Microsoft Azure クラウドプットフォームへの Cisco Secure Email Virtual Gateway および Cisco Secure Email and Web Manager Virtual の展開

公開日：2023 年 5 月 4 日

目次

前提条件

展開作業を開始する前に、以下が利用可能であることを確認してください。

- Microsoft Azure アカウントのログイン情報
- Azure ポータル（https://portal.azure.com/）を起動する任意の Web ブラウザ
- Secure Email Virtual Gateway または Secure Email and Web Manager Virtual のイメージ

- ライセンス（クラシックまたはスマートライセンス）
- [オプション] Azure CLI または PowerShell がインストールされた CentOS または Windows システム

推奨される Azure VM サイズ

仮想モデル	Azure VMサイズ	vCPU/コア	メモリ（RAM）	NIC
C600V	Standard D8s v3	8	32	4*
M600V	Standard D8s v3	8	32	4*

（注） *Secure Email Virtual Gateway および Secure Email and Web Manager Virtual は、最大 **3** つのインターフェイスをサポートします。

（注） Secure Email and Web Manager Virtual M600v モデルの Azure 仮想マシン OS ディスクサイズは、Azure Compute Gallery での 1024 GB を超える OS ディスクとのイメージの共有の制限により、2 TB から 1 TB に減少しています。

Azure プラットフォームで Secure Email Gateway または Secure Email and Web Manager のインスタンスを作成する方法

次の手順を順番に実行します。

手順	操作手順	詳細情報
1	必要なコンポーネントを作成します。	コンポーネントの作成（2 ページ）
2	VM イメージを取得します。	Secure Email Virtual Gateway または Secure Email and Web Manager Virtual のイメージの取得（7 ページ）
3	アクセス制御をアイデンティティ・アクセス管理（IAM）で構成します。	アクセス制御（IAM）の構成（8 ページ）
4	ログインして VM を作成します。	ログインと仮想マシンの作成（10 ページ）

コンポーネントの作成

始める前に:
Azure CLI にアクセスできることを確認してください。詳細については、CLI のアクセス（3 ページ）を参照してください。

CLI のアクセス

クライアントシステムに Azure CLI がインストールされていない場合は、Microsoft Azure ポータルにログインします。グローバル検索ツールの横にある**クラウドシェル**オプションを使用できます。

図 1　　グローバル検索ツール

（注）

- 同じ内容をコピーして使用する場合、コマンドに改行（改行文字）は使用しないでください。改行は、読みやすくする目的でのみ使用されています。改行は単一のスペースに置き換えてください。
  たとえば、

```
az group create
    --name cisco-rg
    --location eastus
```

  このコマンドは次のように実行する必要があります。`az group create --name cisco-rg --location eastus`

- 一部のコマンドで使用されている ' 記号は、常に一重引用符（'）であり、逆引用符（`）ではありません。
- 長い URL またはパスをコピーすると、余分な改行や空白スペースが挿入されることがあります。テキストを CLI またはブラウザにコピーするときは、この余分なスペースを削除する必要があります。そうしないと、「引数が無効です（invalid argument）」というエラーが表示される場合があります。

手順:

次の一連の手順を使用してコンポーネントを作成できます。

1. リソースグループの作成
2. ストレージアカウントの作成
3. ネットワーク セキュリティ グループの作成
4. ネットワーク セキュリティ グループのルールの設定
5. 仮想ネットワークとサブネットの作成
6. 単一のネットワーク インターフェイスの作成
7. 複数のネットワーク インターフェイスの設定

（注） 以降の手順（**1** から **7**）の例で示しているコマンドは、Secure Email Gateway インスタンスを 1 つ作成する場合に使用するものです。

（注） シークレット値と Azure イメージパスには有効期限があります。シークレット値と Azure イメージパスの有効期限が切れている場合は、Cisco TAC にお問い合わせください。シークレット値と Azure イメージパスの詳細は、電子メールで送信されます。

1. リソースグループの作成

CLI で次のコマンドを実行します。

```
az group create
     --name <resource group name>
     --location <location name>
```

例:

```
az group create
    --name cisco-rg
    --location eastus
```

2. ストレージアカウントの作成

CLI で次のコマンドを実行します。

```
az storage account create
    --resource-group <resource group name>
    --name <storage account name>
    --location <location id>
    --sku Standard_LRS
    --kind StorageV2
```

