Amazon Web Services の Amazon Elastic Compute Cloud への Cisco Web セキュリティ仮想アプライアンスおよびセキュリティ管理仮想アプライアンスの導入

発行日：2019 年 3 月 18 日

目次

Cisco コンテンツ セキュリティ仮想アプライアンスについて

Cisco コンテンツ セキュリティ仮想アプライアンスは、仮想アプライアンスの管理（9 ページ）に記載されているわずかな変更を除き、Web セキュリティまたはコンテンツ セキュリティ管理の各物理 ハードウェア アプライアンスと同じように機能します。

Amazon Web Services（AWS）Elastic Compute Cloud（EC2）への導入実装では、Amazon マーケットプレイスで使用できる Amazon マシン イメージ（AMI）を使用します。

注 Cisco Web セキュリティおよびセキュリティ管理仮想アプライアンスは、AWS EC2 でサポートされます。

シスコシステムズ合同会社
www.cisco.com/jp

Amazon マシン イメージ(AMI)について

Amazon マシン イメージ(AMI)を使用すると、EC2 内部に仮想マシン インスタンスを作成することができます。Web セキュリティ アプライアンスおよびセキュリティ管理アプライアンスの AMI は、AWS マーケットプレイスで使用できます。必要な AMI を選択し、導入処理を進めます。

Cisco Web セキュリティおよびセキュリティ管理仮想アプライアンスの AMI

Cisco Web セキュリティおよびセキュリティ管理仮想アプライアンスの AMI の詳細は、以下のとおりです。

Cisco Web セキュリティ仮想アプライアンス(AsyncOS 11.7.0-333)
既存の AsyncOS 11.5.1-115 および 11.5.0-614 導入環境から AsyncOS 11.7.0-333 にアップグレードできます。

Cisco Web セキュリティ アプライアンス リリース向け AsyncOS	仮想アプライアンス	AMI ID
AsyncOS 11.5.1-115	**S100V**	coeus-11-5-91-001-S100V-AMI-300818
	S300V	coeus-11-5-91-001-S300V-AMI-310818
	S600V	coeus-11-5-91-001-S600V-AMI-310818
AsyncOS 11.5.0-614	**S100V**	coeus-11-5-0-614-S100V-AMI-110518
	S300V	coeus-11-5-0-614-S300V-AMI-120518
	S600V	coeus-11-5-0-614-S600V-AMI-120518

Cisco セキュリティ管理仮想アプライアンス(AsyncOS 11-5-1-114)パブリック AMI

コンソールを使用して共有パブリック AMI を検索するには、次の手順を実行します。

1. Amazon EC2 コンソールを開きます。
2. ナビゲーション ウィンドウで、[AMI(AMIs)] を選択します。
3. 最初のフィルタで、[パブリックイメージ(Public images)] を選択します。
4. 検索バーを選択し、必要な仮想アプライアンス モデルに従って、zeus-11-5-1-114-M100V、zeus-11-5-1-114-M300V、または zeus-11-5-1-114-M600V を入力します。

Cisco セキュリティ管理仮想アプライアンス (AsyncOS 11.5.0-108)	AMI ID
M100V	zeus-11-5-0-108-M100V-AMI-040518
M300V	zeus-11-5-0-108-M300V-AMI-050518
M600V	zeus-11-5-0-108-M600V-AMI-050518

ライセンシング

Amazon AWS での導入では、既存の Web セキュリティまたはセキュリティ管理アプライアンスのライセンスを使用することができます。導入後、インスタンスを起動してライセンスをインストールできます。AWS インフラストラクチャのみ有料となり、支払が発生します。

既存のお客様は、テクニカル ノート『Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses』のトピック「Obtain a Virtual License (VLN)」を参照してください。始めてご利用の方は、最寄りのシスコ パートナーにお問い合わせの上、ライセンスを取得してください。

