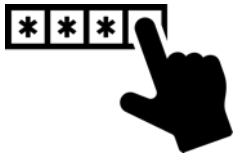
FIDOが求められる背景

ネットバンクなどのスマホアプリやWebアプリのユーザ認証では、セキュリティ上の課題や使い勝手の課題が存在し、それらを公開鍵暗号方式や高度なハードウェアを使って解決する方法をFIDO2は業界標準として規定しています。

①セキュリティ上の課題

パスワードログインをベースとしており、
マルウェア感染やフィッシング攻撃などによる
パスワード漏洩が絶えない。ワンタイムパスワード
による二段階認証もフィッシング攻撃をうける。

②使い勝手の課題



ログインのたびにパスワード入力を
求められたり、送金等の重要処理のたび
二段階認証が必要で、利用者をイライラさせたり、
利用者がパスワードを忘れてしまうことがある。

認証機によるキーペア生成と保管

USBドングル型やスマホ内蔵型で
提供される認証機は、公開鍵
暗号方式で生成されたキーペアを
使い認証を行う。認証機は、署名は
可能だが、秘密鍵はいかなる方法でも取り出せない
特徴があり、これにより認証情報の漏洩を防ぐ。

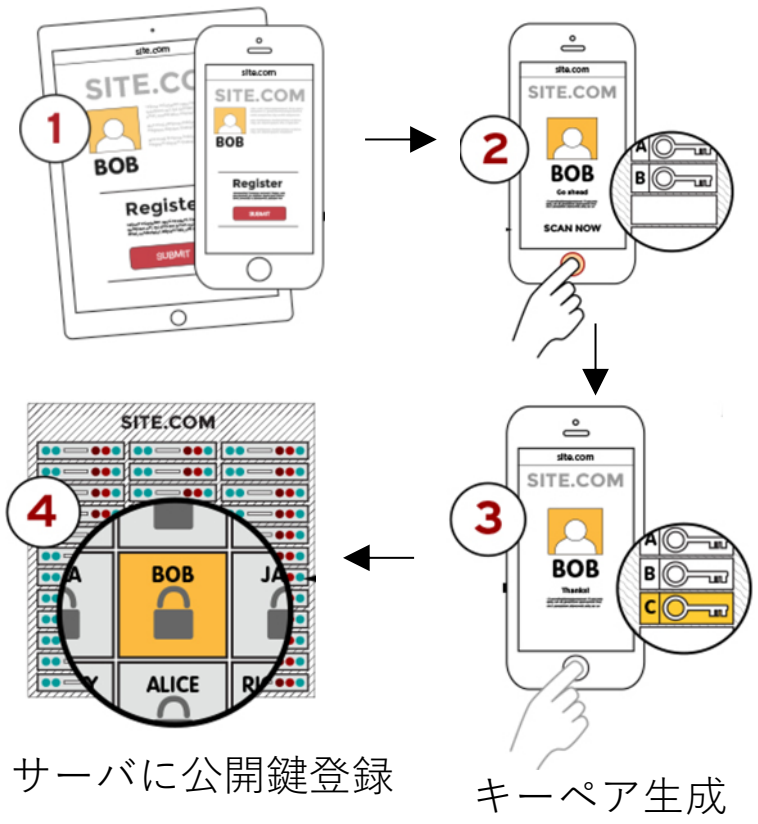
生体認証ログイン

指紋や顔認証といった生体情報を
使い認証機のキーペア生成や署名を行うことにより、
キーボードを使ったパスワード入力より簡単にすばやく
ログインを行うことができ、ユーザのストレスを低減する。
また、パスワードを覚える必要もない。

