新北市政府教育局
資安現況與未來趨勢分析

講師：葉益禎

中華民國111年11月7日

課程大綱

序號	大綱
一	全球及台灣資安威脅現況
二	台灣產業資安曝險分析
三	新興科技之資安議題
四	零信任— 資安管理新觀念
五	問題與討論

全球及台灣資安威脅現況

2021年全球重大資安事件

資料來源: 行政院國家資通安全會報技術服務整理中心

1月

- 俄國駭客發展詐騙攻擊服務，提供**自動化詐騙服務**
- 知名Android遊戲模擬器NoxPlayer**供應鏈**遭受攻擊

2月

- 駭客組織鎖定美國電網，透過**網路釣魚**，誘使下載惡意程式
- 美國佛州**淨水處理廠**遭駭，試圖調高氫氧化鈉濃度

3月

- 駭客組織鎖定微軟**Exchange**安全漏洞發動攻擊
- 駭客鎖定美國納稅人攻擊，以**稅務名義寄送釣魚郵件**

4月

- 北韓駭客**架設資安新創網站**，針對資安人員發起社交工程攻擊
- 北韓駭客鎖定支援加密貨幣付款電商網站攻擊

5月

- 駭客串聯不同惡意程式並**使用逾50個不同網域名稱寄送魚叉式釣魚郵件**
- 美國最大**燃油供應商Colonial遭勒索軟體攻擊**，美國能源部宣布進入緊急狀態

6月

- 俄國駭客鎖定政府、研究機構及國際組織，攻擊，**透過郵件行銷平台寄送惡意郵件**
- 垃圾郵件攻擊行動散布金融木馬程式，利用巨集並**可規避防毒軟體偵測**

7月

- 以色列**軍事級間諜程式Pegasus(飛馬)遭濫用**，涉監控全球政要與記者手機
- 伊朗**火車系統**遭駭客入侵，竄改火車班次延誤或取消之假消息

8月

- 以色列研究機構**透過AI產製萬能金鑰**，成功欺騙人臉辨識系統
- Accenture顧問公司遭**勒索軟體**攻擊，駭客要求限時支付贖金

9月

- 微軟揭露**大規模網路釣魚即服務**，大幅降低網路釣魚攻擊之門檻
- 印尼防疫追蹤APP資料庫未妥善防護，導致**檢測、醫療紀錄等機敏資訊外洩**

10月

- 駭客運用**雲端服務與加密機制**新手法，攻擊全球**航太產業與電信**公司
- 國家級駭客鎖定**電信業者**發起攻擊行動，入侵外部DNS伺服器

11月

- 美國FBI因軟體配置錯誤，遭**駭客假藉名義發送逾10萬封垃圾郵件**
- 駭客利用個已知老舊資安漏洞，**鎖定數百萬台IoT設備發起攻擊**

12月

- 駭客利用廣泛使用於產品與服務日誌程式庫Log4Shell重大漏洞攻擊
- 駭客使用有效程式碼簽章憑證簽署惡意程式，規避資安防護機制

全球資安威脅六大面向

分析全球2021年全球資安威脅與相關研究報告，歸納六大資安威脅趨勢，如下：

教育體系通報最多，人為操作、設定與網站設計疏失最常見

資料來源： iThome 2021.12.17

國內資安通報制度的建立，行政院資安處表示，現在機關都守法懂得通報。從近兩年重大事件通報的根本原因分析來看，許多事件狀況都是**人為疏失**而導致，還有像是**弱密碼**的狀況、**寄送社交工程釣魚信**，至今仍存在，資安管理的落實，以及人員自身有無資安意識，是當前資安推動關鍵。

1. 人為疏失：權限設定錯誤，導致他人可公開檢索、誤放連結、系統不當變更，使民眾資料外洩
2. **弱密碼**：容易被暴力破解或是容易被猜出的密碼
3. 社交工程郵件攻擊：利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取機敏資料

觀注重點

- 系統使用密碼進行驗證時，應強制最低密碼複雜度。
- 內部員工應接受資安認知教育訓練，並針對核心IT系統定期預約弱掃與滲透測試，修補漏洞落實資安防護措施。
- 依資通安全責任等級分級辦法第11條規定，機關、學校人員應依所屬人員完成對應之資通安全教育訓練法定時數要求。

社交工程搭配時事議題做為攻擊主軸

資料來源： NCCST-吳啟文主任 2021.03.09

攻擊啟動從**釣魚郵件**開始，駭客以近期受關注程度高的**政經議題**為由施行攻擊，例如肺炎疫情、總統520就職等，鎖定特定相關機關進行攻擊

1. 主要仰賴的是社交工程技巧，利用人性的弱點誘騙您上當
2. 勒索目標：盜取商業情報、個資、破壞研究工作、阻斷院內核心IT系統服務
3. 駭客會盡可能大量散發這類電子郵件，並經常假冒一些常見的服務或機構，如：PayPal或美國銀行 (Bank of America)

觀注重點

- 對於已知及未知來源的文字簡訊或即時通訊，只要是要求您點選連結或是向您詢問個人資訊的訊息，都應保持警覺。
- 採用一套能與服務整合的防護，直接透過 API 與您的雲端或企業內電子郵件平台整合，來防範內部網路釣魚攻擊。
- 組織可以透過網路釣魚攻擊的模擬和知識考核，準確地評估所需的教育訓練內容，並根據資訊安全標準 ISO27001 幫助組織依循國際認可的最佳實務作法來設計或架構出適用的訓練內容。

APT類型攻擊轉而利用商用工具軟體與服務

資料來源： NCCST-吳啟文主任 2021.03.09

駭客利用網路上現成的**工具程式**或**商用軟體**進行入侵攻擊，並滲透與掌控**AD系統**，利用政府導入**政府共通組態基準(GCB)**以合法的服務，透過**GPO派送**惡意程式進行橫向擴散

1. 什麼是 APT？簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。
2. 勒索目標：盜取商業情報、破壞研究工作
3. APT可能會採取多種手段，像是惡意軟體，弱點掃描，針對性入侵和利用惡意內部人員破壞安全措施
4. GCP :目的在於規範資通訊設備的一致性安全設定，降低駭客入侵管道
5. GPO : 可以控制使用者帳戶和電腦帳戶的工作環境，提供集中化管理

觀注重點

- 除須有郵件過濾機制外，內部員工應定期參與關於社交工程或釣魚郵件之認知訓練課程；此外，當資安事故發生時亦應立即切斷所有內網連線，並在平時就落實將重大核心作業區與含機敏資訊區塊進行隔離控管，以防因釣魚而受入侵的系統影響到組織內重要資料。
- 依據個人資料保護法第18與27條，公務及非公務機關保有個人資料檔案者，應採行適當之安全措施(如:加密)，防止個人資料被竊取、竄改、毀損、滅失或洩漏。組織針對敏感性資料應予以適當的加密技術，確保資料之機密性、完整性、可用性。
- 應定期進行系統安全性更新，修補漏洞並持續追蹤改善。

物聯網攻擊鎖定監視與網通設備

資料來源： NCCST-吳啟文主任 2021.03.09

鎖定機關**監視器**與**網通設備**做為攻擊標的，以**弱密碼/預設密碼**配合已知弱點攻擊程式進行探測並入侵控制

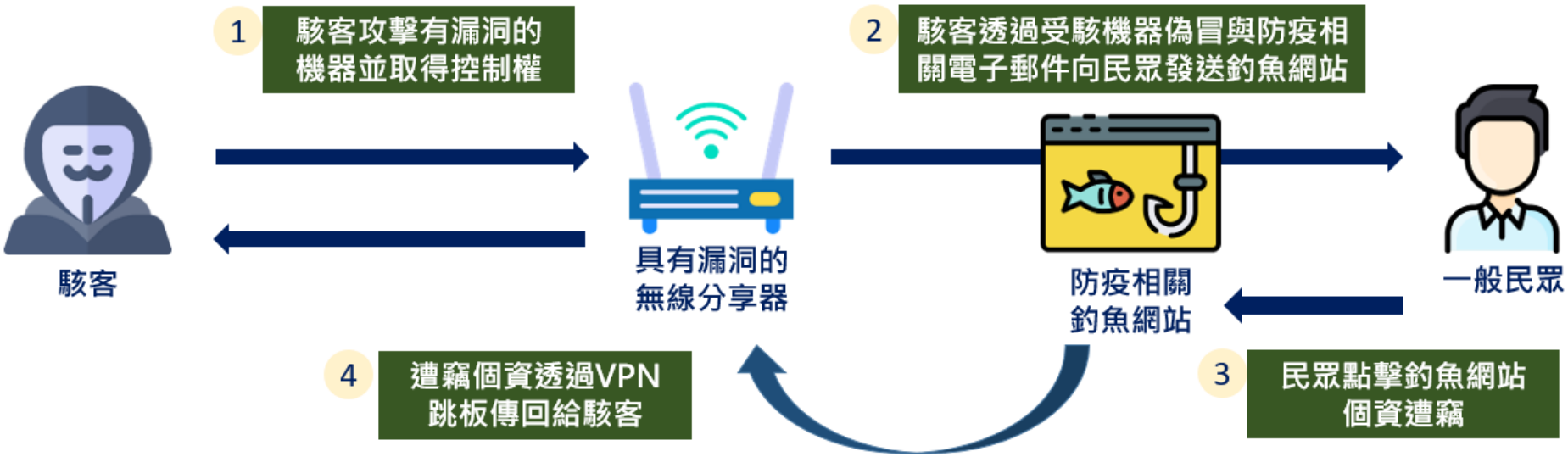
1. 臺灣校園遭遇到的比特幣勒索事件
   - 校園出現連網印表機濫用的情形，自動印出勒索比特幣的恐嚇文件
   - 主要是設備並無設定防護機制，以及不安全的部署，所以容易成為被入侵目標。
   - 廠商沒有做好設備的資安維護，由於存在未知漏洞，可能成為系統安全性的死角。
2. 室內外監視器遭攻擊而不自知，在2014年就有國外網站，直播全球數萬未重新設置密碼的攝影機影像，不少臺灣監視器即時畫面也在其中。

觀注重點

- 應定期進行系統安全性更新，修補漏洞並持續追蹤改善。
- 設備廠商要做好類似隱私衝擊分析（PIA）的工作，讓潛在隱私風險可以被管控
- 建議應定期監控、審查及稽核供應商提供之服務，確保供應商業務流程落實資訊安全管理
- 採用加密連線來防止遭到入侵，並強制使用者變更預設密碼，加入韌體無線更新 (FOTA) 功能，必要時可方便修補韌體。

結合網通設備與社交工程攻擊

防疫期間釣魚網站攻擊手法



■圖來源 : TWCERT -防疫與防駭 - 資安新思維

勒索軟體攻擊風險激增

資料來源： NCCST-吳啟文主任 2021.03.09

由亂槍打鳥轉向**特定目標**，遭鎖定對象包含**委外廠商**、**機關人員**、 **公文系統資料庫主機**、對外服務網站、環控系統、檔案分享系統 等，藉以**癱瘓系統運作**，中斷服務提供

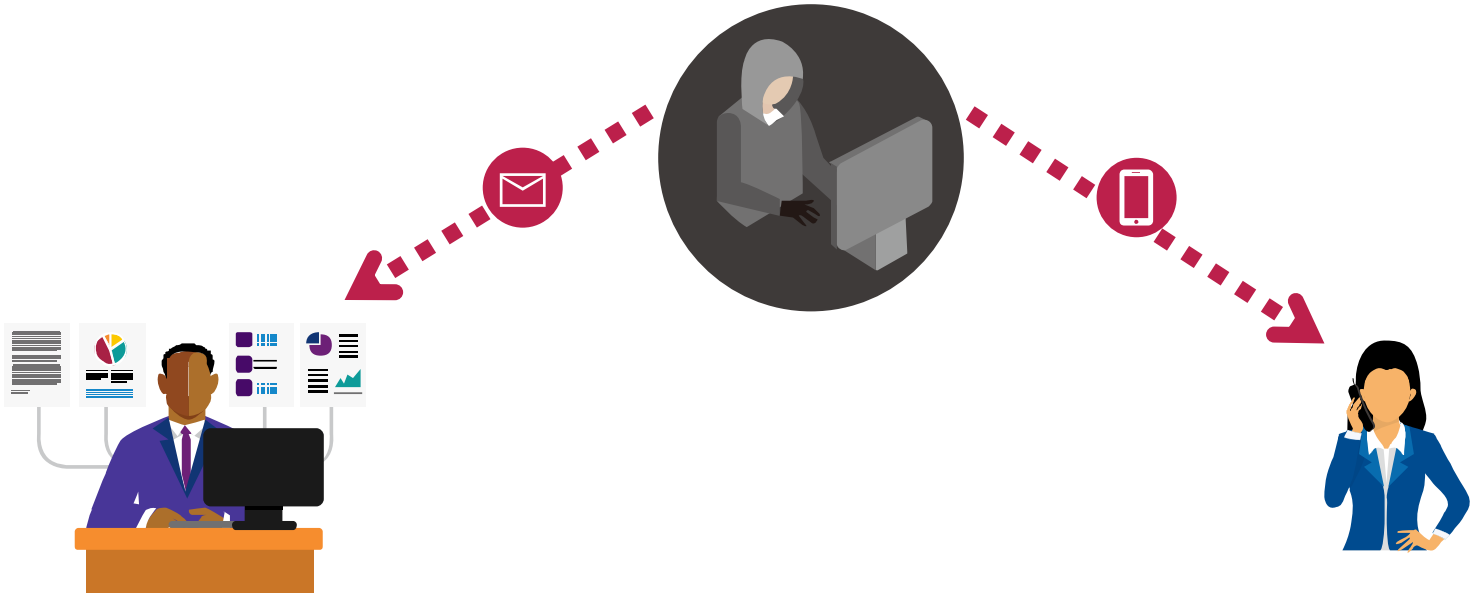
1. 使用者會感染勒索病毒，大多經由不明來源的惡意電子郵件內的附件或連結下載到惡意程式。
2. 兩大類型
   - 封鎖型：將電腦鎖住，讓使用者無法使用。
   - 加密型：將電腦上的重要資料加密 ，但不干擾電腦的功能，通常會在勒索訊息當中加入倒數期限，將所有被加密的資料刪除。

觀注重點

- 建議組織之資安防護措施可落實全天候監控網路安全性、啟用RDP連線使用MFA身份驗證、對員工實施社交工程之教育訓練、將最重要和最新的資料定期備份在離線的儲存裝置上，並定期測試、確認資料可用性與完整性、使用者存取權限採最低權限原則、制定有效的事件回應計畫並依需要進行更新。
- 應定期進行系統安全性更新，修補漏洞並持續追蹤改善。
- 建議組織定期對核心系統進行資料備份，對備份資料定期測試其可用性與完整性，預防遭勒索軟體攻擊時重要資料被加密並無法復原之情形。

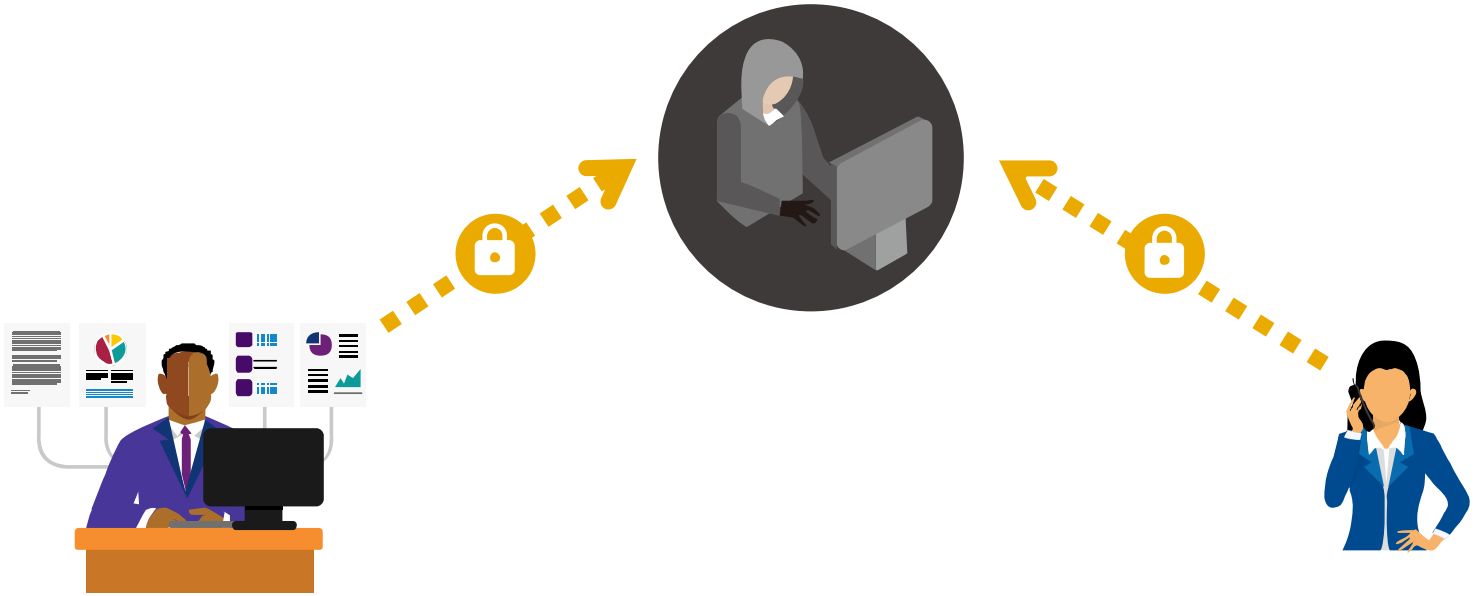
社交工程簡介(1/3)

