

# Cisco Firepower NGIPS シリーズ マイグレーション オプション

## ネットワークの防御力を強化

昨今の攻撃者は、どのような組織に対してもいつでも攻撃をしかけられるだけのリソースと専門的知識を持ち、長期にわたって執拗に攻撃を加えてきます。従来の対策ではもはや通用しません。

ネットワーク資産やデータを最新の脅威から守るには、すべてのネットワーク レイヤおよびリソースを詳細に見渡せる可視性が必要です。そのためには、包括的な最新のセキュリティ インテリジェンスが必要になります。認識機能と自動化を使用して、新しい脅威、新しい脆弱性、日常的なネットワークの変化に適応するダイナミックなアプローチが求められます。

そこで必要とされるのが、Cisco Firepower® NGIPS（次世代侵入防御システム）脅威アプライアンスです。

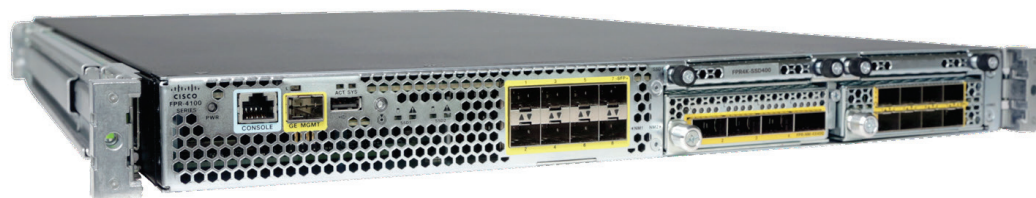
次世代ファイアウォール（NGFW）の採用によってスタンドアロンの侵入防御システム（IPS）の必要性はなくなると考える人は少なくありません。しかし、それは決して真実ではありません。「真の」NGIPS は、可視性を提供し、脅威の検出や対応を行い、マルウェアを検知することができます。また、ファイアウォールの検査と制御が及ばないネットワーク領域で、それらすべてを実行できます。

Cisco Firepower NGIPS 脅威アプライアンスは、既知と未知の双方の脅威に対して、業界トップクラスの可視性と保護能力を発揮します。

Cisco Firepower NGIPS は、次の機能を使用して脅威を阻止します。

- ・ 30,000 超の IPS ルール。ネットワーク内の脆弱性のエクスプロイトを試みるトラフィックを識別してブロック
- ・ レピュテーションベースの IP、URL、DNS セキュリティ インテリジェンス。悪意のあるサイトを識別することで攻撃対象領域の縮小が可能
- ・ 緊密に統合された防御。ネットワークベースの高度なマルウェア攻撃に対抗
- ・ 統合型のサンドボックス テクノロジー。数百の侵入兆候に基づいてゼロデイ攻撃を見極め
- ・ 侵害の兆候（IoC）機能。複数のソースからイベントを関連付けることで、侵害された可能性のあるホストを識別

今すぐ Cisco Firepower NGIPS にアップグレードして、顧客のネットワーク、ユーザ、アプリケーション、情報資産の保護に役立ててください。



## アップグレードは、簡単です

1. 現在の IPS モデルと更新のニーズを確認します。
2. 推奨される移行パスを確認します。
3. 信頼できるシスコ セキュリティ アカウント マネージャまたはパートナーに連絡します。

# Cisco IPS および Firepower (旧 Sourcefire) をご利用のお客様向けのマイグレーションに 推奨される製品

Cisco IDS/IPS 4000 アプライアンス	推奨製品	スループット パフォーマンスの向上
Cisco IPS 4270-20	Firepower 4110	2 倍
Cisco IPS 4360	Firepower 4110	3.2 倍
Cisco IPS 4510	Firepower 4110	1.33 倍
Cisco IPS 4520	Firepower 4120	1.6 倍
Cisco IPS 4520-XL	Firepower 4140	1 倍

FirePOWER 81xx アプライアンス	推奨製品	スループット パフォーマンスの向上
FirePOWER 8120	Firepower 4110	2 倍
FirePOWER 8130	Firepower 4110	1 倍
FirePOWER 8140	Firepower 4120	1.33 倍
Firepower 8xxxx AMP アプライアンス		
FirePOWER AMP 8050	Firepower 4110 AMP	1.5 倍
FirePOWER AMP 8150	Firepower 4120 AMP	1.2 倍
FirePOWER AMP 8150	Firepower 4140 AMP	2 倍

Cisco Firepower NGIPS 脅威アプライアンスの詳細については、[https://www.cisco.com/c/ja\\_jp/products/security/ngips/index.html](https://www.cisco.com/c/ja_jp/products/security/ngips/index.html)を参照してください。

Cisco Advanced Malware Protection の機能の詳細については、<http://www.cisco.com/jp/go/amp/>を参照してください。

Cisco Talos セキュリティ インテリジェンス & リサーチ チームの詳細については、<http://www.cisco.com/jp/go/talos>を参照してください。