出國報告（出國類別：開會）

參加金融研訓院「2025 日本東京金融資安及科技防詐考察團」出國報告

服務機關：臺灣土地銀行
姓名職稱：王倩華資訊安全處處長
派赴國家：日本
出國期間：114 年 5 月 12 日至 5 月 16 日
報告日期：114 年 7 月 2 日

摘　　要

此次研習係活動實地走訪日本金融監理機關、資安實務單位、銀行資安主管部門與資安科技供應商動金融科技等單位，就**「台日金融資安分享交流會」、「日本銀行(BOJ)資安治理」、「AI 運算」、「雲端資安」、「Fintech 與資安」、「科技防詐」等六個主題進行學習與討論**，分享學習內容與心得建議。

目　錄

壹、目的

金融研訓院舉辦「2025 日本東京金融資安及科技防詐考察團」，因日本在國情、法制體系及金融環境與發展上與我國相近，旨在透過實地走訪日本金融監理機關、資安實務單位、銀行資安主管部門與資安科技供應商，深入了解日本在金融資安治理、防詐協作與資安新興科技應用等方面的最新作法，作為我國強化金融資安政策、實務能力與跨國合作策略的重要參考。

貳、過程

今年度本研修班以「台日金融資安分享交流會」、「日本銀行(BOJ)資安治理」、「AI 運算」、「雲端資安」、「Fintech 與資安」、「科技防詐」等六個主題詳述如下。

一、台日金融資安分享交流會

由本國中國信託銀行資安長(吳佑文)、日本瑞穗金融集團資安長及日本信用金庫網路安全中心主任簡報分享在資安威脅、防禦方式及實務作為後與出席之當地金融同業進行討論及交流。

(一) 資安威脅變得更加嚴峻：國家地緣政治因素(近期觀察到多起國家型攻擊，如：Mustang Panda、APT41、Volt Typhoon 等)、攻擊者 (Ransomware-as-a-service、使用 GAI 輔助攻擊行為、無檔案攻擊如 Living Off The Land, LOTL)、金融服務數位化 (數位客服、更多樣化的 API 串接合作)造成資安防守更加困難。

(二) 日本政府因應措施：經濟安全保障推進法 (適用對象：金融機構、基礎設施機構)，對某些特定國家要發生業務關係時需進行申報審查，架構主動網路防禦、警察廳與自衛隊設立網路管理團隊。

(三) 金融機構採取措施：

(1)從不同資訊源蒐集威脅情資，鎖定攻擊者並對其做詳細分析，如為高風險攻擊執行威脅獵捕，強化監控與偵測能力 。

(2)每天蒐集美國網路安全局 CISA 及各國 CERT 等發布的漏洞資訊，根據 CVSS 評分與攻擊案例給出綜合性評估漏洞，最後決定嚴重程度分級，最嚴重要在 48 小時內完成漏洞修補若超過處理期限須執行風險承受管理流程對，強化網路防禦安全。

(3)重要資料進行備份，預防勒索軟體加密檔案時能回復，進行公司內部高階主管及參與金融廳舉辦跨領域資安事件應對訓練與演練，實施經營部門及高階主管訓練以應對緊急狀況，加強資訊資安營運韌性。

(四) 威脅獵捕：針對可疑行為進行分析，由四個主要團隊 (Threat hunting team, SOC team, Red team, CIRT team) 協同合作，其中紅隊跟 SOC team 會形成紫隊針對內部防禦進行驗證；如 2024 年夏天瑞穗銀行接受日本政府指派進行調查，每個月投入 6.5 個人力幫助日本政府執行，調查過程並未檢測到寄生型攻擊，但透過 threat hunting 行動有發現一些以往並未發現的問題，例如日誌設定不完善等，透過威脅獵捕行動可以確認正在使用的日誌設定與監控是否完善，並將持續針對 PowerShell 內容屬於正常或異常設置標準。

二、資安治理

由日本銀行(Bank of Japan,BOJ)是日本的中央銀行就資安治理進行分享。

(一) 資安治理：BOJ 資安治理工作係與金融廳(FSA，日本之金管會)合作，對金融機構資安的要求，由金融廳主導，先由大型銀行來推行，再要求地方機關配合加強管理，完善各項措施，並做自我評估，建立了一套嚴謹且多層次的資安架構。從政策面到技術層面，皆採用國際標準（如 ISO/IEC 27001），並設立資安專責單位負責持續風險監控、事件回應與通報流程。其強調與外部機構（如政府、金融機構及研究單位）合作交流威脅情報，展現出高度的資訊透明與協作意識。

(二) 風險管理：BOJ 的風險管理體系以前瞻性與韌性為核心，強調對潛在系統性風險的預測與模擬。其風險評估框架涵蓋營運風險、財務風險、IT 風險以及聲譽風險，並採用壓力測試與情境模擬進行多層次的風險演練。特別的是，BOJ 並非僅止於符合監理要求，而是主動推動內部風險文化建構，落實風險意識至各層級員工。

