

# AWS EC2 でVPNサーバーを建てる

[ツイート](#)[シェア](#)[B! はてな](#)

新型コロナウイルス(COVID-19)の影響でリモートワークになった企業が多いのではないのでしょうか。

弊社もリモートワークになりました。

そしてそのときに問題になるのが、会社のIPからしか接続を許可していないサービスにどのようにアクセスさせるかという問題です。

弊社はアルバイトの学生が多く勤務しています。

会社にVPNを用意していますが、学生アルバイトの分までアカウントが用意できていないなどの問題があります。

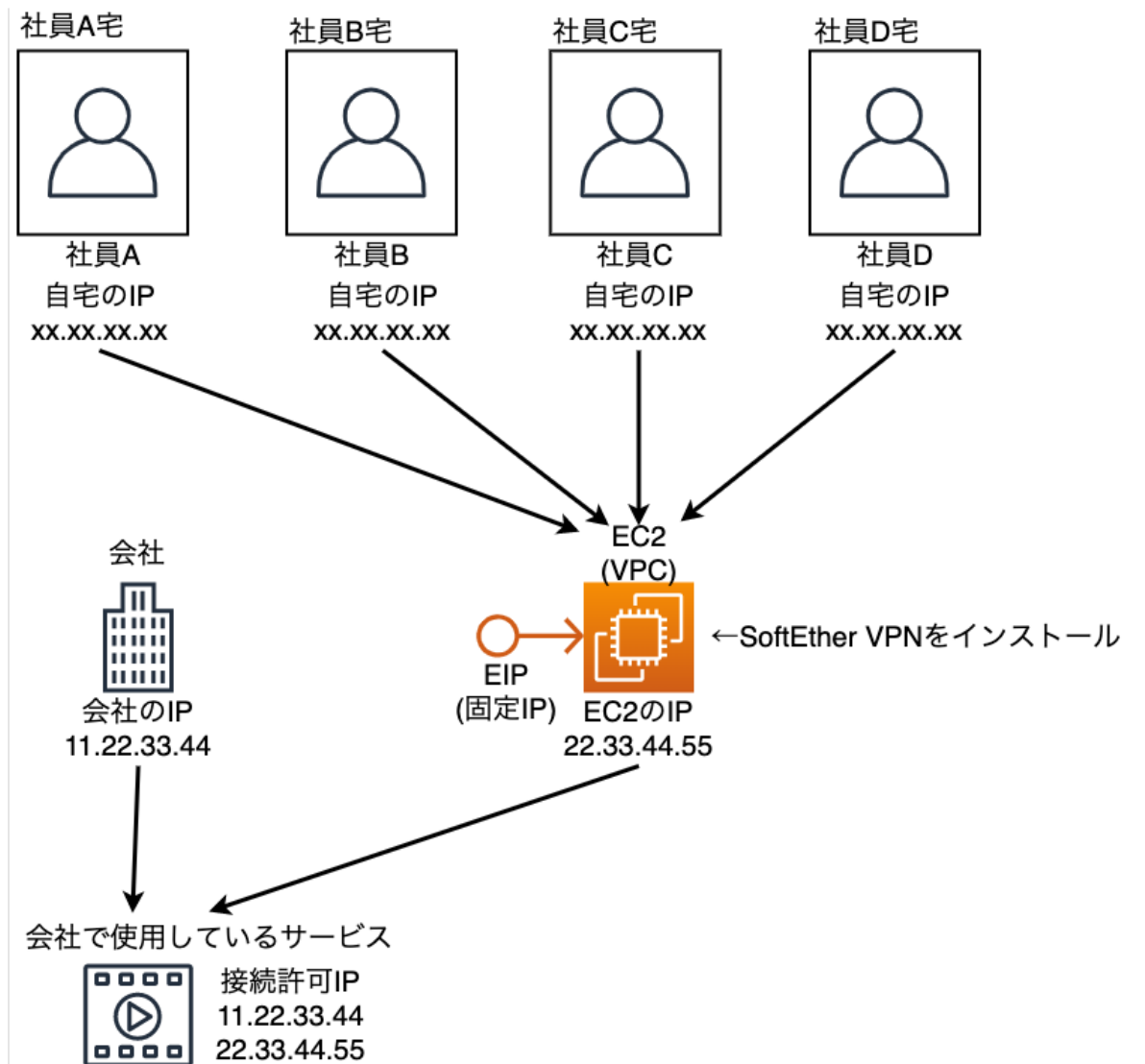
タスク管理ソフトなどにはIP制限をしているので指定のIPからしか接続できません。

