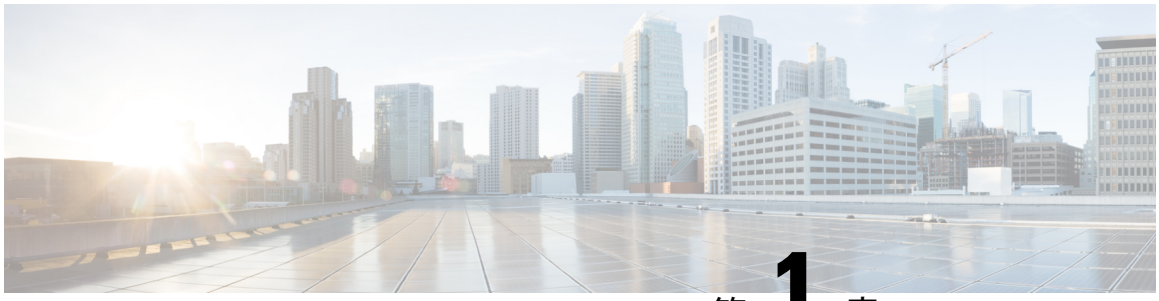
Microsoft Azure Marketplace での Cisco Secure Web Appliance の導入

初版：2022 年 7 月 11 日

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/

目 次



第 1 章

はじめに

Azure Marketplace

Azure イメージを使用して、Azure に仮想マシンインスタンスを作成できます。Secure Web Appliance の Azure イメージは、Azure Marketplace で入手できます。

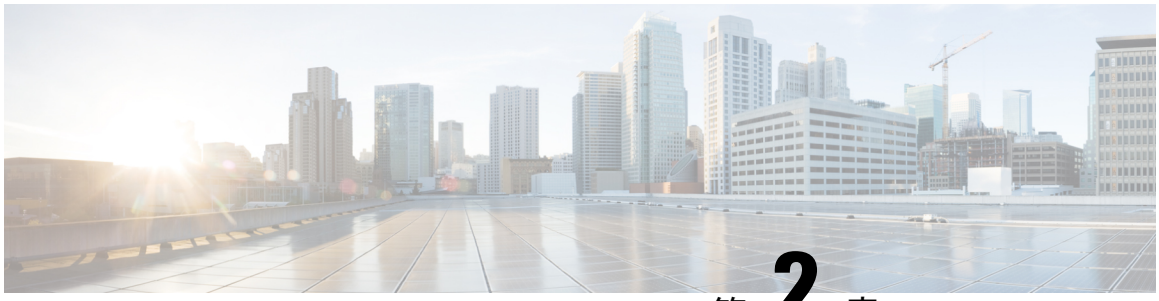
Azure Marketplace は、すべてのソフトウェアニーズに対応する最適な場所であり、エンドツーエンドのソリューションを提供するために Azure で実行できるように認定および最適化されています。

Cisco Secure Web Appliance のライセンス

Microsoft Azure での導入には、既存の Cisco Secure Web Appliance を使用できます。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。Azure インフラストラクチャのみ有料となり、支払が必要になります。

初めてご利用の方は、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。

既存のお客様は、『Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses』の「Obtain a Virtual License（VLN）」を参照してください。



第 2 章

Azure Marketplace での Secure Web Appliance の導入

Azure ユーザーインターフェイスと Azure CLI を使用して、Azure Marketplace に Secure Web Appliance を導入できます。

