デジタル・トラスト時代の生体認証基盤

～Public Biometric Infrastructure (PBI) と関連技術～

高橋 健太

(株)日立製作所　研究開発グループ

自己紹介

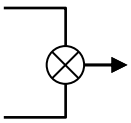
HITACHI
Inspire the Next

◆ 高橋 健太 / Kenta Takahashi

- 博士 (情報理工学) (東京大学)
- ㈱日立製作所　研究開発グループ 主管研究員
- 東京大学 客員准教授 [2015-2020]
- ISO/IEC SC37 (Biometrics) エキスパート [2013-]

◆ 専門

- 生体認証
- 暗号
- 情報セキュリティ



PBI, Cancelable Biometrics

情報セキュリティ脅威の動向

HITACHI
Inspire the Next

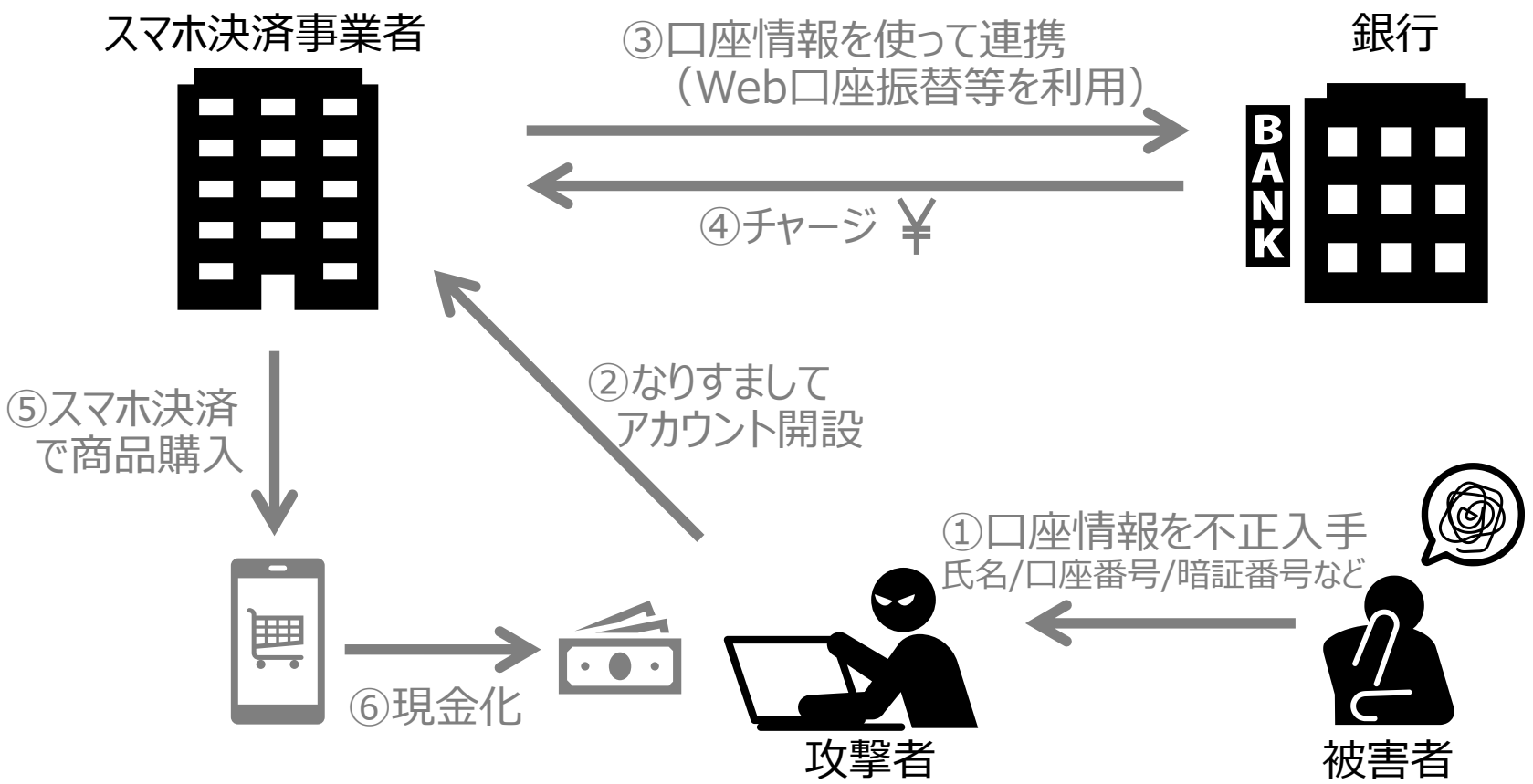
多くの脅威が「認証」に関連

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの 不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの 不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