- 利用人性弱點，應用簡單的溝通和欺騙技倆。
- 利用電子郵件誘騙使用者開啟檔案、點開連結，以植入惡意程式、暗中蒐集機敏性資料。
- 以電話偽裝委外廠商維護人員或上級單位人員，乘機騙取帳號及通行碼



社交工程簡介(2/3)

- 使用者的帳號、通行碼、身分證號碼或其他機敏資料。
- 隨時提高警覺，未經確認不提供資料、不開啟來路不明的電子郵件及附加檔案、不登入未經確認的網站，能避免社交工程的攻擊傷害。



社交工程簡介(3/3)

佯裝資訊人員

- 利用電話佯裝資訊人員，騙取帳號及通行碼。

假冒委外廠商

- 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。

偽造釣魚網站

- 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。

惡意程式附件

- 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中蒐集機敏性資料。

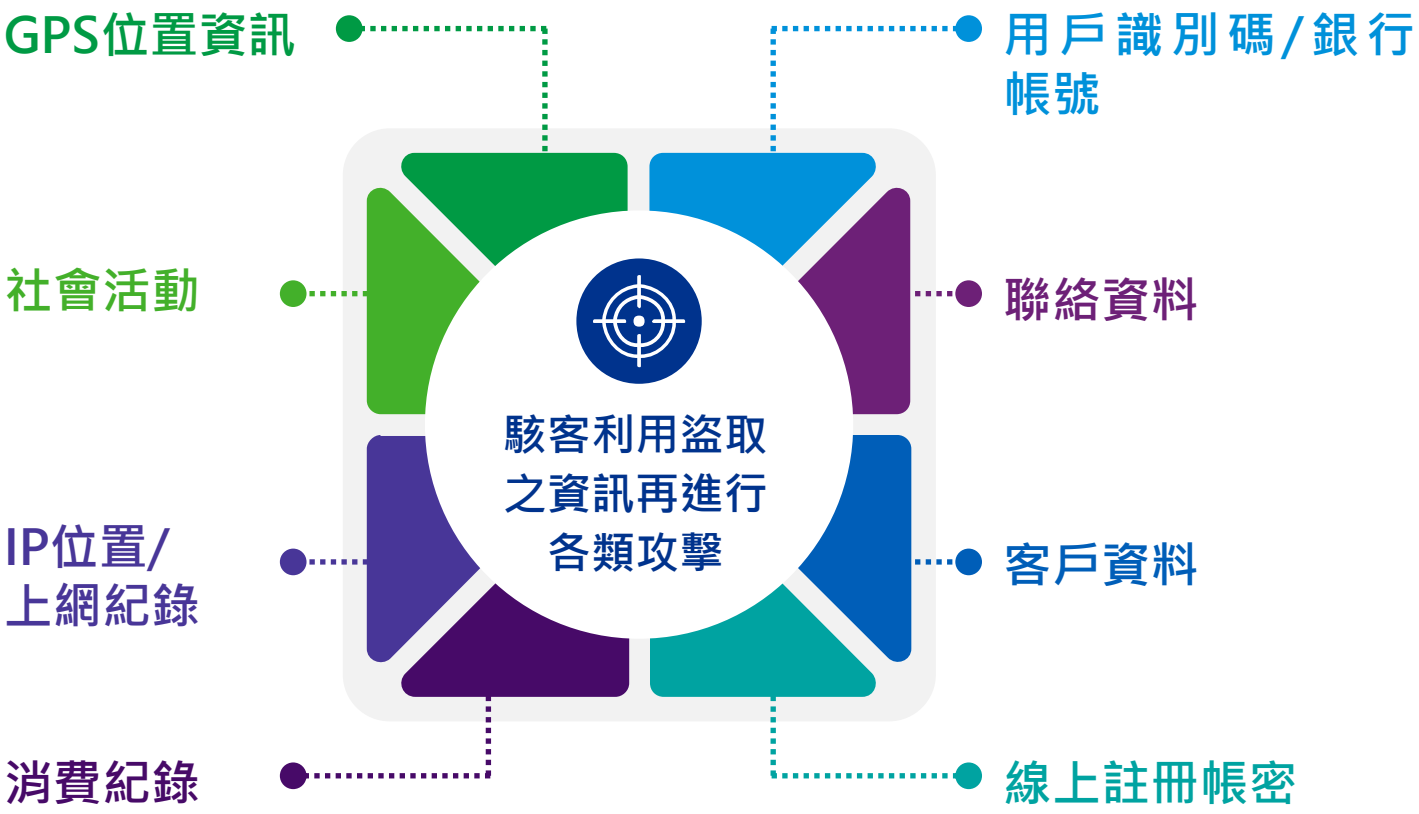
盜用親友名義

- 利用即時通訊軟體，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

冒充軟體更新

- 誘騙使用者下載，如偽裝的修補程式、P2P下載軟體、工具軟體等，乘機植入惡意程式。

駭客想要盜取的資訊


GPS位置資訊
用戶識別碼/銀行帳號
社會活動
聯絡資料
駭客利用盜取之資訊再進行各類攻擊
IP位置/上網紀錄
客戶資料
消費紀錄
線上註冊帳密

電子郵件社交工程攻擊模式

最新社交工程攻擊手法

From: nccst-tw@outlook.com <nccst-tw@outlook.com>
Sent: Friday, October 14, 2022 11:33 AM
Subject: 關於緊急開展第六批資安抽樣審查的通知

行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

資通安全協查函

各收信單位：

進期，行政院國家資通安全會報技術服務中心、國家電腦網絡危機處理暨協調中心，偵測到台北固網鏈路節點、台中固網鏈路節點存在可疑網絡流量，經專家團隊研判，初步判定爲境外惡意網絡攻擊。

現依據國家資通安全管理法[A0030297]（詳見第三章“特定非公務機關資通安全管理”），資通安全事件通報及應變辦法[A0030305]（詳見第三章“特定非公務機關資通安全事件之通報及應變”）相關條文，對貴單位開展緊急資通安全審查。

爲確保此次資安審查真實性，本次審查采用不提前知會，不發佈公告隨機抽樣的審查方式進行。收到此封郵件，則需按要求參加此次資通安全審查。**請下載郵件所附壓縮檔案使用壓縮檔案之工具于10月21日前，完成此次資通安全審查。**

依照國家資通安全管理法，若未按要求完成此次資通安全審查，將按照國家資通安全管理法依法追究相關人員之法律責任。

國家資通安全管理法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297)

行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

附注：壓縮檔案保護密碼爲 nccst2022

最新社交工程攻擊手法(續)

數聯資安
Information Security Service Digital United

資通安全協查函

各收信單位：

進期，數聯資安監控中心及資安整合服務平台偵測到台北固網鏈路節點、台中固網鏈路節點存在可疑網絡流量，經專家團隊研判，初步判定為境外惡意網絡攻擊。

現依據我國資通安全管理法[A0030297]（詳見第三章“特定非公務機關資通安全管理”），資通安全事件通報及應變辦法[A0030305]（詳見第三章“特定非公務機關資通安全事件之通報及應變”）相關條文，對涉事相關單位開展緊急資通安全審查。

為確保此次資安審查真實性，本次審查采用不提前知會，不發佈公告隨機抽樣的審查方式進行。收到此封郵件，代表你需按要求參加此次資通安全審查。請下載郵件所附資通安全審查工具和說明流程，在10月28日之前，完成此次資通安全審查。

依照國家資通安全管理法，未按要求完成此次資通安全審查，并因此造成三級及以上資通安全事件的（依據111年8月23日發佈的資通安全事件通報及應變辦法定級），將按照國家資通安全管理法依法追究相關人員之法律責任。

國家資通安全管理法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297)

資通安全事件通報及應變辦法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305)

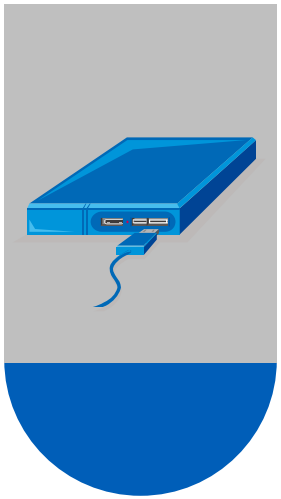
數聯資安

Information Security Service Digital United

附注：壓縮檔案之解壓密碼統一為ISSDU@2022

附件：附件1-ISSDU資通安全審查[11101025].zip

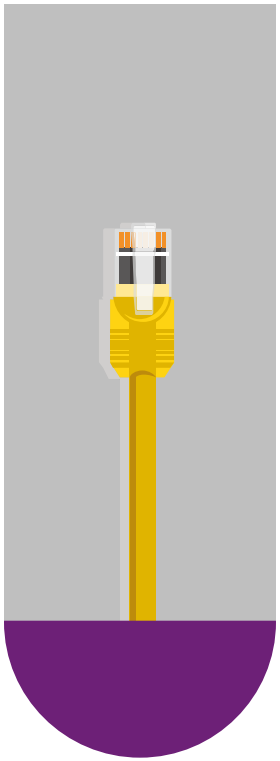
電子郵件社交工程攻擊可能造成的後果



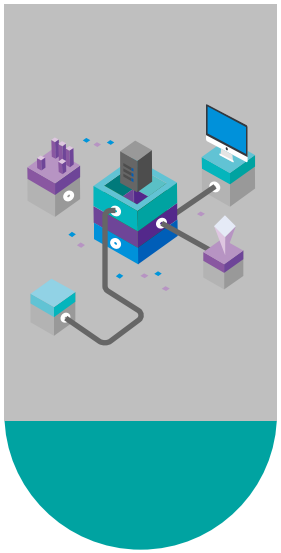
竊取硬碟中的檔案資料

監聽鍵盤輸入的敏感資料

遠端遙控用戶端電腦

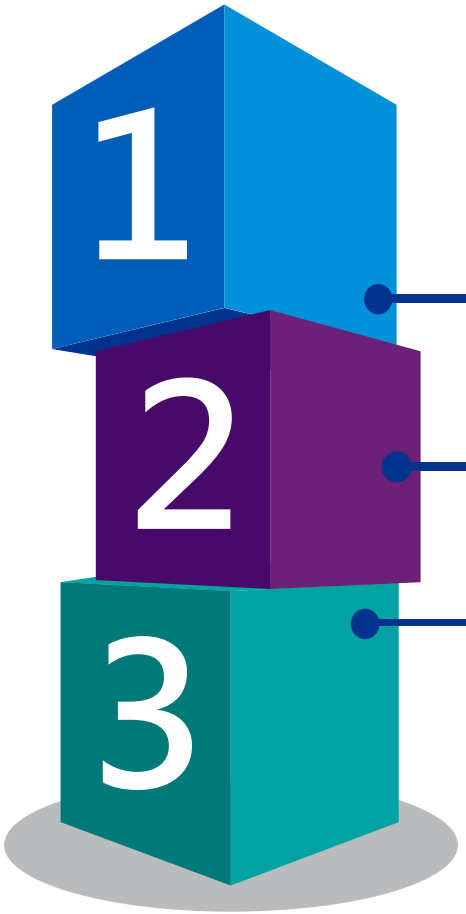


攻擊其他內部的電腦



成為攻擊內部網路的跳板

預防社交工程攻擊應注意的細節



是否為正確的的網址？

點擊網址前，最好再三確認網址是否正確，小心注意似是而非的網址，例如：
www.google.com.tw vs www.g00gle.com.tw
www.taipei101.com.tw vs
www.taipeil0l.com.tw

寄件人是否是熟悉的同事或親友？

可藉由其他的管道連絡寄件者，確認其信件的真偽

從別處連結

若是與自身財務或權益相關的網址連結，建議可利用其他安全的方式進行連結

安全的個人電腦使用習慣

啟用Windows防火牆

對重要資料進行加密、備份

保持在最低的
使用權限

提高警覺，
加強危機意識

- 定期登入你的網路帳號
- 定期確認銀行帳戶、信用卡的交易狀態都正確無異常
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式

安全的電子郵件使用習慣

收信

- 檢查**寄件者的真偽**
- 確認信件**內容的真實度**
- 不輕易開啟郵件中的**超連結以及附件**
- 開啟超連結或檔案前，確認對應軟體 (例如：IE、Office、壓縮軟體) 都保持在**最新的修補狀態**

轉信或寄信

- **未經查證之訊息**，不要轉寄
- 轉寄郵件前先**將他人郵件地址刪除**，避免將別人郵件地址傳出
- 寄送信件給群體收件者時，應將收件者列在**密件副件**，以免收件人資訊外洩。

防止上鉤7撇步

點選連結前，先移動滑鼠檢查真實來源

定期更新瀏覽器漏洞，並更新至最新版本

搜尋網頁，請確認網址真實性，避免以假亂真，比如英文O變造為數字0；字母l變造為數字1

勿回覆要求提供個人資料的電子郵件，即使信中有該公司的商標

不要向不請自來的電訪人員透露任何個人或同事資料

直接在瀏覽器輸入網址或是將常用網站加到我的最愛/書籤清單中

避免開啟網路上之任何附件檔，可利用網路安全軟體先行掃過後再開啟

六個小提醒

1 技術層面

- 修補系統漏洞
- 安裝防毒軟體
- 安裝間諜程式檢查軟體
- 關閉信件預覽

2 三個思考

- 開啟信件前請三思
- 開啟連結時請三思
- 開啟附件檔案時請三思

3 網址內容是否正確

- 應注意**網址是否正確**，在確認網址安全前勿隨意點擊

4 確認寄件者身分的真偽

- 在看到親友同事寄來的信件時，也不能掉以輕心
- 建議再三檢查寄件者電子郵件
- **可利用其他的管道確認寄件者的真偽**

5 以安全的方式連結至網站

- 建議勿點擊來路不明電子郵件中的網址
- 最安全的方式為找到安全的途徑進入該網頁

6 應注意藏於細節內的危險

- 許多的社交工程攻擊都是**利用使用者較為疏於防範的細節**進行攻擊
- 因此必須**要注意藏於細節中的危險**

台灣產業資安曝險分析

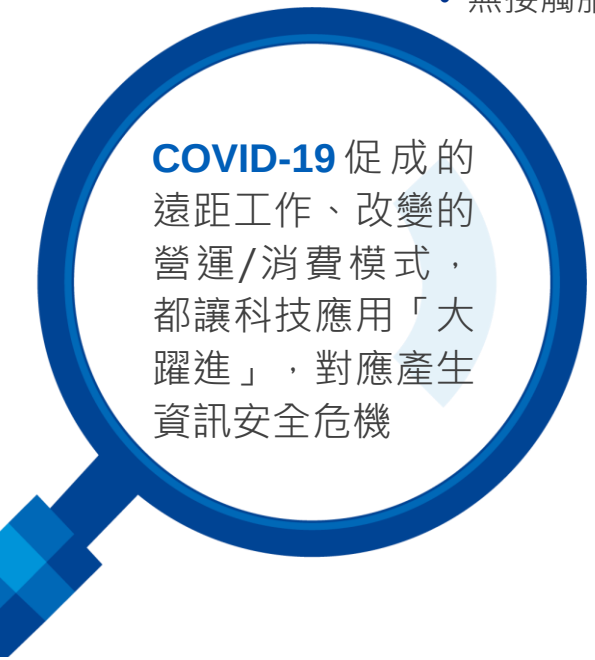
臺灣當今面臨史無前例的資安大挑戰

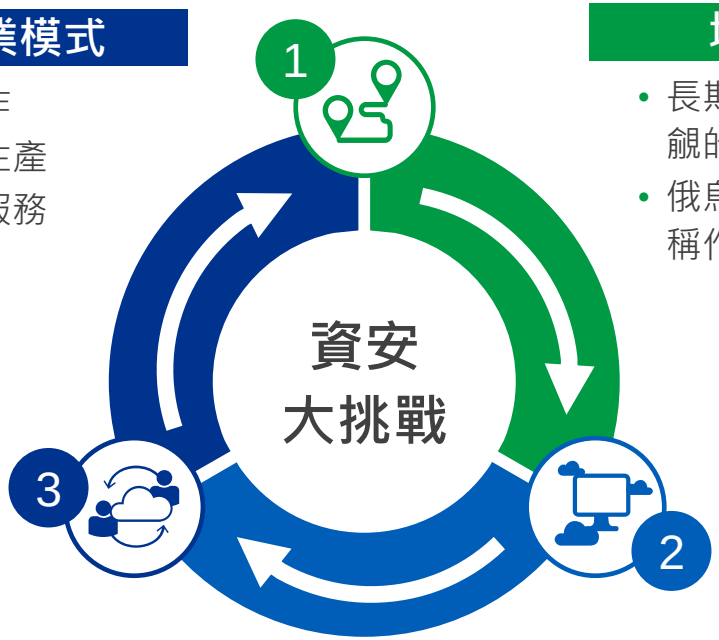
新商業模式

- 遠距工作
- 無人化生產
- 無接觸服務

地緣政治

- 長期為中國駭客覬覦的標的
- 俄烏戰爭催化不對稱作戰





新興科技

- 營運管理制度結合數位科技以提高營運流程效能
- 雲服務、零信任、物聯網、人工智慧、5G、區塊鏈等應用方興未艾

調查作業核心目標

量測全面網路風險

- 資安9項技術檢測
  + 量化人力資源風險4項

比較產業資安現況

- 依營運特性分成六大產業
- 掌握同產業、委外/ 合作廠商所屬產業的曝險控管情況

配置合理資安預算

- 讓讀者以最少的資源(人/財/物力)，處理與改善資安風險

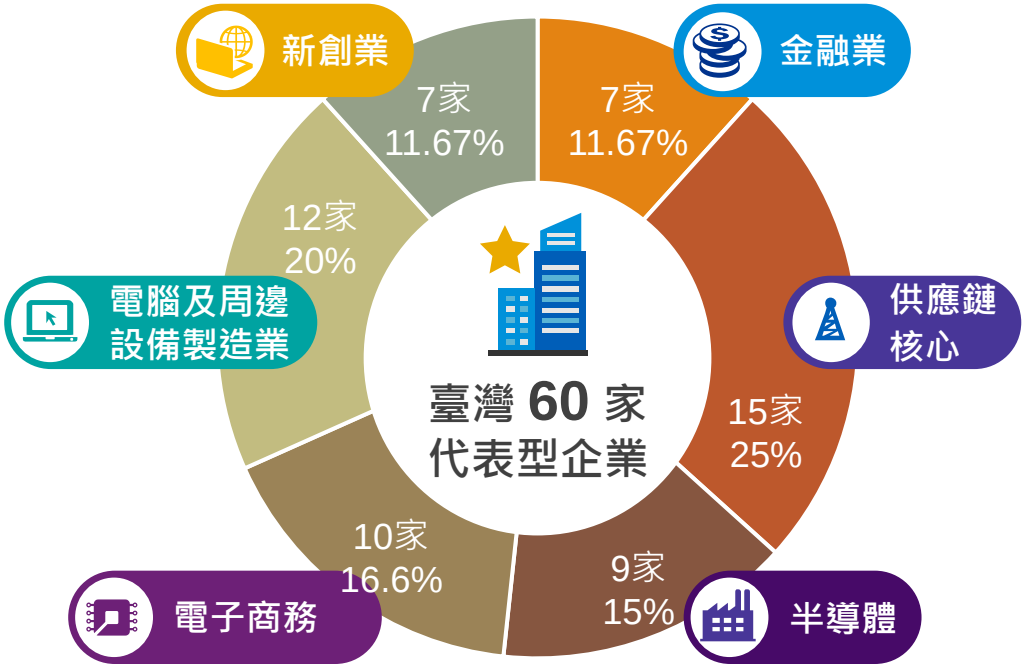
部署資安防禦策略

- 以各面向的檢測結果，給予深入剖析與建議

企業調查範圍

時間：2021年12月-2022年2月

抽樣方法：KPMG 以富比士、證交所及台灣新創競賽所列企業為母體，結合風險評估之經驗，依據六大產業(電腦與周邊、半導體、電商、新創、供應鏈核心與金融)進行分層隨機抽樣。



