教師跨領域研究學社群 「人工智慧研討社群(第一次)」

時間：2019-09-27
地點：S433

分享者：魏澤人教授交大 AI 學院副教授、機器學習 GDE (Google Developers Expert)、人工智慧及數學顧問、花蓮.py 及 GDG 花蓮發起人。

題目： 深度學習及隱私

介紹：機器學習時代，要怎麼定義以及保護資料的隱私？我們將討論資訊秘密及 Differential privacy 的概念，並解釋如何利用秘密分享來訓練深度學習模型。

第二次研習會，我們邀請了交通大學 AI 人工智慧學院的魏澤人教授，來為我們講解 AI 與資料隱私相關部分，以個人資料依賴型的人工智慧 (personal data dependent AI) 相關者案例中，在收集、處理、及利用個人資料，以進行智慧學習和智慧應用時，一個很重要的議題是個人隱私權，如何在分析及處理大量數據時，能夠同時顧及分析的正確完整性及個人的隱私，在此研習會中，演算法 de-identification, Pseudonymization, K-anonymization, DG-SGD algorithm 等都詳細的解釋。

演講人：魏澤人教授

專題演講