例:

```
az storage account create
    --resource-group cisco-rg
    --name ciscosa
    --location eastus
    --sku Standard_LRS
    --kind StorageV2
```

3. ネットワーク セキュリティ グループの作成

（注） Secure Email Gateway または Secure Email and Web Manager Virtual の適切な動作のために開く必要があるポートのリストについては、該当するユーザーガイドの「ファイアウォール情報」の章を参照してください。

CLI で次のコマンドを実行します。

```
az network nsg create
    --resource-group <resource group name>
    --name <security group name>
```

例:

```
az network nsg create
    --resource-group cisco-rg
    --name cisco-nsg
```

4. ネットワーク セキュリティ グループのルールの設定

CLI で次のコマンドを実行します。

```
az network nsg rule create
    --resource-group <resource group name>
    --nsg-name <security group name>
    --name <Rule Name>
    --access <Allow/Deny>
    --protocol <protocol type>
    --direction <Inbound/Outbound>
    --priority <Rule ID>
    --source-address-prefix <source subnet range>
    --source-port-range <port range>
    --destination-port-range <port range>
    --description <description or comments>
```

例：

```
az network nsg rule create
    --resource-group cisco-rg
    --nsg-name cisco-nsg
    --name All_Port_Traffic
    --access Allow
    --protocol "*"
    --direction Inbound
    --priority 110
    --source-address-prefix "*"
    --source-port-range "*"
    --destination-port-range "*"
    --description "Opening traffic on all ports"
```

5. 仮想ネットワークとサブネットの作成

CLI で次のコマンドを実行します。

```
az network vnet create
    -g <resource group name>
    -n <virtual network name>
    --address-prefix <address space>
    --network-security-group <security group name>
az network vnet subnet create
    -g <resource group name>
    -n <virtual network name>
    --address-prefix <address space>
    --subnet-name <subnet name>
    --subnet-prefix <subnet with netmask>
    --network-security-group <security group name>
```

例：

```
az network vnet create
    -g  cisco-rg
    -n cisco-vnet
    --address-prefix 10.1.0.0/16
    --network-security-group cisco-nsg
az network vnet subnet create
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n cisco-mgmt-subnet
    --address-prefixes 10.1.0.0/24
    --network-security-group cisco-nsg
az network vnet subnet create
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n  cisco-data1-subnet
    --address-prefixes 10.1.1.0/24
    --network-security-group cisco-nsg
az network vnet subnet create
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n  cisco-data2-subnet
    --address-prefixes 10.1.2.0/24
    --network-security-group cisco-nsg
```

6. 単一のネットワーク インターフェイスの作成

（注） 要件に基づいて、単一のネットワーク インターフェイス（NIC）または複数の NIC（手順 7. 複数のネットワーク インターフェイスの設定で説明）を作成できます。

CLI で次のコマンドを実行します。

```
az network nic create
    --resource-group <resource group name>
    --name <network interface name>
    --vnet-name <virtual network name>
    --subnet <subnet name>
    --network-security-group <security group name>
```

例：

```
az network nic create
    --resource-group cisco-rg
    --name cisco-mgmt-nic
    --vnet-name cisco-vnet
    --subnet cisco-mgmt-subnet
    --network-security-group cisco-nsg
```

7. 複数のネットワーク インターフェイスの設定

複数の NIC について、異なるインターフェイス名を使用して、単一のネットワーク インターフェイスを作成するために使用したのと同じコマンドを実行できます。

例:

次の例では、3 つの NIC が作成されます。1 つは管理インターフェイスにマッピングされ、他の 2 つのはデータインターフェイスにマッピングされます。

```
az network nic create
    --resource-group cisco-rg
    --name cisco-mgmt-nic
    --vnet-name cisco-vnet
    --subnet cisco-mgmt-subnet
    --network-security-group cisco-nsg
az network nic create
    --resource-group cisco-rg
    --name  cisco-data1-nic
    --vnet-name cisco-vnet
    --subnet  cisco-data1-subnet
    --network-security-group cisco-nsg
az network nic create
    --resource-group cisco-rg
    --name  cisco-data2-nic
    --vnet-name cisco-vnet
    --subnet  cisco-data2-subnet
    --network-security-group cisco-nsg
```

