巧妙化する
サイバー攻撃

- なりすまし
- フィッシング
- 標的型攻撃
- 漏えい情報の売買

:

7億件超のメールアドレスが流出、パスワード2100万件も

Facebook、約5.4億件のユーザーデータがAWSでアクセス可能な状態

Facebook、数億人分のパスワードを平文で保存 2万人以上の従業員が検索可能な状態に

個人情報約480万件が流出

アカウント情報流出、被害は6800万件超に

パスワードは「いずれ」漏えいする

～ Problem of time ～

３.
パスワード問題への解決策

パスワードからの解放
＝ パスワードレス認証

ＦＩＤＯ 認証

（*Fast ID Online Authentication*）

FIDO認証は世界のパスワード問題への答えです

ＦＩＤＯ認証

(*Fast Id Online Authentication*)

- ✓ **シンプルで** *(Simpler)*
- ✓ **堅牢な** *(Stronger)*
- ✓ **認証** *(Authentication)*

認証の種類

知識
(Know)

所有
(Have)

生体
(Are)

所有（*Have*）

生体（*Are*）

ＦＩＤＯの利用ケース

様々な認証のケースに対応

堅牢な認証と鍵管理の仕組み

- 鍵や生体情報は、TPMというセキュリティチップの内部に暗号化して保存
- デバイス（認証器）の外に、鍵や生体情報が出ることはありません。

公開鍵暗号方式

公開鍵と秘密鍵の鍵ペアを利用して、安全に情報のやりとりを行う暗号方式。
公開鍵は誰でも取得可能だが秘密鍵は本人だけが持ち管理する。

堅牢な鍵管理

鍵や生体情報は、認証器のTPM（Trusted Platform Module）というセキュリティチップの内部に暗号化して保存。デバイスの外に出ることはありません。

