

# AWSサイト間VPNの構築（3.AWSのVPN構築）

AWS



## AWSサイト間VPNの構築 (3.AWSのVPN構築)

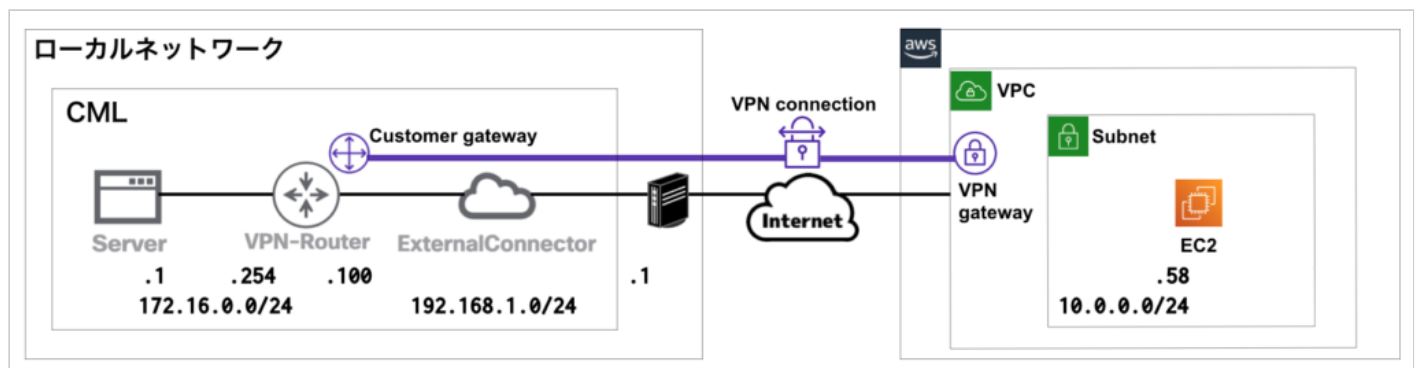
2021.09.20 2021.08.12

[【前回】AWSサイト間VPNの構築（2.AWSのEC2構築）](#)[【次回】AWSサイト間VPNの構築（4.CMLの構築）](#)

## ネットワーク構成

下記のネットワーク構成で、CML上のLAN(172.16.0.0/24)とAWSのサブネット(10.0.0.0/24)が直接通信できるようにします。

※Server(172.16.0.1)からEC2(10.0.0.58)にPingによる疎通確認ができるようにしていきます。



## AWSのVPN構築

AWSのVPNを構築します。

## カスタマーゲートウェイの作成

ローカルネットワーク側のVPNの起点となるカスタマーゲートウェイを作成します。まず、自身が利用しているグローバルIPアドレスを確認します。ここではCMANのIPアドレス確認ページで確認しています。



「aws-vpn-test-cgw」という名前で、ルーティングは「静的」を選択し、IPアドレスは確認した「グローバルIPアドレス」を設定します。

カスタマーゲートウェイ > カスタマーゲートウェイの作成

### カスタマーゲートウェイの作成

ゲートウェイの外部インターフェイスのインターネットでルーティング可能な IP アドレスを指定します。このアドレスは静的である必要があります。また、ネットワークアドレス変換 (NAT) を実行するデバイスの背後のアドレスを使用できます。動的なルーティングでは、ゲートウェイのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) も指定します。これはパブリックまたはプライベート ASN (64512～65534 の範囲内のものなど) とすることができます。

名前

ルーティング ☐ 動的 ☒ 静的

グローバルIPアドレス

IP アドレス

Certificate ARN

Device

\* 必須

キャンセル

「使用可能」となれば、作成完了です。

Name	ID	状態	タイプ	IP アドレス	BGP ASN	Certificate ARN
aws-vpn-test-cgw	cgw-	使用可能	ipsec.1		65000	

