生体認証を用いた利用者の同一性確保

大神 渉[1]　五味 秀仁[1]

概要：ID やパスワードを使った認証に代わり、個人の生体特徴情報を使った生体認証の導入が増加している。特に、従来の生体認証の形態に比べてユーザのプライバシーや安全性に配慮した手法として、分散型生体認証が注目されている。この手法は、ネットワーク上にユーザの生体情報を流すことなく、認証結果をやりとりするため、生体情報の流出のリスクを最小限に留めることができる。本稿では、分散型生体認証を使ってユーザが端末を他人と共有するユースケースにおいて、サービス提供者が登録した本人と利用者が同一人物かという本人性を確認できない問題を提起し、その技術課題を解決するため適切なアクセス制御を行う手法を提案する。

キーワード：分散型生体認証, 本人性, アクセス制御

Ensure User Identity by Using Biometrics

Wataru Oogami[1]　Hidehito Gomi[1]

Abstract: Biometrics authentication has been in widespread use instead of ID and password pair's one. Specially, an authentication method called dispersed biometrics authentication (DBA) is gathering attention because it can more preserve user's privacy and security than conventional biometrics authentication methods. In relative works, they consider how to prevent attack from using system vulnerability or malware in authentication progress. On the other hand, it is not considered to share the use of device by ordinary treatment by its owner. It makes a service provider not to be confirmed its user's identity which is same as register in previous. In this paper, we examine these sharing use cases based on device owner's trust in the DBA. In addition, we propose access control technique using a unique biometrics ID by giving the service provider to notify it.

Keywords: identity verification, dispersed biometrics authentication, access control

1. はじめに

サービスを提供する際、ユーザに identifier (ID) と password (PW) の組み合わせを入力させ、予め登録しておいた組み合わせと照合することで本人かどうかを確認する認証方法は広く普及している。しかし、サービス毎に異なる ID と PW の組を記憶しておくことは難しいため、ユーザは複数のサービスに対して同じ組み合わせを登録することがある。このため、登録しているサービスからこれらの情報の流出が起こった場合に同じ組み合わせを登録した他のサービスまでその影響が及んでしまう。そこで、より強固で記憶に頼らない認証として生体認証の導入が進んでいる。

生体認証とは、指紋や静脈、虹彩など本人しか再現できない身体的な特徴を予め登録しておき、利用者の特徴との一致を確認することで登録者と利用者の一致を確認する認証方法である。生体情報は記憶情報のように忘れたり、所持情報のように紛失したりしないため、ユーザにとって利便性や安全性に優れている。従来の生体認証では、サービス提供者が登録する生体特徴情報を実世界でユーザと相対したうえで本人であることを確認し、その情報を元に利用者の生体情報と照合を行う。そのため、サービス提供者は生体認証に成功した利用者の本人性を確認できる。ここで、本人性とは利用者と予め登録していた人物が確かに同

[1] ヤフー株式会社
Yahoo Japan Corporation

一であることである。このように、生体認証は認証と同時にそのユーザの本人性を確保する本人確認を兼ねて用いられることが多い。さらに、従来の生体認証形態に加えて、ネットワーク上で生体認証の機能をより安全に提供する分散型生体認証という形態が増加している。

分散型生体認証の特徴は、利用者のプライバシーの保護と通信の安全性の両方を確保しているところにある。具体的には、ユーザの所持するスマートフォンなどの端末内で本人の生体特徴情報の照合を完了させるため、それらの情報がネットワーク上に流れない。また、サービス提供者はユーザの端末から認証結果情報を公開鍵方式を使ったメッセージとして受け取るため偽造や改ざんの心配なく、生体特徴情報を受け取らずとも登録者本人が利用していることを確認できる。しかし、この認証方式では、端末の個人所有が暗黙のうちに前提となっており、複数人で端末を共有するユースケースについて十分な検討がされていない。そのため、本人性の確認が十分にできない。これはサービス提供者が照合の内容を正確に知らされることがなく、「いつ」「どの生体特徴情報によって」登録されたものと照合したのか確認することができないためである。

本稿では、分散型生体認証において検討されていない複数人で端末を使うユースケースから、サービス提供者がユーザの本人性を十分に確認できない問題を提起する。また、この問題に対してサービス提供者が期待する本人性を担保するための方法を提案し、現実的なユースケースからこの手法の有効性について議論を行う。

2. 関連技術

従来の生体認証は、ユーザの生体特徴情報をサービス提供者が預かる受領型、生体特徴情報を認証するユーザの所有物にだけ記録する所有物保存型に分類できる。これら 2 つの方法に加え、生体認証をネットワーク上のサービスでも利用するうえで生体特徴情報が流出する可能性を低減しながら通信の安全性を担保する方法として、認証機能と検証機能をユーザの所有する端末とサービスを提供するサーバで分担する分散型の適用が広がっている。これら 3 つの方式は既に社会へ適応されはじめており、それぞれの特徴と違いについて整理する。

2.1 従来型の生体認証

受領型生体認証とは、サービス提供者が直接ユーザの生体特徴情報を預かり、ユーザの認証問い合わせに基づき都度照合する方式である。この方式は、ユーザが認証時に生体特徴情報を提示するだけで利用可能なため、利用状況によりユーザが自由な操作ができない場合などに適しており、一部金融機関における入出金の実証実験 [1] や、ライブ会場での決済 [2] で採用されている。

