



目次

前提条件

- 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
 - IM-SecureSignOn 8.0.6
のファイル構成
 - 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. war ファイルの展
開
 - 2. 鍵セットの作成
 - 3. 設定ファイルの編
集
 - 4. 認証エラー時の
メッセージ設定につい
て
 - 5. 認証を行うテナン
トIDの解決方法につい
て
 - 6. アプリケーション
サーバのセットアップ
 - 7. 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
 - 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

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- 初版
12-21

2014- 第2版 下記を追加・変
04-01 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- 第3版 下記を追加・変更
05-01 しました

- 「[IM-SecureSignOnを無効化するには](#)」を追加

2015- 第4版 下記を追加・変更
08-01 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- 第5版 下記を追加・変更
04-01 しました

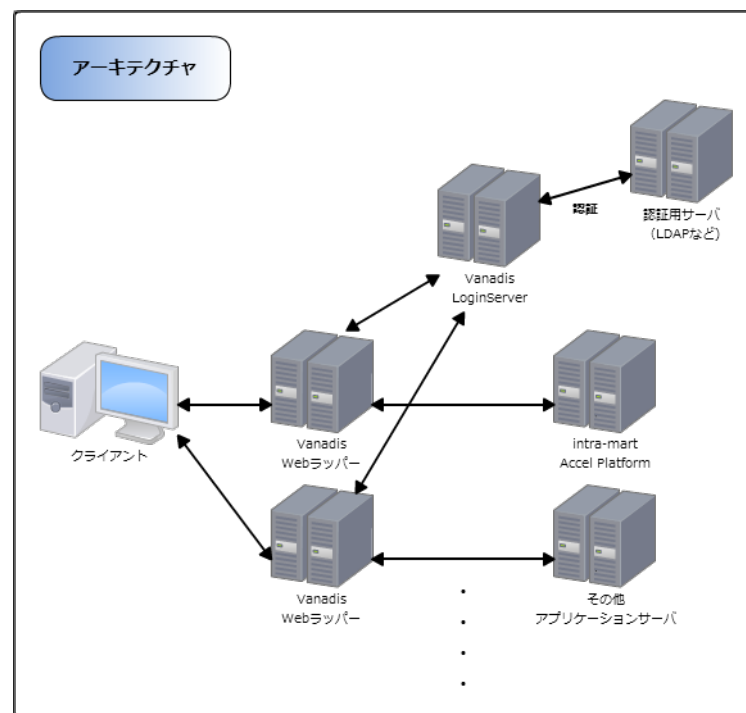
- 「[IM-SecureSignOn 8.0.6 のファイル構成](#)」を変更しました。
- 各種イメージを最新に変更しました

2017- 第6版 下記を追加・変更
12-01 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 ※ 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 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 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 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 VANADIS SecureJoin SSO ラッパー とします。
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 VANADIS SecureJoin SSO ラッパー とします。

変更 年月 日	変更内容
---------------	------

2019- 第7版 下記を追加・変更
12-25 しました

- 「[IM-SecureSignOn 8.0.6 のファイル構成](#)」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「[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- 第8版 下記を変更しまし
12-01 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

2026- 第9版 下記を変更・削除
04-01 しました

- 各種ファイル名・バージョン表記・Web ラッパー のセットアップ手順を最新に変更しました。
- 「[VANADIS SecureJoin SSO Login Server の環境設定](#)」の「[セキュリティプロバイダの追加](#)」を削除しました。

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 Login Server	auth.intra-mart.jp	443(SSL標準ポート)	sso	Tomcatを用いて、SSL環境の VANADIS SecureJoin 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アプリケーションサーバとします。

IM-SecureSignOn 8.0.6 のファイル構成

ディレクトリ / ファイル	説明
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
Tool	各種ツール
Wrapper	Web ラッパー モジュール
Wrapper-plugin	Web ラッパー プラグイン
【PKG】VANADIS_PKGバージョン一覧.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
ReleaseNotes_202504.txt	VANADIS SecureJoin SSO リリースノート
VANADIS SecureJoin 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。

