

誰でも遮断くんAMIの使い方

株式会社サイバーセキュリティクラウド

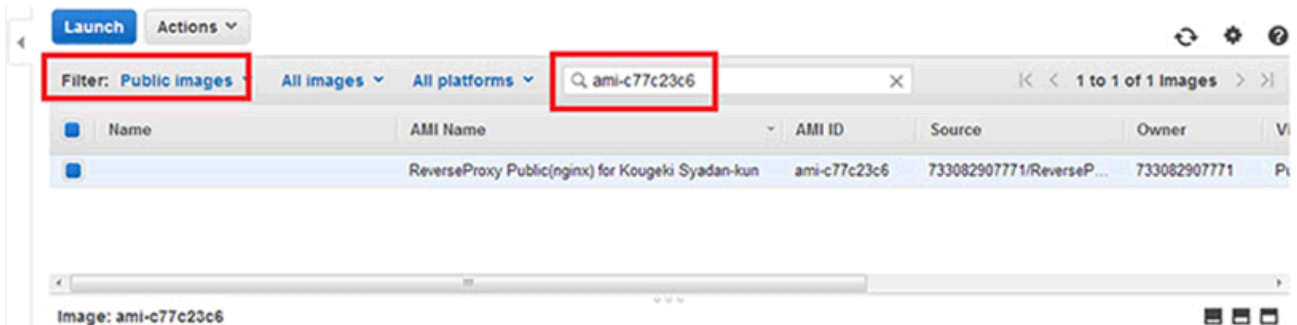
①AMIから誰でも遮断くんを起動

1.AWSマネジメントコンソールを開き、誰でも遮断くんを起動するリージョンに移動し「AMIs」を開きます。

2.該当するAMIを検索します。

Filter: Public imagesを選択し、「AMI-ID」を検索します。

(図は手順の参考例)



• AMI-ID

Asia Pacific (Tokyo) : **ami-7cc7c97d**

Asia Pacific (Singapore) : **ami-16d0fb44**

Asia Pacific (Sydney) : **ami-cb1165f1**

EU (Frankfurt) : **ami-34536329**

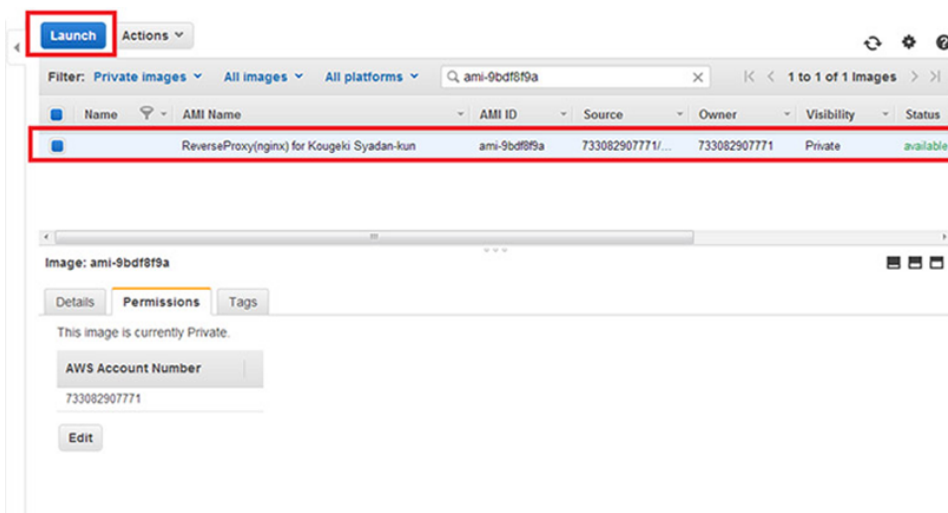
US East (N. Virginia) : **ami-f2d0b29a**

US West (Oregon) : **ami-ef90c0df**

South America (Sao Paulo) : **ami-35ce7d28**

3.表示されたAMIを選択し、「Launch」をクリックします。

AMI name: Daredemo_SyadanKun



①AMIから誰でも遮断くんを起動

4.その後、インスタンスタイプを選択し、EC2の設定を行います。

※推奨インスタンスタイプ

c3.large以上

5.SecurityGroupの設定を行います。

ベンダー推奨設定+攻撃遮断くん用設定を以下に記載します。

<Inbound>

Type	Protocol	Port range	Source
SSH	TCP	22	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
Custom UDP Rule	TCP	873	0.0.0.0/0
Custom UDP Rule	UDP	5405	0.0.0.0/0
Custom UDP Rule	UDP	1514	認証キー購入後に ※1 Sourceをお知らせします
Custom UDP Rule	UDP	1514	
Custom UDP Rule	UDP	1514	

