

# Microsoft Azure AR4050S, AR3050S, AR2050V 接続設定例

---

- ※ 当社検証結果に基づき記載していますが、全てのお客様環境の動作を保証するものではありません。
- ※ 2018年8月現在の仕様に基いて記載しています。今後の仕様変更によっては接続できない可能性があります。

アライドテレシス株式会社

# 目次

## 1. 概要

1. 概要
2. 設定例の構成
3. IPsecのパラメータ

## 2. Microsoft Azureの設定

1. はじめに
2. Microsoft Azure仮想ネットワークの設定

## 3. AR4050Sの設定

1. はじめに
2. AR4050Sの設定
3. 設定の確認

## 4. 動作確認

1. IPsecの確認
2. Microsoft Azure仮想ネットワークの確認
3. 通信の確認

---

# 1.概要

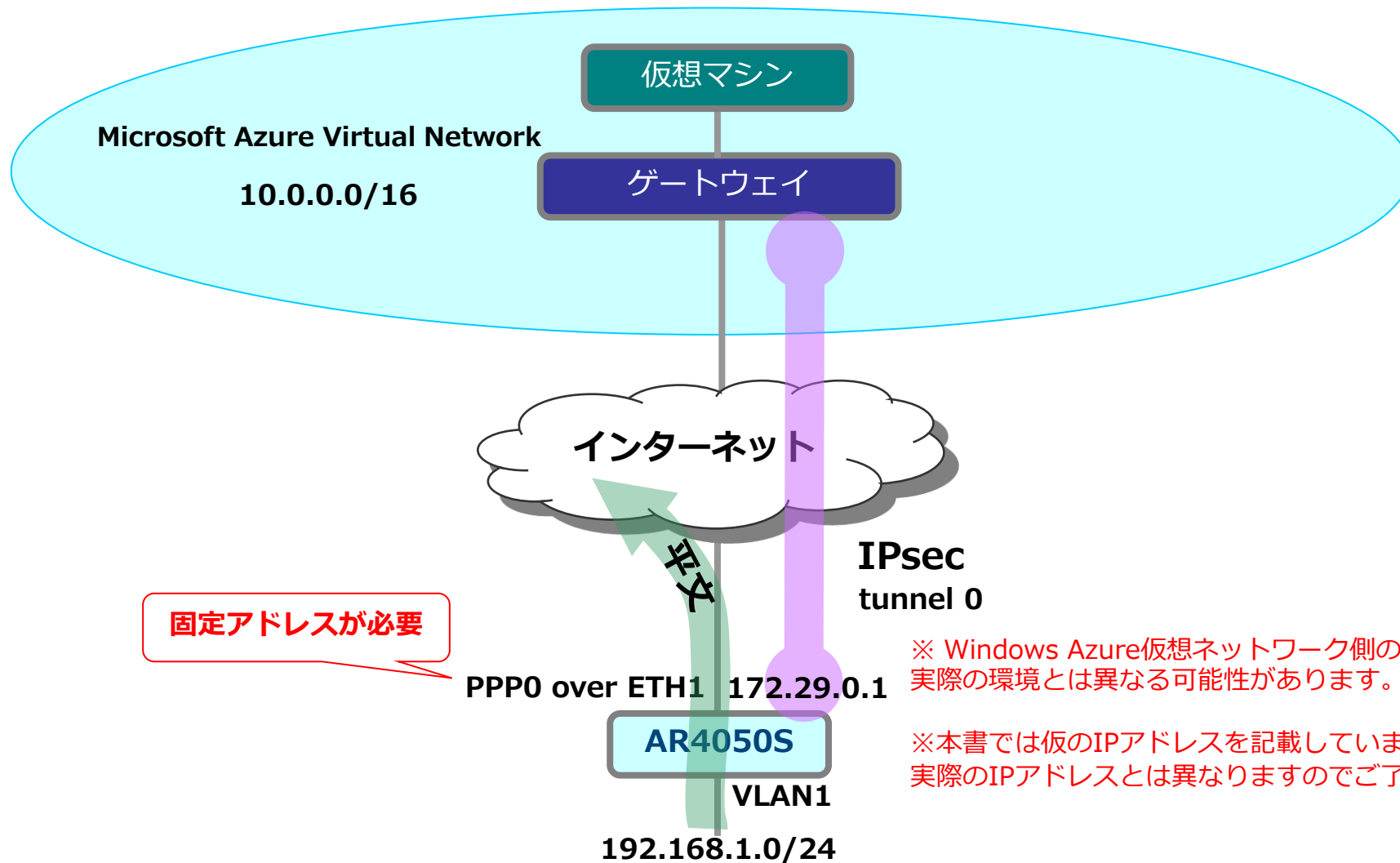
---

# 1-1.概要

- 本書では、Microsoft Azure Virtual Network (以後 Microsoft Azure仮想ネットワーク)のIPsecゲートウェイとIPsec接続を行う設定例を説明します。以降の記述はAR4050Sを前提として説明いたします。
- IPsec接続を行うためにMicrosoft Azure仮想ネットワークに作成するゲートウェイには以下の3つがあり、ゲートウェイによってルーターの設定が変わります。
  1. Basic
    - 1.1. Policy-based VPN gateway
    - 1.2. Route-based VPN gateway
  2. Standard VPN gateway
  3. High Performance VPN gateway
- 本設定例では、AW+ルーター配下の端末からインターネット上のサーバーに直接通信（平文通信）できます。
- AR4050Sはファームウェアバージョン5.4.5-2.1以降をご利用下さい。
- Microsoft Azureに関する技術情報は以下をご参照ください。  
<https://www.microsoft.com/ja-jp/server-cloud/azure/deploy.aspx>

# 1-2.設定例の構成

- 本設定例におけるネットワーク構成は、以下の図の通りです。



※ Windows Azure仮想ネットワーク側の構成図はイメージです。実際の環境とは異なる可能性があります。

※本書では仮のIPアドレスを記載しています。実際のIPアドレスとは異なりますのでご了承ください。

# 1-3.IPsecのパラメータ

- Microsoft Azure仮想ネットワークのIPsecゲートウェイとしてRoute-based VPN gateway、Standard VPN gateway及び、High Performance VPN gatewayでIPsec接続を行う際は、下記パラメータで設定します。

