Cisco Duo

プライバシー データシート

目次

このプライバシーデータシートでは、Cisco Duo における個人データ（または個人を識別できる情報）の処理について説明します。

1. Cisco Duo の機能概要

Cisco Duo（「Duo」）は、クラウドベースのソフトウェアサービスで、独自のアプリケーションやサードパーティ製アプリケーションへのアクセスを保護するために設計された付加的なセキュリティレイヤをお客様に提供します。ほとんどのアプリケーションでは、ユーザ名とパスワードのみでユーザのログインが許可されます。Duo で保護されている場合、最初にお客様/アプリケーション側で（またはお客様の設定に応じて、Duo がホストする SSO の支援を受けて）ユーザ名とパスワードが検証されます。その後、ログインプロセスの完了前に付加的なアクションを実行するようにユーザに求めることにより、Duo の二要素ワークフローがトリガーされます（例：Duo のモバイルアプリ、SMS、電話、またはハードウェアトークンによるログインの確認）。お客様は、アクセスを許可する前にユーザデバイスのセキュリティの状態をさらに確認し、危険なデバイスを持つユーザのアクセスをブロック、通知、または制限できます。また、Duo の使用により、さまざまなユーザグループにどの内部アプリケーションへのアクセスを許可するかを制御して、機密情報の閲覧を制限したり、アプリケーションレベルでポリシーを適用したりすることもできます。

Duo の詳細については、https://duo.com/docs のリンクを参照してください。

サービスを使用するために、個人データの入力を求められる場合があります。以下に、Duo の提供に関連したシスコによる個人データの処理、個人データの場所および転送、さらにプライバシーの原則および法規制に準拠した個人データの保護方法について説明します。お客様が Duo サービスの使用を選択される場合、シスコに個人データを開示する必要があります。シスコは、お客様の個人データを本プライバシーデータシートに従って使用します。本プライバシーデータシートは、シスコプライバシーポリシーの補足資料であることにご留意ください。ここでは、Duo がサービスを提供するために処理する個人データ、その保管場所、ならびにプライバシーの原則および法規制に準拠したデータの保護方法について説明します。

2. 個人データの処理

以下の表に、Duo がサービスを提供するために利用する個人データと、個人データを処理する目的を記載しています。

個人データのカテゴリ	個人データの種類	処理の目的
エンドユーザの登録/認証情報	• ユーザ名（Username） • 電話番号 • 電子メール アドレス（Email address） • 組織名（Organization name） • Duo でホストされる SSO で認証されるユーザの Active Directory ユーザ名およびパスワード（パスワードは各認証の完了に十分な期間だけキャッシュされる）	• アカウントの作成および有効化 • サービスの認証とログイン • セキュリティ機能の提供、サポート、改善、サービスのアップグレードおよび改善
管理者の登録情報	• 名前 • ユーザ名（Username） • 電話番号 • 電子メール アドレス（Email address） • 請求および配送先住所 • Duo 管理者パネルで使用するパスワードの一方向ハッシュ表現 • 役職（Job title） • 組織名（Organization name）	• アカウントの作成および有効化 • サービスの認証とログイン • セキュリティ機能の提供、サポート、改善、サービスのアップグレードおよび改善
エンドユーザデバイスのメタデータ	• デバイスのタイプ • デバイスのオペレーティングシステム、デバイスのバージョン、その他のデバイス特性（例：デバイスが「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る） • 接続情報（Duo サービスへのアクセスに使用される暗号化プロトコルなど） • ブラウザタイプ • IP アドレス • 公開キーインフラストラクチャ証明書がインストールされているかどうか • タイムゾーン（Time zone） • 認証の日時 • 広範な地理的エリア（国または都市レベルの場所） • デバイスがアクセスを試みているアプリケーション • デバイスが特定のプラグインを使用しているかどうか • エンドユーザに関連付けられたデバイスの完全修飾ドメイン名 • デバイス識別子（デバイス名、プロセッサ ID、シリアル番号、UDID、UUID、DNS ホスト名など）	• サービスの提供と維持 • ユーザエクスペリエンスの向上 • セキュリティ機能の向上 • サービス品質の改善 • デバイスやアプリケーションの安全性の確保 • デバイスが安全であることを確認する証明書の発行 • デバイスの認証 • 仮名化された使用状況データや集約された使用状況データを使用して統計分析を実施し、サービスを改善 • 潜在的な、または実際の請求、法的責任、禁止行為、セキュリティリスク、犯罪活動に対する防止、検出、対応、保護

