2023資產管理金融新知暨法遵系列研討會

「金融資安精進措施與零信任戰略」活動實錄

金管會 林裕泰處長

證基會 林丙輝董事長

國際資訊安全人才培育與推廣協會
毛敬豪 理事長

金融科技的蓬勃發展促使數位金融服務的持續創新與開放，包含純網銀的設置、開放銀行的推動、金融機構結合第三方服務業者的跨領域產業資料與服務整合等，提供了完善的客戶體驗，然而，數位時代潮流雖帶來多元及便利的金融服務，卻也導致資通安全的威脅日益嚴峻，惡意使用與攻擊將破壞民眾的信任並危及國家金融穩定，資訊安全成為各國政府須面對的重要議題。證基會爰規劃辦理本場次研討會，安排主管機關、實務專家和與會者分享與交流。

「金融資安精進措施與零信任戰略」議程

日期：112年3月14日(二) 14:00-17:00

地點：台北花園酒店2樓國際廳(台北市中正區中華路二段一號2樓)

時間	主題	講席
14:00-14:10	主辦單位致詞	林丙輝 董事長 證券暨期貨市場發展基金會
14:10-15:00	專題演講1 「金融資安行動方案」2.0 深度解析	林裕泰 處長 金管會 資訊服務處
15:00-15:10	意見交流	
15:10-15:30	中 場 休 息	
15:30-16:50	專題演講2 金融機構零信任防護戰略實務	毛敬豪 理事長 國際資訊安全人才培育與推廣協會
16:50-17:00	意見交流	

主辦單位首長致詞

證基會 林丙輝 董事長

林董事長表示，近來資訊安全已衍生為國安議題，隨著資訊和網路科技的發展，各種金融服務雖帶來便利性，卻也帶來威脅與問題，使民眾困擾，金管會對此積極因應，提出金融行動方案等措施，以提高金融資安韌性；近年疫情的衝擊及國際情勢動盪影響全球，遠距業務蓬勃發展及網路科技加速進步，使得資安問題益顯重要。

有鑑於此，金管會於111年12月27日發布「金融資安行動方案2.0」，期以完備金融資安制度及監理，持續提升金融機構資安防護能量，協助業者及上市公司因應面對，以提供民眾更安心、多樣化且不中斷的金融服務，確保財產資訊及隱私，打造更完善的金融生態圈。

個資的外洩是資安漏洞的源頭，使有企圖人士得以利用並侵入系統從事獲利、犯罪之活動；社交工程也成為詐騙管道，防不勝防。今日的研討會很榮幸邀請到金管會林處長對「金融資安行動方案2.0」詳加說明，並由實務專家毛理事長針對金融機構的零信任戰略實務進行解析，與各位分享經驗與交流。

專題演講1:
「金融資安行動方案」2.0深度解析

金管會資訊服務處　林裕泰 處長

資安問題層出不窮，從事資安的人員著實不易，需時常面對外界的質疑及挑戰，林處長主要針對「金融資安行動方案2.0」的緣由和重點方向進行說明。

首先回顧1.0推動的架構及結果，從原先的KPI進行檢視及檢討，主要成果分為以下部分：

一. 強化資安監理：包含「資安長的設置」、「鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組」，可減少許多內部溝通成本，提供較大的支持，以及「辦理董監事資安教育訓練課程」和「增修訂11項金融資安自律規範或指引」。

二. 資安治理：鼓勵設置資安監控中心，目前仍持續規劃其他項目以獲得成果。

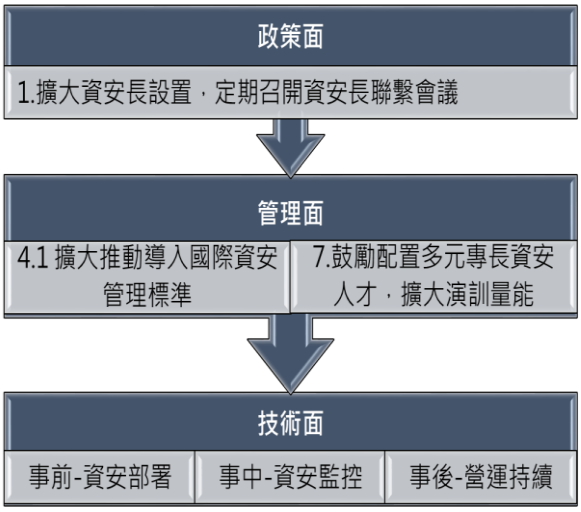
三. 金融韌性：導入資安管理標準，期望金融資安的演練更加確實。尤其著重資安演練，定期與國際合作辦理攻防演練與教育訓練，目前許多金融機構積極參與。

四. 資安聯防：加入F-ISAC以分享情資，從單向到多向，使蒐集到的情資也更為及時有效；此外推動金融機構參加資安監控聯防(F-SOC)，以掌握金融領域資安威脅現況及趨勢。

