資通安全查核重點及缺失案例分享

金融監督管理委員會
證券期貨局 黃仲豪組長
2025.2.21

簡報大綱

01 近期重要資安政策

02 資安缺失態樣

03 案例分享

04 近期宣導事項

1 近期資安政策

強化資訊安全管理

設置資安長

- 背景：進一步推動本會「金融資安行動方案」所定「型塑金融機構重視資安的組織文化」措施，提升證券期貨市場各服務事業對資安議題之決策能量，要求各服務事業符合一定條件者，應指派**副總經理以上或職責相當之人兼任資訊安全長**，綜理資訊安全政策推動及資源調度事務。
- 各服務事業若已指派專任資訊安全長有益於所任職務之有效執行，亦未違本項之立法目的。
- 各服務事業之一定條件授權由主管機關另定之。

強化資訊安全管理

設置資安專責單位

- 背景:提升證券期貨各服務事業對資安之重視，明定業者應設置資訊安全專責單位及主管，負責資安相關工作，並針對不同規模、業務及組織特性事業，命令設置資訊安全專責單位及主管，以利進行差異化管理。
- 證券商應依下列分級標準設置

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3名資安人員不得兼辦資訊或其他與職務有利益衝突之業務。
資本額100億以上，未達200億	資訊安全主管及至少3名資訊安全人員。但已設置資訊安全專責單位者，得配置專責主管及2名專責人員。
資本額40億以上，未達100億	資安主管及至少2名資安人員。
資本額未達40億	至少1名資安人員。

強化資訊安全管理

整併資安聲明書納入內控聲明書

各服務事業每年應將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過。

資安主管及人員應持續接受課程訓練

各服務事業負責資訊安全之主管及人員，每年應至少接受十五小時以上資訊安全專業課程訓練或職能訓練。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程（證券暨期貨市場各服務事業內控處理準則§ 36-2）。

強化資訊安全管理

資安通報機制

證券商發生影響客戶權益或正常營運之資訊服務異常事件或資安事件，應依本會「證券期貨市場資通安全事件通報應變作業注意事項」規定於知悉事件 30 分鐘內至「證券期貨市場資通安全通報系統」辦理事件通報，以利主管機關及相關單位有效掌握事件資訊。

資安執行情形納入業務准駁之考量

證券商申請增加業務種類、增加營業項目、設置分支機構及轉投資國內外事業等事項，申請書件應包括資安自評表。

強化資訊安全管理

- 為強化證券商持續營運不中斷，證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。(證交所113.02.25修正)

等級	第一級(A級)證券商(註) (市占率1%以上且自然人客戶數達公司客戶數50%以上)	第二級(B級)證券商 (市占率未達1%或自然人客戶數未達公司客戶數50%以上)	應辦事項完成日
應辦事項	核心系統可容忍中斷時間為1小時	核心系統可容忍中斷時間為2小時	113年7月底

證券商作業委外應注意事項重點

委外內部作業規範應載明事項(董事會核定)

1.作業委外之政策及原則

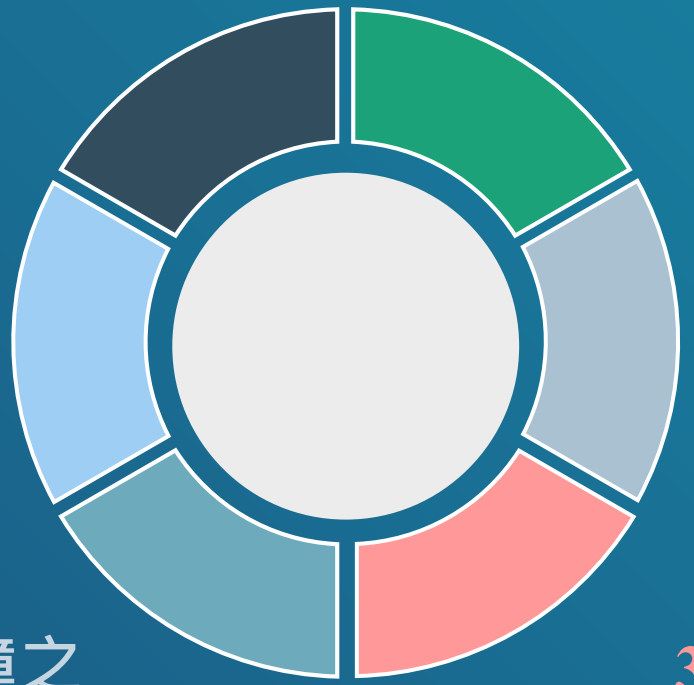
2.專責單位及相關單位對委外事項之權責分工

3.委外事項範圍及委外程序

4.客戶權益保障之作業及程序

5.風險管理原則及程序

6.內部控制原則及程序



資安查核簡介

年度資安例查

- 檢視證券商資安防護辦理情形

選案查核

- 投資人檢舉、資通安全事件、主機共置服務

專案查核

- 特定議題對 證券市場之影響 或 檢視 整體辦理情形

資安查核簡介

資通安全檢查機制

- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技

資安查核作業

14個 資安 控制領域

依嚴重程度扣分

(每年查核約50間)

