Secure Cloud AnalyticsからCisco XDRへの移行

内容

主な変更点

Secure Cloud Analyticsのユーザエクスペリエンスは、2026年10月24日に提供を終了します。Cisco XDRは、SCA由来の検出、調査、資産コンテキスト、通知、エクスポート、および関連するワークフローの運用インターフェイスとなります。

⚠ 注意：専用のSCA-to-XDRカスタマー移行プログラムは9月30日に終了する予定ですが、2026年10月24日はSCAユーザインターフェイスの推奨を取り消す計画の目標期日のままです。Cisco XDRを今すぐ有効化して、以下に説明する準備作業を完了してください。

緊急措置と重要な日付

何が起こっているのか、そして私は今何をすべきか？

ステータス	アクションが必要
詳細	シスコはSCAのユーザエクスペリエンスを廃止し、SCA由来の機能をCisco XDRに移行します。テレメトリと分析は、アクティビティ、検出、インシデント、調査、資産のコンテキスト、対応、および自動化に関するより広範なXDRワークフロー

	の一部となります。
顧客のアクション	2026年10月24日より前に、XDRをアクティブ化し、SCAテナントを接続し、アクセスを検証し、日常の運用にXDR検出とインシデントを使用し、ソーステレメトリカットオーバーにアクティビティを使用し、XDRワークフローをテストし、履歴情報をエクスポートします。

私は何日を予定すればいいですか？

日付	マイルストーン	この意味は –
2026年9月15日	AWSとAzureの構成のセットアップ（一部のお客様向け）	該当する米国およびEMEAのお客様は、推奨されるXDR設定方法に移行します。
2026年9月30日	専用のSCA-to-XDR顧客移行プログラムの終了	プログラムを終了する前に、権限、プロビジョニング、および準備措置を完了します。
2026年10月7日	AWS CloudTrail、Azureアクティビティログ、およびGCP監査ログの検出のカットオーバー	これらの送信元をXDRで操作します。
2026年10月14日	カスタムイベント検出のカットオーバー：XDRで使用可能なインシデントチューニング、ウォッチリスト、およびエンティティグループの設定。	関連するワークフローと設定をXDRに移動します。
2026年10月21日	NetFlow検出カットオーバー	XDRでのNetFlow検出の操作
2026年10月24日	SCAのユーザエクスペリエンスが利用できなくなった	XDRへの移動を完了し、この日付より前の履歴データをエクスポートします。

何も行わない場合、またはXDRをプロビジョニングしていない場合はどうなりますか。

ステータス	非推奨
詳細	SCAのユーザエクスペリエンスが削除される前にCisco XDRをアクティブ化して接続しないと、SCAへのアクセスが失われ、SCA由来のワークフロー、検出、調査、統合、履歴データで使用可能な交換用のXDRエクスペリエンスを利用できなくなります。待機すると、アクティベーション、ユーザ設定、ワークフローの検証、および運用上の変更も、移行の最終部分に圧縮されます。
顧客のアクション	今すぐXDRを有効化して接続し、2026年9月30日までにチームがユーザー設定、ワークフロー検証、エクスポートの準備を完了できるようにします。SCAインターフェイスは、2026年10月24日に廃止される予定です。接続されたXDRテナントがなければ、SCAアクセス終了時に利用可能な代替XDRエクスペリエンスはありません。

廃止、変更、または利用できないもの

同じ形式では明らかに継続しないSCAの概念はどれですか。

ステータス	変更または廃止
詳細	• SCAユーザエクスペリエンス：2026年10月24日に削除されました。 • レガシーSCA Webフック動作：XDRワークフローに置き換えられました。 • SCA観察体験：1対1のXDR機能ではありません。 • サブネットの感度：資産価値の優先順位付けの概念に置き換えられました。 • エンティティ・グループ：資産ラベル、資産グループおよび値スコアリングに置換されます。 • スヌーズ検出の設定：移行されません。可能な場合はインシデント調整を使用してください。 • お客様が制御するアラート優先動作：保持されません。 • 一部のレポート、使用率の低いページ、および機能：廃止またはXDRネイティブのエクスペリエンスに置き換えられます。

