yubico

Protect the Digital You

世界で最も信頼されているセキュリティーキーベンダー

さよならパスワード with YubiKey

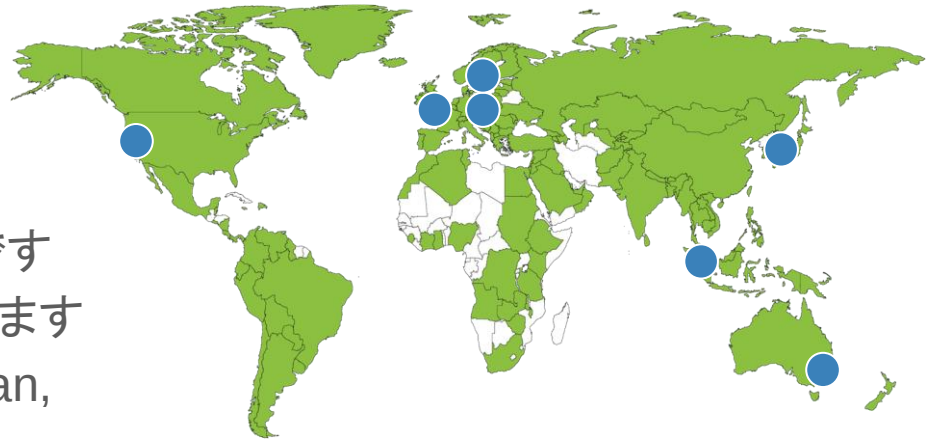
Junichi Ohtomo(大友 淳一)
Vice President Sales Japan and Korea | Yubico
junichi.ohtomo@yubico.com

