Security Cloud Control

目次

今日、組織は重大な課題に直面しています。攻撃者は、セキュリティで保護されていないユーザー、デバイス、ワークロードなど、ネットワーク内の最も脆弱なリンクを悪用しています。この脅威の状況は、従来のデータセンターから分散環境への移行によって複雑になり、複数のタッチポイントで分散したデータの保護が複雑になっています。

これらの脅威に対処するために、多くの組織は複数のセキュリティツールを使用しており、効果的なセキュリティを妨げるサイロ化されたチーム、技術スタック、および管理システムにつながっています。この断片化されたアプローチにより、不要なコスト、デプロイメント時間の延長、一貫性のないセキュリティ、重大なギャップが発生します。

一元化されたプラットフォームがなければ、セキュリティの全体像を把握することは困難です。設定ミスを手動で特定すると、エラーが発生しやすく、侵害につながる可能性があります。セキュリティ機能を最大限に活用して ROI を最大化するためのスキル、時間、リソースが不足しています。さまざまなセキュリティ製品があるため、アクセスまたはポリシーの問題の解決には時間がかかります。管理者は、異なるプラットフォーム間で同様のポリシーを作成するのに時間を使いすぎています。多くの場合、運用上の問題は事後対応的に対処され、ダウンタイムと最適でないパフォーマンスにつながります。実用的ではないアラートと大量のデータにより、緊急性が失われて、分析が停滞し、意思決定が妨げられます。

統合セキュリティ プラットフォームは、セキュリティ環境の包括的なビューを提供し、一貫したポリシー適用を可能にし、障害対応を簡素化し、AI の助けを借りて実用的なインサイトを提供することで、これらの問題を軽減することを目的としています。

さまざまな組織の固有のニーズを満たし、多様なネットワーク ファイアウォール構成をサポートするために、運用の簡素化、セキュリティの強化、および明確性の向上という 3 つの主要な目標に焦点を当てています。シスコは、セキュリティ管理プロセスを合理化し、高度な Cisco Zero Trust と脆弱性保護による防御を強化し、AI 主導のインテリジェンスを通じて明確で実用的なインサイトを提供することを目指しています。

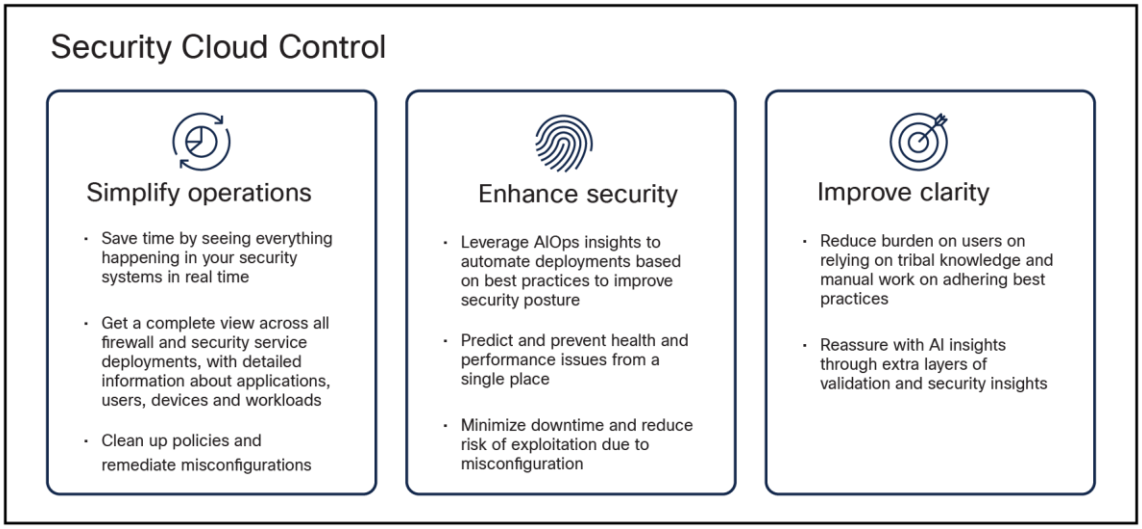

図 1.
Security Cloud Control の設計原則：シンプル、効率的、効果的な管理。

Security Cloud Control

Security Cloud Control は、セキュリティクラウドを統合し、実用的なインサイトをプロアクティブに明らかにし、ハイブリッド環境全体で解決を自動化する、新しい AI ネイティブの管理ソリューションです。一貫した UI エクスペリエンス、共通サービス、およびセキュリティクラウド全体の設定、ログやアラートを接続するデータバスを備えた最新のマイクロアプリケーション アーキテクチャです。AI は最初から組み込まれており、AI アシスタントの機能を超えて、ポリシーと設定をプロアクティブに最適化し、問題を検出して障害対応を行うことができます。これは、チームが Cisco Security への投資を最大限に活用できるように設計されており、時間を節約し、よりシンプルで合理化されたポリシーの利点を活用できます。

Security Cloud Control によって、複数のシスコおよびクラウドネイティブのセキュリティ プラットフォームにおけるセキュリティポリシーとデバイス設定を簡単に管理できます。

Security Cloud Control は、次のポリシーと設定の要素を一元管理します。

- Cisco Multicloud Defense
- Cisco Secure Firewall ASA（オンプレミスと仮想）
- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Meraki™ MX
- Cisco IOS デバイス
- AWS セキュリティグループ

Security Cloud Control には、Firewall Management Center（FMC）のクラウド提供型バージョンも組み込まれており、オンプレミスとクラウドベースのファイアウォール管理の間で完全に統合されたエクスペリエンスが提供されます。これにより、オンプレミスと仮想の両方で、ポリシーと設定の管理が Cisco Secure Firewall Threat Defense（FTD）に拡張されます。

