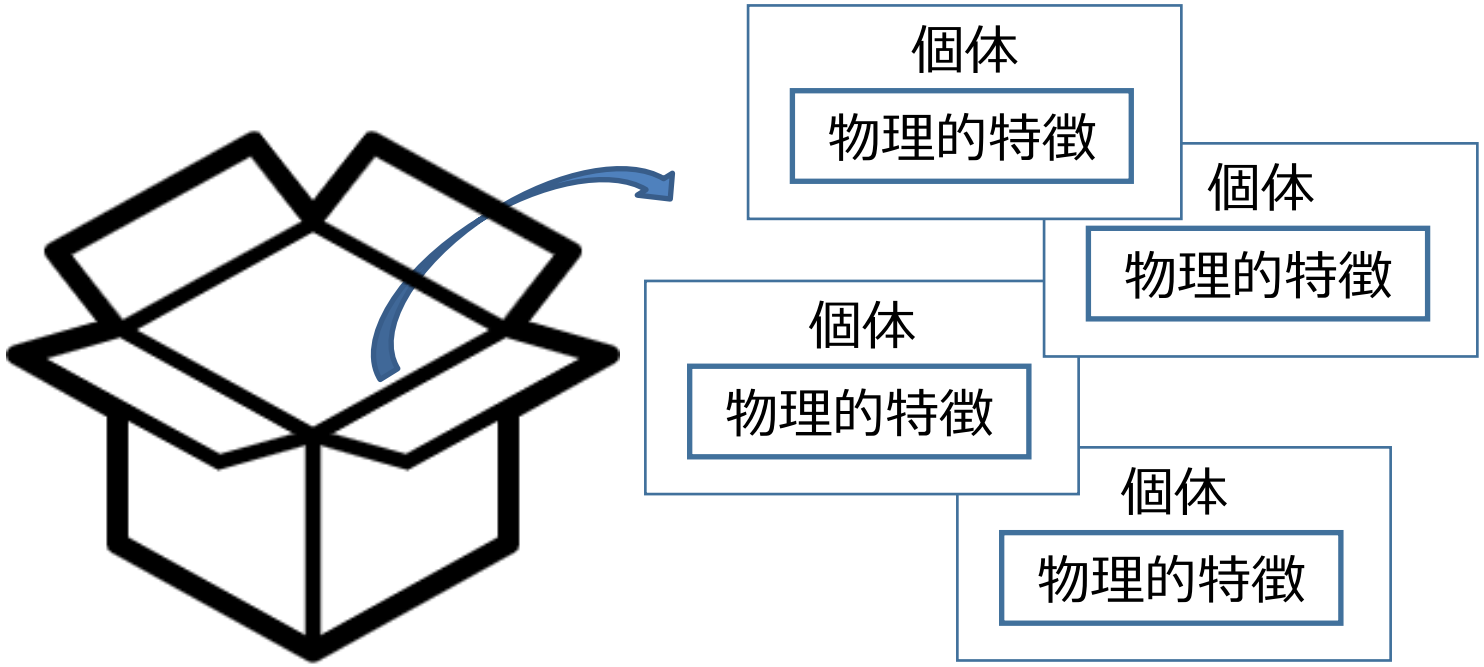
「人工物メトリクスを用いた個体管理技術ガイダンス」のご紹介

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
古原 和邦

この成果は、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）の委託業務（JPNP16007）の結果得られたものです。

人工物メトリクスを用いた個体管理技術ガイダンス

- 製品、デバイス、部品などを、人工物メトリクスを用いて管理する際のガイダンス*
- 人工物メトリクス
  - 物の物理的特徴の計測または測定



* NEDO の委託業務（JPNP16007）において、産総研 CPSEC が企業・大学など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」でとりまとめたもの

ガイダンス紹介ページへのQRコード
https://www.cpsec.aist.go.jp/achievements/artmet

人工物メトリクスを用いた個体管理技術検討委員会

委員（敬称略）

松本　勉	横浜国立大学（委員長）
石山　塁	NEC データサイエンス研究所
海老澤　功	凸版印刷株式会社
川岸　敏之	産業技術総合研究所
高橋　徹	株式会社GAZIRU
仁木　義規	株式会社 村田製作所
原井　謙一	日本ゼオン株式会社
法元　盛久	産業技術総合研究所
牧野　智成	シヤチハタ株式会社
本杉　友佳里	富士フイルムビジネスイノベーション株式会社

ガイダンス紹介ページへのQRコード
https://www.cpsec.aist.go.jp/achievements/artmet

オブザーバ参加組織

- 特許庁国際協力課模倣品対策室（話題提供）
- 大日本印刷株式会社
- 凸版印刷株式会社
- 富士フイルムビジネスイノベーション株式会社

事務局

産総研 CPSEC
古原 和邦、時田 俊雄

事務局補助：
みずほリサーチ＆テクノロジーズ株式会社

人工物メトリクスを用いた個体管理

個体

物理的特徴

人工物メトリクスを用いた個体管理

個体管理の現状

- ID
- シリアル番号
- バーコード
- 二次元コード
- RFID

などを用いた管理

多様なニーズ

タグなどを付けずに管理したい

フォレンジックス用途で使用できるようにしたい(模倣品が原因で**事故**が起きた場合に、それが自社のものでないことを示したい)

ユースケースによる違い

照合or識別

参照データの保管場所

物理的特徴を貼り付ける場合

判定対象の集合

データ取得処理の信用度

AI(機械学習)を使用する場合

利用方式が一種類/複数の場合

ガイダンス紹介ページへのQRコード
https://www.cpsec.aist.go.jp/achievements/artmet

ユースケース毎に、考え方、適用すべき指標、注意点などが異なるため、それらを整理

本ガイダンスの対象範囲

管理対象(模倣品判定対象)の区分*1に対して

- 製品
  - 本体（中身の成分など）
  - 本体・パッケージ（表面）
  - 添付物
    - 印刷物
    - タグ
- 製品情報(製品画像や説明文など)

右記を満たせば区分は問わない

本ガイダンスの対象範囲

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

管理機能(模倣品対策機能)に対して(*2など)

機能		説明
	オバート	目視など人の感覚のみで分かる
	コバート	簡易的な器具を用いるとオバートになる
機械読取可能		機械を用いることで分かる
	フォレンジック	専門分析などで分かる

*1 参考）経済産業省 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「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」調査報告書 デロイト トーマツ コンサルティング 合同会社 2019.03.29 https://www.jpo.go.jp/resources/report/mohohin/document/sonota/kanbetugijutu30fy.pdf

*2 参考）経済産業省「模倣品対策技術及びその普及に向けた調査 」2014 https://www.jpo.go.jp/resources/report/mohohin/document/sonota/kanbetugijutu26fy.pdf

活用例　日本語での用語の辞書として

用語と定義の例

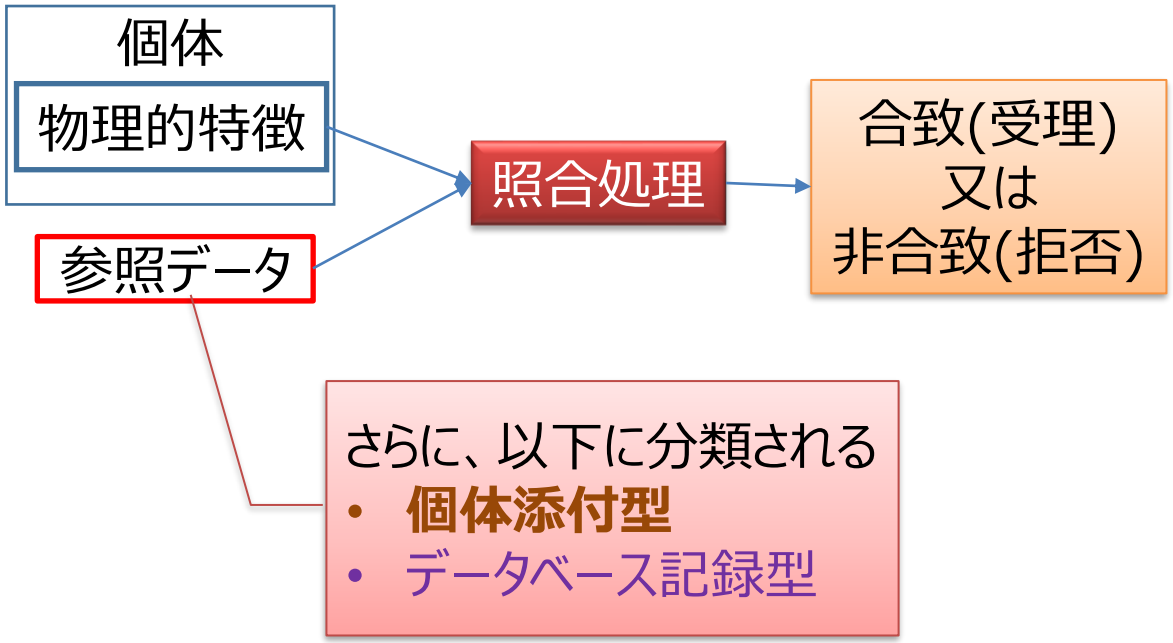
用　語	説　明
全般	
人工物メトリクス	物の物理的特徴の計測または測定用語と定義
人工物メトリクスを用いた個体管理技術	個体の物理的特徴の測定結果を照合または識別することによる管理技術
計測	特定の目的をもって、測定の方法及び手段を考究し、実施し、その結果を用いて所期の目的を達成させること
測定	ある量をそれと同じ種類の量の測定単位と比較して、その量の値を実験的に得るプロセス
コーパス データセット	対象となるデータを大規模に集めてデータベース化した資料 注記：人工物メトリクスの場合、物理的特徴の電子データが「対象となるデータ」に該当する。
シナリオ評価	テストのために用意した個体（物理的特徴を含む）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

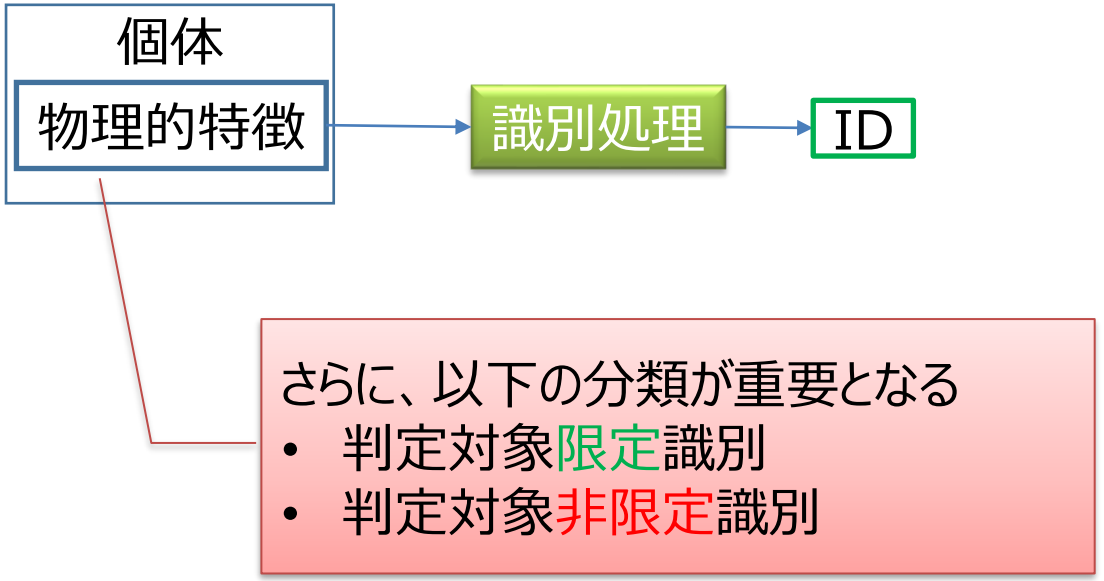
参考文献の例

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/kk28-2-7.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

