Cisco Firepower Management Center

目次

Cisco Firepower™ Management Center は、一元化および統合された合理的な管理を提供することで、シスコ®のネットワーク セキュリティ ソリューションの有効性を高めます。

製品の概要

Cisco Firepower Management Center（旧称 FireSIGHT Management Center）は、さまざまなプラットフォームで動作する特定のシスコセキュリティ製品の管理における中枢として機能します。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。Management Center は、次のソリューションのイベントおよびポリシーを一元的に管理します。

- Cisco Firepower 次世代ファイアウォール（NGFW）
- Cisco ASA with FirePOWER Services
- Cisco Firepower 次世代 IPS（NGIPS）
- Cisco FirePOWER Threat Defense for ISR
- Cisco Advanced Malware Protection（AMP）

Cisco Firepower Management Center は、ネットワークに存在するユーザー、アプリケーション、デバイス、脅威、および脆弱性に関する広範なインテリジェンスを提供します。また、ネットワークの脆弱性を分析するためにこの情報を使用します。その後、配置するセキュリティポリシーと、調査する必要のあるセキュリティイベントについて、調整された推奨事項を提供します。

Management Center は、アクセスを制御し、既知の攻撃から保護するための使いやすいポリシー画面を提供します。高度なマルウェア防御およびサンドボックステクノロジーと統合され、ネットワーク全体のマルウェアの感染を追跡するツールを提供します。これらすべての機能が単一の管理インターフェイスに統合されています。ファイアウォールの管理からアプリケーションの制御までを行い、簡単にマルウェアの感染を調査して修復できます。

図 1.
ポリシー、イベント、デバイスの一元管理

エンタープライズクラスの管理

Cisco Firepower Management Center 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 を参照）。広範なインテリジェンスに加えて、Management Center 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。

機能とメリット

機能	メリット
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。 • Cisco Firepower 次世代ファイアウォール（NGFW） • Cisco ASA with FirePOWER Services • Cisco Firepower NGIPS • Cisco FirePOWER Threat Defense for ISR • Cisco AMP
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。 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。 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。
Cisco Identify Services Engine による統合アクセスポリシー制御	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。 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。
優れた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。 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。 ネットワーク周辺外の脅威を可視化するための Cisco Umbrella を搭載しています。 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	4000 を超える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。 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 50 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。 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。
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。 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。 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。 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。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。（FMC 1000、FMC 2500、FMC 4500 のみ）

