ディープラーニングモデルへの攻撃手法

1　目的

- ディープラーニングを利用した機械学習モデルへの主な攻撃手法と防御方法を学びます。
- AWS への Jupyter のインストール方法および実行方法を学びます。

2　アマゾン EC2 へのログイン

アマゾン EC2 にログインします。

`https://aws.amazon.com/jp/ec2/`

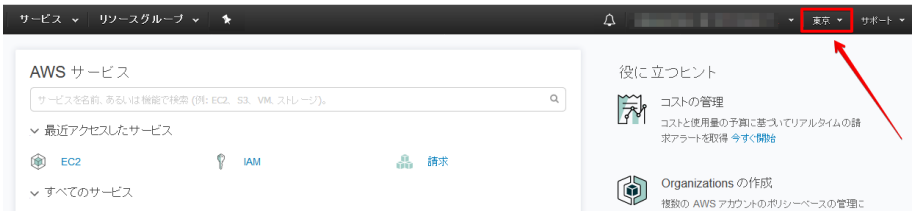
すでにアカウントがある場合

新規にアカウントをつくる場合

今回の授業では、すでにアカウントが作成されています。各自の課題提出フォルダの下に、各自の ID とパスワードが記載されたファイルがあります。そちらに記載された ID とパスワードを使ってログインして下さい。

2.1　リージョンの選択

利用するサーバのリージョンを選択します。

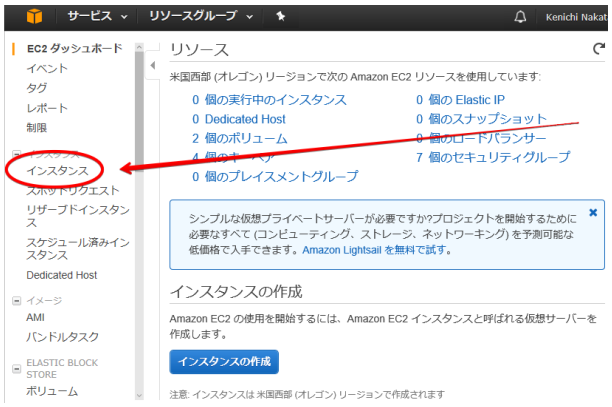


授業では、クリックして「米国東部（バージニア北部）」を選択して下さい。

EC2 サービスを選択します

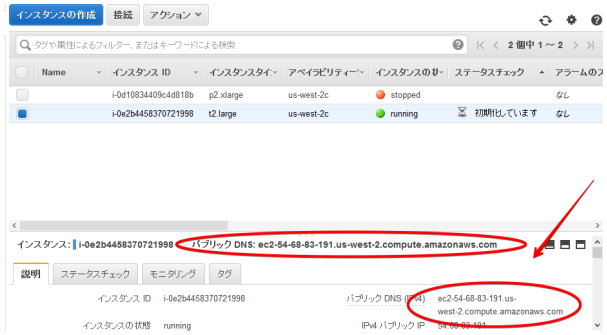
3　インスタンスの起動

以前の授業で作成した GPU 付インスタンスを作成します。授業を欠席して、作成していない人は、テキスト「アマゾン EC2 インスタンスの設定」の「インスタンスの作成」の章をみてインスタンスを作成して下さい。Putty や WinSCP のインストールや設定等を行っていない場合には、同じテキストを参照して、インストール及び設定を行って下さい。



「インスタンス」をクリックします

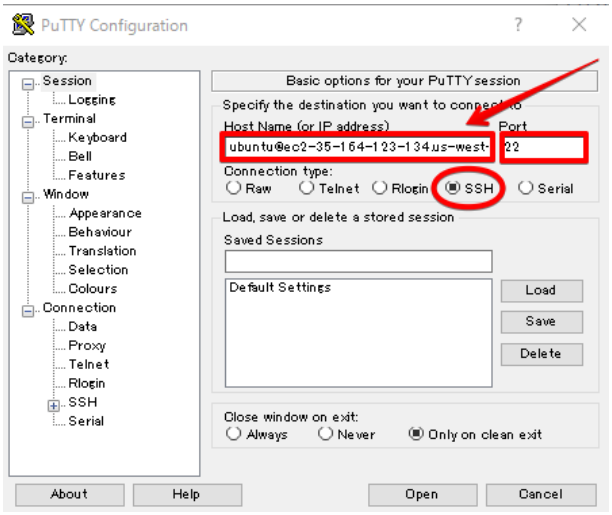
インスタンスが立ち上がっていない場合、「アクション」から「インスタンスの状態/開始」を選択し、インスタンスを立ち上げます。



