人工物メトリクスを用いた個体管理技術ガイダンス

初版（revision 1.0.0.0000）

2022 年 1 月 11 日

国立研究開発法人産業技術総合研究所

サイバーフィジカルセキュリティ研究センター

テクニカルレポート CPSEC-TR-2022001

目次

序文と免責事項（Foreword and Disclaimer）

本ガイダンスは、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）からの受託事業（JPNP16007）の一部として、国立研究開発法人産業技術総合研究所（産総研・AIST）サイバーフィジカルセキュリティ研究センター（CPSEC）が企業・大学等の有識者委員とともに構成した「人工物メトリクスを用いた個体管理技術検討委員会」においてとりまとめたものです。本ガイダンスの内容に寄与した委員の意見は技術者としての個人の知見に基づくものであり、各々が所属する会社等の意見を代表するものではありません。

本ガイダンスの最新版や関連する情報は産総研（AIST）の右記の URL https://www.cpsec.aist.go.jp/achievements/artmet にて提供される予定です。

This document is based on results obtained from a project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

1. はじめに

1.1. 背景と動向

人工物メトリクスは、個体に固有の物理的特徴を測定する技術である。この技術による測定結果を照合または識別することで実現する個体管理技術は、人工的に生産される製品または部品の取引における個体管理や模倣品対策として利用されるようになってきた。ここでは、人工物メトリクスを用いた個体管理技術に関するガイダンスが求められる背景と動向を５つの視点で整理する。なお、本ガイダンスで使用する用語は、「付録１：用語と定義」を参照のこと[1]。

(1) 製品のサプライチェーン・バリューチェーンの管理強化

製品の取引（新品の製造、流通、販売、消費、及び中古品の取引）において、模倣品に起因する被害（機会損失等）や、不良品に起因する被害（事故等）が発生すると、それらの実損に係る被害額以外に、ブランドイメージの低下・失墜（風評被害を含む)、技術的優位性の低下によるイノベーションと創造意欲の減衰などにつながる。このような模倣品や不良品の流通を回避するためには、その前提として、品質が保証された正規品であることの証跡を生成し、模倣品や不良品でないことがチェックできる仕組みによるトレーサビリティの確保が求められる。さらに管理すべき対象を、製品群、製品単体、製品を構成する構成要素（部品）など、要求に応じて管理粒度を細かくすることで、より精緻なトレーサビリティ能力が実現できる。

このように、製品または部品の取引におけるサプライチェーン、あるいはより一般的に個体物の取引を適正化するためのデータを取り出し連携させた価値創造サイクル（バリューチェーン）を機能させるために、トレーサビリティの確保と管理粒度の微細化による管理強化が期待されるようになってきた。

(2) 技術的制約の緩和

製品のサプライチェーンにおけるバリューチェーンの管理強化には、バリューの生成・検証に必要な多様かつ強力なコンピューティング能力と、バリューを維持し流通させるための合理的かつ安定した通信ネットワーク環境が求められる。昨今の通信基盤の普及と計算能力の向上は、人工物メトリクスによる個体管理を実用化するための技術的制約を緩和する傾向にある。

(3) 最新技術への対応

照合または識別技術としての AI（機械学習）の利用、データベースとしての分散型台帳技術（DLT: Distributed Ledger Technology）の適用など、最新技術への対応により、パフ

[1] 用語及び概念の整理には[1][2][3][4][16]などを参考としている。

ォーマンスの向上や実用化に向けた技術課題の解決が図られつつある。このような最新技術への対応として、適用技術の共通化や標準化に関する議論が今後の課題として挙げられる。

(4) 国際的な議論

2015 年に設置された ISO TC 292 は、セキュリティ関連の標準化に向けたテーマを包括的に扱うことを目的に統合された専門委員会である。模倣品対策の標準化は、現在、ISO TC 292（Security and resilience）の WG4（Authenticity, integrity and trust for products and documents）で議論が進められている[2]。

現在、さまざまな分野で、企業間の取引に利用される電子データ交換（EDI: Electronic Data Interchange）が実用化されている。人工物メトリクスを用いた個体管理の管理情報を流通させるためには、これらの EDI を利用可能とするための基盤整備や、サプライチェーン上のイベントの完全性を保証するものとして期待される DLT の機能性を加えるなど、国際的な流通基盤の整備と整合性の確保に関して議論を深めていく必要がある。

このように、海外から第三者認証や規制等の要請が出てきた場合に備えた事前研究として、また、国内での議論の基盤として用語や概念の整理が必要となっている。

(5) 模倣品対策に関連する組織

模倣品対策に関連する組織は、行政、業界団体、国際標準化、研究開発において存在する。

行政においては、内閣に設置された知的財産戦略本部が、権利者・企業の要望を受け模倣品・海賊版対策の政府内の連携体制を整備するため、関係府省が一体となって対策に取り組むよう経済産業省を一元的な相談窓口とすることを決定し、経済産業省は、2004 年 8 月に製造産業局に模倣品対策室(政府模倣品・海賊版対策総合窓口)を開設している。模倣品対策室からは、模倣品・海賊版対策の相談業務に関する年次報告書[6]が発行されている。なお、模倣品対策室は 2020 年 4 月に特許庁に移管されている。

主な業界団体としては、IIPPF、B.P.P.が挙げられる。日本貿易振興機構（JETRO）に設置された「国際知的財産保護フォーラム（IIPPF）[7]」は、模倣品・海賊版など主に海外における知的財産権侵害問題の解決をめざす企業・団体で構成された協議体である。「Brand Protection Partnership（B.P.P.®）[8]」は、YKK 株式会社が主催するブランド保護活動であり、参加する組織の取り組みなどの情報交換を促進することを目的とする。

関連する国際標準化組織としては、前述の ISO TC292（セキュリティとレジリエンス）WG4（模倣品対策）、及びその国内委員会である SG3 があり、模倣品対策技術の研究開発は、企業、大学、産業技術総合研究所（AIST）などで実施されている。

[2] 人工物メトリクスに関しては ISO 22387 として国際標準化が進められており、2022 年 1 月時点のプロジェクトの段階は DIS (Draft International Standard: 国際規格原案)である[5]。

1.2.　目的

本ガイダンスの目的は以下の通りである。

- 国際的な議論や調整を行う際の技術的な下地の形成
- セキュリティ面での考え方の議論と共通認識の醸成
- 人工物メトリクス分野の認知度の向上

人工物メトリクス分野の技術の標準化は、1.1 背景と動向(4)に示すように模倣品対策に関する技術の標準化として開始されたところである。今後は周辺技術の標準化や、管理情報の流通基盤の整備と整合性に関する国際的な議論・調整が見込まれることから、本ガイダンスにより、人工物メトリクス分野の技術全般の体系を整理することを第一の目的とする。

その中でも、セキュリティ面の考え方については、既存のセキュリティ規格や評価基準との整合性の確保に重点を置き、共通認識を醸成することを第二の目的とする。特に、人工物メトリックシステムのユースケースの分類、及びユースケース毎の指標、セキュリティに関連した注意事項等を体系的に整理するとともに、日本語の用語とその使い方の共通化を図ることを目的とする。

また、本ガイダンスを公開し、調達者をはじめ広く一般に、人工物メトリクス分野の技術の認知度向上を目指すことを第三の目的とする。

1.3.　範囲

本ガイダンスの対象範囲を以下に示す。

(1) 対象とする技術

本ガイダンスの対象とする技術は「人工物メトリクスを用いた個体管理技術」であり、個体の物理的特徴の測定結果を照合または識別することによる管理技術を対象とする。

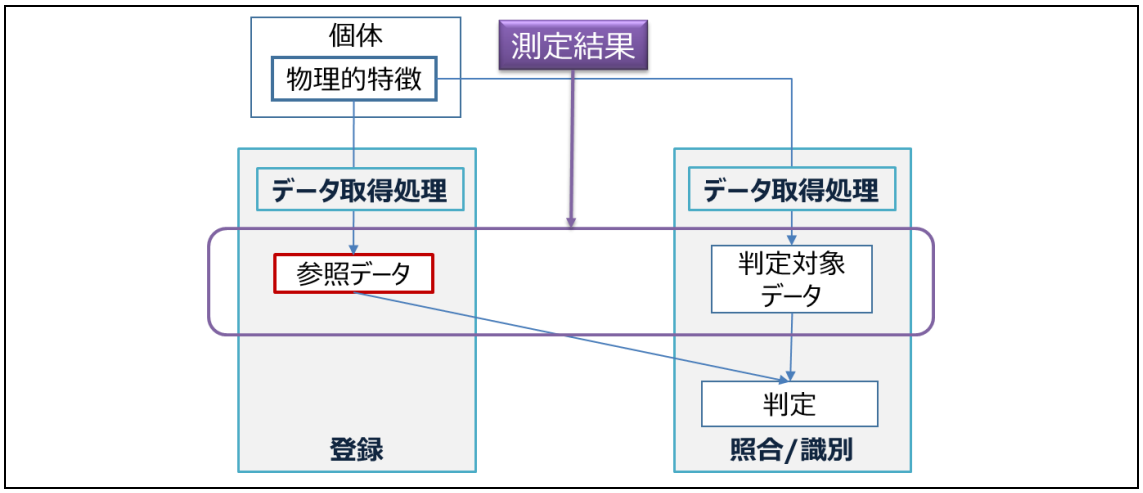


図 1-1 人工物メトリクスを用いた個体管理の概念

以下は、本ガイダンスの対象外である。

- 物理的特徴を照合/識別に用いない技術
  - バーコードや RFID などに記録されたデジタルデータのみを用いる技術など
- 客観的な数量として測定せず主観的な感覚（視覚・聴覚・味覚・嗅覚・触覚など）で行う判定
  - ホログラムの目視での識別、官能検査など

(2) 管理対象区分と本ガイダンスとの関係

管理対象の区分として経済産業省の調査報告書[9]では、①製品（a. 本体（中身の成分など)、b.本体・パッケージ（表面)、c1.添付物（印刷物)、c2.添付物（タグ)）及び ②製品情報（製品画像や説明文など）のように分類している。本ガイダンスは、「個体の物理的特徴の測定結果を照合または識別することによる管理技術」であれば、区分は問わず対象として扱う。

(3) 管理対象判定機能と本ガイダンスとの関係

管理対象を判定する機能として経済産業省の調査報告書[10]では、①オバート機能（目で見てわかる技術を用いて実現される機能)、②コバート機能（簡易的な器具を用いて実現される機能)、③フォレンジック機能（専門分析により実現される機能）に分類している。本ガイダンスは、機械読取可能な技術を対象とするため、②の一部、及び③を対象として扱う。

(4) 対象の管理策及び模倣品対策の分類と本ガイダンスとの関係

対象の管理策を含む模倣品対策の分類として政府模倣品・海賊版対策総合窓口の調査報告書[11]の 9 ページ目では、権利侵害の事前・事後を分け、①事前の予防措置（a.ブランディング、b.権利取得、c.製造と情報管理、d.契約)、②事後のエンフォースメント（e.行政摘発、f.行政訴訟、g.民事訴訟、h.刑事訴訟)、及び③事前・事後の両方に係る模倣品対策（i.調査・監視（モニタリング)、j.共同実施（a.～i.を業界として共同実施））に分類している。本ガイダンスは、「正規及び意図的でない非正規個体を対象にする場合」は、①における a. c.、③における i. 及びそれらの共同実施を対象として扱う。また、「意図的な非正規個体も照合対象にする場合」は、前者に加え、②及び③におけるフォレンジック機能も対象として扱う。

2. 人工物メトリックシステム

2.1. 人工物メトリクス

「人工物メトリクス」とは、物の物理的特徴の計測または測定を示す用語であり、物とその管理技術や情報セキュリティ技術などを結び付けることを目的とする技術である。生体の特徴の計測または測定を示す「バイオメトリクス」と対をなす。

(1) 物理的特徴

人工物メトリクスにおける物理的特徴とは、主観的な感覚量ではなく、客観的な数量に置き換えらえる特徴であり、製造者であっても再現が困難な特徴を用いる。例としては以下が挙げられる。

- 紙を形成する植物繊維の分布状態
- 塗料に含まれる金属微粒子の分布状態
- 個体に固有の微細でランダムな凹凸パターン
- 金属箔のランダムな表面形状

このほかにも、光学特性、磁気特性、電気特性、振動特性など、さまざまな物理特性によって計測可能な物理的特徴を利用した人工物メトリクスが提案されている。

(2) 照合と識別

人工物メトリクスを用いた個体の正規性の判断の形態として、照合（1 対 1 照合）と識別（1 対 N 照合）が存在する。

照合とは、提示された ID または参照データと個体とが対応するか否かを返すアプリケーションであり、参照データの保管場所により、個体添付型（参照データを個体と共に配布する場合）と、データベース記録型（参照データをデータベースまたは分散型台帳などに格納する場合）がある。

識別とは、提示された個体に対応する 0 個または 1 個以上の ID の候補を、識別順位を付けて返すアプリケーションであり、参照データの保管場所はデータベース記録型のみがある。これらの分類を図 2-1 に示す。

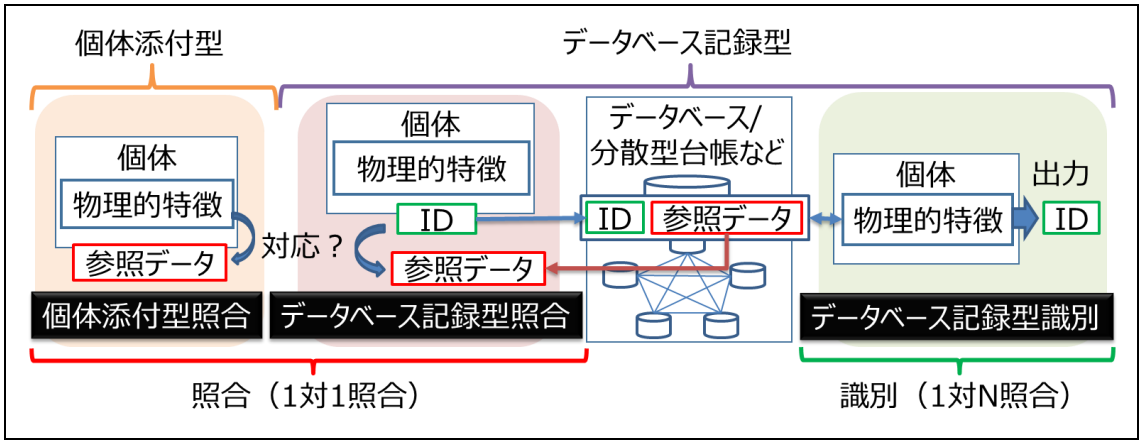


図 2-1 照合/識別と保管場所による分類

なお、判定に用いる物理的特徴の位置は個体の形状などに応じて予め決めておくか、照合の場合には参照データまたは ID とともに配布することも可能である。

照合と識別の使い分けに関する基本的な考え方と例を以下に示す。

- 照合を用いた方がよい場合

  個体とともに ID または参照データを流通させることができる場合。例えば、

  - 個体またはそのパッケージもしくは鑑定書などへ ID または参照データを記載することが可能な場合
  - 製造過程・流通経路の途中で、ID または参照データを含む印字・シール等の改ざん、貼り替えを検知する場合

- 識別を用いた方がよい場合

  個体とともに ID または参照データを流通させることができない場合、または、できるが避けたい場合。例えば、

  - ばら売りの製品や部品にバーコードやシリアル番号などを付けるスペースが無い場合や付けるコストを削減したい場合
  - ID または参照データが記載されていたパッケージ、鑑定書などを紛失している場合

ID が確定すれば、その ID に関連する情報をデータベースなどから入手することが可能となる。また、ID の代わりに直接アプリケーションで必要となる情報を用いることも可能である。個体添付型では、参照データに ID やアプリケーションで必要となる情報を含めることや、参照データのハッシュ値を ID とすることも可能である。

その他、図 2-2 に示すように「製品群/部品群など同じ属性を持つ単位を 1 つの個体」と捉えることも可能である。例えば、ある部品 X に不具合が見つかり、それと同じ製造機械で製造された部品を特定し回収したいケースでは、同じ製造機械で生成されたロットに対して共通の物理的特徴を構成することで、他の製造機械で生成されたロットと区別することが可能となる。

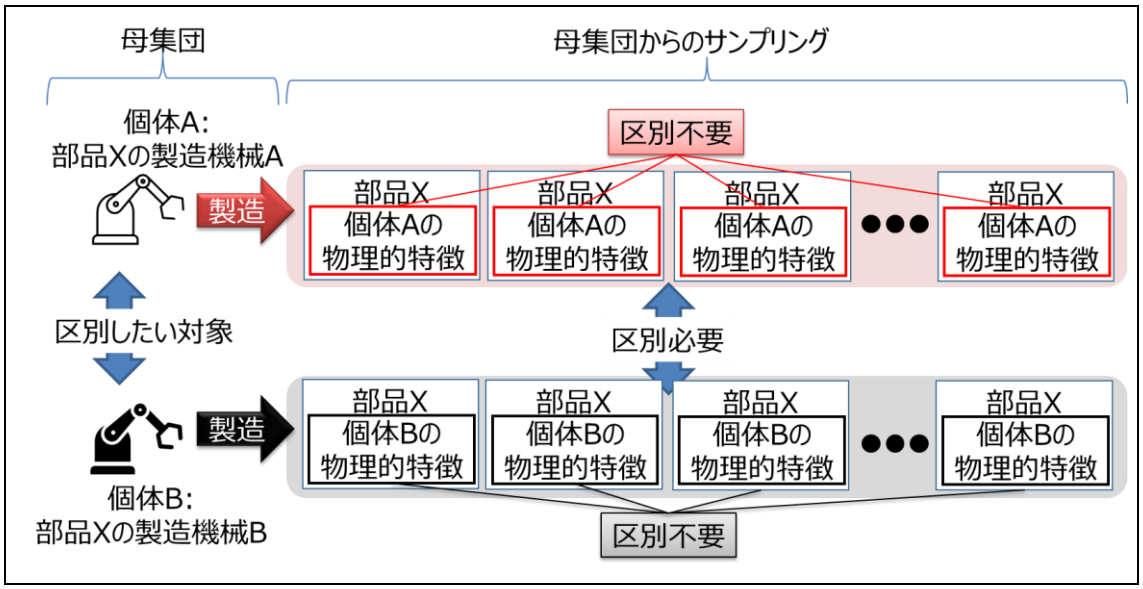


図 2-2 製品群/部品群などを１つの個体と捉える際の考え方

(3) 耐クローン性

人工物メトリクスを用いた個体管理を意図通りに機能させるためには、必要とされる精度で個体を正しく照合または識別する必要がある。一方、複製として作成された意図的な非正規個体（クローンと呼ぶ）が生成され、正規個体を模擬して不正に使用される可能性も考えられる。このようなケースが想定され、対応することが求められる場合、攻撃者がその正規個体の製造方法や検証方法に係る情報を入手したとしても、クローンを作成することを困難とする必要がある。このようなセキュリティ特性を耐クローン性と呼ぶ。

