調　査

急速に脚光浴びる「フィンテック」⑧

－生体認証技術の高度化への挑戦－

信金中央金庫 地域・中小企業研究所主任研究員

藁品　和寿

（キーワード）フィンテック、サイバーセキュリティ、生体認証、指紋

（視　点）

「フィンテック」では、スマートフォンで提供されるさまざまなサービスに代表されるとおり、インターネットをネットワーク基盤としたオンライン取引を前提とするサービスが多い。そのため、なりすまし等による不正送金など犯罪の対象となりやすいことが指摘されている。その対策の一つとして、生体認証技術への注目がますます高まっている。

そこで本稿では、生体認証技術のうち指紋認証技術の高度化に挑戦する株式会社Liquid（東京都千代田区）の取組みを紹介する。

（要　旨）

- 金融機関とフィンテック企業との間でAPIの公開、連携が本格化してくることを見通すと、金融機関側だけがシステム管理態勢を強化してもフィンテック企業のシステムから金融機関のシステムが間接的に攻撃されるリスクも想定しなければならないだろう。こうしたリスクへの対処策の一つとして、取引の相手方の確認を行う「認証」という手続きのうち生体認証技術の重要性はますます高まっている。
- 技術面や利用者の心理面などで多くの課題を抱える生体認証技術はまだまだ開発途上といえるものの、DNA等誤判断がより少ない情報での認証や身体運動での認証などが試されるなど研究は着実に進んでいることから、今後の発展に期待がかかる。
- サイバー攻撃手法が高度化するとともに増加傾向にあるなか、とりわけ「フィンテック」などデジタルバンキングを推進する金融機関にとっては、生体認証を含めて、顧客に過大な負荷をかけずにいかに確実な認証方法をとっていくかが課題となろう。

1. 重要性が高まる情報セキュリティの確保

金融当局は、従来から、金融機関のサイバーセキュリティ管理態勢を含む情報セキュリティ(注1)について、システム管理等の枠組みのなかで監督、検査を実施している。

最近の技術進歩にともない、金融業界でも、「フィンテック」に代表されるとおり、インターネットの利用が拡大傾向にある。この背景の下、サイバー攻撃の手口が巧妙になるなどその脅威が高まるなか、2014年11月に制定されたサイバーセキュリティ基本法において、政府は、金融を含む重要インフラ事業者のサイバーセキュリティ確保のため、政府一丸となって施策を講じることを表明している。

こうしたなか、2015年7月、金融庁は、『金融分野におけるサイバーセキュリティ強化に向けた取組方針』を公表し、サイバーセキュリティ強化に向けた基本的な考え方と5つの方針を明らかにした(**図表1**)。併せて、この方針に実効性を持たせるため、金融機関同士での情報共有の枠組みも示している(**図表2**)。最近脚光を浴びている「フィンテック」では、多くの場合、その基盤としてインターネットが利用されている。金融調査情報28-18『急速に脚光浴びる「フィンテック」⑥－「APIエコノミー」の形成に向けて－』(注2)で紹介したとおり、金融機関とフィンテック

図表1　金融分野のサイバーセキュリティ強化に向けた5つの方針

基本的考え方

○　金融分野のサイバーセキュリティ対策の強化には、官民が一体となって取り組んでいくことが重要。
○　このため金融庁は、金融機関との間で、サイバーセキュリティ確保という共通目的を有しているとの理解の下、建設的な対話を日常的に重ねていくことを目指すとともに、行政当局の立場から金融分野のサイバーセキュリティ強化に貢献するため、以下の5項目に取り組んでいく。

