# 安心・安全な遠隔生体認証（SSRBA）の社会実装に向けた考察
## － Secure and Safe Remote Biometric Authentication －

才所 敏明
(株)IT 企画　158-0083 東京都世田谷区奥沢 6-18-10
E-mail: toshiaki.saisho@advanced-it.co.jp

**あらまし**　サイバー社会の安心・安全は，ネット経由の利用者の確実な本人確認（遠隔認証）に支えられている．筆者は，より確実な本人確認の社会実装を目指し，利用者の生体特徴を利用した安心・安全な遠隔生体認証（SSRBA）構想を提案している．SSRBA は，信頼できる第三者機関により採取された生体情報（生体テンプレート）の使用および信頼できる生体照合器モデル評価機関により内蔵する生体照合の，機能・性能・セキュリティの評価結果証明書が発行された生体照合器の使用により，利用者の手元で生体照合を実施しつつもサービスシステムが照合結果の信頼性を確認できる方式である．本稿では，SSRBA 構想の仕組みを具体化・整理し，サービス提供者，利用者双方のリスクを考察する．その上で，SSRBA のコアコンポーネントである生体照合器への機能・性能・セキュリティ要件へ対応可能な生体照合器の構成例を提案する．最後に，SSRBA の社会実装にあたっての今後の検討課題を整理する．

**キーワード**　遠隔認証，遠隔生体認証，生体照合器，SSRBA，生体テンプレート証明書，生体テンプレートハッシュ証明書

# Considerations for the social implementation of SSRBA
## －Secure and Safe Remote Biometric Authentication－

Toshiaki Saisho
Advanced IT Corporation

6-18-10 Okusawa, Setagaya-ku, Tokyo, 158-0083 Japan
E-mail:　toshiaki.saisho@advanced-it.co.jp

**Abstract**　The safety and security of cyber society is supported by reliable identity verification (remote authentication) of users via the Internet. Aiming to realize more reliable identity verification in society, the author proposes a concept for safe and secure remote biometric authentication (SSRBA) that utilizes users' biometric characteristics. SSRBA is a method that allows the service system to verify the reliability of biometric matching results while performing biometric matching in the user's hands, by using a template (biometric information) collected by a trusted third-party organization and a biometric matching device that has been issued a certificate of evaluation results for functionality, performance, and security of the built-in biometric matching by a trusted biometric matching device model evaluation organization. This paper concretizes and organizes the mechanism of the SSRBA concept and considers the risks to both the service provider and the user. Based on this, we present a proposed internal configuration for a biometric matcher, the core component of SSRBA, that can meet the functionality, performance, and security requirements for the biometric matcher. Finally, we summarize the issues to be considered for the social implementation of SSRBA.

**Keywords** Remote authentication, remote biometric authentication, biometric matcher, SSRBA, biometric template certificate, biometric template hash certificate

## 1. はじめに

サービスシステムがネット経由の利用者を利用者の生体特徴を利用し認証する遠隔生体認証について，筆者は 2000 年頃より，利用者の手元で照合処理を実施しつつも，その照合処理の結果が信頼できるかどうかを判断ができる情報をサービスシステムへ提供することにより，遠隔生体認証を実現する方式を検討してきた（[8]，[9]）．

また，筆者は昨年より，四半世紀前とは異なるサイバー社会の IT 利用環境を前提にあらためて方式を検討，SSRBA 構想を策定，今年の SCIS2025 にて提案した（[1]）．

SSRBA の第一の特徴は，利用者の生体情報の第三者への開示を避け，生体照合は利用者の手元の生体照合

器で実施することである．サービス提供者の管理下にない生体照合器での照合結果の信頼性をサービスシステムが確認できるよう，生体照合器そのものは一定のレベルの耐タンパー性を確保されていること，内蔵される生体照合処理は一定レベルの機能・性能・セキュリティが確保されていることを，信頼できる第三者機関の評価を受け，サービスシステムはその評価結果を入手でき，その評価結果により生体照合器の信頼性を確認できることを想定している．