照合/識別による分類

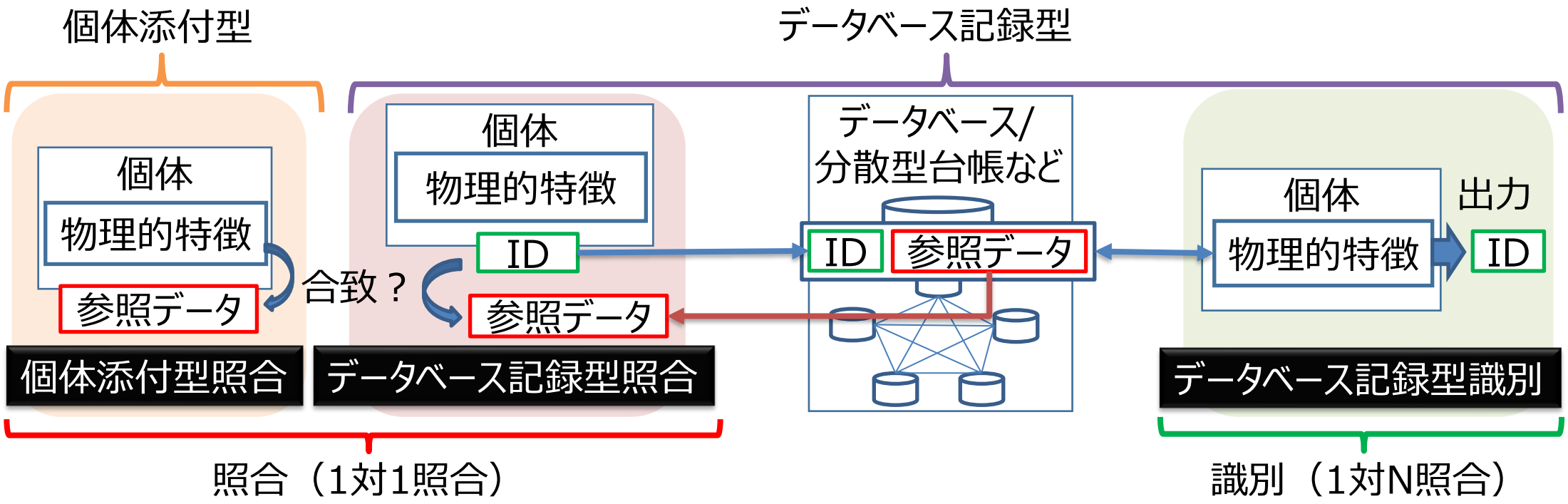
- 照合(1対1照合)
  - 提示されたIDまたは参照データと個体とが対応するか否かを返すアプリケーション
- 識別(1対N照合)
  - 提示された個体に対応する0個又は1個以上のIDの候補を識別順位を付けて返すアプリケーション





参照データの保管場所、による分類

- 照合(1対1照合)
  - **個体添付型**：参照データを個体と共に配付する場合
  - **データベース記録型**：参照データをデータベース/分散型台帳などに格納する場合
- 識別(1対N照合)
  - **データベース記録型**：参照データをデータベース/分散型台帳などに格納する場合



照合と識別との使い分けの例

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
  - 個体またはそのパッケージもしくはその鑑定書などへ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

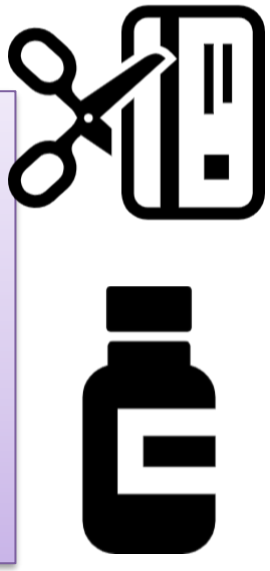
識別を用いた方がよい場合

- 個体とともにID又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
  - 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

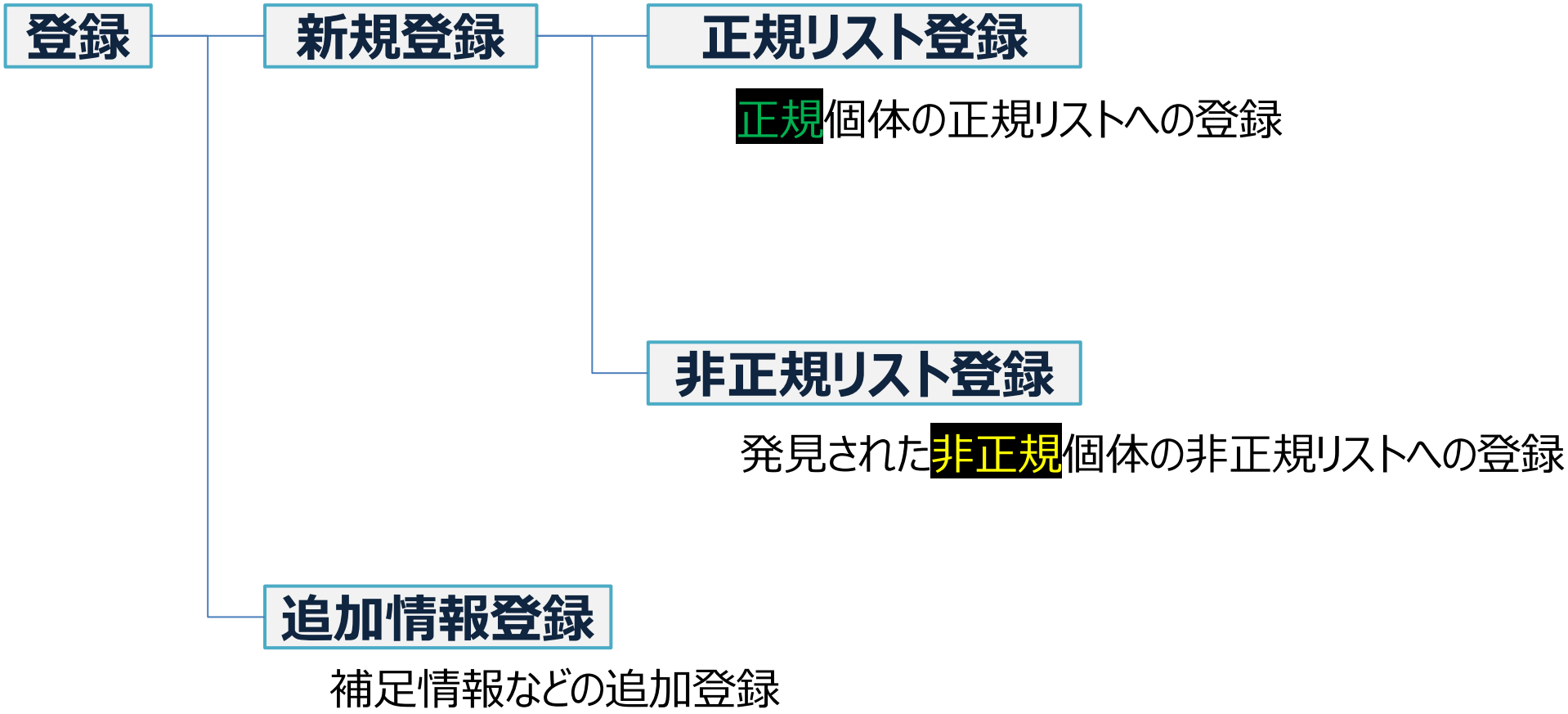
＊ 参照データはデータベースにも保存されている場合。

識別を用いる場合の注意点

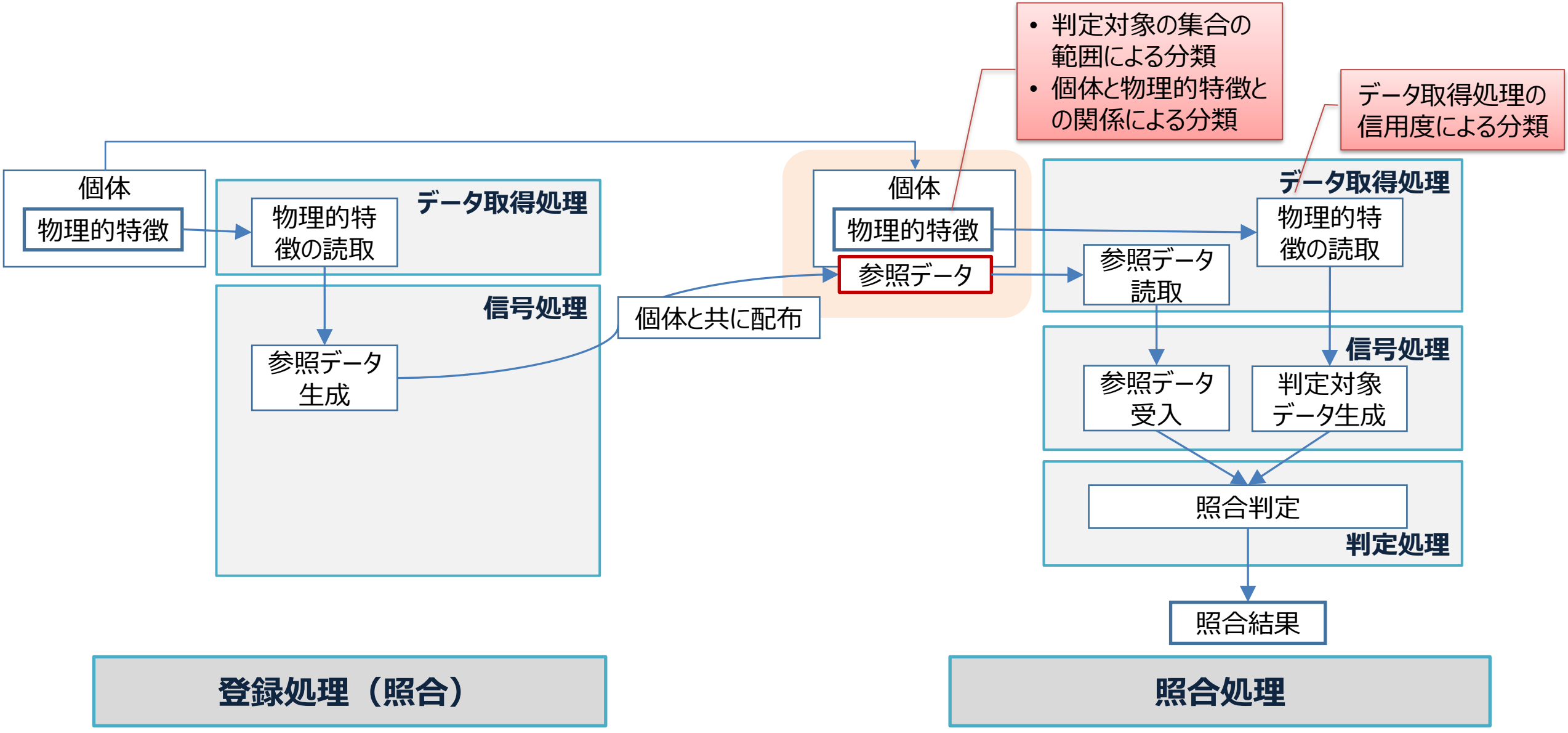
- 一般的に**識別の処理時間と誤識別率**は正規リストへ登録済みの個体数、またはデータベースを検索して得られる候補リスト数の増大に応じて悪化する。
- そのため、それらを許容できる範囲内に登録数または候補リスト数を収める必要がある。
  - 登録数が制限される個体の種類の例：限定品、有効期限のあるもの
  - 予備選択情報の活用
    - ① 個体またはそのパッケージなどに予め記載されている情報(製造日、製造場所、製造番号など)
    - ② 取得した物理的特徴から生成されたデータ



