PBI(Public Biometrics Infrastructure)における公開鍵証明書の再発行方式

鈴木茜[1]　安細康介[1]

概要： ネットワーク社会の拡大や行政サービスの電子化に伴い，個人認証基盤の重要性が高まっている．個人認証基盤には，登録，認証，失効，更新といったライフサイクルが存在することから，持続性のある個人認証基盤を実現するには，要素技術だけでなく，円滑なライフサイクルを実行するための運用技術も重要になる．本研究は，認証技術の一つである生体認証と PKI を融合させた個人認証基盤，PBI において，スマートフォン等のユーザ端末を認証装置として利用する場合の運用性向上に着目したものである．ユーザ端末の紛失時に発生する，ユーザの手続き負担を低減させるために，登録時に生成した予備情報を活用した公開鍵証明書の再発行方式を提案する．

Re-issue Method of Public Key Certificate on Public Biometrics Infrastructure

AKANE SUZUKI[1]　KOUSUKE ANZAI[1]

1. はじめに

ネットワーク社会の拡大, 企業における ICT 活用の進展, 各国における行政サービスの電子化や国民 ID 制度の導入に伴い，ネットワークを介した個人認証の重要性が高まっている．個人認証を実現するにあたって，古くから ID とパスワードが使用されてきたが，なりすまし被害の増大により，セキュリティ強度の高い，PKI(Public Key Infrastructure：公開鍵基盤)へ移行している．

一方で，セキュリティ強度を高めるだけでなく，ユーザの使い勝手にも考慮し，安全性と利便性のバランスが取れた生体認証が普及しつつある．近年，生体認証センサを搭載したスマートフォンが増加していることを背景に，インターネットバンキングのようにユーザ端末の生体認証機能を用いた個人認証も可能になっている．

上述した個人認証には，登録，認証，失効，更新といったライフサイクルが存在する．持続性のある個人認証システムを実現するには，要素技術だけでなく，円滑なライフサイクルを実行するための運用技術も重要になる．

本研究は，生体認証と PKI の技術を融合させた個人認証基盤，PBI(Public Biometrics Infrastructure)システムにおいて，ユーザ端末を認証装置として利用する場合の運用性向上に着目したものである．ユーザ端末の紛失時に発生する，ユーザの手続き負担を低減させるために，登録時に生成した予備情報を活用した公開鍵証明書の再発行方式を提案する．

2. Public Biometrics Infrastructure について

2.1 PBI のコンセプト

ネットワークを介して個人認証を実現する仕組みとして，PKI が一般的である．PKI の安全性・信頼性は秘密鍵の管理に依拠していることから，秘密鍵の格納媒体(IC カード等)の所持や, 秘密鍵活性化のための暗証番号の記憶が必要になり，利便性に問題がある．一方，指紋や静脈などの生体情報に基づいて個人を認証する生体認証技術は，銀行 ATM や企業情報システムへのアクセス制御などへ導入が進んでいる．生体認証システムでは，認証主体が登録生体情報(テンプレート)を管理している．生体情報は機微情報であることから，生体情報の管理と認証処理の実行は，信頼できるサーバで集中的に行う必要があり，大規模な個人認証への適用は困難であると考えられていた．

そこで，IC カードや暗証番号を必要とせず，高度なスケーラビリティを持つ個人認証基盤を実現することを目的とし，PBI が提案されている[1]．PBI は，指紋や静脈などの生体情報そのものを秘密鍵として代替し，一方向変換して元の生体情報に復元困難なテンプレートを活用して, 認証, 署名，暗号化を実現する個人認証基盤である．

2.2 PBI のシステムモデル

PBI システムは，PKI と同様に，認証局がユーザの公開鍵証明書を発行し，ユーザの公開鍵証明書をリポジトリで管理する．登録と認証のフローを下記に示す．

各フローで処理される生体情報として，指静脈，指紋，虹彩など，個人差のある身体の特徴量が想定される．

1（株）日立製作所　研究開発グループ
Hitachi, Ltd. Research & Development Group

(1) **登録フロー**

登録フローの中で，①から③は，ユーザが登録端末を介して実施する処理であり，④は認証主体が認証サーバを介して実施する処理である．

① 登録端末付属のセンサで読取った生体情報の特徴量を抽出し，データ化する

② ①生成したデータと乱数等とを組合せて，一方向変換を行い，PBI 公開鍵を生成する

③ PBI 公開鍵やユーザ ID を含んだ証明書発行要求を生成する

④ 証明書発行要求に含まれる情報や有効期限等の情報に対して，認証局による署名を付与し，公開鍵証明書を発行する

なお，ユーザ自身の端末から登録する場合には，④で生成した公開鍵証明書をユーザ端末に保有する場合がある．

一般的に，生体認証の登録フローは，認証フローでの精度を上げるために，生体情報を複数回かざしたり，複数の生体情報を登録したり，長時間に渡り生体情報をセンサに接触させたりするなど，ユーザにとって負担が重いことが多い．

