



# 次世代学認サービスメニュー： 全体像とロードマップ

佐藤周行（学認）

@第14回佐賀大学統合認証シンポジウム

2022/03/10

# 概要

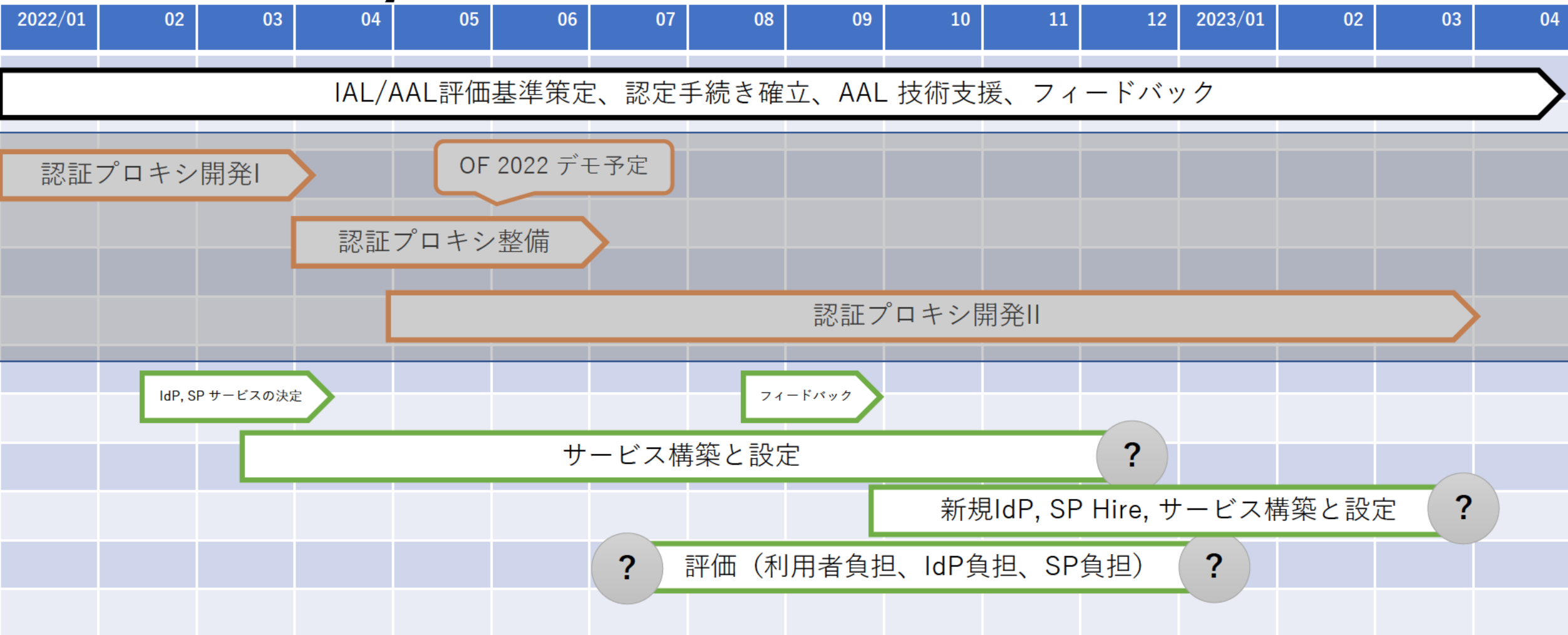
- 昨年も機会をいただいて、この統合認証シンポジウムで「新しい学認」というタイトルで発表しました
  - 同様の発表は2021 NII オープンフォーラム 2021 SINET6説明会でもしてきました
- 今回はそのアップデートになります
- 昨年の発表で示した「コンセプト」の詳細化を進めています
- ターゲットとなるサービスが特定できつつあります（何かありませんでしょうか）
- 実際の利用者の実感を重視しています
- PoCの構築をしなければなりません
- この発表は、スライドとしてタイトルページを含めて42枚、時間として35分を予定しています