登録処理の分類


登録
新規登録
正規リスト登録
正規個体の正規リストへの登録
非正規リスト登録
発見された非正規個体の非正規リストへの登録
追加情報登録
補足情報などの追加登録

個体添付型照合処理の流れと分類との関係



個体と物理的特徴との関係による分類

個体
物理的特徴

• 個体と物理的特徴との関係による分類

管理対象の個体に物理的特徴を有する物を貼り付ける場合

管理対象の個体

物理的特徴を有する物
物理的特徴

管理対象の個体
物理的特徴を有する物
物理的特徴

注意点

貼り替え防止/検出のための
- 貼り付け強度
- タンパーエビデンス性

の確保

管理対象の個体が有する物理的特徴を用いる場合

管理対象の個体
物理的特徴

判定対象の集合の範囲による分類

個体
物理的特徴

- 判定対象の集合の範囲による分類

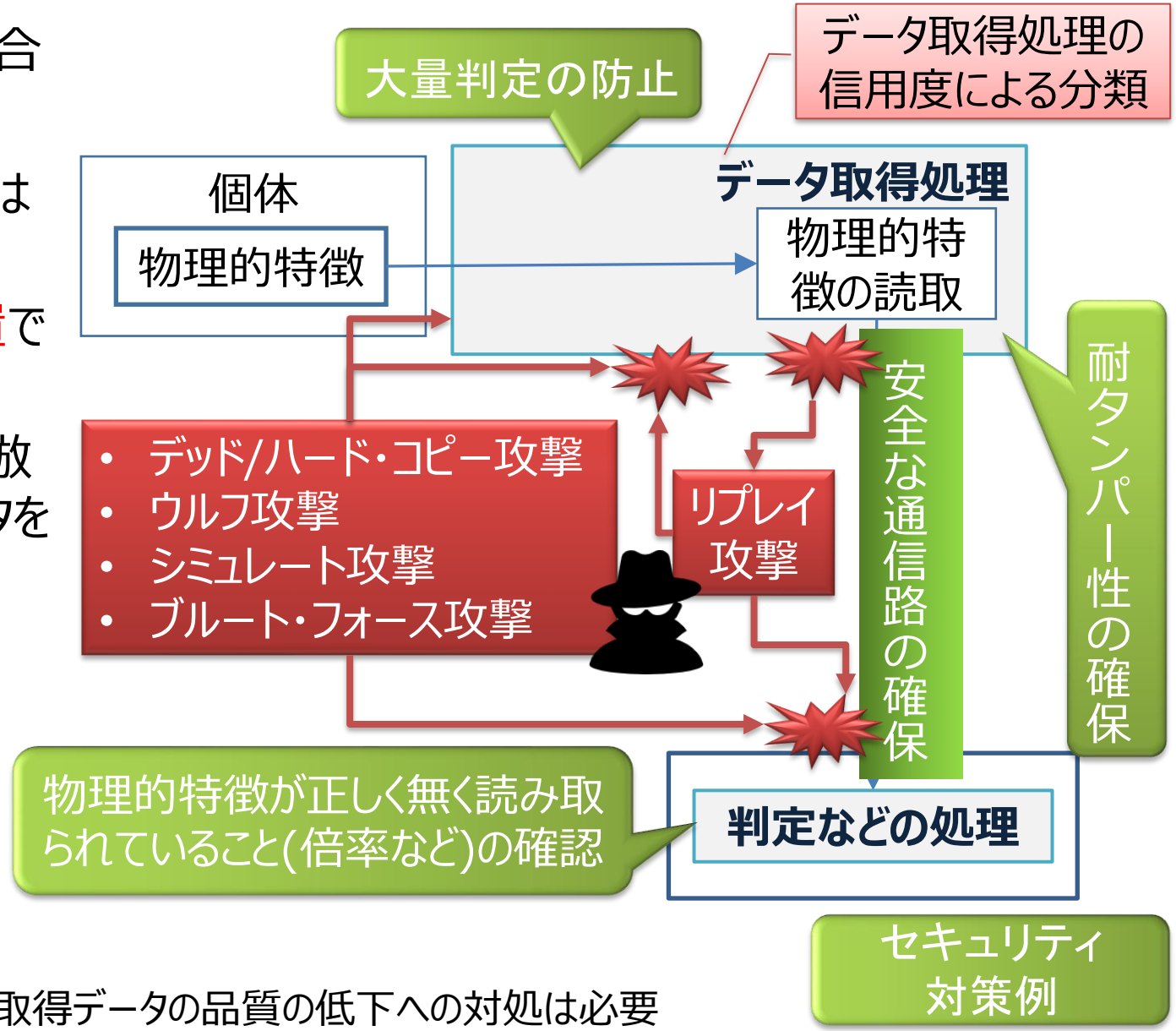
登録に対する不正/攻撃/エラーなどを想定しない場合*

正規/非正規		正規個体（本物）	非正規個体（偽物）	
		正規リスト登録済個体	正規リスト未登録個体	
悪意の有無		意図的に細工または複製された物理的特徴を有さない個体		意図的に細工または複製された物理的特徴を有する個体
個体の分類		正規個体	意図的でない非正規個体	意図的な非正規個体
応用例		• 紛失の検出など	• ラベル張替えの検出 • 混入品の識別など	• 模倣品(複製)の検出など
評価指標	照合	FNMR, FRR	FMR, FAR	CMR, CAR
	識別	FNIR (TPIR=1-FNIR)	FPIR	CFPIR

*登録に対する不正/攻撃/エラーなどを想定する場合は、さらに細かい分類となる。詳しくはガイダンスをご参照下さい。

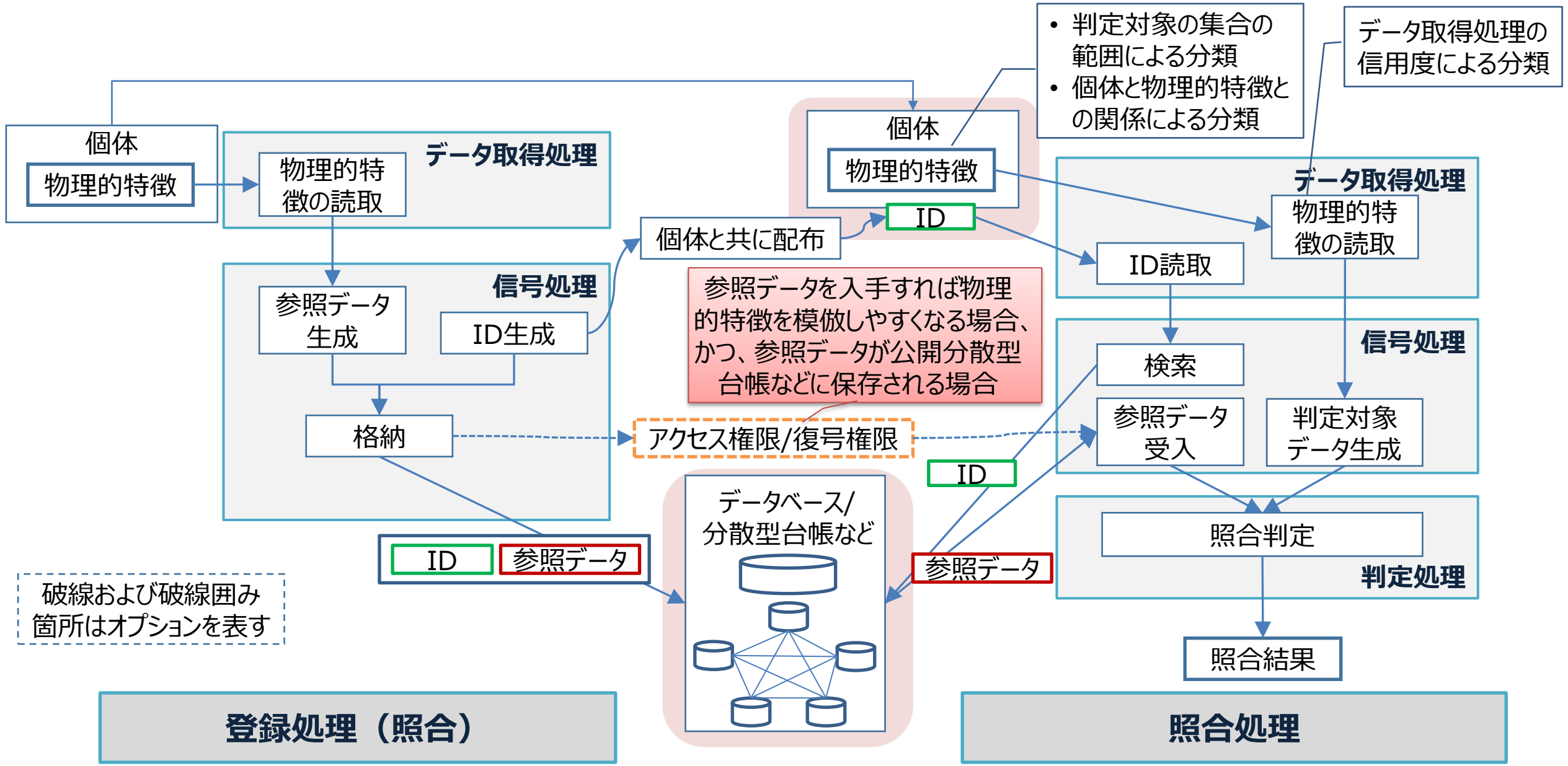
データ取得処理の信用度による分類

- 管理された区画内でデータ取得が行われる場合
  - 例えば管理された工場内など
  - データ取得処理で不正が行われる可能性は小さいと仮定できる*。
- 信用できるとは限らない場所と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
  - 例えば、ブランド品の個人間売買などで模倣品出品者が、自身の装置で取得したデータを用いて、遠隔で判定を行う場合など
  - 右記のような攻撃への対策が必要



