「マルチメディア，分散，協調とモバイル
(DICOMO2014)シンポジウム」 平成26年7月

生体特徴の秘匿マッチングに基づくリモート生体認証システムの試作

小倉孝夫[†1] 森川郁也[†1] 安田雅哉[†1] 長谷部高行[†1] 新崎卓[†1] 津田宏[†1]

生体認証をインターネット上で実現することで，本人確認性の高い様々なサービスを容易に利用可能にするシステムを開発した．インターネットサービスで生体認証を利用する際の課題として，クラウド上に生体情報を預ける不安がある．また，最近ではサービス事業者の代わりに認証サービス行う IdP（Identity Provider）も現れ，ユーザは IDP へ預けているユーザ個人のデータをサービス事業者へ，どのようなデータを提供するか制御したいという要求がある.前者に対しては，手のひら静脈から抽出したバイオ特徴コードを，準同型暗号で保護したままサーバに保存および照合することにより，インターネット上や異組織間であっても安全に生体認証を実現することで解決する．また，後者に対しては，認証・ID 連携の標準的な技術である OpenID Connect と組み合わせ，サービスやデータアクセスに応じて匿名レベルを選択できることで，不要なユーザ個人のデータをサービス事業者へ提供しないようにする．これらの技術をクラウド上で試作・性能評価し，さらにデモンストレーションシステムにより，ネット上での本人確認および匿名化した属性情報を幅広く利用することで，ユーザにとって安全で,かつ利便性があることを示す.

Development of Remote Biometric Authentication System based on Secret Matching of Biometric Feature Codes

TAKAO OGURA[†1] IKUYA MORIKAWA[†1] MASAYA YASUDA[†1]
TAKAYUKI HASEBE[†1] TAKASHI SHINZAKI[†1] HIROSHI TSUDA[†1]

1. はじめに

近年，インターネットサービスの急激な増加に伴い,パスワードによる認証の安全性が問題になっている．インターネットのサービスでは,パスワードによる認証が広く利用されているが，ユーザがパスワードを覚えられる数は一般に数個とサービスに比べて少ない．そのため,パスワードの使いまわしが行われており，一つのサービスでパスワードが漏洩すれば，他のサービスでも利用可能である．このように，別のサイトから漏れたとみられる ID とパスワードを利用するパスワードリスト攻撃が問題となっている．これらの攻撃により，国内の大手ポータルサイト，オンラインショッピングサイトなどが次々に攻撃を受け，サイト利用者のアカウントを用いた不正なログインによる被害が多発している[1].

こうしたことから，人間の記憶力に頼らない生体認証や，一度の認証で多くのサービスへのログインを可能にする ID 連携・シングルサインオンの技術に期待が集まっている．

生体情報には本人にしかない特徴を持つ情報があり，これを利用すると他の人への貸し借りができないため，成りすましの防止が可能である．一方，これらの生体情報を認証で利用すると，身一つで本人認証を行えるが，認証に用いる生体情報は生体部位に依存し，自由に変更することができないため，より慎重に取り扱う必要がある．特に，インターネット上のサーバ（クラウド）に預ける場合，より安全に生体情報の漏洩防止を行わなければならない．端末とクラウド間の通信は SSL や VPN 等の暗号化通信で十分保護はできるが，クラウド内のサーバ側の事故等によるデータ漏洩についても対策する必要がある．

一方，ID 連携の技術により，小規模なサービス事業者の代わりに認証サービスやユーザ個人のデータを預かる IdP（Identity Provider）のサービスが広まりつつある．例えば，Facebook, Twitter, Google 等のソーシャルサイトやポータルサイトが IdP となり，これにより小規模なサービス事業者ではパスワードなどの認証情報や，氏名，住所，連絡先等のユーザの個人データを管理しなくて済む．

また，IdP が，自身の管理しているユーザ個人のデータを，サービス事業者の要求通り全て勝手にサービス事業者へ提供することは，ユーザに不安を与える．そこで，ユーザ個人のデータをサービス事業者へ提供する際，サービス利用に関係ないデータは出さず，ユーザの同意の元で安全に提供する仕組みが必要である．

これらに対し我々は，インターネット越しの生体認証を安全に実現する技術を開発し，試作システムを構築した．このシステムでは，手のひら静脈から取り出したバイオ特徴コード(3.1.1 参照)を，準同型暗号で保護された状態で認

†1 (株)富士通研究所
Fujitsu Laboratories Ltd.

