# Oracle Cloud Infrastructure への ASAv の展開

Oracle Cloud Infrastructure（OCI）に ASAv を導入できます。


- OCI への ASAv の展開について （1 ページ）
- ASAv と OCI の前提条件 （2 ページ）
- ASAv および OCI のガイドラインと制限事項 （3 ページ）
- OCI 上の ASAv のネットワークトポロジの例 （4 ページ）
- OCI への ASAv の導入 （5 ページ）
- OCI 上の ASAv インスタンスへのアクセス （11 ページ）


# OCI への ASAv の展開について

OCI は、オラクルが提供する可用性の高いホスト環境でアプリケーションを実行できるパブリック クラウド コンピューティング サービスです。

ASAv は、物理 ASAv と同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。ASAv は、パブリック OCI で展開できます。その後設定を行うことで、時間の経過とともにロケーションを展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できます。

### OCI のコンピューティングシェイプ

シェイプは、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソースを決定するテンプレートです。ASAv は、次の「標準：汎用」の OCI シェイプタイプをサポートします。

**表 *1:* でサポートされるコンピューティングシェイプ *ASAv***

| OCI シェイプ | 属性 | | インターフェイス |
|---|---|---|---|
| | oCPU | RAM（GB） | |
| VM.DenseIO2.8 | 8 | 120 | 最小 4、最大 8 |
| VM.StandardB1.4 | 4 | 3 | 最小 4、最大 4 |

| OCI シェイプ | 属性 | | インターフェイス |
|---|---|---|---|
| | oCPU | RAM（GB） | |
| VM.StandardB1.8 | 4 | 96 | 最小 4、最大 8 |
| VM.Standard1.4 | 4 | 28 | 最小 4、最大 4 |
| VM.Standard1.8 | 8 | 72 | 最小 4、最大 8 |
| VM.Standard2.4 | 4 | 60 GB | 最小 4、最大 4 |
| VM.Standard2.8 | 8 | 120 GB | 最小 4、最大 8 |
| VM.Standard3.Flex | 4 | 64 | 最小 4、最大 4 |
| | 6 | 96 | 最小 4、最大 6 |
| | 8 | 128 | 最小 4、最大 8 |
| VM.Optimized3.Flex | 4 | 72 | 最小 4、最大 8 |
| | 6 | 84 | 最小 4、最大 12 |
| | 8 | 112 | 最小 4、最大 16 |
| VM.Standard.E4.Flex | 4 | 32 | 最小 4、最大 4 |
| | 6 | 48 | 最小 4、最大 6 |
| | 8 | 64 | 最小 4、最大 8 |

- ASAv には、少なくとも 3 つのインターフェイスが必要です。
- OCI では、1 つの oCPU は 2 つの vCPU に相当します。
- サポートされる vCPU の最大数は 16（8 個の oCPU）です。

ユーザーは、OCI でアカウントを作成し、Oracle Cloud Marketplace の Cisco ASA 仮想ファイアウォール（ASAv）製品を使用してコンピューティング インスタンスを起動し、OCI のシェイプを選択します。

# ASAv と OCI の前提条件

- https://www.oracle.com/cloud/sign-in.html でアカウントを作成します。
- ASAv へのライセンス付与。ASAv にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「Licenses: Smart Software Licensing」を参照してください。

- インターフェイスの要件：
  - 管理インターフェイス
  - 内部および外部インターフェイス
  - （任意）追加のサブネット（DMZ）
- 通信パス：
  - 管理インターフェイス：ASDM に ASAv を接続するために使用され、トラフィックの通過には使用できません。
  - 内部インターフェイス（必須）：内部ホストに ASAv を接続するために使用されます。
  - 外部インターフェイス（必須）：ASAv をパブリック ネットワークに接続するために使用されます。
  - DMZ インターフェイス（任意）：DMZ ネットワークに ASAv を接続するために使用されます。
- ASAv システム要件については、Cisco ASA の互換性 [英語] を参照してください。

# ASAv および OCI のガイドラインと制限事項

### サポートされる機能

OCI 上の ASAv は、次の機能をサポートしています。

- OCI 仮想クラウドネットワーク（VCN）での展開
- インスタンスあたり最大 16 個の vCPU（8 個の oCPU）
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- Single Root I/O Virtualization（SR-IOV）をサポート