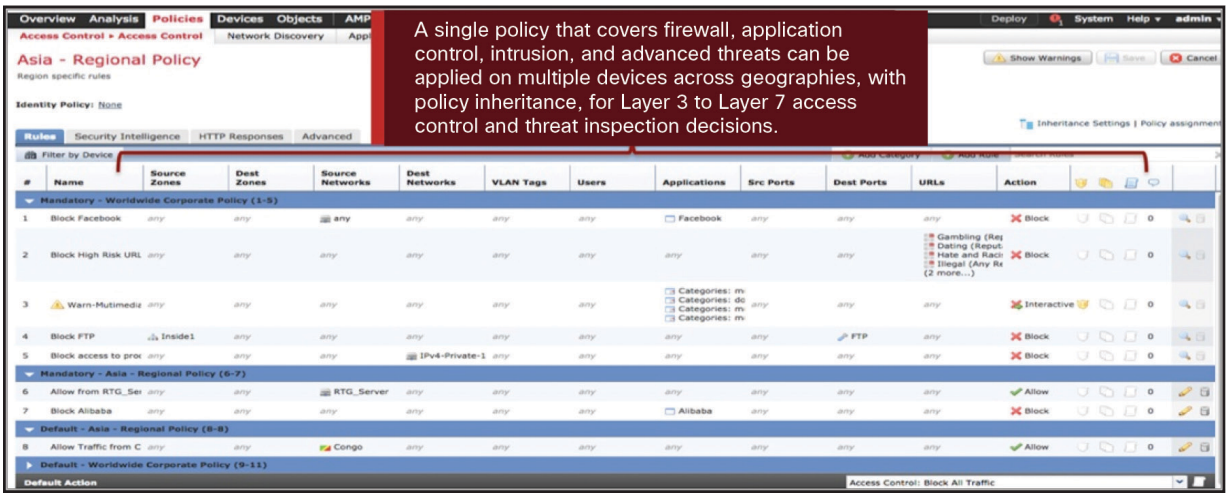

図 2.
複数のセキュリティ機能に対する単一のポリシー

優れた可視性と状況把握

見えないものを守ることはできません。Cisco Firepower Management Center は、環境内で実行されているすべてのものに関するコンテキスト情報を自動的に収集、照合、および表示します。表 1 は、従来型のセキュリティテクノロジーでは検出されなかった脅威媒体に対する幅広いコンテキスト認識が得られることを示しています。ネットワークに関するこの重要な情報は保護ポリシーで使用でき、他のソリューションでは実現できないレベルの保護を提供します。

表 1. 全機能の可視化

カテゴリ	Cisco Firepower Management Center	一般的な IPS	一般的な次世代ファイアウォール
脅威	対応	対応	対応
ユーザー	対応	対応	対応
Web アプリケーション	対応	×	対応
アプリケーションプロトコル	対応	×	対応
ファイル転送	対応	×	対応
マルウェア	対応	×	×
コマンドアンドコントロール サーバー	対応	×	×
クライアント アプリケーション	対応	×	×
ネットワーク サーバー	対応	×	×

カテゴリ	Cisco Firepower Management Center	一般的な IPS	一般的な次世代ファイアウォール
オペレーティング システム	対応	×	×
ルータおよびスイッチ	対応	×	×
モバイルデバイス	対応	×	×
プリンタ	対応	×	×
VoIP 電話	対応	×	×
仮想マシン	対応	×	×
脆弱性情報	対応	×	×

攻撃前、攻撃中、および攻撃後の管理

Cisco Firepower Management Center は「連続的な攻撃」全体（攻撃前、攻撃中、攻撃後）を一元管理します。

攻撃前

- ネットワークで実行されているものに対する優れた可視性を提供するため、保護する必要があるものを確認できます。
- ファイアウォールルールを作成し、環境内での 4000 を超える商用アプリケーションとカスタムアプリケーションの使用方法を制御します。

攻撃中

- 実装する侵入防御レベル、URL レピュテーションルール、および高度なマルウェア防御の要素を定義します。
- たとえば、「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、この国から送信されていて、ファイルが添付されている場合、このレベルの侵入検出を適用し、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」といったポリシーを適用します。

攻撃後

- 攻撃を受けたすべてのデバイスのグラフィカル表示を生成します。
- 攻撃の進行を防ぐためのカスタムルールを簡単に作成できます。
- マルウェアの詳細な分析を提供し、安全に修正します。

動的な防御のための自動セキュリティ

Cisco Firepower 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用し、ネットワークに最適な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。個々のホストが未知の攻撃による侵害の兆候を示すと、通知を受け取ります。
- 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。

オープン API による容易な統合

Cisco Firepower Management Center では、強力で機能豊富な 4 つのアプリケーション 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。

- Management Center 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 Firepower 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、アクティブなスキャナからの脆弱性管理データまたはオペレーティングシステム情報が含まれる場合があります。
- 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 Management Center 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、シスコが提供する多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 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、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。

Threat Intelligence Director

Threat Intelligence Director は、今後の Cisco Firepower Management Center のリリースでまもなく利用できるようになります。オープン API を使用すると、脅威フィードや脅威インテリジェンス プラットフォーム（TIP）などのソースからサードパーティの脅威インテリジェンスを容易に取り込むことができます。Threat Intelligence Director は、Structured Threat Information Expression（STIX）および Trusted Automated Exchange of Indicator Information（TAXII）、または一部のフラット（未フォーマット）ファイル形式の取り込みをサポートします。また、取り込んだインテリジェンスを、IP（IPv4、IPv6）、ドメイン、URL、および SHA-256 などの観察可能な要素（IoC）に分解します。これらの IoC がシスコ セキュリティ アプライアンスにパブリッシュされると、アプライアンスで悪意のあるアクティビティをインラインで自動的にブロックしたり、ネットワークの応答性をモニターしたりできるようになります。

