

第1回FinTechフォーラム(2016年8月23日)

# 生体認証システムのセキュリティ評価と 国際標準化 ～FinTechにおける活用を展望して～

日本銀行金融研究所 情報技術研究センター  
宇根 正志

---

・本発表の内容は発表者個人に属し、日本銀行の公式見解を示すものではありません。

# 情報技術研究センター(CITECS)について

- 金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポートするために、2005年4月に設立。
  - － 主に、①国際標準化の推進、②金融業界内の情報共有体制の整備、③新しい情報セキュリティ技術の研究開発といった役割を担う。

- 最近の主な研究テーマ

- FIDOの活用と安全性上の留意点
- 生体認証システムのセキュリティ
- スマートフォンを用いた取引認証

—— 研究成果は、金融研究所ディスカッション・ペーパーとして公表するほか、情報セキュリティ・シンポジウムにおいても発表。

(URL: <http://www.imes.boj.or.jp/citecs/>)

第17回情報セキュリティ・シンポジウム  
(2016年3月2日開催)



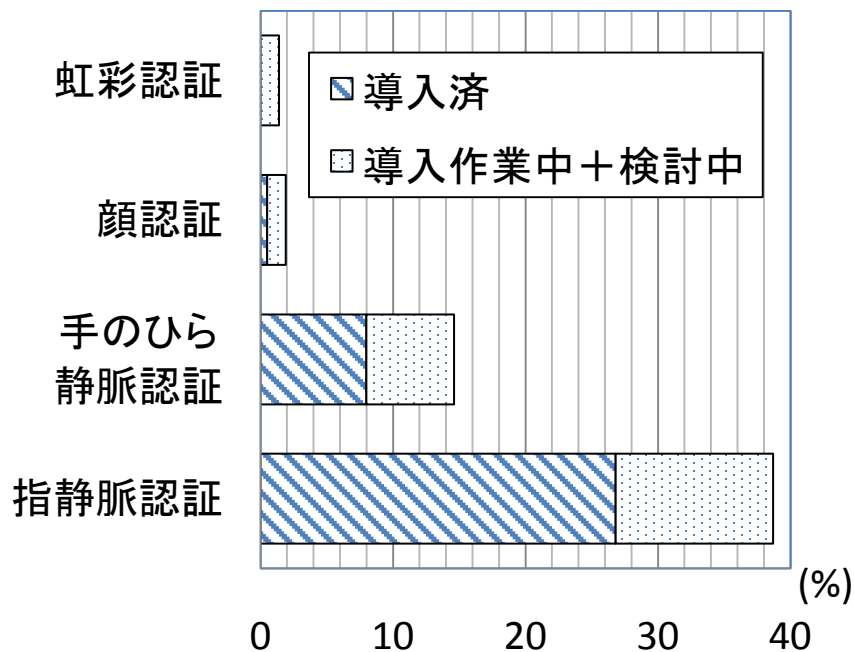
# アジェンダ

1. 金融サービスにおける生体認証の利用
2. 生体認証システムのセキュリティ
  - 人工物を提示して「なりすまし」を試みる攻撃への耐性をどう評価するかが課題
3. セキュリティ評価・認証の実現に向けた検討と国際標準化
  - わが国の産官連携プロジェクト
  - 国際標準化活動
4. FinTechにおける生体認証の活用に向けた課題と留意点

