IMES DISCUSSION PAPER SERIES

生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて

宇根 正志（うね まさし）

Discussion Paper No. 2016-J-2

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2016-J-2
2016 年 2 月

生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて

宇根（うね） 正志（まさし）*

要　　旨

生体認証システムは、身体的な特徴等を利用して個人を認証するシステムである。金融分野では、ATM における取引時の本人確認の手段として静脈のパターンを用いた方式が採用されるなど、同システムの活用が徐々に広がってきている。もっとも、「人工物等が提示された際にそれを身体として誤って受理する」という同システム特有の脆弱性が従来から知られており、これを悪用した攻撃に対するセキュリティを評価するための標準的な手法が確立していないという課題が残されている。

こうしたなか、近年、人工物等を提示する攻撃にかかるセキュリティ評価手法の確立に向けた検討が活発化している。わが国では、静脈のパターンを用いたシステムを対象とするセキュリティ評価・認証が 2016 年度中に試行予定であり、評価・認証を取得したシステムの実現に向けた検討も本格化している。標準的な評価手法等の活用は、生体認証システムにかかるセキュリティ・ガバナンスの向上という観点から有用であり、今後の動向が注目される。

本稿では、生体認証システムのセキュリティ評価手法を巡る最新の動向を、静脈のパターンを用いるシステムに焦点を当てて説明するとともに、今後、生体認証システムを活用していく際の留意点を考察する。

キーワード： 生体認証システム、静脈、人工物、セキュリティ評価、なりすまし、ATM、IC キャッシュカード

JEL classification: L86、L96、Z00

* 日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）

本稿の作成に当たっては、国立研究開発法人産業技術総合研究所特別研究員の大木哲史氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

近年、身体的な特徴を用いて個人を認証するシステム（以下、生体認証システムという）が幅広い分野で利用されるようになってきている。わが国の金融分野における生体認証システムの代表的な用途は、ATM における IC キャッシュカードによる取引での本人確認である。これは、キャッシュカードの偽造対策の 1 つとして、指や手のひらの静脈のパターンを用いる方式が採用され、2000 年代央以降徐々に普及してきている[1]。

こうした生体認証システムでは、「第三者が本人に気づかれずになりすましを試みる」タイプの攻撃を十分な精度で検知・排除することが求められる。ATM における生体認証システムについて言えば、一般に、ATM が設置されるエリアが金融機関等によって厳重に監視されており、攻撃者が、ATM や同装置に内蔵された生体認証システムのセンサー等を金融機関等に気づかれずに改変することは困難である。したがって、まずは、生体認証システムの改変等ではなく、攻撃者が自分の生体特徴を提示するというナイーブな攻撃が想定される。こうした攻撃に対するセキュリティ評価手法については、他人受入率（FAR：false accept rate）等の指標とそれらの測定方法が国際標準化されており（ISO/IEC［2006］）、同指標等を参照してセキュリティ・レベルを確認することができる。次に、より高度な攻撃として、「他人の身体的な特徴等（以下、生体特徴という）にかかる情報を何らかの手段で入手したうえで、人工物等を用いて生体特徴を偽造しセンサーに提示する」というタイプの攻撃（以下、人工物提示攻撃と呼ぶ）が想定される。実際に、人工物が複数の市販の生体認証システムにおいて有意な確率で受け入れられることを示す研究結果が、2000 年代前半以降複数報告されており（宇根・松本［2005］）、こうした攻撃を前提とした評価手法の研究開発が重要な課題として認識されてきた。

そうしたなか、人工物提示攻撃に対するセキュリティ評価手法の確立に向けた研究開発等が最近活発になってきている。例えば、静脈のパターンを用いる方式に関しては、従来わが国の研究者による報告が中心であったが、2015 年 5 月に開催された、生体認証分野の主要な国際学会 ICB 2015（International Conference on Biometrics 2015）において、指の静脈のパターンを用いる 4 つの方式（英・伊・スイス・ノルウェーの研究者からそれぞれ提案されたもの）を対象に、人工物提示攻撃に対するセキュリティを横並びで評価するコンペティションが開催された（Tome *et al.*［2015］）。同コンペティションでは、指の静脈

[1] 金融庁［2015a］によれば、2015 年 3 月末時点において、生体認証機能付きの IC キャッシュカードの発行枚数は全体の 16.4%（2007 年 3 月末時点では 0.6%）となったほか、生体認証対応の ATM の台数は全体の 51.8%（同時点では 15.1%）となった。

のパターンを人工物（材質は紙）によって提示するというタイプの攻撃を前提に、提示された偽の静脈のパターンの検知率等が各方式において測定・発表された。こうした横並びでの評価の研究に加えて、指の静脈のパターンを画像データとして収集しデータベースとして研究目的で活用する試みが進められているほか、同データベースの画像データから人工物を作製し、人工物提示攻撃に対するセキュリティ評価を実施するという内容の研究の報告も行われるようになってきている。

こうした研究に基づき、セキュリティ評価の枠組み整備にかかる検討が進められている。国際標準化に関しては、センサーに何らかの情報を提示してなりすましを試みる攻撃（「入力データ攻撃（presentation attack）」と呼ばれる）にかかるセキュリティ評価手法の国際標準案（ISO/IEC 30107 シリーズ）が、国際標準化機構（ISO：International Organization for Standardization）傘下の標準化団体において審議されている（大木・大塚・寶木［2013］、新崎［2015］）ほか、同攻撃にかかるセキュリティ評価を、情報システム一般を対象とするセキュリティ評価・認証の国際的な枠組みである「コモン・クライテリア（Common Criteria）」において実施するための国際標準案（ISO/IEC 19989）が審議されている（山田［2015］）。また、わが国では、上記の国際標準案の審議に資する検討が2014年度から産官連携によって開始されており、2016年度には、静脈のパターンを用いた生体認証システムを対象とするセキュリティの第三者評価・認証が試行される予定となっている（日本自動認識システム協会ほか［2015］）。

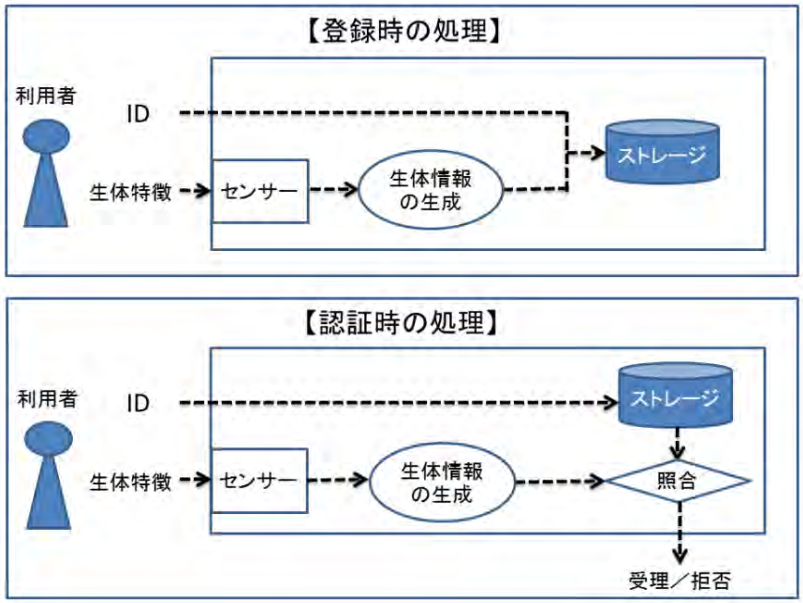
上記の各種検討が進展すれば、現在使用されている生体認証システムのセキュリティを標準的な手法に基づいて評価することが可能となるほか、新たに生体認証システムを導入する、あるいは、既存システムの保守期限到来等を契機としてシステムを更改する際に、人工物等によるなりすましの攻撃に対して客観的な評価を得た生体認証システムを調達できるようになる。その結果、生体認証システムにかかるセキュリティ・ガバナンスの向上につながると考えられるほか、当該システムを活用する金融サービスのセキュリティを顧客にアピールすることもできるようになる。こうした点を踏まえ、生体認証システムの評価・認証に向けた今後の動向を注視しておくことが有用である。

本稿の構成は以下のとおりである。２節では、生体認証システムの構成、人工物提示攻撃、同攻撃に対するセキュリティ評価の考え方を整理する。３節では、静脈のパターンを用いた方式に焦点を当てて、最近の研究や国際標準化の動向、第三者による評価・認証の検討状況を説明する。４節では、今後、金融分野において生体認証システムを活用していく際の留意点を考察する。

２．人工物提示攻撃とセキュリティ評価

(1) 生体認証システムの基本的な構成

生体認証システムでは、センサーに提示された生体特徴等からデジタル化した情報（以下、生体情報という）を生成し認証に用いる。例えば、生体特徴として静脈のパターンを用いる場合、当該パターンの画像データ等から生体情報が生成される。生体認証システムの利用を開始する際には、利用者は自分の生体情報をシステムに登録する（図表 1 参照）。



図表 1. 生体認証システムにおける基本的な処理（概念図）

一般に、利用者が生体特徴をセンサーに提示すると、システムにおいて生体情報が生成され、利用者固有の ID 等の情報とともにストレージに登録される[2]。認証時には、利用者は、ID 等を提示するとともに生体特徴をセンサーに提示する。その際、システムにおいて、「当該認証時に生成された生体情報」と「ID 等に対応づけられて登録されている生体情報」との照合等が実施され、「生体情報の類似度が一定値以上となる」などの判定基準[3]を満たした場合に「受理（認証成功）」の旨が出力される。

---

[2] 現行の ATM での生体認証システムでは、登録された生体情報や ID が IC キャッシュカード内に格納される形態となっており、図表 1 中の「ストレージ」の部分に対応する機能等を IC キャッシュカードが有している。

[3] 人間の身体でなく人工物がセンサーに提示された場合、提示対象が身体の一部か否か（生体か否か）を判定する仕組み（生体検知と呼ばれる）を備えたシステムもあるが、そうしたシステムにおいては生体検知にかかる判定が生体情報の類似度の判定に加えて実施される。

