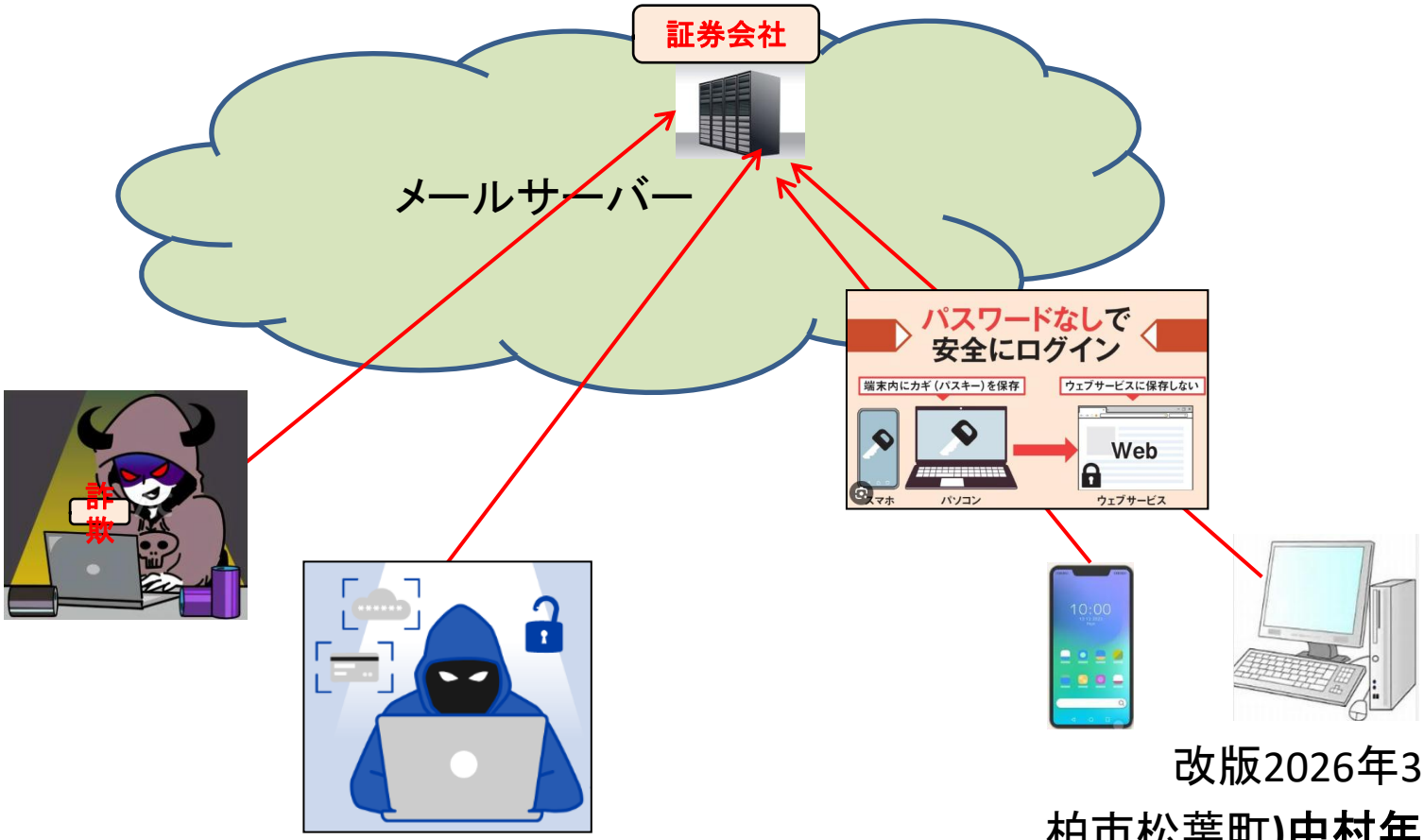
