數位發展一提升資安防護、強化期貨交易安全

期交所資訊規劃部　鄭凱文

前言

隨著數位化浪潮的推動，我國期貨市場正經歷深刻的變革。交易效率的提升伴隨著日益複雜的資安挑戰，高頻交易、雲端服務和跨境交易的普及，使系統安全性與交易即時性成為營運的重要核心議題。然而，面對駭客攻擊手法不斷創新、勒索軟體、釣魚詐騙生成式AI等日益精進的威脅，傳統資安防護已難以有效應對，且面對全球AI治理框架逐漸成形，金融業者不僅需符合國內外的個人隱私和資安法規，還需保障交易資料與客戶隱私安全，並隨著數位發展不斷提升自身的資安能力。

此外，因應期貨市場全球化發展，對第三方供應商和跨境交易合作夥伴的依賴加劇，使供應鏈風險也隨之增加，雲端安全在這些挑戰中顯得尤為重要，隨著越來越多的交易和數據儲存依賴雲端服務，確保雲端環境的安全性已成為保障整體系統穩定的關鍵，業者應加強對雲端基礎設施的保護，實施加密技術以及嚴格控制存取權限，以有效降低雲端漏洞可能帶來的風險，確保資料的機密性、完整性和可用性。

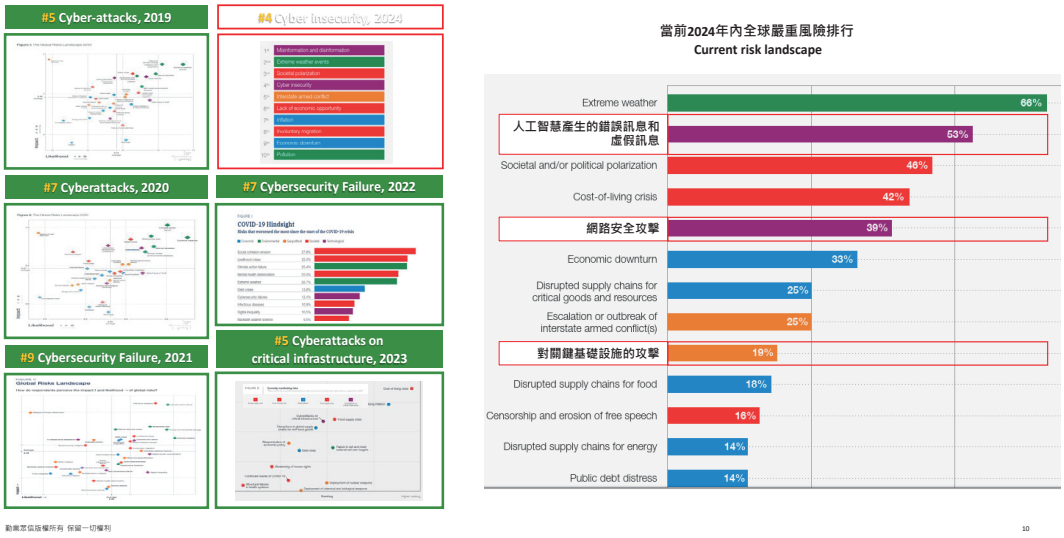
為應對這些新興科技帶來的挑戰，金融業者應建立多層次的資安防護機制，預防潛在威脅，並透過定期的資安演練與系統強化，確保在遭遇攻擊時能迅速回應，維持期貨交易系統的穩定運作，並在數位風險中保持競爭力，為客戶提供安全、穩定的交易服務。

攻擊型態與威脅

依據世界經濟論壇（WEF）全球風險報告，Cybersecurity已連續六年被列為前十大全球風險排行中，Check Point的威脅情報部門Check Point Research數據顯示，113年第三季度全球平均每周網路攻擊次數為1,876次，相較去年同期增加 75%。其中，臺灣的網路攻擊情況尤為嚴重，平均每週遭受4,129次攻擊，位居亞太地區之首。期貨市場因其高頻交易、資金流