### ASAv スマートライセンスのパフォーマンス階層

ASAvは、導入要件に基づいて異なるスループットレベルとVPN接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

| パフォーマンス階層 | インスタンスタイプ（コア/RAM） | レート制限 | RA VPN セッション制限 |
|---|---|---|---|
| ASAv5 | VM.Standard2.4<br>4 コア/60 GB | 100 Mbps | 50 |
| ASAv10 | VM.Standard2.4<br>4 コア/60 GB | 1 Gbps | 250 |
| ASAv30 | VM.Standard2.4<br>4 コア/60 GB | [2 Gbps] | 750 |
| ASAv50 | VM.Standard2.8<br>8 コア/120 GB | 該当なし | 10,000 |
| ASAv100 | VM.Standard2.8<br>8 コア/120 GB | 該当なし | 20,000 |

### サポートされない機能

OCI 上の ASAv は、次の機能をサポートしていません。

- ASAv ネイティブ HA
- トランスペアレント/インライン/パッシブ モード
- マルチ コンテキスト モード
- IPv6

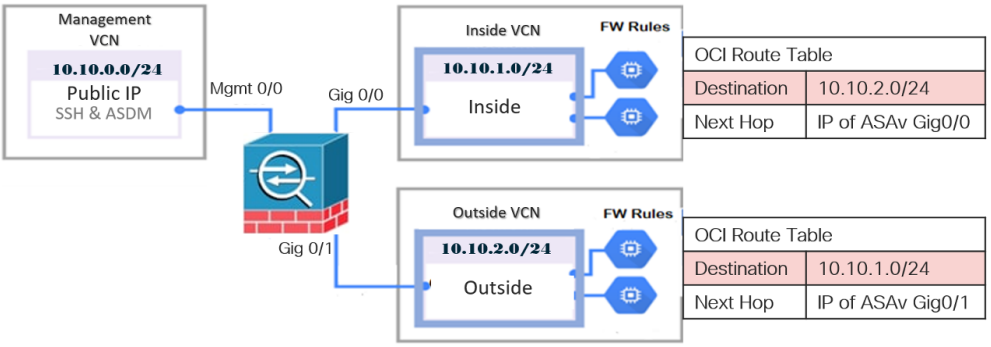
### 制限事項

- OCI に ASAv を展開する場合、Mellanox 5 は SR-IOV モードの vNIC としてサポートされません。
- 静的設定と DHCP 設定の両方で ASAv に必要な個別のルーティングルール。

# OCI 上の ASAv のネットワークトポロジの例

次の図は、ASAv 用の 3 つのサブネット（管理、内部、外部）が OCI 内に設定されているルーテッド ファイアウォール モードの ASAv の推奨ネットワークトポロジを示しています。

図 *1 : OCI* 上の *ASAv* の展開例




# OCI への ASAv の導入

次の手順では、OCI 環境を準備し、ASAv インスタンスを起動する方法について説明します。OCI ポータルにログインし、OCI Marketplace で Cisco ASA 仮想ファイアウォール（ASAv）製品を検索し、コンピューティングインスタンスを起動します。ASAv の起動後に、トラフィックの送信元と接続先に応じて、トラフィックをファイアウォールに転送するようにルートテーブルを設定する必要があります。

## 仮想クラウドネットワーク（VCN）の作成

ASAv 展開用の仮想クラウドネットワーク（VCN）を設定します。少なくとも、ASAv の各インターフェイスに 1 つずつ、合計 3 つの VCN が必要です。

次の手順に進み、管理 VCN を完了できます。次に、[Networking] に戻り、内部インターフェイスおよび外部インターフェイスの VCN を作成します。

### 始める前に

（注） ナビゲーションメニューからサービスを選択すると、左側のメニューにコンパートメントリストが表示されます。コンパートメントはリソースの整理に役立ち、リソースへのアクセスを制御しやすくなります。ルートコンパートメントは、テナントがプロビジョニングされるときに Oracleによって作成されます。管理者は、ルートコンパートメントにさらに多くのコンパートメントを作成し、アクセスルールを追加して、どのユーザーがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracle のドキュメント『コンパートメントの管理（Managing Compartments）』を参照してください。