そして家庭用のルータは固定IPではないことが多いです。

勤務前に毎回許可依頼をするのも手がかかるなーと思ったので、AWS EC2上にVPNサーバーを建ててそこからアクセスさせるようにすれば、許可するIPは一つだけで済みますね。

やっていきましょう。

どのような構成かという図の通りです。



各社員・アルバイトの家からEC2上に建てたVPNサーバーを経由してアクセスさせます。

このようにすることで、EC2インスタンスのIPでアクセスすることが可能になっています。

EC2にSoftEther VPNをインストールしていきます

## AWSコンソールの設定

### VPCの作成

まずはVPCの設定を行います。

VPCを新規作成します。

- 名前タグ : SoftEther-VPN(自由です)

- PV4 CIDR : 10.0.0.0/16

サブネットを作成します。

- 名前タグ : SoftEther-VPN(自由です)
- VPN : 先程作成した SoftEther を指定します
- アベイラビリティゾーン : 今回はap-northeast-1aを指定します
- IPv4 CIDR ブロック : 10.0.32.0/20

インターネットゲートウェイを作成します。

- 名前タグ : SoftEther-VPN (自由です)

作成したらVPCをアタッチしましょう

つぎにルートテーブルを作成します

- 送信先 : 10.0.0.0/16 | ターゲット : local (これは設定されているはずです)
- 送信先 : 0.0.0.0/0 | ターゲット : igw-xxxxxxx (先程設定したインターネットゲートウェイ)

## EC2サーバを作成

Amazon Linux2 の t2.micro で作成しました。(インスタンスタイプは使用人数が多いなら、スペックを上げたほうがいいかもしれません)

VPCに先程作成したSoftEther-VPNを設定します

あとは特に気にすることはないと思います

セキュリティグループに以下を割り当てます

タイプ	プロトコル	ポート範囲	ソース	説明(任意)
SSH	TCP	22	今使用しているIP/32	ssh for TOWN

タイプ	プロトコル	ポート範囲	ソース	説明(任意)
カスタムUDPルール	UDP	4500	0.0.0.0/0	VPN
カスタムUDPルール	UDP	500	0.0.0.0/0	VPN

作成できたらElasticIPを振りましょう

## sshする

sshでアクセスしてタイムゾーンの設定や、必要なパッケージをインストールします

```
sudo timedatectl set-timezone Asia/Tokyo
sudo yum -y update
sudo yum -y install git gcc ncurses-devel readline-devel openssl-devel zsh
```

次にSoftEther VPNをインストールします。

```
$ curl -L -O https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/releases
$ tar xvzf softether-src-v4.32-9731-beta.tar.gz
$ cd v4.32-9731
$ ./configure
$ make
$ sudo make install
```

-----  
Installation completed successfully.

Execute 'vpnserv start' to run the SoftEther VPN Server background service  
Execute 'vpnbridge start' to run the SoftEther VPN Bridge background service  
Execute 'vpncclient start' to run the SoftEther VPN Client background service  
Execute 'vpncmd' to run SoftEther VPN Command-Line Utility to configure \

最後の **Installation completed successfully.** がでていれば成功です。

systemdの起動スクリプトを作成します。

```
$ sudo vim /etc/systemd/system/vpnserver.service
```

```
[Unit]
```

```
Description=Softether VPN Server Service
```

```
After=network.target
```

```
[Service]
```

```
Type=forking
```

```
User=root
```

```
ExecStart=/usr/bin/vpnserver start
```

```
ExecStop=/usr/bin/vpnserver stop
```

```
Restart=on-abort
```

```
WorkingDirectory=/opt/vpnserver/
```

```
ExecStartPre=/sbin/ip link set dev eth0 promisc on
```

```
[Install]
```

