# 大学の現状と次世代認証連携に対する要望

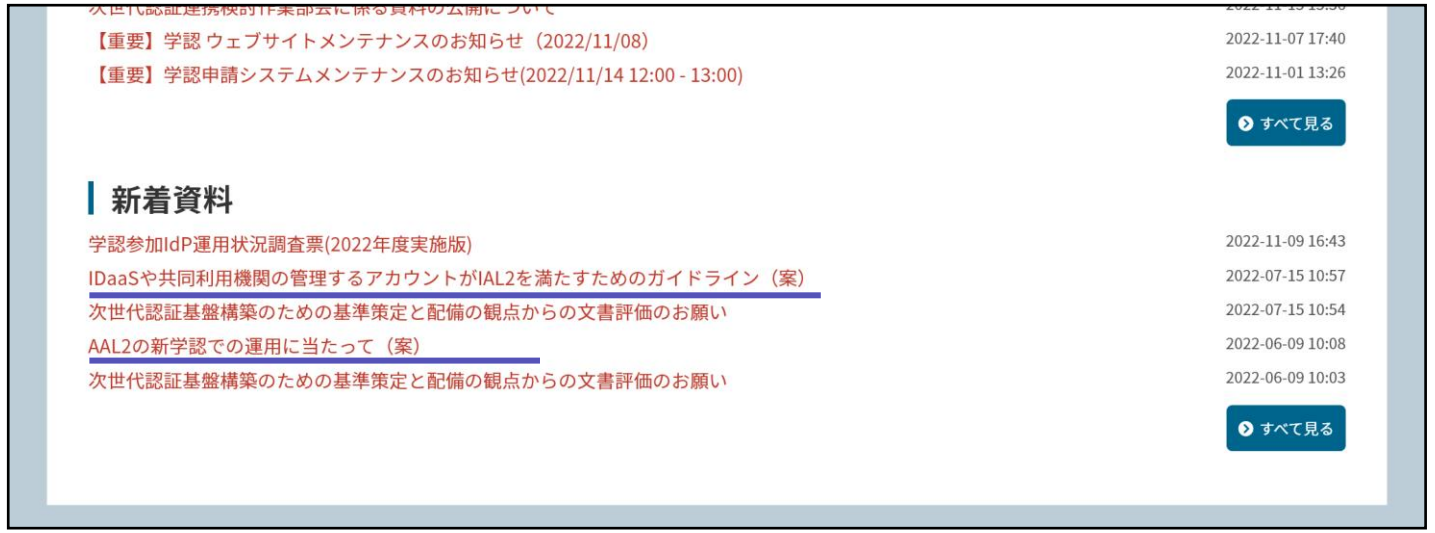
群馬大学総合情報メディアセンター

浜元信州

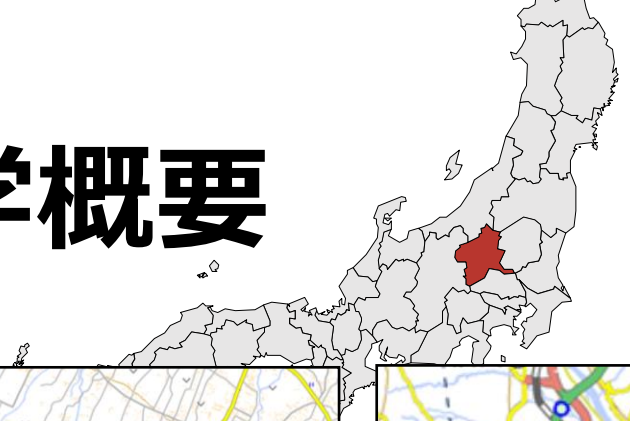
# はじめに

- 次世代認証連携
  - IdPの送出する情報をSPがどこまで信用してよいのか分からないので，一定の基準を作り，遵守することで，IdPを信用してもらいましょう。…ということ？
  - 結果として，いろいろなSPが利用できるようになって便利になる。

