平成１７年度経済産業省　産業技術研究開発委託事業－１

生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化

第４部　バイオメトリクス認証結果保証基盤の研究開発

平成１８年３月

財団法人ニューメディア開発協会

４　バイオメトリクス認証結果保証基盤の研究開発

近年、バイオメトリク認証を従来の物理的アクセス制御だけではなく、情報分野における認証に用いる動きが活発化している。一般的に、バイオメトリクス認証をネットワーク経由で行う場合、クライアント側でユーザのバイオメトリクス情報を取得し、サーバに対してバイオメトリクス情報あるいは照合結果を通知する。このとき、使用したセンサやバイオメトリクス照合装置の種類により、サーバに送られる情報の信頼性が異なるので、情報の信頼性に関する情報をサーバに通知する必要が生じる。しかし現状では、照合を行った環境をサーバに通知するための標準化されたフォーマットは存在しない。

そこで、本章ではクライアント側バイオメトリクス環境をサーバに通知するための共通フォーマットとして、東芝ソリューションにより提案されている ACBio（バイオメトリクスのための認証コンテキスト：Authentication Context for Biometrics。ＢＡＣ(バイオメトリクス認証コンテキスト：Biometric Authentication Context)から 2005 年 11 月に名称変更）について検討する。この技術によって、バイオメトリクス認証結果を保証する事ができるようになる。そして、このフォーマットを標準化することによって、バイオメトリクスがより有力な認証基盤として広く用いられることが期待される。

本章の構成は以下の通りである。

４．１では、ACBio の標準化に向けた国際標準案の策定について、その活動と案の基本的な考え方を述べる。

４．２では、国際標準化に関する主要関係者との意見調整、関係各国との協議について、その内容と標準化案との関係を述べる。

４．３では、標準化案をレビューする目的で設置された標準化仕様WGの活動について述べる。

４．４には、関係する資料を添付した。

４．１　データ項目及びデータ形式の標準化に向けた国際標準案の策定

４．１．１　ISO/IEC JTC 1/SC 27 における活動経緯

今年度の ISO/IEC JTC 1/SC 27 における活動経緯は以下のとおりである。

2005 年 04 月 SC27 オーストリア ウィーン会議

SC27/WG2 の NP に提案

2005 年 08 月 NP 投票

NP に採択 （投票結果：賛成２４、反対１、 棄権７）

エディタ： 東芝ソリューション　才所敏明

2005 年 08 月 1st WD 発行

2005 年 11 月 SC27 マレーシア クアラルンプール会議

1st WD コメント処理、SC37 との連携方針の決定、PJ タイトルを BAC（Biometric Authentication Context）から ACBio（Authentication Context for Biometrics）に変更

2005 年 12 月 Dispostion of comments 発行

2006 年 01 月 SC37 京都会議

ACBio 概要、CBEFF・BioAPI との関係を説明

2006 年 2 月 22 日　2nd WD 発行

上記のとおり、今年度は 2 つの WD（Working Draft）を作成した。また、1stWD のコメント処理結果をまとめた Dispostion of comments も発行した。これらの詳細は、４．４を参照されたい。

４．１．２　1stWD の作成の考え方

ウィーン会議に提出した寄書を基に 1st WD を作成した。ウィーン会議寄書と 1st WD との主な違いは以下のとおりである。

① Entity Information Block を大きく２つの情報に分解した。ひとつはエンティティ（詳細は 1st WD 参照）の機能及びその評価情報を拡張領域に含む X.509 公開鍵証明書であるエンティティ証明書、もうひとつはエンティティがストレージサブプロセスを含む場合に持つテンプレートに関する情報であり本標準案で新たに提案したテンプレート証明書である。テンプレート証明書は、テンプレートの正当性を示す証明書であるが、プライバシーを考慮し、テンプレート自体を含まず、テンプレートが誰のものであるかの情報も含まないものとした。

② Biometric Process Block のデータエレメントに、実データを入れず、ハッシュ値だけを入れるようにした。これも、プライバシーとセキュリティを考慮した結果である。

以上の方針の下に作成したのが 8 月 14 日に発行した 1st WD である。1st WD における BAC の概要は以下のとおりである。

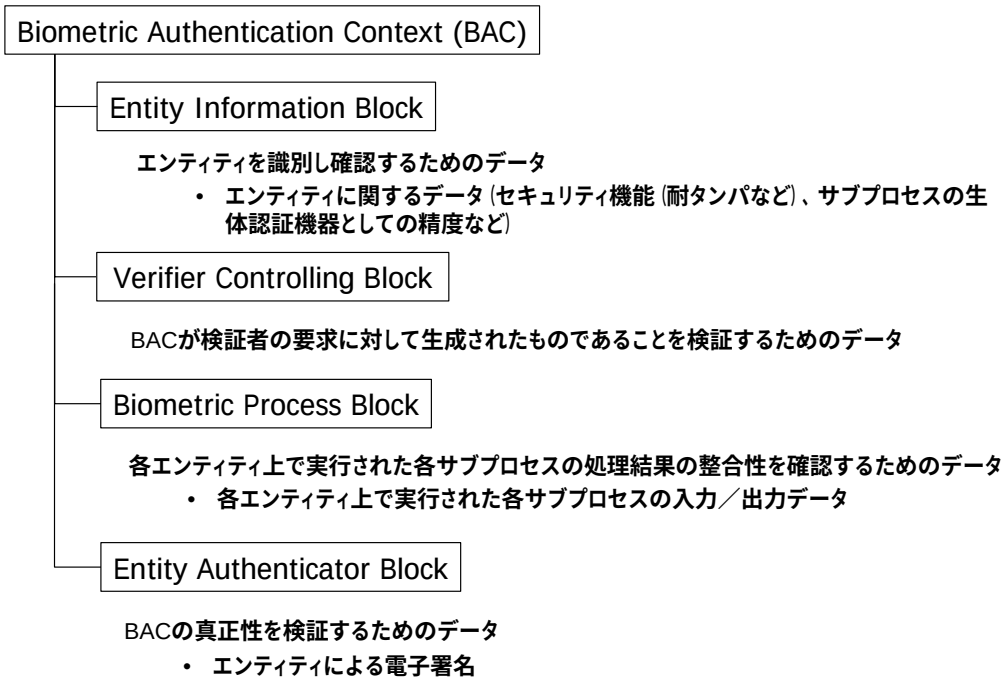


図 4-1　BAC の構造

BAC は、上の図のとおり、４つのブロックから構成される。ここで、エンティティとは、均質なセ

キュリティのレベルを持つ、生体認証プロセスを構成するサブプロセスの集合体である。

Entity Information Block は、エンティティを識別し確認するためのデータである、Entity Certificate と Template Certificate から成る。Entity Certificate は、X.509 証明書であって、拡張領域に Entity Evaluation Report を保持する。Entity Evaluation Report は、エンティティのバイオメトリクス機器としての機能についての精度・品質、セキュリティ機能についての評価結果を記述した報告書である。Template Certificate は、当該エンティティ内にテンプレートが保持されるときだけ（すなわち、ストレージサブプロセスがエンティティに含まれるときだけ）、Entity Information Block に含まれるデータである。Template Certificate は、テンプレートデータの正当性を証明する証明書で、登録組織によって発行される。Template Certificate は、プライバシー問題を考慮して、テンプレートデータの実データは含まず、ハッシュ値だけを含む。

Verifier Controlling Block は、BAC が検証者の要求に対して生成されたものであることを検証するためのデータを含む。具体的には、検証者からのチャレンジをこのブロックに含む。

Biometric Process Block は、各エンティティ上で実行された各サブプロセスの処理結果の整合性を確認するためのデータを含むブロックである。各エンティティ上で実行された各サブプロセスの入力／出力データのハッシュ値を格納することによって、エンティティ間のデータの受渡しが正しく行なわれたかを確認できる。

Entity Authenticator Block は、BAC の真正性を検証するためのデータを含む。具体的には、上の３つのブロックに対するエンティティによる電子署名がこのブロックに含まれる。

1st WD の詳細については、４．４を参照されたい。

４．１．３　2nd WD の作成の考え方

クアラルンプール会議前に、SC 27 の各 NB、SC 17、SC 37、ITU-T から、1st WD に対するコメントが寄せられた。SC 37 からのコメントは、バイオメトリクス標準化を進める SC 37 としての強い関心を感じさせるものであった。コメント及びコメント処理結果の詳細は、４．４を参照されたい。

1st WD から 2nd WD への変更点の主なものは、1st WD に対するコメントへの対応である。

① SC 37 SD2 (用語集) で定義されている用語に変更

Matching を Comparison に変更するなどの変更を実施した。バイオメトリクスを標準化対象にする SC 37 の用語に従うのは当然のことである。

② 1st WD で採用した 5 サブプロセスモデル以外のモデルへの対応

これは SC 37 と SC 17 から出て来たコメントであるが、具体的な内容を含んでいたのは SC 17 からのコメントである。そのコメントでは、Capture したデータがそのまま storage に入るモデルに 1st WD が対応できないことが指摘されていた。これに対しては、サブプロセスと入出力情報を固定的に対応させていたのを、BPU（Biometric Process Block。1st WD の entity から名称変更）の静的な情報を含む BPU Information Block（旧 Entity Information Block）の内部に BPU report という構造を持たせ、その中にサブプロセスと入出力情報を別々に持たせることによって、柔軟な対応ができるようにした。

③ CBEFF との親和性考慮

共通するデータは CBEFF に合わせることによって対応することにした。具体的には BT 証明書

（1st WD のテンプレート証明書から名称変更）に含まれるいくつかの情報を CBEFF の対応する情報の形式に一致させた。

以下については、1st WD に対して寄せられたコメントであるが、今後継続検討することにした。

④ STOC、MOC のカード処理負荷の考慮（SC 17 と連携・検討する）

⑤ BioAPI への影響考慮（SC 37 京都会議での議論を継続する）

以上の他に、2nd WD では CMS（Cryptographic Message Syntax）を採用して、以下に示す ACBioContentInformation タイプのデータの BPU の秘密鍵による SignedData として ACBio を定義した。

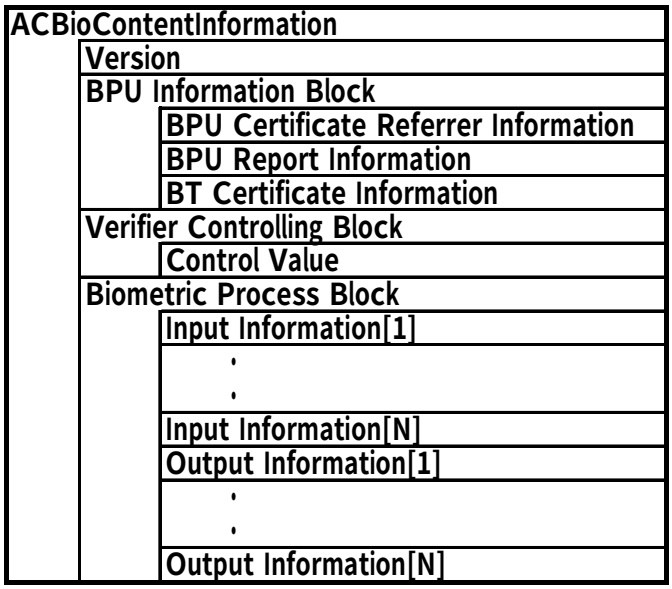


図 4-2　ACBioContentInformation の構造

BPU Information Block は、1st WD の Entity Information Block に替わるものである。1st WD では Entity Certificate の拡張領域に含んでいた Entity Evaluation Report を分離して、BPU Report として独立させた（BPU Report Information は、BPU Report 自体または BPU Report への参照として定義されている）。BT Certificate は、1st WD の Template Certificate に替わるものであり、新たにテンプレート登録時の ACBio も含むように定義した（BT Certificate Information は、BT Certificate 自体または BT Certificate への参照として定義されている）。

