# Cisco Firepower NGIPS

目次

## 統合ネットワーク脅威アプライアンス

Cisco Firepower NGIPS は、優れた可視性、優れたセキュリティ インテリジェンス、および優れた高度な脅威からの保護を提供して、今日の複雑な IT 環境を保護します。

## 製品の概要

Cisco Firepower 次世代 IPS（NGIPS）脅威アプライアンスは、ネットワークの可視性、セキュリティ インテリジェンス、自動化、および高度な脅威からの保護を提供します。業界トップクラスの侵入防御機能と複数の方法を使用して、最も高度なネットワーク攻撃でさえも検出して、それらから保護します。Cisco Firepower NGIPS 脅威アプライアンスのすべてが、Fail-To-Wire/Bypass ネットワークモジュールを介してインラインで動作する機能を提供します。

Cisco Firepower NGIPS は、オペレーティングシステム、モバイルデバイス、ファイル、アプリケーション、およびユーザーに関するデータを含む、ネットワーク環境に関する情報を継続的に検出します。次に、この情報を使用してネットワークマップとホストプロファイルを作成します。これにより、侵入イベントに関してより適切な決定を行うために必要なコンテキスト情報が得られます。この情報は、主要な脅威防御機能の自動化をより適切に実現するための入力としても使用されます。

Cisco TALOS Security Intelligence and Research Group は、世界最大の脅威検出ネットワークを使用して、脅威をリアルタイムで収集して関連付けています。それらの取り組みにより、脆弱性に焦点を当てた IPS ルールと、Firepower NGIPS 向けの IP、URL、および DNS ベースのセキュリティ インテリジェンスが組み込まれています。

セキュリティ自動化によって侵入イベントがネットワークの脆弱性に関連付けられるため、最も重要な脅威に焦点を当てることができます。また、ネットワークの弱点を分析し、適切なセキュリティポリシーを設定するように推奨します。

Cisco Firepower NGIPS 脅威アプライアンスは、既知と未知の両方の脅威において、業界トップクラスの脅威への有効性を提供します。次の機能が含まれています。

- ネットワークの脆弱性をターゲットとする攻撃トラフィックを識別してブロックする IPS ルール
- ネットワークとエンドポイント アクティビティの高度な分析を組み込んだ、高度なマルウェアに対して緊密に統合された防御
- 数百もの侵入兆候を使用してゼロデイ攻撃や回避的な攻撃を識別するサンドボックス分析テクノロジー

## 機能と利点

| 機能 | 利点 |
| --- | --- |
| **優れた有効性** | 業界トップクラスの脅威からの保護機能で、既知と未知の両方のさらなる脅威を阻止します。マルウェアの検出までの時間を短縮し、その損害と拡散を抑制します |
| **状況認識** | リアルタイムの可視性により、ネットワーク内のユーザー、アプリケーション、デバイス、脅威、脆弱性をより詳細に把握し、それらを制御します |
| **高度な脅威からの保護および迅速な修復** | 緊密に統合された AMP ソリューションとサンドボックス ソリューションにより、高度な脅威の迅速な検出、ブロック、封じ込め、修復を行います。新しいソフトウェアやシグネチャが利用可能になる前に、「仮想的に」および瞬時に脆弱性にパッチを適用します |
| **セキュリティの自動化** | 脅威イベント、コンテキスト認識情報、脆弱性データを自動的に関連付けて、スタッフにさらに注意を向け、セキュリティ向上の実施とフォレンジック調査の迅速化を行います |
| **アプリケーションのきめ細かな可視化と制御** | 4000 を超える商用アプリケーションを正確に制御し、カスタムアプリケーションをサポートすることで、ネットワークに対する脅威を軽減します |
| **Cisco Talos Security Intelligence and Research Group からのグローバル脅威インテリジェンス** | 35,000 を超える IPS ルールと、組み込みの IP、URL、DNS ベースのセキュリティ インテリジェンスで、最新の脅威からの保護を提供する世界的な脅威の可視性と分析を活用します |

