

FIDO2対応YubiKeyがグローバルで選ばれる理由とパスキーの展開

yubico

The key to trust

Junichi Ohtomo (大友淳一)

Vice President Sales Japan and Korea

junichi.ohtomo@yubico.com



YubiKey (ユビキー) とは？

- ハードウェア型の認証機
- クレデンシャルを内部にセキュアに保管
- 1つのキーで複数の認証に対応可能
- 電池・電波は不要な物理キー
- 防水・防塵・強靱で家の鍵のようにいつも携帯

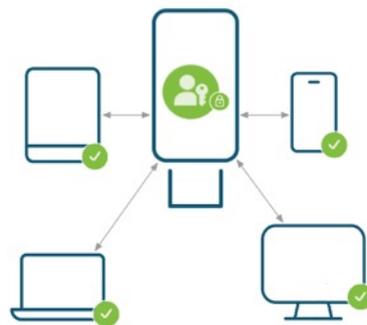


パスキー(Passkey)とはなんですか？

パスワードからの脱却を可能にするアーキテクチャ

パスキー = Discoverable FIDO Credential

マルチデバイスパスキー	シングルデバイスパスキー
<ul style="list-style-type: none">• クレデンシャルがコピーできる ⇒ 複数のデバイスで利用可能• Hardware Attestationなし	<ul style="list-style-type: none">• クレデンシャルはコピーできない ⇒ 特定のデバイスでのみ利用可能• Hardware Attestationあり



Yubico社について

ユーザ認証のグローバルリーダー



Stina Ehrensvärd, Founder



Mattias Danielsson, CEO

800+

パートナーテクノロジーとのインテグレーションの実績

4500+

法人ユーザーの数

19/20

米テクノロジー
超大手企業様の
長期ユーザー

優良

インベスター
(a16z, NEA,
Benioff)

