Duo Security はシスコの
一員となりました。

Duo 導入ベストプラクティスガイド

バージョン 2.1（2019 年 10 月 3 日公開）

目次

はじめに 2

導入計画策定：プロセス図の作成 3

アプリケーションの設定およびテスト：Duo が機能するように設定する 5

ポリシーおよび制御：重要なリソースへのアクセスを保護する 9

エンドユーザ コミュニケーション：全員の理解が必要 11

ヘルプデスクトレーニング：チームの準備 12

Duo サポートおよび役立つリソース 13

Duo 実稼働：シームレスな導入を実現 14

はじめに

Duo は、優れたエクスペリエンスを提供することに注力しています。また、製品の使用方法や参考資料の入手方法など、お客様が必要とされているガイドをご提供します。Duo を導入することで、**データの漏洩やアカウントの乗っ取りから組織と従業員を保護できます。**

このガイドでは、Duo を展開する際の**主な導入段階**について順にご説明します。各段階では、Duo の**ベストプラクティス**と**主なリソース**についても合わせて記載します。このガイドの目的は、できるだけ**簡単かつ正しく** Duo を導入できるようにすることです。

このガイドの内容

- Duo のクラス最高レベルの技術的専門知識に基づいて、**Duo を導入するお客様のために開発したリソース**
- 多くのお客様導入事例に基づく**ベストプラクティスおよび回避すべきリスク**
- エンドユーザ教育に利用できる**テンプレートおよび関連資料**
- さらにサポートが必要な場合の**ご連絡方法の概要**

このガイドの対象者

- **Duo の導入を担当するすべてのお客様**。通常は、セキュリティマネージャ、IT プロジェクトマネージャ、セキュリティ管理者のいずれかとなります。
- **注：**このガイドは、導入のベストプラクティスを中心に記載したもので、Duo のセットアップに関する詳細をすべて示したものではありません。

このガイドを適用できる Duo エディション

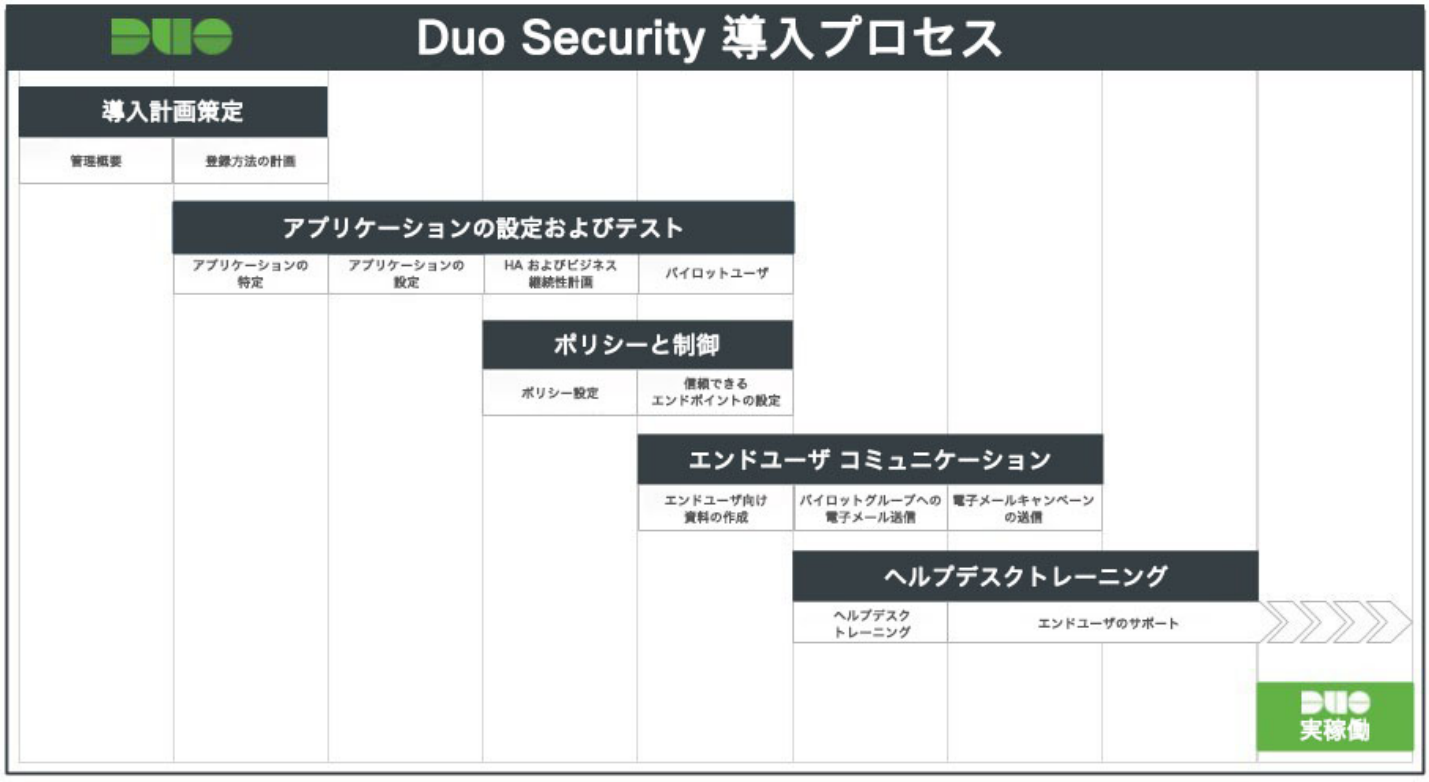
- このガイドに記載されている内容は、**Duo MFA**、**Duo Access** および関連する **Duo Beyond エディション**に適用できます。
- Duo Beyond 固有の内容については、セクション/サブセクションの最初または最後に **Duo Beyond のロゴ（** ）がついています。

