NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

バイオメトリクス認証のAPI

セコム株式会社 IS研究所
サイバーセキュリティ・ディビジョン
松本　泰
yas-matsumoto@secom.co.jp
2004 年 8月 26日

バイオメトリクス認証のAPI

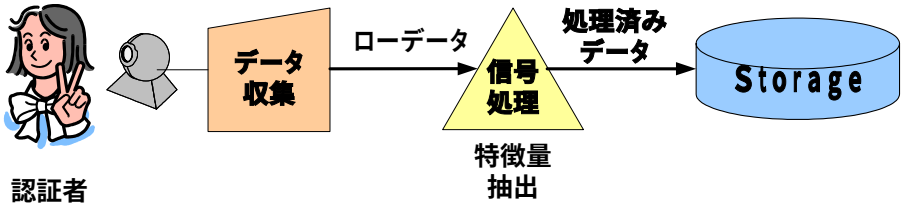
- バイオメトリクス認証の概要
  - バイオメトリクス認証の概要、標準化など
- BioAPIの概要
  - BioAPIを中心としたバイオメトリクス認証のアークテクチャ
- バイオメトリクス認証対応IDカードの実装モデル
  - BioAPIを利用し、カード内で照合を行なうMatch On Card (MOC) の実装モデル
- まとめ

バイオメトリクス認証の概要
バイオメトリクス認証とは

- 3つの認証の分類
  - 本人の記憶に基づくもの（パスワード、PINなど）
  - 本人の所持に基づくもの（ICカードなど）
  - 本人のバイオメトリクス情報に基づくもの（指紋、虹彩など）
- バイオメトリクス認証のふたつのタイプ
  - 指紋や顔など身体的外観に基づくもの（身体的特徴）
  - 音声や署名など行動特性に基づくもの（行動的特徴）
- 登録と認証の概念
  - バイオメトリクス・テンプレートの登録
  - 認証は、テンプレートとの照合により判定する

分類	具体例
身体的特徴	指紋、顔、虹彩、掌形、血管パタン(網膜、掌、甲、指)
行動的特徴	音声、署名

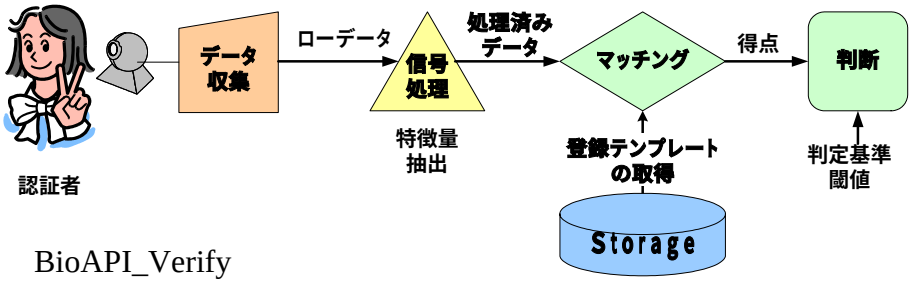
バイオメトリクス認証の概要
バイオメトリクス・テンプレートの登録



BioAPIの関数　BioAPI_Enroll

- バイオメトリクス・テンプレートの登録の手順
  - バイオメトリクス情報の入力
  - 特徴量抽出処理を施し個人を識別する特徴データを生成
  - 登録者の属性と共に保存

