



Cisco ASAv の概要

Cisco 適応型セキュリティ仮想アプライアンス (ASAv) は、仮想化環境に包括的なファイアウォール機能を提供し、データセンタートラフィックとマルチテナント環境のセキュリティを強化します。

ASDM または CLI を使用して、ASAv を管理およびモニタできます。その他の管理オプションを使用できる場合もあります。

- [ハイパーバイザのサポート \(1 ページ\)](#)
- [ASAv のライセンス \(1 ページ\)](#)
- [ASAv のライセンス \(2 ページ\)](#)
- [注意事項と制約事項 \(5 ページ\)](#)
- [ASAv インターフェイスおよび仮想 NIC \(7 ページ\)](#)
- [ASAv と SR-IOV インターフェイスのプロビジョニング \(8 ページ\)](#)

ハイパーバイザのサポート

ハイパーバイザのサポートについては、『[Cisco ASA Compatibility](#)』を参照してください。

ASAv のライセンス

ASAv は Cisco Smart Software Licensing を使用します。詳細については、「スマートソフトウェア ライセンシング (ASAv、ASA on Firepower)」を参照してください。



(注) ASAv にスマートライセンスをインストールする必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。スマート ライセンスは、通常の操作に必要です。

ASAv ライセンスの権限付与と、サポートされているプライベートおよびパブリック導入ターゲットのリソース仕様については、以降の各項を参照してください。

ASAv のライセンス

ASAv ライセンス資格、ライセンスの状態、必要なリソース、およびモデル仕様に関する情報については、次の表を参照してください。

- [表 1: ASAv スマートライセンス資格](#) : ASAv プラットフォームのライセンスの権限付与の条件を満たすリソースシナリオ準拠を示しています。



(注) ASAv は Cisco Smart Software Licensing を使用します。スマートライセンスは、通常の操作に必要です。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。

- [表 2: ASAv ライセンスの状態](#) : ASAv のリソースと資格に関連した状態とメッセージを示しています。
- [表 3: ASAv モデルの説明と仕様](#) : ASAv モデルと関連仕様、リソース要件、および制限事項を示しています。

スマート ライセンス資格

ASAv は Cisco Smart Software Licensing を使用します。詳細については、『[Smart Software Licensing for the ASAv and ASA](#)』を参照してください。



(注) ASAv にスマートライセンスをインストールする必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。スマートライセンスは、通常の操作に必要です。

表 1: ASAv スマートライセンス資格

ライセンスの権限付与	vCPU/RAM	スループット	適用されるレートリミッタ
ラボ エディションモード (ライセンスは不要)	すべてのプラットフォーム	100 Kbps	あり
ASAv5 (100M)	1 vCPU/1 GB ~ 1.5 GB	100Mbps	あり
ASAv10 (1 GB)	1 vCPU/2 GB	1Gbps	あり
ASAv30 (2 GB)	4 vCPU/8 GB	2 Gbps	あり

ライセンスの権限付与	vCPU/RAM	スループット	適用されるレート リミッタ
ASAv50 (10 GB)	8 vCPU/16 GB	10 Gbps	あり

ライセンスの状態

表 2: ASAv ライセンスの状態

状態	リソース対権限付与	アクションおよびメッセージ
Compliant	リソース = 権限付与の上限 (vCPU、GB の RAM)	アプライアンスに最適にリソースが割り当てられます ASAv5 (1vCPU、1G)、 ASAv10 (1vCPU、2G)、 ASAv30 (4vCPU、8G)、 ASAv50 (8vCPU、16G) アクションなし、メッセージなし
	リソース < 権限付与の上限 アンダープロビジョニングされます	ASAv がライセンスのスループットで実行できないとの警告メッセージが記録されている間はアクションなし
Non-compliant	リソース > 権限付与の上限 オーバープロビジョニングされます	ASAv レート リミッタによってパフォーマンスが制限され、コンソールに警告が出力されます。
		ASAv10、ASAv30、および ASAv50 は、エラー メッセージがコンソールに出力された後、リブートします。

モデルの説明と仕様

表 3: ASAv モデルの説明と仕様

モデル	ライセンス要件
ASAv5	スマート ライセンス 次の仕様を参照してください。 • 100 Mbps スループット • 1 vCPU • 1 GB RAM (1.5 GB に調節可能) • 50,000 の同時ファイアウォール接続 • AWS はサポート対象外 • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート
ASAv10	スマート ライセンス 次の仕様を参照してください。 • 1 Gbps スループット • 1 vCPU • 2 GB のメモリ • 100,000 の同時ファイアウォール接続 • c3.large、c4.large、および m4.large インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート

モデル	ライセンス要件
ASAv30	スマート ライセンス 次の仕様を参照してください。 • 2 Gbps スループット • 4 vCPU • 8 GB RAM • 500,000 の同時ファイアウォール接続 • c3.xlarge、c4.xlarge、および m4.xlarge インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート
ASAv50	スマート ライセンス 次の仕様を参照してください。 • 10 Gbps スループット • 8 vCPU（CPU ソケットあたり 8 個以上の物理コアが必要。複数の CPU ソケットにはプロビジョニングできない） • 16 GB メモリ • 2,000,000 の同時ファイアウォール接続 • AWS、Microsoft Azure、または Hyper-V をサポートしません。

