守護日常-資安成長故事

黃鴻運 / 金融聯合徵信中心 資安部

在聯徵中心走過50年的歷程中，資訊安全始終是守護中心穩健前行的重要力量，從單點防護到全面治理，從被動因應到主動監控，資安部在這十年間持續深化防護架構、優化流程設計，確保營運的每一環都建立在安全、穩定的基礎上。本篇文章分享資安部的四個組別近十年的的努力與進展，呈現我們如何在看不見的戰場上，默默守護著聯徵中心與同仁的每一天。

資訊安全組

一、資安防護機制導入

(1) 導入DLP (Data Loss Prevention)：有效防止機密資料透過上網行為外洩個資，系統具備即時內容分析與行為識別能力，能偵測使用者是否有嘗試將關鍵資料輸出至未授權網站或第三方平台，並可依政策自動封鎖或通報，防範非預期的外洩風險。

(2)導入CDR（Content Disarm and Reconstruction）：可在不影響檔案使用的情況下，移除潛藏於文件、圖檔、PDF等檔案內的惡意程式與威脅，避免攻擊透過檔案進入內網。搭配多模組防毒掃描引擎，能同時使用數種防毒引擎進行比對，大幅提升惡意程式偵測率。

(3)導入EDR（Endpoint Detection and Response）端點偵測與回應：即時監控並分析用戶端設備的行為，偵測潛在威脅如惡意程式、異常存取或橫向移動行為。其具備威脅獵捕、自動化回應與事件溯源功能，能在資安事件發生初期快速定位並阻斷攻擊路徑，降低損害範圍。適用於企業端點裝置（如筆電、伺服器、VDI 環境），能有效補強傳統防毒不足之處，提供持續性監控與高效應變能力，提升整體資安防護深度。

(4) 導入Remote Browser Isolation（RBI）遠端瀏覽器隔離：透過在隔離環境中執行所有網頁內容，將潛在的惡意代碼與使用者端完全隔離，避免任何網頁木馬、惡意JavaScript 或零時差漏洞直接影響本機設備。RBI 特別適用於防範來自未知網站、電子郵件連結或雲端應用的網路威脅，不需端點安裝代理程式，即可提供無縫使用體驗與高強度防護，有效提升瀏覽安全性並降低社交工程攻擊風險。

二、情資與資安監控

為強化聯徵中心整體資訊安全防護能量，建立一套具備即時監控、事件通報與應變能力的完整防禦架構，我們同時採行委外 SOC（Security Operations Center）服務與自建資安戰情室並行運作策略，透過委外 SOC，得以 24x7 不間斷監控外部攻擊跡象與內部異常行為，結合自建戰情室進行關鍵事件研判與內部應變，確保資安事件可即時回應並有效控管。

此外，聯徵中心積極導入威脅情資收集機制，定期取得 F-ISAC與FS-ISAC 等資安聯防平台的最新攻擊指標與情資快報，強化預警能力，讓防禦策略能隨全球威脅趨勢持續調整，針對內部系統與裝置，我們也建立完整的弱點掃描與管控流程，搭配風險評估優先級，持續進行修補與控管，有效降低潛在入侵風險。

在資安分析面，聯徵中心參考 MITRE ATT&CK 框架，建立攻擊行為的映射模型，強化事件溯源、攻擊路徑判斷與持續監控機制，確保對攻擊鏈的每個階段皆有偵測與防禦能力。透過上述多元措施，展現本單位對資訊安全的重視，並持續提升監控即應變能力，以因應不斷演化的資安挑戰。

三、導入ISO27001及TPIPAS

已正式導入並通過 ISO/IEC 27001 資訊安全管理系統認證，建立系統化的資安政策、風險評估與控制流程，有效提升組織整體資安治理能力，透過持續性的風險辨識、內部稽核與管理審查，確保資訊資產於機密性、完整性與可用性上皆受到妥善保護。

另外為符合個資保護與資訊安全要求，亦導入臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, TPIPAS）強化對個人資料保護的管理，透過雙軌並行的標準建置與落實，聯徵中心在制度、技術與組織層面全面提升資安防護水準，展現對個資保護與資訊安全持續精進與重視的決心。

四、資安紅隊演練

聯徵中心於106年、108年、111年及113年執行資安紅隊演練，透過模擬真實駭客攻擊手法，驗證聯徵中心資訊系統、資安防護機制及應變流程的完整性與有效性。紅隊演練不僅涵蓋弱點利用、橫向滲透與權限提升等攻擊技術，更進一步測試藍隊在偵測、通報、分析及阻斷威脅的應變能力，演練過程中，亦能針對防禦盲點與實務操作流程進行弱點揭露與強化建議，促進資安治理持續精進。藉由定期辦理紅隊演練，聯徵中心得以從攻防雙面觀點審視資安防護效能，有效提升整體防禦深度與事件應變速度，進一步強化資安團隊實戰經驗與跨部門協作能力。

