新興科技的資安挑戰與應對

資安長　李國良

安碁資訊

Acer Cyber Security Inc.

新興技術浪潮的威脅 – 電子交易

使用者身分識別

- AI 驅動的自動化攻擊
  - ✓ 深偽詐騙
  - ✓ 自動化釣魚與攻擊
- 帳號或憑證竊取
  - ✓ 量子計算破解

惡意攻擊

- 勒索軟體、木馬程式
- DDoS阻斷式攻擊

交易平台管理

- 供應鏈與雲端風險
  - ✓ 第三方服務滲透
  - ✓ API管理不當或漏洞
- 程式快速迭代
  - ✓ 資安技術債的累積
  - ✓ 壓力下的錯誤與疏忽
- 過時系統與未修補漏洞
- 權限管理不當
- 設定配置錯誤

新興技術浪潮的威脅 – 虛擬化與雲端運算

虛擬化 & 容器

- 資源管理不當
- 共用環境的風險
- 不安全的映像檔
- 跨虛擬機攻擊
- 跨容器攻擊
- 橫向防護不足

雲端運算

- 設定配置錯誤
- 權限設定不當或共享
- 分散式的資源管理
- 誤解共同責任模型
- 資料外洩
- 資源盜用與濫用
- 缺乏可視性的管控
- 混合雲的管理風險

新興技術浪潮的威脅 – 人工智慧

被動回答問題，專注於內容創作，需要人類密集提示

生成式AI

- 資料隱私與敏感資訊外洩
- 提示詞注入攻擊
- AI幻覺與錯誤資訊
- 惡意內容生成與詐騙
- 侵權或違反學術倫理
- 模型本身的安全漏洞

主動執行任務，專注於決策與行動，目標導向

代理型AI

- 權限與操作風險
  - ✓ 過度授權
  - ✓ 工具誤用
- 供應鏈與工具鏈漏洞
- 記憶毒化
- 自主決策的不可測性
- 缺乏稽核與追蹤

金管會「金融資安韌性發展藍圖」

- 強化經營階層資安治理職能與問責機制，鼓勵資安法規調適
- 加強資安人才培育與交流，從共通基準邁向策略目標
- 資安左移，安全納入設計
- 推動零信任架構，提升資安防護基準
- 強化資安監控及防護有效性
- 前瞻部署，因應新興科技的挑戰
- 強化供應鏈資安，健全金融資安生態系
- 加強資安情資分析與協同防禦
- 辦理資安攻防演訓，強化資安事件應處能量
- 強化多層次備援機制，確保關鍵金融服務可用性

資料來源：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202512300002&dtable=News

證券商金融檢查缺失 – 資訊安全(1)

– 特權帳號管理作業欠妥（113H2）

- 特權帳號管理有未符最小權限者
- 重要系統特權帳號，未建立帳號使用結果覆核機制，難以防範未經授權使用
- 最高權限帳號納管範圍欠完整

– 防火牆規則設定欠妥（113H2）

- 防火牆規則有允許使用對外連線網際網路及收發電子郵件之個人電腦直接連線正式營運環境伺服器或重要系統之管理網頁（如:防火牆、特權帳號管理系統）
- 防火牆規則有未以最小授權原則設定者
- 防火牆規則未建立定期檢視機制或檢視欠落實

證券商金融檢查缺失 – 資訊安全(2)

– 網段區隔未落實或未有適當區隔機制（113H2）

- 有測試主機與正式主機或備援主機置於同網段
- 透過「TCP/IP 證券交易資訊網路」連接證交所下單，未建置防火牆
- 有對外服務之核心資訊系統，未建置應用程式防火牆

– 對主機系統或資料庫重要安全參數設定有欠妥適（114H1）

- 主機安全參數設定作業欠周全，如：未設定重要稽核原則，不利異常事件追蹤、後台查詢系統未停用網際網路連線等服務程序，不利系統安全
- 料庫參數與設定有欠完整，如：雖有移除或停用原廠範例資料庫、啟用系統追蹤記錄檔，惟未停用與更名最高權限帳號、啟用資料庫稽核存取活動選項參數等