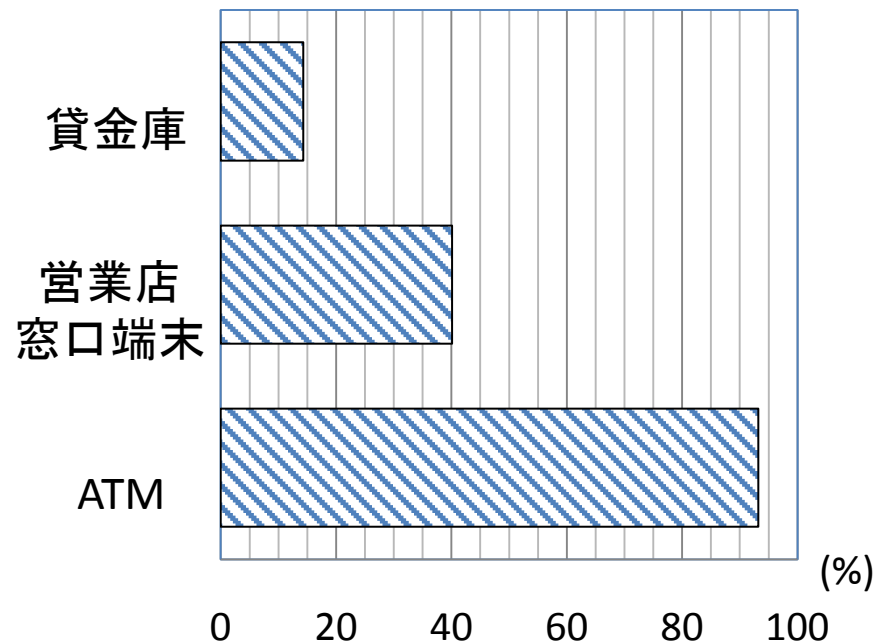
# 金融サービスにおける生体認証の利用(1)

