FIDO認証と公開鍵暗号

ヤフー株式会社
Yahoo! JAPAN 研究所 上席研究員
五味 秀仁

内容

- FIDOアライアンス概要
- FIDO認証
- FIDO認証を用いた応用ソリューション

FIDOアライアンス概要

FIDOアライアンスとは

- オンライン・サービス利用時にパスワードに代わるシンプルで堅牢な認証を実現するための業界団体。
- 経緯
  - 2012年2月に6社で発足。
  - 2017年3月現在、全世界で250以上の組織・団体が参加するまでに拡大。
- 参加団体
  - 金融機関、ネット事業者、セキュリティベンダー、スマートフォン、PC製造事業者、および、政府機関など多種多様に渡る。
- 日本企業
  - ボード：NTTドコモ
  - スポンサー：大日本印刷、DDS、富士通、ISR、三菱東京UFJ銀行、楽天、シグマクシス、ソフト技研、ヤフー・ジャパン

FIDOアライアンスのミッション

1. 技術仕様の策定
   - 次世代の認証技術に関する標準化を目指し、認証サーバーや利用者の端末のソフトウェア一式で技術仕様を策定しています。ただし、FIDO自体は、特定の製品やサービスを開発しません。
2. 適合性認定プログラムの実施
   - FIDOアライアンスで策定した技術仕様を実装した製品やサービスの普及のために、個々の実装の仕様への適合性、および、他の実装との相互接続性を検証する試験を実施しています。
3. 標準化団体への提案
   - 上記FIDO技術をより多くの利用者の方々に利用していただくために、適切な標準化団体とリエゾン関係を構築して相互に連携しながら、標準技術として普及させていくことを目指しています。

FIDOアライアンスの目指す認証とは

パスワードの課題

利便性（Usability）	安全性（Security）
覚えられない	**再利用可能**
入力不便	**漏えいしやすい**

パスワードへの依存度を減らしつつ、利便性と安全性の両面を向上させる

FIDO認証

認証に関する潮流

高性能なセンサーと安全なデータ保管技術による新しい認証形態（モデル）の出現

- **ローカル認証**: ユーザーの検証を保有しているデバイスで実施。
- **継続的認証**: ユーザーの行動情報を絶えず取得し、認証に活用。
- **暗黙的認証**: 認証のための明示的な操作（タッチ操作やジェスチャーなど）なしに認証が完了。
- **コンテキスト認証**: ユーザーが存在するコンテキストに関わる情報を活用して認証。

ユーザーコンテキストからのデータ

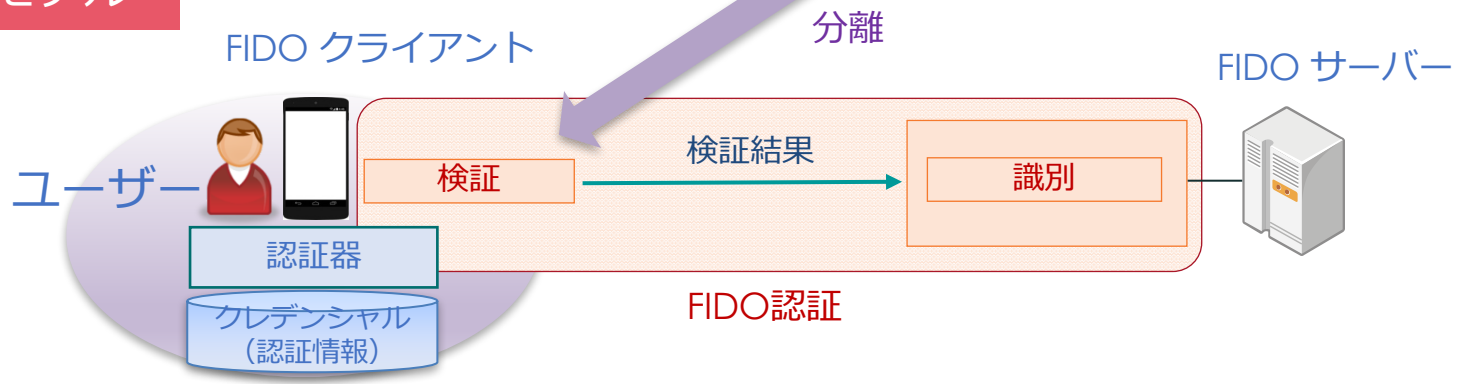
- 位置
- 方角
- 温度
- 音
- 加速度
- 歩数
- 歩行距離
- 他

