Bluesky と AT Protocol

Affiliation: JAIST Ph.D. Student

Name: ADACHI Yuya

E-mail: s2120001@jaist.ac.jp

CreatedAt: 2024-03-02

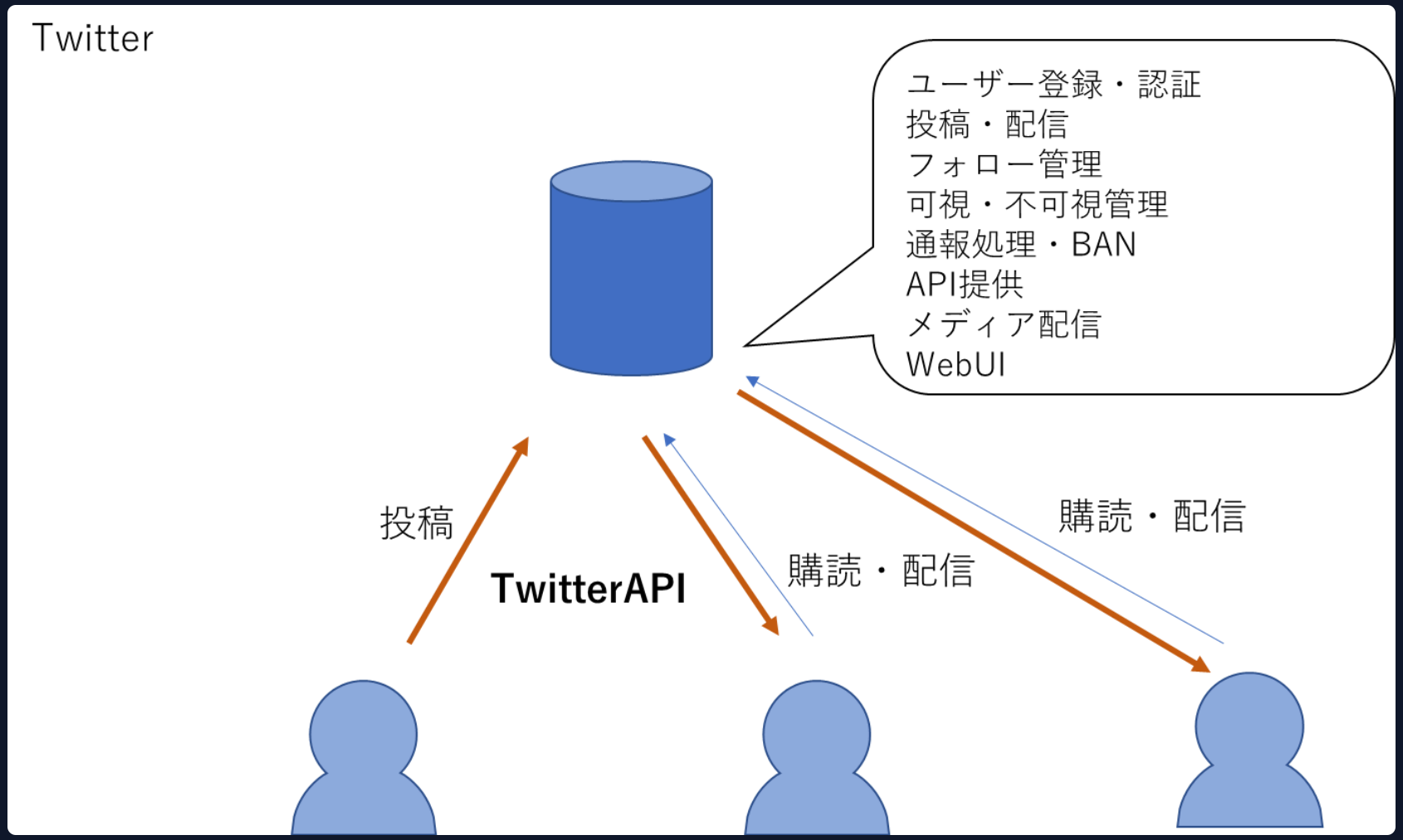
はじめに

- 最初に、中央集権型ソーシャルメディアについて解説します
- 次に、分散型ソーシャルメディアのプロトコルを解説します
    - 技術用語を多用しているので、ご了承ください
    - アプリやサービスの使い方などは少ないです
- Twitter、Mastdon、Misskey、Bluskey の違いを理解してもらうことが目的です
- Bluskey と ATP は、開発途中のサービスとプロトコルです
- 今後、破壊的変更が行われる可能性もあります

