Deloitte.
デロイト トーマツ

パスワードレス認証
―セキュリティ分野における次なるフロンティア―

デロイト トーマツ サイバー合同会社
2023年10月

目次

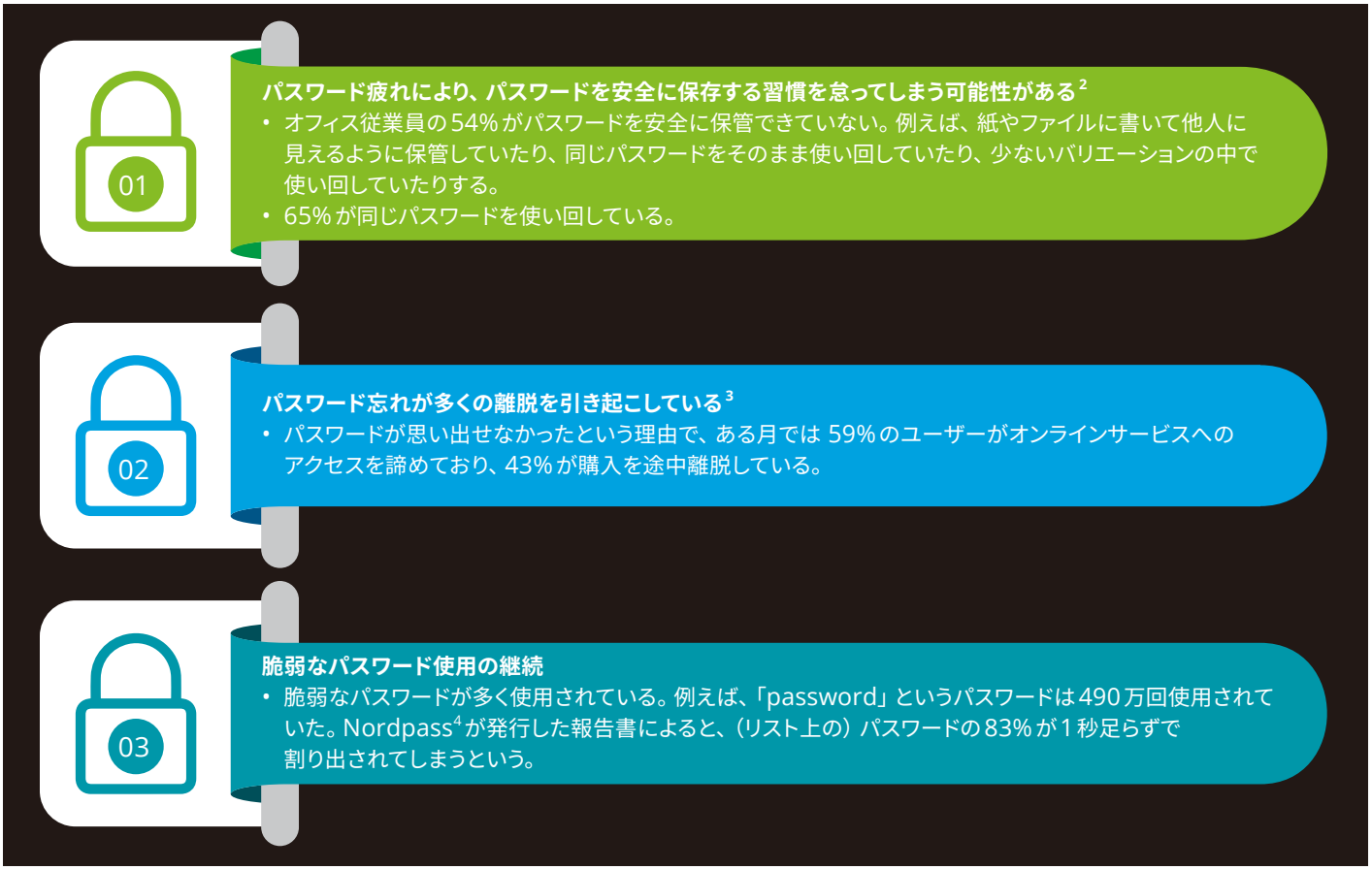
歴史に見るパスワードの意義

我々人類は、歴史の中で秘密のカフェや待ち合わせ場所から、軍の基地といった、アクセスに特別な許可が必要な場所に対してパスワードを用いてきた。パスワードの使用が初めて確認されたのは旧約聖書の時代にまで遡る。その当時、対立していた2つの部族が味方を識別するために合言葉を使用し、方言の違いから合言葉を正しく発音できなかった敵方を、効果的に特定していた。古代ローマの軍人も、合言葉を使用して味方を特定し、城門や軍の機密施設への通路を伝えていた。また、米国の禁酒法時代にも合言葉を知っている常連客のみが秘密の貯蔵庫やカフェに入室できるようにしていたことでも知られている。これが1960年代初期にコンピューターの世界に導入され、現在至るところで使用されるパスワードの歴史である。今日に至るまで、馴染みのある文字や言葉の組み合わせなど、我々が知っているものがネットの世界において我々のプライバシーを最前線で防御してきた。しかし、今こそこの古風な認証方法を放棄する時代が到来しているのではないだろうか。

今日のパスワードの課題

今日、パスワードは拡大するオンラインサービスへのメインゲートウェイであるとともに、あらゆる組織の「クラウンジュエル（守るべき最重要資産やデータ）」にもなっている。パスワードは一元的に管理され、システムとユーザーが知る共有秘密である。パスワードの安全性を確保することは、ユーザーとシステムの両者の責任であり、セキュリティーチームがパスワードの複雑性、有効期限、リカバリー等を考慮し導入した、複雑なポリシーに従うことが要求される。