正確でリアルタイムのコンテキストデータを活用することで、認証のあり方に変化が起こっている。

認証モデルの違い：ローカル vs. リモート

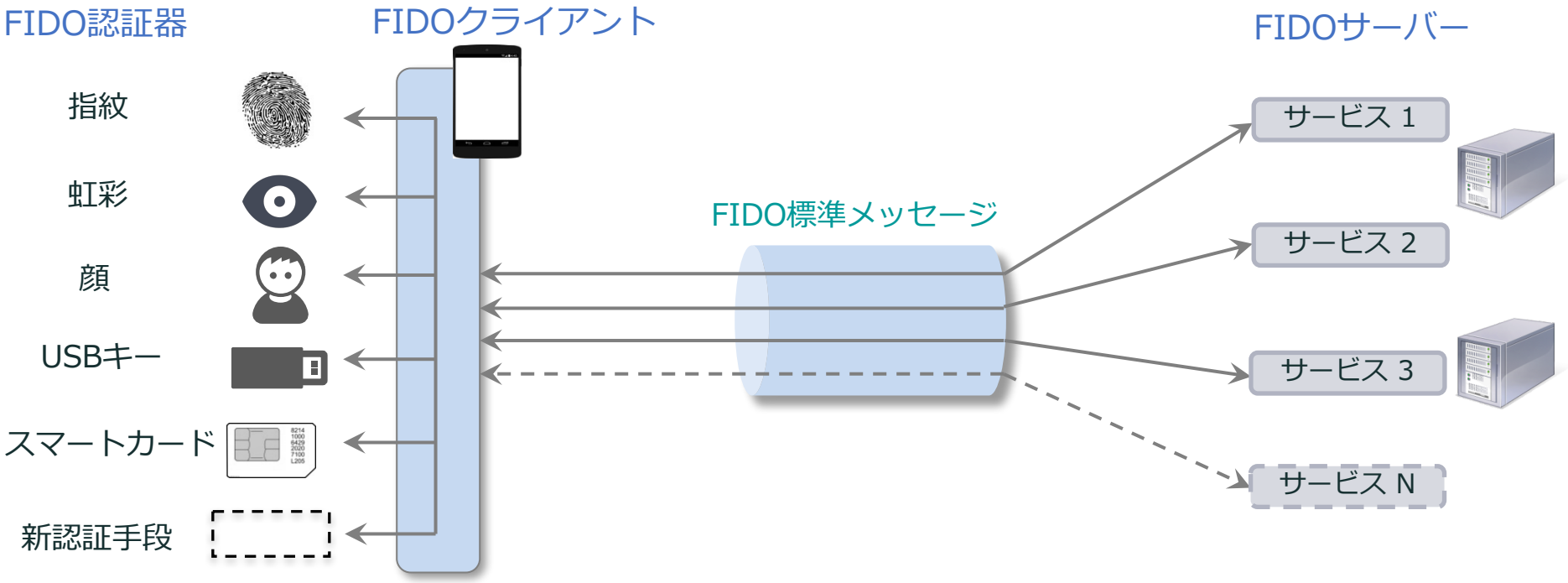
従来的な認証モデル （パスワードなど）

FIDO 認証モデル



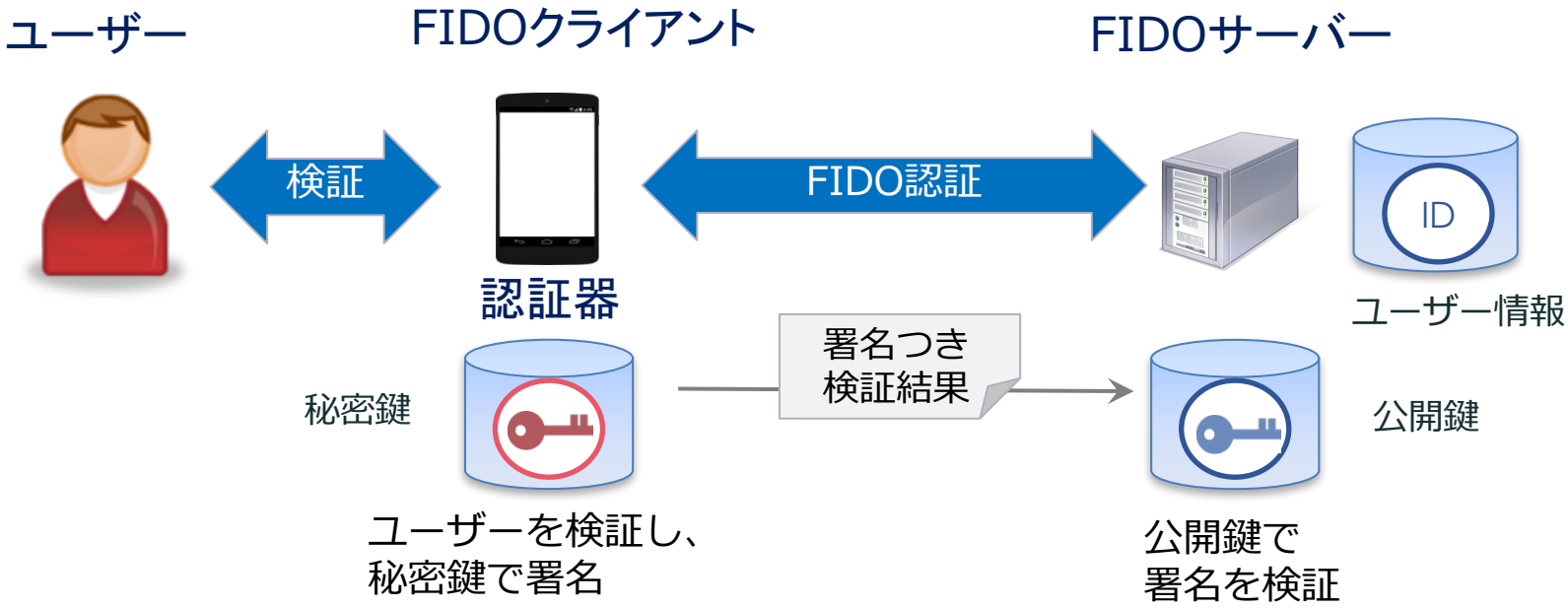
*認証器: 英語では Authenticator

FIDO認証のコンセプト：認証の部品化



認証器が「部品」として組み込まれ、認証のスケーラビリティ（拡張性）が向上

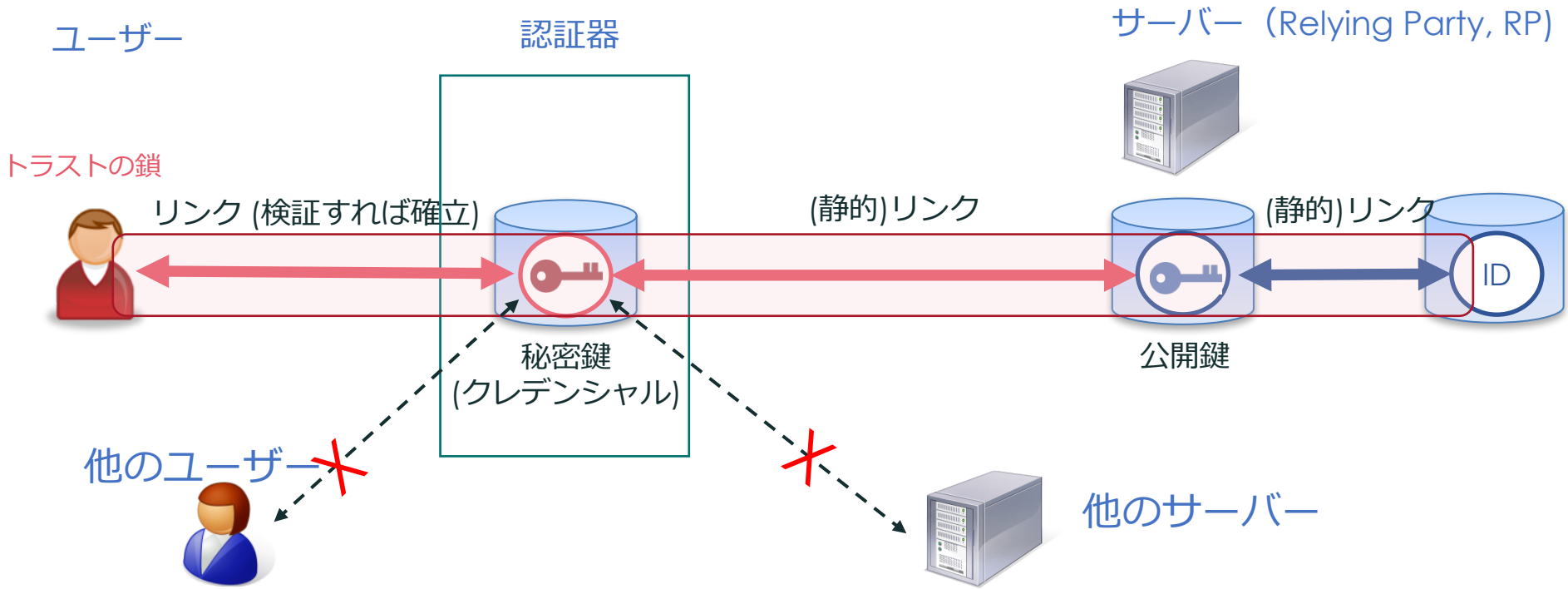
FIDO認証の技術：公開鍵暗号方式を利用



ユーザーが適切な秘密鍵を保有することを確認（検証）することによって認証を実現

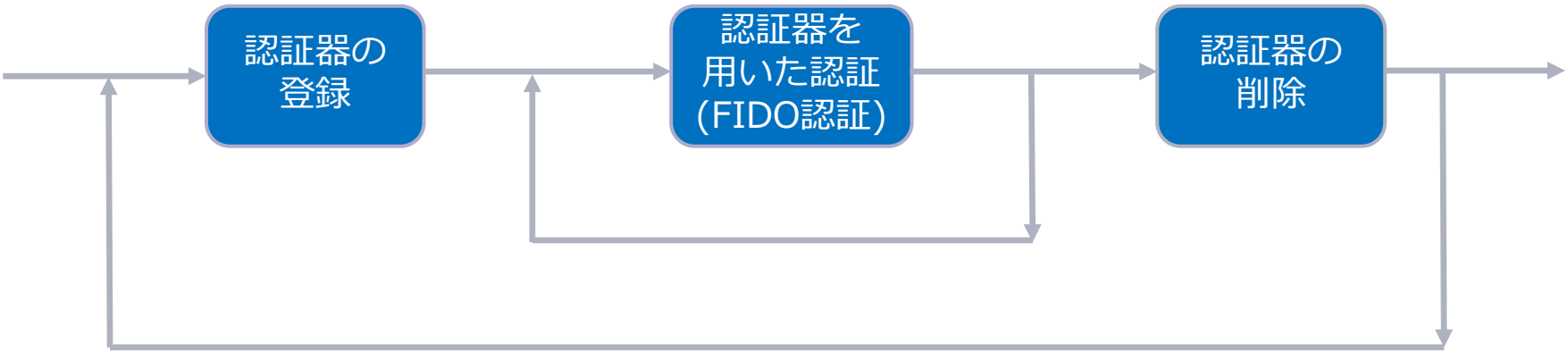
FIDO認証におけるトラスト関係

ユーザー・認証器・サーバー間にトラスト（信頼）を構築



FIDO認証における処理

FIDO認証のための前処理
最初に一度だけ実施

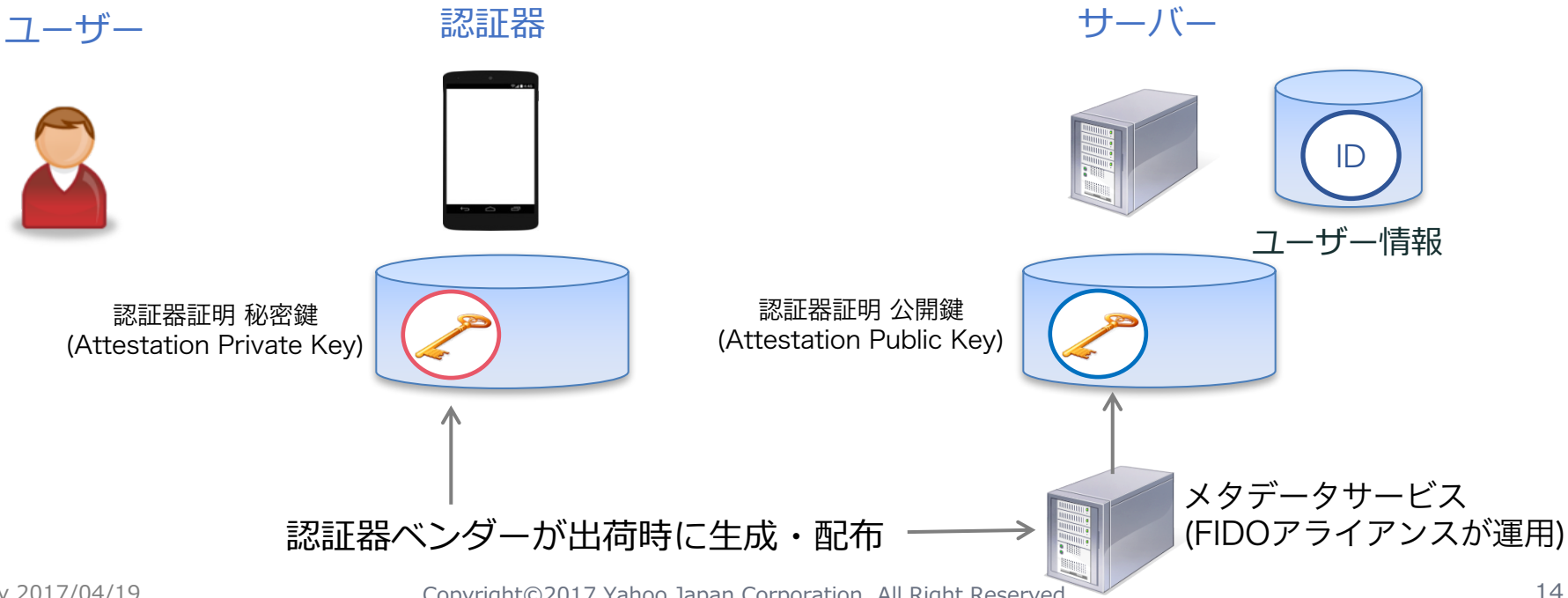