## 優れた特長/他製品との違い/機能

### 次世代侵入防止システムの機能

Cisco Firepower NGIPS は、ネットワーク脅威保護の新しい標準を定めています。リアルタイムのコンテキスト認識、セキュリティ自動化、高度なマルウェア防御、および優れた脅威インテリジェンスを、業界トップクラスのネットワーク侵入防御に統合します。今日の動的な環境を、ますます高度な脅威から保護するために必要な可視性、シンプルさ、オープン性、および有効性を提供するソリューションは他にありません。

Cisco Firepower NGIPS は、次の機能を含むことにより、他の侵入防御ソリューションとは明らかに異なります。

### 優れた脅威保護

- Cisco Firepower NGIPS は、世界で最も人気のある侵入防御ソフトウェアである Snort のコアオープンテクノロジー上に構築されています。脆弱性および異常ベースの検査方法を使用して、悪意のあるホスト、ネットワークマルウェア攻撃、ファイル移動、およびゼロデイ脅威について警告します。
- Cisco Talos Security Intelligence and Research Group では、6,000 億件の電子メール、10 億件を超える Web クエリ、および約 150 万件のマルウェアサンプルを毎日分析して、最新の脅威と脆弱性を識別しています。
- 独立した NSS Labs の侵害検出システムでのテストでは、Firepower NGIPS は脅威を阻止するのに 99.7% の効果があり、攻撃を隠すために使用される回避技術の識別に 100% の効果があることがわかっています。

### リアルタイムのコンテキスト認識

- 収集および分析データには、アプリケーション、ユーザー、デバイス、オペレーティングシステム、脆弱性、モバイルデバイス、クライアント側のアプリケーション、サービス、プロセス、ネットワークの動作、ファイル、および脅威に関する情報が含まれます。
- また、コンテキストデータを IPS ルールで使用して、非常に高いレベルのきめ細かな保護を提供することもできます。

### インテリジェントなセキュリティ自動化

- 侵入イベントは、ネットワークの脆弱性に自動的に関連付けられます。成功する可能性のある攻撃について警告が表示されるため、アナリストは最も重要な脅威に集中できます。
- ネットワークの弱点は分析されて、推奨されるセキュリティポリシーを自動的に生成し、それによって脆弱性に対処します。このプロセスは、アナリストが、常に変化するネットワークに対応し、環境に合わせたカスタムの保護を提供するのに役立ちます。
- 侵害の兆候（IoC）は、未知の脅威に対する脅威検出の別の方法を提供します。侵害される可能性のあるホストは、複数のソース（IPS、セキュリティ インテリジェンス、ネットワークおよびエンドポイントのマルウェア防御など）からの特定のイベントを関連付けることによって識別されます。アナリストは、優先順位付けされたダッシュボードと、アクティビティを検査するクイックリンクにより、侵害を受けたホストを調査し、修復できます。
- キャプティブ ポータル テクノロジーを通じて、および Active Directory と他の LDAP テクノロジーとの統合を通じて、特定のユーザーが IPS イベントに関連付けられます。この機能により、モニタリングと分析が向上し、フォレンジック調査が迅速化されます。

### 高度な脅威からの保護

- 完全に統合された Cisco Advanced Malware Protection（AMP）ソリューションは、回避的および高度なファイル関連の脅威に対処し、成功した攻撃の迅速な追跡、封じ込め、分析、および修復を行う機能を提供します。
- 主要な機能により、回避的なマルウェアや新たなマルウェアの脅威を早期に検出し、業界トップクラスの、検出時間の中央値が 13 時間という短さを実現します（出典：Cisco Annual Security Report、2016 年 1 月）。
- ファイルサンドボックス分析（クラウドまたはオンプレミス）、脅威スコアリング、マルウェアの動作分析により、未知およびゼロデイ攻撃に対処します。
- 組織は、最初の分析でファイルまたはマルウェアが許可された後でも、環境内で悪意のあるコンテンツが新たに識別されるとすぐに警告されます。

### 管理、統合、および展開オプション

- Cisco Firepower Management Center は、Cisco Firepower NGIPS、Cisco Firepower Threat Defense for ISR、および Cisco Firepower NGFW のすべての展開に対して、イベント収集とポリシー管理の単一ポイントを提供します。セキュリティ態勢、ネットワーク内のすべてのポイントでの一貫したセキュリティ、および管理の複雑さの軽減に関する、企業全体の包括的なビューを取得できます。

