cisco Secure

Cisco Duo 機能紹介

デバイスポスチャと証明書に頼らないデバイス認証

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）
2021年10月28日

Agenda

1. Cisco Secure Access by Duo 概要
2. デバイスの信頼性評価
   デバイスポスチャと証明書に頼らないデバイス認証

Cisco Secure Access by Duo
概要

ゼロトラストの基本

安全なユーザと安全なデバイスを識別する

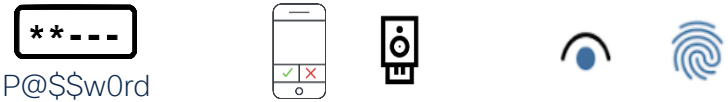
セキュリティ	ユーザエクスペリエンス	デバイス
61%	191	46%
不正侵入の61%以上はID/パスワードの漏洩や、弱いパスワードが原因 - Verizon Data Breach Report	# of passwords：企業で使用する平均のパスワード数 - LastPass Research	脆弱性にパッチを適用していないためにインシデントが発生した組織 - Cisco Cyber Security Report

本人確認とデバイスの健全性確認

Cisco Secure Access by Duo 主要機能

多要素認証（ユーザーの信頼性）

知識要素 ＋ 所有要素 ＋ or 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

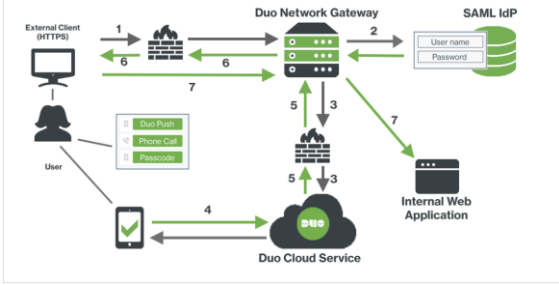
デバイストラスト（信頼性評価）

- ✓ 認証時の検疫機能と管理デバイスかどうかの検査
- ✓ 古いバージョンのOSやブラウザの通知と制御
- ✓ セキュリティソフトウェアの検査
- ✓ 振る舞いベースのリスク分析

