生体認証技術の金融サービスへの適用におけるセキュリティ
― ISO 19092の概要―

2023/3/6

日本銀行 決済機構局

山田朝彦

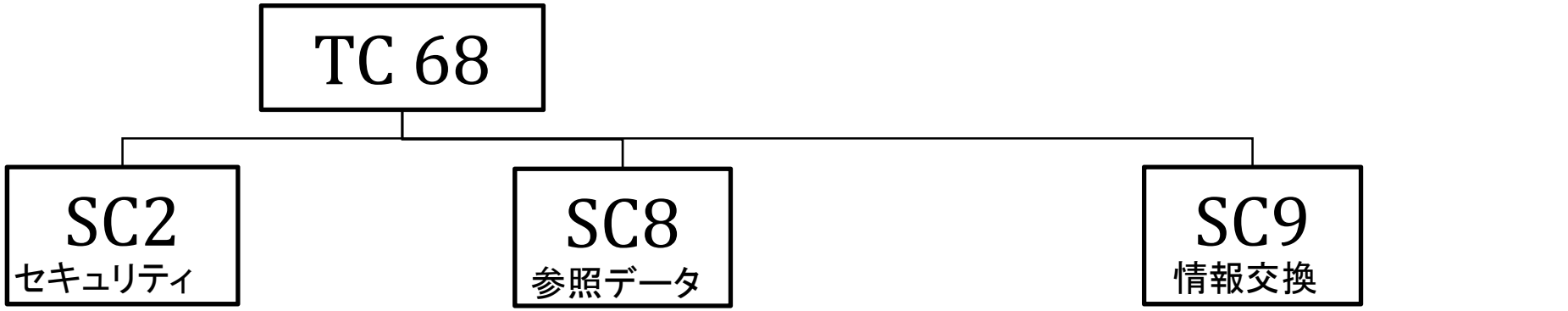
目次

1. ISO 19092とその背景
2. ISO 19092:2023（改訂版）の概要

1. ISO 19092とその背景

ISO 19092

- タイトル：Financial services — Biometrics — Security framework
- 担当委員会：ISO/TC 68/SC 2/WG 13



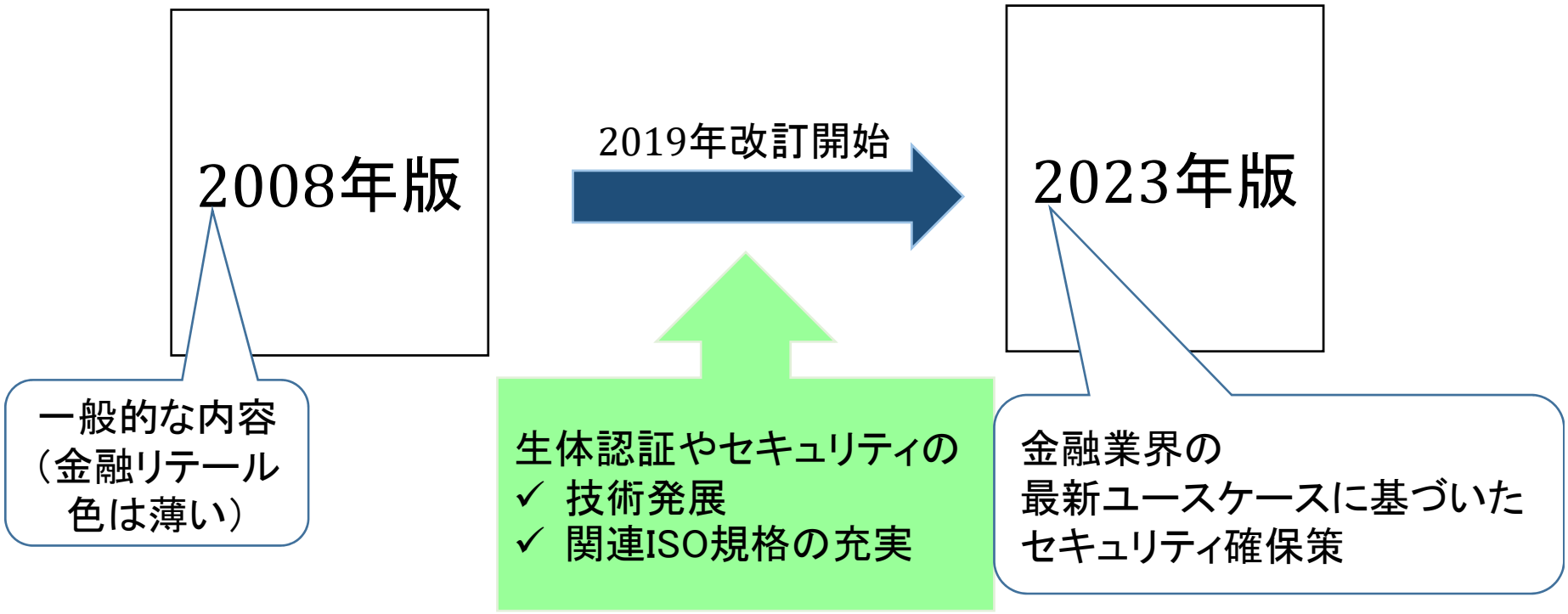
WG 8 :PKI(公開鍵基盤)
WG11:暗号アルゴリズム
WG13:リテール決済のセキュリティ
WG16:TPPのセキュリティ
WG17:デジタル通貨のセキュリティ
WG18:顧客認証技術（e-KYC）
WG19:バーコード決済のセキュリティ

