2021年6月更新　ver.2.0

Hewlett Packard
Enterprise

アプリケーションやSaaSの認証を強化する
IceWall MFA FIDO2オプションのご紹介

日本ヒューレット・パッカード合同会社
Pointnext事業統括　IceWallビジネス推進部

目次

- 生体認証への期待と課題
- IceWall MFA FIDO2オプション
- お問い合わせ

生体認証への期待と課題

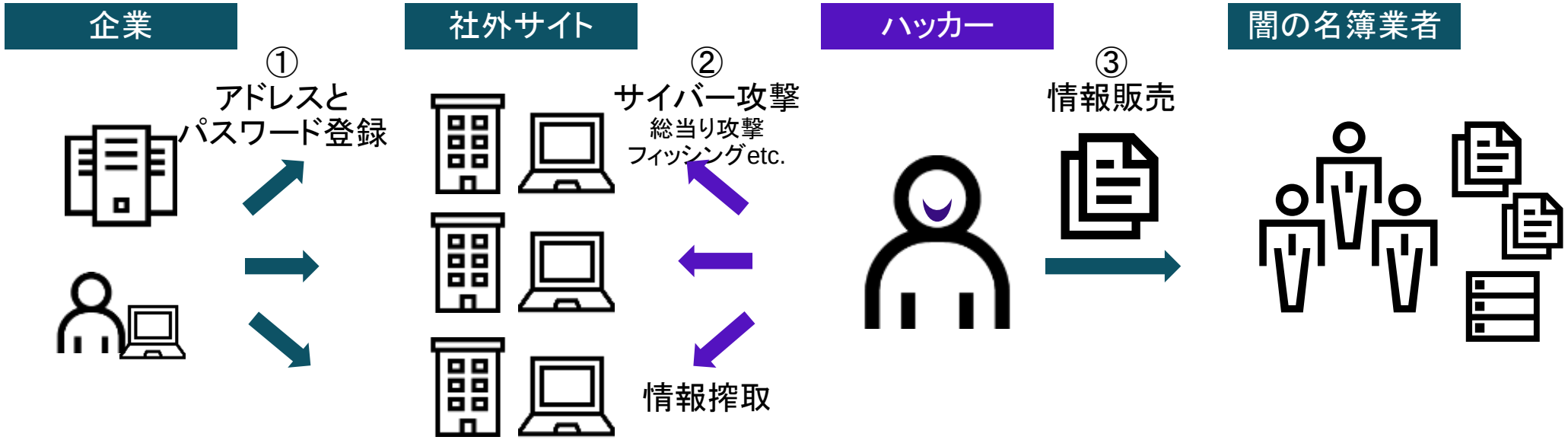
崩れる安全神話・・・パスワードは漏洩するもの

新しい生活様式（ニューノーマル）がもたらす生活の変化と共に、テレワークやDX推進など労働環境の急速な変革も相まって、パスワードに代わる強固な認証が求められています。

大手企業や省庁からも…　メールアドレスとパスワードの漏洩例

「もともとは利用者が限られる闇サイトで売られていたが、現在は誰でもアクセスできるサイトを通じて無料でダウンロード可能な状態にある。リストに記されている組み合わせの総数は、16億件に達する。」

引用元：日経ビジネス　2018年9月10日号　https://business.nikkeibp.co.jp/atcl/report/15/110879/090500858/?P=2



企業の従業員や官公庁職員が仕事用のメールアドレスを使って、取引先やネット通販サイトなどで会員登録

悪意あるハッカーが守りの甘いサイトを攻撃し、メールアドレスとパスワードを取得

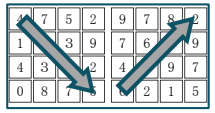
攻撃により入手したメールアドレスとパスワードを闇サイトを通じて販売し、利益を得る

闇の名簿業者が「名寄せ」してメールアドレスとパスワードの組み合わせを増やしていく

生体認証への期待

認証の種類

「記憶」による認証
SYK(Something You Know)



「生体」による認証
SYA(Something You Are)

「所有」による認証
SYK(Something You Have)

