SCIS2025

 1

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

2025年1月29日

（株）IT企画　才所敏明
(株)ZenmuTech
中央大学研究開発機構
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp

共　著　者

辻井重男
中央大学研究開発機構

櫻井幸一
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

1.分類・定義

 2

遠隔認証方式の分類

(1)記憶（秘密の知識確認）による認証
(2)所持（固有の所持物の保有確認）による認証
(3)生体情報（生体の同一性の確認）による認証
　(3-1) 認証者確認（サーバ認証）方式
　(3-2) 被認証者確認（クライアント認証）方式
(3-1) 認証者確認（サーバ認証）方式
　(3-1-1) 生体情報開示方式
　　被認証者の生体情報そのもの、あるいは生体情報を導出できる情報を認証者へ提供
　(3-1-2)生体情報非開示方式
　　被認証者の生体情報を、生体の同一性が検証可能な
　　何らかの非可逆変換を施した情報を認証者へ提供
　　➔キャンセラブルテンプレート方式
　　2001年にキャンセラブルテンプレート方式の概念
　　および生体情報の歪みによる変換方式が提案された
　　2006年に準同型暗号（Homomorphic Encryption）を利用した
　　生体情報を暗号化状態で検証する方式が提案された

(3-2) 被認証者確認（クライアント認証）方式

被認証者がその場で採取した生体情報と、
信頼できる第三者機関が確認した被認証者の生体情報との
同一性の検証を被認証者の手元で行い、検証結果と共に
検証結果の信頼性を示す情報を認証者へ提供

➔2001年に被認証者がPCの利用を想定したBioRAIN構想を提案

被認証者側で実施される生体認証は複数プロセスで構成、を前提とし、
その各プロセスの信頼性、プロセス間の授受データの非改ざん性、を
認証者が検証可能なデータ項目、形式のみを規定し、ISO/IEC SC27へ

➔2009年に国際規格ISO/IEC 24761:2009

（Authentication context for biometrics :ACBio）

日本でも、2005年にスマートフォンが発表され、急速に普及し、
今では、生体認証機能がスマートフォンへ標準搭載される時代へ

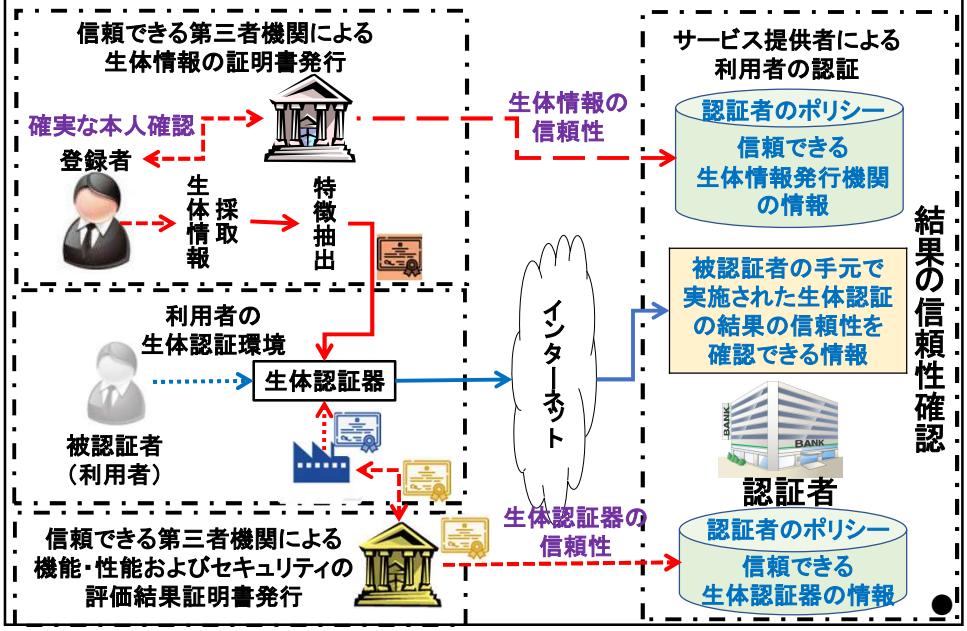
➔安心・安全な遠隔生体認証（SSRBA）構想は、
被認証者確認（クライアント認証）方式を採用しつつ、
＊単一のデバイスでの生体認証を前提とした仕組み
＊当人確認のみではなく、身元確認も含めた本人確認の仕組み
の社会実装イメージ、実装方式を考案したもの

