

# 인공지능 보안

이수미

# | 실습 환경 설정

## 머신러닝 준비물

- ✓ 누구나 동일한 결과를 표현할 수 있게 쉽게 실습하기 위하여
  - ✓ 네트워크에 연결된 컴퓨터
  - ✓ 구글 계정



구글 Colab

## 구글 코랩(Colab)

- ✓ 구글 코랩은 웹 브라우저에서 무료로 파이썬 프로그램을 테스트하고 저장할 수 있는 서비스
- ✓ 클라우드 기반의 주피터 노트북 개발 환경
- ✓ 구글 계정 생성 안내: <http://accounts.google.com/signup>
- ✓ 코랩 접속: <http://colab.research.google.com>

## 구글 코랩(Colab)

✓ 웹 브라우저에서 텍스트와 프로그램 코드를 자유롭게 작성할 수 있는 온라인 에디터, 노트북

The screenshot shows the Google Colaboratory web interface. At the top, a purple box highlights the header area with the text "Colaboratory에 오신 것을 환영합니다" (Welcome to Colaboratory) and a purple arrow pointing to the word "제목" (Title). Below this, a purple box highlights the left sidebar menu with the text "메뉴" (Menu) and a purple arrow pointing to the "시작하기" (Get started) option. Another purple box highlights the "시작하기" section in the main content area with the text "왼쪽 메뉴 닫기" (Close left menu). A purple box highlights a code cell with the text "코드 셀" (Code cell) and a purple arrow pointing to the code input area. A purple box highlights the output of the code cell with the text "출력" (Output) and a purple arrow pointing to the result "86400". A purple box highlights the text area of a code cell with the text "텍스트 셀" (Text cell) and a purple arrow pointing to the text input area. A purple box highlights the code cell's toolbar with the text "셀을 선택하면 이렇게 그림자가 나타납니다." (When you select a cell, a shadow appears like this) and a purple arrow pointing to the toolbar. The code cell contains the following Python code:

```
[ ] seconds_in_a_day = 24 * 60 * 60
seconds_in_a_day
```

The output of the code is "86400". The text area of the code cell contains the following text:

Colaboratory란?

줄여서 'Colab'이라고도 하는 Colaboratory를 사용하면 브라우저에서 Python을 작성하고 실행할 수 있습니다. Colab은 다음과 같은 이점을 자랑합니다.

- 구성이 필요하지 않음
- GPU 무료 액세스
- 간편한 공유

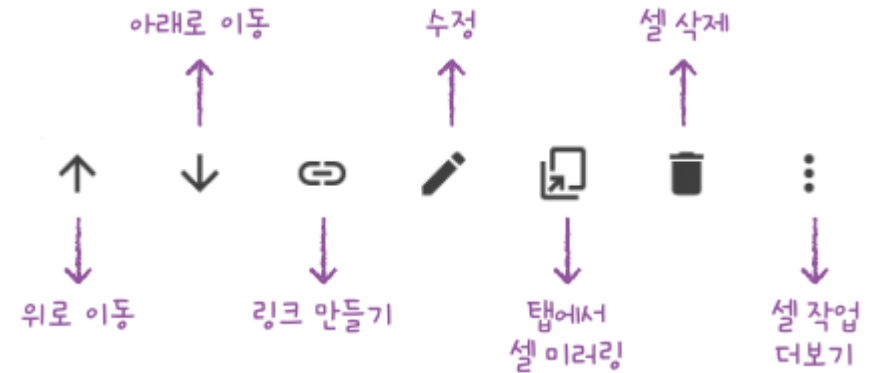
학생이든, 데이터 과학자든, AI 연구원이든 Colab으로 업무를 더욱 간편하게 처리할 수 있습니다. [Colab 소개 영상](#)에서 자세한 내용을 확인하거나 아래에서 시작해 보세요.

## 텍스트 셀

- ✓ 셀은 코랩에서 실행할 수 있는 최소 단위, 즉 셀 안에 있는 내용을 한번에 실행하고 그 결과를 노트북에 나타낸다.