2.2. 人工物メトリックシステムの概念

人工物メトリクスを実現するシステムを、人工物メトリックシステムと呼ぶ。図 2-3、図 2-4、図 2-5 は、それぞれ個体添付型照合処理、データベース記録型照合処理、データベース記録型識別処理の概念図である。

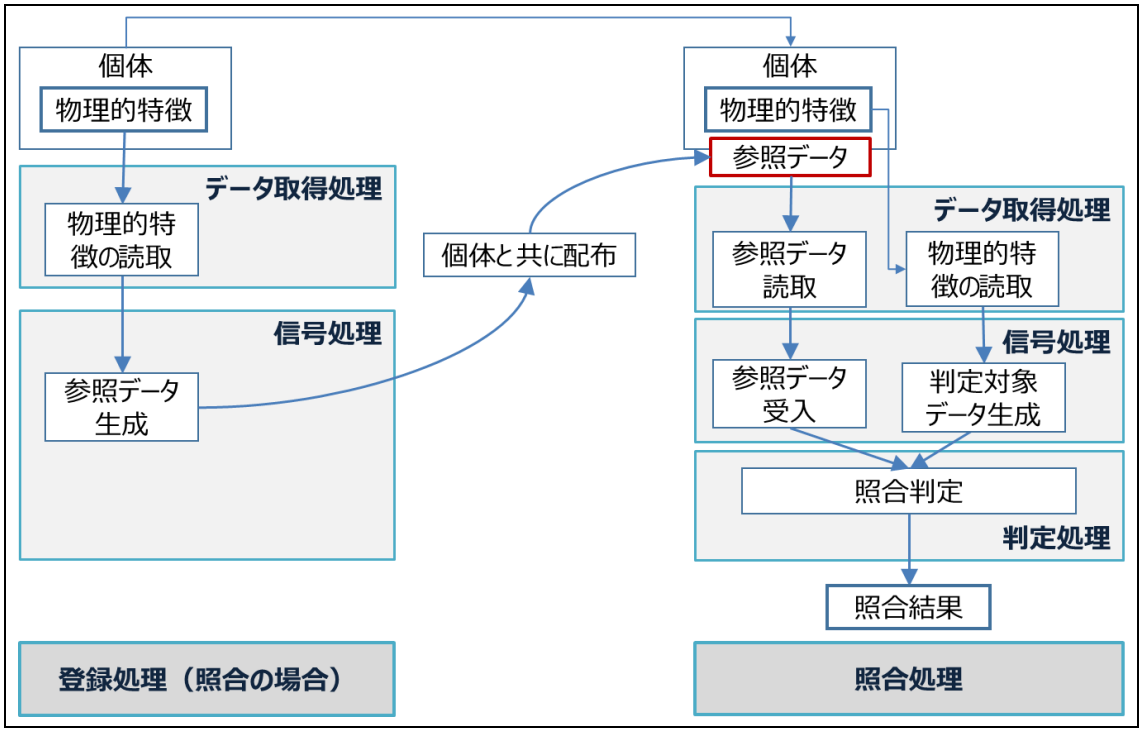


図 2-3 人工物メトリックシステムの概念図（個体添付型照合）

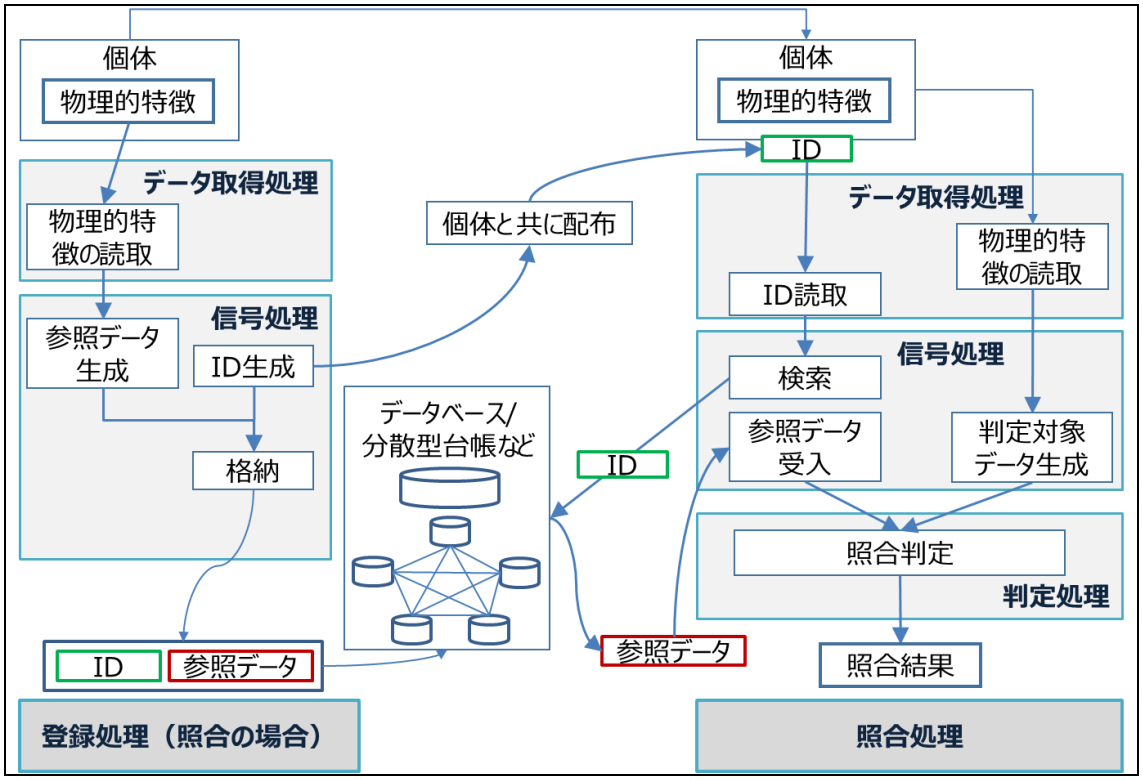


図 2-4 人工物メトリックシステムの概念図（データベース記録型照合）

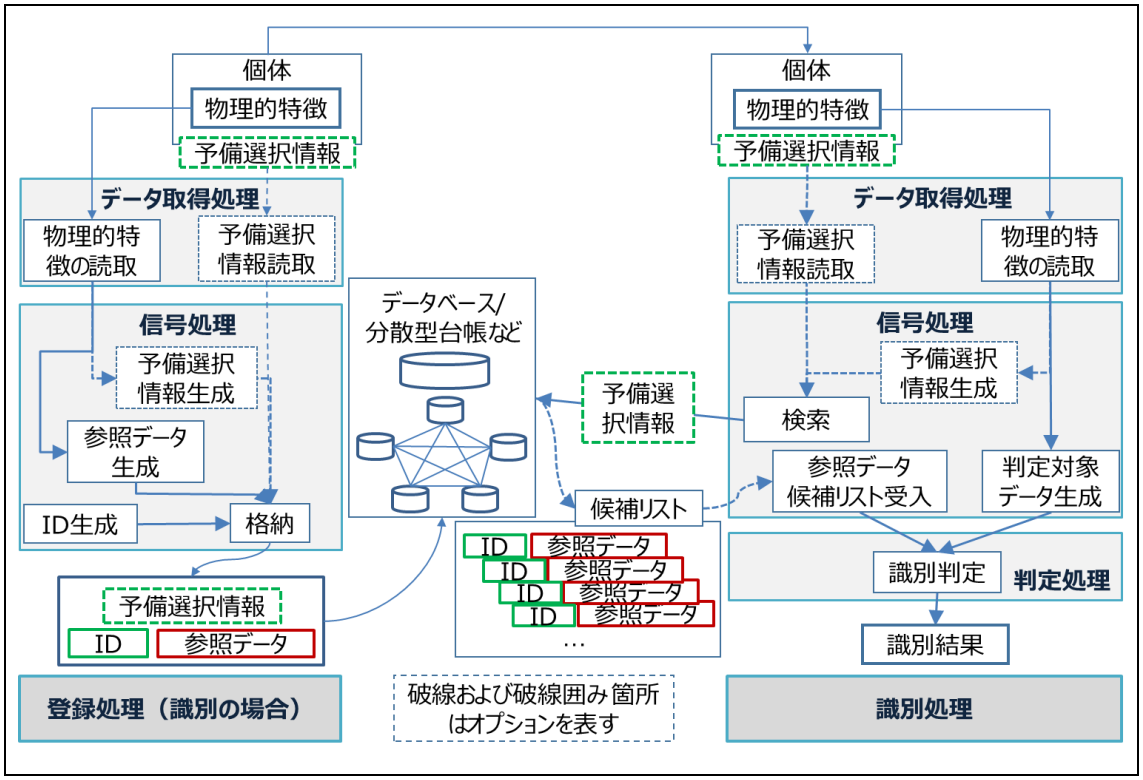


図 2-5 人工物メトリックシステムの概念図（データベース記録型識別）

これらの図から抽出した一般的な人工物メトリックシステムの共通要素を以下に示す。

- 登録処理
  - 配付前の個体の物理的特徴を含む人工物メトリックサンプルをセンサなどによって読み取る。
  - センサ出力を登録用の信号処理に送り、サンプルに特有の再現可能な計測値を抽出し、参照データを生成する。
  - 参照データはデータとして蓄積するか、または個体とともに配付する。
- 照合/識別処理
  - 配付後の個体の物理的特徴を含む人工物メトリックサンプルをセンサなどによって読み取る。
  - その出力を照合または識別用の信号処理に送り、サンプルに固有の再現可能な計測値を抽出し、判定対象データを生成する。
  - 照合の場合は、比較対象の特定の参照データと判定対象データを比較して合致するかどうかを判定する。
  - 識別の場合、比較対象のいくつかの参照データもしくはすべての参照データと比較して合致するものがあるか否かを判定する。
  - 判定は、参照データの特徴と、比較した判定対象データの特徴との類似性に基づいて決定される。

2.3. 人工物メトリックシステムの構成要素

人工物メトリックシステムの構成要素である各サブシステムは以下の通り。

(1) データ取得処理サブシステム

データ取得処理サブシステムは、センサに提示された個体から物理的特徴を含む画像または信号を読取り、人工物メトリックサンプルの電子データを生成する。登録処理（識別の場合）では、個体とともに配布される予備選択情報を読み取ることもある。照合処理または識別処理では、個体とともに配布される参照データまたは ID を読み取ることもあり、識別処理では、個体とともに配布される予備選択情報を読み取ることもある。また、どの物理的特徴または物理的特徴のどの部分を読み取るべきかの情報をチャレンジ情報として受け取り、対応する電子データをレスポンスとして生成することもある。

(2) 信号処理サブシステム

信号処理サブシステムは、人工物メトリックサンプルの電子データから照合または識別に用いられる物理的特徴を抽出し、登録処理の場合は参照データと ID を生成、照合処理または識別処理の場合は、判定対象データを生成する。照合処理の場合、データ取得処理サブシステムから受け渡された ID をもとに、データベースに格納された参照データを検索し、取り出した参照データを受け入れる。識別処理の場合、データ取得処理サブシステムから受け渡された予備選択情報（信号処理サブシステム内で生成されることもある）をもとに、データベースに格納された参照データと ID の候補リストを検索し、取り出した参照データ候補リストを受け入れる。

(3) 判定処理サブシステム

判定処理サブシステムは、信号処理から受け渡された参照データと判定対象データの適合度を比較するための照合スコアを算出し、規定した閾値と照合スコアを比較することにより、参照データと判定対象データが合致するか否かを判定する。照合処理の場合、その判定結果を照合結果として出力する。識別処理の場合、候補リストに含まれる参照データの各々と判定対象データとの照合スコアを順次算出し、規定した閾値と照合スコアを比較することで、判定対象データに合致する参照データに対応する 0 個または 1 個以上の ID 候補を選定し、識別順位を付けて識別結果として出力する。

(4) サブシステム間のデータ伝送

サブシステム間でデータを伝送する場合（データベースや他の連携するシステムとの間のデータの伝送を含む）、伝送されるデータの信頼性、完全性及び機密性を確保するために、暗号技法を用いることができる。

2.4. 人工物メトリックシステムの機能

人工物メトリックシステムの主要な機能は以下の通り。

(1) 登録

登録は、個体から参照データを生成・出力するためのトランザクションを処理する。
登録の一般的な機能には以下が含まれる。

- サンプル収集（登録対象個体の物理的特徴の読取、人工物メトリックサンプルの電子データの生成を含む）
- 参照データ生成（対象領域抽出、物理的特徴の抽出、品質評価（サンプル・物理的特徴が参照データ生成に適切かどうかの判定、判定の結果、不適切な場合の繰り返し登録試行要求など）を含んでもよい）
- ID 生成（データベース記録型照合/識別の場合など ID が必要な場合）
- 予備選択情報の読取または生成（識別の場合。予備選択情報の例としては、①個体またはそのパッケージなどに予め記載されている情報（製造日、製造場所など）、②取得した物理的特徴から生成されたデータ などがある）
- 格納（データベース記録型照合/識別において、ID とその参照データ、予備選択情報を用いている場合にはその情報、その他必要に応じて ID に紐づけられた個体に関する情報など格納する。個体添付型照合においては参照データ、必要に応じて ID、個体に関する情報などを個体に添付または、個体と共に配布する媒体（パッケージ、鑑定書など）に格納する。）
- （必要に応じて）テスト（登録した参照データが、照合処理または識別処理で確実に利用できることを確認するための照合テストまたは識別テストを登録処理に含んでもよい）

登録処理は、①新規登録、②追加情報登録　の２つに分類される。

- 新規登録
  - ホワイトリスト登録処理（正規個体を登録する処理。単に登録または登録処理といった場合には、ホワイトリスト登録処理を意味する）
  - ブラックリスト登録処理（発見された非正規個体をブラックリストに登録する）
- 追加情報登録

  本物・偽物を問わず、その個体の物理的特徴を判定する際に必要となる補足情報を追加登録する処理。例えば、より詳細な判定を行うためのパラメータ情報や専門家による過去の鑑定結果や鑑定履歴などを追加登録し、その後の判定に利用するなど。追加情報の一部は予備選択情報として利用することもある。

参照データ、ID、予備選択情報、及び追加情報は、必要な保護策を講じた上で、個体とともに配布することができる。

(2) 照合

照合は、個体から生成した判定対象データが、指定された個体の参照データと合致するかどうかを検証するためのトランザクションを処理する。

照合の一般的な機能には以下が含まれる。

- サンプル収集（判定対象個体の物理的特徴の読取、人工物メトリックサンプルの電子データの生成を含む）
- 判定対象データ生成（対象領域抽出、物理的特徴の抽出、品質評価（サンプル・物理的特徴が参照データ生成に適切かどうかの判定、判定の結果、不適切な場合の繰り返し登録試行要求など）を含んでもよい）
- 参照データの受入（参照データの読取、または読み取った ID に基づいてデータベース等を検索し参照データを入手）
- 照合スコア算出（受け入れた参照データと判定対象データとの適合度を比較するための照合スコアを算出）
- 照合判定（規定した閾値と照合スコアを比較し、参照データと判定対象データが合致するか否かを判定し、照合結果として出力する。照合トランザクションの方針に基づき判定対象個体の人工物メトリックサンプルの収集から繰り返すことができる）

(3) 識別

識別は、個体から生成した判定対象データが、登録されたどの個体の参照データと合致するのか（または合致する参照データが存在しないか、識別候補となる参照データ(のセット)は何か）を検証するためのトランザクションを処理する。一般的に識別の処理時間と誤識別率は登録済みの個体数、またはデータベースを検索して得られる候補リスト数の増大に応じて悪化する。そのため、それらを許容できる範囲内に登録数または候補リスト数を収める必要がある。登録数が制限される個体の種類としては例えば、限定品、有効期限のあるものなどがあり、また、データベースを検索して得られる候補リスト数を制限するための情報として予備選択情報が活用される。

識別の一般的な機能には以下が含まれる。

- サンプル収集（判定対象個体の物理的特徴の読取、人工物メトリックサンプルの電子データの生成を含む）
- 判定対象データ生成（対象領域抽出、物理的特徴の抽出、品質評価（サンプル・物理的特徴が参照データ生成に適切かどうかの判定、判定の結果、不適切な場合の繰り返し登録試行要求など）を含んでもよい）
- 予備選択情報の読取または生成（必要な場合）

- 参照データ候補リストの受入（必要に応じて予備選択情報を利用して検索し、参照データと ID のセットの候補リストを入手[3]）
- 照合スコア算出（受け入れた参照データ候補リストの各参照データと判定対象データの照合スコアを算出）
- 識別判定（規定した閾値と照合スコアを比較することで、判定対象データに合致する参照データに対応する 0 個または 1 個以上の ID 候補を選定し、識別順位を付けて識別結果として出力する。識別トランザクションの方針に基づき判定対象個体の人工物メトリックサンプルの収集から繰り返すことができる）

識別の判定方針は、①判定対象限定識別、②判定対象非限定識別 の２つに分類される。

- 判定対象限定識別
  正規の個体（登録されている個体）のみを判定対象とする識別
  - 識別対象が未登録という状況を想定しなくてもよいため、0 個の ID を返すという状況を想定しなくてもよい。
  - 識別処理により出力された ID との照合処理を行うと「提示された ID と個体とは対応しない」との結果が返る場合もある。
- 判定対象非限定識別
  正規の個体に加えて非正規の個体（未登録の個体）も判定対象とする可能性のある場合の識別
  - 識別対象が登録済みか未登録かの判定が必要
  - 提示個体の物理的特徴と最も似ていたとしても、その類似度などが、予め定められた閾値以下であればその個体の ID は返さず、提示個体を未登録と判断するなど。

なお、「判定対象限定識別」を使っている場合に未登録の個体を識別すると、その個体に最も類似している登録済みの ID が返される。そのため、未登録個体を識別する可能性の有無については慎重に判断しなければならない。