一方、この方式はサービス提供者とユーザ双方に負担が大きい。まず、サービスを提供するためにはサービス提供者とユーザ間の信頼関係が必要である。もしユーザがサービス提供者のことを信頼出来ず、生体特徴情報を預けることができない場合、ユーザは認証を受けてサービスを利用することができない。また、生体特徴情報はサービス提供者が保存しているため、PW と同様に攻撃や事故などによって流出してしまう可能性がある。このとき、ユーザは生体特徴情報を変更することが難しいため、サービス提供者はそれを厳重に管理することが求められる。そのため、生体特徴の管理や照合をクラウド上などに外部委託しながら、ユーザのプライバシーを保護する研究 [3] がある。

また、**所有物保存型生体認証**とは、サービス提供者の所有するセンサによってユーザの生体特徴情報を抽出し、ユーザが所持する IC カードなどの安全に保管できる物体に保存しておき、ユーザの認証要求時に応じて物体から取り出し、都度照合する方式である。この方式では受領型におけるサービス提供者とユーザ双方の負担を軽減することができ、主に金融機関で指紋や静脈などを用いた ATM 操作の際に、ユーザそれぞれが持つ IC カード内に生体特徴情報を格納して行われる。そのため、IC カードの外に利用者の生体特徴情報が流出しにくく、ネットワークを通じて提供するサービスの提供者がユーザの生体特徴情報を管理するリスクやコストを低減することが可能である。

しかし、この方式では IC カードなどの所有物内の生体特徴情報及び利用者の生体情報の読取りが必要で、サービス提供者がそれらを確実に読み取るための専用の装置を設置する必要がある。そのため、複数のサービスを頻度高く利用することが多いインターネットでの買い物やアカウントへのログインにこの方式を用いることは難しい。

2.2 分散型生体認証

分散型生体認証とは、従来の生体認証の機能を認証と検証の 2 つに分割し、ユーザの所持する端末内で認証を完結させ、サービス提供者はその結果を検証することで本人性の確認を行う方法である。分散型生体認証の認証結果の検証は、非対称鍵を生成し、公開鍵をサービス提供者に登録しておき、ユーザが保存しておく秘密鍵による署名や暗号文を検証することで可能である。そのため、サービス提供者から流出する可能性があるのは登録された公開鍵だけであり、それらが流出しても他のサービスが影響を受けることはない。逆に秘密鍵は端末内から流出しないよう厳重に保存する必要がある。このような特徴をもつため、従来の 2 方式と比較して生体特徴情報を直接サービス提供者が受領して管理することや、サービス毎に異なる IC カードなどの物体を所有し認証の都度読み取る必要がない。そのため、ユーザやサービス提供者の負担が軽く、ログインなどを必要とし頻度に必要とされる認証の機会であっても安全かつ利便性高く利用できるという特徴がある。

分散型生体認証を実現する規格の 1 つとして、FIDO が提案されている。FIDO (Fast IDentity Online) とは FIDO Alliance [4] が推進するユーザ端末内で様々な認証方法をプラグイン可能にするインターフェイスとその認証結果を用いてオンライン上で予め登録したユーザが確かに利用していることを確認するためのメッセージ形式を定める規格である。図 1 に FIDO プロトコルの認証フェーズにおける 2 つの機能を示す。FIDO の規格は認証を行う際、2 つの機

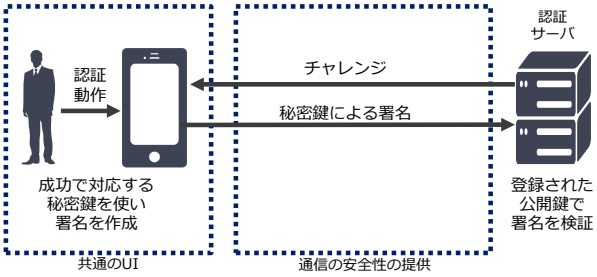


図 1 FIDO 認証時の 2 つの機能

能を提供する。1 つは認証サーバとクライアント間の通信を安全に行うためのメッセージプロトコルであり、もう 1 つはクライアントが端末内で行う様々な認証方法に対応可能な共通のインターフェイスである。前者は予め公開鍵をサービス提供者に登録しておき、対応する秘密鍵をクライアントに保存することで、サービス提供者が都度生成するランダムな文字列 (チャレンジと呼ぶ) に対する署名の検証を行うための機能である。後者は、生体認証だけでなく PIN の入力や二要素認証などの様々な認証方法をユーザが共通のインターフェイスを通じて、利用できる機能である。

FIDO 仕様による認証は次に示す手順に従って行う。認証サーバはユーザの認証要求に対してチャレンジを発行する。ユーザは個人端末に提示されたなかから適切な認証方法を選択して認証を行う。このとき認証は個人端末内でのみ行われ、従来の ID/PW 認証とは異なり認証に必要な情報のネットワークへの流出や認証サーバへの供与はしない。認証が成功した場合、個人端末は認証サーバへ予め登録しておいた公開鍵に対応する秘密鍵を取り出し、チャレンジを含むメッセージへ署名を行う。認証サーバは送られてきた署名に対して登録してある公開鍵を使って検証することができるため、予め登録したユーザと同一人物が個人端末内の認証器によって認証されたことが確認できる。

