Solution Brief

Thales FIDO2デバイス: 強力なパスワードレス多要素認証によるフィッシング攻撃の阻止

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Member of
Microsoft Intelligent Security Association

Microsoft

デジタルトランスフォーメーションを拡大している企業は、あらゆる場所からのアクセスと運用コストの削減を実現するためにアプリケーションとデータをクラウドに移行しています。ユーザーがますます多くのクラウドベースのアプリケーションにログインするようになった今、個人情報の盗難やセキュリティ侵害の主な原因として脆弱なパスワードが浮かび上がってきました。

ThalesのFIDO2デバイスはこのリスクに対処するために、パスワードレスの耐フィッシング認証を提供します。企業はこのデバイスにより、アカウントの乗っ取り防止と、SaaSアプリケーションやWindowsエンドポイントといった機密リソースへの不正アクセスのリスク排除が可能になります。

Thales FIDO2デバイスは同時に複数のアプリケーションをサポートします。FIDO2、U2F、PKI、R-FIDを組み合わせたものを使用して、物理的スペースと論理的リソースの両方にアクセスします。

パスワードレスFIDO2認証

FIDO2認証は、脆弱なパスワードをフィッシング耐性のあるWebAuthnクレデンシャルに置き換えることで、アカウントの乗っ取りリスクをなくします。

FIDO2認証はユーザーのログイン体験を容易にし、パスワード固有の脆弱性を克服するという大きな利点があるため、MFAの最新形態として支持を集めています。その利点には、ユーザーにとって摩擦が少ないこと、フィッシング攻撃に対する高い防御力などが挙げられます。

厳格なコンプライアンスに準拠

Thales FIDO2セキュリティキー、USBトークン、スマートカードにより、あらゆる規制ニーズに対応することができます。どのデバイスもFIDO2およびU2F認証を取得しています。PKIとFIDOを組み合わせたデバイスはNISTの規制に準拠しており、FIPS 140-2またはコモンクライテリア（CC）認証のほか、JavaプラットフォームとPKIアプレットに対してANSSI認証を取得してます。また、電子署名アプリケーションとeシールアプリケーションの両方でeIDAS規則の要件に準拠にしています。

さまざまなユーザー認証の目標達成を実現

Thalesは種類豊富なFIDOデバイスによって、数多くのパスワードレス認証における目標達成を支援しています。

SaaSアプリへのセキュアなアクセス

ユーザーの大半はアプリ間で同じパスワードを使い回しているため、ユーザーにFIDO認証機能を提供することで、セキュリティを劇的に向上させ、ヘルプデスクへの問い合わせを減らすことができます。

フロントラインワーカー向けのネットワークログイン

FIDO2セキュリティキーはパスワードレスMFAを提供し、フロントラインワーカーなどのユーザーがWindows PCやタブレットといった共有デバイスに安全にアクセスできるようにします。

物理的アクセスと論理的アクセスの両方に対応

Thales FIDOスマートカードは、利便性を高めるために物理アクセスをサポートしており、ユーザーはカスタマイズ可能なスマートカード1枚で物理的スペースと論理的リソースの両方にアクセスすることができます。

PKI/CBA環境を近代化

PKIと証明書ベース認証（CBA）に依存している企業は、PKIとFIDOを組み合わせたスマートカードやUSBトークンを使用することで、クラウドとデジタルトランスフォーメーションへの取り組みを促進することができます。レガシーアプリ、ネットワークドメイン、クラウドサービスへのアクセスを保護するための単一の認証デバイスをユーザーに提供することで、運用コストを削減し、ユーザーエクスペリエンスを簡素化します。

セキュアなリモートアクセス

在宅勤務時と移動中のどちらの場合でも、ユーザーは複数の場所にある複数のデバイスからウェブベースのアプリケーションにログインする可能性があります。Thales FIDO認証システムは、エンドポイントデバイスの種類や場所を問わず、MFAによってセキュアなリモートアクセスを可能にすることで企業を保護します。

セキュアなモバイルアクセス

Thales FIDOデバイスは、NFCを使用して非接触型スマートカードをデバイスにタッチするか、SafeNet eToken Fusion USB-Cをスマートフォンにプラグインすることで、ユーザーがモバイルデバイスからあらゆるクラウドリソースに対して認証を行えるようにします。

特権ユーザーのアクセス制御

高い権限を持つ特権ユーザー（管理者、VIPなど）は、機密データにすぐにアクセスできるため、そのようなユーザーのアカウントはスピアフィッシング攻撃やホエーリング攻撃の格好の標的となります。

特権ユーザーに脆弱なパスワードに代わるFIDO2セキュリティキーを提供することで、許可されたユーザーのみが特権リソースにアクセスできるようになります。

IDPとの互換性

Thales FIDO2デバイスは、FIDO2標準をサポートするあらゆるIDプロバイダー（IDP）と互換性があります。

テスト・共同検証済みのIDPのリストはThalesのウェブサイトをご覧ください：https://cpl.thalesgroup.com/access-management/authenticators/fido-devices

対応プラットフォーム

Thales PKI/FIDOセキュリティキーはiOS、Android、Windows 11、10、8、Windows Server OS、macOS、Linuxなど、さまざまなOSをサポートしています。

Thales FIDO2のメリット

最高クラスのセキュリティ

- Thalesは製造サイクル全体を管理し、独自のFIDO暗号ライブラリを開発することで、侵害スクを低減しています。

複数のユースケースに対応

- FIDO、PKI、物理的アクセスを単一のデバイスに統合
- モバイルエンドポイントからの強力な認証を体験

高度なセキュリティ基準に準拠

- U2FおよびFIDO2認証取得済み
- 耐フィッシング認証に関する米国とEUの規制に準拠
- PKI運用のためのFIPSおよびCC認証取得済み

寿命を実現する堅牢性と拡張性

- 硬質成型プラスチック製の耐タンパUSB FIDOキー
- USBポートにダメージを与えない高感度検知機能
- ファームウェアのアップデートをサポートして保守性とアップグレード性を向上

