第一回 SPEDU セミナー

パスキーのすべて

倉林雅

倉林雅（kura）

OpenIDファウンデーション・ジャパン
理事・エバンジェリスト

OpenID・OAuth・パスキー技術の啓発・教育活動に
携わり、現在は某インターネット企業にて
プロダクトマネージャーを担当。

パスワードによる被害状況

パスワードを狙った攻撃手法

- リスト攻撃をはじめとするパスワードを狙った攻撃手法が今も用いられている

	攻撃手法	概要
1	**リスト攻撃（Credential Stuffing）**	これは、他のウェブサイトから漏洩したユーザー名とパスワードのリストを使用して、別のサービスへのログインを試みる手法です。攻撃者は、多くの人が複数のサイトで同じパスワードを使い回していることを利用します。
2	**ブルートフォース攻撃（Brute-Force Attack）**	この手法では、考えられるすべてのパスワードの組み合わせを試行して、正解を見つけようとします。辞書攻撃（よく使われる単語やフレーズのリストを試す）もこれに含まれます。
3	**フィッシング（ Phishing）**	偽のウェブサイトやメール、メッセージなどを使って、ユーザーにパスワードを入力させるように誘導する手法です。例えば、銀行や有名なサービスになりすまして、ログイン情報を盗み取ろうとします。
4	**マルウェア（ Malware）**	キーロガー（キーボード入力を記録するソフトウェア）やトロイの木馬などのマルウェアをコンピュータやデバイスに感染させ、パスワードを盗み取る手法です。
5	**ソーシャルエンジニアリング（Social Engineering）**	人間心理の隙をついて、パスワードなどの機密情報を聞き出そうとする手法です。電話や対面で、信頼できる人物になりすますなどして情報を得ようとします。
6	**パスワードスプレー攻撃（Password Spraying）**	これは、少数の一般的なパスワードを、多数のユーザーアカウントに対して試行する手法です。アカウントロックアウトを防ぎつつ、パスワードの使い回しを狙います。
7	**辞書攻撃（ Dictionary Attack）**	ブルートフォース攻撃の一種ですが、一般的な単語、フレーズ、または以前に漏洩したパスワードのリスト（辞書）を使用してパスワードを推測します。

パスワードリスト攻撃被害

- 推測されやすいパスワードや漏洩したパスワードは市場で出回り、現在も各社サービスでリスト型攻撃が繰り返され被害が後をたたない

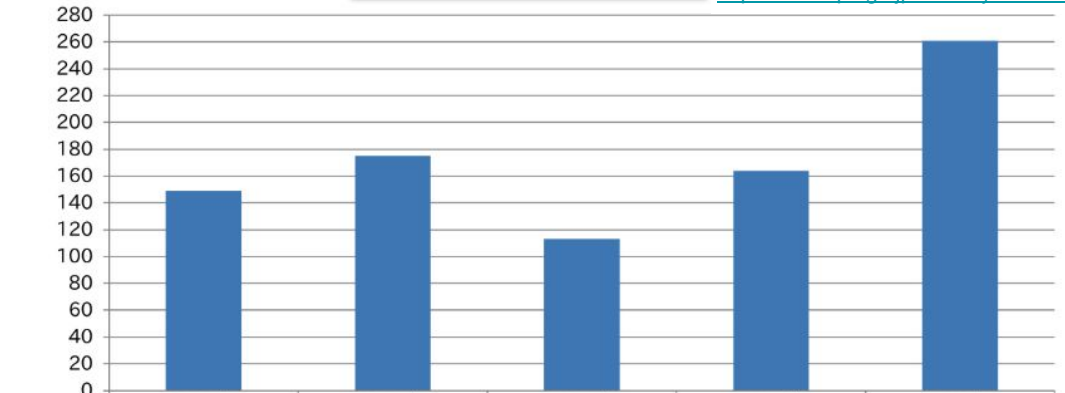
時期	事例
2024年12月	メールアカウントの不正使用によるフィッシングメールの送信について - 北海道大学病院
2024年3月	お茶の水女子大学研究室サーバへの不正アクセスについて
2023年3月	「エン転職」への不正ログイン発生に関するお詫びとお願い - エン・ジャパン
2023年12月	「ショップチャンネル」で不正ログイン注文 - Security NEXT
2022年10月	不正アクセスとアカウント管理に関するご注意 - スクウェア・エニックス
2022年9月	「ニトリアプリ」への不正アクセスによる個人情報流出の可能性に関する お詫びとお知らせ - ニトリホールディングス
2022年7月	サンドラッグの複数関連サイトにPWリスト攻撃 - Security NEXT

不正ログインに関する相談状況

- IPAへの「不正ログイン」に関する相談が前四半期から約59.1%増の261件
- Facebook、Instagramなどに不正ログインされて、自分ではログインできなくなったという相談が多く寄せられた

「不正ログイン」相談件数の推移

情報セキュリティ安心相談窓口の相談状況［ 2025年第1四半期（1月～3月）］
https://www.ipa.go.jp/security/anshin/reports/2025q1outline.html



	2024年 1月～3月	2024年 4月～6月	2024年 7月～9月	2024年 10月～12月	2025年 1月～3月
■相談件数	149	175	113	164	261

フィッシング攻撃被害

- 金融系をはじめユーザーを偽サイトへ誘導してパスワードなどのクレデンシャルを盗み出す
- フィッシング攻撃の被害も継続している

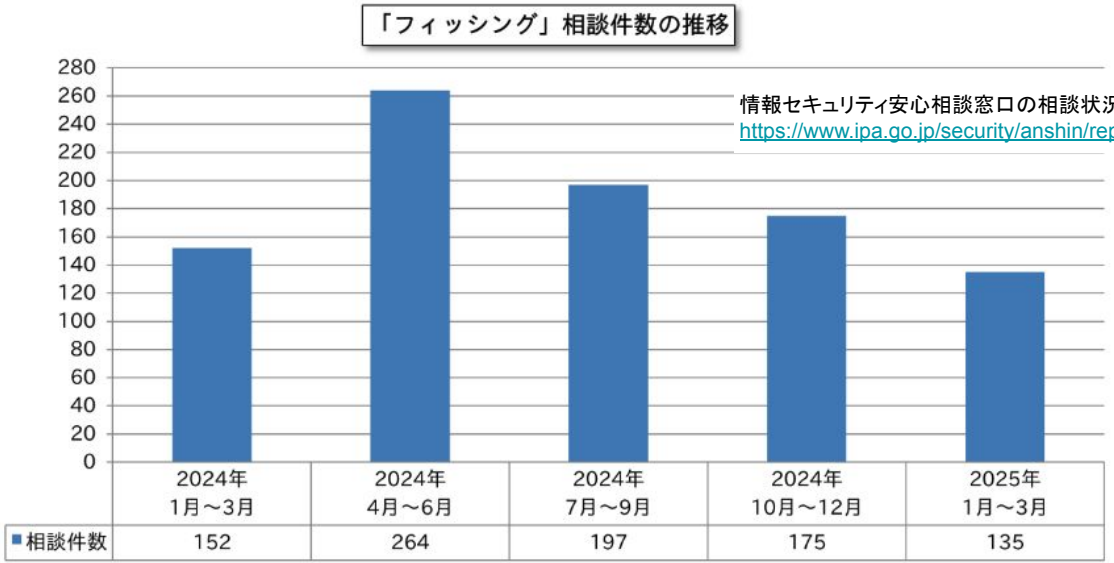
時期	事例
2025年08月06日	SMBC日興証券をかたるフィッシング
2025年07月31日	アコムをかたるフィッシング
2025年06月16日	岩井コスモ証券をかたるフィッシング
2025年06月16日	大和証券をかたるフィッシング
2025年05月21日	PayPayカードをかたるフィッシング
2025年04月30日	GMOクリック証券をかたるフィッシング
2025年04月21日	三菱UFJモルガン・スタンレー証券をかたるフィッシング
2025年04月09日	東京ガスをかたるフィッシング

時期	事例
2025年04月09日	ANA をかたるフィッシング
2025年04月09日	LINE をかたるフィッシング
2025年04月08日	松井証券をかたるフィッシング
2025年04月01日	野村證券をかたるフィッシング
2025年04月01日	楽天証券をかたるフィッシング
2025年04月01日	SBI証券をかたるフィッシング
2025年03月31日	マネックス証券をかたるフィッシング
2025年03月05日	Apple をかたるフィッシング

フィッシング対策協議会
https://www.antiphishing.jp/news/database/

フィッシングに関する相談状況

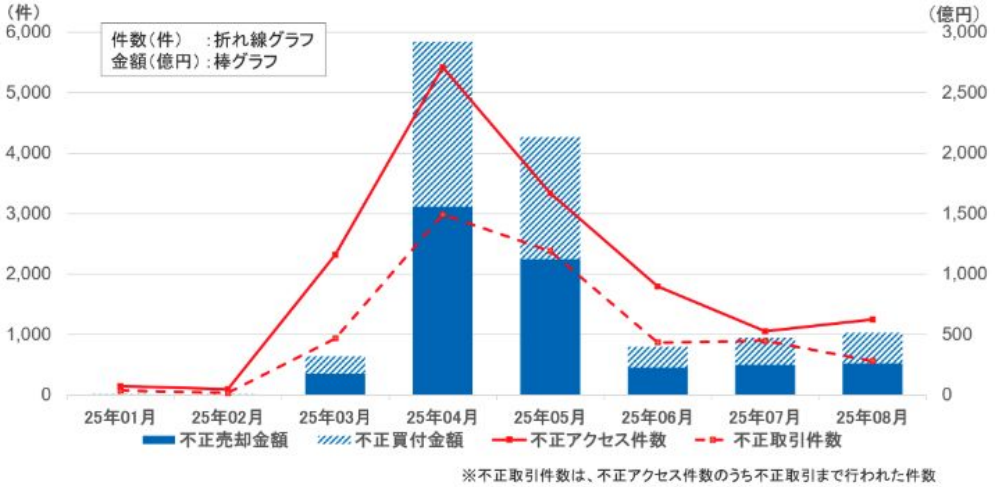
- IPAへの「フィッシング」に関する相談件数は、前四半期から約22.9%減の135件
- 各種サービスや企業を騙ったメールから偽サイトにアクセスして、個人情報やクレジットカード情報などを入力したという相談が寄せられた



情報セキュリティ安心相談窓口の相談状況［ 2025年第1四半期（1月～3月）］
https://www.ipa.go.jp/security/anshin/reports/2025q1outline.html

証券会社の被害状況

- 証券会社のウェブサイトを装った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増

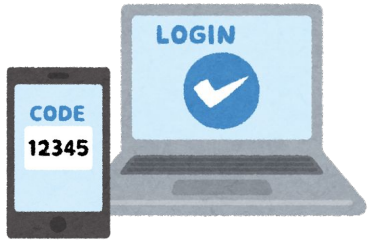


不正取引が発生した証券会社数（社）							
25年1月	25年2月	25年3月	25年4月	25年5月	25年6月	25年7月	25年8月
2	2	5	10	16	7	6	7