資安曝險調查方法之特色

本資安曝險大調查有別於傳統企業內部執行的資安風險評鑑、弱點掃描或滲透測試演練等活動，以及其他問卷、訪談等調查，具備以下特點：

資安曝險評估方式比較

	本資安曝險調查	弱點掃描	滲透測試
侵入式檢測	否	視情況而定	視情況而定
資料提供	網域名稱	URLs、IP (視情況增加測試用帳密)	URLs、IP (視情況增加測試用帳密)
檢測手法	自動化工具檢測	自動化工具檢測	手動組合式攻擊
檢測範圍	外部的網際網路風險	內部的資安漏洞	內部外部潛在的資安漏洞
評估面向	從網路多面向進行分析 例如 應用安全性、人力資源風險等	大範圍偵測主機設備漏洞 例如 Injection、XSS、Security Misconfiguration	透過組合技驗證商業邏輯漏洞 例如 權限跳脫、目錄瀏覽、URL 重新導向等漏洞

探勘的3大面向與14項檢測項目

應用面安全 Application

- **Application Security**
  應用程式風險
- **Domain Attacks**
  網域安全
- **Exposed Services**
  服務暴露風險
- **Technologies**
  技術風險

人力資源風險 Human

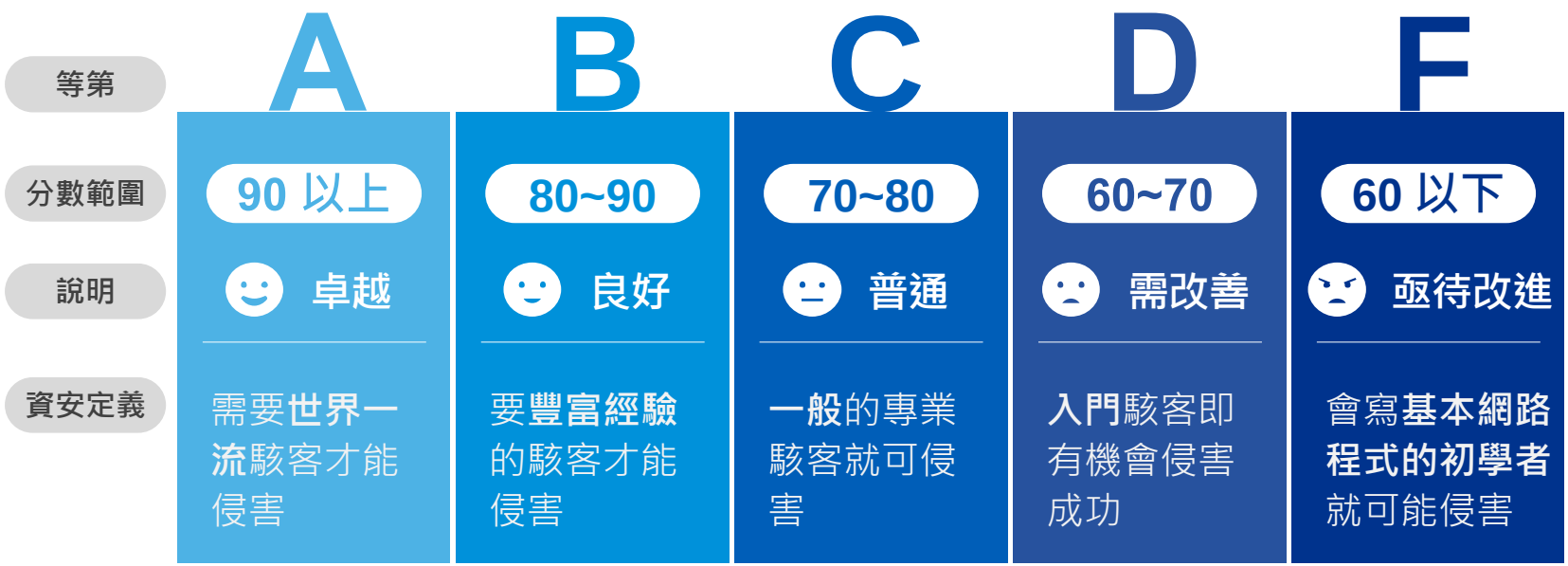
- **Responsiveness**
  資安事件回應力
- **Employee Attack Surface**
  網攻承受力
- **Security Team**
  資安團隊戰力
- **Social Posture**
  社群媒體風險

網路與科技風險 Network and IT

- **Asset Reputation**
  資產聲譽評量
- **Cloud**
  雲端服務風險
- **DNS**
  域名解析風險
- **TLS、Mail Server**
  電子郵件與網路加密風險
- **Web Server**
  網頁系統風險

技術檢測分數意涵

將技術檢測得出的網路防護分數，以每十分為一級距，分為A、B、C、D、F五個等級，提供讀者一個更直觀、易懂的衡量標準



調查結果總覽 – 臺灣產業曝險控管概況

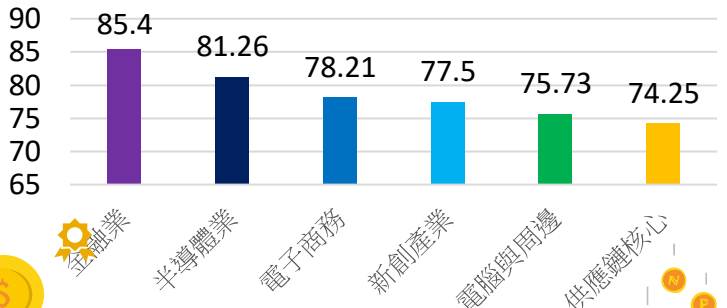
1 平均網路防護分數 **C (78.72)**

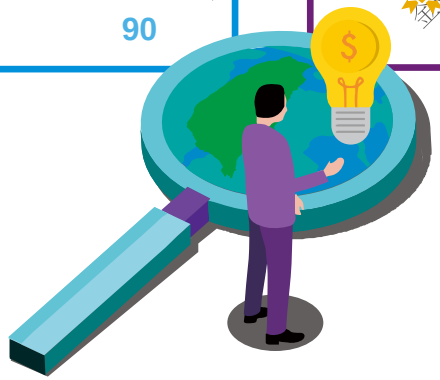
臺灣受調企業平均繳出C級的防護成績單，持續面臨高度網路風險，亟需改善內部的資安現況

F D C B A

60 70 80 90

2 臺灣企業資安模範生地位持續穩固





調查結果總覽 – 網路防護能力總表

分數 低 高

資安曝險評估項目	評估說明	臺灣60家受調企業
應用面安全	應用程式風險	
	網域安全	
	服務暴露風險	
	技術風險	
人力資源風險	資安事件回應力	
	網攻承受力	
	資安團隊戰力	
	社群媒體風險	
網路與科技風險	資產聲譽評量	
	雲端風險	
	域名解析風險	
	電子郵件風險	
	網路加密風險	
	網頁系統風險	

調查主要發現

1 多數企業輕忽社群媒體所衍生的網路攻擊

大部分企業都擁有社群媒體的專頁，且員工也非常容易於社群媒體上暴露自己的公司聯絡資訊，導致駭客發動魚叉式精準社交工程時，成功得手機率大增。

2 臺灣各產業資安人員能量均嚴重不足，企業資安人力亮警訊

臺灣企業在人力資源風險(Human)中，於「資安團隊戰力」相關成績顯示，資安人力缺口十分明顯。60 家受調企業中，經外部情資分析顯示，就可能有高達一半以上企業未配置CISO或資安人員。

3 供應鏈核心產業亟需加強網路防護

原物料、運輸業等產業，不僅在平均網路防護分數墊底，該產業更有高達近50%的企業落在整體排名的倒數15名，網路防護亟待加強。

4 金融業網路防護表現仍最佳，但面臨高度挑戰

金融業於各面向(應用程式、人員、網路與科技)的平均分數皆取得優異的成績。但因金融網路犯罪利益巨大，讓金融業今日仍飽受內外部威脅與挑戰。

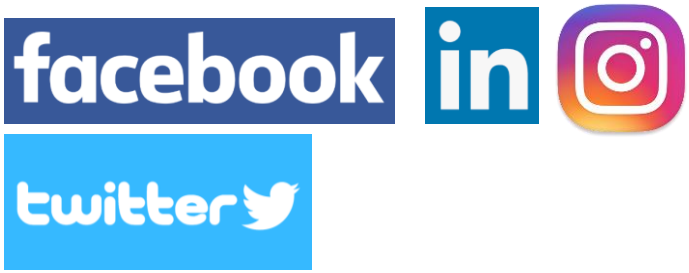
5 導入並驗證資安國際標準，將顯著降低資安曝險

本調查發現國際資訊安全認證能顯著的提升資安能力，且在導入國際資訊安全認證的企業中，資安實力落差意外的處於光譜的兩端，對比通過與宣稱遵循國際資訊安全標準的群體中，資安實力仍可有不可忽視之差距。

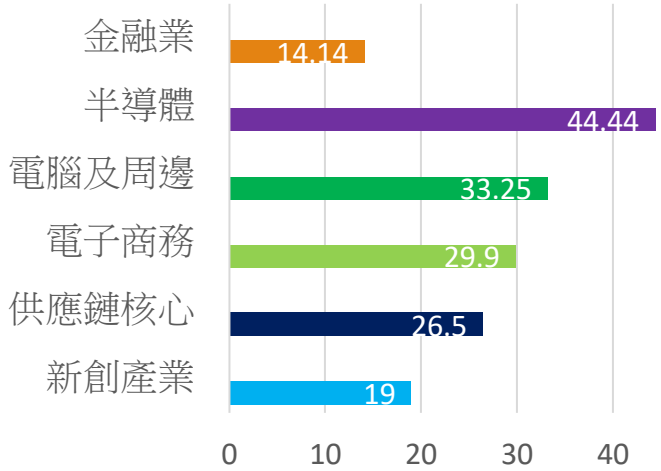
1 多數企業輕忽社群媒體所衍生的網路攻擊

本調查發現不分產業，非常令人意外的，企業數位曝險因子竟來多自於社群媒體。我們在社群媒體風險(Social Posture)檢測中，綜合所有產業平均數為不及格 **(29分, F等級)**。主要原因是目前多數企業大量運用社群媒體 (如Facebook, Twitter, LinkedIn等)觸及受眾，而於有意無意間留下公務聯絡訊息 (如電子郵件、電話等)。另一原因是員工於註冊社群媒體時，時常將目前服務之企業名稱、公司電子郵件等資訊，提交於社群網站的個人資料上。此類行為，使得員工相關資訊十分容易取得，容易讓駭客發動魚叉式社交攻擊，且可透過社群媒體推論企業電子郵件帳號之命名規則，不可不慎。

建議企業應針對社群媒體運用，制定妥適管理規範
並透過資安縱深防禦策略、Anti-spam等機制，有效的協助防護企業電子郵件安全，避免Credential遭到竊取，引發後續更嚴重之後果。



本調查主要社群媒體來源

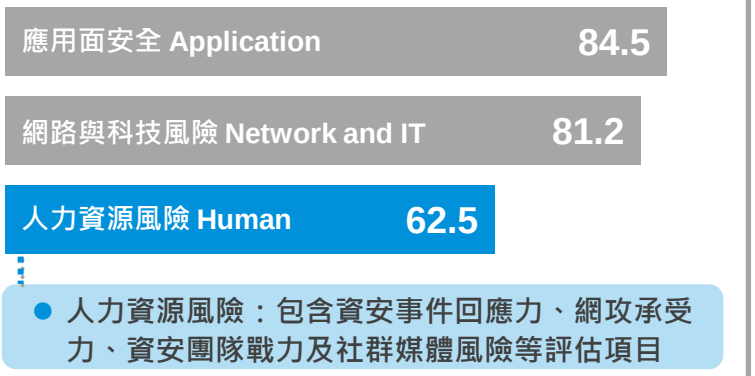


2 臺灣各產業資安人員能量均嚴重不足，企業資安人力亮警訊

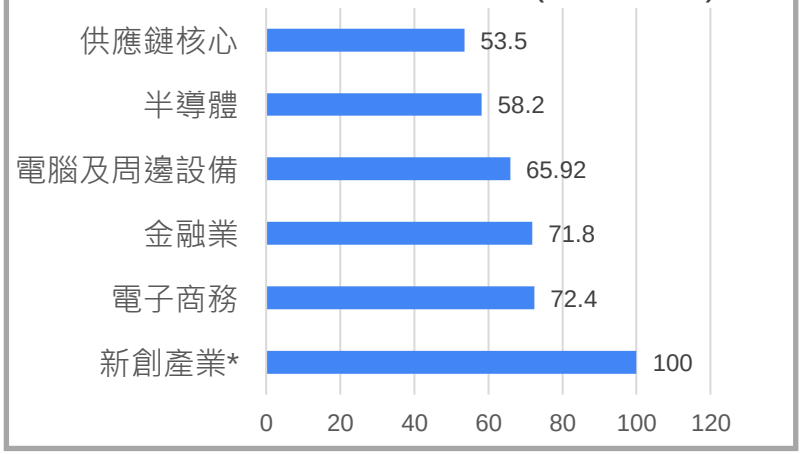
本調查從公開資訊中蒐集受調企業的資料發現，於資安人力評比的項目中，僅有金融業與電子商務兩大產業的資安團隊分數超過70分，其餘皆分數皆差距甚遠。

反觀電子商務及金融業因在用戶期待與主管機關的要求下，對於設置資安人員配置皆有強烈的需求及法規要求，因此相較於其他產業，對於資安人力投入相對較高。

資安曝險分數三大面向－應用面安全、網路與科技風險、人力資源風險



人力資源風險－資安團隊戰力 (依產業區分)



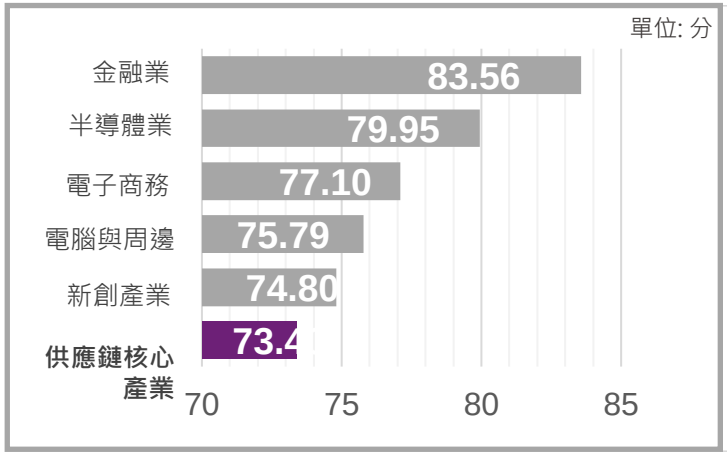
註：因調查工具限制，新創產業中僅有1家可呈現資安團隊戰力相關數據 ，另其餘6家均未有明顯資訊，故分數以呈現該企業為主，而非產業平均。