WG 3：DTI（デジタルトークン識別子）
WG 7：NPI(自然人識別子)
WG10：FISN（金融商品短縮名称・略称コード）
WG 11:vLEI（検証可能な取引主体識別子）
SG 5：DWI（デジタルウォーレット識別子）
CAG：Chair's Advisory Group

WG1：セマンティックモデル
WG3： ISO 8583とISO18245の改正
WG4: ISO 20022の改正
TG1：ATICA（カード取引のメッセージフォーマット）
AG1: ISO20022 RAのオーバーサイト

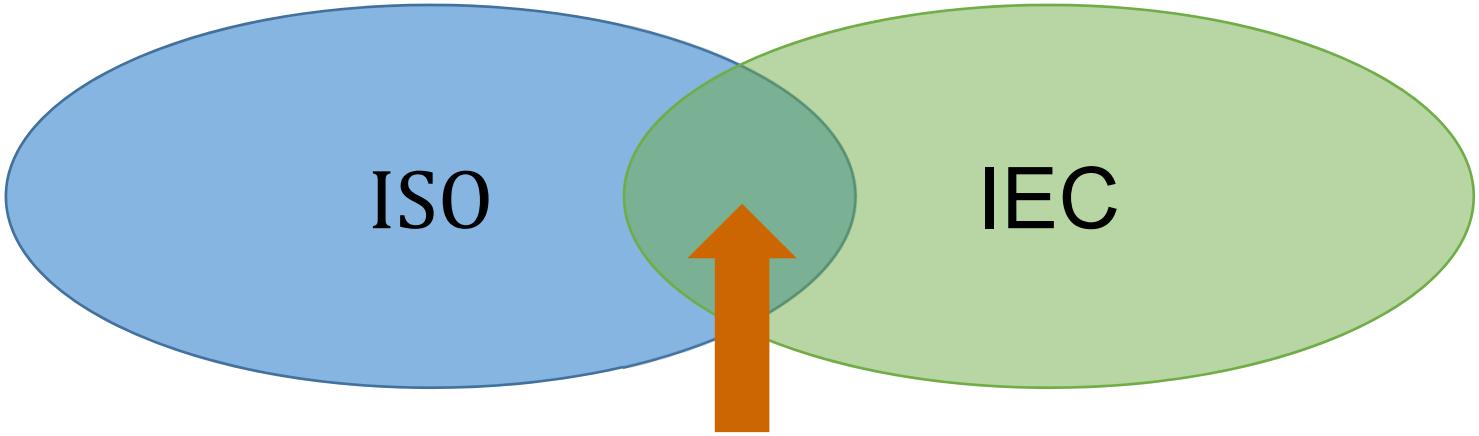
ISO 19092の内容と改訂

- 内容：金融リテール取引で生体認証を利用する際のセキュリティ確保のための枠組みを規定した規格
- 改訂：2008年版から2023年版へ



ISO，IECとJTC 1

- 公的国際標準規格を作成する場
  - ISO：すべての分野（食品安全・農業等を含む）が対象
    International Organization for Standardization（国際標準化機構）
  - IEC：電気及び電子技術が対象
    International Electrotechnical Commission（国際電気標準会議）
  - ISO/IEC JTC 1：ISOとIECの共管で情報技術が対象
    Joint Technical Committee 1（第1合同技術委員会）



