パスキーについて
今日時点の僕が知っていること

Niigata 5分 Tech #6

Yukiya Nakagawa a.k.a Nkzn / 2024.3.29

Who am I

- なかがわゆきや / なかざん（@Nkzn）
- 株式会社モニクルで「くらしとお金の社会課題を解決する」各種事業のインハウス開発に加担しています
- 技術書典開発チームもやってます
  - キャッシュレス決済アプリとWebフロントエンド

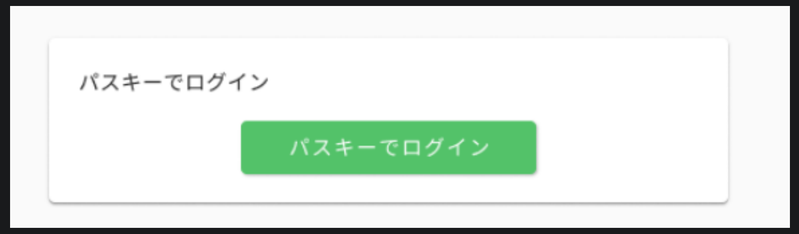
パスキー普及してきましたね

パスキー使ってますか？

パスキー実装してますか？

僕は最近実装してます

- 技術書典Webのパスキーログインを実装中
- 近々リリース予定なのでお楽しみに



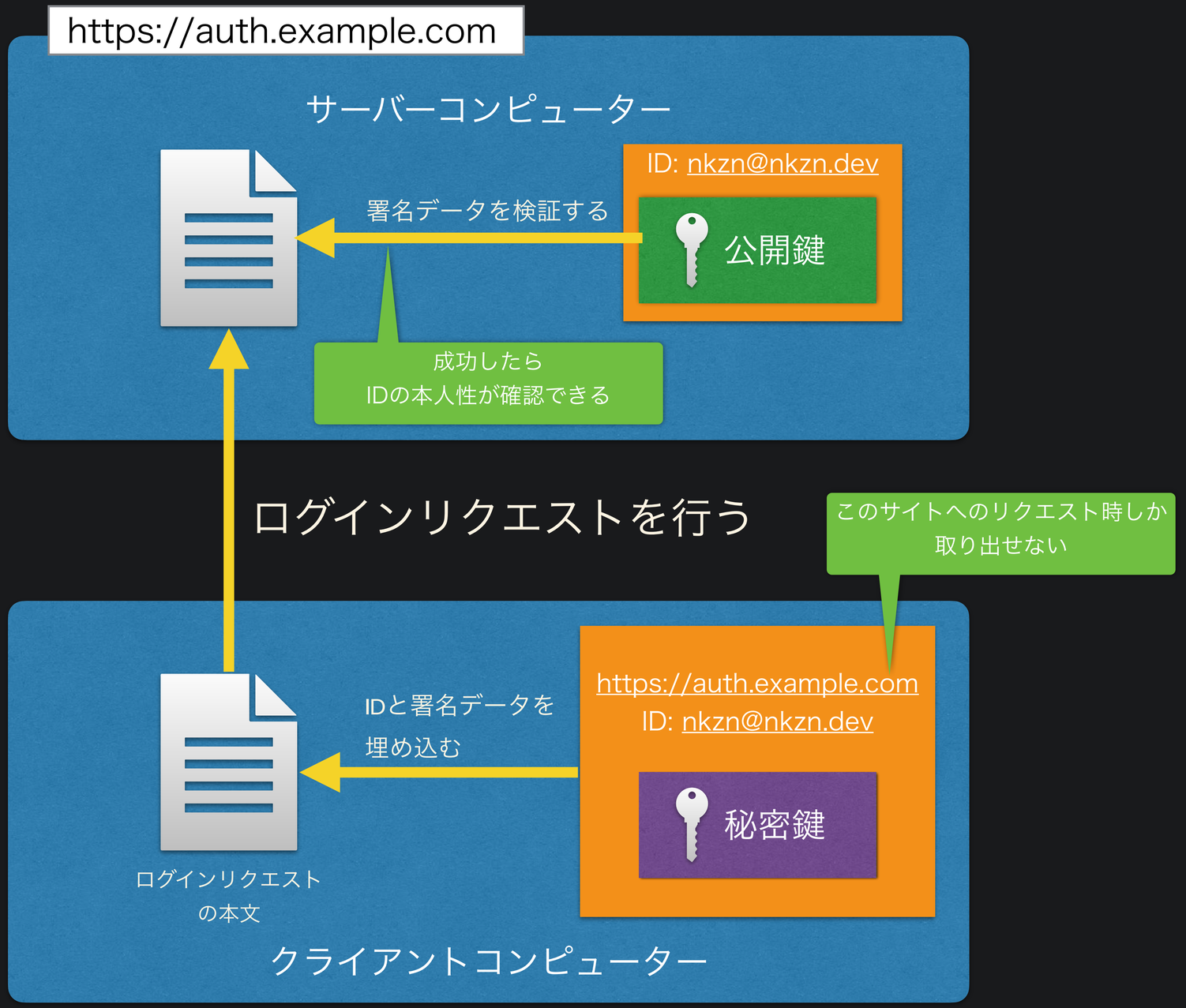
※UIは変わる可能性があります

- おかげさまで解像度がもりもり上がってきた

まだ勉強中ですが
頭の中の整理にお付き合いください

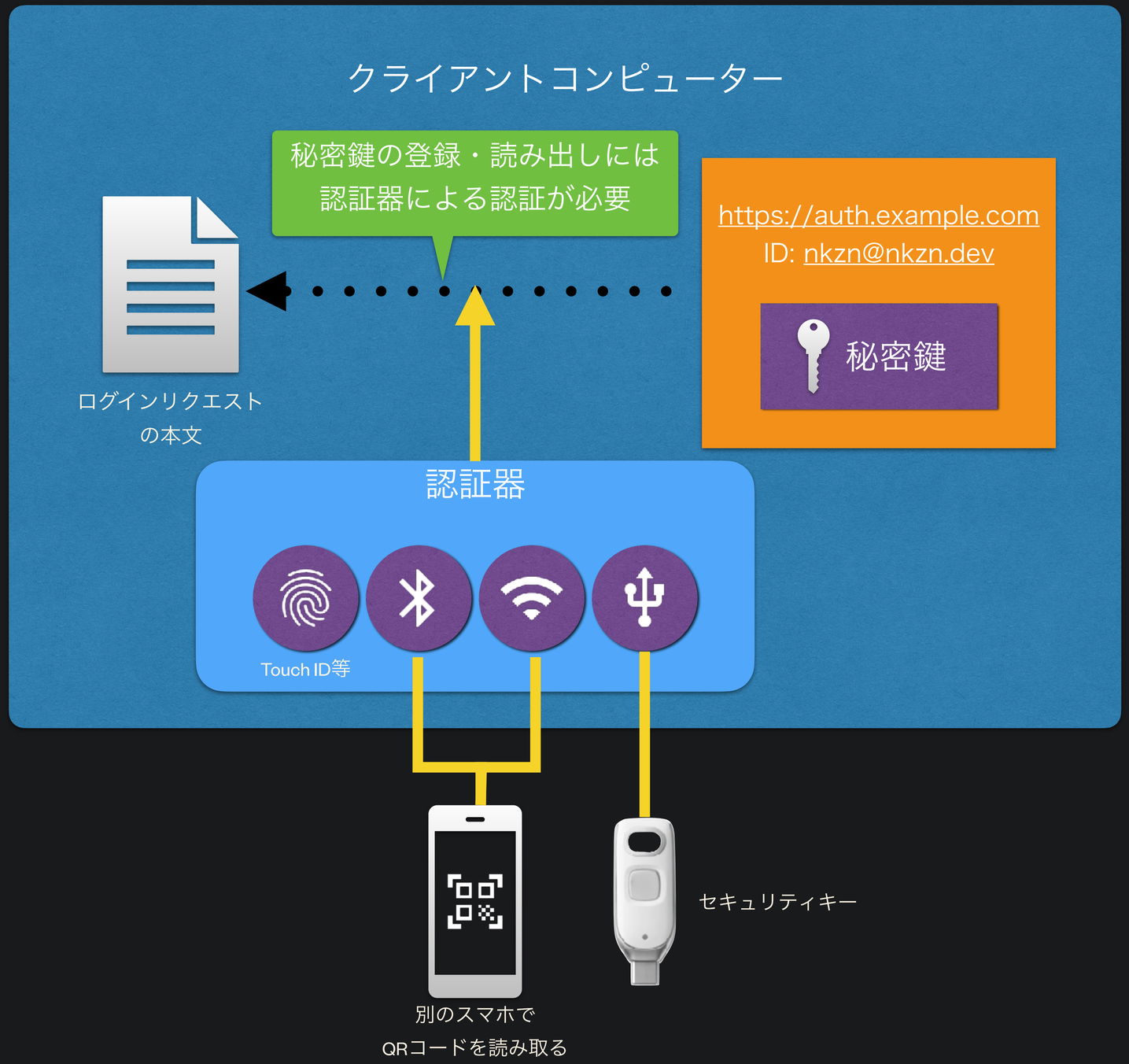
パスキーの
ある側面①

- ログイン時は公開鍵暗号で本人性を確認すれば、サーバーから公開鍵だけ流出しても怖くないし最高じゃね？
- リクエスト先のドメインとセットで秘密鍵を保管しておけば、偽ドメインでフィッシングサイトを作っても真ドメインの秘密鍵が使われることはないから最高じゃね？