AWS での導入

注

- L4 トラフィック モニタ機能は、Web セキュリティ仮想アプライアンスのリリース AsyncOS 11.5 および 11.5.1 ではサポートされていません。
- Web トラフィック タップは、Web セキュリティ仮想アプライアンスのリリース AsyncOS 11.5.1 ではサポートされていません。
- オンプレミスの Cisco E メール セキュリティ アプライアンスは、AWS での Cisco セキュリティ管理アプライアンスの導入ではサポートされていません。

Web セキュリティまたはセキュリティ管理仮想アプライアンスを導入するには、次の手順を実行します。

	操作内容	追加情報
ステップ 1	前提条件となるタスクを完了し、EC2 でのインスタンスの設定前に必要となる情報を取得して環境準備を行います。	環境の準備 (4 ページ)。
ステップ 2	Amazon マーケットプレイスから [AMI] を選択し、適切なインスタンス タイプを選択します。	仮想アプライアンス AMI およびインスタンス タイプの選択 (5 ページ)。
ステップ 3	ネットワーク、サブネット、IP アドレスの割り当て、およびインスタンスを使用可能にするのに必要なその他の詳細を設定し、必要に応じて機能するようにします。 **注** プライマリ ネットワーク インターフェイス (management) が 1 つ、インスタンスに自動的に割り当てられます。必要に応じて、データ インターフェイスを作成することができます (P1 (S100V 用)、P1 および P2 (S300V および S600V 用))。	インスタンスの詳細設定 (6 ページ)。
ステップ 4	デフォルトのストレージ設定を保持するか、必要に応じてタグを設定します。	ストレージの構成とタグの追加 (7 ページ)。
ステップ 5	セキュリティ グループを設定します。すべての構成時の設定を確認し、インスタンスを起動します。	セキュリティ グループの設定、確認、およびインスタンスの起動 (7 ページ)。

	操作内容	追加情報
ステップ 6	アプライアンスにライセンスをインストールし、アプライアンス固有のホスト名で応答する Web インターフェイスを無効にします。`hostheader` コマンドを使用して、変更を確定します。	起動済みインスタンスの設定（7 ページ）。
ステップ 7	アプライアンスの Web インターフェイスに接続します。システム セットアップ ウィザードの実行、コンフィギュレーション ファイルのアップロード、または機能の設定が可能です。	アプライアンスの Web インターフェイスへの接続（8 ページ）。
ステップ 8	（オプション）必要に応じて、AWS EC2 マネジメント コンソールに Elastic IP アドレスを設定します。	Elastic IP アドレスの作成（8 ページ）。
ステップ 9	アプライアンスにライセンスの期限切れアラートを設定します。	ライセンスの有効期限が近い場合にアラートを送信するようアプライアンスを設定する（9 ページ）。

環境の準備

AWS EC2 での Web セキュリティまたはセキュリティ管理仮想アプライアンスの導入に必要なリソースおよびファイルがあることを確認します。これには次が含まれます。

- Web セキュリティまたはセキュリティ管理仮想アプライアンスの有効なライセンス。
- Web セキュリティ アプライアンスに使用する、次のデフォルトのユーザ名およびパスワード。
  - `admin` および `ironport`
- EC2 管理コンソール内のリソース：
  - インスタンスに関連付けることのできる永続的なパブリック IP アドレスが必要な場合は、使用する Elastic IP アドレスを選択するか、新しいアドレスを作成します。新しいインスタンスの起動プロセス時に自動的に割り当てられるパブリック IP アドレスは動的です。
  - 使用する VPC を確認し、不明な場合は導入時に使用する VPC を設定します。デフォルトの VPC を使用することもできます。
  - 管理者や他のユーザがアプライアンスにアクセスする方法に基づいて、アプライアンスに割り当てられる IP アドレスのタイプを決定する必要があります（パブリックまたはプライベート）。
  - 使用する IAM ロールを確認し、不明な場合は導入時に使用する IAM ロールを設定します。
  - サブネットを構成し、ルーティング テーブルにインターネット ゲートウェイを示すデフォルト ルート ポイントが設定されていることを確認します。
  - セキュリティ グループを設定するか、新しいグループを作成します。
  - 正常な通信を行うために仮想アプライアンスで開く最も一般的なポートは、次のとおりです。
    - SSH TCP 22
    - TCP 443
    - TCP 8443
    - TCP 3128
    - （オプション）ICMP（適宜。デバッグ用）