yubico

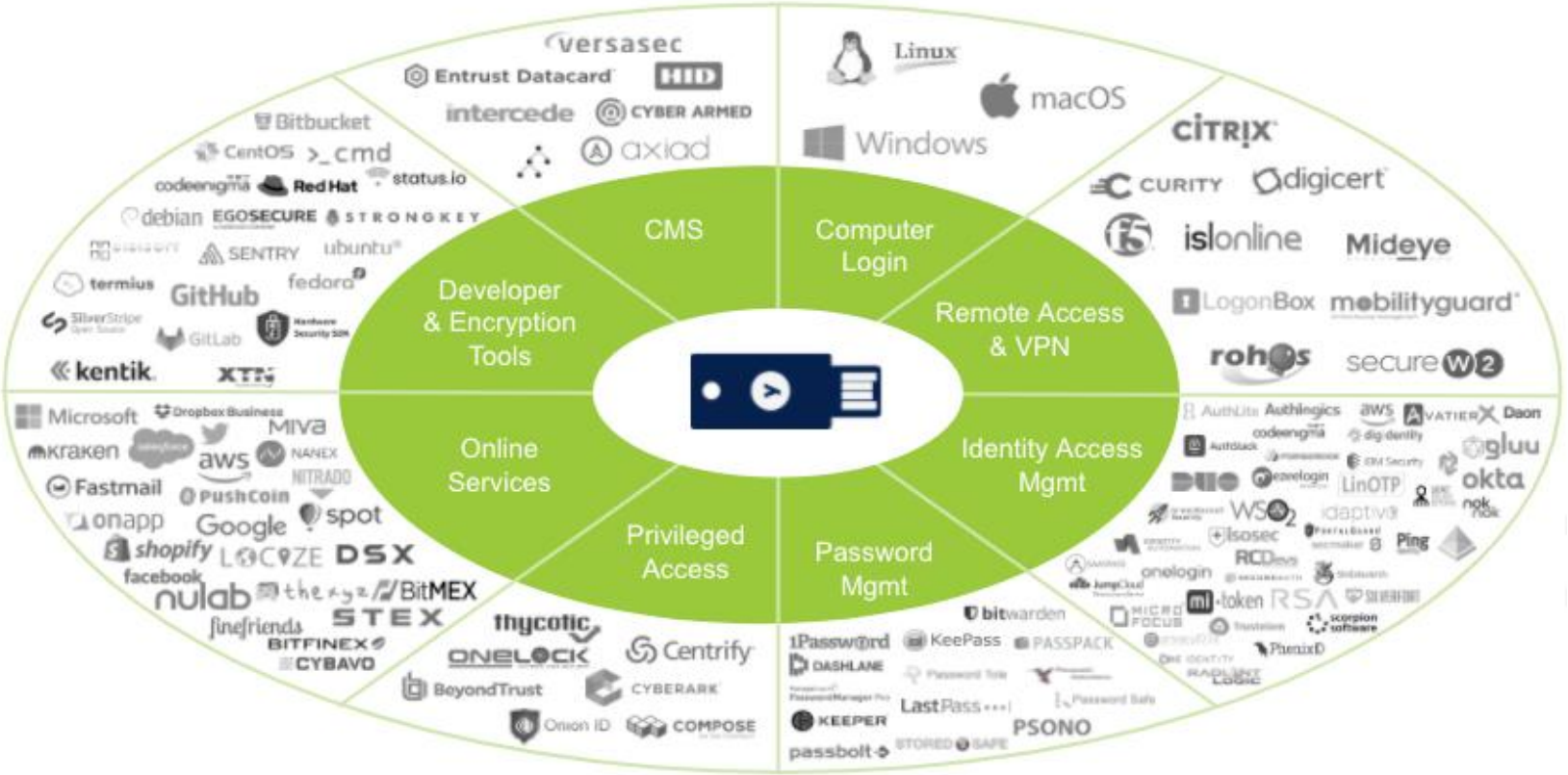
Yubicoについて

Stina Ehrensvärd,CEO & Founder

- 1000万以上のYubiKeyが160カ国で利用されています
- 4000社を超える顧客企業
- 皆様がお使いのIAMソリューションや700種以上のアプリとの連携が可能です
- 240名の社員と7ヵ国にオフィスがあります
  Sweden, USA, Germany, UK, Japan, Australia
- 有力投資家からの投資を受けています
  Andreessen Horowitz, NEA, M Benioff



Yubiquity – 700以上の連携



#1 Security problem: ログイン情報が盗まれる

- **6000億ドル/年** – 世界のIT不正行為の被害
  この5年で2倍になっている！
  出典:Cybersecurity Ventures

- 企業の**3社に1社**が2年以内になんらかの
  情報漏洩を起こすと予測されている
  出典: Cost of a data breach report, IBM, 2019

- **81%**のハッキング事件は盗まれた
  クレデンシャルか総当たり攻撃による
  出典: 2020 Verizon DBIR (Data Breach Investigation Report)

- **強力な他要素認証が唯一の防御策**

Implications of a breach

テレワーク・リモートワークユーザがハッカーに狙われている
Covid-19が明らかにしたテレワークの脆弱性

CNN BUSINESS Markets Tech Media Success Perspectives Videos LIVE TV Edition

Google will let employees work from home until at least next summer

By Brian Fung, CNN
Updated 4:15 AM ET, Tue July 28, 2020

The Internet is drowning in COVID-19-related malware and phishing scams

Emails and websites promise info about the pandemic. In reality, they're shams.

DAN GOODIN - 3/13/2020

Tom Kelly

the coronavirus outbreak is no different. Since January
ve leveraged the COVID-19 pandemic to stage all manner of cyberattacks,
nware take-overs of hospital systems to private network hacking. But the latest

リモートアクセスの
ログイン画面が
インターネット上で
丸見え…

PCが乗っ取られ、リモート
アクセスしている社内
サーバーや重要ファイル
を人質に取られる…

IT管理者と離れた環境で、不審なメールや、不審な添付書類が送られてくる…

Source: 1. "Big tech firms ramp up remote ... vent coronavirus spread", CNN Business, 2020; 2. "Abusing fear", arstechnica.com, 2020

6

SMSによる二段階認証は安全か？
今やスマートフォンもハッキング対象

10億台以上のAndroidデバイスが
マルウェアの脅威晒されている[1]

iPhoneのマイクとカメラが所有者の
操作なしにリモートでハックされた[2]

7

SMSのコードが奪われる可能性

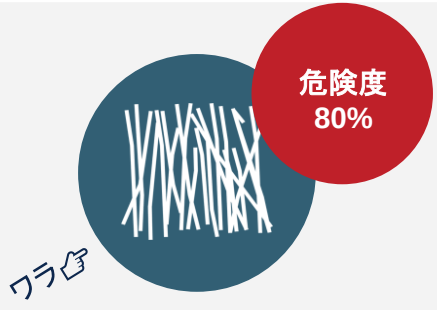
パスワード入力やコード入力を見られる可能性

Source: 1. "More than one billion Android devices at risk of malware threats", Which.co.uk, 2020; 2. "Google Reveals How To Hack An Apple iPhone Within Minutes", Forbes.com, 2020

セキュリティの原点 – 「守ること」 → 進化の時期

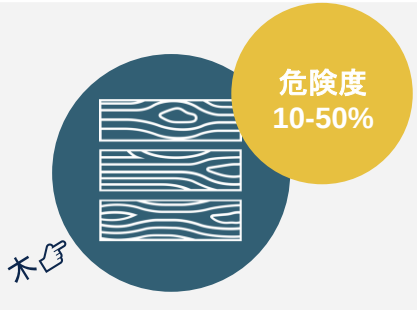
Yubico CEOの先祖がデザインしました…
in Sweden

パスワードはワラの家



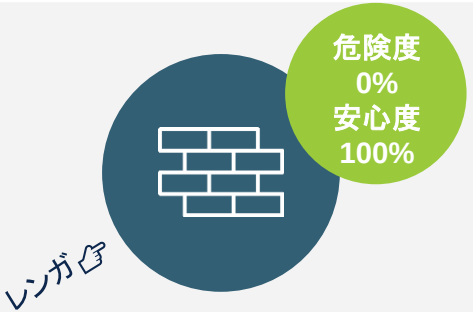
ユーザ名&
パスワード

- 実装が簡単
- "不便さ"についても既知
- 運用にIT部門の手間とコスト
- ハッカーにとってフィッシング対象として狙いやすい



SMS, Email, モバイル等
ベーシックな2FA

- そもそもセキュリティーのためにデザインされた技術ではない
- ネットワークやアプリの既知の脆弱性を利用され攻撃される
- ハッカーにとってフィッシング対象として狙いやすい