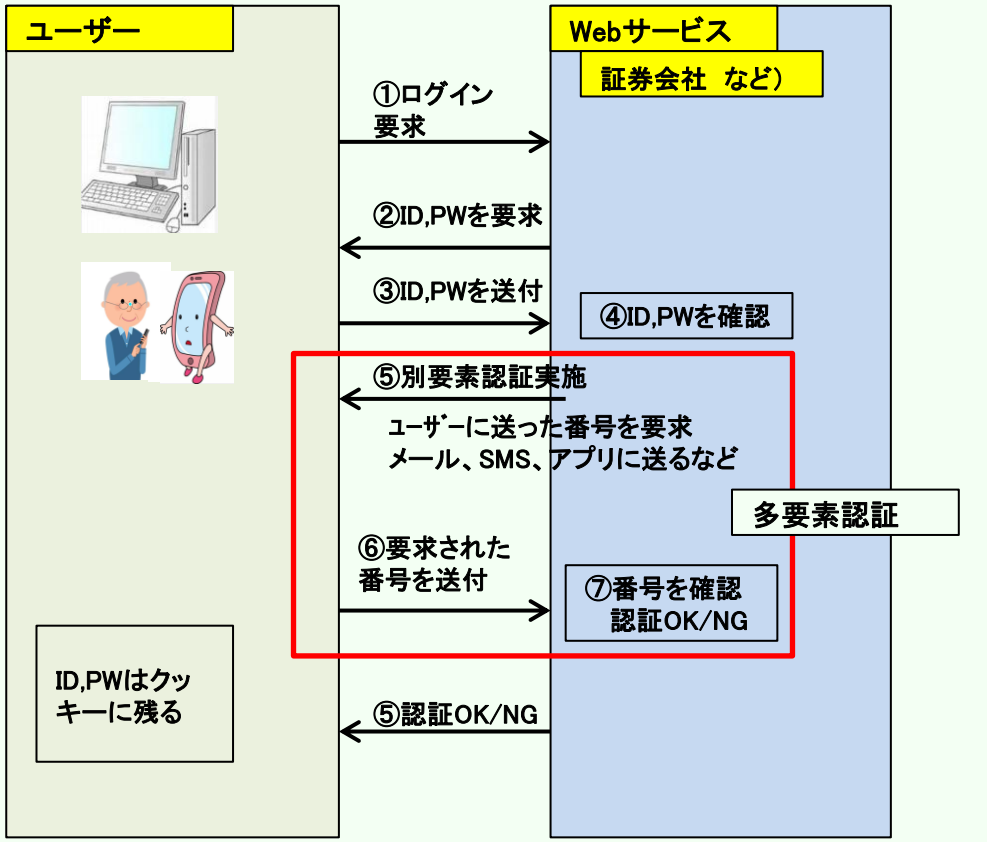
# パスキー認証
# （安全な認証方式）




