近期重大資安事件解析

電腦規劃部

111年9月13日

TAIWAN
STOCK EXCHANGE

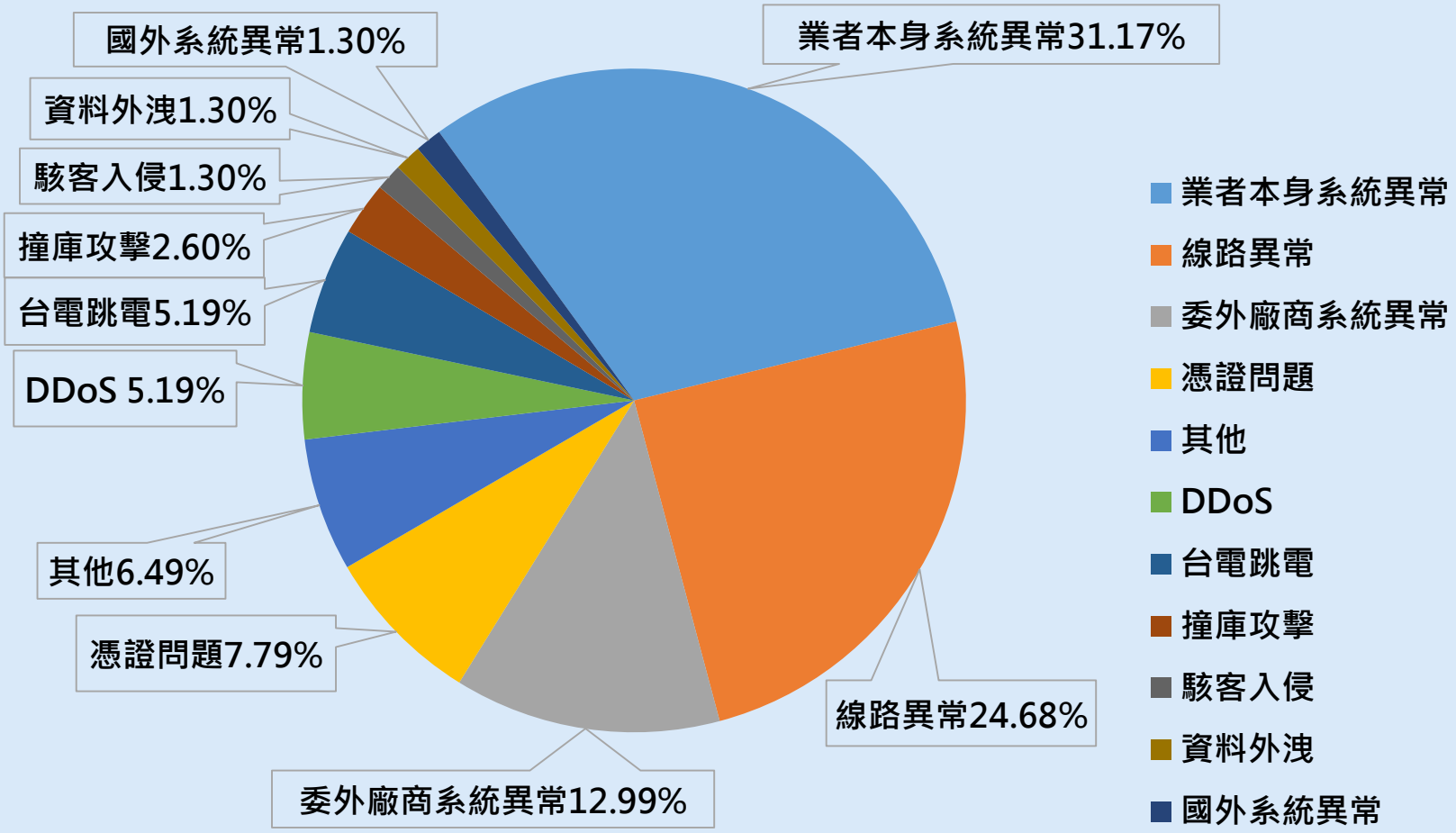
大綱

竭誠為您服務

- 資通安全事件統計
- 資安事件處置與防護分享
- 資安事件通報應變辦法
- SF-CERT 通報應變服務

資通安全事件統計(依事件類型)

