FIDO東京セミナー ＠東京電機大学（2014年10月10日）

FIDO技術の適用による安心・安全なサービスの実現

ヤフー株式会社
Yahoo! JAPAN 研究所 上席研究員
五味 秀仁

あらすじ

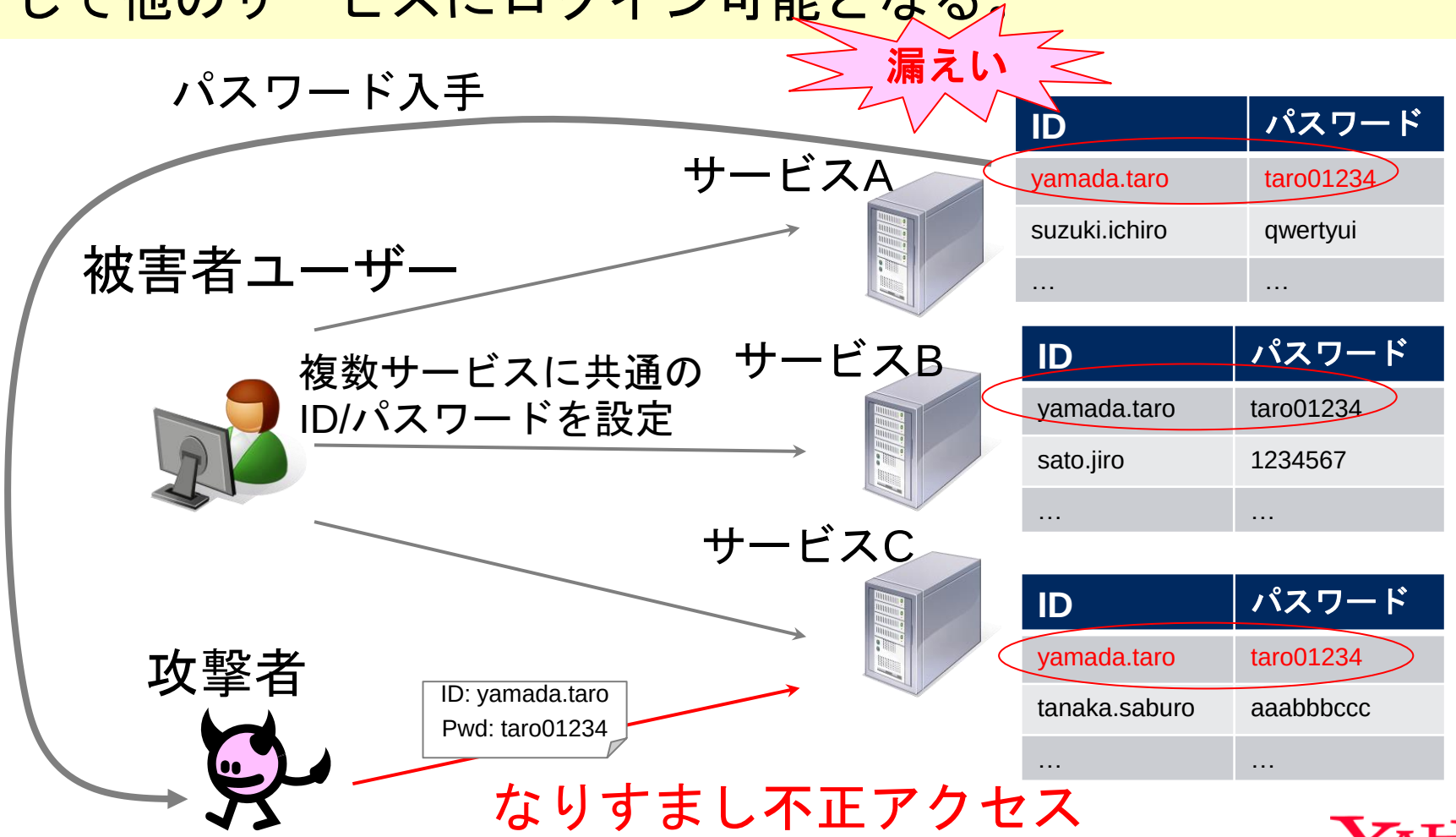
- 課題: パスワード
- ID管理におけるFIDO技術の位置づけ
- FIDO技術の有効性
- FIDO技術を用いたサービス

あらすじ

- **課題: パスワード**
- ID管理におけるFIDO技術の位置づけ
- FIDO技術の有効性
- FIDO技術を用いたサービス

パスワードリスト型攻撃

ユーザーが同一のパスワードを使い回すと、あるサービスのパスワードリストが漏れた場合に、第三者が前記ユーザーになりすまして他のサービスにログイン可能となる。



ID	パスワード
yamada.taro	taro01234
suzuki.ichiro	qwertyui
…	…

ID	パスワード
yamada.taro	taro01234
sato.jiro	1234567
…	…

ID	パスワード
yamada.taro	taro01234
tanaka.saburo	aaabbbccc
…	…

パスワード管理は限界 (1)