●2分

2.SSRBA概要

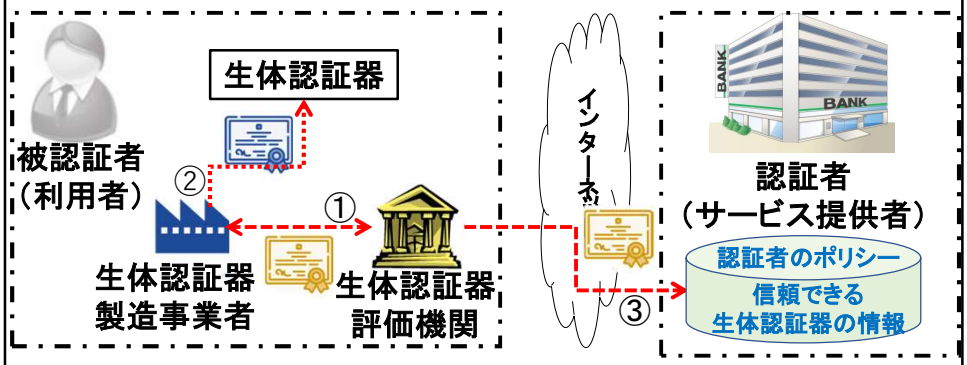
SSRBA概要

Secure and Safe Remote Biometric Authentication



●

（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
②生体認証器への生体認証器証明書の発行（格納）
③認証者システムへの生体認証器モデル評価結果証明書の登録

＜利用者側＞

生体認証器への格納情報

生体認証器証明書
生体認証器秘密鍵

生体認証器証明書

生体認証器証明書識別コード
製造事業者識別コード
生体認証器識別コード
生体認証器公開鍵
生体認証器モデル識別コード
製造事業者署名

＜認証者側＞

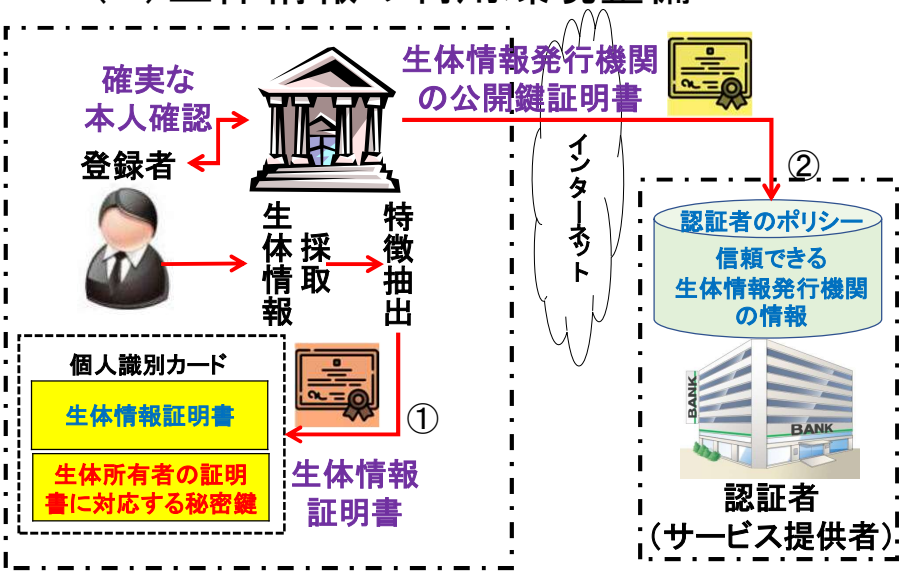
生体認証器評価機関が発行する情報

生体認証器モデル評価結果証明書

生体認証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
生体認証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

