文献紹介
-Digital Identity Guidelines と現状報告

20200513

岡部研M1　畠山

目次

- 文献紹介
  - NIST SP800ー63ー3 (読んでみたかった)
- 今やっていることとこれから
  - 研究室ZTNの構成検討

- 僕の研究内容については次の研究会で
  - DICOMO発表練習も兼ねて

NIST SP800-63-3

原: https://pages.nist.gov/800-63-3/sp800-63-3.html

訳: https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

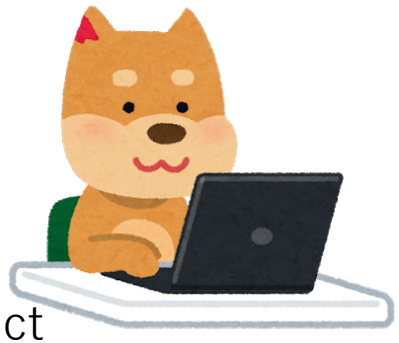
NIST SP 800-63-3とは

- NIST(National Institute of Standards and Technology)
  - 米国標準技術研究所とも
- SP 800シリーズ (Special Publications)
  - NISTが発行するガイドライン群
  - セキュリティとかプライバシーに関すること
- SP 800-63-3
  - Digital Identity Guidelinesの第３版
  - デジタルIDサービスを実装する政府機関の技術要件を定める
  - オープンネットワークを介して政府のITシステムとやり取りするユーザの identity proofing と authentication のガイドライン

Digital Identity とは

※Identity とは
特定のコンテキストにおいて, ある Subject を他と区別できるかたちで表現する, Attribute ないしは Attribute の集合.

- Digital Identity := あるSubjectの一意な表現 on online transaction
  - Subject := 人とか組織とかサービスとかデバイスとか…
- Digital Identity は
  - あるデジタルサービスのコンテキストにおいて 一意
  - 全てのコンテキストを跨いで Subject を一意に識別するとは限らない
  - デジタルサービスは、Accessしてきた Subjectの現実世界でのIdentityを知る必要はない



