



ハイブリッドワークやマルチクラウド環境に最適な次世代ファイアウォールカタログ

# Cisco Secure Firewall



Cisco Secure Firewall 概要	02
Cisco Secure Firewall ポートフォリオ	04
Cisco Firepower 1000 シリーズ	06
Cisco Secure Firewall 3100 シリーズ	08
Cisco Secure Firewall 4200 シリーズ <b>NEW</b>	10
Cisco Secure Firewall Threat Defense (FTD) Virtual	12
Cisco Secure Firewall ASA Virtual	14
Cisco Secure Firewall ライセンス	16
Cisco Secure Firewall 管理ツール	18
Cisco Secure Firewall 移行ガイド	19

2024 年 6 月版

# Cisco Secure Firewall 概要

## ハイブリッドワークやマルチクラウド環境に最適な次世代ファイアウォール

今日のビジネス環境ではパンデミックの到来によるテレワークの急増もあり、オンライン会議やオンラインストレージなど、クラウドアプリケーションやクラウドサービスの利用が急拡大しています。さらに今後もハイブリッドワークなど自由な働き方へのシフトが加速し、クラウド利用がますます増加することが予想されます。

4.7倍

テレワーク（在宅勤務）ユーザーが  
パンデミック前の平均から **4.7倍** に増加<sup>\*1</sup>

62%

オフィス出社を安全に再開するために  
**62%** の組織がオンライン会議の導入を促進<sup>\*1</sup>

21%

パンデミック関連の設備投資対策として  
**21%** の企業がワークロードをパブリッククラウドに移行<sup>\*1</sup>

したがって企業ネットワークでは、一過性の課題としてではなく継続的な課題として、テレワーカーやハイブリッドワーカー、およびクラウドアクセスの増加に対応する必要があります。とりわけ重要な課題となるのが、ネットワークとともに複雑化するセキュリティの確保です。オフィス内からオフィス外へとユーザーやアプリ、リソースが分散し、複雑化するネットワークでは、セキュリティとユーザーエクスペリエンスを両立させるパフォーマンスを確保するのはもちろんのこと、エンドツーエンドでセキュアなネットワークを実現するための可視性や管理性を確保することもまた困難になります。

56%

複雑化するネットワークにおける最大の課題として  
**56%** の IT 担当者が「セキュリティ」と回答<sup>\*2</sup>

50%

複雑化するネットワークにおける最大の課題として  
**50%** の IT 担当者が「管理性」と回答<sup>\*2</sup>

53%

複雑化するネットワークで役立つテクノロジーとして  
**53%** の IT 担当者が「可視性」と回答<sup>\*2</sup>

Cisco Secure Firewall は、複雑化し、変化を続けるネットワークおよび脅威にも対抗できる、統合セキュリティプラットフォームの基礎となるファイアウォールです。業界をリードする Snort 3 侵入防御システム (Intrusion Prevention System ; IPS) や TLS 1.3 で暗号化されたレイヤ 7 トラフィックを復号せずに可視化および制御できる Encrypted Visibility Engine (EVE) など、シスコ独自のセキュリティ機能だけでなく、世界最大の脅威インテリジェンスの 1 つである Cisco Talos による最新かつ最先端のデータベースを活用してネットワークを保護できます。

物理、仮想、およびクラウドネイティブな各種ファイアウォールで構成される充実したポートフォリオによって、あらゆるユースケースに対応可能。それらをクラウドまたはオンプレミスで一元管理できるだけでなく、シスコの各種セキュリティソリューションを統合する Cisco XDR など、さまざまなシスコセキュリティ製品と連携させて効率的に運用できます。



### 卓越したパフォーマンス

従来モデルの 1.3 ~ 18 倍のパフォーマンス



### Snort 3 侵入防御システム

最も巧妙な攻撃にも対抗できる  
業界をリードする侵入防御システム



### 高度なマルウェア防御

マルウェアからネットワークを保護  
万が一の感染時も遡って検知および追跡可能



### 暗号化されたトラフィックを復号せずに可視化

TLS 1.3 暗号化トラフィックを可視化  
レイヤ 7 ルールを適用可能



### 物理および仮想ファイアウォール

ハードウェアアプライアンスだけでなく  
クラウドネイティブなソフトウェアでも提供



### 一元管理

オンプレミスまたはクラウドで  
複数のファイアウォールを一元管理可能



### 世界最大の脅威インテリジェンス

Snort ルールセットなど  
常に最新のデータベースで更新



### XDR

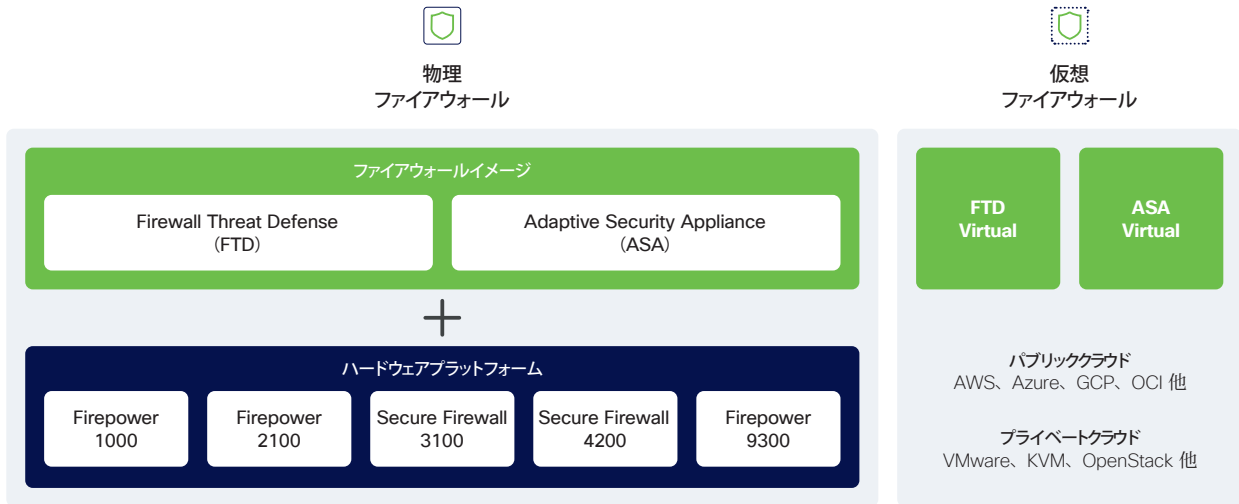
Cisco XDR に統合可能  
より迅速に脅威を検知、調査、対応可能

\*1 詳細は『2021 年グローバル ネットワーキングトレンドレポート』を参照。

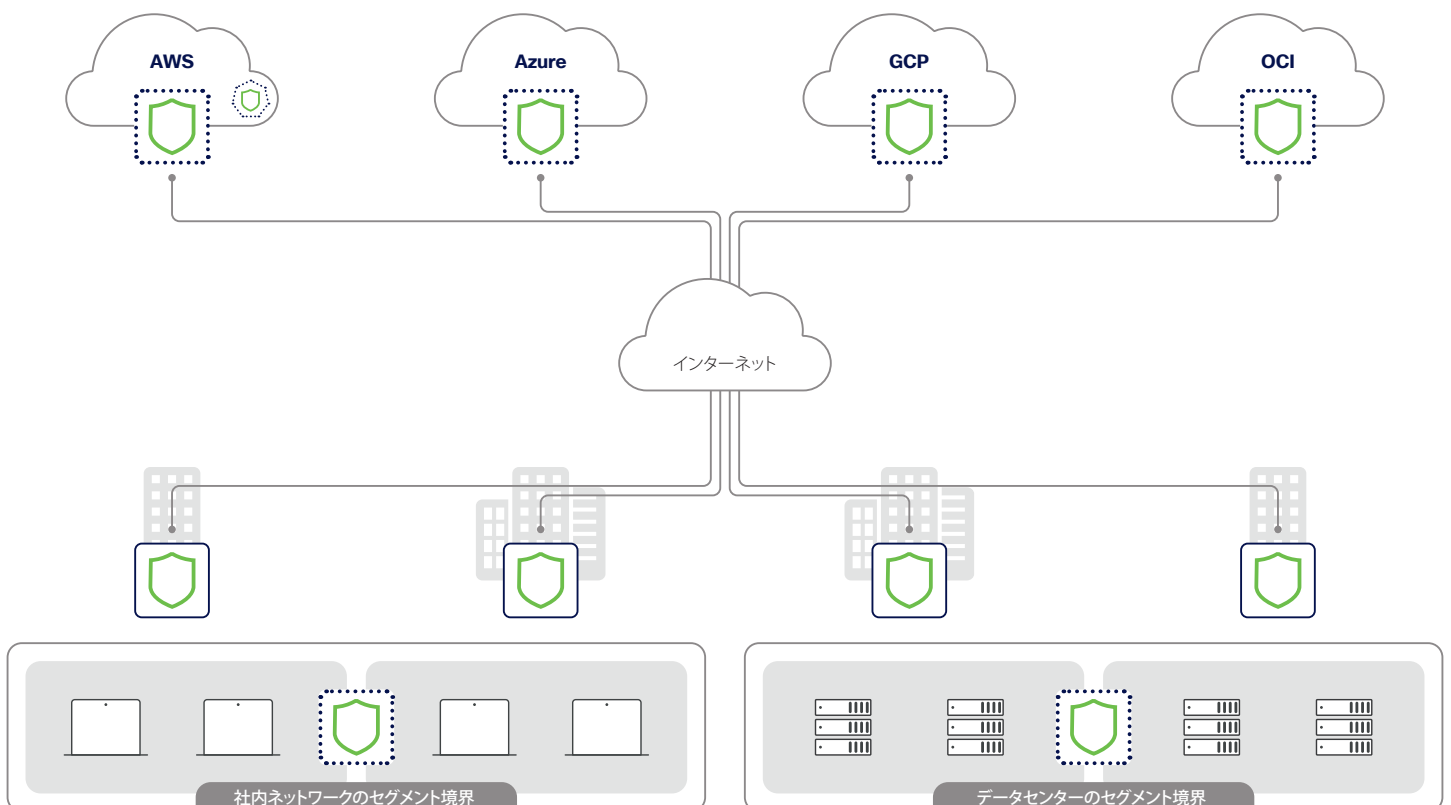
\*2 詳細は『2023 Global Networking Trends Report』を参照。