エンドユーザーにとって、パスワードは漏洩しないことを目的とした複雑なルールに準拠するという、更なる負担を強いることになる。さらにこの負担には、パスワードを忘れた場合の複雑な検証プロセスの実施も含まれている。個人ユーザーは平均で22個のアカウントを所持しており、そのうち16個のアカウントでパスワードを使い回しているという結果がでている[1]。



ユーザーのフラストレーションやパスワード疲れが、パスワードの使い回しの多さや安全性の低い保存方法につながっている。そのためユーザーは、フィッシング詐欺やブルートフォースアタック（総当たり攻撃）によりソフトウェアプログラムを介してパスワードが盗まれるクレデンシャルベースの攻撃に脆弱になっている。

Verizonが発行した2022年データ漏洩／侵害調査報告書によると、パスワードは、まさにセキュリティの最弱リンクであり、データ漏洩の主な原因になっているという。同報告書によると、アプリケーションに対する攻撃の67%[5]がパスワードの侵害から生じたものであり、データ漏洩の82%において、認証情報の盗難やフィッシングとの関連が認められた[6]。

多くの組織ではパスワード侵害のリスク軽減に向け、ワンタイムパスワード（OTP）、認証トークン、プッシュ通知認証、認証アプリを使用した多要素認証（MFA）が導入されている。MFAは認証時のセキュリティに新たなステップが加わるため、フリクションやユーザーのフラストレーションを増加させてしまっている。そしてハッカーは今やアカウントやデータの漏洩を招き得る、プロンプト爆撃、フィッシング、SIMスワップ、アカウント乗っ取りといった巧妙なMFA回避手法を生み出している。

多くの認証手順がもたらすユーザーへの過度な負担を取り除き、現状の仕組みからパスワードを排除することは、今日の時代のニーズである。当該領域でパスワードレス認証の支持が高まりつつある一方、パラダイムシフト（時代の変化への対応）が今後も必要になるだろう。