Threat Intelligence Director は、以下のシスコ セキュリティ アプライアンスで利用可能な脅威インテリジェンスを運用できます。

- Cisco Firepower NGFW
- Cisco Firepower NGIPS

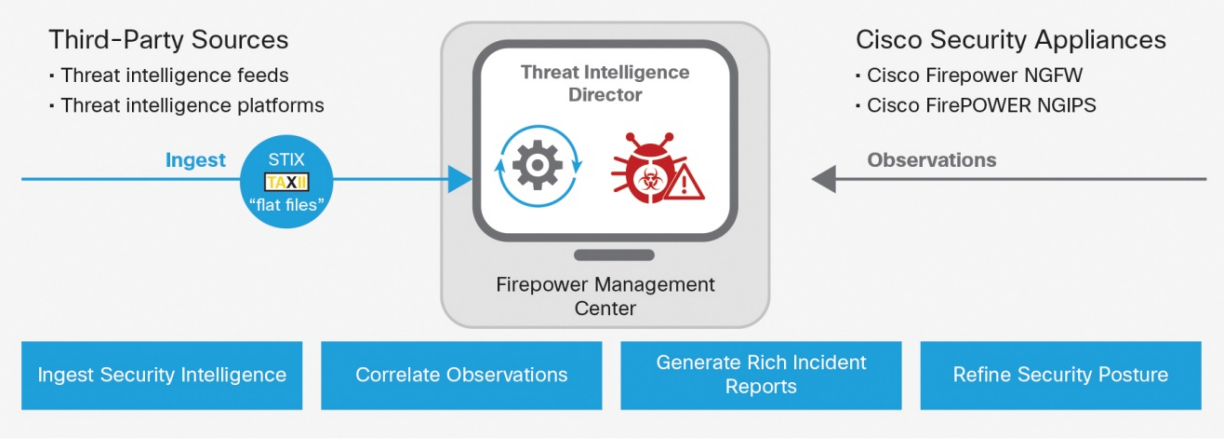

図 3.
Threat Intelligence Director とサードパーティ セキュリティ インテリジェンスの統合

サードパーティのサイバー脅威インテリジェンスと TIP パートナーの最新リストを確認するには、[シスコの Technical Alliance パートナーの一覧]を参照してください。

展開オプション

Cisco Firepower Management Center 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（表 2）。環境に最適な導入方法を選択できます。一般に、物理アプライアンスは、仮想アプライアンスよりも多くのセンサーを管理し、優れたイベントストレージ機能を提供します。仮想アプライアンスには、既存の VM インフラストラクチャを使用できるという利便性があります。また、クラウド コンピューティング サービスを使用して Management Center をホストすることもできます。これらのサービスにより、コンピューティング能力やデータベースストレージに投資することなく、セキュリティを管理できます。また、ニーズの変化に応じて迅速に拡張できる柔軟性が得られます。

NGFWv 上で Threat Intelligence Director を使用する場合、最適なパフォーマンスを得るためには、ホストハードウェアに 15 GB のメモリを搭載することを推奨します。サポート対象の FMC バージョンについては、https://www.cisco.com/c/ja_jp/support/security/defense-center/products-release-notes-list.html で最新のリリースノートを参照してください。

表 2. 展開オプション

展開プラットフォーム
VMware ESX および ESXi ハイパーバイザ
KVM ハイパーバイザ
Amazon Web Service のクラウドプラットフォーム

プラットフォームの仕様

Cisco Firepower 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、ニーズに合ったものをお選びください（表 3 を参照）。以下の管理機能はすべてのモデルで共通です。