證券商金融檢查缺失 – 個人資料保護

– 辦理個人資料安全維護作業有欠確實

- 未將含有客戶個人資料之實體紙本文件及數位檔案資料納入清查範圍（113H1、113H2、114H1）
- 員工個人電腦（含筆電）未建置隨身碟（USB）使用控管措施，或對員工使用內部電子郵件信箱，及利用個人電腦連結外部私人電子郵件信箱傳遞涉及個人資料，未建置控管措施（113H1）
- 寄送董事會、審計委員會、薪資報酬委員會涉 機敏性會議資料及函復外部機關調閱之客戶資 料，未予加密（113H2）
- 將含有客戶個人資料之文件直接放置於開放空間或棄置於資源回收桶（113H2）
- 營業員洽請客戶將身分證明文件以影像圖檔傳送至營業員個人通訊軟體，或營業員翻拍端末機畫面之客戶買賣成交資訊，以個人通訊軟體傳送客戶（114H1）

資訊安全維運的困境

國家級威脅日益增長

惡意軟體持續演進

速度、規模、複雜度提升

警報疲乏

工具繁雜且未整合

壓縮的偵測與回應時間

身分識別和存取權管理

IAM（Identity and Access Management）

- 技術框架、流程與工具
- 確保「正確的人、在正確的時間、因為正確的理由，而獲得正確資源的存取權」
- 包含帳號管理、身分驗證和授權

管理的關鍵做法與核心觀念

- 集中式身分管理與驗證：第三方驗證提供者、多因子驗證、單一登入
- 存取權管理與授權：最小權限原則、角色型存取控制、特權存取管理
- 自動化生命週期管理
- 治理與合規：存取權審核、監控、稽核與清查

零信任架構

Zero Trust（零信任）：安全架構哲學。「永不信任，始終驗證（Never Trust, Always Verify）」

零信任下的 IAM 三大核心原則

- **明確驗證（Verify Explicitly）**：多因子驗證（MFA）、背景資訊（Context）
- **最小權限原則（Least Privilege Access）**：僅給予完成工作所需的「最小範圍」權限
- **假設已遭入侵（Assume Breach）**：微分割（Micro-Segmentation），限制「橫向移動」

零信任的運作

元件	情境說明	在 IAM 中的角色
身分鑑別	你是誰？	強制執行 MFA、無密碼登入（FIDO2, Authenticator）
設備鑑別	你用的設備是否安全？	檢查端點健康狀況（例如：OS 版本、是否有加密、安裝防毒）
信任推斷	綜合判斷是否核准存取？	根據風險動態調整權限（例如：IP在國外）

人工智慧的安全強化

法規與標準

- **台灣 – 人工智慧基本法**：定位 AI 發展為國家政策，列入七大核心治理原則
- **歐盟 – EU AI Act**：全球首部全面性 AI 法律，採「風險導向」分類
- **ISO/IEC 42001人工智慧管理系統（AIMS）**

政策與工具

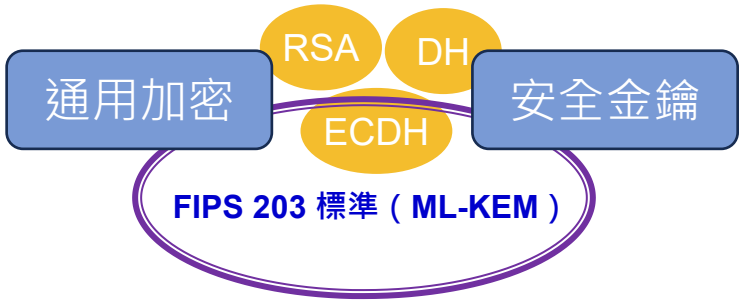
- **政策**：制定內部治理與作業流程
- **全面盤點AI資產**
- **AI 安全勢態管理（AI-SPM）**：評估和改善AI模型、資料和基礎架構的安全勢態
- **隱私強化技術（PETs）**
- **自動化提示詞攻擊與漏洞掃描工具**
- **AI Gateway**

