Webex Calling

本プライバシーデータシートでは、Webex Calling 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。

Webex Calling（「本サービス」または「Webex Calling」）は、シスコが本サービスを取得した企業または個人に提供するクラウドベースのビジネス電話システムであり、権限を持つユーザーが使用できます。

シスコは、本プライバシーデータシートに従って Webex Calling サービスの個人データを処理します。データ管理者とデータ処理者を区別する法域では、お客様との関係を管理するために処理される個人データについては、シスコはデータ管理者となります。一方、Cisco Webex Calling サービスが機能を提供するために処理する個人データについては、シスコがデータ処理者となります。

本プライバシーデータシートは、シスコのプライバシーステートメントの補足資料であることにご注意ください。

Note: 本文書は「Webex Calling Privacy Data Sheet」の参考和訳です。原文（英語）と差異がある場合には、原文の内容が優先します。

1. 概要

Webex Calling は、シスコとその小売/卸売パートナー（「パートナー」）が、許可されたユーザー（それぞれ「ユーザー」）のために本サービスを購入する企業（「お客様」）に提供する、クラウドベースのビジネス電話システムです。本サービスは、包括的なビジネス電話システムを提供する、シスコのクラウドでホストされたサブスクリプションベースのサービスのため、オンプレミス機器は必要ありません。また、次世代モビリティと拡張性という利点も備えています。

お客様が本サービスのユーザーである場合、本プライバシーデータシートに記載されている情報は、以下に示すように、お客様、パートナー、シスコがアクセス可能であり、また、本サービスに関連する情報へのアクセス、使用、監視、削除、保存およびエクスポートに関してお客様のポリシーの適用を受けます。シスコは、お客様が他のユーザーと共有した情報のプライバシーをコントロールせず、プライバシーについての責任を負いません。サービスから情報が削除された後でも、ユーザーまたはお客様が他者と共有した範囲内において、情報のコピーが他の場所で閲覧可能な状態になっている場合があります。

本サービスの詳細については、こちらを参照してください。本サービスには、Webex Calling と Webex App がバンドルされています。オプションで Webex Meetings と Webex Calling 専用インスタンスを追加すれば、包括的なコラボレーション アプリケーション スイートを構築できます。Webex Calling は、共通の Webex ポータル（Control Hub やその他の共通の Webex サービスなど）を活用します。共通ポータルの内容および設定の詳細については、Webex App および Webex Messaging プライバシーデータシートを参照してください。

Webex Calling 専用インスタンスは、シスコとそのリセールパートナーおよびサービスプロバイダー パートナーによって提供されるオプションのクラウドベースのビジネス電話サービスです。詳細については、以下の追補 I を参照してください。

以下に、本サービスと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、ならびにプライバシーの原則および法規制に従った個人データの保護方法について説明します。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利用します。

2. 個人データの処理

以下の表には、本サービスがサービスを提供するために利用する個人データおよびそのデータを処理する目的を記載しています。

Webex Calling は次のことを行いません。

- 自動化された手段のみをベースとする、データ情報カテゴリの権利に影響を与える法的またはその他の重大な影響をもたらす意思決定。
- お客様の個人データの販売。
- シスコのプラットフォームでの広告配信。
- 広告目的での使用状況やコンテンツのトラッキング。
- 通話トラフィックやコンテンツへの干渉。

個人データのカテゴリ	個人データの種類	処理の目的
登録情報	• 認証トークン • 名前とエイリアス • 電子メールアドレス • 電話番号 • クレデンシャル：ユーザー ID、パスワード、PIN • Cookie • 会社名 • 会社の担当者の氏名および役職 • 会社の所在地 • 会社のタイムゾーン • 組織 ID • お客様の注文情報 • SIP 識別子 • ボイスメールボックス番号 • デバイス アクティベーション コード	当社は、登録情報を以下の目的で利用します。 • 本サービスの運用サポートの配信および提供 • サービスのステータス、機能、可用性に関するお客様とのやり取り • 機能と更新の通知 • 本サービスの請求支援 • 本サービスへのアクセスの認証と許可 • 発信者 ID の表示 • 組織内でディレクトリサービスを有効化 • ユーザーや場所にコールをルーティング • 内部および外部のダイヤリングを許可 • お客様の IP フォンの有効化を許可 • お客様のボイスメールおよびボイスメール変換テキストへのアクセスを許可 • 本サービスの使用方法の把握 • お客様の設定に基づくシスコ マーケティング情報の送信

ホストおよび使用状況情報	• クレデンシャル：SIP、Web インターフェイス、XSI
	• プロファイルデータ：サービス機能設定
	• 接続データ：
	  ○ IP アドレス
	  ○ MAC アドレス
	  ○ デバイス識別子：IMEI
	  ○ MSISDN
	  ○ 固定電話番号
	  ○ SIP 番号
	• 利用データ：通信メタデータ、通話ログ
	• 通話詳細レコード（CDR）
		当社は、ホストおよび使用状況情報を以下の目的で利用します。
		• 電話サービスおよびそれに関連する機能の提供
		• 閲覧される画面およびトリガされるイベントなど、本サービスの使用状況の把握
		• 本サービスの請求支援
		• 技術的問題の診断
		• 本サービスの技術的なパフォーマンスを改善するための、集約され