スマートカード - フォームファクタ

製品特徴	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
接触型(ISO 7816)	FIDO & PKI	FIDO & PKI	該当なし	PKI	PKI
非接触型(ISO 14443)	FIDO & PKI	FIDO & PKI	FIDO、物理的アクセス	FIDO、物理的アクセス	FIDO、物理的アクセス
メモリ					
メモリチップ	400 KB Java Flash	400 KB Java Flash	586 KB User ROM	接触型チップ: 400KB Java Flash 非接触型チップ: 586 KB User ROM	接触型チップ: 400KB Java Flash 非接触型チップ:586 KB User ROM
常駐キー、証明書、追加アプレット、データ用に使用可能な空きメモリ	73 KB	55 KB	88.3 – 98.3 KB	接触型:73 KB 非接触型:88.3〜98.3KB	接触型:73 KB 非接触型: 88.3〜98.3KB
キー容量					
FIDO常駐キー	最大8	最大8	最大8	最大8	最大8
PKIキーコンテナ	20	20	該当なし	20	20
対応規格					
Java Card	3.0.4	3.0.5	3.0.4	3.0.4	接触型チップ:3.0.5 非接触型チップ:3.0.4
グローバルプラットフォーム	2.2.1	2.2.1	2.3	接触型チップ:2.2.1 非接触型チップ:2.3	接触型チップ:2.2.1 非接触型チップ:2.3
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Base CSPミニドライバ (SafeNetミニドライバ)	✔	✔	該当なし	✔	✔
暗号化アルゴリズム(PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	✔	該当なし	✔	✔
RSA:RSA最大4096ビット	✔	✔	該当なし	✔	✔
SA OAEP、RSA PSS	✔	✔	該当なし	✔	✔
P-256ビットECDSA、ECDH P-384およびP-521ビット ECDSA	✔	✔	該当なし	✔	✔
ECDH(カスタム構成で	✔	✔	該当なし	✔	✔
利用可能)	✔	✔	該当なし	✔	✔
カード上での非対称鍵ペア生成(RSA最大4096ビット、楕円曲線最大521ビット)	✔	✔	該当なし	✔	✔
対称:AES - セキュアメッセージング用、3DES - Microsoftチャレンジ/レスポンス専用	✔	✔	該当なし	✔	✔

スマートカード - フォームファクタ（続き）

製品特徴	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
認証					
チップ：CC EAL6+	✔	✔	✔	✔	✔
NIST認証 - FIPS 140-2 L2	該当なし	✔	該当なし	該当なし	✔
Javaプラットフォーム：CC EAL5+/ PP java card 認証取得済み	✔	該当なし	該当なし	✔	該当なし
Javaプラットフォーム + PKIアプレット：CC EAL5+/PP QSCD	✔	該当なし	該当なし	✔	該当なし
電子署名とeシールの両方でeIDAS規則準拠	✔	該当なし	該当なし	✔	該当なし
フランスANSSI	✔	該当なし	該当なし	✔	該当なし
物理的アクセス - Mifare Classic構成、DesFire configurations構成	該当なし	該当なし	✔	✔	✔
その他の特長					
オンボードPINポリシー	✔	✔	該当なし	✔	✔
マルチPIN対応	✔	✔	該当なし	✔	✔
カスタマイズとブランディング	✔	✔	該当なし	✔	✔
認証					
Windows 10およびその他のFIDO対応OSでFIDOに対応	✔	✔	✔	✔	✔
Windows、macOS X、LinuxでPKIに対応	✔	✔	該当なし	✔	✔

トークン - フォームファクタ

製品特徴	SafeNet eToken FIDO	SafeNet eToken Fusion	SafeNet eToken Fusion コモンクライテリア(CC)
フォームファクタ	USB-A	USB-AまたはUSB-C	USB-AまたはUSB-C
メモリ			
メモリチップ	400 KB Java Flash	400 KB Java Flash	400 KB Java Flash
常駐キー、証明書、追加アプレット、データ用に使用可能な空きメモリ	90 KB	55 KB	73 KB
キー容量			
FIDO常駐キー	最大8	最大8	最大8
PKIキーコンテナ	該当なし	20	20
対応規格			
Java Card	3.0.4	3.0.4	3.0.4
グローバルプラットフォーム	2.2.1	2.2.1	2.2.1
FIDO 2.0	✔	✔	✔
U2F	✔	✔	✔
Base CSPミニドライバ（SafeNet ミニドライバ）	該当なし	✔	✔
暗号化アルゴリズム(PKI)			
Hash：SHA-1、SHA-256、SHA-384、SHA-512	該当なし	✔	✔
RSA：RSA最大4096ビット	該当なし	✔	✔
SA OAEP、RSA PSS	該当なし	✔	✔
P-256ビットECDSA、ECDH P-384およびP-521ビットECDSA	該当なし	✔	✔
ECDH(カスタム構成で	該当なし	✔	✔
利用可能)	該当なし	✔	✔
カード上での非対称鍵ペア生成(RSA最大4096ビット、楕円曲線最大521ビット)	該当なし	✔	✔
対称：AES - セキュアメッセージング用、3DES - Microsoftチャレンジ/レスポンス専用	該当なし	✔	✔

cpl.thalesgroup.com
お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。

© Thales - September 2023 • EHV3