改版2026年3月

柏市松葉町)**中村年雄**

# 今までの認証方法

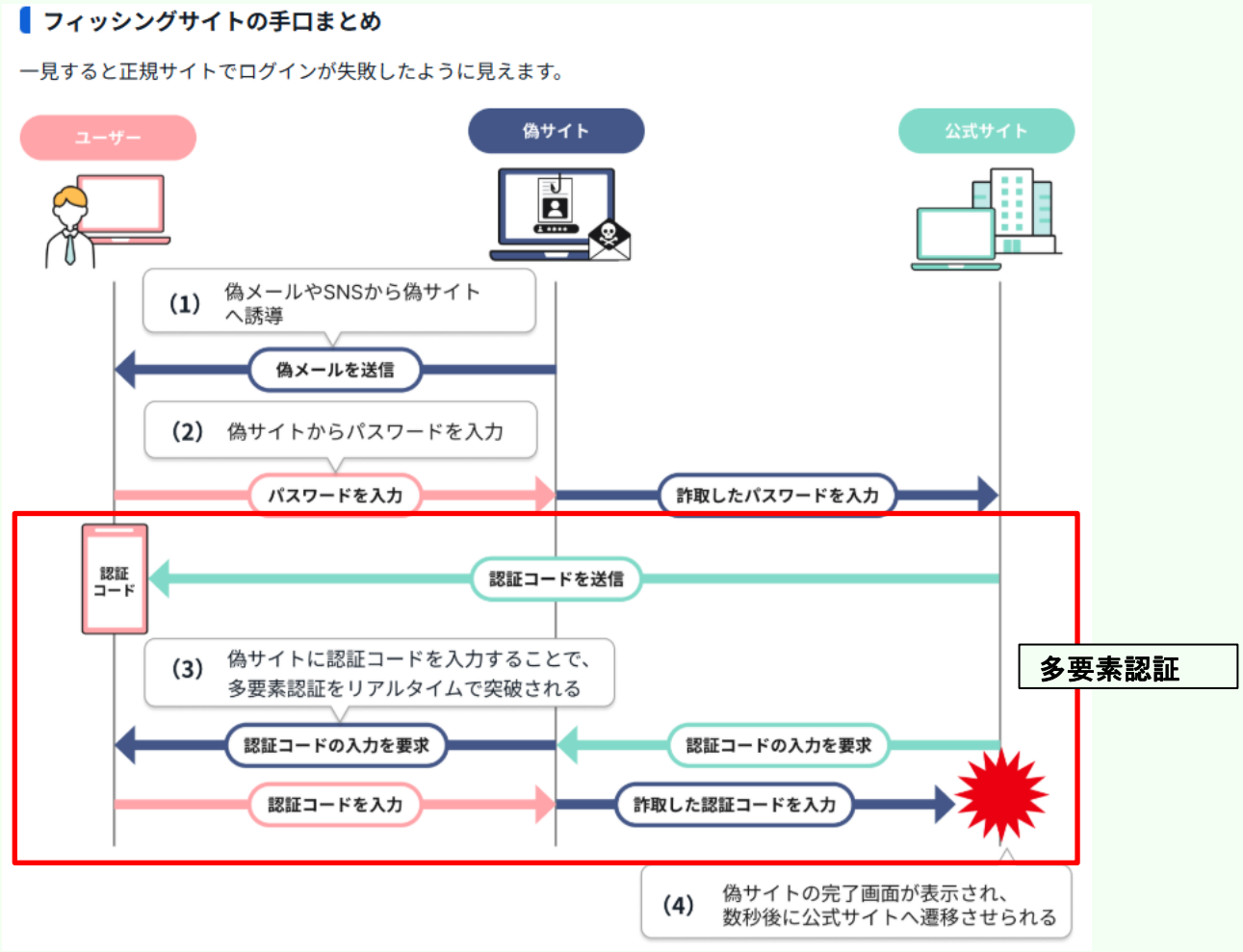



◇ID,PW認証
サービス毎のID,PWを覚えなくてはいけない。

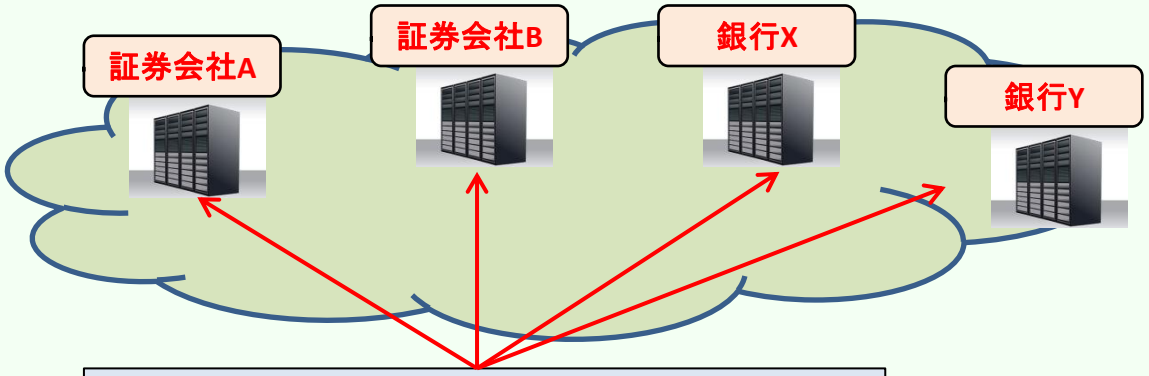
◇単要素認証（ID,PWだけで認証する）
詐欺に弱い！ID,PWが盗まれると終わり。偽メール、遠隔操作により乗っ取られる。