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

- 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 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。
- 「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 で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。

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、Java 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。

※ 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。

— IM-SecureSignOn for Accel Platform セットアップガイド 第9版 2026-04-01

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／復号化に使用します。

操作方法の詳細については、Tool/CertMaker/doc/鍵ファイル作成ツールV2.1.1-マニュアル.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. <%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"
type="master"
login-url="https://auth.intra-mart.jp/sso/login.do"
logout-url="https://auth.intra-mart.jp/sso/logout.do"
cookie-path="/"
require-cookie-encryption="false"
/>
:
</sso-login>
```

コラム

name 値はドット(.)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 Secu

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、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>
```

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。
そのため、Webアプリケーションを動作させるためのアプリケーションサーバ（Tomcat 等）が必要です。

セットアップについては、利用する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。

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して、認証用サーバと VANADIS SecureJoin SSC Server 間をSSLで通信できるようにする必要があります。

SSL証明書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、Java 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. 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。

※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参照してください。



コラム

ほとんどの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、LoginServer/doc/SSOログインサーバV5.1.0-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/wrapperd500_win.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. Webラッパー 管理ツールをインストールするか選択



インストールするを選択してください。

2. インストール先フォルダの選択と識別名を設定



インストール先のフォルダは直接入力、または [参照] ボタンより選択してください。

(例) C:\Program Files\SSO

識別名は任意の名前を設定してください。

※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) imssso

3. 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	192.168.0.1/32	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、クアドレスを設定します。
ユーザID	sysuser	システム設定アカウントを設定。
パスワード	password	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、カンマ(,)区切りで設定します。

例：

```
localhost/32,mypc/32,192.168.0.1/32
```

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。

4. [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。
5. 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。

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 wrapperd500_redhat.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。



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/setup.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	
ADMIN_FLG	false 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

設定項目	備考
INSTDIR	
ADMIN_FLG	true を指定してください。
ADMIN_PORT	
ADMIN_IP	
ADMIN_ID	
ADMIN_PASS	
NAME	

3. Webラッパーインストーラ(SSO/Installer)を実行します。

コラム

インストーラでは主に以下の処理が行われます。

1. setup.conf の設定内容チェック
2. Webラッパー のインストール (ADMIN_FLG が true なら管理ツールもインストール)
3. ファイルオーナー、パーミッションの変更
4. ディレクトリオーナーの変更