(三) 新技術發展與應用：在數位轉型浪潮下，BOJ 亦積極導入新技術，包括 AI 應用、量子安全技術、區塊鏈與雲端運算等。貨幣（CBDC）的研究與實驗亦在進行中。BOJ 特別強調在試驗新技術時的「沙盒機制」，以降低風險、鼓勵創新。

(四) AI 應用：AI 在 BOJ 的應用目前聚焦於資料分析、異常偵測與政策研究輔助。例如，其利用機器學習模型分析金融市場動態、預測宏觀經濟指標走勢；同時也運用自然語言處理技術於金融監理報告、公開言論之語意分析，提升決策效率。

三、AI 運算

至日本 IBM 實地參觀辦公環境，該公司就以下 2 主題進行簡報

(一) 【IBM】Next generation agentic AI SOC threat detection and response

(1) 資安現況與挑戰:

1. 威脅加劇：生成式 AI 讓攻擊更快速、自動且精準，去年逾半數企業因此蒙受 500~2500 萬美元損失。

2.告警過量、工具碎片化：平均每家企業使用 83 種資安工具，來自 29 個供應商，有 51% 告警未處理，分析師負荷過重。

3.亞太成為主要目標：佔全球攻擊事件 34%（2023 年為 23%），日本受攻擊最嚴重，產業以製造、金融與保險為主。

4.金融業常見威脅：網路釣魚、公開應用程式漏洞、憑證竊取，需加強身分驗證、釣魚防禦、基礎建設安全。

(2) 介紹 IBM 代理式 AI 系統 ATOM

發展 Agentic AI（多代理式人工智慧），每個 AI 代理都有獨特的角色負責不同任務，例如：利用威脅情資來源 (如 X-Force 或預測性威脅情資 PTI) 來補充告警資訊、評估風險或推薦行動。由 ATOM 負責協調與整合內外部資源（Graph DB、ServiceNow 等），自動產生事件關聯圖、提升調查與應變效率在增強而非取代現有產品中的人工智慧能力 (如 XSIAM、Sentinel、Real SEC Ops)，在現有基礎之上透過 API 串接彈性加值。

(二) 【IBM】Impact of the Quantum computing era: Opportunities and Threats

(1) 量子時代對金融業的資安衝擊

量子電腦強大運算能力可破解現有的 RSA、ECC 等密碼學造成，攻擊者可偽裝成用戶或伺服器竊取憑證及加密機敏資料，偽造機敏資料及.數位簽章，影響文件真實性、導致惡意軟體植入或合約偽造。

(2) 日本 FSA 與金融業行動

1.2024 年組成 PQC(Post-quantum cryptography) 工作小組（含大型銀行）。
2.發布量子安全報告，預期 2024~2025 年啟動轉型。
3.2030 年設定為轉型目標年（Top Priority），兼顧地區銀行實務可行性。

四、 雲端資安

至日本 AWS 實地參觀辦公環境，該公司就以下 3 主題進行簡報

(一) 【AWS】Cloud Security & Compliance Sharing - Resilience of the Cloud

日本監管環境對使用對雲端使用管理寬鬆，與其他國家 (例如台灣或韓國) 不同，對於金融機構使用雲端服務沒有強制性的事前通知或核准要求，但銀行在進行重大變更事項時需通知監管機構，但無需特別證明或事前批准，要求系統設計需考慮容錯與失敗管理，建立可承受失敗的系統以避免重大損失，重視系統可靠性與穩健性。雖然日本不強制要求對雲端服務供應商 (CSPs) 進行定期第三方稽核，AWS 還是會提供外部稽核報告 (例如 SOC 報告)，客戶可以利用這些報告向監管機關證明合規性

(二) 【AWS】AI Security and Governance Sharing

根據日本的 AI 調查，超過 90% 的銀行、保險及資本公司已經使用 AI。調查顯示，存在「不採取行動的風險」(risk of not taking action)，不使用 AI 可能會影響對客戶服務的品質；惟

AI 應用面臨幻覺、公平性、資料安全、深偽詐騙等多重風險，日本的監管機關（金融廳 FSA 和日本銀行 BOJ）評估金融科技和創新是基於「風險導向」(risk-based approach)，並非因為存在風險就禁止使用，而是評估風險並檢視緩解控制措施。只要風險得到緩解或管理，就可以接受。銀行需有明確 AI 應用策略，並根據風險等級設計差異化的審核與管理流程。

(三) 【AWS】Japan Financial Institutions Cases Sharing

在零利率政策解除、人口結構變化、數位化浪潮以及年輕一代對金融服務的新需求的變革驅動力下，傳統金融機構面臨強烈數位變革，雲端技術在這場數位競爭中扮演著轉型的重要角色。