◇多要素認証（ID,PW＋α ）
詐欺に強い！ID,PWを盗まれてもサービスが乗っ取られない。
しかし別途確認のためにスマホなどが必要で面倒である。

# フィッシングの流れ


フィッシングサイトの手口まとめ
一見すると正規サイトでログインが失敗したように見えます。
ユーザー
偽サイト
公式サイト
(1) 偽メールやSNSから偽サイトへ誘導
偽メールを送信
(2) 偽サイトからパスワードを入力
パスワードを入力
詐取したパスワードを入力
認証コード
認証コードを送信
(3) 偽サイトに認証コードを入力することで、多要素認証をリアルタイムで突破される
多要素認証
認証コードの入力を要求
認証コードの入力を要求
認証コードを入力
詐取した認証コードを入力
(4) 偽サイトの完了画面が表示され、数秒後に公式サイトへ遷移させられる

# パスキーの強み

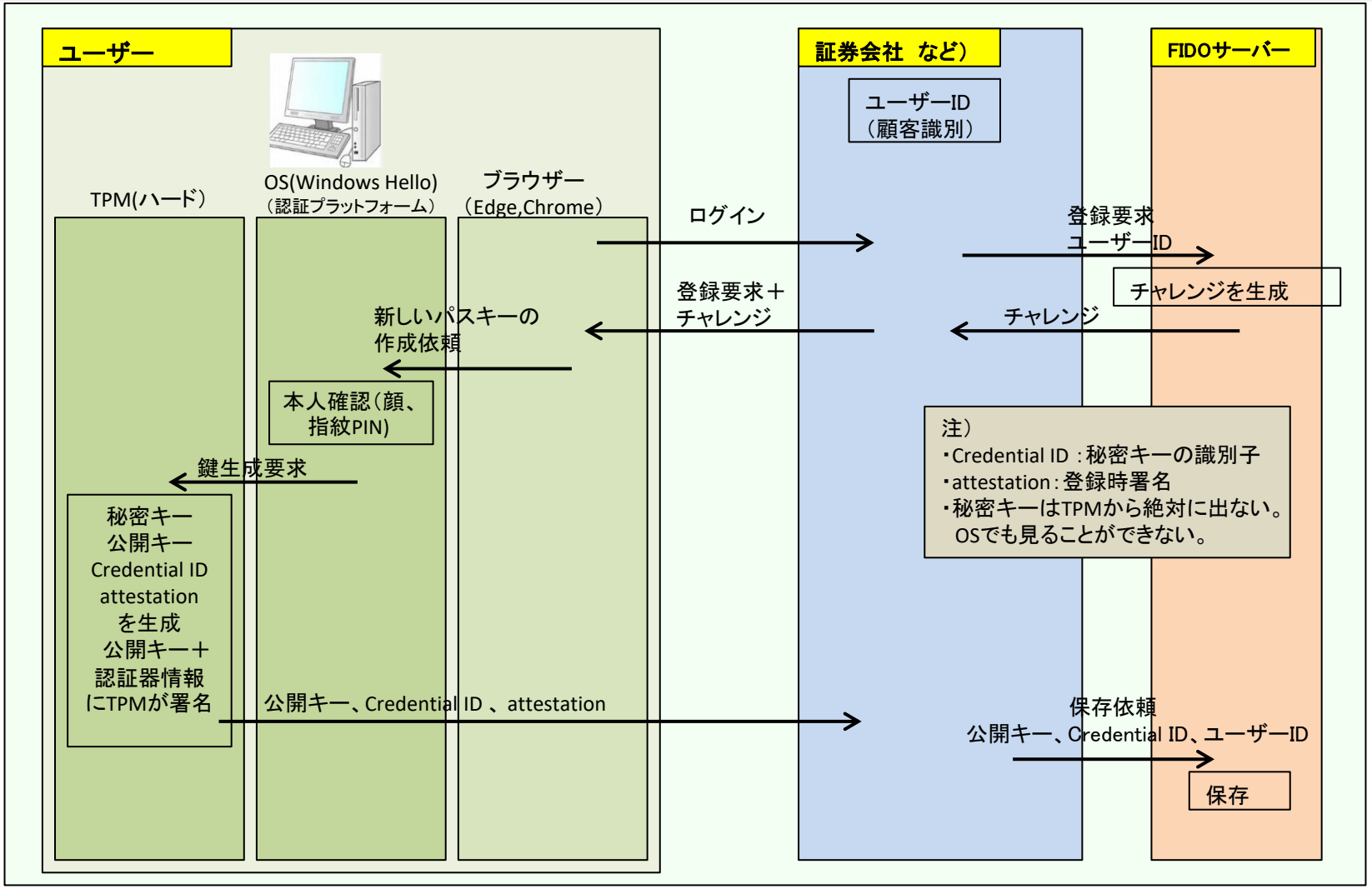



同じ操作（PIN、指紋認証、顔認証）でどこでもログインできる。
個別のログイン方法は必要ない！！

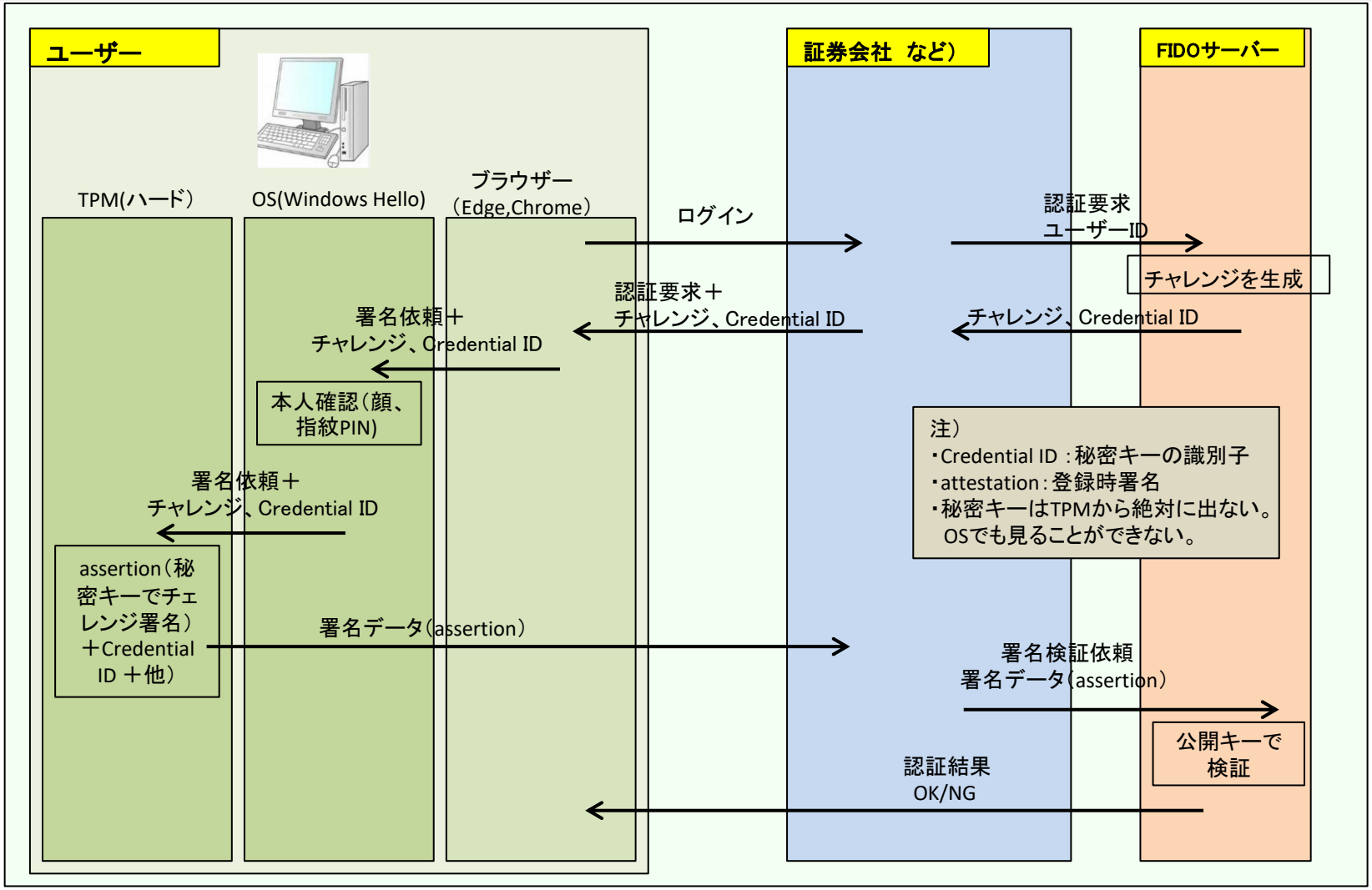
## パスキーの強み

- フィッシングされない
- パスワード漏洩が起きない
- 入力が不要で速い
- PINや生体認証は端末ローカル（特定端末でしか認証できない）で安全
- 秘密鍵は端末外に出ない
- 端末紛失時の復旧手段が複数ある

# パスキーの流れ(登録時）PCの場合



# パスキーの流れ(認証時）PCの場合



# パスキー　スマホ（PCとの対応）

**PC**

TPM

