Cisco Firepower Management Center

Cisco Firepower™ Management Center は、統合および合理化された一元管理機能により、Cisco® ネットワーク セキュリティ ソリューションの効率性を高めます。

製品概要

Cisco Firepower Management Center（旧 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 セキュリティ製品向けの集中管理センターです。すべてのファイアウォールを対象とした完全かつ包括的なユニファイド マネジメント、アプリケーション制御、侵入防御、URL フィルタリング、そして高度なマルウェア防御を実現します。Management Center は、以下のソリューションで、イベントおよびポリシー管理の中心として機能します。

- 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、お客様のネットワークに存在するユーザ、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、これらの情報を使用してネットワークの脆弱性を分析します。その後、どのセキュリティ ポリシーを適用して、どのセキュリティ イベントを調査する必要があるかについて、最適な推奨事項が表示されます。

Management Center には簡単に操作できるポリシー画面が表示され、アクセスの制御と既知の攻撃に対する防御を行うことができます。高度なマルウェア防御とサンドボックス テクノロジーが統合されており、ネットワーク全体のマルウェア感染を追跡するためのツールを備えています。これらすべての機能は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実施し、マルウェアのアウトブレイクを簡単に調査して修復できます。

図 1. ポリシー、イベント、および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、変化するネットワーク リソースおよび運用に関する情報をリアルタイムで検出します。取得した豊富なコンテキスト情報に基づいて、意思決定を行うことができます（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。

- **傾向および高レベルの統計情報。**この情報により、ある時点でのセキュリティ ポスチャとその動向を適時理解することができ、良否を判断することができます。
- **イベントの詳細、コンプライアンス、および調査。**セキュリティ イベントの内容を把握できます。これらの情報は、防御力を高め、セキュリティ侵害の封じ込めを行い、法的措置を講じるのに役立ちます。
- **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、インシデント対応管理を改善することができます。

機能と利点

機能	利点
複数のソリューション間のさまざまなセキュリティ機能を一元管理	次を含むシスコのセキュリティ環境を集中管理できます。 • 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の統合ポリシー管理	ファイアウォール アクセス、アプリケーション制御、脅威防御、URL フィルタリング、高度なマルウェア防御を単一のポリシーで設定 ポリシー管理の簡素化、エラーの削減、および一貫性の強化 複数のセキュリティ ソリューションへの単一ポリシーの展開が可能
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、場所の IP に基づいたアクセス制御、および脅威の迅速な封じ込め コンプライアンスの適用、インフラストラクチャのセキュリティの強化、サービス運用の簡素化を支援
優れた脅威インテリジェンス	Cisco Talos グループのセキュリティ、脅威、および脆弱性に関するインテリジェンスを統合し、最新の脅威から保護 IP ベースと URL ベースのセキュリティ インテリジェンスにより、新しい攻撃手法に対応 搭載されている Cisco Umbrella により、ネットワーク境界の外部にある脅威を可視化 サードパーティの脅威フィードと、STIX/TAXII またはフラット ファイル形式の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可能
アプリケーションの可視性と制御	4,000 を超える商用アプリケーションを正確に制御し、ネットワークに対する脅威をさらに削減 オープン ソース標準の Open App ID を使用した、カスタム アプリケーションの詳細な識別と制御
マルチテナンシー管理とポリシー継承	個別のイベント データ、レポート、ネットワーク マッピングを含む最大 50 個の管理ドメインを作成し、ロールベース アクセス コントロールを通じて適用 各レベルで上位のポリシーが継承されるポリシー階層構造を通じて、一貫性のある効率的な管理を実施
レポートおよびダッシュボード	カスタマイズ可能なダッシュボードとカスタムおよびテンプレート ベースのレポートを通じて、必要な可視性を提供 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生成 ハイパーリンク付きのテーブル、グラフ、チャートにイベントおよびコンテキスト情報が表示され、簡単な操作で分析が可能 ネットワークの動作とパフォーマンスをモニタして異常を検出し、システムの正常性を維持
セキュアブート	セキュアブートは、システムのブート時に FMC ハードウェアで動作しているシスコ ソフトウェアの整合性を検証するためのメカニズムです。署名されていない場合や、ソフトウェアが無効である場合、そのソフトウェアはロードされず、ブートに失敗します。（FMC 1000、FMC 2500。FMC 4500 のみ）

図 2. 単一のポリシーで複数のセキュリティ機能に対応

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、環境で実行されているすべての対象に関するコンテキスト情報を自動的に収集して照合し、表示します。表 1 に、従来のセキュリティ テクノロジーでは検出されない脅威ベクトルに対して提供される広範なコンテキスト認識を示します。ネットワークに関するこれらの重要な情報は、保護ポリシーで使用することができ、他のソリューションでは達成できない高レベルの保護を実現できます。