- 多くのシスコのネットワークセキュリティ製品と統合することで、脅威に対する効果が高まり、複雑さが軽減され、コストが削減されます。たとえば、Cisco Firepower NGIPS の検出により、脅威を迅速に封じ込めるために、シスコの Identity Services Engine（ISE）で自動修復アクション（検疫、ブロックなど）を実行できます。
- 物理 NGIPS プラットフォームと仮想 NGIPS プラットフォームの両方として利用可能なため、他の方法では実用的でないネットワークの一部をセグメント化する優れた手段を提供します。
- Cisco Firepower Threat Defense for ISR は、シスコのサービス統合型ルータ（ISR）で Firepower NGIPS 脅威機能を提供します。セキュリティ インフラストラクチャのフットプリントを増やすことなく、ブランチオフィスやその他の遠隔地にあるセキュリティ上の懸念に対処できます。

**アプリケーション制御および URL フィルタリング**

- Application Visibility and Control は、アプリケーションの使用と、4000 を超える商用アプリケーションへのユーザーアクセスを、きめ細かく制御できるようにします。
- シスコが主導するオープンソースのアプリケーション識別標準である OpenAppID を使用すると、カスタム、ローカライズされた、およびクラウドのアプリケーションを定義して、商用アプリケーションと同じ方法で制御できます。
- URL フィルタリングオプションにより、セキュリティとコンプライアンスの両方が向上します。80 を超えるカテゴリの Web サイトにアクセス制御機能を提供し、2 億を超える個別の URL をカバーします。既知の危険なサイトまたは悪意のあるサイトへのアクセスを防止することで、Web から感染するマルウェアのリスクが軽減されます。

## プラットフォームのサポート

Cisco Firepower NGIPS には、基本製品の一部として Cisco Application Visibility and Control（AVC）が含まれています。オプションのライセンスは、Cisco Advanced Malware Protection（AMP）for Networks および URL フィルタリングに使用できます。Cisco Firepower 2100 シリーズ、4100 シリーズ、9300 シリーズ、3100 シリーズ、および 4200 シリーズのアプライアンスは、Cisco Firepower Threat Defense ソフトウェアイメージを使用します。

Cisco Firepower 2100 シリーズは、4 つの脅威対策重視型 NGFW セキュリティ プラットフォームで構成されるファミリです。このプラットフォームは、脅威に対する優れた防御機能によってビジネスの復元力を提供します。優れたパフォーマンスを安定して確保しつつ、高度な脅威検出機能を有効にできます。これらのプラットフォームには、革新的なデュアルマルチコア CPU アーキテクチャが独自に搭載されています。このアーキテクチャにより、ファイアウォール、暗号化、および脅威検出の各機能を同時に活用することができます。このシリーズのスループット範囲は、インターネットエッジからデータセンターまで幅広い用途に対応します。Network Equipment Building Standards（NEBS）準拠は、Cisco Firepower 2100 シリーズのプラットフォームでサポートされています。

Cisco Firepower 4100 シリーズは、4 つの脅威に焦点を当てた NGIPS セキュリティ プラットフォームのファミリです。最大スループットは、範囲が 12 ～ 24 Gbps で、インターネットエッジからデータセンターまでのユースケースに対応します。省スペース設計で、高速の優れた脅威防御を提供します。

Cisco Firepower 9300 は、サービスプロバイダー、高性能コンピューティングセンター、データセンター、キャンパス、高頻度取引環境、低（5 マイクロ秒未満のオフロード）遅延と優れたスループットを必要とするその他の環境向けに設計された、スケーラブルでキャリアグレードのモジュール式プラットフォームです。Cisco Firepower 9300 は、フローオフロード、プログラムによるオーケストレーション、および RESTful API によるセキュリティサービスの管理をサポートしています。また、Network Equipment Building Standards（NEBS）準拠の設定でも使用できます。

