2026年11月16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

不正アクセスに強い安全なログイン
FPoS による電子証明書型パスキーのご案内

2026年10月以降、連日のように不正アクセスによる被害が報道されており、多くの企業において対策を検討されているものと拝察いたします。
日本通信株式会社（以下、「当社」という）は、従来から、当社が特許を取得した技術である FPoS（FinTech Platform over Security module）による安全なログインを提供していますが、FPoS によるログインは不正アクセスへの対策としても役立てていただけるのではないかと思われますので、FPoS によるログインの仕組みについて、改めてお知らせいたします。

FPoS によるログインの仕組み

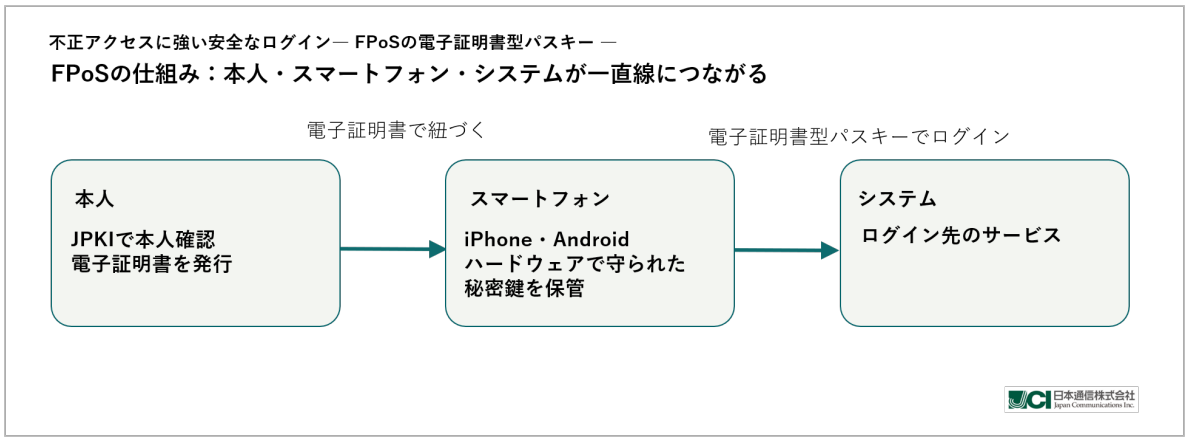
FPoS によるログインの仕組みは、以下のとおりです。

1. マイナンバーカードの公的個人認証サービス（JPKI）でお客様の本人確認を行い、電子署名法の認定を得た電子認証局（認定認証局）が、氏名、住所、生年月日が搭載された認定電子証明書を発行します。この際、認定電子証明書に対応する秘密鍵を、スマートフォン内の安全な（ハッキングされる恐れのない）領域に生成します。
2. 認定電子証明書に対応する秘密鍵を用いた電子署名を検証することでお客様の本人確認を行い、認定認証局が、氏名、住所、生年月日が搭載されない（個人情報を含まない）認証用の電子証明書を発行します(※1)。この際、認証用電子証明書に対応する秘密鍵を、スマートフォン内の安全な（ハッキングされる恐れのない）領域に生成します。
3. お客様がログインする際は、認証用電子証明書に対応する秘密鍵を用いた電子署名を検証することで、お客様本人に間違いないという当人認証を行います。

（※1）ひとつのデジタル ID で複数の電子証明書を使い分ける特許技術を用いています（2026年10月30日公表）。

FPoS によるログインは、PC やタブレット等のブラウザから利用することもできます（ブラウザの画面に表示された QR コードをスマートフォンで読み取り、電子証明書を利用していただきます）。

FPoS によるログインは、お客様の本人確認、電子証明書の発行、秘密鍵の生成、システムへのログインを一直線に結び付けるもので、「誰が、どのスマートフォンで、どのシステムにログインしているか」をひとつながりで確認するため、なりすましが入り込む隙がありません。FPoS によるログインは、いわば、「電子証明書型パスキー」と呼ぶことができます。



同期型パスキーと FPoS によるログインとの違い

警察庁などの公表資料によると、2025 年のフィッシング報告件数は約 245 万件に上り、証券口座への不正アクセスは約 1 万 8 千件に達しました (※2)。パスワードの使い回しやフィッシング等により認証情報が盗まれる事例のほか、二段階認証で用いられる SMS 認証が SIM スワップ等で突破される事例が報告されています。

(※2) 警察庁「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」、金融庁「インターネット取引サービスへの不正アクセス・不正取引にご注意ください」、フィッシング協議会「フィッシングレポート 2026」

同期型パスキーの普及により、証券口座等にログインする際のフィッシングへの耐性は大きく高まりました。しかしながら、同期型パスキーは、同期するアカウントが乗っ取られた場合は無力であり、使用する機器の機種変更や機器復旧時の再発行においても課題があります。

同期型パスキーと FPoS の違いは、以下のとおりです。

観点	同期型パスキー	FPoS（電子証明書型パスキー）
既存のアカウント（ID）との同期	あり	なし
本人確認の厳格性	同期するアカウント（ID）、SMS、メールアドレスに依存する (※3)	公的個人認証サービス（JPKI）による
秘密鍵の安全性	秘密鍵は安全に管理されるが、同期するアカウントが乗っ取られた場合は、不正利用されるおそれがある	秘密鍵はスマートフォン内の安全な領域で生成され、ハッキングされるおそれがない
結び付ける対象	パスキーを使用する機器とログインするシステム (※4)	お客様本人とパスキーを使用する機器とログインするシステム
機種変更または機器復旧時の再発行	同期するアカウント（ID）に依存する	公的個人認証サービス（JPKI）で本人確認を行い、電子証明書を再発行する

(※3) 同期型パスキーにおいて、公的個人認証サービス（JPKI）で本人確認を行うものもあります。
(※4) 同期型パスキーにおいて、公的個人認証サービス（JPKI）で本人確認を行う場合も、お客様本人とスマートフォン内の秘密鍵が電子証明書によって結び付くわけではありません。

FPoS は、電子証明書によって本人とスマートフォン内の秘密鍵を結び付けるため、お客様本人とログインするシステムを結び付けることができるほか、使用する機器の機種変更や機器復旧時においても、本人確認を起点として電子証明書を安全に再発行することができます。

当社が提供するサービスが、社会的な課題を解決する一助となりましたら幸いです。
当社は今後も、FPoS を通じて、安全で安心なデジタル社会の実現に取り組んでまいります。

■「FPoS」の導入に関するご相談窓口
my FinTech 株式会社 事業開発部
https://www.myfintech.co.jp/form/

■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。