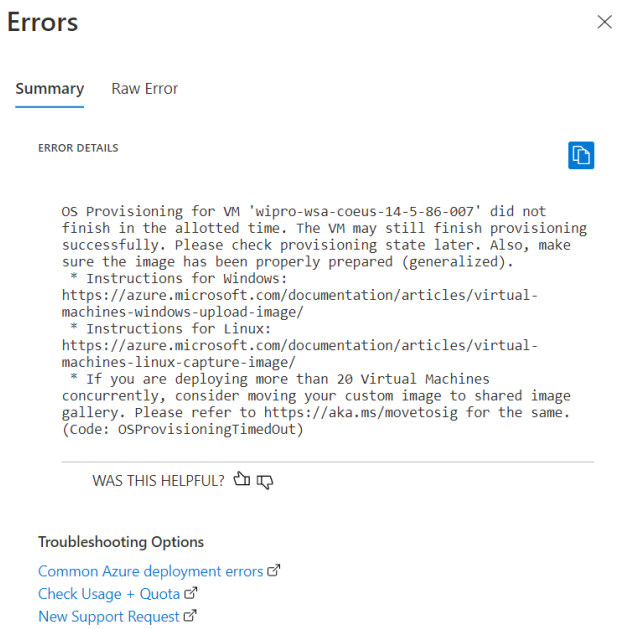
設定の制限

- 次の設定では、Azure Marketplace に Secure Web Appliance を展開することはサポートされていません。
  - レイヤ 4 トラフィックモニタ（Layer-4 Traffic Monitor）
  - Web トラフィックタップ
- Microsoft Azure CLI のみを使用して、Secure Web Virtual Appliance で複数のインターフェイスを作成できます。
- Azure ユーザーインターフェイスから、1 つのインターフェイスのみを使用して Secure Web Appliance インスタンスを設定できます。

その他の情報

- Secure Web Appliance の Azure インスタンスには、インスタンスの正常性ステータスを Azure インフラストラクチャに報告するために必要な WAAgent サポートがありません。Azure は Secure Web Appliance の展開の失敗（タイムアウト）を報告しますが、インスタンスは正常にプロビジョニングされています。[起動診断（Boot diagnostics）] を選択して、仮想マシンの現在のステータスを確認します。

図 *1 : Provisioning Error*



- インバウンドルールは、仮想マシンに着信する特定のトラフィックを許可するか拒否するかを指定するルールの設定です。

  インバウンドルールを変更するには（Cisco Secure Web Appliance へのアクセス）：

  - [仮想マシン（Virtual Machines）] で目的の VM インスタンスを選択します。
  - [Networking] オプションを選択します。

    これで、管理インターフェイスに対してリストされているインバウンドルールを表示できます。

（注） すでに存在する組み込みの3つのセキュリティルールを削除しないでください。

3 つの既定のインバウンドルールは、仮想ネットワーク、ロードバランサなどの Azure 固有のサービスと、許可されたものを除くすべての受信トラフィックを既定でブロックするサービスです。

- Azure でインスタンスを再起動すると、動的に割り当てられたパブリック IP が変更される場合があります。https://www.linkedin.com/pulse/how-remote-desktop-centos-virtual-machine-running-azure-cretuを参照してください
- Azure ユーザーインターフェイスでは、単一のインターフェイスで Cisco Secure Web Appliance の展開がサポートされていますが、Azure CLI を使用して複数のインターフェイスでインスタンスを展開できます。

複数のインターフェイスを持つ Azure インスタンスの展開については、CLI を使用して Azure 環境に Secure Web Appliance を導入する （10 ページ）を参照してください。

Azure ユーザーインターフェイスを使用して Azure Marketplace に Secure Web Appliance を導入する

（注） 仮想マシンの展開は、Azure Marketplace で入手可能なプロビジョニングされたビルドを使用して実行されます。

表 *1* : ユーザーインターフェイスを使用した *Azure* へのデプロイ

	操作手順	詳細情報
ステップ 1	前提条件となるタスクを完了し、Azure 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 （7 ページ）
ステップ 2	Azure Marketplace に進み、目的のビルド用にプロビジョニングされたイメージを選択します。[作成（Create）] をクリックします。	導入でサポートされているインスタンスタイプ （8 ページ）。
ステップ 3	リソースグループ、VM 名、サイズ（RAM と CPU が異なるインスタンスタイプ）を選択します。Azure 環境で、パスワードとして認証タイプを選択し、その他としてライセンスタイプを選択します。	インスタンスの詳細を設定します。 （8 ページ）
ステップ 4	仮想ネットワーク、ディスク、サブネット、およびパブリック IP オプションを設定します。	展開では、すべてのリソースが同じリージョンにある必要があります。

