# Cisco Intersight® Platform

本プライバシーデータシートでは、Cisco Intersight® Platform（「Intersight」）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。

Intersight は、IT 組織が直感的なユーザーポータルを使用して自社のデータセンターとパブリッククラウド環境を分析、簡素化、自動化できるシステム管理機能を提供します。

シスコは、本プライバシーデータシートに従って Intersight 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、Intersight 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、シスコはデータプロセッサとなります。

Note: 本文書は「Cisco Intersight Platform 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

Intersight は、シスコおよびサードパーティの IT インフラストラクチャ向けの組み込み型分析をお客様に提供します。Cisco Intersight では、従来のツールでは不可能だった高度かつインテリジェントな方法で、IT 組織の環境を分析、簡素化、自動化できます。Intersight は、Cisco UCS®、HyperFlex®、厳選されたサードパーティソリューションと統合し、リモートでの展開、構成、継続的なメンテナンスを可能にします。
Intersight は、ユーザーに関する特定の個人データを処理します。以下のセクションに、シスコ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令に従った安全管理措置を記載します。

本プライバシーデータシートは、インフラストラクチャ サービスを含む Intersight Platform に適用されます。詳細については、Cisco Intersight Platform のオファー説明書を参照してください。本プライバシーデータシートの追補 1 では、 接続済み仮想アプライアンス（CVA）またはプライベート仮想アプライアンス（PVA）の 2 つのモードで運用可能な Intersight 仮想アプライアンスを使用する際の個人データ（または個人を識別できる情報）の処理について説明しています。

Intersight はサードパーティの製品やサービスと統合することもできますが、シスコは、Intersight からシスコ以外の製品やサービスに移行されたお客様データについては責任を負いません。該当するサードパーティシステム内のデータの保護は、各サードパーティの契約およびポリシーによって管理されます。

## 2. 個人データの処理

以下の表には、Intersight がサービスを提供するために処理する個人データと、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[1] | 個人データの種類 | 処理の目的 |
|---|---|---|
| **アカウント情報** | • Cisco.com ID<br>• 氏名<br>• 電子メールアドレス<br>• ユーザ ID | アカウント情報は次の目的で使用されます。<br>• アカウントの作成と製品のアクティベーションの実行<br>• サービスへのログイン[2]<br>• クロスドメイン アイデンティティ管理[3]<br>• カスタマーサポートの提供<br>• 本サービスへのアクセスの認証と承認<br>• 本サービスのステータスと可用性に関する最新情報の提供<br>• オプトインマーケティング/セールス担当者の提供<br>• Intersight 機能のトライアルの有効化 |
| **ユーザーのログイン情報** | • 本サービスの個人ユーザーに紐づく、システムによって生成されたキー | ユーザーのログイン情報は、本サービスへのアクセスの認証と承認の目的で使用されます。 |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック** | • 参加者名<br>• 参加者の電子メール<br>• 参加者がフィードバックのフォローアップを開いているかどうかを示す | 参加者からのフィードバックは、次の目的に使用します。<br>• 製品の改善<br>• カスタマーサポートの提供<br>• 製品のバグの特定および解決<br>• 参加者のフィードバックのフォローアップ |

以下の表のデータは、個人のアカウントに関連付けられていることが理由で個人データとなっている可能性がありますが、ほとんどの場合、データセンターまたはエッジロケーションのサーバー、ストレージシステム、スイッチ、およびネットワーク管理システムにのみ関連付けられ、個人のデバイスに接続はされません。

| データカテゴリ[1] | データの種類 | 処理の目的 |
|---|---|---|
| **インベントリおよび設定データ** | • 設定データ<br>  ○ ハードウェアインベントリ<br>  ○ ファームウェアインベントリ<br>  ○ ユーザーラベル<br>  ○ IP アドレス<br>  ○ ドメイン名<br>  ○ サーバー設定インベントリ<br>  ○ ワークフローの設定<br>  ○ ワークフローログ<br>  ○ ライセンスデータ<br>  ○ 設定ポリシー<br>  ○ API キー、OAuth2 トークン<br>  ○ OS ソフトウェアイメージのメタデータ<br>  ○ イベントおよびアラーム | インベントリと設定情報を使用して、次のことを行います。<br>• サービスと関連機能の提供<br>• サービスのサポート契約<br>• テクニカルサポートの提供<br>• サービスが要求するサーバー上の一般的な脆弱性の検出<br>• サービスの使用方法の把握 |