バイオメトリクス認証の概要
照合と判定



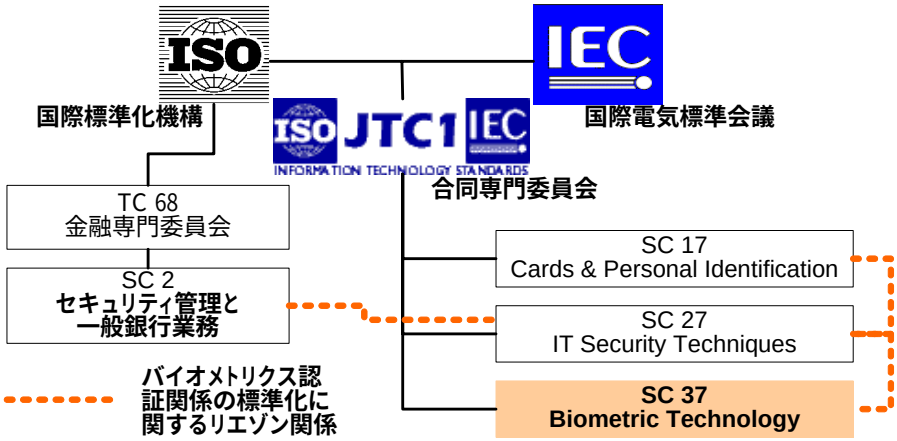
BioAPI_Verify
BioAPI_Identify

認証モード	照合対	説明
Verification	1:1	認証者により申告された登録者の登録テンプレートとの一致／不一致を判定
(Positive) Identification	1:N	認証者が登録済の誰と一致するかを識別
Negative Identification	1:N	認証者が登録済であるか否かを識別

 Page 5

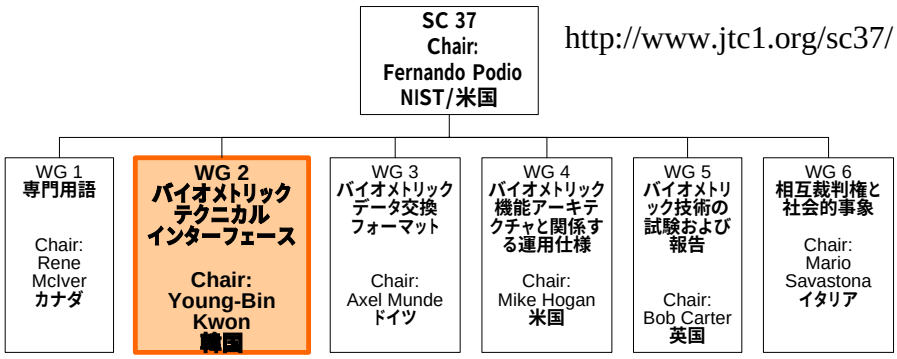
バイオメトリクス認証の概要
バイオメトリクス認証関係の標準化

- 国際標準化
  - 国際標準化機構(ISO)と国際電気標準会議(IEC)の第1 合同専門委員会(ISO/IEC JTC1)内に設置された第37 分科委員会(SC37)が中心



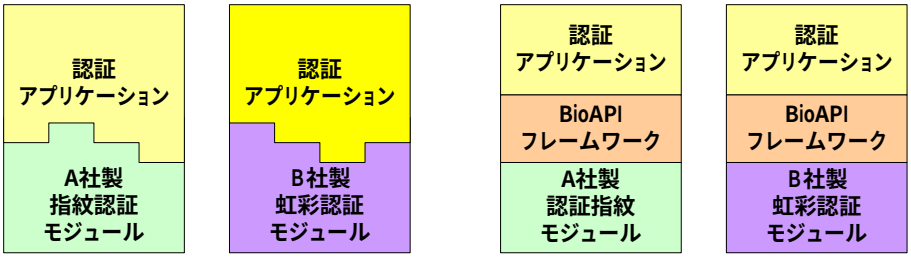
 Page 6

バイオメトリクス認証の概要
標準化動向　ISO/IEC JTC1/SC 37



- SC37　WG2
  - バイオメトリクスコンポーネントやサブシステム間のインターフェースの標準化
  - マルチベンダーシステムに必要なアークテクチャや参照モデルの検討

