# 生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術に係る研究開発
# 研究開発とSociety 5.0との橋渡しプログラム
# (BRIDGE)

## 研究開発等計画書

## （令和５年度様式）

## 令和５年１０月

## 警察庁

〇実施する重点課題に〇を記載（複数選択可）

| 業務プロセス転換・政策転換に向けた取組 | 次期SIP/FSより抽出された取組 | SIP成果の社会実装に向けた取組 | スタートアップの事業創出に向けた取組 | 若手人材の育成に向けた取組 | 研究者や研究活動が不足解消の取組 | 国際標準戦略の促進に向けた取組 |
|---|---|---|---|---|---|---|
| | | | | | ○ | ー |

〇関連するSIP課題に〇を記載（主となるもの）

| 持続可能なフードチェーン | ヘルスケア | 包括的コミュニティ | 学び方・働き方 | 海洋安全保障 | スマートエネルギー | サーキュラーエコノミー | 防災ネットワーク | インフラマネジメント | モビリティプラットフォーム | 人協調型ロボティクス | バーチャルエコノミー | 先進的量子技術基盤 | マテリアルの事業化・育成エコ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

# 資料１「生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術」の概要の全体像（位置づけ）

出典：統合イノベーション戦略2023

## 先端科学技術の戦略的な推進

**国民の安全と安心を確保する**
**持続可能で強靱な社会への変革**

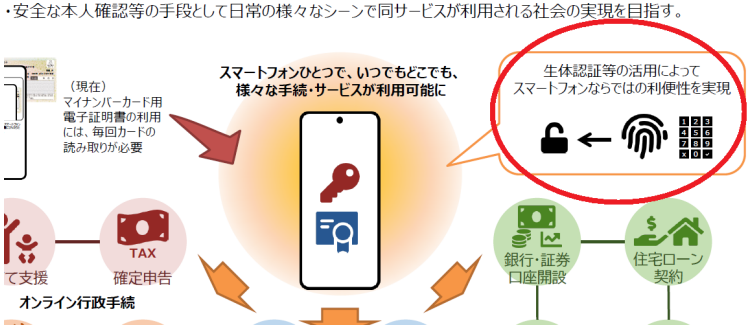
◆ **サイバー空間とフィジカル空間の融合による**
**新たな価値の創出**

- デジタル庁を中心としたデジタル社会の実現に向けた重点計画に基づくベース・レジストリの整備とトラストの確保
- 半導体・デジタル産業戦略の改定と取組の加速、オール光ネットワークやBeyond 5Gの研究開発と国際標準化の推進

### 「マイナンバーカード機能のスマートフォン搭載」によって目指す姿 1

個人認証サービスの電子証明書の機能をスマートフォンに搭載することによって、スマートフォンひとつで、いつでもどこでもオンライン行政手続等を行うことができる環境の構築を目指す。

スマートフォン搭載による利便性の向上等を通じて公的個人認証サービスのユースケースの拡大を促進し、・安全な本人確認等の手段として日常の様々なシーンで同サービスが利用される社会の実現を目指す。




- **デジタル社会の形成**は、Society5.0の実現のための根幹。その**トラストの確保**は、統合イノベーション戦略2023等において、**データ流通の基盤**と位置づけ。
- また、**スマートフォンにおける生体認証**は、マイナンバーカード機能のスマートフォン搭載において、スマートフォンならではの利便性を実現するために重要な機能。
- **令和５年**、英国の消費者団体が、「英国市場で流通する端末装置について、静止画写真で**スマートフォンの顔認証機能**を突破可能。」と発表。
- 警察大学校において、**再現実験**を試みたところ、１機種のスマートフォンにおいて顔認証の**ロック解除に成功**したことから、緊急に調査研究を要望。

ＳＩＰ／ＰＤの提案・意見

# 資料２　「生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術」の概要

【背景・現状・課題】

**１　スマートフォンの生体認証をめぐる情勢と評価・検証の重要性**

今日、スマートフォン等モバイル機器が、生活のあらゆる局面に浸透し、個人に関する重要な情報の多くを記録することとなった。その紛失・盗難等への対策のため、いわゆるロック機能を用いたアクセス制御が標準となり、特に利便性の観点から指紋、顔画像等による生体認証が普及している。

しかし、生体認証機能の安全性を利用者が客観的に把握することは難しい。このため、ひとたび特異な事例に基づく脅威が喧伝された場合、事後関係者がその風評を払拭するためには、大きな努力を要する。

