生体認証における
セキュリティ評価と国際標準化

2016年11月17日

産業技術総合研究所
山田朝彦

本講演での「生体認証」

- Biometric verification(1:1)
- Biometric identification(1:n)は含まない。

本講演での「セキュリティ評価」

セキュリティ評価とは

- 誰（甲）のためのか

  A) 特定の組織、B) 不特定であるが目的・用途を同一とする組織（群）、C) 上記以外

- 誰（乙）が評価するか

  開発者（第一者）、調達者（第二者）、独立評価者（第三者）

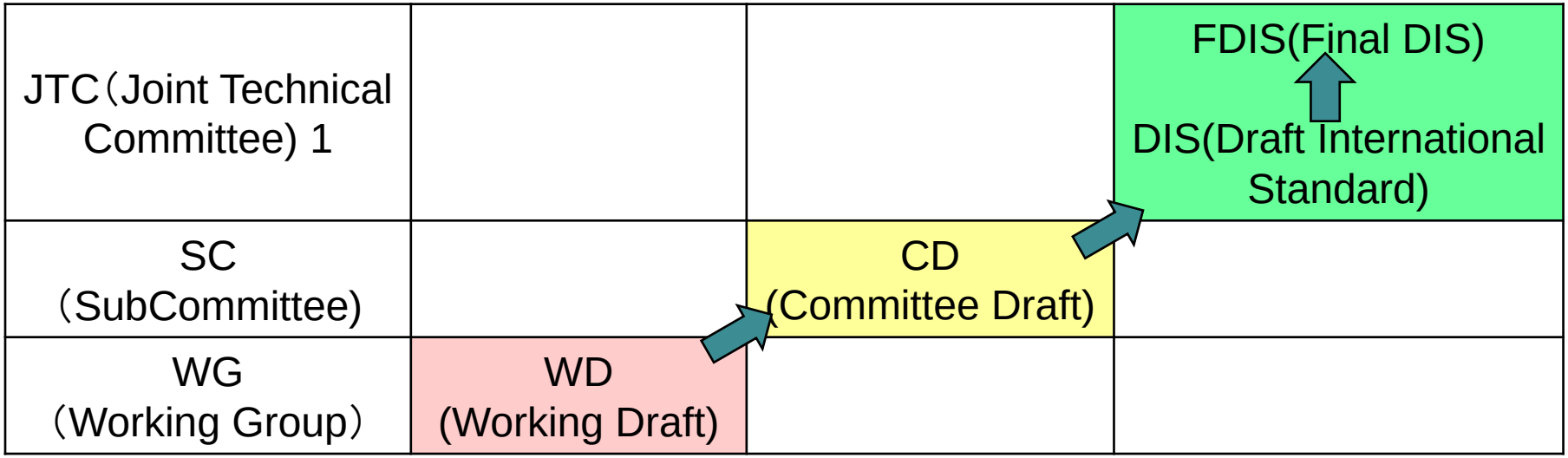
- 評価基準は誰が作るか

  甲、乙、その他

乙＼甲	A	B	C
開発者	○	○	○
調達者	○		
独立評価者	○	○	○

本講演の「国際標準化」

- 国際標準化
  - デファクト標準
  - デジュール標準
    - **ISO（ISO/IEC JTC 1/SC 27（セキュリティ）, SC 37（バイオメトリクス））**
    - ITU
    - IEEE



目次

1. ITセキュリティの評価
2. バイオメトリクスのセキュリティ評価（第1期（英米））
3. ISO/IEC 19792
4. SC 37における関連する国際標準化
5. バイオメトリクスのセキュリティ評価（第2期（欧州））
6. 日本における取組み
7. バイオメトリクスのセキュリティ評価の国際標準化

1．ITセキュリティの評価

CC（ISO/IEC 15408）とは

- 1996年

  CCDB(Common Criteria Development Board)がCC Ver.1を発行

  “**Common Criteria for Information Technology Security Evaluation**”

- 1999年

  ISO/IEC JTC 1/SC 27でISO/IEC 15408として国際標準化

  “Evaluation criteria for IT security”

- CC及びその運用制度で
  第三者による客観的なセキュリティ評価が可能になり、
  IT製品が
  - 適切なセキュリティ機能を持っていること
  - セキュリティ機能が正しく実装されていること

  が保証される。

CC（ISO/IEC 15408）の構成

- パート1: 概説と一般モデル (Introduction and general model)
- パート2: セキュリティ機能要件 (Security functional requirements)
- パート3: セキュリティ保証要件 (Security assurance requirements)