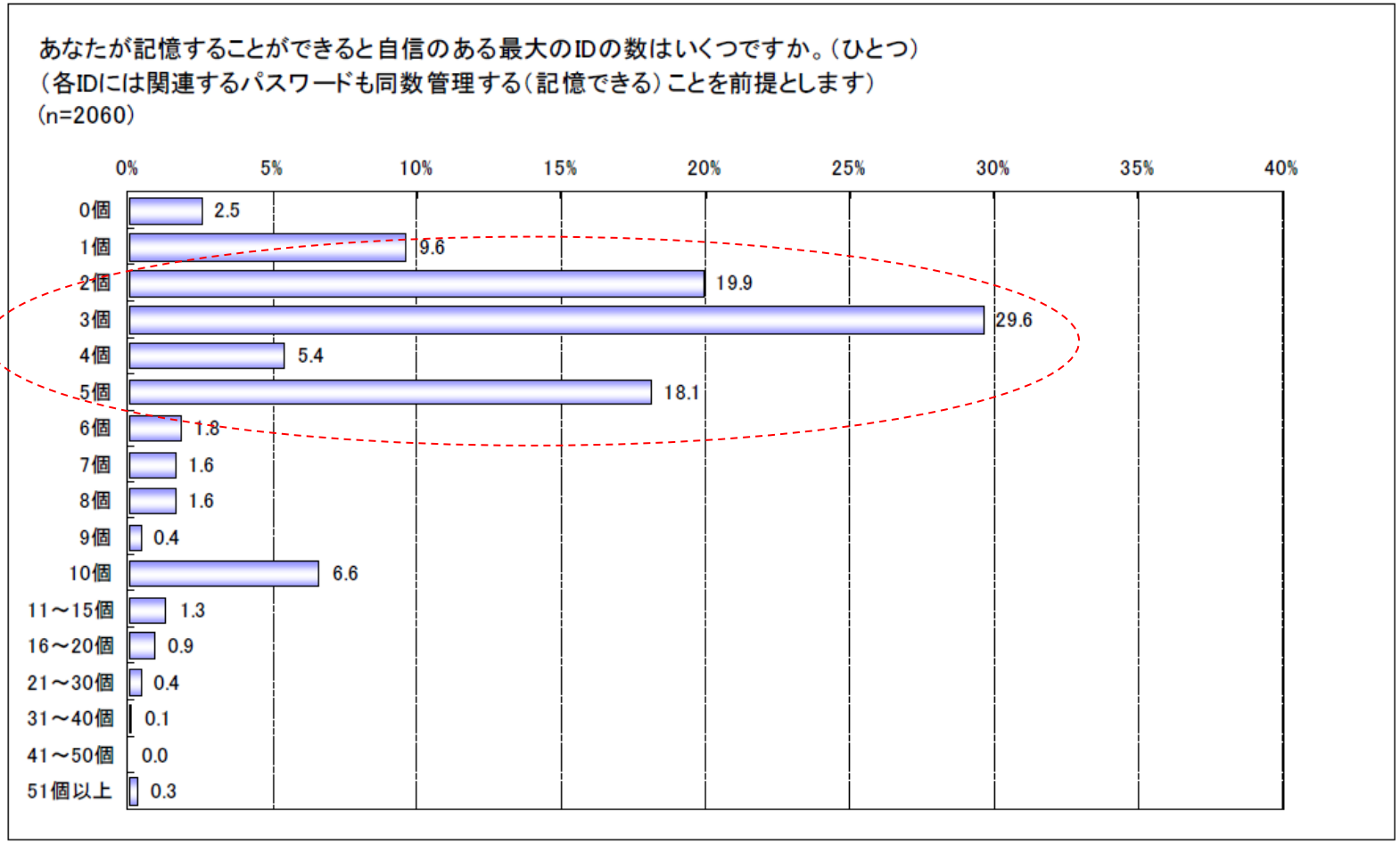
Webサイトのパスワード利用実態調査

- 1ユーザあたり、約14のサイトに対してパスワードを設定
- 約7割が、3種類以下のパスワードを複数サイトで使いまわし

(出展)トレンドマイクロ社プレスリリース
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20130829075331.html

パスワード管理は限界 (2)

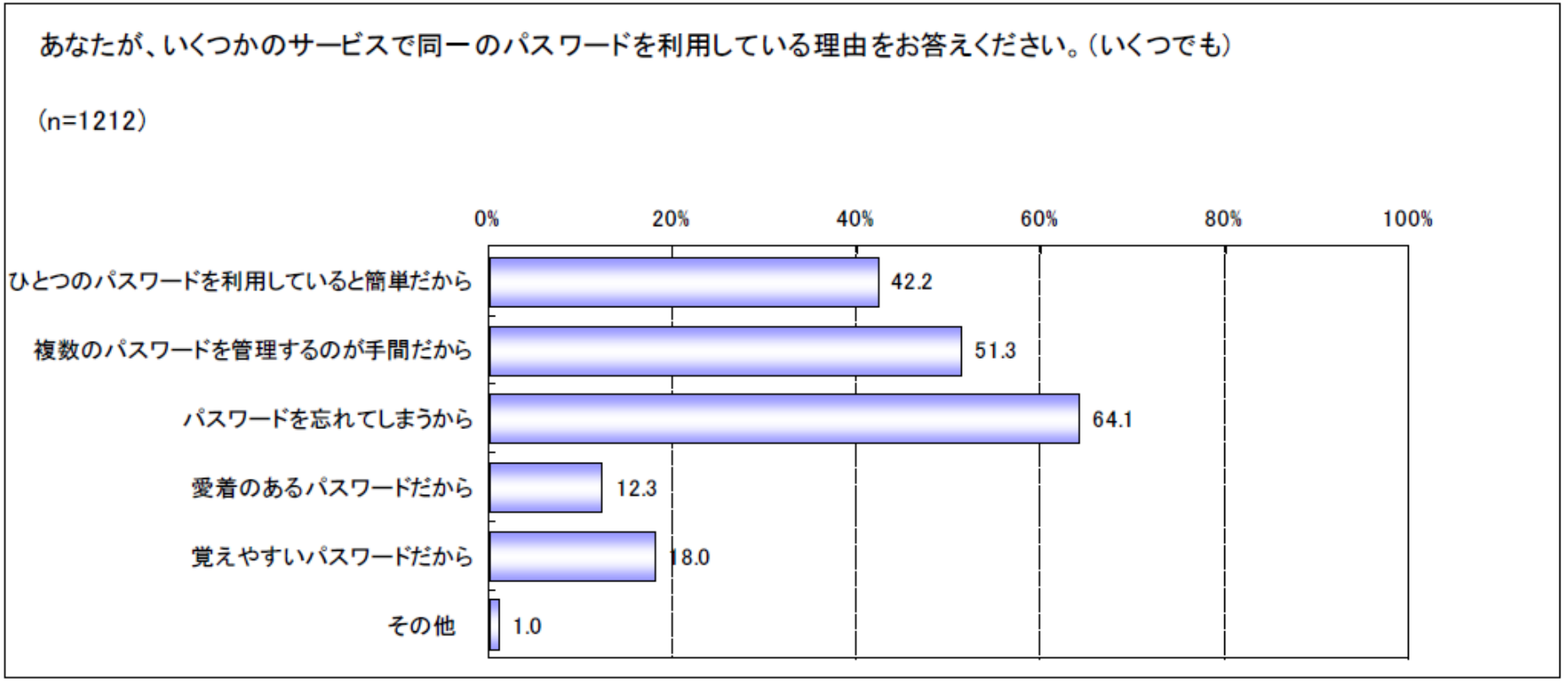
人が記憶できる最大IDの数



(出展) IPAオンライン本人認証方式の実態調査
http://www.ipa.go.jp/security/fy26/reports/ninsho/

パスワード管理は限界 (3)

