クラウド時代の認証システムと生体認証技術

Authentication Systems in Era of Cloud Computing and Role of Biometric Authentication Technologies

山田　朝彦　■YAMADA Asahiko
パキン オソトクラパヌン　■Pakin OSOTKRAPHUN
西村　明夫　■NISHIMURA Akio

クラウド時代の到来でシステムの疎結合化が進み，認証システムも独立したクラウドサービスとしてIDaaS（Identity as a Service）やPAaaS（Pure Authentication as a Service）が出現している。一方，利便性の高い認証技術として生体認証の利用が広がりつつあるが，インターネット環境にあっては，いくつかの技術的な課題が普及の妨げになっている。

東芝ソリューション（株）は，これを解消するため生体認証を安全に利用するための技術を考案し，ISO/IEC 24761（国際標準化機構／国際電気標準会議規格24761）ACBio（Authentication Context for Biometrics）として国際標準化するとともに，ACBioMeister™として製品化した。ACBioMeister™をSSO（Single Sign On）技術と組み合わせることで，生体認証対応PAaaSが実現できる。

The introduction of loosely coupled systems has been accelerating with the wide dissemination of cloud computing in recent years. In the area of authentication systems, independent services as part of identity as a service (IDaaS) and pure authentication as a service (PAaaS) have also been increasing. Although biometric authentication has come into widespread use for user-friendly authentication systems, the introduction of biometric authentication technologies into the Internet environment is hindered by several technical issues associated with information leakage.

To solve these problems, Toshiba Solutions Corporation has developed the Authentication Context for Biometrics (ACBio), a technology that allows biometric authentication to be securely used even in the Internet environment. This technology has been adopted as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24761 international standard. We have also launched a related product called ACBioMeister™. PAaaS for biometric authentication is expected to be implemented by combining ACBioMeister™ with single sign-on (SSO) technologies.

1　まえがき

クラウド時代を迎えて，認証システムに対する要求に変化が生じ，認証を含むID（Identity）管理がクラウドサービスとして独立する傾向にある。クラウド時代は同時にモバイル時代でもあり，モバイル環境でも利便性の高い認証技術が求められている。

ここでは，利便性の高い生体認証技術の，クラウドかつモバイル時代の要求に応える適用方法を，東芝ソリューション（株）が考案し国際標準になったACBioとSSO技術を中心に述べる。

2　認証技術の動向

2.1　クラウド時代の認証システム

ネットワーク技術の発達とともに，システムは疎結合化する傾向にある。1990年代のASP（Application Service Provider）の登場で，企業などの組織内で使用されるサブシステムをアウトソーシングすることが許容されるようになった。この傾向は，システムの維持コストを大きく削減できるため，クラウド時代の到来でより加速されている。システムへの投資力のある企業でさえ，営業支援サブシステムを既存の社内システムからSaaS（System as a Service）に移行した例が少なくない。システムのレイヤから始まったクラウドサービスは，より低位のレイヤのサービスPaaS（Platform as a Service）やIaaS（Infrastructure as a Service）に広がっている。

更にSaaSやPaaSのID管理システムはIDaaSとして独立しつつある。個人情報の管理には多大なコストが必要になるが，個人情報をID管理システムに局所化させることが可能である。IDaaSが独立化すると，ユーザー側からすれば新たにSaaSを利用開始する場合にSaaSやPaaSへのID登録が不要になり，SaaSやPaaSの運営者側からすればID管理のコストが不要になる，というメリットがある。

パスワード認証の安全性が限界に達し，よりセキュリティ強度の高い認証技術として，PKI（公開鍵基盤）技術を使った認証やOTP（One Time Password）トークンを利用した認証の採用が進んでいる。IDaaSが全てのOTPトークンを組み込むのはコストもかかるため，OTPベンダーの中には，IDaaSへの簡易なインタフェースを提供して，純粋に認証だけのクラウドサービスであるPAaaSを開始するベンダーも出始めている。