五、接軌國際，培養資安人才

為接軌國際資安發展趨勢並拓展全球視野，聯徵中心積極參與國際資安交流活動，於108年組團參訪以色列資安產業，深入了解其在威脅防禦、情資聯防與資安創新應用上的實務經驗；109年派員赴美參加 RSA Conference，掌握全球最新資安技術與攻防趨勢；112年更與金融研訓院共同前往新加坡，參訪當地金融機構資安管理與監理實務，強

化國際金融資安對話與合作；113 年派員參加 ISC2 Conference，與國際資安專業人士交流。透過系統性參訪與持續學習，聯徵中心有效強化資安前瞻性規劃與實務應用能力，展現積極對標國際、提升整體資安能量的決心。

授權管制組

一、建置資料庫活動監控系統（Database Activity Monitoring, DAM）

聯徵中心重視資料庫安全性，為即時掌握資料存取情形並防範異常行為，針對資料庫之存取、異動與查詢進行紀錄與分析。協助資安團隊偵測非預期行為，以達監控並即時處理並通報之效益，降低資料外洩風險。亦同步留存資料庫活動軌跡，以供資安稽核及調查用途。

二、導入特權帳號管理系統（Privileged Access Management, PAM）

為有效管理與控管特權帳號使用風險，防範因帳號濫用或被盜用所造成之重大資安事件，聯徵中心導入特權帳號管理系統，統一管理特權帳號、集中控管存取權限並記錄操作軌跡。任一特權帳號使用，皆必須經過層層權責主管把關審核，於限定期間內、最小化權限與範圍經申請核准後使用。系統導入除可降低特權帳號人工作業錯誤風險，並除去人工作業潛在已知資訊之風險，強化整體資安透明度與問責機制。

三、導入主機組態管理系統

針對聯徵中心內部使用之各項作業系統（如Windows/Linux/AIX），參考國家資通安全研究院之政府組態基準等標準，並訂定聯徵中心內部組態基準，為確保其組態設定值符合聯徵中心期望之資訊安全標準，導入主機組態管理系統，將聯徵中心訂定之組態標準針對各主機進行檢測是否合規，聯徵中心各主機於上線前必須經過組態設定值檢核之程序，方得上線，以上線之主機則定期針對其組態設定值進行檢測，透過此系統可即時發現組態設定值不合規之項目，並即時通知管理單位進行修正，確保系統穩定運作與安全性維持在要求之水準，降低潛在弱點所帶來之風險。

四、導入身分治理系統（Identity Governance and Administration, IGA）

有鑑於人員異動，帳號與權限管理作業複雜且容易產生遺漏或過權問題，及定期帳號權限盤點之確實性，聯徵中心導入身分治理系統，以建構完善帳號權限盤點治理。系統具備帳號權限資訊之即時性與正確性，可有效掌握人員帳號權限，另可於帳號權限盤點作業時易識別權限不當授予之情形，進而達成依權責權限最小化原則，提升帳號權限治理成熟度。

五、使用者營運作業環境存取控制

聯徵中心為強化營運環境存取控制，現行非資訊單位採用IC智慧卡雙因子登入機制，資訊及資安單位限定於具備門禁及監視系統獨立設置之操作室及監控室作業，特權帳號皆回收管制並採申請核准後以雙因子機制登入使用，前述二種作業皆使用精簡型終端設備(Thin Client)，且皆不提供外部連線機制，必須於特定場域作業，以防範外部存取遭駭客潛入之風險。

六、定期盤查與檢視作業

新主機上線前必須經過層層資安把關，如特權帳號回收、帳號清查、組態設定結果檢視作業，除上線檢查外皆具備定期檢查機制，如帳號權限盤點作業，確認作業系統、應用系統、資料庫之帳號權限皆依照職責最小化權限授予，確認組態設定值是否皆依照規定設定。

變更管制組

聯徵中心資通系統與設備之變更管理，由資安部規劃推動與執行；首先，持續依變更管理政策需求開發調整變更管理之電子表單，以電子表單之變更作業簽核流程，確立申請、執行、覆核等階段之檢核重點與核定層級，並留存變更作業之相關執行紀錄或軌跡；其次，營運區變更作業持續要求變更程序之執行程序、復原程序、檢核程序內容完整確實，以維護變更作業之正確性；而最高權限及特殊權帳號之變更作業過程，加強以特權帳號管理系統監控與軌跡紀錄留存，以供事後覆核等作業；此外，持續於核心資通系統與第一類電腦系統之系統轉換、架構重大調整或跨版本升級等變更作業前，召開上線協調會議，安排工作項目並檢視相關檢核表，以確保各項準備到位，另持續檢討變更作業以降低變更可能造成之風險，包含減少例行性派工作業、降低緊急變更作業比率、降低程序未完備變更作業比率、核心系統主機變更作業制訂系統日常變更作業選單，逐步將系統參數調整及新增作業目錄等程序改以選單作業等。