同一のパスワードを利用している理由

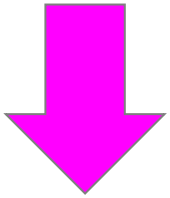


(出展) IPAオンライン本人認証方式の実態調査
http://www.ipa.go.jp/security/fy26/reports/ninsho/

パスワード管理の課題

単一サービスだけの
セキュリティ強化策では
解決困難

外部サービスの脆弱性や
ユーザーのセキュリティ
に関するリテラシーに依存



サービス・事業者を越えて、
業界として取り組むべきもの

「STOP!! パスワード使い回し!!」キャンペーン

Yahoo! JAPANからのお知らせ

2014年9月17日

ヤフー株式会社

STOP!! パスワード使い回し!!

独立行政法人 情報処理推進機構と一般社団法人 JPCERTコーディネーションセンターでは、昨今パスワードリスト型攻撃による不正ログインが多発しているという報告を受け、複数のインターネットサービスにおいて同じパスワードの使用を控えるよう注意喚起をする発表を9月17日に行いました。

Yahoo! JAPANでも、ユーザーのみなさまがインターネットサービスを安全にご利用頂くために、同発表を支持し、その内容をご案内いたします。
詳細は、当該ページをご覧ください。

STOP!! パスワード使い回し!!
スマートフォン
http://www.jpcert.or.jp/m/pr/2014/pr140004.html （外部サイト）
パソコン
http://www.jpcert.or.jp/pr/2014/pr140004.html （外部サイト）

Yahoo! JAPANでは、今後もインターネットの安全・安心な発展をめざし、さまざまな情報提供を進めてまいります。

▲このページのトップへ

あらすじ

- 課題: パスワード
- **ID管理におけるFIDO技術の位置づけ**
- FIDO技術の有効性
- FIDO技術を用いたサービス

FIDOと認証手段

認証の3要素

- **記憶 (Something you know)**: 本人のみが記憶するデータによる
  - （例）パスワード、パスフレーズ、PIN など。
- **所持 (Something you have)**: 本人のみが所持している物による
  - （例）ICカード、ワンタイムパスワードのトークンなど。
- **生体情報 (Something you are)**: 本人の特徴を表すデータによる
  - （例）指紋、音声、虹彩、顔など。