## • わが国の金融機関における利用状況

(イ) 各認証方式を導入している金融機関等の割合



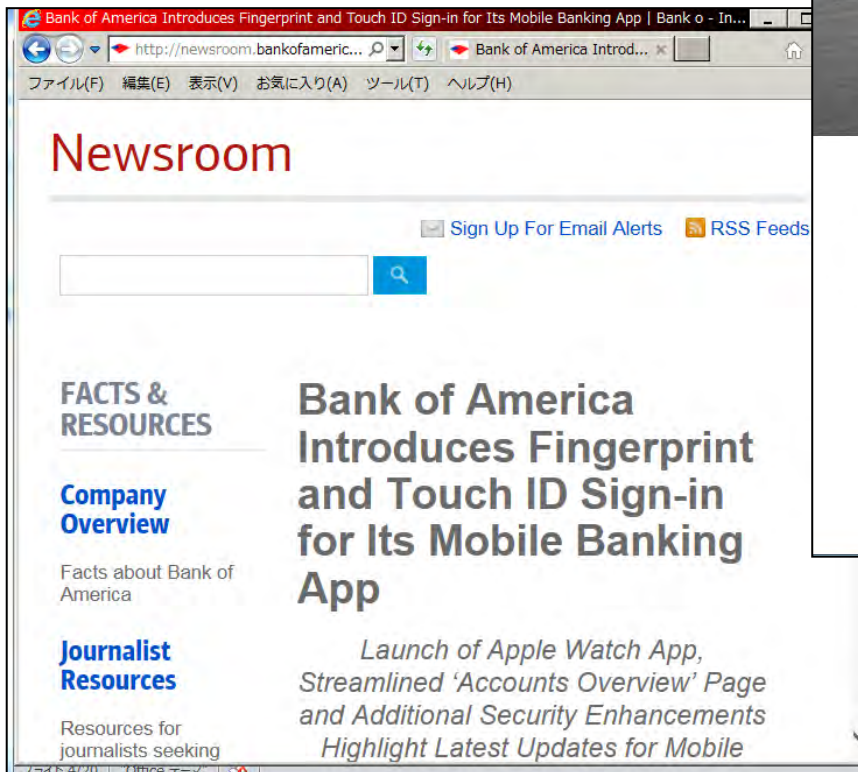
(ロ) 生体認証を導入している金融機関における導入対象



(\*) 出典: 金融情報システムセンター「平成27年度金融機関アンケート調査結果」を基に作成。

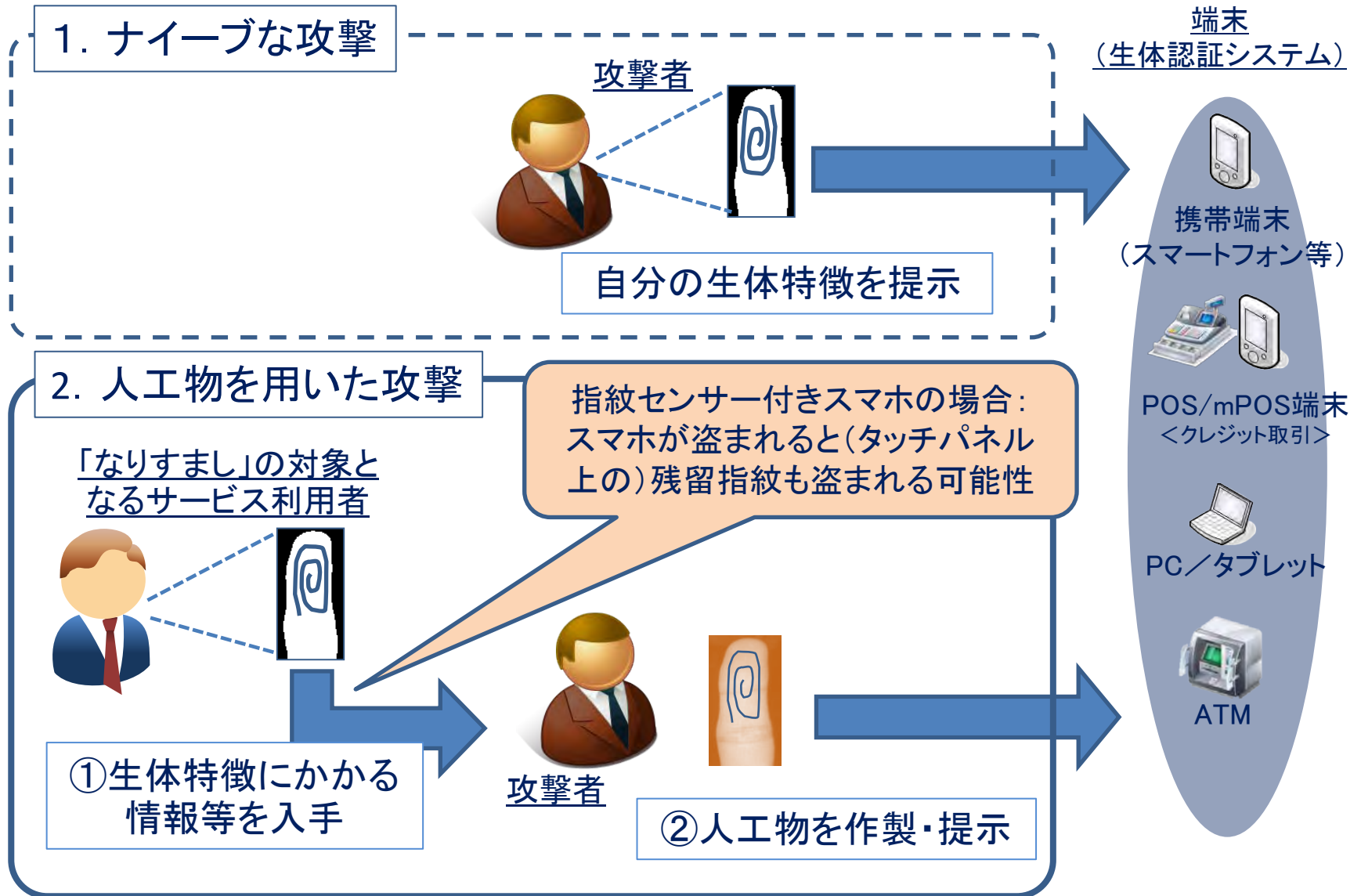
# 金融サービスにおける生体認証の利用(2)

