



GakuNin はIDaaSで。

学術情報基盤オープンフォーラム2016
株式会社セシオス

会社紹介

▲ 株式会社セシオス

設立	2007年5月
資本金	1,300万円
代表取締役	関口 薫
住所	東京都新宿区山吹町365 4F
事業内容	認証・統合ID管理ソフトウェア、サービスの開発、販売 システムインテグレーションサービス
取得資格	プライバシーマーク 取得日 : 2012年10月29日 認定番号 : 17001332

認証・ID管理をコアテクノロジーとしながら、学認や連携先クラウドサービスに対するナレッジを持っている会社です。

製品・ソリューション

▲ 統合ID管理ソフトウェア

▲ Secioss **Identity Manager Enterprise**

- ▲ ID情報や権限情報を連携するシステムに伝播
- ▲ クラウドサービスへの連携も可能

▲ シングルサインオン・アクセス管理ソフトウェア

▲ Secioss **Access Manager Enterprise**

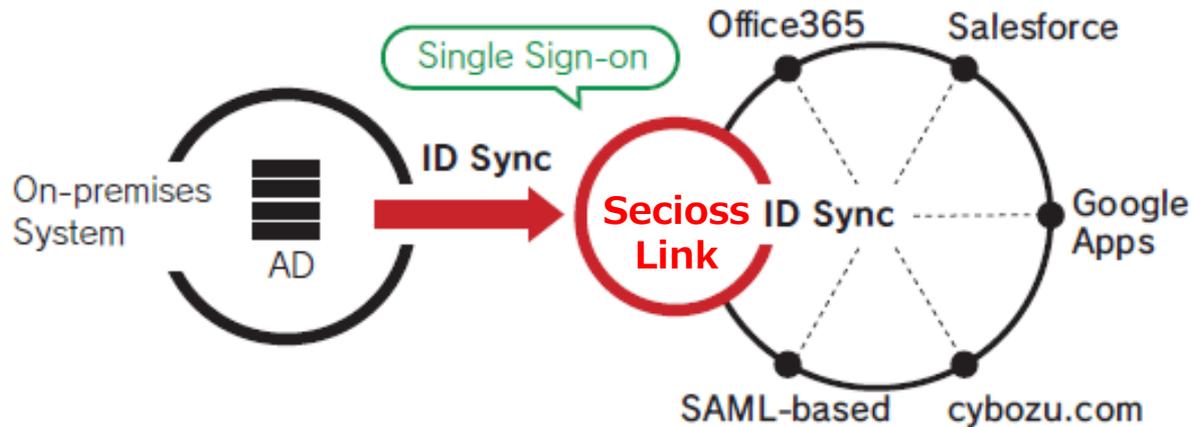
- ▲ SSO、多要素認証、アクセス制御が可能
- ▲ クラウドサービスからオンプレミスシステムとのSSOも可能

▲ IDaaSサービス

▲ Secioss**Link**

- ▲ 統合ID、認証機能を備えたクラウドサービス

ID as a Service **SeciossLink**



ID連携可能なサービス

GoogleApps
Office365
cybozu.com
Salesforce
Dropbox

SSO可能なサービス

学認
GoogleApps
Office365
cybozu.com
Salesforce
Dropbox
SAML対応サービス
SAML未対応サービス
リバースプロキシ方式連携

認証方式

ID/パスワード
証明書認証
ワンタイムパスワード
統合Windows認証
OAuth/OpenID Connect
WS-Federation
端末制限認証
リスクベース認証
FIDO U2F認証