- EC2 インスタンスで AWS を登録する際に必要となる秘密キー（PEM または CER ファイル）にアクセスできることを確認します。また、Web セキュリティまたはセキュリティ管理仮想アプライアンス インスタンスの起動プロセス中に新しい秘密キーを作成することもできます。

注 Windows クライアントでは、PEM ファイルへのアクセスに SSH クライアントが必要となります。

仮想アプライアンス AMI およびインスタンス タイプの選択

AWS アカウントで選択した適切な領域があることを確認します。

1. EC2 管理コンソールに移動します。
2. [Launch Instance] をクリックしドロップダウンリストで [Launch Instance] を選択します。
3. [AWS Marketplace] をクリックします。
4. Cisco Web セキュリティまたはセキュリティ管理仮想アプライアンスのモデルに基づいてインスタンス タイプを選択します。たとえば、Web セキュリティ仮想アプライアンス S300V モデルが必要な場合は、c4.xlarge、および対応する vCPU、vRAM などを選択します。

製品	AsyncOS バージョン	モデル	EC2 インスタンス タイプ	vCPU	vRAM	vNIC	最小ディスク サイズ
Cisco Web セキュリティ仮想アプライアンス	AsyncOS 11.5 以降（Web）	**S100V**	m4.large	2	6 GB	2	250 GB
		S300V	c4.xlarge	4	7.5 GB	4	1024 GB
		S600V	c4.4xlarge	16	30 GB	8	1024 GB

製品	AsyncOS バージョン	モデル	EC2 インスタンス タイプ	vCPU	vRAM	最小ディスク サイズ
Cisco コンテンツ セキュリティ管理仮想アプライアンス	AsyncOS 11.5	**M100V**	m4.large	2	6 GB	250 GB
		M300v	c4.xlarge	4	7.5 GB	1024 GB
		M600v	c4.2xlarge	8	8 GB	2032 GB

注

- 7.5 GB vRAM で S300V アプライアンスを構成すると、仮想マシン イメージの設定が誤っているか、RAID ステータスが最適でないことを示す警告メッセージが表示されます。これらの警告メッセージは、`loadlicense` や `upgrade` といった CLI コマンドを使用している場合に表示されます。これらのメッセージは無視しても差し支えありません。vRAM 構成がアプライアンスの通常の機能に影響を与えることはありません。
- 分割ルーティングを使用する場合は、プロキシのリスニング ポートにパブリック IP アドレス（Elastic IP）を割り当てる必要があります。

5. [Next: Configure Instance Details] をクリックします。

インスタンスの詳細設定

1. インスタンスの数を入力します。

注 分割インスタンスの購入オプションを使用すると、AWS クラウド内に予備のコンピューティング容量を購入できます。詳細については、Amazon EC2 のドキュメントを参照してください。

2. [Network] ドロップダウンリストで適切な VPC を選択します。
3. [Subnet] ドロップダウンリストで、この導入に必要なサブネットを選択します。
4. [Auto-assign Public IP] ドロップダウンリストで、必要なオプションを選択します。
   - [Use subnet setting (Enable)] を選択して、サブネットの設定で指定された設定に従ってパブリック IP アドレスを割り当てます。
   - [有効化(Enable)] を選択して、このインスタンスのパブリック IP アドレスを要求します。このオプションによって、パブリック IP アドレスのサブネットの設定が上書きされます。
   - パブリック IP を自動割り当てする必要がない場合は、[Disable] を選択します。このオプションによって、パブリック IP アドレスのサブネットの設定が上書きされます。
5. IAM ロールを選択します。
6. [Shutdown behavior] を選択します。ここでは [Stop] を選択することをお勧めします。