Cisco Firepower 3100 シリーズは、5 つの脅威に焦点を当てた NGIPS セキュリティ プラットフォームのファミリです。最大スループットは、範囲が 10 ～ 45 Gbps で、インターネットエッジ、データセンター、プライベートクラウドからのユースケースに対応します。高速の優れた脅威防御を提供します。

Cisco Firepower 4200 シリーズは、3 つの脅威に焦点を当てた NGIPS セキュリティ プラットフォームのファミリです。最大スループットは、範囲が 65 ～ 140 Gbps で、インターネットエッジ、通信サービスプロバイダーのネットワーク保護、データセンターからのユースケースに対応します。省スペース設計で、高速の優れた脅威防御を提供します。

## ライセンス

Cisco Firepower NGIPS は、Cisco Smart Licensing とともに販売されます。シスコは、ソフトウェアライセンスの購入、展開、管理、および追跡が非常に複雑になる可能性があることを理解しています。そのため、シスコスマート ソフトウェア ライセンシングを導入しています。これは、お客様がネットワーク全体でシスコのソフトウェアをどのように使用するかを理解するのに役立つ標準化されたライセンスプラットフォームであり、管理のオーバーヘッドを削減し、運用コストを節約します。

スマートライセンスを使用すると、1 つのポータルからソフトウェア、ライセンス、およびデバイスの完全なビューを得ることができます。ライセンスの登録とアクティブ化が簡単で、同一のハードウェア プラットフォーム間でシフトできます。追加情報については、https://www.cisco.com/web/ordering/smart-software-licensing/index.html およびスマートライセンスの関連情報を参照してください。

スマートアカウントについては、こちらをご覧ください。
https://www.cisco.com/web/ordering/smart-software-manager/smart-accounts.html。

## Cisco Smart Net Total Care サポート

シスコの専門知識とリソースにいつでもアクセスでき、迅速に移行できます。

受賞歴のある Cisco Smart Net Total Care™ によって、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。
- 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、マイナーリリースとメジャーリリースの両方を含む）。

- 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、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。

## 製品仕様

パフォーマンスの仕様と機能の特長

表 1 は、Cisco Firepower NGIPS 実行時の Cisco Firepower 2100、4100、9300 シリーズのアプライアンス機能をまとめたものです。

**表 1.** Firepower NGIPS でのパフォーマンス[2] の仕様と機能の特長

| 機能 | Cisco Firepower モデル | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2130 | 2140 | 4115 | 4125 | 4145 | SM-40 を搭載した 9300 | SM-48 を搭載した 9300 | SM-56 を搭載した 9300 | SM-56 x 3 を搭載した 9300 |
| スループット：NGIPS（1024B） | 4.7 Gbps | 9 Gbps | 27 Gbps | 41 Gbps | 55 Gbps | 57 Gbps | 66 Gbps | 73 Gbps | 175 Gbps |
| スループット：NGIPS（450B） | 1.5 Gbps | 3Gbps | 9 Gbps | 15 Gbps | 19 Gbps | 21 Gbps | 23 Gbps | 27 Gbps | 64 Gbps |
| 同時セッションの最大数 | 2M | 3M | 15 M | 25M | 30M | 35M | 35M | 35M | 60M |
| 1 秒あたりの最大新規接続数 | 27K | 57K | 200K | 265K | 350K | 380K | 450K | 490K | 1.1M |
| 統合インターフェイス | 12 x 1GE RJ45、4 x SFP+ | 12 x 1GE RJ45、4 x SFP+ | SFP+ X 8 | SFP+ X 8 | SFP+ X 8 | SFP+ X 8 | SFP+ X 8 | SFP+ X 8 | SFP+ X 8 |
| Fail-to-Wire（FTW）インターフェイスの最大数 | 8 x 1GE RJ45<br>6 x 1GE SX<br>6 x 10G SR<br>6 x 10G LR | | | 16 x 1GE RJ45<br>12 x 1GE SX<br>12 x 10G SR<br>12 x 10G LR<br>4 x 40G SR | | | 12 x 1GE SX<br>12 x 10G SR<br>12 x 10G LR<br>4 x 40G SR | | |
| Cisco Security Intelligence | IP、URL、DNS ベースの脅威インテリジェンスを標準装備 | | | | | | | | |
| ネットワーク向け Cisco AMP | 使用可。標的型マルウェアや執拗なマルウェアの検出、ブロッキング、追跡、分析、封じ込めを行い、連続的な攻撃に攻撃中および攻撃後のいずれのタイミングでも対応可能。また、オプションで Cisco AMP for Endpoints による統合脅威相関機能を使用可能 | | | | | | | | |
| Cisco AMP Threat Grid のサンドボックス | 利用可能 | | | | | | | | |

