SCIS 2025 2025 Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 28– 31, 2025
The Institute of Electronics,
Information and Communication Engineers

安心・安全な遠隔生体認証（SSRBA）
Secure and Safe Remote Biometric Authentication

才所敏明*1 辻井重男*2 櫻井幸一*3
Toshiaki Saisho Shigeo Tsujii Kouichi Sakurai

あらまし サイバー社会の急速な発展が期待され，ネット経由の利用者の確実な本人確認（遠隔認証）が必要なサービスも急増することが想定される．ネット経由の利用者の本人確認方法としては，現在は知識や所有物の確認による本人確認が主流であるが，今後，利用者の生体そのもの確認，生体認証の活用が期待されている．本稿では，ネット経由の利用者の本人確認への生体認証を利用した遠隔生体認証，サービス提供者の管理下に無い，利用者の手元で生体認証を実施しつつも，その生体認証の結果の信頼性をサービス提供者が確認できる，遠隔生体認証方式である SSRBA（Secure and Safe Remote Biometric Authentication）を提案する．SSRBA は，四半世紀前に考案した遠隔生体認証方式 BioRAIN/ACBio を，現在の IT 利用環境下での社会実装を想定して，新たに策定した構想である．本稿では，構想概要および具体的な実装方式を示すと共に，SSRBA のセキュリティに関する考察結果を報告する．

キーワード 遠隔認証，Remote Authentication，生体認証，Biometric Authentication，遠隔生体認証，Remote Biometric Authentication ，SSRBA，BioRAIN，ACBio

1. はじめに

利用者の遠隔認証技術は，1960 年代の MIT（Massachusetts Institute of Technology）の CTSS（Compatible Time-Sharing System）プロジェクトで使用されたパスワード認証が最初と考えられており，その後, 1970 年代には暗号技術を利用した秘密鍵の保有確認による認証方法，1990 年代には IC カード等の所持物による認証方法が提案され，洗練された方式が現在も使用されている．

また 1990 年代には生体の同一性確認による認証方法が提案され，現在ではパソコン，スマートフォン等の個人デバイスの所有者確認に，標準的に使用されている．一方，遠隔生体認証，ネット上のサービス利用時に生体を使用する本人確認については，様々の方法が提案されているが, 現時点で広く利用されている方式は未だ無く，発展途上である．

本稿では，新たな遠隔生体認証方式，筆者らが考案中の「安心･安全な遠隔生体認証（SSRBA：Secure and Safe Remote Biometric Authentication）」を提案する．

2. 遠隔認証技術の分類・定義

本稿では，遠隔認証技術，遠隔地の利用者（被認証者）を認証する技術を，認証に使用する要素，「秘密の知識(Something you know)」，「固有の所持物(Something you have)」「同一の生体(Something you are)」，に応じ分類・定義する．

（1）秘密の知識確認による認証（知識認証）

被認証者があらかじめ登録されている登録者本人しか知りえない秘密の知識を知っているかどうかの確認による認証方式であり，その秘密の知識あるいは秘密の知識を容易に導出できる情報を認証者へ開示するかどうかにより, 秘密開示方式および秘密非開示方式に分類する．

(1-1) 秘密開示方式

*1 (株)IT 企画，(株)ZenmuTech
mail：toshiaki.saisho@advanced-it.co.jp
*2 中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp.
*3 九州大学大学院システム情報科学研究院
&サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所
mail：sakurai@inf.kyushu-u.ac.jp

秘密開示方式は，利用者が利用登録時に秘密の知識を認証者へ提供し，認証者は被認証者がその秘密の知識を知っているかどうかの確認により認証する方式で，1960年代のMITのCTSSや当初のUNIXでの採用に始まるパスワード認証方式や，1970年代に始まった秘密鍵保有の確認による共通鍵暗号技術を利用した認証方式等が該当する．

(1-2) 秘密非開示方式

秘密非開示方式は，利用者は利用登録時には秘密の知識ではなく，秘密の知識の保有確認に使用する検証情報を認証者へ提供し，認証者は被認証者から提供される情報と検証情報から秘密の知識の保有の確認により認証する方式で，ワンタイムパスワード認証方式や，公開鍵暗号技術を利用した認証方式が該当する．

（2）固有の所持物確認による認証（所持物認証）

被認証者があらかじめ登録されている本人しか持ちえない所持物の保有の確認による認証方式であり，所持物固有の通信機能による確認方式と，所持物固有の秘密情報による確認方式に分類する．

(2-1) 所持物固有の通信機能による確認方式

通信機能による確認方式は，信頼できる第三者により所有物との対応が保証されている通信のための情報，その固有の通信のための情報をあらかじめ登録し，その通信のための情報による通信機能の確認により所持物保有を確認し認証する方式で，スマートフォンを利用した電話やショートメッセージによる通信機能を利用した認証方式等が該当する．

(2-2) 所持物固有の秘密情報による確認方式

所持物固有の秘密情報による確認方式は，他のデバイスへの移転の困難さが保証されている被認証者の所持物に格納されている秘密情報が，あらかじめ登録されている秘密情報であることの確認により認証する方式であり，ワンタイムパスワード認証方式で使用される信頼できる第三者により提供されるOTPハードウェアや信頼できる第三者が発行する耐タンパー性が保証されたPKIカードによる認証方式等が該当する．

