出國報告（出國類別：其他）

赴日本參加「2025 日本東京金融資安及科技防詐考察團」

服務機關：臺灣銀行 資通安全處
姓名職稱：洪琳美 科長
派赴國家/地區：日本/東京
出國期間：114 年 5 月 12 日至 114 年 5 月 16 日
報告日期：114 年 6 月 24 日

摘　　要

本次奉派自 114 年 5 月 12 日至 114 年 5 月 16 日，前往日本參加「2025 日本東京金融資安及科技防詐考察團」。經由各場次之交流分享會，由講者介紹日本在金融科技應用、資安技術與防制詐騙手法等面向之推動現況與作法，了解先進國家在監理機制與創新服務之間，如何取得平衡。

本次經由實地參訪日本金融監理機構、資訊廠商、Fintech 機構等單位，報告內容將就各場交流會之講者說明進行重點摘要，並就相關心得收獲進行說明，茲摘錄相關心得如下：

一、臺灣金融機構在資訊安全管理上，主要依循主管機關所公布之規定及程序辦理，強調法規遵循與合規面之執行。相較之下，日本金融機構在資訊安全的管理上，更具有高度的自主性。交流活動中日方講者分享，多數日本金融機構已將資安合規內化為組織文化的一環，資安意識深植於組織運作中。

二、隨著量子電腦技術快速發展，現行加密演算法未來可能面臨被破解之風險。各企業在關注現有資安技術的同時，亦應提前因應新興科技所帶來之潛在威脅。日本政府與相關企業已攜手推動「後量子加密」（Post-Quantum Cryptography, PQC）轉型，透過政策引導與產業合作相互補強。本項轉型亦需高階管理層、系統單位與法遵部門共同參與，以有效落實。

三、日本金融業近年積極導入新科技並推動系統上雲。據報導指出，三菱日聯金融集團（MUFG）於 2017 年，已率先將內部資訊系統遷移至公有雲，成為日本首家全面導入公有雲的銀行，預估五年內可節省約 100 億日圓之成本。此舉除提升營運效率與韌性外，亦有助於確保業務持續性。臺灣金融業可借鏡日本金融業上雲策略，同時預先規劃下雲（Plan B）方案，以備不時之需。

四、日本金融監理機構強調，在創新與穩定之間，須取得平衡，並推動產學合作以促進金融科技永續發展。日本在資安演練方面已建立制度化機制，由政府、主管機關、金融業者與資訊公司協力辦理演習（如 Delta Wall）等，以強化

金融環境之整體資安韌性。

五、日本 FINOLAB 的創新應用令人驚艷，如新創公司與地區電力公司合作，利用電表數據判斷用戶之登記地址，檢核房屋是否為空置狀態、登記之使用人是否與申辦銀行業務之申請人相符等，不僅有助於辨識可疑地點，更成為防範詐騙與阻止人頭帳戶開立的有效手段。

六、各金融機構雖在多數業務（如存款、放款等）等面向上屬於彼此競爭關係，但於資安面則是彼此合作。結合主管機關、協力廠商及業界資源，落實資安聯防並推動情資共享，有助於提升整體防護能力。

此次參訪除聆聽日方講者經驗分享外，活動期間外，能與來自臺灣其他銀行、證券、壽險等業界之金融機構，及財金資訊等金融周邊機構的團員們交流互動，分享各自機構在資安管理上之經驗，不僅拓展了視野，也學習了其他單位相關資安措施值得借鏡處，從交流學習中成長。

目　次

壹、目　的

臺灣金融研訓院為臺灣目前最大的金融研訓機構，除了辦理專業金融證照測驗、金融專題研究發展外，近年亦積極推廣赴國外之金融參訪交流行程，如 112 年新加坡、113 年印度、美國舊金山等地參訪計畫等，以經由相關參訪團隊，見習交流其他地區於金融創新等領域之發展及相關機制。

