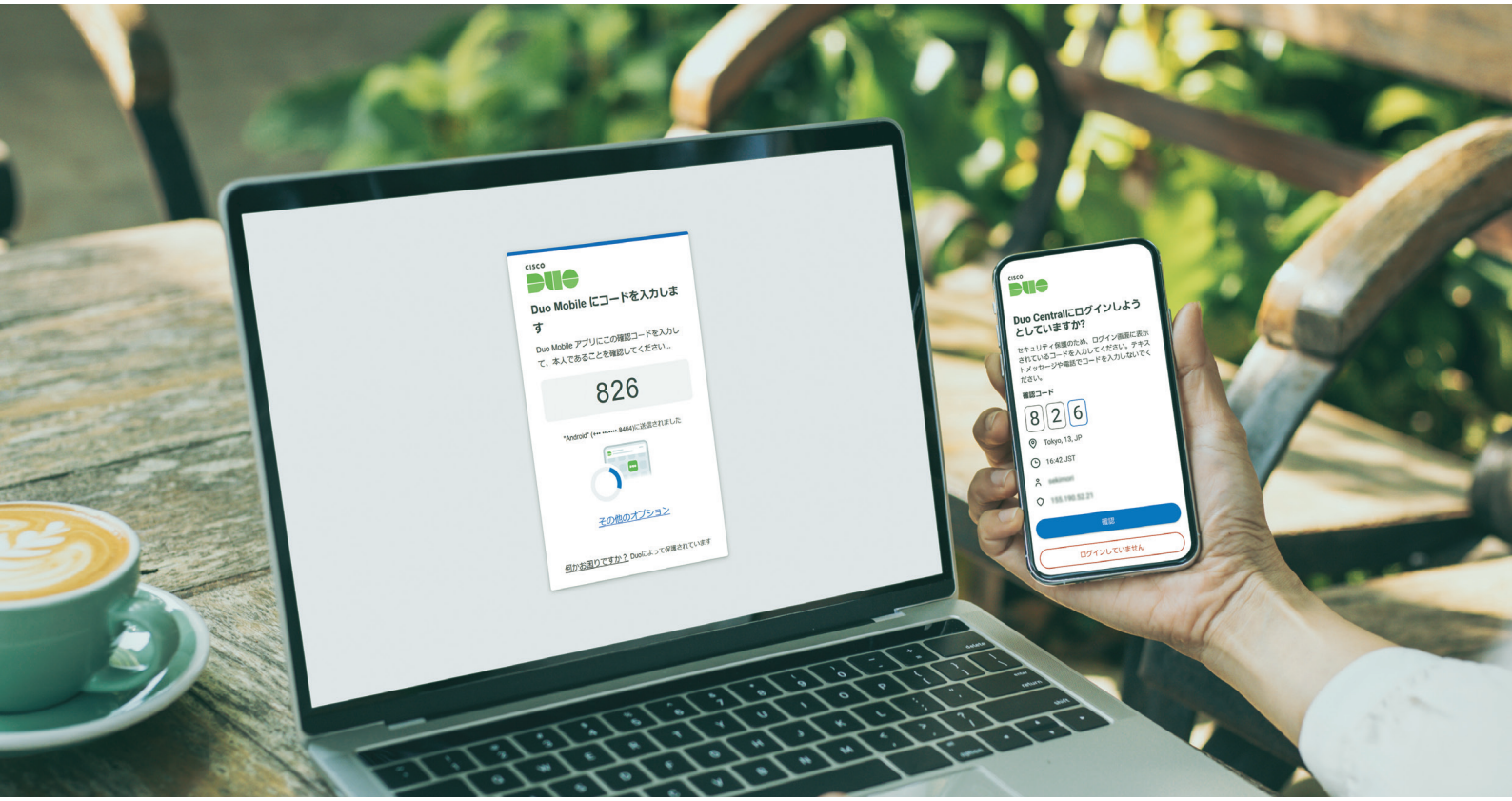
シスコのゼロトラストアクセス管理ソリューション

Cisco Duo



Cisco Duo は、多要素認証とデバイス可視化をベースにセキュアなアクセス管理を実現するソリューションです。
アプリケーションにアクセスしようとするユーザーおよびデバイスに対して**ゼロトラスト**を適用し、
信頼できるユーザーが信頼できるデバイスでアクセスしようとしている場合のみアクセスを許可します。
ユーザーやデバイスだけでなく、接続するネットワークやリスクなど、その他の条件（信頼性）にも基づいてアクセスポリシーを設定可能、
それらの信頼性を継続的に検証することで、不正アクセスやその他の脅威から組織を保護します。
かんたんシンプルな導入と運用管理を実現する SaaS モデルのクラウドサービスとして IT 管理者の負荷を軽減するだけでなく、
パスワードレス認証やシングルサインオンなど、ユーザビリティを向上させる機能も提供します。

