



# 顔認証技術・なりすまし防止技術 Safte（セイフ） サービス概要資料



# 1. 会社概要

# 2. 顔認証Saffe(セイフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

# 1. 会社概要

## 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

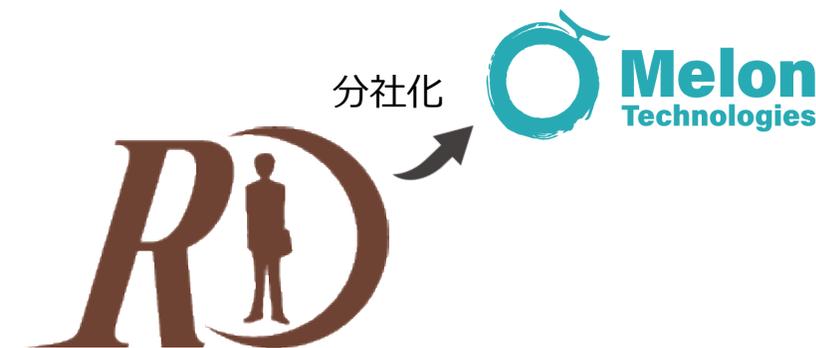
Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

社名	株式会社Melon Technologies
設立	2023年12月1日
資本金	7,632.5万円
代表	代表取締役 齋藤 英樹
所在地	〒150-6018 東京都渋谷区恵比寿4-20-3 恵比寿ガーデンプレイスタワー18階
連絡先	03-5789-5527(代表) / Saffe関連お問合せ E-mail: sales@melon.jp
ホームページ	<a href="https://www.melon.jp">https://www.melon.jp</a>
事業内容	<p>I .プロダクト・ディベロップメント事業</p> <ul style="list-style-type: none"><li>・ <b>顔認証Saffe (セイフ)</b> を中心としたAI関連製品 / サービスの開発・販売・運用保守をおこなう事業</li></ul> <p>II .ソフトウェアコンサルティング事業</p> <ul style="list-style-type: none"><li>・ AI・IoT領域を中心としたソフトウェアコンサルティング</li><li>・ ソフトウェア開発サービスを提供する事業</li></ul>



社名	株式会社R.D.Works
設立	2003年8月28日
資本金	5,001万円
代表	代表取締役 齋藤 英樹
所在地	〒150-6018 東京都渋谷区恵比寿4-20-3 恵比寿ガーデンプレイスタワー18階
連絡先	03-5789-5740(代表) / Saffe関連お問合せ E-mail: saffe@rdworks.co.jp
ホームページ	<a href="https://www.rdworks.co.jp">https://www.rdworks.co.jp</a>
事業内容	<p>I .経営コンサルティング事業</p> <ul style="list-style-type: none"> <li>・ 業務プロセス合理化に関する提案および実現支援</li> <li>・ 情報システムに関する構想策定、および構築・導入支援</li> <li>・ 上記活動に伴うプロジェクトマネジメント支援</li> </ul> <p>II .ソフトウェア事業</p> <ul style="list-style-type: none"> <li>・ ソフトウェアの販売・開発・<b>顔認証Saffe (セイフ)</b> 導入支援</li> <li>・ 上記導入済みの運用保守</li> </ul>



①	代表者名	齋藤 英樹
②	現職	株式会社R.D.Works 代表取締役 株式会社Melon Technologies 代表取締役
③	最終学歴	1997 慶應義塾大学 商学部 卒業
④	職務経歴	1997年 プライスウォーターハウスクンサルティング（現：PwCコンサルティング）入社 2001年 独立開業 2003年 株式会社R.D.Works設立
⑤	主な実績	多くの大企業へコンサルティング・ビジネスソリューションを提供 ビジネス構築力・コンサルティング会社の発展を牽引 日系企業による海外ビジネスの多様なサポート実績 AI・IoT・顔認証領域サポートのトラックレコード
⑥	Melon Technologies 設立に至る経緯	2019年 <b>顔認証ビジネス開始、日本・アジアで顔認証Saffe（セイフ）を代理販売</b> 2023年 新会社 株式会社Melon Technologies 設立



## 1. 会社概要

## 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

## Saffe (セーフ) は英国・ブラジルを拠点とする顔認証技術に特化したIT企業です

Saffeの認証技術は英国の金融庁、FCA(英国金融行為規制機構)にも認めれました

現在、AI技術は目覚ましい進歩と発展を遂げておりますが、Saffeは遡ること2008年、ドイツのフランホッファー研究所で生まれた認証技術で既に16年の歳月、顔認証・なりすまし防止の研鑽が積み重ねられています。その過程で IEEE の生体認証コンペティションでNo1の結果を勝ち取り、近年はアメリカ国立技術標準研究所(NIST)の評価も世界トップレベルであることが証明されました。AI技術の黎明期からの技術研鑽が、現在のパイオニアとしてのポジションを支えています。

### Board of Directors



#### CEO - André Coelho

- UBS , Senior cooperate officer
- Fator Bank



#### COO - Eduardo Carvalho

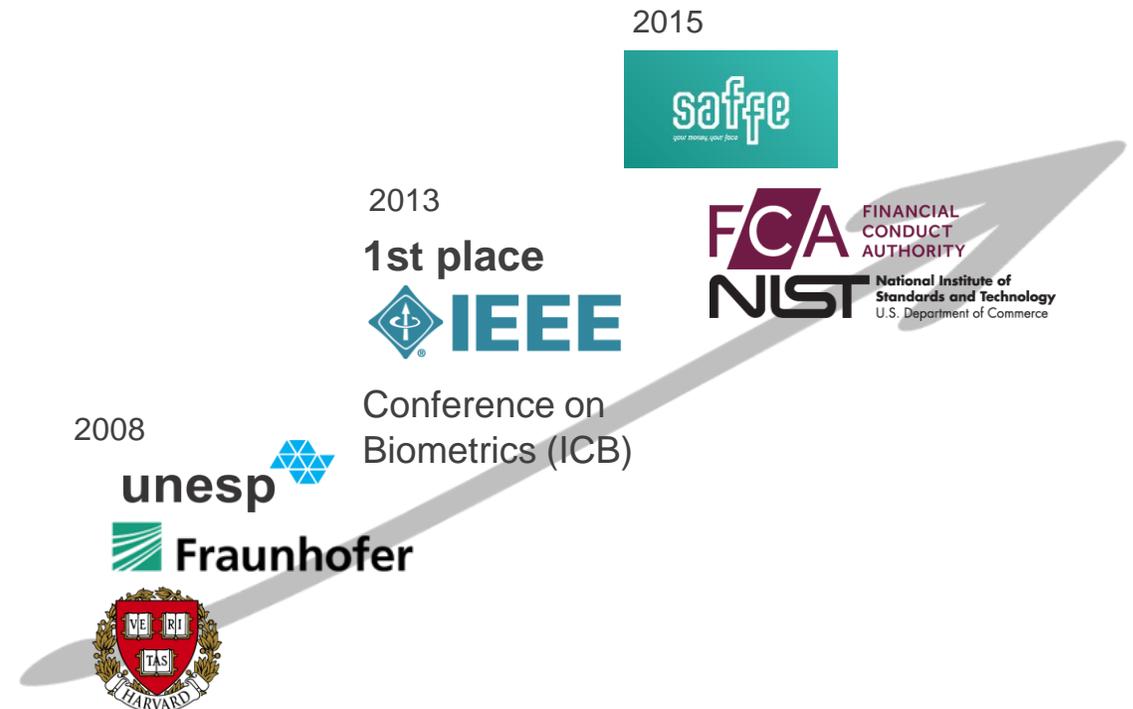
- Fidelity , Founder executive
- BSI



#### CTO - Giovanni Chiachia

- PhD Harvard | Unicamp
- Master Fraunhofer | Unesp

### Biography of Saffe



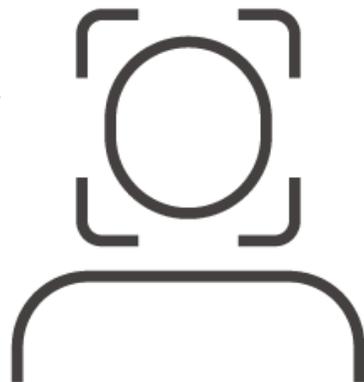
## Saffe社の顔認証技術は世界トップレベルの精度を誇ります

顔認証は **本人を確認する顔認証** と **生体を検知するなりすまし防止** の2つの技術から構成されており、両技術ともNIST(アメリカ国立標準技術研究所)の評価で、世界トップレベルの精度であることが証明されています。

### 顔認証 ( 本人確認 )



OK



グローバルランキング **14位**

### なりすまし防止 ( 生体検知 )



グローバルランキング **1位**

NIST(アメリカ国立標準技術研究所)による評価で **世界TOP14** にランキングされました。(2019年4月時点)

**Saffe社顔認証精度 : 99.46% ※**

入管・防衛などに納入している Panasonic や Toshiba など、名だたる国内メーカー系顔認証と同等の品質であることを担保。  
※精度は ±0.07% の微差です。

**世界水準の顔認証を  
低コストで提供可能。**

普及価格帯であることを強みに、  
弊社は顔認証の社会普及に貢献  
します。

Overall Rank	Vendor	Rank Average	CONSTRAINED & COOPERATIVE BENCHMARKS								NON-COOP.	
			VISAMC 0,0001	Rank	VISA 0,000001	Rank	VISA 0,0001	Rank	MUGSHOT 0,00001	Rank	WILD 0,0001	Rank
1	VisionLabs	3,2	0,0037	2	0,0066	3	0,0012	3	0,0041	1	0,0285	7
2	Imperial College London	5,6	0,0067	6	0,0108	8	0,0022	6	0,0072	5	0,0276	3
3	Vocord	5,8	0,0062	4	0,0102	7	0,0016	4	0,0082	8	0,0282	6
4	Shanghai Yitu Technology	6,2	0,0015	1	0,0026	1	0,0003	1	0,0066	4	0,0325	24
5	N-Tech Lab	10,2	0,0078	9	0,0111	9	0,0021	5	0,0112	26	0,0275	2
6	Tech5 SA	10,6	0,0046	3	0,0063	2	0,0009	2	0,0113	27	0,0310	19
7	Ever AI	11,2	0,0085	10	0,0156	16	0,0038	19	0,0063	3	0,0287	8
8	Hikvision	11,4	0,0096	17	0,0125	10	0,0036	17	0,0093	12	0,0271	1
9	<b>Panasonic</b>	18,2	0,0107	20	0,0180	22	0,0048	28	0,0089	10	0,0295	11
10	<b>Toshiba</b>	18,6	0,0125	25	0,0214	29	0,0047	25	0,0085	9	0,0282	5
11	Gemalto Cogent	19,4	0,0091	13	0,0188	25	0,0032	12	0,0095	14	0,0406	33
12	Shenzhen Inst. Adv. Int. Tech	20,2	0,0067	7	0,0099	6	0,0028	9	0,0109	23	0,0520	56
13	Camvi Technologies	21,2	0,0125	26	0,0221	31	0,0049	29	0,0089	11	0,0288	9
14	<b>Saffe Ltd</b>	24,0	0,0119	23	0,0206	26	0,0054	34	0,0107	21	0,0308	16
15	Anke Investments	24,2	0,0131	31	0,0213	28	0,0056	35	0,0094	13	0,0302	14
16	Cyberlink Corp	28,2	0,0131	30	0,0210	27	0,0050	30	0,0125	33	0,0318	21
17	Remark Holdings	28,4	0,0144	35	0,0256	38	0,0061	36	0,0102	18	0,0304	15
18	ITMO University	28,6	0,0125	24	0,0220	30	0,0046	24	0,0149	40	0,0329	25
19	Cognitec Systems GmbH	29,6	0,0116	21	0,0177	21	0,0036	15	0,0118	29	0,0598	62
20	Sensetime Group Ltd	30,6	0,0063	5	0,0092	4	0,0030	11	0,0130	34	0,9999	99

Source: Tables 4 and 5 from [https://www.nist.gov/sites/default/files/documents/2019/04/15/frvt\\_report\\_2019\\_04\\_12.pdf](https://www.nist.gov/sites/default/files/documents/2019/04/15/frvt_report_2019_04_12.pdf)

※ Face Recognition Vendor Test 1:1。VISAデータセット使用時。FMR(他人受入率)を一定(0.0001)としてFNMR(本人拒否率)を評価。

NIST(アメリカ国立標準技術研究所)による評価で **世界No1** にランキングされました。(2023年9月時点)

**Presentation Attack ( PA, なりすまし攻撃 ) 検知技術評価** のうち、「 PA Type 8(プリント写真/画像) - Media Type: videos(動画) 」において **Saffeが世界1位の評価を獲得**。AI技術を活用し、**ソフトウェアだけで瞬時になりすまし防止・不正防止が可能**なため、**ハードウェア非依存で実装可能**です

結果、iOS、Android、PC、その他デバイスに共通UIで **安全な顔認証を低コストで提供可能** となります。

## 固有の生体検知技術

## 専用ハードウェアの投資が不要



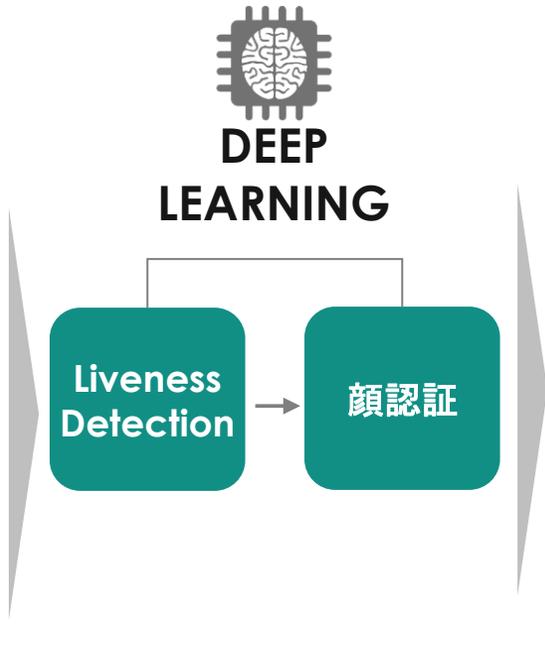
※2:Face Analysis Technology Evaluation(FATE) Part 10: Performance of Passive, Software-Based Presentation Attack Detection(PAD) Algorithms  
PA Type 8- Media Type: videos : BPCER=0.01の場合のAPCER=0±0、 APCER=0.01の場合のBPCER=0.002  
<https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8491.pdf>

# “なりすまし防止”技術の進化

Saffe “なりすまし防止”は画像系機械学習技術である「Convolutional Neural Network (以下、CNN)」を使い、数千万枚の画像を学習させることで実現しています。その結果、**なりすまし不正にみられる特徴の自動検知に成功**しました。また今後、**新しい不正手口が発覚した際にも追加投資は不要で、CNNの追加学習により改善が可能**です。

## 検知可能ななりすまし不正ケース

- ①用紙に印刷された顔写真
- ②スマートフォン、タブレット等の画面に表示された顔画像
- ③3Dマスクを装着した変装  
※現時点では評価版のみ提供



## なりすまし不正にみられる特徴例

- ✓プリント写真や画面表示の画像の再撮影により発生する**不自然な質感**
- ✓なりすまし不正時に見られる**不自然な肌の色**
- ✓スマートフォン、タブレット、PCの画面に表示される画像に見られる**枠などの構成**
- ✓3Dマスクやプリント写真、画面等を使った不正時に生じる**歪みなど**