金融庁からのお願い・注意喚起
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

OTPやSMS認証のフィッシング耐性

- パスワードに加えたワンタイムパスワード（OTP）やパスワードを利用しないSMS認証はパスワードリスト型攻撃の対策としてのは有効である
- しかし、OTPやSMS認証はユーザーによるクレデンシャル（パスワードや確認コードなど）の入力が必要であるため、MiTM（Man in The Middle）やAiTM（Adversary in The Middle）などのフィッシング攻撃への耐性はない



Adversary in The Middle（AiTM）

正規サイトがクレデンシャルを入力する
認証を提供しているとフィッシングは防げない

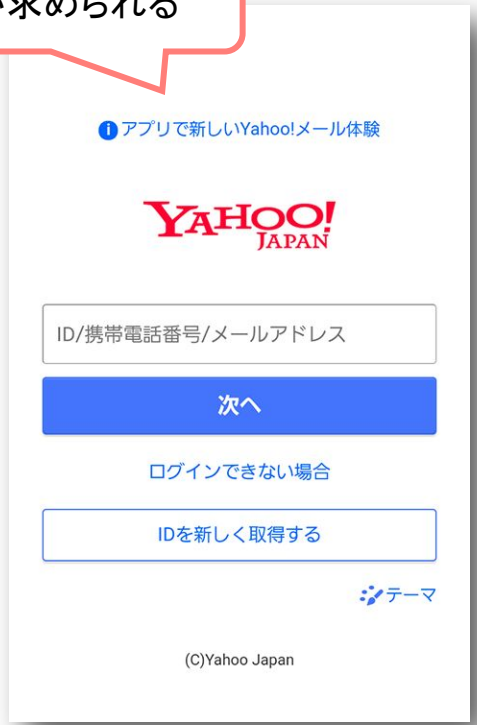
引用:フィッシング対策協議会 フィッシングレポート 2023
https://www.antiphishing.jp/report/phishing_report_2023.pdf

パスキーの概要

パスキーが提供する機能

「セキュリティとUXを両立したユーザー認証」

ログインが求められる


アプリで新しいYahoo!メール体験
YAHOO! JAPAN
ID/携帯電話番号/メールアドレス
次へ
ログインできない場合
IDを新しく取得する
テーマ
(C)Yahoo Japan


アプリで新しいYahoo!メール体験
本人確認
login.yahoo.co.jp で本人確認を行えるよう、指紋認証を行ってください。
センサーをタップします
キャンセル
画面ロックを使用
IDを新しく取得する
テーマ
(C)Yahoo Japan


アプリで新しいYahoo!メール体験
YAHOO! JAPAN
ID/携帯電話番号/メールアドレス
次へ
ログインできない場合
IDを新しく取得する
テーマ
(C)Yahoo Japan
アプリで新しいYahoo!メール体験
本人確認
login.yahoo.co.jp で本人確認を行えるよう、指紋認証を行ってください。
センサーをタップします
キャンセル
画面ロックを使用
IDを新しく取得する
テーマ
パスワードや確認コードを入力せずに
生体認証などでログイン

用語集

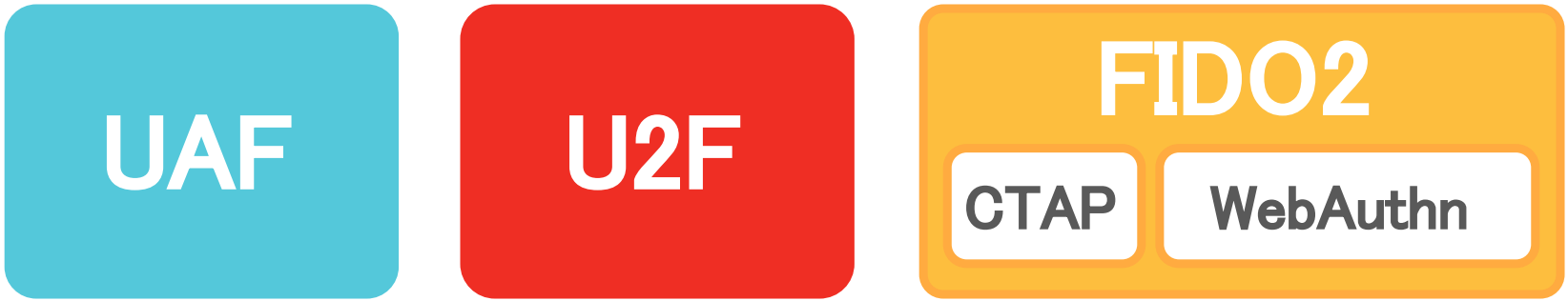
- クレデンシャル情報
  - パスワードや生体情報などユーザー認証に必要な情報
- RP (Relying Party)
  - ユーザーのIDを登録、認証し管理するサーバー（FIDO2 Server）
- Authenticator（認証器）
  - 秘密鍵・公開鍵のペアを生成し、RPへ送信する署名を生成する
- Client-Side
  - Authenticatorやユーザー端末などの総称
- WebAuthn Client
  - ブラウザーなどのUser Agent

FIDOとは

- FIDO = Fast IDentity Online（高速なオンラインID認証）
- 顔や指紋のクレデンシャル情報をサーバーへ送らず保存しない
- 生体認証などのさまざまな認証方法に対応

FIDOで提供している仕様

FIDO Alliancではパスワードレス型、パスワード補完型、FIDO認証を拡大するための拡張仕様を提供している



FIDO UAF

- UAF = Universal Authentication Framework
- 主にスマートフォン（アプリ）を想定した
  パスワードレス型の認証
- 所持認証 + 生体認証など

FIDO U2F

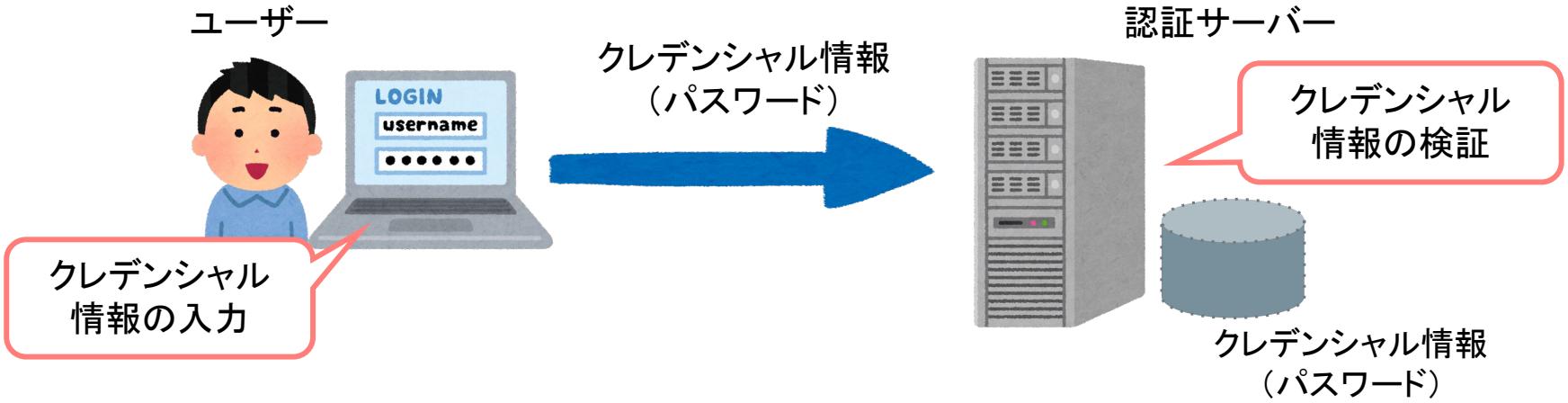
- U2F = Universal 2nd Factor
- 主にPCのWebブラウザーで二要素認証を
  想定したパスワード補完型の認証
- 記憶認証 + 所持認証

FIDO2

- FIDO2の仕様は、FIDO AllianceのClient-to-Authenticator Protocol(CTAP)とW3CのWebAuthnから構成される
- スマートフォンとPCを想定し、一般的なデバイス（USB、BLE、NFCなどが利用できる端末）を活用した認証

従来の認証モデル

- IDとクレデンシャル情報（パスワードなど）を認証サーバーへ送信
- 認証サーバーはIDとクレデンシャル情報を検証し認証
- リスト型攻撃のリスクや、パスワードなどを入力するため通信経路での漏洩やフィッシングでの窃取の懸念あり
- クレデンシャル情報を認証サーバーで保存するため漏洩のリスクは大きい



FIDO認証モデル

- デバイスの認証器(Authenticator)が本人性を検証
- 検証結果に秘密鍵で署名し認証サーバーに送信
- 認証サーバーで公開鍵を使って署名を検証しユーザーを認証
- クレデンシャル情報が流れないため、パスワードのフィッシング耐性あり

CTAPとWebAuthn

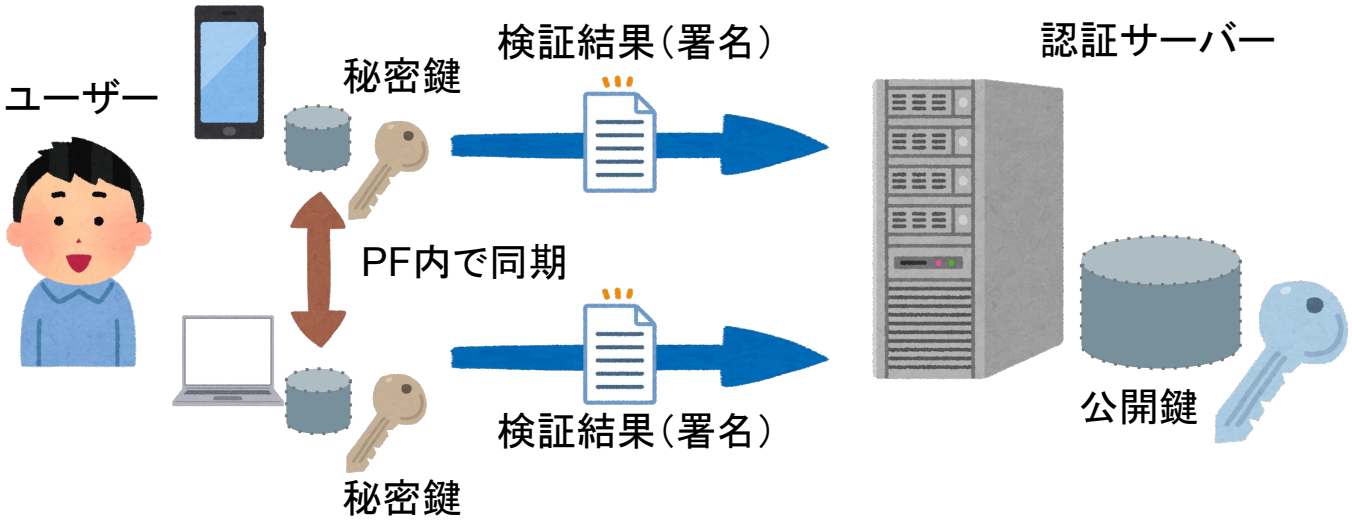
- CTAPはAuthenticator（認証器）とWebAuthn Clientの通信を定義するプロトコル
- WebAuthnはRelying Party（FIDO2認証サーバー）からWebAuthn Client経由でクレデンシャルを操作するプロトコル