<Outbound>

Type	Protocol	Port range	Source
All	All	All	0.0.0.0/0

Services Edit Tokyo Help

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTP	TCP	80	Anywhere 0.0.0.0/0
HTTPS	TCP	443	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	873	Anywhere 0.0.0.0/0
Custom UDP Rule	UDP	5405	Anywhere 0.0.0.0/0

Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

①AMIから誰でも遮断くんを起動

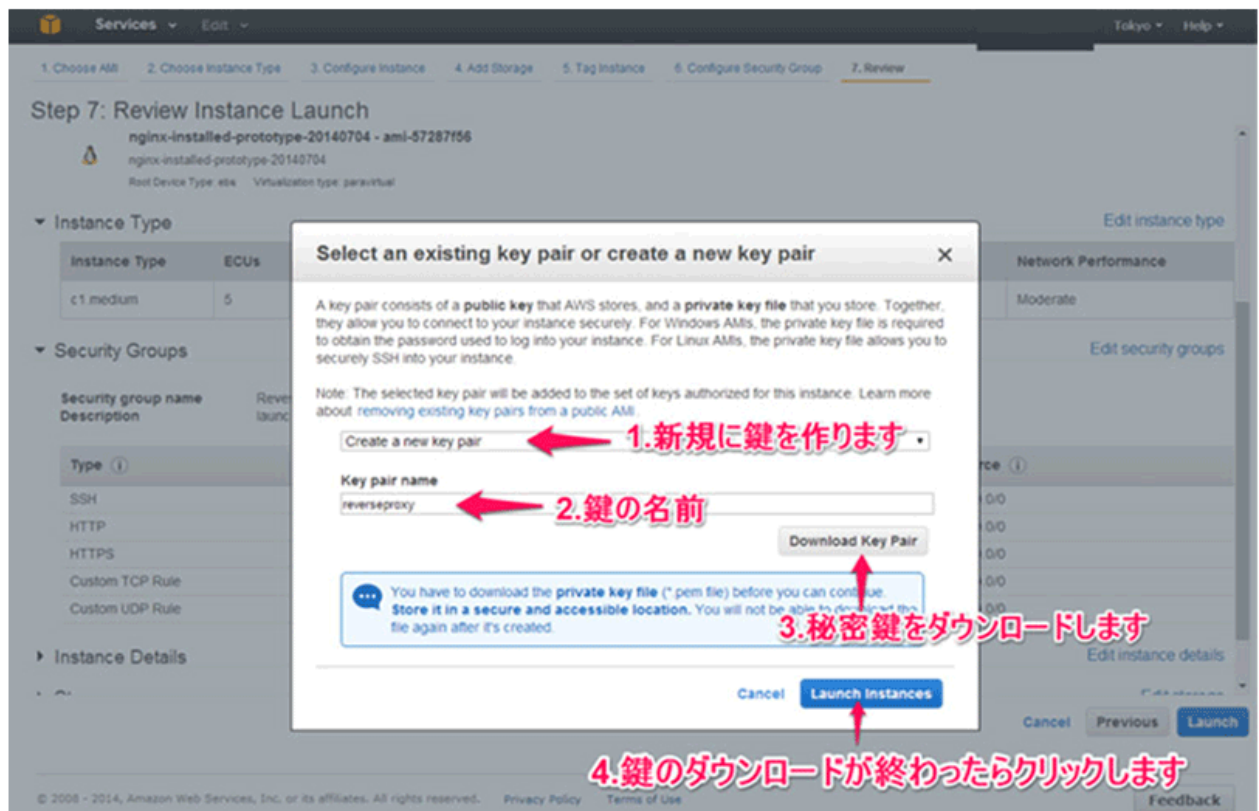
鍵の設定を行います。「Creat a new key pair」を選択し、鍵の名前を設定します。