このようにクラウド時代では，管理コスト低減の要求を受けて，認証システムはID管理システムの一部としてSaaSやPaaSからIDaaSへと委託され，複雑な認証処理もまたIDaaSから純粋に認証サービスだけを提供するPAaaSへと委託され始めている（**図1**）。

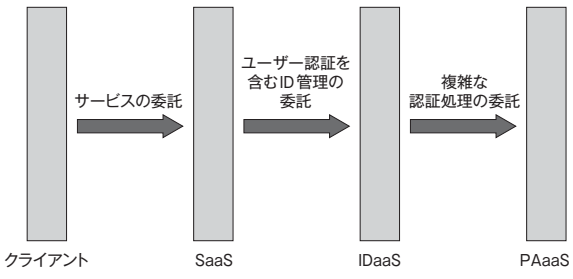

図1. クラウド環境における新しい認証システムの姿 ― クラウド環境では独立した認証サービスが出現している。
New authentication architecture in cloud environment

2.2 クラウド時代に求められる認証技術

ID盗難による被害増大に見られるように，パスワード認証の安全性は限界に達している。そのため，セキュリティ強度のより高い認証技術の採用が進んでいる。その反面，利便性の低下が問題となる。例えば，一度限りのパスワードであるOTPを使うと，セキュリティは向上するが，ユーザーにとっては機器などに表示されるOTPの入力は煩雑である。クラウド時代の到来とともにモバイル時代も到来しており，求められる認証方式はモバイル環境でも使いやすいことが要件になるであろう。

生体認証は，なりすましが難しく，かつ利便性に優れている。スマートフォンにも採用され始めた生体認証は，クラウドかつモバイルの時代の認証技術として期待される。

生体認証は，数少ない事例を除いて，インターネットでの認証には使われてこなかった。インターネット上で利用するには，クライアントでの処理をサーバは信頼できないという技術的な課題があったからである。サーバ照合方式の場合は更に，サーバへの登録生体情報，及び認証時にサーバに送信される生体情報が漏えいする可能性が技術課題としてある。

もし生体認証がこれらの技術課題を解決でき，更に多様なユーザーに適用できれば，生体認証はクラウドかつモバイルの時代の要求に合致する認証技術となる。

3 生体認証の技術課題を解決するACBio

3.1 ACBioの概要

当社は，2章で述べた技術課題を解決する技術として，ACBioを考案した。その成果は，2009年5月にISO/IEC 24761[(1), (2)]として国際標準規格化された。

ACBioは，生体認証技術ではなく，PKIを基礎とした生体認証の補完技術である。基本的な考え方は，以下のとおりである。

(1) 生体認証の処理の一部又は全体を実行する製品それぞれが，処理実行の証拠データを生成する。

(2) 認証サーバは，生体認証に関わる製品が生成した証拠データを検証する。検証に成功すれば，認証サーバはそれぞれの製品の処理が正しいと判断できる。

(3) 証拠データ全体が生体認証の成功を示していれば，認証サーバは，生体認証処理が成功したと判断でき，結果としてユーザーを認証できる。

ただし，認証サーバが証拠データを信頼できるためには，生体認証製品が信頼できることが必要である。

抽象構文記法ASN.1（Abstract Syntax Notation One）を使って前記証拠データのデータ項目及びデータ構造を定義したのが，国際標準ACBioである。より詳細には，国際標準ACBioは，RFC（Request for Comments）3852/5911に定義されている署名付きデータ構造であるSignedDataを適用し，生体認証の証拠となるデータセットをSignedDataの署名対象として定義したものである。SignedData構造を適用した前記証拠データは，ACBioインスタンスと呼ばれる。

