InFoSec Taiwan 2026：07/07-07/08

密碼不夠用了：深偽時代的企業內控新挑戰

PRESENTER：DEREK LIN 林煒傑

講師介紹

現　任

- 財金公司 內部稽核
- 電腦稽核協會 專業發展委員會 委員

曾　任

- 上市櫃科技製造業 內部稽核
- 零售貿易業 內部稽核

專業認證

CIA Certified Internal Auditor

CISA

CISM

專長領域

內部稽核、電腦稽核、電腦稽核工具軟體應用(ACL、Arbutus等)、數據分析、作業流程優化、風險管理

議程

數位信任危機

「量子運算」與「生成式 AI 深偽」正同時攻擊兩根核心信任支柱

量子威脅：Q-Day 時程與 NIST PQC 標準

Shor’s algorithm的威脅及 FIPS 203/204/205 標準

深偽社交工程的新型操作風險

五大威脅路徑與真實詐騙案例

前沿防禦技術

重建數位信任的防禦技術

密碼敏捷性、COSO 內控升級與五年轉型藍圖

從治理框架到行動計畫的完整指引

第一章：數位信任危機

數位世界的兩大信任支柱

數學信任：非對稱密碼學

RSA、ECC 等演算法猶如網路上看不見的「超級防盜鎖」，保護金鑰交換與傳輸安全。TLS 協定、數位憑證、程式碼簽章，每一筆安全交易背後都依賴這層數學防護。

人際信任：生物辨識與特徵

我們透過鏡頭辨認 CFO 的臉，聆聽總經理的聲音，用指紋解鎖設備，這是基於人臉、聲音、指紋等生物特徵建立的「眼見為憑」信任，長久以來被視為最直觀且不可偽造的驗證方式。

⚠ 這兩根看似堅不可摧的支柱，正同時被「量子運算」與「生成式 AI 深偽」侵蝕。

第一章：數位信任危機

企業集體面臨的「治理真空」

許多管理者認為 Q-Day 與深偽詐騙是科幻情節，ISACA's global Quantum Computing Pulse Poll 揭示了全球企業的嚴峻防禦現況：

95%

尚無路線圖

組織沒有任何量子運算應對計畫，僅 5% 將其納入核心決策

44%

從未聽過 PQC

受訪者表示從未聽說過 NIST 後量子密碼學標準

55%

意識到 HNDL

專業人士知道「現在攔截，日後解密」威脅，但多數仍未採取行動

30%

不了解量子能力

資安專家坦承不清楚量子計算的實際破密能力

HNDL（現在攔截，日後解密）：駭客今日竊取並封存加密數據，靜待量子電腦成熟後一次性破解，這是一個已在進行中的威脅，而非未來假設。

ISACA, Despite Rising Concerns, 95% of Organizations Lack a Quantum Computing Roadmap, ISACA Finds, ISACA, April 2025

Donnie Carpenter, Preparing for a Quantum Future: Navigating Accelerated Timelines for Secure Encryption, ISACA, May 2026

第二章：量子威脅

Shor's algorithm的降維打擊

傳統電腦：牆壁般的防禦

面對 RSA、ECC 等非對稱金鑰，傳統電腦需要花費**數百萬年**進行質因數分解或離散對數計算，使其成為現行網路安全的基石。

量子電腦：降維打擊

搭載Shor's algorithm的量子電腦，將同樣的計算難度壓縮至對數多項式時間：

$$O((\log N)^3)$$

這無異於給了駭客一把**「萬能密碼鑰匙」**，能在數小時內破譯 TLS 傳輸協定、數位憑證授權、軟體程式碼簽章與區塊鏈智慧合約，讓全球數位基礎設施瞬間淪為明文赤裸狀態。

第二章：量子威脅

Q-Day 時程，驚人地提前了

加州理工學院（CalTech）與 Oratomic 的最新物理實驗，徹底打破了原本預估 2035 年的安逸時程。中性原子陣列三維量子誤差修正技術，將物理位元開銷大幅縮減。

