バイオメトリック認証コンテキスト

Biometric Authentication Context

高見澤　秀久　■TAKAMIZAWA Hidehisa
岡田　光司　■OKADA Koji
才所　敏明　■SAISHO Toshiaki

東芝ソリューション(株)は，ユーザーが用意するバイオメトリック環境を用いたオープンネットワーク上の本人認証を可能にする，バイオメトリック認証コンテキスト(BAC ： Biometric Authentication Context)を提案している。

BACは，バイオメトリック本人確認プロセスを実行するICカードやバイオメトリックデバイスなどのエンティティが，各自の実行した本人確認プロセスに関する情報とその結果を保証して検証者へ通知するためのフォーマットである。

Toshiba Solutions Corp. has proposed the “Biometric Authentication Context” (BAC), which makes authentication possible through an open network using a biometric environment provided by a claimant. BAC is a format for describing information concerning biometric verification processes and the results of such processes executed and verified by an entity (e.g., IC card, biometric device, etc.) that constructs the biometric environment provided by the claimant, and for transferring this information to a verifier of the authentication.

1 まえがき

バイオメトリック認証とは，身体的特徴(指紋，虹彩，顔など)又は行動的特徴(筆跡，キーストロークなど)により本人認証を行う技術である。認証の要求者から取得した生体データ(サンプルデータ)と，あらかじめ登録された生体データ(テンプレートデータ)とを比較することにより，要求者が本人であることを確認する。

近年では，厳密な本人確認を実現するための手段として，バイオメトリック認証が注目を集めている。例えば，9･11(米国同時多発テロ事件)以降，出入国管理に指紋や顔による本人認証が導入されつつあったり，静脈パターンで本人認証が可能な銀行の現金自動預払機(ATM)が発表されるなど，多くの製品やシステムにバイオメトリック認証が適用され始めている。

更に，インターネットを利用した電子商取引などのオープンネットワーク環境における非対面の認証に，バイオメトリック認証を適応させる動きもみられる。

しかしながら，これまでのバイオメトリック認証は，本人確認プロセスの正当性が保証されている固定的な製品やシステムを用いることが前提である場合が多く，オープンネットワーク環境へ適用させることは困難であると考えられる。

例えば，オンラインバンキングサービスなどでバイオメトリック認証を行うため，ユーザーに特定の製品を購入させたり，特定のシステムの使用を強要したりすることは現実的とはいえない。ユーザーは，自身のパソコン(PC)や携帯電話を用いてサービスが提供されることを望むであろう。そのためには，サービスの提供者が，ユーザーの環境で実行された本人確認プロセスの結果だけを検証するのではなく，ユーザーが用意する環境において実行された本人確認プロセスの正当性も検証することが必要になる。

ここでは，ユーザーが用意するバイオメトリック環境を用いて，オープンネットワーク上の本人認証を実現するための技術である，バイオメトリック認証コンテキスト(BAC：Biometric Authentication Context)について述べる。

2 オープンネットワーク上のバイオメトリック認証の問題

現在，オープンネットワーク上の非対面の認証には，PKI(Public Key Infrastructure：公開鍵認証基盤)技術が広く用いられている。PKIによる本人認証では，認証の要求者は，まず信頼できる第三者機関に秘密鍵と公開鍵を発行してもらい，その秘密鍵を自身が保有するICカードなどの耐タンパデバイスに格納する。そして，要求者はその秘密鍵を用いて署名を生成し，認証を行うサーバにその署名を送信する。サーバが公開鍵を用いてその署名を検証することで認証が成立する。

しかしながら，この認証方式は，“秘密鍵を所持していること”を認証しているのであって，“本人”を認証しているとはいえない。また，秘密鍵を活性化させるためにユーザーにパスワードの入力を求める場合もあるが，これも“知識”の認証であって，本人を認証しているわけではない。そこで，より厳密な本人確認に基づいて秘密鍵を活性化させるため

に，パスワードではなくバイオメトリクスによる本人確認を用いることが検討されている。

ここでは，ユーザーが用意するバイオメトリック環境を用いてオープンネットワーク上で本人認証を行う場合に，バイオメトリック認証の性質に起因して発生する問題について述べる。

2.1　照合精度の違い

現状では，バイオメトリクスを用いたとしても100％の確率で本人確認を行うことはできない。

同一人物の生体データを照合した場合の類似度の分布，及び異なる人物の生体データを照合した場合の類似度の分布を**図1**に示す[(1)]。この図において，横軸は照合した二つの生体データの類似度を，縦軸はその頻度を表している。横軸では右に行くほど類似度が高く，縦軸では上に行くほど頻度が高い。バイオメトリクスを用いた本人確認では，あるしきい値を設定し，類似度がこのしきい値よりも高いと照合成功，低いと照合失敗になる。