## IKEフェーズ1 (ISAKMP SAのネゴシエーション)

認証方式	事前共有鍵 (pre-shared key)
IKE交換モード	IKEv2
Diffie-Hellman (Oakley) グループ	Group2 (1024ビットMODP)
ISAKMPメッセージの暗号化方式	AES256
ISAKMPメッセージの認証方式	SHA-1
ISAKMP SAの有効期限 (時間)	28800秒 (8時間)

## IKEフェーズ2 (IPsec SAのネゴシエーション)

SAモード	トンネルモード
セキュリティープロトコル	ESP (暗号化 + 認証)
暗号化方式	AES256
認証方式	SHA-1
IPsec SAの有効期限 (時間)	3600秒 (1時間)

# 1-3.IPsecのパラメータ

- Microsoft Azure仮想ネットワークのIPsecゲートウェイとしてPolicy-based VPN gatewayでIPsec接続を行う際は、下記パラメータで設定します。

## IKEフェーズ1 (ISAKMP SAのネゴシエーション)

認証方式	事前共有鍵 (pre-shared key)
IKE交換モード	IKEv1 Mainモード
Diffie-Hellman (Oakley) グループ	Group2 (1024ビットMODP)
ISAKMPメッセージの暗号化方式	AES128
ISAKMPメッセージの認証方式	SHA-1
ISAKMP SAの有効期限(時間)	28800秒 (8時間)

## IKEフェーズ2 (IPsec SAのネゴシエーション)

SAモード	トンネルモード
セキュリティープロトコル	ESP (暗号化 + 認証)
暗号化方式	AES128
認証方式	SHA-1
IPsec SAの有効期限(時間)	3600秒 (1時間)

## 2. Microsoft Azureの設定



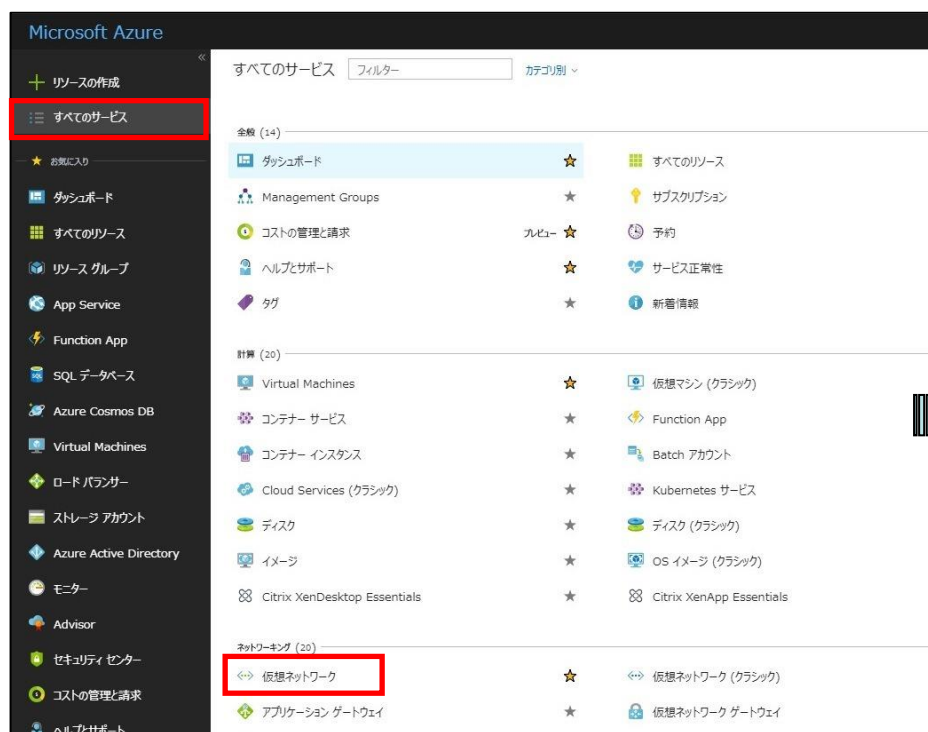
## 2-1.はじめに

- Microsoft Azure仮想ネットワークを設定します。
- Microsoft Azureサブスクリプションの申し込みを行い、Microsoft Azureマネジメントポータルへログインします。  
申込みなどの詳細に関しては、以下をご参照ください。  
<http://msdn.microsoft.com/ja-jp/windowsazure/ee943806.aspx>
- 次頁から掲載している設定画面は2018年8月現在の情報です。  
今後、設定画面が変更される場合がございますのでご了承ください。

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 仮想ネットワークの作成①

- 画面左の[すべてのサービス]、[仮想ネットワーク]の順にクリックします。
- [仮想ネットワーク]画面が表示されるので、画面上の[追加]をクリックします。



## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 仮想ネットワークの作成②

- 表1を参考に、[名前]、[アドレス空間]、[サブスクリプション]、[リソースグループ]、[場所]、[サブネット名前]、[サブネットアドレス範囲]を入力・選択します。
- 入力後は、画面下の[作成]をクリックします。

仮想ネットワークの作成

\* 名前  
Azure ✓

\* アドレス空間 ⓘ  
10.0.0.0/16 ✓  
10.0.0.0 - 10.0.255.255 (65536 アドレス)

\* サブスクリプション  
従量課金 ▼

\* リソースグループ  
 新規作成  既存のものを使用  
Group1 ✓

\* 場所  
東日本 ▼

サブネット

\* 名前  
Gatewaysubnet ✓

\* アドレス範囲 ⓘ  
10.0.0.0/29 ✓  
10.0.0.0 - 10.0.0.7 (8 アドレス)

