# Cisco Secure Firewall Management Center（旧称 Firepower Management Center）

# 目次

## 連携するセキュリティ

Cisco Secure Firewall Management Center（FMC）は、重要なシスコのネットワーク セキュリティ ソリューションを管理するための管理中枢となります。ファイアウォール、アプリケーション制御、侵入防御、URL フィルタリング、および高度なマルウェア防御を完全に統合して管理します。ファイアウォールの管理からアプリケーションの制御、マルウェアの感染の調査および修復まで、迅速かつ簡単に進めることができます。これは広範かつ統合された Cisco Secure ポートフォリオの中でも重要な部分を占め、詳細な分析、ネットワークとクラウド全体のセキュリティ管理の合理化、およびインシデントの調査と対応の迅速化を、シスコとサードパーティのテクノロジー全体で実現します。

## 包括的な可視性とポリシー制御

- 優れた可視性によってネットワークとクラウドで何が実行されているかを把握し、保護が必要な対象を確認できます。
- 疑わしい/悪意のあるトラフィックを迅速に検出し、攻撃の進行を防ぐためのカスタムルールを迅速に作成します。
- フォレンジック機能が組み込まれているため、マルウェアを詳細に分析して安全に修復することができ、攻撃による影響を受けたすべてのデバイスがグラフ形式で表示されます。
- ファイアウォールルールを作成し、環境内で使用される数千もの商用アプリケーションとカスタムアプリケーションを制御します。
- Cisco Secure Workload とコンテキストを共有することで、ネットワーク内のファイアウォールが「ワークロード対応」になり、環境内のあらゆる場所で動的アプリケーションをより適切に保護できるようになります。
- 侵入防御レベル、URL レピュテーションルール、およびマルウェア脅威防御ポリシーを定義します。たとえば、「ファイルが添付されているネットワークトラフィックが、この特定のアプリケーションを使用して特定の国から送信されている場合、このレベルの侵入検査を適用してファイルにマルウェアが含まれていないかを分析して、必要に応じてファイルを統合サンドボックスに送信する」などによって問題を解決します。

## 動的な防御のための自動セキュリティ

Firewall Management Center は、ネットワークの変化を継続的にモニターします。以下の機能により、運用を合理化してセキュリティを改善できます。

- 新たな攻撃イベントとネットワークの脆弱性を自動的に関連付けおよび優先順位付けし、成功した可能性がある攻撃について通知します。セキュリティチームは最も重要なイベントに集中できます。
- ネットワークの脆弱性を分析して、導入すべき適切なセキュリティポリシーを自動的に推奨します。変化する状況に合わせて防御を適応させ、ネットワークに合わせて調整されたセキュリティ対策を実施できます。
- ネットワーク、エンドポイント、侵入、およびセキュリティ インテリジェンスのソースから特定のイベントを関連付けます。個々のホストに未知の攻撃による侵害の兆候が現れると、通知が送信されます。
- ファイルポリシーの条件を適用します。条件を満たすと、自動的にファイルを分析して既知のマルウェアを特定するか、必要に応じて統合サンドボックスにファイルを送信して未知のマルウェアを特定します。

## イベントおよびポリシーの一元的なマネージャ

Firewall Management Center は、次のイベントおよびポリシーの一元的なマネージャです。

- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Secure IPS（旧称 Firepower NGIPS）
- Cisco Firepower Threat Defense for ISR
- Cisco Malware Defense（旧称 Advanced Malware Protection、AMP）

### エンタープライズクラスの管理

Firewall Management Center（FMC）は、ネットワークのリソースおよび操作の変更に関するリアルタイム情報を検出します。情報に基づいて判断を行うための豊富なコンテキスト情報が得られます（図 1）。広範なインテリジェンスに加えて、FMC は次のような詳細情報も提供します。

- **傾向と概要レベルの統計。**この情報は、特定の時点でのセキュリティ態勢と、その変化（改善や悪化）を把握するために役立ちます。
- **イベントの詳細、コンプライアンス、およびフォレンジック。** これらにより、セキュリティイベント中に何が発生したかを把握できます。これらは、防御の改善、侵害の封じ込めの取り組みの支援、および法的な適用措置の支援に役立ちます。
- **ワークフローデータ。**このデータを他のソリューションに簡単にエクスポートして、インシデント対応の管理を改善できます。
- **リアルタイムのデバイスヘルスモニタリング。** 統合された概要ビューから、またはカスタマイズ可能な詳細なステータスページを介して、デバイスのステータスをすばやく確認できます（図 2）。

