Cisco Secure Firewall ASA Virtual の概要

適応型セキュリティアプライアンス仮想（ASA仮想）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、ASA 仮想 を管理およびモニター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 （1 ページ）
- ASA 仮想 のライセンス （1 ページ）
- 注意事項と制約事項 （7 ページ）
- ASA 仮想 インターフェイスおよび仮想 NIC （11 ページ）
- ASA 仮想 と SR-IOV インターフェイスのプロビジョニング （13 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 Secure Firewall ASA の互換性 [英語] を参照してください。

ASA 仮想 のライセンス

ASA 仮想 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） ASA仮想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。

9.13(1) 以降では、サポートされているすべての ASA 仮想 vCPU/メモリ構成ですべての ASA 仮想 ライセンスを使用できます。これにより、さまざまな VM リソースフットプリントに ASA 仮想 を導入できます。セキュアクライアント および TLS プロキシのセッション制限は、モデ

ルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASA 仮想 プラットフォームの権限付与によって決まります。

ASA 仮想 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。

スマートライセンスの権限付与について

すべての ASA 仮想 ライセンスを、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できます。これにより、さまざまな VM リソースフットプリントで ASA 仮想 を実行できます。また、サポート対象の AWS および Azure インスタンスタイプの数も増えます。ASA 仮想 マシンを構成する場合、サポートされる最大 vCPU 数は 16（ASAv100）個です。AWS と OCI 以外のすべてのプラットフォームに展開された ASA 仮想の場合、サポートされる最大メモリは 64GB です。AWS および OCI に展開された ASA 仮想の場合、サポートされる最大メモリは 128GB です。

重要 一度展開した ASA 仮想 インスタンスのリソース割り当て（メモリ、CPU、ディスク容量）は変更できません。何らかの理由でリソース割り当てを増やす必要がある場合（たとえば、ライセンス付与された権限を ASAv30/2Gbps から ASAv50/10Gbps に変更する場合）、必要なリソースを使用して新しいインスタンスを作成する必要があります。

- vCPU：ASA 仮想 は、VMware と KVM を除くすべてのプラットフォームで 1 ～ 16 個の vCPU。
- メモリ：AWS と OCI 以外のすべてのプラットフォームに展開された ASA 仮想の場合、ASA 仮想 は 2GB ～ 64GB の RAM をサポートします。AWS および OCI に展開された ASA 仮想の場合、サポートされる最大メモリは 128GB です。
- ディスクストレージ：ASA 仮想 はデフォルトで最小 8GB の仮想ディスクをサポートします。プラットフォームのタイプに応じて、仮想ディスクのサポートは 8GB ～ 10GB の間となります。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。

重要 ASA 仮想 の最小メモリ要件は 2 GB です。現在の ASA 仮想 が 2 GB 未満のメモリで動作している場合、ASA 仮想マシンのメモリを増やさないと、以前のバージョンからバージョン 9.13(1) 以降にアップグレードできません。また、最新バージョンを使用して新しい ASA 仮想 マシンを再導入できます。

1 つ以上の vCPU を使用して ASA 仮想 を展開するための最小メモリ要件は 4 GB です。

ASA 仮想 バージョン 9.14 以降から最新バージョンにアップグレードするには、ASA 仮想マシンに 4 GB 以上のメモリと 2 vCPU が必要です。

ライセンスされた機能のセッション制限

セキュアクライアントおよびTLSプロキシのセッション制限は、インストールされたASA仮想プラットフォームの権限付与層によって決まり、レート制限の適用を受けます。次の表は、権限付与層とレート制限に基づくセッション制限をまとめたものです。

表 *1*：権限付与による *ASA* 仮想 セッションの制限

権限付与	セキュアクライアント Premium ピア	合計 TLS プロキシセッション	レートリミッタ
標準層、100M	50	500	150 Mbps
標準層、1G	250	500	1 Gbps
標準層、2G	750	1000	[2 Gbps]
標準層、10G	10,000	10,000	10 Gbps
標準層、20G	20,000	20,000	20 Gbps

前の表に示したように、権限付与によって付与されたセッション制限は、プラットフォームのセッション制限を超えることはできません。プラットフォームのセッション制限は、ASA仮想用にプロビジョニングされたメモリ量に基づいて決まります。

表 *2*：メモリ要件による *ASA* 仮想 セッション制限

プロビジョニングされたメモリ	セキュアクライアント Premium ピア	合計 TLS プロキシセッション
2 GB ～ 7.9 GB	250	500
8 GB ～ 15.9 GB	750	1000
16 GB ～ 31.9 GB	10,000	10,000
32 GB ～ 64 GB	20,000	20,000
64 GB ～ 128 GB	20,000	20,000

