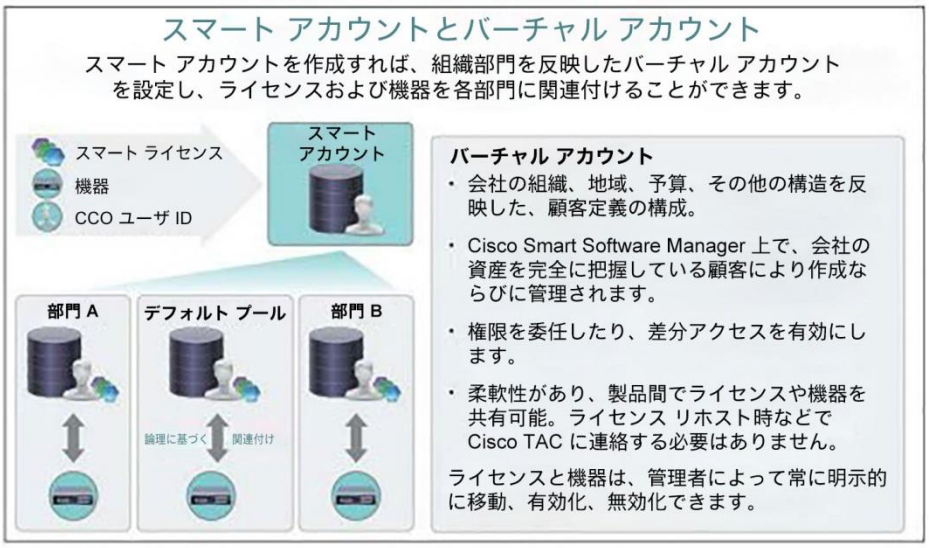
スマート ソフトウェア ライセンス ツールとスマート アカウント管理

このプライバシー データ シートでは、スマート ソフトウェア ライセンス ツールとスマート アカウント管理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. シスコ スマートアカウント機能の概要

シスコ スマート アカウントは、お客様がソフトウェア ライセンスの資産管理に費やす時間を節約できる新しい方法です。Cisco.com のアカウントから、組織全体のシスコ ソフトウェアのライセンスおよび使用権を把握し、管理できます（図1）。スマート アカウントの導入以前は、使用権を把握するのに個別のシスコ ID が必要でした。このため、組織全体でライセンスを把握し、管理する手段が限られていました。



スマート アカウントは、CSSM、LRP、CCW、Software Central を含む複数のツールで利用できます。スマート ソフトウェア ライセンスおよびスマート アカウント管理には以下の機能が含まれています。

1. Software Central（software.cisco.com）：お客様向けポータル。製品のダウンロードとアップグレードの管理、注文、EULA ツール/スマート ソフトウェア ライセンス ツール/スマート アカウント管理へのアクセスを実行できます。
2. License Registration Portal（LRP）：PAK またはその他のレガシー ライセンスにアクセスして管理/使用するメイン サイト。
3. Cisco Commerce Workspace（CCW）：シスコ製品を調達する際のメイン サイト。

2. 個人データの処理

以下の表には、シスコ スマート アカウントがサービスを提供するために利用する個人データの一覧と、シスコが各データを処理する理由を記載しています。

個人データのカテゴリ	個人データの種類	処理の目的
お客様の連絡先の詳細	• 名/姓 • 電子メール アドレス • CCO ユーザ ID • ロール	• アカウントの作成と管理
お客様のアカウントの詳細	該当なし	• 特定のお客様/アカウントに資産を関連付ける
発注情報	該当なし	• 発注のトレーサビリティ • アカウント/お客様が適切なレベルのアクセス権を持っていることを確認する
機器情報	• IP アドレス • ホスト名（オプトアウト可能）	• 発注のトレーサビリティ • アカウント/お客様が適切なレベルのアクセス権を持っていることを確認する

3. データ取り込みプロセス

シスコでは、ソフトウェアの所有権と使用状況に関する情報を提供するソフトウェア インベントリ管理システム、Cisco Smart Software Manager（CSSM）を使用しています。これには、ローカルでソフトウェア インベントリを収集し、その情報を CSSM に送信する Smart Software Manager サテライト（CSSM）も含まれます。

4. 国を跨ぐデータ転送

データは、米国カリフォルニア州のシスコ データセンターでホストおよび管理されます。データはローカル サイトで収集/生成できますが、実稼働インスタンスはカリフォルニア州サンノゼのシスコ データセンターでホストされています。シスコの IT 部門は、レプリケーションおよびシスコ社内の担当者によるデータ アクセスに関連するガバナンスに従っています。すべてのレプリケーション サイトは米国内にあります。