出典：IPA「情報セキュリティ 10大脅威 2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html

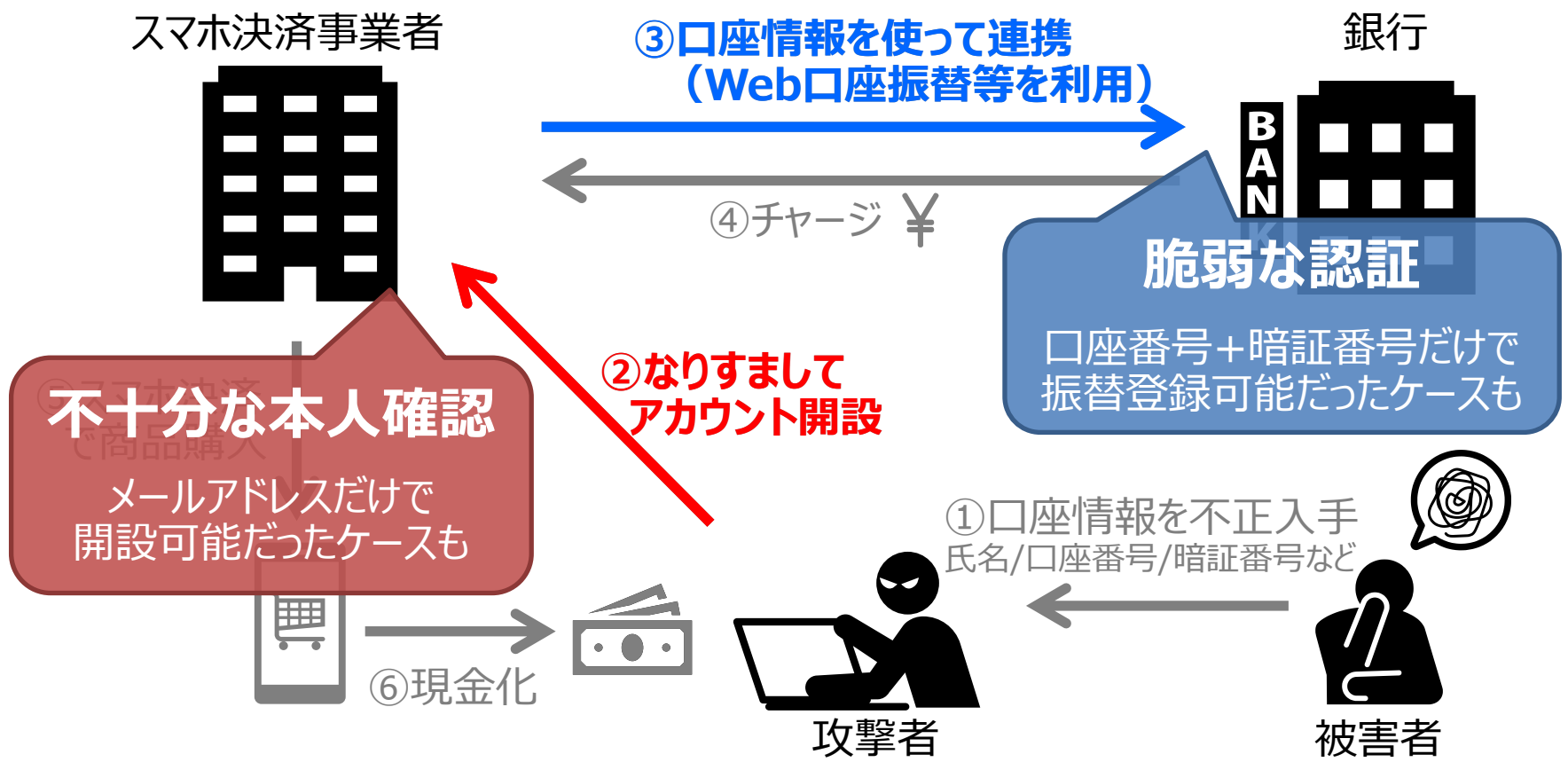
スマホ決済の不正利用問題の構図

多くのスマホ決済サービスが類似の手口で被害に



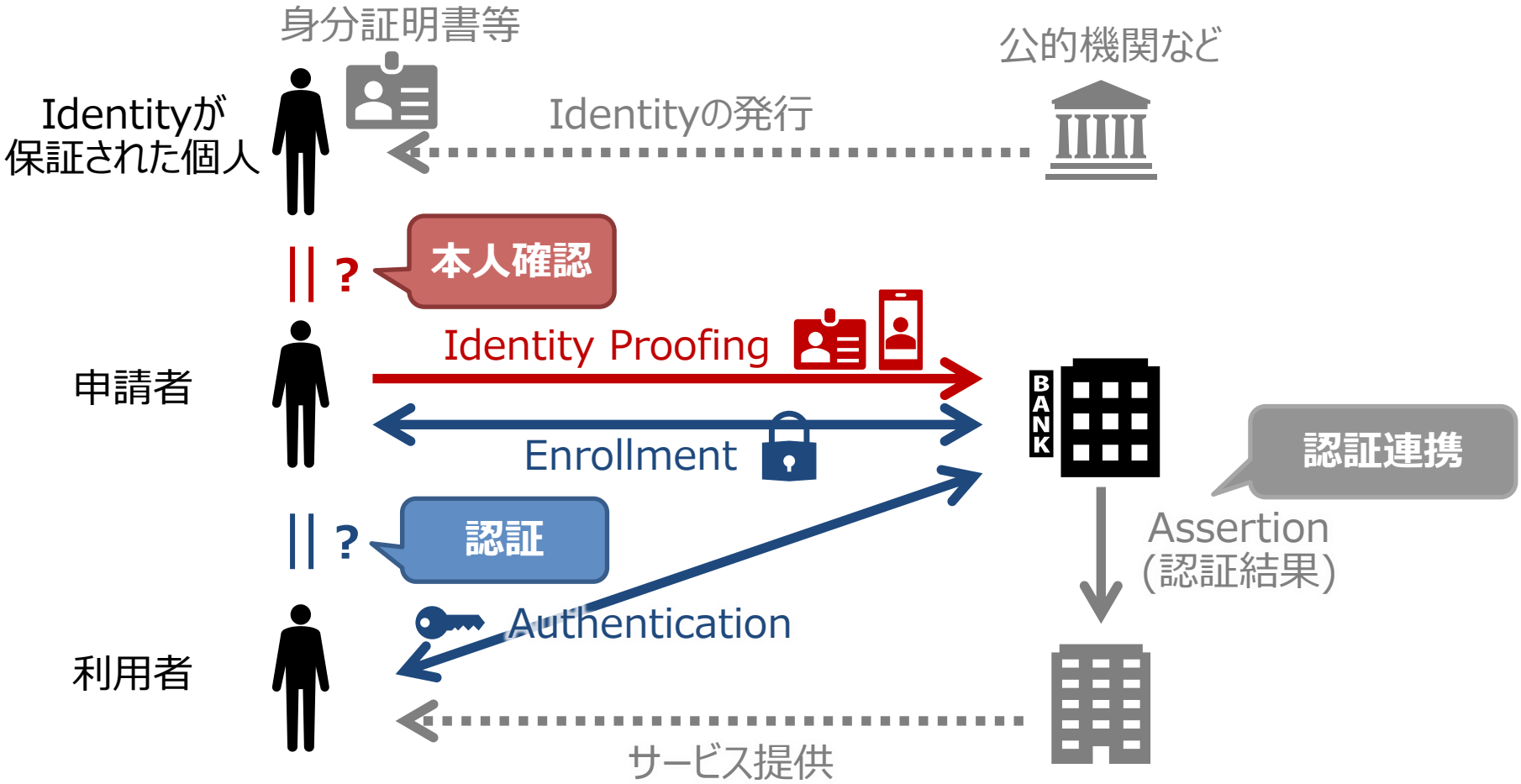
スマホ決済の不正利用問題の構図

狙われた脆弱性は大きく2箇所



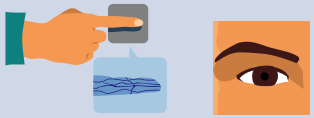
認証に関わる諸概念

本人確認、認証、認証連携



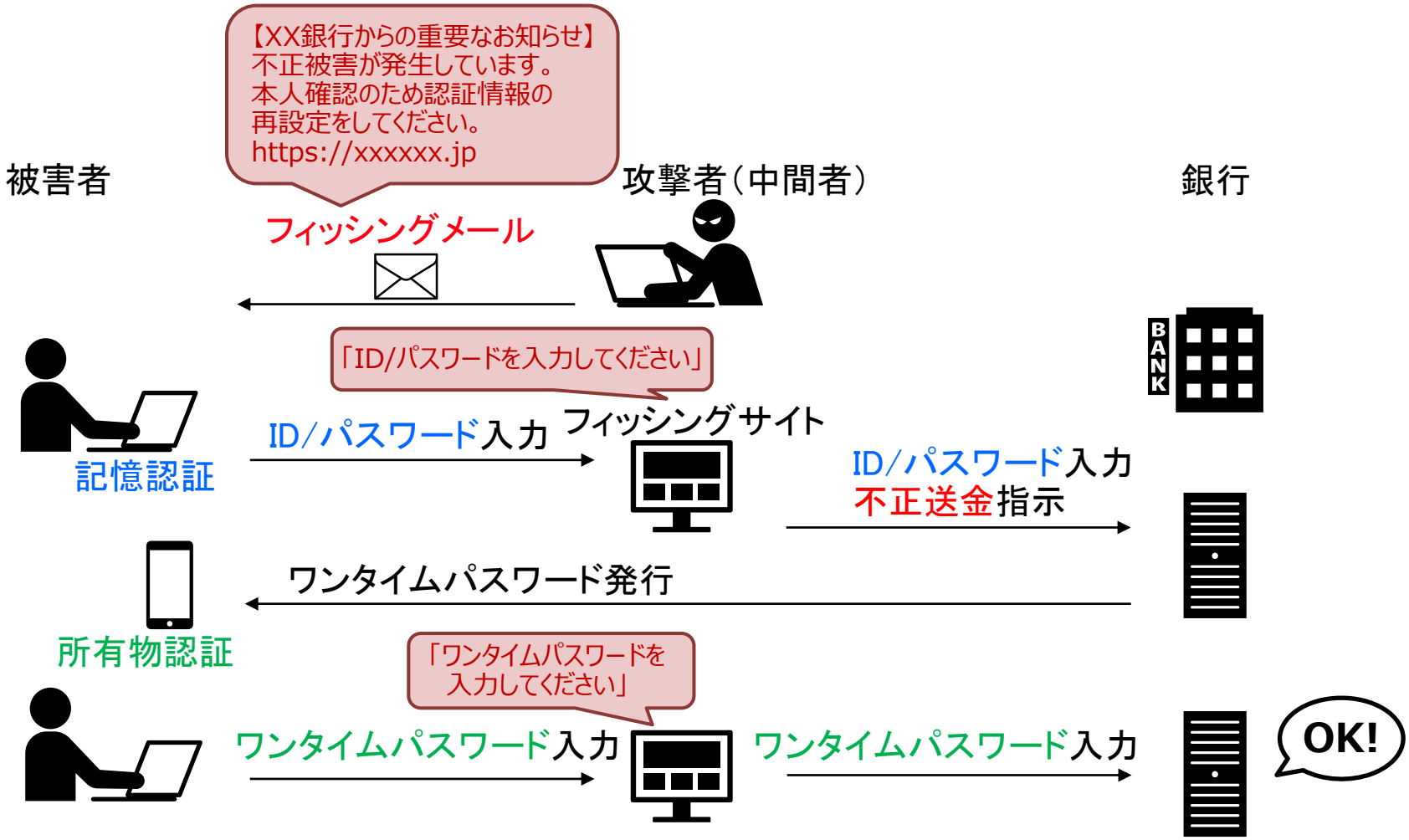
※ NIST SP800-63では本人確認，認証，認証連携それぞれの保証レベル等に関するガイドラインを規定している
※ KYC は金融分野における本人確認の類義語

認証の３要素

種別	例	利点	課題
知識認証 (What you know) 	・パスワード ・暗証番号	・導入コストが低い ・意思確認に好適	・忘れる ・推測される ・不正譲渡可能
所有物認証 (What you have) 	・スマホ ・ICカード ・OTPトークン	・**公開鍵認証と好相性** （オンライン認証特有の 多くの攻撃に対し安全）	・無くす ・盗まれる ・不正譲渡可能
生体認証 (What you are) 	・指紋 ・顔 ・静脈 ・虹彩	・**忘れない** ・**無くさない** ・**本人しか使えない**	・取替え不能 ・個人情報/プライバシ