アクセス制限

IPアドレス制限
ユーザ・グループ単位での制限
時間帯による制限

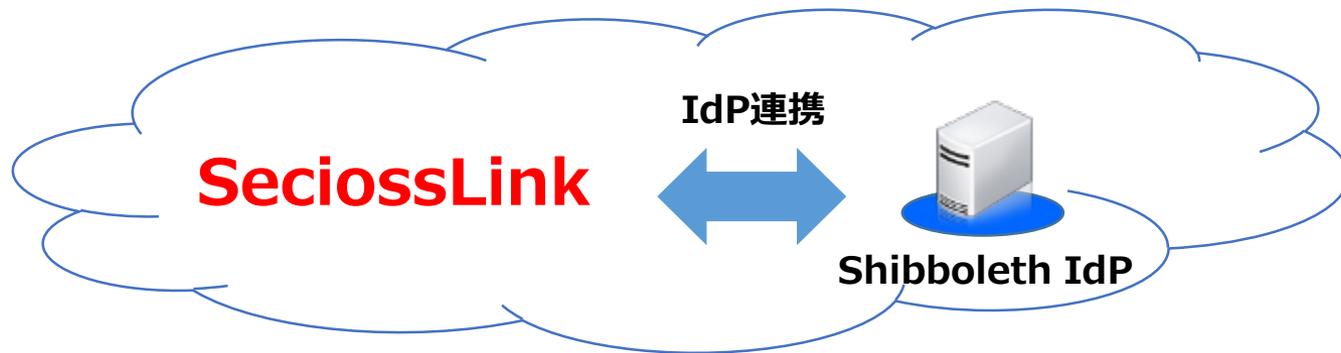
その他便利な機能

統合ID管理機能
パスワードリセット機能
SSOポータル

SeciossLinkからオンプレミスのAD/LDAPに対して情報を同期
ユーザ自身が登録したメールアドレスにパスワードリセット通知を送付
ユーザ専用のポータルサイト

学認連携の経緯

- ▲ 2年ほど前は SeciossLink サービスのフロントにShibboleth IdPを構築、マルチテナント化して学認SPと連携するサービスを行っていました。