シスコは、複数の司法管轄区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転送メカニズムに投資しています。特に、次の点に注意してください。

- 拘束力のある企業ルール
- EU-米国間のプライバシー シールド フレームワーク[英語]
- スイス-米国間のプライバシー シールド フレームワーク[英語]

- APEC クロスボーダー プライバシー ルール [英語]
- EU 標準契約条項

5. アクセス制御

アクセスの方法は最小特権アクセスの原則に従います。アクセス権は、次のロールを使って付与されます。

- スマート アカウント ユーザ：すべてのバーチャル アカウント内の資産を管理できますが、バーチャル アカウントの追加や削除、ユーザ アクセスの管理はできません。
- スマート アカウント管理者：スマート アカウントとそのバーチャル アカウントの全般（ユーザを含む）を管理します。
- スマート アカウント承認者：アカウント所有者に代わって、ライセンス契約の承認のみできます。ロールの追加や使用権とライセンスの関連付けなど、ユーザまたは管理者の権限は含まれません。
- バーチャル アカウントは、お客様が使用権とライセンスを分離するために使えるデフォルトのサブアカウント/コンテナです。バーチャル アカウントはお客様が管理します。お客様の使用権と資産は、バーチャル アカウントのレベルで定義して分離します。
- バーチャル アカウント ユーザ:使用権管理のすべてを実行できますが、ロールを割り当てることはできません。
- バーチャル アカウント管理者：他のユーザにロールを割り当てることができます。範囲はバーチャル アカウントに制限されます。

スマート アカウント管理者の連絡先情報は、同じ組織の従業員とのみ共有されます。シスコ以外の社外の関係者には共有されません（お客様が要求した場合を除く）。スマート アカウントへのアクセス権がないパートナーがアクセス権を得たい場合やスマート アカウント管理者に連絡したい場合は、software.cisco.com にある Smart Account Request Access ツールを利用できます。すべてのスマート アカウント管理者にメッセージが送信されますが、依頼者に管理者の名前は開示されません。

CSSM サテライト アカウント：これらのアカウントにより、お客様は企業 ID とアクセス フェデレーションを使うアクセス制御を統合できるようになります。これは CCO ID 認証に基づくものではなく、お客様の ID とアクセス管理に基づいたローカル認証を使用します。

個人データへのアクセスは次のように制御されます。

- シスコの IT 部門は、レプリケーションおよびシスコ社内の担当者によるデータ アクセスに関連するガバナンスに従っています。
- シスコの内部データの分類、ガバナンス、ポリシーに従い、シスコのユーザは、スマート アカウント プラットフォームへのアクセス権の再検証を定期的に受ける必要があります。
- お客様は、それぞれのスマート アカウント データを選択した誰とでも共有できますが、追加のサード パーティは明示的に追加する必要があります。また、お客様が明示的に要求しない限り、シスコがサード パーティ

と情報を共有することはありません。

6. データ ポータビリティ

お客様（管理者またはユーザ）は、アクセス権を持つデータをエクスポートできます。これには、スマート アカウント プラットフォームで利用できるレポート機能を使います。データ保護で追加のサポートが必要な場合は、privacy@cisco.com に問い合わせるか、TAC サポート リクエストをオープンします。シスコは、アクセス制御の観点からリクエストを検証するために必要なデュー デリジェンスを実施します。

7. データの削除および保持

ユーザ レベルの情報は、スマート アカウント管理者が特定のスマート アカウントからユーザを削除した直後に非アクティブになります。ユーザ レベルの情報（非アクティブ化の後）とユーザ イベント ログは、標準的なシスコのデータ保持および削除のプラクティスに従って管理されます。

スマート アカウント名はお客様固有の資産と使用権に関連付けられているため、シスコによって削除されません。この関連付けはお客様が所有します。このデータをシスコが削除することはありません。

8. 個人データのセキュリティ

スマート ソフトウェア ライセンスとスマート アカウントは、業界標準に従った、法律で求められている技術的および組織的なセキュリティ対策を採用しています。これらは個人データを不正なアクセス、使用、開示から保護するように設計されています。さらに、データは米国カリフォルニア州のシスコのデータセンターでホストされており、データ セキュリティと脆弱性に関するレビューを受け、ベスト プラクティスとコントロールが正しく実施されていることが確認されます。

