



2026 年 9 月 28 日

各 位

会 社 名 株 式 会 社 E L E M E N T S
代 表 者 名 代 表 取 締 役 社 長 長 谷 川 敬 起
(コード番号：5246 東証グロース市場)
問 合 せ 先 経 営 企 画 部 長 泉 光 一 郎
(TEL 03-4530-3002)

「LIQUID Auth Passkey（リキッドオースパスキー）の累計認証件数、15 億件突破」に関する発表

当社は、表題のプレスリリースを行いましたのでお知らせいたします。

詳細は下記のプレスリリースをご参照ください。

2026 年 9 月 28 日

株式会社 Liquid

「LIQUID Auth Passkey（リキッドオースパスキー）」の累計認証件数、15 億件突破

～証券不正取引等の被害による金融庁の監督指針改正、フィッシング耐性のある多要素認証の導入・必須化が進む～

株式会社 Liquid（本社：東京都中央区、代表取締役：長谷川 敬起、以下「Liquid」）は、パスキー認証基盤

「LIQUID Auth Passkey（リキッドオースパスキー）」において、これまでに提供したパスキーの累計認証件数^{*1}が 15 億件を超えたことをお知らせします。

2025 年に証券会社のインターネット取引サービスにおける不正アクセス・不正取引被害（いわゆる証券口座乗っ取り等）が多発したことを受け、金融庁は同年 10 月 15 日に監督指針を改正^{*2}しました。

現在、証券各社を中心とする金融業界では、パスキー等のフィッシング耐性^{*3}のある多要素認証^{*4}の導入・必須化が進んでいます。

LIQUID Auth Passkey について：<https://liquidinc.asia/liquid-auth-passkey>

リキッドオースパスキー

LIQUID Auth Passkey の

累計認証件数

15 億件突破！



^{*1} 「LIQUID Auth Passkey」における、パスキーの作成（登録）および認証（ログイン、重要操作時の再認証）の合計件数。集計期間は 2025 年 10 月～2026 年 8 月

^{*2} 金融庁「金融商品取引業者等向けの総合的な監督指針」等の一部改正（2025/07/15 改正案公表、2025/10/15 改正）：<https://www.fsa.go.jp/news/r7/shouken/20250715/20250715.html>

*3 アクセス中の URL（ドメイン名）を認証デバイスが自動で暗号検証する仕組み。ユーザーが偽サイトに認証情報を入力しても、それを検知して情報流出を自動的に遮断する

*4 信頼性担保のため、「知識（パスワード等）」「所持（認証デバイス等）」「生体（生体データ等）」の3要件から、複数の要素を要求する認証方式。従来の ID・パスワード認証のみの管理に比べアカウントハックやなりすましを強固に防ぐ

■ 要約

- ・Liquid が提供するパスキー認証基盤「LIQUID Auth Passkey」における、累計認証件数（パスキーの作成・登録およびログイン・重要操作時の再認証の合計）が 15 億件を突破した
- ・2025 年に相次いだ「証券口座乗っ取り」等の被害多発を受け、金融庁が「金融商品取引業者等向けの総合的な監督指針」等を改正、ログインや出金等の重要操作時におけるフィッシング耐性のある多要素認証の実装および必須化が監督上の着眼点として明記され、パスキーは証券業界を中心とする金融業界で急速に導入が進んでいる
- ・「LIQUID Auth Passkey」は、証券取引開始時等の急激なスパイクアクセスや、グローバルにおける秒間 3,000 リクエストを安定して処理する高い可用性と堅牢性が評価され、ログイン時のみならず出金や口座情報変更などの重要操作時の再認証でも日常的に活用されている
- ・Liquid は、パスキー登録・リカバリ時の第三者による悪用リスクを防ぐため、オンライン本人確認「LIQUID eKYC」による身元確認や「LIQUID Auth Face」による本人認証を組み合わせた安全なバインディング設計と、各事業者に最適化された柔軟な実装を提案している
- ・今後は、金融機関を騙ったフィッシング被害の増加や金融庁・警察庁と連携した業界横断的な広報、警察庁サイバー警察局による導入呼びかけを背景に、証券業界での豊富な実績とノウハウをもとに、ネット銀行をはじめとする金融業界全般、およびその他多様な業界へ展開を拡大する

■ 背景

「証券口座乗っ取り」被害多発

2025 年、証券会社を装ったフィッシングサイト等でログイン ID やパスワードを窃取し、インターネット証券取引サービスへ不正にアクセスして株式を売買する、いわゆる「証券口座乗っ取り」等の被害が多発しました。