バイオメトリクス認証の概要
バイオメトリクス認証のＡＰＩ



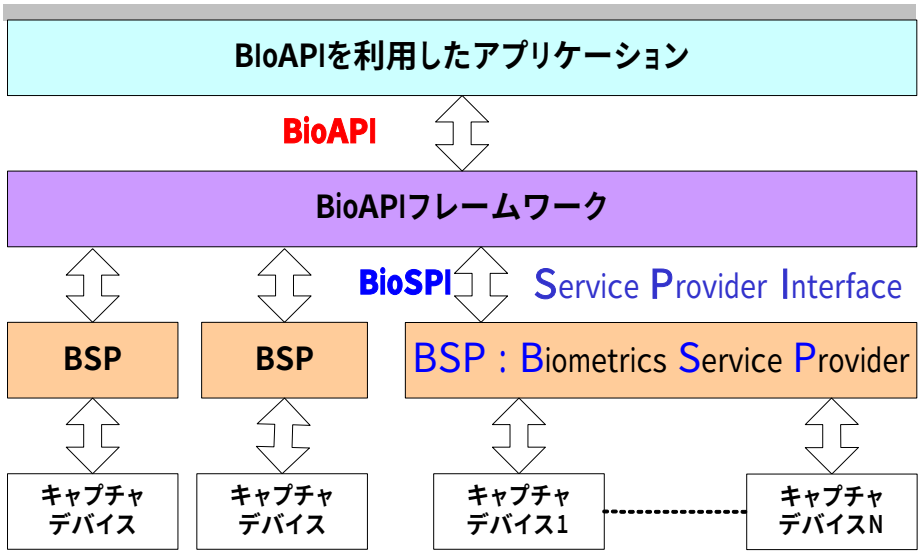
独自APIの世界　　標準化されたAPIの世界

- バイオメトリクス認証のＡＰＩの重要性
  - 多くのバイオメトリクスの認証アルゴリズムや、それぞれのアルゴリズムに依存した登録テンプレートがある中、アプリケーションはそうしたアルゴリズムから独立して設計されるべき。
  - バイオメトリクス認証のＡＰＩの標準化は、アプリケーションの独立性に大きく寄与する。

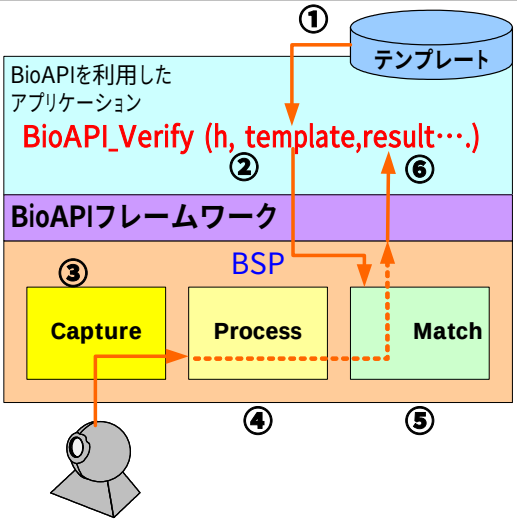
BioAPIの概要
BioAPIの経緯と動向

- 経緯
  - 幾つかの標準API策定の動き→NISTによる統合
  - 1998/4: BioAPI Consortium発足
  - 2000/3: BioAPI Version 1.0
  - 2001/3: BioAPI Version 1.1
    Windows上のﾘﾌｧﾚﾝｽ実装
  - 2002/2: Ver1.1→ANSI化 (ANSI/INCITS 358-2002)
  - 2002/12～: ISO化審議中 (ISO/IEC CD 19784)
  - 2003年10月の最終規格原案(FCD) -> 報告書のﾊﾞｰｼﾞｮﾝ
  - 2005年 IS化の見込み
- 動向
  - 普及はこれから。BioAPI準拠製品は、まだ少ない。
  - 適合性試験などの標準化も並行して進んでいる。