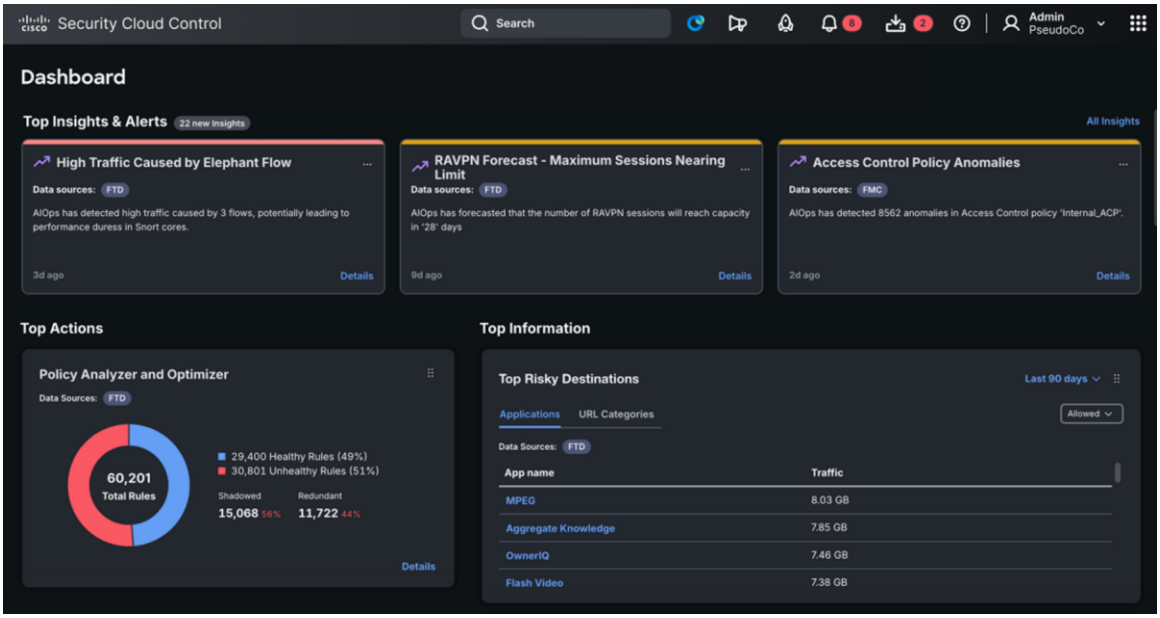

図 2.
統合ダッシュボード：ファイアウォールとセキュリティサービスの包括的なビュー

セットアップは簡単、迅速かつスムーズなため、数時間以内に何百台ものデバイスをオンボーディングして管理を開始できます。直感的なユーザーインターフェイスを採用し、シンプルさに重点を置いているため、トレーニング要件は最小限で済み、学習曲線は数日ではなく数時間で測定されます。

柔軟性と拡張性は、クラウドテクノロジーであるだけでなく、オープン API の特性でもあります。Security Cloud Control はクラウドベースのソリューションであるため、設備投資、ラックスペース、手動によるパッチ適用やアップグレードが不要となり、運用コストが大幅に削減されます。

組織にあるセキュリティデバイスの数（5 台か 5000 台か）は関係ありません。Security Cloud Control を使用すると、ネットワーク運用チームはセキュリティデバイスの管理と保守に費やす時間を削減でき、コアミッションにとって最も重要な作業に集中できます。

シスコは、Firewall AI Assistant を使用して、管理者の操作をさらに簡素化しています。ファイアウォールルール管理の複雑さに対処することで、ネットワークセキュリティに革命をもたらします。

統合ダッシュボードにより、お客様はネットワークとクラウドのセキュリティエコシステム全体をリアルタイムで包括的に把握できます。お客様は、一元化されたグローバル管理者の下で複数のテナントを調整し、何万ものセキュリティデバイスを効率的に管理できます。

Security Cloud Control の可視性と管理のレベルによって、成果をもたらすことができます。Cisco Security Cloud Control は、インテントベースのポリシーを 1 か所で取得し、ネットワーク内のすべてのコントロールポイント全体に変換することから、複数のソリューションにまたがるポリシーの合理化、障害対応、推奨まで、すべてを支援します。

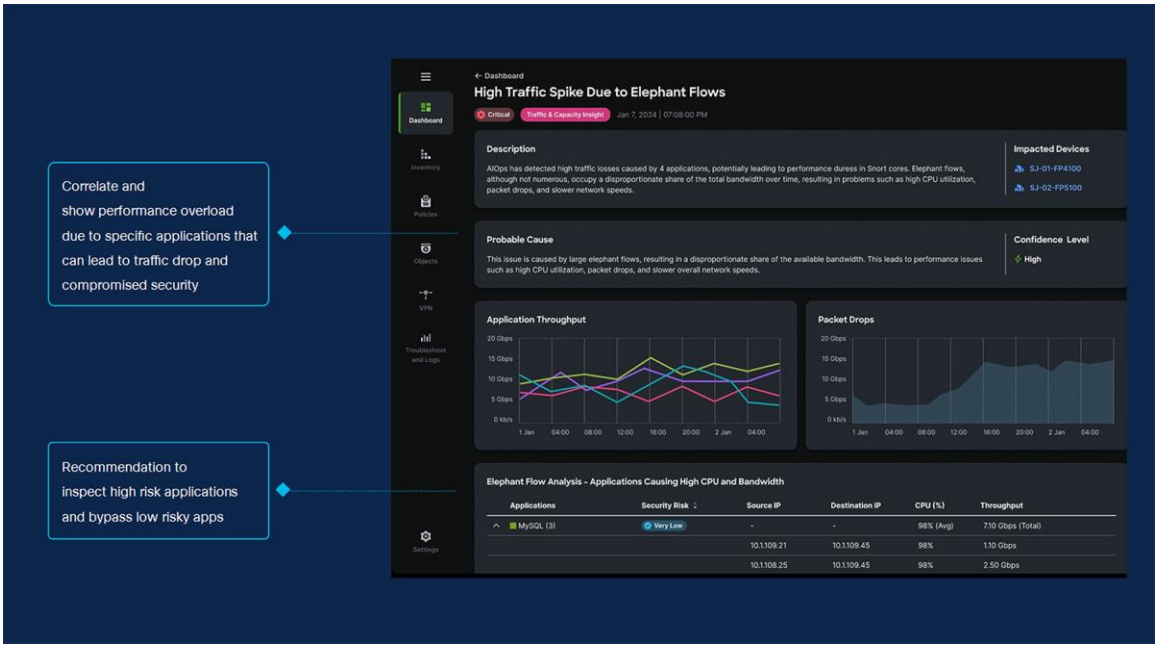

図 3.
AIOps による予測インサイト

Security Cloud Control の利点

Security Cloud Control は、一元化された可視性、合理化されたポリシーデプロイメント、およびリアルタイムモニタリングにより、ネットワークセキュリティ管理を簡素化します。複数のデバイス間でセキュリティポリシーを調和させることで運用効率を向上させ、一貫した保護と脅威への迅速な対応を実現します。

- **管理の簡素化**：拡張ネットワーク全体でセキュリティポリシーとデバイス管理を合理化します。
- **重要なセキュリティインサイト：**シスコの統合ダッシュボードは、ネットワーク内の重大なセキュリティギャップを明らかにします。侵害につながる可能性のある誤って設定されたポリシーを特定し、それらを修正するための実用的な手順を提供します。危険なアプリケーションと URL を検出し、購入したすべてのセキュリティ機能を利用できるようにします。保護が必要な脆弱なアセットを強調表示し、さまざまな製品にわたるすべての管理上の変更を 1 つの一元化された場所に記録します。また、重要なアラートに優先順位を付けて、上位のインサイトとして対処できるようにします。
- **受動的ではなくプロアクティブ：**従来、アラートが大量に表示され、問題を軽減する方法を見つける必要がありました。現在は、プロアクティブなアプローチに移行しています。AI を使用して、システムが最大容量に達する可能性を予測し、問題の原因となっているアプリケーションを特定し、ダウンタイムを回避するためのソリューションを提供します。
- **AI による運用の簡素化：**AI Assistant は、ポリシーを理解し、デプロイメント内の異常を検出するのに役立ちます。問題のあるルールを特定し、必要なアクションを提案し、ルールを作成することもできます。これにより、ネットワーク全体で一貫したポリシーが適用されます。
- **1 回の書き込みですべての場所に適用：**ネットワークオブジェクト（悪意のある IP や URL など）を作成する必要があるのは 1 回だけです。これらは、さまざまなセキュリティ製品間で共有できるため、ネットワーク全体で包括的な保護が実現できます。