設置場所を変更し、パーミッション割当、起動ファイル読み込み、起動、自動起動を設定します。

```
sudo mv v4.32-9731 /opt/vpnserver
```

```
sudo chmod 755 /etc/systemd/system/vpnserver.service
```

```
sudo systemctl daemon-reload
```

```
sudo systemctl start vpnserver
```

```
sudo systemctl enable vpnserver
```

## SoftEtherの設定

sshしたまま設定をしていきます  
仮想HUB、ユーザーの追加を行います

```
$ sudo vpncmd  
vpncmd コマンド - SoftEther VPN コマンドライン管理ユーティリティ  
SoftEther VPN コマンドライン管理ユーティリティ (vpncmd コマンド)  
Version 4.32 Build 9731 (Japanese)  
Compiled 2020/01/01 17:54:10 by buildsan at crosswin  
Copyright (c) SoftEther VPN Project. All Rights Reserved.
```

vpncmd プログラムを使って以下のことができます。

1. VPN Server または VPN Bridge の管理
2. VPN Client の管理
3. VPN Tools コマンドの使用 (証明書作成や通信速度測定)

1を選択します。

次にアドレスを聞かれますので先程関連付けたインスタンスのEIPを入力します

1 - 3 を選択: 1

接続先の VPN Server または VPN Bridge が動作しているコンピュータの IP アドレス  
'ホスト名:ポート番号' の形式で指定すると、ポート番号も指定できます。  
(ポート番号を指定しない場合は 443 が使用されます。)  
何も入力せずに Enter を押すと、localhost (このコンピュータ) のポート 443 に接続  
接続先のホスト名または IP アドレス:xx.xx.xx.xx



仮想HUB名を聞かれるのでなにも入力せずEnterを押します

サーバーに仮想 HUB 管理モードで接続する場合は、仮想 HUB 名を入力してください。

サーバー管理モードで接続する場合は、何も入力せずに Enter を押してください。

接続先の仮想 HUB 名を入力:

VPN Server "xx.xx.xx.xx" (ポート 443) に接続しました。

VPN Server 全体の管理権限があります。

```
VPN server>
```

まずはデフォルトの仮想HUBを削除します  
HubListコマンドで確認できます。

```
HubDelete
```

```
HubDelete コマンド - 仮想 HUB の削除
```

```
削除する仮想 HUB の名前:DEFAULT
```

次に仮想HUBを作成します。  
名前は自由です。  
ここではhacknoteとしたいと思います  
パスワードはあとで使うので忘れないでください

```
VPN Server>HubCreate hacknote
```

```
HubCreate コマンド - 新しい仮想 HUB の作成
```

```
パスワードを入力してください。キャンセルするには Ctrl+D キーを押してください。
```

```
パスワード: *****
```

```
確認入力   : *****
```

```
コマンドは正常に終了しました。
```

作成済みの hacknote の管理画面に移ります

```
VPN Server>HUB hacknote
```

```
Hub コマンド - 管理する仮想 HUB の選択
```

```
仮想 HUB "hacknote" を選択しました。
```

```
コマンドは正常に終了しました。
```

```
VPN Server/hacknote>
```

IPsecEnableコマンドでL2TP/IPSecを有効にします  
この事前共有鍵もあとで使います。

```
VPN Server/hacknote>IPsecEnable /L2TP:yes /L2TPRAW:no /ETHERIP:no /DEFAULT
IPsecEnable コマンド - IPsec VPN サーバー機能の有効化 / 無効化
```

IPsec 事前共有鍵の文字列 (9 文字以下を推奨): \*\*\*\*\*

コマンドは正常に終了しました。



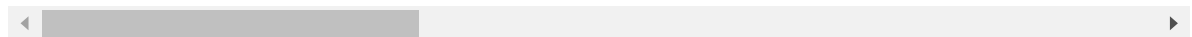
SoftEther がルーターの様に動作する機能を SecureNatEnable コマンドで有効化  
します

```
VPN Server/hacknote>SecureNatEnable
SecureNatEnable コマンド - 仮想 NAT および DHCP サーバー機能 (SecureNAT 機能)
コマンドは正常に終了しました。
```



ルーティングを設定します  
長いです。

```
VPN Server/hacknote>Dhcpset /Start:192.168.30.10 /End:192.168.30.200 /Mask:255.255.255.0
DhcpSet コマンド - SecureNAT 機能の仮想 DHCP サーバー機能の設定の変更
コマンドは正常に終了しました。
```



