



The bridge to possible

データシート  
Cisco Public

# Cisco Registered Envelope Service

プライバシーデータシート

---

# 目次

1. Cisco Registered Envelope Service 機能の概要	3
2. 個人データの処理	3
3. 国境を越えたデータ転送	4
4. アクセス コントロール	4
5. データの削除および保持	5
6. 個人データのセキュリティ	5
7. 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)	6
8. サポートのためにお客様と共有する情報	6
9. 情報セキュリティインシデント管理	6
10. 認定とプライバシー保護法の遵守	7
11. 全般的な情報および GDPR に関する FAQ	7

このプライバシーデータシートでは、Cisco Registered Envelope Service 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 Registered Envelope Service 機能の概要

Cisco Registered Envelope Service（「CRES」）は、お客様の安全な E メールによるコミュニケーションをサポートします。このサービスによって、お客様は登録済みエンベロープを使用して暗号化されたメッセージを送信できます。登録済みエンベロープは、パスワードで保護することもできる暗号化された電子メールです。パスワードによって保護されたエンベロープは、自己の正当性を証明できる認可された受信者のみが開封できます。CRES の詳細については、[https://www.cisco.com/c/ja\\_jp/products/security/registered-envelope-service/index.html?CCID=c000156&DTID=odicdc000016](https://www.cisco.com/c/ja_jp/products/security/registered-envelope-service/index.html?CCID=c000156&DTID=odicdc000016) を参照してください。

CRES は、そのユーザの特定の個人データを処理します。以下に、シスコが CRES 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令に従った安全管理措置を記載します。

## 2. 個人データの処理

以下の表に、CRES がサービスを提供するために利用する個人データと、その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
顧客の連絡先情報	<ul style="list-style-type: none"><li>名前</li><li>電子メールアドレス</li></ul>	<ul style="list-style-type: none"><li>製品の管理：アカウントの作成、ライセンス付与の確認、通常の製品サポートおよび管理。</li></ul>
電子メールエンベロープヘッダー	<ul style="list-style-type: none"><li>送信者</li><li>受信者</li></ul>	<ul style="list-style-type: none"><li>顧客登録とライセンス権限付与の確認</li><li>顧客の問題に関するトラブルシューティング</li></ul>
電子メールデータヘッダー	<ul style="list-style-type: none"><li>差出人</li><li>宛先</li><li>件名</li><li>返信先ヘッダー（CC/BCC を含む）</li><li>添付ファイルの名前/タイトル（添付ファイルの内容ではない）</li></ul>	<ul style="list-style-type: none"><li>差出人、宛先、件名、エンベロープ受信者の識別（例：<a href="mailto:jsmith@company.com">jsmith@company.com</a>）</li><li>顧客の問題に関するトラブルシューティング</li></ul>
暗号化キー	<ul style="list-style-type: none"><li>ユーザごとの一意の暗号化キー</li></ul>	<ul style="list-style-type: none"><li>適切な送信者と受信者が暗号化されたメッセージを開くために使用できる一意のメッセージ ID。</li></ul>
IP アドレス	<ul style="list-style-type: none"><li>エンドユーザのデバイスの IP アドレス</li></ul>	<ul style="list-style-type: none"><li>サービスおよび監査レポートへのユーザセッション接続を維持するために使用</li></ul>
暗号化されたエンベロープ	<ul style="list-style-type: none"><li>暗号化形式の完全な電子メール</li></ul>	<ul style="list-style-type: none"><li>暗号化されたエンベロープの顧客向けクラウドストレージ（オプション。顧客が「Easy Open」機能を有効にしている場合）。シスコではエンベロープを復号化できません。</li></ul>

### 3. 国境を越えたデータ転送

顧客のアカウント情報および CRES によって処理されるデータに関して、クロスボーダー転送が発生します。新しい顧客が CRES サブスクリプションを購入すると、その顧客のアカウント情報は常に米国で作成、処理、保存されます。CRES 製品機能に関連付けられたこの顧客からの、後続のすべてのデータ（電子メールエンベロープヘッダー、電子メールデータヘッダー、暗号キー、IP アドレスデータ、および電子メールストレージが有効になっている場合は暗号化されたエンベロープ）は、CRES が使用するサードパーティのクラウド ホスティング プロバイダーが次のように米国にのみ所在するため、米国で処理されます。

データセンター	説明	場所
Equinix 社	CRES クラウドの Equinix インフラストラクチャは、次の地域で稼働するコロケーション データセンターです。	カリフォルニア（米国）
スイッチ	CRES クラウドのスイッチ インフラストラクチャは、次の地域で稼働するコロケーション データセンターです。	ネバダ（米国）

