築しているホストのアドレス、および、ポート番号を指定してください。 例： *http://localhost:8983/solr/default*
索引サーバ	必須	索引作成時に接続するSolrサーバのURLを設定します。 Solrサーバを構築しているホストのアドレス、および、ポート番号を指定してください。 例： *http://localhost:8983/solr/default*

コラム

参考：各Web Application Serverのデフォルトのポート番号

Resin	8080
Tomcat	8080
Jetty	8983

- 詳細設定

項目	説明
リクエストメソッド	検索時にSolrサーバへ送るリクエストのメソッド（POST または GET）を設定します。
分散検索	複数のSolrサーバに分散配置されたインデックスを横断的に検索する機能の利用有無を設定します。 分散配置していない（冗長化などで、各Solrサーバが同一のインデックスを保持している）場合は、OFFに設定してください。
検索サーバ選択ポリシー	検索リクエストを送るSolrサーバを選択するポリシーを設定します。 **FIRST** 　最初に設定されたURLのサーバを常に利用します。 **ROUNDROBIN** 　設定されたサーバを順番に利用します。 **RANDOM** 　設定されたサーバをランダムで利用します。
索引作成サーバ選択ポリシー	索引を作成するSolrサーバを選択するポリシーを設定します。 同一IDの索引は同じSolrサーバに登録することが推奨されるため、通常はIDHASHから変更する必要はありません。 **IDHASH** 　索引のIDのハッシュ値を用いて、設定されたURLのサーバから利用するサーバを決定します。 **ROUNDROBIN** 　設定されたサーバを順番に利用します。 **RANDOM** 　設定されたサーバをランダムで利用します。
テキスト抽出設定	索引作成時にテキスト抽出するファイルの設定グループを指定します。 テキスト抽出設定（solr-extractor-config.xml）に設定されたテキスト抽出設定グループの名称が選択項目に表示されます。

注意

リクエストメソッドは通常はPOSTから変更する必要はありません。

システム管理

ここではシステム管理の操作を説明します。

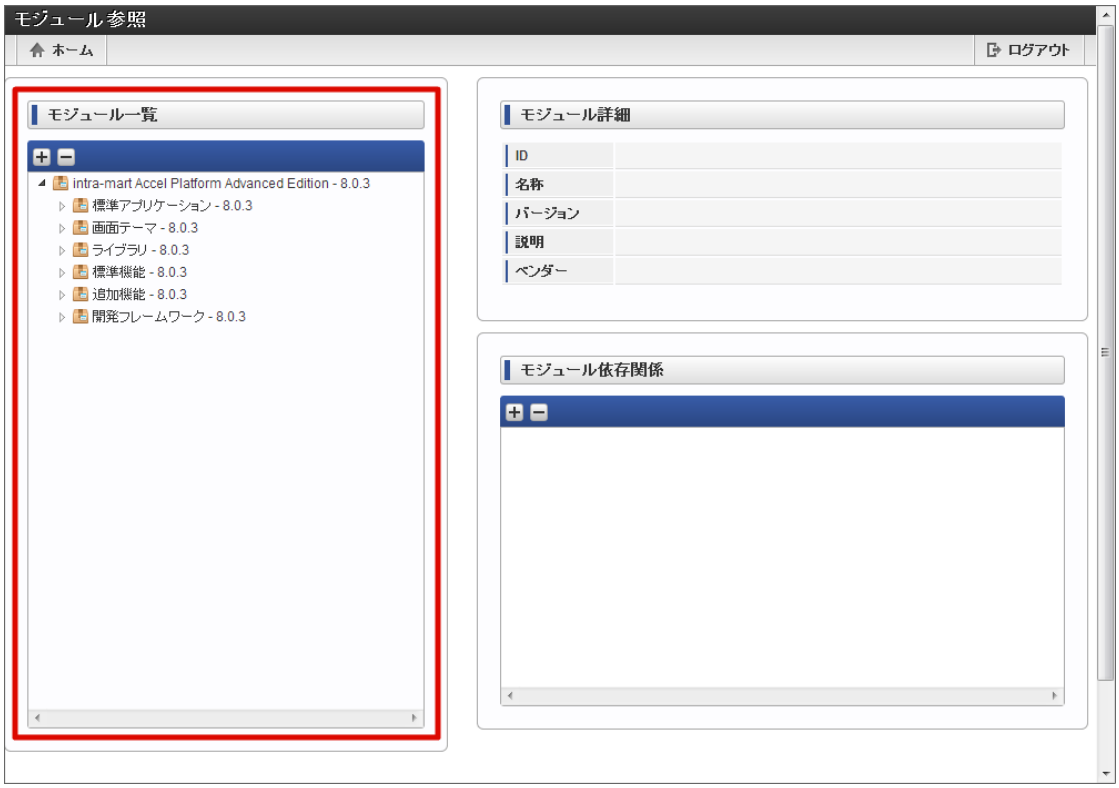
モジュール参照

起動中の テナント環境 を構成しているモジュール情報を参照することができます。

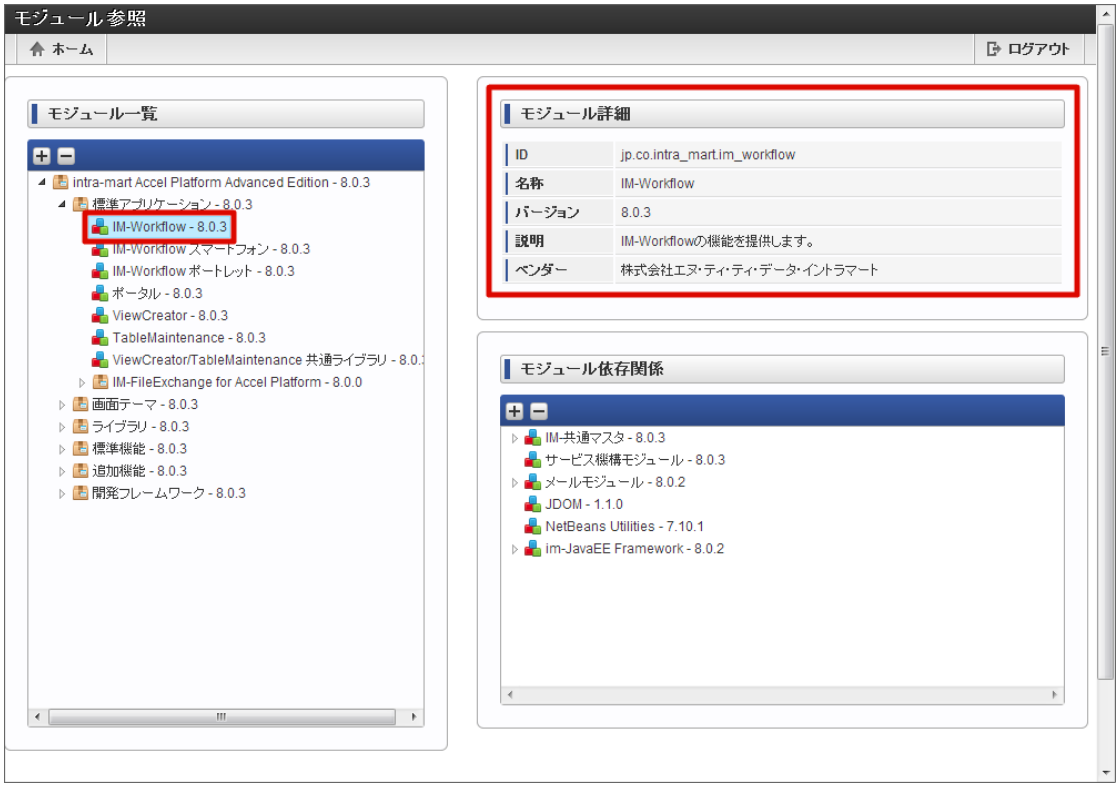
モジュール情報を確認する

1. 「 システム管理 」→「モジュール参照」をクリックします。
2. 「モジュール参照」画面が表示されます。

モジュール一覧
テナント環境 を構成しているモジュールの一覧を表示します。

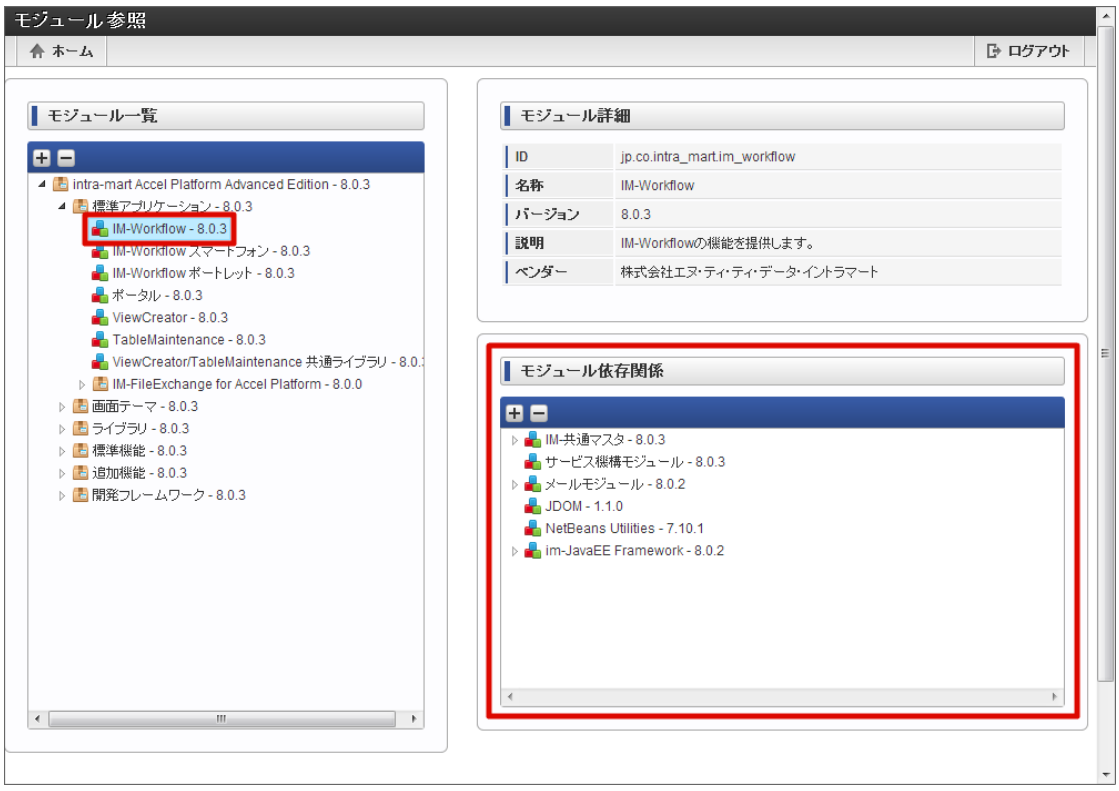


モジュール詳細
モジュール一覧よりモジュールを選択すると、選択されたモジュールの詳細情報が表示されます。



依存関係

モジュール一覧よりモジュールを選択すると、選択されたモジュールが依存しているモジュールが表示されます。



> **注意**
>
> モジュール情報は国際化されていません。
> モジュール情報のロケールはWARファイルの作成を行った際の IM-Juggling のロケールに基づいています。

サービス設定

サービスの起動状況や、アプリケーションサーバの稼働状況などシステムに関する情報を参照できます。

目次

- サービス状況を確認する
- サービスを停止する
- サービスを再開する

注意

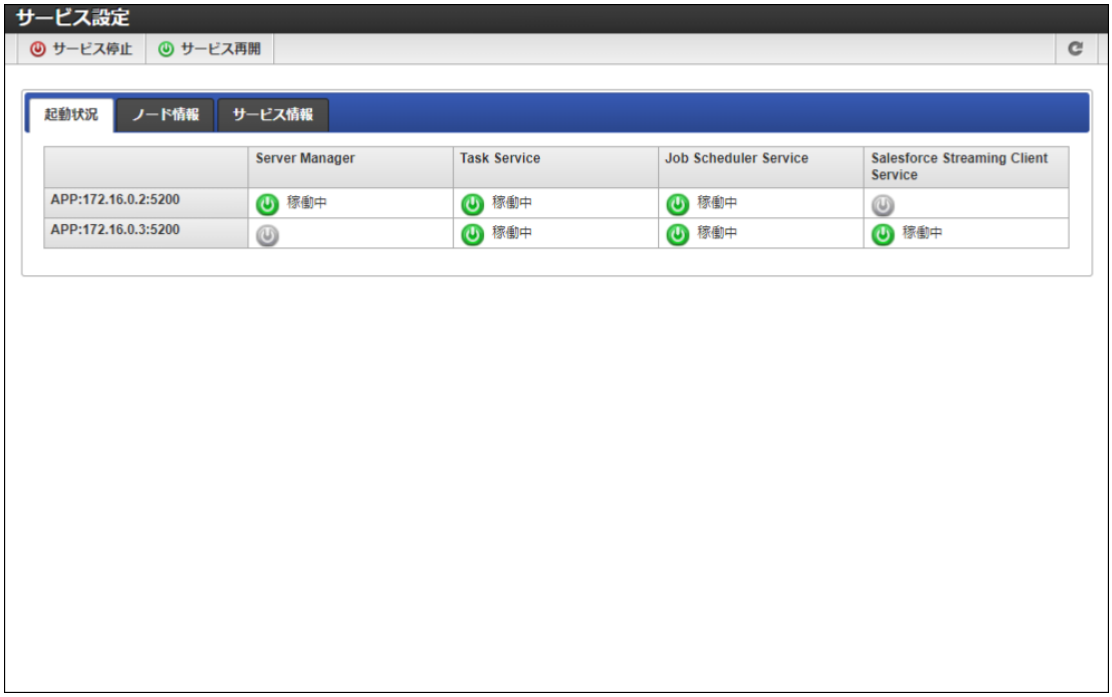
「*サービスを停止する*」、「*サービスを再開する*」 は、intra-mart Accel Platform 2020 Spring(Yorkshire) 以降で利用できます。

サービス状況を確認する

1. 「 システム管理 」→「サービス設定」をクリックします。
2. 「サービス設定」画面が表示されます。

起動情報

アプリケーションサーバ毎にサービスの起動情報を表示します。



サービスの状態

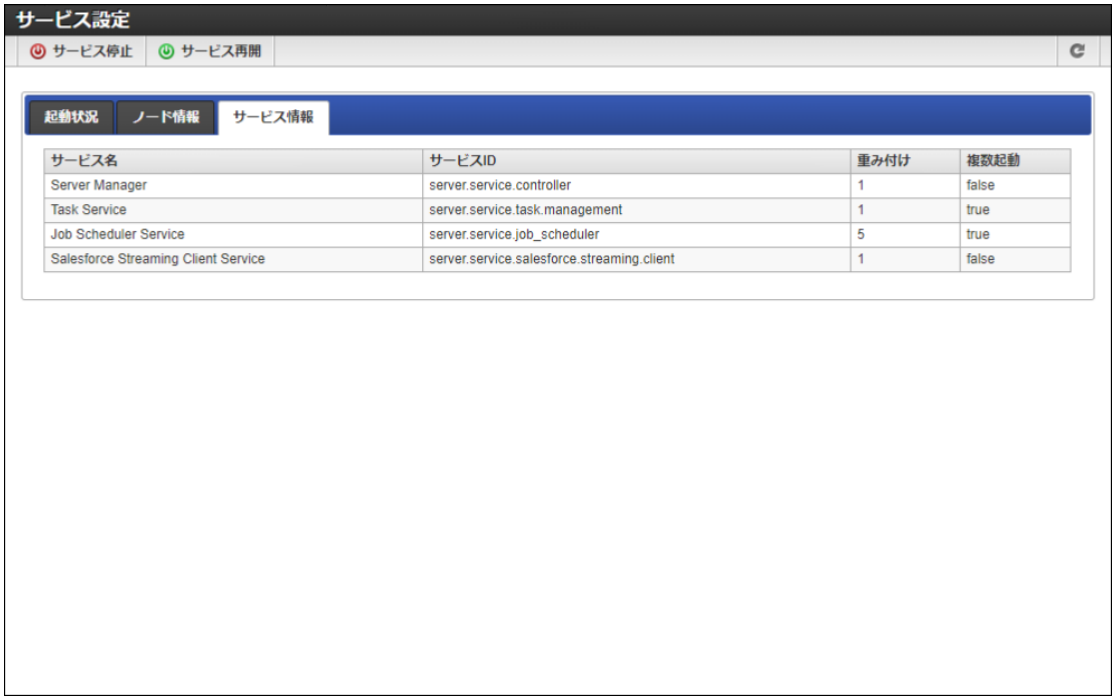
画像	状態	説明
	稼働中	サービスが開始している状態を表します。 各サービスの機能が提供されています。
	スタンバイ	サービスが開始可能な状態を表します。 サービスが開始しているサーバが停止した場合等、代わりにサービスを開始します。
	停止中	サービスが停止している状態を表します。 停止中のサービスはサービスの再開が行われるまで開始されません。

ノード情報

アプリケーションサーバの情報が表示されます。

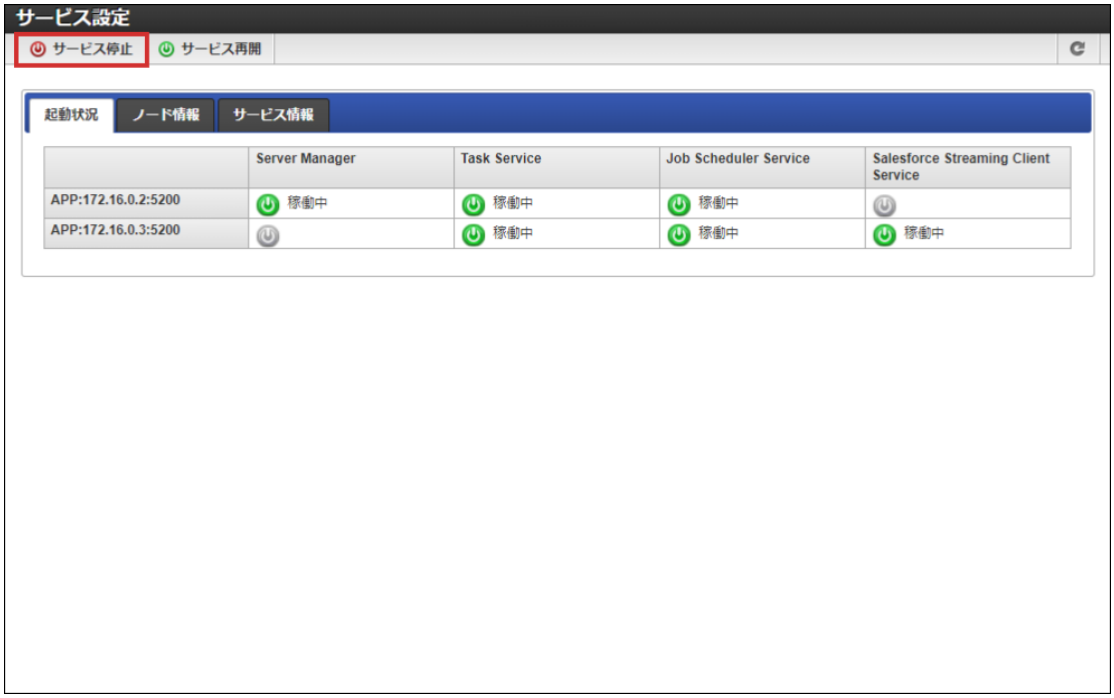
サービス情報

サービス情報が表示されます。

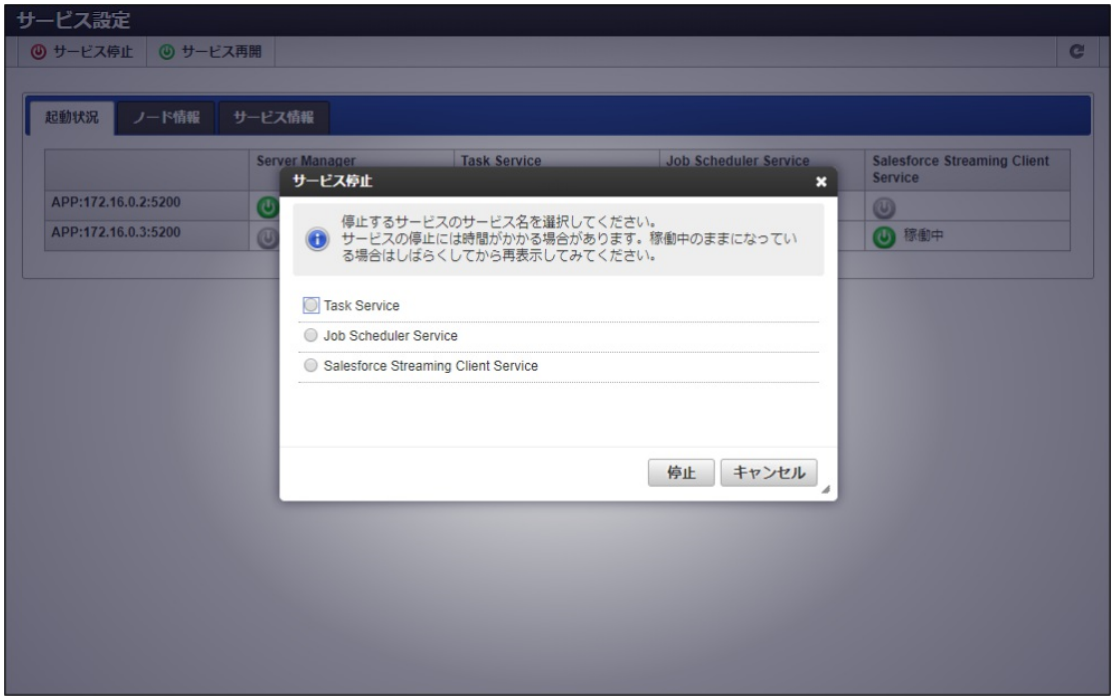


サービスを停止する

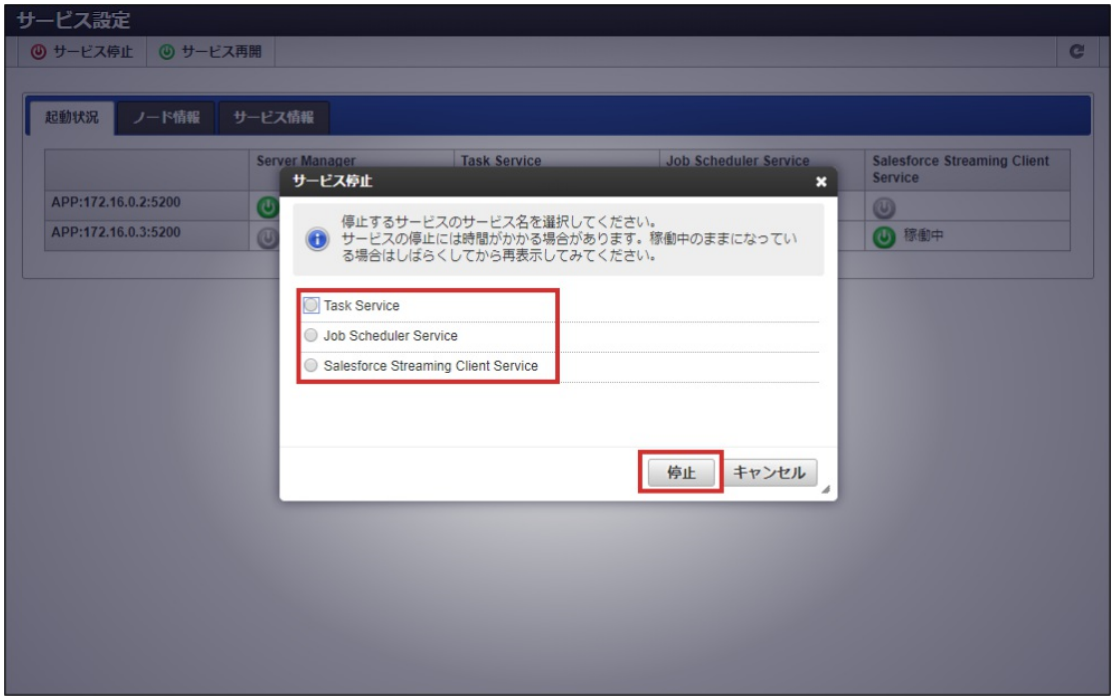
1. 「 システム管理 」→「サービス設定」をクリックします。
2. ツールバーより「サービス停止」をクリックします。



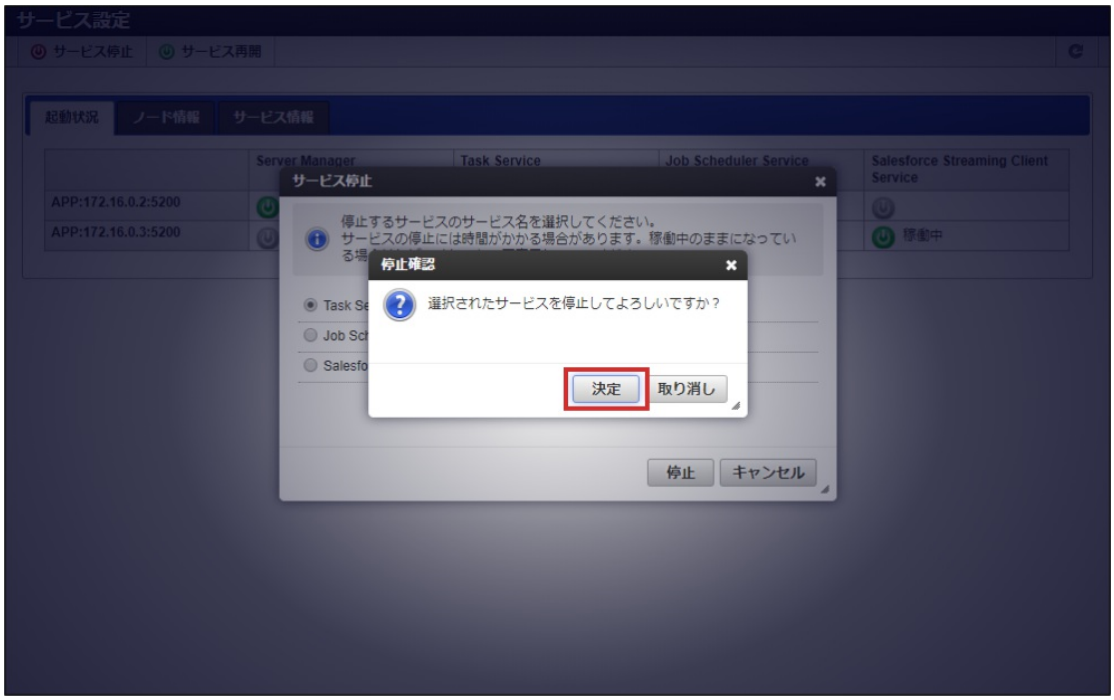
3. サービス停止ダイアログが表示されます。



4. 停止するサービスを選択して「停止」をクリックします。



5. 停止確認ダイアログの「決定」をクリックします。



6. 選択したサービスが停止しました。

コラム

停止したサービスは、サーバを再起動しても開始されません。
サービスを再開したい場合は、「*サービスを再開する*」を行う必要があります。

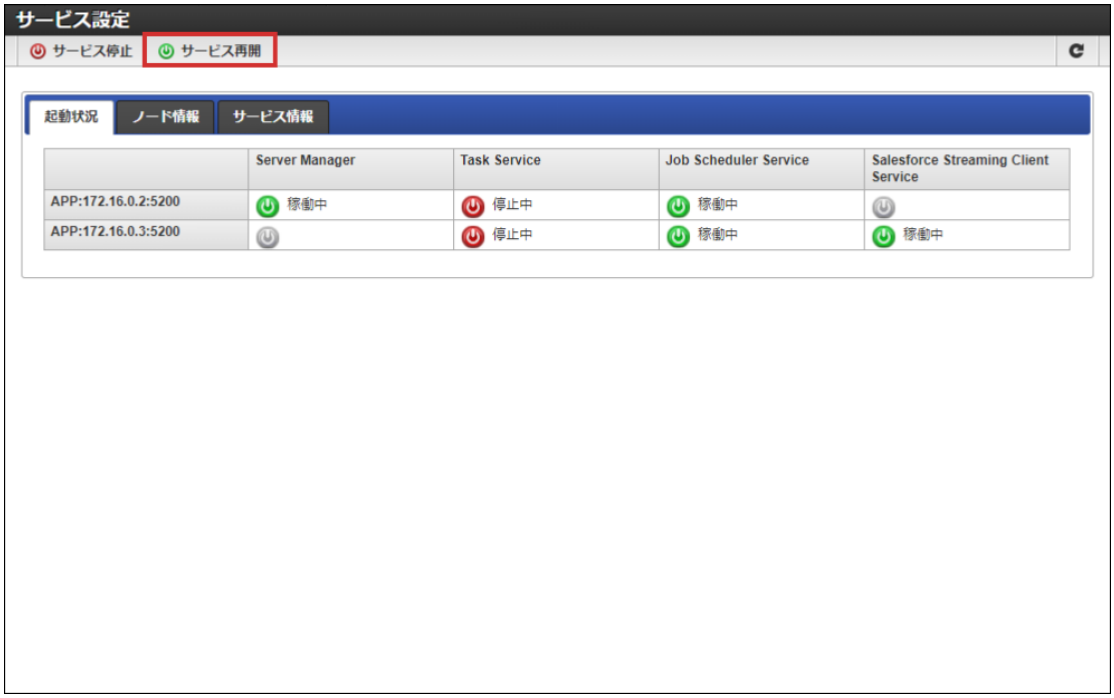
注意

タスクサービス、ジョブスケジューラサービスでタスクやジョブが実行されている場合、サービスを停止しても実行中のタスクやジョブは停止されません。
サービス停止後、実行中のタスクやジョブが存在するかはそれぞれ以下の画面から確認してください。

