次世代認証技術を金融機関が導入する際の留意点：FIDO を中心に

井澤秀益（いざわ ひでみつ）／五味秀仁（ごみ ひでひと）

要　旨

近年、生体認証を活用した次世代認証技術が注目を浴びている。その中でも FIDO（Fast IDentity Online）は、ネットワーク越しの認証に生体認証等を利用するための認証手順を定めた仕様であり、2015 年 12 月末時点で約 250 の団体が関わっており、一部のスマートフォンでは FIDO を活用したサービスが既に提供されるなど、利活用が始まりつつある。

金融機関においては、海外において FIDO を利用したインターネット・バンキングを提供しているところもあり、今後、他の金融機関においても FIDO を活用する動きが出てくるものと予想される。もっとも、FIDO は 2014 年に策定された新しい仕様であるため、国内における詳細な資料や情報がまだ乏しい状況である。金融機関が FIDO をインターネット・バンキングに活用する際には、FIDO に関する正しい理解を行ったうえで、情報セキュリティの観点から安全性を評価し適用可能か否かを判断することが重要となる。

そこで本稿では、FIDO の仕組みについて解説を行ったうえで、FIDO をインターネット・バンキングに適用した場合を想定し、その安全性評価を実施し、金融機関が FIDO を導入する際の留意点の考察を行う。

キーワード：生体認証、FIDO、インターネット・バンキング、安全性評価

本稿の作成に当たっては、国立研究開発法人産業技術総合研究所主任研究員の大塚玲氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいはヤフー株式会社の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

井澤秀益　日本銀行金融研究所企画役補佐
（現システム情報局企画役　E-mail: hidemitsu.izawa@boj.or.jp）
五味秀仁　ヤフー株式会社 Yahoo! JAPAN 研究所上席研究員
（E-mail: hgomi@yahoo-corp.jp）

1. はじめに

インターネット上においてサービス提供者（サーバ）が利用者（ユーザ）を認証する仕組みとして、ID とパスワードを利用した方式があるが、それには数々の問題点があると言われている。例えば、①パスワードを記憶しておき、それを入力するのに手間がかかるという利便性面での問題点や、②記憶できるパスワードには限界があるため、それを種々のサービスで使いまわすことにより生じうるパスワードリスト攻撃（独立行政法人情報処理推進機構・一般社団法人 JPCERT コーディネーションセンター〈Japan Computer Emergency Response Team Coordination Center: JPCERT/CC〉［2014］）のリスクを内包しているという安全性面での問題点、が挙げられる。そこで、パスワードへの依存度を減らすために、生体認証を含む多様な認証手段をインターネット等のオープンなネットワーク上で活用する動きが出てきており、その 1 つとして、FIDO（Fast IDentity Online）がある。

FIDO は、ネットワーク越しの認証に生体認証等を利用するための認証手順（認証プロトコル）を定めた仕様であり、それを策定した FIDO アライアンス（Alliance）は、その理念として、セキュリティ（安全性）と利用者の使いやすさ（利便性）を兼ね備えたものと位置付けている（FIDO Alliance [2014]）。2012 年に FIDO アライアンスが発足して以降、同アライアンスに加入する団体は、E コマース運営業者、パソコンベンダー、スマートフォンベンダー、通信キャリア、ソフトウェアベンダー、金融機関等多岐にわたり、2015 年 12 月末時点で約 250 団体が加入している（FIDO Alliance [2015a]）。このため、ここで開発された方式がデファクト標準となる可能性が指摘されており（瀬戸［2015］）、実際に NTT ドコモ社の一部のスマートフォンにおいては FIDO を活用した同社のサービスが利用可能（NTT ドコモ［2015］）であるなど、既に利活用が始まっている。

他方、金融機関におけるインターネット・バンキング等の各種リテールサービスにおいても、安全性と利便性の両方を考慮に入れたうえでシステムの構成を考えることが重要である。そのような中、FIDO を活用したインターネット・バンキングの仕組みはその解決策の 1 つとなる可能性があると考えられ、バンク・オブ・アメリカ（Bank of America）では FIDO を活用したインターネット・バンキングを既に提供している（Bank of America [2015]）。もっとも、金融機関を巡るセキュリティ情勢は厳しさを増しており、インターネット・バンキングにおいては、マルウエアによる情報盗取や自動送金の手口などによる不正送金事例が数多く報告されているほか（大日向［2015］）、今後は、MitB（Man-in-the-Browser）攻撃のように、さらに巧妙なマルウエアによる攻撃が国内の金融機関で猛威をふるう可能性がある。そのような数々の脅威にさらされている中において、FIDO のように、新しい仕組

みを金融機関が導入する際には、FIDO に関する正しい理解を行ったうえで、情報セキュリティの観点から安全性を評価することが重要となる。特に、前述のような様々な脅威に対して FIDO がどの程度耐性を持つのかについて検討を行うことは重要である。

そこで、本稿では前述の問題意識のもと、次世代認証技術の 1 つである FIDO の仕組みを整理し、金融機関が FIDO を導入する際の留意点について考察する。2 節で、前提知識となる FIDO の仕組みについて解説し、3 節で、FIDO をインターネット・バンキングに適用した場合を想定し、その安全性評価を実施したうえで、金融機関が FIDO を導入する際の留意点の考察を行う。4 節は本稿のまとめである。

2. FIDO の仕組み

本節では、次世代認証技術として FIDO を取り上げ、その仕組みについて FIDO Alliance [2014] をもとに解説する。なお、本稿においては、FIDO アライアンスが定める「FIDO UAF（Universal Authentication Framework）ver 1.0」を FIDO と呼び、説明を行う。

(1) FIDO の概要

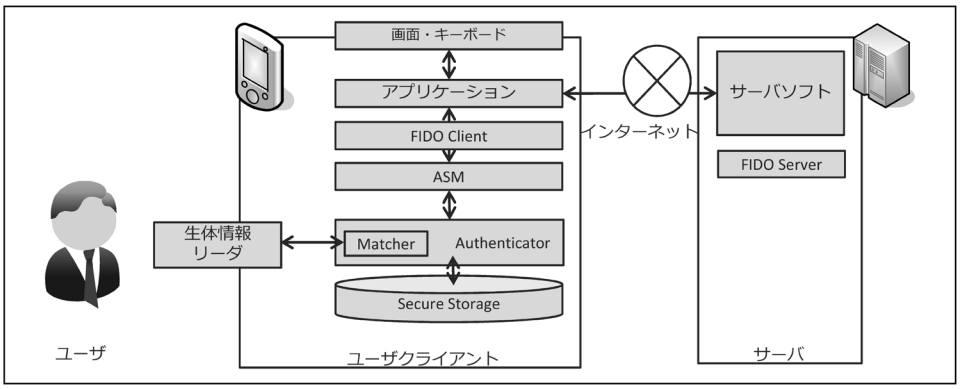
FIDO の主な特徴としては、①ユーザのプライバシーに配慮し、生体情報等の「認証に必要な秘匿すべき情報」をサーバに送信・登録しない点、②生体認証に限らず所有物認証や PIN（Personal Identification Number）認証等、多様な認証要素の利用を想定している点、③様々な端末やサービスが存在する状況においても、統一的なプロトコル（FIDO）で認証を行うことができる点、④「ユーザ認証」に限らず、ユーザの意思に基づいた取引であることをサーバで確認する「取引認証」の仕組みも想定している点、が挙げられる（①④の詳細は補論 1 を参照）。

本稿では、FIDO を活用した生体認証手段を備えたクライアント・サーバシステムの一例（図表 1 を参照）として、図表 2 に示す要素から成るシステムを扱う。

(2) FIDO におけるフロー

FIDO において規定されている登録フェーズ（UAF Registration）と認証フェーズ（UAF Authentication）の説明を行う。登録フェーズは、端末毎・サービス毎に初回に

図表１　FIDO を活用したクライアント・サーバシステムの一例



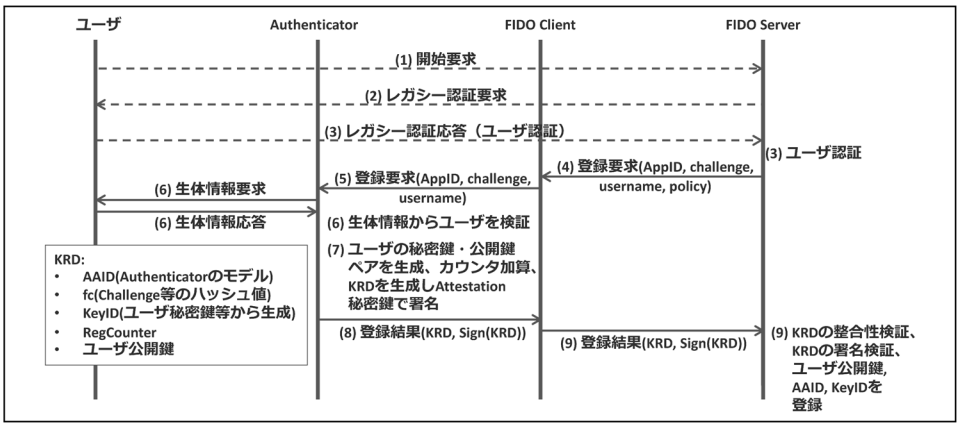
図表２　FIDO における主な構成要素

	要素名称	主な役割
	サーバ	
1	FIDO Server	Authenticator（後述）の登録を行うほか、ユーザからの検証結果を受け付け、ユーザ認証や取引認証を行うソフトウェア。
2	サーバソフト(*)	ユーザクライアントのアプリケーション（後述）に対してサービスを提供するソフトウェア。
	ユーザクライアント	
3	アプリケーション (*)	サービス提供者が作成する専用プログラムやウェブ・ブラウザ等、ユーザからの指示を受け付けるためのソフトウェア。
4	FIDO Client	FIDO Server と通信するソフトウェア。
5	ASM (Authenticator Specific Module)	FIDO Client と Authenticator（後述）間で統一的なインタフェースを提供するソフトウェア。
6	Authenticator	生体認証等の所定の認証手段を用いてユーザの検証を実施するモジュール。ユーザの検証の後、必要な情報に対するデジタル署名を生成するほか、登録フェーズ（後述）では、公開鍵と秘密鍵のペアを生成する。FIDO においてセキュリティ上の要となる要素。
7	生体情報リーダ(*)	ユーザからの生体情報の入力を受け付ける機器。
8	Matcher(*)	あらかじめ登録されたユーザの生体情報と、生体情報リーダによって取得された生体情報とを照合するモジュール。通常は、Authenticator に内包されている。
9	Secure Storage(*)	Authenticator が生成したユーザの秘密鍵や、生体情報を安全に保管するための領域。 Authenticator に内包される場合もある。