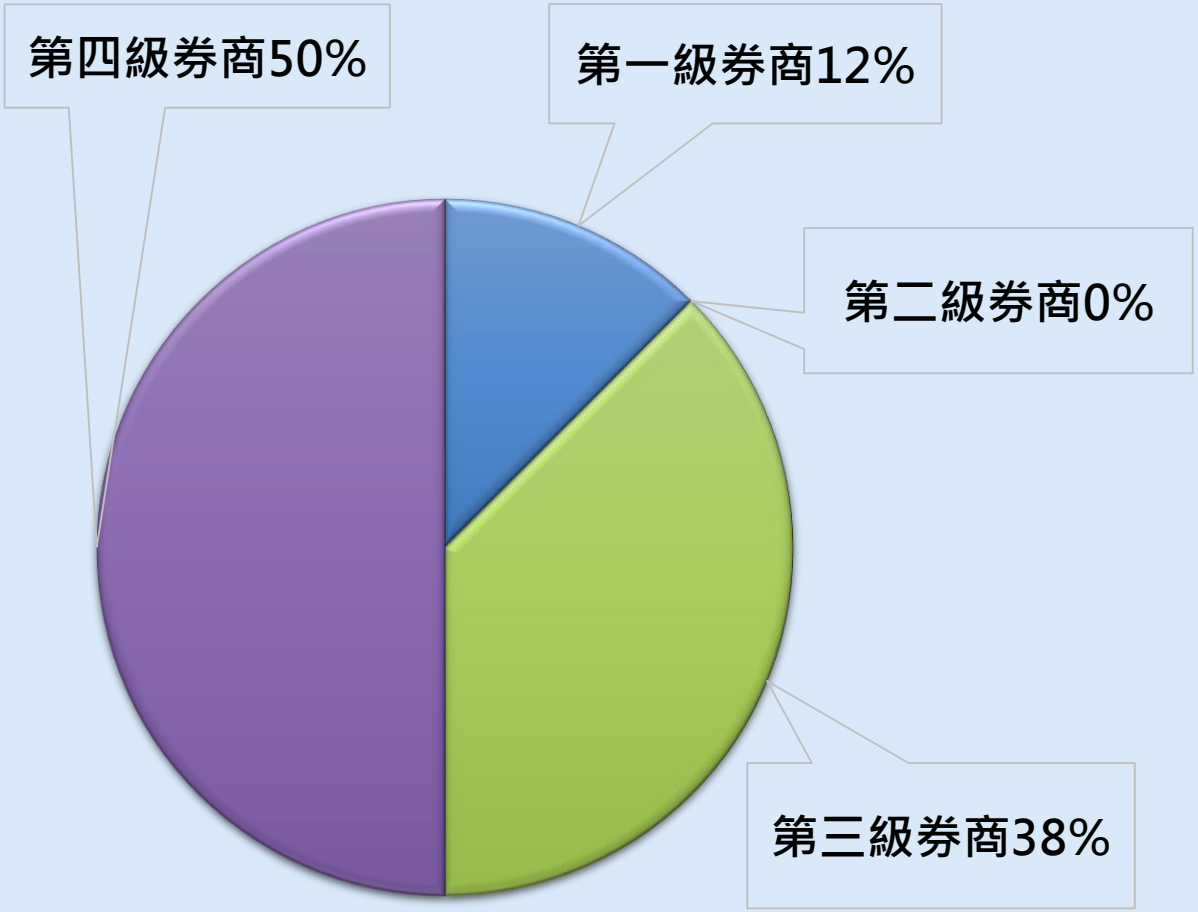
111年1-8月證券商通報事件統計



駭客攻擊事件統計(依業者等級)

竭誠為您服務

111年1月 - 8月證券商駭客攻擊事件統計



駭客攻擊事件類型
（總計8件）

- DDoS
- 撞庫攻擊
- 資料外洩
- 駭客入侵

- 第一級券商(2家)
  (成交金額市佔16.93%)
- 第二級券商(7家)
  (成交金額市佔33.39%)
- 第三級券商(10家)
  (成交金額市佔17.12%)
- 第四級券商(44家)
  (成交金額市佔32.56%)

資通安全事件統計(續)

111年1-8月通報事件類型證券商分級統計

事件類別	第一級券商	第二級券商	第三級券商	第四級券商	小計
業者本身系統異常	9	9	3	3	24
線路異常	1	6	6	6	19
委外廠商系統異常		2	3	5	10
憑證問題		2		4	6
DDOS	1			3	4
台電跳電	1	1	1	1	4
撞庫攻擊			2		2
國外系統異常		1			1
資料外洩			1		1
駭客入侵				1	1
其他		1		4	5
總計	12	22	16	27	77

大綱

- 資通安全事件統計
- 資安事件處置與防護分享
- 資安事件通報應變辦法
- SF-CERT 通報應變服務

資安事件處置與防護分享
撞庫攻擊事件

事件說明

- 110年11月25日，證券商通報部分客戶帳號遭冒用，複委託下單香港深藍科技，緊急暫停複委託電子交易，改採人工下單
- 期間有多家證券業者通報撞庫攻擊、異常登入，及複委託下單成功事件

資安事件處置與防護分享
撞庫攻擊事件(續)

資安防護建議

- 應採雙因子認證機制(例如：下單憑證、綁定裝置、OTP、生物辨識等機制)
  - 網路下單登入時
  - 客戶申請或更新憑證時
    (應增加與登入雙因子之不同因子驗證機制)
- 客戶應使用優質密碼
- 客戶密碼輸入錯誤次數達三次者，應中斷連線
- 應注意客戶異常登錄情形，即時了解異常原因

資安事件處置與防護分享
DDoS攻擊事件

事件說明

- 106年DDoS攻擊事件造成重大影響
- 107年、108年、111年8月市場DDoS攻擊，皆未造成重大影響

資安防護建議

- 備妥流量清洗或流量分流服務
- 必要時與ISP業者合作阻擋境外連線
- 持續辦理DDoS演練，強化應變反應能力
- 今年DDoS攻擊採相同來源IP，建有應用程式防火牆(WAF)業者，可設定連線頻率過高阻擋規則