	• ポータルアクセスの詳細 ○ ユーザーのドメイン名または IP アドレス ○ クライアントから要求されたファイル名および URL ○ ユーザーが本サービスにアクセスする起点となった Web サイト • 地理的位置情報：IP アドレスまたはデバイスロケーションに基づく • 連絡先リスト • Cookie • 請求ファイル • ログファイル（通信トラフィックデータを含む） • デバイス名 • タイムゾーン • 汎用一意識別子 • テキストメッセージのメタデータ	た形による分析および統計分析の実施 • お客様のサポート要求への対応 • 本サービスの請求支援 • 組織管理者に対する分析機能およびレポート機能の提供 • 電話詐欺の検出
ユーザーにより生成される情報	• ボイスグリーティングなどのアップロードされたメディアファイル • ボイスメッセージ • 通話の録音 • テキストメッセージ	当社は、ユーザー生成情報を以下の目的で利用します。 • 異なる場所のユーザーによるコラボレーションを可能にするサービスの提供 • カスタマイズされた保留音の提供 • ボイスメールおよびボイスメール音声のテキスト変換サービスの提供 注：通話の参加者間で音声およびビデオ通話のコンテンツと画面共有コンテンツをルーティングしますが、コンテンツを保持したり保存したりすることはありません（通話録音機能が実行されている場合を除く）。

Webex App
Webex App に関連する個人データ処理の詳細については、Webex App および Messaging プライバシーデータシートを参照してください。

Webex Meetings
Webex Meetings に関連する個人データ処理の詳細については、Webex Meetings プライバシーデータシートを参照してください。ボイスメールのテキスト変換情報は、Webex Assistant サービスを使用しているすべてのお客様に関して処理されます。Webex Assistant に関連する個人データ処理の詳細については、Webex Meetings プライバシーデータシートを参照してください。

テクニカル サポート アシスタンス
お客様が問題の診断および解決のために Cisco Technical Assistance Center（TAC）に連絡すると、Cisco TAC は本サービスから個人データを受信して、処理する場合があります。Cisco TAC のサービス提供プライバシーデータシートでは、シスコによる個人データの処理について記載しています。

3. データセンターの場所

本サービスは、世界中でサービスを提供するために、自社のデータセンターだけでなく、サードパーティ ホスティング プロバイダーおよびビジネスパートナーを利用しています。これらの事業体は、現在以下の国に所在しています（データセンターの場所は随時変更する可能性があります。変更があった場合、本プライバシーデータシートは更新されます）。

サービスコンポーネント	データセンターの場所
	シカゴ（イリノイ州、米国）
	カウンシル・ブラッフス（アイオワ州、米国）
	ダラス（テキサス州、米国）
	フランクフルト（ドイツ）
	ロンドン（英国）
	ロサンゼルス（カリフォルニア州、米国）
主な通話機能	メルボルン（オーストラリア）
	ニューヨーク（ニューヨーク州、米国）
	大阪（日本）
	シドニー（オーストラリア）
	東京（日本）
	トロント（カナダ）
	バンクーバー（カナダ）
	シンガポール
共通の Webex サービス	アムステルダム（オランダ）
	カリフォルニア州（米国）
	ロンドン（英国）
	バージニア州北部（米国）
	オハイオ州（米国）
	テキサス州（米国）

情報は、注文プロセスで指定されたお客様の地域にあるデータセンターに格納されます。TAC 情報は、シスコ データセンターに保存されます。情報には、シスコが業務を行っている場所の担当者もアクセスできます。

4. Webex Data Residency

Webex Calling Data Residency により、お客様のユーザー管理者は、組織のデータをどこに保存するかを選択できます。

お客様のユーザー管理者が Control Hub で作成するために選択した最初の場所は、お客様の主な通話および公衆交換電話網（「PSTN」）サービスがプロビジョニングされる場所です（この場所は、お客様の「通話地域」です）。有料のユーザーアカウントの場合は、EU のお客様を含め、Webex Calling によって処理された個人データは通話地域に保存されます（以下に記載されているものを除く）。無料のユーザーアカウントの場合は、EU のお客様を含め、Webex Calling によって処理されたデータが、アカウント所有者の地域外の Webex データセンターに保存される場合があります。

本サービスの特定の操作や機能を容易にするために、Webex Calling Data Residency には特定の例外が設けられています。具体的には、個人データの越境移転が、次の場合にも発生する可能性があります。（a）ユーザーがシスコプラットフォーム（www.cisco.com など）に登録する場合、（b）お客様が発注情報（業務上の連絡先情報）を提供する場合、（c）ユーザーが通話地域外のユーザーとコラボレーションする場合、（d）ユーザーがシスコの TAC を通じてテクニカルサポートを受ける場合（この場合、ユーザーが最初の TAC リクエスト内で提供した情報が通話地域外に転送される可能性があります）、（e）ユーザーが特定のオプション機能を有効にする場合、（f）ユーザーがスマートフォンの「プッシュ」通知を有効にしている場合（この場合、iOS または Android 機能に関連付けられたスマートフォンプロバイダーが通話地域外にデータを転送する可能性があります）、（g）共通の Webex コアサービスによって提供されるログ、分析、およびユーザー登録/ディレクトリ情報を含む一部の個人データは、お客様のユーザー管理者がこれらのサービスを使用するようにコントロールハブを設定した場所に保存されます。

