Copyright © 2012 NTT DATA INTRAMART CORPORATION

目次

- 改訂情報
- はじめに
- 前提条件
- インストール手順
  - システム構成
  - 各サーバの情報の仮定義
  - インストールファイル構成
  - intra-mart Accel Platform のインストールと設定
    - intra-mart Accel Platform のインストール
    - 設定ファイルの設定
    - warの生成とデプロイ
  - VANADIS SecureJoin SSO Login Server の環境設定
    - 1. セキュリティプロバイダの追加
    - 2. war ファイルの展開
    - 3. 鍵セットの作成
    - 4. 設定ファイルの編集
    - 5. 認証エラー時のメッセージ設定について
    - 6. 認証を行うテナントIDの解決方法について
    - 7. J2EEアプリケーションサーバのセットアップ
    - 8. デプロイ
  - VANADIS SecureJoin SSO Webラッパー のインストール
    - Windows 版のインストール
    - Solaris/Linux 版のインストール
  - VANADIS SecureJoin SSO Webラッパー ユーザ認証モジュールの設定
    - 基本設定
    - 形式変換プラグインの設定
- 動作確認
- IM-SecureSignOnを無効化するには
- IM-SecureSignOn 設定ファイル
  - 概要
  - リファレンス
    - ログアウトURL設定

前提条件

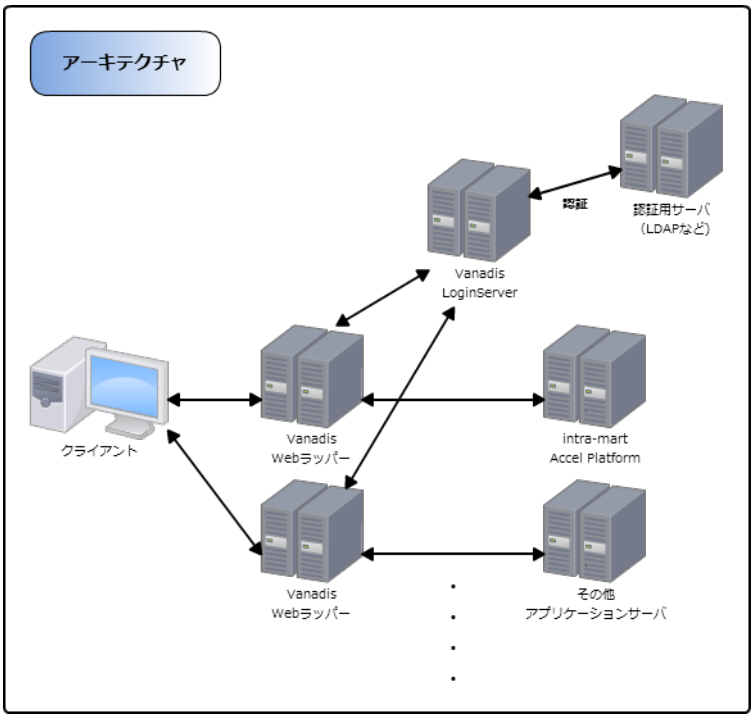
IM-SecureSignOn for Accel Platform をインストールするためには、以下の前提条件があります。

- intra-mart Accel Platform が正常に動作していること。
- intra-mart Accel Platform のパッチに関しましては、常に最新のものを適用するようにしてください。

変更年月日	変更内容
2012-12-21	初版
2014-04-01	第2版　下記を追加・変更しました ▪ 「*認証を行うテナントIDの解決方法について*」を追加 ▪ 「*基本設定*」にアクセス条件として使用できる情報「tntid（テナントID）」を追加
2014-05-01	第3版 下記を追加・変更しました ▪ 「*IM-SecureSignOnを無効化するには*」を追加
2015-08-01	第4版 下記を追加・変更しました ▪ 「*各サーバの情報の仮定義*」に基づいたわかりやすい説明に改善。
2016-04-01	第5版 下記を追加・変更しました ▪ 「*インストールファイル構成*」を変更しました。 ▪ 各種イメージを最新に変更しました
2017-12-01	第6版 下記を追加・変更しました ▪ 「*インストール手順*」 を変更しました。

システム構成

名称	説明
VANADIS SecureJoin SSO Webラッパー	シングルサインオンを制御するプロキシサーバです。 シングルサインオンさせるアプリケーションサーバ毎に設置（インストール）を行います。 ※ アプリケーションサーバが3つある場合は、各アプリケーションサーバに対して1づつ、合計3つインストールします。
VANADIS SecureJoin SSO Login Server	シングルサインオンの認証を処理を制御するサーバです。 シングルサインオンシステムで1つ必要です。
認証用サーバ	VANADIS SecureJoin SSO Login Server が認証を行う際に問い合わせを行うサーバです。 シングルサインオンシステムで1つ必要です。 intra-mart Accel Platform を 認証サーバとして利用可能です。 本マニュアルでは intra-mart Accel Platform を認証サーバとして利用する方法について説明しています。



各サーバの情報の仮定義

説明を進めるに当たって、シングルサインオンアーキテクチャでの各サーバの情報を仮定義します。
以下の定義を元に説明を行います。
実際の設定では、各サーバのホスト名に置き換えて設定してください。

- アプリケーションサーバを2つ。 (内、1つは intra-mart Accel Platform とします)
- 認証サーバに intra-mart Accel Platform を利用します。
  この intra-mart Accel Platform は アプリケーションサーバとして利用するものと同一です。
- シングルサインオンアーキテクチャのドメインは **intra-mart.jp** とします。
  シングルサインオンアーキテクチャに含まれるサーバのドメインは全て同じにしてください。

サーバの種類	ホスト名	ポート番号	コンテキストパス	説明
VANADIS SecureJoin SSO Webラッパー 1	web1.intra-mart.jp	80(標準ポート)	なし	アプリケーションサーバ 1 用の VANADIS SecureJoin SSO Webラッパー とします。

変更年月日	変更内容
2019-12-25	第7版 下記を追加・変更しました ▪ 「*インストールファイル構成*」を変更しました。 ▪ 「*VANADIS SecureJoin SSO Login Server の環境設定*」の「*鍵セットの作成*」を変更しました。 ▪ 「*VANADIS SecureJoin SSO Webラッパー のインストール*」の「*Windows 版のインストール*」と「*Solaris/Linux版のインストール*」を変更しました。 ▪ 各種イメージを最新に変更しました。
2020-12-01	第8版 下記を変更しました ▪ 各種ファイル名・バージョン表記を最新に変更しました

