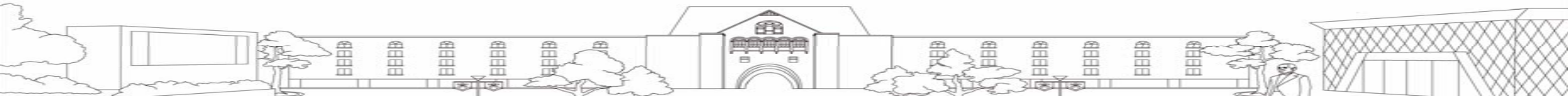
〈学術情報基盤オープンフォーラム2018〉

クラウドを活用した近大流SSO/MFA基盤導入術

学校法人 近畿大学
総合情報システム部

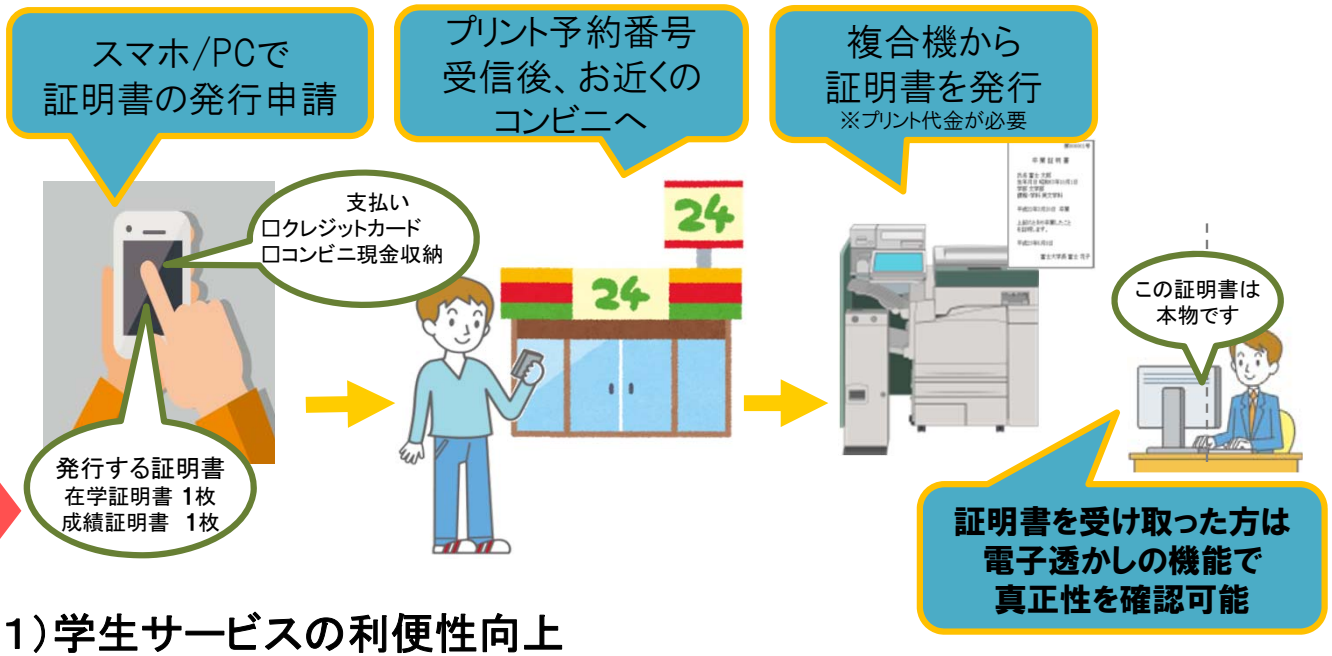
2018-06-21



常識をぶっ壊す
＝
イノベーション

●現在の証明書発行

●コンビニ発行



（1）学生サービスの利便性向上

・学生/卒業生はキャンパスへ行くことなく、身近なコンビニエンスストアで証明書を取得可能。

（2）大学の窓口業務・運用費用の負担軽減

・証明書発行や現金管理など、窓口の業務負担を軽減します

（3）事業継続におけるリスク低減

・証明書発行に必要なデータは、震度7レベルに耐えうる堅牢なデータセンタに保管。
地震などの火災で、万一大学に被害があっても、データセンタが止まる可能性は低い。


時間割
月
火
水
木
金
1
2
3
4
5
6


unipa-test.itp.kindai.ac.jp
BACK
座席予約
EXIT
予約履歴
2017年3月14日（火）
凡例：
A B C D E F G H I J K
1
2
3
4
5
6
7
8
9
10
通路
講壇