（3）固有の生体確認による認証（生体認証）

被認証者が，あらかじめ登録されている本人しか持ちえない生体情報と，その場で採取した生体情報との照合により生体の同一性を確認し，その結果に応じ認証する方式である．

遠隔生体認証は，このような照合処理を，本人確認を求める側で行う認証者照合方式と，本人であることを主張する被認証者側で行う被認証者照合方式に分類される．

(3-1) 認証者照合方式

認証者照合方式は，認証者側での照合処理のために利用者が認証者へ提供する情報の内容により，生体情報開示方式と生体情報非開示方式に分類する．

(3-1-1) 生体情報開示方式

生体情報開示方式では，認証者は利用登録時点で被認証者の生体情報を入手し登録利用者の検証情報（テンプレート）として管理する．被認証者が登録者としての認証を求める場合，被認証者はその時点で生体情報を採取し認証者へ提供，認証者はあらかじめ登録されている検証情報と被認証者から提供された生体情報を利用し生体の同一性の検証（照合）を行い，その結果に応じ認証する方式である．

生体情報を認証者へ開示する遠隔生体認証については，1998年には検証情報として認証者が生体情報を管理しつつ，被認証者の生体情報との照合を認証者側で行う方式，および被認証者側で行う方式が提案されている（[17]）．

なお，生体情報は個人を特定する情報（個人識別符号）であるため，生体情報開示方式は一般の利用者向けのサービスでは採用されていない．

(3-1-2)生体情報非開示方式

生体情報非開示方式は，利用者は登録時点で何らかの変換を施した生体に関する情報（非可逆変換生体情報）を検証情報として認証者へ提供し，更に被認証者はその時点で抽出した生体情報を何らかの変換を施した生体に関する情報（非可逆変換生体情報）を認証者へ提供，認証者は利用登録時点の非可逆変換生体情報との検証（照合）結果に応じ認証する方式である．

様々の生体情報の変換方式が検討されているが，一般にはパラメータ等により異なる非可逆変換生体情報へ変換可能で，万一，認証者に登録した検証情報（テンプレート）が漏洩した場合でも，検証情報を新たな非可逆変換生体情報へ変更でき，キャンセラブルテンプレート方式とも呼ばれている．2001年にはキャンセラブルテンプレートの概念が提案され，生体情報の歪みによる変換方式が示されている（[19]）．また，2006年には，準同型暗号を利用し，生体情報を暗号化状態で照合する方式が提案されている（[20]）．彼らは，加法準同型性を有するPaillier暗号を利用しているが，その後も部分準同型暗号，完全準同型暗号の遠隔生体認証への応用が提案されている．

(3-2) 被認証者照合方式

被認証者照合方式は，その場で採取した被認証者としての生体情報と，あらかじめ登録しておいた信頼できる第三者機関が発行した登録者本人の生体情報との同一性の検証（照合）を被認証者の手元で行い，その結果を認証者へ提供すると共に，被認証者の手元の生体認証処理環境で実施した検証結果の信頼性を認証者が確認できる情報を認証者へ提供する方式である．

被認証者の手元の生体認証処理環境で実施した検証結果の信頼性を認証者が確認できる情報は，生体情報の同一性に関する検証処理が適切に実行されたこと，検証処理には信頼できる第三者機関が発行した利用者の適切な生体情報が使用されたこと，を示す情報を想定している．

2001年に提案したBioRAIN（Biometric Result Assurance Infrastructure）が本方式に該当する（[21]）．

なお，BioRAIN は 2009 年に
ISO/IEC 24761：2009 Information technology — Security techniques — Authentication context for biometrics（略称：ACBio）[2]
として国際規格となっている．

3. SSRBA 概要

本稿で提案する SSRBA は，BioRAIN/ACBio と同様，利用者（被認証者）の手元で実施される生体認証の，結果だけでなく，その結果の信頼性を確認できる情報を提供することにより，サービス提供者（認証者）が生体認証結果の信頼性を確認できる仕組みを目指した構想である．

2011 年には指紋認証や顔認証によるロック解除機能付きスマートフォン出現し，その後，iOS 系，Android 系のスマートフォンの開発ベンダの技術改良・製品投入により，スマートフォンには顔または指紋または両方の生体認証プロセス全体が搭載される時代となった．このように BioRAIN/ACBio を考案した四半世紀前の時代とは大きく変わった IT 機器および IT 利用環境を前提に，また個人情報・プライバシー情報の保護およびサイバー社会における確実な利用者認証への社会の関心の高まりを背景に，近い将来の社会実装の可能性を期待し，新たに考案した構想である．