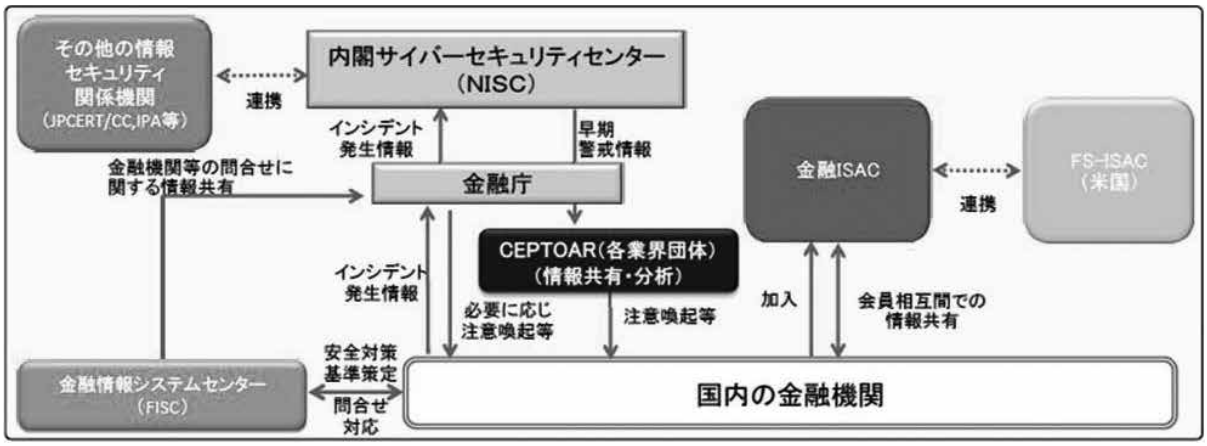
5つの方針

1. サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2. 金融機関同士の情報共有の枠組みの実効性向上
3. 業界横断的演習の継続的な実施
4. 金融分野のサイバーセキュリティ強化に向けた人材育成
5. 金融庁としての態勢構築

(備考) 金融庁 (2015年7月2日)『金融分野におけるサイバーセキュリティ強化に向けた取組方針 (概要)』より抜粋

(注)1. 増島 雅和、堀 天子編著 (2016年)『FinTechの法律』によると、情報セキュリティにおける対応策を検討する際の視点として、「機密性」、「完全性」、「可用性」という概念を示したのは、OECD (経済協力開発機構)が1992年に制定 (2002年改正)した「情報システム及びネットワークのセキュリティのためのガイドライン」である。
2. http://www.scbri.jp/PDFkinyuchousa/scb79h28s18.pdf参照

図表2　金融業界におけるサイバーセキュリティにかかる情報共有の枠組み



（注1）CEPTOAR（セプター）とは、IT障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有する役割を担う組織のこと。
（注2）金融ISACは、日本の金融機関によるサイバーセキュリティに関する情報の共有および分析を行い、金融システムの安全性の向上を推進することにより、利用者の安心・安全を継続的に確保することを目的とした組織。

（備考）金融庁（2016年7月2日）『金融分野におけるサイバーセキュリティ強化に向けた取組方針（概要）』より抜粋

企業との間でAPI[注3]の公開、連携が本格化してくることを見通せば、金融機関は、自行庫内のみでシステム管理態勢を強化するだけではなく、連携するフィンテック企業のシステムから自行庫のシステムが間接的に攻撃されるリスクも想定しなければならないだろう。

こうしたリスクへの対処策の一つとして注目されるのは、取引の相手方の確認を行う「認証」[注4]という手続きである。とりわけ「フィンテック」では、オンラインでの金融取引が中心となるため、なりすまし等による不正送金など犯罪の対象となりやすいことが指摘されている。その対策の一つとして、認証手続きを厳格化して正確性を高めながらも顧客に過大な負担をかけないという観点から、生体認証技術（**図表3**）への注目がます

図表3　生体認証技術の概要

定義	・生体情報を用いて本人確認・認証を行う技術 ・具体的には、以下の要素で構成 　生体情報の取得 　生体情報の特徴量抽出 　照合処理
従来技術の課題	・パスワード等を記憶する必要がある ・安全性に比例して、入力の手間が増大
当技術のメリット	・本人が忘れることなく、恒久的に確実な認証が可能 ・利用者の操作が簡易であり、スムーズな認証が可能

（備考）有限責任監査法人トーマツ『平成27年度産業経済研究委託事業　金融・IT融合（FinTech）の産業金融等への影響に関する調査研究　調査検討結果報告書』より引用