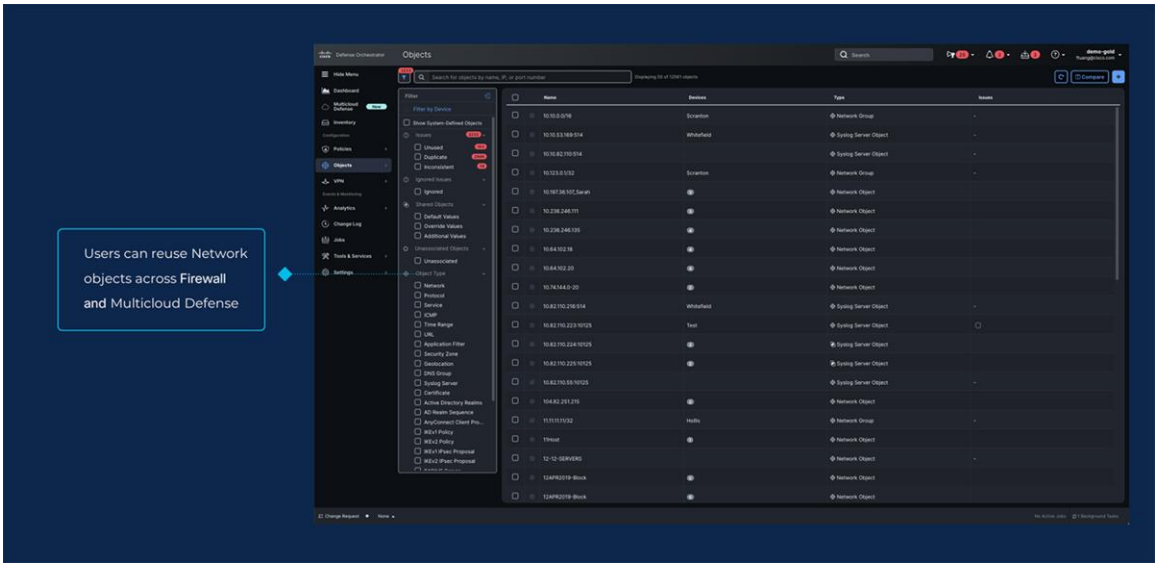

図 4.
一貫したポリシーの適用：オンプレミス環境とクラウド環境でのネットワークオブジェクトの共有

Security Cloud Control の機能

Security Cloud Control は、組織全体でポリシーを調整することにより、セキュリティ態勢を強化します。シスコのソリューションは、セキュリティツールを追加する際にポリシーの状態を保つという課題に対処しています。この点は、地理的に分散した場所やハイブリッドネットワーク環境がある組織に特に役立ちます。

このソリューションにより、分散したセキュリティデバイス全体でポリシー管理の複雑で時間のかかる作業がなくなるため、セキュリティの不整合やギャップを防ぐのに役立ちます。

安全性が高く、常に利用可能で、信頼性の高い、スケーラブルなマルチテナント クラウド ソリューションを使用して、どこからでも管理できます。より短時間かつより少ないリソースでセキュリティ態勢を強化および維持することにより、他の優先事項のためにキャパシティを解放します。

AIOps を使用した運用の簡素化とセキュリティの強化：AIOps は予測的なインサイトと自動化を提供し、管理者が運用を簡素化し、セキュリティ態勢を強化し、運用効率を高め、コストを削減できるようにします。

設定ミスを排除し、ルールを最適化して運用を簡素化：ポリシーアナライザとオプティマイザは、重複、冗長、シャドウ、期限切れ、オーバーラップ、およびマージ可能なルールを検出します。異常の特定とは別に、正確な実装の推奨事項を提供します。このサービスから変更ログとレポートをダウンロードして、ポリシーの最適な状態を維持できます。

ハイブリッド環境の管理（ASA、FTD、Multicloud Defense）：ワークフローの合理化と、クラウドセキュリティとオンプレミス/データセンター ファイアウォールの統合により、Cisco Firewall と Multicloud Defense 間でオブジェクトを共有し、VPN トンネルを作成できるようになりました。静的オブジェクト共有により、ハイブリッド環境全体で一貫したポリシーの結果が得られるため、管理オーバーヘッドがなくなり、設定ミスの可能性が減少します。サイトとクラウド間の VPN トンネルにより、ハイブリッド環境に展開されたアセットは、セキュアな接続を介して相互に通信できます。

既存のプラットフォームの最適化：Security Cloud Control は、オンボーディング時に、何年も運用されているファイアウォール全体の一般的な問題をすぐに特定してフラグを立てることができます。すべてのリスクを評価して特定すると、すべてのデバイスの問題をまとめて迅速に修正でき、デバイスを一貫したより安全な状態にできます。Security Cloud Control は、次の問題の修正に役立ちます。

- **未使用のオブジェクト**は、トラブルシューティング中にヒットして問題を引き起こしたり、監査中に潜在的に望ましくない問題を生じさせたりしないオブジェクトです。
- **重複するオブジェクト**は、多くの場合、デバイス上で見つかり、異なる名前が同じ IP に関連付けられています。重複するオブジェクトを削除すると、アプライアンスの全体的なパフォーマンスを向上できます。
- **一貫性のないオブジェクト**は、展開されたファイアウォール全体で表示が異なるオブジェクトであり、通常、セキュリティの観点から最も重要なオブジェクトの問題です。たとえば、「ブロックリスト」というオブジェクト名があり、一致する変数や IP を持つこのオブジェクトがすべてのデバイスに存在すると想定されている場合、Security Cloud Control はこのオブジェクトをすぐに検証します。オブジェクトがファイアウォールデバイス間で一貫していない場合、Security Cloud Control はアラートを表示し、問題を数秒で解決できるようにします。
- **シャドウルール**は、取って代わる先行ルールが原因でヒットすることがないルールです。

ASA から FTD への移行：Security Cloud Control の組み込み移行ウィザードにより、以前より簡単に環境を ASA から Cisco Threat Defense（FTD）に移行できるようになりました。単一の UI から ASA と FTD の両方を管理できるため、独自のタイムラインで NGFW に移行できます。

一貫したポリシー設計のためのテンプレート：Security Cloud Control を使用して、異なるデバイス間の一貫したポリシー設計を一元的に作成、適用、および管理できるようになりました。テンプレート機能を使用すると、複製およびカスタマイズ可能な「ゴールド構成」を作成できます。完了したら、標準化された構成をエクスポートして、新しいプラットフォームに適用できます。

ファイアウォール OS のアップグレードの簡素化：多くの場合、お客様が直面する最も時間がかかりフラストレーションを感じる課題の 1 つは、機能と脆弱性の両方に対してファイアウォール OS を維持するというものです。Security Cloud Control を使用すると、Cisco ASA または Cisco Threat Defense（FTD）イメージのアップグレードにかかる時間を最大 90% 短縮できます。計画から当て推量が取り除かれ、すべてのデバイスで同時に一括アップグレードを実行できます。