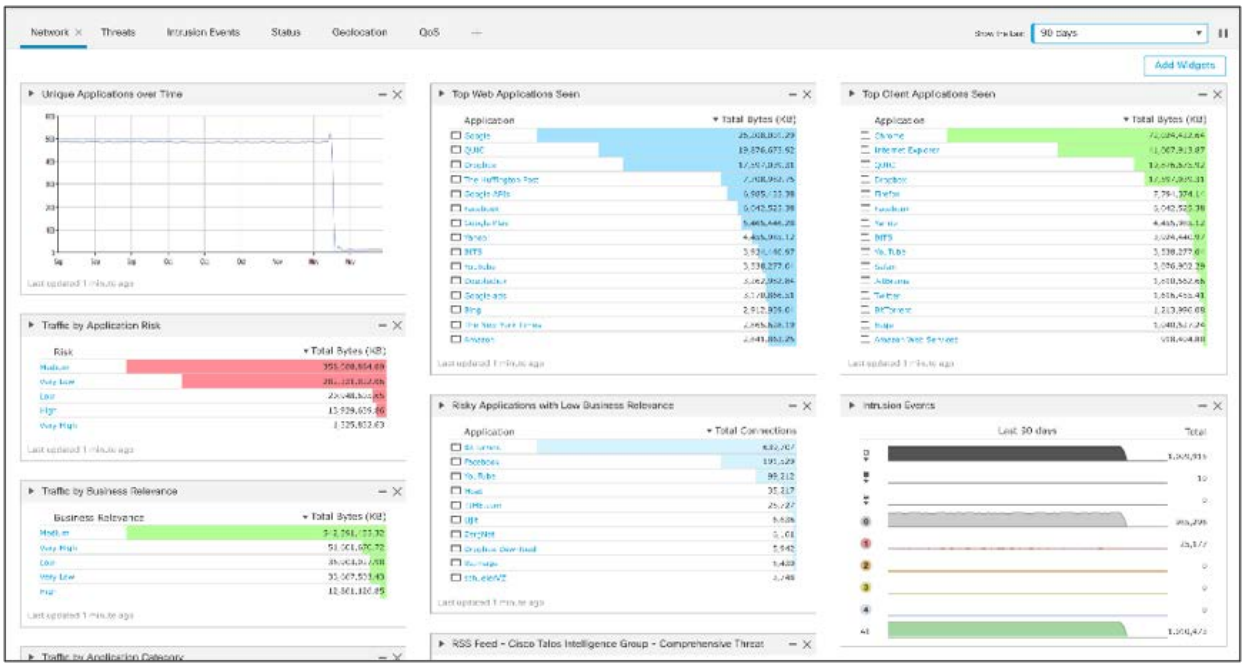


**図 1.**
コンテキストネットワークとセキュリティ情報

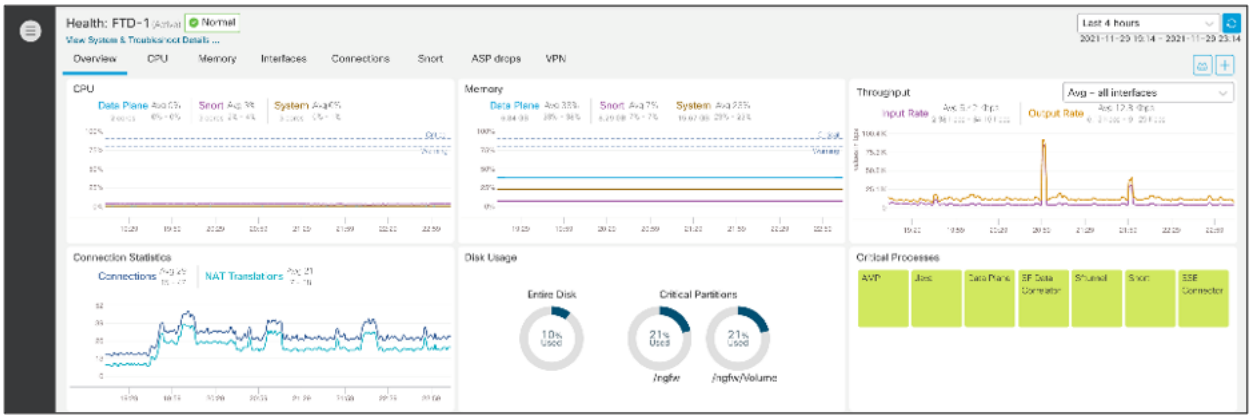


**図 2.**
リアルタイムのデバイスヘルスモニター

## 一元化されたポリシーと運用

- **一貫したポリシーを維持する：**ポリシーを一度作成するだけで、ネットワーク全体の複数のセキュリティ管理にわたって一貫した適用を拡張できます。
- **複雑さの軽減：**アプリケーションのファイアウォール、次世代の侵入防御、ファイルとマルウェアの保護など、緊密に統合されたセキュリティ機能全体で、統合された管理と自動化された脅威の関連付けを実現します。
- **主要なセキュリティ運用機能の高速化：**手動プロセスを排除して効率を向上させます。わずか数回クリックするだけでソフトウェアのアップグレードが完了するため、セキュリティパッチや新機能にすばやくアクセスできます。

# 機能と利点

| 機能 | 利点 |
|---|---|
| **複数のソリューションにわたる複数のセキュリティ機能の統合管理** | 次を含むシスコのセキュリティ環境の中央管理を促進します。<br>• Cisco Secure Firewall Threat Defense<br>• Cisco Secure IPS<br>• Cisco Firepower Threat Defense for ISR<br>• Cisco Malware Defense |
| **複数のセキュリティ機能に対する統合ポリシー管理** | • 単一のポリシーでファイアウォールアクセス、アプリケーション制御、侵入防御、URL フィルタリング、および高度なマルウェア防御の設定を設定します。<br>• ポリシー管理を容易にし、エラーを減らし、一貫性を促進します。<br>• 単一のポリシーを複数のセキュリティソリューションに展開できるようにします。 |
| **ネットワーク検出** | • ネットワークトラフィックのパッシブ分析を通じて、ユーザー、アプリケーション、および多数のデバイスを検出します。<br>• コンテキストを提供し、特定の環境に対する攻撃の影響を判断できるように支援します。<br>• ネットワーク上で検出されたシステムに合わせて侵入防御シグネチャセットを調整できるようにします。<br>• サードパーティの脆弱性管理統合をサポートします。 |

| 機能 | 利点 |
| --- | --- |
| **職務の分離と役割ベースのアクセス制御** | • NetOps や SecOps などの管理ユーザーのペルソナを作成して、責任を明確に定義します。<br>• 詳細な役割ベースのアクセス制御により、ユーザーに自分が担当するアクションのみを実行するための、特定のアクセス権を与えることができます。 |
| **Cisco Identify Services Engine（ISE）による統合アクセスポリシー制御** | • Cisco ISE セキュリティグループタグ、デバイスタイプ、ロケーション IP に基づいてアクセスを制御し、迅速に脅威を封じ込めます。<br>• コンプライアンス施行、インフラストラクチャのセキュリティ強化、およびサービス運用の合理化を支援します。 |