Strong
Authentication

- セキュリティのためにデザインされている
- ネットワーク接続、データの保存、クライアントソフトに依存しない
- フィッシングに対して耐性が極めて高い

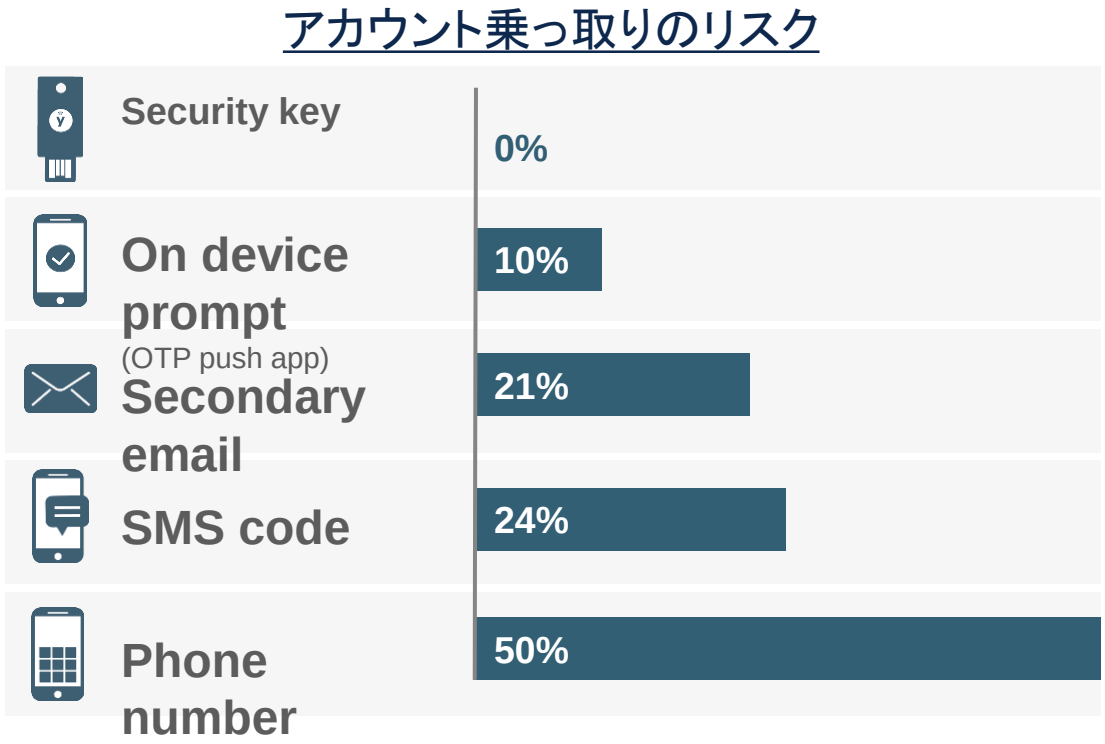
FIDO Security Keys
クレデンシャルの盗難やアカウントハイジャックを防ぐことの証明

Google Security Blog

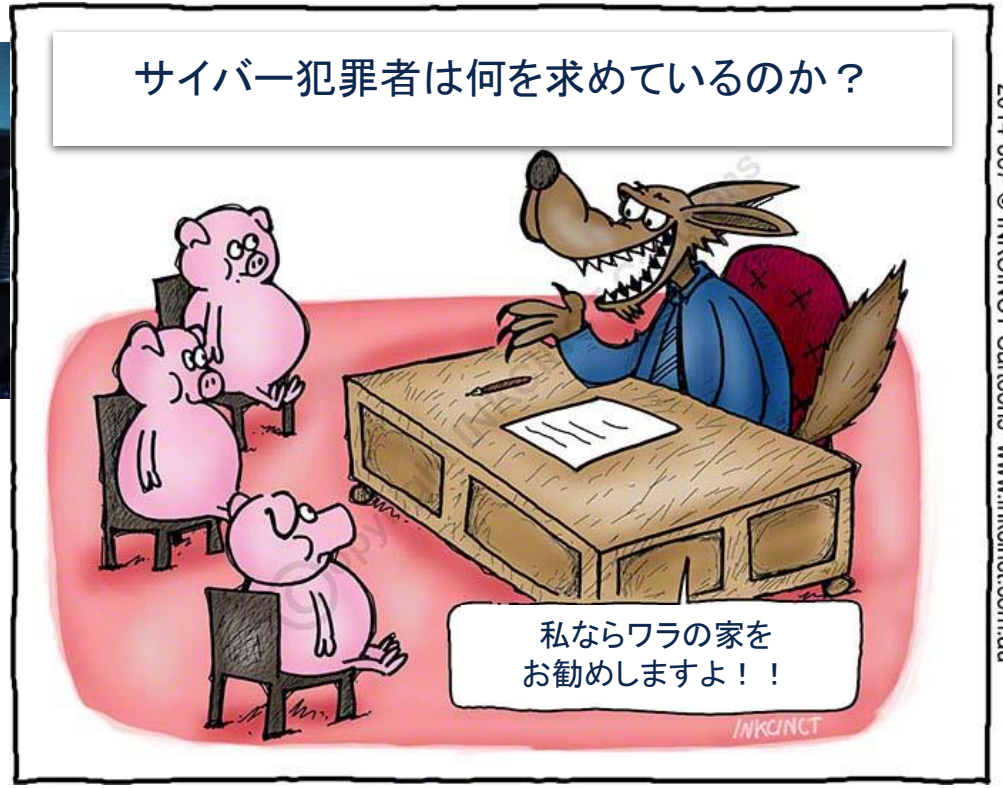
How effective is basic account hygiene at preventing hijacking
May 17, 2019