プラットフォームの制限

ファイアウォール接続、同時接続、およびVLANは、ASA仮想メモリに基づくプラットフォームの制限です。

（注） ASA 仮想 がライセンスされていない状態にある場合、ファイアウォール接続は 100 に制限されます。権限付与によってライセンスが付与されると、接続はプラットフォームの制限に移行します。ASA 仮想 の最小メモリ要件は 2GB です。

表 *3:* プラットフォームの制限

ASA 仮想 のメモリ	ファイアウォールの接続、同時	VLANs
2 GB ～ 7.9 GB	100,000	50
8 GB ～ 15.9 GB	500,000	200
16 GB ～ 31.9	2,000,000	1024
32 GB ～ 64 GB	4,000,000	1024

ASA 仮想 プライベートクラウドの権限付与（VMware、KVM、Hyper-V）

すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できるため、プライベートクラウド環境（VMware、KVM、Hyper-V）に ASA 仮想 を導入する場合の柔軟性が高まります。

（注） ASAv50 と ASAv100 は、HyperV ではサポートされません。

セキュアクライアント および TLS プロキシのセッション制限は、インストールされた ASA 仮想プラットフォームの権限付与層によって決まり、レート制限の適用を受けます。次の表は、プライベートクラウド環境に導入された ASA 仮想 の権限付与層に基づくセッション制限と、適用されるレート制限をまとめたものです。

（注） ASA 仮想 セッション制限は、ASA 仮想 用にプロビジョニングされたメモリの量に基づいています。表 2 : メモリ要件による ASA 仮想 セッション制限 （3 ページ）を参照してください。

表 *4: VMware/KVM/HyperV* プライベートクラウドの *ASA* 仮想：権限付与に基づいてライセンスされた機能の制限

RAM（GB）		権限付与のサポート *				
最小	最大	標準層、100M	標準層、1G	標準層、2G	標準層、10G	標準層、20G
2	7.9	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
8	159	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
16	319	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
32	64	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	20K/20K/20G

RAM（GB）		権限付与のサポート *				
最小	最大	標準層、100M	標準層、1G	標準層、2G	標準層、10G	標準層、20G
*セキュアクライアントセッション/TLSプロキシセッション/権限付与またはインスタンスごとのレート制限。						

ASA 仮想 パブリッククラウドの権限付与（AWS）

すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できるため、さまざまな AWS インスタンスタイプに ASA 仮想 を導入できます。セキュアクライアント および TLS プロキシのセッション制限は、インストールされた ASA 仮想 プラットフォームの権限付与層によって決まり、レート制限の適用を受けます。

次の表は、AWS インスタンスタイプの権限付与層に基づくセッション制限とレート制限をまとめたものです。サポートされているインスタンスの AWS VM の規模（vCPU とメモリ）の内訳については、「AWS クラウドへの ASA 仮想 の導入について」を参照してください。

表 *5 : AWS* 上の *ASA* 仮想：権限付与に基づくライセンス機能の制限

インスタンス	BYOL 権限付与のサポート *				PAYG **
	標準層、100M	標準層、1G	標準層、2G	標準層、10G	
c5.xlarge	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000
c5.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K
c4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
c3.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
m4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
m4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	10K/10K
m4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K

インスタンス	BYOL 権限付与のサポート *				PAYG **
	標準層、100M	標準層、1G	標準層、2G	標準層、10G	
*セキュアクライアントセッション/TLSプロキシセッション/権限付与またはインスタンスごとのレート制限。 ** セキュアクライアント セッション/TLS プロキシセッション。PAYG モードではレート制限は使用されません。					

Pay-As-You-Go（PAYG）モード

次の表に、毎時課金（PAYG）モードにおける各層のスマートライセンス権限付与の概要を示します。PAYG モードは、割り当てられたメモリに基づきます。

表 *6 : AWS* 上の *ASA* 仮想：*PAYG* のスマートライセンス権限付与

RAM（GB）	毎時課金モードの権限付与
2 GB 未満	標準層、100M（ASAv5）
2 GB ～ 8 GB 未満	標準層、1G（ASAv10）
8 GB ～ 16 GB 未満	標準層、2G（ASAv30）
16 GB ～ 32 GB 未満	標準層、10G（ASAv50）
30 GB 以上	標準層、20G（ASAv100）

ASA 仮想 パブリッククラウドの権限付与（Azure）

すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できるため、さまざまな Azure インスタンスタイプに ASA 仮想 を導入できます。セキュアクライアント および TLS プロキシのセッション制限は、インストールされた ASA 仮想 プラットフォームの権限付与層によって決まり、レート制限の適用を受けます。

次の表は、Azure インスタンスタイプの権限付与層に基づくセッション制限とレート制限をまとめたものです。サポートされているインスタンスの Azure VM の規模（vCPU とメモリ）の内訳については、「Microsoft Azure クラウドへの ASA 仮想 の導入について」を参照してください。