FIDO 仕様において認証器は authenticator と呼ばれ、サービス提供者は受け入れ可能な authenticator の集合を指定することができる。authenticator は、典型的には指紋、虹彩、静脈などの各ユーザの個人端末に予め備えられているセンサやハードウェアによる生体認証を指向しているが、PIN コードの入力や 2 段階認証などのソフトウェアによる認証方法をプラグインすることも可能である。

FIDO はユーザ個人のプライバシー保護やサービス提供者のリスク低減、ネットワーク上の安全性の向上を目指しており、標準化が進められている。また、金融機関やインターネット上の決済など財産や生命に関する活用だけでなく、日常的なログインの利便性向上などユーザとサービス提供者の認証の負担を軽減する規格として注目されている。

FIDO 以外にも、分散型生体認証を実現する技術の普及もめざましい。例えば iOS 端末に搭載されている TouchID [5] や Android 端末の FingerprintManagement API [6] は、端末のロック解除など基本的な操作に生体認証を使用できるだけでなく、それらをサードパーティのアプリケーションでも使うためのインターフェイスが公開されている。そのため、個人端末を使った分散型生体認証の適用したサービスはこれから更に広がっていくと考えられる。

2.3 トークンベースアクセス制御

ユーザにトークンを発行し、ユーザが提示したトークンの電子的検証が成功することで該当するリソースへのアクセスを許可する OAuth や Kerberos などのトークンベースアクセス制御と呼ぶ技術がある。この技術は、オンラインのリソースへのアクセス制御に用いられているが、実世界のユーザー行動と結びつけることで、オフラインへの適用も可能である。例えば、実世界の店舗でトークンを発行し、ユーザの個人端末へ配布する。ユーザはそのトークンをサービス提供者に提示し、その検証を行うことで、ユーザに割引サービスを提供するなど実世界のクーポンの偽造や改ざんを防ぐことができ、従来の紙媒体のそれを用いることに比べ安全に実施できる。

また、分散型生体認証の検証機能とそれが実現する制御はユーザの実世界での生体特徴情報の入力をトークン配布のための確認動作と考えると、それらが安全にサービス提供者に渡されるという点でこの技術と関連している。分散型生体認証はトークンベースアクセス制御が実世界の制御で行えるこれらの機能に加えて、実在するユーザーに対して生体特徴情報を用いた認証の機能を持つことから、トークンの所持だけではなく、トークンを配布したユーザと同一かどうかをより確実に確保することができる。

3. 問題「本人性の確保」

分散型生体認証では、暗黙のうちにユーザが所有する端末を所有者自身だけが使うことを想定し、ユーザと端末は必ず 1 対 1 の強固な結びつきがあることを前提としている。しかし、ユーザは他人に端末を共有してもよいと考える信頼関係が成立することがあり、その結果、サービスの利用規約と反するものの、以下のように、ユーザ本人が他人に自らの端末を利用させる場合があることが知られている。

- 一時的な協力関係を築いた他人に貸与する
- 親しい間柄の他人と共有する

これらの場合に対し、サービス提供者は生体認証を用いて

いるにも関わらず、登録を行ったユーザと利用者の一致が確認できないため、本人性を担保したサービスが提供できない。これらは従来の生体認証で考慮されてきた特徴量の偽装や、端末へ不正なアプリケーションを注入する不正・攻撃行為ではなく、ユーザが自身の信頼に基いて端末を正規利用する際の問題であり、十分な検討がされていない。それぞれの場合における例と問題点について考察する。

3.1 協力関係にある他人への貸与

ユーザが端末を共有するケースの 1 つに、金銭などの動機によって、一時的に共通の目的を達するために協力する他人へ端末を貸与することがある。例えば、チケット販売サービスでは、需要の多いイベントのチケットを定価で購入し、希望者に高値で売りつけて利益を得る転売行為が問題視されている。転売をするユーザは、イベントが開催される会場で面識の有無に関わらず、入場に必要な物品を金銭と引き換えに購入者に貸与する。必要な物品とは、健康保険証をはじめとした本人確認用の書類であり、転売対策としてこれらの所持を確認している場合が多いが、これらは貸与されても確実な本人性が確認できないため、転売を防ぐことができない。このような問題意識から、チケット販売サービスでは、サービス提供者が購入者と利用者を強固に紐付けるために生体認証の導入 [7] が広がっている。これらの事例では、事前にサービス提供者が利用者の生体情報を預かる受領型生体認証を実施することが多い。しかし、ユーザのプライバシーや生体情報の保護を視野に分散型生体認証の導入が期待されている。

