

日本銀行 情報セキュリティ・セミナー

生体認証技術の現在地

2026年6月24日

NECフェロー 今岡 仁

自己紹介

今岡 仁

Hitoshi Imaoka

1970年

東京都練馬区出身

1988年(18歳)

巣鴨高等学校 卒業

大阪大学 工学部 応用物理学科 入学

1997年(27歳)

NEC入社 基礎研究所 探索研究部 配属

2002年(32歳)

顔認証の研究開発に携わる

2019年(49歳)

NIST*の顔認証ベンチマークテストにて
5回連続の世界No.1を獲得 *米国国立標準技術研究所
NECフェロー就任

2023年(53歳)

令和5年春の褒章にて紫綬褒章 受章



NECの生体認証技術

1989年研究開発開始。現在世界50以上の国と地域で事業を展開

50年以上の研究開発の歴史を持つ生体認証のパイオニア企業



※NIST: National Institute of Standards and Technology 米国国立標準技術研究所
* 図版内の年月はNEC発表年月です。NISTによるテスト実施時期や結果公表時期とは異なる場合があります。

世界No.1の評価

顔認証だけでなく、主要な生体認証（顔・虹彩・指紋）で世界有数の技術を保有
米国立標準技術研究所（NIST※1）が実施したベンチマークテストにおいて
世界No.1評価を獲得



世界No.1

FRTE 2026 Mar※2

FRTE	2025 Apr※3
FRTE	2024 Feb※4
FRVT	2019
FIVE	2017
FRVT	2013
MBE	2010
MBGC	2009

同FRVT Ongoingで021/8※5,2022/1※6



世界No.1

IREX 2022※7

IREX 10	2021
IREX IX	2018

(Iris Exchange IX)



世界No.1

FRIF TE E1N 2026 Mar※8

MINEX	2016,2006
PFT/PFT II	2013,2009
FpVTE	2012,2003
SlapSeg	2004
ELFT	2007

※1 米国立標準技術研究所(National Institute of Standards and Technology). NISTによる評価結果は米国政府による特定の製品、サービス、企業を推奨するものではありません
※2 FRTE Identification (2026Feb) の Leaderboard [Identification (T>0) by Algorithm] における Gallery: Mugshot, Probe: Mugshot, N=12000000 と Gallery: Visa, Probe: Border, N=1600000 と Gallery: Visa, Probe: Kiosk, N=1600000 と Gallery: Mugshot, Probe: Mugshot ΔT ≧ 12YRS, N=3000000 の4カテゴリでNo.1を獲得
※3 FRTE Identification (2025Mar) の Leaderboard [Identification (T>0)] における Gallery: Mugshot, Probe: Mugshot, N=12000000 と Gallery: Border, Probe: Border ΔT ≧ 10YRS, N=1600000 と Gallery: Mugshot, Probe: Mugshot ΔT ≧ 12YRS, N=3000000 の3カテゴリでNo.1を獲得
※4 FRTE Identification (2024Jan) の Leaderboard [Identification (T>0)] における Gallery: Mugshot, Probe: Mugshot, N=12000000 と Gallery: Visa, Probe: Kiosk, N=1600000 と Gallery: Border, Probe: Border ΔT ≧ 10YRS, N=1600000 と Gallery: Mugshot, Probe: Mugshot ΔT ≧ 12YRS, N=3000000 の4カテゴリでNo.1を獲得

※5 FRVT Ongoing 1:N Identification (2021Aug) の Leaderboard [Identification (T>0)] における Gallery: Mugshot, Probe: Mugshot, N=12000000 と Gallery: Border, Probe: Border ΔT ≧ 10YRS, N=1600000 の2カテゴリでNo.1を獲得
※6 FRVT Ongoing 1:N Identification (2022Jan) の Leaderboard [Identification (T>0)] における Gallery: Mugshot, Probe: Mugshot, N=12000000 と Gallery: Border, Probe: Border ΔT ≧ 10YRS, N=1600000 と Gallery: Mugshot, Probe: Mugshot T ≧ 12YRS, N=3000000 の3カテゴリでNo.1を獲得
※7 IREX 10: Identification Track(2022Sep) の、Two-eye Accuracy、Single-eye Accuracy、Rank Accuracyの3カテゴリでNo.1を獲得
※8 Friction Ridge Image and Features (FRIF) Technology Evaluation (TE) Exemplar One-to-Many (E1N) (2026Feb) の、FpVTE2012 – Class AでNo.1を獲得
* 図版内の年月はNEC発表年月です。NISTによるテスト実施時期や結果公表時期とは異なる場合があります

生体認証技術の概要

様々な認証方法

3種類の認証方法

知識認証

知っていることが前提

暗証番号

パスワード

忘失の可能性、
他人に推測される
可能性あり

所有物認証

所有していることが前提

鍵

カード

証明書

紛失、盗難、貸借の
可能性あり

生体認証



指紋



耳



筆跡



顔



虹彩



DNA



声



静脈



etc.

唯一性により、
なりすましが困難！
忘れない、なくさない！

セキュリティ重視の傾向から知識認証が複雑になり、利便性が低下
知識認証に代わり生体認証の普及が進む

生体認証の方式分類

生体認証は、その特性に応じた活用が必要



- 国内の金融業界では静脈認証がATMの本人確認手段として広く活用
- 近年は、スマートフォンの顔認証や指紋認証などの生体情報を利用したパスキーなど、新たな認証手段の活用が拡大

パスキーとは

パスキーとは

- パスキー（Passkey）は、パスワードを使わずにログインするための認証方式
- ユーザーは、顔認証、指紋認証、PINなどで本人確認を行う
- 裏側では、端末内に保存された暗号鍵を利用して認証
顔認証、指紋認証、PINは暗号鍵を開錠するための手段
- パスキーは実質的にFIDO技術を一般ユーザー向けに使いやすくしたもの
 - FIDO Alliance：標準化団体 / FIDO2：認証技術規格
 - Passkey：FIDO2を利用したユーザー向け実装。

パスキーの課題

- **端末依存**
スマホを紛失、故障、機種変更すると、復旧手続きが必要。
特に高齢者では「スマホを買い替えたら銀行に入れなくなった」問題が起きやすい
- **代替認証の必要性**
パスキーを導入する場合でも、端末を利用できない顧客に対する代替認証・窓口対応・復旧フローを併せて設計する必要がある。

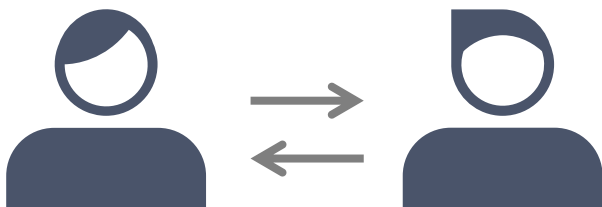
**パスキーは、生体認証(or記憶認証)と所有物認証の組み合わせ
基本的に良い仕組みであるが、所有物認証に起因する難しさもある**