[1] お客様が他のアプリケーションを統合する場合、追加の個人データが処理される場合があります。

[2] お客様がシングルサインオンまたはアイデンティティ プロバイダー サービスを利用する場合、アカウントへのログインのために処理される個人データは異なる場合があります。

[3] お客様が SCIM（System for Cross-domain Identity Management）の使用を有効にしている場合、SCIM に関連する個人データは米国で処理されます。

| | | |
|---|---|---|
| | • サーバーサービス契約<br>○ 請求先住所と配送先住所<br>○ PO 番号<br>○ 契約範囲<br>保証に関する情報 | |
| **ホストおよび使用状況に関する情報** | • ホストのプロビジョニングデータ<br>○ OS のバージョン<br>○ IP アドレス<br>○ ドライバのバージョン<br>○ サーバーのバージョン<br>○ デバイス識別子<br>• テクニカルサポートバンドル | 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。<br>• サービスの使用方法の把握<br>• 技術的問題の診断<br>• サービスの技術的パフォーマンスおよび使いやすさを向上させるための統計的および技術的分析の実施<br>• クライアント エクスペリエンスの最適化の支援 |

Intersight ユーザーは、ファイル経由で直接、またはオーケストレータ統合（ISCD など）を介して識別タグをアップロードでき、Intersight API を使用して Intersight とシスコやサードパーティ アプリケーションを統合することもできます。管理者/Intersight ユーザーがタグ内に個人データ（たとえば、資産に関連付けられている個人の名前、IP アドレス、またはプロセス）を追加することは可能ですが、お勧めできません。Intersight アプリケーション、API、またはその他の統合を使用して、Intersight は追加の個人識別情報を組み込んで処理することができます。

### テクニカルサポートの支援

お客様が問題の診断と解決のために Cisco Technical Assistance Center（TAC）に連絡した場合、Cisco TACは Intersight 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 には、シスコによる個人データの処理について記載されています。Cisco TAC はグローバルサービスとして、トラブルシューティングと分析のためにお客様のテクニカルサポートデータを別の地域に移動することが必要になる場合があります。テクニカルサポートに関する Intersight のデフォルト設定では、インシデント情報の収集が許可されています。これを無効にするには、Disabling Tech Support Bundle Collection [英語] を参照してください。この設定はアカウント管理者のみが変更できます。

## 3. データセンターの場所

お客様は、Intersight アカウントの作成時に地理的リージョン（米国または欧州連合）を選択する必要があります。アカウントのリージョンは、管理対象デバイス（要求されたターゲットとも呼ばれます）からのデータをシスコが保存する場所を決定します。これらのデバイスがそのリージョン外にある場合でも、その場所に保存されます。ただし、シスコは、米国にある要求されていないすべてのデバイスからのインベントリデータと構成データ（上記のセクション 2 の表を参照）を保存します。欧州連合リージョンを選択したお客様が Intersight による管理のためにデバイスを要求すると、シスコはそのデバイスのデータを米国のデータセンターから削除します（インベントリデータと構成データはその後 EU のデータセンターで処理されます）。シスコは、削除されたデータをバックアップシステムに最大 30 日間保持します。お客様の情報（お客様に代わって、製品を調達し管理するためにシスコと連絡を取っている従業員に関連するデータと、お客様にシスコがサービスを提供することによって処理されたデータ）は、そのアカウントのリージョンに保管されます。暗号化されたカスタマーフィードバックは、世界中にあるシスコのデータセンターに保存される場合があります。上記のセクション 2 の脚注 3 に記載のとおり、お客様が SCIM を有効にした場合、シスコはそのアカウント情報を米国で処理します（EU を選択したお客様の場合も同様です）。

# 4. 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移転メカニズムに投資しています。

- 拘束的企業準則（管理者） [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]