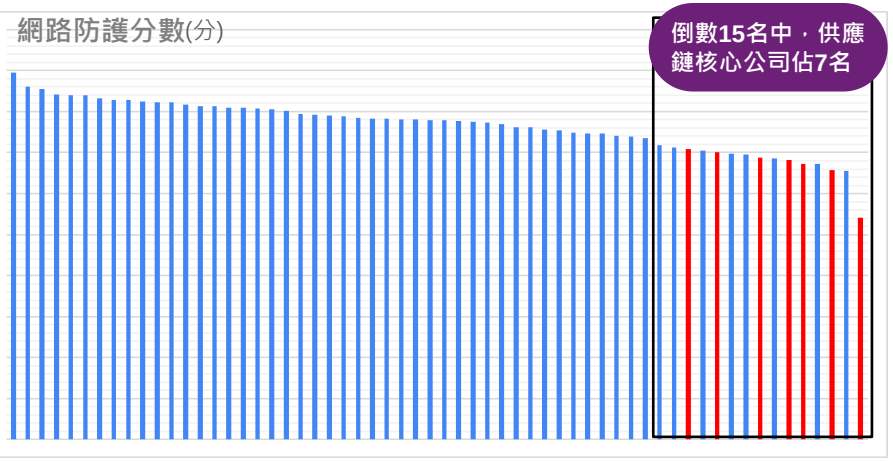
3 供應鏈核心產業亟需加強網路防護

本調查發現原物料、運輸業等這類串聯供應鏈的核心產業資安實力不均，且超過60%的受調企業分數位居C級以下，雖然少數公司(2家位於前五分之一)表現出眾，但多數企業之資安防護能力卻有待加強。

推測其可能原因，為上述產業因近年開始導入大數據與人工智慧等新興科技，智慧應用大幅增加，網路架構更為複雜、系統軟體未能即時更新與升級等，都使駭客有機可乘。KPMG也因此建議原物料、運輸業等這類串聯供應鏈的核心產業，在享受數位化的美好果實時，更應努力提升其網路防護分數。

網路防護分數 (依產業區分)

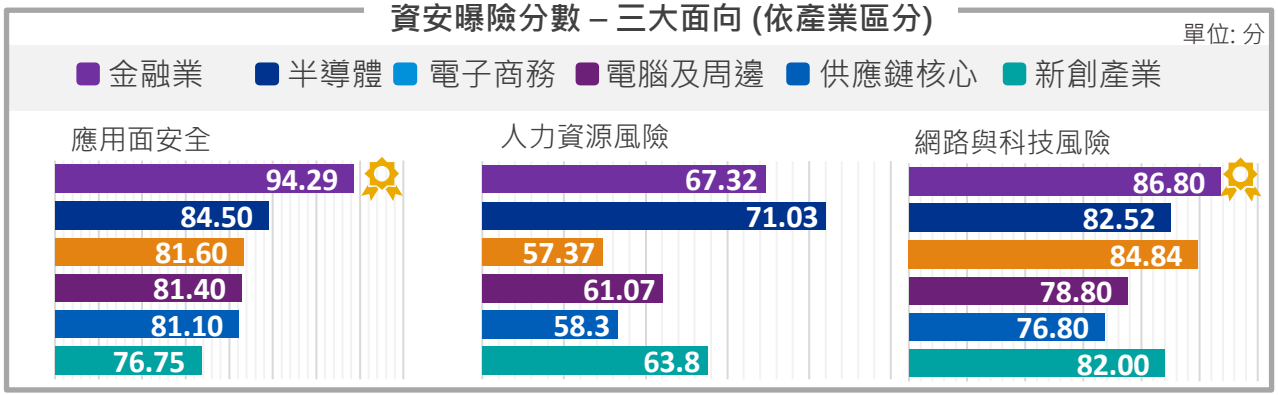




4 金融業網路防護表現最佳，但仍面臨高度挑戰

金融業在網路防護分數的三大面向中，不論是**應用面安全、人力資源風險及網路與科技風險均取得了相較全產業表現優異的成績**。其中臺灣產業表現有待加強的「網路與科技風險」，**金融業仍維持接近86分的高水準，更高於全球金融業平均分數(81分)**。分析國內金融業普遍成為「績優生」，是因為主管機關的高度監理及產業的自律性。在違反金融法規時，除了將遭重罰，信譽下降、創新服務無法順利上線等因素都將造成重大營收損失，因此讓金融業成為台灣企業的資安標竿。

雖然金融業資安能力普遍高於其他產業，然而金融業擁有豐富且價值高的資訊與資產，近年又廣泛使用金融科技、開放金融資料並與多元的第三方合作而擴大曝險層面，因此至今仍為駭客集中精力攻擊之標的。國際研究機構的報告即指出，**金融業受到網路攻擊的可能性為其他業的300倍**，且每年攻擊數都在攀升，而全球**金融企業每年平均承擔網路犯罪的成本更是高達5.28億新台幣**。



5 導入並驗證資安國際標準，將顯著降低資安曝險

在60家台灣企業中，其中有21家企業有取得國際資安管理標準認證，含全數金融業。對比鋪險分數可以發現，成績越高的群組，通過資安國際標準的比例越高。但許多已於年報中提及組織規定落實國際資安標準，但未通過第三方驗證的公司，經本調查結果分析，分數均普遍經不起考驗。

分析情境一：

不考慮產業別，以資安國際標準通過與否評估資安防護能力

- 通過資安國際標準能明顯提升企業資安防護能力

分析情境二：

不考慮是否通過標準的情況下，與金融業進行防護能力比較

- 金融業平均資安防護能力最佳
- 電腦及周邊設備、電子商務、半導體、基礎建設等產業平均資安防護能力明顯較差

分析情境三：

不考慮其他因素，僅以產業類別探討資安防護能力

- 通過資安國際標準平均可提升資安防護能力

曝險分數	取得資安認證企業數	資安認證企業佔比
85 以上	9	64.2% (9/14)
80 ~ 84	3	33.3% (3/9)
75 ~ 79	5	33.3% (5/15)
70 ~ 74	3	21.4% (3/14)
未滿 70	1	12.5% (1/8)
小計	21	60

新興科技之資安議題

想像一下未來的生活


Digital Freight Brokerage
On-demand Van Kit
Local Generation
Urban Consolidation Centre
AV Truck Platooning
Alternative Fuel Station
AV Drive Thru
Battery Stack
Reclaimed Green space
Distribution Networks
Fleet
AV Only Lane
Dense AV parking Hub
Drone Delivery
'Packstations' Drop Boxes
Drivers do route planning and handovers
Delivery to Car
Smart Delivery Vehicles
Crowd Sourced Boot Sharing
City Hall Traffic Brain
Sharing Economy & On-demand Cycle Delivery
Vehichle to Grid Technology
Extensive Chargepoint Networks
Home Charging
Digital Front Door Access
Ultra Low emissions ZONE
Ground Transportation Robot
No Congestion

IoT物聯網的應用

IoT物聯網的應用-穿戴裝置

新興科技資安議題 – 5G網路

5G願景與應用情境

■ 5G應用服務

5G潛在應用服務發展方向上，強調即時、大量、同地點、多人的資料傳輸，目前5G鎖定的應用服務包括智慧聯網汽車、智慧醫療、智慧教育、緊急疏散服務、遊戲服務、智慧家庭/居家安全， 其中智慧聯網汽車、智慧醫療、智慧教育、緊急疏散皆需要建構基礎建設、普及低價的終端，此與社會福利有極大的相關性，推估政府將在5G應用服務下扮演重要的主導角色，也代表著5G為先進國家未來社會發展與產業競爭的核心。

全球資安商 Check Point 發佈 2021 年網路安全趨勢預測，指出 81% 的企業已大規模採用遠距辦公模式，且 74% 的企業預計永久實行此模式，因此企業 IT 和資安團隊應持續注意企業數位轉型後的全新工作模式，以迎接新常態。Check Point 也提醒未來各地企業可能遭到更多與疫情相關的複雜網路攻擊，如以疫苗為誘餌的網路釣魚活動、針對遠距學習者的攻擊、更多的雙重勒索攻擊等；隨著 5G 上路，使用者須注意手機資料外洩及物聯網可能遭駭的風險。5G 將打造一個萬物互聯的高速世界，卻也為犯罪分子和駭客提供了更多攻擊機會。為了保護個人隱私，需要更全面地保護 5G 裝置中的大量資料，防止資料遭洩露、盜竊和篡改，尤其須注意許多資料可能繞過公司網路及其安全控制。

新興科技資安議題 – 5G網路(續)

網路架構出現重大變化，資安風險隨之大幅增加

■ 5G基礎架構的變化

無線存取網路（RAN）等5G的基礎架構中，提供了新的異質接取網路，使得物聯網（IoT）設備能有多種接入網路的做法，大幅增加了攻擊面。

■ 5G網路的虛擬化

為了降低建置成本，5G網路傾向減少使用專屬硬體，而是以軟體提供相關功能的策略發展，同時，為了讓5G電信服務更有彈性，業者也採用網路虛擬化架構，包含導入軟體定義網路（SDN），以及網路功能虛擬化（NFV）等技術，這種將網路虛擬化的做法，也會帶來更為複雜的環境，進而產生有關的弱點。

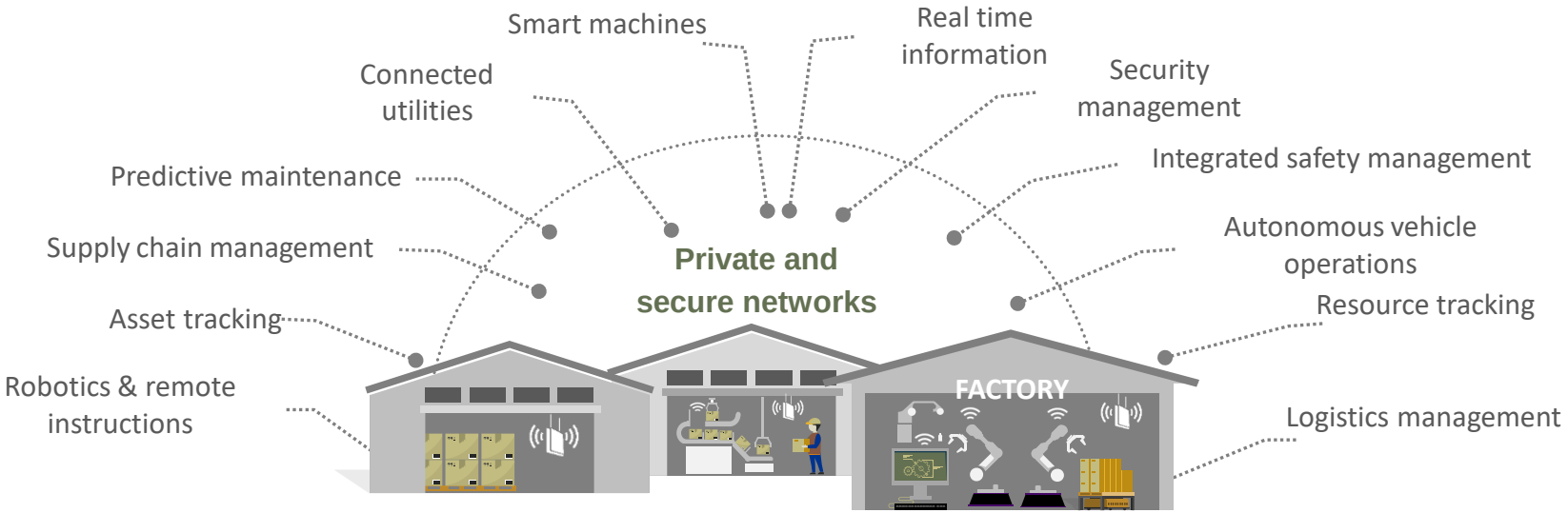
■ 5G應用系統-開源軟體

5G的應用上，電信業者往往透過開源軟體，來開發相關的系統。這些軟體很可能會因為電信業者缺乏弱點管理，潛藏了漏洞而遲遲沒有察覺，再加上駭客也可以直接取得軟體來進行研究，找出可被濫用的弱點。

未來5G應用情境

- 持續優化、專屬服務及確保安全

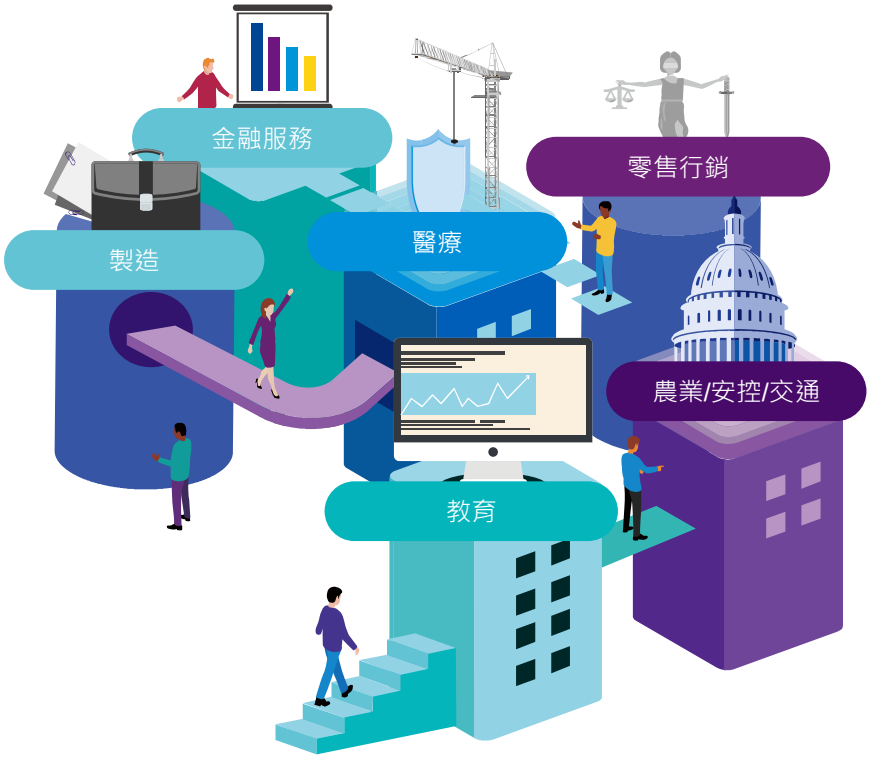
- 私有通訊網路將支持廣泛的運用情境，並將持續地進行優化、特定用途及確保安全性



優化	專屬	安全
可因應不同的IoT實作技術裁適運用，如：QoS、延遲性	區域網路、易於佈署及獨立管理	蜂巢式網路安全與敏感資料當地存儲

人工智慧應用的熱門領域

台灣AI應用五大領域 by 2020軟協AI大數據智慧應用案例分析



AI商業應用發展條件分析

新興科技資安及隱私議題 – AI人工智慧(1/3)

AI 與 ML 遭到不肖利用及濫用的現況

■ Deepfake 深度偽造技術

一項目前廣獲駭客青睞的 AI 技術就是 Deepfake 深度偽造技術，這是一種用來創造或變造影音內容使其看起來幾可亂真的 AI 技術。Deepfake 結合了「深度學習」與「影音變造」兩項技術，由於它所製作出來的影音內容幾可亂真，即使有科技的幫助也很難分辨真偽，因此未來很可能被用於散布假訊息。而在幾乎人人都會使用網際網路與社群媒體的情況下，Deepfake 將以前所未有的速度觸及全球數百萬人口。

Deepfake 技術很容易被有心人士用來扭曲事實以滿足其不良意圖，一個很好的案例就是一段據稱是某位馬來西亞政治人物助理與內閣官員之間的性愛影片。該影片在 2019 年被人釋出，並要求調查該名內閣官員的貪腐行為。重要的是，該影片的出現導致了聯合政府的動盪，證明 Deepfake 確實可能造成政治效應。還有另一個案例是英國能源公司被騙匯了將近 20 萬英鎊 (約合 26 萬美元) 到一個匈牙利銀行帳戶，歹徒利用一段Deepfake 音訊假冒成該公司的執行長來核准這筆匯款。

由於 Deepfake 這樣的 AI 技術隨時可能被歹徒利用，因此一般人有必要知道像這樣的內容可以真實到何種程度，以及歹徒的運用方式。有趣的是，Deepfake 也可用來教導人們認識其不肖用途：2018 年，網路媒體 Buzzfeed 與演員兼導演 Jordan Peele 合作製作了一段美國前總統歐巴馬的 Deepfake 影片，來提醒人們注意 Deepfake 的潛在問題，要人們小心不要輕易相信網際網路上的內容，包括看似真實的影片。

新興科技資安及隱私議題 – AI人工智慧(2/3)

AI 與 ML 遭到不肖利用及濫用的現況

■ 運用 AI 猜測密碼

網路犯罪集團正利用 ML 來提升其猜測使用者密碼的準確度。目前已經有一些較為傳統的方法，如：HashCat 及 John the Ripper 可根據密碼雜湊值的比對來成功猜出某個雜湊值所對應的密碼。然而，在神經網路與生成對抗網路 (Generative Adversarial Network，簡稱 GAN) 的協助下，網路犯罪集團將可分析大量的密碼資料並產生符合統計分布的密碼變化。未來，這將使得密碼的猜測更加精準，進而提高歹徒的獲利機會。

根據一篇 2020 年 2 月發布在地下論壇上的貼文，我們發現有個 GitHub 儲存庫提供了一個密碼分析工具能夠藉由分析 14 億筆登入憑證來產生密碼變化規則。

■ 在社群網路平台上假冒成人類

網路犯罪集團也會利用 AI 來模仿人類行為，例如，AI 能模仿人類使用應用程式的行為來騙過社群媒體平台 (如 Spotify) 的機器人偵測系統。網路犯罪集團會利用這類 AI 技術來製造假流量以捧紅特定藝人，進而從中牟利。