- 海外におけるインターネット・バンキングでの利用
  - － スマートフォン搭載の指紋センサーによる認証を利用。
    - バンク・オブ・アメリカ(2015年9月)
    - KEBハナ銀行(2016年2月)



(出典)・<http://newsroom.bankofamerica.com/press-releases/consumer-banking/bank-america-introduces-fingerprint-and-touch-id-sign-its-mobile-ban>  
・<http://www.hanafn.com/eng/pr/news/newsDetail.do?page=2&seq=3250>

# 生体認証システムのセキュリティ ～「なりすまし」を試みる攻撃への対策が必須～



# 人工物を用いた攻撃 (1)

- ある種の人工物を提示すると、それを身体の一部として誤って受け入れる場合があることが、複数の市販製品・システムでの実験において示されている。

## <主な研究事例>

- 指紋を用いたシステム
  - 指紋と類似の形状の人工物を作製。
  - 素材:グミ、シリコーンなど。
- 虹彩を用いたシステム
  - 虹彩を撮影し、その画像を紙に印刷。
- 静脈のパターンを用いたシステム
  - 静脈のパターンを撮影し、その画像を紙等に印刷。



さまざま人工物  
出典: ルミダイム社ウェブサイト  
(<http://www.lumidigm.com/antispoof.html>)

# 人工物を用いた攻撃 (2): 生体特徴を再現する人工物の例

指紋付き人工指  
(材料:ゼラチン等)



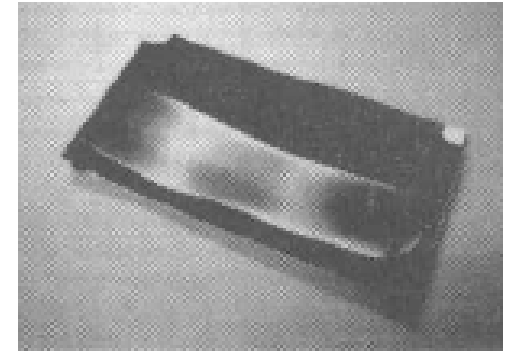
• 出典: 松本勉「生体部分でない対象物の提示による脆弱性評価の方法」  
(<http://www.nmda.or.jp/nmda/bio/pdf/yokohama.pdf>)

人工虹彩(材料:コンタクトレンズ、コピー用紙)



• 出典: von Seelen, U. C., "Countermeasures Against Iris Spoofing with Contact Lenses," Iridian Technologies Inc. ([www.cis.upenn.edu/~cahn/publications/bc05.pdf](http://www.cis.upenn.edu/~cahn/publications/bc05.pdf))

血管パターン付き人工指  
(材料:OHPシート、コピー用紙)



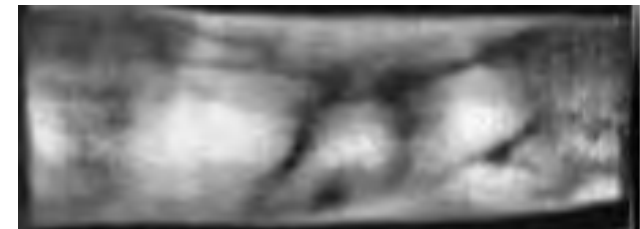
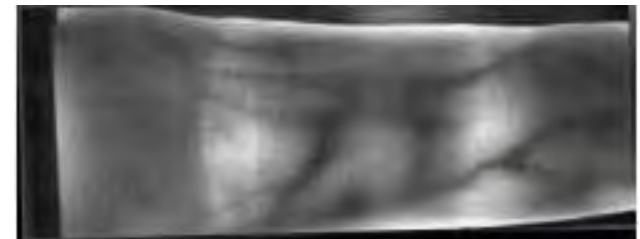
• 出典: 松本勉「生体認証システムのセキュリティ設計とセキュリティ測定」、第7回ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会資料, 電子情報通信学会、2006年