Secure Email Virtual Gateway または Secure Email and Web Manager Virtual のイメージの取得

（注） 長い URL またはパスをコピーすると、余分な改行や空白スペースが挿入されることがあります。テキストを CLI またはブラウザにコピーするときは、この余分なスペースを削除する必要があります。そうしないと、「引数が無効です（invalid argument）」というエラーが表示される場合があります。

手順:

ステップ 1 推奨される Web ブラウザを開き、次の URL にアクセスします。

ステップ 2 URL の形式の例:

```
https://login.microsoftonline.com/<TenantID>/oauth2/authorize?client_id=<ApplicationID>
&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

(注) 中国地域での Azure の展開には、次の形式の URL を使用できます。

```
https://login.chinacloudapi.cn/<Tenant 2
ID>/oauth2/authorize?client_id=<Application (client)
ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

ステップ 3 Azure アカウントのログイン情報を使用してログインします。

ステップ 4 手順 1 で示した URL の `<TenantID>` を Azure テナント ID に置き換えて、リソースグループ内のイメージへのアクセスを取得します。

(注) `<TenantID>` は Azure Active Directory リソースから取得できます。

(注) `<ApplicationID>`(*クライアント ID* とも呼ばれる)はシスコから提供されます。
手順 1 で示した URL でシスコの `<ApplicationID> -3243d803-7fc5-4329-829e-e08c5614c4d2` を使用できます。
サポートが必要な場合は、シスコのテクニカルサポートにお問い合わせください。

`<TenantID>` と `<ApplicationID>` を置き換えた後の URL は次のようになります。

```
https://login.microsoftonline.com/8e1c37c0-b056-432e-81a7-44b1110c95c1/oauth2/authorize
?client_id=3243d803-7fc5-4329-829e-e08c5614c4d2&response_type=code&redirect_uri=https%3
A%2F%2Fwww.microsoft.com%2F
```

アクセス制御(IAM)の構成

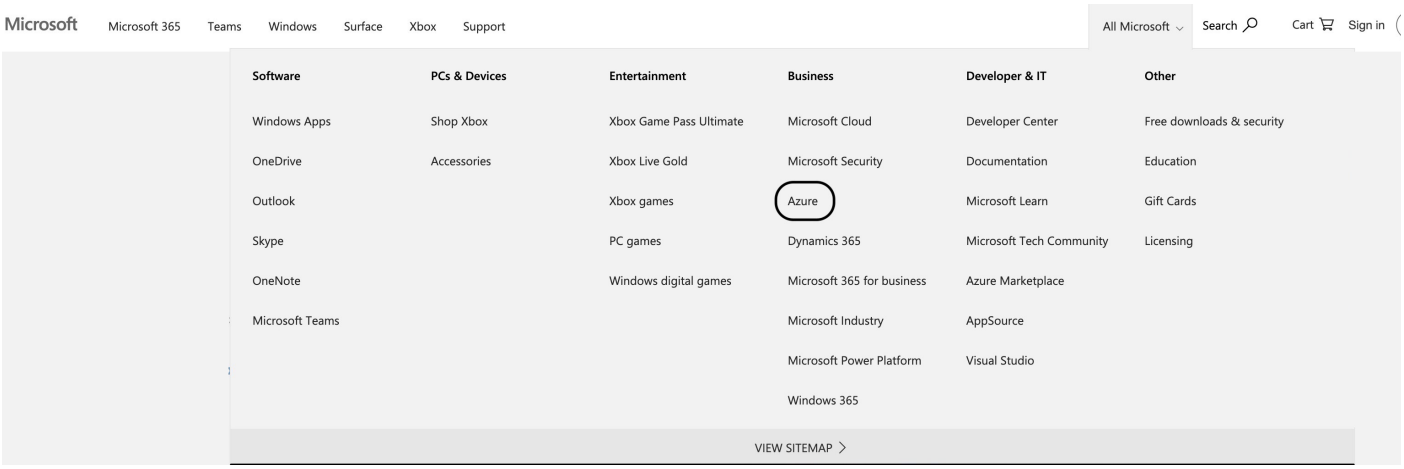
手順:

ステップ 1 Secure Email Virtual Gateway または Secure Email and Web Manager Virtual のイメージの取得 (7 ページ) の手順 1 で示した URL にアクセスするときは、Azure アカウントのログイン情報でログインします。

