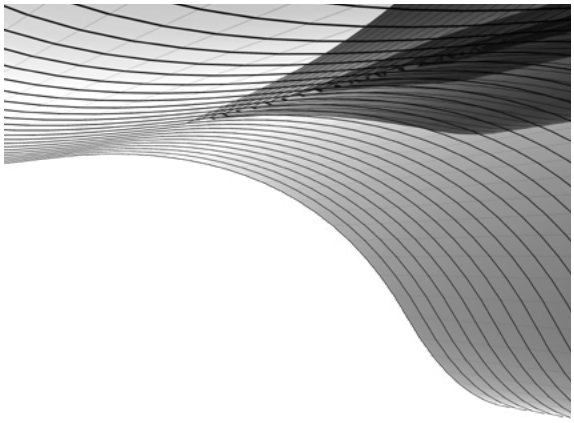
Duo Security is now part of Cisco.

Duo 企業導入ガイド

Duo を企業規模で展開する秘訣



Duo 企業導入ガイド

Duo を企業規模で展開する秘訣

目次

はじめに

Duo は、アプリケーションやサービスにあらゆるデバイスを使用してどこからでも安全にアクセスできる環境を何千もの企業に提供してきました。企業における多要素認証 (MFA) の導入では複雑な条件が絡むことや細やかな対応が必要になることがあります。導入が非常にうまくいった事例を見ると、事前に分析を行って計画を立てています。これはそれほど時間がかかる作業ではなく、セキュリティ実現までの所要時間が短縮され、サポートコストも低くなるという大きな見返りが期待できます。

このガイドは Duo を企業規模で導入してきた経験に基づいています。お客様がセキュリティプログラムを計画し最大限の成果を手にするための一助となれば幸いです。

ユーザーを計画の中心に

多くの場合、導入がうまくいくかどうかの鍵を握っているのはユーザーです。実際に Duo を日々利用するのはユーザーなのですが、技術的な側面に重点を置きすぎてユーザーのことを忘れてしまいがちです。

そのようなやり方で導入を進めてしまうと、ユーザーにとっても企業にとっても不満が残る結果になりかねません。サポート担当者が大きな負担を背負い込むことになり、最悪の場合はユーザーが利用を拒否するかもしれません。経営幹部は以降のプロジェクトに難色を示すでしょうし、それぞれの部署が独自のソリューションに走るなどして、成功を収めるのが難しい状況になっていく可能性があります。セキュリティに関する問題は特に、収拾がつかない状況に陥りがちです。あれもダメこれもダメと言うためにセキュリティプログラムの構築に着手するわけではありません。

導入を成功させるには、ユーザーを中心に考え、それに応じて計画を立てる必要があります。最初のステップでは、ユーザーベースの概要を把握してユーザープロファイルを作成します。次のページにあるような事項を確認しておくと、導入の立案に役立ちます。また推測に基づく判断を避け、特殊な事情を考慮するうえでも参考になります。

詳細については、『**導入ベストプラクティスガイド**』（英語）を参照してください。

ユーザーのタイプ

+ 従業員、請負業者、ベンダーの構成。
+ 各グループが使用するデバイスの所有者。
+ 複数のユーザーで同じデバイスまたはログイン情報を使用するか。

ユーザーの所在地

+ 複数の国や地域にユーザーがまたがっているか。
+ ビジネスの公用語は英語か。他の言語は必要か。
+ 国によってルールや規制が異なっているか。たとえばヨーロッパの一部の国では個人デバイスを業務に使用することを禁じている場合があります。
+ 文化の違いがあるか。たとえばフランスでは仕事と私生活をはっきり区別することが重要であり、個人デバイスを使用することをユーザーが拒否する場合があります。

ユーザーの勤務場所

+ オフィス、在宅、顧客やベンダーのオンサイトで勤務するユーザーがいるか。
+ モバイルデバイスを使用できないコールセンターや製造施設で勤務するユーザーがいるか。
+ 従業員が頻繁に出張して、飛行機、ホテル、コーヒーショップで作業することがあるか。柔軟性が必要か。