これを受け、金融庁は 2025 年 7 月 15 日に「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）を公表し、2025 年 10 月 15 日にこれを改正しました。

ログイン、出金、出金先銀行口座の変更などの重要な操作時において、パスキーによる認証や、PKI（公開鍵基盤）^{*5}をベースとした認証など、「フィッシングに耐性のある多要素認証の実装及び必須化」が、監督上の着眼点として明記されています。

*5 公開鍵暗号技術と電子証明書を用いて、インターネット上での安全な通信を支えるセキュリティの仕組み。データの暗号化に加え、通信相手が本人であることの証明や、データの改ざん防止を実現

証券業界の動向

日本証券業協会も 2025 年 7 月 15 日に「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正案を公表しています*6。

日本証券業協会の調査では、インターネット取引を行う会員は 94 社（2026 年 3 月末）*7でした。同協会は、多要素認証の設定必須化を決定した証券会社全 79 社（2025 年 7 月 7 日時点）の社名を Web にて公表*8しています。

このような動きを受け、現在、証券業界ではパスキーの導入が急速に進んでいます。

「LIQUID Auth Passkey」（旧称「LIQUID Auth」）は、2025 年の証券業界へのサービス提供開始以来、順調に実績を重ねています。

*6 日本証券業協会「インターネット取引における不正アクセス等防止に向けたガイドライン」改正（2025 年 7 月 15 日 改正案公表）

https://www.jsda.or.jp/about/public/bosyu/files/20250715_guideline_public.pdf

*7 日本証券業協会「インターネット取引に関する調査結果（2026 年 3 月末）について」（2026/06/26）

<https://www.jsda.or.jp/shiryoshitsu/toukei/netcyouusa2603.pdf>

*8 日本証券業協会「多要素認証の設定必須化を決定した証券会社」2025 年 7 月 7 日時点

https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/list_tayouso/index.html

金融業界および他業界への広がり

金融機関を騙ったフィッシングによる不正送金・不正取引被害が増加している現状を踏まえ、堅牢性を高めるパスキーを含めたフィッシング耐性のある多要素認証への移行は、証券業界のみならず金融業界全体、そして他業界にも広がりつつあります。

2026 年 4 月 16 日、銀行・信用金庫・信用組合・労働金庫・証券会社が金融庁・警察庁と連携し、「フィッシング耐性のある多要素認証」の認知拡大による金融犯罪の防止を目的とした、業界横断の広報が実施されました*9。

2026 年 9 月、警察庁サイバー警察局はニュースレター「Cyber Police Agency Letter 2026 Vol.12」*10において、サービス事業者に対し「パスワードだけの認証はもう限界です。自社サービスにパスキーを導入し、安全で快適なログインを実現しましょう！」と呼びかけています。

このような動向を受け、「LIQUID Auth Passkey」は、証券会社のほかにも、ネット銀行を含む金融事業者、またその他の事業者へも、導入が急速に拡大しています*11。

*9 金融庁「フィッシング耐性のある多要素認証等に係る官民一体・業界横断的な広報について」（2026 年 4 月 16 日）：<https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html>

*10 警察庁サイバー警察局「Cyber Police Agency Letter 2026 Vol.12」(令和 8 年 9 月号)

https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.12cpal.pdf

*11 「LIQUID Auth Passkey」導入事例 <https://liquidinc.asia/news>

■ 「LIQUID Auth Passkey」の累計認証件数 15 億件について

今回の 15 億件には、ログイン時の認証に加え、出金や出金先口座の変更などの重要操作時の再認証が含まれます。「LIQUID Auth Passkey」の導入企業では、ログイン時だけでなく、こうした重要操作時の再認証にもパスキーが日常的に利用されています。

証券取引では、寄り付きなどの取引開始のタイミングにアクセスが集中します。認証基盤の応答が遅れば、取引の開始そのものに影響します。

「LIQUID Auth Passkey」は、国内大手オンライン証券における取引開始時のスパイクアクセス^{*12}(通常の約 3 倍)を日次で安定処理してきました。また、グローバルでは秒間 3,000 リクエストの処理実績があります。

*12 Web サーバーに短時間で急激なアクセスが集中する現象

■ 金融事業者が、パスキー実装時に抑えるべきポイント

導入を成功させるには、パスキーの安全性と利便性を最大限に活かした設計が鍵となります。

1. 登録時の本人性確認で、パスキーの安全性を確保

パスキーによる認証はフィッシング耐性を持っています。しかし、不正にアカウントへアクセスした第三者がパスキーを登録できる仕組みになっていると、その第三者は、自ら登録したパスキーで以降の認証を通過できてしまいます。このリスクは初回登録時に限らず、パスキーの追加登録、端末変更、アカウント回復の各経路でも生じ得ます。

