SECIOSS Identity Suite Cloud Edition IdP

AD 連携モジュール Ver. 4.0.0

株式会社セシオス | https://www.secioss.co.jp

目次

1　イントロダクション

SECIOSS Identity Suite Cloud Edition IdP　（以降 IdSuite IdP）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。

IdSuite 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。

- 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
- 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。
  パスワードの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。

IdSuite IdP は、オープンソースとして GPL ライセンスにより公開しています。

- プロジェクトサイト：http://sourceforge.jp/projects/secioss-auth/

技術的な質問は以下にお願いします。

- https://groups.google.com/a/secioss.co.jp/d/forum/slink-users

SeciossLink を試用したい場合は、開発環境を以下から申し込むことができます。

- 開発環境のお申込み ＜ https://www.secioss.co.jp/contact2/ ＞

2 インストール

IdSuite IdP の動作環境は以下のとおりです。

- OS
  Windows Server 2012 Standard/Datacenter
  Windows Server 2012 R2 Standard/Datacenter
  Windows Server 2016 Standard/Datacenter

- 有効にする機能
  Web サーバー(IIS)
  アプリケーション開発
  CGI

- ミドルウェア
  Strawberry Perl 5.16.3 < http://strawberryperl.com/ >
  PHP 5.4.44 < http://jp2.php.net/ >

2.1 SECIOSS Identity Suite Cloud Edition IdP 展開

1. secioss-idsuite-cloud-idp-4.x.x.zip を展開して、opt フォルダーを C:¥opt として配置して下さい。
2. C:¥opt¥secioss の[プロパティ] ⇒ [セキュリティ]から、IUSR と Users に対してのアクセス許可を付与して下さい。
3. 以下のフォルダーには IUSR と Users に対してのフルコントロールのアクセス許可を付与して下さい。
   C:¥opt¥secioss¥share¥simplesamlphp¥log
   C:¥Windows¥Temp

2.2 シングルサインオンに必要なソフトウェア及び設定

※SAML の IdP の機能を使用しない場合、本節の設定は不要です。

2.2.1 PHP

1. PHP の Windows binary zip ファイルをダウンロードして、C:¥php に配置して下さい。
2. php.ini-production ファイルを php.ini にリネームして下さい。
3. php.ini ファイルの以下の行をコメントインまたは追記して下さい。

```
error_log = /php/php_errors.log
extension_dir = "ext"
extension=php_ldap.dll
extension=php_openssl.dll
date.timezone = Asia/Tokyo
session.save_path = "/php/tmp"
```

4. 以下のフォルダーを作成してください。
   C:¥php¥pear
   C:¥php¥tmp
5. 以下のフォルダーには IUSR と Users に対してのフルコントロールのアクセス許可を付与して下さい。
   C:¥php

2.2.2 LDAPS 通信設定

IdSuite 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、以下の内容で記述して下さい。

```
TLS_REQCERT never
```

2.2.3 Strawberry Perl のインストール

1. Strawberry Perl をダウンロードし、インストールして下さい。
2. Perl command line を開き、以下のコマンドを実行して、CPAN から Perl モジュールをインストールして下さい。

```
cpan Config::General
cpan Config::IniFiles
cpan Log::Dispatch
cpan Log::Dispatch::FileRotate
cpan Class::Inspector
cpan Convert::ASN1
cpan Net::HTTP
cpan Crypt::SSLeay
```

2.2.4 **IIS マネージャー設定**

1. インターネットインフォメーションサービス(IIS)マネージャーを起動し、以下の仮想ディレクトリを作成し、設定して下さい。

   - SAML IdP
     エイリアス：saml
     パス：C:¥opt¥secioss¥share¥simplesamlphp¥www
     ※ 統合 Windows 認証を行う場合、パス"saml/auth"の Windows 認証を有効に設定して下さい。
   - 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. ハンドラーマッピングから"モジュールマップの追加"を選択し PHP モジュールの追加を行ってください。

設定項目	設定内容
要求パス	*.php
モジュール	FastCgiModule
実行可能ファイル	C:¥php¥php-cgi.exe
名前	PHP

表 1 PHP モジュールの追加設定項目

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。

3.1.1 SSO 設定スクリプト

1. 展開した secioss-idsuite-cloud-idp-4.x.x の conf フォルダーに移動して、設定スクリプト config.pl を実行して下さい。

```
perl config.pl sso
```

