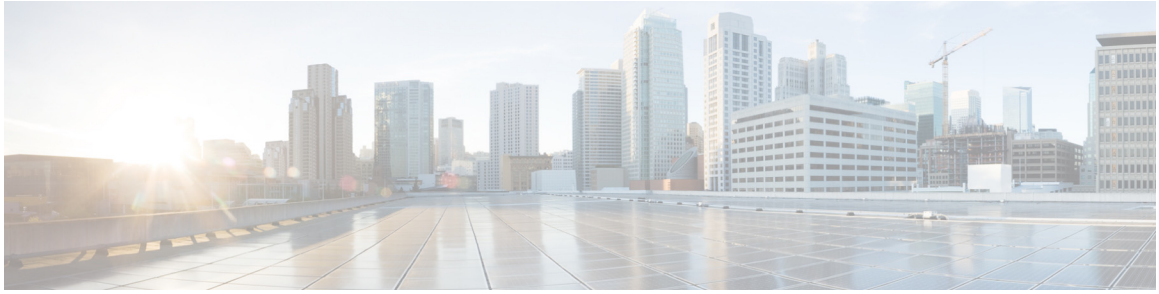

Amazon Web Services の Amazon Elastic Compute Cloud に Cisco Secure Email ゲートウェイ、Secure Web、および Cisco Secure Email and Web Manager 仮想アプライアンスを展開する

公開日:2022 年 7 月 11 日

改訂日:2023 年 2 月 24 日

Cisco Systems, Inc.
www.cisco.com

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機能は、「仮想アプライアンスの管理（13 ページ）」に記載されたわずかな違いのみで、物理的な Cisco Secure Email Gateway（以前の E メール セキュリティ アプライアンス（ESA））、Cisco Secure Web Appliance（以前の Cisco Web セキュリティ アプライアンス（WSA））および Cisco Secure Email and Web Manager（以前のセキュリティ管理アプライアンス（SMA））と同様に機能します。

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） AWS EC2 では、Cisco Secure Email Gateway、Secure Web、および Cisco Secure Email and Web Manager 仮想アプライアンスがサポートされています。

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。Cisco Secure Web Appliance および Cisco Secure Email and Web Manager 向け AMI は、AWS マーケットプレイスで入手できます。Cisco Secure Email Gateway は AWS マーケットプレイスでは入手できません。AMI イメージをプロビジョニングするには、AWS アカウントの詳細（ユーザー名とリージョン）をシスコの営業担当者にお問い合わせください。

必要な AMI を選択し、導入処理を進めます。

Cisco Secure Email Gateway、Secure Web、および Cisco Secure Email and Web Manager 仮想アプライアンス AMI

次の表に、Cisco Secure Email Gateway、Secure Web、および Cisco Secure Email and Web Manager 仮想アプライアンスの AMI の詳細を示します。

Cisco Secure Email Gateway 仮想アプライアンス（AsyncOS 14.0.0-692）

Cisco Secure Email Gateway 仮想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 14.0.0-692	C100V	Cisco Secure Email 仮想ゲートウェイ - 14-0-0-692-C100V-200421.ami
	C300V	Cisco Secure Email 仮想ゲートウェイ - 14-0-0-692-C300V-200421.ami
	C600V	Cisco Secure Email 仮想ゲートウェイ - 14-0-0-692-C600V-200421.ami

Cisco Secure Email and Web Manager 仮想アプライアンス（AsyncOS 14.0.0-404）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-14-0-0-404-M600V を入力します。

Cisco Secure Email and Web Manager 仮想アプライアンス（AsyncOS 14.0.0-404）	AMI ID
M600V	zeus-14-0-0-404-M600V-AMI-230421
M300V	zeus-14-0-0-404-M300V-AMI-230421
M100V	現在、画像は使用できません。

ライセンシング

Amazon AWS での展開では、既存の Cisco Secure Email Gateway、Secure Web、または Cisco Secure Email and Web Manager 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）
- オンプレミスの Cisco Secure Email Gateway アプライアンスは、AWS での Cisco Secure Email and Web Manager アプライアンスの展開ではサポートされていません。

Cisco Secure Email Gateway、Secure Web、または Cisco Secure Email and Web Manager 仮想アプライアンスを展開するには、次の手順を実行します。