一方、分散型生体認証を用いた場合、購入者と利用者の同一性はサービス提供者が生体認証に期待する効果に対して確保できない。例えば、前述の TouchID や FingerprintManagement API をはじめとする仕組みでは、ユーザの指紋の特徴情報を使って認証を行う。これらの機能では、指の怪我やその時の動作により一時的に登録している指紋が使えない場合に、利便性を高める用途で複数の指紋を追加で登録することができる。これらの認証機能の結果は登録日時の情報に関わらず登録されている指紋と照合できたかどうかを判定する。そのため、図 2 に示すように、転売を試みる Alice は必要な物品を貸与する代わりに端末を Bob に貸与し、Bob の指紋を追加で登録することにより、他人であるはずの Bob が Alice を騙ってサービスを利用することができる。登録された生体特徴情報のなかでサービス提供者が目的とする時点以後に登録されたものが利用者によって提示された場合提供を拒否する性質を**時系列同一性**と呼ぶことにする。時系列同一性を確保することで、図 3 に示すように、サービス提供者が本人性を確認したい行動 (購入) が発生した時点 (t_1) を記憶しておき、その後に追加で登録された $t_N (N > 1)$ で確認できる利用者を拒否することができる。一時的な協力関係にある他人へ貸与する可

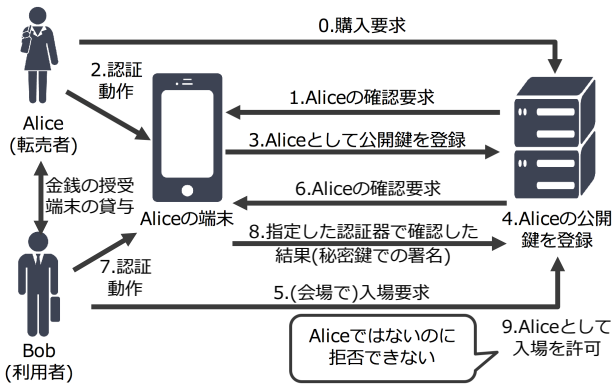


図 2 時系列同一性が無いサービスの例

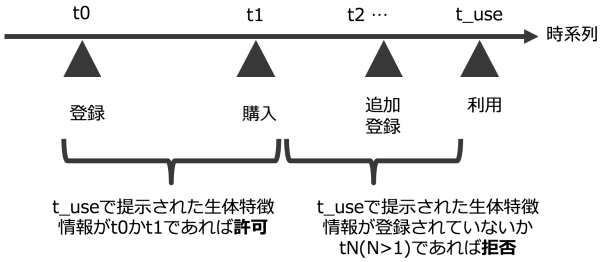


図 3 時系列同一性による提供判断

能性のあるユーザに対して、サービス提供者が時系列同一性のない分散型生体認証を用いた場合、利用者が購入者であることを偽装する可能性があり、その本人性を確保することができないという問題が存在する。

3.2 信頼する他人との共用

ユーザが端末を共有するもう 1 つのケースとして、信頼する他人との共有がある。家族や友人などユーザにとって悪意のない他人と端末を共有する場合、分散型生体認証を通じて自身しか使うことを想定していないサービスが共有している人に提供されることが起こりうる。例えば、家族と端末を共有する場合、画面ロックの解除を逐一持ち主に入力してもらうことは煩わしい。そのため、画面ロックの解除方法を信頼する間柄においては自然と共有されることもある。これは前述の TouchID や FingerprintManagement API などの機能であっても実現可能であり、ユーザは利便性と生体認証への信頼から、本来の用途とは異なるものの、所有者以外のユーザの指紋であっても所有者として登録することができてしまう。

また、これらの機能を使用したサービスも増えており、例えばインターネットの決済の確認においてもユーザ端末におけるこれらの生体認証を用いたサービスが提供されている。この時、サービス提供者は画面ロックと同様の API を用いることで本人が操作していることを確認しているため、実際には共有しているだけで本来は許可してはならないユーザの操作に対してもその承認を取ったこととして

サービスを提供してしまう。そのため、図 4 に示すように

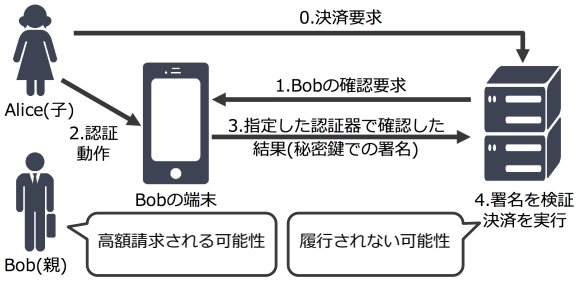


図 4　複数人格識別性が無いサービスの例

親の端末を共有している子供がアプリケーションの課金を行ってしまい、予想以上の高額請求をされるなどサービスでも既に問題となっている。このように信頼する他人と端末を共用するケースでは、どのユーザに紐付いた生体特徴情報と照合できたかという情報が識別されておらず、またサービス提供者にも通知されない。そのため、どのように正確に生体特徴情報と照合が行われたとしても、利用者が複数存在するユーザのどれに該当するのかをサービス提供者が知ることはできない。複数の信頼できるユーザが端末を共有してその生体情報を登録できる状況において、それぞれの本人性を識別できる性質を**複数人格識別性**と呼ぶことにする。サービス提供者が複数人格識別性のない分散型生体認証を用いた場合、信頼関係のあるユーザであっても、意図しないサービス提供が許可されてしまう可能性がある。また、このときサービス提供者も本人性が確認できていないため請求を拒否されてしまうリスクが存在する。