一括 CLI：直感的な Web ベースの UI に加えて、CLI（コマンド ライン インターフェイス）ユーザーに合理化されたユーザーエクスペリエンスも提供します。Security Cloud Control の CLI ツールを使用すると、ユーザーは多数のデバイスで同時に CLI コマンドを一括して実行できます（最も一般的なコマンドのユーザー定義マクロやショートカットの作成機能など）。

変更ログによる変更の監査：お客様は、変更ログを使用して変更を追跡し、加えられた変更、変更時期、および変更者を確認できます。Security Cloud Control UI と CLI ツールの両方で行われたすべての変更がキャプチャされます。

リモートアクセス VPN の監視と管理：キャパシティプランのための 90 日間にわたる履歴ビューを使用した、リモートユーザーセッションとヘッドエンドデバイス全体の可視性。Cisco Security Analytics and Logging を活用して、ユーザートラフィックの可視性を拡張します。

Firewall Management Center のクラウド提供型バージョン：Firewall Management Center のオンプレミスおよび仮想バージョンと同じルックアンドフィールを提供します。

- **包括的な可視性とポリシー制御：**ネットワークとクラウドで実行中の内容に対する優れた可視性を提供し、保護が必要な対象を確認できるようにします。この可視性を使用すると、ファイアウォールルールを作成および管理し、環境内で使用される数千もの Web アプリケーションとカスタムアプリケーションを制御できます。
- **動的防御のための自動セキュリティ：**ネットワークの変化が継続的に監視され、運用が合理化され、セキュリティが向上するため、重要な脅威に集中できます。

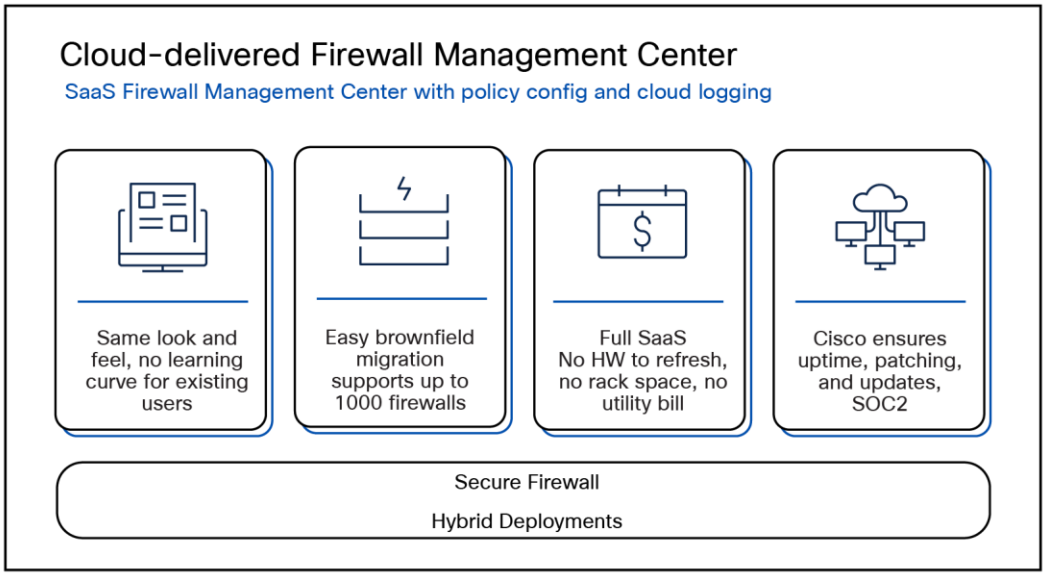

図 5.
Security Cloud Control を介したクラウド提供型 Firewall Management Center の利点。

詳細については、『Cisco Secure Firewall Management Center (formerly Firepower Management Center) Data Sheet』を参照してください。

Multicloud Defense の詳細については、Cisco Multicloud Defense を参照してください。

表 1. 機能とメリット

目的	実現方法
迅速な展開とデバイスのオンボーディング	• Security Cloud Control アカウントは 24 時間以内に割り当てられるため、すぐにデバイスのオンボーディングを開始できます。デバイスは、関連するダウンタイムなしで一括インポートを介して、単なる構成、単一のデバイス、または数千のデバイスとしてオンボードできます。 • ロータッチプロビジョニングにより、大規模なリモート展開が合理化されます。FTD バージョン 7.0.3 以降（7.1 を除く）を実行している Firepower 1000/2000/3000 シリーズで利用できます。
AI Ops：トラフィックとキャパシティのインサイト	• トラフィックとキャパシティのインサイトは、ネットワークトラフィックのリアルタイム分析と履歴分析の両方を提供し、問題の特定と解決、および潜在的な問題の予測を支援します。 • ネットワークセキュリティ管理者は、リソースを最適化し、リスクベースの優先順位付けによって解決までの平均時間を短縮し、ベストプラクティスの推奨事項に合わせることができます。
AI Assistant for Firewall：ルールの作成と分析	• お客様は、ポリシーの目的を説明し、ルールの作成を支援するように AI Assistant に依頼できます。 • Firewall AI Assistant を使用して、管理者の操作を簡素化します。
ポリシーアナライザとオプティマイザを使用したポリシーインサイト	• ファイアウォールポリシーの詳細なレビューと強化。冗長、重複、オーバーラップ、シャドウ、およびマージ可能なルール、および期限切れまたは非アクティブなルールの特定と修正。カスタマイズされた修復の推奨事項を提供することで、ファイアウォールポリシーの合理化と効率性を維持し、デプロイメント時間を大幅に短縮します。
統合ダッシュボード：ファイアウォールとセキュリティサービスの包括的なビュー	• ネットワークとクラウドのセキュリティエコシステム全体をリアルタイムで包括的に把握します。お客様は、一元化されたグローバル管理者の下で複数のテナントを調整し、何万ものセキュリティデバイスを効率的に管理できます。
既存デバイスの最適化のためのオブジェクトおよびポリシー分析	• Security Cloud Control は、オンボーディング時に、最適化が必要な領域を明らかにし、見つかった問題をユーザーが迅速に修正できるようにします。一般的な問題には、デバイス間で重複するオブジェクト、未使用のオブジェクト、一貫性のないオブジェクトが含まれます。また、ヒット率と、決してヒットしないシャドウルールを特定できます。
プロアクティブな構成とポリシー変更のオプション	• Security Cloud Control では、デバイスを一元的に管理する方法を選択できます。必要に応じて、CLI ツールを使用してすぐにデバイスに直接展開し、最も一般的なコマンドの「一括」展開、マクロ、ショートカットを使用可能にできます。次に、UI を使用して、通常の営業時間中にクラウドで変更を「ステージング」し、次のメンテナンス期間でそれらの変更をプッシュする簡単な方法も提供できます。
セキュリティテンプレート	• 既存の「ゴールド構成」を活用して、テンプレートを設計および管理して、新しいデバイスを簡単に一貫して展開できます。
グローバル検索	• Security Cloud Control によって管理されているデバイスをすばやく見つけてアクセスできます。システム内のすべてのデバイスとオブジェクトをスキャンし、インデックスを付けて表示します。イベントベースのインデックス作成プロセスで、デバイスまたはオブジェクトが追加、変更、または削除されるたびに検索インデックスが自動的に更新されます。
ASA から FTD への移行	• Security Cloud Control の組み込み移行ウィザードを使用して、ご使用の環境を ASA から Cisco Threat Defense（FTD）に移行します。
変更ログ	• アカウンタビリティ、監査、および障害対応の目的で、Security Cloud Control 内で行われた設定の変更をトラッキングします。
アウトオブバンドの通知	• ASDM または CLI（SSH）経由で行われた変更は、Security Cloud Control 管理者によってアウトオブバンド（OOB）変更として特定されます。管理者は、この変更を保持するか、元の設定に戻すかを決定できます。
設定のバックアップとロールバック	• Security Cloud Control は、すべての変更後に設定をバックアップし、以前の設定にロールバックする機能を提供します。
シンプルなイメージのアップグレード	• 最新のパッチや機能へのアクセスを高速化するために、OS アップグレードの実行アプローチを合理化します。