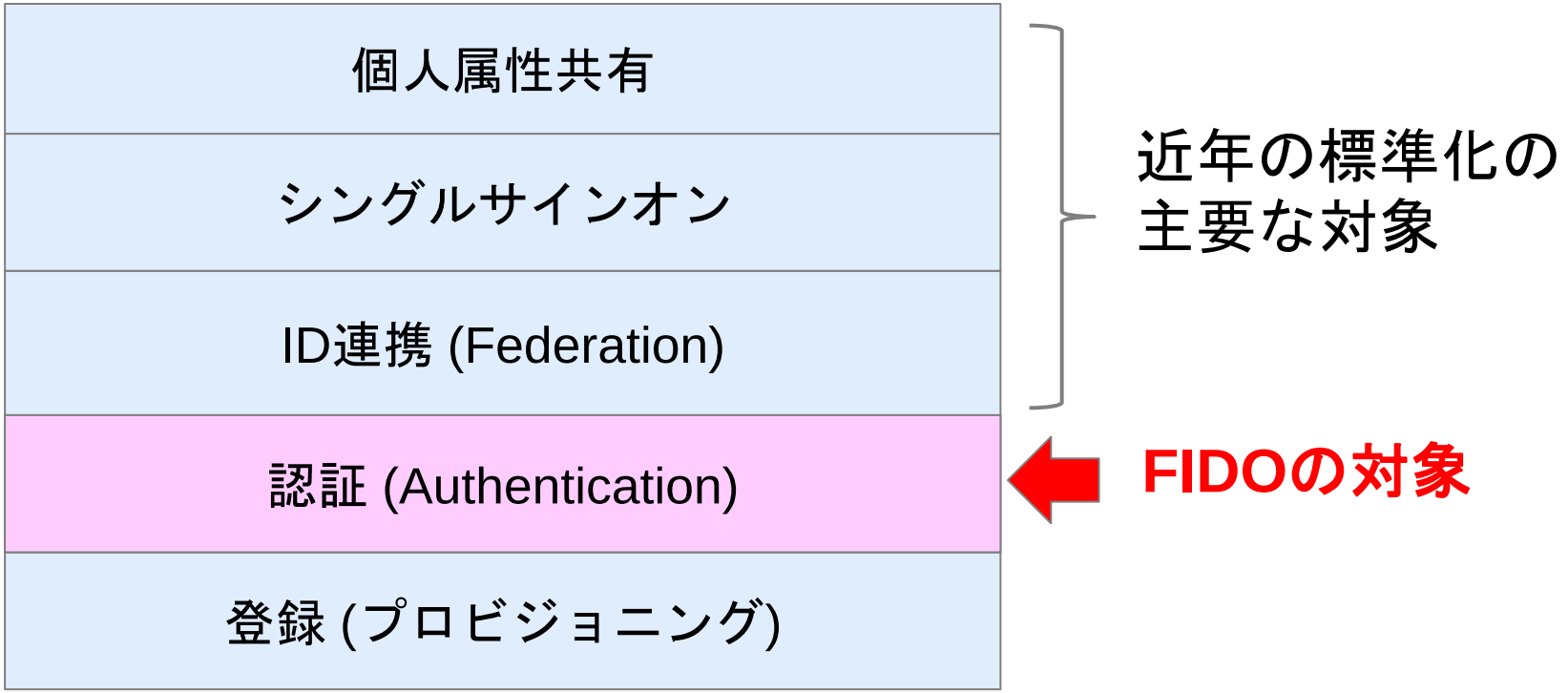
FIDOの主な対象

(出典) オンライン本人認証方式の実態調査報告書 (IPA)
http://www.ipa.go.jp/files/000040778.pdf

FIDOでは、記憶に頼る認証に代わり、
所持や生体情報による認証を採用。

ID管理における機能の階層構造