4.生体情報

（2）生体情報の利用環境整備



①生体情報証明書の発行
②認証者システムへの生体情報証明書発行機関の登録

＜利用者側＞

個人識別カード格納情報

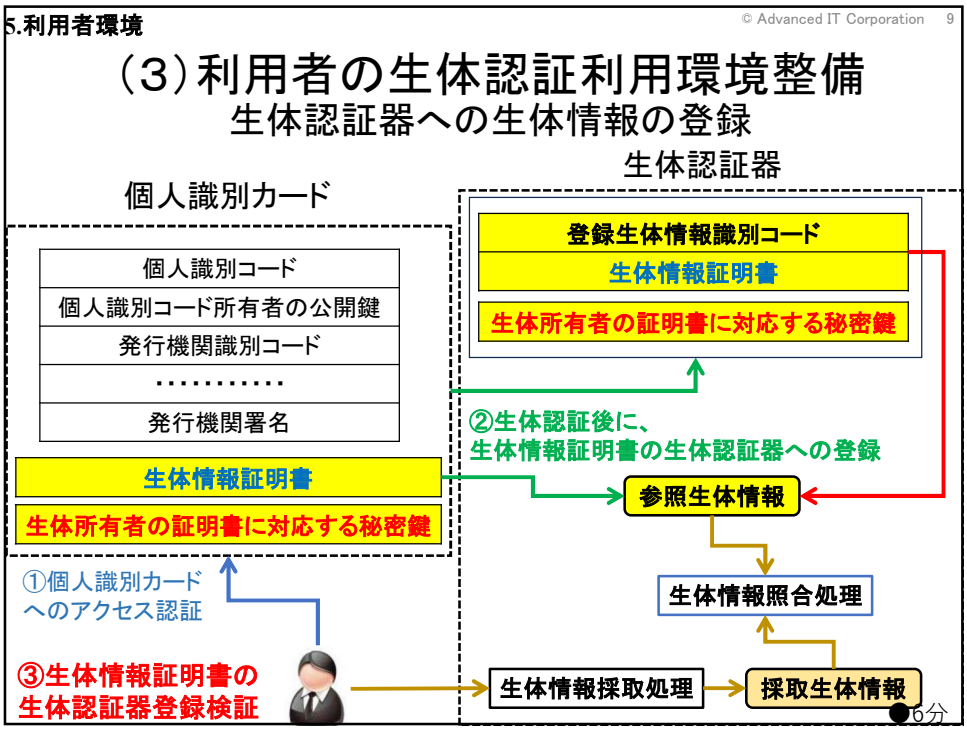
個人識別コード
個人識別コード所有者の公開鍵
発行機関識別コード
・・・・・・・・・・
発行機関署名