某個名為「nulled.to」的論壇上刊登了一個採用 AI 技術的 Spotify 機器人，宣稱可同時模仿多名 Spotify 使用者，它運用了多個代理器來躲避偵測。像這樣的機器人可用來增加特定歌曲的點播次數，進而賺取收入。此外，它還有另一招躲避偵測的技巧就是在建立播放清單時會模仿人類的音樂品味，而不是隨機將歌曲加入清單，因為這樣看起來才不會像是機器人所產生的。

新興科技資安及隱私議題 – AI人工智慧(3/3)

AI 與 ML 遭到不肖利用及濫用的現況

■ 將 AI 技術運用到駭客攻擊

網路犯罪集團正試圖利用 AI 來攻擊主機漏洞，例如，在 Torum 論壇上可以看到有使用者想知道如何運用 DeepExploit 這項具備機器學習能力的滲透測試工具。不僅如此，該名使用者還想知道如何讓 DeepExploit 能夠與 Metasploit 滲透測試平台結合，以便用來蒐集資訊，以及建立並測試漏洞攻擊。

在「rstforums.com」上可以看到一則關於「PWnagotchi 1.0.0」的討論串，這原本是一個用來運用解除認證 (de-authentication) 手法駭入 Wi-Fi 網路的工具。PWnagotchi 1.0.0 利用了神經網路模型以及遊戲化 (gamification) 機制，來提高破解的成功率。當系統成功解除某個 Wi-Fi 認證時，就會獲得獎勵，進而自動改善其自身的運作。

除此之外，也可以在「cracked.to」論壇上看到一則貼文列出了一大串開放原始碼駭客工具。這些工具當中包含了一個採用 AI 技術的軟體，可分析經由資料外洩取得的大量密碼資料。此軟體會利用 GAN 來學習人類修改密碼的方式，例如：將「hello123」改成「h@llo123」，接著再改成「h@llo!23」。

合成變臉A片撈千萬遭判刑

- 小玉和助理莊炘睿從2020年7月20日起，開始盜取多位名人的照片，再利用自行購買的「DEEPFACELAB」程式軟體，透過軟體中的人工智慧模擬演算法（Artificial Intelligence），將台灣多位女星的臉部，合成於日系AV色情影片中，並上網四處兜售，背後不法獲利非常可觀
- 據悉經整理名單後，共計有119人受害；包括藝人柯佳嬿、黑嘉嘉和蔡依林；網紅雞排妹、奎丁和愛莉莎莎；以及民進黨立委高嘉瑜、高雄市議員黃捷和前北市府副發言人黃瀞瑩，都在受害者名單中
- 判處小玉5年6個月有期徒刑，得易科罰金，並沒收不法所得1338萬餘元。但經檢方調查後，僅查扣到小玉名下的912萬餘元財產，日後將追徵剩餘的犯罪所得；小玉名下的一輛2016年份GLC300賓士車，也已委託法務部執行署拍賣，以195萬2000元落槌賣出

資料來源：2022/7/11 引新聞

AI人工智慧的場景風險

- AI運用風險尚未完全可控

關鍵風險*：
是否符合公司治理的道德觀和價值觀？

關鍵風險*：
缺乏可解釋性，無法向客戶或監管機構合理解釋

關鍵風險*：
AI可能做出錯誤且難以挽回的決定，例如批准/拒絕錯誤的貸款申請風險

關鍵風險*：
無法合理控制AI，例如我們可以合理推測AI的決定

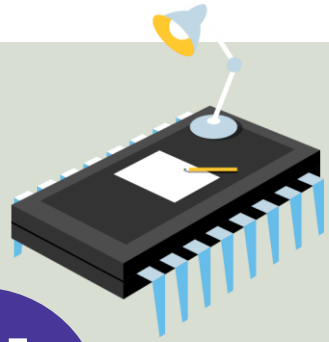
* KPMG client survey across 170 technology risk professionals

AI人工智慧的場景風險

- 機器學習建模及使用過程常見的錯誤

機器和人類一樣聰明嗎？
機器學習的能力可以解決什麼樣的問題？

若非深入研究的專業人士，其實是很難掌握的，
就算是深入研究的專業人士也經常不慎地犯錯，帶來錯誤的結果並產生嚴重的負面影響。



不佳設計

- feature 有signal-poor 、 irrelevant feature或introduce bias
- 模型架構或參數選擇不當、過度配適。

訓練不足

- 訓練與測試資料分配不平衡（例：Amazon用歷史資料訓練及分類應徵者資料，造成性別歧視、以英語做自然語言處理顯示性別刻板印象）
- 訓練資料本身的偏誤。

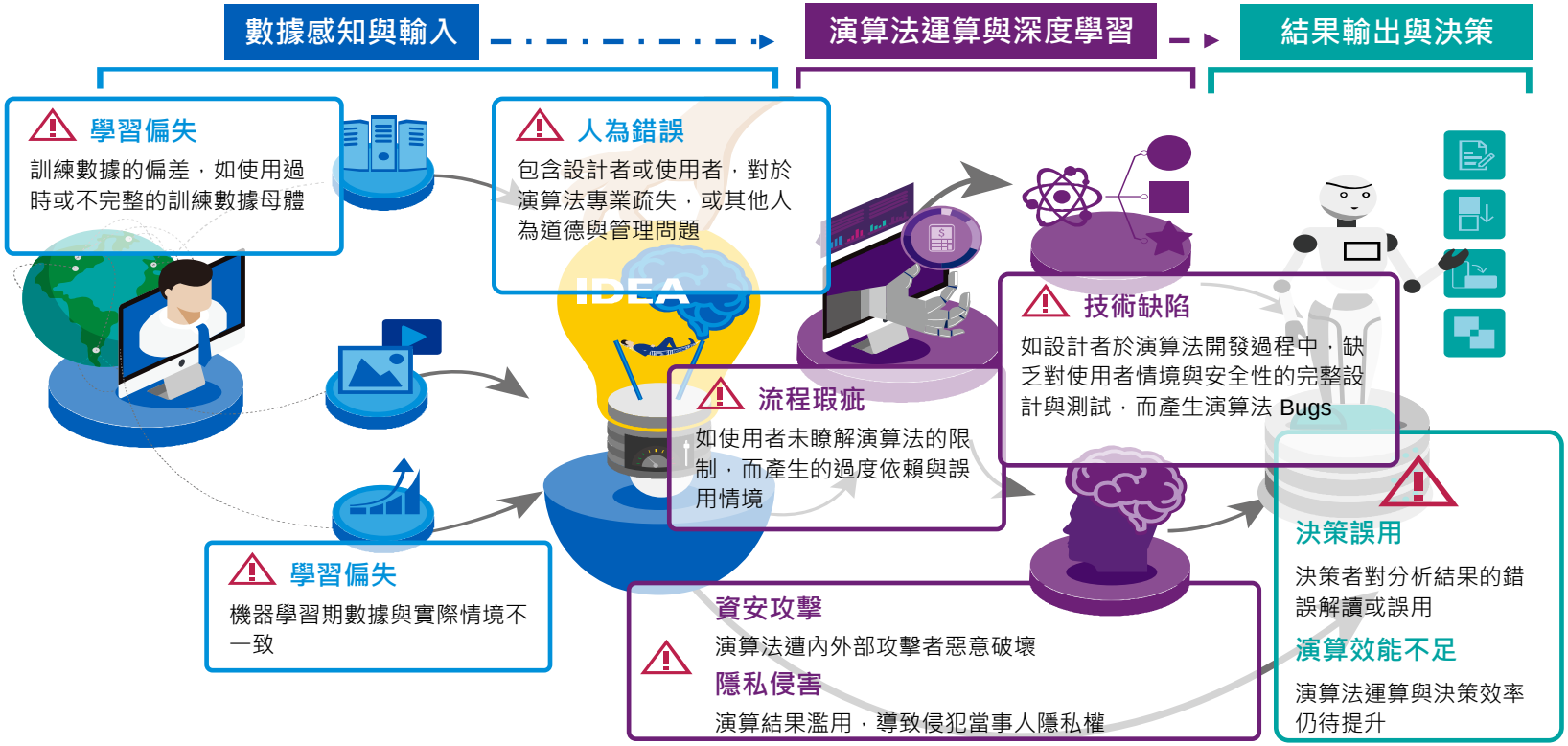
錯誤應用

- 人工智慧受限於訓練資料且有前提假設，無法解決特定問題（例：作文自動批改系統）

AI人工智慧的場景風險

- 誤用AI可能面對預期外的風險

人工智慧演算法所引發的各種風險成因，可分學習偏失、人為錯誤、技術缺陷、流程瑕疵、資安攻擊、隱私侵害、決策誤用、演算效能不足等八類



AI真的精確嗎?分不清足球還是光頭？

- 蘇格蘭因弗內斯足球足球俱樂部首次在直播賽事引入 AI 攝影機。採用 AI 技術原本是為了給球迷更好的觀賽體驗，因由於新冠肺炎疫情大流行，廣大球迷不能到現場看比賽。
- 11 月蘇格蘭足球冠軍聯賽的賽場，AI 攝影機卻將邊線裁判的光頭辨識成足球，瘋狂追了一整場。無論哪支球隊進攻，哪個球員帶球，AI 都視而不見，反而緊盯裁判光頭不放，還時不時給個特寫，全場 90 分鐘的足球盛宴，在家看直播的球迷大部分時間都在圍觀一顆頭。
- 體育賽事期間，有 79% 觀眾會透過社群媒體互動。最普遍的是在 Twitter 發文，對 AI 來講是龐大且有效的檢測資料庫，且球迷推文是情緒檢測的重要指標。4,583 條推文中，有 31.1% 標記為與影像助理裁判（VAR）相關。情感方面，有 25.5% 表示為積極情緒，而 41.1% 表示為負面情緒，其餘為中立情緒。

資料來源：TechNews

AI人工智慧的實用現況

- CEO眼中快速發展的AI伴隨的可能風險

競爭優勢

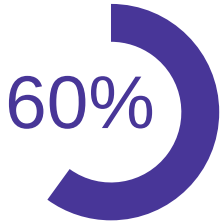
of companies believe **AI is key** to competitive advantage.

- IDC

僅有高階信任

only have a high level of **trust** in their own organization's analytics.

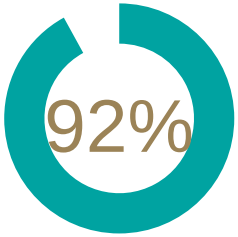
- KPMG's recent Guardians of Trust report



法規限制

see **regulatory constraints** as a barrier to implementing AI.

- IBM IBV AI 2018



可能衝擊信譽

question **trustworthiness** of data, analytics …are worried about the impact on **reputation**.

- KPMG's recent Guardians of Trust report

1 in 20 companies has **extensively incorporated AI** In offerings or processes.

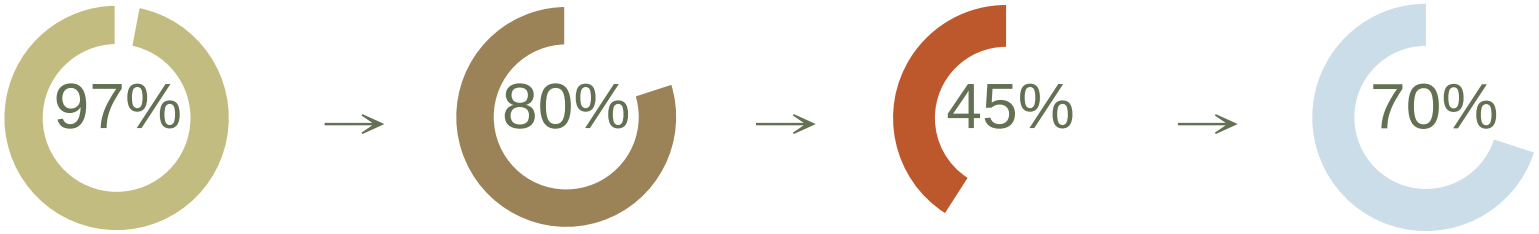
- MIT Sloan Management Review

> "Business leaders need to arm the workforce for a new 'machine age' of artificial intelligence and increasing automation."
> **Duncan Tait** SEVP , Head of Americas and EMEIA Fujitsu

- KPMG's 2018 Global CEO Outlook

AI人工智慧的場景風險

- AI in Control 的重要性



Believe AI is either already being used or is planned for

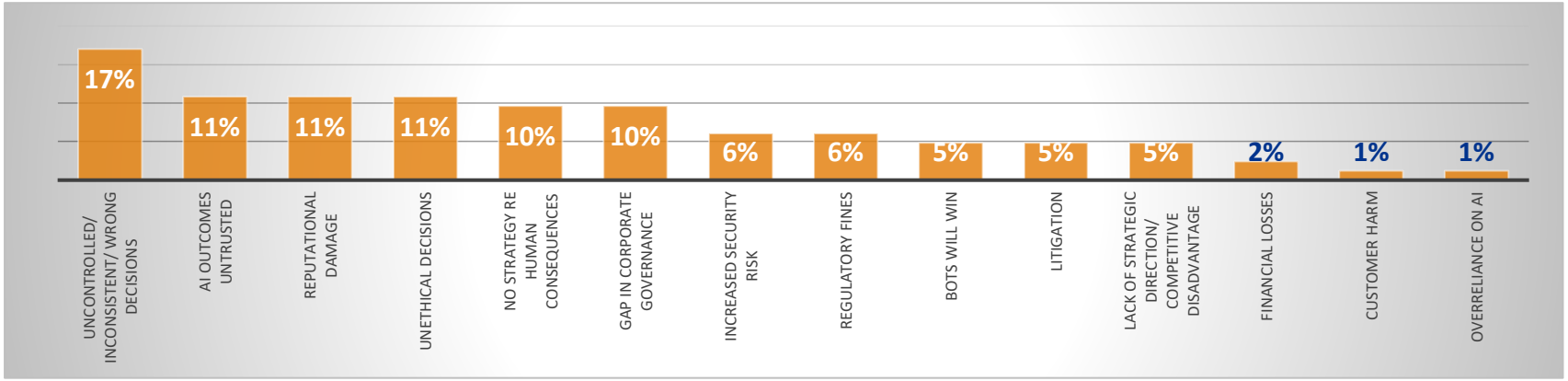
Lacked confidence in AI governance in place

Planned to perform an audit on their AI solutions

Weren't clear what their approach to auditing AI

- KPMG client survey across 170 technology risk professionals

What would be the impact of 'uncontrolled' AI?



不受控不一致錯誤 | 不信任AI結果 | 信譽遭損害 | 違反道德的決定 | 無重新人為判斷策略 | 與企業治理的差距 | 增加的安全風險 | 法規處罰 | 機器人將獲勝 | 訴訟 | 無策略指導/競爭劣勢 | 財物損失 | 客戶傷害 | 過度依賴AI

專家警告AI可能帶來的負面影響

數位安全

- 專家們擔心的是自動化的網路攻擊行動將擴大現有攻擊的規模與效率，亦預期會出現 專門開採人為疏失、軟體漏洞與AI系統漏洞的新型態攻擊行動。

實體安全

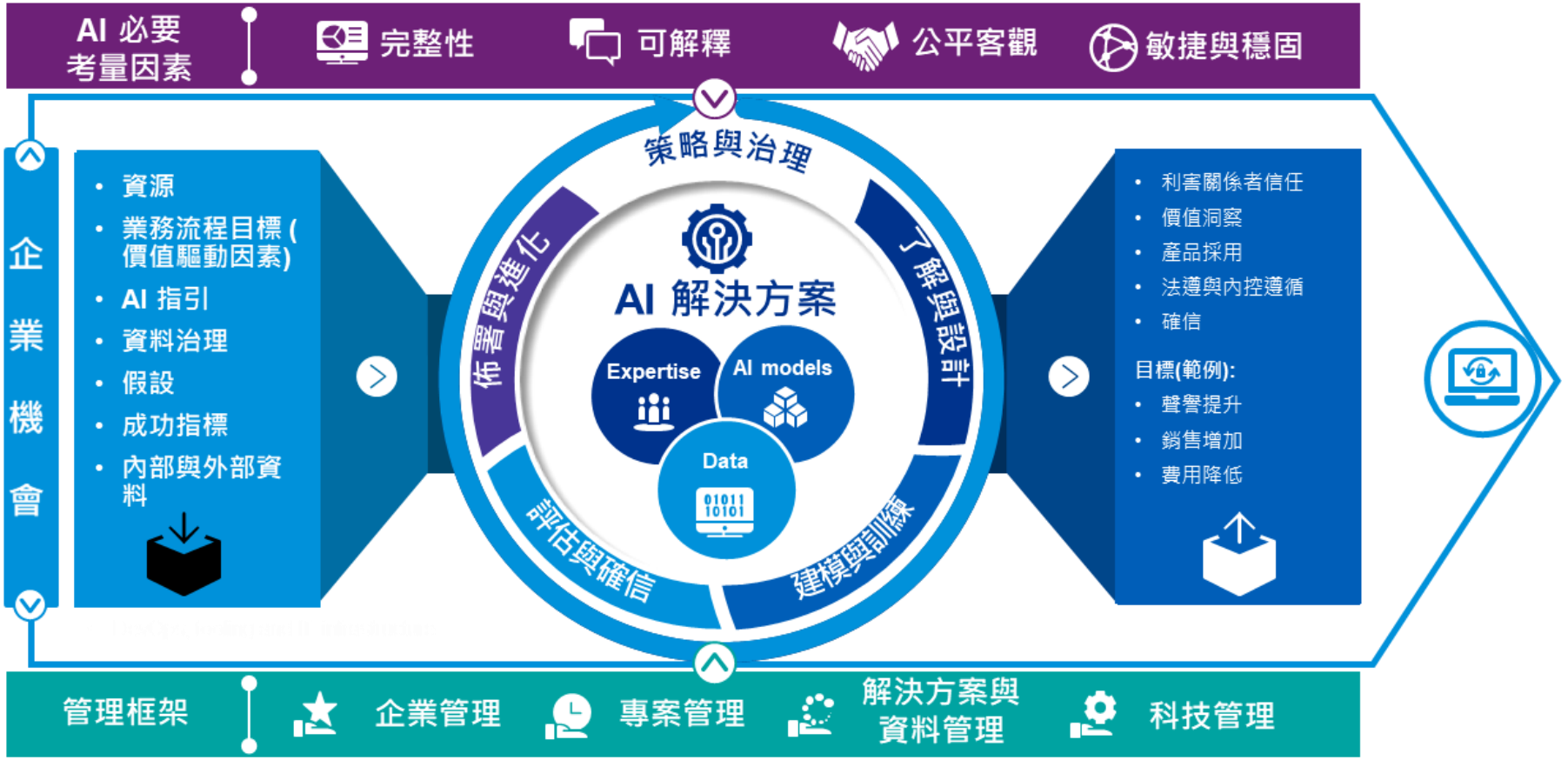
- 專家預期AI將能擴大藉由無人機或其它系統所展開的實體攻擊，或是顛覆傳統攻擊的 新模式，如造成自駕車撞毀，或是遠端操控數千架無人機以展開攻擊等。