| **自動セキュリティ応答** | • セキュリティイベントを関連付けて、ステルス攻撃を特定します。<br>• 次の方法で自動応答をトリガーします。<br>◦ E メール<br>◦ Syslog<br>◦ SNMP<br>◦ 修復モジュール |
| **Cisco Secure 動的属性コネクタ** | • IP アドレスとワークロードが常に変化している場合に、変更を再デプロイすることなく、自動化されたプログラムを使った方法でポリシーを管理できるようにします。<br>• セキュリティポリシーを最新の状態に保つために必要な管理オーバーヘッドを大幅に削減します。<br>• AWS、Azure、VMWare、Office 365 タグで機能します。 |
| **脅威インテリジェンス** | • シスコの Talos® グループのセキュリティ、脅威、および脆弱性のインテリジェンスを統合し、最新の脅威防御を実現します。<br>• IP ベースと URL ベースの両方のセキュリティ インテリジェンスにより新しい攻撃方法に対応します。<br>• STIX/TAXII またはフラットファイル形式で、サードパーティの脅威フィードおよび脅威インテリジェンス プラットフォームからの脅威インテリジェンスの取り込みと関連付けができます。 |
| **アプリケーションの可視化と制御** | • 数千もの商用アプリケーションを正確に制御することで、ネットワークに対する脅威をさらに軽減します。<br>• カスタムアプリケーションの詳細な識別と制御のために、オープンソースの標準 Open App ID を使用します。 |
| **マルチテナントの管理とポリシーの継承** | • 個別のイベントデータ、レポート、およびネットワークマッピングを使用して最大 100 個の管理ドメインを作成し、ロールベースのアクセス制御によって適用します。<br>• 各レベルが上のレベルのポリシーを継承するポリシーの階層構造により、一貫性のある効率的な管理を導入します。 |
| **Cisco Security Analytics and Logging（SAL）の統合** | • 拡張性が高く直感的に操作可能な単一ビューでファイアウォールのログを管理します。<br>• 行動分析によりリアルタイムの脅威検出が実現し、応答時間が短縮されます。<br>• 継続的な分析により、セキュリティ態勢がさらに洗練され、将来の攻撃に対する防御が強化されます。 |
| **SecureX との統合** | • SecureX ™ プラットフォームを活用して、脅威の検出、オーケストレーション、および修復を加速します。<br>• すべての Secure Firewall には、Cisco SecureX の権限が含まれています。<br>• Firewall Management Center の新しい SecureX リボンにより、SecOps は SecureX のオープンプラットフォームに即座に視点を移すことができるようになり、インシデント対応が迅速化されます。 |
| **Cisco Secure Workload との統合** | • Cisco Secure Workload（旧称 Tetration）との統合により、ネットワーク全体およびワークロード全体にわたる最新の分散型動的アプリケーションの包括的な可視性とポリシー適用が可能になり、スケーラブルな方法による一貫した適用が実現します。 |