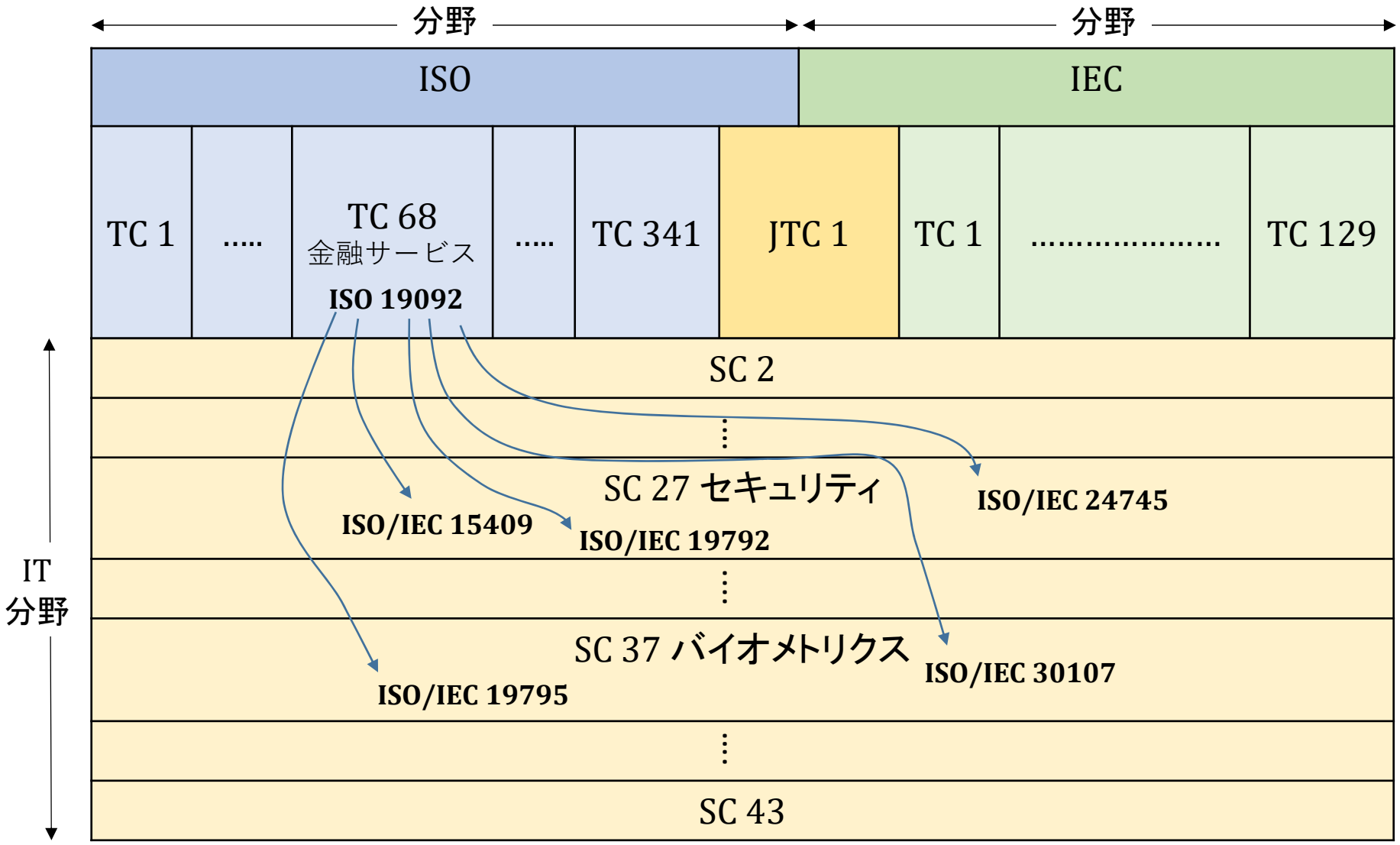
ISO/IEC JTC 1（情報技術）

生体認証とセキュリティの国際標準化

- 生体認証の国際標準化：JTC 1/SC 37*
  Biometrics
  対象：用語、インタフェース、データフォーマット、評価等
- セキュリティの国際標準化：JTC 1/SC 27*
  Information security, cybersecurity and privacy protection
  対象：ISMS、暗号、セキュリティ評価、ID管理・プライバシー等
  （生体認証のセキュリティ含む）

