AXIES 認証基盤部会セミナー
「学術認証基盤における次世代認証と認証強度の考え方」

茨城大学
Ibaraki University

フェデレーション環境における認証方式と認証強度の課題

茨城大学: 野口 宏

会場: キャンパスプラザ京都

認証における(主に)運用面での課題

1. 認証におけるサーバ負荷
2. 認証器の交換とリカバリ
3. 認証強度と有効時間
4. サインアウト(タイムアウト)

当人認証のライフサイクル

1. 認証器登録
   a. 当人認証に用いる認証機と利用者の紐付け
2. 当人認証
   a. 登録済み利用者と申請者が同一であることを確認(認証器)
3. 盗難, 紛失対応
   a. 認証器の無効化
   b. アカウント停止
4. アカウント回復
   a. 停止されたアカウントの回復

「DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」より
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/12cb1a6c/20250930_resources_standard_guideline_identityverification_01.pdf

認証要素

- 知識要素
  - 記憶
- 所有要素
  - ルックアップシークレット
  - 経路外デバイス
  - OTP
  - クライアント証明書
  - FIDO U2F USBドングル
- 生体要素
  - OTP
  - クライアント証明書
  - FIDO U2F USBドングル
- 振る舞い要素
  - ピクチャパスワード
- 位置要素
- 時刻要素

認証器

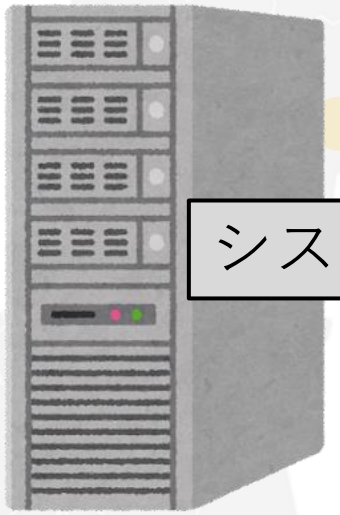
- 記憶 [知識]
  - パスワード
- ルックアップシークレット [所有]
  - 乱数表
- 経路外デバイス: 別チャネル [所有]
  - SMSでのコード送信
  - スマフォアプリへのプッシュ通知
- OTP [所有, 生体]
  - OTPアプリ
  - OTPアプリ(Touch ID等)
- 暗号認証器 [所有, 生体]
  - クライアント証明書
  - FIDO U2F USBドングル
  - FIDO U2F USBドングル(指紋認証)
- 振る舞い
  - Windows:ピクチャパスワード
- 位置
  - IPアドレス, 経路
  - GPS
  - ping遅延
- 時刻
  - 位置との組み合わせ: 急な移動

茨城大学
Ibaraki University

1. 認証におけるサーバ負荷

パスワード

ID: id(a); PW: pw(a)



システムa

クレデンシャルID	システム名	ID	PW
crp(a)	sys(a)	id(a)	pw(a)
:	:	:	:

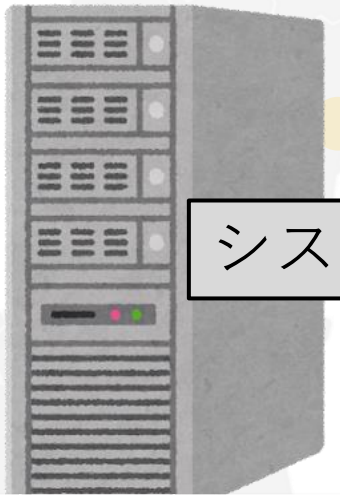
クレデンシャルID	ID	PW
crp(a)	id(a)	pw(id(a))
:	:	:

SMS プッシュ通知

ID: id(a); PW: pw(a)

code
[別回線,t(id(a),i)]

code



システムa

クレデンシャルID	システム名	ID	PW
crp(a)	sys(a)	id(a)	pw(a)
:	:	:	:

クレデンシャルID	システム名	ID	Tel#
crm(a,1)	sys(a)	id(a)	t(a,1)
:	:	:	:

複数の可能性
・電話番号

クレデンシャルID	ID	PW
crp(a)	id(a)	pw(id(a))
:	:	:

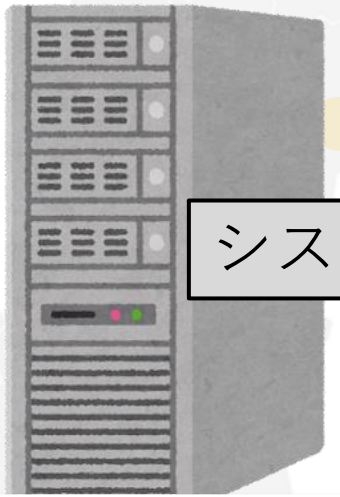
クレデンシャルID	ID	Tel#
crm(a,1)	id(a)	t(id(a),1)
:	:	:

TOTP

ID: id(a); PW: pw(a)

OTP要求

OTP: otp(a,id(a),i,t)



システムa

クレデンシャルID	システム名	ID	PW
crp(a)	sys(a)	id(a)	pw(a)
:	:	:	:

クレデンシャルID	システム名	ID	TOTP種
crm(a,1)	sys(a)	id(a)	o(a,id(a),1)
:	:	:	:

要時刻同期

クレデンシャルID	ID	PW
crp(a)	id(a)	pw(id(a))
:	:	:

クレデンシャルID	ID	TOTP種
crm(a,1)	id(a)	o(id(a),1)
:	:	:

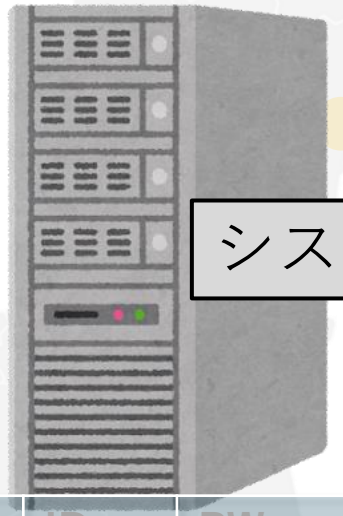
複数の可能性
・認証器:種

Passkeys

ID: id(a)

チャレンジ

アサーション
[チャレンジと
クレデンシャルIDを
秘密鍵で署名]



システムa

クレデンシャルID	システム名	ID	PW
crp(a)	sys(a)	id(a)	pw(a)
:			

クレデンシャルID	システム名	ID	認証器ID	秘密鍵
crm(a,1)	sys(a)	id(a)	at(1)	sk(a,at(1))
:	:	:	:	

複数の可能性
・認証器:鍵組

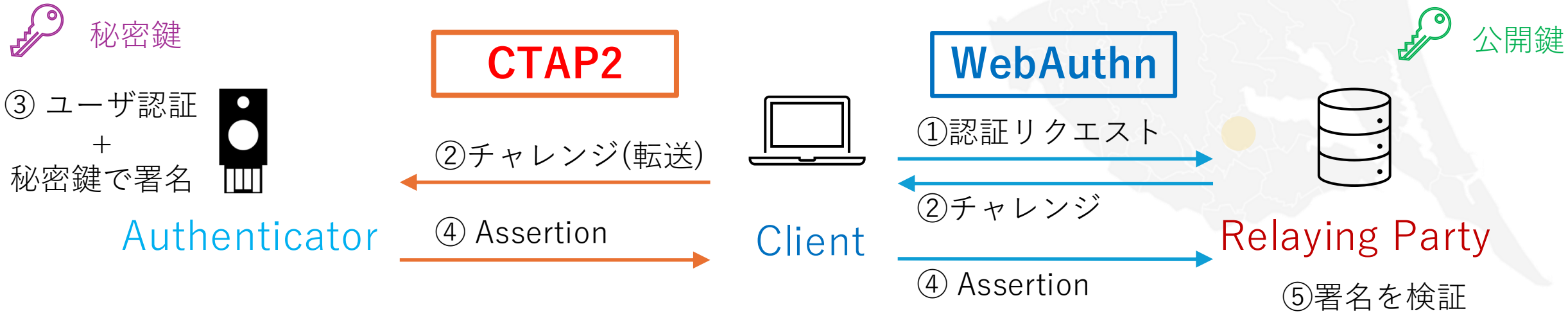
クレデンシャルID	ID	PW
crp(a)	id(a)	pw(id(a))
:		