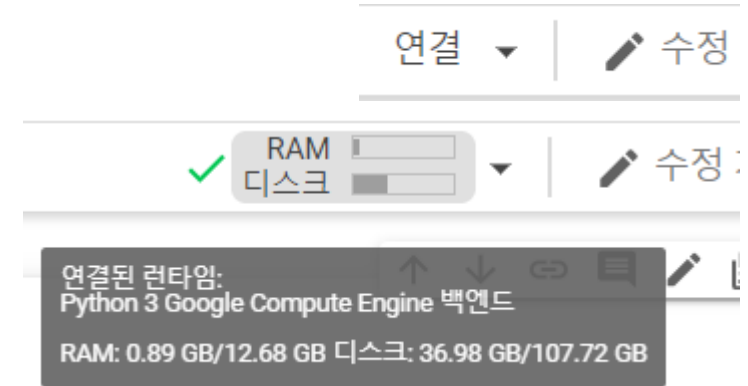


- 1 **Tt** : 현재 라인을 제목으로 바꿉니다. 코랩은 여러 단계의 메뉴를 지원합니다. 이 아이콘을 클릭하면 순서대로 제목의 크기가 바뀝니다.
- 2 **B** : 선택한 글자를 굵은 글자로 바꿉니다. 글자를 선택하지 않고 이 버튼을 누르면 현재 커서 위치에 있는 단어를 굵은 글자로 바꿉니다.
- 3 **I** : 선택한 글자를 이탤릭체로 바꿉니다. 글자를 선택하지 않고 이 버튼을 누르면 현재 커서 위치에 있는 단어를 이탤릭체로 바꿉니다.
- 4 **<>** : 코드 형식으로 바꿉니다. 글자를 선택하지 않고 이 버튼을 누르면 현재 커서 위치에 코드를 입력할 수 있는 코드 블록을 만듭니다.
- 5 **🔗** : 선택한 글자를 링크로 만듭니다. 글자를 선택하지 않고 이 버튼을 누르면 현재 커서 위치에 새로운 링크를 추가합니다.
- 6 **🖼️** : 현재 커서 위치에 이미지를 추가합니다.
- 7 **📊** : 현재 커서 위치에 들어 쓴 블록을 추가합니다.
- 8 **📋** : 현재 커서 위치에 번호 매기기 목록을 추가합니다.
- 9 **📋** : 현재 커서 위치에 글머리 기호 목록을 추가합니다.
- 10 **—** : 현재 커서 위치에 가로줄을 추가합니다.
- 11 **👁️** : 미리 보기 창의 위치를 오른쪽에서 아래로 또는 아래에서 오른쪽으로 바꿉니다. 창의 위치가 어떻게 바뀌는지는 직접 아이콘을 눌러서 확인해 보세요.



## 노트북

- ✓ 코랩은 구글이 대화식 프로그래밍 환경인 주피터를 커스터마이징한 것
- ✓ 코랩 노트북은 구글 클라우드의 가상 서버를 사용
  - ✓ 코드를 실행하기 전이나 연결이 끊어진 상태에서는 [연결]버튼이 활성화
  - ✓ 이 서버의 메모리는 약 12기가이고 디스크 공간은 100기가