ACBioは，生体認証システムのセキュリティ課題を解決する技術である。生体認証システムのセキュリティ脅威は，次の三つに大別される。

（Th1） 生体認証製品又はその内部の処理が不正な別のものに置き換えられる。

（Th2） ある個人αの登録生体情報が別人βの生体情報に置き換えられ，αの登録生体情報として扱われる。

（Th3） 生体認証製品間で授受されるデータが別のデータに置き換えられる。

ここで，生体認証製品とは，指紋読取り装置や，わが国のATM（現金自動預け払い機）で使われている生体情報照合機能付きICカードなどを指す。

前記の脅威は，それぞれに対応して，以下の方法で解消することができる。

（C1） 生体認証処理の一部又は全部を実行する製品が，耐タンパなどの対策によって脅威（Th1）を解消し，更に脅威が解消された製品であることを認証サーバに示す。

（C2） 登録生体情報を格納する製品が（C1）を満たし，更に登録生体情報が誰の生体情報であるかを証明する。

（C3） 生体認証処理に関わる製品が，（C1）を満たし，更に製品間で授受されるデータに置換のないことを確認できるデータを生成し，認証サーバに確認させる。

国際標準ACBioの信頼構造を**図2**に示し，ACBioが生体認証製品に要求する条件を以下に述べる。

（A1） 製造時に，製品ベンダーは，生体認証製品の処理内容を含むBPU（Biometric Processing Unit）報告を製品に組み込む。ここでBPUとは，（C1）を満たす生体認証製品である。BPU報告は，SignedDataを適用したデータであり，製品ベンダーが署名を付与する。

（A2） 製造時に，製品ベンダーは，生体認証製品に公開鍵

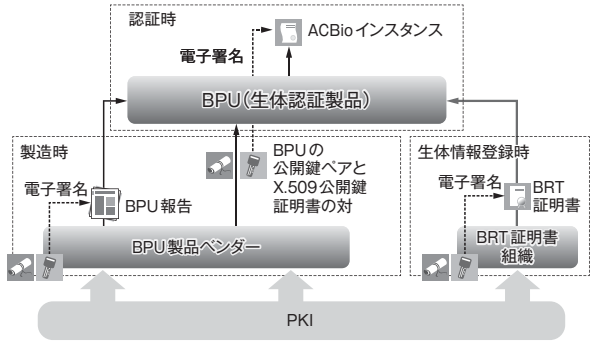

図2. ACBioの信頼構造 ― ACBioインスタンスには種々の署名付きデータが使われる。
Trust establishment in ACBio

ペア及びX.509公開鍵証明書を組み込む。

（A3） 生体情報登録時に，登録生体情報を格納する製品は，登録生体情報のハッシュ値を生成し，TTP（Trusted Third Party）に提出する。前記TTPは，前記ハッシュ値とユーザーIDを含むBRT（Biometric Reference Template：登録生体情報）証明書を発行する。製品は，登録生体情報とBRT証明書を対応付けて保管する。前記TTPをBRT証明書組織と呼ぶ。BRT証明書もSigned-Dataの応用であり，BRT証明書組織が署名を付与する。

（A4） 認証時に，認証サーバが生成した乱数が，各生体認証製品に送られる。各製品は，生体認証に関わる処理を実行するとACBioインスタンスを生成する。ACBioインスタンスには，製品のBPU報告，前記乱数，及び製品に対する入出力データのハッシュ値が含まれ，（A2）で付与された製品の秘密鍵で署名を生成する。登録生体情報が製品に格納され照合に使用される場合，ACBioインスタンスは登録生体情報に対応するBRT証明書も含む。

ACBioは，（C1）を（A1），（A2），及び（A4）によって，（C2）を（A1）～（A4）によって，（C3）を（A1），（A2），及び（A4）によって実現している。また，（A4）でチャレンジレスポンス方式を適用することで，再送攻撃対策をとっている。ここで，（A1）～（A4）による（C1）～（C3）の実現は，認証サーバが製品ベンダーをあらかじめ信頼することを前提にしている。もし生体認証製品を評価し認証するTTPが存在するならば，BPU報告を前記TTPが発行することによって，ACBioを使った生体認証（以下，ACBio認証と呼ぶ）は，認証サーバがあらかじめそのTTPさえ信頼するだけで前記の前提が不要な，より開かれた環境で使うことが可能になる。