導入計画策定：プロセス図の作成

導入計画策定の概要

Duo を導入する前に、まず導入計画を策定します。Duo スタートアップガイドに続けて、管理概要ドキュメントおよびお客様に最適な登録方法に関するガイドを参照し、Duo サブスクリプションの管理方法を学習します。

- Duo では、導入事例に基づいて**導入プロセス**を策定しています（以下を参照）。Duo 導入計画の叩き台としてご利用ください。
- 主な **Duo 導入段階**は白抜き文字で強調されており、各段階で完了すべき**主なタスク**が枠内に記載されています。



- **管理概要**

  ユーザ、ポリシー設定、アプリケーションなどを管理するために、Duo 管理者のさまざまなロールを割り当てる必要があります。アラートとメッセージを設定することで、導入プロセスで問題が発生するのを回避できます。

  - **主なリソース**
    - 管理パネル設定概要
    - Duo 管理者アカウントの管理
    - Duo 管理ロール
    - ヘルプデスクガイド
    - テレフォニークレジット：クレジット不足アラート
    - Duo Prompt ヘルプメッセージのカスタマイズ方法
    - ロックアウトレポートおよび不正行為レポート
  - **ベストプラクティス**
    - **他の Duo 管理者を作成、更新、削除できるのは、「オーナー」ロールを持つ Duo 管理者のみ**です。そのため、1 つのアカウント内に**オーナーロールを持つ管理者を 2 人以上設定することをお勧めします。**
    - ロックアウトレポートおよび不正行為レポートを送信する**電子**メールアドレスを指定します。複数の人がアラートを確認できるように**配布リストを作成することをお勧めします。**
    - ヘルプデスクメッセージ設定を使用して、Duo ブラウザに表示されるユーザ向け**ヘルプメッセージをカスタマイズ**します。
    - お客様の組織が大量のテレフォニークレジットを利用している場合は、テレフォニークレジット不足アラートオプションを設定します。
    - 管理ユニットを活用して、管理者が Duo ユーザとアプリケーションのグループを表示/管理する方法を制御することを検討します。
    - SAML 2.0 対応 ID プロバイダーを導入している場合は、Duo 管理パネルに対するシングルサインオン（SSO）を設定できます。