1 Yubico and Ponemon：The 2020 State of Password and Authentication Security Behaviors Report（2020年パスワードと認証のセキュリティ行動の現状報告書）https://www.nass.org/sites/default/files/2020-04/Yubico%20Report%20Ponemon%202020%20State%20of%20Password%20and%20Authentication%20Security%20Behaviors.pdf
2 Google：https://services.google.com/fh/files/blogs/google_security_infographic.pdf
3 Verizon：2022年データ漏洩/侵害調査報告書 https://www.verizon.com/business/resources/reports/dbir/
4 https://nordpass.com/most-common-passwords-list/
5 Verizon：2022年データ漏洩/侵害調査報告書 https://www.verizon.com/business/resources/reports/dbir/
6 FIDO Alliance：https://media.fidoalliance.org/wp-content/uploads/2021/10/Online-Authentication-Barometer-Oct-2021.pdf

パスワードレス認証とは

パスワードレス認証はユーザーフリクションやWeakest Link（セキュリティの最も弱い箇所）の根本原因を取り除き、パスワードの記憶、保存、送信に加え、設定・再設定の際の複雑なルールへの準拠などの煩わしさを解消するものである。パスワードレス認証により、セキュリティやユーザーエクスペリエンスが向上するとともに、パスワードレスな世界が実現するだろう。

2025年までに、企業内の認証トランザクションの50%以上および一般消費者の認証トランザクションの20%以上でパスワードレス認証が使用されるようになると予想される[7]。

自社のIDやアクセスを管理するIT・サイバーセキュリティ専門家の31%が、パスワードレス認証はID関連活動の最優先事項であると考えている[8]。

FIDO（Fast Identity Online）Allianceにより、シンプルかつセキュアなパスワードレス認証方法とともに、FIDO2と呼ばれる最新の規格が導入された。FIDO2は、ユーザーが普段使用するノートパソコン、デスクトップPC、携帯電話等のデバイスを活用する。また、USB機器や、近距離無線通信（NFC）やBluetooth Low Energy（BLE）を介してユーザーを認証する外部認証器も利用できる。

FIDO Allianceは2013年に設立された組織で、現在、世界をリードするテクノロジー企業、業界団体、政府機関をメンバーに有している。そして、オープンな認証規格を促進し、世界の人々のパスワードへの過度な依存を軽減することを使命に掲げている[9]。

7 Gartner：You, Too, Can Start Enjoying the Benefits of Passwordless Authentication Today（あなたも、パスワードレス認証の恩恵を今日から享受しましょう）
https://www.forbes.com/sites/forbestechcouncil/2023/03/23/embracing-the-end-of-the-password-here-and-now/?sh=a2f93aa30e23
8 https://www.secureauth.com/resource-center/ebooks/esg-report-2022/
9 FIDO Allianceの概要：https://fidoalliance.org/overview/

図1では、デバイス上でのローカル認証や身近なプロトコルを介した接続を活用することで、FIDOがどのように一般的に使用されるデバイスを認証器として利用することを可能にしてきたのかをまとめている。

図1：FIDO認証器　プラットフォーム認証器　VS　ローミング認証器

プラットフォーム認証器

プラットフォーム認証器（内部認証器）は、ユーザーのデバイス（デスクトップPC、ノートパソコン等）に搭載されており、ユーザーはデバイスの生体認証機能（指紋認証、顔認証等）を使用するか、デバイス上でローカルPINを入力することで、認証を行うことができる。

ローミング認証器

ローミング認証器（外部認証器）とは、スマートカード、USB、携帯電話、スマートウォッチ等のデバイスを指す。これらの認証器はUSBを介してユーザーの機器に接続されるか、NFCやBLE経由で検出される。ユーザーは、指紋認証をはじめとするデバイスの生体認証機能やデバイスのローカルPINを使用して認証を行うことができる。モバイル端末をローミング認証器として使用する際は、端末が対応する顔認証や網膜認証等が使用できる。

FIDO2のサポート

ユーザーは指紋・顔スキャン等での認証、または、認証器上の覚えやすいローカルPINでの認証から選択できる。ローミング認証器は、USB、NFC、BLEを介して接続できる。

FIDO2の導入前は、スマートカード、証明書ベース認証、マジックリンク等によりパスワードレスなソリューションが提供されていたが、これらの方法には所有権が存在し、ブラウザやオペレーティングシステムを横断する移動は不可であったことから、ベンダーロックインの原因となったほか、フィッシング耐性やFIDO2と同等の安全性を備えていなかった。