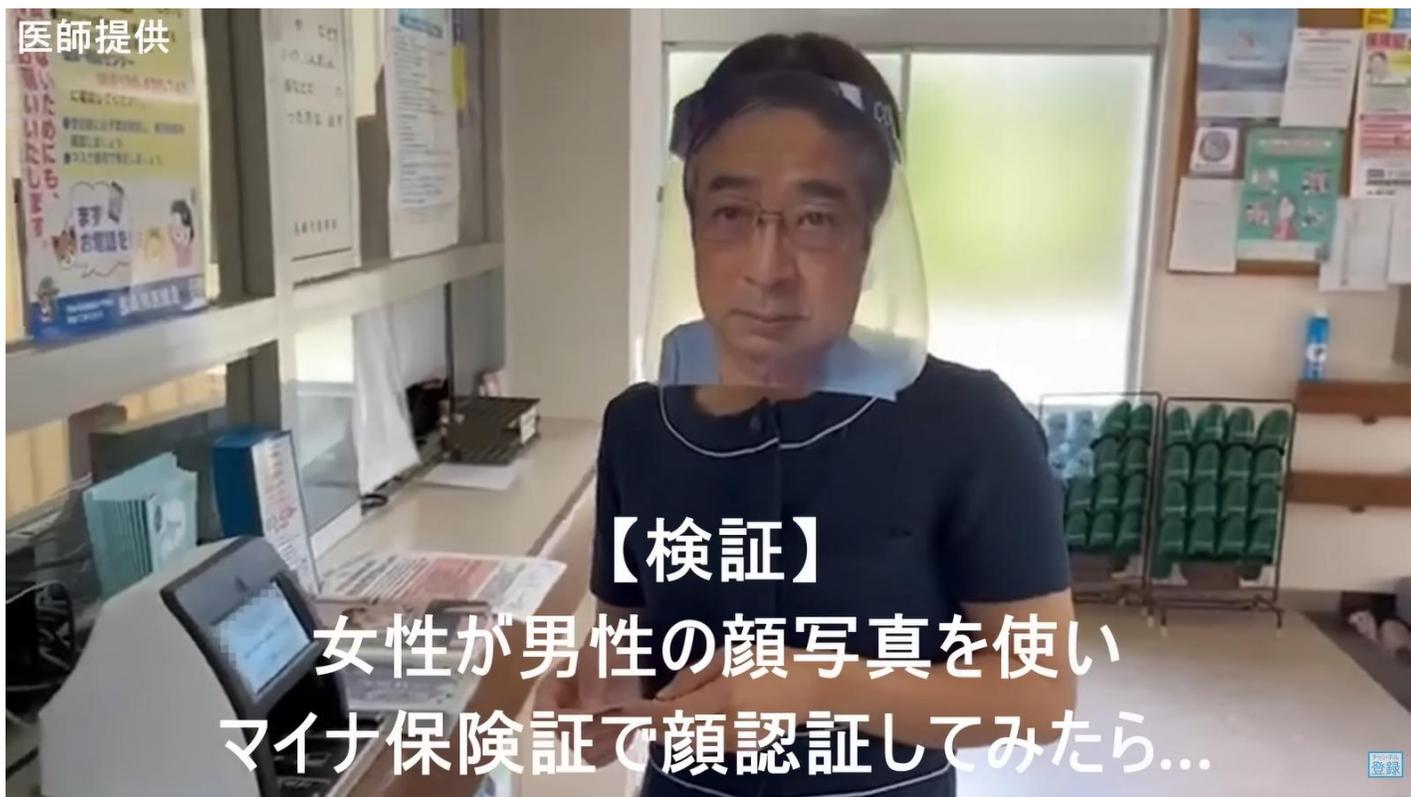


**極めて微妙な差異をAI技術は見抜けます**

そして、グローバルで日々、獲得している顔認証・なりすまし防止のナレッジを共有することで、**安価に**（場合によってはコストフリーで）**精度向上できることがSaffeの強み**となります。

2023年8月2日、某所内科医院の院長が自らの顔写真をお面のようにかぶった女性スタッフに、自らのマイナ保険証を使ってカードリーダーで顔認証を試みたところ、認証が成功してしまい（「なりすまし」が成立してしまい）その後、オンライン資格確認の手続きを進められてしまった。

## 他社顔認証技術で発生した事例 となります



マイナ保険証 信用・信頼の失墜  
（普及の阻害要因）



問題解決

顔認証Saffeは、  
この問題を防ぐことができます！

一度、このような問題が発生すると事業継続性が即、危ぶまれてしまいます。  
このような「なりすまし」をいかに防ぐか、顔認証技術の活用の際に、その重要性をご理解ください。

# 弊社顔認証技術の差別化ポイント

競合サービスと比較して弊社顔認証技術は以下の点で差別化、優位性を有していると考えております。 (競合説明 / 弊社優位性)

弊社技術の競合優位性	差別化ポイントに対する考察 (競合と弊社の対比)	弊社提案先・取引先
あらゆるデバイスに搭載できる 利害関係に縛られない独立系の強みを活かす	国内メーカー系(大手企業)などは「このデバイスでなければ実現できない」というハードウェア依存の課題あり。その分、制約が多く、コストも高価になっており、ビジネスの展開範囲も限定的になっている模様。ハードウェアコストが高くなると物価が安いアジア・オセアニア地域への導入が確実にネックになってくる。弊社はAIモデルがコンパクトであるため、あらゆるデバイスに搭載可能。現地調達でハードウェアを活用することができる。	丸紅株式会社 様 大手鍵メーカー様 大手SI'er様(独立系)
グローバルに強い顔認証である 欧州・南米・アジアでAIモデルを日進月歩で改良	国内顔認証ベンダー(中小企業)などは小規模のデータセットでAIモデルを構築していると聞いている。Saffelは欧州・南米・アジアでAIモデルを日進月歩で改良。人種を問わないグローバルの顔認証技術であり、日本をはじめとするアジア・オセアニア地域でのインバウンド対応に貢献できると考えている。	京成電鉄株式会社 様 コワーキングスペース様
なりすまし防止技術が世界一である 普及に伴う悪用、風評被害、信用と信頼の失墜を防ぐ	他社は赤外線センサーや3Dカメラを用いたりして なりすまし防止 を実現しているケースが散見される。ハードウェア依存の なりすまし防止 は一度、セキュリティを突破されると歯止めが効かなくなり、途端にサービス継続ができなくなる。また、AIで実現している企業においても なりすまし が発生し、事態の收拾に奔走することとなっている。弊社の なりすまし防止 技術は NIST (アメリカ国立技術標準研究所) が世界一であると認めており、安心安全の技術である。昨今、なりすまし防止 単独での機能利用に関するニーズが非常に増えてきており、大手セキュリティ会社様の案件を皮切りに、なりすまし防止機能の単独提供を開始。非常に好評いただいております、更なる引き合いも獲得中。	大手セキュリティ会社様 大手鍵メーカー様 大手印刷会社様
オフラインでも認証できる インターネット接続できない環境でもサービスを継続利用できる	他社はクラウド上にAIモデルを展開して、インターネット経由で顔認証サービスを利用するケースが散見される。インターネット接続が確立できない場合、途端にサービスを利用できなくなるため、ユースケースが非常に限られてしまう。また、クラウド側と都度、問い合わせをおこなわなければならないため、時間を要するため、さらにユースケースが限定される。弊社の顔認証・なりすまし防止はエッジデバイス上で実現可能であるため、オフラインのユースケースにも対応が可能。応答性能も極めて高い。エッジデバイス上に展開するAIモデルもプロテクトしており、知的財産の漏えいリスクも対策済みである。	熊本市交通局 様 アルピコ交通株式会社 様 富山地方鉄道 様 電力事業者様

# 弊社と顔認証Saffe(セーフ)との関係

R.D.Works は Saffe Ltd. と 顔認証事業のグローバル戦略を共に歩む強力なリレーションを2019年に築き、日本国内の独占販売契約を締結。現在、弊社は 日本 の普及を推進、アジア・オセアニア地域を起点に、全世界への顔認証普及を全面的に推進しております。顔認証は顔をアイデンティティとする技術で人種による影響が大きいため、ローカライズが非常に重要となります。R.D.Works / Melon Technologies は日本向けのカスタマイズ・AIモデルの強化、エンドユーザー様へのサービス提供を通じて、アジア・オセアニア地域の導入を推進し、顔認証技術の世界普及とビジネスの成功を実現します。



事業継続性を確保するために以下の対策を講じており、日本国内の独占販売契約を締結しているその先、**20年後（2042年）以降も永続的にビジネスを推進可能なスキームを構築**しております。

Saffe Ltd. との資本提携	R.D.Works から Saffe Ltd. に対して出資。 <b>持ち株比率 10%超 の資本関係</b> を築き、Saffe Ltd. 経営層とのリレーションシップを構築済。さらなる出資も検討しており、 <b>20年後(2042年)以降のリレーションについて、Saffe Ltd. 経営層と合意</b> しています。
取得したデータの帰属	<b>弊社が取得したデータの所有権は弊社に帰属しているため、20年後以降も日本に残り続ける。</b> 失うことはありません。
ナレッジの蓄積	Saffe Ltd. 出身の <b>AIエンジニア</b> を弊社が日本で採用。 <b>顔認証AIモデルの改良・拡張をSaffe Ltd. と共同で実施、日本市場向けカスタマイズも可能。</b> Saffe Ltd. も当該メンバーの在籍を認知しており、関係性は非常に良好です。
知的財産の共有	顔認証AIモデル本体、AIモデルの構築方法、改良・拡張の方法、それらに関連する全てのソースコードなど、 <b>重要な知的財産へのアクセス権を Saffe Ltd. より許諾</b> されています。
Saffe Ltd. 解散に対するリスクヘッジ	万が一、Saffe Ltd. が解散することとなった場合でも <b>R.D.Works が Saffe の知的財産の譲渡を受け、事業を継続できる</b> 契約になっています。
日本やアジアのビジネス、より強固なパートナーシップの構築	<b>日本でのビジネスは R.D.Works や Melon Technologies が独占的・排他的に担っており、Saffe の顔認証技術をアジア・オセアニアに展開していくことで、弊社とSaffe Ltd. とのパートナーシップは更に強固になる。</b> 弊社とSaffe Ltd.は必然的に <b>2042年以降も弊社とのビジネスを継続していく</b> と考えています。

# 1. 会社概要

# 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

# 顔認証Saffe(セーフ) 導入事例 概要

「決済」「eKYC（本人確認）」「セキュリティ」3つの注力分野でユースケースで事例を獲得しています。

決済



- ① 顔認証を活用した乗車運賃の顔パス決済（熊本市交通局様、富山地方鉄道様、アルピコ交通様、他）
- ② 顔認証を活用した乗車チケット発券サービス（京成電鉄株式会社様）
- ③ バス運賃顔認証クレジット決済（スペイン・マドリード）
- ④ スーパーマーケット顔認証決済（コロンビア）

eKYC  
（本人確認）



- ⑤ 顔認証を使った銀行口座開設（ブラジル）
- ⑥ 厚生労働省 支払基金様 マイナンバーカード・オンライン資格確認 システム開発（松村エンジニアリング様）
- ⑦ AI映像監視・顔認証 入退構ソリューション「TRASCOPE-AI」 システム開発（丸紅ネットワークソリューションズ様）

セキュリティ



- ⑧ ホームセキュリティ 顔認証&なりすまし防止（大手セキュリティ会社様）
- ⑨ コワーキングスペース向け 顔認証入退室管理 アクセスコントロール システム開発（fabbit様、JSB様、他）
- ⑩ 保育園・幼稚園向け お子様の見守りシステム開発（桐光学園みどり幼稚園様）

## 顔認証を活用した乗車運賃の顔パス決済（熊本市交通局様、富山地方鉄道様、アルピコ交通様、他）

- スマホアプリから利用者情報を登録し、個人のウォレットを作成。お金をチャージして、顔パス決済を実現。
- 顔認証決済プラットフォームとしてサービスを作り上げており、今後、様々なユースケース、クライアント様への展開を予定。
- 顔認証タブレットに 顔認証Saffe のエンジンを搭載し、交通のユースケースに必要なオフラインでの顔認証を実現。
- 交通事業者様は熊本市交通局(路面電車)、および長野県と富山県のバス運行会社2社を皮切りに実証実験を実施。
  - 詳細は以下プレスリリースをご査証ください。

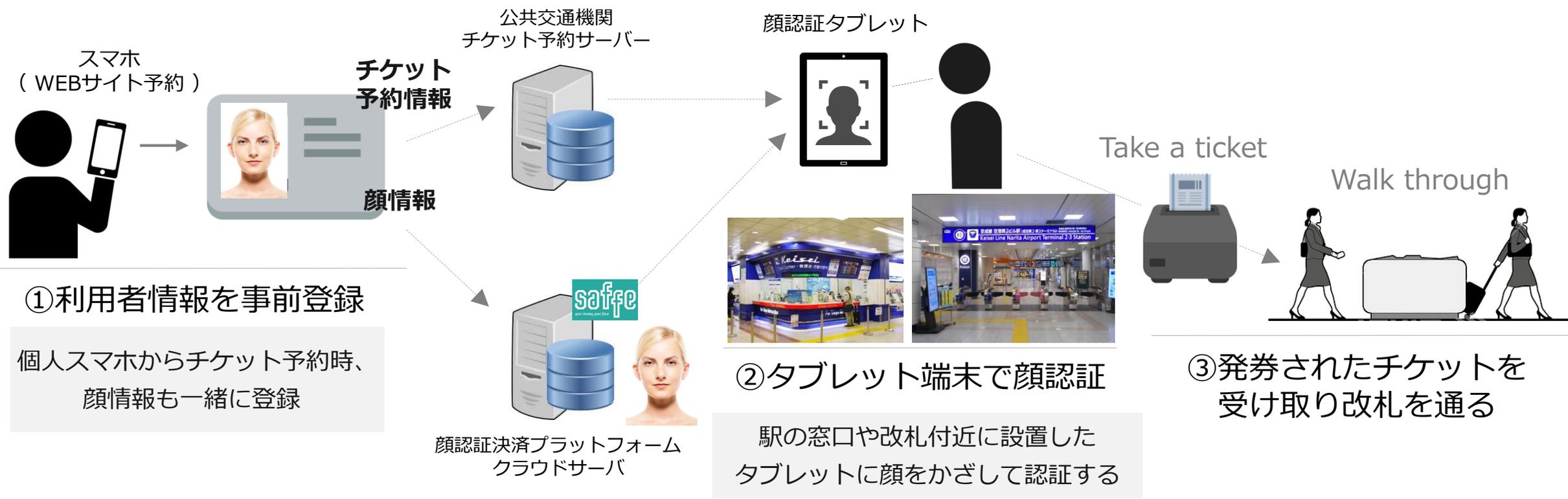
[http://www.kotsu-kumamoto.jp/kihon/pub/detail.aspx?c\\_id=3&id=1447&pg=1](http://www.kotsu-kumamoto.jp/kihon/pub/detail.aspx?c_id=3&id=1447&pg=1)



# 導入事例 ②

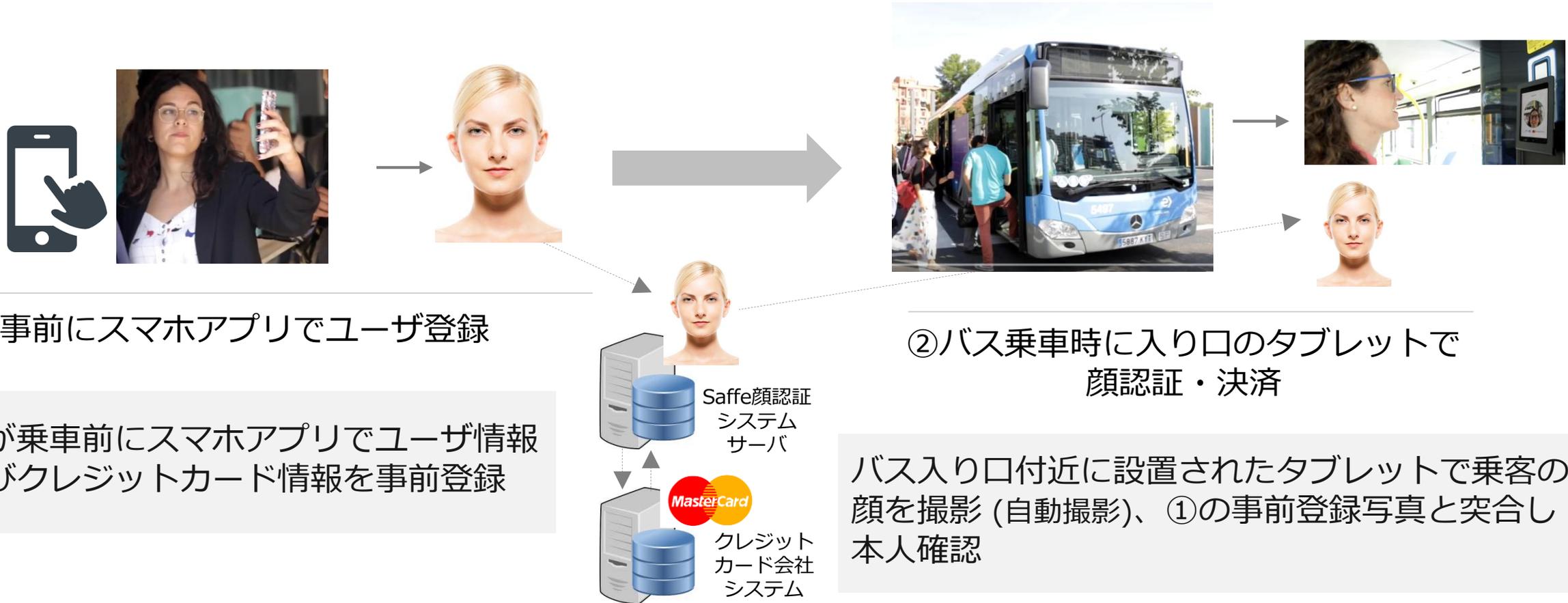
## 顔認証を活用した乗車チケット発券サービス（京成電鉄株式会社様）

- エアポートラインの公共交通機関（京成スカイライナー）で顔認証を活用した乗車チケット発券サービスを開始。WEB予約時に顔情報を事前に登録しておき、チケット発券を顔パスでおこなえるようにする。（2025年1月にサービスイン予定）
- インバウンド客がチケット発券時に待ち行列を作ってしまう。待ち時間は最大30分、経営課題になっている。「顔をかざすだけ」というユニバーサルデザインの認証方法を採用し、チケット発券の待ち行列を解消する。
- クライアント側の擁するシステム開発会社と連携し、一つのソリューション・サービスを作り上げることを目指す。
- 実証実験開始前・開始時にプレスリリースを発表予定。反響が期待される。