**ステップ 1** OCI にログインし、地域を選択します。

OCI は互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

**ステップ 2** **[Networking]** > **[Virtual Cloud Networks]** を選択し、[Create Virtual Cloud Networks] をクリックします。

**ステップ 3** [Name] に、VCN のわかりやすい名前を入力します（例：*ASAvManagement*）。

**ステップ 4** VCN の **CIDR ブロック**を入力します。

**ステップ 5** **[VCN の作成（Create VCN）]** をクリックします。

## ネットワーク セキュリティ グループの作成

ネットワーク セキュリティ グループは、一連の vNIC と、vNIC に適用される一連のセキュリティルールで構成されます。

**ステップ 1** **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[ネットワーク セキュリティ グループ（Network Security Groups）]**を選択し、**[ネットワーク セキュリティ グループの作成（Create Network Security Group）]** をクリックします。

**ステップ 2** [Name] に、ネットワーク セキュリティ グループのわかりやすい名前を入力します（例：*ASAv-Mgmt-Allow-22-443* ）。

**ステップ 3** [Next] をクリックします。

**ステップ 4** セキュリティルールを追加します。

a) ASAv コンソールへの SSH アクセスに TCP ポート 22 を許可するルールを追加します。

b) ASDM への HTTPS アクセスに TCP ポート 443 を許可するルールを追加します。

ASAv は ASDM を介して管理できます。管理するには、HTTPS 接続用にポート 443 を開く必要があります。

**ステップ 5** [作成（Create）] をクリックします。

## インターネットゲートウェイの作成

管理サブネットを公的にアクセス可能にするには、インターネットゲートウェイが必要です。

**ステップ 1** **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[インターネットゲートウェイ（Internet Gateways）]**を選択し、**[インターネットゲートウェイの作成（Create Internet Gateway）]** をクリックします。

**ステップ 2** [Name] にインターネットゲートウェイのわかりやすい名前を入力します（例：*ASAv-IG*）。

**ステップ 3** **[インターネットゲートウェイの作成（Create Internet Gateway）** をクリックします。

**ステップ 4** インターネットゲートウェイへのルートを追加します。

a) **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[ルートテーブル（Route Tables）]**を選択します。

b) ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。

c) **[ルートルールの追加（Add Route Rules）]** をクリックします。

d) **[ターゲットタイプ（Target Type）]** ドロップダウンから、**[インターネットゲートウェイ（Internet Gateway）]** を選択します。

e) 宛先の IPv4 CIDR ブロックを入力します（例：0.0.0.0/0）。

f) **[ターゲット インターネット ゲートウェイ（Target Internet Gateway）]** ドロップダウンから、作成したゲートウェイを選択します。

g) **[ルートルールの追加（Add Route Rules）]** をクリックします。

## サブネットの作成

各 VCN には、少なくとも 1 つのサブネットがあります。管理 VCN の管理サブネットを作成します。また、内部 VCN の内部サブネット、および外部 VCN の外部サブネットも必要です。

**ステップ 1** **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[サブネット（Subnets）]**を選択し、**[サブネットの作成（Create Subnet）]** をクリックします。

