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１～2 部　委託業務実施状況

平成１８年３月

財団法人ニューメディア開発協会

目　　次

１　はじめに

本事業においては、ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７を中核とした国際標準化機関への具体的な標準化提案をする目的のため、バイオメトリクス認証技術を研究開発する企業、大学研究機関、利用を促進する関係機関の総意を形成するべく、また産業界における利用者の幅広い意見を集約し、現行の標準化体制への補完的な提言も含めて取りまとめ、実効性のある提言をまとめていくこととしている。

具体的には、生体情報による個人識別技術（バイオメトリクス）は、他人へのなりすましや、偽造を防ぐ有効な手段として期待されており、安全な社会の実現には不可欠な技術である。その実用化を推進するために、基盤技術である評価基準、評価環境等に関する国際標準案を策定して、国際標準化機構（ＩＳＯ）と国際電気標準会議（ＩＥＣ）の合同専門委員会（ＪＴＣ１）の分科委員会（ＳＣ２７）（ＳＣ３７）等へ提案することを目指して活動した。

本事業は、３年間で一定の成果を挙げることを予定しており、今年度は、その最終年度の事業を実施したので、以下にその内容を報告する。

２　委託業務実施状況

２．１　事業の目的

生体情報による個人識別技術（バイオメトリクス）は、他人へのなりすましや偽造を防ぐ有効な手段として期待されており、安全な社会の実現には不可欠な技術である。その実用化を推進するために、本事業では、基盤技術である評価基準、評価環境等に関する国際標準案を策定して、国際標準化機構（ＩＳＯ）と国際電気標準会議（ＩＥＣ）の合同専門委員会（ＪＴＣ）１の分科委員会（ＳＣ）３７等へ提案することを目指した。

バイオメトリクスを情報セキュリティ分野に適用するには、バイオメトリクスの安全性評価が重要である。しかし現状では、情報セキュリティの観点に基づいたバイオメトリクスの安全性に関する検討が十分とは言えない。

そこで本事業では、以下の４項目の研究開発を実施し、その成果をＩＳＯ／ＩＥＣＪＴＣ１のＳＣ１７、ＳＣ２７、ＳＣ３７等へ提案することを目的として実施した。

１）バイオメトリクスセキュリティ評価基準の研究開発
２）バイオメトリクス認証結果保証基盤の研究開発
３）バイオメトリクスの可搬型メディアに応用するための技術調査
４）金融分野におけるバイオメトリクス認証モデルの開発

２．２　事業の実施状況

（１）バイオメトリクスセキュリティ評価基準の研究開発

バイオメトリクスを情報セキュリティの製品分野に展開する上で重要なバイオメトリクスセキュリティ評価の基準について開発及び国際標準化提案を行った。

具体的には、以下の研究開発を実施した。

（ａ）バイオメトリクスのセキュリティ要件と評価方法の開発

昨年度の成果を国際会議で提案を行ったところ、ＩＳＯ／ＩＥＣ１９７９２（ＳＣ２７）

「バイオメトリクスにおけるセキュリティ評価のフレームワーク」の脆弱性分析として採用が決まったことを踏まえて、今年度は、エディタとして本国際標準原案の詳細かつ具体的な開発を行いＳＣ２７国際会議に提出した。

（ｂ）バイオメトリクスの脅威及び脆弱性公開におけるガイドライン策定

昨年度の成果であるバイオメトリクスの脅威及び脆弱性分析を基に、早稲田大学小松尚久教授との共同研究により、バイオメトリクスの脆弱性公開ガイドライン詳細仕様の策定を行った。

（ｃ）バイオメトリクスの脆弱性の評価実験

横浜国立大学松本教授及び早稲田大学小松教授との共同研究により、バイオメトリクスにおける脆弱性の評価（攻撃）研究を実施した。

（２）バイオメトリクス認証結果保証基盤の研究開発

バイオメトリクスをネットワーク等のオープン環境に適用するには、認証者（認証する組織、人等）に対して安全な環境と認証結果が改竄されていないことを保証する必要がある。本研究開発では、主にＥＣ（電子商取引）／ＥＧ（電子政府）を対象としたモデルを想定する。このモデルでは、ユーザの管理下に置かれたトークン（ＩＣカード等）と、同じくユーザの管理下に置かれたバイオメトリクス照合装置を用いて、ＥＣ／ＥＧサーバに対してユーザの認証結果を伝える。このとき、クライアント側でのバイオメトリクス照合プロセスや、バイオメトリクス装置の妥当性をサーバ側で検証するメカニズムが必要になる。本活動では、ユーザの管理下で行われるバイオメトリクス認証結果の妥当性をサーバ側で検証するためにサーバ側へ通知するデータ項目及びデータ形式の国際標準化を目指し、以下の作業を実施した。