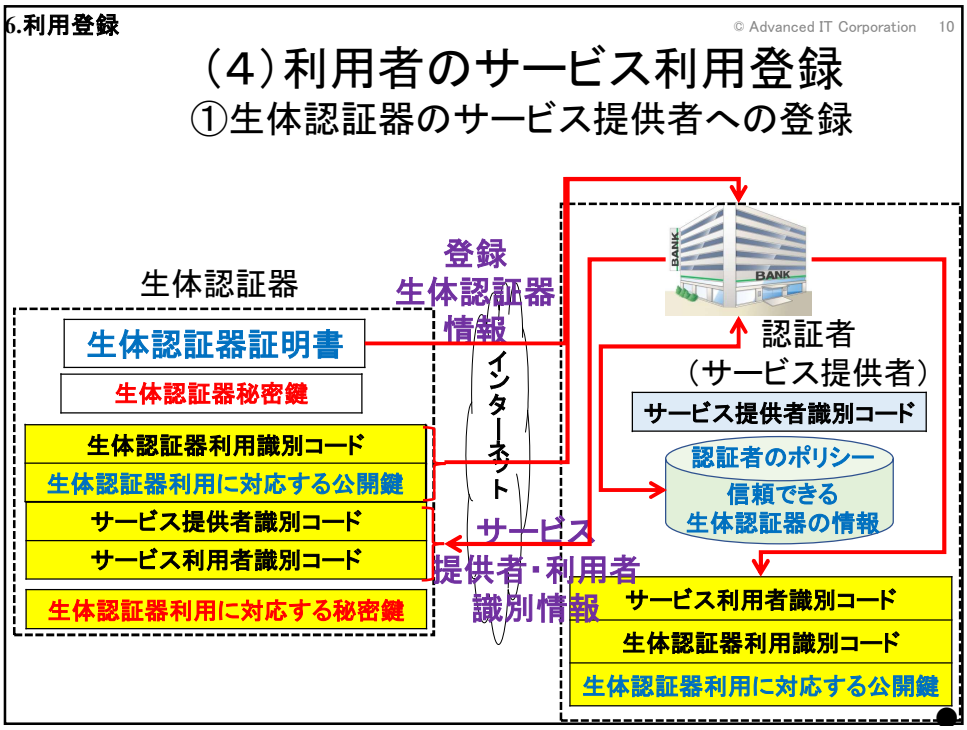
生体情報証明書

生体所有者の証明書に対応する秘密鍵

生体情報証明書

生体情報証明書識別コード
生体情報ハッシュ証明書識別コード（＝生体情報証明書識別コード｜”h”）
発行機関識別コード
生体情報証明書有効期限
生体所有者の証明書に対応する公開鍵
対象の生体部位
生体情報
生体情報のハッシュ値
生体情報ハッシュ証明書としての発行機関署名
生体情報証明書としての発行機関署名


5.利用者環境
© Advanced IT Corporation 9
（3）利用者の生体認証利用環境整備
生体認証器への生体情報の登録
生体認証器
個人識別カード
個人識別コード
個人識別コード所有者の公開鍵
発行機関識別コード
・・・・・・・・・・
発行機関署名
生体情報証明書
生体所有者の証明書に対応する秘密鍵
登録生体情報識別コード
生体情報証明書
生体所有者の証明書に対応する秘密鍵
②生体認証後に、
生体情報証明書の生体認証器への登録
参照生体情報
生体情報照合処理
生体情報採取処理
採取生体情報
①個人識別カード
へのアクセス認証
③生体情報証明書の
生体認証器登録検証
6分


6.利用登録
© Advanced IT Corporation 10
（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
生体認証器
生体認証器証明書
生体認証器秘密鍵
生体認証器利用識別コード
生体認証器利用に対応する公開鍵
サービス提供者識別コード
サービス利用者識別コード
生体認証器利用に対応する秘密鍵
登録
生体認証器
情報
インターネット
サービス
提供者・利用者
識別情報
BANK
認証者
（サービス提供者）
サービス提供者識別コード
認証者のポリシー
信頼できる
生体認証器の情報
サービス利用者識別コード
生体認証器利用識別コード
生体認証器利用に対応する公開鍵

＜利用者側➔認証者側＞

登録生体認証器情報

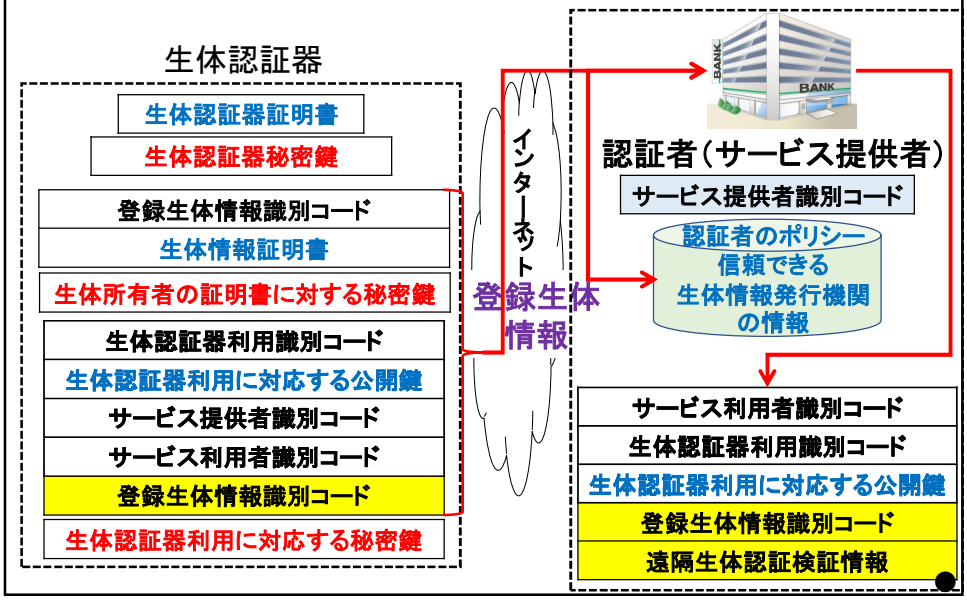
生体認証器証明書
生体認証器利用識別コード
生体認証器利用に対応する公開鍵
生体認証器利用に対応する秘密鍵による署名
生体認証器署名