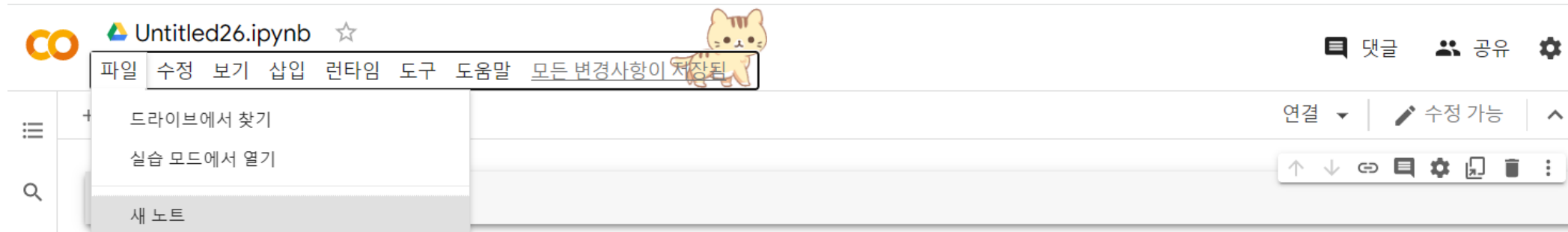


- ✓ 제한사항
  - ✓ 코랩 노트북으로 동시에 사용할 수 있는 구글 클라우드의 가상 서버는 최대 5개
  - ✓ 5개 이상의 노트북을 열어야 한다면 이미 실행 중인 노트북을 저장한 다음 구글 클라우드와 연결을 끊어야 함, 1개의 노트북을 12시간 이상 실행할 수 없음
  - ✓ 구글은 더 많은 메모리와 컴퓨팅 파워를 제공하는 코랩 프로(Colab Pro)를 월 9.99달러, 코랩 프로 플러스(Colab Pro+)는 월49.99달러, 코랩 프로 플러스는 한 번에 최대 24시간 동안 프로그램을 실행할 수 있다.

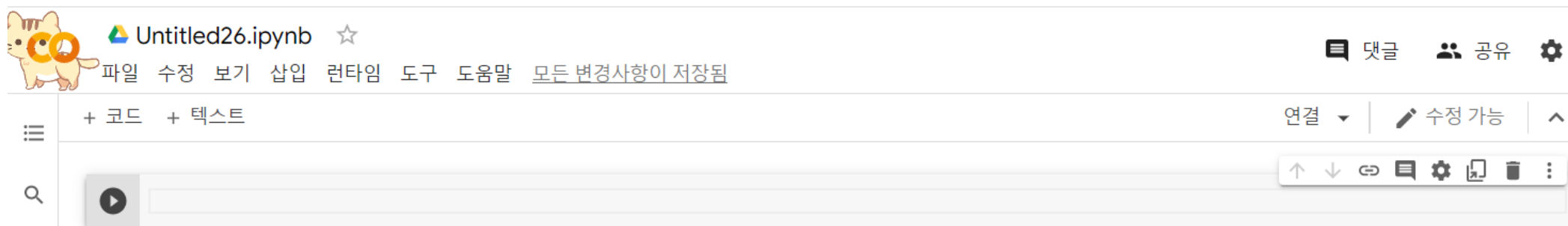
# 새 노트북 만들기

Colab 실습

① [파일]-[새노트]를 클릭해서 새로운 노트북을 만든다.