サーバの種類	ホスト名	ポート番号	コンテキストパス	説明
VANADIS SecureJoin SSO Webラッパー 2	web2.intra-mart.jp	80(標準ポート)	なし	アプリケーションサーバ 2 用の VANADIS SecureJoin SSO Web ラッパー とします。
VANADIS SecureJoin SSO Login Server	auth.intra-mart.jp	443(SSL標準ポート)	sso	Tomcatを用いて、SSL環境を構築した VANADIS SecureJoin SSO Login Server とします。
認証用サーバ	app1.intra-mart.jp	80(標準ポート)	imart	アプリケーションサーバ 1 と同一のサーバとします。
アプリケーションサーバ 1	app1.intra-mart.jp	80(標準ポート)	imart	intra-mart Accel Platform とします。
アプリケーションサーバ 2	app2.intra-mart.jp	80(標準ポート)	other	シングルサインオンを行いたい別のアプリケーションサーバとします。

インストールファイル構成

ディレクトリ / ファイル	説明
_static	ドキュメント用資材
LoginServer	Login Server モジュール
LoginServer-plugin	Login Server プラグイン
LoginServer-test-mode	Login Server テストモード
setup_guide	IM-SecureSignOn for Accel Platform セットアップガイド（本書）
release_notes	IM-SecureSignOn for Accel Platform リリースノート
Tool	各種ツール
Wrapper	Webラッパー モジュール
Wrapper-plugin	Webラッパー JavaScript プラグイン
【PKG】VANADIS_PKGバージョン一覧_20200330.pdf	VANADIS SecureJoin SSO リリースバージョン一覧
【PKG】VANADIS_PKG動作保証プラットフォーム.pdf	VANADIS SecureJoin SSO 動作保証プラットフォーム一覧
index.html	IM-SecureSignOn for Accel Platform ドキュメントルート
ReleaseNotes_202004.txt	VANADIS SecureJoin SSO リリースノート
SSOチュートリアル.pdf	VANADIS SecureJoin SSO チュートリアルガイド

intra-mart Accel Platform のインストールと設定

intra-mart Accel Platform を IM-SecureSignOn for Accel Platform のシステムへ参加させるためのインストールと設定方法について説明します。

インストールおよび設定は、 IM-Juggling で行います。

以下の手順を行うことで、 intra-mart Accel Platform を認証用サーバとしても利用できます。
認証用サーバを利用することで、 intra-mart Accel Platform のアカウントを利用したシングルサインオンが可能です。

intra-mart Accel Platform のインストール

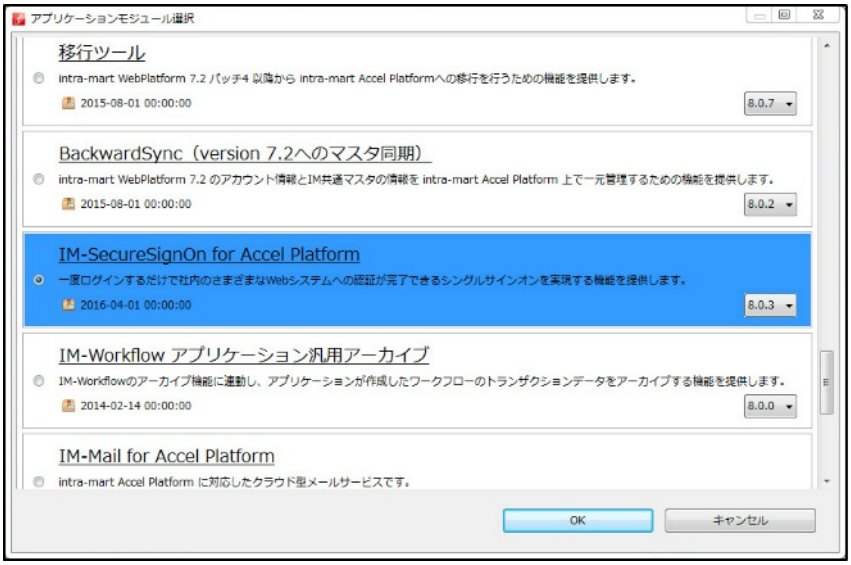
1. intra-mart Accel Platform を IM-SecureSignOn for Accel Platform へ参加させるために、IM-Juggling で 「アプリケーション」タブの右上の[＋]ボタンから
   「アプリケーションモジュール選択」ダイアログを開きます。
2. 「アプリケーションモジュール選択」ダイアログから 「 IM-SecureSignOn for Accel Platform 」を追加します。

はじめに

本ドキュメントは、IM-SecureSignOn のインストール手順と設定の方法について記述しています。
IM-SecureSignOn の標準機能をインストールするには、大きく分けて 3 つの作業が必要です。

1. intra-mart Accel Platform モジュールのインストールと設定
2. VANADIS SecureJoin SSO Login Server モジュールのインストールと設定
3. VANADIS SecureJoin SSO Webラッパー モジュールのインストールと設定

その他の拡張モジュールのインストールは、各ディレクトリの doc 以下のドキュメントを参照してください。



3. 「 IM-SecureSignOn 」を追加すると、 IM-Juggling プロジェクトに conf/im-sso-config.xml が 追加されます。

設定ファイルの設定

IM-Juggling プロジェクトの conf/im-sso-config.xml ファイルをエディタで開き、im-sso-config/logout-linkage タグを編集します。

url 属性には、intra-mart Accel Platform からログアウトした後に表示されるページ（URL）を指定します。

標準の設定では、VANADIS SecureJoin SSO Login Server のログアウト画面を設定します。

- VANADIS SecureJoin SSO Login Server のログアウト画面のURLは、以下の通りです。

  ```
  http://<VANADIS SecureJoin SSO Login Serverのホスト名>:<ポート番号>/sso/logout.do
  ```

- VANADIS SecureJoin SSO Login Server にSSLを適用する場合は、以下の通りです。

  ```
  https://<VANADIS SecureJoin SSO Login Serverのホスト名>/sso/logout.do
  ```

  また、SSLを適用する場合は、 VANADIS SecureJoin SSO Login Server のホスト名 にIPアドレスは指定できません。
  SSL証明書に登録したドメイン名を使用してください。

記述例：

「*各サーバの情報の仮定義*」の場合は、以下の通りです。

```
<?xml version="1.0" encoding="UTF-8"?>

<im-sso-config
   xmlns="http://www.intra-mart.jp/sso/config/im-sso-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/sso/config/im-sso-config ../schema/im-sso-config.xsd">

   <logout-linkage enable="true" url="https://auth.intra-mart.jp/sso/logout.do"/>

</im-sso-config>
```

> **コラム**
>
> HTTP接続において、ポート番号が 80 である場合、ポート番号は省略可能です。
> HTTPS接続(SSL)において、ポート番号が 443 である場合、ポート番号は省略可能です。
> 実際の利用の際には、各ホストに対応するポート番号を必要に応じて付加してください。
>
> 設定ファイルの詳細については *IM-SecureSignOn 設定ファイル* を参照してください。

warの生成とデプロイ

IM-Juggling より warファイルを作成し、デプロイを行います。

VANADIS SecureJoin SSO Login Server の環境設定

VANADIS SecureJoin SSO Login Server とはシングルサインオン時の認証処理およびセッションの管理を行います。

以下の手順で、 VANADIS SecureJoin SSO Login Server の環境設定を行います。
環境設定の詳細については、以下の章で順に説明しています。