例えば、近年、高精細な写真画像から意図せず流出した指紋情報を用い、指紋を偽造してロックを解除した研究事例が報道され、反響を呼んだ。こうした能動的な脅威については、従前、用いられてきた「誤受入率（false accept rate）」等の指標では、安全性を適切に測ることが困難であるため、Android 互換性要件中の「生体認証センサー」において、新たに「なりすまし受入率（imposter accept rate）」が定義され、各端末装置製造事業者は、Googleが定める詳細な手順に従って自ら測定し、自己評価した結果を報告するよう求められるなど、新たな評価・検証の必要が生じている。更には、生成AIによるなりすましの脅威も、現実のものとなりつつある。学術的には、既にオンライン本人確認（eKYC）においてDeepfakeによるなりすまし成功が報告[川名et al.2021]されているが、画像生成AIの進展を踏まえれば、生体認証一般に対する脅威として捉えるべきであり、対抗技術開発の検討が必要である。

**２　スマートフォンの生体認証評価・検証に係る我が国の技術・民間ビジネス水準**

従前から、システム・情報科学技術分野において、生体認証技術は我が国の強みとされてきた。特に、安全性の評価については、平成26～28年度の経済産業省事業を通じ、安全性確認のためのコモンクライテリア認証のためのプロテクションプロファイルを開発し、認証機関（独立行政法人情報処理推進機構）とともに国内の評価機関が発足、実際に生体認証装置を認証するなどしている。

他方、スマートフォンのロック機能に限った場合、生体認証に係る評価・検証が多いとは言えない。実際に、自己評価であるAndroid互換性要件に対し、スマートフォンを用いたアクセス制御に関する国際的な第三者評価である「FIDO認証」には、FIDOバイオメトリクス部品認定があり、指紋、顔貌、虹彩、音声（声紋）といった利用する各生体情報について、偽造受入率（imposter attack presentation accept rate）を専門的に評価するラボテストが必須であるが、我が国国内にラボテスト機関は存在しない。

**３　我が国におけるスマートフォンのアクセス制御状況の技術的実態把握の必要性**

このように、技術的透明性が低いまま生体認証がスマートフォン等において普及したことを背景に、海外では消費者団体等信頼できる機関から、製品の耐偽造能力検証結果に基づく科学的助言が公表され、利用者の安全と製品に対する正当な信頼性の確保が図られている。他方、我が国において、この種の個別具体的なスマートフォンの生体認証機能について、信頼できる機関による評価等の試みは乏しい。スマートフォンのロック機能に関する安全性について、市場における見える化が不十分なままでは、利用者の選好を促すことに繋がらず、サイバーセキュリティの確保において障害となりうる。

# 資料２　「生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術」の概要

【施策内容】

**１　調査**

次に掲げる事項を調査する。

(1)　偽造指紋、顔影像等スマートフォンのロック機能解除に際し現実的に想定される脅威

(2)　当該脅威に対応し、我が国国内の市場等を通じて既に入手可能な生体認証評価技術

**２　実現可能な手法の検討及び提案**

１の調査結果に基づき、科学的に信頼できる耐偽造能力評価手法を提案する。ただし、追加の技術開発が必要な場合、その実現可能性を検討する。

**３　提案手法の実証と実態把握**

実際に、市場に投入される指紋、顔画像等生体認証技術を利用するモバイル機器等製品について、２の手法を適用し、耐偽造能力の実態を把握する。

【研究開発等の目標】

- 現実的な脅威となる偽造手法の特定と科学的に信頼できる耐偽造能力評価手法の開発
- 市場にあるスマートフォン等モバイル機器における生体認証機能の耐偽造能力の実態把握

【社会実装の目標】

- 商工会議所、学術機関、地方公共団体、関係省庁等と連携し、警察が利用者向けの防犯指導や製造事業者等への個別情報提供等を通じて促すことにより、科学的に正しい知識に裏打ちされた生体認証技術を利用するスマートフォン等モバイル機器が社会に普及し、高度情報通信社会の健全な発展に寄与する。
- アクセス制御機能に関する技術的な脆弱性の解消にとどまらず、国民に対して現実に想定される脅威に関する意識の醸成を促すことにより、高度情報通信社会の健全な発展に寄与する。