インストーラが正常に終了した場合は、以降の手順を実施する必要はありません。

インストーラ実行ユーザの権限不足等により3および4の変更に失敗した場合は、以降の手順を実施する必要があります。

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
```

注意

VANADIS SecureJoin SSO は Solaris へのサポートを終了したため、Webラッパー のインストール資材の提供を取止め

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。

WebWrapper Administration Tool

ユーザID

パスワード

ログイン

© 2023 NTTDATA INTELL

〔管理者〕 ユーザID	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. 左ページのメニューから [システム設定] をクリックします。

バージョン情報

起動・停止

システム設定

ACL設定

証明書設定

パスワード変更

ログアウト

3. 設定項目の設定を行います。
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
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。

GLOBAL セクションの設定	
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 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 番号 例：80

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 せん。
-----------	---

COMAUTH セクションの設定

項目	設定内容
HostName	VANADIS SecureJoin SSO Webラッパー のホスト名 (このサーバのホスト名) 例 : web1.intra-mart.jp
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
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)



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://** から指定してください。

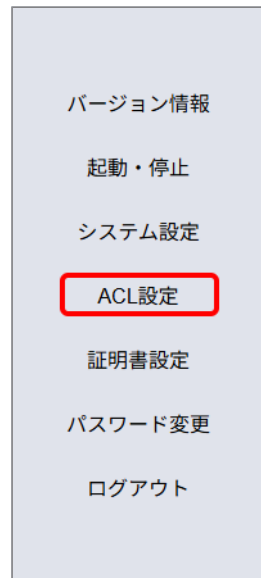
上記の設定例を全て踏まえた場合の記述例は以下の通りです。

システム設定	
バージョン情報	
起動・停止	
システム設定	[GLOBAL] RemoteName app1.imart.intra-mart.jp RemotePort 80 LocalPort 80
ACL設定	
証明書設定	[COMAUTH] HostName web1.intra-mart.jp AuthURL https://auth.intra-mart.jp/sso/login.do ReAuthURL https://auth.intra-mart.jp/sso/login.do IpMismatchURL https://auth.intra-mart.jp/sso/msg/ipmismatch.jsp InvalidSignURL https://auth.intra-mart.jp/sso/msg/invalidsign.jsp FormatErrURL https://auth.intra-mart.jp/sso/msg/formaterr.jsp CookieDomain .intra-mart.jp
パスワード変更	
ログアウト	
保存	

© 2023 NTTDATA INTELL

※ その他の設定可能な項目については、Wrapper/doc/appendix/WebラッパーV5.0.0-設定ファイル詳細説明書.pdf を参照し。

4. 右ページ下段の [保存] ボタンをクリックします。
5. 左ページのメニューから [ACL設定] をクリックします。



6. 以下のように入力し、[保存] ボタンをクリックします。

```
path "/imart/" {allow "(comid=*)";};
```

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、アンパサンド(&)でつなげます

（例）

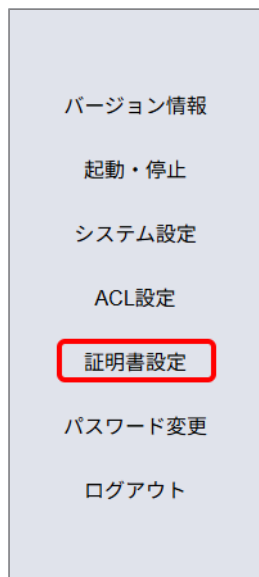
```
(comid=*)&(uid=*)&(roles=*)
```

- 「管理者ロール（super）」を条件に指定する場合

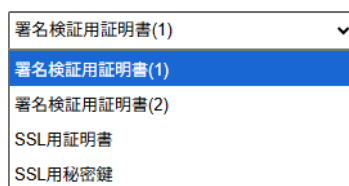
（例）

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

7. 左ページのメニューから [証明書設定] をクリックします。



8. 左上のプルダウンを [署名検証用証明書(1)] に変更します。



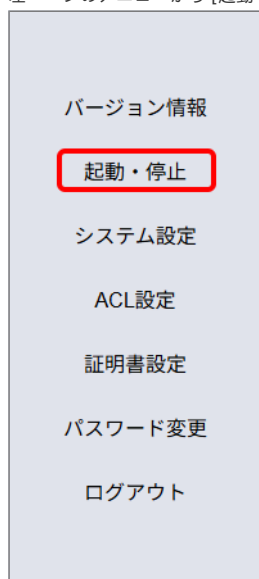
9. 「[鍵セットの作成](#)」で作成した <cert.pem> ファイルの内容を設定します。



コラム

cert.pem の行頭の「--BEGIN CERTIFICATE--」と行末の「--END CERTIFICATE--」を含めて入力してくだ

10. 右ページ下段の [保存] ボタンをクリックします。
11. 左ページのメニューから [起動・停止] をクリックします。



12. 右ページの [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」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 [wrapper-plugin/quotedcookie/doc/形式変換プラグインV2.0.0-セットアップマニュアル.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\wrapperd) にプラグインファイル quotedcookie.dll をコピーします。

• 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: /opt/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
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 設定ファイル(server.conf)へ直接、または、Webラッパー 管理ツールの [システム設定] にて以下の設定を行います。

1. プラグインライブラリファイル名の設定

GLOBAL セクションに下記の内容を追加します。

◦ Windows 版