ユーザー認証
（多要素認証）

多要素認証で
ユーザーの信頼性を確立

デバイストラスト
（デバイス可視化）

OS などの健全性を可視化して
デバイスの信頼性を確立

認証 / アクセス
ポリシー

さまざまな条件に基づく
柔軟なアクセスポリシー設定

シングルサインオンと
リモートアクセス

組織内外のアプリ / サーバーに
かんたんセキュアなアクセス

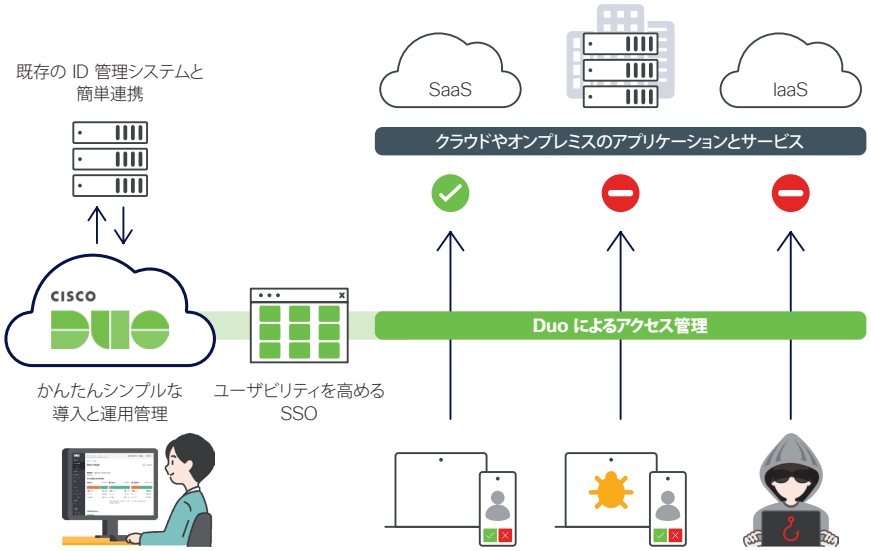
Cisco Duo 概要

Cisco Duo とは

Cisco Duo は、業界をリードするセキュアなアクセス管理ソリューションです。

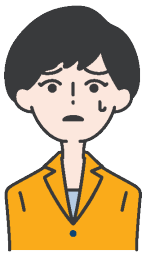
多要素認証とデバイス可視化をベースにしたアクセス管理と多層防御、さらに機械学習によるリスクベース認証のような最先端テクノロジーによって、攻撃者を苛立たせる鉄壁のアクセスセキュリティを提供します。

- **ユーザー認証**
  - 多要素認証（MFA）
  - プッシュ通知フィッシング対策 NEW
  - パスワードレス認証 NEW
  - 脅威検知
- **デバイストラスト**
  - デバイス可視化
  - 信頼済みエンドポイント（Trusted Endpoints）
  - デバイスヘルス
- **認証 / アクセスポリシー**
  - 適応型アクセスポリシー
  - リスクベース認証 NEW
- **シングルサインオンとリモートアクセス**
  - シングルサインオン（SSO）
  - リモートアクセス（Duo Network Gateway）



こんな悩みや課題をすぐに解決！

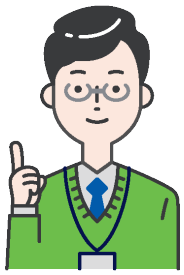
Cisco Duo は、かんたんシンプルに導入および運用管理できる SaaS モデルのクラウドサービスです。次のような悩みや課題をおもちのかたは、ぜひ導入をご検討ください。



- パスワードが流出した場合のなりすましなど、不正アクセスによる情報漏洩が心配。
- OS のバージョンなど、社員が使用する PC やスマートフォンのセキュリティを管理したい。
- クラウドアプリやサービスの利用が増えて、パスワードの管理が面倒。
- 多要素認証を導入したいけれど、運用まで時間や工数がかかりそう。