ICTの取り組み

テレワークで日本を変える
V-CUBE

2015年から開始

WEB会議システム。
移動時間、出張経費を削減

V-CUBE利用件数 **533件/年**

slack

2016年から開始
(2018年に有償版導入)

迅速な情報連携

ICTの取り組み

・パソコンやスマホの紛失、盗難
・メールの誤送信、ブログやWebへの誤掲載
・内部者の犯行（故意）
・ファイル共有ソフトからの漏洩
・システムの脆弱性（Word press等）
・不正プログラム（標的型攻撃、ランサムウェア等）
・不正ログイン（ID/PW乗っ取り）

SSO/MFA導入の背景

- パソコンやスマホの紛失、盗難
- メールの誤送信、ブログやWebへの誤掲載
- 内部者の犯行（故意）
- ファイル共有ソフトからの漏洩
- システムの脆弱性（Word press等）
- 不正プログラム（標的型攻撃、ランサムウェア等）

リテラシー授業

教職員向け研修

システム側で対策

- 不正ログイン（ID/PW乗っ取り）

研修やシステム側で対策することは難しい。
有効な攻撃がいくつか存在するため（次頁）

・パスワードリスト攻撃

ひとつのWebサービスが攻撃され、そこから漏れたIDとパスワードを用いて他のWebサービスでログインを試みる攻撃。たいていの人は複数のWebサービスで同じID（メールアドレス）とパスワードを使い回しているのでこの攻撃が成立する。

・フィッシング攻撃

銀行やGoogle等を装った偽のWebページを作成し、そこにメール等で誘導し、IDとパスワードを入力させて盗み取る攻撃。

・ブルートフォース攻撃（総当たり攻撃）

大量のパスワードを使ってログインを試みる攻撃。

・リバースブルートフォース攻撃（逆総当たり攻撃）

よく使われそうなパスワードを固定し、IDをランダムに入力してログインを試みる攻撃。覚えやすいパスワードを設定しているユーザーはこの攻撃を受ける可能性が高くなる。

➡ 多要素認証・アカウントロック・SSO

多要素認証（MFA）

２つ以上の認証方法を用いてログイン

例）ID/PW＋OTP、ID/PW＋顔認証 etc...