## 仮想プライベートゲートウェイの作成

AWS側のVPNの起点となる仮想プライベートゲートウェイを作成します。

「aws-vpn-test-vgw」という名前で作成しています。

仮想プライベートゲートウェイ > 仮想プライベートゲートウェイの作成

### 仮想プライベートゲートウェイの作成

仮想プライベートゲートウェイは、VPN トンネルの Amazon 側にあるルーターです。

名前タグ

ASN ☒ Amazon のデフォルト ASN ☐ カスタム ASN

\* 必須

キャンセル 仮想プライベートゲートウェイの作成

作成後は状態が「detached」となっているため、VPCにアタッチします。

仮想プライベートゲートウェイの作成

アクション

タグや属性によるフィルター、またはキーワードによる検索

	Name	ID	状態	タイプ	VPC	ASN (Amazon 側)
	aws-vpn-test-vgw	vgw-	detached	ipsec.1	-	64512

「アクション」→「VPCにアタッチ」を選択します。

仮想プライベートゲートウェイの作成

アクション ^

タグや属性によるフィルター、または

仮想プライベートゲートウェイの削除

VPC にアタッチ

VPC からデタッチ

タグの追加/編集

Name	ID	タイプ	VPC	ASN (Amazon 側)
aws-vpn-test-vgw	vgw- detached	ipsec.1	-	64512

作成したVPCを選択しアタッチします。

仮想プライベートゲートウェイ > VPC にアタッチ

## VPC にアタッチ

仮想プライベートゲートウェイにアタッチする VPC を選択します。

仮想プライベートゲートウェイ ID vgw- [redacted]

VPC\* vpc- [redacted] [dropdown arrow] [refresh icon]

\* 必須

キャンセル はい、アタッチします

「attaching」の状態を経由し、

仮想プライベートゲートウェイの作成						
アクション						
タグや属性によるフィルター、またはキーワードによる検索						
	Name	ID	状態	タイプ	VPC	ASN (Amazon 側)
<input checked="" type="checkbox"/>	aws-vpn-test-vgw	vgw-[redacted]	attaching	ipsec.1	vpc-[redacted]   aws-vpn-test	64512

「attached」となれば、作成完了です。

仮想プライベートゲートウェイの作成						
アクション						
タグや属性によるフィルター、またはキーワードによる検索						
	Name	ID	状態	タイプ	VPC	ASN (Amazon 側)
<input checked="" type="checkbox"/>	aws-vpn-test-vgw	vgw-[redacted]	attached	ipsec.1	vpc-[redacted]   aws-vpn-test	64512

## ルートテーブルの設定

仮想プライベートゲートウェイからVPC内にルートを伝播するための設定を行います。

ルートテーブルの「ルート伝播」タブを選択し、「ルート伝播の編集」をクリックします。

VPC > ルートテーブル > rtb- [redacted]

rtb- [redacted] アクション ▼

**詳細 情報**

ルートテーブル ID [redacted] rtb- [redacted]	メイン はい	明示的なサブネットの関連付け -	Edge の関連付け -
VPC vpc- [redacted]   aws-vpn-test	所有者 ID [redacted]		

ルート    サブネットの関連付け    Edge の関連付け    **ルート伝播**    タグ

**ルート伝播 (1)** ルート伝播の編集

Q 仮想プライベートゲートウェイの検索

仮想プライベートゲートウェイ    伝播

vgw- [redacted] / aws-vpn-test-vgw    いいえ

作成した仮想プライベートゲートウェイの伝播の「有効化」にチェックを入れます。

VPC > ルートテーブル > rtb- [redacted] > ルート伝播の編集

## ルート伝播の編集

**ルートテーブルの基本的な詳細**

ルートテーブル ID  
[redacted] rtb- [redacted]

**ルート伝播の編集**

仮想プライベートゲートウェイ	伝播
vgw- [redacted] / aws-vpn-test-vgw	<input checked="" type="checkbox"/> 有効化