政治安全

- 此外，AI還能被用來破壞政治安全，以AI分析大量資料以進行監控，建立有特定目的的宣傳活動或欺騙行為，或者發展出新型態的攻擊，像是進一步分析人類的行為、情緒及信仰以發動攻擊，此一破壞能力除了在極權國家特別明顯之外，也可能破壞民主 國家的公共辯論。

AI人工智慧的場景風險

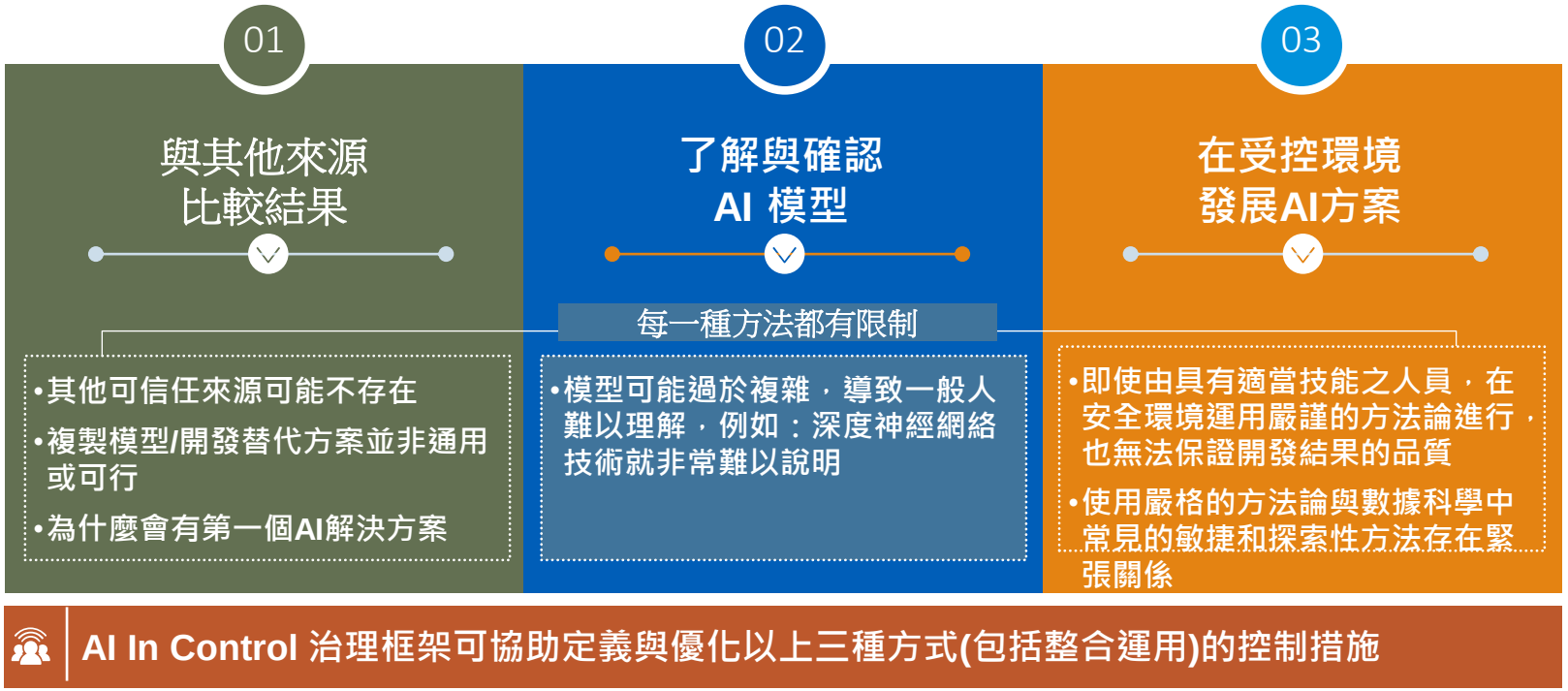
- AI in Control 參考框架



AI人工智慧的場景風險

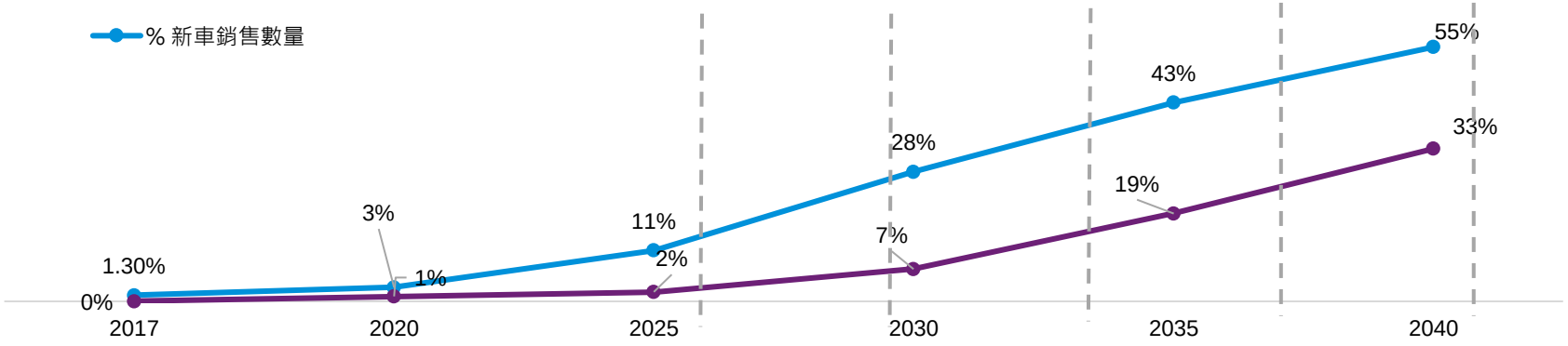
- AI 建立信任的三種方式

- 為了成功運用與推動人工智慧，企業和社會需要能夠信任它可以做出正確的決定 (和/或) 不做出錯誤的決定，所以必須找出適當的方式！



未來電動車的數量將直線上升

自駕電動車的趨勢預測
(2017–40)



從 2024 年開始，電動汽車的前期成本，將在無政府或產業補貼的基礎上變得具有競爭力

預計到 2025 年，中國將佔全球電動汽車市場的近 50%

在歐盟，目標是到 2025 年電動汽車銷量達到 15%，到 2030 年達到 30% 印度的目標是到 2030 年實現 30% 的電動汽車銷量

英國和法國將在 2040 年前停止銷售汽油/柴油汽車

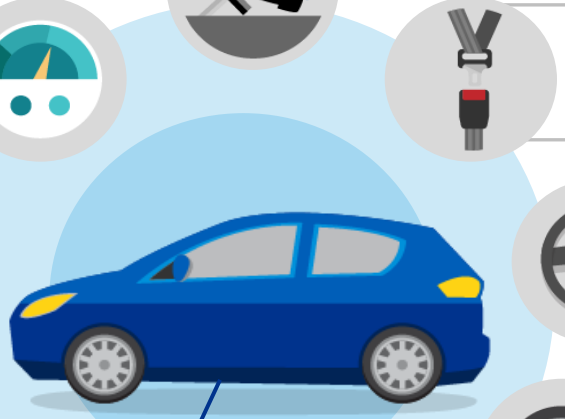
■ 汽車資訊安全

- UN ECE Regulation 155資安規範將成為歐洲車輛及車廠必須遵循的法規
- ISO/SAE 21434 將取代J3061成為汽車資通安全的主流標準
- ISO PAS 5112 將作為資安管控與稽核的指南

■ 車用軟體更新

- UN ECE Regulation 156 軟體更新規範將成為歐洲車輛必須遵循的法規
- **ISO/AWI 24089將成為車軟體更新與管理的主流標準**

新興科技資安及隱私議題 – 自駕車



- 油門/煞車踩踏習慣
- 緊急加/減速行為

- 平均速率
- 里程數
- 儀錶板資訊

- 是否繫安全帶
- 心跳、呼吸偵測

- 車牌號碼
- 車輛辨識碼

- 轉彎
- 喇叭使用紀錄
- 手持方向盤紀錄

- 用電管理情況
- 電池效能

- 車重
- 駕駛/乘客體重
- 胎壓

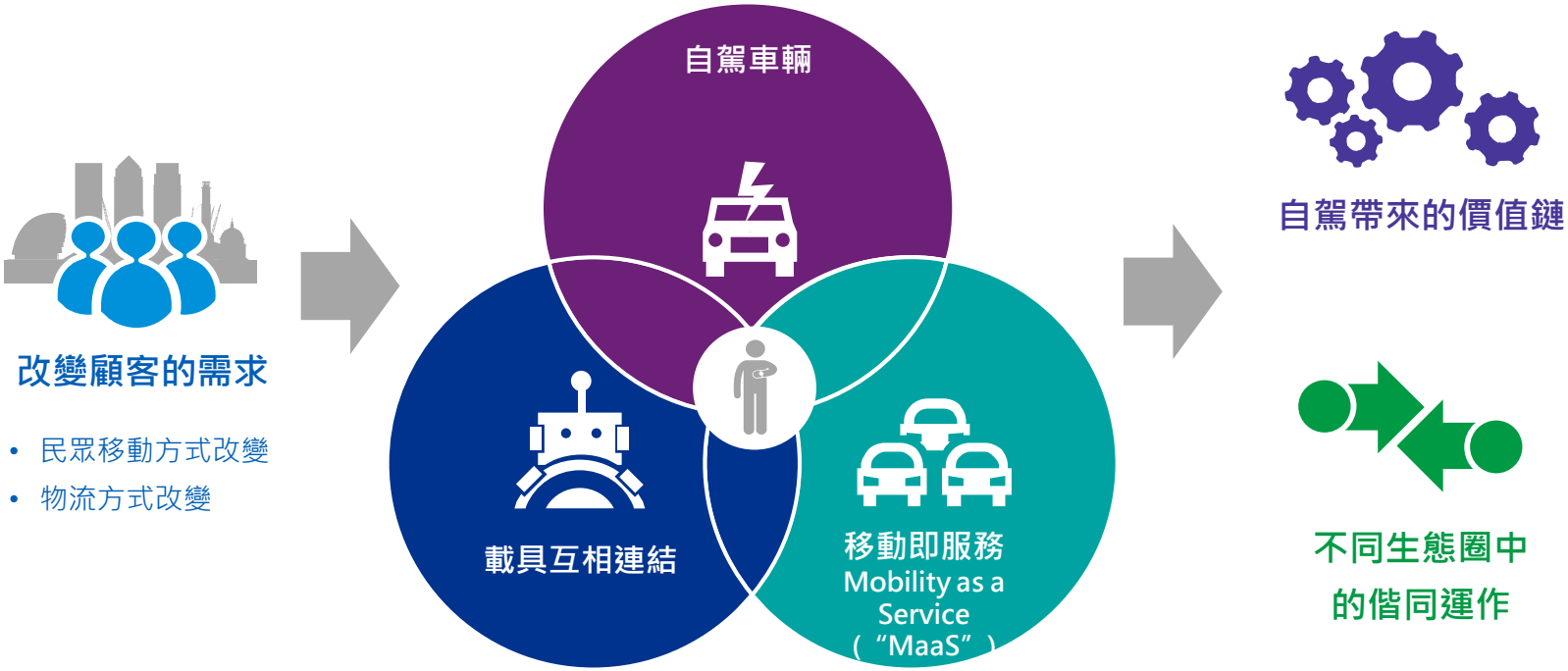
- 軟體版本
- 網路連線狀況
- 安全氣囊部署(體重、體型)
- 開車時段(夜間行駛)
- 系統溫度
- 臉部識別與指紋
- 視線偵測(手機使用情形/專注與疲勞度)
- 駕駛人注意提醒裝置

車載娛樂系統

- 姓名
- 電話與通訊錄
- 導航歷史
- 遠端操控紀錄
- 信用卡資訊
- 搜尋紀錄
- 娛樂、APP偏好
- 聲紋辨識
- 各媒體的信物

！現況：Ford在2021年初與Google簽約，在2023年開始將建置Google系統於車內，也提到創新「個人化」服務

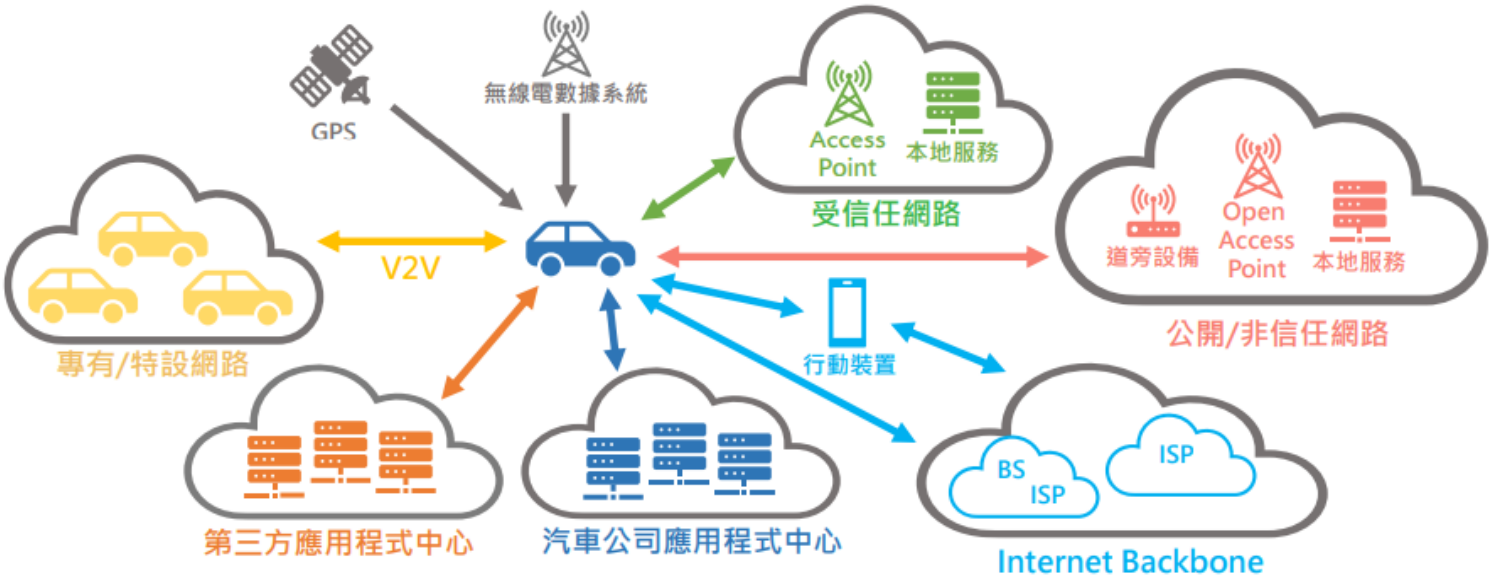
自駕車的需求



- 5G低延遲的傳輸特性，帶動車聯網技術更成熟，然而在享受汽車變得聰明便利的同時，也必須承擔遭受風險，包括個人識別資訊（PII）、車輛的網路與運算資源，甚至是車內儲存的電力等資訊，都應該受到妥善的保護。

自駕車的網路基礎建設將更複雜

- 車輛與外部系統互聯化驅動許多新興服務的發展，但在資安面向卻是資安風險與威脅攻擊面的擴增



https://www.honhai.com/s3/institute/downloads/%E8%87%AA%E9%A7%95%E8%BB%8A%E9%81%8B%E8%A1%8C%E5%AE%89%E5%85%A8%E8%88%87%E9%98%B2%E8%AD%B7-%E4%B8%AD%E8%8F%AF%E8%B3%87%E5%AE%89%E5%9C%8B%E9%9A%9B%E6%B4%AA%E9%80%B2%E7%A6%8F%E7%B8%BD%E7%B6%93%E7%90%86.pdf

網路複雜情況來自於與周遭的通訊

■V2N – 車輛對網路

- 有助於傳播訊息，V2N 也可讓連線更加穩定。

■V2D – 車輛對裝置

- V2D 可利用行人身上的個人裝置或手機將其定位傳送給車輛，讓車輛避開行人。

■V2V – 車輛對車輛

- V2V 可防止車輛之間的碰撞，車輛在行經十字路口時就更安全。

行駛中收集的資料是否為隱私資料?

買車/維修中...