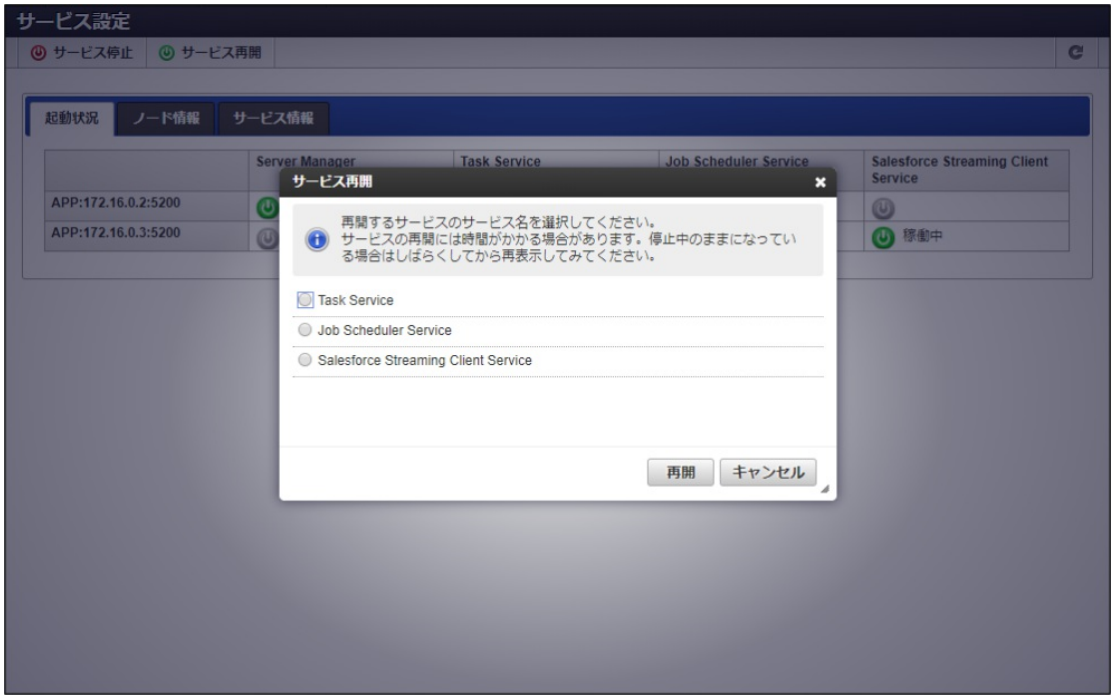
* タスク ： 「*非同期-タスクキュー一覧*」
* ジョブ ： 「テナント管理者操作ガイド」 - 「ジョブネットモニター覧」

サービスを再開する

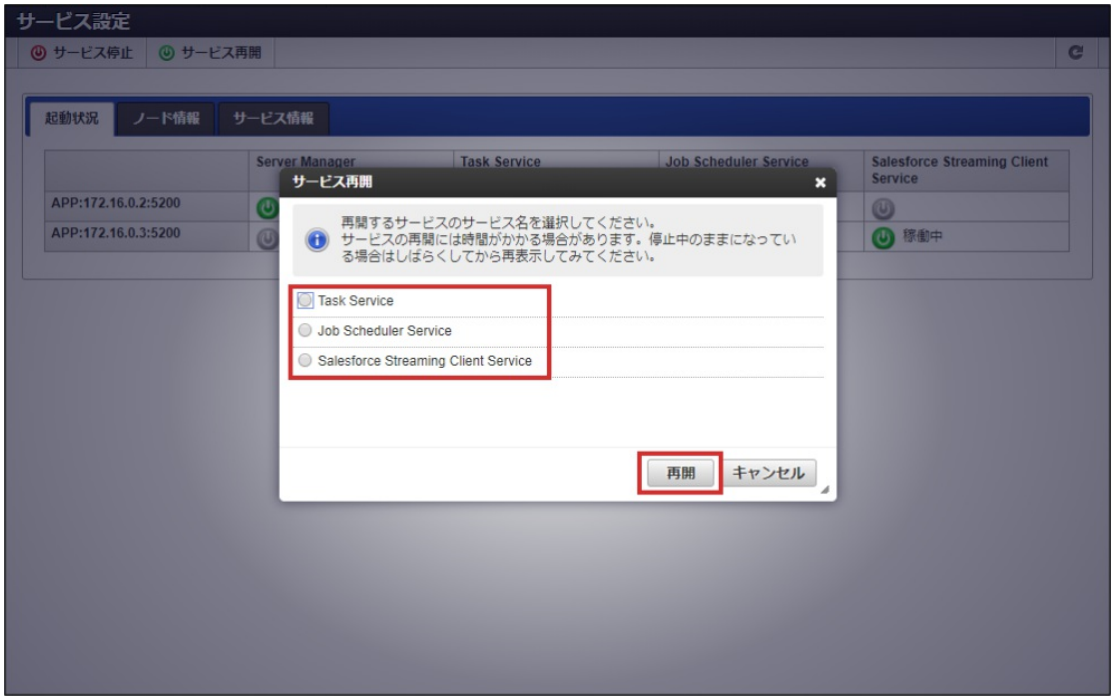
1. 「 システム管理 」→「サービス設定」をクリックします。
2. ツールバーより「サービス再開」をクリックします。



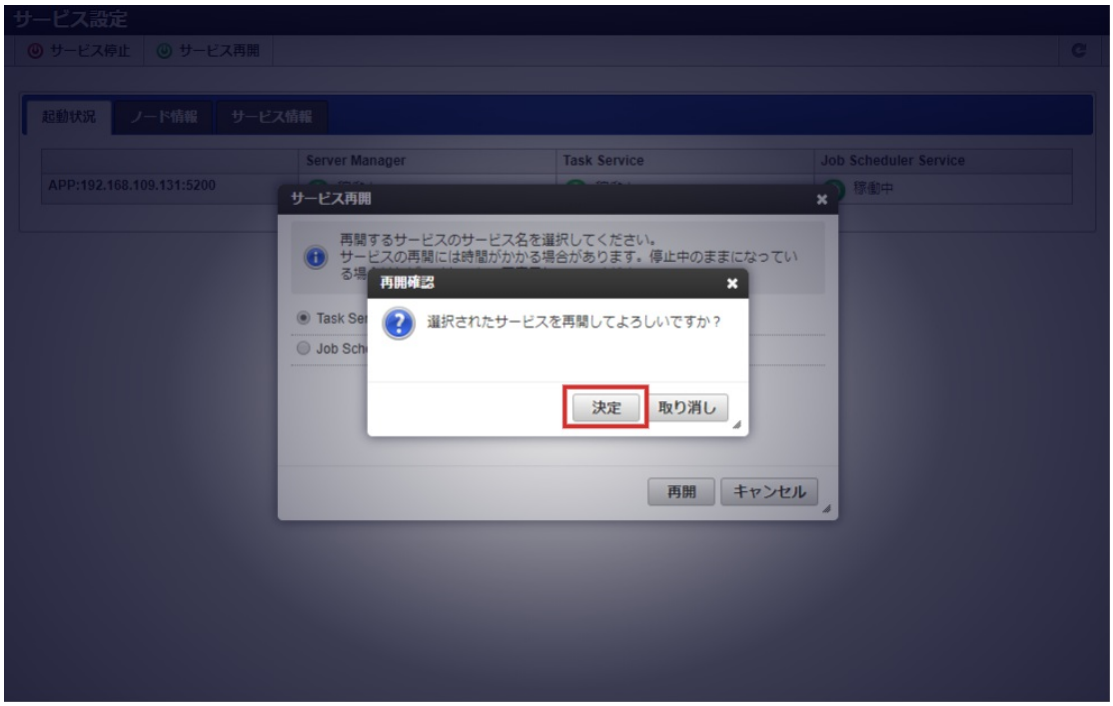
3. サービス再開ダイアログが表示されます。



4. 再開するサービスを選択して「再開」をクリックします。



5. 再開確認ダイアログの「決定」をクリックします。



6. 選択したサービスが再開しました。

アプリケーションロック一覧

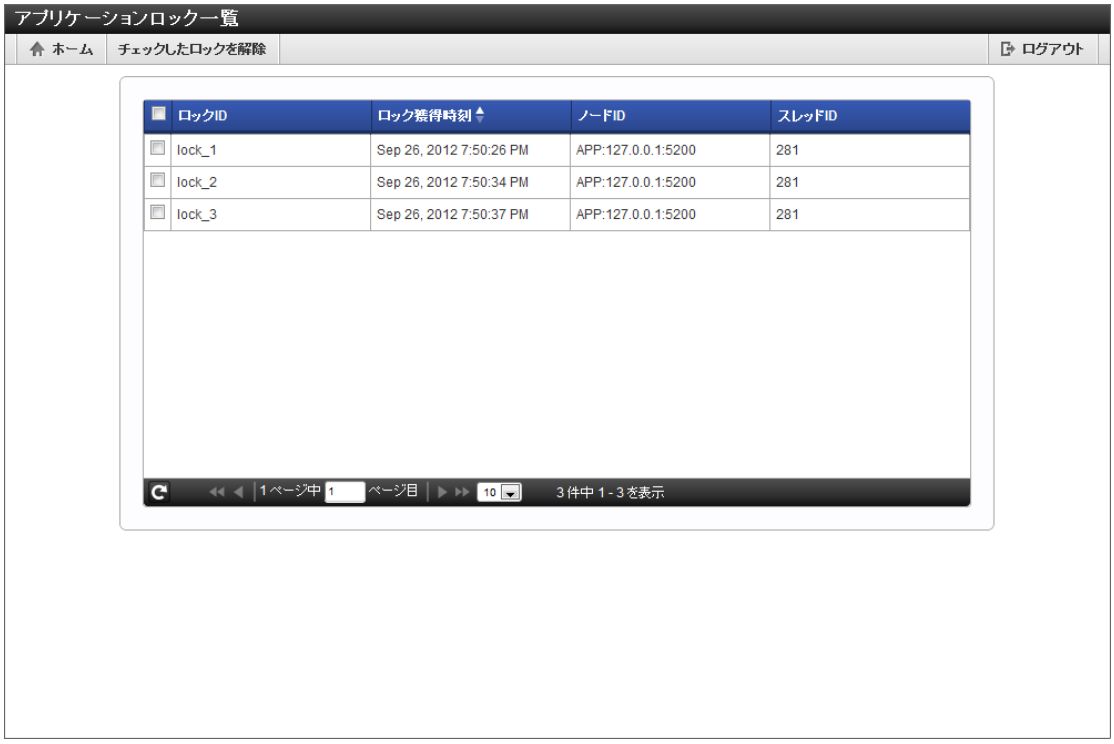
アプリケーションロックされた情報を一覧表示し、必要であればロックの解除を行います。

目次

- アプリケーションロックを確認する
- アプリケーションロックを解除する

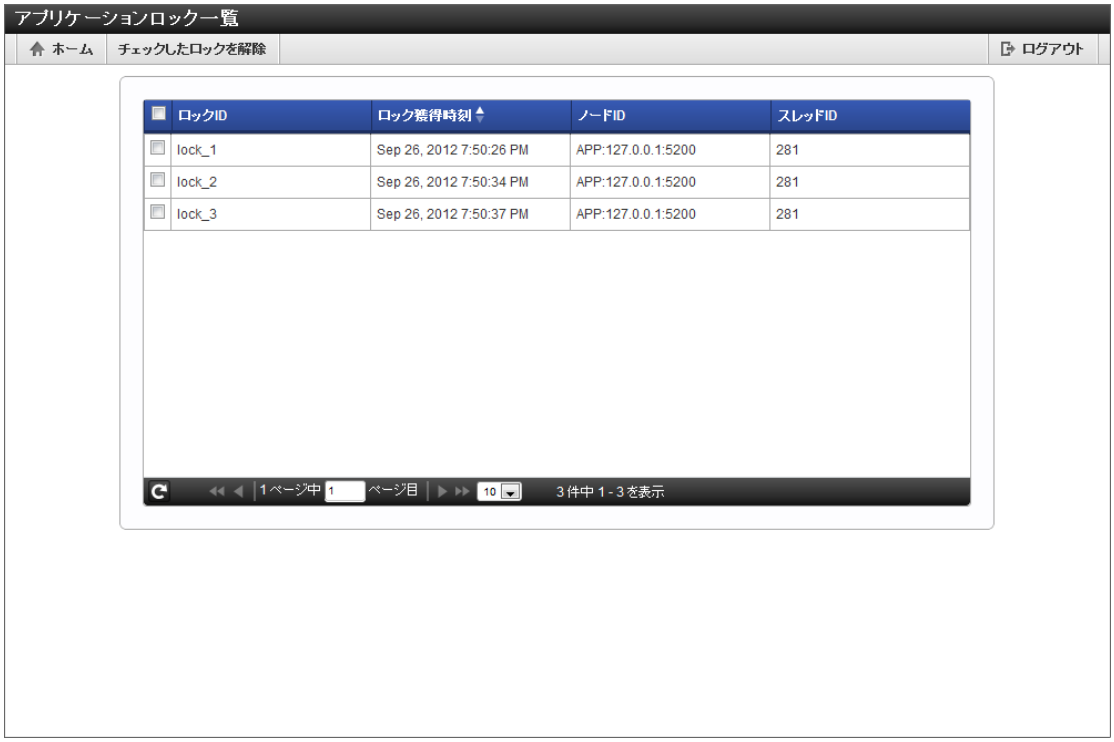
アプリケーションロックを確認する

1. 「 システム管理 」→「アプリケーションロック一覧」をクリックします。
2. 「アプリケーションロック一覧」画面が表示されます。

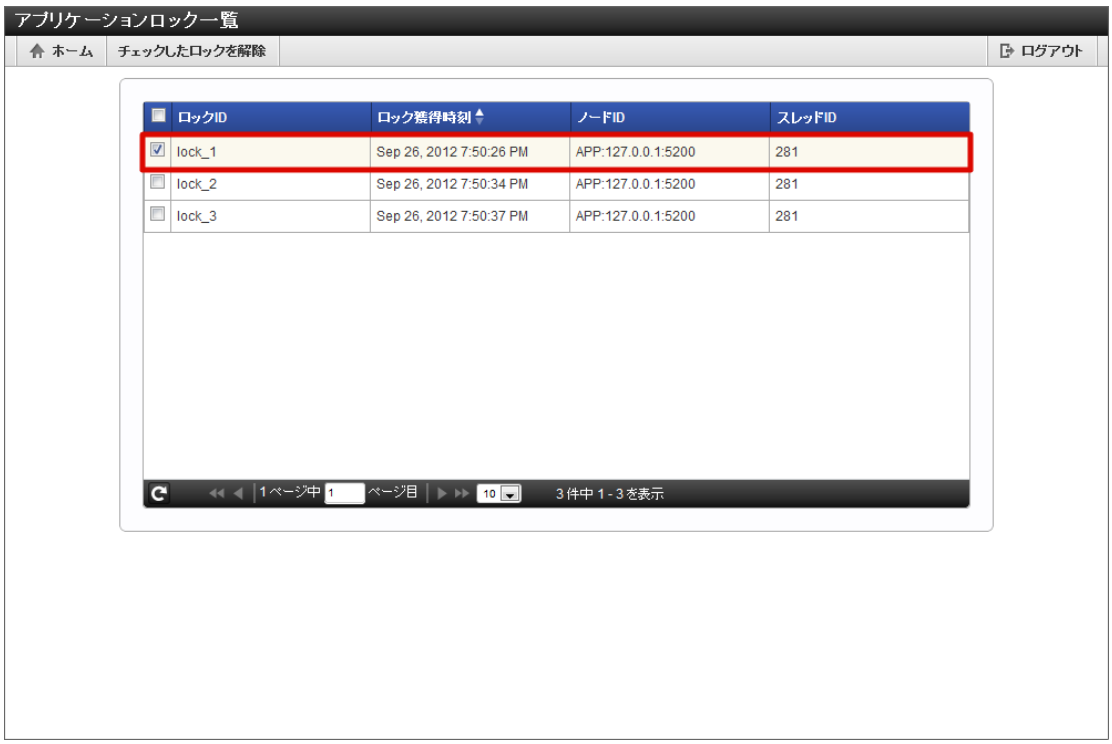


アプリケーションロックを解除する

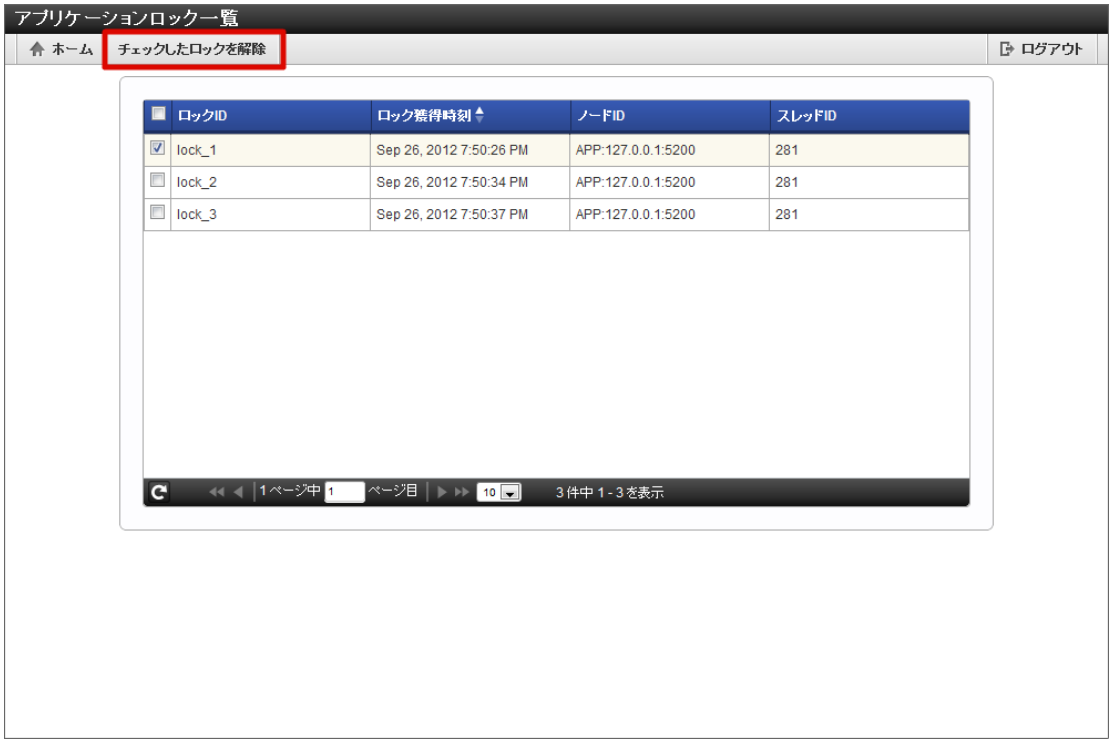
1. 「 システム管理 」→「アプリケーションロック一覧」をクリックします。
2. 「アプリケーションロック一覧」画面が表示されます。



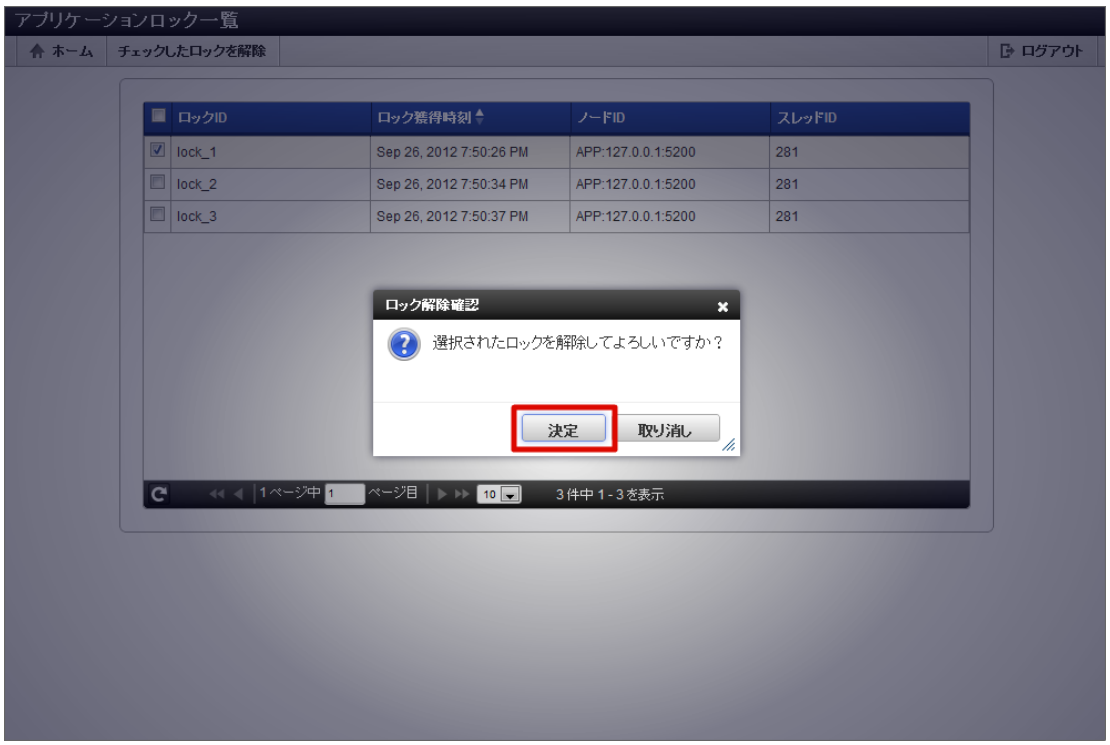
3. 解除したいアプリケーションロックをチェックをいれます。



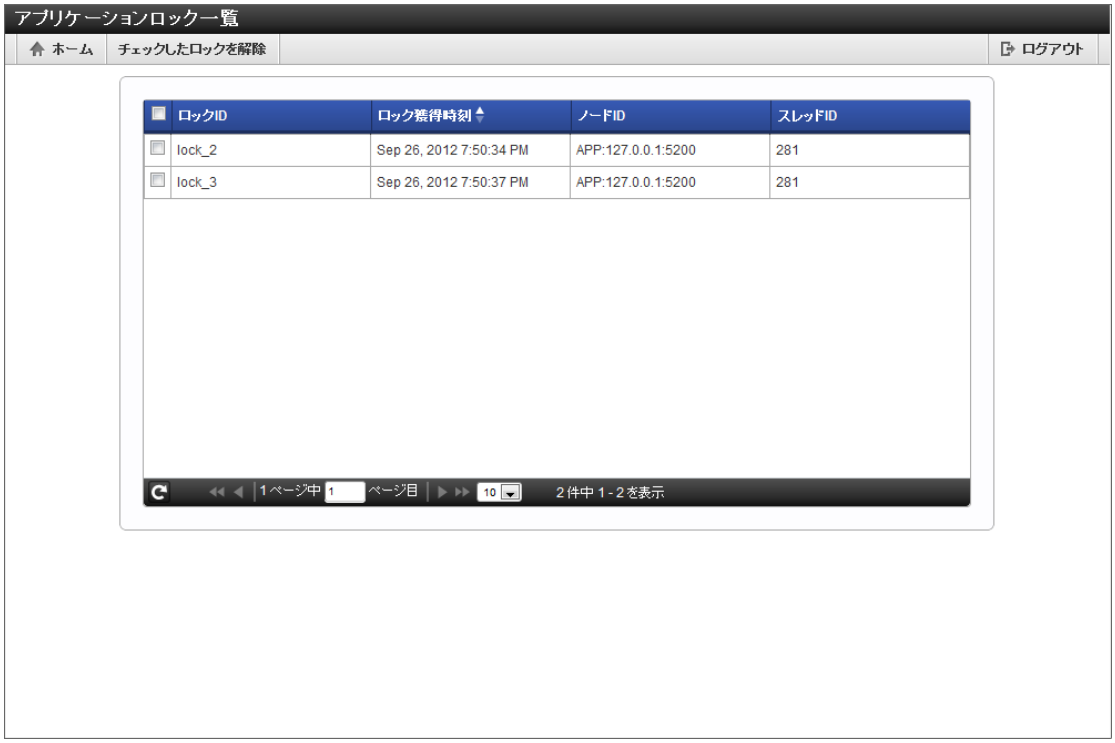
4. 「チェックしたロックを解除」をクリックします。



5. 「決定」をクリックします。



6. アプリケーションロックを解除することができました。



> **注意**
> ロックを開始した処理が終わらないうちにロックを解除してしまうと、処理の実行中に予期しない動作が行われる可能性があります。 その為、ロックを解除する場合は、十分に注意してください。

