2026年５月14日

各　　位

東京都港区虎ノ門四丁目１番 28 号
日本通信株式会社
代表取締役社長兼ＣＥＯ　福田　尚久
（コード番号：9424）
問合せ先　執行役員ＣＦＯ　小平　充
電話 03-5776-1700

デジタルトラスト事業を担う連結子会社 my FinTech について
― 「日本通信ビジョン 2030」における my FinTech の役割 ―

日本通信株式会社（以下、「当社」という）は、５月７日に公表した「日本通信ビジョン 2030」で示した当社の競争力の源泉となるデジタル認証基盤、ならびに当該基盤を活用した事業展開において、デジタルトラスト事業の中核を担う my FinTech 株式会社（以下、「myFinTech」という）について、事業内容、株主構成、ならびに社会的役割をご紹介いたします。

1. my FinTech 株式会社について

myFinTech は、**電子署名法に基づく認定認証局**を運営する事業会社です。当社グループにおいては、競争力の源泉となるデジタル認証基盤を運営する**中心会社**として位置づけられ、携帯通信の認証の要である SIM の提供と、トラストサービス事業者としての認証局運営機能を一体で提供する、国内でも極めて稀有な事業基盤の構築・提供を目指しています。
設立から商用に至るまで相応の時間を要しましたが、これは認定認証局としての厳格な基準への適合、FPoS ライブラリの技術検証、ならびに金融・行政・医療といった高信頼領域での運用実績の積み上げに必要な期間であり、今般、社会実装フェーズに本格的に移行することから、改めて市場・パートナー各位にご紹介する運びとなりました。

2. 中核製品 ―― FPoS ライブラリ（４機能）

myFinTech の商品ポートフォリオの中核を成すのが、**FPoS ライブラリ**です。iPhone 及び Android スマートフォン用のアプリ開発者に提供されるライブラリ（ソフトウェア・コンポーネント）で、以下の４つの機能を一体で提供します。

機能	概要
① **身元確認**	公的個人認証（JPKI）等を用いた、本人実在性の確認（Identity Proofing）。eKYC・口座開設・行政手続等、サービス利用開始時に「その人が実在し、当該本人である

機能	概要
	こと」を確かな手段で確認する機能を提供します。
② 当人認証	iPhone/Android スマートフォンに内蔵された、ハードウェアで守られた秘密鍵を用いた、なりすましを許さない強固な当人認証（Authentication）。サービス利用の都度、「身元確認済みの本人がアクセスしていること」をハードウェア起点で証明します。
③ 電子署名	電子署名法に基づく認定認証局が発行する電子証明書を用いた、法的有効性を備えた電子署名。法的な契約から本人許諾・確認等幅広い分野で活用できます。
④ データ連携	めぶくグラウンド株式会社※1（以下、「めぶくグラウンド」という）が提供するデータ連携基盤と接続し、自己主権型 ID（ダイナミックオプトイン）に基づくデータ連携を実現する機能。利用者は必要な都度、自らの意思でデータ連携を許諾し、その許諾内容は認定電子証明書による電子署名で保全されます。データ連携基盤は許諾された範囲に限り事業者間を仲介する役割を果たし、利用者のオプトインが確認できる場合に限ってデータ流通が成立します。

※1 めぶくグラウンド株式会社：群馬県前橋市・民間企業・大学による官民連携会社。詳細は後述。

これら４機能は単独でも有用ですが、**FPoS ライブラリとして一体提供されることに本質的な価値**があります。すなわち、**「身元確認された本人」が、「当人認証」を経て、自らの意思によるデータ連携の許諾を「電子署名」によって行い、その結果として「データ連携」が許諾された範囲に限り成立する**という、利用者主権のトラストフローを端末側で完結させることができる点に、FPoS ライブラリの独自性があります。

とりわけ④データ連携機能は、**めぶくグラウンド**が提供するデータ連携基盤との接続により実現される、**自己主権型 ID（Self-Sovereign Identity）に基づくダイナミックオプトイン**の実装であり、利用者自身が必要な都度・必要な範囲で・必要な相手にのみデータ連携を許諾し、その意思表示を認定電子証明書による電子署名で確定させ、データ連携基盤が当該許諾の範囲内でのみ事業者間を仲介する、という構造をとります。これにより、金融・医療・行政・地域 DX 等の領域横断的なサービス連携を、利用者の主権を損なうことなく実現します。