• 出典: Sandström, M., "Liveness Detection in Fingerprint Recognition Systems," Master thesis, Linköpings Universitet (<https://intranet.dcc.ufba.br/pastas/gaudi/biometrica/papers/id/perfilino/exjobb.pdf>)



• 出典: Thalheim, et al., "Body Check: Biometric Access Protection Devices and their Programs Put to the Test" (<http://www.heise.de/ct/english/02/11/114>)



• 出典: Tome, et al., "On the Vulnerability of Finger Vein Recognition to Spoofing" ([http://publications.idiap.ch/downloads/papers/2014/Tome\\_IJEEBIO SIG2014.pdf](http://publications.idiap.ch/downloads/papers/2014/Tome_IJEEBIO SIG2014.pdf))



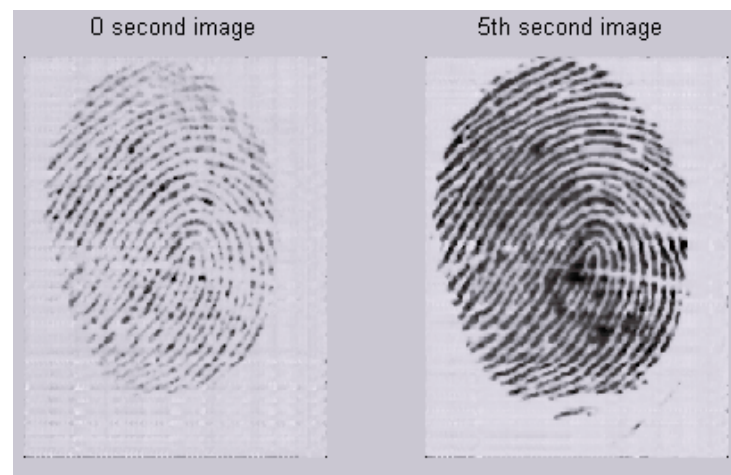
# 人工物を用いた攻撃への対策: 生体(人工物)検知

- センサへの提示物が身体の一部(あるいは、人工物)か否かを検知する技術(liveness detection or artifact detection)の研究が進められている。

