CISCO
SECUREざっくりシリーズ

The bridge to possible

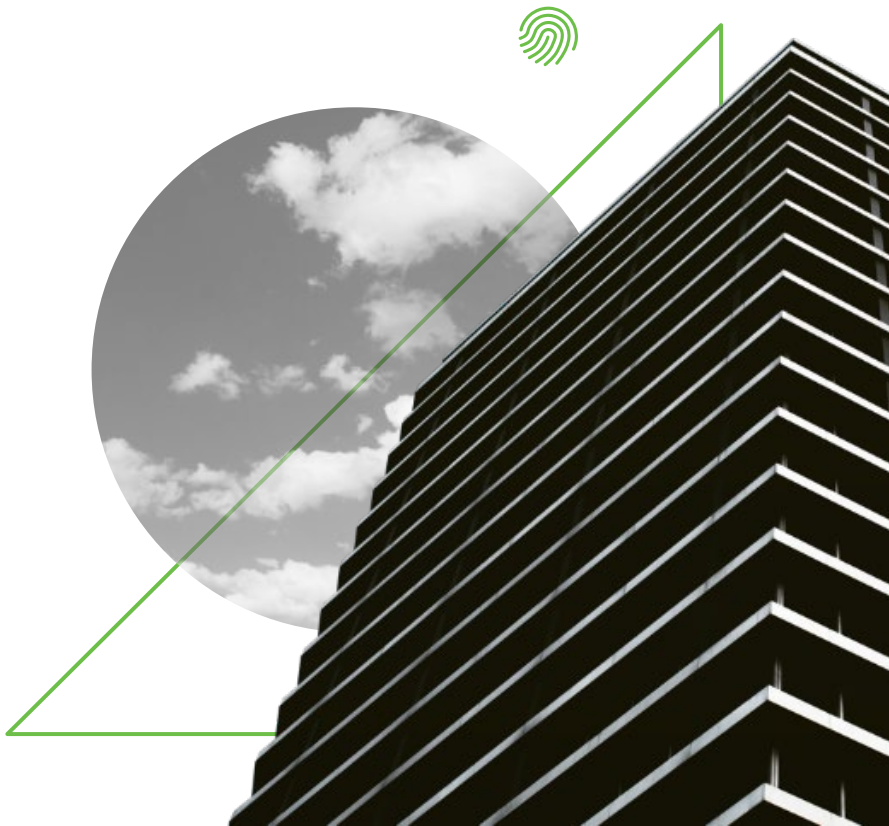
ざっくり Duo Security

シスコシステムズ合同会社
2022年1月

アジェンダ

- Duoとは
- ターゲットとゴール
- 前提知識
- Duoが必要となる背景と課題
- Duoの主要機能の紹介
- Duoの機能と課題との対応付け
- Duoのによる多要素認証
- 代表的な機能の紹介
  - 多要素認証（MFA）
  - デバイス可視化
  - 適応型ポリシー
  - シンプルなセキュアSSO
  - パスワードレス認証
- 補足資料
  - 第三者評価
  - 事例
  - ライセンス情報
- Duoのまとめ
- ネクストステップ

- 参考資料
  - 構成資料



cisco Secure

Duoとは

- アクセスマネジメント領域におけるCisco セキュリティソリューション。
- 代表的な機能としては、クラウド、オンプレの全てのアプリケーションに対して、多要素認証(MFA)を提供し、ID/Password以外の要素を認証に組み込むことで容易に不正アクセス対策を実現。
- デバイスの状態を識別し、アクセス可否の条件として用いることにより、組織が支給していないデバイスや、脆弱なOSやブラウザを持つデバイスのアクセス禁止を実現。

Duoにより全てのアプリケーションの不正アクセスによるデータ漏洩のリスクを軽減します。

ターゲットとゴール

お客様と対面するSE、営業の皆さまが、下記、キーワードを聞いたときに
Duoを思い浮かべて簡易紹介出来るようになって頂ければ幸いです。

前提知識

用語	説明
多要素認証（MFA）	認証時に、IDとパスワード以外に、本人を特定する要素を付加することで、万が一、IDとパスワードが漏洩した際にも、不正アクセスを防止する手法。
シングルサインオン（SSO）	一度のユーザ認証処理によって、独立した複数のアプリケーション、システム上のリソースが利用可能になる機能または環境。SAML認証によって実現する。
SAML	Security Assertion Markup Languageの略称で、SSOやID連携に利用する言語。SAMLを利用して認証することをSAML認証と言い、IdPとSPの役割に分かれて実現する。
IdP	Identity Providerの略称で、アプリケーション、システムにアクセスするユーザーの認証情報を保存・管理するサービス。
SP	Service Providerの略称で、Office 365、Dropboxといったアプリケーション、システムのこと。
ゼロトラスト	利用者や端末、エリアなどを無条件に信頼せずに、リソースやデータへのアクセスに際して、継続的に認証・認可を行うセキュリティモデル。
OTP	One Time Passwordの略称で、一定時間 (数十秒程度) で自動更新、もしくは自動生成されたものが提供され、パスワードの再利用ができない仕組みを実現。
WebAuthn	パスワードに依存しない認証を実現するため技術の一つで、ブラウザや関連するWebサービスの基盤に組み込む標準のWeb API。セキュリティキーはWebAuthnを利用。
境界セキュリティ	FW、IPSのように社内と社外の接点で侵入を防ぐことで社内の安全性を保つセキュリティ。

Duoが必要となる背景と課題
境界セキュリティ以外の新しいセキュリティアプローチが必要

FW/IPSで防げないIDを狙った攻撃の増大

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://www.verizon.com/business/resources/reports/dbir/

求められるゼロトラスト対応

昨今のIT環境の変化により、60%以上の企業がゼロトラスト対応の検討中以上のフェーズ。
*企業IT動向調査報告書 2021 JUAS (売上1,000億～1兆円未満)