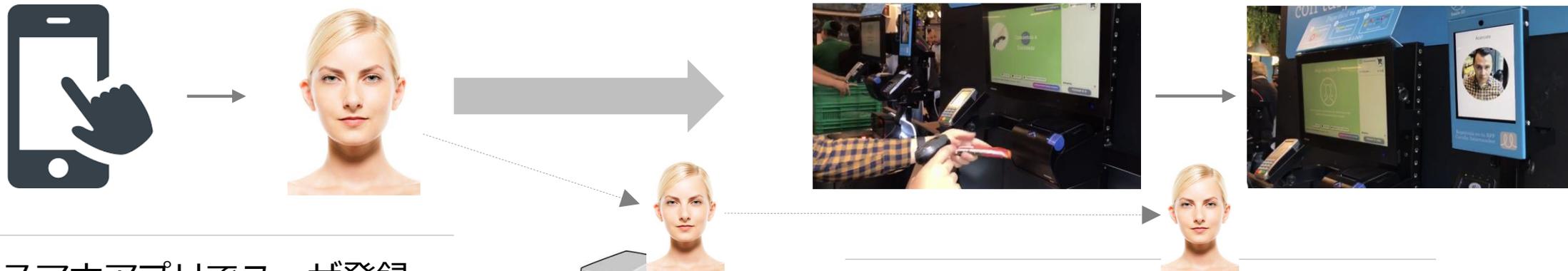
## バス運賃顔認証クレジット決済（スペイン・マドリード）

- クレジットカードのマスターカード社、スペイン大手銀行のサンタンデール銀行との協業により、マドリード市バスのキャッシュレスを顔認証で実現。



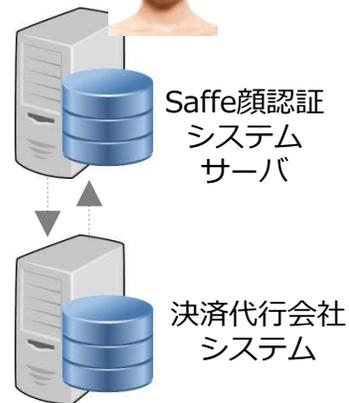
## スーパーマーケット顔認証決済（コロンビア）

- スーパーマーケットのセルフレジにける決済方法として顔認証Saffeのシステムを採用・商用化。
- 顔認証によるキャッシュレス対応店舗を拡大予定。



### ①事前にスマホアプリでユーザ登録

お客様が事前にスマホアプリでユーザ情報およびクレジットカード情報を事前登録



### ②レジにて顔認証・決済

セルフレジにて商品スキャン後、支払い方法として顔パスを選択。セルフレジと連携したタブレットで自撮りした顔写真（自動撮影）と①の事前登録写真と突き合わせ、認証OKなら支払い完了

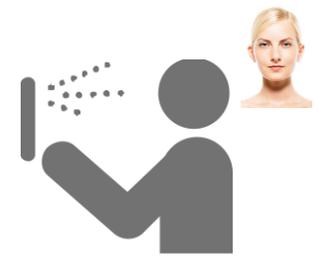
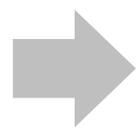
## 顔認証を使った銀行口座開設（ブラジル）

- ブラジル政府が運用する顔認証を使った本人確認プラットフォーム「Datavalid」と連携することで不正口座開設を防止
- ブラジル国内ネット銀行大手のModalmais(クレディスイス系列銀行)において250万人超のユーザが利用中
- 本人確認と同時にブラックリスト上の要注意人物と照合することでセキュリティーを強化



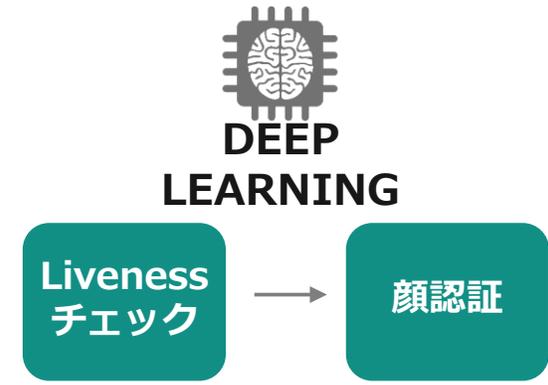
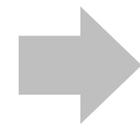
①専用アプリで個人識別番号を含むお客様情報を入力

銀行提供のスマホアプリをダウンロードし、お客様情報とDatavalidに登録済みの運転免許証番号等の個人識別番号を入力



②本人の顔写真を自撮り

スマホアプリでお客様ご本人の顔写真を撮影



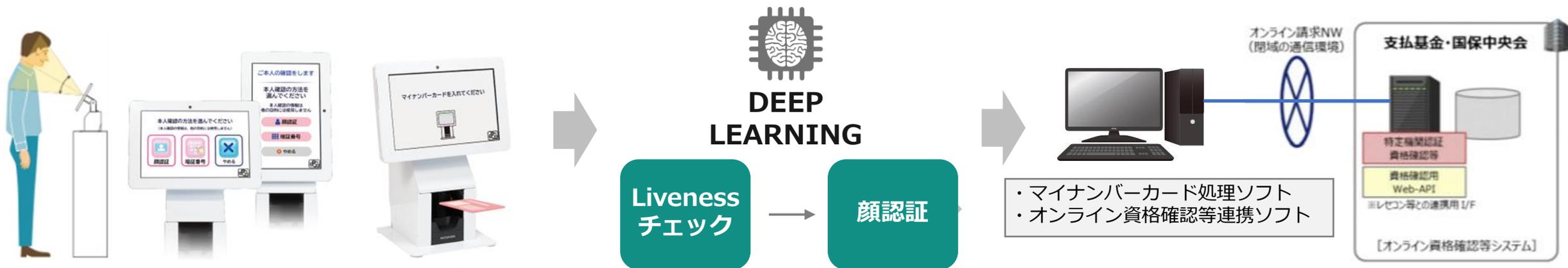
③ ②のなりすましチェック及びDatavalidの顔写真とのマッチング

②の顔写真になりすましがなく、且つ、Datavalidの顔写真とのマッチングがOKであれば口座開設へ

## 厚生労働省 支払基金様 マイナンバーカード・オンライン資格確認 システム開発 (松村エンジニアリング様)

- 健康保険法等の一部改正に伴い、マイナンバーカードを健康保険証として利用可能となった。本件に向け、マイナンバーカードリーダーと顔認証の組合せによるオンライン資格確認等システムを実現。
- Saffe顔認証エンジンを搭載した製品「EXC-9000」が2022年5月に厚労省認可を得て販売開始した。
- 詳細は以下プレスリリースを参照。

<https://prtmes.jp/main/html/rd/p/000000002.000055030.html>



① マイナンバーカードの顔写真読取り  
および本人の顔写真を撮影

顔認証付きカードリーダーにてマイナンバーカード上のお客様情報、及び顔写真を読取るとともに本人の顔写真を撮影

② マイナンバーカードの顔写真と  
本人顔写真をマッチング

本人顔写真に対してなりすまし防止 (Liveness)チェックを行うと同時にマイナンバーカードの顔写真と照合

③ オンライン資格確認

本人確認に問題ない場合はオンライン資格確認の上、保険適用受付手続きへ

## AI映像監視・顔認証 入退構ソリューション「TRASCOPE-AI」 システム開発 (丸紅ネットワークソリューションズ様)

- エッジAIデバイスへSaffe顔認証アルゴリズム搭載し、オフィスビルや食品工場、建設現場等へのアクセス管理を実現。
- 顔認証と同時に入場者の体温測定、マスク検知も実現。 ※マスク着用時でも顔認証可能。
- 詳細は以下プレスリリースを参照。

<https://prtimes.jp/main/html/rd/p/000000403.000017036.html>



## ホームセキュリティ 顔認証&なりすまし防止（大手セキュリティ会社様）

- 既存で既にサービス展開されているホームセキュリティに顔認証を導入。ホームセキュリティデバイスに新たにカメラを搭載、セキュリティの開始・解除で顔認証を活用して本人確認をおこなう。（セキュリティキーだけで解除されない仕組みを実現）
- 元々、「顔認証～なりすまし防止」を他社のサービスで実現しようとしていたが、なりすまし防止に関して致命的な課題（顔を印刷した写真をカメラにかざしたところ、認証が通ってしまう）があり、弊社にご相談をいただいた。
- 弊社からは「なりすまし防止」を機能提供。顔認証は他社製、なりすまし防止は弊社性というハイブリッドのソリューション構成で実現。

RENESAS製 AIボード [ RZ/V2M ]  
AIアクセラレータ DRP-AI を搭載



Safte 「なりすまし防止」  
機能を単体で組み込み



## コワーキングスペース向け 顔認証入退室管理 アクセスコントロール システム開発 ( fabbit様、JSB様、他 )

- セキュリティーカードから顔認証へ。手ぶらによるユーザ利便性向上、事務工数削減、さらに使いまわし防止を実現。
- 詳細は以下プレスリリースを参照。

<https://prtimes.jp/main/html/rd/p/000000001.000055030.html>



①専用タブレットにて  
会員情報を事前登録

専用タブレットにて会員様情報  
(会員情報、顔写真、入室可能期間等)  
を事前登録



②顔パスでエントランスドアロック解錠

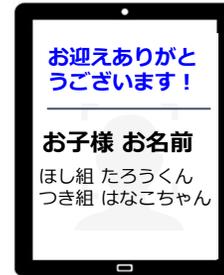
エントランスドアに設置したスマホで入室者の顔写真を撮影、  
①の事前登録時の写真と突き合わせて本人確認、問題なければ  
ドアロック解錠

## 保育園・幼稚園向け お子様の見守りシステム開発（桐光学園みどり幼稚園様）

- 迎えに来る頻度が低く幼稚園教諭から認知されていない保護者の方、特に父親や祖父母でも事前に顔写真等の情報を登録し、園児と紐付けを行うことで、安全な保護者への園児引き渡しを実現。
- 今後、送迎バス内の園児置き去り等の事故防止や園児の安全確保に向け、顔認証を活用した追加施策を予定。



Safe情報管理・  
顔認証システムサーバ



### ①保護者情報を事前登録

専用タブレットにて保護者様情報  
(園児との紐付け、顔写真等)  
を事前登録

### ②顔認証で保護者確認後、園児引き渡し

降園時にお迎えに来た方の顔写真をタブレットで撮影、①の事前登録時の写真と突き合わせて本人確認、園児との紐付けを確認できれば園児引き渡し

# 1. 会社概要

# 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

**Appendix2 : 成長戦略**

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

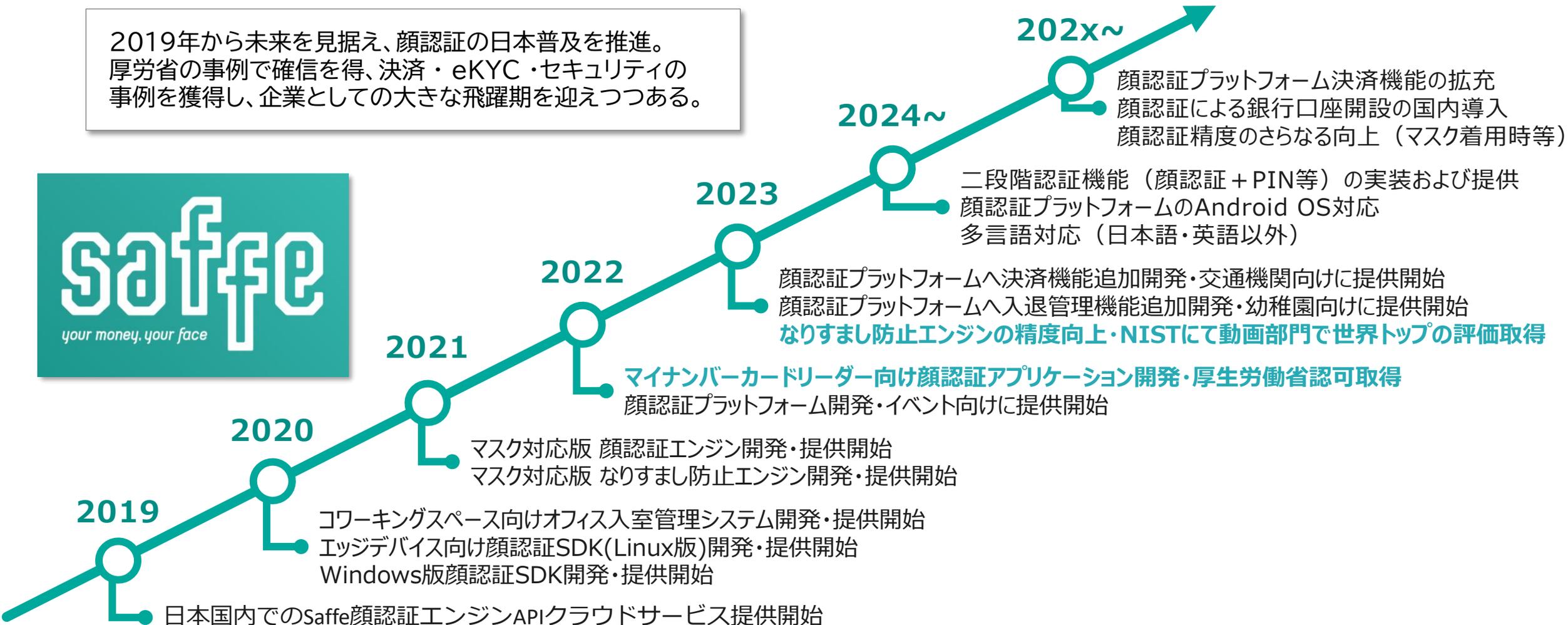
Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

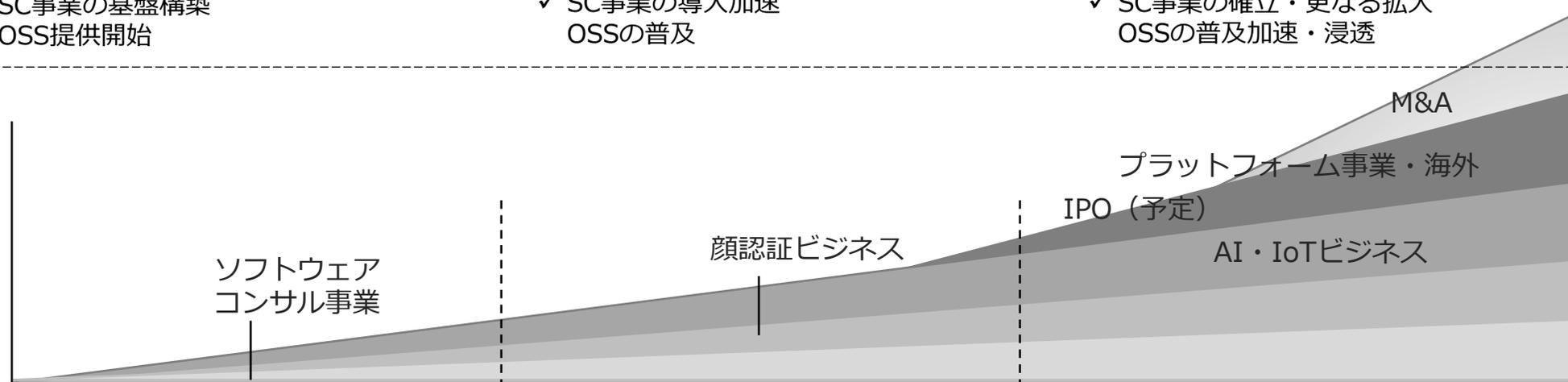
2019年より、R.D.Worksは英国・ブラジルを拠点とする 顔認証・なりすまし防止 技術に特化したIT企業 Saffe Ltd. とアライアンスを組み、日本国内への顔認証技術の普及を推進中。