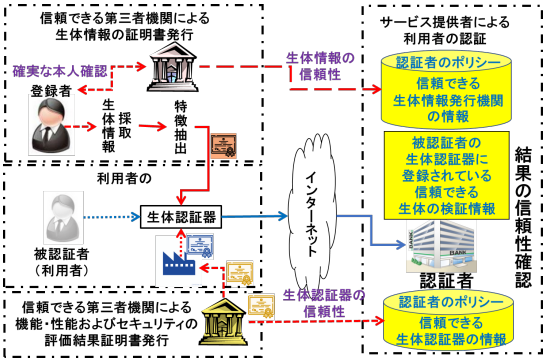


図 1　SSRBA 構成概要

SSRBA をサポートするサービス提供者はまず，信頼できる評価機関が発行する生体認証器モデルの機能・性能・セキュリティの評価結果証明書をベースに，生体認証器モデルを選定しておく．その情報を利用し，利用者が指定してきた生体認証器の使用の可否を判断し，可能な場合はその生体認証器の情報を登録・管理する．

生体情報についても，サービス提供者はまず，信頼できる生体情報の証明書発行機関を選定しておき，利用者が登録時に指定してきた生体情報ハッシュ証明書の発行機関の確認により，対応する生体情報の使用の可否を判断し，可能な場合はその生体情報のハッシュ値および登録されている生体認証器の情報を利用し認証時に使用する遠隔生体認証の検証情報を生成，登録・保管する．サービス提供者が生体認証を求めた場合は，利用者は生体認証に使用した参照生体情報（テンプレート）のハッシュ値および使用した生体認証器の情報等を利用し遠隔生体認証情報を生成しサービス提供者へ送付する．

サービス提供者は，登録されている遠隔生体認証の検証情報と利用者から送付される遠隔生体認証情報が同一かどうかにより，あらかじめ信頼性が確認されている生体認証器および生体情報が使用されたことを確認する．

SSRBA は，以上の仕組みにより，サービス提供者が，利用者が登録時に指定した信頼できる生体認証器の使用，利用者が登録時に指定した生体情報の使用を確認でき，結果として利用者の手元で実施された遠隔生体認証の結果の信頼性を確認できることを目指している．

4. SSRBA の実装方式

4.1 生体認証器の利用環境整備

①生体認証器モデル評価結果証明書の発行

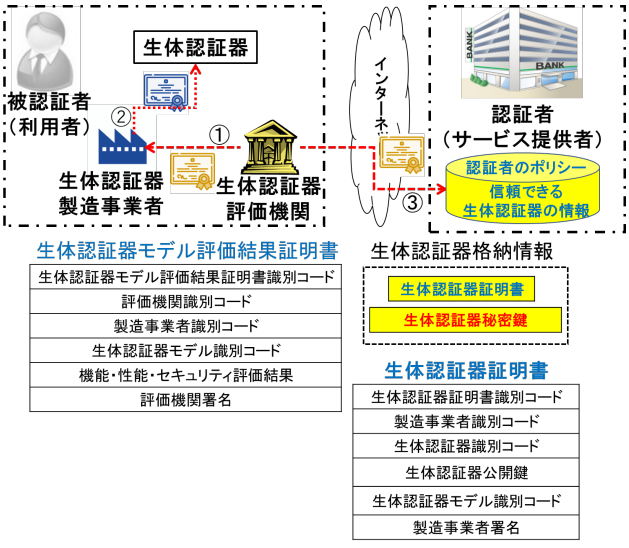
生体認証器評価機関は，生体認証器製造事業者の生体認証器モデルごとに機能・性能・セキュリティの評価を実施し，生体認証器モデルの識別コードに対する評価結果証明書を発行する．評価項目については，サービス提供者が生体認証結果の信頼性を確認できる項目を想定しているが，現時点で詳細は規定していない．

②生体認証器への生体認証器証明書の発行（格納）

製造事業者はそれぞれの生体認証器へ，生体認証器識別コードおよび対応する公開鍵，生体認証器モデル識別コード等から構成される生体認証器証明書，および生体認証器識別コードに対応する秘密鍵を，非改ざん性が保証されたエリアへ格納する．

③サービス提供者による生体認証器モデル評価結果証明書の登録

生体認証による利用者認証が必要なサービス提供者は，生体認証器評価機関から入手した生体認証器モデル評価結果証明書を参考に認証者としてのポリシーに適合するかどうかを判断し，信頼できる生体認証器モデルの評価結果証明書を登録しておく．



[2] 国際規格 ISO/IEC 24761：2009 は，ISO/IEC 24761：2019 に改定されている

図２　生体認証器の利用環境整備

4.2　生体情報の利用環境整備

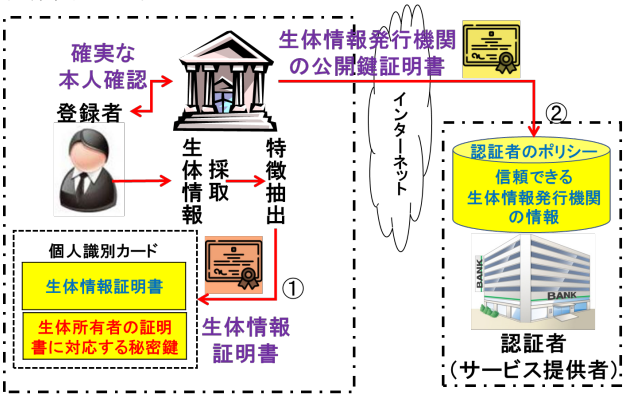
①生体情報証明書の発行

SSRBA では，利用者は，信頼できる第三者機関（政府機関等）の確実な本人確認を受けた上で発行された個人識別カード（日本のマイナンバーカード相当）を保持しているものとする．個人識別カードには，個人識別コード，個人名，住所，秘密鍵，対応する公開鍵証明書等が，格納されていることを想定している．

