Secioss Identity Suite Cloud Edition IdP

マニュアル

３．１．４版

株式会社セシオス

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

目次

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

1. イントロダクション

1.1. Secioss Identity Suite Cloud Edition IdP

Secioss Identity Suite Cloud Edition は、クラウドコンピューティング環境において SAML 2.0 によるシングルサインオンや SOAP による ID 同期をサイト間で実現するソフトウェアです。

Secioss Identity Suite Cloud Edition IdP は、企業に導入することで、企業で管理しているアカウントにより、SaaS 型シングルサインオン/統合 ID 管理サービス SeciossLink とシングルサインオンや、ID の同期を行うことができます。

1.2. 機能

Secioss Identity Suite Cloud Edition IdP には、大きく以下の機能があります。

1.2.1. シングルサインオン

SAML の IdP、企業で管理している ID により、SeciossLink へシングルサインオンが可能となります。

認証には、ID/パスワード認証と統合 Windows 認証を使用することができます。

1.2.2. ID 同期

企業内の Active Directory で管理しているユーザとその OU を組織として、SeciossLink へ同期します。

パスワードについては、同期は行われません。SeciossLink へのユーザ登録時には、ランダムなパスワードが発行されます。

1.3. ソフトウェア環境

- OS： Windows Server 2003、Windows Server 2008
- Web サーバ： IIS 6 以降

2. インストール

2.1. Secioss Identity Suite Cloud Edition IdP

secioss-idsuite-cloud-idp-3.x.x.zip を展開して、opt フォルダを C:¥opt として配置します。

次に C:¥opt¥secioss の[プロパティ]->[セキュリティ]から、IUSR（Windows 2003 Server では IUSR_*<マシン名>*）、Users に対してアクセス許可を与えます。

さらに、以下のフォルダには IUSR、Users に対してフルコントロールのアクセス許可を与えます。

- C:¥opt¥secioss¥share¥simplesamlphp¥log

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

2.2. シングルサインオンに必要なソフトウェア

SAML の IdP の機能を使用しない場合、設定は不要です。

2.2.1. PHP の設定

http://www.php.net/downloads.php から PHP の Windows binary zip ファイルをダウンロードして、インストールして下さい。

PHP の Extension として、以下のモジュールをインストールして下さい。

- php_ldap.dll
- php_openssl.dll

2.2.2. IIS マネージャの設定

使用するソフトウェアについて以下のように仮想ディレクトリを設定します。

- SAML IdP
  エイリアス：saml　パス：C:¥opt¥secioss¥share¥simplesamlphp¥www
- Active Directory へのパスワード同期
  エイリアス：api　パス：C¥opt¥secioss¥var¥www¥api

2.2.3. LDAPS 通信の設定

Identity Suite Cloud IdP のソフトウェアが LDAPS 通信を行うために、ファイル C:¥openldap¥sysconf¥ldap.conf を作成し、”TLS_REQCERT never”と記述して下さい。

2.3. ID 同期に必要なソフトウェア

2.3.1. ActivePerl のインストール

ActivePerl を http://www.activestate.com/activeperl/downloads/からダウンロードして、インストールして下さい。

次に、以下の Perl モジュールをコマンドプロンプトからインストールして下さい。

- Config-General 、 Config-IniFiles 、 Log-Dispatch 、 Log-Dispatch-FileRotate Class-Inspector、Convert-ASN1、Net-HTTP、Crypt-SSLeay
  ppm install <*パッケージ名*>
  ※ Net-HTTP 6.0.5 以上、Crypt-SSLeay 0.60 以上をインストールして下さい。