個人データのカテゴリ	個人データの種類	処理の目的
イベントと使用状況データ	• エンドユーザがサービスにアクセスする方法 • アクセスの日時 • サービスにアクセスする場所を決定する IP アドレス • デバイスのイベント（クラッシュ、システムアクティビティ、ハードウェア設定など）	• サービスの提供と維持 • ユーザエクスペリエンスの向上 • セキュリティ機能の向上 • サービス品質の改善 • 仮名化された使用状況データや集約された使用状況データを使用して統計分析を実施し、サービスを改善 • 潜在的な、または実際の請求、法的責任、禁止行為、セキュリティリスク、犯罪活動に対する防止、検出、対応、保護
認証ログとアクティビティログ	• サービスにアクセスするエンドユーザ • サービスにアクセスするデバイス • サービスによって保護されるアプリケーション • サービスにアクセスする時間 • サービスにアクセスする際のエンドユーザの IP アドレス	• サービスの提供と維持 • ユーザエクスペリエンスの向上 • セキュリティ機能の向上 • サービス品質の改善 • 仮名化された使用状況データや集約された使用状況データを使用して統計分析を実施し、サービスを改善 • 潜在的な、または実際の請求、法的責任、禁止行為、セキュリティリスク、犯罪活動に対する防止、検出、対応、保護

3. 国境を越えたデータ転送

Duo は米国に本拠を置き、国際的に事業を展開しています。Duo は、米国、カナダ、アイルランド、およびドイツの Amazon Web Services（AWS）データセンターを利用しています。サインアップ時に米国またはカナダの電話番号を使用しているお客様は、米国ベースの AWS インスタンスに自動的に配置されます。Duo がサービスの提供を許可されている他の地域の電話番号を使用しているお客様は、自動的に欧州ベースの AWS インスタンスに配置されます。お客様は、Duo で使用する製品インスタンスを任意の地域の AWS ロケーションに配置するようリクエストすることもできます。

AWS では、セキュリティを確保してデータを保護するために強力な制御機能を備えています。物理的なセキュリティ制御には、フェンス、壁、セキュリティスタッフ、ビデオ監視、侵入検知システム、その他の電子的な手段などの境界防御が含まれますが、これらに限定されません。詳細については、AWS マニュアルを参照してください。Duo の物理的セキュリティの詳細については、秘密保持契約を前提として入手可能な Duo の情報セキュリティポリシーに記載されています。

Duo の世界各地のサポートスタッフは、米国やその他の地域に保存されている個人データにアクセスできます。さらに、特定の個人データ（電話番号など）は、認証コードを含むテキストメッセージの送信やエンドユーザがいる場所でログインを検証する VOIP ベースの自動音声発信など、サービスの提供に関連した目的で、Duo のサードパーティベンダーに国境を越えて転送されることがあります。

Duo は、複数の司法管轄区域にわたって合法的にデータを利用できるようにするため、さまざまな転送メカニズムに投資しています。その際、特に以下を考慮しています。

- 拘束的企業準則
- EU - 米国間のプライバシー シールド フレームワーク
- スイス - 米国間のプライバシー シールド フレームワーク

- APEC クロスボーダー プライバシー ルール
- APEC データ処理事業者向けプライバシー識別
- EU 標準契約条項

4. アクセス コントロール

個人データのカテゴリ	アクセス可能者	アクセスの目的
エンドユーザの登録/認証情報	顧客管理者	サービスやその他の管理者情報へのアクセスの変更と制御
	Duo	データアクセスとセキュリティ管理プロセスに応じた本サービスのサポート
管理者の登録情報	Duo	サービスの提供、サポート、アップグレード、改善
エンドユーザデバイスのメタデータ	顧客管理者	顧客ネットワークのポリシーの設定、顧客ネットワークの監視、およびユーザとアプリケーションへのアクセスの制限または承認
	Duo	サービスの提供、サポート、アップグレード、改善
イベントと使用状況データ	顧客管理者	顧客ネットワークのポリシーの設定、顧客ネットワークの監視、およびユーザとアプリケーションへのアクセスの制限または承認
	Duo	サービスの提供、サポート、アップグレード、改善
認証ログとアクティビティログ	顧客管理者	顧客ネットワークのポリシーの設定、顧客ネットワークの監視、およびユーザとアプリケーションへのアクセスの制限または承認
	Duo	サービスの提供、サポート、アップグレード、改善