② 새 노트북은 Untitled[숫자].ipynb 이름으로 만들어지고 노트북에는 다음과 같이 빈 코드의 셀 하나가 들어가 있다



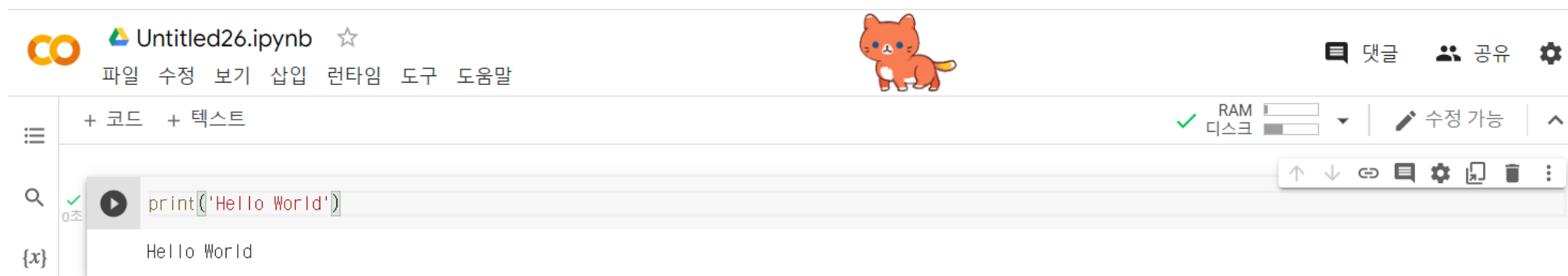


## 새 노트북 만들기

Colab 실습

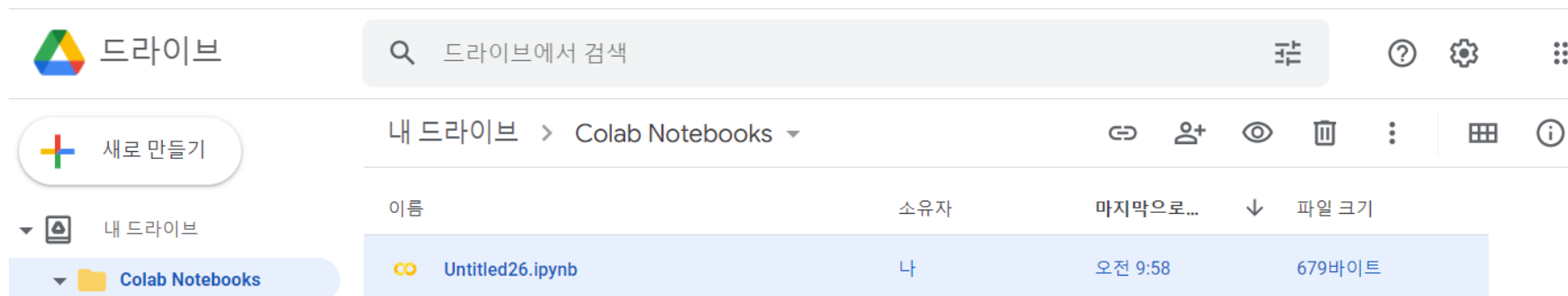
③ 코드 셀에 'Hello World'를 출력하는 `print()` 코드를 작성하고 파일의 이름을 'Hello World'로 저장

※ 코드 셀을 실행하려면 **Ctrl** + **Enter** 키를 누르거나 왼쪽에 있는 플레이 아이콘(▶)을 클릭



④ 노트북은 자동으로 구글 드라이브의 [내 드라이브]-[Colab Notebooks] 폴더 아래 저장

※ 구글 드라이브(<http://drive.google.com>)로 접속, [파일]-[저장] 선택해 수동으로 저장가능



## 새 노트북 만들기

Colab 실습

- ⑤ 노트북 이름 바꾸기, 제목을 마우스로 클릭하면 수정할 수 있도록 바뀐다.  
이 파일의 제목을 'Hello World'로 바꾸기

The image illustrates the process of renaming a Google Colab notebook. It consists of three parts:

- Left Screenshot:** Shows the Colab interface with a notebook titled "Untitled26.ipynb". The title is highlighted with a red box. Below the title bar, the code editor shows a code cell with the text `print('Hello World')`. The output of the cell is "Hello World".
- Right Screenshot:** Shows the same Colab interface after the notebook has been renamed to "Hello World.ipynb". The new title is also highlighted with a red box. The code cell and its output remain the same.
- Bottom Screenshot:** Shows the Google Drive interface. The "Hello World.ipynb" file is listed in the "Colab Notebooks" folder. The file details are as follows:

이름	소유자	마지막으로...	파일 크기
Hello World.ipynb	나	오전 10:04	679바이트

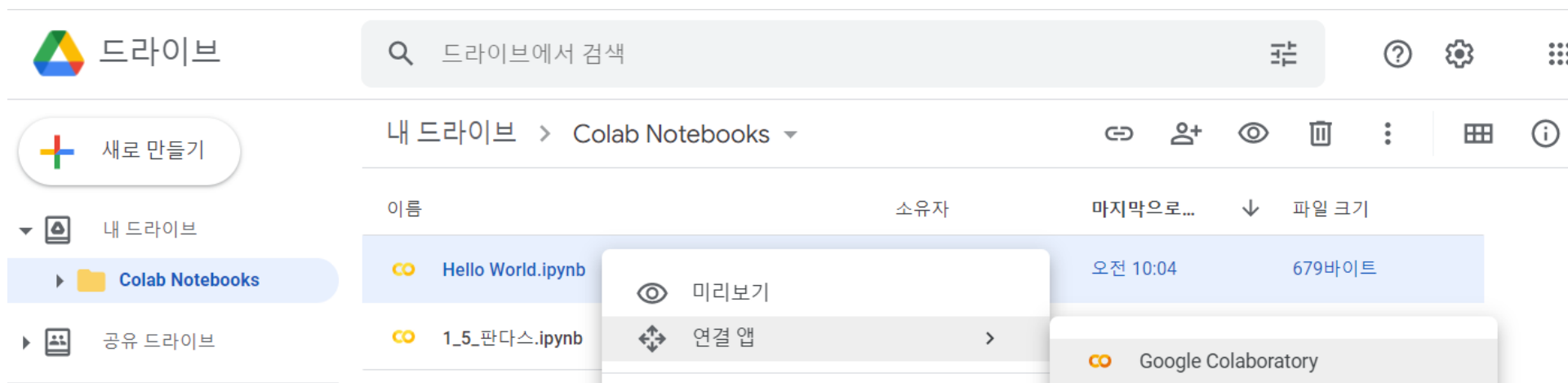
## 새 노트북 만들기

Colab 실습

### ⑥ 코랩 노트북 화면에서 [파일]-[노트 열기] 선택

[구글 드라이브] 선택 - [Colab Notebooks]에 들어간 노트북을 코랩에서 열 수 있음

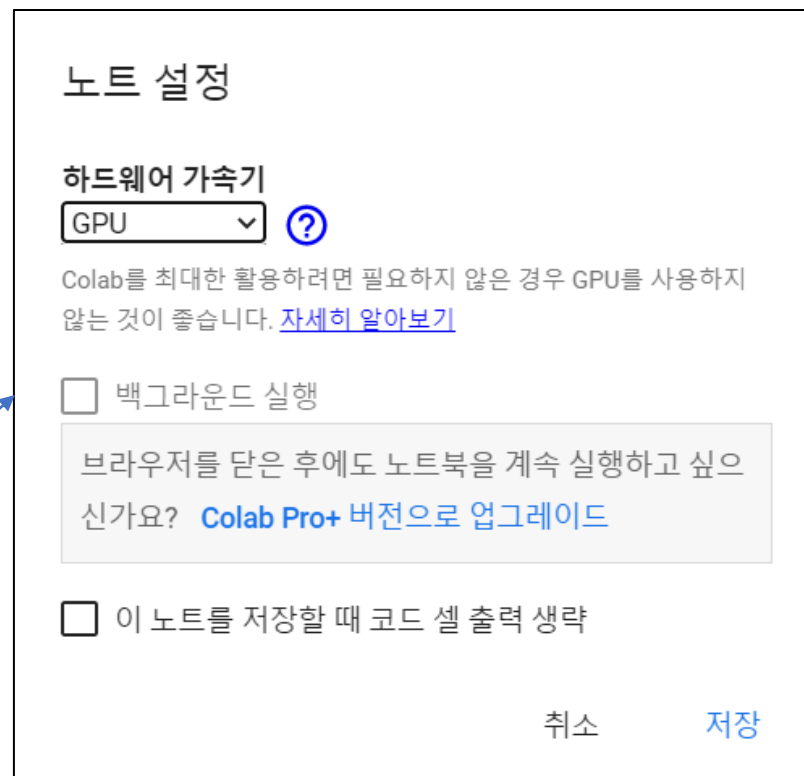
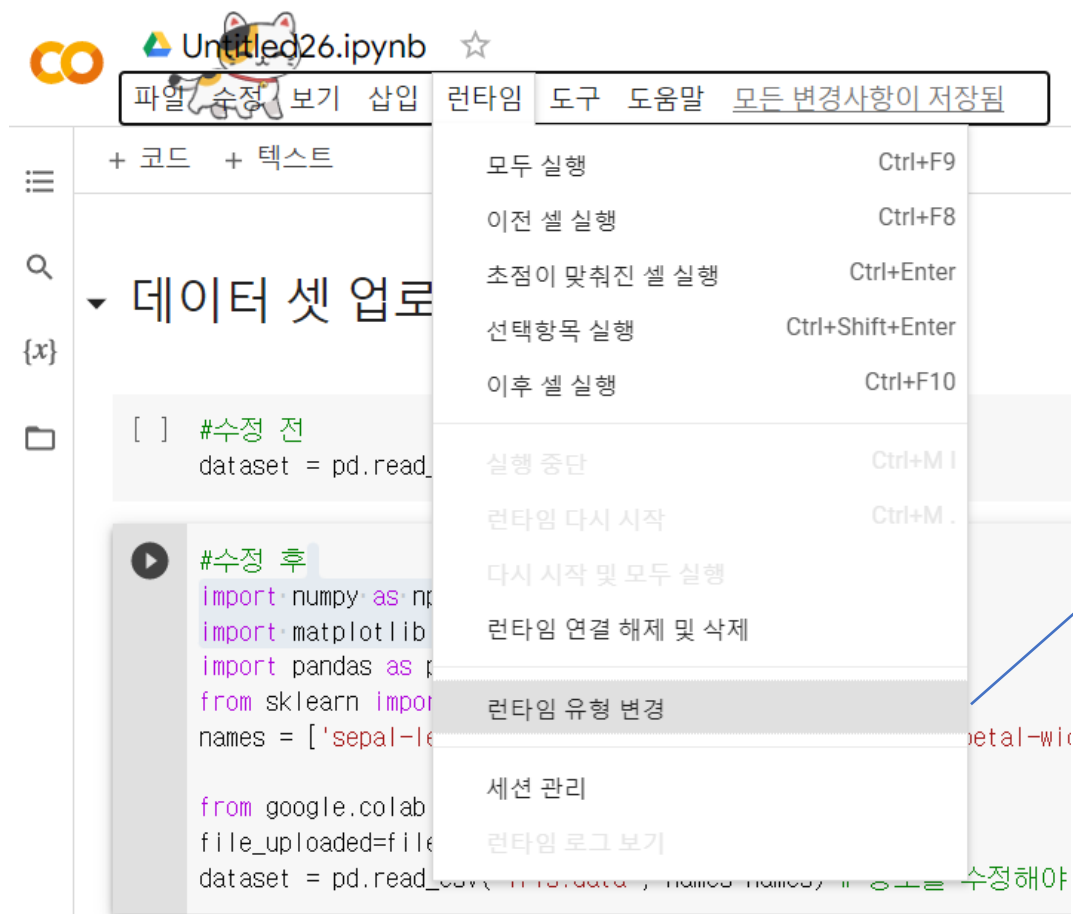
코랩 노트북을 선택하고 마우스 오른쪽 버튼을 클릭, 팝업 메뉴 [연결 앱]-[Google Colaboratory]