キャンセル 保存

伝播が「はい」となれば、設定完了です。

VPC > ルートテーブル > rtb-  
rtb-  
アクション ▼

詳細 情報

ルートテーブル ID rtb-	メイン はい	明示的なサブネットの関連付け -	Edge の関連付け -
VPC vpc-   aws-vpn-test	所有者 ID -		

ルート | サブネットの関連付け | Edge の関連付け | ルート伝播 | タグ

ルート伝播 (1) ルート伝播の編集

Q 仮想プライベートゲートウェイの検索

仮想プライベートゲートウェイ	伝播
vgw- / aws-vpn-test-vgw	はい

## サイト間のVPN接続の作成

カスタマーゲートウェイと仮想プライベートゲートウェイの間でVPNを構築するため、サイト間のVPN接続を下記の通りで作成します。

※VPN接続を作成すると利用料金が発生します※ 利用料金の説明 [→こちら](#)

名前タグ : aws-vpn-test ※任意の名前

ターゲットゲートウェイタイプ : 仮想プライベートゲートウェイ

仮想プライベートゲートウェイ : 作成した仮想プライベートゲートウェイを選択

カスタマーゲートウェイ : 既存

カスタマーゲートウェイID : 作成したカスタマーゲートウェイを選択

ルーティングオプション : 静的

静的IPプレフィックス : ローカルネットワーク (192. 168. 1. 0/24)、CMLのLAN (172. 16. 0. 0/24) を追加

## VPN 接続の作成

VPN 接続を使用して接続するターゲットゲートウェイとカスタマーゲートウェイを選択します。ターゲットゲートウェイの情報を入力済みである必要があります。

名前タグ
aws-vpn-test

ターゲットゲートウェイタイプ
☒ 仮想プライベートゲートウェイ
☐ Transit Gateway

仮想プライベートゲートウェイ\*
vgw-

カスタマーゲートウェイ
☒ 既存
☐ 新規

カスタマーゲートウェイ ID\*
cgw-

ルーティングオプション
☐ 動的 (BGP が必要)
☒ 静的

静的 IP プレフィックス
IP プレフィックス
ソース
状態

192.168.1.0/24	-	-	✕
172.16.0.0/24	-	-	✕

別のルールの追加

トンネル内部 IP バージョン
☒ IPv4
☐ IPv6

トンネルオプションは設定変更不要です。

### トンネルオプション

CIDR 内のトンネルと VPN トンネルの事前共有キーをカスタマイズします。未指定のトンネルオプションは、Amazon によってランダムに生成されます。

トンネル 1 の内部 IPv4 CIDR
Amazon による生成

トンネル 1 の事前共有キー
Amazon による生成

トンネル 2 の内部 IPv4 CIDR
Amazon による生成

トンネル 2 の事前共有キー
Amazon による生成

トンネル 1 の詳細オプション
☒ デフォルトオプションを使用
☐ トンネル 1 オプションを編集

トンネル 2 の詳細オプション
☒ デフォルトオプションを使用
☐ トンネル 2 オプションを編集

このステップを完了すると、VPN 接続料金が発生します。 [料金を表示](#)

作成したVPN接続を確認します。

「詳細」タブで、「仮想プライベートゲートウェイ」と「カスタマーゲートウェイ」と「カスタマーゲートウェイアドレス(ローカル側のグローバルIPアドレス)」が正しく設定されていることを確認します。





「トンネル詳細」タブで、トンネルの設定を確認します。

AWSのVPN接続では、冗長化のためにデフォルトで2つのトンネルが作成されます。

外部IPアドレスは「グローバルIPアドレス」、トンネルインターフェースのIPアドレスは「リンクローカルアドレス」が利用されます。



「静的ルート」タブで、ローカルネットワーク(192.168.1.0/24)、CMLのLAN(172.16.0.0/24)が「使用可能」となっていることを確認します。



これで、AWSサイト間VPN接続のためのAWSのVPN構築は完了です！