Verifier Controlling Block については、1st WD からの変更はない。

Biometric Process Block については、1st WD においては各サブプロセスに対応した部分構造を持っていたのを廃止し、当該 BPU に対する入力情報と出力情報をそれぞれの数だけ持つ単純な構造にした。入力情報及び出力情報は、その入力／出力が生体認証プロセス中で受け渡されるどのデータであるかを示す情報と入力／出力データのハッシュ値から成る対である。

2nd WD の詳細については、４．４を参照されたい。

４．２　国際標準化に関する主要関係者との意見調整、関係各国との協議

以下に時系列で述べる。

４．２．１　2005 年 4 月オーストリアウィーン会議における打合せ

SC 27 のバイオメトリクスのラポータであるドイツの Tekampe 氏とウィーン会議開催の前日 4 月 10 日（日）に寄書の内容について説明し、基本コンセプトに対する同意を得た。

4 月 11 日（月）には Biometrics の Study Period に寄書を出している韓国の Park 氏（テンプレートプロテクションに関する寄書の著者）及び関係者と打合せを実施し、BAC が目指しているものは何であるかを説明した。

４．２．２　2005 年 8 月韓国済州島における打合せ

8 月 14 日に 1st WD を出した直後に韓国済州島で行なわれた WISA（Workshop on Information Security Application）というシンポジウムに出席する Park 氏（24745 Template Protection のエディタ）と Kwon 先生（世宗大学校。キャンセラブルテンプレートに関する寄書の著者）と会って、1st WD の概要説明をし、理解を得た。

４．２．３　2005 年 9 月ドイツエッセン及び米国ローリーにおける打合せ

9 月 5 日（月）にドイツエッセンに SC 27 の Biometrics ラポータの Tekampe 氏を訪問し、1st WD の概要説明をし、理解を得た。氏からの主なコメントは、依拠するモデルを SC 37 の Profile で議論されている粒度の細かいものにすべきではないかというものだった。

9 月 7 日（水）に米国ノースカロライナ州ローリーに SC 27/WG 2 の Biometrics の Study Period のラポータを担当した Griffin 氏を訪問し、1st WD の概要説明をし、理解を得た。エンティティに関する情報は、X.509 の拡張領域を使うのではなく、CMS（Cryptographic Message Syntax）を利用して定義する方が良いとのコメントをもらった。

４．２．４　2005 年 10 月韓国ソウルにおける打合せ

各国の SC 37 関係者に 1st WD を直接送付して意見を求めたが、回答が得られなかった。SC 37 での標準化状況を把握した上の活動ではないとして、SC 37 が BAC に対して懸念を示しているとの情報もあった。そこで 10 月 11 日(月)に SC 37/WG 2 のコンビーナである Kwon 先生（中央大学校）を訪問し、1st WD の概要説明をし、理解を得た。また、SC 37/WG 2 で標準化を進めている CBEFF・BioAPI と BAC との関係についても、２つの標準化を阻害するものではないとの BAC 側の考えを示した。その結果、2006 年 1 月の SC 37 京都会議で BAC についてのプレゼンテーションをしてみてはどうかとの提案をいただいた。その結果が、４．２．７の発表に繋がった。

４．２．５　2005 年 11 月マレーシアクアラルンプール会議における打合せ

AGMonBio (Advisory Group Meeting on Biometrics) ラポータ Tekampe 氏との事前協議を 11 月 6 日（日）に行なった。AGMonBio の内容、進め方について相談し、SC 37 からの新しい提案である JRG（Joint Rapporteur Group：エディタの上に SC27,SC37 の合議グループ設置という提案。SC 27

N4774 では、SC 27 – SC 37 チェアマン間の遠隔会議で合意との記述あり）について相談した。JRG 設置の必要はないとの見解が示された。

４．２．６　2005 年 12 月米国ゲイザーズバーグ及びローリーにおける打合せ

12 月 5 日(月)に NIST（米国メリーランド州ゲイザーズバーグ）に SC 27/WG 3 で 19790 のエディタをしている Randall 氏を訪問し、19790 評価結果の電子フォーマット制定を要求した。19790 ではスコープ外であるが、NIST が作成を予定している FIPS140-3 で考慮できる内容であるので、そちらへの要求を出すようにとのコメントをもらった。

12 月 7 日（水）にはノースカロライナ州ローリーに Griffin 氏を訪問し、検討を開始した 2nd WD の作成方針について、意見をもらった。テンプレート証明書には、テンプレート生成に誰が関わったか（登録機関）の情報とどのように生成されたかの情報（テンプレート生成時の ACBio）が必要ではないかとの意見をもらった。

４．２．７　2006 年 1 月 SC 37 京都会議における発表

1 月 12 日（水）に SC 37/WG 2 において 1 時間のセッションをいただき、ACBio の概要を説明し、CBEFF と ACBio の関係、ACBio を実現するために必要となる API と BioAPI の関係について、ACBio 側の考えを提示した。ACBio に対する理解は得られたが、BioAPI との関係については提示した考えとは異なる考えがあることが示された。

このセッションの結果、ACBio と SC 37/WG 2 の技術と ACBio の関係を検討する Special Group の設置を決定し、その場で 9 名がメンバとして参加を表明した。チェアは Greg Cannon 氏が勤めることとなった。また、第 1 回の会合が、3 月 6 日（月）にワシントン DC で開催されることになった。SC37 専門家グループとの良好な協力関係樹立の可能性が見えてきた。

４．３　標準化仕様WG活動

４．３．１　背景

「バイオメトリクス本人認証結果保証基盤に関する研究開発」の平成 16 年度の成果に基づいて、平成 17 年 4 月、ウィーンにて開催された ISO/IEC JTC1 SC27（IT セキュリティ技術に関する国際標準化機関）WG2（以下、SC27/WG2 と略記）の会議にて、ニューワークアイテム（NWI）としての採択を目指して「Biometric Authentication Context」（以下、BAC と略記）の寄書案を提出した。本提案は同会議での議論の後、本寄書案は SC27/WG2 の国際提案として、SC27 総会にて各国 NB による投票が行われることが決定され、投票期限が平成 17 年 8 月 10 日と定められた。

SC27/WG2 ウィーン会議後、本研究課題では BAC の寄書案が NWI として採択されることを前提とし、平成 17 年 11 月の SC27/WG2 クアラルンプール会合に向けてワーキングドラフト（WD）を作成・提出することを当面の目標とした。この WD 作成に当たり、日本国内の関係者に対して、上記の国際標準活動の状況の周知し、関連技術の情報提供、技術面での意見集約を行うために、標準化仕様ワーキング・グループ（以下、本 WG と略記）が新たに設置されることとなった。本 WG のメンバとして、公益法人、メーカなどのバイオメトリック技術の専門家が選定され、平成 17 年 7 月 1 日本 WG 第 1 回会合が開催された。

４．３．２　活動経過

本WGの構成メンバは表４．３．１に示すとおりである。

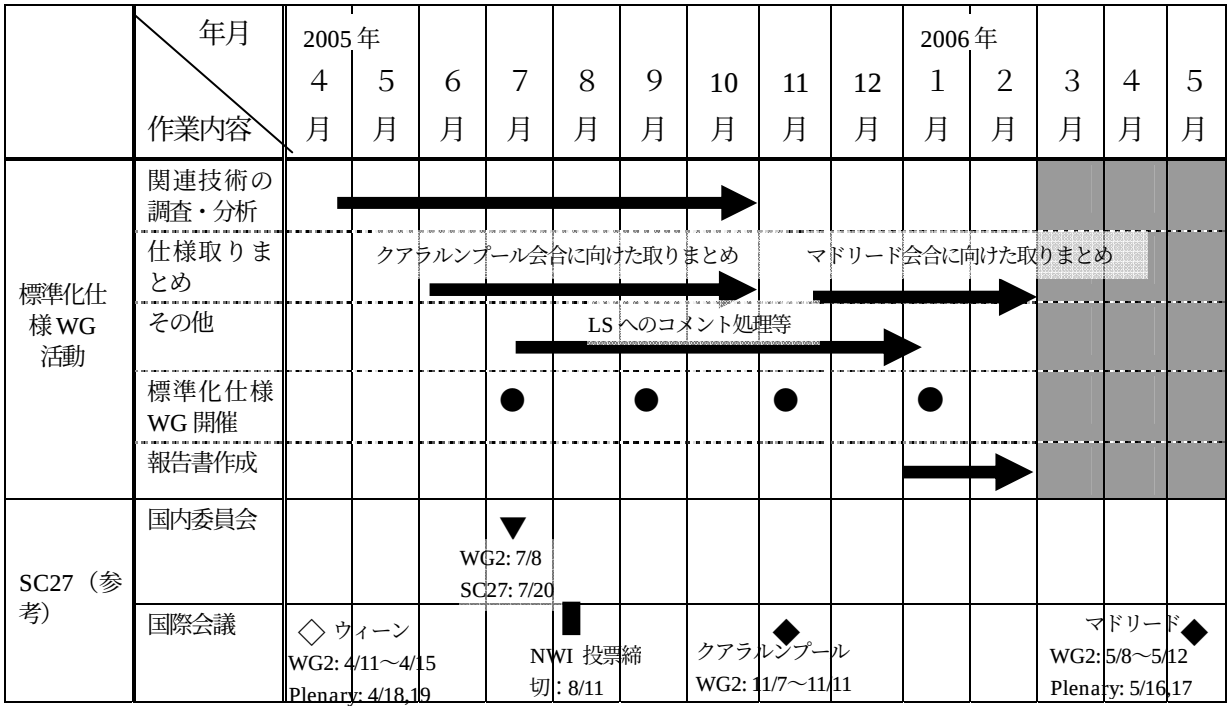
表４．３．１「バイオメトリクス認証結果保証基盤の研究開発WG」名簿

役割	氏名	所属
主査	上繁　義史	（財）九州システム情報技術研究所
幹事	才所　敏明	東芝ソリューション株式会社
委員	磯部　義明	株式会社日立製作所
委員	松本　泰	セコム株式会社
委員	道坂　修	株式会社NTTデータ
委員	山田 朝彦	東芝ソリューション株式会社
委員	尾関　一郎	大日本印刷（株）
オブザーバ	池野　修一	ＢＳＣ基盤技術部会長
オブザーバ	小谷　光弘	経済産業省
オブザーバ	瀬戸　洋一	ＢＳＣ会長代行
オブザーバ	川根　祐二	（財）九州システム情報技術研究所
事務局	岸本　芳典	（財）ニューメディア開発協会
事務局	滝沢　俊男	（財）ニューメディア開発協会

（注）BSC：バイオメトリクス・セキュリティ・コンソーシアム

本WGは表４．３．２のスケジュールに基づいて定期的に会合を持った。

表４．３．２　標準化仕様WG活動スケジュール



各会合は以下の流れで進められた。

i) 国際標準化活動の主体である東芝ソリューションの才所幹事、山田委員より、標準化活動の進捗状況：
   - SC27/WG2 への提案内容に関する技術的内容、
   - SC27/WG2 会合参加報告、
   - WD 作成進捗状況　　ほか

   について報告が行われた。報告内容に基づいて、技術面、活動の推進に関するディスカッションがおこなわれた。

ii) 以下の技術調査結果（添付資料４），５），７），８）参照）について上繁主査から報告が行われ、意見交換が行われた。
   - 他の標準化団体（ISO/IEC JTC1 SC37、ITU-T SG17 など）にて審議が行われているバイオメトリック技術に関する標準化提案（添付資料６）参照)、
   - SC27/WG2 に他国 NB から提案されたバイオメトリック技術に関する標準化提案、
   - その他上記 i)に関連するバイオメトリック技術

各会合の開催概要は下表４．３．３の通りである。開催時の資料、議事録は表中に示す添付資料に掲載されている。出席者数には主査、幹事、委員、オブザーバ、事務局スタッフが含まれる。