（注：ユーザー、認証器ごとに上記処理を繰り返すことになる。）

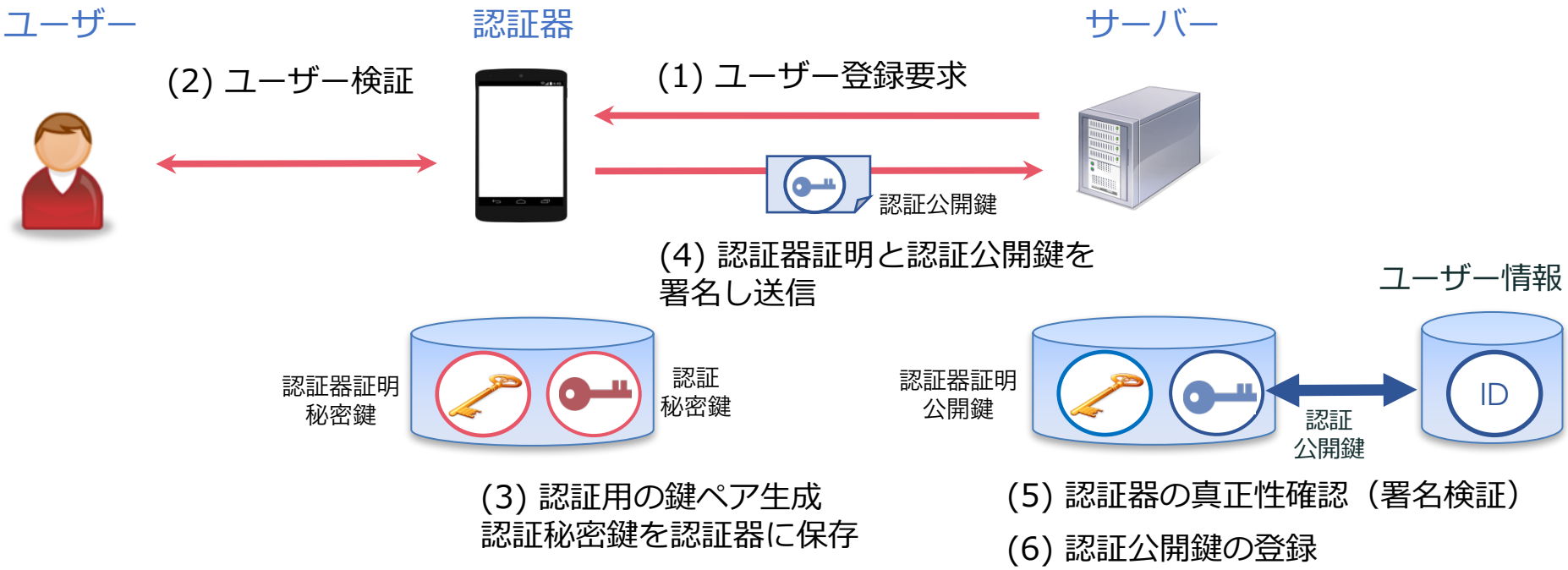
認証器の登録

認証器が適切な実装を有した本物であることを確認し、FIDO認証のための鍵を設定。

登録前の状態

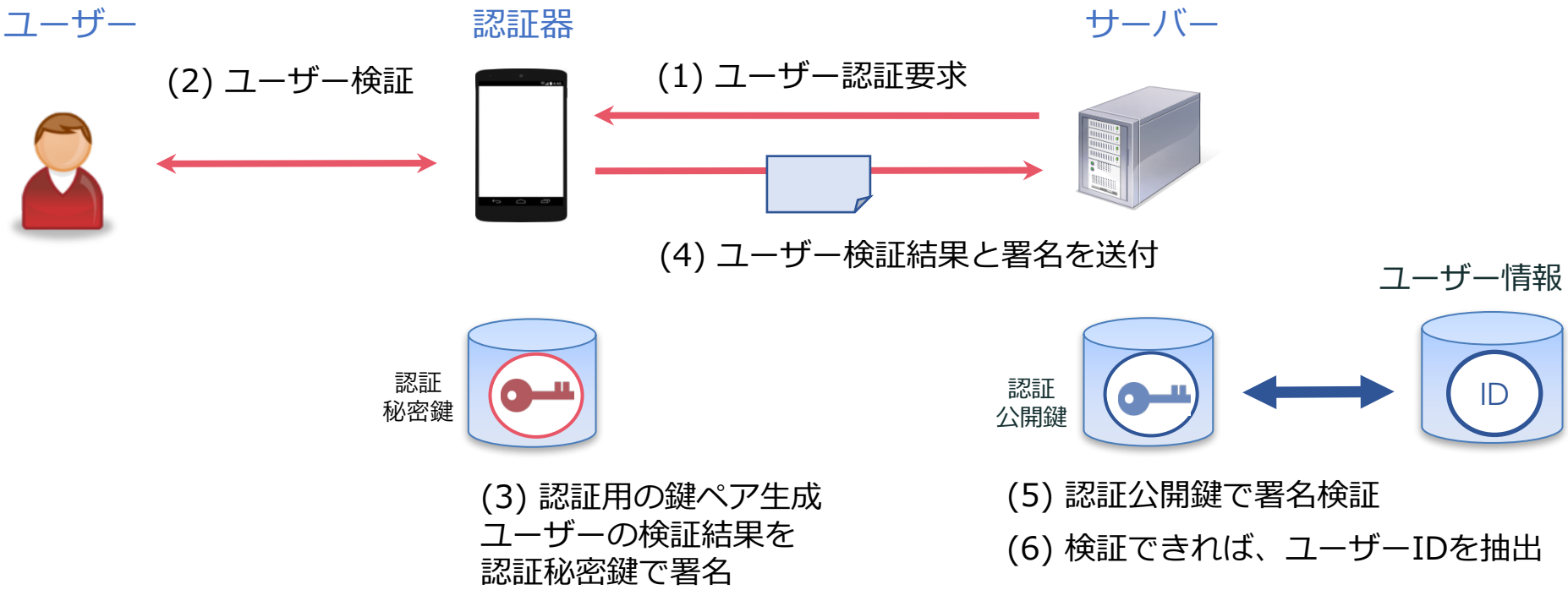


認証器の登録処理



認証器を用いた認証（FIDO認証）

先の登録処理にて認証用鍵の登録が前提



FIDO認証の技術仕様

パスワードレス型: UAF (Universal Authentication Framework) 1.1

- スマホ端末備え付けの認証器で、生体・所持認証（パスワードなし）

パスワード補完型: U2F (Universal 2nd Factor) 1.1

- 主要ブラウザでの、パスワード認証 + セキュリティキーなどの所持認証
  (USB、Bluetooth、NFC対応)

(出典: FIDOアライアンス)

新技術仕様：FIDO 2

Web 認証API仕様:

- Webブラウザーが JavaScriptを用いてクレデンシャル（秘密鍵）にアクセスするためのAPI。
- FIDOアライアンスが提案、ブラウザでの普及のため、標準化団体W3Cにて策定中。