パート2とパート3は、要件のカタログ集。

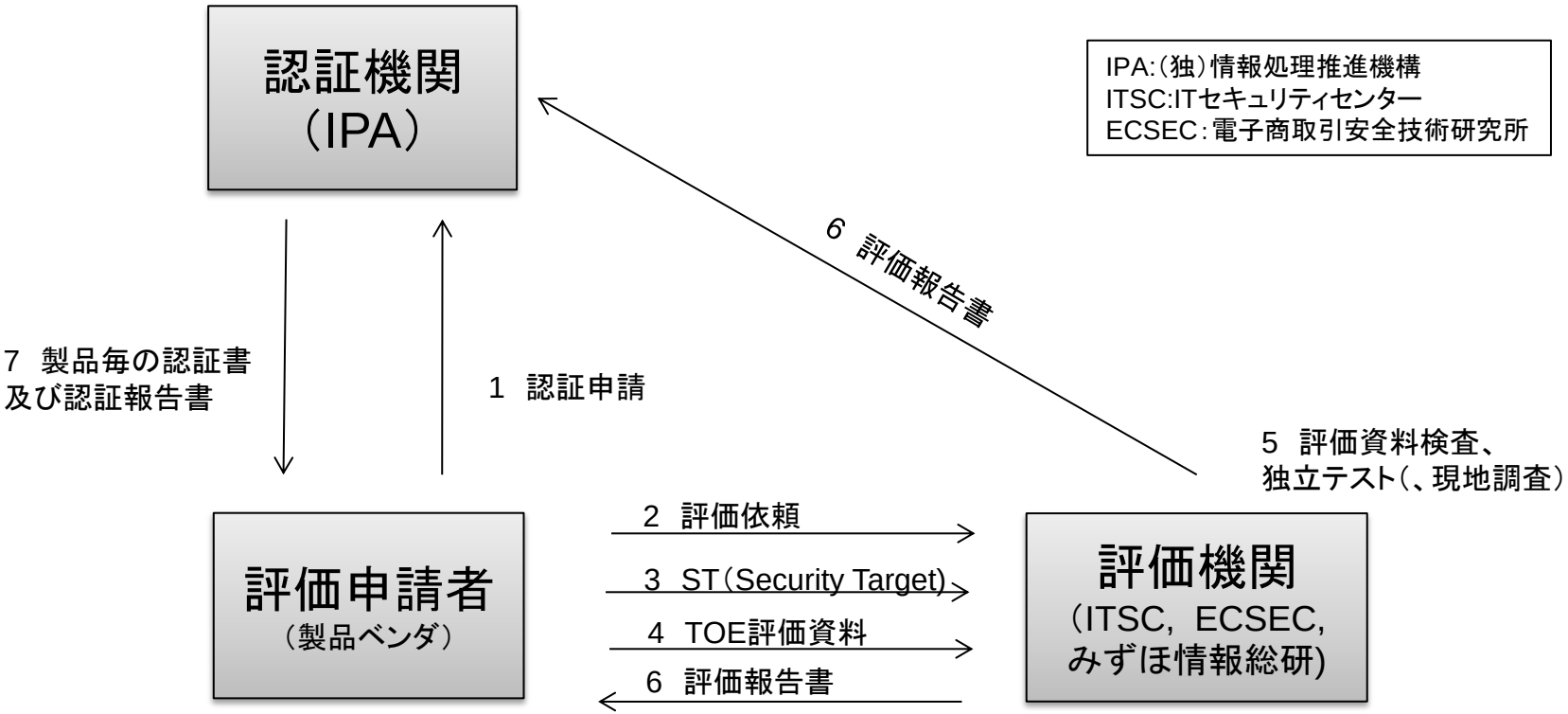
開発者は、評価対象の製品（Target Of Evaluation（TOE））に対する要件を、パート2とパート3から抽出し、セキュリティ設計仕様書であるSecurity Target（ST)を作成する。

評価者は、評価方法を定めたCEM(ISO/IEC 18045)に基づいて、ST及びTOEを評価する。

CEM: “Common Methodology for Information Technology Security Evaluation”

ISO/IEC 18045: “Methodology for IT security evaluation”

CC評価・認証


認証機関
（IPA）
IPA:（独）情報処理推進機構
ITSC:ITセキュリティセンター
ECSEC：電子商取引安全技術研究所
6 評価報告書
7 製品毎の認証書
及び認証報告書
1 認証申請
5 評価資料検査、
独立テスト（、現地調査）
評価申請者
（製品ベンダ）
2 評価依頼
3 ST（Security Target）
4 TOE評価資料
6 評価報告書
評価機関
（ITSC，ECSEC，
みずほ情報総研）

CC認証の相互承認

CC認証は、CCRA加盟国27ヶ国で有効となる。

出典：IPAホームページ

セキュリティ機能要件の例

FIA_UAU.1 認証のタイミング

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: TSF 仲介アクションのリスト]を許可しなければならない。

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

セキュリティ保証要件の体系

セキュリティ機能要件が確実に実装されていることを保証するために、各項目に対して、保証レベル毎に要件を設定する。

保証要件パッケージEAL1からEAL7がある。

<table>
<tr><td></td><td colspan="2">開発者エビデンスを評価者が確認</td><td colspan="2">開発者エビデンスを基に評価者が実施</td></tr>
<tr><td>設計</td><td>ST(セキュリティ設計仕様書)
機能仕様
TOE 設計
セキュリティアーキテクチャ記述</td><td rowspan="4">構成管理証拠資料