BioAPIの概要
BioAPIフレームワーク



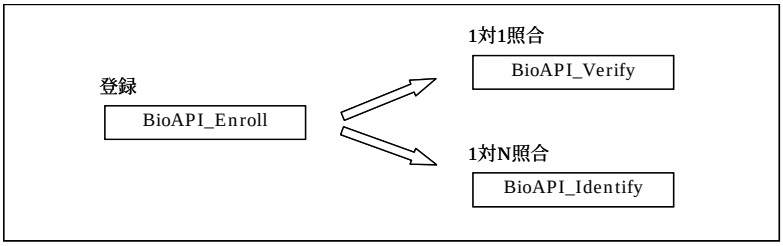
BioAPIの概要
BioAPIの動作



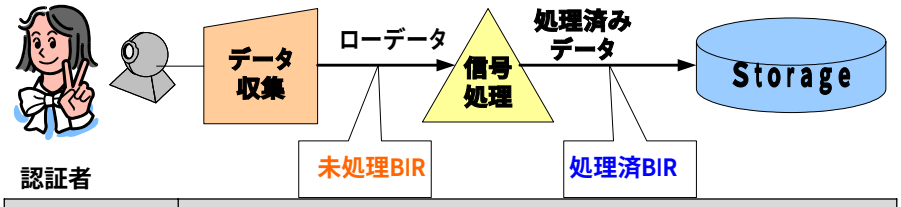
- ① テンプレートを取得する。
- ② BioAPI_Verifyを実行する。
- ③ キャプチャーデバイスからバイオメトリクス情報を取得する。
- ④ 生のバイオメトリクス情報を処理する。
- ⑤ テンプレートとのマッチングを行なう。
- ⑥ マッチング結果を返す。

BioAPIの概要
BioAPIの抽象関数

API名	説明
BioAPI_Enroll	登録を行う。デバイスからバイオメトリクスデータを取り込み、テンプレートを作成する。
BioAPI_Verify	照合(1対1比較)を行う。デバイスからバイオメトリクスデータを取り込み、指定したテンプレートと比較を行って受理・棄却を返す。
BioAPI_Identify	識別(1対多比較)を行う。デバイスからバイオメトリクスデータを取り込み、指定した複数のテンプレートと比較を行い、取り込んだデータに近い順に並べたリストを返す。



BioAPIの概要
BIR (バイオメトリクス情報レコード)



BIRの種類	説明
未処理BIR	センサから取り込んだデータそのもの。顔や指紋などでは画像データ、音声では音声波形データが相当する。
中間BIR	ある程度の処理が行われたBIR。未処理BIRから処理済BIRを生成する途中の段階で存在することがある。中間BIRを使うかどうかはBSPベンダーの実装に依存し、例えばクライアントで1次処理を行い、サーバーで2次処理を行うようなBSPの実装となっている場合、クライアントからサーバーへ伝送されるのが中間BIRである。
処理済BIR	特徴量に変換され、テンプレートとして利用や、テンプレートとの比較に利用できる形式のBIR。

BioAPIの概要
BioAPIのプリミティブ関数

アブスト関数	プリミティブ関数
BioAPI_Enroll	＝BioAPI_Capture＋BioAPI_Process＋BioAPI_CreateTemplate
BioAPI_Verify	＝BioAPI_Capture＋BioAPI_Process＋BioAPI_VerifyMatch
BioAPI_Identify	＝BioAPI_Capture＋BioAPI_Process＋BioAPI_IdentifyMatch

主なプリミティブ関数	説明
BioAPI_Capture	デバイスからバイオメトリクスデータを取り込み未処理BIRへ
BioAPI_CreateTemplate	引数に指定されたバイオメトリクスデータを処理し、テンプレート用の処理済みBIRを作成する
BioAPI_Process	引数に指定されたバイオメトリクスデータを処理し、照合・識別に利用できる処理済BIRを作成する
BioAPI_VerifyMatch	処理済BIRとテンプレートBIRの1対1照合を行う
BioAPI_IdentifyMatch	処理済BIRとテンプレートBIR群の1対多識別を行う