デバイス間連携仕様: CTAP (Client To Authenticator Protocol)

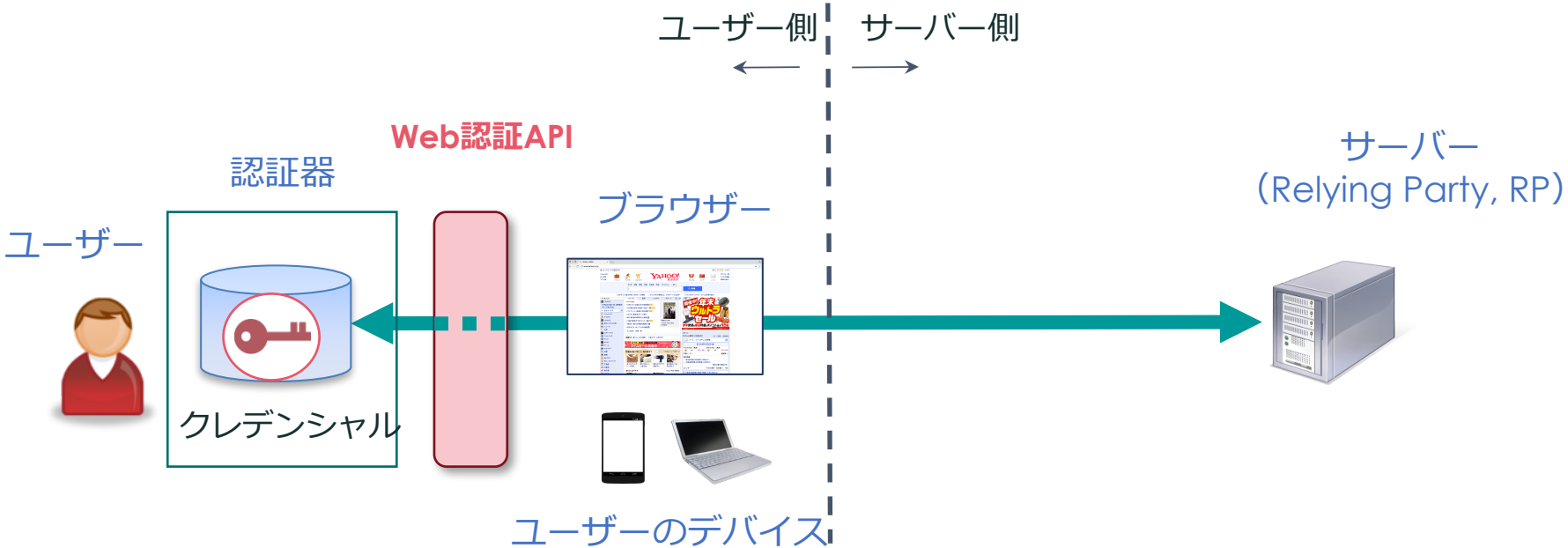
- クライアントと外部認証器間の通信をサポートする認証プロトコル。
- FIDOアライアンスにて策定中。

*API: Application Programming Interface

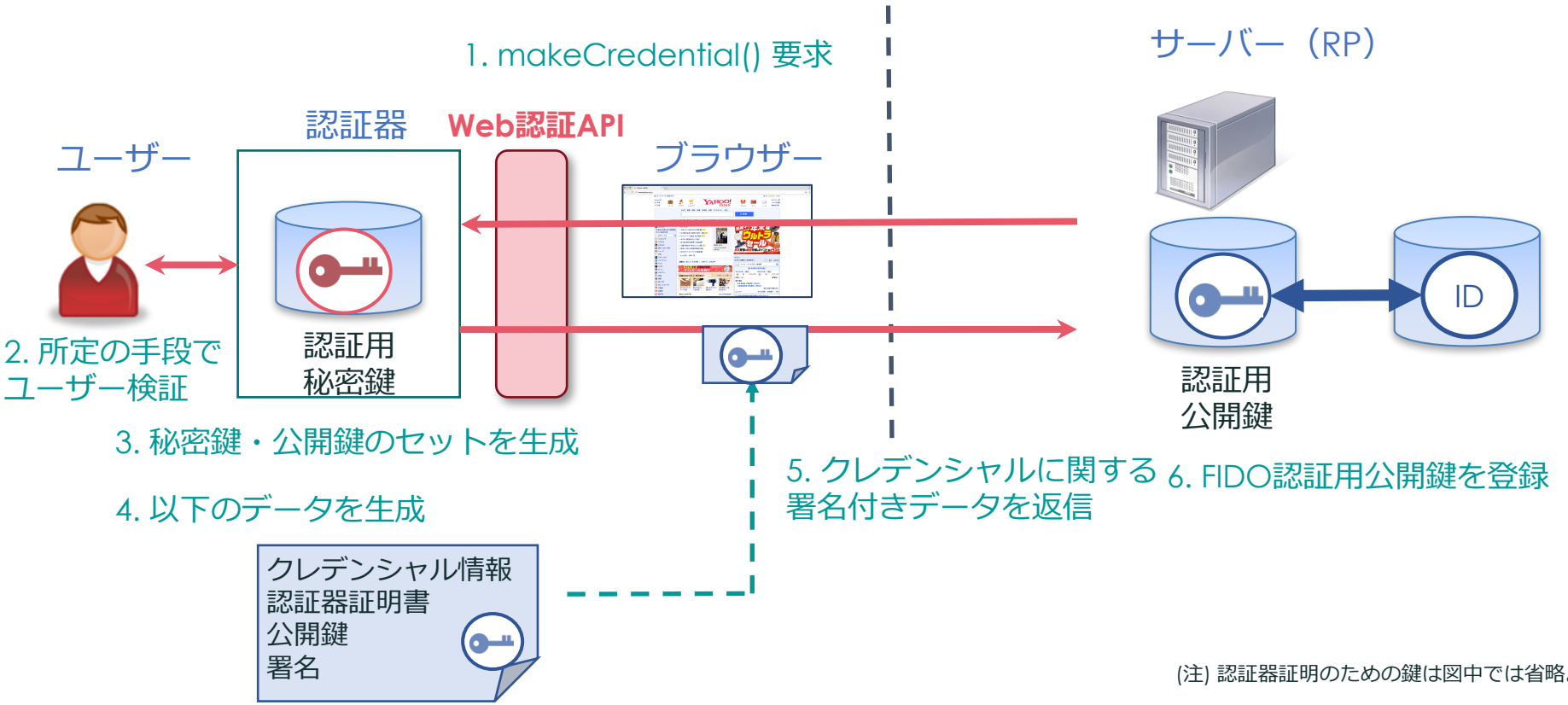
Web認証API

ブラウザーがJavascriptを用いてクレデンシャルにアクセスするための抽象的API

- makeCredential()
- getAssertion()