セキュリティプロバイダの追加

下記の作業手順に従って、セキュリティプロバイダの追加を行います。
※ 以下、JDK のインストールディレクトリを <%java_home%> として説明します。

1. 暗号プロバイダの追加
   Bouncy Castle 暗号プロバイダをインストールします。
   http://www.bouncycastle.org/latest_releases.html より配布されている JCE プロバイダ(bcprov-jdkXX-YYY.jar)を <%java_home%>/jre/lib/ext ディレクトリに配置してください。

   > **コラム**
   > XX は使用する JRE のバージョンに合わせてください。

2. java.security へ暗号プロバイダを追加
   <%JAVA_HOME%/jre/lib/security> にある <java.security> ファイルをテキストエディタで開き、セキュリティプロバイダー一覧に、Bouncy Castle 暗号プロバイダ(org.bouncycastle.jce.provider.BouncyCastleProvider)を追加します。
   security.provider.n で始まる行の次に、以下の設定例を参考に追加してください。
   設定例 （JDK 8u152 の場合）

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=sun.security.ec.SunEC
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
security.provider.8=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.9=sun.security.smartcardio.SunPCSC
security.provider.10=sun.security.mscapi.SunMSCAPI
security.provider.11=org.bouncycastle.jce.provider.BouncyCastleProvider
```

3. JAVA_HOME 環境変数に<%java_home%> を設定

   > **コラム**
   > VANADIS SecureJoin SSO Login Server が暗号プロバイダを追加した JDK で実行されるようにするための設定です。
   > VANADIS SecureJoin SSO Login Server がこの暗号プロバイダを利用して、認証用クッキーを暗号化します。

war ファイルの展開

設定ファイルや鍵セットファイルを更新するために、war ファイルを展開します。(LoginServer/bin/sso.war)
war ファイルの展開には、J2EE に付属の jar コマンドを使用するか、ZIP 形式の圧縮ファイルを展開することが可能なツールを使用してください。
※ 以下、sso.war ファイルを展開したディレクトリを、<%sso_path%> として説明します。

jar コマンドによる、war ファイルの展開例

```
c:¥sso> jar xf sso.war
```

鍵セットの作成

暗号化用鍵セットの作成を行います。
この鍵セットは、VANADIS SecureJoin SSO Login Server が認証用クッキーを暗号化するために用います。
また、証明書ファイルについては VANADIS SecureJoin SSO Webラッパー が認証用クッキーを復号化するためにも使用されます。

付属の 「SSO 鍵ファイル作成ツール」（Tool/CertMaker/bin/CertMaker.exe）を使用して、電子署名および暗号化／復号化に使用する鍵セットを作成します。
操作方法の詳細については、鍵ファイル作成ツール説明書.pdf」（Tool/CertMaker/doc/鍵ファイル作成ツール説明書.pdf）を参照してください。
作成した鍵セットは、<sso.war> ファイルを展開したディレクトリ下の <WEB-INF/signature> ディレクトリに格納してください。

鍵セットの格納先

鍵セット	ディレクトリ	ファイル名
秘密鍵ファイル	<%sso_path%>/WEB-INF/signature	key.pem
証明書ファイル	<%sso_path%>/WEB-INF/signature	cert.pem

> **コラム**
>
> 既存のファイルがある場合は、上書きして構いません。

設定ファイルの編集

ここでは、 VANADIS SecureJoin SSO Webラッパー に対して認証用サーバのURLの設定を行います。

※ 以下、sso.war ファイルを展開したディレクトリを、<%sso_path%> とします。
※ 「*各サーバの情報の仮定義*」のように認証用サーバが intra-mart Accel Platform である場合として説明します。

1. VANADIS SecureJoin SSO Webラッパー の <%sso_path%>/WEB-INF/sso-login.xml ファイルをエディタで開きます。
2. sso-login.xml の sso-login/authenticate/intra-mart/url タグを以下のように書き換えます。

   <url>http://<認証用サーバのホスト名>:<ポート番号>/<コンテキストパス>/sso/certification</url>

   記述例：

   「*各サーバの情報の仮定義*」の場合は、以下の通りです。

   ```
   <sso-login>
     :
     <authenticate>
       :
       <intra-mart>
         :
         <url>http://app1.intra-mart.jp/imart/sso/certification</url>
       </intra-mart>
     </authenticate>
     :
   </sso-login>
   ```

3. sso-login.xml の sso-login/domain タグ内の name, login-url, logout-url 属性を以下のように書き換えます。

   name=".VANADIS SecureJoin SSO Login Server名を除いたドメイン名"
   login-url="https://VANADIS SecureJoin SSO Login Serverのホスト名/sso/login.do"
   logout-url="https://VANADIS SecureJoin SSO Login Serverのホスト名/sso/logout.do"

   記述例：

   「*各サーバの情報の仮定義*」の場合は、以下の通りです。

   ```
   <sso-login>
     :
     <domain
       name=".intra-mart.jp"
        :
       login-url="https://auth.intra-mart.jp/sso/login.do"
       logout-url="https://auth.intra-mart.jp/sso/logout.do"
        :
     />
     :
   </sso-login>
   ```

   > **コラム**
   >
   > name 値は「.」から記述してください。

   > **コラム**
   >
   > VANADIS SecureJoin SSO Login Server に SSL を適用する場合は、 **http://･･･** と記述している箇所に **https://・・・** から始まる値 を指定してください。

4. sso-login.xml の sso-login/environment/portal-url タグを編集することで、ログインのキャンセル時や、 VANADIS SecureJoin SSO Login Server のログアウト画面のボタン押下時に遷移先が指定されていない場合のデフォルトの遷移先 URL を指定します。
   標準の設定では、Webラッパー の URL を指定します。

   http://Webラッパーのホスト名/ACL設定のパス/

   記述例：

   「*各サーバの情報の仮定義*」の場合は、以下の通りです。

```
<sso-login>
   :
  <environment>
     :
    <portal-url>http://web1.intra-mart.jp/imart/</portal-url>
  </environment>
   :
</sso-login>
```

認証エラー時のメッセージ設定について

intra-mart Accel Platform 側での認証エラーに対するメッセージを設定することができます。
標準の実装では、システムエラー時にはその旨を知らせる独自のメッセージを表示するよう設定されています。

- 既存エラーメッセージ表示設定

  標準の実装では、アカウントロック/ライセンス無効/ユーザが存在しない。
  これらの場合について、通常のログイン失敗時のエラーメッセージを表示するよう設定されています。
  それぞれのエラー内容を通知するメッセージを表示させるようにするには、sso-login.xml 内の message-mapping タグのコメントアウトを外します。
  また、エラーメッセージをデフォルトのものにしたい場合は該当する message-mapping タグをコメントアウトします。

  例：ライセンス無効のエラー情報を表示させる場合、