ACBioインスタンスの仕様は指紋認証や，静脈認証，顔認証などの生体認証方式に依存していないので，任意の生体認証方式に適用可能であり，ACBioインスタンスを検証するサーバが一つあれば任意の生体認証方式に対応可能である。したがって，ACBio認証は，2.2節の最後に述べた条件を満たすものであり，クラウドかつモバイルの時代の要求に合致する認証技術である。

3.2 ACBio仕様を実装したACBioMeister™

当社は，国際標準ACBioを適用した製品ACBioMeister™を2012年8月にリリースした。製品構成は，認証クライアント，認証サーバ，及びBRT証明書発行サーバに対応するコンポーネントから成っている。

認証クライアントは，認証プロトコル処理機能とACBioインスタンス生成機能を持つ半製品であり，生体認証製品と組み合わせて認証クライアント製品を作ることができる。併せて，ユニバーサルロボット(株)の可視光てのひら静脈認証製品と組み合わせた製品も提供している。モバイル環境への適用を優先して，現在は，iOS版とAndroid™(注1)版を提供している。国際標準規格の範囲はACBioインスタンスの仕様だけなので，認証プロトコルは当社が独自に開発した。

認証サーバ向けのコンポーネントは，認証プロトコル処理機能とACBioインスタンス検証機能から成る。このコンポーネントは，PAM（Pluggable Authentication Module）実装であるJAAS（Java(注2) Authentication and Authorization Service）の認証モジュールであるため，一般のWebシステムに容易に組み込んで使用することができる。

BRT証明書発行サーバ向けのコンポーネントは，BRT証明書生成モジュールである。しかし，このコンポーネントには，認証サーバと同様に，認証プロトコル処理機能とACBioインスタンス検証機能も実装されている。BRT証明書の選択的な項目として，生体情報登録処理で生成されるACBioインスタンスが，国際標準ACBioで規定されており，この選択的項目の使用が推奨されているからである。

また，ACBioMeister™では，スマートフォンなどのモバイル機器ブラウザ利用時とVPN（Virtual Private Network）利用時に認証のための連携オプションを提供している。

4 ACBio認証を適用したID管理システム

生体認証は認証の利便性向上に貢献するが，別の面で認証の利便性に貢献するのがSSO技術である。WebシステムにおけるSSO技術は，各社の独自技術から標準技術へ移行させるいくつかの活動があったが，2005年にOASIS（Organization for the Advancement of Structured Information Standards）で承認されたSAML（Security Assertion Markup Language）2.0に集約された。これとは別にOpenIDファウンデーションの活動があり，SSO技術はこの両者に二分されている。

（注1） Androidは，Google Inc.の商標又は登録商標。
（注2） Javaは，Oracle Corporation及びその子会社，関係会社の米国及びその他の国における登録商標。

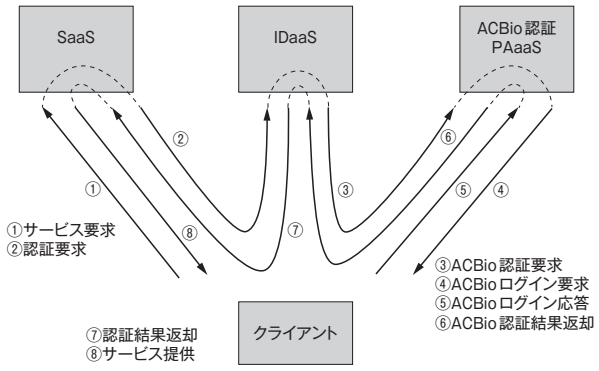

図3．ACBio認証PAaaSの処理概念 ― 認証はSaaSからIDaaSへ委託され，ACBio認証の場合は更にIDaaSからACBio認証PAaaSへ委託される。