Windows　Hello

**スマホ**

①iPhone:Secure Enclave
②Android：StrongBox
（またはTEE（TrustZone）

①iPhone：icloud　Kyechain
②Android：
Google Password Manager

ブラウザー

サービス（証券会社など）

FIDOサーバー

# 付加情報

・**FIDOサーバー**:FIDO（Fast IDentity Online）規格に準拠し、パスワードを使わずに安全な「パスキー認証」を実現するための認証サーバー

・パスキーはアカウントに紐づくのではなくデバイスに紐づく

・PCとスマホでは別々の認証方法が使える。
例：・PC：パスキー、・スマホ：ID，PW

・パスキーを登録しても今までのID＋PWでログインできる
サービス側（証券会社によって異なる。
パスキーを登録するとID,PWではログインできないサービスもある。

・**日本の証券会社の“実情”**はどうか？
現状の傾向をまとめると：
- パスキー導入＝ID＋PW無効化　海外大手サービスでは一般的
→日本では ほぼ無い
- **パスキーとID＋PWの併存→ ほぼ全社これ**
- ユーザーがパスワード無効化できる

・**チャレンジ**
数十バイトのランダムデータ。 同じものは1度しか使われない。

・**TPM**（Trusted Platform Module）：
PC の中にある“独立したセキュリティ専用ハードウェア”。
「小さな金庫」＋「暗号計算専用プロセッサ」