利用者は，個人識別カードの発行と同時に，あるいは別の機会に個人識別カードの提示等による確実な本人確認を受けた上で，生体情報証明書を入手（個人識別カードに格納）できることを想定している．生体情報証明書は，その一部の編集により，サービス提供者等へ提供する生体情報ハッシュ証明書として使用できる構成としており，また，個人識別コードおよび対応する公開鍵のサービス提供者等への提供を避けるため，生体情報ハッシュ証明書の所有者確認には個人識別コードの所有者確認に使用される公開鍵ペアとは別の公開鍵ペアを使用している．生体情報証明書の構成は図３を参照願いたい．

②認証者システムへの生体情報証明書発行機関の登録

利用者の生体認証が必要なサービス提供者は，認証者としてのポリシーに適合する生体情報証明書発行機関から公開鍵証明書を入手し，信頼できる生体情報証明書発行機関を登録しておくことを想定している．



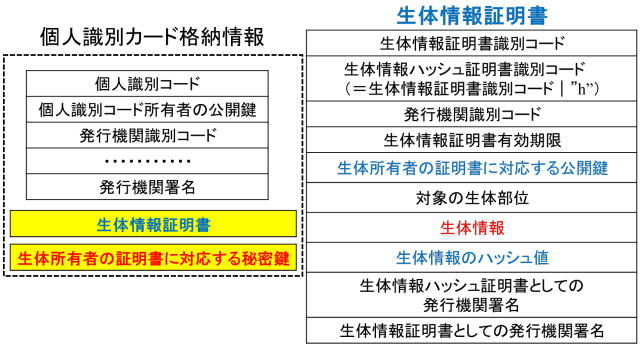


図３　生体情報の利用環境整備

4.3　利用者の遠隔生体認証利用環境整備

①遠隔生体認証利用環境の構成

利用者の環境は，クライアントシステム（PC，スマホ等），生体認証を担当する生体認証器から構成され，生体認証器は TPM/TEE/SE 等で構成された耐タンパーなモジュール/デバイスを想定している．

なお，個人情報・プライバシー情報を管理する耐タンパーなモジュール/デバイスと，機能・性能・セキュリティが保証された生体認証器は，本来は分離した方が望ましいが，本稿では耐タンパーなデバイス/モジュールである生体認証器内に遠隔生体認証に使用する個人情報・プライバシー情報も格納・管理する簡略化した実装方式で説明する．

②生体認証器の利用者環境への登録

生体認証器には，固有の生体認証器識別コードおよび対応する公開鍵等を格納している生体認証器証明書と，その公開鍵に対応する秘密鍵が格納されているものとする．

なお，鍵ペアは本稿では，生体認証器製造メーカが生成し生体認証器へ格納する方式を想定しているが，生体認証器を購入した利用者が自ら生成し，製造事業者へ公開鍵のみ提示し生体認証器証明書の発行・生体認証器への格納を要請し，秘密鍵は利用者が格納する方式の方が望ましいが，本稿では簡略化した製造事業者の製造時格納方式で説明する．

③生体情報の生体認証器への登録

個人識別カードに搭載されている生体情報は，生体認証器を利用した利用者の生体認証による本人確認後に生体認証器に格納され，以降は生体認証器に格納された生体情報が利用されることを想定している．なお，生体認証器内の生体情報ではなく，個人識別カード上の生体情報を直接利用する場合も想定されるが，本稿では生体認証器に登録された生体情報を利用する方式を説明する．

本人確認に成功した後に，個人識別カード上の個人情報が生体認証器に格納される．具体的には，生体情報証明書そのものと利用者（生体所有者）のこの証明書に対応する秘密鍵に，生体認証器内でユニークな登録生体情報識別コードを付与し，格納する．