| 機能 | Cisco Firepower モデル | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2130 | 2140 | 4115 | 4125 | 4145 | SM-40 を搭載した 9300 | SM-48 を搭載した 9300 | SM-56 を搭載した 9300 | SM-56 x 3 を搭載した 9300 |
| **URL フィルタリング：分類されるカテゴリと URL の数** | 2 億 8000 万を超える個別の URL を使用する 80 を超えるカテゴリ | | | | | | | | |
| **自動化された脅威フィードと IPS シグネチャの更新** | あり：Cisco Talos グループ（https://www.cisco.com/c/ja_jp/products/security/talos.html）により、業界トップクラスの Collective Security Intelligence（CSI）を提供 | | | | | | | | |
| **サードパーティおよびオープンソースのエコシステム** | サードパーティ製品との統合を可能にするオープン API：Snort® および OpenAppID のコミュニティリソースにより、新しい脅威および特定の脅威に対応 | | | | | | | | |
| **集中管理** | Firepower Management Center を使用した集中管理設定、ロギング、モニタリング、およびレポート作成 | | | | | | | | |
| **高可用性とクラスタリング** | アクティブ/スタンバイ（Cisco Firepower 9300 搭載のシャーシ内クラスタリングもサポート） | | | | | | | | |
| **Cisco Trust Anchor テクノロジー** | Cisco Firepower 4100 シリーズおよび 9300 のプラットフォームには、サプライチェーンとソフトウェア イメージ アシュアランスのための Trust Anchor テクノロジーが含まれる。詳細については、以下のセクションを参照 | | | | | | | | |

[2] パフォーマンスは、アクティブになっている機能、ネットワークトラフィックのプロトコルミックス、およびパケットサイズの特性によって変化します。パフォーマンスは新しいソフトウェアのリリース時に変化することがあります。サイジングの詳細なガイダンスについては、シスコの担当者にお問い合わせください。

表 2 は、Cisco Firepower NGIPS 実行時の Cisco Firepower 4200 および 3100 シリーズのアプライアンス機能をまとめたものです。

**表 2.** Firepower NGIPS でのパフォーマンス[2] の仕様と機能の特長

| 機能 | Cisco Firepower モデル | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 3105 | 3110 | 3120 | 3130 | 3140 | 4215 | 4225 | 4245 |
| スループット：**NGIPS（1024B）** | 10G | 17G | 21G | 38G | 45G | 65G | 80G | 140G |
| スループット：**NGIPS（450B）** | 4.7G | 7G | 9.8G | 15G | 19G | 24G | 38G | 71G |
| **同時セッションの最大数** | 1.5 Mn | 2 Mn | 4 Mn | 6 Mn | 10 Mn | 15 Mn | 30 Mn | 60 Mn |
| **1 秒あたりの最大新規接続数** | 110 K | 130 K | 170 K | 240 K | 300 K | 350 K | 600 K | 800 K |
| **統合インターフェイス** | 8 x RJ45、8 x 1/10G SFP+ | | | | | 8 x 1/10/25G SFP+ | | |
| **Fail-to-Wire（FTW）インター** | - | - | - | 8 x 1GE RJ45<br>6 x 1GE SX | | 16 x 1GE RJ45<br>12 x 1GE SX | | |