  ```
  <message-mapping id="-1" property="im.login.no.license"/>
  ```

  をコメントアウトから外します。

- 既存エラーに対するメッセージの編集

  標準のエラーメッセージを変更するためには、MessageResources_ja.properties を編集します。
  プロパティファイルはマルチバイト文字が UTF-8 エンコード（”¥u”＋16 進数）されているため、設定内容を変更する場合は、以下の手順で実施してください。

  1. MessageResources_ja.properties ファイルを native2ascii コマンドでテキストファイルに変換します。

     ```
     native2ascii -reverse MessageResources_ja.properties > MessageResources_ja.txt
     ```

  2. MessageResources_ja.txt ファイルを編集します。
  3. Java に付属する native2ascii コマンドで、UTF-8 エンコードしたファイルを作成します。

     ```
     native2ascii MessageResources_ja.txt MessageResources_ja.properties
     ```

認証を行うテナントIDの解決方法について

標準の実装では認証を行う時、<sso-login>/<environment>/<portal-url> から認証対象となるテナントIDを決定しています。
<portal-url> が *http://tenant.intra-mart.jp/imart/home* である場合、*http://tenant.intra-mart.jp* のスラッシュの後から最初のドットまでの文字列、tenant が認証対象のテナントIDとなります。
認証処理は認証対象のテナント内のユーザで行われます。

認証対象のテナントを明示的に設定したい場合は、以下のようにパラメータを追加します。
<tenant-id>default</tenant-id>
この設定を行うことで、認証は必ず指定したテナント内のユーザで認証されます。

設定例：

```
<sso-login>
   :
  <authenticate>
     :
    <intra-mart>
       :
      <tenant-id>default</tenant-id>
    </intra-mart>
  </authenticate>
</sso-login>
```

J2EEアプリケーションサーバのセットアップ

VANADIS SecureJoin SSO Login Server の機能はWebアプリケーションとして提供しています。
Webアプリケーションを動作させるためのJ2EEアプリケーションサーバ(Tomcat 等)が必要となります。

セットアップについては、利用するJ2EEアプリケーションサーバのマニュアルを参照してセットアップを行ってください。

J2EEアプリケーションサーバをSSL環境で運用する場合は、SSL証明書などのセットアップも行ってください。

認証用サーバがSSL環境である場合の設定について

認証用サーバがSSL環境である場合は、認証用サーバのSSL証明書をインストールすることで、認証用サーバと VANADIS SecureJoin SSO Login Server 間をSSLで通信できるようになります。

SSL証明のインストール方法は、以下の通りです。

```
keytool -import -trustcacerts -alias <%任意の別名%> -file <%認証用サーバのSSL証明書ファイルのパス%> -keystore “<%java_home%>/jre/lib/security/cacerts” -storepass changeit
```

デプロイ

1. 変更内容を反映した war ファイルを作成します。

   war ファイルの作成には、J2EE に付属した jar コマンドを使用してください。
   コマンドによる、war ファイルの作成例

   ```
   c:¥sso> jar cf sso.war *
   ```

2. J2EEアプリケーションサーバへデプロイします。

   コンテキストルートパスは sso に設定してください。
   ※J2EEアプリケーションサーバへのデプロイ方法については、使用されるパッケージのマニュアルをご覧ください。

   > **コラム**
   >
   > ほとんどの J2EEアプリケーションサーバは、Web アプリケーションの位置をディレクトリで指定することが可能です。
   > この場合は、war ファイル化せずに、war ファイルを展開したディレクトリの親ディレクトリを指定してください。

※ より詳しい説明については、sso/LoginServer/doc/SSOログインサーバV4.0.2-セットアップマニュアル.pdf を参照してください。

VANADIS SecureJoin SSO Webラッパー のインストール

Windows 版のインストール

インストーラを起動します。(Wrapper/bin/wrapper4101_win32.exe)

ウィザードに表示される以下の質問に回答しながら、インストールを進めてください。

1. インストール先フォルダの選択
   インストール先のフォルダを入力、または ［参照］ ボタンより選択して、［次へ］ボタンを押下してください。
   （例）C:\Program Files\SSO
2. サービス名
   任意の名前を設定。
   ※1台の Web サーバに複数のWebラッパーをインストールする際に、区別するための名称です。
   （例）imsso
3. WebWrapper4 Administration Tool をインストールするか選択
   インストールするを選択

4. 使用する Java を指定
   jdk のパスを指定してください。
   （例）C:\jdk8
5. 使用する Apache Tomcat を指定

項目	記述例	説明
インストール先フォルダ	C:\Program Files\SSO	インストール先のフォルダを入力
アーカイブファイル	C:\apache-tomcat-8.5.23-windows-x64.zip	ダウンロードした Apache Tomcat のファイルパスを入力、または ［参照］ ボタンより選択
Tomcatの実行ファイル名	tomcat8.exe	ダウンロードした Apache Tomcat の実行ファイル名を入力

6. WebWrapper4 Administration Tool をインストールするフォルダを選択
   インストール先のフォルダを入力、または ［参照］ ボタンより選択して、［次へ］ボタンを押下してください。
   （例）C:\Program Files\SSO\wrapadmin\webapps
7. Webラッパー 管理ツールの情報を設定
   以下の記述例を参考に、各項目の情報を設定してください。

項目	記述例	説明
ポート番号	8090	Webラッパー 管理ツールが常駐するポート番号を設定。 ※他で使用されていないポート番号を指定してください。
接続許可するIPアドレス	192.168.0.1	Webラッパー 管理ツールに接続を許可する端末名、または IP アドレス、ネットワークアドレスを設定します。
ユーザ名	sysuser	システム設定アカウントを設定。
パスワード	acluser	システム管理者アカウントのパスワードを設定。

   ※接続許可するIPアドレスには、複数指定することが可能です。その場合は、パイプ(|)区切りで設定します。

   例 ：

```
localhost|mypc|192.168.0.1
```

   ローカルホスト、mypc という名前の端末、192.168.0.1 の IP アドレスを持つ端末から、接続を許可する設定です。
8. ［インストール］ ボタンをクリックすると、インストールが開始します。
9. インストールが終了したら、［完了］ ボタンをクリックしてウィザードを閉じてください。

以上で Webラッパー のインストールは完了です。

Solaris/Linux 版のインストール

1. 配布アーカイブファイルの展開
   展開するアーカイブファイルは、 Wrapper/bin ディレクトリ内にあります。
   以下のコマンド例により、インストール先のディレクトリにファイルを展開してください。