シングルサインオン

- ✓ シングルサインオンによるユーザエクスペリエンス向上

ゼロトラストネットワークアクセス（ZTNA）



- ✓ VPNレスによる内部アプリケーションへのセキュアなアクセス（多要素認証とデバイス可視化も実施）

cisco Secure

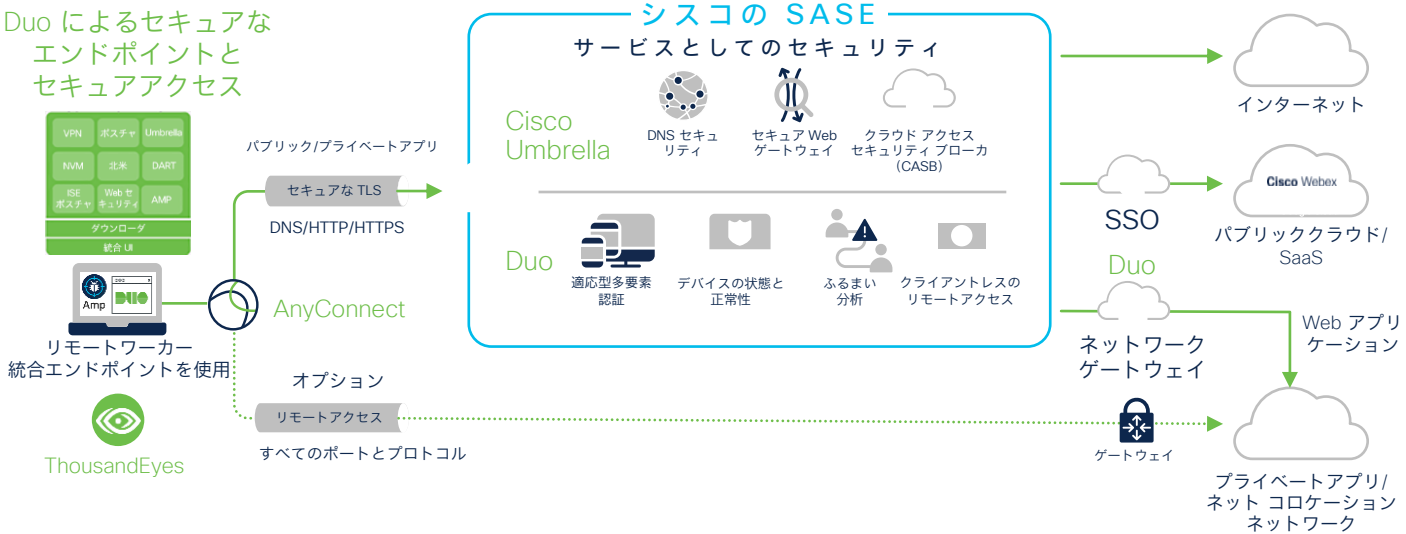
ユースケース：ゼロトラストをベースとした リモートワーカーの保護

必要な機能

- クラウドセキュリティ
- ゼロトラスト セキュアアクセス
- リモートアクセス + ZTNA
- オブザーバビリティ

拡張機能

- MDM
- （統合）Secure Endpoint



大規模ゼロトラスト構築 – Press Release

セキュリティ

ゼロトラスト対応「次世代テレワーク基盤」をドコモ・システムズ、日立、シスコが構築

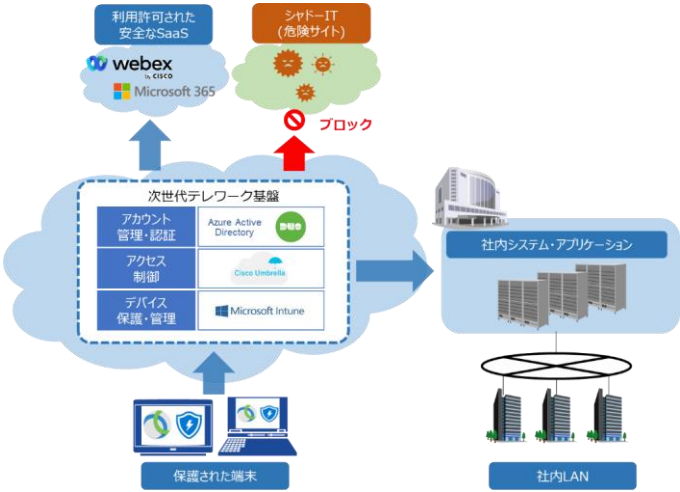
Press Release

～テレワーク環境の安全性と利便性を両立し、コミュニケーションの活性化や生産性の向上を支援～

ドコモ・システムズ株式会社(以下、ドコモ・システムズ)、株式会社日立製作所(以下、日立)、シスコシステムズ合同会社(以下、シスコ)は、ドコモ・システムズのDXプロジェクトの一環として、セキュアで快適なテレワーク環境を整備するため、ゼロトラストネットワーク技術を活用した「次世代テレワーク基盤*1」を構築しました。ゼロトラストネットワークは、アクセス情報をすべて信頼せず(ゼロトラスト)、あらゆる端末や通信のログを取得し、都度認証を行うもので、クラウドシフトが進むDX(デジタルトランスフォーメーション)時代に即したセキュリティモデルです。

本取り組みでは、日立グループのゼロトラストネットワークの導入ノウハウとシスコとの強固なパートナーシップを生かし、先行導入を進めていたMicrosoft 365とシスコのゼロトラスト関連サービスを適材適所に組み合わせ、テレワーク環境の安全性と利便性の両立を実現しました。

2021年7月より、ドコモ・システムズにて、管理部門からシステム開発部門まで700名規模で利用を開始しており、各自の業務端末からインターネットに直接接続し、社内システム・アプリケーションとクラウド上のSaaS*2の双方へセキュアかつ快適にアクセスすることが可能になりました。これにより、今後さらなるコミュニケーションの活性化や生産性の向上が期待されています。