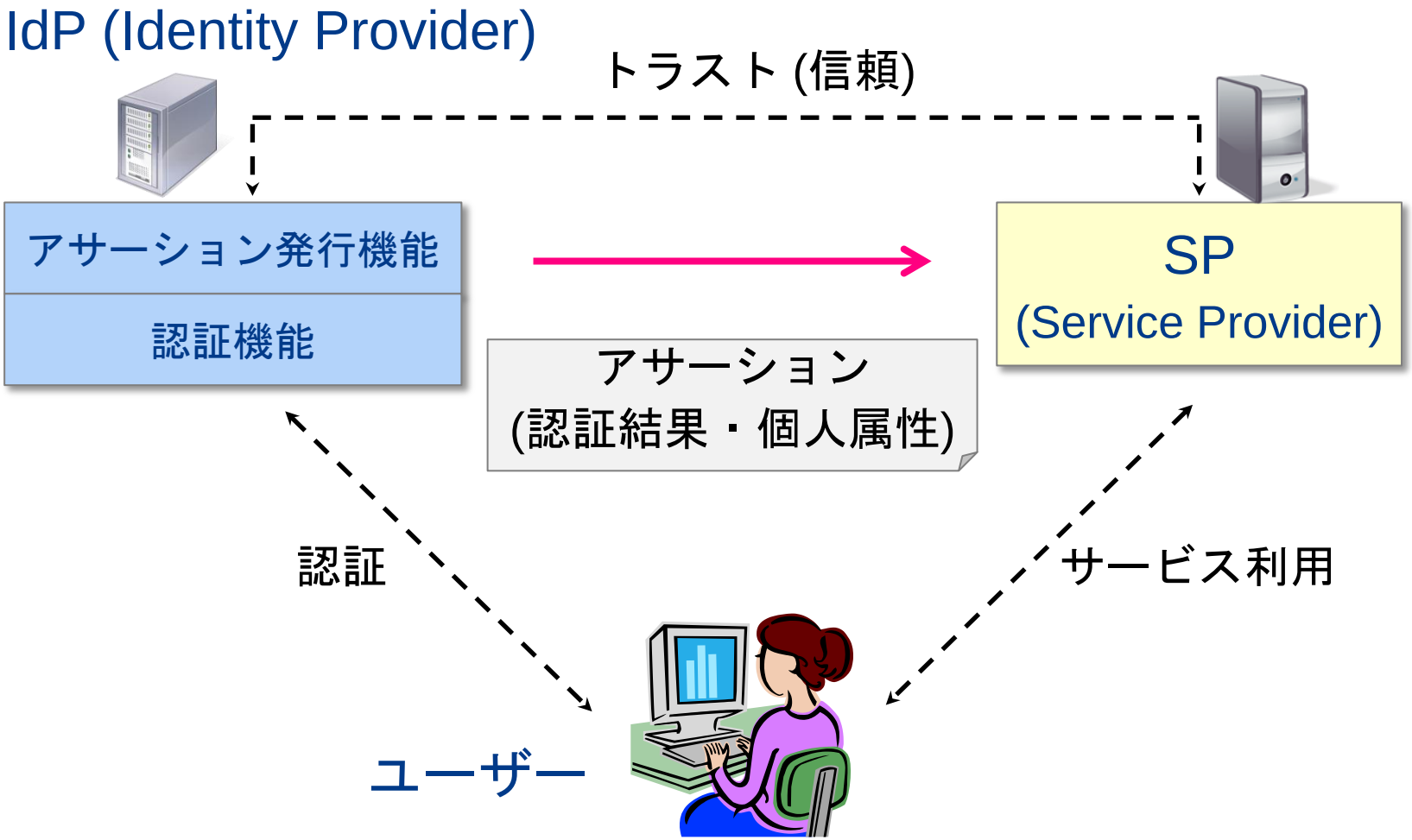
*ID: アイデンティティ。本人性。



FIDO: 課題のピース (認証) の部分を埋める取り組み

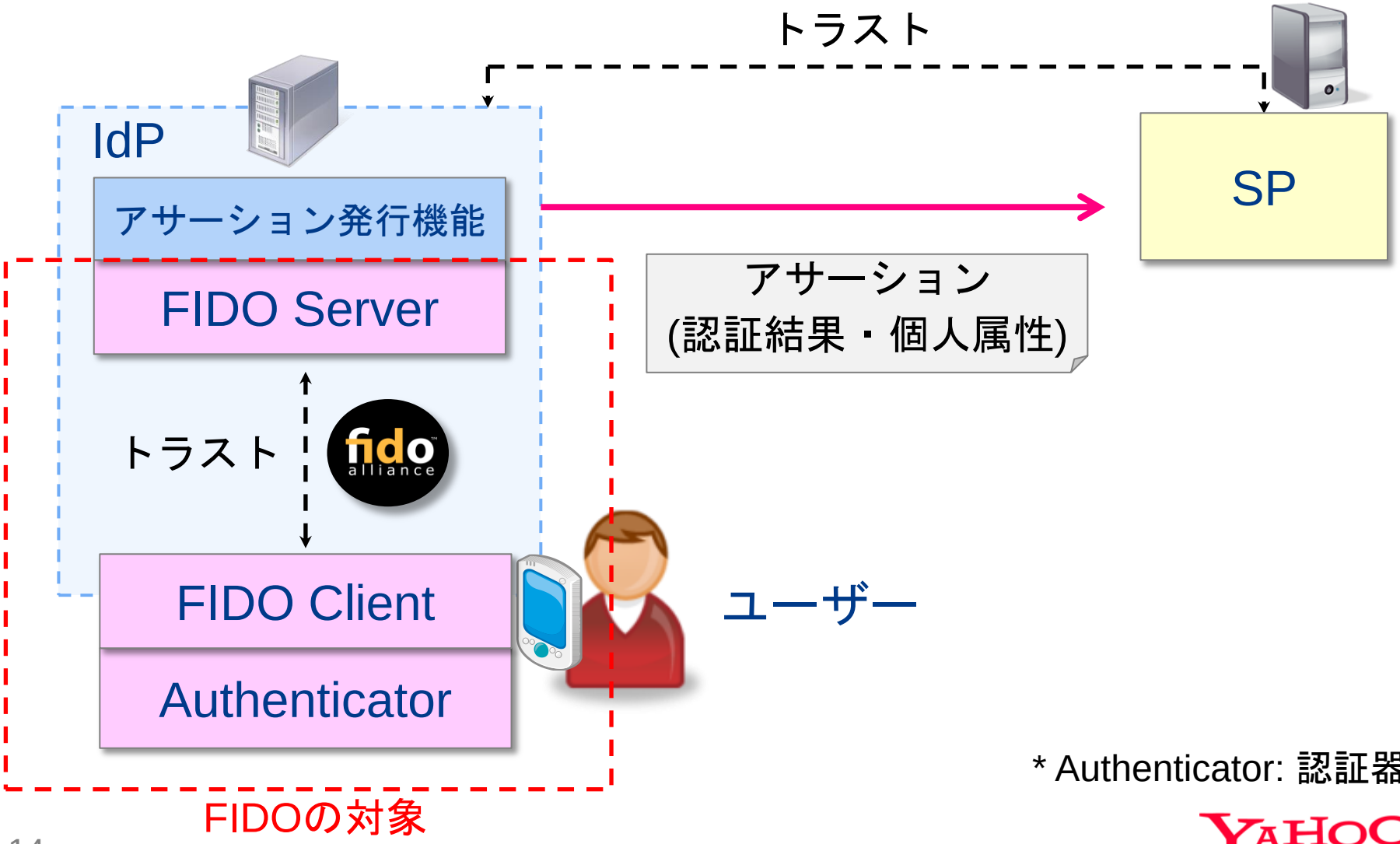
(従来) 分散型ID管理アーキテクチャでのID連携

既存のID連携仕様 (SAML/OpenID/OpenID Connectなど)