⊗ Google 已將內部認證系統的後量子轉型期限硬性訂在 **2029 年**，企業的準備時間比想像中更短暫。

第二章：量子威脅

NIST 後量子密碼正式標準（2024年8月）

NIST 於 2024 年 8 月 13 日正式頒布第一批後量子密碼標準，為企業提供應對量子時代的防禦技術參考：

標準代號	演算法	數學基礎	取代之傳統演算法	主要應用場景與參數
FIPS 203	ML-KEM	Module-LWE (Learning With Errors)	RSA 金鑰交換、ECDH	TLS 1.3 、VPN、SSH；ML-KEM-768 (預設，強度約AES-192)/ ML-KEM-1024 (高階，強度約AES-256)
FIPS 204	ML-DSA	Module-LWE	RSA 簽章、ECDSA	程式碼簽章、數位憑證、合約簽署；ML-DSA-65 (預設，強度約AES-192))/ ML-DSA-87 (高階，強度約AES-256)
FIPS 205	SLH-DSA	密碼雜湊函數(Hash)	RSA、ECDSA	數位簽章、身分驗證；純依賴雜湊抗碰撞性；無模格(Non-lattice)代數漏洞；無狀態(Stateless)特性，適合資源受限之對象。
FIPS 206 (草案中)	FN-DSA	NTRU 格	RSA、ECDSA	嵌入式韌體簽章、資源受限硬體驗證；金鑰生成慢、驗證快；簽章尺寸較小，但浮點數運算極複雜，故尚在審查中。

第三章：深偽威脅

身分驗證的演進史與當前痛點

知識型 (密碼、PIN碼等)

持有型 (Token、金鑰等)

生物特徵 (指紋、人臉、聲紋等)

最棘手的弱點在於生物特徵的**不可變更性（Immutability）**，密碼被盜可重設，但若你的指紋、人臉或聲紋被複製成深偽，你無法換一雙手或換一張臉。這項限制使生物辨識系統在生成式 AI 時代暴露在極大的操作風險之下。

第三章：深偽威脅

深偽技術擊穿生物辨識的五大威脅路徑

1

欺騙攻擊 Spoofing

利用高擬真深偽影音欺騙人臉或語音辨識系統，模仿細微表情、眨眼頻率與肌膚紋理，輕鬆通過一般安檢。

2

規避技術 Evasion

生成符合合法用戶行為特徵的動態影音流，在監控系統中「隱形」，不觸發任何異常行為警報。

3

範本融合 Template Blending

將多個合法用戶特徵融合成全新「假身分」，欺騙跨平台認證系統如國際海關與多國銀行。

4

資料庫篡改 Storage Manipulation

入侵生物資料庫，直接將用戶原始指紋或人臉範本更換為深偽生成範本，實現長期合法入侵。

5

攻擊平民化 Scale & Accessibility

DeepFaceLab 等開源工具普及後，即使低技術犯罪者也能輕易發動逼真的深偽攻擊，門檻急劇降低。

第三章：深偽威脅

知名全球深偽詐騙案例

香港跨國企業分部詐騙案

損失：2,560 萬美元

攻擊者利用總部 CFO 及多名同事的歷史影音，以 AI 即時渲染合成聲音與人臉，在視訊會議中誘騙分部財務人員進行 15 筆跨國撥款。

⚠ 內控失效：視訊口頭指示等同授權；缺乏獨立雙管道驗證；兩千萬級調撥缺乏強認證。

波蘭 Rafał Brzoska 社交工程案

損失：重大品牌名譽受損，股價與市場信任度受挫

攻擊者複製億萬富豪的音影特徵，在社群媒體大量發布高擬真投資廣告，引誘公眾轉入詐騙帳戶。

⚠ 內控失效：外部品牌防護真空；官方影音未導入加密證書鏈，公眾無法辨別真偽。

巴爾的摩 Eric Eiswert 校長偽造案

損失：校長停職，學校營運嚴重動盪

體育主任利用 AI 語音複製工具合成校長辱罵學生及種族歧視的虛假語音並散播。

⚠ 內控失效：調查部門缺乏數位鑑識能力，僅憑聽覺判斷即啟動懲處；無 AI 工具濫用監管規範。

第四章：前沿防禦技術

重建數位信任的重要技術

既然「眼見為憑的直覺」都已靠不住，企業可參考四項關鍵的新型技術工具重建防線：

FIDO2 WebAuthn；C2PA雙軌鑑識；QRNG；AI驅動自適應驗證

第四章：前沿防禦技術

FIDO2 WebAuthn：讓深偽社交工程直接撞牆

FIDO2 的三大密碼學特徵

- **網域 Origin 強綁定**：瀏覽器自動獲取網域並與金鑰密碼學綁定，網域不匹配直接拒絕，完全阻斷釣魚網站攻擊。
- **本地化生物特徵解鎖**：指紋、人臉驗證 100% 在本地安全晶片完成，生物特徵數據絕不離開設備、不經網路傳輸，從根本杜絕重放攻擊
- **CTAP2 物理持有驗證**：通常要求實體觸碰安全金鑰，遠端 AI 劫持無法介入，即使深偽攻擊成功欺騙人員，遠端攻擊者依然無法完成認證