顔認証・虹彩認証の精度の現在

1:1認証と1:N認証

1:1認証

2枚の顔画像が同一人物か否かを判定



スマートフォンやPCなどの
デバイスロック解除や
ATMや決済などの本人確認

**個人を特定するための
「本人確認」領域で活用**

既存分野で多く利用

1:N認証

登録画像データベースから
本人の顔画像を検索

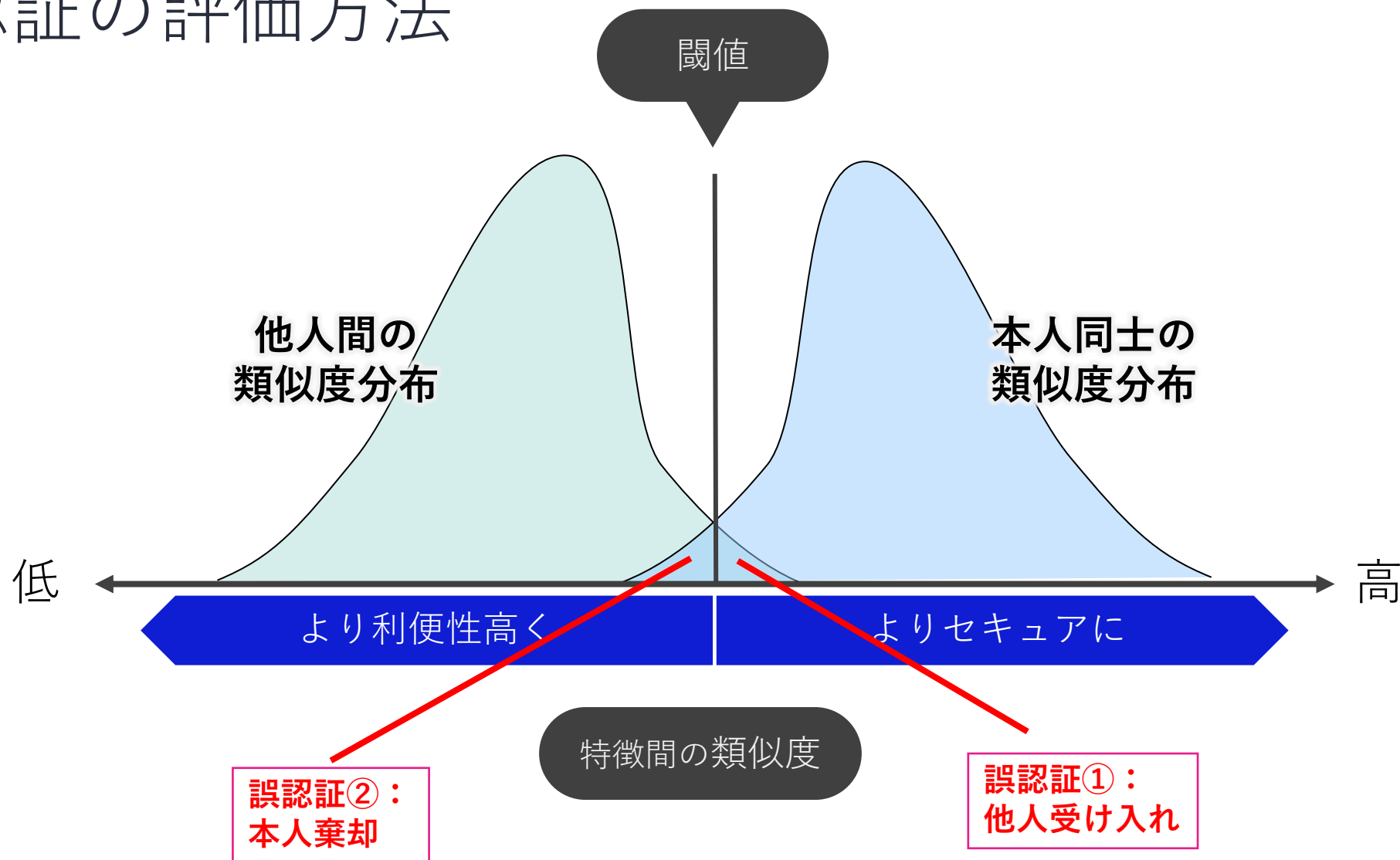


オフィスの入退室管理や
大規模イベント会場の顔パス入場

**多人数の中から
「誰か」を特定する場面で活用**

デジタルIDの普及やシームレスな顧客体験
へのニーズの高まりを背景に、金融を含む
様々な分野で活用範囲の拡大が期待

生体認証の評価方法



一般的な評価方法：他人受け入れ率を一定の値に固定したときの本人棄却率
→ 値が小さいほど高精度

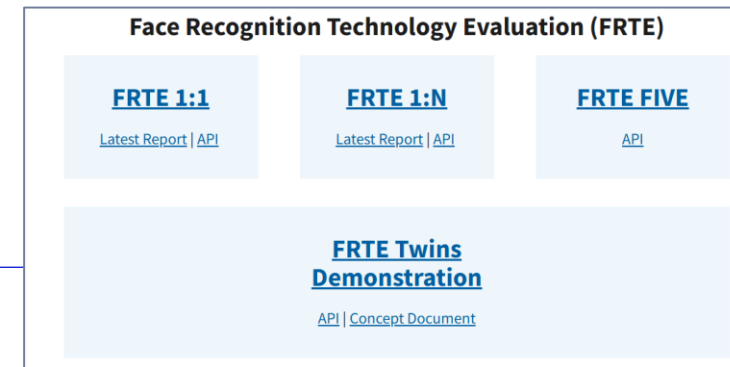
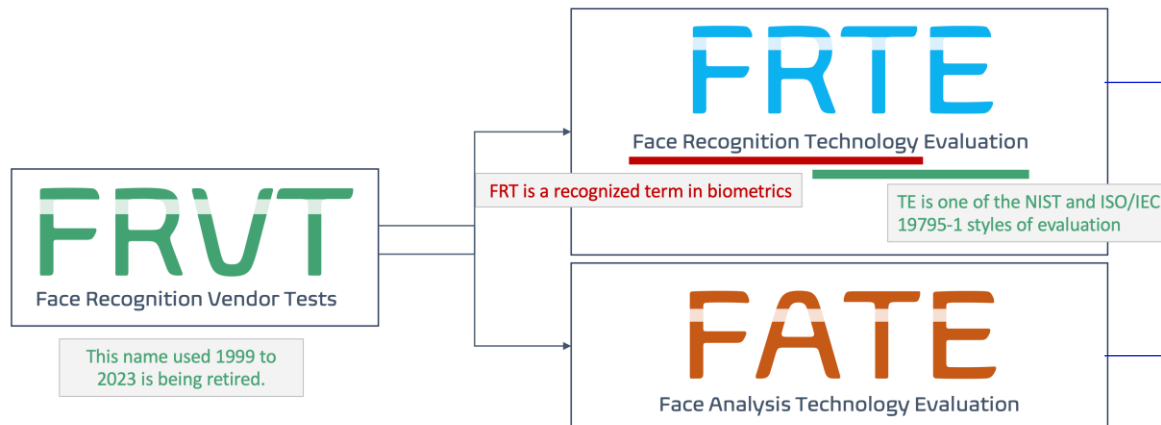
顔認証：Face Recognition Vendor Test(FRVT) とは

評価機関：米国国立標準技術研究所(NIST)

- 技術革新や産業競争力を強化するために設立された機関

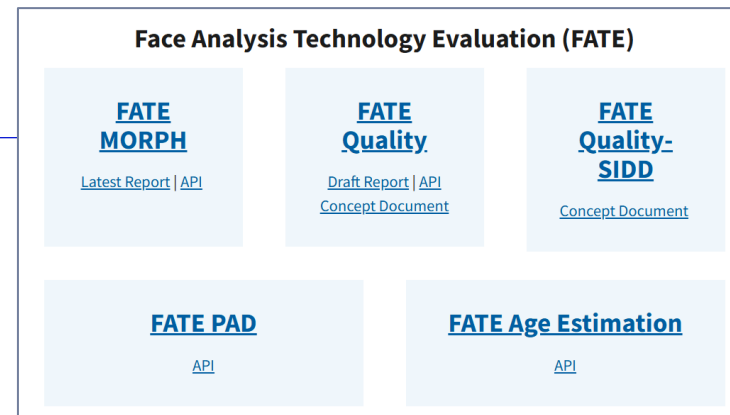
FRVTとは：世界中の有力ベンダーが実力を競う、客観的で公正なベンチマークテスト

