# Cisco Content Security 仮想アプライアンス インストレーション ガイド

**最終更新日：2015 年 6 月 3 日**

# 目次



# Cisco Content Security 仮想アプライアンスについて

Cisco Content Security 仮想アプライアンスは、「Cisco Content Security 仮想アプライアンスの管理」（P.9）に記載されているわずかな変更を除き、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。

## Cisco Content Security 仮想アプライアンス モデル

Cisco Content Security 仮想アプライアンス モデルは、対応する物理ハードウェア アプライアンスの場合と同じようなディスク レイアウト、キューとキャッシュ サイズ、および設定になっています。仮想アプライアンスには、次の表の値が事前設定されています。


Cisco Systems, Inc.
www.cisco.com

| 仮想アプライアンス | ディスク領域 | メモリ | プロセッサ コア数 |
|---|---|---|---|
| **C000V**<br>（評価およびデモのみに使用） | 200 GB | 4 GB | 1 |
| **C100V** | 200 GB | 6 GB | 2 |
| **C300V** | 500 GB | 8 GB | 4 |
| **C600V** | 500 GB | 8 GB | 8 |
| **S000V** | 250 GB | 4 GB | 1 |
| **S100V** | 250 GB | 6 GB | 2 |
| **S300V** | 1024 GB | 8 GB | 4 |

# サポートされる AsyncOS のリリース

| 製品 | 仮想アプライアンスで実行されるリリース |
|---|---|
| Cisco Web セキュリティ | AsyncOS 7.7.5 以降 |
| Cisco E メール セキュリティ | AsyncOS 8.0 以降 |

Cisco Content Security Management Appliance と AsyncOS バージョンの互換性については、http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html [英語] から入手可能な互換性マトリクスで詳しく説明されています。

# システム要件

## ハードウェアと仮想化ハイパーバイザ

Cisco UCS サーバ（ブレードまたはラックマウント）が、仮想アプライアンス用にサポートされている唯一のハードウェア プラットフォームです。

サポートされている仮想化ハイパーバイザは、以下の VMware ESXi のバージョンのみです。

| AsyncOS バージョン | サポートされる VMware ESXi バージョン |
|---|---|
| AsyncOS 8.5.x（Email）<br>AsyncOS 8.0.x（Web） | 4.x、5.0、および 5.1 |
| AsyncOS 8.0（Email）<br>AsyncOS 7.7.5（Web） | 4.x および 5.0 |

他のハードウェア プラットフォームや VMware ハイパーバイザについては「ベスト エフォート」ベースでサポートされます。つまり、当社で支援を試みますが、一部の問題を再現できない、または解決策を保証できない場合があります。他の仮想化ハイパーバイザはサポートされません。

ご使用の仮想アプライアンスをホスティングするサーバの最小要件は以下のとおりです。

- 2 つの 64 ビット x86 プロセッサ（それぞれ 1.5 GHz 以上）
- 8 GB の物理 RAM
- 10k の RPM SAS ハード ドライブ ディスク

## FlexPod ソリューションでの導入

AsyncOS for Email リリース 8.5 以降の場合：

FlexPod ソリューションの一部としての仮想 電子メール セキュリティ アプライアンス の導入の詳細については、http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/white-paper-c11-731731.pdf [英語] を参照してください。CCO ログインにより、このマニュアルにアクセスできるかどうかが決まります。

FlexPod の全般的な情報については、http://www.cisco.com/en/US/netsol/ns1137/index.html [英語] を参照してください。

## VMware ESXi 4.x ファイル システム設定

VMware ESXi バージョン 4.x には、最大 1 TB の仮想ディスク イメージをサポートする 4 MB のデフォルト ブロックサイズがあるファイル システムが付属しています。ただし、より大きいシスコ仮想セキュリティ アプライアンス（例：S300V、C600V）では、1 TB 以上のディスク領域が必要です。これらのモデルを実行するには、新しいデータストアを作成し、8 MB 以上のブロック サイズでフォーマットする必要があります。

ブロック サイズ情報と新しいデータストアの作成方法の手順については、http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003565 [英語] にある VMware の技術文書を参照してください。

# 管理インターフェイスの IP アドレスと DHCP

仮想アプライアンスに最初に電源を入れると、管理ポートは DHCP ホストから IP アドレスを取得します。仮想アプライアンスが DHCP サーバから IP アドレスを取得できない場合は、管理インターフェイスの IP アドレスとして `192.168.42.42` が使用されます。仮想アプライアンスで System Setup ウィザードを実行すると、CLI によって管理インターフェイスの IP アドレスが表示されます。