# GPU 사용하기

Colab 실습

✓ GPU 무료로 제공, 런타임>런타임 유형 변경 선택 후 하드웨어 가속기 옵션에서 GPU 설정



## 데이터 업로드(Colab)

Colab 실습



## 데이터 업로드(Colab)

✓ 사용자 PC에서 파일 업로드하기

① 다음 코드를 입력

```
from google.colab import files  
file_uploaded = files.upload()
```

② 파일 선택 클릭하여 업로드



#수정 후

```
import numpy as np  
import matplotlib.pyplot as plt  
import pandas as pd  
from sklearn import metrics  
names = ['sepal-length', 'sepal-width', 'petal-length', 'petal-width', 'Class']  
  
from google.colab import files # 데이터 불러오기  
file_uploaded=files.upload() # 데이터 불러오기  
dataset = pd.read_csv('iris.data', names=names) # 경로를 수정해야 합니다.
```

파일 선택

선택된 파일 없음

Cancel upload

## 데이터 업로드(Colab)

✓ 구글 드라이브에 폴더를 만들고 필요한 데이터를 업로드

① 다음 코드를 입력

```
from google.colab import drive  
drive.mount('/content/drive/')
```

② 다음과 같이 Google Drive 파일에 액세스하도록 허용하시겠습니까?라는 문구가 나옵니다.

**Google Drive에 연결을 누릅니다**

노트북에서 Google Drive 파일에 액세스하도록 허용하시겠습니까?

이 노트북에서 Google Drive 파일에 대한 액세스를 요청합니다. Google Drive에 대한 액세스 권한을 부여하면 노트북에서 실행되는 코드가 Google Drive의 파일을 수정할 수 있게 됩니다. 이 액세스를 허용하기 전에 노트북 코드를 검토하시기 바랍니다.