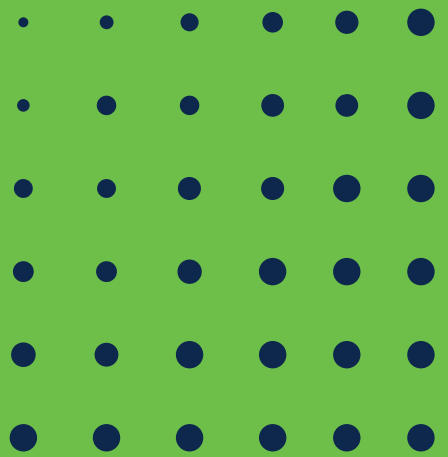


現在、10,000ユーザ以上

出典: https://www.docomo-sys.co.jp/news/pdf/PressRelease20210826.pdf
https://news-blogs.cisco.com/apjc/ja/

デバイスの信頼性評価

デバイスポスチャと
証明書に頼らない
デバイス認証



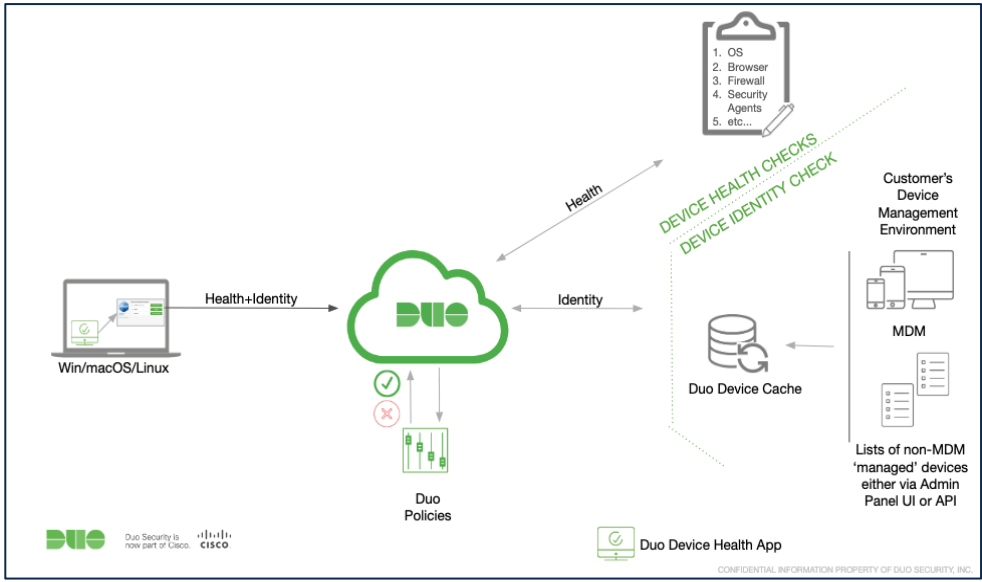
デバイストラスト（信頼性評価）
デバイスポスチャと証明書に頼らないデバイス認証

Device Health（デバイスポスチャ）

- 認証時にデバイスのセキュリティ情報を取得し、信頼性の評価と検疫を実施
- OSバージョン（パッチ）、ブラウザバージョン、Firewallの状態、セキュリティエージェントの動作などを検査

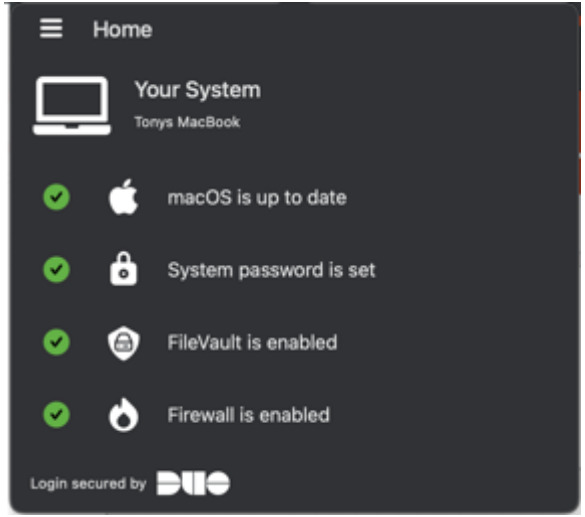
Device Identity（デバイス認証）

- 認証時に、ユニークなDevice ID情報を取得し、Duoに登録されたIDと一致すれば管理デバイスと認識
- デバイスの盗難や紛失の際、Duo Admin PanelでEndpointのDeny Access設定することで、デバイスからのアクセスをBlockすることも可能