| 機能 | 利点 |
| --- | --- |
| **レポートとダッシュボード** | • カスタムおよびテンプレートベースのレポートを使用して、カスタマイズ可能なダッシュボードで必要な可視性を提供します。<br>• 一般情報と特定情報の両方に対応する包括的なアラートおよびレポートを提供します。<br>• 使いやすい分析のために、ハイパーリンクテーブル、グラフ、およびチャートにイベント情報とコンテキスト情報が表示されます。<br>• ネットワークの動作とパフォーマンスをモニターして異常を特定し、システムの正常性を維持します。 |
| **セキュアブート** | • セキュアブートは、システムの起動時に FMC ハードウェアで実行されているシスコソフトウェアの完全性を検証するメカニズムです。<br>• 署名が欠落しているかソフトウェアが無効な場合、ソフトウェアはロードされず、起動は失敗します（ハードウェア FMC アプライアンスのみ） |

## オープン API による容易な統合

FMC では、強力で機能豊富なアプリケーション プログラミング インターフェイスを通じて、サードパーティテクノロジーとの統合が可能です。これらの API には、以下の操作を実行するための接続ポイントが用意されています。

- FMC のイベントデータを、セキュリティ情報イベント管理（SIEM）ソリューションなどの別のプラットフォームに移動します。
- Cisco IPS データベースに含まれる情報をサードパーティのデータで強化します。このようなデータには、脆弱性管理が含まれます。
- ユーザー定義の相関ルールで有効化されたワークフローと修復手順を開始します。たとえば、ワークフローをネットワーク アクセス コントロール（NAC）ソリューションと統合して、感染したエンドポイントを隔離したり、デジタル フォレンジック プロセスを開始したりできます。
- サードパーティのレポートおよび分析機能をサポートするために、これらのソリューションで FMC データベースに対してクエリを実行できるようにします。

これらの API を使用することで、シスコが提供する複数のセキュリティ製品およびワークフローとの統合も可能になります。このような製品には、サンドボックス機能を実現する Cisco Secure Malware Analytics（旧称 Cisco AMP Threat Grid）、アイデンティティデータやネットワークのセグメント化を実現する Cisco Identity Services Engine（ISE）、インターネット全体のドメインを可視化する Cisco Umbrella® などがあります。

Cisco Secure Technology Alliance は、オープンなマルチベンダー製品の統合を促進し、自動化と運用の簡素化を通じてセキュリティの有効性を向上させるセキュリティエコシステムです。シスコは、数百もの主要なセキュリティベンダーと積極的に提携しており、10 を超えるシスコセキュリティ製品と統合しています。最新のリストを表示するには、「Cisco Secure Technical Alliance Partners」にアクセスしてください。

## Cisco SecureX

Cisco SecureX は広範なシスコの統合型セキュリティポートフォリオとお客様のセキュリティ インフラストラクチャ全体とをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティが強化されます。その結果、すでにお持ちのソリューションに組み込む形でセキュリティの簡素化が実現します。