FIDO Alliance^{*13}も、フィッシング可能な認証方式より新たなパスキーの登録を許可することを、アカウント乗っ取りにつながるリスクとして挙げています。

Liquid はこのような不正への対策として、パスキー登録時にオンライン本人確認「LIQUID eKYC (リキッドイーケーワイシー)」による身元確認^{*14}や、「LIQUID Auth Face (リキッドオースフェイス)」による本人認証^{*15}を組み合わせる「バインディング」を推奨、個々のケースに合わせた構成を提案しています。

*13 パスワードに依存しない、安全でシンプルなオンライン認証の標準化を目指して 2012 年 7 月に発足したグローバルな非営利の業界団体 <https://fidoalliance.org/overview/?lang=ja>

*14 申請者が実在するか、申告された属性情報(氏名・住所・生年月日など)が正確か確認すること

*15 現在サービスを利用しているのが、本人自身かを照合すること

2. 事業に最適な実装要件を選択する

パスキーの実装には、王道と呼べるパターンは存在しません。既存の認証システムとの接続方式、パスワード認証からの移行手順、対応するチャンネル、再認証を求める操作の範囲は事業者ごとに異なります。

2025 年のパスキー対応初期には、各金融事業者から Liquid に多くの要件が寄せられ、それらを満たすための設計・実装に関する相談が集中しました。パスキー導入という目的は同じですが、各社の設計はそれぞれ別のものとなりました。Liquid は日本における FIDO Alliance のメンバーとして、世界の最新技術トレンドや日本での事例を踏まえ、WebAuthn および各種デバイスの特性を踏まえた実装方式を提案しています。

■ 2026 年 9 月 25 日の Apple・Google アカウント乗っ取りによる証券不正取引報道について

Liquid からの提言 — パスキーとは独立した端末認証および eKYC による本人再確認が重要 —

Apple や Google のアカウントが乗っ取られ、アカウントに保存・同期されたパスキー^{*16}等を利用して証券口座で不正取引が行われた疑いがある事案が発生したとの報道がありました。

Liquid は、金融事業者に追加対策として「パスキーとは独立した端末認証」ならびに、「リスクに応じた本人再確認」を提言します。

同期パスキーでは、Apple や Google などのアカウントを通じて複数端末でパスキーを利用できます。アカウントそのものが侵害された場合、攻撃者の端末から被害アカウントを利用した「正規のパスキー」による認証が成立します。

そのため今回の事案に対しては、パスキーだけに依存せず、「利用端末が登録済みの端末か」を独立した仕組みで確認することが有効です。「未登録の端末である」など高リスクと判定された環境では、eKYC による本人確認へ誘導し、口座名義人本人であることを再度確認します。

Liquid の本人認証サービス「LIQUID Auth」では、公開鍵暗号を用いた端末認証により登録済み端末かを検証できます。また「LIQUID eKYC」と組み合わせることで、リスクに応じた本人再確認まで一連のフローとして設計できます。

パスキー運用における重要対策

パスキーはフィッシングに強い有効な認証技術です。一方、同期先のアカウントまで含めて侵害された場合に備え、「正しいパスキーか」だけでなく、「いつもの端末か」「本当に口座名義人本人か」を重ねて確認する設計が重要になります。

- ・新しいパスキーの登録・再登録時の本人性確認 eKYC だけでなく、eKYC 登録済容貌との顔認証 (AuthFace) も
- ・アカウントリカバリ時の eKYC 等による再本人確認
- ・未登録の端末からパスキーを利用する際の本人性確認 eKYC だけでなく、eKYC 登録済容貌との顔認証

(AuthFace) も

*16 複数の端末の間で、クラウドを介して自動的に同期されるパスキー

■ 今後の展開

Liquid は、eKYC、端末認証を組み合わせ、パスキー導入後の認証ライフサイクル全体の安全性向上を支援してまいります。

さらに、700 社を超える「LIQUID eKYC」の導入実績を元に、証券業界のみならず、銀行・信金等をはじめとする金融業界、ならびに EC サイト、電子チケット販売、Web メディア、SNS・ゲームなど、アカウントの不正利用が課題となる業界への提供を進めます。

■ パスキーでかわる、ログイン体験「LIQUID Auth Passkey」について

LIQUID Auth Passkey（リキッドオースパスキー）は、パスワード不要のセキュアな認証手段です。スマートフォンなどのデバイスに搭載された顔・指紋・PIN などの認証機能を活用し、ワンアクションで安全なサインインを実現します。ミッションクリティカルな堅牢さや安定性が求められるケースから、既存の認証方式からの移行の離脱率や利便性向上を目的としたケース、モバイルだけでなく PC や Web ブラウザ上でのサインインまで、さまざまなシチュエーションに対応します。