資安監控的部分目前也發展出共同基準，目的包含有：一、希望機制透明及有效化；二、資訊傳遞有標準可循。從1.0到2.0政策進行滾動檢討時會先做資料蒐集，面對網路攻防日趨易攻難守，因應重大數位災害的數位韌性如今也越漸重視，考驗著金融服務系統如何有效存活。而疫情的爆發造成工作型態轉變，使得災防隨之延伸範圍；此外，數位轉型促使的同、異業合作，更是存在更多資安風險，是以透過這兩年彙整的資安監理重點，可放在第三方、數位韌性、零信任和演練實證等部分。

2.0政策所做的改變措施，其方向在於「擴大適用」、「落實深化」和「鼓勵前瞻性思維」，共有九項精進重點，含括技術面、管理面及政策面(如圖一)，以達深化、有效和聯防等目的(表一)，並加強eKYC業務風險對照、第三方風險評估管理與因應新型態資安攻擊等部分。

	推動措施	擴大適用	落實深化	鼓勵前瞻
1	擴大資安長設置，定期召開資安長聯繫會議	V	V	◎
2	因應數位轉型及及網路服務開放，增修訂自律規範		V	
3	深化核心資料保全及營運持續演練		V	V
4	擴大導入國際資安管理標準及建置資安監控機制	V	V	
5	鼓勵資安監控與防護之有效性評估		V	V
6	鼓勵零信任網路部署，強化連線驗證與授權管控			V
7	鼓勵配置多元專長資安人才，擴大攻防演訓量能		V	V
8	提升資安情資分享動能，增進資安聯防運作效能		V	
9	辦理資安攻防演練，規劃重大資安事件支援演訓		V	



圖一 金融資安行動方案2.0金融資安行動方案 2.0改變措施與重點

表一 金融資安行動方案 2.0實施目的

項目	目的
一. 擴大資安長設置	• 一定規模 • 電子交易達一定比例
二. 因應數位轉型及網路服務開放，增修訂自律規範	• 客戶-eKYC與業務風險對照 (以ISO29115為對照標準） • 第三方服務-風險評估與管理 • 居家/異地辦公-因應新型態資安攻擊
三. 深化核心資料保全及營運持續演練	建立平時及終極防護能量
四. 擴大國際資安管理標準驗證和資安監控機制	• 一定規模 • 電子交易達一定比例
五. 鼓勵資安監控與防護有效性	針對所對應到的攻擊技術，研析其特徵與手法，產出相對應之監控平台（SIEM）
六. 鼓勵零信任網路部署	推動政府機關導入零信任網路服務，完善政府網際服務網防禦之深廣度
七. 配置多元專長資安人才	擴大攻防演練量能
八. 提升資安情資分享動能	增進資安聯防運作效能
九. 辦理資安攻防演練	增加跨機構人力與技術資源

從共通基準邁向策略目標，須透過金管會與金融機構合作，持續建立共識、擬定基準與績效指標，進行推動、檢討與精進，推動作法也會依據1.0政策作差異化管理。

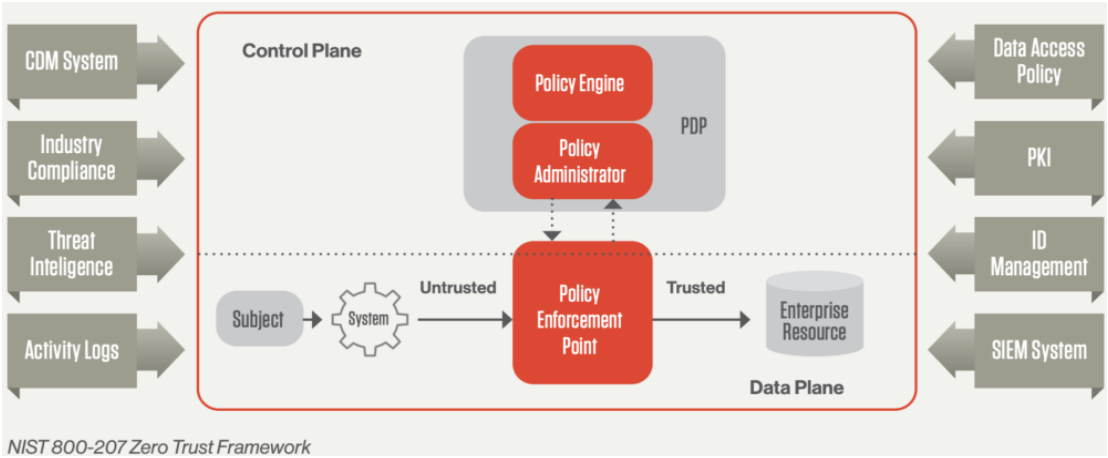
專題演講 2：
金融機構零信任防護戰略實務

國際資訊安全人才培育與推廣協會　毛敬豪 理事長

毛理事長首先提及國家網路安全卓越中心所公布的白皮書 - NIST SP 1800-35，其分為A-E五冊： A 提供資安部門主管所讀； B 部分為架構論述； C 針對技術做說明； D 為如何驗證、評估； E 為維運處理。