2.5. トランザクション

登録/照合/識別の各機能は、判定の方針に従い、提示と入力試行を伴うトランザクションとして実行される。

判定の方針として、複数回の入力試行を許容することもある。また、各入力試行は、品質方針等に基づき、提示の回数または入力時間を制限する設定に依存する。

[3] 予備選択情報を用いない場合は、登録されている全ての参照データが検索される。

3. 人工物メトリックシステムの評価

3.1. 人工物メトリックシステムのセキュリティ特性

(1) セキュリティ特性

ISMS（Information Security Management System）適合性認証制度で参照される国内規格 JIS Q 27000[12]、JIS Q 27001[13]では、維持すべき情報セキュリティ特性として

- 機密性（Confidentiality）
- 完全性（Integrity）
- 可用性（Availability）

が示され、さらに、

- 真正性（Authenticity）
- 責任追跡性（Accountability）
- 否認防止（Non-repudiation）
- 信頼性（Reliability）

などを含めることもあるとしている[12]。

これらのセキュリティ特性と人工物メトリックシステムとの関係は、人工物メトリクスのメカニズムとシステム全体との関係に分け、表 3-1 のように整理できる。この表が示すように、人工物メトリクスのメカニズムが実現すべきセキュリティ特性は、照合/識別の性能（精度）の確保に相当する「真正性」である。他のセキュリティ特性は、システムとの相互作用やシステム運用面からのサポートにより、目標とするセキュリティ特性を実現する。

表 3-1 人工物メトリックシステムとセキュリティ特性との関係

セキュリティ特性	人工物メトリクスのメカニズム	システム全体
機密性	*（システムの構成要素との相互作用によりメカニズムが扱う秘密情報の機密性が保護されること）*	認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しないこと（システムが扱う秘密情報（参照データ等）へのアクセス管理が適切に実行されること）
完全性	*（システムの構成要素との相互作用によりメカニズムが扱うデータの完全性が保護されること）*	システムが扱うデータの改ざんが防止・検知されること
可用性	*（照合/識別の性能（精度）が利用目的と整合し、かつ効果的であること）*	認可されたエンティティが要求したときに、アクセスおよび使用が可能であること（登録、照合/識別の各機能が実行可能であること）
真正性	**照合/識別の性能（精度）が利用目的に対して十分であること**	エンティティは、それが主張するとおりのものであること
責任追跡性	*（照合/識別の判定結果に至る動作の根拠が明確に示せること）*	システムの動作をログ等により第三者がシステム動作を検証可能であること
否認防止	*（システムの構成要素との相互作用により*	主張された事象または処置の発生、及び

	否認防止能力が提供されること）	それらを引き起こしたエンティティを証明する能力が提供されること
信頼性	*（システムの構成要素の動作特性や故障等への耐性が十分であること）*	意図するふるまいと結果とが一貫していること（セキュリティが設計通り実装され機能すること）

人工物メトリックシステムが実現すべきセキュリティを分析するためには、人工物メトリックシステムを利用する環境条件や運用方法など、いわゆる運用環境における各セキュリティ特性の侵害に至る脅威事象（保護資産の特定、及び攻撃者と攻撃方法の特定）を整理・分析し、どのような対策を講じるべきかの方針を立てることが重要である。また、整理した対策方針を、人工物メトリクスのメカニズムとシステムの各機能の仕様に落とし込むための要件と、人工物メトリックシステムをセキュアに運用するための環境に対する要件を整理し、第三者でも評価・検証が可能な方法論に則って保証することが望ましい[4]。

3.2. 人工物メトリックシステムの性能評価

人工物メトリックシステムの性能は、管理対象である個体の照合/識別の判定における各誤り率等を測定し、予め定められた基準を満たすかどうかを図示し分析する方法が有効である。このような性能評価の指標は、利用者である人の生体部位等を照合/識別の判定に利用するバイオメトリックシステムの性能評価の指標が参考となる。ここでは、人工物メトリックシステムにおける、照合、識別における指標・表示方法を示す。

なお、ここに示す指標は、原則としてシナリオ評価（実在するアプリケーションを対象システムとし、モデル化した環境において、モデル化したシナリオにより、システム全体で評価を実施）により実施した測定値から算出する。

注）人工物メトリックシステムにおける、参照データの登録失敗率、及び物理的特徴の取得失敗率は、指標からは除外している。

3.2.1. 照合の指標

(1) 参照データとの照合 1 回当たりの誤り率

- 誤合致率（誤一致率）（FMR: False Match Rate）
- 誤非合致率（誤不一致率）（FNMR: False Non-Match Rate）

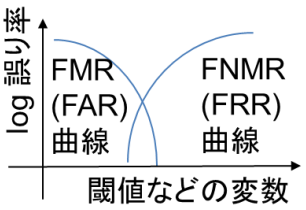
(2) システムが下す最終判定（2 回以上の照合を許す場合など）の誤り率

- 誤受入率（誤受理率）（FAR: False Accept Rate）
- 誤拒否率（FRR: False Reject Rate）

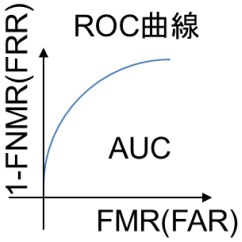
[4] より詳しい情報については付録５　人工物メトリックシステムのセキュリティ評価に関する参考情報を参照するとよい。

(3) 図示による分析

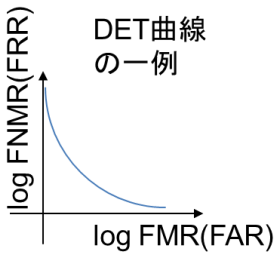
- FMR 曲線と FNMR 曲線（FAR 曲線と FRR 曲線）
  - 横軸を判定閾値とし、誤合致率と誤非合致率（誤受入率と誤拒否率）の閾値との関係を分析する際に利用する。
  - 縦軸の誤り率は対数表示を推奨。



- 照合精度特性曲線（ROC 曲線: Receiver Operating Characteristic Curve）
  - 誤合致率と誤非合致率（誤受理率と誤拒否率）を任意の判定閾値で分析する際に利用する。
  - 複数のシステムの比較や単一システムの異なる条件下での性能を分析することができる。
  - 横軸の誤り率は必要に応じて対数表示とする。
  - AUC: Area Under the Curve の計算に有用



- 検出エラートレードオフ曲線（DET 曲線: Detection Error Trade-off Curve）
  - 誤合致率と誤非合致率（誤受理率と誤拒否率）の傾向を分析する際に利用する。
  - 複数のシステムの比較や単一システムの異なる条件下での性能を分析することができる。
  - 縦軸・横軸ともに対数表示を推奨。



3.2.2. 識別の指標

(1) 出力される ID の候補数が r（識別順位が r 以内）の場合

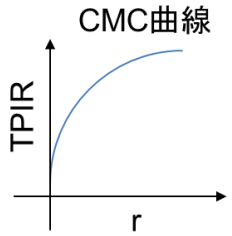
- 識別率（正受入識別率）（TPIR(r): True-Positive Identification Rate）
- 誤拒否識別率（FNIR(r): False-Negative Identification-error Rate）=1-TPIR(r)
- 誤受入識別率（FPIR: False-Positive Identification-error Rate）（判定対象非限定識別を行う場合のみ）

(2) 予備選択を行う場合

- 絞り込み率（PR: Penetration Rate）
- 予備選択誤り（PSE: Pre-Selection Error）

(3) 図示による分析

- 累積識別精度特性曲線（累積照合特性）（CMC 曲線: Cumulative Match Characteristics）
  - 判定対象限定識別において、返ってきた識別順位 r までの中に、対象が含まれるトランザクションの割合を分析する際に利用する。



- FPIR 曲線と FNIR 曲線
  - 横軸を判定閾値とし、誤受入識別率と誤拒否識別率の閾値との関係を分析する際に利用する。
  - 縦軸の誤り率は対数表示を推奨

- 照合精度特性曲線（ROC 曲線）
  - 識別率と誤受入識別率を対比させて分析する際に利用する。
  - 横軸の誤り率は必要に応じて対数表示とする。

- 検出エラートレードオフ（DET 曲線）
  - 誤拒否識別率と誤受入識別率を対比させて分析する際に利用する。
  - 縦軸・横軸ともに対数表示を推奨。

3.2.3. スループット評価

スループットは、単位時間に処理できる登録/照合/識別の各トランザクションの回数を示す。（人による操作を含めて）装置を操作することによる相互作用の開始と終了の手続きを厳密に定義し、操作と計算の全体の処理速度からスループットを計算する。

3.2.4. データの収集

人工物メトリックシステムのデータ取得処理は、物の物理的特徴を含む画像または信号を読取り、それらの参照データを生成する。性能評価をオンラインのシナリオ評価として実施する場合は、このデータ取得処理を含んだ評価を実施するが、オフラインのテクノロジ評価の場合は、読み取った物理的特徴を含む画像、信号または参照データの集合（コーパスと呼ぶ）、及びそれらのデータに関連付けられた情報（ID、追加情報、予備選択情報、アクセス権など。メタデータと呼ぶ）を予め保管しておき、性能評価の指標の計測に繰り返し利用する。コーパスとメタデータは、それぞれ収集の過程で人的誤りやその他の要因により棄損が生じる可能性があり、そのようなコーパス誤り・メタデータ誤りを回避する手段を講じる必要がある。

3.3.　人工物メトリックシステムの耐クローン性評価

本物を偽造し物理的特徴を複製したクローンを提示することで、人工物メトリックシステムの照合または識別をパスしようとする攻撃に対する耐クローン性の指標・表示方法を以下に示す。

3.3.1.　クローンの提示に対する指標

(1) 参照データとの照合 1 回当たりの一致率

- クローン一致率（CMR: Clone Match Rate）

(2) 照合システムが最終的に受け入れる率

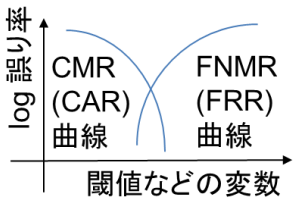
- クローン受理率（CAR: Clone Accept Rate）

(3) 識別システムが最終的に誤って受け入れる率

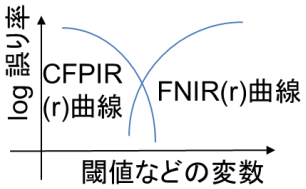
- クローン誤受入識別率（CFPIR(r): Clone False-Positive Identification-error Rate）

(4) 図示による分析

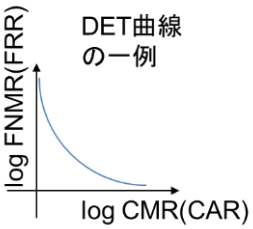
- CMR 曲線と FNMR 曲線（CAR 曲線と FRR 曲線）
  - 横軸を判定閾値とし、クローン一致率と誤非合致率（クローン受理率と誤拒否率）の閾値との関係を分析する際に利用する。
  - 縦軸の誤り率は対数表示を推奨。

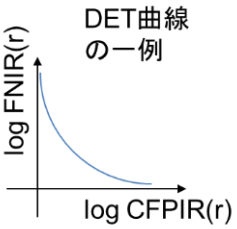


- CFPIR(r)曲線と FNIR(r)曲線
  - 横軸を判定閾値とし、クローン誤受入率と誤拒否識別率の閾値との関係を分析する際に利用する。
  - 横軸の誤り率は必要に応じて対数表示とする。



- 検出エラートレードオフ曲線（DET 曲線: Detection Error Trade-off Curve）
  - クローン一致率と誤非合致率（クローン受理率と誤拒否率）、またはクローン誤受入率と誤拒否識別率の傾向を分析する際に利用する。
  - 縦軸・横軸ともに対数表示を推奨。



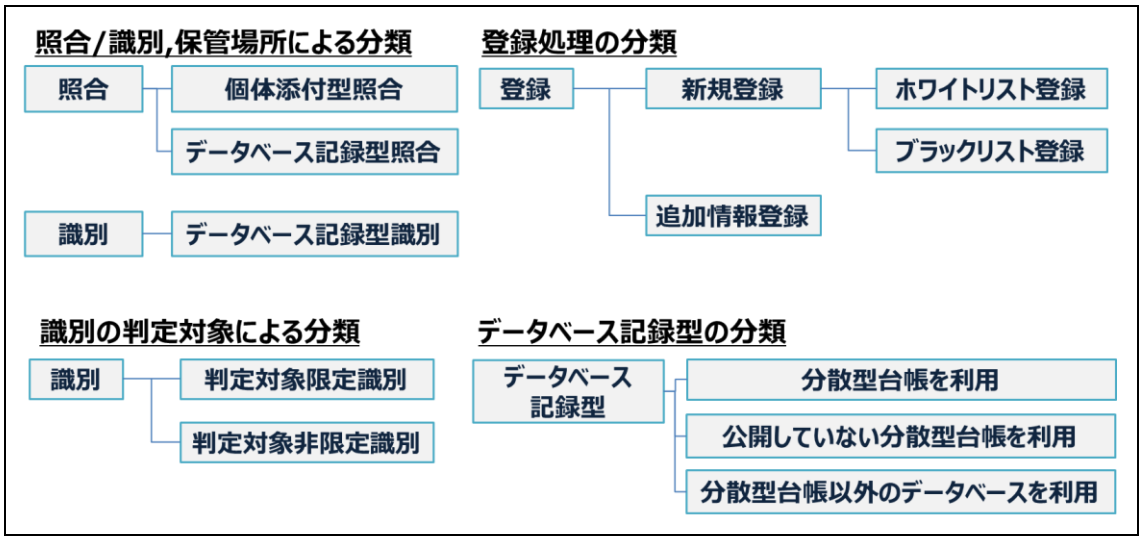


4. 人工物メトリックシステムのユースケースの分類

人工物メトリクスを用いた個体管理を実現するシステムは、利用の目的と方法、個体と物理的特徴の関係、模倣が想定される場合、利用環境の信用度、最新技術（AI など）の適用有無により、いくつかのユースケースに分類することができる。ここでは、以下に挙げる観点でユースケースの分類を試み、各ユースケースにおける注意点を示す。

- 照合/識別及び参照データの保管場所による分類
- 個体と物理的特徴との関係による分類
- 判定対象の集合の範囲による分類
- データ取得処理の信用度による分類
- AI（機械学習）使用の有無による分類
- 利用する方法が１つ/複数の場合による分類

4.1. 照合/識別及び参照データの保管場所による分類



上記の分類図の左上及び 2.1 節の「(2) 照合と識別」のとおり、人工物メトリックシステムは、判定処理として照合/識別のいずれを行うのか及び参照データの保管場所により、「個体添付型照合」、「データベース記録型照合」、「データベース記録型識別」の３種類に分類できる。これらの詳細を後段に示し、その各図中のオレンジ色の網掛けボックスにおいて、いくつかのユースケース分類や関連情報との関係を示す。さらに、データベース記録型は、「分散型台帳（公開、非公開）を利用するタイプ」と「それ以外のデータベースを利用するタイプ」に分類でき、登録処理については、2.4 節の「(1)登録」のとおり「新規登録（ホワイトリスト登録、ブラックリスト登録)」と「追加情報登録」に、識別の判定対象は、2.4 節の「(3)識別」のとおり「判定対象限定識別」と「判定対象非限定識別」に分類できる。

4.1.1. 個体添付型照合

参照データを個体と共に配布し、照合処理（1 対 1 照合）を行うケースである[5]。照合処理のデータ取得処理サブシステムは、個体の物理的特徴の読取りに加え、個体と共に配付された参照データの読取りを行う。参照データが改ざんされる危険性がある場合には、参照データに電子署名またはメッセージ認証子などを付加し、それらに対応する改ざん検出鍵（前者は電子署名検証鍵、後者はメッセージ認証子検証鍵など）を照合処理に持たせる必要がある。また、個体に添付された参照データを入手すれば物理的特徴を模倣し易くなる場合、参照データを暗号し、その復号鍵も照合処理に持たせる必要がある。

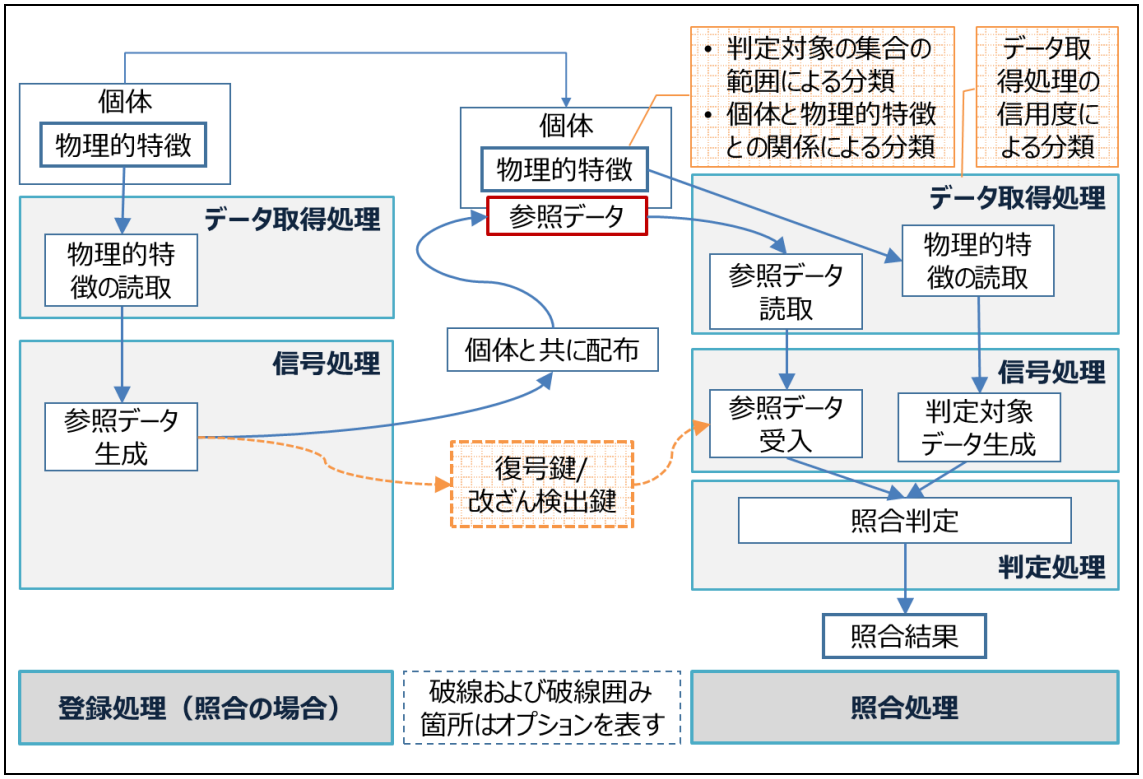


図 4-1 個体添付型照合の流れと分類との関係

4.1.2. データベース記録型照合

登録処理（照合の場合）で生成した参照データとこれを識別するための ID をデータベースに格納する。また、ID は個体と共に配布する。照合処理では、読み取った ID を使ってデータベースを検索し、ID に紐付く参照データを取り出し、照合判定を行う。データベース

