オープンネットワーク上で安全に生体認証を行うための認証コンテキスト技術 ACBio

Authentication Context for Biometrics (ACBio) to Secure Biometric Authentication in Open Networks

山田　朝彦　　岡田　光司　　池田　竜朗
■ YAMADA Asahiko　■ OKADA Koji　■ IKEDA Tatsuro

近年，多くの金融機関のATM（現金自動預け払い機）では，利用者が本人かどうかを確認するために，指紋や静脈パターンなどを用いた生体認証技術が使われている。今後更に，インターネットなどオープンなネットワークを介した情報サービスでも生体認証技術が利用されると思われるが，いくつかの課題がある。

東芝ソリューション（株）は，それらの課題を解決するために，オープンなネットワーク上で安全に生体認証を行うための技術“生体認証のための認証コンテキスト技術 ACBio（Authentication Context for Biometrics）”を開発し，国際標準化活動を行った。ACBioによって，安全で相互運用性の高い生体認証を実現することができる。

Biometric authentication using body and behavioral features such as fingerprints and vein patterns, which has recently been introduced for automatic teller machines of banks, is expected to be applied to remote user authentication for online services such as Internet banking services in the near future.　However, there are several problems related to user privacy, security and convenience, and cost of the service.

To solve these problems, Toshiba Solutions Corporation has developed the Authentication Context for Biometrics (ACBio), a technology for secure remote biometric authentication in open networks such as the Internet, which was standardized as an International Standard.　With ACBio, more secure and convenient biometric authentication is realized.

1　まえがき

近年，様々な情報システムで生体認証技術を採用するケースが増えてきている。例えば，多くの金融機関のATMでは，利用者本人の確認に生体認証技術を採用している。生体認証技術は，指紋や静脈パターンなど，その人だけが持つ身体的・行動的特徴を利用して，あらかじめ登録された生体情報と採取した生体情報の特徴が一致するかを判定することにより，本人かどうかを確認する技術である。偽造あるいはまねしにくい，本人だけが持つ生体情報を利用することで，成り済ましの防止に非常に効果がある，強力な認証技術と考えられている。また，パスワード認証のように，パスワードを忘れてしまい認証ができなくなることがないため，利用者にとっても非常に使いやすい認証技術といえる。

しかし，生体認証技術が一般に普及してきているとはいえ，それらは特定のサービスでの利用にとどまっているのが現状である。例えば，金融機関のATMのように，店舗など特定の場所に設置された機械で利用されるケースがほとんどである。インターネット上のオンラインサービスで利用されるケースは，今のところ見受けられない。これは，オープンなネットワーク上で生体認証技術を利用するには，いくつかの越えなければならない課題があるためである。

そこで，東芝ソリューション（株）は，それらの課題を解決する“生体認証のための認証コンテキスト技術 ACBio（Authentication Context for Biometrics）”を独自に開発した[(1)-(5)]。このACBioは，2005年から国際標準化が進められ，2009年5月にISO（国際標準化機構）とIEC（国際電気標準会議）の国際規格として発行された[(6)]。ここでは，ACBioの概要と特長，及び今後の適用拡大の可能性などについて述べる。

2　生体認証技術の現状と課題

自宅のパソコン（PC）からオンラインサービスを利用するシーンを**図1**に示す。現状では，生体認証技術をオンラインサービスで利用しようとすると，以下に述べるような課題がある。

2.1　プライバシー

従来のパスワード認証と同じように生体認証技術を適用すると，本人確認をするサービス提供者側に生体情報を渡さなければならない。しかし，自分の生体情報がネットワーク上を流れることや，サービス提供者側に生体情報を渡してしまうことに抵抗や不安を感じる人は多い。

2.2　利便性とコスト

生体情報をネットワークに流さずに生体認証を行うためには，サービスごとに専用の生体認証機器を用意し，その機器の中だけで生体認証を実行して認証結果だけをサービス提供者側に通知することとなる。しかしこの場合，以下の問題がある。