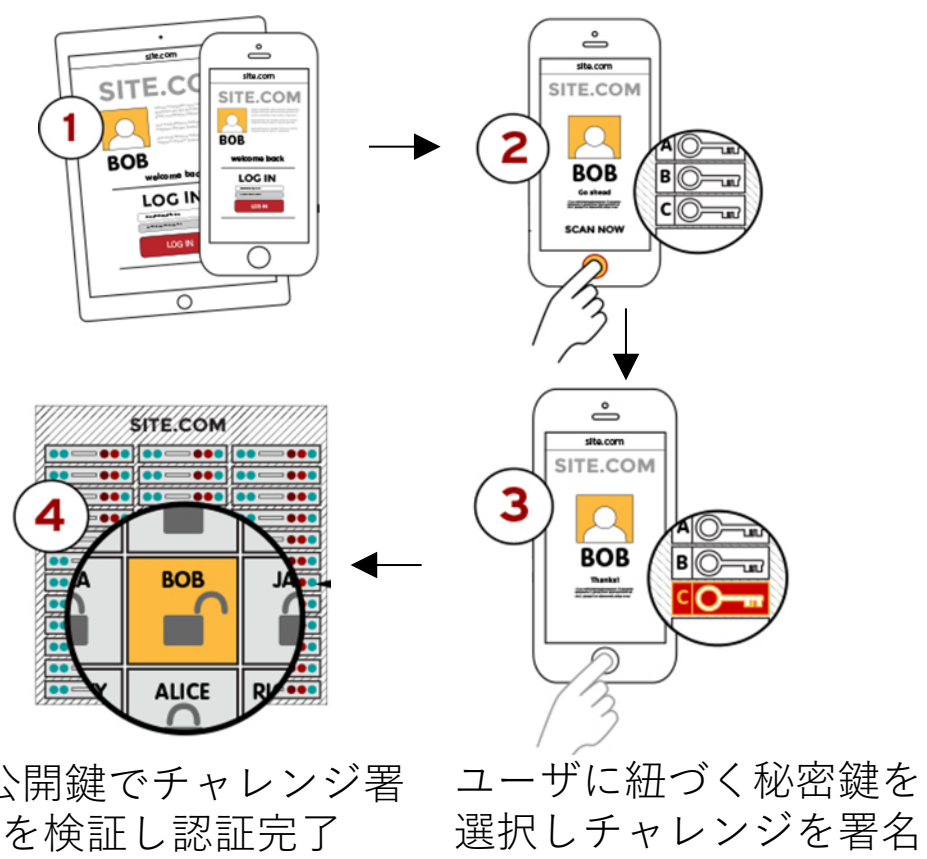
FIDOのしくみ

一般的にWebサービスの認証プロセスは「ユーザ登録」と「ユーザログイン」の２フェーズに分かれ、FIDO認証もこれと同じく「FIDO登録」と「FIDOログイン」からなります。

FIDO登録



FIDOログイン



FIDOの普及について

- 「FIDOが求められる背景」によるとメリットばかりで、FIDOを使わない原因が見当たりませんが、2020年現在FIDOが普及していない理由には以下のものが挙げられます。
  ① ユーザがログインを行う端末であるパソコンやスマホの古いものにはFIDO認証機が内蔵されていないため、FIDOを利用するには別途FIDO認証機（USB型とBLE型などがある）を数千円で購入し、端末とつないで利用しなければならなかった。
  ② パソコンやスマホ提供事業者の代表格であるMS社（Surface PC）、Google社(Chromebook PC、Android端末)、Apple社（Mac、iPhone）のうち、Apple社だけがFIDOアライアンスに参画していなかった。
- しかし、2020年2月にApple社はFIDOアライアンスに加盟し、同年9月のiPhone12の出荷と同時にリリースが予定されているiOS14からSafariブラウザでのFIDO2対応が決定している。
  (※2020/7/10にApple社はiOS14のパブリックベータを配信開始したため希望者は無料で利用が開始できる)
- そのため、生体認証を搭載するFIDO対応端末がひととおりそろうため、2020年後半からFIDOが急速に普及するだろうと予想できます。
  ① MS社：生体認証機能をもつWindows10を搭載したPCやタブレットはFIDO対応済
  ② Google社：生体認証機能をもつAndroidスマホやChromebookはFIDO対応済
  ③ Apple社：iOS14/macOS 11.0 Big Surが2020年9月に無事リリースされると過去の生体認証搭載スマホやmac PCを含めたすべてがFIDO対応になる。