# ISO 5158から参照される生体認証等の規格の概要
## ― JTC 1規格を中心に ―

2022/9/15

日本銀行 決済機構局

山田朝彦

# はじめに

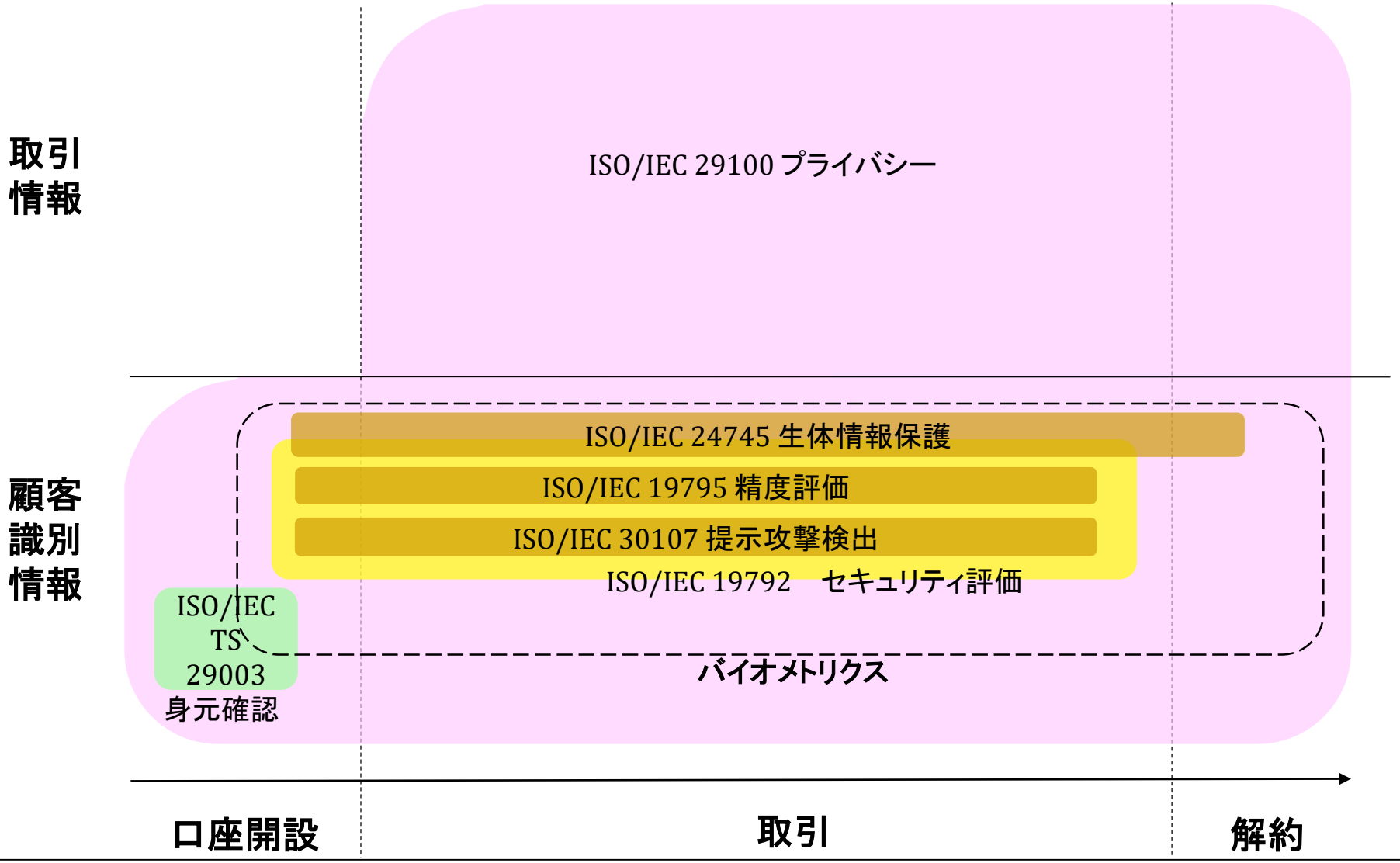
- JTC 1とは
  - ISO（国際標準化機構）とIEC（国際電気標準会議）共管の情報技術（IT）を標準化対象とする合同技術委員会
  - 技術分野ごとに現時点で18のSC（分科委員会）
- ISO 5158から参照されるJTC 1規格
  - ISO/IEC TS 29003:2018 Information technology — Security techniques — **Identity proofing**
  - ISO/IEC 29100:2011 Information technology — Security techniques — **Privacy framework**
  - ISO/IEC 24745:2022 Information security, cybersecurity and privacy protection — **Biometric information protection**
  - ISO/IEC 19792:2009 Information technology — Security techniques — **Security evaluation of biometrics**