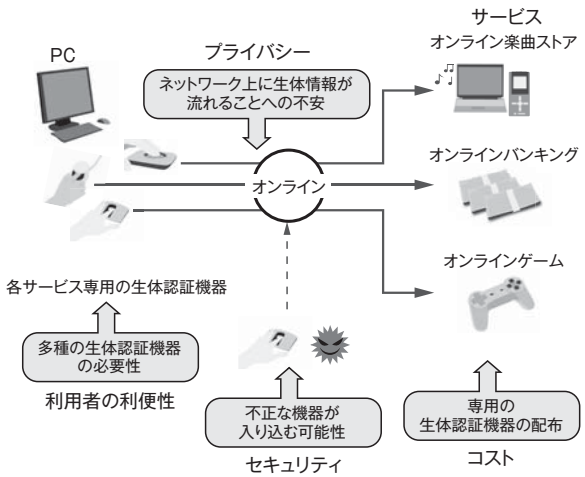

図1. 生体認証をオンラインサービスで利用するときの課題 — 現状では，生体認証技術をオンラインサービスで利用しようとすると，プライバシー，利便性，コスト，及びセキュリティの面で課題がある。

Issues in applying biometrics to online services

(1) 利用者の利便性を阻害　　サービスごとに専用の機器を用意するとなると，複数のサービスを利用する利用者はいくつもの生体認証機器を持たなければならない。一つの生体認証機器でいろいろなサービスを利用できるほうが，利用者にとって便利である。

また，利用者によっては指紋の採取が困難など，サービス提供者が採用している生体認証方式に対応できないという場合がある。このため，利用者が自分自身と相性のよい生体認証方式を選択できるほうがよい。

(2) サービス提供者側の負担　　サービス提供者側にとっても，専用の生体認証機器を多数の利用者全員に配布することは，コスト的に非常に大きな負担になり，現実的ではない。既存のサービスで利用している生体認証機器があれば，それを利用したほうがコストを低減できる。

2.3 セキュリティ

オープンネットワークを介したサービスの場合，不正な生体認証機器が入り込むリスクを考慮しなければならない。このため，安全な生体認証機器で処理が正しく実行されたことを，サービス提供者側で確認できる必要がある。

3 生体認証のための認証コンテキスト ACBio

3.1 生体認証処理の流れとACBioのデータ構造

ACBioは，生体認証の処理内容や結果を通知するための，共通的なデータ構造規格である。

生体認証の処理は，生体情報の採取，採取した生体情報からの固有パターン抽出，あらかじめ登録された生体情報（テンプレート）の保管，採取した生体情報とテンプレートの比較，比較結果から本人性を判定，といった複数のプロセスで実行される。更に，これらのプロセスは，一つの生体認証機器内で実行されることもあれば，複数の機器で連動して実行されることもある。例えば，ATMでの生体認証では，テンプレートが保管されているICカードと，生体情報の採取や比較を行うATM機器が連動して生体認証処理が実行される。更に，オンラインサービスでは，ICカード，センサ，PCなど，より多くの機器の組合せで生体認証処理が実行されることになると考えられる。

そこで，生体認証を行う場合，生体認証処理を実行した各機器が，その内部で実行された生体認証処理プロセスの内容や結果を，ACBioで規定された共通データ構造（ACBioインスタンス）で出力し，サービス提供者側へ送る(注1)。そして，サービス提供者側は，すべての機器から得られたACBioインスタンスを検証することで，生体認証処理全体の内容と結果を検証することができる。

ACBioの具体的なデータ構造を**図2**に示す。

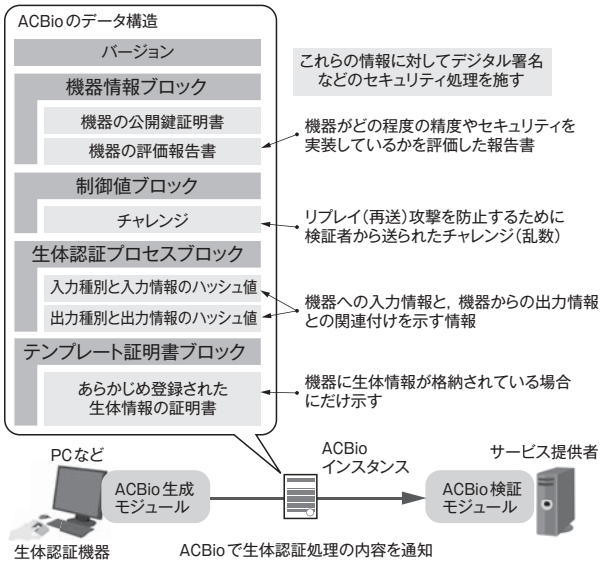

図2. ACBioのデータ構造 — ACBioは，単に処理内容を通知するだけでなく，信頼できる生体認証機器で正しく実行されたことを検証することが可能なデータ構造となっている。

Data structure of ACBio

3.2 ACBioインスタンスによる検証

ACBioは，単に処理内容を通知するだけでなく，“信頼できる生体認証機器で正しく実行されたこと”を検証することが可能なデータ構造となっている。これにより，サービス専用の生