- デバイス、ライセンス、イベント、およびポリシーの一元管理
- ロールベースの管理（表示および管理業務は、管理者ロールまたは管理者グループによってセグメント化され、それぞれ独立）
- カスタムレポートおよびテンプレートベースのレポートを使用できるカスタマイズ可能なダッシュボード
- 一般情報と特定情報の両方に対応する包括的なレポートおよびアラート
- ハイパーリンクテーブル、グラフ、チャートに表示されるイベント情報と状況情報
- ネットワーク動作とパフォーマンスのモニタリング
- 単一障害点を防ぐ堅牢な高可用性オプション
- 関連付けおよび修復機能によるリアルタイムの脅威対応
- オープン API により、ファイアウォール、ネットワーク インフラストラクチャ、ログ管理、SIEM、トラブルチケット生成、パッチ管理などの、サードパーティ製ソリューションや顧客ワークフローと統合

表 3 では、使用可能な Cisco Firepower Management Center の物理アプライアンスと仮想アプライアンスについて、容量とスループットを比較しています。

表 3. Cisco Firepower Management Center のモデル

性能と機能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
管理できるセンサーの最大数	10	50	250	300	500	750	25* 10 2
IPS イベントの最大数	2,000 万	3,000 万	6,000 万	6,000 万	3 億	3 億	1,000 万

性能と機能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
管理インターフェイス	100/100/1000 RJ-45						
メモリ	8 GB（現在出荷中）	32 GB	64 GB	64 GB	128 GB	128 GB	–
CPU	4 コア Xeon	8 コア Xeon	6 コア Xeon	2 x 8 コア Xeon	2 x 10 コア Xeon	2 x 10 コア Xeon	–
イベント記憶域	100 GB	900 GB	1.8 TB	1.8 TB	3.2 TB	3.2 TB	250 GB
最大ネットワークマップサイズ（ホスト/ユーザー）	2,000/2,000	50,000/50,000	150,000/150,000	150,000/150,000	600,000/600,000	600,000/600,000	50,000/50,000
最大フローレート（1 秒あたりのフロー）	2,000 fps	5,000 fps	12,000 fps	12,000 fps	20,000 fps	20,000 fps	不定*
ネットワーク インターフェイス	2 x 1 Gbps	2 x 1 Gbps	2 X 1 Gbps RJ45 オンボード 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 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 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 2 X 10 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	–
冗長機能							
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	×
デュアル電源	×	対応	対応	対応	対応	対応	–
RAID サポート	×	HDD RAID 1	HDD RAID 5	HDD RAID 1	SSD RAID 6	SSD RAID 6	–
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	–
外形寸法（奥行 X 幅 X 高さ）（単位インチ）	27.19 X 16.9 X 1.7（69 X 43 X 4.3 cm）	29.8 X 16.9 X 1.7（75.7 X 43 X 4.3 cm）	28.5 X 16.9 X 1.7（72.3 X 43 X 4.3 cm）	29.8 X 16.9 X 1.7（75.7 X 43 X 4.3 cm）	28.5 X 16.9 X 1.7（72.3 X 43 X 4.3 cm）	29.8 X 16.9 X 1.7（75.7 X 43 X 4.3 cm）	–
出荷時重量	33 ポンド（15 kg）	39 ポンド（17.7 kg）	35.6 ポンド（16.2 kg）	39 ポンド（17.7 kg）	35.6 ポンド（16.2 kg）	39 ポンド（17.7 kg）	–
ワット（最大）	350W	770W	650 W	770W	650 W	770W	–