SecureX の脅威対応機能（旧称 CTR）は、Cisco Talos およびサードパーティの脅威インテリジェンスを統合して、オブザーバブルとも呼ばれる侵害の兆候（IOC）を自動的に調査して素早く脅威を確認します。

Secure Firewall のお客様の場合、ファイアウォール管理センター (FMC) の SecureX リボンを使用すると、管理者は瞬時に視点を切り替えることができるため、より深い脅威の調査を行い、インシデントに関するコンテキストの共有と維持ができるようになります。

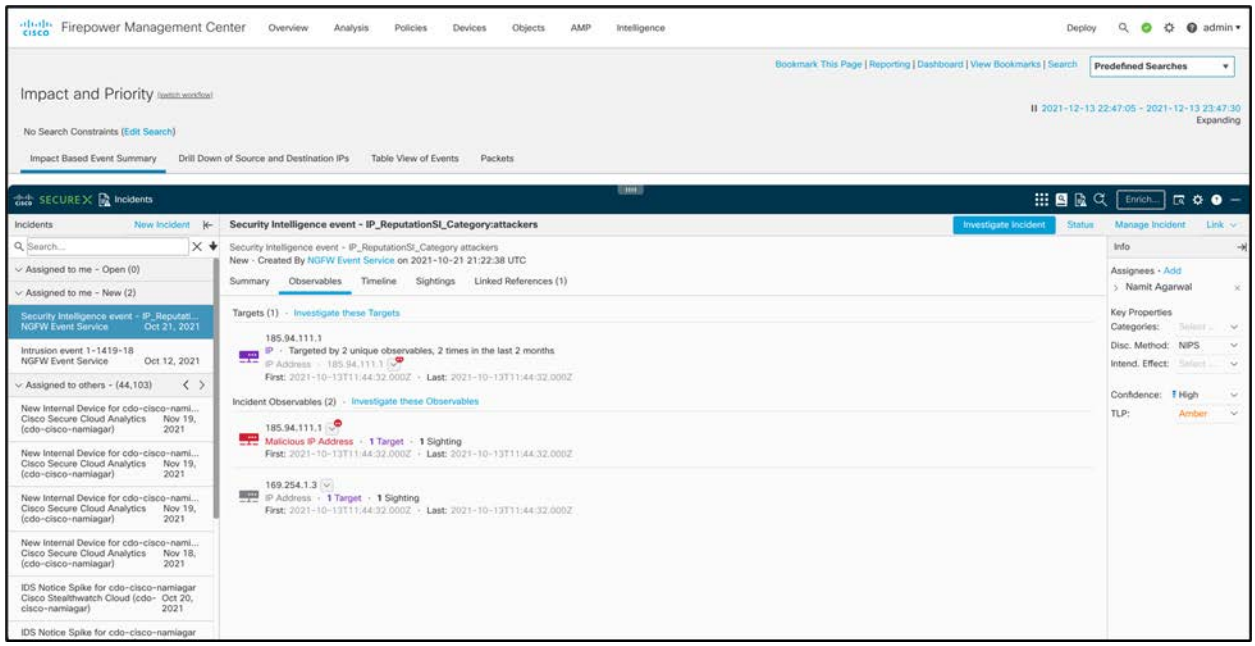


**図 3.**
FMC の SecureX

監視可能なアクション、修復、インシデントエンドポイントの強化の一般的なユースケースについて紹介する、「事前構築済みのワークフロープレイブック」を参照してください。

## 動作の仕組み

Cisco ファイアウォールでは、セキュアな中間クラウドサービスを使用してデータを SecureX に送信します。SecureX Threat Response は、調査対象の IP アドレスに関する検出情報を照会し、アナリストに追加のコンテキストを提供します。Cisco Talos のレピュテーションやユーザー定義フィルタに基づいて、侵入イベントはインシデント管理者の調査対象インシデントに昇格されます。これにより、チームは迅速にインシデントの調査とトリアージを実施し、侵入イベントの分析を確認することができます。

SecureX Orchestrator は FMC API 呼び出しを呼び出すことができるため、管理者はルーチンの FMC タスクを自動化し、効率を向上させることができます。SecureX は、Cisco Secure Firewall および/または Cisco Secure 製品を使用しているお客様向けの標準仕様として利用できます。