(2) 人工物提示攻撃

本稿では、「攻撃者が、なりすまし対象の利用者の生体特徴にかかる情報を何らかの手段で入手したうえで、人工物等を用いて生体特徴を偽造しセンサーに提示する」という攻撃を「人工物提示攻撃」と呼び、検討の対象とする。本攻撃は、なりすまし対象の利用者の生体特徴にかかる情報の入手、および、生体認証システムにおいて誤って受理される人工物等の作製・提示という 2 つの行為から構成される（田村・宇根［2007］）。例えば、ATM における生体認証システムを攻撃対象とした場合、以下の攻撃が想定される（鈴木・宇根［2009］）。

・攻撃者は、IC キャッシュカードの利用者から、同カードおよび暗証番号を盗取する。また、攻撃者は、当該利用者の生体特徴に関する情報を入手し、それを用いて人工物を作製する。そのうえで、攻撃者は、当該利用者になりすまして ATM に向かい、同カードを ATM のカードリーダに挿入するとともに、暗証番号の入力や当該人工物の（センサーへの）提示を行い、当該利用者の預金の不正引出を試みる[4]。

生体特徴にかかる情報の入手方法については、鈴木・宇根［2009］が、生体認証システムのセキュリティに関する国際標準 ISO/IEC 19792（ISO/IEC［2009］）等に基づき整理している。これらのうち、既存の技術等によって回避可能なもの、および、ATM のように、生体認証システムが常時管理されている場合には対策の必要性が低いものを除くと、以下の 4 つが残る（補論 1 を参照）。

【生体特徴にかかる情報の入手の手段】

- 攻撃対象となる生体認証システムのセンサーに残留する生体特徴の痕跡（残留指紋等）を入手する。
- 日常生活で生じる生体特徴の痕跡（グラスの残留指紋等）を入手する。
- 体表に露出している生体特徴を観察して情報を入手する。
- 同一の生体特徴等を利用している他の生体認証システムから情報を入手する。

---

[4] こうした攻撃の成否は、生体特徴にかかる情報の入手や人工物等の作製・提示の可否に加えて、IC キャッシュカードや暗証番号の入手の可否に依存する。これは、IC キャッシュカードや暗証番号の管理にかかる問題であり、生体認証システムのセキュリティとは異なる観点の評価となるが、近年、キャッシュカードの盗難による預金の不正な払戻しが多発している現状*を踏まえると、IC キャッシュカードおよび暗証番号が盗取されるという状況を「発生しうるもの」と位置づけ、生体特徴の入手および人工物の作製・提示の可否を評価する必要がある。

(*) 金融庁［2015b］によれば、2014 年度中に発生したキャッシュカードの盗難による預金等の不正払戻しの件数は、主要行等・地方銀行・第二地方銀行・信金等の合計で 2,848 件（被害金額：12 億 37 百万円）となっている。

上記の方法等によって生体特徴にかかる情報を入手した後、攻撃者は人工物等の作製・提示を行う。その際に想定される攻撃のシナリオとして、静脈のパターンを用いる方式の場合、以下が考えられる。

【人工物等の作製・提示のシナリオ＜静脈のパターンを用いる方式の場合＞】

A) 大根、エポキシ樹脂・人工雪材、紙等、各種人工物の作製にかかる公開情報（例えば、松本ほか［2006］、松本・森下・李［2006］、森田ほか［2014］、Tome, Vanoni and Marcel［2014］）を収集・参照しつつ、攻撃に利用できるリソースや期待される不正利得等を勘案し、作製する人工物を決定して試作する。

B) 静脈のパターンを用いた生体認証システムを入手する、または、既に公開されている方式等を参照しつつ、同様のシステムを作製する。

C) 上記 B のシステムにおいて、試作した人工物を用いて登録・認証処理を繰り返し実施し、「人工物から提示した情報が受理される確率」（攻撃が成功する確率）を測定する。

D) 例えば、「人工物から提示した情報が受理される確率が 95%以上となる」などの一定の基準を設定し、同基準を満足する人工物の作製に成功するまで、作製方法を改良しつつ、上記 B、C を繰り返す。

E) 上記 D の基準を満足する人工物の作製に成功した場合、攻撃者は、攻撃対象のシステムに当該人工物を提示して不正な取引を試みる。

(3) セキュリティ評価の考え方

イ．攻撃に必要なリソースと攻撃成功確率

セキュリティ評価の目標は、概して言えば、「情報セキュリティ技術を実装したシステムにおいて、想定される攻撃に必要なリソース（費用、情報量、時間等）と同攻撃が成功する確率（以下、攻撃成功確率という）との関係を示すこと」と表現できる。こうした関係を明確にすることができれば、それに基づき、「当該技術の採用・導入が、当該攻撃を実施しようとする攻撃者の誘因を喪失させる効果を有しているか否か」を判断することが可能となる。

例えば、サービス提供者は、上記の関係を用いることによって、特定の情報セキュリティ技術の有効性を以下の流れで検討することが考えられる[5]。

[5] 実際に情報セキュリティ技術の導入を検討するにあたっては、当該アプリケーションの重要性、技術導入に伴う費用、導入にかかる時間、システム投資にかかる他案件との優先順位等を総合的に評価したうえで判断されることとなると考えられる。

(ア)当該システムにおいて攻撃が成功した場合に、攻撃者が入手しうる不正利得の上限を試算する。
(イ)上記(ア)で試算した不正利得の上限に、セキュリティ評価の結果として得た「攻撃成功確率」を乗じ、「攻撃実行時に攻撃者が入手しうる不正利得の上限」を試算する。
(ウ)上記(イ)で得た「攻撃者が入手しうる不正利得の上限」と、攻撃に必要なリソース（金額ベースに換算したもの）を比較する。
(エ)当該リソースが「攻撃者が入手しうる不正利得の上限」を上回る場合、攻撃者は、攻撃実行に費やしたリソースを回収することができないと考えられることから、想定される攻撃に対して当該技術は有効と判断することができる。

攻撃に必要なリソースと攻撃成功確率の関係の検討は、人工物提示攻撃の文脈では、「生体特徴にかかる情報の入手」および「人工物等の作製・提示」において、実行に必要なリソースと攻撃成功確率の関係をそれぞれ明らかにすることに対応する。こうした検討のアプローチとして「テスト物体アプローチ」（松本［2006］）が広く知られている。

ロ．テスト物体アプローチ

テスト物体アプローチは、一定の手順によって作製された人工物を「テスト物体」として準備したうえで、評価対象の生体認証システムのセンサーにテスト物体を提示し、それが登録・認証の処理に成功する確率を計測する、というものである。同アプローチにおける評価では、テスト物体を実際に作製し、その際に必要となった費用・スキル・時間等を「攻撃に必要なリソース」として記録するほか、当該テスト物体による登録・認証の処理の成功確率等を記録する。これまでに、指紋、光彩、手のひらや指の静脈のパターン等を用いた市販の生体認証システムの製品を対象に、本アプローチを適用した評価結果が数多く公表されている（例えば、Matsumoto *et al.*［2002］、松本・田中［2007］等）。

テスト物体アプローチの評価結果を活用して生体認証システムの有効性を判断していく場合、以下の 2 つの課題が存在する。

第 1 の課題は、「テスト物体」として使用する人工物の絞込み・選択である。これまでに、さまざまなタイプの人工物やその作製方法が提案され、それらに基づいたセキュリティ評価の研究成果が数多く報告されている。生体認証システムを評価する段階で、それらのすべての人工物を用いてテストを行うとした場合、多くの時間と費用が必要となる。そうした点を考慮すると、既存の多数の人工物の中から、代表的な「テスト物体」を絞り込んでおくことが望ましい。

例えば、比較的少ないリソースで作製可能な人工物から、高度な攻撃を想定した精巧な人工物（作製に多くのリソースが必要なもの）まで、「テスト物体」のバリエーションが考えられるなかで、攻撃に必要なリソースの多寡に対応して少数の代表的な「テスト物体」のセット（最低限必要なものに絞込みしたもの）を準備・標準化しておくことが考えられる（松本・田中［2007］）。

第 2 の課題は、複数の生体認証システムの評価結果を比較可能とするために、テスト物体による評価用の環境や評価尺度を標準化することである。評価用の環境としては、具体的には、評価用の生体特徴のサンプル（あるいは画像等のデータセット）、センサーへのテスト物体の提示方法、評価を行う場所の温度・湿度・光度等が挙げられる。また、時間の経過等に伴ってテスト物体が劣化するという問題も考慮して評価のテストを実施する必要があり[6]、そうした点を加味した評価方法の標準化も課題である。その他の登録・認証処理に影響を与えうる要素を抽出したうえで標準化するとともに、攻撃成功確率としての評価尺度を標準化することも必要である（Busch［2014］）。

このように、人工物提示攻撃にかかるセキュリティ評価手法として、テスト物体アプローチにかかる研究が進められており、同アプローチを今後各種の生体認証システムに適用していくうえで、テスト物体のセットや評価用環境等の標準化が主要な課題となる。次節では、静脈のパターンを用いた方式に焦点を当ててテスト物体アプローチによる最近の評価研究の動向を整理し、同アプローチの課題に関する検討の状況を分析する。

6 例えば、指紋を用いたシステムにおいて、グミによって作成されたテスト物体をセンサーに提示してテストを行う場合、時間の経過とともにテスト物体の表面が乾燥するほか、同一のテスト物体を何度もセンサーに提示するうちに表面の形状が変化することとなる。こうした問題への対応として、同一の生体特徴から同じ素材のテスト物体を複数準備しておき、それらをテストに使用することが考えられる。その場合、異なるテスト物体を使用することに伴う評価結果（攻撃成功確率等）の揺らぎも評価することが求められる。

３．生体認証システムのセキュリティ評価にかかる最近の研究・標準化動向

(1) 静脈のパターンを用いた方式にかかる研究の動向

静脈のパターンを用いた方式を対象とするセキュリティ評価の研究は近年広がりをみせており、いずれもテスト物体アプローチによるものである[7]。従来、こうした研究報告はわが国の研究機関によるものが多数を占めていたが、最近では、スイスの Idiap 研究所をはじめ、欧州の研究機関による研究報告が多くなっている[8]。研究内容は、「被験者から静脈のパターンの画像等を収集してデータベース化したうえで、紙等の比較的入手しやすい素材を用いて人工物を作製し、それらによって提示された情報が誤って受け入れられる確率等を測定する」ものが中心である（各研究報告の概要は補論 2 を参照）。