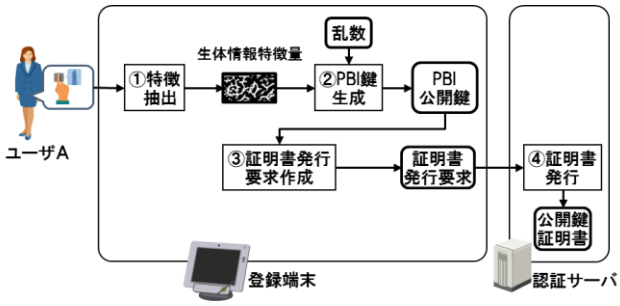

図 1: 登録フロー

(2) **認証フロー**

認証フローの中で，②，③は，ユーザが登録端末を介して実施する処理であり，①，④，⑤は認証主体が認証サーバを介して実施する処理である．

① チャレンジコードを生成し，認証端末へ送信する

② 認証端末付属のセンサで読取った生体情報の特徴量を抽出し，データ化する

③ ②で生成したデータと乱数から，チャレンジコードに対する署名値(レスポンスコード)を生成し，認証サーバへ送付する

④ 公開鍵証明書に含まれる PBI 公開鍵を用いて，署名値(レスポンスコード)の検証を行う

⑤ ④で復号したデータと④のチャレンジコードの一致を確認する

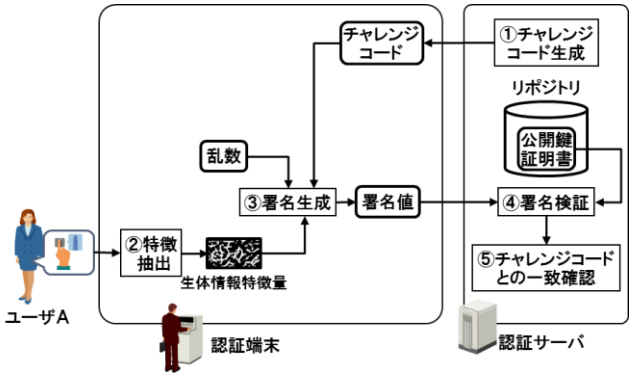

図 2: 認証フロー

2.3 PBI のモバイル端末への適用について

従来の生体認証システムでは，各企業がエンドユーザに提供する装置(ATM や入退室管理装置等)を用いて個人認証を実施していた．近年は，生体認証センサを搭載したスマートフォンが増加し，また，スマートフォンに搭載される汎用的なカメラやマイクを用いて生体認証を行う技術が向上している．例えば，スマートフォンに標準搭載されているカメラで指静脈認証を実現する技術が開発されている[2]．このような背景から，企業が提供する装置だけでなく，個人の端末を用いて生体認証を行うような利用シーンが拡大しつつある．

本稿では，個人のモバイル端末を活用した，PBI の個人認証に着目し，課題の抽出と解決策の検討を行う．

3. ユーザ端末紛失時の問題

スマートフォン等のユーザ端末を認証端末に用いた場合には，ATM や窓口端末のような据え置きの装置と比較して，紛失や盗難の割合が非常に高くなる．紛失や盗難の場合には，ユーザ端末に保存している唯一の情報である公開鍵証明書が外部に流出する可能性がある．２章で述べたように，PBI システムの公開鍵証明書には，生体情報を一方向変換した PBI 公開鍵が含まれるが，元の情報への計算が困難な処理を施している．そのため，生体情報といった機微情報が漏洩することはない．しかしながら，自身の生体情報から抽出したデータを取り替えてユーザに安心感を与えられるように，既存の PKI の運用と同様に公開鍵証明書を失効・再発行させる運用が考えられる．

公開鍵証明書を失効させると，図 1 に示す登録フローを再度実施して，証明書の再発行を要求する必要があり，ユーザ登録時と同様の負担が生じる．

4. ユーザの負担軽減に向けた解決方針

4.1 PKI システムにおける従来技術

３章で述べたように PBI ではユーザ端末紛失時の手続き

負担が問題であった. 例えば, PKI では以下に示す技術で, ユーザの負担軽減を図っている.