注意事項と制約事項

ASAv ファイアウォール機能は Cisco ASA ハードウェア ファイアウォールと非常に似ていますが、次のガイドラインと制限事項があります。

ASAv（すべてのモデル）のガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ハイ アベイラビリティ ガイドラインのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じモデルライセンスを備えていることを確認してください（たとえば、両方の装置が ASAv30s であることなど）。



重要

ASAv を使用してハイ アベイラビリティ ペアを作成する場合は、データ インターフェイスを各 ASAv に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASAv に追加されると、ASAv コンソールにエラーが表示される可能性があります。また、フェールオーバー機能にも影響が出ることがあります。

サポートしない ASA 機能

ASAv は、次の ASA 機能をサポートしません。

- クラスタ
- マルチ コンテキスト モード
- アクティブ/アクティブ フェールオーバー
- EtherChannel
- AnyConnect Premium（共有）ライセンス

ASAv5 のガイドラインと制限事項

パフォーマンスのガイドライン

- 1 秒あたり 8000 接続、最大 25 の VLAN、50,000 の同時セッション、および 50 の VPN セッションをサポートします。
- 9.5(1.200) 以降、ASAv5 のメモリ要件は 1 GB に減りました。ASAv5 の使用可能メモリを 2 GB から 1 GB へダウングレードすることはサポートされません。1 GB のメモリで実行するには、ASAv5 VM を 9.5(1.200) 以降のバージョンで再導入する必要があります。同様に、9.5(1.200) より前のバージョンにダウングレードする場合、メモリを 2 GB に増やす必要があります。
- 場合によっては、ASAv5 のメモリが枯渇状態になります。これは、AnyConnect の有効化やファイルのダウンロードなど、特定リソースの利用が多い場合に発生することがあります。自動的な再起動に関するコンソールメッセージやメモリ使用量に関する重大な syslog が、メモリ枯渇の状態を示します。このような場合、1.5 GB メモリの VM に ASAv5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。
- ASAv5 は、100 Mbps のしきい値に達するとすぐに、パケットのドロップを開始します（100 Mbps をすべて使用できるように、多少のヘッドルームがあります）。ASAv5 は小

さいメモリフットプリントと低スループットを必要とするユーザ向けであるため、不要なメモリを使用することなく多数の ASAv5 を導入できます。

制限事項

- ジャンボ フレームはサポートされていません。
- Amazon Web Services (AWS) ではサポートされません。

ASAv50 のガイドラインと制限事項

パフォーマンスのガイドライン

- 集約トラフィックで 10 Gbps がサポートされます。
- ESXi と KVM でのみサポートされます。
- フルスループットレートを実現するため、CPU ピンニングを推奨します。ESXi 構成でのパフォーマンスの向上および KVM 構成でのパフォーマンスの向上を参照してください。
- 自動 ASP ロードバランシングがサポートされます。「ASAv の自動ロードバランシング」の 79 ページを参照してください。
- SR-IOV インターフェイスの ixgbe-vf vNIC がサポートされます。「ASAv と SR-IOV インターフェイスのプロビジョニング」を参照してください。
-
-

制限事項

- トランスペアレント モードはサポートされていません。
- Amazon Web Services (AWS) 、Microsoft Azure、および Hyper-V ではサポートされません。
- ixgbe NIC はこのリリースではサポートされていません。

ASAv インターフェイスおよび仮想 NIC

ASAv は、仮想プラットフォーム上のゲストとして、基盤となる物理プラットフォームのネットワークインターフェイスを利用します。ASAv の各インターフェイスは仮想 NIC (vNIC) にマッピングされます。

- ASAv インターフェイス
- サポートされている vNIC

ASAv インターフェイス

ASAv には、次のギガビット イーサネット インターフェイスがあります。

- Management 0/0

AWS と Azure の場合は、Management 0/0 をトラフィック伝送用の「外部」インターフェイスにすることができます。

- GigabitEthernet 0/0 ～ 0/8。ASAv をフェールオーバー ペアの一部として導入する場合は、GigabitEthernet 0/8 がフェールオーバー リンクに使用されることに注意してください。

- ASAv50 上の TenGigabitEthernet 0/0 ～ 0/8。ASAv50 をフェールオーバー ペアの一部として導入する場合は、TenGigabitEthernet 0/8 がフェールオーバー リンクに使用されることに注意してください。

- Hyper-V は最大 8 つのインターフェイスをサポートします。Management 0/0 および GigabitEthernet 0/0 ～ 0/6。フェールオーバー リンクとして GigabitEthernet 0/6 を使用できます。

サポートされている vNIC

ASAv は次の vNIC をサポートします。

表 4: サポートされている vNIC

表 5: サポートされている vNIC

vNIC のタイプ	ハイパーバイザのサポート		ASAv のバージョン	注意
	VMware	KVM		
e1000	対応	対応	9.2(1) 以降	VMware のデフォルト
virtio	非対応	対応	9.3(2.200) 以降	KVM のデフォルト
ixgbe-vf	対応	対応	9.8(1) 以降	AWS のデフォルト。SR-IOV サポート用の ESXi と KVM