- コンセプトとしての「トラスト」「トラストフレームワーク」が具体的なサービスになるまでのギャップの特定と解決が求められています
- 今までの解（例：NIST SP800-63）が教科書的に適用されるかと言うと…
  - Missing pieces があります。
  - 「結局は人間関係」というサイエンス/エンジニアリングの対極にある解に陥らないために（結局は必要なんですけど）



# Roadmap



# 学認の計画

- 大学等研究機関が運用するIdPがサービス側から信用されるための基準を作って運用します
  - 学認に参加しているSPがIdPを信用する
  - 貴重な計算・情報リソースにアクセスできるように←従来、SPが本格的な公開を躊躇していたもの
  - 企業ID等、より広いアイデンティティの収容を可能にします（IDaaSの利用を含めて）
- 基準は、現状を正しく評価し、かつIdPが十分「運用可能」なようなものにします
- 基準は、国際基準を見据えたものにします
  - 将来的な国際的相互運用性を提供する



# IdPを運用している研究機関へのお願い

- アカウント発行のポリシーを確認してください
  - 大丈夫なはずですが。「確認」は現状が十分満足できるレベルであることを「確認」することです
- 認証を強くする要請に応えてください
  - パスワードだけの認証での事故多発
  - スマホその他を利用した多要素認証方式の普及
    - 多段階認証への評価見直し（↑の意味で）もありますが
- 上が満たされれば、SPはIdPを強い意味で信用してくれます
- （今後繰り返しますが）学認はその「信用」をサポートします



# 利用者のご利益

- たとえば、スーパーコンピュータの利用申請が大学のIdPからできるようになる

(従来)

- 確認のために顔を見せてください
- 身分証、職員証の名前を確認させてください
- 大学内の利用資格（大学院生以上である、予算を持っている等々）は、書類を所属機関とやりとりすることで確認します

⇒ 全部一度大学内で済んでいるんだけど…



- PLAN: たとえば、スーパーコンピュータの利用資格、本人確認がオンラインでできるように、IdPから出てくるアサーションの保証度を「学認」が保証します
  - IdPが正しく運用されていることを認定します
  - SPにはその「認定」を信頼してもらいます ←学認が「説得」します





# トラストフレームワーク

- このような枠組みを「トラストフレームワーク」と言っ
- 統合認証シンポジウムで初めてお話ししたのは2013年（第7回）でした
- 当初から国際的相互運用性を重視していました
  - motivationはNIHの利用
  - NIHの利用にはLoA 1が必要（後にそううまくいかないことがわかる）
  - LoA1取りましょう。学認が認定できるようにしましょう



鈴木彦文 先生(信州大学)

「信州大学における統合認証とライフログに対する取り組みと学認との連携」

## プログラム (敬称略)

13:30-13:40 あいさつ  
佐賀大学 CIO 中島 晃

13:40-13:50 はじめに  
佐賀大学 総合情報基盤センター長 只木 進一

13:50-14:30 信州大学における統合認証とライフログに対する取り組みと学認との連携  
講師 鈴木 彦文 (信州大学総合情報センター)

14:30-15:10 Shibboleth認証と非Web認証の連携  
- Webメールシステムのシングルサインオン -  
講師 大谷 誠 (佐賀大学総合情報基盤センター)

15:10-15:25 休憩

15:25-16:05 日本のアカデミアにおけるトラストの構築  
-- 認証情報を相手に信用してもらう+認証情報を利用する相手を信用する --  
講師 佐藤 周行 (東京大学情報基盤センター)

16:05-16:45 山形大学のLoA1の認定と信頼フレームワークによる教育基盤の展開  
講師 伊藤 智博 (山形大学工学部学術情報基盤センター)

16:45-17:25 Shibboleth による Office365 Education のシングルサインオン  
講師 上田 浩 (京都大学学術情報メディアセンター)