ファイル操作

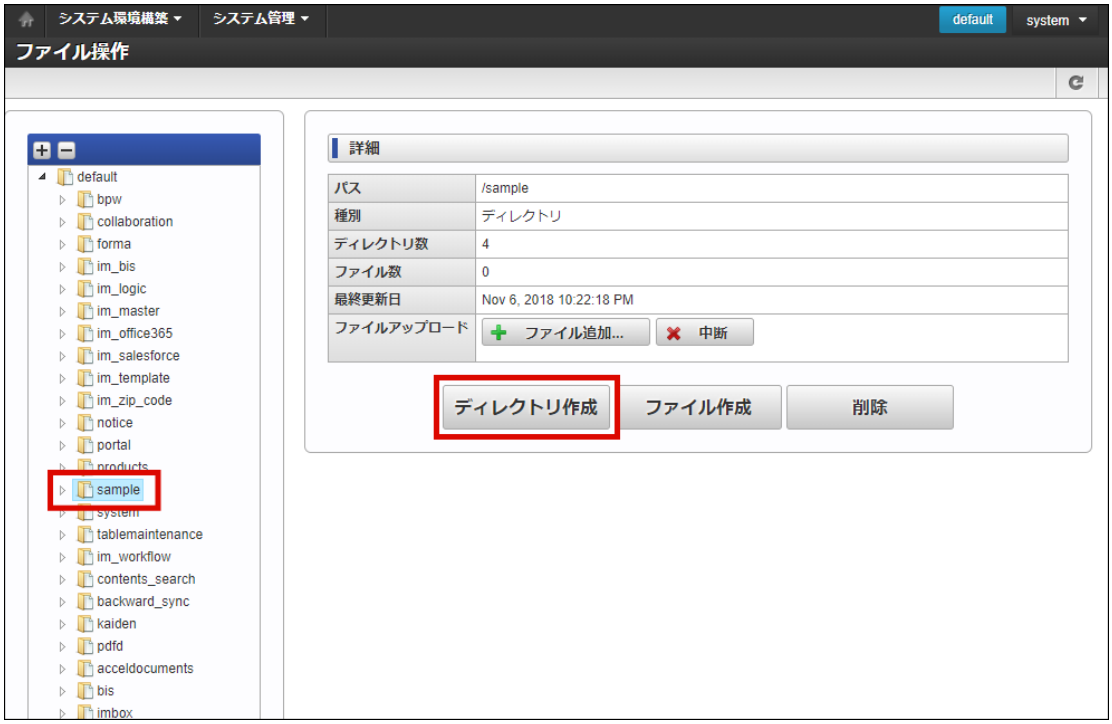
Storage領域に対してディレクトリやファイルの新規作成、ファイルの削除やアップロードなどが行えます。
アップロードされたファイルはStorage領域に保存されます。

目次

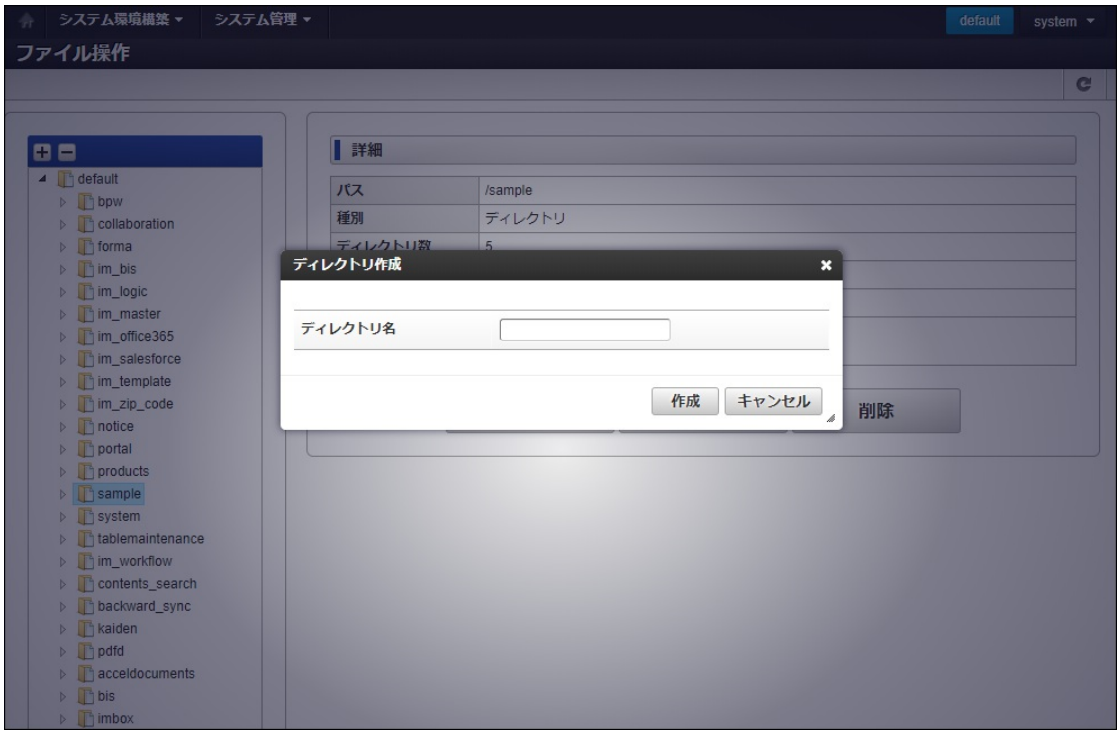
- ディレクトリを作成する
- ファイルを作成する
- ファイルをアップロードする
- ファイルをダウンロードする

ディレクトリを作成する

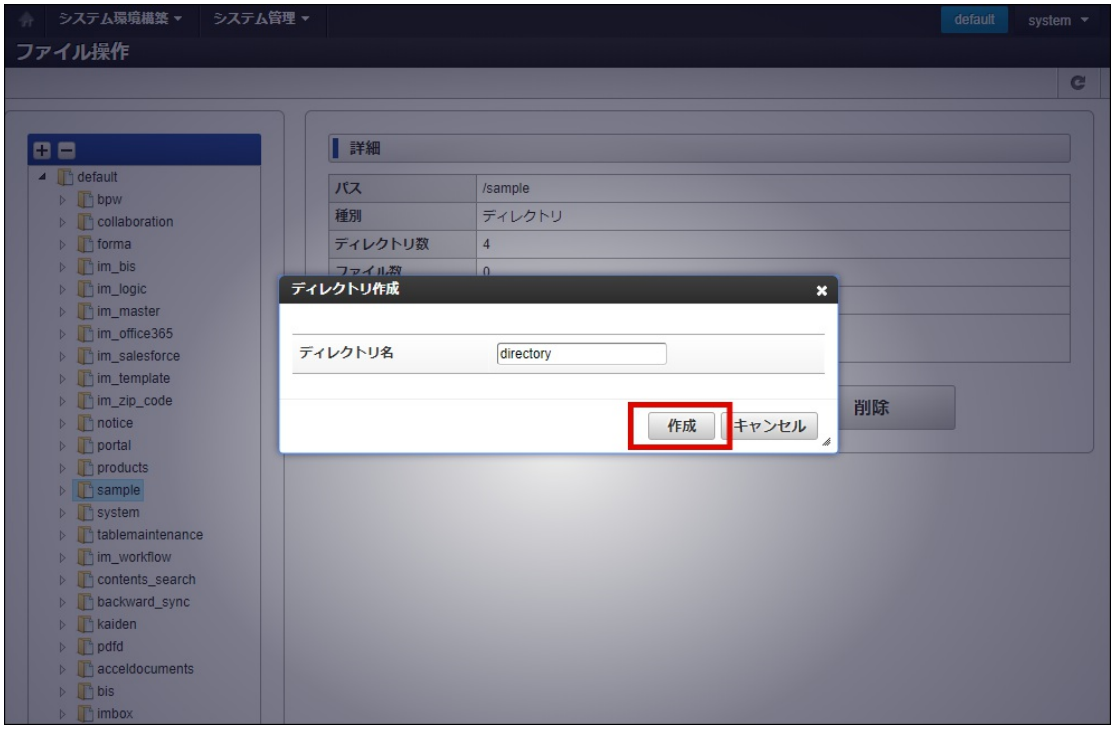
1. 「 システム管理 」→「ファイル操作」をクリックします。
2. 左側のツリーからディレクトリを作成したい位置をクリックします。
   指定したディレクトリ直下に、ディレクトリを作成します。
3. 「ディレクトリ作成」をクリックします。



4. 「ディレクトリ作成」画面が表示されます。



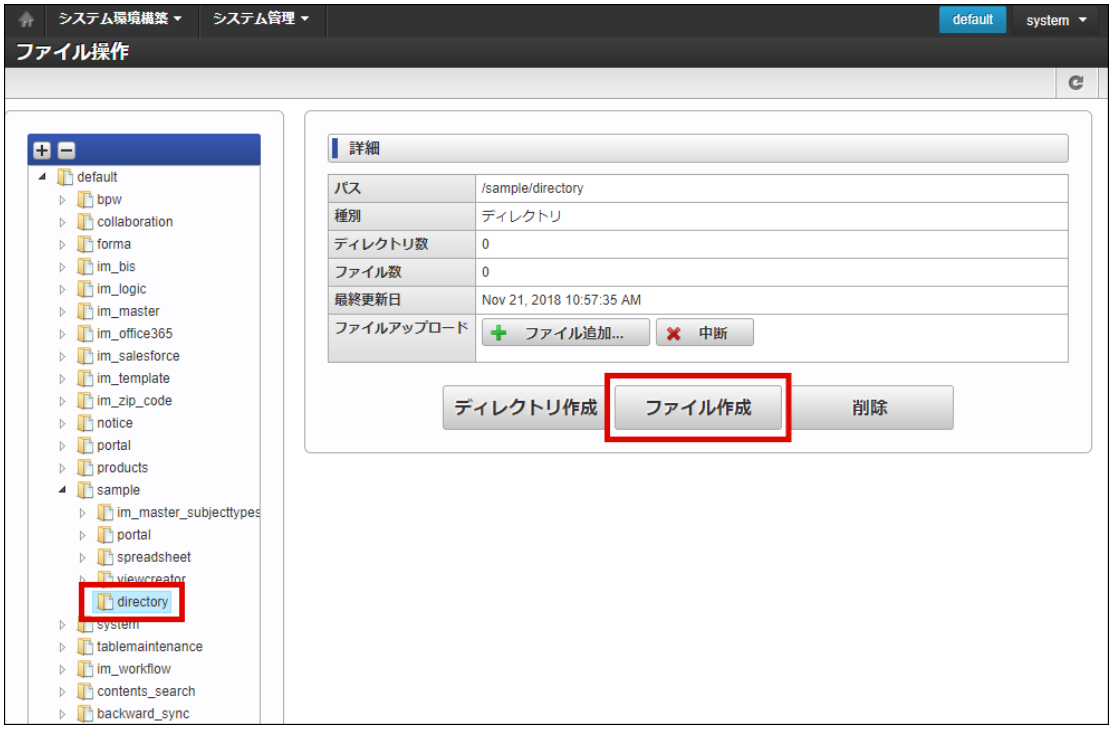
5. 「作成」をクリックします。



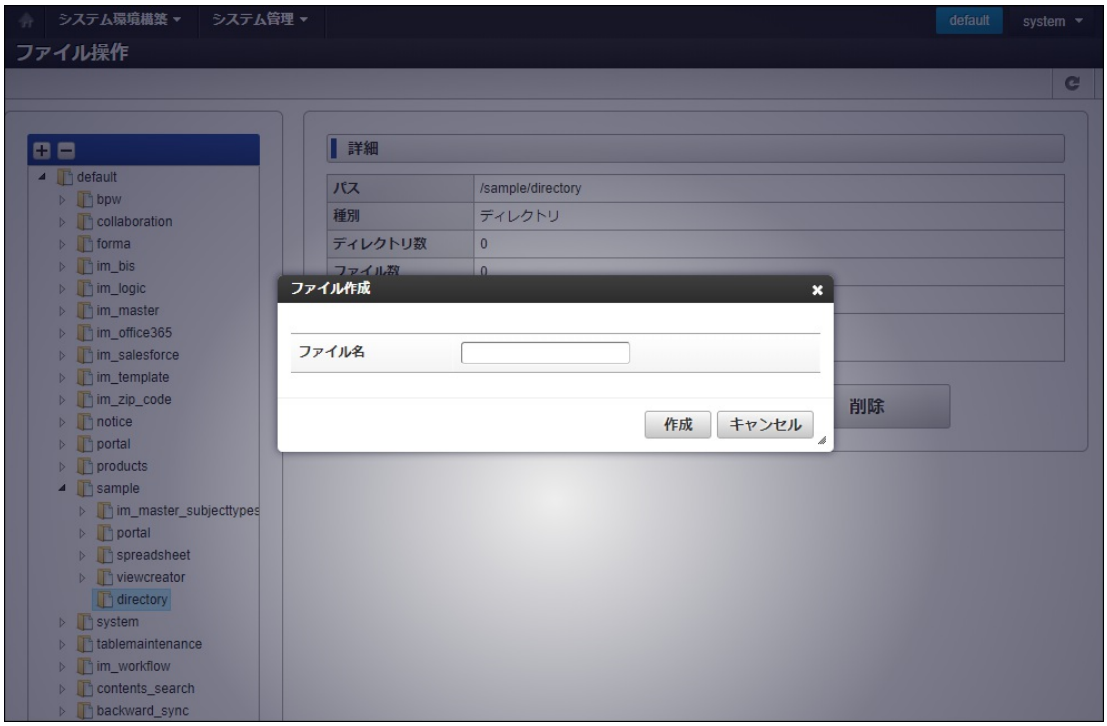
6. ディレクトリを作成できました。

ファイルを作成する

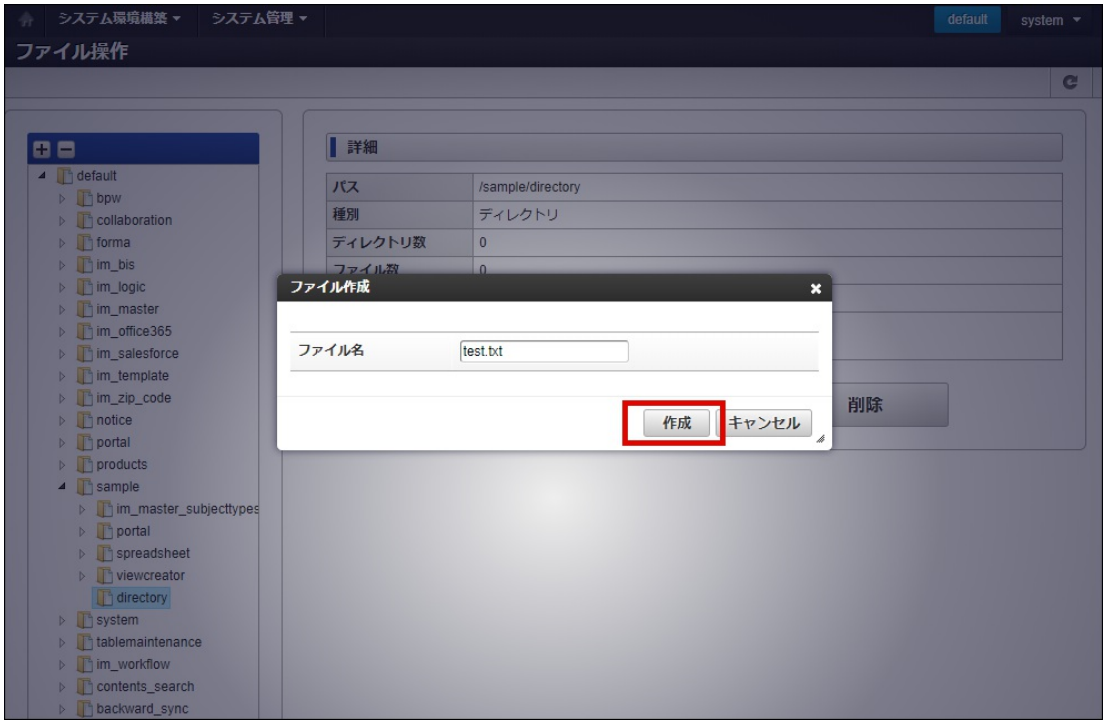
1. 「 システム管理 」→「ファイル操作」をクリックします。
2. 左側のツリーからディレクトリを作成したい位置をクリックします。
   指定したディレクトリ直下に、ディレクトリを作成します。
3. 「ファイル作成」をクリックします。



4. 「ファイル作成」画面が表示されます。



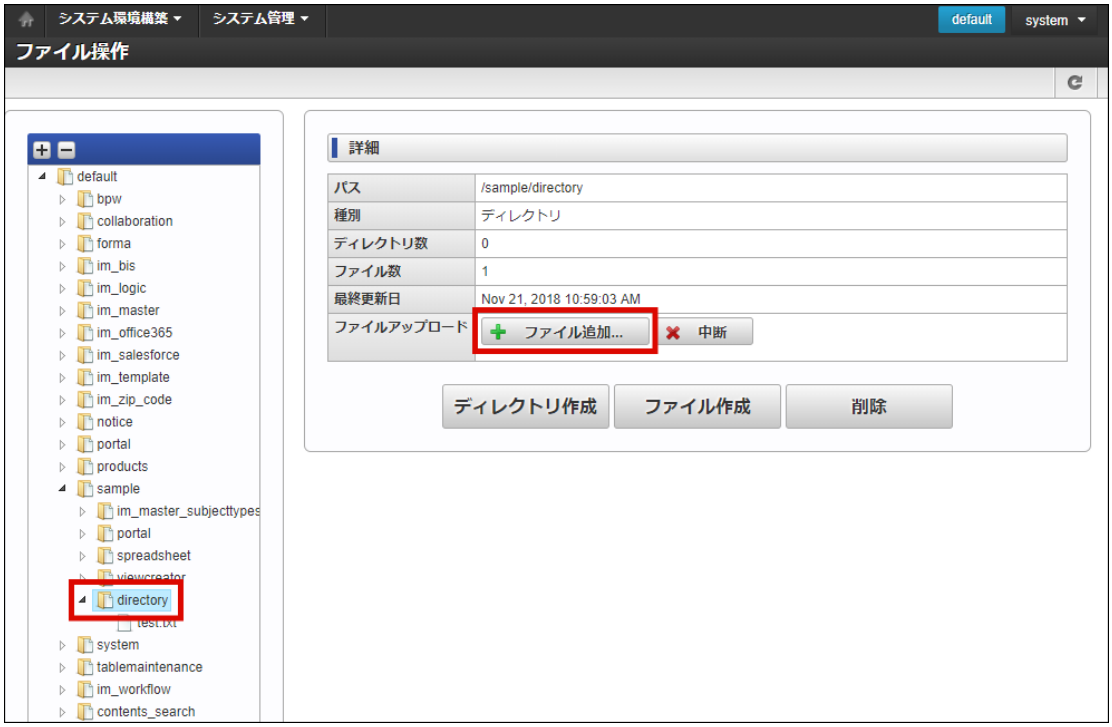
5. 「作成」をクリックします。



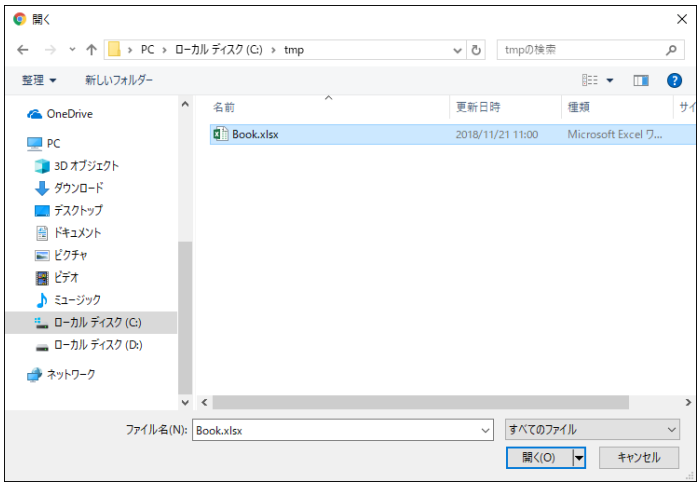
6. ファイルを作成できました。

ファイルをアップロードする

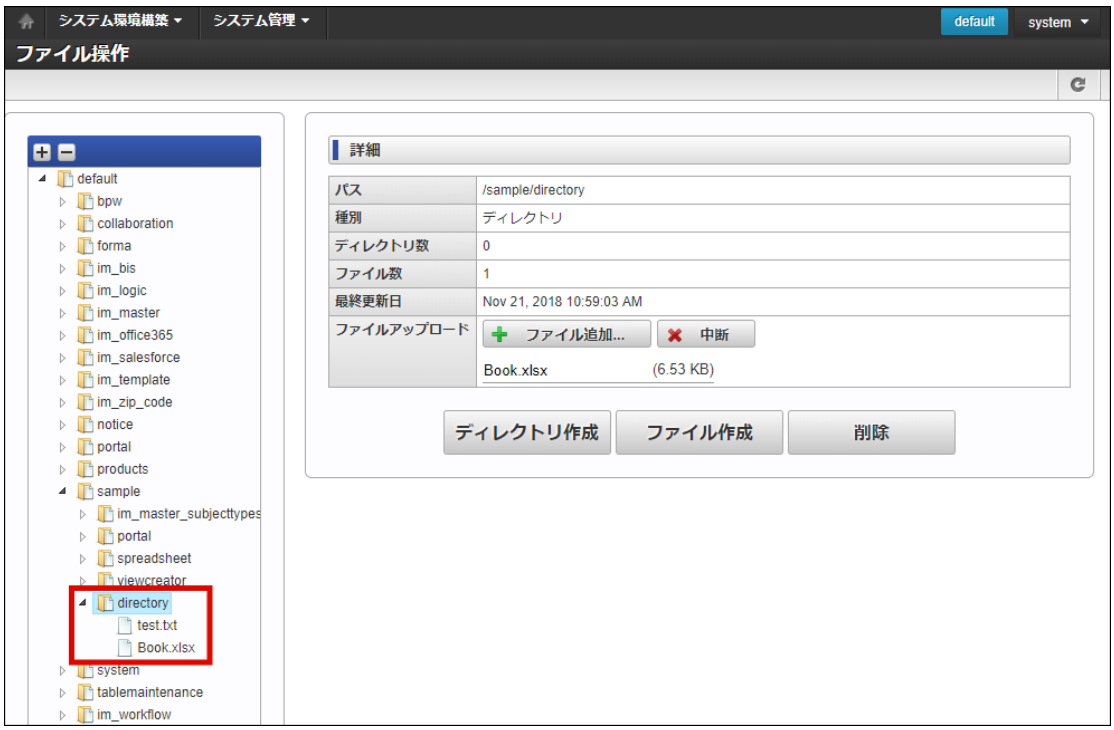
1. 「 システム管理 」→「ファイル操作」をクリックします。
2. 左側のツリーからファイルをアップロードしたいディレクトリをクリックします。
   指定したディレクトリ直下に、ファイルをアップロードします。
3. 「ファイル追加」をクリックします。



4. ファイルを選択します。

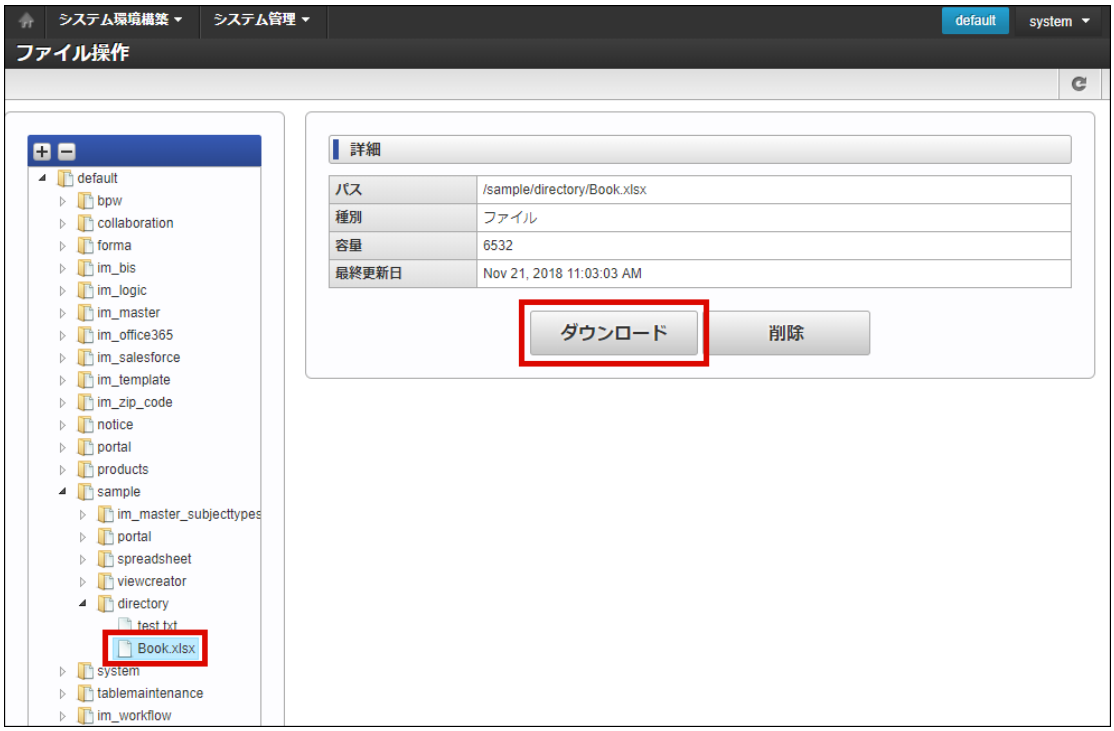


5. ファイルをアップロードできました。

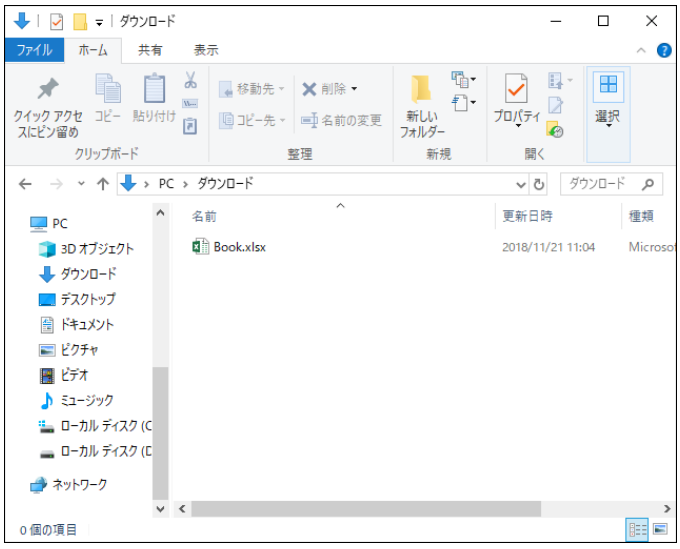


ファイルをダウンロードする

1. 「 システム管理 」→「ファイル操作」をクリックします。
2. 左側のツリーからダウンロードしたいファイルをクリックします。
3. 「ダウンロード」をクリックします。