**SC 27**
**セキュリティとプライバシー**

  - ISO/IEC 19795 (all parts) Information technology — **Biometric performance testing and reporting**
  - ISO/IEC 30107 (all parts) Information technology — **Biometric presentation attack detection**

**SC 37**
**バイオメトリクス**

# 顧客取引のライフサイクルと参照規格



# ISO/IEC 29100
# Privacy framework

背景:

- 20世紀後半から欧米を中心にプライバシー保護の重要性が増し、プライバシー保護は必須である。
- ICTシステムにおけるプライバシー保護は、PII（Personally Identifiable Information 個人識別可能情報）取扱いの管理に帰着する。

29100は、プライバシー保護の枠組みを規定する。

- PIIへの関与者の分類と役割の定義
- プライバシー保護のためのセキュリティ対策への考慮事項
- ITを対象とする既存プライバシー原則の参照

# ISO/IEC TS 29003
# Identity proofing

背景:

- システムへの利用者登録に際して、身元確認（identity proofing自然人との対応の確認）が必要である。

29003は、身元確認について、以下の内容を規定する。

- 身元確認のガイドライン
- 身元確認レベル（Level of Identity Proofing (LoIP), 1から3の3レベル）の定義
- LoIPの各レベルを達成するための要件

# ISO/IEC 19795
# Biometric performance testing and reporting

背景:

- バイオメトリクスを使った認証は、登録生体情報と認証時提示の生体情報が同一かを判定するので、誤判定がある。
  - 同一でないのに同一と判定(誤受入)
  - 同一なのに同一でないと判定(誤拒否)
- 誤受入や誤拒否の発生率は、バイオメトリック製品の精度を表す指標であり、優劣判断の重要な基準

19795シリーズは、精度評価を規定する規格群

- 誤受入率・誤拒否率など評価指標の定義
- 計画作成・データ収集・記録・分析・報告の指針
- パート1の指針に基づき、種々の場合について、各パートで規定

# ISO/IEC 30107 Biometric presentation attack detection

背景:

- 提示攻撃:バイオメトリクスを使った認証製品への攻撃のひとつ
  - 例えば、指紋付きグミ(グミ指)によるなりすまし試行
- 提示攻撃検知の能力は、バイオメトリック製品の優劣判断の重要な基準

30107シリーズは、提示攻撃検知に関する規格群

- パート1:攻撃の分類、検知メカニズム概要
- パート3:評価のための指標や手法を規定
- パート4:パート3のモバイルデバイスへの適用

# ISO/IEC 19792
# Security evaluation of biometrics

背景:

- バイオメトリクスは、多くは認証に使われる。
- 認証は、セキュリティの重要な機能、よって、セキュリティの観点からの評価も重要である。
  - セキュリティ評価の基準・体系としてCC（Common Criteria, コモンクライテリア）があるが、バイオメトリック製品の評価には不足があった。

19792は、バイオメトリック製品のセキュリティ評価のあり方を規定する。

- バイオメトリック製品の脅威分析の考え方
- CCの体系に不足する、精度と提示攻撃検知の評価の要求事項

# ISO/IEC 24745
# Biometric information protection

背景:

- 生体情報は、個人に固有の情報、PIIでもある。漏えいすると、なりすましの原因にもなる。
- 生体情報の保護は、プライバシー・セキュリティの両方の観点から重要である。

24745は、生体情報保護のための要求事項や対策を規定する。

- 生体認証システムモデルの分類と各モデルの脅威分析とセキュリティ要件
- 生体情報とアイデンティティ情報の関連付けに対するセキュリティ要件
- 生体情報と関連するプライバシー保護の指針

# ISO 19092
# Biometrics — Security framework

- 金融サービス向けバイオメトリクスのセキュリティ要件を定めた規格（現在改訂中（FDIS段階））
- 2008年版は金融業界への適用を考慮しない一般的な内容だったが、改訂版は、金融サービスにおける生体認証モデルやそのセキュリティ要件を含んだ内容になっている。

一般論
- バイオメトリクスの技術概説
- 技術面の分析

- バイオメトリクスを使った認証システムの構造
- セキュリティ分析
- バイオメトリクスを使った認証システムのセキュリティ要件（運用も含む）

金融サービスへの適用を考慮

ご清聴ありがとうございました