IDaaSは学認アンケートに耐えられるのか

学術情報基盤オープンフォーラム2017

株式会社セシオス

会社紹介

株式会社セシオス

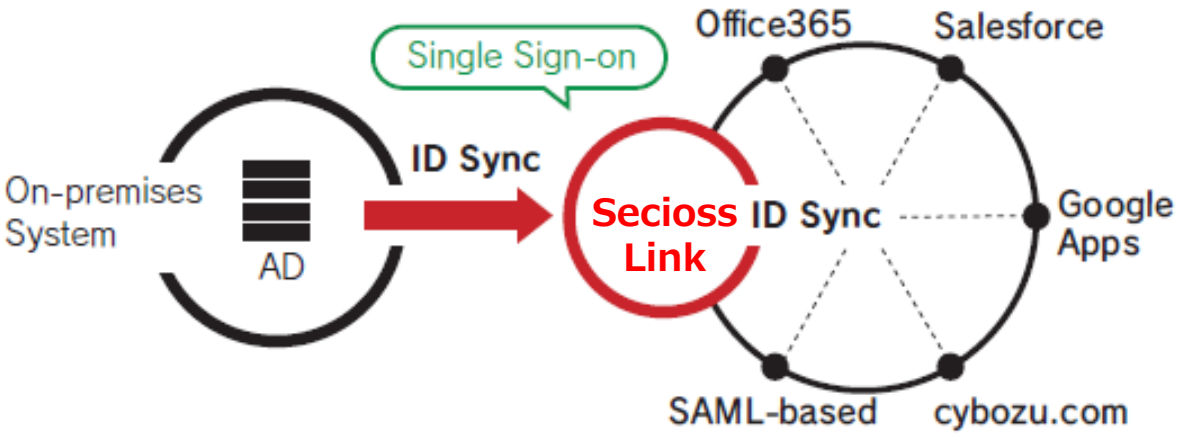
設立	2007年5月
資本金	1,300万円
代表取締役	関口　薫
住所	東京都新宿区山吹町365 4F
事業内容	認証・統合ID管理ソフトウェア サービスの開発、販売 システムインテグレーションサービス

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
クラウドサービスの経験値も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
Box

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

学認アンケートについて

IdP運用で注意すべき3要素

①ガバナンス

- IdP 運用規則や上位の全学セキュリティポリシーが制定されており、それに従って運用されている。

②テクニカル

- ID、属性情報はTrusted DB（組織にとって信頼できるデータベース：学務システムや人事DB）から作成される。
- パスワードポリシー、ID保持期間、ログ保存期間などが規定されている。

③プライバシー

- IdPから送出される個人情報は、関係する法令に従っている。
- 「利用者同意」を得るのが基本。

IDaaS側からの視点

ガバナンス

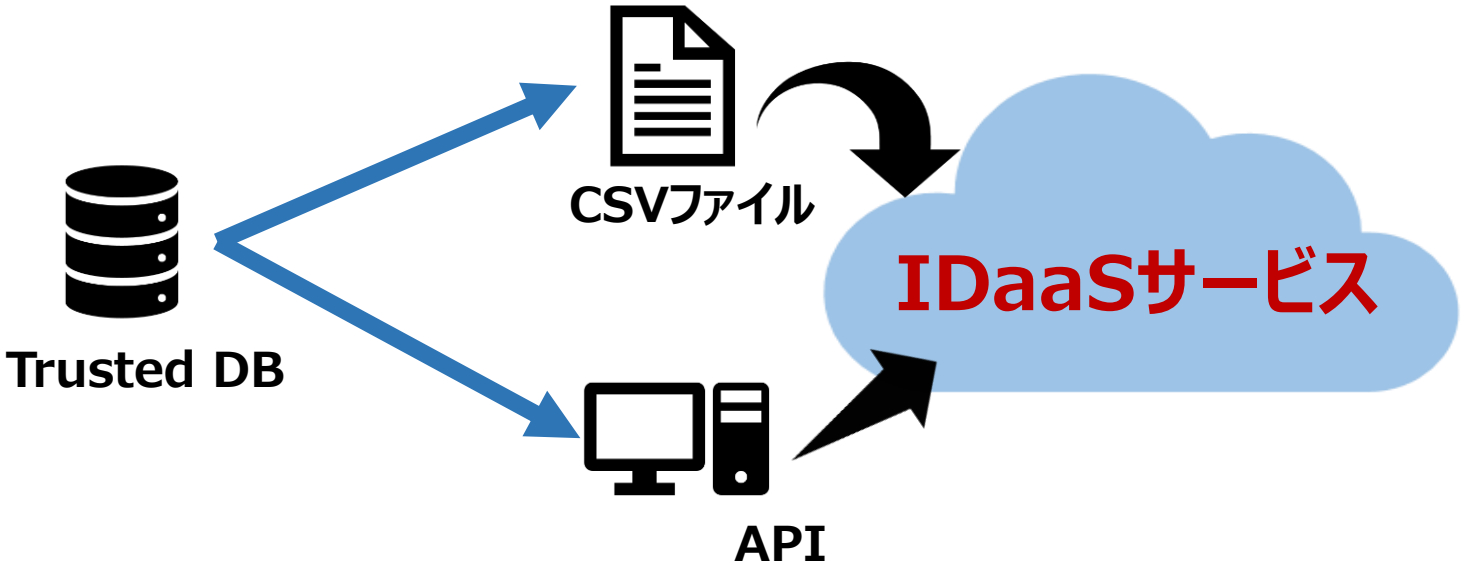
- 学認アンケート（認証基盤構築ガイド）では“学認参加機関による規程の整備が主であり、IDaaS のカバーする範囲ではありません”とあります。