2019年から未来を見据え、顔認証の日本普及を推進。厚労省の事例で確信を得、決済・eKYC・セキュリティの事例を獲得し、企業としての大きな飛躍期を迎えつつある。

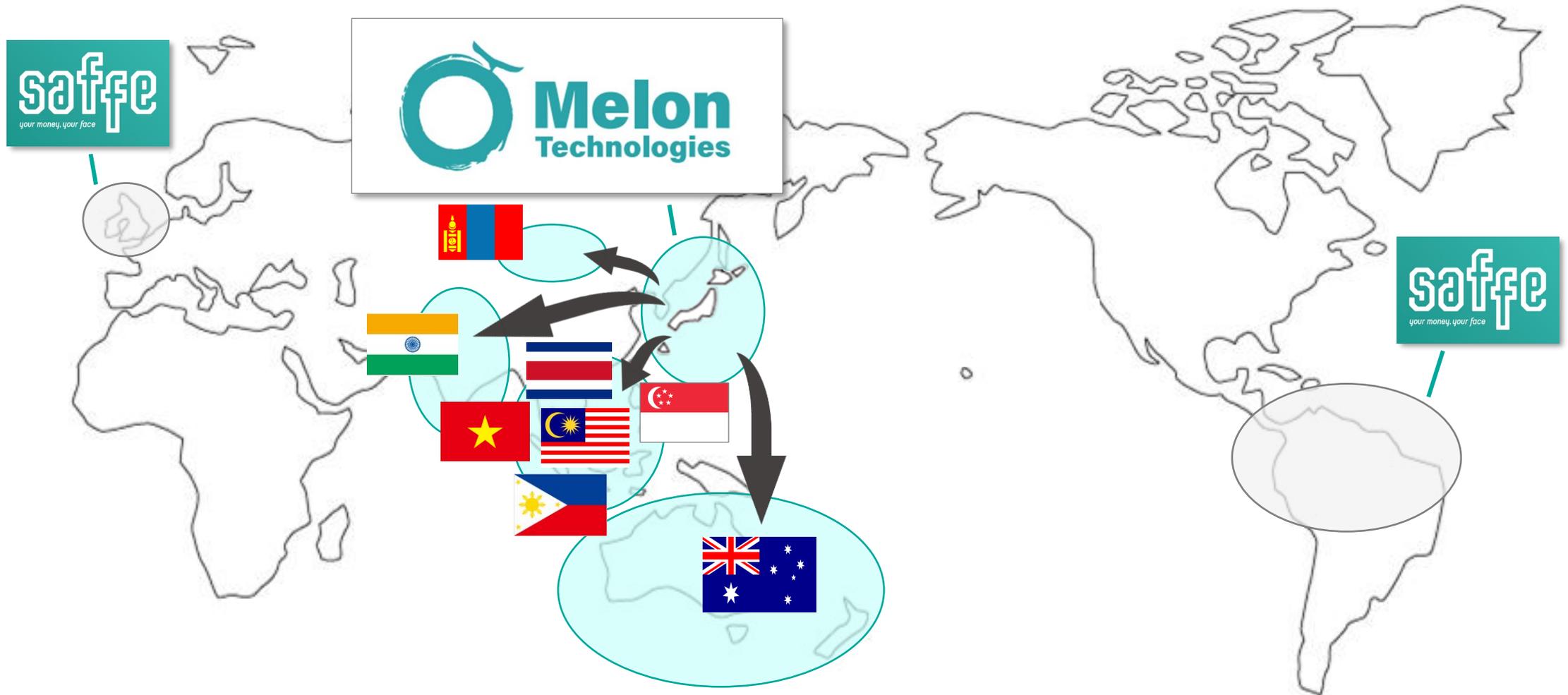


顔認証事業を先行して推進しつつ、AI・IoT領域でもサービス・ソリューションを展開し、  
**社会にさらなる安心安全な利便性を提供します。**

Current Opportunity ~2024年9月期	Mid-term Opportunity ~2028年9月期	Long-term Opportunity ~2031年9月期
<ul style="list-style-type: none"> <li>✓ 大手商社、セキュリティ会社、ハードウェアベンダーとのパートナーシップ確立</li> </ul>	<ul style="list-style-type: none"> <li>✓ 顧客・提携先拡大、ブランド向上 海外進出開始</li> </ul>	<ul style="list-style-type: none"> <li>✓ 日本のトッププレイヤー、M&amp;A 海外展開、プラットフォーム事業</li> </ul>
<ul style="list-style-type: none"> <li>✓ 顔認証の領域拡大                             <ul style="list-style-type: none"> <li>- 交通決済実装</li> <li>- セキュリティ・eKYC確立・導入</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ 顔認証の実装・普及                             <ul style="list-style-type: none"> <li>- 地方交通決済実装・普及</li> <li>- セキュリティ・eKYC実装・普及</li> <li>- 新しい領域の確立・導入</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ 顔認証の社会インフラ化                             <ul style="list-style-type: none"> <li>- 地方交通決済のデファクト</li> <li>- セキュリティ・eKYC普及拡大</li> <li>- 新しい領域への実装・普及</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>✓ AI・IoT領域でのサービス・ソリューション基盤構築</li> </ul>	<ul style="list-style-type: none"> <li>✓ AI・IoT領域でのサービス・ソリューションの普及拡大</li> </ul>	<ul style="list-style-type: none"> <li>✓ AI・IoT領域での顧客浸透・社会インフラ化</li> </ul>
<ul style="list-style-type: none"> <li>✓ SC事業の基盤構築 OSS提供開始</li> </ul>	<ul style="list-style-type: none"> <li>✓ SC事業の導入加速 OSSの普及</li> </ul>	<ul style="list-style-type: none"> <li>✓ SC事業の確立・更なる拡大 OSSの普及加速・浸透</li> </ul>



**アジア・オセアニアへのビジネスを展開予定。** 弊社は日本での導入事例、グローバルの顔認証技術とエンジニアチーム、日本法人の名だたる大手企業とのアライアンス、ハードウェアベンダーとリレーション、持てるリソースをフル活用して、海外展開を目指します。



海外展開に際しては弊社の営業リソースを基軸とし、①丸紅様をはじめとした日系大手クライアント様の営業力・販売チャネルのフル活用、②アクセラレータプログラムを用いたアライアンスの強化、③現地パートナーとの協業、④中長期的な弊社営業リソースの拡充、の4本柱の施策で事業拡大を実現します。

施策② グローバル  
アクセラレータプログラム

PLUGANDPLAY



施策③

アライアンス ( 現地パートナー )

現地のハードウェアメーカー、設置業者、エンジニア、販売代理店、営業担当者など

( MARS Venture Partners, Insight Genie, TOTM Technologies との連携を模索中 )



Engineer

Sales

各国の導入を迅速にスケールするため、  
現地パートナーとのアライアンスを組む

施策①

アライアンス ( 日本法人の大手クライアント )

丸紅様、大手セキュリティ会社様、大手電鉄会社(不動産部門)様、  
大手デバイス製造メーカー様、大手鍵メーカー様、大手印刷会社様



グループ会社の現地法人、営業支社・支店、現地ビジネスに精通した営業員

既にモンゴル、シンガポール、  
オーストラリアの引き合いを  
アライアンスと共に推進

施策④

弊社 営業リソース ( 2024年12月時点の体制 )

代表取締役 齋藤英樹 ( さいとう ひでき )



多くの大企業へコンサルティング・ビジネスソリューションを提供。ビジネス構築力・コンサルティング力で会社の発展を牽引。日系企業による海外ビジネスの多彩なサポート実績があり、英語も堪能。強力なアライアンス構築力を有する。

COO 兼 CFO 長谷川幸 ( はせがわ つかさ )



メガバンクで28年勤務。アジア地域に5年の駐在経験があり、現地のVC・投資アドバイザーと提携。現地市場を開拓した経験と実績あり。英語も堪能。豊富なリーガル面の知見を活用し、アジア・オセアニアのアカウントマネージャーを担う。

カスタマーサクセス 部長 田中仁朗 ( たなか きみお )



エンジニアとして13年の経験があり、コンサルタント・営業として大手商社丸紅をはじめとする名だたる企業のクライアント責任者である。豊富な技術知識に裏打ちされたコミュニケーション能力で顧客から厚い信頼をいただく。日本国内のアカウントマネージャを担う。

現在、進行中の案件と現地動向の調査状況は以下となります。**日本国内の高い知名度と信頼ある実績を基にアジア・オセアニア地域へビジネスを推進**します。

## 【モンゴル】

TransBank of Mongolia と顔認証を活用した eKYC(本人確認)の実現を検討。

## 【タイ】

・MARS Venture Partnersが支援するタイのITセキュリティ会社が提供している、オフィスや工場などの監視システムや勤怠管理システムと、顔認証を連動させる構想もアイデアベースでは提示されている状況。

## 【オーストラリア】

・大手商社(交通部門)、大手電鉄会社(不動産部門)から顔認証の導入に関する相談があり、意見交換。某州にて駅ビル開発、スマートシティ構想に顔認証技術の活用を検討中。

## 【シンガポール】

・Saffe顔認証技術に関心を持つ在星TOTM Technologies Limitedと連携、ネットワーク活用によるシンガポール市場への展開。  
・Saffe顔認証技術に関心を持つ在星Insight Genieとの連携。  
・2024年6月にシンガポールの現地調査を行った処、顔認証の普及はあまり進んでおらず、これからと云った印象。新築のオフィスビルや先進的なコンドミニアムの玄関口に顔認証ゲートが設置されている状況で、散見される程度と云った普及状況。

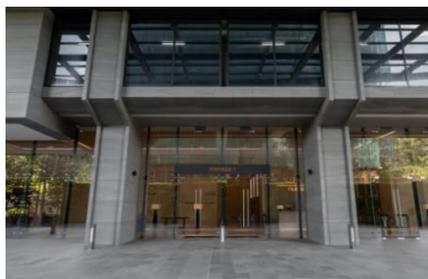
## 【マレーシア】

・長谷川が5年駐在したネットワークを活かしたビジネス展開を見込む。  
・日系企業と政府系企業とのマッチングに強みを有する現地VC・投資アドバイザーのMARS Venture Partnersとの連携・ネットワークを活用し、マレーシア市場へ顔認証ビジネスを展開。  
・2024年4月、AirAsiaは、マレーシア国内に初となる顔認証搭乗システムを導入する旨をプレスリリース。空港を中心とした3Dカメラ等を使った大掛かりな顔認証システムの導入が主流。最近、オフィスビルでの導入が散見されるようになってきたが、マレーシア国内のコンドミニウムや商業施設と云った廉価・手軽な導入が求められる領域では、今後、導入が進むものと期待される。シンガポールよりも普及度としては遅れている印象。

弊社にてシンガポールとマレーシアの現地（日系銀行系の施設）を視察。入館のゲートはあるが、現地はICカードの本人確認が中心で、カードの使いまわし(なりすまし)が可能な状況。弊社はセキュリティと利便性の向上を両立させられる顔認証の市場ポテンシャルを見込んでいます。

## 【視察結果:マレーシア】

MUFG Malaysia / Plaza Conlay, No. 18,  
Jalan Conlay, 50450 Kuala Lumpur



## 【視察結果:シンガポール】

MUFG Singapore / Marina One East Tower,  
7 STRAITS VIEW, 23-01 Singapore



世界水準の顔認証を低コストでグローバル展開。差別化ポイントは以下と考えております。

弊社技術の競合優位性	差別化ポイントに対する考察	競合他社の状況
<p>あらゆるデバイスに搭載できる 利害関係に縛られない独立系の強みを活かす</p>	<p>日本のみならずグローバル展開を見据えた際、弊社は<b>現地のハードウェア・ソフトウェアを活用したソリューションの構築が可能</b>。現地の物価、現地での現物調達・サプライチェーンなども考慮した<b>サステナブルなスキームを構築</b>できる。</p>	<p>他、国内メーカー系の顔認証技術はハードウェアやソフトウェアの制約が多い傾向がある</p>
<p>グローバルに強い顔認証である 欧州・南米・アジアでAIモデルを日進月歩で改良</p>	<p>元来、グローバル由来の顔認証技術であり、<b>多種多様な人種による認証精度はNISTによって証明</b>されている。<b>グローバル展開でも問題ない顔認証技術</b>である。</p>	<p>多種多様な人種、様々な条件下で公平公正に精度検証するNISTの評価を受けていない場合がある</p>
<p>なりすまし防止技術が世界一である 普及に伴う悪用、風評被害、信用と信頼の失墜を防ぐ</p>	<p>日本よりも犯罪発生率の高い諸外国に向けたサービス展開となる。顔認証技術で最もリスクのある「他人をなりすます行為」に対して、弊社技術はAIを活用した<b>世界一のなりすまし防止技術を搭載している点がグローバル展開の強み</b>となる。</p>	<p>他、国内顔認証ベンダーは「なりすまし」に関する課題を抱えている場合がある</p>
<p>オフラインでも認証できる インターネット接続できない環境でもサービスを継続利用できる</p>	<p>日本よりもネットワーク普及率の低いグローバル展開を見据えた際、<b>オフラインでもサービスを利用できる弊社技術がサービス普及に際して非常に重要</b>となる。</p>	<p>他社はオンライン状態を必須条件とするサービスもある</p>

弊社はグローバル経験が豊富なハイスکیلエンジニアを中心に採用。Nathan, Ashley, Hawar の3名は米Bloomberg出身、金融情報や証券・為替の約定を手掛ける大手金融ベンダーでの開発経験を有し、セキュリティを含めて、強固で堅牢なシステムを構築可能な。紹介メンバー以外にも数名のエンジニアがおり、常にグローバルスタンダードの先行事例・オープンソースなどの技術情報を収集し、**先鋭的・モダンなソリューション提案、開発をおこなうことが可能。**チーム内の公用語は**英語**でグローバル展開を見据えた**技術的なコミュニケーションの課題(言語の壁)はありません。**

## Nathan Miniovich (ナタン ミニオヴィッチ)

### CTO・取締役

- ・総合情報サービス企業であるブルームバーグおよびSNS企業LINEの日本法人でITエンジニアとして激務を経験。
- ・先々を見据えた汎用的なシステムアーキテクチャを検討し構築することを得意とする。
- ・日本在住5年目、日本語も堪能でコミュニケーション能力が抜群。R.D.Works入社後は厚生労働省案件に携わり、膨大な仕様書を読み解き、システム開発をおこない、チームでQCDをしっかりとコミットした。



## Ashley Smart (アシュリー スマート)

- ・IT業界の経験は25年以上。直近はブルームバーグの日本法人で10年以上、ITエンジニアとして研鑽を積む。Big Data 分析、機械学習のAI領域を得意とする。一方、電気工学・電子工学にも精通しており、ハードウェアの扱いも非常に長けている。特に、モトローラ社に在籍時、電波集積の基礎となる Base Band を開発し、一時期は米国シェア50% (1億Unit)におよぶほど PowerQuicc III が普及し、会社および世の中に広く貢献。
- ・様々なレイヤーでのエンジニアリングに対応でき、OSレベル・通信プロトコルの基礎レベルに及ぶ開発が可能。

## Hawar Talabani (ハワル タラバニ)

- ・IT業界の経験は25年以上。直近はブルームバーグのロンドン法人～日本法人で16年以上、ITエンジニアとして研鑽を積んできた。あらゆるソフトウェア開発に精通、開発プラットフォーム・開発言語を問わず、高い生産性と品質で成果物をアウトプットすることが可能。高い技術力を見込まれ、フランス政府(軍事省)の開発案件も経験。
- ・豊富な基礎知識と確かな技術を持ち、信頼性の高いソフトウェア開発をおこなうことが可能。

