



2025 年 2 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 福田 尚久
(コード番号：9424)
問合せ先 執行役員 C F O 小平 充
電話 03-5776-1700

日本通信、「デジタル認証モジュール」を提供開始
～ 「貴社のスマホアプリに組み込むことで、次世代標準となる DX 基盤を！」 ～

日本通信株式会社(以下、「当社」という)は、電子署名法の認定電子認証局を運営する当社子会社 my FinTech 株式会社、および産学官金連携会社で「めぶく ID」および「めぶくデータ連携基盤」を提供するめぶくグラウンド株式会社(本社：群馬県前橋市、代表取締役社長：木暮正樹)他との提携により、次世代標準となる DX 基盤「デジタル認証モジュール」を提供開始いたします。

「デジタル認証モジュール」は、スマホアプリの開発用ソフトウェアモジュールとして提供されます。現在スマホアプリを提供している企業他または新規にスマホアプリを提供する企業他は、当該モジュールを自社のスマホアプリに組み込んでご利用いただけます。

「デジタル認証モジュール」は、インターネットを安心して使いつつ、市民一人ひとりに個別最適化されたサービスを提供するための事業者を跨いだデータ連携を、利用者の明示的な同意(自己主権)のもとで実現します。これは、まさに長年にわたり理想とされてきたデジタル社会の実現に向けた大きな一歩です。

<現状の課題>

インターネット利用の大半がスマホへと移行した今日、多くの企業や自治体がスマホアプリを通じてサービスを提供しています。しかし、そこには2つの大きな課題が生じています。

・安全性の課題

利用者の個人情報や財産を扱うアプリでは、詐欺やハッキング等によるアカウントの乗っ取り事件が日々発生しています。安全性を高めるために二経路認証などのセキュリティ強化策が進められていますが、安全性の面で不十分である上に、ユーザーの利便性が損なわれ、使い勝手が低下しています。安全性を確保しつつ、同時に利便性を向上するにはどうしたら良いのか。これが一つ目の課題です。

・データ連携の困難さ

共通 ID を用いて複数の事業者間でデータ連携を行う場合、シングルサインオン事業者（共通 ID 事業者）に認証情報を送信する必要があり、認証を他者に依存する形になります。さらに、同一の ID およびパスワードを複数のサービスで使用することで、ひとたび認証情報が漏洩した場合、連携しているすべてのサービスに影響が及ぶリスクがあります。行政、金融、医療、交通その他の市民生活に密着した重要な分野において、データ連携が進んでいない大きな阻害要因になっています。

DX の目的の一つは、市民一人ひとりに個別最適なサービスを提供し、生活をより便利にすることにあります。しかし現状は「スマホアプリを安心して使えない」ことに加え、「データ連携ができない」という2つの課題により、DX は叫ばれながらも進展していないのが実情です。

<「デジタル認証モジュール」がもたらすメリット>

スマホアプリを提供しているすべての企業や自治体の皆様へのご提案です。

貴社のアプリに「デジタル認証モジュール」を組み込んでください。そうすることで、上記2つの課題を解決するだけでなく、以下の7つの重要なメリットがもたらされます。

- ① マイナンバーカードの署名検証（公的個人認証サービス：JPKI）による**確実な身元確認**が組み込まれます。電子署名法に基づく認定認証事業者である my FinTech 株式会社は、公的個人認証法第十七条第一項第四号に掲げる者として、公的個人認証サービスの提供が認められている署名検証事業者です。
- ② なりすまし、ハッキングできない**確実な本人認証（ログイン）**が組み込まれます。いわゆる ID・パスワードや二経路認証に依らない**確実な認証方法**です。
- ③ **PC から**お客様が安全、確実、簡単にログインする機能が組み込まれます
- ④ 他事業者とのパーソナルデータの**確実なデータ連携**が可能になります。一人ひとりに発行される一意の共通コードにより、事業者を跨いだデータ連携を実現します。なお、この共通コードを利用者が覚える必要は一切ありません。
- ⑤ データ連携可能な仕組みであるにも拘らず、**認証を他者依存することがなく**「独立性責任（Independent Responsibility）」を担保できます。共通 ID を用いる方法とは異なり、各サービス事業者がそれぞれ独自に認証を行い、自社内で認証を完結させることができます。
- ⑥ 自分に関するデータは自分自身がデータの利活用に関する権利を持ち、技術的にも実装すべきとの考え方、すなわちデータに関する自己主権を利用者が実現できるよう、お客様のデータ使用許諾をいつでも、どこでも可能にする**ダイナミック・オプトイン機能**を実装できます。明示的な同意によってのみ動作し、その意思が改ざんされることはありません。さらに、使用許諾の記録はエビデンスとして**確実に**保存され、透明性の高いデータ管理を実現します。
- ⑦ 電子署名法認定の電子証明書を使った**法的根拠を持つ電子署名機能**が組み込まれます。犯罪収益移転防止法、デジタル手続法、携帯電話不正利用防止法等の KYC に対応した、法的裏付けのある「認定電