Microsoft のホームページ(microsoft.com)にリダイレクトされます。

ステップ 2 ページの右上隅にある [すべての Microsoft 製品(All Microsoft)] ドロップダウンリストで [Azure(Azure)] を選択します。

図 2　　Microsoft のホームページ



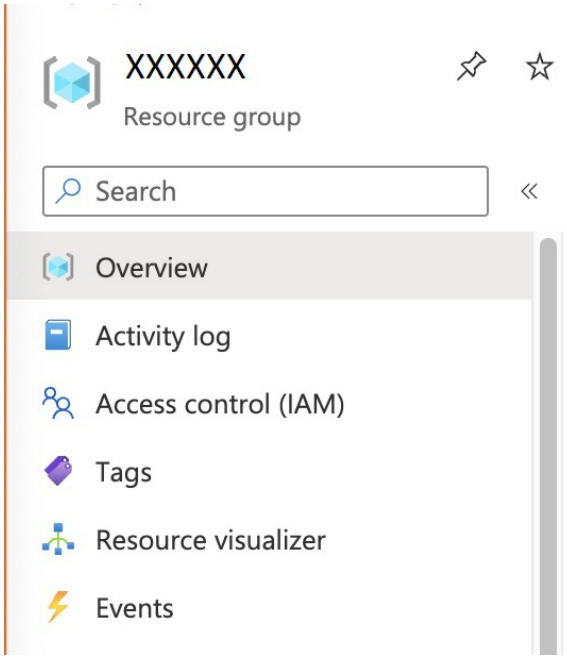
ステップ 3　ページの右上にある [サインイン(Sign In)] オプションをクリックします。

Azure アカウントにログインしているため、Azure ダッシュボードを表示できます。

ステップ 4　共有イメージを追加する必要があるリソースグループを選択します。

ステップ 5　リソースグループで [アクセス制御(IAM)(Access Control (IAM))]を選択します。

図 3　　リソース グループ



ステップ 6　IAM ウィンドウの [このリソースへのアクセス権の付与(Grant access to this resource)] にある [ロールの割り当ての追加(Add role assignment)] を選択します。

新しいウィンドウが開きます。

ステップ 7　[ロール(Role)] で [共同作成者(Contributor)] を選択し、[次へ(Next)] をクリックします。

ステップ 8　アクセス権の割り当て先として [ユーザー、グループ、またはサービスプリンシパル(User, group, or service principal)] を選択します。

ステップ 9 [メンバーの選択(Select Members)] リンクをクリックします。

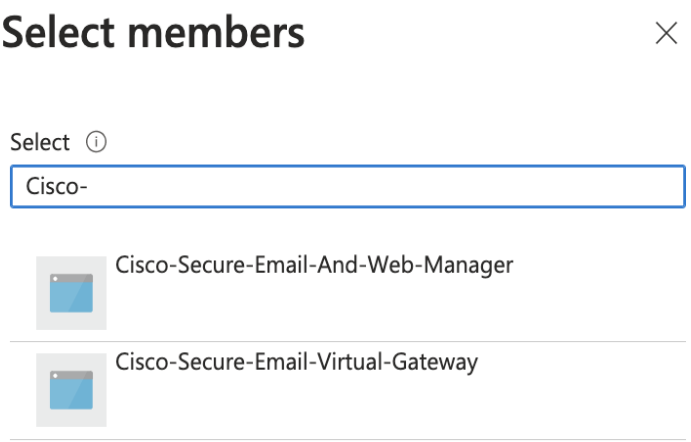
ステップ 10 [Secure Email Gateway ユーザーの場合]:[メンバーの選択(Select Members)] ウィンドウで「**ESA — Cisco-Secure-Email-Virtual-Gateway**」を検索します。

または

[Secure Email and Web Manager ユーザーの場合]:[メンバーの選択(Select Members)] ウィンドウで「**SMA — Cisco-Secure-Email-And-Web-Manager**」を検索します。

ステップ 11 検索結果から、Secure Email Virtual Gateway または Secure Email and Web Manager の必要なバージョンを選択します。

図 4　　[メンバーの選択(Select Members)] ウィンドウ



メンバーを選択すると(たとえば、手順 11 の図の「ESA — Cisco-Secure-Email-Virtual-Gateway」)、そのメンバーがメンバーリストにタイプカテゴリ「アプリ」として表示されます。