パスキー（Passkey）

- 2021年にAppleがWWDCで発表した概念から始まり、Safariで実装された
- FIDOクレデンシャルがプラットフォーム上で同期され、端末紛失や新規端末での移行が可能（一部除く）
- FIDOアライアンスにてGoogleやMicrosoftも方針に賛同
- W3CのWebAuthn API上に実装されている

パスキー認証モデル

- 各プラットフォーム（Apple、Google、Microsoftなど）において秘密鍵が同期されるため、端末ごとの登録が不要になる
- ※ まだパスキーの定義は確定しておらず同期されない端末も含まれる



パスキーの優れている点

リモート攻撃が難しい

脆弱なクレデンシャルを作ることができない

公開鍵が漏れてもアカウントが盗まれる危険性は低い

フィッシング攻撃に強い

ログイン体験がシンプル

パスキーの UXとフロー

パスキーの登録

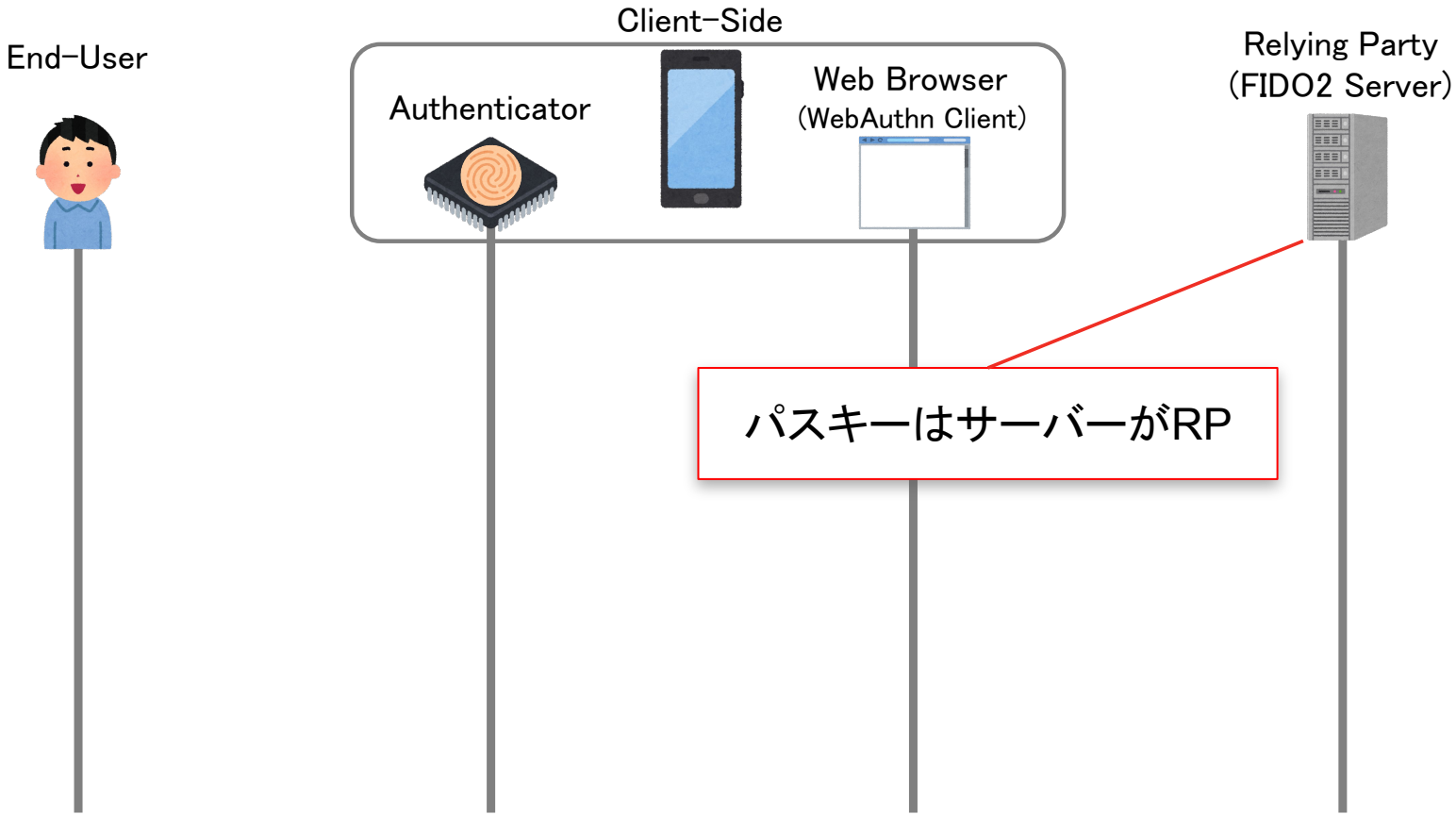
登録のUXは大きく2つに分類できる

- アカウントの新規登録に登録
- 既存アカウントへ任意のタイミングで登録

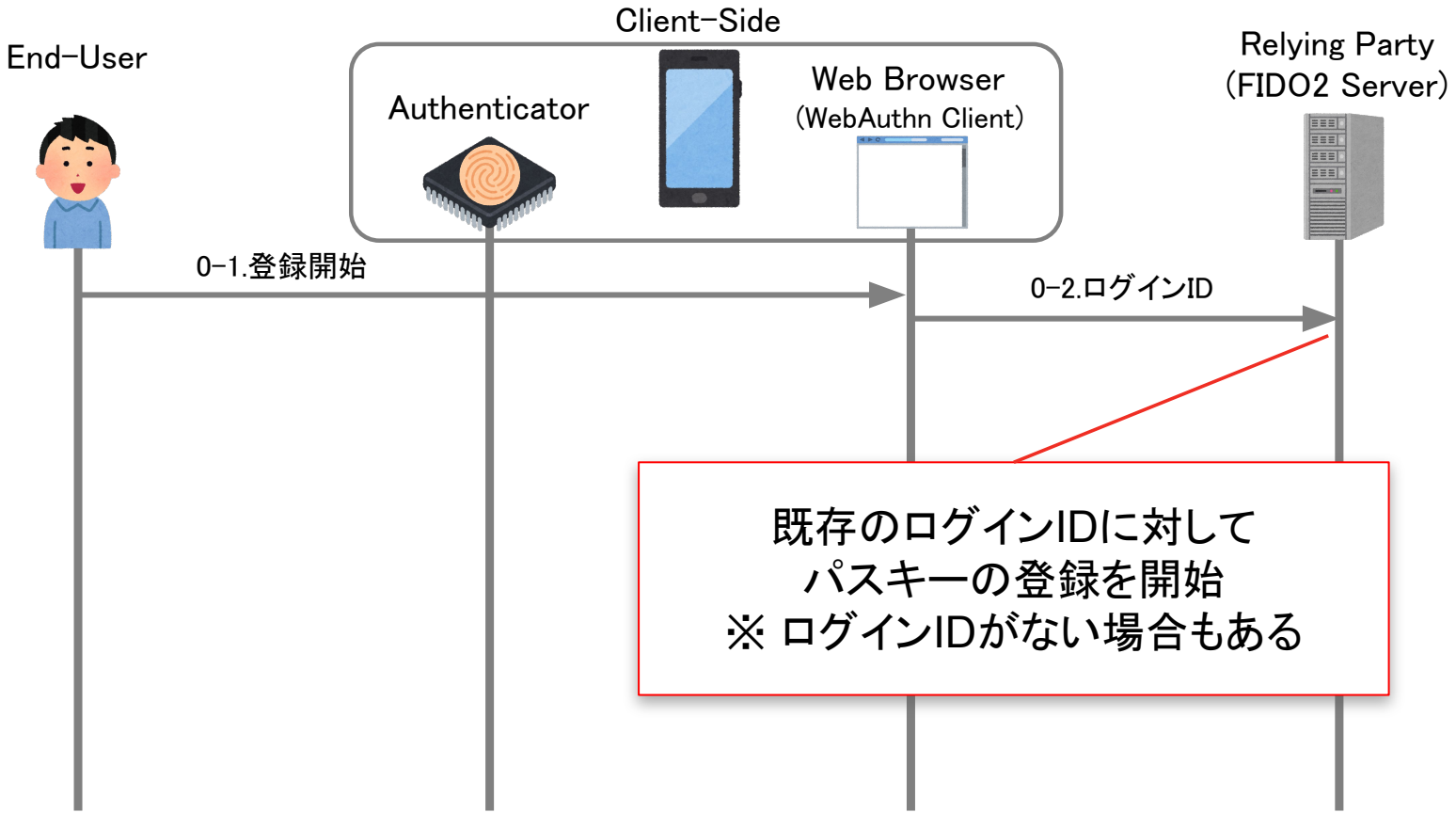