その他の考慮事項

+ これらの中に部署によって異なるものがあるか。
+ まったく異なるシステムを使用している買収先企業を考慮する必要があるか。
+ ユーザーはテクノロジーにどのくらい詳しいか。それはユーザープロファイルによって異なるか。
+ トレーニングやアプローチをカスタマイズする必要があるか。
+ 過去の導入事例はどうだったか。
+ セキュリティに対してユーザーはどのような考えを持っているか。

これらの事項が確認できると、ユーザーに周知していく最適な方法を決めることができます。電子メールを 1、2 通送って登録方法を案内すれば十分であるユーザーもいれば、カフェなどの人が集まる場所にブースを設置して Duo に慣れ親しむことができるようにしておくのが効果的なユーザーグループもいることでしょう。

多くの企業では、旗振り役となる経営幹部を決めています。これによって、Duo に対して肯定的な意見が広がり、ユーザーが早く適応するようになります。たとえばシスコが Duo を展開した際もこのアプローチを採用しました。

旗振り役の経営幹部を決め、また Duo と並行して Office 365 も導入しました。これによって新しいプロセスやソフトウェアに適応するユーザーの負担が軽減されました。新しいセキュリティ機能を導入して Office 365 にスムーズにアクセスできるようにしたことで、導入時にユーザーから高評価を得ることができました。

アプリケーションの調査

企業はそれぞれ独自の環境を有しており、企業規模が拡大するにつれて環境が非常に複雑になる可能性も高くなります。

企業はさまざまな形で成長していきますが、買収、新しい地域への進出、新しい業界や市場への参入などを行った場合は、環境がさらに複雑になる可能性があります。Duo のようなソリューションを導入するのは、環境内のさまざまなアプリケーションや提供しているアクセス権を把握する絶好の機会になります。

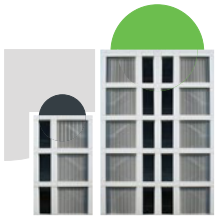
Duo を導入したら、まず特定のアプリケーションまたはサービスを保護します。たとえばシスコが Duo を展開したときは、まず Cisco AnyConnect VPN を Duo で保護しました。その後、体系的なアプローチに沿って VPN を使用せずに個々のアプリケーションにアクセスできるようにし、それらを Duo で保護しました。このタイプのアプローチを取ると、クラウドベースのアプリケーションに段階的に移行することができます。その結果、柔軟性と利用しやすさを最大限に高めながらセキュリティリスクを最小化することができます。

この段階の主な手順

組織で使用されているアプリケーションのリストを作成する

ツールとソフトウェアを標準化できるかどうかを確認する

アプリケーションにアクセスしている人と方法を把握し、必要な関係者のみにアクセス権が提供されていることを確認する



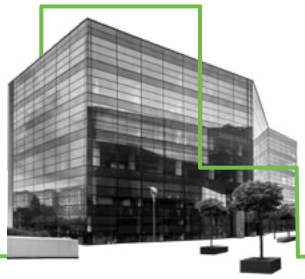
リスクプロファイルまたはユーザーが必要としているアクセスに基づいてアプリケーションの優先順位を付ける

アプリケーションアクセス

リスク要因の中で見過ごされがちなのが、ユーザーがアプリケーションにアクセスする方法、特にリモートワークにおけるアクセス方法です。

保護するアプリケーションをリストアップするだけでなく、次のようなシナリオに該当するかどうかも検討します。

+ ユーザーが複数のユーザー名とパスワードを管理しているか。
+ VPN でネットワーク全体がアクセス可能になっているか。
+ 請負業者やベンダーにどのようなアクセス権を提供しているか。ネットワークはセグメント化されているか。それともユーザーが機密情報に幅広くアクセスできるようになっているか。
+ 自社開発、カスタム、またはその他のアプリケーションをオンプレミスでホストしているか。
+ RDP または SSH プロトコルを使用しているか。



多くの組織では反復的なアプローチを使用して複数の機能やアプリケーションを導入しています。最初の導入で特定の項目を除外した場合は、提供を開始した後、数か月ごとに再検討するようにします。また、**Duo のリリースノート**に登録して、新機能に関する最新情報を入手することもできます。Duo では、アプリケーションアクセスの管理と保護に役立つ次のような機能を提供しています。