## 展開オプション

FMC は、物理アプライアンスまたは仮想アプライアンスとして導入するか、クラウドから導入できます。また、サービスとして使用することもできます。クラウド提供の FMC は、CDO を介して、FMC のすべての利点を利用できます。FMC ソフトウェアのアップデート自体を管理する必要はありません。環境に最適な導入方法を選択できます。詳細については、最新のリリースノートを参照してください。

## ハイパーバイザの互換性とクラウドサポート

Firewall Management Center Virtual は、以下に示すハイパーバイザタイプをサポートしています。FMC Virtual プラットフォームのすべてのモデルは、同じ RAM 要件で動作します（推奨：32 GB、必須：28 GB）。サポートされている現行バージョンおよび FMC バージョンとの互換性については、最新のリリースノートを参照してください。

**表 1.** 仮想アプライアンスのハイパーバイザとクラウドサポート

| ハイパーバイザ | バージョンおよび詳細 |
|---|---|
| **VMware vSphere** | • ESXi サーバー 5.1、5.5、6.0、6.5、6.7、7.0<br>• vCenter Server（オプション）<br>• Windows または LinuxC 向けの vSphere Web クライアント、vSphere クライアント、または OVF ツール |
| **KVM** | • Ubuntu 18.04 LTS<br>• Red Hat Enterprise Linux（RHEL）バージョン 7.1 |
| **ConAmazon Web Services** | • c3.4xlarge：16 個 の vCPU、30 GB<br>• c4.4xlarge：16 個の vCPU、30 GB<br>• c5.4xlarge：16 個の vCPU、32 GB |
| **Microsoft Azure** | Standard_D4_v2：8 個の vCPU、28 GB |
| **GCP** | c2-standard-8：8 個の vCPU、32 GB<br>c2-standard-16：16 個の vCPU、64 GB |
| **OCI** | VM.Standard 2.4、60 GB |
| **Nutanix** | Nutanix AHV（20201105.12 以降） |
| **HyperFlex** | リリース 4.5（1a）<br>FMCv-2、10、25 の場合は、4 ~ 8 個の vCPU、28 ~ 32 GB<br>FMCv-300 の場合は、32 個の vCPU、64 GB |

**注：** 詳細については、『Cisco Firepower Management Virtual Getting Started Guide』を参照してください。

# プラットフォームの仕様

Firewall Management Center にはいくつかのモデルがあります。モニター対象のセンサーアプライアンス（物理と仮想の両方）の数、環境内のホストの数、および予想されるセキュリティイベントレートに応じてお選びください（表 3 を参照）。管理機能はすべてのモデルで共通です。

表 2 は、利用可能な Cisco Firewall Management Center の物理アプライアンスのキャパシティを比較したものです。

**表 2.** Cisco Firewall Management Center Firepower のハードウェアモデル

| 性能と機能 | FMC 1600 | FMC 2600 | FMC 4600 | FMC 1700 | FMC 2700 | FMC 4700 |
|---|---|---|---|---|---|---|
| **管理できるセンサーの最大数** | 50 | 300 | 750 | 50 | 300 | 1,000 |
| **IPS イベントの最大数** | 3,000 万 | 6,000 万 | 3 億 | 3,000 万 | 6,000 万 | 4 億 |
| **管理インターフェイス** | 2 つの内蔵 RJ-45 SFP+ ポート：100 Mbps、1 Gbps、10 Gbps をサポートします。プライマリ管理ポートは eth0 です。eth1、eth2、および eth3 は、セカンダリ管理またはイベントポートとして使用できます。 | | | 2 つの内蔵 10GbE RJ45 OCP3.0 NIC：100 Mbps、1 Gbps、10 Gbps をサポートします。プライマリ管理ポートは eth0 です。eth1、eth2、および eth3 は、セカンダリ管理またはイベントポートとして使用できます。 | | |
| **USB ポート** | USB 3.0 タイプ A ポート X 2 | | | USB 3.0 タイプ A ポート X 2 | | |
| **VGA ポート** | 3 列 15 ピン DB-15 コネクタ X 1：デフォルトで有効 | | | 3 列 15 ピン DB-15 コネクタ X 1：デフォルトで有効 | | |
| **SFP ポート** | 固定 SFP+ ポート X 2 | | | 固定 SFP+ ポート X 2 | | |
| **サポートされた SFP+** | SFP-10G-SR（10 GB） | SFP-10G-SR（10 GB）<br>SFP-10G-LR（10 GB） | SFP-10G-SR（10 GB）<br>SFP-10G-LR（10 GB） | SFP-10G-SR（10 GB）<br>SFP-10G-LR（10 GB） | SFP-10G-SR（10 GB）<br>SFP-10G-LR（10 GB） | SFP-10G-SR（10 GB）<br>SFP-10G-LR（10 GB）<br>SFP-25G-SR-S（25 GB）<br>SFP-10/25G-LR-S（25 GB）<br>SFP-10/25G-CSR-S（25 GB） |
| **メモリ** | 32 GB | 64 GB | 128 GB | 32 GB | 64 GB | 128 GB |
| **RDIMM（内部コンポーネントのみ、フィールド交換不可）** | 16-GB DDR4-2400 MHz DIMM X 2 | 16-GB DDR4-2400 MHz DIMM X 4 | 16-GB DDR4-2400 MHz DIMM X 8 | 16-GB DDR4-3200 MHz DIMM X 2 | 16-GB DDR4-3200 MHz DIMM X 4 | 16-GB DDR4-3200 MHz DIMM X 8 |
| **CPU** | Intel Xeon 4215 プロセッサ X 1 | Intel Xeon 4215 プロセッサ X 2 | Intel Xeon 4214 プロセッサ X 2 | 1P Rome 7232P、120 W | 1P：Rome 7282、120 W | 1P：Rome 7352、155 W |
| **イベント記憶域** | 900 GB | 1.8 TB | 3.2 TB | 900 GB | 1.8 TB | 3.2 TB |