備考：「*」が付いている要素は、FIDO において仕様が規定されていないものの、実際にシステムを実装する際には必要となる要素である。

ユーザが実施する作業であり、FIDO Server がユーザクライアントの Authenticator の登録を行う。これにより、従前使用していた（ID・パスワード等の）認証情報と、FIDO で使用するユーザ情報（後述）を紐付ける。認証フェーズは、サービス

図表 3　登録フェーズにおけるフロー



の利用の度にユーザが実施する作業であり、FIDO Server がユーザ認証や取引認証を行う。

イ．登録フェーズにおけるフロー

登録フェーズにおけるフローの概要の一例を図表 3 に示す。ここでの前提として、現在は ID・パスワード等によるユーザ認証の仕組み（この認証を本稿では、FIDO における認証と区別するため「レガシー認証」と呼び、そのユーザ認証に必要となる認証情報を「レガシー認証情報」[1] と呼ぶ）が既に運用されている状態で、今次 FIDO を新たに導入するものとする。また、FIDO におけるユーザ認証の手段として生体認証を利用するものとする。なお、下記（1）～（3）は FIDO 仕様に規定されていないものであり（図表 3 中の点線部分）、ここではその一例を示す。

（1）ユーザは、アプリケーションを通じて利用を希望するサービスのサーバ（FIDO Server）に接続し、登録フェーズの開始を要求する。
（2）FIDO Server は、ユーザに対してレガシー認証での認証を要求する。
（3）ユーザは、レガシー認証情報を FIDO Server に応答する。FIDO Server は、その情報をもとにユーザ認証を行い、認証に成功すれば次のステップに移る。
（4）FIDO Server は、FIDO Client に対して登録要求を行う。登録要求は、AppID[2]、challenge[3]、username、policy[4] 等から成る。

1 現在のシステムにおいて、ユーザを認証するために ID・パスワードを利用した方式を使用している場合には、その ID・パスワードがレガシー認証情報となる。本稿ではレガシー認証情報は、FIDO の登録フェーズにのみ用いるものとし、後述する認証フェーズでは用いないものとする。
2 サービスを識別するための ID。
3 FIDO Server が生成する乱数。
4 ユーザクライアント側で満たすべき能力や仕様に関してサーバ側で定めた情報。

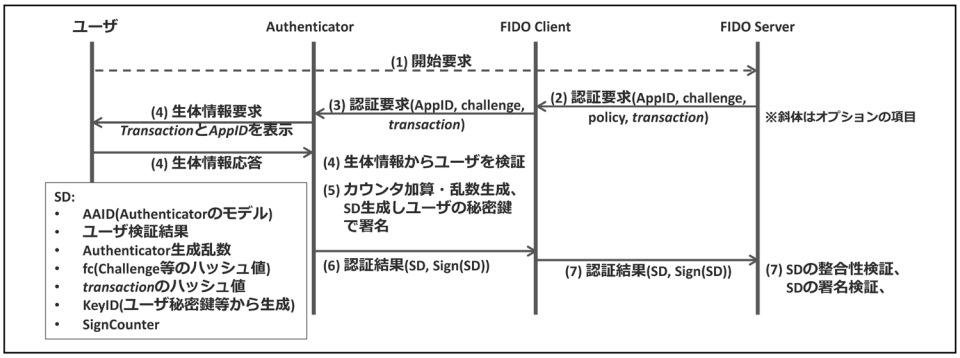
（5）FIDO Client は、policy を解釈し、取引を続行可能であると判断すれば、Authenticator に対して登録要求を行う。
（6）Authenticator は、ユーザに対して生体情報を要求し、ユーザは登録フェーズを続行するならば自らの生体情報を生体情報リーダに提示し Authenticator に送信する。Authenticator は、受信した生体情報と、既に登録済の生体情報[5] とを Matcher にて比較することによりユーザを検証する。
（7）Authenticator は、上記（6）でユーザ検証に成功すれば、①後の認証フェーズで使用するユーザの秘密鍵と公開鍵のペアを生成し、②必要なカウンタ値[6] の加算を行い、③ KRD（Key Registration Data）を生成し、Authenticator が所有する登録用秘密鍵（Attestation 秘密鍵）[7] によってデジタル署名を生成する。ユーザの秘密鍵は Secure Storage にて安全に保管される。KRD は、AAID[8]、fc[9]、KeyID[10]、RegCounter、ユーザの公開鍵等から成る。
（8）Authenticator は、デジタル署名付き KRD を登録結果として FIDO Client に返信する。
（9）FIDO Client は、デジタル署名付き KRD を登録結果として FIDO Server に返信する。FIDO Server は、①上記（4）で送信した登録要求の内容と受信した登録結果の内容との整合性を確認し、② KRD のデジタル署名を検証[11] し、③ KRD に含まれるユーザの公開鍵、AAID、KeyID を当該ユーザのものとして登録する（当該ユーザの Authenticator を登録することを意味している）。これにより、FIDO Server は、AAID と KeyID のペアを FIDO における「ユーザ情報」として、上記（3）で受信したレガシー認証情報と紐付けて管理する。

ロ．認証フェーズにおけるフロー

認証フェーズにおけるフローの概要の一例を図表 4 に示す。ここでの前提として、ユーザは既に登録フェーズを完了しているものとする。このため、レガシー認証情報は認証フェーズにおいては使用しない。なお、下記（1）は FIDO に規定されていないものであり（図表 4 中の点線部分）、ここではその一例を示す。

5 Authenticator に生体情報を登録していない場合には、生体情報を登録するプロセス（当該プロセスは FIDO には未規定）に移行する。ここでは、ユーザクライアントのロック解除等の目的で生体情報を Authenticator に登録済のものとして話をすすめる。
6 FIDO では、登録フェーズを行う度に加算される RegCounter と、認証フェーズを行う度に加算される SignCounter の 2 種類がある。
7 Attestation 秘密鍵は、FIDO 認定を受けた Authenticator とともにユーザクライアントの工場出荷時に埋め込まれるなどして配付され、Secure Storage にて安全に保管される。
8 Authenticator のモデル毎に固有に付与される ID。
9 AppID や challenge などをまとめた値に対するハッシュ値。
10 ユーザの秘密鍵、appID、username 等のセットに対して固有に付与される ID。
11 デジタル署名を検証するための Attestation 公開鍵は、「Metadata サービス」と呼ばれる方法で FIDO アライアンスから各 FIDO Server に配信される。

図表 4　認証フェーズにおけるフロー



（1）ユーザは、アプリケーションを通じて利用を希望するサービスのサーバ（FIDO Server）に接続し、認証フェーズの開始を要求する。このときに、取引内容[12]（transaction）も併せて送信する。

（2）FIDO Server は、FIDO Client に対して認証要求を行う。認証要求に際して、ユーザの認証に加えて、取引内容の確認を要求する場合（取引認証）には、取引内容（transaction）を含めることができる。その場合の認証要求は、AppID、challenge、policy、transaction 等から成る。

（3）FIDO Client は、policy を解釈し、取引を続行可能であると判断すれば、Authenticator に対して認証要求を行う。

（4）Authenticator は、ユーザに対して生体情報を要求し、ユーザは自らの生体情報を生体情報リーダに提示し Authenticator に送信する。ここで、取引内容（transaction）が通信に含まれている場合には、Authenticator は AppID と取引内容（transaction）を画面に表示し、ユーザはそれらを確認したうえで、取引を継続する意思を示すため、自らの生体情報を提示する。Authenticator は、受信した生体情報と、既に登録済の生体情報とを Matcher にて比較することによりユーザを検証する。

（5）Authenticator は、上記（4）でユーザ検証に成功すれば、①必要なカウンタ値の加算や乱数を生成し、② SD（Signed Data）を生成し、ユーザの秘密鍵にてデジタル署名を生成する。取引内容（transaction）が通信に含まれている場合の SD は、AAID、ユーザ検証結果、上記①で生成した乱数、fc、KeyID、SignCounter、transaction のハッシュ値等から成る。

（6）Authenticator は、デジタル署名付き SD を認証結果として FIDO Client に返信する。

（7）FIDO Client は、デジタル署名付き SD を認証結果として FIDO Server に返信す

12 インターネット・バンキングにおける振込み指図情報や、電子商取引における商品購入情報のこと。

る。FIDO Server は、①上記（2）で送信した認証要求の内容と受信した認証結果の内容との整合性を確認し、② SD のデジタル署名を検証する。それらに成功すれば、当該取引が正当なユーザからのものであるとみなし、認証を完了する。また、取引内容（transaction）が通信に含まれている場合に上記①②が成功すれば、ユーザの正当性に加えて、取引内容（transaction）が改ざんされておらず、ユーザの意思に基づいたものとみなす。この取引内容（transaction）を上記（4）でユーザが確認し、その結果を（7）で FIDO Server が検証する取引認証の仕組みを「Transaction Confirmation」と FIDO では呼んでいる。

3. 金融機関が FIDO を導入する際の留意点

本節では、金融機関が FIDO を活用したインターネット・バンキングのサービスを提供する際の安全性評価を実施し、そのうえで、金融機関が FIDO を活用する際の留意点を考察する。

（1） 安全性評価の前提

FIDO を活用したインターネット・バンキングにおける安全性評価を実施するにあたり、防御側・攻撃側それぞれに前提をおいて検討する。防御側の前提とは、想定するインターネット・バンキングやそのセキュリティ対策、ユーザクライアント環境や取引フローに関する想定である。また、攻撃側の前提とは、不正送金を実施することを目的とした攻撃者の攻撃手法や能力に関する想定である。