目的	実現方法
潜在的な問題のトラブルシューティング	• Security Cloud Control には、ライブログをプルして PacketTracer を実行する機能が組み込まれており、デバイスの障害対応に役立ちます。
簡易検索	• オブジェクト名、アクセス制御リスト（ACL）名、ネットワーク、またはアプリケーションポリシー要素を検索して、デバイスタイプ全体でのポリシーの適用方法を確認します。

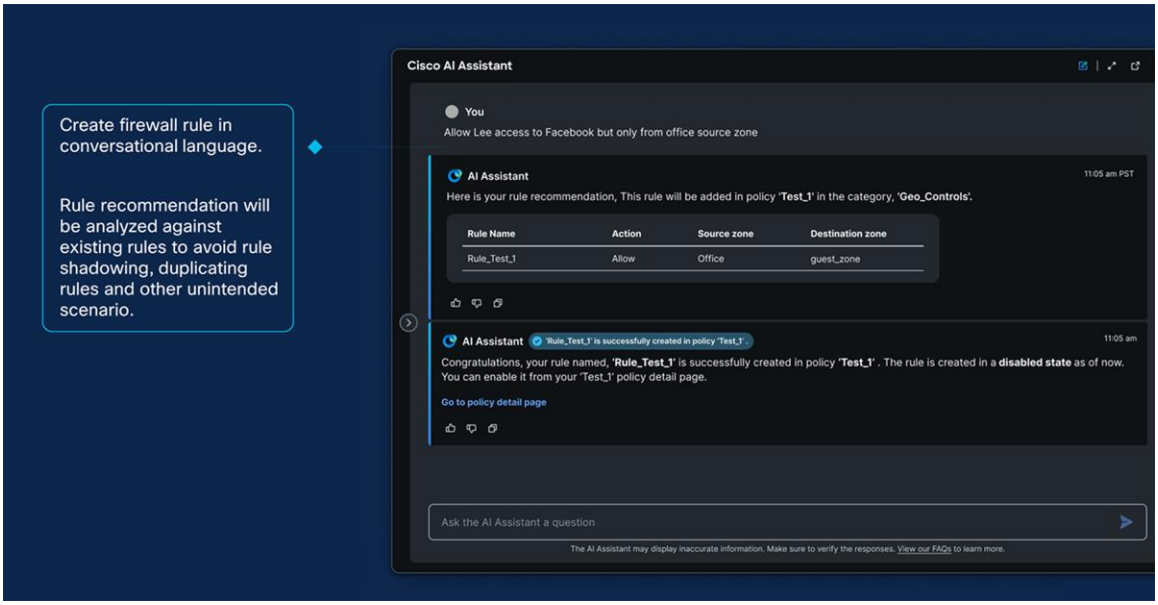

図 6.
ファイアウォールルール作成の AI Assistant

Security Analytics and Logging（SAL）SaaS の概要

SAL（SaaS）と呼ばれるクラウドネイティブのデータストアを備えた、クラウドで提供される Software-as-a-Service（SaaS）

SAL（SaaS） は、Cisco Firepower® Threat Defense（FTD）ソフトウェアを実行する次世代ファイアウォール（NGFW）と、適応型セキュリティアプライアンス（ASA）ソフトウェアを実行するデバイス向けに、管理プラットフォームに依存しないクラウドベースおよびクラウド配信のログ管理を提供するフル機能のサービスです。SAL（SaaS）では、Security Cloud Control（CDO）の API を介して、ファイアウォール イベント ログの イベント表示ができます。

Cisco Security Logging and Troubleshooting：組織はファイアウォールログをクラウドに保存し、Security Cloud Control のイベントビューアに視覚的に表示できます。トラブルシューティングのために、ファイアウォールプラットフォームからの履歴イベントやライブ イベントを関連付けます。