クレデンシャルID	ID	認証器ID	公開鍵
crm(a,1)	id(a)	at(1)	pk(id(a)at(1))
:	:	:	

FIDO2

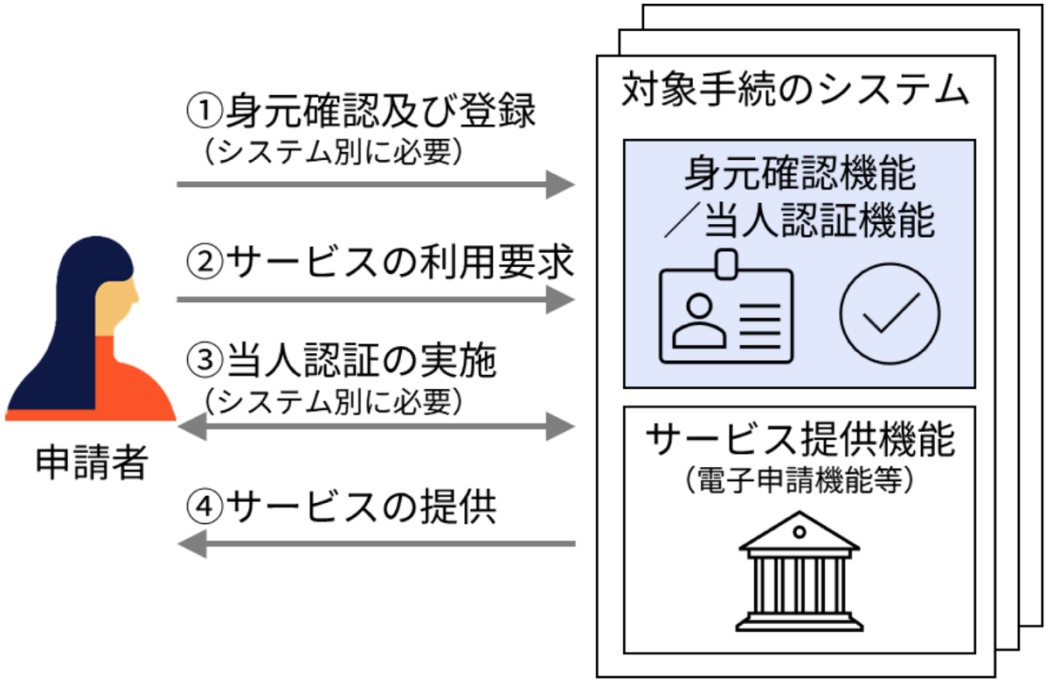
- FIDO Alliance策定の公開鍵暗号を使用したパスワードレス認証の規格

- **WebAuthn**
  Webブラウザで利用可能なユーザ認証のためのAPI
- **CTAP2**(Client-to-Authenticator Protocol 2)
  Client Deviceと外部のAuthenticatorの通信のためのプロトコル