# 第7回統合認証シンポジウム プログラム (2013) より



- 当時のアメリカでは、OMB 04-04 とそれを具体化したNIST SP800-63が定められていた
- 当時、オバマ政権は、NSTIC、FICAM等を組織し、当時立ち上がりつつあったIdP, SPによるSSOに信頼性を与えようとしていた
  - 米国内でも、末端まで理解されていたか非常に疑問
- 現在、Kantaraが認定作業を行っている





# Join. Innovate. Trust.






Kantara Initiative is a unique global 'commons' that operates conformity assessment, assurance and grant of Trust Marks against de-jure standards under its Trust Framework program whilst in parallel nurturing 'beyond-the-state-of-the-art' ideas and developing specifications to transform the state of digital identity and personal data agency domains.

[About us](#)

[Trust Operations](#)

[Support us](#)

View the Kantara Initiative Approved Full Services and Component Services, Accredited Assessors, & Registered Applicants

Full Services	Component Services	Accredited Assessors	Registered Applicants	Lapsed
<a href="#">view details</a>	<b>Company</b>	<b>Class of Approval</b>	<b>Type</b>	<b>Assurance Levels</b>
<a href="#">View Details</a>		Classic	Accredited Assessors	1
<a href="#">View Details</a>		Classic & NIST 800-63 rev.3	Accredited Assessors	ALs 1,2,3,4; IAL2,IAL3; AAL2, AAL3; FAL2, FAL3
<a href="#">View Details</a>		Classic & NIST 800-63 rev.3	Accredited Assessors	ALs 1,2,3,4; IAL2, IAL3; AAL2, AAL3; FAL2, FAL3
<a href="#">View Details</a>		Classic & NIST 800-63 rev.3	Accredited Assessors	ALs 1,2,3,4; IAL2,IAL3; AAL2, AAL3; FAL2, FAL3
<a href="#">View Details</a>		Classic & NIST 800-63 rev.3	Accredited Assessors	ALs 1,2,3,4; IAL2, IAL3; AAL2, AAL3; FAL2, FAL3

# 学認の立場

- 信頼を獲得するための「基準」を管理運用します
- KantaraのLoA1 (Classic) の認定を自らできるようにしています
- 「基準」として、3つくらい表に出ているものがあります
  - REFEDS Assurance Framework
  - NIST SP800-63
  - IGTF



# REFEDS Assurance Framework

REFEDS スペース ▾



ページ

ブログ

スペース ショートカット

Baseline Meeting notes

子ページ

Assurance Home

REFEDS Assurance Framew...

検索

?

ページ / Assurance Home

## REFEDS Assurance Framework ver 1.0

Mikael Linden が作成し、7 19, 2021 に Nicole Harris が最終更新

Identifier: <https://refeds.org/assurance>

### Abstract

To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces a framework for assurance and its expression using common identity federation protocols.

This framework splits assurance into the following orthogonal components:

- the identifier uniqueness;
- the identity assurance; and
- the attribute assurance.

The assurance of authentication is not covered by this specification. The Credential Service Provider assigns one or more values from one or more components to each credential and delivers the value(s) to the Relying Party in an assertion. For conformance to this framework, only meeting the baseline expectations for Identity Providers is required.

To serve the Relying Parties seeking for simplicity, the components are further collapsed to two assurance profiles (with the arbitrary names Cappuccino and Espresso) which cover all components. This framework also specifies how to represent the values using federated identity protocols, currently SAML 2.0 and OpenID Connect.