https://juas.or.jp/cms/media/2021/04/JUAS_IT2021.pdf

セキュリティと利便性の両立

セキュリティ強化が必要なのは理解できるが、セキュリティを強化することで、利便性が悪くなると、業務効率が悪くなり現場からのクレームが心配。

Duoの主要機能の紹介

多要素認証

知識要素 ＋ 所有要素 ＋ or 生体要素

P@$$w0rd

- ✓ ユーザの認証は瞬時に – ワンタップで承認
- ✓ パスワード漏洩による不正アクセスを防御
- ✓ クラウド、オンプレ全てのアプリに対応可能

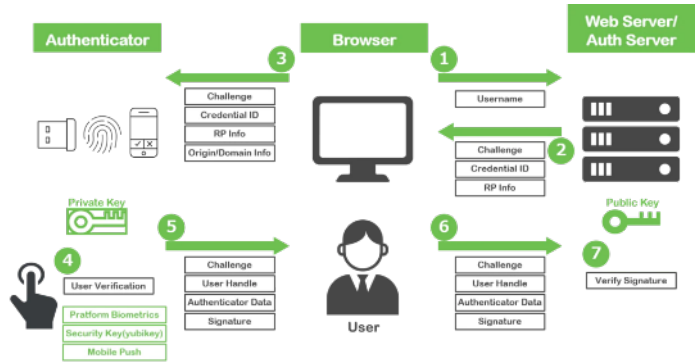
デバイスの信頼性評価

- ✓ 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

パスワードレス認証



- ✓ パスワードレス機能により、セキュリティと利便性の両立を実現

cisco Secure

Duoの主要機能と課題の対応付け

多要素認証

FW/IPSで防げないIDを狙った攻撃の増大

・本人特定をより厳密に行うことで不正アクセス対策を実現

✓ パスワード漏洩による不正アクセスを防御

✓ クラウド、オンプレ全てのアプリに対応可能

デバイスの信頼性評価

求められるゼロトラスト対応

・厳密な本人特定に加えて、継続的に接続されるデバイスの状態に応じた制御も行うことでリスクあるデバイスのアクセス禁止を実現

✓ 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

✓ 振舞いベースのリスク分析

シングルサインオン

セキュリティと利便性の両立

・SSO機能を提供することで、異なるシステム間での認証情報の連携を実現

・生体要素と所有要素により本人を多要素認証することで煩雑なパスワード管理からの解放を実現

✓ 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

パスワードレス認証

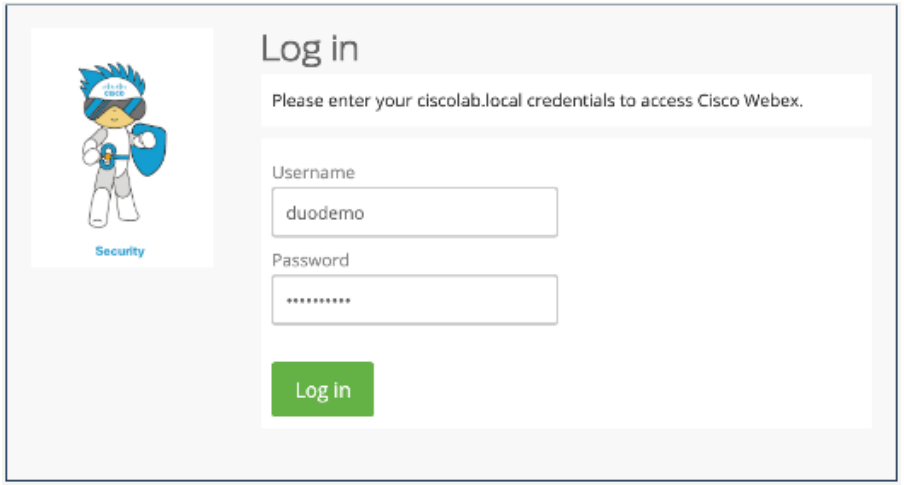
✓ パスワードレス機能により、セキュリティと利便性の両立を実現

Duoによる多要素認証

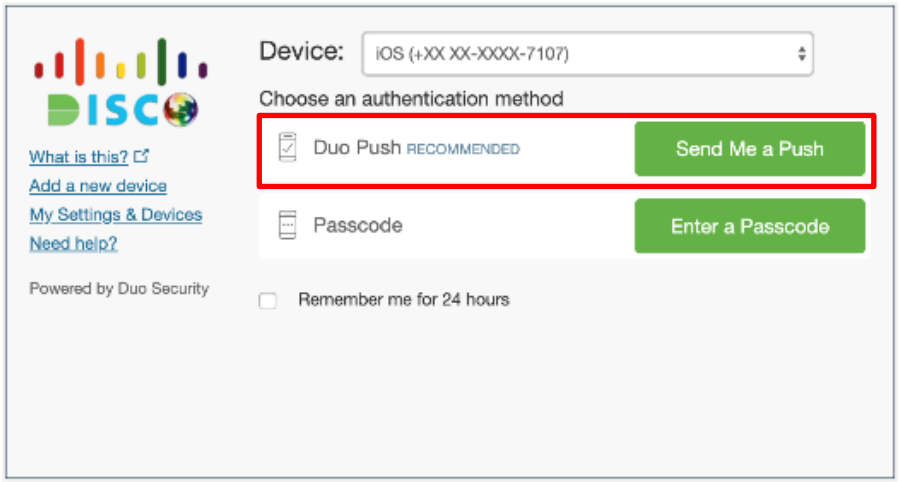
例）Webexログイン時のSAML認証ユーザエクスペリエンス

1 Webexログイン – メールアドレス入力

2 Duo SSO (SAML IdP) へリダイレクトし、プライマリ認証



3 多要素認証方法選択(Duo Push)



4 Duo Pushで認証

5 Webexログイン成功

Duoによる多要素認証
例）WebexとDuoのSAML認証連携イメージ

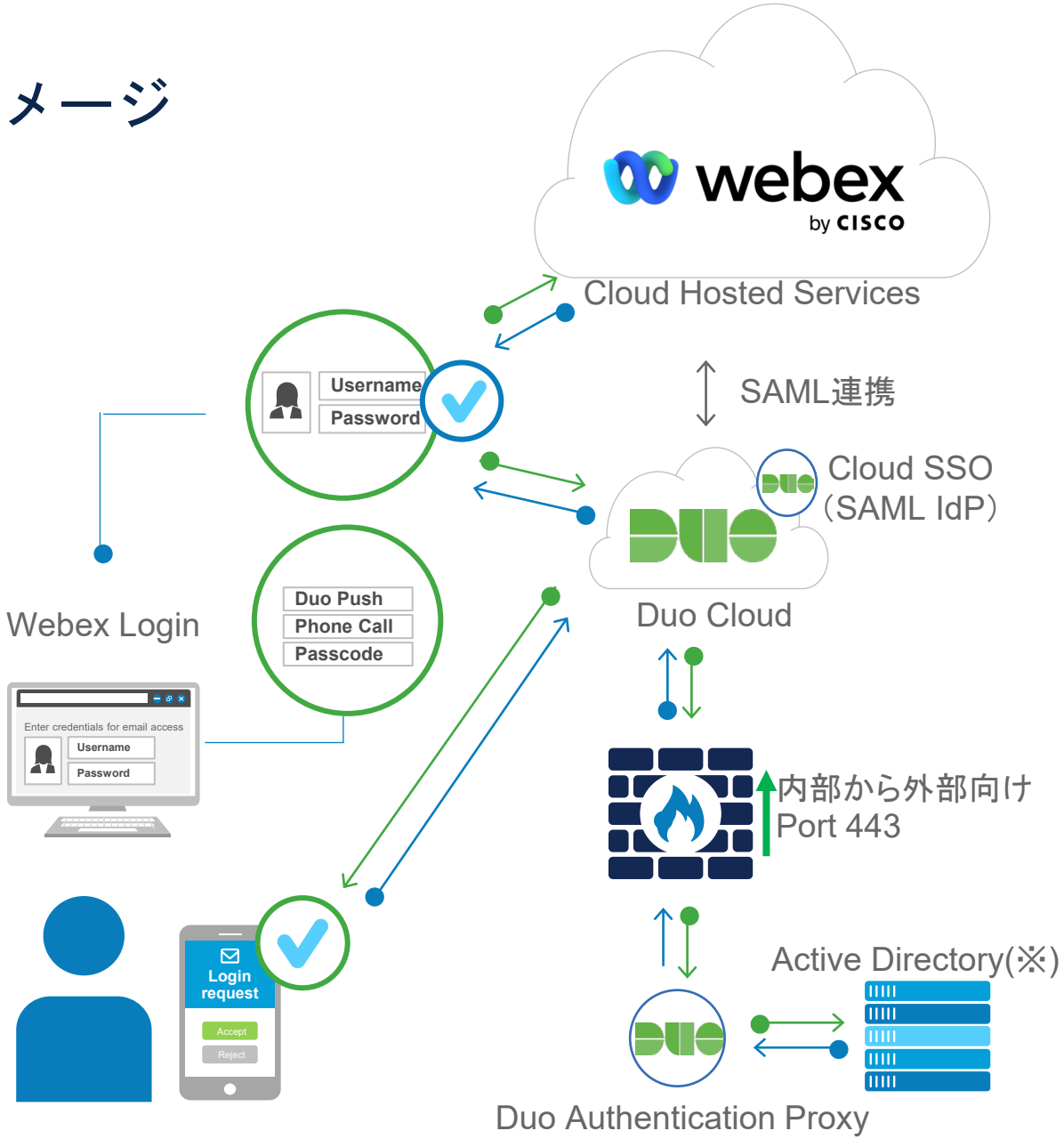
Duo SSO (SAML) インテグレーション

概要:

Duo SSOでSAML IdP機能を提供し、クラウド上のDuo SSOにリダイレクトすることにより、SAML(SP)をサポートするアプリケーションに、多要素認証を追加

特徴:

- SaaSアプリケーションと簡単統合
- まだWeb SSOソリューションを持っていない場合にはSSOポータルとしても利用可能
- Duo SSOでプライマリ認証とセカンダリ認証分離します