- **Duo 登録方法の決定**
  - **主なリソース**
    - ユーザ登録オプション
    - Duo ポリシーガイドには、ポリシー設定によってユーザ登録にどのような影響があるかに関する情報が記載されています。
  - **ベストプラクティス**
    - Duo では、外部ディレクトリからユーザを同期して、管理者がユーザを登録/削除する負担を軽減することを推奨しています。
    - **同期したユーザに送信される電子メールをカスタマイズする**には、[登録電子メールを同期ユーザに送信（Send enrollment email to synced users）] オプションを使用します。登録電子メールに会社のロゴを含めることができます。
    - Duo ユーザ登録に関するステータスの違いを理解してください。

アプリケーションの設定およびテスト：Duo が機能するように設定する

アプリケーションの設定およびテストの概要

策定した計画を実行するには、まず、**アプリケーションを特定して設定**し、続いて**テスト**します。保護するアプリケーション数に制限はなく、各アプリケーションを個別に管理できます。Duo Beyond サブスクリプションを利用している場合は、Duo Network Gateway を追加して、内部 Web アプリケーションや SSH サーバへのアクセスを保護することもできます。導入を成功させるには、実稼働前に**アプリケーションとエンドポイントをテストして試使用してみる**ことが重要です。

- **アプリケーションを特定する**
  Duo は、事前設定されたソリューションと、SAML、RADIUS、LDAP などの汎用設定のどちらを利用しても、オンプレミスおよびクラウドベースのさまざまなアプリケーションを保護できます。
  - **主なリソース**
    - サポートされるアプリケーションと機能に関するエディション別のリスト
    - Duo とアプリケーションを統合する際、多くの場合ローカルコンポーネントは不要です。ただし、特定の機能にはローカル認証プロキシサービスが必要です。認証プロキシリファレンスガイド には、プロキシの設定オプションに関する詳細情報が記載されています。RADIUS および LDAP に関する汎用マニュアルも利用できます。
    - Duo の SSO ソリューションである Duo Access Gateway を利用すれば、クラウドベースのアプリケーションへのアクセスを保護し、組織で利用する Web ベースアプリケーションのランチャーページを作成できます。
      https://duo.com/product/every-application/single-sign-on
    - Duo Network Gateway を利用すれば、Duo Prompt の多要素認証機能とデバイスインスペクション機能により、オンプレミス アプリケーションにリモートからアクセスできます。Duo Network Gateway は、Duo Access Gateway または任意の SAML 対応 IdP に接続できます。オンプレミス Web アプリケーションへのリンクをアプリケーションランチャーに追加できるため、従業員が簡単に検索できます。

- **ベストプラクティス**
  - 対象のアプリケーションに関する Duo ドキュメントを読み、認証プロキシ、Duo Access Gateway、SAML 対応 ID プロバイダーなど、準備に時間がかかったり、別のリソースが必要になったりする前提条件がないか確認してください。
  - 広く利用されている、機密性の高いアプリケーションから始めることをお勧めします。
    - 多くのユーザが利用するアプリケーションは、登録されればすぐに利用されます。Office 365 は、多くのユーザが電子メールやカレンダーなどの生産性向上ツールを使用するため、そのよい例です。このようなアプリケーションから始めれば、ほとんどのユーザが登録されて、すぐに 2FA の操作に慣れることができます。
    - センシティブデータを含む、またはセンシティブデータに直接アクセスするシステムやアプリケーションを Duo の初期導入対象に組み込めば、それらのアプリケーションの保護から優先的に始められます。
- **考慮事項**
  - コンプライアンスに対応する必要はありませんか。PCI、HIPAA、DEA などの外部規制や、CISO などの社内のリーダーから導入期限を設定されていませんか。
  - 導入に必要なリソースは十分ですか。テスト環境は整っていますか。組織に十分な IT スタッフがいない場合、または、スタッフの技術スキルが限られている場合、ネイティブアプリケーションまたは、シンプルな統合アプリケーションを選択し、Duo プロジェクトの範囲を段階的に拡張していくことをお勧めします。リソースが豊富な場合は、複数のアプリケーションを同時に導入することも検討してください。
  - 選択したアプリケーションのユーザエクスペリエンスはどのようになるでしょうか。アプリケーションを選択する際は、2FA の採用に対するユーザの意欲を考慮します。登録する際に Duo Prompt が表示され、セルフサービスで進められるアプリケーションから始めるか、すぐに 2FA を導入できるユーザグループを最初に登録することから始めます。
  - 価値が高く標的となりやすい特定のアプリケーションまたはユーザグループに関連したセキュリティインシデントが過去にありましたか。
  - 特定の時期に組織または IT スタッフに負荷が集中することがありますか。たとえば、教育機関における年度始めや、小売業における 11 月から 12 月にかけての繁忙期などです。税務事務所の場合、3 月と 4 月は新しい IT プロジェクトを実施するのは避けた方がよいでしょう。
  - 最も多くのユーザに利用される、リスクの高いアプリケーションを保護したら、次に以下の保護を検討します。
    - 人事ポータルまたは給与システム
    - 特権アクセス
    - リモートアクセス
    - スタンドアロンの Web アプリケーションまたはクラウド ID 管理ソリューション