＜認証者側➔利用者側＞

サービス提供者・利用者識別情報

サービス提供者識別コード
サービス利用者識別コード
サービス提供者署名

②生体情報のサービス提供者への登録



 13

＜利用者側➔認証者側＞

生体情報ハッシュ証明書

登録生体情報

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
生体所有者の証明書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

生体情報ハッシュ証明書識別コード（＝生体情報証明書識別コード｜”h”）
発行機関識別コード
生体情報証明書有効期限
生体所有者の証明書に対応する公開鍵
対象の生体部位
生体情報のハッシュ値
生体情報ハッシュ証明書としての発行機関署名

＜認証者側＞

認証者（サービス提供者）が登録・管理

遠隔生体認証検証情報

＝Hash（サービス提供者識別コード
｜サービス利用者識別コード
｜生体認証器利用識別コード
｜生体情報のハッシュ値）

7.利用者認証

 14

（5）サービス提供者による利用者認証

生体認証器

生体認証器証明書
生体認証器秘密鍵
登録生体情報識別コード
生体情報証明書
生体所有者の証明書に対応する秘密鍵
生体認証器利用識別コード
生体認証器利用に対応する公開鍵
サービス提供者識別コード
サービス利用者識別コード
登録生体情報識別コード
生体認証器利用に対応する秘密鍵

遠隔生体認証結果

インターネット

認証者
（サービス提供者）

サービス提供者識別コード

サービス利用者識別コード
生体認証器利用識別コード
生体認証器利用に対応する公開鍵
登録生体情報識別コード
遠隔生体認証検証情報

 15

＜利用者側➔認証者側＞

遠隔生体認証結果

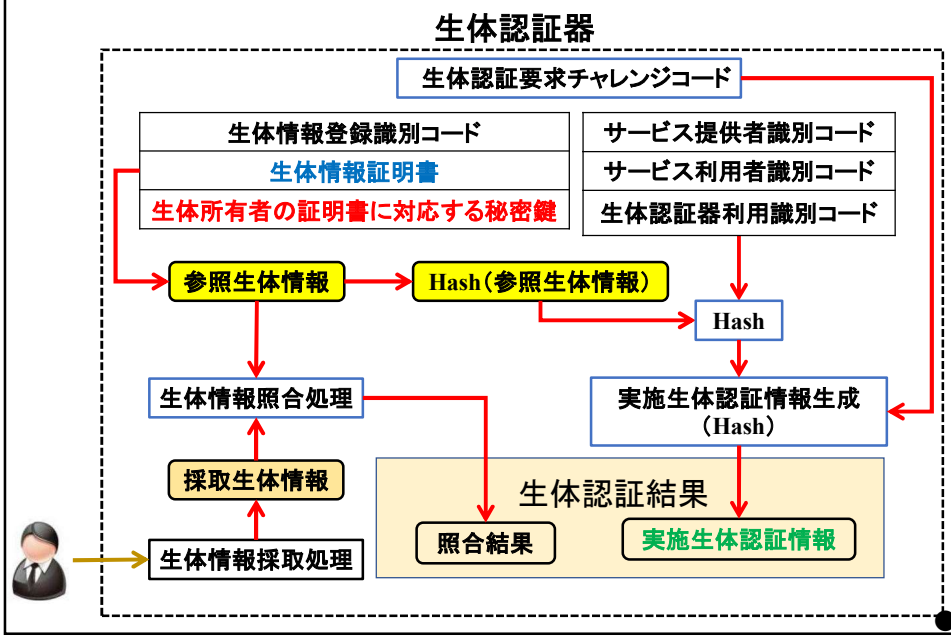
サービス利用者識別コード
照合結果
実施生体認証情報
生体認証器利用に対応する 秘密鍵による署名