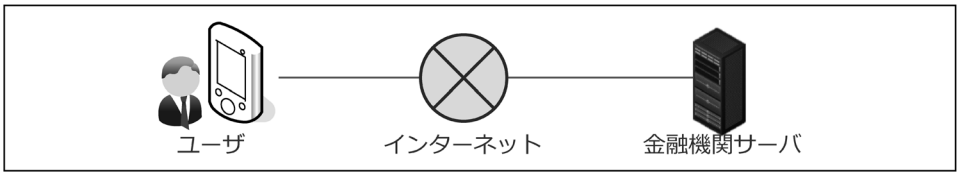
イ. 防御側の前提

FIDO を利用したインターネット・バンキングの構成については、FIDO をインターネット・バンキングのサービスに適用している事例（Bank of America [2015]）を一部参考に、以下の前提を置く。

- ユーザは所有する Android を OS とするスマートフォン[13]（以下、デバイスと呼ぶ）を利用し、金融機関が提供する Android 用アプリケーション（以下、バンキ

13 ここでは、後述する TEE（Trusted Execution Environment）の実装が進んでおり（GlobalPlatform [2015]）、今後インターネット・バンキングのプラットフォームとして普及が予想されるスマートフォンを想定することとし、PC を使った取引は本稿では取り扱わない。

図表 5　想定するインターネット・バンキングの構成



ング・アプリと呼ぶ）を使用することにより、インターネット回線を経由して金融機関サーバに接続することとする（図表 5）。

- ユーザは 1 種類のデバイスのみを FIDO のインターネット・バンキングの認証に使用する（例えば、スマートフォンと PC の両方を使用した取引は行わない）こととする。
- 金融機関サーバは堅牢に構築されているため攻撃者からの攻撃を受けないこととする。

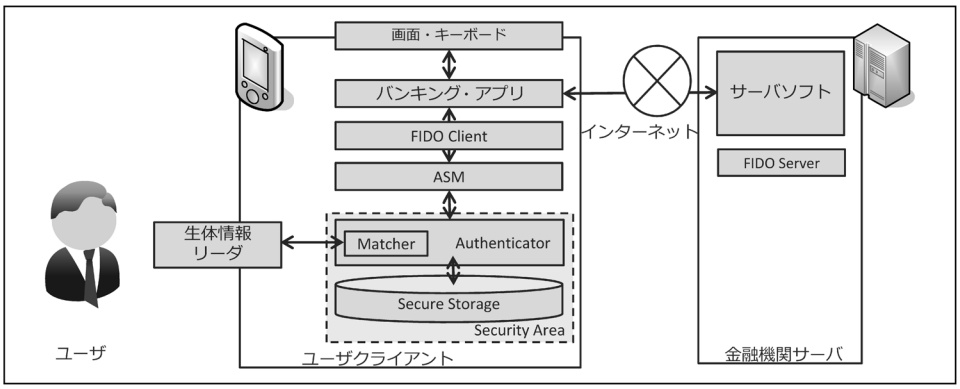
ユーザのデバイスについては、FIDO 対応デバイスを提供している事例（NTT DOCOMO, INC. [2015]）を一部参考に、以下の前提を置く（図表 6）。

- FIDO アライアンス認定を取得した Authenticator、ASM、FIDO Client がデバイスに既に導入されていることとする。Authenticator におけるユーザ認証の手段としては、生体認証（指紋認証もしくは虹彩認証）を利用することとする。
- ユーザの使用時以外はデバイスがロックされており、生体認証によるロック解除をしなければデバイスを使用できないこととする。また、ユーザ本人の生体情報のデバイスへの登録は済んでいることとする。
- デバイスはデバッグモードになっておらず、デバイスを PC に接続しても当該デバイスを操作できないこととする。
- Matcher、Authenticator、Secure Storage については、TEE 等、通常環境とは隔離された領域（以下、セキュリティ・エリア〈Security Area〉と呼ぶ）に配置されており、セキュリティ・エリア内においてはどのようなマルウエアでも活動できないこととする。
- デバイスは、後述する Trusted UI（Trusted User Interface）を備えていないこととする。

インターネット・バンキングのフローについては、2 節（2）の Transaction Confirmation を参考に以下の前提を置く。

（登録フェーズ）…デバイス毎・サービス毎（金融機関毎）に初回実施する。

図表 6　想定するアーキテクチャ



Step1. ユーザは、生体情報を提示し、デバイスのロックの解除を行ったうえで、バンキング・アプリを立ち上げる[14]。

Step2. ユーザは、レガシー認証情報[15]をバンキング・アプリを通じて金融機関サーバに提示する。金融機関サーバは、登録要求をデバイスに送信する。

Step3. ユーザは、生体情報を生体情報リーダに提示する。Authenticator はユーザの検証を行い、検証に成功すれば登録結果（デジタル署名付き KRD）を金融機関サーバに送信する。金融機関サーバは、登録結果の内容を検証し、問題が無ければレガシー認証情報と FIDO でのユーザ情報（AAID および KeyID）とを紐付けて管理する。

（認証フェーズ）…登録フェーズ終了後、各種取引操作の都度実施する。

Step1. 登録フェーズの Step1. と同様である。

Step2. ユーザは、バンキング・アプリを通じて取引内容（transaction）である振込み先や振込み金額情報等を、金融機関サーバに送信する。

Step3. 金融機関サーバは、取引内容（transaction）を含む認証要求をデバイスに送信する。ユーザは、画面に表示された取引内容（transaction）等を確認する[16]。

Step4. ユーザは、Step3 の結果、取引を継続したいと希望するときには自らの生体情報を生体情報リーダに提示する。Authenticator はユーザの検証を行い、検

14 バンキング・アプリについては、ログインに必要となる ID、パスワードの情報はアプリに保存してあるため、毎回ユーザが入力する必要が無いものとする。

15 レガシー認証情報は、振込み時に必要となる認証情報（ワンタイムパスワード等）を想定し、当該認証情報はワンタイムパスワード生成器等の専用機器で生成されるものとし、専用機器には攻撃者はアクセスできないものとする。

16 取引内容の確認においては、FIDO で規定されている Transaction Confirmation の仕組みを用いるものとする。「取引内容確認メッセージ」として、①利用金融機関名、②振込み先口座情報、③振込み金額情報、④振込み日時等が表示されるものとする。

図表 7　攻撃者のデバイスへのアクセス方法の違いによる場合分け

攻撃者がデバイスへアクセスする方法
ケース A：物理アクセス（ネットワーク経由でのアクセスが困難であり、物理的なアクセスに限定される場合） 攻撃例：攻撃者が、ユーザのデバイスを盗取し、デバイスロックの解除を試み、デバイスの操作を行う。
ケース B：ネットワークアクセス（物理的なアクセスが困難であり、ネットワーク経由でのアクセスに限定される場合） 攻撃例：攻撃者がユーザのデバイスに対してマルウエアを感染させ、ネットワーク経由で攻撃を実施する。

証に成功すれば認証結果（デジタル署名付き SD）を金融機関サーバに送信する。金融機関サーバは、認証結果の内容を検証し、問題がなければ当該取引を実行する。

ロ．攻撃側の前提

攻撃者がユーザのデバイスにアクセスする方法によって場合分けを行う（図表 7）。また、攻撃手法として、インターネット・バンキングにおける不正送金の 2 大手口（警察庁［2013］）である「フィッシングによる手口」と「マルウエアによる手口」に加えて、デバイスへの物理アクセスが可能になった時にデバイスをロック解除されるといった「生体認証でのなりすまし」についても想定する。

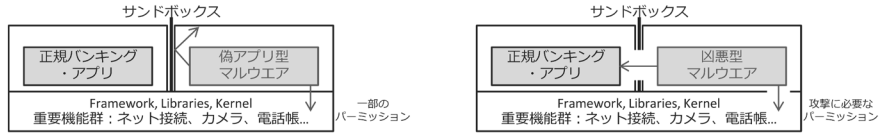
（手口 1：フィッシングによる手口・攻撃者の前提）

- 攻撃者は、金融機関のサイトを模した偽のサイト（以下、フィッシングサイトと呼ぶ）を構築し、当該サイトに接続してきたユーザから受信した情報を盗取できることとする[17]。また攻撃者は、盗取した情報をなりすましの手段として使用することができることとする。

17 ユーザが、自らのデバイスを使ってフィッシングサイトにアクセスすることを想定するものであり、図表 7 の「ケース B：ネットワークアクセス」を想定した攻撃手法である。また、フィッシングサイトに接続してきたユーザから生体情報を盗取する攻撃も考えられるが、正規の FIDO における仕組みでは生体情報をサーバに送信することは無く、当該攻撃が起こりうる可能性が高いのはマルウエアが介在する場合であるため、当該攻撃は後述の（手口 2）に分類する。

図表 8　マルウエアの能力による場合分け

マルウエアの種類	マルウエアの能力
偽アプリ型	正規のバンキング･アプリとは別のアプリとして独立して存在し[18]、サンドボックス[19]により、正規のバンキング･アプリで扱うファイル・メモリや前述のセキュリティ・エリアにアクセスできないものの、最低限のパーミッション[20]はユーザにより許可されているものとする。
凶悪型	サンドボックスを回避し、正規のバンキング･アプリが扱うファイル・メモリにアクセス可能であり、攻撃に必要なパーミッションを持つほか、任意のコードの実行が可能[21]。ただし、セキュリティ･エリアに対しては当該能力が無いものとする。



（手口 2：マルウエアによる手口・攻撃者の前提）

- 攻撃者は、金融機関サーバをマルウエア感染させることはできない一方で、ユーザのデバイスに対してマルウエア感染させることができることとする[22]。こうしたマルウエアの能力によって場合分けを行う（図表 8）。

（手口 3：生体認証でのなりすまし・攻撃者の前提）

- 攻撃者は、生体情報リーダに何らかの情報を提示することによってユーザになりすます攻撃[23]を実施できることとする。

攻撃側の前提のまとめとして、ケース A、B および、手口 1～3 の関係をまとめると図表 9 の通りとなる。

18 正規のバンキング・アプリ等を再パッケージ（Repackaging）し海賊版として配布するタイプのマルウエアを想定する（大居［2013］）。

19 Android 等において備わっている、アプリケーションやそれが扱うデータを論理的に隔離するセキュリティ上の機能。

20 アプリケーションが、デバイスの重要な機能群（カメラ、電話帳等）にアクセスを許可されること。

21 具体例としては、①マルウエアがルート権限を奪取する場合や、②正規のバンキング・アプリの開発環境が汚染されており、同アプリに不正コードが仕込まれている場合等が挙げられる。上記①については、ルート権限を奪取する Android マルウエアの存在が報告されている（Zhou and Jiang [2012]）。上記②については、実際に iPhone の開発環境である Xcode が改ざんされ、それが第三者により配付されたことにより、当該開発環境で作成されたアプリケーションに不正なコードが埋め込まれた事例（XCodeGhost）が報告されている（Xiao [2015]）。