- 技術革新や産業競争力を強化するために設立された機関
- 多様な人物（性別・年齢・国籍）が認証対象、実運用を想定
- Ongoing形式で評価され各ベンダーが随時プログラムを提出し評価更新が可能



顔認証評価

- ・ 1:1(静止画)
- ・ 1:N (静止画)
- ・ FIVE(動画)
- ・ Twins(双子)



顔分析評価

- ・ モーフィング
- ・ 品質(全体)
- ・ 品質(個別)
- ・ プレゼンテーション
- ・ 年齢推定

顔認証：Face Recognition Technology Evaluation (FRTE)

1:N Identification

Algorithm	登録人数	マグショット 1200万人	マグショット 160万人	ウェブ カム 160万人	マグショット 横顔 160万人	ビザ 国境 160万人	ビザ キオスク 160万人	ビザ 経年10年 160万人	ビザ 経年12年 300万人
		Mugshot	Mugshot	Mugshot	Mugshot	Visa	Visa	Border	Mugshot
		Mugshot	Mugshot	Webcam	Profile 90°	Border	Kiosk	Border ΔT ≥ 10 YRS	Mugshot ΔT ≥ 12 YRS
gazsmartvisionai_002	2024-12-03	0.0007 ⁽²⁾	0.0005 ⁽¹⁾	0.0057 ⁽¹⁾	0.0460 ⁽¹⁾	0.0013 ⁽¹⁾	0.0443 ⁽¹⁾	0.0211 ⁽⁶⁾	0.0031 ⁽³⁾
nec_010	2025-01-24	0.0007 ⁽¹⁾	0.0006 ⁽²⁾	0.0057 ⁽²⁾	0.0462 ⁽²⁾	0.0015 ⁽²⁾	0.0444 ⁽²⁾	0.0052 ⁽¹⁾	0.0019 ⁽¹⁾
cloudwalk_mt_002	2023-02-24	0.0017 ⁽¹⁷⁾	0.0015 ⁽²⁶⁾	0.0113 ⁽²³⁾	0.0484 ⁽³⁾	0.0016 ⁽³⁾	0.0478 ⁽⁴⁾	0.0157 ⁽²⁾	0.0030 ⁽²⁾
stcon_004	2026-01-26	0.0013 ⁽⁷⁾	0.0007 ⁽⁷⁾	0.0069 ⁽⁶⁾	0.0701 ⁽⁷⁾	0.0018 ⁽⁴⁾	0.0469 ⁽³⁾	0.0181 ⁽⁴⁾	0.0047 ⁽⁸⁾
megvii_004	2023-10-18	0.0011 ⁽⁵⁾	0.0009 ⁽¹⁶⁾	0.0081 ⁽¹³⁾	0.0599 ⁽⁶⁾	0.0019 ⁽⁵⁾	0.0565 ⁽¹⁰⁾	0.0167 ⁽³⁾	0.0053 ⁽⁹⁾
innovatrics_015	2025-09-29	0.0012 ⁽⁶⁾	0.0008 ⁽¹²⁾	0.0065 ⁽³⁾	0.0815 ⁽¹²⁾	0.0021 ⁽⁶⁾	0.0564 ⁽⁹⁾	0.0252 ⁽⁹⁾	0.0040 ⁽⁵⁾
sensetime_011	2026-03-12	0.0009 ⁽³⁾	0.0006 ⁽³⁾	0.0065 ⁽⁴⁾	0.0717 ⁽⁸⁾	0.0021 ⁽⁷⁾	0.0741 ⁽³⁶⁾	0.0229 ⁽⁷⁾	0.0043 ⁽⁷⁾

- NEC
- すべての評価で2位以内
 - 実利用の際に重要な指標である経年変化に対する精度が際立って高い

顔認証 1:N認証：FPIR-FMIR曲線

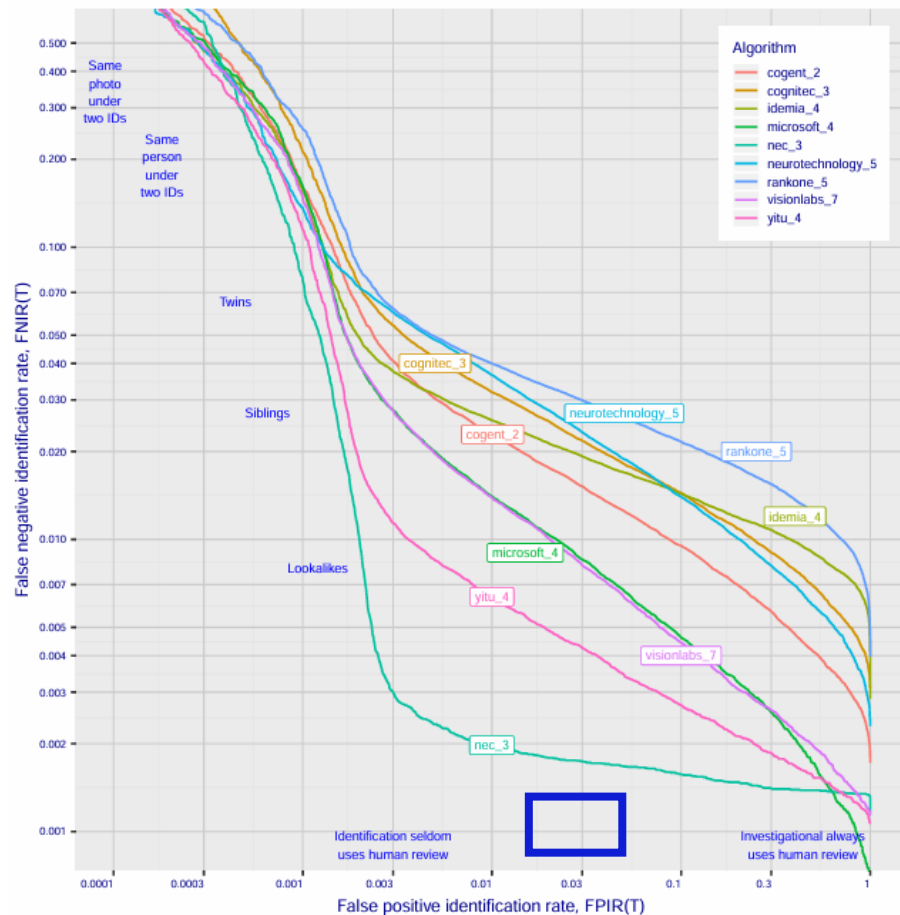
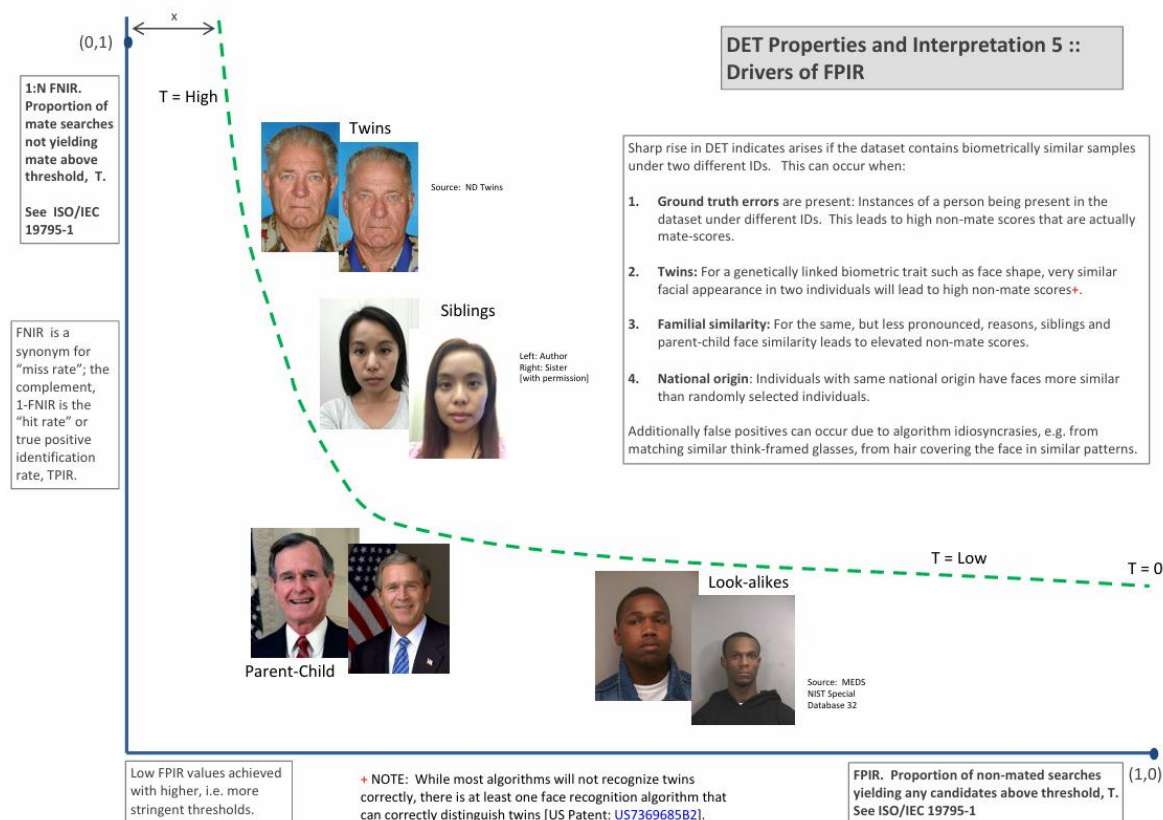