構成リスト</td><td></td><td rowspan="3">脆弱性評定</td></tr>
<tr><td>開発</td><td>テスト証拠資料
テストカバレージ証拠</td><td>独立テスト</td></tr>
<tr><td>運用</td><td>配付証拠資料
利用者準備ガイダンス
利用者操作ガイダンス</td><td></td></tr>
<tr><td>保守</td><td>欠陥修正手続き証拠資料</td><td colspan="2"></td></tr>
</table>

2.バイオメトリクスのセキュリティ評価（第1期（英米））

Protection Profile (PP)

- 製品分野毎のセキュリティ要件定義書
  - TOE概要
  - セキュリティ課題定義
    関与者、資産、前提条件、脅威、組織のセキュリティ方針
  - セキュリティ対策方針
    TOEが脅威に対してどう対策するか等
  - 拡張コンポーネント定義
    CCパート2及びパート3の要件に不足があれば定義
  - 要件定義
    セキュリティ機能要件
      セキュリティ対策方針の実現（書換え）
    セキュリティ保証要件
- 製品ベンダ基準でのCC評価は調達者の意に沿うとは限らない。
- 調達者の要求に沿った（PPに適合した）CC評価が必要である。

バイオメトリックPP作成の試み

- 2001年　英国

  Biometric Device Protection Profile

  未完

  豊富な内容。CCパート2のセキュリティ機能要件の使用（詳細化）を試みるが、内容に不足。

- 2007年　米国

  U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments

  U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments

  ともに2010年に失効

  豊富な内容。拡張機能コンポーネントも定義するが、CCパート2のセキュリティ機能要件の使用（詳細化）に問題あり。

CEMの補完の試み

- 2001年　カナダ

  Biometric Technology Security Evaluation under the Common Criteria

  Manfred BrombaのWebページに以下の記載があるが、リンク切れで内容確認できず。

  The methodology used for the first ever evaluation of a biometric technology under the Common Criteria

- 2002年　CCRA

  Biometric Evaluation Methodology Supplement (BEM)