証サーバに預け，高速に照合できる．また，異なる組織間で認証・ID 連携が可能な OpenID Connect プロトコル用い，サービス事業者毎に生体認証の機能をサポートしなくても，容易に生体認証の適用を可能にした．

さらに，サービス事業者へはユーザの個人データを一部匿名化してユーザ同意に基づいて安全に提供することができる．

2. 全体モデル定義

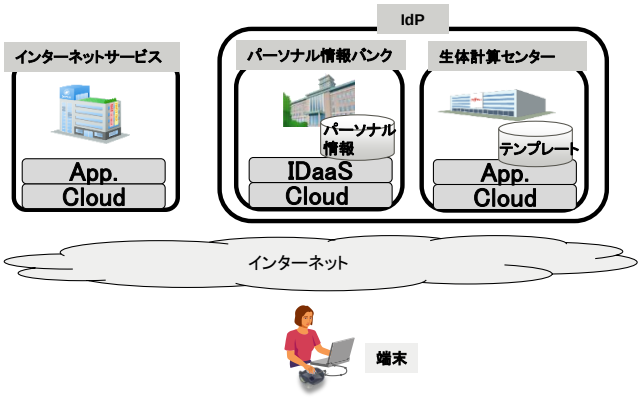

図 1　全体構成モデル

今回，リモート生体認証で本人確認を可能にする IdP アーキテクチャを開発した（図 1）．リモート生体認証は，ユーザが事前に登録した生体情報（暗号化されたバイオ特徴コードを，以下，テンプレートと呼ぶ）と認証時に暗号化したバイオ特徴コード（以下，照合データと呼ぶ）とで暗号化したまま照合する機能（以下，秘匿計算機能と呼ぶ）と照合結果を復号して認証結果を判定する機能（以下，判定機能と呼ぶ）から構成する．

IdP はパーソナル情報バンクと生体計算センターという二つの機関から成り，全体構成は以下の通りである．

インターネットサービス：インターネット上で生体認証を利用したサービスである．ユーザがサービスを利用する際，パーソナル情報バンク，生体計算センターの生体認証サービスを利用し，サービスログインする．

パーソナル情報バンク：認証サービスのフロントであり，生体認証の判定機能と IdP の機能を持つ．ここでは，生体認証の他，ユーザの氏名，住所，生年月日，資格等の属性情報を預かり，ID/属性管理を行う IDaaS(Identity as a Service)をインターネットサービスに提供する．

生体計算センター：ユーザのテンプレートを事前に登録し，テンプレートと照合データとで秘匿計算する機能を持つ．

生体情報の預かり先とユーザ個人のデータを預かるパーソナル情報バンクとを分離したアーキテクチャにすることで，パーソナル情報バンク内の運用管理者等の悪用および誤操作による被害を防止することが可能である．

3. 全体技術構成

今回，開発した技術は，背景で述べた生体情報をクラウドで預かる不安を解決する，手のひら静脈から生成するバイオ特徴コード，暗号化したまま照合する準同型暗号化技術，さらに，ユーザ個人のデータをサービス事業者へ提供する不安を解決するための ID 連携技術を示す．（図２）

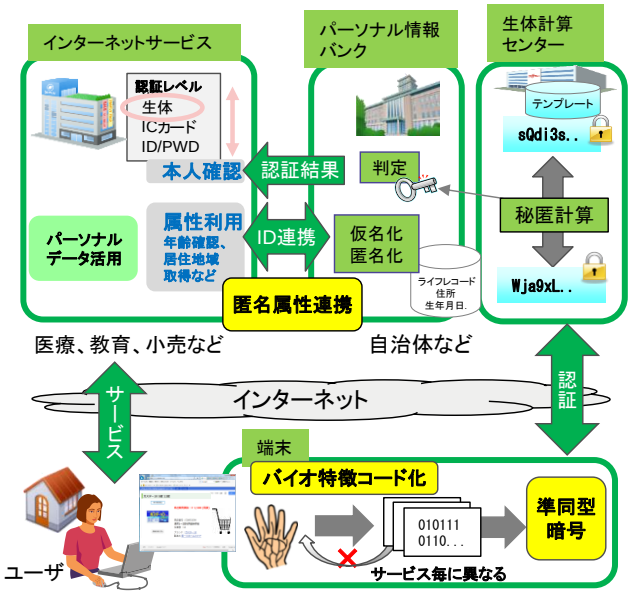

図 2　全体技術構成

3.1 リモート生体認証

3.1.1 バイオ特徴コード

(1)バイオ特徴コードが解決する課題

生体認証の利用が拡大するにつれて，認証システムの中で生体情報をより簡単に取り扱いたいというニーズが高まっている．1 つの生体情報から複数の生体特徴情報を生成できれば，サービスごとに異なる情報を登録することができる．また，生体特徴情報が漏えいした場合でも，変換条件 を変えて新しい生体特徴情報を生成して登録することで安心してサービスを使い続けることが可能である．