4.　提案「生体特徴情報の識別と管理」

ネットワークを通じたサービスの提供者が分散型生体認証を実施する際、時系列同一性と複数人格同一性の確保が必要である。サービス提供者がユーザの端末内にある認証器を通じてこれらの性質を確保するために生体特徴情報を識別し、管理する方法を提案する。

4.1　認証器とその構成

提案手法について述べる前に、分散型生体認証が用いる認証器およびその構成を整理する。認証器とは、FIDO の authenticator や TouchID などのユーザ端末内の閉じた環境でのみ認証を行い、認証した結果をアプリケーションに伝える機能や装置を指すものとする。認証器の構成は仕様や環境によって異なるが、特徴は共通している。認証器の特徴を抽象的に整理した図 5 を示す。

認証器は、生体特徴情報を読み取るセンサとテンプレート DB により構成され、アプリケーションは Application Program Interface (API) 経由で認証器の機能を利用する。テンプレートとは登録済みのユーザの生体特徴情報のこと

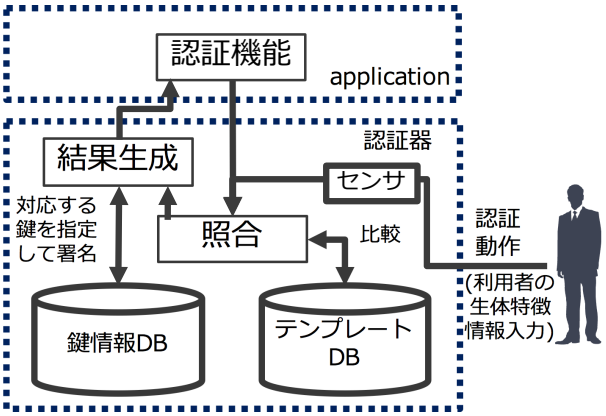


図 5　認証器の構成

を指し、テンプレート DB によって管理される。また、鍵情報 DB は認証器もしくはアプリケーションが持つデータベースであり、例えば、FIDO では図 5 のように認証器の内部に保持するが、TouchID の機能ではこのようなデータを認証器以外の機能 (Keychain API) を使って実現される。鍵情報 DB は、分散型生体認証で用いられることの多い公開鍵方式に則り、生成した秘密鍵を格納しておく。アプリケーションは認証を必要とするときに API を使って認証器を呼び出す。このとき、認証器は利用者へセンサに生体特徴情報を入力することを促す。

認証器は入力された利用者の生体特徴情報とテンプレートを比較・照合し、登録されたテンプレートのうちいずれかと合致するかを比較する。合致した場合、認証が成功したと判断し、認証器はその結果情報をアプリケーションに伝える。このとき結果情報は、認証器の構成によって異なる。例えば、FIDO 仕様では認証が成功したことを伝えるために予めサービス提供者に登録しておいた公開鍵に対応する秘密鍵を認証器が保管しておき、サービス提供者が生成したチャレンジに署名を行う。また、TouchID などの機能では認証が成功したか否かをアプリケーションに伝え、アプリケーションが鍵情報 DB から適切な秘密鍵を使って署名や暗号文の作成を行う。最後にアプリケーションがサービス提供者にこれらの認証結果を伝えることで、サービス提供者は認証結果を検証 (あるいは復号) することで、生体認証の成否を確認することができ、利用者へのサービスの提供可否を決定する。

4.2　本人性の確保

認証器の仕様や認証結果を伝える認証メッセージの内容を変更することで時系列同一性や複数人格識別性を確保するために必要な要件を整理する。サービス提供者は「いつ」登録された「誰 (ユーザ)」に対して認証器が照合したのかを把握することが必要である。認証器はテンプレートと利用者の生体特徴情報の照合を行うため、どのテンプレートに合致するかは明らかである。この時、認証器と認証メッ

セージが満たす要件は以下のように考えられる。

テンプレート DB の要件　認証器は登録されるそれぞれのテンプレート 1 つにつき、端末内で唯一の ID(Unique Biometric ID; UBID と呼ぶ) を付番する。UBID は照合する生体特徴情報の単位に対して 1 つを付番する。UBID はテンプレート DB のインデックスとしてつける。テンプレート DB は複数の認証器が各々管理し、認証器ごとの記号を UBID の文字列内に含むことで端末内の一意性を確保する。例えば指紋認証を行う認証器で、製造者が xyz、モデルが 2016a だとするとき、ある指紋 1 つに対して付番する UBID は、fgrprt−xyz−2016a−0001 のように付番する。

認証メッセージの要件　認証メッセージは、サービス提供者の認証要求に対してアプリケーションもしくは認証器が発行するメッセージであり、分散型生体認証では公開鍵と秘密鍵の組み合わせによって生成する署名や暗号文が用いることが多い。前提として、対応する公開鍵はユーザに紐付けてサービス提供者に予め登録しておく。認証器が作成した認証メッセージはサービス提供者が公開鍵を使って検証・復号することで認証の成否について知ることができる。提案手法では、認証の成否に加えて、UBID もしくは UBID との関連が判断できる情報を認証メッセージの内容を変更してサービス提供者に通知する必要がある。