3. 設定

3.1. シングルサインオン

SAML の IdP の機能を使用しない場合、設定は不要です。

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

3.1.1. Identity Suite Cloud IdP の設定

展開した secioss-idsuite-cloud-idp-3.x.x の config フォルダに移動して、設定スクリプト config.pl を実行して下さい。

perl config.pl sso

- ホスト名： 本ソフトウェアを導入したサーバの URL
- LDAP サーバ URI： 認証用の Active Directory/LDAP サーバの URI
- LDAP サーバ ベース DN： Active Directory/LDAP サーバのベース DN
- LDAP サーバ ユーザ DN： Active Directory/LDAP サーバに接続するユーザの DN
- LDAP サーバ パスワード： Active Directory/LDAP サーバに接続するパスワード
- 認証方式 [1.ID/パスワード認証 2.統合 Windows 認証]：
  Identity Suite Cloud IdP の認証方式

次に、SAML 認証に使用する PEM 形式の秘密鍵、公開鍵を以下の場所に置いて下さい。

- 秘密鍵：C:¥opt¥secioss¥share¥simplesamlphp¥cert¥PrivateKey.pem
- 公開鍵：C:¥opt¥secioss¥share¥simplesamlphp¥cert¥PublicKey.pem

公開鍵は、SeciossLink の SAML ID プロバイダの設定において登録を行います。

3.1.2. SeciossLink の設定

SeciossLink の管理画面にログインして、「シングルサインオン」->「AD/LDAP 認証(SAML)」とクリックして、以下の項目に設定を行って下さい。

- URL：本ソフトウェアを導入したサーバの URL
- SAML 公開鍵：認証用公開鍵
- パスワード同期：
  Active Directory/LDAP サーバにパスワードを同期する場合「有効」にチェック
- LDAP サーバ ユーザ DN：
  パスワード同期で Active Directory/LDAP サーバに接続するユーザの DN
  （例）cn=Administrator,cn=Users,dc=example,dc=com
- LDAP サーバ パスワード：
  Active Directory/LDAP サーバに接続する際のパスワード

※“LDAP サーバ ユーザ DN”、“LDAP サーバ パスワード”は、“パスワード同期”が有効の場合に設定します。

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

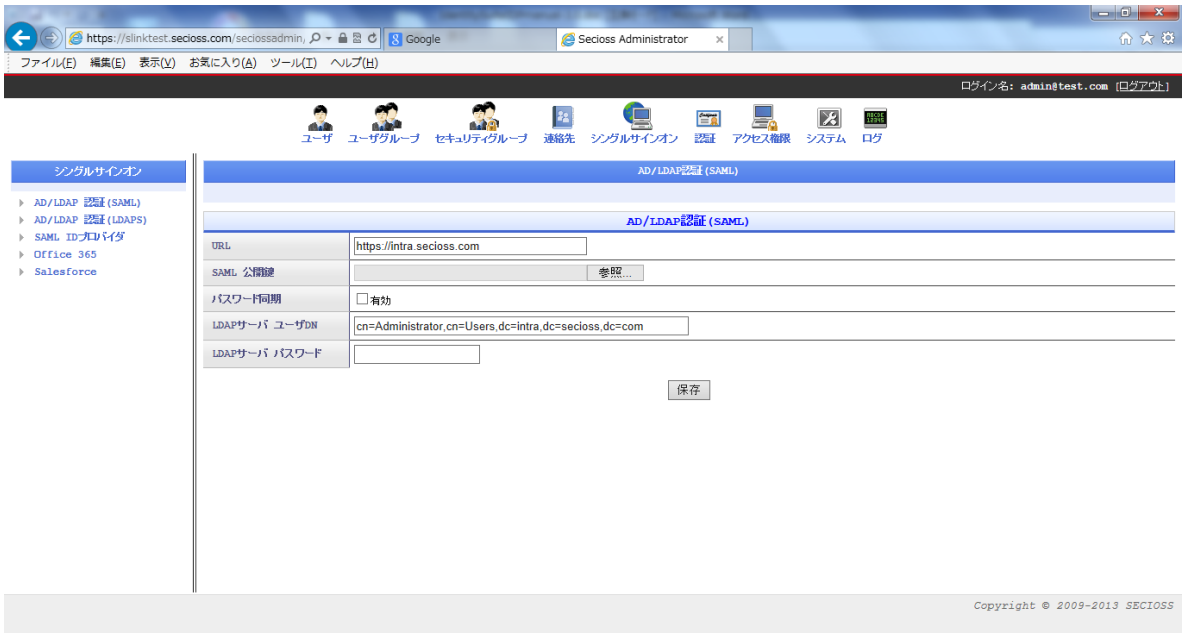

図 2 AD/LDAP 認証(SAML)の設定画面

3.2. ID 同期

3.2.1. ID 同期の設定

展開した secioss-idsuite-cloud-idp-3.x.x の config フォルダに移動して、設定スクリプト config.pl を実行して下さい。