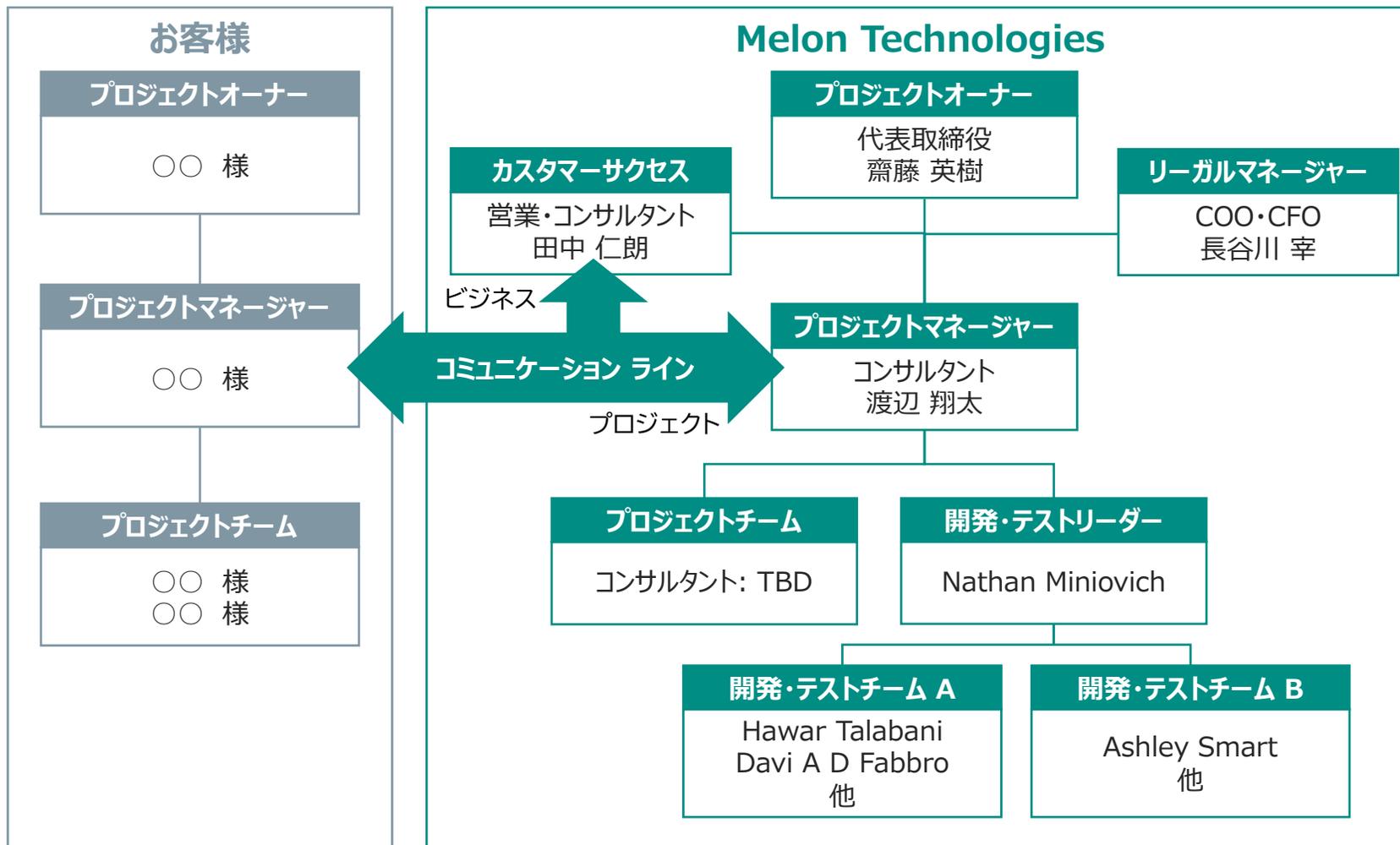
## Davi A D Fabbro (ダヴィ ファブロ)

- ・Saffe Ltd.でAIエンジニアとして顔認証Saffeのエンジン、学習モデルの構築に従事し、3年前にR.D.Worksに移籍。
- ・大学は修士課程で機械学習[Machine Learning]を専攻。画像分析系のAIを得意領域としている。



ハイスキルなエンジニアの有り余るパフォーマンスを最大限引き出すための体制を構築。  
 エンジニア以外にも豊富な経験とスキルを持つマネージャーで盤石な布陣を固められています。

## 体制



## 役割

<b>プロジェクトオーナー</b>	<ul style="list-style-type: none"> <li>プロジェクト決定事項の承認</li> <li>※ステアリングコミッティを設けず、プロジェクトオーナーの承認を最終承認とする</li> </ul>
<b>リーガルマネージャー</b>	<ul style="list-style-type: none"> <li>法務、労務、管理全般</li> <li>プロジェクト支援</li> </ul>
<b>カスタマーサクセス</b>	<ul style="list-style-type: none"> <li>提案、見積、契約、請求</li> <li>プロジェクト支援</li> </ul>
<b>プロジェクトマネージャー</b>	<ul style="list-style-type: none"> <li>プロジェクト進捗管理、課題管理、リスク管理、品質管理</li> <li>コミュニケーション推進</li> <li>プロジェクト成果物承認</li> </ul>
<b>プロジェクトチーム</b>	<ul style="list-style-type: none"> <li>プロジェクトマネジメント支援</li> <li>ドキュメンテーション等実タスクの遂行</li> <li>システム・成果物品質管理</li> </ul>
<b>開発・テストリーダー</b>	<ul style="list-style-type: none"> <li>要件定義</li> <li>システム設計レビュー</li> <li>システム開発レビュー</li> <li>テスト設計・成績レビュー</li> </ul>
<b>開発・テストチーム</b>	<ul style="list-style-type: none"> <li>システム設計、環境構築、開発</li> <li>テスト設計、テスト実行</li> </ul>

# 1. 会社概要

# 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性( なぜ、顔認証なのか? )

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表( 物理認証や他生体認証との比較 )

現在、世界的に“パスワードレス認証”が急速に普及しています。スマートフォンやタブレット、パソコンでFaceIDなどのロック解除機能が気軽に使われるようになりました。パスワードレス認証は旧来より、指紋認証・静脈認証・虹彩認証などの生体認証が先行しましたが、専用のデバイスを必要とする制約から普及がなかなか進みませんでした。コロナ禍で更に、接触型・近接型の生体認証が避けられることとなり、その時流の中で今、**非接触で遠距離でも実現可能な顔認証**が注目を集め始めています。**画像認識系AIを活用している技術が多く、カメラとAI処理可能なコンピューティングで容易に実現できることが特徴**です。

## 顔認証



専用デバイスが**不要**

(カメラとAI処理が可能なコンピュータだけでOK)

## 他、生体認証

### 接触型



### 近接型



専用デバイスが**必要**

# 顔認証の“なりすまし”に関する危険性と回避策

顔認証は非接触型・搭載デバイスの制約がないことがメリットである一方、“なりすまし”の懸念があります。他人が、本人の写真をスマホなどに表示したり、光沢紙に印刷をしてカメラにかざし、顔認証を不正に成功させようとする行為を“なりすまし”と称し、顔認証が普及する昨今、この問題がクローズアップされています。その問題を解決するため、赤外線センサーを用いて体温を計測する方法を組み合わせたり、認証時の指示（右を向いてください、左を向いてください、まばたきをしてください）などのオペレーションを組み合わせた回避策を講じていますが、顔認証の利点であるデバイスの制約が少ない、顔をかざすだけで認証ができる利便性が失われてしまう残念な実情が世の中にあります。

一方、弊社の **Saffe(セフ)** はなりすまし防止をAI技術で実現をしており、上記のような弊害がありません。



現在、**顔認証はまだまだ“世の中に普及しているとは言いづらい状況”**かと思えます。**国籍や言語、世代の壁を越えた、顔をかざすだけというユニバーサルデザインの技術**であるにも関わらず、普及が進まない理由は大きく4つあると考えております。

### 顔認証 普及の阻害要因

1. 顔認証にリスクを感じる、安全面で大丈夫かどうか不安がある
2. 導入コストが高い、費用対効果が見いだせない
3. どのように活用できるのか、どのように導入したらいいのかイメージが湧かない
4. 顔認証があたりまえの技術として認識されていない、まだ馴染みがない

上記を払拭し、**利便性の高い社会を安全に実現する**ため、Melon Technologiesは**顔認証Saffeの日本国内への普及を目指しております。**

## 顔認証 普及の阻害要因

1. 顔認証にリスクを感じる、安全面で大丈夫かどうか不安がある
2. 導入コストが高い、費用対効果が見いだせない
3. どのように活用できるのか、どのように導入したらいいのかイメージが湧かない
4. 顔認証が あたりまえの技術 として認識されていない、まだ馴染みがない

客観的な、第三者の公平公正な審査の結果こそが不安の解消につながると考えております。

そこで、NIST[アメリカ国立技術標準研究所]の評価を受け、  
前述 **世界トップレベルの技術** であることが証明されました。

## 顔認証 普及の阻害要因

1. 顔認証にリスクを感じる、安全面で大丈夫かどうか不安がある
2. 導入コストが高い、費用対効果が見いだせない
3. どのように活用できるのか、どのように導入したらいいのかイメージが湧かない
4. 顔認証が あたりまえの技術 として認識されていない、まだ馴染みがない

特殊なハードウェアを必要としない、AI技術だけで確立された 顔認証・なりすまし防止 を活用することで現在、未来に対してコストパフォーマンス良く、普及ができると考えています。

# 特殊なデバイスを必要としない“なりすまし防止”技術（現在）

Saffe を活用することでハードウェアコストを低減することができ、かつ、“なりすまし防止”に必要な認証処理時間も格段に低減することが可能となります。

## ハードウェアコスト

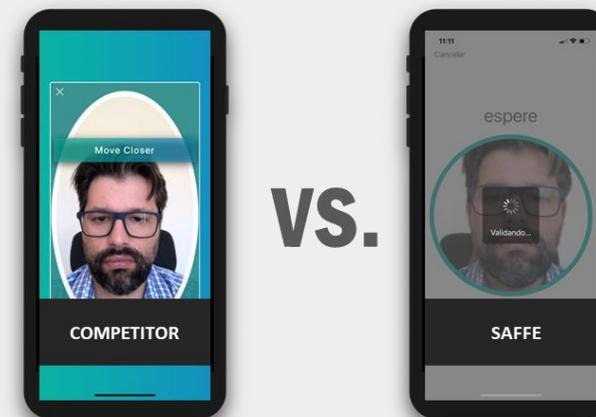
コロンビアのスーパーマーケットにおける顔認証決済のコンペで **競合他社と比較し、顔認証用ハードウェアコストを80%削減**した提案をおこなうことができました。

顔認証タブレット 1台あたりのコスト

競合他社X	: 1,000USD
Saffe	: 200USD ( 80% off )

これは競合他社が“なりすまし防止”用に3Dカメラを搭載した高価なタブレットを必要としたためです。

## 認証処理時間

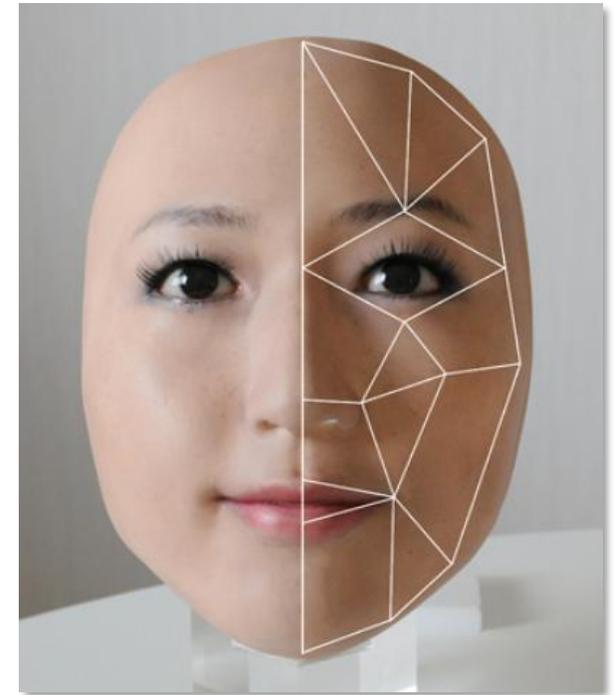
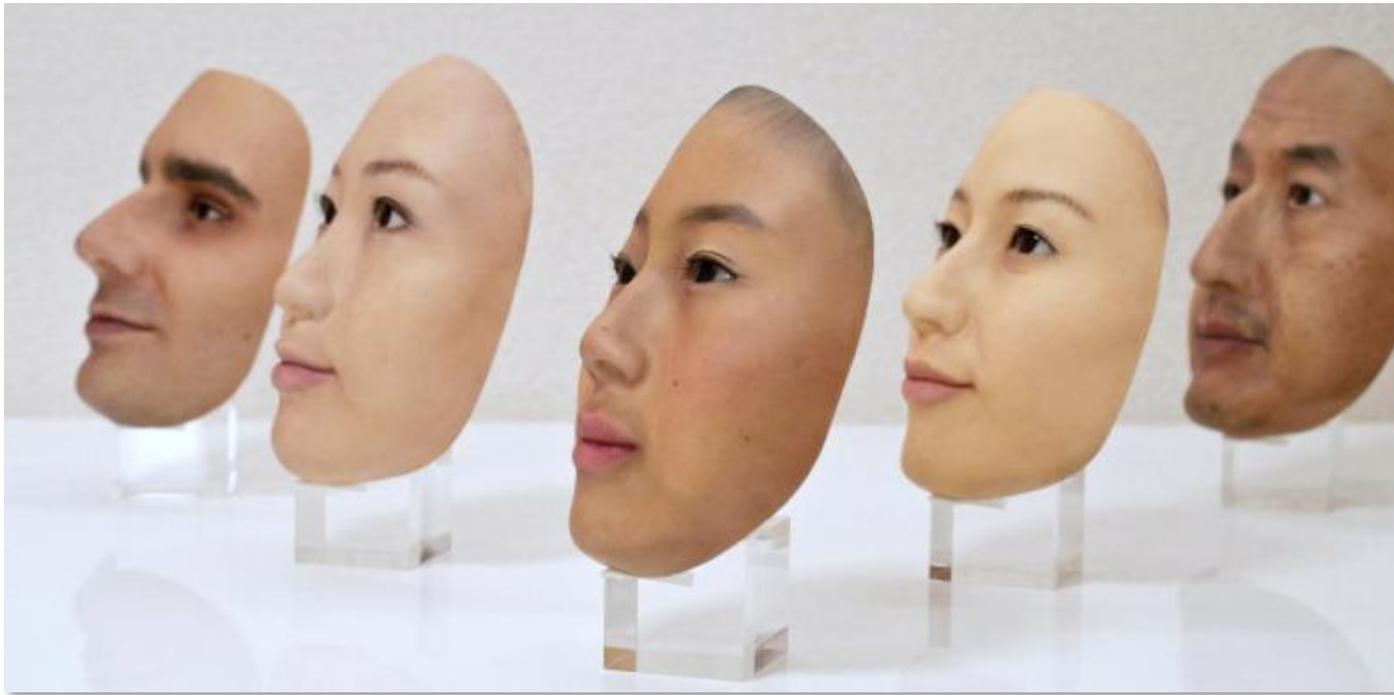


 **6X FASTER**

他社技術は3Dカメラなどを使わない場合、左右に顔を向けたり、まばたき等の動作で生体チェックをおこなうため、**Saffeの6倍の認証時間を要する**比較結果のケースがありました。

“なりすまし”などの犯罪行動は残念なことに日々、進化を遂げており、ハードウェア依存の防御は突破されてしまうと、途端に無力化されてしまいます。

AI(ソフトウェア)技術はアップデートが可能で、日々進化する犯罪に対してコストパフォーマンスよく対抗できる唯一のアプローチ方法であると考えています。



## 顔認証 普及の阻害要因

1. 顔認証にリスクを感じる、安全面で大丈夫かどうか不安がある
2. 導入コストが高い、費用対効果が見いだせない
3. どのように活用できるのか、どのように導入したらいいのかイメージが湧かない
4. 顔認証が あたりまえの技術 として認識されていない、まだ馴染みがない