# 仮想アプライアンスの設定

| | 操作 | 詳細情報 |
|---|---|---|
| 1. | シスコから仮想アプライアンスのライセンスを取得します。 | 「仮想アプライアンスのライセンス」（P.9）。 |
| 2. | シスコから仮想アプライアンスのイメージと MD5 ハッシュをダウンロードします。 | MD5 ハッシュでアプライアンス イメージのデータ整合性を確認する必要があります。<br>「Cisco Content Security 仮想アプライアンスのイメージのダウンロード」（P.5）。 |
| 3. | （任意）ネットワークで複数の仮想アプライアンスを実行する場合は、イメージのクローンを作成します。 | 「仮想アプライアンスのクローン作成」（P.5）。 |
| 4. | ESX ホストまたはクラスタ上に仮想アプライアンスを配置します。 | 「仮想アプライアンスの導入」（P.5）。 |
| 5. | 断続的な接続の問題を防止します。 | 仮想マシンでの未使用のネットワーク インターフェイス カード（NIC）の無効化。 |
| 6. | Cisco Content Security 仮想アプライアンスでランダム故障を避けるために仮想マシンの同期を設定します。 | 「重要 ランダム故障の防止」（P.6） |
| 7. | DHCP が無効の場合は、ネットワーク上にアプライアンスをセットアップします。 | 「DHCP が無効の場合は、ネットワーク上にアプライアンスをセットアップします。」（P.6） |
| 8. | ライセンス ファイルをインストールします。 | 「仮想アプライアンスのライセンス ファイルをインストールします。」（P.7）。 |
| 9. | アプライアンスの Web UI にログインし、物理アプライアンスの場合と同様にアプライアンス ソフトウェアを設定します。<br>例えば、以下を行うことができます。<br>• System Setup ウィザードの実行<br>• コンフィギュレーション ファイルのアップロード<br>• 手動による機能の設定。<br>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。 | • 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）、オンライン ヘルプまたはご使用の Cisco Content Security アプライアンスのユーザ ガイドを参照してください。<br>• 物理アプライアンスから設定を移行するには、ご使用の E メールまたは Web セキュリティ アプライアンス用の最新の AsyncOS リリースのオンライン ヘルプまたはリリース ノート（ホット パッチのリリース ノートを除く）を参照してください。 |

# Cisco Content Security 仮想アプライアンスのイメージのダウンロード

**はじめる前に**

シスコからご使用の仮想アプライアンスのライセンスを取得します。

**ステップ 1** ご使用の仮想アプライアンスの [Cisco Download Software] ページに移動します。

- E メール セキュリティの場合：
  http://software.cisco.com/download/release.html?mdfid=284900944&flowid=41782&softwareid=282975113&release=8.0.0&relind=AVAILABLE&rellifecycle=GD&reltype=latest [英語]
- Web セキュリティの場合：
  http://software.cisco.com/download/release.html?mdfid=284806698&flowid=41610&softwareid=282975114&release=7.7.5&relind=AVAILABLE&rellifecycle=GD&reltype=latest [英語]

**ステップ 2** ダウンロードする仮想アプライアンス モデル イメージの [Download] をクリックします。

**ステップ 3** ローカル マシンにイメージを保存します。

# 仮想アプライアンスのクローン作成

環境内で複数の仮想セキュリティ アプライアンスを実行する場合は、次の手順に従います。

- シスコは、仮想セキュリティ アプライアンスを初めて実行する前に、そのアプライアンスのクローンを作成することを推奨します。
- 仮想アプライアンスのライセンスが強制的にインストールされた後に仮想セキュリティ アプライアンスのクローンを作成するとライセンスが失効します。ライセンスを再インストールする必要があります。
- クローンを作成する前に仮想アプライアンスをシャット ダウンする必要があります。
- すでに使用されている仮想アプライアンスのクローンを作成する場合は、詳細について、「すでに使用中の仮想アプライアンスのクローン作成」（P.8）を参照してください。

仮想マシンのクローンを作成する手順の詳細については、
http://www.vmware.com/support/ws55/doc/ws_clone.html [英語] にある VMware の技術文書を参照してください。

# 仮想アプライアンスの導入

**はじめる前に**

- 仮想アプライアンスを導入する ESX ホストまたはクラスタを設定します。詳細については、「システム要件」（P.2）を参照してください。
- ローカル マシンに VMware vSphere クライアントをインストールします。
- 「Cisco Content Security 仮想アプライアンスのイメージのダウンロード」（P.5）に示すように、イメージをダウンロードします。

**ステップ 1** 固有のディレクトリで仮想アプライアンスの .zip ファイルを解凍します（例：`C:\vESA\C100V` または：`\ vWSA \ S300V`）。

**ステップ 2** ローカル マシンの VMware vSphere クライアントを開きます。

**ステップ 3** 仮想アプライアンスを配置する ESX ホストまたはクラスタを選択します。

**ステップ 4** [File] > [Deploy OVF Template] を選択します。

**ステップ 5** 作成したディレクトリ内の OVF ファイルへのパスを入力します。

**ステップ 6** [Next] をクリックします。

**ステップ 7** ウィザードを完了します。

# 重要 ランダム故障の防止

Cisco Content Security 仮想アプライアンスでのランダムな故障を回避するために、仮想マシン固有のタイミングの特異性に対処する必要があります。これらの問題を回避するには、仮想マシンで正確なタイムスタンプ カウンタの同期を有効にします。