Research based on **350,000 users** and real-world hijacking attempts.

The majority of the **FIDO Security Keys** used in the study were from **Yubico** using **FIDO U2F**, the technology that stopped account takeovers.



あなたはどんな家に住みたいですか？



あなたはどんな家に住みたいですか？

ハッキングされた後に…

ログを分析する…

すでに情報はとられてます

身代金を要求されることも

あらゆる規模で利用できる最新の認証

安全な「家」(Secure House)を作るための基本とは？

- 誰でも簡単に使える(ITの知識に依存しない)
- セキュリティ強度が高い
- どこからでも使える
- シンプルで標準化された技術で

+ FIDOに対応したサービスや
SSO/Federation

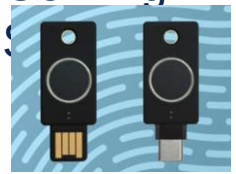
パスワードから解放され華麗なITライフを！

14

YubiKey Hardware Family

PCとモバイルのためにさまざまな形態

Coming



Yubico Blogで詳細を公開中

- Fips 140-2
- FIDO/U2F
- FIDO2
- Waterproof
- Crush Resistant

yubico

Protect the Digital You

世界で最も信頼されているセキュリティーキーベンダー

cisco Secure

Duo & Yubico 共催

さよならパスワード 次の時代のセキュリティとは？

シスコシステムズ合同会社
村上　英樹 (テクニカル ソリューションズ アーキテクト)
2020年12月17日

Agenda

1. 新しい働き方と
   アイデンティティの関係
2. Duo機能概要
   （多要素認証）
3. Yubico+Duo事例

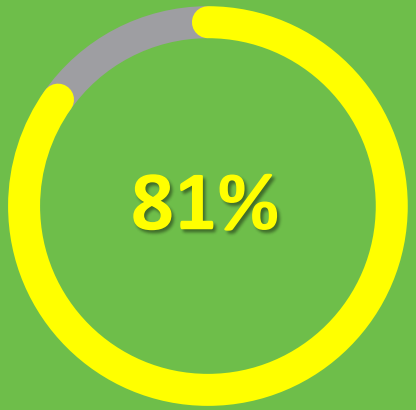
新しい働き方と
アイデンティの関係

現実の脅威：不正侵入は、ID/パスワード漏洩から
セキュリティの新しいアプローチが必要とされる

Targeting Identity

81%のハッキングによる侵害は、パスワード漏洩や弱いパスワードなど、クレデンシャルに関連している

*Verizon Data Breach Investigations Report



* https://gblogs.cisco.com/jp/2020/06/unpacking-2020s-verizon-dbir-human-error-and-greed-collide/

NISCの注意喚起
テレワーク実施者の方へ

https://www.nisc.go.jp/security-site/telework/

～あなたのセキュリティは大丈夫ですか？～

オフィスを離れ自宅や公共のスペースなど、場所や通勤等にとらわれず働くことを可能にするテレワーク。実施が増えている一方、オフィス環境と異なったり、攻撃者に狙われたりして、思わぬリスクに晒される可能性がありますので、いままで以上に各自が求められるセキュリティ対策を実践することが重要です。

テレワークを実施される方は、お使いになるシステムに求められる要件や以下の注意すべきポイントに気を付けて、仕事上の情報漏えい等や自らの端末・機器等を守る意識を高めましょう。