ユーザ管理の要件　ユーザ管理はユーザが自己申告する識別子ではなく、UBID とその登録時間を用いて行う。これは、自己申告する識別子を用いた場合に次のような問題が起こることが懸念されるからである。例えば Alice が登録した生体特徴情報を Bob であるとして登録しておき、Bob の認証が必要な際に Alice がその生体特徴情報を使って Bob になりすますことができる。このとき、複数人格識別性が確保できない。サービス提供者は、サービスを提供したいユーザ群をユーザ DB として管理する。

これら 3 つの要件を満たし、UBID によって利用者と照合するテンプレートを紐付けて管理することで時系列同一性と複数人格同一性を確保する。鍵情報 DB の所在によって実現方法が異なるため、FIDO 仕様のように認証器内に鍵情報を持つ**認証器署名型**と TouchID や FingerprintManagement API を使ってアプリケーションが署名を作成する**アプリケーション署名型**の 2 つを提案する。

4.2.1　認証器署名型

認証器署名型とは、図 6 に示すように、認証器の中で UBID と秘密鍵を 1 対 1 で関連付けて管理する方法である。アプリケーション及びサービス提供者は認証器が発行した署名を検証することで、対応するユーザが利用していることを確認できる。

機能的な要件　認証器はテンプレート DB 及び鍵情報 DB の参照情報として UBID を付番する。アプリケーションはユーザ DB の中にサービス提供を許可するユーザの鍵情報 DB に対応した公開鍵を保存しておく。

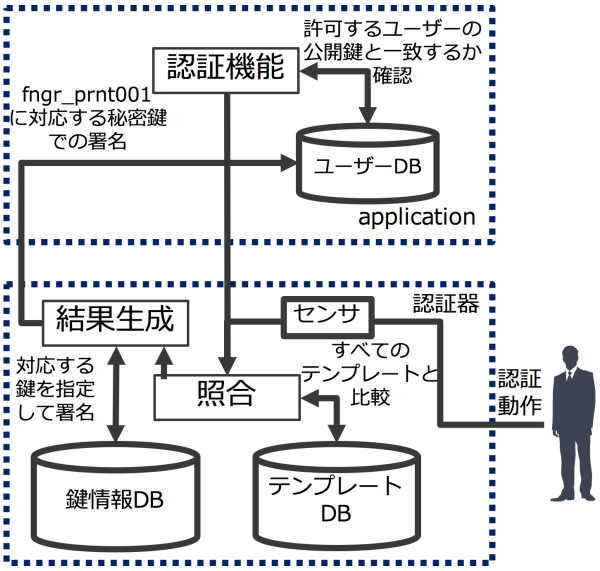


図 6　認証器署名型の例

認証　アプリケーションはサービス提供者が生成したチャレンジとともに認証器に認証要求をする。認証器はユーザから生体特徴情報を受け取り、照合を行う。照合が成功した際、用いたテンプレートに紐づく UBID を特定し、認証メッセージ作成機能を呼び出す。認証メッセージ作成機能では指定された UBID に紐づく秘密鍵を使い、例えばチャレンジに署名を施した上で、それをアプリケーションに返却する。署名を受け取ったアプリケーションは、予めユーザ DB に登録されている公開鍵を使ってそれを検証することで、どのユーザによって登録されたテンプレートと利用者が一致するかがわかる。ここで、後日追加で生体特徴情報を登録した人や登録されている他の人のものが使われた際には UBID に紐付く異なる秘密鍵で署名を施すため、登録時とは異なるユーザが利用していることが分かる。サービス提供者はこのようにして判明したユーザに対してサービスの提供可否を決定する。

4.2.2　アプリケーション署名型

アプリケーション署名型とは、図 7 に示すように、認証器から UBID を含む認証結果を受け取った後、アプリケーションが対応した秘密鍵を選択して認証メッセージを作成する方法である。サービス提供者はアプリケーションが発行した認証メッセージに対応する公開鍵に登録されている登録者と利用者の一致を確認することができる。

機能的な要件　認証器はテンプレート DB の参照情報として UBID を付番する。また、認証器は毎回認証した結果として UBID を返却し、アプリケーションは受け取った UBID を元に鍵情報 DB に登録されている鍵を取り出して認証メッセージを作成する。ユーザ DB には UBID とその登録時間、及び対応する秘密鍵のキーを格納しておく。