シスコは、Intersight SaaS プラットフォームに代わるオンプレミスソフトウェア仮想アプライアンスも提供しており、お客様のデータセンター内でほとんどの Intersight 機能を実装できます。Intersight 仮想アプライアンスのデータ処理に関する情報については、本プライバシーデータシートの追補 1 を参照してください。

# 5. アクセス制御

次の表には、Intersight 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、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 | アクセス権者 | アクセスする目的 |
|---|---|---|
| **アカウント情報** | Cisco Intersight サポートチーム | • サービスのサポートと製品の改善 |
| | 顧客 | • 個人データの使用に関する個々のお客様ポリシーに基づく |
| **ユーザーのログイン情報** | お客様 | • 本サービスへのアクセスの認証と承認 |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック** | シスコのエンジニアとサポートスタッフの限定グループ | • 参加者の回答への応答。技術的な問題を診断し、統計的および技術的な分析を実施して、サービスの使いやすさおよび技術的パフォーマンスを向上させる |
| **インベントリおよび設定データ** | シスコのエンジニア、サポートスタッフ、およびライセンス運用の制限付きグループ | • ライセンス付与を検証し、通常の製品サポートと運用を提供する |
| | 顧客 | • 製品の管理と運用 |
| **ホストおよび使用状況情報** | シスコのエンジニアとサポートスタッフの限定グループ | • 技術的な問題を診断し、統計的および技術的な分析を実施して、サービスの使いやすさおよび技術的パフォーマンスを向上させる |

# 6. データポータビリティ

データポータビリティ要件は、Intersight には適用されません。

# 7. データの削除と保持

次の表には、Intersight 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。

| 個人データの種類 | 保持期間 | 保持する理由 |
|---|---|---|
| **アカウント情報およびユーザーのログイン情報** | • Intersight アカウントが有効である限り、アカウント情報およびユーザーのログイン情報は、Intersight アカウントの削除後最大 30 日間保持されます | • アカウントの作成、製品の有効化、製品の使用状況の通知、トレーニング、サポート。お客様のライセンスの記録保持 |
| **インベントリおよび設定データ** | • Intersight アカウントが有効である限り、インベントリおよび設定データは、Intersight アカウントの削除後最大 30 日間保持されます | • 製品の機能と推奨事項<br>• アカウントを再作成する場合のお客様のサポート |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック** | • Intersight アカウントが有効である限り、カスタマー フィードバック データは、Intersight アカウントの削除後最大 30 日間保持されます | • 製品の機能と推奨事項<br>• カスタマーサポートの提供<br>• 製品のバグの特定および解決<br>• 参加者のフィードバックのフォローアップ |
| **ホストおよび使用状況情報** | • セッション情報を除き、Intersight アカウントが有効である限り、ホストおよび使用状況の情報は、Intersight アカウントの削除後最大 30 日間保持されます | サービスの技術的パフォーマンスを向上させるための統計的および技術的分析の実施 |
| **FullStory 内に保存されるセッション情報*** | • FullStory と共有されるセッション情報は、最長 2 年間保持されます | • 製品の機能と推奨事項<br>• バグの特定および解決など、製品の改善支援 |
| *** 地理的リージョンとして EU を選択したお客様のデータは、FullStory と共有されることも、FullStory によって処理されることもありません。** | | |

# 8. 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。

以下に、シスコの暗号化アーキテクチャに関する追加情報を示します。

| 個人データのカテゴリ | セキュリティ制御と対策 |
|---|---|
| **アカウント情報** | 移送中および保管中に暗号化します |
| **ユーザーのログイン情報** | 移送中および保管中に暗号化します |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック** | ブロックおよびオブジェクトデータストア内の転送中および保管中の暗号化 |
| **インベントリおよび設定データ** | ブロックおよびオブジェクトデータストア内の転送中および保管中の暗号化 |
| **ホストおよび使用状況情報** | ブロックおよびオブジェクトデータストア内の転送中および保管中の暗号化 |