SSRBA の第二の特徴は，生体照合器内の生体照合処理に使用されるテンプレートとして，信頼できる第三者機関が利用者の確実な本人確認の上に採取された生体情報（生体テンプレート）を使用することである．信頼できる第三者機関が生体情報を採取し発行する生体テンプレート証明書を，利用者が手元の生体照合器へ登録の上，利用することを想定している．また，生体照合器内の照合処理において信頼できる第三者機関が発行した利用者の生体テンプレートの使用をサービスシステムが確認できる仕組みを提供する．

SSRBA は，利用者の手元の生体照合器を使用しつつも，その照合処理の信頼性，照合処理結果の信頼性をサービスシステムが確認できる仕組みにより，利用者は生体情報を開示することなく，生体による利用者認証を可能とする構想である．厳密には，単純な生体認証ではなく，信頼できる物理的な認証器（生体照合器）と組み合わせた多要素認証であるが，生体照合結果の信頼性を確認でき，信頼できる生体認証であることが特徴である本構想を，安心・安全な遠隔生体認証 SSRBA と称している．

本稿では，第 2 章にて SSRBA の概要，第 3 章にて生体照合器の機能仕様，第 4 章にて利用者登録・認証に関わるサービスシステムの機能仕様，第 5 章にて SSRBA 機能仕様のリスク考察，および生体照合器の構成例，第 6 章にて SSRBA の社会実装に向けた検討課題，をまとめている．

## 2. 安心・安全な遠隔生体認証 SSRBA 概要

### 2.1. SSRBA が想定するサービス環境

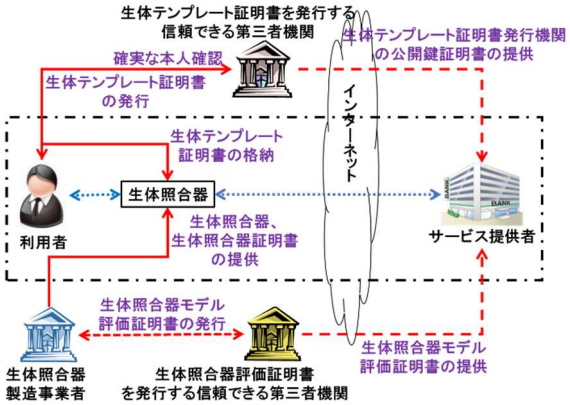


図 1　SSRBA が想定する利用環境

安心・安全な遠隔生体認証 SSRBA における生体による利用者認証手続きは，図 1 の一点鎖線で囲んだ範囲の，利用者の手元の生体照合器とサービス提供者のサービスシステムの間で実施する．

SSRBA では，利用者認証手続きが正しく機能するために必要な，生体照合器の信頼性の確保・確認のための仕組みおよび生体テンプレートの信頼性の確保・確認のための仕組みを含む利用環境を想定している．

### 2.2. 利用者の手元の生体照合器の機能

SSRBA では，生体照合器には以下の機能を想定している．

① 生体照合器証明書の管理

信頼できる生体照合器製造事業者が発行し内蔵されている生体照合器証明書を安全・確実に管理する．

② 生体テンプレート証明書の登録・管理

信頼できる第三者機関が利用者に対し発行した生体テンプレート証明書であることを確認し登録，安全・確実に管理する．

③ サービスシステムへの利用登録対応

生体認証による利用登録のための，生体照合器証明書，生体テンプレートハッシュ証明書等をサービスシステムへ提供し，生体照合器の利用情報を登録・管理する．

④ サービスシステムへの利用認証対応

生体による利用認証のための，生体照合器の利用情報に基づく照合処理を実施し，照合結果とその照合結果の信頼性検証に使用される生体照合実施情報をサービスシステムへ提供する．

### 2.3. サービス提供者のシステムの機能（利用者登録・認証に関わる機能）

SSRBA では，サービスシステムには利用者の利用登

録・認証に関する以下の機能を想定している.

① 生体照合器証明書による利用者の生体照合器の信頼性確認

利用者から提供される生体照合器証明書により，利用者の生体照合器がサービスシステムのポリシーに合致した機能･性能･セキュリティかどうかを確認する.

② 生体テンプレートハッシュ証明書による，利用者の生体テンプレートの信頼性確認

利用者から提供される生体テンプレートハッシュ証明書により，生体テンプレートハッシュ証明書に対応する利用者の生体テンプレート証明書が，サービスシステムが信頼できる機関の発行かどうかを確認する.