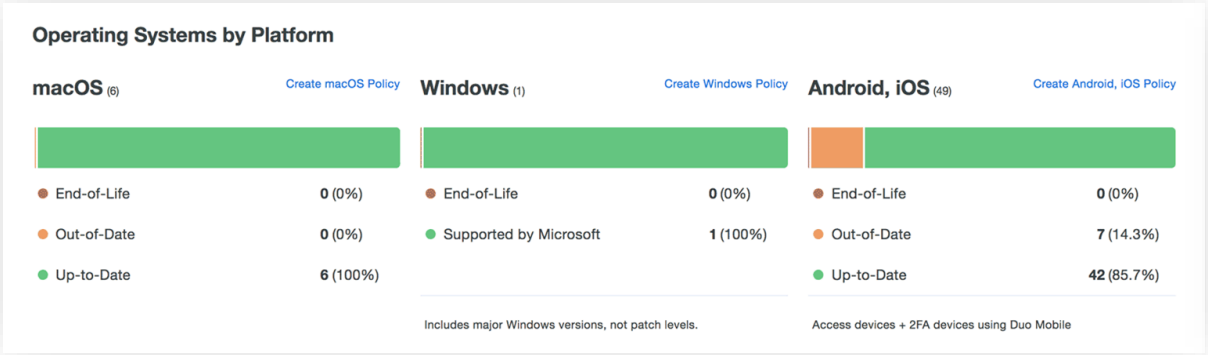
デバイスのポスチャと正常性

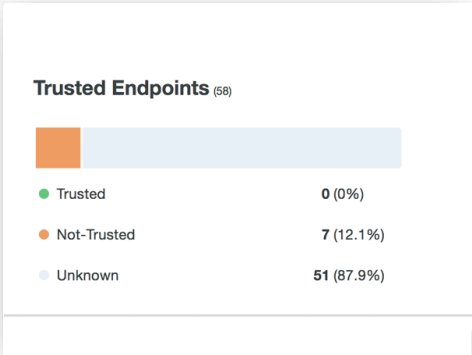
- 最新のソフトウェアを実行しているか？
- 暗号化されているか？
- パスコードで保護されているか？
- 画面ロックが適用されているか？
- ファイアウォールは有効か？
- 生体認証は有効か？
- デバイスは管理対象か BYOD か？



全てのデバイスを包括的に可視化

Duoで収集されるセキュリティ関連情報





モバイルデバイスの可視化

- ✓ コーポレートマネージド 状態
- ✓ バイオメトリックス (指紋/顔認証) 状態
- ✓ スクリーンロック 状態
- ✓ OS コンディション (Tampered) 状態
- ✓ 暗号化 状態
- ✓ プラットフォーム タイプ
- ✓ デバイス OS タイプ & バージョン
- ✓ デバイス オーナー
- ✓ Duo Mobile バージョン