実行後の入力設定内容は以下のようになります。

設定項目	設定内容
ホスト名	本ソフトウェアを導入したサーバの URL (例) https://idp.example.com
LDAP サーバ URI	認証用の Active Directory/LDAP サーバの URI (例) ldaps://idp.example.com
LDAP サーバ ベース DN	Active Directory/LDAP サーバのベース DN (例) DC=idp,DC=example,DC=com
LDAP サーバ ユーザ DN	Active Directory/LDAP サーバに接続するユーザの DN (例) CN=Administrator,CN=Users,DC=idp,DC=example,DC=com
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]	IdSuite IdP の認証方式

表 2 SSO スクリプト設定項目

2. SAML 認証に使用する PEM 形式の秘密鍵、公開鍵を以下のフォルダーに配置して下さい。
   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。

   PrivateKey.pem/PublicKey.pem は Linux 上にて以下のようなコマンドで作成可能です。

```
openssl genrsa 2048 > PrivateKey.pem
openssl req -new -x509 -key PrivateKey.pem -out PublicKey.pem -days 3650 ¥
        -subj "/C=JP/ST=Tokyo/L=Shinjuku-ku/O=SECIOSS, Inc./CN=Example"
```

3.1.2 SeciossLink 側設定

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。

設定項目	設定内容
URL	本ソフトウェアを導入したサーバの URL (例) https://idp.example.com
SAML 公開鍵	前項で設定した PublicKey.pem
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 ※"パスワード同期"が有効の場合、"LDAP サーバ ユーザ DN"、"LDAP サーバ パスワード"設定します。
LDAP サーバ ユーザ DN	Active Directory/LDAP サーバに接続するユーザの DN (例) CN=Administrator,CN=Users,DC=idp,DC=example,DC=com
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

表 3 AD/LDAP 認証(SAML)設定項目

3.2 シングルサインオン(マルチフォレスト構成)

マルチフォレスト構成で統合 Windows 認証を行う場合、複数存在する Active Directory 毎に IdSuite IdP を導入するとともに、ユーザを認証先の IdSuite IdP に振り分けるサービス（以降ディスカバリーサービス）を導入する必要があります。

ディスカバリーサービスが動作するサーバは全ユーザからアクセス可能であることが必要です。単独のサーバとして動作させること可能で、Active Directory に導入した IdSuite IdP と同居することも可能です。

3.2.1 ディスカバリーサービス設定

ディスカバリーサービスが動作するサーバに IdSuite IdP をインストールして下さい。
"/opt/secioss/share/simplesaml/config/config.php"の$config に idplist の設定を追加して下さい。

idplist には、ユーザのアクセス元 IP アドレス（正規表現での指定が可能です）と認証先の IdSuite IdP のログイン URL を対にして設定して下さい。

以下の例では、"192.168.1.*"に一致する IP アドレスからのアクセスは"https://idp1.example.com"に、それ以外の IP アドレスからのアクセスは"https://idp2.example.com"にユーザを振り分けます。

```
'idplist' =>array(
    'LOCATION 1' => array(
        'ip'   => '192¥.168¥.1¥..*',
        'url' => 'https://idp1.example.com/saml/saml2/idp/SSOService.php'
    ),
    'LOCATION 2' => array(
        'ip' => '.*',
        'url'=> 'https://idp2.example.com/saml/saml2/idp/SSOService.php'
    ),
),
```

ユーザのアクセス元 IP アドレスが、idplist に設定した IP アドレスに合致しなかった場合、idplist に設定してあるサーバから認証先を選択する画面が表示されます。例の設定では、"LOCATION 1", "LOCATION 2" の選択表示となります。1 回認証先のサーバに割り振られると、同じブラウザを使用している間は 30 日間同じ認証先に割り振られます。

3.2.2 SSO 設定スクリプト

設定は“3.1.1SSO 設定スクリプト”に従って行って下さい。

なお、“ホスト名”には、ディスカバリーサービスが動作するサーバの URL を設定して下さい。

3.2.3 SeciossLink 側設定

SeciossLink の管理画面にログインして、「シングルサインオン」⇒「SAML ID プロバイダ)」とクリックして、以下の項目に設定を行って下さい。

設定項目	設定内容
エンティティ ID	ディスカバリーサービスのサーバの URL
ログイン URL	<ディスカビリサービスのサーバの URL>/saml/iwadiscovery.php
ログアウト URL	<ディスカビリサービスのサーバの URL>/saml/iwamultilogout.php
送信するエンティティ ID	“テナント固有のエンティティ ID”にチェックしない
ID の属性	ユーザ ID
SAML 公開鍵	認証用公開鍵