```
% gunzip -c wrapperd4101_xxx.tar.gz | tar xvf -
```

   SSO ディレクトリが作成され、ファイルが展開されます。
   ※ コマンド例で示した、ファイル名の「xxx」の部分は、各プラットフォームよって異なります。
   ご利用の環境にあわせて変更してください。

> **注意**
> 既に存在するファイルは上書きされてしまいますので、バージョンアップインストールの場合は、事前に設定ファイル等を退避させてください。

2. Webラッパーインストール前の準備
   SSO ディレクトリ内のインストーラ設定ファイル(SSO/Installer.conf)をテキストエディタで開き、インストール方法により下記の設定項目を指定してください。

> **コラム**
> ディレクトリ設定箇所は絶対パスで指定する必要があります。

> **コラム**
> ディレクトリのパスにスペースを含む場合、ダブルクォートで囲むか、エスケープする必要があります。

   - Webラッパーのみをインストールする場合

設定項目	備考
INSTDIR	

設定項目	備考
ADMIN_FLG	0 を指定してください。

- Webラッパーと管理ツールをインストールする場合（Tomcat 同時インストール）

設定項目	備考
INSTDIR	
ADMIN_FLG	1 を指定してください。
ADMIN_CONTEXT	
JAVA_HOME	
TOMINS_FLG	1 を指定してください。
TOMCAT_ARCHIVE	
ADMIN_PORT	

- Webラッパーと管理ツールをインストールする場合（既存 Tomcat を使用）

設定項目	備考
INSTDIR	
ADMIN_FLG	1 を指定してください。
ADMIN_CONTEXT	
JAVA_HOME	
TOMINS_FLG	0 を指定してください。
CATALINA_HOME	
CATALINA_CONF	
CATALINA_PORT	
ADMIN_PORT	

3. Webラッパーインストーラ(SSO/Installer)を実行します。
   次の質問に対して、適切な値を設定してください。
   1. 管理ツールユーザ名
   2. 管理ツールパスワード
   3. 管理ツール接続許可IP
      名前解決が可能なホスト名、IPアドレス、ネットワークアドレスによる指定が可能です。
      例： localhost|mypc|192.168.0.1
      （ローカルホスト、mypc という名前の端末、192.168.0.1 の IP アドレスを持つ端末から、接続を許可します。）
4. ファイルオーナー、パーミッションの変更
   Webラッパー 管理ツールから Webラッパー の「起動／停止」が行えるように設定します。
   以下のコマンドを実行してください。

```
# chmod 755 SSO/rc/
# chmod 4755 SSO/wrapperd/wrapperd
# chown root:root SSO/rc/*
```

5. ディレクトリオーナーの変更
   Webラッパー は通常 nobody で実行されます。
   インストール先ディレクトリの所有者をnobodyに変更します。
   適切な所有者が設定されないと、ログファイルを書き込めないため、Webラッパー は起動に失敗します。
   以下のコマンドを実行してください。

```
# chown nobody:nobody SSO/wrapperd
```

VANADIS SecureJoin SSO Webラッパー ユーザ認証モジュールの設定

基本設定

VANADIS SecureJoin SSO Webラッパー 管理ツールで設定を行います。
それぞれインストールした VANADIS SecureJoin SSO Webラッパーに対して設定が必要です。
複数台ある場合は、それぞれ設定してください。

1. ブラウザから VANADIS SecureJoin SSO Webラッパーの管理ツールを起動します。管理者でログインしてください。

［管理者］ ユーザ名	VANADIS SecureJoin SSO Webラッパーのインストール時に設定したアカウント

パスワード	VANADIS SecureJoin SSO Webラッパーのインストール時に設定したパスワード

2. 左ページメニューから [システム設定] - [基本設定] をクリックします。

3. 右画面の各フィールドが、以下の設定になっていることを確認してください。
以下の内容は、「*各サーバの情報の仮定義*」の VANADIS SecureJoin SSO Webラッパー 1 を「例」として、各項目の設定について説明します。

> **コラム**
> 実際に設定を行うときは、ご利用の環境に合わせて値を変更してください。

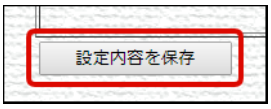
全体的な設定

項目	設定内容
RemoteName	VANADIS SecureJoin SSO Webラッパー が 管理するアプリケーションサーバのホスト名（ドメイン名または IP アドレス） 例 ： app1.imart.intra-mart.jp
RemotePort	VANADIS SecureJoin SSO Webラッパー が 管理するアプリケーションサーバのポート番号 例 ： 80
HostName	VANADIS SecureJoin SSO Webラッパー のホスト名（このサーバのホスト名です。） 例 ： web1.intra-mart.jp
LocalPort	VANADIS SecureJoin SSO Webラッパー のポート番号 例 ： 80 ※他で使用されていないポート番号を指定してください。 （注意） VANADIS SecureJoin SSO Webラッパー 管理ツールのポート番号ではありません。
User	VANADIS SecureJoin SSO Webラッパー 起動ユーザ（Solaris/linux 専用メニュー）
Group	VANADIS SecureJoin SSO Webラッパー 起動グループ（Solaris/linux 専用メニュー）
AuthURL	VANADIS SecureJoin SSO Login Server のログイン認証用URL 例 ： **https://auth.intra-mart.jp/sso/login.do**
ReAuthURL	VANADIS SecureJoin SSO Login Server の再認証用URL 例 ： **https://auth.intra-mart.jp/sso/login.do**
CancelURL	認証キャンセル時の表示 URL（空白）
IpMismatchURL	CheckIP でアドレス不一致の場合に表示する URL 例： **https://auth.intra-mart.jp/sso/msg/ipmismatch.jsp**
InvalidSignURL	CheckSignature で署名不正の場合の表示 URL 例： **https://auth.intra-mart.jp/sso/msg/invalidsign.jsp**
FormatErrURL	認証データフォーマットエラー時の表示 URL 例： **https://auth.intra-mart.jp/sso/msg/formaterr.jsp**
CookieDomain	要求、応答クッキーの送出ドメイン（サーバ名を除いたドメイン名） 例 ： .intra-mart.jp （'.' から始まります）
CertFile	認証クッキー電子署名検証用証明書 <cert.pem> ファイルの内容を設定 「*鍵セットの作成*」で作成した <cert.pem> ファイルの内容です。

> **コラム**
> VANADIS SecureJoin SSO Login Server に SSL を適用する場合は、**http** と記述する箇所を **https://**・・・から始まる値を指定してください。

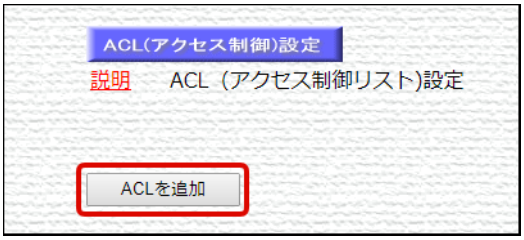
> コラム
> CertFile には cert.pem の行頭の「-----BEGIN CERTIFICATE-----」と行末の「-----END CERTIFICATE-----」を含めて入力してください。

4. 右ページ下段の [設定内容を保存] をクリックします。

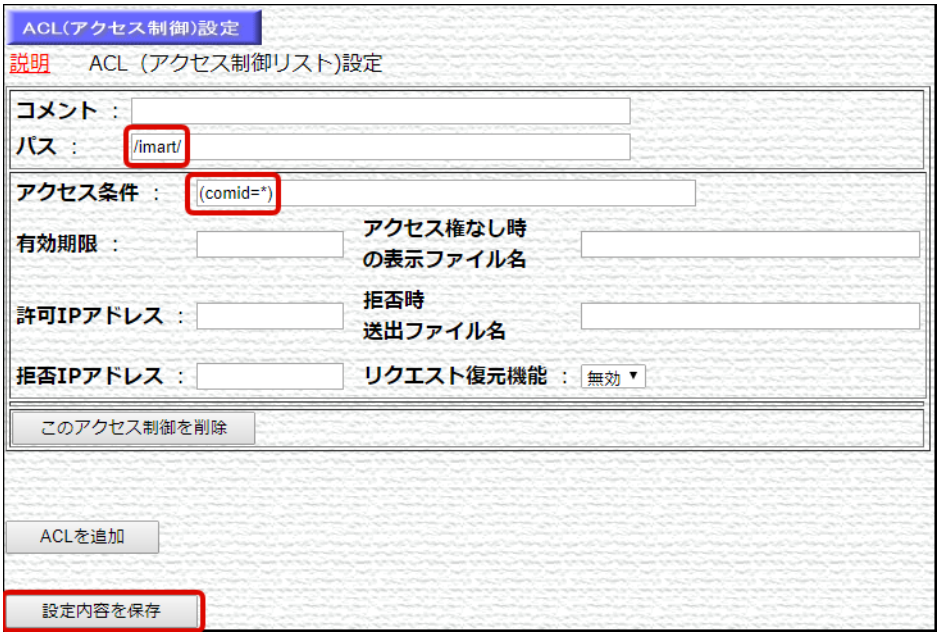


5. 左ページのメニューから [ACL設定] をクリックします。

6. 右ページの [ACLを追加] ボタンをクリックします。



7. 以下のように入力し、[設定内容を保存]ボタンをクリックします。



コラム

intra-mart Accel Platform を認証する場合は、以下に示す情報を得ることができます。
必要に応じて、アクセス条件に項目を追加して、アクセス制御を行ってください。

項目	内容
comid	ユーザ情報（ユーザID） （例） master
uid	ユーザID
tntid	テナントID
pwd	パスワード
name	ユーザ名
roles	ロール名一覧（ロール名の “|” 区切り） （例） |super|guest|user1|user2|

アクセス条件の記述例は以下の通りです。参考にしてください。

- 複数のアクセス条件を指定する場合は、「&」でつなげます

  （例）