	操作手順	詳細情報
ステップ 5	ネットワーク セキュリティ グループの作成デフォルトのインバウンドルールを使用するか、ルールを追加します。必要に応じて、**ブート診断**を [はい（Yes）] に設定します。 ゲスト設定は、Day 0 を提供するために使用されます。	インスタンスの詳細を設定します。 （8 ページ）
ステップ 6	要件に応じて、名前、グループ、チーム、モデル、目的などのタグを作成します。	インスタンスの詳細を設定します。 （8 ページ）
ステップ 7	変更を確認し、Azure インスタンスを展開します。	Secure Web Appliance の Azure インスタンスには、インスタンスの正常性ステータスを Azure インフラストラクチャに報告するために必要な WAAgent サポートがありません。Azure は Secure Web Appliance の展開の失敗（タイムアウト）を報告しますが、インスタンスは正常にプロビジョニングされています。
ステップ 8	インスタンスの [概要（Overview）] ページに移動し、インスタンスのステータスを確認します。ステータスは、[実行中（Running）] である必要があります。コンソールとブラウザからのログ記録に使用できるパブリック IP を割り当てる必要があります。	
ステップ 9	• CLI、SSH から Azure インスタンスにアクセスします（インバウンドルールが [許可（Allow）] に設定されている場合）。 • **loadlicense** コマンドを使用して、変更を確定します。	• 必要なポートについては、環境の準備 （7 ページ）を参照してください。 • SSH アクセスと Web アクセスについては、起動済みインスタンスの設定（9 ページ）を参照してください。 .

	操作手順	詳細情報
ステップ 10	Cisco Secure Web Appliance 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。	Cisco Secure Web Appliance のユーザーインターフェイスに接続します。 （9 ページ）。
ステップ 11	Cisco Secure Web Appliance にライセンスの期限切れアラートを設定します。	Cisco Secure Web Appliance 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 （10 ページ）。

環境の準備

Secure Web Appliance を展開するには、以下が必要です。

- Secure Web 仮想アプライアンスの有効なライセンス。
- Secure Web Appliance 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。
  - ユーザー名：admin
  - パスワード：IronPort

  デフォルトの認証情報は、後でシステムセットアップ ウィザードの設定で変更できます。
- Azure の展開に必要なリソース：
  - インスタンスが属するリソースグループ。
  - 仮想ネットワークまたはサブネット
  - パブリック IP アドレス（ユーザーインターフェイスを介してインスタンスを作成するときに選択）
  - ネットワーク セキュリティ グループ
  - ネットワーク セキュリティ グループに追加されたインバウンドおよびアウトバウンドルール
  - 開いている仮想アプライアンスが通信するには、次のポートを使用します。
    - SSH 用の SSH TCP 22
    - TCP 8443 UI および NGUI
    - TCP 3128
    - TCP 443

導入でサポートされているインスタンスタイプ

Cisco Secure Web Appliance のモデルに基づいてインスタンスタイプを選択します。

AsyncOS 14.5 以降では、各モデルを展開するための推奨事項は次のとおりです。

表 *2:* 導入でサポートされているインスタンスタイプ

モデル	インターフェイスの最大数	Azure
S100V 3 コア、8GB RAM、ディスク 200GB	2	Standard_F4s_v2 Standard F4s v2 には 4 つの vCPU、8 GiB RAM があります
S300V 5 コア、12GB RAM、ディスク 500GB	4	Standard_F8s_v2 Standard F8s v2 には 8 つの vCPU、16 GiB RAM があります
S600V 12 コア、24GB RAM、ディスク 750GB	4	Standard_F16s_v2 Standard F16s v2 には 16 個の vCPU、32 GiB RAM があります