DDoS 保護 ⓘ  
 Basic  Standard

サービス エンドポイント ⓘ  
無効 有効

作成 Automation オプション

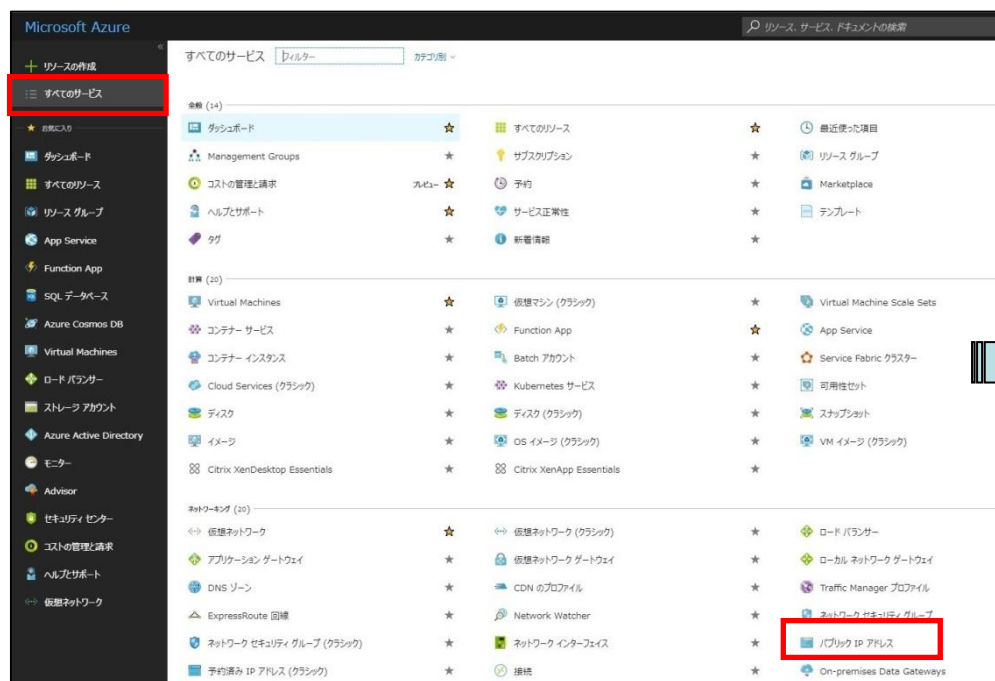
名前	Azure
アドレス空間	10.0.0.0/16
サブスクリプション	※契約に応じて適切なものを選択してください
リソースグループ	新規作成 Group1
場所	東日本
サブネット 名前	Gatewaysubnet
サブネット アドレス範囲	10.0.0.0/29

表1. 仮想ネットワークの作成

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● パブリックIPアドレスの設定①

- 画面左の[すべてのサービス]、[パブリックIPアドレス]の順にクリックします。
- [パブリックIPアドレス]画面が表示されるので、画面上の[追加]をクリックします。



## 2-2. Microsoft Azure仮想ネットワークの設定

### ● パブリックIPアドレスの設定②

- 表2を参考に、[名前]、[SKU]、[IPバージョン]、[IPアドレスの割り当て]、[サブスクリプション]、[リソースグループ]、[場所]を入力・選択します。
- 入力後は、画面下の[作成]をクリックします。

パブリック IP アドレスの作成

\* 名前  
Azure-GIP ✓

\* SKU ⓘ  
 Basic  Standard

\* IPバージョン ⓘ  
 IPv4  IPv6

\* IPアドレスの割り当て  
 動的  静的

\* アイドルタイムアウト(分) ⓘ  
 4

DNS名ラベル ⓘ

.japaneast.cloudapp.azure.com

IPv6 アドレスを作成します

\* サブスクリプション  
従量課金

\* リソースグループ  
 新規作成  既存のものを使用  
Group1

\* 場所  
東日本

**作成** Automation オプション

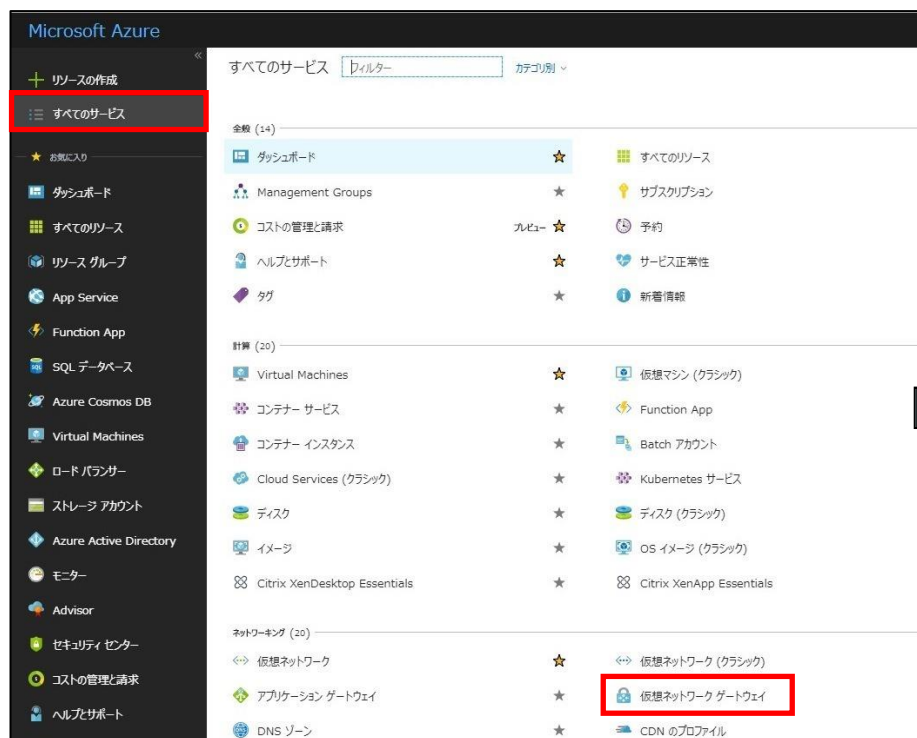
名前	Azure-GIP
SKU	Basic
IPバージョン	IPv4
IPアドレスの割り当て	動的
サブスクリプション	※契約に応じて適切なものを選択してください
リソースグループ	既存のものを使用 Group1
場所	東日本

表2. パブリックIPアドレスの設定

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 仮想ネットワーク ゲートウェイの作成①

- 画面左の[すべてのサービス]、[仮想ネットワーク ゲートウェイ]の順にクリックします。
- [仮想ネットワーク ゲートウェイ]画面が表示されるので、画面上の[追加]をクリックします。



## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 仮想ネットワーク ゲートウェイの作成②：Route-based VPN gatewayの場合

- 表3を参考に、[名前]、[ゲートウェイの種類]、[VPNの種類]、[SKU]、[仮想ネットワーク]、[パブリックIPアドレス]、[サブスクリプション]、[場所]を入力・選択します。
- 入力後は、画面下の[作成]をクリックします。

名前	Azure-Gateway
ゲートウェイの種類	VPN
VPNの種類	ルートベース
SKU	Basic
仮想ネットワーク	Azure
パブリックIPアドレス	既存のものを使用 Azure-GIP
サブスクリプション	※契約に応じて適切なものを選択してください
場所	東日本