*SC: SubCommittee

公的国際標準化の構造


分野
分野
ISO
IEC
TC 1
.....
TC 68
金融サービス
ISO 19092
.....
TC 341
JTC 1
TC 1
.....
TC 129
SC 2
SC 27 セキュリティ
ISO/IEC 15409
ISO/IEC 19792
ISO/IEC 24745
SC 37 バイオメトリクス
ISO/IEC 19795
ISO/IEC 30107
SC 43
IT
分野

2. ISO 19092:2023（改訂版）の概要

ISO規格とその構造

ISO規格：

活動またはその結果に対する規則や指針（要求事項や推奨事項）を提供

ISO規格の構造（構造は決められている）：

序文（Introduction）

1. 適用範囲（Scope）
2. 引用文書（Normative references）
3. 用語及び定義（Terms and definitions）
4. 記号及び略語（Symbols and abbreviated terms）
5. （以下本文）

適用範囲（Scope）

- バイオメトリクスを使った認証（生体認証）をリテール取引に使うためのセキュリティの枠組みを定める。

生体情報の登録者の確認

生体情報のライフサイクルにわたる管理

生体情報採取のハードウェアに対するセキュリティ要件

生体認証システムのアーキテクチャに関わるセキュリティ要件

生体認証への脅威・脆弱性と対策

本体の構造

5. 金融サービスにおけるバイオメトリクス
6. バイオメトリクス概論（モダリティ、システム）　一般論
7. 金融生体認証システム構築の考慮事項
8. 金融生体認証システムのアーキテクチャ
9. 金融生体認証システムの脅威と脆弱性
10. 金融生体認証システムのセキュリティ要件

金融サービスへの
適用を考慮

附属書A（参考）生体認証環境の脅威と脆弱性

附属書B（参考）生体認証実装シナリオ

附属書C（規定）生体認証セキュリティ管理策チェックリスト

5.金融サービスにおけるバイオメトリクス

- 金融サービス向け生体認証入門
  - 金融サービスにおけるPIN認証の利用シーンと対比して、生体認証を説明
    - 類似点
    - 相違点（長短比較）
    - その結果として検討すべきセキュリティ懸念事項への対策
  - 本書の概要提示
    - システム構成要素
    - 構成要素間の通信
    - セキュリティの脅威に至る脆弱性・リスクとそれらへの対応策
  - 個人デバイスを考慮