③ SSRBA 利用者の登録

サービスシステムは利用登録時に，利用者固有の識別コードに対応させ，生体照合器利用情報を特定する情報，生体照合検証情報等を，利用者管理情報として登録する.

④ SSRBA 利用者の認証

サービスシステムは利用認証時に，生体照合器から提供される生体照合実施情報と，利用者識別コードに対応し管理されている利用者管理情報を使用し，①，②で信頼性が確認された生体照合器および生体テンプレートが使用されたかどうかを確認する．その後に，生体照合結果がサービスシステムのポリシーに合致するかどうかで，利用者としての認証の是非を判断する.

### 2.4. 生体照合器の信頼性の確保･確認のための仕組み

生体照合器はモデルごとに，信頼できる第三者機関が，国際標準（ISO/IEC 19795，5152，29794，19790，19792，19989，30107 等）に基づいて評価し，モデル識別コードを含む評価結果証明書を発行することを想定している.

生体照合器モデル評価結果証明書は，評価機関あるいは製造事業者経由，SSRBA を採用するサービスシステムへ提供されるものとする.

製造事業者は，製造する生体照合器に内蔵する生体照合器証明書へ生体照合器識別コードと共にモデル識別コードを含めるものとする.

また製造事業者は，保守契約等で利用者の個人情報等の収集が想定されるが，生体照合器識別コードと利用者の個人情報等との連結情報は安全に管理することを想定している.

### 2.5. 生体テンプレートの信頼性の確保･確認のための仕組み

利用者の生体テンプレート証明書は，信頼できる第三者機関が，国際標準（ISO/IEC 29115 等）や NIST のガイドライン（SP 800-63-3）に基づく対面での確実な本人確認の上で生体を採取し，多目的に個人の特定に利用される各国政府が付与する利用者の国民 ID 等を含めずに，発行するものとする（[7]）.

発行した生体テンプレート証明書は，耐タンパーなデバイスへ格納し利用者へ提供，利用者がデバイスを安全に管理の上，生体照合器へ生体テンプレート証明書を登録することを想定している.

## 3. 生体照合器の機能仕様

### 3.1. 生体照合器証明書の管理機能

生体照合器証明書は製造事業者が発行し，生体照合器に内蔵され利用者へ提供されることを想定している.また，信頼できる第三者機関が生体照合器のモデルごとの機能・性能・セキュリティの評価結果証明書を発行することを想定し，サービスシステムが生体照合器の信頼性確認に使用できるよう、生体照合器証明書には生体照合器モデル識別コードを含めている.

生体照合器証明書の構成を図 2 に示す．なお，生体照合器公開鍵は，生体照合器ごとに生成された鍵ペアの公開鍵であり，秘密鍵は利用者が保有・管理し，生体照合器の所有の証明に使用する.

| 生体照合器証明書識別コード |
|---|
| 製造事業者識別コード |
| 生体照合器識別コード |
| 生体照合器公開鍵 |
| 生体照合器モデル識別コード |
| 製造事業者署名 |

図 2　生体照合器証明書

なお、生体照合器証明書には，生体照合器の特定、ひいては所有者の特定に繋がる情報である，生体照合器証明書識別コード，生体照合器識別コード，生体照合器公開鍵が含まれており，生体照合器内での安全・確実な管理を想定している.

### 3.2. 生体テンプレート証明書の登録･管理機能

信頼できる生体テンプレート証明書発行機関は、生体テンプレートと共に生体テンプレートハッシュ証明書を内蔵する生体テンプレート証明書を発行する．その構成を図 3 に示す.

| 生体テンプレート証明書識別コード |
|---|
| 発行機関識別コード |
| 証明書有効期限 |
| 対象の生体部位 |
| 証明書に対する生体部位所有者の公開鍵 |
| 生体テンプレート |
| 生体テンプレートハッシュ |
| 生体テンプレートハッシュ証明書としての発行機関署名 |
| 生体テンプレート証明書としての発行機関署名 |