表 1. 全機能の可視化

カテゴリ	Cisco Firepower Management Center	一般的な IPS	一般的な次世代型ファイアウォール
脅威	対応	対応	対応
ユーザ	対応	対応	対応
Web アプリケーション	対応	非対応	対応
アプリケーション プロトコル	対応	非対応	対応
ファイル転送	対応	非対応	対応
マルウェア	対応	非対応	非対応
コマンドアンドコントロール サーバ	対応	非対応	非対応
クライアント アプリケーション	対応	非対応	非対応
ネットワーク サーバ	対応	非対応	非対応
オペレーティング システム	対応	非対応	非対応
ルータとスイッチ	対応	非対応	非対応
モバイル デバイス	対応	非対応	非対応
プリンタ	対応	非対応	非対応
VoIP 電話	対応	非対応	非対応
仮想マシン	対応	非対応	非対応
脆弱性情報	対応	非対応	非対応

攻撃前、攻撃中、攻撃後の管理

Cisco Firepower Management Center では、攻撃前、攻撃中、および攻撃後の「攻撃サイクル」全体にわたる管理が統合されています。

攻撃前

- 高度な可視化機能により、ネットワークで何が実行されているかを表示することができ、保護する必要があるものを簡単に確認できます。
- ファイアウォール ルールを作成し、4,000 を超える商用アプリケーションとカスタム アプリケーションが環境内でどのように使用されるかを制御できます。

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おり、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。

実行後

- 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、環境を安全に修復します。

セキュリティの自動化による動的な防御

Cisco Firepower Management Center は、ネットワークの変化を継続的にモニタします。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することができます。

- 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て、成功の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。
- ファイルのポリシー条件を適用します。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 による簡単な統合

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、セキュリティ情報とイベント管理（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。そのようなデータには、脆弱性管理データや、アクティブなスキャナから得られたオペレーティング システム情報が含まれます。

- ユーザ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、識別データの共有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。

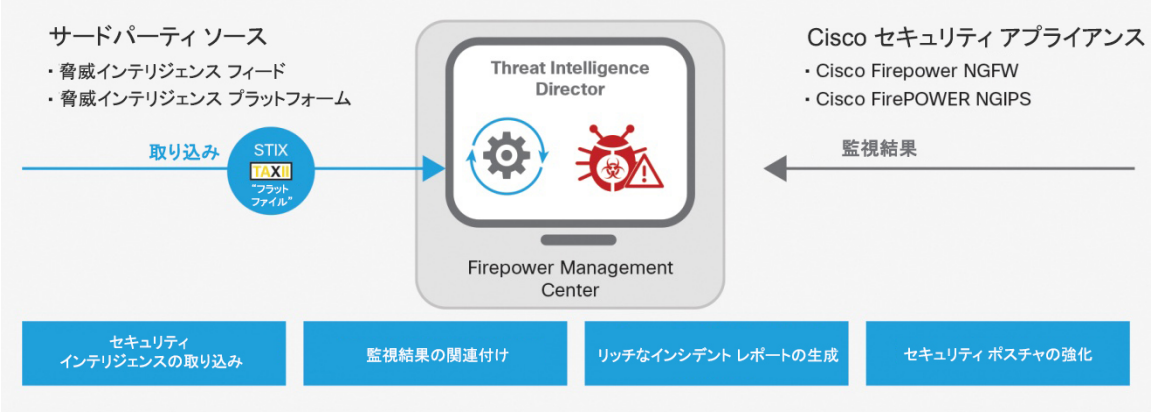
Threat Intelligence Director

Threat Intelligence Director は、Cisco Firepower Management Center の今後のリリースで近日中に利用可能になります。オープン API を使用すると、Director で、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。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。Threat Intelligence Director は、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 はシスコ セキュリティ アプライアンスにパブリッシュされ、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、ネットワークの応答性をモニタ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することができます。

- 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、[シスコの技術アライアンス パートナーの一覧](#) [英語] を参照してください。

導入オプション

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。物理アプライアンスは、通常、仮想アプライアンスと比べて多数のセンサーを管理し、大規模なイベント 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。さらに、必要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、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。

表 2. 導入オプション

導入プラットフォーム	最小バージョン レベル
VMware ESX および ESXi ハイパーバイザ	バージョン 5.x
KVM ハイパーバイザ	バージョン 6.1
Amazon Web Services クラウド プラットフォーム	バージョン 6.0