## あらゆるユースケースに対応できる柔軟なポートフォリオ

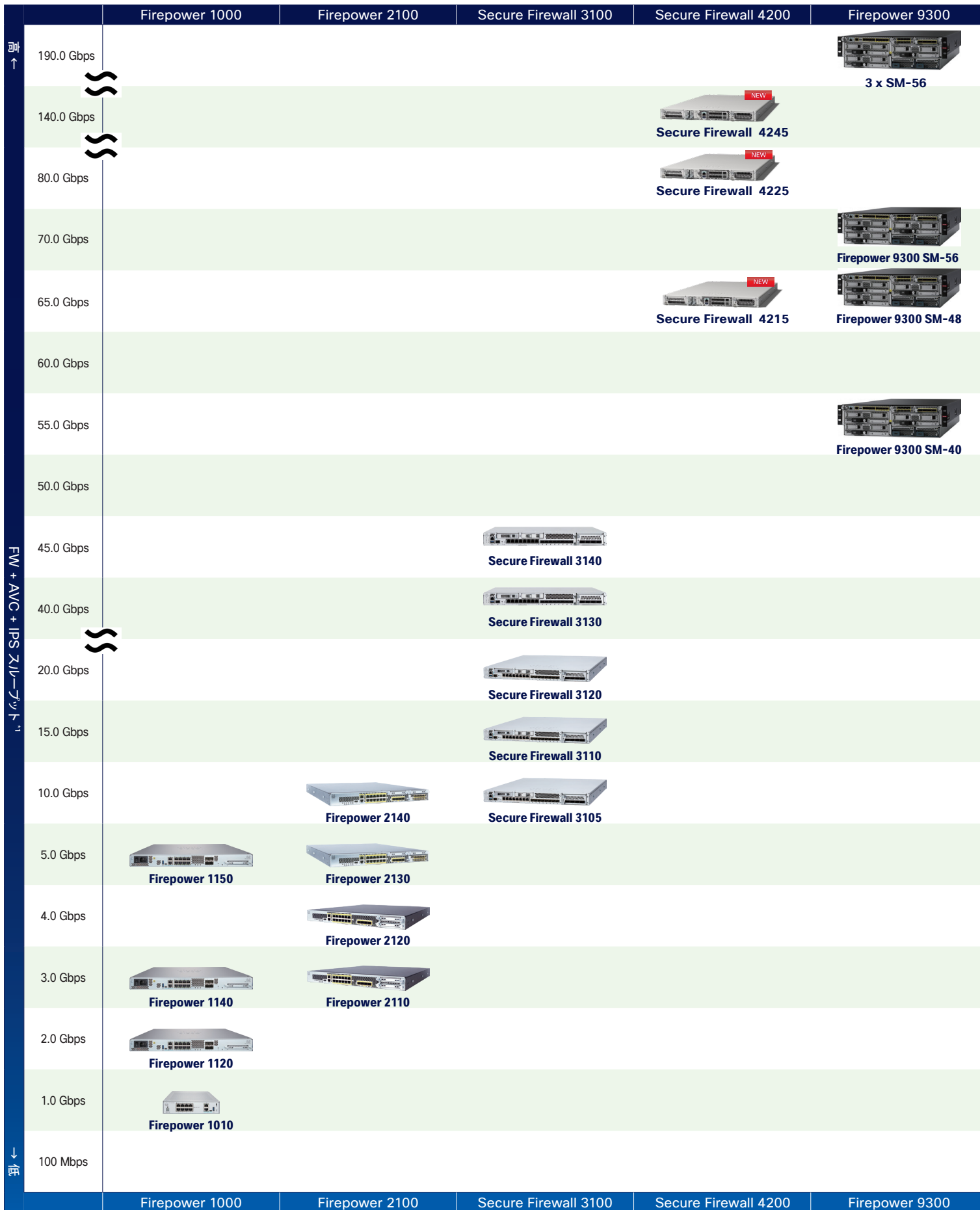
Cisco Secure Firewall は、小規模向けから大規模向けまで幅広いラインアップの物理ファイアウォール、プライベートおよびパブリッククラウドでスケール可能な仮想ファイアウォールで構成されます。物理および仮想ファイアウォールは、Snort 3 侵入防御システムや高度なマルウェア防御を含むレイヤ 7 次世代ファイアウォールとして機能する Firewall Threat Defense (FTD) ソフトウェアイメージ、または長年にわたって実績を積み上げてきたレイヤ 3 & 4 ベーシックファイアウォールとして機能する Adaptive Security Appliance (ASA) ソフトウェアイメージを選択できます。



\*1 詳細は『2021年グローバルネットワーキングトレンドレポート』を参照。  
\*2 詳細は『2023 Global Networking Trends Report』を参照。



## Cisco Secure Firewall ポートフォリオ (FTD)



## Secure Firewall Threat Defense (FTD) Virtual

70.0 Gbps



65.0 Gbps

60.0 Gbps

55.0 Gbps

50.0 Gbps

45.0 Gbps

40.0 Gbps

35.0 Gbps

30.0 Gbps

25.0 Gbps

20.0 Gbps

15.0 Gbps

10.0 Gbps

5.0 Gbps

4.0 Gbps

3.0 Gbps

2.0 Gbps

1.0 Gbps

100 Mbps

FW + AVC + IPS スループット<sup>\*1</sup>

## クラスターパフォーマンス

Cisco Secure Firewall 3100 シリーズ、4200 シリーズ、Cisco Firepower 9300 シリーズ、Cisco Secure Firewall Threat Defense (FTD) Virtual はクラスタリングをサポートします。クラスター全体の最大スループットは、クラスターを構成する各ノードの最大スループット合計の約 80% です。たとえば、単独で最大 10.0 Gbps スループットのノード 8 台で構成されるクラスター全体の最大スループットは、 $10.0 \times 8 \times 0.8 = 64.0$  Gbps です。



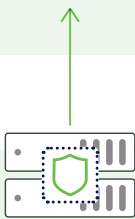
8 × Secure Firewall 3140  
288.0 Gbps  
FW + AVC + IPS<sup>\*1</sup>



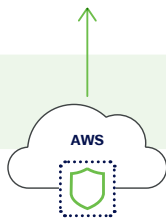
8 × Firepower 4245  
900 Gbps  
FW + AVC + IPS<sup>\*1</sup>



6 × Firepower 9000 SM-56  
326.4 Gbps  
FW + AVC + IPS<sup>\*1</sup>



FTDv on ESXi/KVM/OpenStack



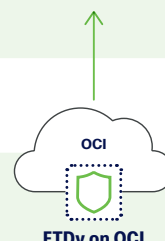
FTDv on AWS



FTDv on Azure



FTDv on GCP



FTDv on OCI

## Secure Firewall Threat Defense (FTD) Virtual

\*1 1,024 バイト HTTP トラフィック。

# Cisco Firepower 1000 シリーズ

## Cisco Firepower 1010

890 Mbps  
FW + AVC  
(FTD)

880 Mbps  
FW + AVC + IPS  
(FTD)

400 Mbps  
IPsec VPN  
(FTD)

75 ヒア  
IPsec VPN  
(FTD)

5 インスタンス  
VRF  
(FTD)

6 × 1GE  
RJ45

2 × 1GE  
PoE+ RJ45

1 × 内蔵 SSD<sup>\*1</sup>

電源アダプタ

ファンレス



## Cisco Firepower 1120

2.3 Gbps  
FW + AVC  
(FTD)

2.3 Gbps  
FW + AVC + IPS  
(FTD)

1.2 Gbps  
IPsec VPN  
(FTD)

150 ヒア  
IPsec VPN  
(FTD)

5 インスタンス  
VRF  
(FTD)

8 × 1GE  
RJ45

4 × 1GE  
SFP

1 × SSD  
スロット<sup>\*2</sup>

1 × 内蔵電源



## Cisco Firepower 1140

3.3 Gbps  
FW + AVC  
(FTD)

3.3 Gbps  
FW + AVC + IPS  
(FTD)

1.4 Gbps  
IPsec VPN  
(FTD)

400 ヒア  
IPsec VPN  
(FTD)

10 インスタンス  
VRF  
(FTD)

8 × 1GE  
RJ45

4 × 1GE  
SFP

1 × SSD  
スロット<sup>\*2</sup>

1 × 内蔵電源



## Cisco Firepower 1150

5.3 Gbps  
FW + AVC  
(FTD)

4.9 Gbps  
FW + AVC + IPS  
(FTD)

2.4 Gbps  
IPsec VPN  
(FTD)

800 ヒア  
IPsec VPN  
(FTD)

10 インスタンス  
VRF  
(FTD)

8 × 1GE  
RJ45

2 × 1GE  
SFP

2 × 10GE  
SFP+

1 × SSD  
スロット<sup>\*2</sup>

1 × 内蔵電源



\*1 デフォルトで 1 × 200 GB SSD を搭載 (現場交換不可)。 \*2 デフォルトでは 1 × 200 GB SSD を搭載。

## ハードウェア製品型番 &amp; 仕様

## Cisco Firepower 1000 シリーズ

製品型番		ダウンリンク / アップリンク ポート							ストレージ		電源	
FTD モデル (FTD イメージで出荷)	ASA モデル (ASA イメージで出荷)	1GE RJ45	1GE SFP	10GE SFP+	25GE SFP28	40GE QSFP+	100GE QSFP28	NM スロット	スロット	デフォルト	スロット	デフォルト
FPR1010-NGFW-K9 <sup>*1</sup>	FPR1010-ASA-K9	8 <sup>*2</sup>								1 × 200 GB M.2 SATA SSD		115 W AC 電源アダプタ
FPR1010E-NGFW-K9 <sup>*1</sup>	FPR1010E-ASA-K9	8								1 × 200 GB M.2 SATA SSD		115 W AC 電源アダプタ
FPR1120-NGFW-K9 <sup>*1</sup>	FPR1120-ASA-K9	8	4						1	1 × 200 GB SATA SSD		1 × 100 W AC
FPR1140-NGFW-K9 <sup>*1</sup>	FPR1140-ASA-K9	8	4						1	1 × 200 GB SATA SSD		1 × 100 W AC
FPR1150-NGFW-K9 <sup>*1</sup>	FPR1150-ASA-K9	8	2	2					1	1 × 200 GB SATA SSD		1 × 100 W AC

\*1 CCW では FPRnnnn-BUN を推奨 (nnnn は対応モデル番号)。同一構成 2 台の高可用性バンドル製品型番は FPRnnnn-FTD-HA-BUN (nnnn は対応モデル番号)。\*2 PoE+ 給電対応 2 ポートを含む。

## パフォーマンス

## Cisco Firepower 1000 シリーズ FTD モデル

指標	1010	1120	1140	1150
FW + AVC スループット <sup>*1</sup>	890 Mbps	2.3 Gbps	3.3 Gbps	5.3 Gbps
FW + AVC + IPS スループット <sup>*1</sup>	890 Mbps	2.3 Gbps	3.3 Gbps	4.9 Gbps
FW 同時セッション数 (AVC 有効時の最大)	100,000	200,000	400,000	600,000
FW 新規接続数 / 秒 (AVC 有効時の最大)	6,000	15,000	22,000	28,000
IPS スループット <sup>*1</sup>	900 Mbps	2.6 Gbps	3.5 Gbps	6.1 Gbps
TLS スループット <sup>*2</sup>	195 Mbps	850 Mbps	1.2 Gbps	1.4 Gbps
IPsec VPN スループット <sup>*3</sup>	400 Mbps	1.2 Gbps	1.4 Gbps	2.4 Gbps
IPsec VPN スループット <sup>*3</sup> (IPsec フローオフロード <sup>*4</sup> 有効時の予測値)				
VPN ピア数 (最大)	75	150	400	800
VRF インスタンス数 (最大)	5	5	10	10
クラスタリング				