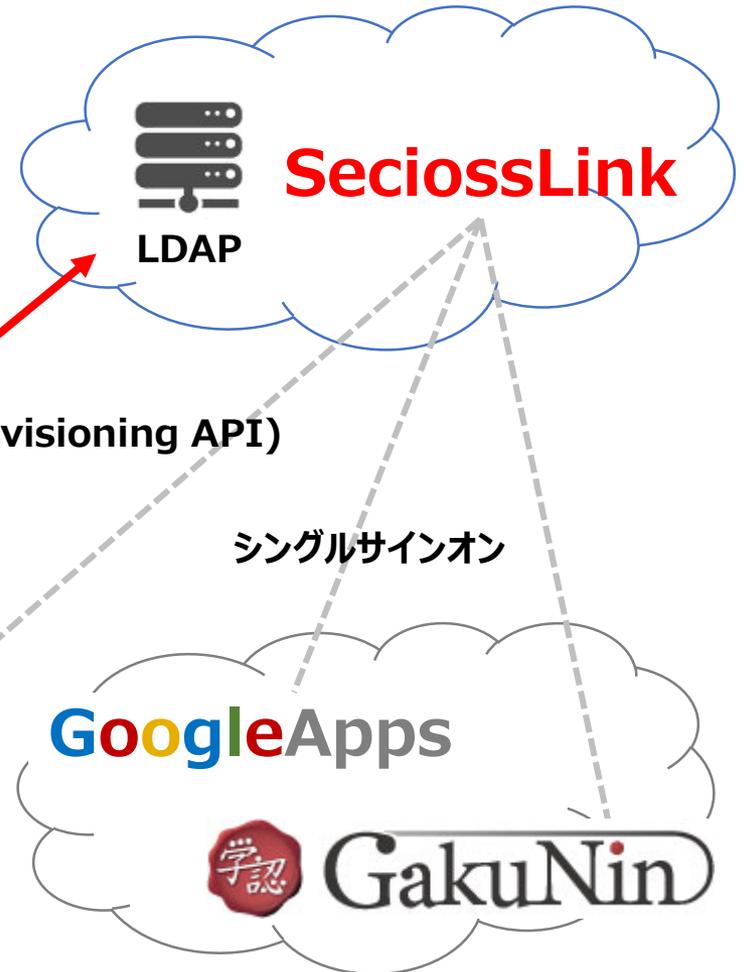
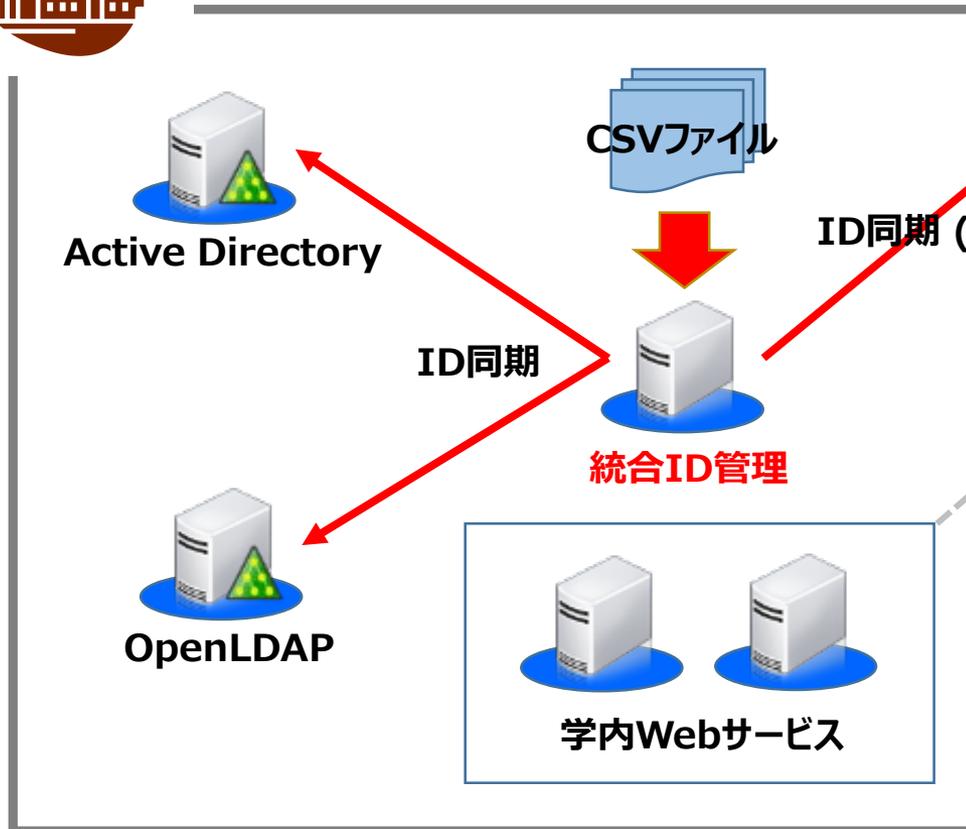
IdP連携により、SeciossLinkが持つ多要素認証機能やアクセス制御の機能を利用できますが、Shibboleth IdPは顧客ごとに設定ファイルを作成、パスを分けるなどの設定を弊社側で、全て手動で行う仕組みでした。
これでは大変だと思い・・・

- ▲ 昨年、サービス本体に学認SPと連携する機能を実装。SeciossLink 本来の使い方(WebGUIからの設定)で、学認SPと連携できるようになりました。