Figure 1: Miss rates across the false positive range

Face Recognition Vendor Test (FRVT) Part 2: Identification | NIST



FRVT2018の評価：双子、親子、兄弟姉妹、親族が性能低下の要因の一つ

虹彩認証 Iris Exchange (IREX) 10: Ongoing Evaluation of Iris Recognition

	Matcher	Submission Date	Accuracy (FNIR)	Search Time (sec)	Template Creation Time (sec)	Template Size (bytes)	FTE Rate
1	neurotechnology_020	2026-05-05	0.0020 ± 0.0003	4.6 ± 0.4	2.0 ± 0.3	19 349 ± 23	0
2	nec_007	2022-12-22	0.0022 ± 0.0004	12 ± 3	1.03 ± 0.06	18 280 ± 0	0
3	innovatrics_002	2023-04-05	0.0024 ± 0.0003	3.2 ± 0.6	1 ± 1	8 280 ± 0	0.000007
4	idemia_002	2023-06-13	0.0026 ± 0.0004	11 ± 5	1.5 ± 0.1	130 879 ± 6 017	0
5	hikvision_007	2023-01-15	0.0029 ± 0.0004	16 ± 7	3 ± 1	15 404 ± 0	0
6	thales_001	2022-12-10	0.0030 ± 0.0004	14 ± 6	1.6 ± 0.6	43 362 ± 0	0
7	irisid_012	2026-04-10	0.0034 ± 0.0004	8 ± 2	0.82 ± 0.02	11 268 ± 0	0.000007
8	omnigarde_000	2026-02-03	0.0041 ± 0.0005	1.61 ± 0.09	2.02 ± 0.06	38 530 ± 0	0

2026年5月21日時点の結果 [FNIR @ FPIR = 0.01](#)__Enrolled Population: 500K people

<https://pages.nist.gov/IREX10/>

生体認証への攻撃に対する防御方法と防御性能

攻撃方法の全体像

プレゼンテーション攻撃/モーフィング/敵対的攻撃の比較

	プレゼンテーション攻撃	モーフィング攻撃	敵対的攻撃
主な攻撃対象	生体認証センサー (カメラ/画像取得装置)	登録画像 (パスポート写真、ID登録画像)	AIモデルの判定ロジック (顔認証、なりすまし検知、 モーフィング検知、ディープフェイク検出)
攻撃対象レイヤー	画像取得レイヤー (取得時)	画像/データレイヤー (画像そのもの)	モデル/推論レイヤー (内部表現と決定境界)
典型的な攻撃手法	・印刷された写真 (プリント攻撃) ・画面上での動画再生 ・マスクまたは物理的な人工物	2人以上の顔の合成 ・ランドマークベースのモーフィング ・GANベースのモーフィング ・拡散モデルベースのモーフィング ・印刷・スキャンによるモーフィング	・視覚的に検知困難なノイズ注入 ・リアルタイムでの敵対的変換 ・光や投影パターンを用いた物理的攻撃
対策(例)	・受動的生体検知 (テクスチャ、動き、反射率) ・能動的生体検知 (チャレンジ・レスポンス： まばたき、頭部動作) ・マルチモーダルPAD (RGB+赤外線+深度) ・管理された画像取得環境	・登録時確認のためのS-MAD (単一画像MAD) ・信頼できる参照写真を用いたD-MAD(差分型MAD) ・発行時の信頼できる画像取得 ・疑わしいケースに対する人による審査	・敵対的学習 (ステップ勾配攻撃よりサンプル生成) ・ランダム化スムージング (証明可能な頑健性) ・入力データの前処理 (正規化、再エンコード) ・モデルの多様性/アンサンブルアプローチ

プレゼンテーション攻撃

プレゼンテーション
攻撃とは



印刷された顔画像



画面上で動画再生



マスクまたは物理的な人工物

実際に使われる
技術の例

- 3D形状確認
例：Apple Face ID、一部Android端末 ⇒ 顔の奥行きを測定。写真は平面なので弾ける。
- 赤外線（IR）
近赤外画像を撮影。本物の顔と写真ディスプレイは反射が異なる。皮膚反射特性、目の周辺構造、顔表面の質感など
- Active Illumination
赤外線パターンを照射。本物の顔と写真ディスプレイでは反射が異なる
- 動き解析
例：まばたき、微小頭部運動、表情変化
- テクスチャ解析
画像から印刷物、ディスプレイマスクを識別

プレゼンテーション攻撃：iBetaによる性能評価

- ISO 30107-3は「PAD（Presentation Attack Detection）をどう評価するか」を定義した試験標準
- iBetaはNIST/NVLAP認定試験機関として、その試験を実施
- iBetaは独自に攻撃難易度を定義 Level 1, Level 2, Level 3
- **Level 3は2025年以降に導入された最新レベルで、深刻な金融詐欺や国家レベルの攻撃を想定**

iBetaの攻撃難易度

<https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/>

レベル	所要時間	専門知識	アーティファクト（攻撃媒体）の入手元	許容限界	攻撃例
1	被験者または生体種別ごとに8時間	なし	一般的な家庭やオフィス環境で容易に入手できる協力者および機材	侵入成功率または照合成功率 0% を許容	写真、動画リプレイ
2	被験者または生体種別ごとに2～4日	中程度：対象モダリティで少なくとも1回のPAD評価に参加し、対象システムの生体検知機能について理解している	協力者は必要。機材はより高価（例：3Dプリンタ、レジンマスク、ラテックスマスク）	侵入成功率または照合成功率 1% を許容	3Dマスク、高品質アーティファクト
3	生体種別ごとに7日、被験者ごとに4日	高度：対象モダリティのプレゼンテーション攻撃について少なくとも16時間の調査経験があり、対象モダリティで少なくとも10回のPAD評価に参加した経験を有する	協力者に加え、被験者データ取得のための潜在的情報源を利用。特殊環境やアクセサリを用いた高精細・高リアリズムな顔マスクなどを使用	侵入成功率または照合成功率 5% を許容	ハイパーリアルマスク、カスタム攻撃、最適環境