4. ファイルをダウンロードできました。



> **コラム**
> **ディレクトリ・ファイルの移動**
> ツリーのノードをドラック&ドロップするとディレクトリおよびファイルの移動ができます。

データベース操作

データベースに対してSQL文を直接実行するための簡易ツールです。

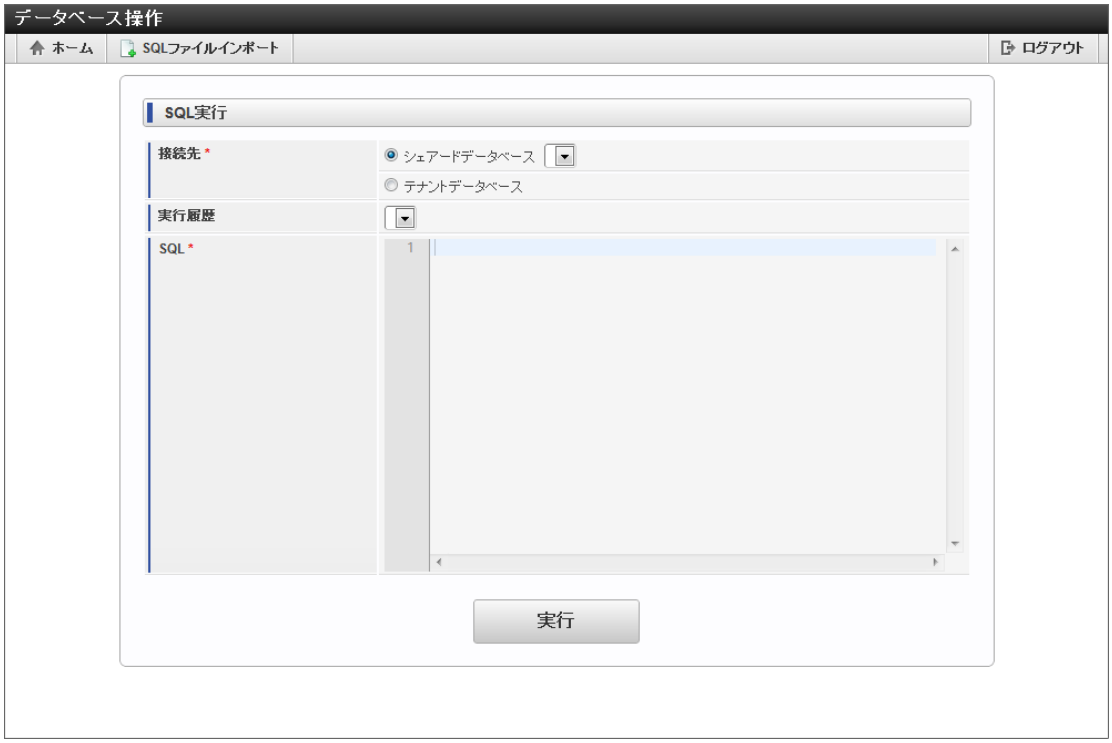
実行方法には、テキストエリアにSQL文を記入して実行する「SQL実行」と、ファイルに定義したSQL文を実行する「SQLファイルインポート」の方法があります。

目次

- SQLを実行する
- SQLファイルをインポートし実行する

SQLを実行する

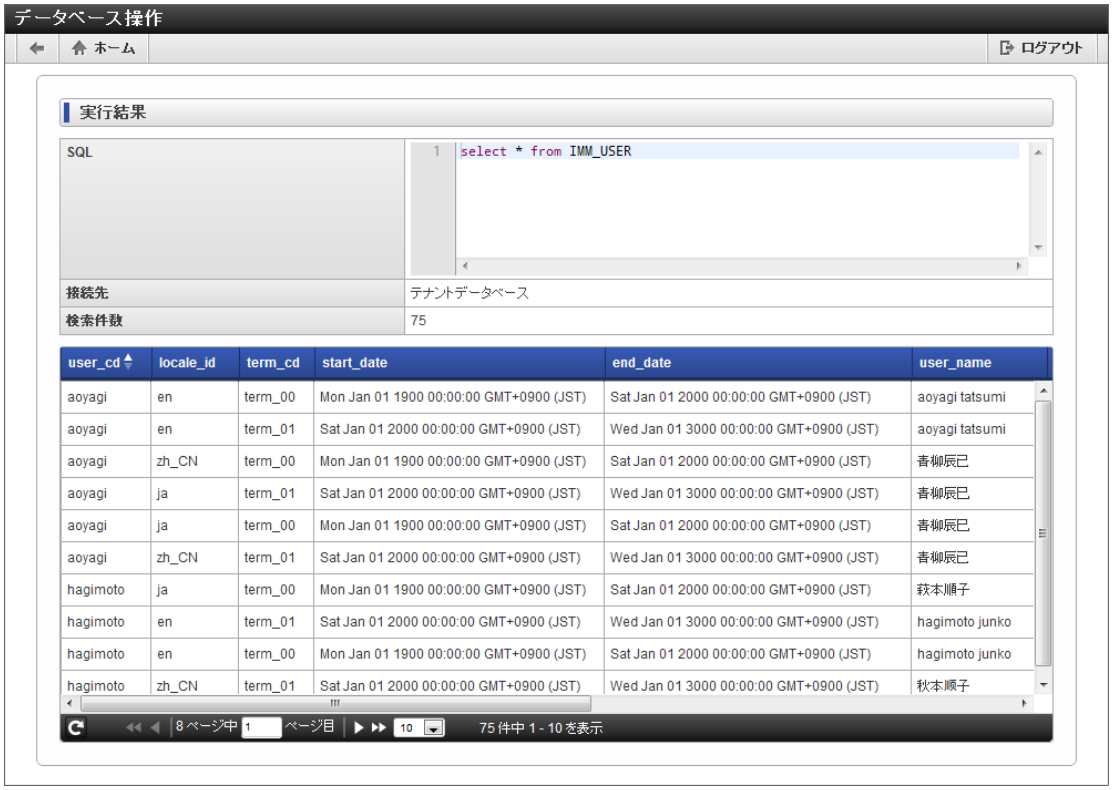
1. 「 システム管理 」→「データベース操作」をクリックします。
2. 「データベース操作」画面が表示されます。



- 接続先
  登録した「シェアードデータベース」または、「テナントデータベース」から選択します。

3. 「実行」をクリックします。

4. SQLを実行できました。

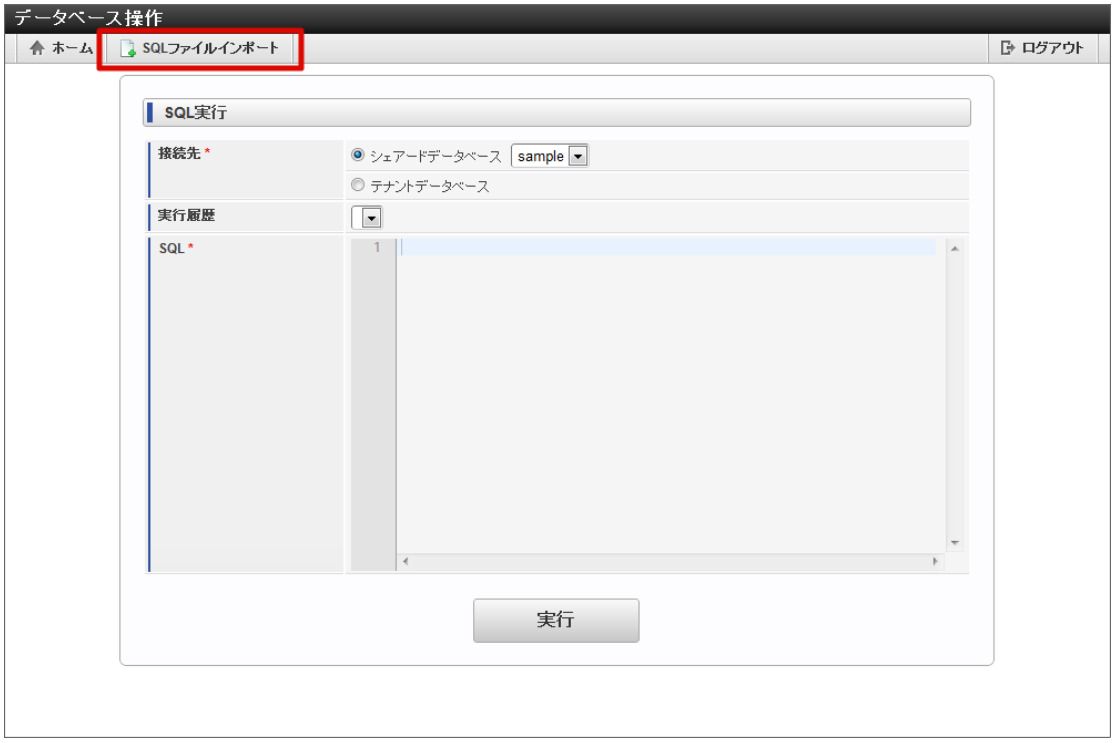


> **コラム**
> シェアードデータベースの設定は **「システム管理」-「シェアードデータベース設定」** を参照してください。

> **コラム**
> **実行履歴を参照する**
> 実行したSQLは最新10件まで実行履歴として残され、コンボボックスから日付を選択するとそのSQLが表示されます。

SQLファイルをインポートし実行する

1. 「 システム管理 」→「データベース操作」をクリックします。
2. 「SQLファイルインポート」をクリックします。

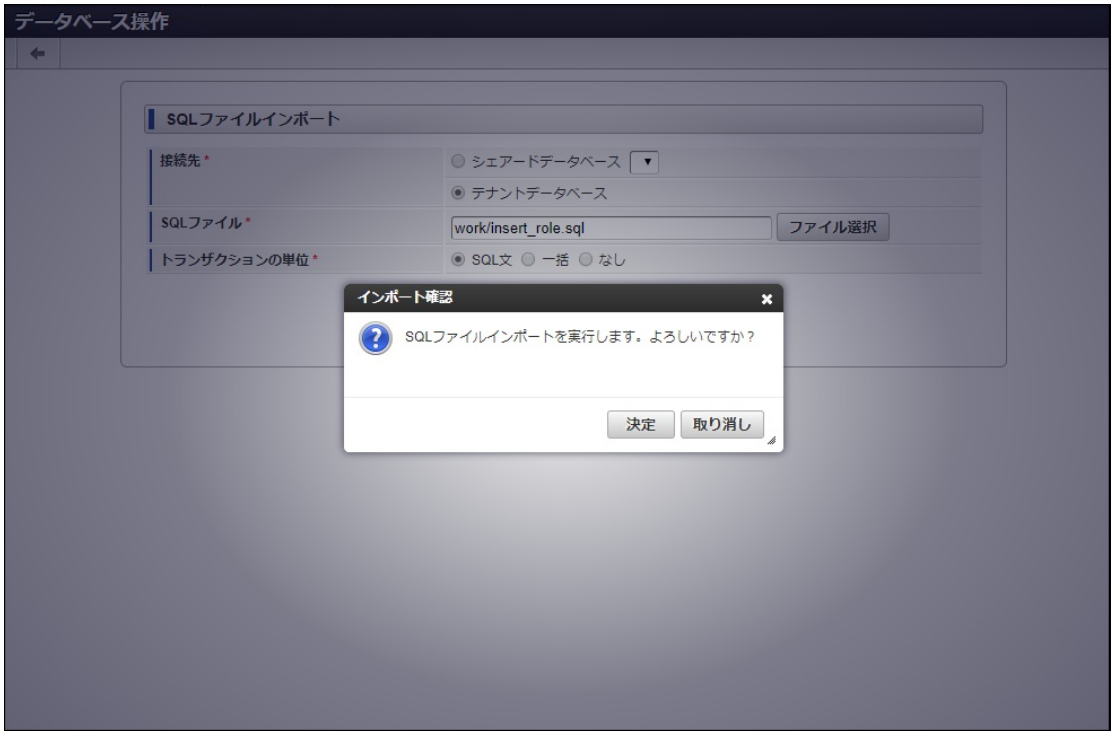


3. 「データベース操作」画面が表示されます。

- 接続先
  登録した「シェアードデータベース」または、「テナントデータベース」から選択します。
- SQLファイル
  「ファイル選択」をクリックし、「ファイル選択ダイアログ」画面よりファイルを選択します。
- トランザクションの単位
  - SQL文
    トランザクションをSQL文単位に設定します。
    SQL文を発行する度にコミットまたはロールバック処理が行われます。
    途中でエラーが発生した場合も、全てのSQL文が実行されます。
  - 一括
    トランザクションを一括に設定します。
    ファイルに定義された全てのSQL文を実行後、コミット処理を行います。
    途中でエラーが発生した場合は、ロールバック処理を行って処理を終了します。
    ※但しDDL文を発行した際のトランザクションの挙動は、データベースに依存します。
  - なし
    トランザクションを設定しません。
    ファイルに定義されたSQL文を1行実行毎にコミット処理を暗黙で行います。
    途中でエラーが発生した場合は、処理を終了します。
    ※PayaraのOracle XADataSourceを使用する環境で、DDL文を含むファイルのインポートを行う場合に選択します。

4. 「インポート」をクリックします。

5. 「決定」をクリックします。



6. SQLファイルのインポートが実行できました。

注意

- SQLファイル内は、SQL文ごとに「セミコロン（；）＋ 改行」で区切って記述してください。
- インポートするファイルの文字コードはStorage領域の文字コードと同じ文字コードで保存してください。
  文字コードが異なると、文字化けが発生する可能性があります。

非同期-タスクキュー一覧

非同期処理を利用してビジネスロジックを実行するために必要な情報（タスクメッセージ）はタスクキューに登録されます。

- 並列タスクキュー
  同時に処理を行うことが可能なタスクメッセージのみで構成されるタスクキューです。
- 直列タスクキュー
  逐次的に処理を行うことが必要なタスクメッセージのみで構成されるタスクキューです。

詳細は **「非同期仕様書」** を参照してください。

この画面ではタスクキューの参照、タスクメッセージの操作を行うことができます。

目次

- 直列タスクキューを登録する
- 直列タスクキューを参照する
- 並列タスクキューを参照する
- タスクの実行詳細を確認する
- 処理中タスクを終了する

直列タスクキューを登録する

1. 「 システム管理 」→「非同期-タスクキュー一覧」をクリックします。
2. 「直列タスクキュー追加」をクリックします。

3. 「直列タスクキュー追加」画面が表示されます。

- 初期状態

  「Active」の場合

  直列タスクキューの先頭からタスクメッセージを取得しビジネスロジックを実行できる状態です。

  「Inactive」の場合

  直列タスクキューの先頭からタスクメッセージを取得できない状態です。

4. 「追加」をクリックします。

5. 直列タスクキューを追加できました。

> **コラム**
> **削除したい場合**
> 対象の直列タスクキューの「×」をクリックします。

直列タスクキューを参照する

1. 「 システム管理 」→「非同期-タスクキュー一覧」をクリックします。
2. 「非同期-タスクキュー一覧」画面が表示されます。

3. 「直列タスクキュー」に登録されているタスクメッセージの「詳細」をクリックします。

4. 「非同期-直列タスク詳細」画面が表示されます。

- 状態

  「Active」の場合

  直列タスクキューの先頭からタスクメッセージを取得しビジネスロジックを実行できる状態です。

  「Inactive」の場合

  直列タスクキューの先頭からタスクメッセージを取得できない状態です。

- 処理中タスク

  処理中のタスクを表示します。処理中のタスクを「終了」、「中断」可能です。

  詳細は「 *処理中タスクを終了する* 」を参照してください。

- 待機中タスク

  待機中のタスクを表示します。各タスクの「×」をクリックすると削除できます。

並列タスクキューを参照する

1. 「 システム管理 」→「非同期-タスクキュー一覧」をクリックします。
2. 「非同期-タスクキュー一覧」画面が表示されます。

3. 「並列タスクキュー」に登録されているタスクメッセージの「詳細」をクリックします。

4. 「非同期-並列タスク詳細」画面が表示されます。

- 状態

  「Active」の場合

  並列タスクキューの先頭からタスクメッセージを取得しビジネスロジックを実行できる状態です。

  「Inactive」の場合

  並列タスクキューの先頭からタスクメッセージを取得できない状態です。

- 処理中タスク

  処理中のタスクを表示します。処理中のタスクを「終了」「中断」可能です。

  詳細は「 *処理中タスクを終了する* 」を参照してください。

- 待機中タスク

  待機中のタスクを表示します。各タスクの「×」をクリックすると削除できます。

タスクの実行詳細を確認する

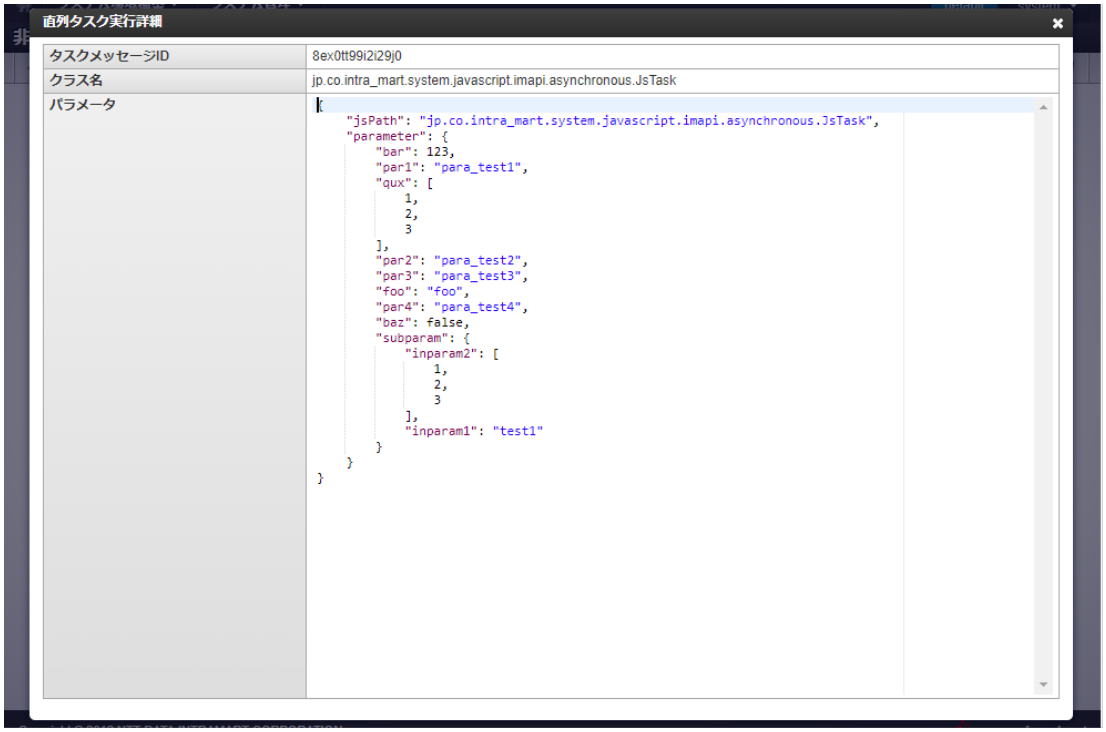
1. 「 システム管理 」→「非同期-タスクキュー一覧」をクリックします。
2. 「非同期-タスクキュー一覧」画面が表示されます。

3. 「直列タスクキュー」に登録されているタスクメッセージの「詳細」をクリックします。

4. 「非同期-直列タスク詳細」画面が表示されます。

5. 待機中タスクの「実行詳細」の「表示」をクリックします。

6. 待機中タスクの「実行詳細」画面が表示されます。



処理中タスクを終了する

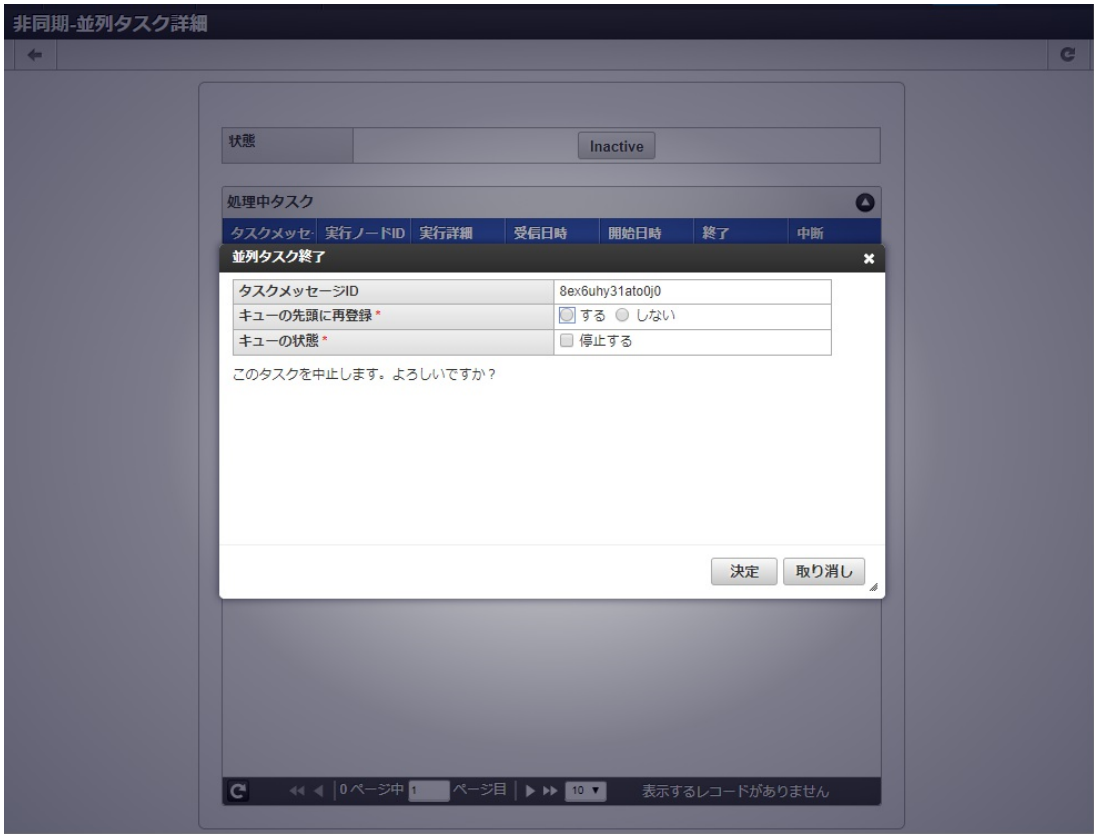
1. 「 システム管理 」→「非同期-タスクキュー一覧」をクリックします。
2. 「非同期-タスクキュー一覧」画面が表示されます。

3. 「並列タスクキュー」に登録されているタスクメッセージの「詳細」をクリックします。

4. 「非同期-並列タスク詳細」画面が表示されます。

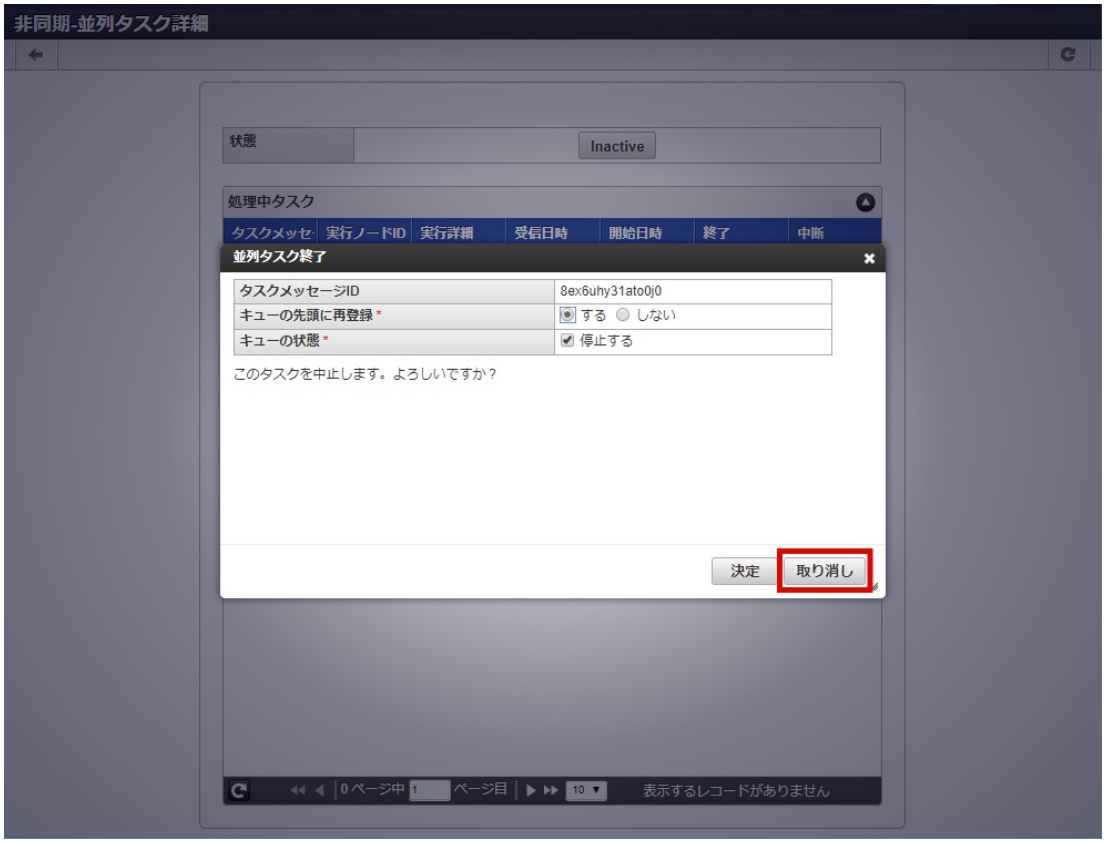
5. 処理中タスクの「終了」をクリックします。

6. 「並列タスク終了」画面が表示されます。



- キューの先頭に再登録
  「する」を選択した場合、キューの先頭に登録されます。
  「しない」を選択した場合、キューには登録されず破棄されます。
- キューの状態
  「現状のまま」を選択した場合、「Active」の状態でキューに登録されます。
  「停止する」を選択した場合、「Inactive」の状態でキューに登録されます。

7. 「決定」をクリックします。



8. タスクを終了できました。

コラム

タスクを「中断」したい場合

対象のタスクメッセージの「中断」をクリックします。

> **注意**
>
> 処理中タスクを終了・中断できるかどうかは実行中の非同期タスクの実装に依存します。
> 終了・中断の処理を実装していないタスクに対して、終了・中断を行ってもそのまま処理は実行されます。

シェアードデータベース設定

シェアードデータベースは 1 つのテナントで複数のデータベースを使用する場合、または WARファイルによる複数テナント や バーチャルテナントによる複数テナント で 1 つのデータベースを使用する場合に利用できます。