本次奉派自 114 年 5 月 12 日至 114 年 5 月 16 日，代表本行參加金融研訓院主辦，財金資訊股份有限公司協辦之「2025 日本東京金融資安及科技防詐考察團」，參訪團隊係由金融研訓院林副院長帶隊，參與學員除金融研訓院同仁，亦包含財金資訊股份有限公司、臺灣期貨交易所、臺灣證券交易所、臺灣集中保管結算所、證券櫃檯買賣中心等金融周邊機構及 11 家公民營之金融機構等，參訓學員共計 25 人，部分銀行亦由資安長親自出席並與日本方分享臺灣之金融資安實務經驗，此外，曾經在日本求學與工作之 LINE Pay 公司謝資安長擔任隨團顧問，偕同大家一起前往日本交流學習，參訪日本金融監理機構、資訊廠商、Fintech 新創機構等單位。

貳、過　程

一、參訪團隊成員

本次參訪行程之學員計有 25 位，由國內金融周邊機構及國內公、民營之銀行、證券及壽險機構組成，金融研訓院除工作人員外，亦安排一位同仁參訓，參訪團成員服務單位清單如下：

No.	類別	服務機構	服務單位
1	金融周邊單位	財金資訊股份有限公司	企劃部
2	金融周邊單位	財金資訊股份有限公司	研發部
3	金融周邊單位	財金資訊股份有限公司	資安部
4	金融周邊單位	臺灣期貨交易所股份有限公司	期貨商輔導部
5	金融周邊單位	臺灣期貨交易所股份有限公司	資訊規劃部
6	金融周邊單位	臺灣證券交易所	券商輔導部

No.	類別	服務機構	服務單位
7	金融周邊單位	臺灣證券交易所	資通安全組
8	金融周邊單位	臺灣集中保管結算所	數位暨資安部
9	金融周邊單位	證券櫃檯買賣中心	資訊部
10	金融周邊單位	證券櫃檯買賣中心	券商輔導組
11	銀行	臺灣銀行	資通安全處
12	銀行	臺灣土地銀行	資訊安全處
13	銀行	彰化商業銀行	資訊安全處
14	銀行	台北富邦銀行	資訊安全管理部
15	銀行	中國信託商業銀行	資訊安全部
16	銀行	玉山銀行	資安管理處
17	銀行	永豐銀行	資訊安全處
18	銀行	台中商業銀行	總行
19	銀行	國泰世華商業銀行	資訊安全部
20	銀行	國泰世華商業銀行	核心資訊部
21	銀行	國泰世華商業銀行	數據生態營運部
22	壽險	國泰人壽保險	總公司
23	壽險	國泰人壽保險	資訊安全部
24	證券/金控	元大證券/元大金控	資訊安全管理部/資訊安全部
25	其他	台灣金融研訓院	資訊處
26	其他(隨團顧問)	LINE Pay	資訊安全長

二、參訪行程

有關本次參訪主題，分為資訊安全、資安治理、AI 運算、雲端資安、Fintech 等與資訊安全及科技防詐相關之面向議題，以下為本次考察團之行程安排：

日程	行程資訊	主題	地點
114/5/12(一)	搭機赴日本東京		
114/5/13(二) 交流活動一	台日金融資安分享交流會	【資訊安全】 由光盾資訊科技(RayAegis	東京都立産業貿易センター浜松町館

日程	行程資訊	主題	地點
		Japan)資安公司、中國信託商業銀行、日本 Mizuho 瑞穗銀行、信用合作社等代表，以交流研討方式進行	
114/5/13(二) 交流活動二	日本銀行(BOJ)	【資安治理】 日本資安治理實務	BOJ 貨幣博物館
114/5/13(二) 交流活動三	日本 IBM	【AI 運算】 金融業的人工智慧應用與治理 後量子運算安全	虎之門之丘車站大樓
114/5/14(三) 交流活動四	日本 AWS	【雲端資安】 雲端應用與新科技資安探討 日本銀行客戶分享使用案例	Amazon Japan Headquarters
114/5/14(三) 交流活動五	日本金融廳 (FSA)	【FinTech 與資安】 金融科技創新成長策略 資安韌性發展與管理	FSA 會議室
114/5/15(四) 交流活動六	FINOLAB	【科技防詐】 日本詐騙新趨勢 防詐科技應用實例分享	FINOLAB 會議室
114/5/16(五)	搭機返國		