- **アプリケーションの設定**
  - **主なリソース**
    - アプリケーションの保護方法
    - アプリケーション設定マニュアル
    - ハウツービデオ：アプリケーション統合
    - 認証プロキシリファレンスガイド
    - 認証プロキシに関するベストプラクティスガイド

  - **ベストプラクティス**
    - Duo をインストールして設定することで、サポート対象の多くのアプリケーションを**さまざまな方法**で保護できます。また、Duo アプリケーションを構築し、最適なエンドユーザ エクスペリエンスや管理ユーザエクスペリエンスを実現することもできます。
      - 詳細については、Duo のアプリケーションマニュアルやナレッジベースをご覧ください。
    - Duo 管理パネルでアプリケーションに**わかりやすい名前**を付けます。
      - アプリケーション名は、エンドユーザに対する **Duo Push のリクエストにはっきりと表示されます**。そのためユーザは、2FA を要求しているアプリケーションを特定できます。
      - わかりやすいアプリケーション名を付けると、Duo 管理パネルでアプリケーションを見つけたり、**認証ログ**の結果をフィルタ処理したりするのが容易になります。
    - **アプリケーション SKEY** は、**特権パスワード**と同じように扱ってください。SKEY を含んだスクリーンショットやプレーンテキストを電子メールで送信しないでください。Duo のサポート技術者に対しても同様です。SKEY を送信する必要がある場合は、SHA-256 ハッシュを使用することをお勧めします。

- **Duo アプリケーションのテスト**
  - **ベストプラクティス**
    - **テスト環境**で Duo アプリケーションをテストします。テストすることで、エンドユーザが問題に遭遇する前に潜在的な問題を特定できます。
      - セットアップできる Duo アプリケーションの数に制限はありません。**エンドユーザに導入する前に、ラボ環境または仮想マシン**で Duo を統合することをお勧めします。
      - Duo Network Gateway を使用してオンプレミスアプリケーションに対する SSH アクセスまたはアプリケーションアクセスを実現している場合は、ネットワーク外部から VPN クライアントを使用せずに対象のアプリケーションにアクセスできることを確認してください。
    - テスト環境または実稼働環境のどちらでアプリケーションを使用しているかがわかるように、Duo 管理パネルで**アプリケーションにラベルを付けます。**
      - 例：*Eng-SSH-TEST* と *Eng-SSH-PROD* は、それぞれテスト環境用と実稼働環境用に設定された 2 つの別々の Duo Unix アプリケーションです。

- **ハイアベイラビリティ/ディザスタリカバリ設定**
  - **主なリソース**
    - ビジネス継続性確保のための Duo ガイド
    - ハイアベイラビリティ/ディザスタリカバリのための Duo Authentication Proxy のセットアップ
    - ハイアベイラビリティを実現する Duo Access Gateway のセットアップ
    - ハイアベイラビリティを実現する Duo Network Gateway のセットアップ
  - **ベストプラクティス**
    - Duo failmode オプションと、そのオプションをサポートしている統合ソリューションについて理解します。
      - **Duo Authentication Proxy** を含む認証ワークフローと、WINLOGON/RDP や UNIX PAM などのほとんどのインストーラベースの統合ソリューションでは、一般的に failmode を設定できます。
    - 長期間サービスが中断している場合に、認証ワークフローから **Duo を除外するための緊急対応計画**を策定してください。
      - 対応計画は、**アプリケーションごと**に策定する必要があります。