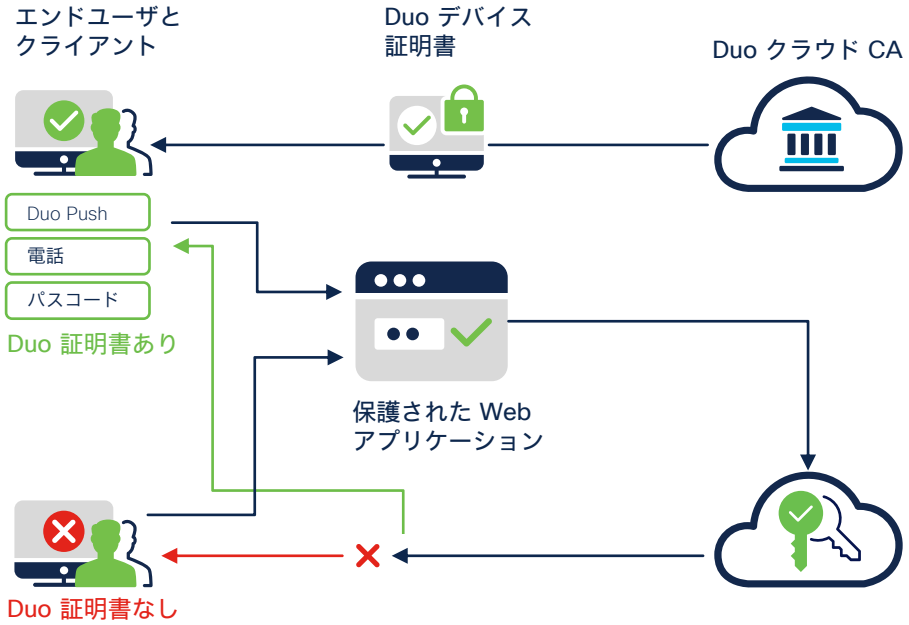
ラップトップ/デスクトップの可視化

- ✓ コーポレートマネージド 状態
- ✓ デバイス オーナー
- ✓ OS タイプ & バージョン
- ✓ ブラウザ タイプ & バージョン
- ✓ Flash & Java プラグイン バージョン
- ✓ OS, ブラウザ, プラグイン 状態
- ✓ ディスク 暗号化
- ✓ Firewall
- ✓ セキュリティソフトウェアの検査

信頼できるデバイスの検査

証明書ベースのデバイス認証

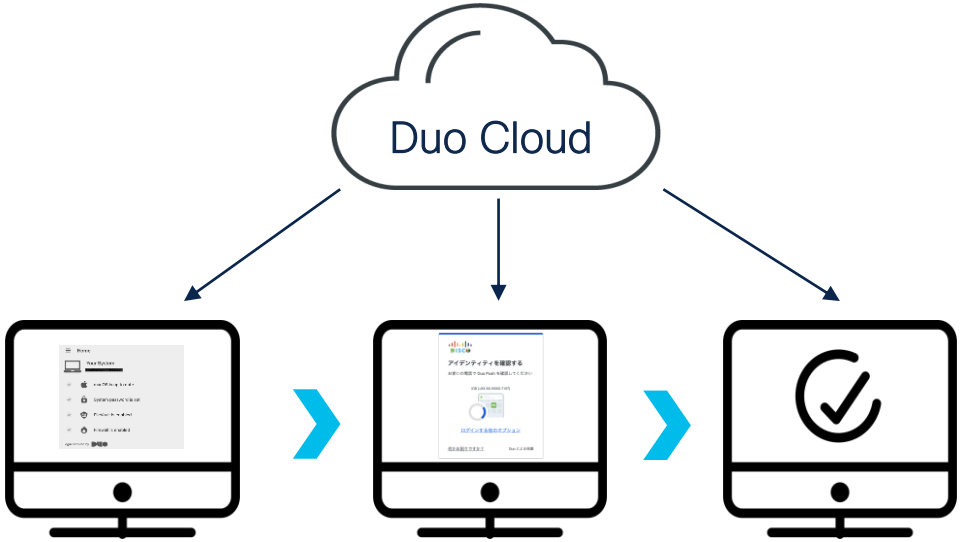
1. Duo が、管理対象デバイスに、Duo のクラウドベース PKI からクライアント認証の証明書を発行する
2. ユーザが、Duo で保護されたブラウザベースのアプリケーションにログインすると、Duo のインラインプロンプトが表示される
3. Web アプリケーションへの最初のログインが成功すると、クライアントは Duo にリダイレクトされる
4. Duo のクラウドサービスが、信頼できるエンドポイントのポリシー設定を、アクセス試行に適用する
5. Duo プロンプトが、ユーザの個人ストアで Duo デバイス証明書の有無を確認する。存在する場合、Duo は、エンドポイントを信頼済みとして報告する
6. Duo の証明書が存在しない場合、エンドポイントに証明書がない（つまり、管理対象エンドポイントではない）と報告する。そのデバイスのアプリケーションへのアクセスはブロックされる可能性がある