# 9. 副処理者

Intersight は、個人データの副処理者としてサービスプロバイダーを利用します。その際、サービスプロバイダーとの契約において、シスコが提供するのと同じレベルのデータ保護機能を提供し、情報セキュリティを確保することを確約させます。現在の副処理者のリストを以下に示します。副処理者は随時変更される場合があります。その際には、変更を反映して本プライバシーデータシートは更新されます。

| 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 | 上記のセクション 2 のすべてのデータカテゴリ。転送中および保存中は暗号化されます。 | インフラストラクチャ プロバイダー | 米国、ドイツ |
| Sentry.io** | アカウント、ホスト、および使用状況の情報。転送中および保存中は暗号化されます。 | エラーの追跡およびサポート | 米国 |
| FullStory** | アカウント、ホスト、および使用状況の情報。転送中および保存中は暗号化されます。 | サポート | 米国 |

*** シスコが暗号化キーを管理しています。**
**** 地理的リージョンとして EU を選択したお客様については、Sentry.io も FullStory も副処理者して機能しません。**

# 10. 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。

## 11. 認証およびプライバシー要件の遵守

セキュリティ & トラスト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。Intersight は、次の認定を受けています。

- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- SOC 2 Type 2、SOC 3
- CSA CSTAR Level 1
- FIPS 140-2 準拠

## 12. 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

<table>
<tr><td colspan="3">個人情報保護管理責任者（CPO）<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES</td></tr>
<tr><td>Americas プライバシー責任者<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES</td><td>APJC プライバシー責任者<br>Cisco Systems, Inc.<br>Bldg 80, Lvl 25, Mapletree Biz City,<br>80 Pasir Panjang Road,<br>Singapore, 117372<br>SINGAPORE</td><td>EMEA プライバシー責任者<br>Cisco Systems, Inc.<br>Haarlerbergweg 13-19, 1101<br>CH Amsterdam-Zuidoost<br>NETHERLANDS</td></tr>
</table>

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関する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 における主たる監督機関は、Dutch Autoritiet Persoonsgegevens（オランダデータ保護機関）となります。

## 13. 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 1：Intersight 仮想アプライアンス

本追補では、接続済み仮想アプライアンス（「CVA」）またはプライベート仮想アプライアンス（「PVA」）の 2 つのモードで運用可能な Intersight 仮想アプライアンスを使用する際の個人データ（または個人を識別できる情報）の処理について説明しています。

Cisco Intersight Platform プライバシーデータシートの本追補 1 は、シスコのオンライン プライバシー ステートメントを補足するものです。

## 1. Intersight 仮想アプライアンスの概要

Cisco Intersight 仮想アプライアンスでは、展開が容易な VMware OVA、Microsoft Hyper-V Server VM および Linux の KVM ハイパーバイザで Intersight の管理機能が提供されるため、自社に残すシステムの詳細を制御できます。仮想アプライアンスのフォームファクタによって、intersight.com が完全には満たしていない追加データの局所性、セキュリティ、またはコンプライアンスのニーズに対応します。

CVA は、Intersight の管理機能を提供し、どのシステムの詳細を自社に残すかを制御することを可能にします。CVA の展開では、自動更新および全機能の利用に必要なサービスへのアクセスのため、シスコおよび Intersight サービスに接続する必要があります。

PVA は、Intersight の管理機能を提供します。PVA はシスコに接続することなく動作するため、システムの詳細を自社から持ち出さずに済みます。PVA では https://intersight.com でアプライアンスアカウントを作成する必要があります。以下および上記の Cisco Intersight Platform プライバシーデータシートに記載されているように、PVA と CVA の両方において、アプライアンスアカウントは一部のデータを処理します。ユーザーが手動更新を選択した場合、CVA はアプライアンスアカウントを使用することもあります。