図 3　生体テンプレート証明書

生体照合器で使用する生体テンプレートが信頼できる生体テンプレート証明書発行機関が発行したものであることをサービスシステムへ示すために，生体テンプレート証明書そのものではなく，生体テンプレートを除いた生体テンプレートハッシュ証明書（図 4）をサービスシステムへ提供することを想定している．

| 生体テンプレートハッシュ証明書識別コード |
|---|
| 発行機関識別コード |
| 証明書有効期限 |
| 対象の生体部位 |
| 証明書に対する生体部位所有者の公開鍵 |
| 生体テンプレートハッシュ |
| 生体テンプレートハッシュ証明書としての発行機関署名 |

図 4　生体テンプレートハッシュ証明書

生体テンプレート証明書発行機関は，本人確認後に生体部位所有者に証明書に対する鍵ペアを生成し，証明書内に公開鍵を格納する.秘密鍵は利用者へ提供し，その証明書が対象とする生体部位の所有者であることを示すために使用される．証明書発行機関は各国政府発行の国民 ID カード（日本の場合はマイナンバーカード）を利用し確実な身元確認，当人確認を行うことを想定しているが，利用者の匿名性確保のために，国民 ID や紐づけられた鍵ペアの使用は避け，新たに発行した鍵ペアを使用する．

生体テンプレート証明書発行機関は、証明書を所有者確認機能付きのセキュアなデバイスへ格納し、利用者へ提供され、生体照合器への登録時には所有者確認を想定している。なお、所有者確認機能付きのセキュアなデバイスについては、本稿では規定していない。

生体テンプレート証明書は、生体照合器に複数登録されることを想定し，証明書にはシリアル番号等の識別コードを付与し管理する。図 5 に，登録生体テンプレート証明書情報の構成を示す．

| 登録生体情報識別コード |
|---|
| 生体テンプレート証明書 |

図 5　登録生体テンプレート証明書情報

### 3.3. サービスシステムへの利用登録対応機能

利用登録時には，使用する生体照合器の信頼性確認のため，図 2 に示す生体照合器証明書を，生体照合器の秘密鍵所有を示すための署名を付与し，サービスシステムへ提供する．また同様に，使用する生体テンプレートの信頼性確認のため，図 4 に示す生体テンプレートハッシュ証明書を，証明書に対する生体部位所有者の秘密鍵による署名および生体照合器の署名を付与し，サービスシステムへ提供する．

利用登録時には，図 6 に示す利用情報を生体照合器内に登録する．生体照合器を利用するサービスシステムは複数が想定され，多くの生体照合器利用情報が生体照合器内で管理されることを想定している．

| 生体照合器利用識別コード |
|---|
| 生体照合器利用に対する公開鍵 |
| サービスシステム識別コード |
| サービス利用者識別コード |
| 登録生体テンプレート証明書識別コード |

図 6　生体照合器利用情報

その後，サービスシステムによるの利用者の登録のために，登録生体テンプレート証明書識別コードを除く生体照合器利用情報へ生体照合器利用情報に対する秘密鍵による署名および生体照合器の署名を付与し，サービスシステムへ提供する．

### 3.4. サービスシステムへの利用認証対応機能

利用認証時には，図 6 の生体照合器利用情報に基づいて生体照合を実施，照合結果と共に使用された生体テンプレートの情報を含む生体照合実施情報を算出する．それぞれに，生体照合器利用情報に対する秘密鍵による署名を付与しサービスシステムへ提供する．なお,図 7 に生体照合実施情報の算出方法を示している．

```
生体照合実施情報
  ＝Hash(Hash( サービスシステム識別コード
             | サービス利用者識別コード
             | 生体照合器利用識別コード
             | Hash(使用した生体テンプレート) )
    | チャレンジコード)
```

図 7　生体照合実施情報の算出方法

## 4. サービスシステムの機能仕様（利用者登録・認証に関わる機能）

### 4.1. 生体照合器の信頼性確認機能

生体照合器から提供される図 2 の生体照合器証明書により生体照合器のモデルを確認し，生体照合器モデル識別コードに対応する信頼できる評価機関が発行する生体照合器モデル評価結果証明書，図 8 に構成を示している証明書の＜機能・性能・セキュリティ評価結果＞を使用し，利用者が使用する生体照合器の信頼性を確認することを想定している．なお、＜機能・性能・セキュリティ評価結果＞については，本稿では規定していない．

| 生体照合器モデル評価結果証明書識別コード |
|---|
| 評価機関識別コード |
| 製造事業者識別コード |
| 生体照合器モデル識別コード |
| ＜機能・性能・セキュリティ評価結果＞ |
| 評価機関署名 |

図 8　生体照合器モデル評価結果証明書

生体照合器の信頼性を確認後，生体照合器固有の識別コードを内蔵する生体照合器証明書は安全に保管される（利用者の利用認証時には使用しない）.