（注） Pay-As-You-Go（PAYG）モードは現在、Azure 上の ASA 仮想 ではサポートされていません。

表 *7: Azure* 上の *ASA* 仮想：権限付与に基づくライセンス機能の制限

インスタンス	BYOL 権限付与のサポート *				
	標準層、100M	標準層、1G	標準層、2G	標準層、10G	標準層、20G
D1、D1_v2DS1、DS1_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
D2、D2_v2、DS2、DS2_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
D3、D3_v2、DS3、DS3_v2	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4、D4_v2、DS4、DS4_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D5、D5_v2、DS5、DS5_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
D2_v3	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D8_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
F4、F4s	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
F8、F8s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
F16、F16s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
*セキュアクライアントセッション/TLSプロキシセッション/権限付与またはインスタンスごとのレート制限。					

注意事項と制約事項

ASA 仮想 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。

ASA 仮想（すべての権限付与）のガイドラインと制限事項

スマートライセンスのガイドライン

- サポートされる vCPU の最大数は 16 です。AWS と OCI 以外のすべてのプラットフォームに展開された ASA 仮想の場合、サポートされる最大メモリは 64GB です。AWS および

OCI に展開された ASA 仮想の場合、サポートされる最大メモリは 128GB です。すべての ASA 仮想 ライセンスを、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できます。

- ライセンスされた機能およびライセンスされていないプラットフォーム機能のセッション制限は、VM メモリの量に基づいて設定されます。
- セキュアクライアントおよびTLSプロキシのセッション制限は、ASA仮想プラットフォームの権限付与によって決定されます。セッション制限は、ASA 仮想 モデルタイプ（ASAv5/10/30/50/100）に関連付けられなくなりました。
- セッション制限には最小メモリ要件があります。VM メモリが最小要件を下回っている場合、セッション制限はそのメモリ量でサポートされる最大数に設定されます。
- 既存の権限付与に変更はありません。権限付与 SKU と表示名には、引き続きモデル番号（ASAv5/10/30/50/100）が含まれます。
- 権限付与は、レート制限を介して最大スループットを設定します。
- お客様の発注プロセスに変更はありません。

ディスク ストレージ

ASA 仮想 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ライセンス権限付与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 2Gbps の権限付与であることなど）。

重要

- ASA 仮想 を使用して高可用性（HA）ペアを作成する場合は、データインターフェイスを各 ASA 仮想 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 ASA 仮想 に追加されると、ASA 仮想 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。
- リソースが一致していなくても、2 つの ASA virtual インスタンス間の HA を設定できます（例：一方のインスタンスが 8GB RAM でもう一方のインスタンスが 16GB RAM の場合など）。この構成は、ヒットレスアップグレードを容易にするためにサポートされています。ただし、リソース割り当ての変更が完了するまでに必要な期間を超えて、リソースが一致しない状態で HA を実行することは推奨されません。

サポートしない ASA 機能

ASA 仮想 は、次の ASA 機能をサポートしません。

- クラスタリング（ AWS、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

- ASA 仮想 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）

1 GB 権限付与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 1 GB プラットフォーム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。

10 GB 権限付与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。
- ASA 仮想 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、パフォーマンスの調整およびパフォーマンスの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。
- ASA 仮想 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）
- Hyper-V ではサポートされていません。

20 GB 権限付与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 20 Gbps がサポートされます。
- ASA 仮想 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、パフォーマンスの調整およびパフォーマンスの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。

制限事項

- ASA 仮想 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）
- 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）および Hyper-V ではサポートされません。

ASA 仮想 インターフェイスおよび仮想 NIC

ASA 仮想 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。ASA 仮想 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。

- ASA 仮想 のインターフェイス
- サポートされている vNIC

ASA 仮想 のインターフェイス

ASA 仮想 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。ASA 仮想 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。

ASA 仮想 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

ASA 仮想 では次の vNIC がサポートされています。同じ ASA 仮想 での vNIC の混在（e1000 と vmxnet3 など）はサポートされていません。

表 *8*：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		ASA 仮想 バージョン	注意
	VMware	KVM		
VMXNET3	対応	非対応	9.9(2) 以降	VMware のデフォルト 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 （12 ページ）を参照してください。
e1000	対応	対応	9.2(1) 以降	VMware では推奨されません。
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。
i40e-vf	非対応	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 ASA 仮想 導入の LRO を無効にする必要があります。

ASA 仮想 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 ASA 仮想 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

ASA 仮想 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。

ASA 仮想 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

ASA 仮想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。ASA 仮想 のライセンス （1 ページ） には、さまざまな ASA 仮想 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 ASA 仮想 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 ASA 仮想 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 ASA 仮想 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、ASA 仮想 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 ASA 仮想 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

CPU

- x86_64 マルチコア CPU

  Intel Sandy Bridge 以降（推奨）

（注） シスコでは、ASA 仮想 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 ASA 仮想（プライマリ装置）に障害が発生すると、スタンバイ ASA 仮想 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 ASA 仮想 装置の新しい MAC アドレスで更新されます。その後、ASA 仮想 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。