1 つの生体情報から複数の生体特徴情報を生成するこのような技術は，「キャンセラブルバイオメトリクス」あるいは「リニューアブルバイオメトリクス」と言われている．元の静脈画像や抽出された静脈特徴パターンを変換条件に基づいて変形し，システムに登録して利用することで「キャンセラブルバイオメトリクス」を実現できるが，照合の際には，従来の静脈認証と同等のパターン照合処理が必要となり，この処理に時間がかかるという課題がある．そのため，静脈画像からそのパターンの特徴を数値化したバイオ特徴コードを抽出し，その特徴コードを用いて単純な数値計算で照合を行うことで処理時間を短縮する方法が研究されている[2]．しかし，その実現には，静脈画像パターンを取得するたびに変化する手の傾きや形などに影響されな

い安定した特徴コードを生成する高度な技術が必要である．

(2)バイオ特徴コードの開発

我々は手のひら静脈画像から 2048 ビットの特徴コードを抽出して照合する技術を開発した[3].(図 3)この技術のポイントを以下に示す．

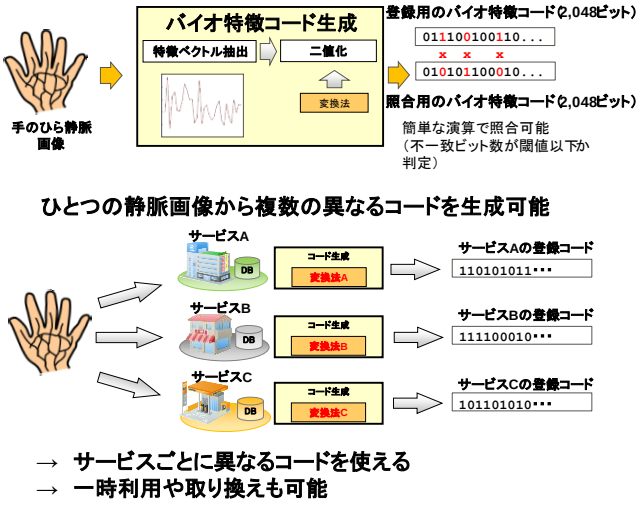

図 3 バイオ特徴コード

1)手のひら静脈画像の正規化

手のひら静脈画像の手の輪郭情報を用いて，手のひら静脈画像の位置補正や形状補正を行うための画像正規化を行う．この画像正規化により，センサーから取得された手のひら静脈画像を，一定の位置と形に置かれた静脈画像のように変換し，大まかな位置合わせを行うとともに，大きな変形を取り除く．この画像正規化手法により，特徴コードの抽出再現性を向上させている．

2)バイオ特徴コードの抽出

手のひら静脈画像から特徴コードを抽出する方法に関しては，画像の各部分での情報量に応じて画像領域を分割し，分割した領域から静脈パターンの特徴成分を抽出して，情報量削減の技術を用いて最終的に 2048 ビットの特徴コードを抽出する．画像領域を適応的に分割することで，多少の位置ずれや変形があっても影響を受けにくい特徴抽出方式を実現している.抽出された特徴コードから元の画像を類推することは困難である．

特徴コードは完全なデジタル情報であり，各種の秘匿技術，暗号技術との連携も容易であり，連携時のデータ変換による認証性能の劣化はない．また本技術を用いることにより，1 つの生体情報から複数の特徴コードを作成できるため，盗難・漏えい時にも新しい特徴コードを生成できる．さらに，手のひら静脈認証だけではなく指紋認証への適用も可能である．