**Android, iPhoneのバージョンもあり、この評価がすべてではない。個々の認証デバイスでの性能が重要
レベル1, 2が中心だったが、レベル3に到達するベンダが出てき始めている**

モーフィング攻撃に対する検知性能 NIST評価

NISTIR8931報告書(2023/09/20)
This track is currently CLOSED

- 45組織/82アルゴリズム
- APCER (Attack Presentation Classification Error Rate)→ 攻撃画像を見逃す率 (低いほど安全)
- BPCER (Bona Fide Presentation Classification Error Rate)→ 本物を誤って攻撃と判定する率 (低いほど利便性が高い)
- 攻撃方法を公開しているデータと非公開のデータの両方で評価



印刷された写真やタブレットの動画による攻撃

- 複数ベンダで APCER = 0 (攻撃見逃しゼロ) BPCERも 0.01%未満という非常に高い性能
- 多くのアルゴリズムで、動画入力の方が静止画よりPAD性能が向上



シリコンマスクによる攻撃

- 複数方式で APCER $\leq$ 1% BPCER $\leq$ 1%に近い性能を達成しており、検出技術は比較的成熟

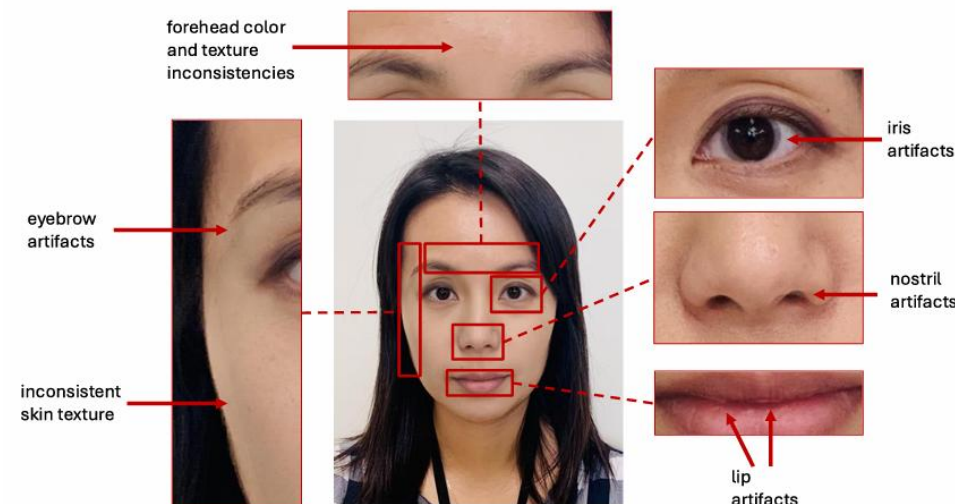
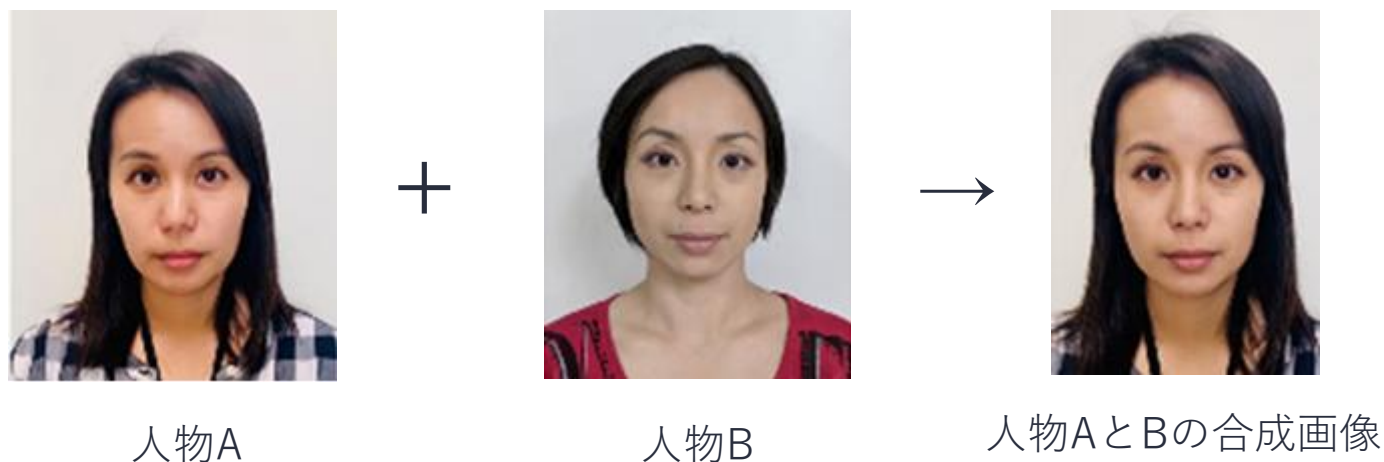
課題

- ズームした写真や動画、一部の非公開PAタイプでは性能が大きく低下し、未知の攻撃への一般化が今後の課題

https://pages.nist.gov/frvt/html/frvt_pad.html

モーフィング攻撃

モーフィング攻撃とは、顔認証・本人確認で使う写真を、2人以上の顔を合成した“中間顔”にして登録する攻撃



このモーフ画像は、AにもBにもある程度似ている。

Aが通れる、Bも通れるという状態を作ることができる可能性が生じる。
一方で不自然な顔画像であるため、AもBもどちらも通れない可能性もある

モーフィング加工の痕跡例

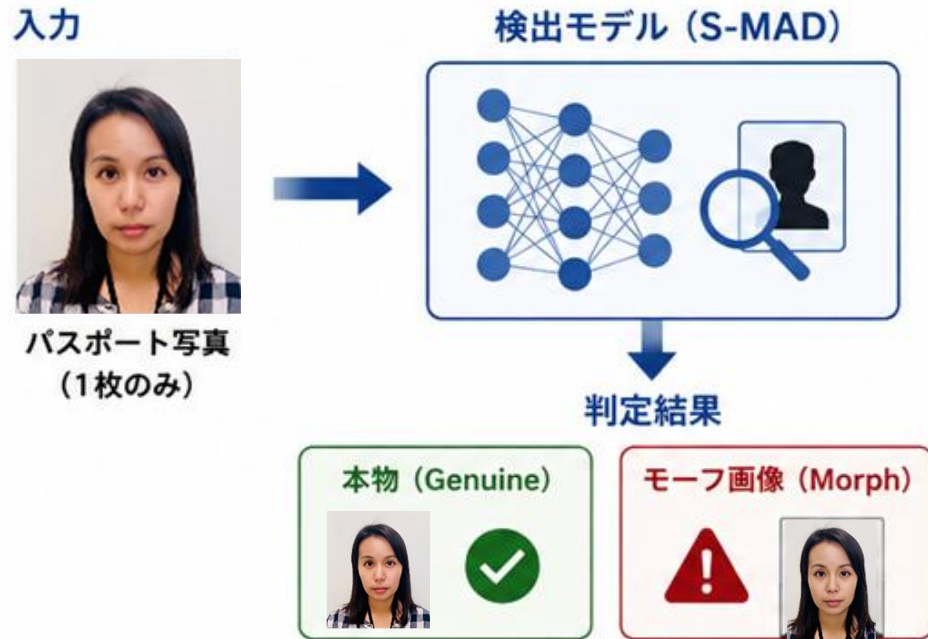
https://pages.nist.gov/frvt/reports/morph/fate_morph_4B_NISTIR_8584.pdf