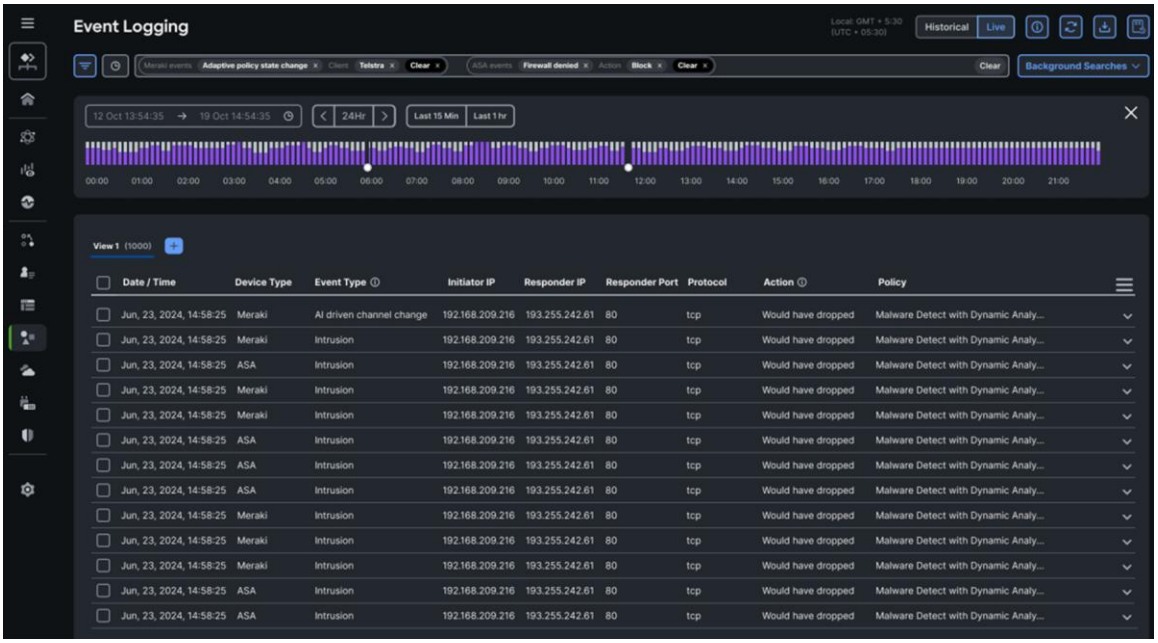

図 7.
統合されたクラウドベースのライブロギングにより、トラブルシューティング機能を拡張し、監査のための履歴の可視性を提供します。

Cisco Security Analytics and Logging（SaaS）を実行するために必要なコンポーネントとセットアップ：

Secure Event Connector：クラウド展開からファイアウォール イベント ログをキャプチャするには、Secure Event Connector（SEC）が必要です。SEC は、オンプレミスまたはクラウドの Secure Device Connector（SDC）にインストールできるコンテナ化されたアプリケーションであり、スタンドアロンモードで実行するように設定することもできます。Firepower Threat Defense（FTD）デバイスおよび適応型セキュリティアプライアンス（ASA）デバイスからイベントを受信し、クラウド内の Cisco SAL に転送します。インストール手順については、こちらを参照してください。SEC は SAL（SaaS）にログを送信するための最もスケーラブルなルートですが、Cisco Firepower バージョン 6.5 以降を実行しているファイアウォールデバイスは、SEC を必要とせずにイベントログを SAL クラウドに直接送信できます。この機能は、ファイアウォールデバイスごとに最大 8,500 イベント/秒（eps）の持続的なピークレートを確実にサポートすることがわかっています。Cisco Firewall Management Center（FMC）バージョン 7.0 では、「統合」設定を通じて、管理下にあるデバイスのクラウドへの直接ルートがサポートされています。

プラットフォーム サポート マトリックス：Security Cloud Control がサポートするシスコのセキュリティデバイス

Security Cloud Control でサポートされるシスコのセキュリティデバイス

製品	ASA のソフトウェアバージョン	FTD バージョン
ASAv	8.4 以降	該当なし
ASA 5506-X、ASA 5512-X	8.4 以降	該当なし
ASA 5525-X、5545-X、5555-X	8.4 以降	該当なし
ASA 5585-10、5585-20、5585-40、5585-60	8.4 以降	該当なし
ISA 3000	8.4 以降	7.0.3 以降（7.1 を除く）
Firepower 1010、Firepower 1120、Firepower 1140、Firepower 1150	9.8 以降	7.0.3 以降（7.1 を除く）
Firepower 2110、Firepower 2120、Firepower 2130、Firepower 2140	9.8 以降	7.0.3 以降（7.1 を除く）
Firepower 3105、Firepower 3110、Firepower 3120、Firepower 3130、Firepower 3140	3100、3120、3130、3140 の場合は 9.17.1、3105 以降の場合は 9.19.1	7.1 以降
Firepower 4112、Firepower 4115、Firepower 4125、Firepower 4145、	9.4 以降	7.0.3 以降（7.1 を除く）
Firepower 4215、Firepower 4225、Firepower 4245	9.20 以降	7.4 以降
Firepower 9300	9.4 以降	7.0.3 以降（7.1 を除く）
FTDv：KVM、VMware、Azure	NA	7.0.3 以降（7.1 を除く）
Meraki MX	NA	NA
Cisco IOS（SSH）：CLI ツールと変更ログのみに限定	NA	NA

発注情報

Security Cloud Control（SCC）のファイアウォール管理/マルチクラウド防御には、ASA、FTD、および Multicloud Defense をカバーするテナント権限の基本サブスクリプションが必要です。ファイアウォールをご利用のお客様には、デバイス管理の権限付与のためのデバイスごとのライセンスサブスクリプションがあります。デバイス ライセンス サブスクリプション（無制限ロギングのサブスクリプション付き）は別途ご利用いただけます。1 年、3 年、5 年のサブスクリプションをご利用いただけます。

Multicloud Defense の場合、製品ライセンスは、すべてのクラウド環境で消費されたゲートウェイ時間の集約に基づきます。この製品には、Advantage と Premier の 2 つの階層があります。Threat、マルウェア、URL フィルタリング、サポートなどのファイアウォール デバイス ライセンスは、別途購入する必要があります。ロギングとトラブルシューティングのユースケースには、Security Logging and Analytics を追加することもできます。

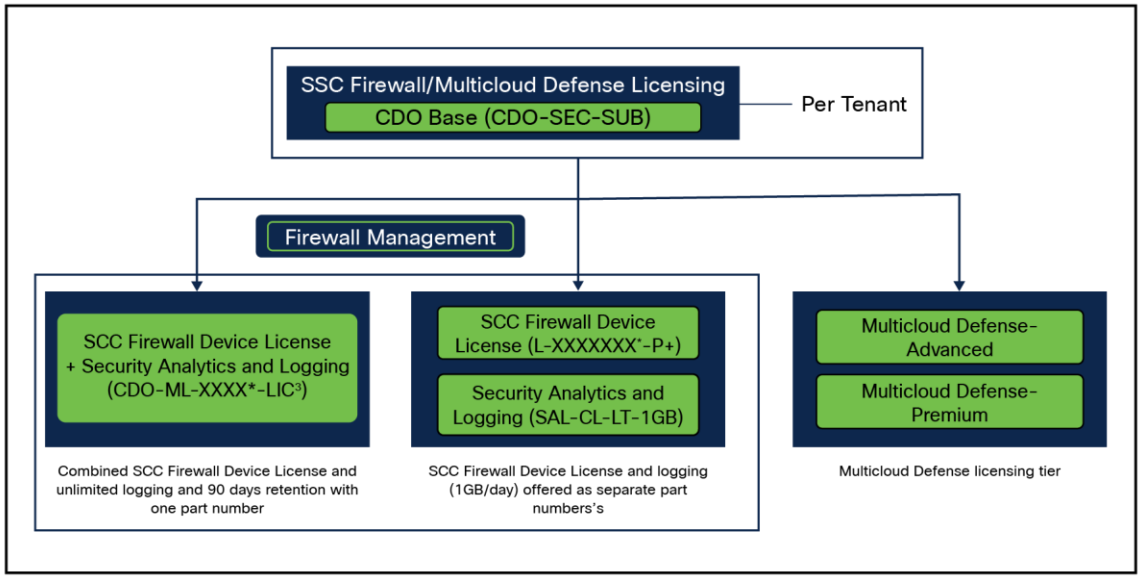

図 8.
Security Cloud Control ライセンス構造のファイアウォール管理/マルチクラウド防御

* firepower モデルを示します。たとえば、10 台の Cisco FPR1010 デバイスを注文し、これらのデバイスを無制限のロギングと 90 日間の保持期間で SCC ファイアウォール デバイス ランセンスから管理する場合、製品番号は CDO-ML-FP1010-LIC となり、CDO-SEC-SUB（テナント権限）が付きます。別の例として、10 台の Cisco FPR3110 デバイスを注文し、これらのデバイスを個別のロギング（1GB/日）で SCC から管理する場合、製品番号は L-FPR3110-P= と SAL-CL-LT-1GB の 2 つとなり、CDO-SEC-SUB（テナント権限）が付きます。関連するサブスクリプション期間を選択します。