Subject

Digital Identity

通信

Service

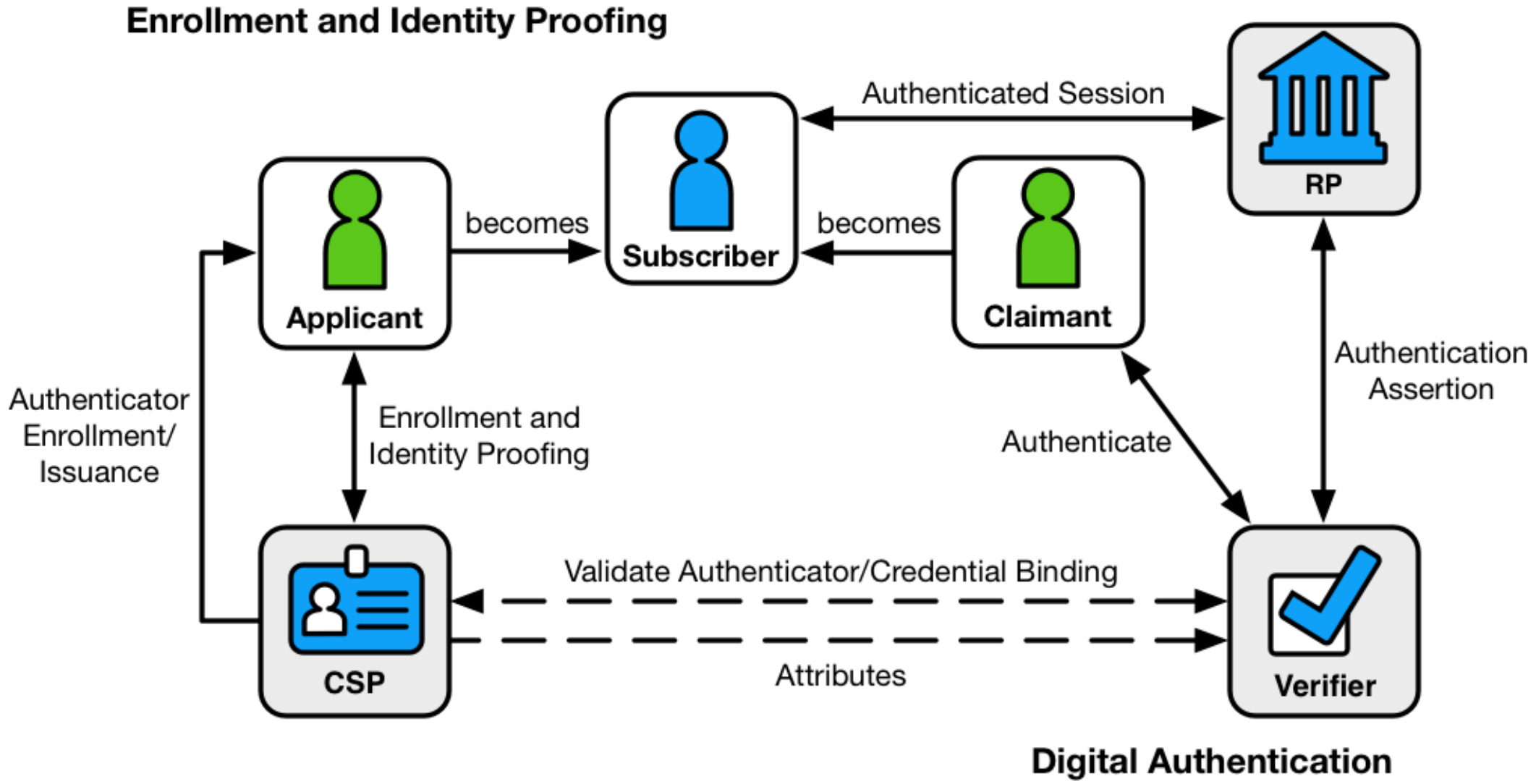
Digital Identity Model

- Service が Subject の Digital Identity を知るためには
  - Subject の Digitial Identity のEnroll(登録)
    - -> Identity Proofing
  - アクセスしてきたSubject のDigital Identityの主張を検証
    - -> Digital Authentication

Identity Proofing と Authentication

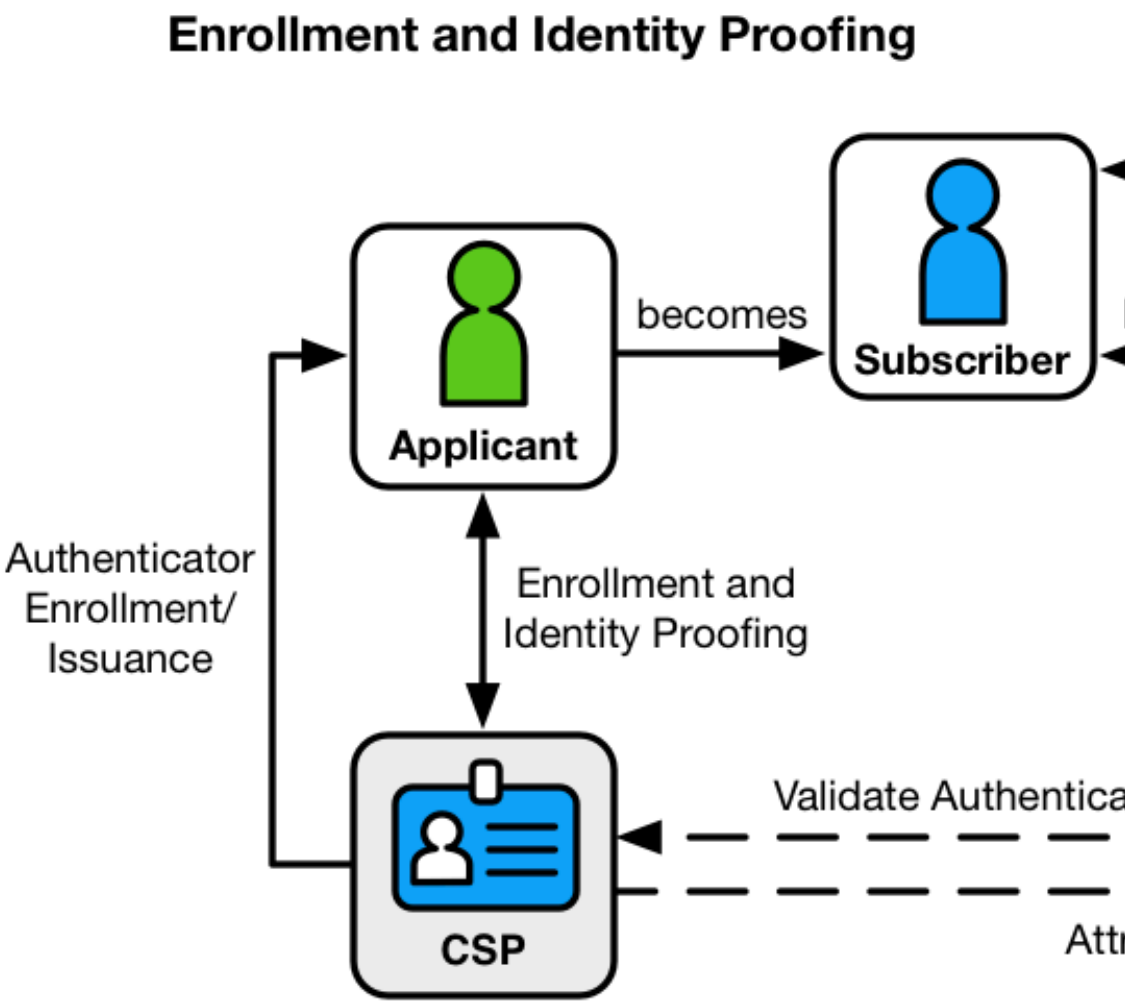
- Identity Proofing :=
  - ある Subject が主張する自分自身であることを証明する行為
  - Ditital Identity と現実のIdentityの紐付け
- Digital Authentication
  - サービスにアクセスしようとしている Subject が自分の Digital Identity に紐づけられた正当な Authenticator(passwordなど) を管理下に置いていることを証明する行為
- Authentication に成功したとは
  - サービスにアクセスしてきたSubjectが
    以前にアクセスしていたSubjectと同一であることを
    適切なリスクに基づいて保証されたということ