クラス最高のエクスペリエンスを提供するために、ユーザーのデバイスとクライアントは地理的に最も近い Webex Calling データセンターに接続し、ユーザーの現在の場所に対して可能な限りローカルに通話を維持することができます。組織が PSTN に Cisco Calling Plan（CCP）を使用している場合、PSTN ブレークアウトが地理的に最も近い地域にあることも意味します。地域メディアの詳細については、https://help.webex.com/ja-jp/article/nixlytw/Webex-Calling-Regional-Media-for-Cloud-Connected-PSTN-(CCP) を参照してください。

5. データの越境移転メカニズム

シスコは、複数の法域にまたがる合法的なデータの使用を可能にするための複数の移転メカニズムに投資しています。主要なものは以下のとおりです。

- 拘束的企業準則 [英語]
- APEC 域内の個人データ越境移転ルール [英語]
- APEC 個人データ処理者認定 [英語]
- EU 標準契約条項 [英語]
- EU・米国間データ プライバシー フレームワーク、および英国の EU・米国間データ プライバシー フレームワークの拡張版 [英語]
- スイス・米国間データ プライバシー フレームワーク [英語]

6. アクセス制御

以下の表には、Cisco Webex Calling サービスがサービスを提供するために利用する個人データ、データへのアクセス権者、アクセスする目的を記載しています。

個人データのカテゴリ	アクセス権者	アクセスする目的
登録情報	エンドユーザーポータルを利用するユーザー	情報の変更、管理、および削除
	Control Hub ポータルを利用するお客様	• お客様のポリシーに従ったユーザーの管理およびサービスの管理 • 情報の変更、管理、および削除
	Control Hub ポータルを利用するパートナー	• 契約条件に従った本サービスのプロビジョニング、請求およびサポート • パートナーは、認証トークンまたはクレデンシャルにアクセスすることはできません
	シスコ	シスコのデータアクセスとセキュリティ管理プロセスに従った本サービスのサポート
ホストおよび使用状況情報	エンドユーザーポータルを利用するユーザー	• やり取りに関する情報と使用履歴の閲覧 • サービス機能の設定および連絡先リストなどの情報の更新
	Control Hub ポータルを利用するお客様	お客様のポリシーに従ったユーザーの管理およびサービスの管理
	Control Hub ポータルを利用するパートナー	契約条件に従った本サービスの請求およびサポート
	シスコ	• シスコのデータアクセスおよびセキュリティ管理プロセスに従った、本サービスの配信、サポートおよび改善 • 詐欺行為の検出および防止
ユーザーにより生成される情報	エンドユーザーポータルを利用するユーザー	ユーザーは、お客様の個人データに関するポリシーに従って、ユーザーが生成または受信したコンテンツのアクセス、変更または削除が可能
	Control Hub ポータルを利用するお客様	機能および電話番号割り当ての変更、制御および削除
	Control Hub ポータルを利用するパートナー	顧客データの抽出要求またはエンドユーザーの監査要求への対応、エンドユーザーの権利の遵守
	シスコ	本サービスのサポートのためにお客様がシスコと共有しない限り、シスコはこのデータにアクセスしません。アクセスする際は、シスコのデータアクセスおよびセキュリティ制御プロセスに従います

7. データポータビリティ

次の個人データは、機械で読み取ることのできる形式で利用できます：登録情報、ユーザー生成情報（ボイスメッセージを除く）、通話ログ、連絡先リスト、サービス機能設定、CDR。お客様は、上記のデータのいずれも、要求をパートナー（シスコに要求を提出する必要があります）に提出することにより取得できます。データの可用性には、下記セクション 8 に記載されている削除および保持のポリシーが適用されます。ユーザーは、通話ログおよびボイスメッセージをエンドユーザーポータルからダウンロードできます。それ以外の種類で利用可能な個人データはいずれも、取得を希望するユーザーが、各組織の管理者を通じて要求する必要があります。

8. データの削除および保持

お客様は、要求をパートナーに送信することで、本サービス上で保持されている個人データの削除を要求できます。パートナーは TAC リクエストを開いて、シスコに連絡する必要があります。お客様が削除の要求を行った場合、適用法に基づき、またはシスコの正当な事業目的のためにデータの保持が必要でない限り、シスコは要求されたデータを 30 日以内にそのシステムから削除するよう努めます。シスコが Webex Calling 内の特定カテゴリのデータを保持する必要がある場合、保持の理由および期間は以下の表のとおりです。Webex App および Webex Meetings のデータの削除および保持に関する詳細については、Cisco Trust Center を参照してください。