・**StrongBox**：高級スマホ
物理的に独立したセキュリティチップ

・**TEE（TrustZone）**中級、低級スマホ
物理的には独立していない。CPU内部のSecure World

- 高級機種 → StrongBox（＋TEE）
- 中級機種 → TEE（TrustZone）＋Keystore
- 低級機種 → ソフトウェアKeystore（TEEなし）

・**キーの保管場所**

PCの中（TPM）
秘密キー(サービスごと)
・SBI証券用秘密キー　A
・楽天証券用秘密キー　B
・XXXX用j秘密キー　C

証券会社
・A顧客用
PC用公開キー
スマホ用公開キー
・・・
・X顧客用公開キー

・ブラウザーにはメタデータを保存、同期の機能がある。メタデータとはサービスのドメイン（例：sbi.co.jp）、公開キー、Credential ID，どの方式（TPM/Secure Enclaveka） など

・**Credential ID**：秘密キーの識別子
・**attestation**：登録時署名（チャレンジも含まれる。） デバイスの信頼性（“鍵の出自”を保証）
・**assertion**:認証時署名（チャレンジも含まれる。） 本人の認証
・秘密キーはTPMから絶対に出ない。
OSでも見ることができない。

# 事前準備

## PC

Windows Helloの“本人確認手段“の設定
・“設定”－“アカウント”－“サインオプション”
サインインする方法に“顔認証”“指紋認証”“PIN”から選び設定する。