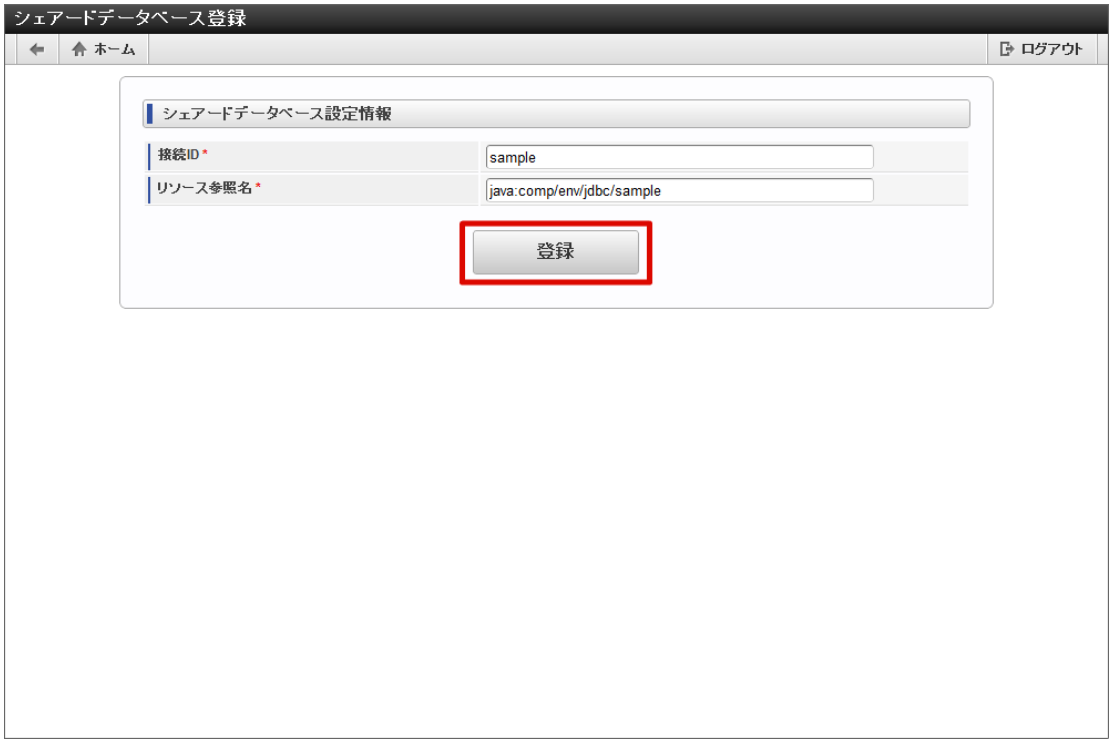
シェアードデータベースを登録する

1. 「 システム管理 」→「シェアードデータベース設定」をクリックします。
2. 「新規登録」をクリックします。

3. 「シェアードデータベース登録」画面が表示されます。

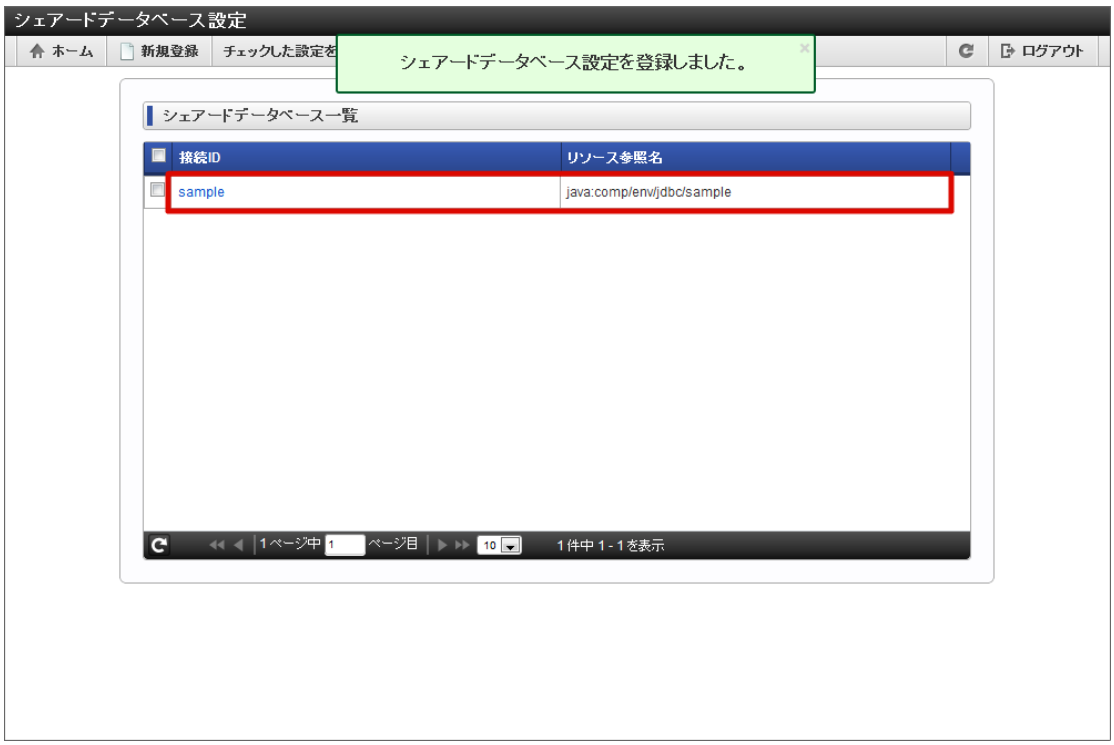
- 接続ID
  接続IDを入力します。（シェアードデータベースでユニークなID）
- リソース参照名
  使用するデータソースのJNDI名を入力します。

4. 「登録」をクリックします。



5. 「決定」をクリックします。

6. シェアードデータベースを登録することができました。



コラム

「編集」する場合

対象の「接続ID」をクリックします。

コラム

「削除」する場合

1. 「シェアードデータベース一覧」から削除したいシェアードデータベースにチェックを入れます。
2. 「チェックした設定を削除」をクリックします。

> **注意**
>
> 設定内容は、システムストレージに保存されます。
>
> システムストレージにデータベース設定が存在する場合、その設定内容が反映されます。
> その為、WARを再作成する際にデータベース設定を変更しても反映されない可能性があります。

ログインセッション一覧

操作中のテナントのログイン状況を参照・無効化することができます。

二重ログイン防止機能

二重ログイン防止機能とは、既にログイン中のユーザと同じユーザで別の環境（ブラウザ）からログインできないようにするための機能です。

一般ユーザのログイン時にログインセッション情報がデータベースに登録されます。ログイン中、その情報は保持されています。
別の環境より同じユーザでログインしようとした際に、ログインセッション情報が存在する場合はログインできません。

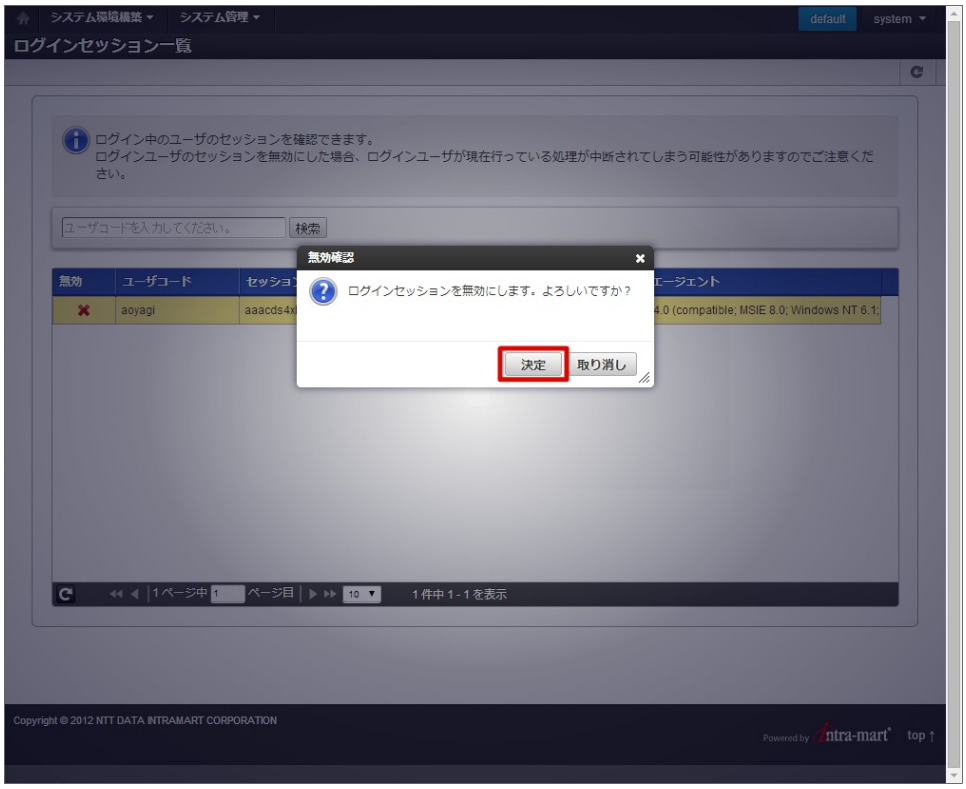
二重ログインが検出されると認証失敗となり、以下のような認証エラー画面が表示されます。

セッションの無効化の操作

システム管理者は、操作中のテナントのテナント管理者および一般ユーザのログインセッションを無効化することができます。
ログインセッションを無効化すると、ログイン中のユーザは強制的にログアウトされます。このため、行っていた処理も中断されてセッションタイムアウトの画面が表示されます。

1. 「システム管理」→「ログインセッション一覧」をクリックします。
2. 一覧よりログインセッションを無効化したいユーザの無効アイコン「×」をクリックします。

3. 確認ダイアログの「決定」をクリックします。



4. ログインセッションを無効化できました。

一般ユーザ管理

詳細は「IM-共通マスタ 管理者操作ガイド」-「ユーザ」を参照してください。

ポートレット管理

詳細は「ポータル 管理者操作ガイド」-「標準ポートレットを初期化する」を参照してください。

ポータル設定

詳細は「ポータル 管理者操作ガイド」-「ポータル設定を変更する」を参照してください。

クロスオリジンリソース共有設定

クロスオリジンリソース共有設定を一覧表示します。
クロスオリジンリソース共有設定の新規登録、編集、削除、インポート、エクスポートなどの操作が行えます。

コラム

クロスオリジンリソース共有の詳細については、以下のドキュメントを参照ください。

- https://developer.mozilla.org/ja/docs/Web/HTTP/CORS （日本語）
- https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS （English）
- https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Access_control_CORS （中文）

注意

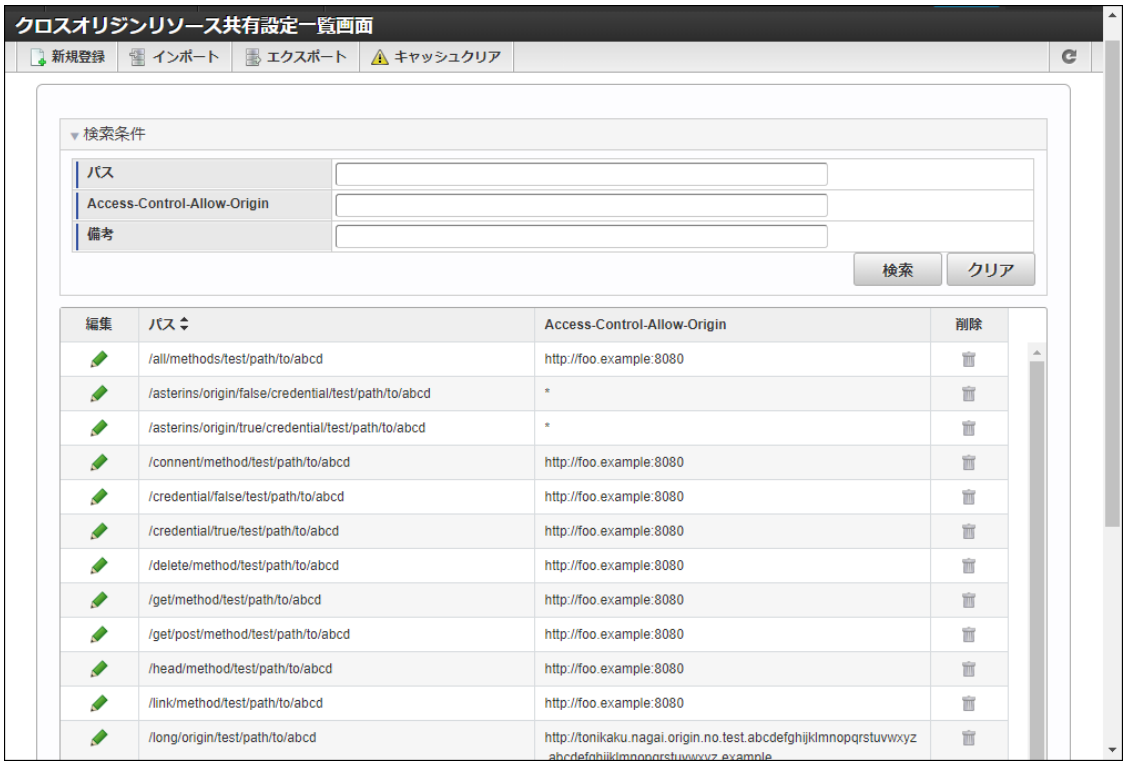
クロスオリジンリソース共有設定は、intra-mart Accel Platform 2019 Summer(Waltz) 以降で利用できます。

目次

- クロスオリジンリソース共有設定の一覧を確認する
- クロスオリジンリソース共有設定を登録する
- クロスオリジンリソース共有設定をインポートする
- クロスオリジンリソース共有設定をエクスポートする
- クロスオリジンリソース共有設定のキャッシュ情報を削除する

クロスオリジンリソース共有設定の一覧を確認する

1. 「システム管理」→「クロスオリジンリソース共有設定」をクリックします。



ツールバー項目の説明

項目	説明
新規登録	クリックすることで、クロスオリジンリソース共有設定の新規登録を行います。
インポート	クリックすることで、クロスオリジンリソース共有設定のインポートを行います。
エクスポート	クリックすることで、クロスオリジンリソース共有設定のエクスポートを行います。
キャッシュクリア	クリックすることで、クロスオリジンリソース共有設定のキャッシュをクリアします。
最新情報	クリックすることで、クロスオリジンリソース共有設定の最新情報を取得します。

検索エリアの説明

項目	説明
パス	「パス」での部分一致の絞り込み条件です。 入力しない場合は、すべてが検索対象です。
Access-Control-Allow-Origin	「Access-Control-Allow-Origin」での部分一致の絞り込み条件です。 入力しない場合は、すべてが検索対象です。
備考	「備考」での絞り込み条件です。 入力しない場合は、すべてが検索対象です。
検索ボタン	「パス」と「Access-Control-Allow-Origin」と「備考」の３項目によって絞り込み検索を行います。 ３項目を AND 条件で検索します。

項目	説明
クリアボタン	「パス」と「Access-Control-Allow-Origin」と「備考」の３項目に入力された値をクリアします。

リスト項目の説明

リスト項目	説明
編集	アイコンをクリックすることで、クロスオリジンリソース共有設定の編集を行います。
パス	パスを表示します。
Access-Control-Allow-Origin	Access-Control-Allow-Origin を表示します。
削除	アイコンをクリックすることで、クロスオリジンリソース共有設定の削除を行います。

クロスオリジンリソース共有設定を登録する

1. 「システム管理」→「クロスオリジンリソース共有設定」をクリックします。
2. 「新規登録」をクリックします。

3. 「クロスオリジンリソース共有設定 - 新規登録」画面が表示されます。

- パス
  設定を行うリソースのパスを入力します。

  > **コラム**
  >
  > PathVariables を利用したリソースに対する設定を行いたい場合は、リソースのパス設定と同様に、**{xxxx}** 形式で指定してください。
  > 例えば、設定を行うリソースのパスが「/app/bar/{id}」だった場合は、同様に「/app/bar/{id}」と指定することで設定を行うことが可能です。
  >
  > PathVariables については、「スクリプト開発モデル プログラミングガイド - PathVariables」を参照してください。

- Access-Control-Allow-Origin
  クロスドメインリソース共有を許可するアクセス元 Origin を入力します。

  > **コラム**
  >
  > 国際化ドメイン名を使用する場合は、 Punycode 変換されたドメイン名を入力してください。
  > ただし、 Internet Explorer をお使いの場合は国際化ドメイン名を使用することはできません。

- Access-Control-Allow-Methods
  リソースへアクセスするときに使用できるメソッドを選択します。
- Access-Control-Allow-Headers
  リソースへアクセスするときに使用できるリクエストヘッダを入力します

  > **コラム**
  >
  > OAuth や Basic 認証を使用する場合は、 Authorization ヘッダを設定してください。

- Access-Control-Expose-Headers
  レスポンスヘッダのうち、クライアントがアクセスできるヘッダを入力します。
- Access-Control-Allow-Credentials
  リソースへアクセスするときに資格情報を使用できるかどうかを選択します。
- Access-Control-Max-Age
  プリフライトリクエストの結果をキャッシュしてよい期間を入力します。
- 備考
  必要に応じて備考を入力します。

コラム

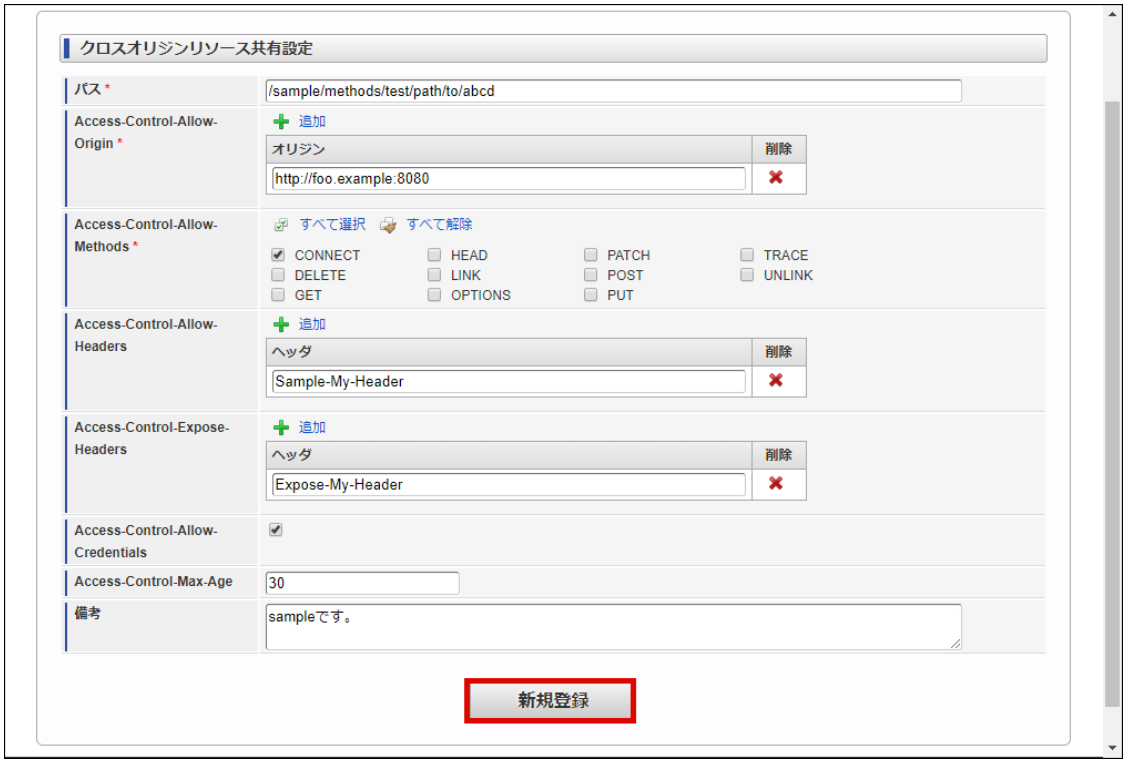
各項目の詳細については、以下のドキュメントを参照ください。

- Access-Control-Allow-Origin
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Allow-Origin （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Origin （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Allow-Origin （中文）
- Access-Control-Allow-Methods
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Allow-Methods （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Methods （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Allow-Methods （中文）
- Access-Control-Allow-Headers
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Allow-Headers （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Headers （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Allow-Headers （中文）
- Access-Control-Expose-Headers
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Expose-Headers （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Expose-Headers （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Expose-Headers （中文）
- Access-Control-Allow-Credentials
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Allow-Credentials （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Credentials （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Allow-Credentials （中文）
- Access-Control-Max-Age
  https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Access-Control-Max-Age （日本語）
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Max-Age （English）
  https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Access-Control-Max-Age （中文）

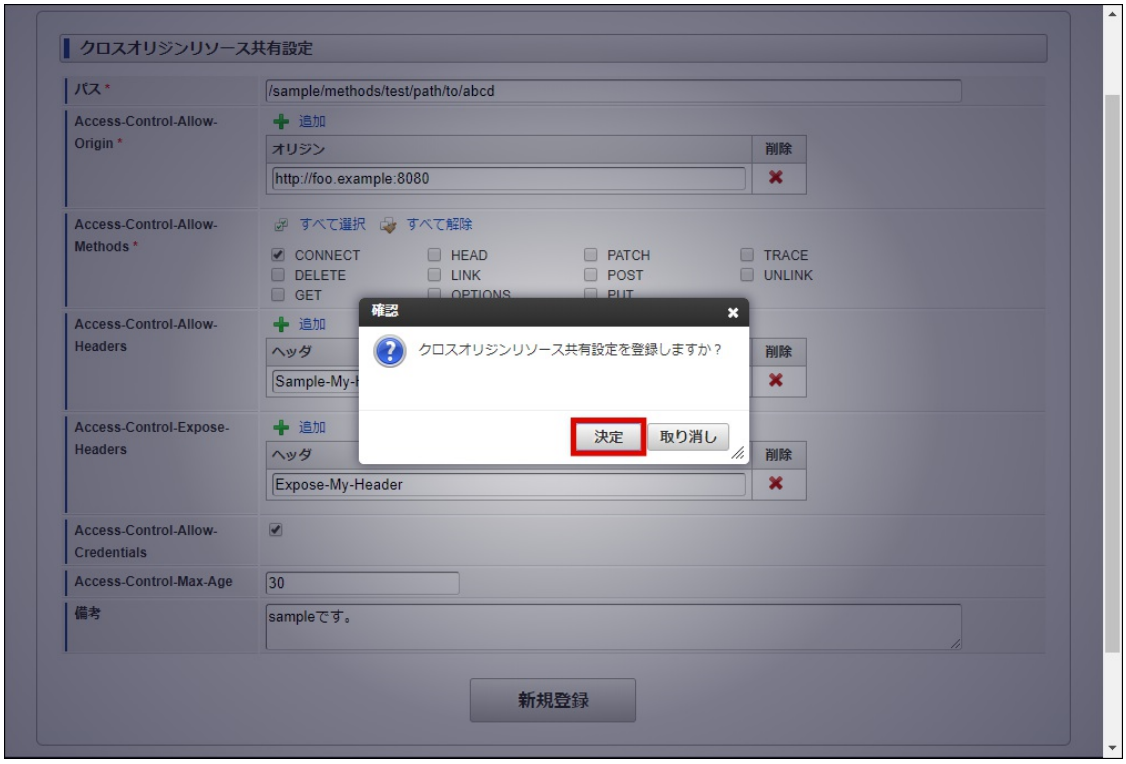
コラム

IM-LogicDesigner のロジックフロールーティング情報で、レスポンスヘッダに Access-Control-Allow-Origin が指定されている場合、 IM-LogicDesigner の設定が優先されます。

4. 「新規登録」をクリックします。



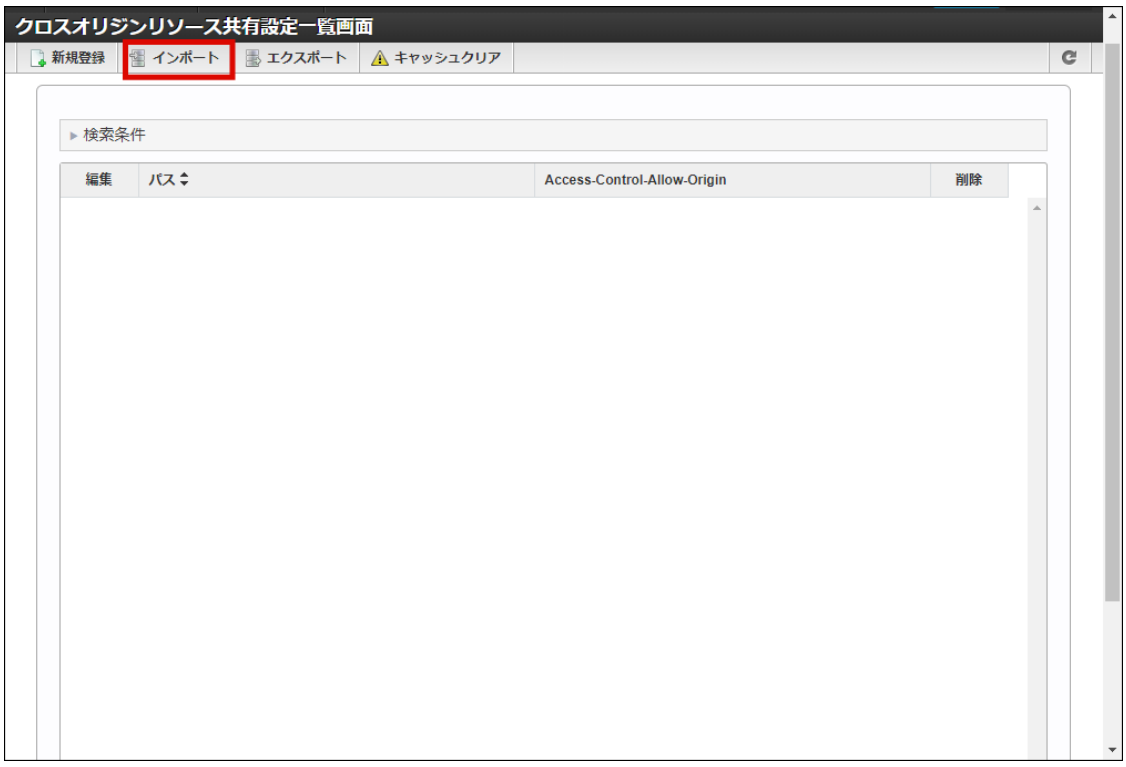
5. 「決定」をクリックします。



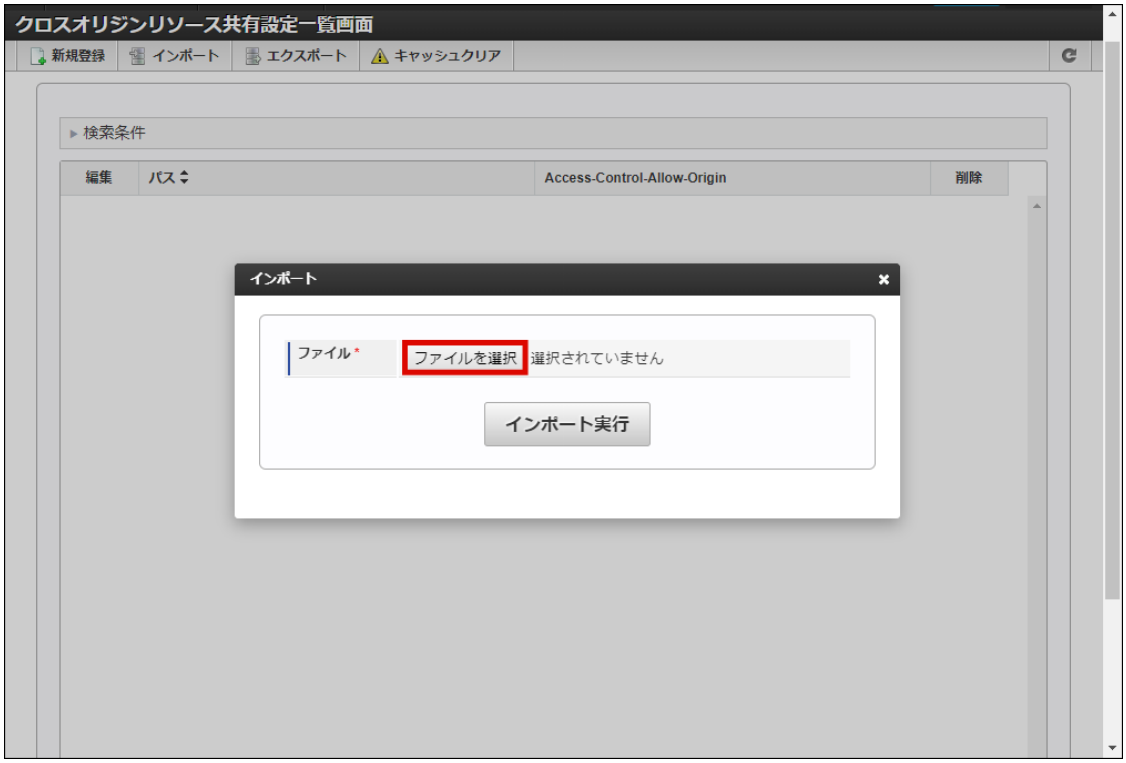
6. クロスオリジンリソース共有設定を登録できました。

クロスオリジンリソース共有設定をインポートする

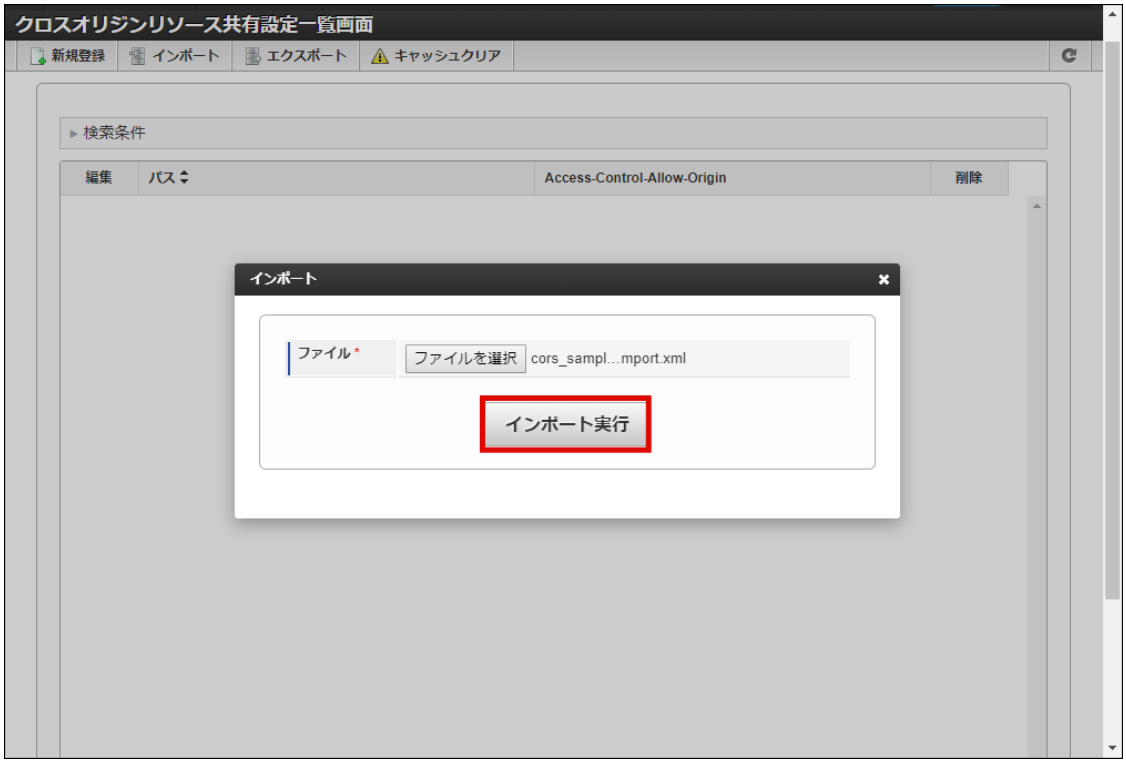
1. 「システム管理」→「クロスオリジンリソース共有設定」をクリックします。
2. 「インポート」をクリックします。