perl config.pl idm

- テナント： テナント ID
- LDAP サーバ URI： ID 同期を行う Active Directory/LDAP サーバの URI
- LDAP サーバ ベース DN： Active Directory/LDAP サーバのベース DN
- LDAP サーバ ユーザ DN： Active Directory/LDAP サーバに接続するユーザの DN
- LDAP サーバ パスワード： Active Directory/LDAP サーバに接続するパスワード
- 送信先ユーザ ID：
  SeciossLink に接続するユーザのユーザ ID（@テナント ID は含みません。）
- 送信先パスワード： SeciossLink に接続するパスワード
- 同期するエントリ[1.組織 2.ユーザグループ 3.セキュリティグループ 4.連絡先]：
  同期を行うエントリの種類（番号をカンマ区切りで指定します。）
- 組織のベース DN： 同期対象とする組織のベース DN
- ユーザグループのベース DN： 同期対象とするユーザグループのベース DN
  例： ou=Groups
- 連絡先のベース DN： 同期対象とする連絡先のベース DN

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

例： ou=Contacts

- 組織から除外する OU： 同期対象外とする OU（カンマ区切りで複数指定できます。）
  例： People,Groups

3.2.2. 同期対象ユーザの設定

LDAP サーバに ID 同期用のグループとして”cn=idsync,ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>”を作成し、同期対象とする LDAP サーバのユーザをそのグループのメンバに登録して下さい。

3.2.3. 管理者権限の設定

管理者権限をユーザに付与する場合、グループ”cn=admin,ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>”を作成し、グループのメンバに対象ユーザを追加して下さい。

3.2.4. 許可するサービスの同期

Google Apps、Office365、Salesforce 等のサービスの利用をユーザに許可する場合、以下のグループを作成して、対象とするユーザをメンバに追加して下さい。

- Google Apps 許可グループ： cn=googleapps,ou=Services,ou=IDsuite, <*LDAP サーバ ベース DN*>
- Office 365 許可グループ： cn=office365,ou=Services,ou=IDsuite,<LDAP サーバ ベース DN>
- cybozu.com 許可グループ： cn=cybozu,ou=Services,ou=IDsuite,<LDAP サーバ ベース DN>
- Salesforce 許可グループ： cn=salesforce,ou=Services,ou=IDsuite, <*LDAP サーバ ベース DN*>

3.2.5. セキュリティグループの同期

SeciossLink のセキュリティグループに対して同期を行う場合、同期対象とするグループは”ou=Security,ou=IDsuite, <*LDAP サーバ ベース DN*>”の配下に作成して下さい。
グループを階層化する場合、下位階層のグループを上位階層のグループのメンバに登録して下さい。ただし、上位階層のグループは必ず１つまでとして下さい。複数のグループのメンバとしてグループを登録した場合、所属するグループの中の１つの配下に同期されます。

3.2.6. サービスのロールの同期

Office 365 のライセンス、管理者ロールや Salesforce のプロファイル等、サービスのロールを同期する場合、”ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>” 配下に以下のよう

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

なグループを作成して、ロールを割り当てるユーザをメンバに追加して下さい。

3.2.6.1. Office 365

・ ライセンス

cn=<ライセンス名>,ou=<Office 365 プラン名>,ou=Office365,ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>

・ 管理者ロール

cn=<管理者ロール名>,ou=管理者ロール,ou=Office365,ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>