（ａ）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

ユーザ管理下で行われるバイオメトリクス認証の結果妥当性をサーバ側で検証可能にするための、ユーザ管理下の装置からサーバへ送付するデータ項目及びデータ形式について国際標準案（ＡＣＢｉｏ）を策定し、ＳＣ ２７へ提案した。

（ｂ）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

ＳＣ ２７、ＳＣ３７を始めとする各国際標準化団体での関連する標準化提案に対して、策定した国際規格案の視点から分析した。分析結果を基に、必要に応じ、ＡＣＢｉｏ国際標準案に対してコメントした。

（ｃ）標準化仕様WG活動

国内関係者への、策定原案、海外キーパーソン・関係各国の動向、国際標準化の見通しなどを報告するとともに、意見を聞きながら標準化活動を進めた。

（３）バイオメトリクスの可搬型メディアに応用するための技術調査

本事業では、対象とするバイオメトリクス＋トークン（ＩＣカード等）による本人認証システムにおけるアーキテクチャのモデル化とこれに対するセキュリティ機能･運用の双方を裏付けるセキュリティ分析を実施し、機能面と運用面の双方を考慮したシステム全体のセキ

ュリティ仕様（以下「セキュリティプロファイル」という。）を定めることを目的として実施した。

今年度は、平成１６年度の成果を引き継ぎ、以下の内容を検討した。

（ａ）セキュリティプロファイルの仕様拡充

平成１６年度はトークンを使用した職員認証システム（バイオメトリクスによる検証機能）を適用対象としたセキュリティプロファイルを策定したが、今年度はその適用範囲を広げ、バイオメトリクステンプレートを生成しトークンに格納するバイオメトリクス登録システムのためのセキュリティ仕様を検討し、ＳＣ３７国際会議に提案した。

（ｂ）国際規格素案の策定と業界内の意見集約・合意形成

平成１６年度成果と上記（ａ）による仕様拡充部分の国際標準案を策定し、国内外標準化機関（ＳＣ３７）へ提案した。また標準案策定にあたり、バイオメトリクスセキュリティコンソーシアム運用仕様策定部会ホームランドセキュリティタスクフォース内のセキュリティプロファイルサブワーキンググループを継続して活用し、業界有識者のコメント収集及び合意形成を行い、提案活動を実施した。

（４）金融分野におけるバイオメトリクス認証モデルの開発

金融業界では、印鑑と通帳の不正利用により、認証基盤の信頼性に影響が出ている。また、キャッシュカードのＩＣカード化などによりＡＴＭの利便性と安全性の向上への要求がある。昨年度は、金融分野における生体認証に関連する国際標準規格の調査を行い、金融におけるバイオメトリクスを利用した認証基盤の問題点の洗い出しと相互運用性を確保した認証モデルの開発を行った。

今年度は、金融分野の関連する国際標準規格ＩＳＯ／ＣＤ１９０９２を調査検討した昨年度に引き続き国際標準規格の調査とドキュメントへのコメントを行った。また、今後の重要なサービスとなるウエッブバンキングに関して、バイオメトリクス認証モデルを開発し、安全性を確保した端末との相互認証及び関係する法的な問題を洗い出し検討した。

（５）国際規格案骨子作成及び国際標準化活動

１）バイオメトリクスセキュリティ評価基準の研究開発

・ＩＳＯ／ＩＥＣ　ＪＴＣ１／ＳＣ２７の標準化案件である「バイオメトリクスにおけるセキュリティ評価のフレームワーク」作成への貢献を目的に活動した。
具体的には、株式会社日立製作所／三村昌弘がＣｏ－ｅｄｉｔｏｒとして国際標準化委員会の中心的な立場で国際標準原案の作成活動を行った。

・バイオメトリクスの脅威及び脆弱性公開におけるガイドラインに関しては、電子情報通信学会ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会（委員長：半谷精一郎教授（東京理科大））において 2005 年 9 月に開催されたパネル討論で議論し、国際標準化を見据えた検討を行った。

２）バイオメトリクス認証結果保証基盤の研究開発

ユーザの管理下で行われるバイオメトリクス認証の結果の妥当性をサーバ側で検証するために必要なサーバ側へ通知するデータ項目及びデータ形式の国際標準案を策定し、ＳＣ２７へ提案した。また、速やかな国際標準化を目指し、国内外関係機関との協議を行った。