아니요


Google Drive에 연결

## 데이터 업로드(Colab)

Colab 실습

✓ 구글 드라이브에 폴더를 만들고 필요한 데이터를 업로드

③ 계정 선택 화면이 나오는데 ‘자신의 계정을 선택’한 후  
액세스 허용 메시지가 표시되면 **허용**을 누릅니다

 Google 계정으로 로그인



계정 선택

Google Drive for desktop(으)로 이동

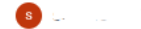


 다른 계정 사용

계속 진행하기 위해 Google에서 내 이름, 이메일 주소, 언어 환경설정, 프로필 사진을 Google Drive for desktop과(와) 공유합니다. 앱을 사용하기 전에 Google Drive for desktop의 [개인정보처리방침](#) 및 [서비스 약관](#)을 검토하세요.



Google Drive for desktop에서 내 Google 계정에 액세스하려고 합니다



이렇게 하면 Google Drive for desktop에서 다음 작업을 할 수 있습니다.

-  Google Drive 파일 보기, 수정, 생성, 삭제 
-  Google 포토의 사진, 동영상, 앨범을 봅니다. 
-  모바일 클라이언트 구성 및 실험 정보 가져오기 
-  프로필 및 연락처와 같은 Google 사용자 정보 조회 
-  Google Drive 파일 작업 기록 조회 
-  Google Drive 문서 보기, 수정, 생성, 삭제 

Google Drive for desktop 앱을 신뢰할 수 있는지 확인

민감한 정보가 이 사이트 또는 앱과 공유될 수 있습니다. 언제든지 [Google 계정](#)에서 액세스 권한을 확인하고 삭제할 수 있습니다.

Google이 [데이터를 안전하게 공유](#)하는 방법을 알아보세요.

Google Drive for desktop의 [개인정보처리방침](#) 및 [서비스 약관](#)을 확인하세요.

