IDaaS及び認証ソフトウェアにおけるMFAの現状

株式会社セシオス
マーケティング部　才川

Agenda

1. **会社紹介**
2. **製品紹介**
    - 当社製品群について
    - IDaaS：SeciossLink(セシオスリンク)
    - 導入事例
3. **多要素認証の利用状況**

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	東京都豊島区南池袋3-14-11 中町ビル6F
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	 IS 686961 / ISO 27001  IS 686961 / ISO 27001 CLOUD 686962 / ISO 27017 ISMS情報セキュリティ・クラウド 取得日　：2018年6月18日 認定番号：IS 686961 / ISO 27001 （適用範囲：池袋本社） CLOUD 686962 / ISO 27017（適用サービス：SeciossLink）

製品紹介：当社製品群について

クラウドとオンプレミスの製品があります。ご要件に応じて最適な製品を提案します。

製品紹介

SECIOSS LINK

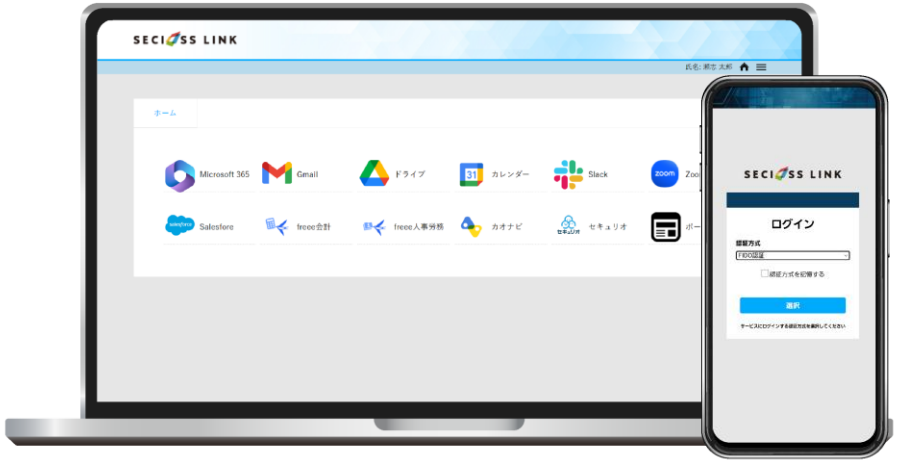
SeciossLinkとは

ID管理と認証、ゼロトラストに対応した

国産セキュリティプラットフォーム「SeciossLink」

主な機能

- ID管理
- シングルサインオン
- プロビジョニング
- アクセス制御
- 多要素認証
- セキュリティ



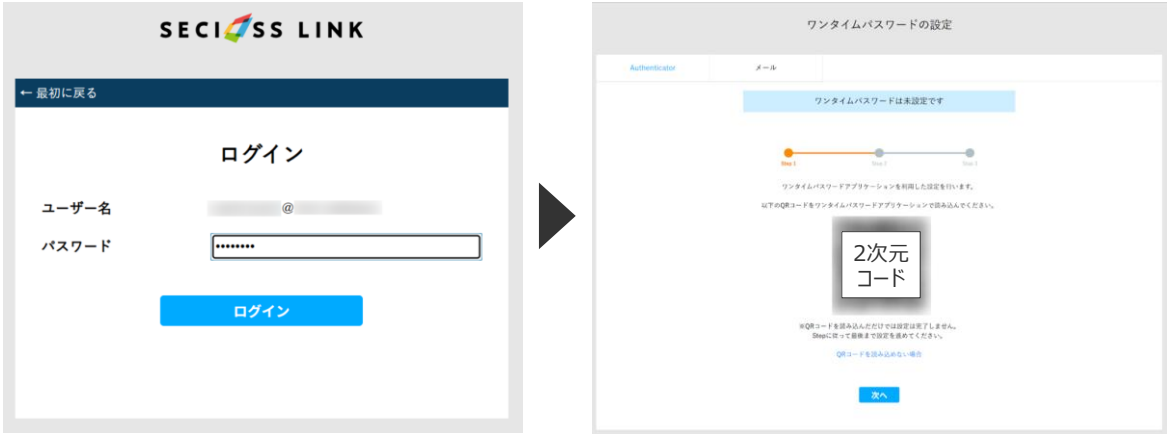
https://www.secioss.co.jp/seciosslink/

機能：多要素認証設定の強制化

SeciossLinkはクラウドサービスながら、細かな機能が多数あります。

多要素認証設定の強制化

ワンタイムパスワードが未設定のユーザーに対して、ログイン後に設定画面を表示させる機能です。



導入事例：国立大学様

3万超が利用するSSO認証基盤を IDaaSに刷新

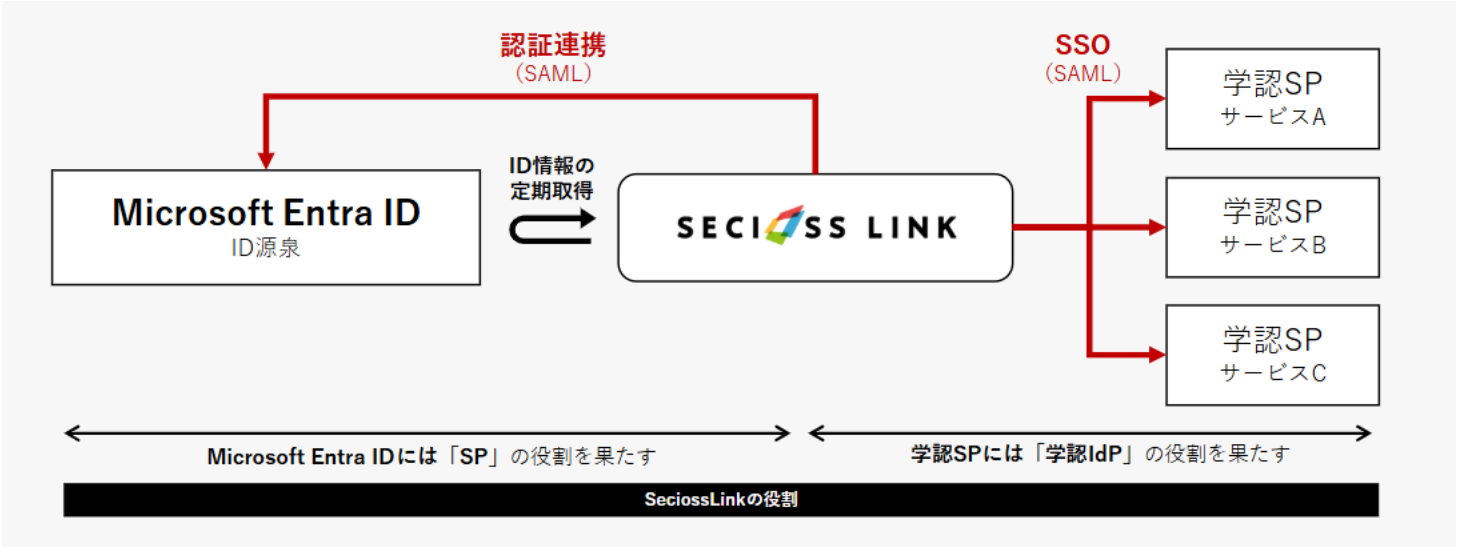
	課題	効果
①	➢ 大学外からのアクセス時のセキュリティをより強化したい	ワンタイムパスワード認証やFIDO認証などの最新の認証方式も利用可能に。セキュリティを強化。