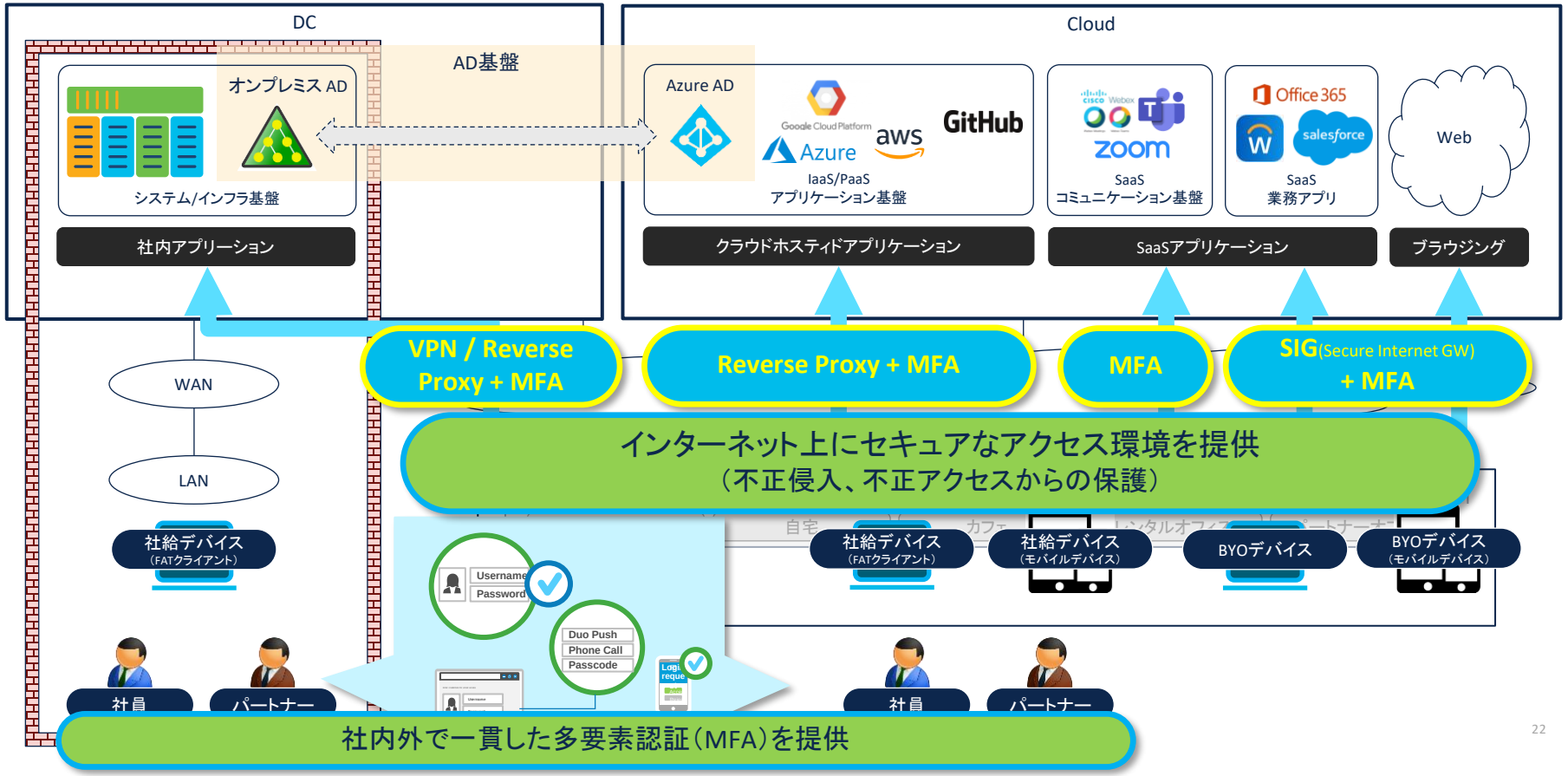
- **複雑なパスワードや多要素認証を使いましょう**

※お使いになるシステムで用いるパスワードは複雑にし、貴重品のように管理しましょう。
※多要素認証が利用できる場合は、是非活用しましょう。USBキー等は絶対になくさないようにしましょう。

- **端末や機器を最新にアップデートしましょう**

※OSやソフト、アプリ、機器をアップデートしてセキュリティの穴をふさぎましょう。セキュリティソフトも忘れずに。社内システムの場合は規程に従いましょう。
※古いルータなど、初期管理用パスワードが弱いことがあるため、しっかりしたものか確認しましょう。

新しい働き方とゼロトラストセキュリティ



Duo機能概要
（多要素認証）

Cisco Secure Access by Duo が提供する機能

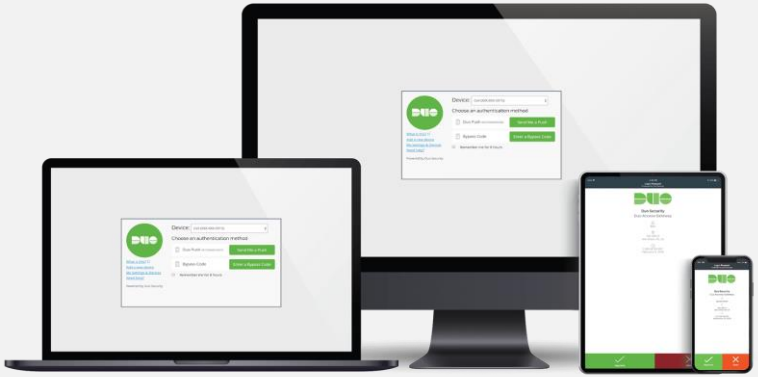
多要素認証によるユーザーの信頼

多要素認証

- 知識要素
- 所有要素
- 生体要素

- ✓ ユーザの認証は瞬時に – ワンタップで承認
- ✓ パスワードに依存しないセキュアなアクセス
- ✓ パスワード漏洩による不正アクセスを防御

端末の信頼性評価



- ✓ 管理デバイスかどうかを検査
- ✓ 危険なデバイスを監視
- ✓ 古いバージョンのOSやブラウザの通知
- ✓ Anti-Virus/Anti-Malwareの検査