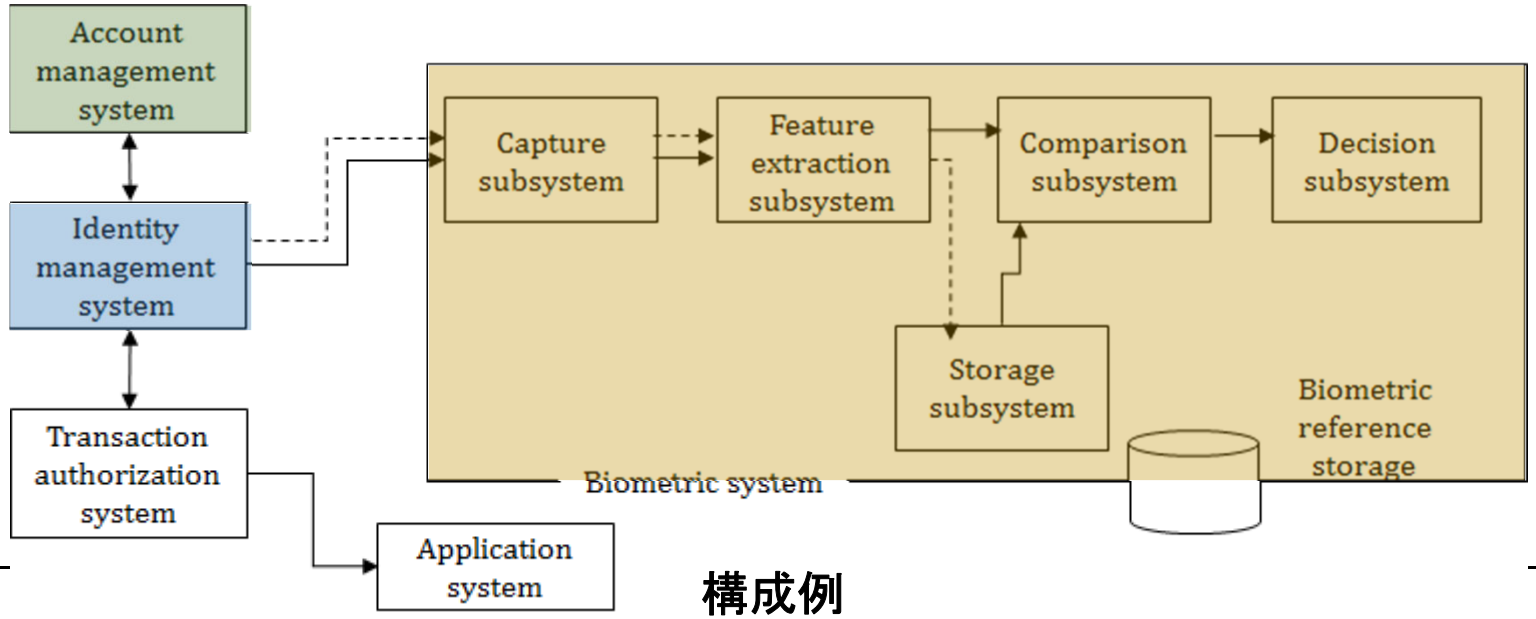
6.バイオメトリクス概論（モダリティ、システム）

- モダリティ

  指紋、声紋、虹彩、顔、署名、静脈、掌紋、キーストローク

- 生体認証システムの構成
  - Id管理システム
  - アカウント管理システム
  - バイオメトリックシステム

利用シナリオは
ユーザ登録（既存）
→生体情報登録
→生体認証



構成例

7.金融生体認証システム構築の考慮事項

設計と運用での考慮事項

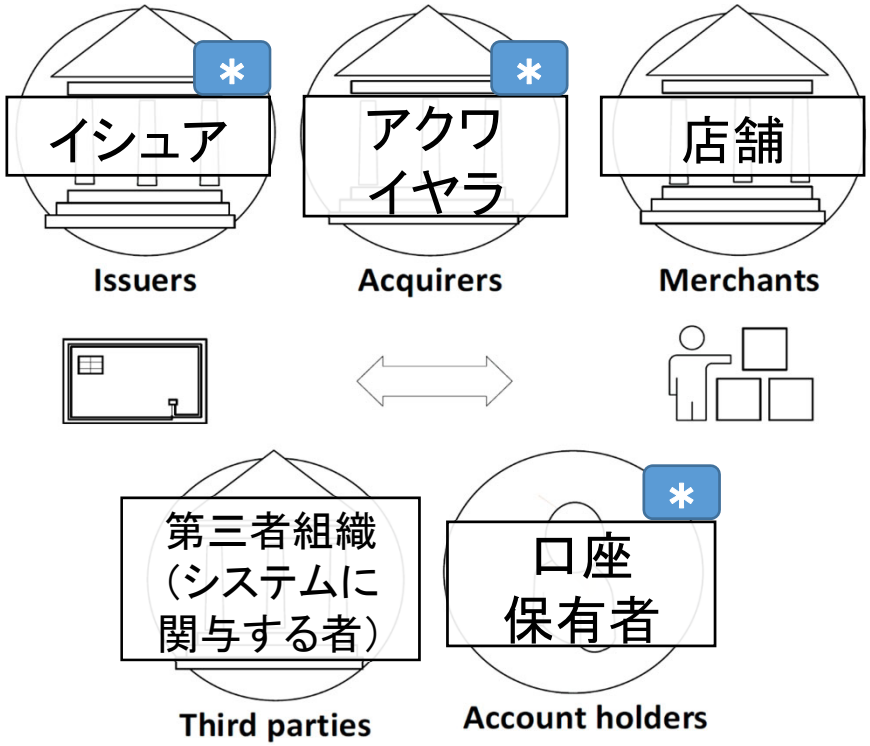
- モダリティの特性
  普遍性・弁別性・受容性・安定性・提示攻撃耐性等
- 照合精度（誤受入率・誤拒否率等）
  影響要因（登録生体情報の採取方法・数、照合の試行回数等）
- 照合精度評価
  被験者の選択、事前トレーニング、製品仕様準拠
  （詳細はISO/IEC 19795シリーズ参照）
- 提示攻撃検知（偽造生体等の検知）
  詳細はISO/IEC 30107シリーズ参照
- 相互運用性
  生体情報データ形式、採取デバイス、モダリティ、セキュリティ保証レベル