[5]添付された参照データに対応する個体が明確な場合には識別処理（1 対 N 照合）は不要であるが、対応が（例えば、流通過程などにおいて）不明確になった場合には識別処理（1 対 N 照合）を行うことも可能である。また、ID を必要とする場合には、参照データに ID を含めておき、個体添付型照合が受理された後に、その ID を出力することも可能である。

に格納された参照データを入手すれば物理的特徴を模倣し易くなる場合、参照データを保護する必要がある。一般的には、暗号化とアクセス制御による技術的な対策に加え、アクセス権限/復号権限の安全な受け渡し手続きなどによる対応が求められる。

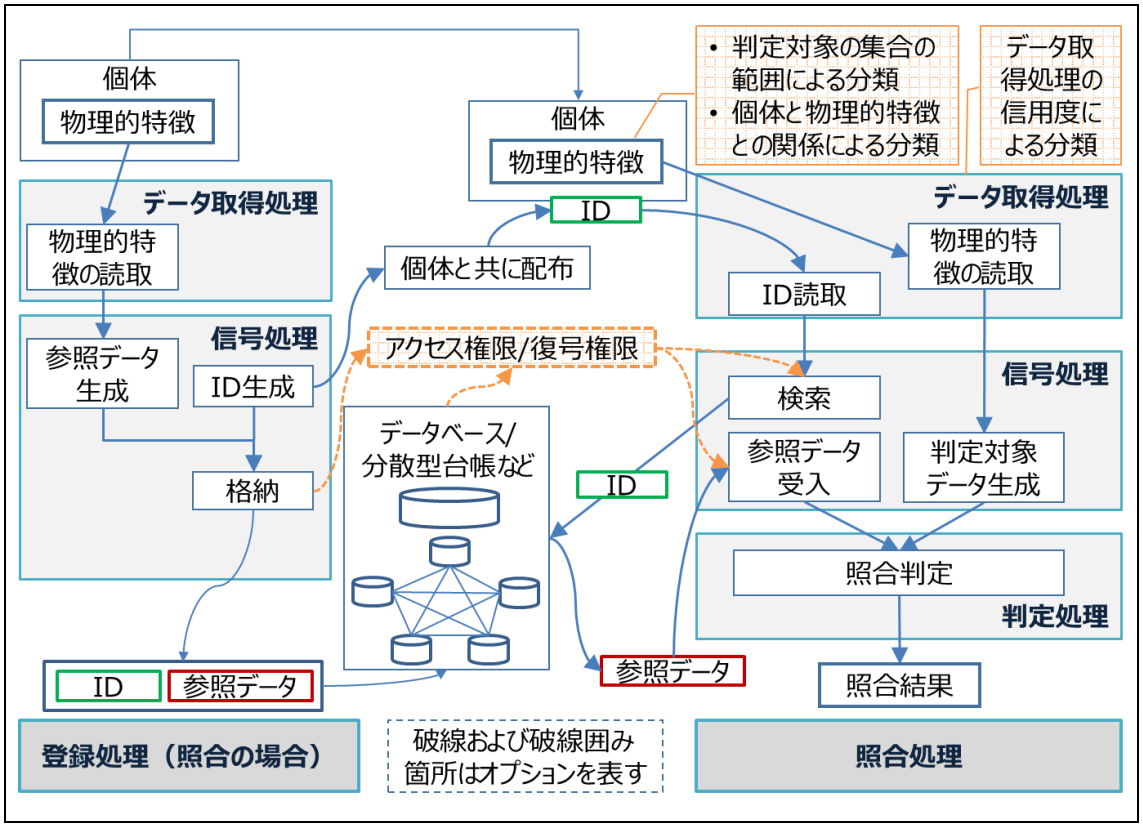


図 4-2 データベース記録型照合の流れと分類との関係

4.1.3. データベース記録型識別

登録処理（照合の場合）で生成した参照データとこれを識別するための ID をデータベースに格納する。識別処理では、個体の物理的特徴を読取り、判定対象データを生成し、データベースから取り出した参照データと順次照合を行い、識別の方針に従い 0 個または 1 個以上の ID 候補を選定し、識別順位を付けて識別結果を出力する。識別処理において、照合する参照データを絞り込むために、予備選択情報を適用することができる。予備選択情報は、予め記載されている予備選択情報を個体と共に配布する場合、登録処理（識別の場合）と識別処理共に同様の方法で、取得した物理的特徴から予備選択情報を生成する場合などがある。

データベースに格納された参照データを入手すれば物理的特徴を模倣し易くなる場合、参照データを保護する必要がある。一般的には、暗号化とアクセス制御による技術的な対策に加え、アクセス権限/復号権限の安全な受け渡し手続きなどによる対応が求められる。

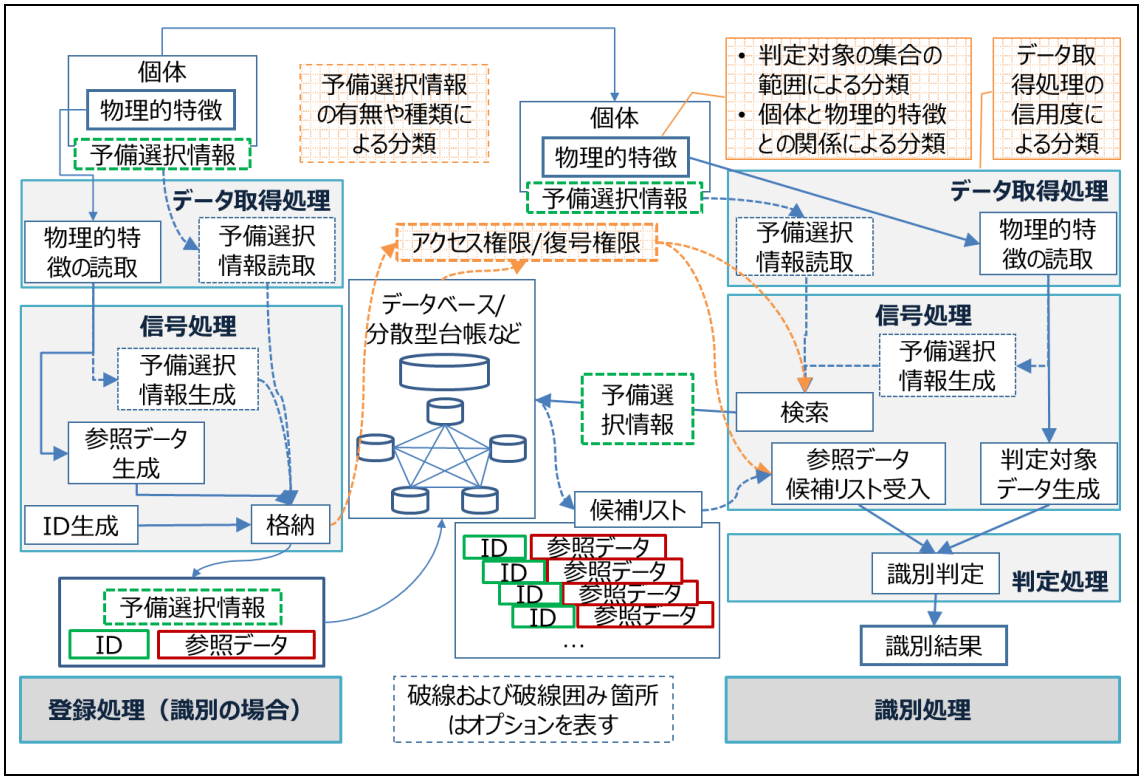


図 4-3 データベース記録型識別の流れと分類との関係

4.1.4. 照合/識別に関連する注意点

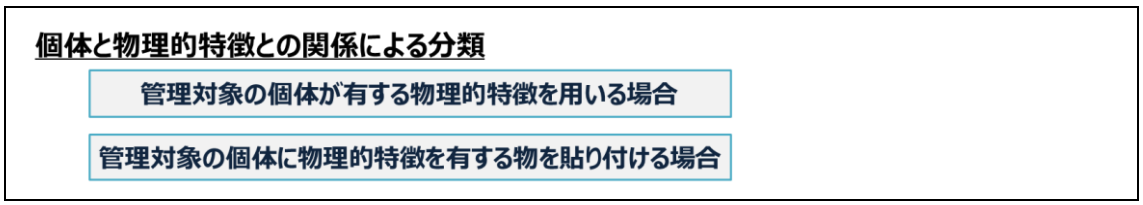
(1) 参照データの保管場所に伴う注意点

参照データは、個体添付型（照合の場合）では、個体と共に配布するのに対し、データベース記録型では３つのケース（①公開分散型台帳を利用する場合、②公開していない分散型台帳を利用する場合、③分散型台帳以外のデータベースを利用する場合）に分類できる。それぞれのケースに伴う注意点を示す。

- 個体添付型
  - ✧ 参照データの中身の完全性を確保するために電子署名、メッセージ認証子などの付加が重要（ただし、付加後も、参照データ毎の削除、差替、複製の追加は可能となる）
  - ✧ 参照データを攻撃者が入手できれば物理的特徴を模倣しやすくなる場合には、秘匿性の確保と信頼できるエンティティ（信頼できる利用者/管理者など）のみへアクセス権限や復号権限を付与することが重要
- データベース記録型
  - ➢ 公開分散型台帳を利用する場合
    - ✧ 参照データを攻撃者が入手できれば物理的特徴を模倣しやすくなる場合には、秘匿性の確保と信頼できるエンティティ（信頼できる利用者/管理者など）のみへアクセス権限や復号権限を付与することが重要

- 公開していない分散型台帳を利用する場合
  - 盗聴、改ざん、なりすましの行われる可能性のある通信路を経由して利用する場合には利用者認証と通信路の保護が重要
- 分散型台帳以外のデータベースを利用する場合
  - データベースへの不正(書替等)を想定する場合、完全性と可用性の確保が重要
  - 盗聴、改ざん、なりすましの行われる可能性のある通信路を経由して利用する場合には相互認証（利用者認証、サーバ認証）と通信路の保護が重要

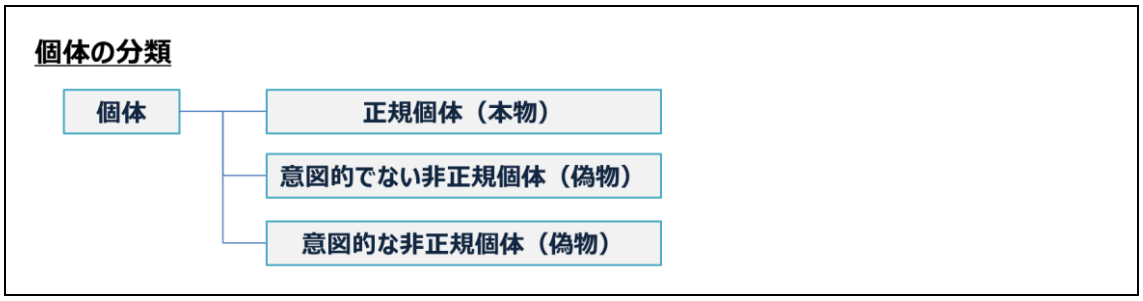
4.2.　個体と物理的特徴との関係による分類



人工物メトリックシステムの管理対象の個体が有する物理的特徴を用いる場合に対し、管理対象の個体に物理的特徴を有する物を貼り付けるケースでは、貼り替え防止のための貼付け強度の確保、貼り替え検出のためのタンパーエビデンスの確保などの対策が必要となる。

4.3.　判定対象の集合の範囲による分類

(1) 個体の分類



人工物メトリックシステムが扱う個体は、①正規個体（本物）、②意図的でない非正規個体（偽物）、③意図的な非正規個体（偽物）に分類される。登録に対する不正・攻撃・エラーを想定しない場合、図 4-4 上部のとおり①のみがホワイトリスト登録され、②、③はホワイトリスト登録されていない状態となる。一方、登録に対する不正・攻撃・エラーを想定する場合、①であってもホワイトリスト登録されていない状態、②、③であってもホワイトリスト登録されている状態についても考慮する必要がある。

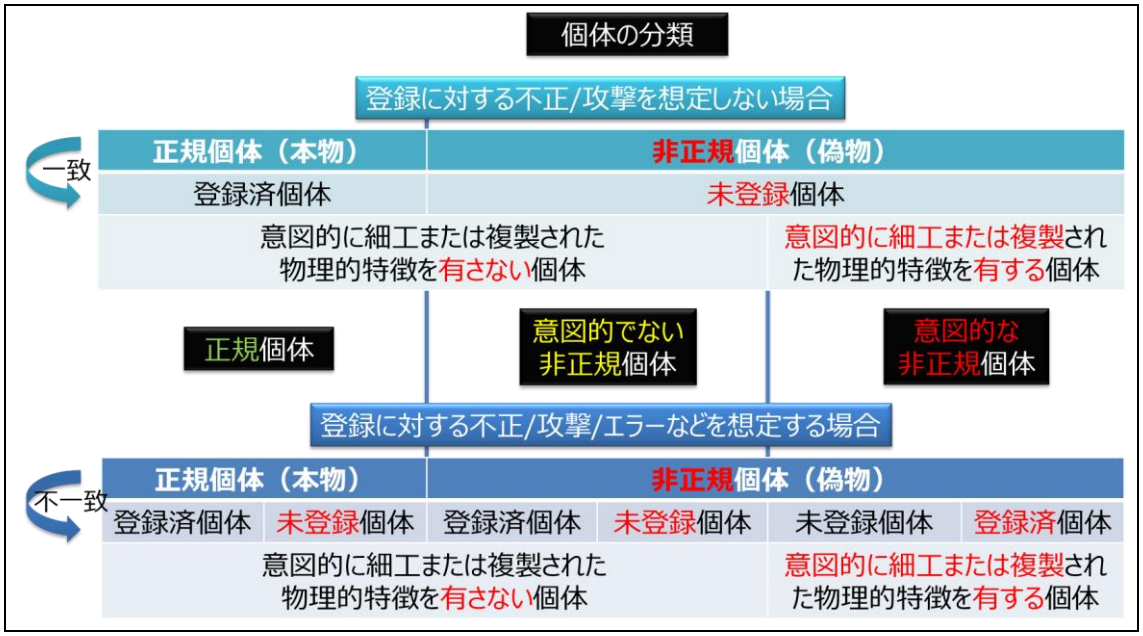


図 4-4 判定対象の集合の範囲の分類

また、登録処理やデータベースの信頼性やセキュリティ対策が十分であり、登録に対する不正・攻撃・エラーを想定しない場合においても、判定対象とする個体の種類に応じて考慮しなければならないセキュリティ要件や用いるべき指標が異なるため注意が必要である。具体的には、②、③を判定対象とする場合はブルート・フォース攻撃、③を判定対象とする場合はデッド・コピー/ハード・コピー攻撃、ウルフ攻撃、シミュレート攻撃などへの耐性が必要となる。逆に、判定対象を①のみとする用途では上記攻撃への耐性は不要であり、①と②のみを判定対象とする用途では③への攻撃耐性は不要となる。

判定対象を①のみとする用途の例としては以下のような場合がある。

- 個体紛失の有無のみを検出できればよく、紛失した事実の偽装が行われない場合の例
  - 工場などの管理された区画内において、事故等により製造ラインから落ちたり滞留したりした個体が無いことを監視する場合など。具体的手法としては、ある時点において、管理個体の ID（参照データ添付型の場合には参照データのハッシュ値を ID として）一覧表を作成しておき、その後、手元にあるすべての個体の判定を行い、識別処理の場合には判定対象限定識別を用いて得られた ID、照合処理の場合には照合された ID を、前述の一覧表の ID と突き合わせ、突き合わせが行われなかった ID に対応する個体を紛失していると判断するなど[6]

また、①と②のみを判定対象とする用途としては以下のような例がある。

- 意図的でない非正規個体の混入の有無を検出する場合の例

[6] なお、突き合わせ一覧表にない ID が得られた場合は混入ともなる。

- 照合処理の場合
  - 正規個体（製品・商品）に対してシール、パッケージ、鑑定書等により付与されている ID が、製造過程・流通経路の途中で入れ替わっていないことを、照合処理により検出するなど[7]
- 識別処理の場合
  - 工場などの管理された区画内において、管理対象である高品位部品の集合に、別のラインなどで生産された低品位の部品が混入していないか判定対象非限定識別を用いて検出するなど

(2) 照合における判定対象の集合と指標

照合の対象として、①正規個体のみ、②意図的でない非正規個体も対象に追加、③さらに意図的な非正規個体も対象に追加 とする場合の判定対象の集合、及び推奨する照合の指標を 図 4-5 に示す。

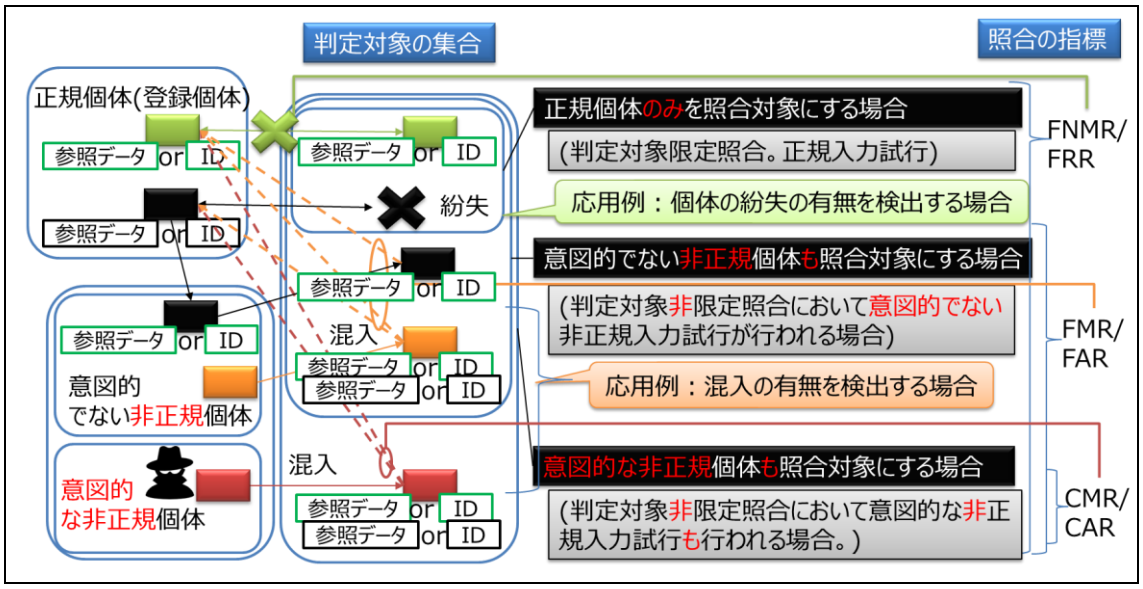


図 4-5 判定対象の集合の範囲による分類：照合の場合

(3) 識別における判定対象の集合と指標

識別の対象として、①正規個体のみ、②意図的でない非正規個体も対象に追加、③さらに意図的な非正規個体も対象に追加 とする場合の判定対象の集合、及び推奨する識別の指標を 図 4-6 に示す。