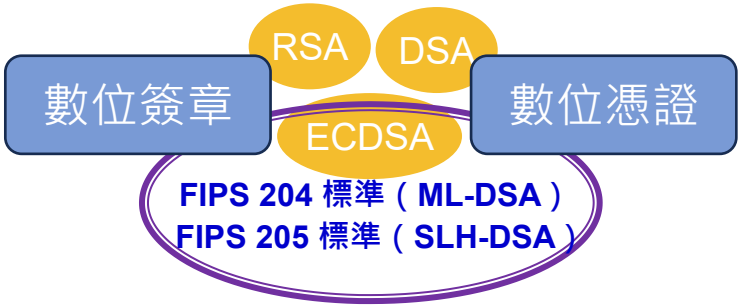
後量子加密

背景

- 用以對抗量子電腦對現存加密演算法弱點的攻擊
- 先竊取、後解密（HNDL, Harvest Now, Decrypt Later）

NIST於 2024 年 8 月正式發布後量子加密標準集





數位發展部數位產業署《後量子密碼遷移指引》

金管會預定在2026年發布金融業PQC遷移的參考指引

資訊安全的組態管理

為什麼重要

- **確保系統、伺服器、網路設備、應用程式始終處於「安全狀態」**
- **快速復原**
- **符合法規**
- **減少影子 IT**

組態管理的關鍵步驟

- **識別與基準建立（Baseline）**：參考國際標準（如 CIS Benchmarks 或 NIST），建立一個安全性基準
- **變更控制（Change Control）**：系統設定的修改都必須經過審核、測試與紀錄。這能防止因為一次「錯誤的設定」而導致資料毀損或外洩
- **狀態稽核與監控（Auditing & Monitoring）**：使用人工或自動化工具持續監測，以確認目前的設定未偏離當初設定的基準

雲端安全治理關鍵要素

- **共同責任模型（Shared Responsibility Model）**

圖片來源：CIS

- **雲端原生應用程式防護平台（CNAPP）**：整合了雲端安全態勢管理（CSPM）、雲端工作負載保護平台（CWPP）、身分識別與存取管理（CIEM）
- **資料防護**：加密傳輸中與待用資料，須符合 GDPR、ISO/IEC 27018 等合規要求
- **安全開發（DevSecOps）**：將安全性整合至 CI/CD 流程，確保程式碼部署符合安全規範
- **雲端財務管理（FinOps）**：監視與管理雲端的資源，避免誤用與濫用

API的安全管理 – API盤點

關鍵要素一、API 盤點

- **流量分析法**
  - ✓ 分析網路流量來發現實際運行的 API
  - ✓ 捕捉隱藏的「影子API 」
- **代碼與配置掃描**
  - ✓ 從開發階段就將 API 納入管理
  - ✓ Postman：測試和驗證API
  - ✓ Swagger：定義和描述API
- **主動掃描**
  - ✓ 利用自動化工具主動探測內外網環境
嘗試識別 HTTP 服務並進行端點爬取
  - ✓ 有助於發現「殭屍 API」

分類	欄位	說明
基本資訊	URL	API 的完整路徑（如 /api/login ）
	Method	GET, POST, PUT, DELETE 等
安全狀態	認證方式	無、API Key、OAuth 2.0、JWT 等
	資料敏感	是否涉及 PII、信用卡、醫療資訊
維運管理	負責人	誰負責開發與維護
	版本狀態	現行版本、過渡版本、或已廢棄
網路環境	曝露層級	外部公開或僅限內網

API的安全管理 – API防護

關鍵要素二、API防護

- **強化認證：** 棄用單純的 API Key，改用 OAuth 2.0 或 OIDC（OpenID Connect），並搭配 JWT（JSON Web Tokens）
- **最小特權原則：**確保用戶只能存取其權限範圍內的資源
- **多因子驗證（MFA）：**對於涉及核心金流或敏感設定的 API，要求二次驗證
- **防範暴力破解：**針對每個 IP 或每個 User ID 限制每秒請求數
- **配額管理：**根據服務等級協定（SLA）分配流量上限，防止單一服務異常消耗所有後端資源
- **強制加密：**全面使用 TLS 1.2/1.3 加密傳輸，禁止明文 HTTP
- **資料去識別化：**針對 PII 資料進行遮罩（Masking）或標記化（Tokenization）
- **回應內容過濾：**應嚴格定義 Response Schema，避免將資料全數吐出

供應鏈安全管理

供應鏈安全的面向

- **實體與物流安全**：確保產品在生產、運輸到交付過程的完整性
- **軟體供應鏈安全**：確保使用的開源元件、第三方軟體沒有後門
- **服務供應鏈安全**：管理外部委外廠商存取公司內部資源的權限
- **軟體物料清單（SBOM）**：列出產品內所有的函式庫與元件，以便發現漏洞時能快速清查
- **共用環境安全**：管理不同業者共用平台
- **API 安全**：管理與第三方服務進行串接

如何結合 IAM 與 Zero Trust

應用情境	傳統做法	IAM + Zero Trust
廠商維護存取	給予 VPN 帳密，可存取整個網路	Just-in-Time：僅在維護時間開啟權限，結束即刪除
第三方系統介接	使用 API Key，權限通常過大	Micro-Segmentation：只能存取特定的網路或單一資源
身分確認	相信供應商提供的員工帳號	Federation + MFA：廠商必須通過多因素驗證才能進入系統