認証　アプリケーションはサービス提供者が生成したチャレンジとともに認証器に認証要求をする。認証器は

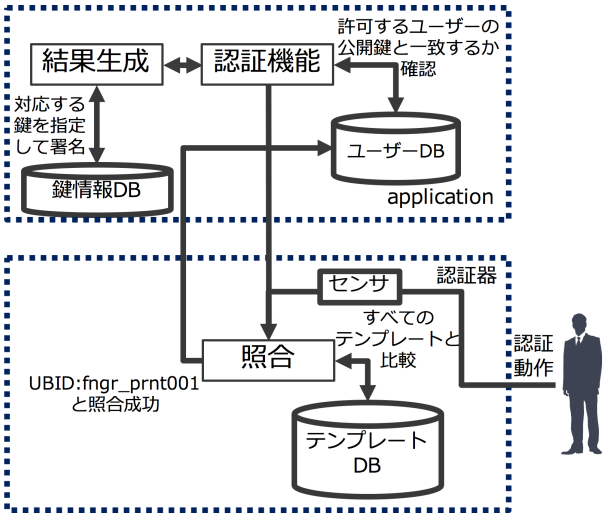


図 7　アプリケーション署名型の例

ユーザから生体特徴情報を受け取り、すべてのテンプレートと照合を行う。照合が成功した際、用いたテンプレートから UBID を特定し、認証結果と合わせて UBID をアプリケーションに通知する。アプリケーションは認証器による認証が成功したとき、その UBID がユーザ DB に登録されているかどうかを確認する。アプリケーションがそのユーザに対してサービス提供の許可を行う場合、参照した秘密鍵のキーを使って鍵情報 DB にアクセスし、必要な鍵を使って認証メッセージを作成する。サービス提供者は送り返された認証メッセージを検証することで適切なユーザがアプリケーションを利用していることがわかる。

4.3　ユースケース・実装例

提案手法を適用した分散型生体認証を適用した電子チケット販売サービスにおいて、購入から利用するまでのユースケースを通じて、提案手法がどのようにして時系列同一性及び複数人格識別性を確保するか考察する。ここでは、Alice がアプリケーションを通じてチケットを購入する。前提として、Alice は自身が購入したチケットには規約として、転売や本人以外の利用を認めていないものとし、サービス適用者はこの規約をユーザに遵守させるために分散型生体認証を適用したアプリケーションを提供している。アプリケーションは、購入時と利用時に指紋認証を施す。利用時とはチケットサービスでは来場した際に係員に対してチケットを提示する直前を指す。このとき、Alice がこのチケットを夫の Bob への譲渡や第三者の Charlie に転売によって使わせることができなければ、提案手法によって時系列同一性と複数人格識別性が確保できる。図 8 に各ユースケースとその制御を示す。

自身の使用　まず、Alice が自身のチケットを利用できることを示す。Alice は自分の端末を用いてアプリケーションを立ち上げ、自分の指紋を使って認証を行い、チケットを購入する。この時、システムはアプリケーション署名型を採用しており、アプリケーションは認証器から照合したユーザの指紋テンプレートの UBID: a001 をうけとる。アプリケーションは、ユーザ DB に購入したチケット、UBID(a001)、購入完了時間と秘密鍵のキーを登録する。次に、Alice が会場でチケットを利用して入場する際、チケットアプリケーションを通じて係員の目前で指紋認証を行う必要がある。これは、指紋認証を行ったユーザと来場したユーザを一致させるために必要な措置であり、係員がまさに目前にいる利用者が購入したユーザであることを確認することができる。アプリケーションは Beacon 信号を使って係員が近づいたことを検知すると、指紋認証画面が起動して Alice に指紋を提示することを求める。Alice は係員の目の前で購入時と同じ指を認証器に通すことで認証が成功し、認証器から UBID : a001 を受け取ったアプリケーションは対応する秘密鍵を鍵情報 DB から取り出し、チャレンジに署名をうってサービス提供者に送信する。サービス提供者が署名を検証した後、アプリケーションはチケットを表示し、Alice はそれを係員に提示することで入場できる。

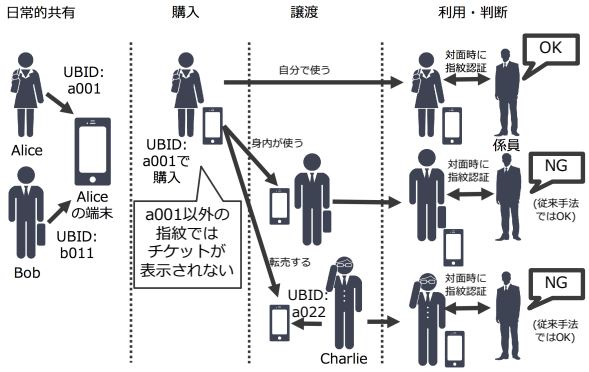


図 8　チケット販売サービスにおけるユースケース

身内の使用　次に、端末を共有している夫の Bob が認証を行った場合その使用を拒否できることを示す。まず、日常的に共有して使うため端末には Alice と Bob それぞれの指紋情報が UBID: a001 と b011 として登録してある。Alice は、a001 の指紋でチケットを購入する。アプリケーションは前述のとおり、認証器から返された a001 と購入時間および対応する秘密鍵のキーをユーザ DB に登録する。Alice は譲渡禁止のチケットであったものの、別の用事ができたため夫の Bob にチケットを端末ごと譲渡する。当日、Bob が会場に来ると、アプリケーションが係員の近接を検知し、指紋認証画面を提示され、Bob は係員の目前で指紋を入力する。ここで、提案手法を適用していない従来のアプリケーションでは、認証器の a001 と b011 での認証結果が同一となり、Bob と Alice は他人であるのに入場を許可してしまう。一方、提案手法を実装したアプリケーションでは、利用時の指紋認証で UBID: b011 が返される。そのため、Bob は指紋認証が成功しても、ユーザ DB に登録されておらず、登録されていても購入者と異なる利用者