認証の仕組み

FIDO認証器を使用したログインを行うには、ユーザーはウェブ、SaaS、モバイルアプリ等のサービスに認証器を登録する必要がある。

ユーザーは、ビジネス要件やセキュリティ要件に基づき、プラットフォーム認証器やローミング認証器に登録を行い、PIN、指紋スキャン、パターンのスワイプ等から使用したいローカル認証方法を選ぶことができる。ユーザーがサービスに登録する際は、暗号鍵ペア（公開鍵と秘密鍵）が生成され、ユーザーのデバイスに安全に保存されるようになっている。この鍵ペアはFIDO認証情報、またはシンプルにパスワードレス認証情報と言われる（図2）。

図2：FIDO2認証情報のユーザー登録

パスワードレス認証用にデバイスを登録すると、ユーザーは指紋、PIN、顔スキャンなど、登録したデバイスが対応する方法でサービスにログインすることができる。この裏では、FIDO2が標準的な公開鍵暗号方式を使用し、保存された認証情報を基にユーザーを認証している。

パスワードレス認証情報はデバイスとサービスごとに登録する必要があることからユーザーにとって煩わしい作業になる可能性があり、デバイスの盗難や置き忘れがあった場合においては、レガシーパスワードのような安全性の低いリカバリープロセスに依存することになりかねない。

この問題に対処するため、FIDO2はマルチデバイス対応の検出可能な認証情報（パスキー）を導入した。パスキーはユーザーのクラウドサービスプロバイダー内で安全に保管され、デバイスを交換したり、盗難に遭ったりした際にもユーザーが使用できるようになっている。ユーザーがパスワードレス認証情報を自身の携帯電話に登録し、別のデバイスから同じアプリケーションにアクセスした場合、ユーザーが希望すれば、その携帯電話から登録した認証情報を使用するよう促される。BLEやNFCを介して認証情報を検出するには、モバイル端末とノートパソコンの双方が物理的に近くに置かれている必要があるため、パスキー使用の全行程は、簡単かつユーザーフレンドリーでありながらも、安全性が高くなるよう設計されている。

パスワードに代わる認証方式として、パスキーは主要な多国籍テクノロジー企業[10]で採用されており、各社のプラットフォームに導入されている。

[10] https://fidoalliance.org/tech-times-apple-google-and-microsoft-are-pushing-passkeys-passwordless-future/

パスワードレス化のメリット

パスワードレス認証はセキュリティとプライバシーの均衡を保つとともに、ユーザーエクスペリエンスの向上や統合・導入の簡易化を実現することから、パスワードに代わる強力な選択肢となっている。

図3：FIDO2のメリット

ユーザー体験がフリクションレスに

- ユーザーは生体認証、PIN、パターンなど、自身がデバイス上で安心して使える認証方法を選択することができる

- 検出可能な認証情報により、ユーザーはデバイス間で同じ認証情報を使用してサービスにアクセスできる

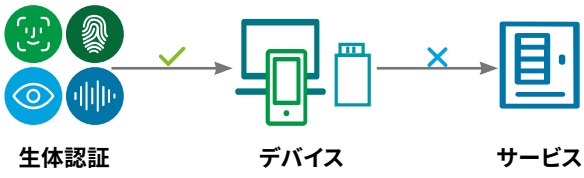
セキュリティの向上

- FIDO2は、2つの認証要素を組み合わせた多要素認証を使用する設定になっている

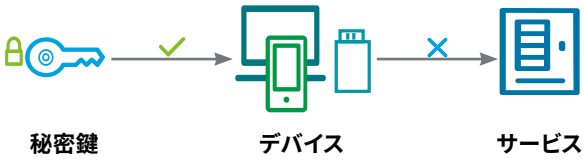
- 攻撃者が盗難可能な共有秘密やパスワードが存在せず、登録時やログイン時に認証器が物理的に近くに置かれている必要があるため、耐フィッシング性が高い