事例：構成



国立大学法人 上越教育大学 様



学認SP設定画面



シングルサインオン | SAMLサービスプロバイダ

サービスプロバイダ設定

サービスプロバイダ																													
サービスID	testsp1																												
サービス名*	学認テストフェデレーション																												
エンティティID*	https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp																												
Assertion Consumer Service	https://test-sp1.gakunin.nii.ac.jp/Shibboleth.sso/ 追加																												
ログアウトURL	<input type="text"/> <input type="checkbox"/> ログアウトの署名																												
アクセス先URL	<input type="text"/>																												
IDの属性	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent																												
ユーザIDの属性	ユーザID																												
送信する属性	<table border="1"><tbody><tr><td><input checked="" type="checkbox"/> ユーザID</td><td>属性名 seccrossSystemid</td></tr><tr><td><input checked="" type="checkbox"/> ユーザIDテナントID</td><td>属性名 urn:oid:1.3.6.1.4.1.5923.1.1.1.6</td></tr><tr><td><input checked="" type="checkbox"/> メールアドレス</td><td>属性名 urn:oid:0.9.2342.19200300.100.1.3</td></tr><tr><td><input type="checkbox"/> 社員番号</td><td>属性名 employeeNumber</td></tr><tr><td><input checked="" type="checkbox"/> 姓</td><td>属性名 urn:oid:1.3.6.1.4.1.32264.1.1.1</td></tr><tr><td><input checked="" type="checkbox"/> 名</td><td>属性名 urn:oid:1.3.6.1.4.1.32264.1.1.2</td></tr><tr><td><input checked="" type="checkbox"/> 別名</td><td>属性名 urn:oid:1.3.6.1.4.1.32264.1.1.3</td></tr><tr><td><input type="checkbox"/> 組織</td><td>属性名 ou</td></tr><tr><td><input type="checkbox"/> 地域</td><td>属性名 seccrossLocaleCode</td></tr><tr><td><input type="checkbox"/> 言語</td><td>属性名 preferredLanguage</td></tr><tr><td><input type="checkbox"/> ユーザグループ</td><td>属性名 seccrossGroup</td></tr><tr><td><input type="checkbox"/> セキュリティグループ</td><td>属性名 seccrossSecurityGroup</td></tr><tr><td><input checked="" type="checkbox"/></td><td>属性名</td></tr><tr><td><input checked="" type="checkbox"/></td><td>属性名</td></tr></tbody></table>	<input checked="" type="checkbox"/> ユーザID	属性名 seccrossSystemid	<input checked="" type="checkbox"/> ユーザIDテナントID	属性名 urn:oid:1.3.6.1.4.1.5923.1.1.1.6	<input checked="" type="checkbox"/> メールアドレス	属性名 urn:oid:0.9.2342.19200300.100.1.3	<input type="checkbox"/> 社員番号	属性名 employeeNumber	<input checked="" type="checkbox"/> 姓	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.1	<input checked="" type="checkbox"/> 名	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.2	<input checked="" type="checkbox"/> 別名	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.3	<input type="checkbox"/> 組織	属性名 ou	<input type="checkbox"/> 地域	属性名 seccrossLocaleCode	<input type="checkbox"/> 言語	属性名 preferredLanguage	<input type="checkbox"/> ユーザグループ	属性名 seccrossGroup	<input type="checkbox"/> セキュリティグループ	属性名 seccrossSecurityGroup	<input checked="" type="checkbox"/>	属性名	<input checked="" type="checkbox"/>	属性名
<input checked="" type="checkbox"/> ユーザID	属性名 seccrossSystemid																												
<input checked="" type="checkbox"/> ユーザIDテナントID	属性名 urn:oid:1.3.6.1.4.1.5923.1.1.1.6																												
<input checked="" type="checkbox"/> メールアドレス	属性名 urn:oid:0.9.2342.19200300.100.1.3																												
<input type="checkbox"/> 社員番号	属性名 employeeNumber																												
<input checked="" type="checkbox"/> 姓	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.1																												
<input checked="" type="checkbox"/> 名	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.2																												
<input checked="" type="checkbox"/> 別名	属性名 urn:oid:1.3.6.1.4.1.32264.1.1.3																												
<input type="checkbox"/> 組織	属性名 ou																												
<input type="checkbox"/> 地域	属性名 seccrossLocaleCode																												
<input type="checkbox"/> 言語	属性名 preferredLanguage																												
<input type="checkbox"/> ユーザグループ	属性名 seccrossGroup																												
<input type="checkbox"/> セキュリティグループ	属性名 seccrossSecurityGroup																												
<input checked="" type="checkbox"/>	属性名																												
<input checked="" type="checkbox"/>	属性名																												

