学認AAL2認証器レジストリについて

2025年6月18日　学術情報基盤オープンフォーラム 2025

トラスト・デジタルID基盤研究開発センター 水元 明法

学認AAL2 認証器レジストリ 公開中

- https://level2.gakunin.jp/
- https://level2.gakunin.jp/en/

学認AAL2認証器レジストリ

Search

auth-reg

登録済み認証器　認証器の詳細　認証器運用時のリスク評価　認証器レジストリとは　お問い合わせ

Update(最終更新日 2024/04/24)

- 2024/04/24 公開版
- 2024/04/01 登録済み認証器に以下を追加
  - Google Authenticator
  - Microsoft Authenticator
  - FIDO準拠デバイス
  - UPKI電子証明書発行サービス クライアント証明書
- 2024/04/01 認証器運用時のリスク評価シートを掲載

登録済み認証器

登録済み認証器一覧

認証器名または準拠標準	認証器バージョン	提供会社	認証器種類	認証器カテゴリ	要素			承認日	審査学認基準	記載情報更新日
					所持	生体	知識			
Google Authenticator	6.0	Google	Single-Factor OTP Device（単要素OTPデバイス）	単要素	○			2024/2/29	Ver.1.0	2024/4/1
Microsoft Authenticator	6.2312.8150	Microsoft	Single-Factor OTP Device（単要素OTPデバイス）	単要素	○			2024/2/29	Ver.1.0	2024/4/1
FIDO(FIDO2)	1.2 Proposed Standard	FIDO Alliance の仕様に基づき設計や製造を行う認証器メーカ	Multi-Factor Cryptographic Device（多要素暗号デバイス）	多要素	○	□	□	2024/2/29	Ver.1.0	2024/4/1
FIDO(CTAP1(U2F))	1.2 Proposed Standard	FIDO Alliance の仕様に基づき設計や製造を行う認証器メーカ	Single-Factor Cryptographic Device（単要素暗号デバイス）	単要素	○			2024/2/29	Ver.1.0	2024/4/1
FIDO(UAF)	1.2 Proposed Standard	FIDO Alliance の仕様に基づき設計や製造を行う認証器メーカ	Multi-Factor Cryptographic Device（多要素暗号デバイス）	多要素	○	□	□	2024/2/29	Ver.1.0	2024/4/1
UPKI電子証明書発行サービス・クライアント証明書	2023年12月14日の仕様変更準拠	SECOM Trust Systems Co., Ltd.	Single-Factor Cryptographic Software（単要素暗号ソフトウェア）	単要素	○			2024/3/29	Ver.1.0	2024/4/1