インスタンスの詳細を設定します。

ステップ 1 リソースグループを選択します。

ステップ 2 VM マネージャ名を入力します。

Azure リソース名には、特殊文字\/""[]:|<>+=;、?*@&、空白、または「_」で始まるか「.」または「-」で終わる文字を含めることはできません。

ステップ 3 [リージョン（Region）] を選択します。

これは、リソースグループに基づいて自動的に取得されます。

ステップ 4 Azure Marketplace から画像を選択します。

ステップ 5 展開するモデルに合わせてサイズを選択します。

たとえば、S300V モデルの展開にはインスタンスタイプ F8_S_V2 が推奨されます。

ステップ 6 パスワードを認証タイプとして選択します。

[ユーザー名（Username）] と [パスワード（Password）] を入力します。

（注） ユーザー名に予約語を含めることはできません。

ただし、展開後は、デフォルトの認証情報を使用して **SSH** にアクセスできます。

- ユーザー名：admin
- パスワード：IronPort

ステップ 7 インバウンドポートには、SSH、HTTPS などがあります。

ネットワーク セキュリティ グループでも同じように変更できます。

ステップ 8 [その他（other）] をライセンスタイプとして選択します。

ステップ 9 ディスクとして SSD または HDD を選択します。

ステップ 10 仮想ネットワークを選択し、仮想ネットワークで設定したサブネットを選択します。

ステップ 11 カスタム ストレージ アカウントで管理設定を有効にします。

ステップ 12 タグを追加し、VM インスタンスを確認して作成します。

起動済みインスタンスの設定

ステップ 1 検索バーで、仮想マシンをフィルタリングします。

ステップ 2 仮想マシンを選択し、VM 名を検索します。

仮想マシンは、取得したパブリック IP アドレスで実行されている必要があります。

ステップ 3 カスタマイズされた DNS 名を設定します。

ステップ 4 必要なポートのセキュリティのために、必要な IP アドレスをインバウンドルールに追加します。

ステップ 5 SSH を使用し、次の認証情報を使用してインスタンスに接続します。

- ユーザー名：admin
- パスワード：IronPort

ステップ 6 必要に応じて、機能キーを追加します。

ステップ 7 **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。

ステップ 8 インターフェイス設定を実行し、ポート 8443 を有効にして、Azure VM の DNS 名を使用してユーザーインターフェイスを使用できるようにします。

ステップ 9 [確定する（Commit）] をクリックします。

Cisco Secure Web Appliance のユーザーインターフェイスに接続します。

アプライアンスのソフトウェアを構成するには、ユーザー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、パブリック IP アドレスが [概要（Overview）] タブに表示されます。デフォルトのクレデンシャルは次のとおりです。

- ユーザー名：admin
- パスワード：IronPort

ステップ 1 Web アクセスの形式 `https://<hostname>:8443`。
ステップ 2 **システム セットアップ ウィザード** を実行します。
ステップ 3 コンフィギュレーション ファイルのアップロード
ステップ 4 機能を手動で構成します。

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。関連情報 （17 ページ） を参照してください。

Cisco Secure Web Appliance 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

詳細については、『AsyncOS ユーザーガイド』の「アラートの管理」トピックを参照してください。

CLI を使用して Azure 環境に Secure Web Appliance を導入する

CLI を使用して、Azure 環境に Secure Web Appliance を導入できます。

さまざまなオペレーティングシステムに Azure CLI をインストールする手順については、https://docs.microsoft.com/en-us/cli/azure/install-azure-cliを参照してください。

または、Azure ユーザーインターフェイスの検索バーの横にクラウドシェルがあります。クラウドシェルを使用して、Azure ユーザーインターフェイスから Azure CLI コマンドを実行できます。

.

ステップ 1 Azure アカウントにログインするには、Azure コンソールで次のコマンドを実行します。

az login -u <username> -p <password>

az account set --subscription <subscription_id>

subscription_id は、ストレージアカウントから取得できます。

ステップ 2 管理インターフェイスの NIC を作成するには、次のコマンドを実行します。

az network nic create --resource-group <Resource_group_name> --name <M1_interface_name> --vnet-name <Virtual_network>--subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

ステップ 3 P1 インターフェイスの NIC を作成するには、次のコマンドを実行します。

az network nic create --resource-group <Resource_group_name> --name <P1_interface_name > --vnet-name <Virtual_network> --subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

ステップ 4 管理インターフェイスのパブリック IP を作成するには、次のコマンドを実行します。

az network public-ip create --resource-group <Resource_group_name> --name <M1-IP>

ステップ 5 データインターフェイスのパブリック IP を作成するには、次のコマンドを実行します。

az network public-ip create --resource-group <Resource_group_name> --name <P1-IP>