前節で示したテスト物体アプローチの課題に着目しつつ、最近の主な研究の特徴・傾向と研究課題を整理すると、以下の図表 2 のとおりである。

図表 2. 静脈のパターンを用いた方式での最近の主な研究の特徴と課題

主な研究の特徴・傾向	研究課題
イ.「攻撃者が生体特徴にかかる情報を入手した状態（攻撃者に有利な状況）」を想定し、「人工物等の作成・提示」に焦点を当てて評価した研究が大半。	イ.「生体特徴にかかる情報の入手」に必要なリソースや攻撃成功確率等に関する評価について検討することが求められる。
ロ. 簡便な手法で作製された人工物をテスト物体として用いた評価研究が多く、作製に多くのリソース等を必要とする人工物による評価研究が少ない。 例えば、静脈のパターンの画像等を市販のプリンターで紙に印刷してテスト物体とするものが挙げられる。	ロ. 評価に用いられる人工物が簡便な手法で作製されるものに偏り、テスト物体としてのバリエーションに乏しい。より多くのリソースを要するテスト物体にかかる検討が求められる。
ハ. 複数の評価尺度が使用されており、統一されていない。評価用環境についても研究報告によって区々。	ハ. 評価尺度（攻撃成功確率：一致と誤って判定する確率）や評価用環境の標準化が求められる。

[7] 人工物提示攻撃にかかるセキュリティ評価でなく、性能評価（人間の生体特徴による照合・判定の正確さを評価するもの）に関しては、テスト物体を用いた評価にかかる研究成果が米国や中国の研究者からも報告されている。

[8] 欧州における研究の活発化には、欧州委員会による生体認証システムの評価プロジェクト BEAT（Biometrics Evaluation and Testing）の開始（2012 年）が背景として挙げられる。BEAT は、生体認証システムの評価のためのオープンなプラットフォームの提供、セキュリティ評価手法の確立、コモン・クライテリアに則った評価・認証のためのドキュメントの整備等を目的としており、Idiap 研究所等の欧州の研究機関が参画している。

イ．生体特徴にかかる情報の入手に関する評価の必要性

最近の主な研究報告では、攻撃を構成する行為のうち、「人工物等の作製・提示」の評価に焦点を当てた研究が多く、「生体特徴にかかる情報の入手」の評価を対象としたものが少ない。従来から、静脈のパターンを用いた方式については、「静脈が体内に存在し、日常生活において静脈のパターンが外部に残留する場面を想定困難であることから、指で触れたグラス等にパターンが残留する指紋や、外部から容易に撮影できる顔画像等に比べて、生体特徴にかかる情報を本人の協力なしに入手しづらいという意味で、相対的に安全性が高い」といわれている。しかし、筆者が知る限り、静脈のパターンにかかる情報の入手困難性についての評価結果がこれまで報告されておらず、同評価は静脈のパターンを用いた方式にとって重要な課題といえる。

ロ．より多くのリソースを要するテスト物体の検討の必要性

第 2 に、最近の研究報告の多くが、紙や OHP シート等を用いて比較的簡便な手法で作製された人工物を「テスト物体」として利用しており、作製により多くのリソースを要する人工物を用いた研究が少ない。その結果、テスト物体となる人工物のバリエーションが限定され、より多くのリソースを投入する攻撃者を想定した評価が困難になっている。さまざまな攻撃者を想定した評価の実施、および、「テスト物体」のバリエーションの増加という観点から、より多くのリソースを要する人工物の作製等にかかる検討が必要である[9]。

ハ．評価尺度等の標準化の必要性

第 3 に、人工物を用いた評価尺度（攻撃成功確率）が統一されていないという課題が挙げられる。研究報告をみると、評価尺度として、例えば「人工物等によって提示された情報を『登録された生体情報と一致』と誤って判定する確率」、あるいは、「人工物等が提示された際に『人間の身体の一部が提示された』と誤って判定する確率」が使用されるなど、研究報告によって区々であり、評価結果の比較が困難となっている。また、評価実施時の環境も区々となっている。今後、こうした評価尺度等の標準化が課題である[10]。

---

[9] 例えば、日本自動認識システム協会ほか［2015］においては、3D プリンター、電子ペーパー、液晶等の装置や技術を活用した検討が考えられると指摘している。

[10] 評価用環境の整備の観点では、指や手のひらの静脈のパターンの画像等の研究用データベースが Idiap 研究所によって提供されるようになっている。この結果、各研究者が独自に静脈のパターンの画像等を収集する必要がなくなり、研究実施のハードルが低下したほか、生体認証システムのうち、生体情報の生成や照合・判定にかかるアルゴリズム部分の評価を同一環境で実施可能となった。なお、生体特徴にかかるデータベースは、指や手のひらの静脈のパターンだけでなく、指紋、顔画像、虹彩についても整備・提供されている（Li *et al.*［2014］）。

(2) わが国の産官連携プロジェクトにおける検討の動向

イ．概要

わが国では、上述の研究課題等を含むセキュリティ評価手法に関する検討が、「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・推進基盤構築」のなかで進められている（日本自動認識システム協会ほか［2015］）。この産官連携プロジェクトは、日本自動認識システム協会・産業技術総合研究所・OKI ソフトウェアが主体となって 2014 年度から 3 年間の計画で実施中であり、生体認証システム特有の脆弱性や脅威（人工物提示攻撃も含まれる）を考慮したセキュリティ評価手法の確立や、生体認証システムの第三者によるセキュリティ評価・認証の実現等を目指している。

ロ．セキュリティ評価手法の検討

セキュリティ評価手法の検討は、静脈のパターンを用いた生体認証システムや装置を主たる対象としている。本プロジェクトの 2014 年度成果報告書（日本自動認識システム協会ほか［2015］）を参照し、セキュリティ評価手法に関する検討の流れや図表 2 の研究課題にかかる検討項目を整理すると、以下の図表 3 のとおりである。

図表 3. セキュリティ評価手法にかかる産官連携プロジェクトでの検討の流れ

<table>
<tr><th>検討の流れ</th><th>図表 2 の研究課題にかかる検討項目</th></tr>
<tr><td>(A)人工物作製等に関して公開されている情報を収集する。</td><td rowspan="2">○「より多くのリソースを要するテスト物体の検討」にかかる検討項目
・静脈のパターンの画像等を収集する機器の作製
・複数の素材を組み合わせた人工物の作製
・高価な素材や機器による人工物の作製
✓ 人工物作製の方法として、静脈のパターンの 2 次元画像を 3 次元画像に変換するツールや 3D プリンターの活用等を検討。
・人工物作製の費用・時間等の算出</td></tr>
<tr><td>(B)攻撃方法や人工物の作製方法を検討し、評価試験用の人工物を作製する。</td></tr>
<tr><td>(C)人工物を評価対象のシステムに提示し、登録・認証に成功する確率等を測定する。</td><td rowspan="2">○「評価尺度等の標準化」にかかる検討項目
・攻撃成功確率の検討（APCER 等を厳密に定義）
・試験を行う環境（評価用環境）にかかる検討
✓ 評価結果の再現性確保のために、ロボットを用いて人工物を提示する試験を実施。
✓ 試験実施時の環境（温度、照明等）の設定について、評価を実施しつつ検討。</td></tr>
<tr><td>(D)評価手法の妥当性等を検討し、最終的に評価手法を決定する。</td></tr>
</table>

（備考）日本自動認識システム協会ほか［2015］を参照して作成。

研究課題のうち、「より多くのリソースを要するテスト物体の検討」および「評価尺度等の標準化」については、それぞれの課題に対する具体的な検討項目が準備され、検討が進められている。一方、「生体特徴にかかる情報の入手の評価」については、「攻撃者が攻撃対象の個人の静脈のパターンにかかる情報を取得済み」という（攻撃者に有利な）状況を前提としており、今後の課題として位置づけられている[11]。

セキュリティ評価の主眼である「攻撃に必要なリソースと攻撃成功確率との関係の明確化」という観点では、「攻撃成功確率」の検討が行われているほか、「攻撃に必要なリソース」については、コモン・クライテリアに則った評価の際に用いられる「攻撃ポテンシャル（attack potential）」として検討されている。攻撃ポテンシャルは、想定する攻撃の実行の難易度を示す概念であり、攻撃を実行するために必要となる、「時間」「専門技術」「知識」「機会（の多寡）」「機材」の5項目をそれぞれ評価してスコア化し、それらの合計値として示される[12]。上記の各項目は攻撃に必要なリソースをそれぞれ異なる観点から捉えたものであり、「攻撃ポテンシャル（スコアの合計値）が大きいほど、攻撃に必要なリソースが大きい」という関係となる。同リソースの多寡を検討する場合、攻撃ポテンシャルをどのように算出するかが課題となるが、本プロジェクトでは、既存の研究報告で示されている人工物作成・提示の方法を対象に、上記の 5 つの観点から分析して攻撃ポテンシャルを試算するなど（同検討の概要については補論 3 を参照）、標準的な同試算方法の確立を目指している。

攻撃ポテンシャルの試算方法が確立すれば、試算の過程で明確となる攻撃の特性に基づいて、金額ベースで換算した「攻撃に必要なリソース」を導出し、同リソースと攻撃成功確率との関係を明確にすることが可能になると考えられる。実際に同リソースを検討する際には、ベンダーと連携し、コモン・クライテリアに則ったセキュリティ評価・認証の際に用いられた「テスト物体」の情報を参照しつつ、当該テスト物体による攻撃にかかる費用（リソース）を上記の 5 つの観点から試算することになると考えられる。

詳細は後述するが、こうした検討の成果を、人工物提示攻撃を考慮したセキュ

---

11 本取扱いに関して、2014 年度の成果報告書では、「静脈のパターンを用いた認証方式は、攻撃対象者の静脈のパターンを得るのが難しいことが他の認証方式に優る重要な特徴の 1 つ」としたうえで、「『攻撃者が攻撃対象の個人の静脈のパターンにかかる情報を取得済み』という前提では同方式の安全性の高さを十分に主張できないことから、今後、攻撃対象者の静脈のパターンの情報を入手することの困難性を考慮した評価方法を検討する必要がある」旨が記載されている。

12 上記の 5 項目の考え方やスコアの算出方法等は、コモン・クライテリアに則ったセキュリティ評価方法論（CEM : Common Evaluation Methodology、CCMB［2012］）に記述されている。セキュリティ評価やテストを実施する際の要件の内容は、攻撃ポテンシャルの値に応じて決定され、その値が大きいほど、セキュリティ評価の項目が増加するほか、それらの内容もより高度なものとなる。