表3. 仮想ネットワーク ゲートウェイの作成 (Route-based VPN gateway)

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 仮想ネットワーク ゲートウェイの作成②：Policy-based VPN gatewayの場合

- 表4を参考に、[名前]、[ゲートウェイの種類]、[VPNの種類]、[SKU]、[仮想ネットワーク]、[パブリックIPアドレス]、[サブスクリプション]、[場所]を入力・選択します。
- 入力後は、画面下の[作成]をクリックします。

仮想ネットワーク ゲートウェイの作成

\* 名前  
Azure-Gateway ✓

ゲートウェイの種類  
 VPN  ExpressRoute

VPN の種類  
 ルートベース  ポリシーベース

\* SKU  
Basic

アクティブ/アクティブ モードの有効化

\* 仮想ネットワーク  
Azure

\* パブリック IP アドレス  
 新規作成  既存のものを使用  
Azure-GIP

選択したサブスクリプションおよび場所 '東日本' で Public IP Addresses を表示しています。

BGP ASN の構成

\* サブスクリプション  
従量課金

リソース グループ  
Group1

\* 場所  
東日本

作成 Automation オプション

名前	Azure-Gateway
ゲートウェイの種類	VPN
VPNの種類	ポリシーベース
SKU	Basic
仮想ネットワーク	Azure
パブリックIPアドレス	既存のものを使用 Azure-GIP
サブスクリプション	※契約に応じて適切なものを選択してください
場所	東日本

表4. 仮想ネットワーク ゲートウェイの作成 (Policy-based VPN gateway)



## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 接続の作成①

- 画面左の[すべてのサービス]、[接続] の順にクリックします。
- [接続]画面が表示されるので、画面上の[追加]をクリックします。

The image shows two screenshots from the Microsoft Azure portal. The left screenshot displays the 'All Services' page, where the 'Connections' service is highlighted in a red box. The right screenshot shows the 'Connections' page, where the '+ Add' button is highlighted in a red box. An arrow points from the 'Connections' service in the left screenshot to the 'Connections' page in the right screenshot.

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 接続の作成②

- 表5を参考に、[接続の種類]、[サブスクリプション]、[リソースグループ]、[場所]を選択します。
- 選択後は、画面下の[OK]をクリックします。

The screenshot shows a '接続の作成' (Create Connection) dialog box with the following settings:

- 接続の種類**: サイト対サイト (IPsec)
- サブスクリプション**: 従量課金
- リソースグループ**: Group1 (Selected: 既存のものを使用)
- 場所**: 東日本

An 'OK' button is located at the bottom of the dialog.

接続の種類	サイト対サイト(IPsec)
サブスクリプション	※契約に応じて適切なものを選択してください
リソースグループ	既存のものを使用 Group1
場所	東日本

表5. 接続の作成(基本)

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 接続の作成③

- [仮想ネットワーク ゲートウェイを選択]をクリックし、先ほど作成した仮想ネットワーク ゲートウェイ(本例では「Azure-Gateway」)を選択します。

The screenshot displays the 'Virtual Network Gateway' configuration wizard in the Azure portal. It is divided into three main sections:

- 接続の作成 (Connection Creation):** Shows a progress indicator with three steps: 1. 基本 (Basic) - completed with a green checkmark; 2. 設定 (Configure) - currently active and highlighted in blue; 3. 概要 (Summary) - pending.
- 設定 (Configuration):** Contains several fields:
  - \* 仮想ネットワーク ゲートウェイ (Virtual Network Gateway):** A dropdown menu highlighted with a red box, showing '仮想ネットワーク ゲートウェイを選択...' (Select virtual network gateway...) and a right-pointing arrow.
  - \* ローカル ネットワーク ゲートウェイ (Local Network Gateway):** A dropdown menu showing 'ローカル ネットワーク ゲートウェイを選...' (Select local network gateway...) and a right-pointing arrow.
  - \* 接続名 (Connection Name):** An empty text input field.
  - \* 共有キー (PSK) (Shared Key (PSK)):** An empty text input field.
  - BGP を有効にする (Enable BGP)
- 仮想ネットワーク ゲートウェイ... (Virtual Network Gateway...):** A panel on the right showing a message: '1 つの接続を持つ仮想ネットワークを使用するには、仮想ネットワーク ゲートウェイに関連付ける必要があります。詳細情報' (To use a virtual network with one connection, you must associate it with a virtual network gateway. See details). Below the message, a dropdown menu is highlighted with a red box, showing 'Azure-Gateway Group1' with a lock icon.

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 接続の作成④ - ローカル ネットワーク ゲートウェイの作成

- [ローカル ネットワーク ゲートウェイを選択]、[新規作成]の順にクリックします。
- 表6を参考に、[名前]、[IPアドレス]、[アドレス空間]を入力します。
- 入力後は、画面下の[OK]をクリックします。

The screenshot displays the Azure portal interface for creating a Local Network Gateway. It is divided into four main panes:

- 接続の作成 (Connection Creation):** Shows a progress indicator with three steps: 1. 基本 (Basic) - 基本設定を構成してください (Basic settings), 2. 設定 (Settings) - 接続設定を構成してください (Configure connection settings), and 3. 概要 (Overview) - 確認と作成 (Review and create). Step 2 is currently active.
- 設定 (Settings):** Shows the gateway type selection. '仮想ネットワーク ゲートウェイ' (Virtual Network Gateway) is set to 'Azure-Gateway'. 'ローカル ネットワーク ゲートウェイ' (Local Network Gateway) is selected, with a red box around the selection button and a red exclamation mark icon.
- ローカル ネットワーク ゲートウェイの... (Local Network Gateway...):** Shows a '+ 新規作成' (New) button highlighted with a red box. Below it, it says '結果がありません' (No results).
- ローカル ネットワーク ゲートウ... (Local Network Gateway...):** Shows the configuration fields: '名前' (Name) is 'AR4050S', 'IP アドレス' (IP Address) is '172.29.0.1', and 'アドレス空間' (Address Space) is '192.168.1.0/24'. Each field is highlighted with a red box. There is also an 'OK' button at the bottom right, also highlighted with a red box.