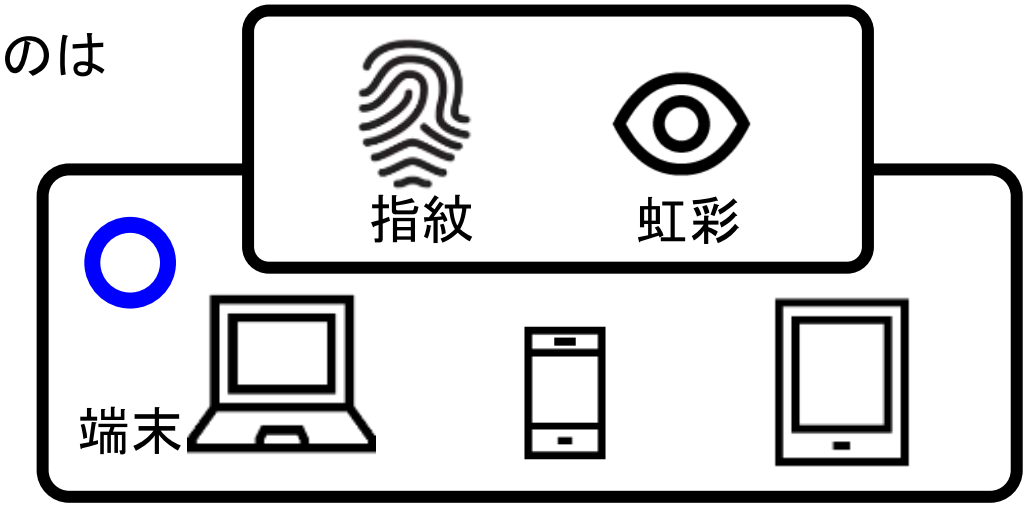
「生体」による認証の利点

- 忘却・紛失・寿命切れの心配が無い
- 鍵デバイスの持ち歩きや
  キーボード入力などが不要で、
  利用者への負担が極めて低い

以前は生体認証デバイスのコストが課題だったが、
近年はスマートデバイス内蔵の指紋認証や顔認証の
普及により、大幅に改善している

これまでの生体認証の課題

生体認証は普及したが、守るのは
特定の「端末」だった。



△ SaaS

△ Web

△ 課題

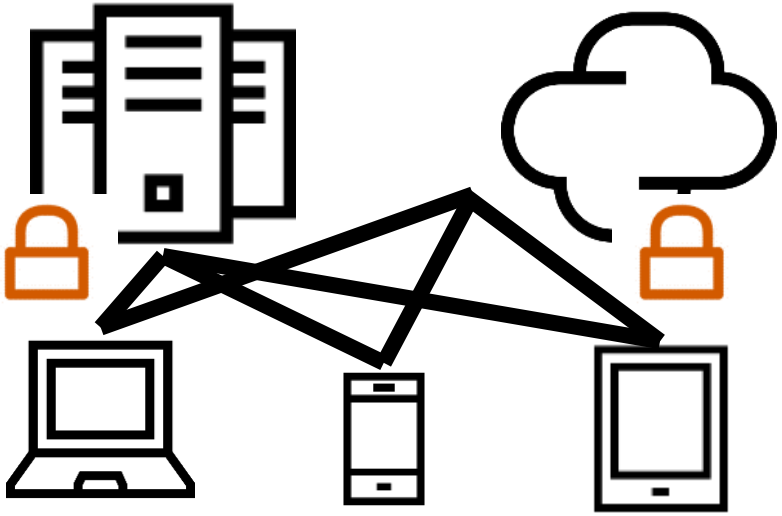
- 端末は認証強化できても、WebアプリケーションやSaaSの強化は苦手
  - 既存Webアプリケーションで生体認証するには、大幅な改修が必要。SaaSだと更に難しい。
  - 仮に対応できても、特定方式に依存すると汎用性がなく、ベンダーロックとなり高コスト。
  - 生体情報の集約が必要で、漏洩防止対策に加え、プライバシーへの配慮も求められる。
- デバイス依存が強く、マルチデバイスに対応できない
  - 特定の端末OSやバージョン用に、別々の認証アプリが必要。または一部OSに非対応。
- 別途専用機器が必要なケースもあり、更にコストが嵩む

