# ASAv の概要

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、データセント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することができます。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

ハイパーバイザのサポートについては、Cisco ASA の互換性 [英語] を参照してください。

## ASAv のライセンス

ASAv はシスコ スマート ソフトウェア ライセンシングを使用しています。詳細については、「Smart Software Licensing」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、以降の各セクション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（2 GB 推奨） | 100Mbps | あり |
| ASAv10（1 GB） | 1 vCPU/2 GB | 1Gbps | 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 |
|---|---|---|---|
| ASAv30（2 GB） | 4 vCPU/8 GB | 2 Gbps | あり |
| 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<br>（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<br>ASAv5（1vCPU、1G）、ASAv10（1vCPU、2G）、ASAv30（4vCPU、8G）、ASAv50（8vCPU、16G）<br>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<br>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<br>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<br>次の仕様を参照してください。<br>• 100 Mbps スループット<br>• 1 vCPU<br>• 1 GB RAM（1.5 GB に調節可能）<br>（注） 最適なパフォーマンスを実現するには、ASAv5 に 2 GB のメモリを推奨します。<br>• 50,000 の同時ファイアウォール接続<br>• AWS はサポート対象外<br>• 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<br>次の仕様を参照してください。<br>• 1 Gbps スループット<br>• 1 vCPU<br>• 2 GB のメモリ<br>• 100,000 の同時ファイアウォール接続<br>• c3.large、c4.large、および m4.large インスタンスで AWS をサポート<br>• 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<br>次の仕様を参照してください。<br>• 2 Gbps スループット<br>• 4 vCPU<br>• 8 GB RAM<br>• 500,000 の同時ファイアウォール接続<br>• c3.xlarge、c4.xlarge、および m4.xlarge インスタンスで AWS をサポート<br>• 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<br>次の仕様を参照してください。<br>• 10 Gbps スループット<br>• 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）<br>• 16 GB メモリ<br>• 2,000,000 の同時ファイアウォール接続<br>• 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 ASA ハードウェア ファイアウォールとよく似ていますが、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

### ディスク ストレージ

ASAv は、デフォルトで最大 8 GB の仮想ディスクをサポートします。ディスクサイズを 8 GB を超えて増やすことはできません。VM リソースをプロビジョニングする場合は、この点に注意してください。

### 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 を使用して高可用性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ことがあります。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。

- クラスタリング（KVM と VMware を除くすべての権限付与）
- 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

### 制限事項

- ASAv は、x710 NIC の 1.9.5 i40en ホストドライバと互換性がありません。これより古いバージョンまたは新しいバージョンのドライバは動作します。（VMware のみ）

# 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。
- 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ー向けであるため、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。
- 9.5(1.200) 以降、AVAv5 のメモリ要件は 1 GB に減りました。ASAv5 で使用可能なメモリを 2 GB から 1 GB にダウングレードすることはサポートされていません。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。

（注） 最適なパフォーマンスを実現するには、ASAv5 に 2 GB のメモリを推奨します。

- 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。
  - CLI から `show memory` コマンドを使用して、システムで使用可能な最大メモリと現在の空きメモリ量の概要を表示できます。
- 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）。

### 制限事項

- ASAv5 は AnyConnect HostScan 4.8 と互換性がありません。これには 2 GB の RAM が必要です。
- ASAv5 は Amazon Web Services（AWS）ではサポートされていません。
- ジャンボ フレームはサポートされていません。

# ASAv10 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

- 9 つ以上の設定済み e1000 インターフェイスを使用した ASAv10 のジャンボフレーム予約によって、デバイスがリロードされる場合があります。**ジャンボ フレーム予約**が有効になっている場合は、インターフェイスの数を 8 つ以下に減らしてください。インターフェイスの正確な数は、その他の構成済み機能の操作で必要となるメモリの量によって異なりますが、8 つより少なくすることはできます。

# 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。
- ASAv のパフォーマンスを向上させるために、次のプラクティスがサポートされています。
  - NUMA ノード
  - 複数の RX キュー
  - SR-IOV プロビジョニング
  - 詳細については、VMware での ASAv のパフォーマンス調整およびKVM での ASAv のパフォーマンス調整を参照してください。
- 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。
- ジャンボフレーム予約で e1000 インターフェイスと i40e-vf インターフェイスが混在していると、i40e-vf インターフェイスがダウン状態のままになる場合があります。**ジャンボフレーム予約**が有効になっている場合は、e1000 ドライバと i40e-vf ドライバを使用するインターフェイスのタイプが混在しないようにしてください。

### 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。
- ASAv は、x710 NIC の 1.9.5 i40en ホストドライバと互換性がありません。これより古いバージョンまたは新しいバージョンのドライバは動作します。（VMware のみ）
- Amazon Web Services（AWS）、Microsoft Azure、および Hyper-V ではサポートされません。
- Ixgbe vNIC 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 のインターフェイス
- サポートされている vNIC

