



TOHOKU
UNIVERSITY

学術情報基盤オープンフォーラム2024
AXIES認証基盤部会・学認合同企画セッション

東北大学における SSO認証基盤の更新

国立大学法人 東北大学
情報部デジタル変革推進課
デジタルイノベーションユニット専門員
小野崎 伸久

2024年6月12日(水)



東北大学では、2023年度にSSO認証基盤の更新を行い、クラウドサービスIDaaS（Identity as a Service）の(株)セシオス社製「SeciossLink」を導入しました。

本発表では、システム更新の背景、新システムの要件、構築・移行時に発生した課題と解決策等を紹介します。

はじめに





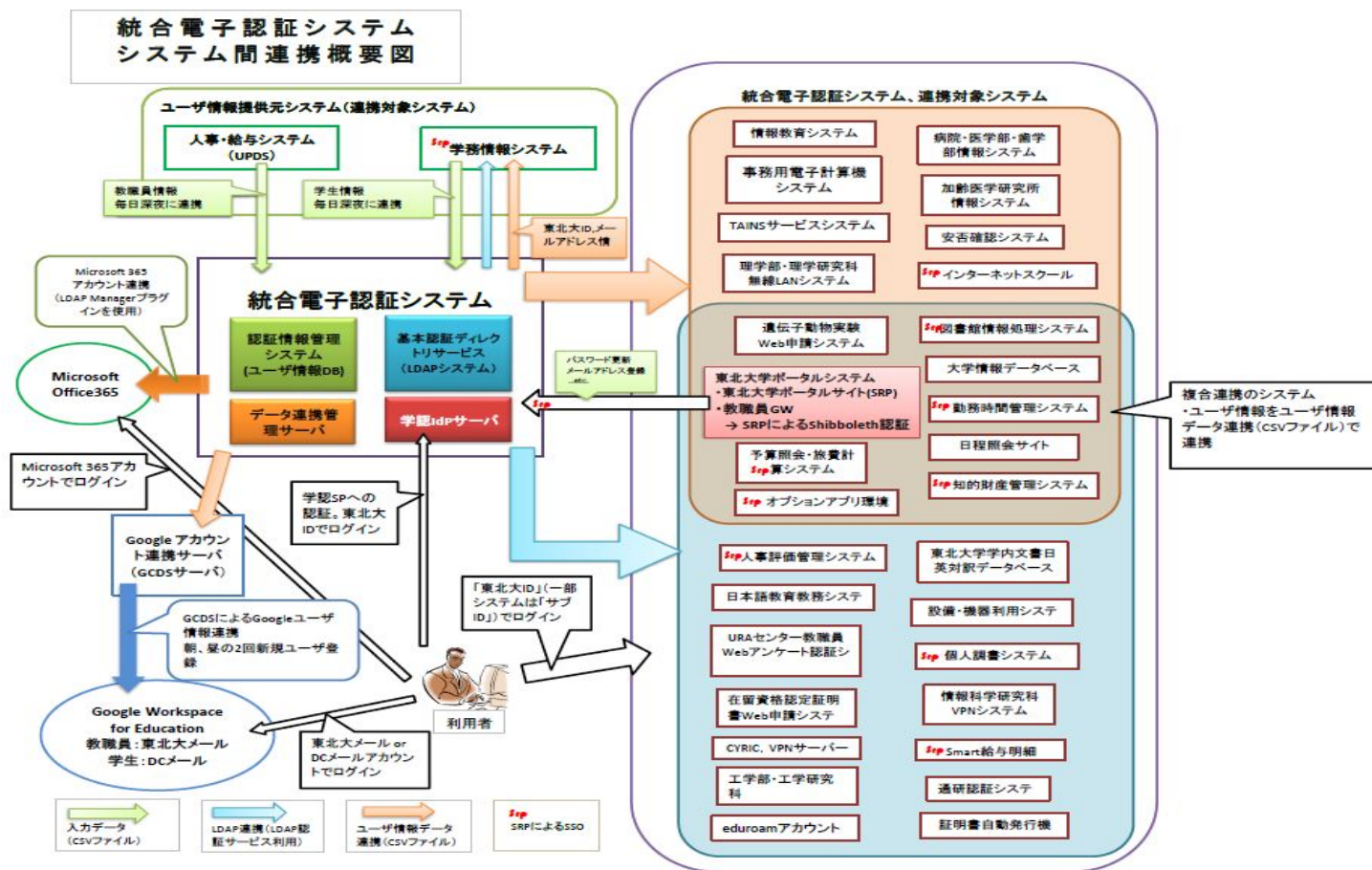
- 東北大ID
 - 統合電子認証システムから、教職員および学生等の東北大学構成員（約3万人）に対して発行される、全学一意のIDである。
 - 人事給与システム、学務情報システムを源泉としている。それ以外の構成員は申請により発行。
- Google Workspace（全学メール）
 - 東北大IDに紐づいて発行されるGoogle Workspaceアカウントである。
 - 2019年に別々に稼働していた教職員用の東北大メールと学生用のDCメールからGoogleに統合した。メール以外のドライブ、Meet、Classroom等を含めて活用。
 - 東北大ID無効後も猶予期間やメール転送期間あり。Alumniメールへの切替もあり。
 - 東北大IDのライフサイクルと異なるため、SSOは行っていない。
- Microsoft365
 - 東北大IDに紐づいて発行されるMicrosoft365アカウントである。
 - Officeのインストールライセンスを主目的として導入。
 - Teams等も利用可能。
 - SSO認証基盤更新に合わせて東北大IDのSSOに切り替え。