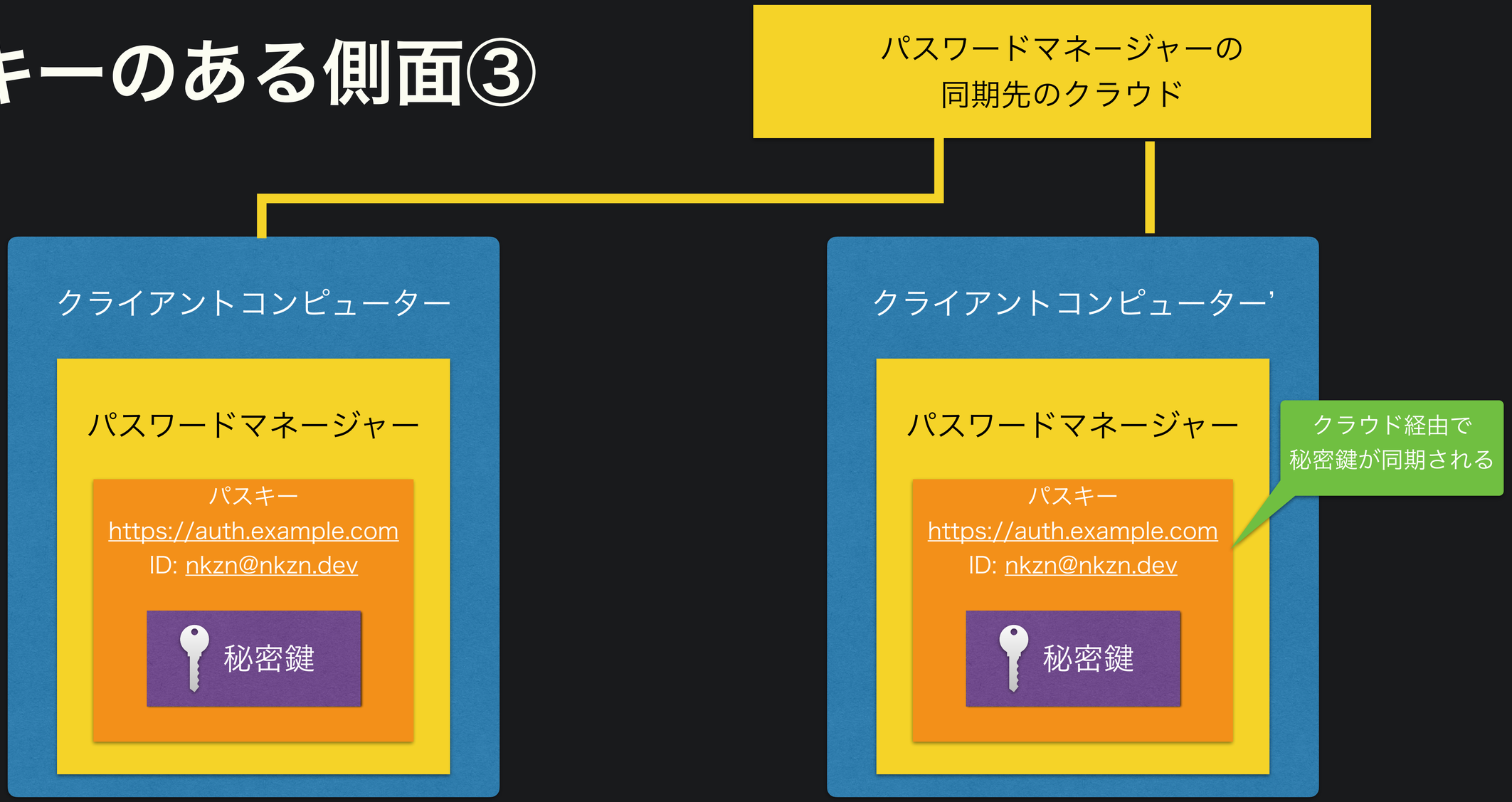


パスキーの
ある側面②

- 秘密鍵の利用には認証器による認証が必要
- 最低でも所有認証が少ない操作で行われる
- Touch ID等を使った場合は同時に生体認証も行われる
- 操作としては1回なので簡単かつ早い