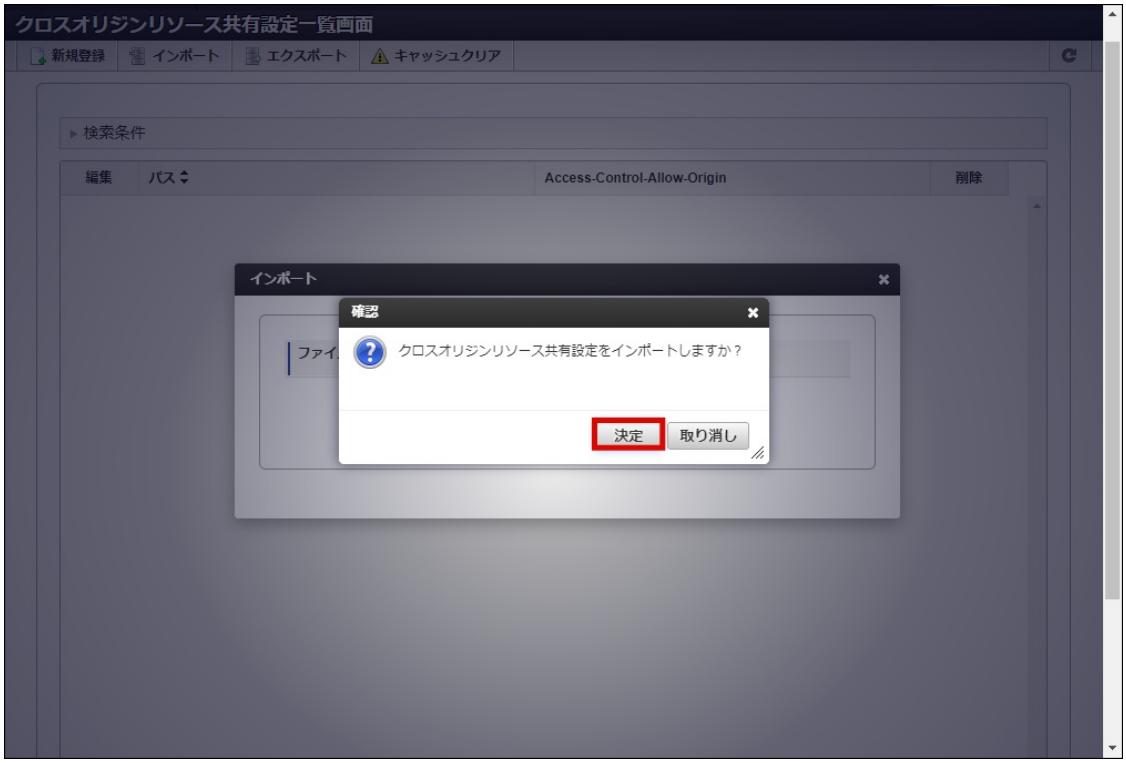
3. 「ファイルを選択」でインポートファイルを選択します。



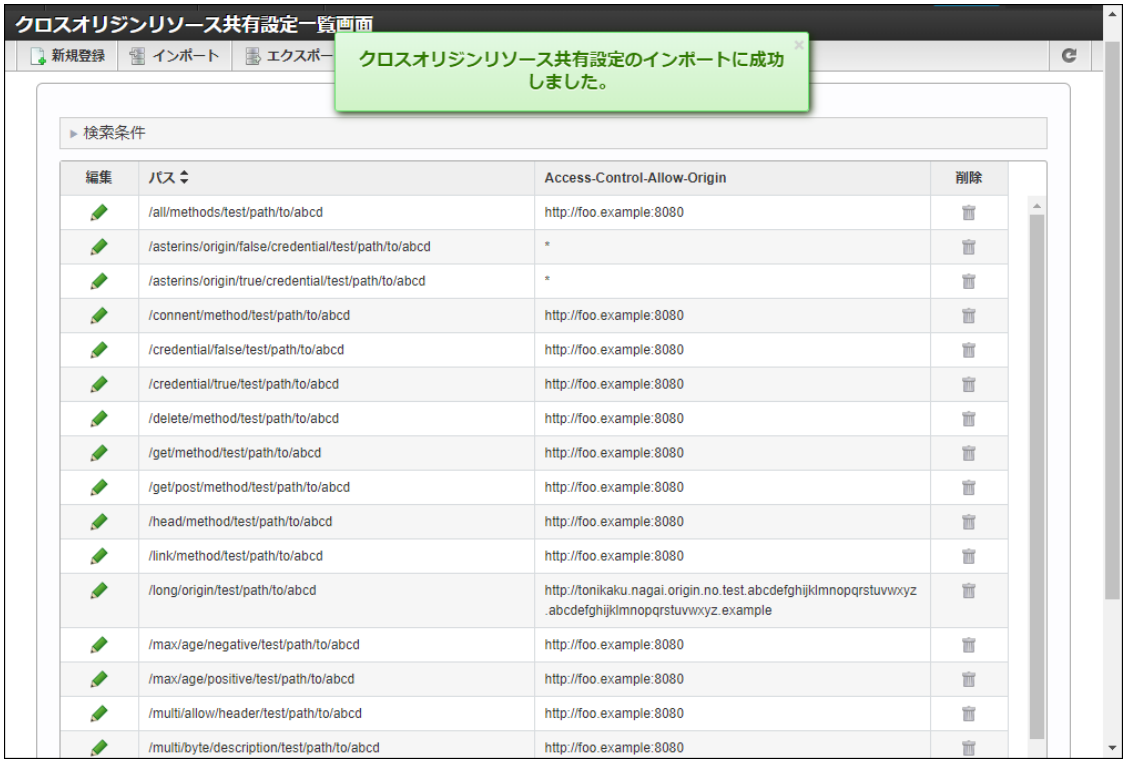
4. 「インポート実行」をクリックします。



5. 「決定」をクリックします。

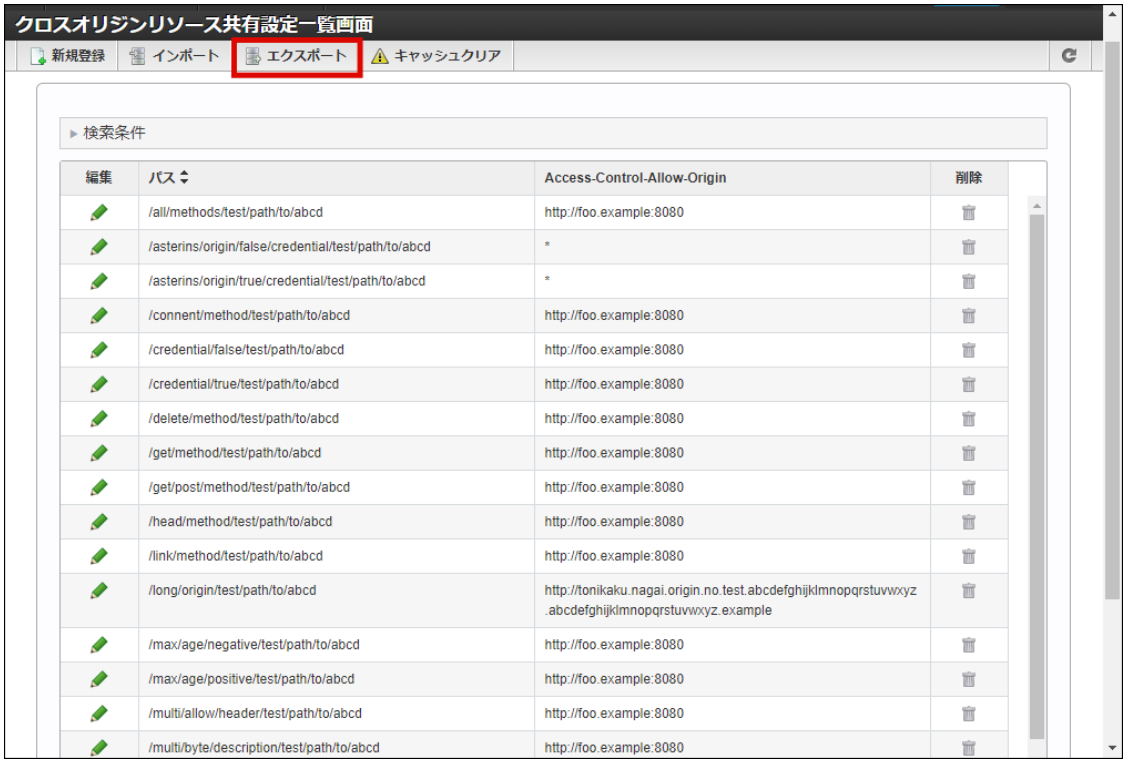


6. クロスオリジンリソース共有設定をインポートできました。

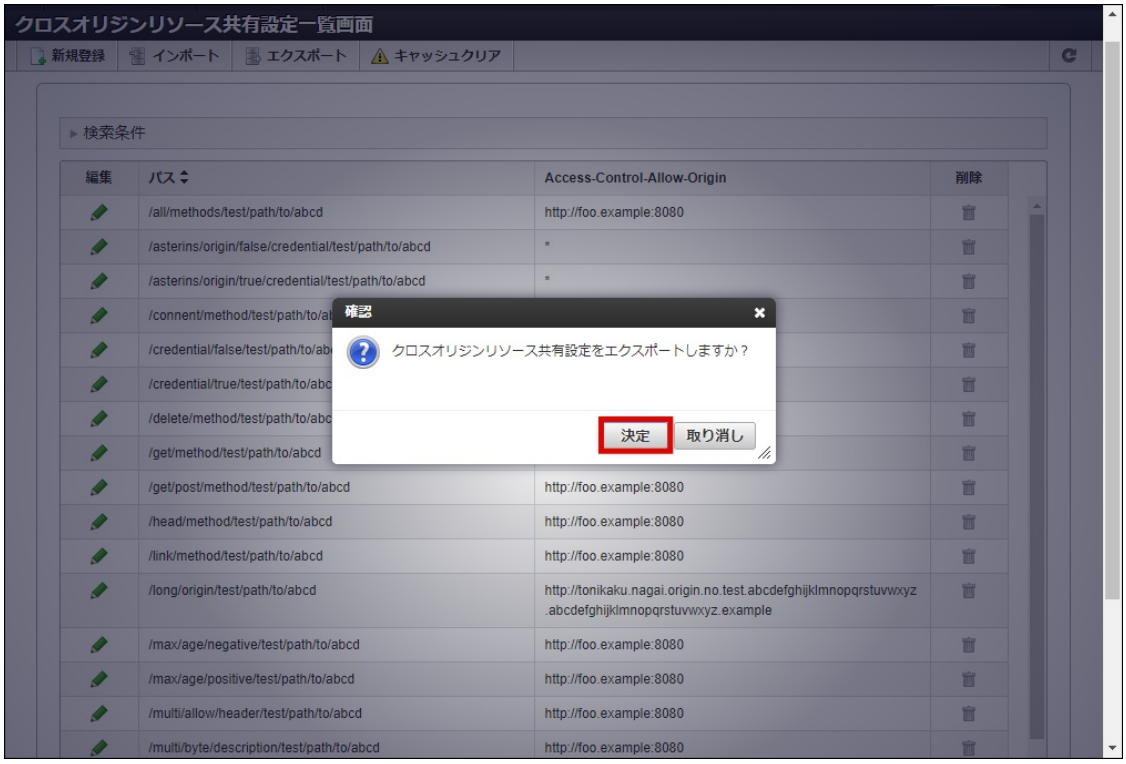


クロスオリジンリソース共有設定をエクスポートする

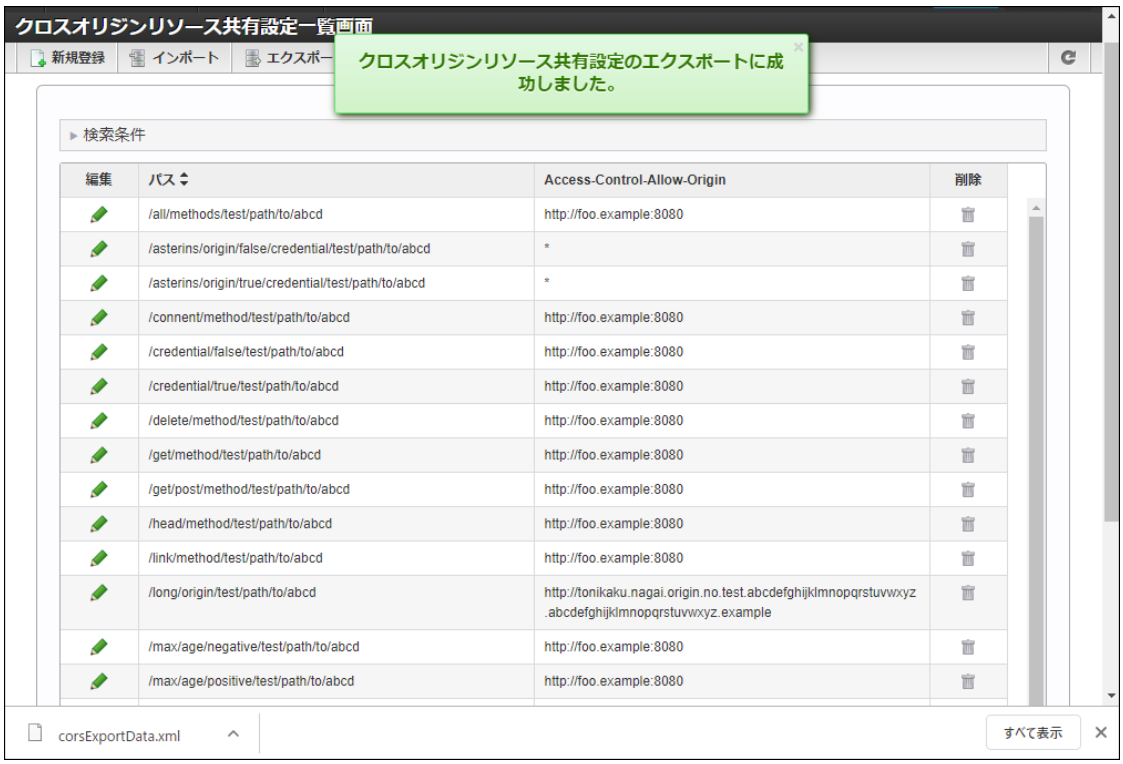
1. 「システム管理」→「クロスオリジンリソース共有設定」をクリックします。
2. 「エクスポート」をクリックします。



3. 「決定」をクリックします。



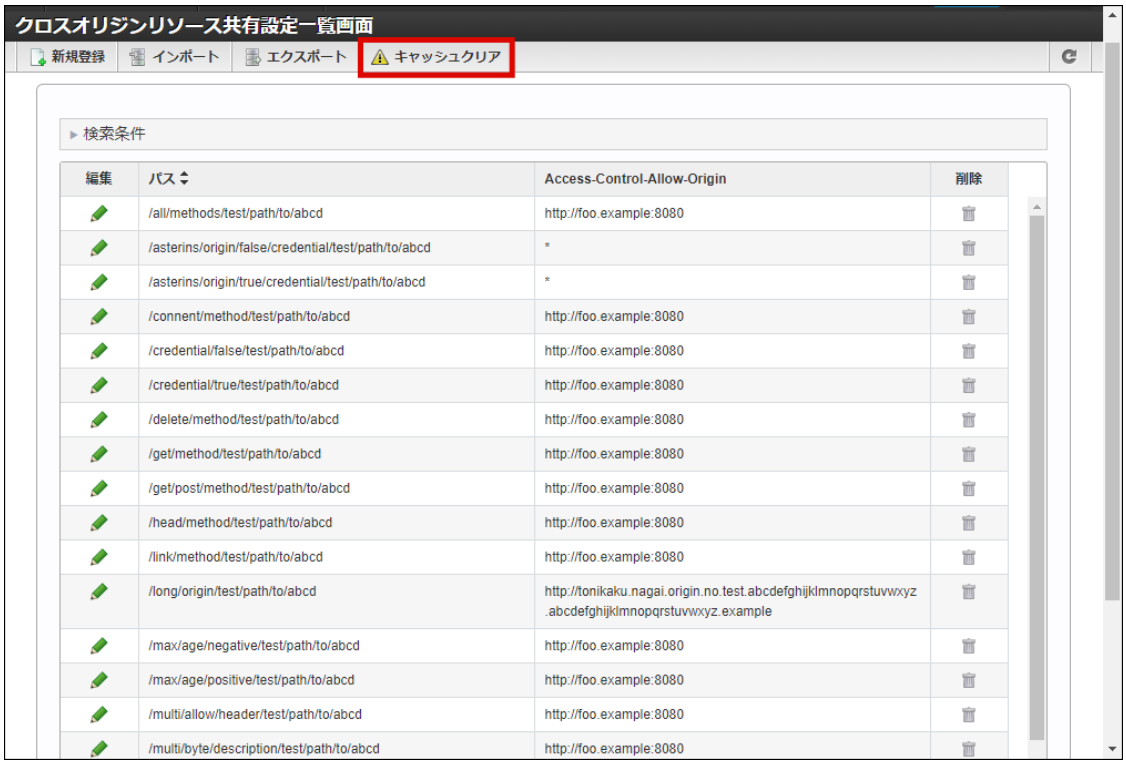
4. クロスオリジンリソース共有設定をエクスポートできました。



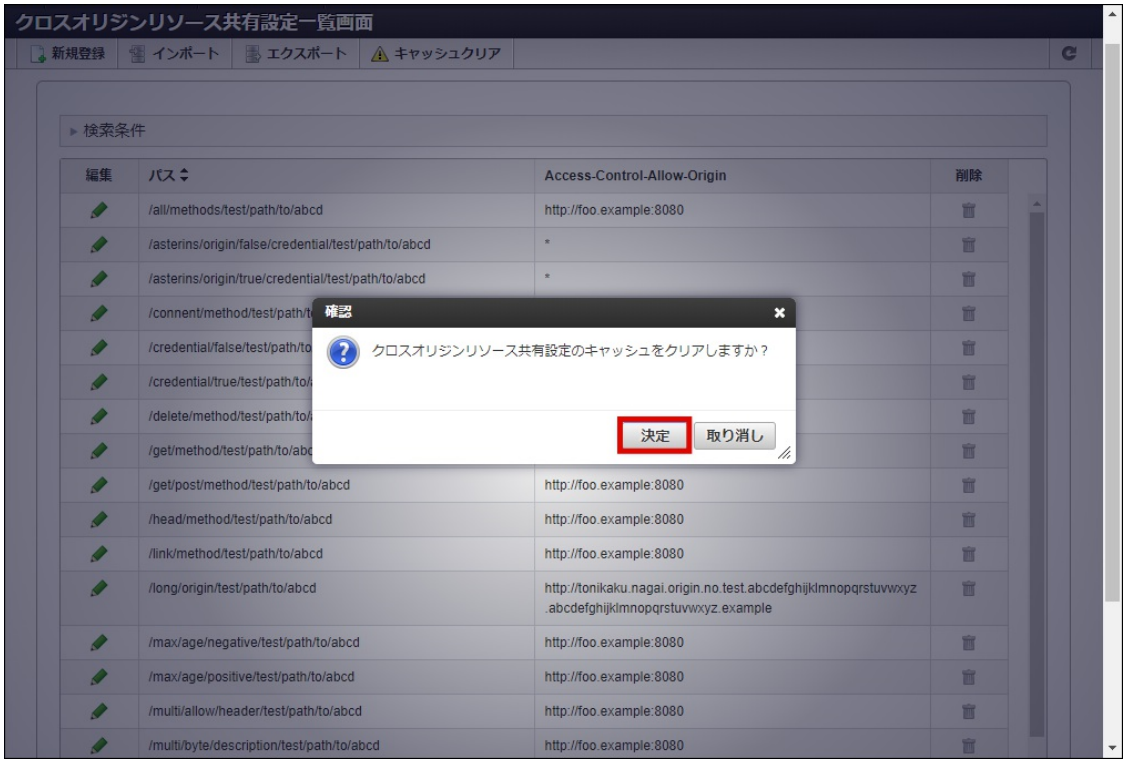
クロスオリジンリソース共有設定のキャッシュ情報を削除する

クロスオリジンリソース共有設定は、クロスオリジンリクエストを処理する度に参照されるため、高速化を目的として設定した内容がキャッシュされています。
設定通りにクロスオリジンリクエストが処理されない場合は、キャッシュ情報を削除してください。

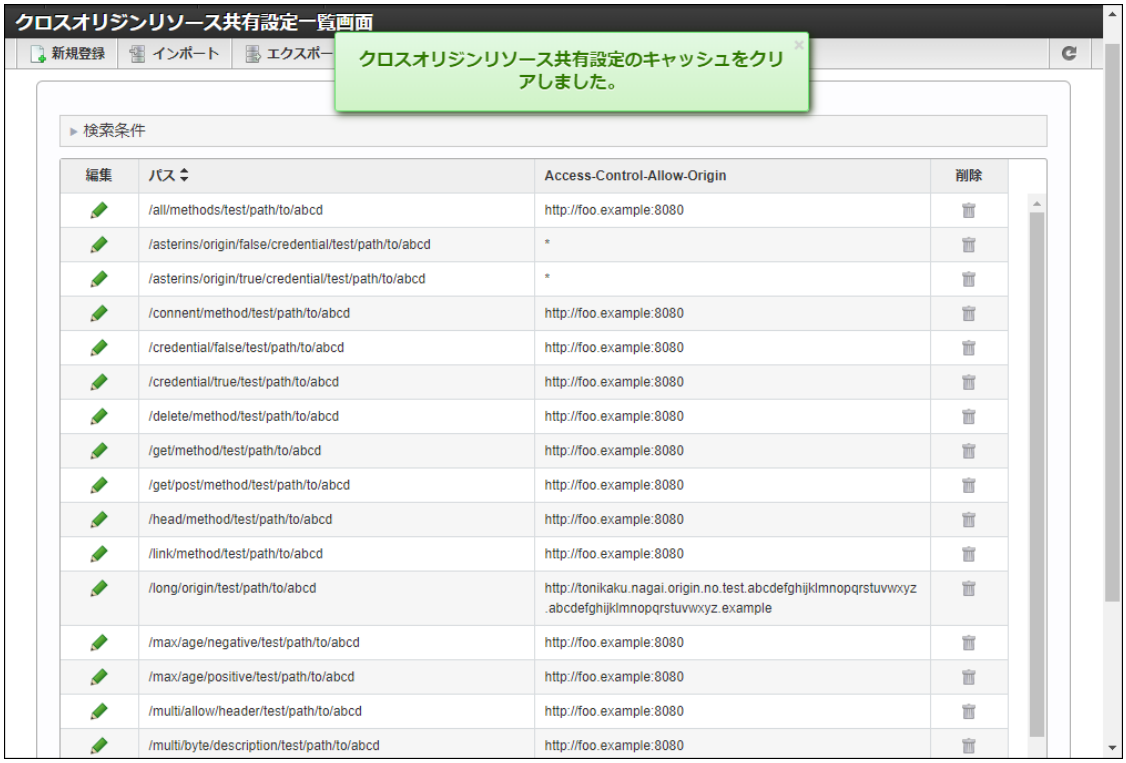
1. 「システム管理」→「クロスオリジンリソース共有設定」をクリックします。
2. 「キャッシュクリア」をクリックします。



3. 「決定」をクリックします。



4. クロスオリジンリソース共有設定のキャッシュが削除されます。



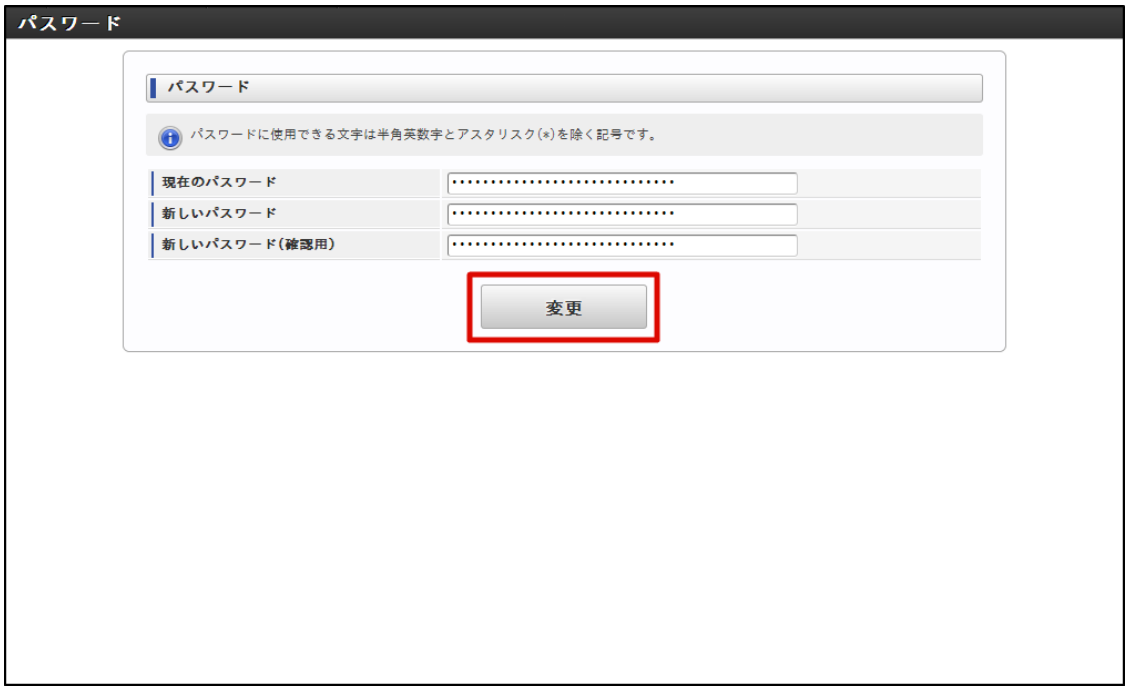
システム管理者設定

ここではシステム管理者の設定についてを説明します。

パスワードを変更する

ログイン中のシステム管理者のパスワードを変更します。

1. 画面右上のユーティリティメニュー →「個人設定」→「パスワード」をクリックします。
2. 現在のパスワード、新しいパスワードと新しいパスワード（確認用）を入力します。
3. 「変更」をクリックします。