### 4.2. 生体テンプレートの信頼性確認機能

生体照合器から提供される生体テンプレートハッシュ証明書が，信頼できる生体テンプレート証明書発行機関の発行かどうかを，発行機関の公開鍵証明書を利用し検証，信頼性を確認する．

生体テンプレートハッシュ証明書発行機関の信頼性を確認後，生体テンプレート証明書固有の情報を含む生体テンプレートハッシュ証明書は安全に保管される（利用者の利用認証時には使用しない）.

### 4.3. 利用者の登録機能

生体照合器および生体テンプレートハッシュ証明書の信頼性を確認後，利用者へ固有の識別コードを割り当て，利用者の生体照合器へ通知する．

その後，利用者の生体照合器より，生体照合器利用情報に対する秘密鍵による署名，生体照合器の署名が付与された生体照合器利用情報が提供される．サービスシステムでは，2 つの署名の検証により，信頼性を確認した生体照合器が生体照合器利用情報に対する秘密鍵の所有を確認する．利用者の認証では，信頼性が確認された生体照合器の使用の確認に，生体照合器の署名ではなく、生体照合器利用情報に対する秘密鍵による署名を使用する．

その後，サービスシステムは利用者識別コードに対応させ，生体照合器利用情報および生体照合検証情報を，利用者管理情報として登録する．利用者管理情報の構成を図 9 に示している．

| サービス利用者識別コード |
|---|
| 生体照合器利用識別コード |
| 生体照合器利用に対する公開鍵 |
| 生体照合検証情報 |

図 9　利用者管理情報

なお，生体照合検証情報の算出方法を図 10 に示している．

生体照合検証情報
＝Hash（サービスシステム識別コード
｜サービス利用者識別コード
｜生体照合器利用識別コード
｜生体テンプレートハッシュ）

図 10　生体照合検証情報の算出方法

### 4.4. 利用者の認証機能

生体照合器から提供される生体照合実施情報と，利用者識別コードに対応し管理されている利用者管理情報を使用し，利用登録時に信頼性が確認された生体照合器および生体テンプレートが使用されたかどうかを確認する．

具体的には、生体照合器利用に対する公開鍵による署名検証により、利用登録時に信頼性を確認した生体照合器が使用されたことを確認し、生体照合実施情報と生体照合検証情報の一致の確認により、利用登録時に信頼性を確認した生体テンプレートが使用されたことを確認する。

その後に，生体照合結果がサービスシステムのポリシーに合致するかどうかで，利用者としての認証の是非を判断する．

## 5. SSRBA 機能仕様のリスクと対応状況・要件

本章では，想定中の SSRBA 機能仕様における、生体照合器（利用者）とサービスシステム（サービス提供者）間のリスクについて，SSRBA で想定するリスクへの対応方針を整理している．

### 5.1. 生体照合器証明書による使用する生体照合器の信頼性確認

(1)サービスシステム側で想定されるリスク

①　生体照合器証明書の偽造・改ざん

製造事業者の公開鍵による署名検証で検知可能（製

造事業者による秘密鍵の秘匿管理）

② 異なる生体照合器証明書によるなりすまし

生体照合器証明書に付与した生体照合器の秘密鍵による署名の、証明書内の公開鍵による検証で検知可能（生体照合器による秘密鍵の秘匿管理）

(2)利用者側で想定されるリスク

① 製造事業者からの利用の特定に繋がる情報の漏洩

製造事業者による生体照合器証明書と利用者情報の対応の秘匿管理で対応可能

② サービスシステムからの利用者の特定に繋がる情報の漏洩

サービスシステムによる生体照合器証明書の秘匿管理で対応可能

## 5.2. 生体テンプレートハッシュ証明書による使用する生体テンプレートの信頼性確認

(1)サービスシステム側で想定されるリスク

① 生体テンプレートハッシュ証明書の偽造・改ざん

証明書発行機関の公開鍵による署名検証で対応可能（証明書発行機関による秘密鍵の秘匿管理）

② 異なる生体テンプレートハッシュ証明書によるなりすまし

生体テンプレートハッシュ証明書に生体照合器内で付与した生体部位所有者の証明書に対する秘密鍵による署名の、ハッシュ証明書内の公開鍵による検証により、異なる生体部位所有者の証明書を検知可能（生体照合器による秘密鍵の秘匿管理）