※Duoはセキュリティ上の理由からプライマリ認証情報を持たないので、Active DirectoryやAzureAD等のIdPとの連携が必要です。

Duoによる多要素認証
既存認証システムとの容易な連携

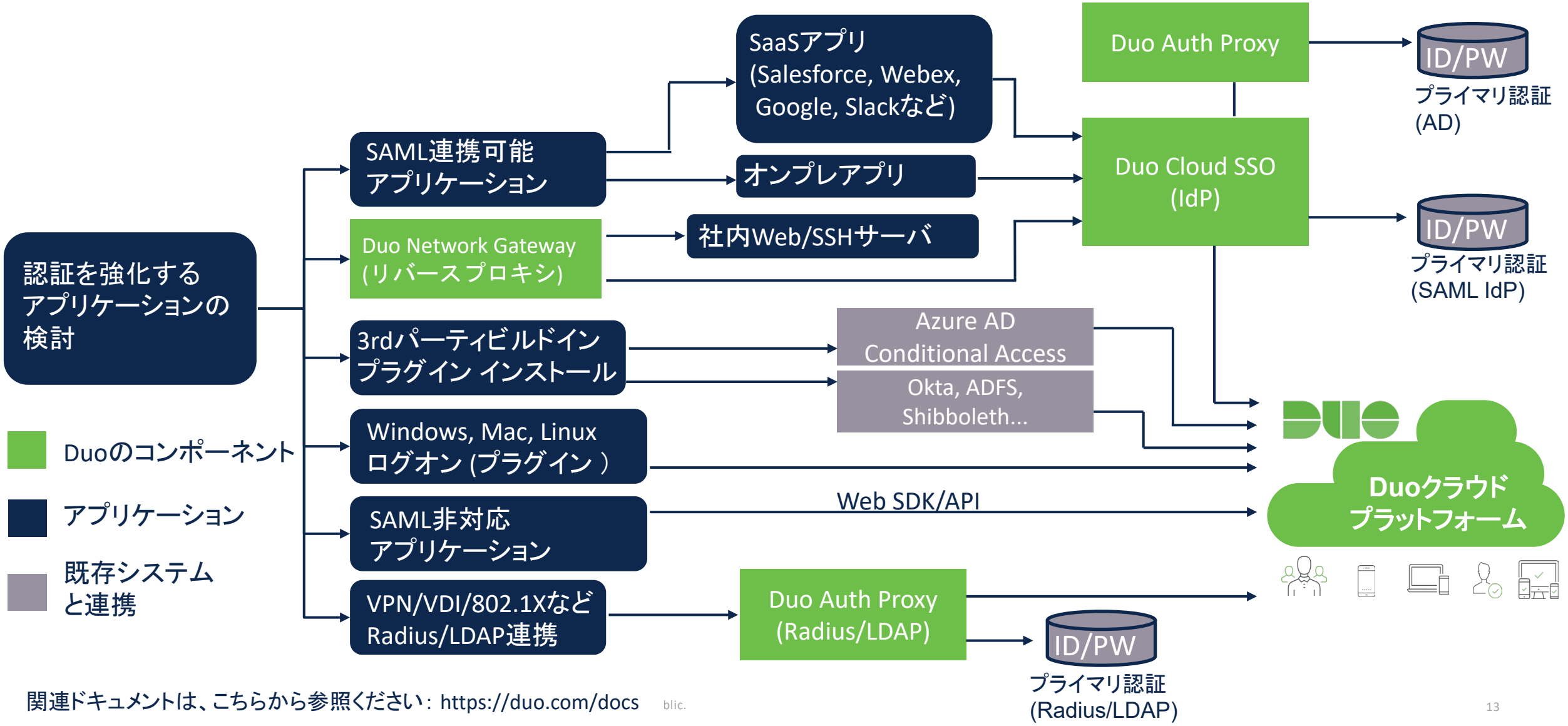
- 認証情報(プライマリ認証)は、別の場所で保存されている
- 複数のアイデンティティ/SSOプラットフォームをDuoで統合（多要素認証基盤）
- すべてのアプリケーションで一貫したエンドユーザーエクスペリエンスとセキュリティのポリシー管理を提供
- すべてのアプリケーションでデバイスの可視性と信頼性確認が可能となる

Duoによる多要素認証
様々なアプリケーションに対応

Microsoft	VPNs	Cloud Apps	On-Premises	SSO	Custom
Office 365	CISCO	salesforce	Epic	Microsoft Azure	REST API
Outlook	f5	Google Apps	ORACLE PEOPLESOFT	Active Directory Federation Services	WEB SDK
Remote Desktop Services	CITRIX	amazon web services	vmware Horizon View	okta	RADIUS
Windows Server	paloalto NETWORKS	box	>_SSH unix	PingIdentity	LDAP
RRAS	Pulse Secure	slack	Shibboleth	onelogin	SAML
					OIDC

詳細情報: https://duo.com/docs

Duoによる多要素認証
アプリケーション種別に応じたDuoでの対応方法



関連ドキュメントは、こちらから参照ください：https://duo.com/docs

代表的な機能の紹介

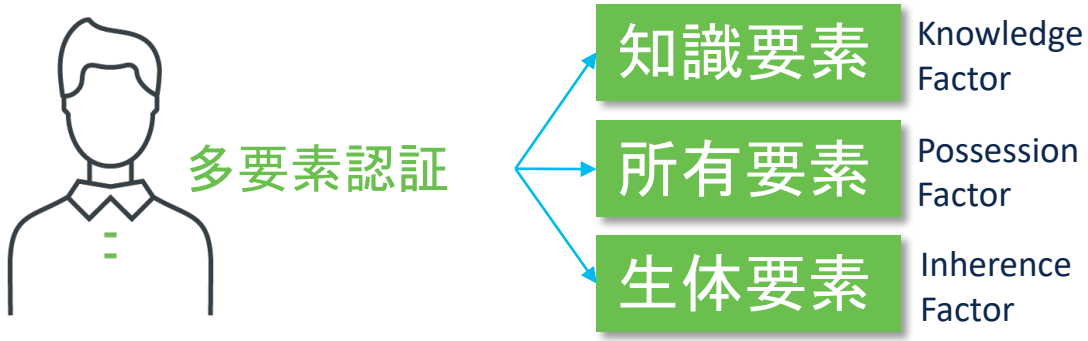
1. 多要素認証（MFA）
2. デバイス可視化
3. 適応型ポリシー
4. シンプルなセキュアSSO
5. パスワードレス認証

多要素認証（MFA）

Duo MFAの認証

ユーザは、既存のプライマリ認証を利用しログイン
(*ユーザが知っているもの* = username + password)

Duo は、ユーザにセカンダリ認証を求める (例：*ユーザが所有しているもの* = ユーザのスマートフォンのDuo Mobile Appに Push 通知を送信)



Duo MFAによって

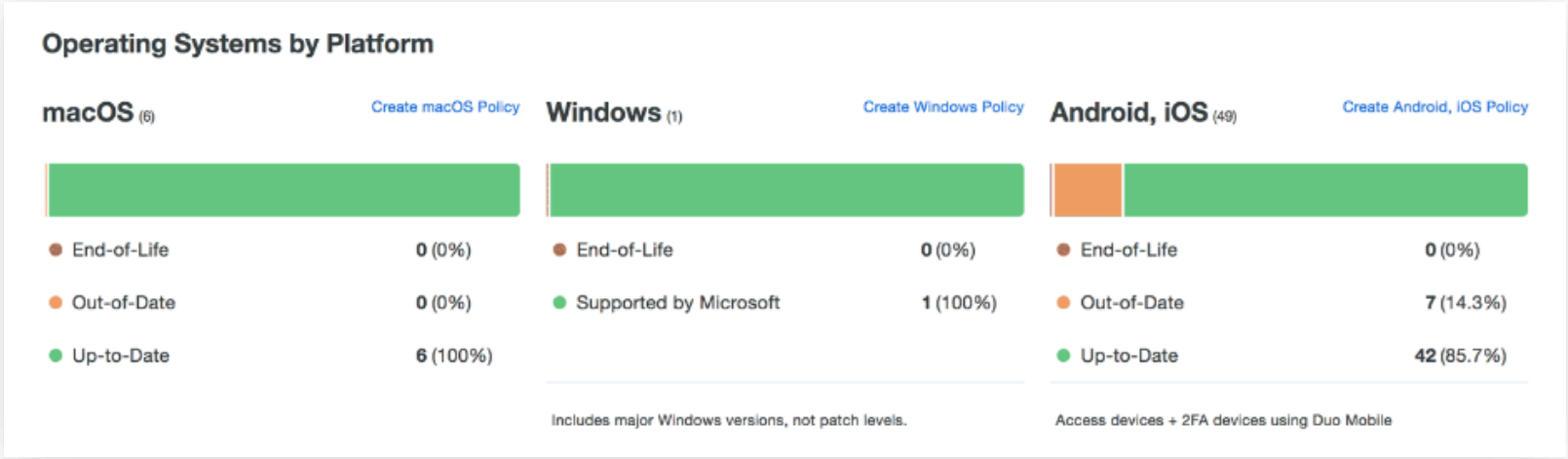
- ✓ アイデンティティベースの攻撃を防ぐ
- ✓ 攻撃者による盗まれたパスワードや侵害されたパスワードの利用を阻止する
- ✓ パスワードのみへの依存度を下げる