モーフィング攻撃の防御方法

S-MAD (Single-Image Morphing Attack Detection)

単一画像モーフィング検知

単一画像のみをみて、モーフィング画像かどうか判定

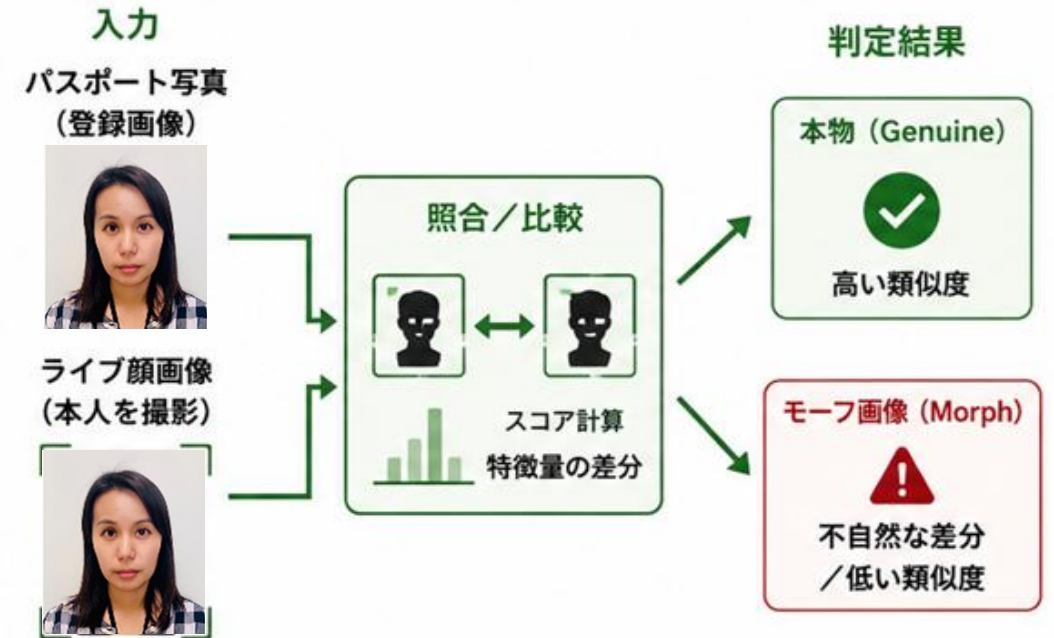


一枚の写真の中の不自然さや合成痕跡を検出

D-MAD (Differential-Image Morphing Attack Detection)

差分型モーフィング検知

登録画像とライブ画像を比較して、モーフィング画像かどうか判定



登録画像とライブ画像の違い、差分を利用

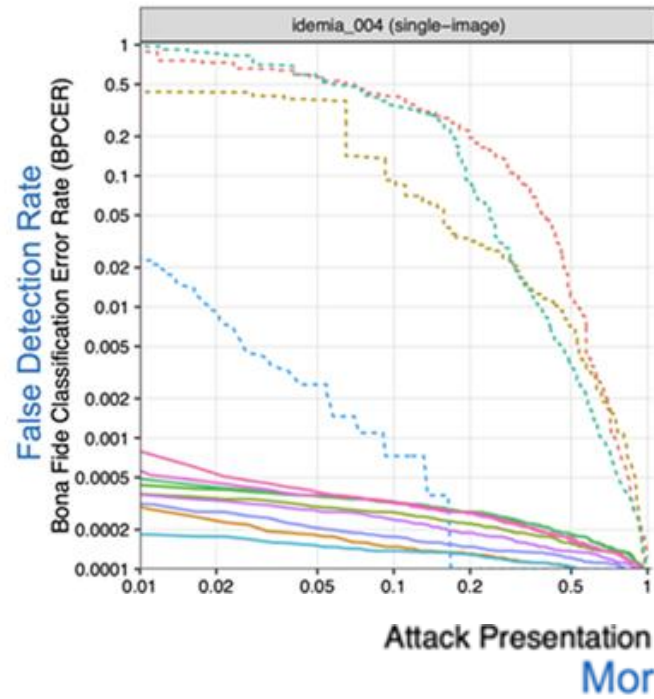
- AI進化への追従：ディープフェイクなどによる超高精細な合成は見落とすリスクあり
- 画質依存：写真の解像度が低い場合、ノイズなのか合成痕跡なのかの判別が難しい

- インフラの必要性：その場で本人の顔を正確に撮影するため、カメラや照明環境が必須
- 処理コスト：2つのデータをリアルタイムで比較するためS-MADに比べシステム負荷高

モーフィング攻撃に対する検知性能の比較 NIST評価

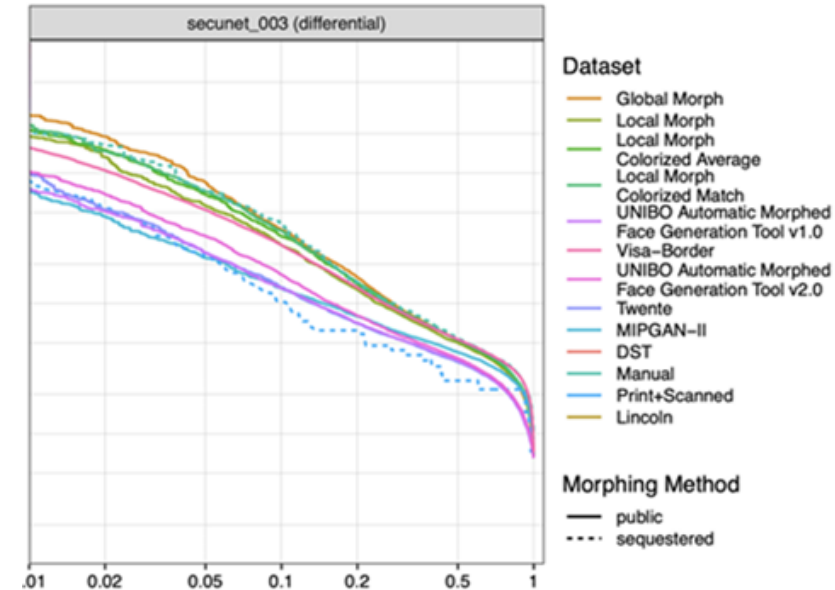
S-MAD

(Single-Image Morphing Attack Detection)



D-MAD

(Differential-Image Morphing Attack Detection)



- S-MADは特定のモーフ生成器で学習している場合には有効だが、未見のモーフタイプでは精度が非常に悪いことが多く、現時点では未知手法への汎化性が低い
- 一方、D-MADについては、公開手法・秘匿手法を含むすべてのモーフ方式に対して性能がより一貫している

https://pages.nist.gov/frvt/reports/morph/fate_morph_4B_NISTIR_8584.pdf

https://pages.nist.gov/frvt/html/frvt_morph.html

今後に向けて 1:N認証の進展

1:N認証の現在：顔認証はこれからどのように広がっていくのか？

認証精度の向上により、徐々に実利用が広がりつつある

NEC本社 オフィス入退場（顔認証）



NEC本社 顔認証決済（顔認証＋番号）



JR東日本/上越新幹線実証実験（顔認証）



マルチモーダル認証（顔認証＋虹彩認証）



顔・虹彩のマルチモーダル認証

ウォークスルー型の顔・虹彩マルチモーダル生体認証技術のプレスリリース(2025年12月)