表4．3．3　標準化仕様 WG 開催概要

会　合	開催日	出席者数	議　題
第1回会合	H17/7/1	11 名	1. 開会 （1）配布資料確認 2. 議題 （1）WG 設置目的等説明 （2）WG メンバの自己紹介 （3）WG 活動内容について （4）技術説明
第2回会合	H17/9/16	10 名	1. 前回議事録の確認 2. 議事 （1） 標準化活動の進捗状況 （2） WD 案の説明 （3） 関連技術の調査結果報告
第3回会合	H17/11/22	9 名	1. 前回議事録の確認 2. 議事 （1） SC27/WG2 クアラルンプール会合参加報告 （2） 関連技術の調査結果報告
第4回会合	H18/1/24	6 名	1. 前回議事録の確認 2. 議事 （1） 国際標準化の進捗状況について （2） 関連技術の調査結果報告 （3） 標準化仕様 WG の活動のまとめ

４．３．３　本WGの活動のまとめ

本節では、本 WG 発足に至った経緯と活動目的、活動内容の概要について報告した。本 WG の活動初期に SC27/WG2 日本提案（BAC）は NWI 採択を受け、プロジェクト番号 24761 が与えられた。それに伴い、本 WG 内において、SC27/WG2 のクアラルンプール会合（平成 17 年 11 月）、およびマドリード会合（平成 18 年 5 月）に向けて WD 作成、修正のための意見集約が十分に図られた。

SC27/WG2 クアラルンプール会合にて、BAC は名称が変更され「Authenticate Context for Biometrics」（略称 ACBio）となり、国際標準化活動として着実に軌道に乗りつつあるものと思われる。才所幹事、山田委員より SC37 京都会合（平成 18 年 1 月）の WG2 にて ACBio の説明が行われ、同 WG との協力関係が築かれたことも、今後の標準化活動推進にとって大変意義深いものと言えよう。本 WG としては、早期の国際標準化実現を祈念する次第である。

４．４　添付資料

WG 活動に関する資料について、以下添付資料１）～添付資料１３）に示す。

1）　「バイオメトリクス認証結果保証基盤の研究開発 WG」名簿
2）　標準化仕様 WG スケジュール
3）　第 1 回標準化仕様 WG 資料－オープンネットワーク上での運用を包含したバイオメトリック認証のフレームワークに関する技術比較
4）　標準化仕様 WG 第 1 回会合議事録
5）　第 2 回標準化仕様 WG 資料－韓国からの 24745（Biometric Template Protection）の 1st WD 素案に関する調査結果
6）　第 2 回標準化仕様 WG 資料－Baseline document for Telebiometrics System Mechanism の調査報告
7）　第 2 回標準化仕様 WG 資料－調査報告：「Korean NB contribution for Biometric Data Authentication using Practical Digital Signature」の内容について
8）　第 2 回標準化仕様 WG 資料－「Korean NB contribution for Biometric Data Authentication using Practical Digital Signature」調査報告補足資料：「Practical Digital Signature Generation using Biometrics」
9）　標準化仕様 WG 第 2 回会合議事録
10）　第 3 回標準化仕様 WG 資料－Authentication Context for Biometrics（ACBio）と Bio Application Programming Interface（BioAPI）Version1.1 との関連について
11）　標準化仕様 WG 第 3 回会合議事録
12）　第 4 回標準化仕様 WG 資料－Authentication Context for Biometrics（ACBio）と Bio Application Programming Interface（BioAPI）Version2.0 との関連について
13）　標準化仕様 WG 第 4 回会合議事録

添付資料１）

「バイオメトリクス認証結果保証基盤の研究開発 WG」名簿

役割	氏名	所属
主査	上繁　義史	（財）九州システム情報技術研究所
幹事	才所　敏明	東芝ソリューション株式会社
委員	磯部　義明	株式会社日立製作所
委員	松本　泰	セコム株式会社
委員	道坂　修	株式会社 NTT データ
委員	山田 朝彦	東芝ソリューション株式会社
委員	尾関　一郎	大日本印刷（株）
オブザーバ	池野　修一	ＢＳＣ基盤技術部会長
オブザーバ	小谷　光弘	経済産業省
オブザーバ	瀬戸　洋一	ＢＳＣ会長代行
オブザーバ	川根　祐二	（財）九州システム情報技術研究所
事務局	岸本　芳典	（財）ニューメディア開発協会
事務局	滝沢　俊男	（財）ニューメディア開発協会

（注）BSC：バイオメトリクス・セキュリティ・コンソーシアム

添付資料２）

第１回標準化仕様 WG 資料

平成 17 年 7 月 1 日

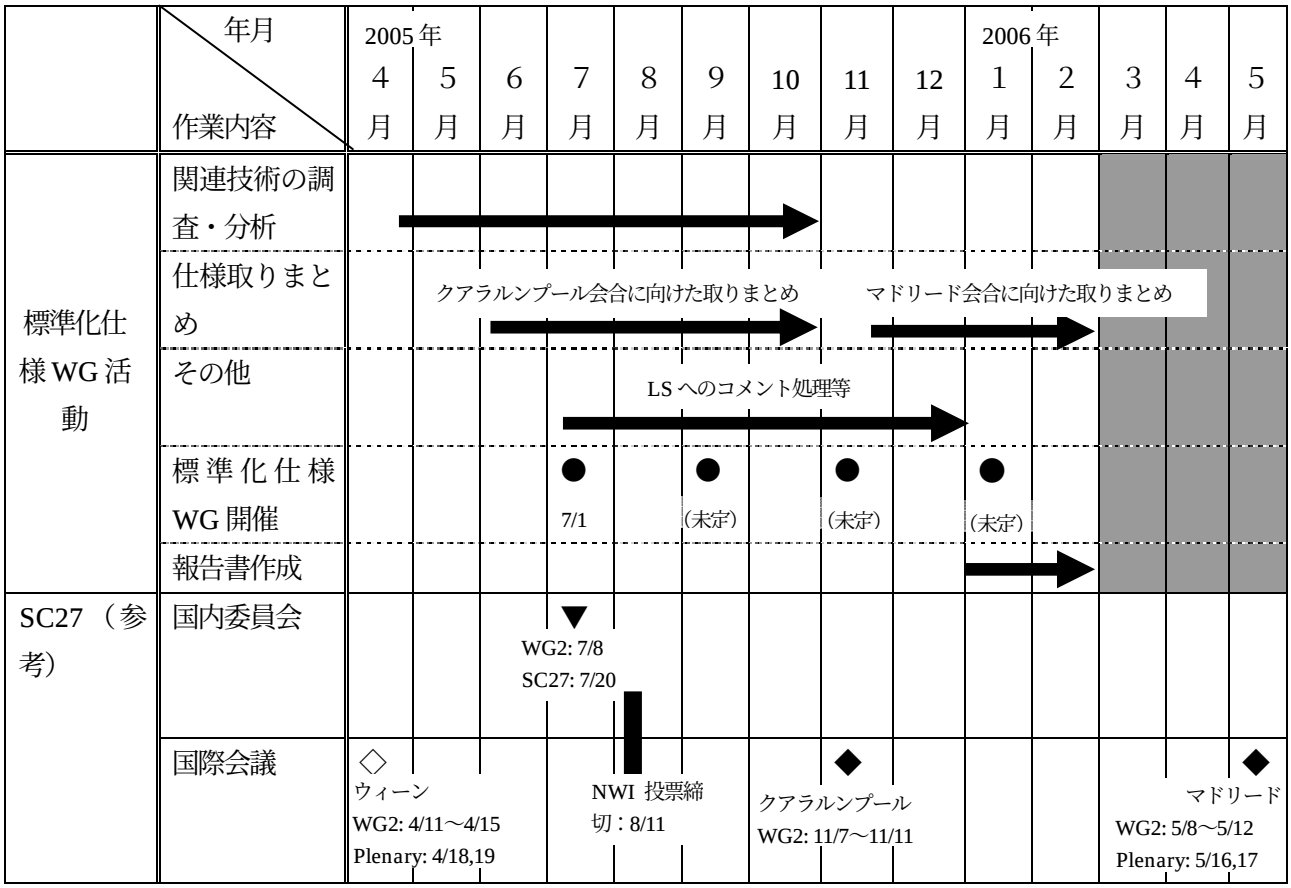
標準化仕様 WG スケジュール案

作成者：（財）九州システム情報技術研究所
上繁　義史

本 WG では，主査，幹事を中心に SC27/WG2 ウィーン会合（2005 年 4 月）での NP 提案を軸とした標準化仕様の取りまとめ，関連技術の調査分析，LS（リエゾンステートメント）のコメント処理等のワーキングを行い，その状況について WG 委員各位に報告する．また，WG 委員各位よりコメントをいただきながら標準化仕様等の内容を精査する．

本 WG の活動スケジュール案を下表に示す．

表　標準化仕様 WG スケジュール案



以上

添付資料３）
第１回標準化仕様 WG 資料

平成 17 年 7 月 1 日

オープンネットワーク上での運用を包含したバイオメトリック認証のフレームワークに関する技術比較(1)

作成者：（財）九州システム情報技術研究所
上繁　義史

1. 技術比較の目的

本 WG では ISO/IEC JTC 1/SC27/WG2 提案，ITU-T SG17 日本提案をはじめ他の関連技術について技術比較を行い，その共通点，相違点，適用範囲などを明らかにして標準化仕様策定の参考としていく．

2. 技術比較の現状

現在，オープンネットワーク上での運用を包含したバイオメトリック認証のフレームワークに関する提案が日本から ISO/IEC JTC 1/SC27/WG2[1]と ITU-T SG17[2],[3]に対して出されている．これらの提案はバイオメトリック認証における各種情報についての証明書に基づいて，認証結果を信頼する仕組みを提供するものである．ここで言う「各種情報についての証明書」には，

- ◆ バイオメトリックデバイスの精度，安全性に関する証明書，
- ◆ バイオメトリックテンプレートに関する証明書，
- ◆ 認証結果（マッチングスコアや閾値などを含む）に関する証明書

等が含まれている．

これらの提案には上のような共通点が見られると共に，以下の点で相違が見られる．

- ◆ ISO/IEC JTC 1/SC27/WG2 提案では，認証結果を検証するためのバイオメトリック認証情報のデータ形式を提案している．
- ◆ ITU-T SG17 日本提案では，PKI との連携を前提としたバイオメトリック認証の運用モデル，認証方法（プロトコル）を提案している．

参考文献：

[1] “Biometric Authentication Context”, ISO/IEC JTC 1/SC27 N4402, Apr. 2005.
[2] “Baseline document for Telebiometrics System Mechanism”, ITU-T Q8/SG17, Mar. 2005.
[3] “A New Study Item on Telebiometrics – A Framework of biometric authentication technologies on Public Key Infrastructure”, ITU-T Q10/SG17, Mar. 2004.

以上

添付資料４）

平成 17 年 7 月 6 日

「バイオメトリクス認証結果保証基盤の研究開発」に関わる WG
第 1 回 WG 議事録

作成者：（財）九州システム情報技術研究所
上繁　義史

日時：平成 17 年 7 月 1 日(金)　15：00～17：30

場所：(財)ニューメディア開発協会 D 会議室（東京都港区三田 1-4-28　三田国際ビル 23 階）

出席者：主査　上繁義史，幹事　才所敏明氏（東芝ソリューション），
委員　磯部義明氏（日立製作所），松本泰氏（セコム），山田朝彦氏（東芝ソリューション）
オブザーバ　池野修一氏（セコム），小谷光弘氏（経済産業省），
松尾聡，川根祐一（（財）九州システム情報技術研究所）
事務局　岸本芳典氏，滝沢俊男氏（（財）ニューメディア開発協会）
以上 11 名

次第：

1. 配布資料確認
2. 議事
   (1) 目的等説明
   (2) WG メンバーの自己紹介
   (3) WG 活動内容について
   (4) 技術説明
      i) 関連標準化活動の概要
      ii) ISO 提案内容
      iii) 両提案の技術比較
3. その他
   (1) 次回予定
   (2) ISIT の紹介

議事要旨：

１．議事

(1) 目的等説明

◆ 事務局滝沢氏より資料 2 に基づいて WG 設立の経緯，目的について紹介があった.