[7] 照合処理では ID（または参照データ）との組み合わせが正しくなくなった時点でその個体は非正規個体となるため、非正規個体が混入している状態となる。

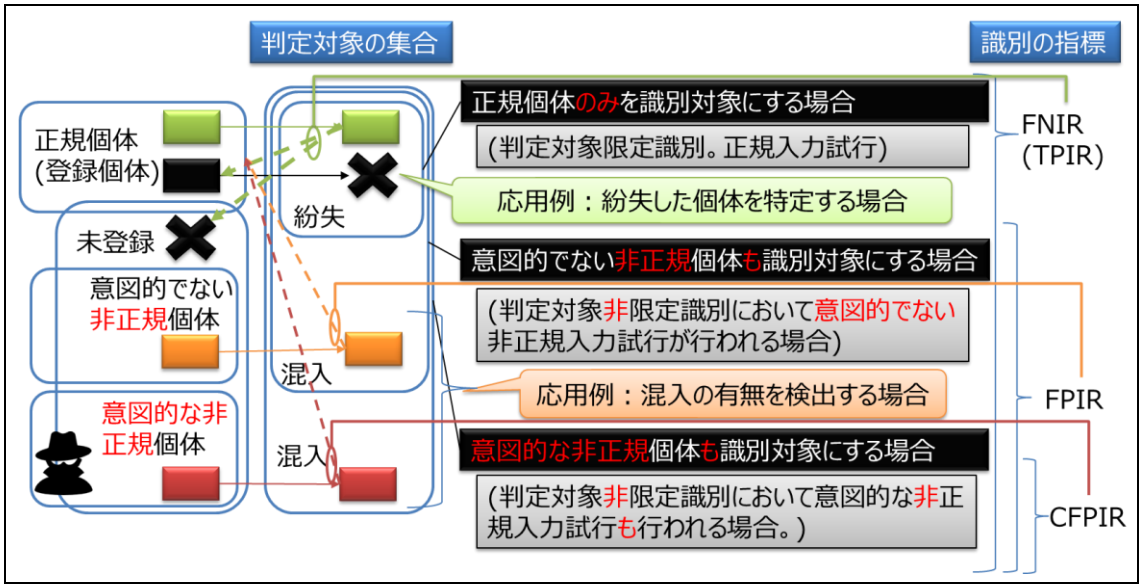


図 4-6 判定対象の集合の範囲による分類：識別の場合

(4) 識別かつ個体と共に予備選択情報が配布される場合の判定対象の集合と指標

個体と共に識別のための予備選択情報が配布される場合、非正規個体と共に配布される予備選択情報にも改ざん、貼り替えが行われていることを想定する必要がある。意図的な非正規個体を想定した性能評価では、予備選択情報の貼り替え防止・検知のメカニズムも含めた評価が求められる。判定対象の集合及び推奨する照合の指標については、識別の場合と同様である（ 図 4-7 を参照）。

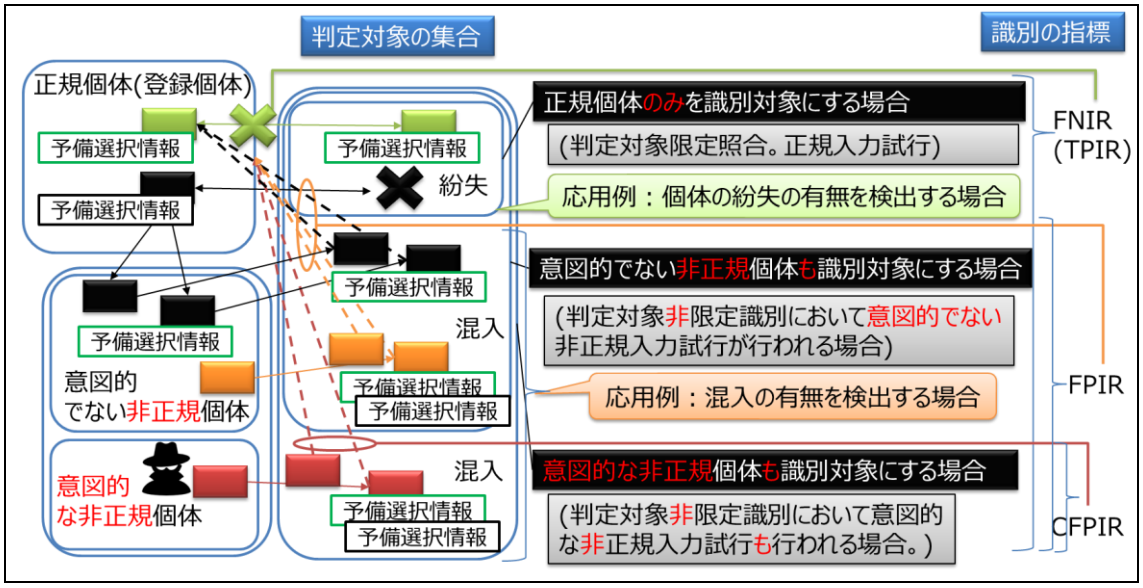


図 4-7 判定対象の集合の範囲による分類：識別かつ個体と共に予備選択情報が配布される場合

4.4.　データ取得処理の信用度による分類

データ取得処理の信用度による分類

悪意はなく、または意図的でないが信用度が低くなる場合

意図的または悪意により信用度が低くなる場合

人工物メトリックシステムのデータ取得処理は、センサを搭載する読取装置で実行される。読取装置の信頼性や動作環境や操作者の信用度の違いにより、取得データの品質の劣化、不正なデータの取得などが想定される。

- 悪意はなく、または意図的でないが信用度が低くなる場合
  例えば、未熟練者が操作することによる取得データの劣化、データ取得環境の違いによる取得データの劣化など
  - 操作者の熟練度、装置や環境の違いに対する取得データの品質確保が重要
  - 個体の物理的特徴をカメラで取得する場合に対しては、カメラスペックや撮影環境の違いを抑えるために考慮すべき項目を付録２，３にまとめてある。
- 意図的または悪意により信用度が低くなる場合
  例えば、必ずしも信用できるとは限らない場所において、必ずしも信用できるとは限らないデータ取得装置で取得されたデータを用いて判定等を行う場合などでは、リプレイ攻撃リスクが高くなるほか、質の悪い模倣品（物理的特徴を複写機でコピーしただけのものなど）、シミュレート攻撃により生成されたものや電子データなどの受け入れリスクが高くなる。
  - 読取装置に電子データを直接流し込めなくするための耐タンパー性の確保及び対象が間違いなく読み取られていることの確認などが重要

4.5.　AI（機械学習）使用の有無による分類

ここでは、人工物メトリックシステムの照合または識別メカニズムに AI（機械学習）を適用する場合の注意点を示す。なお、ここでの AI は、必要となる学習済みモデルをデータセットから自動的に生成する場合を対象とし、例えば、ルールを人が確認しながら生成するルールベース AI などは対象外とする。

以下に、AI（機械学習）を適用する人工物メトリックシステムの各フェーズにおいて想定される攻撃を示す。なお、攻撃の名称は「機械学習品質マネジメントガイドライン 第 2 版 (revision 2.1.0)」[16]（以下、AIQM と呼ぶ）を参考にしている。

- 機械学習用データセット入手時/機械学習時
  - データポイズニング攻撃（データセット改ざん/追加/削除）
    - 正規個体データの削除/教師ラベル改ざん

- ✧ 正規個体データへのバックドア型ポイズニング攻撃
- ✧ 非正規個体の訓練データ追加

➢ 正規個体データの漏洩

- 学習済みモデル管理時
  - ➢ モデルポイズニング攻撃
  - ➢ モデル情報の漏洩
- 照合/識別時
  - ➢ 学習済みモデルへの（大量）問い合わせ
  - ➢ AI が受け入れる非正規個体の提示

(1) 機械学習への汎用的な攻撃方法による影響

人工物メトリクスを用いた個体管理に影響を及ぼす可能性のある機械学習への汎用的な攻撃方法について、影響度合いとその条件、理由等を 表 4-1 に示す。

表 4-1 機械学習への汎用的な攻撃方法と人工物メトリクスを用いた個体管理との関連

機械学習への汎用的な攻撃方法	攻撃方法の説明	人工物メトリクスを用いた個体管理との関連（条件、理由等）
データポイズニング攻撃	機械学習に用いるデータセットに意図的な改変を加える攻撃	大
バックドア型データポイズニング攻撃	特定の入力に対してのみ機能するようなデータポイズニング攻撃	大
モデルポイズニング攻撃	訓練済みモデルに対して不正な動作などを埋め込む攻撃	大
モデル抽出攻撃	運用時に、入力データに対する出力の振る舞いを観察することで、訓練済みモデルと同様の動作をするモデルを抽出する攻撃	中（照合が受理される、または、正しい ID に識別される入力を特定することが本質で、訓練済みモデルと同様の動作をするモデルを抽出する必要は無いため）
回避攻撃（敵対的データ）	運用時に機械学習利用システムに特定の改変した入力（敵対的データ）を与えることで、機械学習要素に想定外の誤動作を生じさせる攻撃	中（照合が受理される、または、正しい ID に識別される入力を行うことが本質で、人の解釈を保持する範囲に限定される敵対的データの入力に拘る必要は無いため）
解釈/説明機能を誤動作させる攻撃	敵対的データなどを用いて AI の解釈/説明機能によって出力される説明内容の価値を下げたり、間違った説明を生成したりする攻撃	
メンバシップ推測攻撃・モデルインバージョン攻撃・性質推測攻撃	機械学習に用いたデータセットについての情報を摂取する攻撃	小（通常、機械学習に用いるデータセットに個人情報やプライバシに関連する情報は含まれていないため）

なお、敵対的データ（adversarial example）の作成は、「照合が受理される、または正しい ID に識別される入力の把握」とその範囲内の非正規個体を作成できるかが重要となる。

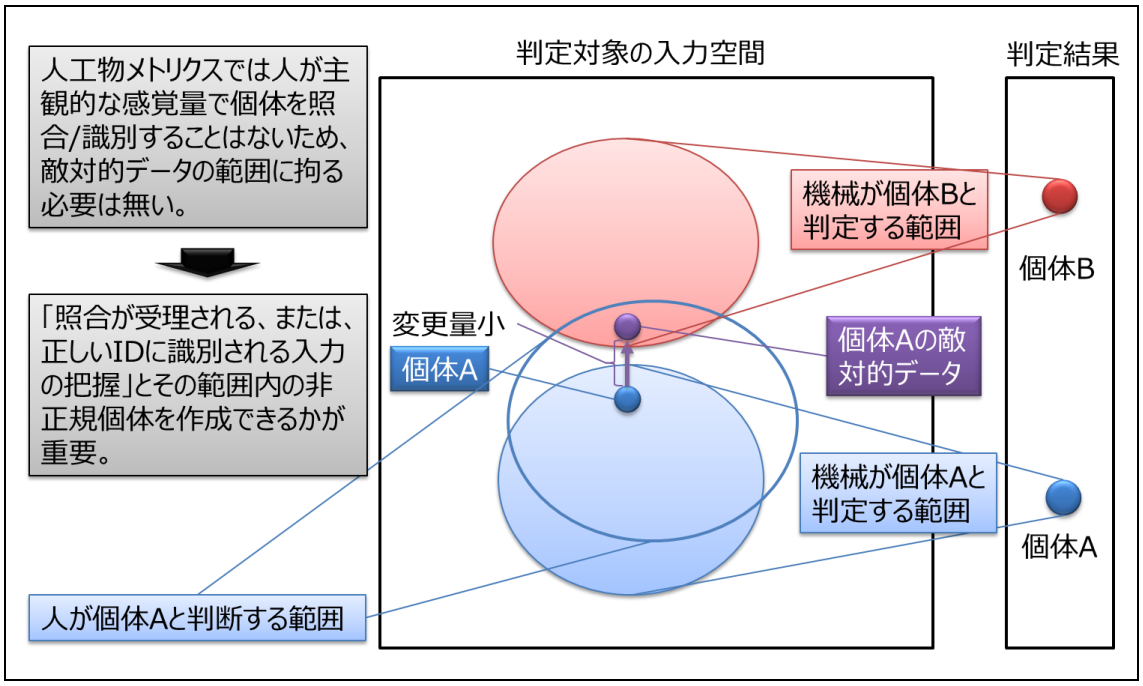
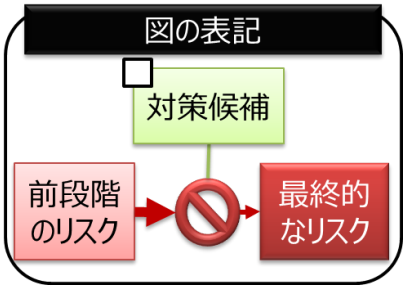


図 4-8 敵対的データとの関係

(2) 対策候補とリスクへの影響

AI を適用する人工物メトリックシステムにおいて、適用する学習済みモデルを訓練データから自動的に生成する場合の各フェーズで想定される攻撃への対策候補により、リスクがどのように変化するのか（残存するリスクがどの指標によって分析できるか）を 図 4-9 にまとめる（この図の表記法は右の通り）。



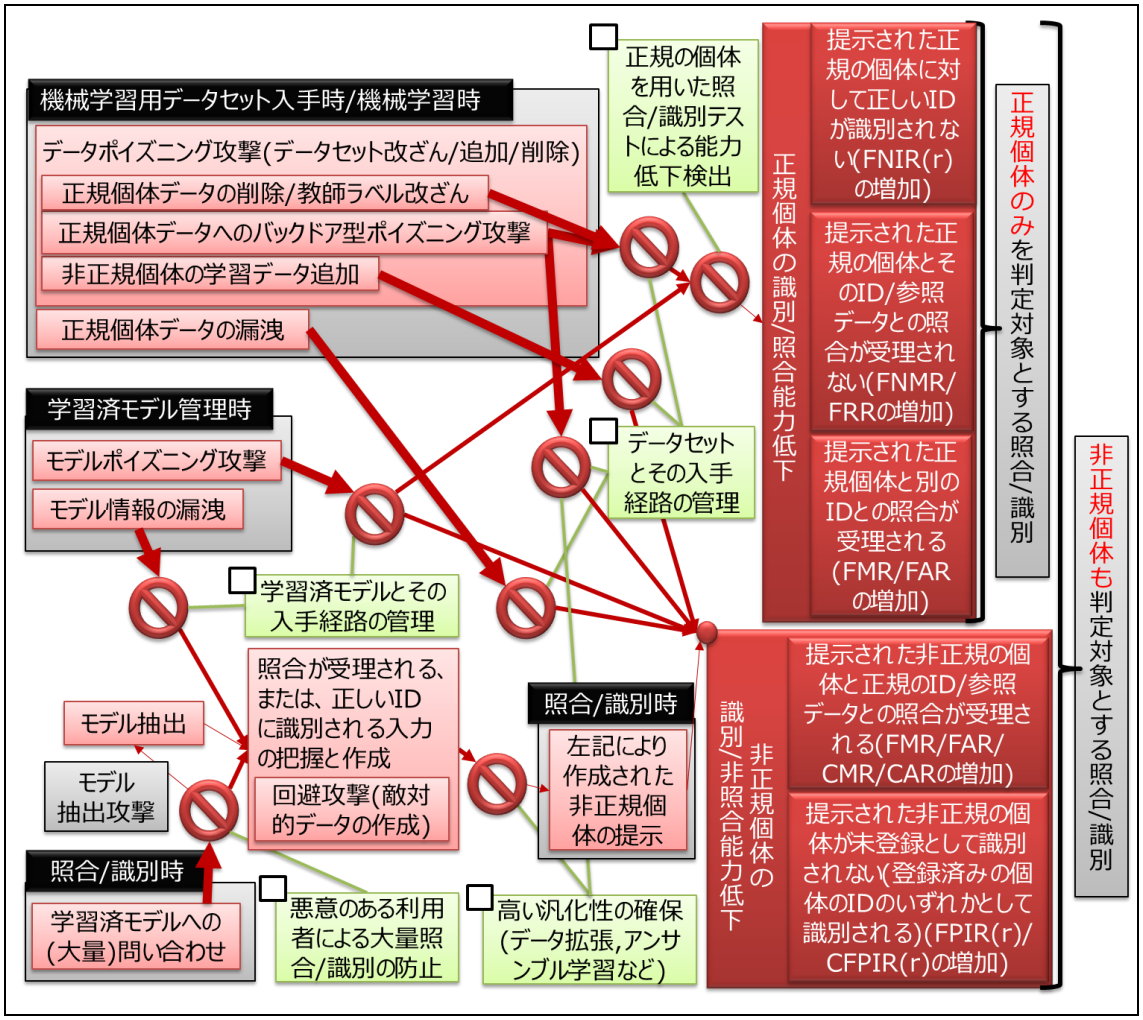


図 4-9 学習済みモデル生成の各フェーズのリスク・対策候補・指標の関係

(3) 機械学習モデル構築における学習用データの構成

機械学習モデルが、人工物メトリックシステムの処理内の特定の機能（単独または複数）に適用される場合、機械学習モデルの予測/分類性能は、人工物メトリックシステムの性能特性に影響を与える。機械学習モデル構築時の学習用データ（訓練データ、教師ラベル、検証（バリデーション）データ、評価（テスト）データなど）を構成する際に、収集するコーパスやメタデータが学習用データとして利用され、これらのデータの誤りが学習用データを介してそのモデルの性能に影響を与える場合、性能評価に利用するコーパスやメタデータの誤り回避に準じる手段が求められる。そのうえで、機械学習モデル構築の目的に適した学習用データの構成とすることが望ましい。