これからは、端末だけを認証強化する時代ではない！

これまで

管理された
特定の端末を守れば
情報を守れた

これから



マルチデバイス利用を前提に、
端末と直接紐づかない
WebやSaaS上の情報を守る必要がある

WebやSaaS、スマホアプリなど、
様々な利用シーンで生体認証が求められている

これから求められる生体認証ソリューション

1. 標準規格をベースに、低コストでベンダロックされない

2. SaaSにも適用できる

3. スマホやタブレットなどマルチデバイスに対応できる

4. アプリ改修が不要で、広い範囲に適用できる

5. 生体情報の集約・管理が不要

これらの要望を実現するのが IceWall MFA FIDO2オプション

IceWall MFA FIDO2オプション

- FIDOとは
- IceWall MFA FIDO2オプションとは

FIDO とは（Fast IDentity Online）

The FIDO Alliance

- パスワードに依存しないユーザー認証を目指す団体。2012年設立。
- 約200社の様々な企業等（下記例）が加盟。
  - IT、EC　　Google、Microsoft、Apple、Amazon、Yahoo!Japan、楽天
  - 金融　　Bank of America、三菱UFJ銀行、VISA、Master Card、JCB
  - 通信　　NTTドコモ、KDDI、LINE
  - 認証デバイス Yubico、飛天
- FIDO 1.0 仕様を公開:　　2014年12月
  - UAF（パスワードレス認証）およびU2F（追加認証）
- FIDO2仕様を公開:　　2018年4月
  - W3C WebAuthn　　2019年3月勧告化
    - 標準化団体W3Cが標準仕様を策定（W3C：HTML、XML、SOAP等のWeb標準仕様を策定している団体）
    - Web Authentication: An API for accessing Public Key Credentials Level 1
    - クライアント（ブラウザ）のAPI仕様、Authenticatorの仕様
  - FIDO CTAP（Client To Authenticator Protocol）
    - クライアント（ブラウザ）と外部Authenticator間の仕様。（USB、Bluetooth、NFC）

日本国内でのFIDO導入状況

FIDO Alliance Japan WG資料より（2019/7/4）

IceWall MFA FIDO2オプションとは

標準規格である「FIDO2」および「W3C Web Authentication」を採用し、各種端末OS標準の生体認証等と連携したパスワードレス認証や、他の認証方式と組み合わせた多要素認証を実現。
SaaSを含む幅広いWebアプリケーションやネイティブアプリケーションの認証を強化します。

マルチデバイスで

Windows Hello

iOS/Mac Touch ID

iOS Face ID

Android 標準 生体認証

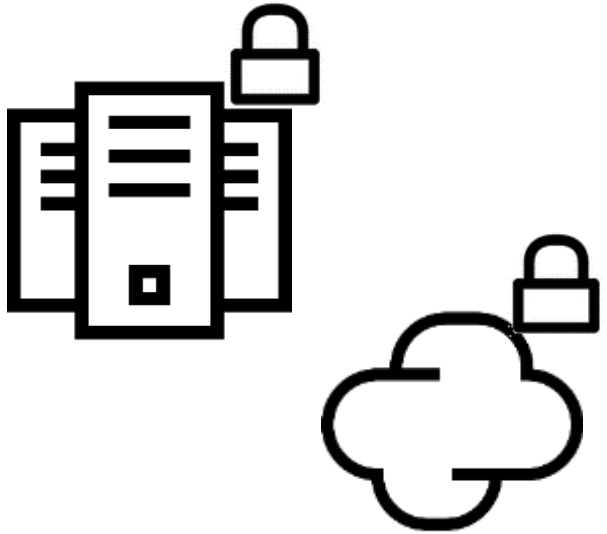
セキュリティキー

生体認証

多要素認証

IceWall MFA FIDO2オプション

WebアプリケーションやSaaSへ



IceWall MFA FIDO2オプションの利用イメージ（iOS - Touch IDの場合）

SafariでWebにアクセス

Touch ID を求められる

Webやクラウドにログイン完了

Webやクラウドにアクセスすると、デバイス固有の生体認証を求められる

・利用イメージ動画も公開中： https://www.hpe.com/jp/ja/software/icewall/demomovie.html

IceWall MFA FIDO2オプションの特長 (1/2) ～Web ＆ マルチデバイス ～

- 生体認証等により、端末ではなく**SaaSを含む幅広いアプリケーションを認証強化**できる
  - アプリケーションの改修は不要、SaaSにも適用できる
- **マルチデバイス対応**
  - Windows 10、iOS/iPadOS、Android、Mac
  - 必要な登録作業を行えば、個人所有の端末も利用できる
- **認証機器の追加コスト不要**
  - 各デバイスOS標準の生体認証を利用できる
  - Windows Hello、Apple Touch ID、Apple Face ID、Androidの指紋・虹彩認証、セキュリティキーなどが利用できる