\*1 1,024 バイト HTTP トラフィック。\*2 RSA 2,048 ビットキーと AES256-SHA 暗号化を使用した TLS 1.2 トラフィックが 50% の想定。  
\*3 1,024 バイト TCP トラフィック、Fastpath 有効時。\*4 Secure Firewall 3100 でサポート。

## Cisco Firepower 1000 シリーズ ASA モデル

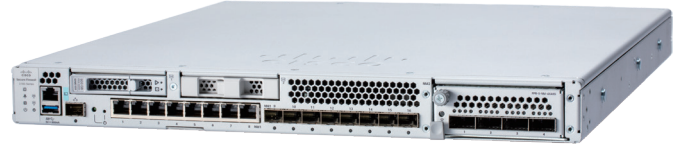
指標	1010	1120	1140	1150
ステートフル インスペクション FW スループット <sup>*1</sup>	2.0 Gbps	4.5 Gbps	6.0 Gbps	7.5 Gbps
ステートフル インスペクション FW スループット (マルチプロトコル <sup>*2</sup> )	1.4 Gbps	2.5 Gbps	3.5 Gbps	4.5 Gbps
FW 同時セッション数 (最大)	100,000	200,000	400,000	600,000
FW 新規接続数 / 秒 (最大)	25,000	75,000	100,000	150,000
IPsec VPN スループット <sup>*3</sup>	500 Mbps	1.0 Gbps	1.2 Gbps	1.7 Gbps
IPsec VPN スループット <sup>*3</sup> (IPsec フローオフロード <sup>*4</sup> 有効時の予測値)				
VPN ピア数 (最大)	75	150	400	800
セキュリティコンテキスト (デフォルト / 最大)		2 / 5	2 / 5	2 / 25
クラスタリング				

\*1 1,500 バイト UDP トラフィック。\*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。  
\*3 450 バイト UDP L2L トラフィック。\*4 Secure Firewall 3100 でサポート。

# Cisco Secure Firewall 3100 シリーズ

## Cisco Secure Firewall 3105

10.0 Gbps FW + AVC (FTD)	10.0 Gbps FW + AVC + IPS (FTD)	5.5 Gbps IPsec VPN (FTD)	2,000 ピア IPsec VPN (FTD)	10 インスタンス VRF (FTD)	8 ノード クラスター (FTD)
8 × 1GE RJ45	8 × 10GE SFP+	1 × ネットワーク モジュール スロット	Fail-To-Wire ネットワーク モジュール		
2 × SSD スロット <sup>*2</sup>	2 × 電源 モジュール スロット <sup>*3</sup>				



## Cisco Secure Firewall 3110

17.0 Gbps FW + AVC (FTD)	17.0 Gbps FW + AVC + IPS (FTD)	11.0 Gbps IPsec VPN (FTD)	3,000 ピア IPsec VPN (FTD)	15 インスタンス VRF (FTD)	マルチ インスタンス <sup>*1</sup> (FTD)	8 ノード クラスター (FTD)
8 × 1GE RJ45	8 × 10GE SFP+	1 × ネットワーク モジュール スロット	Fail-To-Wire ネットワーク モジュール			
2 × SSD スロット <sup>*2</sup>	2 × 電源 モジュール スロット <sup>*3</sup>					



## Cisco Secure Firewall 3120

21.0 Gbps FW + AVC (FTD)	21.0 Gbps FW + AVC + IPS (FTD)	13.5 Gbps IPsec VPN (FTD)	7,000 ピア IPsec VPN (FTD)	25 インスタンス VRF (FTD)	マルチ インスタンス <sup>*1</sup> (FTD)	8 ノード クラスター (FTD)
8 × 1GE RJ45	8 × 10GE SFP+	1 × ネットワーク モジュール スロット	Fail-To-Wire ネットワーク モジュール			
2 × SSD スロット <sup>*2</sup>	2 × 電源 モジュール スロット <sup>*3</sup>					



## Cisco Secure Firewall 3130

38.0 Gbps FW + AVC (FTD)	38.0 Gbps FW + AVC + IPS (FTD)	33.0 Gbps IPsec VPN (FTD)	15,000 ピア IPsec VPN (FTD)	50 インスタンス VRF (FTD)	マルチ インスタンス <sup>*1</sup> (FTD)	8 ノード クラスター (FTD)
8 × 1GE RJ45	8 × 25GE SFP28	1 × ネットワーク モジュール スロット	Fail-To-Wire ネットワーク モジュール			
2 × SSD スロット <sup>*2</sup>	2 × 電源 モジュール スロット <sup>*4</sup>					



## Cisco Secure Firewall 3140

45.0 Gbps FW + AVC (FTD)	45.0 Gbps FW + AVC + IPS (FTD)	39.4 Gbps IPsec VPN (FTD)	20,000 ピア IPsec VPN (FTD)	100 インスタンス VRF (FTD)	マルチ インスタンス <sup>*1</sup> (FTD)	8 ノード クラスター (FTD)
8 × 1GE RJ45	8 × 25GE SFP28	1 × ネットワーク モジュール スロット	Fail-To-Wire ネットワーク モジュール			
2 × SSD スロット <sup>*2</sup>	2 × 電源 モジュール スロット <sup>*4</sup>					



\*1 将来のソフトウェアリリースで対応予定。 \*2 デフォルトで 1 × 900 GB SSD を搭載。 \*3 デフォルトで 1 × 400 W AC 電源モジュールを搭載。 \*4 デフォルトで 2 × 400 W AC 電源モジュールを搭載。



## ハードウェア製品型番 & 仕様

### Cisco Firepower 3100 シリーズ

製品型番 <sup>*1</sup>		ダウンリンク / アップリンク ポート (ネットワークモジュール搭載ポート)							ストレージ		電源	
FTD モデル (FTD イメージで出荷)	ASA モデル (ASA イメージで出荷)	1GE RJ45	1GE SFP	10GE SFP+	25GE SFP28	40GE QSFP+	100GE QSFP28	NM スロット	スロット	デフォルト	スロット	デフォルト
FPR3105-NGFW-K9	FPR3105-ASA-K9	8		8 (8)				1	2	1 × 900 GB NVMe SSD	2	1 × 400 W AC
FPR3110-NGFW-K9	FPR3110-ASA-K9	8		8 (8)				1	2	1 × 900 GB NVMe SSD	2	1 × 400 W AC
FPR3120-NGFW-K9	FPR3120-ASA-K9	8		8 (8)				1	2	1 × 900 GB NVMe SSD	2	1 × 400 W AC
FPR3130-NGFW-K9	FPR3130-ASA-K9	8		(8)	8 (8)	(4)		1	2	1 × 900 GB NVMe SSD	2	2 × 400 W AC
FPR3140-NGFW-K9	FPR3140-ASA-K9	8		(8)	8 (8)	(4)		1	2	1 × 900 GB NVMe SSD	2	2 × 400 W AC

\*1 CCW では FPRnnn-BUN を推奨 (nnn は対応モデル番号)。FTD モデル同一構成 2 台の高可用性バンドル製品型番は FPR3100-FTD-HA-BUN。

### Cisco Firepower 3100 シリーズ用ネットワークモジュール

製品型番	製品説明	対応モデル				
		3105	3110	3120	3130	3140
FPR3K-XNM-8X10G	8 × 10GE SFP+ ネットワークモジュール	✓	✓	✓	✓	✓
FPR3K-XNM-8X25G	8 × 25GE SFP28 ネットワークモジュール				✓	✓
FPR3K-XNM-4X40G	4 × 40GE QSFP+ ネットワークモジュール				✓	✓



FPR3K-XNM-8X10G



FPR3K-XNM-4X40G

## パフォーマンス

### Cisco Firepower 3100 シリーズ FTD モデル

指標	3105	3110	3120	3130	3140
FW + AVC スループット <sup>*1</sup>	10.0 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
FW + AVC + IPS スループット <sup>*1</sup>	10.0 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
FW 同時セッション数 (AVC 有効時の最大)	1,500,000	2,000,000	4,000,000	6,000,000	10,000,000
FW 新規接続数 / 秒 (AVC 有効時の最大)	90,000	130,000	170,000	240,000	300,000
IPS スループット <sup>*1</sup>	10.0 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
TLS スループット <sup>*2</sup>	3.2 Gbps	4.8 Gbps	6.7 Gbps	9.1 Gbps	11.5 Gbps
IPsec VPN スループット <sup>*3</sup>	5.5 Gbps	8.0 Gbps	10.0 Gbps	17.8 Gbps	22.4 Gbps
IPsec VPN スループット <sup>*3</sup> (IPsec フローオフロード <sup>*4</sup> 有効時の予測値)	NA	11.0 Gbps	13.5 Gbps	33.0 Gbps	39.4 Gbps
VPN ヒア数 (最大)	2,000	3,000	6,000	15,000	20,000
VRF インスタンス数 (最大)	10	15	25	50	100
FTD インスタンス数 (最大)	NA	2	2	4	5
クラスタリング	8	8	8	8	8

\*1 1,024 バイト HTTP トラフィック。 \*2 RSA 2,048 ビットキーと AES256-SHA 暗号化を使用した TLS 1.2 トラフィックが 50% の想定。  
\*3 1,024 バイト TCP トラフィック。 Fastpath 有効時。 \*4 FTD バージョン 7.2 以降でサポート。

### Cisco Firepower 3100 シリーズ ASA モデル

指標	3105	3110	3120	3130	3140
ステートフル インスペクション FW スループット <sup>*1</sup>	10.0 Gbps	18.0 Gbps	22.0 Gbps	42.0 Gbps	49.0 Gbps
ステートフル インスペクション FW スループット (マルチプロトコル <sup>*2</sup> )	9.0 Gbps	15.0 Gbps	17.0 Gbps	39.0 Gbps	43.0 Gbps
FW 同時セッション数 (最大)	1,500,000	2,000,000	4,000,000	6,000,000	10,000,000
FW 新規接続数 / 秒 (最大)	150,000	300,000	500,000	875,000	1,100,000
IPsec VPN スループット <sup>*3</sup>	5.5 Gbps	8.0 Gbps	10.0 Gbps	14 Gbps	17 Gbps
IPsec VPN スループット <sup>*3</sup> (IPsec フローオフロード <sup>*4</sup> 有効時の予測値)	TBD	12.0 Gbps	15.4 Gbps	28.0 Gbps	33.0 Gbps
VPN ヒア数 (最大)	2,000	3,000	7,000	15,000	20,000
セキュリティコンテキスト (デフォルト / 最大)	2 / 100	2 / 100	2 / 100	2 / 100	2 / 100
クラスタリング	8	8	8	8	8

\*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。  
\*3 450 バイト UDP L2L トラフィック。 \*4 ASA バージョン 9.18 以降でサポート。

# Cisco Secure Firewall 4200 シリーズ NEW

## Cisco Secure Firewall 4215

65.0 Gbps  
FW + AVC  
(FTD)

65.0 Gbps  
FW + AVC + IPS  
(FTD)

45 Gbps  
IPsec VPN  
(FTD)

20,000 ピア  
IPsec VPN  
(FTD)

8 ノード  
クラスター  
(FTD)