名前	AR4050S
IPアドレス	172.29.0.1
アドレス空間	192.168.1.0/24

表6. ローカル ネットワーク ゲートウェイの作成

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● 接続の作成⑤

- 表7を参考に、[接続名]、[共有キー (PSK)]を入力します。
- 入力後は、画面下の[OK]をクリックします。

接続の作成 × 設定 □ ×

1 基本  
基本設定を構成してください ✓

2 設定  
接続設定を構成してください >

3 概要  
確認と作成 >

\* 仮想ネットワークゲートウェイ ⓘ  
Azure-Gateway >

\* ローカルネットワークゲートウェイ ⓘ  
(新規) AR4050S >

\* 接続名  
Azure-Connection ✓

\* 共有キー (PSK) ⓘ  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1... ✓

BGPを有効にする ⓘ

OK

接続名	Azure-Connection
共有キー (PSK)	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234

表7. 接続の作成

## 2-2. Microsoft Azure仮想ネットワークの設定

- 接続の作成⑥
  - ・ 設定内容を確認し、画面下の[OK]をクリックします。

接続の作成	概要																
<p><b>1</b> 基本 基本設定を構成してください ✓</p> <hr/> <p><b>2</b> 設定 接続設定を構成してください ✓</p> <p><b>3</b> 概要 確認と作成 &gt;</p>	<p>基本</p> <table><tr><td>接続の種類</td><td>サイト対サイト (IPsec)</td></tr><tr><td>サブスクリプション</td><td>従量課金</td></tr><tr><td>リソース グループ</td><td>Group1</td></tr><tr><td>場所</td><td>東日本</td></tr></table> <p>設定</p> <table><tr><td>仮想ネットワーク ゲートウェイ</td><td>Azure-Gateway</td></tr><tr><td>ローカル ネットワーク ゲートウェイ</td><td>(新規) AR4050S</td></tr><tr><td>接続名</td><td>Azure-Connection</td></tr><tr><td>共有キー (PSK)</td><td>ABCDEFGHIJKLMNOPQRSTUVWXYZ1234</td></tr></table>	接続の種類	サイト対サイト (IPsec)	サブスクリプション	従量課金	リソース グループ	Group1	場所	東日本	仮想ネットワーク ゲートウェイ	Azure-Gateway	ローカル ネットワーク ゲートウェイ	(新規) AR4050S	接続名	Azure-Connection	共有キー (PSK)	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234
接続の種類	サイト対サイト (IPsec)																
サブスクリプション	従量課金																
リソース グループ	Group1																
場所	東日本																
仮想ネットワーク ゲートウェイ	Azure-Gateway																
ローカル ネットワーク ゲートウェイ	(新規) AR4050S																
接続名	Azure-Connection																
共有キー (PSK)	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234																
	<p>OK</p>																

## 2-2. Microsoft Azure仮想ネットワークの設定

### ● ゲートウェイIPアドレスの確認①

- 画面左の[すべてのサービス]、[接続]の順にクリックします。
- [接続]画面上の[Azure-Connection]をクリックします。

The screenshot shows the Microsoft Azure portal interface. On the left-hand side, there is a navigation pane with a list of services. The 'すべてのサービス' (All Services) link is highlighted with a red rectangular box. The main area of the page displays a grid of service categories. In the bottom right corner of this grid, the '接続' (Connections) link is highlighted with a red rectangular box. A large blue arrow points from this screenshot towards the right-hand screenshot.

The screenshot shows the '接続' (Connections) page in the Microsoft Azure portal. At the top, there are buttons for '+ 追加' (Add), '列の編集' (Edit Columns), and '更新' (Refresh). Below this, there is a search bar and a dropdown menu for 'すべてのリソース グループ' (All Resource Groups). A table with one item is displayed. The table has columns for '名前' (Name), '状態' (Status), and 'ピア 1' (Peer 1). The single row in the table is 'Azure-Connection', and this row is highlighted with a red rectangular box.

## 2-2. Microsoft Azure仮想ネットワークの設定

- ゲートウェイIPアドレスの確認②

- [Azure-Connection]の[概要]画面上の[仮想ネットワーク ゲートウェイ]のIPアドレスを確認します。

Azure-Connection 接続

検索 (Ctrl+/)

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

設定

共有キー

→ 移動   ↓ 構成のダウンロード   🗑 削除

リソースグループ (変更)	データ入力
Group1	0 B
状態	データ出力
接続中	0 B
場所	仮想ネットワーク
東日本	Azure
サブスクリプション (変更)	仮想ネットワーク ゲートウェイ
従量課金	Azure-Gateway (0000-0000-0000)
サブスクリプション ID	ローカル ネットワーク ゲートウェイ
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	AR4050S (0000-0000-0000)
タグ (変更)	
タグを追加するにはここをクリック	



---

## 3. AR4050Sの設定

---

## 3-1.はじめに

- AR4050Sの設定に必要な情報は下記です。  
設定前に情報をまとめておくと便利です。

設定項目	本例	お客様情報
PPPユーザー名	user@ispA	
PPPパスワード	isppasswdA	
AR4050S ppp0 (WAN側) IPアドレス	172.29.0.1/32	
AR4050S vlan1 (LAN側) IPアドレス	192.168.1.254/24	
共有キー	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234	
Tunnel interface IP address	172.30.0.1/32	
ゲートウェイIPアドレス	172.16.0.1	
LAN側ネットワークのサブネット	192.168.1.0/24	
Microsoft Azure仮想ネットワークのサブネット	10.0.0.0/16	

## 3-2. AR4050Sの設定

- ログイン

- AR4050Sにログインします。  
工場出荷時設定のCLIの ログインID/PW は下記の通りです。

```
awplus login: manager
```

```
Password: friend ←実際には表示されません
```

```
Last login: Fri Nov 13 17:09:55 JST 2015 on ttyS0
```

```
AlliedWare Plus (TM) 5.4.5 11/12/15 03:11:03
```

```
awplus>
```

- モードの移行

- 非特権EXECモードから、特権EXECモードに移行します。

```
awplus> enable
```

- 特権EXECモードからグローバルコンフィグモードに移行します。

```
awplus# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
awplus(config)#
```

## 3-2. AR4050Sの設定

- スパニングツリープロトコルの無効化
  - LANポートにおいて初期状態で有効化されているスパニングツリープロトコル (RSTP) を無効化します。

```
awplus(config)# no spanning-tree rstp enable
```