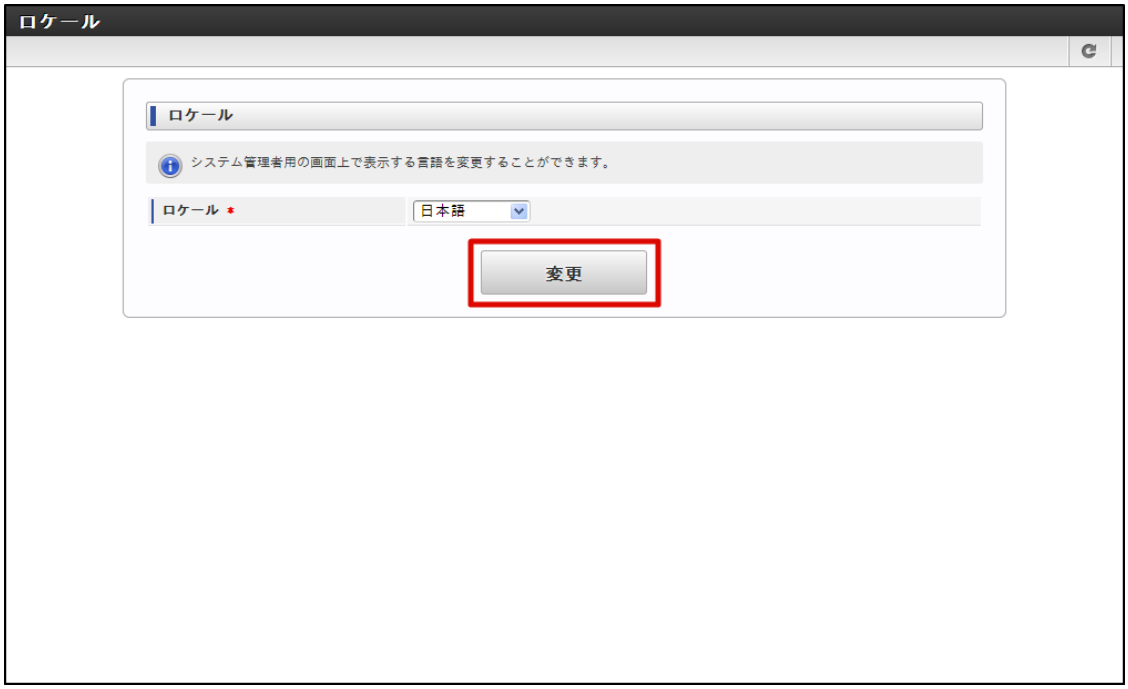


4. システム管理者のパスワードが変更されます。

ロケールを変更する

ログイン中のシステム管理者のロケールを変更します。

1. 画面右上のユーティリティメニュー →「個人設定」→「ロケール」をクリックします。
2. ロケールから変更したい表示のロケールを選択します。
3. 「変更」をクリックします。



4. システム管理者のロケールが変更されます。

> **コラム**
>
> intra-mart Accel Platform 2013 Winter 以前のバージョンから 2014 Spring 以降へアップデートした場合、ロケールは未選択状態です。
>
> ロケールが未選択状態の場合、システム管理者画面のロケールはブラウザのロケール設定によって決定されます。
> しかし、ブラウザによっては画面表示や処理のタイミングでロケールが適切に解決されないことがあります。
> そのため intra-mart Accel Platform 2014 Spring 以降では、ロケールを明示的に設定することを推奨しています。
>
> ロケールを選択して変更後、再度未選択状態に戻すことはできません。

多要素認証を設定する

多要素認証とは、本人であると特定するために複数の要素をユーザに要求する認証です。
多要素認証を利用すると、ログイン時に通常のパスワードの他に、確認コードを入力することがユーザに求められます。
これにより、もしパスワードが盗まれてしまったとしてもアカウントが不正に利用されることを防げます。

ここでは、システム管理者が多要素認証を利用する方法を紹介します。

項目

- 多要素認証を有効化する
- 多要素認証を無効化する
- バックアップコードを作成する
- 信頼済みブラウザ情報を削除する
- 期限切れブラウザ情報を削除する

多要素認証を有効化する

1. 「ユーティリティメニュー」→「システム管理者設定」→「多要素認証設定」の順にクリックします。
2. 「多要素認証設定」画面が表示されます。

3. Step 1 のメッセージに従って、認証アプリを取得して「次へ」をクリックします。

4. Step 2 のメッセージに従って、認証アプリでバーコードをスキャンして「次へ」をクリックします。

5. Step 3 のメッセージに従って、確認コードを入力して「有効化」をクリックします。

6. 多要素認証を有効化できました。

多要素認証を無効化する

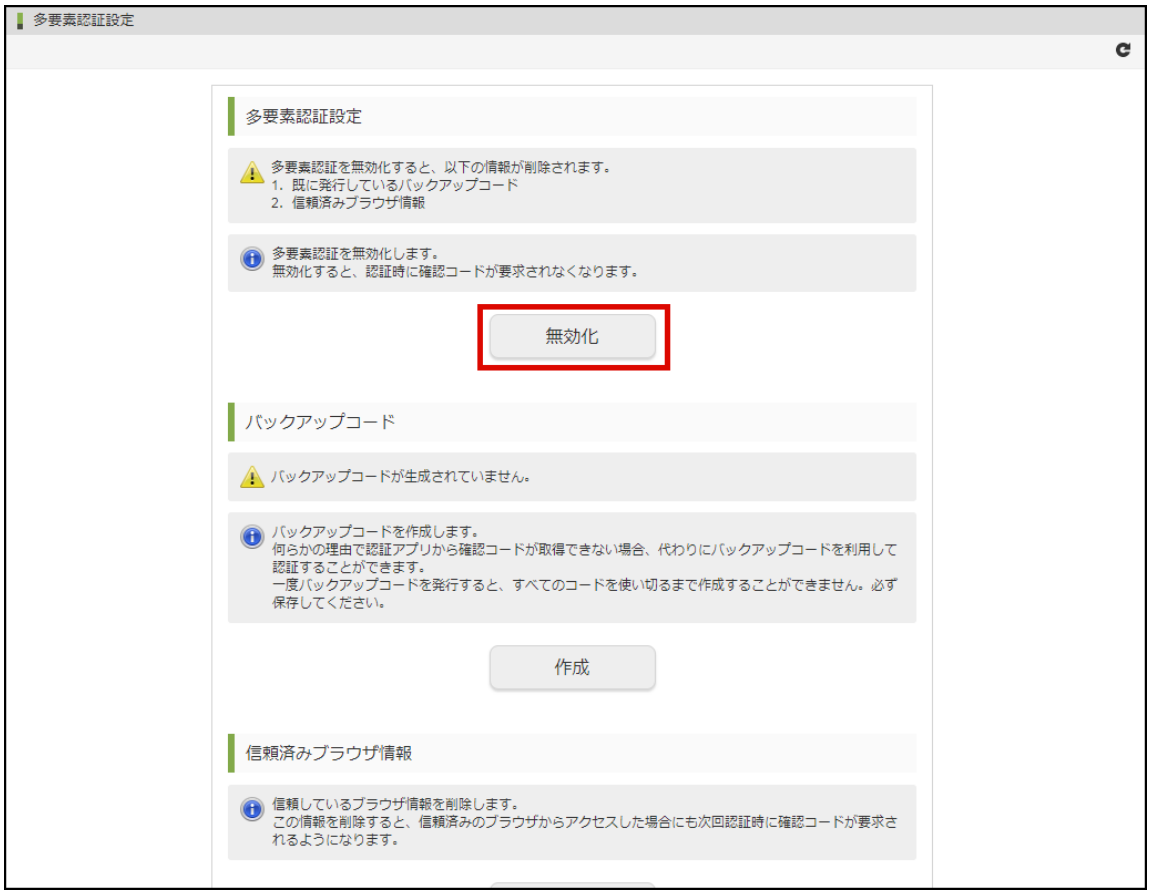
注意

多要素認証を無効化すると、以下の情報が削除されます。

1. 既に発行しているバックアップコード
2. 信頼済みブラウザ情報

1. 「ユーティリティメニュー」→「システム管理者設定」→「多要素認証設定」の順にクリックします。
2. 「多要素認証設定」画面が表示されます。

3. 「無効化」をクリックします。



4. 多要素認証を無効化できました。

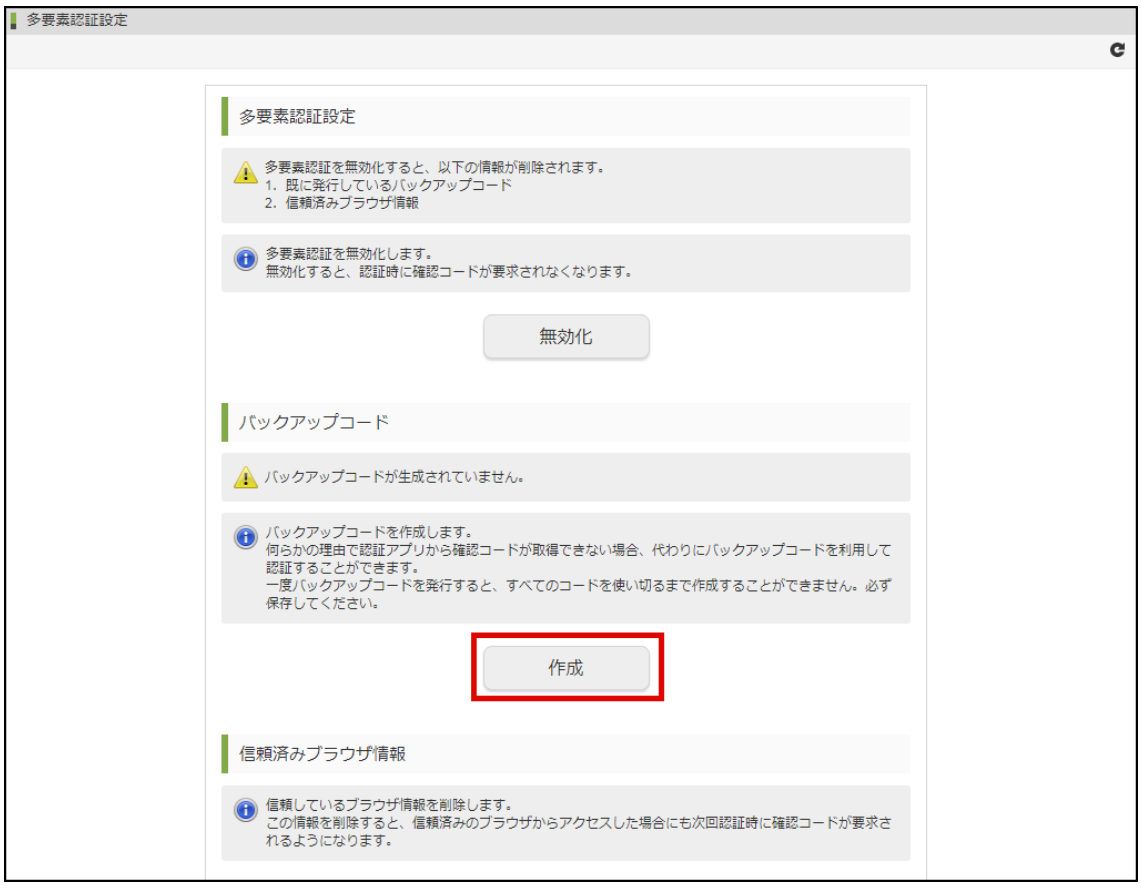
バックアップコードを作成する

> **注意**
>
> 一度バックアップコードを発行すると、すべてのコードを使い終わるまで再作成することができません。
> バックアップコードはスクリーンショットを撮ったりメモに残したりして、必ず保存してください。

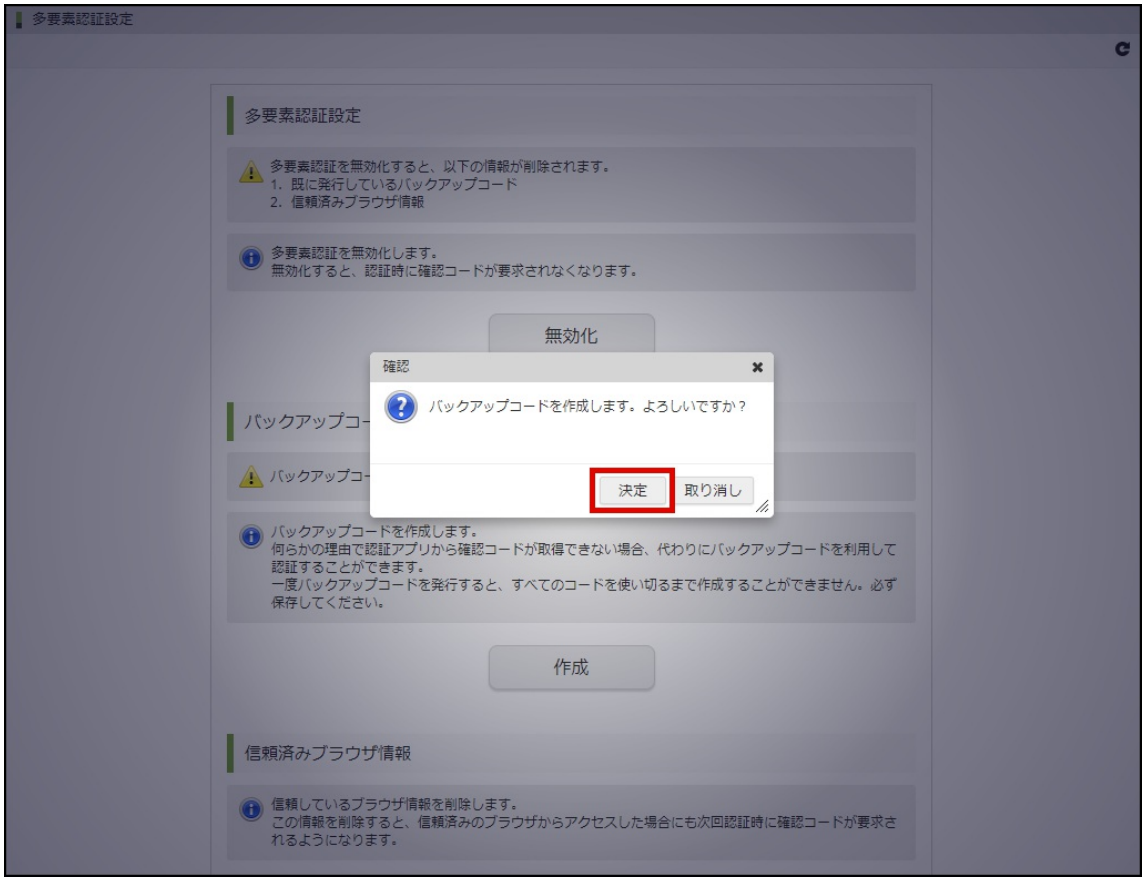
> **注意**
>
> バックアップコードはパスワードと同等の価値を持つ大切なコードです。
> 保存したスクリーンショットやメモは安全に保管しておくことをおすすめします。