その後、「Download Key Pair」をクリックすると秘密鍵をダウンロードできます。

鍵のダウンロードが終わったら「Launch instances」をクリックして誰でも遮断くんを起動させてください。

※ここでダウンロードした鍵ファイルは2度とダウンロードすることはできません。

誤って削除しないよう、ご注意ください。



起動した誰でも遮断くんには、必ずEIPを設定してください。

※UIPを設定しないと、攻撃遮断くんを設定することができません。

以上でAMIを使用した誰でも遮断くんの起動は完了です。

②nginxのセットアップ方法

ELB+EC2複数台の場合のnginxセットアップ方法①

1.起動した誰でも遮断くんインスタンスにログインし、 root にスイッチします。

2.SSLを使用する場合（httpsを使用する場合）は、**ELBに設置したものと同一の証明書、秘密鍵ファイルを以下のディレクトリに設置**します。

※nginxのコンフィグ内のデフォルトのディレクトリは以下の通りです。

※ファイル名は一例です

証明書：/etc/nginx/conf.d/ssl/hogehoge.com.crt

秘密鍵：/etc/nginx/conf.d/ssl/hogehoge.com.key

3.以下のコマンドを実行し。対話型設定スクリプトを実行します。

```
# cd /home/ec2-user/nginx/nginx-setting-scripts/
```

```
# ./set-dns.sh
```

4.「設定するプロトコルを選択してください。 1.HTTP, 2.HTTPS, 3.HTTP&HTTPS」と表示されるので、使用するプロトコルの番号を入力し、Enterキーを押します。

例)3 [Enter]

5.「内部管理用ホスト名を入力してください。」と表示されるので、内部管理用のホスト名を記載しEnterキーを押します。※nginxの設定ファイルなどに使用されますが、任意の名称を記載してください。

例) hogehoge.com.host-001 [Enter]

6.「IPアドレス、またはFQDNを入力してください。」と表示されるので、**ELBのPublic DNS名**を入力し、Enterキーを押します。

例) unknown-0000000000.ap-northeast-1.elb.amazonaws.com

7.「転送対象のURLを入力してください。※http://やhttps://は省略してください。」と表示されるので、転送対象のURLを記入し、Enterを押します。

例) www.hogehoge.com

②nginxのセットアップ方法

ELB+EC2複数台の場合のnginxセットアップ方法②

8.(4)で 2または3を選択した場合、「証明書ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書ファイル名の場合】 hoge.hoge.com.crt

9.(4)で 2または3を選択した場合、「証明書鍵ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書鍵ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書鍵ファイル名の場合】 hoge.hoge.com.key

10. 「nginx: the configuration file /etc/nginx/nginx.conf syntax is ok」 「nginx: configuration file /etc/nginx/nginx.conf test is successful」

「エラーが発生していない場合、次のコマンドでNGINXの設定を再読み込みしてください。」

と表示されることを確認する。

※エラーが発生している場合は、nginxが表示したメッセージから修正対応を行う

11.Nginxの設定をリロードする

```
# service nginx reload
```

12.IPアドレス、またはPublic DNSからアクセスし、正しくWEBページが表示されることを確認します。問題なく表示されれば、nginxの設定は完了です。

②nginxのセットアップ方法

アプライアンス型LBがある場合のnginxセットアップ方法①

1.起動した誰でも遮断くんインスタンスにログインし、 root にスイッチします。

2.SSLを使用する場合（httpsを使用する場合）は、**転送先サーバーに設置したものと同一の証明書、秘密鍵ファイルを以下のディレクトリに設置**します。

※nginxのコンフィグ内のデフォルトのディレクトリは以下の通りです。

※ファイル名は一例です

証明書：/etc/nginx/conf.d/ssl/hogehoge.com.crt

秘密鍵：/etc/nginx/conf.d/ssl/hogehoge.com.key

3.以下のコマンドを実行し。対話型設定スクリプトを実行します。

```
# cd /home/ec2-user/nginx/nginx-setting-scripts/
```

```
# ./set-dns.sh
```

4.「設定するプロトコルを選択してください。 1.HTTP, 2.HTTPS, 3.HTTP&HTTPS」と表示されるので、使用するプロトコルの番号を入力し、Enterキーを押します。

例)3 [Enter]

5.「内部管理用ホスト名を入力してください。」と表示されるので、内部管理用のホスト名を記載しEnterキーを押します。

※nginxの設定ファイルなどに使用されますが、任意の名称を記載してください。

例) hogehoge.com.host-001 [Enter]