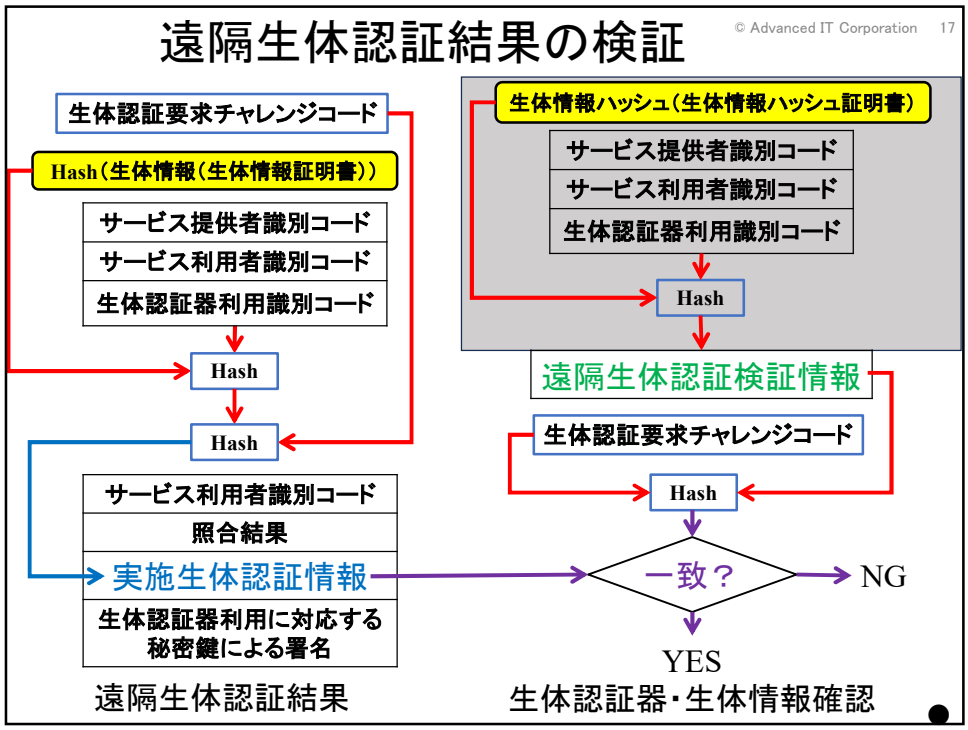
実施生体認証情報

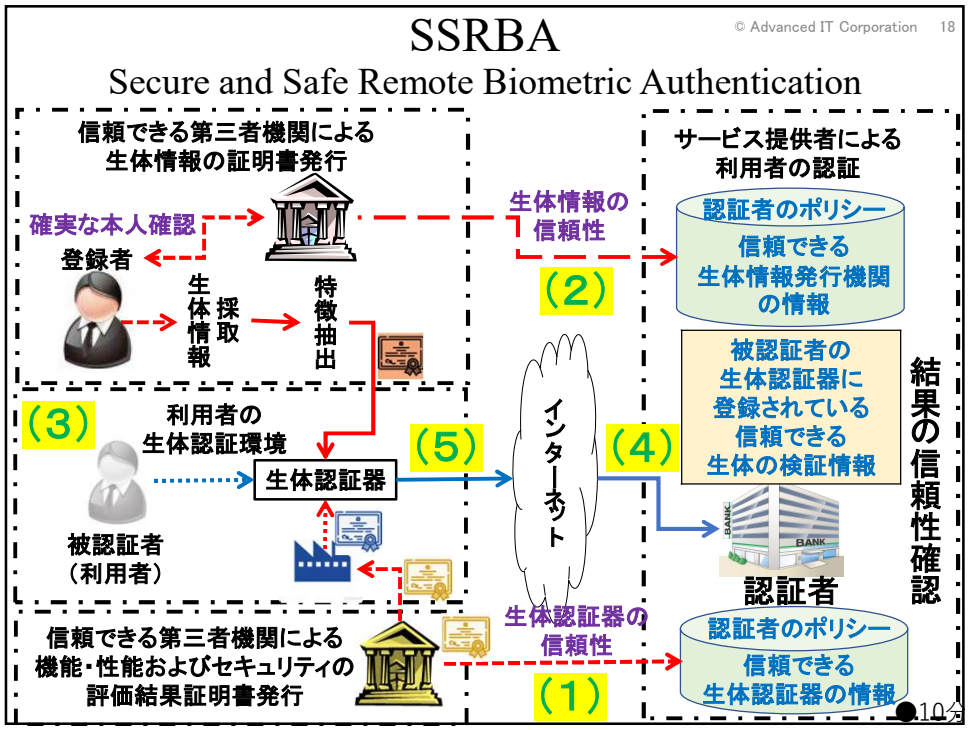
＝Hash（Hash（ サービス提供者識別コード
｜ サービス利用者識別コード
｜ 生体認証器利用識別コード
｜ Hash（参照生体情報））
｜ チャレンジコード）