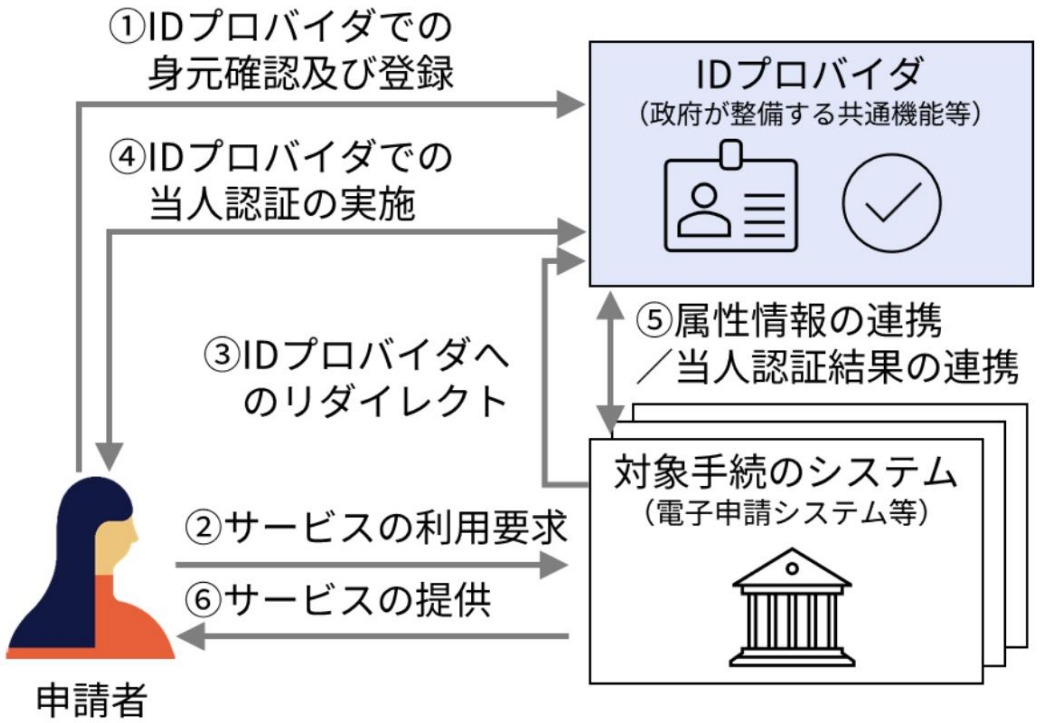


非連携モデルと連携モデル

非連携モデルの概要図
non-federated model



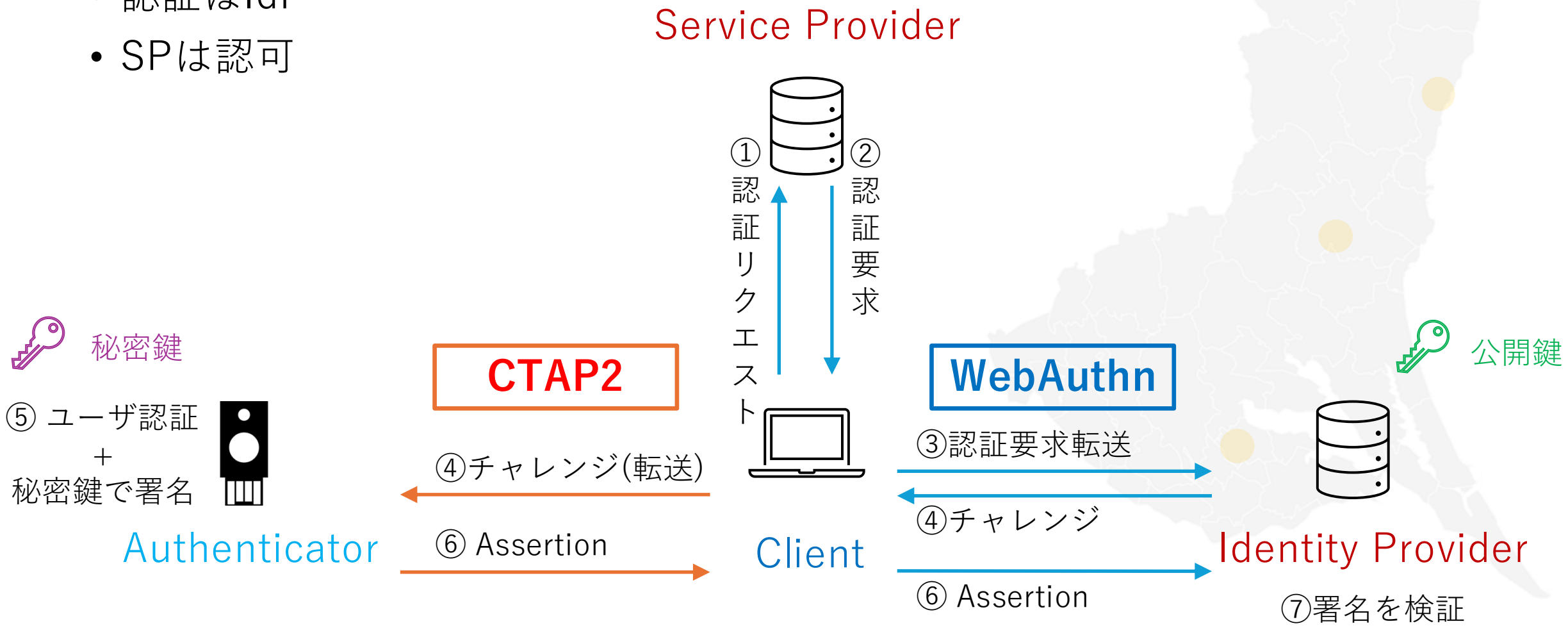
連携モデルの概要図
federated model



「DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」より
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/12cb1a6c/20250930_resources_standard_guideline_identityverification_01.pdf