■ データ連携のガバナンス ―― myFinTech とめぶくグラウンドの独立ガバナンス

データ連携基盤を提供する**めぶくグラウンドは、官民連携の事業会社**として設立されており、データの取り扱い方針および運用は、同社の**データガバナンス委員会（委員長：國領 二郎・慶應義塾大学名誉教授）**が決定する仕組みとなっています。これにより、データ連携基盤の運用は特定事業者の利害から独立し、利用者の主権と公共性に立脚したガバナンスのもとに置かれます。

FPoS ライブラリおよび認定認証局を運営する myFinTech と、データ連携基盤を運営するめぶくグラウンドが**別会社として設計されている**ことには、明確な制度設計上の意義があります。すなわち、**認証・電子署名の主体（myFinTech）とデータ連携・ガバナンスの主体（めぶくグラウンド）を構造的に分離する**ことで、データ連携に対する独立したガバナンスを効かせ、利用者にとっても、参加事業者にとっても、信頼に足るデータ流通の場を提供します。これは、特定事業者にデータが集中・寡占される構造を構造的に排除する、**日本型のトラスト・アーキテクチャ**の実装でもあります。

3. FPoS のセキュリティ構造 ――SSO 型 ID プロバイダーとの本質的な違い

FPoS の優位性を理解するうえで重要なのが、現在広く普及している SSO（シングルサインオン）型の ID プロバイダーとの構造的な違いです。SSO 型認証は利便性に優れる一方で、社会インフラとして用いるには**看過しがたい構造的脆弱性**を抱えています。FPoS は、これらの脆弱性をハードウェア起点のトラストによって構造的に解決する設計を採用しています。

	SSO 型 ID プロバイダー	FPoS
当人認証の主体	依拠する事業者は自ら当人認証を行わず、外部 ID プロバイダーの認証結果に依拠する。	事業者自身が、利用者の電子証明書による電子署名で当人認証（ログイン）を行うため、外部 ID プロバイダーに依拠しない。
秘密鍵・認証情報の所在	ID プロバイダーが認証情報を集中管理。利用者の認証情報が事業者側に保管される構造。	秘密鍵は利用者のスマートフォンのハードウェア領域（セキュアエレメント／SIM）にのみ存在。コピー不可。myFinTech を含む第三者は一切保有しない。
情報漏洩リスク	認証情報が一箇所に集中するため、外部攻撃のみならず内部犯行による漏洩が発生した場合、依拠する全事業者・全利用者に甚大な被害が波及。	そもそも秘密鍵を集中保管する場所が存在しない。漏洩しうる対象（鍵そのもの）が存在しないため、外部攻撃・内部犯行のいずれによっても、なりすましは構造的に不可能。
なりすましの可能性	認証情報の窃取・流出により、第三者が当該利用者になりすまして広範なサービスにアクセス可能となるリスク。	秘密鍵が利用者の物理デバイス内のハードウェア領域から取り出せないため、利用者本人の端末を物理的に保有しない限り、なりすましは原理的に不可能。

FPoS の本質は、**「秘密鍵が、それを使う利用者本人の手元から一歩も外に出ない」**という、セキュアエレメントの物理特性に基づく構造的なトラストにあります。秘密鍵はスマートフォンのハードウェア領域に格納され、コピーも抽出も不可能です。発行主体である myFinTech を含めて、いかなる第三者もこの鍵を保有しません。

また、依拠する事業者は、外部の ID プロバイダーの認証結果に依拠するのではなく、**電子証明書による電子署名でログイン（当人認証）を直接受け取る**ことができます。これにより、事業者は自らの責任のもとで当人認証を完結でき、第三者 ID プロバイダーへの依存に伴う認証主体の希薄化、ならびに集中型認証基盤の漏洩リスクから解放されます。これは、SSO 型認証では構造的に達成できない、**金融・医療・行政のような高信頼領域に求められるトラスト水準**そのものです。

4. FPoS サーバ ―― ライブラリに呼応する基盤システム

FPoS ライブラリ（クライアント側）と対をなすのが、myFinTech が運営する **FPoS サーバ**です。認定認証局としての証明書発行・失効管理、鍵のライフサイクル管理、署名検証、監査証跡の保全といった、トラストサービスの基盤機能を担います。クライアント側の FPoS ライブラリとサーバ側の FPoS サーバが密接に連動する