3.2.6.2. cybozu.com

・ 利用するサービス

cn=<サービス名>,ou=利用するサービス,ou=Cybozu,ou=Roles,ou=IDsuite,<LDAP サーバ ベース DN>

3.2.6.3. Salesforce

・ プロファイル

cn=<プロファイル名>,ou=プロファイル,ou=Salesforce,ou=Roles,ou=IDsuite,<*LDAP サーバ ベース DN*>

※ Office365 のライセンス名、Office 365 プラン名、管理者ロール名、Salesforce のプロファイル名は、SeciossLink の管理画面のユーザ情報の “Office365 のロール”、“Salesforce のロール” に表示されている値を使用して下さい。

3.2.7. 同期する属性

同期する Active Directory の属性は、以下になります。

エントリの種類	Active Directory の属性	必須	SeciossLink の項目
ユーザ	sAMAccountName	○	ユーザ ID
	employeeNumber		社員番号
	sn	○	姓
	givenName	○	名
	msDS-PhoneticLastName		姓（かな）
	msDS-PhoneticFirstName		名（かな）
	displayName		別名
	mail	○	メールアドレス
	proxyAddresses		メールエイリアス
	c		地域、言語
	userAccountControl	○	ユーザ状態
	company		会社名

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

	department		部署
	title		役職
	physicalDeliveryOfficeName		事業所
	telephoneNumber		電話番号
	facsimileTelephoneNumber		FAX
	mobile		携帯電話番号
	homePhone		自宅電話番号
	co		国
	potalCode		郵便番号
	st		都道府県
	l		市区群
	streetAddress		町名・番地
グループ	sAMAccountName	○	グループ名
	cn	○	表示名
	mail		メールアドレス
	description		説明
	groupType		Office 365 種類
	member		メンバ
組織	ou	○	組織名
	description		説明
連絡先	mail	○	メールアドレス
	sn	○	姓
	givenName	○	名
	msDS-PhoneticLastName		姓（かな）
	msDS-PhoneticFirstName		名（かな）
	displayName		別名
	company		会社名
	department		部署
	title		役職
	physicalDeliveryOfficeName		事業所
	telephoneNumber		電話番号
	facsimileTelephoneNumber		FAX
	mobile		携帯電話番号
	homePhone		自宅電話番号
	co		国

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

	potalCode		郵便番号
	st		都道府県
	l		市区群
	streetAddress		町名・番地

表 1 同期する属性

3.2.8. 同期の実行

同期の実行は、以下のコマンドを実行して下さい。
定期的に同期を行うには、コマンドをタスクに登録して、定期的に実行するようにして下さい。

```
perl c:¥opt¥secioss¥sbin¥idsync idp
```

データの差分チェックの行う場合は、以下のコマンドを実行して下さい。

```
perl c:¥opt¥secioss¥sbin¥idsync –r idp
```

3.2.9. ID 同期における注意事項

- Active Directory のグループ idsync のメンバから外されたユーザは、SeciossLink、および同期対象のサービスから削除されます。
- Active Directory の許可するサービスのグループのメンバから外されたユーザは、該当するサービスからユーザが削除されます。
- Active Directory のサービスのグループのメンバから外されたユーザは、該当するサービスの該当するロールの権限を失います。例えば、Office 365 の“Exchange Online”グループのメンバから外された場合、ユーザは Echange Online を使用できなくなります。
- Active Directory のユーザの sAMAccountName を変更した場合、SeciossLink の“AD/LDAP 認証”では、ID 同期が実行される前、SeciossLink のユーザのユーザ ID に該当するユーザが Active Directory に存在しないため、認証が失敗してしまいます。また、ID 同期を実行した場合、変更前の値をユーザ ID とする SeciossLink のユーザ、および同期対象のサービスのユーザが削除され、変更後の値をユーザ ID とする SeciossLink のユーザ、および同期対象のサービスのユーザが追加されます。
- Office 365 との ID 同期を行っていて、メールアドレスを変更した場合、SeciossLink から Office 365 への ID 同期は 1 時間に 1 回実行されるため、SeciossLink と Office 365 のユーザ ID（SeciossLink のメールアドレス）との間に最大 1 時間不整合が発生している期間があります。この間にメールアドレスを変更したユーザが Office 365 へログ