詳細情報 - https://duo.com/docs/trusted-endpoints

信頼できるデバイスの検査

証明書に頼らないデバイス認証



1. **Duo が、管理対象デバイスに、Duo Device Health アプリケーション (DHA) をインストールする**
2. ユーザが、Duo で保護されたブラウザベースのアプリケーションにログインすると、Duo のインラインプロンプト (Duo プロンプト) が表示される
3. Web アプリケーションへの最初のログインが成功すると、クライアントは Duo にリダイレクトされる
4. Duo のクラウドサービスが、信頼できるエンドポイントのポリシー設定を、アクセス試行に適用する
5. **Duo プロンプトが、DHAを介してユニークなDevice IDを取得し、Duoに登録されたIDかどうか確認する。存在する場合、Duo は、エンドポイントを信頼済みとして報告する**
6. **Duo で管理するデバイスのユニークなIDが存在しない場合、管理対象エンドポイントではないと報告する。そのデバイスのアプリケーションへのアクセスはブロックされる可能性がある**

Device Health as Trust (DHAT)

インテグレーション動作仕様

統合方法	サポートステータス	デバイストラスト（デバイス認証）決定プロセス
Jamf Pro	サポート済み	DuoはJamf APIコールを利用して、お客様のJamfテナントでアクティブに管理されているデバイスのリストを更新 認証時、Jamf で管理されているデバイスかをチェック
Active Directory (Domain Joined Device)	サポート済み	ADドメインに参加しているデバイスが前提（Domain SIDをDuoに登録） 認証時、ADドメインに参加しているデバイスかをチェック
MS Intune VM Workspace One Meraki SM	サポート予定 （今年中）	DuoはIntune/WS1/MerakiのAPIコールを利用して、お客様のIntune/WS1/Meraki テナントでアクティブに管理されているデバイスのリストを更新 認証時、Intune/WS1/Meraki で管理されているデバイスかをチェック
Unmanaged Device ・上記以外のツール ・手動設定	サポート予定 （来年前半）	事前にAPIおよび手動でデバイスのユニークなIDをDuoに登録 認証時、事前に登録されたユニークなIDと一致するかチェック

Device Health as Trust (DHAT) 設定

DHAベースデバイス認証

✓ Jamf Pro Integration

1. **Create a Jamf API user**

   1. In the Jamf Console Navigate to System Settings > Jamf Pro User Accounts & Groups
   2. Click " + New"
   3. Create either a **Standard Account** or add an **LDAP Account**
   4. In the **"Account"** tab, enter a username and password. Copy the username and password into the form below.
   5. Set the **"Privilege Set"** to **"Auditor"**
   6. Save the new user