| 機能 | Cisco Firepower モデル | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 3105 | 3110 | 3120 | 3130 | 3140 | 4215 | 4225 | 4245 |
| フェイスの最大数 | | | | 6 x 10G SR<br>6 x 10G LR<br>6 x 25G SR<br>6 x 25G LR | | 12 x 10G SR<br>12 x 10G LR<br>12 x 25G SR<br>12 x 25G LR | | |
| **Cisco Security Intelligence** | IP、URL、DNS の脅威インテリジェンスを標準装備 | | | | | | | |
| **Cisco Malware Defense** | 使用可。標的型マルウェアや執拗なマルウェアの検出、ブロッキング、追跡、分析、封じ込めを行い、連続的な攻撃に攻撃中および攻撃後のいずれのタイミングでも対応可能。また、オプションで Cisco Secure Endpoint による統合脅威相関機能を使用可能 | | | | | | | |
| **Cisco Secure Malware Analytics** | 使用可 | | | | | | | |
| **URL フィルタリング：分類されるカテゴリと URL の数** | 120 以上 | | | | | | | |
| **自動化された脅威フィードと IPS シグネチャの更新** | あり：Cisco Talos グループ（https://www.cisco.com/c/ja_jp/products/security/talos.html）により、業界トップクラスの Collective Security Intelligence（CSI）を提供 | | | | | | | |
| **サードパーティおよびオープンソースのエコシステム** | サードパーティ製品との統合を可能にするオープン API：Snort® および OpenAppID のコミュニティリソースにより、新しい脅威および特定の脅威に対応 | | | | | | | |
| **Cisco Trust Anchor テクノロジー** | Secure Firewall 3100 および 4200 には、サプライチェーンとソフトウェア イメージ アシュアランスのための Trust Anchor テクノロジーが含まれる。詳細については、以下のセクションを参照 | | | | | | | |

[2] パフォーマンスは、アクティブになっている機能、ネットワークトラフィックのプロトコルミックス、およびパケットサイズの特性によって変化します。パフォーマンスは新しいソフトウェアのリリース時に変化することがあります。サイジングの詳細なガイダンスについては、シスコの担当者にお問い合わせください。

## 発注情報

Cisco Firepower NGIPS、使用可能なオプション、およびハードウェア部品の発注情報については、『Cisco Network Security Ordering Guide』を参照してください。以下は、Firepower NGIPS に関連する具体的なコンポーネントをリストした一連の表です。

**表 3.** Cisco Firepower 2100 シリーズ 脅威アプライアンスバンドル

| 製品番号（アプライアンス プライマリ バンドル） | 説明 |
|---|---|
| **FPR2130-BUN（FRP2140-NGFW-K9）** | Cisco 2130 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR2140-BUN（FPR2140-NGFW-K9）** | Cisco 2140 シリーズ アプライアンス：専用 IPS として機能 |

**表 4.** Cisco Firepower 4100 シリーズ 脅威アプライアンスバンドル

| 製品番号（アプライアンス プライマリ バンドル） | 説明 |
|---|---|
| **FPR4115-BUN（FPR4115-NGIPS-K9）** | Cisco Firepower 4115 NGIPS アプライアンス、1RU、2 X ネットワークモジュールベイ |
| **FPR4125-BUN（FPR4125-NGIPS-K9）** | Cisco Firepower 4125 NGIPS アプライアンス、1RU、2 X ネットワークモジュールベイ |
| **FPR4145-BUN（FPR4145-NGIPS-K9）** | Cisco Firepower 4145 NGIPS アプライアンス、1RU、2 X ネットワークモジュールベイ |
| **ハードウェアアクセサリ** | |
| ラックマウント、スペアファン、電源、ソリッドステートドライブ（SSD）などの付属品については、発注ガイドを参照してください | |

**表 5.** Cisco Firepower 4200 シリーズ 脅威アプライアンス PID

| 製品番号（アプライアンス プライマリ バンドル） | 説明 |
|---|---|
| **FPR4215-K9** | Cisco 4215 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR4225-K9** | Cisco 4225 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR4245-K9** | Cisco 4245 シリーズ アプライアンス：専用 IPS として機能 |
| **ハードウェアアクセサリ** | |
| ラックマウント、スペアファン、電源、ソリッドステートドライブ（SSD）などの付属品については、発注ガイドを参照してください | |