### 1. Terms and definitions



# REFEDSの方針

- 基準は他のものを借りてくる
  - Kantara, IGTF
- 基準は小分けにされていて、各々の基準が満たされているかどうかの値を与える
  - 大分野として
    - アイデンティティのユニークネス
    - アイデンティティの保証度
    - 属性の保証度
- 値の集合を「プロファイル」として定義する
  - Cappuccino, Espresso





# NIST SP800-63の方針

- 保証度を3つの基準から評価する (1, 2, 3)
  - Identity Assurance Level
  - Authentication Assurance Level
  - Federation Assurance Level
- 3つの基準について、具体的に満たす条件を定める
  - 慎重なリスク評価と議論の結果
- 認定機関は他に委託する
  - InCommon
  - Kantara



# NIST SP800-63批判 (positive/negative)

- トラストフレームワーク構築のために、NIST SP800-63の検討は避けては通れないというのが世間/業界の常識
- 本来は米連邦サービスを利用するための基準
  
- で、Practicalにはどうか（日本で大丈夫か？）



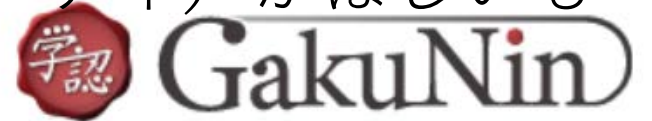
# NIST SP800-63は役に立つか？

- **ポイントを外しているのではないか？**

- 本人確認より、本人が属している組織の信頼度の方が重要
  - 特に（日本の）大学は信頼の起点になれるはず
- サービス提供側からすれば、資格確認（due diligence）のほうが本質的に重要
- サービス提供側からすれば、本人の保証度とともに、属性のassurance, freshnessが重要
- IdP（CSP）に属していない人はどうすればいいのか？

→ **素朴に実装しようとするといろいろな問題が出てくる**

- 本来、われわれ（研究教育に携わる者のコミュニティ）がほしいものはなにか？



- 大学、企業に属し（属していなくても良いが）、その組織の信頼の上に立って、研究コミュニティを作る（基本に帰る）
  - 組織をまたがるのは当たり前
  - 企業研究者の組織化が大切
- Orphan identityの収容
- 組織の信頼性を利用しながら、その組織がどのくらいまじめにやっているかで評価
- 組織内属性の評価 **KYC**



# ということで、NISTは微妙に引っかかる

- サービス提供側が納得するかの議論が抜けがちになる
  - NIST SP800-63では、対象サービスが「米連邦サービス」だから、割り切れた
  - SPを含めた議論が必要（従来のやり方の再評価を含む）
    - 例：スーパーコンピュータ利用申請のときに、「対面」を一回はさむ
- 利用者にとっての便宜をはかることが first priority
- サービス提供側にとっても、アイデンティティ管理は負担
  - 管理の軽減は利益になるはず
  - しかし、その負担が「権力」の源泉でもあった



# 学認トラスト

- 学認は信頼度を「認定する」
- 認定に当たっての評価基準を公表する
- SPは、認定されたIdPからのアサーションを信頼する
- このような世界を作るために、一度、みな集まって話をしよう
  - NIST SP800-63は本格的なリスク評価を経た信頼のおけるものであることを認め、ベースラインとして採用する



## お知らせ

- 【重要】学認 ウェブサイトメンテナンスのお知らせ (2022/2/16) 2022-02-10 16:47
- 【重要】学認サービスの一部停止について (2022/01/16) 2022-01-07 17:17
- 【復旧済み】障害による学認サービスデスクの停止について (2021/12/02) 2021-12-02 12:27
- 【アンケート】多要素・多段階認証で利用可能な要素について ← 2021-11-17 11:21
- 【重要】学認 ウェブサイトメンテナンスのお知らせ (2021/11/18) 2021-11-09 17:26

▶ すべて見る

## 新着資料

- 学認参加IdP運用状況調査票(令和3年度実施版) 2021-11-09 13:10
- 次世代認証基盤構築のための基準策定と配備の観点からの文書評価のお願い ← 2021-11-08 11:26
- CrPCrPSテンプレート (案) ← 2021-11-08 10:51
- IAL2の新学認での運用に当たって (案) ← 2021-11-08 10:51
- 学認技術運用基準新旧対照表(v2.5 : v2.6) 2021-10-25 14:28