三、交流活動

(一) 交流活動一：臺日金融資安分享交流會

首場交流活動為「臺日金融資安分享交流會」，由光盾資訊科技(RayAegis Japan)主辦，除了台灣的參訪團成員外，來自日本「瑞穗金融集團」及「信用金庫銀行」等主要金融機構資訊安全長(CISO)等成員亦出席，本場交流活動中，日本方計有 28 位來自各金融領域之資安主管與同仁參與，值得一提的是，除實體會議外，主辦單位

亦開放遠端參與方式，事前開放無法親臨現場之日本金融機構報名參加，約有來自日本關西和九州地區 10 餘位金融同業，透過線上會議方式參與，活動現場亦同步提供中、日雙語翻譯服務。

本場研討會的交流重點，著重於臺日兩國在金融科技創新與網路安全領域的共同挑戰，以「臺日金融機構網路安全對策」為主題，隨著數位化發展，金融機構面臨的網路攻擊風險日益增高，跨國間的知識分享亦顯得尤為重要。除主辦單位外，亦由臺灣「中國信託商業銀行」與日本「瑞穗金融集團」之資安長(CISO)，以及日本「信用金庫」資安主管進行分享。

分享主題	分享單位	重點摘錄
台日金融資安分享	光盾資訊科技 (RayAegis Japan)	■ 台日金融監理差異 (1) 日本的監理方式，大多採自願性規範，多數金融機構自發性很高，在資安自我管理方面完善。日本方面由 ISAC Japan 主導情資共享，並定期舉行聯合演練，約有400多家機構參與防禦合作。 (2) 臺灣的主管機關，則經由發布各項法令法規，要求金融機構依相關規範辦理，並定期執行資安治理、資安檢測等相關控制措施，同時進行內外部稽核，確保各金融機構之合規性，其監理方式與日本相比，略有不同。 ■ 2025年重要資安威脅： (1) 供應鏈問題：講者分享2025年1月至5月，約偵測到1,300餘支惡意

分享主題	分享單位	重點摘錄
		JavaScript 程式，甚至有在 ATM 中發現者。 (2) DDoS 攻擊頻繁：大多金融機構面對流量較大或網站首頁大量連線之因應，已無太大問題，講者建議可進一步思考新的 DDoS 測試方式，將漏洞的單點 Denial-of-Service 加入測試：如正規表示式 Regular Expression Denial of Service、圖像處理 Denial of Service、Hash Table Collision Dos，以及其他可能造成計算及空間資源大量耗盡之漏洞。
管理資安風險機制之有效性	中國信託商業銀行 吳佑文資安長	■ 銀行風險情境之掌握與評估 (1) 銀行需要了解可能面臨之資安風險情境：情資蒐集團隊，可經由蒐集和閱讀全球資安新聞、情資報告等資安情資來源，及時獲取新出現的攻擊樣態與攻擊手法。 (2) 針對上開蒐集到之風險，進行分類並歸納，建立組織之「資安風險情境清單」，並定期進行年度風險情境評估，評估的標準可依據各風險情境發生的可能性及其對金融機構可能造成的影響，確定其風險等級，採取後續因應措施。 ■ 縱深防禦機制設計：組織之縱深防禦機制，必須根據不同之攻擊路徑及手

分享主題	分享單位	重點摘錄
		法進行設計。每種攻擊方式會有相對應之防禦措施，針對這些防禦機制，除了建立防禦關卡和控制措施外，亦需要設立各項監控指標，並針對上開指標加以觀測，以確保相關控制措施及監控指標之有效性。 ■ 檢視縱深防禦機制的有效性： (1) 講者指出，即使組織已設有縱深防禦機制並配置相關監控指標，但若指標未告警，亦不全然代表防禦機制必定有效，依據相關新聞報導等案例顯示，即使防禦設置與指標正常，惡意攻擊者仍然有可能突破防禦。 (2) 關於有關防禦機制無法有效運作的原因可能包括：監控範圍缺漏、防護失效或人員疏失（如未依 SOP 程序辦理）等。因此，藍隊監控團隊成員，除辦理監控外，亦應主動定期驗證組織內部縱深防禦之有效性。可經由設計有效性之測試及驗證劇本，利用實際手法進行測試，用以確認在攻擊路徑上對應之縱深防禦機制是否有效，經由測試演練劇本，驗證組織之後續通報、監控告警等機制流程，是否與預期相同。