既存アカウントへの登録には工夫が必要

- ログイン直後にパスキー登録を促す
  プロモーションを表示
- パスキーの管理画面から登録
- パスワードログイン時に自動登録など

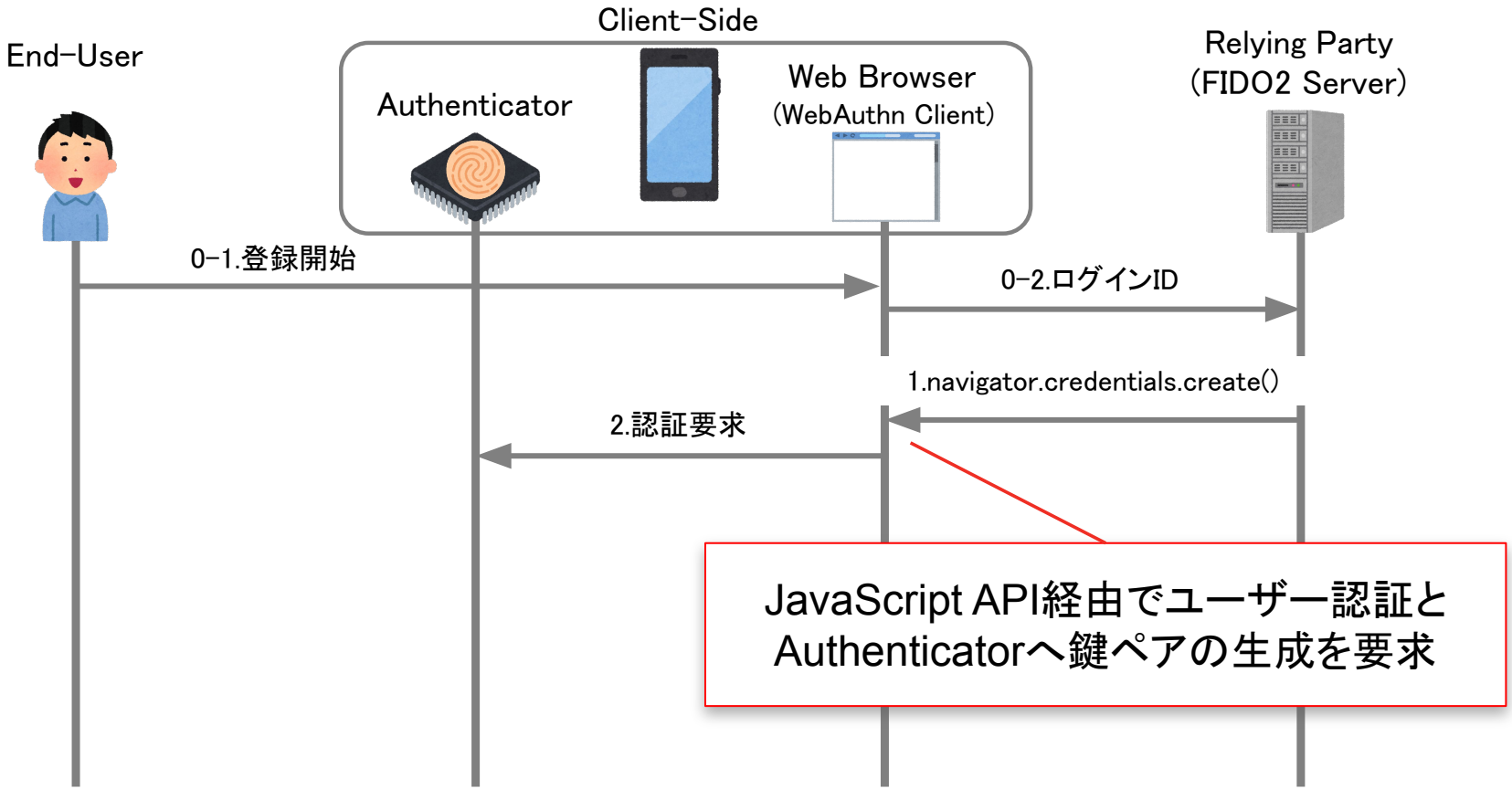
パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
パスキーはサーバーがRP

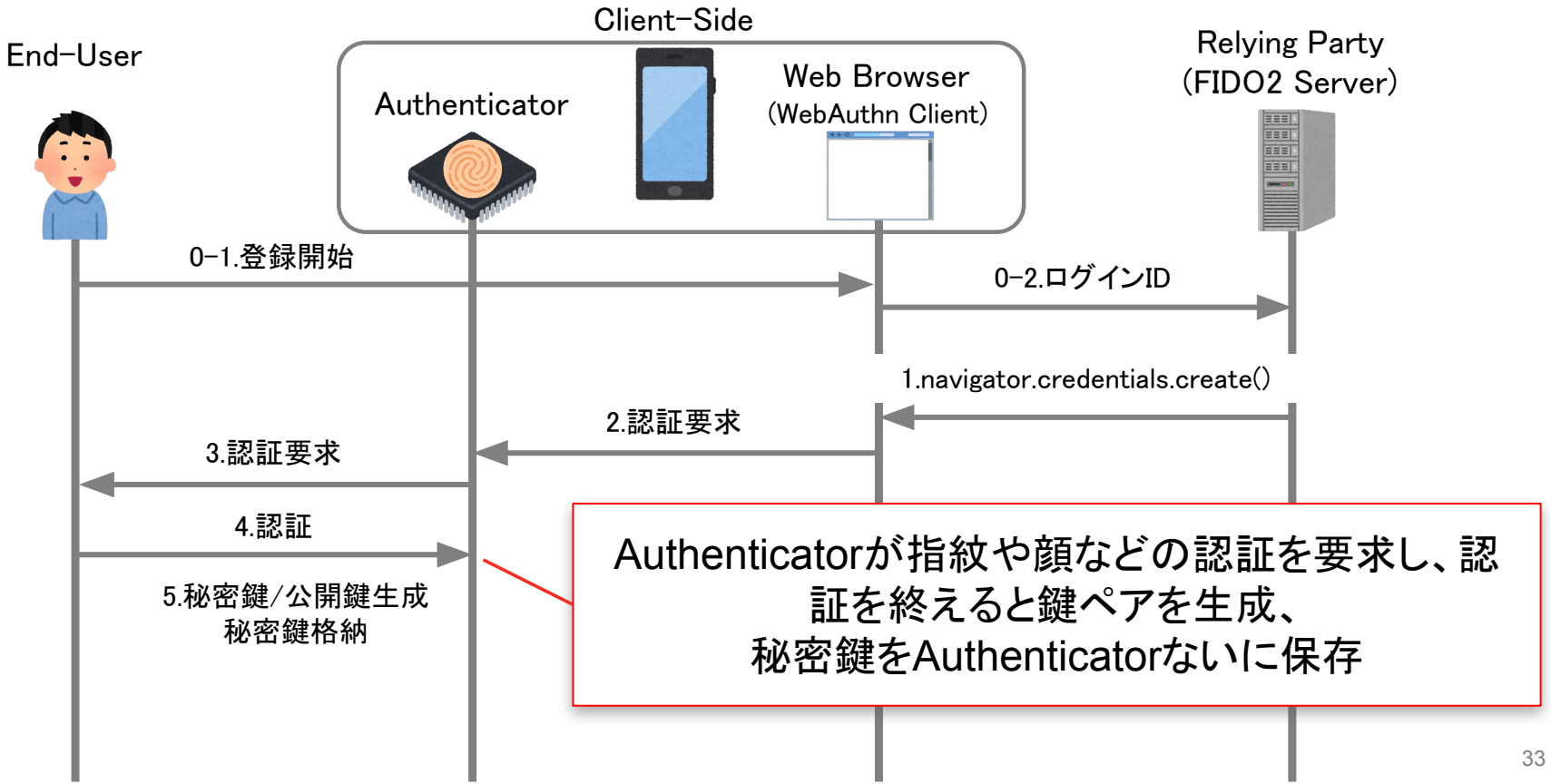
パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
既存のログインIDに対して
パスキーの登録を開始
※ ログインIDがない場合もある

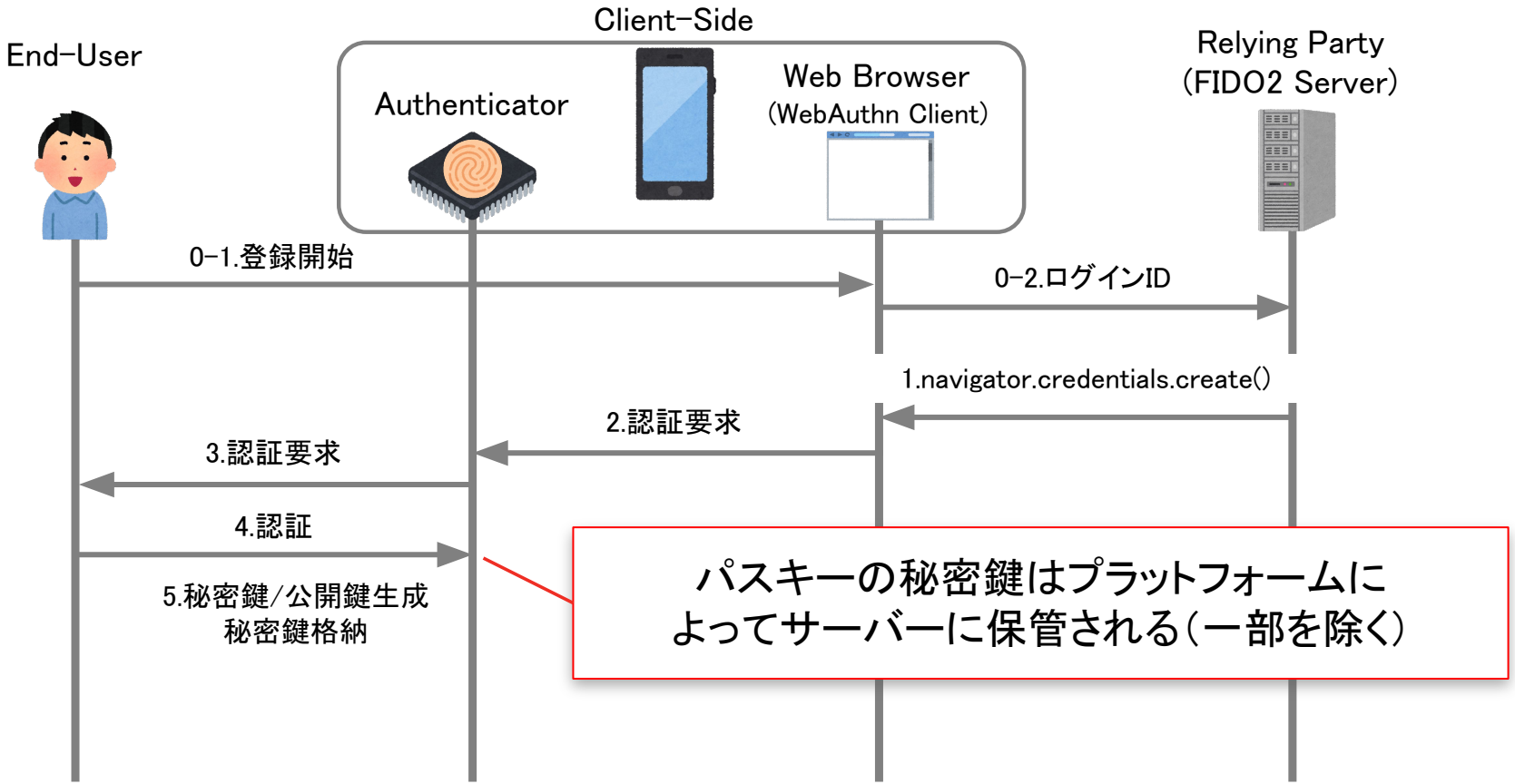
パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
1.navigator.credentials.create()
2.認証要求
JavaScript API経由でユーザー認証と
Authenticatorへ鍵ペアの生成を要求

