バイオメトリクスのための認証コンテキスト（ACBio）

プライバシーにも考慮した，より信頼性の高い生体認証へ

生体認証技術が日常の生活にも使われるようになっています。生体認証は，本人以外は認証されえない強固な個人認証技術ですが，インターネットなどのオープンなネットワーク上で利用するには，仕組みとして十分であるとは言えません。

オープンネットワーク上で安心して生体認証を利用できるようにする仕組みが，ここで紹介する ACBio です。ACBio は，ISO/IEC JTC 1（国際標準化機構／国際電気標準会議 Joint Technical Committee 1）において，国際標準化が進められています。

生体認証の現状

生体認証が使われるようになってきている理由は，強固な本人認証が可能であること，利便性が高いことが挙げられます。しかし，普及してきているとはいえ，銀行の ATM（自動預払機）などの限定されたシステムだけであり，また，それらは専用線を使った，いわば閉じたシステムです。

これに対して，従来使われてきたパスワード認証は，企業内システムだけでなく，消費者を対象とするネットビジネスなどにも，幅広く利用されています。生体認証も，パスワード認証と同様に，将来的にはより広く利用されるであろうと考えられます。

オープンネットワークでの生体認証

従来のパスワード認証の方式を図示したのが**図1**の(a)です。ユーザーは，あらかじめパスワードを登録しておき，認証を受けるときに（例えば，インターネットで買い物をするときに）パスワードを入力します。あらかじめ登録されたパスワードと入力されたパスワードの一致をもって，ユーザーを認証します。

この方式を生体認証に応用すると(b)のようになります。しかし，これはユーザーにとってうれしい実施形態ではありません。プライバシーに対する意識が高まっている現在では，自分の生体情報（たとえ生体情報自体ではなく，生体情報をデータ変換したものであっても）を第三者に預けることに対して，抵抗を感じる人は多いと思います。

プライバシーを考慮すると(c)のようになります。生体情報はあくまで自分の手もとに置くのが(c)です。例えば，自分が所有する IC カードなどのデバイスに生体情報を格納します。しかし，(c)の方式では，プライバシーの問題は解決しますが，認証結果利用者（例えば，オンライン店舗）は認証の成否を受け取るだけで，その結果を信じてよいかを判断することはできません。

(c)を改良して認証結果利用者が結果を信じてよいか判断できるようにしたのが，東芝ソリューション（株）が提案する(d)の ACBio（Authentication Context for Biometrics）です。

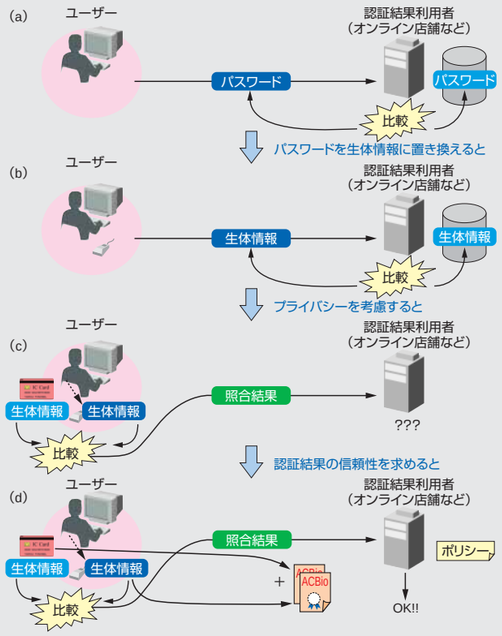

図1．パスワード認証と種々の生体認証 ― オープンネットワーク上での生体認証では，プライバシーを考慮し，かつ，認証結果利用者が認証結果を信頼できるようにすることが必要です。その一つの解が ACBio です。

ACBio の概要

ACBio が定義するのは，データ構造です。図 1 (d) にあるように，生体認証に利用されるデータや機器に関する情報を，ACBio が定めるデータ構造に詰め込んで，認証結果利用者が確認できるようにします。ACBio のデータによって，生体認証の実行と認証結果の利用がオープンネットワークを介していても，認証結果利用者は生体認証が正しく実行されたかどうかを判断することができます。