通常，同一人物の生体データを照合した場合の類似度の分布と，異なる人物の生体データを照合した場合の類似度の分布の一部は重なってしまう。そのため，しきい値の設定によっては，同一人物の生体データを照合しているにもかかわらず，照合が失敗してしまう場合や，反対に，異なる人物の生体データを照合しているにもかかわらず，照合が成功してしまう場合がある。

一般に，前者が発生する確率をFRR（False Rejection Rate：本人拒否率），後者が発生する確率をFAR（False Acceptance Rate：他人受入れ率）と呼ぶ。FRRとFARは，指紋，虹彩，顔などのバイオメトリクスの特性，照合アルゴリズム，そして製品やシステムなどによって異なる。

そのため，検証者は本人確認の結果だけでなく，本人確認プロセスにおけるバイオメトリクスの特性，照合アルゴリズム，そして製品やシステムなど，その本人確認プロセスに関する情報についても知っておく必要がある。

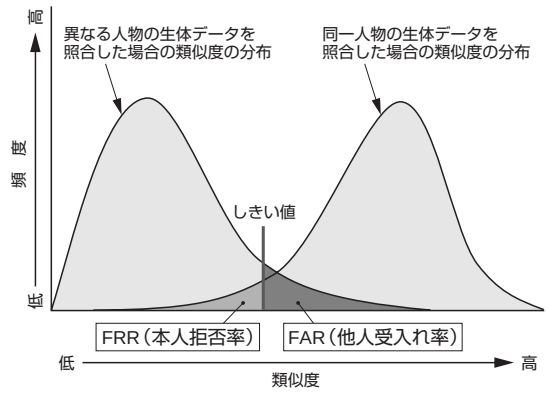

図1．類似度の分布 ― バイオメトリクスを用いた本人確認では，設定したしきい値に基づいて，本人であるかどうかを判断する。

Distribution of similarity

2.2　多様なバイオメトリック環境

一般に，バイオメトリクスを用いた本人確認は，以下の五つのプロセスによって構成される[(2)]。

⑴　データ収集　　入力装置やセンサ装置などを用いて認証の要求者から読み取った生体情報を出力するプロセス

⑵　信号処理　　入力された生体情報を，照合処理を行うためのサンプルデータに変換して出力するプロセス

⑶　格納　　あらかじめ格納されたテンプレートデータを出力するプロセス

⑷　照合　　入力されたサンプルデータとテンプレートデータとを比較して算出した類似度を出力するプロセス

⑸　判定　　入力された類似度とあらかじめ設定されたしきい値をもとに判定した本人確認結果を出力するプロセス

バイオメトリクスを用いた本人確認プロセスのフローを**図2**に示す。

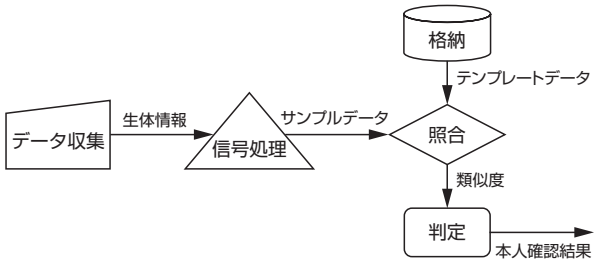

図2．本人確認プロセスの流れ ― バイオメトリクスを用いた本人確認は，複数のプロセスにより構成される。

Biometric verification process flow

これらの本人確認プロセスは，ICカードやバイオメトリックデバイスなどのエンティティによって実行されるが，どのエンティティがどのプロセスを実行するかによって，実装形態は異なってくる。

例えば，サンプルデータを生成するためのバイオメトリックデバイス，テンプレートデータを格納したICカード，そしてPCにより構成されたバイオメトリック環境を考える。この場合，照合プロセスを行うエンティティには，PC，バイオメトリックデバイス，そしてICカードなど，複数の実装形態が考えられる。

2.3　プライバシーの問題

バイオメトリック認証で用いられる生体データは，一般に“生涯不変”，“万人不同”と言われており，簡単に変更することができるパスワードなどと違って，慎重に取り扱われなけ

ればならない。そのため，ユーザーが生体データの流出を懸念して，自身の生体情報をネットワークに流したくないという場合も考えられる。

この場合，検証者がユーザーの生体データを取得することなく，本人確認プロセスに使用された生体データの正当性を検証する仕組みが必要となる。

3 BAC

東芝ソリューション(株)は，以上の問題を踏まえ，ユーザーが用意するバイオメトリック環境を用いて，オープンネットワーク上の本人認証を実現するためのフレームワークを提案している[(3),(4)]。