特徴コード同士の対応するビットを比較し，ビットが相違する数，すなわちハミング距離を測ることで，他人受入率 10 万分の 1 レベルの識別性能で照合ができる．またコード化の際の変換条件を変えることで異なる特徴コードを生成でき，サービスごとに別のコードを登録したり，一定期間ごとにコードを更新したりすることが可能である．さらにハミング距離の計算は従来のパターン照合より非常に高速である．一般的な PC を使用して二つのコードを照合する場合，従来なら数ミリ秒かかるが，この技術では約 1/1000 となる約 1 マイクロ秒に短縮可能である．

3.1.2 一括型準同型暗号に基づく生体認証プロトコル

(1)準同型暗号方式の適用課題

バイオ特徴コードを暗号化したまま照合する技術として，準同型暗号を利用する．準同型暗号は暗号化したまま加算や乗算などの演算ができ，特徴コードを二値ベクトルと見なしてベクトル間の内積を計算することでハミング距離計算が可能になる．従来の準同型暗号では，ビットごとにデータの暗号化が行われていた．また，暗号化されたデータ間で内積を計算するには，暗号化されたビットごとに乗算を行った後，それぞれの結果を加算していた．そのためビット長に比例して処理時間が遅くなるという問題があり，実用化する上での課題となっていた．

(2)一括型準同型暗号方式

図 4 に今回のシステムで採用している準同型暗号方式[4],[5],[6]の概要を示す．イデアル格子ベースの準同型暗号を用い，前述の特徴コードを二値ベクトルとして一括して暗号化し，秘匿ハミング距離計算を行う．従来方式の 10 分の 1 程度の処理時間および暗号文サイズで 2048 ビットコード間の秘匿ハミング距離計算を行え，実用的な時間・通信負荷でネットワーク越しの生体認証を実現できる．

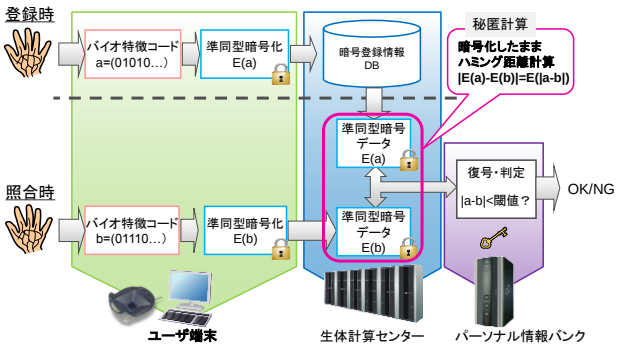

図 4　準同型暗号方式

1)　複数ビットの一括暗号化方式による高速化

二つの平文を暗号化する際に，多項式の掛け算が持つ特性を利用し，一つは昇順にもう一つは降順にビット列を並びかえた上で各々を係数とした多項式に変換する工夫をすることで，暗号化したままでビット列の内積の一括計算を

実現した（図 5）．これにより，従来のビットごとに暗号化し秘匿計算する処理に比べて，処理性能を飛躍的に向上した．例えば 2048 ビットのデータを用いた場合は 2048 倍の高速処理が可能となるなど，ビット長に比例した処理時間の短縮を実現した．

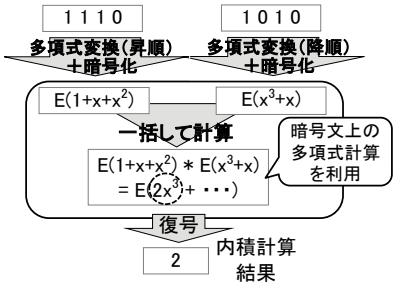

図 5　一括暗号化方式による高速化

3.2 リモート生体認証における ID 連携技術の適用

(1) ID 連携技術の適用課題

異なるサービス事業者や組織間でシングルサインオンを行うためには，認証・ID 連携の技術が必要である．現在，サービス事業者と IdP 間で OpenID[7],SAML[8]等のプロトコルが利用されている．コンシューマ向けのインターネットサービスでは OpenID, Salesforce 等と連携するための企業向けサービスでは SAML が利用されている．

また，Web サービス間（Facebook,Twitter 連携等）でユーザデータの連携を行うためには，ユーザデータへのアクセスを権限委譲する仕組みが必要であり，OAuth 2.0[9]仕様が広く利用されている．

最近では，OAuth2.0 を拡張して，サービス事業者と IdP 間の ID 連携プロトコルとして OpenID Connect[10]が出現し，Yahoo! Japan, Google 等で利用され，次世代のインターネットの ID 連携標準プロトコルとして期待されている．