表 4 SAML ID プロバイダ設定項目

3.3 ID 同期

3.3.1 同期設定スクリプト

展開した secioss-idsuite-cloud-idp-4.x.x の conf フォルダーに移動して、設定スクリプト config.pl を実行して下さい。

```
perl config.pl idm
```

実行後の入力設定内容は以下のようになります。

設定項目	設定内容
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 (例) ldaps://idp.example.com
LDAP サーバ ベース DN	Active Directory/LDAP サーバのベース DN (例) DC=idp,DC=example,DC=com
LDAP サーバ ユーザ DN	Active Directory/LDAP サーバに接続するユーザの DN (例) CN=Administrator,CN=Users,DC=idp,DC=example,DC=com
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）
組織のベース DN	同期対象とする組織のベース DN (例) ou=Organizations
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 (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可能） (例)　People,Groups

表 5 ID 同期スクリプト設定項目

「3.2」マルチフォレスト構成の場合、以下のオプション”multi”で実行し、２台目 LDAP を設定してください。

```
perl config.pl idm multi
```

SeciossLink の“AD/LDAP 認証（LDAPS）”の認証を行う場合、展開したパッケージ内 C:¥opt¥secioss¥etc¥lism-idp.conf にある <!--- LDAP AUTH … ---> のコメントアウトを外して SeciossLink の“AD/LDAP 認証（LDAPS）”で設定した 1 台目、2 台目の LDAP サーバの URI で、それぞれ LDAPAUTH_URI1、LDAPAUTH_URI2 を置き換えて下さい。

3.3.2 Active Directory 側同期用ツリー構成

Active Directory から SeciossLink へ ID を同期させる場合、Active Directory 全体でなく、同期対象のユーザ、セキュリティグループ、連絡先などを同期グループとしたツリー構造の作成が必要です。ID 同期及び各サービス同期用のツリー構成は表 3、表 4 を参照して作成してください。ツリーの DN 内容は大小文字区別するので、ご注意ください。

同期対象（SeciossLink 側）	以下同期用セキュリティグループ（AD 側）を作成
ユーザ	“cn=idsync,ou=Roles,ou=IDsuite,<*LDAP* サーバ ベース *DN*>” を作成し、グループのメンバとして対象ユーザを登録
組織	設定スクリプト「同期するエントリ」項目の選択設定が必要。 表 2 [組織のベース DN]で設定した DN 配下の組織(ou)が同期対象
ユーザグループ	設定スクリプト「同期するエントリ」項目の選択設定が必要。 表 2 [ユーザグループのベース DN]で設定した DN 配下のグループ（cn）が同期対象
連絡先	設定スクリプト「同期するエントリ」項目の選択設定が必要。 表 2 [連絡先のベース DN]で設定した DN 配下の連絡先(cn)が同期対象
SeciossLink セキュリティグループ※	設定スクリプト「同期するエントリ」項目の選択設定が必要。 “**ou=SecurityGroups,ou=IDsuite**, <*LDAP* サーバ ベース *DN*>” を作成し、配下に同期対象とするグループを作成する
管理者権限	“cn=admin,ou=Roles,ou=IDsuite,<*LDAP* サーバ ベース *DN*>” を作成し、グループのメンバとして対象ユーザを登録

