證券商資安查核重點暨案例分享

TAIWAN
STOCK EXCHANGE

大綱

一、資安查核與輔導

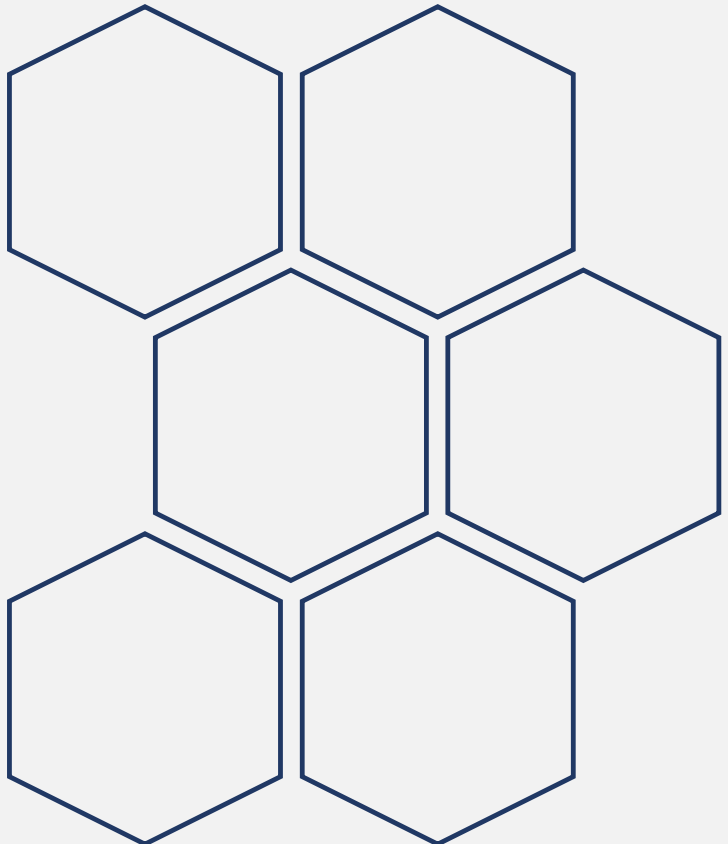
二、資安查核重點

三、常見缺失說明

四、案例說明

五、未來展望

TAIWAN
STOCK EXCHANGE



資安查核與輔導

資安查核與輔導

強化資安

資安法等六子法

金融資安行動方案/資本市場藍圖

證券期貨業者分級及其資安防護標準

協助制定

- 新興科技管控參考指引
- 資通系統安全防護基準參考指引
- 供應鏈風險管理參考指引
- 網路安全防護基準參考指引
- 資訊作業韌性參考指引
- 日誌留存參考指引
- 資安事件應變處理參考指引

協助公會訂定自律規範及參考

- 內部控制制度標準規範 CC-10000~CC-22000
- 建立證券商資通安全檢查機制

修訂法規並輔導業者

- 分級防護應辦事項

已於109年修訂至內控及建立證券商資通安全檢查機制(110、111、112三年實施)

資安查核與輔導

查核	輔導	聯防
檢視法規遵循情形，確保資安防護量能。	研議實務可行性規範，協助業者落實法規要求。	資安事件情資流通，強化資安聯防。


中時新聞網

金管會領證券F4 打造韌性市場

陳柔蓁

2022年8月30日 週二 下午7:03

資料來源：中時新聞網、iThome

資安查核與輔導

- 年度資安查核
  年度例查(約140項查核項目)
- 專案查核
  多因子驗證導入情形，主機共置服務作業
- 選案查核
  投資人檢舉案、主管機關指示事項
- 強化輔導
  前一年度資安異常通報事項、前一年度漏未通報、缺失重複發生

資安查核與輔導

資安缺失暨相關處置

處置	1.注意改善 2.併課違約金5萬元至43萬元不等
依據	(營業細則)第135條第2項、 第138條第2項

資安查核與輔導

缺失重複發生，本公司得依營業細則處置如下

重複次數	一	二	三	四
處置	1.警告 2.併課新臺幣100萬元以下違約金	1.警告 2.併課新臺幣200萬元以下違約金	暫停3個月以下之買賣	暫停買賣
依據	1.第136條 2.第138條第2項	1.第136條 2.第138條第3項(半年內再次發生)	第139條	第142條第1項第5款