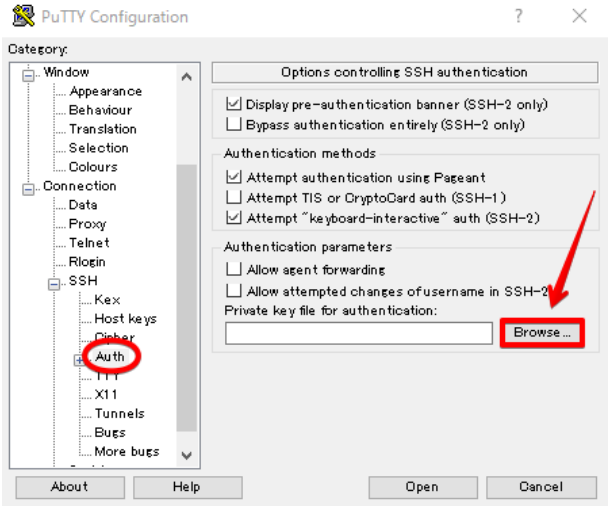
インスタンスの状態が「running」になったら、インスタンスの「パブリック DNS」を確認します。

4　PuTTY セッションの開始

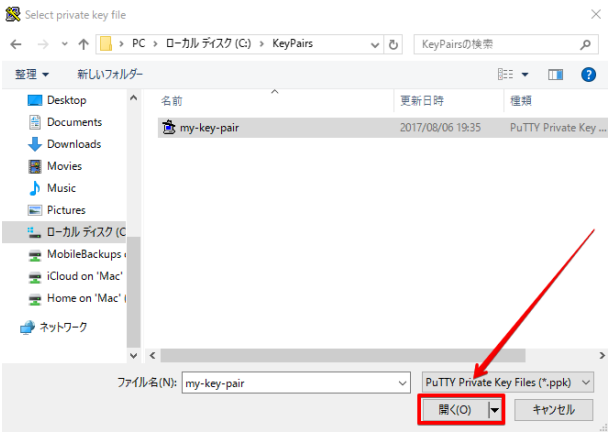
[スタート] メニューで [All Programs]-[PuTTY]-[PuTTY] を選択し、PuTTY を開始します。



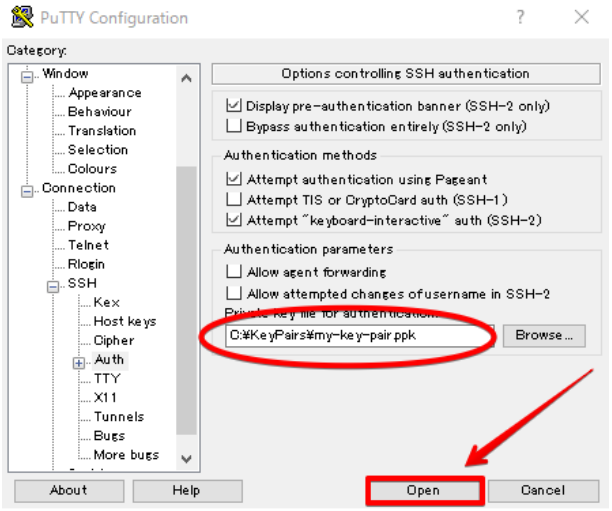
①「Host Name」に「ubuntu@(パブリック DNS)」を入力します。
②「Connection Type」を「SSH」とします。
③「Port」が「22」となっていることを確認します。



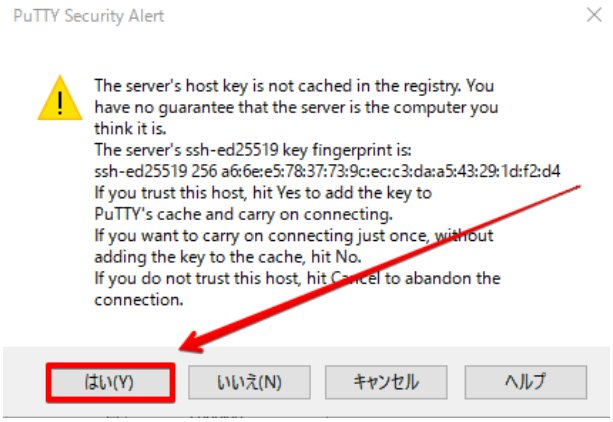
① [Category] ペインで、[Connection]、[SSH] の順に展開し、[Auth] を選択します。
②「Browse」をクリックします。