+ **Duo SSO**（シングルサインオン）を使用するとアプリケーションへのアクセスがシンプルになり、複数のユーザー名とパスワードを使用する負担を軽減することができます。SSO は生産性向上とリスク低減に役立ちます。使用するパスワードが多くなるとユーザーは同じパスワードを使い回したり、複雑でないパスワードを作成したりしがちになり、侵害を受けやすくなります。シングルサインオンを使用すれば、**Duo Central** という 1 つの場所にアクセスするだけで複数のアプリケーションを起動できるようになります。サブスクリプションには Duo SSO と Duo Central の両方が含まれています。
+ **Duo Network Gateway** を導入すれば、VPN クライアントを使用せずに社内の Web アプリケーションや SSH セッションに安全にアクセスできるようになります。承認されたユーザーとデバイスのみにアクセスを制限することで、侵害のリスクを低減させることができます。
+ RDP、Unix、AWS、その他の開発者ツールおよび環境については指定された統合を使用して、監査証跡を残しながらすべてのアクセス試行が保護されるようにします。
+ Web SDK と API を使用すれば、あらゆるワークフローやカスタムアプリケーションに Duo の機能を組み込むことができます。
+ **Duo Trust Monitor** は疑わしいログイン試行について警告し、管理者はアクセスポリシーを適宜強化することができます。
+ **ポリシー**を使用して、国、ネットワーク、デバイスの正常性などの要因に基づいてアクセスを制限することができます。ポリシーはアプリケーションごとにカスタマイズできます。これには SSO や Duo Network Gateway を介してアクセスするアプリケーションも含まれます。

デバイスの信頼性

Duo を展開したところ予想の 3 ～ 4 倍の数のデバイスがアプリケーションやデータにアクセスしていたというお話をお客様からよく伺います。

不適切なデバイスは企業を危険にさらします。たとえば更新が行われていない、脱獄（ジェイルブレイク）されている、画面ロックが設定されていない、マルウェアに感染しているといった場合です。ユーザーは電子メール以外のものにも個人デバイスでアクセスすることが多いものです。

Duo を展開するときは、デバイスとアクセスの保護方法に関する次のような項目を確認することが重要です。

+ 企業所有デバイスからのアクセスのみを許可するか。アプリケーションによってアクセス許可が異なるか。
+ 個人デバイスの使用に関する正式なポリシーがあるか。どのようにそれを実施しているか。
+ BYOD（個人所有デバイス持込）を許可するか。
+ 個人デバイスで MDM（モバイルデバイス管理）の使用を必須にするか。
+ デバイスが一定レベルのセキュリティ状態を満たしていることを確認してからアクセスを許可することが重要であるか。
+ ユーザーの個人デバイスにセキュリティ状態の要件を課すか。

どこから始めればよいか迷う場合は、次のような方法で最適なアプローチを探ることができます。

+ **Device Insights** のレポートを確認して、デバイスの全体的な状況を把握します。今すぐ対処する必要があるリスクがないか確認します。たとえば医療機関において脱獄されたデバイスが検出された場合や、Flash プラグインを使用しているデバイスがある場合などです。
+ 修復の基本方針を決定します。
  - 個人デバイスにポリシーを適用するか。
  - デバイスを修復する猶予期間をユーザーに与えることにするか、デバイスを修復してからでないとアプリケーションにアクセスできないようにするか。
  - 企業所有デバイスを更新するための管理者権限がユーザーにあるか。
+ **ユーザーを教育**してセキュリティのベストプラクティスを教え、私生活でもそれらのベストプラクティスを実践するためのヒントを提供します。
+ リスクの状況を詳しく把握できると、セキュリティプラクティスを継続的に進化させていくことができます。
+ Duo のお客様の多くは、**Duo エンドポイント修復**ポリシーを使用してエージェントレス ポスチャ チェックを実施することから始めています。これは手間をかけずに大きな成果を挙げられるアプローチです。
+ よりきめ細かなポスチャチェックを行いたい場合や、個人デバイスや請負業者のデバイスに対してより強力でありながら干渉を最小限に抑えたアクセス制御を行いたい場合は、**Duo Device Health アプリケーション**を展開します。これは MDM やウイルス対策（AV）エージェントなどの既存のエンドポイント セキュリティ スタックを補完する軽量アプリです。
+ 企業の管理対象デバイスのみにアクセスを制限する必要がある場合は **Trusted Endpoints** を展開します。アクセス制限は、アプリケーションごとに設定できます。たとえば電子メールは最新の個人デバイスでアクセスできるようにし、人事情報は企業所有の管理対象デバイスのみにアクセスを制限することが可能です。