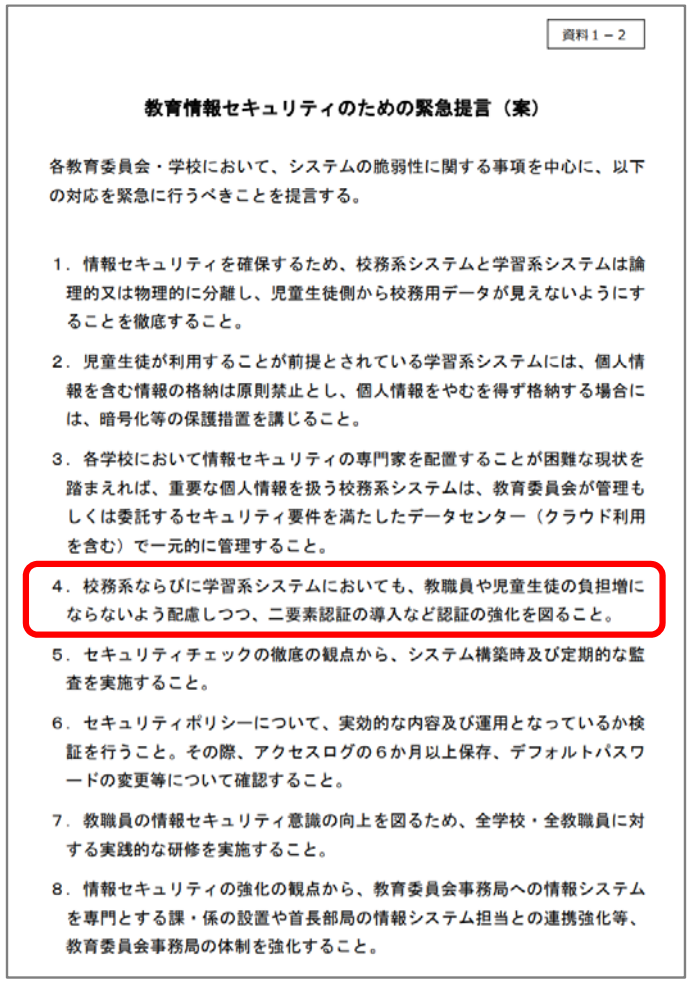
アカウントロック

パスワードを複数回間違えるとしばらくログインできなくなる

シングルサインオン（SSO、共通認証）

１つのサービスにログインすれば、他のサービスに自動でログイン

SSO/MFA導入の背景



資料１－２

教育情報セキュリティのための緊急提言（案）

各教育委員会・学校において、システムの脆弱性に関する事項を中心に、以下の対応を緊急に行うべきことを提言する。

1．情報セキュリティを確保するため、校務系システムと学習系システムは論理的又は物理的に分離し、児童生徒側から校務用データが見えないようにすることを徹底すること。

2．児童生徒が利用することが前提とされている学習系システムには、個人情報を含む情報の格納は原則禁止とし、個人情報をやむを得ず格納する場合には、暗号化等の保護措置を講じること。

3．各学校において情報セキュリティの専門家を配置することが困難な現状を踏まえれば、重要な個人情報を扱う校務系システムは、教育委員会が管理もしくは委託するセキュリティ要件を満たしたデータセンター（クラウド利用を含む）で一元的に管理すること。

4．校務系ならびに学習系システムにおいても、教職員や児童生徒の負担増にならないよう配慮しつつ、二要素認証の導入など認証の強化を図ること。

5．セキュリティチェックの徹底の観点から、システム構築時及び定期的な監査を実施すること。

6．セキュリティポリシーについて、実効的な内容及び運用となっているか検証を行うこと。その際、アクセスログの６か月以上保存、デフォルトパスワードの変更等について確認すること。

7．教職員の情報セキュリティ意識の向上を図るため、全学校・全教職員に対する実践的な研修を実施すること。

8．情報セキュリティの強化の観点から、教育委員会事務局への情報システムを専門とする課・係の設置や首長部局の情報システム担当との連携強化等、教育委員会事務局の体制を強化すること。

文科省　2020年代に向けた教育の情報化に関する懇談会。教育情報セキュリティのための緊急提言（案） 平成28年7月28日

① 教育情報システム管理者は、盗難防止のため、職員室等で利用する校務用端末及び校務外部接続用端末のワイヤーによる固定、教室等で使用する指導者用端末の保管庫による管理等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 教育情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 教育情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を設定しなければならない。【推奨事項】

④ 教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の二要素認証を設定しなければならない。【推奨事項】