ことで、エンドユーザーの端末から認証局までの一貫したトラストインフラが完成します。

- **認定認証局機能：** 電子署名法準拠の証明書発行・運用
- **身元確認・鍵管理基盤：** 公的個人認証（JPKI）等を活用した身元確認、SIM／セキュアエレメントへの鍵プロビジョニング・更新・失効
- **認証・署名検証 API：** 金融機関・自治体・医療機関等の業務システムから容易に呼び出し可能
- **データ連携接続機能：** めぶくグラウンドのデータ連携基盤と接続し、認定電子証明書で署名された利用者のオプトイン許諾の発行・管理・検証を担う
- **監査・証跡管理：** 規制業界での利用に耐える、長期保存と検証可能性

5. 株主構成 —— 通信・金融インフラ・コンサルティングの戦略的連携

myFinTech は、日本を代表する通信・金融インフラ・コンサルティング各社による戦略的株主構成を有しています。各株主はそれぞれの領域の知見と顧客基盤を myFinTech に持ち寄り、FPoS の社会実装を多面的に支える体制を構築しています。

株主	事業領域・myFinTech における役割
日本通信株式会社（筆頭株主）	ネオキャリアとして 2026 年 11 月から自社 eSIM 基盤を運営する通信事業者。スマートフォン内蔵の安全なハードウェア領域に秘密鍵を格納する FPoS に加え、eSIM 内のセキュアエレメントを使う FPoS IoT を提供。
SocioFuture 株式会社（旧 日本 ATM）	金融機関向け ATM 運営・金融 IT で国内屈指の実績を持つ。金融現場における高信頼運用ノウハウと金融機関ネットワークを、FPoS の金融ユースケース実装に活用。
アクセンチュア株式会社	グローバル総合コンサルティングファーム。
合同会社デロイト トーマツ	総合コンサルティングファーム。トラストサービスのガバナンス、規制対応、リスク管理体制の構築に知見を提供。

通信キャリア（日本通信）、金融インフラ（SocioFuture）、グローバルコンサルティングファーム（アクセンチュア及びデロイト トーマツ）という、それぞれの領域で国内最高水準の実績を持つ 4 社が株主として名を連ねていることは、myFinTech が単なるスタートアップではなく、**日本社会全体のトラスト基盤を担う事業会社として設計されている**ことを示しています。

6. 日本通信ビジョン 2030 における戦略的位置づけ

日本通信は、ビジョン 2030 において「デジタルに『信頼』を取り戻す」取り組みを進めています。myFinTech は、その中で **FPoS というプラットフォームの提供主体**として、認証局運営とライブラリ／サーバの双方を一手に担う、ビジョン 2030 の実現に不可欠な存在です。

- **金融分野：** Zero Fraud Banking を実現する次世代認証基盤
- **医療分野：** 電子処方箋・健康データ共有におけるトラスト基盤
- **行政・地域 DX：** 地域社会 OS 実装における認証・署名基盤
- **IoT・モビリティ：** セキュアエレメントを起点とするデバイストラスト

日本通信は、myFinTech を通じて、**ハードウェア起点のトラストを社会全体に提供する事業者**として、引き続き積極的な事業展開を進めてまいります。今後、myFinTech から具体的なサービス開始・パートナーシップ締結等の発表を順次行ってまいりますので、ご注目をお願い申し上げます。

【my FinTech の会社概要】

会社名	my FinTech 株式会社
所在地	東京都港区
事業内容	電子署名法に基づく認定認証局の運営／FPoS ライブラリ及び FPoS サーバの開発・提供／関連トラストサービスの提供
株主	日本通信株式会社（筆頭株主）／SocioFuture 株式会社／アクセンチュア株式会社／合同会社デロイト トーマツ
親会社	日本通信株式会社（東証プライム市場：9424）

以上

■日本通信について

日本通信株式会社は、1996 年の創業以来、通信業界に革新をもたらし、MVNO 市場を切り拓いてきたパイオニアです。シンプルで合理的なモバイル通信サービスを中心に事業を展開し、安定した収益モデルを確立しつつ、さらなる成長を目指しています。特許技術を活用した無線専用線「閉域 SIM 間通信」やデジタル認証技術「FPoS」を強みとし、認証技術をコアにモバイル通信サービス及びデジタル認証基盤の提供にも注力しています。国際セキュリティ基準 PCI DSS 認定を取得したモバイル専用線は警察や銀行などの厳しい分野で採用。FPoS は世界最高水準のセキュリティと利便性を両立しています。「安全・安心にビットを運ぶ」というミッションのもと、国境を越えた安全なモバイル環境の社会インフラ構築を目指し、持続可能な成長と企業価値の向上に取り組んでいます。