- SRP (Secure Reverse Proxy) システム (旧SSO認証基盤)
 - 2010年導入 (WisePointのカスタマイズ)
 - 学外アクセス時は二段階認証
 - 東北大ID／パスワード認証に加えてイメージマトリクス認証も行われる。
 - Shibboleth認証
 - 教職員グループウェア
 - リバースプロキシ代理認証
 - 財務会計、学務情報、ISTU、勤務時間管理システム等
 - 学内ネットワークに閉じたシステムに学外からログイン可能
 - 設定変更の度にサービス再起動が必要なため、気軽にできない。
- 学認Idp
 - 2014年導入
 - Shibbolethに対応
 - 学認SPにログインするためだけに構築されたIdp。
 - SRPとは別システムである。構築・保守ベンダーも異なる。



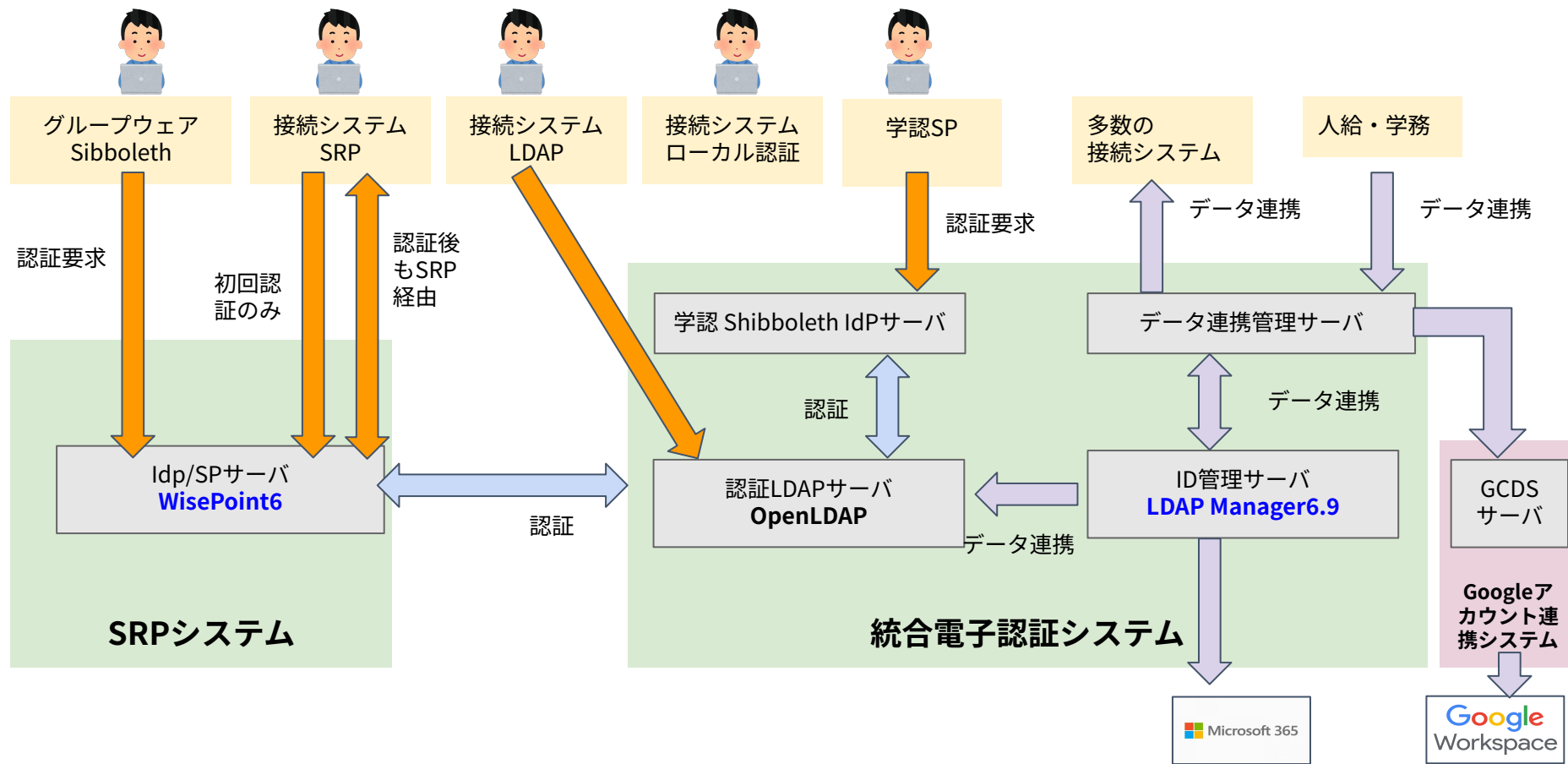
システム更新前の構成





システム更新前の構成（簡易版）

7





SRPシステムのログインイメージ

8



学外
off campus



東北大 ID + PW 認証
Tohokudai ID + PW



イメージマトリクス認証
Image-Matrix Authentication



ポータルサイトから
各種情報サービスへ
Campus Services
via Portal Site



学内ネットワーク
Campus LAN



東北大 ID + PW 認証
Tohokudai ID + PW



不要
