證券商資通安全查核常見缺失態樣

臺灣證券交易所 券商輔導部

2019年10月25日

TAIWAN
STOCK EXCHANGE

簡報大綱

竭誠為您服務

- 強化市場資安防護能力
- 常見查核缺失態樣
- 其他注意事項

TAIWAN STOCK EXCHANGE

強化市場資安防護能力

竭誠為您服務

- **資安即國安 (2016國家戰略目標)**
- 資通安全管理法已於2019年元旦實施
- 證券期貨業採行之資安防護強化措施：

市場緊急事件應變

- 資安通報系統
- 金融資安資訊分享與分析中心

強化業者體質

- 強化證券期貨業者DDoS防護水準
- 配置資訊專責人力
- 擴大資安查核深度及廣度
- **研提證券期貨業者資通安全防護標準**

設置資訊安全專責單位

- 證券期貨各服務事業應設置資訊安全專責單位及主管，負責資安制度之規劃、監控及執行。
- 針對不同規模設置資訊安全專責單位及主管，以進行差異化管理

分級標準	資安單位暨人力編制
資本額200億以上	應設資安專責單位，資安主管及至少2名資安人員(參照一般銀行)
資本額100億以上，未達200億	資安主管及至少2名資安人員
資本額40億以上，未達100億	資安主管及至少1名資安人員
資本額未達40億	至少1名資安人員

擴大資安查核深度及廣度(1)

竭誠為您服務

持續輔導證券商落實執行「建立證券商資通安全檢查機制」

- 每年由證交所或櫃買中心對證券商進行資安外部稽核
- 參考近期證券業重大資安事件，訂定年度資通安全重要查核項目

擴大資安查核深度及廣度(2)

- 查核作業採差異化分級管理
- 持續輔導，強化業者資安防護能力

分級標準	查核重點
資本額未達40億	建立證券商資通安全檢查機制
資本額40億以上，未達100億	1. 建立證券商資通安全檢查機制 2. 社交工程、網路釣魚、個資去識別化等
資本額100億以上	1. 建立證券商資通安全檢查機制 2. 社交工程、網路釣魚、個資去識別化等 3. 滲透測試、資安健診、資安監控中心等

TAIWAN
STOCK EXCHANGE

簡報大綱

竭誠為您服務

- 強化市場資安防護能力
- 常見查核缺失態樣
- 其他注意事項

缺失態樣類型

- 本(108)年度迄今，由檢查局及證交所、櫃買中心辦理查核所見缺失態樣：

檢查局

- 網路安全管理
- 電腦系統及作業安全管理
- 個資安全防護

證交所、櫃買中心

- 風險評鑑與管理
- 資產分類與控制
- 實體與環境安全
- 通訊與作業管理
- 存取控制
- 系統開發及維護
- 新興科技應用
- 新興科技資訊安全自律規範(券商公會)

檢查局查核缺失態樣(1)

- **網路安全管理**
  - 防火牆設定規則過鬆(特定伺服器對網段進行任意服務)
  - 沒有建內部防火牆
  - 網段位置未妥適:正式網段有測試主機

檢查局查核缺失態樣(2)

• 電腦系統及作業安全管理

- 弱點掃描未依系統重要性規範掃描頻率，建議在一定期間內依重要程度進行掃描
- 中、低風險弱點無評估紀錄
- 弱點修補不確實

檢查局查核缺失態樣(3)

- **個資安全防護**
  - 未建立資料外洩防護機制
  - 未建立上網行為管理機制
  - 未建置電子郵件來信驗證機制

證交所、櫃買中心查核缺失態樣(1)

• 風險評鑑與管理（CC-11000）

- 風險評鑑管理未確定公司各作業可接受之資訊安全風險等級
- 辦理網路下單業務，未依規每年至少辦理資通安全風險評鑑乙次

證交所、櫃買中心查核缺失態樣(2)

• 資產分類與控制 (CC-14000)

- 未訂定有資訊資產分級標示與處理之相關規範
- 資訊資產清冊未就資訊系統訂定資訊分級，區分機密性、敏感性及一般性

證交所、櫃買中心查核缺失態樣(3)