サービス提供側として運用規定は設けています。

- インフラへのアクセスは社内からのみ可能
- 認証はID/Passに加えてアクセスキー認証
- VPN接続は可能。アクセスには証明書が必要。
- 24/365のシステム監視。
- プログラム展開など、ほとんどは自動運用（Chef）
- テストも自動テストを一部で利用（Selenium）
- ISMS27017（クラウドセキュリティ認証）取得進行中

テクニカル

- Trusted DBと直結するケースは少ない。
  - 人事や学務システムから出力されるCSVデータを利用
  - ID管理システムからAPI経由でデータを作成



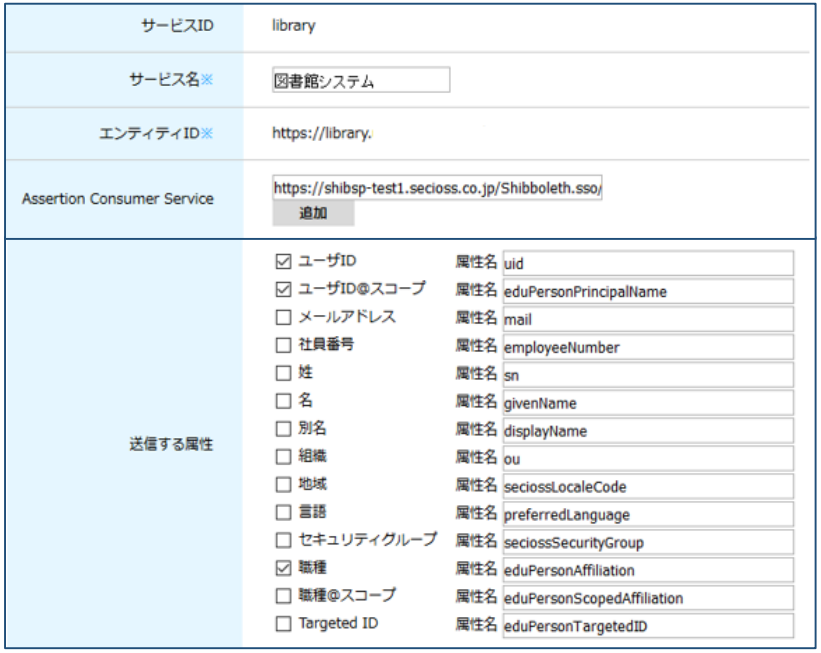
- 標準で「パスワードポリシー」や「操作・認証ログ取得」機能や「ワンタイムパスワード」機能を備えています。

プライバシー

- 属性送信時の「同意機能」があります。
- サービス連携設定では、送信属性を任意で設定することができます。

【送信属性 同意画面】

【送信属性 設定画面】



結論として・・・
IDaaSは学認アンケートに耐えられるのか？

まとめ

ガバナンス	▲	参加機関による規程の整備が主だが、 IDaaS提供側のポリシーも重要。
テクニカル	●	IDaaS側で対応できる部分が多い。
プライバシー	●	IDaaS側で対応できる部分が多い。

- IDaaS提供側にとっても、“理想的なIdP運用”の実現は簡単ではありません。
- 学認アンケートを通じて、常に改善していくことが重要だと認識しています。

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