Duo多要素認証オプション

認証(MFA)設定
- ユーザグループやアプリケーションごとに 多様なMFAオプションを設定できる
- 容易にユーザ自身でMFAデバイスの追加や削除が可能
  複数MFAデバイス登録可能（認証時に選択可能）

ユーザの使い易さと柔軟性のために複数のオプション（MFAデバイス）を利用可能
- Duo Push 通知
- モバイルパスコード
- 電話へのコール
- SMS
- HOTP トークン
- U2F/WebAuthn（生態認証）
- 緊急時のバイパスコード発行

Duo Mobile

Soft Token

SMS


Biometrics


Phone Callback

Hardware Token


U2F Token

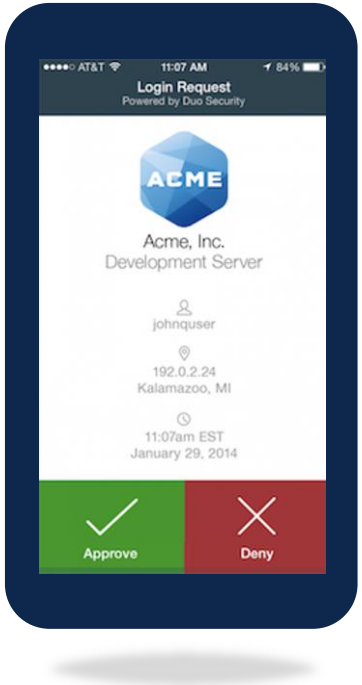
Duo Push 通知

特徴

- 多要素認証オプションの中で最も利用され、より安全な認証方法
  - ✓ 80%以上の認証で利用（Duoユーザ）
  - ✓ メッセージごとに暗号化（公開鍵暗号）
- 簡単に使える – スマートフォンやスマートウォッチで通知を受け、ワンタップで本人確認ができる

留意するポイント

- Duo Push 通知は、iOS および Android で利用可能
- 秘密鍵をモバイルデバイスに安全に保存
- プッシュ通知で追加の生体認証（iOS, Android 機能）を必要とするように設定することが可能



FIDO U2F

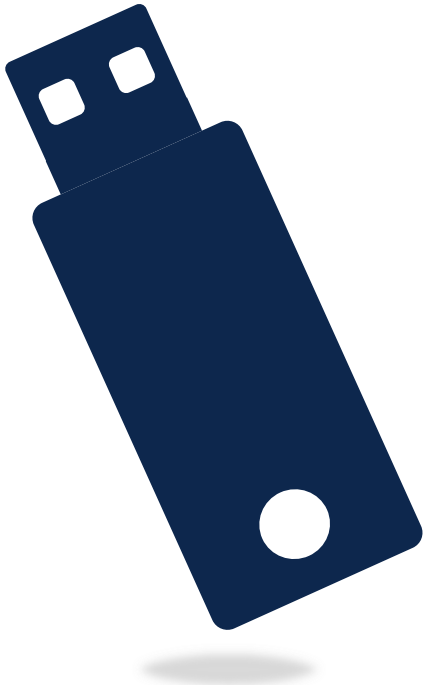
特徴

U2F (universal two factor) セキュリティキー

- ユーザフレンドリーな使いやすさ – ユーザーは、ラップトップの側面に接続したデバイスをタップして本人確認を行う
- 安全 – フィッシングされない、管理ポータルからリモートで無効にすることができる