Authentication processes applying ACBio authentication PAaaS

SAMLとOpenIDでは技術の詳細は異なるが，いずれも，認証を要求する主体であるRP（Relying Party）が，認証する主体であるSAMLのIdP（Identity Provider）又はOpenIDのOP（OpenID Provider）の認証結果を利用する。2.1節で述べたSaaSとIDaaSの関係は，まさにRPとIdP又はOPの関係に対応する。実際にIDaaSは，SAMLやOpenIDの技術を使って実現されている。

ACBio認証を容易にシステム導入できるようにするには，PAaaSとしてACBio認証が提供され，IDaaSとPAaaSの間でID連携させられればよい。ACBio認証に対応する部分はクライアントとPAaaSだけに局所化でき，導入も容易になる。

ACBio認証PAaaSの処理概念を**図3**に示す。IDaaSが，ACBio認証PAaaSにACBio認証を委託する。

5　展望

前記したように，ACBio認証PAaaSを実現するためのID連携が確認でき，クラウド時代の利便性とセキュリティを両立させるACBio認証のサーバ側の環境は整った。しかし，ACBio認証を適用した生体認証製品が少ないだけでなく，モバイル環境で誰もが容易に使える生体認証製品が提供されているとは言えない。モバイル環境で利用可能で，多様なユーザーのニーズに応える利便性の高い生体認証製品の充実が望まれる。

スマートフォンなどモバイル機器へ搭載された生体認証製品のほか，銀行ATMで採用されている生体認証機能搭載のICカードなど小型可搬機器も，いつでもどこでも利用可能な生体認証製品として期待される。ICカードにACBioが適用されれば，ICカードだけでなく，SIM（Subscriber Identity Module）カードなどのICチップ搭載ストレージデバイスへ適用され，様々なシーンでACBio認証が利用可能になる。

ICカードの標準コマンドはISO/IEC 7816シリーズで規定されており，生体認証の機能はISO/IEC 7816-11で規定されている。ISO/IEC 7816-11は，2012年から改訂作業が開始され，生体認証機能の拡充のため，新コマンドであるPBO（Perform Biometric Operation）コマンドの仕様検討がISO/IEC JTC（Joint Technical Committee）1/SC（Subcommittee）17で進められている。ICカード上のACBioの処理は，PBOコマンドの機能として実現されることがSC 17で2013年6月に決議され，仕様検討が進められている。

ACBioがセキュリティを担当するSC 27で国際標準化された後，生体認証の標準API（Application Programming Interface）であるBioAPIでのACBio処理は，バイオメトリクスを担当するSC 37でISO/IEC 19784-1の追補3とISO/IEC 17985-4が標準化されたことによって可能になった。ISO/IEC 7816-11のPBOコマンドと併せて，生体認証応用システムを容易に開発できる環境が整備されつつある。

6　あとがき

生体認証と組み合わせたACBio認証を，更にSSO技術と組み合わせることで，クラウド環境で認証技術の中心となるサービスPAaaSを構築できることを示した。当社は，ACBioの技術をACBioMeister$_{TM}$として製品化しているが，今後，PAaaSサービスの早期立上げを目指す。

文　献

(1) ISO/IEC 24761:2009. Information technology ―Security techniques― Authentication context for biometrics.
(2) ISO/IEC 24761:2009/Cor 1:2013. Information technology ― Security techniques― Authentication context for biometrics TECHNICAL CORRIGENDUM 1.

山田　朝彦　YAMADA Asahiko, D.Sc.
東芝ソリューション（株）IT研究開発センター 研究開発部，理博。バイオメトリクス及び情報セキュリティの国際標準化活動に従事。
Toshiba Solutions Corp.

パキン　オソトクラパヌン　Pakin OSOTKRAPHUN
東芝ソリューション（株）IT研究開発センター 研究開発部。情報セキュリティの研究・開発に従事。
Toshiba Solutions Corp.

西村　明夫　NISHIMURA Akio
東芝ソリューション（株）流通・金融ソリューション事業部 運輸・モバイルソリューション技術部参事。ACBioの事業化推進に従事。
Toshiba Solutions Corp.