次の表には、Webex Calling サービスが使用する個人データ、個人データを保持する必要がある期間、保持する理由を記載しています。

個人データのカテゴリ	保持期間	保持する理由
登録情報	本サービスの終了時またはユーザーが無効化されてから 7 年。	シスコの財務デューデリジェンスの一環としてお客様から得た情報を含め、登録時に収集したデータは、シスコのビジネスレコードを構成し、シスコの財務および監査ポリシー、および税に関する要件に従って保持されます。
ホストおよび使用状況情報	• クレデンシャル、プロファイルデータ、連絡先リスト、地理位置情報、接続データおよび使用状況データは、サービスが終了するかユーザーが無効化されるとすぐに削除されます。 • ポータルアクセスの詳細データは 90 日後に削除されます。 • 通信トラフィックデータを含むログファイルは 30 日後に削除されます。ただし、EEA 諸国およびスイスでは 7 日後に削除されます。 • CDR と通話ログは 23 か月後に削除されます。ただし、EEA 諸国とスイスでは 6 か月後に削除されます。 • 請求ファイルは 7 年後に削除されます。	本サービスの使用および運用を通じて作成される計測およびロギングシステムにより生成された情報は、シスコのサービス提供、シスコの財務および監査ポリシーの遵守、ならびに税に関する要求事項の記録の一部として保持されます。
ユーザーにより生成される情報	• ユーザーはいつでもボイスメールを削除できます。 • ボイスメールなどのデータは、サービスが終了するかユーザーが無効化されるとすぐに削除されます。 • 通話録音データは 40 日後に削除されます。 • アップロードされたメディアファイルは、サービスが終了するかユーザーが無効化されるとすぐに削除されます。 • テキストメッセージは 400 日後に削除されます。	• 通信記録、テキスト、通信履歴は本サービスを提供するために保持されます。 • お客様は、音声通信記録の組織全体での保持期間を設定できます。 • アップロードされたメディアファイルは、お客様またはユーザーが当該データを削除すると本サービスでも保持されません。

9. 個人データのセキュリティ

シスコは、個人データを偶発的な紛失や不正アクセス、不正使用、改ざん、漏洩から保護するために設計された、適切な技術的、組織的措置を講じています。

本サービスは ISO 27001: 2013 および SOC 2 タイプ I の認証を受けていて、これらの規格に基づき、不正アクセスまたは法律によって要求される情報開示からお客様の個人データを保護するために、技術的および組織的なセキュリティ措置を講じています。本サービスには、NIST 800-53 コントロールファミリーも組み込まれています。これ

は本サービスが、情報および情報システムを保護するために、管理、運用、技術面において均衡のとれた包括的な情報セキュリティプログラムを導入していることを示しています。

当社の Webex Calling 向け暗号化アーキテクチャに関する情報の概要を以下に記載します。Webex App の暗号化アーキテクチャに関する情報は、Webex App および Webex Messaging プライバシーデータシートで確認できます。

個人データのカテゴリ	セキュリティ制御と対策
登録情報	• すべての地域で転送中に暗号化されます。 • すべてのリージョンで保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。
ホストおよび使用状況情報	• すべてのリージョンで転送中および保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。
ユーザーにより生成される情報	• IP デバイスの暗号化サポート状況に応じて、すべての地域で転送中に暗号化されます。 • ボイスメールメッセージ、ボイスメール変換テキスト、FAX メッセージは、すべてのリージョンで保存時に暗号化されます。 • シスコの暗号化キーは、デフォルトで Webex クラウドキー管理システム（KMS）によって保存および管理されます。Pro Pack for Control Hub アドオンを使用しているお客様は、Control Hub 経由で独自の暗号化キーを KMS にアップロードして管理するか、独自のキー管理システム（ハイブリッド データ セキュリティ）とキーを使用するかを選択できます。

本サービスでは、転送中および保管時のデータの保護について、データの種類別にそれぞれ別の暗号化方式を使用します。このセクションでは、「お客様」または「お客様の」はユーザーを指します。

メディア暗号化

お客様がコール中に送信する音声、ビデオ、画面共有データ、通話録音データ、ボイスメールの保護には、メディア暗号化が使用されます。お客様がコールを行うと、お客様のデバイスから当社のサーバーに届くメディアが暗号化されます。メディアは、当社がコールを管理できるよう、当社のサーバーで復号されます。他のコールへの参加者が公衆電話網で接続されるか、暗号化をサポートしていない場合を除き、メディアは他の参加者への送信前に再度暗号化されます。電子メールで送信されるボイスメールおよびボイスメール変換テキストは、状況対応型暗号化を使用します。

トランスポート暗号化

音声およびビデオ通話を除く、本サービスとの間のすべての接続の保護には、トランスポート暗号化（HTTPS とも呼ばれる）が使用されます。

他の制御の仕組み：

- すべてのバックアップは暗号化されます。
- 通話録音ファイルへのアクセスは、最小特権の原則に基づいて制御され、制限されます。
- シスコの従業員、ベンダー、および契約業者はすべて、情報システムにアクセスする前に認証を受けます。
    - シスコ処理システムやサービスの機密性、整合性、可用性、復元力を継続的に確保するために定期的な監査を実施します。