留意するポイント

- Yubico など、パートナーから提供されている
- U2Fセキュリティキーは、ブラウザのサポートが必要
- ユーザーがキーを紛失する可能性がある



WebAuthn

特徴

WebAuthn (Web Authentication) フレームワーク

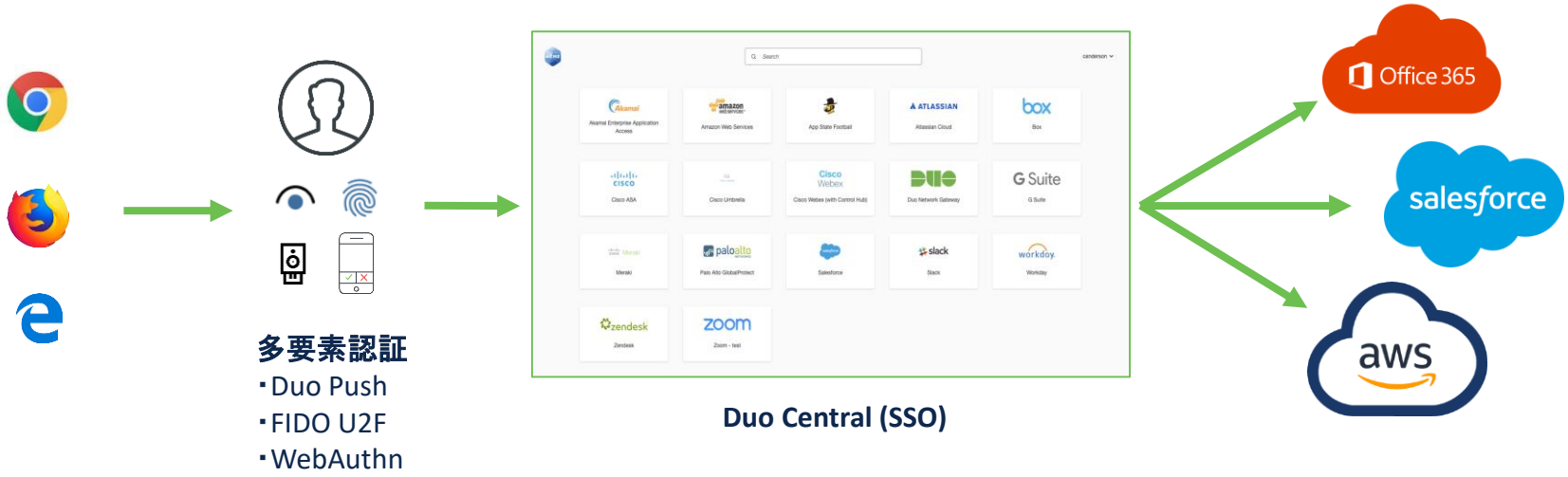
- Touch-ID やWindows Helloのような生体認証を認証方法として使用できるようになる
- 多くのブラウザプラットフォームに拡大

留意するポイント

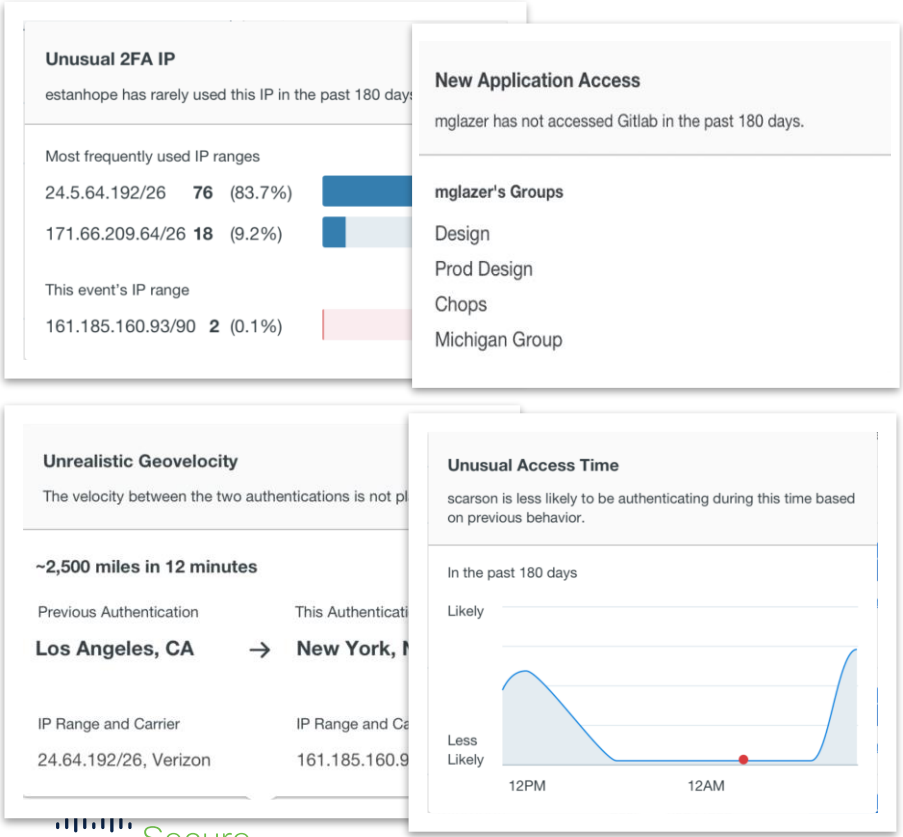
- ブラウザ側でのサポートが必要
- 今後も拡張される分野

Duo Central（シングルサインオン）

- ユーザーは、Duo Central (SSO)を介して、SAMLフェデレーションされた任意のアプリケーションに任意のブラウザから接続できる



Trust Monitor (リスク解析、脅威検知)



Duo Trust Monitor は、企業/組織環境でアクセスアクティビティの調整されたベースラインを作成：

- 通常アクセスする人
- どのアプリケーション
- どのデバイスから
- いつ（時間）
- どこから（場所）

Trust Monitor機能により、異常または危険なユーザー認証の試みをハイライトし、アクセスポリシーを修正または更新することができる。

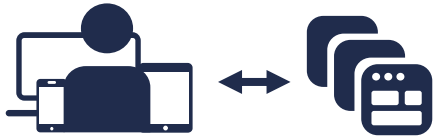
Yubico+Duo事例

Over 20,000 Customers

- 3000+ Technology
- 500+ Higher Education
- 600+ Healthcare
- 1500+ Financial Services
- 350+ Government
- 80+ Fortune 500

Duo Security is now part of Cisco.