分享主題	分享單位	重點摘錄
金融機構如何因應日益嚴峻與多樣化的網路威脅，並分享 Mizuho 資安策略與實務	瑞穗金融集團 資安長(CISO) Osamu Terai 先生	■ 整體趨勢與威脅現況 (1) 地緣政治風險提升：如俄烏戰爭，受地緣政治影響，造成國家級攻擊者活躍。 (2) 攻擊技術進化：目前已出現如 RaaS(Ransomware as a service, 勒索軟體即服務)、Living Off The Land(利用合法工具行動)、生成式 AI 應用等攻擊手法。 (3) 資安風險多元化。 ■ 瑞穗金融集團對於威脅情報與獵捕(Threat Hunting)之作法： (1) 日常蒐集情資來源涵蓋 FS-ISAC、社群媒體、暗網(Dark Web)等。 (2) 利用 MITRE ATT&CK 框架，模擬國家級駭客組織 MirrorFace 之攻擊場景，該駭客組織自2019年起，針對日本發起了網路間諜攻擊活動，竊取日本相關技術和機密資訊。 ■ 日本政府之因應政策：制定《經濟安全保障推進法案》、資安審查等法案，用以強化資安治理，以保障日本國內之關鍵基礎設施，以及確保戰略技術和物資、防止相關技術外流，避免因受網路攻擊而導致社會與經濟受巨大影響。此外，亦同步建立警察機構與自衛隊等專責資安部隊。

分享主題	分享單位	重點摘錄
		■ Mizuho 瑞穗集團資安策略：建立橫跨 Mizuho 子公司之 CISO 組織、組成 CIRT 及紅隊/藍隊/紫隊等團隊，以提升集團之實戰演練與威脅獵捕能力，同時，亦同步關注即時回應與攻擊面管理(ASM)。
信用金庫業界的網路安全對策與支援	信用金庫 網路安全中心主管 Koji Nkajima	■ 日本信用金庫之定位：信用金庫為服務中小企業與當地居民的協同組織之地區性金融機構，其業務包含存款、放款、匯兌等，並已逐漸拓展至投信、保險等領域。 ■ 日本信用金庫現況(截至2023年3月)： (1) 單位總數：254間、分行：7,106間 (2) 營收狀況：存款160兆日圓、放款79兆日圓 (3) 員工總數：約9.9萬人 ■ 信金資訊系統中心(SSC)之角色與任務：擔任全國信用金庫之系統支援與連結平台、提供共同開發、穩定運行、提升效率的資訊系統服務，亦即全日本信用金庫之資訊作業，統一由該中心維運管理。 ■ 資安對策： (1) 透過 Face To Face 專網、網站服務，實現符合金融業資安規範的架構。

分享主題	分享單位	重點摘錄
		(2) 系統設計讓信用金庫內部 IP 不對外曝光，並支援日誌查閱。 (3) 提供低負擔的主機代管與網站管理服務。 ■ 非系統面之各項資訊安全支援措施： (1) 舉辦定期資安演練與訓練、提供相關教材與學習資源，如線上教育訓練站台。 (2) 提供諮詢窗口與專家派遣服務。 (3) 開辦仿冒釣魚網站自動偵測與通報服務、標靶式郵件攻防演練。

(二) 交流活動二：日本銀行

於日本銀行參訪活動前，日方先安排團隊成員參訪位於東京中央區日本橋的「貨幣博物館(Currency Museum)，此博物館係由日本銀行金融研究所設立，為一個專門展示日本貨幣歷史之博物館，博物館內之展出內容，係依時代劃分，展示從古代貝幣、刀幣到日本近代紙鈔的演變歷程，有助於參訪者深入了解日本貨幣發展。從實體展示至多媒體之互動說明，介紹了貨幣之鑄幣技術與日本近期發表新鈔之防偽設計，有助於從中了解日本經濟發展與貨幣制度。此外，館內還介紹說明了日本央行的三大核心職能：貨幣發行、物價穩定及金融市場維護，整體的參觀動線，及與參觀者之互動，十分友善。