表 6 ID 同期ツリー作成

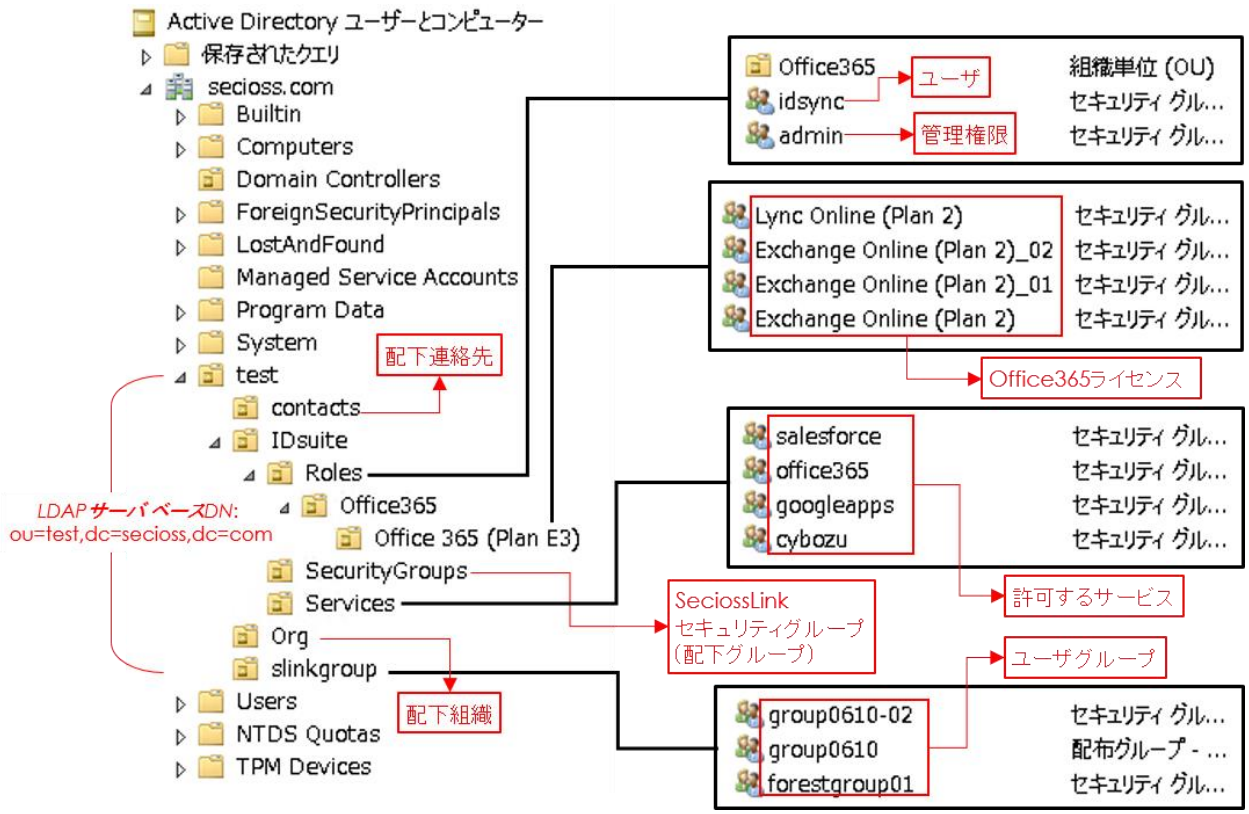
※ SeciossLink セキュリティグループは SeciossLink 特有のアクセス制御用グループで、その他のシステムで定義した“セキュリティグループ”とは異なります。SeciossLink セキュリティグループを階層化する場合、下位階層のグループを上位階層のグループのメンバに登録して下さい。ただし、上位階層のグループは必ず 1 つまでとして下さい。複数のグループのメンバとしてグループを登録した場合、所属するグループの中の 1 つの配下に同期されます。

許可するサービス	以下セキュリティさグループを作成し、サービスを許可するユーザをメンバとして登録
GoogleApps	cn=googleapps,ou=Services,ou=IDsuite, <*LDAP* サーバ ベース *DN*>

Office365	cn=office365,ou=Services,ou=IDsuite,<LDAP サーバ ベース DN>
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*>
※ Office365 のライセンス名、プラン名、管理者ロール名は、SeciossLink の管理画面のユーザ情報の"Office365 のロール"に表示されている値を使用して下さい。	
Salesforce	cn=salesforce,ou=Services,ou=IDsuite, <*LDAP* サーバ ベース *DN*>
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*>
※ Salesforce のプロファイル名は、SeciossLink の管理画面のユーザ情報の"Salesforce のロール"に表示されている値を使用して下さい。	
cybozu.com	cn=cybozu,ou=Services,ou=IDsuite,<LDAP サーバ ベース DN>
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>

