**Appendix１；**

3.1\_MITRE-ATT&CK-Cloud-Matrixから攻撃再現性のための頻度カウントを抽出するPythonコード

**概要：**

* MITRE ATT&CKのCloud Matrixに基づき、攻撃テクニックの再現性（過去利用頻度）を自動集計するPythonスクリプト一式。
* STIX 2.0形式でエクスポートしたMITRE ATT&CKデータを入力し、攻撃グループ（intrusion-set）、キャンペーン、マルウェア／ツールごとに各テクニックの使用回数をカウントし集計。
* 集計結果をテクニックID・テクニック名とともにCSVファイルへ自動出力。以降のリスク評価やデータ分析の基礎資料として汎用利用が可能。
* クラウド環境の攻撃分析や再現性スコアリングの自動化を実現し、オープンなMITREデータとPython標準ライブラリやpandas、stix2ライブラリのみで構築され、検証の再現性が高いプログラム例。
* 本論文の「攻撃再現性スコアリング」手法で必要となる実利用頻度データの収集実装例として、研究や実務で幅広く応用可

Google Colab用Pythonコード（MITRE ATT&CK STIX 2.0読み込み・Cloud Matrixスコアリング自動集計・CSV出力対応）

#  必要なライブラリのインストール（初回のみ）  
!pip install -q stix2  
  
#  ライブラリの読み込み  
import json  
import pandas as pd  
from stix2 import parse  
  
#  Google Colab にファイルをアップロード  
from google.colab import files  
uploaded = files.upload()  
  
#  STIX JSONファイル名の指定  
stix\_file\_name = list(uploaded.keys())[0]  
  
#  JSON読み込み  
with open(stix\_file\_name, "r", encoding="utf-8") as f:  
stix\_data = json.load(f)  
  
#  STIXオブジェクトの抽出  
stix\_objects = stix\_data.get("objects", [])  
  
#  Technique情報を抽出（Cloud Matrixに限定）  
techniques = {}  
for obj in stix\_objects:  
if obj.get("type") == "attack-pattern":  
platforms = obj.get("x\_mitre\_platforms", [])  
if "Cloud" in platforms:  
technique\_id = None  
for ext\_ref in obj.get("external\_references", []):  
if ext\_ref.get("source\_name") == "mitre-attack" and "attack-pattern" in ext\_ref.get("external\_id", ""):  
technique\_id = ext\_ref.get("external\_id")  
if technique\_id:  
techniques[obj["id"]] = {  
"technique\_id": technique\_id,  
"name": obj.get("name", ""),  
"group\_usage": 0,  
"campaign\_usage": 0,  
"software\_usage": 0  
}  
  
#  Relationshipを走査して使用回数をカウント  
for obj in stix\_objects:  
if obj.get("type") == "relationship":  
target\_ref = obj.get("target\_ref")  
if target\_ref in techniques:  
source\_ref = obj.get("source\_ref", "")  
if source\_ref.startswith("intrusion-set--"):  
techniques[target\_ref]["group\_usage"] += 1  
elif source\_ref.startswith("campaign--"):  
techniques[target\_ref]["campaign\_usage"] += 1  
elif source\_ref.startswith("malware--") or source\_ref.startswith("tool--"):  
techniques[target\_ref]["software\_usage"] += 1  
  
#  データフレームに変換  
df = pd.DataFrame([  
{  
"Technique ID": data["technique\_id"],  
"Technique Name": data["name"],  
"Group\_Usage\_Count": data["group\_usage"],  
"Campaign\_Usage\_Count": data["campaign\_usage"],  
"Software\_Usage\_Count": data["software\_usage"]  
}  
for data in techniques.values()  
])  
  
#  CSVとして保存 & ダウンロード  
output\_csv = "cloud\_matrix\_technique\_usage\_stats.csv"  
df.to\_csv(output\_csv, index=False)  
files.download(output\_csv)