(2) WG メンバーの自己紹介

◆ WG メンバーの名表（資料 1）に従って自己紹介を行った.

(3)　WG 活動内容について

◆ 資料 3 に基づき，上繁より活動内容，2006 年 2 月までの活動スケジュールについて案の説明を行った.

◆ 幹事才所氏より，WG の活動について以下 2 点について確認が行われた.

- WD 原案作成，LS コメント原案作成を東芝ソリューションが行う.
- 上記原案に対して WG でコメントをいただく.

◆ WG 活動内容，活動スケジュール案は了承された.

(4)　技術説明

i)　関連標準化活動の概要

◆ 磯部委員より資料 4 に基づき ITU-T の標準化動向及び提案技術の概要が紹介された.

- ITU-T SG17 の標準化活動
- ITU-T SG17 Q8 テレバイオメトリクスに関連する標準化活動
- モスクワ会議での提案内容の概要
- 2005 年 10 月ジュネーブ会合での WD 提案

◆ 質疑応答

- -ITU-T からのリエゾンステートメントの回答期限について（上繁）
  - 回答期限としては 9 月末となっている（磯部委員）
  - SC27 では公式な議論は ITU-T のジュネーブ会合に間に合わない（幹事才所氏）

  ⇒国内での非公式な活動として，当 WG において見解のすり合わせを行うこととなった.
- -提案プロトコルについて（山田委員）
  - アプリケーション層での処理を想定している（磯部委員）
- -SG17 での活動について（才所幹事）
  - アプリケーションレイヤのテレコムセキュリティ及び言語の標準化を行っている.（磯部委員）
  - 各クエスチョン（課題）が ISO での WG に相当（磯部委員）
  - WP（ワーキングパーティ）でいくつかの関連する課題を纏めて扱う. 現在は 6 つある.（磯部委員）

ii)　ISO 提案内容

❖ ISO への提案の経緯

◆ 幹事才所氏よりウィーン会合までの活動の経緯が紹介された.

- BAC では他の標準化（モジュールの安全性，照合精度，データ品質，テンプレート証明書等）を利用する
- SC27/WG2 ブラジル会合，ウィーン会合にて提案⇒現在 NWI 投票中
- 他国の動向（グリフィン氏，テカンペ氏のコメント)が紹介された.

◆ 質疑応答

- -米国 NIST の本事案に関する活動について（オブザーバ池野氏）
  - 本事案については NIST から出席はなく，NP 提案も出てこなかった（幹事才所氏）

◆ コメント

- -NIST の中で東芝提案 BAC の影響について議論が行われている（幹事才所氏）
- -BioAPI との整合は難しいのではないか(磯部委員)

❖ ISO への提案内容

◆ 山田委員より資料 5 に基づいて提案内容（Biometric Authentication Context; BAC）に関して説明がなされた,

- -WD 案の位置づけ
- -BAC で解決したいこと
- -BAC のアプローチ
- -提案の詳細

◆ 質疑応答

- -エンティティ証明書の entityEvaluationReport について（オブザーバ池野氏，磯部委員）
  - 19795 にて評価結果のレポートが提示されるものと期待している（幹事才所氏）
  - エンティティの機能に関するプロファイル情報を持つ必要があるかもしれない（山田委員）
- -BAC では情報をハッシュ値で持つことになっているが，元データの改ざんを Verifier が検証できないのではないか（磯部委員）
  - 各エンティティが安全であることが前提（幹事才所氏）
  - 各エンティティ間の通信（セキュアでない通信）に用いる（幹事才所氏）
  - Evaluation Organization があることが望ましいと思う（山田委員）

◆ コメント

- -金融で署名と同時に BAC を用いるケースが考えられる(松本委員)
- -本提案はプラットホーム認証に近いと思われる（松本委員）

iii) 両提案の技術比較

◆ 上繁より東芝提案と日立提案について，共通点，相違点の概要について紹介した.

◆ 質疑応答

- 比較対象について（磯部委員）
  - 2 社の提案だけではなく，関連する技術についても比較検討を行う（上繁）

❖ メーリングリストの作成について

- 会合以外にもメール審議，コメントの議論ができるように NMDA にてメーリングリストを作成することとなった.

2. その他

(1) 次回予定

◆ 9月上旬で日程を調整する.

(2) ISIT の紹介

◆ オブザーバ松尾より ISIT について紹介がなされた.

以上

添付資料５）

平成 17 年 9 月 16 日

調査報告：「Korean NB contribution for Biometric Data Authentication using Practical Digital Signature」の内容について

報告者：（財）九州システム情報技術研究所
第 2 研究室　研究員　上繁義史

1. 寄書案の概要

本寄書案はバイオメトリクスデータの保護を組み込んだディジタル署名について述べている．ポイントは 2 点ある．バイオメトリクスをディジタル署名（鍵）生成と復元に用いている点と，ユーザがテンプレート情報を含んだ印刷物（2 次元バーコードなど）を所持する点である．

2. 本寄書案の特徴

- バイオメトリクスをディジタル署名鍵の生成と復元に利用している．
  - ユーザのサンプルデータ，鍵生成アルゴリズム，擬似乱数生成器を用いて署名鍵とテンプレート情報が生成される．（文中では transformed biometrics と表記）
  - 署名鍵の復元にバイオメトリクスを利用している．
  - 基礎技術として，バイオメトリクス暗号化技術を想定している．
    - 同技術に関する詳細は参考文献[10]，[11]に記述されている．
    - 参考文献[10]の調査概要は補足資料を参照されたい．
- バイオメトリクスのテンプレートに相当する情報を所持物に格納している．
  - 所持物として対タンパ・デバイスは仮定しない．
    - 理由として，スマートカード等が広く普及していないことを挙げている．
  - 所持物として 2 次元バーコードを印刷した紙片を想定している．
    - メリットとして，オフラインで使用可能であり，データベースへのアクセスが不要となること，損傷したシンボルからデータ回復が可能なことを挙げている．

3. 所見

- バイオメトリクスの利用方法を署名鍵の生成，復元に限定しており，一般的なバイオメトリクス認証のプロセスとは異なる．
- 通信データは署名データのみのであり，バイオメトリクスのセンシティブデータは含まれない．
- テンプレートに相当する情報の格納方法として，印刷物を選んだ意図が不明瞭である．
  - 実装が容易という点以外にメリットが見当たらない．
  - どのようにセキュリティ性が担保されるのか不明瞭である．（Two-factor Security について言及しているが，一般論にとどまっているように思われる）

以上

添付資料６）

平成 17 年 9 月 12 日

Baseline document for Telebiometrics System Mechanism の調査報告

（財）九州システム情報技術研究所
第 2 研究室　研究員　上繁　義史

1. 概要

本寄書では PKI 上でのバイオメトリック認証を行うメカニズム（Telebiometrics System Mechanism）について提案している．章立ては下記の通り．

- TSM の前提条件
- 認証モデル（9 種類）
- 脅威
- サーバ側の認証ポリシ
- クライアントの環境
- TSM の処理フローとプロトコル
- 認証に必要なデータのフォーマット

2. 特徴

基本的には PKI への付加的要素としてバイオメトリクス認証を取り扱っている．前提条件として以下の 6 つを挙げている．

1) 公開鍵証明書発行を行う TTP
2) バイオメトリック情報の登録及び署名を付加する TTP
3) バイオメトリック技術の閾値，精度評価の結果を認証し，署名を付加する TTP
4) バイオメトリックデバイスのコモンクライテリアに基づく安全評価結果を認証し，署名を付加する TTP
5) モデルによっては，TTP がバイオメトリック登録情報を管理する必要がある．
6) モデルによっては，TTP がバイオメトリック(認証結果？) の検証を行う必要がある．

所見：上記の条件のうち，3）～6）は SC27/WG2 提案 Biometrics Authentication Context (BAC) と共通すると思われる．

◆　TSM のモデルとして 9 つのモデルを定義している．

モデルはバイオメトリックロウデータの取得をクライアントで行うことを前提として，テンプレートの保管，テンプレートのダウンロード，マッチングをクライアント，サーバ，TTP のいずれに配置するかに基づいて分類したものである．

表　TSM のモデルとその概要

テンプレートの保存 / マッチング先	クライアント	サーバ	TTP
クライアント	Local Model	Download Model	RFC3039 Client Matching Model
	サーバに結果を返す	サーバからテンプレートをダウンロード	テンプレートをクライアントにダウンロード
サーバ	Attached Model	Centre Model	RFC3039 Server Matching Model
	テンプレートとロウデータをサーバに送信	ロウデータをサーバに送信	テンプレートをサーバにダウンロード
TTP	Matching outsourcing by client	Matching outsourcing by Server	Storage & Matching outsourcing
	ロウデータとテンプレートをクライアントから TTP に送信, TTP に照合依頼	サーバがクライアントからロウデータを受け取り, テンプレートと共に TTP に送信, TTP に照合を依頼	ロウデータを TTP に送信, TTP は照合結果をサーバに伝送

◆　各モデルについて脅威とその対策について述べられている.

- 基本的にクライアント上の処理について不正データ送出の脅威を挙げている（ロウデータ, 照合結果）対策として，クライアント認証を挙げている.
- サーバや TTP における個人情報（+バイオメトリック情報）保護に対する脅威として，不正なサーバ，不正な TTP，ネットワークからの不正アクセスを挙げ，対策として PKI によるサーバ，TTP の認証，セッション鍵交換による暗号化を挙げている.

◆　TSM のプロトコルが 2 種類提案されている.

◆　ケース 1：クライアントとユーザが一体のケース（例：ユーザが自分の PC を使っている場合など）

◆　ケース 2：クライアントとユーザが別のケース（例：ユーザがトークンを使って PC を利用する場合など）

◆ TSM にて使用するデータのフォーマットとして以下の 3 種類が挙げられている.