中央集権型ソーシャルメディア：概要

- 全てのデータは、プラットフォームの運営者によって一元管理されている
  - Facebook、Instagram、pixiv、Twitter、YouTube など
- 様々な権利は、プラットフォームの運営側にある
  - 生殺与奪、データの所有権、アルゴリズムの選択権 など
- プラットフォームの運営側に掛かる負担が大きい
  - 技術的な負担、法的な負担、社会的な負担 など

中央集権型ソーシャルメディア：アーキテクチャ



https://qiita.com/gpsnmeajp/items/eb665d639f088b85454e

分散型ソーシャルメディア：概要

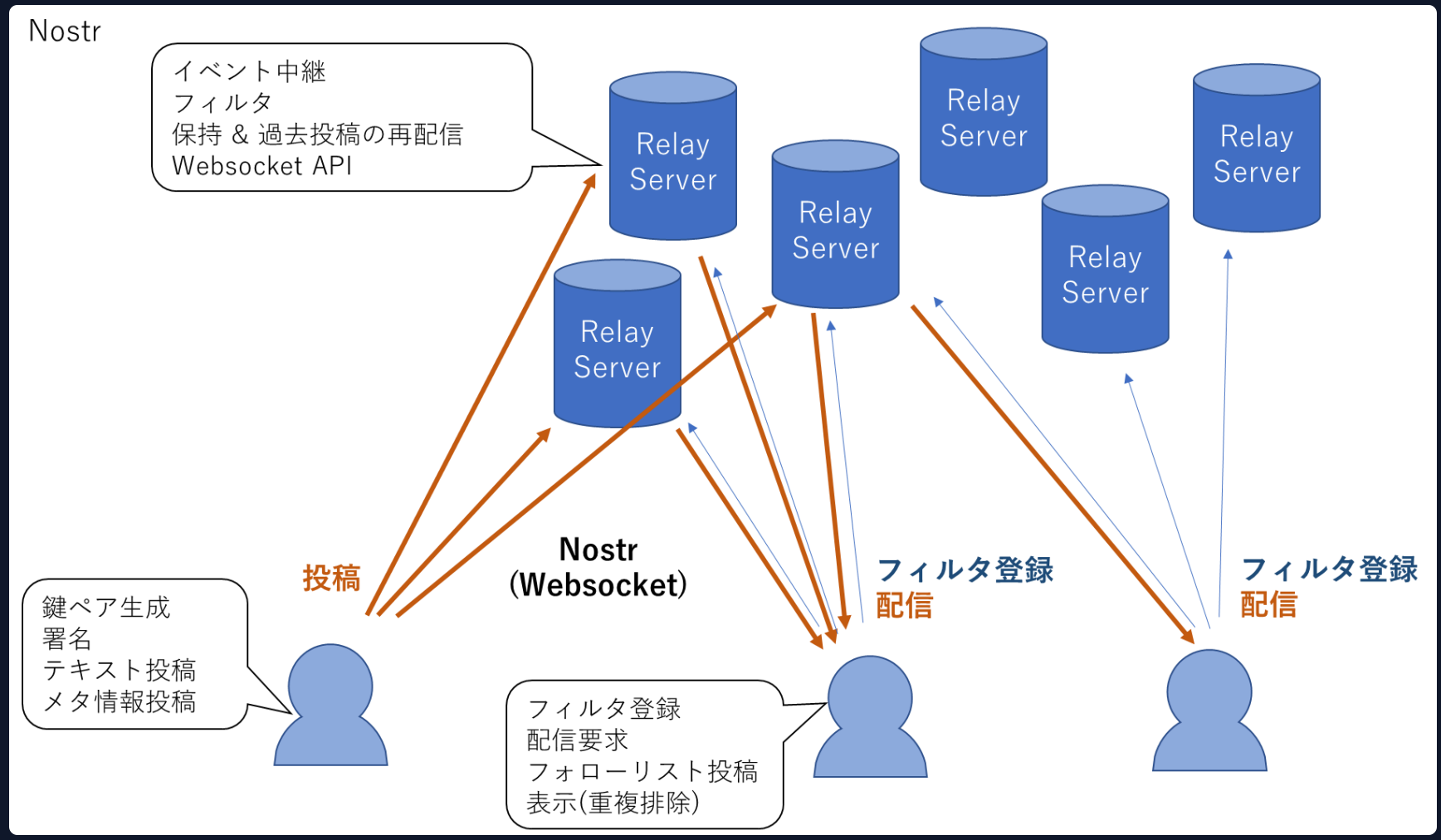
- 中央集権型ソーシャルメディアの問題点が色々とわかってきた
- これが分散型ソーシャルメディアが色々と出てきた原因
- ここから代表的な分散型プロトコルを解説する