- **エンドユーザパイロットを実施する**
  - **主なリソース**
    - コンセプト実証の導入
  - **ベストプラクティス**
    - 円滑に導入するために、複数のフェーズで Duo のパイロットテストを実施することをお勧めします。
      - **フェーズ 1：**IT 部門または技術に精通したユーザのパイロットグループでテストを行い、Duo が機能し、ログインエクスペリエンスが想定どおりであることを確認します。
      - **フェーズ 2：**IT グループでログインエクスペリエンスを確認したら、技術に精通していない業務部門の小さなユーザグループに導入して、ユーザ教育に抜けがないかを確認し、大規模に導入した場合の状態を想定します。

ポリシーおよび制御：重要なリソースへのアクセスを保護する

ポリシーおよび制御の概要

Duo のポリシーを利用すると、アプリケーションにアクセスできるユーザや、アクセスできる条件に関するルールを簡単に作成できます。ポリシーをユーザグループまたはアプリケーションごとに**カスタマイズ**したり、全体に共通するカスタマイズを実施したりすることで、導入環境内のアクセスをきめ細かく制御できます。ユーザ登録戦略では、ポリシーに関する設定も通知されます。Duo Beyond の登録者は、**信頼できるエンドポイントに関するポリシーを設定**してデバイスの信頼性をチェックすることで、環境内をさらに詳細に管理できます。

- **Duo ポリシーを利用してユーザアクセス制御をカスタマイズする**
  - 主なリソース
    - ポリシーおよび制御に関する参考資料
    - Duo ポリシーガイド：Duo のポリシーエンジンを利用したアクセス設定
  - ベストプラクティス
    - 登録、グループ、ユーザのステータスによって、ポリシーの実装に影響が及ぶ可能性があることに注意してください。
    - ポリシー実装シナリオによっては、目的の成果を達成するために、**アプリケーションポリシーとグループポリシーの両方が必要**になる場合があります。
      手始めとして、他の Duo のお客様が実装した**最も一般的なポリシー制御**の一部をご紹介します。導入する際の参考にしてください。
      - ユーザは最新バージョンの Duo Mobile を導入する必要がある
      - モバイルユーザは画面ロックを有効にする必要がある
      - ユーザは最新バージョンの iOS を利用している、または、Android に最新のセキュリティパッチを適用している必要がある
      - 信頼できるエンドポイントを使用している場合にのみユーザにアクセスを許可する
      - 匿名 IP からのアクセスは拒否する
      - サポートされていないブラウザからのアクセスは拒否する

- **信頼できるエンドポイントの設定およびテストの概要**
  - **主なリソース**
    - 信頼できるエンドポイントに関する参考資料
    - 信頼できるエンドポイントに関するベストプラクティスガイド
    - Duo でデバイスの信頼を確立する方法
    - 信頼できるエンドポイントに関するナレッジベースの記事
  - **ベストプラクティス**
    - 信頼できるエンドポイントに関するグローバルポリシーでは、デバイスが信頼できるかどうかがデフォルトで確認されますが、デバイスが信頼できない場合でもアクセスはブロックされません。デフォルトのグローバル設定はそのままにし、アプリケーションまたはユーザグループに適用するポリシーを追加して、信頼ステータスに基づいて許可または拒否することを推奨します。
    - エンドユーザのモバイルデバイスからセキュアなアプリケーションにアクセスするたびにセキュリティポスチャをチェックするように、Duo Mobile を統合した信頼できるエンドポイントを使用することを検討してください。Duo Mobile を有効にするとユーザにプロンプトが表示され、認証の前に Duo Mobile を開いてデバイスのヘルスチェックを実行するように求められます。
  - **信頼できるエンドポイントのテストとトラブルシューティング**
    - 組織はそれぞれ異なるため、この機能を展開して適用する方法も異なります。一般的な導入シナリオについては、導入設定のヒントに記載されています。
    - エンドユーザ エクスペリエンスを確認するためにテストを実施することをお勧めします。
      - ユーザが認証中に別のプロンプトが表示されるか
      - ブロックポリシーが設定されている場合、信頼されていないデバイスからアクセスを試みるとブロックされるか
    - 包括的なテスト計画の一環として、次のような方法でアプリケーションにアクセスするテストを検討します。
      - Android や iOS などのモバイル OS を含む複数の OS を使用する
      - デスクトップとモバイルデバイスの両方でシックアプリケーションを使用する（該当する場合）
      - モバイルブラウザを含むさまざまなブラウザを使用する
    - テストのために手動登録機能を統合している場合は、テストデバイスで手動登録用の証明書をダウンロードしてインストールしても、デバイスの信頼性をチェックすることにはならないことに注意してください。該当のテストデバイスに関連付けられたユーザをテストユーザグループに追加し、そのテストグループを手動登録統合機能に関連付けるようにしてください。また、手動登録証明書は、最初に使用するユーザにのみ関連付けられることにも注意してください。ただし、1 台のマシンでユーザログインにごとに別々の証明書を関連付けることができます。
    - **トラブルシューティング**：信頼されたエンドポイントに関する一般的な質問や問題のリストについては、信頼されたエンドポイントに関するナレッジベースの記事を参照してください。

