

AWSサイト間VPNの構築（1.AWSの基本設定）

AWS



AWSサイト間VPNの構築 （1.AWSの基本設定）

2021.08.11 2021.08.10

[【次回】AWSサイト間VPNの構築（2.AWSのEC2構築）](#)

AWSサイト間VPN接続とは

VPN(Virtual Private Network)とは、インターネットをはじめとする共用のネットワーク上に仮想的な専用線を構築し、セキュアな通信を実現するための技術です。AWSサイト間VPN(AWS Site-to-Site VPN)は、「ローカル環境(オンプレミス環境等)」と「AWSのVPC」との間でVPNを構築し、相互のLAN同士の通信を可能にします。

AWSサイト間VPNの接続料金

AWSのサイト間VPNの接続料金は以下の通りとなっています。(2021年8月現在)

1時間あたり5円程度のため、1日120円ほどで検証環境を構築することが可能です。検証が終わった後は、AWS上のVPN接続を削除することを忘れないようにしましょう。

[製品](#) / [ネットワーキングとコンテンツ配信](#) / [AWS VPN](#) / ...

AWS VPN の料金

AWS サイト間 VPN および Accelerated サイト間 VPN への接続料金

Amazon VPC への AWS サイト間 VPN 接続を作成した場合、VPN 接続をプロビジョニングして利用可能となっている各 VPN 接続時間に対してお支払いいただきます。1 時間に満たない VPN 接続時間も 1 時間とみなして課金されます。また、VPN 接続を介して転送されるすべてのデータに対しても、標準的な AWS データ転送料金が発生します。VPN 接続に対する課金を止めるには、AWS マネジメントコンソール、コマンドラインインターフェイス、または API を使用して VPN 接続を削除します。

リージョン: アジアパシフィック (東京) ⇅

サイト間 VPN 接続ごとに 0.048USD/時間

AWS サイト間 VPN でのデータ転送には、[EC2 オンデマンド料金ページ](#)で説明されているデータ転送料金が発生します。

また、EC2のデータ転送料金が発生しますが、1GBまでは無料となっています。

データ転送

以下の料金は、Amazon EC2 に「受信 (イン)」/「送信 (アウト)」されるデータ転送量を基にしています。

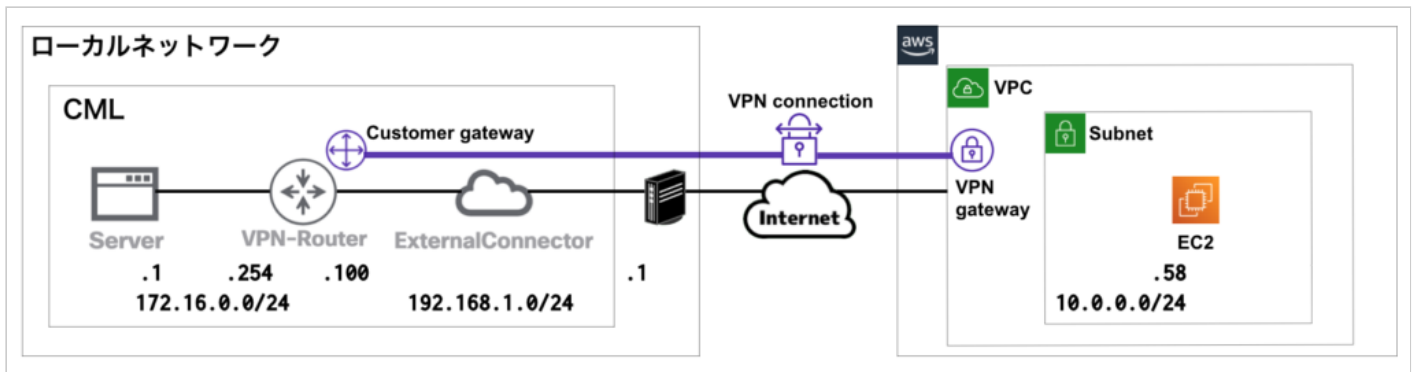
リージョン: アジアパシフィック (東京) ⇅

	料金
インターネットから Amazon EC2 へのデータ転送 (イン)	
すべてのデータ受信	0.00USD/GB
Amazon EC2 からインターネットへのデータ転送 (アウト)	
1 GB/月まで	0.00USD/GB
次の 9.999 TB/月	0.114USD/GB
次の 40 TB/月	0.089USD/GB
次の 100 TB/月	0.086USD/GB
150 TB/月以上	0.084USD/GB