實際應用場景

登入免密碼：掃QR code或指紋、人臉辨識後，即可登入。

消費秒結帳：啟用Passkeys後，驗證指紋或人臉後即可付款。

行動自然人憑證：金鑰存在手機裡，僅本地驗證，即可通過驗證程序；以及避免實體卡遺失風險。

第四章：前沿防禦技術

C2PA 與雙軌鑑識：揭穿 AI 數位證據的畫皮

C2PA（內容來源和真實性聯盟）將檔案的修改歷史打包為加密的「內容憑證」並進行簽署。然而，單純的 C2PA 有兩大缺陷，企業必須升級至「雙軌鑑識」：

C2PA「不具備」偵測Deepfake(深偽)或判斷內容真偽的功能。

TrueScreen 則內建了多重AI鑑識引擎，會主動掃描檔案，抓出AI生成痕跡與修圖篡改，通常兼容C2PA。

- 雙軌鑑識控制的核心邏輯：C2PA 驗證「歷史」，雙軌鑑識驗證「當下」。兩者互補，才能形成完整的數位證據防護鏈。

QRNG 與 AI 自適應驗證：運作原理與防禦機制

量子隨機數生成器 (QRNG)

利用量子力學固有不可預測性，生成「真正隨機數」，根絕傳統偽隨機數可能被預測的弱點。

- **絕對金鑰安全：**為加密金鑰提供真正隨機來源，防範未來量子電腦暴力破解。
- **強化 MFA 抗量子能力：**確保一次性密碼 (OTP) 等驗證因素在強大算力下仍不可預測。

越早納入QRNG，越能提早防範目前HNDL(現在蒐集、日後解密)，以及未來後量子時代的暴力破解風險。

AI 驅動自適應驗證
AI-driven Adaptive Authentication

透過機器學習與深度學習，即時分析使用者「典型行為模式」（如登入時間、位置、設備、打字節奏）進行風險評估。

- **動態風險攔截：**AI偵測行為模式偏差，即使深偽生物特徵吻合，亦觸發額外驗證。
- **「深偽意識」辨識：**識別人類難已發現的微小異常，有效偵測並減輕深偽攻擊。
- **平衡安全與便利：**高風險時提高門檻，低風險時維持順暢體驗。

杜絕過一道門，後面暢行無阻的單點故障風險，AI自適應驗證是「預設偽造，持續驗證」，並在驗證與體驗之間取得平衡。

第六章：密碼敏捷性

密碼敏捷性(Cryptographic-Agility)

密碼敏捷性(靈活)是指企業在不中斷日常營運、不修改應用程式核心代碼與底層硬體架構的前提下，能夠系統性、自動化、安全地更換或升級任何密碼組件與演算法的能力。這是後量子過渡期對抗HNDL攻擊、維護企業營運不中斷的**最核心能力**。缺乏密碼敏捷性的企業，在Q-Day到來時將面臨大規模系統癱瘓或被迫全面重寫程式的災難性代價。

密碼敏捷性(Cryptographic Agility)成熟度四階段

階梯 1：建立全域加密資產能見度

淘汰手工 Excel 記錄，部署動態掃描工具，精確標示哪些系統、容器、代碼或硬體 HSM 仍在使用易受量子攻擊的 RSA、ECC等非對稱加密技術，自動化生成標準 CBOM。

階梯 2：風險評估與優先級劃分

評估數據的「保密壽命要求」。凡生命週期大於五年、面臨 HNDL 威脅的資產（核心專利、智慧財產權、病患個資），列為第一優先遷移級別。

階梯 3：升級、培訓與非生產環境測試

後量子格密碼公鑰與密文尺寸大於經典密碼(RSA、ECC等)，易引發網路延遲。在測試環境模擬部署 ML-KEM、ML-DSA 憑證，全面測試防火牆與 WAF 等對大憑證的解析相容性。

階梯 4：自動化、集中化、分離策略控制

應用層代碼僅調用抽象介面（如 CryptoService），實際演算法由底層設定檔控制，未來升級只需更改設定檔，無需修改任何程式碼。利用集中式 PKI 平台（如 Keyfactor）統一規範演算法，阻斷私自部署自製、硬編碼等不合規的灰色地帶。