Digital Identity Model



https://pages.nist.gov/800-63-3/sp800-63-3.html#63Sec4-Figure1

Identity Proofing



用語

- Applicant :登録される前のSubject
- Subscriber :CSPに登録されたSubject
- CSP(Credential Service Provider)
  - Applicantの登録先
  - Subscriber の Credentialを発行する trusted entity
- Credentials :
  - Identity と Authenticator を紐付けるデータ構造
- Authenticator: パスワードとか

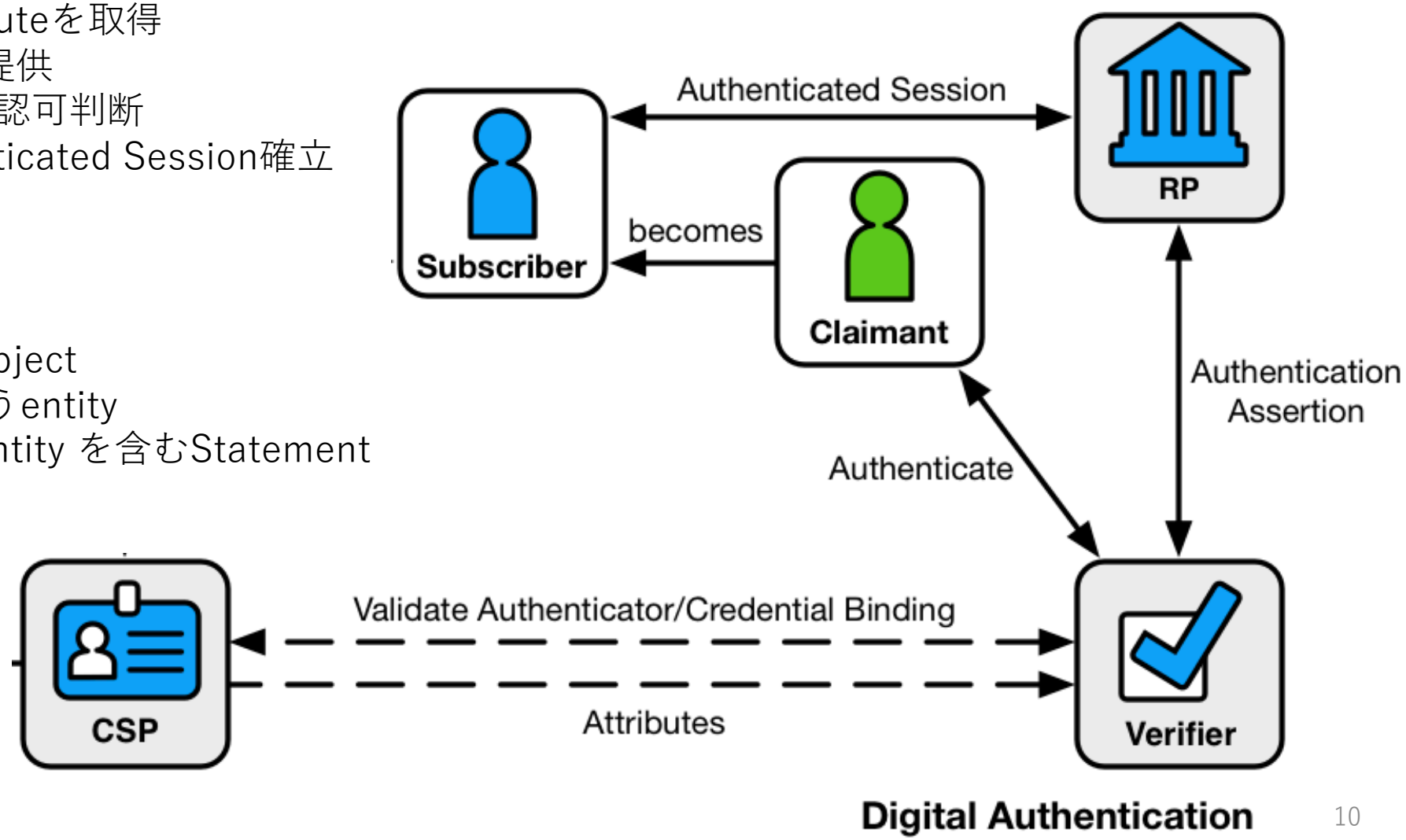
Enrollment and Identity Proofing Process

