

# SafeNet FIDO2 デバイス パスワードを排除してセキュリティを強化



2020年代に向けて、企業は自社のデジタルトランスフォーメーションを拡大してクラウドに移行しつつあり、セキュリティ侵害の大部分がID盗難に関連するものとなってきています。多くの組織は、PKIベースの認証など、強力な認証方式に投資してきました。

これらの組織は現在、新しいユースケースに対応し、同時にセキュリティと利便性の最良なバランスを維持するという課題に直面しています。

すべてのデバイスから、シームレスでパスワードを入力しない、パスワードレスログオン環境を実現するにはどうすればよいでしょうか。自社の認証方式を捨てて置き換えることなく、新しいユースケースに対応するにはどうすればよいでしょうか。タレスはデジタルセキュリティの世界最先端の企業として、SafeNet IDPrime 3940 FIDO(スマートカード)とSafeNet eToken FIDO(USBトークン)という2つのSafeNet FIDO2デバイスによって対処します。これらの新しいソリューションにより、組織はクラウドを採用してもセキュリティ保護され、また統合されたアクセス管理および認証製品を通して、ハイブリッド環境全体をセキュリティ保護されたアクセスで結ぶことができます。

## パスワードレス認証

パスワードレス認証では、パスワードを他のID確認方法に置き換え、確実性と利便性を向上させます。この種類の認証には、ユーザーのログインを簡略化し、テキストベースのパスワードの本質的な脆弱性を克服できる大きな利点があることから、採用が広がっています。長所として、手間が少なくなる、各アプリにより高いレベルのセキュリティが与えられる、従来型のパスワードが不要になるなどが挙げられます。

## PKI顧客向けの利便性

このソリューションの特に大きな利点の1つは、PKI 認証を使用している組織が、PKI とFIDO を組み合わせたスマートカードを使用して、ユーザーが単一の認証機器で従来型のアプリ、ネットワークメイン、クラウドサービスにセキュリティ保護されたアクセスを行えるようにすることにより、クラウドとデジタルトランスフォーメーションを推進できることです。

## FIDO2 とPKI をサポートするオールインワンデバイス

SafeNet IDPrime 3940 FIDO スマートカードは、PKI ベースのアプリケーション用に設計されました。SafeNet ミニドライバが付属し、追加のミドルウェアなしにMicrosoft®環境をネイティブでサポートしており、完全な統合を行えます。

このデュアルインターフェイスのスマートカードは、接触型インターフェイスでも非接触型ISO14443インターフェイスでも通信を行え、一部のNFCリーダーとも互換性があります。

SafeNet IDPrime 3940 FIDO スマートカードは、Java プラットフォーム用にCC EAL5+/PP Java Card 認定、Java プラットフォームとPKI アプレットの組み合わせ用にCC EAL5+/PP QSCD 認定済みです。SafeNet IDPrime 3940 はFrench ANSSI により認定済みで、eSignature およびeSeal アプリケーションの両方についてeIDAS規制に従い認定済みです。さらに、SafeNet IDPrime 3940 FIDO はFIDO2.0及びU2F 標準をサポートしています。

## タッチセンスオプション付きのUSBトークン

SafeNet eToken FIDO はUSBトークンで、従業員向けのパスワードなし認証の導入を考えている企業に理想的なソリューションです。この認証機器は、小型の在席検出機能付きタンパーエビデント(不正改造防止)USBで、ユーザーの所有物(物理トークン)、ユーザーの知識(PIN)、ユーザーの行為(トークンに触れる)という3要素を確認します。

### 主要な利点

SafeNet FIDO2 デバイスを使用すると、企業はあらゆる環境で強力な、セキュリティ保護されたパスワードなしの認証を使用できます。

次のような主要な利点があります。

- PKI とFIDO を組み合わせたスマートカードにより、クラウドを採用してもセキュリティ保護され、またハイブリッド環境の全体をセキュリティ保護されたアクセスで結合
- 複数のオペレーティングシステムに簡単にアクセスでき、セキュリティを保護
- クラウドのアプリやネットワークドメインにパスワードなしでアクセス
- 現行のPKI 認証スキーマを活用できるため、完全な置き換えが不要
- ユーザーのすべての要求に、単一の認証機器で対応
- CC 認定済み
- すべてのデバイスとOS をサポート(ミドルウェアの導入が不要)
- 完全にカスタマイズ可能
- デジタルシグネチャや電子メール暗号化に理想的