(2)利用者側で想定されるリスク

① 生体テンプレート証明書発行機関からの利用者の特定に繋がる情報の漏洩

証明書発行機関による生体テンプレート証明書と利用者情報の対応の秘匿管理で対応可能

② サービスシステムからの利用者の特定に繋がる情報の漏洩

サービスシステムによる生体テンプレートハッシュ証明書の秘匿管理で対応可能

## 5.3. 生体照合器利用に対する公開鍵による生体照合器の使用確認

生体照合器利用に対する公開鍵は，生体照合器固有の公開鍵に代わって，サービスシステムが利用認証時に信頼性が確認された生体照合器の使用を確認する署名検証での使用を想定している．

(1)サービスシステム側で想定されるリスク

① 生体照合器利用に対する公開鍵の不正登録

生体照合器利用情報に対する，生体照合器利用に対する公開鍵による署名および生体照合器の署名の検証により検知可能（生体照合器内での鍵ペア生成，秘密鍵の秘匿管理）

(2)利用者側で想定されるリスク

サービスシステムへ新たに提供する情報は，生体照合器利用識別コードおよび生体照合器利用に対する公開鍵のみであり，利用者の特定に繋がる情報ではなく，利用者側のリスクは無い．

## 5.4. 生体照合実施情報，照合結果による利用者の認証

(1)サービスシステム側で想定されるリスク

① 利用者のなりすまし，異なる生体照合器の使用，異なる生体テンプレートの使用，による不正な生体照合結果

生体照合実施情報の次のハッシュ値により検知可能（生体照合器内の生体照合処理の非改ざん性）

Hash（ サービスシステム識別コード
｜サービス利用者識別コード
｜生体照合器利用識別コード
｜Hash（生体テンプレート））

② 生体照合実施情報の再利用による不正な実施情報

図 7 で示すように，サービスシステムからの生体照合要請時にチャレンジコードを指定することで対応可能

(2)利用者側で想定されるリスク

サービスシステムへ新たに提供する情報は，生体照合実施情報のみであり，利用者の特定に繋がる情報ではなく，利用者側のリスクは無い．

## 5.5. 生体照合器の構成例

本節では，パソコンに接続され使用される生体照合器を想定し，第 3 章，第 4 章の機能仕様，本章のセキュリティ考察結果を前提に，生体照合器の構成例を示す．

生体照合器では，生体情報や秘密情報を管理し，それらを使用した照合処理・認証対応処理を実施するため，その処理結果の信頼性を維持するには，生体情報や秘密情報の漏洩・改ざん防止，処理ソフトウェアの改ざん防止が必要である．そこで，生体照合器への物理的・ハードウェア的攻撃に対応しては，FIPS140-3 のレベル 2~3 相当の耐タンパー性を想定している．また，ソフトウェア的攻撃に対しては TEE の保護機能の利用を想定している．