NECは厳格な本人確認が求められるシーンでも、手ぶらで立ち止まることなくストレスフリーに認証を行う、ウォークスルー型の顔・虹彩マルチモーダル生体認証技術を世界で初めて開発。世界No.1の認証精度を有するNECの顔認証技術と虹彩認証技術を組み合わせ、歩いている利用者を屋内外問わず高精度かつ高速に認証



https://jpn.nec.com/press/202512/20251203_02.html

虹彩と顔を組み合わせることによる一般的なメリット

- ・ 3つのモーダルの統合(顔/左目/右目)より、高精度認証
- ・ プレゼンテーション攻撃、モーフィング攻撃に対して強固
- ・ 虹彩と顔が同時に取得できることにより利便性の維持

World IDプロジェクト

- ・ OpenAIのサムアルトマンが共同創業者であるTools for Humanityが開発
- ・ 虹彩認証がメインで、顔認証が補助
- ・ オーブと呼ばれる専用端末で認証

生体認証の安心を支える仕組みづくり

生体認証とデジタルエシックス（倫理）

公平性

透明性

プライバシー
保護

...

生体認証にかかわらず、AI・デジタルの課題
技術だけでなく、「使う側のルールや配慮」が問われる時代
一方で、法やガイドラインだけでは明確に決められないことも多
く、本当に使ってよいのか悩んでしまう状況

みんなが「安心して使える」仕組みであるために
エシックス（倫理）は不可欠

デジタル化がもたらす様々な懸念

データ収集 と利用の 危険性	データ漏洩 と不正利用	オープン データ 取り扱い	個人情報 保護	セキュリ ティ	サイバー いじめ	オンライン ハラスメン ト
デジタル フットプリ ント	フェイク ニュース	デジタル 依存症	炎上リスク	監視社会	デジタル リテラシー	デジタル デバイド
AIによる ホワイトカ ラー失業	AI安全性	AIアルゴリ ズムの 透明性	AIによる 人間判断の 関与	AI軍事利用	AI判断に おける 多様性確保	労働搾取

...

デジタル化を進めることに今一歩難しさを感じる

エシックスがもたらすアドバンテージ



イラスト: iStock.com/Mykyta Dolmatov

法・ルール・ガイドラインの
根底に、エシックス・文化・
社会がある

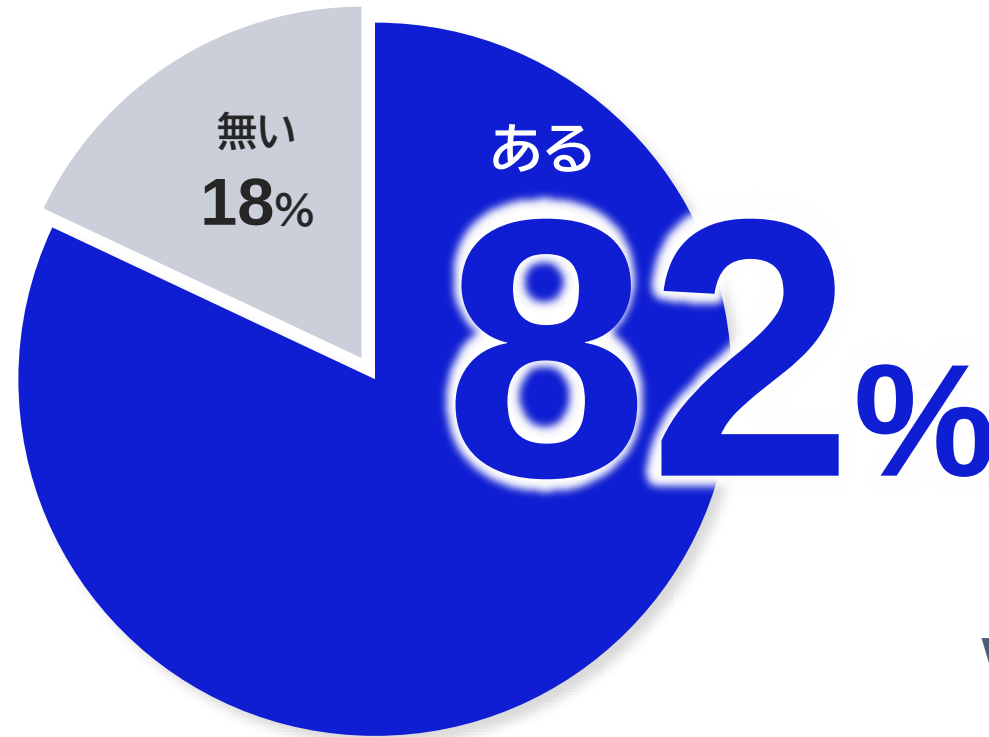
物事を進めていくうえで、
氷山の下が大きい

**DXを進めるためには、様々な懸念と対峙する必要があり、
エシックスは、これらの懸念に対処ためのツール**

■約8割の消費者が、サービス利用時に「不信感」を抱いた経験を持つ

Q. 過去に、『デジタル技術を活用して提供されているサービス』を利用した際に不誠実だと感じた経験はありますか。

全回答者 [n:1,597]



- 消費者は、透明性の欠如による「見えない不安」、不親切なUX/UIによる「ワナのような設計」に不信感を持つ

82%の人が感じた不誠実さの内容

透明性の欠如

何度も広告や案内が出てくる (43%)

誤解を招く表示や誘導 (クリック誘導など) (33%)

自分の情報が知らないところに
勝手に渡ってしまう (32%)

意図しない有料サービスに申し込まれてしまう
恐れ・不安がある (31%)

個人情報の取り扱いに関して透明性がなく不安
(31%)

意図的ともとれる不親切なUX/UI

退会や解約のやり方がわかりにくい (37%)

操作ミスを誘発する画面設計 (27%)

不明瞭な料金体系や追加費用 (25%)

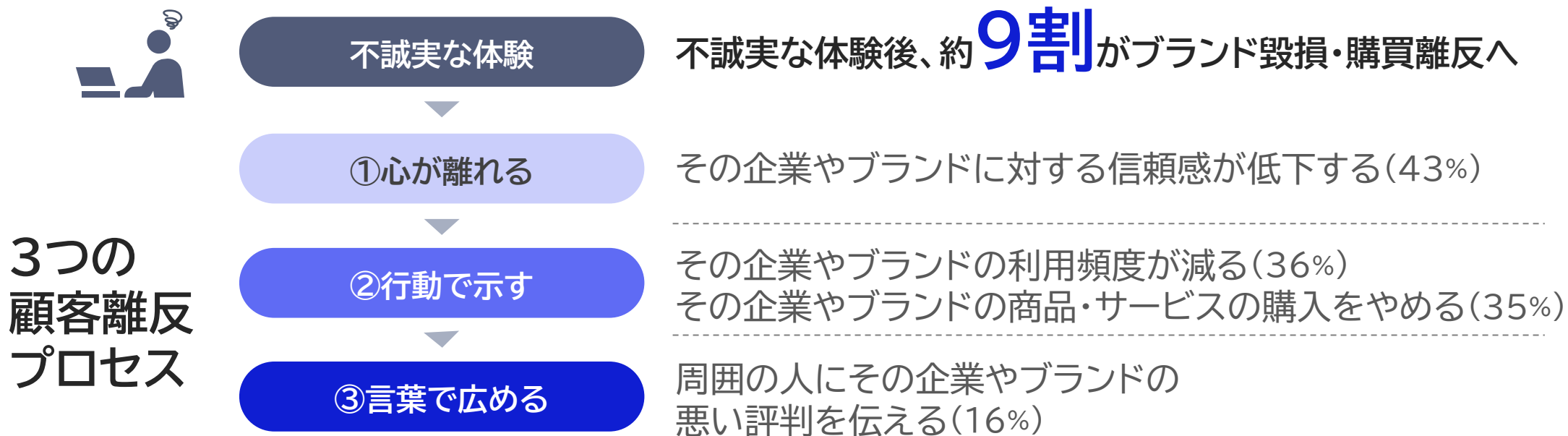
意図的に操作を複雑にして
利用者を引き留めようとする (25%)