「 論より証拠 」、人は様々な先行事例を目の当たりにして、  
自分事として捉えやすくなるなと考えています。

導入事例を獲得すると共に、世の中に事例を紹介することで顔認証の普及を推進しています。

「決済」「eKYC（本人確認）」「セキュリティ」3つの注力分野で先行事例を獲得しております。

## 決済



① 顔認証を活用した乗車運賃の顔パス決済（熊本市交通局様、富山地方鉄道様、アルピコ交通様、他）

② 顔認証を活用した乗車チケット発券サービス（京成電鉄株式会社様）

③ バス運賃顔認証クレジット決済（スペイン・マドリード）

④ スーパーマーケット顔認証決済（コロンビア）

## eKYC （本人確認）



⑤ 顔認証を使った銀行口座開設（ブラジル）

⑥ 厚生労働省 支払基金様 マイナンバーカード・オンライン資格確認 システム開発（松村エンジニアリング様）

⑦ AI映像監視・顔認証 入退構ソリューション「TRASCOPE-AI」 システム開発（丸紅ネットワークソリューションズ様）

## セキュリティ



⑧ ホームセキュリティ 顔認証&なりすまし防止（大手セキュリティ会社様）

⑨ コワーキングスペース向け 顔認証入退室管理 アクセスコントロール システム開発（fabbit様、JSB様、他）

⑩ 保育園・幼稚園向け お子様の見守りシステム開発（桐光学園みどり幼稚園様）

丸紅株式会社様（交通インフラプロジェクト部）とのリレーションがあり、交通系の事例を中心に取り組んでおります。

## 顔認証 普及の阻害要因

1. 顔認証にリスクを感じる、安全面で大丈夫かどうか不安がある
2. 導入コストが高い、費用対効果が見いだせない
3. どのように活用できるのか、どのように導入したらいいのかイメージが湧かない
4. 顔認証が あたりまえの技術 として認識されていない、まだ馴染みがない

**「国や地方公共団体などが推進する技術は確かなものである」という点、印象ベースではあるかもしれませんが、さらなる普及の後押しにつながると考えております。**

厚生労働省様（ 社会保険診療報酬支払基金様 ）が主導するマイナンバーカードを活用した保険資格確認で、**Saffe 顔認証・なりすまし防止技術が審査を合格し、許認可をいただくことができました。**2024年時点で、5社が許認可を受けておりますが、グローバルの技術で許認可をいただいているのは当社のみとなります。非常に厳しい審査ながらも、顔認証技術を国内普及するため、皆様に安心してご利用いただけるようにするため、取り組みました。R.D.Works および Saffe Ltd. としては**向こう10年間の顔認証のサービス提供を誓約しております。**今後も顔認証の国内導入を強く、推進して参ります。顔認証Saffeを安心してご用命いただければ幸いです。



ひと、暮らし、みらいのために

## 厚生労働省

Ministry of Health, Labour and Welfare



社会保険診療報酬支払基金  
Health Insurance Claims Review & Reimbursement Services



厚生労働省様向け  
顔認証サービス  
提供の義務

# 10年

## 1. 会社概要

## 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

# 1. 世界各国に於ける顔認証技術の利用状況

## 侵害的に広く利用している国のトップ3は中国、ロシア、UAE

人口が多い上位99の国と地域を対象に、政府機関や警察、空港、学校、銀行、職場、バス、電車で顔認証技術がどのように利用されているかを調査、分析した。

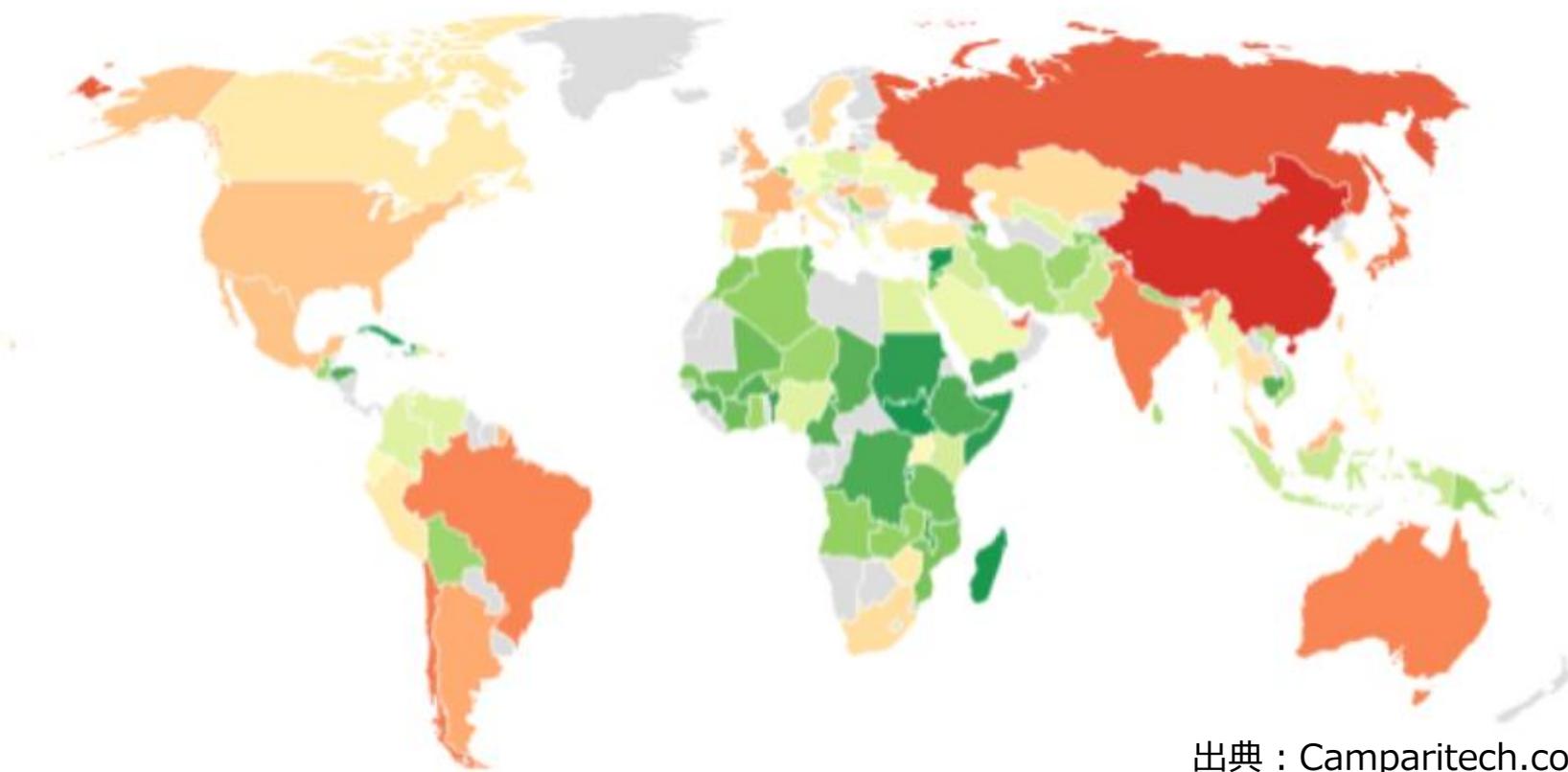
ITやカメラを用いた顔認証技術は現在、さまざまな場面で使われており、多くの人にとって日常生活の一部となっている。専門家によると、2020年に38億ドル規模だった世界の顔認証技術市場は、2025年には85億ドル規模に成長する見通し。

顔認証技術を禁止していることが知られている国は、ベルギーとルクセンブルクのみ。

### The global map of facial recognition technologies



顔認証技術の利用状況 色が赤いほど利用範囲が広い

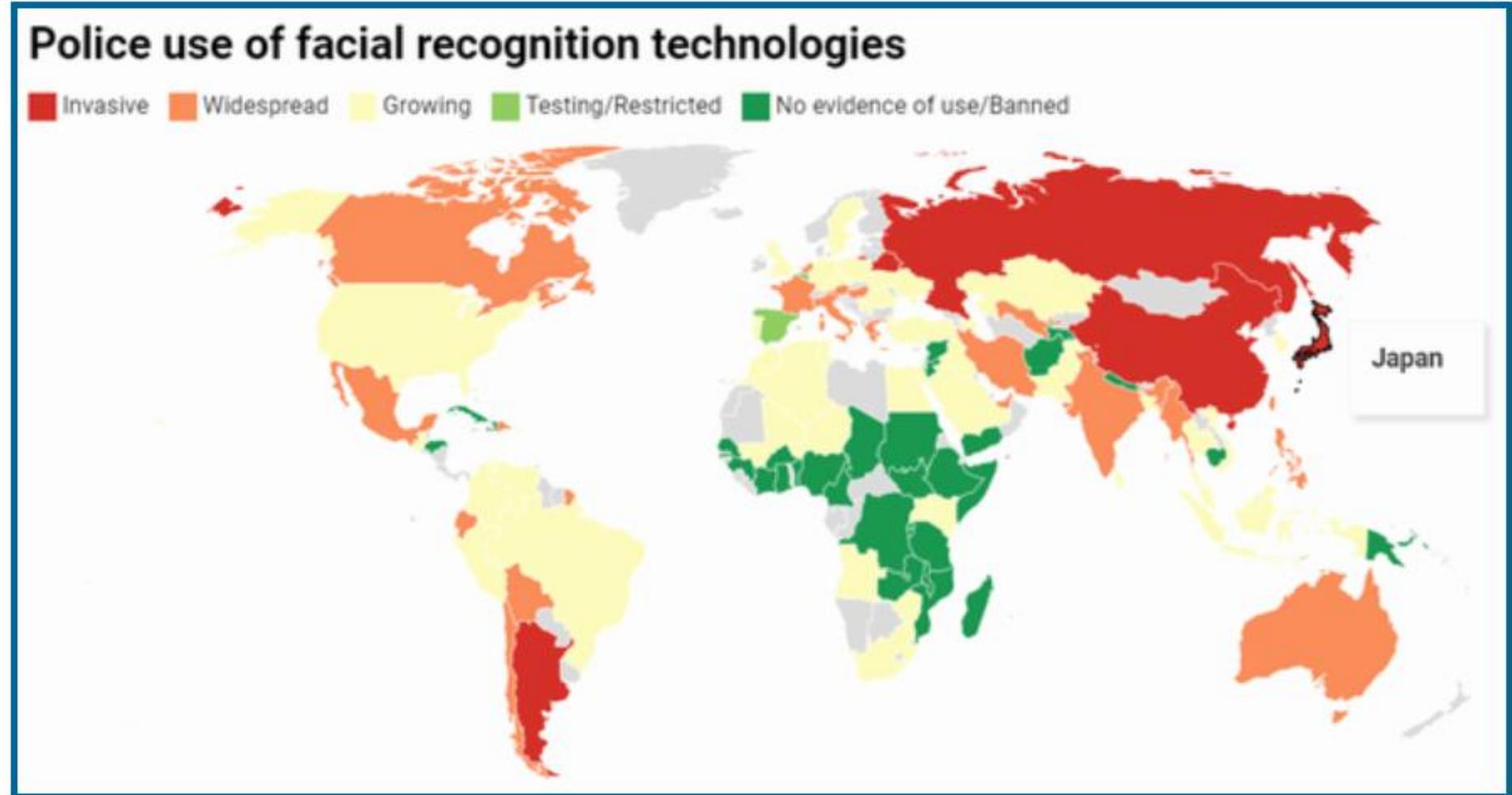


出典 : Camparitech.com

## 2. 警察に於ける顔認証技術の利用状況

### Police use of facial recognition technologies

警察の70%が何らかの顔認識技術を利用



警察に於ける顔認識技術の利用状況 色が赤いほど利用範囲が広い

出典 : Camparitech.com

## 3. Comparitechによる調査結果

### 政府機関の70%が顔認識技術を大規模に利用

- ① ほぼ80%の国で一部の銀行と金融機関が顔認識技術を利用
- ② 政府機関の70%が顔認識技術を大規模に利用
- ③ 警察の70%が何らかの顔認識技術を利用
- ④ 60%の国が一部の空港で顔認識技術を利用
- ⑤ 40%程度の国で顔認識技術が一部の職場に実装済み
- ⑥ 40%以上の国が何らかの顔認識技術を利用、COVID-19の感染追跡、モニタリング、抑制を図っている
- ⑦ 20%近くの国で一部の学校が顔認識技術を利用
- ⑧ 20%の国で一部のバスで顔認識技術が利用され、30%の国で一部の電車／地下鉄で顔認識技術を利用

出典 : [Comparitech.com](https://www.comparitech.com)

# 4. 侵害的に利用している国

## 政府機関の70%が顔認識技術を大規模に利用

顔認識技術が広く利用されている  
上位22カ国の内訳 総合得点  
\*はCOVID-19対策を含む。

各国の総合得点は0~40点の範囲にあり、得点が少ない国ほど、顔認識技術を広く、侵害的に利用している。次に挙げる22カ国は総合得点が最も少ない。

	総合得点	総合得点*	政府機関	警察	空港	学校	銀行/金融	職場	バス	電車	COVID-19対策
中国	5	6	0	0	1	0	1	1	1	1	1
ロシア	9	10	1	0	1	1	1	2	2	1	1
UAE	10	11	1	1	1	1	1	2	1	2	1
チリ	12	13	1	1	2	2	1	2	2	1	1
インド	12	13	1	1	2	2	1	2	2	1	1
日本	12	14	1	0	1	2	1	3	2	2	2
オーストラリア	13	14	1	1	1	3	1	3	2	1	1
ブラジル	13	15	3	2	1	1	1	2	1	2	2
アルゼンチン	16	18	1	0	1	5	1	2	5	1	2
フランス	17	18	2	1	1	5	1	3	3	1	1
ハンガリー	17	18	1	1	2	5	2	2	2	2	1
マレーシア	17	19	1	2	1	2	1	2	5	3	2
英国	17	20	2	2	1	5	1	2	2	2	3
メキシコ	18	20	1	1	2	5	2	2	3	2	2
米国	18	20	2	2	1	3	1	2	5	2	2
台湾	19	20	2	1	1	2	1	2	5	5	1
ルーマニア	19	21	1	2	1	1	1	3	5	5	2
スペイン	19	24	2	3	2	5	1	2	1	3	5
カザフスタン	20	22	2	2	3	4	1	5	1	2	2
南アフリカ	20	22	1	2	2	3	2	3	5	2	2
台湾	20	22	1	2	2	2	1	5	5	2	2
スウェーデン	20	25	3	2	2	5	1	3	2	2	5

出典 : Camparitech.com

## 5. 各国の利用状況

### 中国 (5点)

中国は顔認識技術の最大の利用国としてしばしば名前が挙がる。中国の政府機関と警察は顔認識技術を広範に、そして多くの場合、プライバシーを侵害する監視手法とともに利用している。例えば、蘇州市は顔認識技術を利用して、パジャマを着て外出した7人を特定し、市の「WeChat」アカウントで画像を公開した。中国のある公園は顔認識技術を用いて、人々がトイレトペーパーを盗むのを防いでいる。学校が顔認識技術を使って、生徒がどの程度熱心に授業を聞いているかを把握している場合も多い。生徒が集中していないように見えると、成績が下がってしまう。

### ロシア (9点)

8つのカテゴリー全てにおいて、ロシアで顔認識技術が利用されていることは明らかだった。最近では、ロシアの反体制派指導者アレクセイ・ナワリヌイ氏の収監に対する抗議デモの前に、顔認識技術によって抗議者が特定され、勾留されたとのうわさが流れた。

### UAE (10点)

上位22カ国の多くと同様に、UAEは多くのカテゴリーで「プロセスのスピードアップ」と「詐欺防止」のために、顔認識技術を導入している。政府サービスへのアクセスから学校の出席登録まで、顔認識技術は幅広く利用されている。アブダビの警察もパトロールカーをアップグレードして顔認識技術を導入し、不審者や指名手配者の特定に役立てている。

出典 : [Camparitech.com](https://www.camparitech.com)

## 6. 各国の利用状況(2)

### 日本・チリ・ インド (12点)

これらの国は、全てのカテゴリで顔認識技術のある程度利用している。最も懸念される事項として、日本では顔認識技術と市民のソーシャルメディアアカウントを組み合わせ、犯罪者の追跡に用いていることが挙げられる。国家公安委員会は約1000万人の日本人の顔画像を保管しており、警察がデータベースにアクセスできるようにした。顔認識技術とともに利用できるようにするためだ。

チリでは2022年までに市民の大部分が、顔認識技術を利用した電子IDカードを持つようになる。インドでは、中央政府と州政府で、約16種類の顔認識技術システムが使われており、さらに17種類の顔認識技術システムが開発されている。

### オーストラリア・ ブラジル (13点)

オーストラリアの警察は、物議を醸しているClearviewの顔認識技術を使っていることが明らかになった。同社はソーシャルメディア画像を使ってデータベースを作成していたことが判明している。ブラジルでは政府機関と警察による顔認識技術の利用はまだ普及していないが、増加している。学校と公共交通機関で、顔認識技術は既に広く実装されている。