（注）3. APIとは、「Application Programming Interface」の略である。簡単にいうと、異なるソフトウェア同士のデータ連携を可能にするルールのことである。オープンAPIによるデータ連携でサービス同士がつながることにより、サービス利用者は、つながったそれぞれのサービスを利用できるようになり、利用者にとってのサービス機能が充実する。
4. 増島 雅和、堀 天子　編著（2016年）『FinTechの法律』によると、認証手続きは、継続的取引での相手方の同一性の確認、マネー・ロンダリングやテロ資金供与などの防止、という二つの側面から重要になる。

ます高まっている。

そこで本稿では、生体認証技術のうち指紋認証技術の高度化に挑戦する株式会社Liquid（東京都千代田区）の取組みを紹介する。

2. 株式会社Liquid（東京都千代田区）における生体認証技術の高度化への挑戦

(1) 会社の概要

同社は、2013年12月、久田康弘CEOにより、生体認証・空間認識エンジン「Liquid（リキッド）」の研究、開発を目的として設立された（**図表4**）。同社社名の“Liquid”には、液体のように世界の津々浦々に自社のシステムが浸透させたいという想いを込めている。グループ会社（100%出資子会社）には、同社システムの販売促進を担う㈱Liquid Japanと、応用技術の研究を担う㈱Recreation Labがあり、今回取材に応じていただいた保科秀之氏は、㈱Liquid Japanの代表取締役として、わが国での同社システムの普及に努めている。なお、同社は、フィンテック企業のためのコワーキングスペース「FINOLAB（フィノラボ）[注5]」に入居している。

創設者の久田CEOは、大学在学中に、自ら得意とする統計数理の知識、ノウハウを活かしてFX（外国為替証拠金取引）のトレーディングシステムを開発し、学生起業家となった。大学卒業後は、外資系金融機関に就職し、コンサルティングやIPO（新規株式公開）支援などで実務経験を重ねながら幅広い人脈ネットワークを構築した。このときに構築した幅広い人脈が現在のビジネス展開に大いに活かされているという。

2010年に入りスマートフォンが普及し始めると、久田CEOは、近い将来、インターネットの世界が“PCからスマホへ（キーボードレスへ）”、“ブログからインスタグラムへ（文字から画像・動画へ）”と移行していくだろうと推測し、「画像・動画を解析するビジネスはできないか」を模索、探究した。そのなかで、久田CEOは、当時、社会的に問題となっていたカードの不正利用やID・パスワードの不正利用などの“なりすまし”に着目し、利用者の利便性を損なわずにセキュリティ対応の高度化を図る手段として生体認証技術に注目した。

図表4　同社の概要

同社の概要

法人名	株式会社Liquid
代表	久田 康弘
本部所在地	東京都千代田区大手町
設立	2013年12月
事業内容	生体認証・空間認識エンジン「Liquid」の研究・開発

（備考）1. 写真（右）は取材に応じていただいた（株）Liquid Japanの保科秀之代表取締役
2. 信金中央金庫 地域・中小企業研究所作成

(注)5. 2016年10月に、電通、電通国際情報サービス、三菱地所との協業で、わが国で初めてのフィンテック集積拠点として、東京都千代田区丸の内に設置された。2017年2月にリニューアル移転（千代田区大手町）している。

2013年12月、久田CEOが同社を創業すると、一般的な1対1認証ではなく1対N（複数）認証のできる生体認証のための検索エンジンの開発に取り組んだ。当初、大学を含む関係各所から、当該エンジンの開発は困難ではないかとの疑問の声が多く寄せられた。そこで、2015年2月から約2年間、総務省のベンチャー創出支援事業「I-Challenge!（アイ・チャレンジ）」に採択されて研究を重ね、クラウド技術の高度化など技術進歩の後押しもあって(注6)、生体認証エンジン「Liquid」の独自開発に至ることができた。現在、同社は、このLiquidエンジンにさらに磨きをかけながら、当該エンジンを活用したシステムの開発、提供に努めている。

