Aoi

ユーザー認証について絶対的な権威のないサービス間連携を実現する

~SSOの新しいカタチを模索して~

藤松勇滉 ’20 8/24

Aoiを俯瞰する前に

問題意識の共有

既存のSSO技術は、いろいろな使い方があるが、例えば他者の提供する認証サービスを使用して開発工数の削減や、セキュリティの向上を図ることが目的の場合、他者への信頼をすることで、その目的は達成される。「他者」への信頼を必要とする。

Bitcoinの発明により、「他者」への信頼を、システムに移行することができるのではないか？といった動きが広がっている。

Aoiの概要
AoiはSSOプロトコル

作品概要：Chrome拡張、Node.jsで実装。非対称鍵での署名を使用。拡張機能が認証をサポートする。(フローや既存SSOとの相違点は後ほど)

Aoiでできること

☑一つの鍵でいろんなサービスにログイン。

☑絶対的な権威なしにユーザーの妥当性を判断。

☑いろんなサービスに対してのログインで、ユーザーの同一性を確認。(鍵が同一であれば)

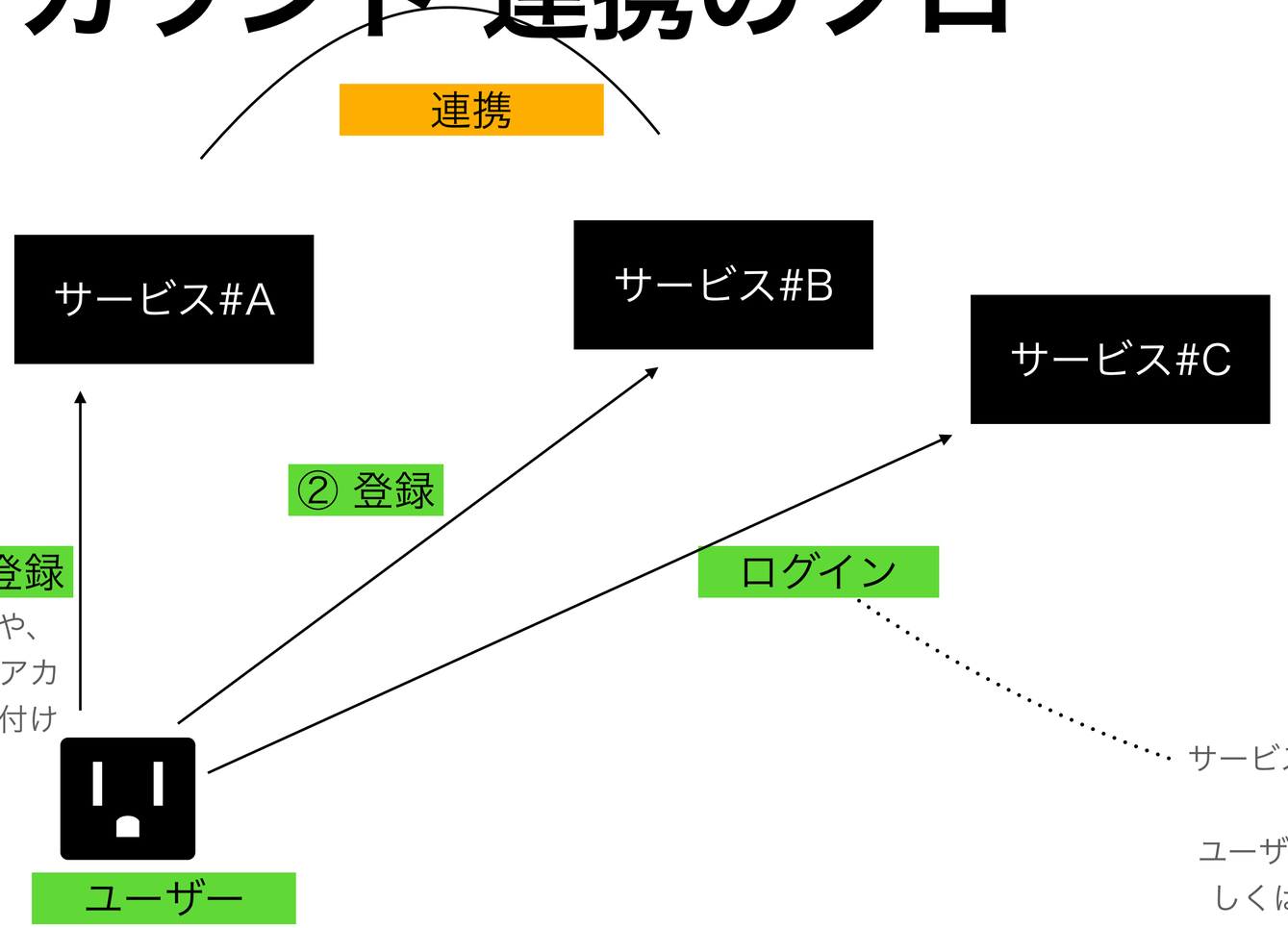
ここでの信頼性とは、サービス間における信頼性を指します。

既存のSSOとなにか違うのか

既存のSSOはID ProviderとRelying Partyの間に明確な上下関係が存在する。認証を委託する側と、委託を受ける側では、委託されるほうが必要な信頼性は高いし、その必要な信頼性によってID Providerは必然的に権威を持つようになる。認証が他者への絶対的な信頼の上に成り立つので、その「他者」は、やろうと思えば不正し放題。

もっとセキュアで、上下関係なくして、ウェブで共通につかえるSSOをプロトコルレベルで作らない？ → Aoiが開発された

Aoi アカウント 連携のフロー



この”登録”とは、サービス#Aや、サービス#Bのそれぞれの内部アカウントにAoiの鍵（1つ）を紐付ける作業

サービス#Cはサービス#A,#Bを連携先として提示しているとする。
ユーザーはサービス#Aか#Bを選択できる。もしくは、どちらも利用してログインできる。