生体情報や秘密情報の管理および使用する処理を TEE で実施する，生体照合器の機能・データ構成例を図 11 に示している．

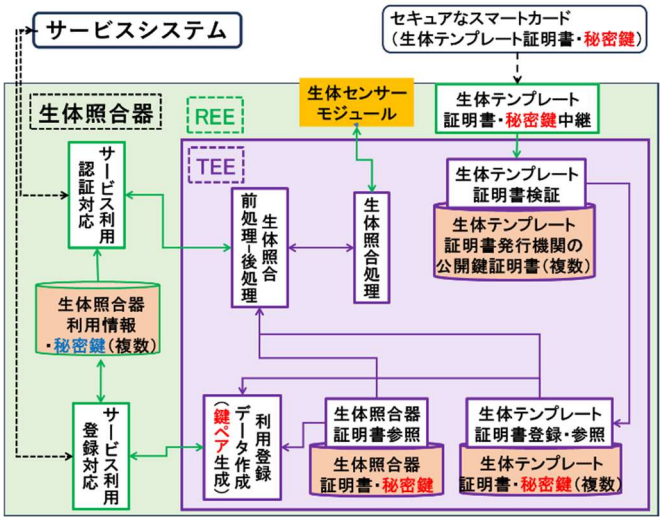


図 11　生体照合器の機能・データ構成例

ただし，REE に配置しているサービス利用登録対応および利用認証対応の処理および生体照合器利用情報については，生体情報や秘密情報の漏洩リスクは無いが，改ざんされた場合はサービスの利用ができなくなるリスクが残る．対策が必要な場合は，改ざん検知・復旧機能の追加，あるいは，SSRBA 対応の機能・データをすべて TEE 配置することを想定している．

## 6. SSRBA の社会実装に向けての検討課題

本章では，SSRBA の社会実装に向け検討すべき今後の課題と，対応案あるいは検討にあたっての配慮事項等を整理する．

(1)生体テンプレート証明書発行機関

対面での確実な本人確認が求められる証明書発行には，利用者の負担も大きい．そこで，国民 ID カードの発行等，同様の要件が求められる手続きと同時に可能なことが望ましい．日本の場合は，マイナンバーカードの発行と同時に，証明書発行機関としては自治体が，というのが一つの候補となろう．

生体テンプレート証明書発行機関をどうするか，発行機関が管理する情報を，生体テンプレート証明書そのもの，生体テンプレートハッシュ証明書，更に圧縮した情報，のいずれにするかなど，社会の安心・安全の維持の重要性と社会受容性を念頭においた検討が必要となろう．

(2)生体テンプレート証明書および秘密鍵を格納するセキュアなデバイス

セキュアなデバイスとしては，証明書発行機関が国民カード発行機関であれば，証明書および秘密鍵も国民カードに格納というのも候補の一つであろう．日本の場合は，異論もあるがマイナンバーカードへの搭載も候補となろう．

(3)クライアントシステム

生体照合器はパソコンをはじめ様々のクライアントシステムに接続し，生体認証を必要とするサービス利用に使用することを想定している．

本稿では，生体照合器に生体センサーも搭載されている想定であるが，将来はクライアントシステムが保有する生体センサーの利用へ発展することも想定される．

クライアントシステムと生体照合器の統合については，他のクライアントシステムでの利用容易性，統合するクライアントシステムと生体照合器の使用年数の相違も念頭においた検討が必要であろう．

(4)生体照合器モデル評価機関

生体照合器モデル評価機関は，公的機関・民間機関両方の可能性を想定しているが，民間機関の場合は信頼性を担保するための監査・評価や認定等の制度が必要となろう．

(5)生体照合器

5.5 節で記載したように，生体照合器の発展に応じ管理すべきデータ，実行すべき処理は TEE に配置されることになろうが，それでも利用者の手元での処理，使用されるデータの非改ざん性の確認機能が必要な場合も想定される．独立したリモートアテステーション機能の追加，あるいは利用認証時の生体照合器からサービスシステムへ提供する生体照合実施情報に非改ざん性の検証結果の追加，等の対応も必要となろう．

生体照合器，本稿の SSRBA では指紋を前提にしているが，将来的には国民カードとの統合，IC 旅券との統合等も想定され，国際民間航空機関 (ICAO) で定めている指紋，顔，虹彩の 3 種の生体照合のサポートも必要となろう．

(6)生体照合器製造事業者

生体照合器製造事業者は，生体照合器モデル評価機関の評価を受けた生体照合処理と共に，SSRBA で規定する様々の機能・データ管理モジュールの実装が求められる．

生体照合器については，実装されている機能モジュールのリモート更新サービスが必要であり，(5)で述べたリモートアテステーション機能とも絡むが，リモート検査・認定等のサービスも必要となる可能性があろう．

なお，このようなサービスは，生体照合器に限らず，今後数多く利用されることが想定される，個人情報・プライバシー情報や資産・資金を格納・利活用に使用されるセキュアワレットに対しても，必要となろう．