ASAv と SR-IOV インターフェイスのプロビジョニング

Single Root I/O Virtualization (SR-IOV) により、さまざまなゲストオペレーティングシステムを実行している複数の VM が、ホストサーバ内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM がネットワーク アダプタとの間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバの CPU 負荷が低下します。最近の x86 サーバプロセッサには、SR-IOV に必要なダイレクトメ

モリの転送やその他の操作を容易にする Intel VT-d テクノロジーなど、チップセットの拡張機能が搭載されています。

SR-IOV 仕様では、次の 2 つのデバイス タイプが定義されています。

- 物理機能 (PF) : 基本的にスタティック NIC です。PF は、SR-IOV 機能を含む完全な PCIe デバイスです。PF は、通常の PCIe デバイスとして検出、管理、設定されます。単一 PF は、一連の仮想関数 (VF) の管理および設定を提供できます。
- Virtual Function (VF) : ダイナミック vNIC に似ています。VF は、データ移動に必要な最低限のリソースを提供する、完全または軽量の仮想 PCIe デバイスです。VF は直接的には管理されず、PF を介して配信および管理されます。1 つ以上の VF を 1 つの VM に割り当てることができます。

SR-IOV は、PCI 標準の開発および管理が公認されている業界組織である Peripheral Component Interconnect Special Interest Group (PCI SIG) によって定義および管理されています。SR-IOV の詳細については、『[PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology](#)』を参照してください。

ASAv 上で SR-IOV インターフェイスをプロビジョニングするには、適切なオペレーティングシステム レベル、ハードウェアと CPU、アダプタ タイプ、およびアダプタ設定から始まる計画が必要です。

SR-IOV インターフェイスに関するガイドラインと制限事項

ASAv の導入に使用する具体的なハードウェアは、サイズや使用要件によって異なります。[ASAv のライセンス \(1 ページ\)](#) は、さまざまな ASAv プラットフォームのライセンスの権限付与の条件を満たすリソースシナリオ準拠を示しています。加えて、SR-IOV 仮想機能には特定のシステム リソースが必要です。

ホスト オペレーティング システムとハイパーバイザ サポート

SR-IOV サポートと VF ドライバは、以下で使用できます。

- Linux 2.6.30 カーネル以降

SR-IOV インターフェイスを備えた ASAv は、現在、次のハイパーバイザでサポートされます。

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

ハードウェア プラットフォーム サポート

このセクションでは、SR-IOV インターフェイスに関するハードウェア ガイドラインについて説明します。以下はガイドラインであって要件ではありませんが、このガイドラインに従っていないハードウェアを使用すると、機能の問題や性能の低下につながる可能性があります。

SR-IOV をサポートしており、SR-IOV 対応 PCIe アダプタを搭載したサーバが必要です。以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。



(注) メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。

- VT-d 対応のチップセット、マザーボード、および CPU については、『[virtualization-capable IOMMU supporting hardware](#)』を参照してください。VT-d は、SR-IOV システムに必須の BIOS 設定です。
- VMware の場合は、オンラインの『[Compatibility Guide](#)』で SR-IOV サポートを検索できます。
- KVM の場合は、『[CPU compatibility](#)』を確認できます。KVM 上の ASAv では、x86 ハードウェアしかサポートされないことに注意してください。



(注) シスコでは、ASAv を [Cisco UCS C シリーズ ラック サーバ](#) でテストしました。Cisco UCS-B サーバは ixgbe-vf vNIC をサポートしていないことに注意してください。

SR-IOV でサポートされている NIC

- [Intel Ethernet Server Adapter X520 - DA2](#)
- [Intel Ethernet Server Adapter X540](#)

CPU

- x86_64 マルチコア CPU
Intel Sandy Bridge 以降（推奨）



(注) シスコでは、ASAv を 2.3GHz の Intel Broadwell CPU (E5-2699-v4) でテストしました。

- コア

- CPU ソケットあたり 8 個以上の物理コア
- 単一のソケット上で 8 コアにする必要があります。



(注) CPU ピンニングは、ASAv50 上でフルスループット レートを実現するために推奨されています。[ESXi 構成でのパフォーマンスの向上](#)と[KVM 構成でのパフォーマンスの向上](#)を参照してください。

BIOS 設定

SR-IOV は、BIOS だけでなく、ハードウェアで実行しているオペレーティング システム インスタンスまたはハイパーバイザのサポートも必要です。システム BIOS で次の設定をチェックします。

- SR-IOV が有効になっている。
- VT-x (仮想化テクノロジー) が有効になっている。
- VT-d が有効になっている。
- (オプション) ハイパースレッディングが無効になっている。

システムごとに BIOS 設定にアクセスして変更する方法が異なるため、ベンダーのマニュアルでプロセスを確認することをお勧めします。

制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の ASA プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。
- Cisco UCSB サーバは ixgbe-vf の vNIC をサポートしません。