TAIWAN
STOCK EXCHANGE

資安查核重點

資安查核重點

風險在哪裡？

外部威脅

- 駭客、天災...→防範未然

內部弱點

- 員工、門禁...→防微杜漸

資安查核重點

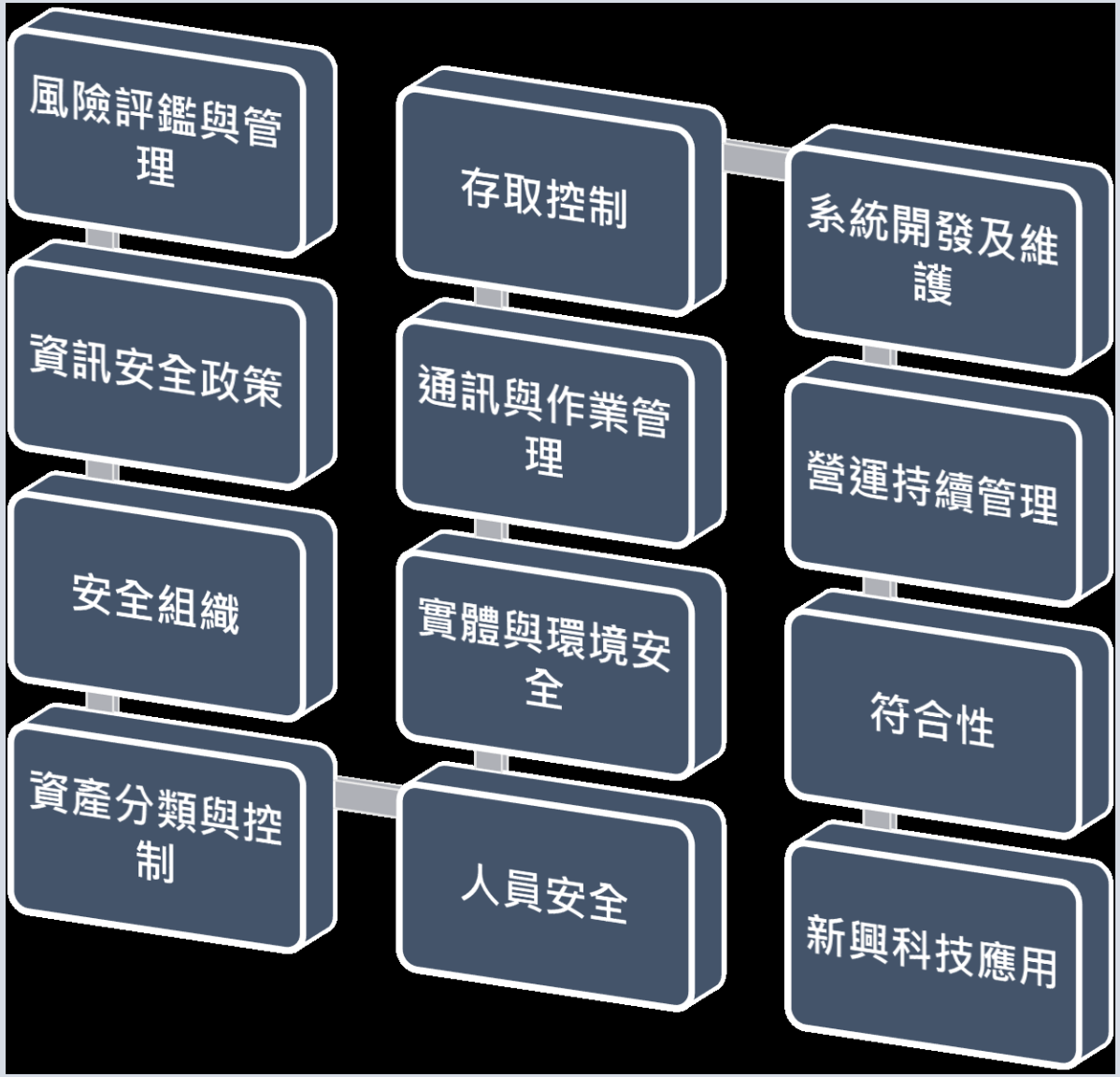

強化登入及憑證下載驗證
主機共置服務
資通安全檢查機制
資安防護彙總
個人資料保護
駭客攻擊防護
金檢年度查核重點

資安查核重點