エンドユーザ コミュニケーション：全員の理解が必要

エンドユーザ コミュニケーションの概要

Duo がどのようなものであるか、Duo を利用するとどうなるか、Duo をどうやって登録するかについて知る必要がある**エンドユーザ**が大勢いるはずです。以下に、**ユーザにわかりやすいテンプレートとリソースを示します。**優れたエンドユーザ コミュニケーション プランを策定することで導入が促進され、導入の際のヘルプデスクの負担が大幅に軽減されます。

- **エンドユーザ向けコミュニケーション資料の構築**
  - **主なリソース**
    - Duo ユーザガイド
    - Duo Push 推進ガイド
    - ビデオ：Duo へようこそ（エンドユーザ向け）
    - ビデオ：Duo スタートアップ - Duo Mobile の登録および Duo Push の利用
    - ビデオ：Duo Push による二要素認証
    - Duo のデモ Web サイト
  - **テンプレート**
    - エンドユーザ教育用電子メール コミュニケーション テンプレート
    - カスタマイズ可能な Duo 導入サイネージテンプレート
  - **ベストプラクティス**
    - ユーザに Duo Push を利用するように働きかけます。Duo Push は、安全に認証できる安価で簡単な方法です。Wi-Fi またはデータ通信対応携帯電話サービスのいずれかで動作し、どの国でも使用できます。
    - **登録リンクとアクティベーションリンクの有効期限が異なることに注意してください。**登録リンクの期限は 30 日です（再送しても期限は延長されません）。アクティベーションリンクは、デフォルトで 24 時間後に期限切れになります。
    - 一部のユーザでは、**フィッシング**に関するアラートが発生する可能性が高いことを想定しておきます（該当ユーザでは、Duo からの電子メールがフィッシング攻撃であると認識される可能性がある）。
    - お客様の会社で**電子メールフィルタ**を使用している場合、no-reply@duosecurity.com をホワイトリストに登録します。
    - Duo Mobile を信頼できるものとして導入する場合は、エンドユーザの操作がどのように変わるかを知らせるエンドユーザ向け通知内容を策定して送信することを検討します。詳細については、こちらのナレッジベースの記事を参照してください。

ヘルプデスクトレーニング：チームの準備

ヘルプデスクトレーニングの概要

ヘルプデスクの従業員は、サポートの最初の窓口です。ヘルプデスクをサポートするために、**便利なガイド**を作成しました（以下のリンク）。また、Duo の概要や、組織のために信頼できるアクセスを確保することの重要性に関して**ヘルプデスクチームを教育する方法**についても記載しています。

- **ヘルプデスクチームの準備を整える**
  - **主なリソース**
    - ヘルプデスクガイド
    - Duo ナレッジ ベース
    - Duo システムステータスページ
      Duo 管理パネル
  - **ベストプラクティス**
    - ヘルプデスクのスタッフは、**Duo と二要素認証に関する知識がまったくない**ことを前提とします。
      - 「二要素認証とは」というビデオを観てもらい、2FA の概要を説明します。
      - 自分のスマートフォンを見せるか、**Push からの通知デモ**を利用して、Duo Push のデモンストレーションを行います。
    - Duo の管理者に対して、管理者アカウントがユーザアカウントとは異なること、管理者アカウントは管理パネルと保護されたアプリケーションの両方にアクセスできる必要があることを再度説明します。
    - ヘルプデスクチームに対して、**重大度が緊急の問題が発生した場合、電子メールではなく電話で** Duo サポートに連絡してすぐに対処する必要があることを徹底します。
      - 業務が停止し、手続きによって回避できる策もない場合は、**重大度は緊急**であると考えられます。