安価かつ容易に、幅広いアプリやサービスを認証強化できる

IceWall MFA FIDO2オプションの特長 (2/2) ～端末に閉じた生体認証～

- **予め登録した端末に利用を限定し、不正利用を防止**
  - 不特定多数の端末からのアクセスを禁止できる
  - 登録時は、ワンタイムパスワード認証等でなりすましを防止
- **生体情報のサーバーへの集約・管理は不要**
  - 生体認証は、端末内に閉じた形で行われる
  - 端末内での生体認証の後、サーバー側へ利用者の正当性を示す情報を送ることでサーバー側の認証を実施
- FIDOアライアンスの認定取得済み（FIDO2）

IceWall MFA
FIDO2オプション

fido CERTIFIED FIDO2

生体情報のサーバー集約が不要で、利用端末も限定できる。

IceWall MFA FIDO2オプションで利用できる認証デバイス（認証器）

Windows Hello

Touch ID

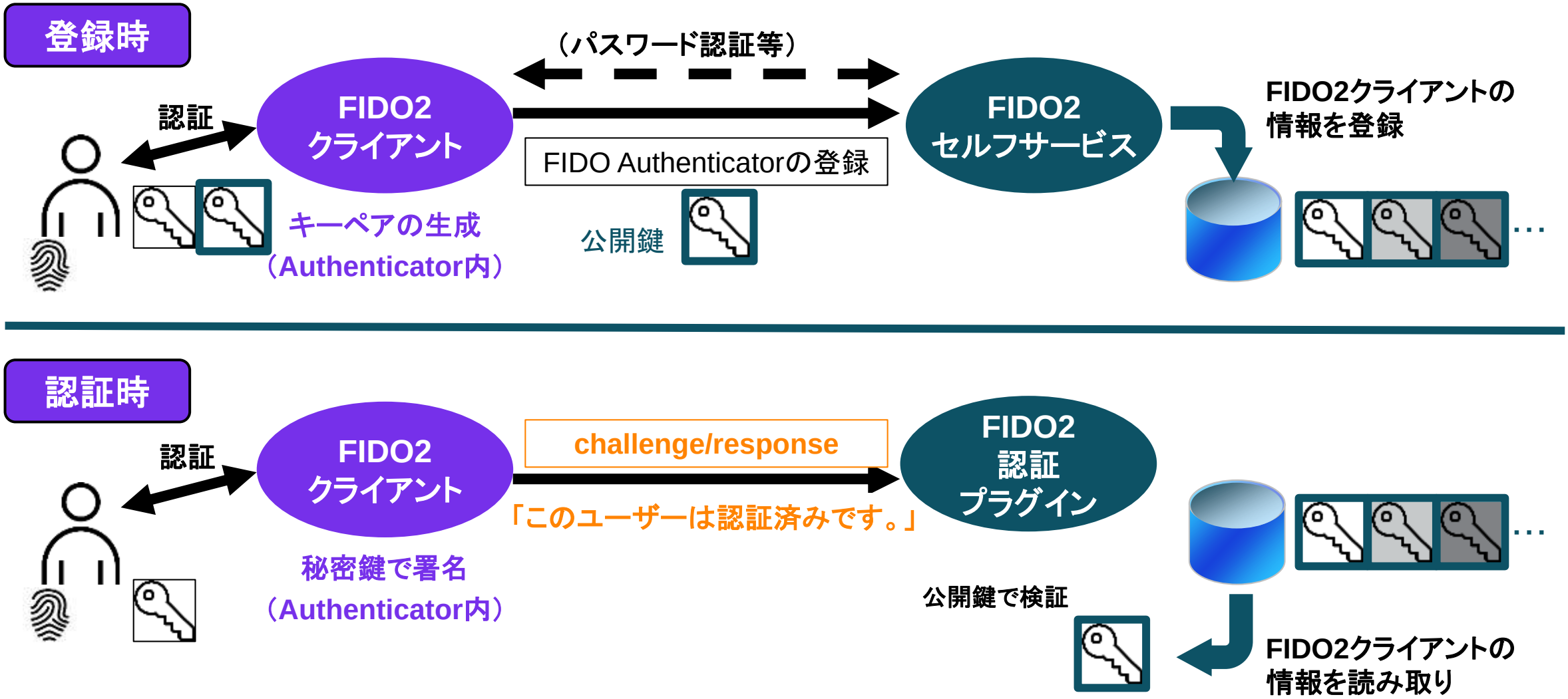
Face ID

Android標準の指紋、光彩認証

セキュリティーキー

日頃利用している端末に内蔵された認証デバイスを用いて、
生体情報の再登録なしにWebやSaaSを認証強化できます

端末登録と認証の動作



IceWall MFA FIDO2クライアントライブラリ

IceWall MFA FIDO2オプションと連携して、ネイティブアプリケーションでFIDO2認証を実装するためのライブラリです。

- 対応プラットフォーム
  - iOS/iPadOS、Android、Windows10
- 対応認証デバイス（認証器）
  - 各OS標準の内蔵生体認証、PIN
- 提供機能
  - Credential作成機能：端末登録時に、FIDO2仕様（W3C WebAuthn仕様）準拠のCredentialを作成
  - Assertion作成機能 ：認証時に、FIDO2仕様（W3C WebAuthn仕様）準拠のAssertionを作成

IceWall MFA FIDO2 オプションの対応動作環境

端末OS	端末ソフトウェア（ブラウザー）	パスワードレス認証		多段階認証	
		端末内蔵生体/PIN	FIDO2トークン	端末内蔵生体/PIN	FIDO2、U2Fトークン
Windows 10	Edge	○	○	○	○
	Chrome	○	○	○	○
	Firefox	○	○	○	○
iOS/iPadOS	Safari	○	○	○	○
	Edge	○	○	○	○
Android	Chrome	○ *1	ー	○	○
macOS 10	Safari	○	△ *2	○	○