リティ評価手法に関する国際標準案（ISO/IEC 30107 シリーズ）等に反映させる方向で検討されている。

ハ．第三者によるセキュリティ評価・認証の実現に向けた検討

上記の検討によってセキュリティ評価手法が確立すれば、次の論点は、「誰が、どのような体制に基づいて、個々の生体認証システムの評価・認証を実施するか」である。セキュリティ評価の結果が信頼され幅広い分野で活用されるようにするためには、「専門的な評価技術を有する（当該システムのベンダー以外の）中立的な組織が、コンセンサスを得た標準的な手順に沿ってセキュリティ評価を実施する」とともに、「同評価が適切に実施されたことを公的機関が認証する」という体制が望ましい。こうしたニーズは情報システム・製品一般について以前から存在しており、汎用の情報システム・製品にかかる第三者による情報セキュリティ評価・認証の枠組みとして、コモン・クライテリア（Common Criteria）が 1999 年に ISO/IEC 15408 として国際標準化され[13]、2000 年代前半には同国際標準に基づく評価・認証制度が構築された[14]。その後、本枠組みに基づく評価・認証がスマートカードをはじめとして各種の情報システム・製品に適用されており、生体認証システムのセキュリティ評価に関しても本枠組みの活用が合理的な対応と考えられる。

ただし、生体認証システムのセキュリティ評価をコモン・クライテリアにおいて実施するためには、人工物による提示を誤って受け入れるなどの生体認証システム特有の脆弱性を考慮したセキュリティ要件等を、現行のコモン・クライテリアには規定されていないことから新たに定義する必要がある。通常、評価対象のシステムの開発者（ベンダー等）は、評価・認証を受ける際には、当該システムの利用環境、想定される脅威、セキュリティ機能、当該セキュリティ機能を保証するための要件（試験内容にかかる要件を含む）等を記述する「セキュリティ設計仕様書（ST：Security Target）」を作成し、評価対象のシステムや実際に行ったテストにかかる資料等を評価機関に提出する。仮に、生体認証システムを評価対象とした場合、人工物提示攻撃へのセキュリティ要件として、例えば、「人工物による生体特徴の提示（人工物提示攻撃）を検知する」などの要件を（ISO/IEC 15408 シリーズには規定されていないことから）別途独自に定義し、当該要件等を記述したセキュリティ設計仕様書を準備する必要がある。

---

13 コモン・クライテリアにおける第三者評価・認証の手続きについては補論 4 を参照。

14 コモン・クライテリアの枠組みに基づく評価・認証の枠組みは各国で制度化されており、わが国では、「IT セキュリティ評価及び認証制度（JISEC: Japan Information Technology Security Evaluation and Certification Scheme）」との名称で 2001 年に制度化され、2015 年 3 月末までに 467 件の認証実績がある（金子・村田［2015］）。また、わが国の政府機関におけるシステム調達の場面では、JISEC による評価・認証を取得した情報システムの調達が推奨されている。

こうしたことから、2015 年 10 月末時点では、筆者が知る限り、人工物提示攻撃の検知・排除を要件として定義しているセキュリティ設計仕様書や、そうした設計仕様書に基づいて評価・認証を取得したシステムはほとんど知られていない[15]。また、人工物の提示を検知する機能にかかる要件を規定した「セキュリティ要求仕様書[16]（PP：Protection Profile）」として、指紋を用いた方式を前提とした同仕様書がドイツにおいて開発されているものの、同仕様書には、生体認証システムの一部（人工物を検知する機能を有する部分等）を評価対象としており、生体認証システム全体を評価対象としていないという問題がある。

こうした状況に対して、本プロジェクトでは、人工物を検知する機能に加え、生体情報の生成や判定の機能も含めた生体認証システム全体を対象とするとともに、人工物の検知の機能にかかる要件等を新たに盛り込んだセキュリティ要求仕様書（Yamada［2015］）の作成を進めている。これによって、開発者（ベンダー等）は、セキュリティ設計仕様書を作成する際に、同要求仕様書に記載されているセキュリティ要件等を参照することができるようになる。また、わが国の ISO 傘下の標準化団体は、当該要求仕様書の内容を ISO/IEC 15408 シリーズ等に反映させるための国際標準案（ISO/IEC 19989）の審議開始を提案し、現在当該標準案の審議が進められている（山田［2015］）。

上記のセキュリティ要求仕様書を活用し、2016 年度中に、静脈のパターンを用いた生体認証システムの評価・認証をわが国において試行することが予定されており、人工物提示攻撃を考慮した第三者による評価・認証を取得した生体認証システム（静脈のパターンを用いた方式によるもの）の実現に近づきつつあるといえる。

(3) 国際標準化の動向

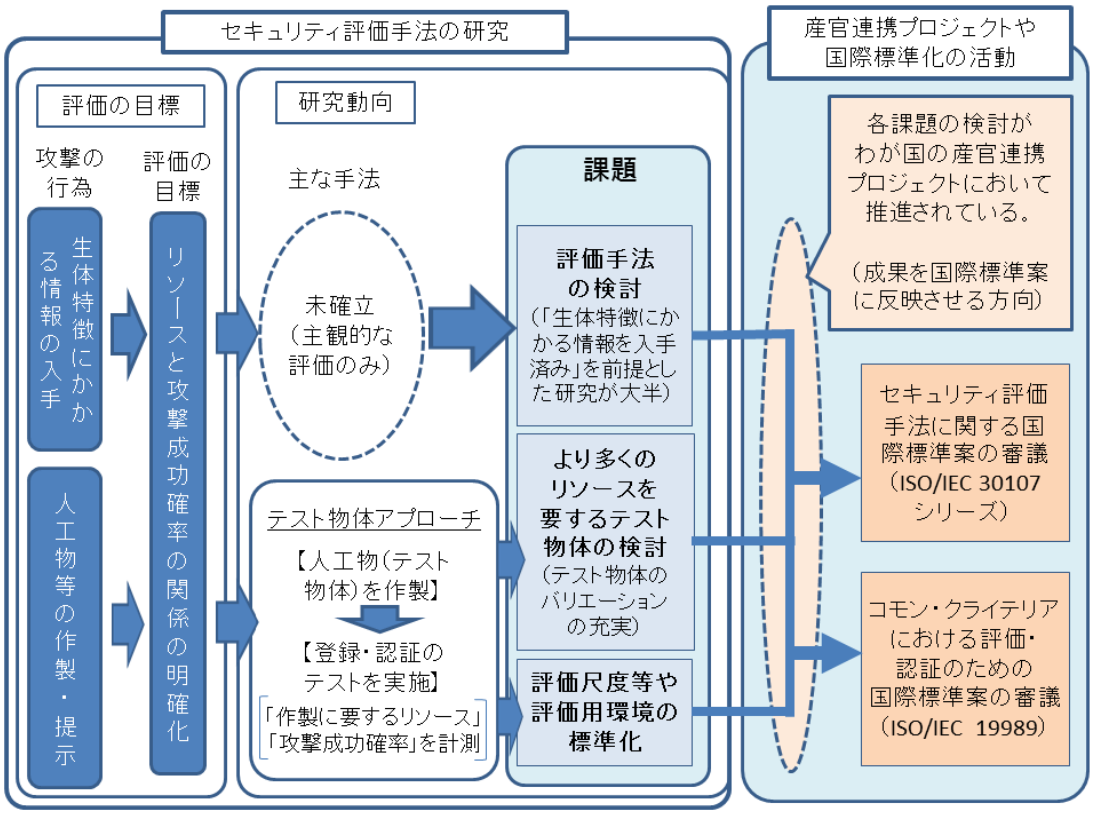
上記(2)の検討と並行して、生体認証システムのセキュリティ評価・認証の実現に向けて国際標準化が進められている。すなわち、人工物提示攻撃等を想定したセキュリティ評価手法を規定する国際標準案（ISO/IEC 30107 シリーズ）、

---

15 コモン・クライテリアのポータルサイト（https://www.commoncriteriaportal.org/）には、第三者による評価・認証を取得した情報システム・製品のリストが掲載されているが、人工物提示攻撃の検知の機能を有する生体認証システムや機器は 2015 年 12 月末時点で 1 件のみとなっている。これは、ドイツで評価・認証を取得した指紋認証機器（Federal Office for Information Security［2013］）であり、同機器のセキュリティ設計仕様書（Morpho［2013］）には、「提示されたものが偽造物か否かを検知可能であること」というセキュリティ機能の要件が独自に定義されている。

16 セキュリティ要求仕様書は、情報システム・製品の利用者（あるいは利用者側の業界団体等）が当該システム・製品に求める機能やセキュリティ要件等を記述するものであり、当該システム・製品の開発者が同要求仕様書を参照して実際のシステム・製品開発を実施できるようにするために準備される。同要求仕様書の基本的なフォーマットや記述すべき事項は ISO/IEC 15408 シリーズに規定されているほか、同要求仕様書に記述するセキュリティ要件等は同国際標準から選択・引用することとなっている。

および、生体認証システムのセキュリティ評価に必要なセキュリティ要件等を規定する国際標準案（ISO/IEC 19989）がそれぞれ審議されている。研究課題から国際標準化活動に至る検討の流れは、図表 4 のとおりである。



図表 4. 生体認証システムの評価・認証の実現に向けた活動の全体像

ISO/IEC 30107 シリーズは、「バイオメトリクス」の国際標準化を担当する ISO/IEC JTC1/SC37 において審議されている。本国際標準案は、入力データ攻撃にかかるセキュリティ評価手法をスコープとしており（Busch［2014］）、本稿において検討対象としている人工物提示攻撃も含まれている。2015 年 10 月 6 日時点では、ISO/IEC 30107 シリーズは、「入力データ攻撃検知（Presentation Attack Detection）」というタイトルのもとで、攻撃とその対策にかかる概念や用語の定義、セキュリティ評価のためのテストの方法、評価尺度、評価結果を示すデータ形式等を規定する方向で審議されている（新崎［2015］）。セキュリティ評価のためのテストの方法に関しては、テスト物体の利用が前提となっているほか、評価の対象に応じて 3 種類のテスト[17]を規定する内容となっている。評価尺度に