## <主な手法の事例>

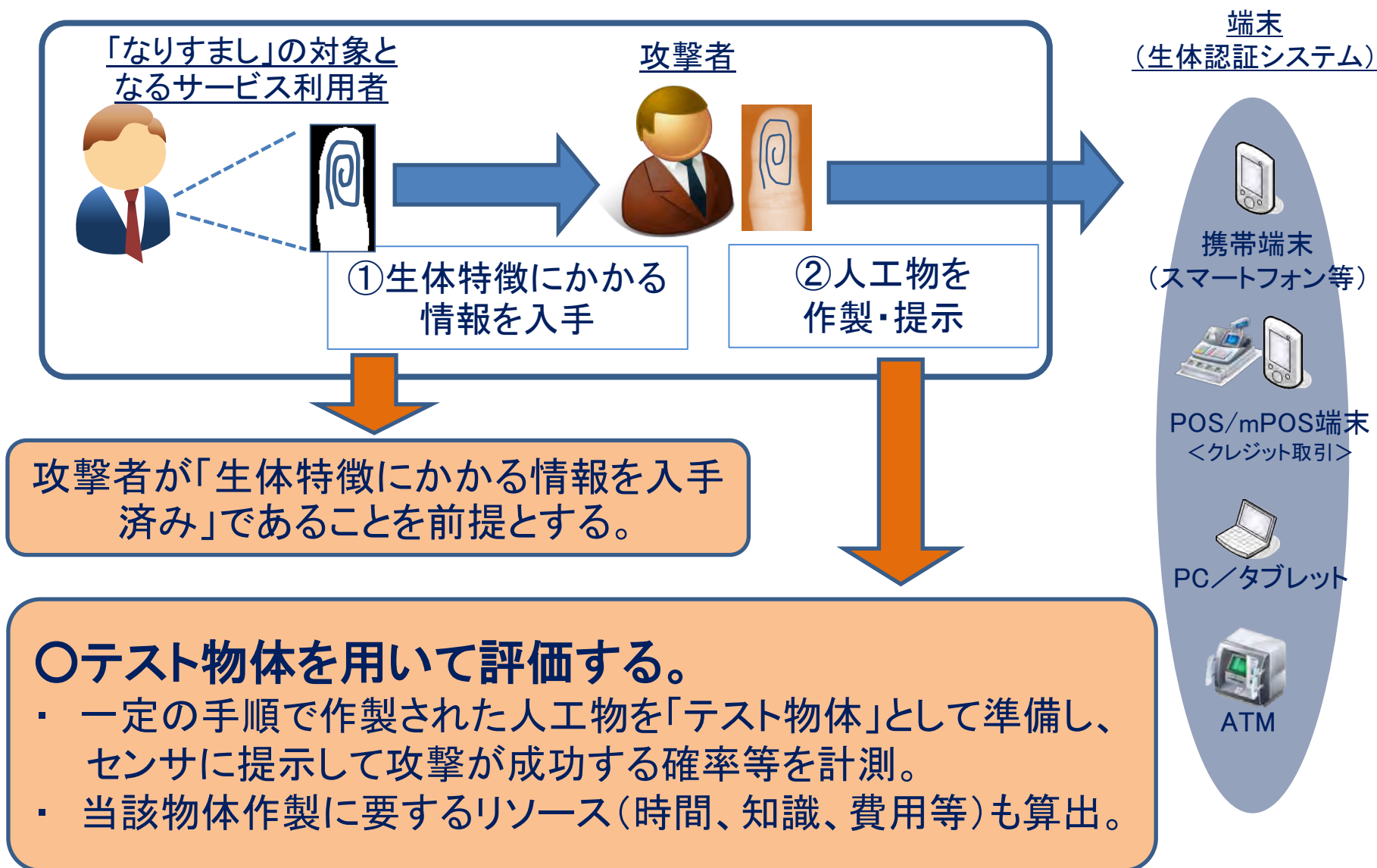
- 指紋を用いたシステム
  - 発汗、形状・色彩の変化、血流(脈波)、温度、反射光等を利用。
- 虹彩を用いたシステム
  - 光量に応じた瞳孔のサイズの変化、眼球の動き等を利用。
  - 虹彩を含む静止画(虹彩のエッジや背景の濃淡パターン)の特徴を利用。
- 静脈のパターンを用いたシステム
  - 血流(脈波)を利用。

## 発汗による指紋画像の変化



・出典: Tan, B. and S. Schuckers, "Liveness Detection Using An Intensity Based Approach in Fingerprint Scanners" (<http://www.clarkson.edu/biosal/pdf/livenessdet.pdf>)

# 人工物を用いた攻撃にかかる評価（現状）



# セキュリティ評価・認証の実現に向けた検討と 国際標準化：わが国の産官連携プロジェクト

- 2014年度より、わが国の産官連携プロジェクト\*において、コモン・クライテリア (ISO/IEC 15408シリーズ) に則った生体認証システムの評価・認証の実現を目指し、
  - ① テスト物体を用いたセキュリティ評価手法の検討
  - ② 同検討結果の国際標準化が推進されている。
- 2015年度、人工物を用いた攻撃を考慮したプロテクション・プロファイルを作成 (IPAの認証を取得)。
  - プロテクション・プロファイル：コモン・クライテリアに則った評価を実施する際に用いられるセキュリティ要求仕様書。
- 2016年度に、静脈のパターンを用いた生体認証システムの評価が試行される見通し。