「二要素認証⇒安全」とは限らない

中間者攻撃型のフィッシングによるネットバンキング不正利用が多発

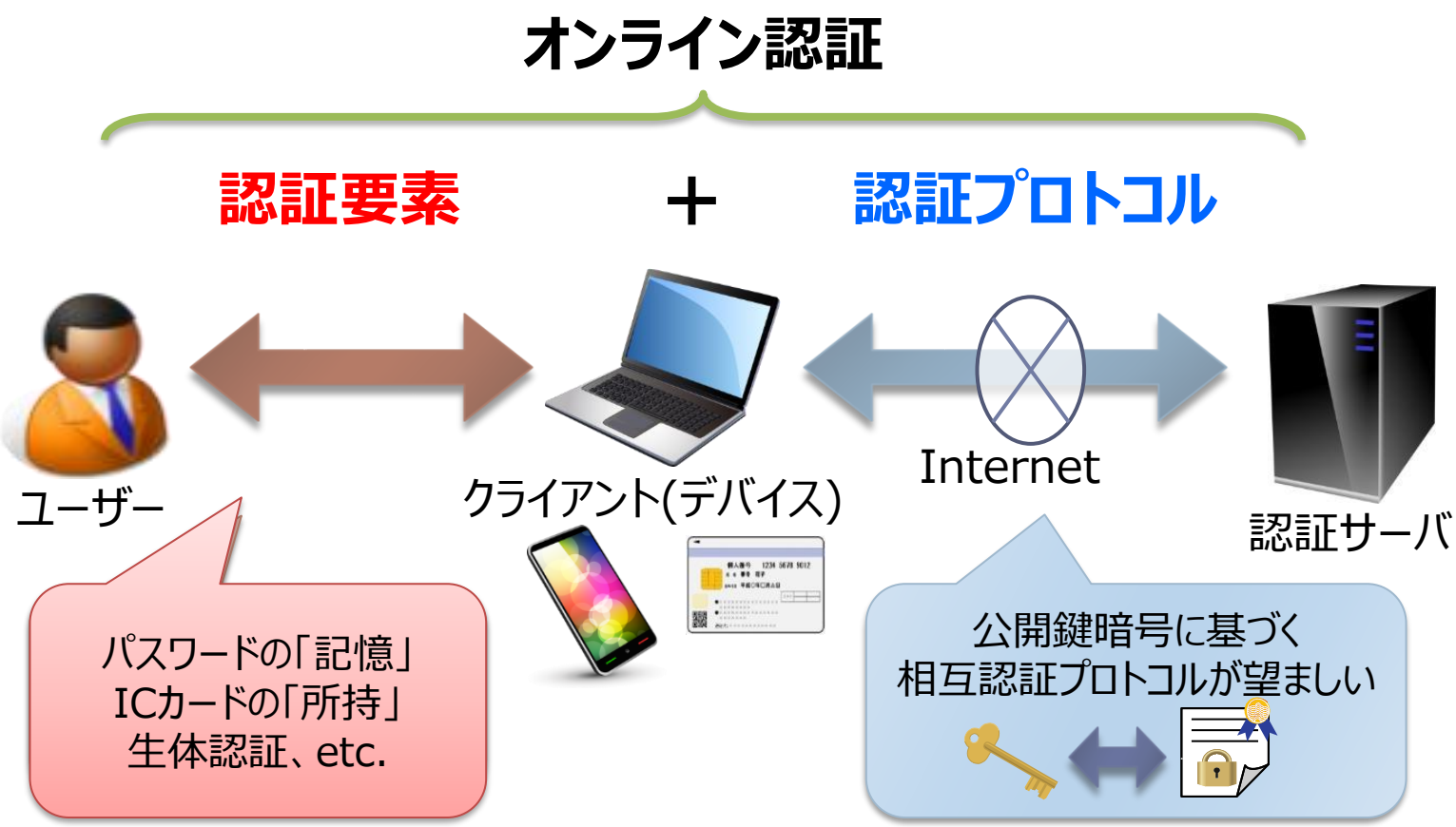


※参考：トレンドマイクロ，「国内ネットバンキングの二要素認証を狙うフィッシングが激化」，https://blog.trendmicro.co.jp/archives/22696