廃止または移動が予想されるレポート項目または統合項目はどれか？

ステータス	予想される変更
詳細	例としては、クラウドポスチャウォッチリスト、Kubernetesモニタリング、AWS可視化/ダッシュボード/セッション検索/IP検索エクスペリエンス、MerakiとUmbrellaのコンテキスト統合、Eメールベースの月次レポートと毎日のアラート要約などがあります。このリストでは、各レガシーページを1対1で置き換えることはできません。

今回の移行で私に求められていないことは何ですか。

ステータス	このタイプのアクションはありません
詳細	シスコはお客様に対し、既存のネットワークセンサーの再配備、UX移行のためだけにクラウドログ取り込みを再構成する、サポートされている標準検出設定オブジェクトを手動で再作成する、またはSCAを長期的なパラレルコンソールとして保持するといった指示は行いません。

お客様の準備状況チェックリスト

1. 2026年9月30日までにCisco XDRをアクティブ化し、既存のSCAテナントを接続することで、移行プログラムが終了する前にチームが準備作業を完了できます。
2. ユーザを作成し、サインインを検証して、XDRで適切なアクセスを確認します。
3. 検出、インシデント、アクティビティの確認、調査、資産に関する洞察/デバイスに関する洞察

4. すべてのSCA Webフック、エクスポート、通知、SIEM/SOARハンドオフ、およびカスタム自動化をXDRワークフローまたは別のXDR操作サーフェスにマッピングします。
5. 各ソースが利用可能になったときに、アクティビティで必要なソーステレメトリを検証します。
6. 各ソースをカットオーバーする前に、必要な検出と対応プレイブックを検証します。
7. サブネットの感度、エンティティグループ、スヌーズ、アラートの優先度、ウォッチリスト、スキャナルール、信頼できるネットワーク、資産価値の優先順位付けを確認します。
8. 従来のレポート、SCA専用ページ、およびAPIの依存関係のインベントリを作成し、代替案や輸出要件を特定します。
9. 2026年10月24日より前に、必要なアラート、観測、未加工のログ、設定レコード、およびレポートをエクスポートします。

新しいXDRエクスペリエンスで自分の道を見つける

SCAをご利用のお客様にはCisco XDRの使用権がありますか。

ステータス	移行の一部として利用可能
詳細	既存のSCAのお客様には、移行の一部としてCisco XDRの使用権が与えられます。目的は、コアワークフローがXDRに移行する間もSCA値を維持することです。
顧客のアクション	サポートが必要な場合は、Cisco XDRをアクティブ化し、既存のSCAテナントを接続して、Cisco XDRアクティベーションプロセスを使用します。

SCA機能はCisco XDRのどこに配置されますか。

SCA関数	XDR宛先
アラートとアラートワークフロー	XDRの検出とインシデント
観察とイベント指向の調査	XDRアクティビティとXDR調査
イベント ビューア	XDR調査とアクティビティ
デバイスコンテキスト	資産の分析/デバイスの分析
Webhook、通知、エクスポート、ダウンストリーム配信	XDRワークフロー
検出設定	各設定がマイルストーンに到達すると、XDR設定が行われる

SCAは日常的に使用するパラレルコンソールとして引き続き使用できますか。

ステータス	いいえ
詳細	SCAのユーザエクスペリエンスは、2026年10月24日に削除される予定です。オーバーラップ期間を使用して、XDR運用モデルの練習、ワークフローの検証、およびランブックの更新を行います。

検出、インシデント、監視のユースケース

検出は単に1対1で移動しているだけですか。

ステータス	モデルの変更
詳細	必要ありません。シスコは、すべてのレガシーSCAアラートを変更されていないXDRオブジェクトとしてコピーするのではなく、検出コンテンツと運用モデルを進化させています。名前、ロジック、証拠、相関関係、および結果が変わる可能性があります。
顧客のアクション	XDR検出の結果、証拠、およびインシデントの相関を、運用する必要があるセキュリティシナリオに照らして評価します。名前の照合だけを受け入れとして使用しないでください。