- 註冊與購買表格資訊
- 駕照資訊 (含照片)
- 銀行匯款紀錄
- 未清償債務
- 信用額度與評分
- 車齡、使用狀況
- (預約) 維修紀錄
- 客訴紀錄
- 車險資訊

充電中...

- 常拜訪之充電站
- 每次充電量
- 其他影響電量消耗之參數

回家/上班中...

- 自家住址
- 工作地點

開車中...

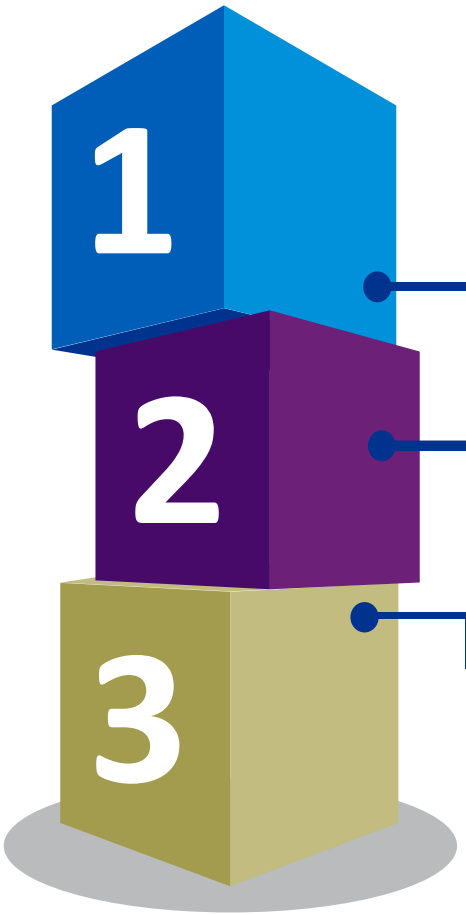
- 實況影片紀錄
- 安全事件短片
- 路人、騎士外貌
- 路線、紅綠燈與路標位置
- 行駛道路類型與海拔高度
- 天氣

從事日常活動中...

- 一般商家拜訪紀錄
- 敏感場所 (ex.醫院、法院、寺廟) 拜訪紀錄
- 旅遊熱區

自駕車蒐集資料的種類

爭議？ 過去：CCTV以「**監視**」為目的蒐集資料
現在：**自駕車**以「**自駕**」為目的蒐集資料



外部資訊

目的：改善**塞車/交通**狀況
Ex.路標、紅綠燈位置、
路況、天氣

自駕車資訊

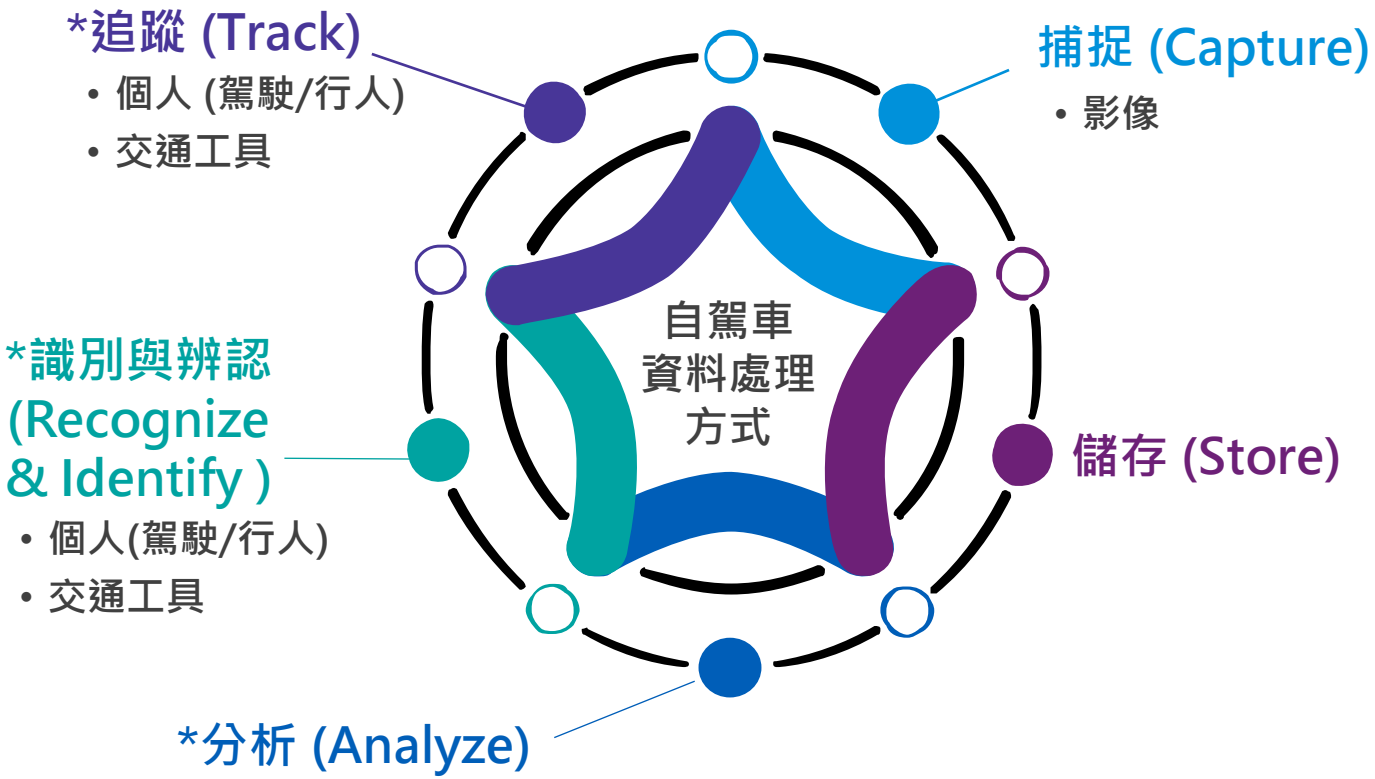
目的：了解自駕車的**使用狀況**
Ex. 里程數、耗油/電量、
位置、車牌、充電記錄與
管理情況

關係人資訊

目的：提升**安全**、**降低成本**
Ex.駕駛開車行為、生物特徵、
路人及騎士、手機連載資訊
(聯絡人、聊天與搜尋紀錄、
行事曆、付款資訊)

！關係人之資訊又分為「敏感」與「不敏感」

自駕車資料處理的方式



*：表示為次要(Secondary)用途

- 消費者接受度**最大**：「捕捉」
- 消費者接受度**最小**：「追蹤」與「辨認」

自駕車蒐集資料的四大用途

提升使用者體驗

① 客製化喜好清單
② (生物特徵)自動調整座位、鏡子角度及位置
③ 優化(環保!)路線、導航
④ 提供即時路況資訊
⑤ 「車內」購物
⑥ 自動填寫線上表單

提升安全

① 緊急呼救及搶救
② 警告及自動停駛
③ 駕駛有動機改善開車行為
④ (聲紋資料)確認說出開車指令者是駕駛本人
⑤ 識別出危險駕駛所開的車
⑥ 遠端診斷自駕車

創造新收益模式

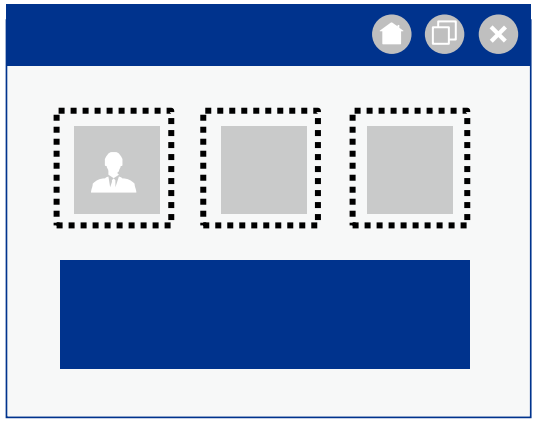
① 商業廣告
② 販售給第三方
③ 車上娛樂
④ 「移動即服務」：共享經濟、租車

降低成本及費用

① 車禍究責(提供證據)
② 駕駛節省保費
③ 降低塞車現象

自駕車公司如Lyft、Waymo等，都提倡「**Open Data**」，讓蒐集的資料透明、可取得

資安風險：科技與技術



- 駭客能**遙控**有**連結雲端**的自駕車，不須實體到場即可駭得資訊並販賣與不肖運用

自駕車專用的**軟體**，在設計時往往有**Bug**，造成安全疑慮

資安風險：案例分享

1

1. 特斯拉開進墓園時，展現「電子陰陽眼」，在空無一人的情況下偵測到「人(鬼？)」→ 若在前方無車的情況下「偵測到其他汽車」，則會自動降速、煞車。

2

因Tesla Model X key fobs軟體更新時有瑕疵，讓駭客能便宜購入舊型electronic control unit (ECU)，利用弱點進行攻擊。駭客用藍芽連線後，即可在90秒間駭入Model X，重新寫該軟體的程式並取得解鎖車子的密碼。

3

1.McAfee 安全研究員在限速為35英里的路標上黏上膠帶，成「85」英里，特斯拉的Autopilot因此被騙，加速直至駕駛自己選擇煞車

2.在特斯拉的雨刷前放上下雨的情境，讓特斯拉自動開啟雨刷功能

4

兩名駭客利用「電子繼電器系統、鑰匙干擾技術」。其中一名駭客把電線放在頭上做為(假)電子鑰匙的訊號，欺騙特斯拉的車載電腦系統以進行攻擊(key fob relay attack)，於30秒成功駭得汽車。

5

騰訊安全研究員利用多個弱點，在遠端駭入特斯拉，進而控制車鎖、煞及天窗等。

演算法風險：道德與商業

- 因為自駕車的程式是「人」寫的，因此在面對道路狀況時，選擇如何自駕車的操作方式，往往會牽涉到**道德**與**商業**的問題。

車主 vs 路人

上班族 vs 軍警醫人員

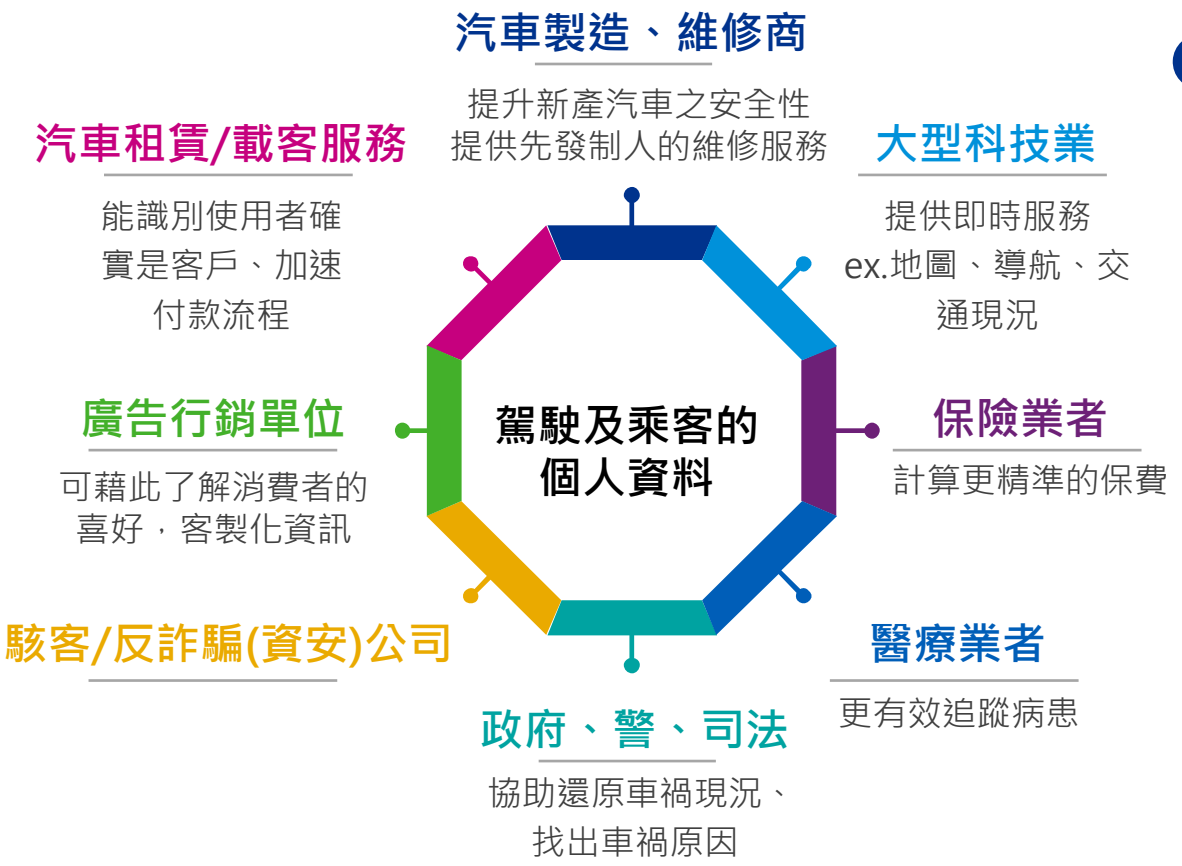
小孩

身心殘障

動物

隱私風險：未經個資主體同意即販售資訊

- 自駕車所蒐集的資訊，往往在**未經個資主體**(Data Subject)**同意**下，即販售給第三方，造成(潛在)個資外洩。對駕駛/乘客個資有興趣的第三方包含：



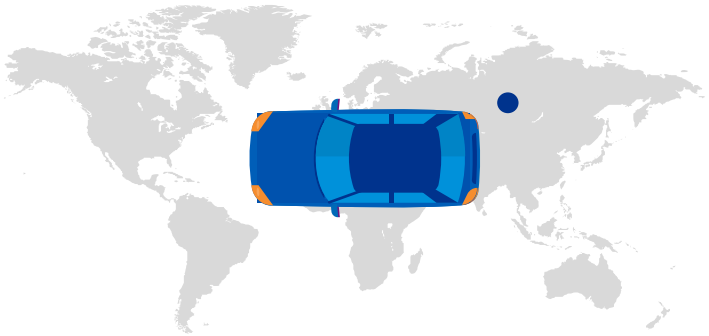
但...誰能擁有資訊?

- 購買自駕車者
- 製造自駕車者
- 個資主體
- 個資蒐集者
- 個資處理者

爭議

隱私風險：追蹤與定位

- 自駕車利用GPS、物聯網技術，不但能**追蹤個人的地理位置**，更有可能因此**間接蒐集「敏感的」**個人資訊，包含收入級距、病歷、政治傾向、性傾向、犯罪記錄等。



追蹤個人的地理位置

間接蒐集敏感個人資訊

- 教堂/清真寺/寺廟
- 政治人物/政黨辦公處
- Gay酒吧
- 法庭
- 醫院/診所(心理診所、墮胎、整形、愛滋…等)

隱私風險：「選擇」退出 (Opt-out)

01 只要沒有選擇退出，則會**一直**(Always-on)、**隨車移動地**蒐集資料，不能彈性選擇

02 若選擇退出，則可能會**影響**自駕車的**運作**、**軟體的更新**

03 若選擇退出，**是否有負面隱射**之意？例如：自己去的地點為較私密、駕駛行為不佳

04 駕駛可選擇是否讓科技技術蒐集個資，但**乘客、路人**等**無法**→ **共享汽車、汽車租賃的使用者**能選擇「Opt-out」？
(似Google Street View的爭議)

資安及隱私議題 – 法規遵循

與時俱進性

法規制定往往費時，在自駕車發展快速之際，**法規能否跟上科技技術**之發展？

一致性

用自駕車蒐集個人資料時，也**需要跟其他方法蒐集到的個資一樣**，依法定保存年限保留嗎？

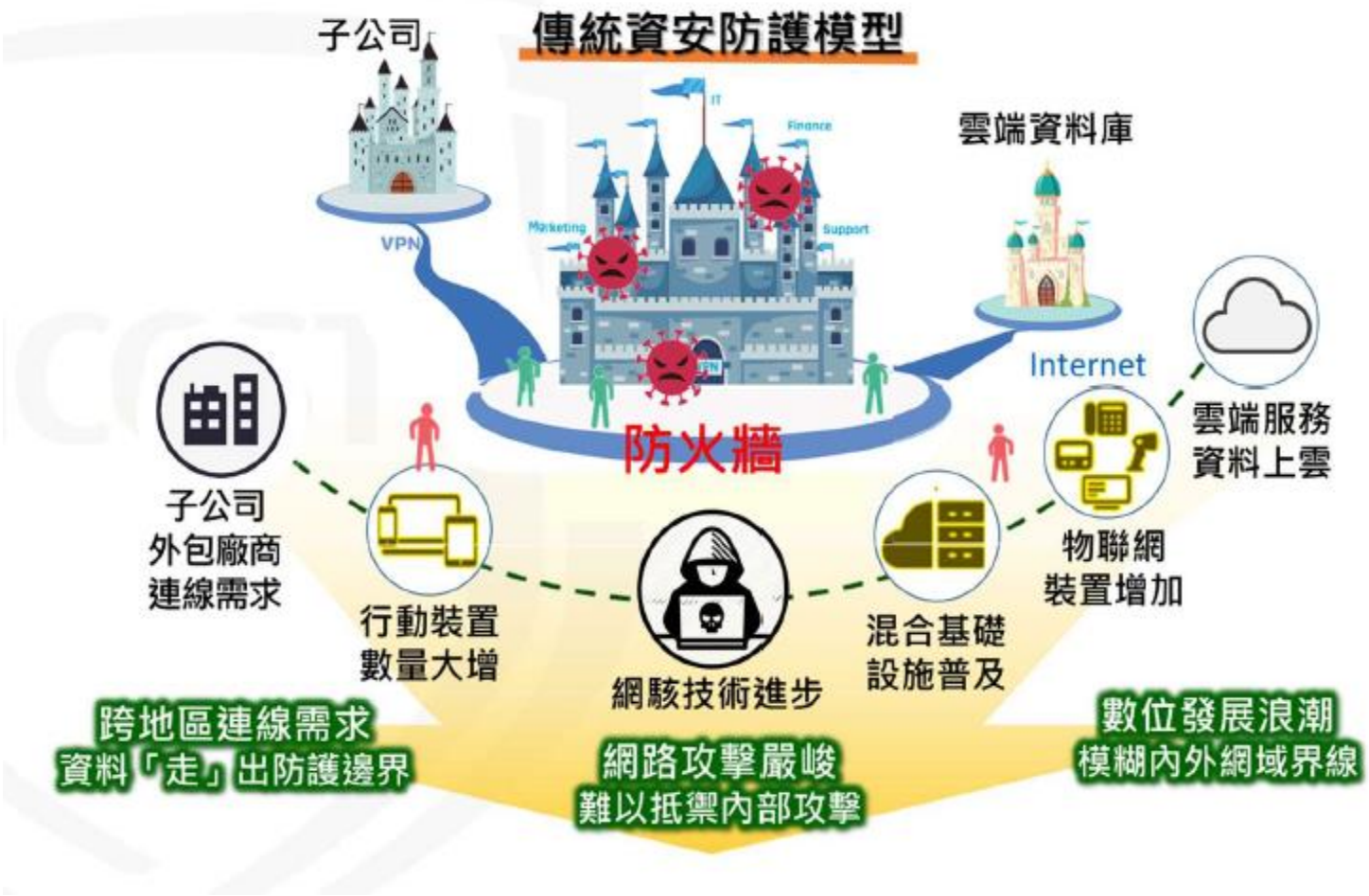
零信任
— 資安管理新觀念

迅速改變的大環境

永不信任、 始終驗證

1 驅動因素	數位 轉型	自攜 裝置	遠端 工作	新冠疫情 (COVID-19)	遠端 存取
2 考量重點	扁平/變動式 網路	全有或全無 存取	橫向 移動	內部 威脅	嚴格的 存取
3 主要影響者	身分、網路 和端點	學研單位	資安領導者	大規模雲環境	政府機關