# ASAv のインターフェイス

ASAv 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 ペアの一部として展開する場合は 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。

（注） 構成を簡単に移行できるように、Ten GigabitEthernet（VMXNET3 ドライバで使用可能なインターフェイスなど）にはGigabitEthernet というラベルが付いています。これは表面的なものであり、実際のインターフェイス速度には影響しません。

ASAv では、E1000 ドライバを 1 Gbps リンクとして使用してギガビット イーサネット インターフェイスが定義されます。VMware ではE1000 ドライバの使用が推奨されなくなってい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 では次の vNIC がサポートされています。同じ ASAv での vNIC の混在（e1000 と vmxnet3 など）はサポートされていません。

**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 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 | × | 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 |

| vNIC のタイプ | ハイパーバイザのサポート | | ASAv バージョン | 注意 |
|---|---|---|---|---|
| | VMware | KVM | | |
| VMXNET3 | 対応 | × | 9.9(2) 以降 | vmxnet3 を使用する場合は、TCP パフォーマンスの低下を避けるために大量受信オフロード（LRO）を無効にする必要があります。VMware および VMXNET3 の LRO を無効にします （10 ページ）を参照してください。 |
| i40e-vf | × | 対応 | 9.10(1) 以降 | SR-IOV サポート用の KVM |

### VMware および VMXNET3 の LRO を無効にします

Large Receive Offload（LRO）は、CPU オーバーヘッドを削減することによって、高帯域幅ネットワーク接続のインバウンドスループットを向上させる手法です。これは、1 つのストリームからの複数の着信パケットを大きなバッファに集約してから、ネットワークスタックの上位に渡されるようにすることによって、処理する必要があるパケットの数を減らすことによって機能します。ただし、LRO は、ネットワークパケット配信のフローが一貫せず、輻輳しているネットワークで「バースト」する可能性がある場合に、TCP パフォーマンスの問題を引き起こす可能性があります。

**重要** VMware は、デフォルトで LRO を有効にして、全体的なスループットを向上させます。したがって、このプラットフォームで ASAv 導入の LRO を無効にする必要があります。

ASAv マシンで LRO を直接無効化できます。設定変更を行う前に、仮想マシンの電源をオフにします。

1. vSphere Web Client インベントリで ASAv マシンを検索します。
   1. 仮想マシンを検索するには、データセンター、フォルダ、クラスタ、リソースプール、またはホストを選択します。
   2. [Related Objects] タブをクリックし、[Virtual Machines] タブをクリックします。
2. 仮想マシンを右クリックして、[Edit Settings] をクリックします。
3. [VM Options] をクリックします。
4. [Advanced] を展開します。
5. [Configuration Parameters] の下で、[Edit Configuration] ボタンをクリックします。
6. [Add Parameter] をクリックし、LRO パラメータの名前と値を入力します。
   - Net.VmxnetSwLROSL | 0

- Net.Vmxnet3SwLRO | 0
- Net.Vmxnet3HwLRO | 0
- Net.Vmxnet2SwLRO | 0
- Net.Vmxnet2HwLRO | 0

（注） オプションで、LROパラメータが存在する場合は、値を調べて必要に応じて変更できます。パラメータが 1 に等しい場合、LRO は有効です。0 に等しい場合、LRO は無効です。

7. [OK] をクリックして変更を保存し、[Configuration Parameters] ダイアログボックスを終了します。
8. [保存（Save）] をクリックします。

詳細については、次の VMware サポート記事を参照してください。

- VMware KB 1027511
- VMware KB 2055140

# 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、ホストサーバー内の単一の 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ーの CPU 負荷が低下します。最近の x86 サーバー 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、およびアダプタの設定から始める計画が必要です。

# 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） には、さまざまな ASAv プラットフォームに関するライセンスの権限付与条件に準拠するリソースシナリオが説明されています。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ています。

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

### ハードウェア プラットフォーム サポート

（注） サポートされている仮想化プラットフォームを実行できる任意のサーバークラスの x86 CPU デバイスに ASAv を導入する必要があります。

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ーが必要です。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 ラックサーバーでテストしました。Cisco UCS-B サーバーは 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 イーサネット ネットワーク アダプタ X710

注目 ASAv は、x710 NIC の 1.9.5 i40en ホストドライバと互換性がありません。これより古いバージョンまたは新しいバージョンのドライバは動作します。（VMware のみ）

- 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 および ASAv100 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。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている ASAv（プライマリ装置）に障害が発生すると、スタンバイ ASAv 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ ASAv 装置の新しい MAC アドレスで更新されます。その後、ASAv は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに

通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。