導入戦略

企業規模の展開の次のステップでは、組織に Duo を導入する方法を計画します。

段階的に導入

段階的な導入は、次のようなさまざまな方法で行えます。

- 部門単位 (IT 部門など) または機能領域単位 (人事、経理など)
- 地域単位 (国別、拠点別など)
- 本社、オフィス、リモートワーカー

一気に導入

一気に導入する場合は、すべてのユーザーに Duo を同時に提供します。このアプローチが必要になる場合としては、侵害を受けた場合、侵害を受ける恐れがある場合、環境に大きな変化があった場合などがあります。たとえば自然災害が発生してすべてのユーザーが急遽在宅勤務をすることになり、一部のユーザーが個人デバイスを使用して必要なアプリケーションにアクセスする場合などがあります。

シスコでは段階的な導入アプローチを採用し、6 か月をかけて Duo と Office 365 を導入しました。電子メールで案内を送付したのに加えて、Office 365 への初回ログイン時に Duo への登録を促すメッセージを表示しました。ユーザーはその時点で登録するか、2 週間以内に登録することができます。2 週間が経過した時点で Duo に登録していないユーザーは Office 365 にアクセスできなくなります。ログインフローの一部として 2 週間の要件をユーザーに通知するページをカスタム API を使用して表示しました。

一気に導入する場合は、「テスト、調整、導入」という 3 段階のプロセスを踏みます。テストは小さなグループで行うことが重要です。多くの場合、このグループは IT 部門とスーパーユーザーまたはインフルエンサーで構成されます。このアプローチの基本的なコンセプトは、発生する可能性がある問題を特定して、それらに対処するかまたは調整を行うというものです。また、これらの初期のユーザーは他のユーザーに影響を与える役割も果たします。好意的な意見を広めて機運を盛り上げ、迅速な導入を促進します。

たとえばシスコは既存の MFA ソリューションを Duo に置き換えましたが、ユーザーがこの変化に不満を感じてなかなか登録が進まないだろうとチームは予測していました。そこで Duo の導入と Office 365 の導入を同時に行うことにし、新しい魅力的な体験として社内にアピールしました。Duo によってセキュリティが強化されただけでなく、Office 365 によって主要な業務リソースにあらゆる場所から簡単にアクセスできるようになりました。このとき初めてセキュリティはユーザーの前に立ちはだかるものではなく、ユーザーエクスペリエンスを向上してくれるものとして迎えられたのです。

詳しい手順については『**Duo ポリシーガイド**』(英語) をご覧ください。

コミュニケーション

コミュニケーションについて考えるときに重要なのは、導入したときに戸惑いが広がらないように Duo に親しんでもらうことです。

多くの組織では、MFA を導入する前にセキュリティ侵害が発生しています。当然ながらユーザーは警戒心が強くなっており、登録の案内を送っても信用しないかもしれません。

コミュニケーションは明確かつ簡潔で、ユーザーと同じ目線に立っていることが必要です。脅したり怖がらせたりせずに、Duo の使いやすさとセキュリティの重要さを強調するとユーザーは受け入れやすくなります。また人は一般的に、自分の目的意識を駆り立てるものに引き寄せられます。

セキュリティを共同責任の感覚に結び付けると納得しやすくなり、目的意識を持ってもらうことができます。たとえば医療分野では、インフルエンザの予防接種をすることが全員を保護するために必要です。患者の情報を保護することを説明するときは、これと同じ共同責任の考え方を使用すると非常に効果的です。ここで重要なのは、恐怖心に訴えかけないことです。そうすると人は無力感を覚え、自分が何をしても重要ではないと思ってしまうからです。

便利なエンドユーザー教育用**コミュニケーション テンプレート**をご用意しましたのでご利用ください。

ユーザーとのコミュニケーションにはさまざまな形式があります。

+ ポスター (デジタルおよび紙)。
+ 電子メールによる導入の告知。
+ Wiki、SharePoint、イントラネットなど多くの人が使用するツールへの投稿。
+ チームミーティングやタウンホールでの告知。
+ 人が集まる場所にブースやテーブルを設置して質問に答える。