傳統資安防護的侷限性



資料來源：國安局、技服中心

發展趨勢和驅動因素

數位企業[1]

80%

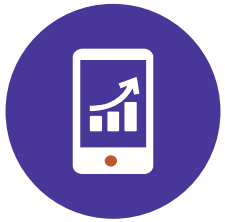
將在2022年運用「零信任」的網絡存取模式，給予生態系夥伴數位企業應用，

智慧自動化

67%

的組織正尋求智慧自動化來降低額外的人力

終端



70%

成功的侵害都源自於終端

VPN[1]

60%

的企業將在2023年漸漸淡出VPN的使用，導向「零信任」

遠距工作 [2]

40%

的員工在未來將使用「遠距工作」的商業模式

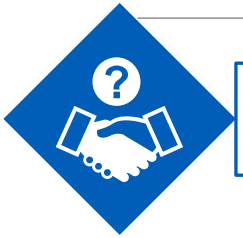
雲端

63%

的資安長 (CISOs) 都認為設置、實施資料在多雲環境的存取政策是很有挑戰性的

資料來源[1]: *Market Guide for Zero Trust Network Access, Published: 08 June 2020, ID: G00726817*
資料來源[2]: *BCG*.com, June 2020, **Remote Work Works—Where Do We Go from Here?**

到底甚麼是零信任？



最新術語：永不信任、 始終驗證！

定義	方法	結果
「零信任」是一個以資料為核心、更著重身分驗證的模型；被設計來應對當今「無邊界」網路世界下的挑戰	「零信任」 策略在網路間的實施並不是一次性或完全一致的。因為不同的環境與保護標的都是不同的	緊密結合以下兩者： 1.簡化的整體安全架構，與 2.應用程式和基礎架構
「零信任」模型是建構於永遠不信任組織資安邊界內、外的任何事物	權衡身分識別與存取管理(IAM)、端點策略與網路分段所做的努力，來為 「零信任轉型」建構實作案例	改善使用者體驗，使體驗更值得信任
必須驗證試圖連接到組織系統的所有連線，通過後才授予存取權限	首先解決雲環境和應用程式，再於現做環境部署符合潮流的應用	透過自動化和精簡的規則庫來簡化營運流程，同時精簡了法規遵循與審計要求

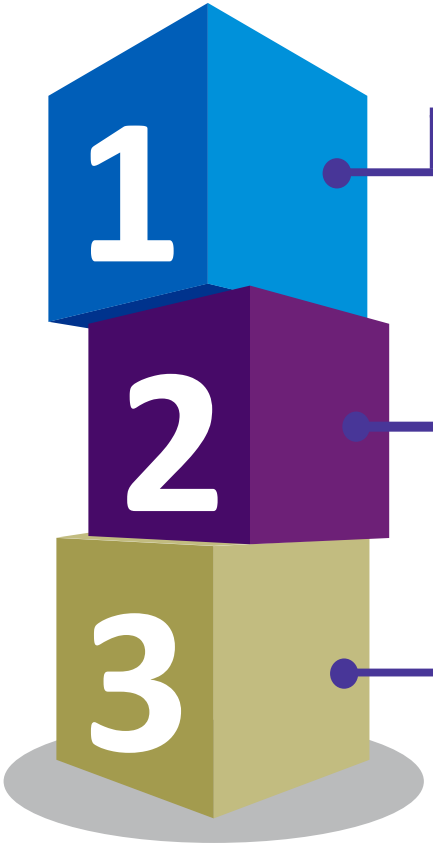
實施「零信任」安全模型的原因與優點

四大原因

1. **連結性：**當今企業跨應用的服務、網路、使用者和設備間的連結日益複雜，網路邊界大幅擴展
2. **多元使用者：**當今企業內的使用者除了員工，還有承包商、第三方供應商
3. **豐富的設備：**當今企業使用的設備在物聯網及技術進步下更多元
4. **全球分散：**當今跨國佈局的策略，與遠端使用者、可攜式設備(BYOD)、雲服務等，皆不再侷限於單一國家

以上原因都使當今的資安威脅更**複雜、精密**(Sophisticated)

三大優點



1. 給予資安防護人員更多**偵測最新威脅**的機會
2. 擁有**更多可快速部署的策略**，來因應資安事件
3. 讓資安防護人員可以**更敏銳**地辨認細微的資安威脅

最終目標: **降低資料外洩**、**橫向移動**攻擊的機率

「零信任」安全模型的核心概念

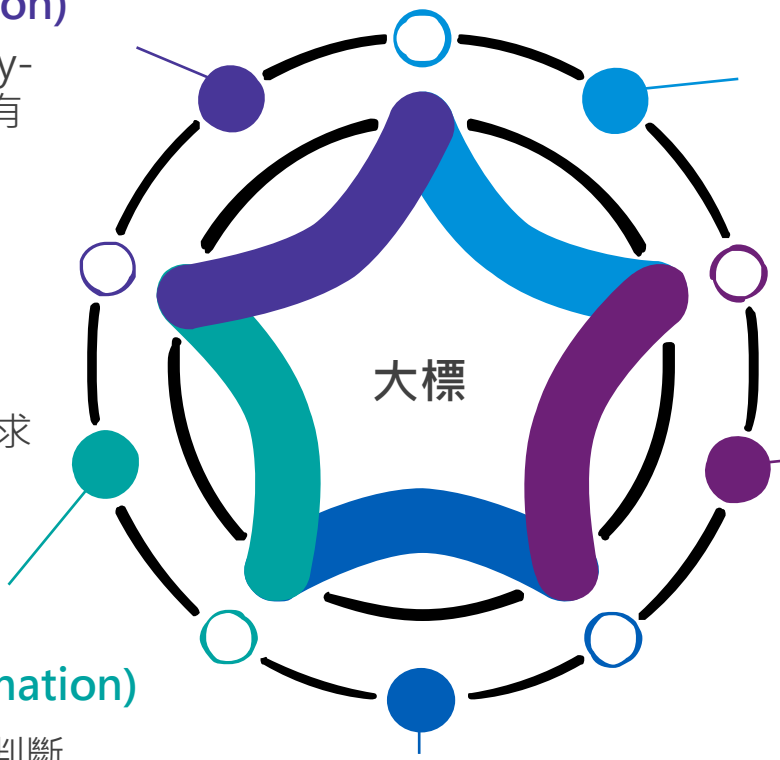
■**零信任，即以「假設資安事件已發生(Assumed Breach)」的思維來設計之安全模型**

持續驗證 (Continuous Verification)

- 「預設為拒絕 (Deny-by-Default)」的政策：沒有資源是天生被信任的
- 假定所有對重要資源、網路的需求都是**惡意**的
- 假定所有的裝置與設備都已**遭駭**
- 假定在同意所有存取需求時，都**伴隨著風險**

多方資源 (Multiple Resources)

- 零信任模型以**資料**為核心(Data-Centric)
- 動態、靜態資料皆蒐集
- 對使用者、裝置進行**多因子驗證**(Multi-factor Authentication)



即時資訊 (Real-time Information)

- 以供「持續」判斷是否給予存取權限

細緻 (Granular)

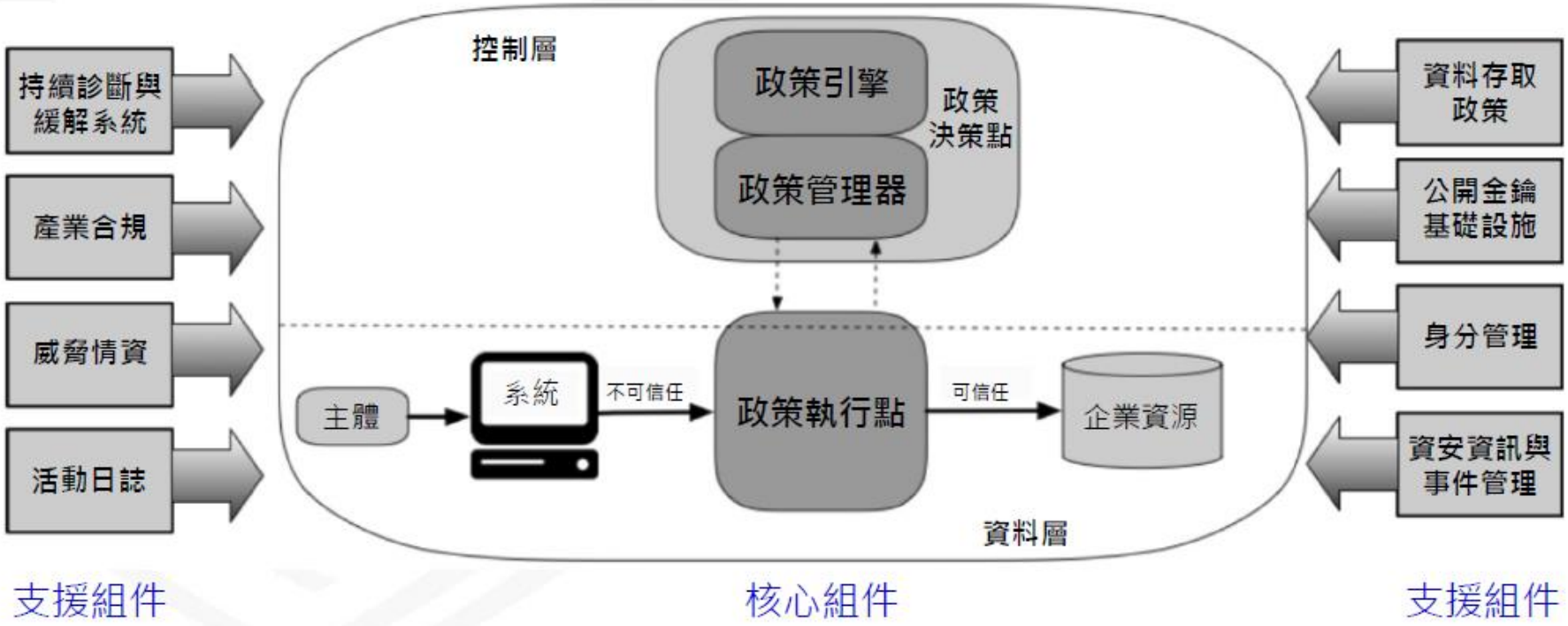
- 存取控制的設計與實施

最小權限原則 (Least-privileged Access)

- 只授予完成任務必須要有的最低權限
- 持續(而非一次性)判斷是否給予存取權限
- 網路**分段**(Segmented)以降低橫向移動(Lateral Movement)攻擊的機率

NIST標準之零信任架構

- NIST SP 800-207將零信任架構分成核心組件與支援組件
  - 核心組件：執行鑑別、決定授權及管理連線
  - 支援組件：支援存取決策的資訊與系統

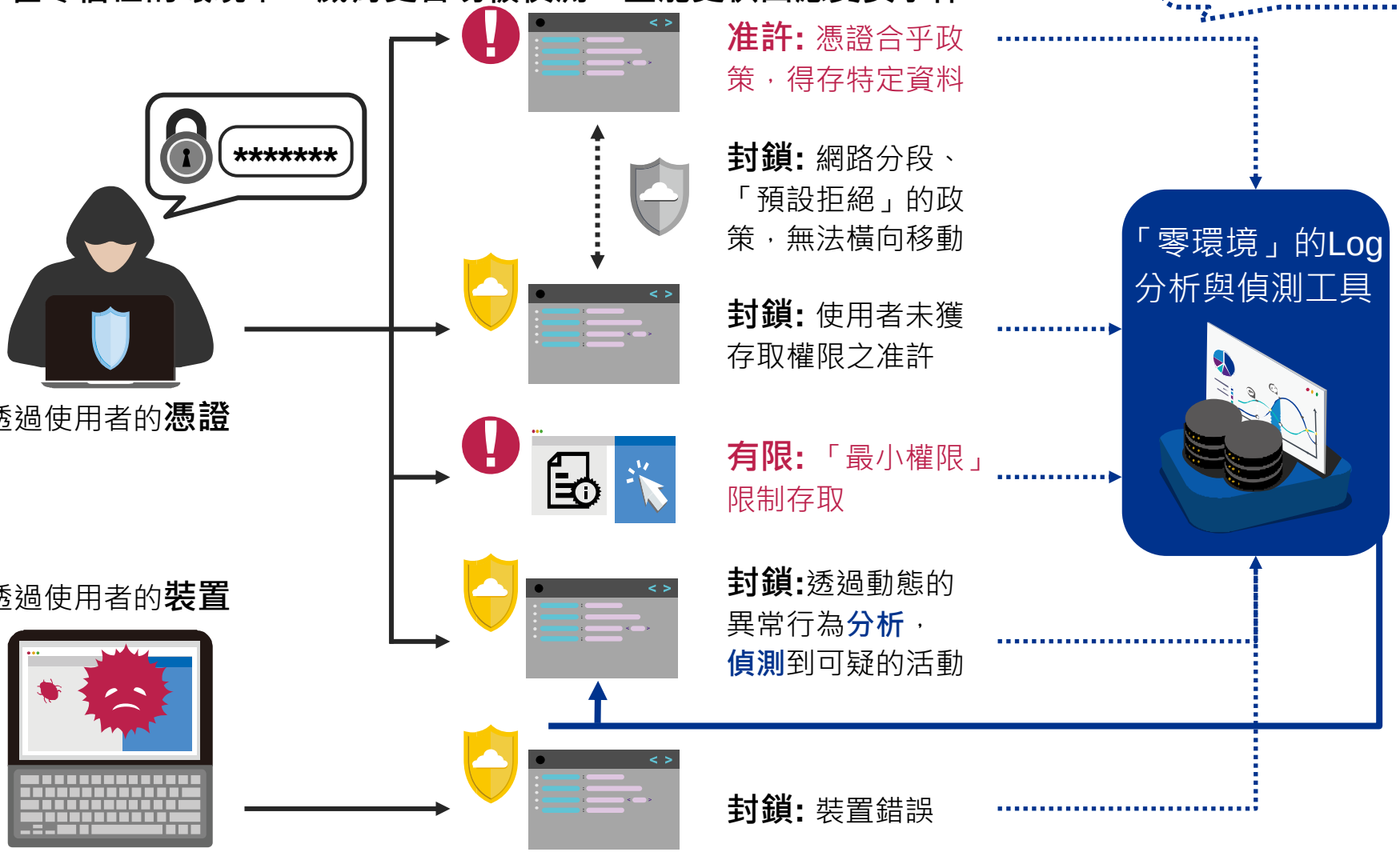


資料來源：技服中心

「零信任」環境的應用

■在零信任的環境下，威脅更容易被偵測，且能更快因應資安事件

將每個活動的log記錄餵進工具裡



走向成熟的「零信任」環境

- 「零信任」要完全成熟需要許多時間、能力/知識，因此可以採「漸進」的方式部署

部署「零信任」的漸進式旅程

有零信任

無零信任

- 準備：初步的發現與評估活動
- 基礎：初步實施根本的資源
- 中階：整合根本的資源並持續精煉
- 進階：部署進階的保護、控制、分析

實施的四大困難

1. **未有完全的支持**
   包含領導階層、管理人員與一般使用者的支持
2. **資源規模化的困難**
   要「持續」判斷是否給予存取權，需要完善的資源
3. **無法持續堅持零信任**
   人員可能對持續實施零信任感到疲憊
4. **對組織的了解不足**
   不夠了解有/無形資產、使用者、商業流程，讓評估存取需求的效力有限

問題與討論