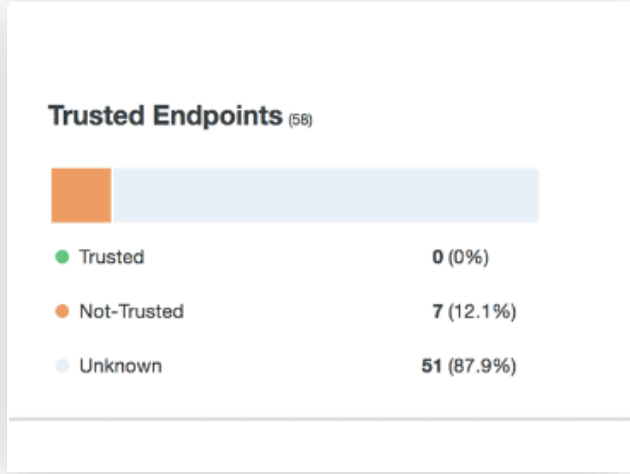
MFA設定

- 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）

複数のMFAオプション

デバイス可視化





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(※)
- ✓ Anti-virus/Anti-malware(※)

cisco Secure

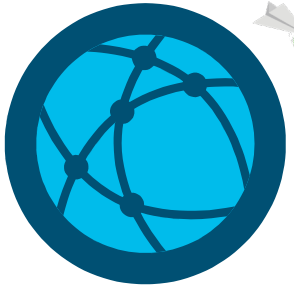
※要Device Healthエージェント

適応型ポリシー
カスタマイズ可能なアクセスポリシー設定により、セキュリティリスクを削減

Role-Based Policy
個々のユーザやグループに基づき、誰がアプリケーションにアクセスできるかを決定するためのポリシーを実行

Location-Based Policy
特定のジオロケーションからのアプリケーションへのアクセスを認可あるいは不認可

Device-Based Policy
セキュアで保護されたデバイスあるいはマネージドデバイスのアクセスを許可し、危険なデバイスによるアクセスを防止



Network-Based Policy
IPアドレス、サブネットやレンジに基づくアクセスの許可、あるいはTorのような匿名ネットワークからのアクセスを拒否

セキュリティポリシー設定例

- ジェイルブレイクしたiOSやAndroidデバイスがアプリケーションにアクセスするのを防ぐ。
- アクセスするはずのない国からのアクセスを防ぐ。
- Windows XP、7等の期限切れOSを利用しているユーザがアプリケーションにアクセスするのを防ぐ。
- AWSを使った開発で、社内からのみのアクセスを許可し、社外（自宅などからの）からのアクセスを許可しない。
- SFDCへのアクセスは社内からは多要素認証不要だが、社外からは多要素認証を必要とする。

等々

シンプルなセキュアSSO

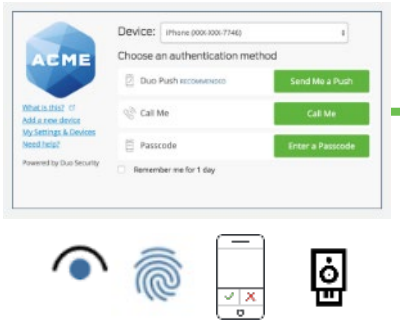
Duo Centralによるユーザとデバイスの信頼によるDuoのシングルサインオン

ブラウザ アクセス

ブラウザにて、ランチャーに対してログイン

【プライマリー認証(※)】
ユーザ名、パスワード

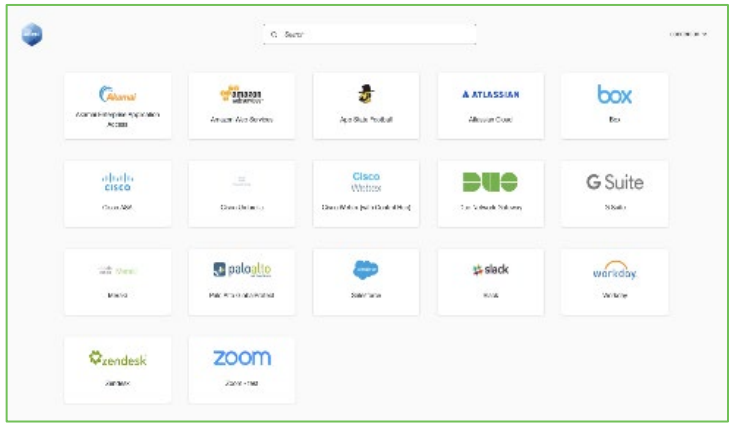
多要素認証



Duo Promptから2要素目の認証方法を選択

【２要素目の認証】
・Duoプッシュ
・ワンタイムパスワード
・セキュリティキー
etc.

Duo Central (SSO)



【 ランチャーが起動 】

・このランチャー上のシステムはログインせずに利用可能
・ログイン保持時間はポリシーで設定可能

SAML対応アプリ

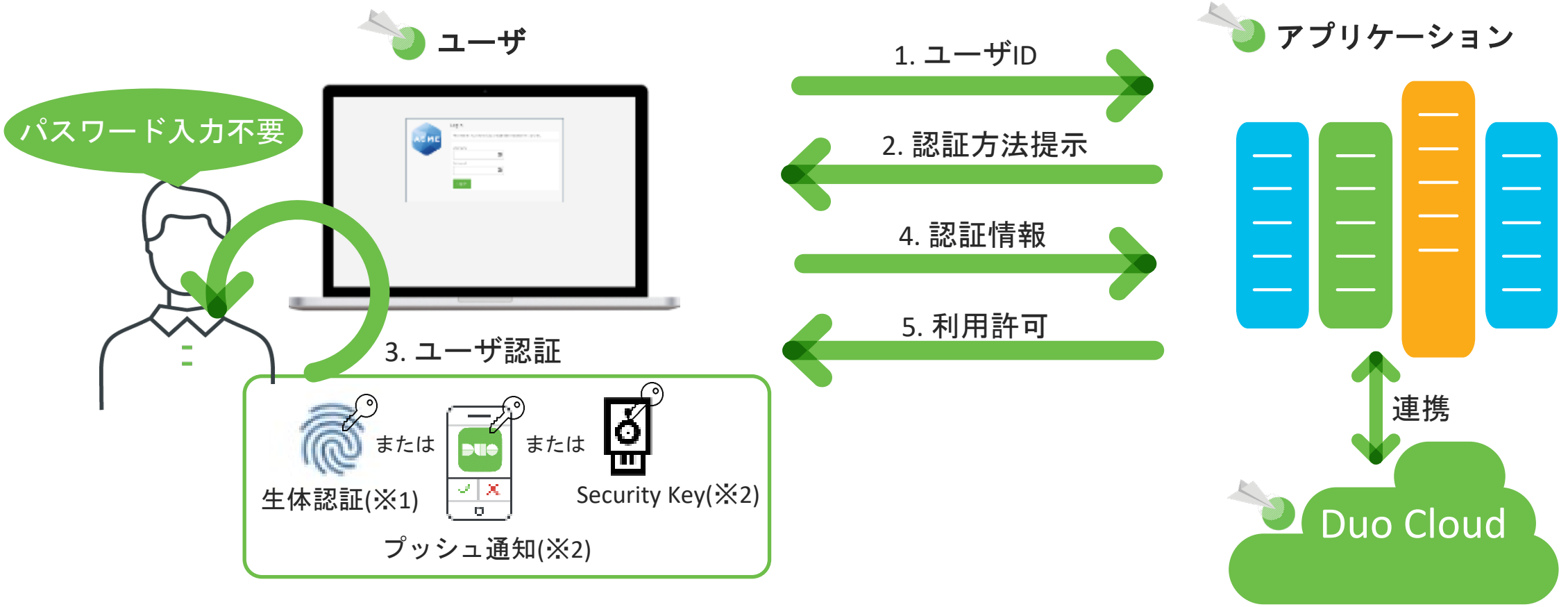
【 アプリケーション起動 】

・全てのSAMLアプリケーションが多要素認証対応可能
・Duo Centralの認証結果を維持したままアプリケーションにアクセス可能。

※Duoはプライマリ認証情報を持たないので、Active DirectoryやAzureAD等のIdPとの連携が必要です。

パスワードレス認証

パスワード入力無しに秘密鍵と生体認証等により多要素認証を実現



※1　Touch ID, Face ID, Windows Hello, Android fingerprint and face recognition
※2　生体認証もしくはPINコードによる保護が必要。