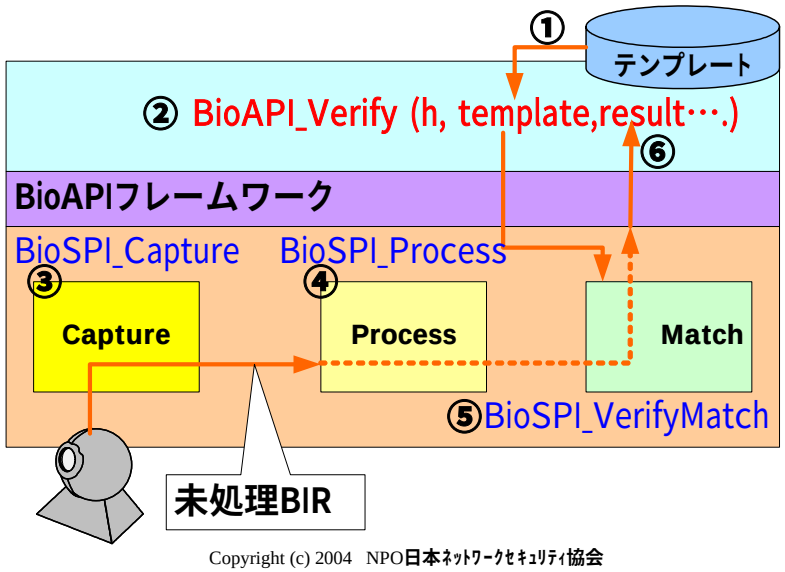
BioAPIの概要
BSPの実装 – 色々なBSP

BSPのタイプ	説明
照合BSP	1対1の照合をサポートし、1対多の識別はサポートしないBSP
識別BSP	1対多の識別をサポートするBSP
キャプチャーデバイス	バイオメトリクス情報の取得だけを行い、処理や照合はサポートしないBSP
照合エンジン	バイオメトリクス情報の処理と1対1照合をサポートするが、バイオメトリクス情報の取得はサポートしないBSP
識別エンジン	バイオメトリクス情報の処理と1対多識別をサポートするが、バイオメトリクス情報の取得はサポートしないBSP

BioAPIの概要
主なSPI 関数

主なSPI 関数	照合	識別	デバイス	照合エンジン	識別エンジン
BioSPI_EnableEvents	○	○	○		
BioSPI_Capture			○		
BioSPI_CreateTemplate				○	○
BioSPI_Process				○	○
BioSPI_VerifyMatch				○	○
BioSPI_IdentifyMatch					○
BioSPI_Enroll	○	○			
BioSPI_Verify	○	○			
BioSPI_Idnetify		○			
BioSPI_Cancel	○	○	○	○	○

BioAPIの概要
照合ＢＳＰの動作

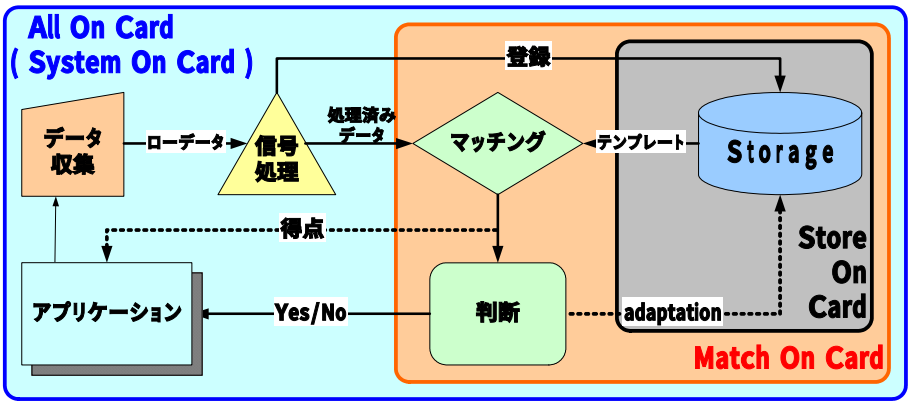


バイオメトリクス認証対応IDカードの実装モデル
バイオメトリクス認証対応IDカードの動向

- 9/11テロ移行、米国において盛んに検討されてきた
- 多くのIDカードプロジェクトが発足しバイオメトリクス認証対応が検討されている

プロジェクト名	プロジェクトの内容
米国防総省(DoD)の共通アクセスカード(CAC)	国防総省職員の身分証明証カード。否認防止署名、署名・認証、暗号の3組の証明書が格納される。2003年11月現在380万枚のCACが配布されている。2004年4月に430万枚の配布が終了する予定。
米国運輸保安局(TSA)のTWIC	TWIC（Transportation Worker Identification Credential）カードは、空港、港湾、長距離トラックなどの運輸関係に従事する全ての職員用の共通アクセス・カード
共通役務庁(GSA)のスマートアクセス共通IDカード	連邦政府関連の3つのビルの入退室管理を1箇所で管理し、指紋のストアオンカード機能(STOC)も採用した身分証明書である。2004年にはPKIの導入を予定している。