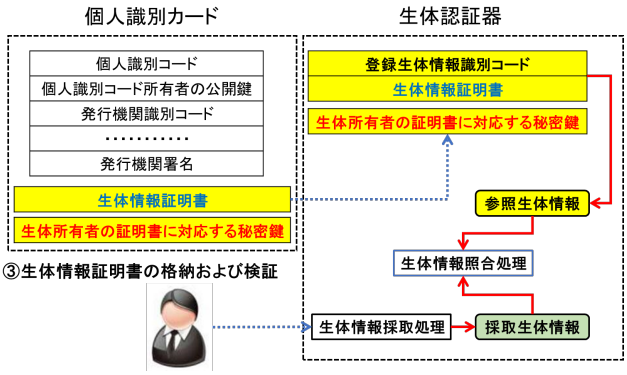


図４　利用者の生体認証利用環境整備
（生体情報の登録および検証）

4.4　利用者のサービス利用登録

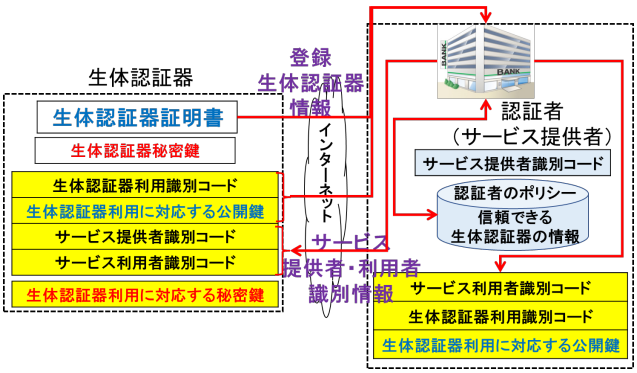
①生体認証器のサービス提供者への登録

利用者が遠隔生体認証を必要とするサービスへ登録す

る場合，まず使用する生体認証器がそのサービス提供者のポリシーに適合しているかどうかの確認のため，利用者は生体認証器証明書，生体認証器利用識別コードおよび生体認証器利用に対応する公開鍵へ，生体認証器利用に対応する秘密鍵による署名，生体認証器の署名を付与した登録生体認証器情報をサービス提供者へ送付，サービス提供者は生体認証器証明書の検証後，証明書内の生体認証器モデル識別コードから“信頼できる生体認証器の情報”内に登録されている生体認証器モデル評価結果証明書の内容を確認し，指定された生体認証器がポリシーに適合するかどうか判定することを想定している．また，生体認証器情報内の，生体認証器利用に対応する公開鍵による署名検証により，生体認証器利用の識別コードを確認し，今後の利用者認証時の生体認証器利用の指定・確認に使用する．

サービス提供者は，利用者の生体認証器が使用可能な場合は，利用者にサービス利用者識別コードを割り付け，そのサービス利用者識別コードに生体認証器利用識別コードおよび生体認証器利用に対応する公開鍵を対応させ格納する．

また，サービス提供者としての識別コードと利用者のサービス利用者識別コードを，署名付きで利用者に送付，利用者はサービス提供者の署名確認によりサービス提供者を確認後，サービス利用者識別コードとサービス提供者識別コードを，生体認証器利用識別コードと関連付け生体認証器へ登録する．



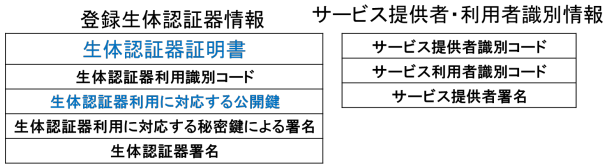


図５　サービス提供者への生体認証器の登録

②生体情報のサービス提供者への登録

利用者は，使用する生体情報証明書に対応する登録生体情報識別コードを生体認証器利用識別コードに対応させ登録する．また，使用する生体情報に対応する生体情報ハッシュ証明書，登録生体情報識別コード，生体認証器利用識別コードへ，生体所有者の証明書に対応する秘密鍵による署名および生体認証器利用に対応する秘密鍵による署名を付与しサービス提供者へ提供する．サービス提供者は，生体情報ハッシュ証明書内の発行機関識別コードから発行機関が”信頼できる生体情報発行機関の情報“に登録されているかどうか，認証者ポリシーに適合するかどうか，の確認をおこなう．なお，生体情報ハッシュ証明書は生体情報証明書の構成要素を再構成し生成する．

生体認証に使用する生体情報が，サービス提供者のポリシーに適合すると判断された場合は，サービス提供者による利用者認証時に使用される，遠隔生体認証検証情報を算出し，サービス利用者識別コードに対応させ格納する．

③利用者情報登録の確認

サービス提供者は，利用者の登録情報が正しく機能するかどうかの確認のため，遠隔生体認証試行を利用者に依頼し，利用者が生体認証を試みる．結果として遠隔生体認証が成功した場合は，利用者登録は終了する．

