「數位時代下的國民身分證與身分識別」研討會

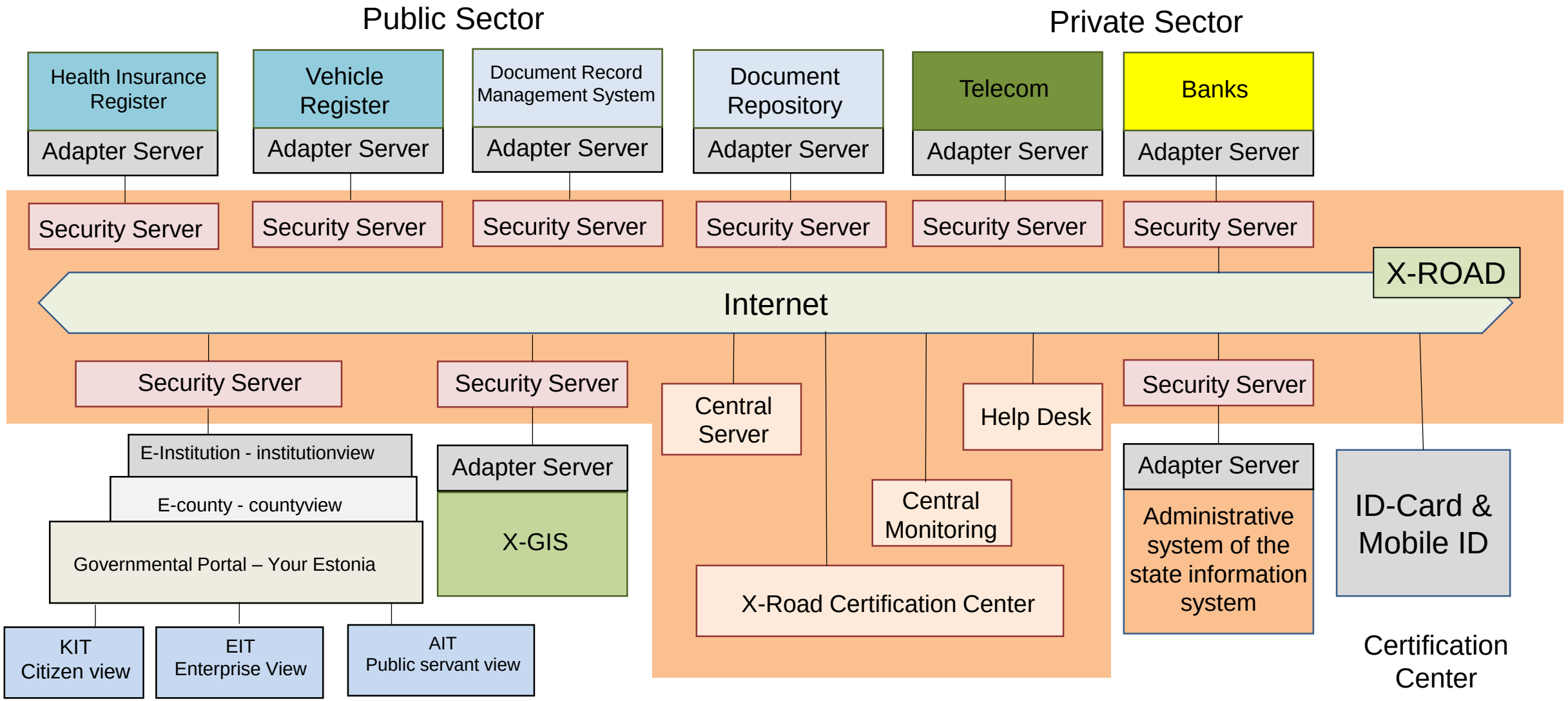
T-Road的資料庫串連與數位身分證的近用控制

主講人：查士朝

國立臺灣科技大學資訊管理系 教授

國立臺灣科技大學資通安全研究與教學中心主任

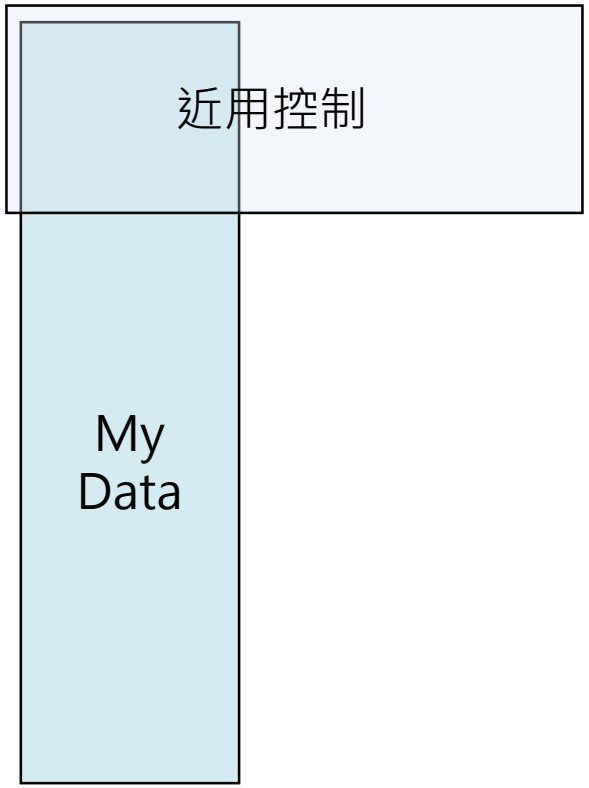
T-ROAD 與 X-ROAD



https://e-estonia.com/estonian-cyber-security-innovation/

T-ROAD 或是 My Data 為近用控制其中一環

- 在 OECD 的個人隱私與跨境個人資料流通保護綱領當中的個人參與 (Individual participation) 原則：
  - 個人應該要有權力去取得其相關的個人資料，並檢驗其正確性
- 在 GDPR 中，有四項相關的權力
  - Article 15: 查詢、閱覽與複製權
  - Article 16: 當事人有權要求資料收集者對於所收集之資料進行更正及補全
  - Article 17 刪除權或被遺忘權：當個資蒐集、處理目的消失，或遭違法處理，當事人得請求刪除其個資或連結
  - Article 20 資料可攜權：可將資料轉移到其他系統而不會受到阻擋