1. Applicant が CSP に申請
2. CSP は Applicant に対して Identity Proofing を行う
    1. 成功すれば Applicant は Subscriber に
3. Subscriber と CSP の間で Credential が確立
    1. Authenticator の用意
4. CSP は Credentials と enrollement data を管理
5. Subscriber は自身の Authenticator を管理

Authentication

Authentication Process
1. Claimant が Verifier に Authenticator の保持管理を証明
2. Verifier は CSP とインタラクション
    1. Credentials を検証し、Subscriberであるか検証
    2. 任意でClaimantのAttributeを取得
3. Verifier はAssertionをRPに提供
    1. RPはAssertionをもとに認可判断
4. Subscriber – RP間のAuthenticated Session確立

用語
- Claimant: 認証される前のSubject
- Verifier: Identity の検証を行うentity
- Assertion: Subscriber の Identity を含むStatement



Digital Authentication

Federation and Assertions

- RP、CSP、Verifier は独立していることもある
  - Identity Federation
    - Federation : 一連のネットワークシステム間で Identity および Authentication 情報の伝搬を行うためのプロセス.
  - Assertions
    - Authenticationプロセスが完了すると、Verifierはその結果を含むAssertionを発行
    - 時には、Subscriberの属性を伝えることも
  - Relying Party
    - RPはAssertionをもらって
      - Authenticated Identityやその他の要素をもとにAuthorization（認可）を行う
      - Authorizationはこのガイドラインの範囲外

LOA (Level of Assurance)

- Digital Identity に潜むリスク
  - Ditital Identtity って本物? 保証(Assurance)されてる？
- 例えば
  - Identity Proofing -> 虚偽申告、身分詐称(そもそも違う人)
  - Authentication -> オレオレ詐欺、アカウントはっく(前と違う人)
  - Federation -> Assertionの改竄
- 防ぐには
  - 身分詐称とかは、身分証(免許証とか)確認すれば防げそう
  - ２要素認証とか強い認証をすればアカウントハック防げそう
  - AssertionのIntegrity(完全性)を担保すれば良さそう
- それぞれには強度のレベルあり

IAL, AAL, FAL

- Identity Assurance を個別の要素ごとに分割
  - それぞれSP800ー63Xの形で文書が分割されてる
- IAL(Identity Assurance Level)
  - Identity Proofing プロセスについて
  - SP 800-63A Enrollment and Identity Proofing
- AAL(Authenticator Assurance Level)
  - Authentication プロセスについて
  - SP 800-63B Authentication and Lifecycle Management
- FAL(Federation Assurance Level)
  - Federation プロセスについて
  - SP 800-63C Federation and Assertions

IAL

- Applicant が Identity Proofing を行い登録するリスクについて
- 3つの IAL は, Attacker による不正な Identity の主張が成功してしまった場合を想定した被害想定に基づく

- IAL1: Applicant を特定の現実のIdentityと紐づける必要はない
  - Attributeは全てself-assertedなもの
- IAL2: Claimed Identity が現実に存在し、Applicantがその Identityと紐づいていることを検証し証明する
  - Remote or 対面でのIdentity Proofing
- IAL3: 対面でのIdentity Proofingが要求される。