生体認証は，一般に複数の機器の上で実行されます。ACBio は，機器ごとに生成され，以下の情報を含みます。

⑴ 当該機器上の処理は十分な精度及び品質を持っているか
⑵ 当該機器上の処理はセキュアに実行されているか
⑶ あらかじめ正しく登録された生体情報が正しく使われたか
⑷ ほかの機器上の処理との間でデータは正しく授受されたか

ACBio のデータ構造は，詳細には**図2**に示すとおりです。ここで，登録された生体情報の証明書や機器の入出力に関する情報の中に，生体情報や入出力データそのものを含まず，ハッシュ値だけを含むようにしています。これによって，認証結果利用者が生のデータを知ることなく，生体認証が正しく実行されたかどうかを判断することを可能にしています。

以下の情報に対するSignedData		
	機器に関する情報ブロック	
		機器の公開鍵証明書
		機器の評価報告書（精度，品質，セキュリティに関する）
		登録された生体情報の証明書（機器が生体情報を格納する場合のみ）
	処理の対応を示す情報ブロック	
		認証結果利用者からのチャレンジ
	機器の入出力に関する情報ブロック	
		入力種別と入力情報のハッシュ値（入力数分）
		出力種別と出力情報のハッシュ値

図2．ACBio のデータ構造 ― SignedData とは，IETF（Internet Engineering Task Force）の RFC（Request For Comments）3852 で定義されている電子署名を含むデータ形式です。

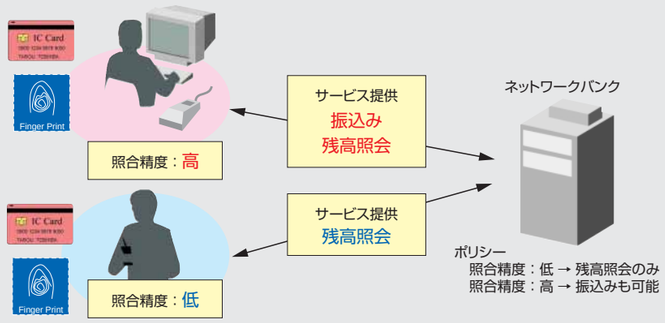

図3．オンラインバンキングへの応用例 ― ACBio により照合デバイスの精度も検証でき，精度によりサービスレベル（振込み，残高照会）を切り替えることができます。

ACBio の国際標準化

ACBio は，2005 年 8 月に，投票国 32 か国中 24 か国の賛成をもって，ISO/IEC JTC 1 / SC 27 / WG 2（SubCommittee 27 / Working Group 2）の新作業項目に採択されました。

SC 27 はセキュリティ技術の標準化を行っていますが，SC 27 とは別にバイオメトリクスの標準化を行っている SC 37 もあります。ACBio は，SC 37 をはじめ，IC カードに関する標準化を行っている SC 17，金融関係の標準化を行っている ISO/TC 68 とも連携しながら，標準化を進めています。特に，SC 37 には ACBio を検討するための SGonACBio（Special Group on ACBio）を設置し，標準案が更新されるたびにレビューを実施しています。

ISO/IEC における標準化では，たくさんのステップが必要になります。そのため，標準化されるまでにはまだ 2 年ほどかかる見込みです。

ACBio の国際標準化によってもたらされるもの

まず，ACBio によって，特定の機器を指定しなくても，正しい認証結果か否かを判断可能になるので，ネットワーク環境における生体認証の相互運用性が向上します。

次に，**図3**に示すように，ACBio によって機器の照合精度を参照できるので，取引内容に応じて使用される機器の条件をポリシーとしてあらかじめ登録しておき，使用された機器によって取引内容を変えることが可能になります。

また，機器のセキュリティ問題が明らかになった場合など，上記ポリシーを書き換えるだけで問題が生じた機器を排除することができるようになり，問題への迅速な対応が可能になります。

より良い生体認証の実現のために，最短の国際標準化を目指します。

山田　朝彦
東芝ソリューション（株）
IT 技術研究所
戦略企画担当主査