データシート

Cisco Public

Cisco Security Cloud Control for Government データシート

© 2025 Cisco and/or its affiliates. All rights reserved.

目次

© 2025 Cisco and/or its affiliates. All rights reserved.

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、実用的なインサイトによりエンドユーザーの生産性を向上させることで、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、高機能な Cisco Zero Trust により防御を強化し、明確で実用的なインサイトで脆弱性に対する保護を提供することを目指しています。

Security Cloud Control for Government

Security Cloud Control は、Cisco Security Cloud に対応したシスコの統合型クラウドネイティブ セキュリティ管理インターフェイスです。セキュリティソリューションを単一の一貫したインターフェイスに集約することで、防御を簡素化し、強化します。このアプローチにより、サイロが解消され、複雑さが軽減され、エンドツーエンドの可視性が提供されます。その結果、組織はインフラストラクチャ全体でセキュリティの脅威に積極的に対処できるようになります。

Security Cloud Control for Government は、以下全体の管理を統合します。

- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Secure Firewall Adaptive Security Appliance（ASA）（オンプレミスと仮想）
- Cisco Multicloud Defense for Government

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）および Adaptative Security Appliance（ASA）に拡張されます。

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

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。

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、これらの成果をもたらすことができます。Security Cloud Control は、インテントベースのポリシーを 1 ヵ所で取得し、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。

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。
- **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。
- **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。

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。

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

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。

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。

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

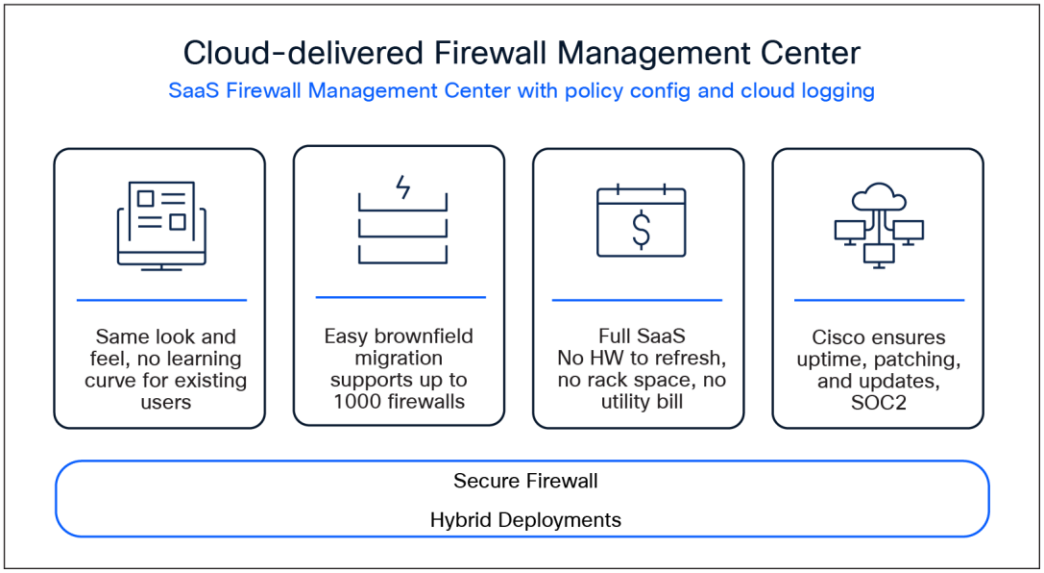

図 1.
Security Cloud Control for Government を介したクラウド提供型 Firewall Management Center の利点。

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

Multicloud Defense for Government の詳細については、製品 Web ページ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。
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	• 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

© 2025 Cisco and/or its affiliates. All rights reserved.

目的	実現方法
更のオプション	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。
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。
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。

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）

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、Adaptive Security Appliance（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 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。

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 Adaptive Security Appliance（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

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

© 2025 Cisco and/or its affiliates. All rights reserved.

プラットフォーム サポート マトリックス：Security Cloud Control for Government がサポートす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
Cisco Firepower 1010、1120、1140、1150	9.8 以降	7.0.3 以降（7.1 を除く）
Cisco Firepower 2110、2120、2130、2140	9.8 以降	7.0.3 以降（7.1 を除く）
Cisco Firepower 3105、3110、3120、3130、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
Cisco Firepower 4112、4115、4125、4145	9.4 以降	7.0.3 以降（7.1 を除く）
Cisco Firepower 4215、4225、4245	9.20 以降	7.4 以降
Cisco Firepower 9300	9.4 以降	7.0.3 以降（7.1 を除く）
Secure Firewall Threat Defense 仮想（FTDv）：KVM、VMware、および Azure	該当なし	7.0.3 以降（7.1 を除く）

発注およびプロビジョニング情報

Security Cloud Control Firewall Management for Governmentの発注手順の詳細については、『Security Cloud Control Firewall Management for Government 発注ガイド』を参照してください。

注文を行うには、シスコの注文ホームページをご覧ください。

Security Cloud Control Firewall Management for Government ライセンス SKU

表 2.