ＳＣ２７、ＳＣ３７を始めとする各国際標準化団体での標準化提案に対しては、策定した国際規格素案の関連技術動向の視点からの分析結果に基づき、必要に応じコメントなどを行った。

３）バイオメトリクスの可搬型メディアに応用するための技術調査

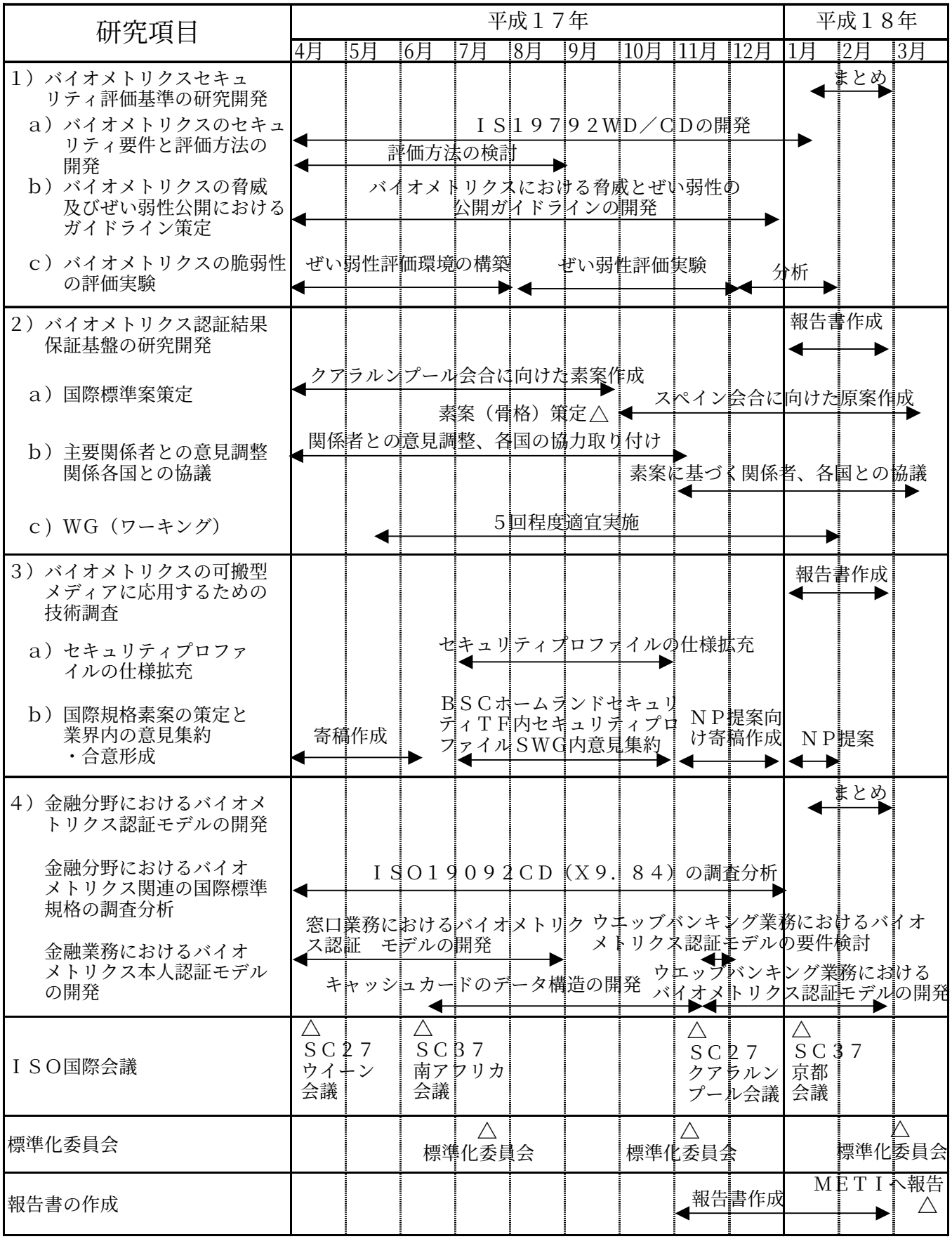
セキュリティプロファイルを国際標準案として、ＩＳＯ／ＩＥＣ　ＪＴＣ１／ＳＣ３７／ＷＧ４へ提案した。

具体的には同ＷＧの扱う「高セキュリティ環境下の従業員認証の為のプロファイル」（ＣＤ２４７１３－２）に対する寄稿として平成１７年６月に開催予定のＳＣ３７国際会議で提案を行った後、国際的な合意形成に努めた。平成１７年度事業成果として前記国際会議の結果を踏まえたセキュリティプロファイルを取りまとめ、平成１８年１月に京都で開催されたＳＣ３７国際会議で新規国際提案を行った。