認証に必要な情報の設定

送信属性マッピング

現状、属性名には値を入力する必要がありますが、今後はテンプレートや選択方式で利用できるようにしたい。

シングルサインオン | SAMLサービスプロバイダ

設定

設定	
メタデータの自動更新	URL: <input type="text"/>
ユーザ同意取得	<input type="checkbox"/> 有効 <input type="checkbox"/> 属性値の更新後に再度同意を取得
Targeted IDを生成するソルト	<input type="text"/>

保存

メタデータ自動更新機能

送信属性同意機能

承認情報はサービス側で保持しています。

多要素認証・アクセス制御

- ▲ 学認SPログイン時、多要素認証が利用できます。
 - ▲ Office365は「ID/Pass」でログイン
 - ▲ CiNiiは「ID/Pass」+「証明書」でログイン
- ▲ ユーザ・グループ単位・SP単位でアクセス制御可能です。
 - ▲ Office365は学生(グループ)のみ利用可
 - ▲ CiNiiは教職員・院生(グループ)のみ利用可

【認証ルールの設定】

The screenshot shows a web interface for configuring authentication rules. At the top, there is a field for 'ID' with the value 'Login'. Below this, there are two columns: '認証方法一覧' (List of authentication methods) and '選択した認証方法' (Selected authentication methods). The 'List of authentication methods' column contains a scrollable list of options including 'ID/パスワード認証', 'SAML認証', '証明書認証', 'ワンタイムパスワード', 'ワンタイムパスワード(PIN確認)', 'ワンタイムパスワード(メール認証)', 'U2F認証', 'スマートフォン認証', 'PC端末認証', 'リッチクライアント端末認証', 'AD/LDAP認証(外部ユーザ)', '統合Windows認証(外部ユーザ)', 'AD/LDAP認証(SAML)', 'AD/LDAP認証(LDAPS)', '統合Windows認証', 'アクセスキー認証', and 'アクセスキー確認'. The 'Selected authentication methods' column currently shows 'ID/パスワード認証' and 'ワンタイムパスワード'. At the bottom, there are buttons for '追加 AND>', '追加 OR>', and '削除'.

【アクセス制御の設定】

The screenshot shows a web interface for configuring access control. It has a title 'ネットワークの設定' (Network Settings). There are two main sections: 'IPアドレス' (IP Address) and 'ネットワークアドレス' (Network Address). Each section has an input field and a list of instructions. For 'IPアドレス', the instructions are: '● IPアドレスはカンマ区切りで複数指定することができます。先頭に"|"を付加すると指定したIPアドレス以外のIPアドレスに合致します。例: (192.168.1.1, 192.168.100.1)'. For 'ネットワークアドレス', the instructions are: '● ネットワークアドレスはカンマ区切りで複数指定することができます。先頭に"|"を付加すると指定したネットワークアドレス以外のネットワークアドレスに合致します。例: (192.168.1.0/24, 192.168.100.0/24)'. At the bottom right, there is a blue button labeled '更新' (Update).

送信属性同意画面

サービスに送信する情報

アクセスしようとしているサービス: gakunin 02

属性名	値
<input checked="" type="checkbox"/> ユーザID	test001@test.com
<input checked="" type="checkbox"/> 姓	テスト
<input checked="" type="checkbox"/> 名	一郎
<input checked="" type="checkbox"/> 職種	学生

上の情報はこのサービスを利用するために必要です。このサービスにあなたの情報を送信することに同意しますか？

今後は自動的にこの情報を送信する

同意する

拒否する

サービス利用のメリット

- ▲ クラウドサービスですので、HW不要、申し込み後、直ぐに利用できます。
- ▲ サービス基盤は冗長化されており、バックアップを定期的に取り得しているため、障害やサービス停止のリスクを低減できます。
- ▲ 設定は全てWebGUIから行うことができますので、SPの追加が比較的容易です。



サービスを利用することで、初期コスト、
運用コストを削減することができます。

とはいえ・・・年間サービス利用料はかかりますのでご注意を。

ご清聴ありがとうございました。



<http://www.secioss.co.jp>