8.金融生体認証システムのアーキテクチャ(1)

以下の設定でアーキテクチャを提示

登場人物

＊：生体情報採取デバイスの運用者（いずれか）

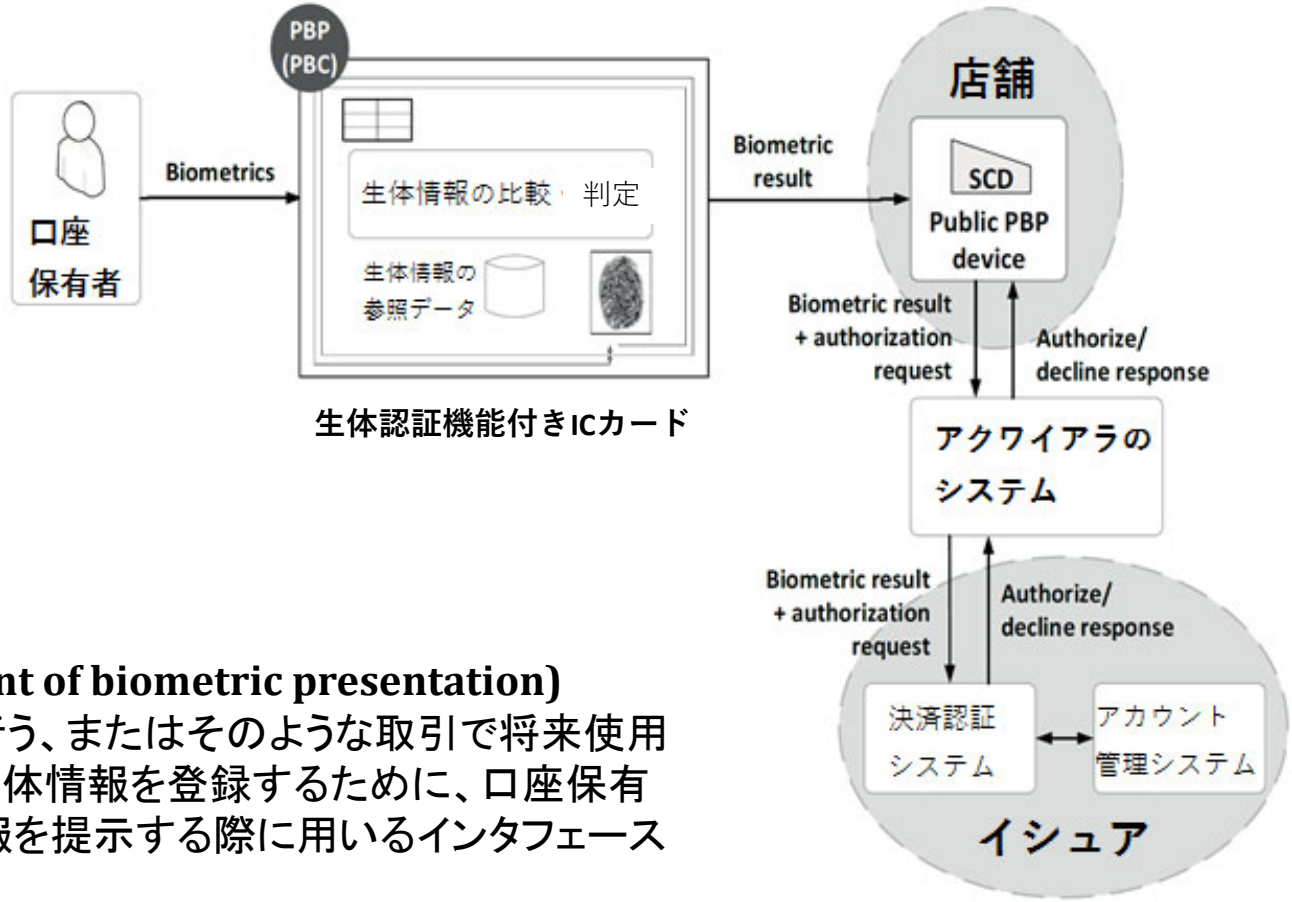


生体情報採取デバイス

- 共有の安全な暗号化デバイス
- 利用者用の生体認証機能付きICカード
- 利用者用の生体認証機能付きモバイル機器
- 共有の生体認証機能付きモバイル機器

口座保有者：事前にId管理システムに登録済

8.金融生体認証システムのアーキテクチャ(2)
例：利用者用の生体認証機能付きICカードの場合

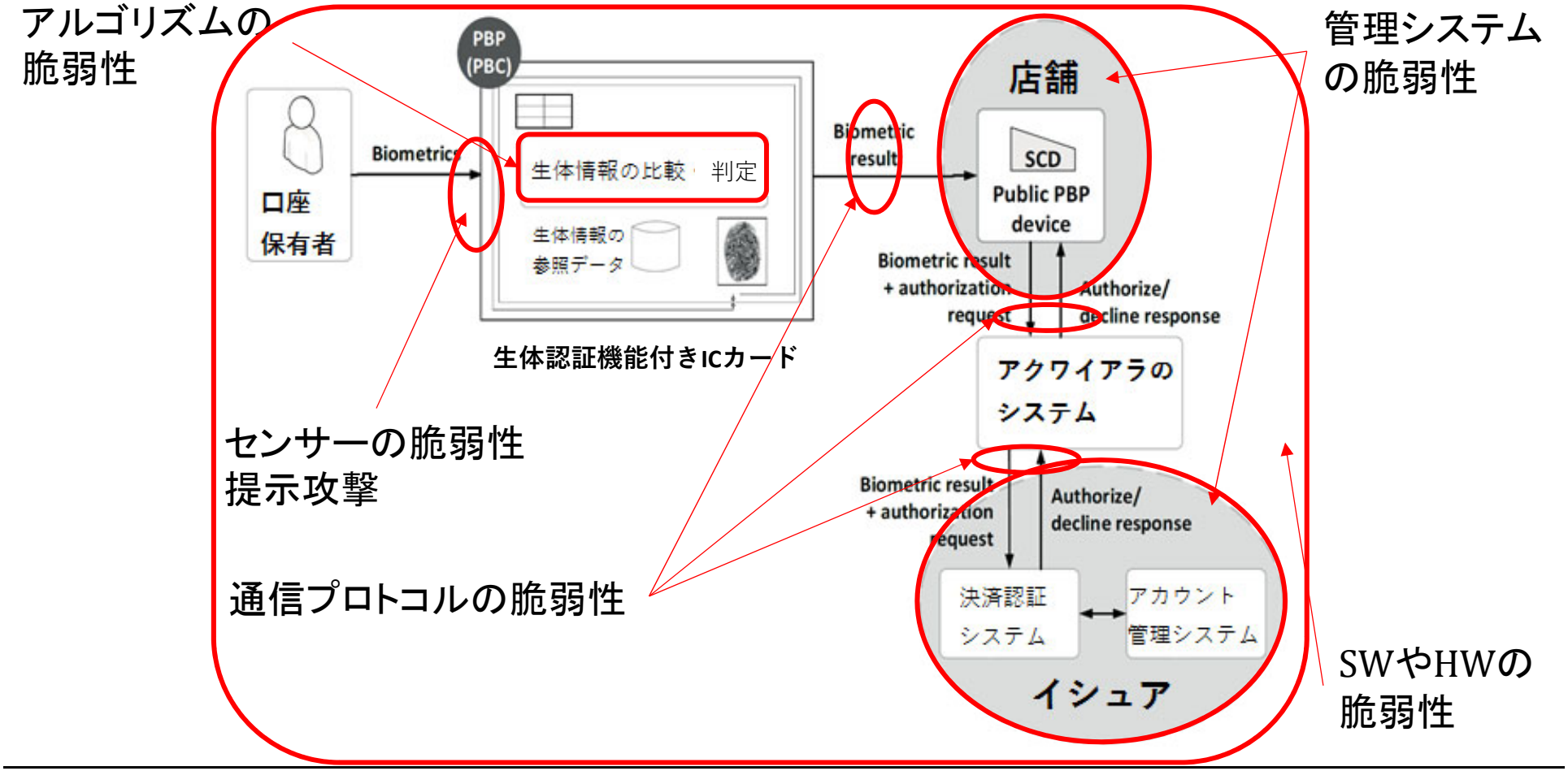


生体認証機能付きICカード

注：PBP (point of biometric presentation)