Image-Matrix Authentication
is not required



ポータルサイトから
各種情報サービスへ
Campus Services
via Portal Site

システム更新





【現行システムの課題】

1. 学外アクセス時の「二段階認証」を「多要素認証」にグレードアップしてセキュリティを強化したい。
多要素認証については、パスワードレス等、常に最新の方式を使えるようにしたい。
2. クラウドサービスへのSSOに対応したい。
3. 業務システム用Idpと学認サービス用Idpを統合したい。
4. BCP対策を強化したい。

【新システムに移行する際の要件】

1. SAMLやShibbolethに未対応の学内既存システムにも引き続きSSOできるようにしたい。
2. 学認Idpで使用しているスコープ及びentityIDを継続利用したい。
(変更するとアカウントデータに影響あり)



製品	A製品	B製品	C製品	SeciossLink
形式	パッケージ	パッケージ	IDaaS	IDaaS
学認Idp	○	○	△ (entityID継続不可)	○
SAML認証	○	○	○	○
リパースプロキシ代理認証方式	○	× (別サーバが必要)	× (別サーバが必要)	× (別サーバが必要)
イメージマトリクス認証	○	×	×	×
パスワードレス認証(FIDO2)	○	○	△ (オプション)	○
TOTP認証 (トークン)	○	○	○	○
TOTP認証 (メール)	○	○	○	○
このブラウザを信頼する	×	○	×	○
不審挙動検知	×	×	×	○
日英切替	×	○	×	○