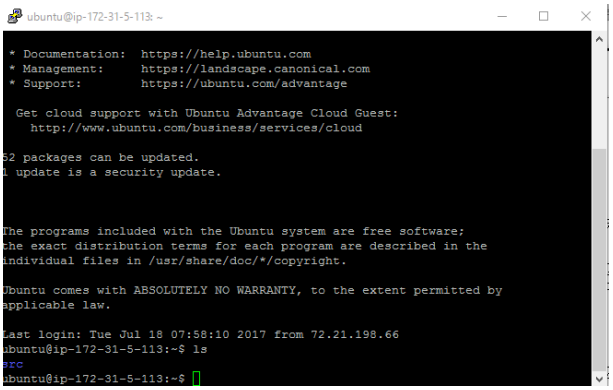
①先ほど保存した ppk ファイルを選択します。
②「開く」を押します。



①選択した ppk ファイルのパスが入力されていることを確認します。
②「Open」を押します。



「はい (Y)」を押します。



SSH クライアントでインスタンスに接続しました

5　作業用ディレクトリの作成

5.1　ツールの取得

今回は、AWS でのデフォルトの環境で作業を行いますので、環境の切り替えの必要はありません。

```
cd ~/Lesson/tools
git pull
cd ..
```

（参考　前回の事業を欠席している人は上記の変わりに、以下の通り行って下さい）

```
cd ~
mkdir Lesson
cd Lesson
git clone https://github.com/k1nk/tools.git
```

6　jupyter の設定

Jupyter Notebook (読み方は「ジュパイター・ノートブック」または「ジュピター・ノートブック」) とは、ノートブックと呼ばれる形式で作成したプログラムを実行し、実行結果を記録しながら、データの分析作業を進めるためのツールです。以前の授業で Anaconda をインストールしていますが、Anaconda をインストールすると、jupyter も合わせてインストールされます。ただし、このままでは、AWS の外部からのアクセスができません。アクセスできるようにするためには、jupyter の設定および、AWS のファイアウオールの設定が必要になります。

6.1　jupyter の設定

```
jupyter notebook --generate-config
```

jupyter notebook の設定用ファイル「 /.jupyter/jupyter_notebook_config.py」が作成されます。jupyter notebook にログインするためのパワードをを設定します。この設定ファイルにパスワードのハッシュ値を計算します。ログイン時に入力する任意のパスワードを 2 回入力し、ハッシュ値を取得してください。

```
python -c 'from notebook.auth import passwd;print(passwd())'
>>>
sha1:d1414e6ac5ff:369c16e757d9b49f15d3fad7d6399934ebad4a53
```

実際のハッシュ値は、パスワードにより上記とは異なったものとなります。ここで得られたハッシュ値を設定ファイルに記載します。外部からアクセスするために必要な設定情報も合わせて、設定ファイルに記載します。エディタで設定ファイルを開きます。

```
nano ~/.jupyter/jupyter_notebook_config.py
```

下記の設定をファイルの最後に追記します。nano は、Ctrl+w を押してから Ctrl+v を押すことによりファイルの最後に移動します。ファイルの最後の部分に下記の設定をコピー＆ペーストして下さい。ハッシュ値の部分は、実際に得られたものを記載して下さい。

```
c.IPKernelApp.pylab = 'inline'
c.NotebookApp.ip = '*'
c.NotebookApp.open_browser = False
c.NotebookApp.port = 8888
c.NotebookApp.password = u'sha1:d1414e6ac5ff:369
    c16e757d9b49f15d3fad7d6399934ebad4a53'
```

6.2 AWS のファイアウオールの設定

Amazon EC2 の管理画面にアクセスし、インスタンスの一覧を表示します。ウィンドウ下部の [説明] タブ内の [セキュリティグループ] の項目の士セキュリティグループ名をクリックします。