AAL

- Authenticationで使うAuthenticatorの信頼レベル
- 3つの AAL は, Attacker が Authenticator を手中に収めシステムに Access できてしまった場合を想定した被害想定に基づく

- AAL1: Authenticatorの管理がある程度の確度で保証される
  - Single-factor or multi-factorでauthenticationは幅広く使える
- AAL2: 高い確度で保証
  - multi-factorで
- AAL3: 非常に高い確度で保証
  - 暗号プロトコルを介して、鍵の所有証明(Prrof of Posession)

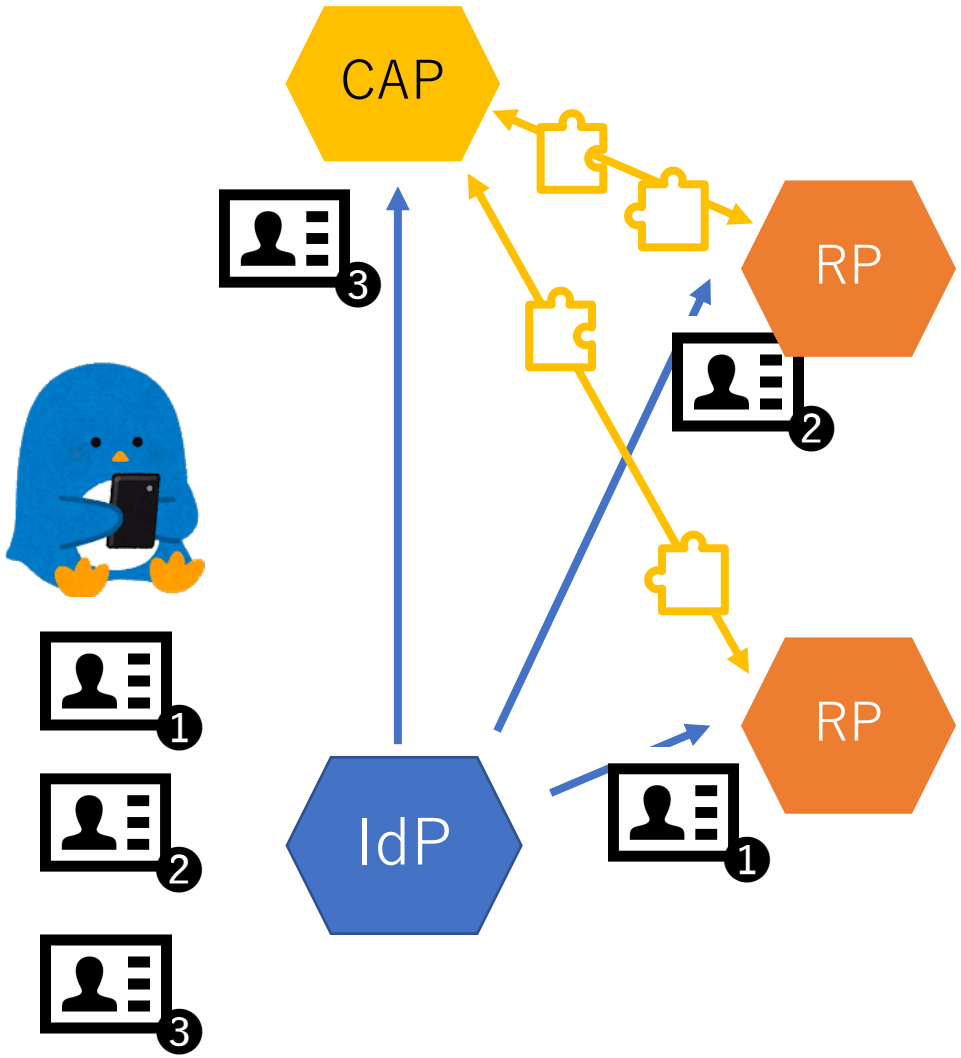
FAL

- Federation 環境で Assertionを利用する際の要件
- 3つの FAL は, Attacker が Federated Transaction をコントロールできる状況に陥った場合を想定した被害想定に基づく

- FAL1: Bearer assertion, signed by IdP.
  - Bearer 、Assertionを持った人は誰でも使える
- FAL2: FAL1 + encrypted to RP
- FAL3: Holder of key assertion, signed by IdP and encrypted to RP
  - 特定のRPのみAssertionが使える