Duo なら、

- 多要素認証でユーザーが「**本人である**」ことを確認するため、流出してしまったパスワードによる不正アクセスを防止できます。パスワード流出のリスクを軽減するパスワードレス認証もサポートします。
- OS やブラウザのバージョン、アンチウイルスソフトウェアの有無など、PC やスマートフォンのセキュリティ健全性を認証時に確認、不適切な場合にはアクセスを制限できるだけでなく、アップデートや適切な設定をユーザーに促すこともできます。
- ポータルに一度ログインするだけでクラウドアプリやサービスを利用できる、シングルサインオンを提供します。SAML プロトコルを使用できるオンプレミスのアプリもサポートします。
- Active Directory などの既存の ID 管理システムと簡単に連携させることができるため、きわめて短期間で導入できます。わかりやすい管理画面で各種設定もスムーズ、さらに既存の ID 管理システムとはあくまで別システムであるため、万が一、それらから ID/ パスワードが漏洩した場合でも安心です。



無料デモまたは 30 日間の無料トライアル

無料デモまたは 30 日間の無料トライアルで、Cisco Duo の効果を体験してください。シスコのプロフェッショナルや販売代理店が丁寧にサポートします。

WEB Cisco Duo 無料デモまたは 30 日間の無料トライアル
www.cisco.com/c/ja_jp/products/security/duo/index.html#~demo

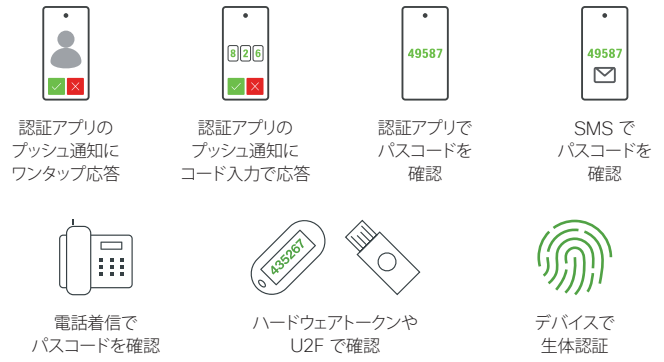
Cisco Duo 主な機能紹介

多要素認証（MFA）

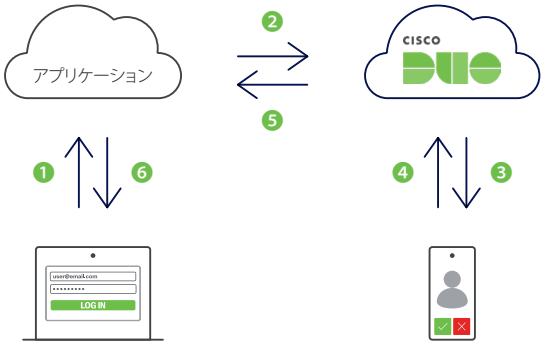
Cisco Duo は、最もシンプルに導入できる**多要素認証**（Multi-Factor Authentication；MFA）ソリューションです。ユーザー名やパスワードによる 1 つ目の認証方式（知識認証）に加えて、ユーザーが所持するデバイスによる所有者認証、指紋や顔などユーザー本人の生物学的特徴による生体認証のように、さまざまな要素を 2 つ目以降の認証方式とすることで、アプリケーションにアクセスしようとしているユーザーが「**本人である**」という信頼性を確立することができます。

Active Directory などの既存の ID 管理システムと簡単に連携させることができるだけでなく、ユーザー自身が認証デバイスを自己登録できるため、きわめて短期間で導入することができます。さらにユーザー自身が認証方式や認証デバイスをカスタマイズできるセルフポータルもサポートするため、運用管理の負担も軽減できます。

ユーザー自身でさまざまな認証方式を選択可能



多要素認証の流れ



1. アプリケーションにアクセスしたい PC（アクセスデバイス）で 1 つ目の認証
2. Duo に 2 つ目の認証要求を送信
3. 認証アプリ搭載スマートフォン（認証デバイス）に 2 つ目の認証を要求（プッシュ通知）
4. 認証アプリで 2 つ目の認証（プッシュ通知にワンタップで応答）
5. アプリケーションに 2 つ目の認証成功を送信
6. アプリケーションへのアクセスを許可

プッシュ通知フィッシング対策 NEW

多要素認証が普及しつつある中、多要素認証そのものを狙った攻撃や回避する攻撃も増加しています。その代表的な攻撃の 1 つが「**多要素認証疲労攻撃**」または「**プッシュ通知フィッシング**」と呼ばれる攻撃です。

これらの攻撃では、ID とパスワードを詐取した攻撃者がくり返しログインを試行して正規ユーザーの認証デバイスにプッシュ通知を送信、ユーザーが根負けしてプッシュ通知に応答してしまう事態を狙います。

Cisco Duo では**プッシュ通知フィッシング対策**として、認証アプリ（Duo Mobile）のプッシュ通知による多要素認証でコード確認（数字の照合）を適用できます。これによって、不正なプッシュ通知にワンタップで応答してしまう事態を未然に防ぐことが可能です。