8 × 25GE  
SFP28

2 × ネットワーク  
モジュール  
スロット

Fail-To-Wire  
ネットワーク  
モジュール

2 × SSD  
スロット<sup>\*1</sup>

2 × 電源  
モジュール  
スロット<sup>\*2</sup>



## Cisco Secure Firewall 4225

80.0 Gbps  
FW + AVC  
(FTD)

80.0 Gbps  
FW + AVC + IPS  
(FTD)

80 Gbps  
IPsec VPN  
(FTD)

25,000 ピア  
IPsec VPN  
(FTD)

8 ノード  
クラスター  
(FTD)

8 × 25GE  
SFP28

2 × ネットワーク  
モジュール  
スロット

Fail-To-Wire  
ネットワーク  
モジュール

2 × SSD  
スロット<sup>\*1</sup>

2 × 電源  
モジュール  
スロット<sup>\*2</sup>



## Cisco Secure Firewall 4225

140.0 Gbps  
FW + AVC  
(FTD)

140.0 Gbps  
FW + AVC + IPS  
(FTD)

140 Gbps  
IPsec VPN  
(FTD)

30,000 ピア  
IPsec VPN  
(FTD)

8 ノード  
クラスター  
(FTD)

8 × 10GE  
SFP+

2 × ネットワーク  
モジュール  
スロット

Fail-To-Wire  
ネットワーク  
モジュール

2 × SSD  
スロット<sup>\*3</sup>

2 × 電源  
モジュール  
スロット<sup>\*4</sup>



\*1 デフォルトで 2 × 1.8 TB SSD を搭載。\*2 デフォルトで 1 x 1900 W AC 電源モジュールを搭載。\*3 デフォルトで 2 x 1900 W AC 電源モジュールを搭載。

## ハードウェア製品型番 & 仕様

### Cisco Secure Firewall 4200 シリーズ

FTD モデル (FTD イメージで出荷)	ASA モデル (ASA イメージで出荷)	ダウンリンク / アップリンク ポート (ネットワークモジュール搭載ポート)							ストレージ		電源	
		1GE RJ45	1GE SFP	10GE SFP+	25GE SFP28	40GE QSFP+	100GE QSFP28	NM スロット	スロット	デフォルト	スロット	デフォルト
FPR4215-NGFW-K9	FPR4215-ASA-K9		(24)	(24)	8 (24)	(8)	(8)	2	2	2 × 1.8 TB SSD	2	1 × 1,200 W AC 1 × 1,900 W AC
FPR4225-NGFW-K9	FPR4225-ASA-K9		(24)	(24)	8 (24)	(8)	(8)	2	2	2 × 1.8 TB SSD	2	1 × 1,200 W AC 1 × 1,900 W AC
FPR4245-NGFW-K9	FPR4245-ASA-K9		(24)	(24)	8 (24)	(8)	(8)	2	2	2 × 1.8 TB SSD	2	1 × 1,200 W AC 1 × 1,900 W AC

\*1 CCW では FPRnnnn-BUN を推奨 (nnnn は対応モデル番号)。FTD モデル同一構成 2 台の高可用性バンドル製品型番は FPRnnnn-FTD-HA-BUN (nnnn は対応モデル番号)。

### Cisco Secure Firewall 4200 シリーズ用ネットワークモジュール (一部抜粋)

製品型番	製品説明	対応モデル		
		4215	4225	4245
FPR-X-NM-8X10G	8 ポート 1/10Gb SFP+	✓	✓	✓
FPR-X-NM-8X25G	8 ポート 1/10/25Gb SFP+	✓	✓	✓
FPR-X-NM-4X40G	4 ポート 40 Gb QSFP/QSFP+	✓	✓	✓
FPR-X-NM-4X200G	4 ポート 40/100/200 Gb QSFP28/QSFP	✓	✓	✓
FPR-XNM-2X100G	2 ポート 100-Gb QSFP56/QSFP28/QSFP	✓	✓	✓
FPR-X-NM-6X25LRF	6 ポート 25 Gb SFP LR シングルモード ハードウェア バイパス	✓	✓	✓
FPR-X-NM-8X1GF	8 ポート 銅線 1 Gb 1000Base-T ハードウェアバイパス	✓	✓	✓

## パフォーマンス

### Cisco Secure Firewall 4200 シリーズ FTD モデル

指標	4212	4225	4245
FW + AVC スループット <sup>*1</sup>	65.0 Gbps	80.0 Gbps	140.0 Gbps
FW + AVC + IPS スループット <sup>*1</sup>	65.0 Gbps	80.0 Gbps	140.0 Gbps
FW 同時セッション数 (AVC 有効時の最大)	15,000,000	30,000,000	60,000,000
FW 新規接続数 / 秒 (AVC 有効時の最大)	350,000	600,000	800,000
IPS スループット <sup>*1</sup>	65.0 Gbps	80.0 Gbps	140.0 Gbps
TLS スループット <sup>*2</sup>	20 Gbps	30 Gbps	45 Gbps
IPsec VPN スループット <sup>*3</sup>	45 Gbps	80 Gbps	140 Gbps
VPN ピア数 (最大)	20,000	25,000	30,000
クラスタリング	8	8	8

\*1 1,024 バイト HTTP トラフィック。 \*2 RSA 2,048 ビットキーと AES256-SHA 暗号化を使用した TLS 1.2 トラフィックが 50% の想定。  
\*3 1,024 バイト TCP トラフィック。 Fastpath 有効時。

### Cisco Secure Firewall 4200 シリーズ ASA モデル

指標	4215	4225	4245
ステートフル インスペクション FW スループット <sup>*1</sup>	90.0 Gbps	95.0 Gbps	180.0 Gbps
ステートフル インスペクション FW スループット (マルチプロトコル <sup>*2</sup> )	65.0 Gbps	85.0 Gbps	100.0 Gbps
FW 同時セッション数 (最大)	40,000,000	80,000,000	80,000,000
FW 新規接続数 / 秒 (最大)	1,400,000	1,700,000	2,000,000
IPsec VPN スループット <sup>*3</sup>	50.0 Gbps	60.0 Gbps	70.0 Gbps
VPN ピア数 (最大)	20,000	25,000	30,000
セキュリティコンテキスト (デフォルト / 最大)	2 / 250	2 / 250	2 / 250
クラスタリング	8	8	8

\*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。  
\*3 450 バイト UDP L2L トラフィック。

# Cisco Secure Firewall Threat Defense (FTD) Virtual

## Cisco Secure Firewall Threat Defense (FTD) Virtual on VMware ESXi/KVM/OpenStack

15.5 Gbps  
FW + AVC7.0 Gbps  
FW + AVC + IPS8.0 Gbps<sup>\*1</sup>  
IPsec VPN10,000 ピア  
IPsec VPN30 インスタンス  
VRF16 ノード  
クラスター<sup>\*2</sup>

\*1 VMware ESXi および KVM で Intel QAT 有効時。 \*2 VMware ESXi および KVM でサポート。



## Cisco Secure Firewall Threat Defense (FTD) Virtual on Amazon Web Services

8.6 Gbps  
FW + AVC8.4 Gbps  
FW + AVC + IPS4.0 Gbps  
IPsec VPN10,000 ピア  
IPsec VPN30 インスタンス  
VRF16 ノード  
クラスター

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Microsoft Azure

5.0 Gbps  
FW + AVC4.5 Gbps  
FW + AVC + IPS4.0 Gbps  
IPsec VPN10,000 ピア  
IPsec VPN30 インスタンス  
VRF16 ノード  
クラスター

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Google Cloud Platform

9.9 Gbps  
FW + AVC9.7 Gbps  
FW + AVC + IPS4.0 Gbps  
IPsec VPN10,000 ピア  
IPsec VPN30 インスタンス  
VRF16 ノード  
クラスター

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Oracle Cloud Infrastructure

2.4 Gbps  
FW + AVC2.4 Gbps  
FW + AVC + IPS1.5 Gbps  
IPsec VPN10,000 ピア  
IPsec VPN30 インスタンス  
VRF

## ベースソフトウェア ライセンス製品型番

### Cisco Secure Firewall Threat Defense (FTD) Virtual

製品型番	製品説明	製品型番	製品説明
FRPTD-V-K9	Secure FTD Virtual 非階層型永続ライセンス	FTD-V-nS-BSE-K9 <sup>*1</sup>	Secure FTD Virtual 階層型サブスクリプション ライセンス

\*1 CCW では FTDV-SEC-SUB が必要。n = 5、10、20、30、50、または 100。

## パフォーマンス (プライベートクラウド)

### Cisco Secure Firewall Threat Defense (FTD) Virtual on VMware ESXi/KVM/OpenStack (ソフトウェアバージョン 7.0 以降)

指標	ライセンスタイプ <sup>*1</sup>	FTDv5	FTDv10	FTDv20	FTDv30	FTDv50	FTDv100
	仕様	4 × vCPU	4 × vCPU	4 × vCPU	8 × vCPU	12 × vCPU	16 × vCPU
FW + AVC スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	3.0 Gbps	5.5 Gbps	10.0 Gbps	15.5 Gbps
FW + AVC + IPS スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	3.0 Gbps	5.5 Gbps	10.0 Gbps	15.5 Gbps
FW + AVC スループット (450 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.5 Gbps	3.0 Gbps	5.0 Gbps	7.0 Gbps
FW + AVC + IPS スループット (450 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.0 Gbps	2.0 Gbps	3.0 Gbps	7.0 Gbps
同時セッション数 (最大)		100,000	100,000	100,000	250,000	500,000	2,000,000
新規接続数 / 秒 (最大)		12,500	20,000	20,000	20,000	40,000	130,000
IPsec VPN スループット <sup>*2</sup>		100 Mbps	1.0 Gbps	1.1 Gbps	2.0 Gbps	4.0 Gbps	6.0/8.0 Gbps <sup>*3</sup>
VPN ピア数 (最大)		250	250	250	250	750	10,000
VRF インスタンス数 (最大)		30	30	30	30	30	30
クラスターリング		16 <sup>*4</sup>	16 <sup>*4</sup>	16 <sup>*4</sup>	16 <sup>*4</sup>	16 <sup>*4</sup>	16 <sup>*4</sup>

\*1 階層型サブスクリプションのライセンスタイプ。 \*2 1,024 バイト TCP トラフィック、Fastpath 有効時。 \*3 VMware ESXi および KVM で Intel QAT 有効時は 8.0 Gbps。 \*4 VMware ESXi および KVM でサポート。

## パフォーマンスガイドライン (パブリッククラウド)

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Amazon Web Services (ソフトウェアバージョン 7.0 以降)

指標	ライセンスタイプ <sup>*1</sup>	FTDv5	FTDv10	FTDv20	FTDv30	FTDv50	FTDv100
	AWS インスタンスタイプ	c5.xlarge	c5.xlarge	c5.xlarge	c5.2xlarge	c5.4xlarge	c5.4xlarge
FW + AVC スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	2.2 Gbps	4.3 Gbps	8.6 Gbps	8.6 Gbps
FW + AVC + IPS スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	2.2 Gbps	4.3 Gbps	8.4 Gbps	8.4 Gbps
FW + AVC スループット (450 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	830 Mbps	1.4 Gbps	3.8 Gbps	3.8 Gbps
FW + AVC + IPS スループット (450 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	830 Mbps	1.4 Gbps	3.2 Gbps	3.2 Gbps
同時セッション数 (最大)		100,000	100,000	100,000	200,000	2,000,000	2,000,000
新規接続数 / 秒 (最大)		24,500	24,500	24,500	45,900	82,800	82,800
IPsec VPN スループット <sup>*2</sup>		100 Mbps	1.0 Gbps	1.4 Gbps	1.4 Gbps	4.0 Gbps	4.0 Gbps
VPN ピア数 (最大)		250	250	250	250	750	10,000
VRF インスタンス数 (最大)		30	30	30	30	30	30
クラスターリング		16	16	16	16	16	16