動性及價格變動迅速的特性，以及地緣政治因素影響，成為駭客攻擊的主要目標之一，這些攻擊可能造成交易系統中斷、財務損失、數據洩露及聲譽損害。

世界經濟論壇（WEF）全球風險報告，Cybersecurity 連續六年被列為前十大全球風險



資料來源：勤業眾信

以下整理金融業者面臨的資安威脅攻擊型態說明：

1. **新型態DDoS 攻擊**（Distributed Denial of Service）：自疫情至今，隨著全球政治局勢緊張，基於政治動機的DDoS攻擊再度活躍，主要以耗盡網路及系統資源來阻斷服務。根據Microsoft報告顯示，該公司每天平均防禦約1,700次DDoS攻擊，NETSCOUT則統計2023年全球超過1,300萬次攻擊。Cloudflare觀測到，因臺灣大選及地緣政治緊張情勢，對臺DDoS攻擊流量年增3,370%，2024年第1季達450萬次。DDoS出租平台普及推動攻擊增長，2022年增長20%。StormWall指出，2023年受攻擊最嚴重的行業為金融、政府及零售，政府部門受攻擊增加了108%。
2. **釣魚及勒索攻擊**（Phishing & Ransomware）：Google 2024年網路安全預測指出，生成式AI與大型語言模型（LLMs）將使網路釣魚更加精細，透過量身定制的真實假訊息增加欺騙性；另一方面駭客利用動態策略傳播勒索軟體，頻繁變更主機名稱、路徑等，並結合時事元素，傳播方式也從過去的電子郵件附件轉向URL連結和網頁瀏覽，占比已達七成以上。從這些趨勢顯示，網路攻擊手法日益精進，防範措施需隨之提升。
3. **供應鏈攻擊**（Supply Chain Attack）：依Gartner預測，到2025年全球約有45%的組織將因軟體供應鏈遭受攻擊，成長率相較2021年增加約三倍。根據Cybersecurity Ventures的報告，至2031年，全球因這類攻擊導致的組織損失將高達1,380億美元。社交工程與網路釣魚是最常見的入侵方式，其他威脅途徑還包括憑證竊取、入侵開發流

程（CI/CD）、系統漏洞、開源元件的利用、偽冒網域名稱，以及內部人員威脅。這些趨勢強調了組織在軟體供應鏈安全上加強防護的重要性。

4. **資通系統弱點攻擊**：攻擊者持續利用未修補的高風險漏洞發動攻擊，並結合AI技術，提升攻擊精準度與複雜性。例如，駭客組織利用合法工具和修改檔案時間等手法干擾鑑識活動，讓偵測難度大幅提高。同時，AI技術被應用於零時差漏洞利用，使攻擊更加迅速且難以預測。在雲端環境中，錯誤的防火牆設定和弱密碼成為攻擊的突破點，導致金融業者雲端資源被入侵，用於挖礦或發動惡意攻擊。這些趨勢顯示，攻擊模式正變得更加精密且多樣化，金融業者需加強漏洞管理、密碼強度、雲端資安設定，應採用主動式威脅檢測與防禦工具，才能有效應對日益升級的網路威脅。
5. **生成式AI威脅**：因生成式AI的快速發展帶來多項安全威脅，包括攻擊者利用AI開發更精密的網路釣魚、深偽技術製造虛假影像與音頻，以及在選舉中散布虛假資訊干預政治決策。此外，生成式AI對雲端安全與資料隱私構成挑戰，並可能影響社會信任與秩序，為應對這些威脅，各方需採取措施，包括加強AI驅動的威脅偵測技術、制定法律規範、提升公眾辨識虛假資訊的能力，以確保AI的安全與負責任應用。
6. **雲端應用服務威脅**：根據Thales 2023年雲端安全研究報告，組織逐漸採用多雲策略，使用多個雲端服務供應商已成為趨勢，報告顯示2023年有75%的受訪者表示會將機敏資訊放置於雲端，較2021年的49%大幅增加，這些機敏資訊平均約占雲端資料的40%。然而，儘管越來越多機敏資訊存於雲端，只有45%的機敏資料會被加密。人為錯誤被認為是導致雲端資料外洩的主要原因，超過一半的受訪者指出，由於雲端架構的複雜性，使得管理和操作雲端資料變得困難，進而導致資料外洩風險增加。

資料來源：Check Point 2024年5月至10月全球最易遭受攻擊產業表

為應對多樣化的資安威脅，金融業者應盡早建立多層次的資安防護措施，採用高效的DDoS防護監控及告警機制、可識別釣魚及詐騙行為的AI偵測工具、強化供應鏈安全檢查流程，加強資通系統漏洞修補機制並提升內部員工的資安意識，防範內部人員威脅，若使用雲端服務則應加強機敏資料的加密和嚴格的授權控制，持續強化資安架構防範潛在攻擊，維持客戶信任，以確保在面對不斷演變的網路威脅時具備足夠韌性與市場競爭優勢。