* 操作者が未熟練の場合や、データ取得環境の違いによる取得データの品質の低下への対処は必要

データベース記録型照合処理の流れと分類との関係

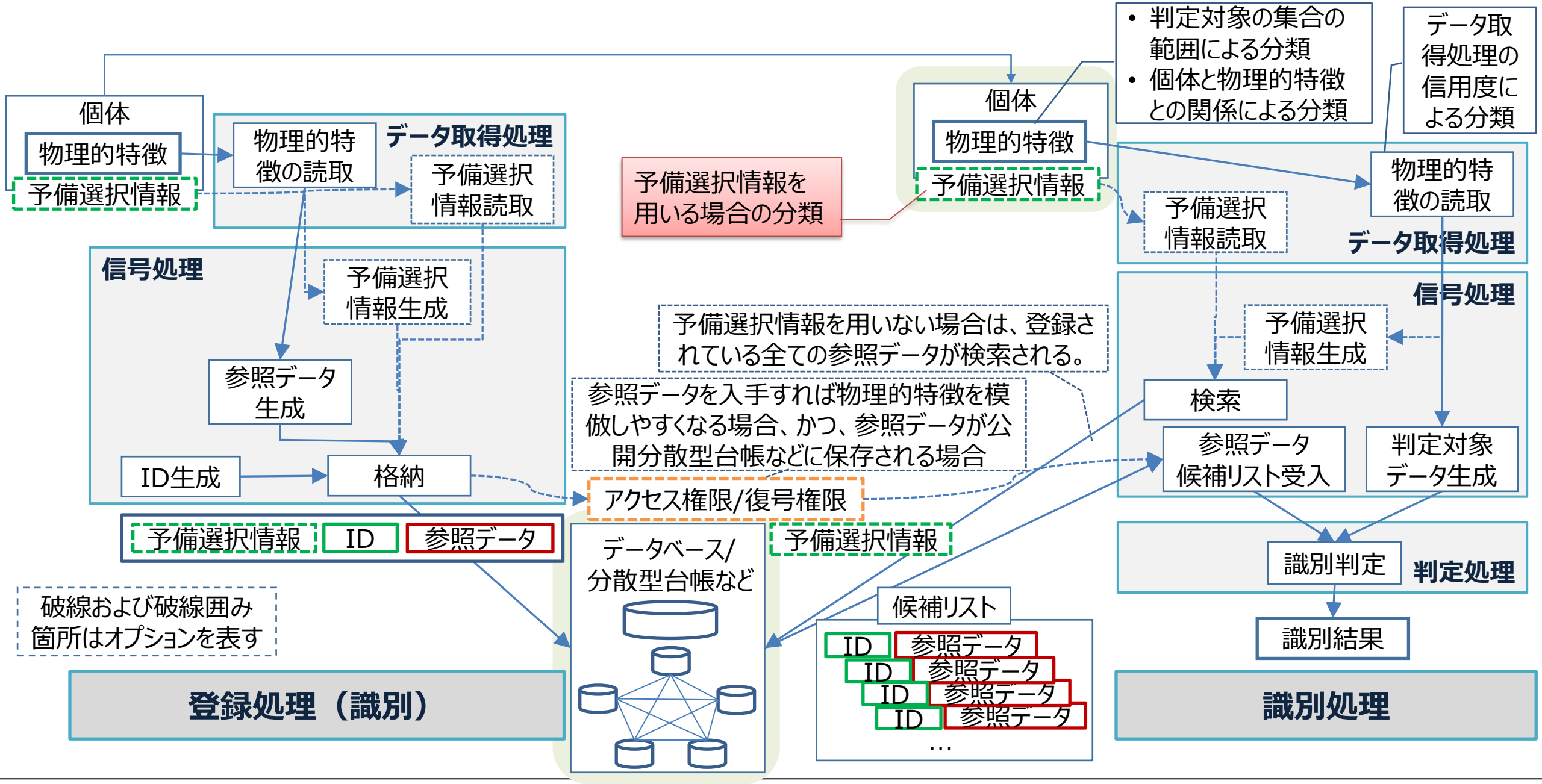


参照データの保管場所による分類と必要な機能

必要なセキュリティ機能 ＼ 分類	個体添付型（照合のみ）	データベース記録型		
		公開分散型台帳	公開していない分散型台帳	分散型台帳以外のデータベース
秘匿性 [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]	参照データの暗号化と信頼できるエンティティ(利用者/管理者など)のみへの復号権限の付与			
			または、盗聴の行われる可能性のある通信路経由で利用する場合、認証された利用者との間の通信路の保護	盗聴、改さん、なりすましの行われる可能性のある通信路経由で利用する場合、相互認証(利用者認証、サーバ認証)されたエンティティ間の通信路の保護
完全性 (および**否認不可性**) [非正規個体の物理的特徴が不正に添付または登録される可能性がある場合]	参照データへの電子署名、メッセージ認証子などの付加 (付加後も、参照データ毎の削除、差替、複製の追加は可能。差替、複製の追加に対しては、FMR, FAR の小ささを確認。)	分散型台帳により提供される		
可用性	参照データの冗長化			データベースの冗長構成

FMR: False Match Rate　　FAR: False Accept Rate

データベース記録型識別処理の流れと分類との関係



予備選択情報を用いる場合の分類

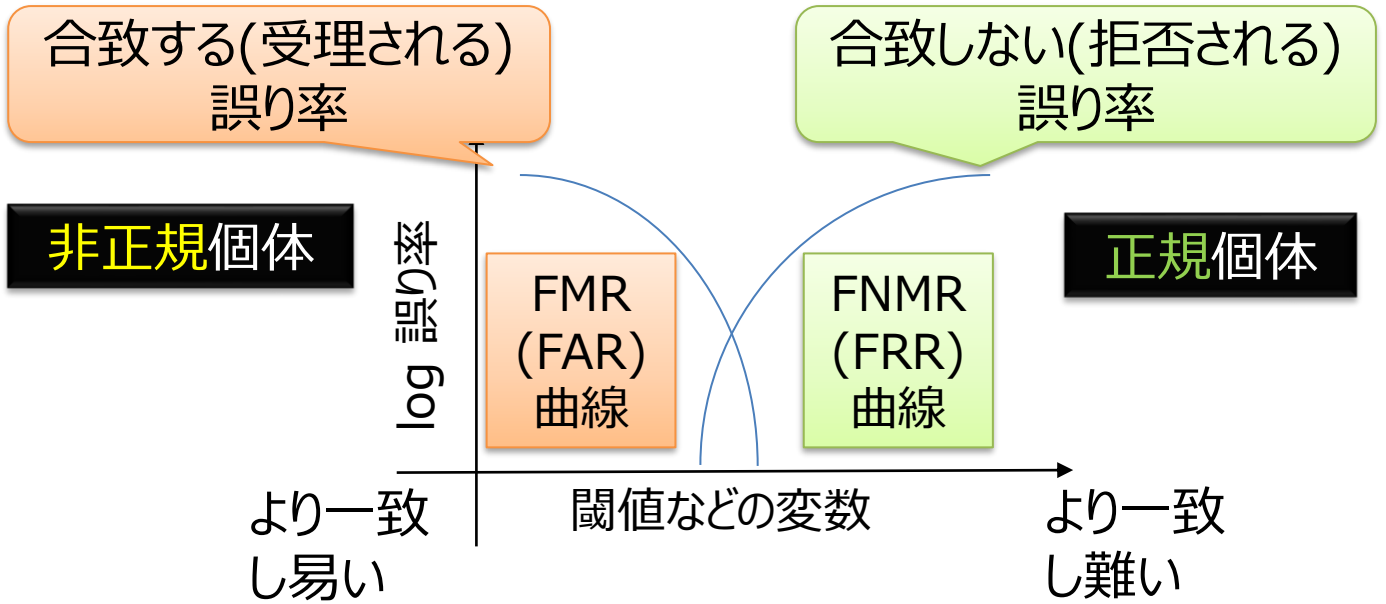
- 予備選択情報の例
  - 個体またはそのパッケージなどに予め記載されている情報
    - 例）製造日、製造場所、製造番号など
  - 取得した物理的特徴から生成されたデータ
- 予備選択を行う場合の指標
  - 絞込み率 PR (Penetration Rate)
  - 予備選択誤り PSE (Pre-Selection Error)

識別を用いる場合の注意点

- 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の例: 限定品、有効期限のあるもの
  - 予備選択情報の活用

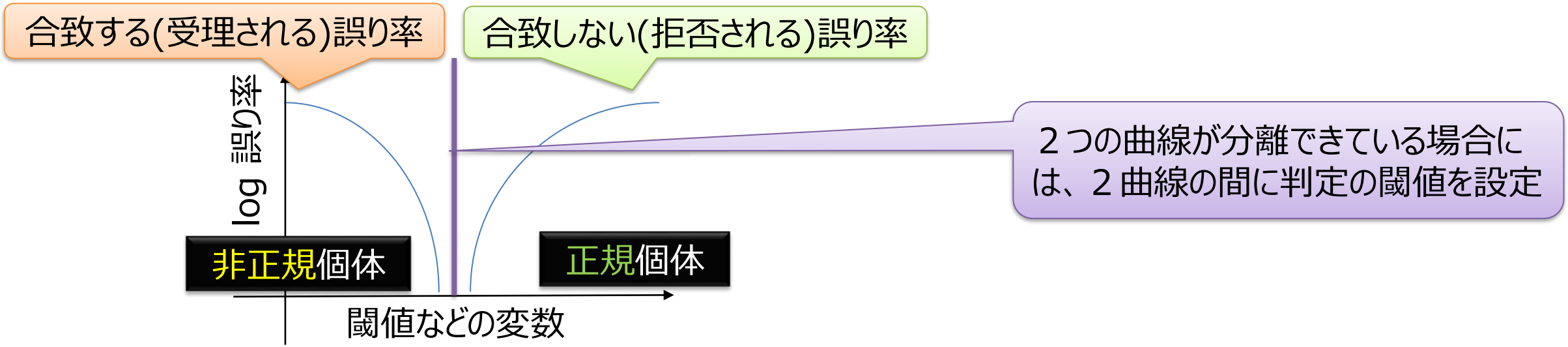
照合に対する指標 FMR, FAR, FNMR, FRR

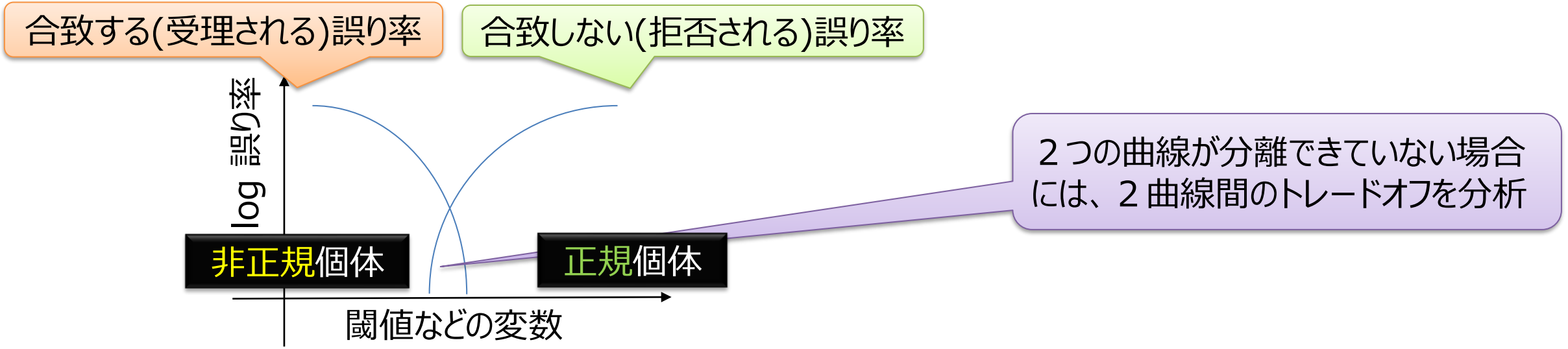
- 参照データとの照合１回当たりの誤り率
  - 誤合致率(誤一致率) FMR
  - 誤非合致率(誤不一致率) FNMR
- システムが下す最終判定の誤り率
  (2回以上の照合を許す場合など)の誤り率
  - 誤受入率(誤受理率) FAR
  - 誤拒否率(誤拒否率) FRR



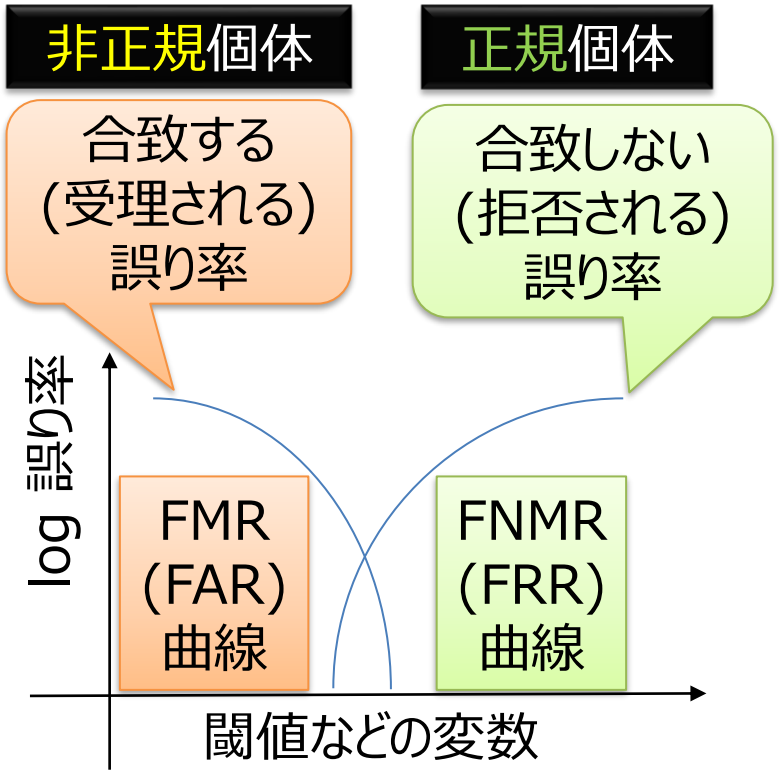
FMR: False Match Rate
FNMR: False Non-Match Rate
FAR: False Accept Rate
FRR: False Reject Rate