注意 [Terminate] を選択すると、インスタンスとそのすべてのデータが削除されます。

7. (オプション) [Protect against accidental termination] チェック ボックスをオンにします。
8. (オプション) 要件に従って、[Monitoring]、[EBS-optimized instance]、および [Tenancy] などその他のオプションを確認し、選択します。
9. [Network Interface] を選択します。
   - 必要に応じて、以前に作成したネットワーク インターフェイスからインターフェイスを追加できます。
   - 別のネットワーク インターフェイスを追加するには、[Add Device] を選択します。インスタンスの起動時は、ネットワーク インターフェイスを最大 2 つまで指定できます。インスタンスの起動後は、ナビゲーション ペインで [Network Interfaces] を選択して、ネットワーク インターフェイスを追加します。
   - ネットワーク インターフェイスを複数指定している場合は、パブリック IP アドレスを自動割り当てできません。
   - 1 つのインスタンス タイプに作成できるネットワーク インターフェイスの数には上限があります。仮想アプライアンス AMI およびインスタンス タイプの選択 (5 ページ) のステップ 4 を参照してください。
   - スタティック IP アドレスを作成するには、Elastic IP アドレスの作成 (8 ページ) を参照してください。

ストレージの構成とタグの追加

1. デフォルトのストレージ オプションを保持します。必要に応じて、それらのオプションを編集することができます。

   注 シスコでは、すべての導入においてプロビジョンド IOPS SSD を使用することをお勧めします。General Purpose SSD を使用することもできますが、プロビジョンド IOPS SSD を指定することで最適なパフォーマンスを発揮します。インスタンスで初めてログインできるようになるまで、最大で 45 分ほどかかる場合があります。

2. 必要なタグを入力します。インスタンスのタグは 1 つまたは複数作成できます。

   たとえば、キーに *name*、その値に *Cisco wsa* と入力できます。

セキュリティ グループの設定、確認、およびインスタンスの起動

1. 導入時に、適切な [Security Group] を選択します。
2. [Review and Launch] をクリックします。
3. 構成を確認し、すべての詳細が要件と一致していることを確認します。
4. インスタンスを起動します。
5. 既存のキー ペアを選択するか、新しいキー ペアを作成してダウンロードします。キー ペアのないインスタンスの作成はサポートされていません。
6. [Launch] をクリックしてインスタンスを起動します。
7. [Instances] をクリックします。

   これで、新しく設定されたインスタンを EC2 の [Instances] ページに表示できるようになります。インスタンスの確認が正常に終了すると、[Status Checks] 列の下に緑のチェック マークと [2/2 checks passed] が表示されます。
8. （オプション）システム ログを表示するには、次の手順を実行します。
   a. [Instances] ページで、インスタンスを選択します。
   b. [Actions] をクリックします。
   c. [Instance Settings] の [Get System Log] をクリックします。
   d. ログイン プロンプトが表示されたら、インスタンスが動作していることになります。
9. （オプション）パブリック IP をインスタンスに割り当てることを選択した場合は、パブリック IP アドレスを使用してアクセスできるかどうかを確認します。

起動済みインスタンスの設定

1. EC2 ナビゲーション パネルで [Instances] をクリックします。
2. インスタンスを選択して、[Connect] をクリックします。
3. [Connect to Your Instance] ダイアログ ボックスで接続情報を確認します。この情報は、SSH を介して仮想アプライアンスに接続する場合に必要となります。これには、パブリック DNS と使用した PEM ファイルが含まれます。キーが公開されていないことを確認します。

   注 デフォルトのユーザ名は `admin` で、表示されたルートではありません。

4. SSH クライアントを使用して、インスタンスに接続します。
5. `loadlicense` コマンドを使用して、CLI 経由でライセンスを貼り付けるか、ファイルからロードします。

   注 推奨される 7.5 GB vRAM を使用した S300V アプライアンスの場合、仮想マシン イメージの設定が誤っているか、RAID ステータスが最適でないことを示す警告メッセージが表示されます。これらの警告メッセージは、`loadlicense` や `upgrade` といった CLI コマンドを使用している場合に表示されます。これらのメッセージは無視しても差し支えありません。vRAM 構成がアプライアンスの通常の機能に影響を与えることはありません。