４）金融分野におけるバイオメトリクス認証モデルの開発

ＩＳＯ／ＴＣ６８の標準化動向を見据えて、国内委員会（事務局：日本銀行金融研究所）を通して金融分野におけるバイオメトリクス認証モデル（ウェブバンキングにおけるバイオメトリクス認証モデル）の提案を図るため、ＩＳＯ１９０９２－２のウェブバンキングの記載を削除し、別パートとするように国内委員会に提言した。

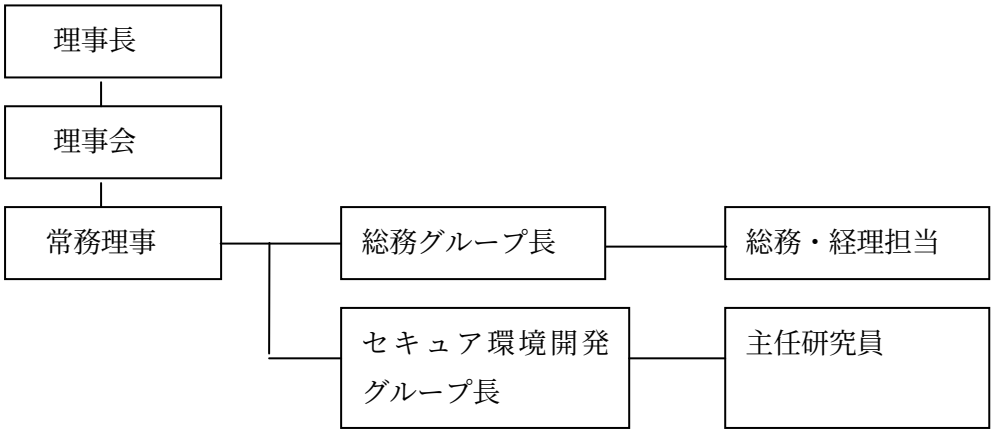
２．３　研究開発スケジュール



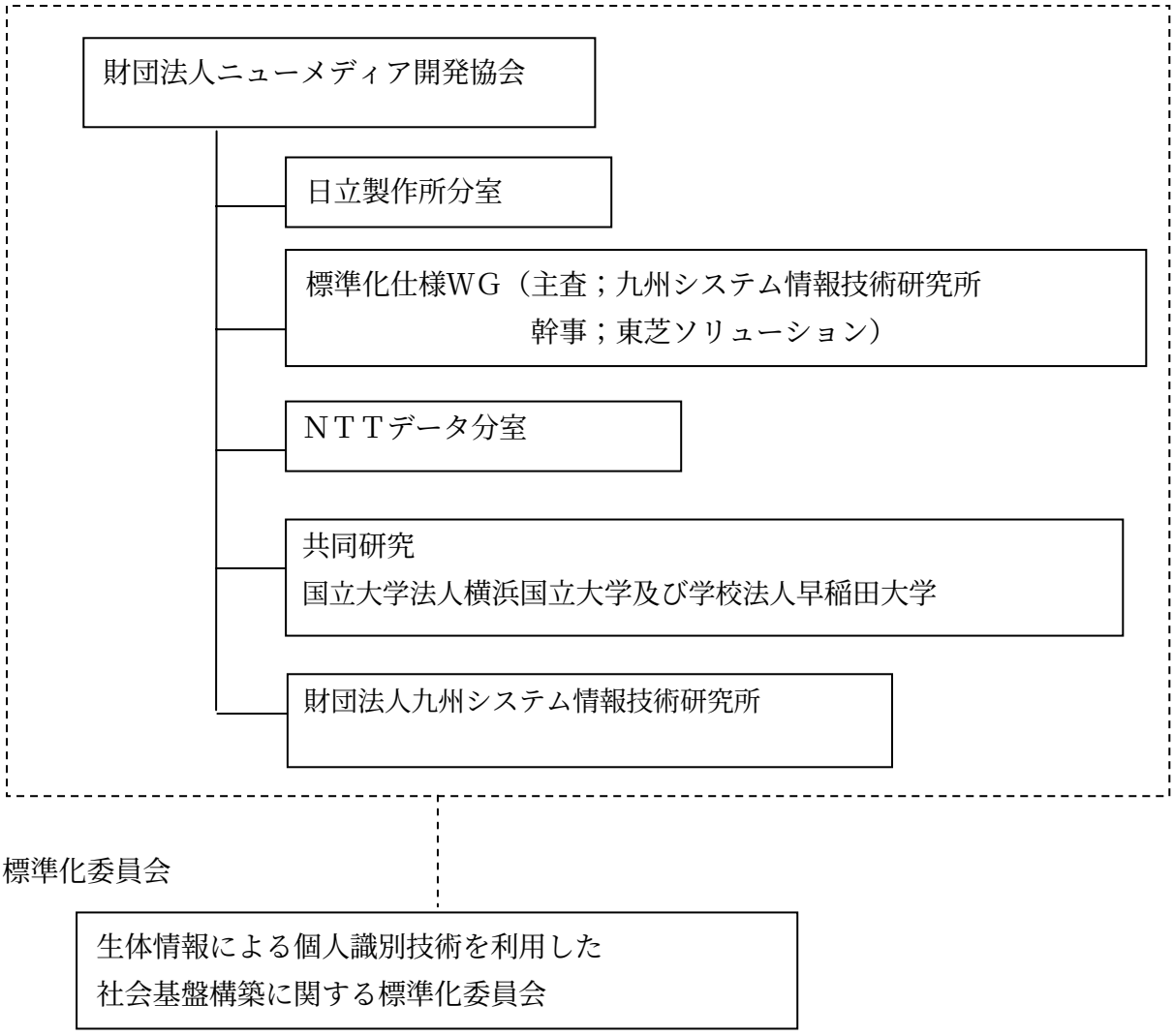
２．４　研究開発の実施体制

２．４．１　管理体制及び研究組織

（１）管理体制



（２）研究組織



社団法人日本自動認識システム協会の担当分も含めて行った。

２．４．２　標準化委員会構成メンバー

標準化委員会は、以下のメンバーで構成され、当初予定通り計３回実施した。

役割	氏名	所属
委員長	半谷精一郎	東京理科大学工学部電気工学科
幹事	瀬戸　洋一	SC37 国内委員会
委員	瀬戸　和吉	経済産業省産業技術環境局
委員	梅沢　茂之	経済産業省製造産業局
委員	牧内　勝哉	経済産業省商務情報政策局
委員	大山　永昭	SC17 国内委員会
委員	宝木　和夫	SC27 国内委員会
委員	梅崎　太造	名古屋工業大学大学院
委員	新保　史生	筑波大学大学院図書館情報メディア研究科
委員	鷲見　和彦	京都大学大学院情報学研究科
委員	池野　修一	BSC（ﾊﾞｲｵﾒﾄﾘｸｽｾｷｭﾘﾃｨｺﾝｿｰｼｱﾑ）基盤技術部会
委員	宇都宮　康夫	JAISA のバイオメトリクス部会
委員	上繁　義史	財団法人九州システム情報技術研究所
委員	国分　明男	財団法人ニューメディア開発協会