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

インすると、Office 365 において認証エラーが発生します。

4. ログ

4.1. シングルサインオン

4.1.1. ログファイル

シングルサインオンに関するログは以下のファイルに出力されます。

C:¥opt¥secioss¥share¥simplesamlphp¥log¥simplesamlphp.log

4.1.2. ログメッセージ

メッセージ	説明
<ユーザ ID> successfully authenticated	ユーザ<ユーザ ID>が認証に成功しました。
/saml/saml2/IdP/SSOService.php - UserError: ErrCode:PROCESSAUTHNREQUEST: Unable+to+locate+metadata+for+<*エンティティ ID*>	SeciossLink の<エンティティ ID>がメタデータに存在しません。
/saml/saml2/IdP/SSOService.php - UserError: ErrCode:GENERATEAUTHNRESPONSE: Unable+to+load+private+key	SAML 認証用の秘密鍵が存在しません。
UserError: ErrCode:CONFIG: LDAP+search+returned+zero+entries	LDAP の検索に失敗しました。

表 2 シングルサインオンメッセージ一覧

4.2. ID 同期

4.2.1. ログファイル

ID 同期に関するログは以下のファイルに出力されます。

C:¥opt¥secioss¥var¥log¥lism.log

4.2.2. ログメッセージ

メッセージ	説明
Differential check starting	データの差分チェックを開始しました。 データの差分チェックは以下のコマンドを実行した場合です。

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

	c:¥opt¥secioss¥sbin¥idsync
Differential check finished	データの差分チェックが終了しました。
Data=IDP Object=<*エントリの種類*> Total=<*全件数*> Add=<*追加処理件数*>(<*追加処理の成功件数*> succeeded) Modify=<*変更処理の件数*>(<*変更処理の成功件数*> succeeded) Delete=<*削除処理の件数*>(<*削除処理の成功件数*> succeeded) Error/Skip=<*処理の失敗件数*>	データの差分同期による更新処理の結果です。 エントリの種類にはユーザ(User)、組織(Organization)、ユーザグループ(Group)、セキュリティグループ(SecurityGroup)、連絡先(Contact)があり、差分同期を行ったエントリの種類毎に結果が出力されます。
Binding by <*バインド DN*> failed: [retry="<*リトライ回数*>]." <*エラーの詳細*>	SeciossLink 接続時の認証に失敗しました。 リトライが行われた場合はリトライ回数も表示されます。
Searching by <*検索条件*> at <*検索のベース DN*> failed: [retry="<*リトライ回数*>]." <*エラーの詳細*>	SeciossLink のデータ検索に失敗しました。 リトライが行われた場合はリトライ回数も表示されます。
Adding <*追加したデータの DN*> failed: [retry="<*リトライ回数*>]." <*エラーの詳細*>	SeciossLink へのデータ追加に失敗しました。 リトライが行われた場合はリトライ回数も表示されます。
Modifying <*変更したデータの DN*> failed: [retry="<*リトライ回数*>]." <*エラーの詳細*>	SeciossLink のデータ変更に失敗ました。 リトライが行われた場合はリトライ回数も表示されます。
Deleting <*削除したデータの DN*> failed: [retry="<*リトライ回数*>]." <*エラーの詳細*>	SeciossLink のデータ削除に失敗しました。 リトライが行われた場合はリトライ回数も表示されます。
Searching in IDP failed(81)	SeciossLink のデータ検索に失敗しました。 “3.2.1SeciossLink との接続設定”の設定値が正しいか確認して下さい。
Synchronizing <*データ*> failed(<*エラーコード*>)	<*データ*>に対する更新の同期が失敗しました。
Can't connect <AD *サーバ*>	<*AD サーバ*>に接続できませんでした。 **“エラー! 参照元が見つかりません。** Active Directory との接続設定”の設定値が正しいか確認して下さい。