製品番号	説明
FWM-FED-SEC-SUB	Cisco Security Cloud Control Firewall Management for Government サブスクリプション
FWM-FED-BASE	基本テナントエンタイトルメント：12 ～ 60 ヵ月のサブスクリプションが利用可能
無制限のロギングストレージおよび 90 日間の保持期間を含むクラウド管理ライセンス	
FWM- FED-ML-FP1010	ASA または FTD イメージを実行している FPR1010 のクラウド管理およびロギング
FWM- FED-ML-FP1010E	ASA または FTD イメージを実行している FPR1010E のクラウド管理およびロギング
FWM-FED-ML-FP1120	ASA または FTD イメージを実行している FPR1120 のクラウド管理およびロギング

© 2025 Cisco and/or its affiliates. All rights reserved.

製品番号	説明
FWM-FED-ML-FP1140	ASA または FTD イメージを実行している FPR1140 のクラウド管理およびロギング
FWM-FED-ML-FP1150	ASA または FTD イメージを実行している FPR1050 のクラウド管理およびロギング
FWM-FED-ML-1210CE	ASA または FTD イメージを実行している FPR1210CE のクラウド管理およびロギング
FWM-FED-ML-1210CP	ASA または FTD イメージを実行している FPR1210CP のクラウド管理およびロギング
FWM-FED-ML-1220CX	ASA または FTD イメージを実行している FPR1220CX のクラウド管理およびロギング
FWM-FED-ML-1230	ASA または FTD イメージを実行している FPR1230 のクラウド管理およびロギング
FWM-FED-ML-1240	ASA または FTD イメージを実行している FPR1240 のクラウド管理およびロギング
FWM-FED-ML-1250	ASA または FTD イメージを実行している FPR1250 のクラウド管理およびロギング
FWM-FED-ML-FP2110	ASA または FTD イメージを実行している FPR2110 のクラウド管理およびロギング
FWM-FED-ML-FP2120	ASA または FTD イメージを実行している FPR2120 のクラウド管理およびロギング
FWM-FED-ML-FP2130	ASA または FTD イメージを実行している FPR2130 のクラウド管理およびロギング
FWM-FED-ML-FP2140	ASA または FTD イメージを実行している FPR2140 のクラウド管理およびロギング
FWM-FED-ML-FP3105	ASA または FTD イメージを実行している FPR3105 のクラウド管理およびロギング
FWM-FED-ML-FP3110	ASA または FTD イメージを実行している FPR3110 のクラウド管理およびロギング
FWM-FED-ML-FP3120	ASA または FTD イメージを実行している FPR3120 のクラウド管理およびロギング
FWM-FED-ML-FP3130	ASA または FTD イメージを実行している FPR3130 のクラウド管理およびロギング
FWM-FED-ML-FP3140	ASA または FTD イメージを実行している FPR3140 のクラウド管理およびロギング
FWM-FED-ML-FP4112	ASA または FTD イメージを実行している FPR4112 のクラウド管理およびロギング
FWM-FED-ML-FP4115	ASA または FTD イメージを実行している FPR4115 のクラウド管理およびロギング
FWM-FED-ML-FP4125	ASA または FTD イメージを実行している FPR4125 のクラウド管理およびロギング
FWM-FED-ML-FP4145	ASA または FTD イメージを実行している FPR4145 のクラウド管理およびロギング
FWM-FED-ML-FP4215	ASA または FTD イメージを実行している FPR 4215 のクラウド管理およびロギング
FWM-FED-ML-FP4225	ASA または FTD イメージを実行している FPR 4225 のクラウド管理およびロギング
FWM-FED-ML-FP4245	ASA または FTD イメージを実行している FPR 4245 のクラウド管理およびロギング
FWM-FED-ML-F9K-S40	ASA または FTD イメージを実行している FPR9K-SM40 のクラウド管理およびロギング
FWM-FED-ML-F9K-S48	ASA または FTD イメージを実行している FPR9K-SM48 のクラウド管理およびロギング
FWM-FED-ML-F9K-S56	ASA または FTD イメージを実行している FPR9K-SM56 のクラウド管理およびロギング

© 2025 Cisco and/or its affiliates. All rights reserved.