②nginxのセットアップ方法

アプライアンス型LBがある場合のnginxセットアップ方法②

6. 「IPアドレス、またはFQDNを入力してください。」と表示されるので、**ロードバランサーのIPアドレス、またはFQDN**を入力し、Enterキーを押します。

例) 123.45.67.xxx

7. 「転送対象のURLを入力してください。※http://やhttps://は省略してください。」と表示されるので、転送対象のURLを記入し、Enterを押します。

例) www.hogehoge.com

8.(4)で 2または3を選択した場合、「証明書ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書ファイル名の場合】 hogehoge.com.crt

9.(4)で 2または3を選択した場合、「証明書鍵ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書鍵ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書鍵ファイル名の場合】 hogehoge.com.key

「nginx: the configuration file /etc/nginx/nginx.conf syntax is ok」

「nginx: configuration file /etc/nginx/nginx.conf test is successful」

「エラーが発生していない場合、次のコマンドでNGINXの設定を再読み込みしてください。」

と表示されることを確認する。

※エラーが発生している場合は、nginxが表示したメッセージから修正対応を行う

Nginxの設定をリロードする

```
# service nginx reload
```

IPアドレス、またはPublic DNSからアクセスし、正しくWEBページが表示されることを確認します。

問題なく表示されれば、nginxの設定は完了です。

②nginxのセットアップ方法

LBがない場合、または共用サーバを用いている場合のnginxセットアップ方法①

1.起動した誰でも遮断くんインスタンスにログインし、 root にスイッチします。

2.SSLを使用する場合（httpsを使用する場合）は、**転送先サーバーに設置したものと同一の証明書、秘密鍵ファイルを以下のディレクトリに設置**します。

※nginxのコンフィグ内のデフォルトのディレクトリは以下の通りです。

※ファイル名は一例です

証明書：/etc/nginx/conf.d/ssl/hogehoge.com.crt

秘密鍵：/etc/nginx/conf.d/ssl/hogehoge.com.key

3.以下のコマンドを実行し。対話型設定スクリプトを実行します。

```
# cd /home/ec2-user/nginx/nginx-setting-scripts/
```

```
# ./set-dns.sh
```

4.「設定するプロトコルを選択してください。 1.HTTP, 2.HTTPS, 3.HTTP&HTTPS」と表示されるので、使用するプロトコルの番号を入力し、Enterキーを押します。

例)3 [Enter]

5.「内部管理用ホスト名を入力してください。」と表示されるので、内部管理用のホスト名を記載しEnterキーを押します。

※nginxの設定ファイルなどに使用されますが、任意の名称を記載してください。

例) hogehoge.com.host-001 [Enter]

6.「IPアドレス、またはFQDNを入力してください。」と表示されるので、**ロードバランサーのIPアドレス、またはFQDN**を入力し、Enterキーを押します。

例) 123.45.67.xxx

7.「転送対象のURLを入力してください。※http://やhttps://は省略してください。」と表示されるので、転送対象のURLを記入し、Enterを押します。

例) www.hogehoge.com

②nginxのセットアップ方法

LBがない場合、または共用サーバを用いている場合のnginxセットアップ方法②

8.(4)で 2または3を選択した場合、「証明書ファイル名を入力してください。
※拡張子も含めて入力してください。」と表示されるので、(2)で設置した
証明書ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書ファイル名の場合】 hoge hoge.com.crt

9.(4)で 2または3を選択した場合、「証明書鍵ファイル名を入力してください。
※拡張子も含めて入力してください。」と表示されるので、(2)で設置
した証明書鍵ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書鍵ファイル名の場合】 hoge hoge.com.key

10. 「nginx: the configuration file /etc/nginx/nginx.conf syntax is
ok」 「nginx: configuration file /etc/nginx/nginx.conf test is
successful」

「エラーが発生していない場合、次のコマンドでNGINXの設定を再読み込
みしてください。」

と表示されることを確認する。

※エラーが発生している場合は、nginxが表示したメッセージから修正対応
を行う

11. 転送先WEBサーバーが複数台ある場合は、以下の対応を行います。

vi /etc/nginx/conf.d/default.conf

```
upstream backend.hostname {  
server xxx.xxx.xxx.xxx:80;  
server yyy.yyy.yyy.yyy:80; } ← upstream backend. hostname内にserverの設定を  
追加  
※hostnameは(5)で設定した管理用ホスト名
```