1) テンプレートフォーマット
2) バイオメトリックデバイス証明書フォーマット

3)　伝送データフォーマット

所見：1）は従前のもの．2)は EAL レベルで安全性を証明し，閾値で精度を証明する．3)は SC27/WG2 提案（BAC）を参照する形になっている．

・ ただし，SC27/WG2 提案で定義している Template Certificate と ITU-T SG17 提案で定義している Template Format が矛盾する可能性が高い．
  - SC27/WG2 提案の Template Certificate には所有者に関する情報が一切盛り込まれずに Issuer の署名が付されている．また，テンプレートに関する情報は，テンプレートのハッシュ値のみである．
  - ITU-T SG17 提案の Template Format には所有者の公開鍵証明書と対応付ける情報を含めて Issuer の署名が付されている．また，テンプレート情報として CBEFF を用いている．

⇒署名を付す情報の内容に異なる部分があり，併用するには Template Certificate と Template Format を同時に持つ必要があるが，これは現実的な解とは考えにくい．

以上

添付資料７）

平成 17 年 9 月 16 日

韓国からの 24745（Biometric Template Protection）の 1st WD 素案に関する調査結果

（財）九州システム情報技術研究所
第 2 研究室　研究員　上繁　義史

1. 調査内容：

[1]　スコープ

◆　バイオメトリックテンプレート保護のためのセキュリティ技術の標準化

[2]　バイオメトリックテンプレート保護の概説

◆　本件ではテンプレート情報のセキュリティについて，機密性と完全性を考える．（プライバシについては技術的に定義できないため，この標準化からは除いている）

◆　スコープとしては登録から検証におけるテンプレート保護を考える．

[3]　バイオメトリックテンプレート生成のプロセスの概説およびセキュリティ要件について

◆　本章では，文章の大半を 19092-1（金融サービスにおけるバイオメトリクス，TC68/SC2）からのコピー&ペーストにて作成している．

◆　センサによるデータ収集～信号処理による特徴抽出，テンプレート作成のプロセスを概説している．

◆　セキュリティ要件として，

- バイオメトリックテンプレートと関連データのプライバシを保持できること，
- バイオメトリックデータと認証結果の完全性が保持できること．
- 送信者～受信者間のバイオメトリックデータと認証結果のソースと送り先について相互認証されていること．
- 必要であれば，バイオメトリックデータの機密性を確保すること

を挙げているが，それらは MAC あるいはディジタル署名，耐タンパデバイスにより解決できることを指摘している．（ただし，具体的な用例は言及されていない）

[4]　バイオメトリックテンプレート利用時のセキュリティ要件について

◆ 本章では，文章の大半を 19092-1（金融サービスにおけるバイオメトリクス，TC68/SC2）からのコピー&ペーストにて作成している．

◆ セキュリティ要件として，上で述べた 4 項目のうち，3 項目：

- バイオメトリックデータと認証結果の完全性が保持できること．
- 送信者～受信者間のバイオメトリックデータと認証結果のソースと送り先について相互認証されていること．

➢ 必要であれば，バイオメトリックデータの機密性を確保すること

を挙げているが，それらは MAC あるいはディジタル署名，耐タンパデバイスにより解決できることを指摘している．（ただし，具体的な用例は言及されていない）

[5] バイオメトリックテンプレート保護のシナリオ

◆ ウィーン会議では本文の大半を占めていたが，今回の文献では Annex A となっている．（ただし，今回の文献では内容の記述はなし）

2. 所見：

◆ バイオメトリクス認証の基本的なプロセス（データ収集～スコアの判定）について TC68/SC2 の CD19092-1（金融サービスにおけるバイオメトリクス）Chapter 8，Chapter9 を参照している．

➢ CD19092-1 Chapter8 および Chapter9 は以下の項目を含んでいる．

✓ Chapter 8：Basic principles of biometric architectures

✓ Chapter 9：Management and Security Requirements

➢ 本文献におけるテンプレート保護のセキュリティ要件に関する記述は大半が CD19092-1 のデッドコピーである．

⇒少なくとも要件の詳細について記述すべきではないかと考える．

➢ テンプレート保護のセキュリティ要件において，キャンセル可能なバイオメトリックテンプレート生成技術の必要性について指摘しているが，具体的にどのような性質を持つかについて言及がなされていない．

⇒具体的な要件までは指示すべきと考える．

◆ セキュリティ技術については他の標準を参照することを明示するにとどまり，具体的なテンプレート保護技術については言及がなかった．

⇒SC37 における Data Exchange に関する標準化との関連について言及が必要かと思われる．

以上

添付資料８）

Supplementary Explanation about the Report of **Korean NB Contribution for Biometrics Data Authentication using Biometrical Digital Signature**

Practical Digital Signature Generation using Biometrics

Authors: Taekyoung Kwon, Jae-Il Lee

Computational Science and Its Applications, LNCS (Lecture Notes in Computer Science) Vol. 3043, Springer-Verlag, pp.728-737, May 2004.

Reader: Yoshifumi UESHIGE (ISIT)

Agenda

- Introduction
- Preliminaries
- Basic of Our Scheme
- Practical Biometric Digital Signature Generation
- Conclusion

Introduction

- Current digital signature has a invertible drawbacks
  - The signer must carefully hold & possess a signing key.
    - The signing key is not memorable at all.
- It is desirable occasionally to derive the signing key from biometrics rather than keeping it in an external hardware device.
- This paper describes generating digital signature from biometrics.

Preliminaries

- Related works
  - Digital signature key generation from iris code (2001)
  - Method of deriving RSA parameter from multi modal techniques combining iris, retina, fingerprint (2002)

  ⇒**Above methods require biometric sample which is as same as registered sample!**
  - Activation of signing key stored in smartcard by using biometric authentication

  ⇒**Smartcards must hold a private key or a biometric templates securely.**

Preliminaries

- This paper proposes
  - A simple method for generating digital signatures using biometrics
    - **The digital signature can be verified by the existing cryptographic algorithm (e.g. RSA)**
    - **The hardware device is not used as storage of a signing key or biometric template.**

Preliminaries

- Definition
  - Security parameters: k, l
    - k: general one (say 160 bits),
    - l: special one (say 1024 bits) for public keys
  - Digital Signature Scheme: $\Sigma = \left(G_\Sigma\left(1^l\right), S, V\right)$
    - G_Σ: probabilistic algorithm returning a **public-private key pair** from input 1^l
    - S, V :**signing** algorithm & **verifying** algorithm run in **polynomial time**
  - Public Key Infrastructure
    - **Infrastructure based on Public Key Encryption** using digital certificates of public keys issued by Certificate Authority

Basics of Our Scheme

- Basic concept
  - Drawbacks of deriving a private key from one's biometric only are followings:
    - **The derived value is to be obsolete** once the biometric template is compromised.
    - **The possible number of keys are limited** by the number of biometrics enrolled by the user.
    - The compromise of biometric template implies the **permanent corrupt of the user's corresponding biometrics.**
  - Threat : **Hill-Climbing Attack**
  - Requirements are
    - **To randomize** the signing key derived from biometrics
    - **To keep the biometric template** from hill-climbing attackers.

Basics of Our Scheme

- Basic concept (cont'd)
  - Formal model
    - User : $U=\{B,P\}$, B: biometrics , P: possession
    - Σ: given signature scheme
    - $T_1 : \langle G_\Sigma(1^l), G_R(1^k), B \rangle \rightarrow \langle B_T, P_T \rangle$ initial key generation & key hiding
    - $T_2 : \langle B, B_T, P_T \rangle \rightarrow G_\Sigma$ key recovery & signature generation
    - G_R: random number generator from 1^k
- Basic tools
  - Biometric encryption
  - 2D Bar codes

Practical Biometric Digital Signature Generation

- Assumption
  - Hash-and-sign RSA primitive
    - Public key: $<e, N>$, $<d, N>$
      - $N=pq$, p, q: prime, $ed \equiv 1 \bmod \phi(N)=(p-1)(q-1)$
      - Public key is certified by CA.
    - Signature S: $s \leftarrow \mathrm{H}(m, r)^d \bmod N$, $r \leftarrow_R \{0,1\}^{k_\Sigma}$
      - m: message
    - In the case of two-party RSA, public key is split into two shares such that $d \equiv d_1 d_2$
  - Biometrics data
    - $f(x)$: 2D image
    - $F(u)$: Fourier Transform of $f(x)$. The u denotes spatial frequency.

Practical Biometric Digital Signature Generation

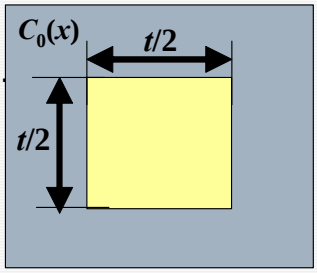
- Assumption (cont'd)
  - Correlation of two images:
    $$c(x) = \int_{-\infty}^{\infty} f_1(v) f_0^*(x+v) dv$$
    - f_1:verification image, f_0: enrolled image
  - Training images: $\left\langle f_0^1(x), f_0^2(x), \Lambda\ , f_0^T(x) \right\rangle$
  - Filter function $H(u)$ which represents
    $$H_s(u) = e^{-i\varphi_{A_0}(u)} e^{i\varphi_R(u)}$$
    - The phase of the complex conjugate of training set images: $e^{-i\varphi_{A_0}(u)}$
    - The random phase-only function: $e^{i\varphi_R(u)}$
    - This filter is calculated during either enrollment or verification.

Practical Biometric Digital Signature Generation

- Key Generation (T_1 Transformation)
  - Input: Series of users biometric data:
    $$\left\langle f_0^1(x), f_0^2(x), \Lambda\ , f_0^T(x) \right\rangle$$
  - Key Split: public-private key pair $<e, N>$, $<d, N>$
    - d_1: t-bit integer, prime
    - d_2 : $d_2 = dd_1^{-1} \bmod \Phi(N) + k\Phi(N)$, for large k
  - Image Processing: A series of input images are combined with a random phase array to create two output arrays, $H_s(u)$, and $c_0(x)$,where
    $$H_s(u) = e^{-i\varphi_{A_0}(u)} e^{i\varphi_R(u)}$$
    $$c_0(x) = \mathrm{FT}^{-1}\left\{A_0(u) \cdot \left|H_0(u)\right| \cdot H_s(u)\right\}$$

Practical Biometric Digital Signature Generation

- Key Generation (T_1 Transformation) (cont'd)
  - Encoding
    - For majority encoding d_1 (t bits), the central $(t/2)\mathbf{x}(t/2)$ portion of $c_0(x)$ must be extracted & binarized. ⇒binarized template at $\mathbf{x} = (x, y)$
    - From the binarized template, a look up table, L , is composed to encode d_1.



  - Possession
    - $P=\{B_T, P_T\}$, $B_T=\{H_s(u),L\}$, $P_T=\{d_2,N\}$
    - P is printed by an arbitrary 2D bar code (PDF417, QR codes)

Practical Biometric Digital Signature Generation

- Signature Generation (T_2 Transformation)
  - Input: Series of biometric data $\left\langle f_1^1(x), f_1^2(x), \Lambda\ , f_1^T(x) \right\rangle$
  - Image Processing: A series of input images are combined with $H_s(u)$ and a new output array $c_1(x)$,where $c_1(x) = \mathrm{FT}^{-1}\left\{A_1(u) \cdot \left|H_1(u)\right| \cdot H_s(u)\right\}$
  - Majority Decoding:
    - For majority-decoding d_1 from given lookup table L, central $(t/2)\mathbf{x}(t/2)$ portion of $c_1(x)$ must be extracted & binarized.⇒a new binarized template at $\mathbf{x} = (x, y)$
    - From the new binarized template & L, a new table L' is composed for decoding d_1
  - Signature Generation: $M^d = \left(M^{d_1}\right)^{d_2}$

Practical Biometric Digital Signature Generation

- Analysis
  - Security against Wiener's Attack
    - In 1990, M. Wiener showed that instances of the RSA cryptosystem using low secret exponent are insecure.
    - Wiener's Attack is based on the continued fraction algorithm.
    - In this analysis, the result shows the large integer k can prevent this system from Wiener's Attack launched on the small partial secret d_1.

Practical Biometric Digital Signature Generation

- Analysis (cont'd)
  - On Practicality
    - In this system,
      - Size of d_2 is about $k+l$ bits. ($k<l$)
      - ⇒As for the length of d_2 , the digital signature is eventually generated on an arbitrary computing machine equipped with the necessary scanners.
    - When the number of modular N multiplication is most expensive,
      - Proposed algorithm require the double of the usual RSA signature generation time.
    - ⇒The authors believe that proposed scheme is practical in the real world.

Conclusion

- This paper has described
  - Biometrics-based digital signature generation
    - It is the combination of biometric encryption, biometric verification, and bar code technology.

添付資料９）

平成 17 年 11 月 8 日

「バイオメトリクス認証結果保証基盤の研究開発」に関わる WG

第 2 回 WG 議事録

作成者：（財）九州システム情報技術研究所
第 2 研究室　研究員　上繁　義史

日時：平成 17 年 9 月 16 日（金）15：00～17：30
場所：ニューメディア開発協会　D 会議室
出席者：主査　上繁義史（（財）九州システム情報技術研究所）
　　幹事　才所敏明（東芝ソリューション），
　委員　磯部義明（日立製作所），松本泰（セコム），山田朝彦（東芝ソリューション）
　オブザーバ　池野修一（セコム），小谷光弘（経済産業省），
　　川根祐二（（財）九州システム情報技術研究所）
　事務局　岸本芳典，滝沢俊男（（財）ニューメディア開発協会）

（敬称略）

3. 前回議事要旨の確認

- 前回議事要旨は内容の修正なく承認された.