第五章：COSO 內控升級

新一代企業內控與治理體系

技術工具的導入僅為戰術手段。真正的防禦核心，在於將 PQC 與深偽防禦機制，系統性地織入企業的 **COSO 內部控制整合框架**與 **ISO 27001 資訊安全管理體系**之中。

第五章：COSO 內控升級

COSO 五大要素的新興技術升級

① 控制環境

成立「新興技術與密碼防禦委員會」，將 PQC 與深偽風險納入 BCP。全組織灌輸**「預設其偽造，持續驗證」**的零信任稽核文化。

② 風險評估

在 RCM 中新增兩大獨立風險：「量子解密：HNDL導致的長期機密性洩露」及「AI即時深偽導致非授權大額撥款與核心資料篡改」。

③ 控制活動

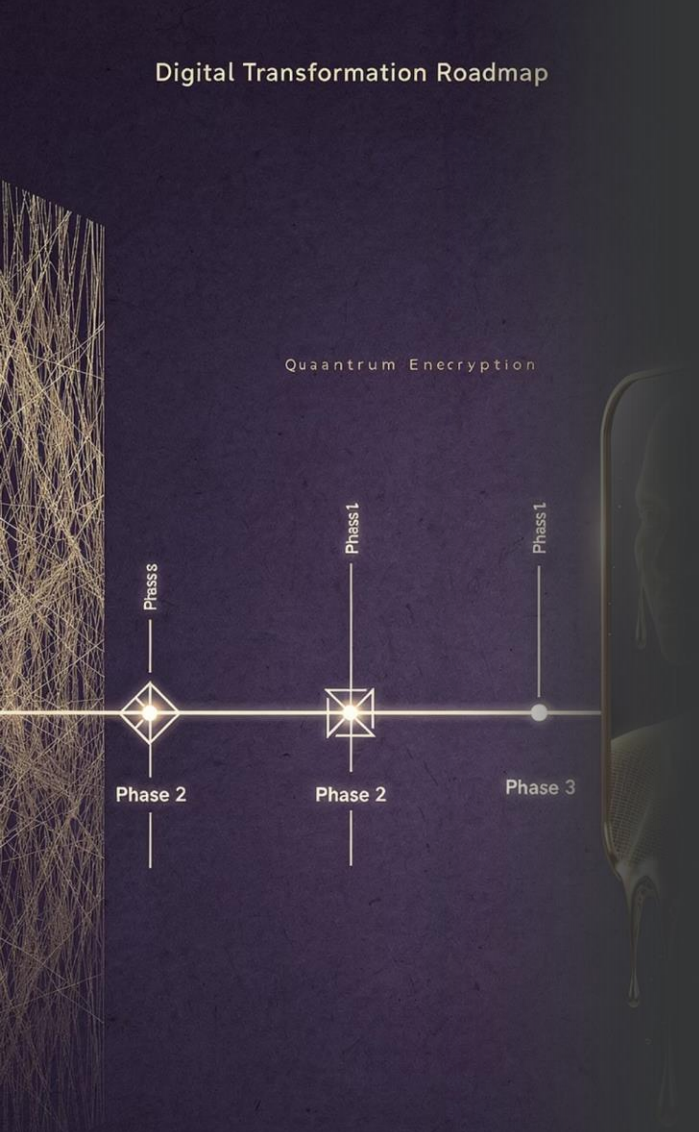
主資料變更強制實施**「雙管道覆核控制」**與「四眼原則」。大額撥付設計多層審核，各節點強制使用抗量子、抗釣魚驗證技術。

④ 資訊與溝通

引入自動化加密資產發現程式，動態維護**密碼材料清單（CBOM）**，讓管理階層與監管機構隨時掌握密碼合規狀態。

⑤ 監督活動

導入自動化 GRC 平台（如 BIC GRC），動態檢視內控強韌度，定期進行深偽社交工程**紅隊演練**與量子壓力測試。



第七章：五年轉型藍圖

企業五年實務轉型行動藍圖

以下四個實施階段，明確定義核心行動與內控對應指標，協助企業將「數位信任網重組」變革平滑落地。每個階段目標環環相扣，形成完整的後量子與深偽防禦縱深。

第一階段

動態防護與清查

現在 — 2026 年底

第二階段

內部憑證與簽章遷移

2026 — 2027 年

第三階段

外部系統轉型與調優

2027 — 2028 年

第四階段

純粹 PQC 與經典退役

2028 — 2030 年

第七章：五年轉型藍圖

第一階段：動態防護與清查（現在 — 2026年底）

核心實作行動

- 啟動全企業加密資產清查，自動產出標準 CBOM
- 網路傳輸強制部署 ML-KEM-768 混合加密模式，防範 HNDL 威脅
- 汰換舊有 MFA，高風險與特權帳戶強制實施 FIDO2 WebAuthn 實體金鑰登入