	Chrome	○	○	○	○

端末OS	端末ソフトウェア	パスワードレス認証		多段階認証	
		端末内蔵生体/PIN	FIDO2トークン	端末内蔵生体/PIN	FIDO2、U2Fトークン
Windows 10/iOS/ iPadOS/Android	FIDO2ライブラリを使ったネイティブアプリケーション	○ *3	ー	○ *3	ー

*1 ブラウザ標準機能では対応していませんが、HPE　IceWallアプリを利用することで実現可能です（Android用（OS標準内蔵指紋/虹彩認証）。
*2 一部デバイスで非対応。
*3 お客様開発のネイティブアプリケーション用にFIDO2ライブラリ を提供（Windows .NET/iOS/iPadOS/Android。別途有償）。
・「端末内蔵生体/PIN」では、Windows Hello（Windows）、Face ID/Touch ID/PIN（iOS/iPadOS、又はAndroid標準の指紋/虹彩認証/PINを利用可能です。
対応するセキュリティキーや最新の動作環境は、「IceWall MFA FIDO2 オプション動作確認済み認証器一覧 」を参照ください。
https://h50146.www5.hpe.com/products/software/security/icewall/mfa/pdfs/IW_MFA40FIDO2Device.pdf

お問い合わせ

お問い合わせおよび周辺サービス

お電話でのお問い合わせ（日本ヒューレット・パッカード　カスタマー・インフォメーションセンター）

0120-268-186 / 03-6743-6370（スマートフォン・携帯電話から）

受付時間： 月曜日～金曜日 9:00-19:00

（土、日、祝祭日、年末年始および5月1日を除く）

Webフォームからのお問い合わせ **www.hpe.com/jp/iw-contact**

最新/詳細情報

- **HPE IceWall 公式サイト**
  www.hpe.com/jp/icewall
- **お客様事例**
  www.hpe.com/jp/iw-casestudy
- **技術レポート（新規レポート随時公開中）**
  www.hpe.com/jp/iw-report
- **カタログ**
  www.hpe.com/jp/iw-catalog
- **IceWallトレーニングコース**
  www.hpe.com/jp/iw-training

各種サービス

- 導入サービス
- コンサルティングサービス
- エンジニア様向け技術トレーニング
- 海外拠点への導入・コンサルティングサービス

THANK YOU