日本雲端使用案例介紹

SBI Securities：將線上交易系統遷移至 AWS (初期採用 Lift and Shift 模式)，每天處理超過 360 萬筆交易，雲端的擴展性能應對難以預測的交易量高峰。在架構上採用混合模式，訂單管理在雲端，與證券交易所的連線仍保留在地端，主要考量交易延遲性。

Nomura：使用生成式 AI 自動化廣告審查流程。審查人員從 3 人減少到 2 人，成果正擴展至集團資產管理公司。

Sumitomo Life (保險)：在 AWS 上建構資料平台，分析健康促進計畫 (Vitality app) 的數據。加速服務開發，推出創新產品 (如流感補償保險) 。

SBI Net Bank (BaaS)：領先的 BaaS 提供者，服務超過 20 家公司，預計很快將擴展到 50 家以上 (包含日本航空、高島屋百貨、日本職棒隊伍) 。

MUFG：利用 AWS 的 GenAI 技術提升企業銷售效率，建構類似 RAG (Retrieval-Augmented Generation) 的平台，分析公司財報(損益表、資產負債表)，透過聊天機器人提供洞見。研究時間縮短 95%，潛在客戶生成量提升 10 倍。

五、Fintech 與資安

至日本金融廳(FSA)就其推動金融科技創新概況、建立具資安韌性的金融體系及資安策略進行分享

(一) FSA 支持金融科技創新具體作為

(1) 設置金融科技支援平台 (FinTech Support Desk)：提供單一窗口協助相關應用於創新的業務之諮詢，FSA 盡力在五個工作天內回覆諮詢，諮詢面向領域包含區塊鏈，跨境支付或現金服務，證券、保險、募資等及資訊安全。

(2) 更新相關法規：Web3.0、穩定幣、安全型代幣、NFT 法規界定、託管規範等。

(3) 成立金融科技概念驗證中心 FinTech Proof of Concept (POC) Hub：PoC Hub 成立於 2017 年，提供金融創新試驗的輔導，目的在消除金融科技公司和金融機構嘗試進行創新時可能存在的猶豫和擔憂。評估 POC 案件之清晰性、社會意義、創新程度、使用者保護與可行性，決定是否提供支援；如果決定支持某個 POC，FSA 會在內部成立一個團隊，並在需要時與相關部門和機構合作，支持金融科技公司和金融機構進行創新展示，在一定期間內提供支持，包括實驗期間和之後的持續建議。

(二) 建立具資安韌性的金融體系及資安策略

(1) 日本政府整體資安架構 2014 年制定《資安基本法》，將 NISC（國家資安中心）作為資安戰略指揮中樞。2015 年制定網路安全戰略，制定政府網路安全目標和實施計畫的中期戰略。2024 年網路安全聚焦法制、回應能力、供應鏈風險、國際合作等面向。關鍵基礎設施保護網路安全政策，將 15 個部門定為關鍵基礎設施(包含金融部門)。

(2) FSA 最近發布了金融領域的網路安全指引，該指引於去年十月發布，適用於所有金融實體，但考慮到金融機構的規模差異，指引的應用採取分層方法，設有基本要求和進階要求

(3) Delta Wall IX 演練（2024）：覆蓋 170 家金融機構，情境包含：線上服務癱瘓、業務中斷、客戶資訊外洩， 強調 PDCA 循環與業界經驗分享， 開放遠端參與，強化實際應變能力。

(4) 紅隊演練（TLPT）：模擬真實攻擊情境、檢視人員、技術與流程的防護能力 已在區域性金融機構進行概念驗證，目標是推廣至全國性使用。

六、科技防詐

至金融科技創新社群(FINOLAB，是一個會員制社區和空間，為提供新創企業加速業務成長的後台共享服務，提供金融科技生態系統創新並創建 Fintech 業務，FSA 亦為其會員)，參觀實體環境及就下列 2 主題進行簡報

(一) 【FINOLAB】FinTech+金融詐騙

(1) 政府的監管沙盒制度 (Regulatory Sandbox) 允許在現有法規不允許的情況下測試，如某銀行與電力公司合作，利用電力供應數據偵測虛假帳戶，最初由於隱私法規禁止電力公司分享數據，他們透過監管沙盒制度進行測試，經過幾個月的測試，他們獲准使用該數據來預防詐欺活動。

(2) 在提供 BaaS(Banking as a Service)的發展下，銀行提供類似 Open API 的架構，可讓第三方非銀行業機構共同合作，如 JR 東日本鐵道公司和樂天銀行合作推出 JRE Bank 服務，依解帳戶持有人使用的銀行服務，每年可獲得優惠券外也可享有 JR 東日本的票券折扣