資安挑戰

金融市場正面臨日益嚴峻且複雜的資安挑戰。Gartner預測，2025年的資安挑戰將因數位轉型加速、AI和量子技術的快速發展而更加顯著。全球終端使用者的資安支出預計將達2,120億美元（新臺幣約6.77兆元），較2024年1,839億美元（新臺幣約5.88兆元）增長15.1%。隨著金融業者對代理型AI和雲端技術依賴的加深，AI治理平台和監控的重要性將日益突出，以確保這些系統的運行安全及合規性。

此外，量子計算的突破可能使現有的加密技術面臨失效風險，金融業者需提早部署後量子密碼學以保護敏感資料。同時，物聯網設備的快速普及進一步擴大了攻擊面。Check Point預測，到2025年，物聯網裝置的數量將達320億台，大幅增加網路攻擊的可能性。供應鏈攻擊的風險也隨之提升，應要求在邊緣計算和多雲環境中採取嚴格的端點安全措施與資安治理策略，從而有效應對未來的多層次威脅，具體可能遭遇的資安挑戰如下：

1. **數位身分與生物辨識安全**：隨著數位身分驗證和生物辨識技術在期貨交易中的廣泛應用，保護這些敏感數據成為重點。深偽技術的發展使得假冒身分驗證的風險增加，金融業者需採取更先進的多因素驗證、行為分析和生物辨識防偽技術，以確保交易的安全性。
2. **勒索軟體與雙重勒索**：期貨市場因其龐大的數據和資金流而成為勒索軟體的主要攻擊目標。雙重勒索手法加劇金融業者所面臨的風險，攻擊者在加密數據前先竊取數據，並威脅公開這些敏感資訊以威逼機構支付贖金。為應對這一挑戰，應加強資料備份、災難恢復策略，並實施更全面的威脅監控。
3. **量子計算的加密威脅**：隨著量子計算逐步成熟，現有的加密算法面臨破解的風險。量子計算的強大解密能力使得金融業者在數據保護方面面臨潛在危機，應提前引入後量子密碼學來確保其敏感數據的長期安全。
4. **供應鏈攻擊**：金融業者通常依賴第三方供應商提供的技術和服務，供應鏈的資安風險因此成為一大隱患。攻擊者可能利用供應商的系統漏洞進行入侵，影響整個金融體系。為此，需要加強供應商管理和審核，並實施供應鏈安全監控與必要的稽核活動，確保供應廠商符合資安標準。
5. **虛假資訊與市場操縱**：深偽技術和 AI創造虛假資訊的能力可能為期貨市場帶來操縱風險。攻擊者可能發布假消息引發股價波動或引導錯誤投資決策。金融業者需加強對市場資訊的審查，並利用 AI 工具識別虛假資訊，以保護市場和客戶的信任。

6. **雲端安全與多雲管理**：金融業者採用多雲或混合雲架構，也帶來管理和安全上的複雜性，不同雲環境中的數據一致性和存取控制成為一大挑戰，需採用雲端原生的資安技術，並確保不同雲端供應商之間的安全管理協同。
7. **內部威脅管理**：內部的員工或供應鏈可能擁有大量敏感數據的存取權限，內部威脅風險不可忽視。金融業者需要透過加強的存取控制、行為監控和安全培訓，以及導入零信任架構來降低內部威脅風險。

金融業者在面對快速變動的市場中，面對來自網路攻擊、內部威脅、合規壓力和供應鏈風險的多重挑戰，應導入自動化資安系統、零信任架構、異地備份及雲端防護策略，確保交易系統的穩定性和資料的安全性，持續透過強化資安防護機制降低潛在風險，在期貨市場競爭中保持優勢。

人工智慧（AI）

隨著期貨市場數位化的深化與多層次應用，人工智慧（AI）已成為提升資安防護與交易系統效率的關鍵工具。為鼓勵金融業者以負責任創新為核心，應用可信賴的AI技術，發展更貼近民眾需求的金融服務，金融監督管理委員會於113年6月20日發布「金融業運用人工智慧（AI）指引」。該指引旨在推動金融業者善用AI提升服務效率、風險管理與資安防護，並確保消費者權益與市場秩序。指引強調在導入AI時需遵循公平性、隱私保護、系統穩健性與透明性等原則，並建立治理架構監督AI的應用，涵蓋AI系統生命週期管理、第三方合作規範，以及風險控管與流程自動化的優化。

資料來源：BSI 英國標準協會

在資安防護層面，AI可實現多項應用：

1. **威脅偵測與回應**：AI可協助分析用戶與設備行為，識別未經授權存取、異地登入或數據異常流量等異常活動。在偵測到威脅時，啟動隔離程序，遏制威脅擴散，確保系統