また、攻撃者がシステム管理者を装ってユーザーに応答を促すような事態に備えて、不審なログインに対する迅速なアラート機能も提供します。

PC ブラウザに表示された確認コードを Duo Mobile で入力してログイン

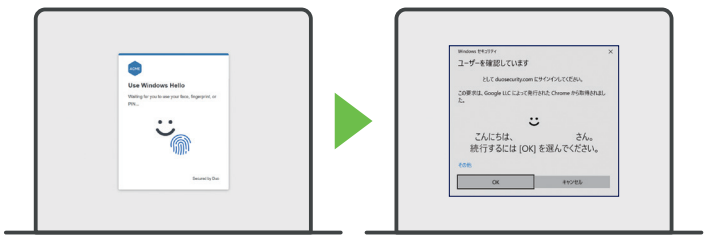
パスワードレス認証 NEW

クラウドアプリやサービスの利用が増えるにつれて、パスワードによる認証方式のデメリットがますます懸念されるようになってきました。

- **IT 管理者**：パスワードリセットなどへの対応に膨大な時間と労力がかかる
- **ユーザー**：アプリやサービスごとに異なるパスワードの入力と管理が面倒
- **セキュリティ**：不正アクセスの原因のほとんどが流出したパスワード *1

そこで注目されているのが**パスワードレス認証**です。Cisco Duo では、次のような複数のパスワードレス認証方式をサポートします。

- Windows Hello
- Touch ID と Face ID
- Android バイオメトリクス
- FIDO2 セキュリティキー
- Duo Mobile（パスワードレス オーセンティケータとして機能）



Windows Hello によるパスワードレス認証画面例

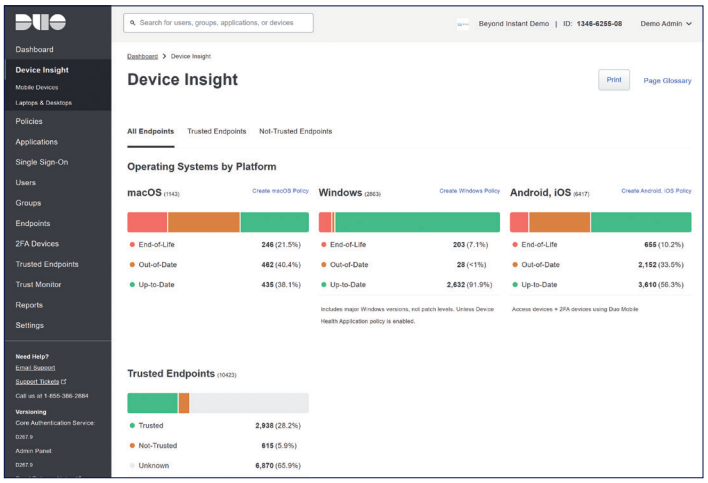
*1　参考：ベライゾン『**2022 年データ漏洩 / 侵害調査報告書**』など。

デバイストラスト

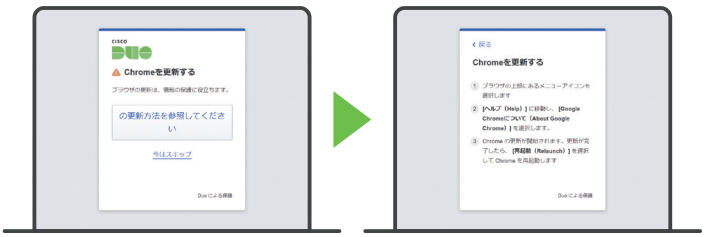
Cisco Duo によって、アプリケーションにアクセスしようとするデバイスの OS やブラウザ、プラグインのバージョン、暗号化やファイアウォールの有無、さらに企業所有か個人所有かどうかなど、さまざまな情報を取得して可視化することができます。

一般的なモバイルデバイス管理（MDM）ソリューションほかとは異なり、認証時のリアルタイムな情報を取得してアクセスポリシーに反映することができるため、より強固なアクセスセキュリティが実現します。

さらに、ユーザーが使用する OS やブラウザのバージョンが古い場合のように、セキュリティ健全性が低いとみなせる場合にはアクセスを拒否できるだけでなく、ユーザー自身で健全性を回復する方法、たとえばブラウザのアップデート方法を通知することができるため、ヘルプデスクとして介入すべき機会を減少させながら、組織全体のセキュリティを強化することができます。