零信任發展受到各國政府高度重視，這是累積過去慘痛教訓後集大成的成果。美國國家標準暨技術研究院(NIST)在2020年推出SP 800-207零信任標準後，美國國防部接著在2021年提出零信任參考架構，白宮更於5月發布行政命令，展現對零信任的重視，同時帶動企業採納零信任這套被視為最能抵禦網路威脅的架構，台灣政府目前也著手推動中。零信任是沒有邊際的，希望所有使用者

能在組織外的網路都能受到授權認證，而推動這件事包含了上雲端的問題。整個零信任800的框架核心就是做決定、是否有權限去接觸公司資源，分為兩步驟：一為大腦決策，二為主控（如圖一）。



圖一　零信任核心框架示意圖

「金融資安行動方案2.0」有三大方向：擴大資安長設置、因應數位轉型增修訂自律規範、鼓勵金融業擁抱零信任。金融業導入零信任網路有三大核心機制，包括身份鑑別、設備鑑別和信任推斷，也得搭配網路與資源的細化權限管控機制。

為何有零信任，源自於供應鏈的資安問題越來越嚴重，尤其以勒索病毒為最大挑戰，這在歐洲網路局(ENISA)中有詳細報告，而「閻羅王勒索病毒」為目前最麻煩者。勒索病毒之組織有不同集團，最初為個體戶，後來變成組織駭客，再來是平台化，接著甚至產生資料仲介。

勒索病毒執行四件事（LEDS）：「封鎖」、「加密」、「刪掉」並「竊取資料」，而最常見的是加密和刪除，至於哪些資產最容易被封鎖就是風險評估的重點。勒索病毒有其步驟性，分別為：「執行」、「動作」、「發勒索信」，最後「溝通」，黃金時刻即在「執行」步驟，卻也是最困難的部分。

資安上很大的改變是由眾生防禦轉為零信任階段，面對勒索病毒的攻擊，須透過不斷演練以減緩問題，現今紫隊（紅+藍攻防）演練之防護對台灣頗為重要。

供應鏈(Supply Chain)的問題在於系統供應商；供應鏈的資安問題被重視始於2018年台積電勒索病毒事件，有鑑於此，供應商的管理評估有幾種方式：一為out & in 從外部評估；二為in & out 問卷、實際監控資料。既有供應鏈資

安的要求、勒索病毒的挑戰，該如何看待零信任？零信任的決策器分為PDP和PEP，前者為思考判斷，後者為執行和落實；有四種配置模式（如圖二），目前最常見的為前兩種。而做決策需要「存取請求」、「主體資料庫與歷史」、「資產資料庫」和「威脅情資與日誌」等五種資訊，以作為支持「信任演算法」之關鍵。

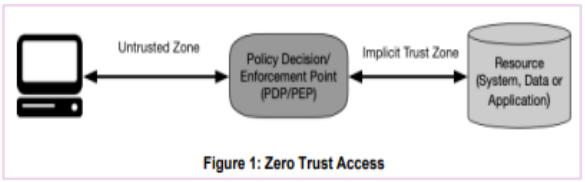


Figure 1: Zero Trust Access

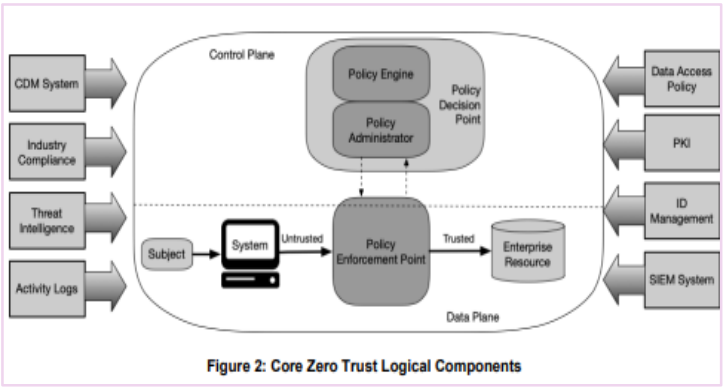


Figure 2: Core Zero Trust Logical Components

圖二　零信任決策之配置模式

我國零信任推動架構分為三階段-「身分鑑別」(對的人)、「設備鑑別」(對的設備)及是否有完整的「信任推斷」機制，目前我國資安廠商較著重在「身分鑑別」這部分，毛理事長接著對SP 1800-35 B 之適用對象、方法、架構、資安特性等進行說明。

企業會遇到的大挑戰包含：目前沒有合適的防火牆機制、缺少合適的角色定義(組織內、管理層次、跨組織)、IT部門缺乏穩定度和可靠性(如何因應複雜的IT環境)、可適性、被各種攻擊包圍、缺少互相交換共通機制的共識、如何善用現在已投資的設備及資源、如何整合不同的商用解決方案、使用者的擔憂、是否有範本、缺少共通語言、成熟度、非大企業所專屬以及沒有完全的解決方法。若遵從SP 1800-35，其益處在於使用者可以安全接觸資源、保護營運資產、對內賊有嚇阻效果、降低資料外洩風險、改善可視度和落實風險評估，也能幫助評估現有資源之優劣勢。

勒索病毒雖討厭卻也創造合作目標，毛理事長建議大家可詳讀並參考SP 1800-35以達到目標。