②	➢ クラウドサービスをSSO連携したい。 ➢ 業務システム用のIdPと学認サービス用のIdPを統合したい	2つあったIdPを統合し、認証基盤を一元化して管理コストを削減。省力化に貢献。

https://www.secioss.co.jp/casestudy/tohoku/

SECIOSS

ユースケース

Microsoft Entra IDのアカウント情報を使って学認サービスにログイン



https://www.secioss.co.jp/casestudy/20231213

導入事例

セシオスのウェブサイトで事例やユースケースを多数紹介しています。ご参考ください。

共有アカウントのSSOでセキュアな運用を実現

国立大学法人 北海道国立大学機構

SAME　大学・研究機関

事例を見る

3万超が利用するSSO認証基盤をIDaaSに刷新！クラウド移行が成功した秘訣とは？

国立大学法人 東北大学

SeciossLink　大学・研究機関

事例を見る

ID管理・認証のクラウド化に成功！ID管理をIDaaSに移行する方法とは？

東北工業大学

SeciossLink　大学・研究機関

事例を見る

IDaaSの利用でシングルサインオン認証基盤を一括リプレイス

新潟薬科大学

SeciossLink　大学・研究機関

事例を見る

IDが統一され、様々なクラウドサービスへの利便性が良くなり、学生が活発に活用するようになった！

東京未来大学

SeciossLink　大学・研究機関

事例を見る

京都大学からの独立で必要になった、ITシステム・人事、経理システムの構築が半年で可能に！

京都大学iPS細胞研究財団

SeciossLink　団体

事例を見る

Microsoft Entra IDのアカウント情報を使って学認サービスにログイン

ユースケース

SeciossLink　ユースケース

事例を見る

https://www.secioss.co.jp/casestudy-interview

多要素認証の利用状況

セシオス製品の多要素認証

SeciossLink/SAMEでは**複数の認証方式を組み合わせた多要素認証が可能**です。

認証方式の例

- ID/パスワード認証
- ワンタイムパスワード認証(OTP)
  メール、アプリケーション、ハードウェアトークン
- 証明書認証
- FIDO認証(パスキー)
- AD/LDAP認証
  ※ADまたはLDAPでパスワード認証をする認証方式
- SAML認証(外部IdP認証)
- 統合Windows認証(デスクトップSSO)