---

(\*) 戦略的国際標準化加速事業：クラウドセキュリティに資するバイオメトリクス認証のセキュリティ評価基盤整備に必要な国際標準化・普及基盤構築

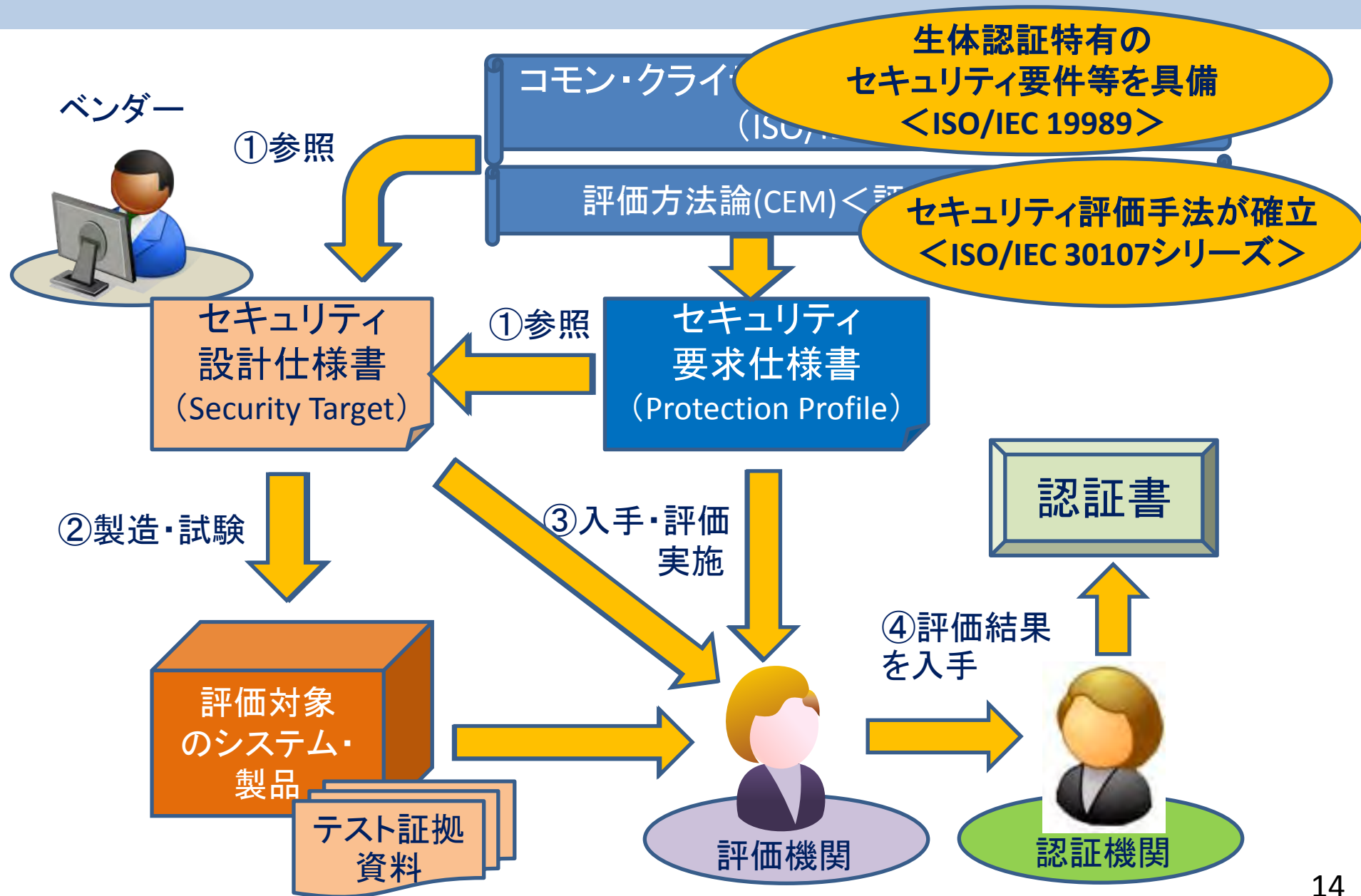
# テスト物体を用いた評価手法の検討

課題	主な検討の概要
テスト物体の バリエーション の充実	<p>(静脈のパターンを用いたシステムを主な対象に)</p> <ul style="list-style-type: none"><li>・人工物を作製(複数の素材の組合せ、高価な素材・機器の使用等を考慮)。<ul style="list-style-type: none"><li>➢ 3Dプリンタ等も活用。</li></ul></li><li>・人工物の作製にかかる費用・時間等を算出。</li></ul>
評価尺度や 評価環境の 標準化	<ul style="list-style-type: none"><li>・攻撃成功確率を定義(APCER*等)。</li><li>・評価のための試験を実施する環境を検討。<ul style="list-style-type: none"><li>➢ 試験結果の再現性確保のために、ロボットを用いた人工物提示を検討。</li><li>➢ 試験実施時の環境(温度、照明等)の設定を検討。</li></ul></li></ul>

# 国際標準化活動

- セキュリティ評価手法にかかる検討等の成果を国際標準とする方向で検討が進められている。
- ISO/IEC 30107シリーズ
  - ISO/IEC JTC1/SC37(バイオメトリクス)において審議中。
  - 人工物を提示する攻撃に対する安全性の評価方法、評価尺度等にかかる事項が規定される見込み。
- ISO/IEC 19989
  - ISO/IEC JTC1/SC27(セキュリティ)において審議中。
  - 人工物の提示を検知・排除するためのセキュリティ要件等が規定される見込み。

# 標準化が進展した後の姿(概念図)



# FinTechにおける生体認証の活用に向けた課題と留意点： 標準化のメリット

- 視点：生体認証システムの調達者、同システムを活用する金融サービスの提供者

これまでの状況	標準化後の状況