２曲線間のトレードオフを分析する必要性の有無





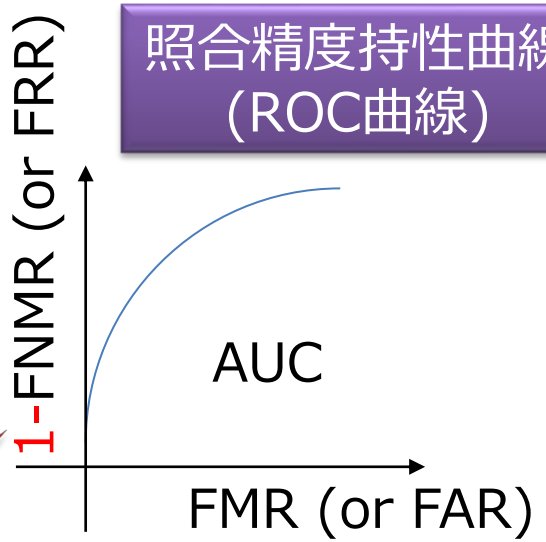
FMRとFNMR, FARとFRRとのトレードオフの図示



ROC曲線とDET曲線の一番大きな違い

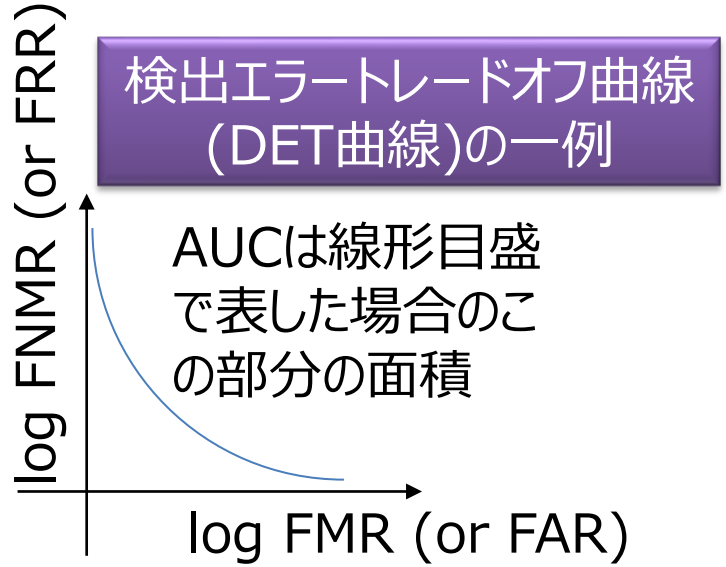
AUCが広いほどよいトレードオフ関係にある

照合精度持性曲線
(ROC曲線)



統計の分野では従来より
ROC曲線が用いられてい
たという経緯がある

検出エラートレードオフ曲線
(DET曲線)の一例



対数目盛で小さな誤り率の関係
を見るならDET曲線の方がよい

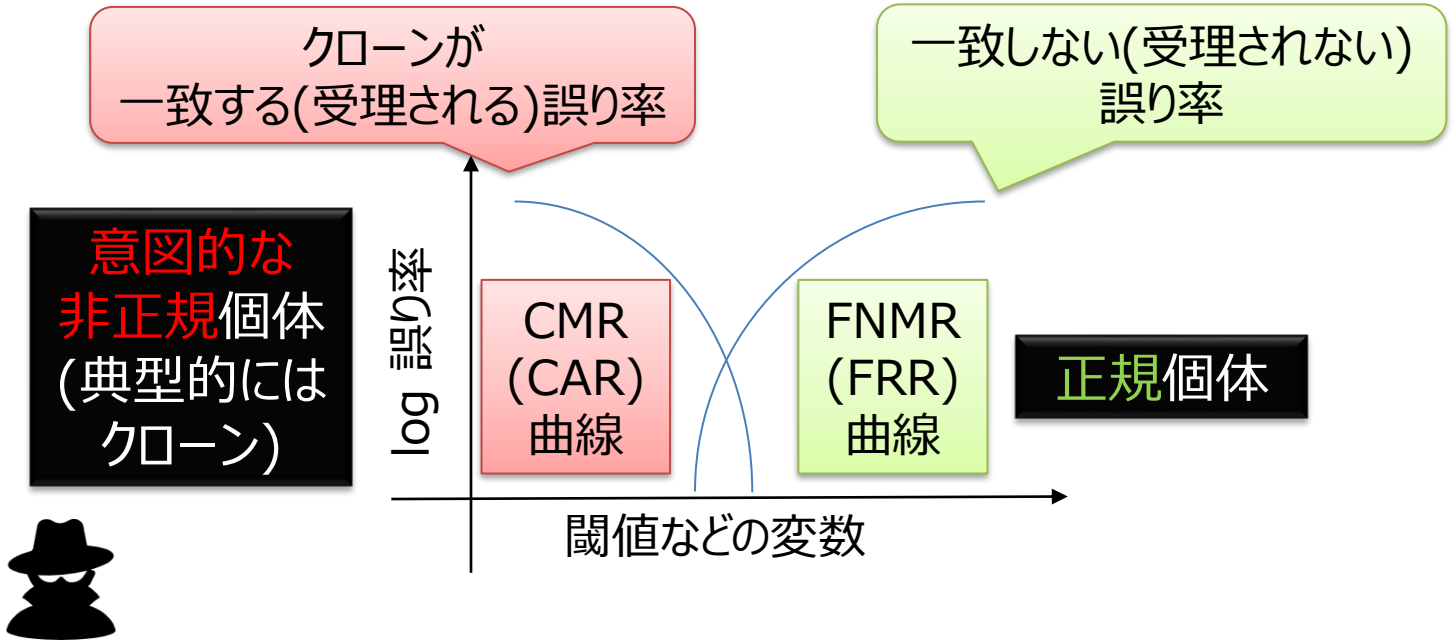
FMR: False Match Rate
FNMR: False Non-Match Rate

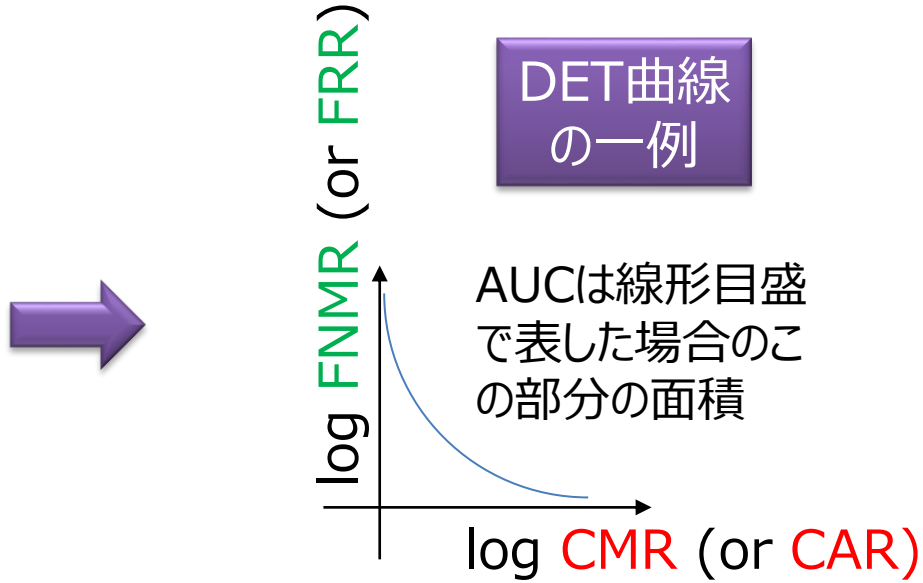
FAR: False Accept Rate
FRR: False Reject Rate

ROC: Receiver Operating Characteristic
DET: Detection Error Trade-off
AUC: Area Under the Curve

意図的な非正規個体(複製:クローン)提示に対する指標

- クローン一致率 CMR
  - Clone Match Rate
  - 1回の照合でクローンが参照データと一致する率
- クローン受理率 CAR
  - Clone Accept Rate
  - 最終的にクローンを受理する率

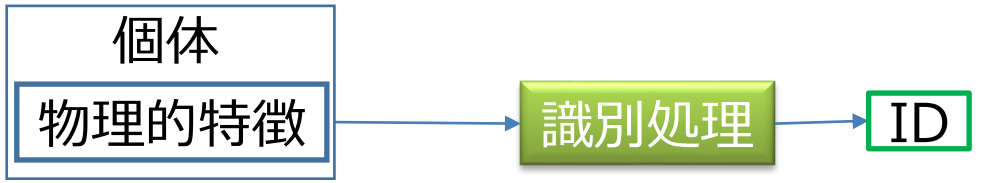




FNMR: False Non-Match Rate

DET: Detection Error Trade-off
AUC: Area Under the Curve

識別処理での登録/未登録判定の必要性による分類



- 判定対象限定識別
  - **定義:** 正規個体(正規リストに登録されている個体)のみを判定対象とする識別
  - **補足:**
    - 識別対象を未登録と判定するための閾値は不要でとにかく類似度の高いIDを返す。
    - 識別処理により出力されたIDとの照合処理を行うと「非合致(拒否) 」が返る場合もある。
- 判定対象非限定識別
  - **定義:**非正規個体(正規リストに未登録の個体)も判定対象とする可能性のある場合の識別
  - **補足:**
    - 類似度等が閾値以下のIDを正規リスト未登録と判定するなどの足切り処理を行う。
    - 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。

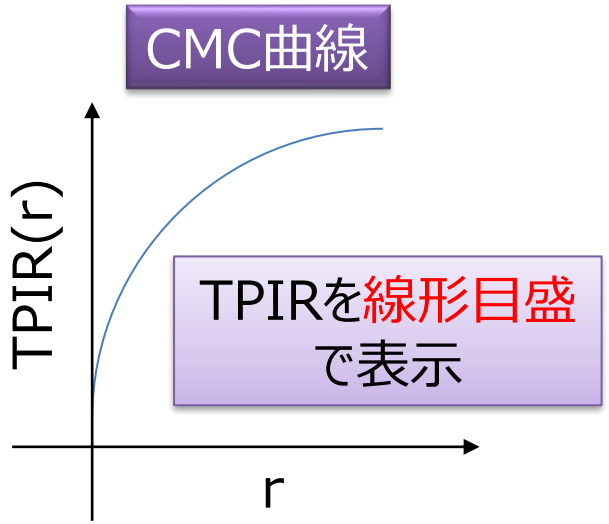
注意点

「判定対象限定識別」を使っている場合に非正規個体を識別すると、その判定対象は登録済みとして処理されるため、(類似度等が閾値以下の場合には警告を発するようにするか) 予め正規リストに未登録の個体を識別する可能性の有無について慎重に判断することが重要となる。