10. 副処理者

当社は、ユーザー生成情報、登録情報、ホスト情報、または使用状況情報を、当社による本サービスの提供と改善に利用することを目的として、他のシスコ事業体またはサービスプロバイダー、契約業者、または他のサードパーティと共有できます。共有データには、集約統計または個別データが含まれる場合があります。すべての情報共有はシスコのプライバシーステートメントに従って行われます。当社は、お客様がシスコに期待できるものと同等レベルのデータ保護および情報セキュリティを提供できるサードパーティのサービスプロバイダーと契約します。当社が、メンバーまたはユーザーの情報を貸与または販売することはありません。個人データにアクセスできるサードパーティのサービスプロバイダーの現在のリストは、要求に応じて提供可能です。

副処理者	個人データ	サービスの種類	データセンターの場所
Amazon Web Services 社	登録情報、ホスト情報、利用情報、ユーザーにより生成されるコンテンツ	データセンターとホスティングプロバイダー	米国 ドイツ オランダ 英国 ブラジル オーストラリア 日本 シンガポール
Dubber 社	登録情報	通話録音クラウドソリューション（お客様が通話録音ソリューションを有効にしている場合のみ）	米国 英国 ドイツ 日本 オーストラリア
Imagicle 社	登録情報	Webex Calling 用アテンダントコンソール（お客様が購入した場合のみ）	米国 カナダ 英国 ドイツ 日本 オーストラリア
LogiSense 社	登録情報、ホスト情報、利用情報	課金ソリューションプロバイダー（お客様が課金サービスを購入している場合のみ）	米国 英国
RedSky 社	登録情報	米国およびカナダの E911 サービスプロバイダー	米国
Tango Networks 社	登録情報、ホスト情報、利用情報	Webex Go/eSIM プロバイダー	米国 英国
Telynx 社	登録情報	Cisco Calling Plan サービスプロバイダー（お客様が Cisco Calling Plan サービスを購入している場合のみ）	米国 英国

11. 情報セキュリティインシデント管理

違反およびインシデントの通知プロセス

シスコのセキュリティ & トラスト部門内の情報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、データ中心のインシデントへの全社的な対応を管理しています。インシデント指揮官が、シスコ プロダクト セキュリティ インシデント レスポンス チーム（PSIRT）、シスコ セキュリティ インシデント レスポンス チーム（CSIRT）、およびアドバンスド セキュリティ イニチアチブ グループ（ASIG）を含む多様なチームを活用して、シスコの対応を指示および調整します。

PSIRT は、シスコ製品およびネットワークに関連する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。PSIRT は、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、およびその他のベンダーと協力して、シスコ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ています。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を詳しく説明しています。

シスコ通知サービスに登録することで、重大度が「緊急」および「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 アドバイザリを含めた、重要なシスコ製品および技術に関する情報を購読し、受け取ることができます。このサービスでは、通知のタイミングおよび通知の配信方法（電子メールメッセージまたは RSS フィード）をお客様が選択できます。情報へのアクセスレベルは、購読者とシスコとの取引関係によって決定されます。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、シスコのセールス担当者にお問い合わせください。

12. 認証およびプライバシー保護法の遵守

セキュリティおよび信頼部門およびシスコ法務部は、リスクおよびコンプライアンスに関する管理ならびにコンサルテーションサービスを提供し、セキュリティおよび規制の遵守をシスコ製品やサービスの設計に組み込むための支援をしています。本サービスは、プライバシーを考慮して構築されており、グローバルなプライバシー要件に準拠した方法で使用できるように設計されています。

さらにシスコは、厳しい社内標準に従うだけでなく、情報セキュリティに対するシスコの取り組みを示すために、第三者機関による検証も受け続けています。本サービスは次の認証を受けています。

- ISO 27001
- SOC 2 Type II
- SOC 3
- HIPAA 構成証明

13. データ主体の権利の行使

本サービスによりご自身の個人データが処理されたユーザーには、本サービスによって処理された個人データに対して、アクセス、是正、処理の中断、または削除を要求する権利があります。

シスコは、要求に対応する前に、ID（通常はシスコアカウントに関連付けられた電子メールアドレス）の確認を依頼します。リクエストに応じることができない場合は、その理由を提示します。ユーザーの雇用主がお客様/管理者である場合は、応答を得るためにユーザーの雇用主にリダイレクトする場合がある点にご注意ください。

リクエストは、次の方法で送信できます。

1）シスコのプライバシー リクエスト フォーム
2）次の宛先に郵送する

個人情報保護管理責任者（CPO） Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas プライバシー責任者 Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	**APJC プライバシー責任者** Cisco Systems, Inc. Bldg. 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	**EMEA プライバシー責任者** Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

シスコは、問い合わせとリクエストにタイムリーかつ十分に対応できるよう努めます。シスコが処理または移転した個人データに関連するプライバシーについての懸念が未解決のままとなっている場合は、シスコの米国を拠点とするサードパーティの紛争解決プロバイダーに問い合わせることができます。または、管轄区域内のデータ保護監督機関に問い合わせて支援を受けることもできます。EU では、シスコはオランダを主たる拠点としています。そのため、EU におけるシスコの関係当局は、Dutch Autoritiet Persoonsgegevens（オランダデータ保護機関）となります。

14. 一般情報

一般的な情報ならびにシスコのセキュリティおよびプライバシープログラムに関連する 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。最新バージョンについては、Cisco Trust Center の「個人データのプライバシー」セクションをご確認ください。