## 2. 個人データの処理と仮想アプライアンス

お客様が CVA を使用する場合、接続モードで動作し、ホストされている Intersight サービスに接続する必要があります。以下の表には、アプライアンスアカウントの作成時、CVA の自動更新時および Intersight.com のサービスへのアクセス時に Intersight が処理する個人データと、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[4] | 個人データの種類 | 処理の目的 |
|---|---|---|
| **アカウント情報** | • Cisco.com ID<br>• 氏名<br>• 電子メールアドレス<br>• ユーザ ID<br>• ユーザーのログイン情報 | アカウント情報は次の目的で使用されます。<br>• SaaS アカウントを作成し、製品のアクティベーションを実行して、アプライアンスを SaaS アカウントに要求する<br>• サービスへのログイン[5]<br>• クロスドメイン アイデンティティ管理[6]<br>• SaaS アカウントへのアクセスの認証および承認<br>• カスタマーサポートの提供 |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック[7]** | • 参加者名<br>• 参加者の電子メール<br>• 参加者がフィードバックのフォローアップを開いているかどうかを示す | 参加者からのフィードバックは、次の目的に使用します。<br>• 製品の改善<br>• カスタマーサポートの提供<br>• 製品のバグの特定および解決<br>• 参加者のフィードバックのフォローアップ |

PVA と CVA の両方の更新バンドルをダウンロードすると、Intersight は、上記の表に記載されている目的で使用されるアカウント情報を収集します。Intersight は、ダウンロードを記録する監査ログも保持します。

以下の表のデータは、CVA の展開により共有される場合があり、個人のアカウントに関連付けられていることが理由で個人データとなっている可能性がありますが、ほとんどの場合、データセンターまたはエッジロケーションのサーバー、ストレージシステム、およびネットワーク管理システムにのみ関連付けられ、個人のデバイスに接続はされません。

[4] お客様が他のアプリケーションを統合する場合、追加の個人データが処理される場合があります。

[5] お客様がシングルサインオンまたはアイデンティティ プロバイダー サービスを利用する場合、アカウントへのログインのために処理される個人データは異なる場合があります。

[6] お客様が SCIM（System for Cross-domain Identity Management）の使用を有効にしている場合、SCIM に関連する個人データは米国で処理されます。

[7] データは、お客様によって有効化された場合、またはテクニカルサポートを提供するために必要な場合に、特定のケースでのみ収集されます。

| データカテゴリ[4] | データの種類 | 処理の目的 |
|---|---|---|
| **インベントリおよび設定データ** | アプライアンスデータ<br>○ アプライアンス ID（シリアル番号）<br>○ アプライアンスの IP アドレス<br>○ アプライアンスのホスト名<br>○ アプライアンス上のデバイスコネクタのバージョンと公開キー<br><br>エンドポイントデータ<br>○ シリアル番号と PID（Connected TAC に対応するため）<br>○ UCS ドメイン ID<br>○ プラットフォームタイプ<br><br>○ エンドポイント ターゲット タイプ：Cisco UCS ファブリック インターコネクト、統合管理コントローラ、Cisco HyperFlex System[7]<br>○ ファームウェアバージョン[7]<br>○ IP アドレス[7]<br>○ ドメイン名[7]<br>○ ホスト名[7]<br>○ ワークフローログ[7]<br>○ デバイスコネクタのバージョンと公開キー[7] | エンドポイントターゲットに関する情報は次の目的で使用されます。<br>• テクニカルサポートの提供<br>• プロアクティブな RMA の提供<br>• デバイスコネクタのバージョン、公開キー、および以下の # の付いたその他のデータは、デバイスコネクタのバージョンがサポート対象外の可能性があるデバイスをアップグレードする目的で使用されます。 |
| **ホストおよび使用状況情報** | • データのモニタリング<br>○ アラーム[7]<br>○ アプライアンスの正常性に関するデータ<br>○ アプライアンスの CPU 使用率<br>○ アプライアンスのメモリ使用率<br>○ アプライアンスのディスク使用率<br>○ サービスの統計情報<br>• テクニカルサポートバンドル[7] | 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。<br>• 技術的問題の診断<br>• テクニカルサポートの提供<br>• プロアクティブな RMA の提供 |

# 3. データセンターの場所と仮想アプライアンス

仮想アプライアンスのユーザーが Intersight にアクセスすると、お客様の情報は、上記の Intersight プライバシーデータシートのセクション 3 に記載されているとおりに保存されます。

# 4. 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移転メカニズムに投資しています。

- 拘束的企業準則（管理者） [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]