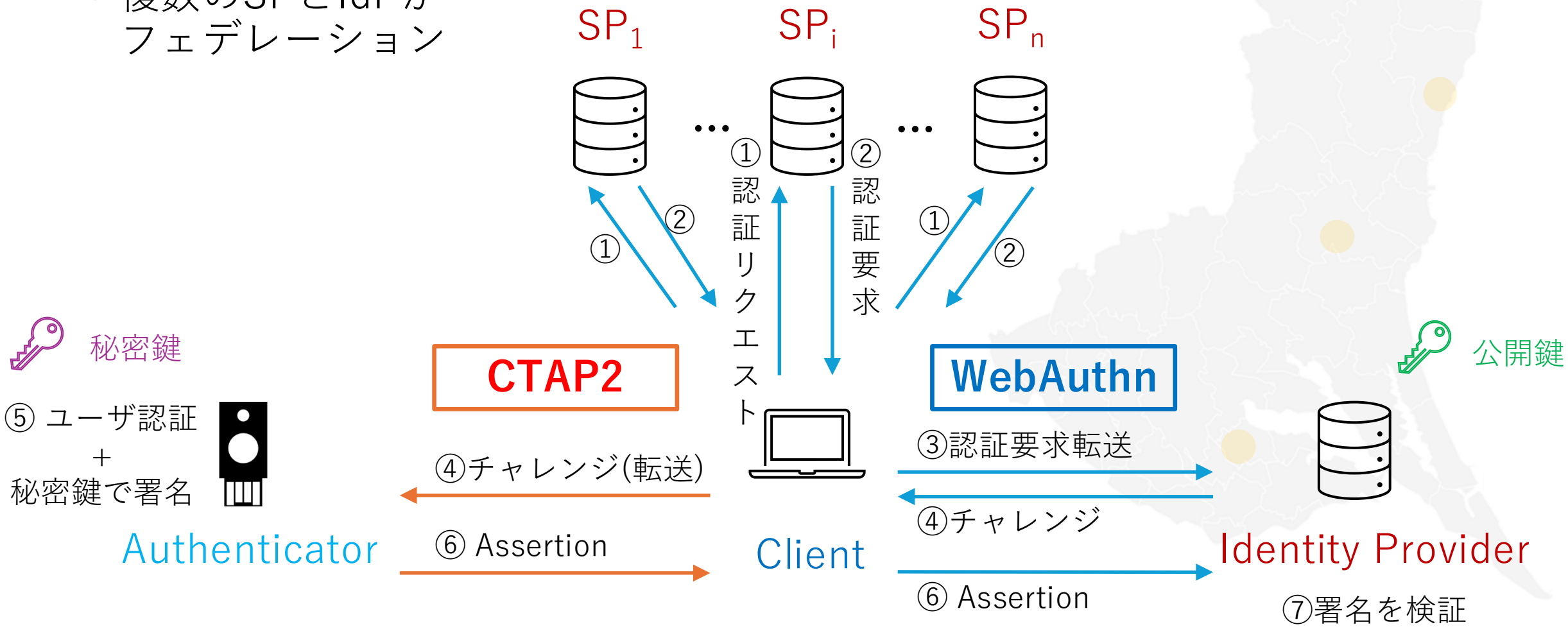
フェデレーション環境

- 認証はIdP
- SPは認可



フェデレーション環境

- 複数のSPとIdPがフェデレーション



2. 認証器の交換とリカバリ

認証器の交換

- スマフォ
  - SMS
  - プッシュ通知(アプリ)
  - TOTP
  - Passkeys
- パスワードマネージャ
  - TOTP
  - Passkeys
- ハードウェアキー
  - Passkeys

リカバリ

- バックアップ
  - (できることを知らない)
- 複数の種類
  - 一つは継続できるもの
- 同種でも複数
  - パスワードマネージャ
    - スマフォ標準 + サードパーティ
  - PWmgr + ハードウェアキー
  - ハードウェアキー x2

3. 認証強度と有効時間

- 認証強度と有効時間
  - 強度が高い
    ➡ より機微な情報の取り扱い
    ➡ 有効時間を短く
  - AAL: 1 ⇆ 3
    有効時間: 長 ⇆ 短