アラートワークフローにXDRインシデントまたは検出を使用する必要がありますか。

ステータス	成果による選択
詳細	インシデントを使用して、人為的な対応、アナリストによる通知、トリアージ、エスカレーション、ケース管理、および協調的な対応を行います。検出機能を使用して、個々の結果、検出レベルのエクスポート、およびマシン間の自動化を行います。アクティビティはテレメトリサーフェスです。
顧客のアクション	必要に応じてインシデントから人間の通知と対応プロセスをトリガするようにランブックを更新します。検出を使用して、詳細な分析、エクスポート、および検出レベルの自動化を行います。

観察ベースのユースケースは継続するか。

ステータス	1対1ではない
詳細	従来の観測名、UIオブジェクト、またはトリガ条件が残ることを想定しないでください。目標は、アクティビティ、検出、インシデント、およびより広範な相関を通じて、同等または改善されたカバレッジです。
顧客のアクション	2026年10月24日より前に、ランブック、ダッシュボード、自動化の依存関係を特定して更新します。

主にNetFlowに依存していて、EDRを導入できない場合はどうすればいいですか。

ステータス	まだ範囲内
詳細	既存のネットワークセンサーと取り込みは引き続き機能し、移行されたネットワーク検出を引き続き使用するためにEDRを導入する必要はありません。
顧客のアクション	XDR検出、結果、インシデント、インシデントチューニング、および利用可能な資産コンテキストを使用します。エンドポイントの可視性に大きな制約がある場合は、導入固有のガイダンスを要求する。

通知、エクスポート、Webフック、自動化

SCA Webフックはどうなりますか。

ステータス	移行およびテスト
詳細	XDR自動化ワークフローは、通知、エクスポート、ダウンストリーム自動化の長期的なコントロールポイントです。ターゲットエクスポートパスはOCSFに合わせて調整されており、レガシーSCAアラートおよび観測モデルよりも詳細なコンテキスト検出情報を提供できます。
顧客のアクション	Webhookが人、SIEM、SOAR、またはその他のシステムに検出情報を送信する場合は、XDRワークフローでその動作を再作成してテストします。

検出ワークフローとインシデントワークフローの違いは何ですか。

ステータス	一致するトリガーの使用
詳細	データの移動、エクスポート、およびマシン消費に検出指向のワークフローを使用します。インシデント指向のワークフローを使用して、より広範な業務アクティビティや、Eメール、Slack、Webexなどの人的通知を行います。どちらもエクスポートをサポートできます。

SIEM、SOAR、またはカスタムダウンストリーム統合に対してどのような変更がありますか。

ステータス	レビューが必要
詳細	SCA固有のWebフック、ペイロード、アラート名、またはエクスポートが変更されないことを前提としないでください。ターゲットエクスポートパスはOCSFに沿っており、より完全でコンテキストに応じた検出の詳細を提供できます。
顧客のアクション	依存関係をXDRワークフローとXDRデータモデルに移行し、ダウンストリームの受信とランブックの動作をテストします。

NVMの通知とエクスポートを変更する必要がありますか。

ステータス	NVMカットオーバーが完了しました
詳細	NVMの検出は、2026年5月にXDRに移行しました。従来のNVM webhookパターンを使用しているお客様は、2026年5月15日のカットオーバーまでに、通知を移動してXDRワークフローにエクスポートする必要がありました。
顧客のアクション	NVMのXDRワークフローパターンの使用と検証を続行します。

ソースカットオーバーの前にテストすべきものは何ですか。

ステータス	必要な準備状況の確認
顧客のアクション	各送信元について、検出トリガーまたはインシデントトリガー、通知ペイロードまたはエクスポートペイロード、ダウンストリーム受信、フィルタリングまたはルーティングルール、および更新されたRunbook応答をテストします。送信元がSCAエクスペリエンスを離れる前にテストします。

テレメトリのソースとソースごとのカットオーバー

XDRアクティビティでは、いつテレメトリを使用できますか。

日付	テレメトリマイルストーン	顧客のアクション
2026年8月19日	アクティビティのONAデータテレメトリ	ONAテレメトリの確認を開始します。
2026年8月26日	アクティビティのCTBデータテレメトリ	CTBテレメトリのレビューを開始します。
2026年9月16日	アクティビティのAWS VPCフローログ、Azureフローログ、GCP VPCフローログ	クラウドフローテレメトリのレビューを開始します。
2026年9月23日	XDRでのAWSソースの設定	必要に応じて、XDRの設定手順を使用します。
2026年9月30日	AWS CloudTrail、Azureアクティビティログ、およびアクティビティのGCP監査ログ	監査ログテレメトリの確認を開始します。