【対象施策の出口戦略】

- 商工会議所、学術機関、地方公共団体等と連携し、警察のサイバー防犯指導・助言において、実態把握等結果を活用し、スマートフォン等のアクセス制御に関する知識の普及・啓発に努める。
- スマートフォン等モバイル機器製造事業者等に対し、関係者の利害を損なわないよう配慮しつつ、検証結果について個別に情報提供する。
- 研究結果を基に関係省庁と連携し、生体認証を用いたアクセス制御機能利用製品のセキュリティ向上に向けた取組を推進する。

# 資料３　「対象施策名」のＢＲＩＤＧＥの評価基準への適合性

## ○統合イノベーション戦略や各種戦略等との整合性

デジタル社会の形成は、Society5.0の実現のための根幹をなす。特に、インターネット上で本人であることなどを証明し、送信元のなりすましや改ざん等を防止するための仕組みである「トラスト」の確保は、統合イノベーション戦略2023（令和５年６月９日閣議決定）及びデジタル社会の実現に向けた重点計画（同日閣議決定）において、データ流通の基盤として位置づけられている。

また、スマートフォンにおける生体認証は、「マイナンバーカード機能のスマートフォン搭載」において、スマートフォンならではの利便性を実現するために重要な機能として位置づけられており、そのトラストの確保は、我が国デジタル社会において不可欠と考えられる。

## ○重点課題要件との整合性

重点課題のうち、「６　国際的な研究開発動向や社会ニーズの観点から、研究活動が不足している課題」に該当する。

具体的には、概要に記載のとおり、我が国の強みとされる生体認証技術について、特にその評価・検証技術が既にあるにも関わらず、FIDOバイオメトリクス部品認定における偽造受入率の第三者評価のためには、外国のテストラボに依頼せざるを得ない実態がある。