(3) 金融詐騙案件量持續提升: 語音（vishing）與簡訊（smishing）詐騙，並利用 AI 提升真實感。詐騙目標已從個人客戶擴展到企業客戶，對網路銀行和線上券商造成嚴重威脅。

(二) 【FINOLAB】防詐科技應用實例分享

金融業在打擊詐騙方面的主要挑戰

(1) 許多系統較傳統，特別是地區性銀行缺乏知識、經費及對工具的了解。系統多由大型系統整合商構建，導入新功能昂貴且耗時，不利於應對快速變化的犯罪手法

(2) 高齡化人口與新科技推廣困難：引入新科技 (如 FIDO、無密碼登入) 在日本需要非常久的時間。年輕使用者佔比低 (約 7-10%)，企業為了避免造成使用者困擾，不會強制推行新工具，而是緩慢導入

(3) 犯罪手法進化：使用 AI (如語音釣魚詐騙)，或利用虛擬機、跳板登入。

近期重大犯罪案例分享

證券帳戶被盜：日本樂天證券

手法：透過釣魚網站取得使用者帳號密碼，登入投資帳戶 (日本投資帳戶可存錢)

獲取資金方式：將證券帳戶資金轉出至銀行帳戶，或操縱交易量低的股票價格來獲利

問題點：證券轉銀行帳戶時認證方式不夠完善 (多只比對帳戶名稱)。操縱股價手法使得難以證明買股票者是犯罪者

影響：造成 1600 多億日圓損失

FSA 事後對策：強制實施多因子驗證 (MFA)，之前因為考慮使用性而未強制要求

日本正在推行的新對策/討論

(1) 新的指導方針 (2024/8)：防詐騙規範不再只針對大型金融機構，而是擴展到地區性銀行，要求所有銀行遵守同樣詳細的規範，因小型銀行也會發生詐騙事件

(2) 假帳戶策略 (2025/4)：討論讓警察開設銀行帳戶，將其提供給犯罪者使用，以便追蹤金流走向 (反向釣魚/偵查)。

(3) 討論即時犯罪資訊共享平台：日本全國銀行協會正在討論建立平台，讓金融機構之間可以即時分享犯罪資訊 (過往多為事後向監管機關報告)。

(4) 在防詐科技應用部分，已有部分金融企業加強對網路銀行的異常登入分析，透過客戶歷史操作行為進行建模並設計風險閥值，並搭配金融機構黑名單情資共同建立安全防護網，降

低並主動攔阻詐欺者透過外洩帳密登入至銀行系統的風險。2024 年 FSA 首次發出全金融業強化資安的統一命令。不再依規模區分，全面要求加強防詐。

參、心得與建議

一、 台日資安比較：防禦方法、技術、管理架構很多都非常相似，加上地緣政治相近，許多攻擊態樣跟趨勢也都相近；與台灣差異為是台灣整體金融資安發展由行政院術數位發展部主導，要求各中央目的事業主管機關訂定及執行，包含治理、規範、演練 (DDoS)、技術查核等，都會定期檢視並有所要求；日本主管機關多為協助角色，給予各金融業較大的彈性，而各金融業自治也做得非常完善，統籌情資部分也是由 ISAC 辦理。

二、 生成式 AI 不僅是攻擊工具，也可善加利用做為防禦工具：AI 常被用來生成惡意內容（如釣魚郵件、Deepfake），但同時生成式 AI 也可以在防禦端扮演多代理人協作角色，主動評估、整合、行動，甚至學習分析師的處理邏輯進行自我強化，作為資安防禦的工具。資安防禦不只是技術問題，更是「效率問題」；資安團隊面對的挑戰不只是技術強度，而是「處理速度」與「資源分配」，當告警量大到系統或人力無法處理時，告警就會無意義，如何讓資安「智能化轉型」，學會如何與 AI 協作強化分析與到應變，是資安人才未來應加強之技能。

三、 因應量子電腦運算能力發展，「量子安全」其實是一場涵蓋系統盤點、風險評估、組織流程優化的長期工程。所以轉型不只是 IT 的任務，而是整個企業營運策略的一環。資安不能只著重在「現在的威脅」，而應放眼「未來的防禦」；量子運算雖然尚未完全問市，但對現有加密技術的威脅已經存在。即便量子電腦現在還無法破解 RSA 或 ECC，加密資料卻可能「現在被竊取、未來被解密」。資安防線必須提前布局，避免機敏資料被竊風險。主動為 5~15 年後的風險預做準備。

四、 資安已成為金融穩定的核心議題，面對全球駭客攻擊形式及手法多變及複雜，維持運營環境維持系統穩定度為首要，金融機構須針對組織規模與風險特性建立自行資安防禦策略，先訂定風險等級再決定各項防護措施能讓資源得到較好的利用，資安不只是技術問題，更是組織治理與風險溝通的整體工程。