(注1) ACBioでは，均質なセキュリティ強度を持ち，連続した生体認証処理のプロセスから成るハードウェア又はソフトウェアをBPU（Biometric Process Unit）と呼んで，このBPUごとにACBioインスタンスを出力する仕様となっている。

体認証機器だけを利用しなければならないという課題を解決できる。また，ACBioインスタンスには生体情報自体を含まなくてもよいため，生体情報がネットワーク上を流れてしまうという課題も解決できる。各生体認証機器から出力されたACBioインスタンスで検証できる内容は以下のとおりである。

(1) 生体認証機器は，生体認証処理として十分な精度と機器として十分な安全性を備えているか　　ACBioインスタンスの“機器情報ブロック”には，その機器が備える生体認証処理の精度や，機器が安全に実装されているかを評価した結果を示す機器評価報告書が記述される。この機器評価報告書は，公的又は業界団体などの第三者評価機関が製品を評価して発行することを想定している。サービス側は，この機器評価報告書を検証することで，生体認証処理の精度や機器の安全性を確認できる。

(2) 生体認証機器で正しく生体認証処理が実行されたか　　ACBioはチャレンジ−レスポンス認証に対応しており，サービス提供者側から送られてきたチャレンジ（乱数）がACBioインスタンスの“制御値ブロック”に記述される。更に，ACBioインスタンス全体に対して，機器が保持する秘密鍵を用いて電子署名又は認証子が生成され，ACBioインスタンスに付与される。これによって，ACBioインスタンスのリプレイ（再送）攻撃が防止されるとともに，正しい機器で処理が実行されたことを検証できる。

(3) 複数の生体認証機器の間で，データが正しく授受されたか　　ACBioインスタンスの“生体認証プロセスブロック”には，機器で実行された生体認証処理プロセスの種別と，機器の入出力のハッシュ値が記述される。これにより，複数の機器で生体認証処理が行われた場合でも，機器間で正しくデータが授受されたかどうかを検証できる。また，前述の制御値ブロックの値が同一であるかを確認することで，一貫した生体認証処理であることも検証できる。

(4) 正しいテンプレートが使われたか　　最後に，採取した生体情報との比較に用いられたテンプレートが正しいものかどうかを検証できる必要がある。このため，テンプレートを保管する機器が出力するACBioインスタンスの“テンプレート証明書ブロック”には，テンプレート証明書が記述される。このテンプレート証明書は，信頼できる第三者機関が，あらかじめ採取した生体情報が本人のものであることを確認したうえで，それを保証するために発行されることを想定している。サービス提供者側は，このテンプレート証明書を検証することで，正しいテンプレートが用いられたことを確認できる。

3.3 国際標準化

ACBioは，ISO/IEC JTC 1/SC 27(注2)で，ISO/IEC 24761 Authentication Context for Biometricsとして2005年から国際標準化のプロジェクトが開始され，当社がエディター（編さん責任者）を務めた。そして，2009年5月に国際規格として発行された。

また，ISO/IEC JTC 1/SC 37で審議されているそのほかの生体認証技術の国際規格（ISO/IEC 19785-4 CBEFF Part 4(注3)，ISO/IEC 19784-1 BioAPI Part 1 Amd.3(注4)）でも，ACBioを利用する仕組みが検討されている。これらについても当社がエディターを務め，国際標準化を進めている。

4 ACBioへの期待

ACBioに対応した機能を携帯電話などに搭載することによって，**図3**に示すように日常生活の様々なシーンで，生体認証を用いた，より手軽で安全な本人確認の仕組みが実現される。これにより，利用者とサービス提供者にとって，次のようなメリットが生まれる。

(1) 生体認証機器の利用者専用化　　携帯電話などにACBio機能が搭載されれば，オンラインやオフラインを問わず，携帯電話一つで様々なサービスに対して生体認証を使った本人確認を行うことができる。利用者は，いくつ