NEC 『AI時代に変化する消費者意識調査2025』, https://jpn.nec.com/dx/consumer_survey/index.html

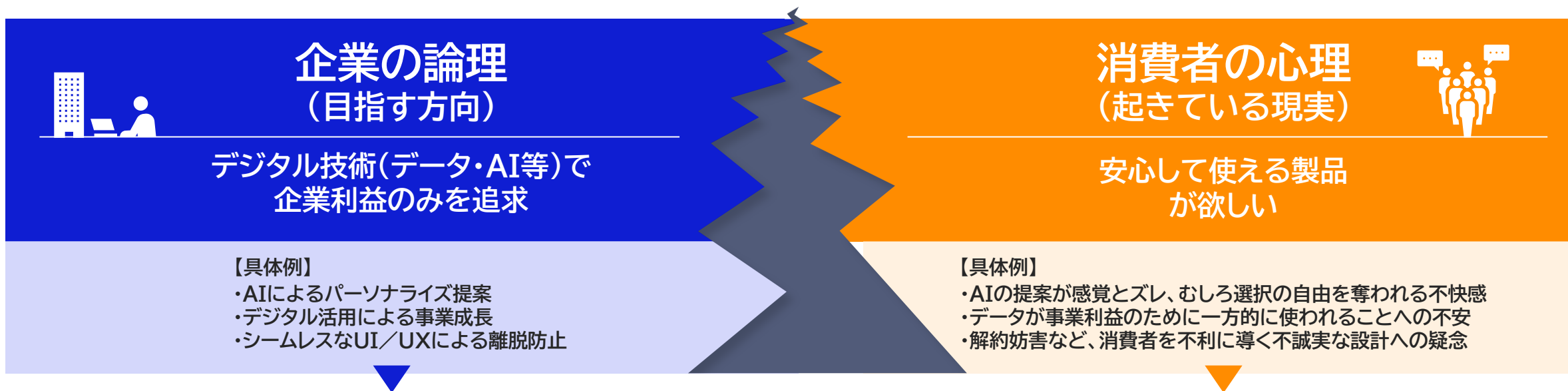
- 不誠実な体験をした顧客は、①「心」が離れ、②「行動」で示し、③「言葉」で広めるという「3つの顧客離反プロセス」を引き起こす

Q. そのような不誠実な体験をした場合、あなたの購買行動や、その企業・ブランドに対する印象にはどのような変化があると感じますか。

AIやデータを活用したサービスに対し不誠実だと感じたことがある人[n:1,305]



企業と消費者の間にある、深い溝



…これらは、
本来ポジティブな企業活動である

企業のあり方を問う「覚醒した顧客」の登場や、
「プロセス」を評価する新たな価値観

この深い溝を埋め、持続的な信頼関係を築くための、新たな指針が求められている
両者をWin-Winの関係にするための「デジタルエシックス(倫理)」

デジタルエシックスによる社会実装にあたって

■ デジタルエシックスは、社会を前向きに進めるための原動力になる

- 技術がアクセルで、エシックスがブレーキの役割と考えていませんか？

■ プロセスの最初から組み込むことが重要

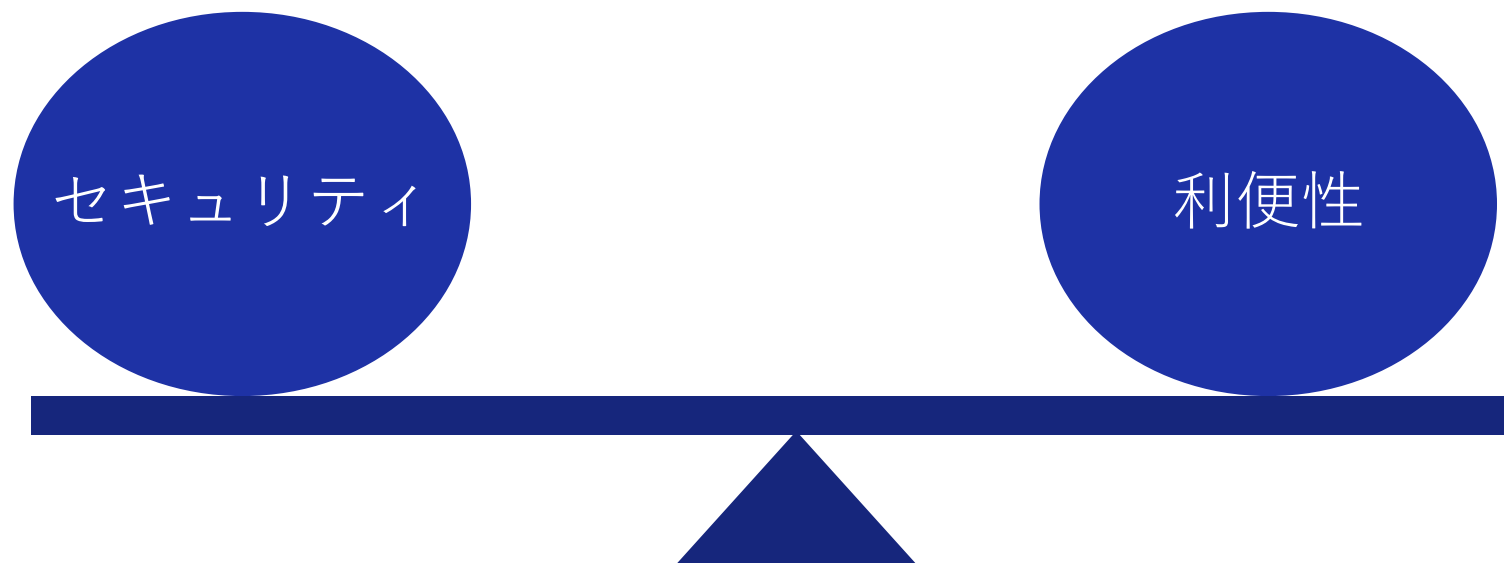
- 最後に管理部門に確認して、
プロジェクト全体が失敗に終わることはありませんか？

■ 我々の仕事は社会的な状況を踏まえたうえでの判断の連続

- エシックスは特定の役割の人だけ考えればよいと思っていないですか？

まとめ

- 顔認証を中心として、生体認証の精度、攻撃に対する防御について説明
- 生体認証の活用事例、デジタルエシックスの考え方を紹介
- セキュアな本人認証を実現するには、
生体認証を活用したホルダーバインディング（所有者との結び付け）が必須**
- 世の中に広がっていくサービスになるには、
セキュリティと利便性のバランスが重要**



NEC

\Orchestrating a brighter world