취소

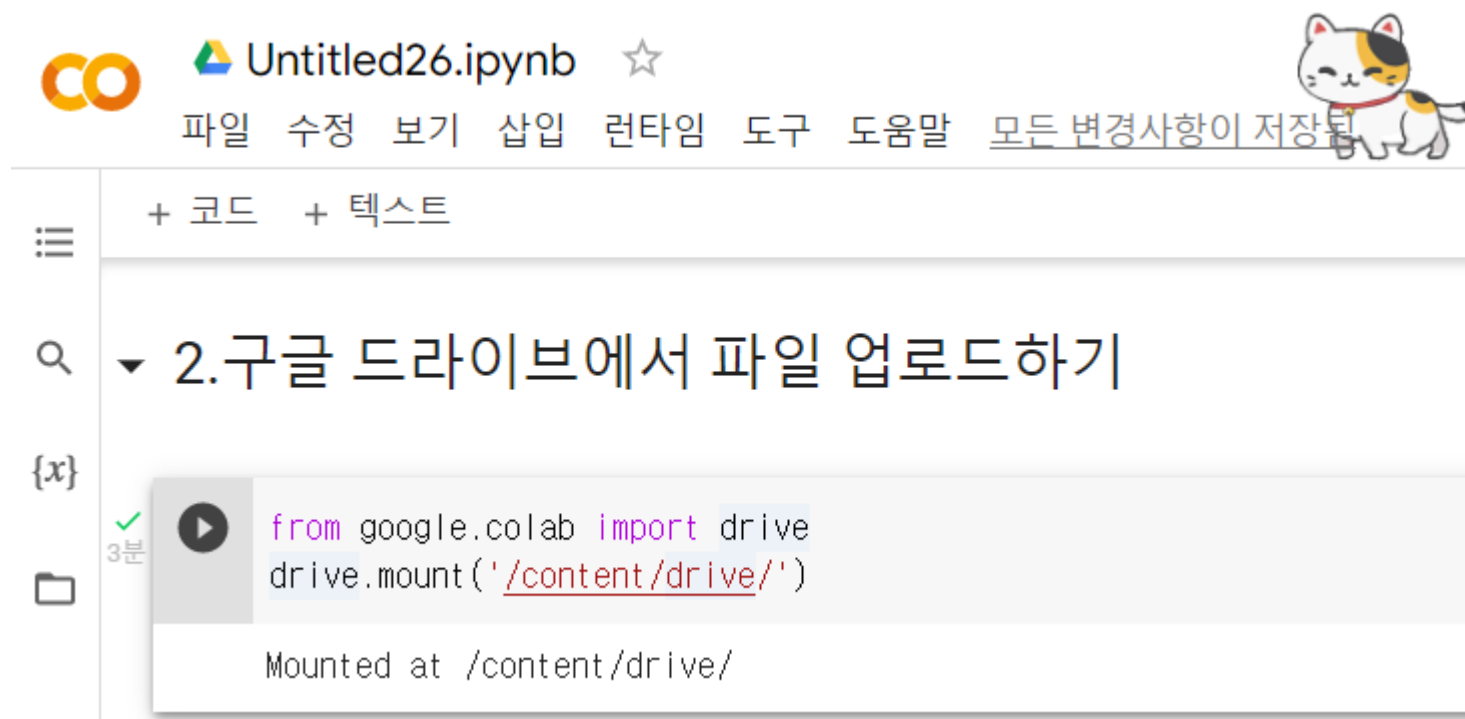
허용



## 데이터 업로드(Colab)

✓ 구글 드라이브에 폴더를 만들고 필요한 데이터를 업로드

④ 구글 드라이브에 제대로 연결되면 다음과 같이 Mounted at /content/drive/ 메시지가 출력



## 데이터 업로드(Colab)

✓ 구글 드라이브에 폴더를 만들고 필요한 데이터를 업로드

⑤ 왼쪽 폴더 아이콘을 클릭하여 원하는 데이터 파일을 선택 후 마우스 오른쪽 버튼을 눌러 경로 복사 선택

The screenshot shows the Google Colab interface. On the left, the file explorer shows a folder named 'drive' which is expanded to show 'MyDrive'. Inside 'MyDrive', there is a folder named 'Data' which is also expanded. Inside 'Data', there is a folder named 'titanic' which is expanded. Inside 'titanic', there is a file named 'credit card.csv' which is highlighted. A red box is drawn around the folder icon in the 'Data' folder. A context menu is open over the 'credit card.csv' file, showing options: 다운로드, 파일 이름 바꾸기, 파일 삭제, 경로 복사 (highlighted), and 새로고침. On the right, the code editor shows a code cell with the following code: 

```
from google.colab import drive
drive.mount('/content/drive/')
```

 The code cell is titled '2.구글 드라이브에서 파일 업로드하기' and has a status of 'Mounted at /content/drive/'.

## 데이터 업로드(Colab)

✓ 구글 드라이브에 폴더를 만들고 필요한 데이터를 업로드

⑥ 복사한 경로로 코드의 데이터셋 위치를 수정한 후 실행



0초

```
[4] import pandas as pd
```







```
data = pd.read_csv('/content/drive/MyDrive/Data/credit_card.csv', sep=',')  
data.head()
```

	CUST_ID	BALANCE	BALANCE_FREQUENCY	PURCHASES	ONEOFF_PURCHASES	INSTALLMENTS_PURCHASES
0	C10001	40.900749	0.818182	95.40	0.00	95.4
1	C10002	3202.467416	0.909091	0.00	0.00	0.0
2	C10003	2495.148862	1.000000	773.17	773.17	0.0
3	C10004	1666.670542	0.636364	1499.00	1499.00	0.0
4	C10005	817.714335	1.000000	16.00	16.00	0.0

## summary

- ✓ 코랩: 구글 계정이 있으면 누구나 사용할 수 있는 웹 브라우저 기반의 파이썬 코드 실행 환경
- ✓ 노트북: 코랩의 프로그램 작성 단위, 일반 프로그램 파일과 달리 대화식으로 프로그램을 만들 수 있기 때문에 데이터 분석이나 교육에 매우 적합
- ✓ 구글 드라이브: 구글이 제공하는 클라우드 파일 저장 서비스, 코랩에서 만든 노트북은 자동으로 구글 클라우드의 'Colab Notebooks' 폴더에 저장되고 필요할 때 다시 코랩에서 열수 있다.

### 텍스트 셀 툴바

	제목 전환		굵게		기울임 꼴
	코드로 형식 지정		링크 삽입		이미지 삽입
	들여쓰기		번호 매기기 목록 추가		글머리 기호 목록 추가
	가로줄 추가		마크다운 미리 보기 위치 변경		

Q&A