▶ すべて見る

# IAL (Identity Assurance Level)

- 大前提：大学はトラストの起点
  - 入学試験の際の高校との文書のやり取り、住民票の提出、対面での学生証手渡し（コロナでだいぶ…）
  - 「普通の組織」としての採用プロセス。文科省の統制（研究者番号等）
  - 「大学」というだけで、組織の信頼度が高い（はず）
- NIST準拠を意識しながら、IdPの今までの努力に報いる方法はないか？





# 学認のIAL評価ドキュメント

- 学認は、「認定」において必要な評価の基準を定めました

1. CSPの大学内での定義と、それに従うNIST/KIAFの読み替えの方針

- - NISTやKIAFの文書のモデルでは従来IdPと呼ばれていたものをCSP (Credential Service Provider) といい、パスワードや証明書などのクレデンシャルを利用者に発行するサービスを行うところを規制の対象としている。そのモデルではVerifierが、そのクレデンシャルを検証してRP (SP) にアサーションを発行する役割を持っている。我々が一般的に考えるIdPは、Verifierと (クレデンシャルの発行という意味での) 一部のCSPの機能を合わせた機能を持っている。CSPの持つ利用者登録は、大学や研究所でいえば、学務や人事を担当する部局の責任の下行われるだろう。CSPとIdPがNISTのモデル的には不完全に分離して運用されていることから、例えば本文書内でのIAL2の実現主体が (我々の言う) IdPなのかCSPなのか、振れることになる。
  - ここでは、最初にこの誤解を生じかねない事態を整理することから始めたい。



- 1.1 大学や研究所で学務や人事がCSPとして利用者登録をおこなっている場合
  - 現在、統一アカウントの運用が大学で普通に観察されるようになってきている。アカウントの発行は、例えば情報基盤センターで行うのではなく、学務や人事の組織にとって信頼できるデータベース（以下Trusted DBと言う）から直接プロビジョニングされる。また、IdPの運用を外部委託（IDaaS）していても、Trusted DBに接続されていればここに当てはまる。
  - このような場合、NISTで規定されているCSPの身元確認は、入学、採用時のプロセスとそれを反映したTrusted DBの維持管理の一部として行われる。このような場合、IdPを運用する部署はNISTに定められたIAL維持のためのアクションの多くについて責任を持つ必要はない。組織の成熟度（入学や採用が事故なく円滑に行われていること）を評価すれば足りる。IdPは、アカウントの生成プロセスとそのポリシーについて、上位の規程を参照しながら定めることで足りる。
- 1.2 IdPが、組織内で運用する共同利用のサービスのIdPとして、アカウントを運用している場合
  - 例えば、共同利用システムを運用していて、組織外部の利用者にアカウントを発行して運用する大学の部局や研究所がこれに当てはまる。この場合は、以降規定することがフルセットで当てはまる。ただし、大学や研究所のアカウントが十分信用できるのなら、それを利用してアカウントを作成する場合、IAL審査のコストを大きく下げることができる。この意味でもホームとなる機関でのIAL（とAAL）は重要である。



- 2 CSPの運用範囲内で定めることと、より上の大学運営にかかわることの分離
  - 以上の観察に基づき、以降ではNIST/KIAFの文書のうち、規定をタイプ1, 2に分類して議論し、新学認参加のIdPが措置することを定める。
- ほとんどのIdPが（運用を整理することで）基準を満たすことができると期待する
  - 「まじめさ」への期待



# SPが求める属性の提供

- 値の保証の宣言：CrPCrPS (Credential Policy/Credential Practice Statement)
  - 欧米の慣習（他人に対しては文書の「契約」で縛る）として、IdPの保証する範囲を文書にして公表する
  - Kantaraとcompatibleなやり方
  - ここで、保証する属性を宣言する
  - REFEDSでは、eduPersonAffiliationの値とそのfreshnessを値で表現
    - それだけではないだろう…



# 様々なアイデンティティと属性の収容

- 特に学認に参加していないところ（企業等）からの参加者をどう収容するか（IDaaS等）
- SPからの声大きいことを認識
  - 従来はSPが個別に「審査」を行ってアカウントを付与
    - 特に全国共同利用の性格をもつ研究所
- 資格確認を統一基準（学認基準）で行う
  - KYC（本人の身元確認） < 組織の評価、組織内での身分（属性）確認、属性のfreshness確認