この提案のコンセプトは，ユーザーが用意するバイオメトリック環境で実行された本人確認プロセスの正当性を，検証者側で検証できるようにしようというものである。これを実現するために，本人確認プロセスを実行する各エンティティは，各自の実行した本人確認プロセスに関する情報及びその結果を保証して検証者へ通知する。ここでは，これらの保証は，PKIや業界団体が提供する保証基盤によって実現されることを想定している。

しかしながら，バイオメトリクスを用いた本人確認プロセスは，ユーザーが用意する多種多様なバイオメトリック環境の下で，複数のエンティティの組合せによって実行される。したがって，個々のエンティティの処理結果の正当性だけでなく，本人確認プロセス全体の情報を記述でき，かつ正当性を保証することができる汎用的なフォーマットが必要となる。

そこで当社は，BACという汎用的なフォーマットを提案している[(4),(5)]。**図3**に示すようにBACは，エンティティ情報，プロセス情報，及び署名ブロックから構成される。

エンティティ情報には，エンティティ自身が備える安全性や照合精度など，本人確認プロセスを実行したエンティティに関する情報を記述する。また，このエンティティを保証する，PKIや業界団体が提供する保証基盤に関する情報も記述する。検証者は，この情報をもとに，このエンティティで生成されたBACの検証を行う。

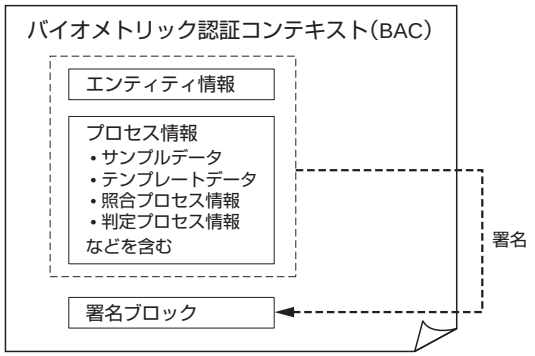

図3．BACの構造 — BACは，エンティティ情報，プロセス情報，及び署名ブロックによって構成される。
Structure of BAC

プロセス情報には，エンティティが実行した本人確認プロセスに関する情報及びその結果を記述する。プロセス情報には，以下の四つの情報から，エンティティが実行した本人確認プロセスに関する情報だけを選択して記述する。

(1) サンプルデータ　ユーザーから取得したサンプルデータを格納する。プライバシーの問題などから生体データを検証者に通知したくない場合には，サンプルデータのハッシュ値を格納する。

(2) テンプレートデータ　エンティティが持つテンプレートデータを格納する。プライバシーの問題などから生体データを検証者に通知したくない場合には，テンプレートデータのハッシュ値を格納する。

(3) 照合プロセス情報　照合処理で使用したバイオメトリクスの特性や照合アルゴリズムなど，照合処理に関する情報を記述する。また，照合に使用したサンプルデータ及びテンプレートデータも格納する。検証者は，照合プロセスで使用したサンプルデータ及びテンプレートデータを，この本人確認プロセスで取得されたサンプルデータ及びテンプレートデータと比較することで，それぞれのデータの正当性を検証する。プライバシーの問題などから，生体データを検証者に通知したくない場合には，照合に使用したサンプルデータ及びテンプレートデータのハッシュ値を格納する。

(4) 判定プロセス情報　本人確認の判定基準となるしきい値などの判定プロセスに関する情報，及び本人確認の結果を記述する。

署名ブロックには，エンティティ情報及びプロセス情報に対して，エンティティが前記の保証基盤によって発行された秘密鍵を用いて生成した署名を格納する。これにより検証者は，エンティティ内で実行されたプロセスが，エンティティにより保証されていることを検証する。

このようにBACでは，本人確認プロセスの結果だけでなく，本人確認プロセスに関する情報として，プロセスごとに特有の情報を記述する。これにより，ユーザーのバイオメトリック環境において実行された照合処理の信頼性についても，検証者側で検証することができる。

また，BACは，個々のエンティティの処理結果の正当性だけでなく，本人確認プロセス全体の情報を記述でき，かつ正当性を保証することができる汎用的なフォーマットである。これにより，検証者がユーザーのバイオメトリック環境の実装形態によらず本人確認プロセス全体を検証することを可能にする。

そして，検証者が，本人確認プロセスにおいて使用された生体データの正当性を検証する場合に，生体データそのものを検証するのではなく，生体データのハッシュ値を検証することで，プライバシーの問題を解決することができる。