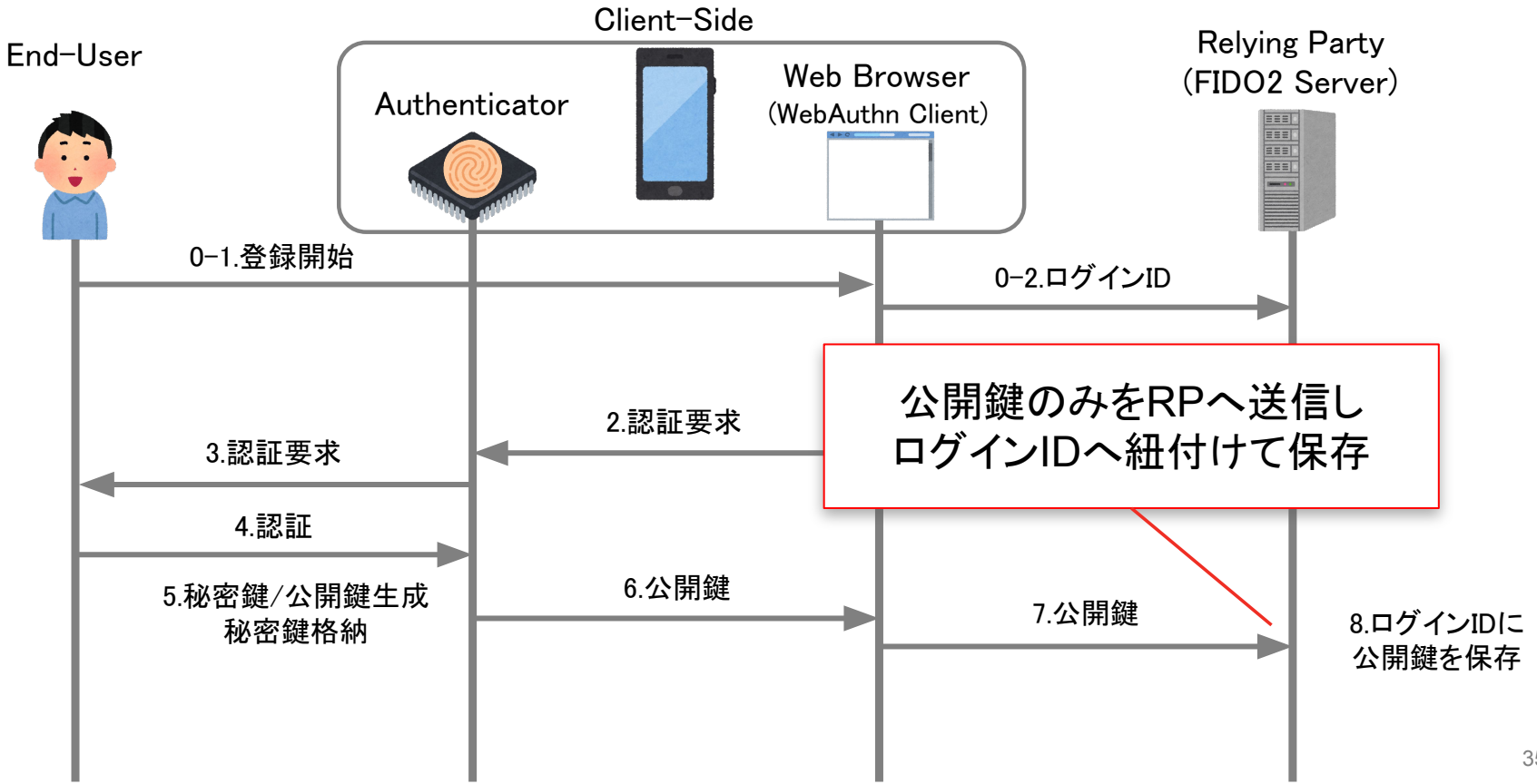
パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
1.navigator.credentials.create()
2.認証要求
3.認証要求
4.認証
5.秘密鍵/公開鍵生成
秘密鍵格納
Authenticatorが指紋や顔などの認証を要求し、認証を終えると鍵ペアを生成、
秘密鍵をAuthenticatorないに保存

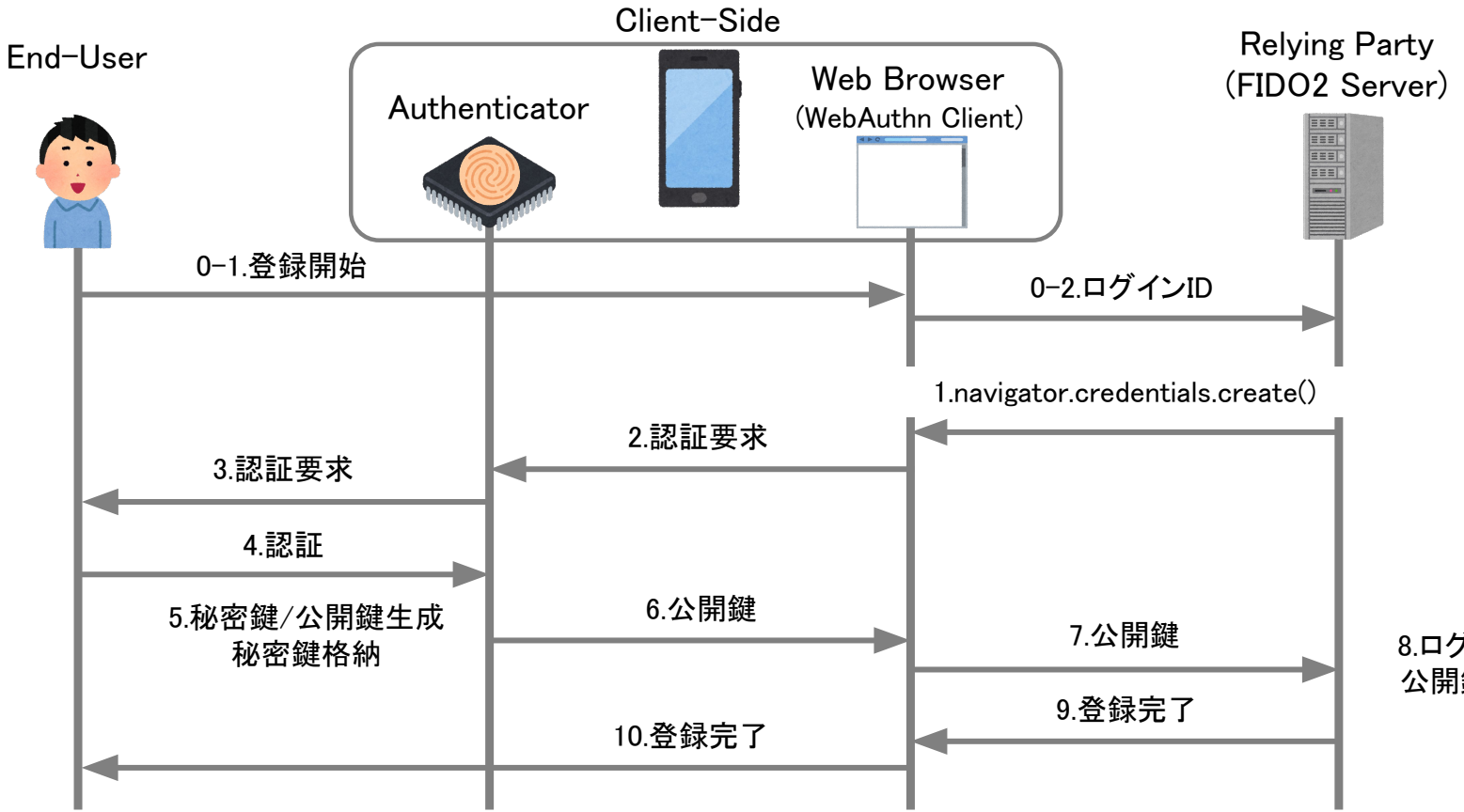
パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
1.navigator.credentials.create()
2.認証要求
3.認証要求
4.認証
5.秘密鍵/公開鍵生成
秘密鍵格納
パスキーの秘密鍵はプラットフォームに
よってサーバーに保管される（一部を除く）

パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
公開鍵のみをRPへ送信し
ログインIDへ紐付けて保存
2.認証要求
3.認証要求
4.認証
5.秘密鍵/公開鍵生成
秘密鍵格納
6.公開鍵
7.公開鍵
8.ログインIDに
公開鍵を保存

パスキー登録フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.登録開始
0-2.ログインID
1.navigator.credentials.create()
2.認証要求
3.認証要求
4.認証
5.秘密鍵/公開鍵生成
秘密鍵格納
6.公開鍵
7.公開鍵
8.ログインIDに
公開鍵を保存
9.登録完了
10.登録完了