Duo for
Workforce



Customer : Facebook

Challenge
- 煩わしさのない強力なセキュリティが必要
  - ✓ 既に利用しているモノ（パスワード）と既に所有しているモノ（スマホなどのデバイス）を組み合わせる二要素認証に注目
  - ✓ 使いやすさ、柔軟なオプション、迅速な導入、そしてサポートのオーバーヘッドを最小限に抑えられるという特長を備えた、強力なセキュリティ

Solution
- Duoの二要素認証では、数多くのソリューションを統合することができる
- 二要素とUSB ポート内で OTP トー クンとして機能する **Yubico 社の YubiKey Nano を組み合わせ**

Business Outcomes
- SSH ログインを頻繁に使用するユーザはラップトップの側面をタップするだけで安全に認証されるだけでなく、移動中やデバイスを紛失した場合にもさまざまな認証方式を選択可能になった
- Linux サーバに導入された Duo の二要素認証は、**Facebook 社内で利用が拡張され、現在では VPN、Windows Server、Splunk、OWA などにも導入**

Facebook 社の開発者は、システム開発中に社内のネットワークやデータベースにアクセスします。その際、ソースコードとユーザデータへのセキュリティリスクを回避するため、悪意ある攻撃から開発者を保護しなければなりません。Facebook 社のセキュリティ文化は、開発者が迅速に対応でき、セキュリティを簡単に確保できるようにすることに重点が置かれています。そのため、汎用性と効率が高く、コードを書くために開発サーバにログインするためのワークフロープロセスを合理化できるセキュリティソリューションを必要としていました。1 日に数万のSSH セッションが、60 以上の対話型セッション、および 3,000 を超える非対話型認証が実行されるなか、現状よりも手間をかけることなくニーズをサポートするセキュリティが必要でした。

Learn more

Duo Securityライセンス

Duo MFA

- 多要素認証
- シングルサインオン（SSO）
- 全てのアプリケーションを保護
- SAML2.0 フェデーレーション クラウドアプリを保護
- 適応型グループベースポリシー制御

Duo Access

Duo MFA機能を含む

- デバイスの可視化
- デバイスベースポリシー
- トラストモニター

Duo Beyond

Duo Access機能を含む

- 信頼されるエンドポイントの検出
- Duo Network Gateway（リバースプロキシ）
- Anti-Virus/Anti-Malwareの検知

詳細情報: https://www.cisco.com/c/dam/global/ja_jp/products/catalog/pdf/cisco-duo-security-brochure.pdf

無償でDuoをご利用いただけます！

注）Duo Beyond機能をご利用の場合、ライセンスのアップグレードが必要となりますので、担当営業までご連絡ください。

■30日間フリートライアル申し込みサイト

https://www.cisco.com/c/m/ja_jp/duo/trial.html


cisco
Secure

Duoパスワードレスへの旅

パスワードレス認証とは？

真のパスワードレスは、パスワードに頼らずにユーザーのアイデンティティを強固に保証し、ユーザーは生体認証、セキュリティキー、またはモバイルデバイスを使用して認証を行うことができます。これにより、あらゆる企業のユースケース（ハイブリッド、クラウド、オンプレミス、レガシーアプリ）に対応した安全なアクセスを提供します。

Duoは、技術的なパートナーシップを通じて、ユーザビリティと、より強固な認証を両立させた真のパスワードレスの未来に向けて革新を進めています。パスワードレスは、管理者の負担を軽減し、企業のセキュリティリスクを軽減しながら、ユーザーに抵抗のないログイン体験を提供します。

パスワードレスへの道

段階的なアプローチで、完全なパスワードレスの未来へ：

1 Reduce Reliance

パスワードへの依存を減らす
-> 多要素認証

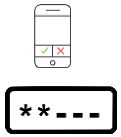
2 Less Passwords

パスワードの利用を少なくする
-> シングルサインオン

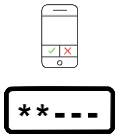
3 True Passwordless

真のパスワードレス
-> U2F, WebAuthn, Duo Mobile

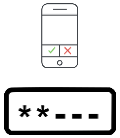
パスワードに依存しない



リモートワークで自宅から、管理されているラップトップにアクセス



SSO経由でWebアプリケーションへアクセス



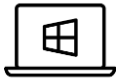
オンプレアプリを利用するためにVPN接続

コーヒーショップからEmailを送信

個人のラップトップでEmailをチェック

シングルサインオン以外でもパスワードレス

リモートワークで自宅から、管理されているラップトップにアクセス



SSO経由でWebアプリケーションへアクセス

オンプレアプリを利用するためにVPN接続

コーヒーショップからEmailを送信

個人のラップトップでEmailをチェック

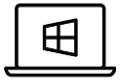
リモートワークで自宅から、管理されているラップトップにアクセス

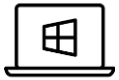
SSO経由でWebアプリケーションへアクセス

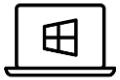
オンプレアプリを利用するためにVPN接続

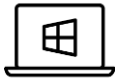
コーヒーショップからEmailを送信

個人のラップトップでEmailをチェック









Trust Monitor