追補 I：Webex Calling 専用インスタンス

本追補では、Webex Calling 専用インスタンスにおける個人データ（または個人を特定できる情報）の処理について説明します。

1. 概要

Webex Calling 専用インスタンスは、シスコとそのリセールパートナーおよびサービスプロバイダー パートナー（以下「パートナー」といいます）が、許可されたユーザー（以下「ユーザー」といいます）のために同サービスを購入する会社（以下「お客様」といいます）に提供する、クラウドベースのビジネス電話サービスです。

Webex Calling 専用インスタンスは、シスコのコール制御エンジンである CUCM（Cisco Unified Communications Manager）が装備された、シスコのクラウド コーリング ポートフォリオの一部です。Webex Calling 専用インスタンスは、シスコ コラボレーション Flex Plan が提供するオファーの一部としてバンドルされています。これらのオファーには、Webex App や Webex Meetings など、市場投入プランと共通サブスクリプションプランを促進するシスコの主要な商用ツールおよび管理ツールが含まれています。

2. 個人データの処理

以下の表には、本サービスがサービスを提供するために利用する個人データおよびそのデータを処理する目的を記載しています。

Webex Calling 専用インスタンスは、以下を行いません。

- 自動化された手段のみをベースとする、データ情報カテゴリの権利に影響を与える法的またはその他の重大な影響をもたらす意思決定。
- お客様の個人データの販売。
- シスコのプラットフォームでの広告配信。
- 広告目的での使用状況やコンテンツのトラッキング。通話トラフィックやコンテンツへの干渉。

お客様が本サービスのユーザーである場合、本追補に記載されている情報は、以下に示すように、お客様、パートナー、シスコがアクセス可能であり、また、本サービスに関連する情報へのアクセス、使用、監視、削除、保存およびエクスポートに関してお客様のポリシーの適用を受けます。シスコは、お客様が他のユーザーと共有した情報のプライバシーをコントロールせず、プライバシーについての責任を負いません。サービスから情報が削除された後でも、ユーザーまたはお客様が他者と共有した範囲内において、情報のコピーが他の場所で閲覧可能な状態になっている場合があります。

以下の表には、本サービスでサービス提供のために利用する個人データと、そのデータを当社が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
登録情報	• 管理者ログイン情報 • 会社または組織の電子メールアドレス • 会社または組織のタイムゾーン • 会社または組織のアカウント ID • 社名または組織名 • 会社または組織の電話番号 • 会社または組織の所在地 • デバイス アクティベーション コード • エンドユーザーのログイン情報 • ログイン ID またはエイリアス ID • SIP 識別子 • ユーザーの電子メールアドレス • ユーザーのプロフィール写真 • ボイスメールボックス番号 • ボイスメールの PIN • 電話番号（携帯、勤務先） • ユーザー名	当社は、登録情報を以下の目的で利用します。 • 本サービスの運用サポートの配信および提供 • サービスのステータスおよび可用性に関するお客様とのやり取り • 他のユーザーへのアイデンティティの表示 • お客様への機能と更新の通知 • 請求関連 • カスタマーコンタクトの有効化、インシデント対応、顧客関係管理 • シスコ マーケティング コミュニケーションの送信 • 本サービスへのアクセスの認証と許可 • 本サービスの提供
ホストおよび使用状況情報	• 実行されたアクション • CallManager 構成 • CallManager データベース • クライアントバージョン • Cookie • デバイス情報 • エンドユーザーの IP アドレス（個人デバイス） • エンドユーザーの MAC アドレス （個人デバイス） • 位置情報 • ログイン時刻 • MAC アドレス（非個人デバイス） • オペレーティングシステム（種類とバージョン） • システムログ • ユーザーエージェント識別子	当社は、ホストおよび使用状況情報を以下の目的で利用します。 • サービスの使用方法の把握 • サポートリクエストへの対応と問題の診断 • 分析の実施と統計分析の集約 • サービスおよびその他のシスコ製品やサービスの改善 • 地理位置情報は、場所を IP phone などのデバイスに割り当て、適切なシスコインフラストラクチャを通じてコールをルーティングするために使用されます。
ユーザーにより生成される情報	• インスタントメッセージ、チャット、会話 • ボイスメッセージ	当社は、ユーザー生成情報を以下の目的で利用します。 異なる場所のユーザーによるコラボレーションを可能にするサービスの提供
システムにより生成される情報	• コールデータのレコード • コールの詳細 • デバイスアクセス情報 •	当社は、システム生成データを以下の目的で利用します。 お客様による課金情報の生成、トラフィック分析の実行、デバイス使用状況の把握を可能にするため
サポート情報	• 連絡先名（姓と名） • お客様のケースの添付書類 • カスタマーサポートチケット番号 • 組織名または社名	当社は、サポート情報を以下の目的で利用します。 • 本サービスの運用サポートの配信および提供 • 技術的問題の診断

お客様は、オンプレミスデバイス（電話など）を通じて、コールログなどの情報を収集することもできます。この情報は、お客様のポリシーに従って管理および保持されます。

3. データセンターの場所

Webex Calling 専用インスタンスは、本サービスを世界中で提供するために、自社のデータセンターだけでなくサードパーティ ホスティング プロバイダーおよびビジネスパートナーを利用しています。これらの事業体は、現在以下の国に所在しています（データセンターの場所は随時変更する可能性があります。変更があった場合、本プライバシーデータシートは更新されます）。