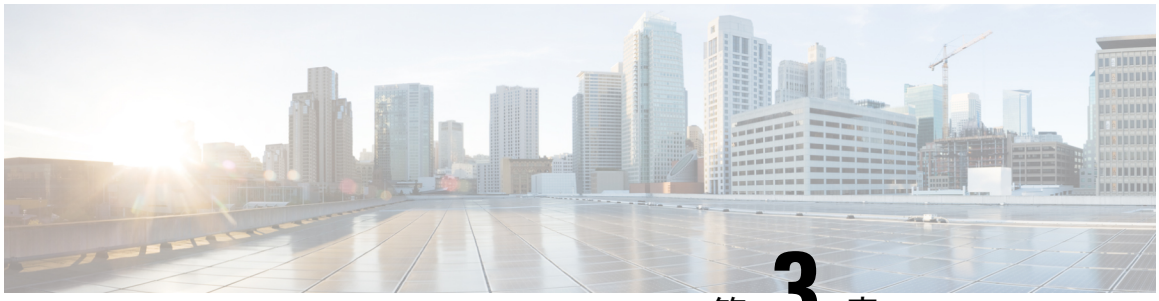
ステップ 6 作成したパブリック IP を対応するインターフェイスに割り当てるには、次のコマンドを実行します。

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <M1_interface_name> --name ipconfig1 --public-ip <M1-IP>

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <P1_interface_name> --name ipconfig1 --public-ip <P1-IP>

ステップ 7 管理インターフェイスとデータインターフェイスを備えた VM を作成するには、次のコマンドを実行します。

az vm create --resource-group <Resource_group_name> --name <VM_Name> --image <Image_name> --size <instance_type> --admin-username rtestuser --admin-password ironport_123 --nics <M1_interface_name > <P1_interface_name >



第 3 章

仮想アプライアンスの管理

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。

表 *3*：仮想アプライアンスの *CLI* コマンド

コマンド	仮想 Cisco Secure Web Appliance でサポートされているか？	情報
loadlicense	有	仮想アプライアンス用のライセンスをインストールすることができます。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	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	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	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を保持します。
revert	対応	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を保持します。

コマンド	仮想 Cisco Secure Web Appliance でサポートされているか？	情報
reload	対応	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。 （注） このコマンドは、Cisco Secure Web Appliance でのみ使用可能です。

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

showlicense	有	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。

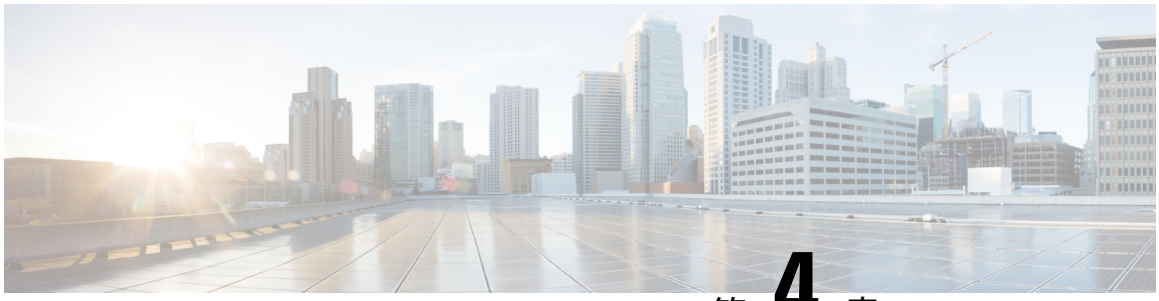
Azure モニタリング

このトピックでは、Secure Web Appliance の Microsoft Azure 監視のサポートを提供します。

表 *4 : Azure* モニタリング

Monitor Type	Secure Web Appliance へのサポート	Comments
Application Insights	×	Secure Web Appliance では [Azureエージェントの更新（Update Azure Agent）] が利用できないため、Application Insights を有効にすることはできません。
Alerts	対応	カスタムアラートとデフォルトアラートの両方を使用できます。

Monitor Type	Secure Web Appliance へのサポート	Comments
ログ	×	Secure Web Appliance では [Azureエージェントの更新（Update Azure Agent）] が利用できないため、Application Insights を有効にすることはできません。
メトリック	対応	—
診断設定	×	Secure Web Appliance の [診断設定（Diagnostic Settings）]を有効にすることはできません。



第 4 章

関連情報

関連情報

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 リリースの関連資料を参照してください。

- セキュア Web アプライアンスのユーザーガイド
- Cisco Secure Web Appliance リリースノート
- Secure Email および Web Manager のユーザーガイド
- Cisco Secure Email および Web Manager リリースノート
- Secure Email Gateway のユーザーガイド
- Cisco Secure Email Gateway リリースノート

Cisco TAC

追加のサポートについては、以下の Cisco TAC にお問い合わせください。

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

Cisco TAC

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。