- LANインターフェース設定
  - LAN側インターフェース (vlan1) にIPアドレスを設定します。

```
awplus(config)# interface vlan1  
awplus(config-if)# ip address 192.168.1.254/24  
awplus(config-if)# exit
```

- PPPインターフェース作成
  - ETH 1 インターフェース上にPPPインターフェースを作成します。

```
awplus(config)# interface eth1  
awplus(config-if)# encapsulation ppp 0
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

### ● PPPoEインターフェース設定

- PPPインターフェースにWAN側のIPアドレスを設定します。
- LCP EchoパケットによるPPP接続の監視を有効にします。
- ISPから通知されたPPPユーザー名やパスワードを設定します。
- PPPインターフェースを通過するTCPパケットのMSS値の自動書き換えを有効にします。

```
awplus(config)# interface ppp0
awplus(config-if)# ip address 172.29.0.1/32
awplus(config-if)# keepalive
awplus(config-if)# ppp username user@ispA
awplus(config-if)# ppp password isppasswdA
awplus(config-if)# ip tcp adjust-mss pmtu
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

### ● エンティティの設定

- ファイアウォールやNATのルール作成時に使うエンティティ（通信主体）を定義します。
- 内部ネットワークを表すゾーン「private」と外部ネットワークを表すゾーン「public」を作成します。

```
awplus(config)# zone private
awplus(config-zone)# network lan
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# ip subnet 10.0.0.0/16
```

```
awplus(config)# zone public
awplus(config-zone)# network wan
awplus(config-network)# ip subnet 0.0.0.0/0 interface ppp0
awplus(config-network)# host ppp0
awplus(config-host)# ip address 172.29.0.1
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

### ● アプリケーションの設定

- ファイアウォールやNATのルール作成時に通信内容を指定するために使う「アプリケーション」を定義します
- IPsecのESPパケットを表すカスタムアプリケーション「esp」を定義します。
- ISAKMPパケットを表すカスタムアプリケーション「isakmp」を定義します。

```
awplus(config)# application esp  
awplus(config-application)# protocol 50
```

```
awplus(config)# application isakmp  
awplus(config-application)# protocol udp  
awplus(config-application)# sport 500  
awplus(config-application)# dport 500
```

## 3-2. AR4050Sの設定

- ファイアウォール、NATの設定
  - ISAKMPパケット、ESPパケットは通しつつ他の外側からの通信を遮断し、内側からの通信は自由に行えるようにファイアウォールのルールを設定します。
  - LAN側ネットワークに接続されているすべてのコンピューターがダイナミックENAT機能を使用できるように設定します。

```
awplus(config)# firewall
```

```
awplus(config-firewall)# rule 10 permit isakmp from public.wan.ppp0 to public.wan
```

```
awplus(config-firewall)# rule 20 permit isakmp from public.wan to public.wan.ppp0
```

```
awplus(config-firewall)# rule 30 permit esp from public.wan to public.wan.ppp0
```

```
awplus(config-firewall)# rule 40 permit esp from public.wan.ppp0 to public.wan
```

```
awplus(config-firewall)# rule 50 permit any from private to private
```

```
awplus(config-firewall)# rule 60 permit any from private to public
```

```
awplus(config-firewall)# protect
```

```
awplus(config)# nat
```

```
awplus(config-nat)# rule 10 masq any from private to public
```

```
awplus(config-nat)# enable
```



## 3-2. AR4050Sの設定

- IPsec設定 : **Route-based VPN gatewayの場合**

- IKEフェーズ1のポリシー「Azure-isakmp」とフェーズ2のポリシー「Azure-ipsec」をそれぞれ作成します。

```
awplus(config)# crypto isakmp profile Azure-isakmp
```

```
awplus(config-isakmp-profile)# version 2
```

```
awplus(config-isakmp-profile)# lifetime 28800
```

```
awplus(config-isakmp-profile)# transform 1 integrity sha1 encryption aes256 group 2
```

```
awplus(config)# crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.16.0.1
```

```
awplus(config)# crypto isakmp peer address 172.16.0.1 profile Azure-isakmp
```

```
awplus(config)# crypto ipsec profile Azure-ipsec
```

```
awplus(config)# lifetime seconds 3600
```

```
awplus(config-ipsec-profile)# transform 1 protocol esp integrity sha1 encryption aes256
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

- IPsec設定 : **Policy-based VPN gatewayの場合**

- IKEフェーズ1のポリシー「Azure-isakmp」とフェーズ2のポリシー「Azure-ipsec」をそれぞれ作成します。

```
awplus(config)# crypto isakmp profile Azure-isakmp
```

```
awplus(config-isakmp-profile)# version 1 mode main
```

```
awplus(config-isakmp-profile)# lifetime 28800
```

```
awplus(config-isakmp-profile)# transform 1 integrity sha1 encryption aes256 group 2
```

```
awplus(config)# crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.16.0.1
```

```
awplus(config)# crypto isakmp peer address 172.16.0.1 profile Azure-isakmp
```

```
awplus(config)# crypto ipsec profile Azure-ipsec
```

```
awplus(config)# lifetime seconds 3600
```

```
awplus(config-ipsec-profile)# transform 1 protocol esp integrity sha1 encryption aes128
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

- トンネルインターフェース設定
  - IPsecトンネルインターフェースtunnel0を作成します。
  - IPsecトンネルの始点(自装置)と終点(仮想ネットワークゲートウェイ)を指定します。
  - IKEフェーズ2で使用するポリシーを指定します。
  - IPsec通信を行うネットワークの範囲を指定します。
  - トンネリング方式を指定します。
  - IP通信を有効にするためにIPアドレスを設定します(このIPアドレスは通信に使用されません)
  - トンネルインターフェースを通過するTCPパケットのMSS値の書き換えを有効にします。

```
awplus(config)# int tunnel0
awplus(config-if)# mtu 1300
awplus(config-if)# tunnel source ppp0
awplus(config-if)# tunnel destination 172.16.0.1
awplus(config-if)# tunnel protection ipsec profile Azure-ipsec
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 10.0.0.0/16
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# ip address 172.30.0.1/32
awplus(config-if)# ip tcp adjust-mss 1260
```

赤字には25ページのお客様情報を入力ください。

## 3-2. AR4050Sの設定

### ● ルート設定

- デフォルトルートを設定します。
- Microsoft Azure仮想ネットワーク宛の通信がIPsecトンネルを経由するように設定します。またIPsecトンネルが確立するまでは、このルートを使用できないよう設定します。