また、我が国国内市場に流通するスマートフォンの生体認証機能の安全性に関する実態について、利用者等の目線から信頼でき、かつ網羅的に把握できる報告は存在していない。

## ○ＳＩＰ型マネジメント体制の構築

警察大学校サイバーセキュリティ対策研究・研修センター所長がＰＤとなり、研究開発計画の策定・変更、予算配分等の権限を集中する。

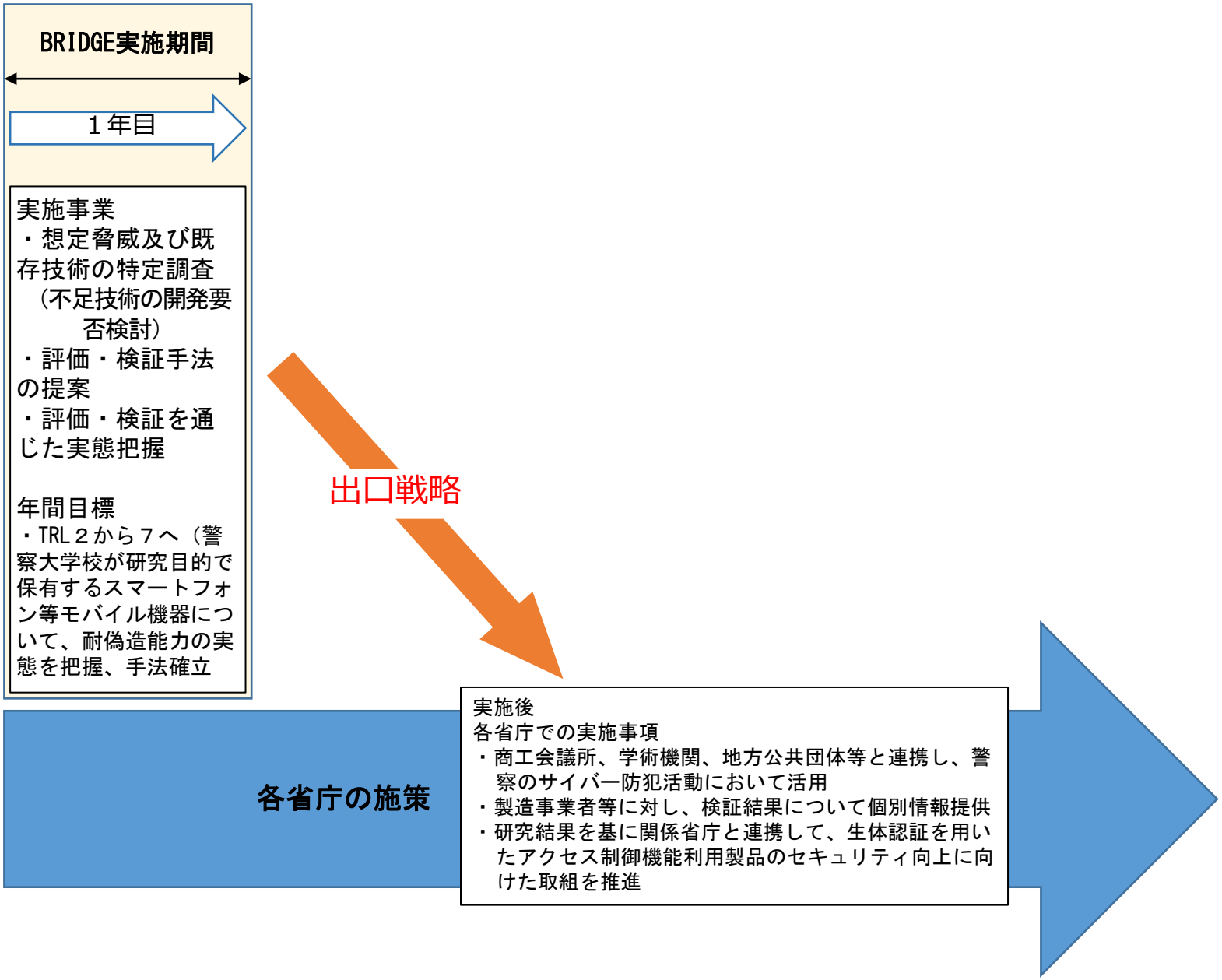
## ○民間研究開発投資誘発効果、財政支出の効率化

学術有識者、民間事業者等との事前検討を通じ、民間の立場において市販製品の試験・検査を伴う研究が困難な理由として、対象製品の入手が挙げられた。そこで、犯罪の取締りのための情報技術の解析及びサイバー事案の防止対策を目的とした研究用として警察大学校において取得・保有する物品を官給（貸与）することで、研究活動の不足について解消を図るとともに、財政支出の効率化に努める。

## ○想定するユーザー

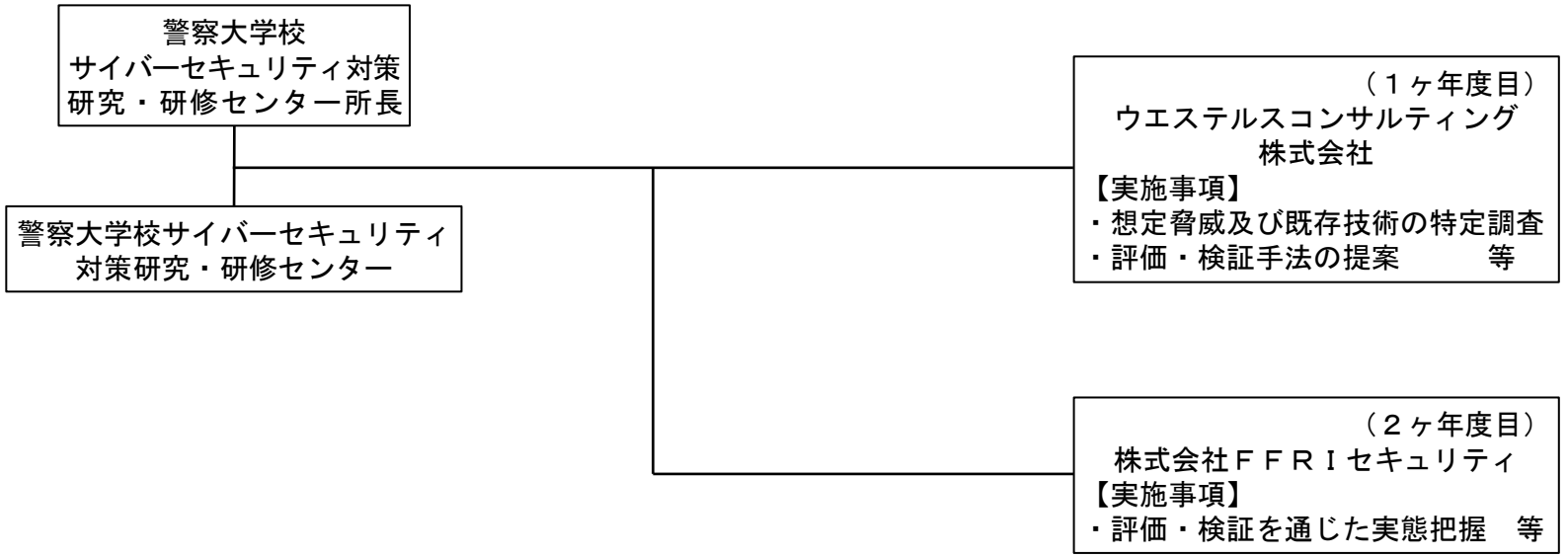
都道府県警察及び警察庁において、主に国民一人一人に向けた情報セキュリティ意識の向上その他サイバー防犯意識啓発活動等に際し、実態把握結果を適切に利用する。