金融取引を行う、またはそのような取引で将来使用するための生体情報を登録するために、口座保有者が生体情報を提示する際に用いるインタフェース装置

9.金融生体認証システムの脅威と脆弱性

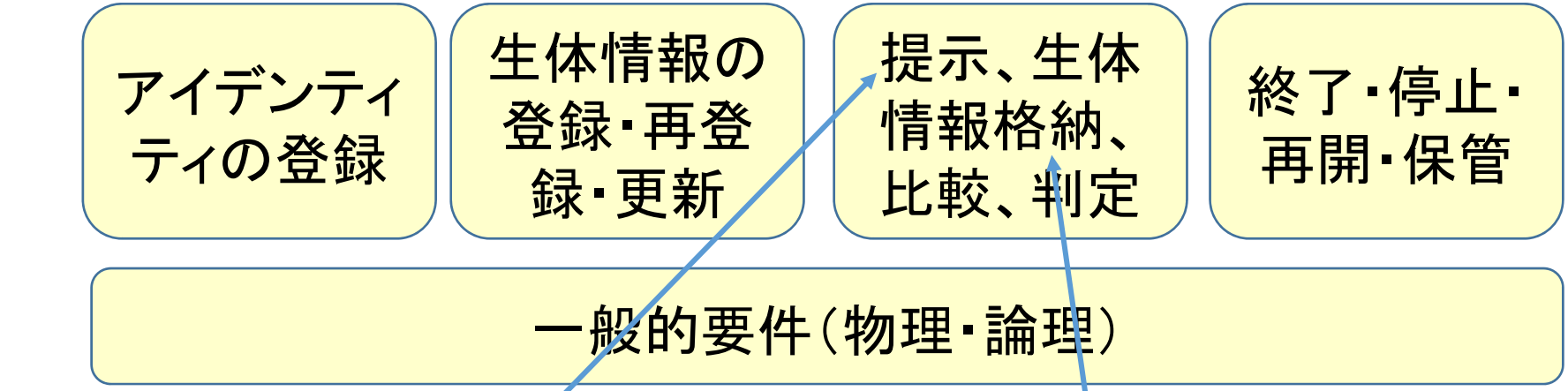
8のアーキテクチャに照らして、一般的な脅威・脆弱性を示す。



注：全ての脅威・脆弱性を示すものではない

10.金融生体認証システムのセキュリティ要件

いくつかの観点に分けて、セキュリティ要件を提示



例）
- 提示攻撃検知機能が備わっていなければならない。
- 人の監視下にない機器では、不正の証拠記録・対応の機能が備わっていなければならない。

例）
- 分割して格納すること（韓国内で実施）も要件の選択肢になっている。

附属書

- 附属書A
  - ICカードとモバイル機器の**脆弱性と緩和策**
- 附属書B
  - ICカード・モバイル機器を使った**実装例**
- 附属書C
  - **セキュリティ管理策チェックリスト**（一般（物理・論理）と登録生体情報のライフサイクル全体）

関連国際標準規格

- ISO/IEC 19792　バイオメトリクスのセキュリティ評価
- ISO/IEC 19795　バイオメトリクスの性能評価
- ISO/IEC 24745　生体情報保護
- ISO/IEC 27553-1　モバイル機器上でバイオメトリクスを使う認証のセキュリティ及びプライバシーの要件：パート1　ローカルモード
- ISO/IEC 30107シリーズ　提示攻撃検知

ご清聴ありがとうございました