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 : 2013 年 7 月 3 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

内容

Cisco Systems, Inc.
www.cisco.com

Cisco Content Security 仮想アプライアンスについて

Cisco Web および電子メール セキュリティ アプライアンスはお使いのネットワークでホストできる仮想マシンです。これらの 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.8）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。

このマニュアルでは、Cisco Web および電子メール セキュリティ仮想アプライアンスを扱います。

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 モデルには物理ハードウェア アプライアンス対応物と同様のディスク レイアウト、キューとキャッシュ サイズ、および設定があります。仮想セキュリティ アプライアンスは、次のパラメータであらかじめ設定されています。

仮想アプライアンス	ディスク容量	キュー / キャッシュ領域	メモリ	プロセッサ コア
C000V （評価用のみ）	200 GB	10 GB	4 GB	1
C100V	200 GB	10 GB	6 GB	2
C300V	500 GB	70 GB	8 GB	4
C600V	500 GB	70 GB	8 GB	8
S000V	250 GB	50 GB	4 GB	1
S100V	250 GB	50 GB	6 GB	2
S300V	1024 GB	200 GB	8 GB	4

サポートされた AsyncOS のリリース

仮想セキュリティ アプライアンスでは AsyncOS の次のリリースを実行できます。

- 仮想電子メール セキュリティ アプライアンス: 電子メール セキュリティ用の AsyncOS 8.0
- 仮想 Web セキュリティ アプライアンス: Web セキュリティ用の AsyncOS 7.7.5

セキュリティ管理用の AsyncOS 8.0 以降を実行する Cisco セキュリティ管理アプライアンスを使用して、仮想 Cisco Web セキュリティ アプライアンスの設定を管理できます。

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。**VMware ESXi バージョン 4.x と 5.0** が、サポートされている唯一の仮想化ハイパーバイザです。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「最善努力」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、すべての

問題を再現したり、解決策が保証できないこともあります。他の仮想化ハイパーバイザはサポートされません。

シスコでは、仮想アプライアンスをホスティングするサーバが次の最低要件を満たすことを推奨します。各々 1.5 GHz 以上の 2 台の 64 bit x86 プロセッサ、8 GB の物理 RAM および 10k RPM SAS ハード ドライブ ディスク。

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）では、1 TB 以上のディスク容量が必要です。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 にある VMware 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` を使用します。仮想アプライアンスで System Setup ウィザードを実行すると、CLI は管理インターフェイスの IP アドレスを表示します。

仮想アプライアンスの設定

	アクション	追加情報
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。	このライセンス ファイルには、アプライアンスの実行機能に加えて、仮想アプライアンスのすべての機能キーが含まれます。 「仮想アプライアンスのライセンス ファイル」（P.8）
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。 「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.4）
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.4）
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配置」（P.5）
5.	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！ランダム故障の回避」（P.5）

	アクション	追加情報
6.	（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。	または `loadlicense` コマンドを実行する際に、アプライアンスの CLI にライセンス ファイルをコピーして貼り付けることができます。詳細については、「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.6）を参照してください。
7.	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.6）
8.	Web UI（`http://` < IP アドレス > にログインしてください：`8080`）にログインし、次の処理を実行します。 • システム セットアップ ウィザードの実行 • 仮想アプライアンス用に特に変更した設定ファイルをアップロードします。 • 手動で機能を設定します。	• System Setup ウィザードを実行する詳細については、Cisco Security アプライアンスのユーザ マニュアルの指示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、Cisco Content Security 仮想アプライアンスの設定移行ツールの *リリース ノート*を参照してください。 • 手動で機能を設定するには、オンライン ヘルプまたは AsyncOS のリリースのユーザ マニュアル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

シスコから仮想アプライアンスのライセンスを取得します。

手順

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

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

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 イメージについて [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。

- シスコでは、初めて実行する前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詳細については、「すでに使用中の仮想アプライアンスのクローン作成」（P.7）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 にある VMware 技術文書を参照してください。

仮想アプライアンスの配置

はじめる前に

- 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.4）に示すように、イメージをダウンロードします。

手順

ステップ 1 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で 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！ランダム故障の回避

Cisco Content Security 仮想アプライアンスでランダムでトラブルシューティングが困難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ため、仮想マシンで正確なタイムスタンプ カウンタの同期を可能にします。

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 にある VMWare の『Timekeeping in Virtual Machines』を参照してください。

手順

ステップ 1 vSphere クライアント 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 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 3 [Options] タブをクリックし、[Advanced] > [General] を選択します。

ステップ 4 [Configuration Parameters] をクリックします。

ステップ 5 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 6 設定ウィンドウを閉じ、アプライアンスを実行します。

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する場合は、イメージごとに次の手順を実行する必要があります。

手順

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` を使用します。

ステップ 3 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での 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 4 `loadlicense` コマンドを実行します。

ステップ 5 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 を使ってライセンス 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 6 ライセンス契約を読み、同意します。

ステップ 7 （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。
- 残りの手順については、「仮想アプライアンスの設定」（P.3）を参照してください。