	操作内容	詳細
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（5 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。 （注） Cisco Secure Email Gateway は AWS マーケットプレイスでは入手できません。AMI イメージをプロビジョニングするには、AWS アカウントの詳細（ユーザー名とリージョン）をシスコの営業担当者にお問い合わせください。	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（6 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（9 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（10 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（10 ページ）。
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（11 ページ）。

	操作内容	詳細
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（11 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（12 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（12 ページ）。

環境の準備

AWS EC2 での Cisco Secure Email Gateway、Secure Web、または Cisco Secure Email and Web Manager 仮想アプライアンスの展開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。次のようなものがあります。

- Cisco Secure Email Gateway、Secure Web、または Cisco Secure Email and Web Manager 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ー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ー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、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. [インスタンスを起動（Launch Instance）] をクリックし ドロップダウンリストで [インスタンスを起動（Launch Instance）] を選択します。
3. [AWS マーケットプレイス（AWS Marketplace）] をクリックします。

（注） Cisco Secure Email Gateway は AWS マーケットプレイスでは入手できません。AMI イメージをプロビジョニングするには、AWS アカウントの詳細（ユーザー名とリージョン）をシスコの営業担当者にお問い合わせください。

4. 仮想アプライアンス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、Secure Web 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 Secure Email Gateway 仮想アプライアンス	AsyncOS 14.0 以降（電子メール）	**C100V**	c4.xlarge	4	7.5 GB	1 (*)	200 GB
		C300V	c4.2xlarge	8	15 GB	1 (*)	500 GB
		C600V	c4.4xlarge	16	30 GB	1 (*)	500 GB

(*) デフォルトでは単一の NIC が表示されますが、ユーザーはインスタンスを開始するときに追加のインターフェイスを作成できます。

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 Secure Web 仮想アプライアンス	AsyncOS 14.5 以降（Web）	**S100V**	c5.xlarge	4	8 GB	2	200 GB
		S300V	c5.2xlarge	8	16 GB	3	500 GB
		S600V	c5.4xlarge	16	32 GB	3	750 GB
	AsyncOS 14.0 以降（Web）	**S100V**	m4.large	2	8 GB	2	200 GB
		S300V	c4.xlarge	4	7.5 GB	3	500 GB
		S600V	c4.4xlarge	16	30 GB	3	750 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 Secure Email and Web Manager 仮想アプライアンス	AsyncOS 14.0 以降	**M100V**	現在、画像は使用できません。	-	-	-
		M300V	c4.xlarge	4	7.5 GB	1024 GB
		M600V	c4.2xlarge	8	15 GB	2032 GB

（注）

- 7.5 GB vRAM で C100V と 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。
- Secure Web 仮想アプライアンスで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。

Coeus 14.5 の AWS での Secure Web Appliance（SWA）の導入

AsyncOS 14.5 の展開を正常に完了するには、次の手順を実行します。

ステップ 1 次の表に示すように、対応する **C4** インスタンスタイプで AMI を展開します。

モデル	インスタンス タイプ
S100V	m4.large
S300V	c4.xlarge
S600V	c4.4xlarge

ステップ 2 インスタンスがアクティブになったら、**SSH** と管理者のログイン情報を使用してインスタンスに接続し、その到達可能性を確認します。

ステップ 3 Secure Web Appliance CLI を使用してインスタンスをシャットダウンし、AWS CLI を使用してインスタンスを確認します。

ステップ 4 インスタンスを更新するには、アクセスキー ID とシークレットアクセスキーを使用して AWS CLI を接続します。

ステップ 5 EC2 インスタンスで ENA がすでに有効になっているかどうかを確認するには、インスタンス ID とリージョンを指定して次のコマンドを実行します。

```
aws ec2 describe-instances --instance-id <your-instance-id> --query
"Reservations[].Instances[].EnaSupport" --region <your-region>
```

- ENA が正常に有効化されると、ステータスが「**True**」として返されます。ステップ 7 に進みます。
- ENA が有効になっていない場合、空の文字列が返されます。次のステップに進みます。

ステップ 6 EC2 インスタンスで ENA を有効にするには、次のコマンドを実行します。

```
aws ec2 modify-instance-attribute --instance-id <your-instance-id> --ena-support --region
<your-region>
```