5. データポータビリティ

お客様は、Duo 管理者パネルを使用してデータにアクセスできます。こうしたデータの抽出およびエクスポートの依頼については、privacy@cisco.com までお問い合わせください。

6. データの削除および保持

お客様は privacy@cisco.com に通知することにより、個人データの削除をいつでも求めることができます。お客様が、Duo によって保存された個人データの削除を要求された場合、Duo は、適用法によって義務付けられた範囲内で、対象となるデータを Duo のシステムから消去するか匿名化します。また、Duo は、以下に記載する正当な業務上の目的のために必要な管理データ（課金記録など）を保持することがあります。

Duo は、個人データの保持に継続的かつ正当なビジネスニーズがある限り、個人データを保持します。これには、お客様が本サービスに関して少なくとも 1 つのアクティブなアカウントを持っている間、個人データを常に保持することが含まれます。ただし、お客様は、以下に示すように、ユーザ/管理者の登録情報とログを削除できます（手動で削除された特定のデータが Duo のシステムから完全に消去されるまでに最大 30 日かかる場合があることに注意してください）。

Duo マルチテナントサービスは、顧客データのデータ整合性と可用性に関する強力な保証を提供するように構築されています。このアーキテクチャのコアコンポーネントは、以前に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性とのバランスをとる必要があります。

次の表で、Duo のデフォルトの個人データ保持ポリシーについて説明します。このポリシーは、お客様が Duo 管理パネル内で利用可能な他のアクションを実行しないすべての場合に適用されます。

個人データのカテゴリ	アカウント削除後の保持期間	保持の理由
エンドユーザの登録/認証情報	1 年（お客様がそれ以前に削除しない限り）*	この保持期間が選択されたのは、過去に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性の間でバランスを取るためです。また、このデータのコピーも、本サービスのセキュリティ、品質、および機能の改善をサポートするために保持されます。こうした目的で使用される際、すべての個人データは仮名化されます（IP アドレスは、脅威の検出および関連したセキュリティ上の理由により元の形式で使用することが必要なため、例外となります）。指定された保持期間が期限切れになると（IP アドレスの場合は収集から 1 年間）、前述の目的で使用されたすべての個人データは削除または匿名化されます。これは、その他の実稼働データやアカウント情報が再度識別可能にならないようにするためです。 * Duo がホストする SSO の Active Directory パスワードは、各認証の完了に十分な期間しかキャッシュされない点に注意してください。
管理者の登録情報	1 年（お客様がそれ以前に削除しない限り）	この保持期間が選択されたのは、過去に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性の間でバランスを取るためです。また、このデータのコピーも、本サービスのセキュリティ、品質、および機能の改善をサポートするために保持されます。こうした目的で使用される際、すべての個人データは仮名化されます（IP アドレスは、脅威の検出および関連したセキュリティ上の理由により元の形式で使用することが必要なため、例外となります）。指定された保持期間が期限切れになると（IP アドレスの場合は収集から 1 年間）、前述の目的で使用されたすべての個人データは削除または匿名化されます。これは、その他の実稼働データやアカウント情報が再度識別可能にならないようにするためです。
エンドユーザデバイスのメタデータ	1 年（お客様がそれ以前に削除しない限り）	この保持期間が選択されたのは、過去に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性の間でバランスを取るためです。また、このデータのコピーも、本サービスのセキュリティ、品質、および機能の改善をサポートするために保持されます。こうした目的で使用される際、すべての個人データは仮名化されます（IP アドレスは、脅威の検出および関連したセキュリティ上の理由により元の形式で使用することが必要なため、例外となります）。指定された保持期間が期限切れになると（IP アドレスの場合は収集から 1 年間）、前述の目的で使用されたすべての個人データは削除または匿名化されます。これは、その他の実稼働データやアカウント情報が再度識別可能にならないようにするためです。