パスキーの認証

ログイン体験は2つ考えられる

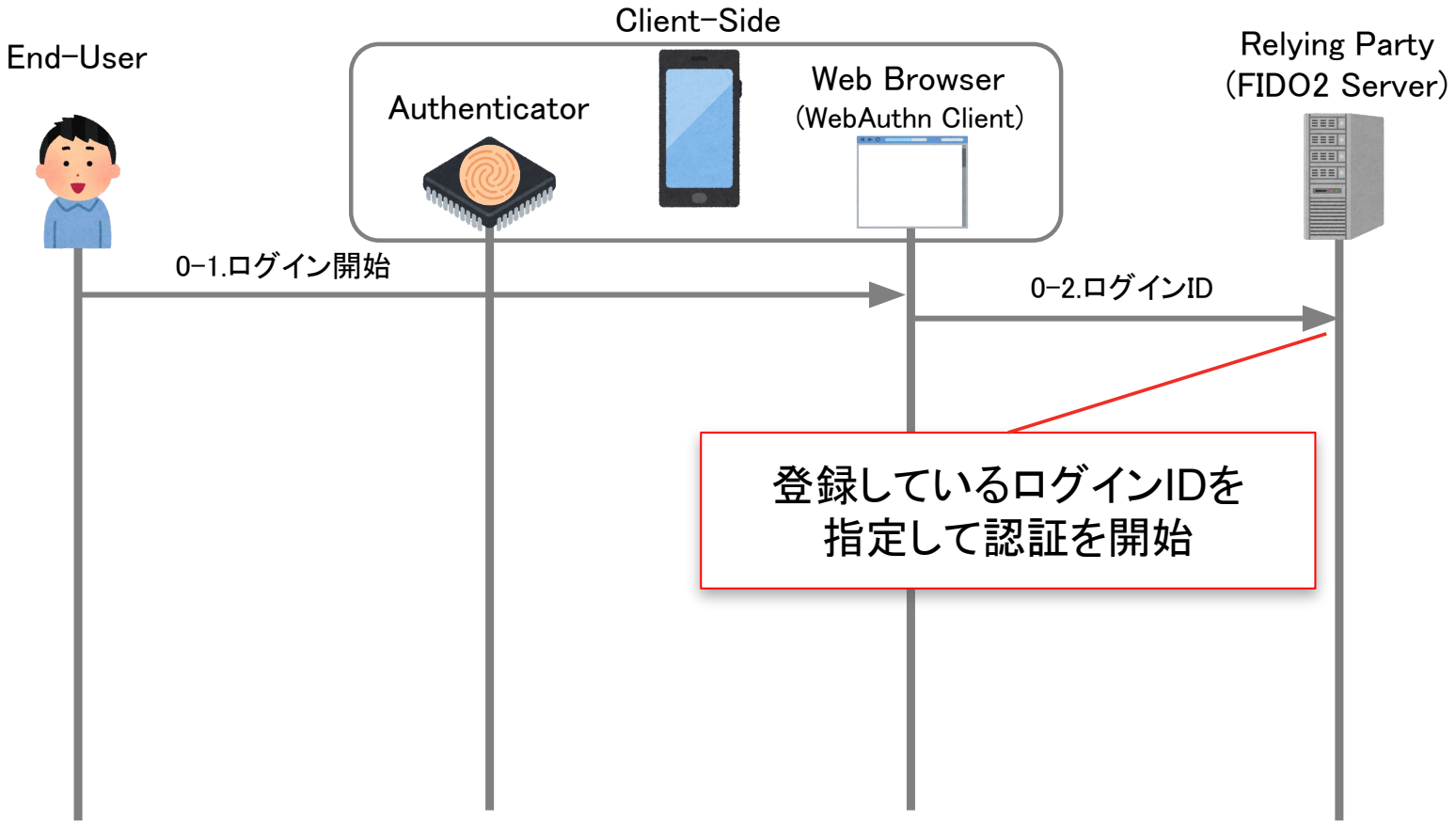
ワンボタンログイン方式

- ログインボタンをタップしアカウントを選択して認証する

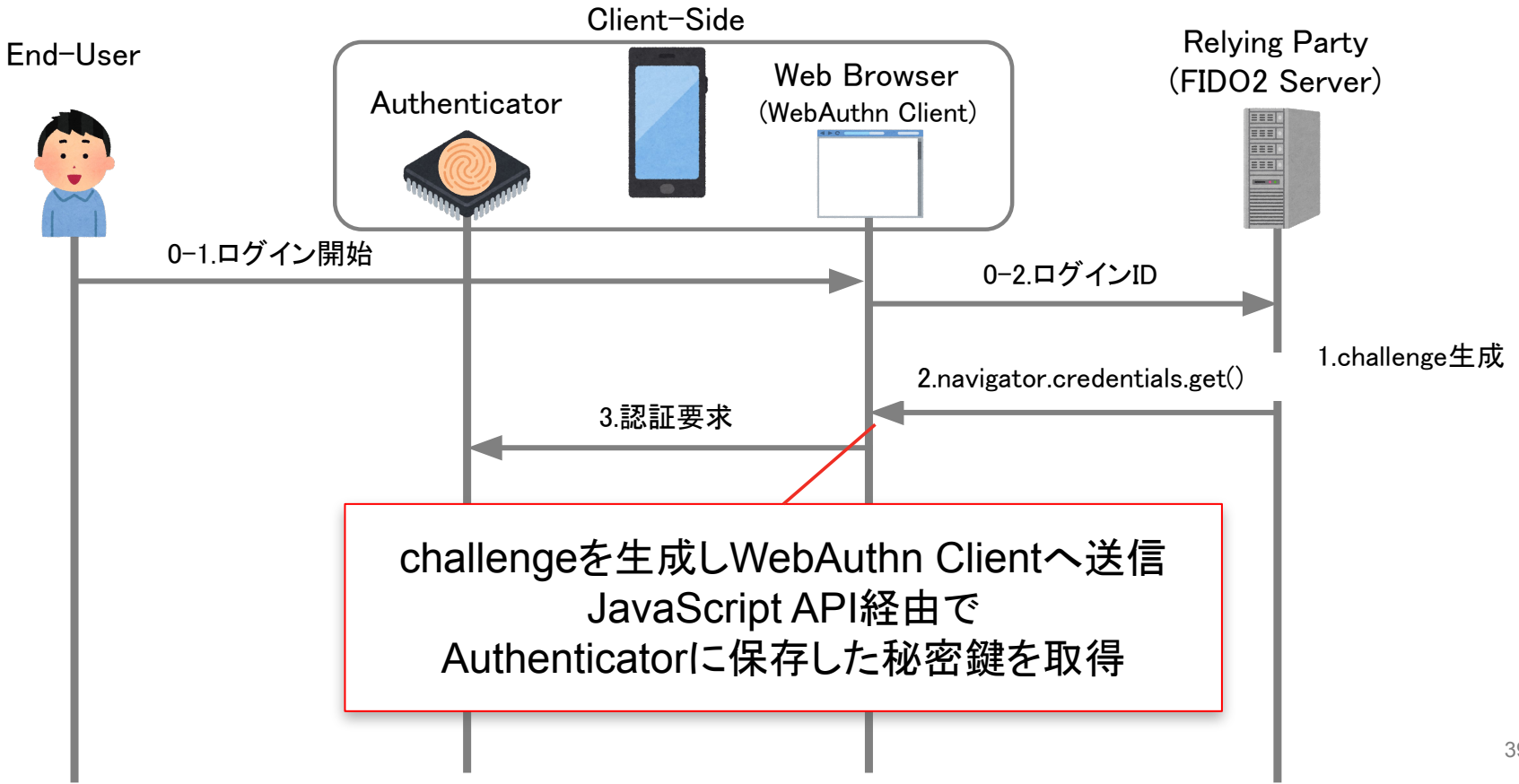
フォームオートフィル方式

- パスワードログインのフォームのオートフィル機能にアカウントを表示し認証する

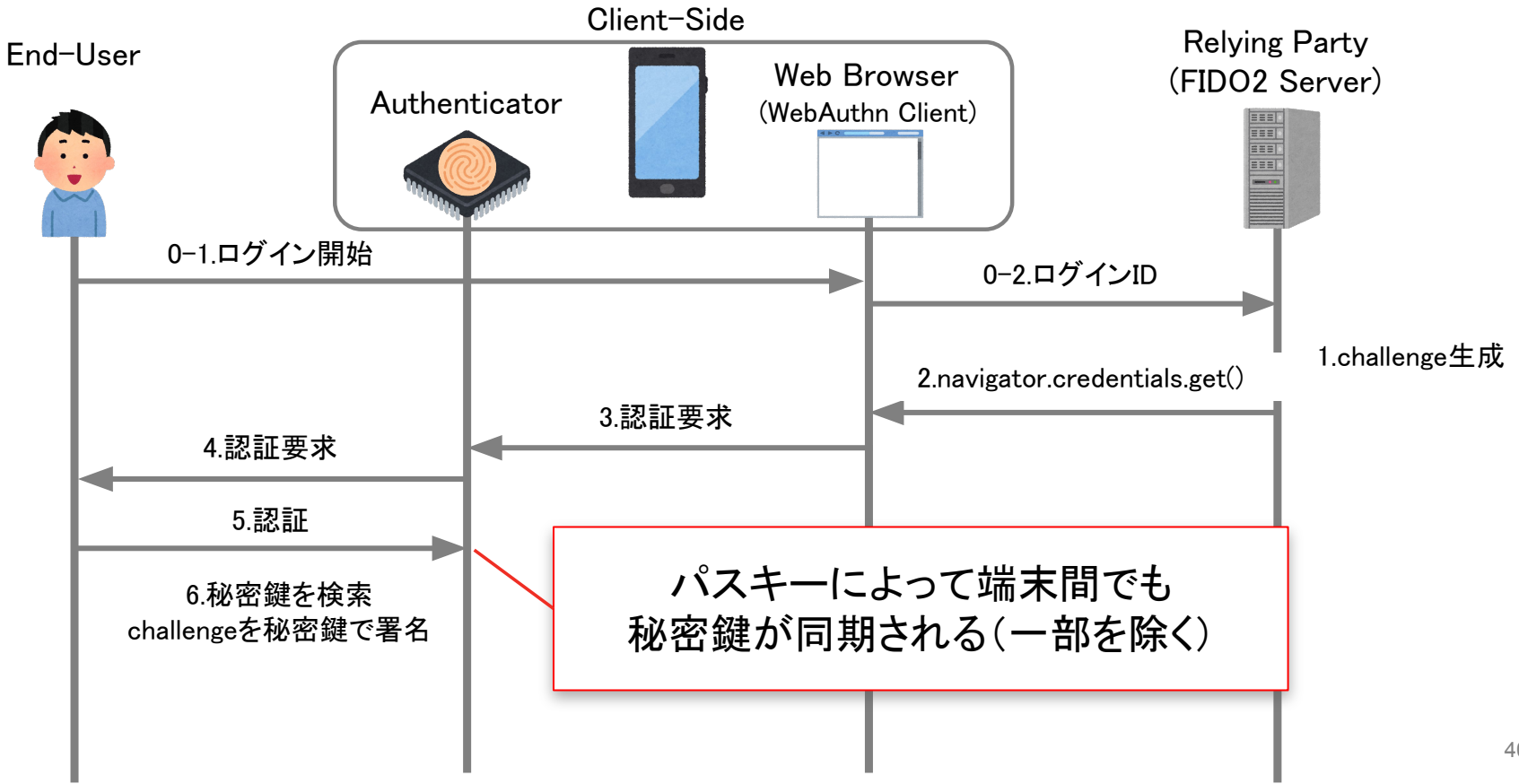
パスキー認証フロー


Client-Side
End-User
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
登録しているログインIDを
指定して認証を開始