[17] 具体的には、(A)人工物等を検知する主たる機能を担う「入力データ攻撃検知サブシステム（presentation attack detection subsystem）」に焦点を当てた評価（どの程度の頻度で人工物を正しく検知できたかなどをテストするもの）、(B)上記(A)の評価に加えて、提示された生体特徴のデー

関しては、本節(2)の産官連携プロジェクトで検討対象となっている APCER（Attack Presentation Classification Error Rate）[18]等を盛り込む方向で検討されている。

ISO/IEC 19989 は、「情報セキュリティ」の国際標準化を担当する ISO/IEC JTC1/SC27 において審議されており、2015 年 10 月 6 日時点では、タイトルが「生体認証システムにおける入力データ攻撃検知のセキュリティ評価（Security Evaluation of Presentation Attack Detection for Biometrics）」となっている（山田［2015］）。同国際標準案の内容に関しては、ISO/IEC 15408 シリーズの規定を補足するために、人工物提示攻撃等を検知・排除する機能に関する要件（セキュリティ機能要件）や、当該機能が適切に実装されていることを確認・保証するための要件（セキュリティ保証要件）を規定するほか、当該攻撃等にかかるセキュリティ評価手法の一部（ISO/IEC 30107 シリーズを引用）についても規定する方向で検討が進められている。

タの品質等をチェックする「生体特徴データ取得サブシステム（data capture subsystem）」も対象とする評価、(C)上記(B)の評価に加えて、生体情報を照合する「照合サブシステム（comparison subsystem）」も対象とする評価、の 3 つが規定されている。評価対象となる生体認証システムによっては、これらのサブシステムが別々に構成され、個々のサブシステムの評価が可能となるケースが想定される。

[18] 産官連携プロジェクトにおいては、一定の攻撃ポテンシャルに属するさまざまな種類のテスト物体のうち、「センサーに提示した際に『（テスト物体でなく通常の）身体の一部の提示』と誤って判定する確率（の平均値）」が最大となるテスト物体を選択し、同テスト物体を提示した際の当該確率を APCER と定義している。すなわち、APCER は、こうした攻撃に対して「最悪の場合の攻撃成功確率」を意味するものとなっている。

４．今後金融分野において生体認証システムを活用するうえでの留意点

(1)　第三者による評価・認証を得た生体認証システムの登場

上記３．において示したように、国際的な研究活動、わが国の産官連携プロジェクト、生体認証システム関連の国際標準化等が積極的に進められており、セキュリティ評価手法の確立、および、生体認証システムのセキュリティにかかる第三者による評価・認証の実現が展望できる情勢となってきている。セキュリティ評価手法等に関する国際標準については、ISO/IEC 30107 シリーズおよび ISO/IEC 19989 の標準化が 2017 年度中に完了する見込みとなっている。第三者による評価・認証を取得した生体認証システムが調達可能となる時期については、現時点では特定困難であるものの、わが国の産官連携プロジェクトにおいて静脈のパターンを用いた生体認証システムの試行的な評価・認証が 2016 年度中に実施予定であることを踏まえると、国内での評価・認証にかかる具体的な検討も同年度中に本格化していくとみられる。

金融分野においては、ATM における本人確認の用途をはじめとして生体認証システムが活用されているものの、標準的なセキュリティ評価手法の確立に向けた取組みが現在進行中であることを踏まえると、生体認証システムのセキュリティを標準的な手法によって評価することがこれまで困難であったと考えられる。足許の産官連携プロジェクトの検討や国際標準化によって今後セキュリティ評価手法が確立すれば、ベンダーの協力のもとで当該手法を既存のシステムに対して適用して評価を実施し、（これまで把握が困難であった）当該システムのセキュリティのレベルを標準的な手法に基づいて把握することが可能になる。これによって、生体認証システムに関して、「コストに見合ったセキュリティ対策となっているか」、あるいは、「セキュリティ・リスクが許容できるレベル以下に制御されているか」といった事項を把握可能になるという意味で、セキュリティ・ガバナンスの向上につながると考えられる。

今後、金融機関が新たな金融サービスを提供していくなかで生体認証システムの利用を検討する場面が想定され、その際に標準的なセキュリティ評価手法を活用することが考えられる。例えば、スマートフォンによるモバイル・バンキングにおける本人確認等の手段として、パスワードの代わりに生体認証システムの利用を検討するケースが想定される[19]。そうした際に、従来であればベン

[19] 例えば、米国では、バンク・オブ・アメリカがモバイル・バンキングにおいて Android 端末や iOS 端末での本人確認の手段として指紋を用いた方式を既に利用している（Bank of America［2015］）。本サービスは、新しいユーザ認証方式として注目を集めている「FIDO（Fast Identity Online）」を活用したものであり、一部のスマートフォンで利用可能となっているほか、マイクロソフト社のウィンドウズ 10 に標準装備される予定となっていることから、今後、他の金融機関においても採用される可能性があるとみられている。

ダーが独自に実施した評価結果を参照する以外に方法がなかったが、国際標準化等が進展すれば、ベンダーの協力を得ながら標準的なセキュリティ評価手法による評価結果を参照することが可能となる。また、採用の候補となる複数の生体認証システム間でセキュリティ・レベルを比較することも可能となる。

また、金融機関は、第三者による評価・認証を取得した生体認証システムの活用を顧客に説明することによって、同システムのアプリケーションのセキュリティにかかる顧客の安心感を高めることができる。これは、「セキュリティ対策に積極的に取り組む」という姿勢を示すことにもつながり、当該金融機関のサービスに対する顧客の信頼向上にもつながると考えられる。

一方、こうした評価・認証を取得したシステムを利用する場合、評価・認証を取得していないシステムに比べて、システム調達にかかるコストが割高になる可能性がある。第三者による評価・認証を取得するためには、生体認証システムの開発者は、セキュリティ設計仕様書の作成、評価機関・認証機関への評価・認証申請にかかる準備等を実施する必要があるほか、評価・申請の費用を負担しなければならない[20]。こうしたコストは、当該システムを調達する際の費用に転嫁される可能性がある。

(2) 生体認証システム導入にかかる検討の手順

金融機関が第三者によるセキュリティ評価・認証を取得した生体認証システムを今後導入していく場面としては、「現時点では利用しておらず、新規に生体認証システムを導入する」という場合と、「既に生体認証システムを利用しており、当該システムの更新の際に導入する」という場合の 2 つが想定される[21]。これらのケースにおいて、人工物提示攻撃への対策の観点から、アプリケーションのセキュリティ要件に合致したシステムを選択する際には、以下の手順で検討することが考えられる。

【検討の流れ】

(ア)（導入の候補となる生体認証システム（第三者による評価・認証を取得したもの）を選択する。

---

[20] 評価機関による評価実施にかかる費用については、評価対象となるシステムの内容、評価にかかる期間等に依存して決定される。また、認証申請にかかる費用については、JISEC における認証機関による認証の場合、申請対象のシステムに応じて 50～100 万円程度の手数料が必要となる（情報処理推進機構［2015b］）。

[21] 金融情報システムセンターによる「平成 27 年度金融機関アンケート調査結果」では、調査対象の金融機関のうち、指の静脈のパターンを用いた方式、手のひらの静脈のパターンを用いた方式に関して「導入済」と回答した先はそれぞれ 26.8%、8.0%となっているほか、「導入に向けて作業中」および「検討中」と回答した先は、それぞれ 12.4%、6.6%となっている（金融情報システムセンター［2015］）。

- ✓ 生体認証システムのベンダーへのヒアリング等を実施し、第三者による評価・認証を取得したシステムの有無のほか、適用する予定のアプリケーションと当該システムの相性等について確認する。

(イ) 同システムのセキュリティ設計仕様書や、セキュリティ評価の際に実施したテストにかかる情報（テスト証拠資料等）を当該ベンダーから入手する。

(ウ)同設計仕様書等を参照しつつ、想定される脅威（攻撃者）、セキュリティ対策の方針・機能、セキュリティ評価の結果等が、導入対象となるアプリケーションのセキュリティ要件と整合的であるかを確認する。

- ✓ 整合的であれば、当該システムを、「人工物提示攻撃にかかるセキュリティの観点から導入の候補として適格」と判断する。

上記(ウ)における整合性確認の際に留意すべきと考えられる主な確認事項を、セキュリティ設計仕様書の構成に基づいて具体的に整理すると、次頁の図表 5 のとおりである。

図表 5 に示した(A)～(J)について確認するなかで、例えば、テスト物体の種類やセンサーへの提示方法等、当該システムへの攻撃の手掛りになってしまう可能性のある情報については、公開されたセキュリティ設計仕様書に記載されない場合がある。そうした情報については、当該ベンダーに確認することが必要となる。

また、図表 5 の確認事項に加えて、「テスト物体を用いた評価が既知の主要な攻撃を反映しているか」、および、「当該テスト物体による攻撃に必要なリソースをどのように試算したか（攻撃ポテンシャルの評価）」についてもベンダーに確認する必要がある。これらの点については、セキュリティ設計仕様書には記載されず、評価機関による評価の際に当該ベンダーから評価機関に対して提出されるテスト証拠資料等に記載されることになるとみられる。したがって、金融機関は、当該ベンダーに対して、上記事項にかかる情報の提供や確認を求めることが必要になると考えられる。

図表 5. セキュリティ設計仕様書の構成と主な確認事項

セキュリティ設計仕様書（ST）の構成		金融機関による主な確認事項
主要項目	主な記載事項	
セキュリティ設計仕様書の概要（Introduction）	・ST の対象のシステム（以下、「システム」と記載）の用途・特徴 ・システムを構成するハード・ソフト等	(A) システムの用途が金融機関のアプリケーションに合致するか。 (B) システムのハード・ソフトと当該アプリケーションとの間の相性に問題ないか。 (C) 当該システム全体が評価対象としてカバーされているか（漏れはないか）。
適合主張（Conformance Claims）	・本 ST が準拠しているコモン・クライテリアの版の説明	(D) 本 ST がコモン・クライテリアの最新の版に準拠して作成されているか。
セキュリティ課題定義（Security Problem Definition）	・想定する脅威、情報資産、エンティティ ・運用時の前提条件（運用環境にかかる物理的条件等） ・セキュリティ対策方針	(E) 記載されている脅威に、当該アプリケーションで想定される脅威（人工物提示攻撃）が含まれているか。 (F) 運用時の前提条件が当該アプリケーションにおける前提と整合的であるか。 (G) セキュリティ対策方針に上記(E)への対策の方針が記載されているか。
セキュリティ対策方針（Security Objectives）	・機能と運用面での具体的なセキュリティ対策方針 ・当該セキュリティ対策方針と脅威・前提条件等の対応関係	(H) 具体的なセキュリティ対策方針として、「センサーへの人工物の提示を一定レベル以上の確率で検知・排除する」「一定回数の認証に失敗した場合にはシステムをロックする」等の記載があるか。
拡張コンポーネント定義・セキュリティ要件・評価対象の仕様の要約（Extended Component Definition, Security Requirements, TOE Summary Specifications）	・セキュリティ機能にかかる要件（セキュリティ機能要件） ・セキュリティ機能の実装の確実性を保証するための要件（セキュリティ保証要件） ・新たに定義した要件 ・上記要件が充足されていることの論拠	(I) 上記(H)のセキュリティ対策方針に対応するセキュリティ機能要件が設定されているか。 (J) 人工物を検知（あるいは排除）する確率が当該アプリケーションの要件（他人受入率等）と合致しているか。 ✓ 記載がない場合は、当該ベンダーに確認する。