標準的な手法での評価が困難	<ul style="list-style-type: none"><li>・国際標準に基づく評価結果を参照できる。<ul style="list-style-type: none"><li>➤ 評価結果の信頼性が向上し、当該サービスに対する顧客の安心感が高まる。</li><li>➤ セキュリティ・ガバナンスが向上。</li></ul></li></ul>
セキュリティの観点からシステム間の比較が困難	<ul style="list-style-type: none"><li>・異なるシステム間で評価結果を比較できる。<ul style="list-style-type: none"><li>➤ 同程度のセキュリティと評価されたシステムを相互に連携させることが展望できる。</li><li>➤ セキュリティ・レベルの差異に応じたリスク対策やサービスの検討も可能。</li></ul></li></ul>

# FinTechにおける生体認証の活用に向けた課題と留意点： 標準化のメリットを享受するために

- 評価・認証済みシステムにかかる情報の収集
  - ✓ セキュリティ設計仕様書 (Security Target)
    - 「システムの用途」「想定する脅威」「運用時の前提条件」「セキュリティ対策方針」等を確認。
    - セキュリティ要件を充足しているかを、APCER等の評価尺度に基づいて確認。
  - ✓ テスト証拠資料
    - 実施されたテストの内容・結果を確認。
- システム導入作業にかかる検討
  - ✓ システム導入時の作業手順の見直し、標準化された評価手法に対応したセキュリティ要件の設定、ベンダーから入手すべき情報の特定等。



# まとめ

- 生体認証システムのセキュリティ評価・認証の枠組み実現が展望できる状況になってきている。
  - 国際標準化にかかる審議が進展。
  - 2016年度には、静脈パターンを用いたシステムの評価が試行される予定。
- 今後、標準化された評価手法等を活用し、FinTech等におけるセキュリティ・ガバナンスや顧客の安心感の向上につなげていくことが有用。
  - 異なる生体認証システムを利用したサービス・端末間で、セキュリティ・レベルの比較が可能に。
- 国際標準化等を「安全なFinTechの実現に資するもの」と捉え、それをどう活用するかを検討していくことが重要。