シスコは、複数の司法管轄区域にまたが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
顧客の連絡先情報	顧客 シスコの従業員 - シスコのセールスマネージャー、ライセンスオペレーター、CRES オペレーターおよびサポートスタッフのみ	製品の管理：アカウントの作成、ライセンス付与の確認、通常の製品サポートおよび管理。
電子メールエンベロープヘッダー、電子メールデータヘッダー	顧客管理者	製品管理、監査、レポート生成
	Cisco Dev オペレーター	CRES の構成とトラブルシューティング、メンテナンス
IP アドレス	Cisco Dev オペレーター	CRES のトラブルシューティングとメンテナンス
暗号化されたエンベロープ暗号化キー	Cisco Dev オペレーター	CRES のトラブルシューティングとメンテナンス

## 5. データの削除および保持

個人データのカテゴリ	保持期間	保持の理由
顧客の連絡先情報	現時点では、削除が要求されるまで保持	管理目的
電子メールエンベロープヘッダー 電子メールデータヘッダー 暗号化キー	10 年	サービス提供 注：お客様は、暗号化キーをロックしたり、暗号化キーを期限切れに設定したりすることができます（たとえば、自動的にキーを期限切れにするポリシーを作成できます）。
IP アドレス	90 日間	監査
暗号化されたエンベロープ	最大 15 日間で設定可能	モバイルデバイスでデバイス上のアプリケーションまたはソフトウェアを必要とせずにエンベロープを開く方法を提供するため。

### 削除

10 年間の保持期間が終了すると、CRES はすべての電子メールエンベロープヘッダー、電子メールデータヘッダー、および暗号化キーを CRES から自動的に消去します。ロックまたは期限切れに設定された暗号化キーは、引き続き 10 年間の削除期間の対象となります。すぐには削除されません。上記にかかわらず、お客様は Cisco TAC リクエストをオープンにして、シスコによる CRES ユーザアカウントの削除を要求することができます。お客様は、監査ログに含まれている IP アドレスを削除できません。CRES は、上記の保持期間の終了後に IP アドレスを消去します。

## 6. 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
顧客の連絡先情報	保管中のデータのディスクレベル (SAN 暗号化) 実行中のデータ (TLS 暗号化)
電子メールエンベロープヘッダー	保管中のデータのディスクレベル (SAN 暗号化) 実行中のデータ (TLS 暗号化)
電子メールデータヘッダー	保管中のデータのディスクレベル (SAN 暗号化) 実行中のデータ (TLS 暗号化)
暗号化されたエンベロープ	保管中のデータ (AES-256 を使用して暗号化されたペイロード) 保管中のデータ (キーサーバに保管されているキーは、暗号化キーとソルトを組み合わせたハッシュ値です)
暗号化キー	保管中のデータのディスクレベル (SAN 暗号化) 実行中のデータ (TLS 暗号化)
IP アドレス	保管中のデータのディスクレベル (SAN 暗号化) 実行中のデータ (TLS 暗号化)

## 7. 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）

シスコは、同レベルのデータ保護を提供する契約を締結しているサードパーティのクラウド ホスティング プロバイダーと提携しています。

副データ処理事業者	個人データ	サービスタイプ	データセンターの場所	セキュリティアシュアランス
Equinix 社	電子メールエンベロープヘッダー 電子メールデータヘッダー 暗号化キー IP アドレス	CRES は、Equinix データセンターを活用して、CRES のグローバル サービス フットプリント、セキュリティアシュアランス、柔軟なサービスおよび耐障害性を提供します。	カリフォルニア (米国)	ISO 27001、SSAE 18 SOC 1 Type II、SOC 2 Type II
スイッチ	電子メールエンベロープヘッダー 電子メールデータヘッダー 暗号化キー IP アドレス	CRES は、スイッチデータセンターを活用して、CRES のグローバル サービス フットプリント、セキュリティアシュアランス、柔軟なサービスおよび耐障害性を提供します。	ネバダ (米国)	SSAE 18 SOC I Type 2、SOC II Type 2

## 8. サポートのためにお客様と共有する情報

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、お客様が提供した個人データを CRES から取得して、処理する場合があります。Cisco TAC のサービス提供に関するプライバシーデータシートには、シスコによる個人データの処理方法が記載されています。シスコは、お客様の問題解決を支援する以外の目的で個人データを処理することはありません。詳細については、TAC Support Essentials Privacy Data Sheet を参照してください。詳細については、[TAC Support Essentials Privacy Data Sheet](#) を参照してください。

## 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：シスコのセキュリティおよびトラスト部門内のデータ保護/プライバシーチームは、データインシデント対応プロセスを調整し、データ中心インシデントに対する全社的な対応を管理しています。インシデント対応リーダーが、Cisco Product Security Incident Response Team (PSIRT)、Cisco Security Incident Response Team (CSIRT)、Advanced Security Initiatives Group (ASIG) などの多様なチームを活用して、シスコの対応を調整して指示します。

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、公表を担っています。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、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 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、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。

シスコ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、以下のプライバシー情報転送メカニズムを活用しています。

- [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](#)

## 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。プライバシーデータシートの最新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。

©2021 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2021 年 6 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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>

お問い合わせ先