進捗とこれから

ZTFで使うIDの仮名性



- ZTFのentityが結託してIDとユーザの関係を調べる -> 名寄せ

  - 同じユーザのものかどうか
- IdPと結託するとすぐバレる
- RP と CAP が結託するとすぐバレる
- RPのみが結託した時の名寄せリスク
  - CAPが提供するコンテキストの類似度で同じユーザのものかどうかの確からしさが判断できそう

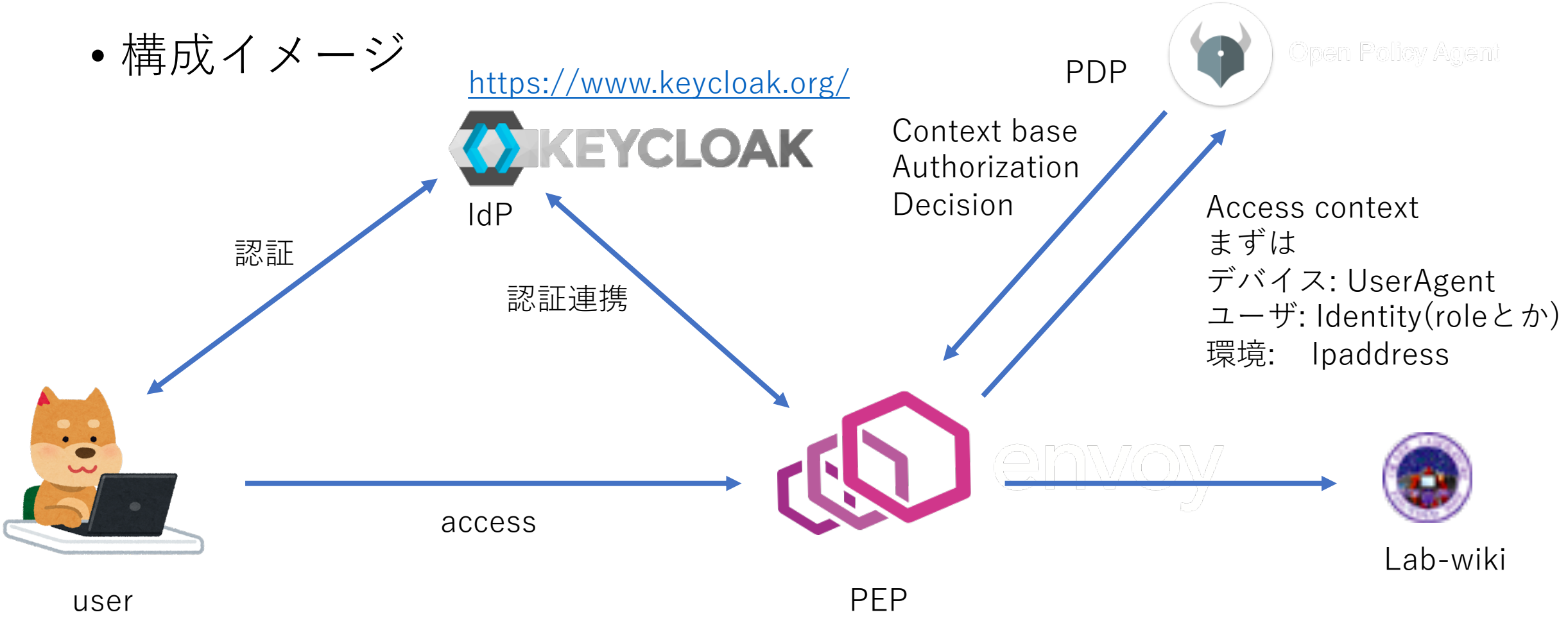
卒論を発表

- [今やってること]DICOMO2020カメラレディ原稿
  - 5/18 23:59 〆切
- [これから]DICOMO2020発表プレゼン
  - 6/25に発表、次回の研究会で練習します
- [これから]英語版の作成
  - いい感じの発表の場が見つかってない
  - とりあえずDICOMOの原稿ができたらそれを翻訳
  - インターネットの適当な場所にアップしておく

研究室のゼロトラスト化

https://www.openpolicyagent.org/

- 構成イメージ



⭕(検討中) https://www.envoyproxy.io/

❌(見送り) https://www.ory.sh/oathkeeper/

…原稿書いたらもっとがんばりマス

あとは...

- 講義
  - レポートが多いよお
- BGP
  - 楽しい