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の基本設定

ここでは、検証用にAWS上で、VPC・インターネットゲートウェイ・ルートテーブル・サブネットを作成/設定していきます。

VPCの作成

検証用のVPCを作成します。

「aws-vpn-test」という名前で作成し、「10.0.0.0/16」のCIDRブロックを割り当てています。

VPC > お使いの VPC > VPC を作成

VPC を作成 情報

VPC は、Amazon EC2 インスタンスなどの AWS オブジェクトによって使用される AWS クラウドの分離された部分です。

VPC の設定

名前タグ - オプション
「Name」というキーと、指定した値を使用してタグを作成します。

aws-vpn-test

IPv4 CIDR ブロック 情報

10.0.0.0/16

IPv6 CIDR ブロック 情報

☒ IPv6 CIDR ブロックなし
☐ Amazon 提供の IPv6 CIDR ブロック
☐ IPv6 CIDR 所有 (ユーザー所有)

テナンシー 情報

デフォルト

インターネットゲートウェイの作成

インターネット経由でVPNを構築するため、インターネットゲートウェイを作成します。

「aws-vpn-test-igw」という名前で作成しています。

VPC > インターネットゲートウェイ > インターネットゲートウェイの作成

インターネットゲートウェイの作成 情報

インターネットゲートウェイは、VPC をインターネットに接続する仮想ルーターです。新しいインターネットゲートウェイを作成するには、ゲートウェイの名前を以下から指定します。

インターネットゲートウェイの設定

名前タグ
「Name」というキーと、指定した値を使用してタグを作成します。

タグ - オプション

タグは、AWS リソースに割り当てるラベルです。各タグはキーとオプションの値で構成されています。タグを使用してリソースを検索およびフィルタリングしたり、AWS のコストを追跡したりできます。

キー

値 - オプション

削除

新しいタグを追加

さらに 49 個の タグ を追加できます。

キャンセル

インターネットゲートウェイの作成

作成したインターネットゲートウェイをVPCにアタッチします。

「アクション」→「VPCにアタッチ」を選択します。

VPC > インターネットゲートウェイ > igw-

igw- / aws-vpn-test-igw

詳細 情報

インターネットゲートウェイ ID
igw-

状態
Detached

VPC ID
-

所有者

アクション ▲
VPC にアタッチ
VPC からデタッチ
タグを管理
削除

タグ

タグを管理

< 1 > ⌂

Key	Value
Name	aws-vpn-test-igw

作成したVPCを選択し、「インターネットゲートウェイのアタッチ」をクリックします。

VPC > インターネットゲートウェイ > VPC にアタッチ (igw-)

VPC にアタッチ (igw-) 情報

VPC
インターネットゲートウェイを VPC にアタッチし、VPC がインターネットと通信することを有効にします。アタッチする VPC を以下で指定してください。

使用可能な VPC
インターネットゲートウェイをこの VPC にアタッチします。

▶ AWS Command Line Interface コマンド

キャンセル **インターネットゲートウェイのアタッチ**

インターネットゲートウェイの状態が「Attached」となれば、VPCへのアタッチは完了です。

インターネットゲートウェイ igw- が正常に vpc- にアタッチされました

VPC > インターネットゲートウェイ > igw- / aws-vpn-test-igw アクション ▼

詳細 情報

インターネットゲートウェイ ID igw-	状態 Attached	VPC ID vpc- aws-vpn-test	所有者
--------------------------	-----------------------	-------------------------------	---------