個人データのカテゴリ	アカウント削除後の保持期間	保持の理由
イベントと使用状況データ	1 年（お客様がそれ以前に削除しない限り）*	この保持期間が選択されたのは、過去に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性の間でバランスを取るためです。また、このデータのコピーも、本サービスのセキュリティ、品質、および機能の改善をサポートするために保持されます。こうした目的で使用される際、すべての個人データは仮名化されます（IP アドレスは、脅威の検出および関連したセキュリティ上の理由により元の形式で使用することが必要なため、例外となります）。指定された保持期間が期限切れになると（IP アドレスの場合は収集から 1 年間）、前述の目的で使用されたすべての個人データは削除または匿名化されます。これは、その他の実稼働データやアカウント情報が再度識別可能にならないようにするためです。 * 特定のデバッグログは、カスタマーサポートの目的、セキュリティレビュー、およびシステムパフォーマンスのパターンの監視とアラートのため、最大 90 日間、Duo のシステム内で保持される場合があります。
認証ログとアクティビティログ	1 年（お客様のログ保持設定によっては 1 年未満）	この保持期間が選択されたのは、過去に削除されたお客様に関連付けられているデータを消去する必要性と、その他のアクティブなお客様に関連付けられているデータが適切に維持および保護されていることを保証する必要性の間でバランスを取るためです。また、このデータのコピーも、本サービスのセキュリティ、品質、および機能の改善をサポートするために保持されます。こうした目的で使用される際、すべての個人データは仮名化されます（IP アドレスは、脅威の検出および関連したセキュリティ上の理由により元の形式で使用することが必要なため、例外となります）。指定された保持期間が期限切れになると（IP アドレスの場合は収集から 1 年間）、前述の目的で使用されたすべての個人データは削除または匿名化されます。これは、その他の実稼働データやアカウント情報が再度識別可能にならないようにするためです。
サービスのバックアップ	上記で指定された期間を超えて 3 年	バックアップは毎日、生成および暗号化され、データの整合性とサービスの復元力を保持するためにコールドストレージに移されます。この保持期間は、お客様が、独自の法的開示またはフォレンジックのニーズに応えるために、履歴データへのアクセスを要求するシナリオの大部分をカバーするのに十分な期間として選択されました。
Duo の財務、監査、またはその他の法的義務に関連したデータ	関連した義務を果たすために必要な期間	Duo は、金融取引の証拠、監査要件、またはその他の法的義務に関連した特定のデータを保持する必要がある場合があります。そのようなデータの保持は、その法的義務とシスコのエンタープライズ記録保持スケジュールに沿って、こうしたデータを保持するために Duo が必要とされるタイムラインに関連付けられます。

7. 個人データのセキュリティ

個人データのカテゴリ	暗号化のタイプ
エンドユーザの登録/認証情報	Transport Layer Security（TLS）経由の転送における暗号化。暦年 2018 年以降に確立されたすべてのお客様のアカウントを保管時に暗号化。
管理者の登録情報	Transport Layer Security（TLS）経由の転送における暗号化。暦年 2018 年以降に確立されたすべてのお客様のアカウントを保管時に暗号化。
エンドユーザデバイスのメタデータ	Transport Layer Security（TLS）経由の転送における暗号化。暦年 2018 年以降に確立されたすべてのお客様のアカウントを保管時に暗号化。

個人データのカテゴリ	暗号化のタイプ
イベントと使用状況データ	Transport Layer Security（TLS）経由の転送における暗号化。暦年 2018 年以降に確立されたすべてのお客様のアカウントを保管時に暗号化。
認証ログとアクティビティログ	Transport Layer Security（TLS）経由の転送における暗号化。暦年 2018 年以降に確立されたすべてのお客様のアカウントを保管時に暗号化。

Duo は、2018 年より前に作成されたアカウントに対して保管時の暗号化を有効にすることに積極的に取り組んでいます（該当するアカウントの保管時の暗号化は、support@duosecurity.com に問い合わせることで依頼できます）。データが暗号化されているかどうかにかかわらず、Duo は複数の手法を使用してお客様のデータを保護しています。そうした手法には、データストアと Duo プラットフォームの他のコンポーネントとの間におけるネットワーク セグメンテーション、ロールや責任に基づいたデータストアへの最小限のアクセス権限の付与、攻撃対象領域を最小化するための生産アセットのセキュリティ強化などが含まれますが、これらに限定されません。

8. サードパーティ サービス プロバイダー（副データ処理事業者）

Duo は、お客様がシスコに期待するレベルと同一レベルのデータ保護および情報セキュリティが確保されることを契約で確約できる場合に、サービスプロバイダーと連携します。Duo サービスに関連した副データ処理事業者の現在のリストは以下のとおりです。