\*1 階層型サブスクリプションのライセンスタイプ。永続ライセンスの 4 × vCPU インスタンスは FTDv20、8 × vCPU インスタンスは FTDv30、16 × vCPU インスタンスは FTDv100 に相当。  
\*2 1,024 バイト TCP トラフィック、Fastpath 有効時。

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Microsoft Azure (ソフトウェアバージョン 7.0 以降)

指標 <sup>*1</sup>	ライセンスタイプ <sup>*2</sup>	FTDv5	FTDv10	FTDv20	FTDv30	FTDv50	FTDv100
	Azure VM タイプ	D3_v2, D3	D3_v2	D3_v2	D4_v2	D5_v2	D5_v2
FW + AVC スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.4 Gbps	1.5 Gbps	5.0 Gbps	5.0 Gbps
FW + AVC + IPS スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.4 Gbps	1.5 Gbps	4.5 Gbps	4.5 Gbps
FW + AVC スループット (450 バイト HTTP トラフィック)		100 Mbps	700 Mbps	700 Mbps	940 Mbps	1.0 Gbps	1.0 Gbps
FW + AVC + IPS スループット (450 バイト HTTP トラフィック)		100 Mbps	700 Mbps	700 Mbps	920 Mbps	1.0 Gbps	1.0 Gbps
同時セッション数 (最大)		100,000	100,000	100,000	250,000	1,500,000	1,500,000
新規接続数 / 秒 (最大)		11,550	11,550	11,550	12,480	14,540	14,540
IPsec VPN スループット <sup>*3</sup>		100 Mbps	830 Mbps	830 Mbps	1.6 Gbps	4.0 Gbps	4.0 Gbps
VPN ピア数 (最大)		250	250	250	250	750	10,000
VRF インスタンス数 (最大)		30	30	30	30	30	30
クラスターリング		16	16	16	16	16	16

\*1 高速ネットワーク有効時。 \*2 階層型サブスクリプションのライセンスタイプ。永続ライセンスの 4 × vCPU VM タイプは FTDv20、8 × vCPU VM タイプは FTDv30、16 × vCPU VM タイプは FTDv100 に相当。  
\*3 1,024 バイト TCP トラフィック、Fastpath 有効時。

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Google Cloud Platform (ソフトウェアバージョン 7.0 以降)

指標	ライセンスタイプ <sup>*1</sup>	FTDv5	FTDv10	FTDv20	FTDv30	FTDv50	FTDv100
	GCP マシンタイプ	c2-standard-4	c2-standard-4	c2-standard-4	c2-standard-8	c2-standard-16	c2-standard-16
FW + AVC スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.5 Gbps	5.0 Gbps	9.9 Gbps	9.9 Gbps
FW + AVC + IPS スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.4 Gbps	5.0 Gbps	9.7 Gbps	9.7 Gbps
FW + AVC スループット (450 バイト HTTP トラフィック)		100 Mbps	450 Mbps	450 Mbps	1.7 Gbps	2.3 Gbps	2.3 Gbps
FW + AVC + IPS スループット (450 バイト HTTP トラフィック)		100 Mbps	450 Mbps	450 Mbps	1.2 Gbps	2.0 Gbps	2.0 Gbps
同時セッション数 (最大)		100,000	100,000	100,000	250,000	2,000,000	2,000,000
新規接続数 / 秒 (最大)		12,000	12,000	12,000	45,000	84,000	84,000
IPsec VPN スループット <sup>*2</sup>		100 Mbps	1.0 Gbps	1.5 Gbps	1.5 Gbps	4.0 Gbps	4.0 Gbps
VPN ピア数 (最大)		250	250	250	250	750	10,000
VRF インスタンス数 (最大)		30	30	30	30	30	30
クラスターリング		16	16	16	16	16	16

\*1 階層型サブスクリプションのライセンスタイプ。永続ライセンスの 4 × vCPU マシンタイプは FTDv20、8 × vCPU マシンタイプは FTDv30、16 × vCPU マシンタイプは FTDv100 に相当。  
\*2 1,024 バイト TCP トラフィック、Fastpath 有効時。

## Cisco Secure Firewall Threat Defense (FTD) Virtual on Oracle Cloud Infrastructure (ソフトウェアバージョン 7.0 以降)

指標 <sup>*1</sup>	ライセンスタイプ <sup>*2</sup>	FTDv5	FTDv10	FTDv20	FTDv50	FTDv100
	OCI シェイプタイプ	VM.Standard2.4	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8	VM.Standard2.8
FW + AVC スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
FW + AVC + IPS スループット (1,024 バイト HTTP トラフィック)		100 Mbps	1.0 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
FW + AVC スループット (450 バイト HTTP トラフィック)		100 Mbps	410 Mbps	410 Mbps	920 Mbps	920 Mbps
FW + AVC + IPS スループット (450 バイト HTTP トラフィック)		100 Mbps	390 Mbps	390 Mbps	910 Mbps	910 Mbps
同時セッション数 (最大)		250,000	250,000	250,000	2,000,000	2,000,000
新規接続数 / 秒 (最大)		4,900	4,900	4,900	10,000	10,000
IPsec VPN スループット <sup>*3</sup>		250	250	250	750	10,000
VPN ピア数 (最大)		100 Mbps	1.0 Gbps	1.2 Gbps	1.5 Gbps	1.5 Gbps
VRF インスタンス数 (最大)		30	30	30	30	30
クラスターリング						

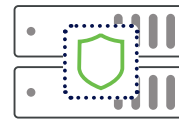
\*1 準仮想化モードで起動時。 \*2 階層型サブスクリプションのライセンスタイプ。永続ライセンスの 4 × OCPU シェイプタイプは FTDv20、8 × OCPU シェイプタイプは FTDv30 に相当。  
\*3 1,024 バイト TCP トラフィック、Fastpath 有効時。

# Cisco Secure Firewall ASA Virtual

## Cisco Secure Firewall ASA Virtual on VMware ESXi/KVM/OpenStack

20.0 Gbps  
FW8.0 Gbps  
IPsec VPN20,000 ピア  
IPsec VPN16 ノード  
クラスター<sup>\*1</sup>

\*1 VMware ESXi および KVM でサポート。



## Cisco Secure Firewall ASA Virtual on Amazon Web Services

16.0 Gbps  
FW5.5 Gbps  
IPsec VPN20,000 ピア  
IPsec VPN16 ノード  
クラスター

## Cisco Secure Firewall ASA Virtual on Microsoft Azure

11.0 Gbps  
FW6.5 Gbps  
IPsec VPN20,000 ピア  
IPsec VPN16 ノード  
クラスター

## Cisco Secure Firewall ASA Virtual on Google Cloud Platform

16.0 Gbps  
FW7.2 Gbps  
IPsec VPN20,000 ピア  
IPsec VPN

## Cisco Secure Firewall ASA Virtual on Oracle Cloud Infrastructure

3.0 Gbps  
FW620 Mbps  
IPsec VPN20,000 ピア  
IPsec VPN

## ベースソフトウェア ライセンス製品型番

### Cisco Secure Firewall ASA Virtual

製品型番	製品説明	製品型番	製品説明
L-ASAvnS-K9=	Secure Firewall ASA Virtual 永続ライセンス	L-ASA-V-nS-K9=	Secure Firewall ASA Virtual サブスクリプション ライセンス

\*1 n = 5、10、30、50、または 100。

## パフォーマンス (プライベートクラウド)

### Cisco Secure Firewall ASA Virtual on VMware ESXi/KVM/OpenStack (ソフトウェアバージョン 9.16 以降)

指標	ライセンスタイプ	ASAv5	ASAv10	ASAv30	ASAv50	ASAv100
	仕様	1 × vCPU	1 × vCPU	4 × vCPU	8 × vCPU	16 × vCPU
ステートフル インスペクション FW スループット <sup>*1</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	10.0 Gbps	20.0 Gbps
ステートフル インスペクション FW スループット (マルチプロトコル <sup>*2</sup> )		100 Mbps	1.0 Gbps	2.0 Gbps	10.0 Gbps	20.0 Gbps
FW 同時セッション数 (最大)		50,000	100,000	500,000	2,000,000	4,000,000
FW 新規接続数 / 秒 (最大)		12,500	60,000	200,000	350,000	600,000
IPsec VPN スループット <sup>*3</sup>		100 Mbps	750 Mbps	2.0 Gbps	4.0 Gbps	8.0 Gbps
IPsec VPN ピア数 (最大)		50	250	750	10,000	20,000
AnyConnect またはクライアントレス VPN ユーザーセッション数		50	250	750	10,000	20,000
クラスターリング				16 <sup>*4</sup>	16 <sup>*4</sup>	16 <sup>*4</sup>

\*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。

\*3 AES 暗号化を使用した 450 バイト UDP トラフィック。 \*4 VMware ESXi および KVM でサポート。

## パフォーマンス (パブリッククラウド)

## Cisco Secure Firewall ASA Virtual on Amazon Web Services (ソフトウェアバージョン 9.16 以降)

指標	ライセンスタイプ	ASAv5	ASAv10	ASAv30	ASAv50	ASAv100
	AWS インスタンスタイプ	c5.large	c5.large	c5.xlarge	c5.2xlarge	c5n.4xlarge
ステートフル インспекション FW スループット <sup>*1</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	10.0 Gbps	16.0 Gbps
ステートフル インспекション FW スループット (マルチプロトコル <sup>*2</sup> )		100 Mbps	1.0 Gbps	2.0 Gbps	4.5 Gbps	8.0 Gbps
FW 同時セッション数 (最大)		50,000	100,000	500,000	2,000,000	4,000,000
FW 新規接続数 / 秒 (最大)		12,500	62,000	90,000	120,000	200,000
IPsec VPN スループット <sup>*3</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	3.5 Gbps	5.5 Gbps
IPsec VPN ピア数 (最大)		50	250	750	10,000	20,000
AnyConnect またはクライアントレス VPN ユーザーセッション数		50	250	750	10,000	20,000
クラスターリング				16	16	16

\*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。 \*3 AES 暗号化を使用した 450 バイト UDP トラフィック。