  CEM（旧版）に対する補完

  性能に関する評価方法の記述はあるが、提示型攻撃（なりすまし）に関する評価方法の記述はない。

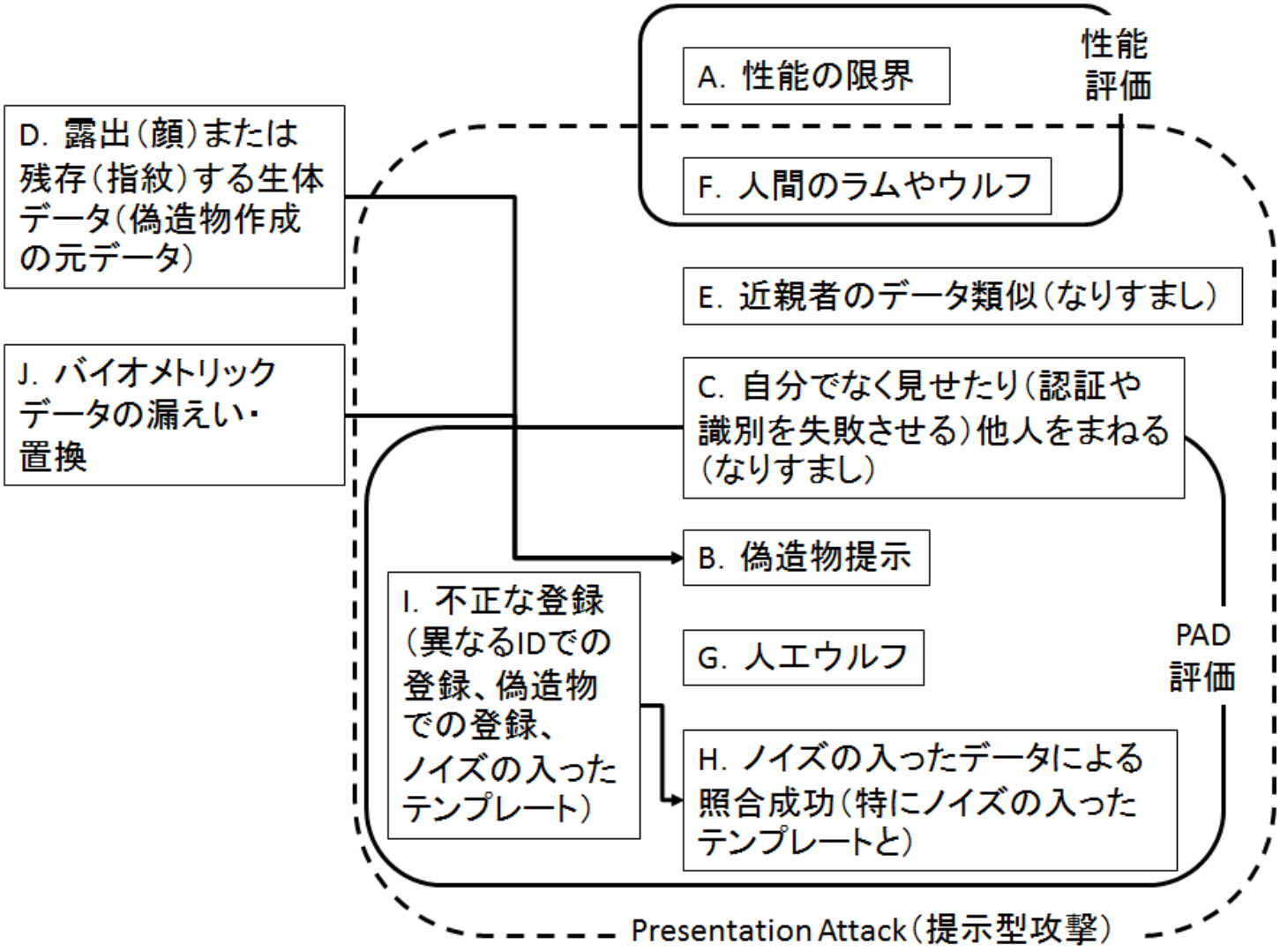
  使用実績はないと思われる。

3. ISO/IEC 19792

ISO/IEC 19792:2009

- タイトル：Security evaluation of biometrics
- 編集者：N. Tekampe（TUViT（ドイツ評価機関））
  副編集者：三村（日立）、大塚（産総研）
- バイオメトリック製品固有のセキュリティ評価を規定（一般のIT製品のCC評価では不足）
  - エラー率（性能）　　ISO/IEC 19795を参照
  - 脆弱性評価　　考慮事項を具体化
  - ~~プライバシー~~
- CCの考え方に沿って評価の枠組みを示したが、要件拡張、CEM補完していない（そのままCC評価には使えない）。
- その後のバイオメトリック製品のCC評価の方向付けをした。

ISO/IEC 19792による脆弱性とその整理



4. SC 37における関連する国際標準化

ISO/IEC 19795（性能評価）

- タイトル：Biometric performance testing and reporting
- パート1（2006年）
  性能評価を実施するに当たっての種々の指針を提示
  - 計画作成
  - データ収集
  - 分析のための指標 (FTE，FAR，FRRなど)
  - 記録
  - 報告
- パート2（ 2007年）
  技術評価とシナリオ評価に対しより詳細な指針を提示
- パート3（2007年）
  モダリティ固有のテスト
- その他パート7まで国際標準化