タグ タグを管理

Key	Value
Name	aws-vpn-test-igw

ルートテーブルの設定

VPCのルートテーブルにインターネットゲートウェイを設定します。

VPCの画面で、メインルートテーブル(rtb-XXXXXXX)をクリックします。

The screenshot shows the AWS Management Console interface for a VPC named 'aws-vpn-test'. The '詳細' (Details) tab is selected. The VPC ID is 'vpc-...', the status is 'Available', and the IPv4 CIDR is '10.0.0.0/16'. The 'メインルートテーブル' (Main Route Table) is highlighted with a red box, showing it is associated with the VPC. Other details include 'DNS ホスト名' (DNS Hostnames) set to '無効' (Disabled), 'DNS 解決' (DNS Resolution) set to '有効' (Enabled), and 'メインネットワーク ACL' (Main Network ACL) set to 'acl-...'.

「ルート」タブを選択し、「ルート編集」をクリックします。

The screenshot shows the AWS Management Console interface for the 'ルート' (Routes) tab of the VPC 'aws-vpn-test'. The 'ルート' tab is highlighted with a red box. The 'ルート (2)' section shows a list of routes. The 'ルートを追加' (Add Route) button is highlighted with a red box. The table below shows the existing route:

送信先	ターゲット	ステータス	伝播済み
10.0.0.0/16	local	アクティブ	いいえ

「ルートを追加」をクリックします。

The screenshot shows the AWS Management Console interface for the 'ルートを追加' (Add Route) dialog box. The '送信先' (Destination) is '10.0.0.0/16', the 'ターゲット' (Target) is 'local', and the 'ステータス' (Status) is 'アクティブ'. The 'ルートを追加' button is highlighted with a red box. At the bottom, there are buttons for 'キャンセル' (Cancel), 'プレビュー' (Preview), and '変更を保存' (Save Changes).

送信先に「0.0.0.0/0」、ターゲットに「作成したインターネットゲートウェイ(igw-XXXXXXX)」を入力し、「変更を保存」をクリックします。

ルートテーブル > rtb-XXXXXXX > ルートを編集

ルートを編集

送信先	ターゲット	ステータス	伝播済み
10.0.0.0/16	local	アクティブ	いいえ
0.0.0.0/0	igw-XXXXXXX	-	いいえ

ルートを追加

キャンセル プレビュー **変更を保存**

追加したルートが表示されていれば、ルートテーブルの設定は完了です。

ルートテーブル ID: rtb-XXXXXXX

ルート (2)

送信先	ターゲット	ステータス	伝播済み
10.0.0.0/16	local	アクティブ	いいえ
0.0.0.0/0	igw-XXXXXXX	アクティブ	いいえ

サブネットの作成

EC2を配置するサブネットを作成します。

作成したVPC(aws-vpn-test)を選択します。

VPC > サブネット > サブネットを作成

サブネットを作成 情報

VPC

VPC ID

この VPC にサブネットを作成します。

vpc- [選択] (aws-vpn-test) ▼

関連付けられた VPC CIDR

IPv4 CIDR

10.0.0.0/16

「aws-vpn-test-subnet1」という名前で、CIDRブロックは「10.0.0.0/24」を割り当てます。

サブネットの設定

サブネットの CIDR ブロックとアベイラビリティゾーンを指定します。

サブネット 1 (1 個中)

サブネット名

「Name」というキーと、指定した値を使用してタグを作成します。

aws-vpn-test-subnet1

名前の長さは最大 256 文字です。

アベイラビリティゾーン [情報](#)

サブネットが存在するゾーンを選択するか、Amazon が選択するゾーンを受け入れます。

指定なし

IPv4 CIDR ブロック [情報](#)

10.0.0.0/24

▼ タグ - オプション

キー

Name

値 - オプション

aws-vpn-test-subnet1

削除

新しいタグを追加

さらに 49 個の タグ. を追加できます。

削除

新しいサブネットを追加

キャンセル

サブネットを作成

これで、AWSサイト間VPN接続のためのAWSの基本設定は完了です！