データセンターの場所
アムステルダム（オランダ）
ダラス（テキサス州、米国）
フランクフルト（ドイツ）
ロンドン（英国）
ロサンゼルス（カリフォルニア州、米国）
メルボルン（オーストラリア）
シンガポール（シンガポール）
シドニー（オーストラリア）
東京（日本）
ワシントン D.C.（コロンビア特別区）（米国）

発注プロセス中にパートナーがシスコに提供する情報は、お客様の主たる地理的地域に最も近いデータセンターに保存されます。TAC 情報は、シスコ データセンターに保存されます。情報には、シスコが業務を行っている場所の担当者もアクセスできます。

4. アクセス制御

以下の表には、Webex Calling 専用インスタンスがサービスを提供するために利用する個人データ、当該データへのアクセス権者、アクセスする目的を記載しています。

個人データのカテゴリ	アクセス権者	アクセスする目的
登録情報	エンドユーザーポータルを利用するユーザー	情報の変更、管理、および削除
	Control Hub ポータルを利用するお客様	· お客様のポリシーに従ったユーザーの管理およびサービスの管理 · 情報の変更、管理、および削除
	Control Hub ポータルを利用するパートナー	· 契約条件に従った本サービスのプロビジョニング、請求およびサポート · パートナーは、認証トークンまたはクレデンシャルにアクセスすることはできません

	シスコ	シスコのデータアクセスとセキュリティ管理プロセスに従った本サービスのサポート
ホストおよび使用状況情報	エンドユーザーポータルを利用するユーザー	· やり取りに関する情報と使用履歴の閲覧 · サービス機能の設定および連絡先リストなどの情報の更新
	Control Hub ポータルを利用するお客様	お客様のポリシーに従ったユーザーの管理およびサービスの管理
	Control Hub ポータルを利用するパートナー	契約条件に従った本サービスの請求およびサポート
	シスコ	· シスコのデータアクセスおよびセキュリティ管理プロセスに従った、本サービスの配信、サポートおよび改善 · 詐欺行為の検出および防止
ユーザーにより生成される情報	エンドユーザーポータルを利用するユーザー	ユーザーは、お客様の個人データに関するポリシーに従って、ユーザーが生成または受信したコンテンツのアクセス、変更または削除が可能
	Control Hub ポータルを利用するお客様	機能および電話番号割り当ての変更、制御および削除
	Control Hub ポータルを利用するパートナー	顧客データの抽出要求またはエンドユーザーの監査要求への対応、エンドユーザーの権利の遵守
	シスコ	本サービスのサポートのためにお客様がシスコと共有しない限り、シスコはこのデータにアクセスしません。アクセスする際は、シスコのデータアクセスおよびセキュリティ制御プロセスに従います
システムにより生成される情報	シスコ	サービスの継続的な運用に使用され、ログへのアクセス、デバッグ情報、データのモニタリングが含まれる場合があります
サポート情報	シスコ	サービスの問題を解決するために使用され、ユーザーが作成したチケットおよびユーザーが提供した関連イベントデータへのアクセスが必要です

5. データポータビリティ

個人データは、コール詳細レコード（CDR）を通じて、マシンで読み取り可能な形式で使用できます。お客様は、上記のデータのいずれも、要求をパートナー（シスコに要求を提出しなければなりません）に提出することにより取得できます。データの可用性には、「データの削除および保持」セクションに記載されている削除および保持のポリシーが適用されます。

6. データの削除および保持

お客様は、要求をパートナーに送信することで、本サービス上で保持されている個人データの削除を要求できます。パートナーは TAC リクエストを開いて、シスコに連絡する必要があります。お客様が削除の要求を行った場合、適用法に基づき、またはシスコの正当な事業目的のためにデータの保持が必要でない限り、シスコは要求されたデータを 30 日以内にそのシステムから削除するよう努めます。シスコが特定のカテゴリのデータを保持する必要がある場合、保持の理由および期間は以下の表のとおりです。

個人データのカテゴリ	保持期間	保持する理由
登録情報	• サービス終了後 3 ヵ月以内に削除	シスコの財務デューデリジェンスの一環としてお客様が提供した情報を含め、登録時に収集したデータは、シスコのビジネスレコードを構成し、シスコの財務および監査ポリシー、および税に関する要求事項に従って保持されます。
ホストおよび使用状況情報	• 通信トラフィックデータを含むログファイルは、7 年後またはサービス終了時に削除 • コールの詳細情報は、13 ヵ月後に削除、またはサービス終了時に要求に応じて削除 • その他のホストおよび使用状況に関する情報は、サービス終了後 3 ヵ月以内に削除	本サービスの使用および運用を通じて作成される計測およびロギングシステムにより生成された情報は、シスコのサービス提供、シスコの財務および監査ポリシーの遵守、ならびに税に関する要求事項の記録の一部として保持されます。
ユーザーにより生成される情報	• ユーザーが生成した情報は、お客様またはユーザーの裁量で削除可能 • サービス終了後 3 ヵ月以内に削除	• 記録はサービスを提供するために保持されます • お客様は、音声通信記録の全社的な保持期間を設定することができます
システムにより生成される情報	• トラップとログは 18 ヵ月間、またはサービス終了から 3 ヵ月間保持されます • 診断データは 24 ヵ月間、またはサービス終了から 3 ヵ月間保持されます	• 本サービスの使用および運用中に作成された計測およびロギングシステムが生成する情報は、シスコの運用および監査ポリシーの記録の一部として保持されます。
サポート情報	• チケットと関連イベントは 7 年間保持されます • 標準レポートは最大 3 年間保持されます。	• サポートチケットシステムおよび標準レポートが生成する情報は、シスコのサービス提供および監査ポリシーの記録の一部として保持されます。