表 7 許可サービス同期ツリー作成

一般的な Active Directory 同期用のツリー構成は図の設定例を参考してください。



3.3.3 同期する Active Directory 属性一覧

Active Directory と SeciossLink と ID 同期を行う際、以下の属性がマッピングされます。必須属性に値が空の場合、同期エラーになりますので、ご注意ください。

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
	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

	msExchHideFromAddressLists		アドレス帳表示
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
	msExchHideFromAddressLists		アドレス帳表示
	msExchRequireAuthToSendTo		組織内のユーザのみこのグループへのメール送信を許可
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
	potalCode		郵便番号
	st		都道府県
	l		市区群

	streetAddress		町名・番地

表 8 Active Directory 同期属性一覧

3.3.4 **同期実行**

同期の実行は、以下のコマンドを実行して下さい。マルチフォレスト構成の場合、オプション”-m” を付けてください。同期を行う前に、データの差分チェックのみを行うことをお勧めします。同期内容を確認後、同期を実行してください。

自動同期を行うには、コマンドをタスクに登録し、定期的に実行するようにして下さい。

```
:: 差分チェック
perl c:¥opt¥secioss¥sbin¥idsync –r idp

:: フォレスト構成の差分チェック
perl c:¥opt¥secioss¥sbin¥idsync –r –m idp

:: 同期実行
perl c:¥opt¥secioss¥sbin¥idsync idp

:: 同期実行(エラーをスキップ)
perl c:¥opt¥secioss¥sbin¥idsync -C idp

:: フォレスト構成の同期実行
perl c:¥opt¥secioss¥sbin¥idsync –m idp
```

3.3.5 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、ユーザの Echange Online 使用ができなくなります。
- Active Directory のユーザの sAMAccountName を変更した場合、認証が失敗してしまいます。SeciossLink の"AD/LDAP 認証"では、ID 同期が実行される前、SeciossLink のユーザ ID に該当するユーザが Active Directory に存在しないと判断するため、認証が失敗します。
  また、ID 同期を実行した場合、変更前の sAMAccountName をユーザ ID とした SeciossLink ユーザが削除され、変更後の sAMAccountName を新しいユーザ ID として SeciossLink 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 同期を行う後、メールアドレスを変更した場合、SeciossLink から Office 365 への ID 同期は最大 45 分/回で実行されるため、SeciossLink と Office 365 のユーザ ID（SeciossLink のメールアドレス）との間に最大 45 分の不整合が発生する期間があります。この間にメールアドレスを変更したユーザが Office 365 へログインすると、Office 365 において認証エラーが発生します。
- フォレスト構成の場合、同期する Active Directory とのパスワード同期はできません。

4 ログ

シングルサインオン及び ID 同期を行う際のログが Active Directory に保存されています。

4.1 シングルサインオン

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

各ログメッセージは以下の表に示します。

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 9 SSO ログメッセージ

4.2 **ID 同期**

ID 同期に関するログは同期ログと更新ログの 2 種類が出力されます。

4.2.1 **同期ログ**

同期ログは C:¥opt¥secioss¥var¥log¥lism.log ファイルに出力されます。ログメッセージは以下の表に説明します。

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。 差分チェックは以下のコマンドを実行した場合 c:¥opt¥secioss¥sbin¥idsync –r
Differential check finished	データの差分チェックが終了
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: 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,リトライ回数表示されます。
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,リトライ回数表示されます。
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,リトライ回数表示されます。
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,リトライ回数表示されます。
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リトライ回数表示されます。
Searching in IDP failed(81)	SeciossLink のデータ検索に失敗しました。 “3.3.1 同期設定スクリプト”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 10 同期ログメッセージ

4.2.2 **更新ログ**

更新に関するログは以下のファイルに出力されます。ログメッセージは以下の表に示します。

C:¥opt¥secioss¥var¥log¥audit.log

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 11 更新ログメッセージ

4.3 **Active Directory へのパスワード同期**

Active Directory/LDAP へのパスワード同期に関するログは、ファイル C:¥opt¥secioss¥var¥log¥auth.log に出力されます。ログメッセージに関しては以下の表に示します。

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、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。

表 12 AD パスワード同期ログメッセージ

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 13 エラーコード対応

SeciossLink の更新ログに出力されるエラーメッセージは以下の表に示します。

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 14 SeciossLink 更新ログエラーメッセージ