Duo サポートおよび役立つリソース

Duo サポートの概要

上記のリソース以外にさらにサポートが必要な場合は、サポートチーム**にお問い合わせください。**ケースは、カスタマーチケットポータルで作成します。チケットポータルでは、チケットを簡単に作成し、ログ、設定、スクリーンショットなどの技術情報を Duo サポートと安全に共有できます。support@duosecurity.com では常時メールを受け付けています。

直接問い合わせが必要な場合や緊急のサポートが必要な場合は、**（866）760-4247** までお電話ください。米国以外のお客様は、こちらで各国の電話番号をご確認ください。

Duo のサポートチームは、**月曜日から金曜日の午前 9 時から午後 6 時（現地時間）**まで対応しております。これ以外の時間は、Duo サポートに連絡して、Duo のサービスに緊急の問題が発生したことを報告してください。緊急とは、「**Duo のサービスによってお客様の業務が停止し、手続き上の回避策がない**」場合と定義されています。新規セットアップまたは導入に関する一般的なご質問は、緊急とは見なされないことに注意してください。

Duo サポートに問い合わせできるのは、Duo 管理パネルに登録されている管理者のみです。すぐにサービスを受けられるように、Duo Push 認証（またはその他の方法）用の ID と 10 桁のアカウント ID をご用意ください。

役立つリソースの概要

Duo は、優れたエクスペリエンスを提供することに注力しています。以下は、**Duo サブスクリプションを最大限に活用するために役立つ主なリソース**です。

- Duo ナレッジベース：Duo の広範なナレッジベースを検索すれば、お客様の一般的な問題に関する回答をすぐに得られます。
- Duo マニュアル：さまざまなデバイスやアプリケーションに関する詳細な導入マニュアル、インストールや設定に関する情報が記載されています。
- Duo コミュニティ：Duo の公開フォーラムで Duo ユーザやセキュリティの専門家と連携して情報交換できます。
- ステータスページ：Duo システムの現在のステータスを確認できます。
- カスタマーチケットポータル：新しいケースの作成、過去のリクエストの確認、CSAT フィードバックの送信ができます。
- 製品リリースノート：登録すれば、新しいリリースノートが投稿され次第、電子メールが送信されます。
- Duo ブログ：Duo の公式ブログ。製品およびセキュリティ業界の最新情報を入手できます。
- 今後の Duo イベントおよびウェビナー：今後のイベントやウェビナーに関する最新情報が記載されています。
- その他のリソース：ガイド、ハウツーマニュアル、インフォグラフィック

Duo 実稼働：シームレスな導入を実現

Duo 実稼働の概要

おめでとうございます！すべての手順を完了し、スムーズでシームレスな導入を実現するための準備が整いました。確実に稼働日を迎えるために、Duo の実稼働に関する**最終チェックリスト**を以下に示します。

Duo 実稼働チェックリスト：

- ❑ **Duo の導入に関して社内に告知する**
  - ❑ **イントラネットまたは従業員コミュニティの Web ページ**に Duo に関する通知を投稿します。
  - ❑ **会社のイベント**や**プレゼンテーション**で Duo を告知します。
  - ❑ 会社のあらゆる場所に Duo のポスターを掲示します。共有エリアや昼食場所などが最適です。
- ❑ **ヘルプデスクの準備状況**とヘルプデスクチームの **Duo エスカレーション計画**を確認します。
- ❑ それぞれの組織（エンドユーザ、ヘルプデスク、IT 管理者）に電子メールを送信し、Duo がいつから実稼働するかを通知します。

このガイドや Duo の導入プロセス、その他ご覧になったドキュメントに関して、ぜひフィードバックやご意見をお寄せください。電子メール：liftoff-feedback@duo.com