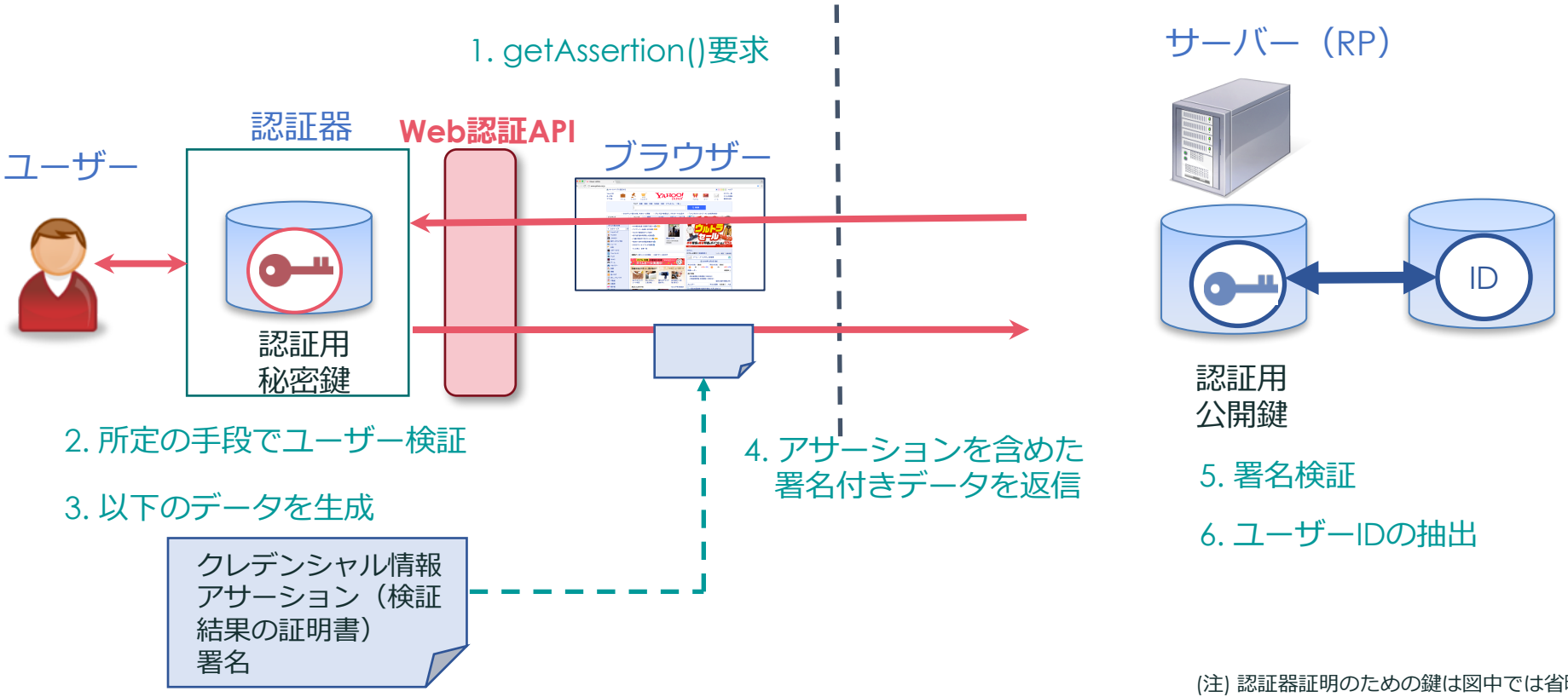


Web認証における認証器の登録



(注) 認証器証明のための鍵は図中では省略。

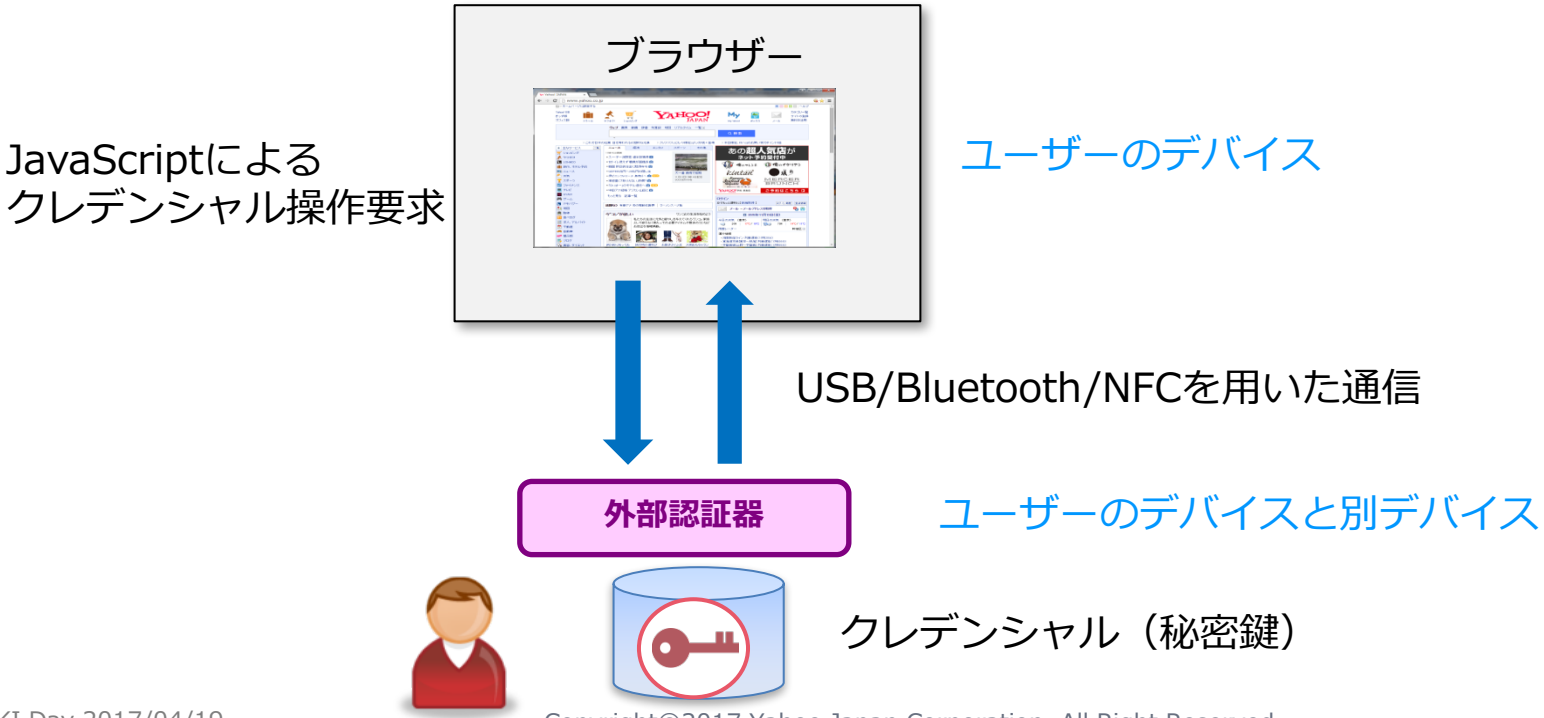
認証器を用いたWeb認証



(注) 認証器証明のための鍵は図中では省略。

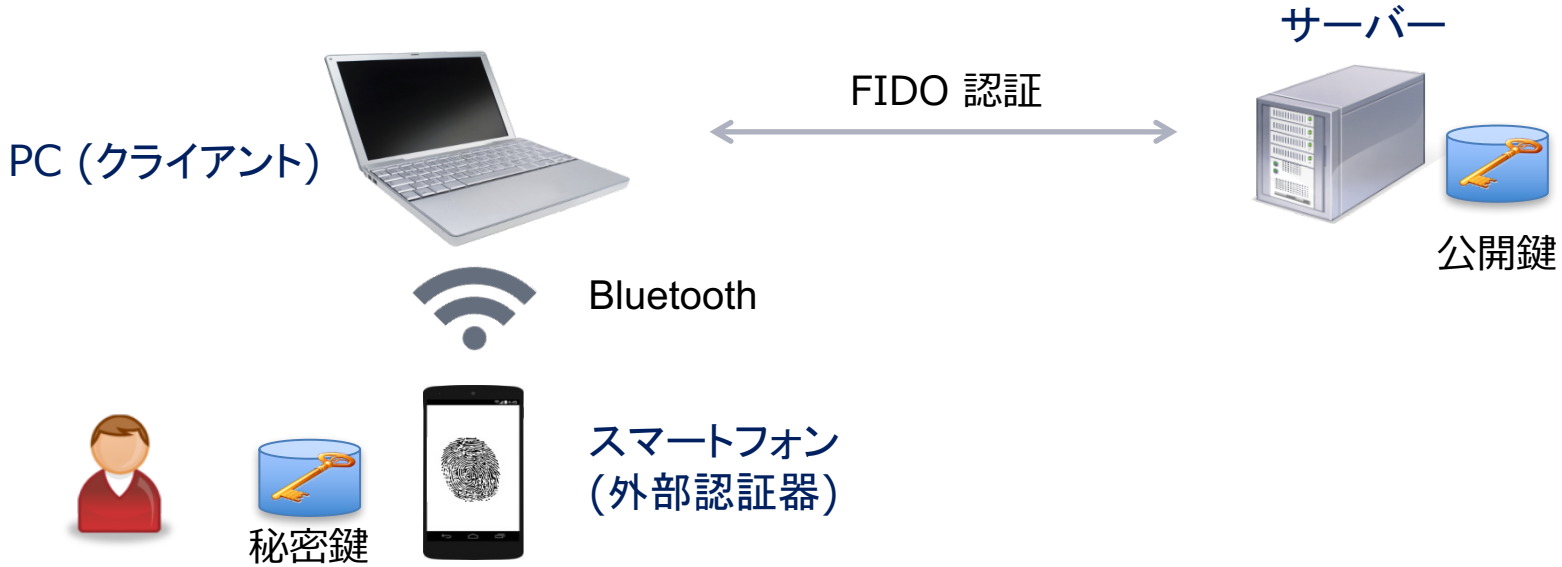
CTAP (Client To Authenticator Protocol)