ここで、インバウンド／アウトバウンドについて、許可する通信を指定することができます。インバウンドでは必要最低限が許可されています。デフォルトで、「SSH(TCP ポート 22 番)」が許可されています。アウトバウンドは、デフォルトで全てのトラフィックが許可されています。ここでは、インバウンドの TCP ポート 8888 番を許可します。

「インバウンド」タブをクリックします。

「編集」ボタンをクリックします。

「ルールの追加」ボタンをクリックします。

①「カスタム TCP」を選択します。
②「8888」を入力します。
③「0.0.0.0/0」を入力します。
④必要に応じて説明を入力します。
⑤「保存」ボタンを押します。

送信元「0.0.0.0/0」はインターネット全体を意味します。

①インバウンドルールが設定されました。
②「インスタンス」をクリックしてインスタンスの表示画面に戻ります。

7　jupyter notebook の起動

端末から、

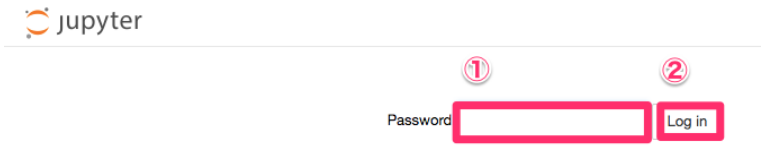
```
cd ~/Lesson/tools
jupyter notebook &
```

として、jupyter notebook をバックグラウンドで起動します。

インスタンスの「パブリック DNS」を確認します。

「パブリック DNS」を確認

ノートＰＣのブラウザから「http://(パブリック DNS):8888/」でアクセスできます。※あるいは「http://(パブリック IP):8888/」でもアクセスできます。



①先ほど設定したパスワードを入力します。

②「Log in」ボタンを押します。

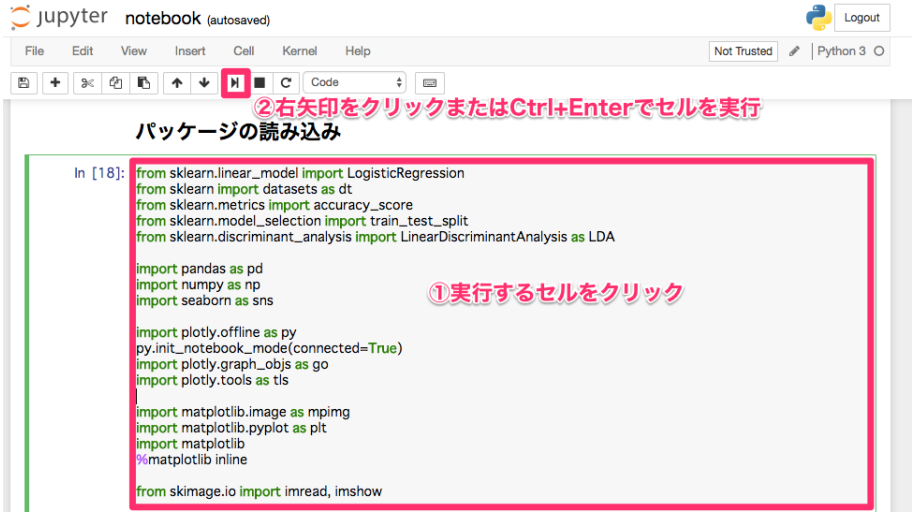
jupyter にログインしました。

8　notebook の実行

課題のノートブックを開きます。

「notebook.ipynb」を開きます。

ノートブックは文章やプログラムが記載されたセルからなります。ノートブックのセルに記載されたプログラムは実行することができます。



①実行するセルをクリックします。
②クリックまたは「Ctrl+Enter」で実行します。

セルの実行中は括弧内が「*」になります。
セルの実行が終わると番号が表示されます。
また、プログラムの出力がある場合には、実行結果が下に表示されます。

キーボードの上下の矢印で現在選択されているセルを移動します。説明を読みながら、セルのプログラムを上から順番に実行してみましょう。

セルをダブルクリックすると、セルの内容を編集できます。プログラムのセルは「Ctrl+Enter」で実行し、文章のセルは「Ctrl+Enter」で確定します。セルを挿入して、プログラムや文章を記載することができます。ショートカットキーがキーボードマークのボタンを押すと表示されます。