  ```
  (comid=*)&(uid=*)&(roles=*)
  ```

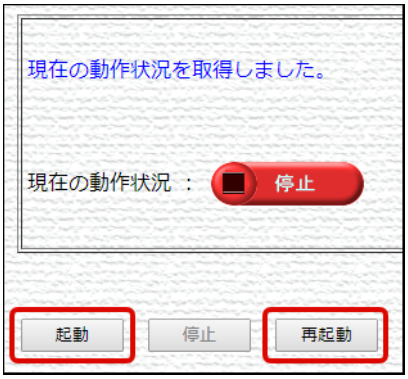
- 「管理者ロール（super）」を条件に指定する場合

  （例）

  ```
  (roles=*|super|*)
  ```

8. 左ページのメニューから [起動／停止] をクリックします。

9. 右ページの [起動] または[再起動] ボタンをクリックして、起動します。



以上で、Webラッパー 管理ツールでの設定は終了です。

形式変換プラグインの設定

Login Server で使用する Apache Tomcat において 5.5.26 以降または 6.0.16 以降のバージョンを使用する場合には、「形式変換プラグイン」の設定を行う必要があります。設定方法は以下の通りです。

詳細については「VANADIS SSO WebWrapper 形式変換プラグイン 【インストール・設定マニュアル】」wrapper-plugin/quotedcookie/doc/形式変換プラグイン_インストール・設定マニュアル.pdf を参照してください。

プラグインファイルの配置

各 OS のプラグラインファイルは、wrapper-plugin/quotedcookie/bin 配下の各 OS 名のディレクトリに保存されています。

- Windows 版

  Webラッパー の実行モジュール（wrapperd.exe）があるディレクトリ
  （例：C:\Program Files\SSO\imsso\wrapperd）にプラグインファイル quotedcookie.dll をコピーします。

- Solaris/Linux 版

  Webラッパー の実行モジュール（wrapperd または wrapperd.bin）があるディレクトリ

（例：/usr/local/SSO/wrapperd）にプラグインファイル quotedcookie.so（HP-UX 環境では、拡張子は .so ではなく sl）をコピーします。
また、HP-UX 環境では、本プラグインに実行権限が付与されていなければなりません。
必要に応じてコマンド（chmod +x ファイル名）を実行してください。

設定

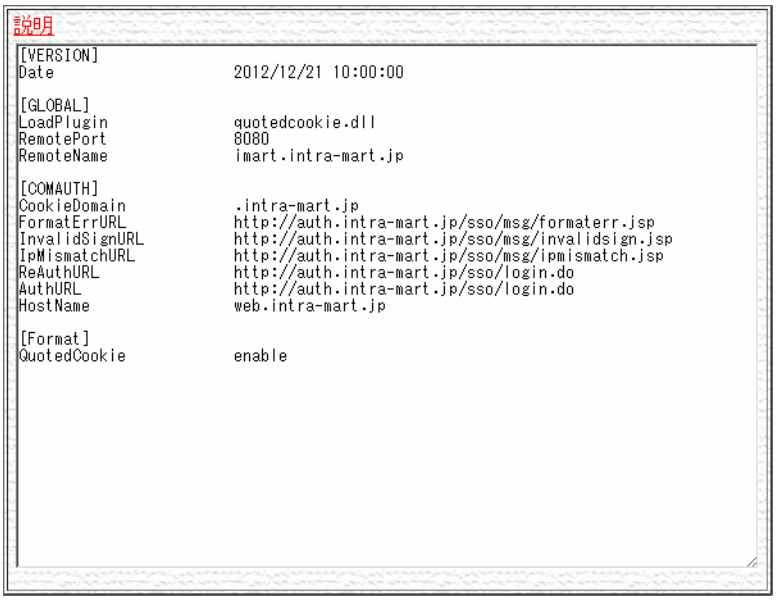
Webラッパー 管理ツールで設定を行います。

1. プラグインライブラリファイル名の設定
   Webラッパー 管理ツールの [システム設定] → [カスタム設定] より、『LoadPlugin』（プラグインライブラリファイル名）コピーしたプラグインファイル名を入力します。

   または、WebWrapper 設定ファイル(server.conf)の GLOBAL セクション “LoadPlugin” ディレクティブにコピーしたプラグインファイル名を記述します。

2. 本プラグイン独自の設定
   Webラッパー 設定ファイル(server.conf)へ直接、または、Webラッパー 4.3.1（以降）管理ツールの [上級者設定] → ［システム設定］ より、下記の内容を追加します。