ネットワークセンサーを再導入するか、クラウドログの取り込みを再設定する必要がありますか。

ステータス	いいえ。UXの移行のみではありません。
詳細	既存のネットワークセンサーとクラウドログの取り込みはこのフェーズでも機能し続け、ユーザエクスペリエンスと検出がXDRに移行しているため、再導入や再設定を行う必要はありません。
重要な例外	センサーおよび統合で使用されるパブリックIPアドレスまたはエンドポイントが変更される可能性があります。ファイアウォールルール、プロキシ許可リスト、およびその他のネットワーク制御を確認します。シスコは、設定の変更が必要となる前に、必要なXDRエンドポイントの詳細を提供します。

ソースの検出がカットオーバーされるのはいつですか。

ステータス	ソース固有のスケジュール
詳細	カットオーバー時には、その送信元のテレメトリと検出は、SCAユーザエクスペリエンスを通じて使用できなくなります。 • 2026年10月7日： AWS CloudTrail、Azureアクティビティログ、およびGCP監査ログの検出。 • 2026年10月14日：カスタムイベント検出。 • 2026年10月21日：NetFlow検出。

設定、チューニング、ウォッチリスト、およびアセットコンテキスト

検出設定は移行されますか。

ステータス	段階的な移行
詳細	サポートされている標準構成オブジェクトは、より広範な検出エンジン移行の一部として移行することが想定されています。NVMの検出設定は2026年5月にXDRに移行しましたが、その他の設定は機能が使用可能になるに従って移行します。
顧客のアクション	シスコが導入に関する特定の指示を発行しない限り、移行のためだけに標準設定を手動で再作成しないでください。

サブネット感度、エンティティグループ、スヌーズの代わりになるものはどれか？

ステータス	概念の変更
詳細	• サブネットの感度：Asset Insights / Device Insightsのデバイス値の優先順位付けスコアに置き換えられました。2026年9月30日までにXDR Device Insightsで予定されています。 • エンティティグループ：設定は2026年10月14日にXDR Device Insightsでスケジュールされます。既存のグループはラベルに移行し、資産ラベルと価値評価が優先順位付けに使用されます。 • 再通知：再通知された設定は移行されません。インシデント調整は2026年10月14日に利用可能になる予定です。

ウォッチリストはいつ移動しますか。

ステータス	2026年10月14日予定
詳細	ウォッチリストの設定は、2026年10月14日にXDRで利用可能になる予定です。既存のウォッチリストは移行されますが、ロジックが保持されている間に用語とルールの表示が変更される可能性があります。
顧客のアクション	移行中のウォッチリストに依存するルール、抑制、およびワークフローを検証します。

それでも、SCAと同じようにアラートの優先度を設定できますか。

ステータス	いいえ
詳細	アラートの優先度は、シスコの脅威調査を使用してハードセットされており、顧客管理による誤検出の抑制制御ではありません。

センサー、クラウド統合、および運用状態

FTD、ISE、AWS、Azure、またはGCPの統合は変更されないままですか？

ステータス	ビジネスクリティカルなパスの検証
詳細	すべての統合で同じUI、ワークフロー、または構成方法が保持されるとは限りませ

	ん。GCP構成は既にXDR内に存在し、次にAWSとAzureが移動します。オンプレミスのセンサー関連の移行項目は10月に移動します。
顧客のアクション	製品固有のガイダンスに照らして、FTD、ISE検疫、エンリッチメント、SAL接続ワークフロー、およびその他のビジネスクリティカルな統合を検証します。

センサーの健全性、活性、フロー配信、および音量を同じ方法でモニタできますか。

ステータス	準備状況のレビュー
詳細	シスコは移行中もセンサーとインジェストの動作を維持していますが、すべてのSCAモニタリングページまたはワークフローが1対1で移行することを約束しているわけではありません。
顧客のアクション	依存している状態、プロトコル、フロー量、および配信チェックのインベントリを作成し、それらのXDR動作パスを検証します。