Security Cloud Control の注文の詳細については、『Guidelines for Quoting Security Cloud control Products Ordering Guide』を参照してください。購入方法については、シスコの購入案内のページを参照してください。

表 2. テナント権限の Security Cloud Control XaaS ライセンスのファイアウォール管理/マルチクラウド防御

製品番号	説明
CDO-SEC-SUB	SCC ファイアウォール/マルチクラウド防御 XaaS サブスクリプション

表 3. Security Cloud Control 基本ライセンス サブスクリプション テナント権限のファイアウォール管理/マルチクラウド防御：1 年、3 年、5 年のサブスクリプションが利用可能

製品番号	説明
CDO-BASE-LIC	SCC ファイアウォール/マルチクラウド防御の基本ライセンス サブスクリプション

表 4. ロギング権限付与のための SAL Saas logging and troubleshooting XaaS ライセンス

製品番号	説明
SAL-SUB	SAL Xaas サブスクリプション

表 5. シスコのファイアウォールを管理するための Firewall Management for Security Cloud Control ライセンス：1 年、3 年、5 年のサブスクリプションを利用可能

製品番号	説明
L-FPR1010-P=	ASA または FTD イメージを実行している FPR1010 の SCC ファイアウォール デバイス ライセンス
L-FPR1120-P=	ASA または FTD イメージを実行している FPR1120 の SCC ファイアウォール デバイス ライセンス
L-FPR1140-P=	ASA または FTD イメージを実行している FPR1140 の SCC ファイアウォール デバイス ライセンス
L-FPR1150-P=	ASA または FTD イメージを実行している FPR1150 の SCC ファイアウォール デバイス ライセンス
L-ASA5505-P=	ASA または FTD イメージを実行している ASA 5505 の SCC ファイアウォール デバイス ライセンス
L-ASA5506-P=	ASA または FTD イメージを実行している ASA 5506 の SCC ファイアウォール デバイス ライセンス
L-ASA5506W-P=	ASA または FTD イメージを実行している ASA 5506W の SCC ファイアウォール デバイス ライセンス
L-ASA5506H-P=	ASA または FTD イメージを実行している ASA 5506H の SCC ファイアウォール デバイス ライセンス
L-ASA5508-P=	ASA または FTD イメージを実行している ASA 5508 の SCC ファイアウォール デバイス ライセンス
L-ASA5512-P=	ASA または FTD イメージを実行している ASA 5512 の SCC ファイアウォール デバイス ライセンス
L-ASA5525-P=	ASA または FTD イメージを実行している ASA 5525 の SCC ファイアウォール デバイス ライセンス

製品番号	説明
L-ASA5545-P=	ASA または FTD イメージを実行している ASA 5545 の SCC ファイアウォール デバイス ライセンス
L-ASA5555-P=	ASA または FTD イメージを実行している ASA 5555 の SCC ファイアウォール デバイス ライセンス
L-ASA5585-P=	ASA または FTD イメージを実行している ASA 5585 の SCC ファイアウォール デバイス ライセンス
L-ASAV-P=	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）の SCC ファイアウォール デバイス ライセンス
L-FPRTD-V-P=	仮想 FTD（FTDv5/10/20/30/50/100）の SCC ファイアウォール デバイス ライセンス
L-FPR2110-P=	ASA または FTD イメージを実行している FPR 2110 の SCC ファイアウォール デバイス ライセンス
L-FPR2120-P=	ASA または FTD イメージを実行している FPR 2120 の SCC ファイアウォール デバイス ライセンス
L-FPR2130-P=	ASA または FTD イメージを実行している FPR 2130 の SCC ファイアウォール デバイス ライセンス
L-FPR2140-P=	ASA または FTD イメージを実行している FPR 2140 の SCC ファイアウォール デバイス ライセンス
L-FPR3105-P=	ASA または FTD イメージを実行している FPR 3105 の SCC ファイアウォール デバイス ライセンス
L-FPR3110-P=	ASA または FTD イメージを実行している FPR 3110 の SCC ファイアウォール デバイス ライセンス
L-FPR3120-P=	ASA または FTD イメージを実行している FPR 3120 の SCC ファイアウォール デバイス ライセンス
L-FPR3130-P=	ASA または FTD イメージを実行している FPR 3130 の SCC ファイアウォール デバイス ライセンス
L-FPR3140-P=	ASA または FTD イメージを実行している FPR 3140 の SCC ファイアウォール デバイス ライセンス
L-FPR4112-P=	ASA または FTD イメージを実行している FPR 4112 の SCC ファイアウォール デバイス ライセンス
L-FPR4115-P=	ASA または FTD イメージを実行している FPR 4115 の SCC ファイアウォール デバイス ライセンス
L-FPR4125-P=	ASA または FTD イメージを実行している FPR 4125 の SCC ファイアウォール デバイス ライセンス
L-FPR4145-P=	ASA または FTD イメージを実行している FPR 4145 の SCC ファイアウォール デバイス ライセンス
L-FPR4215-P=	ASA または FTD イメージを実行している FPR 4215 の SCC ファイアウォール デバイス ライセンス
L-FPR4225-P=	ASA または FTD イメージを実行している FPR 4225 の SCC ファイアウォール デバイス

製品番号	説明
	ライセンス
L-FPR4245-P=	ASA または FTD イメージを実行している FPR 4245 の SCC ファイアウォール デバイス ライセンス
L-FPR-9K-P=	ASA または FTD イメージを実行している FPR 9300 シリーズの SCC ファイアウォール デバイス ライセンス
L-ISA3000-P=	ASA または FTD イメージを実行している ISA 3000 の SCC ファイアウォール デバイス ライセンス
L-MX64-P=	Meraki MX64 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX65-P=	Meraki MX65 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX67-P=	Meraki MX67 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX84-P=	Meraki MX84 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX100-P=	Meraki MX100 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX250-P=	Meraki MX250 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-MX450-P=	Meraki MX450 プラットフォーム用 SCC ファイアウォール デバイス ライセンス
L-AWS-SG =	Amazon Web Services VPC セキュリティグループの SCC ファイアウォール デバイス ライセンス

表 6. 無制限のロギングと 90 日間の保持期間付き、Cisco ファイアウォールの管理用 SCC ファイアウォール デバイス ライセンス：1 年、3 年、5 年のサブスクリプションが利用可能。

製品番号	説明
CDO-ML-FP1010-LIC	FPR 1010 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP1010E-LIC	FPR 1010E ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP1120-LIC	FPR 1120 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP1140-LIC	FPR 1140 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP1150-LIC	FPR 1150 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP2110-LIC	FPR 2110 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP2120-LIC	FPR 2120 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP2130-LIC	FPR 2130 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP2140-LIC	FPR 2140 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP3105-LIC	FPR 3105 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP3110-LIC	FPR 3110 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス

製品番号	説明
CDO-ML-FP3120-LIC	FPR 3120 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP3130-LIC	FPR 3130 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP3140-LIC	FPR 3140 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4112-LIC	FPR 4112 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4115-LIC	FPR 4115 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4125-LIC	FPR 4125 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4145-LIC	FPR 4145 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4215-LIC	FPR 4215 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4225-LIC	FPR 4225 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FP4245-LIC	FPR 4245 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-F9K-S40-LIC	FPR 9K-SM40 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-F9K-S48-LIC	FPR 9K-SM48 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-F9K-S56-LIC	FPR 9K-SM56 ASA または FTD イメージのロギング付き SCC ファイアウォール デバイス ライセンス
CDO-ML-FTDV5-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（100Mbps）
CDO-ML-FTDV10-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（1Gbps）
CDO-ML-FTDV20-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（3Gbps）
CDO-ML-FTDV30-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（5Gbps）
CDO-ML-FTDV50-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（10Gbps）
CDO-ML-FTDV100-LIC	FTDV 基本ライセンスのロギング付き SCC ファイアウォール デバイス ライセンス（16Gbps）

表 7. 1 年、3 年、5 年のサブスクリプション付きの Cisco Logging and Troubleshooting が利用可能

製品番号	説明
SAL-CL-LT-1GB	License Logging and Troubleshooting（1GB/日）
SAL-CL-LT-OVRG	License Logging and Troubleshooting 用の使用量ベースの超過料金 PID。発注時には請求されませんが、使用資格が超過した場合の超過料金の計算に使用されます。
SEC-LOG-CL	90 日間のストレージ（GB/日）のクラウドロギング
SAL-CL-1GB-(1/2/3)Y-EXTN*	1 年、2 年、3 年のログ保持期間（デフォルトの 90 日から増加）。
SEC-CL-DR-(1/2/3)Y*	クラウドでのログ保持を 1 年、2 年、または 3 年に延長するデータ保持の拡張。
SAL-CL-LT-1GB	License Logging and Troubleshooting（1GB/日）

*ログの保持期間はオプションで 1、2、または 3 年に延長可能

セキュリティ購入プログラム

このオファーは、次の PID で セキュリティ エンタープライズ ライセンス契約購入プログラムを活用します：CDO、SAL（SaaS）アラカルト PID への Choice EA PID のマッピング。

表 8.

EA 2.0 ATO	EA 2.0 請求 PID	EA 3.0 ATO	EA 3.0 請求 PID	アラカルト履行 PID
E2F-SEC-CDO	E2SF-O-CDO55s08P	E3-SEC-CDO	E3S-CDO5508P	L-ASA5508-P=
E2F-SEC-CDO	E2SF-O-CDO5516P	E3-SEC-CDO	E3S-CDO5516P	L-ASA5516-P=
E2F-SEC-CDO	E2SF-O-CDO5525P	E3-SEC-CDO	E3S-CDO5525P	L-ASA5525-P=
E2F-SEC-CDO	E2SF-O-CDO5545P	E3-SEC-CDO	E3S-CDO5545P	L-ASA5545-P=
E2F-SEC-CDO	E2SF-O-CDO5555P	E3-SEC-CDO	E3S-CDO5555P	L-ASA5555-P=
E2F-SEC-CDO	E2SF-O-CDO-BASE	E3-SEC-CDO	E3S-O-CDO-BASE	CDO-BASE-LIC
E2F-SEC-CDO	E2SF-O-CDOFPR9K	E3-SEC-CDO	E3S-CDOFPR9K	L-FPR-9K-P=
E2F-SEC-CDO	E2SF-O-FPR1010-P	E3-SEC-CDO	E3S-CDOFPR1010-P	L-FPR1010-P=
E2F-SEC-CDO	E2SF-O-FPR1120-P	E3-SEC-CDO	E3S-CDOFPR1120-P	L-FPR1120-P=
E2F-SEC-CDO	E2SF-O-FPR1140-P	E3-SEC-CDO	E3S-CDOFPR1140-P	L-FPR1140-P=
E2F-SEC-CDO	E2SF-O-FPR1150-P	E3-SEC-CDO	E3S-CDOFPR1150-P	L-FPR1150-P=
E2F-SEC-CDO	E2SF-O-FPR2110-P	E3-SEC-CDO	E3S-CDOFPR2110-P	L-FPR2110-P=
E2F-SEC-CDO	E2SF-O-FPR2120-P	E3-SEC-CDO	E3S-CDOFPR2120-P	L-FPR2120-P=
E2F-SEC-CDO	E2SF-O-FPR2130-P	E3-SEC-CDO	E3S-CDOFPR2130-P	L-FPR2130-P=
E2F-SEC-CDO	E2SF-O-FPR2140-P	E3-SEC-CDO	E3S-CDOFPR2140-P	L-FPR2140-P=
E2F-SEC-CDO	E2SF-O-FPR3110-P	E3-SEC-CDO	E3S-CDOFPR3110-P	L-FPR3110-P=
E2F-SEC-CDO	E2SF-O-FPR3120-P	E3-SEC-CDO	E3S-CDOFPR3120-P	L-FPR3120-P=
E2F-SEC-CDO	E2SF-O-FPR3130-P	E3-SEC-CDO	E3S-CDOFPR3130-P	L-FPR3130-P=
E2F-SEC-CDO	E2SF-O-FPR3140-P	E3-SEC-CDO	E3S-CDOFPR3140-P	L-FPR3140-P=
E2F-SEC-CDO	E2SF-O-FPR4110-P	E3-SEC-CDO	E3S-CDOFPR4110-P	L-FPR4110-P=
E2F-SEC-CDO	E2SF-O-FPR4112-P	E3-SEC-CDO	E3S-CDOFPR4112-P	L-FPR4112-P=
E2F-SEC-CDO	E2SF-O-FPR4115-P	E3-SEC-CDO	E3S-CDOFPR4115-P	L-FPR4115-P=
E2F-SEC-CDO	E2SF-O-FPR4120-P	E3-SEC-CDO	E3S-CDOFPR4120-P	L-FPR4120-P=

EA 2.0 ATO	EA 2.0 請求 PID	EA 3.0 ATO	EA 3.0 請求 PID	アラカルト履行 PID
E2F-SEC-CDO	E2SF-O-FPR4125-P	E3-SEC-CDO	E3S-CDOFPR4125-P	L-FPR4125-P=
E2F-SEC-CDO	E2SF-O-FPR4140-P	E3-SEC-CDO	E3S-CDOFPR4140-P	L-FPR4140-P=
E2F-SEC-CDO	E2SF-O-FPR4145-P	E3-SEC-CDO	E3S-CDOFPR4145-P	L-FPR4145-P=
E2F-SEC-CDO	E2SF-O-FPR4150-P	E3-SEC-CDO	E3S-CDOFPR4150-P	L-FPR4150-P=
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-1Y	E3-SEC-SAL-LT	E3S-SALLT-STG-1Y	SAL-CL-1GB-1Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-2Y	E3-SEC-SAL-LT	E3S-SALLT-STG-2Y	SAL-CL-1GB-2Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-3Y	E3-SEC-SAL-LT	E3S-SALLT-STG-3Y	SAL-CL-1GB-3Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SAL-ESS	E3-SEC-SAL-LT	E3S-SAL-LT	SAL-CL-LT-1GB

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

Cisco Defense Orchestrator：詳細情報

Firewall Management Center：詳細情報

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-736847-16 11/24