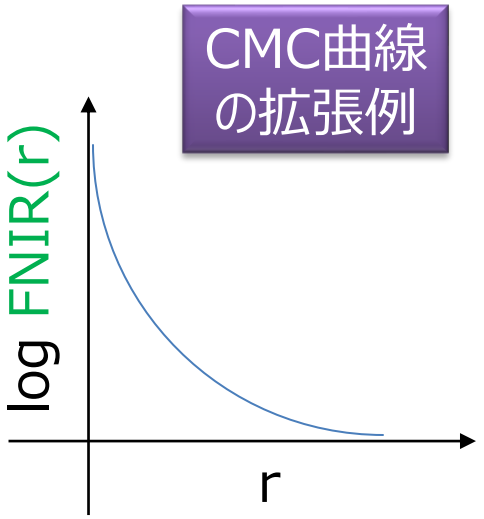
識別に対する指標 FNIR(r), TPIR(r), CMC曲線

- 誤拒否識別率 FNIR(r)
  - False-Negative Identification-error Rate
  - 最大r個のID候補に正しいIDが含まれない誤り率
- 識別率(正受入識別率) TPIR(r)=1-FNIR(r)
  - True-Positive Identification Rate

- 累積識別精度特性曲線
  (累積照合特性) CMC曲線
  - Cumulative Match Characteristics



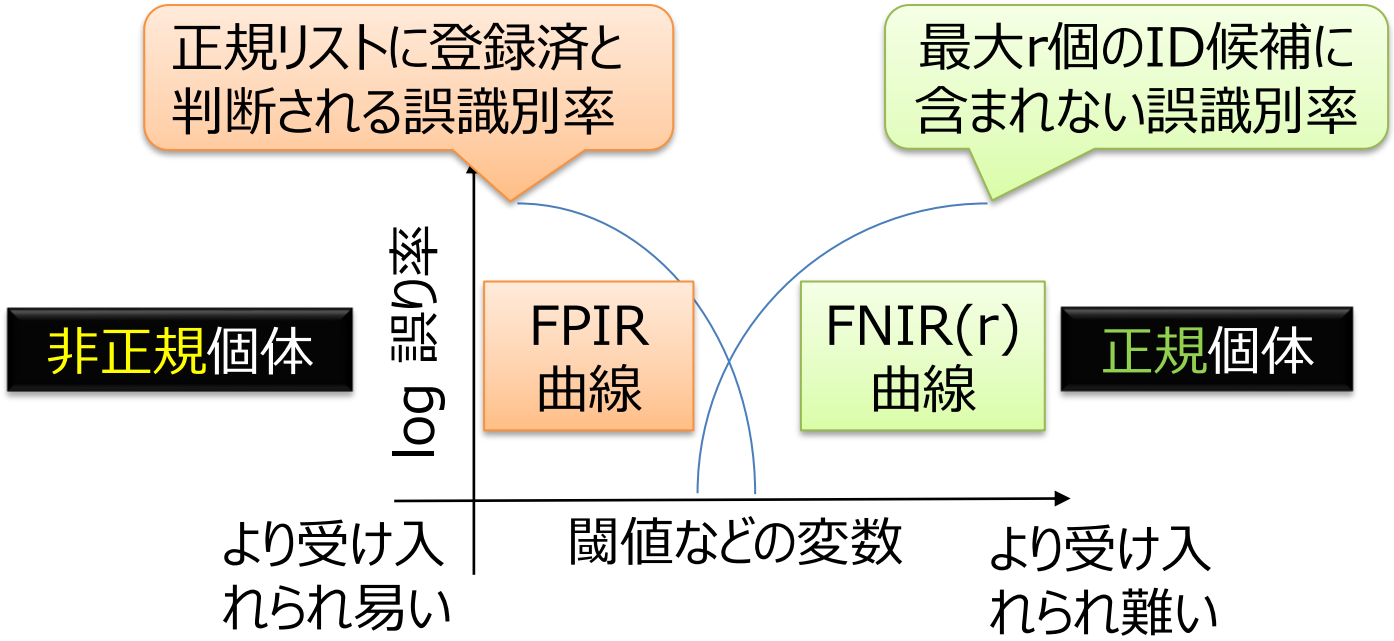
統計の分野では従来より上記のようなCMC曲線が用いられていたという経緯がある



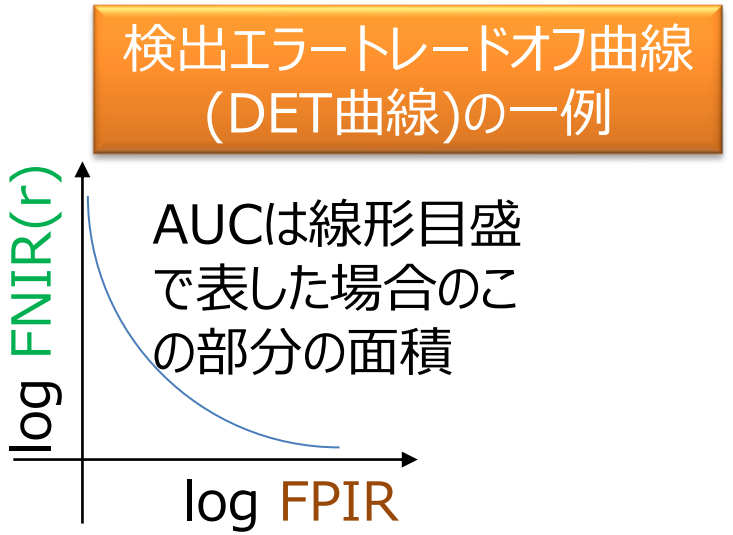
小さな誤り率の関係を見るためには
FNIR(r)を対数目盛で表した方がよい

判定対象非限定識別で追加すべき指標：FPIR

- 誤受入識別率 FPIR
  - False-Positive Identification-error Rate
  - 閾値を超えているIDが１つ以上出力される誤り率



AUCが広いほどよいトレードオフ関係にある

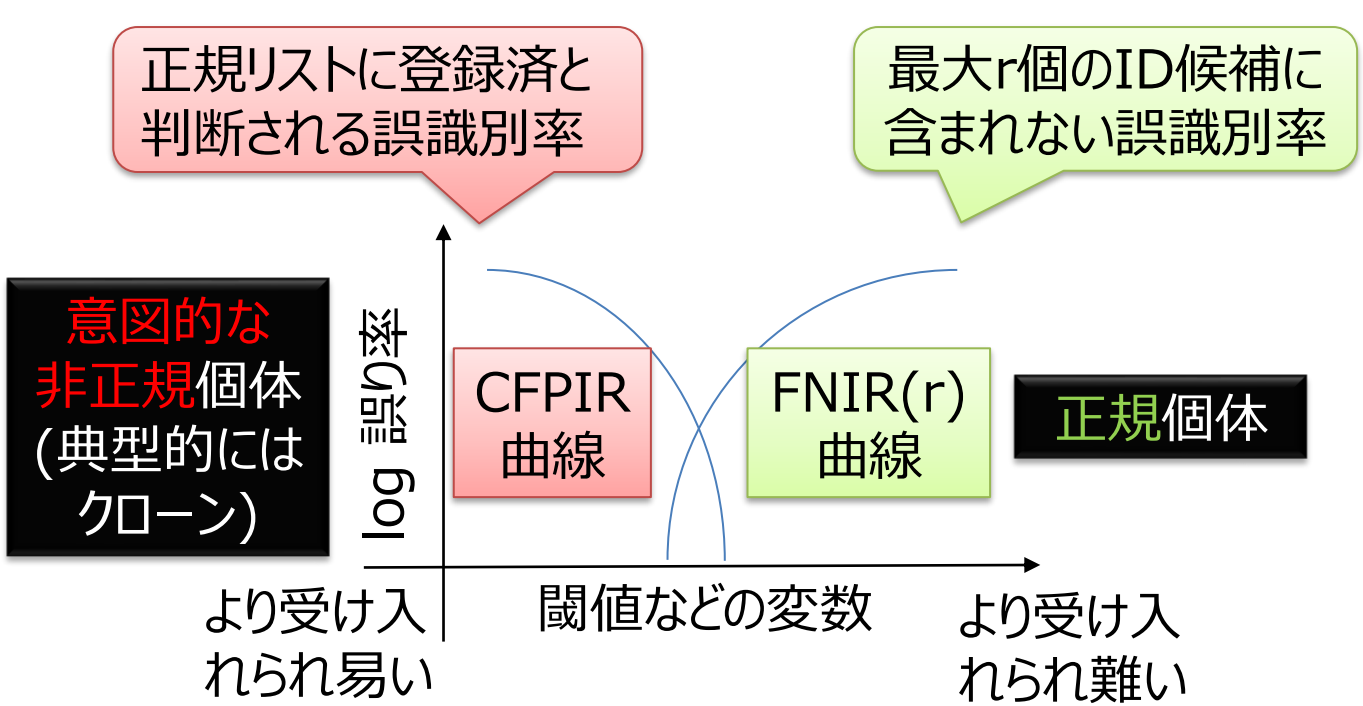


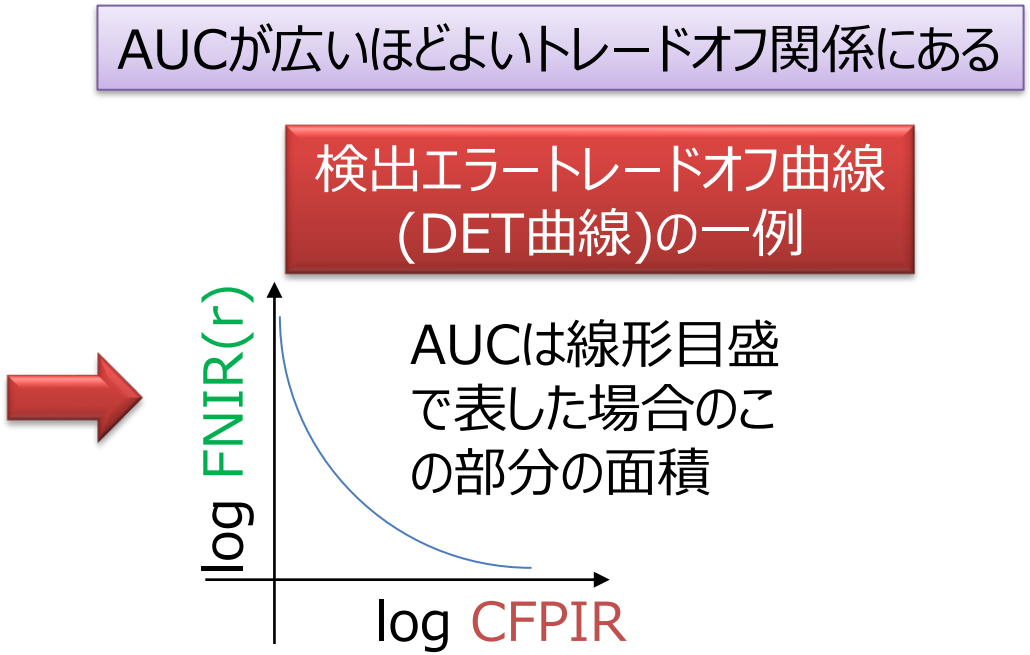
FNIR: False-Negative Identification-error Rate

DET: Detection Error Trade-off
AUC: Area Under the Curve

判定対象非限定識別で追加すべき指標: CFPIR

- クローン誤受入識別率 CFPIR
  - Clone False-Positive Identification-error Rate
  - クローンに対して閾値を超えているIDが１つ以上出力される誤り率
- クローン成功率 CSR(r)
  - Clone Success Rate
  - 閾値を超えているID最大r個の中にクローン元の個体のIDが含まれる誤り率
  - CFPIR ≧ CSR(r)