当社の暗号化アーキテクチャに関する追加情報は、下記の表や次項以降のとおりです。

個人データのカテゴリ	暗号化のタイプ
お客様の連絡先の詳細	保管中ではなく移送中に暗号化（保管中のデータを保護する方法は上記を参照）
お客様のアカウントの詳細	保管中ではなく移送中に暗号化（保管中のデータを保護する方法は上記を参照）
発注情報	保管中ではなく移送中に暗号化（保管中のデータを保護する方法は上記を参照）
機器情報	保管中ではなく移送中に暗号化（保管中のデータを保護する方法は上記を参照）

9. サード パーティのサービス プロバイダー（副処理者）

シスコは登録情報、ホストおよび使用状況情報、ユーザ生成情報を、どのサードパーティ サービス プロバイダーにも送信することなく本サービスを提供します。

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

シスコの Security & Trust Organization 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 インシデント対応チーム（PSIRT）、シスコ セキュリティ インシデント対応チーム（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。

Cisco Notification Service に登録することで、重要度が「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、お客様の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保護法の遵守

セキュリティ & トラスト部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。シスコおよびその基になるプロセスは、EU 一般データ保護規則および世界中の他のプライバシー保護法上のシスコの義務を満たすように設計されています。

シスコは複数の管轄区域における合法的なデータの利用に関連する、以下のプライバシー転送メカニズムを活用しています。

- 拘束力のある企業ルール
- EU-米国間のプライバシー シールド フレームワーク [英語]
- スイス-米国間のプライバシー シールド フレームワーク [英語]
- APEC クロスボーダー プライバシー ルール [英語]
- EU 標準契約条項

厳しい社内標準に従うことに加えて、シスコはまた、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、サードパーティによる検証も継続的に行っています。シスコ サービスは、次の認証を受けています。

- ISO 27001

12. 一般情報と GDPR に関する FAQ

スマート アカウントにより、お客様はそれぞれの資産と使用権をどのように管理して保護できますか。
シスコ スマート アカウントは、管理するソフトウェア ライセンスの資産管理にお客様が費やす時間を節約できる新しい方法です。Cisco.com Web サイトのアカウントから、組織全体のシスコ ソフトウェアのライセンスおよび使用権を把握して管理できます。スマート アカウントの導入以前は、使用権を把握するのに個別のシスコ ID が必要でした。このため、組織全体でライセンスを把握し、管理する手段が限られていました。スマートアカウントを開設すると、組織内の部門、地域、または拠点ごとのライセンス管理に役立つサブアカウント（バーチャル アカウント）を柔軟に作成できます。ライセンスは、必要に応じてバーチャル アカウント内でプールすることができます。スマート アカウントでは、ロールベースのユーザ アクセス制御をサポートしています。これにより、スマート アカウント レベルまたはバーチャル アカウント レベルで、アカウント管理者に権限を委任できます。さらに、バーチャル アカウントまたはエンタープライズレベル アカウントに対するパートナーの可視性と管理権限を管理できます。
https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/smart-software-manager-satellite/at-a-glance-c45-734361.pdf

スマート アカウントのライセンスと使用権には組織内の複数の個人がアクセスできますか。
はい。スマート アカウントには必要な数の管理者またはユーザを追加できます。各ユーザまたは管理者は、必要に応じて、スマート アカウント全体または個々のバーチャル アカウント（スマート アカウント フォルダ）のいずれかにアクセスできます。追加のユーザは、スマート アカウントのセットアップ時に定義することも、software.cisco.com で「Manage my Smart Account」アプリケーションから定義することもできます。

パートナーは、権限付与後に顧客のスマート アカウントを確認またはアクセスできますか。
パートナーやシステム インテグレータなどのサード パーティは、お客様からスマート アカウント全体、またはお客様が指定したバーチャル アカウント（スマート アカウント フォルダ）のいずれかへのアクセス権が提供されている場合のみ、お客様のスマート アカウントにアクセスのみできます。スマート アカウントでは、それぞれのスマート アカウントに対する完全なアクセス権をパートナーに簡単に提供できます。スマート アカウントの初期セットアップ時に、または software.cisco.com で「Manage my Smart Account」アプリケーションを開いた際に、パートナーの連絡先を承認ユーザのリストに追加します。

顧客が 2 つの異なるパートナーから多数のライセンスを購入してスマート アカウントに配布した場合、パートナーはスマート アカウントにある使用権の総数を確認できますか。
確認できるようにするかどうかはお客様がコントロールできます。お客様は、両方のパートナーにスマート アカウント全体へのアクセス権を付与することも、各パートナーに一部のアクセス権のみを付与することもできます。

シスコのセキュリティ コンプライアンス プログラムおよび GDPR の準備に関連する一般情報ならびに FAQ（よくある質問）については、Cisco Trust Center をご確認ください。