Web サービスにおいて，パスワードに代わりに，スマートフォン等の端末に保管した秘密鍵を利用して認証を行う方式において，スマートフォン等を消失すると秘密鍵が消失し，再度登録しない限り，サービスの利用ができなくなるという問題がある．鍵の消失の課題についての解決策として，鍵をインターネット上のサーバに保管しておき，端末に代わってキーストア上の秘密鍵で認証処理を実現する方法が提案されている[3,4]．サーバのキーストアにアクセスするために別途認証が必要となるが，キーストアと携帯電話ネットワーク間では事前にセキュアに接続できるように認証用の鍵や接続に関する情報を交換しておき，端末と携帯電話ネットワーク間は回線認証により認証を行うなど，ユーザの負担を軽減している．

4.2 課題の解決方針

PKI システムにおける従来技術においては，ユーザの利便性や個人情報保護の観点から，二つの課題がある．その一つは，端末消失時には，利用者が使用していたサービスの鍵管理サーバにアクセスするための認証用の鍵がなくなるため，利用者が窓口を訪問して，新たな端末へ認証用の鍵の再登録を行う必要があり，ユーザの利便性に課題がある．また，二つ目の課題は，サービスの全ユーザ分の秘密鍵をサーバ上で管理するため，万が一サーバ上の情報が漏洩した場合には影響範囲が広い．そのため，秘密鍵の管理に対して，厳重なセキュリティ対策などに運用コストがかさむことが課題である．

PKI システムにおける従来技術の課題を考慮し，PBI システムにおける，ユーザ端末紛失時の問題の解決方針を設定する．

(ア) 利便性の確保
　新たな端末でサービスを再開するにあたって，追加の登録手続きを発生させない

(イ) 秘密情報の非保持
　ユーザ端末や認証サーバ側で，ユーザの秘密情報を管理しない

(ウ) 本人性の確認
　サービスの再開後も，従来の PBI システムと同等レベルで本人性を確認する

5. 予備情報を活用した再発行方式の提案

5.1 提案方式の処理

ユーザによる再発行手続きを簡略化するために，登録時にサーバ保管した予備情報から新しい証明書を仮発行し，認証時と同じ手順で利用開始できる方式を提案する．

(1) **登録フロー**

提案方式の登録フローに関して，図 1 で示した PBI の既存の登録フローとの違いを記述する．図 3 の処理①で読取った生体情報から N 個の PBI 公開鍵を生成する(図 3 の処理②)．さらに，N 個の PBI 公開鍵に対して，それぞれの証明書発行要求を作成する (図 3 の処理③)．認証サーバでは，N 個の証明書発行要求から本番用の証明書発行要求を 1 枚選択して証明書を発行し (図 3 の処理④)，残りの N-1 個の証明書発行要求を予備データとして保管する．発行された公開鍵証明書は，公開鍵証明書の発行先が所有するユーザ端末にダウンロードし，ハードディスク等に保存される(図 3 の処理⑤)．

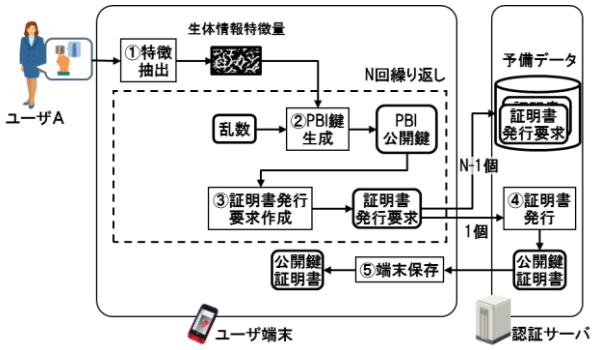

図 3: 提案方式の登録フロー

(2) **失効／再発行フロー**

図 4 に示す通り，ユーザが個人認証に使用している端末を紛失した場合には，失効と再発行の手続きを行う．紛失専用の緊急ダイヤル等に連絡し，紛失したユーザ端末に存在する証明書の失効を要請する．この際，電話等で氏名，住所等の個人情報が通知され，認証主体に登録されている情報との一致を確認し，申請者の本人確認が行われる．次に，ユーザが申告した端末に保存されている証明書を失効させる(図 4 の処理①)．さらに予備データから一つの証明書発行要求を選択し，新しい証明書を仮発行する(図 4 の処理②)．秘密情報を用いた厳密な本人確認が行われていないため，新しい証明書は，一時保留の状態で証明書発行情報に登録される(図 4 の処理③)．