コミュニケーションの方法には状況に応じていくつかの選択肢があります。リードタイムが 30 日以上ある場合は、以下を検討できます。

+ 電子メールを何通か送信して Duo の概要と今後の予定を説明する。
+ カフェ、ロビー、休憩室など、人が集まる場所に紙のポスターを掲示する。
+ 社内 Wiki で通知する。
+ 人が集まる場所にあるスクリーンや会議室の中にデジタルポスターを掲示する。Duo では**作成済みポスターアセット**のキットをご用意しています。

リードタイムが短い場合は、次のことを検討します。

+ 上級幹部が電子メールを 1 通か 2 通 (数日以内に) 送信して、セキュリティと Duo を導入することの重要さを強調する。
+ マネージャが主導してメッセージを上から下に伝える。
+ サポートを利用できることを強調する。

早期導入者や導入支援者については、次のことを検討します。

影響力のあるユーザーグループに Duo を受け入れてもらい、模範となってもらいます。これは組織のコンプライアンスに大きく貢献します。このグループは、上級幹部、部門横断的な初期テスターのグループ、または特定の部門で構成できます。

これらの人は他のユーザーが登録するのを支援し、Duo の導入推進担当として活動します。変化は誰にとっても難しいものであり、新しいテクノロジーやプロセスを簡単に導入できることはめったにない、ということを忘れないようにします。使いやすさをアピールする機会を増やすほど導入はスムーズになります。

また組織特有の文化やポリシーを考慮して、それに合わせてメッセージを調整することも重要です。たとえば次のようなことを行います。

組織特有の考慮事項があるかどうかを確認します。例 : 個人デバイスの使用に関するポリシーを変更する必要があるか。ユーザーは個人の電話を使用して認証することに抵抗があるか。Duo アプリで行えることと行えないことをユーザーに教育する必要があるか。

こういった事項についてはプロセスの早い段階で対処します。Duo に対する信頼を築き、チームはできる限りの準備を整えておく必要があります。

もちろん、ユーザーが直面している問題にも注意を払います。

トレーニングとサポート

利用開始までに電子メールで何度か説明するだけでユーザーの準備が十分整ったとおっしゃる企業がほとんどですが、ヘルプデスクチームをトレーニングして準備しておくことも重要です。これもユーザーベースによって異なります。

ワークフォースが分散している場合、たとえば複数の地域に分かれている場合や在宅勤務の従業員がいる場合は、1つの場所に集まるのが難しいことがあります。追加のトレーニングが必要な場合は、次のような方法を検討します。

+ 短時間のバーチャルトレーニング セッションを数回開催して、Duo の設定方法と使用方法を説明する。
+ 短時間のビデオやウェビナーを作成し、FAQ や社内のランディングページに投稿する。
+ バーチャル「ブース」またはホットラインを最初の数週間設置することを検討する。
+ ロビーやカフェなどの人が集まる場所に IT 部門がテーブルを設置して、Duo の設定がうまくいかない人の相談に乗っている企業もあります。
+ グループによっては、人間によるきめ細かなサポートが必要な場合があります。従業員でない医師が勤務しているある医療機関では、休憩室にテーブルを設置しました。そこでは、デバイスが最新であることを確認し Duo への登録を支援するサービスを提供していました。

Duo は他のソリューションと比べて導入時のヘルプデスクチケットが大幅に少なかったとおっしゃる組織がほとんどです。多くの場合、問い合わせの内容はユーザー自身のデバイスに関する問題や、Duo アプリケーションのダウンロードに関するものです。**Duo Level Up** を利用すれば、最も一般的な問題についてヘルプデスクにトレーニングを提供できます。これは管理者向けの無料のオンライントレーニングおよび認定プログラムです。

組織の規模と予想される問い合わせ件数に応じて、専用の電話相談窓口を短期的に開設し、Duo の導入に関する質問に答えることができます。ある大規模な医療機関では多くのユーザーが同じ場所にいなかったため、このアプローチが有用でした。また直接雇用していない医師にとってもこれが役立ちました。