副データ処理事業者	個人データ	Service type	データセンターの場所
AWS	エンドユーザ登録/認証情報、エンドユーザ デバイス メタデータ、管理者の登録情報、イベントおよび使用状況データ、認証ログとアクティビティログ	クラウドベースのインフラストラクチャとホスティング、分析、データストレージ	US、カナダ、アイルランド、ドイツ、オーストラリア
認定セキュリティソリューション d/b/a keyfactor	エンドユーザ登録/認証情報、デバイス ID（シリアル番号など）	Duo Beyond に登録されているデバイスに対する証明書を発行および管理する PKI サービス	US
Twilio 社	エンドユーザの登録/認証情報	認証用の電話および SMS	US
Nexmo 社	エンドユーザの登録/認証情報	認証用の電話および SMS	US
Clickatell 社	エンドユーザの登録/認証情報	認証用の電話および SMS	US
Bandwidth 社	エンドユーザの登録/認証情報	認証用の電話および SMS	US
Google	エンドユーザの登録/認証情報	認証用の SMS およびプッシュ通知	US、アイルランド
Apple	エンドユーザの登録/認証情報	認証用の SMS およびプッシュ通知	US

副データ処理事業者	個人データ	Service type	データセンターの場所
Rackspace 社	エンドユーザ登録/認証情報、エンドユーザ デバイス メタデータ、管理者の登録情報、イベントおよび使用状況データ、認証ログとアクティビティログ	データストレージ、コールドバックアップのホスティング	US、UK
Microsoft	エンドユーザ登録/認証情報、エンドユーザ デバイス メタデータ、管理者の登録情報、イベントおよび使用状況データ、認証ログとアクティビティログ	任意の Microsoft Azure サービスと統合できるため、お客様が管理するクラウドアプリケーションへの保護レイヤの追加や、お客様が管理する Azure AD ユーザディレクトリと Duo 製品の同期が可能	US

9. 情報セキュリティインシデント管理

侵害およびインシデントの通知プロセス

Duo 内のセキュリティチームは、データインシデント対応プロセスを調整し、データ関連のインシデントに対する Duo の対応を管理しています。Duo チームは、特定のインシデントに適用可能で必要な場合には、Cisco Product Security Incident Response Team（PSIRT）および Cisco Security Incident Response Team（CSIRT）を含む、シスコ内のインシデント対応チームと連携して機能します。

Duo のセキュリティチームは、Cisco PSIRT チームと協力して、Duo 製品とネットワークに関連したセキュリティ脆弱性の報告受付、調査、および公表を管理します。また、お客様、独立したセキュリティ研究者、コンサルタント、業界団体、他のベンダーと協力して、Duo 製品およびネットワークのセキュリティに関する潜在的な問題を特定します。Duo のセキュリティ対応手順とシスコ セキュリティセンターでは、セキュリティインシデントの報告プロセスが詳しく説明されています。

シスコ通知サービスに登録すれば、重要なシスコ製品およびテクノロジーに関する情報を定期的に受け取れます。その中には、重要度が「緊急」または「重要」のセキュリティ脆弱性に関するシスコ セキュリティ アドバイザリなどが含まれています。このサービスでは、通知のタイミングおよび通知の方法（電子メールメッセージまたは電話）をお客様が選択できます。情報へのアクセスレベルは、お客様とシスコとの取引関係によって決まります。製品またはセキュリティ通知に関する質問や懸念がある場合は、シスコのセールス担当者にお問い合わせください。

10. 認定とプライバシー保護法の遵守

セキュリティ & トラスト部門とシスコ法務部門は、リスクおよびコンプライアンスに関する管理サービスやコンサルティングサービスを提供し、シスコ製品/サービスの設計にセキュリティや規制遵守機能を組み込むための支援を行っています。シスコおよびシスコが実施するプロセスは、EU 一般データ保護規制（GDPR）および世界中の他のプライバシー保護法に基づいてシスコが責務を果たせるように設計されています。厳しい社内標準に従うことに加えて、シスコは、情報セキュリティに対するシスコの真摯な取り組みを示すために、SOC2 Type II 監査レポート、サービスの 2 つの FedRAMP 認可エディションなどのサードパーティによる検証も行っています。

11. 全般的な情報および GDPR に関する FAQ

全般的な情報および、シスコのセキュリティ コンプライアンス プログラムや GDPR 対応に関連する FAQ（よくある質問）については、Cisco Trust Center をご確認ください。

シスコのプライバシーデータシートは、毎年（または必要に応じて）見直され、更新されます。最新のバージョンについては、https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html を参照してください。

お問い合せ先

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
http://www.cisco.com/jp