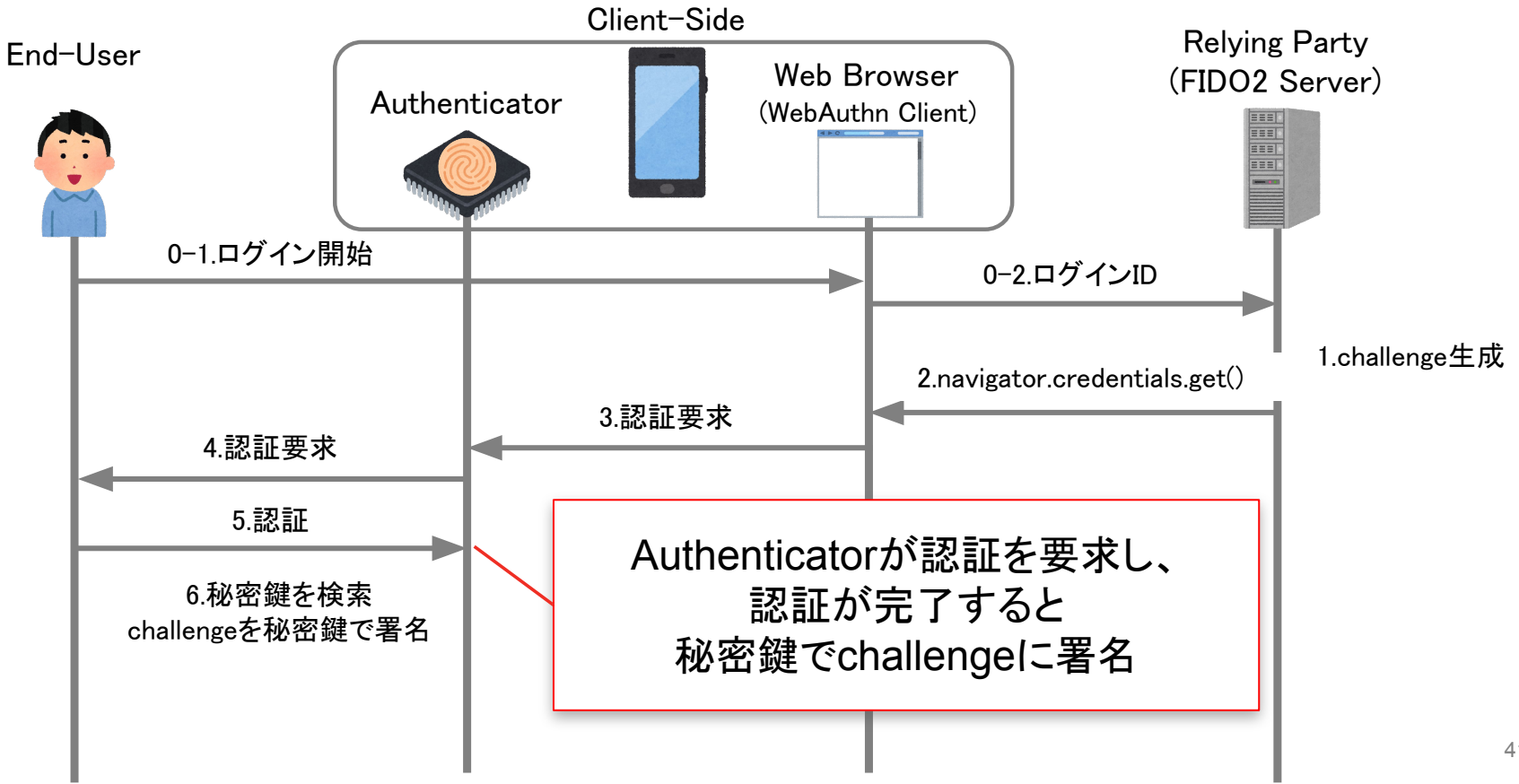
パスキー認証フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
1.challenge生成
2.navigator.credentials.get()
3.認証要求
challengeを生成しWebAuthn Clientへ送信
JavaScript API経由で
Authenticatorに保存した秘密鍵を取得

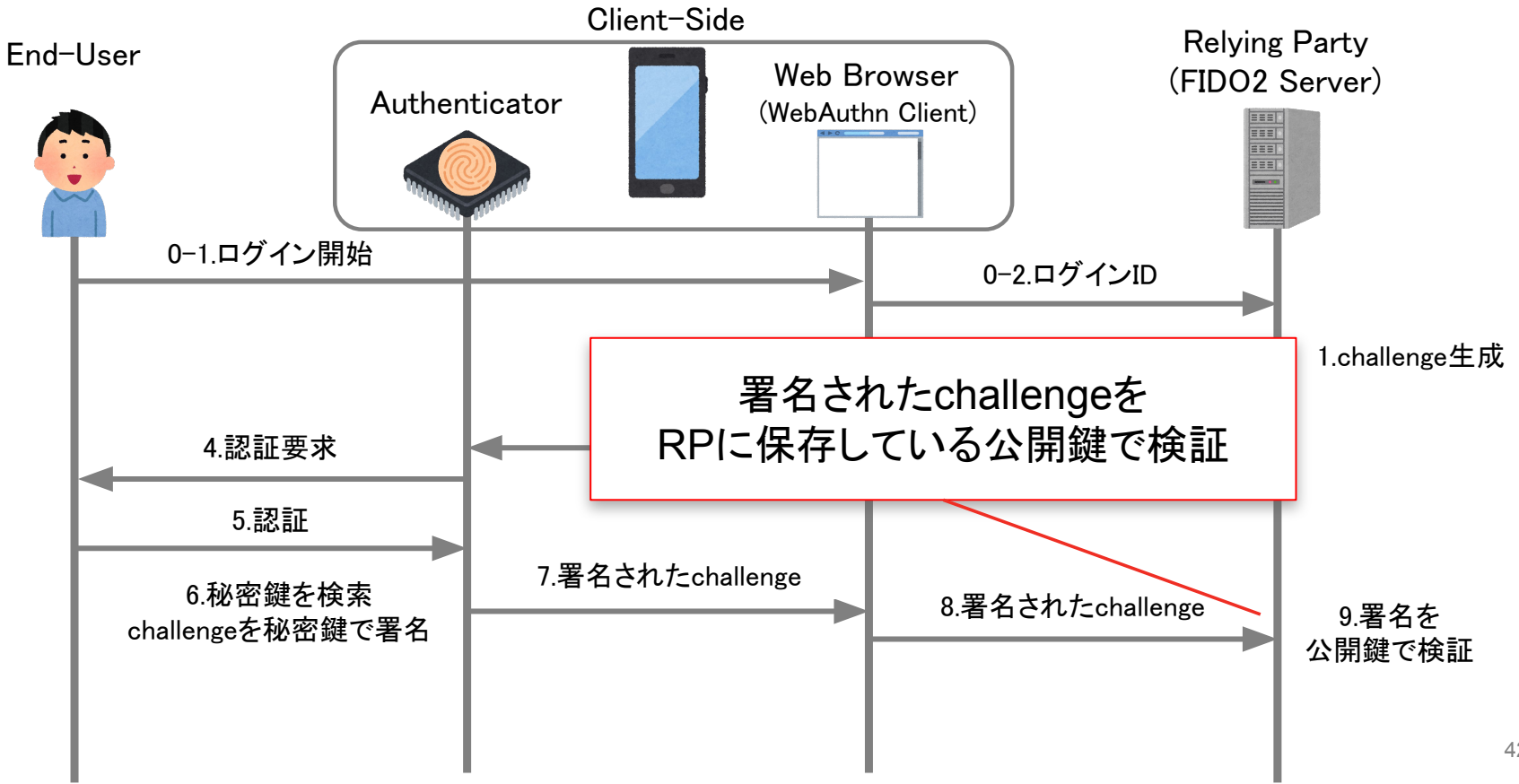
パスキー認証フロー


Client-Side
End-User
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
1.challenge生成
2.navigator.credentials.get()
3.認証要求
4.認証要求
5.認証
6.秘密鍵を検索
challengeを秘密鍵で署名
パスキーによって端末間でも
秘密鍵が同期される(一部を除く)

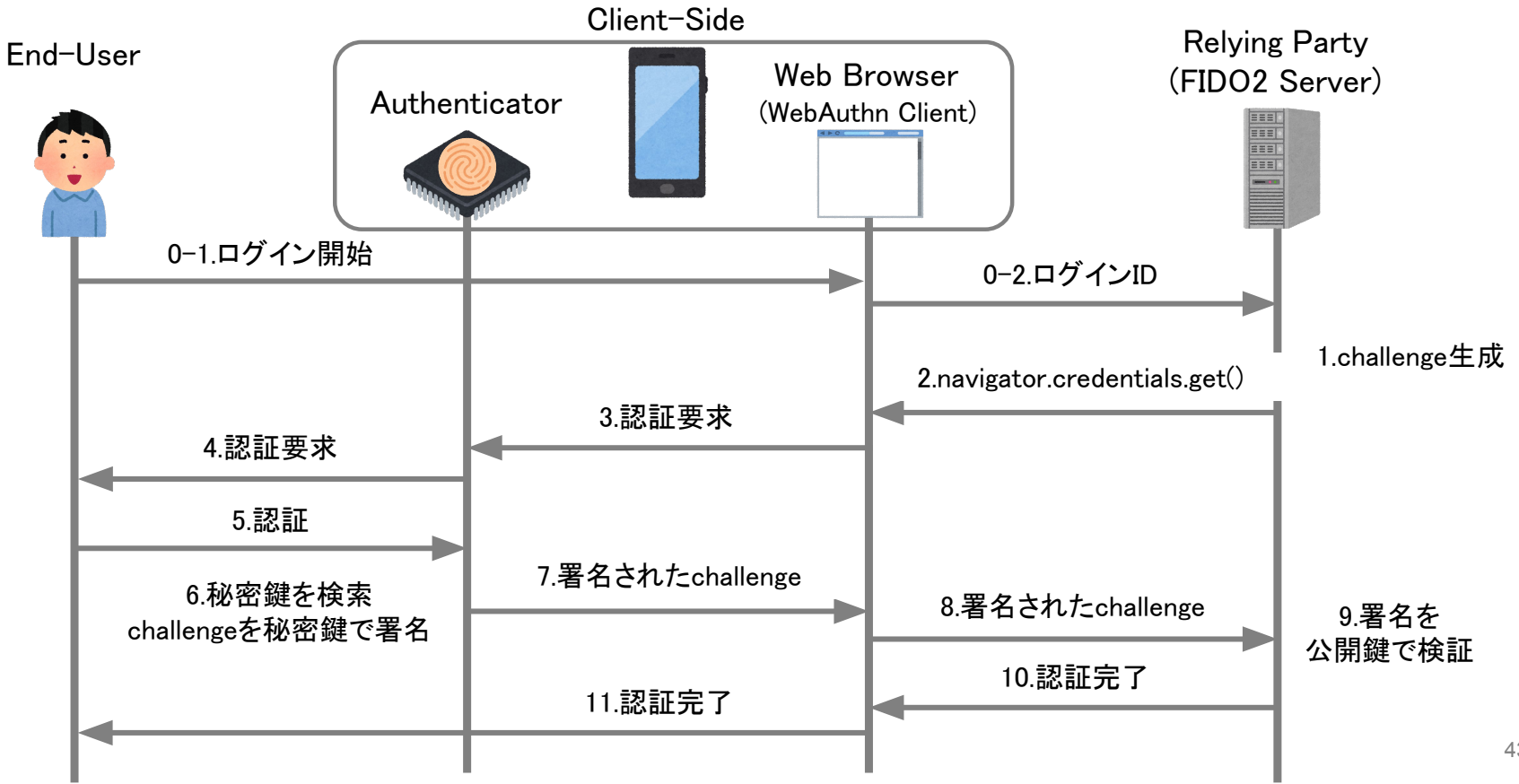
パスキー認証フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
1.challenge生成
2.navigator.credentials.get()
3.認証要求
4.認証要求
5.認証
6.秘密鍵を検索
challengeを秘密鍵で署名
Authenticatorが認証を要求し、
認証が完了すると
秘密鍵でchallengeに署名

パスキー認証フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
1.challenge生成
署名されたchallengeを
RPに保存している公開鍵で検証
4.認証要求
5.認証
6.秘密鍵を検索
challengeを秘密鍵で署名
7.署名されたchallenge
8.署名されたchallenge
9.署名を
公開鍵で検証