**ステップ 2** [Name] にサブネットのわかりやすい名前を入力します（例：*Management*）。

**ステップ 3** **[サブネットタイプ（Subnet Type）]** を選択します（推奨されるデフォルトの **[地域（Regional）]** のままにします）。

**ステップ 4** **CIDR ブロック**を入力します（例：10.10.0.0/24）。サブネットの内部（非公開）IP アドレスは、この CIDR ブロックから取得されます。

**ステップ 5** **[ルートテーブル（Route Table）]** ドロップダウンから、以前に作成したルートテーブルのいずれかを選択します。

**ステップ 6** サブネットの **[サブネットアクセス（Subnet Access）]** を選択します。

管理サブネットの場合、これは**パブリックサブネット**である必要があります。

**ステップ 7** **[DHCP オプション（DHCP Option）]** を選択します。

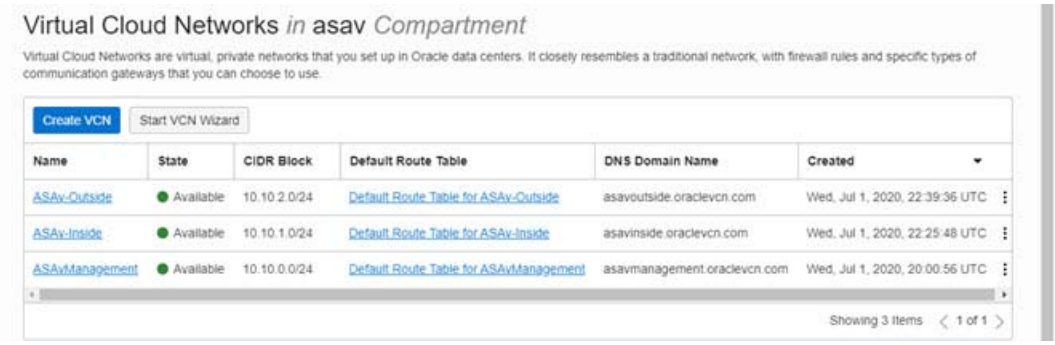
**ステップ 8** 以前作成した **[セキュリティリスト（Security List）]** を選択します。

**ステップ 9** **[サブネットの作成（Create Subnet）]** をクリックします。

### 次のタスク

VCN（管理、内部、外部）を設定すると、ASAv を起動できます。ASAv VCN 構成の例については、次の図を参照してください。

図 *2: ASAv* クラウドネットワーク




# OCI での ASAv インスタンスの作成

Oracle Cloud Marketplace の Cisco ASA 仮想ファイアウォール（ASAv）製品を使用して、コンピューティング インスタンスを介して OCI に ASAv を導入します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[マーケットプレイス（Marketplace）] > [アプリケーション（Applications）]**を選択します。

**ステップ 3** マーケットプレイスで「Cisco ASA virtual firewall (ASAv)」を検索して、製品を選択します。

**ステップ 4** 契約条件を確認し、[Oracle の利用規約とパートナーの契約条件を確認して同意します。（I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.）] チェックボックスをオンにします。

**ステップ 5** [インスタンスの起動（Launch Instance）] をクリックします。

**ステップ 6** [Name] に、インスタンスのわかりやすい名前を入力します（例：*ASAv-9-15*）。

**ステップ 7** [シェイプの変更（Change Shape）] をクリックし、ASAv に必要な oCPU の数、RAM の量、およびインターフェイスの数が指定されたシェイプ（VM.Standard2.4 など）を選択します（表 1 : でサポートされるコンピューティングシェイプ ASAv （1 ページ）を参照）。

**ステップ 8** **[仮想クラウドネットワーク（Virtual Cloud Network）]** ドロップダウンから、[管理 VCN（Management VCN）] を選択します。

**ステップ 9** 自動入力されていない場合は、**[サブネット（Subnet）]** ドロップダウンから [管理サブネット（Management subnet）] を選択します。

**ステップ 10** **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** にチェックを入れ、管理 VCN に設定したセキュリティグループを選択します。

**ステップ 11** **[パブリック IP アドレスの割り当て（Assign a Public Ip Address）]** オプションボタンをクリックします。

**ステップ 12** **[SSH キーの追加（Add SSH keys）]** の下で、**[公開キーの貼り付け（Paste Public Keys）]** オプションボタンをクリックして、SSH キーを貼り付けます。

Linux ベースのインスタンスは、パスワードの代わりに SSH キーペアを使用してリモートユーザーを認証します。キーペアは、秘密キーと公開キーで構成されます。インスタンスを作成するときに、秘密キー

をコンピュータに保持し、公開キーを提供します。ガイドラインについては、『Linuxインスタンスでのキーペアの管理（Managing Key Pairs on Linux Instances）』https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htmを参照してください。

**ステップ 13** **[詳細オプションの表示（Show Advanced Options）]** リンクをクリックして、オプションを展開します。

**ステップ 14** （任意）[スクリプトの初期化（Initialization Script）] の下で、[クラウド初期化スクリプトの貼り付け（Paste Cloud-Init Script）] オプションボタンをクリックして、 ASAv の第 0 日用構成を指定します。第 0 日用構成は、ASAv の起動時に適用されます。