```
[GLOBAL]
LoadPlugin quotedcookie.dll
```

◦ Linux 版

```
[GLOBAL]
LoadPlugin quotedcookie.so
```

2. 本プラグイン独自の設定

FORMAT セクションに下記の内容を追加します。

```
[FORMAT]
QuotedCookie enable
```

システム設定	
バージョン情報	
起動・停止	
システム設定	[GLOBAL] RemoteName app1.imart.intra-mart.jp RemotePort 80 LocalPort 80 LoadPlugin quotedcookie.dll
ACL設定	
証明書設定	
パスワード変更	[COMAUTH] HostName web1.intra-mart.jp AuthURL https://auth.intra-mart.jp/sso/login.do ReAuthURL https://auth.intra-mart.jp/sso/login.do IpMismatchURL https://auth.intra-mart.jp/sso/msg/ipmismatch.jsp InvalidSignURL https://auth.intra-mart.jp/sso/msg/invalidsign.jsp FormatErrURL https://auth.intra-mart.jp/sso/msg/formaterr.jsp CookieDomain .intra-mart.jp CertFile cert.pem
ログアウト	
保存	
© 2023 NTTDATA INTELL	

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。

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-SecureSignIn 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。

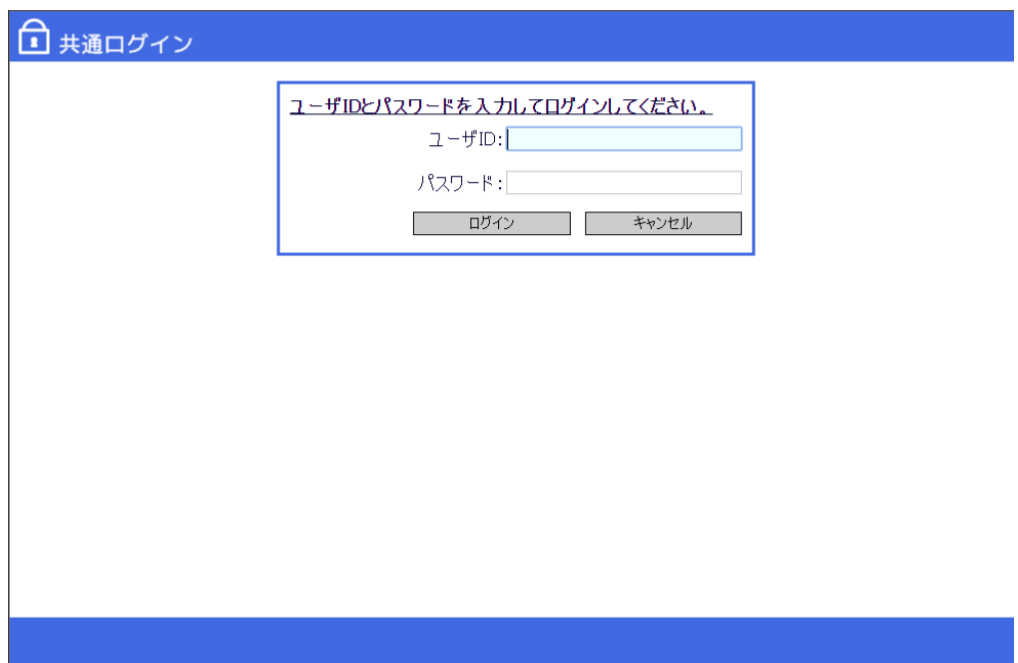


4. intra-mart Accel Platform をログアウトすると、VANADIS SecureJoin SSO Login Server のログアウト画面が表示されま



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 for Accel Platform セットアップガイド 第9版 2026-04-01

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のjarファイルを含めずに 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、追加します)。

```
<?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、追加します)。

```
<?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>
```

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
url	ログアウト後の遷移先URLの設定を行います。	○	なし