CC評価適用への課題

- 開発者の性能テスト結果を評価者はどう検証できるか。
- 開発者テストと同程度の精度を求めれば、ほぼ同数の被験者が必要になる。

  ⇨ 多くの被験者を集めるには費用が必要
- 第三者による性能評価があれば良いが、全てのモダリティでの実現は難しい。

  NISTは、指紋・顔・虹彩だけ（ボーダーコントロールで使用するモダリティ）

ISO/IEC 30107（提示型攻撃）

- タイトル：Biometric presentation attack detection
- パート1　Framework（2016年）

  Presentation Attack Instrument（PAI）の類型化、PADメカニズム概要
- パート2　Data formats（DIS段階）

  検知結果を伝達するためのデータフォーマット
- パート3　Testing and reporting（DIS段階）

  評価対象システム（3分類）毎の評価内容

  なりすまし/隠匿のためにPAIが持つべき性質

  PADが望まない提示方法

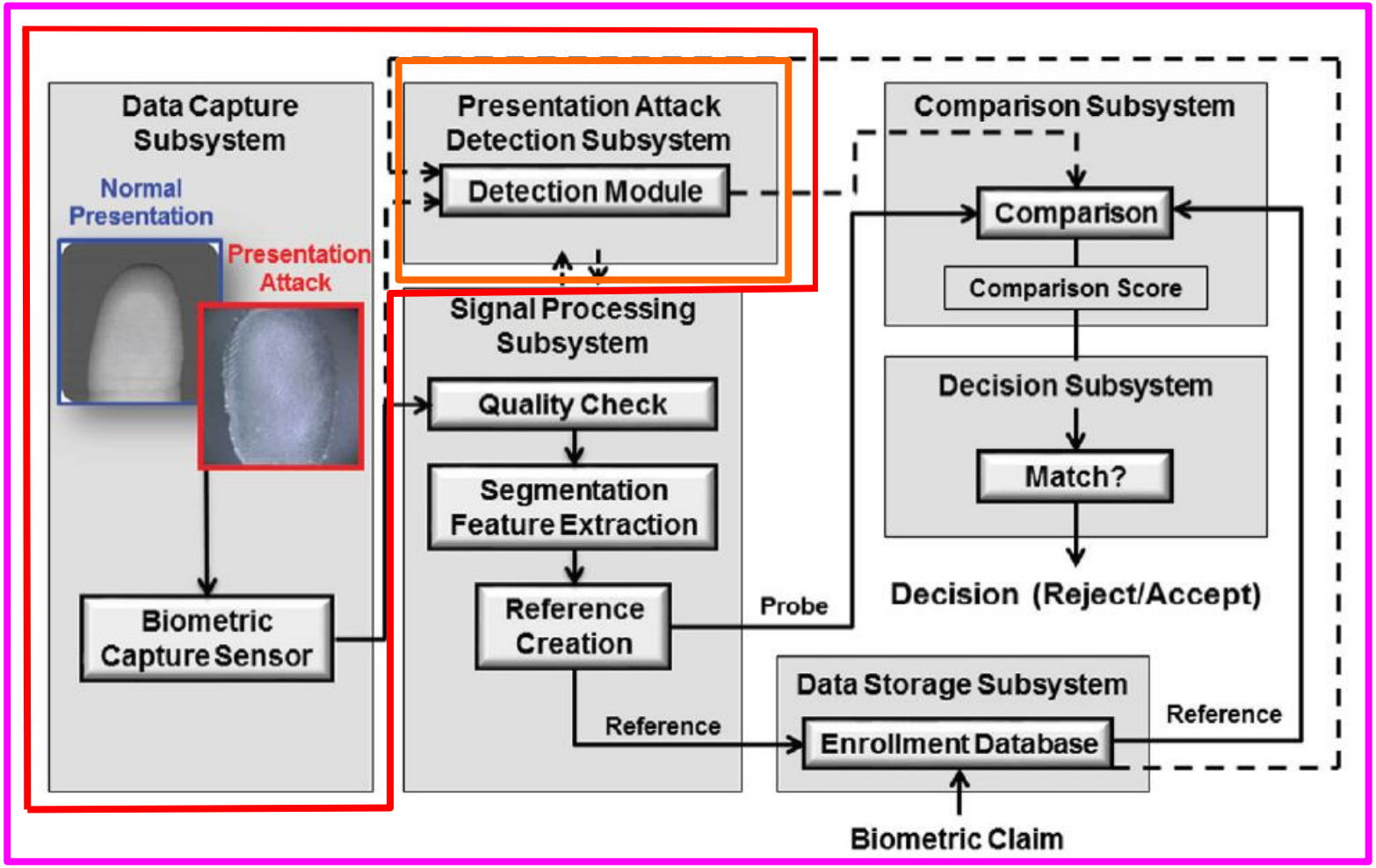
  PAIの作成、PAIを使った評価

  評価メトリクス

    PAIの誤受入率（PAIのクラス毎）、非PAIの誤拒否率

    評価対象システムの3分類毎に提示

PADサブシステムの位置付け（一例）



5.バイオメトリクスのセキュリティ評価（第2期（欧州））

ドイツにおけるバイオメトリックPP作成

- 2008年

  Biometric Verification Mechanism Protection Profile (BVMPP)

  照合メカニズムを対象にしているが、誤受入、誤拒否は考慮されていない。

  使用されたかは不明。

- 2009年

  Fingerprint Spoof Detection Protection Profile (FSDPP)

  TOEは指紋のPADサブシステム

  PADの拡張機能要件、脆弱性評定の拡張保証要件も定義

  サポート文書（CEM補完文書（FSDEG））はSC 27に寄書提出

  Fingerprint Spoof Detection Protection Profile based on Organization Security Policies (FSDPP_OSP)

  FSDPPとほぼ同じだが、FSDPPの脅威を組織のセキュリティ方針として扱っている。

  その結果、保証要件から脆弱性評定を除外している。

  Morpho（現Safran I&S）製品が2013年にCC認証取得

EUのBEATプロジェクト

- Biometric Evaluation And Testing
- 2012年3月から2016年2月（4年間）
- 総費用：約4,744,000ユーロ
- 実施内容：
  - 評価プラットフォームの開発
    スイスIdiapが公開
  - CC評価のための文書開発
    ISO/IEC 19792に基づいたCC評価
      性能の独立テストの実施
      脆弱性評定における新しい攻撃能力計算とその例
    成果は、D6.5として公開、SC 27のISO/IEC 19989（後述）へ寄書提出

BEATの攻撃能力計算

Factor	Value		
	Identification	Exploitation	Note
Elapsed Time			
<= one day	0	0	
<= one week	1	2	
<= two weeks	2	4	
<= one month	4	8	
> one month	8	16	
Expertise			
Layman	0	0	
Proficient	2	4	
Expert	4	8	
Multiple experts	8	Not Applicable	
Knowledge of TOE			
Public	0	Not Applicable	
Restricted	2	Not Applicable	
Sensitive	4	Not Applicable	
Critical	8	Not Applicable	
Window of Opportunity 1) Access to TOE			
Easy	0	0	
Moderate	2	4	
Difficult	4	8	
Window of Opportunity			
2) Access to Biometric Characteristics			
Immediate	Not Applicable	0	2D, 3D（Face）
Easy	Not Applicable	2	Fingerprint
Moderate	Not Applicable	4	Iris
Difficult	Not Applicable	8	Vein
Equipment			
Standard	0	0	
Specialised	2	4	
Bespoke	4	8	