22 攻撃者がネットワーク経由でユーザのデバイスに対してマルウエア感染させることを想定するため、前述の「ケース B：ネットワークアクセス」を想定した攻撃手法となる。

23 攻撃者がユーザになりすます方法の詳細は 3 節（3）ニ．で説明する。攻撃者が、ユーザのデバイスに対して、何らかの情報を提示することを想定するため、図表 7 の「ケース A：物理アクセス」を想定した攻撃方法となる。また、マルウエアによる生体情報の盗取等は、マルウエアによる手口（手口 2）に分類する。

図表 9　攻撃の前提におけるケース A、B および手口 1～3 の関係

	手口 1：フィッシング	手口 2：マルウエア	手口 3：生体認証でのなりすまし
ケース A：物理アクセス	想定しない	想定しない	想定する
ケース B：ネットワークアクセス	想定する	想定する	想定しない

図表 10　インターネット・バンキングのフロー毎の攻撃成功の定義

フェーズ	攻撃成功の定義
登録フェーズ	攻撃者が、利用可能な生体情報（攻撃者自身の生体情報や、攻撃者が盗取したユーザの生体情報）をユーザのレガシー認証情報と紐付けて、攻撃者のアクセス可能なデバイスで登録に成功すること。
認証フェーズ	攻撃者が、ユーザの意思に反して攻撃者の口座に不正送金を実施すること。 ※なお、登録フェーズにおいて攻撃が成功すれば、攻撃者が利用可能な生体情報と攻撃者のデバイスを使って認証フェーズにて自由な振込みができるため、攻撃が成功することとなる。

ハ．攻撃成功の定義

攻撃成功とは、不正送金を成功させることとし、フェーズ毎に分解すると、図表 10 のいずれかの攻撃に成功することと定義する。

(2)　安全性評価

本節（1）の前提をもとに、FIDO を活用したインターネット・バンキングにおける安全性評価を実施する。

イ．登録フェーズにおける攻撃

登録フェーズにおいて、ケース毎および攻撃手口毎の攻撃の成否について評価すると図表 11 の通りとなる。なお、攻撃が成功する具体的なシナリオおよび分析手法については、補論 2 に記載する。また、攻撃が成立する場合において、その対策手法に関する考察は、本節（3）にて述べる。

ロ．認証フェーズにおける攻撃

認証フェーズにおいて、ケース毎および攻撃手口毎の攻撃の成否について評価すると図表 12 の通りとなる。なお、攻撃が成功する場合の具体的なシナリオおよび分析手法については、補論 2 に記載する。また、攻撃が成立する場合において、その対策手法に関する考察は、本節（3）にて述べる。

図表 11　ケース毎、手口毎の攻撃成否に関する評価（登録フェーズ）

アクセス方法 / 攻撃の手口		ケースA：物理アクセス	ケースB：ネットワークアクセス
手口1：フィッシング		—	攻撃成立
手口2：マルウエア	偽アプリ型	—	攻撃成立
	凶悪型	—	攻撃成立
手口3：生体認証でのなりすまし		攻撃不成立	—

図表 12　ケース毎、手口毎の攻撃成否に関する評価（認証フェーズ）

アクセス方法 / 攻撃の手口		ケースA：物理アクセス	ケースB：ネットワークアクセス
手口1：フィッシング		—	攻撃不成立
手口2：マルウエア	偽アプリ型	—	攻撃不成立
	凶悪型	—	攻撃成立
手口3：生体認証でのなりすまし		攻撃成立	—

（3）　金融機関の FIDO 導入にかかる留意点

前述した安全性評価（図表 11、図表 12）に関していくつか特徴的な点を抽出し、金融機関が FIDO を導入する際の留意点を考察すると以下の通りである。

イ．登録フェーズのレガシー認証情報について（ネットワークアクセス）

登録フェーズにおいては、レガシー認証情報が金融機関サーバに送られるが、これはリスクを伴う作業である。攻撃者がユーザのレガシー認証情報を盗取することが可能であれば、盗取した情報を使って攻撃者自身のデバイスで登録フェーズを実施し、ユーザの口座をコントロールできてしまうからである。

「ケースB：ネットワークアクセス（攻撃者がユーザのデバイスに対してネットワーク経由でのアクセスを行う場合）」において、攻撃者がレガシー認証情報を盗取する方法としては、①フィッシングサイトに誘導させ、ユーザを騙してレガシー認証情報を盗取する方法、②凶悪型マルウエアを通じて、ユーザが正規バンキング・アプリに入力したレガシー認証情報を攻撃者が盗取する方法、③偽アプリ型マルウエアをユーザにインストールさせたうえで、当該アプリに対してレガシー認証情報を入力させ盗取する方法、の 3 つが考えられる。その結果として、攻撃者が自身のデバイスを使用し、盗取したレガシー認証情報を使うことにより登録フェーズが不正に行われる。

このようなレガシー認証情報の盗取の多くは、FIDO 自体に問題があるというよ

りは、FIDO に移行する前段階でレガシー認証方式を使っていることに起因する問題である。レガシー認証情報を盗取されないようにすることが、登録フェーズにおけるセキュリティ対策のポイントとなる。

このため、金融機関における留意点としては、以下の事項が考えられる。

(1) ユーザに対して、「レガシー認証情報を正規の金融機関サイト以外で入力しない」旨の注意喚起を行うこと（上記①対策）
(2) ユーザに対して、「凶悪型マルウエア感染の原因である OS の脆弱性に対処するため、デバイスの OS を常に最新の状態で使用する」旨の注意喚起を行うこと（上記②対策）
(3) ユーザに対して、「アプリのインストール時に、許可するパーミッションをよく吟味する」旨の注意喚起を行うこと（上記②対策）
(4) 作成する正規バンキング・アプリに脆弱性が無いように十分なテストを実施することや、アプリ開発環境が信頼できることを確認すること（上記②対策）
(5) ユーザに対して、偽アプリをインストールすることが無いように、正規アプリのインストール方法[24] を分かりやすく示すこと（上記③対策）
(6) アプリストアに偽アプリが出現していないかどうか監視すること（上記③対策）
(7) レガシー認証情報を使用せずに登録フェーズを実施する方式[25] を検討すること（上記①②③対策）
(8) 普段から、ユーザのデバイスを認証しておき、普段とは異なるデバイスからの登録フェーズは認めない（一定の利用実績のあるデバイスからのみ登録フェーズを認める）仕組みとすること

ロ. 登録フェーズのレガシー認証情報について（物理アクセス）

「ケース A：物理アクセス（攻撃者がユーザのデバイスに対して物理的なアクセスを行う場合）」において、攻撃者がレガシー認証情報を盗取する方法は特に見当たらない。本安全性評価では、攻撃者がユーザのデバイスに物理的アクセスができたとしても、レガシー認証情報となるワンタイムパスワード等を生成するための専

24 具体的には、バンキング・アプリのインストール時には、①正規の金融機関のウェブ・サイトからのリンクを辿って公式アプリストアに行き、②公式アプリストアにおけるアプリケーション作成者情報を確認しインストールすることや、③公式アプリストア以外からアプリケーションをインストールしないような設定をデバイスにしておくこと、が挙げられる。

25 例えば次のような方法が考えられる。金融機関の窓口等で（行員による本人確認が行われた）ユーザが登録フェーズの一部（図表 3 の(1)および(4)～(9)）を実施し、FIDO Server において登録される「FIDO におけるユーザ情報」（AAID および KeyID のペア）をユーザが認識できるようにしておく。金融機関の窓口端末（安全な端末）にて「FIDO におけるユーザ情報」と「ユーザの口座情報」とを紐付ける作業を実施する。

用機器（脚注 15 を参照）にはアクセスできないという前提を置いたためである。前提とは異なるものの、仮に、レガシー認証情報となるワンタイムパスワード等がスマートフォンで生成・保存される場合には、攻撃者は、生体認証でのなりすまし（手口 3）等により、レガシー認証情報を盗取する可能性がある。このため、金融機関における対策・留意点としては、「ワンタイムパスワード等のレガシー認証情報は、登録フェーズで使用するデバイス（スマートフォン等）で生成・保存しないこと」が考えられる。

ハ．認証フェーズのマルウエア攻撃について

デバイス上のマルウエアは「ケース B：ネットワークアクセス（攻撃者がユーザのデバイスに対してネットワーク経由でのアクセスを行う場合）」において大きな脅威となりうる。認証フェーズにおいては、マルウエアにより、MitB 攻撃に類似した形でユーザの意図せざる取引が行われる可能性がある。その具体的な方法を検討するために、Transaction Confirmation における攻撃の一例を整理すると、攻撃者は（A）取引内容（振込み先と金額情報）を改ざん（例：「A さんに 1 万円振込み」を「X さんに 100 万円振込み」と改ざん）して金融機関サーバに送信できること、（B）ユーザが確認する取引内容確認メッセージを改ざんできること（例：「X さんに 100 万円振込み」との表示を「A さんに 1 万円振込み」との表示に改ざん）、の 2 点が必要となる。

上記（A）に関しては、凶悪型マルウエアであれば、同マルウエアが正規バンキング・アプリのメモリ情報を書き換えるなどして（株式会社 FFRI［2012］）、ユーザが正規バンキング・アプリに入力した取引内容を改ざんし、その内容を金融機関サーバへ送信可能となる。