- 外部認証器とクライアント・プラットフォーム間の通信プロトコルを規定。



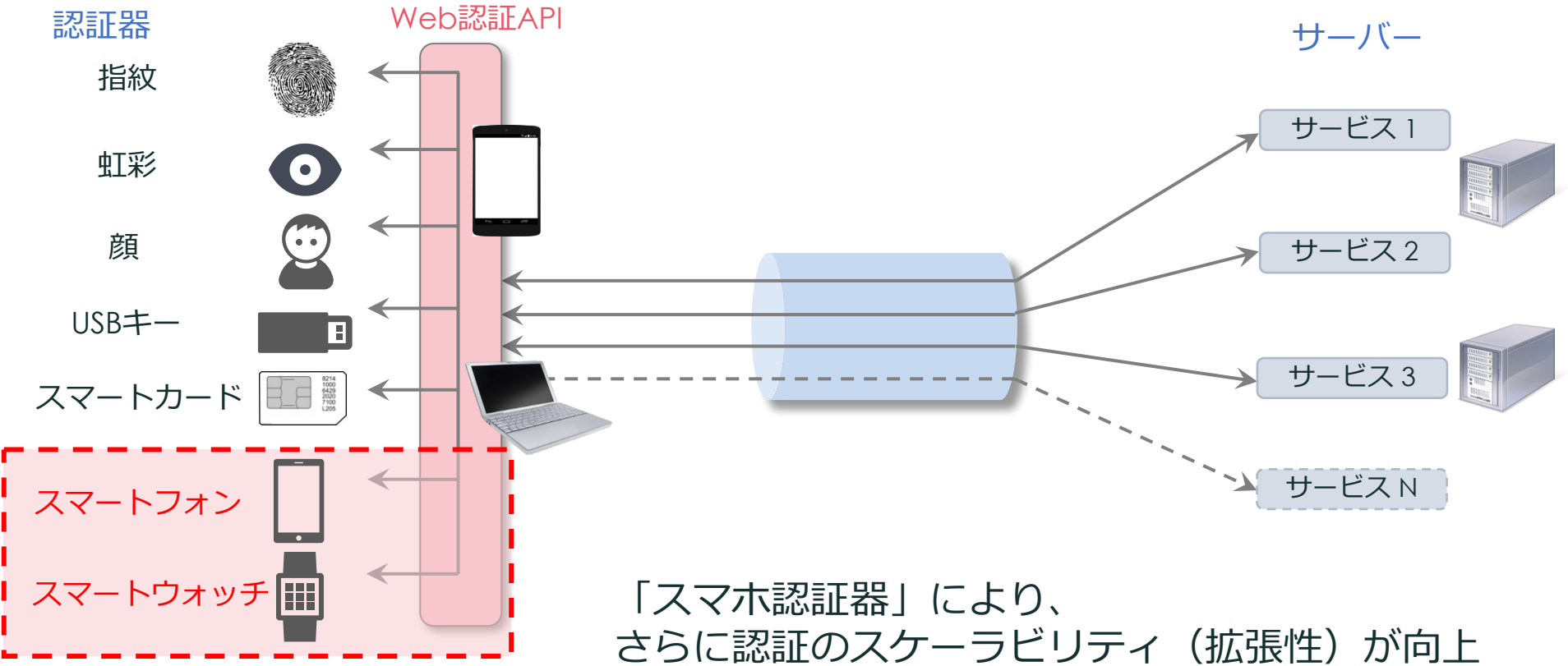
CTAP のユースケース

（例）PC上のアプリケーション利用時の認証を、スマートフォンで行う。



ユーザーは、自らの保有するデバイスを認証器として用い、デバイスをまたがって認証できる。（特定のデバイスに認証機能を集約させることができる。）

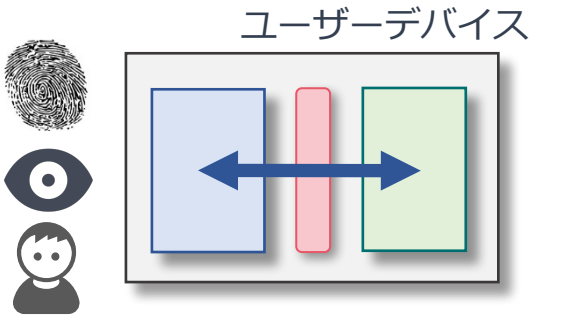
スマートフォンも一つの認証器に



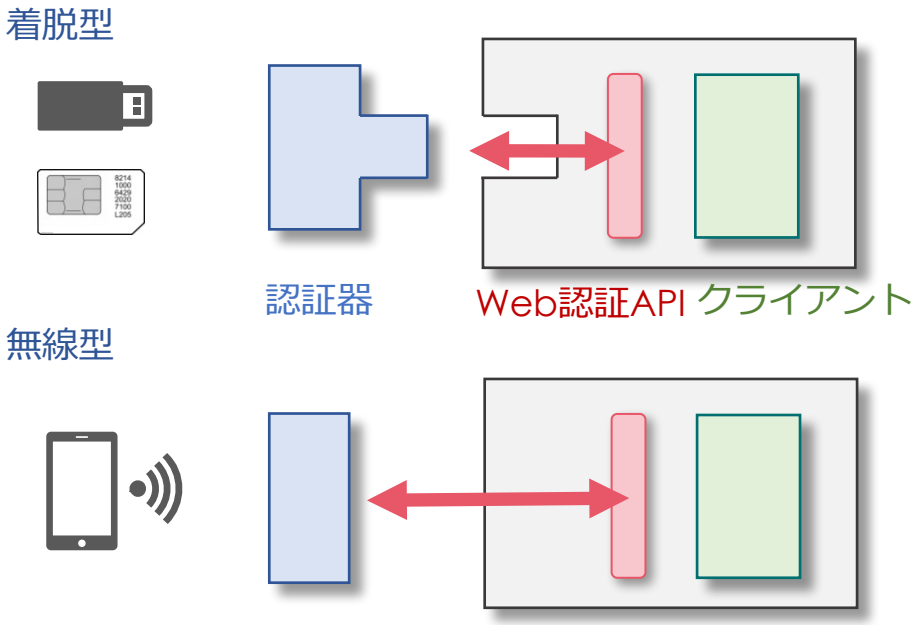
「スマホ認証器」により、
さらに認証のスケーラビリティ（拡張性）が向上

認証器のバリエーション

内蔵認証器



外部認証器

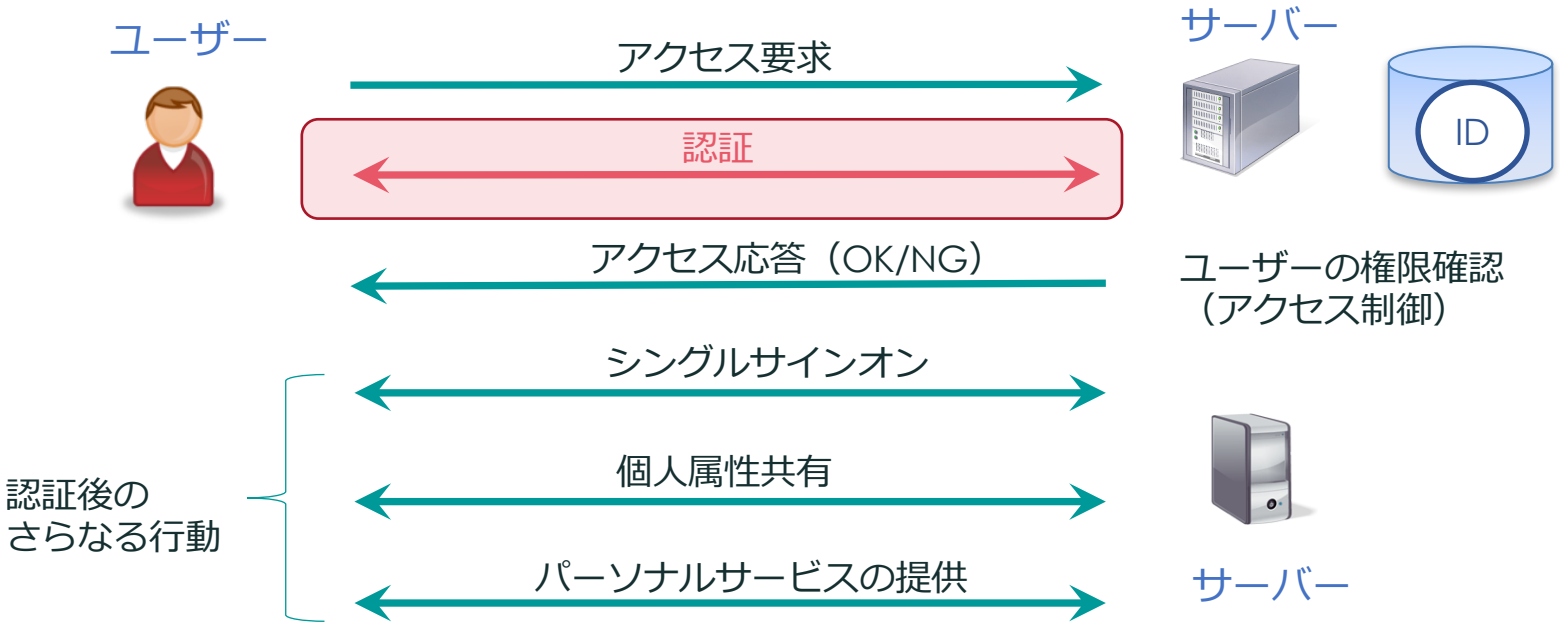


CTAP (Client To Authenticator Protocol)