## VPNユーザーの追加

続いてVPNユーザーを追加とそのユーザーのパスワードを設定していきます。

ユーザー名 : user1

パスワード : HogeHoge1234 とします

```
VPN Server/hacknote>UserCreate user1 /Group:none /REALNAME:none /NOTE:none
UserCreate コマンド - ユーザーの作成
コマンドは正常に終了しました。
```



```
VPN Server/hacknote>UserPasswordSet user1 /PASSWORD:Hogehoge1234
```

UserPasswordSet コマンド - ユーザーの認証方法をパスワード認証に設定しパスワード:  
コマンドは正常に終了しました。



必要な人数分追加していきましょう

exitで抜けます

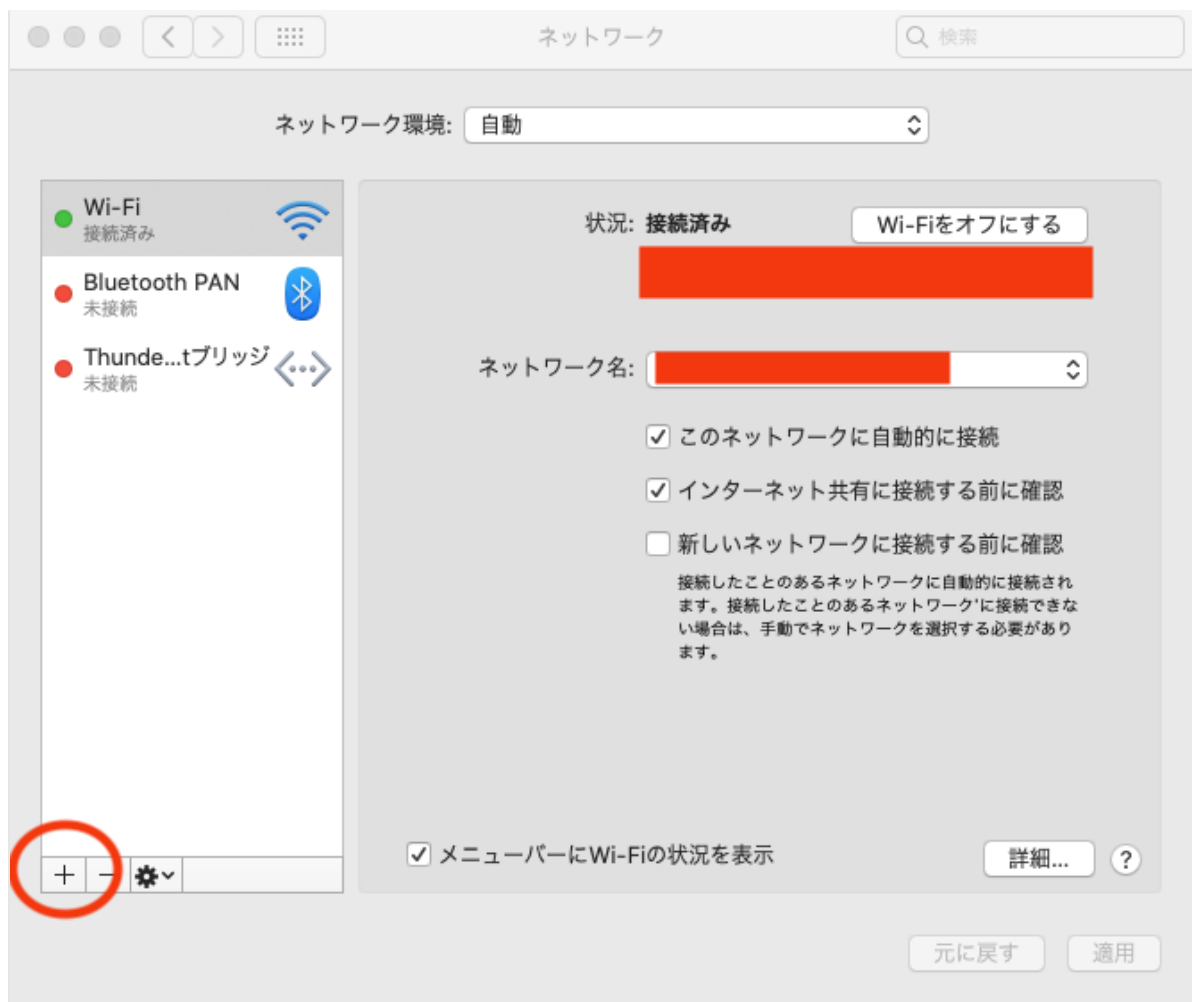
```
VPN Server/hacknote>exit
```

## クライアント設定

---

### Macの場合

画面左上のアップルのマークから システム環境設定 > ネットワーク と進みます  