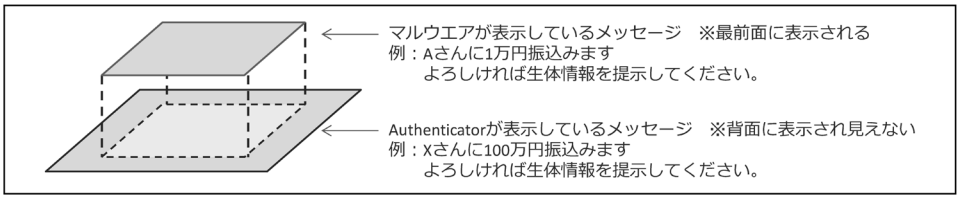
上記（B）に関しては、「ディスプレイ・オーバーレイ（Display Overlay）攻撃[26]」（FIDO Alliance [2014]）により取引内容をユーザが正しく確認できなくなる可能性がある。ディスプレイ・オーバーレイ攻撃は、Authenticator が表示している取引内容確認メッセージの上に、マルウエアが表示したメッセージを覆い[27] ユーザに偽の取引内容確認メッセージを見せる攻撃である（図表 13 を参照）。こうすることによりユーザは背面の Authenticator が表示したメッセージ（例：X さんに 100 万円振込み）が見えなくなり、取引の改ざんに気付くことができなくなる。

このため、金融機関における対策・留意点としては、本節（3）イ．で述べた（2）～

26 本攻撃手法は、ウェブページ上でリンクやボタン等を偽装・隠ぺいしてクリックを誘う攻撃である「クリックジャック攻撃」（Huang *et al.* [2012]）の 1 つの応用例であり、より一般的には「UI リドレッシング攻撃（Redressing Attacks）」（Niemietz and Schwenk [2012]）と呼ばれている。

27 Android における「toast」の仕組みや、「WindowManager」における優先度の悪用により、マルウエアの表示する通知メッセージが最前面に描画される可能性がある（Richardson [2010]、Niemietz and Schwenk [2012]、Android Developers [2016a]）。

図表 13　ディスプレイ・オーバーレイ攻撃が起こる仕組み



（6）と同様に、ユーザのデバイスのマルウエア対策のほか、以下の対策が考えられる。

ディスプレイ・オーバーレイ攻撃への対策として、マルウエア感染しても画面の表示内容が信頼できるものであることを確保する仕組みの導入[28]が考えられる。これを実現する方法として 3 種類紹介する。1 つ目の方法としては、本節（1）イ．で述べた防御側の前提とは異なるものの、取引内容確認を「別の専用デバイス」で実施するということが考えられる。「別の専用デバイス」がマルウエア感染しない限り、ユーザは取引内容を正しく確認することができる[29]。

2 つ目の方法としては、バンキング・アプリの実装において、ディスプレイ・オーバーレイ攻撃を検知する仕組みを導入することが考えられる。Android には OS の標準機能として、ユーザが（画面上を）タッチした場所に対して、他のメッセージが上から覆い被さっていないかを判別する機能[30]がある。この機能を利用して、バンキング・アプリの取引内容確認メッセージにおいて、振込み先や振込み金額が記されている部分をユーザにタッチしてもらい、当該部分に他のメッセージが覆い被さっていないかを確認するということが考えられる。もっとも、凶悪型マルウエアによる攻撃の場合には、メッセージが覆い被さっているかを判定するフラグが使用するメモリ領域を、マルウエアにより書き換えられ、判定結果が改ざんされる可能性があり、完全な対策ではない点には留意が必要である。

3 つ目の方法として、デバイスの Trusted UI を活用するという方法がある（Global-Platform [2013]）。Trusted UI を備えたデバイスであれば、画面表示機能がセキュリティ・エリアの管理下に置かれ、通常環境から隔離・保護されるため、ディスプレイ・オーバーレイ攻撃の影響を受けないとされている（Coombs [2015]）。筆者たちが調べる限り、一部のスマートフォンでは Trusted UI の装備が報じられている（Dyke [2015]）。なお、FIDO では、金融機関サーバが、Authenticator において

28 より正確に言えば「ユーザが画面を通じて確認した取引内容（transaction）と Authenticator がデジタル署名した取引内容（transaction）とが同一であることを担保する仕組み」を導入したうえで、「ユーザが取引継続の意思を持ったときにのみデジタル署名が行われること」が必要と言える。

29 ただし、取引の意思（取引続行もしくは取引中止）を別の専用デバイスに入力し、当該情報を安全に金融機関サーバに送信する必要がある。

30 例えば、Android の「MotionEvent」の仕組みにおいて、「FLAG_WINDOW_IS_OBSCURED」というフラグが存在する（Android Developers [2016b]）。

Trusted UI が使用可能かどうかを確認できる仕組みがある[31]。

このため、金融機関における留意点としては、以下の事項が考えられる。

（1）Trusted UI の今後の実装動向について留意すること
（2）認証フェーズにおいて、ユーザの Authenticator が Trusted UI を利用可能でないと認識した場合には、その認証フェーズがリスクの高い取引になる可能性を認識すること

ニ．生体認証でのなりすましについて

攻撃者がユーザのデバイスを盗取した場合など、「ケース A：物理アクセス（攻撃者がユーザのデバイスに対して物理的なアクセスを行う場合）」においては、生体認証でのなりすましのリスクも意識する必要がある。生体認証として指紋認証を利用している場合を例にとると、次のような 3 種類の攻撃方法が考えられる。（イ）攻撃者が（システムが誤認することを期待して）自らの指紋を提示する方法、（ロ）攻撃者がユーザの指紋等を何らかの方法で盗取し、それに模した人工物を生体情報リーダに提示する方法[32]、（ハ）攻撃者がユーザの意図に反してユーザに指紋を提示させる方法[33]、などが考えられる。特に、認証フェーズにおいては、攻撃者に生体認証でのなりすましが行われてしまうと、端末のロック解除から取引内容の確認まで攻撃に必要なことが全て実施されてしまうため、大きな問題となりうる。

上記（ハ）については、技術的に解決することが容易ではないと考えられる。上記（イ）（ロ）に関しては、「ユーザクライアント側にて個人が検証され、その結果をサーバ側が信頼する」という FIDO のモデル固有の問題点と、「ユーザクライアントにおける生体認証でのなりすましの検知精度」の問題点に分けて考えることができる。

前者の「FIDO のモデル固有の問題点」に対処すべく、FIDO においては、ユーザクライアントの検証結果が改ざんされることへの対策や、Authenticator が不正なものに入れ替えられることへの対策を行っている（補論 1（1）を参照）。もっとも、「FIDO アライアンス認定を取得した Authenticator か否かを金融機関サーバにて確認する仕組み」については、FIDO アライアンスは、FAR や APCER 等のセキュリ

31 Metadata サービスを通じて、金融機関サーバが Authenticator 毎（AAID 毎）にそれぞれ Trusted UI が利用可能かを確認できる。また、各認証フェーズにおける通信において、ユーザクライアントから金融機関サーバに AAID がデジタル署名付きで送信される。金融機関サーバは、AAID をキーにして「当該取引で使用されている Authenticator が Trusted UI を利用可か否か」を確認することができる。

32 実際に当該方法で iPhone の生体認証の突破に成功したと主張している団体がある（Chaos Computer Club [2013]）。

33 例えば、ユーザが眠っている間に、攻撃者がユーザの指をユーザのデバイスの生体情報リーダに押し付ける方法が考えられる。

ティ評価指標[34]を検査しているわけではなく、基本的にはFIDOのプロトコルに則ってサーバ・クライアント間で通信ができるかを確認しているに過ぎない点には留意が必要である。

後者の「ユーザクライアントにおける生体認証でのなりすましの検知精度」の問題点に対処すべく、FIDOにおいては、金融機関サーバがMetadataサービスを通じて、Authenticator毎の一部のセキュリティ評価指標（FAR等）を確認することが可能である。もっとも、それらの評価指標にかかる情報は、基本的にはAuthenticatorベンダーの自己評価値であり、FIDOアライアンスが評価したわけではない点には留意が必要である。このため、コモン・クライテリア（ISO/IEC 15408）等により第三者評価されたAuthenticatorを使用することや、第三者評価されたセキュリティ評価指標を金融機関が把握することが重要となる。

一般に、生体認証のセンサーに何らかの情報を提示してなりすましを試みる攻撃は、「プレゼンテーション攻撃」と呼ばれ、その評価については国際標準案（ISO/IEC 30107シリーズ）において標準化の作業が行われている（新崎［2015］、宇根［2016］）。また、生体認証システムのセキュリティ評価に必要なセキュリティ機能要件等を規定する国際標準案（ISO/IEC 19989）が審議されている（山田［2015］、宇根［2016］）。今後、Authenticatorにかかる第三者評価が活用されることにより、金融機関が「ユーザクライアントにおける生体認証でのなりすましの検知精度の問題点」に対処可能となる可能性がある。

このため、金融機関における対策・留意点としては、以下の事項が考えられる。

（1）FIDOアライアンスによるAuthenticatorの認定はセキュリティ評価指標への認定ではないことを認識すること
（2）Authenticatorがコモン・クライテリア等の第三者評価を受けたものか調査しておくこと
（3）第三者によって評価されたものである場合には、Authenticatorのセキュリティ評価指標[35]を当該取引のリスクと紐付けることが可能となることを認識すること（例えば、FARが高いAuthenticatorからの取引は、FARが低いものからの取引よりもリスクが高いなど）
（4）デバイスの盗難の届出がユーザからあった場合には直ちに当該デバイスの取引

34 FAR（False Accept Rate）は他人を本人と誤って判定する確率であるほか、APCER（Attack Presentation Classification Error Rate）は人工物が提示された際に「人間の身体の一部が提示された」と誤って判定する確率である。

35 FIDOにおいては、登録フェーズ、認証フェーズともに、ユーザクライアントから金融機関サーバに対してAAIDがデジタル署名付きで送信される。金融機関は、AAIDを確認することにより当該通信におけるAuthenticatorのベンダ名とモデル名が確認できる。上記（2）のように金融機関がAuthenticatorのセキュリティ評価指標をあらかじめ調査しておけば、AAIDをキーにして「当該取引で使用されているAuthenticatorのセキュリティ評価指標」を確認することができる。

を中止すること
(5) ユーザの意図に反して生体情報が提示されることを想定し、振込み先情報、振込み時刻等を利用した、振込み操作の異常を検知する技術（以下、異常検知技術という）を導入すること

ホ．生体情報のリプレイ攻撃リスクについて

凶悪型マルウエアに感染したデバイスにおいては、生体情報のリプレイ攻撃リスクが存在する。提示されたユーザの生体情報をマルウエアが、生体情報リーダとMatcher 間（補論 2 の図表 A-1 の④を参照）において盗取し、それを再送（リプレイ）することにより生体認証を突破できる可能性があり、ユーザの意思に反して、生体認証やその後続手続きである取引承認のデジタル署名が行われてしまう可能性がある。本インターネット・バンキングのシステムにおける盗取に限らず、他のシステムにおいて生体情報を盗取されたとしても、原理的には本インターネット・バンキングにおいて攻撃が成立する。これらの攻撃は、生体情報リーダおよび当該リーダと Matcher 間の通信経路がセキュリティ・エリア内に無いことに起因する。