```
[Format]
QuotedCookie enable
```



すべての設定が完了しましたら、Webラッパー を再起動して設定を反映させます。

動作確認

VANADIS SecureJoin SSO Login Server および、VANADIS SecureJoin SSO Webラッパー が起動していることを前提に、IM-SecureSignOn の動作確認を行ってください。

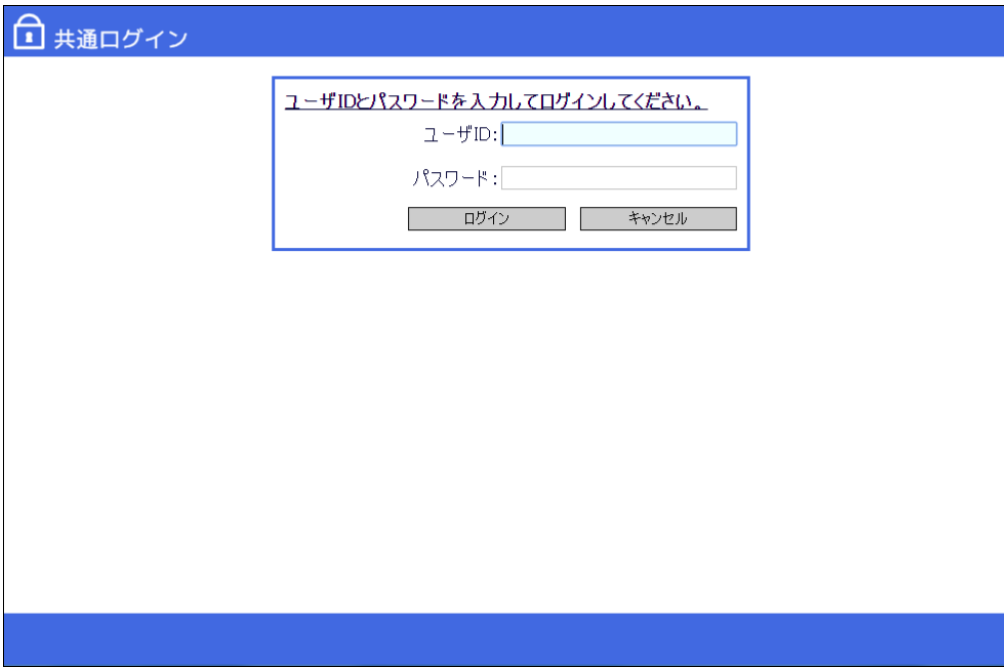
1. ブラウザから、以下のような URL を発行します。

   http://Webラッパーのホスト名/ACL設定のパス/

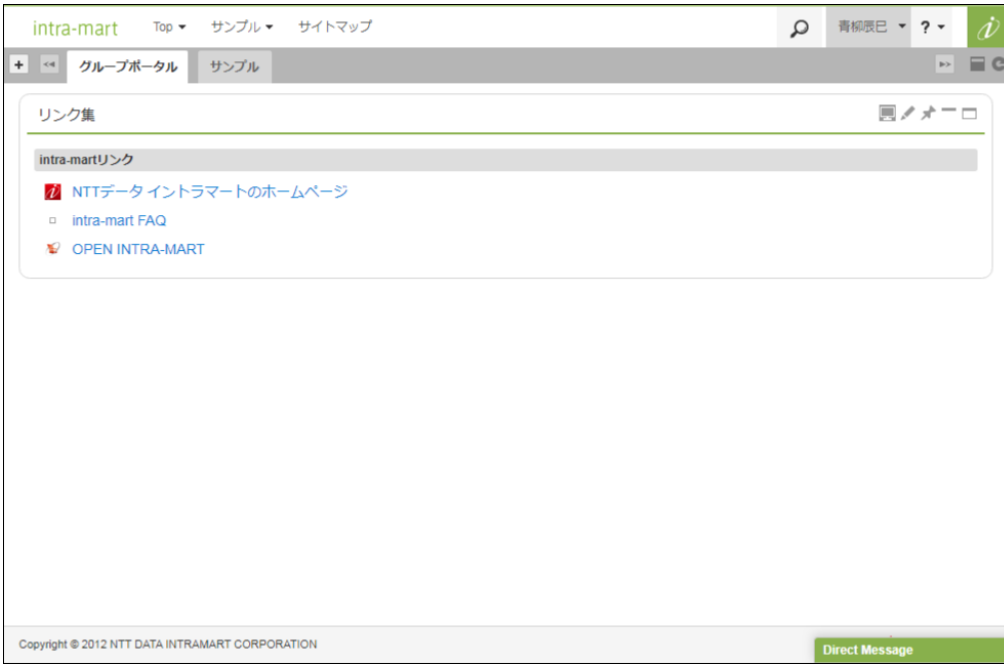
   ※ VANADIS SecureJoin SSO Webラッパー のホスト名には、*基本設定* に設定したものを記述します。
   ※ ACL 設定のパスには、*基本設定* で設定したものを記述します。

   （例）「*各サーバの情報の仮定義*」の内容で設定した場合、URL は **http://web1.intra-mart.jp/imart/** です。

2. 以下の、ログイン画面が表示されます。

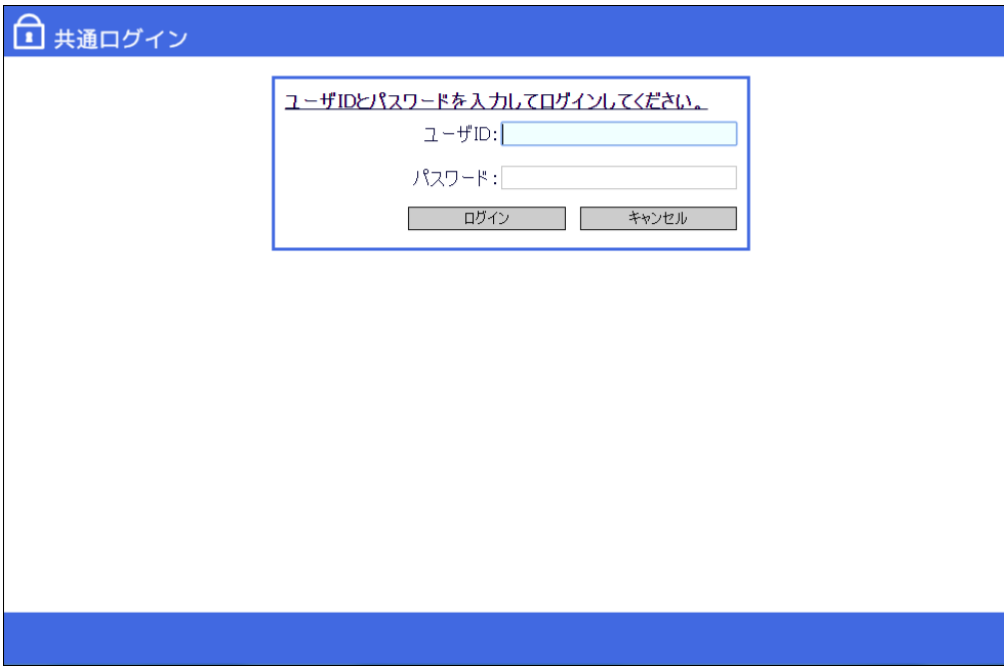


3. 任意のユーザで、intra-mart Accel Platform にログインします。
   intra-mart Accel Platform のメインページが表示されます。



4. intra-mart Accel Platform をログアウトすると、 VANADIS SecureJoin SSO Login Server のログアウト画面が表示されます。

5. 「OK」ボタンを押下します。
   以下の、ログイン画面が表示されたら、インストールおよび設定は成功です。



IM-SecureSignOnを無効化するには

IM-SecureSignOn for Accel Platformを無効化したい場合、以下の手順を実施するか、または単にIM-SecureSignOn for Accel Platformモジュールを含めずに war を作成し、再デプロイを行ってください。

1. <（展開したwar）>/WEB-INF/conf/im-sso-config.xml ファイルを開きます。
   - <im-sso-config>/<logout-linkage>/<@enable> を false に設定します。