FNIR: False-Negative Identification-error Rate

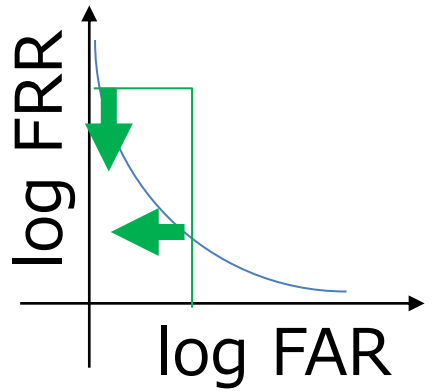
DET: Detection Error Trade-off
AUC: Area Under the Curve

FIDO Allianceにおけるバイオメトリクスでの必須要件

- 標本から推定した**母集団**の80%片側**信頼区間**の上限
  - FRRにおいては5/100未満
  - FARにおいては1/10,000未満

1/10,000はパスワード換算で
ランダムな数字４桁程度の非常に低いレベル：
セキュリティ用途を考慮した場合の最低ライン

DET曲線



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手軽に行う用途もあるため。

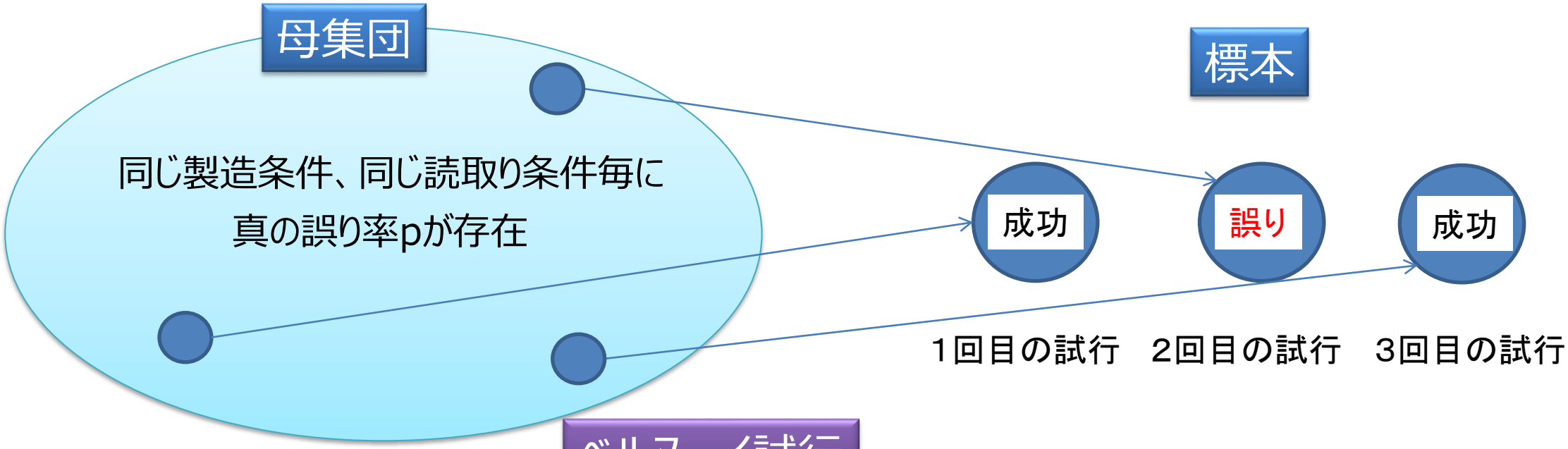
用途に応じて適切な水準を選択する

FIDO Alliance, “FIDO Biometrics Requirements Final Document”, https://fidoalliance.org/specs/biometric/requirements/, 2020.10

母集団と標本の誤り率

母集団の誤り率の信頼区間：
$p' - L(k,n,\alpha) \leqq p \leqq p' + U(k,n,\alpha)$
ここで α は (1-信頼係数)

標本の誤り率：
$p'=k/n=1/3$
ここで n は試行回数、k は失敗の回数

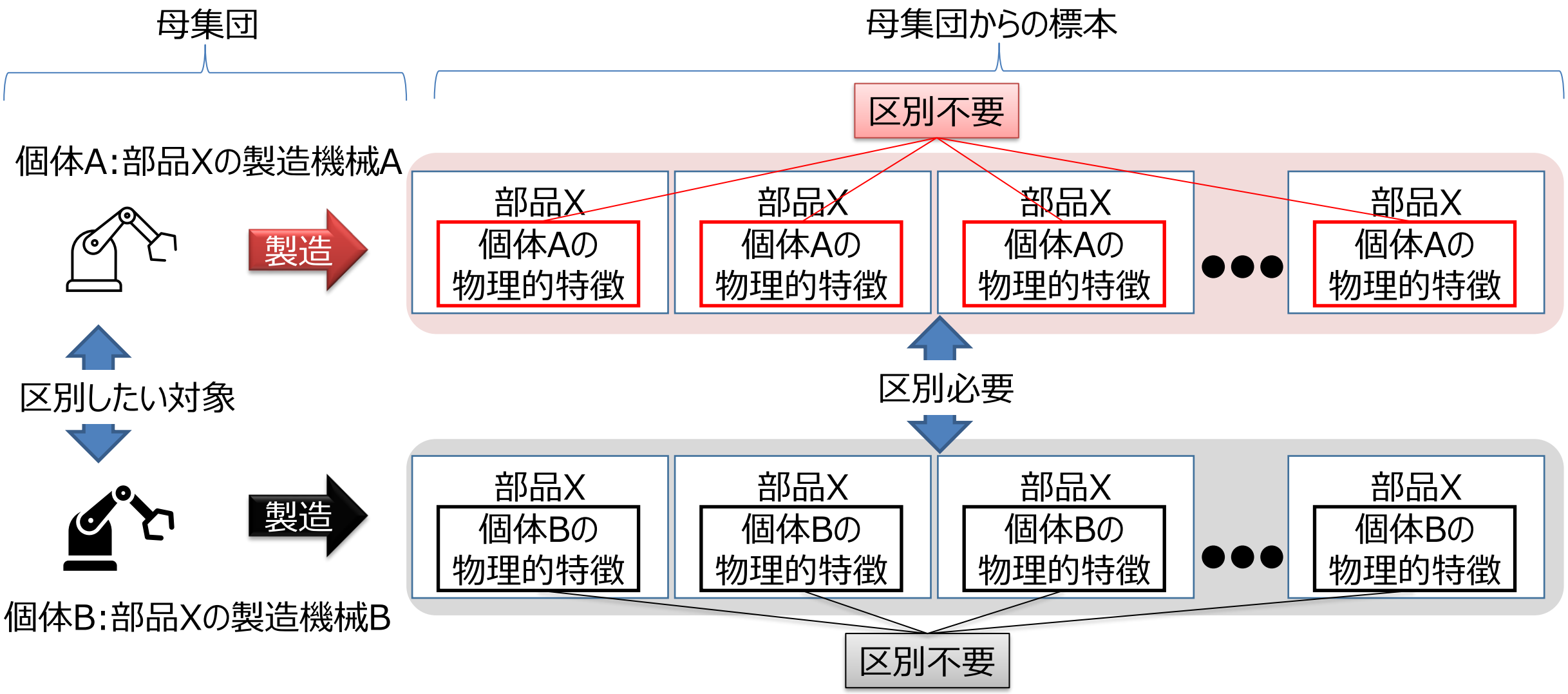


ベルヌーイ試行

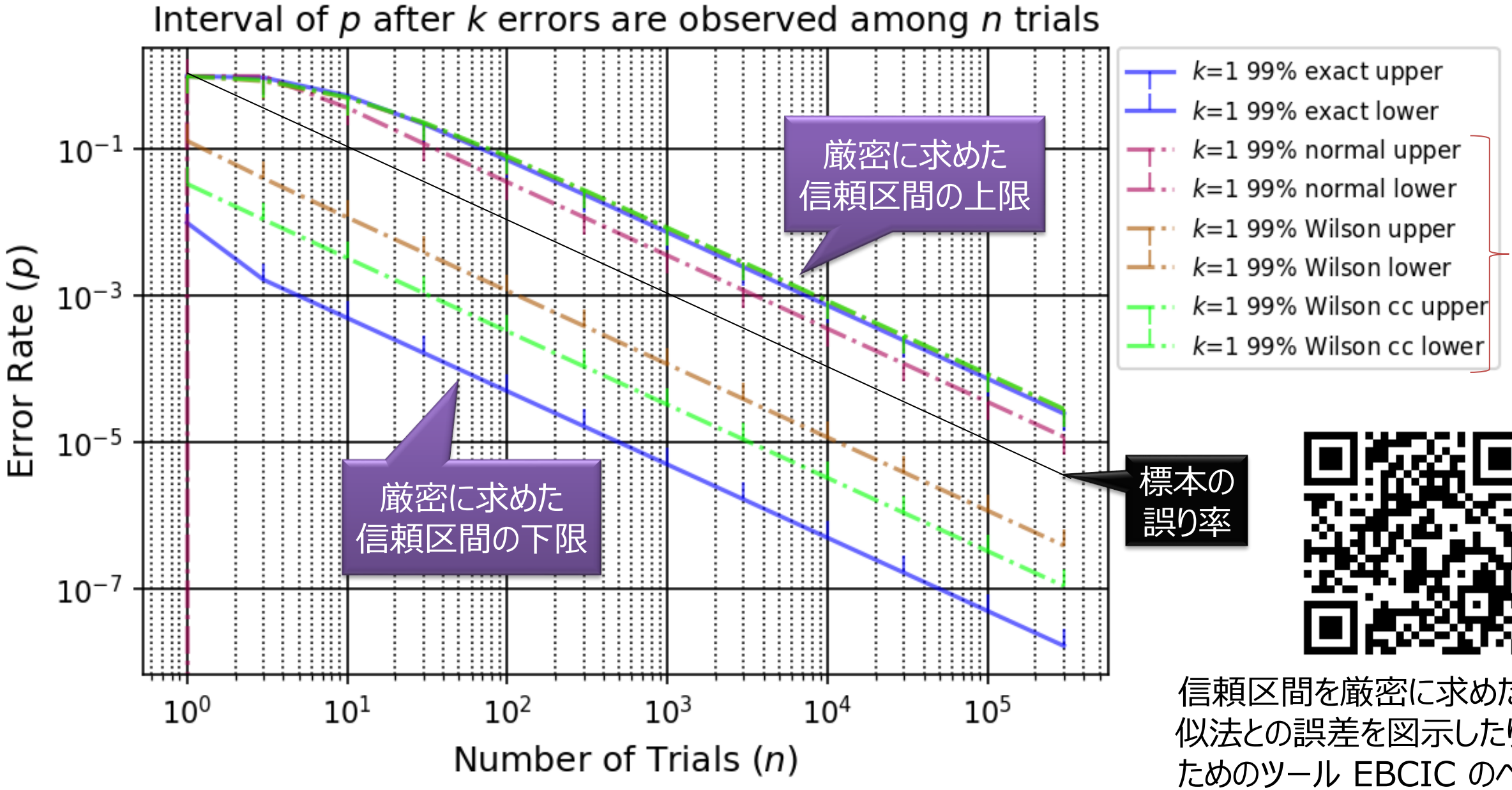
- 試行の結果は２種類（成功または誤りのいずれかなど）
- ２種類の試行結果の確率は試行を通してそれぞれ一定
- 各試行は独立

製品群/部品群などを一つの個体と捉えるユースケース

ニーズの例：ある部品Xに不具合が見つかった場合、それと同じ製造機械で生産された部品を特定し回収したい。



近似された手法で計算された信頼区間の誤差



信頼区間を厳密に求めたり近似法との誤差を図示したりするためのツール EBCIC のページ

誤り率の信頼区間を EBCIC を用いて求める方法

Linux/WSLターミナルを用いる場合

PyPI (Python Package Index) ebcic packageのインストール

```
$ pip install ebcic
```

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
```

信頼区間を計算するためのコマンド例:

- 試行回数100回中、誤り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、誤り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、誤り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
```