ステップ 12 [次へ(Next)] をクリックし、[確認と割り当て(Review + Assign)] をクリックします。

(注) Azure Compute Gallery で共有しているイメージから VM を作成するには、Azure CLI、PowerShell、または CloudShell のいずれかを使用する必要があります。

ログインと仮想マシンの作成

次の手順を順番に実行します。

ステップ 1 CloudShell CLI にログインします。

クライアントシステムに Azure CLI がインストールされていない場合は、Microsoft Azure ポータルにログインします。グローバル検索ツールの横にある**クラウドシェル**オプションを使用できます。

図 5　　グローバル検索ツール

（注）

- 同じ内容をコピーして使用する場合、コマンドに改行（改行文字）は使用しないでください。改行は、読みやすくする目的でのみ使用されています。改行は単一のスペースに置き換えてください。
- 一部のコマンドで使用されている ' 記号は、常に一重引用符（'）であり、逆引用符（`）ではありません。
- 長い URL またはパスをコピーすると、余分な改行や空白スペースが挿入されることがあります。テキストを CLI またはブラウザにコピーするときは、この余分なスペースを削除する必要があります。そうしないと、「引数が無効です（invalid argument）」というエラーが表示される場合があります。

ステップ 2　クラウドシェルで次のコマンドを実行します。

```
az login
    --service-principal
    -u '<Application ID>'
    -p '<Secret Value>'
    --tenant '<Cisco Tenant ID>'
```

（注）　<Application ID>、<Secret Value>、および <Tenant ID> はシスコで共有されます。手順 2 で示すコマンドで使用している <Tenant ID> はシスコのテナント ID です。サポートが必要な場合は、Cisco TAC にお問い合わせください。

例：

```
az login
      --service-principal
      -u '3243d803-7fc5-4329-829e-e08c5614c4d2'
      -p 'qRG8Q~98CjkILX3deMT3X4DGz7rr36uTpIUrOaNv'
      --tenant '18965413-d29e-40cb-a6e7-79aa456932b7'
```

次の応答が得られます。

```
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "18965413-d29e-40cb-a6e7-79aa456932b7",
    "id": "c9554b3f-247f-46b8-b0df-453c91e115ae",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Primary Cisco Account",
    "state": "Enabled",
    "tenantId": "18965413-d29e-40cb-a6e7-79aa456932b7",
    "user": {
      "name": "3243d803-7fc5-4329-829e-e08c5614c4d2",
      "type": "servicePrincipal"
    }
```

```
  }
]
```

ステップ 3 クラウドシェルで `az account get-access-token` コマンドを実行します。

次の応答が得られます。

```
{
  "accessToken": "eyJ0eXAiOiJKV1QiLCJhbqKZi9W8MRfCtw",
  "expiresOn": "2022-08-29 20:23:43.000000",
  "subscription": "c9554b3f-247f-46b8-b0df-453c91e115ae",
  "tenant": "18965413-d29e-40cb-a6e7-79aa456932b7",
  "tokenType": "Bearer"
}
```

（注） アクセストークンには有効期限があります。

ステップ 4 シスコのテナント ID ではなく、独自のテナント ID を使用して **az login** コマンドを再度実行します。

```
az login
    --service-principal
    -u '<Application ID>'
    -p '<Secret Value>'
    --tenant '<Client Tenant ID>'
```

例：

```
az login
      --service-principal
      -u '3243d803-7fc5-4329-829e-e08c5614c4d2'
      -p 'qRG8Q~98CjkILX3deMT3X4DGz7rr36uTpIUrOaNv'
      --tenant '972e674c-3473-4c04-b501-0825a01c25a2'
```

（注） 手順 4 で使用している `<Tenant ID>` は独自のテナント ID です。

手順 2 で示したのと同様の応答が得られます。

ステップ 5 クラウドシェルで `az account get-access-token` コマンドを実行します。

手順 3 で示したのと同様の応答が得られます。

ステップ 6 仮想マシンの作成（13 ページ）で `az vm create` コマンドを実行して仮想マシンを作成します。

仮想マシンの作成

アクセストークン（ログインと仮想マシンの作成（10 ページ）の手順 3 で生成）の有効期限が切れる前に、`az vm create` コマンドを実行する必要があります。次の例で提供されているものと同じユーザー名とパスワードを使用します。