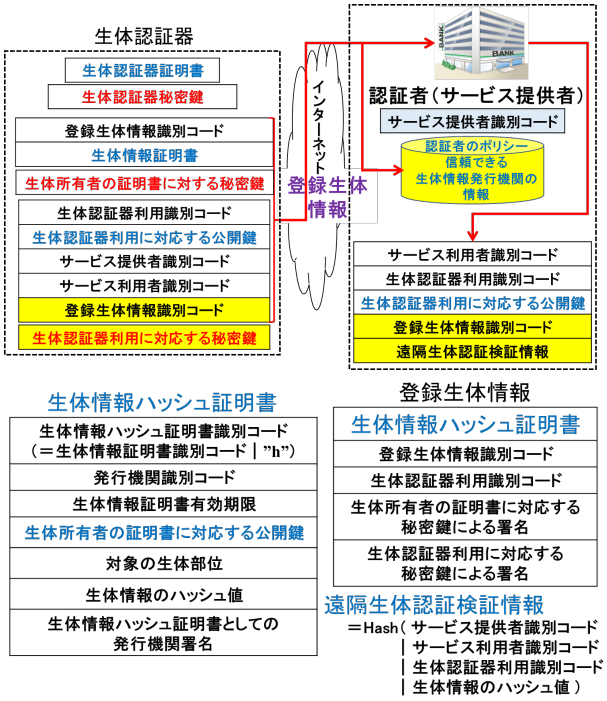


図６　サービス提供者への使用生体情報の情報を登録

4.5　サービス提供者による利用者認証

①利用者による認証要求

利用者は使用するサービス提供者へサービス利用者識別コードを送信し，認証を求める．

②サービス提供者が求める遠隔生体認証に関する情報の利用者への送付

サービス提供者はサービス提供者識別コードと共に，サービス利用者識別コードに対応する生体認証器利用識別コードを利用者に送付し，遠隔生体認証を求める．

利用者は，生体認証器利用識別コードに対応する登録生体情報識別コードから使用する生体情報証明書を特定する．

③生体認証器による生体認証

使用する生体情報証明書から抽出した生体情報（テン

プレート）およびセンサーモジュールから採取した利用者の採取生体情報を生体認証器の照合モジュールへ入力し，照合結果を得る．

次に，使用した生体情報（テンプレート）のハッシュ値や認証者からのチャレンジコードなどから，今回の実施生体認証情報を作成する．

生体認証器は，照合結果と実施生体認証情報に，生体所有者の証明書に対応する秘密鍵による署名，生体情報利用に対応する秘密鍵による署名，生体認証器利用に対応する秘密鍵による署名を付与し，サービス提供者へ提供する．

④サービス提供者による遠隔生体認証結果の判断

サービス提供者は，サービス利用者識別コードに対応する遠隔生体認証検証情報と今回の生体認証要求時のチャレンジコードとのハッシュ値と，利用者から送付された遠隔生体認証結果内の実施生体認証情報の一致を確認することにより，利用登録時に信頼性を確認した生体認証器および信頼性を確認した生体情報が使用されたことが確認でき，その後に遠隔生体認証の照合結果の信頼性を確認の上，照合結果の可否を判断することを想定している．

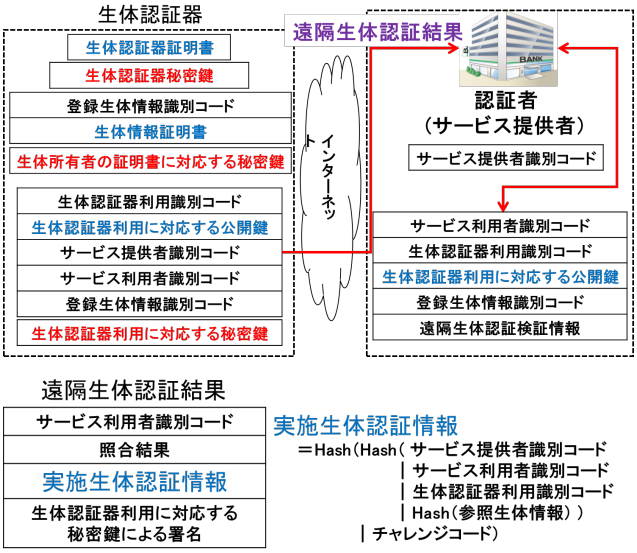


図７　サービス提供者による利用者認証

5.　SSRBA 利用者のリスクと対応状況

本章では，SSRBA で取り扱う情報による利用者の生体情報漏洩のリスク，個人情報漏洩のリスクを整理し，SSRBA における対応策および各機関・事業者に対する運用要件，および利用者自身の利用環境における配慮事項を整理する．なお，通信上の情報漏洩，なりすまし等は，本稿では省略しているが，別途対応することを想定している．

5.1　生体情報証明書発行機関

SSRBA では，生体情報証明書発行機関としては利用者の個人識別カードを発行する信頼できる公的機関を想定しており，生体情報証明書発行機関から利用者の生体情報および個人情報の漏洩は無いもの（漏洩があってはならないもの）と想定している．

なお，個人識別カードを発行する信頼できる公的機関以外の機関が担当する場合は，利用者の個人情報の確認，また個人識別カードへの書込み等も行う機関であるため，同等の信頼性が保証された機関である必要がある．

5.2　生体認証器製造事業者

[生体情報漏洩のリスク]

生体認証器製造事業者は，利用者の生体情報および関連する情報は一切扱わないため，生体情報漏洩のリスクは無い．

[個人情報漏洩のリスク]

利用者は生体認証器の保守契約等にて，氏名・住所等の個人情報を製造事業者等に提供する場合も多く，登録生体認証器情報内の生体認証器証明書に含まれている固有の生体認証器証明書の識別コード，生体認証器の識別コードおよび生体認証器の公開鍵と個人情報が連結され利用・管理されることになる．生体認証器製造事業者には，顧客情報の確実な保護が期待される．

5.3　サービス提供者

[生体情報漏洩のリスク]

利用登録時に，利用者はサービス提供者へ，登録生体認証器情報および登録生体情報を送付する．

登録生体認証器情報には，利用者の生体に関する情報は一切含まれておらず生体情報の漏洩のリスクは無い．

登録生体情報には，生体情報そのものは含まれていなく，生体情報のハッシュ値が含まれているが，ハッシュ関数の一方向性のため，生体情報の復元は不可能であり，生体情報漏洩のリスクは無い．