- **實體與環境安全**（CC-16000）
  - 未依程序進行資訊設備報廢

證交所、櫃買中心查核缺失態樣(4)

• 網路安全管理（CC-17010）

- 未定期或適時修補網路運作環境之安全漏洞（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等），並留存相關紀錄
- 未定期評估自身網路系統安全（ 1.未定期檢視防火牆之安全規則，2.未就防火牆系統軟體辦理定期評估更新機制）
- 防火牆進出紀錄及其備份未依規定至少保存三年
- 個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦未安裝防毒軟體並及時更新程式及病毒碼
- 網路下單系統偵測網頁與程式異動、記錄未通知相關人員處理。

證交所、櫃買中心查核缺失態樣(5)

• 電腦系統及作業安全管理 (CC-17020)

- 電腦系統容量評估及壓力測試範圍欠完整
- 證券經紀商之電腦系統未訂定定期(每年至少一次)內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序，或未定期對系統容量進行壓力測試
- 電腦系統或網路未適當區分使用者使用權限

證交所、櫃買中心查核缺失態樣(6)

• 存取控制 (CC-18000)

- 未依個人資料保護法，妥善處理客戶及公司內部人個人資料
- 尚未建立主機交易系統之稽核日誌紀錄，或未設有專人定期檢視
- 未定期審查並檢討久未使用之使用者權限
- 每一使用者未限用唯一代碼
- 資通安全存取控制之密碼管理作業，尚未能全面使用優質密碼設定，或未能定期3個月以內更新相關使用者之密碼
- 電腦或伺服器帳號密碼未妥善保管

證交所、櫃買中心查核缺失態樣(7)

• 存取控制 (CC-18000)

- 檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備，使用預設或簡易之帳號密碼
- 未訂定電腦系統機密性、敏感性之報表列印或瀏覽適當之管制程序
- 重要系統之稽核紀錄未依規留存三年

證交所、櫃買中心查核缺失態樣(8)

• 系統開發及維護（CC-19000）

- 未使用之應用系統功能未照應用程式變更作業(含版本控制)之控管程序辦理下線作業
- 辦理網路下單業務，未確實辦理網路系統弱點掃瞄作業
- 已完成之程式因故需維護時，未依據經過正式核准之程序辦理
- 未訂有因應資訊異常或緊急狀況需異動程式時應遵循之作業相關規範

證交所、櫃買中心查核缺失態樣(9)

• 新興科技應用（CC-21100）

- 未制訂物聯網相關資訊安全規範與管理辦法之規定或建立物聯網設備管理清冊
- 辦理行動應用APP開發及維護作業，未訂有管理規範及標準作業流程
- 未更新物聯網設備之預設密碼
- 未訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法

證交所、櫃買中心查核缺失態樣(10)

- **公會新興科技資訊安全自律規範**
  - 證券商同業未設有防範網路釣魚之機制

TAIWAN
STOCK EXCHANGE

簡報大綱

竭誠為您服務

- 強化市場資安防護能力
- 常見查核缺失態樣
- 其他注意事項

• 電腦作業與資訊提供 (CC-10000)

- 公司應按其電腦作業之方式及資訊處理部門之規範，以本章所列舉之作業項目為最低標準，訂定本身之電腦作業規範，以作為執行內部控制與內部稽核之依據；公司之資訊處理部門受託證券、期貨相關事業子公司之資訊軟、硬體設備及作業管理者，應視資訊作業之安全性、業務之責任劃分及相關資訊人員管理，訂定適切之電腦作業規範。

弱點掃描

• 民眾檢舉證券商官網弱點

- 107年8月至108年7月有熱心民眾使用免費弱點掃描網站或軟體，對共17家證券商官網進行弱點掃描，並將發現的弱點以email方式向主管機關檢舉上開證券商官網有資安風險，建議相關單位進行後續作業以保障民眾權益。

資通安全查核缺失公告

揭誠為您服務

• 證券商資通安全查核缺失公告

- 證券商申報單一窗口系統->證券商公告->交易所公告
- 每年1月1日公告去年查核缺失(證交所查核缺失)
- 自2020年1月1日起適用

落　　幕

謝謝您的聆聽