# 5. 仮想アプライアンスのアクセス制御

本追補 1 の上記のセクション 2 に記載されている Intersight が収集する個人データは、上記の Intersight プライバシー データシートの本文のセクション 5 に記載されている表に定められたとおりに使用およびアクセスされます。

# 6. データポータビリティ

データポータビリティ要件は、Intersight 仮想アプライアンスには適用されません。

# 7. データの削除と保持

本追補 1 の上記のセクション 2 に記載されている Intersight が収集する個人データは、以下の表に記載されているとおりに保持および使用されます。

| 個人データの種類 | 保持期間 | 保持する理由 |
|---|---|---|
| **アカウント情報およびユーザーのログイン情報** | • Intersight アカウントが有効である限り、アカウント情報およびユーザーのログイン情報は、Intersight アカウントの削除後最大 30 日間保持されます | アカウントの作成、製品の有効化、製品の使用状況の通知、トレーニング、サポート。お客様のライセンスの記録保持 |
| **インベントリおよび設定データ**<br><br>**（CVA のみ）** | • Intersight アカウントが有効である限り、インベントリおよび設定データは、Intersight アカウントの削除後最大 30 日間保持されます | • 製品の機能と推奨事項 |
| **Intersight を使用して個人（「参加者」）から寄せられたカスタマーフィードバック** | • Intersight アカウントが有効である限り、カスタマー フィードバック データは、Intersight アカウントの削除後最大 30 日間保持されます | • 製品の機能と推奨事項<br>• カスタマーサポートの提供<br>• 製品のバグの特定および解決<br>• 参加者のフィードバックのフォローアップ |
| **ホストおよび使用状況情報**<br><br>**（CVA のみ）** | • Intersight アカウントが有効である限り、ホストおよび使用状況の情報は、Intersight アカウントの削除後最大 30 日間保持されます | サービスの技術的パフォーマンスを向上させるための統計的および技術的分析の実施 |

# 8. Intersight.com の仮想アプライアンスデータにおける個人データのセキュリティ

シスコは、本追補 1 の上記のセクション 2 に記載されている Intersight が収集する個人データについて、上記の Intersight プライバシー データシートの本文のセクション 8 に記載されている表のとおりに、適切な技術的および組織的措置を実施しています。

# 9. Intersight.com の仮想アプライアンスデータの副処理者

Intersight 仮想アプライアンスは、個人データの副処理者としてサービスプロバイダーを利用します。その際、サービスプロバイダーとの契約において、シスコが提供するのと同じレベルのデータ保護機能を提供し、情報セキュリティを確保することを確約させます。現在の副処理者のリストを以下に示します。副処理者は随時変更される場合があります。その際には、変更を反映して本プライバシーデータシートは更新されます。

| 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 | 上記のセクション 2 のすべてのデータカテゴリ。転送中および保存中は暗号化されます。* | インフラストラクチャ プロバイダー | 米国、ドイツ |
| *** シスコが暗号化キーを管理しています。** | | | |

# 10. 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**

本プライバシーデータシートの上記の本文に記載されているとおり、侵害およびインシデントの通知プロセスは、Intersight の通知プロセスと同等です。

# 11. 認証およびプライバシー要件の遵守

セキュリティ & トラスト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。仮想アプライアンスは、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い、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。

# 12. 仮想アプライアンスに関するデータ主体の権利の行使

上記のセクション 2 に記載されているとおり、Intersight によって個人データを収集された仮想アプライアンスユーザーは、その個人データへのアクセス、修正、処理の停止、または削除を要求する権利を有します。

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）**<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES | | |
| **Americas プライバシー責任者**<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES | **APJC プライバシー責任者**<br>Cisco Systems, Inc.<br>Bldg 80, Lvl 25, Mapletree Biz City,<br>80 Pasir Panjang Road,<br>Singapore, 117372<br>SINGAPORE | **EMEA プライバシー責任者**<br>Cisco Systems, Inc.<br>Haarlerbergweg 13-19, 1101<br>CH Amsterdam-Zuidoost<br>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関する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 における主たる監督機関は、Dutch Autoritiet Persoonsgegevens（オランダデータ保護機関）となります。

## 13. 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。