AIQM は、学習用データ構成フェーズにおいて、データセットの生成と使用法の計画化までのステップを、以下のように定義している。

表 4-2 機械学習モデル構築における学習用データの構成ステップ

ステップ	概要
1. データセット設計・調整ステップ	未加工の生データセットの生成、前処理用プログラムの作成
2. 訓練用前処理ステップ	生データセットを訓練に適したデータセットに加工（以下の各処理を実施。目的に応じて、各処理を順不同、並列、繰り返し実施）。
データ選別	データセットの被覆性、均一性を考慮して訓練と評価のデータを選別。
データクリーニング	ノイズ除去、データ整形、欠損値補完、外れ値除去
データ拡張	データ数確保・過学習防止のためのデータ生成・追加
ラベル付加	正解（教師用）のラベル付け
特徴抽出・選択	有用な特徴量の抽出・付加、不要な特徴量の選択・削減
3. データ準備ステップ	データセットの使用法の計画化（訓練用、検証（バリデーション）用、評価（テスト）用の分離、または各用途での使用と入れ替えの計画など）

(4) 機械学習モデル構築における反復訓練

機械学習モデルの訓練に必要なハイパーパラメータを設定し、データセットを用いて訓練と検証（バリデーション）を繰り返し実施しながらハイパーパラメータを調整することで、実装用学習モデル（学習済みモデル）としてのパラメータを獲得する。

AIQM は、反復訓練フェーズにおいて、反復訓練により実装用学習モデルの生成までのステップを、以下のように定義している。

表 4-3 機械学習モデル構築における反復訓練ステップ

ステップ	概要
1. モデル設計・調整ステップ	ハイパーパラメータの設計、訓練用プログラムの作成、バリデーション・テスト後のハイパーパラメータの調整
2. 訓練ステップ	訓練用のデータセットを使用して機械学習モデルを訓練。
3. バリデーションステップ	バリデーション用のデータセットを使用して学習モデルの評価指標によりモデルを評価。 複数のハイパーパラメータで複数の機械学習モデルを訓練し、相対的に評価して妥当性を判断。
4. 後処理ステップ	実運用環境に合わせるためのモデル変換等により、実装用学習モデルを生成。 注）システム全体の構築の一部として後処理ステップを実施する場合、反復訓練後の品質確認・検証段階における品質との数値的同等性の確認、及びシステム全体の検証段階における再検証が必要となることを想定。
モデル変換	計算精度の変更、モデルの圧縮・高速化
モデル最適化	推論の効率化（モデルのコンパイル（並列化、ベクトル化など））

学習用データによる学習の効果を観察しながら反復訓練を進める手順は以下の通り。

- データセットから、訓練データと検証（バリデーション）データのサブセットを任意に選択し、機械学習モデルの訓練と検証（バリデーション）を繰り返しながら、学習曲線（Training Error）とバリデーション曲線（Validation Error）を分析し、学習曲線に対するバリデーション曲線の乖離の傾向（過学習の傾向）を観察する。

- 必要に応じて過学習を抑制するハイパーパラメータを調整し上記を繰り返す。
- 過学習に至らない学習回数をハイパーパラメータとして、K-分割交差検証（K-fold cross-validation）により、機械学習モデルの反復訓練をやり直す。

ハイパーパラメータの主な調整方法（探索方法）は以下の通り。

- 手動による調整
- グリッドサーチ（Grid Search）
- ランダムサーチ（Random Search）
- ベイズ最適化（Bayesian Optimization）

なお、反復訓練、及びハイパーパラメータの調整は、どの程度の汎化能力を持たせるかなど、具体的な状況に応じた試行錯誤や主観的な判断によるところが大きいことに留意する必要がある。

(5) 機械学習モデルの正確性・安定性の検査

機械学習モデルの正確性・安定性の検査は、一般的にはソフトウェア開発における単体テストに位置付けられる。検査は、訓練学習プログラムと予測・推論プログラム（学習済みモデルが機能の振る舞いを定めているもの）のそれぞれを対象とする。訓練学習プログラムはその学習済みモデルの安定性に対する正解値を予め知ることが困難であること、また予測・推論プログラムの出力は確定的ではなく確からしさを伴う相対的な値であることから、これらのプログラムは、学習データに含まれていない入力データに対する出力の期待値を確定的に定義することが難しく、テスト不可能プログラムに分類される。予測・推論プログラムに関しては、テスト時補完（テスト時に多様なデータを補完したり、敵対生成ネットワーク（GAN: Generative Adversarial Network）によるデータ生成法と組み合わせたりする方法）などの手法を適用し、モデルの正確性・安定性を評価する。

AIQM は、各フェーズ（①反復訓練、②品質確認・検証、③品質管理・運用）に適用可能な、機械学習モデルの安定性の評価と向上に関する以下の技術を紹介している。

- 交差検定（cross validation）
- 正則化（regularization）
- 敵対的データ生成（adversarial example generation）
- 最大安全半径（maximum safe radius）
- 汎化誤差上界（generalization error bound）
- 敵対的訓練/ロバスト訓練（adversarial training / robust training）
- ランダムスムージング（randomized smoothing）
- 敵対的データ検知（adversarial example detection）

4.6.　利用する方法が１つ/複数の場合による分類

人工物メトリックシステムが単一の目的で利用される場合、データ取得のための読取装置のセンサ（カメラなど）の切り替えは不要である。一方、複数の利用目的・利用方式への対応を要するシステムの場合（例えば、税関、個人間売買など）、個体管理方式に応じて、データ取得のための読取装置のセンサ（カメラなど）の切り替えが必要となることが想定され、この切り替えの負荷を低減することが将来的に求められる可能性がある。読取装置のセンサとしてカメラを用いる場合に、そのスペックを揃えるために検討すべき項目の候補を付録２にまとめてある。

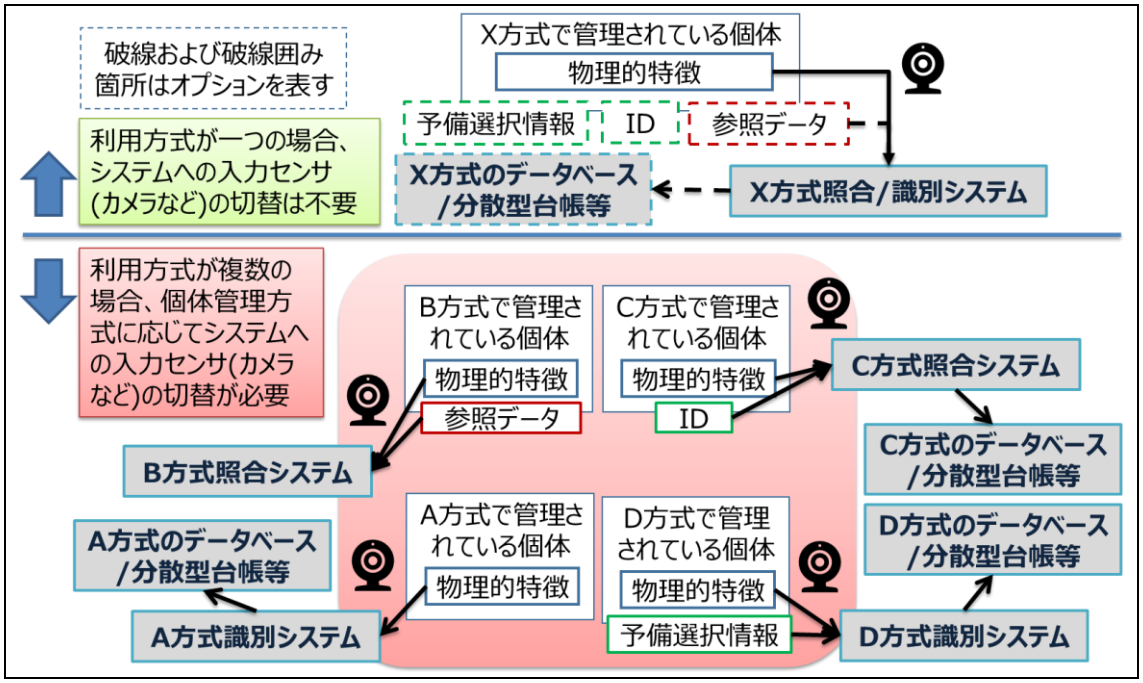


図　4-10 利用方式が１つの場合と複数の場合における入力センサの切り替え有無

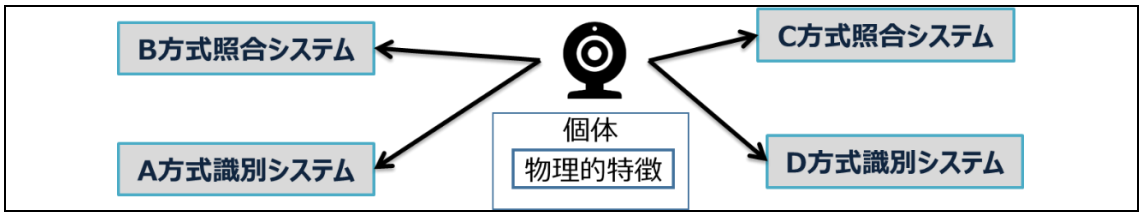


図　4-11 入力センサの共通化

付録

付録１　用語と定義

用　語		説　明
全般		
	人工物メトリクス	物の物理的特徴の計測または測定
	人工物メトリクスを用いた個体管理技術	個体の物理的特徴の測定結果を照合または識別することによる管理技術
	計測	特定の目的をもって、測定の方法及び手段を考究し、実施し、その結果を用いて所期の目的を達成させること
	測定	ある量をそれと同じ種類の量の測定単位と比較して、その量の値を実験的に得るプロセス
	コーパス データセット	対象となるデータを大規模に集めてデータベース化した資料 注記：人工物メトリクスの場合、物理的特徴の電子データが「対象となるデータ」に該当する。
	シナリオ評価	テストのために用意した個体（物理的特徴を含む）を対象とし、プロトタイプまたは模擬的なアプリケーションを使用して、包括的なシステム性能を判定する評価
	テクノロジ評価	既存のサンプル、または特別に収集したサンプルのコーパスを用い、システムの一部を構成する技術やアルゴリズムの性能を判定する評価
ユースケース		
	個体	個々独立に他の物とその存在を区別して認識されるもの
	物理的	一般に、空間・時間・重量など、数量に置き換えられる条件に関連するさま
	特徴	他と比べて特に目立ったり、他との区別に役立ったりする点
	物理的特徴	（主観的な感覚量ではなく）客観的な数量に置き換えられる特徴
	参照データ	登録時に個体から抽出した物理的特徴に基づいて生成され判定時に参照されるデータ
	判定対象データ	判定対象の個体から抽出した物理的特徴に基づいて生成された判定に用いるデータ
	ID 参照データ ID	生成した参照データをユニークに特定するための識別子 注記：本識別子には、URI(Uniform Resource Identifier)、URL、アドレスなども含まれる。

用　語	説　明
予備選択情報	データベース/分散型台帳などの検索において、結果となる参照データの数を減らすための情報
候補リスト	予備選択情報を用いてデータベース/分散型台帳などを検索することにより得られた参照データの集合
アクセス権限	対象（データベース/分散型台帳など）を使用するための権限
復号権限	データベース/分散型台帳に格納された、暗号化されたデータを復号するための権限
読取	センサや入力装置によりデータを取得すること
生成	定義された手続きによりデータを生成すること
受入	読取または検索により取得したデータを、正当なデータとして信号処理内部に受け入れること
検索	ID または予備選択情報に紐づくデータを検索すること
判定（処理）	システムにおいて照合/識別要求の正当性を確度高く判定すること
格納	生成したデータを、データベース/分散型台帳などに格納すること
保存	データを、データベース/分散型台帳などに保存すること
登録（処理）	個体から抽出した物理的特徴に基づいて参照データを生成し、生成した参照データを抽出した個体に紐づけて管理すること
照合（処理） 1 対 1 照合	提示された ID または参照データと個体とが対応するか否かを返すアプリケーション
識別（処理） 1 対 N 照合	提示された個体に対応する 0 個または 1 個以上の ID の候補を識別順位を付けて返すアプリケーション
データ取得（処理）	個体の物理的特徴、及び個体に付与された参照データや ID を取得すること
信号処理	取得したデータから、必要に応じて個体固有の特徴を抽出したり、抽出した特徴の品質を評価したりするなどの処理を行うこと。登録処理では、抽出した特徴から参照データを生成する。
個体添付型照合、個体記録型照合	参照データが個体と共に配布される照合（処理）
データベース記録型照合/識別	参照データがデータベース/分散型台帳などに格納される照合（処理）/識別（処理）
正規の個体 正規個体	本来登録されるべき個体（攻撃により登録されない場合もある）
非正規の個体 非正規個体	本来登録されるべきでない個体（攻撃により登録される場合もある）

用　語		説　明
	意図的でない非正規個体	意図的に細工または複製された物理的特徴を有さない非正規個体
	意図的な非正規個体	意図的に細工または複製された物理的特徴を有する非正規個体 注記：意図的な非正規個体の内、複製により作成されたものをクローン、なるべく多くの参照データと照合または識別されるように複製または意図的に細工されたものをウルフとよぶ。
	判定対象限定照合/識別	正規の個体のみを判定対象とする照合/識別 注記：登録に対する不正や攻撃を想定しない場合には登録個体限定照合/識別と同じ
	判定対象非限定照合/識別	正規の個体のみを判定対象とするとは限らない照合/識別 注記：登録に対する不正や攻撃を想定しない場合には登録個体非限定照合/識別と同じ
	登録個体限定照合/識別	登録個体のみを判定対象とする照合/識別
	登録個体非限定照合/識別	登録個体のみを判定対象とするとは限らない照合/識別
	トランザクション	個体の登録、照合または識別を目的とした利用者による一連の入力試行 注記：トランザクションには、次の３つの種別がある。登録または登録失敗が生じる登録処理、照合判定結果を生じる照合処理、識別判定結果を生じる識別処理
	入力試行	システムに対する１つの個体の提示
	正規入力試行	使用法に忠実に行う、正規の個体の単一の入力試行
	非正規入力試行	非正規個体の単一の入力試行 注記：非正規個体の種類によりさらに「意図的でない非正規入力試行」、「意図的な非正規入力試行」などに分類される。
	意図的でない非正規入力試行	意図的でない非正規個体の単一の入力試行
	意図的な非正規入力試行	意図的な非正規個体の単一の入力試行
指標		
	誤非合致率、誤不一致率、FNMR	正規入力試行において、その判定対象データが、それに対応する正しい参照データに合致しないと誤判定された割合 注記：測定または観測された誤非合致率は、予測誤合致率または期待誤合致率と異なる（前者は、後者を見積もるために使われる可能性がある。）。
	誤合致率、誤一致率、FMR	意図的でない非正規入力試行において、その判定対象データが、それ以外の参照データに合致すると誤判定された割合

用　語	説　明
誤拒否率、FRR	照合トランザクションにおいて、個体とそれに対応している ID または参照データを誤って拒否する率
誤受入率、FAR	照合トランザクションにおいて、個体とそれに対応していない ID または参照データを誤って受理する率
照合スコア	参照データ間の類似の度合を得点化した値 注記：本ガイダンスでは ISO/IEC 19795-1:2021 [19]に合わせて照合スコアが高いほど類似しているとし、判定対象非限定識別の場合には照合スコアが予め定められた閾値以下の場合にはホワイトリスト登録されていないと判断する。
正受入識別率、誤受理率、TPIR	正規個体の識別トランザクションにおいて、システム出力の順位の高い最大 r 個の ID 候補が正しい ID を含む率 注記：正しい ID を含むとは、その ID が ID 候補の上位 r 位までに含まれることであり、かつ識別対象非限定識別の場合の ID 候補は照合スコアが予め定められた閾値を超えている必要がある。
誤拒否識別率、FNIR	正規個体の識別トランザクションにおいて、システム出力の順位の高い最大 r 個の ID 候補が正しい ID を含まない率 注記：誤拒否識別率＝1－正受入識別率
誤受入識別率、FPIR	非正規個体の識別トランザクションにおいて、照合スコアが予め定められた閾値を超えている ID をシステムが 1 つ以上出力する率 注記：判定対象限定識別において登録に対する不正や攻撃が行われていない場合には、すべての判定対象は登録されているため、誤受入識別はない。
ブルート・フォース攻撃	大量の非正規個体を次々と判定させ正規個体として誤照合または誤識別されるものを探す攻撃
クローン	意図的な非正規個体の内、複製により作成されたもの
複製	美術品などを原作どおりに再現すること。また、そうしたもの
デッド・コピー攻撃、ハード・コピー攻撃	判定時に意図的な非正規個体としてクローンを提示することにより誤判定を生じさせようとする攻撃
ウルフ	意図的な非正規個体の内、なるべく多くの参照データと照合または識別されるように複製または意図的に細工されたもの
ウルフ攻撃	判定時に意図的な非正規個体としてウルフを提示することにより誤判定を生じさせようとする攻撃
クローン受入率、クローン受理率、CAR	照合トランザクションが拒否すべきクローンを誤って受理する率

用　語		説　明
	クローン合致率、クローン一致率、CMR	照合アルゴリズムが 1 回の照合において、不一致と判断すべきクローンを誤って一致と判定する率
	クローン誤受入識別率、CFPIR	クローンに対する識別トランザクションにおいて、システムが ID を 1 つ以上出力する率
	クローン成功率、CSR (Clone Success Rate)	クローンに対する識別トランザクションにおいて、システム出力の順位の高い最大 r 個の ID 候補がクローン元の個体の ID を含む率 注記：CFPIR ≧ CSR
	リプレイ攻撃	事前に正規個体の電子データを不正に取得しておき、判定時にその電子データを不正に判定処理に返す攻撃 注記：データ取得処理の信用度が低い場合に対処が必要となる。
	シミュレート攻撃	事前に複数の正規個体や人工物メトリックシステムに関する情報を入手・解析し、入手できていない正規個体の物理的特徴を推測し、それを製造し判定時に提示するか、その電子データを判定時に不正に判定処理に返す攻撃 注記：入手していない正規個体の物理的特徴の推測は、各正規個体の物理的特徴や参照データが独立しておらず従属関係にある場合に可能となる場合がある。また、電子データを判定時に不正に判定処理に返す攻撃は、データ取得処理の信用度が低い場合に対処が必要となる。
照合/識別に AI（機械学習）を使う場合の注意点		
	敵対的データ	機械学習要素に入力すると想定・直感と異なる推論結果が出力されるよう、意図的に構成されたデータ
	データポイズニング攻撃	機械学習に用いるデータ（訓練データ、教師ラベルなど）に意図的な改変を加える攻撃
	モデルポイズニング攻撃	訓練済みモデルに対して不正な動作などを埋め込む攻撃
	回避攻撃(敵対的データ)	運用時に機械学習利用システムに特定の改変した入力（敵対的データ、adversarial example）を与えることで、機械学習要素に想定外の誤動作を生じさせる攻撃
	モデル抽出攻撃	運用時に、入力データに対する出力の振る舞いを観察することで、訓練済みモデルと同様の動作をするモデルを抽出する攻撃
	メンバシップ推測攻撃・モデルインバージョン攻撃・性質推測攻撃	訓練データについての情報を摂取する攻撃