右下あたりの + マークを押します



インターフェース : VPN

VPNタイプ : L2TP over IPSec

サービス名 : AWS VPN (L2TP)

とします

サービス名は自由です

インターフェースを選択し、新しいサービス名を入力してください。

インターフェース: VPN

VPNタイプ: L2TP over IPSec

サービス名: AWS VPN (L2TP)

キャンセル 作成

サーバーアドレス : ElasticIP

アカウント名 : ユーザー名@仮想HUB名

を入力します



状況: 未構成

構成: デフォルト

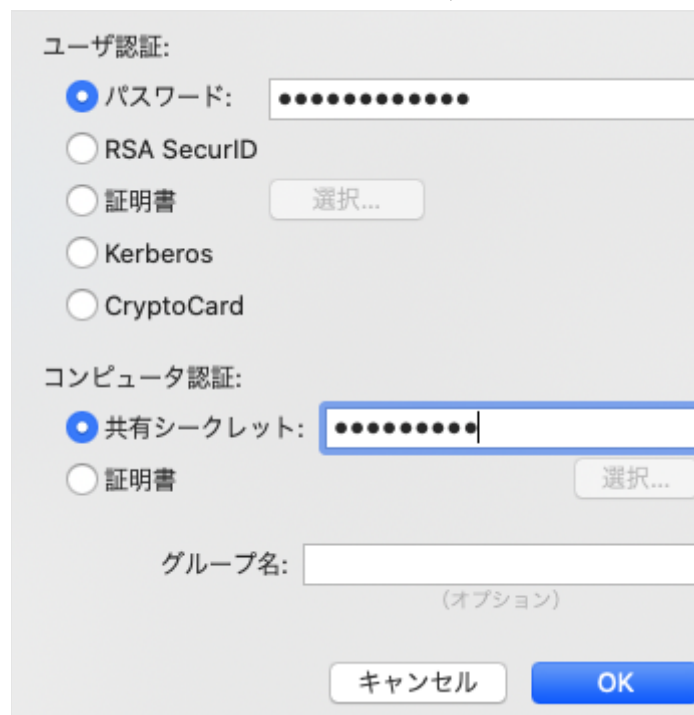
サーバアドレス: XX.XX.XX.XX

アカウント名: user1@hacknote

認証設定...

接続

認証設定を押してユーザーのパスワードと共有鍵を入力します



ユーザ認証:

☒ パスワード: .....

☐ RSA SecurID

☐ 証明書 選択...

☐ Kerberos

☐ CryptoCard

コンピュータ認証:

☒ 共有シークレット: .....|

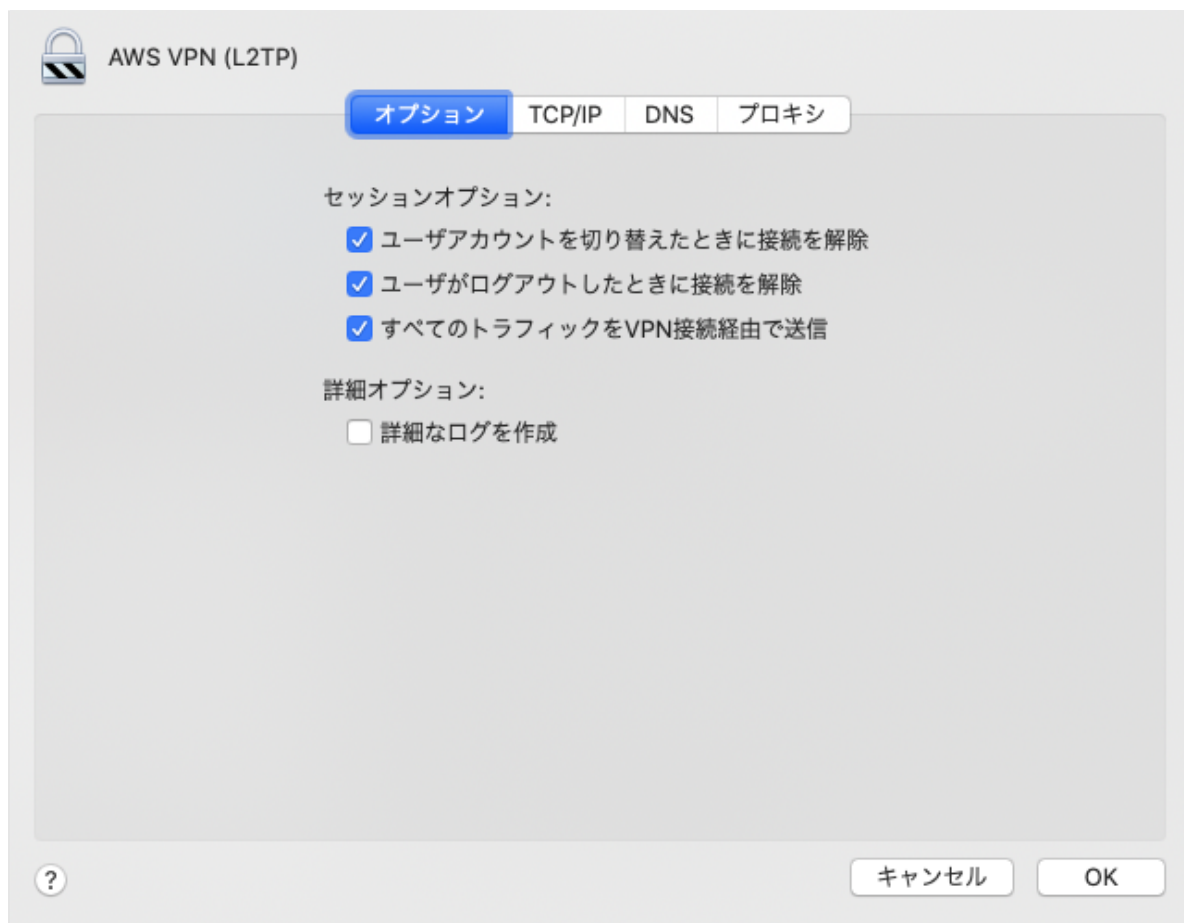
☐ 証明書 選択...

グループ名: (オプション)

キャンセル OK

詳細を押します

オプションを以下のようにします



適用を押して、接続を押します。

Google検索で whatmyip で検索して適当なサイトでIPを調べると、EIPになっているはずです！

## Windows10の場合

---

設定 > ネットワークとインターネット > VPN をクリックします

VPNを追加するをクリックします

このように入力します。

### VPN接続を追加

VPN プロバイダー

Windows (ビルトイン)

接続名

AWS VPN

サーバー名またはアドレス

Elastic IP

VPN の種類

事前共有キーを使った L2TP/IPsec

事前共有キー

●●●●●●●●

サインイン情報の種類

ユーザー名とパスワード

ユーザー名 (オプション)

パスワード (オプション)

☒ サインイン情報を保存する

保存

キャンセル

接続名：自由です

サーバーまたはIPアドレス：設定しているElastic IPを入力してください

VPNの種類：事前共有キーを使ったL2TP/IPsec

事前共有キー：先程作成した鍵

サインイン情報の種類：ユーザー名とパスワード

ユーザー名：設定したユーザー名@仮想HUB名

パスワード：ユーザー作成時のパスワード

保存を押して、作成したVPNを選択して、接続をクリックすればOKです

## あとがき

サクッとVPNサーバーを構築できたのでハッピーです

EC2はデータ通信量でも課金されるので使い方を気をつけないと、高額な請求をされますね…

BGMとしてyoutubeで音楽を聞いていたとかやると、結構な課金額かもしれませ

ん...

料金について記事を書きました => [EC2+SoftEther でのVPNサーバーの料金](#)