補足情報

1. 第三者評価
2. 事例
3. ライセンス

第三者評価

GartnerとITreviewにおいてお客様からの非常に高い評価を獲得

Gartner PeerInsightsの「Voiceofthe Customer」：Access Managementで、Duoがカスタマーチョイスとして認められました。

Duo Security Named a 2021 Gartner Peer Insights Customers' Choice for Access Management | Duo Security

「ITreview Grid Award 2021 Fall」のSSO（シングルサインオン）部門と多要素認証（MFA）部門で、Cisco Secure Access by Duoが「Leader」を初受賞しました。

Cisco Secure Access by Duo が ITreview の多要素認証（MFA）と SSO（シングルサインオン）部門で「Leader」を初受賞

事例
海外だけでなく国内でも導入実績が増加中

Cisco Secure Access by Duo 導入事例

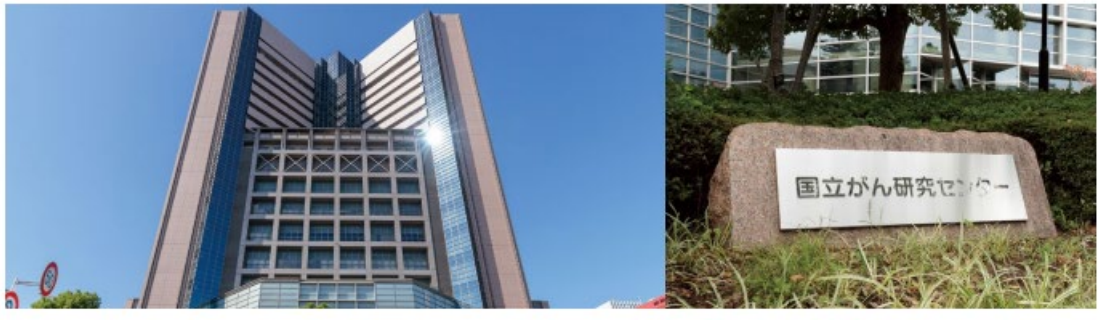
株式会社 CAMPFIRE

信頼性を高める包括的なセキュリティ強化の皮切りとして
全社に多要素認証（MFA）を展開

Cisco Secure Access by Duo 導入事例

国立研究開発法人 国立がん研究センター

多要素認証と PC 健全性確認で安全性を高め
テレワーク拡大に向けた先行導入を実施



DUO お客様成功事例 テクノロジー

Facebook

ソーシャルメディア大手がエンジニアのセキュリティを確保し、
1万人を超えるユーザを保護するために導入したソリューション

DUO お客様成功事例 教育

デューク大学

米国の私立大学が導入した柔軟で信頼できる
多要素ソリューション

ライセンス情報

機能		Duo MFA	Duo Access	Duo Beyond
ユーザトラスト（多要素認証；MFA）	iOSおよびAndroid向けモバイルアプリ「DuoMobile」のプッシュ通知による認証	●	●	●
	アプリ、SMS、電話着信、ハードウェアトークンによるパスコード認証、生体認証(U2FとWebAuthn)	●	●	●
	電話着信認証およびSMS認証クレジット	●	●	●
	ユーザによる自己登録と自己管理	●	●	●
デバイストラスト（デバイスの可視化）	アプリケーションにアクセスするすべてのデバイスを把握できるダッシュボード	●	●	●
	危険なデバイスを監視および識別		●	●
	ノートPC・デスクトップPCのセキュリティ健全性を可視化（Duoデバイスヘルスアプリケーション）		●	●
	モバイルデバイスのセキュリティ健全性を可視化		●	●
	ノートPCおよびデスクトップPCが企業所有か個人所有か識別			●
	モバイルデバイスが企業所有か個人所有か識別			●
	アンチウイルスやアンチマルウェアなどサードパーティ製エージェントが有効かどうか識別			●
適応型認証/ポリシー	セキュリティポリシーをアプリケーション全体または個別に割り当て	●	●	●
	ネットワークが承認済みかどうかに基づいたポリシー適用	●	●	●
	ユーザグループ別にセキュリティポリシーを割り当ておよび適用	●	●	●
	ユーザの場所（ロケーション）に基づいたポリシーを適用		●	●
	匿名ネットワークをブロック		●	●
	ソフトウェアのサポート期限、暗号化やファイアウォールの有無など、セキュリティ健全性に基づいたノートPCおよびデスクトップPCでのポリシー適用		●	●
	暗号化や改ざん、画面ロック、生体認証の有無など、セキュリティ健全性に基づいたモバイルデバイスでのポリシー適用		●	●
	セキュリティ健全性が低い場合にデバイスを修正するようにユーザに通知		●	●
	エンドポイント管理システムでの登録状況に基づいたデバイスのアプリケーションアクセス制限			●
	MDM登録状況に基づいたモバイルデバイスのアプリケーションアクセス制限			●
シングルサインオン（SSO）とリモートアクセス	無制限でのアプリケーション統合	●	●	●
	すべてのクラウドアプリケーションに対してSSOを提供	●	●	●
	社内Webアプリケーションへ安全にアクセス (Duo Network Gateway)			●
	SSH経由で特定の社内サーバへ安全にアクセス (Duo Network Gateway)			●
	AWS、Azure、GCPでホストされているアプリケーションへ安全にアクセス			●
トラストモニター（リスク分析、脅威検知）	ユーザの振る舞い（ユーザ、デバイス、アプリケーション、ロケーション、時間など）を分析し、脅威を検知		●	●

Duoのまとめ

1 不正アクセス対策としての多要素認証機能を提供

ハードウェアトークン以外にも様々な多要素認証に対応
クラウド、オンプレミスの全てのアプリケーションに対応

2 継続的に接続するデバイスの状態を監視

脆弱性を持つ古いOS、ブラウザでのアクセスを禁止
ファイアウォール、アンチウィルスソフトの起動確認による認可

3 セキュリティと利便性の両立を実現

SSOによるアプリケーションログインの簡素化
パスワードレス認証によるパスワード管理からの解放

ネクストステップ

- 概要、デモ
  - PSU-VoD-SEC-Duo-01 概要のご紹介-Duo-01 Overview
  - PSU-VoD-SEC-Duo-02 機能のご紹介-Duo-02 Feature Introduction
  - PSU-VoD-SEC-Duo-03-機能概要-アーキテクチャとデモ - Duo-03 Feature, Architecture-Demo
  - PSU-VoD-SEC-Duo dCloudを使ったデモ方法-Duo Demo
  - PSU-VoD-SEC-Duoライセンスの説明-Duo license
  - Duo 発注ガイド
- 設定資料
  - PSU-VoD-SEC-Duo ポリシーガイド-Duo Policy Guide
  - PSU-VoD-SEC-Duo 多要素認証でのハードウェアトークンの利用-Duo-D100 YubiKey OTP
  - PSU-VoD-SEC-Duoによる特権ユーザ不正アクセス防御-Duo MFA for Windows Logon
  - PSU-VoD-SEC-Duo Network Gateway(DNG)によるゼロトラストネットワークアクセス(ZTNA)-Duo Zero Trust Network Access

参考
6つの導入シナリオ

1. Duo Built-in 3rd party
2. プラグイン/パッケージ
3. Duo Authentication Proxy
4. Duo SSO/SAML
5. Duo Network Gateway
6. カスタム WebSDK/API

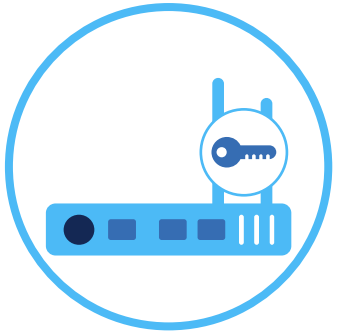
Duo - 6つの導入シナリオ

Duo Built-in 3rd party

プラグイン/パッケージ
インストール

Duo Authentication Proxy

Duo SSO/SAML



Duo Network Gateway

カスタム WebSDK/API

Duo Build-in（サードパーティアプリケーション）

インテグレーション

概要:

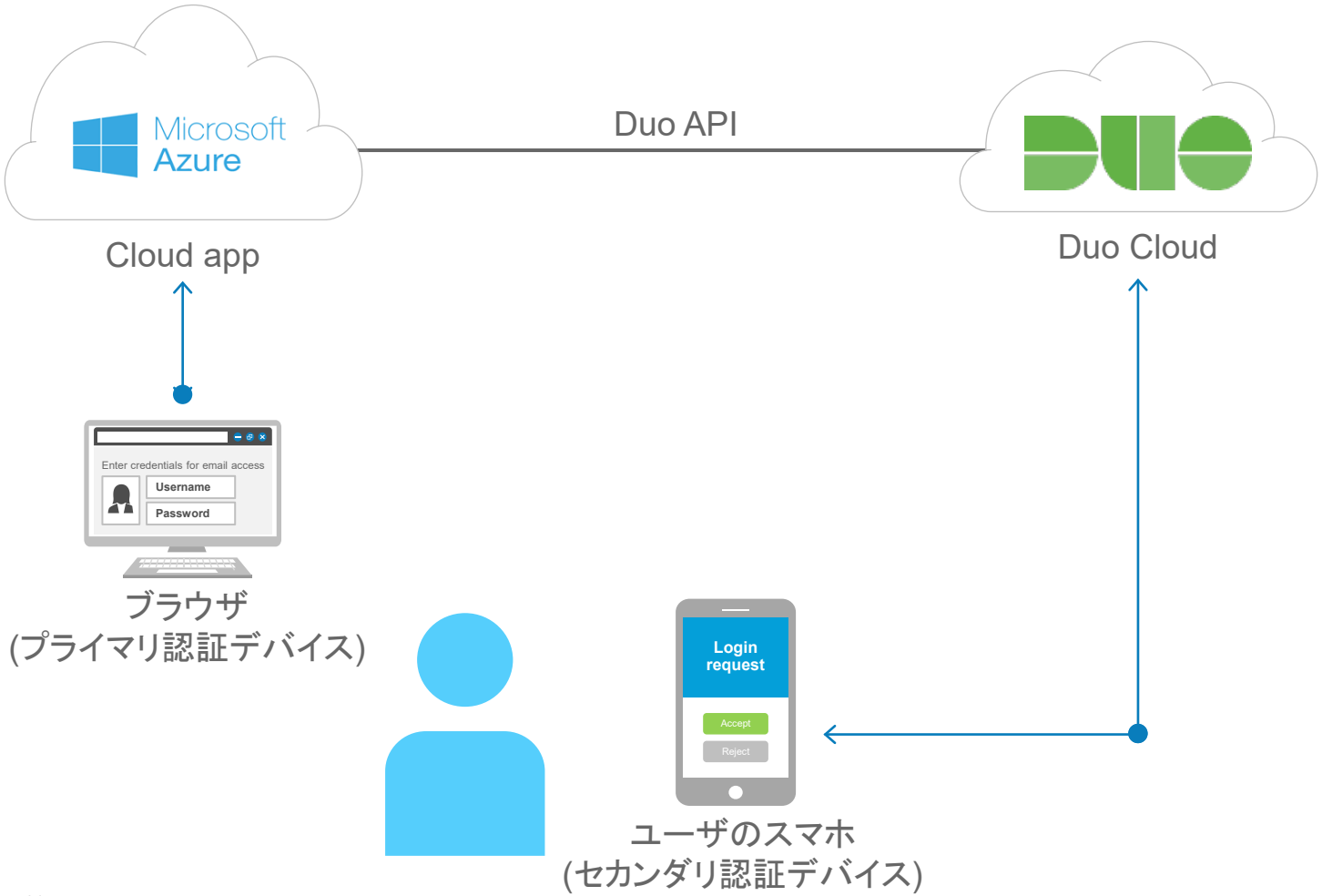
Duoが組み込まれ、アクティベーションの準備が出来ているサードパーティアプリケーションの保護をサポート

特徴:

- 導入時の作業がほとんど必要ない

インテグレーション例

Microsoft Azure　okta　LastPass



プラグイン/パッケージのインストール

インテグレーション

概要:

Duoがアプリケーション用に準備したパッケージを利用し、直接統合を可能にする

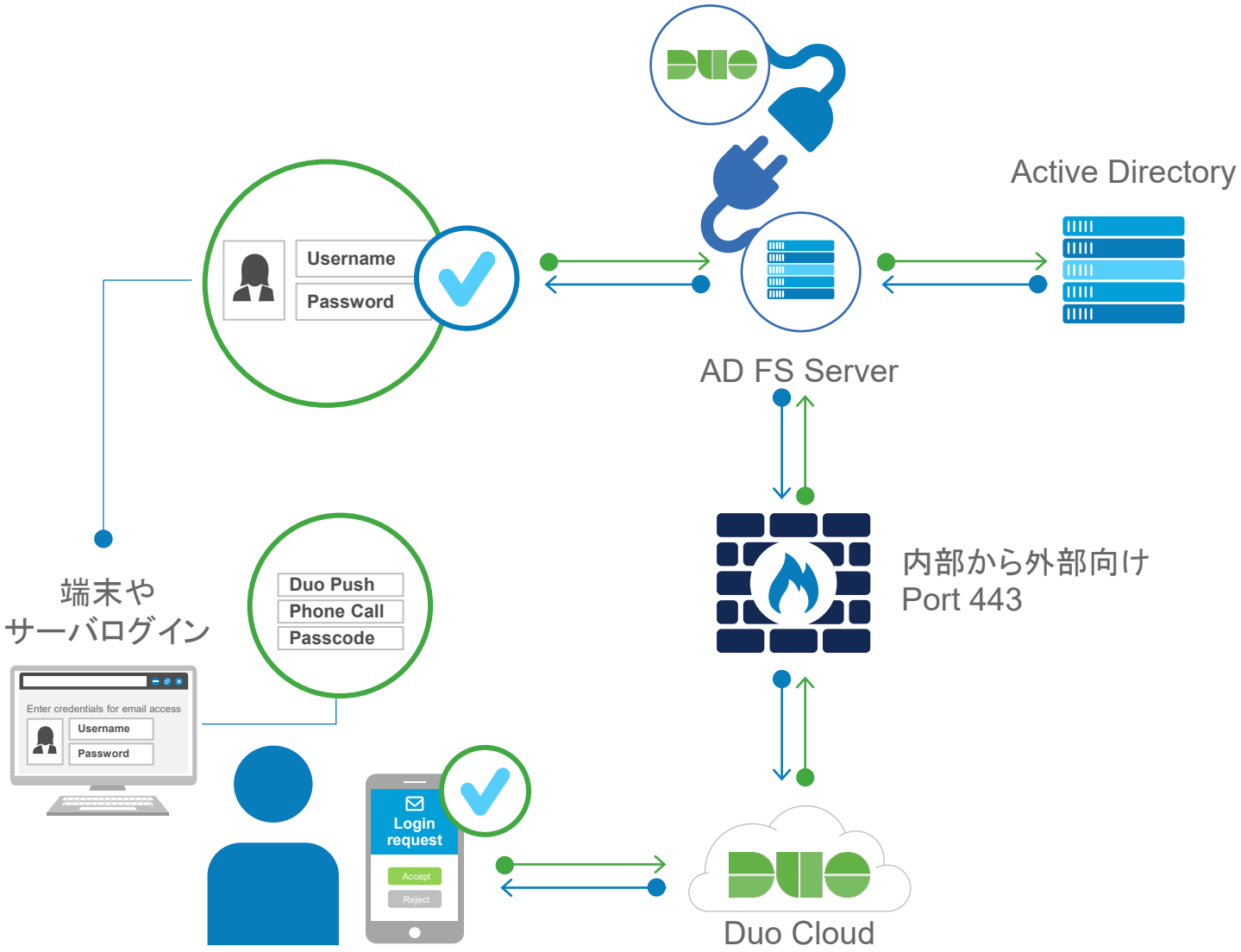
特徴:

- Windows/MACログイン時にMFA適用
- Unix/LinuxのSSHログイン時にMFA適用

インテグレーション例

Microsoft Active Directory Federation Services

Unix/Linux SSH



Duo Authentication Proxy

DAP インテグレーション

概要:

Duoクラウドとのアプリケーション統合により、RADIUSまたはLDAPをサポートするアプリで、MFAが可能

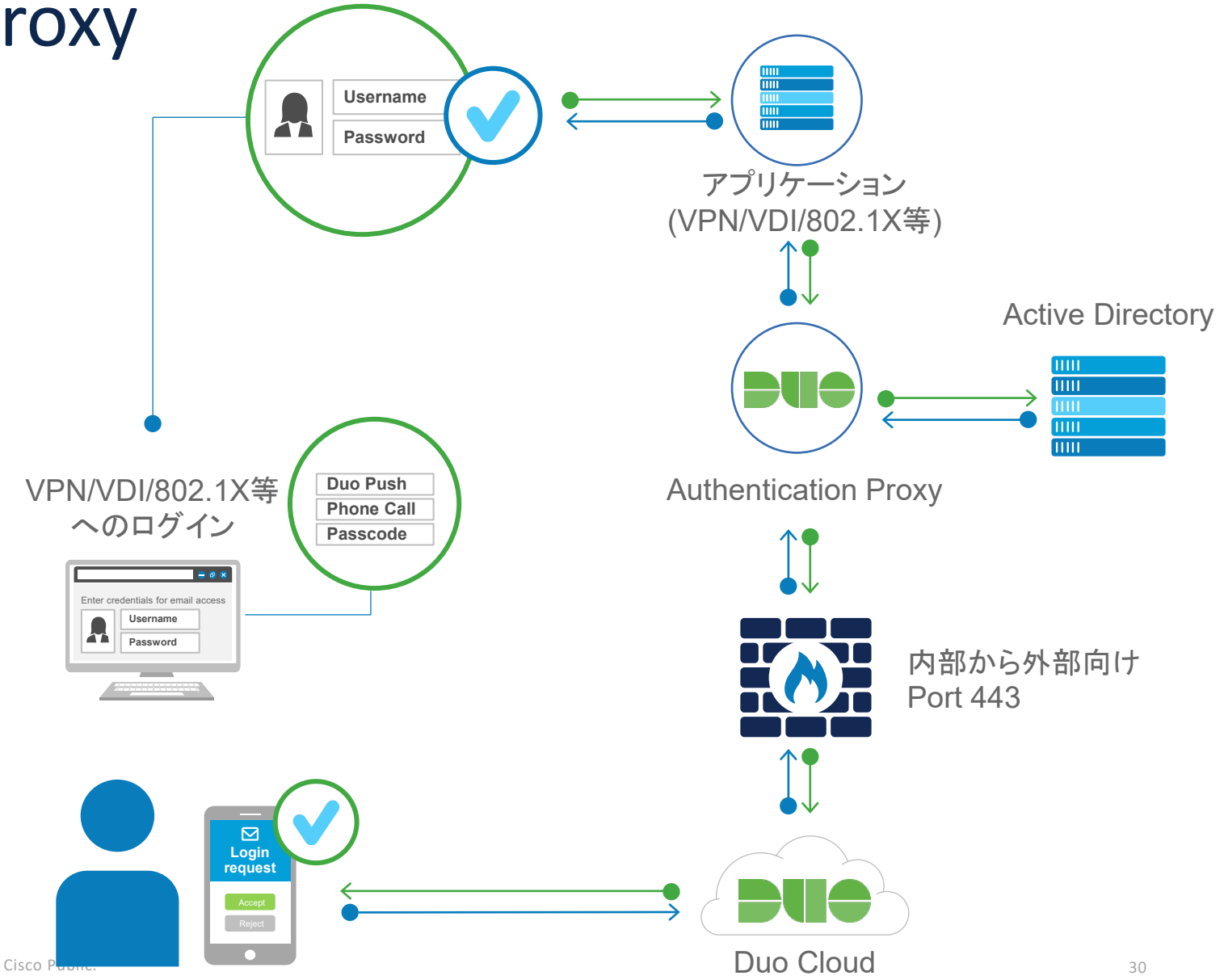
特徴:

- VPN/VDI/802.1X等で利用可能
- DAPのコンポーネントをインストールする必要があります

インテグレーション例

CISCO

Citrix NetScaler



Duo SSO

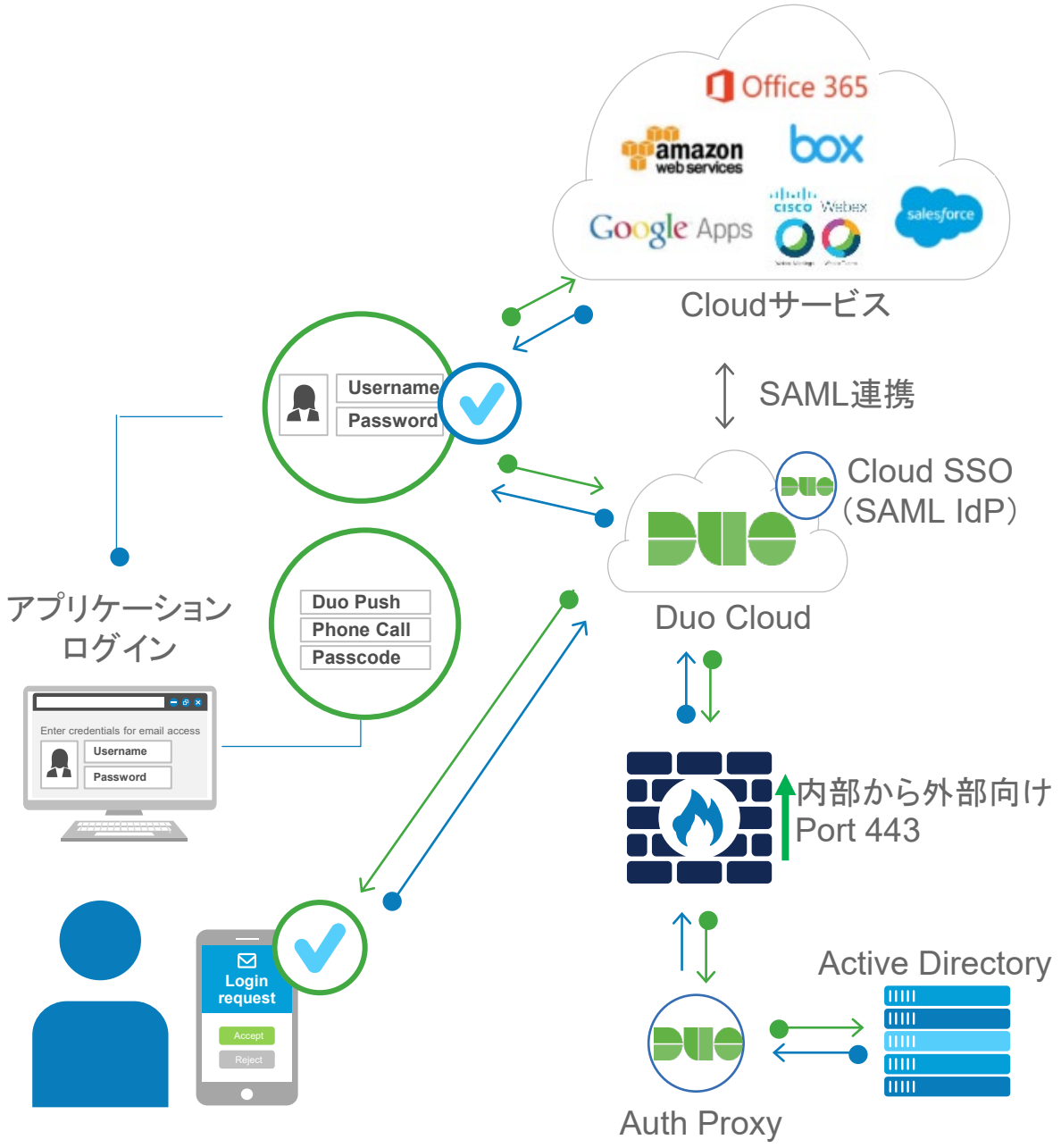
Duo SSO (SAML) インテグレーション

概要:

Duo SSOでSAML IdP機能を提供し、クラウド上のDuo SSOにリダイレクトすることにより、SAML(SP)をサポートするアプリケーションに、MFAを追加

特徴:

- SaaSアプリケーションと簡単統合
- まだWeb SSOソリューションを持っていない場合にはSSOポータルとしても利用可能
- Duo SSOでプライマリ認証とセカンダリ認証分離します



※Duoはセキュリティ上の理由からプライマリ認証情報を持たないので、Active DirectoryやAzureAD等のIdPとの連携が必要です。

Duo Network Gateway (DNG)