⑤ 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】

⑥ 教育情報システム管理者は、モバイル端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。【推奨事項】

文科省教育情報セキュリティポリシーに関するガイドライン（抜粋）
平成２９年１０月１８日策定

目的

- 利便性
- セキュリティ

実演します。

●OTPの採用理由

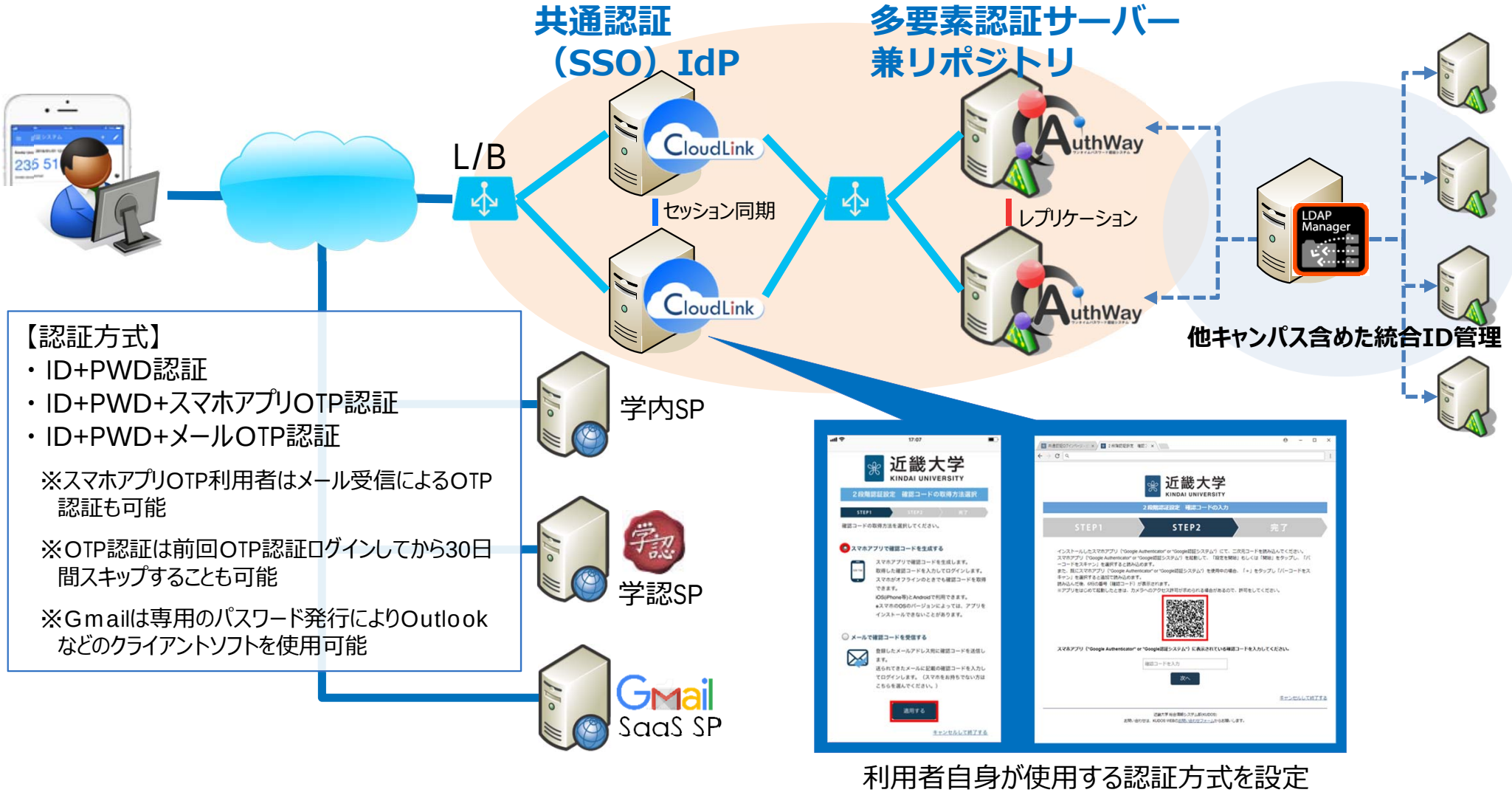
・運用コストと利用者負担の観点で、クライアント証明書等は不採用。

・OTPのMFAはGmailやFacebookやSlackなどの人気サービスで提供されているため、慣れているユーザが多い。

・メール送信方式も用意したことで、ガラケーユーザにも対応。

・管理者用アカウントはChromeの拡張機能のコードジェネレーターで対応。

システム構成



【認証方式】
- ID+PWD認証
- ID+PWD+スマホアプリOTP認証
- ID+PWD+メールOTP認証

※スマホアプリOTP利用者はメール受信によるOTP認証も可能

※OTP認証は前回OTP認証ログインしてから30日間スキップすることも可能

※Gmailは専用のパスワード発行によりOutlookなどのクライアントソフトを使用可能

利用者自身が使用する認証方式を設定

LDAP Manager（EXGEN）

アカウント管理システム。源泉からデータを受け取り、AD/LDAPにアカウント情報を同期

CloudLink（IP3）

SAML IdP（Shibboleth同様の機能）、SSOログイン画面のUI、MFA設定画面UI、MFAスキップ用のcookie発行

AuthWay（IP3）

パスワード認証、MFA認証（スマホOTP、メールOTP）、MFA設定情報（メルアド等）、アカウントロック

Shibboleth/OpenLDAPではなく

CloudLink/AuthWayを選んだ理由

- 多要素認証機能を備えたSSO基盤であること
  （ShibbolethでMFAを実現するにはプログラム修正が必要）
- サイバー攻撃対策として、攻撃されやすいOSSを避けた
- 利用者の操作性を考慮したインターフェースがパッケージ機能として提供されている
- FIDO2.0/Web Authnの実装を見据えたパッケージであること
- 47,000人の利用に耐えうる性能であること（後述の負荷試験結果参照）