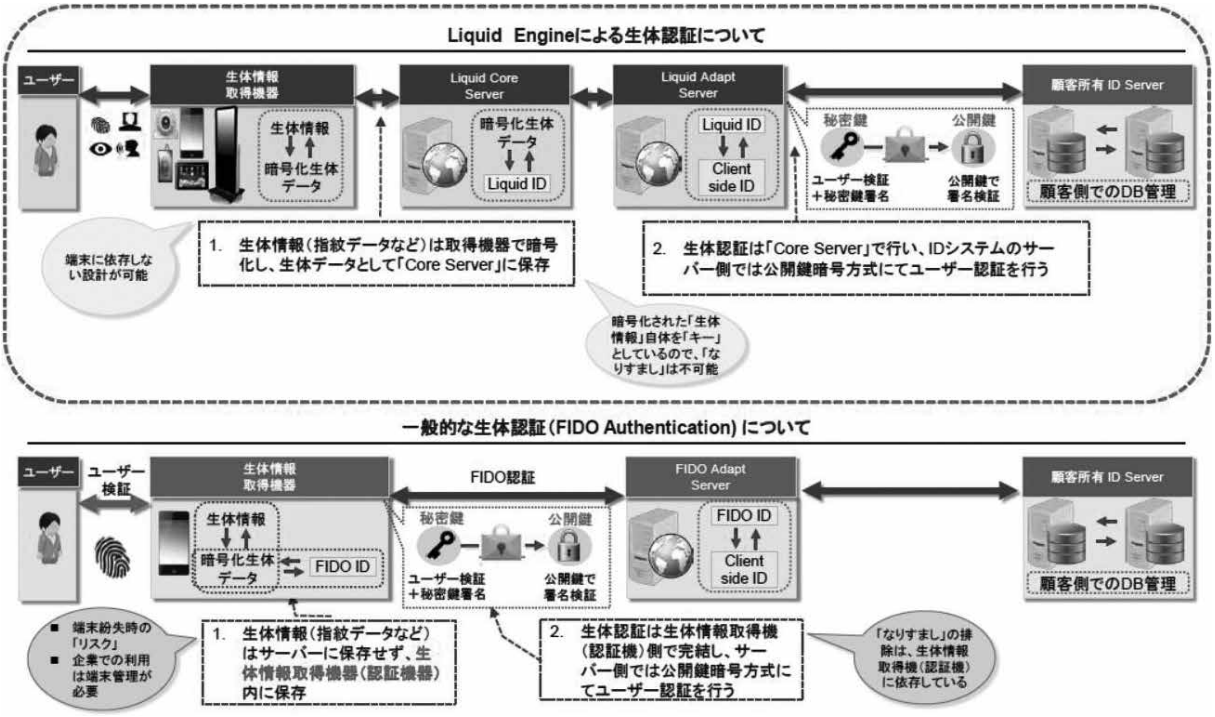
(2) 取組みの概要

同社の生体認証エンジン「Liquid」のシステム構成は、専用アプリをダウンロードしたスマホ等の情報端末と指紋認証デバイスだけである(注7)。標準化された生体認証技術であるFIDO（Fast IDentity Online、次世代オンライン認証規格）と比べると、大きな特長として、「生体情報をスマホ等の認証機器ではなくクラウドサーバー上で保存するため、“なりすまし”の防止を不可能にできること」、「クラウドサーバー上で生体情報を管理することから、生体情報漏えいの責任は全面的に同社になること」が挙げられる(注8)（**図表5**）。FIDOでは、生体情報がスマホ等の情報端末に保存されるため、利用者には端末紛失リスクの負担が及ぶことになる。この利用者負担を解消できる同社の生体認証技術は、利用者利便にかなったものといえよう。また、技術面においては、人工知能（AI）を活用することで、大規模な指紋画像データを効率的に検索して認証をより高速化することが実現できた。なお、同社の生体認証エンジン「Liquid」は、2016年7月、わが国とシンガポールにおいて既に特許を取得している。