## 製品の特徴

## SafeNet IDPrime 3940 FIDO スマートカード



メモリ	<ul style="list-style-type: none"><li>SafeNet IDPrime 3940 は400KBのJava フラッシュメモリチップを基礎としています。標準のSafeNet IDPrime 3940 FIDO には、20キーのコンテナが付属します。</li><li>この標準構成では、証明書や他のアプレットとデータのため73KBを使用可能です。</li></ul>
標準	<ul style="list-style-type: none"><li>BaseCSPミニドライバ(SafeNetミニドライバ)</li><li>Global Platform 2.2.1</li><li>Java Card 3.0.4</li><li>ISO 7816およびISO 14443</li><li>FIDO2.0及びU2F準拠</li></ul>
オペレーティングシステム	<ul style="list-style-type: none"><li>FIDOアプリケーションは、Windows 10 および他のFIDO 準拠のオペレーティングシステムでサポートされています。</li><li>標準PKIアプリケーションは、Windows、MAC OS X、Linuxでサポートされています。</li></ul>
暗号化アルゴリズム	<ul style="list-style-type: none"><li>ハッシュ: SHA-1、SHA-256、SHA-384、SHA-512</li><li>RSA: RSA 4096ビットまで</li><li>RSA OAEPおよびRSA PSS</li><li>P-256ビットECDSA、ECDH。P-384およびP-521ビットECDSA、ECDHはカスタム構成で利用可能</li><li>オンカードの非対称キーペアの生成 (RSA 4096ビットまで、楕円曲線521ビットまで)</li><li>対称: AES - セキュリティ保護されたメッセージングとMicrosoft Challenge/Response専用の3DES</li></ul>
通信プロトコル	<ul style="list-style-type: none"><li>T=0、T=1、PPS、3.57MZで最高446Kbpsのポーレート (TA1=97h)</li><li>T=CL、ISO 14443 type A、最高速度848 Kbps</li></ul>
その他の機能	<ul style="list-style-type: none"><li>オンボードのPINポリシー</li><li>マルチPINのサポート</li><li>SafeNet IDPrimeファミリのカードは、お客様の必要に合わせてカスタマイズ可能(カード本体とプログラミング)</li></ul>

## チップの特徴

技術	<ul style="list-style-type: none"><li>組み込みの暗号化エンジンによる対称および非対称暗号化</li></ul>
寿命	<ul style="list-style-type: none"><li>最小500,000回の書き込み/消去サイクル</li><li>最短でも25年間データを保持</li></ul>
認定	<ul style="list-style-type: none"><li>CC EAL6+</li></ul>
セキュリティ	<ul style="list-style-type: none"><li>SafeNet IDPrimeスマートカードは、サイドチャネル攻撃、侵襲性攻撃、高度なフォルト攻撃、その他の種類の攻撃に対して、複数のハードウェアおよびソフトウェアによる対策を内蔵しています。</li><li>The SafeNet IDPrime 3940 FIDOはJavaプラットフォーム用にCC EAL5+/PP Java Card認定済み、JavaプラットフォームとPKIアプレットの組み合わせ用にCC EAL5+/PP QSCD認定済み、eSignatureとeSealの両方についてeIDAS認定済みで、French ANSSIにより認定済みです。</li></ul>

## 製品の特徴

## SafeNet eToken FIDO



メモリ	• 90K
標準	• APIおよび標準のサポート: FIDO2.0及びU2F
オペレーティングシステム	• FIDOアプリケーションは、Windows 10および他のFIDO準拠のオペレーティングシステムでサポートされています。

## 物理的特性

寸法	• 6mm*8mm*40.5mm
動作温度	• 0°C~70°C (32°F~158°F)
保存温度	• 40°C~85°C (-40°F~185°F)
湿度定格	• 0~100%、結露なきこと
防水等級	• IP X7 – IEC 529 -
USBコネクタ	• USB type A、USB 1.1と2.0をサポート (Full speed)
筐体	• 硬質鋳造プラスチック、タンパーエビデント (不正改造防止)
メモリのデータ保持期間	• 最短10年間
メモリセルの書き込み回数	• 最低500,000回

SafeNet IDPrime 3940 FIDO/SafeNet eToken FIDOは、Microsoft Azure Active Directoryアカウントと互換性があります。

## タレスのSafeNetアクセス管理および認証ソリューションについて





タレスの業界最先端のアクセス管理および認証ソリューションは、企業がエンタープライズIT、Web、およびクラウドベースのアプリケーションへのアクセスを集中管理し、セキュリティを保護するためのソリューションです。ポリシーに基づくSSOと汎用的な認証手法を活用することで、企業は侵入を効果的に防止し、クラウドへの移行を安全に行い、規制への準拠を簡素化できます。

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。

その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー

## タレスについて

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

Contact us – For all office locations and contact information, please visit [cpl.thalesgroup.com/contact-us](http://cpl.thalesgroup.com/contact-us)