これらにより，ID 連携の環境が整いつつあり，生体認証を利用することで高い本人確認性が得られるが，すべてのサービスに対して生体認証を利用する必要はない．プライバシーに関する機微情報（医療のカルテ情報，個人の機密情報等）や金融等に関しては慎重に扱われるべきである．そのような情報をインターネットサービスで扱う際，一つの手段として生体認証を利用することが望ましい．そのため，サービスの種類や扱う情報に応じて，柔軟に認証方式を選択できる必要がある．

また，SAML や OpenID Connect では認証の後，サービス事業者にユーザ個人のデータ（属性）を提供することが可能であるが，できる限り，不要な情報はサービス事業者に提供しないことが重要である．例えば，地域が特定できれば良い場合，住所情報をすべて提供するのではなく，都道府県の情報のみ提供ができるような匿名化の機能が必要である．

(2) 認証方式および匿名化によるサービス提供

様々なインターネットサービスに対応できるように柔軟に認証方式を選択できるようにした．OpenID Connect プロトコルのインタフェースに要求認証方式のパラメータを追加して実現した．これにより，サービス，データ（購入品の種類，参照するファイル等），アクション（ファイルの参照/書き込み，ショッピングサイトの購入/決済等），ユーザ環境（通常とは異なる IP アドレスや端末等）に応じて柔軟に認証方式(パスワード認証, IC カード認証，生体認証等)を選択できるようにした．

さらにユーザ個人のデータを目的に応じてサービス事業者へ提供するため，サービスや購入品の種類によって，ユーザに提供する ID/属性に関して，匿名の度合いを変更できる匿名レベルを定義した．匿名レベルは，レベル値が高いほど，匿名化による曖昧性が高い．例えば，ID の匿名レベルでは，次の 2 つの ID を用意した．①仮名 ID：サービス間での名寄せを防止するため異なるサービス間では異なる ID を発行する．ただし，同一のサービスサイトには同一の ID とする，②無名 ID：サービスを問わず，同一サービスでも，毎回，異なる ID を発行する．仮名 ID は無名 ID より匿名性は低く，サービス事業者側ではユーザの同一性を担保できるため，ユーザ毎に購入履歴を管理できる等の利点がある．属性に関しても，同様に，住所を市区町村まで提供するよりも，都道府県まで提供する方が，匿名性が高い．これらの ID/属性の匿名化機能を実現するため OpenID Connect プロトコルのインタフェースに ID/属性の匿名レベルのパラメータを追加して拡張した．

これらにより，生体認証による強固な本人確認に基づきつつ，本来の身元は明かさず仮名でサービスを受けたり，サービスを受けるのに最低限必要な精度の属性だけを明かしたりすることができる(図 6).

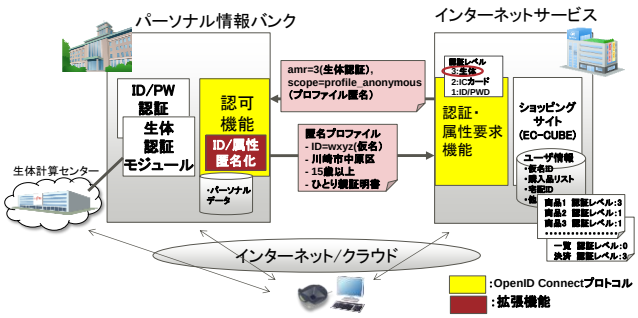

図 6　OpenID Connect プロトコル拡張

4. 試作および評価

4.1 試作システム

今回の試作したシステムでは，社内に構築したクラウドを用いて複数の VM (Virtual Machine)でシステムを構築した（図 7）．

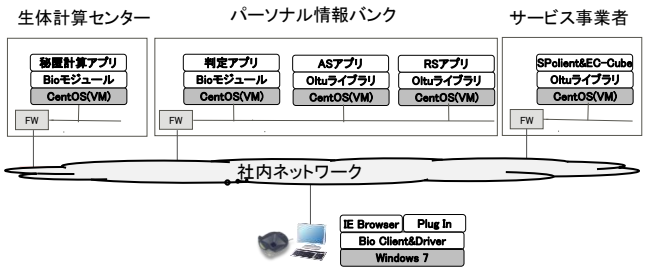

図 7　システム構成図

手のひら静脈からバイオ特徴コードを抽出する機能を配備した端末，準同型暗号によりハミング距離を計算する秘匿計算アプリ，そのハミング距離の結果から認証結果を判定する判定アプリ，OpenID Connect をサポートするユーザの属性認可判定機能(AS アプリ)，リソース管理機能(RS アプリ)，サービス事業者としてショッピングサイトのアプリ等を開発した．