（注） このコマンドは出力を返しません。ステップ 5 に進みます。

ステップ 7 次の表に示すように、インスタンスタイプを **C4** から **C5** に変更します。

モデル	インスタンス タイプ
S100V	c5.xlarge
S300V	c5.2xlarge
S600V	c5.4xlarge

ステップ 8 インスタンスを開始します。

（注） coeus 14.0 から coeus 14.5 への AWS インスタンスのアップグレードはサポートされていません。coeus 14.5 で新しいインスタンスを展開することをお勧めします。

coeus-14-0 で実行している AWS インスタンスがあり、互換性のある設定を作成して、新しく展開された coeus 14.5 インスタンスをロードする場合は、coeus-14-0 インスタンスを coeus 14.5 にアップグレードします。その後、設定をダウンロードします。詳細については、『Cisco Secure Web Appliance User Guide』の「Save, Loading, and Resetting the Appliance Configuration」トピックを参照してください（互換性のある coeus 14.5 の設定を取得する場合にのみ推奨）。

新しく展開された coeus 14.5 インスタンスに互換性のある設定をロードする手順については、『Cisco Secure Web Appliance User Guide』の「Loading the Appliance Configuration File」トピックを参照してください。

詳細については、次を参照してください。

- AWS CLI のインストールとセットアップについては、https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html [英語] を参照してください。
- AWS CLI を使用するためのセットアップと前提条件の設定については、https://docs.aws.amazon.com/cli/latest/userguide/getting-started-prereqs.html [英語] を参照してください。

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. [ネットワーク（Network）] ドロップダウンリストで適切な VPC を選択します。
3. [サブネット（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. [パブリック IP の自動割り当て（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。
   - [サブネット設定の使用（有効化）（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、[無効化（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. [シャットダウン動作（Shutdown behavior）] を選択します。ここでは [停止（Stop）] を選択することをお勧めします。

注意 [終了（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）[不慮の終了からの保護（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、[モニタリング（Monitoring）]、[EBS 最適化インスタンス（EBS-optimized instance）]、および [テナント（Tenancy）] などその他のオプションを確認し、選択します。
9. [ネットワークインターフェイス（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、[デバイスの追加（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 [ネットワークインターフェイス（Network Interface）] 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（6 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（12 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 [セキュリティグループ（Security Group）] を選択します。
2. [確認して起動する（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. [起動（Launch）] をクリックしてインスタンスを起動します。
7. [インスタンス（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スを EC2 の [インスタンス（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、[ステータスチェック（Status Checks）] 列の下に緑のチェック マークと [2/2 チェック合格（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. [インスタンス（Instances）] ページで、インスタンスを選択します。
   b. [アクション（Actions）] をクリックします。
   c. [インスタンス設定（Instance Settings）] の [システムログの取得（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

（注） Cisco Secure Web Appliance では、デフォルトの「admin」ユーザーの SSH アクセスは、キーベースの認証でのみ機能します。パスワードベースの認証は、`userconfig` CLI コマンドおよびアプリケーション GUI の [システム管理（System Administration）] > [ユーザー（User）] を使用して設定されたユーザーが使用できます。

1. EC2 ナビゲーション パネルで [インスタンス（Instances）] をクリックします。
2. インスタンスを選択して、[接続（Connect）] をクリックします。
3. [インスタンスへの接続（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ー名は `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 C100V および 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 Secure Web 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ー名とパスワードは、それぞれ `admin` と `ironport` です。

次の表に、仮想アプライアンスのデフォルトポートを一覧表示します。

製品	HTTP ポート（HTTP Port）	HTTPS ポート（HTTPS Port）
Cisco Secure Web Appliance	8080	8443
Cisco Secure Email Gateway	80	443
Cisco Secure Email and Web Manager	80	443

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（17 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. [新規アドレスの割り当て（Allocate New Address）] をクリックします。
3. [割り当て（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、[閉じる（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. [アドレス（Actions）] をクリックし、[アドレスの関連付け（Associate address）] を選択します。
6. [リソースの種類（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. [関連付け（Associate）] をクリックします。
10. [閉じる（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（17 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 リリースのユーザー 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 Secure Email Gateway および Cisco Secure Web 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 SMTP プロキシ（Cisco Secure Email Gateway）、Web プロキシ（Cisco Secure Web Appliance）として機能するか、または隔離済みメッセージを自動的に処理します（Cisco Secure Email and Web Manager）。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ーが隔離を管理することはできませんが、管理アプライアンスは引き続き管理対象 Cisco Secure Email Gateway 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ー 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 Secure Email Gateway、Secure Web または Secure Web or Cisco Secure Email and Web Manager 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 Cisco Secure Email Gateway でサポートされている	仮想 Cisco Secure Web Appliance でサポートされているか？	仮想 Cisco Secure Email and Web Manager でサポートされているか？	情報
`loadlicense`	対応	対応	対応	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`	対応	対応	—	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`	対応	対応	—	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`	対応	対応	—	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`	対応	対応	—	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ー 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`	対応	対応	—	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 Secure Web Appliance でのみ使用可能です。