92%

ITサポート負荷
の軽減

99.9%

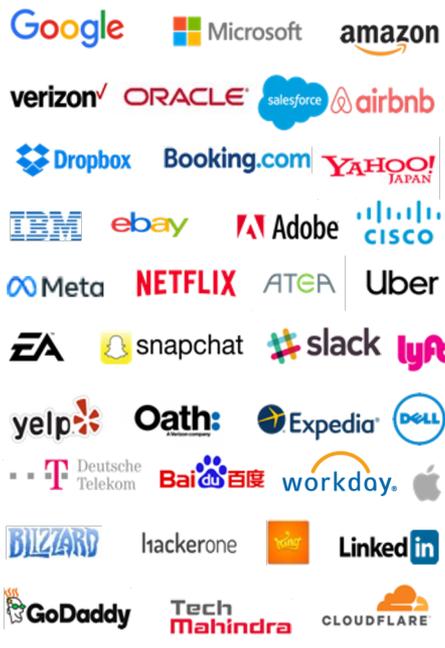
資格情報盗難リスク
の軽減を実現

22m+

Yubikeyの全世界
での販売実績

業種業態を問わない多くの利用実績

ハイテク



金融サービス



小売・製造



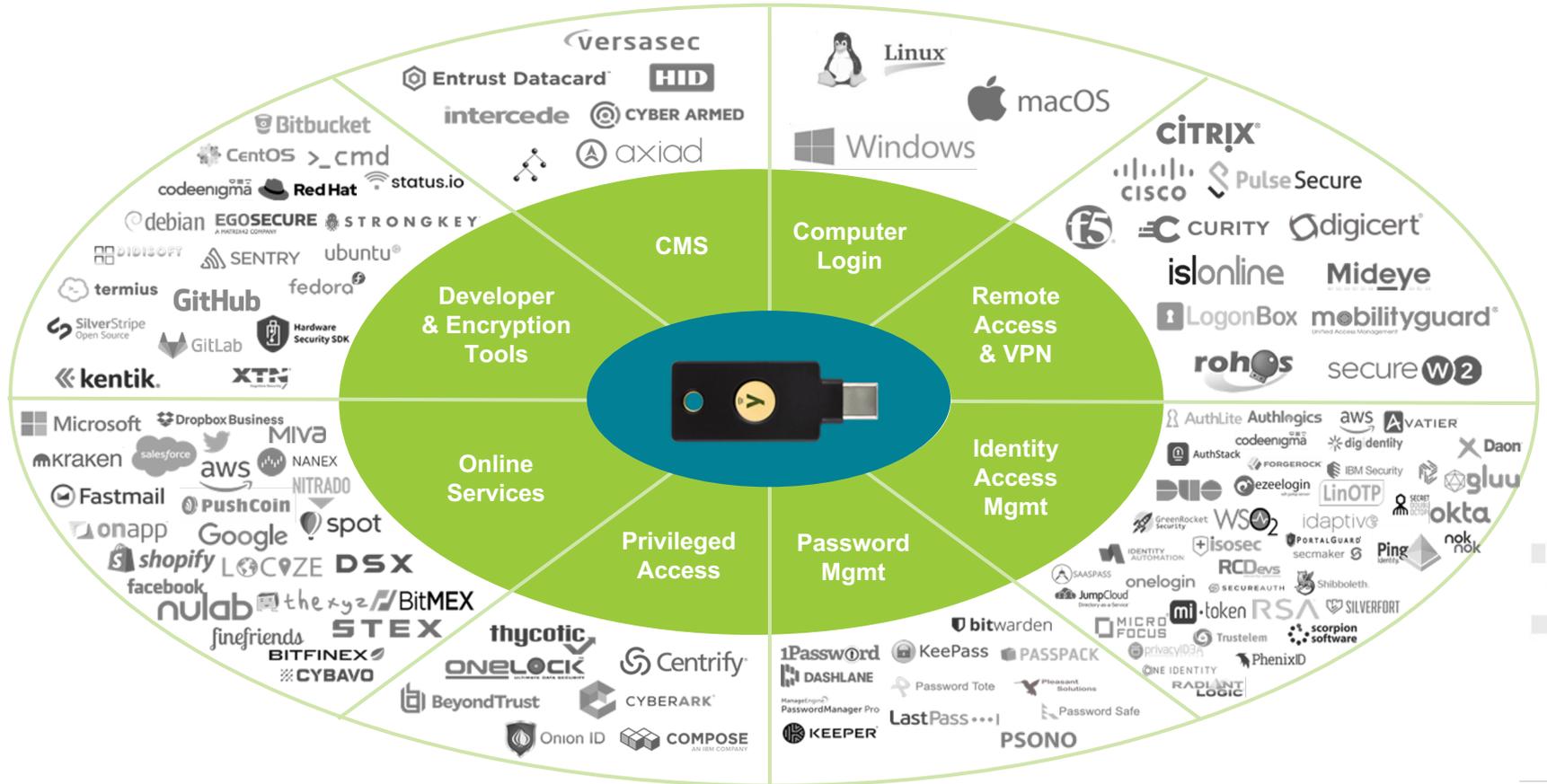
政府・教育



その他



800を超えるアプリやサービスに対応済み



yubico

Yubicoは新しい「認証」をデザインしています

もちろんYubiKeyはFIDO2/WebAuthnを利用したパスワードレスにも対応！

暗号鍵を
格納する
専門のHW



一つのキーで
様々なアプリ、
サービスに対応



偽サイトに誘導
されないために
オリジナルURL
を記憶



FIDOに対応した
サービスは複数の
キーを登録可能



タッチすること
でユーザの存在
を確認



多くのOSやブラ
ウザがYubiKey
に対応済み



yubico

YubiKeyを利用するビジネスシナリオTop7



特権ユーザ

特権アカウント
の利用保護



モバイル 利用制限 ユーザ

コールセンターの
ようなモバイルを
利用できない環境



共有端末

共有端末利用
ユーザの個々の
アカウントを保護



リモート ワーカー

家や出先からの
アクセスを保護



オフィス ワーカー

認証のUX向上と
セキュリティ担保を
同時に実現
(モバイルより速い)



協力会社 取引先

共通システムを
利用する
取引先からの
アクセスを保護



顧客の顧客

自社が提供する
サービスに
アクセスする
顧客を保護

- セキュリティ
保護の最大化

- セキュリティ
保護の最大化
- 多要素認証の
モダナイズ

- セキュリティ
保護の最大化
- 他要素認証の
モダナイズ

- セキュリティ
保護の最大化
- 働き方改革

- 多要素認証の
モダナイズ
- ゼロトラスト

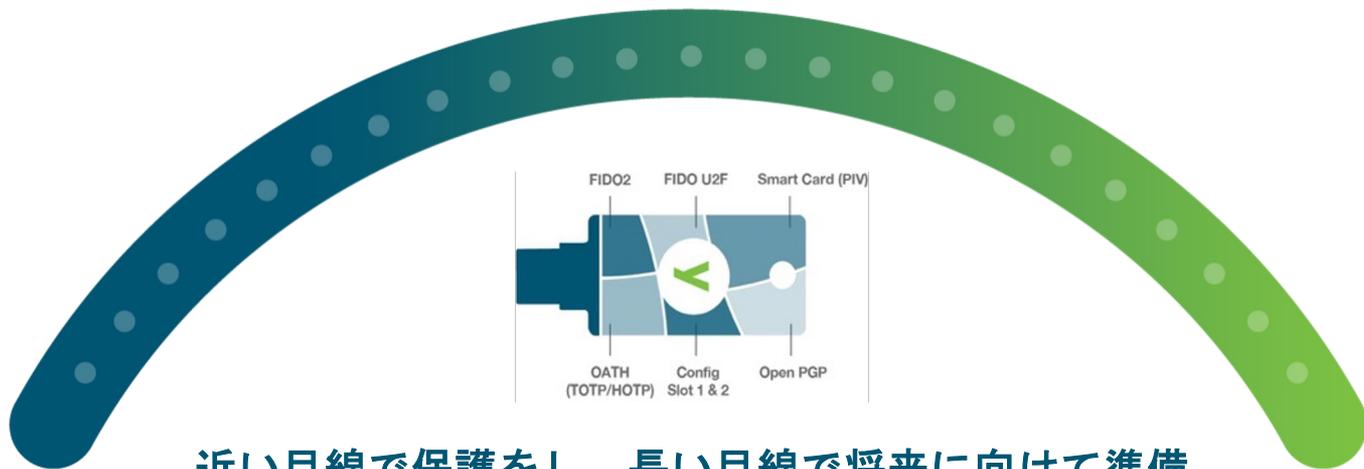
- セキュリティ
保護の最大化
- コンプライアンス
遵守の徹底

- DXを促進
- 利用ユーザの
安心感



*YubiKeys comply with government regulations (FIPS, DFARS, GDPR, PSD2, CSPN) and leading open authentication standards (FIDO, PIV, OATH, W3C)