- CEMに基づいてはいるが、各値を調整している。
- 攻撃の識別と実施に分けて計算し、合計値を攻撃能力とする。
- モダリティ毎の攻撃実施の し難さを考慮している。

6. 日本における取組み

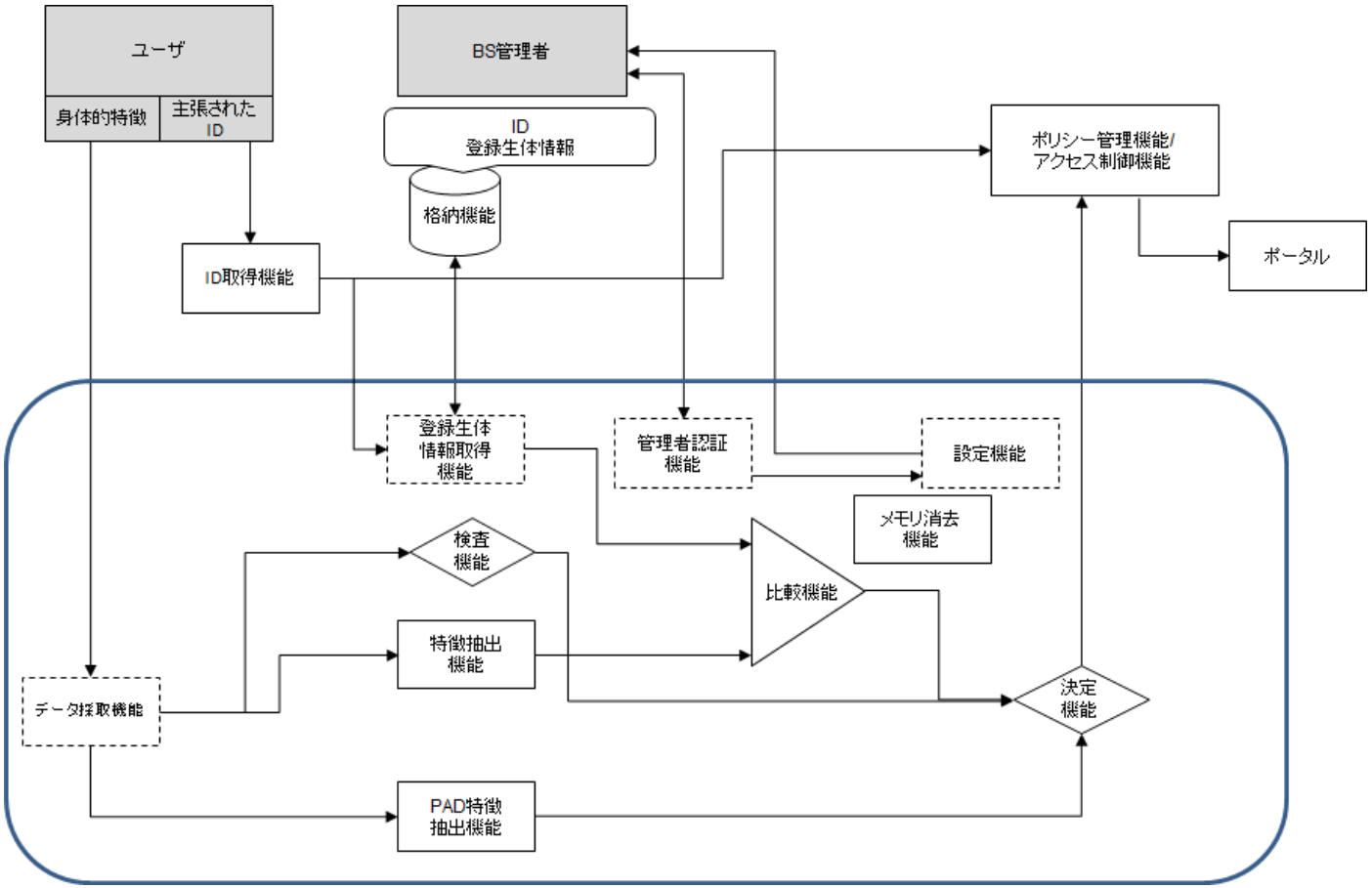
経済産業省事業

- 名称：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））
- 実施期間：2014年4月から2017年3月（3年間）
- 実施内容：
  - 2014年度：ISO/IEC 19792に基づいた照合PPの作成
    性能とPADを評価するためのPP（モダリティ非依存）
  - 2015年度：上記PPを登録も含めたPPに拡張、2016年度の準備
    登録を含むPPは世界初
  - 2016年度：パイロット評価・認証（静脈製品対象）
- 実施体制：JAISA、産総研、OKIソフト、産学から成る委員会