性能と機能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
電源モジュール	110 V で 最大 9.5 A、50/60 Hz 220 V で 最大 4.75 A、50/60 Hz	100 ~ 240 VAC（公称） 90 ~ 264 VAC（最小/最大） 100 VAC で最大 9.5 A 208 VAC で最大 4.5 A	自己範囲：90 ~ 264 VAC 公称範囲：100 ~ 120 VAC 公称範囲：200 ~ 240 VAC 7.6 A（100 VAC で最大） 3.65 A（208 VAC で最大）	100 ~ 240 VAC（公称） 90 ~ 264 VAC（最小/最大） 100 VAC で最大 9.5 A 208 VAC で最大 4.5 A	自己範囲：90 ~ 264 VAC 公称範囲：100 ~ 120 VAC 公称範囲：200 ~ 240 VAC 7.6 A（100 VAC で最大） 3.65 A（208 VAC で最大）	100 ~ 240 VAC（公称） 90 ~ 264 VAC（最小/最大） 100 VAC で最大 9.5 A 208 VAC で最大 4.5 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	10 ~ 35°C	5 °C ~ 35 °C	5°C ~ 40°C	5 °C ~ 35 °C	5°C ~ 40°C	5 °C ~ 35 °C	-

*注：3 つの費用対効果の高い仮想 FMC ライセンスオプションを利用して、2 個、5 個、または 25 個のセンサーを管理できます。

仮想 Cisco Firepower Management Center のパフォーマンスは、選択した仮想環境（CPU、メモリ、ストレージなど）に大きく依存します。

共通機能

- 統合 Lights-Out Management（LOM）
- シスコの次世代セキュリティソリューション（NGIPS、NGIPS およびアプリケーション制御、NGFW）の一元管理

注： Cisco ASA with FirePOWER Services 製品を扱う場合、Cisco Firepower Management Center では、展開されている FirePOWER 部分のみを管理します。

表 4 に、Management Center で管理できる Cisco Firepower 製品のサポート対象バージョンを、関連するハードウェア プラットフォームとともに示します。

表 4. サポートされている Firepower バージョンと関連プラットフォーム

管理プラットフォーム	ソフトウェア リビジョン レベル	ハードウェア プラットフォーム
Cisco Firepower Management Center	Cisco Firepower Threat Defense 6.x（NGFW）	ASA 5500-X（ASA 5585-X 以外） Cisco 2100 シリーズ（min FMC 6.2.1） Cisco Firepower 4100 シリーズ Cisco Firepower 9300
	FirePOWER サービス 6.x	ASA 5500-X
	Cisco Firepower NGIPS 6.x	Cisco Firepower 7000 Cisco Firepower 8000
	ISR 6.x 向け FirePOWER Threat Defense（Cisco Firepower サービス）	4000 シリーズ ISR ISR G2
	FirePOWER サービス 5.4.x	ASA 5500-X

管理プラットフォーム	ソフトウェア リビジョン レベル	ハードウェア プラットフォーム
	Cisco Firepower NGIPS 5.4.x	Cisco Firepower 7000 Cisco Firepower 8000

ハイパーバイザの互換性

Cisco Firepower Management Center 仮想アプライアンスは、次のハイパーバイザタイプをサポートしています。現在サポートされているバージョンと FMC バージョンとの互換性については、https://www.cisco.com/c/ja_jp/support/security/defense-center/products-release-notes-list.html で最新のリリースノートを参照してください。

表 5. 仮想アプライアンスのハイパーバイザサポート

ハイパーバイザ	バージョンおよび詳細
VMware vSphere	5.1、5.5、6.0 • ESXi サーバー • vCenter Server（オプション） • Windows または Linux 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 14.04 LTS Red Hat Enterprise Linux（RHEL）バージョン 7.1
Amazon Web Services	AWS インスタンスタイプ：c3.xlarge および c3.2xlarge

注文情報

ライセンシング

バージョン 6.0 以降、Cisco Firepower Management Center を使用するためにライセンスキーは必要ありません。バージョン 5.4 以前では、引き続き製品認証キー（PAK）またはスマートキーが必要です。バージョン 6.0 にアップグレードすると不要になります。

Cisco Smart Net Total Care サポート

Cisco Smart Net Total Care™ は、高い実績を誇るテクニカルサポートサービスです。お客様の会社の IT スタッフは、Cisco Technical Assistance Center（TAC）のエンジニアや Cisco.com の豊富なリソースにいつでも直接アクセスできます。ここでは、エキスパートによる迅速な対応と、ネットワークの重大な問題を解決するための詳細なアドバイスが提供されます。