**はじめる前に**

- 計時の基礎、仮想タイムスタンプ カウンタ、および正確な同期の詳細については、http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf [英語] にある VMWare の『Timekeeping in Virtual Machines PDF』を参照してください。
- ご使用のバージョンの vSphere クライアントの手順は、次の手順とは異なる場合があります。これを汎用ガイドとして使用し、必要に応じてご使用のクライアントのマニュアルを参照してください。

**ステップ 1** vSphere Client で、マシンのリストから仮想アプライアンスを選択します。

**ステップ 2** 仮想アプライアンスの電源を切ります。

**ステップ 3** アプライアンスを右クリックし、[Edit Settings] を選択します。

**ステップ 4** [Options] タブをクリックし、[Advanced] > [General] を選択します。

**ステップ 5** [Configuration Parameters] をクリックします。

**ステップ 6** 次のパラメータを編集または追加します。

```
monitor_control.disable_tsc_offsetting=TRUE
monitor_control.disable_rdtscopt_bt=TRUE
timeTracker.forceMonotonicTTAT=TRUE
```

**ステップ 7** 設定ウィンドウを閉じ、アプライアンスを実行します。

# DHCP が無効の場合は、ネットワーク上にアプライアンスをセットアップします。

**(注)** 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

**ステップ 1** vSphere クライアント コンソールから、`interfaceconfig` を実行します。

**ステップ 2** 仮想アプライアンス管理ポートの IP アドレスを書き留めます。

**(注)** 管理ポートは DHCP サーバから IP アドレスを取得します。アプライアンスが DHCP サーバにアクセスできない場合は、デフォルトで `192.168.42.42` が使用されます。

**ステップ 3** `setgateway` コマンドを使用して、デフォルト ゲートウェイを設定します。

**ステップ 4** 変更を確定します。

# 仮想アプライアンスのライセンス ファイルをインストールします。

**(注)** 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

### はじめる前に

(任意) ライセンス ファイルをアップロードする仮想アプライアンスへの FTP 接続を実行します。端末にライセンスを貼り付ける場合は、この作業を行う必要はありません。

**ステップ 1** 端末アプリケーションの SSH または Telnet を使用して、`admin/ironport` ユーザとしてアプライアンスの CLI にログインします。

**(注)** vSphere クライアント コンソールを使用して CLI にライセンス ファイルの内容を貼り付けることはできません。

**ステップ 2** `loadlicense` コマンドを実行します。

**ステップ 3** 次のいずれかのオプションを使用してライセンス ファイルをインストールします。

- オプション 1 を選択して、端末にライセンス ファイルの内容を貼り付けます。
- すでに FTP を使用してライセンス ファイルをアプライアンスの `configuration` ディレクトリにアップロードした場合は、オプション 2 を選択して、ライセンス ファイルを `configuration` ディレクトリにロードします。

**ステップ 4** ライセンス契約を読み、同意します。

**ステップ 5** (任意) `showlicense` を実行して、ライセンスの詳細を見直します。

### 次の作業

- 管理インターフェイスの IP アドレスの詳細については、「管理インターフェイスの IP アドレスと DHCP」(P.3) を参照してください。
- 残りのセットアップ手順については、「仮想アプライアンスの設定」(P.4) を参照してください。

# 別の物理ホストへの仮想アプライアンスの移行

VMware® VMotion™ を使用して、実行中の仮想アプライアンスを別の物理ホストに移行できます。

要件：

- 両方の物理ホストのネットワーク構成が同じである必要があります。
- 両方の物理ホストに、仮想アプライアンスのインターフェイスがマップされているものと同じ定義済みのネットワークへのアクセス権がなければなりません。
- 両方の物理ホストに、仮想アプライアンスで使用するデータストアへのアクセス権がなければなりません。このデータストアには、ストレージ エリア ネットワーク（SAN）またはネットワーク接続ストレージ（NAS）が有効です。
- 電子メール セキュリティ仮想アプライアンスのキューにはメールを含めません。

VMotion を使用した仮想マシンの移行手順については、VMware の技術文書を参照してください。

# すでに使用中の仮想アプライアンスのクローン作成

**はじめる前に**

- 仮想マシンのクローンを作成する手順の詳細については、http://www.vmware.com/support/ws55/doc/ws_clone.html [英語] にある VMware の技術文書を参照してください。
- ご使用のアプライアンスのネットワーク設定およびセキュリティ機能の管理方法については、ご使用の Cisco Content Security 製品およびリリースのユーザ ガイドを参照してください。