Nostr：概要

- Notes and Other Stuff Transmitted by Relays の
- リレーサーバーと呼ばれる複数のサーバーを介して情報が伝達する
- 自己証明は、暗号鍵技術と電子署名技術で実現している

https://github.com/nostr-protocol/nostr

Nostr：アーキテクチャ



https://qiita.com/gpsnmeajp/items/77eee9535fb1a092e286

Nostr：欠点と欠点

利点

- サーバーを信頼しないことで、検閲耐性 と 回復力 を獲得
- 暗号鍵技術と電子署名技術によって、改ざんを防止
- P2P アーキテクチャではなく、C/S アーキテクチャを拡張している

欠点

- スパムブロックが難しい
- なりすまし防止が難しい
- 秘密鍵は漏れれば一巻の終わり

https://github.com/nostr-protocol/nostr

Nostr：まとめ

- 絶対に流行らないハッカー用ソーシャルメディア
- あまりにもピーキーな設計思想のプロトコルとサービス
- リレー分散型 や 無責任中継型 と呼ばれることもある

https://github.com/nostr-protocol/nostr

ActivityPub：概要

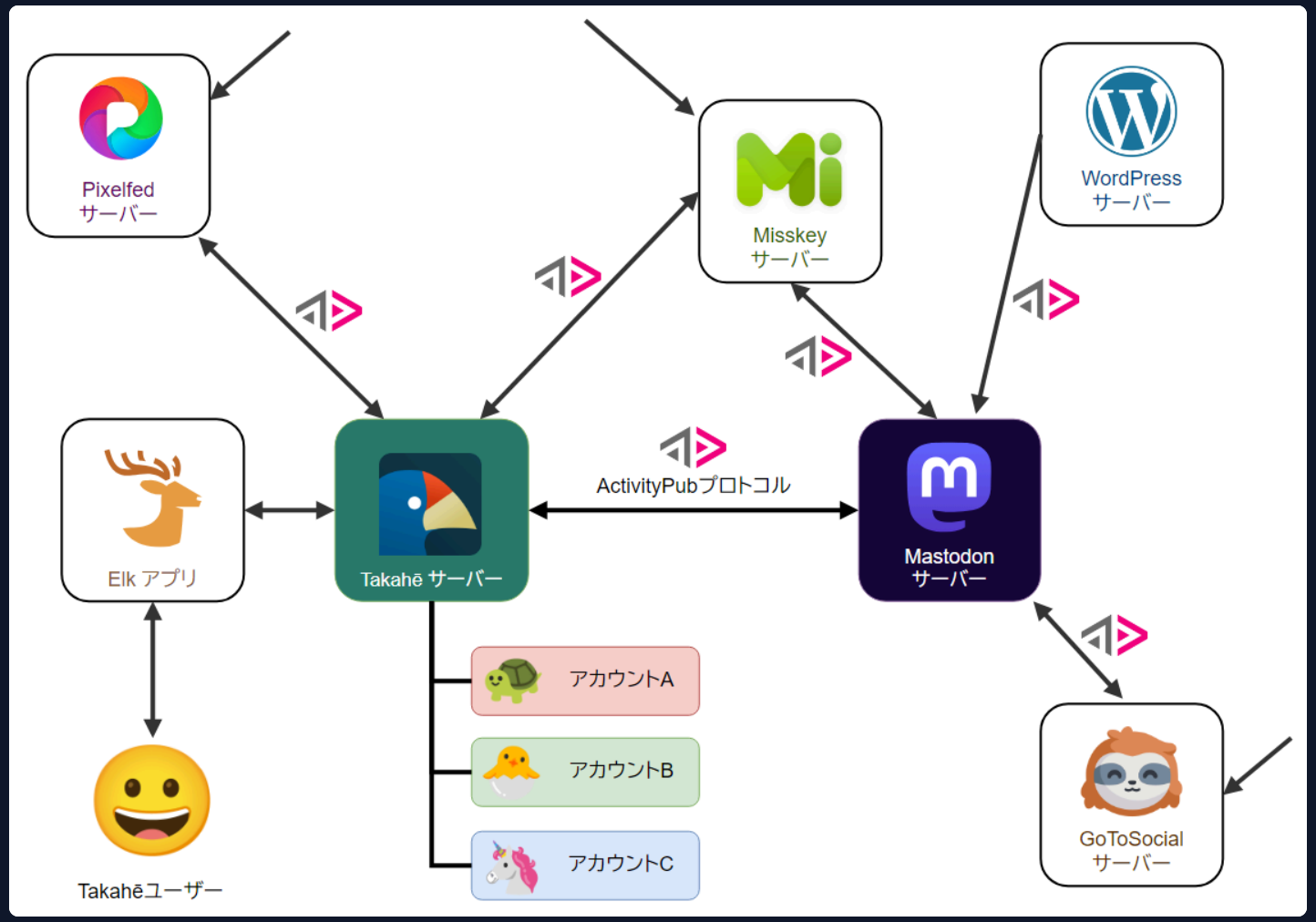
- ActivityPub は、W3C によって開発されているプロトコル

- ActivityPub の大きな特徴として以下が挙げられる
  - インスタンスと呼ばれるサーバーに分散する
  - インスタンス間を ActivityPub で通信する

- これにより、中央集権型が持つ問題を解決しようとした

- 連合分散型 や 地方分権型 などと呼ばれることもある

ActivityPub：アーキテクチャ



https://gihyo.jp/article/2023/09/takahe-01

ActivityPub：問題点 (1)

- 結局、大きなインスタンスに人が集中する
  - Mastodon.social や Misskey.io など
  - モノリシックアーキテクチャなのでスケールが難しい
  - 中央集権型の問題である負担が解決されていない

- タイムラインアルゴリズムは手軽にイジれない
  - 構造的にサーバー負荷が大きいので難しい
  - グローバル TL の、これじゃない感がすごい
    - 最初は楽しいけど、すぐに見なくなる

ActivityPub：問題点 (2)

- アカウントポータビリティが低い
  - 引っ越しする際は引っ越し元インスタンの協力が必要
  - 引っ越す際に自分の投稿は持っていけない
  - やっていることは引越し先インスタンに新しいアカウントを作っている
  - アカウントの同一性を証明することが難しい