ONAまたはCTBのイメージ配布、宛先URL、サービスキー、またはパブリックIPアドレスは変更されますか。

ステータス	ネットワークの依存関係の確認
詳細	このフェーズではセンサーの再導入は不要ですが、テレメトリの宛先は送信元がXDRに移行するにつれて変更される可能性があります。
顧客のアクション	関連するソースカットオーバーの前に、ファイアウォールルール、プロキシアテントリスト、宛先URL、およびサービスキーの依存関係を確認します。公開された移行手順なしでセンサーの予防的変更を行わないでください。

履歴データ、レポート、および管理

SCAユーザエクスペリエンスがオフになると、履歴SCAデータはどうなりますか。

ステータス	2026年10月24日より前にエクスポート
詳細	SCAインターフェイスを介した履歴データへのアクセスは、ユーザエクスペリエンスが削除された時点で終了します。生のテレメトリは、検出移行パスの前および経由でXDRに取り込まれますが、SCAは履歴を取得するための長期的な場所ではありません。 • アラートとオブザベーションは、SCAコンソールからCSVとしてエクスポートできます。 • ネットワークトラフィックやクラウドログなどの生のログは、必要に応じてCSVとしてエクスポートできます。 • エクスポートの前に、監査、調査、保存に関する証拠の要件を定義します。

すべてのSCAレポート機能はXDRに移行しますか。

ステータス	一部は廃止または交換

詳細	一部のレポート機能、使用率の低いページ、およびレガシー機能は、XDRネイティブの検出、調査、アクティビティ、および資産インサイトのエクスペリエンスによって廃止または置き換えられる予定です。
顧客のアクション	運用に必要なインベントリのレポートを今すぐ作成し、XDRエクスペリエンス、エクスポート、または交換のワークフローを特定します。

移行の完全性を実証する方法は？

ステータス	証明アーティファクトの定義
顧客のアクション	必要な記録と証拠を定義し、2026年10月24日より前に必要なSCA履歴をエクスポートし、必要なソースごとにXDRの可視性を検証します。移行は、顧客管理による個別システムへの一括の再インポートではありません。

SCA側に保存された管理者情報はどうなりますか。

ステータス	廃止前の文書化
詳細	2026年10月24日以降も、SCAに保存されたお客様が目に見える構成、管理情報、履歴が引き続き使用できるようになることを想定しないでください。
顧客のアクション	管理、監査、または履歴参照に必要なものはすべてエクスポートまたは文書化し、XDRを対象の運用インターフェイスとして使用します。

APIおよびカスタム統合

Get Observations API、SCA Devices API、またはその他のSCA固有のAPIを置き換えるものは何ですか。

ステータス	インベントリの依存関係
詳細	シスコは、すべてのSCA APIについて、1対1のAPI置き換えに関する最終的なマトリックスを公開していません。アクティビティ、検出、インシデント、ワークフロー、資産インサイト/デバイスインサイト、およびXDR調査を中心に計画します。
顧客のアクション	インベントリの直接的な依存関係は現在あり、2026年10月24日以降も従来のエンドポイント名が残っていることが前提ではありません。

従来のインシデント作成方法とカスタム自動化はどうなりますか。

ステータス	移行期として扱う
詳細	FAQでは、すべてのレガシーインシデント作成方法またはAPIについて、正式な公開停止日を設定しているわけではありません。目標とする方向は、XDRのカスタムセキュリティイベントと検出、XDRモデルでのインシデント生成、成果管理のためのインシデントチューニングです。
顧客のアクション	SCAの観察、アラート名、デバイス、Webフック、エクスポート、またはレポートを使用するすべての自動化を、XDRワークフロー、検出、インシデント、アクティビティ、またはAsset Insightsユースケースにマッピングします。関連するソースカットオーバーの前に、エンドツーエンドの動作をテストします。

完了した移行項目

NVM検出の移行

ステータス	��完了
解決策	NVMの検出と関連する検出設定は、2026年5月にXDRに移行しました。レガシーNVMの通知とエクスポートに依存するお客様は、XDRワークフローを使用してワークフローパターンを検証する必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。