# ORTHROS, mAP

- ORTHROS: 学認の外のアイデンティティ提供を吸収する PROXY
- mAP: 研究コミュニティをサポートするための属性提供サーバ

→ 詳細は別プレゼンで



# AAL (Authentication Assurance Level)

- 強い保証度を提供するときに、password onlyはもう無理…
  - 2年前の統合認証シンポジウムで、Office365への不正アクセスに対処する経験のプレゼンがありました（弘前大）
- 特に、貴重な計算・情報リソースへアクセスする場合
  - 公開鍵認証の設定がSPごとに（アイデンティティ管理とともに）されている

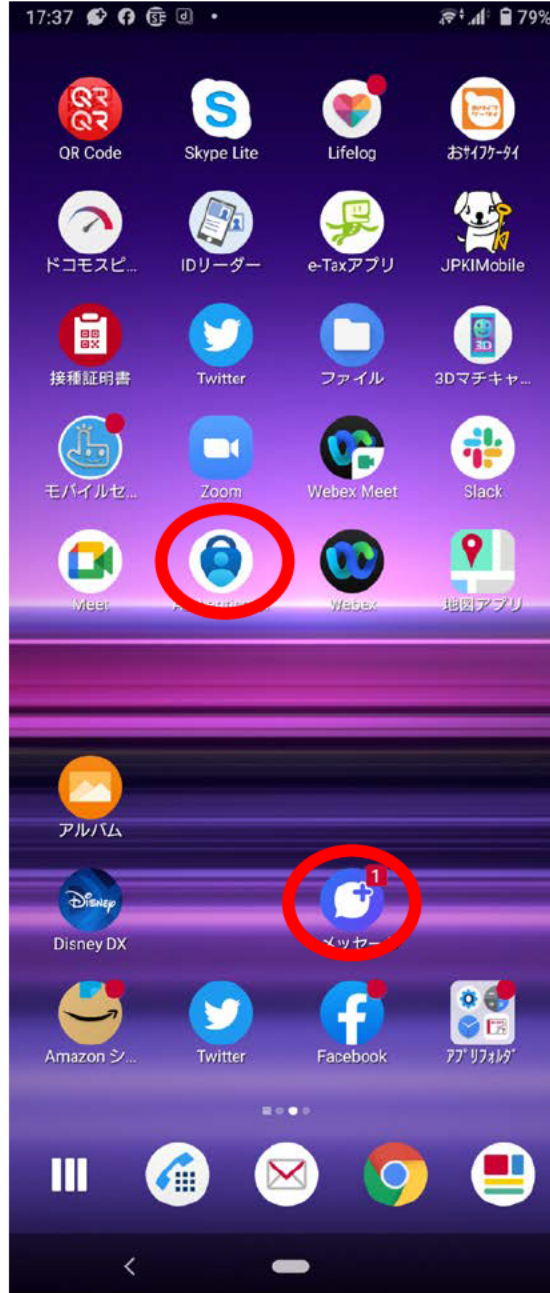


# ここ数年での多要素認証の普及

- (多要素認証ではないが) Googleをはじめとする多段階認証の信頼度↑
- SMSを利用したOTPが生き残る
  - フィッシング対応で少しはやらなくなった↓ (提供側も、都度発生する費用をどこに転嫁すればよいのか悩ましい)
- SmartphoneでのAuthenticator提供
  - MS ADでもサポート
- 証明書認証その他従来手法に代わって急速に普及した
  - 古い世代が置き去りに☺







# パスワードの利用

- パスワードは依然重要な認証手段
- パスワードはなくなるならない
  - パスワードの運用、パスワードポリシーが問題
- パスワードに関してのNIST SP800-63の方針は
  - 個人情報を扱うサービスへのログインはパスワードonly禁止
  - そのかわり、パスワードポリシーは「8文字以上」のみ
  - 「定期変更等を強制してはならない」ということにお墨付きを与えた文書の一つでした