●SSO/MFAパッケージへの新規実装

・MFA30日間スキップ機能
・マニュアル不要の分かりやすいMFA設定UI
・エラー出力（問い合わせフォームへのエラーコード反映）
・MFA利用者向けメールソフト専用パスワード発行（利用者自身がWebで確認）
・共通認証ログインデザイン（共通認証への周知や告知はSPごとに設定可能）
・パスワード誤入力によるアカウントロックまでのカウントダウン回数表示
・スマホアプリ（Google Authenticator）へのコード追加時の表示名設定
・管理者向けアカウントロック解除専用GUI

→全てパッケージ機能として追加（≠カスタマイズ・アドオン）

●LDAP Managerの新規実装

・管理者向けMFAの解除機能

・パスワード変更Web GUIのSSO化

（管理者向け、利用者向け：パスワード変更/リセットWeb）

→全てパッケージ機能として追加（≠カスタマイズ・アドオン）

※以下、2018年6月リリース予定

・ 管理者により、MFAの利用を特定ユーザー/特定部署に限定して強制する機能（個別処理および一括処理）

・ パスワードリセットを自ら行うことができない利用者がパスワードを忘れた場合、管理者がリセットしたパスワードを通知する際に本人確認の信頼性度合いにより共通認証への初回ログイン時にパスワード変更を強制する機能

対象者　　：　約47,000人

開始時期　：　2018年3月

対象SP　　：　学認SP5、その他SP8

データ等

・負荷試験の結果、1,500件/10秒の同時アクセス（2台負荷分散環境）まで利用可能。
※試験中、1,500を超えたあたりでエラーが散見。
※クライアント1台当たりの応答時間は平均約5秒、最大で約10秒程度。
・ロードバランサはClassicよりも Applicationのほうが若干成功数が上回った。

CloudLink

項目	説明	設定値 #1	設定値 #2	設定値 #3
vCPU	vCPU数	2	2	2
メモリ	物理メモリ	8GiB	15.25GiB	15.25GiB
インスタンスタイプ		m4.large	r4.large	r4.large
ロードバランサ		Classic	Classic	Application