作成したPPのTOE

可能な限り汎用的なTOE

データ採取機能・管理機能はオプショナル、テンプレートDBはTOE外



拡張機能要件（登録）

FIA_EBT.1　登録時の生体情報の検査

FIA_EBT.1.1　TSFは、TSF の利用者による品質が低い登録のための生体情報の使用を防止しなければならない。

FIA_EBT.1.2　TSFは、TSF の利用者による登録のための偽造生体の使用を防止しなければならない。

FIA_EBT.2　生体情報登録失敗率の低い生体情報登録

FIA_EBT.2.1　TSFは、FTE[割付：X]以下で動作する登録のための生体情報の受け入れメカニズムを提供しなければならない。

拡張機能要件（照合）

FIA_BVR.1 精度の高いバイオメトリック照合

FIA_BVR.1.1　TSFは、各利用者にFAR[割付：X]以下、FRR[割付：Y]以下で動作するバイオメトリック照合メカニズムを提供しなければならない。

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合

FIA_BVR.4.1 TSFは、TSF の利用者による品質が低い照合のための生体情報の使用によるバイオメトリック照合の成功を防止しなければならない。

FIA_BVR.4.2

TSF は、TSF の利用者による照合のための偽造生体の使用によるバイオメトリック照合の成功を防止しなければならない。

サポート文書

- PPに適合するTOEの評価のためのCEM補完
- FSDEGやBEATプロジェクト成果を基に作成した。
- 性能の独立テストの評価方法は、統計学を活用して、新たに作成した。

  ①被験者100人で独立テストを実施する。

  ②FTE・FAR・FRRについて、開発者テストの結果に照らして、評価者独立テストの事象発生確率5%未満の結果が出ていないことを確認する。

  ③誤受入・誤拒否について、開発者テストと評価者独立テストで、スコア分布に有意差がないことを確認する。

  ④②または③が確認できない場合は、被験者を追加して独立テストを再度実施する。

7.バイオメトリクスのセキュリティ評価の国際標準化

ISO/IEC 19989の成立まで

- 2011年1月　SC 37会議でISO/IEC 30107 成立
- 2012年5月　上記を受けて、SC 27会議でSP (Study Period) on Security evaluation of anti-spoofing techniques for biometrics が成立
- 2012年10月　上記SPにドイツがFSDEGを寄書提出
- 2014年4月　ドイツが新規作業項目を計画するもエディタ出せず、日本に協力打診
- 2014年6月　日本から新規作業項目提案
- 2014年10月　SC 27会議でプロジェクト成立、山田（産総研）が編集者に就任

ISO/IEC 19989概要

- プロジェクト名： Security evaluation of presentation attack detection for biometrics
- 内容：偽造物検知のCC評価認証に必要な（既存CCには不足する）セキュリティ機能要件・セキュリティ保証要件・評価方法論を定める
- 作成方法：FSDEGを最大限活用して原案作成
- 実際の目標：経済産業省事業の成果反映
- 目標達成への課題：プロジェクトスコープ（PADのセキュリティ評価）と経済産業省事業スコープ（性能評価も含む）の乖離