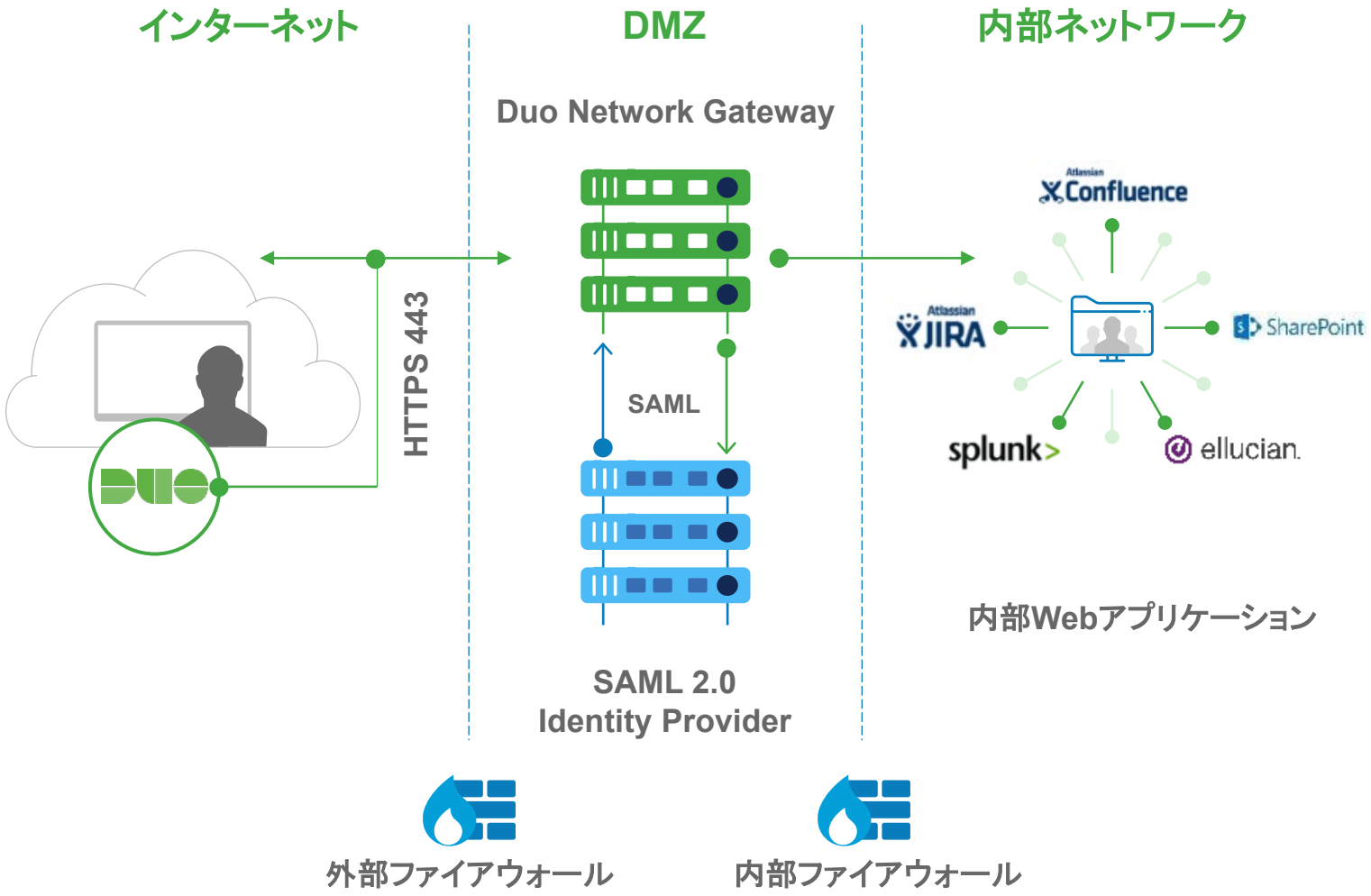
DNG インテグレーション

概要:

ユーザがVPN接続を必要とせず、オンプレミスのアプリやWebサイトに MFAを使ってアクセスできる

特徴:

- ネットワーク全体では無く、アプリ間でアクセスを有効にする
- プライマリ認証に SAML IdPが必要
- 現在、HTTP(S) と SSH プロトコルに対応
- SSHは、クライアントに DuoConnect Clientのインストールが必要



カスタム WebSDK/API

WebSDK/API インテグレーション

概要:

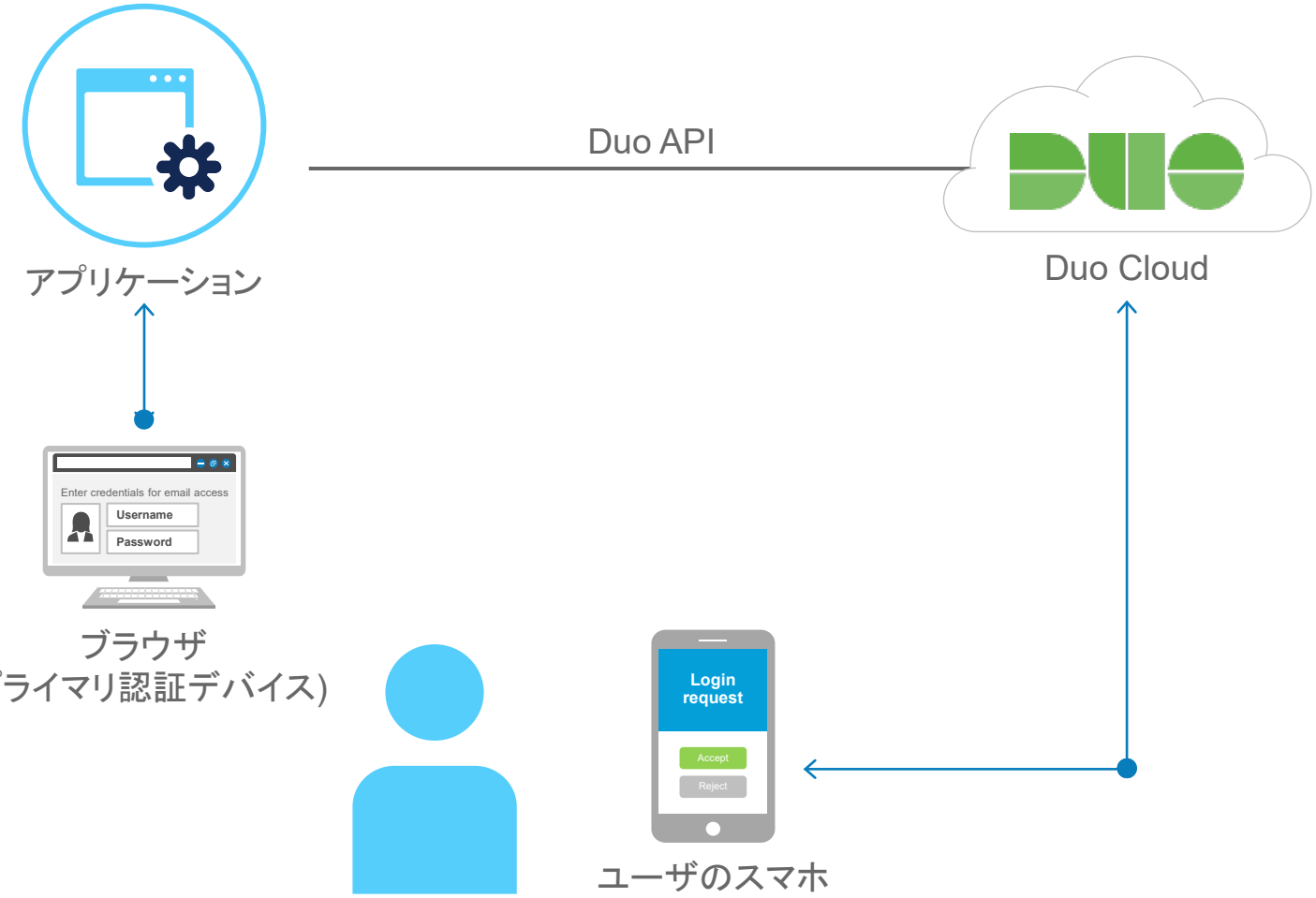
他の方法で統合出来ない場合、Duoをアプリケーションにコーディングできる

特徴:

- 自分でコードを作成可能でアプリのソースコードにアクセスできる必要がある
- 他の方法よりも作業が多くなるが、柔軟性は高い

Example libraries

C# node JS Java Ruby python



Secure