建立證券商資通安全檢查機制

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



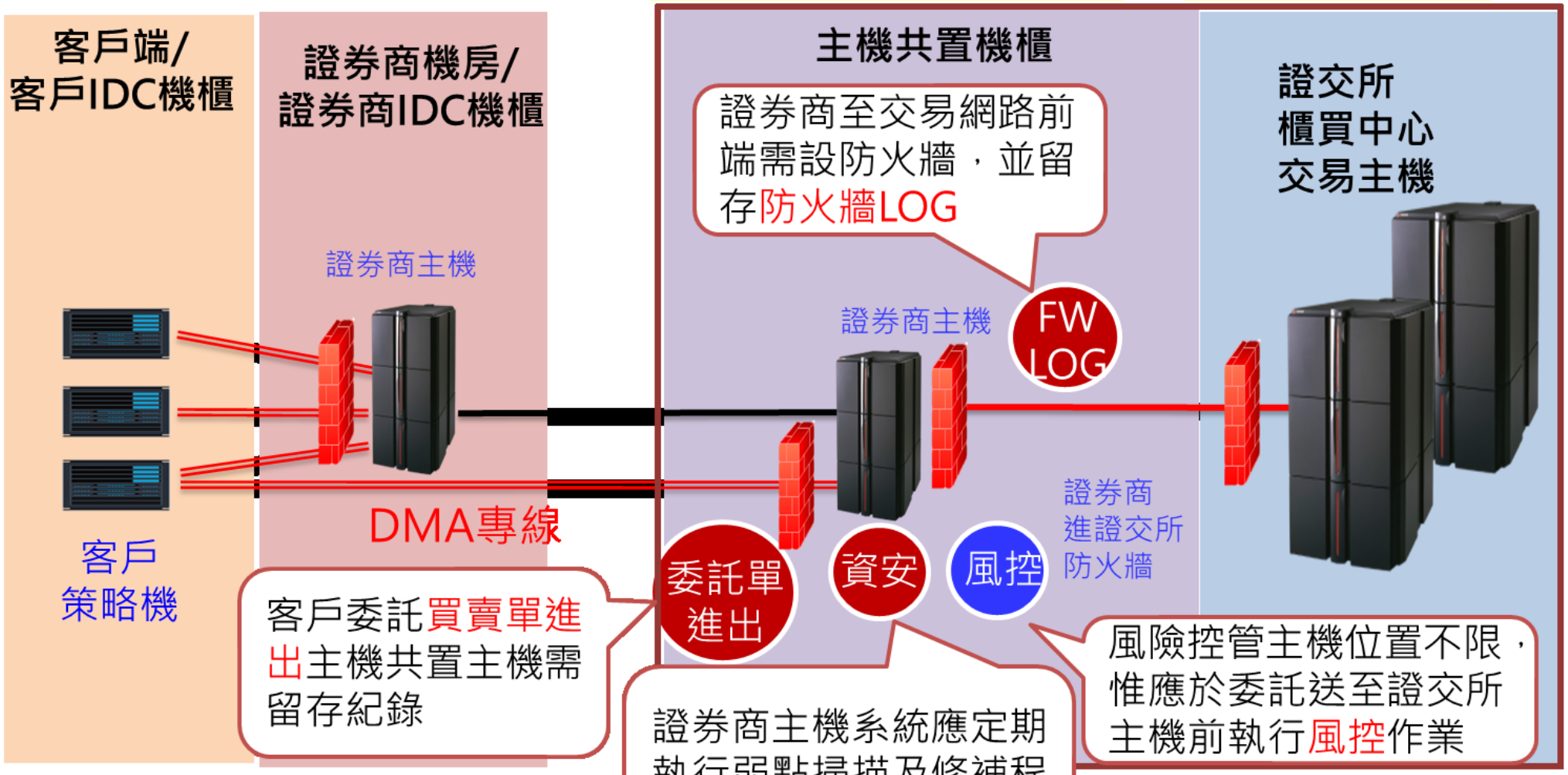
資安查核重點

金融檢查重點	• 檢查局年度查核重點(本國銀行、壽險業)
機敏資料作業	• 端點防護資料外洩
登入及憑證下載	• 網路交易系統驗證完整性
駭客攻擊防護	• 異常活動檢視、資料備份落實情形