YubiKey – パスワードレスやゼロトラストへの「橋」



近い目線で保護をし、長い目線で将来に向けて準備

適切なパスキーの利用手段

サービスプロバイダ

一般のユーザー

複数のデバイスで、
コピー可能なパスキーを
利用して、気軽に
安全にサービス
利用してもらう



ハイリスク下のユーザー

セキュリティーキーで
パスキーを利用することで、
より高い安全性を提供



上級のユーザー

セキュリティーキーで
パスキーを利用することで、
差別化を図る



企業・組織

第一線のワーカー

認証の安全性はもとより、
環境に依存しない
セキュリティーキーで
パスキーを利用



オフィスワーカー

クレデンシャルの保存場所が
特定できるようにAttestation
を設定できるセキュリティー
キーが求められる場合が多い



特権ワーカー

最もリスクが高いユーザで
あり、クレデンシャルの保存
場所を特定する必要が
ある。Attestationは必須



YubiKey Portfolio



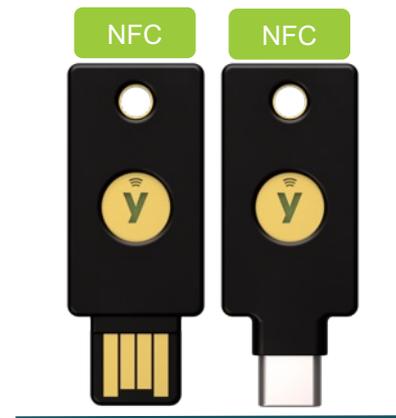
YubiKey 5 Series Multi-protocol

- WebAuthn
- FIDO2
- U2F
- Smart card
- Yubico OTP
- OATH-HOTP
- OATH-TOTP
- OpenPGP
- Static Passwords



YubiKey Bio Series FIDO-only and Biometrics

- WebAuthn
- FIDO2
- U2F



Security Key NFC FIDO-only

- WebAuthn
- FIDO2
- U2F



事例：CERN



管理者アカウントや管理者アクセスを保護

要件

- 共有コンピューティングサービスのアカウント保護
- 世界中の研究者が個別に利用しているBYODデバイスからのアクセス
 - Linux, Mac OS, Windows
 - SSHログインを含む
- だれでも簡単に利用できる多要素認証デバイス

YubiKeyの導入

- 数ヶ月という短期間で初回導入
- システムやデバイスの変更なし（サーバー側での変更はあり）
- SSOとの連携も実施

「YubiKeyの導入や利用状況に関して言うと、スタッフから特別な意見を聞いていません。つまり、全体的に満足しているという証です。不満の声がないため、YubiKeyの導入は大成功だと言えます」

CERN IT部門CISO, Stefan Lueders氏

事例：Hyatt様

職務形態に合わせて柔軟なソリューションの組み合わせ

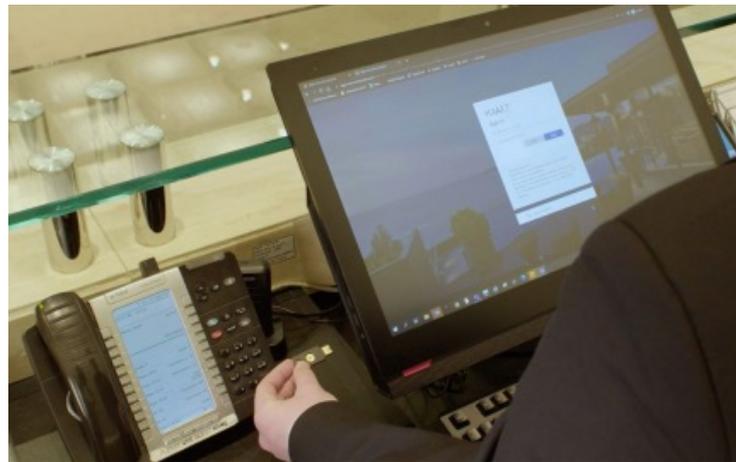
- グローバルでの利用
- Azure AD + YubiKeyを中心にしたデプロイ
 - コーポレート従業員：FIDO2 + Windows Hello for Business
 - ホテルフロント：FIDO2 + 共有PC
 - コールセンター：FIDO2
 - 契約社員：TOTP

業務やアクセスする場所に関係なく、YubiKeyをMFA+パスワードレス認証で利用することで、お客様の前で認証のために携帯電話を見ずにフィッシング対策を実現できる

HYATT®



事例紹介YouTube



yubico

Thank you from the Yubico team!