以AI治AI

- 威脅偵測與預警
  - 使用 ML偵測未知威脅
  - 自動化關聯分析提升偵測準確度

- 自動化防禦
  - 即時部署防禦措施阻擋攻擊
  - 自動隔離受感染系統

- 落實法規遵循和倫理準則
- 遵守隱私保護與資料治理

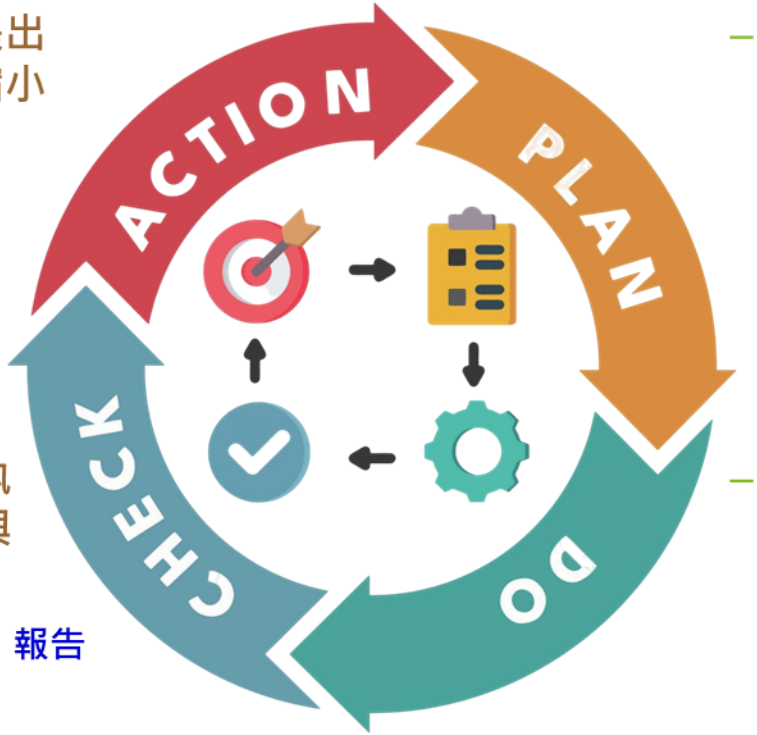
- 攻擊歸因與分析
  - 分析攻擊特徵識別攻擊者
  - 預測可能的攻擊目標

- 系統強化
  - 自動化漏洞修補與更新
  - 預測潛在安全風險

持續不斷的改善

- 制定資訊安全政策、建立風險評估方法，並規劃控制措施和目標
  - 年度目標
  - 預算與資源管理
  - 定期性作業排程
  - 重點優化項目

- 根據計畫階段制定的規範，實際執行資安計劃與控制措施
  - 建置符合目標的管控措施
  - 定期性作業執行、紀錄、報告
  - 重點優化項目的建置



- 監控與查核資安措施的執行成效，並將實際成果與預期目標進行比較
  - 內外部稽核計畫、執行、報告
  - 監控各項量測指標
  - 抽查與成效評估

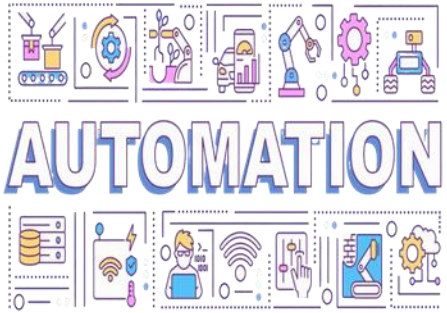
- 根據查核階段的結果，提出修正方案並採取行動來縮小差距
  - 矯正與改善作為
  - 調整目標、監測值
  - 管理審查

資安維運的建議

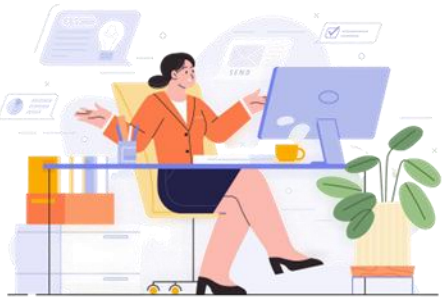
- EASM（外部攻擊面管理）
- 攻防演練/紅隊演練
- DDoS演練

- Defense In Depth
  - ✓ Physical Controls
  - ✓ Technical Controls
  - ✓ Administrative Controls

- 降低人力負擔
- 過濾無效警訊、規則調校
- SOAR（安全協調、自動化和回應）
- NOC/SOC/ISAC/CERT
- CNAPP
  - ✓ CSPM、CWPP、CIEM



- 資安教育訓練
- 資安認知課程
- 日常演練參與
- 宣導、情資分享



THE BEST IS YET TO COME