バイオメトリクス認証対応IDカードの実装モデル
各種の実装モデル



X9.84 ***Biometric Information Management and Security*** より

バイオメトリクス認証対応IDカードの実装モデル
各モデルの特徴

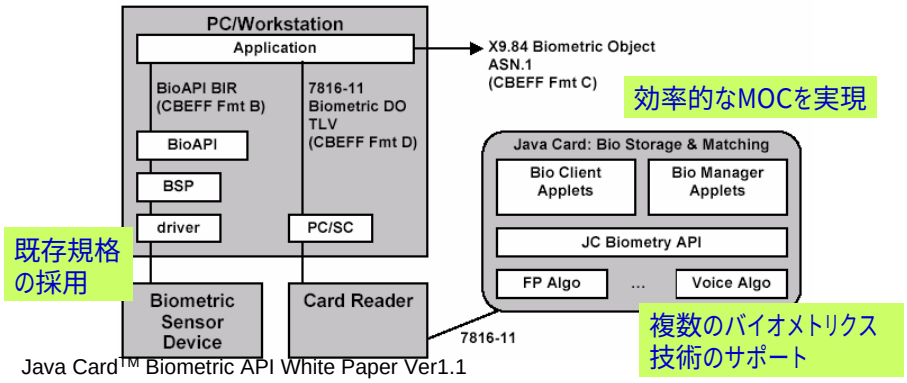
方式	内容	備考
STOC (Storage On Card)	カード上にバイオメトリクス情報（テンプレート）を格納する。 カード外で比較	電子パスポート フィジカルセキュリティ 比較的信頼がおける場所における認証に利用される
MOC (Match On Card)	カード上で比較 カード外にバイオメトリクス情報（テンプレート）を出さない PKIの私有鍵の活性化	ネットワークでの認証 PIN(記憶による認証）をバイオメトリクスによる認証に置き換えたスマートカードであり今後有望な技術。 プライバシ問題に対応
System On Card	カード上でキャプチャを行う	スキャナの一体化は現在のスマートカードでは困難かつ高価。スマートカード以外の携帯デバイスで有効

バイオメトリクス認証対応IDカードの実装モデル
バイオメトリクス認証対応IDカードの要求

- 標準的なIDカードの要求（米国のGSC-ISのバイオメトリクス認証対応の案 -「スマートカード・バイオメトリクス相互運用性研究報告書」より）
  - 複数のバイオメトリクス技術のサポートを必須
  - 技術タイプとベンダーの中立を必須
    - 特定のICカードに依存しない
    - 特定のバイオメトリクス認証技術に依存しない
  - 接触型と非接触型のスマートカードのサポートを必須
  - 多要素認証を必須とする (スマートカード + バイオメトリクス)
  - セキュリティメカニズムをサポートしなければならず、低いセキュリティ環境においても、同様に提供

バイオメトリクス認証対応IDカードの実装モデル
Java Card Biometric APIを利用したMOCモデル

- Java Card ForumのBiometry TFが策定
- 2002/7にVer1.0、2002/8にVer1.1をリリース。
- Java Card上で認証(MOC)を行なう上でのAppletと認証クラスとのインターフェースを規定



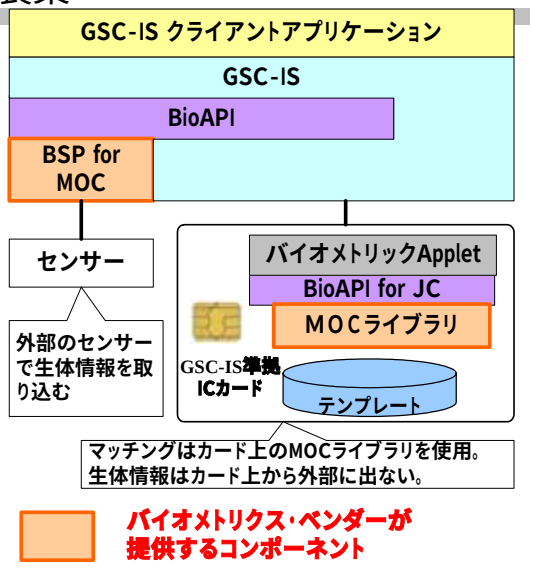
Java Card™ Biometric API White Paper Ver1.1
http://www.javacardforum.org/Documents/Biometry/JCBiometricsAPI_WhitePaper.pdf