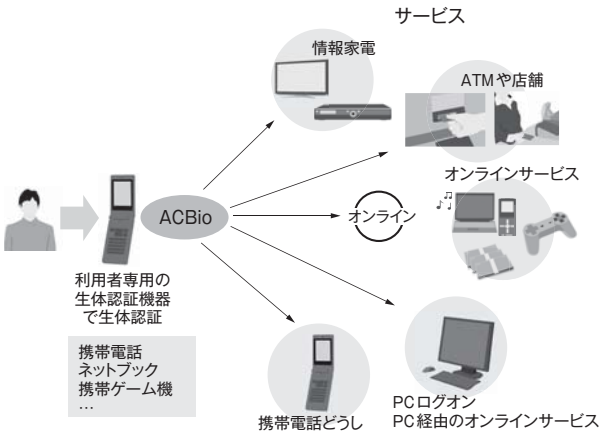

図3. ACBioを使った生体認証の活用例 — 携帯電話にACBio機能を搭載することにより，携帯電話一つで様々なサービスに対して生体認証を使った本人確認を行うことができる。

Examples of user authentication services using ACBio

(注2) ISO/IEC JTC 1（第一合同技術委員会）は，それぞれの専門分野を担当するSC（専門委員会）から構成される。SC 27専門委員会はITセキュリティ技術を担当する専門委員会，SC 37専門委員会は生体認証技術を担当する専門委員会。

(注3) CBEFF（Common Biometric Exchange Formats Framework）は，生体情報データを共通的に取り扱うためのデータ構造規格。CBEFF Part 4では，CBEFFにおける各種セキュリティ情報を格納するためのセキュリティブロックを規定している。

(注4) BioAPI（Biometric Application Programming Interface）は，生体認証に関連するアプリケーションの共通的なインタフェースを規定したAPI規格。BioAPI Part 1 Amd.3ではBioAPIにセキュリティ情報の取扱いを追加した追補仕様を規定しており，この中でACBioを授受する仕組みが検討されている。

もの生体認証機器を持つ必要がなくなり，自分に合った生体認証機器を選択できる。

(2) 検証モジュールの共通化　　サービス提供者側にとっても，ACBioに対応する検証モジュールを一つだけ用意すれば，多様な生体認証方式と生体認証機器とに対応できるようになる。これにより，生体認証技術を採用する際の初期導入コストなどの軽減が期待できる。また，将来的に，より強力な生体認証方式や，安くて安全な生体認証機器が登場してきたとしても，それらがACBioに対応していれば移行導入しやすくなる。

5　あとがき

現在，生体認証機器の小型化が進んできており，携帯電話をはじめとする様々な機器に搭載され始め，より多様な分野で生体認証技術へのニーズが高まると思われる。その際，このACBio機能を搭載することで，安全かつ相互運用性の高い生体認証技術の適用が可能となる。

今後，当社は，製品へのACBio機能の実装や，パスワードを廃止したい消費者サービスあるいは企業情報サービスの領域に対して，ACBioを用いた生体認証ソリューションの提案をより積極的に進めていきたい。

文　献

(1) 池田竜朗，ほか．“本人確認環境認証方式の提案”．コンピュータセキュリティシンポジウム2002（CSS2002）．大阪，2002-10，情報処理学会 コンピュータセキュリティ研究会．2002，p.337－342.

(2) Okada, K., et al. "Extensible Personal Authentication Framework using Biometrics and PKI". IWAP 2004 PreProceedings. Fukuoka, Japan, 2004-10, p.96－107.

(3) 高見澤秀久，ほか．バイオメトリック認証コンテキスト．東芝レビュー．60，6，2005，p.28－31.

(4) 山田朝彦．バイオメトリクスのための認証コンテキスト（ACBio）．東芝レビュー．61，9，2006，p.74－75.

(5) 山田朝彦，ほか．“バイオメトリクスのセキュリティ標準化の一側面”．暗号と情報セキュリティシンポジウム（SCIS2008）．宮崎，2008-01，電子情報通信学会 情報セキュリティ研究専門委員会．2008，3B4-4.（CD-ROM）．

(6) ISO/IEC 24761：2009. Information technology－Security techniques－Authentication context for biometrics.

山田　朝彦　YAMADA Asahiko, D.Sc.

東芝ソリューション(株) IT技術研究所 研究開発部主任研究員，理博。運用を中心としたシステムセキュリティの研究・開発に従事。情報処理学会会員。

Toshiba Solutions Corp.

岡田　光司　OKADA Koji, D.Eng.

東芝ソリューション(株) IT技術研究所 研究開発部研究主務，工博。情報セキュリティ技術の基礎研究及び応用開発に従事。国際暗号学会（IACR），電子情報通信学会会員。

Toshiba Solutions Corp.

池田　竜朗　IKEDA Tatsuro

東芝ソリューション(株) IT技術研究所 研究開発部主任。情報セキュリティ技術の開発に従事。情報処理学会会員。

Toshiba Solutions Corp.