FIDOアーキテクチャとID連携

FIDOは、従来のID連携とは補完関係、ID連携を強化

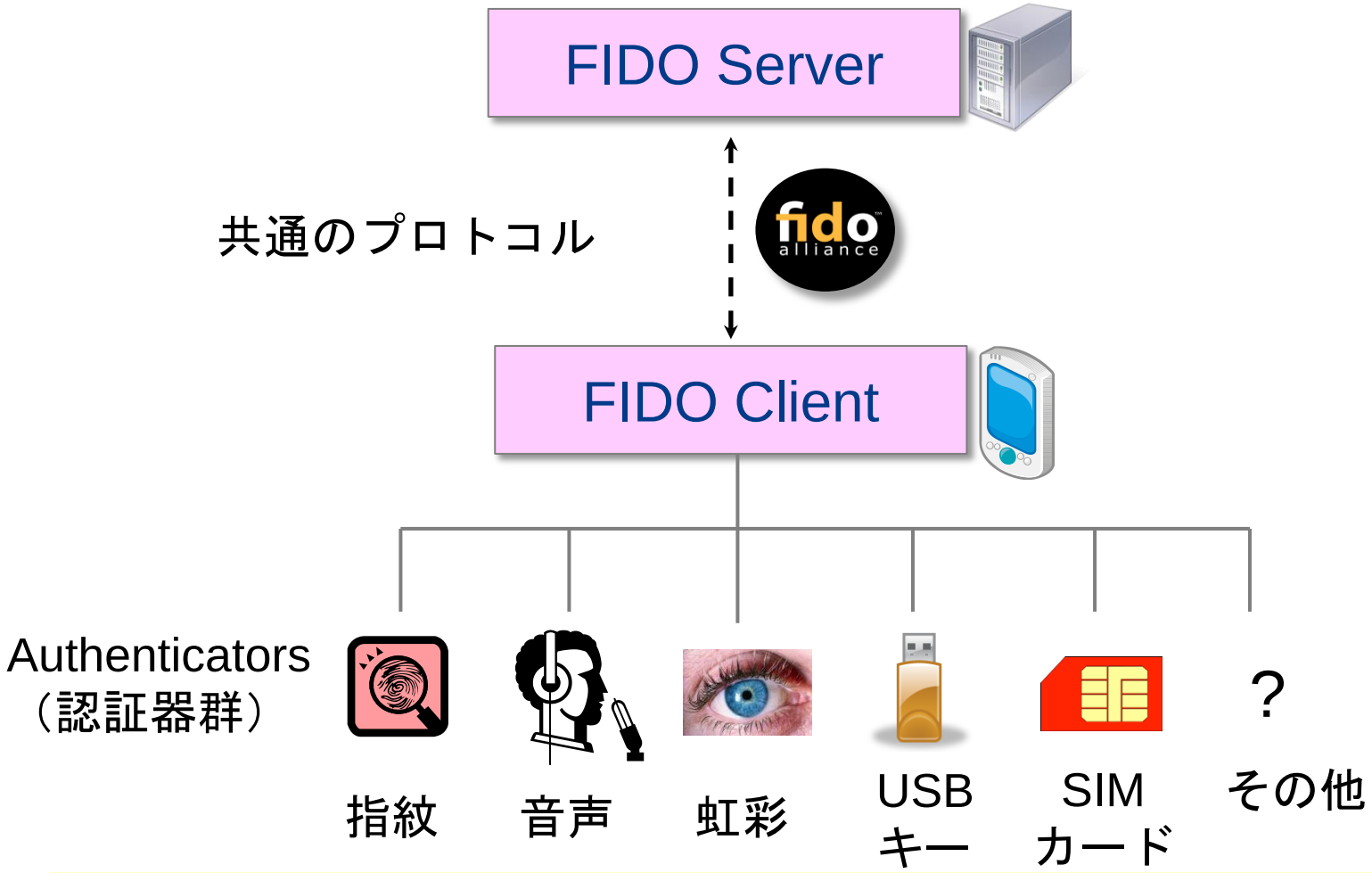


* Authenticator: 認証器

あらすじ

- 課題: パスワード
- ID管理におけるFIDO技術の位置づけ
- **FIDO技術の有効性**
- FIDO技術を用いたサービス

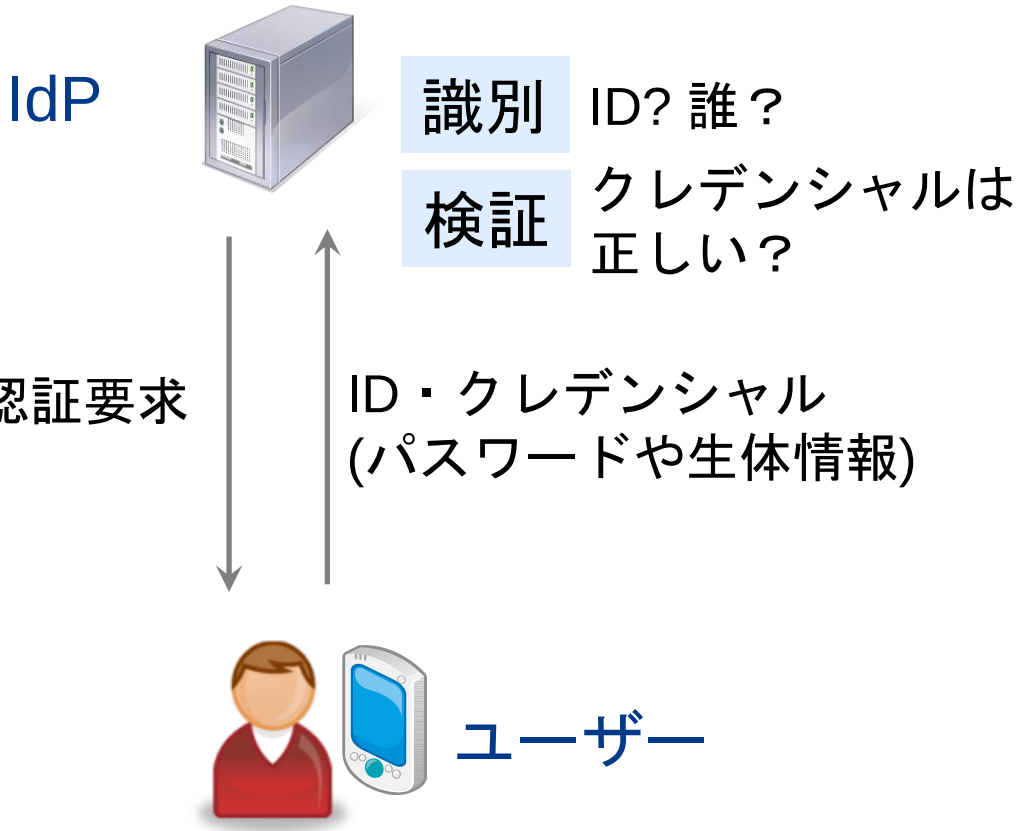
認証機能の部品化: Pluggable Authentication



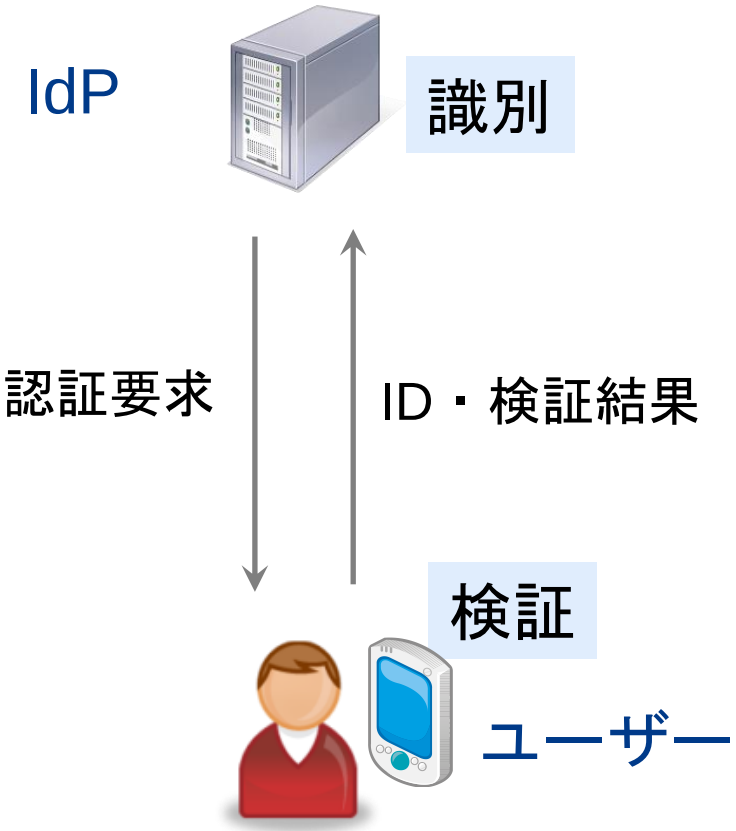
認証器をプラグイン的に追加、組み合わせ、
多要素認証、認証の強化を実現

認証機能の分解

従来の認証



FIDOの認証



FIDO認証は、ローカルな検証で、効率性が良い。
ネットワーク上に生体情報などの漏洩リスク減。
（プライバシー保護に有効）

認証の信頼レベル (Level of Assurance)