多要素認証の例

多要素認証の利用状況：集計方法

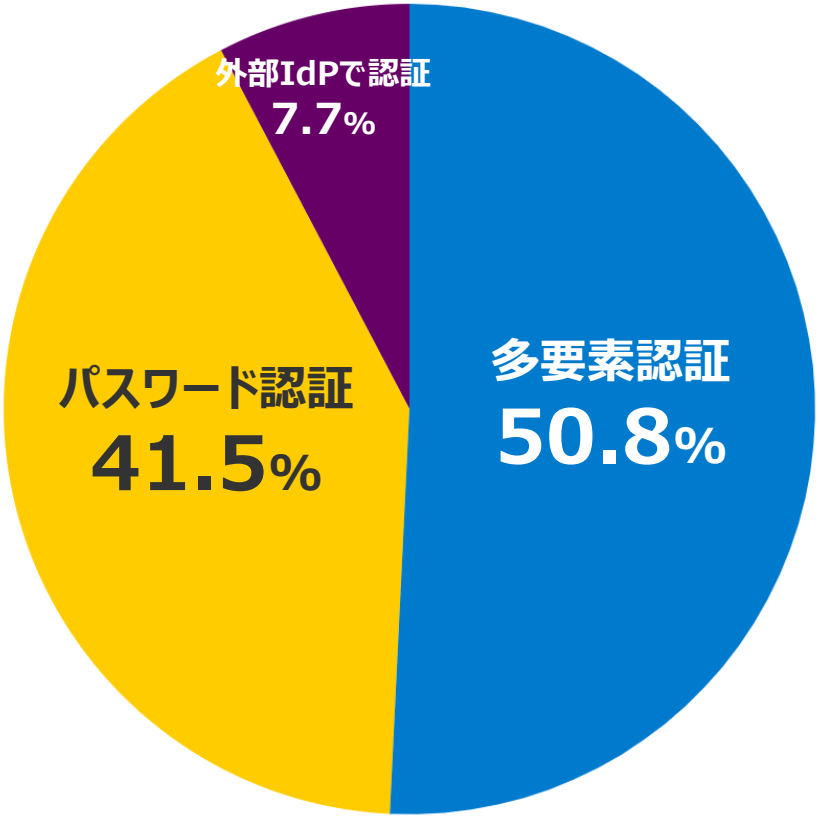
- 対象
  - SeciossLinkとSAMEの契約顧客（大学・研究機関）

- 集計
  - 学内・学外で認証ルールが異なる場合は、
    いずれかで多要素認証が使われていれば「多要素認証を使っている」と判断した

  - AD/LDAP認証はID/パスワード認証と合算し、「パスワード認証」とした

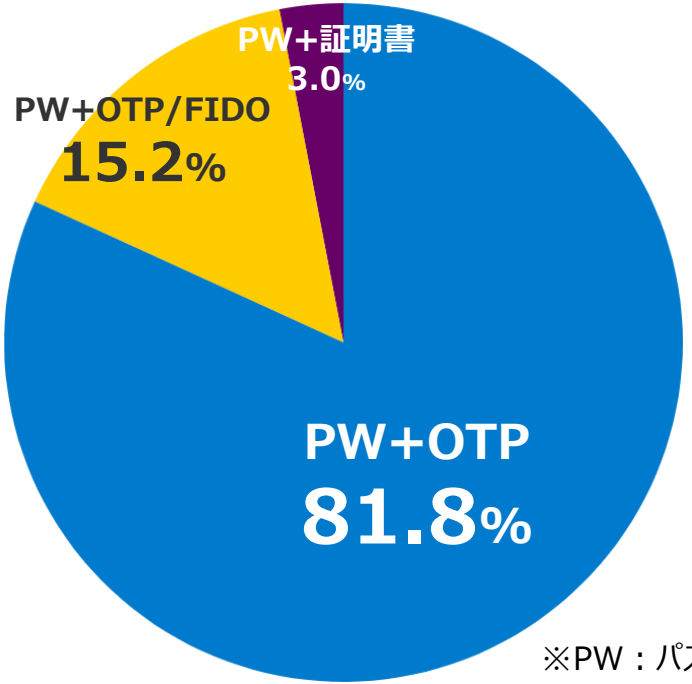
多要素認証の利用状況

大学・研究機関の約51%が多要素認証の利用し、次いでパスワード認証、SAML認証でログインしています。



多要素認証の利用：認証方式の内訳

多要素認証を利用するお客様の**<u>97%がワンタイムパスワード認証を使用</u>**しています。
FIDO認証も選べるように設定しているお客様が15%います。



OTPの利用率は
97%

PW+OTPとFIDOの
併用は15.2%

※PW：パスワード認証、OTP：ワンタイムパスワード認証

多要素認証の利用状況：まとめ

- SeciossLink/SAMEをご利用中の大学・研究機関のお客様の50%が多要素認証の利用している
    - 一方で、お客様の40%がパスワード認証でログインしている

- 多要素認証の97%がワンタイムパスワード認証を使用している
    - 15%のお客様がFIDO認証(パスキー)も使えるように設定している

考察

- **なぜFIDO認証が普及していないのか？**
  - ワンタイムパスワードで不便さを感じていない可能性がある

    → 大規模大学でもFIDOの登録数が1%未満

セシオスでは、引き続き「わかりやすく、使いやすい製品づくり」と
FIDO・パスキーに関するノウハウ共有などの情報発信強化を行っていきます

株式会社セシオス

https://www.secioss.co.jp/