バイオメトリクス認証対応IDカードの実装モデル
米国GSC-ISのMOCモデルの実装方針

- 米国GSC-ISのMOCモデルの実装方針
  - 2003年8月に「スマートカード・バイオメトリクス相互運用性研究報告書」を発表。ここで、MOCモデルの実装方針、実装案を示している。
- バイオメトリクス標準の活用
  - MOCにとって重要なバイオメトリクス標準（BioAPI、JCF 2.2 Biometry API、CBEFF）を、できるだけ活用
- 政府スマートカード相互運用性仕様（GSC-IS）の活用
  - GSC-IS基本サービス・インタフェース（BSI）をバイオメトリクスをサポートするために拡張
- バイオメトリクス・ベンダーから中立
  - フレームワークは、特定のバイオメトリクス技術から中立
- 専門技術領域の分離
  - フレームワークは、バイオメトリクス・ベンダーのために統合を単純化し、スマートカード・ミドルウェアの専門知識を要求しない

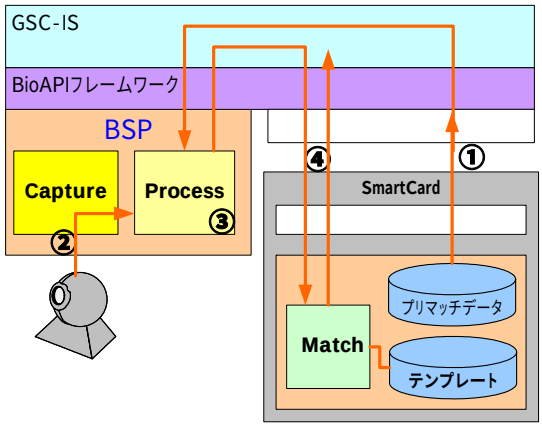
バイオメトリクス認証対応IDカードの実装モデル
GSC-ISのMOCモデル実装案

- 米国 ANSI/INCITS M1が、GSC-ISのバイオメトリクス認証対応を検討。成果として「スマートカード・バイオメトリクス相互運用性研究報告書」を発表
- 特定のバイオメトリクス技術に依存せず、複数のバイオメトリクス技術に対応
- ベンダーの依存性を最小にする



バイオメトリクス認証対応IDカードの実装モデル プリマッチの手法

- プリマッチ
  - 照合をふたつに分け、カード上の照合の計算量を減らす。
- ①BioAPI_DBGetBIRを使ってカードより、プレマッチデータ取得する。
- ②BioAPI_Captureを使ってデバイスから処理前のテンプレートを取得する。
- ③BioAPI_CreateTemplateを使って、プレマッチデータを処理すると同時に、MOCのために処理済みBIRを生成する。
- ④MOCのために処理済みBIRをカードに転送して、カード上で照合を行う。