## Cisco Secure Firewall ASA Virtual on Microsoft Azure (ソフトウェアバージョン 9.16 以降)

指標 <sup>*1</sup>	ライセンスタイプ	ASAv5	ASAv10	ASAv30	ASAv50	ASAv100
	Azure VM タイプ	D3_v2	D3_v2	D3_v2	D4_v2	D5_v2
ステートフル インспекション FW スループット <sup>*2</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	5.5 Gbps	11.0 Gbps
ステートフル インспекション FW スループット (マルチプロトコル <sup>*3</sup> )		100 Mbps	1.0 Gbps	1.0 Gbps	1.5 Gbps	2.5 Gbps
FW 同時セッション数 (最大)		50,000	100,000	500,000	2,000,000	4,000,000
FW 新規接続数 / 秒 (最大)		10,000	10,000	10,000	10,000	10,000
IPsec VPN スループット <sup>*4</sup>		100 Mbps	1.0 Gbps	1.75 Gbps	3.5 Gbps	6.5 Gbps
IPsec VPN ピア数 (最大)		50	250	750	10,000	20,000
AnyConnect またはクライアントレス VPN ユーザーセッション数		50	250	750	10,000	20,000
クラスターリング				16	16	16

\*1 高速ネットワーク有効時。 \*2 1,500 バイト UDP トラフィック。 \*3 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。 \*4 AES 暗号化を使用した 450 バイト UDP トラフィック。

## Cisco Secure Firewall ASA Virtual on Google Cloud Platform (ソフトウェアバージョン 9.16 以降)

指標	ライセンスタイプ	ASAv5	ASAv10	ASAv30	ASAv50	ASAv100
	GCP マシンタイプ	c2-standard-4	c2-standard-4	c2-standard-4	c2-standard-8	c2-standard-16
ステートフル インспекション FW スループット <sup>*1</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	7.6 Gbps	16.0 Gbps
ステートフル インспекション FW スループット (マルチプロトコル <sup>*2</sup> )		100 Mbps	1.0 Gbps	2.0 Gbps	7.2 Gbps	12.0 Gbps
FW 同時セッション数 (最大)		50,000	100,000	500,000	2,000,000	4,000,000
FW 新規接続数 / 秒 (最大)		12,500	48,000	60,000	82,000	160,000
IPsec VPN スループット <sup>*3</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	3.3 Gbps	7.2 Gbps
IPsec VPN ピア数 (最大)		50	250	750	10,000	20,000
AnyConnect またはクライアントレス VPN ユーザーセッション数		50	250	750	10,000	20,000
クラスターリング						

\*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。 \*3 AES 暗号化を使用した 450 バイト UDP トラフィック。

## Cisco Secure Firewall ASA Virtual on Oracle Cloud Infrastructure (ソフトウェアバージョン 9.16 以降)

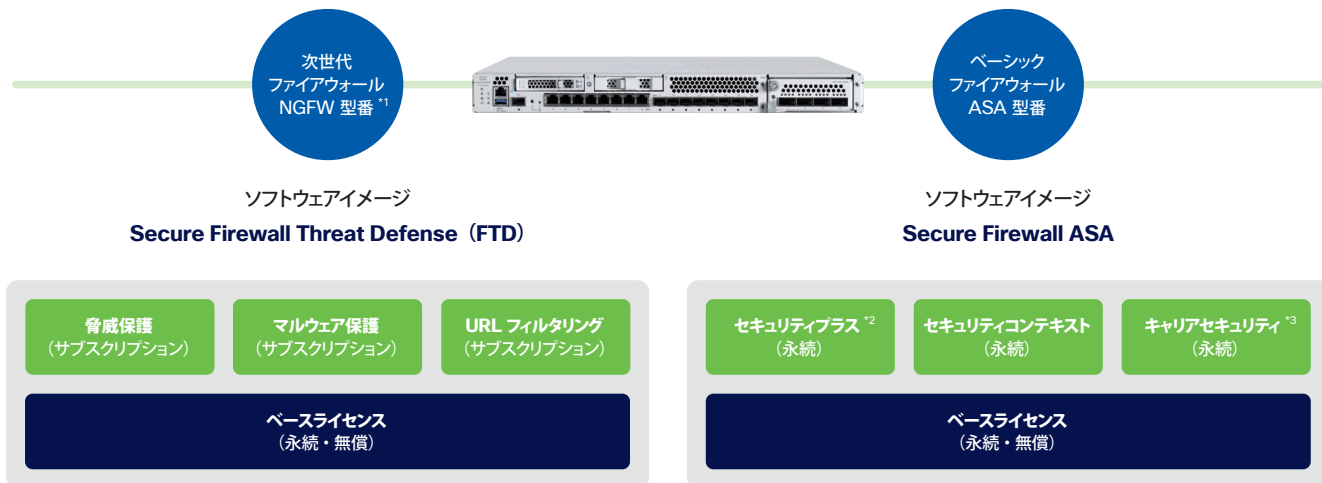
指標	ライセンスタイプ	ASAv5	ASAv10	ASAv30	ASAv50	ASAv100
	OCI シェイプタイプ	VM.Standard2.4	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8	VM.Standard2.8
ステートフル インспекション FW スループット <sup>*1</sup>		100 Mbps	1.0 Gbps	2.0 Gbps	TBD	TBD
ステートフル インспекション FW スループット (マルチプロトコル <sup>*2</sup> )		100 Mbps	1.0 Gbps	2.0 Gbps	2.3 Gbps	3.0 Gbps
FW 同時セッション数 (最大)		50,000	100,000	500,000	2,000,000	4,000,000
FW 新規接続数 / 秒 (最大)		12,500	26,600	26,600	26,600	38,200
IPsec VPN スループット <sup>*3</sup>		100 Mbps	550 Mbps	550 Mbps	550 Mbps	620 Mbps
IPsec VPN ピア数 (最大)		50	250	750	10,000	20,000
AnyConnect またはクライアントレス VPN ユーザーセッション数		50	250	750	10,000	20,000
クラスターリング						

\*1 準仮想化モードで起動時。 \*1 1,500 バイト UDP トラフィック。 \*2 主として TCP ベースのプロトコル / アプリケーション (HTTP、SMTP、FTP、IMAPv4、BitTorrent、および DNS など)。 \*3 AES 暗号化を使用した 450 バイト UDP トラフィック。

# Cisco Secure Firewall ライセンス

## 選べるソフトウェア & ライセンス

Cisco Secure Firewall は、Snort 3 侵入防御システムや高度なマルウェア防御を含むレイヤ 7 次世代ファイアウォール、またはレイヤ 3 & 4 ベーシックファイアウォールとして機能します。Cisco Secure Firewall の購入時には、それぞれのファイアウォールに対応するソフトウェアイメージを搭載したハードウェア（物理ファイアウォールの場合<sup>\*1</sup>）またはソフトウェア（仮想ファイアウォールの場合）を選択します。レイヤ 7 次世代ファイアウォールのソフトウェアイメージ Secure Firewall Threat Defense (FTD) では、必要なセキュリティ機能をサブスクリプションライセンスで有効化します。



\*1 Firepower 9300 では NGFW/ASA 型番に非対応。FTD を選択する場合、CCW では FPR9K-FTD-BUN を推奨。  
\*2 Firepower 1010 でアクティブ/スタンバイ フェイルオーバーを有効化。  
\*3 Secure Firewall 3100/4200 および Firepower 4100/9300 で Diameter、GTP/GPRS、SCTP を有効化。

## Cisco Secure Firewall ソフトウェアイメージの主な機能比較

主な機能	Secure Firewall Threat Defense (FTD)	Secure Firewall ASA
ビルトイン管理ツール	<ul style="list-style-type: none"> <li>Secure Firewall Device Manager (FDM)</li> </ul>	<ul style="list-style-type: none"> <li>Adaptive Security Device Manager</li> </ul>
一元管理 / 自動化ツール	<ul style="list-style-type: none"> <li>Secure Firewall Management Center (FMC)</li> <li>クラウド提供型 FMC (cdFMC)</li> <li>Cisco Defense Orchestrator (CDO)</li> </ul>	<ul style="list-style-type: none"> <li>Cisco Security Manager (CSM)</li> <li>Cisco Defense Orchestrator (CDO)</li> </ul>
ファイアウォール動作モード	<ul style="list-style-type: none"> <li>トランスペアレント</li> <li>ルーテッド</li> <li>マルチインスタンス</li> </ul>	<ul style="list-style-type: none"> <li>トランスペアレント</li> <li>ルーテッド</li> <li>マルチコンテキスト</li> </ul>
ファイアウォール	<ul style="list-style-type: none"> <li>ステートフル ファイアウォール</li> <li>レイヤ 7 プロトコル検査</li> <li>NAT</li> </ul>	<ul style="list-style-type: none"> <li>ステートフルファイアウォール</li> <li>レイヤ 7 プロトコル検査</li> <li>NAT</li> </ul>
次世代ファイアウォールなど高度な脅威対策	<ul style="list-style-type: none"> <li>アプリケーションの可視化と制御</li> <li>Snort 3 侵入防御システム</li> <li>高度なマルウェア保護 (AMP)</li> <li>Secure Malware Analytics 連携</li> <li>URL フィルタリング</li> <li>Web セーフサーチと Youtube for Schools</li> <li>SSL 復号 (ハードウェア アクセラレーション)</li> <li>Encrypted Visibility Engine</li> </ul>	
サイト間 VPN	<ul style="list-style-type: none"> <li>IPsec IKEv1/v2</li> </ul>	<ul style="list-style-type: none"> <li>IPsec IKEv1/v2</li> </ul>
リモートアクセス VPN	<ul style="list-style-type: none"> <li>Secure Client (旧 AnyConnect)</li> <li>ZTNA リモートアクセス</li> </ul>	<ul style="list-style-type: none"> <li>Secure Client (旧 AnyConnect)</li> <li>サードパーティクライアント</li> </ul>
アクセス制御	<ul style="list-style-type: none"> <li>ゾーンベース</li> <li>IP アドレスベース</li> <li>ジオロケーションベース</li> <li>VLAN ベース</li> <li>ポートベース</li> <li>ユーザ ID/グループベース</li> <li>アプリケーション ID ベース</li> <li>SGT ベース</li> </ul>	<ul style="list-style-type: none"> <li>IP アドレスベース</li> <li>VLAN ベース</li> <li>ポートベース</li> <li>ユーザ ID/グループベース</li> <li>SGT ベース</li> </ul>
アイデンティティ制御	<ul style="list-style-type: none"> <li>SGT ベースでトラフィックポリシーを適用</li> <li>ISE 連携で迅速な脅威の封じ込め</li> </ul>	<ul style="list-style-type: none"> <li>SGT ベースでトラフィックポリシーを適用</li> </ul>
ネットワークディスカバリ	<ul style="list-style-type: none"> <li>ネットワーク / アプリケーション / ユーザ ディスカバリ</li> <li>インパクト解析</li> </ul>	
アナリティクス	<ul style="list-style-type: none"> <li>デバイスヘルス</li> <li>カスタマイズ可能なレポート</li> <li>CISCO XDR</li> </ul>	<ul style="list-style-type: none"> <li>デバイスヘルス</li> <li>Cisco XDR</li> </ul>