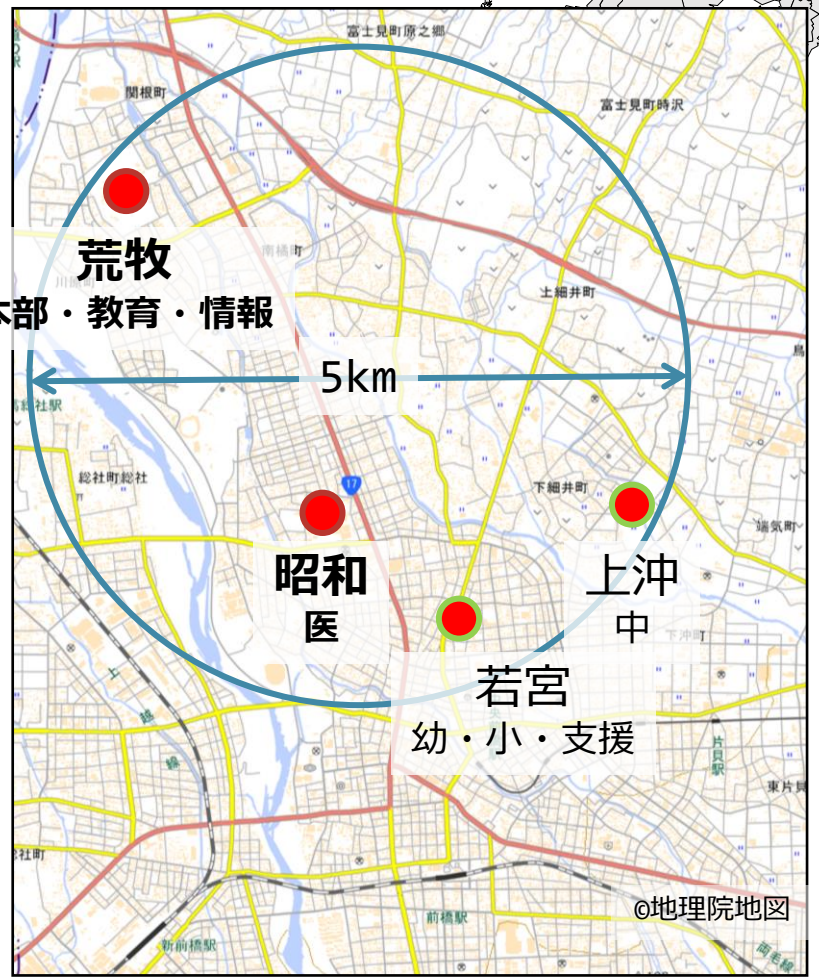
- IAL2（身元確認）
- AAL2（当人確認）
- 案は出ているようですが，読み込めてないです。