### アルゼンチン (16点)

首都ブエノスアイレスでは顔認識技術が、未成年の注意人物を含むデータベースとリンクされているとの報道があった。リアルタイム顔認識技術システムによって誤って特定、勾留された人々に関する記事も幾つか出ている。アルゼンチンではバスと学校を除く他のほとんどのカテゴリでも、顔認識技術が利用されている。

出典 : [Camparitech.com](https://www.camparitech.com)

## 7. 各国の利用状況(3)

### フランス・英国・ハンガリー・マレーシア (17点)

フランスと英国、ハンガリーは、学校を除く全てのカテゴリーで、マレーシアはバスを除く全てのカテゴリーで、顔認識技術を利用している。この4カ国は、政府機関や警察、銀行、空港で、顔認識技術が広く利用されているか、または利用が増加している。公共交通機関でも利用が進んでいる。

### 米国・メキシコ (18点)

メキシコの学校では、顔認識技術の利用例は知られていない。だが、メキシコでもバス以外の他のカテゴリーでは、顔認識技術が広く利用されているか、または利用が増加している。米国でも顔認識技術の利用が増加しているが、バスにはまだ導入されていない模様だ。

### 台湾・スペイン・ルーマニア (19点)

この4カ国は、ほとんどのカテゴリーで顔認識技術の普及が進んでいるが、まだ導入されていないカテゴリーがある。導入されていないカテゴリーは、ルーマニアでは公共交通システム、スペインでは学校、台湾ではバスだ。

### タイ・カザフスタン・南ア・スウェーデン (20点)

これらの国では大抵の場合、顔認識技術の普及度はカテゴリーによってまちまちだ。なお、スウェーデンでは、学校における顔認識技術の利用は禁止されている。

出典 : Camparitech.com

## 8. 顔認証2大輸出国の米国と中国の状況

### 中国が顔認識技術で世界最大の輸出国に

#### 「監視社会」の拡大に高まる懸念

シンクタンクのブルッキングス研究所が23年1月中旬に発表した調査結果によると、顔認識技術を含む中国企業の輸出案件は201件、次いで米国企業は128件と、中国企業が顔認識技術で世界を牽引していることが明らかになっている。この研究にはハーバード大学とマサチューセッツ工科大学（MIT）の研究者が参加した。

また中国は、全般的なAIの分野でも世界のトップに立っている。136の輸入国に対する1,636件の輸出案件のうち、250件は何らかのAIを含むものだったのだ。2番目に多い輸出国は米国で、215件のAI関連の取引があった。

こうした輸出によって他国の政府は監視を強化でき、市民の人権が損なわれる可能性がある」と報告書は主張している。

### 米国で加速する「中国の技術」の規制

#### 米国の警察では顔認識技術の導入が進展

米国では、世界的に中国の技術を制限することへの超党派の関心が高まっている。前大統領のドナルド・トランプの下、米国政府は米国やほかの地域におけるファーウェイ（華為技術）の5G技術の使用を制限することを目的とした規制を導入し、中国のAI企業に狙いを定めた半導体の禁輸措置を講じた。

米国の警察では顔認識技術の導入が進んでおり、一部の都市は使用を制限しているものの、使用を限定したり制限したりする全国的な規制は存在しない。Clearview AIなど一部の米国企業は、監視カメラで撮影した人物の画像と、オンライン上の身元情報とを結びつけることができる顔認識ツールを開発し、輸出している。この使い方は法的な正当性なしに市民のプライバシーを侵害するものであると、市民の自由人権団体が主張しているものだ。

# 9. 米国政府機関が活用するAI顔認識の可能性

## 米国政府機関によるAI顔認識の活用事例

### 米国の政府機関によるAI顔認識の活用事例

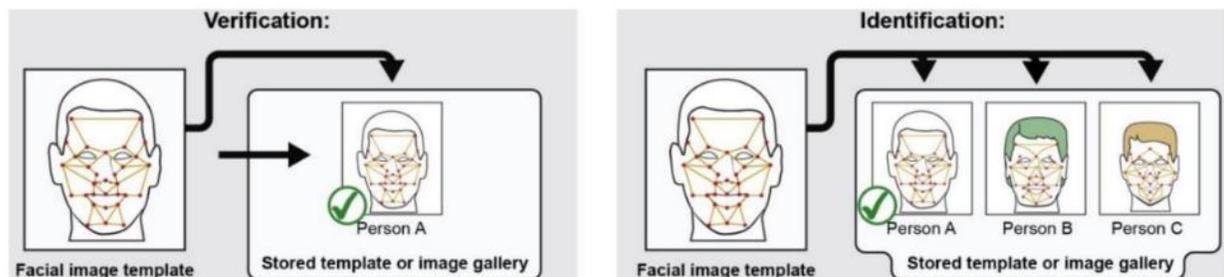
世界米国政府説明責任局（Government Accountability Office : GAO）が2022年6月29日に公開したレポートでは、米国の政府機関によるAI顔認識の活用事例が示されている。政府機関によるAI顔認識の目的は、

- ①パソコン、スマートフォンへのアクセス制御に利用される「デジタルアクセス・サイバーセキュリティ」、
- ②捜査対象者の特定、行方不明者や犯罪被害者の特定に利用される「国内法執行」、
- ③施設や建物などへの物理的なアクセスの制御に利用される「物理的セキュリティ」、
- ④空港での国内旅行者、米国への入国を申請する旅行者の身元を確認する「国境と輸送のセキュリティ」、
- ⑤テロリストと疑われる人物調査に利用される「国家安全保障と防衛」、
- ⑥車の運転中の注意力を評価するために使用されるアイトラッキングなど「その他」

の6つに分類されるトップに立っている。136の輸入国に対する1,636件の輸出案件のうち、250件は何らかのAIを含むものだったのだ。2番目に多い輸出国は米国で、215件のAI関連の取引があった。

こうした輸出によって他国の政府は監視を強化でき、市民の人権が損なわれる可能性がある」と報告書は主張している。

図表 1 AI 顔認識における検証(左)と識別(右)の概要



- ①検証機能とは、スマートフォンやコンピューターなどに保存されている顔データと、カメラを通じて認識される顔データを照合し、同一人物か否かを判定する本人確認の仕組み
- ②識別とは、1人の顔データを特定の場所に保存されている複数の顔データと照合して、一致または一致する可能性のある人物を特定する仕組み

# 10. 米国政府機関が使用するAI顔認識システムの目的

## 米国政府機関によるAI顔認識の活用事例

Federal Agency	Purpose					
	Digital access	Domestic law enforcement	Physical security	Border and transportation security	National security and defense	Other
Department of Agriculture	●	⊗	⊗	⊗	⊗	⊗
Department of Commerce	●	⊗	●	⊗	⊗	⊗
Department of Defense	⊗	●	●	⊗	●	●
Department of Energy	●	⊗	●	⊗	⊗	⊗
Department of Health and Human Services	●	●	●	⊗	⊗	⊗
Department of Homeland Security	●	●	⊗	●	●	⊗
Department of the Interior	●	●	⊗	⊗	⊗	⊗
Department of Justice	●	●	●	⊗	●	●
Department of State	⊗	⊗	⊗	●	●	⊗
Department of the Treasury	●	●	⊗	⊗	⊗	⊗
Department of Veterans Affairs	●	⊗	⊗	⊗	⊗	⊗
Agency for International Development	●	⊗	⊗	⊗	⊗	⊗
Environmental Protection Agency	●	⊗	⊗	⊗	⊗	⊗
General Services Administration	●	⊗	⊗	⊗	⊗	⊗
National Aeronautics and Space Administration	●	⊗	⊗	⊗	⊗	●
National Science Foundation	●	⊗	⊗	⊗	⊗	⊗
Office of Personnel Management	●	⊗	⊗	⊗	⊗	⊗
Social Security Administration	●	⊗	⊗	⊗	⊗	⊗

Legend: ● = Yes, ⊗ = No

### 国防省と財務省の例

国防総省は、「国内法執行」、「物理的セキュリティ」、「国家安全保障と防衛」、「その他」の4つの目的のためにAI顔認識を利用している（左図表赤枠の●部分）。

また、財務省は、「デジタルアクセス・サイバーセキュリティ」、「国内法執行」の2つの目的のためにAI顔認識を利用していることがわかる（左図表青枠の●部分）。

# 11. アメリカ市場における顔認証利用状況

## 1億3,100万人が毎日顔認証を利用

顔認証技術の普及により、利便性に加えて「安全性」への関心が高まる

サイバーリンク（本社：台湾新北市）による、アメリカ人による顔認証の一般的な利用状況を分析したアメリカ市場に関する調査報告によると、1億3,100万人ものアメリカ人が毎日顔認証を使用しており、その半数が様々な使用状況において、毎日少なくとも3つの異なるアプリケーションを通じて顔認証機能を使用している。

顔認証機能を利用する人のうち、68%がパソコンやスマートフォンなど個人端末のロック解除に、51%が健康管理やチケット購入などモバイルアプリへのログインに、さらに42%の人々はインターネットバンキングへのログインに使用している。

若い世代ほど顔認証を利用する頻度が高く、全体的に顔認証の利用に対してよりオープンな姿勢を示している。18～34歳の57%が1日1回以上何らかの顔認証を利用しているのに対し、35～54歳では40%、55歳以上では24%にとどまっている。また、若年層は、自分の顔が保存・販売されないこと（43%、他の層より4～8ポイント高い）、明確に説明された注意書きや利用規約を提供されること（37%、他の層より4～8ポイント高い）に対して、他の層より強いこだわりを持っている。また、一度導入すると、75%が1日1回以上利用しており、ユーザーから高い支持を得ている。

顔認証技術の利用に前向きな人のうち、データ、個人情報、資産の保護が向上するならば、店舗での買い物、レストランでの食事、旅行中の顔認証に前向きであると答えた人の割合が最も高かった（54%）。また、家庭や職場の安全性向上のために検討すると答えた人も多くいる（42%）。また、利便性も重要で、顔認証に前向きな人の45%が「行列の待ち時間が減るなら」、43%が「必要なものをより早く、より便利に手に入れられるなら」と回答している。また、「マスクの着用」（23%）、「人と会わない」（20%）、「VIP待遇」（20%）は、重要度は低いものの、重要視されている。

今回の報告では、ほとんどの消費者が顔認証を使用する際、データのセキュリティを非常に重視していることを指摘しており、消費者の個人データの悪用防止をする必要がある。

## 12. 日本におけるAI顔認識活用の可能性

### 日本においても、社会の安心・安全の確保に向け、顔認識の普及が見込まれる

国民のプライバシーに最大限配慮したルール作りや透明性を確保する情報公開ルールが必要

以上のように、米国ではAI顔認識が政府機関において幅広く活用されている。これは、AI顔認識が今後さらに社会に幅広く浸透していく可能性を示唆する。一方、政府機関の従業員がAI顔認識を使用して1,000件以上の目的外の顔認識検索を行っていた事実も判明しており、プライバシーに関連する法を順守しない行動に伴うリスクが懸念されている

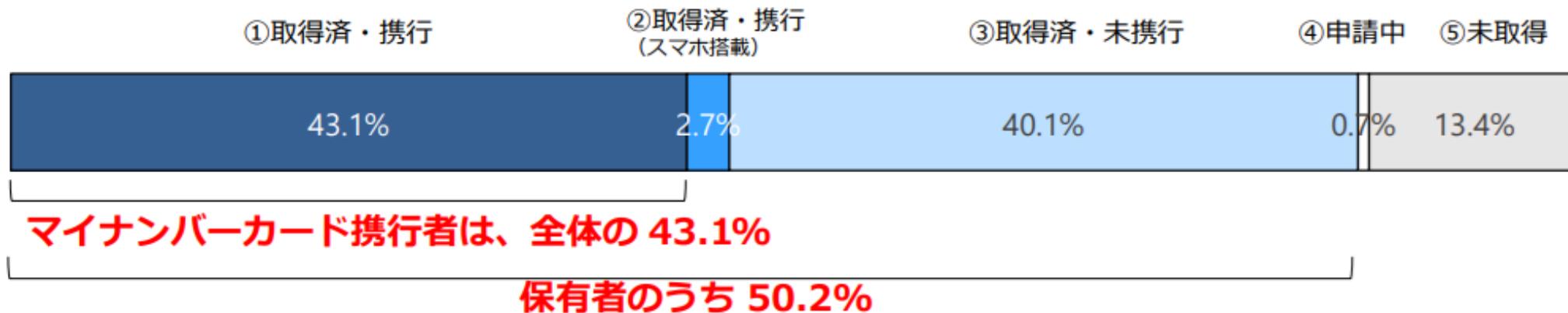
今後、日本においてもAI顔認識の普及が見込まれる中、政府機関や民間事業者がAI顔認識を利用する場合、国民のプライバシーに最大限配慮したルール作りに加えて、誰がいつどのような目的でAI顔認識を利用したのかについて、公の場で確認できる仕組みを構築することが求められる。加えて、万が一政府機関や民間事業者によるAI顔認識の利用に疑義が生じた場合に、国民がその運用実態を確認できるような透明性を確保する情報公開ルールも必要になるだろう。

AI顔認識を積極的に活用していくことは、社会の安心・安全の確保につながる可能性がある。ただ一方で、プライバシー確保の観点からも、国民的な議論を踏まえた上で実施可否を慎重に判断すべきテーマでもあるといえるだろう。

出典：第一生命経済研究所 LIFE DESIGN REPORT

# 13. 日本におけるマイナンバーカードの普及

## マイナンバーカードの普及率は85.9%、保有者の内半数は携行者 (2023年12月調査)



## 保有者の約 4 割弱がマイナ保険証を利用したいと考えている (2024年2月調査)

Q.あなたは、マイナ保険証について、どのような印象や考えをお持ちですか。それぞれについて、あなたのお気持ちに近いものを1つお答えください。



マイナンバーカードを携行している人が、医療機関・薬局でマイナ保険証を利用すれば、マイナ保険証の利用率が大きく伸びる可能性  
⇒医療機関・薬局におけるお声かけ等の取組が重要

出典：厚生労働省「マイナ保険証利用促進のための取組・支援策について」

# 14. マイナ保険証の利用促進に向けた取り組み

## マイナンバーカード医療機関・薬局への支援金

### 目的

医療機関等において、カードリーダーの操作に慣れない患者への説明など、マイナ保険証の利用勧奨に取り組んでいただくことで、マイナ保険証の利用促進を図ります。

### 概要

マイナ保険証の利用率(初診・再診・調剤)<sup>※1</sup>が、2023(R5)年10月から5%ポイント以上増加した医療機関等を対象に、支援を実施します。

※1は次頁参照

### 期間

**2024(R6)年1月～11月**

※前半期:2024(R6)年1月～5月(5ヶ月間) / 後半期: 2024(R6)年6月～11月(6ヶ月間)

### 支援内容

- 前半期(又は後半期)のマイナ保険証平均利用率と、2023(R5)年10月の利用率を比較し、次頁の表の増加量に応じた支援単価を、前半期(又は後半期)のマイナ保険証総利用件数に乗じた額が支援金として交付<sup>※2</sup>されます。

### 医療機関・薬局への支援金

2023.10の利用率からの増加量	前半期(2024.1～5)支援単価	後半期(2024.6～11)支援単価
5%pt以上	20円/件	—
10%pt以上	40円/件	40円/件
20%pt以上	60円/件	60円/件
30%pt以上	80円/件	80円/件
40%pt以上	100円/件	100円/件
50%pt以上	120円/件	120円/件

### 診療報酬上の評価

#### 【医療DX推進体制整備加算】

マイナ保険証、電子処方箋などの「医療DX推進体制」を評価

<初診> 8点(歯科6点、調剤4点)

施設要件(例)

- ①マイナ保険証での取得情報を診療室で使用できる体制【R6.6～】
- ②マイナ保険証の利用勧奨の掲示【R6.6～】
- ③マイナ保険証利用実績が一定程度(●%)以上であること【R6.10～】
- ④電子処方箋を発行できる体制(薬局は受け付ける体制)【R7.4～】
- ⑤電子カルテ情報共有サービスを活用できる体制【R7.10～】