 16

遠隔生体認証結果の生成

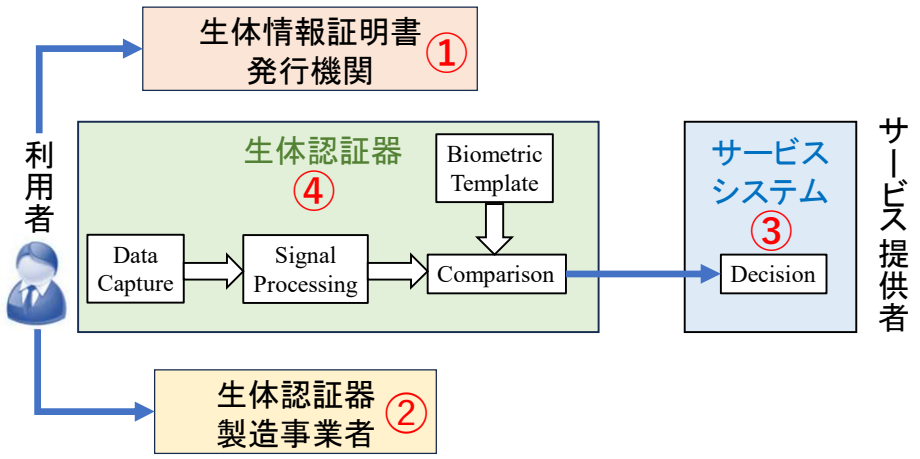



遠隔生体認証結果の検証
© Advanced IT Corporation 17
生体認証要求チャレンジコード
Hash（生体情報（生体情報証明書））
サービス提供者識別コード
サービス利用者識別コード
生体認証器利用識別コード
Hash
Hash
サービス利用者識別コード
照合結果
実施生体認証情報
生体認証器利用に対応する秘密鍵による署名
遠隔生体認証結果
生体情報ハッシュ（生体情報ハッシュ証明書）
サービス提供者識別コード
サービス利用者識別コード
生体認証器利用識別コード
Hash
遠隔生体認証検証情報
生体認証要求チャレンジコード
Hash
一致？
NG
YES
生体認証器・生体情報確認


SSRBA
© Advanced IT Corporation 18
Secure and Safe Remote Biometric Authentication
信頼できる第三者機関による
生体情報の証明書発行
確実な本人確認
登録者
生体情報採取
特徴抽出
(3)
利用者の
生体認証環境
生体認証器
被認証者
（利用者）
信頼できる第三者機関による
機能・性能およびセキュリティの
評価結果証明書発行
生体情報の
信頼性
(2)
(5)
インターネット
(4)
生体認証器の
信頼性
(1)
サービス提供者による
利用者の認証
認証者のポリシー
信頼できる
生体情報発行機関
の情報
被認証者の
生体認証器に
登録されている
信頼できる
生体の検証情報
認証者
認証者のポリシー
信頼できる
生体認証器の情報
結果の信頼性確認
10分