4. 議事

（4）　標準化活動の進捗状況

◆　才所幹事より，Biometrics Authentication Context の標準化活動について報告があった.

◆　報告の概要は下記の通りである.

- NWI 投票：可決（賛成 24，反対 1，棄権 7）
  - ・ アメリカより以下のコメント，提案が付されていたとのこと.
    - BioAPI，CBEFF との調整が必要とのコメントが多く見られたとのこと.
    - USANB よりコエディタを推薦（CBEFF のエディタ）があったとのこと.
  - ・ ワーキングの参加国は 15 カ国
- リエゾンステートメントに対する各標準化団体の反応：
  - ・ SC37：BAC の BioAPI（FDIS），CBEFF への影響を懸念している．境界領域のテーマについてニュートラルな立場で議論できる場がほしいという提案があったとのこと.
    ⇒SC27 としての回答が必要．SC27 関係者とヒアリング中
  - ・ SC68：協力の姿勢とのこと.
- 1stWD を SC27 に送付したとのこと.
  - ・ 各国からのコメント期限：10 月 14 日

（5） WD 案の説明

◆ 山田委員より，1stWD に関して説明がなされた.

◆ NWI 承認により ISO のプロジェクト番号 24761 が付与されたとのこと.

◆ 1stWD 作成に当たり，第 1 回標準化仕様 WG 提出分から下記の点について，追加・修正を行った.

- 上繁主査のコメントに対応
- Annex（BAC のプロトコル例：MOC，STOC）を追加
- Annex（BAC の生成例：MOC，STOC）を追加

◆ 今後の展開として以下を挙げた.

- エンティティ証明書内の評価レポートを考える（X.509：エクステンションフィールドを利用）
- 暗号モジュール, バイオメトリクス関係のセキュリティレベル評価を入れる.（19792 の成果を活用）
- 機能の評価レポートをいれる.
- BioAPI に影響を与える方法と，与えない方法を考えている.

（6） 関連技術の調査報告

◆ 上繁主査より，下記関連標準化文書，および関連技術について調査結果が報告された.

i) Biometrics Template Protection 1stWD（ISO/IEC JTC1 SC27/WG2）

- スコープは「バイオメトリックテンプレート保護のためのセキュリティ技術の標準化」
- バイオメトリクス認証の基本的なプロセス(データ収集～スコアの判定)について TC68/SC2 の CD19092-1（金融サービスにおけるバイオメトリクス）Chapter 8，Chapter9 を参照している.
- テンプレート保護のセキュリティ要件において，キャンセルブルバイオメトリックテンプレート生成技術の必要性を指摘しているが，具体的性質について言及がない.
- セキュリティ技術については他の標準を参照することにとどまり，具体的なテンプレート保護技術について言及がなかった.
- 上記について，委員より国際のコメント期限が 10 月であり，回答の判断を WG2 に仰ぐ必要があるとのコメントがあった.

ii) Korean NB contribution for Biometric Data Authentication using Practical Digital Signature（ISO/IEC JTC1 SC27/WG2）

- 本寄書案はバイオメトリクスデータの保護を組み込んだディジタル署名について述べている. ポイントは 2 点ある. バイオメトリクスをディジタル署名(鍵)生成と復元に用いている点と，ユーザがテンプレート情報を含んだ印刷物（2 次元バーコードなど）を所持する点である.
- バイオメトリクスの利用方法を署名鍵の生成，復元に限定しており，一般的なバイオメトリクス認証のプロセスとは異なる.
- 上記について，下記のごとき意見が出された.
  - スコープを明確にすべきである.（同文書に記載がなかった）

- 署名等のアルゴリズムが限定される可能性がある.
- バックデータを韓国 NB に提出していただく必要がある.

iii) Baseline document for Telebiometrics System Mechanism（ITU-T SG17）

- 本寄書では PKI 上でのバイオメトリック認証を行うメカニズム（Telebiometrics System Mechanism）について提案している．章立ては下記の通り.
  - TSM の前提条件
  - 認証モデル（9 種類）
  - 脅威
  - サーバ側の認証ポリシ
  - クライアントの環境
  - TSM の処理フローとプロトコル
  - 認証に必要なデータのフォーマット
- SC27/WG2 提案（BAC）を参照する形になっているが, BAC に含まれる Template Certificate と ITU-T SG17 提案で定義している Template Format が異なる内容をもっており冗長となる.

(4) 次回日程

◆ 次回会合：11 月 22 日（火）午前中（午後は基準認証委員会会合が予定されている）

以上

添付資料１0）

平成 17 年 11 月 22 日

Authentication Context for Biometrics（ACBio）と Bio Application Programming Interface（BioAPI）Version1.1 との関連について (1)

作成者：（財）九州システム情報技術研究所
第 2 研究室　研究員　上繁義史

1. 概　要

SC27/WG2 提案の Authentication Context for Biometrics（ACBio）は，オープン環境におけるバイオメトリック認証に関して認証環境，精度，結果などについて各エンティティが生成するデータ構造を規定する．ACBio の生成がアプリケーション層などの上位レイヤで行われる場合，ACBio との連携が不可欠と考えられる．そこで BioAPI（バージョン 1.1）に基づいて ACBio との整合性について検討を行った．その結果，BIR と ACBio に現段階で互換性がないこと，BioAPI にて定義されている構造体の一部に ACBio に利用可能なものがあることが分かった．

2. 詳　細

(1)　BioAPI で想定しているバイオメトリック認証のモデル

BioAPI ではバイオメトリック認証のモデルについて図 1 のような実装を想定している．図 1 では各エンティティ（ACBio の用語）が BIR を生成することを想定していることがわかる．

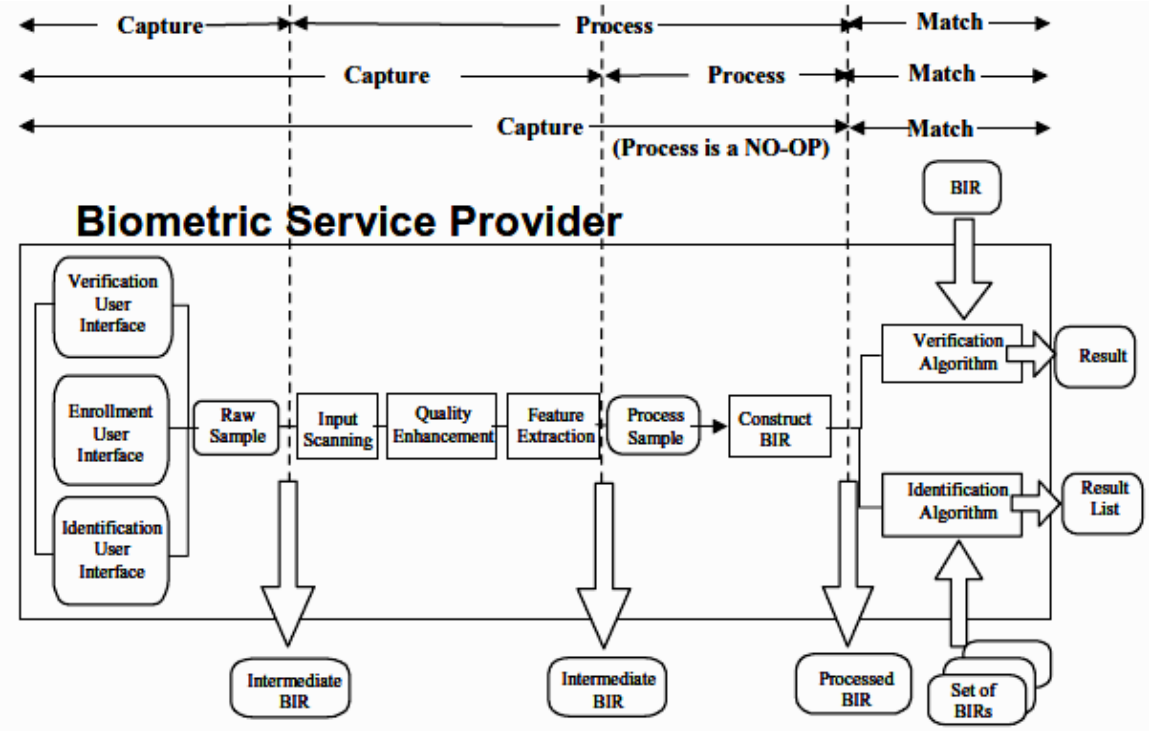


図１　BioAPI で想定しているバイオメトリック認証の実装のパターン（出展：BioAPI Specification Version 1.1）

(2)　Biometric Identification Records（BIR）

BIR は図 2 のようなデータ構造を持っており，Header 内の Format フィールドにて Opaque Biometric Data のフォーマットが識別される．BIR のデータ構造は CBEFF 形式に準拠して定義されており，Opaque Biometric Data として独自形式を用いる場合にはフォーマットの識別情報の登録が必要となる．

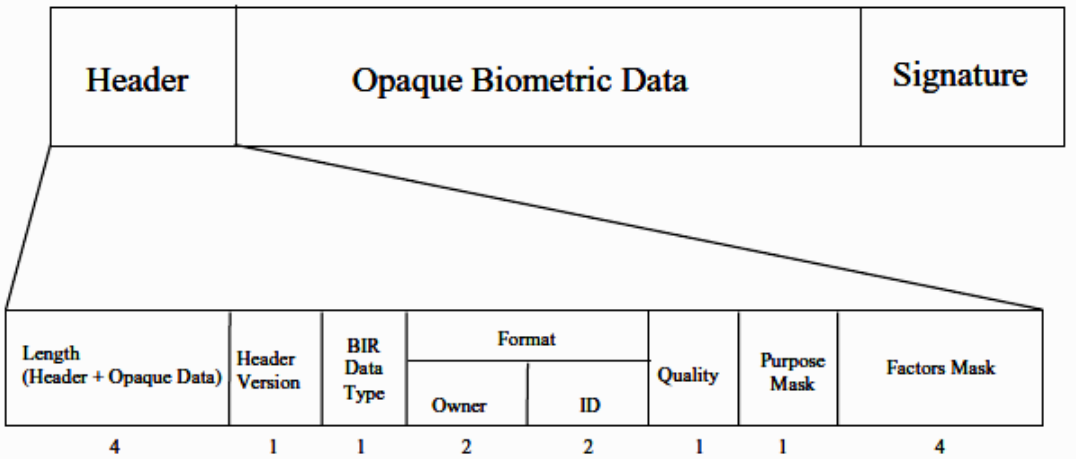


図 2　Biometric Information Records のデータ構造（出展：BioAPI Specification Version 1.1）

(3)　ACBio と BioAPI との関連

- ACBio は BIR のフィールド Opaque Biometric Data に含むためには少なくとも ACBio が Opaque Biometrics Data の形式の一つとして登録され，Data Type が必要となる．
- ACBio はロウデータやテンプレート，処理データなどの Sensitive データは扱わないことを特徴としているが，BIR ではロウデータ，中間データ，処理後のサンプルを含むことを前提としている．ACBio が BIR の Data Type として登録されない場合，以下のケースが考えられる．
  - ACBio において，同一エンティティ内のサブプロセス間では BIR の生成は不要となり BioAPI とは矛盾しないと考えられる．
  - BioAPI では，エンティティ間通信にて BIR を送受信することとなっている．BIR 送信の際 ACBio を BIR の付加情報として添付することために BioAPI と連動する API を独自に持つか，BioAPI の拡張として API を定義する必要がある．
- BioAPI 定義の構造体 **BioAPI_BOOL**, **BioAPI_BSP_SCHEMA, BioAPI_DEVICE_SCHEMA, BioAPI_CANDIDATE 等**において ACBio 生成に利用可能なメンバが存在する．

```
typedef  uint32 BioAPI_BOOL;
#define BioAPI_FALSE            (0)
#define BioAPI_TRUE             (!BioAPI_FALSE)
```

```
typedef struct bioapi_candidate {
        BioAPI_IDENTIFY_POPULATION_TYPE Type;
        union {
            BioAPI_UUID_PTR BIRInDataBase;
            uint32 *BIRInArray;
        } BIR;
        BioAPI_FAR   FARAchieved,
        BioAPI_FRR   FRRAchieved,
} BioAPI_CANDIDATE, *BioAPI_CANDIDATE_PTR;
```