```
awplus(config)# ip route 0.0.0.0/0 ppp0  
awplus(config)# ip route 10.0.0.0/16 tunnel0  
awplus(config)# ip route 10.0.0.0/16 null 254
```

### ● コンフィグの保存、確認

- 設定は以上となります。
- 現在の設定内容を起動時コンフィグとして保存します。
- 設定（ランニングコンフィグ）を表示します。
- 次頁の「入力コマンド一覧」を参考に、設定に誤りが無いかご確認ください。

```
awplus# copy running-config startup-config  
awplus# show running-config
```

赤字には25ページのお客様情報を入力ください。

## 3-3. 設定の確認

- 入力コマンド一覧：**Route-based VPN gatewayの場合**
  - 「show running-config」で設定を確認できます。下記のコマンドが表示されているかご確認ください。

```
!  
no spanning-tree rstp enable  
!  
interface eth1  
  encapsulation ppp 0  
!  
interface vlan1  
  ip address 192.168.1.254/24  
!  
interface ppp0  
  keepalive  
  ppp username user@ispA  
  ppp password isppasswdA  
  ip address 172.29.0.1/32  
  ip tcp adjust-mss pmtu  
!  
zone private  
  network lan  
  ip subnet 10.0.0.0/16  
  ip subnet 192.168.1.0/24  
!  
zone public  
  network wan  
  ip subnet 0.0.0.0/0 interface ppp0  
  host ppp0  
  ip address 172.29.0.1  
!  
application esp  
  protocol 50  
!  
application isakmp  
  protocol udp  
  sport 500  
  dport 500
```

```
!  
firewall  
  rule 10 permit isakmp from public.wan.ppp0 to public.wan  
  rule 20 permit isakmp from public.wan to public.wan.ppp0  
  rule 30 permit esp from public.wan to public.wan.ppp0  
  rule 40 permit esp from public.wan.ppp0 to public.wan  
  rule 50 permit any from private to private  
  rule 60 permit any from private to public  
  protect  
!  
nat  
  rule 10 masq any from private to public  
  enable  
!  
crypto ipsec profile Azure-ipsec  
  lifetime seconds 3600  
  transform 1 protocol esp integrity SHA1 encryption AES256  
!  
crypto isakmp profile Azure-isakmp  
  version 2  
  lifetime 28800  
  transform 1 integrity SHA1 encryption AES256 group 2  
!  
crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.16.0.1  
!  
crypto isakmp peer address 172.16.0.1 profile Azure-isakmp  
!  
interface tunnel0  
  mtu 1300  
  tunnel source ppp0  
  tunnel destination 172.16.0.1  
  tunnel protection ipsec profile Azure-ipsec  
  tunnel local selector 192.168.1.0/24  
  tunnel remote selector 10.0.0.0/16  
  tunnel mode ipsec ipv4  
  ip address 172.30.0.1/32  
  ip tcp adjust-mss 1260  
!  
ip route 0.0.0.0/0 ppp0  
ip route 10.0.0.0/16 tunnel0  
ip route 10.0.0.0/16 Null 254  
!  
end
```

各コマンドの詳細は、コマンドリファレンスを参照ください。

[http://www.allied-telesis.co.jp/support/list/router/ar3050s\\_ar4050s/manual.html](http://www.allied-telesis.co.jp/support/list/router/ar3050s_ar4050s/manual.html)

## 3-3. 設定の確認

- 入力コマンド一覧 : **Policy-based VPN gatewayの場合**
  - 「show running-config」で設定を確認できます。下記のコマンドが表示されているかご確認ください。

```
!  
no spanning-tree rstp enable  
!  
interface eth1  
  encapsulation ppp 0  
!  
interface vlan1  
  ip address 192.168.1.254/24  
!  
interface ppp0  
  keepalive  
  ppp username user@ispA  
  ppp password isppasswdA  
  ip address 172.29.0.1/32  
  ip tcp adjust-mss pmtu  
!  
zone private  
  network lan  
  ip subnet 10.0.0.0/16  
  ip subnet 192.168.1.0/24  
!  
zone public  
  network wan  
  ip subnet 0.0.0.0/0 interface ppp0  
  host ppp0  
  ip address 172.29.0.1  
!  
application esp  
  protocol 50  
!  
application isakmp  
  protocol udp  
  sport 500  
  dport 500
```

```
!  
firewall  
  rule 10 permit isakmp from public.wan.ppp0 to public.wan  
  rule 20 permit isakmp from public.wan to public.wan.ppp0  
  rule 30 permit esp from public.wan to public.wan.ppp0  
  rule 40 permit esp from public.wan.ppp0 to public.wan  
  rule 50 permit any from private to private  
  rule 60 permit any from private to public  
  protect  
!  
nat  
  rule 10 masq any from private to public  
  enable  
!  
crypto ipsec profile Azure-ipsec  
  lifetime seconds 3600  
  transform 1 protocol esp integrity SHA1 encryption AES128  
!  
crypto isakmp profile Azure-isakmp  
  version 1 mode main  
  lifetime 28800  
  transform 1 integrity SHA1 encryption AES256 group 2  
!  
crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.16.0.1  
!  
crypto isakmp peer address 172.16.0.1 profile Azure-isakmp  
!  
interface tunnel0  
  mtu 1300  
  tunnel source ppp0  
  tunnel destination 172.16.0.1  
  tunnel protection ipsec profile Azure-ipsec  
  tunnel local selector 192.168.1.0/24  
  tunnel remote selector 10.0.0.0/16  
  tunnel mode ipsec ipv4  
  ip address 172.30.0.1/32  
  ip tcp adjust-mss 1260  
!  
ip route 0.0.0.0/0 ppp0  
ip route 10.0.0.0/16 tunnel0  
ip route 10.0.0.0/16 Null 254  
!  
end
```

各コマンドの詳細は、コマンドリファレンスを参照ください。

[http://www.allied-telesis.co.jp/support/list/router/ar3050s\\_ar4050s/manual.html](http://www.allied-telesis.co.jp/support/list/router/ar3050s_ar4050s/manual.html)

---

## 4. 動作確認

---

## 4-1. IPsecの確認

- ISAKMP SAの確立状態

- 下記コマンドを実行し、ISAKMP SAの確立状態がEstablishであることを確認します。