※2022年7月頃の情報です。
現在は仕様が変わっている可能性があります。



【メリット】

1. 常に最新機能（最新方式の多要素認証等）が利用できる。
2. セキュリティパッチ等の対応をお任せできる。
3. 可用性・完全性（負荷分散、バックアップ、BCP対策等）をお任せできる。

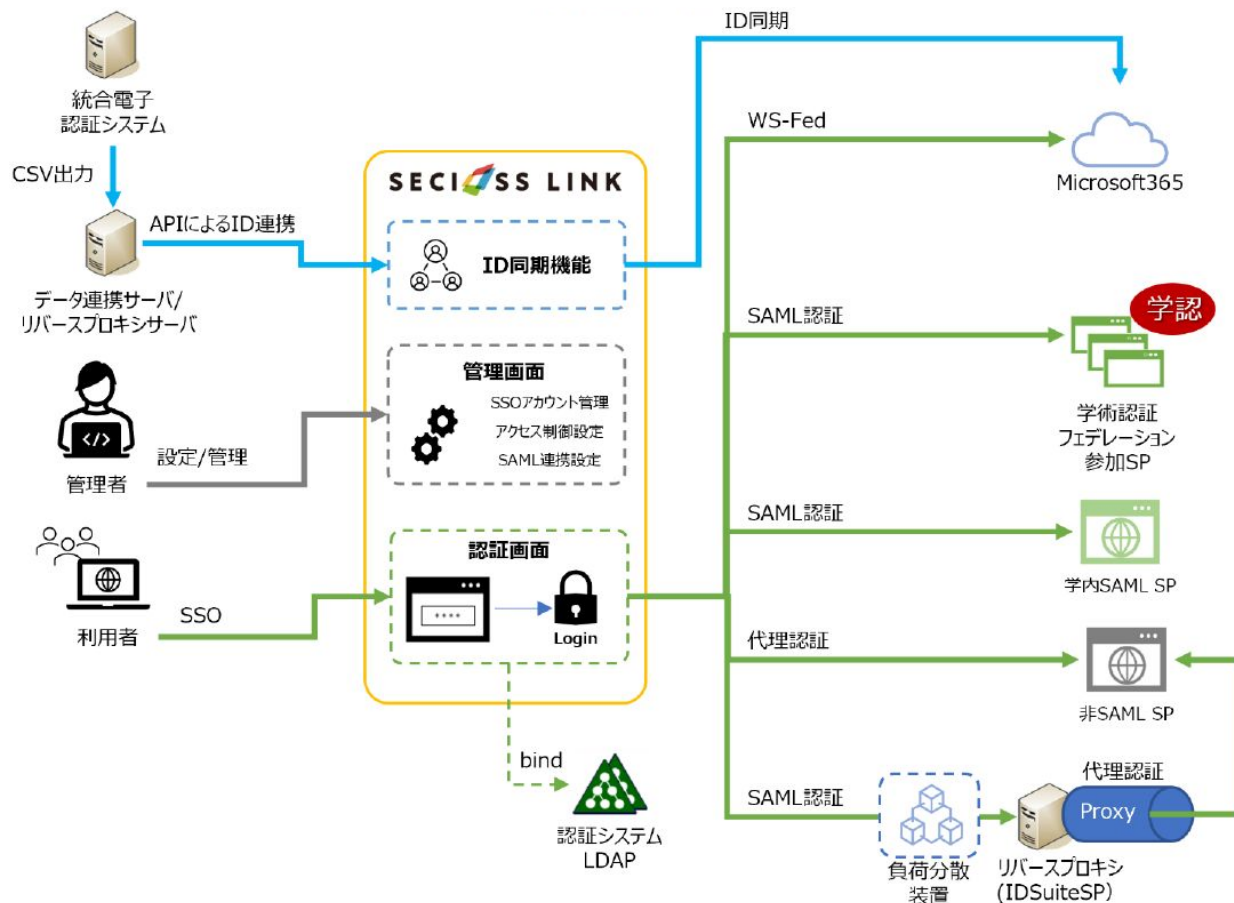
【デメリット】

1. パッケージと比較して費用が高い。
2. IDaaSは本学独自の要件に応じてカスタマイズできない。
⇒パッケージをカスタマイズする場合、本来の性能が落ちたり、保守費用があがるため、デメリットもある。