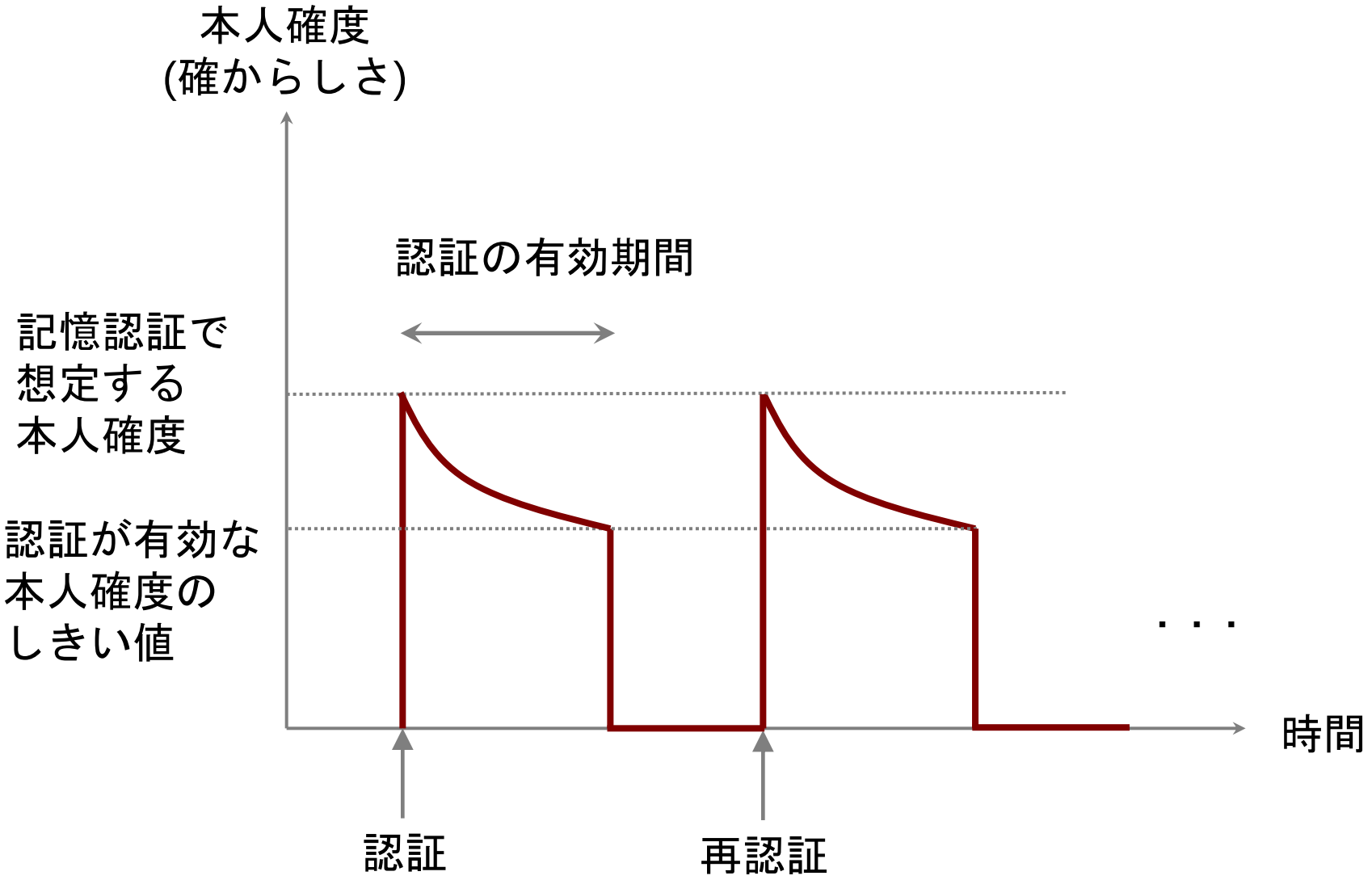
NIST (米国国立標準技術研究所) 電子認証ガイドライン：
リモート認証の基準を規定。

- **レベル 1**: 低、パスワードなど (6桁以上)
  - 本人確認なし (自己申告)
- **レベル 2**: 中、パスワードなど (8桁以上)
  - 本人確認、ならびに、その証拠の提示あり
- **レベル 3**: 高、パスワードだけでなく、2要素以上
  - 公的身分証明書
- **レベル 4**: 特高、ハードウェアによる、暗号プロトコルを通した鍵の所持
  - 対面による本人確認