このため、金融機関における対策・留意点としては、本節（3）イ．で述べた凶悪型のマルウエア対策に加えて、以下の事項が考えられる。

(1) ユーザのデバイス（Authenticator）における内部構造を調査し、生体情報リーダに加えて、当該リーダと Matcher 間の通信経路がセキュリティ・エリア内にあるか無いかを調査しておくこと[36]
(2) 仮にセキュリティ・エリア内に無い場合には、当該取引はリスクが高くなる可能性を認識しておくこと

ヘ．振込み限度額のリスク管理について

以上のように、FIDO の仕組みにおいては、生体認証でのなりすましの脅威があるほか、従来のインターネット・バンキングと同様に、マルウエアの脅威が大きいものとなる。マルウエアや生体認証でのなりすましへの留意点は前述の通りであるが、これらのリスクをゼロにすることは難しいと考えられる。万が一攻撃を受けたときの被害を軽減する策や、取引の異常を検知する技術も重要になると考えられる。

このため、金融機関における対策・留意点としては、以下の事項が考えられる。

36 なお、FIDO の Metadata サービスにより、各 Authenticator の Matcher がセキュリティ・エリア内に存在するか否かを金融機関は確認することができる。ただし、Metadata サービスでは、生体情報リーダおよび当該リーダと Matcher 間の通信経路に関して確認する方法は無い。

（1）ユーザが高リスクのサービス（例：新規振込み先への振込み操作）を利用する場合には、従来のインターネット・バンキングと同様に、振込み限度額を設定しておくこと
（2）振込み先情報、振込み金額等を利用した、振込み操作の異常検知技術を導入すること
（3）当該異常検知技術を導入する際のリスク値を算出する際に、a）デバイスの種類（OS の種類）によるマルウエア感染リスクの違いや、b）第三者によって評価された Authenticator のセキュリティ・レベル評価指標（FAR や APCER 等）や、c）デバイスの生体情報リーダ自身および当該リーダと Matcher 間の通信経路がセキュリティ・エリア内にあるか否かの情報、d）デバイスで Trusted UI が使用可か否かの情報を利用することができる点に留意すること

4. まとめ

本稿では、まず FIDO における登録フェーズおよび認証フェーズにおけるフローの解説を行った。次に、FIDO における Transaction Confirmation の仕組みを、スマートフォンを使ったインターネット・バンキングに適用した場合において、攻撃側・防御側の前提条件を置いたうえで、安全性評価を実施した。攻撃者の手口として 3 種類（フィッシング、マルウエア、生体認証でのなりすまし）を想定し、攻撃者がユーザのデバイスに物理的にアクセスする場合とネットワークアクセスする場合とに分け、それぞれの場合で攻撃の可否を評価した。

そうした評価を踏まえ、金融機関が FIDO を導入する際の留意点について考察した。特に重要な点を要約すると、①登録フェーズにおけるレガシー認証情報が盗取されることについて十分注意すること、②従来のインターネット・バンキングと同様に、マルウエアの脅威に対して引き続き注意する必要があること、③生体認証でのなりすましも脅威となりうること、④第三者により評価された Authenticator のセキュリティ・レベルや評価指標等を有効に活用すること、⑤デバイスのセキュリティ対策（Trusted UI や、生体情報リーダがセキュリティ・エリア内にあるか否か等）に関する情報の収集を行い、異常検知技術に活用することが挙げられる。

今後、上記④については、Authenticator の第三者評価・認証の取得や、上記⑤については、Trusted UI 搭載デバイスの普及が求められよう。ただ、このような課題があるものの、FIDO は EC サイトにおける決済やインターネット上の各種サービスにおけるログインに広く活用されることを想定して策定されているものであり、FIDO アライアンスの加盟メンバー数が年々増加している状況に鑑みると、そうした課題の解決とともに、FIDO が、ネットワーク越しの生体認証等のデファクト標

準になる可能性がある。現在はその移行期にあるとも考えられる。

インターネット・バンキングにおける不正事件の手口は日々巧妙化している。また、FIDO に関しても、FIDO 2.0 の策定に向けた動きがあるが（FIDO Alliance [2015b]、近藤［2015］）、最新の方式だけにその動向には留意が必要である。このように、インターネット・バンキングの不正送金事例に関する国内外の動向や学界の動向に注視しつつ、次世代認証技術の 1 つである FIDO の動向に注意しながら、金融機関におけるインターネット・バンキングの将来像を考えることが今後重要になると考えられる。

参考文献

宇根正志、「生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて」、『金融研究』第 35 巻第 4 号、日本銀行金融研究所、2016 年、55～90 頁（本号所収）

大居司、「Android プラットフォームの基本的なセキュリティ機構」、『Android セキュリティ・バイブル 2013』、日経エレクトロニクス/日経コミュニケーション編、2013 年

大日向隆之、「オンラインバンキング不正送金の手口と対策」、日本銀行金融研究所第 16 回情報セキュリティ・シンポジウム講演資料、2015 年（http://www.imes.boj.or.jp/citecs/symp/16/ref4_oohinata.pdf）

株式会社 FFRI、「Man in the Browser in Android の可能性」、FFRI Monthly Research、2012 年（http://www.ffri.jp/assets/files/monthly_research/MR201212_Man_in_the_Browser_in_Android.pdf）

警察庁、「不正送金及び不正アクセス等の被害について」、警察庁フィッシング対策セミナー資料、2013 年（https://www.antiphishing.jp/news/pdf/apcseminar2013npa.pdf）

近藤裕介、「次世代認証プロトコル FIDO の動向」、Yahoo! JAPAN Tech Blog、2015 年（http://techblog.yahoo.co.jp/security/fido-introduction/）

新崎卓、「SC37 Biometrics 標準化報告 WG3 Biometric Data interchange Formats」、JAISA バイオ関係標準化セミナー資料、日本自動認識システム協会、2015 年

瀬戸洋一、「ビッグデータ時代のバイオメトリクスにおけるプライバシー保護」、『最新自動認識技術 2015（月刊自動認識 2015 年 9 月増刊号）』、日本工業出版、2015 年

タオソフトウェア株式会社、『Android Security 安全なアプリケーションを作成するために』、株式会社インプレスジャパン、2012 年

竹森敬祐、「スマートフォンのセキュリティ」、日本銀行金融研究所第 13 回情報セキュリティ・シンポジウム講演資料、2011 年（http://www.imes.boj.or.jp/citecs/symp/13/ref2_takemori.pdf）

独立行政法人情報処理推進機構・一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center : JPCERT/CC）、「STOP!! パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」、JPCERT/CC、2014 年（https://www.jpcert.or.jp/pr/2014/pr140004.html）

山田朝彦、「SC27（情報セキュリティ）におけるバイオメトリクス関係プロジェクト」、JAISA バイオ関係標準化セミナー資料、日本自動認識システム協会、2015 年

NTT ドコモ、「『FIDO Alliance』に加入―生体情報を使った新しいオンライン認証を提供開始―」、NTT ドコモ報道発表資料、2015 年（https://www.nttdocomo.co.jp/

info/news_release/2015/05/26_00.html）
Android Developers, “WindowManager.LayoutParams,” Android Developers, 2016a (http://developer.android.com/reference/android/view/WindowManager.LayoutParams.html).
————, “MotionEvent,” Android Developers, 2016b (http://developer.android.com/reference/android/view/MotionEvent.html).
Bank of America, “Bank of America Introduces Fingerprint and Touch ID Sign-in for Its Mobile Banking App,” Bank of America Newsroom, September 15, 2015 (http://newsroom.bankofamerica.com/press-releases/consumer-banking/bank-america-introduces-fingerprint-and-touch-id-sign-its-mobile-ban).
Chaos Computer Club, “Chaos Computer Club breaks Apple TouchID,” September 21, 2013.
Coombs, Rob, “Securing the Future of Authentication with ARM TrustZone-based Trusted Execution Environment and Fast Identity Online (FIDO),” ARM White Paper, 2015 (https://www.arm.com/files/pdf/TrustZone-and-FIDO-white-paper.pdf).
Dyke, Rob, “The Benefits of Trusted User Interface,” Trustonic Blog, September 2, 2015 (https://www.trustonic.com/news-events/blog/benefits-trusted-user-interface).
FIDO Alliance, “FIDO UAF Complete Specifications,” FIDO Alliance, 2014 (https://fidoalliance.org/specifications/download/).
————, “Members: Bringing together an ecosystem,” FIDO Alliance, 2015a (https://fidoalliance.org/membership/members/).
————, “FIDO Authentication Poised for Continued Growth as Alliance Submits FIDO 2.0 Web API to W3C,” FIDO Alliance, 2015b.
GlobalPlatform, “GlobalPlatform Device Technology Trusted User Interface API Version1.0,” GlobalPlatform Device Specifications, 2013 (http://www.globalplatform.org/specificationsdevice.asp).
————, “The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market ,” GlobalPlatform White Paper, 2015.
Huang, Lin-Shung, Alex Moshchuk, Helen Jiahe Wang, Stuart Schechter, and Collin Jackson, “Clickjacking: Attacks and Defenses,” *Proceedings of 21st USENIX Security Symposium*, 2012.
Niemietz, Marcus, and Jorg Schwenk, “UI Redressing Attacks on Android Devices,” Blackhat ABU DHABI 2012, 2012.
NTT DOCOMO, INC., “FIDO Alliance Seminar in D. C. Case Study: NTT DOCOMO,” FIDO Seminar in D. C., 2015 (https://fidoalliance.org/wp-content/uploads/NTT_DOCOMO_case_study_FIDO-Seminar-DC_10_05_15.pdf).
Ratha, Nalini K, Jonathan H. Connell, and Ruud M. Bolle, “Enhancing security and privacy

in biometrics-based authentication systems," *IBM Systems Journal*, Vol. 40, No. 3, 2001, pp. 614–634.

Richardson, David, "Tapjacking," Lookout Mobile Security Blog, December 6, 2010 (https://blog.lookout.com/look-10-007-tapjacking).