認証要素と認証プロトコル

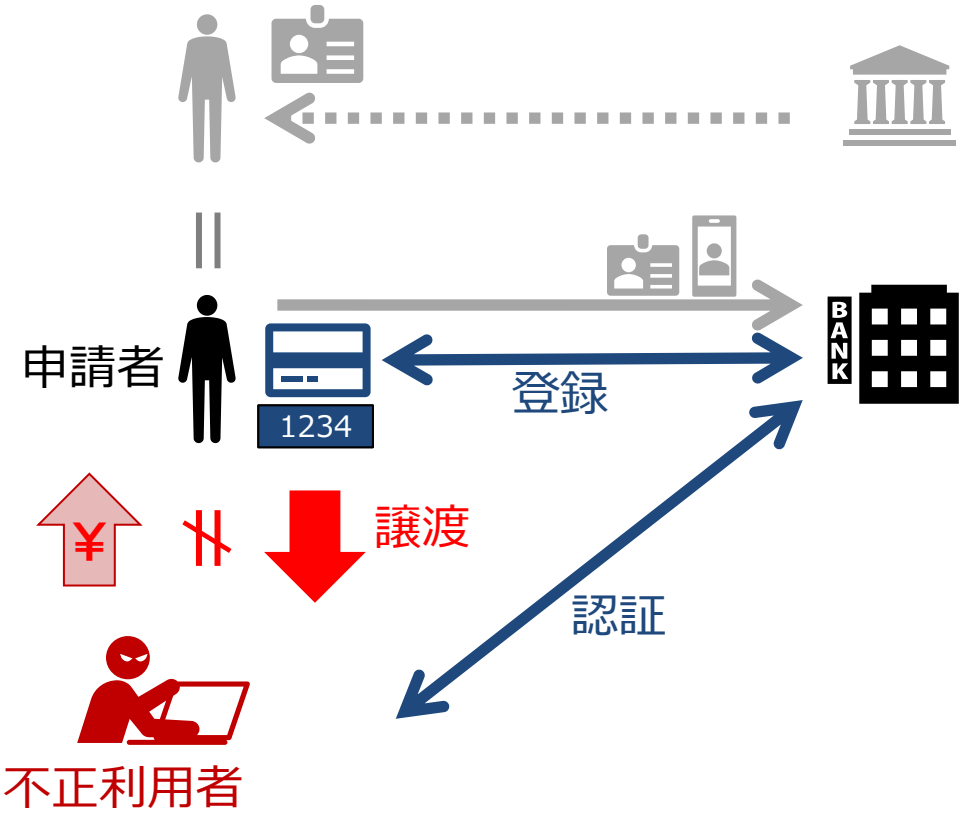
HITACHI
Inspire the Next

中間者攻撃などに対しても安全な暗号学的認証プロトコルが必要



認証器の不正譲渡問題

所有物/記憶は容易に譲渡可能。銀行口座の不正売買が横行



事例

口座不正利用に伴う口座の利用停止・強制解約等の件数の推移

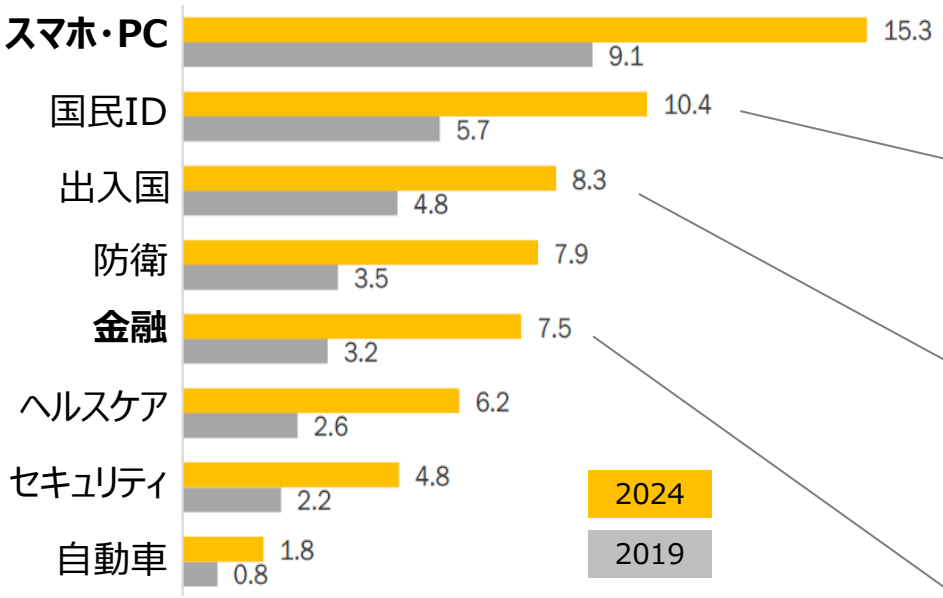
時期	利用停止	強制解約等	合計
平成26年度	54,893件	30,129件（28,227）	56,795件
平成27年度	51,969件	27,148件（23,823）	55,294件
平成28年度	52,753件	29,880件（26,795）	55,838件
平成29年度	42,454件	24,121件（21,636）	44,939件
平成30年度	40,193件	18,694件（16,058）	42,829件

※出典: 全国銀行協会,「金融犯罪の手口 / 銀行口座の売買」,
https://www.zenginkyo.or.jp/hanzai/7323/

生体認証への期待

紛失・忘却の心配がなく便利、盗難・不正譲渡に対する耐性
スマホ、金融などへ適用拡大し、市場規模は2024年に7兆円

生体認証 アプリケーション別 市場規模 (USD Million)



出典: Biometric System Market – Global Forecast to 2024, ©MarketsandMarkets, 2019.

生体認証の課題

生体認証データの保護が大きな課題
生体検知(偽造対策)、精度向上、低コスト化も

市場の成長ドライバ、制約、機会、課題

出典: Biometric System Market – Global Forecast to 2024, ©MarketsandMarkets, 2019.