於參訪完貨幣博物館後，團隊一行人轉往位於貨幣博物館附近的商辦會議室，聽取日本銀行簡報，經由簡報者有田先生介紹，日本銀行作為政府銀行，對民間金融機構進行監視、規劃建議與現場稽核，並強調對於金融監理除了辦理業務檢查外，

更應注意輔導與預防。

日本銀行目前除辦理金融機構的支援角色外，其業務範圍亦包含對相關技術發展（如生成式 AI）進行研究與提出報告，講者提及 AI 目前於日本銀行的應用上，主要在於資料分析、異常偵測等面向，並提醒組織在創新推動的同時，也要考量強化風險辨識與跨國合作，並針對 AI 帶來的挑戰，提早進行因應。

(三) 交流活動三：日本 IBM

日本 IBM 公司，位於日本東京虎之門大樓 31 樓的「IBM Innovation Studio」，為 IBM 全球數十個創新中心之一，現場並同時展示幾個應用人工智慧之運用場景：如透過手機掃描名片上之 QR Code，即可於手機上顯示含有該名片人物之多維度自我介紹影片，將名片由傳統平面式，走向 3D 立體場景，由名片上印的人員，實際以聲音及影像顯示方式進行自我介紹，有助於對方更理解該名片所代表之人。此外，現場亦展示了當民眾（被保人）發生車損欲申請理賠時，透過人工智慧的輔助，可實現快速保險理賠申請等情境。

於日本 IBM 參訪過程中，IBM 代表進行了二場分享會，第一場分享係說明透過多代理(Multi-Agent) AI 技術，協助客戶「偵測威脅、調查事件、加速回應」，建立名為 ATOM(Autonomous Threat Operations Machine)的平台，此平台內建置有多個 Agent 協助組織執行各項作業：如檢視監控 SIEM(Security Information and Event Management)平台資料之 Agent、比對攻擊手法並給與因應建議之 Agent 等，打造有如「AI 資安團隊」的監控團隊，透過導入該 ATOM 架構，有利於企業提升資安自動化及協同作業能力，經由 IBM 統計分析，可協助處理組織約 6 成的監控事件，整體加快處理效率約 3 倍以上，幫助組織之資安監控人員，能更專注於處置高風險之威脅，實現 SOC 更為自動、自主化運作。

IBM 的第二場演說，則聚焦於量子電腦，量子電腦對現有加密構成潛在威脅，

當量子電腦成熟後，現今常用的非對稱加密（如 RSA、ECC 等演算法）可能會被破解，導致金融業、政府、醫療等重要領域的資料面臨機密性、完整性和可用性風險。依據講者分享指出，目前日本政府已啟動 PQC 轉型推廣，日本金融廳(FSA)並已發布相關報告，以及於 2024 年成立工作小組，設定 2030 年為轉型目標年(Top Priority)，IBM 講者建議金融機構制定加密資產盤點、遷移策略與管理機制，並以 2030 年中，完成高優先系統轉型為目標。

整體而言，IBM 認為 PQC 的轉型需長期投入，因此，建議從策略規劃、風險評估到實施解決方案分階段進行，及早思考此議題及規劃因應。經由 IBM 的分享得知，日本政府及日本相關金融業，已經開始著手合作推動後量子加密(PQC)轉型，面對相關技術變革，需要政府政策支援，並與產業協同合作彼此相輔相成。除了資安部門外，亦涉及企業高層、系統及法令遵循等多部門的協同合作。