FIDO認証を用いた
応用ソリューション

認証: セキュア・トラストアプリケーションのための基盤

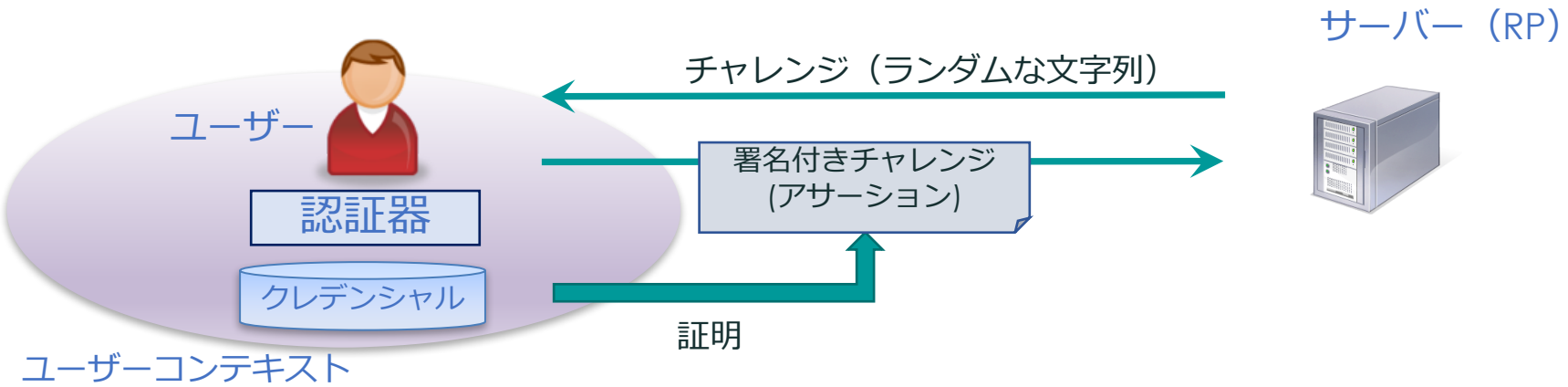
一般的なアクセス制限つきシステム



認証が起点になり、様々なオンライン上の行動につながる。

FIDO認証のセマンティクス（意味）

- ユーザーが本人であると主張通りの人であることを検証したということ
- ユーザーが認証器のすぐそばにいる（存在する）こと
- ユーザーが、自分のアイデンティティ（本人性）、コンテキスト、取引などに関して確認した（同意した）ということ

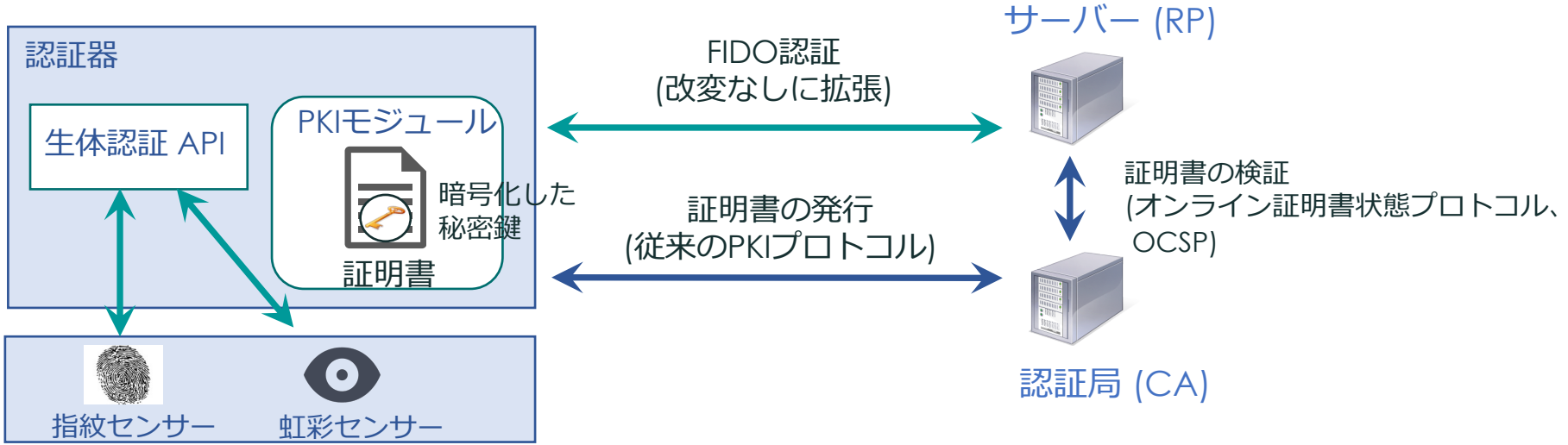


FIDO認証は、ユーザーのアイデンティティやコンテキストを証明する機構を備える。

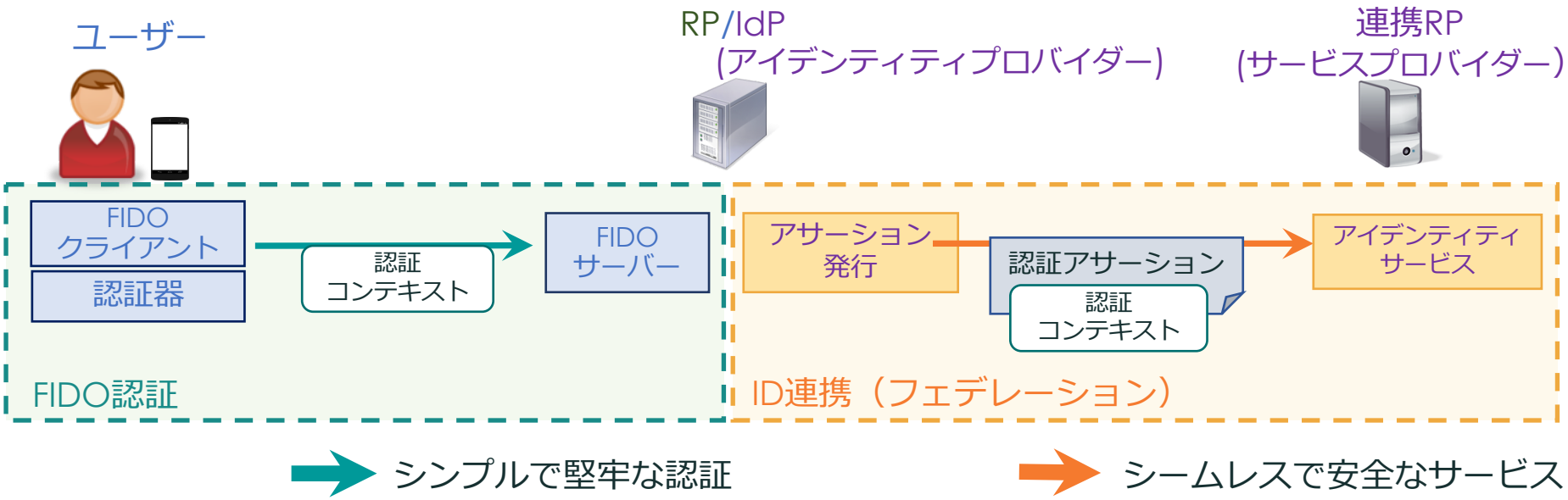
認証器の応用展開

既存・新規の認証方式を実装した認証器の展開を期待
- 生体認証
- 行動特性
- ウェアラブル機器

（例）証明書ベースの認証を実装した認証器 (韓国KICAのユースケース)