（備考）セキュリティ設計仕様書の構成については Morpho［2013］を参考にした。

５．おわりに

2002 年、横浜国立大学の松本勉教授の研究チームにより、「市販の指紋認証システムにおいて、グミで作製した人工物（表面に指紋の形状が形成されたもの）が誤って人間の指として高い頻度で受け入れられた」旨が国際学会において発表された（Matsumoto, *et al.*［2002］）。本発表を契機として、「人工物による疑似生体特徴の提示を誤って受理してしまう」という脆弱性が生体認証システム特有の脆弱性として国際的にも広く認識されるようになり、本脆弱性を悪用した攻撃にかかるセキュリティ評価手法の確立が重要な課題として位置づけられた。その後、標準的な評価手法の確立に至っていないのが実情であるが、学界での研究、わが国の産官連携プロジェクト、国際標準化活動等の進展によって、人工物提示攻撃等にかかるセキュリティ評価手法の確立・標準化、および、生体認証システムの第三者によるセキュリティ評価・認証の枠組みが実現しつつある。

今後、生体認証システムを利用している金融機関にとっては、国際標準化が進められているセキュリティ評価手法に基づき、既存システムのセキュリティ評価を当該ベンダーと連携して実施することが可能となる。また、第三者によるセキュリティ評価・認証を取得したシステムを調達・活用できるようになれば、中立的な機関による評価結果を参照することが可能となる。こうした取組みは、生体認証システムに関するセキュリティ・ガバナンスを一段と向上させることを可能にするほか、顧客に対して、生体認証システムを活用するアプリケーションのセキュリティを一層明確にアピールすることができるというメリットにもつながる。

生体認証システムのセキュリティ評価手法の確立に向けた動きは今後も継続していく。金融機関においては、こうした動向をフォローするとともに、標準的なセキュリティ評価手法等をどのように活用していくかについて検討することが重要であろう。

【参考文献】

宇根正志・松本　勉、「生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に」、『金融研究』、第 24 巻第 2 号、日本銀行金融研究所、2005 年 7 月、35～83 頁

大木哲史・大塚　玲・寶木和夫、「生体認証装置に対するなりすまし攻撃とその安全性評価法について」、『バイオメトリクス研究会資料』、BioX2013-16、2013 年、59～64 頁

金子朋子・村田松寿、『セキュリティ評価基準コモンクライテリアとその認証制度の動向』、コンピュータセキュリティシンポジウム発表資料、2015 年

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」、『金融情報システム』、No.388、金融情報システムセンター、2015 年

金融庁、『偽造キャッシュカード問題等に対する対応状況（平成 27 年 3 月末）』、2015 年 a

――――、『盗難キャッシュカードによる預金等不正払戻し（被害発生状況・補填状況）』、2015 年 b

情報処理推進機構、『ISO/IEC 15408 IT セキュリティ評価及び認証制度』、2015 年 a

――――、『IT セキュリティ認証申請等のための手引き(CCM-02-A)』、2015 年 b

新崎　卓、『SC37 Biometrics 標準化報告 WG3 Biometric Data Interchange Formats』、JAISA バイオ関係標準化セミナー発表資料、2015 年 10 月

鈴木雅貴・宇根正志、「生体認証システムの脆弱性の分析と生体検知技術の研究動向」、『金融研究』、第 28 巻第 3 号、日本銀行金融研究所、2009 年 10 月、69～106 頁

田村裕子・宇根正志、「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、『金融研究』、第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年、53～100 頁

――――・――――、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」、『金融研究』、第 27 巻別冊第 1 号、日本銀行金融研究所、2008 年、79～114 頁

日本自動認識システム協会・産業技術総合研究所・OKI ソフトウェア、『平成 26 年度工業標準化推進事業委託費　戦略的国際標準化加速事業　国際標準共同研究開発・普及基盤構築事業：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　成果報告書』、2015 年

松本　勉、「バイオメトリクスのセキュリティ評価方法の開発に向けて」、『生体

医工学』、Vol. 44、No. 1、2006 年、日本生体医工学会、54-61 頁
————・田中瑛一、「指静脈認証システムのテスト物体によるセキュリティ測定法の研究」、『2007 年暗号と情報セキュリティシンポジウム予稿集』、3F3-4、電子情報通信学会、2007 年
————・————、「透過光利用バイオメトリック認証システムのためのテスト物体作製方法」、『2008 年暗号と情報セキュリティシンポジウム予稿集』、3B4-1、電子情報通信学会、2008 年
————・森下朋樹・李　文、「バイオメトリクスにおける生体検知と登録失敗(3) ―静脈認証システムに関する研究（その 2）―」、『電子情報通信学会技術研究報告』、Vol. 106、No. 51、電子情報通信学会、2006 年、53～60 頁
森田遼伍・井沼　学・大塚　玲・今井秀樹、「静脈認証模擬システムへのウルフ攻撃に対する安全性評価」、『2014 年暗号と情報セキュリティシンポジウム予稿集』、2014 年
山田朝彦、『SC27（情報セキュリティ）におけるバイオメトリクス関係プロジェクト』、JAISA バイオ関係標準化セミナー、2015 年 10 月
Bank of America, *Bank of America Introduces Fingerprint and Touch ID Sign-in for its Mobile Banking App*, Bank of America Newsroom, September 15, 2015.
Busch, Christoph, “Related Standards,” *Handbook of Biometric Anti-Spoofing*, Springer, 2014, pp.205-215.
Common Criteria Maintenance Board (CCMB), *Common Criteria Evaluation Methodology for IT Security Evaluation*, Version 3.1, 2012.
Federal Office for Information Security, *Certification Report BSI-DSZ-CC-0790-2013 for MorphoSmart Optic 301, Version 1.0*, 2013.
Future of Identity in the Information Society (FIDIS), *D6.1: Forensic Implications of Identity Management Systems*, 2006.
International Organization for Standardization (ISO) , and International Electrotechnical Commission (IEC), *ISO/IEC 19792 Information technology – Security techniques – Security evaluation of biometrics*, 2009
————, and ————, *ISO/IEC 19795-1 Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*, 2006.
Li, Stan Z., Javier Galbally, Andre Anjos, and Sebastien Marcel, “Evaluation Databases,” *Handbook of Biometric Anti-Spoofing*, Springer, 2014, pp.247-278.
Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, “Impact of Artificial “Gummy” Fingers on Fingerprint Systems,” *Optical Security and Counterfeit Deterrence Techniques IV, Proceeding of SPIE*, Vol. 4677, SPIE (The International Society for Optical Engineering), 2002, pp. 275-289.

Miura, Naoto, Akio Nagasaka, and Takafumi Miyatake, “Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles,” *Proceedings of IAPR conference on machine vision applications*, 2005, pp. 347–350.

Morpho, *MorphoSmart Optic 301 Public Security Target SSE-0000096154-01*, 2013.

Raghavendra, Ramachandra, Manasa Avinash, Sebastien Marcel, and Christoph Busch, “Finger vein Liveness Detection Using Motion Magnification,” *Proceedings of the 7th IEEE International Conference on Biometrics: Theory, Applications and Systems* (*BATS*), 2015.

————, Kiran B. Raja, Jayachander Surbiryala, and Christoph Busch, “A low-cost multimodal biometric sensor to capture finger vein and fingerprint,” *Proceedings of International Joint Conference on Biometrics*, 2014, pp.1-7.

Tome, Pedro, Ramachandra Raghavendra, Christoph Busch, Santosh Tirunagari, Norman Poh, B. H. Shekar, Diego Gragnaniello, Carlo Sansone, Luisa Verdoliva, and Sebastien Marcel, “The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks,” *Proceedings of IAPR International Conference on Biometrics 2015*, 2015.

————, and Sebastien Marcel, “On the Vulnerability of Palm Vein Recognition to Spoofing Attacks,” *Proceedings of IAPR International Conference on Biometrics 2015*, 2015.

————, Matthias Vanoni, and Sebastien Marcel, “On the Vulnerability of Finger Vein Recognition to Spoofing,” *Proceedings of IEEE International Conference of the Biometrics Special Interest Group 2014*, 2014.

Ton, Bram, *Vascular Pattern of the Finger: Biometric of the Future? Sensor Design, Data Collection and Performance Verification*, Master Thesis, University of Twente, 2012.

Une, Masashi, Akira Otsuka, and Hideki Imai, “Wolf Attack Probability: A Theoretical Security Measure in Biometrics-Based Authentication Systems,” *IEICE Trans. Inf. & Syst.*, Vol. E91-D, No. 5, 2008, pp.1380-1389.

Wang, Yiding, and Zhanyong Zhao, “Liveness Detection of Dorsal Hand Vein Based on the Analysis of Fourier Spectral,” *Biometric Recognition*, Springer International Publishing, 2013, pp.322-329.

Yamada, Asahiko, *Protection Profile for Biometric Verification Products* (*BVPPP*), Version 1.0, 2015

Zhou, Yingbo, and Ajay Kumar, “Human Identification Using Palm-Vein Image,” *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 4, 2011, pp.1259-124.