パスキーのある側面③



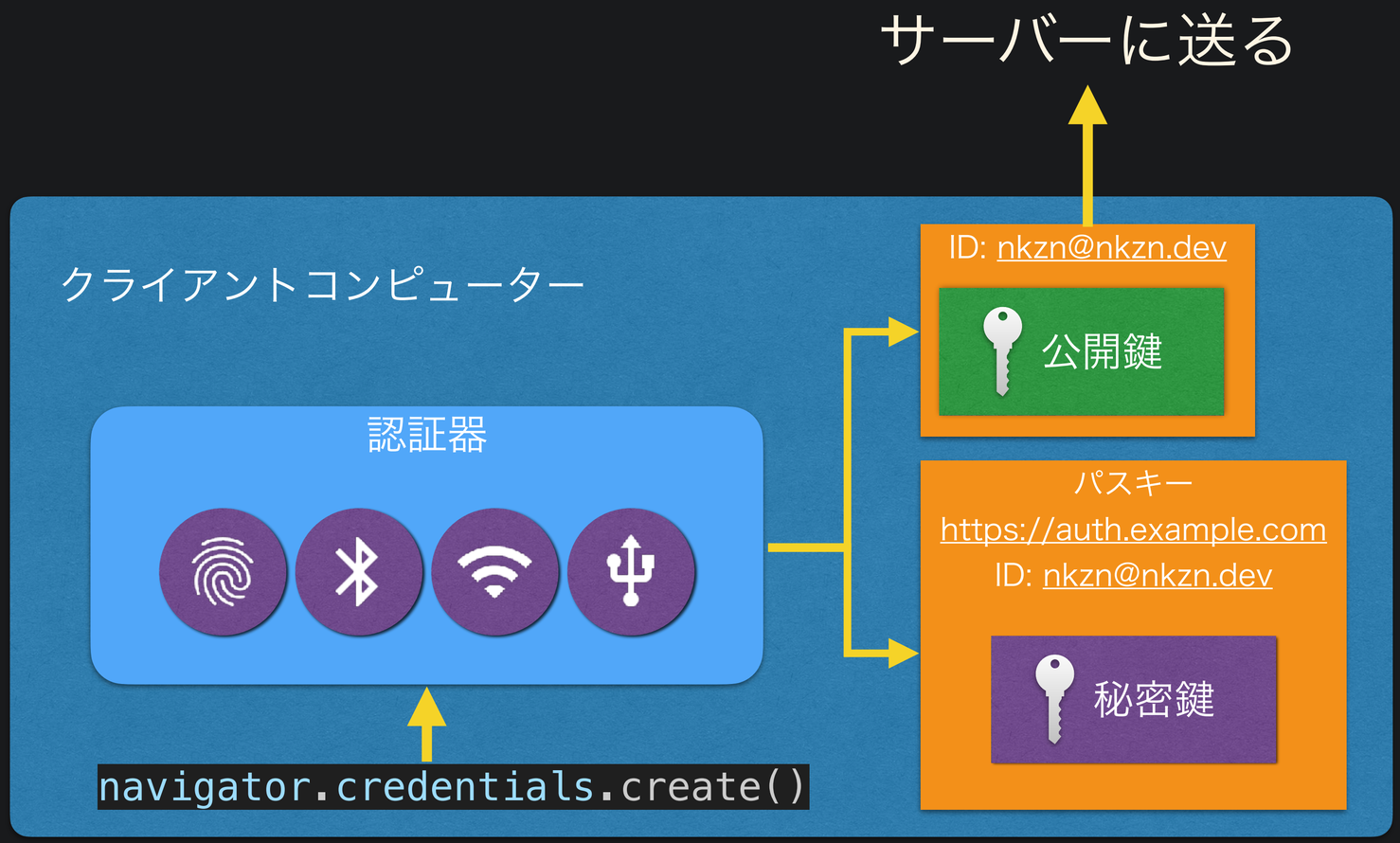
デバイス間で秘密鍵が共有されるので、所有している他のデバイスでもログインが容易

パスキーのある側面③

- 異なるパスワードマネージャー同士でのパスキーの共有はサポートされていない
  - GoogleパスワードマネージャーはAndroidとChromeのパスキーだけを共有する
  - iCloudキーチェーンはiOS系とmacOSとSafariのパスキーだけを共有する
  - Microsoft AuthenticatorはWindowsのパスキーだけを共有する
- サードパーティのパスワードマネージャーはプラットフォームを跨いで共有する
  - 1 Passwordは1 Passwordを利用する可能な限りのプラットフォームへパスキーを共有する

鍵発行と認証器

- FIDOアライアンスから認定を受けた認証器 (Authenticator) で鍵を発行する
- どこのパスワードマネージャーに登録するかはユーザーが選べる



FIDO2

- ログインリクエストのペイロードのフォーマットや署名方法、認証器の規格やワークフローなどがプラットフォームごとにまちまちだと困るので、FIDOアライアンスが標準化した
- 主な内訳は次の2つ
  - W3C Web Authentication (WebAuthn)
  - Client-to-Authenticator Protocols (CTAP)

認証のUIを表示する方法

`navigator.credentials.get()` を呼び出す

ボタン等で始める

（mediation: “required”）

フォームのID欄で始める

（mediation: “conditional”）

（事前に<input type=“email webauthn”>とか仕込んでおく）

サーバーサイドの話

- サーバーの役割としては次の2つとなる
  - navigator.credentials.get() に渡すパラメータの発行
  - navigator.credentials.get() で署名された結果を受け取って検証する
  - 1回のログインで navigator.credentials.get() の前後に1回ずつサーバーにリクエストすることになる
- パスワードを確認するのと比べればはるかに難しいので、自前では実装できない人も多そう
- IDaaSの対応が進むとパスキーが普及していきそう
  - Auth0, Okta, GMOトラストログイン, StartInなど、パスキー対応を歌うIDaaSは増えてきている
  - Firebase AuthenticationはH1 2024にプレビュー版が出るかも

WebAuthn

- デモサイト: https://webauthn.io/

参考文献

- https://goo.gle/passkeys
- https://fidoalliance.org/specifications/
- https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/
- https://webauthn.io/
- https://blog.agektmr.com/2019/03/fido-webauthn
- https://blog.agektmr.com/2022/12/passkey
- https://blog.agektmr.com/2023/12/passkey-mythbusting
- https://firebase.uservoice.com/forums/948424-general/suggestions/46647016-support-authentication-with-passkeys
- https://moneyforward-dev.jp/entry/2023/04/05/134721