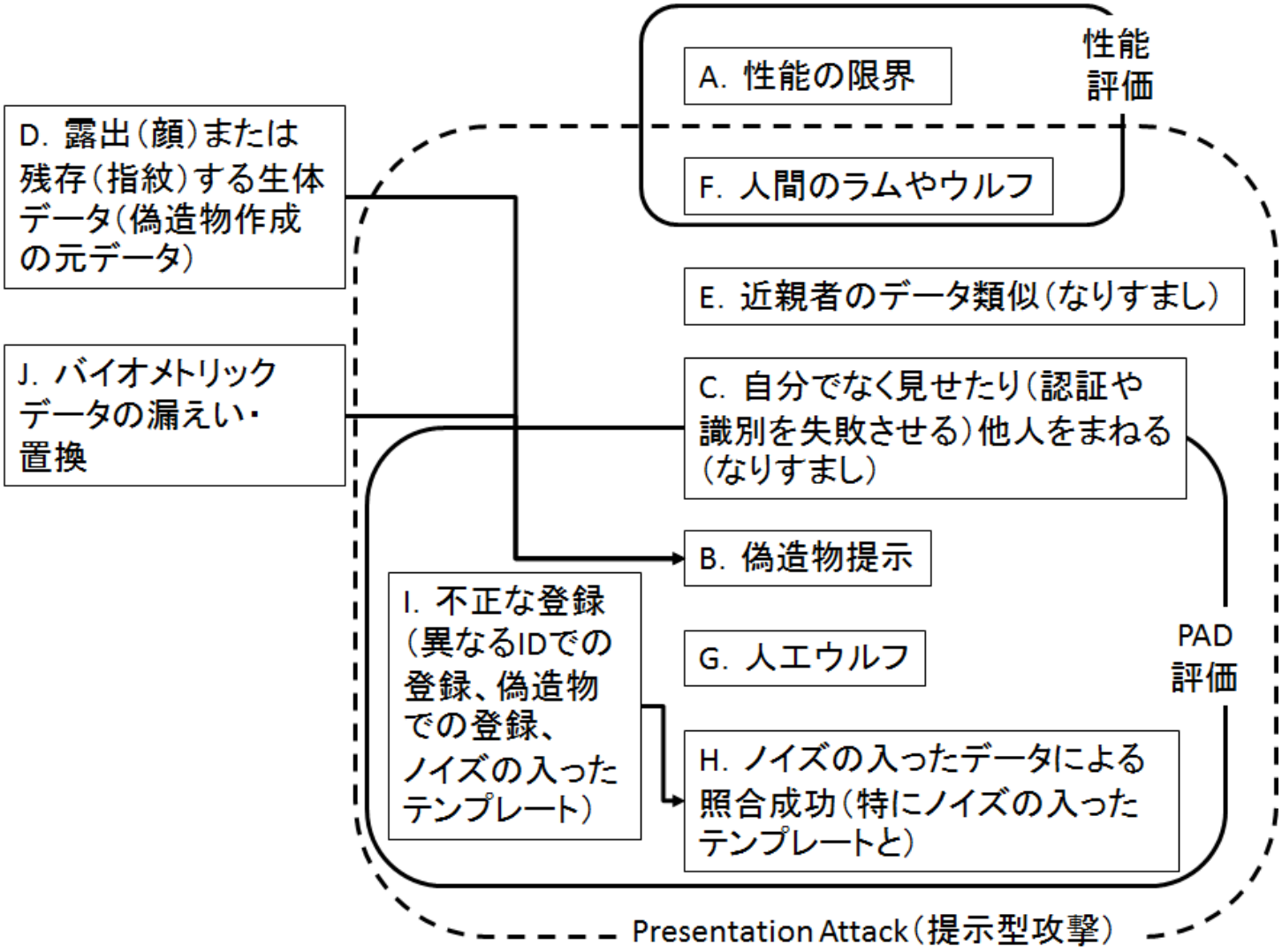
ISO/IEC 19989のスコープ拡張

- 2015年10月SC 27会議にドイツ・フランスからBEAT成果を寄書提出
  日本からSP on Security evaluation of biometric performance based on ISO/IEC 15408 and 18045を提案し成立（ラポータ：山田（産総研））
- 2016年4月SC 27会議で上記SPをISO/IEC 19989に統合
  - タイトルをCriteria and methodology for security evaluation of biometric systemsに変更
  - 2パート分割し、SPの内容をパート1 性能、パート2 PAD
- 2016年10月SC 27会議で3パートに再分割
  - パート1　枠組み、パート2　性能、パート3 PAD
  - 編集者はパート1とパート3が山田（産総研）、パート2がJ. Bringer (Safran I&S)

ISO/IEC 19989の構成

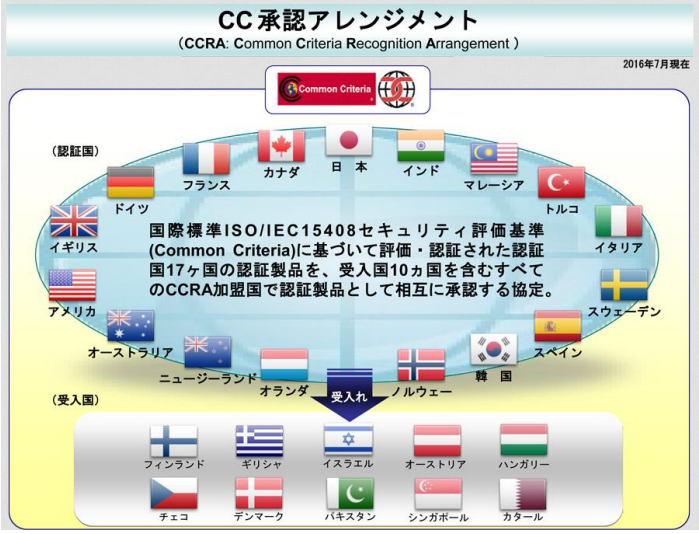
- パート1
  - 用語：15408、18045、30107各パートの用語を参照
  - 評価範囲：19792の示した脆弱性の整理
  - 拡張セキュリティ機能要件：
    - TOEがPADサブシステムの場合←FSDEG
    - TOEがバイオメトリックシステム全体←経済産業省事業PP
  - CEMへの補完←FSDEG、BEAT、経済産業省事業
- パート2
  - 独立テストに関するCEM補完←経済産業省事業
- パート3
  - PADにおけるテストと脆弱性評定の関係←FSDEG、経済産業省事業
  - 攻撃能力計算と攻撃例←BEAT

ISO/IEC 19792による脆弱性とその整理



経済産業省事業のPPを世界に

- IPAの協力で、当該PPをCCRAでcPP（collaborative PP（CCRA加盟国共通のPP））化する活動を開始した。
  - iTC（international Technical Community)
    議長：J. Bringer（Safran I&S）
    編集者：N.Tekampe（TUViT）、山田（産総研）
- cPPはCCRA加盟国で調達要件になる可能性が高い。



出典：IPAホームページ

ご清聴ありがとうございました