聯徵中心營運區與OA區之資料檔案輸出入管理，由資安部規劃建置維運輸出入管理系統，以及持續依輸出入管理政策需求開發新增功能；首先，OA區輸入與營運區輸出有各區獨立之電子表單，以電子表單之作業簽核流程，確立申請、執行、覆核等階段之檢核重點與核定層級；此外，OA區資料檔案輸入須以API連接資安檢測系統掃描資料檔案，檢測無病毒無異常，經主管審核檢視後才可放行輸入至營運區，營運區資料檔案輸出須經輸出入系統之個資掃描功能予以檢測並產出報表，經主管審核檢視後才可放行輸出；另輸出入系統提供非人工作業之排程自動化傳輸機制；另屬特定需求需輸出至外部單位，有設置白名單管控之專屬傳送機制；而所有資料檔案輸出入相關作業皆留存軌跡紀錄備查。

資料檔案以媒體(例如光碟或USB行動碟)之方式提供，進入聯徵中心內部前皆加強須經媒體資安檢測作業以降低感染惡意程式之機率，媒體經資安檢測系統掃描資料檔案，檢測無病毒無異常，才可將資料檔案放行進入聯徵中心內部進行後續作業。

聯徵中心營運區為獨立網路與辦公區網路有實體隔離，並嚴格限制對營運區網路進行連線，聯徵中心持續落實營運區終端機操作室、資料管制室作業環境區域之門禁權限管控、設備攜出入管控及作業用設備管控措施，並持續更新維護管控措施所需之軟體、硬體與環境；門禁權限管控，人員進出門禁權限須經申請奉核後以最小需求原則授予，未具門禁權

限之人員進入，需由已授權人員全程陪同，資安部每月覆核人員進出記錄，每季檢視門禁權限以確保人員門禁授權之合適性，另門禁出入口有攝影設備(CCTV)，監錄人員進出情形並留存備查；設備攜出入管控，不得攜帶任何具備輸出、輸入或儲存之設備(例如手機、筆記型電腦)進出作業環境區域，如需攜帶前述設備進出，依資訊設備管理作業規範，須經申請奉核後才可辦理；作業用設備管控，於營運區終端機操作室作業須使用精簡型終端設備(ThinClient)，精簡型終端設備限制無法使用USB介面之儲存設備，且側錄人員操作畫面並留存備查。

測試組

聯徵中心為落實資訊安全相關法規，成立專責測試組進行法規規定之相關測試作業，包括功能測試、整合測試、壓力測試、滲透測試等，並於107年將測試組由資訊部移至資安部，以達成開發與測試在不同部門之牽制機制。測試組過去十年相關精進作為如下：

一、擴充測試資料庫內測試資料之深度及廣度

聯徵中心重視資料庫安全性，以提供會員不同情境之測試資料，除了提供會員平日各項查詢所需測試資料外，並提供新成立之3家純網銀開業前之各種功能測試及壓力測試所需之測試資料。

二、導入測試資料使用合成之虛擬資料

由研究部、資訊部、資安部、徵信部等跨部門成立之專案，使用統計軟體產製與真實資料相似之合成資料供不同需求之測試所需。此合成資料不但符合檢核邏輯，並且與真實資料一樣符合跨資料之邏輯檢查，例如授信資料、額度資料、各類擔保品等相關資料之間的邏輯關聯性。此合成資料亦與真實資料一樣有比例分配之設計，期許此合成資料庫能與真實資料極度相似，且可依需要製作大量及多年度之合成資料。

三、導入自動化測試工具

■API類測試工具：

最近10年來，聯徵中心有越來越多使用API 之應用系統，不論是內部系統互相呼叫、還是介接外部機構，亦或是提供會員之各項查詢服務，皆會使用API之機制。測試組於109年開始使用API測試工具軟體進行相關API類之測試作業。

■GUI類測試工具：

此工具係對GUI類應用系統錄製測試情境，並檢視測試結果是否與預期結果相符。

■壓力測試工具：

此工具係業界使用相關廣泛之壓力測試軟體，可對中心提供會員之查詢服務，或API類應用系統進行壓力測試(Load Test)及持續性測試(Persistent Test)。因資通安全法等相關法規規定，對外服務之新系統上線前，或是對外服務之原系統升級，皆需進行壓力測試，此壓力測試軟體提供可客製化之壓力測試功能，可視需要進行壓測scripts之客製化，以達成需特殊處理之應用系統壓力測試。