デバイスに関するさまざまな情報を把握できるダッシュボード



ブラウザのアップデート方法など、ユーザー自身によるセキュリティ健全性の回復方法を通知

デスクトップ / モバイルアプリでもユーザー自身がセキュリティ健全性と回復方法を確認可能

リスクベース認証 NEW

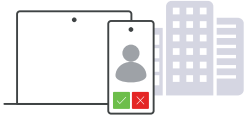
テレワークが普及し、ハイブリッドワークが一般的になりつつある現在、ユーザーが場所を変えて異なるネットワークから、あるいは異なるデバイスでアプリケーションにアクセスすることは、もはや珍しくありません。

セキュリティの観点では攻撃者のターゲットが拡大し、潜在的なリスクもまた増加していることになるため、ユーザー認証の重要性はますます高まっています。しかし、強固なユーザー認証、たとえば短期間にくり返し要求される認証は、ユーザビリティを低下させて生産性の向上を妨げる要因ともなります。

Cisco Duo の**リスクベース認証**は、このようなセキュリティとユーザビリティのトレードオフを解消するために開発されました。ユーザー認証の時間、IP アドレスや Wi-Fi フィンガープリントに基づく場所、認証失敗のパターンなど、リスクを示唆するさまざまな情報（リスク兆候）を機械学習によるアルゴリズムで評価し、リスクの高低に基づいて認証方式や再認証までの時間を動的に変化させるテクノロジーです。

リスクベースで動的に変化する認証方式

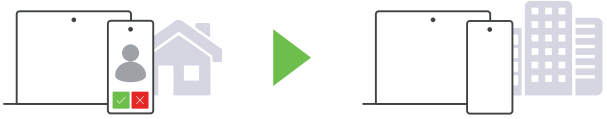
自宅からアクセス（低リスク）
Duo Mobile のプッシュ通知に
ワンタップ応答で OK



会社からアクセス（低リスク）
Duo Mobile のプッシュ通知に
ワンタップ応答で OK

カフェなど外出先からアクセス（高リスク）
Duo Mobile のプッシュ通知に対するワンタップ応答は自動的に利用不可
コード確認で応答、またはパスコードや生体認証などのリスク耐性が高い認証方式に制限

リスクベースで動的に変化する再認証時間



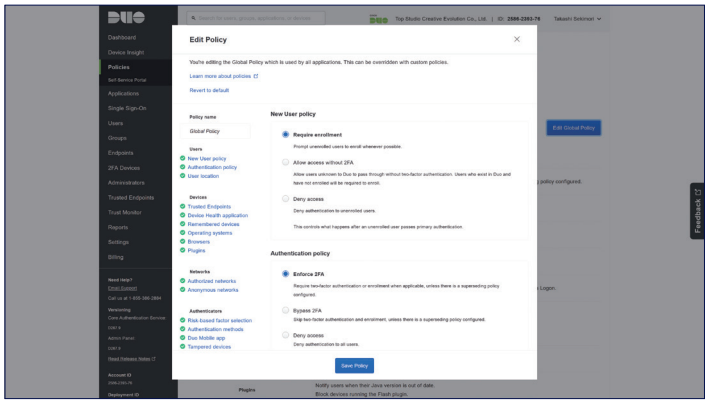
自宅から会社に移動（低リスクから低リスク）
管理者が設定した再認証時間内であれば（たとえば 8 時間）、
自宅から会社に移動しても再認証を要求されない

自宅からカフェなど外出先に移動（低リスクから高リスク）
管理者が設定した再認証時間内であっても、
自宅からカフェなど外出先に移動すると再認証を要求される

適応型アクセスポリシー

ゼロトラストに基づき、「**デフォルトで拒否（default deny）**」および「**明示的に許可（explicit allow）**」する**最小権限のアクセスポリシー方式**を採用。許可する条件を必要に応じて追加するシンプルなポリシー構造によって、運用管理の負担を軽減しながら厳格にアプリケーションアクセスを制御できます。

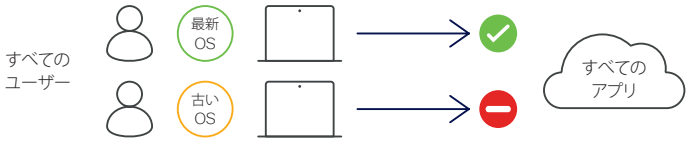
すべてのユーザーおよびアプリケーションに適用される**グローバルポリシー**によって組織全体のアプリケーションアクセスを効率的に制御しつつ、特定のアプリケーションに適用できる**カスタムポリシー（アプリケーションポリシーとグループポリシー）**によってきめ細やかに制御することが可能です。