(四) 交流活動四：日本 AWS

此場交流會來到日本 AMAZON 亞馬遜總部，其辦公大樓位於東京目黑區的 ARCO Tower，該大樓對於來訪來賓皆要求需單一之通行碼，用以進行人員進出大樓之驗證，同時，於發給來賓佩掛之識別證背面，明確給予發生急難時之避難場所與緊急聯絡人員、電話等資訊，日本與臺灣同屬地震活躍板塊，此舉有助於發生急難時來訪來賓聯繫使用，讓人印象深刻。

於日本 AWS 交流活動中，該公司活動主持人於會議一開始，即發表了 AWS 機房於本(2025)年 6 月起，將於臺灣落地的新聞，經由建立 AWS 基礎設施「區域」(region)，讓臺灣企業能申請使用位於台灣本地之資料中心。

在 AWS 參訪過程中，講者說明了日本在金融服務業中人工智慧(AI)與雲端技術的應用現況及相關監管要求。如同首場臺日金融會談之與會者所分享，日本的金融監管環境相對而言較為寬鬆，但銀行在採用新技術時，仍應高度重視風險管理、合規性，並應注意與監管機構的溝通，在雲端服務與 AI 應用方面，亦須關注資料安全

等潛在風險。

此外，AWS 講者也分析了雲端運算對金融機構之益處，透過導入雲端，不僅有助於企業提升運營效率，並能促進跨產業合作。但需注意於系統設計上，應考量失敗的可能及「下雲」的策略程序，以確保業務持續運作。此外，教育推廣對於提升客戶與監管機構對新技術的理解亦相當重要，透過客戶、雲端業者、主管機關等各方的理解與支持，有助於金融機構建立穩健且安全的金融科技應用環境。

在日本 AWS Japan Cloud Security and Compliance - Resilience of the Cloud 主題分享活動中，主要聚焦於日本在雲端服務領域的監管作業與適應性。講者指出日本相較其他地區的主管機關，對雲端技術的態度更為友善。但亦提醒各金融機構，在關鍵業務遷移至雲端時，應與主管機關等核心監管機構保持良好溝通，事前通知主管機關預計採行之措施與作法，以維持良好關係。

AWS 的第二場分享為 Navigating AI Compliance，基於亞太地區金融業人工智慧應用的快速發展，以及監管機構對風險管理與合規性的高度關注，金融機構應依據 AI 應用的風險等級，建立差異化之管理流程，強化系統的可解釋性與安全性。此外，持續掌握監管趨勢與技術創新，不僅有助於提升銀行 AI 應用的合規性，也能有效降低潛在風險，確保金融科技發展之穩健。目前 AI 已被利用於網路安全與防範詐騙等運用上，結合外部與企業自身持有的數據，進行 AI 訓練與檢測。講者在分享中同時指出，在 AI 發展上，AI 偏見、AI 幻覺問題目前尚難以完全根除，現階段可透過結合 AI 對 AI 檢查，以及人工審查(Human in the Loop)加以輔助，同時，建議金融機構在使用相關雲端 AI 服務時，應對自身與供應商之責任分工，明確進行定義。

AWS 最後一場分享主題為 AWS Japan Financial Institutions Cases Sharing，探討日本金融產業在面對來自非傳統領域的競爭與合作壓力時，應積極導入雲端、AI 等創新技術，以提升整體運營效率與市場競爭力。金融機構同時需應對資料安全、災害備援等挑戰，傳統金融服務業(FSI, Financial Services Institute)企業可強化跨界合作(如 NTT DoCoMo、PayPay、Rakuten 等公司之合作案例)、推動數位轉型並完善風險

管理，透過審慎評估雲端技術的效益與風險，促進產業的穩健發展與創新突破。

(五) 交流活動五：日本金融廳(FSA)

日本金融廳為日本政府負責金融監管之主管機關，與我國金融監督管理委員會相似，涵蓋監管銀行、保險、證券等金融機構之監理，在此場次的交流活動中，日方進行了兩場簡報，分別為「金融科技創新」及「建立強韌金融體系，以應對網路安全風險」兩項主題。

日本金融廳強調在推動金融科技創新時，必須就金融體系穩定、使用者保護與反洗錢(AML)/反恐融資(CFT)之間，取得適當平衡，以確保金融創新與監管要求相互協調，維持市場安全與秩序。