用　語		説　明
	解釈/説明機能を誤動作させる攻撃	敵対的データなどを用いて AI の解釈/説明機能によって出力される説明内容の価値を下げたり、間違った説明を生成したりする攻撃
	機械学習モデルの正確性	一定の品質が担保された学習データ（訓練用データ、テスト用データ、検証（バリデーション）用データからなる）に含まれる具体的な入力データに対して、機械学習要素が期待通りの反応を示すこと
	機械学習モデルの安定性	学習データに含まれない入力データに対して、機械学習要素が期待する反応を示すこと

付録２　カメラスペック項目候補

用途に応じてカメラのスペックを規定する際の項目の例

- 読取り時に必要なデータのタイプ（静止画のみ、動画のみ、静止画または動画いずれでもよい、など）
- 受入可能な静止画、または、動画のファイル形式
- 必要な倍率（最低〇倍など）
- 必要な画素数（最低〇〇万画素など）
- カラー、モノクロ（カラー不可、モノクロ不可など）
- 必要な階調（一色につき:２階調以上、16 階調以上、256 階調以上、など）
- 被対象物の種類とサイズ（〇〇mm～〇〇cm など）
- 撮影可能距離（〇〇cm～〇〇cm など）
- 視野(FOV)/画角/焦点距離（対角線画角〇〇°～〇〇°など）
- シャッタースピード
- 撮像デバイスの種類（MOS 型、CCD 型、など）
- カメラ側で行われてはならない画像処理（最近のカメラは画像を美しく見せるなどの目的でさまざまな処理が入っている場合があるため。記述例：RAW 形式データを取得できること。ローパスフィルターレスであること。など）
- カメラなどの読取装置との通信方式
- その他の制約や条件（例えば、ISO 感度、手ブレ補正機構など）

付録３　撮影環境

物理的特徴をカメラで取得する場合において、登録時と判定時の画像を一致させるための環境条件

- 撮影時の光の状況（光源の種類、波長、フィルターの種類、角度、など）
- 撮影角度（画像歪み）

付録４　個体と共に配布する情報の共通化

個体とともに配布する情報（ID/参照データ/予備選択情報）の共通化

- 格納及び読取り方法
  - 物理的特徴を光学的に読み込み場合において、読取装置を共通化する場合
    - ２次元コード
    - バーコード
  - 周りに存在する個体を把握してから、照合を行う場合
    - IC タグ

付録５　人工物メトリックシステムのセキュリティ評価に関する参考情報

実際に運用される人工物メトリックシステムは、①対象とする個体の特性、②人工物メトリクスに則って計測する物理的特徴、③システムが提供する機能、④システムの構成要素、⑤システムの利用方法、⑥システムを利用する関係者、⑦そのシステムの運用環境などに基づき、考慮すべきセキュリティの側面を洗い出す必要がある。

情報セキュリティマネジメントの側面（例えば④～⑦など）を重点とするセキュリティ評価の場合、ISO/IEC 27000 ファミリで構成される情報セキュリティマネジメントシステム（ISMS）に関する国際規格の枠組みが参考となる。システム構成要素の製品のセキュリティ機能の側面（例えば③～⑤など）を重点とするセキュリティ評価の場合、ISO/IEC 15408 及び ISO/IEC 18045 に関する国際規格[8]の枠組みが参考となる。人工物メトリクスの性能評価の側面（例えば①～③など）に関する評価については、1.1(4)に示すように、ISO TC292 WG4 において議論が進められているところである。また、人工物メトリクスとバイオメトリクスは、対象物の特徴量を計測し照合/識別を行うという点で、性能評価などに関する枠組みが類似することから、バイオメトリクスの性能評価の国際規格である ISO/IEC 19795 ファミリが参考となる。

ここでは、実際の人工物メトリックシステムを導入する場合を想定し、その主要な機能性（照合/識別の性能、及び耐クローン性の実現）をセキュリティ機能性として評価する場合の考え方と評価手順の概要を示す。

(1) セキュリティに影響する運用環境の分類

人工物メトリックシステムを利用した個体管理の一般的な運用モデルを 図 付録 5-1 に示す。

[8] IT 製品のセキュリティに関する評価・認証を実施する IT セキュリティ評価及び認証制度（JISEC）[14]では、これらの国際規格の元となる国際標準（CC：Common Criteria と CEM：Common Evaluation Methodology）が利用されている[15]。

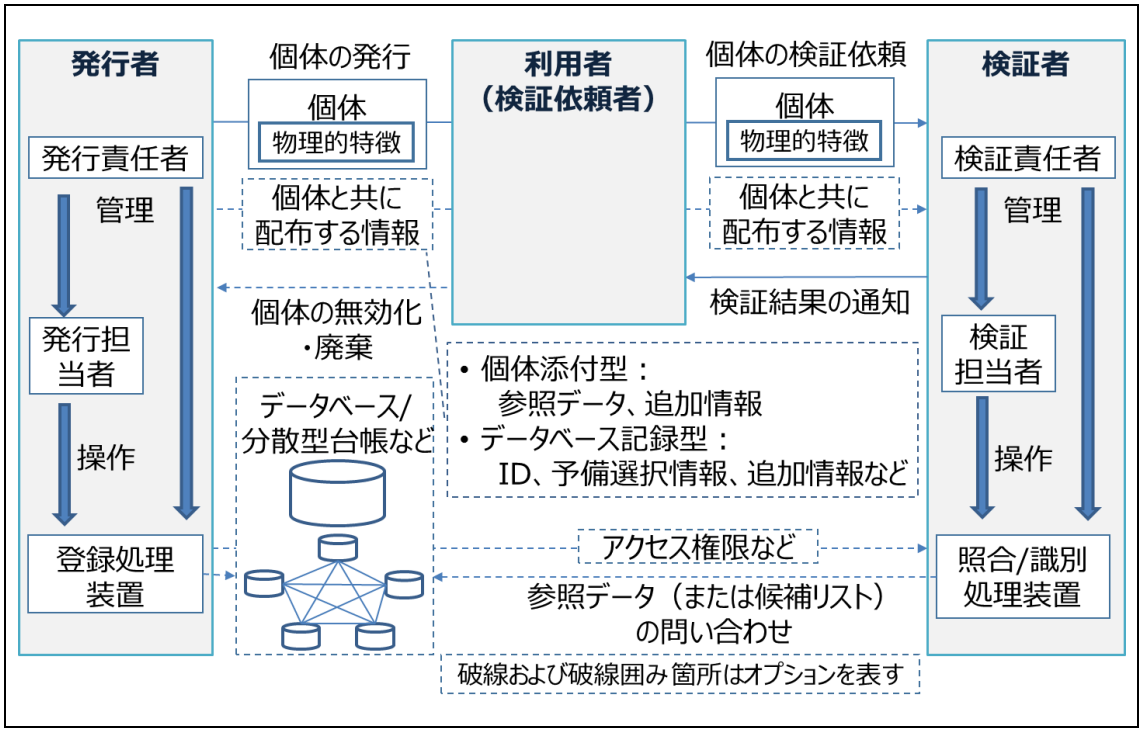


図 付録 5-1 人工物メトリックシステムを利用した個体管理の一般的な運用モデル

特定の個体が、正規の個体であることを証明したいニーズ（あるいは非正規の個体かどうかを確認したいニーズ）を持つ主体を「利用者」とする。利用者は、対象の個体の検証（照合または識別）を「検証者」に依頼する。検証者は、人工物メトリックシステムの「照合/識別処理装置」を操作して、依頼を受けた個体の照合または識別を検証する。この検証の仕組みを適正に運用するために、「発行者」は、製造された個体を利用者に提供する前に、人工物メトリックシステムの「登録処理装置」を操作して、正規の個体の参照データを生成し、追加情報等とともにデータベース/分散型台帳などに保管したうえで、その個体を発行する（個体添付型の場合は、参照データ、追加情報を個体と共に配布する）。

人工物メトリックシステムを用いた個体管理の実運用においては、発行者、検証者、利用者がすべて独立の場合、発行者と検証者が同一の場合、利用者と検証者が独立の場合など、利用目的に応じて、主体の位置付けを決めることができる。また、データベースの運用は、共用（発行者が構築・運用、検証者が参照。分散型台帳の場合など）または個別（発行者が構築、その複製を検証者に移管）とすることが考えられる。

各主体の信頼性については、個体管理のサービス提供者である発行者、検証者に関しては、システム運用環境の組織や拠点のセキュリティマネジメントが信頼できる（例えば ISMS 認証を取得）、装置の校正能力が信頼できる（例えば ISO/IEC 17025 認定を取得）、装置システムのセキュリティ機能が保証されている（例えば ISO/IEC 15408 に準じたコモンクライテリア認証を取得）のように、国際標準への対応状況などにより、客観的に判断できることが望ましい。また、利用者を含めて、各主体が適切な主体であること（例えば、反社会的

勢力と関係しないことなど）を、何らかの方法で確認するといった対応により、主体の信頼性を担保することも考えられる。いずれにしても、ここで示すセキュリティ評価の対象は、運用環境の各主体の信頼性を前提としたうえでの、人工物メトリックシステム（情報セキュリティ技術としての人工物メトリクスを含む）の機能性とその運用方式に焦点を当て考える。なお、セキュリティの課題、対策方針、及びセキュリティ要件の分類と表記方法は、ISO/IEC 15408 を参考としている。

(2) セキュリティに関する課題と対策方針の分類

人工物メトリックシステムのユースケース分類「4.3 判定対象の集合の範囲による分類」では、対象とする個体の分類を、①正規個体（本物）のみ、②意図的でない非正規個体（偽物）も含む、③意図的な非正規個体（偽物）も含む、の３つに分類した。人工物メトリクスのメカニズムに対する基本的な課題は、照合/識別の性能及び耐クローン性として十分な効果が得られないことである。また、運用環境の各主体の信頼性を前提とした場合においても、人工物メトリックシステムが扱う情報資産への第三者アクセスを起点とする課題への対策は必要である。これらを踏まえ、人工物メトリックシステムのセキュリティに関する基本的な課題と対策方針、及び第三者アクセスの課題（主となるもの）と対策方針は、以下となる。ここでは、T：threat（脅威）と O：Objective（対策方針）を使って、課題（脅威）と対策方針を識別する。

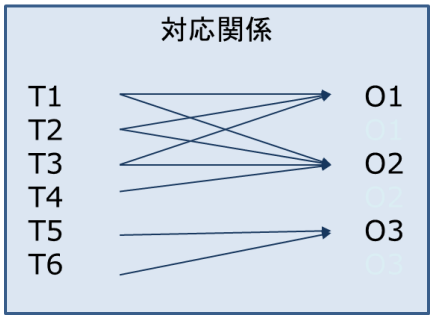
- 基本的な課題（照合/識別の性能、耐クローン性）
  - (T1) 正規個体が、その個体として照合/識別されない
  - (T2) 意図的でない非正規個体が、正規個体として照合/識別される
    - ✧ 登録時に、たまたま照合してしまうような参照データが複数登録された場合（その懸念がある場合）も、意図的でない非正規個体が混入していると考えられるため、T2 に該当する
  - (T3) 意図的な非正規個体が、正規個体として照合/識別される
  - (T4) 登録個体（正規個体）が、ブラックリスト登録個体（意図的な非正規個体）として識別される
  - (T5) 品質を満たしていない参照データが登録される
  - (T6) 品質を満たしていない判定対象データで照合/識別される

- 第三者アクセスの課題（主となるもの）
  - (T7) ネットワーク経路上のデータの不正アクセス
    - ✧ 参照データの搾取/改ざん、結果通知の改ざん、送信元・宛先の成りすまし
  - (T8) データベースへの不正アクセス
    - ✧ 参照データの搾取/改ざん、ID/予備選択情報/追加情報の改ざん

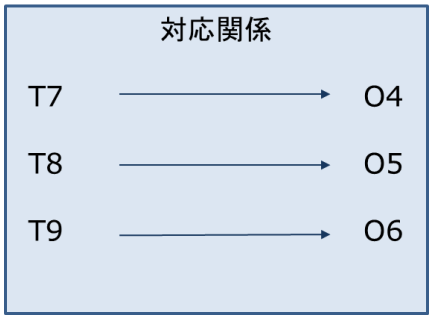
- （T9）登録処理装置、照合/識別処理装置への不正アクセス
  - 許可されない操作による非正規個体の登録、照合/識別の実行

- 対策方針
  - （01）定義された性能を満たす照合機能を提供
    - 判定対象の個体の集合に基づく指標を満たす性能（①正規個体のみ、②意図的でない非正規個体も含む、③意図的な非正規個体も含む）
  - （02）定義された性能を満たす識別機能を提供
    - 判定対象の個体の集合に基づく指標を満たす性能（①正規個体のみ、②意図的でない非正規個体も含む、③意図的な非正規個体も含む）
  - （03）品質を満たしていない参照データ/判定対象データの使用を防止
    - 登録時、及び照合/識別時の生成データの品質検査
  - （04）ネットワーク経路上の保護
    - 高信頼チャネルの確立、経路暗号化など
  - （05）データベース機能のアクセス制御とデータの保護
    - データベースが具備すべ機能（利用エンティティの識別認証、各データベース機能のアクセス制御など）
    - データの機密性/完全性保護（データの暗号化、電子署名/メッセージ認証子/ハッシュ関数/ブロックチェーン/分散型台帳などを利用した改ざん検出など、管理区画内での運用と利用）
  - （06）装置機能のアクセス制御
    - 操作者/管理者の識別認証、利用機能のアクセス制御など

これらの課題（脅威）と対策方針の関係は以下の通りである。



基本的な課題と対策方針の関係



第三者アクセスの課題と対策方針の関係

実際の運用環境を伴う特定の人工物メトリックシステムのセキュリティに関する課題を整理する際には、これらの分類を参考に、個別要因から生ずる課題とその対策を含めて検討する必要がある。

(3) セキュリティ要件の例

基本的な課題とその対策方針は、人工物メトリックシステムのメカニズムとして設計、実装する必要がある。O1、O2、及び O3 の対策方針を、人工物メトリックシステムのセキュリティ要件を形式的に定義すると以下のようになる。実際のシステムのセキュリティ要件とする場合は、[選択]は、列挙された指標から実際に保証する指標を選択し（複数選択可能）、[割付]には、指示対象の具体的な数字や基準値を記入する。基準値は、試験前は目標値、試験後は実測値、もしくは実測値から信頼区間推定により保証できる保証値とし、その値がどのような処理に基づいたものかがわかるようにする。例えば、意図的でない非正規個体の FMR の基準値として「目標値 10^{-5} 未満」、「標本数 10^{5} における実測値 0.0005 未満」、「95%信頼区間の上限 4.6×10^{-5} 未満」のように記入する。信頼区間は、近似的に求める方法が複数存在しているが、誤り率が小さい場合や標本数が少ない場合などにおいては近似誤差が大きくなるため注意が必要である。近似を用いない正確な信頼区間の値は EBCIC :Exact Binomial Confidence Interval Calculator[17]を用いて求めることができ、近似値的に求められた信頼区間との差を算出したり図示したりすることもできる。なお、互いに独立で同一の二項分布に従う N 回の試行で偶然に誤った回数が 0 である確率が 5%になる誤り率を p とすると、95%信頼水準に対して $p \approx 3/N$ となる（3 の法則）。そのため、一般的には誤り率の実測値が 0 である場合でも 95%信頼区間の推定値と同等の保証値としてこの 95%信頼水準の p を適用する。信頼水準 95%以外の実測値 0 の信頼区間も EBCIC を用いて求めることができる。

コラム：誤り率の信頼区間を EBCIC を用いて求める方法

1. PyPI (Python Package Index) ebcic package のインストール
   pip コマンドが利用可能になっているターミナルで以下のコマンドを実行
   ```
   $ pip install ebcic
   ```
2. コマンドラインヘルプ(引数の使い方、バージョン情報など)の表示
   ```
   $ python -m ebcic -h
   ```
3. 信頼区間を計算するためのコマンド例
   - 試行回数 100 回中、誤った回数が 0 回の場合の誤り率の 95%片側信頼区間の上限の表示
     ```
     $ python -m ebcic -k 0 -n 100 -c 95 -u
     ```
   - 試行回数 100 回中、誤った回数が 1 回の場合の誤り率の 95%両側信頼区間の下限と上限の表示
     ```
     $ python -m ebcic -k 1 -n 100 -c 95 -lu
     ```
   - 試行回数 100 回中、誤った回数が 1 回の場合の誤り率の 95%片側信頼区間の上限の表示（-k の引数が 0 より大きく -n の引数より小さい場合、-c の引数には片側信頼区間のパーセンテージを confi_perc_for_one_sided として 2* confi_perc_for_one_sided - 100 を指定する。本例の場合 2*95 – 100 = 90 を指定。）
     ```
     $ python -m ebcic -k 1 -n 100 -c 90 -u
     ```

EBCIC の詳細な使い方及び最新版は[17]を参照するとよい。

- 個体の照合（01 を実現するためのセキュリティ要件）
  - 正規個体の照合（FNMR/FRR）
    - 登録済みの正規個体について[選択: FNMR [割付:X1] 以下、FRR [割付:Y1] 以下]で動作する照合メカニズムを提供すること。
  - 非正規個体の照合（FMR/FAR）
    - 非正規個体について[選択: FMR [割付:X] 以下、FAR [割付:Y] 以下]で動作する照合メカニズムを提供すること。
    - 非正規個体に対する FMR/FAR は、非正規個体の種類により変わるため、対象とする非正規個体の種類を明確にすること。

- ✧ 非正規個体の種類は大きく「意図的でない非正規個体」と「意図的な非正規個体」に分かれ、さらに「意図的な非正規個体」にはクローンやウルフなどが含まれる。
- ✧ クローンに対する FMR/FAR を取り分け CMR/CAR と定義し指標名で区別してもよい。