"□"はいずれかを選択する。

認証器レジストリとは？

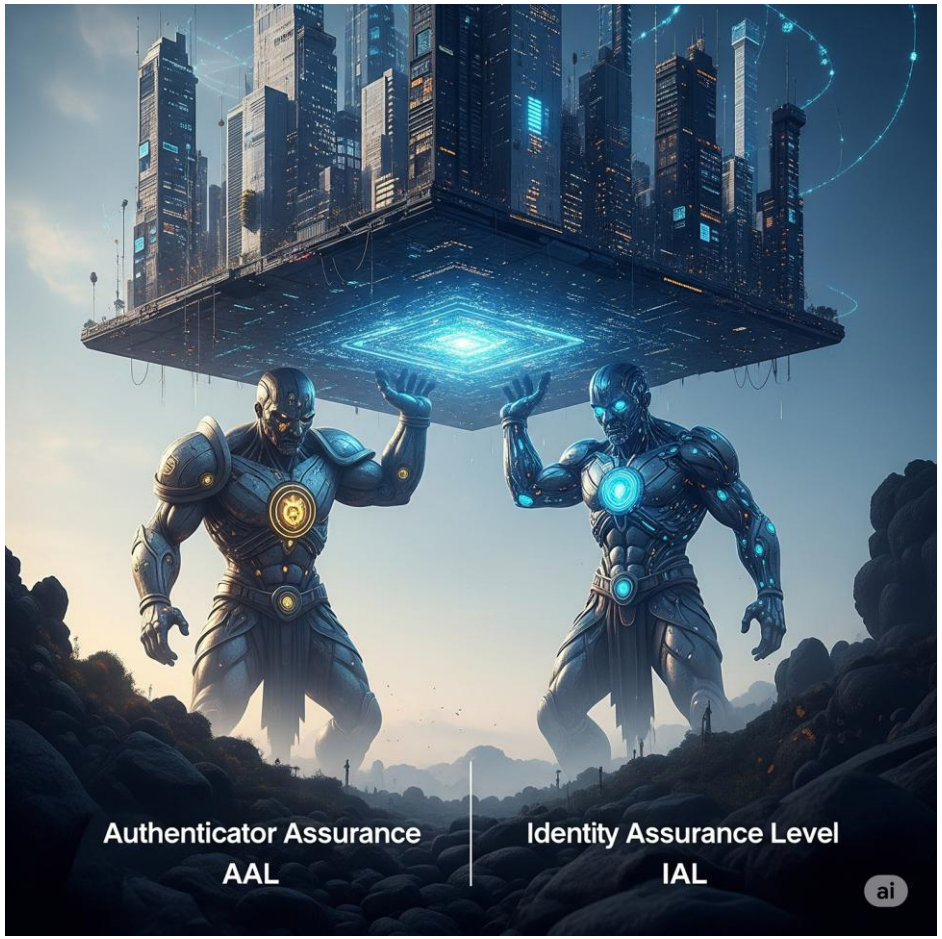
- 学認が提供する、学認AAL2対応認証器と関連する情報が登録されたレジストリ
  - 学認は「認証器」の性能を調査し、AAL2の認証に利用できる認証器がわかるレジストリを用意する
  - 大学・研究機関は、本レジストリを参照することで、AAL2に対応した認証器を容易に選択・導入することができる
  - 学認参加機関の求めに応じて認証器の審査・認定を行った場合、その結果を登録して定期的に更新する
- AAL2水準の認証とは？
  - パスワードに加えて、スマートフォンアプリやICカードなどの要素を用いた多要素認証を指し、セキュリティ強度を高める。

レジストリの必要性と現状

- なぜレジストリが必要なのか？
  - 近年、サイバー攻撃の巧妙化・増加に伴い、大学・研究機関における情報セキュリティ対策の強化が喫緊の課題となっている
  - 特に、個人情報や研究データなどの重要情報を保護するため、強固な認証システムの導入が不可欠である
  - しかし、認証器は多種多様であり、各機関が個別に調査・評価することは大きな負担となる
    - この認証器はどのタイプに該当するのか？
    - この認証器は学認AAL2基準のチェック項目を満たすか？
    - この認証器は単体で単要素か？多要素か？
  - そこで、学認AAL2認証器レジストリが重要な役割を果たす

レジストリがもたらすメリット

- 大学・研究機関にとってのメリット
  - AAL2認証器の導入・運用コストの削減
  - 認証システムのセキュリティレベル向上
  - 最新のセキュリティ情報へのアクセス
  - 運用担当者の負担軽減
- 学認全体へのメリット
  - 学術情報環境全体のセキュリティ強化
  - 各機関における認証システムの標準化
  - セキュリティに関する情報共有の促進