子証明書」を利用することができます。

「デジタル認証モジュール」がもたらすメリットの詳細は、別紙をご確認ください。

<具体的な先行事例>

デジタルの最大の強みは個別最適化にあります。前橋市が提供した子育て給付金（自治体給付金）では、マイナンバーカード、自治体が保有する住民情報、めぶく ID、およびめぶくデータ連携基盤を活用し、「めぶく Pay」による給付申請時に給付対象者を自動識別する仕組みを導入しました。これにより、通常 1～2 か月かかる給付手続きが、申請受領後 1～2 週間程度で給付完了する迅速なサービス提供が実現しました。

このようなデータ連携の仕組みは、他の分野にも応用可能です。例えば、病院、薬局、交通、自治体などがデータ連携することで、高齢者の病院送迎や薬局での処方箋を個別最適化し、ワンクリックでの許諾によって手配できるワンストップサービスの提供も可能です。

<「デジタル認証モジュール」のご提供価格について>

スマホアプリによりサービス提供している企業や自治体において現在採用されている公的個人認証サービス(JPKI)およびセキュリティ対策にかかる費用の 4 分の 1 以下の価格にてご提供いたします。インターネットという社会インフラは、安全かつ安価に利用できるようにすべきであるとの当社の基本理念に基づくものであり、現在の主力事業であるモバイル通信サービス『日本通信 SIM』と同一の考え方に基づく提供方針です。

当社は今後も、安全・安心にビットを運ぶことを使命とし、サービス・製品を通じて社会に貢献し、持続可能な企業価値の向上を目指してまいります。

■「デジタル認証モジュール」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/お問い合わせフォーム>

■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。

※文中の社名、商品名は、各社の商標または登録商標です。

<「デジタル認証モジュール」がもたらすメリット>

スマホアプリを提供しているすべての企業や自治体の皆様へのご提案です。

貴社のアプリに「デジタル認証モジュール」を組み込んでください。そうすることで、上記2つの課題を解決するだけでなく、以下の7つの重要なメリットがもたらされます。

- ① マイナンバーカードの署名検証（公的個人認証サービス：JPKI）による**確実な身元確認**が組み込まれます。

マイナンバーカードの2024年12月末時点での保有率は77.1%で、有効申請受付数では約1億820万枚となり、人口の約86%を占めています。非対面で確実に身元確認できる方法が、これほど普及している国は他にありません。デジタル認証モジュールは、マイナンバーカードを利用した公的個人認証サービス（JPKI）を活用することで、従来型のeKYC、すなわち免許証等の写真をアップロードする方法に比べて比較にならないレベルの身元確認を提供します。電子署名法に基づく認定認証事業者であるmy FinTech 株式会社は、公的個人認証法第十七条第一項第四号に掲げる者として、公的個人認証サービスの提供が認められている署名検証事業者です。

- ② なりすまし、ハッキングできない**確実な当人認証（ログイン）**が組み込まれます。いわゆるID・パスワードや二経路認証に依らない確実な認証方法です。

システムへのログインでは、IDとパスワード、さらに二経路認証を使うのが一般的です。IDやパスワードをシステム側でデータベースとして保持し、ログイン時に入力されたIDとパスワード（さらに二経路目のパスワード他）が一致するか否かによってログインの可否を判別しています。しかし、この方法ではIDやパスワード、さらには二経路目の認証情報を中間者攻撃のような方法で盗むことが可能です。さらに不正アクセスの多くは内部犯行によるものであり、IDやパスワードが保存されたデータベース情報を内部から盗まれた場合には甚大な被害が生じます。

これに対して、デジタル認証モジュールが提供するログイン方法は、スマホの安全な領域に保持される秘密鍵と、その対となる公開鍵を記載した電子証明書を用いたハッキングできない仕組みでログインの可否を判別しています。具体的には、ログインを試みた場合、システム側からランダムな文字列がスマホに送信されます。この文字列をスマホ内の安全な領域に保持される秘密鍵で暗号化し、電子証明書とともにシステム側に送信されます。システム側は、電子証明書の有効性を確認するとともに、電子証明書に記載された公開鍵を使って復号します。復号された文字列がシステム側から送信したランダムな文字列と一致した場合には、電子証明書と一対になっている秘密鍵で暗号化されたことを証明できる、すなわち電子証明書の保持者であり、秘密鍵の保持者がログインを試みていることがわかるため、これによりログインを許可します。

この方法では、秘密鍵が盗まれない限り、インターネット上からのハッキングでなりすましのログインはできません。秘密鍵は、スマホの安全な領域（HSM：ハードウェアセキュリティモジュール）内で生成・保存されており、外部からのアクセスが極めて困難です。これにより、極めて高い安全性を確保するとともに、二経路認証のような不便を感じることなく簡便にご利用いただけます。

③ **PCから**お客様が安全、確実、簡単にログインする機能が組み込まれます

ログインを試みる PC 上に生成された QR コードを、デジタル認証モジュールを組み込んだスマホアプリで読み取ることで、上記②の説明と同じ認証プロセスを経たログインが可能です。QR コードで表現されている内容が上述のランダムな文字列として扱われ、スマホ内の秘密鍵で暗号化し、システム側に送信することでログインする機能です。