**表 6.** Cisco Firepower 3100 シリーズ 脅威アプライアンス PID

| 製品番号（アプライアンス プライマリ バンドル） | 説明 |
|---|---|
| **FPR3105-NGFW-K9** | Cisco 3105 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR3110-NGFW-K9** | Cisco 3110 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR3120-NGFW-K9** | Cisco 3120 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR3130-NGFW-K9** | Cisco 3130 シリーズ アプライアンス：専用 IPS として機能 |
| **FPR3140-NGFW-K9** | Cisco 3140 シリーズ アプライアンス：専用 IPS として機能 |
| **ハードウェアアクセサリ** | |
| ラックマウント、スペアファン、電源、ソリッドステートドライブ（SSD）などの付属品については、発注ガイドを参照してください | |

**表 7.** Cisco Firepower 9300 シリーズ 脅威アプライアンスバンドル

| 製品番号（アプライアンス プライマリ バンドル） | 説明 |
|---|---|
| **FPR9K-SM40-FTD-BUN** | Cisco Firepower 9300 SM-40 FTD バンドル |
| **FPR9K-SM48-FTD-BUN** | Cisco Firepower 9300 SM-48 FTD バンドル |
| **FPR9K-SM56-FTD-BUN** | Cisco Firepower 9300 SM-56 FTD バンドル |
| ハードウェアアクセサリ | |
| ラックマウント、スペアファン、電源、ソリッドステートドライブ（SSD）などの付属品については、発注ガイドを参照してください | |

**表 8.** Cisco Firepower 2100 シリーズ Fail-to-Wire（FTW）ネットワークモジュール

| 製品番号 | 製品の説明 |
|---|---|
| **FPR2K-NM-6X10LR-F** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール |
| **FPR2K-NM-6X10LR-F=** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール（スペア） |
| **FPR2K-NM-6X10SR-F** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール |
| **FPR2K-NM-6X10SR-F=** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール（スペア） |
| **FPR2K-NM-6X1SX-F** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール |
| **FPR2K-NM-6X1SX-F=** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール（スペア） |
| **FPR2K-NM-8X1G-F** | Cisco Firepower 8 ポート 1G 銅 FTW ネットワークモジュール |
| **FPR2K-NM-8X1G-F=** | Cisco Firepower 8 ポート 1G 銅 FTW ネットワークモジュール（スペア） |

**表 9.** Cisco Firepower 4100 シリーズ Fail-to-Wire（FTW）ネットワークモジュール

| 部品番号 | 製品の説明 |
|---|---|
| **FPR4K-NM-2X40G-F** | Cisco Firepower 2 ポート 40G SR FTW ネットワークモジュール |
| **FPR4K-NM-2X40G-F=** | Cisco Firepower 2 ポート 40G SR FTW ネットワークモジュール（スペア） |
| **FPR4K-NM-6X10LR-F** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール |
| **FPR4K-NM-6X10LR-F=** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール（スペア） |
| **FPR4K-NM-6X10SR-F** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール |
| **FPR4K-NM-6X10SR-F=** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール（スペア） |
| **FPR4K-NM-6X1SX-F** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール |
| **FPR4K-NM-6X1SX-F=** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール（スペア） |

| 部品番号 | 製品の説明 |
| --- | --- |
| **FPR4K-NM-8X1G-F** | Cisco Firepower 8 ポート 1G 銅 FTW ネットワークモジュール |
| **FPR4K-NM-8X1G-F=** | Cisco Firepower 8 ポート 1G 銅 FTW ネットワークモジュール（スペア） |