# 学認としては

- **規程1.1** パスワードを認証器として用いる時は以下を満たさなければならない。
- a. パスワードの要件：
  - 利用者が設定する場合は8文字以上、システムがランダムに設定する場合は6文字以上でなければならない。システムがブラックリスト等への登録等、設定を禁止しているパスワードが設定されるようになってはならない。
- 本文書の基本になるKIAF1440（及びNIST SP800-63）では、個人識別情報（PII）を扱う際にはパスワードのみの認証を禁止している。つまり、重要な情報は多要素認証で守るという姿勢を明確にしている。したがって、パスワード認証単独に要求する強度は必ずしも高いとは言えない。この姿勢を正しく理解し、日本でパスワード認証のみを使っている機関が多くあること、そこでPIIを含む情報を処理していることが行われていることを考えれば、ここで定める基準が参加機関でより強力なパスワードポリシーを定めることの妨げにはならない。
- 
- 注) 例えば、総務省では以下でパスワードの一般的なポリシーを提示している。
- [https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/business/staff/01.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html)



# 多要素認証の運用は実は大変で…

- AALは、**認証器そのものの評価**と運用の評価にわかれる
- 認証器そのものの評価は、学認がなんとかしましょう
- 学認は、容認できる認証器を集めて**認証器レジストリ**を運用します
  - 大学個別で認証器の評価をする負担ができるだけかからないように
  - 大学個別の経験を学認にお寄せください



# このスライドを見ている方々へ

- Authenticator等、多要素認証器を開発、リリースしているベンダーの方々（e.g. Microsoft, Google, Y!J, …）、さまざまなコンソーシアム（FIDO, …）の協力をぜひいただきたいと思えます
- 大学個別で認証器を運用している場合も、その評価をもとにレジストリへ登録することができます
- よろしくお願ひします



# AAL2

- 多要素認証の運用が大変であるという状況は変わっていない
  - 「運用まで含めて高いレベル」を求めるなら特に≠SPとしては当然求めてくる
- Smartphoneの普及、その上でのauthenticatorの提供
  - BYODを恒常的に仮定してよいのか？という問題はあるが…
- PCやSmartphoneでの様々なauthenticatorの提供
- 少し前に進むことができるのではないか？
  - 少なくとも、高度なサービスを求める利用者に対しては



# AALの評価基準文書

- AALの評価基準文書を用意しています
- NIST準拠を意識しています
- 認証器の種類については**レジストリの運用**の形で学認が責任をもちます
  - 認証器本体の運用については「学認レジストリに登録されているもの」と記すつもりです
- 一方、認証器の運用は各大学で注意深く行う必要があります



# 認証器の運用での注意

- 認証器の利用者とのバインディング
  - 本人確認、認証器の配布、…
  - これが、運用がスケールしない最大の原因
  - 全学レベルでの高いレベルの運用は必要としないまでも、一定の人たち（SPが強い認証を要求する人たち）に対しては高いレベルの運用が必要
  - →がんばりましょう
- セキュリティパラメタの管理
  - Defaultの運用をすれば（多分）大丈夫





# どのくらい早期に始められるか

- 有志のIdPとSPに集まっていたいただいて、PoCレベルのものをできるだけ早く始められるようにがんばっています
  - タイムリーな情報発信をこころがけます
- 利用者にとっては
  - 良いサービスが新規にフルオンラインで提供されるご利益が期待できます
  - 利用者のアイデンティティの運用と認証は、少し厳格になる
    - SPが安心できるように



# 終わりに

- 次世代学認のサービスメニューを示しました
  - アイデンティティの保証↑
  - 認証の保証↑
  - SPのもつ貴重な計算・情報リソースをフルオンラインで利用可能になる範囲を拡大
- 学認は、大学（IdP）とサービス（SP）を、上記の面からサポートします