(7)サービス提供者（サービスシステム）

SSRBA では，利用者の匿名性を重視しつつも，利用者の不正・不法・悪意のある行為が確認され捜査・調査機関等から合法的要請があれば，利用者の特定のための情報，生体情報器証明書および生体テンプレートハッシュ証明書，を提供できるよう安全・確実に格納しておくことを想定している．社会の安心・安全を維持するための，利用者にサイバー社会へのアクセスを認可したサービスシステム（提供者）の重要な社会的責任であろう．

## 7. おわりに

本稿では，SSRBA の構想について，まず利用者の手元の生体照合器およびサービス提供者のシステムの機能，管理データを具体的に定義し，次にセキュリティを考察し生体照合器の機能・データ配置案を提示した．

また，SSRBA は現時点の IT 環境を前提に考案した構想であるが，ICT の発展に支えられたサイバー社会の拡大が期待され，一方ではサイバー社会での不正・不法な行為や悪意・無責任な行為の増大も懸念される。安心・安全な遠隔生体認証（SSRBA）は、安心・安全なサイバー社会を目指した研究であり，IT 環境の変化に応じ SSRBA への期待も変化する中，想定される社会実装時に必要となるであろう検討課題等を整理した．

将来，サイバー・フィジカル社会の進展，その中でのサイバー社会の役割の増大は必至で，現状でも様々の事故・事件に直面するサイバー社会の安心・安全の維持に向けた対策は喫緊の課題である．サイバー社会における不正・不法，悪意のある行為・無責任な行為の氾濫の要因の一つは，現状のサイバー社会の匿名性の偏重にある．利用者の一人一人の自由な活動を保証するためには匿名性は重要であるが，不正・不法，悪意のある行為・無責任な行為については，安心・安全な社会が維持できるような仕組み，そのような行為を行った利用者を特定する仕組みも不可欠であろう．

筆者は，安心・安全なサイバー社会の実現に不可欠な利用者の匿名性と特定性の両立の実現を目指し，研究活動を展開している．利用者の特定性の確保のためには，利用者の確実な認証が不可欠であり，SSRBA は生体情報による利用者の確実な認証の仕組みを提供しつつ，利用者の匿名性を確保する仕組みを組み込んだ安心・安全な遠隔生体認証である．

サイバー社会の課題克服を目指した研究開発の進展により，サイバー社会の一層の安心・安全の実現を期待したい．

## 文　献


[1] 才所敏明，辻井重男，櫻井幸一，”安心・安全な遠隔生体認証（SSRBA）Secure and Safe Remote Biometric Authentication”，暗号と情報セキュリティシンポジウム（SCIS2025)，2025.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20250129SSRBAPaper.pdf

[2] 才所敏明 ”遠隔生体認証機能を備えたブロックチェーンサービス基盤の提案 BSIwRBA - Blockchain Service Infrastructure with Remote Biometric Authentication-”，第 107 回コンピュータセキュリティ研究会（CSEC107)，2024.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20241114ISEC-Paper.pdf

[3] 才所敏明，辻井重男，“ブロックチェーンサービス基盤に関する考察”，暗号と情報セキュリティシンポジウム（SCIS2023)，2023.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20230124SCIS2023BSIpaper.pdf

[4] 才所敏明，辻井重男，櫻井幸一，”自己主権型アイデンティティ情報利活用基盤（SSIUF：Self-Sovereign Identity-information Utilization Framework）― 利用者の匿名性と特定・追跡性の両立 ―”，情報処理学会・第 84 回全国大会，2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220305IPSJ84SSIUFPaper.pdf

[5] 才所敏明，辻井重男，櫻井幸一，”分散型 ID（DID）/検証可能属性証明（VC）技術を利用した自己主権型アイデンティティ情報利活用基盤（SSIUF）に関する考察”，暗号と情報セキュリティシンポジウム（SCIS2022)，2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220119SCISPaper.pdf

[6] 才所敏明，辻井重男，櫻井幸一，”自己主権型アイデンティティ情報利活用基盤に関する考察”，コンピュータセキュリティシンポジウム 2021（CSS2021）．
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20211028CSS2021Paper.pdf

[7] “Digital Identity Guidelines”， NIST Special Publication 800-63-4. 2025.
https://csrc.nist.gov/pubs/sp/800/63/4/final

[8] 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”，コンピュータセキュリティシンポジューム（CSS2002)，2002.

[9] 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”，コンピュータセキュリティシンポジューム（CSS2001)．