参考）ＦＩＤＯの標準化

Online Crypto Protocol Standardization

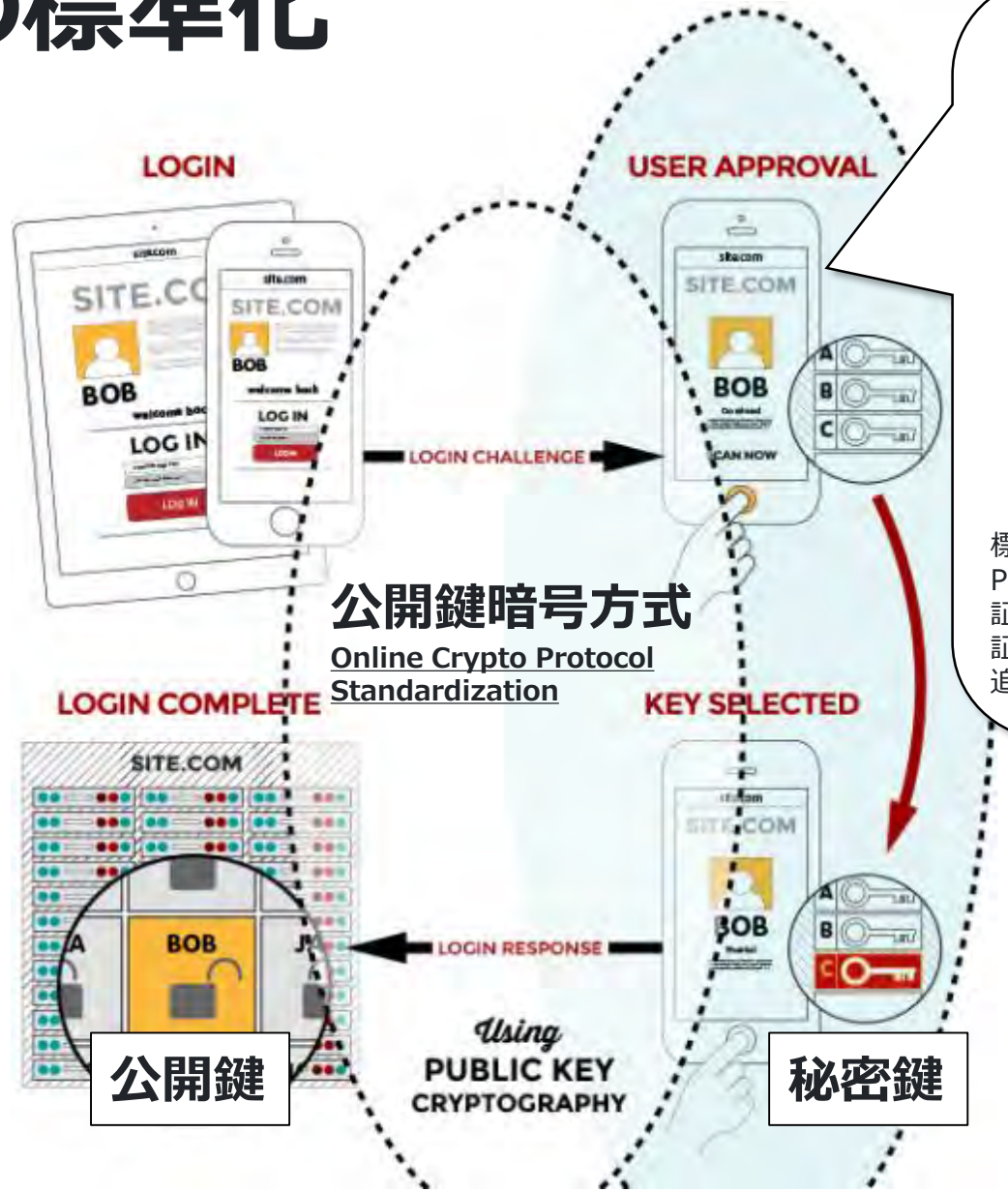
（オンライン暗号プロトコルの標準化）

クライアントとオンラインサービスの間で使用する認証プロトコルを「公開鍵暗号方式」に基づいて標準化。

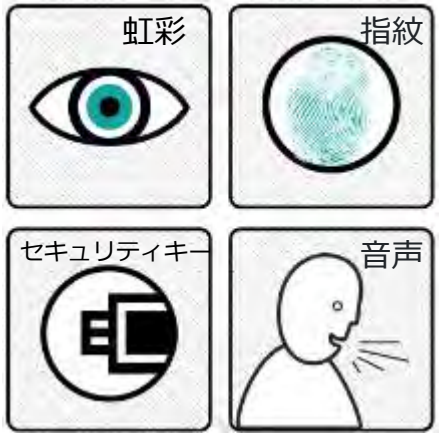
Client Standardization for Local Authentication

（デバイス上の認証に関するクライアント標準化）

FIDO標準では、ユーザー操作によるデバイス上の認証方法について共通のインターフェースを定義。OSやWebブラウザのネイティブサポートが進んでいます。



Client Standardization for Local Authentication



標準化されたインターフェースを介して、PINコード、生体認証（顔認証、音声認証、虹彩認証、指紋認証等）、2段階認証デバイスなど、さまざまな認証方法を追加することが可能です。