## Cisco Secure Firewall Threat Defense (FTD) サブスクリプション ライセンス (抜粋)

## Cisco Secure Firewall Threat Defense (FTD) 脅威保護 + マルウェア保護 + URL フィルタリング サブスクリプション ライセンス

製品型番			対応モデル	対応シリーズ
1 年間	3 年間	5 年間		
L-FPR1010T-TMC-1Y	L-FPR1010T-TMC-3Y	L-FPR1010T-TMC-5Y	Firepower 1010	Firepower 1000
L-FPR1120T-TMC-1Y	L-FPR1120T-TMC-3Y	L-FPR1120T-TMC-5Y	Firepower 1120	
L-FPR1140T-TMC-1Y	L-FPR1140T-TMC-3Y	L-FPR1140T-TMC-5Y	Firepower 1140	
L-FPR1150T-TMC-1Y	L-FPR1150T-TMC-3Y	L-FPR1150T-TMC-5Y	Firepower 1150	
L-FPR2110T-TMC-1Y	L-FPR2110T-TMC-3Y	L-FPR2110T-TMC-5Y	Firepower 2110	Firepower 2100
L-FPR2120T-TMC-1Y	L-FPR2120T-TMC-3Y	L-FPR2120T-TMC-5Y	Firepower 2120	
L-FPR2130T-TMC-1Y	L-FPR2130T-TMC-3Y	L-FPR2130T-TMC-5Y	Firepower 2130	
L-FPR2140T-TMC-1Y	L-FPR2140T-TMC-3Y	L-FPR2140T-TMC-5Y	Firepower 2140	
L-FPR3105T-TMC-1Y	L-FPR3105T-TMC-3Y	L-FPR3105T-TMC-5Y	Secure Firewall 3105	Secure Firewall 3100
L-FPR3110T-TMC-1Y	L-FPR3110T-TMC-3Y	L-FPR3110T-TMC-5Y	Secure Firewall 3110	
L-FPR3120T-TMC-1Y	L-FPR3120T-TMC-3Y	L-FPR3120T-TMC-5Y	Secure Firewall 3120	
L-FPR3130T-TMC-1Y	L-FPR3130T-TMC-3Y	L-FPR3130T-TMC-5Y	Secure Firewall 3130	
L-FPR3140T-TMC-1Y	L-FPR3140T-TMC-3Y	L-FPR3140T-TMC-5Y	Secure Firewall 3140	
L-FPR4215T-TMC-1Y	L-FPR4215T-TMC-3Y	L-FPR4215T-TMC-5Y	Secure Firewall 4215	Secure Firewall 4200
L-FPR4225T-TMC-1Y	L-FPR4225T-TMC-3Y	L-FPR4225T-TMC-5Y	Secure Firewall 4224	
L-FPR4245T-TMC-1Y	L-FPR4245T-TMC-3Y	L-FPR4245T-TMC-5Y	Secure Firewall 4245	
L-FPR9K-40T-TMC-1Y	L-FPR9K-40T-TMC-3Y	L-FPR9K-40T-TMC-5Y	Firepower 9000 SM-40	Firepower 9300
L-FPR9K-48T-TMC-1Y	L-FPR9K-48T-TMC-3Y	L-FPR9K-48T-TMC-5Y	Firepower 9000 SM-48	
L-FPR9K-56T-TMC-1Y	L-FPR9K-56T-TMC-3Y	L-FPR9K-56T-TMC-5Y	Firepower 9000 SM-56	
L-FPRTD-V-TMC-1Y	L-FPRTD-V-TMC-3Y	L-FPRTD-V-TMC-5Y	非階層型 (FPRTD-V-K9)	Secure FTD Virtual
FTD-V-5S-TMC			階層型 (FTD-V-5S-BSE-K9)	
FTD-V-10S-TMC			階層型 (FTD-V-10S-BSE-K9)	
FTD-V-20S-TMC			階層型 (FTD-V-20S-BSE-K9)	
FTD-V-30S-TMC			階層型 (FTD-V-30S-BSE-K9)	
FTD-V-50S-TMC			階層型 (FTD-V-50S-BSE-K9)	
FTD-V-100S-TMC			階層型 (FTD-V-100S-BSE-K9)	

## Cisco Secure Firewall Threat Defense (FTD) サブスクリプション ライセンス製品型番の見方

製品型番例	対応モデル	製品型番に含まれる文字列 (x)	対応セキュリティサービス	製品型番に含まれる数字 (y)	期間
L-FPR1010T-x-yY <sup>1</sup>	Firepower 1010	T	脅威保護	1	1 年間
L-FPR2110T-x-yY <sup>1</sup>	Firepower 2110	AMP	マルウェア保護	3	3 年間
L-FPR3105T-x-yY <sup>1</sup>	Secure Firewall 3105	URL	URL フィルタリング	5	5 年間
L-FPR4215T-x-yY <sup>1</sup>	Secure Firewall 4215	TM	脅威保護 + マルウェア保護		
L-FPR9K-40T-x-yY <sup>2</sup>	Firepower 9000 SM-40	TC	脅威保護 + URL フィルタリング		
L-FPRTD-V-x-yY <sup>3</sup>	Secure FTD Virtual (非階層型)	TMC	脅威保護 + マルウェア保護 + URL フィルタリング		
FTD-V-5S-x <sup>4</sup>	Secure FTD Virtual (階層型)				

- \*1 CCW では FPR $nnnn$ T-x または L-FPR $nnnn$ T-x= (追加時) が必要 (nnnn は対応モデル番号、x は対応セキュリティサービス)。詳細は発注ガイドを参照。  
 \*2 CCW では FPR9K-FTD-BUN を推奨、L-FPR9K- $nn$ T-x が必要 (nn はセキュリティモジュール対応モデル番号、x は対応セキュリティサービス)。詳細は発注ガイドを参照。  
 \*3 CCW では L-FPRTD-V-x= が必要 (x は対応セキュリティサービス)。詳細は発注ガイドを参照。  
 \*4 CCW では FTDV-SEC-SUB および FTD-V- $n$ S-BSE-K9 が必要 (n は対応階層モデル番号)。詳細は発注ガイドを参照。

## Cisco Secure Firewall ASA 永続ライセンス (抜粋)

## Cisco Secure Firewall ASA セキュリティプラス ライセンス

製品型番	製品説明	対応モデル
FPR1010-SEC-PL	アクティブ / スタンバイ フェイルオーバー ライセンス	Firepower 1010

## Cisco Secure Firewall ASA セキュリティコンテキスト ライセンス

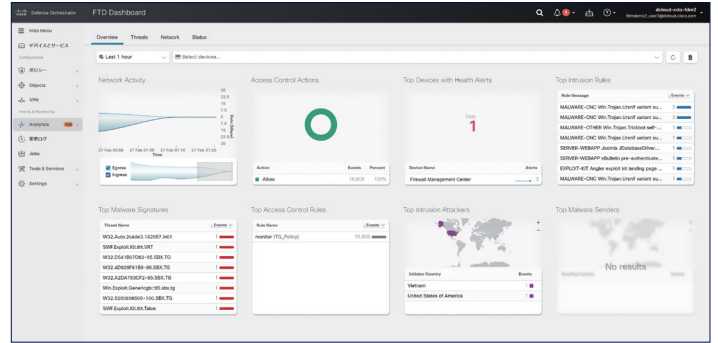
製品型番	製品説明	対応シリーズ
L-FPR1K-ASASC-5	5 × セキュリティコンテキスト ライセンス	Firepower 1000
L-FPR1K-ASASC-10	10 × セキュリティコンテキスト ライセンス	
FPR2K-ASASC-5	5 × セキュリティコンテキスト ライセンス	Firepower 2100
FPR2K-ASASC-10	10 × セキュリティコンテキスト ライセンス	
FPR3K-ASASC-5	5 × セキュリティコンテキスト ライセンス	Secure Firewall 3100
FPR3K-ASASC-10	10 × セキュリティコンテキスト ライセンス	
FPR4K-ASASC-10	10 × セキュリティコンテキスト ライセンス	Firepower 4100
L-F9K-ASA-SC-10	10 × セキュリティコンテキスト ライセンス	Firepower 9300

# Cisco Secure Firewall 管理ツール

## 選べる管理ツール

Cisco Secure Firewall はデバイス内蔵の管理ツール、およびオンプレミスまたはクラウドの一元管理ツールで設定管理できます。一元管理ツールでは、管理対象デバイスの種別や数に応じたライセンスの購入が必要です。

Cisco Secure Firewall Threat Defense (FTD) の統合管理ツールとしては、Secure Firewall Management Center (FMC) もしくは Cisco Defense Orchestrator (CDO) を選べます。FMCは、オンプレミス環境で高速に、かつ FTDの機能を最大限利用したい場合に最適です。CDOは、クラウド、もしくはマルチクラウド環境で、様々なセキュリティデバイスを統合監視したい場合に最適です。