「LIQUID Auth Passkey」について：<https://liquidinc.asia/liquid-auth-passkey/>

■ 顔認証を、もっと安全に、もっと身近に クラウド型顔認証サービス「LIQUID Auth Face」について

「LIQUID Auth Face（リキッドオースフェイス）」は、顔認証を利用して、ネットバンキング、EC、ATM、オンライン試験、自動入退室管理などの幅広い場面において、サービスの利用者が利用開始時に登録された利用者本人であるかを確認するサービスです。高い信頼性が求められる金融領域で培ってきた安全性をそのままに、日常のさまざまなシーンで使える顔認証ソリューションを提供しています。

さらに、パスワードや SMS 認証に依存しない認証手段として、近年深刻化するフィッシングや SIM スワップといった不正リスクの低減にも貢献します。

「LIQUID Auth Face」について：<https://liquidinc.asia/liquid-auth/>

■ eKYC 市場シェア 7 年連続 No.1^{*17}である「LIQUID eKYC」について

ネット上の契約や口座開設時の身元確認をオンライン完結で行うサービスです。独自の AI・生体認証・OCR 技術により、ユーザーの離脱を最小限に抑えるスムーズな体験を実現。マイナンバーカード・運転免許証などの

本人確認書類の撮影、ICチップ読み取り、公的個人認証（JPKI）など多様な方式に対応しています。近年、生成AIの普及に伴い、不正やなりすましの手口が高度化・巧妙化するなか、券面の撮影だけでなくICチップを読み取ることで本人確認の確実性を高めるeKYCの必要性が一段と高まっています。フィッシング耐性のある多要素認証であるパスキーの登録時の本人確認や、アカウントリカバリ時の本人確認など、eKYCの活用シーンも急速に広がっています。ELEMENTSグループ合計で累計本人確認件数1.5億件、導入実績は700社を超えました。

「LIQUID eKYC」について：<https://liquidinc.asia/liquid-ekyc/>

公的個人認証について：<https://liquidinc.asia/jpki/>

***17 ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場 2026」eKYC市場：ベンダー別売上金額シェア（2019年度～2025年度予測）**

■ 株式会社 Liquid について

Liquidは、生体認証を活用し、認証を空気化することで、世界約80億人全ての人があるがままの状態であらゆるサービスを簡単・安全に使える、なめらかな社会の実現を目指しています。また、金融の取引時確認（犯罪収益移転防止法）、携帯電話契約（携帯電話不正利用防止法）、中古品買取（古物営業法）、不動産取引、CtoC取引などにおける本人確認のオンライン化の流れに合わせ、業界や導入事業者をまたがって横断的に不正検知を行う仕組みを提供し、利便性とセキュリティの両面を追求して参ります。

所在地：東京都中央区日本橋本町 3-9-4 日本橋ライフサイエンスビルディング 6

代表者：代表取締役 長谷川 敬起

設立：2018年12月

事業内容：生体情報、生体行動に特化した画像解析・ビッグデータ解析（LIQUID eKYC、LIQUID Auth等）

Web：<https://liquidinc.asia>

身元確認サービス「LIQUID eKYC」<https://liquidinc.asia/liquid-ekyc/>

所持認証サービス「LIQUID Auth Passkey」<https://liquidinc.asia/liquid-auth-passkey/>

クラウド型顔認証サービス「LIQUID Auth Face」<https://liquidinc.asia/liquid-auth/>

デジタルIDウォレット「PASS」<https://liquidinc.asia/smartcity/>

外国人向けデジタルIDウォレット「GPASS」<https://liquidinc.asia/gpass/>

■ 株式会社 ELEMENTS について

所在地：東京都中央区日本橋本町 3-9-4 日本橋ライフサイエンスビルディング 6

代表者：代表取締役社長 長谷川 敬起

証券コード：東証グロース市場 5246

設立：2013 年 12 月

事業内容：生体認証・画像解析・機械学習技術を活用した個人認証ソリューション、衣食住における個人最適化ソリューション、個人情報管理クラウドサービスの開発・提供

Web：<https://elementsinc.jp/>

※本プレスリリースに記載されている会社名および製品・サービス名は、各社の登録商標または商標です。

<本件に関するお問い合わせ先>

ELEMENTS グループ 広報（株式会社 Liquid）

E-mail：pr@elementsinc.jp