4 BACを用いたバイオメトリック認証の例

ユーザーが用意するバイオメトリック環境を用いたオープンネットワーク上の本人認証で，BACを使用する例を**図4**に示す。ここでは，以下の三つのバイオメトリック環境で実行された本人確認プロセスを，サーバが検証して，ユーザーの本人認証を行う。

⑴ 家庭用PC
⑵ 携帯端末（携帯電話，携帯情報端末（PDA）など）
⑶ 不正なデバイス

家庭用PCのバイオメトリック環境は，ユーザーのテンプレートを格納したICカードと，家庭用PCに接続されたバイオメトリックデバイスにより構成されている。そして携帯端末のバイオメトリック環境は，バイオメトリック機能を備えた携帯端末により構成されている。家庭用PC及び携帯端末におけるエンティティは，保証基盤によって保証されている。一方，不正なデバイスのバイオメトリック環境におけるエンティティは，どの保証基盤からも保証されていない。

BACを用いた本人認証では，まず，サーバがクライアントに対して認証要求を送信する。認証要求を受け取ったクライアントは，自身のバイオメトリック環境において本人確認プロセスを実行し，本人確認プロセスを実行したエンティティはBACを生成する。クライアントにおける本人確認プロセスが完了したら，クライアントは生成したすべてのBACをサーバに送信する。サーバは受信したすべてのBACを検証し，認証の可否を決定する。

家庭用PC及び携帯端末を用いて本人認証を行った場合の例では，それぞれのBACに記述された本人確認プロセスの結果は成功である。また，それぞれの本人確認プロセスを実行したエンティティは，保証基盤によって保証されている。そのため，家庭用PC及び携帯端末を用いて本人認証を行った場合の例は成功となる。

しかしながら，不正なデバイスのバイオメトリック環境を用いて本人認証を行った場合の例では，本人確認プロセスの結果が成功であったとしても，そのデバイスはどの保証基盤からも保証されていないため，認証は失敗となる。

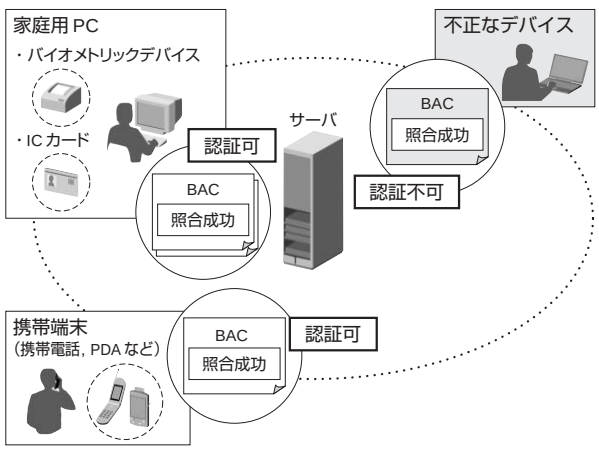

図4．BACを用いたバイオメトリック認証の例 ― BACを用いることで，多様なクライアント環境でのバイオメトリック認証を実現することができる。
Example of biometric authentication using BAC

5 あとがき

BACにより，インターネットなどのリモート環境におけるバイオメトリック認証が可能になるとともに，バイオメトリクスのウェブサービスへの応用が広く期待される。現在，相互互換性を確保するために，標準化活動を進めている。

文 献

⑴ 日本工業標準調査会．JIS-TR X0053:2002指紋認証システムの精度評価方法．2002，74p．
⑵ American National Standards Institute. X9.84-2003 Biometric Information Management and Security for the Financial Services Industry. 2003, 134p.
⑶ 池田竜朗，ほか．本人確認環境認証方式の提案．CSS 2002 論文集．**2002**，16，2002，p.337－342．
⑷ Okada, K., et al. "Extensible Personal Authentication Framework using Biometrics and PKI". IWAP 2004 PreProceedings. Fukuoka, Japan, 2004-10, p.96－107.
⑸ 吉井大吾，ほか．バイオメトリクスを用いた個人認証フレームワークにおける本人確認プロセスに関するプロファイルの一考察．CSS 2004 論文集．**2004**，11，2004，p.211－216．


高見澤　秀久　TAKAMIZAWA Hidehisa
東芝ソリューション（株）SI技術開発センター SI技術担当。情報セキュリティ技術の研究・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）SI技術開発センター SI技術担当主任，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。電子情報通信学会会員。
Toshiba Solutions Corp.


才所　敏明　SAISHO Toshiaki
東芝ソリューション（株）SI技術開発センター 戦略企画担当参事。情報セキュリティ技術の研究・開発に従事。情報処理学会，電子情報通信学会，ACM，IEEE会員。
Toshiba Solutions Corp.