次に、**[クラウド初期化スクリプト（Cloud-Init Script）]** フィールドにコピーして貼り付けることができる day0 構成の例を示します。

ASA コマンドの詳細については、『ASA 構成ガイド』および『ASA コマンドリファレンス』を参照してください。

**重要** この例からテキストをコピーする場合は、サードパーティのテキストエディタまたは検証エンジンでスクリプトを検証して、形式エラーを防止し、無効な Unicode 文字を削除する必要があります。

```
!ASA Version 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

**ステップ 15** [作成（Create）] をクリックします。

### 次のタスク

**[作成（Create）]** ボタンをクリックした後、状態が [プロビジョニング（Provisioning）] として表示される ASAv インスタンスをモニターします。

**重要** ステータスをモニターすることが重要です。ASAv インスタンスの状態が [プロビジョニング（Provisioning）] から [実行中（Running）] に移行したら、ASAv ブートが完了する前に必要に応じて VNIC を接続する必要があります。

# インターフェイスの接続

ASAv は、1 つの VNIC が接続された状態で実行状態になります（**[コンピューティング（Compute）] > [インスタンス（Instances）] > [インスタンスの詳細（Instance Details）] > [接続された VNIC （Attached VNICs）]**を参照）。これはプライマリ VNIC と呼ばれ、管理 VCN にマッピングされます。ASAv が最初の起動を完了する前に、vNIC が ASAv で正しく検出されるように、以前作成した他の VCN サブネット（内部、外部）の vNIC を接続する必要があります。

**ステップ 1** 新しく起動した ASAv インスタンスを選択します。

**ステップ 2** **[接続された VNIC（Attached VNICs）] > [VNIC の作成（Create VNIC）]**の順に選択します。

**ステップ 3** [名前（Name）] に、VNIC のわかりやすい名前を入力します（例：*Inside*）。

**ステップ 4** [仮想クラウドネットワーク（Virtual Cloud Network）] ドロップダウンから VCN を選択します。

**ステップ 5** [サブネット（Subnet）] ドロップダウンからサブネットを選択します。

**ステップ 6** **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** をオンにして、選択した VCN 用に設定したセキュリティグループを選択します。

**ステップ 7** [送信元と宛先のチェックをスキップ（Skip Source Destination Check）] をオンにします。

**ステップ 8** （オプション）[プライベート IP アドレス（Private IP Address）] を指定します。これは、VNIC に対して特定の IP を選択する場合にのみ必要です。

IP を指定しない場合、OCI はサブネットに割り当てられた CIDR ブロックから IP アドレスを割り当てます。

**ステップ 9** [変更の保存 (Save Changes)] をクリックし、VNIC を作成します。

**ステップ 10** 展開で必要となる各 VNIC について、この手順を繰り返します。

# 接続された VNIC のルートルールの追加

内部および外部のルートテーブルにルートテーブルルールを追加します。

**ステップ 1** **[Networking] > [Virtual Cloud Networks]** を選択し、VCN に関連付けられているデフォルトルートテーブル（内部または外部）をクリックします。

**ステップ 2** **[ルートルールの追加（Add Route Rules）]** をクリックします。

**ステップ 3** [ターゲットタイプ（Target Type）] ドロップダウンから、[プライベート IP（Private IP）] を選択します。

**ステップ 4** [宛先タイプ（Destination Type）] ドロップダウンから、[CIDR ブロック（CIDR Block）] を選択します。

**ステップ 5** [宛先のIPv4 CIDRブロック（Destination IPv4 CIDR Block）] に宛先の IPv4 CIDR ブロックを入力します（例：0.0.0.0/0）。

**ステップ 6** [ターゲット選択（Target Selection）] フィールドに VNIC のプライベート IP アドレスを入力します。

VNICにIPアドレスを明示的に割り当てていない場合は、VNICの詳細（**[コンピューティング（Compute）]**> **[インスタンス（Instances）]** > **[インスタンスの詳細（Instance Details）]** > **[接続された VNIC（Attached VNICs）]**）で自動割り当てされた IP アドレスを確認できます。

**ステップ 7** **[ルートルールの追加（Add Route Rules）]** をクリックします。

**ステップ 8** 展開で必要となる各 VNIC について、この手順を繰り返します。

（注） ASA Virtual の（静的および DHCP）設定に必要な個別のルーティングルール。

# OCI 上の ASAv インスタンスへのアクセス

セキュアシェル（SSH）接続を使用して、実行中のインスタンスに接続できます。

- ほとんどの UNIX スタイルのシステムには、デフォルトで SSH クライアントが含まれています。
- Windows 10 および Windows Server 2019 システムには、OpenSSH クライアントが含まれている必要があります。Oracle Cloud Infrastructure によって生成された SSH キーを使用してインスタンスを作成した場合に必要になります。
- その他の Windows バージョンの場合は、http://www.putty.org から無償の SSH クライアントである PuTTY をダウンロードできます。

### 前提条件

インスタンスに接続するには、次の情報が必要です。

- インスタンスのパブリック IP アドレス。アドレスは、コンソールの [インスタンスの詳細（Instance Details）] ページから取得できます。ナビゲーションメニューを開きます。**[コアインフラストラクチャ（Core Infrastructure）]** の下で、**[コンピューティング（Compute）]** に移動し、**[インスタンス（Instances）]** をクリックします。次に、インスタンスを選択します。あるいは、コアサービス API の ListVnicAttachments および GetVnic 操作を使用できます。
- インスタンスのユーザー名とパスワード。
- インスタンスを起動したときに使用した SSH キーペアの秘密キー部分へのフルパス。キーペアの詳細については、「Managing Key Pairs on Linux Instances」を参照してください。

（注） 第 0 日用構成で指定したログイン情報を使用するか、インスタンスの起動時に作成した SSH キーペアを使用して、ASAv インスタンスにログインできます。

# SSH を使用した ASAv インスタンスへの接続

UNIX スタイルのシステムから ASAv インスタンスに接続するには、SSH を使用してインスタンスにログインします。

**ステップ 1** 次のコマンドを使用して、ファイルの権限を設定し、自分だけがファイルを読み取れるようにします。