※SSLを使用する場合は以下の対応も実施

vi /etc/nginx/conf.d/default_ssl.conf

```
upstream backend.hostname ssl{  
server xxx.xxx.xxx.xxx:80;  
server yyy.yyy.yyy.yyy:80; } ← upstream backend. hostname ssl内にserverの設  
定を追加  
※hostnameは(5)で設定した管理用ホスト名
```

②nginxのセットアップ方法

LBがない場合、または共用サーバを用いている場合のnginxセットアップ方法③

12.Nginxの設定をリロードする

```
# service nginx reload
```

13.IPアドレス、またはPublic DNSからアクセスし、正しくWEBページが表示されることを確認します。

問題なく表示されれば、nginxの設定は完了です。

②nginxのセットアップ方法

VirtualHostを設定している場合のnginxセットアップ方法①

※nginxの設定方法に関する内容となるため、あくまで参考レベルとする

1.起動した誰でも遮断くんインスタンスにログインし、 root にスイッチします。

2.SSLを使用する場合（httpsを使用する場合）は、ELBに設置したものと同一の証明書、秘密鍵ファイルを以下のディレクトリに設置します。

※nginxのコンフィグ内のデフォルトのディレクトリは以下の通りです。

※ファイル名は一例です

証明書：/etc/nginx/conf.d/ssl/hogehoge.com.crt

秘密鍵：/etc/nginx/conf.d/ssl/hogehoge.com.key

3.以下のコマンドを実行し。対話型設定スクリプトを実行します。

```
# cd /home/ec2-user/nginx/nginx-setting-scripts/
```

```
# ./set-dns.sh
```

4.「設定するプロトコルを選択してください。 1.HTTP, 2.HTTPS, 3.HTTP&HTTPS」と表示されるので、使用するプロトコルの番号を入力し、Enterキーを押します。

例)3 [Enter]

5.「内部管理用ホスト名を入力してください。」と表示されるので、内部管理用のホスト名を記載しEnterキーを押します。

※nginxの設定ファイルなどに使用されますが、任意の名称を記載してください。

例) hogehoge.com.host-001 [Enter]

6.「IPアドレス、またはFQDNを入力してください。」と表示されるので、ELBのPublic DNS名、またはロードバランサー、転送先サーバーのIPアドレスまたはFQDNを入力し、Enterキーを押します。

例) unknown-0000000000.ap-northeast-1.elb.amazonaws.com

②nginxのセットアップ方法

VirtualHostを設定している場合のnginxセットアップ方法②

7.「転送対象のURLを入力してください。※http://やhttps://は省略してください。」と表示されるので、転送対象のURLを記入し、Enterを押します。

例) www.hogehoge.com

8.(4)で 2または3を選択した場合、「証明書ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書ファイル名の場合】 hogehoge.com.crt

8.(4)で 2または3を選択した場合、「証明書鍵ファイル名を入力してください。※拡張子も含めて入力してください。」と表示されるので、(2)で設置した証明書鍵ファイル名を入力し、Enterを押します。

例) 【(2)で記載した証明書鍵ファイル名の場合】 hogehoge.com.key

10.「Nginx: the configuration file /etc/nginx/nginx.conf syntax is ok」「Nginx: configuration file /etc/nginx/nginx.conf test is successful」

「エラーが発生していない場合、次のコマンドでNGINXの設定を再読み込みしてください。」

と表示されることを確認する。

※エラーが発生している場合は、nginxが表示したメッセージから修正対応を行う

11.Nginxの設定をリロードする

```
# service nginx reload
```

12.Virtualhostの設定を行うため、再度(2)の手順から実施します。

※(6)のIPアドレス、FQDNは同じ設定で(7)の転送先URLが異なる設定となる

13.IPアドレス、またはPublic DNSからアクセスし、正しくWEBページが表示されることを確認します。

問題なく表示されれば、nginxの設定は完了です。

③攻撃遮断くんの認証キーセットアップ方法

認証キー購入後に、セットアップ方法をお知らせします。

④DNS情報の変更

ご利用のDNSサービスにて、対象WEBサイトのURLへ設定を行います。
A record (誰でも遮断くんのIPアドレス)、または C record (誰でも遮断くんのホスト名) を用い、今回作成した誰でも遮断くんへ転送されるようレコード設定を行ってください。

DNS情報が反映され次第、URLにアクセスし接続状態を確認します。

問題がなければ、誰でも遮断くんAMIを利用した、クラウド型WAFのセットアップは完了です。