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

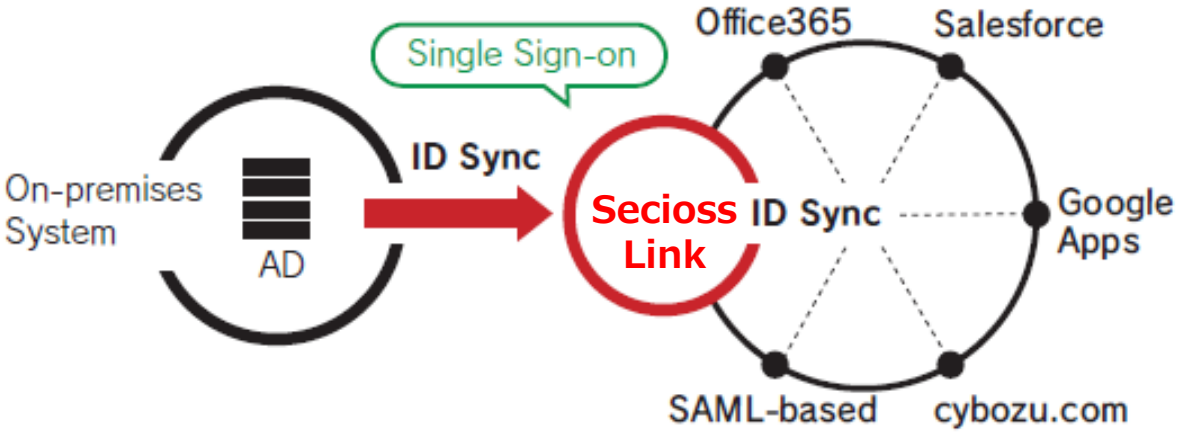
設立	2007年5月
資本金	1,300万円
代表取締役	関口　薫
住所	東京都新宿区山吹町365 4F
事業内容	認証・統合ID管理ソフトウェア、サービスの開発、販売 システムインテグレーションサービス
取得資格	プライバシーマーク 取得日　：　2012年10月29日 認定番号　：　17001332

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
  - **SeciossLink**
  - 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

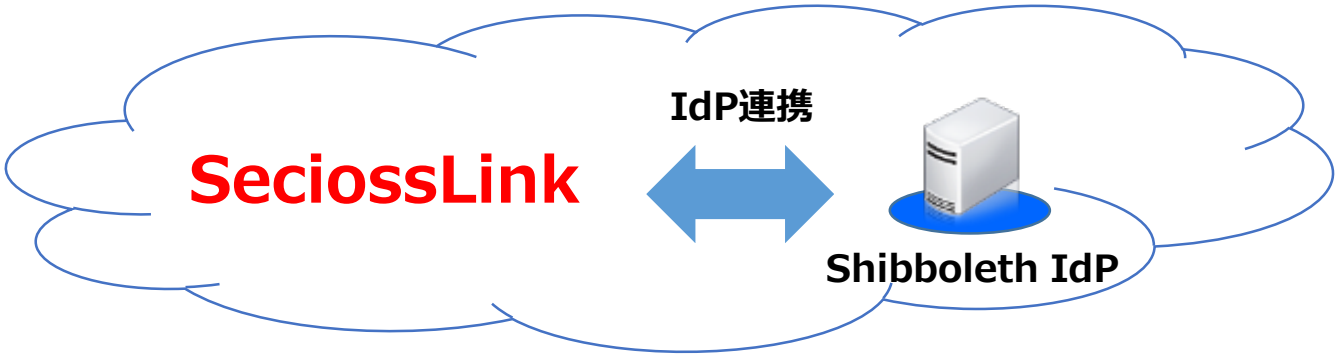
IPアドレス制限
ユーザ・グループ単位での制限
時間帯による制限

その他便利な機能

統合ID管理機能	SeciossLinkからオンプレミスのAD/LDAPに対して情報を同期
パスワードリセット機能	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
SSOポータル	ユーザ専用のポータルサイト