Smart Net Total Care は、以下のデバイスレベルのサポートを提供します。

- Cisco TAC の専門エンジニアへの 365 日 24 時間のグローバルアクセス
- Cisco.com の豊富なオンラインナレッジベース、リソース、ツールにいつでもアクセス可能
- 2 時間、4 時間、または翌営業日（NBD）の代替品先出し配送のほか、修理のための返却（RFR）を含むハードウェア交換オプション

- 継続的なオペレーティング システム ソフトウェアのアップデート（ライセンスされている機能セットの範囲内でマイナーリリース、メジャーリリースの両方を含む）
- Cisco Smart Call Home 対応の一部のデバイスでのプロアクティブな診断とリアルタイムアラート

さらに、オプションの Cisco Smart Net Total Care オンサイトサービスでは、お客様の拠点にフィールドエンジニアを派遣して交換部品を設置し、ネットワークの最大品質を維持できるようにサポートします。Smart Net Total Care の詳細については、https://www.cisco.com/c/ja_jp/services/technical/smart-net-total-care.html を参照してください。

注文方法

表 6 は、Cisco Firepower Management Center の仮想アプライアンスと物理アプライアンス、およびスペアハードウェアの発注情報を示しています。追加の構成オプションとアクセサリについては、『Cisco Network Security Ordering Guide』を参照してください。

表 6. 発注情報

Cisco Firepower Management Center（ハードウェア）アプライアンス	
部品番号	**製品の説明**
FS750-K9	Cisco Firepower Management Center 750 シャーシ、1 ラックユニット（RU）
FMC1000-K9	Cisco Firepower Management Center 1000 シャーシ、1RU
FS2000-K9	Cisco Firepower Management Center 2000 シャーシ、1RU
FMC2500-K9	Cisco Firepower Management Center 2500 シャーシ、1RU
FS4000-K9	Cisco Firepower Management Center 4000 シャーシ、1RU
FMC4500-K9	Cisco Firepower Management Center 4500 シャーシ、1RU
Cisco Firepower Management Center（ハードウェア）スペア	
FS-PWR-AC-650W=	Cisco Firepower 650W AC 電源（FS2000、FS4000 用）
FS-PWR-AC-779W=	Cisco AC 電源 770 W（FMC1000、FMC2500、FMC4500 用）
Cisco Firepower Management Center（ソフトウェア）仮想アプライアンス	
FS-VMW-SW-K9	Cisco Firepower Management Center、仮想（VMware）Firepower ライセンス
FS-VMW-10-SW-K9	Cisco Firepower Management Center、仮想（VMware）Firepower ライセンス、10 デバイス用
FS-VMW-2-SW-K9	Cisco Firepower Management Center、仮想（VMware）Firepower ライセンス、2 デバイス用

購入方法については、「購入案内」を参照してください。

保証情報

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

シスコサービス

シスコでは、お客様のビジネスを支援する多様なサービスプログラムをご用意しています。これらのサービスは、スタッフ、プロセス、ツール、パートナーをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。シスコのサービスは、お客様のネットワーク投資を保護してネットワーク運用を最適化するだけでなく、ネットワーク インテリジェンスの強化や事業拡張に向けた新しいアプリケーションの導入準備という面でもサポートします。シスコのセキュリティサービスの詳細については、https://www.cisco.com/jp/go/services/security を参照してください。

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

詳細については、以下のリンクを参照してください。

- Cisco Firepower Management Center
- Cisco Firepower 次世代ファイアウォール
- Cisco Firepower 次世代 IPS（NGIPS）
- Cisco Advanced Malware Protection（AMP）
- Cisco FirePOWER Threat Defense for ISR
- シスコ セキュリティ サービス

サービスプロバイダー環境での Cisco Firepower の詳細については、https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/service-provider-security-solutions/ を参照してください。

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 10:00 - 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

0524-2022-000-X