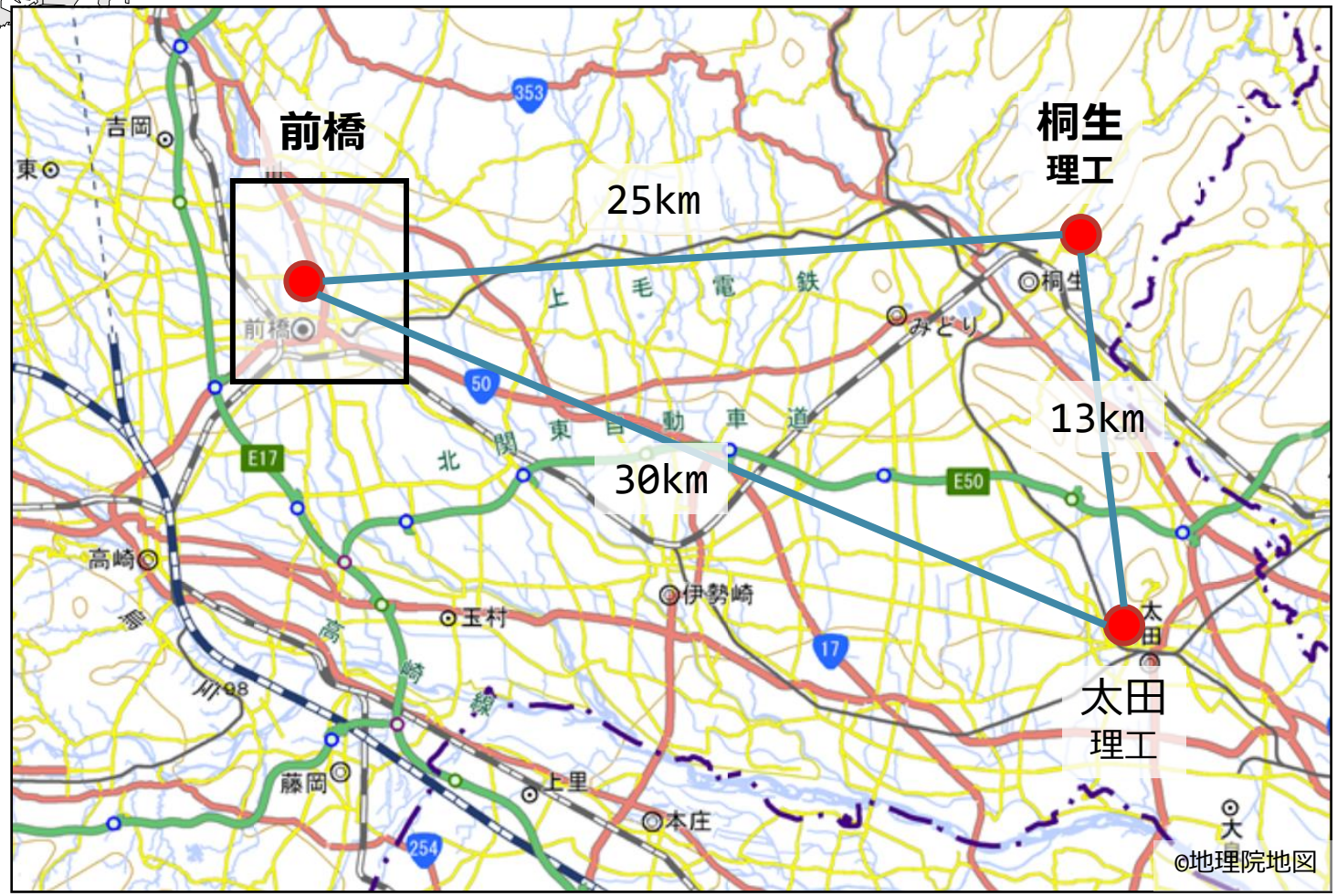


# 群馬大学概要

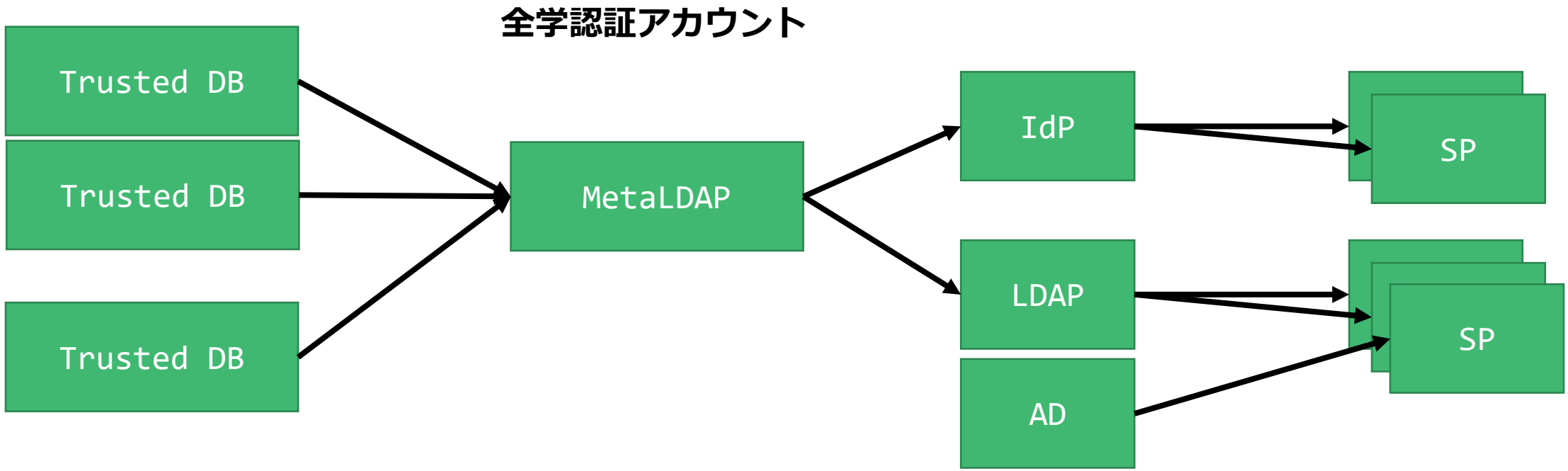


- 学生約6,500人／教職員約2,500人
- 共同教育学部（附属幼・小・中・支援）
- 情報学部（社会情報）
- 医学部（医・保健）・医学部附属病院・生体調節研究所
- 理工学部



# 群馬大学の認証基盤




**アカウント生成**
**アカウント配布**

身元確認(IAL)
(Trusted DB)

当人確認(AAL)
eKYC
多要素

**認証・認可**

| | |
|---|---|
| 学内SSO | 23SP |
| 学内LDAP | 12SP |
| 学外SSO | 23SP |

# Trusted DB

- 学務部の学生DB
  - 学生
  - 非正規学生
    （科目等履修生/聴講生/研究生など）
- 人事給与DB
  - 常勤職員
  - 非常勤職員
  - 常勤教員
  - 非常勤教員

- 学務部のDB
  - 卒業生・単位取得退学者
- 総務部の職員名簿
  - 名誉教授
- 研究推進部のDB
  - 特別研究員
  - 共同研究員
  - 教職員支援機構研修員
  - 外国人研究者
  - 協力研究員

＊学認連携しているものには下線

# アカウント配布・削除

- 発行
  - 学生：　　学務部が　　対面で実施（オリエンテーション）
  - 事務職員：　情報基盤係が対面で実施（採用日に係に伝達）
  - 教員：　　**総務部経由**で対面・学内便・郵送
    （採用書類の電子メール?）
- 削除
  - 学生：　　卒業時
  - 事務職員：　退職後3か月
  - 教員：　　退職後3か月
    （+採用前3か月：半期採用の非常勤講師のアカウントを消さないための措置）

# 再発行

- パスワード再発行
  1．本人確認書類の写真とIDを対面で照合
  2．本人確認を代理人に依頼（本人からの委任状）
  3．本人確認書類の情報と既知の情報を照合して郵送（主に卒業生・名誉教授のみ）