AuthWay

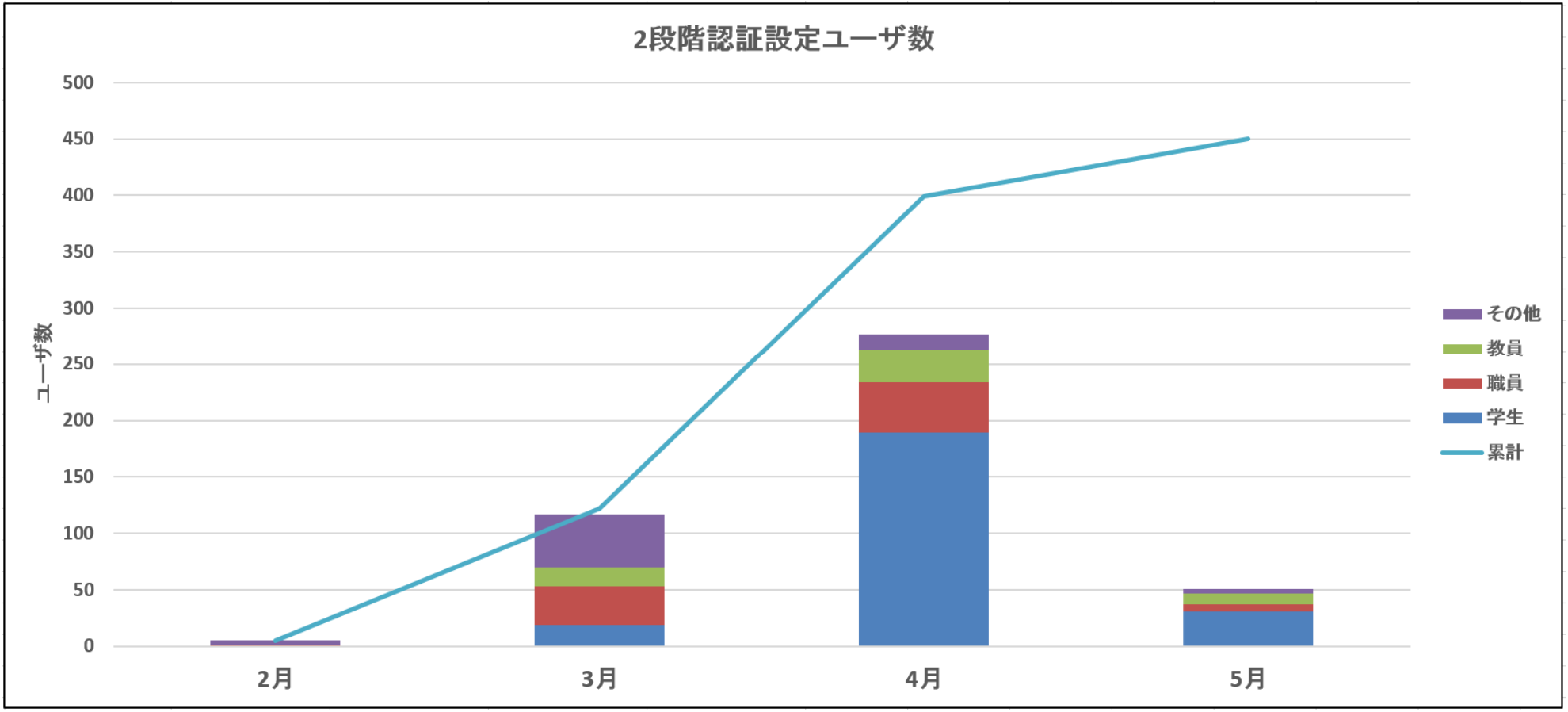
項目	説明	設定値 #1	設定値 #2	設定値 #3
vCPU	vCPU数	2	2	2
メモリ	物理メモリ	8GiB	8GiB	8GiB
インスタンスタイプ		m4.large	m4.large	m4.large

対象	説明	設定値 #1	設定値 #2	設定値 #3
	同時アクセス数	1,520件	3,000件	3,000件
CloudLink	CPU最大使用率	60%	70%	75%
	ログイン処理リクエスト	1,520件	2,565件	2,811件
	ログイン成功	1,520件	2,075件	2,580件
	平均応答時間	5秒	30秒	30秒
	最大応答時間	10秒	55秒	60秒
	500エラー	0件	145件	321件
	TLSネゴシエーションエラー	0	0件	40件
AuthWay	CPU最大使用率	22%	29%	40%
	平均応答時間	0.1秒	0.1秒	5秒
	最大応答時間	0.1秒	2秒	15秒

※ ログイン成功数はhttpdのログからログイン後の画面遷移（303）に成功した件数。
※ 500エラーはhttpdのログから件数を取得。ログイン成功後に500エラーが出たり
したのでログイン処理リクエスト＝ログイン成功＋５００エラーとはならない。

共通認証へのアクセス

1	延べログイン数	4月	224,591
		5月	188,422
2	ユニークログイン数	4月	22,601
		5月	21,888
3	1分間の最大ログイン数	4月	151
		5月	114
4	1分間の最大アクセス数	4月	183
		5月	127


2段階認証設定ユーザ数
ユーザ数
500
450
400
350
300
250
200
150
100
50
0
2月
3月
4月
5月
その他
教員
職員
学生
累計

・CloudLink,AuthWayに期待すること

✓　ログから生成する統計データ・レポーティング

✓　ログ解析機能（攻撃者の排除等）

・MFA必須化について

→部門単位で順次必須化（難易度高め）

さいごに

・自分が利用可能なSP（学認SP、独自SP）のみが表示されるポータル的なもの

→イメージはOneloginのアプリ

→CloudLinkに搭載されているので今後実装するかも。

→NIIのクラウドゲートウェイサービスでは現状、運用的に厳しい。

さいごに

Web Authentication(FIDO2.0)

パスワードレス、生体認証（顔認証、指紋認証）、USBキー、etc...

さいごに


近畿大学
KINDAI UNIVERSITY