生体認証データの漏洩は現実の脅威

FIDO: Fast Identity Online

HITACHI
Inspire the Next

スマートフォンなどユーザデバイス側で生体情報を管理

■サーバがデバイスを暗号学的に認証し，デバイスがユーザを生体認証する

✓ 生体情報はユーザデバイス内に留まり、ネットワークを流れない

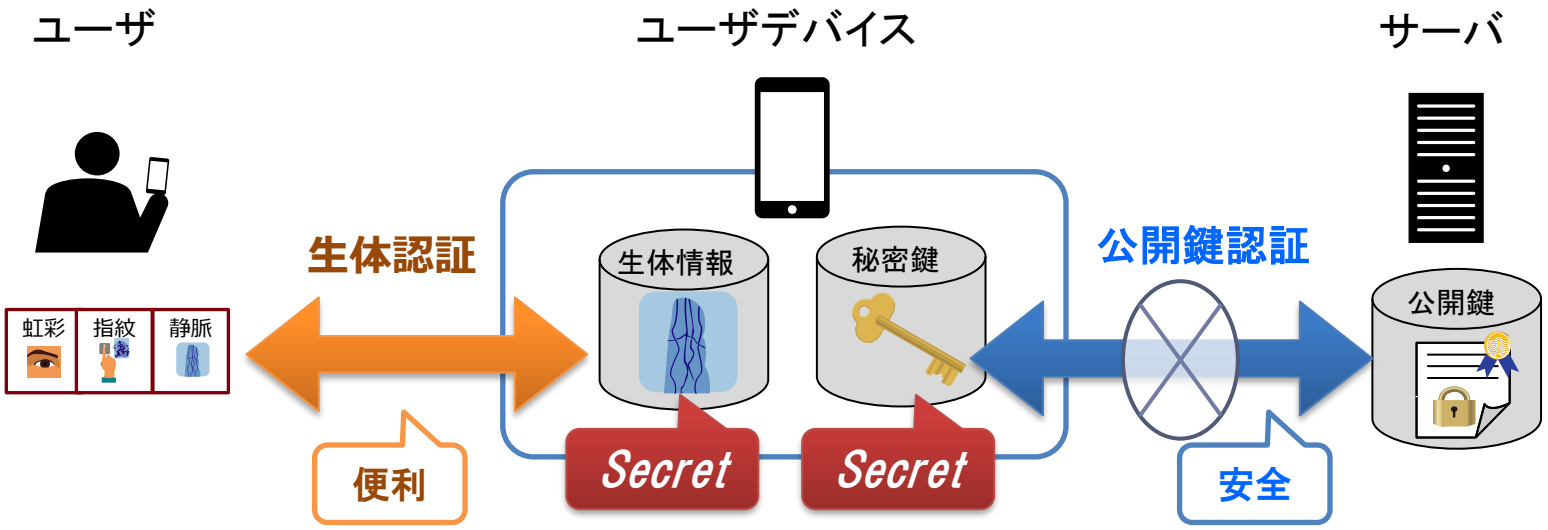
✓ デファクトスタンダード化しつつあり、対応機種やサービスが拡大中

❗ デバイスが秘密鍵と生体情報を保持 ⇒ 2つの*Secret*の安全な管理が必要

❗ 登録済みのユーザデバイスからしかサービスにアクセスできない

⇒ 紛失時や買替え時には再度、本人確認と登録が必要（**アカウントリカバリ問題**）

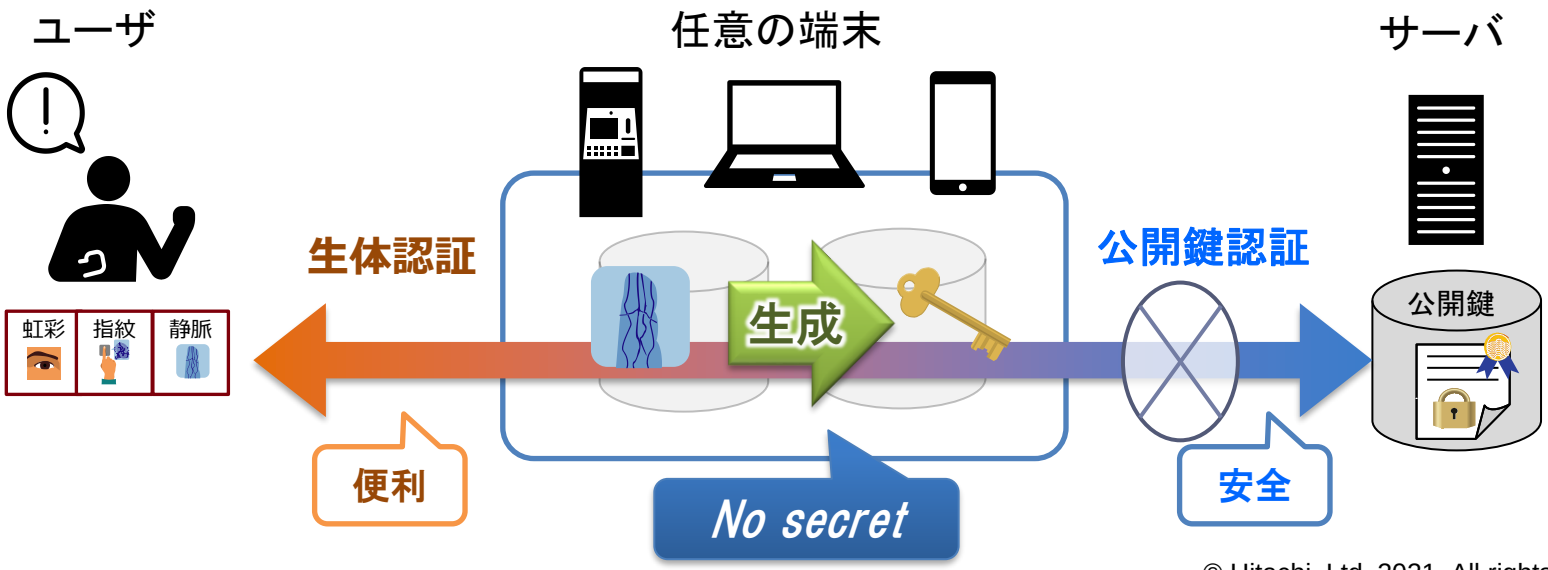
共用端末(ATMやPOSなど)での「手ぶら認証」には適用できない



更なる技術発展の方向性

ユーザデバイスに限定されず、どこからでも安全・便利にアクセス可能に

- 生体認証の利便性、公開鍵認証プロトコルのセキュリティを両立
- ユーザ固有の *Secret* (生体情報, 秘密鍵) は、**どこにも保持しない**
  - 任意の端末から任意のサービス/資産にアクセス可能 ⇒ **デバイスフリー**
- そんなこと可能？
  - 生体情報から都度, 秘密鍵を生成できれば実現可能
  - 認証処理の瞬間のみ *Secret* が存在. 保護すべき時間を極小化することでリスクを極小化



PBI: Public Biometric Infrastructure

HITACHI
Inspire the Next

生体認証と暗号技術をアルゴリズムレベルで融合した認証技術

PBI
【技術要素】
生体電子署名
生体暗号

ＰＢＩの特長

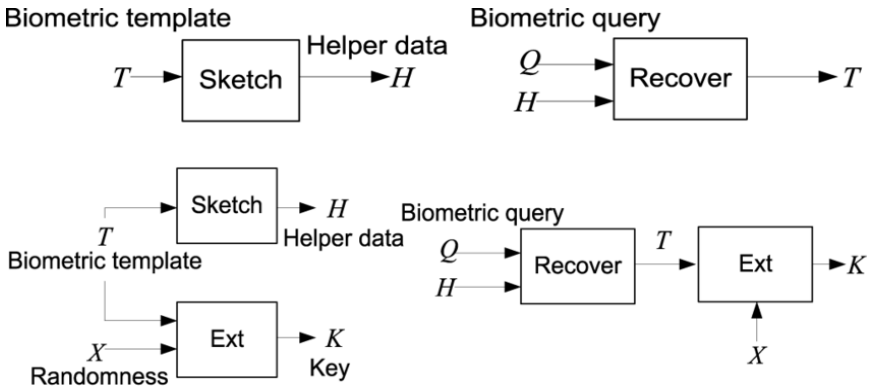
◆ 秘密鍵の保存・管理が不要
- ICカードや暗証番号を使わず、便利で安全なPKIを実現
- 生体情報に基づく確実な本人確認と、公開鍵認証の安全性を両立

◆ 生体情報（特徴情報を含む）の保存・管理が不要
- 生体情報を直接利用せず，公開鍵や署名に「一方向性変換」して利用

PBIの実現技術

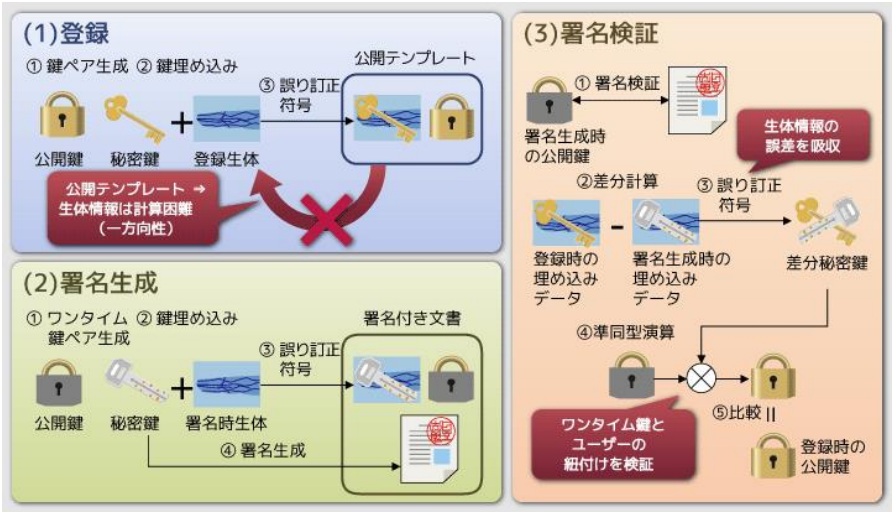
(1) 鍵抽出アプローチ：

- 生体情報の「誤差」を訂正し、秘密鍵を安定的に抽出
- 訂正用情報(補助情報)を登録時に作って保存しておき、認証時に利用
- 既存の暗号技術と組合わせ可能
- 例. Fuzzy Extractor [1,2]