別の物理ホストに仮想アプライアンスを移行します。

シスコでは、他の物理サーバに仮想アプライアンスを移行するため VMware の vMotion の使用をサポートしています。仮想アプライアンスを移行するため、次の要件に従う必要があります。

- 物理ホストは共に、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されたネットワークへのアクセス権がなければなりません。
- 物理ホストは共に、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いけません。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メールがないことを確認します。

仮想アプライアンスはオンライン中に移行できます。

vMotion を使用した仮想マシン移行の詳細については、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 にある VMware 技術文書を参照してください。
- 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、Web 用の Cisco AsyncOS または電子メール用 Cisco AsyncOS のリリースのユーザ マニュアルを参照してください。

手順

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は、CLI で `suspend` コマンドを使ってアプライアンスを停止させ、アプライアンスがキューにあるすべてのメッセージを配信できるように十分な遅延期間を入力します。

ステップ 2 CLI で `shutdown` コマンドを使って、電子メールまたは Web 仮想セキュリティ アプライアンスをシャットダウンします。

ステップ 3 仮想アプライアンスのクローン作成

ステップ 4 VMware vSphere Client を使っ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。

- 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。
- ネットワーク設定を変更します。
- 電子メール セキュリティ仮想アプライアンス：
  - 隔離の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。

- Web セキュリティ仮想アプライアンス：
  - 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 の `dianostic > reporting > deletedb` コマンドで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、セキュリティ管理アプライアンスにクローン作成されたアプライアンスを追加します。

ステップ 5 VMware vSphere クライアントおよび再開処理を使用して元の仮想アプライアンスを起動します。これが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の動作を再開します。

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 ファイル

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。

ライセンス ファイルのインストールの詳細については、「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.6）を参照してください。

機能キーはライセンスに含まれています。機能キーは、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。新しい機能キーの購入の際は、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。

仮想アプライアンスのライセンスに機能キーが含まれるため、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、Web 用の Cisco AsyncOS または電子メール用の　Cisco AsyncOS のユーザ マニュアルにあります。

仮想アプライアンスのハードウェア設定の変更

シスコでは、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のみのコマンド、`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。まず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。
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 オプションで情報は返されません。 1. ディスク検証の実行 2. 実行中のタスクのモニタ 3. ディスク検証結果の表示 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。

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`

詳細情報の入手先

Cisco Content Security 製品の情報源には次が含まれます。

- 「Cisco 通知サービス」（P.10）
- 「マニュアル」（P.10）
- 「Knowledge Base」（P.10）
- 「シスコ サポート コミュニティ」（P.11）

- 「カスタマー サポート」（P.11）
- 「シスコ アカウントの登録」（P.11）
- 「マニュアルに関するフィードバック」（P.11）

Cisco 通知サービス

購読すると、セキュリティ勧告、フィールド通知、販売終了やサポート終了ステートメント、ソフトウェア アップデート、既知の問題に関する情報など、Cisco Content Security アプライアンスに関する通知が配信されます。

受信する情報の頻度やタイプなどのオプションを指定できます。ご使用の製品ごとに購読する必要があります。

購読は、http://www.cisco.com/cisco/support/notifications.html で行えます。

Cisco.com アカウントが必要です。アカウントをお持ちでない場合は、「シスコ アカウントの登録」（P.11）を参照してください。

マニュアル

Cisco Content Security 仮想アプライアンスのドキュメント セットには、次のドキュメントとマニュアルが含まれます（すべてのタイプがすべてのアプライアンスおよびリリースに使用できるとは限りません）。

- 『*Cisco AsyncOS for Web User Guide*』
- 『*Cisco AsyncOS CLI Reference Guide*』
- 『*Cisco AsyncOS for Email User Guide*』
- 上記製品と設定移行ツールのリリース ノート。

このドキュメントおよびその他のドキュメントは、次の場所にあります。

マニュアルの内容 Cisco Content Security 製品	**参照先**
電子メール セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Web セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
コンテンツ セキュリティ管理アプライアンス	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Content Security アプライアンスの CLI リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco IronPort 暗号化	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

Knowledge Base

Cisco Content Security 製品に関する情報に関するナレッジ ベースのアクセス先：

http://www.cisco.com/web/ironport/knowledgebase.html

（注） サイトにアクセスするには Cisco.com のユーザ ID が必要です。Cisco.com ユーザ ID をお持ちでない場合は、「シスコ アカウントの登録」（P.11）を参照してください

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。特定のシスコ製品に関する一般的な問題や、技術情報について話し合う場を提供します。フォーラムにトピックを投稿して、他のユーザに質問したり、情報を共有したりできます。

シスコ サポート コミュニティへのアクセス先：

- 電子メール セキュリティと関連管理：
  https://supportforums.cisco.com/community/netpro/security/email
- Web セキュリティと関連管理：
  https://supportforums.cisco.com/community/netpro/security/web

カスタマー サポート

サポートの入手方法：

海外：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

サポート サイト：http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

シスコ アカウントの登録

Cisco.com の数々のリソースへアクセスするには、シスコ アカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は、https://tools.cisco.com/RPF/register/register.do で登録できます。

関連トピック

- 「Cisco 通知サービス」（P.10）
- 「Knowledge Base」（P.10）

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/