內控升級指引

- 指派企業 PQC 轉型負責人（Migration Lead），成立跨部門治理小組
- 修訂身分認證控制政策，禁止密碼與簡訊驗證
- 將 FIDO2 物理持有認證列為剛性准入控制點

第七章：五年轉型藍圖

第二階段：內部憑證與簽章遷移（2026 — 2027年）

核心實作行動

- 企業內部 PKI、Active Directory 及 CA 根憑證升級為 ML-DSA-65
- 軟體發布 CI/CD 管線全面部署抗量子程式碼簽章與數位印章
- 部署 GRC 平台，將深偽防禦流程標準化

內控升級指引

- 建立深偽與量子解密專屬風險卡片，自動定量評估財務與名譽風險
- 強制實行大額撥款與供應商帳戶變更的「雙管道覆核」
- 全面落實「四眼原則」審核控制

第七章：五年轉型藍圖

第三階段：外部系統轉型（2027 — 2028年）

🎯 核心實作行動

- 對外部客戶與供應商的 Web 服務、API 憑證遷移至 ML-DSA 演算法
- 聯合 CDN 與 WAF 服務商進行技術調優，解決大憑證封包傳輸引發的網路延遲
- 導入鑑識C2PA雙軌影片溯源機制，防範品牌與主管深偽影音對外擴散

📋 內控升級指引

- 將第三方 API 的後量子與防偽準備度列為供應鏈評估要點
- 企業對外發布之重大業績公告、CEO 發言影音，強制附帶TrueScreen內容憑證
- 由公關與相關部門聯合雙重確認

第七章：五年轉型藍圖

第四階段：純粹 PQC 與經典退役（2028 — 2030年）

核心實作行動

- 廢除過渡期混合部署模式，全面停用並徹底廢除 RSA、ECC 等經典加密演算法
- 整套密碼基礎設施無縫切換至純後量子密碼（Pure PQC）
- 定期利用 GRC 平台自動生成抗量子與抗 AI 欺詐之內控檢視報告

內控升級指引

- 監督活動：透過GRC系統生成對監管機構（金管會、SEC、eIDAS 審計機構）的PQC與AI防禦報告
- 確保營運持續與無瑕疵合規紀錄

第八章：WEF指導原則

世界經濟論壇(WEF)的五大指導原則

這場變革本質上是「數位信任網的系統性重組」，企業可參考世界經濟論壇（WEF）2023年7月發布的五大原則：

制度化組織治理架構

董事會正式將量子威脅與 AI 深偽列為「重大風險」，從治理層級著手，制度化轉型並確保預算配置。

全面深化組織風險感知

防範深偽與認識後量子威脅列為各階層年度必修訓練，秉持「零信任」與「持續專業懷疑」並織入企業文化，持續驗證才能持續信賴。

整合至現行框架，拒絕孤立處理

量子與深偽風險須納入 COSO ERM、ISO 27001 及 BCP 之中，使 PQC 混合部署、CBOM 清查與雙管道覆核成為日常合規測試的剛性指標。

以密碼敏捷性引導未來技術採購

未來採購任何軟硬體、雲端服務、IoT 終端及各項系統，須將「具備密碼敏捷性」、「支援 FIPS 203/204/205」及「支援 FIDO2 WebAuthn」納入考量。

推動供應鏈與生態系協同防禦

量子威脅與深偽詐騙具高傳染性，單一組織無法獨善其身。企業應與客戶、上下游供應商、金融監管及產業安全聯盟共享 PQC 測試經驗與深偽威脅情報，建立端到端防禦生態。

信任的重建，從今天開始

Q-Day 不是科幻小說的情節，Google 已將內部系統的後量子轉型期限訂在 2029 年。深偽詐騙不是遙遠的威脅，香港那 2,560 萬美元已經消失在視訊通話結束後的幾小時之內。

立即開始

啟動 CBOM 清查、部署 FIDO2 驗證標準，今天就能做的事，不要等到 2026 年底。

系統性整合

將 PQC 與深偽防禦織入 COSO 框架，讓內控體系成為防禦的脊梁，而非事後補救。

保持敏捷(靈活)

密碼敏捷性是最重要的能力投資，未來的演算法升級，不該對整個系統有重大調整，而是僅調整底層設定。