| 性能と機能 | FMC 1600 | FMC 2600 | FMC 4600 | FMC 1700 | FMC 2700 | FMC 4700 |
|---|---|---|---|---|---|---|
| **最大ネットワークマップサイズ（ホスト/ユーザー）** | 550,000/50,000 | 150,000/150,000 | 600,000/600,000 | 550,000/50,000 | 150,000/150,000 | 600,000/600,000 |
| **最大イベントレート（イベント数/秒）** | 5000 eps | 12,000 eps | 20,000 eps | 5000 eps | 12,000 eps | 30,000 eps |
| **ネットワーク インターフェイス** | 2 x 1 Gbps | 2 X 1 Gbps RJ45 オンボード<br>2 X 10 Gbps SFP+（Cisco Commerce Workplace 経由で SFP を発注） | 2 X 1 Gbps RJ45 オンボード<br>2 X 10 Gbps SFP+（Cisco Commerce Workplace 経由で SFP を発注） | 2 X 1 Gbps RJ45 オンボード<br>2 X 10 Gbps SFP+（Cisco Commerce Workplace 経由で SFP を発注） | 2 X 1 Gbps RJ45 オンボード<br>2 X 10 Gbps SFP+（Cisco Commerce Workplace 経由で SFP を発注） | 2 X 1 Gbps RJ45 オンボード<br>2 X 10/25 Gbps SFP+（Cisco Commerce Workplace 経由で SFP を発注） |
| **セキュアブート** | 対応 | 対応 | 対応 | 対応 | 対応 | 対応 |
| **冗長性機能** | | | | | | |
| **ハイアベイラビリティのサポート** | 対応 | 対応 | 対応 | 対応 | 対応 | 対応 |
| **システム電源** | 770-W AC 電源装置 X 2、ホットスワップ可能および 1 + 1 冗長化 | | | 1050 W AC 電源装置 X 2、ホットスワップ可能および 1 + 1 冗長化 | | |
| **消費電力** | 2626 BTU/時 | | | 2626 BTU/時 | | |
| **ストレージ** | 1.2 TB 10-K SAS HDD X 2<br>RAID-1 X 10、ホットスワップ可能 | 600-GB 10-K SAS HDD X 4<br>RAID 5（ホットスワップ対応） | 1.2 TB 10-K SAS HDD X 10<br>RAID-6 X 10、ホットスワップ可能 | 1.2 TB 10-K SAS HDD X 2<br>RAID-1 X 10、ホットスワップ可能 | 600-GB 10-K SAS HDD X 4<br>RAID 5（ホットスワップ対応） | 1.2 TB 10-K SAS HDD X 10<br>RAID-6 X 10、ホットスワップ可能 |
| **RAID コントローラ** | 1 基：シャーシには、PCIe スタイルの Cisco モジュール型 RAID コントローラカード専用のライザを内蔵（内部コンポーネントのみ、フィールド交換不可） | | | 1 基：シャーシには、PCIe スタイルの Cisco モジュール型 RAID コントローラカード専用のライザを内蔵（内部コンポーネントのみ、フィールド交換不可） | | |
| **物理仕様および環境仕様** | | | | | | |
| **フォーム ファクタ** | 1 RU | 1 RU | 1 RU | 1 RU | 1 RU | 1 RU |
| **寸法（奥行 X 幅 X 高さ）** | 75.7 X 43 X 4.3 cm（29.8 X 16.9 X 1.7 インチ） | | | 76.2 X 42.9 X 4.3 cm（30 X 16.9 X 1.7 インチ） | | |
| **出荷時重量** | 16.6 kg（32.2 ポンド） | 16.8 kg（34.1 ポンド） | 17.0 kg（36 ポンド） | 16.6 kg（32.2 ポンド） | 16.8 kg（34.1 ポンド） | 17.0 kg（36 ポンド） |
| **ワット（最大）** | 770W | 770W | 770W | 1,050 W | 1,050 W | 1,050 W |