(2)プリミティブ構成アプローチ:

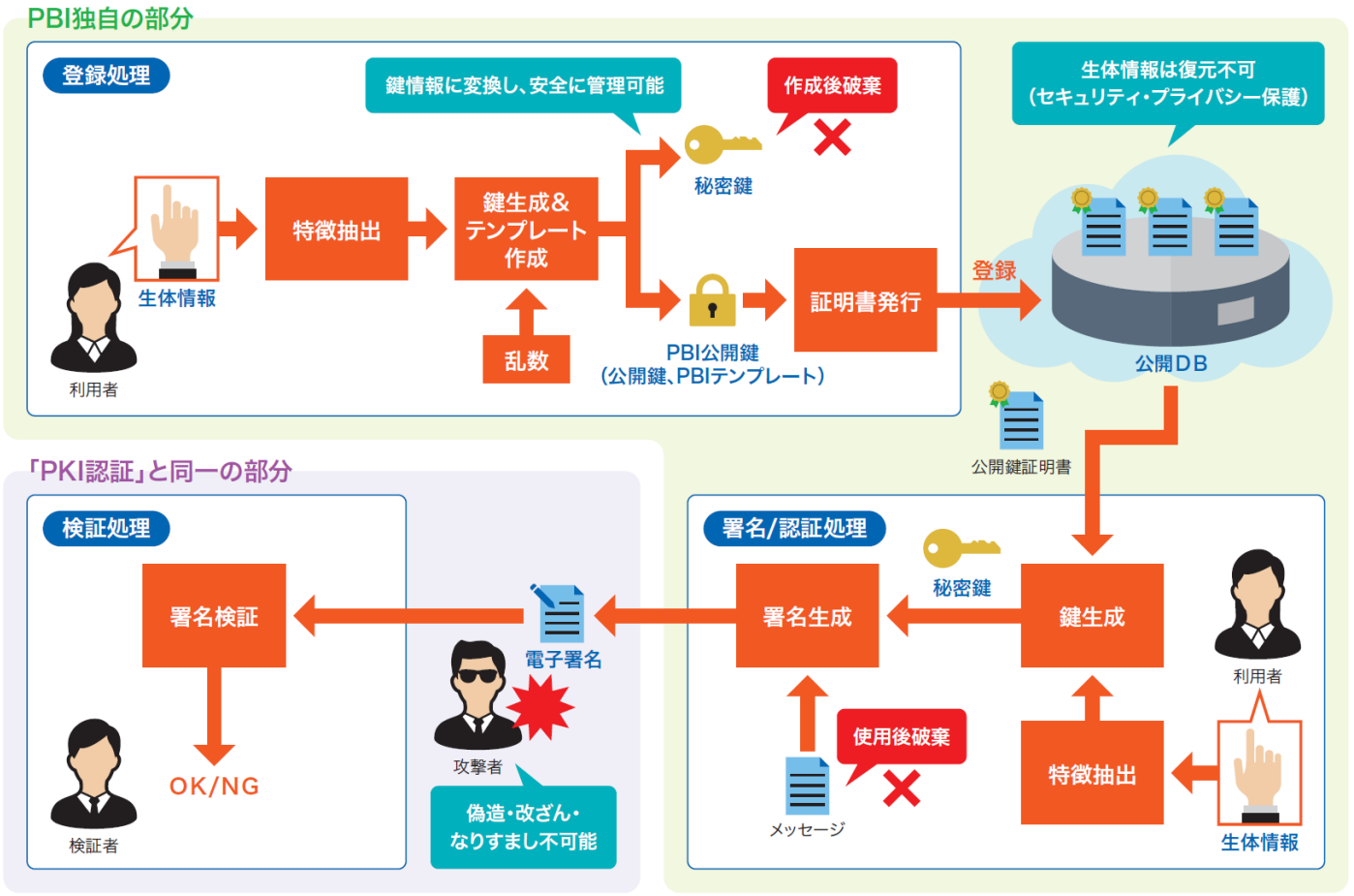
- 秘密鍵に誤差を許容する新しい暗号アルゴリズムを構成
- 認証時に補助情報は不要
- 例: Fuzzy Signature [3]



[1] Y. Dodis, et. al., “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,“ SIAM J. Comput., 38(1):97-139, 2008.
[2] T. Murakami, et. al., “Optimal Sequential Fusion for Multibiometric Cryptosystems,” Elsevier Information Fusion, Vol.32, pp.93-108, 2016.
[3] K. Takahashi, et. al., “Signature Schemes with a Fuzzy Private Key”, International Journal of Information Security, 2019.

PBIシステムの概要

- 生体情報に乱数を作用させ安全なデータ(PBI公開鍵や電子署名)に変換して登録・認証
- 生体情報や秘密鍵はどこにも保存せず。漏洩リスクが最小化され、デバイス所持も不要
- 乱数を変更することで登録データ(PBI公開鍵)の破棄・更新が可能