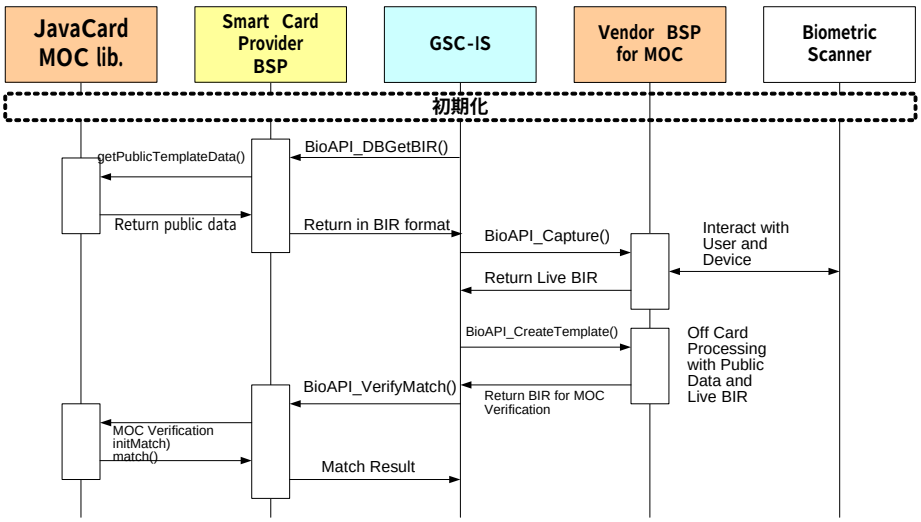


バイオメトリクス認証対応IDカードの実装モデル GSC-ISのMOCモデル実装案 続き

提供コンポーネント	内容
MOCのためのベンダー BSP (BSP for MOC)	MOCモデルをサポートするBioAPIのサービスプバイダー。バイオメトリクス情報の取得と、MOCのプリマッチ用データの処理、特徴量抽出の処理、Card上で照合を行うためのMOC用のテンプレートの生成などを行う。
MOCライブラリ	JavaCard上に実装する照合ライブラリ。 JavaCard Biometry APIに適合する必要がある。

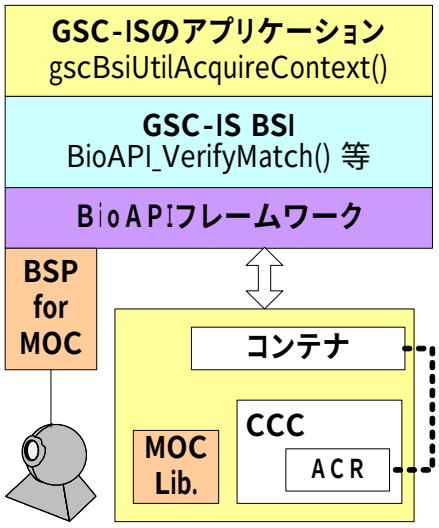
テンプレート種類	保管場所	照合処理の場所	備考
プライベート テンプレート	カード上	カード上で行われ決してカード外に出ない	非接触カードなど少ない電力での照合が重要
プリマッチング用 テンプレート	カード上	カード外	JavaCard Biometry APIではパブリックデータと称している

バイオメトリクス認証対応IDカードの実装モデル プリマッチの手法　続き



バイオメトリクス認証対応IDカードの実装モデル GSC-ISのフレームワークとMOCモデル

- 論理的にカードとの接続の確立
- gscBsiGcGetContainerProperties を使って、ジェネリックコンテナ・カード・サービスのためにACR ACR(Access Control Rules)を取得する。例えば、バイオメトリクス認証 (照合) が、バッファサービスの読み出しのために必要な場合、このサービスのためにACRは BSI_ACR_BIOMOCが返される。
- gscBsiUtilAcquireContext()を使って、ジェネリックコンテナ・スマートカード・サービスのために、ACRの条件を満たす認証を行う。ここでは、MOCによるバイオメトリクス認証が行われる。
- BSI呼び出しを介してジェネリックコンテキスト・スマートカード・サービスをアクセスする。
- セキュリティコンテキストを開放する。



まとめ

- バイオメトリクス認証の発展には、APIの標準化は不可欠。
- 標準化されたバイオメトリクス認証API(BioAPI)は、バイオメトリクス認証特有の問題を解決して行く。
- 標準化されたバイオメトリクス認証APIは、他のセキュリティフレームワークと結合して使われていく。

参考

- セキュリティAPIに関する技術調査
  - http://www.ipa.go.jp/security/fy15/reports/sec_api/index.html
  - Part 5. バイオメトリクス認証の API
    - http://www.ipa.go.jp/security/fy15/reports/sec_api/documents/api2003_5.pdf
- 各国バイオメトリクスセキュリティ動向の調査
  - http://www.ipa.go.jp/security/fy15/reports/biometrics/
  - http://www.ipa.go.jp/security/fy15/reports/biometrics/documents/biometrics2003.pdf
- 本人認証技術の現状に関する調査
  - http://www.ipa.go.jp/security/fy14/reports/authentication/
- Text of FCD 19784, BioAPI
  - http://www.jtc1.org/FTP/Public/SC37/DOCREG/37N0311.pdf
- Smart Card Biometric Interoperability Study Report
  - http://www.ncits.org/tc_home/m1htm/docs/m1030398.pdf