シンプルでわかりやすいユーザーインターフェイス

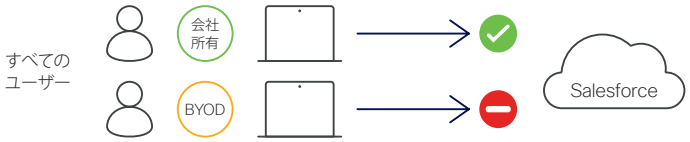
グローバルポリシー例

デバイスのセキュリティ健全性が低い場合はアクセスできないように設定



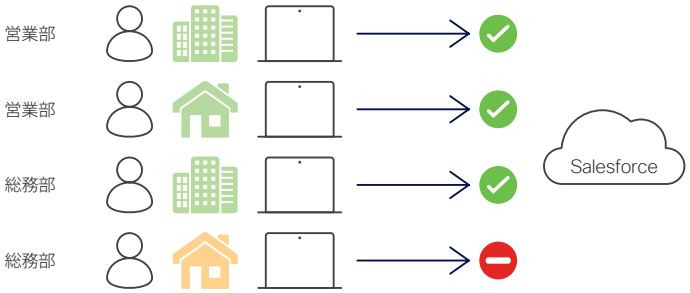
アプリケーションポリシー例

Salesforce では会社所有デバイスによるアクセスのみ許可



グループポリシー例

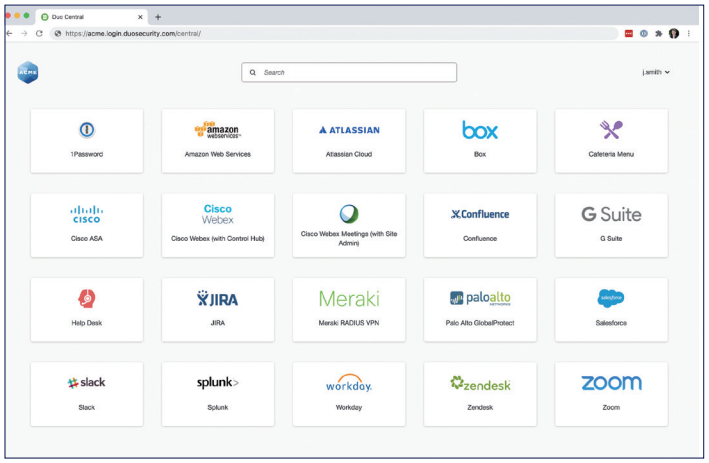
Salesforce では総務部ユーザーに対して社内からのアクセスのみ許可



シングルサインオン（SSO）

Cisco Duo は、クラウド / オンプレミスを問わず、さまざまなアプリケーションに一元的にアクセスできる**シングルサインオン**（Single Sign-On；SSO）をサポートします。専用のポータル（**Duo Central**）に一度ログインすれば、登録済みアプリケーションに認証なしでアクセスすることができるため、ユーザビリティが劇的に向上します。

シングルサインオンはパスワードへの依存を低下させるソリューションであると同時に、パスワードレス認証を導入するための土台にもなります。

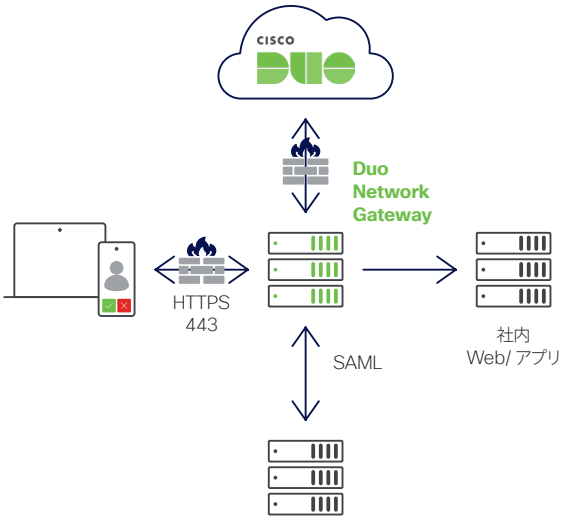


Duo のシングルサインオンでユーザーが利用できる専用ポータル（Duo Central）

リモートアクセス

Cisco Duo は、VPN なしでも安全なリモートアクセスをサポートします。**Duo Network Gateway** を利用すれば、ユーザーは社外からでもオンプレミスまたはパブリッククラウドの社内サイトやアプリケーション、およびサーバーにアクセス可能です。

Cisco Secure Client などの既存の VPN サービスに Duo を組み合わせることで、より安全なリモートアクセス VPN を提供することもできます。