表 3 ID 同期メッセージ一覧

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

4.2.3. 更新ログファイル

ID 同期の更新に関するログは以下のファイルに出力されます。

C:¥opt¥secioss¥var¥log¥audit.log

4.2.4. ログメッセージ

メッセージ	説明
type=[add|modify|delete] dn=<更新したデータの DN> result=<エラーコード> 属性名>:[+-=]<値>;<値>… <属性名>:…	更新内容のログです。 更新の種類 ・ add：追加 ・ modify：変更 ・ delete：削除 属性の更新の種類 ・ +：追加 ・ -：削除 ・ =：置換

表 4 更新ログメッセージの一覧

4.3. Active Directory/LDAP へのパスワード同期

4.3.1. ログファイル

Active Directory/LDAP へのパスワード同期に関するログは、以下のファイルに出力されます。

C:¥opt¥secioss¥var¥log¥auth.log

4.3.2. ログメッセージ

メッセージ	説明
Can't read config.ini	設定ファイルが読み込めません。
Set password configuration	設定ファイルの設定値が存在しません。
LDAP bind success	Active Directory/LDAP の認証に成功しました。
LDAP bind failed	Active Directory/LDAP の認証に失敗しました。
Parameter error	Active Directory/LDAP 接続ユーザの DN、接続ユーザのパスワードが渡されていません。
Changing password failed: <詳細メッセージ>	パスワードの変更に失敗しました。
Changing password succeeded	パスワードの変更に成功しました。

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

表 3 Active Directory/LDAP へのパスワード同期ログメッセージ一覧

4.3.3. SeciossLink の更新ログに出力されるエラーメッセージ

メッセージ	説明
Bind DN or password is incorrect	Active Directory/LDAP に対する認証に失敗しました。 ※Active Directory/LDAP 接続ユーザの DN、接続ユーザのパスワードが正しいか確認して下さい。
Parameter error	Active Directory/LDAP 接続ユーザの DN、接続ユーザのパスワードが設定されていません。
Not authenticated	Active Directory/LDAPへの認証が行われていません。
Changing password failed: <詳細メッセージ>	パスワードの変更に失敗しました。

表 4 SeciossLink の更新ログに出力されるエラーメッセージ

5. エラーコード

代表的な LDAP のエラーコードとその対応方法です。

エラーコード	エラー内容	対応方法
19	属性値が条件を満たさない値です。	追加、または変更しようとしたデータに SeciossLink の条件を満たさない値が含まれているので、更新内容を確認して下さい。
21	属性値が属性構文に違反した。	追加、または変更しようとしたデータに不正な属性値が含まれているので、更新内容を確認して下さい。
32	エントリが存在しない。	変更、または削除しようとしたエントリが存在していないので、SeciossLink と AD の該当データを確認して下さい。
50	更新の権限がありません。	SeciossLink に接続したユーザにデータの更新権限がありません。該当ユーザに管理者権限が付与されているか、または自身のテナントに AD/LDAP との ID 同期が許可されているか確認

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.

		して下さい。
53	許可されていないデータへの更新を行っています。	自身のテナントで連絡先の使用が許可されていない状態で、連絡先を同期しようとしている可能性があります。
65	オブジェクトクラスに必要な属性がないか、使用できない属性が指定されている。	追加、または変更しようとしたデータ内の属性に過不足があるので、更新内容を確認して下さい。
66	リーフエントリ以外に実行できない更新要求である。	配下にエントリが存在するエントリに対して削除を行おうとしているので、更新内容を確認して下さい。
68	既にエントリが存在している。	追加しようとしたエントリが既に存在しているので、SeciossLink の該当データを確認して下さい。 ユーザを削除後、5 日間経過する前に同一ユーザ ID のユーザを登録しようとした場合、このエラーが発生します。

表 5 エラーコード一覧

Copyright © 2009-2013 SECIOSS Corporation. All rights reserved.