## スマホ

Android9以降のスマホはほぼ問題なく使える。

① 生体認証 or PIN を設定
設定 → セキュリティ → 画面ロック
- 指紋
- 顔
- PIN

のいずれかを設定
② Google パスワードマネージャーをオン
設定 → パスワードとアカウント → Google
「パスワードマネージャー」をオン
③ StrongBox または TEE が有効（自動）
これはユーザーが設定する必要はない。
スマホが対応していれば自動で使われる。

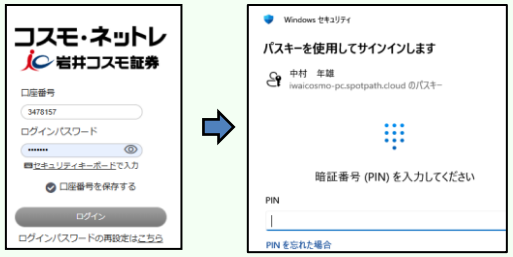
# 実例

## 岩井証券

①今までのID、PWでログインする。
②第二要素認証としてパスキーでログインする。

ログインに今までのID、PWが必要。
第二要素認証としてパスキーでログインできるので便利。ログインがPCだけでできる（メール、SMNなどを確認しないでもできる）は便利。

パスキーでないとログインできなくなる。




## SBI証券

①パスキーでログイン
　注）ID,PWでもログインできる。
　ログイン画面にどちらかを選ぶようになっている。

今までのID,PWだけでログインできる。
パスキーを導入した意味がない！
フィッシング詐欺に弱い。


## 楽天証券

①IDのみを入力する。
②画面に出たQRコードをスマホで読み取りパスキーログインが完了。

パスキーを使うのに今までのIDが必要（PWは不要）
スマホが必須。使いづらい！

注）①パスキーの目的はID,PWが無くてもログインできること。
　②ID,PWを残す理由：「パスキーが使えない端末の人もいる」、「PC,スマホを紛失や故障した人が困る」 など
　Goole,Microsoft,Apple,多くの海外銀行　などはパスキーだけでログイン可能。当たり前

# パスキー（付加情報（２））

**★端末を紛失・故障したらどうするのか？**ここが一番気になるところ。
実は、パスキーは “単一端末に閉じない仕組み” が用意されている。
A. 同じアカウントで同期されるパスキー（クラウド同期型）
Google、Apple、Microsoft のパスキーはアカウントに紐づいて複数端末に自動同期 されます。
例：
- iPhoneで作ったパスキー → iPad、Macにも自動でコピー
- Androidで作ったパスキー → 他のAndroid端末にも同期
- Windows Helloのパスキー → Microsoftアカウントでバックアップ

**1台壊れても、他の端末でログイン可能**

★ 日本の多くのサービスが「パスキー＋ID/PW併存」なのはなぜ？
理由はシンプルで、移行期間だからです。（→早い話が日本人はデジタル化に対応できない人がシニア中心に多いからです。）
- 日本のWebサービスはまだパスキー完全移行が進んでいない
- ユーザーの端末環境がバラバラ（古いAndroid、ガラホ、PCなど）
- パスキーだけにすると「ログインできない人」が大量に出る

そのため、現状は パスキーは“便利な追加手段” として提供されているだけで、
パスワード廃止はこれから という段階です。
海外（Google、Microsoft、Apple）はすでに
「パスキー優先・パスワードはほぼ使わない」方向に進んでいます。

★ Microsoft アカウントのクラウドとは何か？
これは「Microsoft アカウントの設定・秘密情報・暗号鍵などを安全に保存するためのクラウド基盤」のこと。
具体的には：
- Windows Hello の設定
- パスキーの暗号化バックアップ
- Edge のパスワード
- デバイスの暗号化キー（BitLocker 回復キーな）
- Microsoft Store の購入履歴
- ライセンス情報

# パスキー（秘密キー）の復元流れ

**パスキーは端末依存である。端末の紛失又は故障した場合にどうなるのか？→他端末で復元が必要**