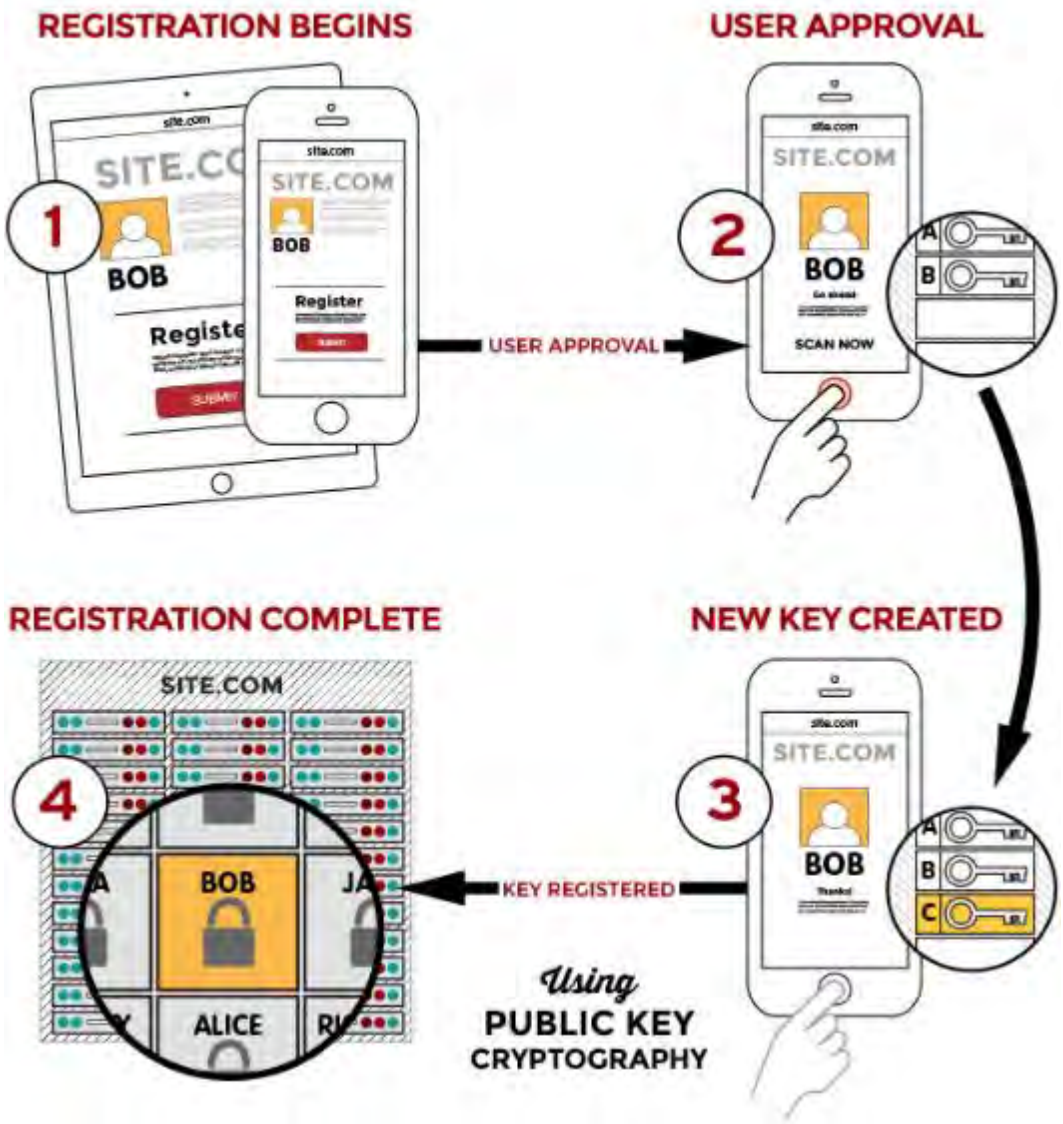
参考）ＦＩＤＯ登録（Registration）

1. ＦＩＤＯに対応したオンラインサービスの登録を開始すると、デバイス上で利用可能な「FIDO認証器」を選択

2. ユーザーは、指紋認証・セキュリティキーなど「FIDO認証器」を選択し、ロックを解除

3. ユーザーのデバイスは、新しい鍵のペア（公開鍵と秘密鍵）を生成

4. 公開鍵がオンラインサービスに送信され、ユーザーアカウントと関連付けられます。秘密鍵や生体情報はデバイスの「FIDO認証器（TPM）」に保存されます。



参考）ＦＩＤＯログイン（Login）

1. ＦＩＤＯに対応したオンラインサービスは、登録済みのデバイスでログインするように、ユーザーにチャレンジを送信します。

2. ユーザーは、登録時と同じ方法を使って、「FIDO認証器」 をロック解除します。

3. デバイスは秘密鍵を選択し、サービスから提供されたチャレンジに署名します。

4. デバイスは、署名付きのチャレンジをサービスに応答します。サービスは、保管している公開鍵を用いて応答の検証を行い、ユーザーをログインさせます。