- このように、まだまだ多くの課題が残っている状況

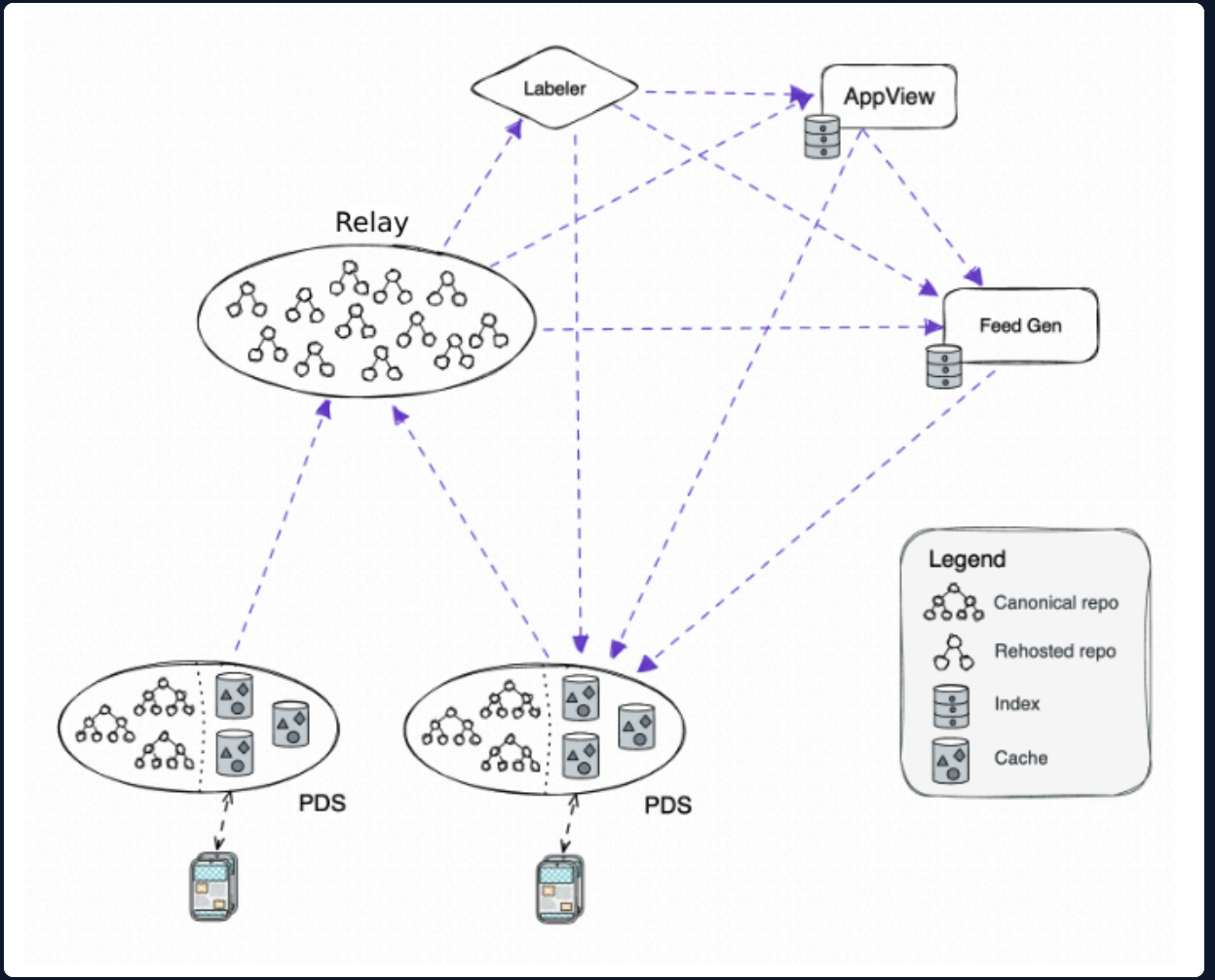
AT Protocol：概要

- AT Protocol は、Bluesky (組織) が開発するプロトコル
- Authenticated Transfer Protocol の略称
- Bluesky (サービス) は、AT Protocol のリファレンス実装
- ActivityPub が持つ問題の解決を目指している
- そのため、アーキテクチャは ActivityPub に似ている