1. 「ユーティリティメニュー」→「システム管理者設定」→「多要素認証設定」の順にクリックします。
2. 「多要素認証設定」画面が表示されます。

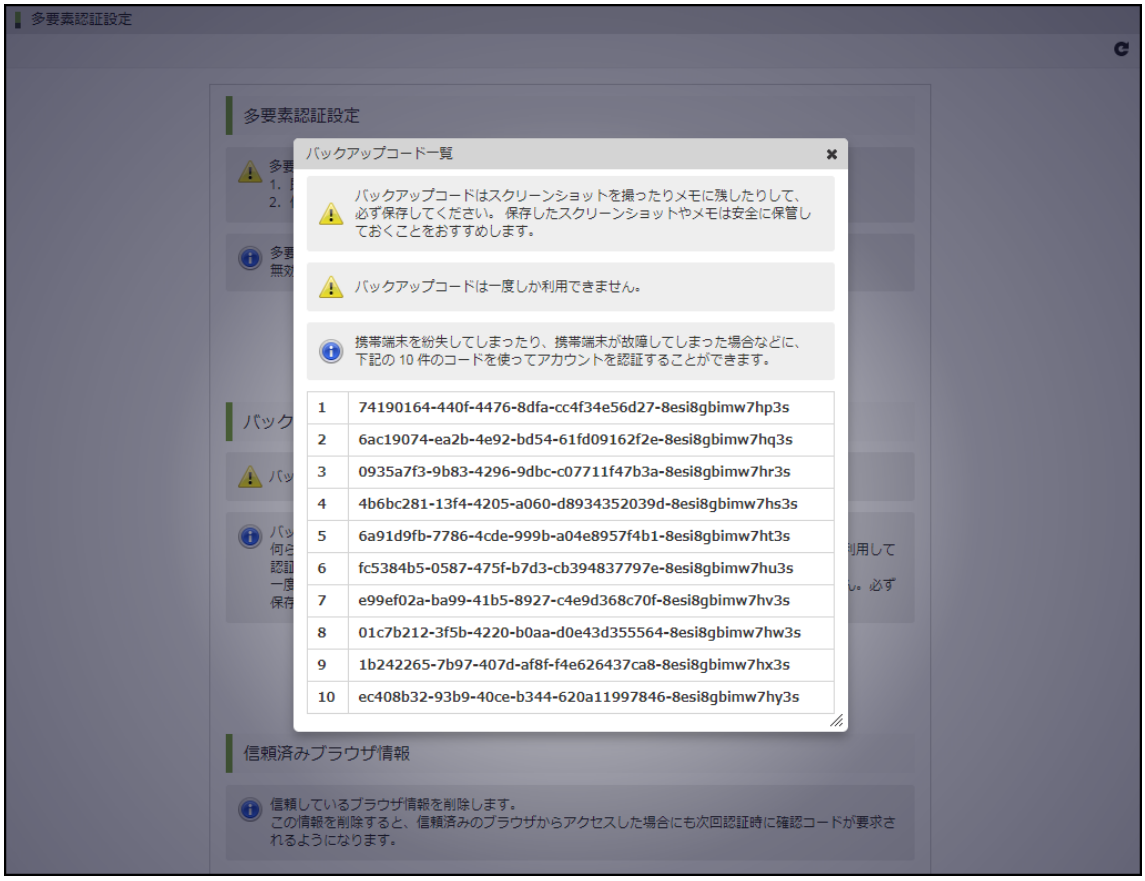
3. 「作成」をクリックします。



4. 「決定」をクリックします。



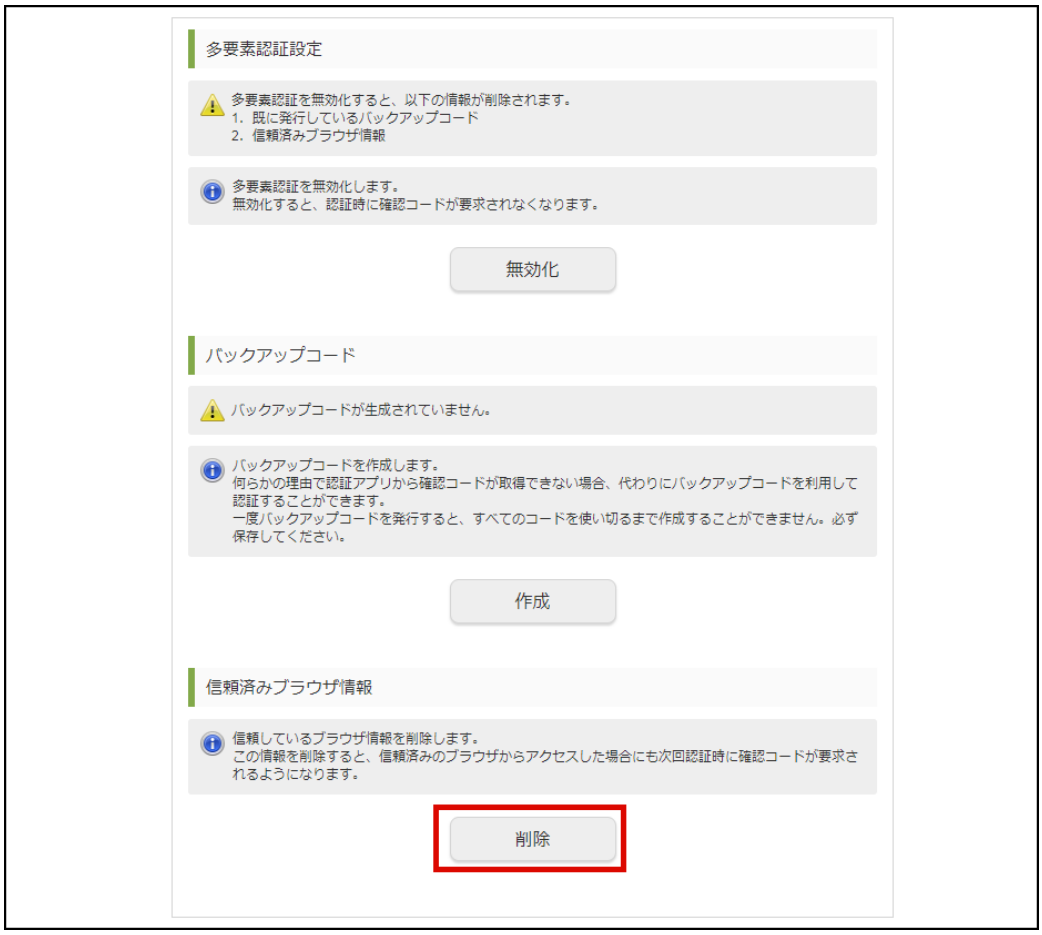
5. バックアップコードが作成されました。



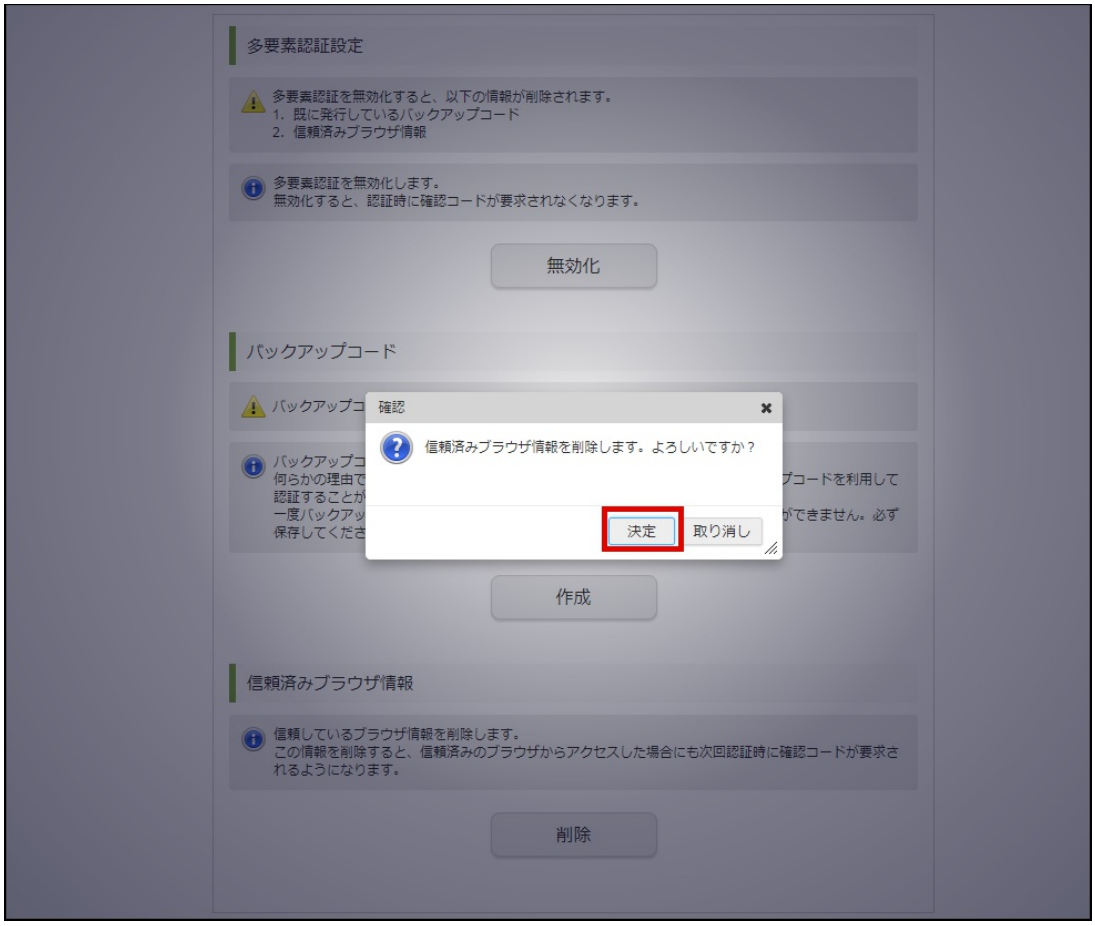
信頼済みブラウザ情報を削除する

1. 「ユーティリティメニュー」→「システム管理者設定」→「多要素認証設定」の順にクリックします。
2. 「多要素認証設定」画面が表示されます。

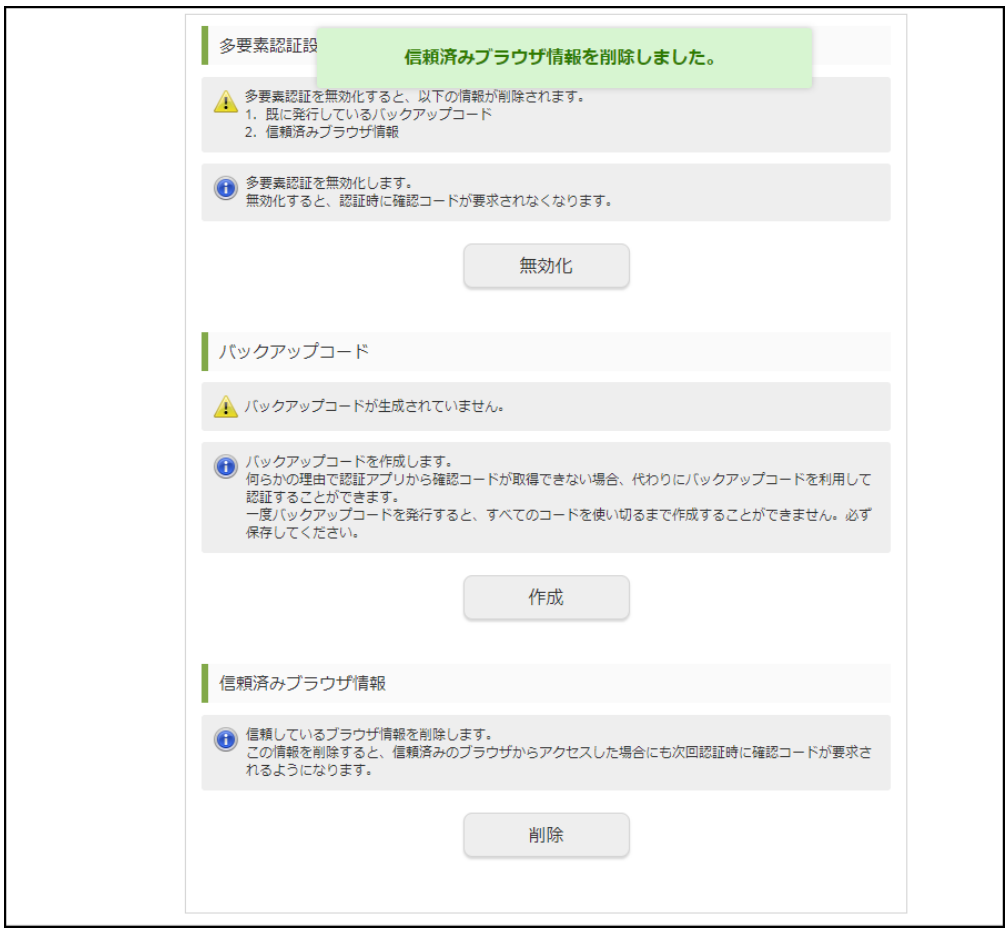
3. 「削除」をクリックします。



4. 「決定」をクリックします。



5. 信頼済みブラウザ情報が削除されました。

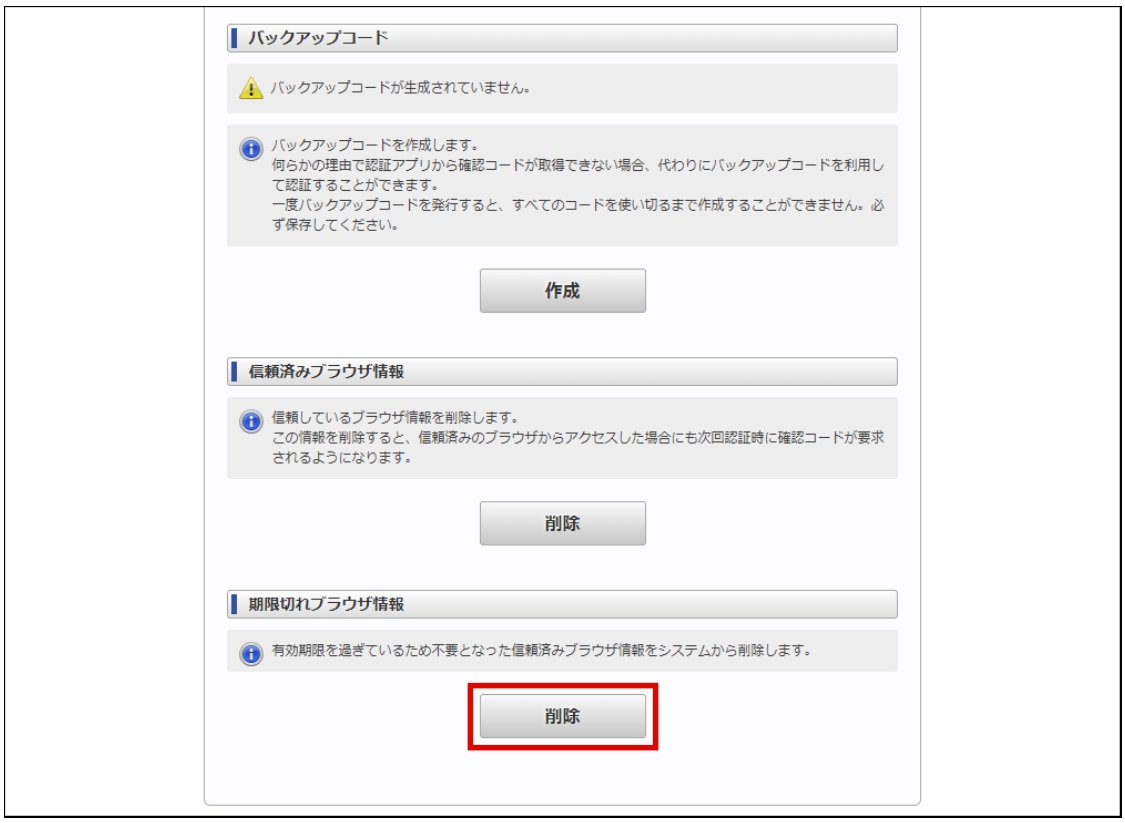


期限切れブラウザ情報を削除する

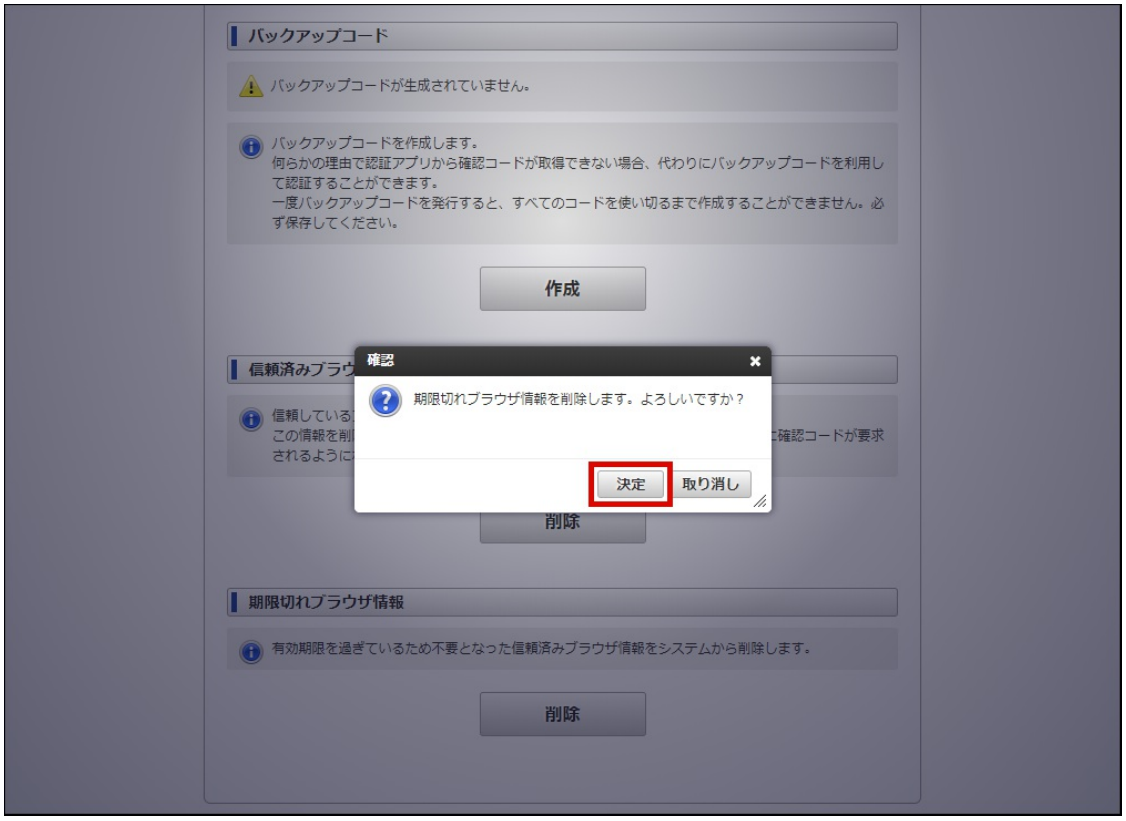
1. 「ユーティリティメニュー」→「システム管理者設定」→「多要素認証設定」の順にクリックします。

2. 「多要素認証設定」画面が表示されます。

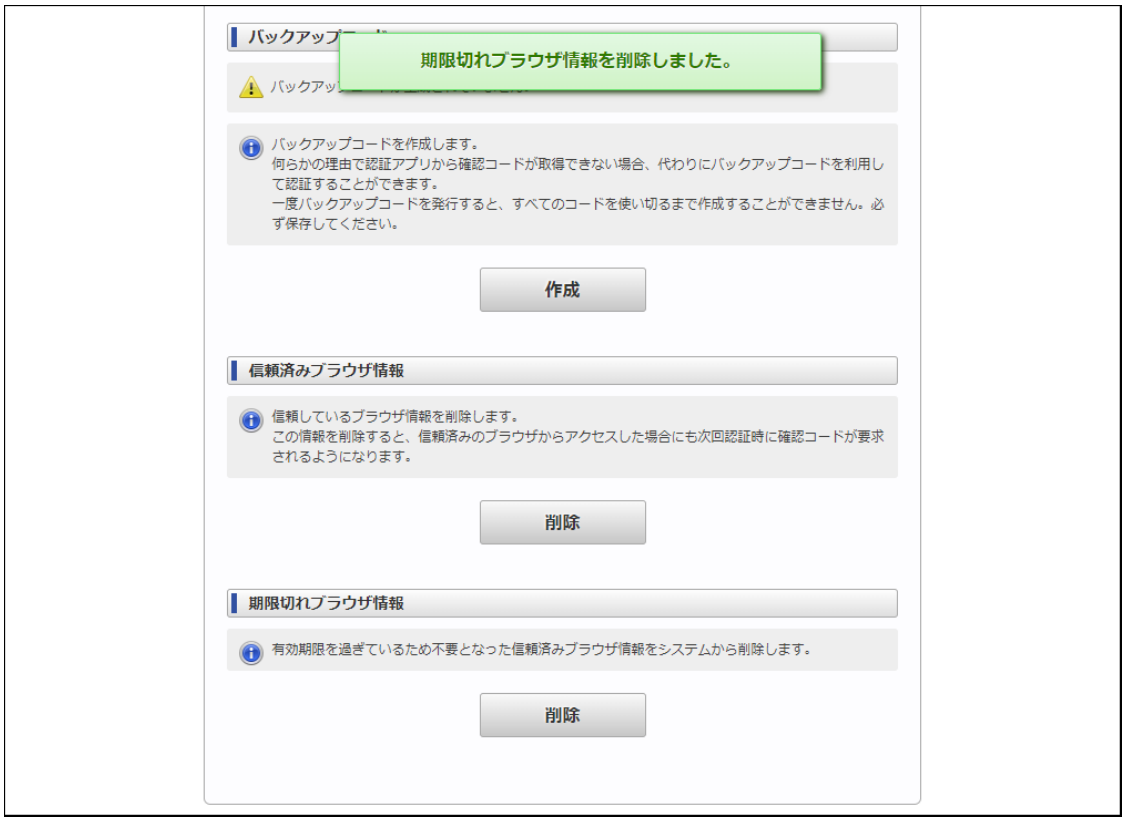
3. 「削除」をクリックします。



4. 「決定」をクリックします。



5. 期限切れブラウザ情報が削除されました。



多要素認証を行う

ここでは多要素認証を利用したログインついてを説明します。

項目

- 確認コードを利用してログインする
- バックアップコードを利用してログインする
- ログインできなくなってしまった場合

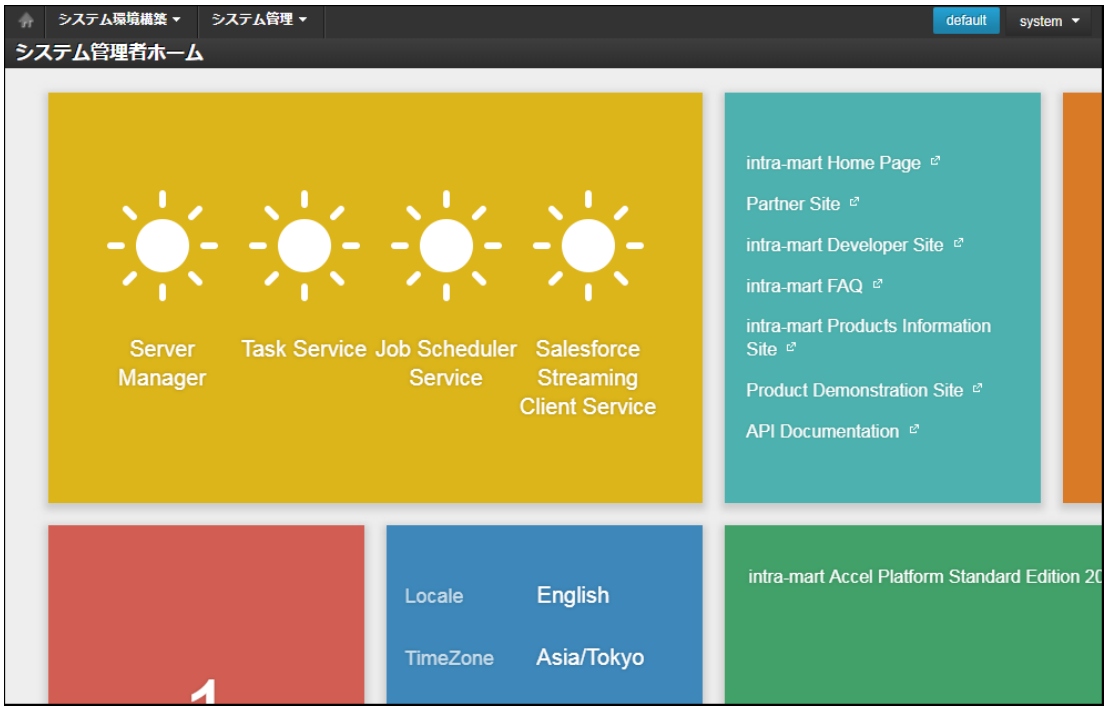
確認コードを利用してログインする

1. *システム管理者としてログインする*に従ってパスワードを入力して認証します。
2. 「確認コード入力」画面が表示されます。

3. 認証アプリに表示されている確認コードを入力して「ログイン」をクリックします。

> **コラム**
>
> 「このブラウザでは次回から表示しない」を ON にしてログインすることで、一定期間そのブラウザが記憶されます。
> 記憶されたブラウザを使ってログインする際は、パスワードの入力だけでログインすることができます。
>
> 「*信頼済みブラウザ情報を削除する*」で記憶されたブラウザの情報を削除することができます。

4. ログインできました。



バックアップコードを利用してログインする

コラム

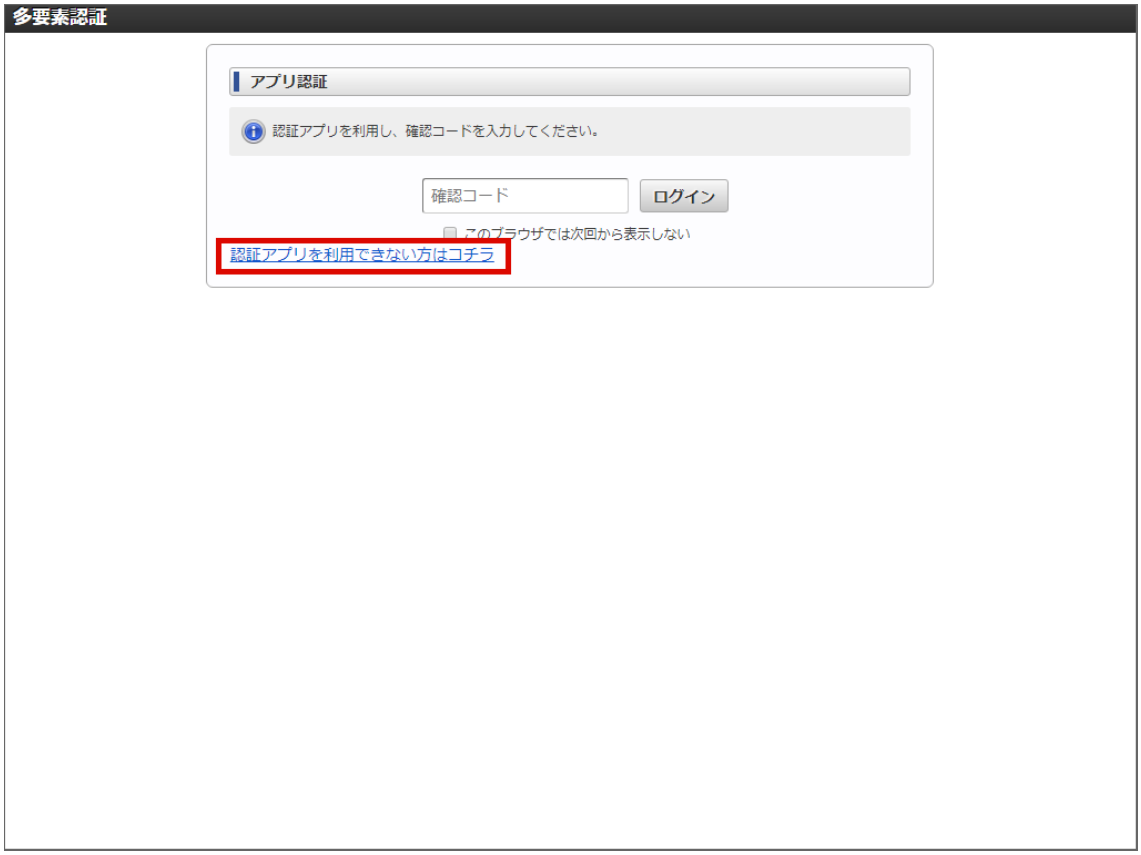
携帯端末を紛失してしまったり携帯端末が故障してしまったなどで確認コードの入力ができない場合に、事前に作成したバックアップコードを入力することでログインできます。
バックアップコードの作成方法は、「*バックアップコードを作成する*」を参照ください。

注意

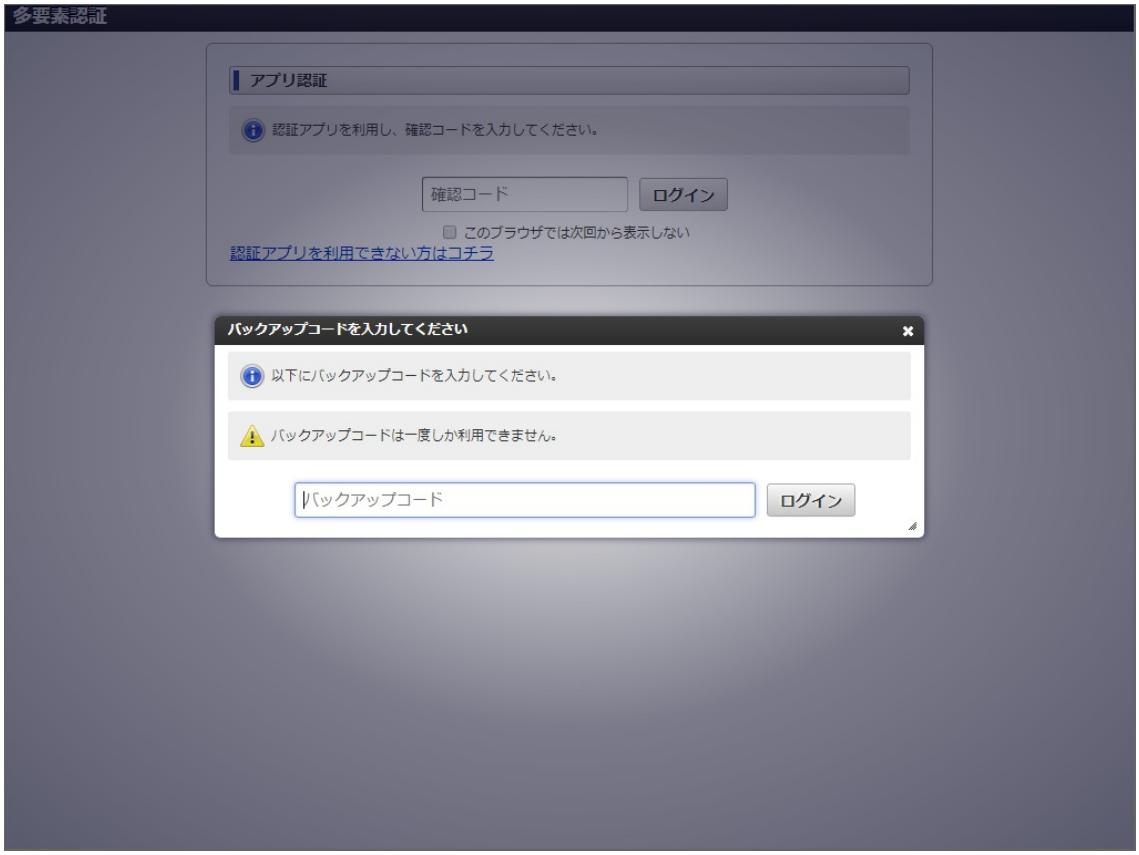
バックアップコードは一つのコードにつき一度しか利用できません。

1. *システム管理者としてログインする* に従ってパスワードを入力して認証します。
2. 「確認コード入力」画面が表示されます。

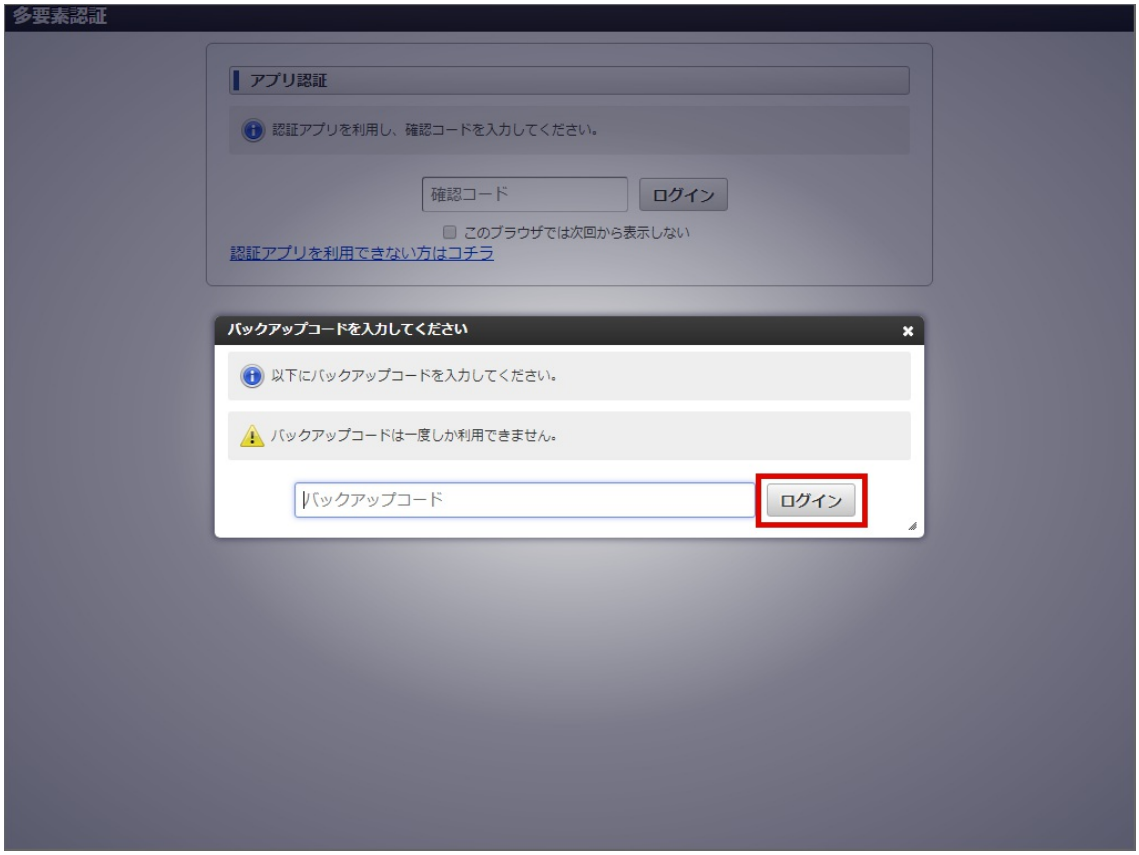
3. 「認証アプリを利用できない方はコチラ」をクリックします。



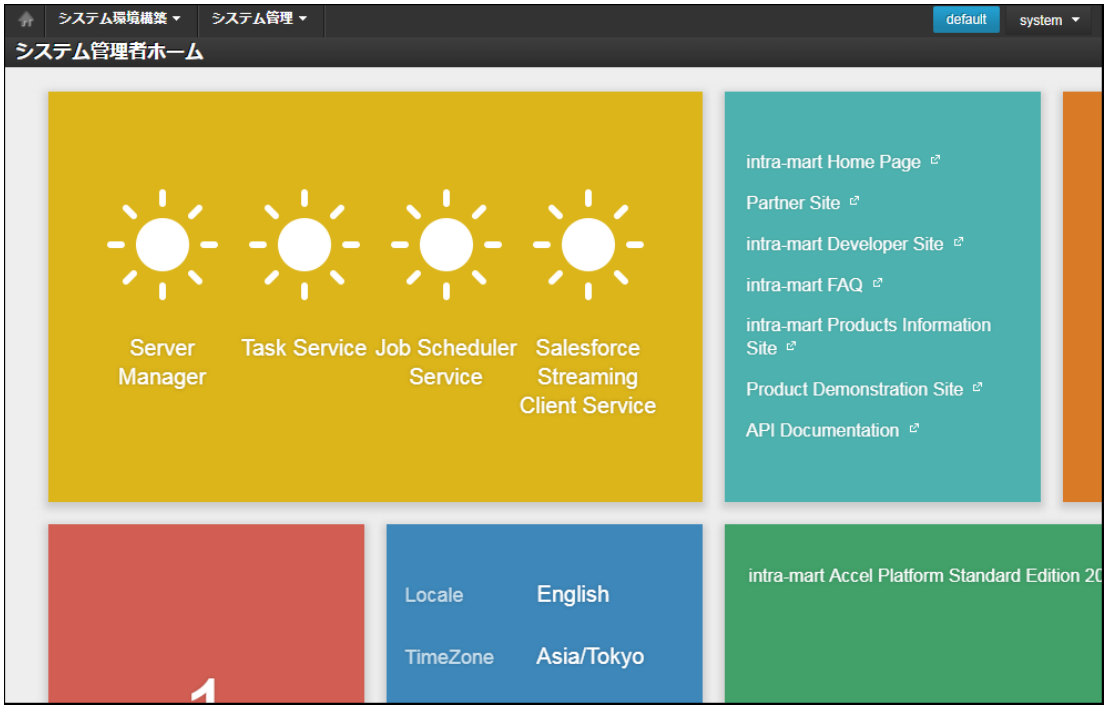
4. バックアップコード入力ダイアログが表示されます。



5. バックアップコード入力して「ログイン」をクリックします。



6. ログインできることを確認します。



ログインできなくなってしまった場合

多要素認証機能を有効にしている場合、ユーザコード・パスワードでの認証後に確認コードの入力を求められます。
システム管理者に対する多要素認証機能を無効化するためには以下のシステムプロパティを設定します。

プロパティ名	jp.co.intra_mart.system.mfa.certification.MultiFactorAuthAdminCertification.disable
プロパティ値	true

指定例

```
-Djp.co.intra_mart.system.mfa.certification.MultiFactorAuthAdminCertification.disable=true
```