プライバシー バイ デザイン

- ユーザーの生体認証データはデバイス上でローカルに保管される



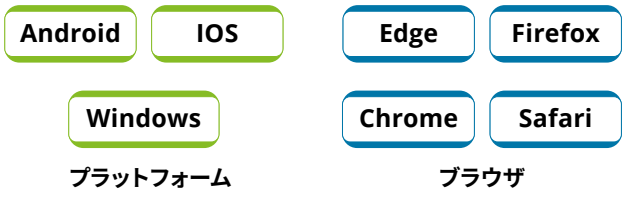
- ユーザーのFIDO認証秘密鍵はデバイスから移動しない



- サービスごとに異なるFIDO認証情報を使用しているため、ユーザーアクティビティの追跡ができない

統合や導入の簡易性

- 主要なプラットフォームやブラウザがFIDO2に広く対応している



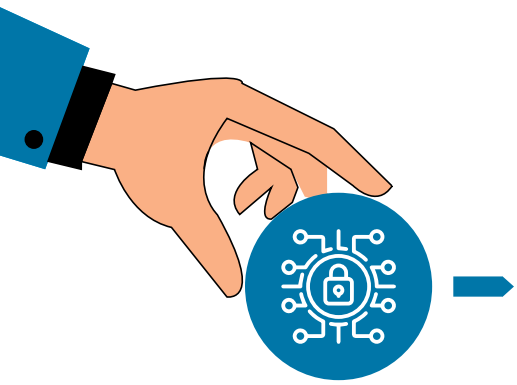
- 簡単なJavaScript API呼び出しを行うことで、ウェブサイトやアプリケーションでのFIDO2サポートの構築が可能になる
- 主要なアクセス管理ベンダーや認証技術ベンダーがFIDOに対応している

パスワードレス化を推進する際に考慮すべき重要事項

組織がパスワードレス化を推進するにあたり、ユーザーエクスペリエンス、セキュリティ、テクノロジー面での準備にどのように取り組むのかについて、注意を払う必要がある。主な重要事項は以下の通り。

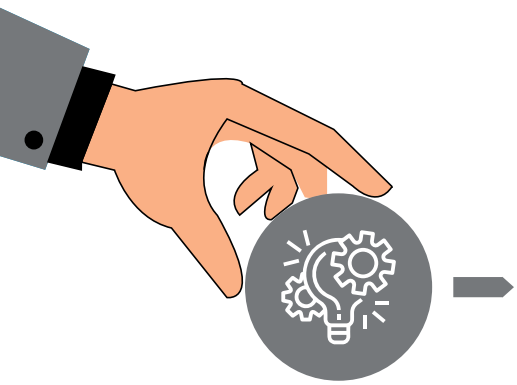
ユーザーエクスペリエンス

- ユーザーがパスワードレス化を支持し、採用するかは、いかに簡単に新しい認証方法へ移行できるかに左右されるだろう。移行の簡易化にあたり、PIN、指紋スキャン、顔認証など、ユーザーが慣れ親しんだ方法で認証を行えるようにする必要がある。
- 生体認証やNFC、BLEといった新しい技術を安全に使用するためには、ユーザー層に応じたラーニングカーブを考慮する必要があり、トレーニングが必要となるだろう。組織はFIDO Alliance UX Guidelines（FIDO Allianceのユーザーエクスペリエンスに関する指針）[11]を活用することで、一貫したユーザーエクスペリエンスの設計を実現し、導入の最大化を促進することができる。



セキュリティ

- デバイスの故障、紛失、交換に係るリカバリープロセスは、適切に設計され、安全なものでなければならない。ユーザーを認証情報ベースの攻撃の危険に晒し得るパスワードや古いリカバリー方法に依存させてしまうことはあってはならない。
- 重要なアプリケーションや金融系アプリケーションを対象に、適応型認証や行動的生体認証に係るレビューを実施する必要がある。これは、潜在的なバッドアクターによるユーザーの認証器や認証情報へのアクセスを防ぐうえで役立つだろう。
- 新たな攻撃ベクトルに関する最新情報を常に入手し、将来を見越したリスク緩和フレームワーク・計画を策定することは極めて重要である。さらに、全体的なリスク管理プロセスにおいて、定期的なセキュリティレビューを計画し、全体的なセキュリティ態勢の見直しについても検討する必要がある。