AT Protocol：スケーラビリティ

- 人が多いところに集まるのはソーシャルメディアの宿命
- 人の増減に対応できるようにスケーラビリティを確保する
- マイクロアーキテクチャを想定してプロトコルを設計している
- Lexicon と XRPC によって定義、制御している
  - ここでは割愛するが気になる人は ATP Docs を参照してください
  - ATP Docs：https://atproto.com/

AT Protocol：アーキテクチャ



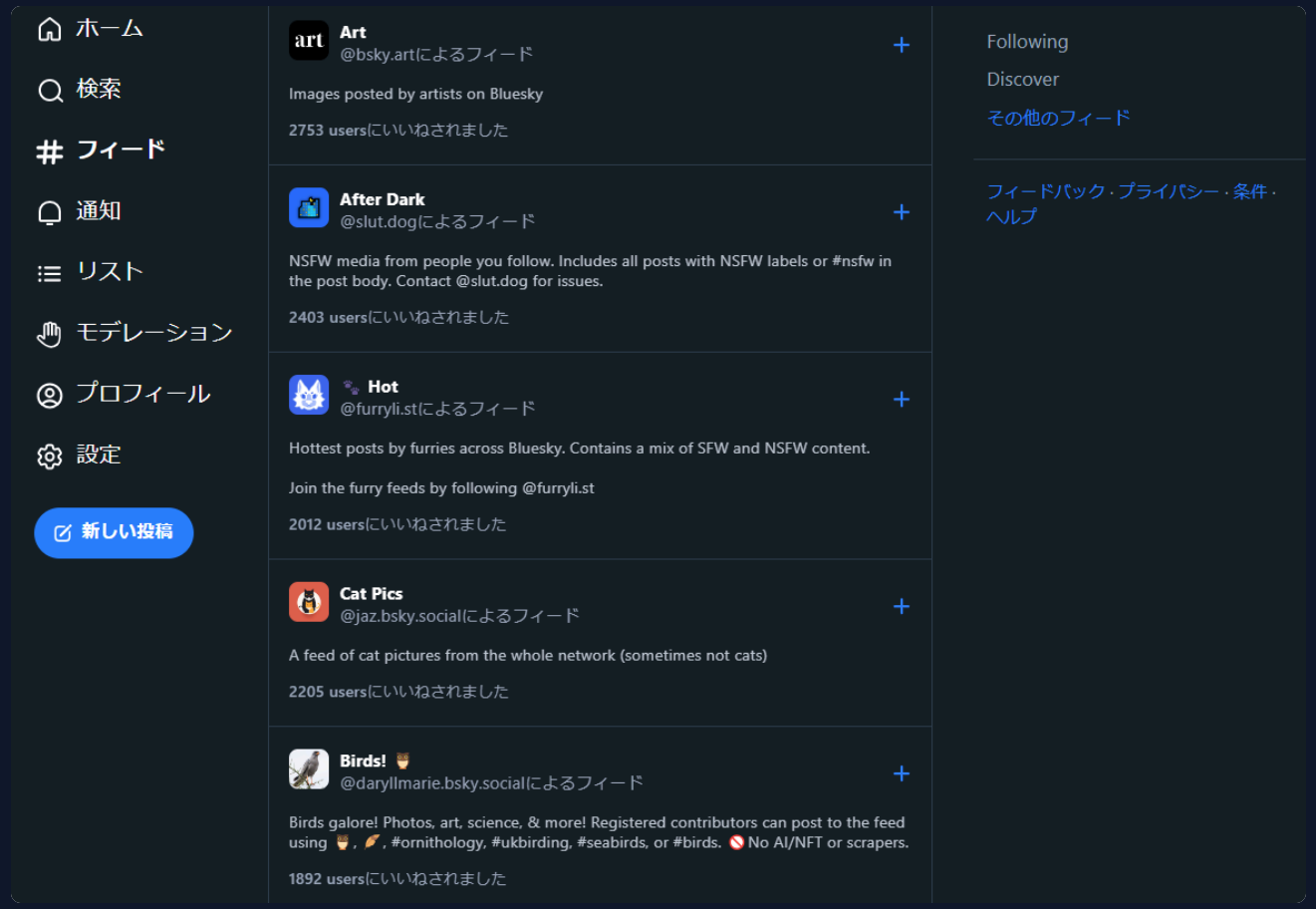
https://bsky.social/about/blog/5-5-2023-federation-architecture