## Cisco Secure Firewall Threat Defense (FTD) 管理ツールの主な機能比較

	Secure Firewall Device Manager (FDM)	Secure Firewall Management Center (FMC)	Cisco Defense Orchestrator (CDO) クラウド提供型 FMC (cdFMC)
管理ツール種別	<ul style="list-style-type: none"> <li>オンプレミス</li> <li>デバイス内蔵</li> </ul>	<ul style="list-style-type: none"> <li>オンプレミス</li> <li>マルチデバイス管理</li> </ul>	<ul style="list-style-type: none"> <li>クラウド</li> <li>マルチプラットフォーム管理</li> <li>マルチデバイス管理</li> </ul>
管理対象デバイス種別	<ul style="list-style-type: none"> <li>FTD モデル</li> </ul>	<ul style="list-style-type: none"> <li>FTD モデル</li> </ul>	<ul style="list-style-type: none"> <li>FTD モデル (cdFMC)</li> <li>ASA モデル (CDO)</li> <li>Meraki MX など</li> </ul>
対応導入モード	<ul style="list-style-type: none"> <li>高可用性</li> </ul>	<ul style="list-style-type: none"> <li>高可用性</li> <li>マルチインスタンス</li> <li>クラスターリング</li> </ul>	<ul style="list-style-type: none"> <li>高可用性</li> <li>マルチインスタンス</li> <li>クラスターリング</li> </ul>
可視化	<ul style="list-style-type: none"> <li>アプリケーション</li> <li>ユーザー</li> </ul>	<ul style="list-style-type: none"> <li>ネットワーク</li> <li>アプリケーション</li> <li>ユーザー</li> <li>ホストプロファイル</li> <li>ダイナミックオブジェクト</li> </ul>	<ul style="list-style-type: none"> <li>アプリケーション</li> <li>ユーザー</li> <li>ホストプロファイル (SAL<sup>1</sup> で生成)</li> </ul>
アクセス制御	<ul style="list-style-type: none"> <li>セキュリティインテリジェンス</li> <li>アイデンティティポリシー</li> <li>きめ細やかな IPS &amp; マルウェアポリシー</li> <li>URL &amp; アプリケーション フィルタリング</li> <li>L2 ~ 7 ルール</li> <li>TLS1.3 復号</li> <li>TLS1.3 サーバーアイデンティティ ディスカバリー</li> </ul>	<ul style="list-style-type: none"> <li>プレフィルタルール</li> <li>セキュリティインテリジェンス</li> <li>アイデンティティポリシー</li> <li>きめ細やかな IPS &amp; マルウェアポリシー</li> <li>URL &amp; アプリケーション フィルタリング</li> <li>L2 ~ 7 ルール</li> <li>ダイナミックオブジェクト</li> <li>暗号化フロー可視化</li> <li>TLS1.3 復号</li> <li>QUIC 検出</li> </ul>	<ul style="list-style-type: none"> <li>プレフィルタルール</li> <li>セキュリティインテリジェンス</li> <li>アイデンティティポリシー</li> <li>きめ細やかな IPS &amp; マルウェアポリシー</li> <li>URL &amp; アプリケーション フィルタリング</li> <li>L2 ~ 7 ルール</li> <li>ダイナミックオブジェクト</li> <li>暗号化フロー可視化</li> <li>TLS1.3 復号</li> <li>QUIC 検出</li> </ul>
ネットワーク	<ul style="list-style-type: none"> <li>ECMP</li> <li>デュアル ISP</li> </ul>	<ul style="list-style-type: none"> <li>アプリケーション対応ルーティング</li> <li>ループバック インターフェイス</li> <li>DVTI</li> <li>リンクヘルスモニタリング</li> <li>DIA</li> <li>ECMP</li> <li>デュアル ISP</li> <li>管理用データ インターフェイス</li> </ul>	<ul style="list-style-type: none"> <li>アプリケーション対応ルーティング</li> <li>ループバック インターフェイス</li> <li>DVTI</li> <li>リンクヘルスモニタリング</li> <li>DIA</li> <li>ECMP</li> <li>デュアル ISP</li> <li>管理用データ インターフェイス</li> </ul>
脅威インテリジェンス	<ul style="list-style-type: none"> <li>Talos</li> </ul>	<ul style="list-style-type: none"> <li>Talos</li> <li>CTID<sup>2</sup> によるサードパーティフィード</li> <li>サードパーティ脆弱性データベース</li> <li>MITRE ATT&amp;CK 対応イベントログ</li> </ul>	<ul style="list-style-type: none"> <li>Talos</li> <li>SAL 統合による脅威インテリジェンス強化</li> <li>MITRE ATT&amp;CK 対応アナリティクス &amp; アラート</li> </ul>
自動化	<ul style="list-style-type: none"> <li>設定ウィザード</li> <li>コンテキストヘルプ</li> </ul>	<ul style="list-style-type: none"> <li>Firepower 推奨事項</li> <li>関連ルール</li> <li>迅速な脅威の封じ込め</li> <li>CTID<sup>2</sup></li> <li>CiscoXDR Orchestration によるワークフロー自動化</li> </ul>	<ul style="list-style-type: none"> <li>迅速な脅威の封じ込め</li> <li>Cisco XDR Orchestration によるワークフロー自動化</li> </ul>
イベントログ	<ul style="list-style-type: none"> <li>FDM</li> <li>Syslog</li> <li>SAL<sup>1</sup> クラウド (90 日、最大 3 年間)</li> </ul>	<ul style="list-style-type: none"> <li>FMC</li> <li>Syslog</li> <li>eStreamer</li> <li>SAL<sup>1</sup> オンプレミス</li> <li>SAL<sup>1</sup> クラウド (90 日、最大 3 年間)</li> </ul>	<ul style="list-style-type: none"> <li>CDO</li> <li>Syslog</li> <li>SAL<sup>1</sup> クラウド (90 日、最大 3 年間)</li> <li>オンプレミス FMC とのハイブリッドロギング</li> </ul>
アナリティクス	<ul style="list-style-type: none"> <li>ダッシュボード</li> <li>Cisco XDR</li> </ul>	<ul style="list-style-type: none"> <li>ダッシュボード</li> <li>Cisco XDR</li> </ul>	<ul style="list-style-type: none"> <li>ダッシュボード (CDO)</li> <li>SAL</li> <li>Cisco XDR</li> </ul>

\*1 SAL : Security Analytics and Logging. \*2 CTID : Cisco Threat Intelligence Director.

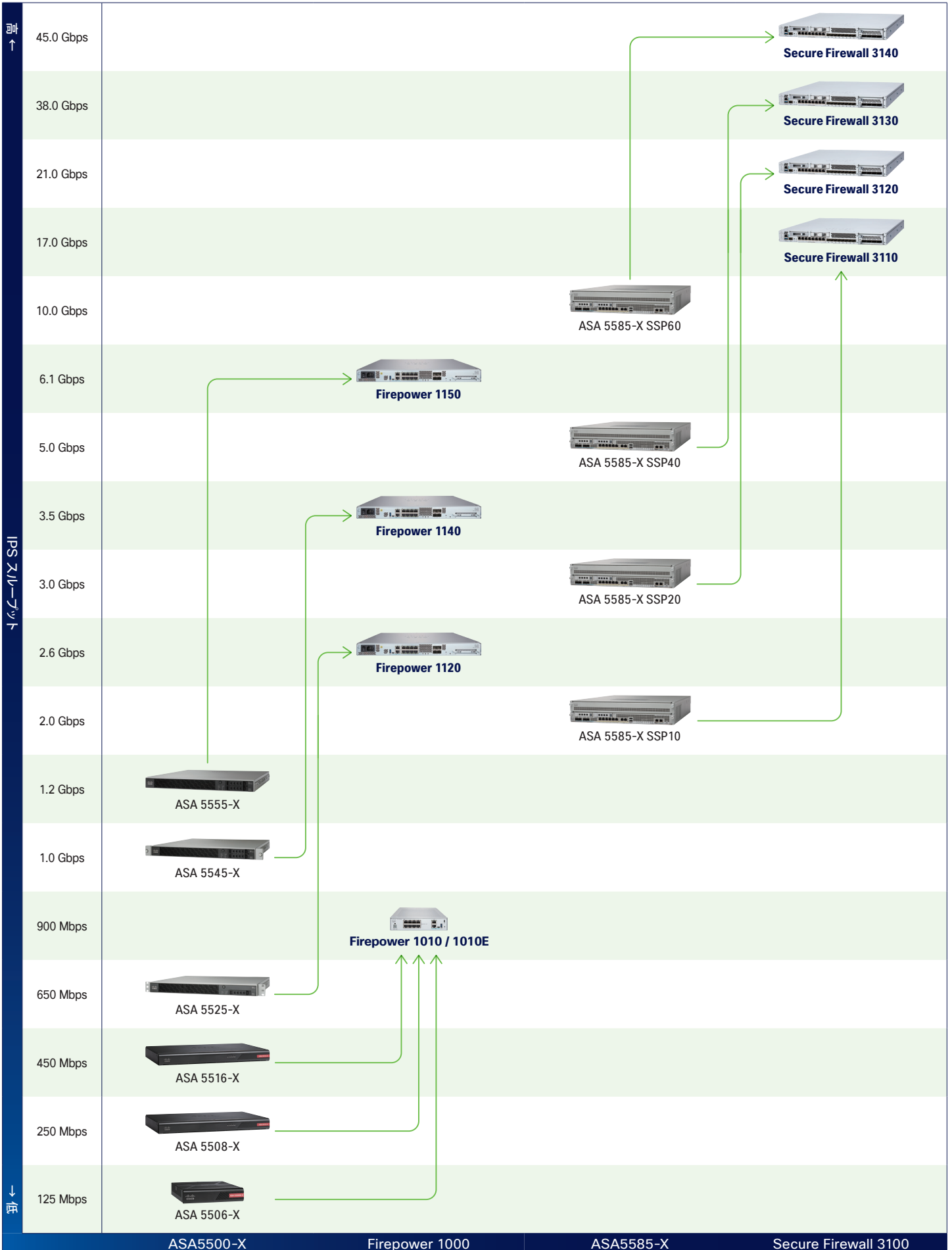
## Cisco Secure Firewall ASA 管理ツールの主な機能比較

	Adaptive Security Device Manager (ASDM)	Cisco Security Manager (CSM)	Cisco Defense Orchestrator (CDO)
管理ツール種別	<ul style="list-style-type: none"> <li>オンプレミス</li> <li>デバイス内蔵</li> </ul>	<ul style="list-style-type: none"> <li>オンプレミス</li> <li>マルチデバイス管理</li> </ul>	<ul style="list-style-type: none"> <li>クラウド</li> <li>マルチプラットフォーム管理</li> <li>マルチデバイス管理</li> </ul>
管理対象デバイス種別	<ul style="list-style-type: none"> <li>ASA モデル</li> </ul>	<ul style="list-style-type: none"> <li>ASA モデル</li> </ul>	<ul style="list-style-type: none"> <li>FTD モデル (cdFMC)</li> <li>ASA モデル (CDO)</li> <li>Meraki MX など</li> </ul>
対応導入モード	<ul style="list-style-type: none"> <li>アクティブ / スタンバイ高可用性</li> <li>アクティブ / アクティブ高可用性</li> <li>クラスターリング</li> <li>VPN ロードバランシング</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ / スタンバイ高可用性</li> <li>アクティブ / アクティブ高可用性</li> <li>クラスターリング</li> <li>VPN ロードバランシング</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ / スタンバイ高可用性</li> </ul>
VPN 管理	<ul style="list-style-type: none"> <li>Secure Client 設定 (GUI)</li> <li>ホストスキャン</li> <li>ダイナミック アクセスポリシー</li> <li>ポリシー &amp; ルールベース VPN</li> </ul>	<ul style="list-style-type: none"> <li>Secure Client 設定 (GUI)</li> <li>ホストスキャン</li> <li>ダイナミック アクセスポリシー</li> <li>ポリシー &amp; ルールベース VPN</li> </ul>	<ul style="list-style-type: none"> <li>Secure Client 設定 (GUI/CLI)</li> <li>ホストスキャン (CLI)</li> <li>ダイナミック アクセスポリシー (CLI)</li> <li>ポリシー &amp; ルールベース VPN</li> </ul>
ファイアウォール管理自動化	<ul style="list-style-type: none"> <li>ヒットカウント</li> <li>設定ウィザード</li> </ul>	<ul style="list-style-type: none"> <li>ルール最適化</li> <li>設定共有</li> <li>使用レポート</li> </ul>	<ul style="list-style-type: none"> <li>オブジェクト競合</li> <li>ルール最適化</li> <li>設定テンプレート</li> <li>CLI マクロ</li> </ul>
イベントログ	<ul style="list-style-type: none"> <li>イベントビューア</li> <li>Syslog</li> <li>外部ログサーバーへの NetFlow データ送信</li> <li>セキュアコネクタによる SAL<sup>1</sup> クラウド統合</li> </ul>	<ul style="list-style-type: none"> <li>イベントビューア &amp; レポートマネージャ</li> <li>Syslog</li> <li>外部ログサーバーへの NetFlow データ送信</li> <li>セキュアコネクタによる SAL<sup>1</sup> クラウド統合</li> </ul>	<ul style="list-style-type: none"> <li>イベントビューア</li> <li>強化された VPN モニタリング &amp; レポート</li> <li>クロス起動による SAL<sup>1</sup> クラウド統合</li> </ul>

\*1 SAL : Security Analytics and Logging.

# Cisco Secure Firewall 移行ガイド

Cisco ASA 5500-X シリーズ & Cisco Firepower 1000 シリーズ & Cisco Secure Firewall 3100 シリーズ ポジショニングマップ



シスコ お問い合わせ窓口



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](https://cisco.com/jp/go/vdc_callback)



©2024 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は 2024 年 4 月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。



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](https://cisco.com/jp)