であることを判断できるためその利用を防ぐ制御が可能である。従って、**複数人格識別性が確保できている**といえる。

協力関係にある他人の使用　最後に Alice が第三者の Charlie に転売を行った際に端末を貸与したとしても、Charlie の使用を拒否できることを示す。Alice は、UBID: a001 の指紋によってチケットを購入する。アプリケーションは前述のとおり、UBID (a001) と購入時間、対応する秘密鍵のキーをユーザ DB に登録する。Alice は高価で売買されていることを知り、購入したチケットを転売しようとしている。適当なマッチングサービスを使い、購入者 Charlie と Alice の取引が決まった。アプリケーションが登録されている指紋を使った認証を用いることを知っている Alice はイベント当日に端末を Charlie に渡すことでチケットを提示して入場させることを思いつく。そこで、Alice は当日 Charlie に会い、端末を渡した上で、Charlie の指紋 (UBID: a022) を登録した。これによって Charlie は Alice の端末のロック解除を含めた指紋認証を成功させることもできるようになった。Alice の端末をもった Charlie が入場ゲートに近づくと、アプリケーションが係員の近接を検知し、指紋認証画面を提示され、Charlie は係員の目前で指紋を入力する。提案手法を適用していない従来のアプリケーションでは、仮に複数人格識別性があったとしても登録された a022 の指紋は Alice であると認識されるため認証を成功させてしまう。一方、提案手法を用いたアプリケーションでは、UBID: a001 及びその登録時間より以前の時間に登録された指紋と照合されたかどうかを確認できるため、認証器による認証が成功してもそれに対応する認証メッセージの作成は行われない。そのため、Charlie はロック画面は解除できるものの、このアプリケーションによってサービス提供者がチケット画面を提供しないため Alice と Charlie による転売取引は成立しない。したがって提案手法により、**時系列同一性も確保できている**といえる。

4.4 UBID ベースアクセス制御の可能性

アプリケーションが UBID 毎にユーザを管理することで時系列同一性及び複数人格識別性をサービス提供者が確保できることは既に示した。一方、提案手法はサービス提供者のポリシに沿ったアクセス制御だけではなく、ユーザが端末を共有する他人に対して適用したいアクセス制御にも活用することができる。例えば、親が子供のアプリケーション操作に対して制限するペアレンタルコントロールや信頼できる相手であっても見せたくないデータやプライバシーを守るデータロック機能が必要となる場合が多い。

提案手法を用いて、UBID ベースでユーザ管理をアプリケーション単位で可能にすれば、例えば子供と端末を共有していても、ロックを解除して使っているユーザが子供であることがわかる。そのため、親が子供に許可しないアプリケーション内での購買行動や年齢制限コンテンツへのアクセス行動などを登録しておくことで予め制御できる。これは、従来のペアレンタルコントロールでも可能だが、ユーザの切り替えやペアレンタルコントロールモードの解除操作など意識的に利用しているユーザ管理を適切に行えなければこれらの制御が適用できない課題があった。一方、提案手法を用いると、現在の利用者が親子それぞれどちらの操作であるかをサービス提供者やあるいは端末自身が感知して制御を行うため、これらの管理を行わずに済む。このようにネットワークを通じて提供されるサービスにかぎらず、生体認証を通した基本操作であっても提案手法を適用することでこれまでになかった利便性を向上させる使い方ができる。

5. おわりに

分散型生体認証において、他人と端末を共有するユースケースでは時系列同一性と複数人格識別性が確保できない問題を提起した。また、その技術的課題に対し、認証器とサービス提供者及びそのアプリケーションとの協調動作によって、各テンプレートを識別してユーザを管理することで両方の性質を確保できることを示した。提案手法はサービス提供者のリスクやコスト低減をし、ユーザのプライバシーを保護する分散型生体認証の特徴的利点を損なわず、認証及び本人確認の精度を向上させることができる。

今後の課題として、認証器が組み込みや OS など比較的レイヤの低いプログラムで扱うことが多いため、デバイスを提供する事業者と協力しなくては提案手法を実現することは難しい。そこで、サービス提供者の要望としてこうした本人性確保の必要性を訴え、認証器の選択肢として提案手法が適用可能なものを増やしていきたい。

参考文献

[1] 「指紋認証システム」の ATM 取引開始について ｜お知らせ｜イオン銀行. https://www.aeonbank.co.jp/news/2016/0428_01.html.

[2] Liquid Pay - 現金もクレジットカードもいらない生体認証決済システム. http://liquidinc.jp/liquidpay.html.

[3] Hu Chun, Yousef Elmehdwi, Feng Li, Prabir Bhattacharya, and Wei Jiang. Outsourceable two-party privacy-preserving biometric authentication. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pp. 401–412, NY, USA, 2014. ACM.

[4] Fast IDentity Online. https://fidoalliance.org/.

[5] Use Touch ID on iPhone and iPad. https://support.apple.com/en-us/HT201371.

[6] FingerprintManager. https://developer.android.com/reference/android/hardware/fingerprint/FingerprintManager.html.

[7] Akitoshi Okumura, Takamichi Hoshino, Susumu Handa, and Yugo Nishiyama. Identity confirmation to issue tickets using face recognition. Technical Report 2, NEC Informatec Systems Ltd., may 2016.