Xiao, Claud, "Novel Malware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store," paloalto networks blog, September 17, 2015.

Zhou, Yajin, and Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," *Proceedings of IEEE Symposium on Security and Privacy*, 2012, pp. 95–109.

補論 1.　FIDO における特徴

ここでは、FIDO における以下の 2 点の特徴について詳しく説明する。

- ユーザのプライバシーに配慮し、生体情報等の「認証に必要な秘匿すべき情報」をサーバに送信・登録しない点
- 「ユーザ認証」に限らず、ユーザの意思に基づいた取引であることをサーバで確認する「取引認証」の仕組みも想定している点

(1)　生体情報等をサーバに送信・登録しない点

FIDO においては、生体情報をサーバに送信・登録せず、「ユーザクライアント側にて個人が検証され、その結果をサーバ側が信頼する」というモデルとなっている。このため、①ユーザクライアントにおける検証結果が攻撃者に改ざんされるリスクや② Authenticator が不正なものに入れ替えられ検証結果が信頼できなくなるリスクがある。

上記①に関しては、（A）Matcher において生成されるユーザの検証結果にかかる情報を改ざんする方法、（B）Authenticator にて生成される SD（2 節（2）ロ．を参照）を偽造する方法が考えられる。

これらに対して、FIDO では、(i) Authenticator が（攻撃者が容易に介入できない）安全な領域に設置されることを想定したうえで、Authenticator の中にある Matcher にてユーザを検証し、検証に成功したときのみ Authenticator にて SD に対するデジタル署名を付すことが規定されている（上記（A）への対策）。また、FIDO では、(ii) ユーザの秘密鍵は Authenticator と同じく安全な Secure Storage にて格納することが想定されているため、攻撃者は、自らが生成した SD に対してデジタル署名を付すことは困難である（上記（B）への対策）。FIDO においては、安全な領域の実装方法の例として、TEE（Trusted Execution Environment）や Secure Element[37] を例示している。

上記②に関して、攻撃者が Authenticator を偽物（生体認証でのなりすましの検知精度の低いもの）に入れ替えてしまい、検証結果が信頼できなくなるという攻撃方法が考えられる。

これに対して、FIDO では、(iii)「ユーザデバイス側で使用される Authenticator が FIDO アライアンスにおける認定取得製品か否か」ということをサーバ側で確認

37 外部からの解析に耐えるように設計され、安全にデータを格納し、処理するための演算処理機能を持ったハードウェアの総称。

できる仕組みがある。具体的には、登録フェーズにおいて、KRD（2節（2）イ．を参照）に対して Authenticator の Attestation 秘密鍵でデジタル署名することにより、FIDO アライアンスにおける認定取得製品であることをサーバ側で確認できる（認定取得製品でなければ Attestation 秘密鍵を所有していないため）。もっとも、FIDO アライアンスにおける認定取得製品は、FAR（False Accept Rate）や APCER（Attack Presentation Classification Error Rate）等のセキュリティ評価指標を検査しているわけではなく、FIDO のプロトコルに準拠しているかの検査を行っているだけである点には留意が必要である。

（2） 取引認証の仕組みについて

FIDO においては Transaction Confirmation の仕組みがオプションとして規定されており、取引内容（transaction）に対して、ユーザが取引継続の意思表示を行い、その結果をサーバ側で確認する仕組みがある。

図表 4 において、（1）にてユーザは実行したい取引内容（transaction）をサーバ側に送信し、（4）にてユーザはこれから行われようとしている取引内容（transaction）について画面を通じて確認する。ユーザが取引を続行する意思があれば、自らの生体情報を生体情報リーダに提示して取引を続行する意思表示をする。その後、（5）にて Authenticator は、ユーザ検証に成功した場合に、取引内容（transaction）のハッシュ値をはじめとするデータ（SD）に対してデジタル署名を行い、（6）および（7）にて当該情報がサーバ側に送信される。

仮にユーザクライアントがマルウエアに感染している状況下にあり、マルウエアによって、取引内容を改ざんされたり、自動的に攻撃者への送金指図を出されたりした場合においても、Transaction Confirmation の仕組みにより、「ユーザが画面を通じて確認した取引内容（transaction）と、Authenticator がデジタル署名した取引内容（transaction）とが同一であること」と「ユーザが取引継続の意思を持ったときのみにデジタル署名が行われること」が担保できれば、マルウエアによる不正送金は阻止できる（ユーザは不正送金が行われる前に攻撃を検知できる）。もっとも、当該条件をマルウエアにより崩されれば攻撃者による不正送金が成功することになる。3 節（3）ハ．においてその手法および対策を紹介している。

補論 2.　具体的な攻撃のシナリオ

図表 11 および図表 12 に示した内容において具体的な分析手法および攻撃シナリオ例を以下の通り示す。

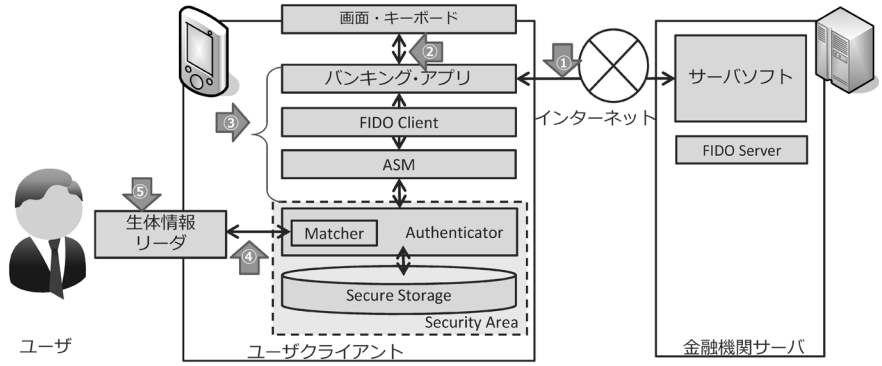
具体的な分析手法としては、登録フェーズおよび認証フェーズのそれぞれの Step 毎（3 節（1）イ．を参照）に、ケースに応じて想定される攻撃を洗い出したうえで、具体的な攻撃手口および攻撃箇所を検討する。そして、Step 全体を通じて考えたときに、最終的に 3 節（1）ハ．で示した攻撃成功につながるか否かを検証する。なお、攻撃可能な箇所は、Ratha, Connell, and Bolle [2001] を参考に図表 A-1 の通り整理する。

（1）　登録フェーズにおける攻撃について

登録フェーズにおける Step 毎に、想定される攻撃の内容、ケース毎の攻撃の手口、図表 A-1 の攻撃可能箇所を整理すると、図表 A-2 の通りとなる。

図表 A-2 をもとに、ケース毎、攻撃手口毎の攻撃成否を整理すると図表 A-3 の通

図表 A-1　攻撃可能な箇所



箇所	攻撃者による攻撃の内容の例
①	ユーザクライアントと金融機関サーバ間の通信を改ざん・盗聴する。 フィッシングサイトを設置し、同通信を改ざん・盗聴する。
②	ユーザへの表示内容を改ざん・盗聴する。 ユーザが入力する内容を改ざん・盗聴する。
③	バンキング・アプリ・FIDO Client・ASM の各コンポーネントがやり取りする情報を、改ざん・盗聴する。偽のコンポーネントを利用する。
④	生体情報リーダと Matcher 間のデータを改ざん・盗聴する。
⑤	生体情報リーダに対して、ユーザになりすますための情報を提示する。

図表 A-2　Step 毎の攻撃手口の整理（登録フェーズ）

Step	各 Step における通常時のユーザのフロー	各 Step で想定される攻撃の内容（攻撃者が実施する行動）	「ケース A：物理アクセス」において攻撃を成立させるために必要な手口	「ケース B：ネットワークアクセス」において攻撃を成立させるために必要な手口 ※括弧内の数字は図表A-1の攻撃可能箇所を示す。	
Step1	デバイスロックを解除	デバイスロックを不正に解除	不要（備考 1）	不要（備考 1）	
Step2	レガシー認証情報を入力・送信	レガシー認証情報を盗取	有効な方法は無し（備考 2）	手口 1（フィッシング）によってレガシー認証情報を盗取（①）	手口 2（マルウエア）によってレガシー認証情報を盗取（②③）
Step3	生体情報を提示（ユーザ検証）し、登録要求を継続	ユーザ検証を不正に実施	不要（備考 1）	不要（備考 1）	

備考 1：登録フェーズにおいて攻撃を成立させるために最低限必要な事項は、「攻撃者が Step2 においてレガシー認証情報を盗取する」ことである。これができれば、攻撃者は自身のデバイスで登録フェーズを実施し、攻撃が成功する。本安全性評価では、脚注 15 で述べた通り、「レガシー認証情報は攻撃者がアクセスできない専用機器で生成する」という前提であるため、レガシー認証情報を盗取するために Step1 や Step3 において攻撃を行う必要は無い。

備考 2：「ケース A：物理アクセス」の場合、利用可能な手口が「手口 3（生体認証でのなりすまし）」のみという前提を置いているが（図表 9）、この手口を使ってレガシー認証情報を盗取する有効な方法は見当たらない。ただし攻撃者が、手口 3 を使ってデバイスのロックを不正に解除し、デバイスにマルウエアを仕込んだうえで、当該デバイスを正規ユーザに返却することにより、ケース B の手口 2 に帰着させることも考えられる。本稿では、そのような場合はケース B にて論じている。

図表 A-3　ケース毎、手口毎の攻撃成否に関する評価（登録フェーズ）

攻撃の手口 ＼ アクセス方法		ケース A：物理アクセス	ケース B：ネットワークアクセス
手口 1：フィッシング		—	攻撃成立（イ） 【Step2①】
手口 2：マルウエア	偽アプリ型	—	攻撃成立（ロ） 【Step2②】【Step2③】
	凶悪型	—	攻撃成立（ハ） 【Step2②】
手口 3：生体認証でのなりすまし		攻撃不成立	—

りとなる（本文中の図表 11 と同じ内容）。図表 A-3 内の【　】は、攻撃成立の場合の図表 A-2 で示した Step および攻撃箇所を示す。なお、同図表中の「—」で示した部分は、図表 9 で示した「想定しない」攻撃手口を指す。