補論 1. 生体特徴にかかる情報の入手の方法

鈴木・宇根［2009］は、ISO/IEC 19792 等を引用し、なりすまし対象の個人に気づかれることなく生体特徴にかかる情報を入手する方法を以下のとおり分類・整理している。

項番	生体特徴の入手方法	考えられる対策例
1	攻撃対象の生体認証システム内部から、登録されている生体情報等、生体特徴にかかる情報を盗取。	・当該システムへのアクセス監視やシステム変更時の発報・検知を行うなど、厳格に管理。 ・テンプレート保護型生体認証技術を採用。
2	攻撃対象の生体認証システムのセンサーに残留する生体特徴の痕跡（残留指紋等）を入手。	・センサーに痕跡が残らない生体特徴を採用。 ・認証時におけるセンサー上の痕跡を除去。
3	日常生活上発生する生体特徴の痕跡（コップの残留指紋等）を入手。	日常生活上痕跡が残らない生体特徴を採用。
4	体表に露出している生体特徴の場合、当該特徴を観測して情報を入手。	体表に露出しない生体特徴を採用。
5	認証時の判定結果（類似度）等が数値で表示される場合、疑似生体特徴を何度もシステムに提示し、その際に得られる一連の数値に基づいて生体特徴を推定（ヒル・クライミング攻撃）。	・判定結果等を出力しない仕様を採用。 ・一定回数連続して認証に失敗した場合、新たな認証処理を開始しない仕様を採用。 ・ヒル・クライミング攻撃に対して一定の耐性を有する方式を採用。
6	同一の生体特徴等を利用している他の生体認証システムから入手。	・他のシステムでは未使用の生体特徴を採用。 ・他のシステムに、生体情報にかかる情報の暗号化や、テンプレート保護型生体認証技術の採用を推奨・促進。
7	なりすまし対象の個人の生体部位を分離して入手。	分離された生体部位から当該情報を入手できない生体特徴を採用。
8	正規の生体認証システムの設置場所に偽のセンサーを設置し、同センサーに生体特徴を提示させて入手。	・当該設置場所を厳重に監視し、偽センサー等を検知・排除。 ・偽センサー等について利用者に注意喚起。

これらのうち、生体認証システムおよびその設置場所が監視等によって厳重に管理されている場合に実行困難と考えられるものは項番 1、8 であり、追加的な対策の必要性は低い。項番 7 についても、当該個人は直ちに事象発生を検知してサービス提供者に通報可能であり、追加的な対策の必要性が低いといえる。また、項番 5 については、運用による対策やテンプレート保護型生体認証技術の採用等、既存の技術によって対策可能であり、追加的な検討の必要性が低いと考えられる。項番 6 も、項番 5 と同様の対応が可能と考えられるものの、同対応の主体は他のシステムの運営者であり、当該生体認証システムの運営者が直接対応することは不可能であることから、項番 1、5 とは異なり、検討対象とする必要があると考えられる。

こうした点を踏まえると、生体特徴にかかる情報の入手方法として検討対象

とすべき項目は、項番 2（センサー等への残留）、3（日常生活上の生体特徴の痕跡）、4（生体特徴の露出）、6（同一の生体特徴等を利用している他の生体認証システムからの入手）の 4 つとなる。

補論２．静脈のパターンを用いる方式にかかる最近の主な研究報告

テスト物体アプローチに関連する最近の主な研究報告のうち、静脈のパターンを用いる方式に関してセキュリティ評価を実施しているものについて、概要を整理すると以下のとおりである。

人工物提示攻撃に関する研究に加え、なりすまし対象の個人の生体特徴ではないが、「多数の（登録されている）生体情報と誤って“一致”と判定されるパターン」（「ウルフ」と呼ばれる）を人工物によって提示する攻撃に関する研究も発表されている。後者の研究においても人工物の作製方法が検討されており、テスト物体アプローチに関連している。

(1) 指の静脈のパターンを用いる方式に関する評価研究

イ．人工物提示攻撃に関するもの

文献	評価対象	評価の概要	備考
Tome, Vanoni and Marcel［2014］	・指の静脈のパターンを用いる生体認証システム ・認証方式は、既存の方式（Miura, Nagasaka and Miyatake［2005］等）をベースに独自に開発。同方式を先行研究（Ton［2012］）の装置を利用して実装。	【想定する攻撃】 ・個人の指の静脈のパターンの画像を何らかの手段で入手したうえで、同画像に基づいて人工物を作製しセンサーに提示する。 【評価に用いられた人工物】 ・人間の指から静脈のパターンの画像を取得し、一定の画像処理を実施。同画像を市販のレーザー・プリンターによって高品質紙に印刷した後、黒インクで静脈部分を強調して描画し人工物とした。 【評価とその内容】 ・被験者（50 名）の指 100 本分の静脈のパターンの情報を予めシステムに登録。そのうえで、上記人工物をセンサーに提示し、一定の判定しきい値のもとで、登録された情報とそれぞれ照合。 ・人工物で提示されたパターンが登録されたものと一致と判定される確率が約 80%となり、人間の指を提示した場合の誤一致率（約 4%）を大きく上回った。	・何らかの手段で指の静脈のパターンの画像を入手することを前提としており、特段の評価はなし。 ・人工物の作製方法については、指の静脈のパターンの画像をプリンターで紙に印刷するという、比較的簡素な手法を採用。

Tome *et al*.［2015］	・指の静脈のパターンを用いた 4 種類の認証方式 ・各方式は、英（サリー大学）、伊（ナポリ大学）、スイス（Idiap 研究所）、ノルウェー（イェービク大学）の各研究チームからそれぞれ提案されたもの。各方式を対象に、同一のセンサーおよび画像処理方式によって取得・生成された画像を照合する。	【想定する攻撃】 ・個人の指の静脈のパターンの画像を何らかの手段で入手したうえで、同画像に基づいて人工物を作製しセンサーに提示する。 【評価に用いられた人工物】 ・被験者の指から静脈のパターンの画像を取得し、一定の画像処理を実施。得られた画像を市販のプリンターによって紙に印刷し、人工物とした。 【評価とその内容】 ・評価の目的は 4 種類の認証方式間での判定性能を比較すること。 ・まず、各認証方式共通の作業として、以下の 3 項目を実施。いずれも Idiap 研究所において事前に実施しデータベースとした。 ✓ 指の静脈のパターンの画像 A（220 枚、被験者 110 名）を登録。 ✓ それらの各画像に一定の処理を施したうえで、紙に印刷して人工物を作製。 ✓ 各人工物をセンサーに提示し、それぞれ画像 B（220 枚）を取得。 ・次に、画像 A と画像 B を共通のデータセットとしたうえで、4 種類の認証方式それぞれにおいて、一定の判定しきい値のもとで、画像 A と画像 B を照合。 ・照合の結果、4 種類のうち 2 種類の認証方式（Idiap 研究所の研究チームによる方式、イェービク大学の研究チームによる方式）において、人工物からの画像を「人間の指の静脈のパターンの画像」と判定する確率がそれぞれ 1.5%、11.0%となり、人間の指同士での誤一致率（いずれも 0.00%）を上回った。 ・残りの 2 種類の認証方式では、上記のいずれの確率も 0.00%となった。	・何らかの手段で指の静脈のパターンの画像を入手することを前提としており、特段の評価はなし。 ・人工物の作製方法については、指の静脈のパターンの画像を一定処理後にプリンターで紙に印刷するという、比較的簡素な手法を採用。 ・指の静脈のパターンの画像、および、人工物から取得した画像をともにデータベース化したことにより、評価用の環境を同一としたうえで、異なる生体認証のアルゴリズムの比較を可能とした。

Raghavendra *et al.*［2015］	・指の静脈のパターンを用いた生体認証システム（生体検知あり） ・静脈のパターンの動画を撮影し、血流の有無を手掛りに人工物を検知する方式。まず、血流による画像の変化を検出して人工物の判定・検知を実施し、人工物でないと判定された場合、静脈のパターンの照合を実施。	【想定する攻撃】 ・個人の指の静脈のパターンの画像を何らかの手段で入手し、同画像に基づいて人工物を作製してセンサーに提示する。 【評価に用いられた人工物】 ・100 人の被験者の指（両手の人差指と中指、合計 4 指）から静脈のパターンの画像（静止画）をセンサー（透過光型）で取得。画像に一定の処理を施したうえで、インクジェット・プリンターとレーザー・プリンターでそれぞれ高品質紙に印刷し人工物とする。 【評価とその結果】 ・被験者から指の静脈のパターンの動画（合計 600 ファイル、各動画は 25 フレーム）を撮影するとともに、それらの動画から、静脈のパターンの静止画を生成して登録（人工物の作製にも利用）。 ✓ 血流の検知については、動画の最初と最後のフレームの画像の変化を抽出し、変化量が一定値を超えた場合に生体の指と判定するもの。 ・250 枚の人工物を作製・提示し、対応する個人の指の静脈のパターンの動画および静止画との照合を実施した結果、人工物の提示を誤って人間の指の提示と判定する確率が、インクジェット・プリンターによる人工物の場合には 2.40%となったほか、レーザー・プリンターによる人工物の場合には 5.20%となった。 ✓ 生体検知の仕組みを有しない、指の静脈パターンを用いた他の生体認証システム（Raghavendra *et al.*［2014］）において、上記の人工物を提示し当該確率を計測したところ、インクジェット・プリンターによる人工物の場合には 90.62%となったほか、レーザー・プリンターによる人工物の場合は 91.87%となった。	・何らかの手段で指の静脈のパターンの画像を入手することを前提としており、特段評価はなし。 ・人工物の作製方法については、指の静脈のパターンの画像を一定処理後にプリンターで紙に印刷するという比較的簡素な手法を採用。 ・指の静脈のパターンの動画や人工物から取得した動画をデータベース化。評価用環境を同一としたうえで、異なる生体認証システムの比較を可能とした。 ・血流による画像の変化を検出する仕組みを提案。人工物の提示を誤って人間の指と誤判定する確率を計測。