# 資料４　イノベーション化に向けた工程表



# 資料５　実施体制

## 実施体制



# 資料6　「生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術」の目標及び達成状況（1年目）

○施策全体の目標　・・・・現に市場に流通するスマートフォン等の生体認証機能を用いたアクセス制御について、耐偽造性の観点から警察が実態を把握。

| テーマ等 | 当年度目標 | 目標の達成状況（年度末報告） |
|---|---|---|
| ①　想定脅威及び既存技術の特定調査 | 現在、Android互換性要件中の「生体認証センサー」、ISO/IEC30107、その他各種学術論文等において、偽造生体情報によるなりすまし手法が公開されている（開始時の作業仮説としてTRL2と評価）ことから、特にスマートフォン等モバイル機器において普及している指紋及び顔画像について、生体情報の偽造手法を網羅的に調査する。 | （ー） |
| ②　評価・検証手法の（開発又は）提案 | ①の調査により判明した生体認証一般に対する偽造生体情報の脅威について、警察と連携して現実的と考えられる脅威を特定した上、必要に応じ、オープンソースのディープフェイクによる偽顔影像の作成等新たな手法を開発しつつ、実機検証に用いる手法を提案する。 | （ー） |
| ③　評価・検証を通じた実態把握 | 警察大学校において研究用として取得・保有するスマートフォン等モバイル機器の中から、適当なものを選別し、②で提案・開発した手法を適用して手法自体を検証するとともに、スマートフォン等モバイル機器の生体認証機能における耐偽造性能の現状について、実態把握を試みる（TRL7へ。計画期間終了後に追加的な評価・検証が必要となったときに実施可能な態勢が官民に整うことを目標とするため）。 | （ー） |

# 生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術に係る研究開発【概要】

問題意識：　スマホの認証方法として、指紋認証や顔認証といった生体認証が普及しているが、偽造した画像を使うなどすることにより、これらの認証方法を突破することが可能ではないか？

目　　的：　現実的に実行可能と思われる攻撃手法により、スマホの生体認証を突破できるか否かについて検証を行い、その結果に基づき、安全な利用方法について検討・普及を行う。

研究開発事項：　各種の攻撃手法に対するスマホの生体認証の耐性を効果的・効率的に検証するための手法（検証手順等）を開発する。また、警察大学校で保有するスマホを対象とした検証を行うことで当該手法の有効性を確認するとともに、実際に防犯指導を行う上で必要となる知見を得る。

最終成果物のイメージ：

| 認証 | 攻撃手法 | 機種A | 機種B | 機種C | 機種D | 検証結果に対する考察 |
|---|---|---|---|---|---|---|
| 指紋認証 | 攻撃1 | ○ | ○ | ○ | ○ | 指紋認証は、攻撃2や攻撃3の手法により突破されることがあり得る。「情報窃取やなりすましを防ぐために、指紋認証を利用する利用者は○○に留意する必要がある。」と公表する。機種B、Dについては、製造事業者に伝達する。 |
| | 攻撃2 | ○ | × | ○ | ○ | |
| | 攻撃3 | ○ | ○ | ○ | × | |
| 顔認証 | 攻撃1 | ○ | ○ | ○ | ○ | 顔認証は、攻撃2や攻撃3の手法により突破されることがあり得る。「情報窃取やなりすましを防ぐために、顔認証を利用する利用者は○○に留意する必要がある。」と公表する。機種Cについては、製造事業者に伝達する。 |
| | 攻撃2 | ○ | ○ | × | ○ | |
| | 攻撃3 | ○ | ○ | × | ○ | |