(a) **BioAPI_BOOL**　　(c) **BioAPI_CANDIDATE**

(b) **BioAPI_DEVICE_SCHEMA**　　(d) **BioAPI_BSP_SCHEMA**

図３　BioAPI 定義のうち ACBio にて利用可能な構造体の例

```
typedef struct _bioapi_device_schema {
            BioAPI_UUID ModuleId;
            BioAPI_DEVICE_ID DeviceId;
            BioAPI_BIR_BIOMETRIC_DATA_FORMAT DeviceSupportedFormats;
            uint32 NumSupportedFormats;
            uint32 SupportedEvents;
            BioAPI_STRING DeviceVendor;
            BioAPI_STRING DeviceDescription;
            BioAPI_STRING DeviceSerialNumber;
            BioAPI_VERSION DeviceHardwareVersion;
            BioAPI_VERSION DeviceFirmwareVersion;
            BioAPI_BOOL AuthenticatedDevice;
      } BioAPI_DEVICE_SCHEMA, *BioAPI_DEVICE_SCHEMA_PTR;
```

```
typedef struct _bioapi_bsp_schema{
            BioAPI_UUID ModuleId;
            BioAPI_DEVICE_ID DeviceId;
            BioAPI_STRING BSPName;
            BioAPI_VERSION SpecVersion;
            BioAPI_VERSION ProductVersion;
            BioAPI_STRING Vendor;
            BioAPI_BIR_BIOMETRIC_DATA_FORMAT BspSupportedFormats;
            uint32 NumSupportedFormats;
            uint32 FactorsMask;
            uint32 Operations;
            uint32 Options;
            uint32 PayloadPolicy;
            uint32 MaxPayloadSize;
            sint32 DefaultVerifyTimeout;
            sint32 DefaultIdentifyTimeout;
            sint32 DefaultCaptureTimeout;
            sint32 DefaultEnrollTimeout;
            uint32 MaxBspDbSize;
            uint32 MaxIdentify;
            BioAPI_STRING Description;
            char Path;
      }BioAPI_BSP_SCHEMA, *BioAPI_BSP_SCHEMA_PTR;
```

添付資料１１）

平成 18 年 1 月 24 日

修正：平成 18 年 2 月 2 日

「バイオメトリクス認証結果保証基盤の研究開発」に関わる WG

第 3 回 WG 議事録

作成者：標準化仕様 WG 主査　上繁　義史

（(財）九州システム情報技術研究所）

日時：平成 17 年 11 月 22 日（火）10：00～12：00

場所：ニューメディア開発協会 D 会議室

出席者：主査　上繁義史（九州システム情報技術研究所）

幹事　才所敏明（東芝ソリューション）

委員　磯部義明（日立製作所）

松本　泰（セコム）

山田朝彦（東芝ソリューション）

オブザーバ　小谷光弘（経済産業省）

川根祐二（九州システム情報技術研究所）

事務局　滝沢俊男（ニューメディア開発協会）

岸本芳典（ニューメディア開発協会）

（敬称略）

1. 前回議事要旨の確認

・修正無しで承認された.

2. 議　事

（1）標準化会合の進捗状況

・資料に基づき山田委員より以下の通り報告があった.

i) Advisory Group Meeting on Biometrics ラポータとの事前協議

・Tekampe 氏（ラポータ）と事前協議を行った.

－SC37 より，Joint Rappourtor Group（SC27，SC37)の合議グループ設置の提案があったとのこと

＋JRG は不要と考えるが、AGMonBio で議論する.

ii)AGMonBio の会合

・各セッションの結果を Recommendation として HOD に上げる

・JRG の利点がなく，従来のリエゾンでよいと考える.

・BAC の名称の問題⇒ACBio に改称予定である旨説明

iii)BAC プロジェクトセッション

・以下について議論が行われたとのこと.

・SC37 との協力関係について

－SC27 と SC37 のチェア間の合意はないことを確認.
⇒SC37 にリエゾンシステムの改良へ向けた働きかけを行う

・コメント処理について
－SC27NB ドイツ，ポーランド，アメリカからコメントがあった.
－ドイツ NB：
＋SC37 の用語に順じるべきである⇒対応する旨回答.
＋BAC の名称変更が必要⇒ACBio への改称を行う旨回答.
＋ハッシュが入っていることを分かりやすく明示すべきである.
⇒対応する旨回答.
＋カードへの処理負荷を考える必要がある.
⇒SC17 と連携を検討する旨回答.
＋CBEFF とのデータとの共通性を考慮する必要がある.
⇒CBEFF のデータで流用できるものを共用することを検討する旨回答.
＋全体で Accept
※ドイツ NB に一部読み違いあり⇒BAC の命名意図について，日本より説明
・ポーランド NB：
－Editorial な指摘が 1 件⇒対応する旨回答.
・アメリカ NB：
－BAC 構造，テンプレート証明書のシンタクスを定義する必要がある.
＋シンタクスの案を出してくれた.
⇒19092-2，CBEFF との整合性を考慮した上で、受け入れる予定である.
－Verifier Controlling Value の定義誤り？
－用語"authenticator"の利用を再考する必要がある.
・SC37 からのコメント：
－SC37（WG2）からリエゾンメンバがリストアップされているが来なかった.
－BioAPI への影響を懸念
⇒現行の API を変更することなく拡張できると考える旨回答.
－CBEFF への影響への懸念
⇒BAC と CBEFF は目的が異なり統一に必要がないと考える.
一部重複する部分があるため，その部分については統一する旨回答.
－PKI との連携の難しさへの懸念
⇒PKI に拘らず，それ以外のモデルについても考える旨回答.
具体的なモデル例の提示を要請
・SC17 からのコメント
－SC37 の用語に従う必要がある⇒対応する旨回答
－5 サブプロセスモデル以外にも対応できるようにすべきである
⇒検討する旨回答.
・ITU-T からのコメント

－SC37 を含めた合議体制の構築が必要

＋SC17, SC27, SC37, ITU-T で！

⇒SC37 へのリエゾン回答と同様の回答をするとのこと.

－評価方法論の検討が必要

⇒SC37/WG5，SC27/WG3 の成果活用の旨回答

－証明書の URI の指示方法を保護

⇒検討する旨回答

・コメント処理結果，2ndWD を SC27 に提出.（締切：12 月 15 日）

(v) HoD ミーティング

・苗村先生が出席

・SC37 提案の JRG 対応方針を議論.

・SC37 への LS 内容確認

・SC27 新体制への移行（WG を 3 つ⇒5 つ）

－理由は WG1 が拡大しすぎたため.

－WG2：タイムスタンプを WG4，バイオメトリクスを WG5 に移す.

－WG5：Privacy, Identity and Biometric Security

・質疑応答：

＋質問（磯部委員）：SC37 のリエゾンは参加していないのか？

⇒回答（山田委員）：自分らのセッションには来ていない.

回答（才所幹事）：5 名指名されたと聞いたので議論ができるのを期待していた

＋コメント（才所）：12/15 までにコメントを提出するが，LS 原案は了承された．LS 対応については

SC27 の WG2，WG3 が絡むため，両方一括して出すとのこと.

リエゾンシステム改良（SC27，SC37 関係者の相互招待）が決まっている.

＋質問（滝沢氏）：アメリカが送ってくれたものとは？

⇒回答（山田委員）：ASN.1 形式のテンプレート証明書等の内容を送ってくれた．CBEFF との整合性を考慮すべきと考えている.

＋質問（小谷オブザーバ）：会議参加国は Active Participation か？

⇒ちがう.

＋質問（小谷オブザーバ）：SC17 の IC カードの関連は？

⇒回答（山田委員）：通信負荷よりも記憶データのサイズが問題．CBEFF とは管理情報でいくつか共通項があるので一本化を図りたい.

＋質問（磯部委員）：パスポートのように，特徴抽出結果を登録するのではなく，（正規化された）画像が格納されている場合, 登録データについても前処理が必要となる場合があるが、ACBio はこのモデルに対応しているのか？

⇒回答（山田委員）：現在はなっていないので対応する.

＋質問（磯部）：その際，CBEFF は係らないのか？

⇒回答（山田委員）：ロウデータの出力に関しては係るが，BAC が渡されるタイミングはロウデ

ータが渡されるのとは異なるタイミングとなる.

回答（山田委員）：BioAPI との関係において, BAC を生成する必要があることを知らせる API と BAC の出力を要求する API を定めれば良い.

＋質問（磯部委員）：上記内容は今回のリエゾンには書かれているのか？

⇒回答（山田委員）；書かれていない

回答（才所幹事）：何らかのタイミングで提示する.

（2）関連技術に関する調査報告

・上繁主査より BioAPI（Version1.1）と ACBio の関係について資料に基づき説明が行われた.

・BioAPI のバイオメトリックデータを格納する BIR に ACBio のデータを格納する場合には, BioAPI の Data Type への ACBio の追加が必要.

・BioAPI に定義されている構造体のメンバが ACBio と共通するものがあり，ACBio は必ずしも BioAPI と矛盾するとはいえない.

・質疑応答：

－質問（小谷オブザーバ）：BioAPI で定義されている構造体と ACBio と違いは？

⇒回答（上繁主査）：少なくとも報告で挙げたものは共通項と考えている.

－コメント（磯部委員）：バージョン 2 の違いはエンティティ通信の部分が PC 内で複数の Biometric Function Provider がある．バージョン 2.0 を調査すべきである.

⇒回答（上繁主査）：次回 WG 会合までに調査する.

・コメント（才所幹事）：ACBio で担当する部分を十分に絞り込む必要がある．本プロジェクトではセキュリティのフレームワークの定義に集中する．このフレームワークを使うアプリケーションについてはそれぞれの標準化団体に検討をお願いしていくことになる.