以下に、具体的な攻撃シナリオの例を見ていく。図表 A-2 で示した Step および攻撃箇所は、【　】内に示す。

イ．「手口１：フィッシング」と「ケース B：ネットワークアクセス」の場合

- 攻撃者が、ユーザをフィッシングサイトに誘導し、ユーザに対して言葉巧みに「レガシー認証情報を入力して下さい」と指示を出す。ユーザが、その指示に従えば、攻撃者は（ユーザの）レガシー認証情報と、自らの生体情報を使って自らのデバイスで登録フェーズを実施し、攻撃が成功する【Step2 ①】。

ロ．「手口２：偽アプリ型マルウエア」と「ケース B：ネットワークアクセス」の場合

- 攻撃者は、例えば、銀行口座の管理を便利にするためのアプリケーションと称して、偽アプリ型マルウエアを作成する。ユーザが当該マルウエアを立ち上げ、マルウエアがユーザに対して「銀行口座の管理を便利に行うためレガシー認証情報を入力して下さい」と指示を出す。ユーザがその指示に従えば、マルウエアは攻撃者に当該情報を送信する。攻撃者は（ユーザの）レガシー認証情報と、自らの生体情報を使って自らのデバイスで登録フェーズを実施し、攻撃が成功する【Step2 ②】【Step2 ③】。

ハ．「手口２：凶悪型マルウエア」と「ケース B：ネットワークアクセス」の場合

- ユーザがレガシー認証情報を正規のバンキング・アプリに入力し、凶悪型マルウエアがキーロガー等（竹森［2011］、タオソフトウェア株式会社［2012］）によって当該情報を盗取し攻撃者に送信する。攻撃者は（ユーザの）レガシー認証情報と、自らの生体情報を使って自らのデバイスで登録フェーズを実施し、攻撃が成功する【Step2 ②】。

(2)　認証フェーズにおける攻撃について

認証フェーズにおける Step 毎に想定される攻撃の内容、ケース毎の攻撃の手口、図表 A-1 の攻撃可能箇所を整理すると、図表 A-4 の通りとなる。

図表 A-4 をもとに、ケース毎、攻撃手口毎の攻撃成否を整理すると図表 A-5 の通りとなる（本文中の図表 12 と同じ内容）。図表内の【　】は、攻撃成立の場合の図表 A-4 で示した Step および攻撃箇所を示す。なお、図表中の「―」で示した部分は、図表 9 で示した「想定しない」攻撃手口を指す。

以下に、具体的な攻撃シナリオの例を見ていく。図表 A-4 で示した Step および

図表 A-4　Step 毎の攻撃手口の整理（認証フェーズ）

Step	各 Step における通常時のユーザのフロー	各 Step で想定される攻撃の内容（攻撃者が実施する行動）	「ケース A：物理アクセス」において攻撃を成立させるために必要な手口 ※括弧内の数字は図表A-1の攻撃可能箇所を示す。	「ケース B：ネットワークアクセス」において攻撃を成立させるために必要な手口 ※括弧内の数字は図表A-1の攻撃可能箇所を示す。	
Step1	デバイスロックを解除	デバイスロックを不正に解除	手口３（生体認証でのなりすまし）により、攻撃者がデバイスロックを不正に解除（⑤）	不要（備考 3）	
Step2	取引内容を送信	取引内容を改ざんして送信	不要（備考 1）	手口２（マルウエア）により、攻撃者が取引内容を改ざんして送信（②③）	
Step3	取引内容確認メッセージを確認	偽の取引内容確認メッセージを提示	不要（備考 2）	手口２（マルウエア）により、攻撃者が取引内容確認メッセージを偽装（②③）	不要（備考 4）
Step4	生体情報を提示（ユーザ検証）	ユーザ検証を不正に実施	手口３（生体認証でのなりすまし）により、攻撃者が不正にユーザ検証を突破（⑤）	不要（備考 5）	手口２（マルウエア）により、攻撃者が不正にユーザ検証を突破（④）

備考 1：この場合には、攻撃者がユーザのデバイスに物理的にアクセスでき、Step1 にてデバイスロックを不正に解除できている。このため、攻撃者は、取引内容を改ざんするまでもなく、（攻撃者）自身の口座への送金指図（取引内容）を作成し送信すればよい。取引内容を改ざんする必要が無いという意味において、（攻撃は）「不要」と記している。

備考 2：この場合には、攻撃者がユーザのデバイスに物理的アクセスでき、Step1 にてデバイスロックを不正に解除できており、Step2 にて攻撃者への送金指図が既に行われている。このため、攻撃者は、偽の取引内容確認メッセージを提示するまでもなく、表示された「（攻撃者）自身の口座への送金確認メッセージ」を確認すればよい。偽の取引内容確認メッセージを提示する必要が無いという意味において、（攻撃は）「不要」と記している。

備考 3：この場合には、ユーザ本人が通常使用のためにユーザ自身のデバイスのロック解除を実施することが想定される。このため、攻撃者がデバイスロックを不正に解除しなくても、Step2 以降を攻撃者が実施することが可能であり、（攻撃は）「不要」と記している。

備考 4：この場合には、ユーザ本人がデバイスを使用しており、Step2 においてユーザが気付かないところで取引内容が改ざんされており、次の Step4 においてユーザ検証が不正に実施される。このため、Step3 にて偽の取引内容確認メッセージを提示せずとも、攻撃者は「攻撃者への振込みの取引内容（transaction）」をユーザに提示すればよい（次の Step4 にて、ユーザの意図に反してユーザ検証が実施されるため）。このため、攻撃者が偽の取引内容確認メッセージを提示する必要が無いことから、（攻撃は）「不要」と記している。

備考 5：この場合には、ユーザ本人がデバイスを使用しており、Step2 においてユーザが気付かないところで取引内容が改ざんされており、Step3 において同じく取引内容確認メッセージが偽装されている。ユーザからすると、自身の意図する取引内容を送信し（Step2）、取引内容確認メッセージでそれを確認しているため（Step3）、ユーザは疑いを持つことなく、自らの生体情報を提示することにより取引を実行しようとする。このため、ユーザ検証を攻撃者が不正に実行する必要が無いことから、（攻撃は）「不要」と記している。

図表 A-5　ケース毎、手口毎の攻撃成否に関する評価（認証フェーズ）

攻撃の手口＼アクセス方法		ケース A：物理アクセス	ケース B：ネットワークアクセス
手口１：フィッシング		—	攻撃不成立（備考 1）
手口２：マルウエア	偽アプリ型	—	攻撃不成立（備考 2）
	凶悪型	—	攻撃成立（ロ） 【Step2②】【Step3②】 または 【Step2②】【Step4④】
手口３：生体認証でのなりすまし		攻撃成立（イ） 【Step1⑤】【Step4⑤】	—

備考 1：原理的には、攻撃者が、ユーザをフィッシングサイトに誘導し、当該サイト上で「攻撃者へ振込みを行ってください」と指示を出し、ユーザがバンキング・アプリを使って振込みを実施してしまうと攻撃が成功する。もっとも、本稿ではそのような攻撃手法は、ユーザの意図せざる振込みではないという整理を行い、攻撃不成立としている。

備考 2：この場合、攻撃を成立させるためには、正規 Authenticator が改ざんされた取引内容に対してデジタル署名を付す必要があるが、そのためには、正規 FIDO Client と偽バンキング・アプリとを接続する必要がある。もっとも FIDO の仕様では、FIDO Client は接続可能なアプリケーションを「FacetID」と呼ばれる ID で識別できる仕組みがあり、Android においては、FacetID を Context（アプリケーションの環境情報を受け渡すために使用されるもの）から取得する実装例が示されている。偽アプリ型マルウエアの前提では、サンドボックスの仕組みにより、偽バンキング・アプリが正規バンキング・アプリの Context を取得することが困難であると考えられるため、攻撃不成立としている。

攻撃箇所は、【　】内に示す。

イ．「手口３：生体認証なりすまし」と「ケース A：物理アクセス」の場合

- 攻撃者が、ユーザのデバイスのロック解除を、生体認証でのなりすましにより行う。具体的ななりすましの手法については、3 節（3）ニ．で詳しく述べる【Step1⑤】。そのうえで攻撃者は、ユーザのデバイスからバンキング・アプリを立ち上げ、自口座への振込み指示を行った後、Transaction Confirmation による確認（攻撃者への振込み指示）を、生体認証でのなりすましにより実施する【Step4 ⑤】。

ロ．「手口２：凶悪型マルウエア」と「ケース B：ネットワークアクセス」の場合

- ユーザが正規バンキング・アプリを立ち上げ、取引内容（例：A さんに 1 万円振込み）を入力するが、凶悪型マルウエアが正規のバンキング・アプリのメモリ情報を書き換えるなどして（株式会社 FFRI［2012］）当該情報を改ざん（例：X さんに 100 万円振込み）して、金融機関サーバに送信する【Step2 ②】。金融機関サーバは認証要求を正規バンキング・アプリに送信し、正規 Authenticator が取引内容確認メッセージを表示（例：X さんに 100 万円振込み確認表示）するが、凶悪型マルウエアはタイミングを見計らい、「ディスプレイ・オーバーレイ（Display

Overlay）攻撃」（3 節（3）ハ．を参照）により当該画面上に、マルウエアが作成したメッセージ（例：A さんに 1 万円振込み確認表示）を出す【Step3 ②】。ユーザはマルウエアが作成した最前面のメッセージ内容を確認し、自らの生体情報を提示してしまうと、X さんに 100 万円の振込みが行われてしまう。

- 凶悪型マルウエアは、生体情報リーダと Matcher 間で通信されるユーザの生体情報を盗聴し保持しておく。次に、ユーザが正規バンキング・アプリを立ち上げ、前述と同じ要領で取引内容を改ざんしたうえで、金融機関サーバに送信する【Step2 ②】。金融機関サーバは認証要求を正規バンキング・アプリに送信し、正規 Authenticator が取引内容確認メッセージを表示（例：X さんに 100 万円振込み確認表示）する。ユーザは不正な振込みであると気付いて取引をキャンセルしようとするが、凶悪型マルウエアは、Matcher にユーザの生体情報を流し込み（リプレイ攻撃）、それが Matcher で受理されれば、当該取引がユーザの意図に反して（自らの生体情報を提示しないにも関わらず）実行されてしまう【Step4 ④】。