テクノロジー

- FIDO2はほとんどのプラットフォームとブラウザ[12]でサポートされているが、旧バージョンの場合動作するとは限らない。同様に、パスキー[13]の導入状況もプラットフォームベンダーによって差異がある。組織はパスワードレス化の推進を計画すると同時に、社内で最も使用されているプラットフォームとブラウザのバージョンを確認する必要がある。
- 自社のパスワードレス認証への対応状況を理解するうえで、組織はオンプレミスとクラウドの両方で、所有するアプリケーションの現状を評価する必要がある（パスワードベースの古いアプリケーションの見直し等）。最新のアプリケーションであっても、基本バージョンではパスワードレス認証をサポートしていない可能性や、この機能の有効化にあたり追加コストが必要になる可能性もある。

11 FIDO Alliance: https://fidoalliance.org/ux-guidelines/
12 https://webauthn.me/browser-support
13 https://passkeys.dev/device-support/

パスワードレス認証を様々な業界で導入することは可能だろうか

FIDO2パスワードレス認証は、あらゆる状況で普遍的に適用可能であり、従業員と顧客の双方に適応することができる。また、業界、ユーザーの期待、セキュリティ、規制要件に基づき、カスタマイズしていく必要がある。

従業員にとって、パスワードレス認証の導入は、フリクションの軽減、リモートワークの実現、ヘルプデスクのパスワードリセット関連のコスト削減、パスワードリセットに費やす時間の短縮に役立つだろう。

- プラットフォーム認証器は、在宅勤務やオフィス勤務を問わず、自身専用のノートパソコンやデスクトップPCを所有する従業員に最適である。
- ローミング認証器は、コールセンター、ITアウトソーシング、小売業の現場担当者等、機器を共有する従業員に導入できる。小売業ではユーザーIDの共有が一般的であるが、説明責任の所在が不明確になり得るため、導入はその改善に役立つだろう。
- 携帯電話をローミング認証器として使用することで、組織はリモートでの安全なログイン、特権アクセス、重要なインフラアクセスに広く使用されてきたハードウェアトークンを段階的に廃止することができる。
- パスキーは、ユーザーデバイスのクラウドサービスに保管され、組織での管理は行われないため、セキュリティの観点から使用許可が下りない可能性がある。したがって、組織の従業員への展開は推奨されない。

ベンダーやパートナーにおいても同様で、自身のデバイスを使用して認証を行うことで、ログインに関する問題の連絡や解決に係る運用コストの削減が促進されるだろう。

顧客にとっては、複数のデバイスからサービスにアクセスできるようにするフリクションレスな体験の実現が最優先事項である。組織はこの体験を安全に提供することを目指しており、パスワードレス化がこの実現を促進するだろう。

- リテールバンキング、eコマース等のB2C領域で事業を行う組織は、パスワードレス化を推進することで、顧客認証情報の盗難に係る漏洩リスクの軽減に役立てられるだろう。そして、プラットフォーム認証器、ローミング認証器、パスキーに関連するFIDO2機能の導入を検討することで、安全かつシームレスなユーザーエクスペリエンスを実現できるだろう。
- 銀行や電気通信業界等の規制産業では、顧客認証の単一要素としてのFIDO2規格について、規制当局の承認が正式に得られていない場合があるため、導入は困難になる可能性がある。パスキーの容認についても同様の課題に直面するだろう。
- FIDO認証器として使用する携帯電話等のFIDO2ローミング認証器は、SMS OTP以上のセキュリティを実現することから、規制産業、非規制産業を問わず、SMS OTP[14]に代わる2要素認証方法と見なされるだろう。

[14] FIDO2 Authentication in line with RBI Master Directions（インド準備銀行のマスターディレクションに準拠したFIDO2認証）：
https://media.fidoalliance.org/wp-content/uploads/2022/09/FIDO-White-Paper-_-FIDO-Authentication-in-Digital-Payment.pdf