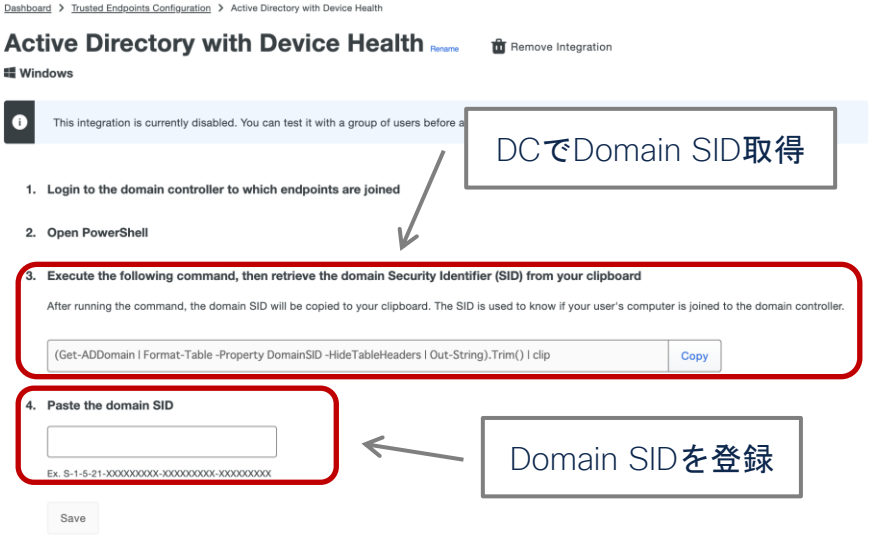
Jamfによる APIユーザ作成方法

2. **Provide account credentials**

   1. Enter the username and password from step 1 into the form below
   2. Enter the api details

Jamfにアクセスするapiユーザの情報を登録

✓ Active Directory Integration



DCでDomain SID取得

Domain SIDを登録

詳細情報

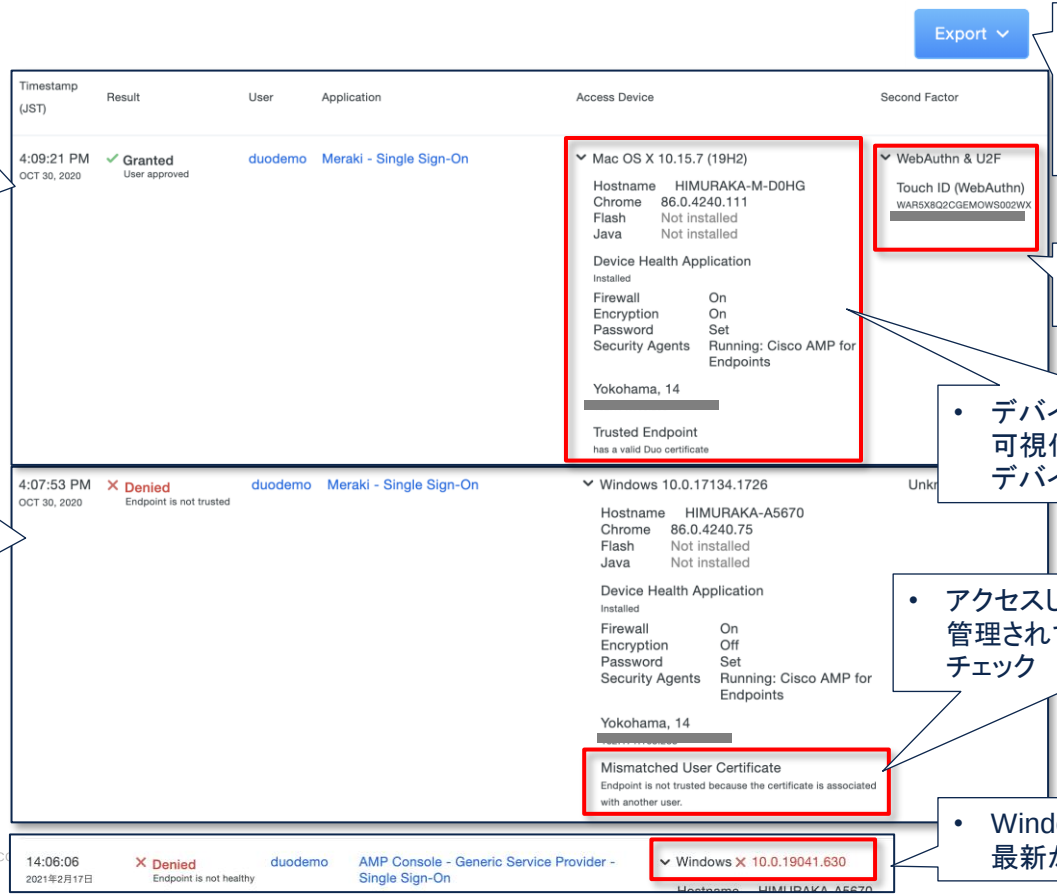
Jamf Integration: https://duo.com/docs/trusted-endpoints-jamf