但是有幾個議題

近用控制面

- T-ROAD 目前主要滿足的是資料可攜，政府應該還是要去訂定各機關持有個資的公告與查詢標準
- 提供資料最小化與選擇
- 建議更進一步要考慮連結問題

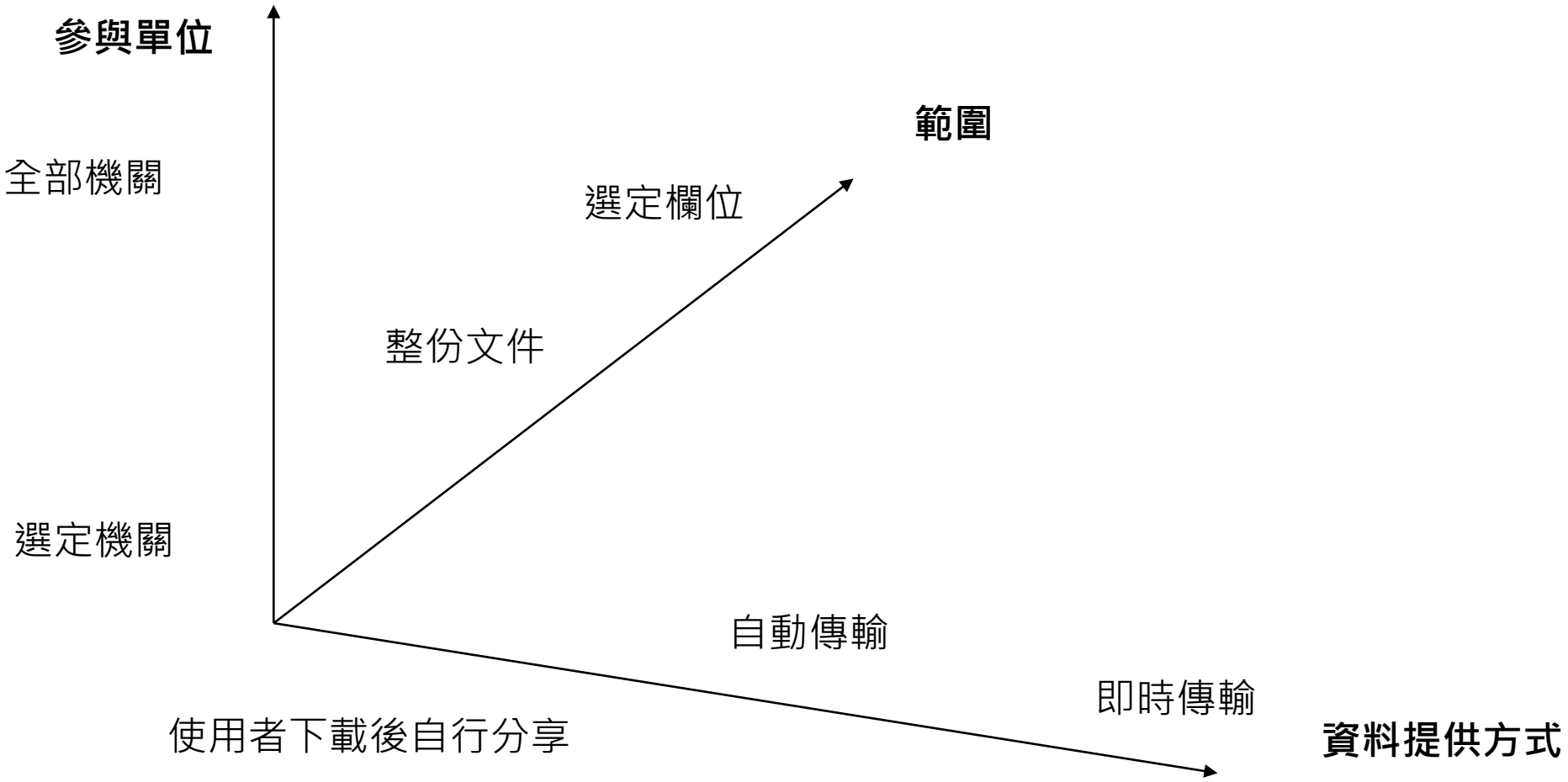
身分鑑別面

- 臨櫃身分驗證議題
- 隔離環境的驗證議題

資料分析面

- 資料保護衝擊分析或隱私衝擊分析

資料交換方式



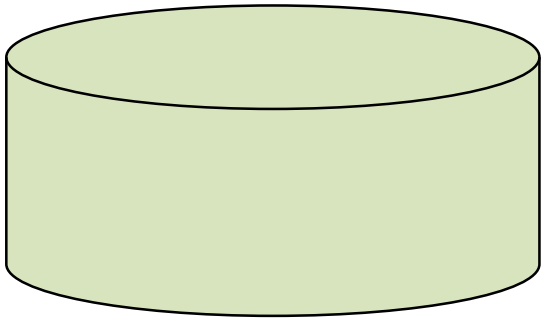
資料的連結問題

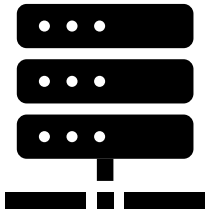
- 讓人知道某單位已經有哪些資料很重要
- 甚至在某些情況下應該提醒

User(ID, A1, A2, B1)

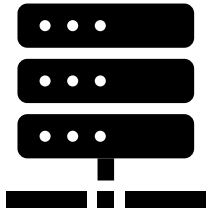
User(A1, A2, B1)

User(A1, A2) ⟵ User(A1, B1)