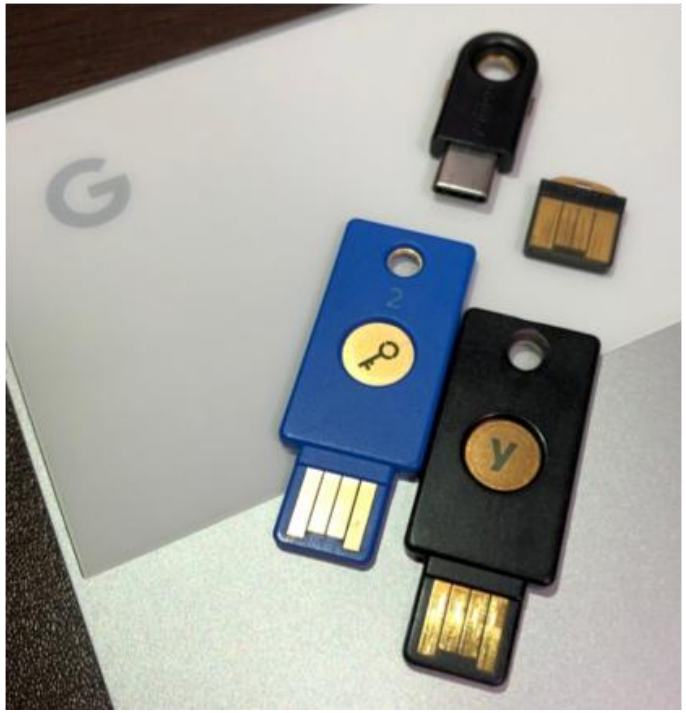


どんな情報が？

- 記載内容
  - AAL2基準適合認証器の一覧
    - **FIDO認証を取得した認証器**
    - **OTPデバイス：MS/Google Authenticator**
    - **UPKIのクライアント証明書**
    - **経路外デバイス：tiqr**
  - 認証器の詳細（認証器ごと）
  - 認証器運用時のリスク評価
  - 認証器レジストリとは
  - NIST SP800-63B supplement和訳版
  - お問い合わせ（フォームへ）
- コンテンツはGitHubで管理
  - https://github.com/gakunin/auth-reg

FIDO認証を取得した認証器

- FIDOアライアンスが提供する認定制度で認められた認証器
  - 学認が個々の製品を直接審査するのではなく、国際的な標準化団体であるFIDO Allianceの認定リストを信頼し、レジストリに登録
  - FIDOアライアンスのWebサイトにて一覧が提供されている
  - 網羅したJSONファイルが取得可能
    - https://fidoalliance.org/metadata/
- 多要素/単一要素暗号デバイス



ワンタイムパスワード

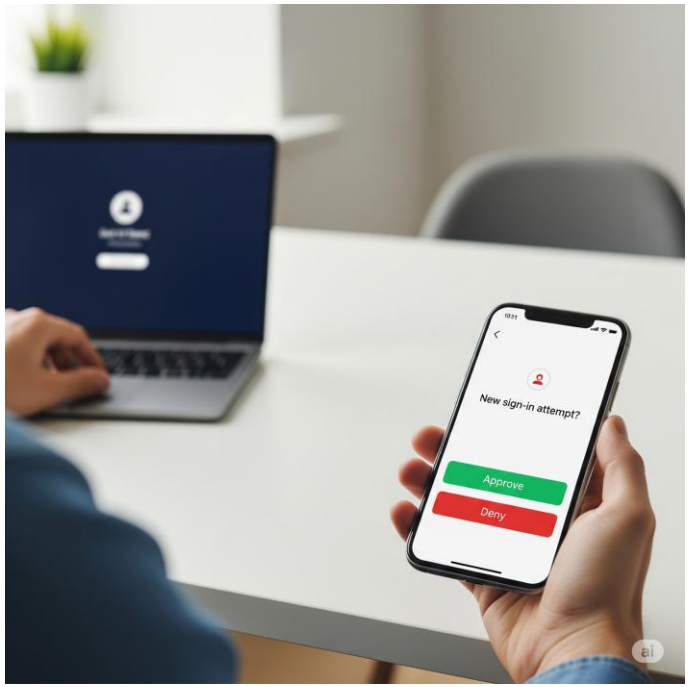
- スマートフォンにインストール
  - Microsoft Authenticator
  - Google Authenticator
- PCにインストール（ブラウザ拡張など）
  - WinAuth
  - Authenticator.cc
- 単一要素OTPデバイス

UPKI クライアント証明書

- UPKIの認証局から発行されるクライアント証明書
  - 個人認証用
- 単一要素暗号ソフトウェア

経路外デバイス

- tiqr
  - https://tiqr.org/
- 経路外デバイス
- メインの通信とは「別の経路」を使う認証方法
  - PCでウェブサイトにログインしようとする時（**メインの経路**）
  - 認証の確認がスマートフォンに届く（**別の経路**）
- スマートフォンが「経路外デバイス」として扱われることが多い



まとめ

- 認証器レジストリで、安全・簡単な多要素認証導入を
- 信頼できる認証器情報を提供
- 今後の展開
  - 学認は、参加機関のニーズに応じて認証器の審査・登録を継続し、常に最新の情報を提供します
  - 本レジストリの活用を通じて、学術情報基盤全体のセキュリティ強化に貢献していきます