プラットフォームの仕様

Cisco Firepower Management Center には複数のモデルがあります。モニタ対象のセンサー 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）。すべてのモデルが、以下のような共通の管理機能を備えています。

- 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（管理者ロールまたはグループに基づく、セグメント化および隔離されたビューおよび職責）
- 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
- シングル ポイント障害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のキャパシティとスループットを比較しています。

表 3. Cisco Firepower Management Center のモデル一覧

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
MaxIPS イベント	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（現行製品）	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）	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	12000 fps	20,000 fps	20,000 fps	環境に応じて異なる`
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	-
冗長性機能							
ハイ アベイラビリティのサポート	非対応	対応	対応	対応	対応	対応	非対応
デュアル電源	非対応	対応	対応	対応	対応	対応	-
RAID サポート	非対応	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							
筐体サイズ	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU	-
寸法（奥行 X 幅 X 高さ）（cm）	69 X 43 X 4.3（27.19 X 16.9 X 1.7 インチ）	75.7 X 43 X 4.3（29.8 X 16.9 X 1.7 インチ）	72.3 X 43 X 4.3（28.5 X 16.9 X 1.7 インチ）	75.7 X 43 X 4.3（29.8 X 16.9 X 1.7 インチ）	72.3 X 43 X 4.3（28.5 X 16.9 X 1.7 インチ）	75.7 X 43 X 4.3（29.8 X 16.9 X 1.7 インチ）	-
出荷重量	15 kg（33 ポンド）	17.7 kg（39 ポンド）	16.2 kg（35.6 ポンド）	17.7 kg（39 ポンド）	16.2 kg（35.6 ポンド）	17.7 kg（39 ポンド）	-
ワット（最大）	350 W	770 W	650 W	770 W	650 W	770 W	-
電源	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 100 ～ 120 VAC 公称 200 ～ 240 VAC 公称 100 VAC で最大 7.6 A 208 VAC で最大 3.65 A	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 100 ～ 120 VAC 公称 200 ～ 240 VAC 公称 100 VAC で最大 7.6 A 208 VAC で最大 3.65 A	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	前面から背面へ	前面から背面へ	前面から背面へ	前面から背面へ	前面から背面へ	前面から背面へ	-
動作温度	10 ～ 35 °C	5 ～ 35 °C	5 ～ 40 °C	5 ～ 35 °C	5 ～ 40 °C	5 ～ 35 °C	-

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）に応じて大幅に異なります。

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）の集中管理

注： Cisco ASA with FirePOWER Services 製品を扱う場合、Cisco Firepower Management Center では、導入の 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. サポート対象の Firepower バージョンと関連するプラットフォーム

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 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**
	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 の仮想アプライアンスは、表 5 に示すハイパーバイザのバージョンをサポートします。

表 5. 仮想アプライアンスによるハイパーバイザのサポート

ハイパーバイザ	バージョンおよび詳細	仮想 Cisco Firepower Management Center のバージョン
VMware vSphere	5.1、5.5、6.0 • ESXi サーバ • 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	5.4、6.0
KVM	Ubuntu 14.04 LTS Red Hat Enterprise Linux（RHEL）バージョン 7.1	6.1
Amazon Web Services	AWS インスタンス タイプ：c3.xlarge および c3.2xlarge	6.0.1、6.1

発注情報

ライセンス

バージョン 6.0 以降では、Cisco Firepower Management Center の使用にライセンス キーは必要ありません。バージョン 5.4 以前では、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）の代替品先行手配のほか、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、http://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html [英語] を参照してください。

発注方法

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（シスコ ネットワーク セキュリティ発注ガイド）』[英語] 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	
製品番号	**製品説明**
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 650 W 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

シスコ製品の購入方法については、「購入案内」を参照してください。

保証に関する情報

保証については、Cisco.com の製品保証 [英語] のページを参照してください。

シスコのサービス

シスコは、お客様の成功を支援する幅広いサービス プログラムを用意しています。これらの革新的なサービス プログラムは、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 サービスは、ネットワーク インテリジェンスおよびビジネスの能力を高めるためのネットワーク投資の保護、ネットワーク運用の最適化、および新しいアプリケーションのためのネットワークの準備を支援します。シスコのセキュリティ サービスの詳細については、http://www.cisco.com/jp/go/services/security/ にアクセスしてください。

Cisco Capital

目標の達成を支援するファイナンス

Cisco Capital では、目標を達成し、競争力を維持するために必要なテクノロジーの取得を支援します。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムは、お客様がハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に取得できるようにします。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら

関連情報

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 については、次の URL を参照してください。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/ [英語]

お問い合せ先

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
http://www.cisco.com/jp

C78-736775-04JA 18.04