オブザーバ	勝亦　眞人	経済産業省産業技術環境局
オブザーバ	小谷　光弘	経済産業省産業技術環境局
オブザーバ	宮川　寧夫	独立行政法人情報処理推進機構
オブザーバ	宇田川荘二	社団法人日本自動認識システム協会
客員研究員	磯部　義明	株式会社日立製作所
客員研究員	三村　昌弘	株式会社日立製作所
客員研究員	才所敏明	東芝ソリューション株式会社
客員研究員	山田　朝彦	東芝ソリューション株式会社
客員研究員	梅田　伸明	株式会社ＮＴＴデータ
客員研究員	道坂　修	株式会社ＮＴＴデータ
事務局	中嶋　晴久	社団法人日本自動認識システム協会
事務局	林　義昭	財団法人ニューメディア開発協会
事務局	滝沢　俊男	財団法人ニューメディア開発協会
事務局	岸本　芳典	財団法人ニューメディア開発協会

２．４．３　標準化仕様WGメンバー

標準化仕様WGは、以下のメンバーで構成され、計４回実施した。

役割	氏名	所属
主査	上繁　義史	財団法人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	大日本印刷株式会社
オブザーバ	池野　修一	ＢＳＣ基盤技術部会
オブザーバ	小谷　光弘	経済産業省産業技術環境局
オブザーバ	瀬戸　洋一	ＢＳＣ会長代行
オブザーバ	川根　祐二	財団法人九州システム情報技術研究所
事務局	岸本　芳典	財団法人ニューメディア開発協会
事務局	滝沢　俊男	財団法人ニューメディア開発協会

２．４．４　共同研究

大学との共同研究については、以下の先生方により実施した。

共同研究者	大学名・所属	備考
松本　勉	横浜国立大学大学院環境情報研究院教授	脆弱性の研究
小松　尚久	早稲田大学理工学部コンピュータ・ネットワーク工学科教授	脆弱性及び対策手法の研究