AT Protocol：Feed (1)

- Bkuesky では、タイムラインを Feed と呼ぶ
- 公式が提供している Feed は以下の 2 つです
  - Following：フォローしている人のポストが **時系列** で流れる
  - Discover：Trending content from your personal network
- Custom Feeds (後述)

AT Protocol：Feed (2)

- ユーザーが表示させる情報を自由にカスタマイズ出来る
- 現在、40,000 を超える Custom Feeds が公開されている



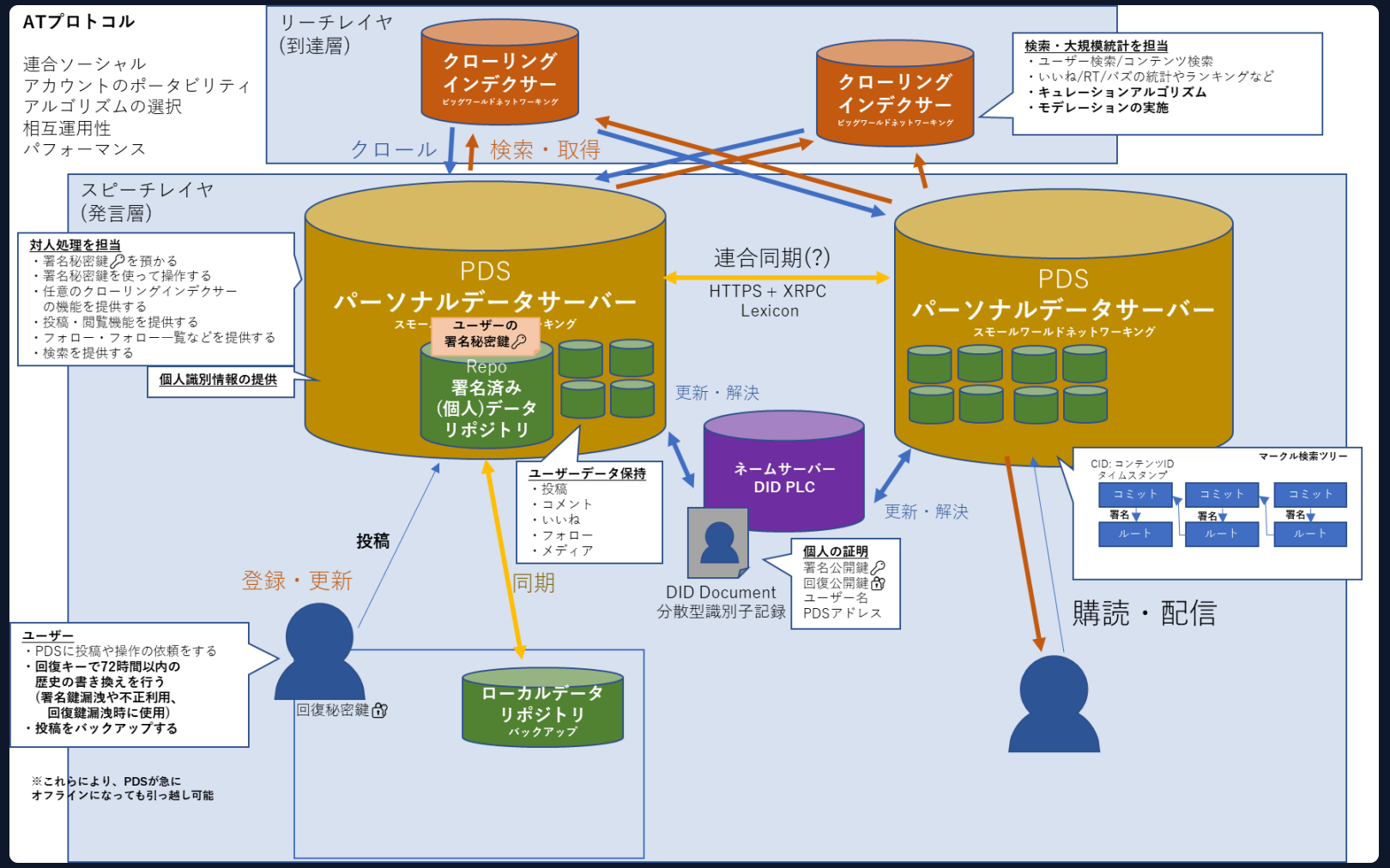
AT Protocol：Feed (3)