- 認証強度の指定
  - SP
  - IdP

- 認証の有効時間の指定
  - SP
  - IdP

  - OAuth2.0 (RFC9470)
    - “max_age”で指定

茨城大学
Ibaraki University

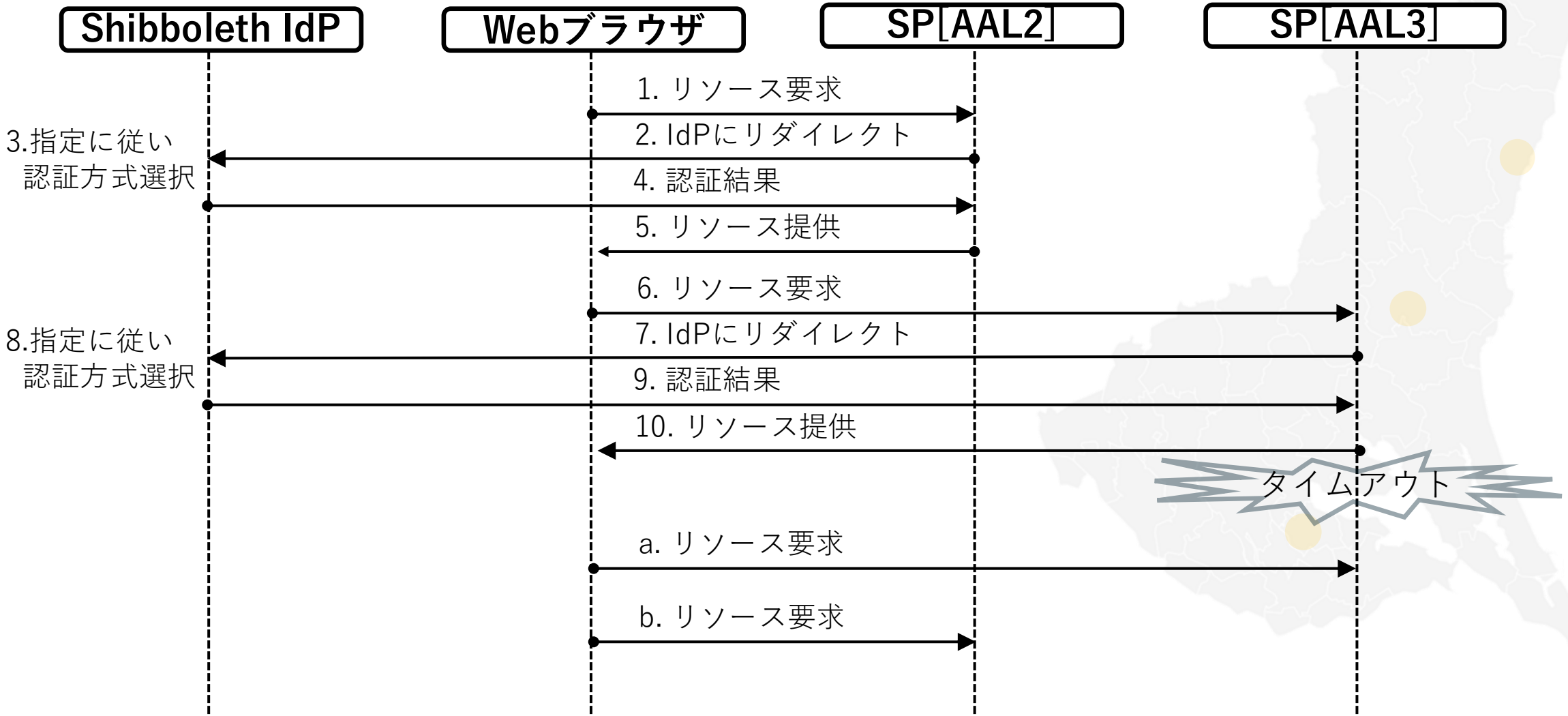
4. サインアウト

フェデレーション環境でのサインイン

- SSO (シングル・サインオン)
  - サインインの作業は1度のみで様々なサービスから認可

- ステップアップ認証
  - 認証時の認証強度(AAL) > 要求認証強度　⇨ 再認証不要
  - 認証時の認証強度(AAL) < 要求認証強度　⇨ 要求認証強度で再認証

認証のタイムアウト


Shibboleth IdP
Webブラウザ
SP[AAL2]
SP[AAL3]
1. リソース要求
2. IdPにリダイレクト
3.指定に従い
認証方式選択
4. 認証結果
5. リソース提供
6. リソース要求
7. IdPにリダイレクト
8.指定に従い
認証方式選択
9. 認証結果
10. リソース提供
タイムアウト
a. リソース要求
b. リソース要求

認証のタイムアウト

- a(AAL3のSPへ要求)の場合
  - 再認証

- b (AAL2のSPへ要求)の場合
  - 再認証無しでのサービス利用を希望

  - 3においてAAL2で認証した場合 ⇨ 再認証無しでサービス利用(†)
    - AAL3はタイムアウトしたがAAL2はしてない
  - 3においてAAL3で認証した場合 ⇨ 再認証必要? (‡)
    - AAL3はタイムアウトしてAAL2では認証してない

サインオンとサインアウト

- シングル・サインオン ⇆ シングル・サインアウト
  - サインオン: 認証作業は1度のみ
  - ➡ サインアウト: 1度の作業でサインインした全てからサインアウト

- ステップアップ認証 ⇆ ステップダウン・サインアウト(?)
  - 認証: 高レベル要求時は再認証
  - ➡ サインアウト: 低レベル要求時は再認証不要
    †, ‡で異なる処理
    (suして作業終了後にexit)

まとめ

- 4つの課題
  1. 認証におけるサーバ負荷
  2. 認証器の交換とリカバリ
  3. 認証強度と有効時間
  4. サインアウト(タイムアウト)

ご清聴ありがとございました