サービス利用時には，利用者はサービス提供者へ遠隔生体認証結果を送付する．

遠隔生体認証結果には，生体情報の照合結果と，使用した生体認証器を特定する情報，使用した参照生体情報を特定する情報，参照生体情報等から構成される情報のハッシュ値である実施生体認証情報から構成されており，生体情報漏洩のリスクは無い．

[個人情報漏洩のリスク]

利用登録時に利用者がサービス提供者へ送付する登録生体認証器情報には，個人を直接特定する情報は含まれておらず，個人情報の漏洩のリスクは無い．ただし，生体認証器の識別コードは，生体認証器製造事業者が管理する顧客情報との突合せにより利用者の個人情報を特定でき，個人情報の漏洩につながるリスクがある．

登録生体情報にも，個人を直接特定する情報は含まれておらず，個人情報の漏洩のリスクは無い．ただし，生体情報ハッシュ証明書の識別コードから，生体情報証明書識別コードを導出でき，また生体所有者の証明書に対応する公開鍵も生体情報証明書固有の情報であり，生体情報発行機関が管理する情報との突合せにより利用者の

個人情報を特定でき，個人情報の漏洩につながるリスクがある．生体情報証明書発行機関は，利用者の生体情報および個人情報の漏洩の無い信頼できる機関を想定しているが，サービス提供者にも，登録生体情報の確実な保護が期待される．

サービス提供者には，生体認証器および生体情報登録時に提供を受ける，生体認証器識別コードおよび生体情報ハッシュ証明書識別コードの確実な保護が期待される．

サービス利用時には，利用者はサービス提供者へ遠隔生体認証結果を送付するが，遠隔生体認証結果には利用者の新たな個人情報漏洩のリスクを引き起こす情報は含まれていない．

5.4　利用者の遠隔生体認証環境

利用者は自身の遠隔生体認証環境にて，生体情報，個人情報を利用・保管しており，その管理には十分な配慮が求められる．

個人情報が格納されている個人識別カードは，SSRBA 利用者に限らず，その安全な管理に利用者は配慮する必要がある．SSRBA 利用者は，その個人識別カードに生体情報を搭載するので，一層の配慮が求められる．

更に，SSRBA では，生体認証器へ生体情報を登録の上，遠隔生体認証に利用することを想定している．現状，生体情報の個人識別カードから生体認証器への登録は，生体情報による本人確認を前提としているが，その生体認証のため生体認証器の生体認証モジュールへ個人識別カード上の生体情報を一時的に格納する方式としている．利用者の生体情報を生体認証器にも搭載することは，生体認証器が一定の耐タンパー性が確認されているとはいえ，その管理には十分な配慮が求められる．

6.　おわりに

本稿では，安心・安全な遠隔生体認証の仕組み SSRBA を提案した．SSRBA は，生体認証を利用者の手元で完結させる遠隔生体認証方式（被認証者認証方式）であり，具体的な実装方式を考案し，SSRBA の実装可能性を示した．

SSRBA に利用者認証結果の信頼性は，生体情報証明書と生体認証器の信頼性が前提である．

生体情報証明書は，公的機関あるいはそれに準じる信頼できる生体情報証明書発行機関による確実な本人確認の上での，その機関の管理下の生体認証装置による確実な生体情報採取の上での発行と個人識別カードへの格納を想定しており，技術上および管理・運用上の，生体情報証明書の信頼性を揺るがすリスクは小さいと考えられる．

一方，生体認証器の信頼性は，認定・認証制度やガイドライン等で一定の信頼性が期待できる生体認証器モデル評価機関および生体認証器製造事業者による生体認証を構成する機能・性能・セキュリティ技術の確実な実装およびその評価の信頼性に大きく依存する．機能・性能・セキュリティ技術や検査・評価技術については，本稿では規定していないが，以下のような多くの技術が国際標準化されまた議論がされており，SSRBA ではその成果の利用を想定している．

ISO/IEC 19795：生体認証の精度評価
ISO/IEC 5152：生体認証の精度評価
（少サンプル数）
ISO/IEC 19792：生体認証のセキュリティ評価
ISO/IEC 19790：暗号モジュールの
セキュリティ要求事項
ISO/IEC 24745：生体情報の保護
ISO/IEC 30136：生体情報保護の性能評価
ISO/IEC 27553：生体認証のセキュリティ・
プライバシー要件（モバイル機器）
ISO/IEC 30107：提示攻撃検知

生体認証器モデル評価機関は，研究開発の状況，国際標準化の動向・成果をベースに，機能・性能・セキュリティ評価および評価結果証明書を発行することを想定している．

さて，サイバー社会の進展と共に，より確実な本人確認が必要なサービスは急増するものと想定しており，遠隔生体認証技術への期待は大きい．

遠隔生体認証技術については，本稿の２章にて分類・定義を整理しているが，サイバー社会で広範に利用されるサービスでは，認証者認証方式の中の生体情報非開示方式，キャンセラブルテンプレート方式の利用が期待され，現在も活発な研究が展開され，様々の方式が提案されている．