Jupyter, Jupyter-lab, Visual Studio Code などでも実行可能です。
詳細は以下をご参照下さい。

信頼区間を厳密に求めたり近似法との誤差を図示したりするためのツール EBCICのページ

AI(機械学習)使用の有無による分類と注意点

- 本ガイダンスで対象とする「照合/識別のためのAI(機械学習)」の範囲：
  - 照合/識別に必要となる処理(学習済モデル)をデータセットから自動的に生成する場合。
- 本範囲外：
  - 照合/識別に必要となる処理(信号処理、判定処理など)を人が生成する場合。
  - 例、ルールベースAIのルールを人が生成する場合。

フェーズ毎の注意点

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

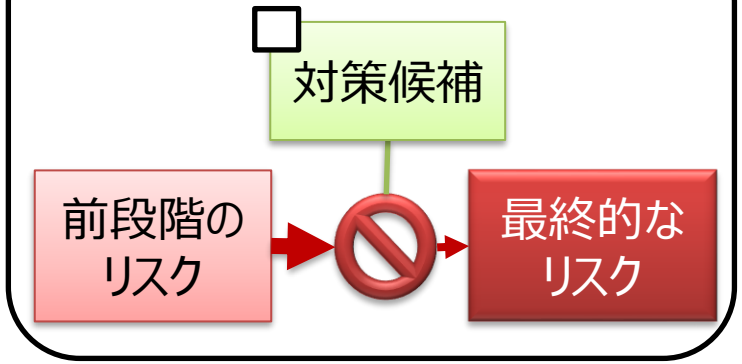
学習済モデル管理時

- 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

2ページ後の図の表記

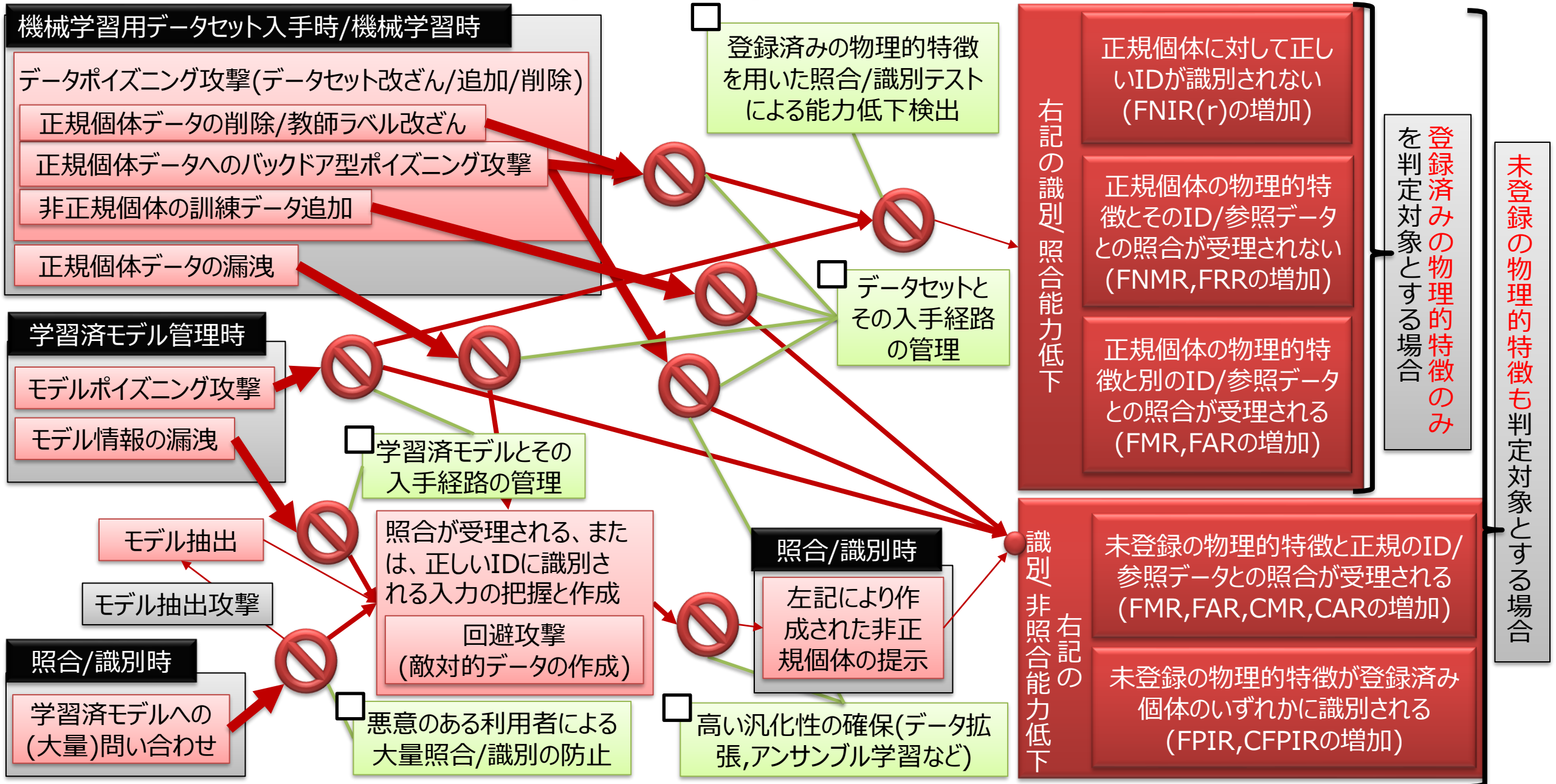


用語については[1]またはそれを微修正したものを使用。
[1] 産総研「機械学習品質マネジメントガイドライン 第 2 版 (revision 2.1.0)」2021.7

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	学習済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、学習済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、学習済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、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	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）

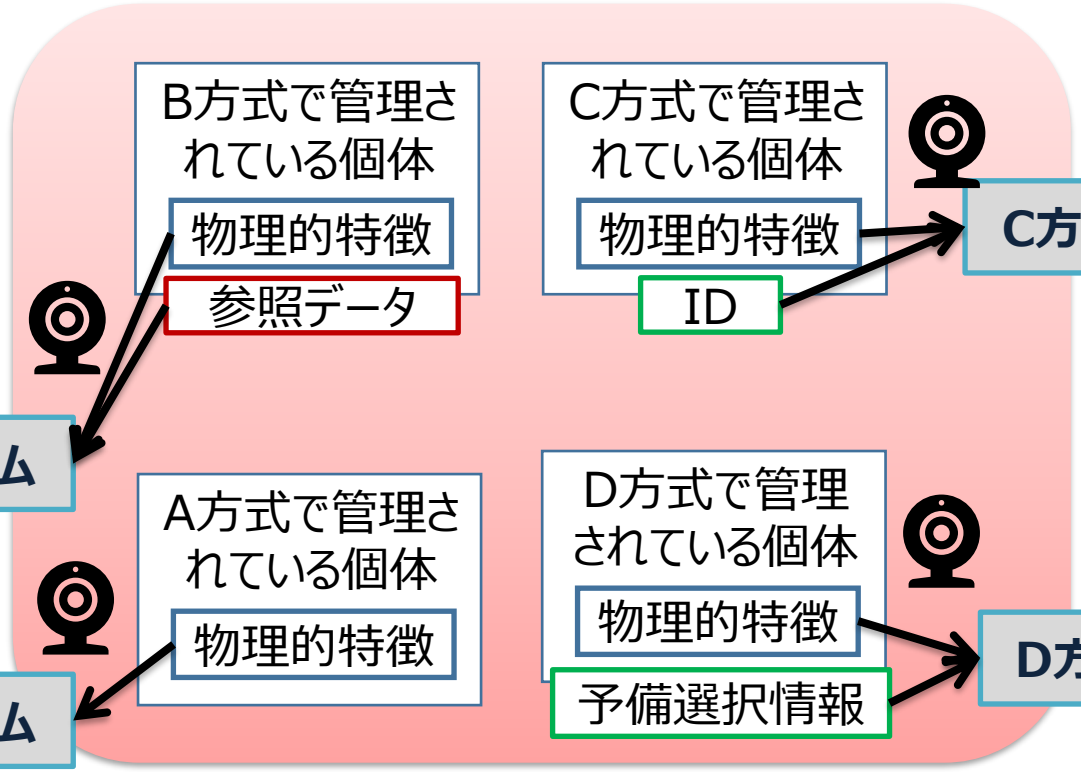
照合/識別にAI(機械学習)を使う場合の注意点



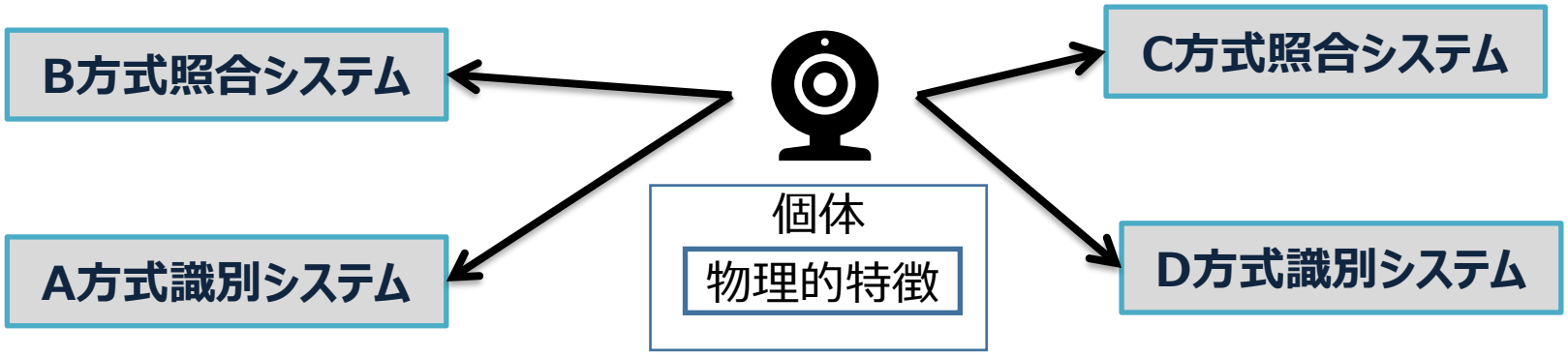
複数の方式を利用する場合

複数の商品や部品を扱い、商品/部品毎に管理方式が異なる場合

個体管理方式に応じてシステムへの入力センサ(カメラなど)の切替が必要



将来、上記のニーズが高まる場合には、用途毎の入力センサ(カメラなど)の共通化が必要となってくる。



まとめ

- 「人工物メトリクスを用いた個体管理技術ガイダンス」について紹介
  - 人工物メトリクスのユースケース毎に、考え方、適用すべき指標、注意点などが異なるため、それらを整理
  - 日本語での用語の辞書としても利用可能
- ユースケースの分類
  - 照合か識別か
    - 照合（個体添付型、データベース記録型）
    - 識別（判定対象限定識別、判定対象非限定識別 による指標の違い）
  - 物理的特徴として個体が有するものを用いる場合/偽造困難な物理的特徴を貼り付ける場合
  - データ取得処理の信用度
  - AI(機械学習)を使用する場合
  - 利用方式が複数の場合
- 指標と図
  - 照合用: FNMR, FMR, FRR, FAR, CMR, CAR, ROC曲線, AUC, DET曲線
  - 識別用: TPIR, FNIR, CMC曲線
  - 判定対象非限定識別用: FPIR, CFPIR, ROC曲線, AUC, DET曲線

ガイダンス紹介ページへのQRコード
https://www.cpsec.aist.go.jp/achievements/artmet

ご清聴ありがとうございました。