- 2段階認証のリセット（コロナ対応により追加）
  - **本人確認書類の写真とセルフィー**をメールで送付してもらい，2段階認証を送信元メールアドレスに変更する

# 認証・認可

- 2要素認証
  - ID + OTP(アプリ or メールアドレス)
  - 学外からのアクセスのみ適用
  - 学生は現在のところ希望者のみ
  - 一部SPは2要素認証不要（Google/MSなどの重要サービスには必須）
- 実装
  - セシオス社の製品を利用
    （Secioss Access Manager Enterprise Edition: 通称SAME）
  - オンプレとクラウド(Azure)で冗長化
  - Shibbolethを独自実装した製品（拡張できる？）

# 課題など

- 共同教育学部
  - 群馬大学と宇都宮大学で一つの教育学部
  - 現状，2つのIDを持つ
  - 来年度から学認を利用した認証にする予定
  - 人が行き来するようになったらSSOでないサービスどうするか。

- システム更新
  - IDaaSへの移行は，2023年の調達では見送り

# 要望

- IAL2,AAL2のガイドラインなどの文書が簡単ではない。（この手の文書は仕方ないですが）
- 製品でカバーできる部分は，どの部分をどうすると要件を満たすのか示して欲しい。（学認クラウドチェックリストのようなもの？）
- 監査はある？

パスワード検証側の要件：

以下を認定基準とする。

1. 設定されたパスワードを長さ制限なしに検証すること
2. システムがランダムに設定する場合はランダム性の要件を充たしていること
3. パスワード入力に際してヒントを与えないこと
4. 不適切と定めたパスワードを登録させないこと。拒否の場合は理由を提示すること
5. スロットリングを実装すること
6. パスワードが突破されたと判断した場合はパスワード変更を安全な方法で強制できること
7. パスワードを格納する場合は、ハッシュ化、ソルトについて「適切に」暗号学的な処理がなされていること。