**表 10.** Cisco Firepower 4200 シリーズ Fail-to-Wire（FTW）ネットワークモジュール

| 部品番号 | 製品の説明 |
| --- | --- |
| **FPR4K-XNM-6X1SXF** | Cisco 4200 アプライアンス 6X1G FTW Netmod、SX マルチモード |
| **FPR4K-XNM-6X1SXF=** | Cisco 4200 アプライアンス 6X1G FTW Netmod、SX マルチモード（スペア） |
| **FPR4K-XNM-6X10SRF** | Cisco 4200 アプライアンス 6X10G FTW Netmod、SR マルチモード |
| **FPR4K-XNM-6X10SRF=** | Cisco 4200 アプライアンス 6X10G FTW Netmod、SR マルチモード（スペア） |
| **FPR4K-XNM-6X25SRF** | Cisco 4200 アプライアンス 6X25G FTW Netmod、SR マルチモード |
| **FPR4K-XNM-6X25SRF=** | Cisco 4200 アプライアンス 6X25G FTW Netmod、SR マルチモード（スペア） |
| **FPR4K-XNM-6X25LRF** | Cisco 4200 アプライアンス 6X25G FTW Netmod、LR シングルモード |
| **FPR4K-XNM-6X25LRF=** | Cisco 4200 アプライアンス 6X25G FTW Netmod、LR シングルモード（スペア） |

**表 11.** Cisco Firepower 3100 シリーズ Fail-to-Wire（FTW）ネットワークモジュール

| 部品番号 | 製品の説明 |
| --- | --- |
| **FPR3K-XNM-6X1SXF** | Cisco 3100 アプライアンス 6X1G FTW Netmod、SX マルチモード |
| **FPR3K-XNM-6X1SXF=** | Cisco 3100 アプライアンス 6X1G FTW Netmod、SX マルチモード（スペア） |
| **FPR3K-XNM-6X10SRF** | Cisco 3100 アプライアンス 6X10G FTW Netmod、SR マルチモード |
| **FPR3K-XNM-6X10SRF=** | Cisco 3100 アプライアンス 6X10G FTW Netmod、SR マルチモード（スペア） |
| **FPR3K-XNM-6X25SRF** | Cisco 3100 アプライアンス 6X25G FTW Netmod、SR マルチモード |
| **FPR3K-XNM-6X25SRF=** | Cisco 3100 アプライアンス 6X25G FTW Netmod、SR マルチモード（スペア） |
| **FPR3K-XNM-6X25LRF** | Cisco 3100 アプライアンス 6X25G FTW Netmod、LR シングルモード |
| **FPR3K-XNM-6X25LRF=** | Cisco 3100 アプライアンス 6X25G FTW Netmod、LR シングルモード（スペア） |

**表 12.** Cisco Firepower 9300 シリーズ Fail-to-Wire（FTW）ネットワークモジュール

| 部品番号 | 製品の説明 |
| --- | --- |
| **FPR9K-NM-2X40G-F** | Cisco Firepower 2 ポート 40G SR FTW ネットワークモジュール |
| **FPR9K-NM-2X40G-F=** | Cisco Firepower 2 ポート 40G SR FTW ネットワークモジュール（スペア） |
| **FPR9K-NM-6X10LR-F** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール |
| **FPR9K-NM-6X10LR-F=** | Cisco Firepower 6 ポート 10G LR FTW ネットワークモジュール（スペア） |
| **FPR9K-NM-6X10SR-F** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール |
| **FPR9K-NM-6X10SR-F=** | Cisco Firepower 6 ポート 10G SR FTW ネットワークモジュール（スペア） |
| **FPR9K-NM-6X1SX-F** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール |
| **FPR9K-NM-6X1SX-F=** | Cisco Firepower 6 ポート 1G SX 光ファイバ FTW ネットワークモジュール（スペア） |

## 保証情報

すべてのシスコのハードウェアおよびソフトウェア製品は、少なくとも 90 日間保証されます。一部の製品については、保証期間が長くなります。Firepower NGIPS 製品の製品保証の詳細については、https://www.cisco.com/c/ja_jp/products/warranty-listing.html を参照してください。

## Cisco Firepower NGIPS 向けのシスコおよびパートナーのサービス

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。Cisco Firepower NGIPS の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、および他社製製品を購入するのに、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。

## 次の手順

Cisco Firepower NGIPS 脅威アプライアンスの詳細については、https://www.cisco.com/go/ngips を参照してください。

Cisco Advanced Malware Protection の詳細については、https://www.cisco.com/go/amp を参照してください。

シスコの Talos Security Intelligence and Research Group の詳細については、
https://www.talosintelligence.com/ を参照してください。

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 C78-742472-03 07/25