6. アプライアンス固有のホスト名で応答する Web インターフェイスを無効にします。`adminaccessconfig > hostheader` CLI を使用して変更を確定します。

   『Cisco Web Security Appliance User Guide』の「Perform System Administration Tasks」章の「Additional Security Settings for Accessing the Appliance」トピックを参照してください。

アプライアンスの Web インターフェイスへの接続

アプライアンスのソフトウェアを構成するには、Web インターフェイスを使用します。インスタンスを選択すると、IP アドレスが [説明(Description)] タブに表示されます。デフォルトのユーザ名とパスワードは、それぞれ `admin` と `ironport` です。https のデフォルト ポートは 8443、http のデフォルト ポートは 8080 です。

たとえば、以下を行うことができます。

- System Setup ウィザードの実行

  注 IP アドレスとデフォルト ゲートウェイは AWS から選択します。これらの設定は保持できます。すべてのマルウェアを [ブロック(Block)] に設定することをお勧めします。

- コンフィギュレーション ファイルのアップロード
- 手動による機能の設定
- アプライアンスのアクセスと設定の手順の詳細については(必要な情報の収集を含む)、その他の情報(12 ページ)の関連する場所から入手可能なオンライン ヘルプ、またはお使いの AsyncOS リリースのユーザ ガイドを参照してください。
- 物理アプライアンスから設定を移行するには、お使いの AsyncOS リリースのリリース ノートを参照してください。

機能キーはそれぞれの機能を有効にするまでアクティブ化されません。

Elastic IP アドレスの作成

Elastic IP アドレスを作成するには、次の手順を実行します。

1. EC2 ナビゲーションペインで [Elastic IPs] をクリックします。
2. [Allocate new address] をクリックします。
3. [Allocate] をクリックします。新しいパブリック IP アドレスが割り当てられます。IP アドレスをクリックするか、[Close] をクリックします。
4. 作成した IP アドレスを選択します。

5. [Actions] をクリックし、[Associate Address] を選択します。
6. [Resource type] を選択します。
7. ドロップダウン リストでインスタンスを選択します。
8. プライベート IP アドレスを選択し、Elastic IP アドレスを関連付けます。
9. [Associate] をクリックします。
10. [Close] をクリックします。

ライセンスの有効期限が近い場合にアラートを送信するようアプライアンスを設定する

その他の情報（12 ページ）の関連する場所から入手可能なオンライン ヘルプ、またはお使いの AsyncOS リリースのユーザ ガイドを参照してください。

仮想アプライアンスの管理

仮想アプライアンスのライセンス

注 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。テクニカル サポートのトンネルに関する情報は、AsyncOS リリースのユーザ ガイドにあります。

Cisco コンテンツ セキュリティ仮想アプライアンスでは、ホスト上で仮想アプライアンスを実行するための追加ライセンスが必要です。このライセンスは複数のクローン作成された仮想アプライアンスに使用できます。

Cisco Web セキュリティ仮想アプライアンスの場合：

- 個々の機能の機能キーごとに有効期限が異なる可能性があります。
- 仮想アプライアンス ライセンスの有効期限が切れた後も、アプライアンスは 180 日間のセキュリティ サービスなしで引き続き Web プロキシとして機能するか（Cisco Web セキュリティ アプライアンス）、または隔離済みメッセージを自動的に処理します（セキュリティ管理アプライアンス）。この期間中、セキュリティ サービスは更新されません。コンテンツ セキュリティ管理アプライアンス では、管理者とエンド ユーザが隔離を管理することはできませんが、管理対象アプライアンスでは引き続き管理対象 E メール セキュリティ アプライアンス からの隔離済みメッセージを受け入れ、スケジュールされた隔離済みメッセージの削除が実行されます。

注 AsyncOS バージョンを復帰させた場合の影響については、ご使用の AsyncOS のリリースのオンライン ヘルプまたはユーザ ガイドを参照してください。

仮想アプライアンスの電源オフ

強制リセット、電源オフ、およびリセットの各オプションは完全にはサポートされていません。Cisco Web セキュリティまたはセキュリティ管理仮想アプライアンスを実行中のインスタンスを終了したり停止したりすることができます。