新システムの構成

13

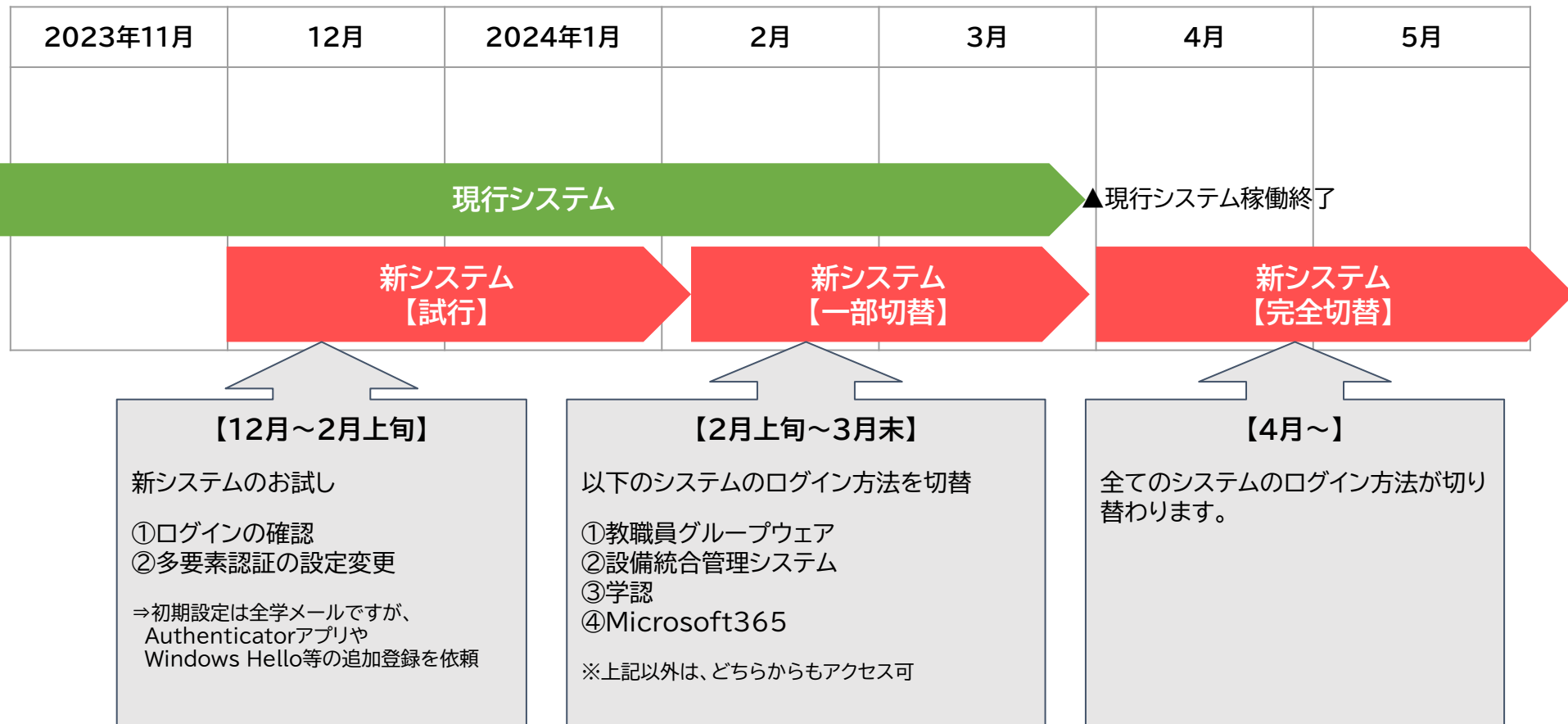




データシナジー創生機構 - Single Sign-On

<https://sites.google.com/tohoku.ac.jp/oids-out/sso>

The video thumbnail features the Tohoku University logo and name in the top right corner. The text "Single Sign-On" is displayed below the university name. In the center, there is a large, semi-transparent play button icon. Overlaid on the play button is the text "2分でわかる" (Understand in 2 minutes) in a pink, sans-serif font, and below it, "東北大ID ログイン" (Tohoku University ID Login) in a larger, bold, pink, sans-serif font.