**ステップ 1** 電子メール セキュリティ仮想アプライアンスのクローンを作成する場合：
CLI で `suspend` コマンドを使用してアプライアンスを一時停止し、アプライアンスがキュー内のすべてのメッセージを配信するのに十分な遅延期間を入力します。

**ステップ 2** CLI で `shutdown` コマンドを実行して、仮想アプライアンスをシャット ダウンします。

**ステップ 3** 非初期状態のクローンとして、仮想アプライアンスのクローンを作成します。

**ステップ 4** VMware vSphere Client を使用してクローンを作成したアプライアンスを起動し、次を実行します。

- クローン作成された仮想アプライアンスにライセンス ファイルをインストールします。
- ネットワーク設定を変更します。

  電源投入時に、ネットワーク アダプタは自動的に接続しません。IP アドレス、ホスト名、および IP アドレスを再設定します。次に、ネットワーク アダプタの電源を入れます。
- クローン作成された電子メール セキュリティ仮想アプライアンスの場合：
  - 隔離されたすべてのメッセージを削除します。
  - メッセージ トラッキングおよびレポーティングのデータを削除します。
- クローン作成された Web セキュリティ仮想アプライアンスの場合：
  - プロキシ キャッシュを消去します。
  - CLI で `authcache > flushall` コマンドを使用してプロキシ認証キャッシュを消去します。
  - CLI で `dianostic > reporting > deletedb` コマンドを使用して、レポーティングおよびトラッキングのデータを削除します。

- 認証領域の場合は、ドメインに再参加します。
- 認証の設定の場合は、リダイレクト ホスト名を変更します。
- 元の仮想アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、クローン作成されたアプライアンスをセキュリティ管理アプライアンスに追加します。

**ステップ 5** VMware vSphere クライアントを使用して元の仮想アプライアンスを起動して、動作を再開します。正常に動作していることを確認します。

**ステップ 6** クローン作成されたアプライアンスで動作を再開します。

# Cisco Content Security 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

Cisco Content Security 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。

AsyncOS for Email Security 8.5.x の場合：

- ライセンスの期限が切れた後、このアプライアンスは 180 日間、セキュリティ サービスなしでメールの配信を続行します。この期間中、セキュリティ サービスは更新されません。
- ライセンスの有効期限に関するアラートを受け取るようにアプライアンスを設定するには、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。
- 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。

すべてのリリースの場合：

- 機能キーは仮想アプライアンスのライセンスに含まれています。機能キーは、該当の機能がアクティブ化されてない場合でも、ライセンスと同時に失効します。新しい機能キーを購入する場合は、新しい仮想アプライアンスのライセンス ファイルをダウンロードしてインストールする必要があります。
- 機能キーが仮想アプライアンスのライセンスに含まれるため、AsyncOS 機能の 30 日間評価はありません。

**(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。

**関連項目**

- 「仮想アプライアンスのライセンス ファイルをインストールします。」（P.7）

# 仮想アプライアンスのハードウェア設定の変更

シスコは、IP インターフェイスの削除、アプライアンスの CPU コアや RAM サイズの変更など、Cisco Content Security 仮想アプライアンスのハードウェア設定の変更はサポートしていません。このような変更が行われると、アプライアンスがアラートを送信することがあります。

# 仮想アプライアンスの CLI コマンド

Cisco Content Security 仮想アプライアンスには既存の CLI コマンドに対する更新が含まれ、仮想アプライアンス専用のコマンドである `loadlicense` が含まれます。次の CLI コマンドが変更されています。

| コマンド | 情報 |
|---|---|
| **loadlicense** | 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** | 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** | 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** | 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** | AsyncOS 8.5 for Email Security からは、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** | 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、Web セキュリティ アプライアンスでのみ使用可能です。 |
| **diagnostic** | 次の `diagnostic > raid` のサブメニュー オプションでは、情報は返されません。<br>`1. Run disk verify`<br>`2. Monitor tasks in progress`<br>`3. Display disk verify verdict`<br>このコマンドは、電子メール セキュリティ アプライアンスでのみ使用可能です。 |
| **showlicense** | ライセンスの詳細を表示します。<br>追加の情報は、`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`

# トラブルシューティング

## 断続的な接続の問題

**問題**　断続的な接続の問題。

**ソリューション**　未使用のすべての NIC が ESXi で無効になっていることを確認します。

## ランダム故障

**問題**　原因が明らかでないランダムな故障が発生します。

**ソリューション**　「重要 ランダム故障の防止」（P.6）を参照してください。

# 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 |
|---|---|
| Web セキュリティ アプライアンス | http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html [英語] |
| 電子メール セキュリティ アプライアンス | http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html [英語] |