7. 個人データのセキュリティ

シスコは、個人データを偶発的な紛失や不正アクセス、不正使用、改ざん、漏洩から保護するために設計された、適切な技術的、組織的措置を講じています。

本サービスは ISO 27001: 2013 および SOC 2 タイプ I の認証を受けていて、これらの規格に基づき、不正アクセスまたは法律によって要求される情報開示からお客様の個人データを保護するために、技術的および組織的なセキュリティ措置を講じています。本サービスには、NIST 800-53 コントロールファミリーも組み込まれています。これは本サービスが、情報および情報システムを保護するために、管理、運用、技術面において均衡のとれた包括的な情報セキュリティプログラムを導入していることを示しています。

当社の Webex Calling 向け暗号化アーキテクチャに関する情報の概要を以下に記載します。Webex App の暗号化アーキテクチャに関する情報は、Webex App および Webex Messenger プライバシーデータシートで確認できます。

個人データのカテゴリ	セキュリティ制御と対策
登録情報	• すべての地域で転送中に暗号化されます。 • すべてのリージョンで保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。
ホストおよび使用状況情報	• すべてのリージョンで転送中および保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。

ユーザーにより生成される情報	• IP デバイスの暗号化サポート状況に応じて、すべての地域で転送中に暗号化されます。 • ボイスメールファイルとテキスト変換ファイルは、すべてのリージョンで保存時に暗号化されます。
システムにより生成される情報	• すべての地域で転送中に暗号化されます。 • すべてのリージョンで保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。
サポート情報	• すべての地域で転送中に暗号化されます。 • すべてのリージョンで保存時に暗号化されます。 • すべての認証パスワードは、暗号化またはハッシュアルゴリズムにより保護されています。

本サービスでは、転送中および保管時のデータの保護について、データの種類別にそれぞれ別の暗号化方式を使用します。このセクションでは、「お客様」または「お客様の」はユーザーを指します。

メディア暗号化

お客様がコール中に送信する音声、ビデオ、画面共有データ、通話録音データ、ボイスメールの保護には、メディア暗号化が使用されます。お客様がコールを行うと、お客様のデバイスから当社のサーバーに届くメディアが暗号化されます。メディアは、当社がコールを管理できるよう、当社のサーバーで復号されます。他のコールへの参加者が公衆電話網で接続されるか、暗号化をサポートしていない場合を除き、メディアは他の参加者への送信前に再度暗号化されます。

トランスポート暗号化

音声およびビデオ通話を除く、本サービスとの間のすべての接続の保護には、トランスポート暗号化（HTTPS とも呼ばれる）が使用されます。

他の制御の仕組み：

- すべてのバックアップは暗号化されます。
- 通話録音ファイルへのアクセスは、最小特権の原則に基づいて制御され、制限されます。
- シスコの従業員、ベンダー、および契約業者はすべて、情報システムにアクセスする前に認証を受けます。
    - シスコ処理システムやサービスの機密性、整合性、可用性、復元力を継続的に確保するために定期的な監査を実施します。

8. サードパーティのサービスプロバイダー（副処理者）

シスコはサプライヤを使用して、マネージドサービスの提供を支援します。シスコのサプライヤ契約では、個人データに関して、シスコとほぼ同レベルのデータ保護と情報セキュリティが求められます。さらに、Webex Calling 専用インスタンスは請負業者を使用して現在のスタッフを増強しています。シスコの請負業者は、ほぼ同様のセキュリティおよびプライバシー管理を提供し、通常、シスコのテクノロジー、ツール、およびプロセスを使用することが求められます。本サービスの副処理者の現行リストを以下に示します。

副処理者	個人データ	サービスタイプと追加のセキュリティ情報	データセンターの場所
ServiceNow 社	お客様の連絡先情報（名前、電話、電子メール）、IP アドレス、デバイス名	運用能力： https://www.servicenow.com/company/trust.html#	グローバル

ScienceLogic 社	IP アドレス、デバイス名	サービスパフォーマンス： https://sciencelogic.com/product/resources/sciencelogic-platform-security-posture	グローバル
Splunk 社	IP アドレス、デバイス名	サービスパフォーマンス： https://www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html	グローバル

9. データ主体の権利の行使

本サービスによりご自身の個人データが処理されたユーザーは、パートナーに連絡して、本サービスによって処理された個人データに対してアクセス、是正、処理の中断、または削除をリクエストすることができます。