```
awplus# show isa sa
```

Peer	Cookies (initiator:responder) Encryption	Integrity	Group	Auth DPD	Ver NATT	Expires State
172.16.0.1	b6d4f457692b198f:3042fa40859161c6 AES256	SHA1	2	PSK yes	2 no	26713s Established

- 上記のように表示されない場合は、ISAKMP SAの確立に失敗しています。共有キーやISAKMPポリシーが正しく設定されているかご確認ください。



## 4-1. IPsecの確認

- IPsec SAの確立状態

- 下記コマンドを実行し、IPsec SAが確立していることを確認します。

```
awplus# show ipsec sa
```

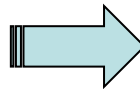
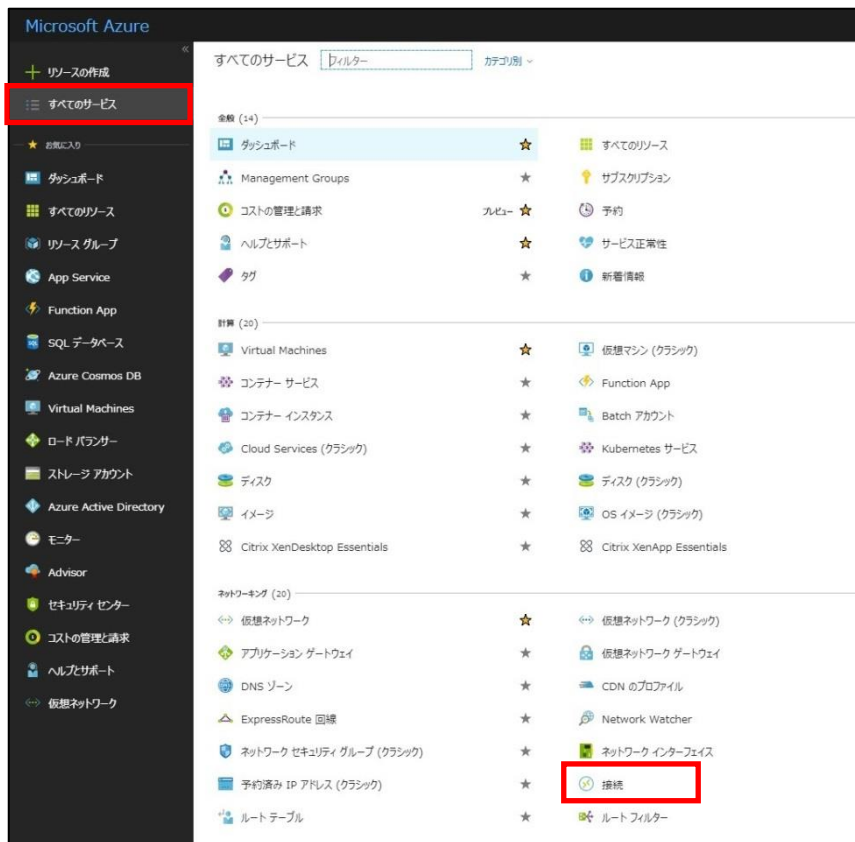
Peer	SPI (in:out) Encryption	Mode Integrity	Proto PFS	Expires
172.16.0.1	c74bd754:27e7f6a0 AES256	tunnel SHA1	ESP -	3130s

- 上記のように表示されない場合は、IPsec SAの確立に失敗しています。IPsecポリシーが正しく設定されているかご確認ください。

# 4-2. Microsoft Azure仮想ネットワークの確認

## ● 接続の確認①

- 画面左の[参照]、[接続]の順にクリックします。
- [接続]画面上の[Azure-Connection]をクリックします。



## 4-2. Microsoft Azure仮想ネットワークの確認

### ● 接続の確認②

- [Azure-Connection]の[概要]画面上の[状態]が[接続済み]になっていることを確認します。

The screenshot shows the 'Azure-Connection' overview page. The left sidebar contains navigation options: '概要' (Overview), 'アクティビティ ログ' (Activity Log), 'アクセス制御 (IAM)' (Access Control (IAM)), 'タグ' (Tags), and '設定' (Settings). The main content area displays connection details for 'Group1'. The '状態' (Status) field is highlighted with a red box and shows '接続済み' (Connected). Other details include 'データ入力' (Data Input) at 0 B, 'データ出力' (Data Output) at 64 B, '場所' (Location) as '東日本' (East Japan), and 'サブスクリプション' (Subscription) as '従量課金' (Pay-as-you-go). The '仮想ネットワーク' (Virtual Network) is 'Azure', and the '仮想ネットワークゲートウェイ' (Virtual Network Gateway) is 'Azure-Gateway (AR4050S)'. The 'ローカル ネットワークゲートウェイ' (Local Network Gateway) is 'AR4050S'.

項目	値
リソースグループ (変更)	Group1
状態	接続済み
場所	東日本
サブスクリプション (変更)	従量課金
サブスクリプション ID	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
タグ (変更)	タグを追加するにはここをクリック
データ入力	0 B
データ出力	64 B
仮想ネットワーク	Azure
仮想ネットワークゲートウェイ	Azure-Gateway (AR4050S)
ローカル ネットワークゲートウェイ	AR4050S

## 4-3. 通信の確認

- 仮想ネットワーク上の仮想マシンと通信ができることを確認します。
  - 仮想マシンの作成方法については、以下をご参照ください。  
<https://msdn.microsoft.com/ja-jp/windowsazure/dn194020>
  - 仮想マシンのIPアドレス（本例では「10.0.0.100」）に対してpingが通ることを確認します。  
ルーター上でpingを実行する際は、パケットがファイアウォールによって破棄されないよう始点IPアドレスを指定してください。

```
awplus # ping 10.0.0.100 source 192.168.1.254
PING 10.0.0.100 (10.0.0.100) from 192.168.1.254 : 56(84) bytes of data.
64 bytes from 10.0.0.100: icmp_req=1 ttl=127 time=7.71 ms
64 bytes from 10.0.0.100: icmp_req=2 ttl=127 time=7.53 ms
64 bytes from 10.0.0.100: icmp_req=3 ttl=127 time=7.07 ms
64 bytes from 10.0.0.100: icmp_req=4 ttl=127 time=6.89 ms
64 bytes from 10.0.0.100: icmp_req=5 ttl=127 time=7.06 ms

--- 10.0.0.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 6.899/7.256/7.716/0.330 ms
```