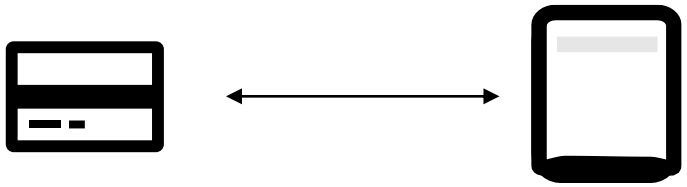


A 單位



B 單位

隔離環境驗證議題



如何確定卡片是真的？

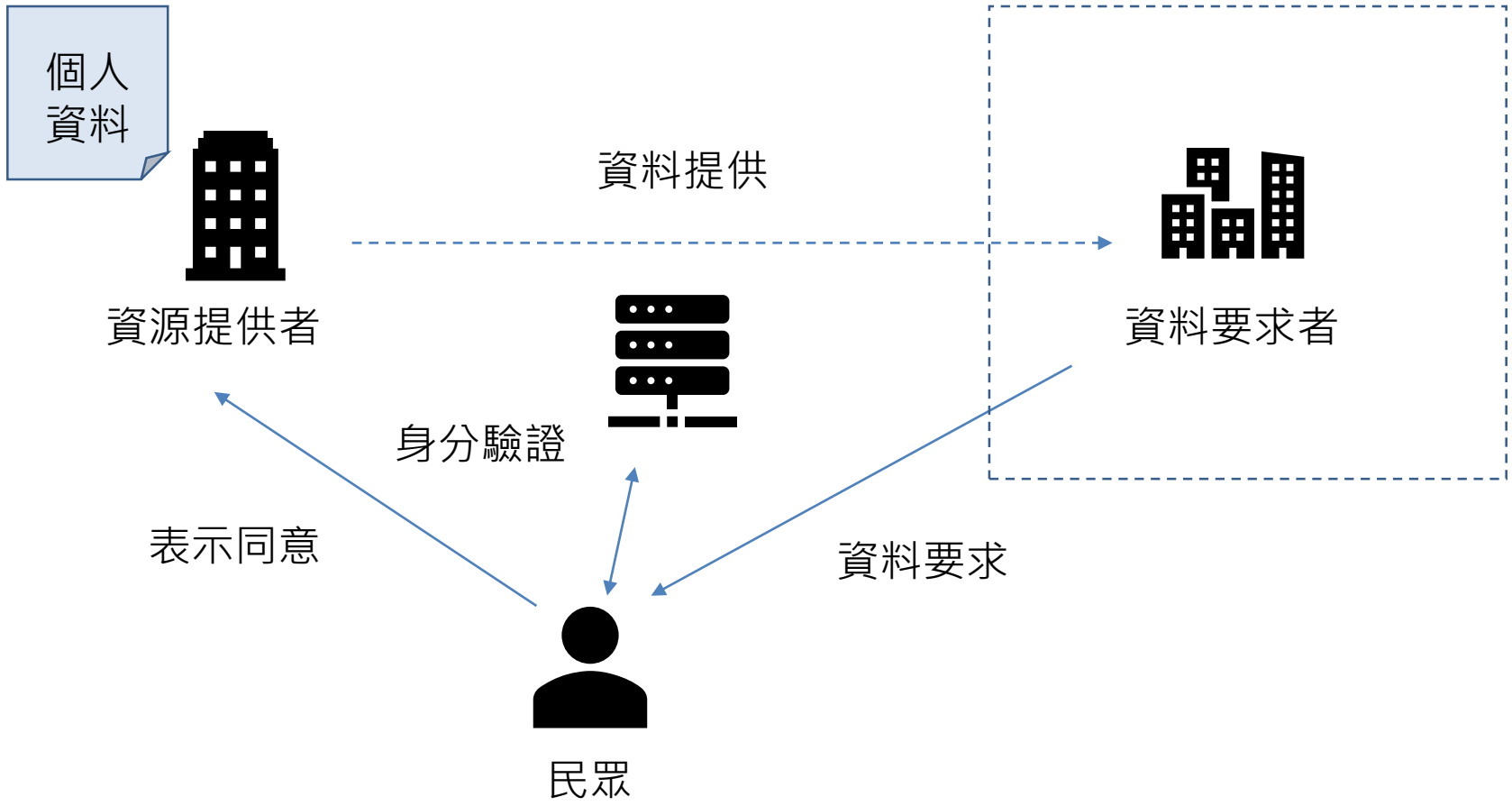
- 簽章？
  - 離線時如何驗證？
  - 沒有自然人憑證的 EID 要如何驗證？
- SAM
  - 要有特規的讀卡機嗎？

不是說會有問題，而是應該要先規劃好。

真的要和歐盟討論 GDPR 的適足性認定的話，其實不是智慧就好

- 對於依據個人剖繪進行自動化決策的限制
- 對於 Profiling 的定義：
  - 建立個人剖繪指的是對於自然人以任何自動處理的方式使用個人資料去對該自然人進行評估，而可以對該自然人進行分析或預測
  - *'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;*
- 若有相關行為必須要透明 (Article 13)，且讓使用者能夠知道結果 (Article 15)，並且可以決定不被建立個人資料檔案而分析 (Article 22)
- 若有可能對於自然人的自由或權利造成重大風險，則應進行衝擊分析 (Article 35)

更進一步對於參與單位的安全要求



結論

- 愛沙尼亞在 2007 年遭遇大規模的 DDoS 攻擊，雖然據說資料沒有被竊取，但是它們深深的去思考問題以及怎樣讓民眾相信他們資安做的好
- 建議像美國一樣有 SONR 揭露的要求，並且讓民眾知道資料被分享過去後對方會擁有那些資料
- 除了線上作業，建議更進一步考慮到民眾臨櫃作業與隔離作業環境的身分驗證方式
- 要做智慧應用，要滿足 GDPR 的適足性認定，應該要有對於自動決策的隱私衝擊分析要求
- 除了 T-ROAD 本身，接收方有沒有能力保管資料，以及是否有遵守規定，這點建議要有一個規範
- 資料的近用除了資料交換之外，建議建立其他近用控制的標準

感謝各位的聆聽