- Custom Feeds は簡単に作って公開することが出来る
- SkyFeed (https://skyfeed.app/) という公式ツールを使う

AT Protocol：アカウントポータビリティ (1)

- ATP では、Decentralized identifiers (DIDs) を利用してアカウントポータビリティを確保している
- DID は W3C が標準化している規格
- 詳しい仕様に関しては公式ドキュメント (https://www.w3.org/TR/did-core/) を参照してください
- Blusky のアカウントは DID PLC Directory (https://web.plc.directory) に保管されている

AT Protocol：アカウントポータビリティ (2)



https://qiita.com/gpsnmeajp/items/eb665d639f088b85454e

AT Protocol：アカウントポータビリティ (3)

- ブラウザだけで自分のアカウント情報を呼び出すことが出来る
- https://plc.directory/[YOUR_DID] を叩くと呼び出せる


```json
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/multikey/v1",
    "https://w3id.org/security/suites/secp256k1-2019/v1"
  ],
  "id": "did:plc:nuzfbrq7kncg6fp26lf5bvx3",
  "alsoKnownAs": ["at://l7u7ch.bsky.social"],
  "verificationMethod": [
    {
      "id": "did:plc:nuzfbrq7kncg6fp26lf5bvx3#atproto",
      "type": "Multikey",
      "controller": "did:plc:nuzfbrq7kncg6fp26lf5bvx3",
      "publicKeyMultibase": "zQ3shwZbiHHQnWwCfNZb6XmwQpSpnHBuG1BdT6ETKsbD3kGYm"
    }
  ],
  "service": [
    {
      "id": "#atproto_pds",
      "type": "AtprotoPersonalDataServer",
      "serviceEndpoint": "https://hydnum.us-west.host.bsky.network"
    }
  ]
}
```

AT Protocol：アカウントポータビリティ (4)

- 先日、PDS が公開されて連合が試験的に開始
- 公式 PDS から他の PDS に引っ越すと戻ってこれない (実装中)
- 自分のポストをローカルにバックアップする機能が実装済み
- PSD 間でポストデータを移行する機能は実装中

AT Protocol：Q & A (1)

Q. 今後、Bluesky や ATP は流行るのか？

A. Bluesky 自体は、革新的な機能を実装しているわけでもなく、あくまでも ATP のリファレンス実装である。そのため、爆発的にユーザーを獲得することは無いと思われる。一方、ATP 自体は、様々なサービスに組み込まれる可能性を秘めている。何気なく登録したサービスが ATP ベースのサービスだったみたいなことは十分に起こり得ると思う。

AT Protocol：Q & A (2)

Q. 今後、どのような ATP ベースのサービスが誕生するか？

A. 現在、ATP のリファレンス実装である Bluesky はテキストベースのマイクロブログサービスとして公開されている。しかし、ATP のコア部分である Lexicon と XRPC は、Binary Large OBject (Blob) に拡張可能である。そのため、pixiv や YouTube のようなマルチメディアサービスが徐々に誕生していくと思われる。また、独自機能を追加した PDS や BGS も徐々に出てくると思われる。PDS では、RAW データを保管するクラウドストレージと SNS が混じったようなサービスが、BGS では Google BigQuery のようなクエリごとの従量課金制サービスの登場が予想されます。