パスキー認証フロー


End-User
Client-Side
Authenticator
Web Browser
(WebAuthn Client)
Relying Party
(FIDO2 Server)
0-1.ログイン開始
0-2.ログインID
1.challenge生成
2.navigator.credentials.get()
3.認証要求
4.認証要求
5.認証
6.秘密鍵を検索
challengeを秘密鍵で署名
7.署名されたchallenge
8.署名されたchallenge
9.署名を
公開鍵で検証
10.認証完了
11.認証完了

パスキーのよくある疑問・誤解

同期しないパスキーの方が安全なのでは？

- 同期するパスキーと同期しないパスキーの2種類がある
  - 同期しないパスキーは認証器の仕様に依存するため、パスキーが作成できない場合もある
- 同期しないパスキーであれば、セキュリティキーなどを物理的に窃取されない限りはリモート攻撃は不可能
- 同期パスキーよりも同期しないパスキーの方が安全ではある
- 一方で、同期しないパスキーを登録した認証器に依存するため、ログインやアカウントリカバリーの観点でUXが低下することを考慮しなければいけない

パスワードマネージャーのアカウントが乗っ取られたら？

- パスワードマネージャーが乗っ取られたらパスキーが一網打尽になる可能性はある
- パスワードマネージャーの仕様にもよるが、Googleパスワードマネージャーでは、デバイスのPINまたは専用のPINの登録が必須であり、パスキーの暗号化に用いられている
- パスワードマネージャーのアカウントが乗っ取られても、PINで復号されるまでにパスキーを無効化するなどの対策を講じることで被害を最小化することはできる

パスキーにアクセスできなくなったら？

- 同期するパスキーであっても、パスワードマネージャーが使えないブラウザーや同期できないOSの場合には、パスキーにアクセスできないことがある
- 導入サービス（Relying Party）はパスキー以外の認証方法やアカウントリカバリーを用意しておく必要がある

	Windows	macOS	iOS/iPadOS	Android	Linux	ChromeOS
Googleパスワードマネージャー	🔄*1 *2	🔄*1	🔄	🔄	🔄*1	🔄*1
Appleパスワード		🔄	🔄			
Windows Hello	✅					
3rd Partyパスワードマネージャー	🔄*3	🔄*3	🔄	🔄	🔄*3	🔄*3

*1 Chromeのみ *2 要TPM *3 拡張機能として

パスキーの導入・普及・ IDaaS対応状況

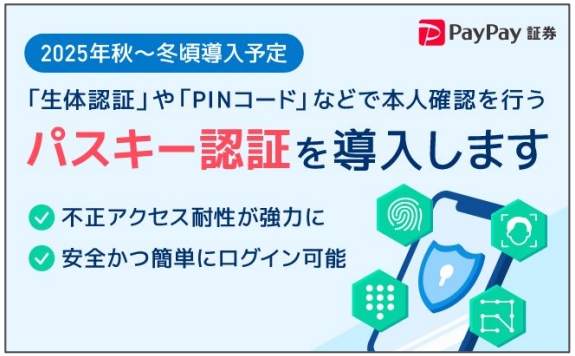
証券各社の導入状況

- フィッシング攻撃による証券口座乗っ取りを受けて、今年に入って証券各社の導入が相次いでいる

楽天証券

https://www.rakuten-sec.co.jp/web/info/info20250718-02.html

PayPay証券



https://www.paypay-sec.co.jp/notice/20250829_1.html

SBI証券

https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=none&dir=service&file=home_security_fido2.html

コンシューマーサービスの普及状況

- 国内外はじめ多くのコンシューマーサービスでパスワードなどの既存の認証手段からパスキーへの移行が進んでいる（2024年12月時点）

Google

8億のアカウントがパスキーを使用

LINEヤフー

Yahoo!のアクティブ**2,700万人**スマフォの**50%**がパスキーを利用

KDDI

au IDのFIDO認証を**1,300万人**が利用

NTT docomo

パスキーによるdアカウント認証が**50%**到達

Amazon

1億7,500万人のパスキー登録

メルカリ

パスキー登録者数が**700万人**

東急

TOKYU IDユーザーの**45%**がパスキーを所有

引用：2024年にパスキーの導入が倍増　150億を超えるオンラインアカウントでパスキーによる迅速で安全なサインインが可能に
https://fidoalliance.org/passkey-adoption-doubles-in-2024-more-than-15-billion-online-accounts-can-leverage-passkeys/?lang=ja

IDaaSのパスキー対応状況

- 主要なIDaaSにおいても従業員認証（Workforce Identity）および顧客認証（Customer Identity and Access Management: CIAM）の両方、またはそのいずれかでパスキーを活用するための機能を提供している。

提供企業	サービス	IDaaSの種類
Microsoft	Microsoft Intra ID（旧Azure AD）	Workforce / CIAM
Okta	Okta Identity Cloud	Workforce / CIAM
	Auth0 (現 Okta Customer Identity Cloud)	CIAM
Google	Google Workspace	Workforce

提供企業	サービス	IDaaSの種類
Amazon (AWS)	Amazon Cognito	CIAM
Ping Identity	Ping Identity Platform	Workforce / CIAM
ForgeRock	ForgeRock Identity Platform	Workforce / CIAM

エクスジェンネットワークス：国産DaaS「Extic」
https://www.exgen.co.jp/extic/function-auth.html

EXGEN NETWORKS

製品情報 ソリューション コラム 資料ダウンロード セミナー・イベント お知らせ サポート 会社情報 お問い合わせ

Trusted Identity Center
eXTIC

認証機能

サービス概要 | 認証機能 | ID管理機能 | 仕様 | 導入事例 | 価格 | 無料トライアル | 利用規約

業務効率を向上させるSSO、安全で簡単なパスキー（FIDO2）認証など利便性とセキュリティを高める認証機能を備えています。

Extic資料ダウンロード

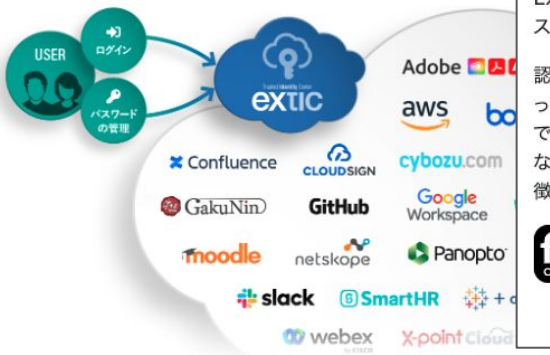
SSO機能

国内でよく利用されるクラウドサービスを中心に、多くのクラウドサービスに対してSAML2.0によるシングルサインオンを行えます。

また、我が国の学術認証フェデレーションである「学認（GakuNin）」を介して、世界各国との学術認証連携が可能になる「eduGAIN」にも対応しています。

※学認で使用するIdP証明書はUPKI証明書を推奨しています。UPKI証明書以外の証明書をご利用になりたい場合は、弊社営業までご相談ください。

連携システム一覧



パスキー（FIDO2）に対応

パスキー対応のセキュリティキーや、普段ご利用の認証器（Windows Hello、Apple Touch IDなど）をExticに登録することで、パスワードレスによる認証が行えます。

認証器として顔認証や指紋認証といった生体認証デバイスを用いることで本人性をさらに高めることができ、なりすまし攻撃にも強いといった特徴があります。

fido CERTIFIED FIDO2

まとめ

まとめ

- 従来のパスワードリスト攻撃に加えて、証券各社を中心にフィッシング攻撃の被害が相次いでいる
- ユーザーによるクレデンシャル情報の入力を不要とするパスキーであればフィッシング攻撃にも耐え、同時にUXも優れている
- パスキーにはクレデンシャルをクラウド間で同期する機能もあり（一部のケースを除く）、複数デバイス間でパスキーによる認証が可能
- コンシューマー、エンタープライズにおいてパスキーの導入・普及が進んでいる

「パスキーのすべて」の概要

紙版・電子版絶賛発売中

「パスキー」はパスワードレス認証を実現する認証技術です。

本書では、開発者はもちろん、企画職やデザイン職、セキュリティ担当などの認証に携わる方々に向けた内容になっています。

- 従来の認証技術の課題と比較して何が優れているのか
- パスキーの導入で知っておくべき特性
- パスキーの登録・認証・管理画面などのUX設計
- WebサイトだけでなくiOSやAndroidの具体的な実装
- パスキーが登場する以前の歴史から最新の仕様までの解説
- 読者の疑問や質問に答えるコラムも充実

本書についての詳細はこちら

本書の構成

第1章　パスキー導入が求められる背景
── 既存の認証方法とパスキーの背景を知ろう

第2章　パスキーを理解する
── パスキーの特徴や利点を理解しよう

第3章　パスキーのユーザー体験
── パスキーの体験をイメージしよう

第4章　サポート環境
── ユーザーの環境ごとに利用できる機能を確認しよう

第5章　パスキーの UXを実装する
── UXの実現に必要なメソッドやパラメータを知ろう

第6章　WebAuthn APIリファレンス
── クライアントとサーバの実装の詳細を確認しよう

第7章　スマホアプリ向けの実装
── AndroidとiOSにおける実装を確認しよう

第8章　パスキーのより高度な使い方
── より効果的な活用とUX向上方法を知ろう

第9章　パスキー周辺のエコシステム
── 標準化の流れや開発者向け情報を確認しよう

付録A　クライアント用 Extensionの解説
── 後方互換や先進的な活用のための拡張機能をみてみよう

付録B　iOS実装サンプル
── サンプルアプリを動かしてみよう

本書についての詳細はこちら

コラム一覧

第1章

- NIST SP 800-63
- 公開鍵暗号をざっくりと理解する

第2章

- ディスカバラブルでないクレデンシャル
- パスキーは多要素認証ではない場合もあるのでは？
- アカウントのライフサイクルとパスキーの関係性

第3章

- パスキーの他人との共有
- クロスデバイス認証のしくみ

第5章

- PINを使わず，生体認証だけでパスキーを利用できるようにすることはできますか？

第6章

- パスキーの同期を禁止する方法はある？

第7章

- アプリで利用している生体認証とパスキーは何が違うの？

パスキーを使って便利で安全なログイン体験

パスワードに代わる次世代認証技術「パスキー」を徹底解説！

最新WebAuthn Level 3仕様をカバーし、
実装の解説はもちろんのこと、
皆さんの疑問にお応えするコラムも充実。

パスキーとアプリの生体認証の違いは？
パスキーは多要素認証なのか？

ぜひ本書で確認してください。

パスキーのすべて
——導入・UX設計・実装

本日ご紹介できなかったパスキーの特性や
よくある疑問・誤解の答えも盛りだくさんです
続きはぜひ本書でご確認ください

パスワードに悩む方々の手助けになれば幸いです
ご清聴ありがとうございました

EOP