8.考察

SSRBA：利用者（被認証者）のリスク（1）
― 個人情報・プライバシー情報の漏洩 ―



① 生体情報証明書発行機関

個人情報、生体情報を保有

➔個人情報・生体情報漏洩のリスク

➔確実な管理が期待できる信頼できる公的機関を想定

② 生体認証器製造事業者

生体情報は一切扱わない➔生体情報漏洩のリスク無し

保守契約等で、生体認証器識別コードと個人情報の対応を管理

➔個人情報漏洩のリスク

➔顧客情報の確実な管理を想定

③ サービス提供者（サービスシステム）

生体情報は、ハッシュ値のみ➔生体情報漏洩のリスク無し

個人情報は、保有せず➔個人情報漏洩のリスク無し

登録生体認証器情報内の生体認証器証明書には、以下の情報を含む

生体情報証明書識別コード、生体認証器識別コード、生体認証器公開鍵

➔生体認証器製造事業者の顧客情報との突合により、個人情報漏洩のリスク

➔複数のサービス提供者の登録生体認証器情報の突合により、
利用者の複数サービス利用が確認でき、利用者特定につながるリスク

➔登録生体認証器情報の確実な管理を想定

登録生体情報内の生体情報ハッシュ証明書には、以下の情報を含む

生体情報ハッシュ証明書識別コード、
生体所有者の証明書に対応する公開鍵、生体情報のハッシュ値

➔生体情報発行機関の管理情報との突合により、個人情報漏洩のリスク

➔複数のサービス提供者の登録生体情報の突合により、
利用者の複数サービス利用が確認でき、利用者特定につながるリスク

➔登録生体情報の確実な管理を想定

④ 利用者（生体認証器）

個人識別カードは個人情報、生体情報を格納

➔個人情報・生体情報漏洩のリスク

➔個人識別カードは耐タンパーなデバイス、
パスワード、生体によるアクセス制御を想定

➔利用者の自己責任で確実な管理を想定

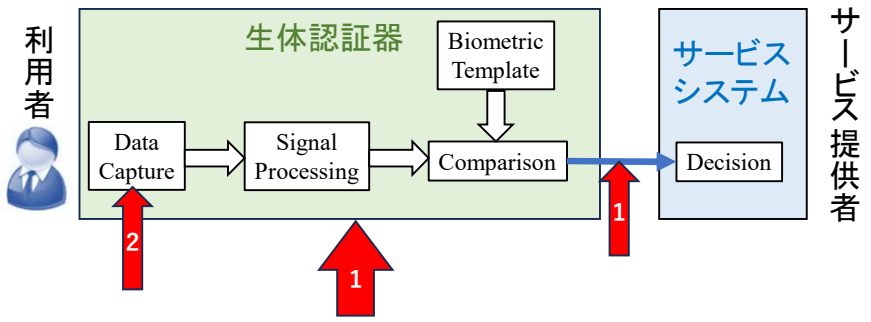
生体認証器は生体情報を格納

➔生体情報漏洩のリスク

➔生体認証器は耐タンパーなデバイス、
パスワード、生体によるアクセス制御を想定

➔利用者の自己責任で確実な管理を想定

SSRBA：サービス提供者（認証者）のリスク（2）
ー　利用者のなりすまし　ー



② 生体情報採取時の攻撃　　① 生体情報採取後の攻撃

①

生体情報採取後の攻撃（インジェクション攻撃）

想定している生体認証器のセキュリティ機能（耐タンパー性）
および　生体認証器とサービスシステム間の通信のセキュリティ仕様
➔生体認証採取後の攻撃へは原則対応可能か
ISO/IEC 19790：暗号モジュールのセキュリティ要求事項
ISO/IEC 24759：暗号モジュールのテストの要求事項
欧州規格：CEN/TS 18099　Biometric data injection attack detection
＜運用開始後にも、適宜の（リモートからの）再検査・評価が必要＞

②

生体情報採取時の攻撃（プレゼンテーション攻撃）

生成AIを活用したディープフェイクによるなりすまし攻撃が活発に提案
➔信頼できる検知技術、検知レベル評価技術は、研究開発中
➔未だ社会実装には時期尚早
➔NISTも検討中だが、SP800-63B（2023年）では
生体認証技術の適用を推奨できないとの判断で、不掲載
国際規格：ISO/IEC 30107　Biometric presentation attack detection

9.おわりに

遠隔生体認証技術の社会実装に向けての課題

1)プレゼンテーション攻撃（PA）への対応

生体認証センサーへの偽造・変造生体・生体情報の提示によるなりすまし攻撃検知技術（PAD）や検知レベルの評価技術に関する研究開発が展開されているが、未だ社会実装には時期尚早

NIST SP800-63B（2023年）:

生体認証技術の社会実装には、生体認証処理に対する追加の信頼が必要

アメリカ政府機関がユーザ認証を行うシステムを構築する際、現時点では生体認証技術の適用を推奨できないとの判断

(2)被認証者側の生体情報センサーやそれを含む生体認証器の信頼性確保・検証

現状のSSRBAによる生体認証結果の信頼性は、被認証者側の生体認証器に強く依存

➔生体認証器の信頼性に対する継続的評価方法の検討

➔セキュアワレットとの役割分担・相互検査機能の可能性検討

終

ご清聴、ありがとうございました。