的安全性和業務的連續性。

2. **動態存取控制**：基於零信任架構，AI可依風險狀態動態調整存取權限，限制高風險用戶操作，提升存取管理的安全性與靈活性。
3. **身分驗證與管理**：透過行為生物辨識技術，AI可利用打字速度、鼠標軌跡等行為特徵進行無感驗證並偵測假冒嘗試，保護數據安全，同時強化多因子驗證效能。
4. **物聯網與邊緣安全**：因應物聯網設備和邊緣計算的普及，AI能協助驗證設備的合法性，並持續監控設備的行為，防範異常活動。在偵測到可疑設備時啟動隔離程序，阻止攻擊在物聯網環境中蔓延，從而保障邊緣設備和整體網路的安全性。
5. **威脅情報分析與共享**：AI利用威脅情報進行預測性分析，提前識別攻擊向量，促進跨組織情報共享，加速應對新興威脅，提升防禦能力。

透過妥善應用AI，可顯著提升風控與資安能力，包括即時偵測異常行為、預測市場風險及自動化應對攻擊。為有效管理AI帶來的挑戰，建議金融業者採用可解釋的AI模型，定期進行安全測試，並結合零信任架構，全面提升資安水平。隨著AI技術的持續進步，在競爭激烈的市場中保持領先地位。

雲端安全

隨著數位轉型加速，雲端運算在金融領域中的應用日益普及，金融業者藉助雲端架構提升運算效率、降低成本並增強市場彈性。然而，雲端服務的開放性與對外部資源的依賴也帶來了新的資安挑戰。如何在享受雲端便利的同時確保資料安全與合規，已成為金融業者的重要課題，可參考國家資通安全研究院所公布之「政府機關雲端服務應用資安參考指引」[1]。

雲端應用的資安挑戰包括資料洩露與未授權存取風險，因開放架構可能導致敏感資料外洩，而供應商資安薄弱處也容易成為攻擊目標。同時，公有雲、私有雲與本地系統的混合使用需統一資安標準以防止漏洞，為加強雲端安全，金融業者應逐步導入零信任架構，透過多重驗證與條件式控制，確保只有授權用戶能存取雲端資源，並對所有資料進行端對端加密，同時建立異地備份，以確保系統受損時可快速恢復；為保障供應商資安，需定期檢查供應商的資安措施是否符合標準；為了降低金融業者建置或使用雲端服務可能風險，辦理雲端服務採購作業時，可參考行政院公共工程委員會113年5月17日公布之「資訊雲端服務採購契約範本」。

在雲端風險管理方面，金融業者應建立一致的資安標準，統一本地與雲端資源的管理策略，避免平台管理差異帶來的風險，並透過SIEM系統即時監控安全狀態，運用系統自動處理系統找出潛在威脅，提升監控效率；在為了障交易系統在高流量下的穩定性，應部署負載平衡和彈性技術，確保平台穩定運行，同時採用多地區備援策略，確保在災難情境中可迅速切換，保持服務不中斷。

---

[1] 「政府機關雲端服務應用資安參考指引」下載網址：https://s.moda.gov.tw/qT8BKGCx5DoJ

資料來源：數位發展部資通安全署-113年資安署_資安推動重點工作簡報

雲端技術可為金融業者帶來彈性與效率，但同時伴隨資安風險，應思考建立完整雲端資安防護策略，並強化與雲端供應商的合作與稽核，以有效降低風險，確保交易系統在市場波動與網路威脅下穩定運行。

結論

隨著數位轉型深入推進，期貨市場的交易系統和資安防護正面臨日益嚴峻的挑戰。高頻交易、雲端應用和人工智慧等技術的廣泛應用雖提升了業務效率和靈活性，但也引入了更為複雜的網路威脅和合規挑戰。金融業者必須採取多層次的資安策略，以有效應對這些風險。

人工智慧（AI）在資安防護中逐漸成為關鍵力量，協助即時偵測異常交易行為，強化客戶驗證和合規管理，並提升資安透明度與自動化能力。同時，金融業者需在雲端安全方面持續加強傳輸加密、異地備份及零信任架構，以確保雲端資源的安全和合規性。AI自動化技術進一步提升了雲端防護的精準度，有助於防範資料洩露和供應鏈攻擊，並透過與雲端供應商的緊密合作及稽核機制，打造高效的防護體系。

在技術創新與風險管理之間找到平衡，是金融業者在競爭激烈的全球市場中保持優勢的關鍵。唯有如此，才能為客戶提供安全、穩定的交易服務，並持續鞏固市場信任。 CNFA