SAML 2.0 ID プロバイダー

Cisco Duo 製品エディション

Cisco Duo 製品エディション概要

Cisco Duo は、アクセス管理に必要な機能に応じて、次の 3 つの製品エディションから選択することができます。

Essentials

- 多要素認証（MFA）
- コード確認ありプッシュ通知による プッシュ通知フィッシング対策
- パスワードレス認証
- 基本的なデバイス可視化
- 信頼済みエンドポイントにのみアクセスを許可
- 承認済みネットワークからのみアクセスを許可
- アクセスポリシー
- シングルサインオン（SSO）

Advantage

Essentials に加えて

- 脅威検知
- 高度なデバイス可視化
- デバイスヘルス
- 適応型アクセスポリシー
- リスクベース認証

Premier

Advantage に加えて

- Cisco Secure Endpoint などの EPP 連携対応 デバイスヘルス
- VPN レス リモートアクセス

Cisco Duo 製品型番

Cisco Duo は、組織の大小を問わず簡単に導入および運用できる、SaaS モデルで提供されます。ユーザー数に応じたライセンスを 1 ～ 5 年のサブスクリプションとして契約します。

Cisco Duo ライセンス *1

製品説明		サブスクリプション期間	ライセンス単位	最低数量
DUO-ESSENTIALS	Duo Essentials エディション ライセンス	1 ～ 5 年	ユーザー	1 ～
DUO-ADVANTAGE	Duo Advantage エディション ライセンス	1 ～ 5 年	ユーザー	1 ～
DUO-PREMIER	Duo Premier エディション ライセンス	1 ～ 5 年	ユーザー	1 ～

*1　CCW では DUO-SUB が必要。詳細は発注ガイドを参照。

Cisco Duo サポートサービス

Cisco Duo の契約時には、サポートサービスも契約する必要があります。必要なサポートに応じて、無償と有償の 2 つのサービスレベルから選択することができます。

有償の **Premium Support（Duo Care）**では、お客様が Duo を最大限に活用できるように専任の担当者が成功事例に基づいてプロジェクト / 運用支援や技術 / 運用支援を提供。ユーザーからの個別の問い合わせが可能な限り発生しないように、設計、設定段階から運用、ヘルプデスク対応まで、計画的にサポートします。日本の専任担当者に直接問い合わせることも可能です。

Cisco Duo サポートサービス提供比較

サポート	無償 Basic Support	有償 Premium Support（Duo Care）
テクニカルサポート（電話またはオンラインでケースを申請）	24 時間 365 日 *1（重大度 1） 平日 9:00 ～ 17:00（重大度 2 ～）	24 時間 365 日
シビラティ（重大度）1 および 2 のオンラインによるケース申請に対する初回応答目安	1 時間 *1（重大度 1） 2 時間 *1（重大度 2）	1 時間 *1（重大度 1） 2 時間 *1（重大度 2）
VIP サポート回線		✓
電話優先対応		✓
サポートチケットポータル	✓	✓
統合方法ガイダンス	✓	✓
Knowledge Base や Duo Community など、オンラインリソースのアクセス権	✓	✓
Duo クラウドサービスのステータスをリアルタイムで確認	✓	✓
稼動時間 SLA	99.90%	99.95%
お客様専任のカスタマーサクセス マネージャによるプロジェクト / 運用支援		✓
お客様専任のカスタマーソリューション エンジニアによる技術 / 運用支援		✓