（1）リモート生体認証における HTTPS 通信フロー

リモート生体認証を行う部分に関しては端末，パーソナル情報バンク，生体計算センターの 3 者モデルで認証を行う仕組みを提案する．このとき HTTPS の利用を前提とする．HTTPS は通信路上での盗聴・改竄や，主にサーバ側のなりすましを防止する手段として，現在広く普及しており，イントラネットを含む様々な環境下で通信が可能な手段である．ただし，HTTPS は 2 者間通信のみを保護し 3 者間通信時の中継者による脅威には対応できない点，および端末からサーバへのリクエストをトリガーとする通信しかできない点といった制約があり，これらを考慮した安全な通信フローの実現が必要である．

バイオ特徴コードの秘匿計算を行うため，パーソナル情報バンクは復号のための秘密鍵を保持する．準同型暗号化された特徴コードはユーザのフロントであるパーソナル情報バンクを経由して生体計算センターに送付されるが，このときパーソナル情報バンクは秘密鍵で復号できてしまう，という課題がある．その解決として，端末では準同型暗号化に加えて共通鍵暗号化（AES-128-CBC）を行い，パーソナル情報バンクでは特徴コードを復号できないようにする．そのため，事前に端末と生体計算センターの計算アプリとの間でセッションごとの共通鍵を交換しておく．これにより，経由するパーソナル情報バンク内でのデータ漏洩を防止でき，端末からクラウドへ送付される暗号化した特徴コードは，一度も復号されないまま，認証判定が可能となる（図 8）．

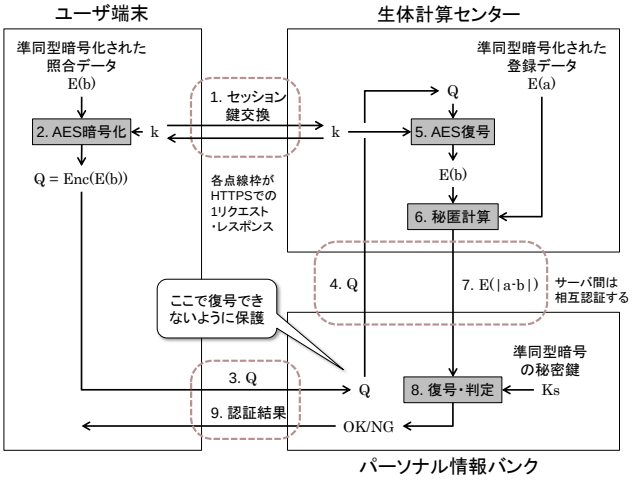

図 8 HTTPS を利用した通信フロー

（2）認証レベルおよび匿名レベル

柔軟に認証方式を変更するため，ショッピングサイトの販売商品の属性（商品種別，型名，価格等）の一つとして「認証レベル」を定義した．オープンソース(OSS)のショッ

図 9　匿名レベルによるパーソナル情報の提供画面

ピングサイト構築ツール（EC-CUBE）を用いて，ツールのプログラム変更なしに属性の追加が可能であり，データベースで管理ができる．商品購入の際の認証レベルのチェックおよび認証レベルの通知に関しては，EC-CUBE で用いられている PHP 言語のプログラム改修を行い，数十行の変更量のみで対応できた．

医薬品販売のショッピングサイトを利用シーンとして，認証レベルの高い医薬品を購入する際，サービス事業者側では年齢や福祉資格(ひとり親証明書)等を確認することを想定した．IdP ではユーザ個人のデータをサービス事業者へ提供するため，ユーザの同意が必要であり，その同意を示す画面を図 9 に示す．また，認証レベルの低い健康食品（栄養ドリンク）を購入する場合では，年齢や福祉資格等の確認を必要としないため，匿名レベルを高く設定してユーザが安心してショッピングサイトを利用できるようにした．