☑未制定 規範
嚴 重 缺 失（扣 10 分）

☑未依規定 執行
中 等 缺 失（扣 5 分）

☑未留下 操作記錄
輕 微 缺 失（扣 2 分）

追蹤改善

最近3年
150份查核報告
(736項缺失)

資料治理
合併成(65種 缺失態樣)

2 欠失態様分析

3 案例分享

資安事件因應作為-證券商遭駭客撞庫攻擊事件

◆110年11月下旬，3家證券商通報其複委託下單系統遭駭客撞庫攻擊，且有客戶帳戶遭偽冒下單港股(深藍科技)情事。證券商以錯帳處理，投資人權益不受影響。

遭駭券商緊急應變	全面清查	加強客戶APP登入及取得憑證之安控措施	宣導措施	完備資安規範
• 關閉港股電子交易改採人工接單 • 提醒客戶立即變更密碼，封鎖可疑來源IP • 向刑事警察局及法務部調查局報案 • 強化憑證申請機制 • 於公開資訊觀測站及公司官網公告提醒投資人提高警覺	• 函請證券商清查使用下單系統之安全性	• 證券商下單APP登入落實**採多因子認證** • 客戶申請或更新憑證，應增加與登入雙因子之**不同因子驗證機制** • 未落實者，督導證交所要求業者應即修改系統或暫停服務	• 向業者宣導強化資安措施，落實資安內控規範 • 提醒投資人妥善保管投資帳號及密碼	• 督導證交所研修「建立證券商資通安全檢查機制」及「證券商、期貨商電子憑證交付作業要點」有關密碼管理及憑證交付等規定

近期資安重大事件案例

基礎設施服務商異常

事件原因：複委託之上手證券商網路異常，致無法進行交易

影響範圍：造成相關證券商投資人之複委託無法正常下單

處理措施：要求上手證券商強化持續營運作業

近期資安裁罰事件案例

電子下單平台無法登入

事件原因：期貨行情劇烈震盪，大量投資人登入下單平台，
欲確認持有部位，並進行委託，人數達平日之２倍，
造成系統服務異常

影響範圍：查詢帳務資料回應緩慢、投資人登入異常

強化措施：評估整體資源配置（前、中、後台、憑證系統、資料庫）
優化程式效能（放寬可允許連線數、調整資料庫連線機制）
加強故障復原程序 與 壓力測試
提高警戒標準

近期資安裁罰事件案例

委外廠商管理不當

事件原因：證券商對測試系統與正式系統未隔離，並提供廠商高權限帳號及遠端登入功能，廠商於盤中進行系統下單測試。

影響範圍：造成1.4億元鉅額錯帳，回補後虧損113萬

處理措施：落實網段區隔
加強上線管控作業

近期資安裁罰事件案例

未落實資安防護致惡意程式攻擊

事件原因：證券商對外系統遭受攻擊。

影響範圍：部分內網主機遭植入惡意程式。

處理措施：停用多部內部主機上特定高權限帳號
落實網段區隔
加強異常連線監控
弱點程式修補

US financial regulation + Add to myFT

Robinhood to pay biggest fine among more than $100mn imposed by SEC

Broker agrees $45mn settlement as part of data breach while Blackstone and KKR among those penalised by US regulator

The penalties imposed by the SEC stem from a crackdown on Wall Street over use of 'off-channel' messaging systems © Kent Nishimura/Bloomberg

4 近期宣導事項

推動證券商導入零信任架構相關規劃

先行機構導入分享研討會	挑選之導入零信任先行示範單位，將零信任架構導入經驗與其他證券商分享。
參考指引解析說明會	依金管會發布「金融業導入零信任架構參考指引」，對框架概念、導入策略、建議實作參考原則分級進行說明。
零信任系列說明會	根據五大支柱共36個參考原則，分享導入實務及案例，並提供導入零信任架構相關諮詢常見問題及解決方向。

證券期貨市場資通安全事件通報應變作業注意事項

初步通報	應於知悉事件 30 分鐘內進行初步通報。
正式通報	查明事實後，應於24小時內轉為正式通報。
解除通報	事件處理完成後，應於3日內解除通報。

謝謝聆聽