④ 他事業者とのパーソナルデータの**確実なデータ連携**が可能になります。一人ひとりに発行される一意の共通コードにより、事業者を跨いだデータ連携を実現します。なお、この共通コードを利用者が覚える必要は一切ありません。

上述の「データ連携の困難さ」での説明の通り、データ連携を行おうとすると共通 ID や統合 ID という概念を考えがちですが、認証という極めて重要な機能を他者（共通 ID 事業者他）に依存することになるため、重要な個人情報や金銭のような財産の運用に関わる分野では使用が難しく、データ連携が進まないのが今日の状況です。

マイナンバーカードの普及により、これを「トラストアンカー」として活用することで、一人ひとりに一意の共通コードを割り当てる仕組みを提供するのがデジタル認証モジュールです。このモジュールを組み込んだ様々なアプリには、その数だけ電子証明書が発行され、その中に共通コードが記載されています。これにより、事業者を跨るデータ連携を安全かつ確実に行うことが可能となりました。さらに、引越しなどでマイナンバーカードの電子証明書が更新された場合でも、本人の許諾があれば my FinTech 株式会社が運営する電子署名法認定の電子認証局が更新情報を取得することができます。引越前と後でマイナンバーカードの電子証明書が変更されても、デジタル認証モジュールの仕組みを活用すれば、同一人物であることを特定することが可能です。この仕組みにより、マイナンバーカードのトラストアンカー機能を発揮しながら、安全で信頼性の高いデータ連携を実現します。

⑤ データ連携可能な仕組みであるにも拘らず、**認証を他者依存することがなく**「独立性責任 (Independent Responsibility)」を担保できます。共通 ID を用いる方法とは異なり、各サービス事業者がそれぞれ独自に認証を行い、自社内で認証を完結させることができます。

共通 ID を使用する場合、複数の事業者が同一の ID とパスワードを共有し、分散されたデータを事業者間でデータ連携します。しかしながらこの方法の場合、例えば当社のような通信事業者は、通信という極めて重要なサービスを提供するための利用者認証を共通 ID 事業者に依存することになります。その場合、当社としての独立性責任を持つことができないため、現実的な選択肢にはなり得ません。ましてや、銀行などの金融機関や医療情報を管理する病院、さらには行政機関などで共通 ID を使うことが極めて困難な理由は、この独立性の欠如にあります。

一方、デジタル認証モジュールは、上述②の通り各事業者が自らの責任で認証を行う仕組みでありながら、電子証明書に記載の一意の共通コードによってデータ連携を実現するため、各事業者は独立性責任を果たすことが可能です。

⑥ 自分に関するデータは自分自身がデータの利活用に関する権利を持ち、技術的にも実装すべきとの考え方、すなわちデータに関する自己主権を利用者が実現できるよう、お客様のデータ使用許諾をいつでも、どこでも可能にする**ダイナミック・オプトイン機能**を実装できます。明示的な同意によってのみ動作し、その意思が改ざんされることはありません。さらに、使用許諾の記録はエビデンスとして

確実に保存され、透明性の高いデータ管理を実現します。

データ連携で最も重要な点は本人のデータ使用許諾です。今日一般的に使われている方法は、スマホでの利用の場合、アプリをダウンロードして使い始める際に提示される利用規約等において、データの使用許諾を求めている、利用者がこれに同意することでデータの使用許諾、オプトインを得ています。しかしながらこの方法で提示される利用規約等は、法律用語で、かつ抽象的に記述されているため、理解すること自体が難しいのが現状です。

これに対してデジタル認証モジュールは、現段階ではめぶくグラウンド株式会社が提供するめぶくデータ連携基盤を通して、必要な時に必要な内容に関して簡単に使用許諾を得られる仕組み、「ダイナミック・オプトイン」を実装しています。例えば A 病院で診察を受ける際に、一年前の検査データ（画像データや血液検査データ他）が B 病院に保存されている場合、そのデータを A 病院に送るということに関してデータの使用許諾を求められたら、どなたでも使用許諾の判断ができると思います。本来のデータ使用許諾は、このような「ダイナミック・オプトイン」であるべきだと考え、これを実装し、同時に広く提唱しています。

- ⑦ 電子署名法認定の電子証明書を使った[法的根拠を持つ電子署名機能](#)が組み込まれます。犯罪収益移転防止法、デジタル手続法、携帯電話不正利用防止法等の KYC に対応した、法的裏付けのある「認定電子証明書」を利用することができます。

例えば地方自治体が市民からの申請を受け付けるデジタル技術については、総務省令により、a) マイナンバーカードの電子証明書を使った署名検証、または b) 電子署名法の認定証明書を使った署名検証のいずれかと定められています。同様のことは、金融における犯罪収益移転防止法他でも定められています。

デジタル認証モジュールが提供する電子署名法の認定電子証明書は、法律により法的根拠が明確に示されています。これを活用することで、行政や金融をはじめとする様々な分野の DX が実現可能となります。

※文中の社名、商品名は、各社の商標または登録商標です。