その他のヒントについては、『**ヘルプデスクガイド**』を参照してください。

成功の測定

導入がうまく進んで Duo が好評を得ました。おめでとうございます。でも、それでおしまいというわけにはいきません。導入に成功したことをどのように証明しますか。

セキュリティがきちんと機能している場合、何も起きないことが成功の証になります。何も起きないことが成果なのだと、経営陣にどう説明すればよいのでしょうか？目に見える成果をほとんど挙げないツールに対して予算を確保するにはどうすればよいのでしょうか？

マネージャやその上のマネージャがどのような結果に基づいて評価されるかを把握します。ROI、継続的な運用コスト、総所有コスト、リスク回避、従業員の満足度などが考えられます。

シンプルなレポートとレポートカードを 1 か月ごとまたは四半期ごとに発行することで、この大切な投資を目に見える形にし、自分の部署が企業全体に影響を与えていることをアピールすることができます。

以下は、企業規模での Duo の導入が成功したことを判断するための一般的な項目を評価基準ごとに示したものです。

一般的な評価指標

- ヘルプデスクチケットの数
- 展開の所要時間
- 登録ユーザー数
- 保護されているデバイスの数
- 保護されているアプリケーションの数
- VPN アクセス

脅威の状況

- 保護されているアプリケーションの割合
- 修復されたデバイスの数
- 回避したフィッシング攻撃の件数
- 新しい脅威（ゼロデイ脆弱性、一般的なマルウェア攻撃）に対する対応時間

財務面への影響

- 他のソフトウェアとのサポートコストの比較
- 推定侵害コスト / ユーザー数

将来を見据える

強力なセキュリティ態勢が整うと、リスクを予測し、予期しない事態に備えられるようになります。新しいアプリケーションの評価プロセスに Duo を組み入れている組織ではより強力な保護が実現され、脅威により適切に対応できることが分かっています。たとえばある大手不動産会社ではクラウドを中心に据えた戦略への移行を進めており、新しいアプリケーションのリクエストをすべて確認して Duo で保護する必要があるかどうかを判断しています。また別の企業では、新しいソフトウェアがリクエストされると潜在的なリスクを洗い出して定量化し、責任者であるエグゼクティブにそのリスクを承認してもらっています。これによって率直な意見交換が行われ、十分な情報に基づいて選択できるようになります。

2020 年に世界中の企業がテレワークに急速に移行し、多くの企業で新しい働き方が支援されるようになりました。オフィスの外で働いたことがなかった従業員は、使い慣れない VPN を使用して個人デバイスで業務アプリケーションにアクセスすることになりました。危機に対する備えがあった組織は、適切かつ迅速にこの事態に適応することができました。

ユーザーが望んでいる働き方、また将来必要になる働き方を把握し、それらのシナリオを支援できるよう、できる限りの準備を行うことが大切です。デバイスをどのように保護するか。出張や請負業者によるアクセスにどのように対応するか。アクセスが必要になる重要資産には何があるか。またそれらは保護されているか、といった事項を確認していきます。

計画と準備、そして事業継続計画の策定を行うことで、どのようなデバイスを使用してどこで作業していてもユーザーを確実に接続できるようになります。

まとめ

企業はそれぞれ独自の環境を有しており、新しいツールを導入するには膨大な作業が必要になることがあります。このガイドで説明した要因を考慮し、それに応じて計画を立てれば、社内の賛同を得て成功を収めることができます。

これまで多くの企業がこれらの戦略を使用して関係者を満足させ、サポートコストを削減し、そして何より組織の保護を実現してきました。お客様もぜひ、同じように成功を手にしてください。

信頼できるユーザーと信頼できるデバイスだけをアプリケーションに接続

シスコグループの一員となった Duo Security は、業界をリードする多要素認証 (MFA) およびワークフォース向けゼロトラストのプロバイダです。Duo のゼロトラスト セキュリティ プラットフォームである Duo Beyond を使用すれば、すべての重要なアプリケーションにあらゆるユーザーがあらゆるデバイスを使用してどこからでも安全にアクセスできるようになります。

Duo は、Dresser-Rand、Etsy、Facebook、Paramount Pictures、Random House、Zillow など、世界の 20,000 社以上のお客様に信頼されているパートナーです。Duo はミシガン州アナーバーで設立され、デトロイト、テキサス州オースチン、カリフォルニア州サンフランシスコ、ロンドンにも続々とオフィスを展開しています。

duo.com で 30 日間の無料トライアルをお試しください