目前為了減少金融科技公司與金融機構在進行創新示範時的疑慮與發展，日本金融廳於 2017 年，設置了金融科技概念驗證(PoC)中心，並推出金融科技支援窗口，提供企業一站式諮詢服務，協助金融科技發展過程中，可快速適應監管要求並同時保持技術創新。

除了上述作為外，身為主管機關的日本金融廳，亦積極與民間進行產學界合作，舉辦日本金融科技週(Japan Fintech Week)等活動，在日本金融科技週活動中，涵蓋研討會、工作坊、新創簡報與交流會，吸引全球的金融科技業者、監管機構與投資人參與，透過展示日本在區塊鏈、AI、數位貨幣等領域的政策與應用成果，以促進新創合作及吸引外資，強化日本成為亞洲金融科技樞紐的地位，推動產業發展與創新應用。

最後，在面對日益複雜的資安攻擊情境下，日本金融廳認為，網路安全除了技術問題外，亦涉及組織內、外部人員和整體業務流程。為了提升日本金融業的網路安全，日本金融廳除了制定了一系列的指導方針，並積極提供金融機構各種支援與資源，包括舉辦跨金融業界資安演習(Delta Wall)，以提升整體金融體系對網路攻擊

的應變能力，參與機構在限定時間內，根據各金融業別（如證券、銀行、保險）的情境進行應對，包括內部通報、系統隔離、資訊公開，並與外部單位（如主管機關、同業）協調等活動，協助金融機構模擬與應對潛在威脅，演練結束後，日本金融廳亦彙整各機構之優、缺點，提供個別回饋，並鼓勵各金融機構進行 PDCA 回饋循環機制，以強化其組織資安韌性。

日本金融廳經由 Delta Wall 資安演習，達到公助（與政府、主管機關之通報）、自助（金融機構本身即時應變及決策能力）、共助（與同業的情資分享）三大層次的防禦。除了提升單一金融機構的應變能力，並有助於強化整體金融體系在面對複雜資安威脅時之協同防禦能力。

(六) 交流活動六：FINOLAB

最後一場交流活動，來到位於東京大手町的金融科技創新社群(FINOLAB)，此創新聚落致力於推動 FinTech 產業的發展與跨領域合作，亦是日本首個也是規模最大的金融科技孵化與加速中心。FINOLAB 成立於 2016 年，係由三菱地所、電通株式會社及電通技術研究所的共同合作項目所成立，提供共享辦公空間、專業諮詢、創業資源及業界交流機會，吸引了眾多金融科技新創企業、金融機構及監管機構參與其中，包含了新創企業會員、業界團體會員、FinTech 相關等國內、外機構。

經由金融科技創新中心 Shibata 先生分享，FINOLAB 聚集了超過 800 位會員、57 家新創公司與 30 家企業，並促成多起的企業跨界合作，日本金融科技已從傳統金融業務延伸至綠色金融與 Web3 等新興領域，展現多元發展趨勢。儘管 2024 年創投資金略有減少，整體產業仍保持穩健成長，持續推動創新與技術應用。

對於詐騙的因應方面，講者於分享過程中指出，現今詐騙手法日益多元，包括語音詐騙(Vishing)與簡訊詐騙(Smishing)已成為常見手法，目前詐騙集團亦結合人工智慧 AI 技術以提升欺詐的真實感與臨場感。詐騙不分國界，日本的受害對象和臺灣

相同，已從個人戶擴大至公司戶，除了對網路銀行與券商造成威脅，亦導致受害及損失金額不斷攀升，為有效應對這些威脅，須透過強化身份驗證機制、異常行為偵測及不斷的使用者教育訓練，以提升整體防禦能力，降低詐騙風險。

此外，於本交流會中，透過 Caulis 新創公司技術長的分享，說明了日本金融犯罪隨著疫情發展以及無現金化推動，詐騙案件（如假帳單、釣魚網站、簡訊詐騙與信用卡盜刷等）急增。以日本境內來說，2023 年網路金融損失達百億日圓，2024 年上半年 SNS 簡訊詐騙損失已近 800 億日圓，金融產業面臨的相關挑戰包含：使用者裝置老舊、老年人口難以適應創新技術、犯罪者使用 AI 等技術規避追查及監控系統仍較為傳統等，因此，持續培養企業及民眾資安意識相當重要。