パスワードレスな組織を実現するための準備

パスワードレス認証への移行は単なる技術変更ではなく、ユーザー、セキュリティ、ビジネス、テクノロジーチーム等のあらゆるステークホルダーの意識変革でもある。パスワードレス認証の導入を検討している組織は、自社の導入戦略を策定すると同時に、以下を考慮する必要がある。

プログラムが掲げる目標と成果を定義する
組織のビジョン、ビジネス、セキュリティ、プライバシー、ユーザビリティ、規制要件を理解し、プログラムが掲げる目標と期待される成果を定義する。これには、ユーザーエクスペリエンスの向上、ヘルプデスクのコスト削減、サイバーセキュリティの脅威に晒されるリスクの軽減などが挙げられる。

プラットフォームベースのアプローチを採用する
アクセス管理プラットフォームにより、パスワードレス認証とパスワードベース認証の両方が可能になるため、導入を柔軟に進めることが可能となる。アクセス管理プラットフォームや認証専門ベンダーはFIDO2に対応しており、プロトコルやテクノロジーの進化の中で自社製品を強化してくだろう。

小さく始めて、成功を積み重ねる
ビジネスに最大のインパクトをもたらし、ユーザー層に最適で、技術面でも適応するアプリケーションを特定する。初めて成し遂げた成功から学習し、その成功を基に、最終的には段階的な方法でパスワードレス認証を企業環境全体に拡大させていく。

現実的かつ達成可能な導入目標を設定する
パスワードレス認証への移行は単なる技術変更ではなく、意識改革でもある。パスワードレス化の実現において、PCログイン時のMFAの使用から着手する。一方で、ユーザーがパスワードを引き続き使用できるよう選択肢も残しつつ、導入が進み成熟度が高まるにつれて段階的にパスワードを廃止していく。

ユーザーエクスペリエンス、コミュニケーション、トレーニングに主眼を置き、導入を最大化させる
パスワードレス化の実現には、エンドユーザーがパスワードレス認証を支持し、導入していくことが不可欠である。時間をかけてユーザーの意識を高め、導入に向けたガイドラインを展開することが重要である。

プログラムで収めた成功を評価しレビューする
ユーザーからのフィードバックを求め、改善に向けて課題と学習内容を振り返る。プログラムで収めた成功の評価・報告を行うため、アプリケーションごとのパスワード使用率やパスワードレスでの登録・ログイン数などの評価基準を構築する。

完全なパスワードレス化に向けた準備はできているだろうか

各ベンダー、プラットフォーム、アプリケーションがFIDOプロトコルのサポート構築を進めるに伴って、パスワードレス認証のサポートも徐々に広がっている。導入コスト、規制ガイドライン、ユーザーの準備状況などの要因が本格的な導入に影響を及ぼす可能性があるが、基本認証要素と先進認証要素はパスワードレス認証が受け入れられるようになっても引き続き共存することになるだろう。組織は、全体的なセキュリティとユーザーエクスペリエンスの改善に向け、パスワードレスログイン導入の検討に着手する必要がある。そして、パスワードレスな組織へのスムーズな移行に向け、アクセス管理ベンダーや認証専門ベンダーが提供するフレームワークやアーキテクチャの活用も考慮すべきである。

連絡先

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

星澤 裕二
パートナー　Cyber Advisory
デロイト トーマツ サイバー合同会社
yuji.hoshizawa@tohmatsu.co.jp

Tarun Kaura
Leader – Cyber Advisory, Risk Advisory
Deloitte India
tkaura@deloitte.com

Anand Venkataraman
Partner, Risk Advisory
Deloitte India
anandv@deloitte.com

櫻田 仁詩
シニアマネジャー　Cyber Advisory
デロイト トーマツ サイバー合同会社
hitoshi.sakurada@tohmatsu.co.jp

寄稿者

Sabiha Hetavkar

Deloitte.

デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイトアジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、(www.deloitte.com）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301