一方，被認証者認証方式としては，2002 年に BioRAIN 構想発表後も，類似する研究発表・方式提案は見当たらず，今回，あらためて SSRBA 構想および実装方式を提案することとした．今後も被認証者認証方式の可能性を追求すべく，SSRBA を中心に，研究を展開する予定である．

参考文献

[1] Corey Nachreiner，“Digital authentication: The past, present and uncertain future of the keys to online identity”，GeekWire，2018. https://www.geekwire.com/2018/digital-authentication-human-beings-history-trust/

[2] Robert Morris，Ken Thompson，“Password Security: A Case History”, Bell Laboratories, 1979. https://rist.tech.cornell.edu/6431papers/MorrisThompson1979.pdf

[3] Adi Shamir，“Identity-based cryptosystems and signature schemes”，Weizmann Institute of Science Israel，1985.

https://dl.acm.org/doi/10.5555/19478.19483
[4] Ralph C. Merkle, ”Secure Communications Over Insecure Channels “, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley,1978.
https://dl.acm.org/doi/pdf/10.1145/359460.359473
[5] Leslie Lamport. “Password Authentication with Insecure Communication”, SRI International, 1981.
https://dl.acm.org/doi/pdf/10.1145/358790.358797
[6] N. Haller, “The S/KEY One-Time Password System”, Bellcore, 1995.
https://datatracker.ietf.org/doc/html/rfc1760
[7] Chu-Hsing Lin, Yi-Yi Lai, “A Fingerprint-based User Authentication Scheme for Multimedia Systems”, Department of Computer Science and Information Engineering, Tunghai University, 2004.
https://www.researchgate.net/publication/4124726_A_fingerprint-based_user_authentication_scheme_for_multimedia_systems
[8] Loren M Kohnfelder, “Towards a Practical Public-key Cryptosystem”, MIT, 1978.
https://dspace.mit.edu/bitstream/handle/1721.1/15993/07113748-MIT.pdf
[9] Jingwei Huang, David M. Nicol, “An anatomy of trust in public key infrastructure”, University of Texas/ University of Illinois, 2017.
https://www.researchgate.net/publication/321453911_An_anatomy_of_trust_in_public_key_infrastructure
[10] “A Review on Remote User Authentication Schemes Using Smart Cards”.
https://link.springer.com/chapter/10.1007/978-3-642-37949-9_64
[11] Roger M. Needham, Michael D. Schroeder, “Using Encryption for Authentication in Large Networks of Computers”, Xerox Palo Alto Research Center, Dec. 1978.
https://dl.acm.org/doi/10.1145/359657.359659
[12] J. G. Steiner, B. Clifford Neuman, and J.I. Schiller, “Kerberos: An Authentication Service for Open Network Systems”, the Winter 1988 Usenix Conference.
https://www.researchgate.net/publication/3195303_Kerberos_An_Authentication_Service_for_Computer_Networks
[13] Fengling Han, Mohammed Alkhathami and Ron Van Schyndel, “Biometric-Kerberos Authentication Scheme for Secure Mobile Computing Services”, RMIT University, 2013.
https://ieeexplore.ieee.org/document/6743949
[14] Chu-Hsing Lin, Yi-Yi Lai, “A fingerprint-based user authentication scheme for multimedia systems”, Tunghai University, 2004.
https://ieeexplore.ieee.org/document/1394355
[15] George J. Tomko, Colin Soutar, George J. Schmidt, “Fingerprint controlled public key cryptographic system”, Mytec Technology Inc., 1996.
https://www.freepatentsonline.com/5541994.pdf#google_vignette
[16] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, B.V.K. Vijaya Kumar, “Biometric Encryption (TM) - Enrollment and verification procedures”, Proceedings of SPIE, 1998.
https://www.researchgate.net/publication/252555352_Biometric_Encryption_TM_-_Enrollment_and_verification_procedures
[17] G.I. Davida, Y. Frankel, B.J. Matt, “On enabling secure applications through off-line biometric identification” IEEE Symposium on Security and Privacy, 1998.
https://ieeexplore.ieee.org/document/674831
[18] N. K. Ratha, J. H. Connell, R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Thomas J. Watson Research Center, 2001.
https://ieeexplore.ieee.org/document/5386935
[19] Vishal M. Patel, Nalini K. Ratha, Rama Chellappa, “Cancelable Biometrics: A Review”, IEEE Explore, 2015.
https://ieeexplore.ieee.org/document/7192838
[20] Berry Schoenmakers, Pim Tuyls, “Efficient binary conversion for paillier encrypted values”, EUROCRYPT'06, 2006.
https://www.researchgate.net/publication/221347884_Efficient_Binary_Conversion_for_Paillier_Encrypted_Values
[21] 池田竜朗, 大岸伸之, 藤澤要, 森尻智昭, 才所敏明, “本人確認保証フレームワーク(BRAIN)の研究”, 東芝, CSS2001.
[22] 池田竜朗,森尻智昭,才所敏明, “本人確認環境認証方式の提案”, 東芝, CSS2002.