4.2 性能評価

大規模システムのための性能ボトルネック箇所の抽出を狙いとして，リモート生体認証の性能測定を行った．端末とパーソナル情報バンク，生体計算センター間のリモートで生体認証する通信フロー（図 8）に関して，1 回の生体認証における各処理時間を計測した．各処理時間は通信処理を除く，暗号化処理のアプリ処理時間を測定した．なお，自動的に繰り返し測定するため,ユーザが手をかざす時間やバイオ特徴コードに変換する処理の時間は含まれていない.また，今回の測定はクラウド（図 7）上の環境で，表 1 の通りである．端末も，現在利用できる静脈センサーのドライバーが 32 ビット Windows でしか動作しないため，64 ビット PC 上に 32 ビット Windows 7 をインストールして計測した．

表 1 .評価環境

クラウド	ホストマシン/CPU		PRIMERGY RX200 S6 / インテル® Xeon® プロセッサー E5503 [2GHz]
	ゲスト	CPU	1コア割り当て
		メモリ	15 GB
		OS	CentOS 5.6 (32bit)
		ミドルウェア	OpenSSL 1.0.1e-fips
端末	マシン/CPU		LIFEBOOK P772/E /インテルCORE i5 2.60GHz
	メモリ		4 GB
	OS		Windows7 (32 bit)

図 8 のセッション鍵の生成要求から認証判定結果通知までの全体処理時間および各主な処理時間の計測を 100 回行い，平均時間を表 2 に示す．全体処理時間では約 1.4 秒程度かかり，アプリ処理時間が約 1.1 秒を占め，その他は HTTPS の暗号処理,クラウド上の通信処理等にかかっていると考える．アプリ処理の内訳として生体計算センターの処理時間の割合が高く，大規模システムを考慮すると，今後，秘匿計算処理の性能改善が必要である．

表 2　計測結果

項目		処理時間
全体処理		1414 ms
端末処理		318 ms
生体計算センター	共通鍵生成処理	47 ms
	秘匿計算処理	402 ms
パーソナル情報バンク	復号･判定処理	342 ms
その他		305 ms

5. まとめ

手のひら静脈からのバイオ特徴コード抽出，一括型準同型暗号，および OpenID Connect プロトコルにより，インターネット上のサービスでも容易に生体認証を利用できるシステムを開発した．

今後は，実証実験ができるように，システムを考慮したセキュリティおよび品質の向上を進め，さらに，バイオ特徴コードや準同型暗号の基本的な性能向上を図る．今回はユーザ個人の静的なデータ（属性情報）のみ扱ったが，インターネット上に分散している動的なデータ（ソーシャルデータ，嗜好やショッピングサイトの履歴等）についても考慮し，生体認証に基づきユーザ個人のデータや許諾を利用したサービス実現のための機能を充実させていく．

参考文献

1) 情報処理推進機構, 「全てのインターネットサービスで異なるパスワードを！」, 2013 年 8 月の呼びかけ, 2013 年 8 月 1 日, https://www.ipa.go.jp/security/txt/2013/08outline.html

2) Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security.EURASIP Journal on Advances in Signal Processing, 1–17, 2008.

3) 富士通研究所, “世界初！手のひら静脈画像から 2048 ビットの特徴コードを抽出して照合する認証技術を開発”,2013.8.5 富士通研究所プレスリリース http://pr.fujitsu.com/jp/news/2013/08/5.html

4) 富士通研究所, “世界初！暗号化したまま統計計算や生体認証などを可能にする準同型暗号の高速化技術を開発”, 2013.8.28 富士通研究所プレスリリース, http://pr.fujitsu.com/jp/news/2013/08/28.html

5) M. Yasuda, T. Shimoyama, J. Kogure, K.Yokoyama and T. Koshiba, “Packed homomorphic encryption based on ideal lattices and its applications to biometrics", In Modern Cryptography and Security Engineering (MoCrySEn 2013), Springer LNCS 8128, 55–74, 2013.

6) 小暮,小柴,酒見,下山,武仲,安田,横山,“準同型暗号を用いた秘匿生体認証", SCIS2014, 2014.

7) OpenID Foundation, “OpenID Authentication 2.0 – Final”, http://openid.net/specs/openid-authentication-2_0.html

8) OASIS “P rofile for the OASIS Security Assertion Language (SAML)V2.0” OASIS Standard, 15 March 2005

9) OAuth2.0,IETF RFC6749, “The OAuth 2.0 Authorization Framework”

10) OpenID Foundation,“OpenID Connect Core 1.0”, http://openid.net/specs/openid-connect-core-1_0.html