（3）次回会合予定

次回会合：平成 18 年 1 月 24 日　15：00～17：00

以上

添付資料１２）

平成 18 年 1 月 24 日

Authentication Context for Biometrics（ACBio）と Bio Application Programming Interface（BioAPI）Version2.0 との関連について

作成者：標準化仕様 WG 主査　上繁　義史
（(財）九州システム情報技術研究所）

１　概　要

SC27/WG2 提案の Authentication Context for Biometrics（ACBio）は，オープン環境におけるバイオメトリック認証に関して認証環境，精度，結果などについて各エンティティが生成するデータ構造を規定する．ACBio の標準化，また ACBio と関連する標準化において，実装上のインタフェースを規定している BioAPI との関連性（整合性）が十分に保証される必要がある．
本報告では，ACBio に先行して SC37 にて標準化が進められている BioAPI Ver 2.0 Part 1（FDIS）について調査を行い，ACBio 等との整合性について検討を行った結果について述べる．

２　BioAPI Ver 2.0 について

1）　BioAPI アーキテクチャ

図 1 に BioAPI API/SPI のモデル図を示す．下図によれば，一つの BioAPI Framework が複数の SPI を介して BSP（Biometric Service Provider）を（もしくは図 2 のように BFP（後述）により間接的に）管理することが出来る．また，BioAPI Framework は対応する API を介して複数のアプリケーションに対応することが出来る構造となっている．

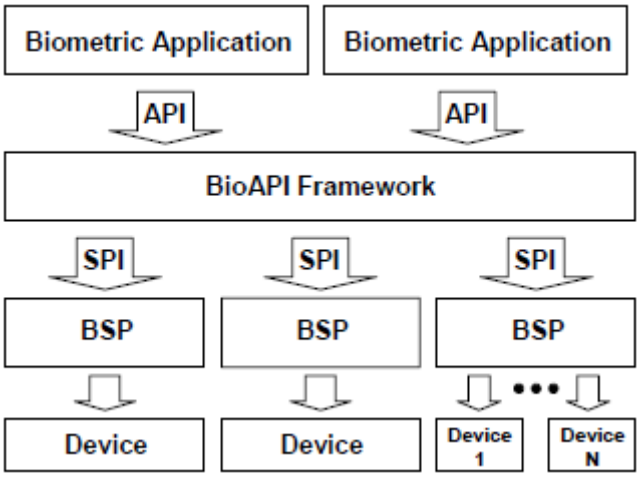


図 1　BioAPI API/SPI のモデル（出展：ISO/IEC FDIS 19784-1）

2）　Biometric Service Provider（BSP）

BioAPI Ver 2.0 では BSP は「ユニット（Unit）」と，インタフェースを通じて直接接続されるか，もしくは BFP（Biometric Function Provider）を通じて間接的に接続される．「ユニット」はデバイス等をより抽象化した概念である．なお，ユニットは 19784-1 では『現在』以下のカテゴリーが定義されている．

- Sensor Unit
- Archive Unit
- Matching algorithm Unit
- Processing algorithm Unit

※　BioAPI Ver 1.1 では BSP はインタフェースを通じて「デバイス」に接続されていた.

3)　Biometric Function Provider（BFP）

BFP は BioAPI Ver 2.0 において拡張された部分である. BFP は Function Provider Interface（FPI）を介して外部 BSP 関数を BSP に提供する．現在 BFP には 4 種類のカテゴリー：

- Sensor BFP
- Archive BFP
- Matching algorithm BFP
- Processing algorithm BFP

が存在するが，文中では"the current categories"と表現しており，上記以外のカテゴリーにも整合する余地を残していると考えられる.

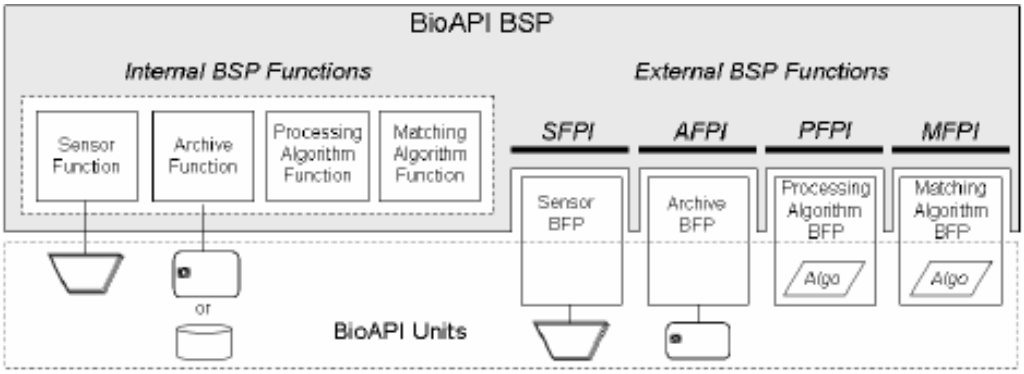


図 2　BSP アーキテクチャ（出展：ISO/IEC FDIS 19784-1）

※　BSP は複数の Units を管理することが出来るが，Attach できるのは一つまでである.

※　FPI については 19784-1 では標準化されていない.

4)　Biometric Information Record（BIR）

BIR は図 3 に示すようにセキュリティに関する拡張を中心に更新されている．すなわち，ヘッダ（SBH），Opaque Biometric Data Block（BDB），Security Block（SB）の先頭に，それぞれ BIR のデータ長，BDB のデータ長，SB のデータ長が加わり，なおかつ SBH にセキュリティに関するデータが格納される形式となっている. なお, BDB は基本的に BioAPI Ver 1.1 から変更は見られない.

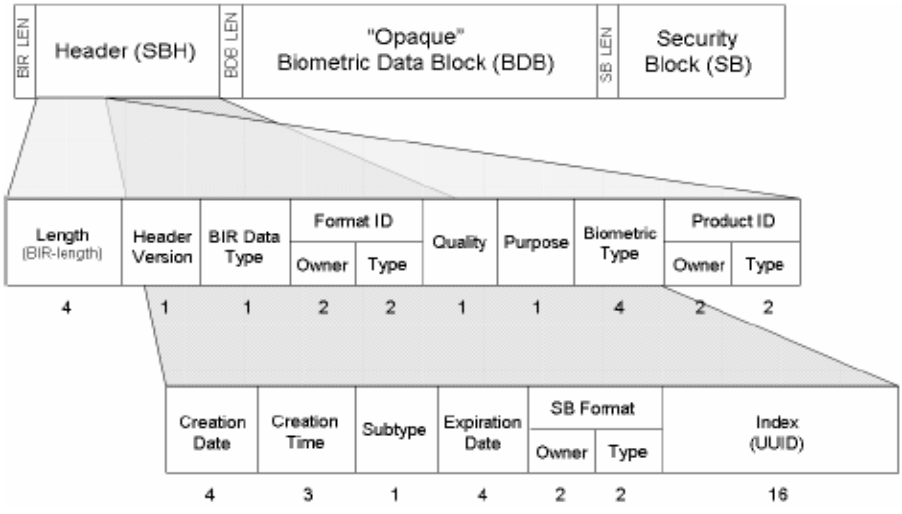


図3　Biometric Information Record（出展：ISO/IEC FDIS 19784-1）

3. BioAPI 変数型，マクロ定義

BioAPI Ver 2.0 において，Ver1.1 からの拡張，更新は主に以下の項目についてである：

- BFP に関する構造体
- Unit に関する構造体（デバイスに関する構造体を Modify したもの）
- BIR のヘッダ（SHB）のセキュリティに関するデータ（時間，日付の書式）等

4. ACBio との互換性に関する評価

- BSP もしくは BFP にて，ユニットの状態をチェックする（デバイスが問題なく動作，もしくはエラーなど）ことが可能であり，ACBio を構成するコンテクストの一部については BioAPI Ver 2.0 にて生成可能と考えられる.
- BFP とユニットについては，上記で述べたように現在 4 つのカテゴリーについてのみの標準化となっている．BFP にてプライベートな関数（標準に書かれていない関数）の拡張が可能であれば，ACBio における entityEvaluationReport の参照，生成が可能になると思われる.
- ACBio の Template Certificate について，BIR のデータを一部共用することが可能であるが，基本的に BIR の BDB 中で Sensitive Data を扱うというコンセプトには更新がなく，完全な互換性は保証されない.
- 基本的に BioAPI Ver 2.0 において，単一の BioAPI Framework にて複数のアプリケーションに対応する形式となっており, BioAPI Framework を介さずに生体認証のアプリケーションを動作させることは出来ない．ACBio の生成は，アプリケーション（図 1 の Biometric Application）上で API を介してユニットの動作状況についてのデータを取得して，行うことが考えられる.

以上

添付資料１３）

平成 18 年 2 月 2 日

「バイオメトリクス認証結果保証基盤の研究開発」に関わる WG
第 4 回 WG 議事録

作成者：標準化仕様 WG 主査　上繁　義史
（九州システム情報技術研究所）

日時：平成 18 年 1 月 24 日（火）15：00～17：30

場所：ニューメディア開発協会 D 会議室

出席者：主査　上繁義史（九州システム情報技術研究所）
委員　磯部義明（日立製作所）
山田朝彦（東芝ソリューション）
オブザーバ　小谷光弘（経済産業省）
川根祐二（九州システム情報技術研究所）
事務局　滝沢俊男（ニューメディア開発協会）
（敬称略）

1. 前回議事要旨の確認

・ 要修正部分をメールにて確認の上，承認

2. 議　事

（1）国際標準化の進捗状況について（山田委員）

(i)　SC37 京都会合参加報告

・ 才所幹事，山田委員が SC37/WG2（アプリケーションインタフェース）の標準化の席で ACBio についてプレゼンを行った.
－Other Topic にて時間をいただいた.（11 日午後）
－出席者は 20 名程度.

・ 才所幹事，山田委員より，SC37 側の懸念に対して説明がなされた.
－SC37 から BioAPI，CBEFF への影響について懸念が示された.
⇒才所幹事，山田委員より，ACBio とこれらとの目的が異なっており，影響が（ほとんど）生じないと考えている旨回答した.
＋ CBEFF と Template Certificate の共通項目⇒CBEFF の形式を Template Certificate にて参照する旨回答した.
＋ BioAPI については ACBio に関する処理を行う API を（２つ）追加すればよいと考えられる旨回答した.
－SC37/WG2 内にて ACBio について SC37 としての見解をまとめるために，Special Group が設置されることとなった.（3 月 6 日，もしくは 7 日に開催予定）

・質疑応答等：
－質問（小谷オブザーバ）：CBEFF との親和性とは CBEFF で使えるデータは使うという意味か？

⇒回答（山田委員）：テンプレートの有効期限，発行者など，CBEFF とテンプレート証明書に共通するものは，CBEFF の定義を適用するということである

－質問（小谷オブザーバ）：（SC37/WG2 にて設置される）Special Group のメンバーは？

⇒回答（山田委員）：メンバーは以下の通り

Greg Cannon（Chair をつとめる），Fred Herr（CBEFF Editor), John Larmouth, Alessandro Triglia, Krister Walfridsson, Toshio Nakamura, Cathy Tilton（BioAPI Editor），Young Bin Won（WG２ コンビーナ）

－質問（上繁主査）：SC37/WG2 で指摘された BVP の不十分さとは何か？

⇒回答（山田委員）5 サブプロセス以外のモデルに適用できない点である.

－質問（磯辺委員）：説明の図では，BioAPI Units に ACBio の実体があるようだが.

⇒回答（山田委員）：BioAPI Unit＝エンティティと考えて図示していた.（SC37 で「そうでない」との指摘があった.）

(ii)　SC27/WG2 マドリード会合に向けての取り組み

・1st WD へのコメントに対応し，2nd WD2 を提出する.

（2）関連技術調査報告（上繁主査）

- BioAPI Ver 2.0（FDIS 19784-1）について，Ver1.1 との違いを中心に概要を報告.
- ACBio と BioAPI Ver 2.0（FDIS 19784-1）の構造に齟齬がないかについてコメントを報告.
- 質疑応答等：

－コメント（山田委員）：Biometric Application のレベルではなく BioAPI Unit と同じレベルで実装しないとできないだろう．BioAPI に ACBio 生成に関する関数が組み込まれるのがベストと考える.

－コメント（山田委員）：SC37 からは，ベンダが実装する上で困らないようにとのコメントがあった.

－コメント（山田委員）：CBEFF に整合するように ACBio の仕様を書いて，パトロンフォーマットと共通の枠組みの中で実装されればよいと考える.

－コメント（磯部委員）：ACBio に対応する実体である BIR と齟齬（矛盾）がなければ問題ない.

－コメント（磯部委員）：BioAPI におけるカテゴリーはバイオメトリクスの処理についてのカテゴリーであって，セキュリティは対象外ではないかと思う．それぞれのカテゴリーで ACBio の情報生成がなされれば良いと考える.

（3）活動のまとめ

- 上繁主査より，第 1 回 WG～第 4 回 WG の活動および WG に関連する諸活動について総括，コメントがあった.
- 各委員，オブザーバより WG の活動についてコメント.

以上

４．５　添付資料　ＩＳＯ／ＩＥＣＷＤ２４７６１．２

以下に、提案されたＡＣＢｉｏ（ＩＳＯ／ＩＥＣＷＤ２４７６１．２）ドキュメントの写しを示す。