（注） ユーザー名とパスワードを別のログイン情報に置き換えないでください。

```
az vm create
    --resource-group <resourcegroup in which the vm needs to be created>
    --name <vm name>
    --image <this is shared image gallery path that will be shared by cisco>
    --size <VM size>
    --admin-username <username 'admin' cannot be used, so enter a dummy username>
    --admin-password <similarly enter a dummy password>
    --nics <network interfaces using which VM comes up>
    --public-ip-sku Standard
```

例：

```
az vm create
    --resource-group cisco-rg
    --name cisco-01
    --image
    '/subscriptions/c9554b3f-247f-46b8-b0df-453c91e115ae/resourceGroups/cisco-cs-rg/pro
    viders/Microsoft.Compute/galleries/CiscoContentSecurity/images/14.0.2/versions/14.0
    .2'
    --size Standard_D8s_v3
    --admin-username dummy
    --admin-password Dummy@123456
    --nics cisco-mgmt-nic cisco-data1-nic cisco-data2-nic
    --public-ip-sku Standard
```

クラウドシェルでこのコマンドを実行すると、「実行」状態に移行します。新しいインスタンスが指定した VM 名の仮想マシンで作成されていることを確認する必要があります。仮想マシン自体は「実行」状態のままです。

'Microsoft.Network' または 'Microsoft.Compute' について、「*"Resource provider 'Microsoft.Network' used by this operation is not registered. We are registering for you. Registration failed. Please register manually*」のようなエラーメッセージが表示される場合は、サブスクリプションのリソースプロバイダーを Azure ポータルから手動で登録する必要があります。詳細な支援を受ける場合は、シスコの TAC に連絡してください。

（注）

- 仮想インスタンスが正常に作成されても、VM 作成コマンドの実行後にエラーメッセージが表示され、Azure からの展開ステータスが「失敗（Failed）」または「タイムアウト（Timed Out）」とマークされる場合があります。このメッセージは無視できます。この問題は、今後のビルドで解決される予定です。
- 起動診断またはシリアルコンソールを使用して、作成された VM の実際の状態を確認できます。

- 仮想マシンを作成するためにクラウドシェルで実行されるコマンドは自動的に停止しません。VM が正常に起動したら、「Ctrl + C」を押してコマンドを手動でキャンセルする必要があります。
- VM への接続には、デフォルトのユーザー名とパスワード（admin または ironport）が使用されます。ダミーのユーザー名とパスワードは使用されません。
- 第 2 世代のイメージは、Azure プラットフォームに展開した後に起動しません。第 2 世代のイメージを展開した後、仮想マシンを再起動する必要があります。

既知の問題

次の既知の問題のリストは、AsyncOS 15.0 - Secure Email Virtual Gateway および Secure Email and Web Manager Virtual に該当します。

- CSCwe45170：[AZURE] 15.0 Gen2 イメージが D8s_v3 インスタンスサイズと Standard HDD で起動できない。
- CSCwd70737 - Azure：[ESA/SMA] - Azure インスタンスが断続的に起動に失敗する。
- CSCwa52321：[azure] ipcheck コマンドの出力でディスクサイズが「0」と表示される。
- CSCwa52346：[azure] ipcheck コマンドの出力でプラットフォームが「unknown」と表示される。
- CSCwa52452：[azure] gpart show コマンドで想定していない da1 パーティションが出力される。
- CSCwa68102：[インターフェイス（Interface）] ページでホスト名をスパム隔離用に設定しても NAT 環境で [スパム隔離（Spam quarantine）] ページがロードされない。

仮想ゲートウェイのサポートの利用

（注） 仮想ゲートウェイ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 Secure Email Virtual Gateway または Cisco Secure Email and Web Manager Virtual 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。

発注書を参照すると、仮想ゲートウェイ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。

関連資料

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 Secure Email 製品のドキュメント：	参照先
Cisco Secure Email Virtual Gateway	https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html
Cisco Secure Email and Web Manager Virtual	https://www.cisco.com/c/en/us/support/security/content-security-management-virtual-appliance/series.html

サービスとサポート

（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 TAC：https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマーサポートにアクセスすることもできます。手順については、ユーザー ガイドまたはオンライン ヘルプを参照してください。