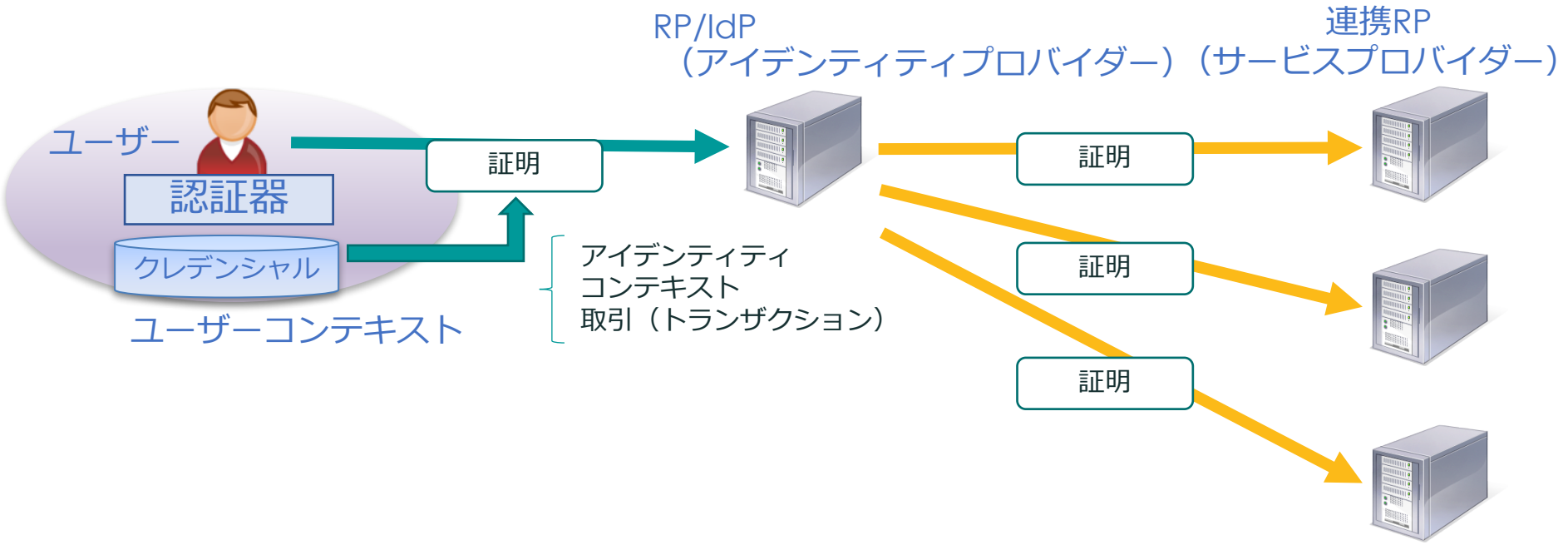


FIDO認証とID連携



FIDO認証とID連携を組み合わせると、認証コンテキストは認証器から連携RPへと伝搬。

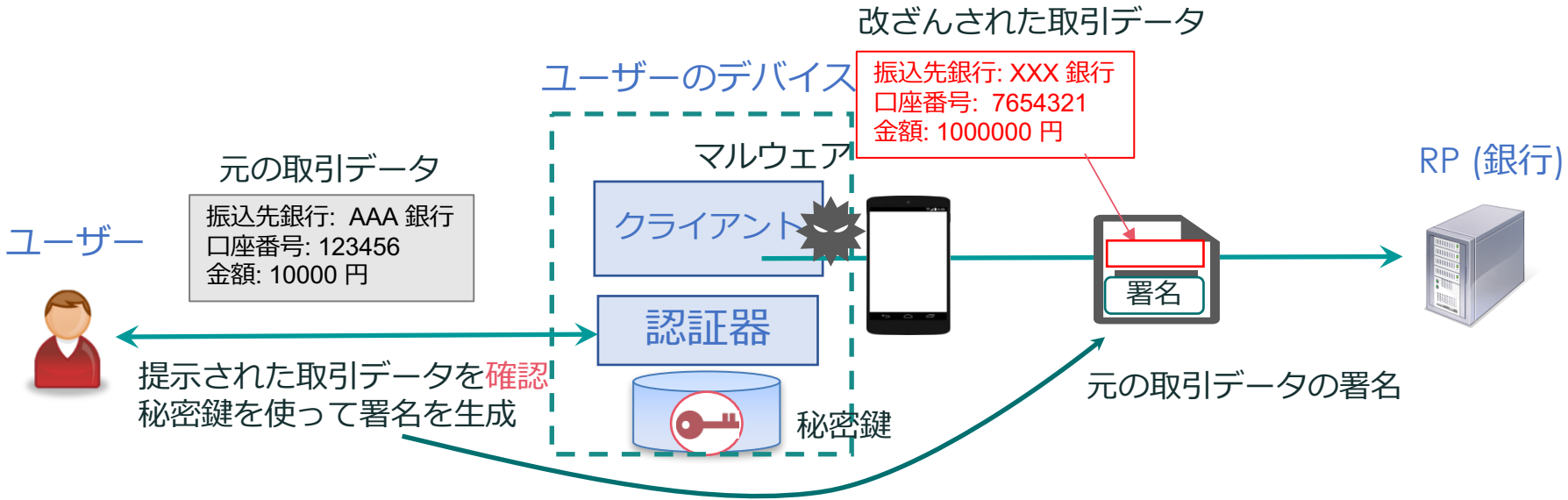
証明情報の伝搬



認証器で生成されたユーザーの証明情報を使えば、インターネット規模で
トラストなアプリケーションを提供することができる。

取引（トランザクション）認証

MITM (Man-in-the-Middle) 攻撃から取引データの改ざんを保護
(既にUAF仕様でサポート、海外の銀行で導入事例あり)

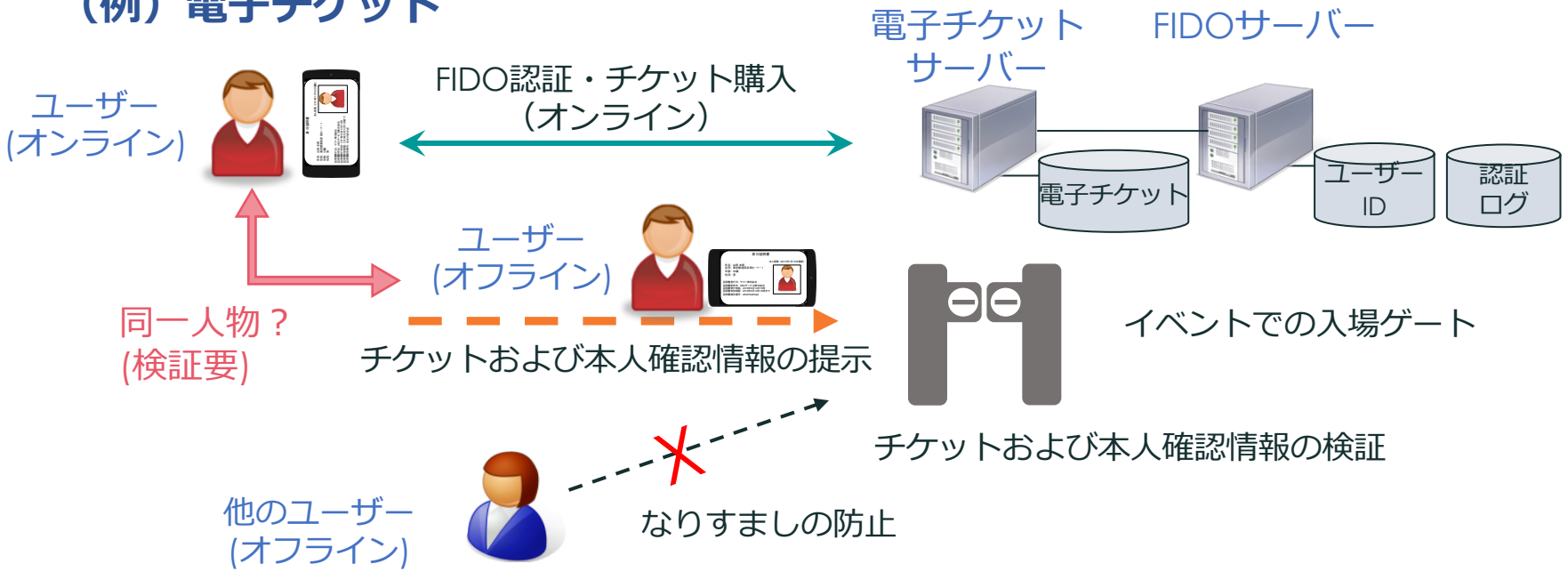


署名付き取引データを改ざんしても、署名検証により改ざんを検出し、不正送金を防止可能

オフラインでの本人確認

リアルタイムで生体によるFIDO認証を用いれば、現実世界のサービスへのアクセス時に「本人確認」が可能となる。

（例）電子チケット



まとめ

- FIDO認証モデル
  - 公開鍵暗号を用いた認証
  - 部品化した認証器によるローカル認証
- Web認証APIとCTAP
  - ブラウザを通じたクレデンシャルの操作
  - 多様なデバイス形態と通信プロトコルによる認証器をサポート
- FIDO認証を用いたソリューション展開
  - 認証器の導入展開
  - アイデンティティ連携システムの拡張
  - アイデンティティ・コンテキストの証明