学認連携の経緯

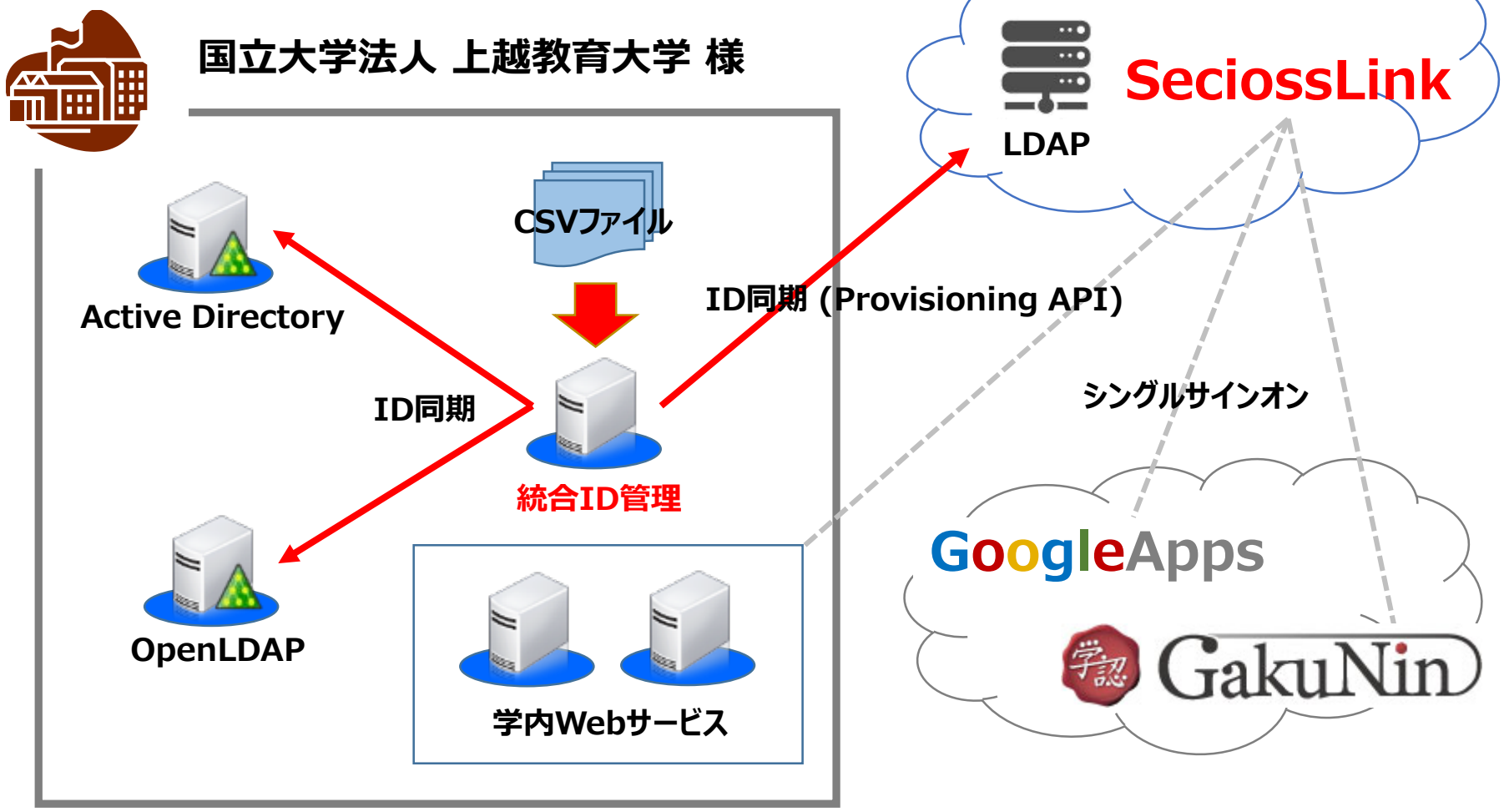
- 2年ほど前は SeciossLink サービスのフロントにShibboleth IdPを構築、マルチテナント化して学認SPと連携するサービスを行っていました。



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
Active Directory
CSVファイル
ID同期
統合ID管理
OpenLDAP
学内Webサービス
ID同期 (Provisioning API)
LDAP
SeciossLink
シングルサインオン
GoogleApps
GakuNin

学認SP設定画面

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。

メタデータ自動更新機能

送信属性同意機能

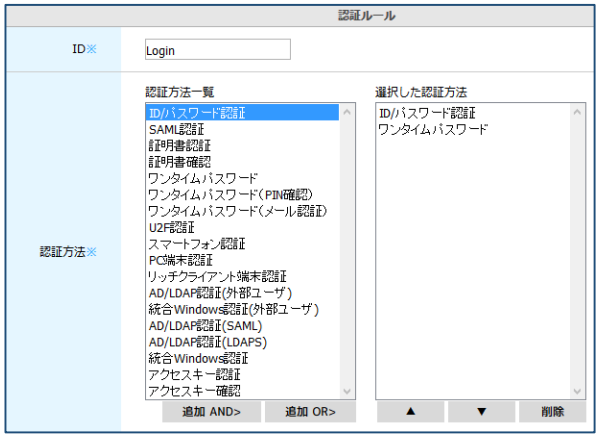
承認情報はサービス側で保持しています。

多要素認証・アクセス制御

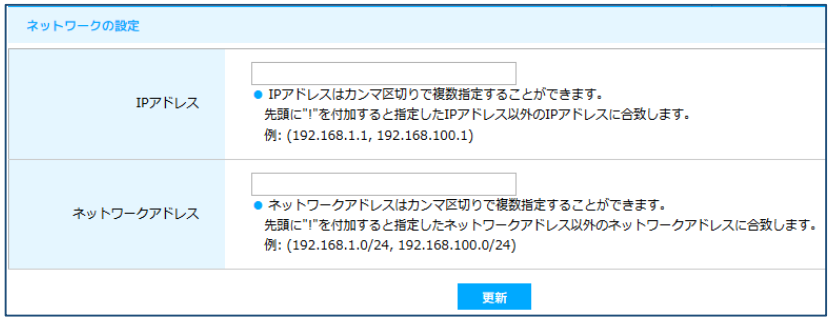
- 学認SPログイン時、多要素認証が利用できます。
  - Office365は「ID/Pass」でログイン
  - CiNiiは「ID/Pass」+「証明書」でログイン

- 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】



【アクセス制御の設定】



送信属性同意画面


SECIOSS SeciossLink
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
ユーザID
test001@test.com
姓
テスト
名
一郎
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
Copyright © SECIOSS CORP. All rights reserved.

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。

株式会社セシオス

http://www.secioss.co.jp