AD Integration: https://duo.com/docs/trusted-endpoints-adds

認証ログ - 可視化
証跡管理

- 誰が/いつ/どのアプリケーションに/どの端末でアクセスしたかをロギング

- ユーザ/デバイスのチェックを強化し、アプリケーション毎のポリシー適用によって、不適切な場合はアクセス拒否



- ログのExport(手動）
※ログの自動エクスポートはSplunk ConnectorかAPIを使って自動化が可能

- 多要素認証で使った方法も記録

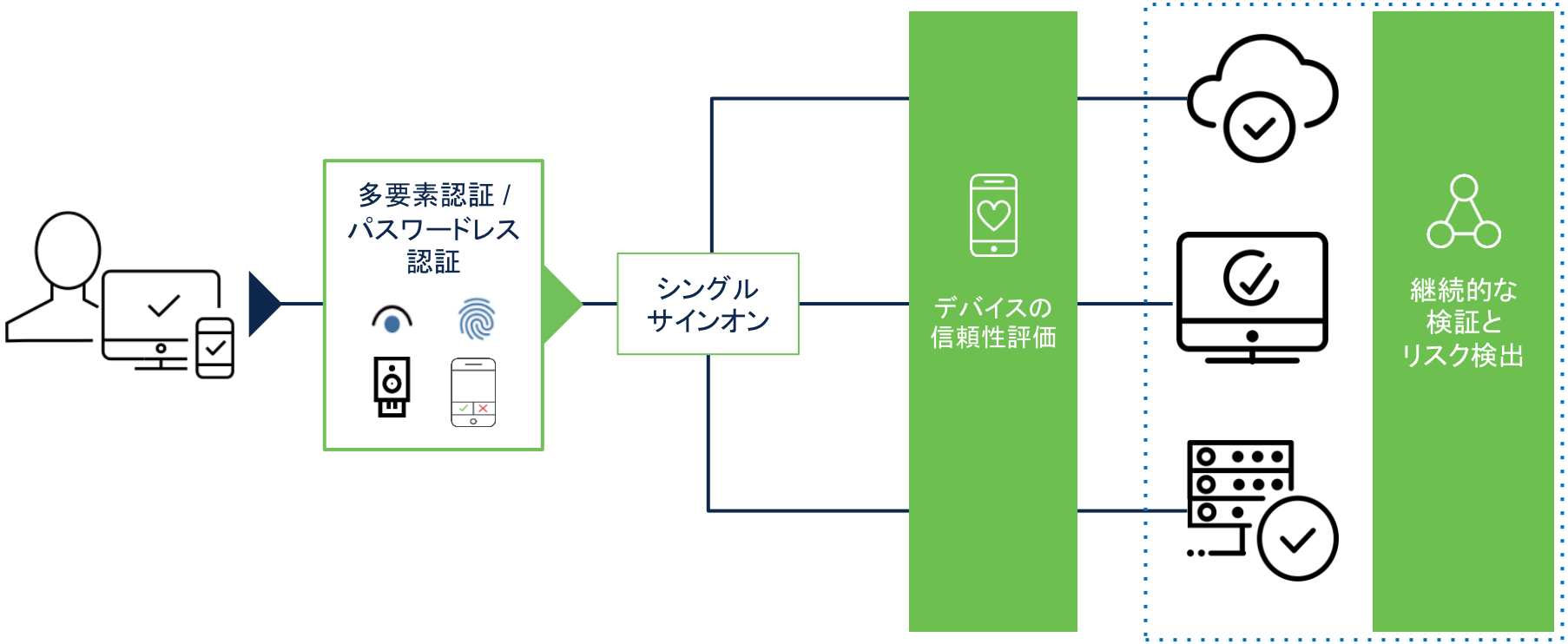
- デバイスポスチャによる可視化されたアクセスデバイスの情報

- アクセスした端末が管理されている端末かどうかチェック

- Windows Updateが最新かチェック

信頼されたユーザとデバイスの継続的な検査

デバイスの信頼性評価、継続的なリスク検出を行いゼロトラストを実現する



無償でDuoを体験いただけます！

注）デバイス認証機能の評価は、Duo Beyond ライセンスが必要となりますので、担当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://engage2demand.cisco.com/LP=24824

Cisco Secure Access by Duo （Duoセキュリティ）無料デモ・30日間無料トライアルお申込み


cisco
Secure