10

出典：厚生労働省「マイナ保険証利用促進のための取組・支援策について」

# 15. マイナ保険証の利用促進に向けた取り組み(2)

## マイナ保険証を基本とする仕組みに移行 (現行の健康保険証の発行は令和6年12月2日に終了)

- ① 窓口に来た患者の方々に対して、「保険証をお持ちですか。」ではなく、「マイナンバーカード(マイナ保険証)をお持ちですか。」とお声をかけていただく
- ② マイナ保険証利用促進のための患者向けリーフレットなどによる周知、健康保険証の利用申込みに関する掲示等による案内
- ③ 各医療機関等のHPの外来予約・入院手続きのページにおいて、持参するものとして「保険証」のみを案内している事例がみられるが、「マイナンバーカード」をご案内いただく
- ④ 利用率の目標設定、担当者の配置やマイナ保険証利用者のための専用レーンの設定
- ⑤ カードリーダーの操作に慣れない患者へのご説明(支援金による支援) (→2)
- ⑥ 診察券・子ども医療費助成などの受給者証のマイナンバーカードへの一体化

マイナンバーカードをお持ちの方は、こちらで健康保険証利用の申込みが可能です。

本当に簡単！マイナンバーカード持って良かった！

カンタンに




デジタル庁 MIC 総務省 厚生労働省

健康保険証利用の申込みのお問合せ先

マイナンバーセンター 0120-95-0178

受付時間: 平日 9時30分～20時0分 土日祝: 9時30分～17時30分

出典：厚生労働省「マイナ保険証利用促進のための取組・支援策について」

# 16. 顔認識技術の3つの用途

## ①と②の用途については法令・社会受容面での課題は少ないが、③の用途は課題が多い

### ①本人同意に基づき個人認証の目的で行われる顔認証サービス

- Facial Authentication / Facial Verification (顔認証)
- 多くは1-to-1照合
- スマホやPCのログイン、空港の顔認証ゲート、テーマパークの年間パス、顔認証決済、ビル入退館など

### ②容疑者の顔写真と犯罪者DB等の顔画像を捜査目的で照合する顔照合

- Facial Matching (顔照合)
- 1-to-many照合
- 警察機関による利用

### ③公共空間などで（本人同意なく）不特定多数を対象に行われる自動顔認識

- Automated Facial Recognition (AFR) / Live Facial Recognition (LFR) (自動顔認識)
- many-to-many照合
- 警察機関（サーベイランス）や民間企業（万引き犯顔認識、リピート顧客分析等）による利用

出典：Institute for International Socio-Economic Studies

# 17. 顔認識技術の3つの用途毎の対応

## 課題の多い③の用途では、日本に於いても大阪駅前ビルと札幌市の実証実験で炎上

### ①本人同意に基づき個人認証の目的で行われる顔認証サービス

- 空港ゲートでの顔認証や店舗での決済時の顔認証、オフィスへの入退時の顔認証などは、本人が同意した上でのデータ利用であるため、（日米欧の）法律上は基本的には問題ない（前述のようにEU・英国では同意強制や映り込みは不可）
- また、顔認証以外の選択肢を用意することで「同意強制」を避ける、顔認証には専用レーンを用意することで「映り込み」を避けるといった対応を行うことで、社会的な受容性の面でも問題ないと考えられる

### ②容疑者の顔写真と犯罪者DB等の顔画像を捜査目的で照合する顔照合

- 犯行現場等で取得された「容疑者」の顔写真に対する顔照合であり、犯罪と無関係の一般市民の権利を侵害するものではない
- 顔照合DBの内容が（一般市民を含まない、不正確な情報に基づかない、SNSなどの情報を目的外利用しないなど）適切であり、人種・性的バイアスに十分に配慮されたソフトウェアが用いられ、またシステムによる自動判断ではなくヒューマンチェック（人間の関与）を保証する制度設計がなされていれば、特に利用を制限する理由は見当たらない

### ③公共空間などで（本人同意なく）不特定多数を対象に行われる自動顔認識

- 欧米における顔認識技術に対する批判は③の用途に集中。主な懸念は次の5点。①顔画像の取得の容易さ、②透明性の欠如、③行動の自由の萎縮効果、④顔認識技術の精度、⑤顔認識技術におけるバイアス
- 日本での炎上事例（大阪駅前ビル実証、札幌市実証）も③の用途（誤認を含む）

出典： Institute for International Socio-Economic Studies

# 18. 日米欧における顔認識と法規制/社会的受容性

## 日本では、①と②の用途に対する社会的受容性はある

日本では、民間企業が店舗等で個人の顔特徴データを取得する際に、個人情報保護法上は、本人同意までは求められず、本人に利用目的等を通知または公表をすればよいこととなっている

しかし、後述のように不特定多数の個人に対する自動顔認識に対しては抵抗感が強く、社会的コンセンサスが得られにくい用途であるため、民間企業が日本国内でこの③の利用を行うに当たっては慎重な検討と対応が求められる

日本においては、警察や自治体等の公的機関が公道などの公共空間で監視カメラを用いて顔特徴データを取得したり自動顔認識を行うことは、明示的に規制されている訳ではない。しかし、不特定多数の個人に対する自動顔認識に対しては国内においても抵抗感が強く（※）、社会的コンセンサスが得られにくい用途となっている

		日本	米国	欧州・英国
①本人同意の下の顔認証	法律上は可能か	○	○	○ (ただし同意の強制や、同意のない個人からの顔特徴データ取得は×)
	社会的受容性はあるか	○	○	○
②容疑者写真の顔照合	法律上は可能か	○?	△ (サンフランシスコ市等で×)	○
	社会的受容性はあるか	○	○	○
③公共空間での自動顔認識(警察利用) ※本人同意なし	法律上は可能か	○?	△ (サンフランシスコ市等で×)	○
	社会的受容性はあるか	△	△	△
③'店舗等での自動顔認識(民間利用) ※本人同意なし	法律上は可能か	○	△ (テキサス州、イリノイ州、ワシントン州で×)	×
	社会的受容性はあるか	△	△	×

出典： Institute for International Socio-Economic Studies

# 1. 会社概要

# 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

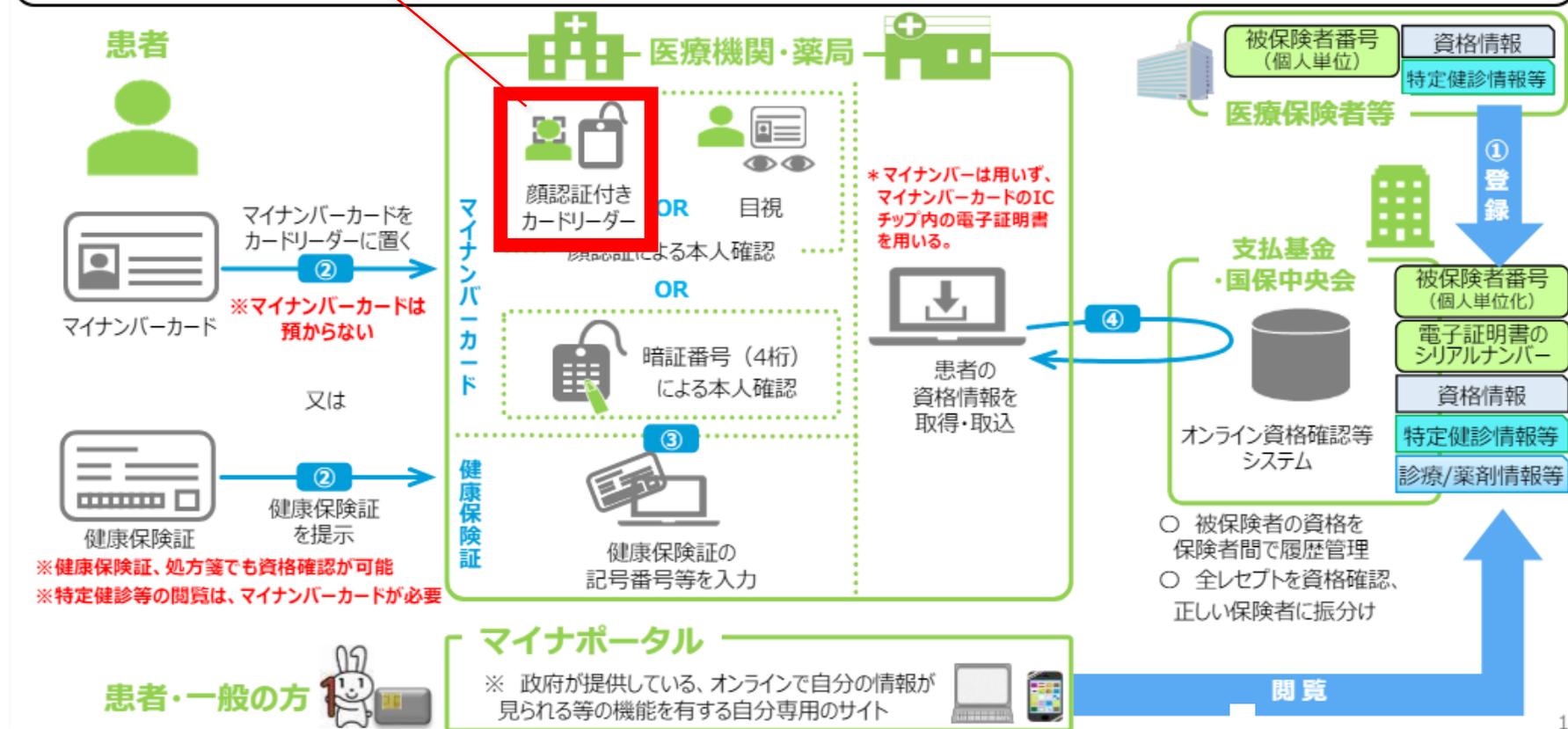
Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)



- オンライン資格確認等システムの導入により、
  - ① 医療機関・薬局の窓口で、**患者の方の直近の資格情報等（加入している医療保険や自己負担限度額等）が確認できる**ようになり、期限切れの保険証による受診で発生する過誤請求や手入力による手間等による**事務コストが削減**できます。
  - ② また、マイナンバーカードを用いた本人確認を行うことにより、医療機関や薬局において特定健診等の情報や診療/薬剤情報を閲覧できるようになり、**より良い医療を受けられる環境**となります（マイナポータルでの閲覧も可能）。



出典：総務省WEBサイト「マイナンバー制度」

販売企業	富士通Japan株式会社	パナソニックコネク 株式会社	株式会社アルメックス	キャノンマーケティング ジャパン株式会社	アトラス情報サービス 株式会社
製造企業	株式会社PFU			カードサービス株式会社 (旧 株式会社レスターキャステック)	株式会社 松村エンジニアリング
製品名	Caora	顔認証付きカードリーダー (マイナンバーカード対応)	Sma-paマイナタッチ	Hi-CARA	EXC-9000
製品名イメージ					

紙幣鑑別機/真がん判定装置のパイオニア 松村エンジニアリング

# MATSUMURA



世界中の偽造紙幣の鑑別を可能とすること  
 常に新しい技術とアイデアを持ち  
 巧妙化する偽造紙幣を見破ること  
 こうして社会に貢献することが私たちの使命です

商号	株式会社 松村エンジニアリング ( Matsumura Engineering Co., Ltd. )
代表者	代表取締役会長兼社長 松村 喜秀
設立	昭和63年(1988年)9月24日
資本金	1,000万円
本社	〒111-0052 東京都台東区柳橋二丁目1 8 番 4 号
	TEL 03-6858-6611 (代表)
事業内容	セキュリティ関連製品の開発・製造・保守

## ソフトウェア開発 全般を担当

### 顔認証機能付きカードリーダー EXC-9000



厚生労働省が提供する数百ページに及ぶ仕様を読み込み、アプリケーションを実装しました。

### 顔認証

ICチップに格納された写真と  
カメラ撮影した写真の照合

カメラの映像



カメラ撮影した写真



照合



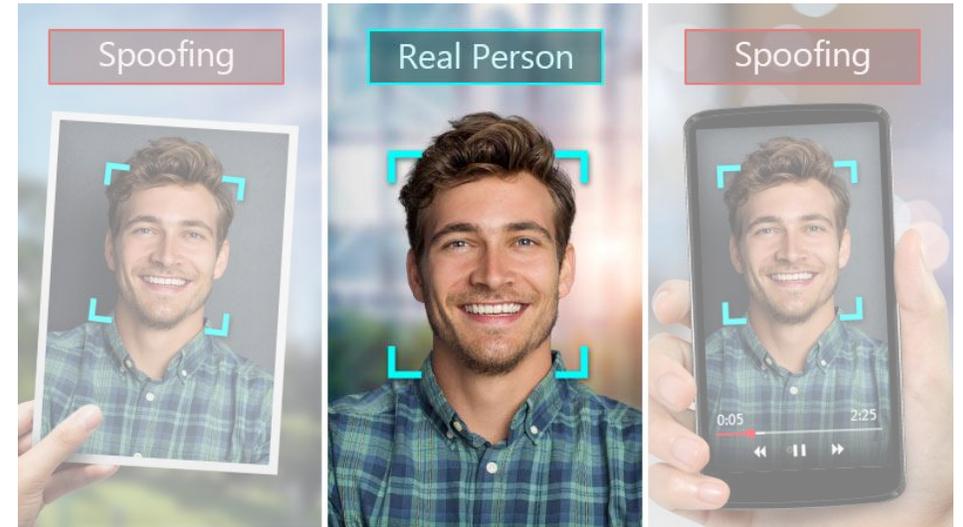
OK

マイナンバーカードの  
ICチップから読み取った写真



### なりすまし防止

カメラ撮影した写真の なりすまし を判別



NG

OK

NG

# 1. 会社概要

# 2. 顔認証Saffe(セーフ) 技術紹介

Appendix1 : 導入事例

Appendix2 : 成長戦略

Appendix3 : 顔認証の可能性(なぜ、顔認証なのか?)

Appendix4 : 顔認証技術、世界の利用状況

Appendix5 : マイナンバーカード関連、弊社の取り組み紹介

Appendix6 : 他認証方式との比較表(物理認証や他生体認証との比較)

# 他認証方式との比較表 - 物理認証との比較（参考情報）

比較軸	顔認証Saffe	ICカード認証	QRコード認証
認証精度	高い（99.46%）	高い（100%）	高い（100%）
偽装発生のリスク	AI技術 なりすまし を防止	カード複製や共用でなりすまし可能	QRコードの共有でなりすまし可能
接触性	非接触、遠距離可能（5mほど）	接触が必要	非接触、近距離のみ
ユーザー体験	顔をかざすだけ	カードの携帯と挿入・接触が必要	スマホの操作、紙への印刷が必要
設置要件	一般的なスマホやカメラで十分	専用カードリーダーが必要	スマホや専用カメラが必要
実装コスト（初期）	20万円～	100万円～300万円	200万円～500万円
実装コスト（月額）	2万円～	5万円～	5万円～
認証速度	高速（1秒未満）	高速（1秒未満）	中速（1～3秒）
環境条件の影響	光量や顔の向きに影響	影響なし	カメラ性能や光条件に影響
バージョンアップ	ソフトウェア更新	ハードウェア更新	ハードウェア・ソフトウェア更新
耐用年数	5～10年	3～5年	5～10年
利用範囲	広範囲（スマホ、監視カメラ、入退室管理）	入退室管理、決済	簡易認証、決済
技術成熟度	高い（AI進化で改善が期待される）	非常に高い（広く普及）	高橋（導入が容易）

# 他認証方式との比較表 - 他生体認証との比較（参考情報）

比較軸	顔認証Saffe	指紋認証	静脈認証	虹彩認証
認証精度	99.46%	97~99%	99%以上	99%以上
偽装発生のリスク	低い(AI技術 なりすまし を防止)	精巧な偽装に脆弱	非常に低い	非常に低い
認証距離	0.3m ~ 5m	0m	0.01m	0.01m
接触性	非接触(衛生的)	接触が必要(衛生面で課題)	非接触(衛生的)	非接触(衛生的)
ユーザー体験	顔をかざすだけ	指をセンサーに接触	手をセンサーに近づける	目をセンサーに近づける
設置要件	一般的なスマホやカメラで十分	特殊な装置が必要	特殊な装置が必要	特殊な装置が必要
実装コスト(初期)	20万円 ~	30~200万円	200~500万円	300~1,000万円
実装コスト(月額)	2万円 ~	1~5万円	20~50万円	30~70万円
メンテナンス	カメラのレンズ清掃	センサー清掃	内部清掃、点検必要	校正が必要
バージョンアップ	ソフトウェア更新	ハードウェア更新	ハードウェア更新	ハードウェア更新
耐用年数	5~10年	5~8年	8~15年	8~15年



**Melon**  
**Technologies**