同社は、総務省のベンチャー創出支援事業「I-Challenge!」に採択された2015年以降、経済産業省(注9)などの省庁に加えて、ハウステンボス(株)(注10)、(株)イオン銀行(注11)、トレイダーズホールディングス(株)(注12)など多くの企業と実証実験などに取り組んでいる。生体認証エンジン「Liquid」を活用した決済システムは、2015年2月から「Liquid Pay（リキッド・ペイ）」というサービス名で提供されており、同社の主力サービスの一つとなっ

(注)6. 現在の技術であれば、例えばセンサーで指紋の凹凸や指の温度と空気の温度の違いなどを生体検知することで、指紋認証において、シリコンでの指紋偽造などの“なりすまし”に対応できる。
7. 現在は指紋認証での実証実験やサービス提供を進めているが、コア技術である生体認証エンジン「Liquid」は、指紋以外の静脈、顔、虹彩などの生体情報にも適用できる。
8. ただし、1対N認証であり、かつ生体情報をクラウドサーバーで管理するスキームであるがゆえに、FIDOに比べて認証スピードは若干遅くなる。そのため、さらなる認証の高速化を目指して人工知能技術（AI）を活用しており、同様のスキームの生体認証技術のなかでは、同社の認証スピードは圧倒的に優位となっている。
9. 現在、KDDIなどとともに、訪日外国人向けに、指紋認証を活用してパスポート提示不要で宿泊施設へのチェックインを可能にする実証実験に取り組んでいる。
10. 2015年10月から、同社サービス「Liquid Pay」を利用して、園内地域通貨・テンボス通貨の運営を開始した。
11. 店頭手続きやATM利用の際に、指紋認証のみで本人確認のできるサービスの実証実験に取り組み、現在、同行神田店で実際に利用されている。
12. 生体認証技術を活用した金融取引システムにかかる共同調査および研究開発に取り組んでいる。

図表5　生体認証エンジン「Liquid」の仕組み



（備考）同社資料「FinTechにおける生体認証とセキュリティについて」より抜粋

ている。また、2016年12月からは、生体認証のみでカード不要の決済システム「Liquidレジ（指紋センサー搭載レジスター）」(注13)を出荷、販売しており、2017年2月末現在、東京都内にある中小小売店を中心に1,000店舗以上と契約している。さらに、フィンテックの取組みでは、2017年1月から、(株)みずほフィナンシャルグループとともに、振込みや残高照会をカード・現金不要で可能にする「手ぶらで決済」(注14)（**図表6**）の実証実験を進めている。

図表6　同社が開発した生体認証決済システム「手ぶらで決済」

（備考）信金中央金庫 地域・中小企業研究所撮影

(3) 今後の展望

現在、実証実験段階のサービスが多いものの、同社では、それぞれに確かな手ごたえを感じている。2016年2月に経済産業省（IoT

(注)13. 中小企業がLiquidレジを導入するにあたっては、軽減税率対策補助金などを活用できるため、実質的に費用ゼロで導入できる。なお、決済手数料は、決済金額の1%程度である。
14. 更新系API連携で実証実験に取り組んでいる。セキュリティの観点から他人受入率（他人が認証を試みたときに本人と誤認してしまう確率）を1兆分の1の確率へと圧倒的に低下させるため、親指と人差し指の2本で指紋認証する仕組みとしている。

推進ラボ(注15)）で開催された「第1回先進的IoTプロジェクト選考会議」では、指紋による訪日観光客の個人認証への同社の取組みが、252件のなかから見事、グランプリに選出され表彰を受けた。同社の生体認証エンジン「Liquid」の技術が、専門家を含めた第三者から高い評価を受けた結果といえる。ハウステンボス（長崎県佐世保市）やイオン銀行神田店（東京都千代田区）においては、実証実験を終えて「Liquid Pay」のサービスが実際に開始されるなど、「Liquid Pay」の利用者数およびトランザクション数は着実に増えている。また、2017年2月、インドネシアにおいて、大手財閥サリムグループと合弁会社を設立し、生体情報を利用する大規模な次世代認証プラットフォームの構築に向けて取り組むことを公表した(注16)。