`diagnostic`	対応	対応	—	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. Monitor tasks in progress`
				`3. Display disk verify verdict`
				このコマンドは、Cisco Secure Web Appliance でのみ使用可能です。

`showlicense`	対応	対応	対応	ライセンスの詳細を表示します。 仮想 Cisco Secure Web Appliance 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 Secure Email Gateway 仮想アプライアンスの製品 ID コード（PID）（15 ページ）
- Cisco Secure Web 仮想プライアンスの製品 ID コード（PID）（16 ページ）

Cisco Secure Email Gateway 仮想アプライアンスの製品 ID コード（PID）

機能	PID	説明
Cisco Secure Email	CSEMAIL-SEC-SUB	オンプレミス、クラウド、またはハイブリッドに導入できる Cisco Secure Email ソフトウェア サブスクリプション ライセンス。 この最小在庫管理単位（SKU）では、前払いオプションおよび年次請求オプションのみを使用できます。
Essential		内容： • スパム対策フィルタリング • アウトブレイク フィルタリング • Sophos Anti-Virus フィルタリング • Cisco Secure Email マルウェア防御：レピュテーションと Cisco Threat Grid サンドボックス分析機能を含む

機能	PID	説明
メリット		内容: • すべての Essential 機能 • Cisco Secure Email Encryption Service • シスコのデータ損失防止(DLP)
Premier		内容: • すべての Advantage 機能 • Cisco Secure Awareness トレーニング
アドオン:インテリジェンス マルチスキャン		複数のスパム対策分類子の結果を、インバウンドバンドルおよびプレミアムバンドルの Cisco IPAS 分類子と組み合わせることで、追加のスパム対策分類機能を提供します。スパム検出率は向上しますが、誤検出が増える可能性があります。
アドオン:グレイメールの安全な登録解除		正規のマーケティング電子メールを受信したユーザーは、サードパーティを介して安全に登録解除できます。
アドオン:McAfee Anti-Malware		インバウンドバンドルとプレミアムバンドルに付属する Sophos Anti-Virus エンジンのアドオンとして、追加のウイルス対策保護を提供します。
アドオン:イメージアナライザ		電子メールに含まれる画像のアダルトコンテンツのスキャンを提供します。多くの場合、DLP とともに導入され、許容可能なユーザーポリシーを実装します。
中央集中型電子メール管理	SMA-EMGT-LIC	すべての中央集中型 Cisco Secure Email 機能。

Cisco Secure Web 仮想プライアンスの製品 ID コード(PID)

機能	PID	説明
Cisco Secure Web	WEB-SEC-SUB	Cisco Web セキュリティ統合 SKU
Web Security Essentials	WSA-WSE-LIC	内容: • Web Usage Controls • Web レピュテーション

機能	PID	説明
Web Security Advantage	WSA-WSP-LIC	内容: • Essentials 機能 • Sophos および Webroot Anti-Malware シグネチャ
Web セキュリティプレミア	WSA-WSS-LIC	内容: • Advantage 機能 • Cisco Advanced Malware Protection • Cisco Cognitive Threat Analytics • Cisco Threat Grid
McAfee Anti-Malware	WSA-AMM-LIC	—
高度なマルウェア防御	WSA-AMP-LIC	—
SMA 中央集中型 Web 管理	SMA-WMGT-LIC	すべての中央集中型 Secure Web 機能。
SMAアドオン:高度なレポート - 上位データ層	SMA-WSPL-HIGH-LIC	—
SMAアドオン:高度なレポート - 下位データ層	SMA-WSPL-LOW-LIC	—

Cisco TAC

Cisco TAC の連絡先情報(電話番号を含む):
https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

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
Cisco Secure Email and Web Manager	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Cisco Secure Web Appliance	https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html
Cisco Secure Email Gateway	https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html

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。