仮想アプライアンスの CLI コマンド

以下は、仮想アプライアンスの CLI コマンドに関する変更点です。

コマンド	仮想 WSA でのサポートの有無	仮想 SMA でのサポートの有無	情報
loadlicense	あり	あり	このコマンドを使うと、仮想アプライアンスにライセンスをインストールすることができます。最初にこのコマンドを使用してライセンスをインストールしないと、仮想アプライアンスの System Setup ウィザードは実行できません。
etherconfig	あり	—	仮想アプライアンスにペアリングのオプションは含まれていません。
version	あり	—	このコマンドは、UDI、RAID および BMC 情報を除き、仮想アプライアンスに関するすべての情報を返します。
resetconfig	あり	—	このコマンドを実行すると、アプライアンス上に仮想アプライアンス ライセンスおよび機能キーが残ります。
revert	あり	—	ご使用のアプライアンスのオンライン ヘルプおよびユーザ ガイドのシステム管理の章で動作が説明されています。
reload	あり	—	このコマンドを実行すると、アプライアンスで仮想アプライアンス ライセンスおよびすべての機能キーが削除されます。このコマンドは、Cisco Web セキュリティ アプライアンスでのみ使用可能です。

diagnostic	あり	—	次の `diagnostic > raid` サブメニュー オプションでは、情報は返されません。
			`1. Run disk verify`
			`2. 実行中のタスクのモニタ`
			`3. Display disk verify verdict`
			このコマンドは、Web セキュリティ アプライアンスでのみ使用可能です。

showlicense	あり	あり	ライセンスの詳細を表示します。 Cisco Web セキュリティ仮想アプライアンスの追加情報は、`featurekey` コマンドを使用して入手できます。

仮想アプライアンスの SNMP

仮想アプライアンスの AsyncOS はハードウェア関連の情報については報告せず、ハードウェア関連のトラップは生成されません。次の情報は、クエリーから除外されます。

- `powerSupplyTable`
- `temperatureTable`
- `fanTable`
- `raidEvents`
- `raidTable`

仮想アプライアンスのサポートの取得

注 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco コンテンツ セキュリティ仮想アプライアンスのサポート ケースを報告する場合は、契約番号と製品 ID コード（PID）を提供する必要があります。

発注書を参照するか以下の一覧を参照すると、仮想アプライアンスで動作中のソフトウェア ライセンスに基づく PID を特定できます。

- Cisco 仮想 Web セキュリティ アプライアンスの製品 ID コード（PID）（11 ページ）
- 仮想コンテンツ セキュリティ管理アプライアンスの製品 ID コード（PID）（12 ページ）

Cisco 仮想 Web セキュリティ アプライアンスの製品 ID コード（PID）

機能	PID	説明
Web Security Essentials	WSA-WSE-LIC=	内容： • Web Usage Controls • Web レピュテーション
Web Security Premium	WSA-WSP-LIC=	内容： • Web Usage Controls • Web レピュテーション • Sophos および Webroot Anti-Malware シグネチャ
Web Security Anti-Malware	WSA-WSM-LIC=	Sophos および Webroot Anti-Malware シグネチャが含まれます。
McAfee Anti-Malware	WSA-AMM-LIC=	—
高度なマルウェア防御	WSA-AMP-LIC=	—

仮想コンテンツ セキュリティ管理アプライアンスの製品 ID コード（PID）

機能	PID	説明
すべての中央集中型 Web セキュリティ機能	SMA-WMGT-LIC=	—
すべての中央集中型電子メール セキュリティ機能	SMA-EMGT-LIC=	

Cisco TAC

Cisco TAC の連絡先情報（電話番号を含む）：
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html [英語]

その他の情報

サポート オプションに関する情報などの詳細については、ご使用の AsyncOS リリースのリリース ノートとユーザ ガイドまたはオンライン ヘルプを参照してください。

Cisco Content Security 製品のマニュアル：	入手場所
コンテンツ セキュリティ管理アプライアンスs	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web セキュリティ アプライアンスs	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html