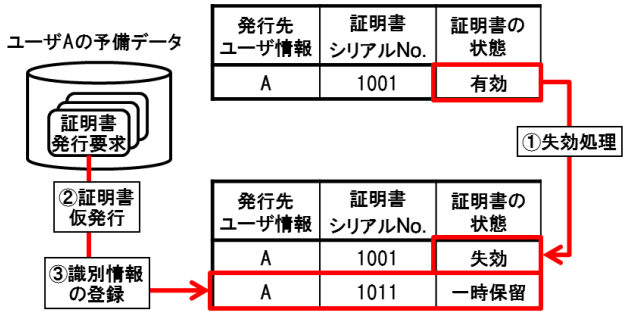

図 4: 提案方式の失効／再発行フロー

(3) 再発行後の認証フロー

ユーザは，紛失後に入手した新しい端末や紛失後に発見された既存の端末で認証処理を行い，各種 Web サービスを再開するができる．

図５の提案方式の再発行後の認証フローに関して，図２で示した PBI の既存の認証フローとの違いは以下の通りである．

認証サーバから識別情報を活用して新証明書をユーザ端末にダウンロードし，ユーザ端末に保存する (図５の処理①②)．図２と同様に，読取った生体情報と乱数から署名値を生成する(図５の処理③④)．署名値と共に認証サーバに送付された新証明書を用いて署名検証が行われる(図５の処理⑤)．署名検証の成功により再発行手続きの本人確認が完了し，新証明書を有効化する(図５の処理⑥)．その後，再度，通常の認証処理が行われ，サービスの利用を再開できる(図５の処理⑦)．

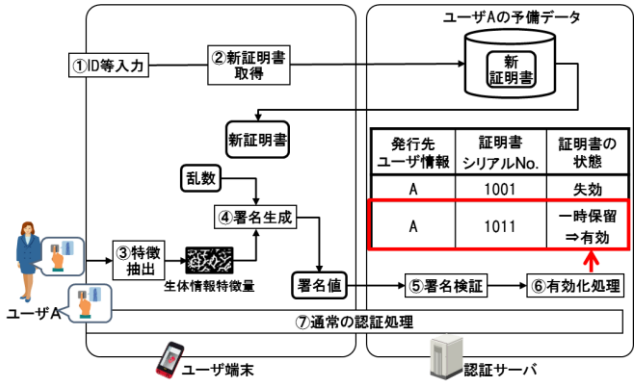

図 5: 提案方式の再発行後の認証フロー

5.2 提案方式の評価

提案方式に関して，４章で提示した解決方針に沿っているかに基づいて，評価を行う．

(ア) 利便性の確保

(2)失効／再発行処理に示すように，ユーザが窓口に出向かずに，電話等の簡易な本人確認でユーザが紛失した端末に保持されている証明書を特定し，手続きを実施することができる．

(イ) 秘密情報の非保持

(1)登録処理に示すように，認証サーバで，再発行のために保持する予備データは証明書発行要求のみである．証明書発行要求には，既存の PKI システムと同様に発行先のユーザ情報が含まれ，また，PBI システム特有の PBI 公開鍵が含まれる．PBI 公開鍵は，生体情報一方向変換したデータであり，元の情報に復元できないため，秘密情報には当たらない．また，PKI では証明書発行要求を作成すると，対応する秘密鍵を保管する必要があるが，PBI では生体情報から署名を生成するため，ユーザ端末に秘密鍵といった秘密情報が保持されない．

(ウ) 本人性の確認

(3)再発行後の認証フローに示すように，本人の生体情報で署名させることにより，本人確認を行い，新しい証明書を有効化している．本人にしか，新しい証書による認証を成功させることができないことから，サービス再開後も本人性を確保することができる．

6. おわりに

本稿では，生体認証と PKI の技術を融合させた個人認証基盤，PBI システムにおいて，ユーザ端末を認証装置として利用する場合の運用性向上に着目したものである．ユーザ端末の紛失時に発生する，ユーザの手続き負担を低減させるために，予備情報を活用した公開鍵証明書の再発行方式を提案した．

本方式の実装評価や FIDO(Fast IDentity Online)といったオンライン認証規格への準拠は今後の研究とする．

参考文献

[1] 高橋健太，村上隆夫，加賀陽介，松原佑生子，米山裕太，本部栄成，西垣正勝，“テンプレート公開型生体認証基盤”，SCIS 2012， 1F1-3，2012

[2] 三浦直人，中崎渓一郎，市毛健志，松田友輔，長坂晃朗，宮武孝文，“可視光画像に基づく非接触型複数指静脈認証”，SBRA 2016， S2-7，2016

[3] 緒方祐介，中谷裕一，山下高生，岩田哲弥，“WEB サービス向けの鍵による認証における鍵の管理に関する考察”，2015 年電子情報通信学会総合大会，BS-4-4，2015

[4] 中谷裕一，緒方祐介，山下高生，岩田哲弥，“運用性とコストを考慮したセキュアなユーザ認証方式の提案”，2015 年 電子情報通信学会総合大会，B-7-86，2015