資安查核重點

主機共置服務

- 證券商就上述項目，應訂有內稽內控制度並留存稽核軌跡



資安查核重點

查核總結會議

- 資安組織與人力配置
- 網路與系統防護
- 程式變更管理
- 持續營運量能
- 機敏資料防護

常見缺失說明

常見缺失說明

	類別	缺失
1	營運持續	未依主管機關「證券期貨市場資通安全事件通報應變作業注意事項」規定，向主管機關辦理資通安全事件通報。
2	存取控制	未定期審查並檢討久未使用之使用者權限。
3	存取控制	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。
4	網路安全管理	網路下單未採多因子驗證方式。
5	網路安全管理	未定期或適時修補網路運作環境之安全漏洞。

常見缺失說明

1.未落實資安通報
形成資安聯防缺口

金融資安聯防體系

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

事前防患未然

F-ISAC彙整分析全球資安事件情資，發布駭客威脅預警，並培育資安專業人員，讓金融業者得以事先防範。

事中防微杜漸

F-SOC關聯分析金融業者回傳之事件資訊，探究潛在之可疑行為與攻擊風險，結合情資分享平台強化聯防監控體系。

事後降低傷害

F-CERT協同資安廠商提供應變處理服務，協助金融業者進行損害控制，期能降低損害，儘早恢復金融服務。

資料來源：金融資安資訊分享與分析中心

常見缺失說明

2. 未定期審查並檢討久未使用之使用者權限
3. 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。

資料來源：財團法人台灣網路資訊中心

常見缺失說明

4.網路下單未採多因子驗證方式、重複使用知識因，子進行驗證。

資料來源：資安人

常見缺失說明

5. 未依規定期評估網路系統安全、未依評估結果進行弱點修復。

資料來源：iThome

案例說明

案例說明

- 110年11月〇〇證券察覺到部份客戶之海外複委託下單，出現購買港股「深藍科技控股」之異常案件，隨即清查客戶相關交易帳戶。

- 主因是APP下單之憑證申請僅使用「出生年月日」或「弱密碼」，遭到駭客破解下載憑證並偽冒下單。

圖片來源：自由時報

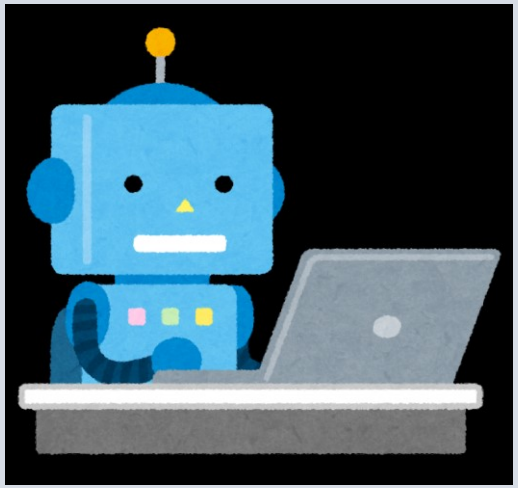
案例說明-撞庫攻擊

透過各種管道取得投資人帳號等資訊

透過腳本執行撞庫攻擊，確認可用帳號

盜用帳號透過APP申請交易憑證

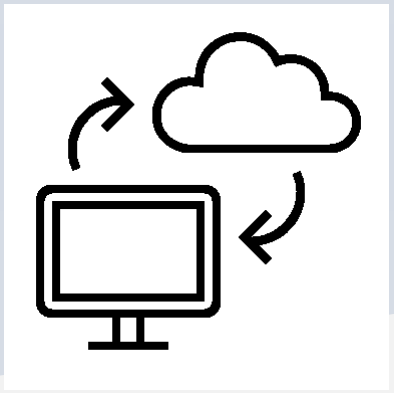
複委託偽冒下單



未來展望

未來展望

機密不外洩	資料不錯誤	服務不中斷



期待證券商資安落實C.I.A.，達成「零容忍」目標。

TAIWAN
STOCK EXCHANGE

簡報結束
敬請指導