同社は、今後、国内外で成功事例を次々とつくりだしていくことにより、社名に含意されている想いのとおり、同社のシステムを世界の津々浦々に普及させたいと意気込む。

3. おわりに　ー今後の発展に期待がかかる生体認証技術ー

有限責任監査法人トーマツが経済産業省から受託した『平成27年度産業経済研究委託事業　金融・IT融合（FinTech）の産業金融等への影響に関する調査研究　調査検討結果報告書』によると、生体認証技術については、本稿で事例紹介した**(株)Liquid**が取り組む指紋認証に加えて、DNAでの認証など誤判断がより少ない情報での認証や、ジェスチャーや眼球の動きなど身体運動での認証など、さまざまな認証方法での研究が進められている。一方で、生体情報は、唯一性という特徴を持つことから、情報漏えい時に生体情報を変更できないという技術面での課題などに加えて、利用者が事業者に対して生体情報を提出することに躊躇するという心理面での不安を払拭しなければならないというそもそもの課題が指摘されている（**図表7**）。多くの課題を抱える生体認証技術はまだまだ途上といえるものの、研究は着実に進んでいることから、今後の発展に期待がかかる。

トレンドマイクロ株式会社は、2017年1月に公表したプレスリリース(注17)で、2016年1月から11月にかけてのランサムウェア(注18)被害が前期比3.4倍と急増したことを受けて、2016年は『日本における「サイバー脅迫」元年』といえる年になったと指摘している。また併せて、オンライン銀行詐欺ツール(注19)の国内検出台数が過去最大の98,000台に達したことをトピックとして取り上げられ、金融機関における今後の被害増加が懸念されている。

サイバー攻撃手法が高度化するとともに増

(注)15. IoT推進ラボでは、政府関係機関、金融機関、ベンチャーキャピタル等と連携し、成長性・先導性、波及性（オープン性）、社会性等の観点から優れたIoTプロジェクトに対して、資金支援やメンターによる伴走支援、規制改革・標準化等に関する支援を行っている。
16. 同社ニュースリリース参照（http://liquidinc.asia/20170223/）
17. http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20170106014256.html参照
18. 感染したパソコンの操作をロックしたり、ファイルを勝手に暗号化して復旧の代わりに金銭を要求する不正プログラムで、「身代金要求型ウィルス」とも呼ばれる。
19. 感染すると、オンライン取引のログイン情報に加えて、クレジットカードの利用者情報を詐取されるケースもある。

図表7　生体認証技術の概要

技術自体	・情報流出時の回復不可能性 情報が流出した場合、生体情報を変更することができず、修復が不可能 ・セキュリティと利便性のトレードオフ なりすまし防止の性能を上げた場合、本人であっても否認される可能性が高くなり利便性が低下する関係
費用対効果	・コストが高止まり 標準技術が存在せず大規模に生産されないため、機器等の単価が下がりにくい 厳格なデータ管理が求められることもコスト上昇要因
ビジネスへの適用時	・情報提供への不安 生体情報を事業者へ提供することへの心理的抵抗 ・利用者の習熟 生体認証を強要する場合、ユーザ名＋パスワード入力に慣れた顧客の離反を招く可能性がある

（備考）有限責任監査法人トーマツ『平成27年度産業経済研究委託事業　金融・IT融合（FinTech）の産業金融等への影響に関する調査研究　調査検討結果報告書』より引用

加傾向にあるなか、とりわけ「フィンテック」などデジタルバンキングを推進する金融機関にとっては、生体認証を含めて、顧客に過大な負荷をかけずにいかに確実な認証方法をとっていくかが課題となろう。

〈参考文献〉

・金融庁（2016年7月2日）『金融分野におけるサイバーセキュリティ強化に向けた取組方針（概要）』

・トレンドマイクロ（2017年1月10日）『トレンドマイクロ、「2016年国内サイバー犯罪動向」速報版を発表～ランサムウェア被害報告件数が過去最大、日本における「サイバー脅迫」元年に～』

・増島 雅和、堀 天子編著（2016年）『FinTechの法律』日経BP

・有限責任監査法人トーマツ（2016年3月18日）『平成27年度産業経済研究委託事業　金融・IT融合（FinTech）の産業金融等への影響に関する調査研究　調査検討結果報告書』