構築・移行時に発生した課題と解決策





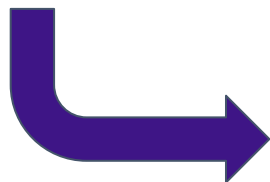
課題	解決策
痒い所に手が届かない機能があった。 例えば、SeciossLinkポータル画面のSSO先アプリケーションの名称が「日英表示切替」に未対応だった。	どんどん要望をあげた。 ⇒どんどん機能追加していただいた。 リリース情報 - Secioss Help Center
4月1日の年度更新を想定したテストを行ったところ、ID登録処理の処理時間が長く、業務開始時間までに間に合わない懸念があった。	改善を依頼した。 ⇒SeciossLink内のボトルネック箇所が特定され、そのサーバリソースを増強していただき、処理速度が改善された。
テスト工程で不具合のような動作が発覚した。	改善を依頼した。 ⇒早急に改修していただいた。

※言いにくいこともありました。

- 
- ・要望に真摯に対応していただけるクラウドサービスを選択する。
 - ・クラウドサービスといえども、テストは細かく行う。



課題	解決策
ユーザーからの問い合わせ対応 ⇒自己解決してほしい。 でも、問い合わせを減らすために、 難しそうな機能を制限することはNG。	● ユーザーガイドをGoogleサイトで公開 ● ショート動画も公開 ● 日英両方用意
学外でログインできない人への対応 ⇒電話で本人確認して個別対応するのは大変。	通知用メールアドレス変更について、本人申請フォーム、事務担当者・教職員の代理申請フォームを作成し自動化 (GoogleAppsScriptとSeciossLinkのAPIを活用し、ワンタイムパスワードの通知先メールアドレスの更新まで自動化)



・ユーザーマニュアルや問い合わせ対応もDX化していく。



課題	解決策
ワンタイムパスワードでログインできない。 ⇒本人はスマートフォンで操作しており、メールに通知されたパスワードを正しく入力しているという。	メールを開く際にワンタイムパスワード画面を閉じていたため、再アクセス時に別のワンタイムパスワードが発行され、ログインできなかった。 ⇒再発防止策としてワンタイムパスワード画面に「画面を閉じないで」とJavascriptで追記。 ⇒SeciossLinkにも要望をあげている。
iPhoneでFIDO認証ができない	iPhoneのGmailアプリに内蔵されたGoogleブラウザが原因だった。（SafariやChromeは正常動作） ⇒問い合わせが1名なので再発防止策は保留。

※ 3～4月に問い合わせが多かったが、4月中旬以降は落ち着いた。

※ 言いにくいこともありました。



- ・ MFAは普及されつつあるが、まだ使ったことがないユーザーもいる。事前に問い合わせを想定することも難しいのでベンダーと協力して対応。

まとめ





- IDaaSを導入して良かったこと
 - 利便性とセキュリティ強化のバランスが取れている
 - 学外アクセス時の多要素認証
 - 最新のパスワードレス認証にも対応
 - 不審挙動検知メール（でも精度はあげてほしい）
 - ブラウザを信頼する
 - DXにより、SSOの案件が増えたが、迅速に対応できている
 - 動作が遅い等の問題もない
 - SINET仙台（宮城）ノードのメンテナンス時も、IDaaSは稼働しているので、MicrosoftアカウントへのSSOも無事に動いた
- IDaaSを導入するときに気を付けること
 - 課題と解決策ページに記載した通り、ベンダーと密に会話していくことが重要。

おまけ





東北大学は、New Normal時代における新たな大学の姿を先導し、学生・教職員が、今まで以上に学業や教育・研究活動に専念できる場をこれからも提供して参ります。

ご意見・ご感想・ミーティング依頼等はお気軽に[こちら](#)よりご連絡ください。

東北大学のDXに関する最新情報は[Web](#)をご覧ください。

東北大学 DX

🔍 検索