```
<?xml version="1.0" encoding="UTF-8"?>

<im-sso-config
   xmlns="http://www.intra-mart.jp/sso/config/im-sso-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/sso/config/im-sso-config ../schema/im-sso-config.xsd">

 <logout-linkage enable="false" url="https://auth.server.co.jp/sso/logout.do"/> <!-- enable="false" を設定 -->

</im-sso-config>
```

2. <（展開したwar）>/WEB-INF/plugin/jp.co.intra_mart.foundation.security.certification.sso.user.provider.vanadis_8.0.0/plugin.xml ファイルを開きます。
   - <plugin>/<extension>/<sso-user-providers>/<@enable> を false に設定します（enable 属性がない場合、追加してください）

```
<?xml version="1.0" encoding="UTF-8"?>
<plugin>
 <extension point="jp.co.intra_mart.foundation.security.certification.sso.user.providers">
  <sso-user-providers
    id="jp.co.intra_mart.foundation.security.certification.sso.user.provider.vanadis"
    name="Vanadis SSO User Provider"
    version="8.0.0"
    rank="90"
    enable="false"> <!-- enable="false" を設定または追加 -->
    <sso-user-provider class="jp.co.intra_mart.sso.provider.VanadisSSOUserProvider"/>
  </sso-user-providers>
 </extension>
</plugin>
```

3. <（展開したwar）>/WEB-INF/plugin/jp.co.intra_mart.foundation.admin.tenant.context.tenant.resolver.vanadis_8.0.1/plugin.xml ファイルを開きます。
   - <plugin>/<extension>/<tenant-id-resolvers>/<@enable> を false に設定します（enable 属性がない場合、追加してください）

```
<?xml version="1.0" encoding="UTF-8"?>
<plugin>
 <extension point="jp.co.intra_mart.foundation.admin.tenant.context.tenant.resolvers">
  <tenant-id-resolvers
    id="jp.co.intra_mart.foundation.admin.tenant.context.tenant.resolver.vanadis"
    name="Vanadis Tenant Id Resolver"
    version="8.0.1"
    rank="90"
    enable="false"> <!-- enable="false" を設定または追加 -->
    <tenant-id-resolver class="jp.co.intra_mart.foundation.admin.tenant.context.VanadisTenantIdResolver"/>
  </tenant-id-resolvers>
 </extension>
</plugin>
```

4. <（展開したwar）>/WEB-INF/plugin/jp.co.intra_mart.foundation.admin.tenant.context.tenant.validator.vanadis_8.0.1/plugin.xml ファイルを開きます。
   - <plugin>/<extension>/<tenant-id-validators>/<@enable> を false に設定します

```
<?xml version="1.0" encoding="UTF-8"?>
<plugin>
 <extension point="jp.co.intra_mart.foundation.admin.tenant.context.tenant.validators">
  <tenant-id-validators
   id="jp.co.intra_mart.foundation.admin.tenant.context.tenant.validator.standard"
   name="Standard TenantIdValidator"
   version="8.0.1"
   rank="100"
   enable="false">
   <tenant-id-validator class="jp.co.intra_mart.system.admin.context.StandardTenantIdValidator">
    <!-- テナントID解決必須チェック -->
    <init-param>
     <param-name>required_tenant_id</param-name>
     <param-value>true</param-value>
    </init-param>
    <!-- テナントID存在チェック -->
    <init-param>
     <param-name>valid_tenant_id</param-name>
     <param-value>true</param-value>
    </init-param>
   </tenant-id-validator>
  </tenant-id-validators>
 </extension>
</plugin>
```

IM-SecureSignOn 設定ファイル

項目

- 概要
- リファレンス
  - ログアウトURL設定

概要

IM-SecureSignOn 利用時における、ログアウト後の遷移先 URL の設定を行います。
VANADIS SecureJoin SSO Login Server においてログアウト URL が未指定である場合に、本設定が利用されます。

モジュール	IM-SecureSignOn for Accel Platform
フォーマットファイル (xsd)	WEB-INF/schema/im-sso-config.xsd
設定場所	WEB-INF/conf/im-sso-config.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<im-sso-config
   xmlns="http://www.intra-mart.jp/sso/config/im-sso-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/sso/config/im-sso-config ../schema/im-sso-config.xsd">

      <logout-linkage enable="true" url="https://auth.server.co.jp/sso/logout.do"/>

</im-sso-config>
```

リファレンス

ログアウトURL設定

タグ名　logout-linkage

ログアウト後の遷移先URLの設定を行います。

【設定項目】

```
<im-sso-config
   xmlns="http://www.intra-mart.jp/sso/config/im-sso-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/sso/config/im-sso-config ../schema/im-sso-config.xsd">

      <logout-linkage enable="true" url="https://auth.server.co.jp/sso/logout.do"/>

</im-sso-config>
```

必須項目	○
複数設定	×
設定値・設定する内容	なし
単位・型	なし
省略時のデフォルト値	なし
親タグ	im-sso-config

【属性】

属性名	説明	必須	デフォルト値
enable	本タグの設定を有効にするかどうかの設定を行います。	○	なし

属性名	説明	必須	デフォルト値
url	ログアウト後の遷移先URLの設定を行います。	○	なし