Caulis 公司為日本網路安全新創公司，於 2015 年成立，主要致力於雲端詐欺檢測服務，並積極與金融單位合作。經由開發「詐欺警報」(Fraud Alert)等不正當存取之檢測服務，協助金融機構防範網路釣魚、帳戶盜用及洗錢風險，其提供之即時風險驗證與惡意行為偵測系統，已有部分金融機構導入，並協助降低詐騙風險，Caulis 的 eKYC 服務，結合電力公司資訊確認與金融服務申請之用戶居住地址是否相符，降低不正常的帳戶開設等詐騙風險。

叁、心得及建議

經由本次參訪日本監管機關（日本金融廳、日本銀行）、科技產業(IBM、AWS)與金融新創產業(FINOLAB)，及首場臺日代表之金融交流分享會，茲列出相關心得及建議如下：

一、台灣的金融資安遵循，主要由主管機關規定並公告程序後，由金融機構依據相關要求執行，強調法令法規之遵循與合規性。日本方面與臺灣相比，強制性的規範相對較少，於交流活動中日本講者分享，日本的金融機構自發性較高，多數組織已將資安合規遵循內化為員工之 DNA，培養組織之資安意識。

二、在量子電腦的發展下，未來經由相關技術，突破現有的加密演算法已非難事，企業對於資訊安全議題，除了關注現有技術，亦應注意新興科技所可能帶來之威脅，日本政府及日本相關企業，已著手合作推動後量子加密（PQC）轉型，面對相關技術變革，需要政府政策支援和產業協同合作彼此相輔相成。除了資安部門外，亦涉及企業高層、系統及法令遵循等部門之通力合作。

三、日本金融業近年積極擁抱新科技並規劃上雲，依據報導指出，日本最大的金融機構「三菱日聯金融集團」(MUFG)於 2017 年將該集團內部的資訊系統移至雲端，為日本第一家導入公有雲的銀行，並估計在五年內節省約 100 億日圓的成本，大型銀行將系統上雲，有助於確保持續營運、降低營運成本並提升營運韌性。臺灣部分金融同業目前亦有已將系統上雲者，可參考日本之推動作法，同時對於下雲的 Plan B 方案，亦應於事前完成規劃準備。

四、日本金融監理機構提到，在鼓勵企業創新與金融穩定之間，應取得平衡，並強化產學合作，以推動金融科技穩定發展。此外，日本相關的資安演練均已制度化，由政府、主管機關協同金融機構及資訊公司進行測試作業，辦理 Delta Wall 等演習作業，達到公助、自助、共助三贏。

五、日本 FINOLAB 在金融科技產品的產出讓人眼睛為之一亮，如透過與電力公司合作，經由電表數據等資訊，判斷客戶是否實際居住登記地址，或房屋處於空置狀態，並與客戶於銀行開戶資訊進行相互比較，除了能有效識別可疑地點，亦能比對兩者資訊是否相符，是否有假帳戶申請之情形，成為防範詐騙、阻止人頭開立帳戶參考之創新應用。

六、如同交流過程中與會者所分享，在很多金融業務面向上，金融業間彼此是競爭的，只有於資安面向上，彼此是合作的關係，金融機構除了建構自身防禦機制外，也應與政府、協力廠商及金融同業密切合作，聯合作戰勝過於單打獨鬥，透過彼此建立聯防、情資共享等機制，以共同面對外界資安風險。

此次參訪活動中，除了聆聽日方講者經驗分享外，活動時間外（如交通過程或用餐時間），能與來自臺灣其他銀行、證券、壽險等業界之金融機構，及財金資訊等金融周邊機構的團員們交流互動，分享各自機構在資安管理上之經驗，經由無論是資訊安全技術面或管理面的交流，學習了其他金融單位相關資安措施值得借鏡處，有助於形成彼此「共好」的資安防線，從交流學習中獲益良多。