ロ．ウルフのパターンを人工物によって提示する攻撃に関するもの

文献	評価対象	評価内容	備考
森田ほか［2014］	・指の静脈のパターンを用いた生体認証システム ・既存の認証方式（Miura, Nagasaka and Miyatake［2005］）を実装したシステムを開発。	【想定する攻撃】 ・ウルフとなるパターンを人工物によってセンサーに提示する、というもの。ウルフとして、Une, Otsuka and Imai［2008］が理論的に示したパターンを使用。 【評価に用いられた人工物】 ・ウルフを印刷した OHP シート（複数枚）、白色のプラスチック板、オレンジ色のゴム板を重ねて人工物（1 個）を作製。 【評価とその結果】 ・人間の指を用いて静脈のパターン（70 指分）の情報を予めシステムに登録。そのうえで、上記人工物をセンサーに提示し、一定の判定しきい値のもとで登録された情報とそれぞれ照合。 ・照合の結果、人工物を誤って人間の指として一致と判定する確率が 39.2%～62.5%となり、人間の指を提示した場合の誤一致率（0.00%～0.0038%）を大きく上回った。	・生体特徴にかかる情報の入手に関しては、「攻撃者が攻撃対象のシステムの認証方式を分析しウルフを特定する」というものであり、ウルフの特定の成功が前提となっている。 ・人工物の作製方法に関しては、松本・田中［2008］の手法をベースとして、OHP シート等の複数の素材を組み合わせる手法を提案。

(2) **手のひらの静脈のパターンを用いる方式に関する評価研究**

文献	評価対象	評価内容	備考
Tome and Marcel［2015］	・手のひらの静脈のパターンを用いた生体認証システム（生体検知なし）。 ・既存の認証方式（Zhou and Kumar［2011］）をベースに独自の認証方式を提案。同方式を実装したシステムを開発。	【想定する攻撃】 ・人間の手のひらの静脈のパターンの画像を何らかの方法で入手したうえで、同画像に基づいて人工物を作製しセンサーに提示する。 【評価に用いられた人工物】 ・手のひらの静脈のパターンの画像を取得し、一定の画像処理を実施。得られた画像を市販のプリンターによって紙に印刷し人工物とした。 【評価とその結果】 ・50 人の被験者の左右の手のひらから取得された静脈のパターンの画像（合計 1 千枚）を準備。これらの画像は、Idiap 研究所のデータベースから取得。静脈のパターンの画像に一定の処理を施したうえで、システムに登録するとともに、それぞれ紙に印刷して人工物を作製。 ・上記人工物をセンサーに提示し、対応する手のひらの静脈のパターンの情報と照合。人工物を誤って人間の手のひらとして一致と判定する確率が 43～75%となり、手のひらを提示した場合の誤一致率（3～9%）を大きく上回った。	・何らかの手段で静脈のパターンの画像を入手することを前提としており、特段の評価はなし。 ・人工物の作製方法については、手のひらの静脈のパターンの画像を一定処理後にプリンターで紙に印刷するという、比較的簡素な手法を採用。 ・手のひらの静脈のパターンの画像がデータベース化されたことにより、評価用の環境を同一としたうえで、異なる生体認証システムの比較評価が可能。

補論３．人工物の作製にかかる攻撃ポテンシャルの評価

わが国における産官連携プロジェクトでは、静脈のパターンを用いた方式を対象に、人工物提示攻撃の攻撃ポテンシャルを評価している（日本自動認識システム協会ほか［2015］）。人工物の作製方法の事例（5 件）を対象にスコアを算出したうえで、攻撃ポテンシャルが 5 段階（basic、enhanced-basic、moderate、high、beyond high）のどのレベルに相当するかを検討している。その際、人工物の作製に必要なスキルや時間・機材等のリソースにかかる評価を実施しており、評価の考え方が示されている。評価結果の概要は以下のとおりである。

静脈のパターンにかかる人工物作製の攻撃ポテンシャル

研究報告	評価対象の人工物作製方法	攻撃ポテンシャルと評価の考え方
FIDIS［2006］	静脈のパターンの画像を紙に印刷。それを、手、ペットボトル、ペットボトルにゴム手袋をかぶせたもの（1 種類）にそれぞれ装着し、センサーに提示。	○攻撃ポテンシャル：スコア 7［basic］ ・センサー等の当該機器の知識に加え、人体の光学特性にかかる専門知識が必要であり、「攻撃に必要な専門技術」の観点で「熟練（proficient）」と評価。 ・人工物は比較的短時間で作製可能であり、「攻撃に要する時間」の観点で「1 日以内」と評価。 ・「攻撃に必要な機材」の観点で「標準的な機材（standard）」で作製可能と評価。
Wang-Zhao［2013］	静脈のパターンの画像を紙に印刷。それを手に貼り付けてゴム手袋をかぶせ、センサーに提示。	○攻撃ポテンシャル：スコア 8［basic］ ・センサー等の当該機器の知識に加え、人体の光学特性にかかる専門知識が必要であり、「攻撃に必要な専門技術」の観点で「熟練（proficient）」と評価。 ・人工物は比較的短時間で作製可能であり、「攻撃に要する時間」の観点で「2 日～1 週間」と評価。 ・「攻撃に必要な機材」の観点で「標準的な機材（standard）」で作製可能と評価。
Tome, Vanoni and Marcel［2014］	静脈のパターンの画像（一定の処理を実施）を、白紙、OHP シート、高品質紙、ボール紙にそれぞれ印刷。	
森田ほか［2014］	静脈のウルフパターンを OHP シートに印刷。ゴム・白プラスチック板に当該用紙を貼付け。	
松本・森下・李［2006］	人工物として、大根、エポキシ樹脂と人工雪剤の混合物に加え、ガラス製試験管や透明ビニール・チューブにビニール・テープと紙（静脈のパターンの画像を印刷したもの）を貼り付けたものをそれぞれ作製。	○攻撃ポテンシャル：スコア 13［enhanced-basic］ ・センサーや光の拡散・反射等にかかる専門知識が必要であり、「攻撃に必要な専門技術」の観点で「熟練（proficient）」と評価。 ・人工物作製にやや特殊な素材（人工雪剤やエポキシ樹脂）を利用しており、「攻撃に要する時間」の観点で「1～2 週間」と評価。 ・「攻撃に必要な機材」の観点で「特殊な機材（specialized）」が必要と評価。

（備考）上記図表は日本自動認識システム協会ほか［2015］の記述を参照して作成。

補論４．コモン・クライテリアにおけるセキュリティ評価・認証の流れ

コモン・クライテリアにおける情報システムや製品（以下、情報システムという）のセキュリティ評価・認証は、以下の流れで実施される（田村・宇根［2008］、情報処理推進機構［2015a］）。

(A) 情報システムの利用者（あるいは利用者の業界団体等）が、同システムの使用環境やセキュリティ機能等を内容とする「セキュリティ要求仕様書（PP：Protection Profile）」を作成する。

- ✓ 具体的には、PP には、同システムの概要、利用する環境、セキュリティ機能にかかる要件（「セキュリティ機能要件」と呼ばれる）、当該機能が適切に実装されていることを確認するための要件（「セキュリティ保証要件」と呼ばれる）等が記述される。
- ✓ セキュリティ機能要件やセキュリティ保証要件等、PP に記載するべき情報の雛形が ISO/IEC 15408 シリーズに規定されており、利用者は、同国際標準の記述に適合した形式で PP を作成することが求められる。利用者は、作成した PP が ISO/IEC 15408 シリーズに適合していることの審査を評価機関に対して依頼することが可能であり、「適合している」旨が認められれば、コモン・クライテリアの公式サイトに登録・公表される。実際の運用では、利用者が PP を独自に作成する場合よりも、情報システムの開発者（ベンダー等）が汎用的な PP を作成して公表するケースが多い。
- ✓ 生体認証システムの評価の場合、同システムが使用される環境、想定すべき攻撃者のリソース（攻撃ポテンシャル）、アプリケーションに応じたセキュリティ要件を、ISO/IEC 15408 シリーズに基づいて記載する必要があるが、同システム特有の脆弱性に対応するためのセキュリティ保証要件等が ISO/IEC 15408 シリーズに記載されておらず、新たに準備する必要がある。

(B) 情報システムの開発者は、登録・公表された PP 等を参考にしつつ、同システムが想定する脅威やセキュリティ機能等を内容とする「セキュリティ設計仕様書（ST：Security Target）」を作成する。

- ✓ ST には、当該システムの名称・識別子、用途・特徴、同システムを構成するハード・ソフト想定する脅威、セキュリティ対策の方針、運用環境、セキュリティ機能要件、セキュリティ保証要件等が記述される。これらは、PP と同じく、ISO/IEC 15408 シリーズを参照して記載

する。また、開発者が ST を作成する際に参考にした PP があれば、当該 PP の名称・識別子も ST に記載される。

- ✓ 生体認証システムの評価の場合、同システムが想定する脅威（攻撃ポテンシャルも含まれる）や用途、実装しているセキュリティ機能を ISO/IEC 15408 に基づいて記載する必要があるが、同システム特有の脆弱性に対応するためのセキュリティ保証要件等が記載されておらず、新たに準備する必要がなる。

(C) 開発者は、情報システムのセキュリティ評価を評価機関に依頼するとともに、当該評価結果の認証を認証機関に依頼する。

- ✓ 評価機関は、国際試験所認定協力機構（ILAC : International Laboratory Accreditation Cooperation）に加盟する機関から「評価機関」としての認定を得た組織である。2015年9月末現在、わが国では、4つの組織（一般社団法人ITセキュリティセンター評価部、株式会社ECSEC Laboratory評価センター、みずほ情報総研株式会社情報セキュリティ評価室、TÜV Informationstechnik GmbH Evaluation Body for IT-Security）が評価機関となっている。どの評価機関に評価を依頼するかについては、各評価機関が有する人材・設備等を確認したうえで決定することとなる。
- ✓ わが国の認証機関は独立行政法人情報処理推進機構である。

(D) 評価機関は、PP や ST のほか、開発者から提出されたテスト証拠資料等を参考にしながら、「当該システムのセキュリティが本当に ST 記載の要件を満足しているか」を評価する。

- ✓ 評価結果は、認証機関に報告される。個別のシステムにかかる評価を具体的にどのように実施しているかに関しては、各評価機関のノウハウやスキルに依存しており、非公開とされるケースが多い。

(E) 認証機関は、評価機関による評価結果を受領し、評価のプロセスや内容の適切性を確認する。「適切」と判定した場合、認証機関は、当該システムに対して認証書を開発者に対して発行する。

- ✓ 認証を得た情報システム等の情報は情報処理推進機構の関連ウェブサイト等に掲載されるほか、情報セキュリティ評価・認証結果の相互認証体制（コモン・クライテリア承認アレンジメント、Common Criteria Recognition Arrangement）に基づき、同加盟国 25 か国にも周知される。