製品番号	説明
FWM-FED-ML-FTDV5	FTDV 基本ライセンスのクラウド管理およびロギング、100Mbps
FWM-FED-ML-FTDV10	FTDV 基本ライセンスのクラウド管理およびロギング、1Gbps
FWM-FED-ML-FTDV20	FTDV 基本ライセンスのクラウド管理およびロギング、3Gbps
FWM-FED-ML-FTDV30	FTDV 基本ライセンス、5Gbps用のクラウド管理およびロギング
FWM-ML-FTDV50	FTDV 基本ライセンスのクラウド管理およびロギング、10Gbps
FWM-FED-ML-FTDV100	FTDV 基本ライセンス、16Gbps用のクラウド管理およびロギング

表 3. 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-FED-SUB	SAL XaaS サブスクリプション
Security Analytics サブスクリプション（1 年、3 年、および 5 年）	
SAL-FED-SUB	Cisco Security and Analytics and Logging for Government
SAL-FED-ESS-1YR/2YR/3YR	Cisco Security and Analytics and Logging for Government Essentials 階層（ログの保持期間は 1 年、2 年、または 3 年）。
SAL-FED-PRE-1YR/2YR/3YR	Cisco Security and Analytics and Logging for Government Premium 階層 ログの保持期間は 1 年、2 年、または 3 年です。
SVS-SAL-FED-SUP-S	Cisco Security and Analytics and Logging for Government の基本サポート

表 4. Firewall Management in Security Cloud Control：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
FWM-FED-FPR1010	ASA または FTD イメージを実行している FPR1010 のクラウド管理
FWM-FED-FPR1120	ASA または FTD イメージを実行している FPR1120 のクラウド管理
FWM-FED-FPR1140	ASA または FTD イメージを実行している FPR1140 のクラウド管理
FWM-FED-FPR1150	ASA または FTD イメージを実行している FPR1150 のクラウド管理
FWM-FED-FPRTD-V=	Virtual FTD のクラウド管理（FTDv5/10/20/30/50/100）
FWM-FED-FPR2110	ASA または FTD イメージを実行する FPR 2110 のクラウド管理
FWM-FED-FPR2120	ASA または FTD イメージを実行する FPR 2120 のクラウド管理
FWM-FED-FPR2130	ASA または FTD イメージを実行する FPR 2130 のクラウド管理
FWM-FED-FPR2140	ASA または FTD イメージを実行する FPR 2140 のクラウド管理
FWM-FED-FPR3105	ASA または FTD イメージを実行する FPR 3105 のクラウド管理

© 2025 Cisco and/or its affiliates. All rights reserved.

製品番号	説明
FWM-FED-FPR3110	ASA または FTD イメージを実行する FPR 3110 のクラウド管理
FWM-FED-FPR3120	ASA または FTD イメージを実行する FPR 3120 のクラウド管理
FWM-FED-FPR3130	ASA または FTD イメージを実行する FPR 3130 のクラウド管理
FWM-FED-FPR3140	ASA または FTD イメージを実行する FPR 3140 のクラウド管理
FWM-FED-FPR4112	ASA または FTD イメージを実行している FPR 4112 のクラウド管理
FWM-FED-FPR4115	ASA または FTD イメージを実行している FPR 4115 のクラウド管理
FWM-FED-FPR4125	ASA または FTD イメージを実行している FPR 4125 のクラウド管理
FWM-FED-FPR4145	ASA または FTD イメージを実行している FPR 4145 のクラウド管理
FWM-FED-FPR4215	ASA または FTD イメージを実行している FPR 4215 のクラウド管理
FWM-FED-FPR4225	ASA または FTD イメージを実行している FPR 4225 のクラウド管理
FWM-FED-FPR4245	ASA または FTD イメージを実行している FPR 4245 のクラウド管理
FWM-FED-FPR9K	ASA または FTD イメージを実行する FPR 9300シリーズのクラウド管理

注：表 3 に記載されているPIDはすべて、1年、3年、および5年のサブスクリプションPIDで利用できます。例：FWM-FED-FPR4225 は、FWM-FED-FPR4225-1Y、FWM-FED-FPR4225-2Y、および FWM-FED-FPR4225-3Y として使用できます。

関連リソース

Cisco Security Cloud Control Web ページ

Cisco Secure Firewall Management Center Web ページ

Cisco Secure Firewall Web ページ

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。

Cisco および Cisco 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国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

Printed in USA C78-736847-17 09/25

© 2025 Cisco and/or its affiliates. All rights reserved.