- 個体の識別（02 を実現するためのセキュリティ要件）
  - ➢ 正規個体の読取/識別（FNIR/(TPIR)）
    - ✧ 登録済みの正規個体の読取りに対して rank [割付:Y]以下の場合に FNIR[割付:X] 以下で動作する識別メカニズムを提供すること。
  - ➢ 非正規個体の読取/識別（FPIR）
    - ✧ 非正規個体の読取りに対して rank [割付:Y]以下の場合に FPIR[割付:X] 以下で動作する識別メカニズムを提供すること。
    - ✧ FPIR は非正規個体の種類にも依存するため、対象とする非正規個体の種類を明確にすること。
    - ✧ 非正規個体の種類は大きく「意図的でない非正規個体」と「意図的な非正規個体」に分かれ、さらに「意図的な非正規個体」にはクローンやウルフなどが含まれる。
    - ✧ クローンに対する FPIR を取り分け CFPIR と定義し指標名で区別してもよい。

- データの品質（03 を実現するためのセキュリティ要件）
  - ➢ 参照データ/判定対象データの品質
    - ✧ 参照データ/判定対象データが品質仕様を満たしていることを検証するメカニズムを提供すること。

(4) 性能に関する評価方法の例

人工物メトリックシステムの実装が、照合/識別の性能を要求するセキュリティ要件を満たしていることを証明するためには、指標の定義通りの試験（試験条件に適合する複数のサンプル個体を用意し、登録/照合/識別の試行等を組み合わせた試験）を行い、計測した値をもとに評価を実施する。参考として、パスワードに代わる認証技術の仕様に関する規格策定と普及を推進する FIDO Alliance から公開されているバイオメトリクスの要求文書[18]では、母集団の信頼区間の推定に関して以下の必須要件を提起している。

- ➢ 標本から推定した母集団の 80%片側信頼区間の上限が FRR においては 5/100 未満、FAR においては 1/10,000 未満となること。

なお、推測統計においては通常 95%や 99%などの信頼区間が用いられるところを本要件で

は 80%と低い水準が用いられており、また、FAR 1/10,000 はパスワードに換算すると数字 4 桁の非常に弱いパスワードに相当する。そのため、ブルート・フォース攻撃などが想定される用途では、大量の判定処理を試せないようにするなどのセキュリティ対策も別途必要となる。一方、人工物メトリクスにおいては高いセキュリティレベルが要求される用途以外にも、悪意のある攻撃が想定されない状況において物の管理を行う用途もある。そのような場合では、用途に応じて適切な水準を選択する必要がある。

以下は、照合と識別の代表的な指標に対する評価方法である。

- 照合（FNMR または FRR の場合）
  - FNMR =（誤不一致の試験回数）/（全試験回数）
    - 誤不一致の試験回数：誤って不一致と判断された試験の回数
    - 全試験回数：誤不一致率の試験の総回数
  - 評価条件
    - 1 個体あたり 1 回の試行を行う（n 回の試行を行うためには n 個の個体が必要）[9]。
    - 試験毎に個体から情報を読み取るのではなく、予め読み取っておいた参照データを使用してもよい。
  - 評価
    - セキュリティ要件「正規個体の照合（FNMR/FRR）」で定義した基準値を満たすかどうかを評価する。例えば「FNMR（95%信頼区間の上限 10^{-5} 未満）」のような割付の場合、標本となる実測値の集合から 95%信頼区間推定を行い、その上限（高いほうの推定値）が 10^{-5} 未満となるかを判定する。

- 照合（FMR または FAR の場合）
  - FMR =（誤一致の試験回数）/（全試験回数）
    - 誤一致の試験回数：誤って一致と判断された試験の回数
    - 全試験回数：誤一致率の試験の総回数
  - 評価条件
    - FMR または FAR は照合を行う個体の種類にも依存するため、その種類を明確にする。
    - 意図的な非正規個体を照合対象とする場合、それらの物理的特徴は登録されていないため、照合判定用に取得した参照データ 1 つに対して、別の個体のものとして登録されている参照データと各 1 回の照合を行う（意図的な非正

[9] 1 個体を複数回独立して判定する場合の誤り率と、複数の独立した個体を 1 回ずつ判定する場合の誤り率が等しいと仮定できる場合には、各個体を複数回読み取ることにより試行回数を増やすことも可能である。

規個体 m 個、登録個体 n 個の場合、m×n 回の試行を行う）[9]。

- ✧ 意図的でない非正規個体を照合対象とする場合、それらの物理的特徴は登録されていないか、別の個体のものとして登録されている。照合対象の個体の物理的特徴が登録されていない場合、別の個体のものとして登録されている参照データと各 1 回の照合を行う（物理的特徴が登録されていない意図的でない非正規個体 m 個、登録個体 n 個の場合、m×n 回の試行を行う）[9]。照合対象の個体の物理的特徴が別の個体のものとして登録されている場合、その個体以外のものとして登録されている参照データと各 1 回の照合を行う（物理的特徴が登録されている意図的でない非正規個体 n 個の場合、n×(n-1)回の試行を行う）[9]。
- ✧ 試験毎に個体から情報を読み取るのではなく、予め読み取っておいた参照データを使用してもよい。ただし、オフラインのテクノロジ評価（計算機上で参照データ同士の照合試行のみを繰り返す場合）においては、参照データの組み合わせで試行する（物理的特徴が別の個体のものとして登録されている意図的でない非正規個体の照合試行回数は全体で n(n-1)/2 となる）。
- ✧ FAR の場合は、照合トランザクションとしてのデータ取得の失敗を加味した誤受入率を測定する。

➢ 評価

- ✧ セキュリティ要件「正規個体の照合（FMR/FAR）」で定義した基準値を満たすかどうかを評価する。

● 識別（FNIR（TPIR）の場合）

➢ FNIR(r) =（誤拒否識別の試験回数）/（全試験回数）

誤拒否識別の試験回数：正規個体が誤って拒否された試験の回数

全試験回数：誤拒否識別率の試験の総回数

➢ 評価条件

- ✧ 正規入力試行が行われる場合に適用する。
- ✧ 判定対象非限定識別、判定対象限定識別のどちらを対象としているのかを明確にする。
- ✧ 誤拒否の判定条件を明確にする。例えば、判定対象非限定識別において正規入力試行を行う場合、応答された ID の識別順位が r 位を超えるか、照合スコアが予め定められた閾値以下[10]であれば誤拒否とするなど。判定対象限定識別において正規入力試行を行う場合は、閾値の確認は不要となる。
- ✧ 事前に正規個体をすべて登録する（一般的に FNIR はこの登録サイズに依存する）。

[10] ISO/IEC 19795-1:2021[19]の場合の例。

- ✧ 1 登録個体あたり 1 回の試行を行う[9]（rank 及び閾値は要件に指定した値を設定）。
- ➢ 評価
  - ✧ セキュリティ要件「正規個体の読取/識別（FNIR）」で定義した基準値を満たすかどうかを評価する。

- 識別（FPIR の場合）
  - ➢ FPIR =（誤受入識別の試験回数）/（全試験回数）
    - ✧ 誤受入識別の試験回数：非正規個体がホワイトリスト登録済み個体として誤って受入れられた試験の回数
    - ✧ 全試験回数：誤受入識別率の試験の総回数
  - ➢ 評価条件
    - ✧ 判定対象非限定識別において非正規入力試行が行われる場合のみ適用する。
    - ✧ 誤受入の判定条件を明確にする。例えば、非正規個体の識別処理の応答である ID の集合に、照合スコアが予め定められた閾値を超えているホワイトリスト登録済み ID のいずれかが含まれている場合に誤受入とする[11]など。
    - ✧ 事前に正規個体をすべて登録する（一般的に FPIR はこの登録サイズに依存する）。
    - ✧ FPIR は非正規個体の種類にも依存するため、想定する非正規個体の種類を明確にする。
    - ✧ 未登録の 1 個体あたり 1 回の試行を行う（n 回の試行を行うためには n 個の未登録個体が必要）[9]。
  - ➢ 評価
    - ✧ セキュリティ要件「非正規個体の読取/識別（FPIR）」で定義した基準値を満たすかどうかを評価する。

(5) データの品質に関する評価方法の例

参照データ/判定対象データが品質仕様を満たしていることを検証するメカニズム（データ品質検査機能など）の評価は、人工物メトリクスの対象とする個体の物理的特徴や読取装置の状態など、品質仕様に影響を与える要因を分析し、適切なテスト方法を検討する必要がある。

- データの品質検査機能の評価

[11] ISO/IEC 19795-1:2021[19]の場合の例。識別処理により出力される ID が照合スコア順にならんでいる場合には、それらの内のトップスコアが予め定められた閾値を超えていることに等しい。

- 参照データ/判定対象データの品質に影響を与える要因を洗い出す。
  - 汚れ、磨耗、変形または経年劣化
  - 読取装置の不具合や不正使用
  - 読取部分（センサー部分）の汚れや不具合
  - 作製可能なクローンの特性
  - その他の要因
- ユースケースとして装置の品質検査機能による対策に応じたテスト方法を適用。
- 性能評価/耐タンパー性評価は、データ品質検査機能を動作させて実施する。

(6) 個体と物理的特徴との関係に関する評価方法の例

人工物メトリックシステムのユースケース分類「4.2 個体と物理的特徴との関係による分類」に示した、管理対象の個体に物理的特徴を有する物を貼り付けるケースでは、個体の強度とタンパーエビデンスの確保、及び十分な貼付け強度が求められる。ISO/IEC 15408 では、セキュリティ要件を実現する機能性が侵害される可能性（識別された脆弱性という）について、想定する攻撃能力と許容する脆弱性とのバランスに基づいた分析、及びテスト（侵入テストという）を実施し、個体の強度、貼付け強度などの耐性が十分とみなせるかを判断する。

- 貼付け強度の評価（脆弱性の観点）
  - 参考となる規格の例
    - JIS K 6849 引張り接着強さ試験方法[21]
    - JIS K 6850 剛性被着材の引張りせん断接着強さ試験方法[22]
    - JIS K 6852 圧縮せん断接着強さ試験方法[23]
    - JIS K 6853 割裂接着強さ試験方法[24]
    - JIS K 6855 衝撃接着強さ試験方法[25]

- 個体の強度とタンパーエビデンスの評価（脆弱性の観点）
  - ISO/IEC 15408 などを参考に、攻撃者の攻撃能力/攻撃方法を想定した脆弱性の分析、及び必要に応じて疑似的に攻撃を試みる方法を考案し、そのテストを実施する。

(7) 物理的特徴の劣化試験の例

人工物メトリクスが対象とする物理的特徴の経日変化や劣化により、物理的特徴の計測が適正に実施することができず、人工物メトリクスの有効性が損なわれるおそれがある。劣化の原因となる物理特性に対する劣化試験を実施することで、計測対象の物理的特徴の有効性に係る特性を把握することが重要である。

- 暴露試験
  - 耐候性試験（耐光性試験、UV 試験、大気暴露試験[26]など）
  - 促進耐侯性試験[27]（太陽光、紫外線、キセノンなど）
  - 促進腐食試験（金属材料への塩水などによる腐食性など）
- 耐摩耗性試験
  - 塗膜、塗料、ゴム、金属、プラスチック、布、板紙などの表面形状に表れる物理的特性の耐摩耗性など
  - 回転型/直線方向型、研磨紙/センサの使用など、目的の劣化試験規格を満たす検査方法/装置を選定しなければならない。
- 温度変化試験
  - JIS C 60068 規格群[28]による環境試験（電気・電子）温度変化試験など
- 冷熱衝撃試験（ヒートショック試験）
  - 電子基板、車載部品などの急激な温度変化で熱応力や熱ひずみによる不具合など

工業製品はさまざまな国や地域で使用されるため、気象条件や各地域固有の使用法、または個別の規制などにより、それぞれの製品分野/材料/素材を対象とした劣化試験に関する規格が制定されている（ISO、IEC、JIS、ASTM、DIN、ECE、SAE、JASO、EIAJ、MIL など）。製品分野/材料/素材、物理的特徴に影響を与える特性、使用法、または市場要求に基づいた劣化試験を計画し、用途として対象規格に適合した試験装置・検査装置を使用した劣化試験を実施または委託することが望ましい。

(8) 評価手順の概要

人工物メトリックシステムの性能評価を中心とする評価手順は、バイオメトリクスの性能評価の規格（ISO/IEC 19795-1[19]、ISO/IEC 19795-2[20]など）に示された評価手順が参考となる。人工物メトリクスを用いたシステムの導入を検討する場合、対象とする個体の物理的特徴が有する特性と、それをセンサで読取り生成した参照データ/判定対象データを用いた照合方式の組み合わせが、結果としてセキュリティ要件を満たす性能を確保できることを評価する。導入時の性能評価は、方式の検証段階、少サンプル個体による実証段階、実用を想定した多サンプル個体による性能評価段階など、フェーズ毎に実施されるが、以下に示すような評価手順を繰り返し実施することで対応できる。

- 評価計画
  - 評価対象の特定
    - 運用環境、システム、アプリケーション
  - テスト仕様の作成
    - テスト構成/条件、測定すべき指標、性能要因

- ✧ 性能評価用データ（個体種別、条件、規模）
- ✧ テストツールの準備

➢ テスト体制の組成

- データ収集
  - ➢ コ―パス誤り回避
    - ✧ 取得した物理的特徴の誤りの回避方法
  - ➢ メタデータ誤り回避
    - ✧ 取得した ID 等の誤りの回避方法
  - ➢ テスト実施・測定データの収集
    - ✧ ISO/IEC 19795-2[20]などを参考としたシナリオ評価テスト、テクノロジ評価テストの実施
- 分析と記録管理
  - ➢ 測定データから指標の値算出
  - ➢ 要件に対する結果の分析
    - ✧ 特性曲線の比較・分析
    - ✧ 信頼区間の推定
    - ✧ 要件に対する結果の判定
  - ➢ テストに係る記録の保管
    - ✧ ISO/IEC 19795[19][20]、ISO/IEC 17025[29]、JIS Q 17025:2018[30]などを参考とした記録方法、保管方法
  - ➢ 評価結果の報告

変更履歴

＜revision 1.0.0.0000＞

2022 年 1 月 11 日　初版発行

参考文献

[1] 松本弘之, 宇根正志, 松本勉, 岩下直行, 菅原嗣高, “人工物メトリクスの評価における現状と課題”, 日本銀行金融研究所, 金融研究, https:/www.imes.boj.or.jp/research/papers/japanese/kk23-b1-3.pdf, 2004.6

[2] 田村裕子, 宇根正志, “人工物メトリック・システムにおける耐クローン性の評価手法の構築に向けて”, 日本銀行金融研究所, 金融研究, https://www.imes.boj.or.jp/research/papers/japanese/kk23-b1-3.pdf, 2009.7

[3] JIS X 8101-1:2010, “情報技術―バイオメトリック性能試験及び報告―第 1 部：原則及び枠組み”, 2010

[4] JIS X 8101-2:2010, “情報技術―バイオメトリック性能試験及び報告―第 2 部：テクノロジ評価及びシナリオ評価の試験方法”, 2010

[5] ISO DIS 22387, “Security and resilience — Authenticity, integrity and trust for products and documents — Validation procedures for the application of artefact metrics”, https://www.iso.org/standard/80717.html

[6] 政府模倣品・海賊版対策総合窓口, “年次報告書ホームページ”, https://www.jpo.go.jp/resources/report/mohohin/nenji.html

[7] JETRO, “国際知的財産保護フォーラム（IIPPF）ホームページ” https://www.jetro.go.jp/theme/ip/iippf/

[8] YKK, “Brand Protection Partnership ホームページ”, https://www.ykkfastening.com/brand/counterfeit.html

[9] 経済産業省, “模倣品対策に係る取組の効果に関する定量的把握手法の整理及び技術的手段を活用した効果的な対策手法の普及支援策に関する調査”, 平成３０年度知的財産権ワーキング・グループ等侵害対策強化事業　調査報告書, https://www.jpo.go.jp/resources/report/mohohin/document/sonota/kanbetugijutu30fy.pdf, 2019.3

[10] 経済産業省, “模倣品対策技術及びその普及に向けた調査”, 平成２６年度知的財産権ワーキング・グループ等侵害対策強化事業　調査報告書, https://www.jpo.go.jp/resources/report/mohohin/document/sonota/kanbetugijutu26fy.pdf, 2015.3

[11] 政府模倣品・海賊版対策総合窓口, “模倣品・海賊版対策の相談業務に関する年次報告”, https://www.meti.go.jp/press/2018/06/20180629002/20180629002-2.pdf, 2018.6

[12] JIS Q 27000:2019, “情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”, 2019

[13] JIS Q 27001:2014, “情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項”, 2014

[14] IPA, “IT セキュリティ評価及び認証制度（JISEC）”, https://www.ipa.go.jp/security/jisec/index.html
[15] IPA, “セキュリティ評価基準（CC/CEM）　ホームページ”, https://www.ipa.go.jp/security/jisec/cc/index.html, 2018.3
[16] 産業技術総合研究所, “機械学習品質マネジメントガイドライン 第 2 版 (revision 2.1.0)”, https://www.digiarc.aist.go.jp/publication/aiqm/guideline-rev2.html, 2021.7
[17] GitHub, “EBCIC: Exact Binomial Confidence Interval Calculator”, https://github.com/KazKobara/ebcic
[18] FIDO Alliance, “FIDO Biometrics Requirements Final Document”, https://fidoalliance.org/specs/biometric/requirements/, 2020.10
[19] ISO/IEC 19795-1:2021, “Information technology – Biometric performance testing and reporting – Part1: Principles and framework”, 2021
[20] ISO/IEC 19795-2:2007, “Information technology – Biometric performance testing and reporting – Part2: Testing methodologies for technology and scenario evaluation”, 2007
[21] JIS K 6849:1994 “引張り接着強さ試験方法”, 1994
[22] JIS K 6850:1999 “接着剤−剛性被着材の引張りせん断接着強さ試験方法”, 1999
[23] JIS K 6852:1994 “接着剤の圧縮せん断接着強さ試験方法”, 1994
[24] JIS K 6853:1994 “接着剤の割裂接着強さ試験方法”, 1994
[25] JIS K 6855:1994 “接着剤の衝撃接着強さ試験方法”, 1994
[26] 日本ウエザリングテストセンター, “大気暴露試験ハンドブック”, http://www.jwtc.or.jp/info/docs/handbook_taiki-bakuro-shiken.pdf, 2007.1
[27] 日本ウエザリングテストセンター, “促進暴露試験ハンドブッ”, http://www.jwtc.or.jp/info/docs/handbook_sokushin-bakuro-shiken.pdf, 2009.4
[28] JIS C 60068 シリーズ, “環境試験方法－電気・電子”
[29] ISO/IEC 17025:2017, “General requirements for the competence of testing and calibration laboratories”, 2017
[30] JIS Q 17025:2018, “試験所及び校正機関の能力に関する一般要求事項”, 2018