| 性能と機能 | FMC 1600 | FMC 2600 | FMC 4600 | FMC 1700 | FMC 2700 | FMC 4700 |
|---|---|---|---|---|---|---|
| **電源** | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.5 A<br>208 VAC で最大 4.5 A | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.5 A<br>208 VAC で最大 4.5 A | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.5 A<br>208 VAC で最大 4.5 A | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.2 A<br>230 VAC で最大 5.2 A | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.2 A<br>230 VAC で最大 5.2 A | 100 ~ 240 VAC（公称）<br>90 ~ 264 VAC（最小/最大）<br>100 VAC で最大 9.2 A<br>230 VAC で最大 5.2 A |
| **エアーフロー** | 前面から背面 | 前面から背面 | 前面から背面 | 前面から背面 | 前面から背面 | 前面から背面 |
| **動作温度** | 50 ~ 95°F（10 ~ 35°C） | | | 50 ~ 95°F（10 ~ 35°C） | | |

表 3 は、利用可能な Cisco Secure Firewall Management Center の仮想アプライアンスのキャパシティを比較したものです。

**表 3.** Cisco Firewall Management Center Virtual（FMCv）のモデル

| 性能と機能 | FMCv(2/10/25) | FMCv300 |
|---|---|---|
| **管理できるセンサーの最大数** | 2<br>10<br>25 | 300 |
| **IPS イベントの最大数** | 1,000 万 | 6,000 万 |
| **メモリ** | 32 GB | 64 GB |
| **CPU** | 8/4 vCPU | 32 vCPU |
| **イベント記憶域** | 250 GB | 2.2 TB |
| **最大ネットワークマップサイズ（ホスト/ユーザー）** | 50,000/50,000 | 150,000/150,000 |
| **最大イベントレート（イベント数/秒）** | 可変 | 12,000 eps |
| **ハイパーバイザとクラウドのサポート** | VMware、KVM、AWS、Azure、GCP、OCI、Nutanix、Hyperflex、OpenStack | VMware、AWS、OCI |
| **ハイアベイラビリティのサポート** | VMware、AWS、OCI（FMCv2 ではサポートされていません） | VMware、AWS、OCI |

クラウド提供型の FMC は、ニーズに合わせて拡張できます。互換性、サポートされているバージョン、展開、およびブラウザ要件の詳細については、リリースノートを参照してください。

## 発注情報

仮想および物理 アプライアンスおよびクラウド提供型サービスの注文およびライセンス情報については、『Cisco Network Security Ordering Guide』を参照してください。購入をご希望の場合は、シスコ発注ホームページにアクセスするか、シスコのセールス担当者へお問い合わせいただくか、1 800 553 6387 までお電話ください。

## 保証情報

保証情報については、Cisco.com の「製品保証」ページを参照してください。

## 詳細情報

- シスコ セキュリティ管理ポートフォリオ
- Cisco Secure Firewall
- Cisco Secure Firewall Management Center リリースノート
- Secure IPS（NGIPS）
- マルウェア防御
- シスコのセキュリティ分析とロギング
- サービスプロバイダーのためのネットワークセキュリティと信頼
- セキュリティのためのサービス
- Cisco Firepower Management Center（過去モデル）データシート


シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

**お問い合わせ先**
**お電話での問い合わせ**
平日 9:00 - 17:00
**0120-092-255**

**お問い合わせウェブフォーム**
cisco.com/jp/go/vdc_callback





シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp



1017-2023-000-X