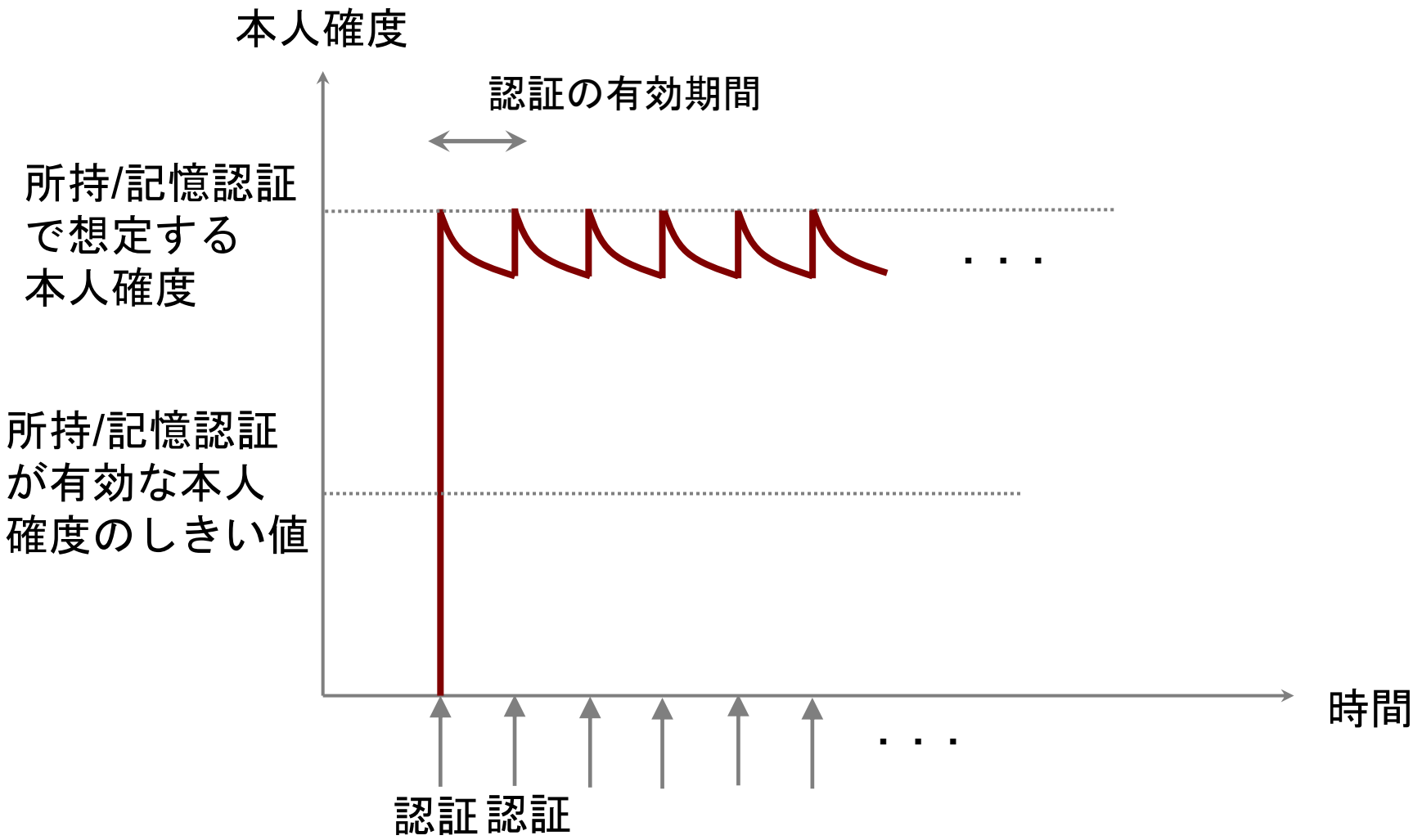
FIDO認証でサポート？

(ご参考) NIST Electronic Authentication Guideline SP800-63
経済産業省 ID連携トラストフレームワーク

本人確度と時間の関係: 記憶認証の場合



本人確度と時間の関係: 所持/生体認証の場合



本人確度が下がる前に、ユーザーに少ない負担で
継続的な認証を実施可能　→ 認証のあり方が変わる

あらすじ

- 課題: パスワード
- ID管理におけるFIDO技術の位置づけ
- FIDO技術の有効性
- **FIDO技術を用いたサービス**

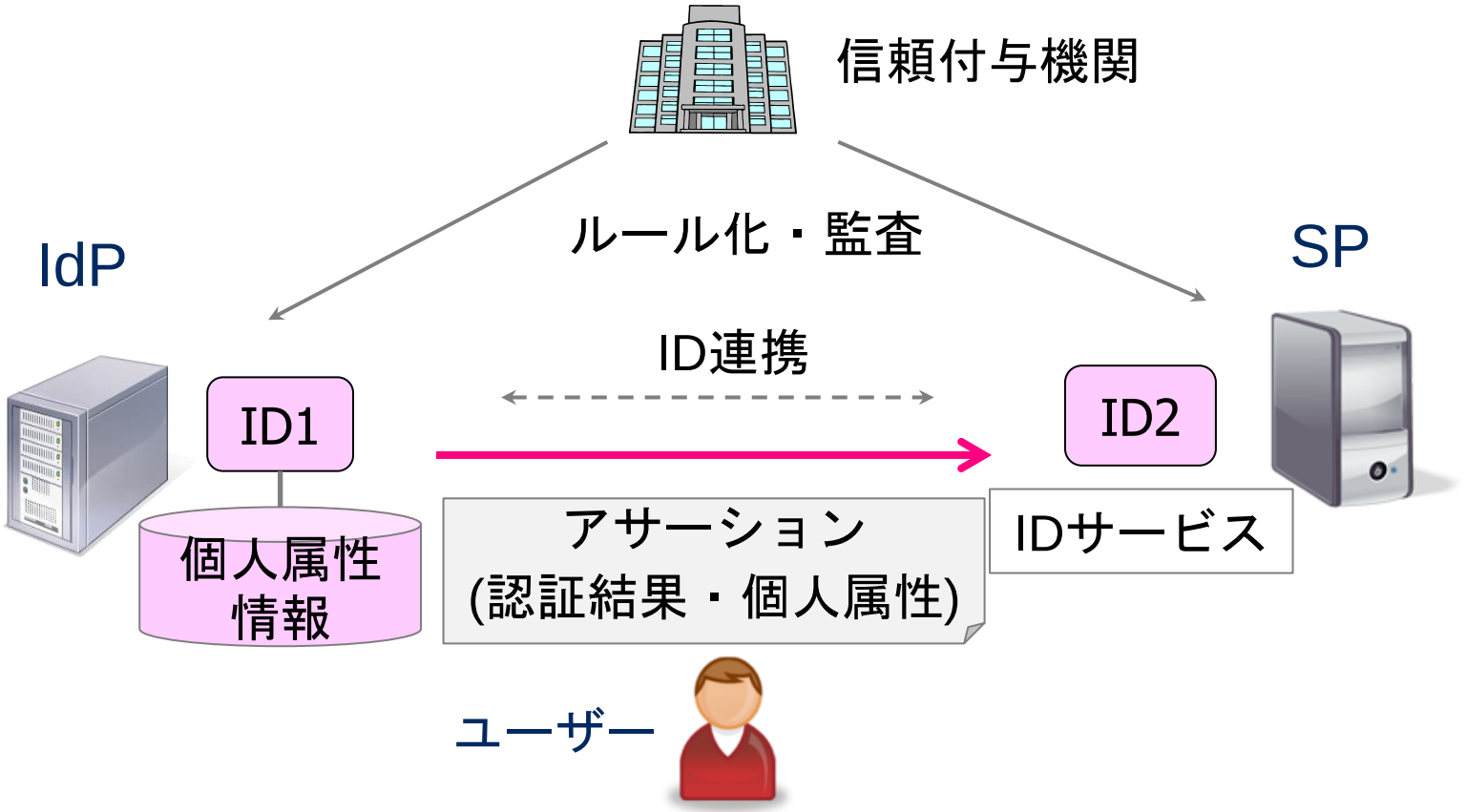
デモ: FIDO指紋認証(DDS社)を通じてヤフオクを使う

ユーザー体験（おもてなし）の確認

- 認証へのストレス・心理的障壁を下げる
- お客様のシームレスなサービス利用

経済産業省 ID連携トラストフレームワーク

IdP/SPの要件を規定し、互いにトラスト (信頼)できるコミュニティを形成することで、ビジネスを活性化させようというもの



FIDOシステムは、認証の信頼レベル(LoA)を高められ、
信頼性の高いフレームワークの基盤の一部にできる可能性がある。

まとめ

まとめ

- FIDOでは、パスワードの課題を解決を目指す
- FIDOの利用は、認証のあり方を変える可能性あり
  - 認証手段をプラグイン的に追加
  - 認証を強化、認証手段をカスタマイズ
  - ローカルな検証
  - 継続的な認証
- FIDOとID連携は補完関係
  - 簡単・便利で安心・安全なサービスの提供に役立つ可能性あり
  - ID連携トラストフレームワークの実現の基礎となる可能性あり

ご清聴ありがとうございました

コンタクト先: hgomi@yahoo-corp.jp