```
$ chmod 400 <private_key>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

**ステップ 2** インスタンスにアクセスするには、次の SSH コマンドを使用します。

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、ASAv インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。

# OpenSSH を使用した ASAv インスタンスへの接続

Windows システムから ASAv インスタンスに接続するには、OpenSSH を使用してインスタンスにログインします。

**ステップ 1** このキーペアを初めて使用する場合は、自分だけがファイルを読み取れるようにファイルの権限を設定する必要があります。

次の手順を実行します。

a) Windows Explorer で、秘密キーファイルに移動し、ファイルを右クリックして **[プロパティ（Properties）]** をクリックします。
b) **[セキュリティ（Security）]** タブで、**[詳細設定（Advanced）]** をクリックします。
c) **[オーナー（Owner）]** が自分のユーザーアカウントであることを確認します。

d) **[継承の無効化（Disable Inheritance）]** をクリックし、**[継承された権限をこのオブジェクトの明示的な権限に変換する（Convert inherited permissions into explicit permissions on this object）]** を選択します。
e) 自分のユーザーアカウントではない各権限エントリを選択し、**[削除（Remove）]** をクリックします。
f) 自分のユーザーアカウントのアクセス権限が **[フルコントロール（Full Control）]** であることを確認します。
g) 変更を保存します。

**ステップ 2** インスタンスに接続するには、Windows PowerShell を開き、次のコマンドを実行します。

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、ASAv インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。

# PuTTY を使用した ASAv インスタンスへの接続

PuTTY を使用して Windows システムから ASAv インスタンスに接続するには、次の手順を実行します。

**ステップ 1** PuTTY を開きます。

**ステップ 2** **[カテゴリ（Category）]** ペインで、**[セッション（Session）]** を選択し、次の内容を入力します。

- **ホスト名または IP アドレス**：

  **<username>@<public-ip-address>**

  ここで、

  <username> は、ASAv インスタンスのユーザー名です。

  <public-ip-address> は、コンソールから取得したインスタンスのパブリック IP アドレスです。

- **ポート**： 22
- **接続タイプ**： SSH

**ステップ 3** **[カテゴリ（Category）]** ペインで、**[Window]** を展開し、**[変換（Translation）]** を選択します。

**ステップ 4** **[リモート文字セット（Remote character set）]** ドロップダウンリストで、**[UTF-8]** を選択します。

Linux ベースのインスタンスでデフォルトのロケール設定は UTF-8 です。これにより、PuTTY は同じロケールを使用するように設定されます。

**ステップ 5** **[カテゴリ（Category）]** ペインで、**[接続（Connection）]**、**[SSH]** の順に展開し、**[認証（Auth）]** をクリックします。

**ステップ 6** **[参照（Browse）]** をクリックして、秘密キーを選択します。

**ステップ 7** **[開く（Open）]** をクリックして、セッションを開始します。

インスタンスに初めて接続する場合は、「サーバーのホストキーがレジストリにキャッシュされていない（the server's host key is not cached in the registry）」というメッセージが表示されることがあります。**[はい（Yes）]** をクリックして、接続を続行します。

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。