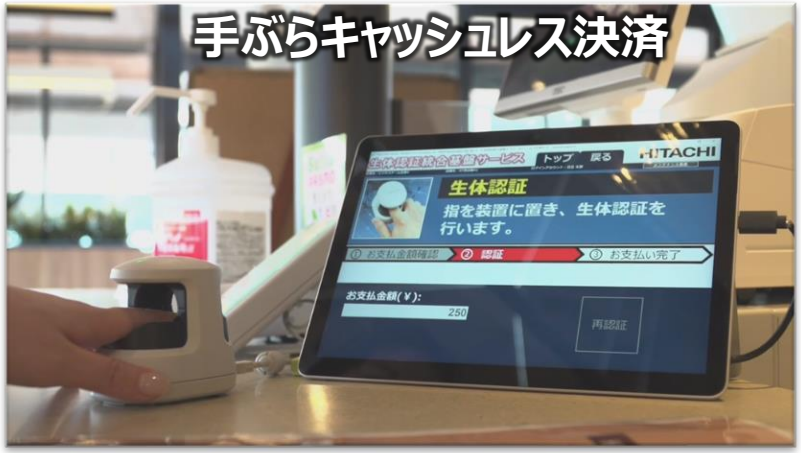
出典：日立ソリューションズ,「公開型生体認証基盤　Biometric Signature Server」, https://www.hitachi-solutions.co.jp/bss/

実用化例

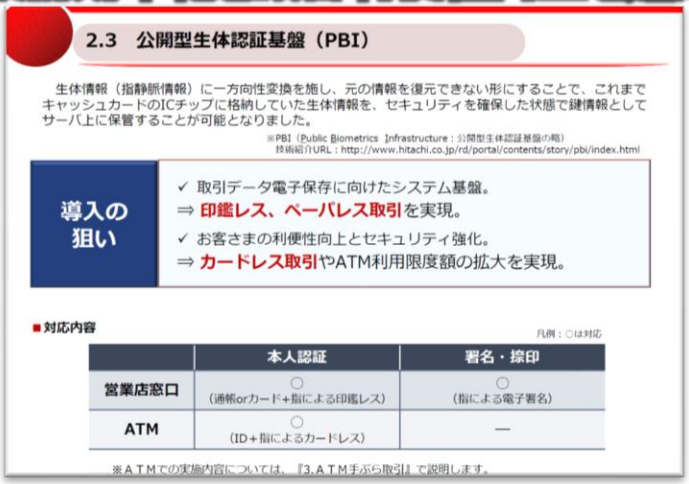
銀行取引、キャッシュレス決済などへ適用進む

手ぶら銀行取引

手ぶらキャッシュレス決済



業務効率化と顧客利便性向上を達成



2.3 公開型生体認証基盤（PBI）

生体情報（指静脈情報）に一方向性変換を施し、元の情報を復元できない形にすることで、これまでキャッシュカードのICチップに格納していた生体情報を、セキュリティを確保した状態で鍵情報としてサーバ上に保管することが可能となりました。

※PBI（Public Biometrics Infrastructure：公開型生体認証基盤の略）
技術紹介URL：http://www.hitachi.co.jp/rd/portal/contents/story/pbi/index.html

導入の狙い

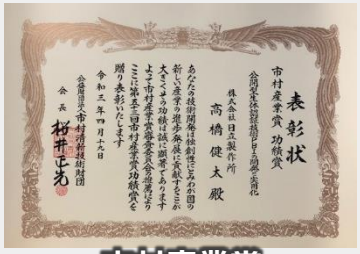
- ✓ 取引データ電子保存に向けたシステム基盤。
  ⇒ **印鑑レス、ペーパレス取引**を実現。
- ✓ お客さまの利便性向上とセキュリティ強化。
  ⇒ **カードレス取引**やATM利用限度額の拡大を実現。

■対応内容　　凡例：○は対応

	本人認証	署名・捺印
営業店窓口	○（通帳orカード+指による印鑑レス）	○（指による電子署名）
ATM	○（ID+指によるカードレス）	—

※ＡＴＭでの実施内容については、『3.ＡＴＭ手ぶら取引』で説明します。

産業界・学術界からの評価



市村産業賞
功績賞
2021年4月

日刊工業新聞
十大新製品賞
増田賞（最高位賞）
2021年1月

米 R&D Magazine社
R&D100 Awards
2020年9月

他、ドコモ・モバイル・サイエンス賞 優秀賞（2016年）
情報処理学会　長尾真特別記念賞(2015年) など

出典：(株)山口フィナンシャルグループ,「新営業店システム導入に伴うペーパーレスの取組について」
日本銀行金融機構局金融高度化センター主催　ITを活用した金融の高度化に関するワークショップ(第３期)
https://www.boj.or.jp/announcements/release_2018/data/rel180314c3.pdf

標準化動向

HITACHI
Inspire the Next

生体情報保護技術の国際標準化が進む

■テンプレート保護技術のスキームに関する標準規格
- ISO/IEC 24745:2011 “Biometric information protection”
- NIST SP800-63B “Digital Identity Guidelines” において
  サーバ側で生体情報を照合する場合の必須要件(SHALL)として引用されている

■テンプレート保護技術の安全性・性能評価に関する標準規格
- ISO/IEC 30136:2018
  “Performance testing of biometric template protection schemes”

国内ガイドラインにおける扱い

■個人情報保護委員会 Q&A [1]
- テンプレート保護技術で適切に保護したデータが万一漏洩しても、
  個人データは実質的に漏洩していないと判断される

■FISCガイドライン [2]
- 「テンプレートのデータ保護について、「取り消し可能なバイオメトリクス認証」
  （Cancellable biometrics）など技術動向を考慮することが望ましい。」

[1] 個人情報保護委員会「「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ」
https://www.ppc.go.jp/personalinfo/faq/2009_APPI_QA/
[2] FISC ガイドライン「金融機関等コンピュータシステムの安全対策基準・解説書」
https://www.fisc.or.jp/publication/guideline_pdf.php

まとめ

HITACHI
Inspire the Next

1. 情報セキュリティ脅威の動向とユーザ認証
   - スマホ決済の不正利用など、近年の脅威の多くは「認証」に関連
   - 「二要素認証⇒安全」とは限らない。暗号学的に安全な認証プロトコルが必要
   - 所有物・記憶は、二要素認証であっても不正譲渡が容易

2. 生体認証への期待と課題
   - 紛失・盗難・忘却の心配がなく、不正譲渡も防止。市場拡大中
   - 課題は生体認証データの保護
   - ユーザデバイス側で生体情報を管理するFIDO規格がデファクト化

3. PBI (Public Biometric Infrastructure)
   - 生体認証と暗号技術をアルゴリズムレベルで融合した、新しい認証技術
   - ユーザデバイスに限定されず、どこからでも安全・便利にアクセス可能
   - 手ぶらの銀行取引・キャッシュレス決済などへ適用進む