*1　日本語による対応は平日 9:00 ～ 18:00。

Cisco Duo 製品エディション機能比較

セキュリティサービス / 機能			Essentials	Advantage	Premier
ユーザー認証	多要素認証（MFA）	iOS/Android 向け認証アプリ（Duo Mobile）のプッシュ通知による多要素認証	✓	✓	✓
		セキュリティキー、FIDO2、OTP、電話着信、SMS、およびハードウェアトークンによる多要素認証	✓	✓	✓
		アプリケーションを無制限で統合可能	✓	✓	✓
		ユーザーによる自己登録と自己管理	✓	✓	✓
		1 ユーザーあたり年間 100 クレジット分の電話着信認証および SMS 認証	✓	✓	✓
	プッシュ通知 フィッシング対策 NEW	iOS/Android 向け認証アプリ（Duo Mobile）のプッシュ通知による多要素認証でコード確認（数字の照合）を適用	✓	✓	✓
		フィッシング耐性がある要素を利用するように制限	✓	✓	✓
		不審なログインに対する迅速なアラート	✓	✓	✓
	パスワードレス認証 NEW	Duo SSO やサードパーティ製 SSO アプリケーションにパスワードレス認証を適用可能	✓	✓	✓
		パスワードレス オーセンティケータとして iOS/Android 向け認証アプリ（Duo Mobile）を提供	✓	✓	✓
	脅威検知	機械学習によって異常または危険なログインを顕在化、潜在的な攻撃をリアルタイムで検知（Trust Monitor）		✓	✓
		認証に使用するデバイスの新規登録を検知		✓	✓
デバイストラスト	デバイス可視化	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（Device Insight）	✓	✓	✓
		OS やブラウザの更新状況、セキュリティポリシーの遵守状況など、PC やモバイルデバイスのセキュリティ健全性を可視化		✓	✓
		フル機能のダッシュボード、認証ログ、およびカスタムレポートによって、コンプライアンス監査や管理の簡素化を実現		✓	✓
	信頼済みエンドポイント （Trusted Endpoints）	管理対象デバイスや登録済みデバイスにのみアプリケーションアクセスを許可	✓	✓	✓
		デバイス登録によって BYOD デバイスやサードパーティ製デバイスの信頼性を確認	✓	✓	✓
		Landesk や JAMF、Microsoft Intune など、エンドポイント管理システム（EMM）での登録状況に基づいてデバイスのアプリケーションアクセスを制限	✓	✓	✓
		AirWatch や MobileIron、Microsoft Intune など、モバイルデバイス管理（MDM）での登録状況に基づいてモバイルデバイスのアプリケーションアクセスを制限	✓	✓	✓
		Cisco Secure Endpoint と統合、危険なデバイスをブロック	✓	✓	✓
	デバイスヘルス	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、PC のセキュリティ健全性に基づくポリシーを適用		✓	✓
		暗号化や改ざん、画面ロック、生体認証の有無など、モバイルデバイスのセキュリティ健全性に基づくポリシーを適用		✓	✓
		セキュリティ健全性を自己回復する方法をユーザーに通知、ヘルプデスクの介入が不要		✓	✓
		Crowdstrike、SentinelOne、Cisco Secure Endpoint など、エンドポイント保護製品（EPP）の有無に基づいてデバイスのアプリケーション アクセスを制限			✓
認証 / アクセスポリシー	適応型アクセスポリシー	グローバルまたはユーザーグループ別に認証を割り当ておよび適用	✓	✓	✓
		ネットワークが承認済みかどうかに基づいてポリシーを適用	✓	✓	✓
		アプリケーション別にポリシーを割り当ておよび適用		✓	✓
		Tor、プロキシ、VPN など、匿名ネットワークからの認証試行をブロック		✓	✓
		デバイスのセキュリティ健全性に基づいてポリシーを適用		✓	✓
	リスクベース認証 NEW	リアルタイムなリスク兆候に基づいて認証要件を動的に調整		✓	✓
		Wi-Fi フィンガープリントなどの正確なリスク兆候に基づいてリスクレベルを決定、ユーザーのプライバシーを保護しながらリスクベースのポリシーを適用		✓	✓
		セッションを長期にわたって有効化、リスク兆候が変化した場合のみ再認証を要求		✓	✓
シングルサインオンとリモートアクセス	シングルサインオン（SSO）	SAML 2.0 および OpenID Connect（OIDC）対応アプリケーションをサポートするクラウドベース SSO（Duo SSO[*1]）	✓	✓	✓
		アプリケーションを無制限で統合可能	✓	✓	✓
		アプリケーションアクセスの簡素化とユーザーによるデバイスの自己登録と自己管理をサポート（Duo Central）	✓	✓	✓
		パスワードレスでログイン可能（Duo Central）	✓	✓	✓
		Microsoft、Okta、Ping など、既存のオンプレミスまたはクラウドの ID プロバイダーと統合可能	✓	✓	✓
		一般的に使用される OpenID Connect（OIDC）および OAuth 2.0 認証および認可フローをサポート（認可コード、クライアント資格情報、リフレッシュトークン、および PKCE）	✓	✓	✓
	リモートアクセス （Duo Network Gateway）	オンプレミスまたはマルチクラウドでホストするプライベートアプリケーションへの VPN レス リモートアクセスを提供			✓
		SSH、RDP、および SMB 経由で社内 Web アプリケーションおよびサーバーへの安全なアクセスを提供			✓
		AWS、Azure、GCP でホストするアプリケーションへの安全なリモートアクセスを提供			✓

*1　オンプレミスベースの SSO は Duo Access Gateway で提供。

Cisco Duo 日本語 Web サイト
www.cisco.com/jp/go/duo

Cisco Duo 英語 Web サイト
duo.com

シスコ お問い合わせ窓口

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
cisco.com/jp

2375-2306-02A-TO