資安事件處置與防護分享
業者資料外洩事件

事件說明

- 111年8月業者通報自行設計且內部使用之顧客關係管理APP具設計瑕疵，遭特定攻擊來源竄改參數撈取客戶資料

資安防護建議

- 系統上線應通過「源碼掃描」安全檢測；定期辦理弱點掃描
- 內部應用APP不應採公開上架方式讓不特定人下載
- 除涉及投資人使用之行動應用程式外，建議具存取客戶資料功能且公開上架之行動應用程式，應採行以下安全措施：
  - 通過財團法人全國認證基金會（TAF）行動應用APP資安檢測
  - 採行雙因子認證機制

資安事件處置與防護分享
加密勒索攻擊

事件說明

- 107年駭客利用業者可任意上傳檔案系統弱點，上傳惡意程式、植入勒索軟體，導致上百台伺服器資料遭加密勒索

資安防護建議

- 落實資料備份
- 限制檔案上傳格式（檔名過濾特殊字元、使用白名單檢查結尾副檔名、限制上傳目錄之程式執行權限）
- 例行作業避免使用高權限執行
- 高權限帳號存取控管
- 內部網段區隔控管

資安事件處置與防護分享
ISP業者斷線事件

事件說明

- 111年6月ISP業者網路服務異常，導致12家證券商、9家期貨商通報下單系統無法提供服務

資安防護建議

- 檢視核心系統線路備援機制之完整性及有效性，若僅採用單一電信公司網路線路服務，可能因單一電信公司較長時間(或於關鍵時刻)服務異常，影響交易或結算帳務功能
- 若網路下單服務受影響，應即時啟用備援機制，並提醒投資人暫時採用其他替代下單機制
- 若投資人自身網路受影響，提醒改用WIFI等其他連線方式

資安事件處置與防護分享
委外及供應鏈安全

TAIWAN STOCK EXCHANGE

竭誠為您服務

事件說明

- 111年7月駭客利用委外憑證系統漏洞進行入侵攻擊
- 111年8月駭客利用老舊架構中台系統漏洞進行入侵攻擊

資安防護建議

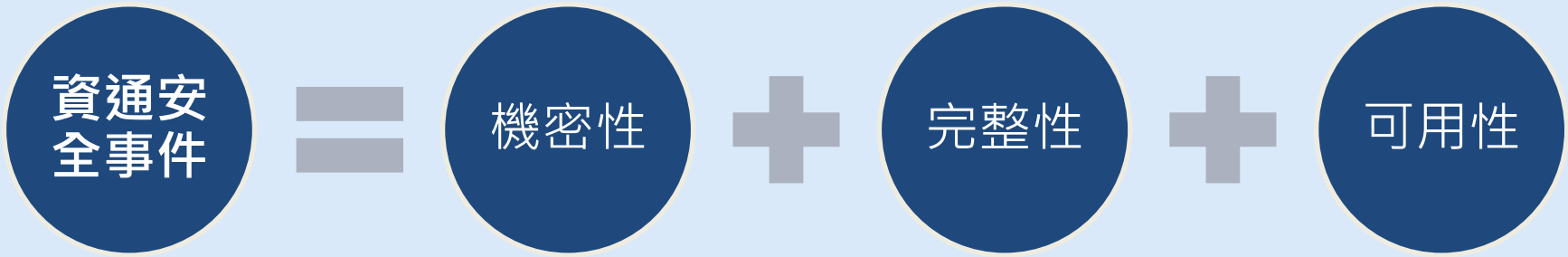
- 定期檢視暴露於網際網路服務系統之必要性
- 原則禁止防火牆對外連線，僅開放必要之點對點連線
- 應用系統上線前應通過源碼檢測；應用程式與系統皆應執行弱點掃描
- 定期執行所有系統源碼檢測及弱點掃描

大綱

- 資通安全事件統計
- 資安事件處置與防護分享
- 資安事件通報應變辦法
- SF-CERT 通報應變服務

資安事件通報應變

- **依據「證券期貨市場資通安全事件通報應變作業注意事項」，發生重大影響客戶權益或正常營運之資訊服務異常事件，以及資通安全事件，依本注意事項辦理**



資安事件通報應變(續)

初步通報

知悉事件30分鐘內辦理

正式通報

於查明事件後儘速辦理

解除通報

事件處理完成後

大綱

- 資通安全事件統計
- 資安事件處置與防護分享
- 資安事件通報應變辦法
- SF-CERT 通報應變服務

SF-CERT通報應變服務

竭誠為您服務

事前準備

- 資安事件應變處理參考指引
- 日誌留存參考指引
- 資安演練(DDoS演練、通報演練、電子郵件社交工程演練、資安事件應變桌面演練)
- 事件應變訓練

事中應變

- 7*24 電話關懷、顧問諮詢
- 現場事件應變、數位證據保全、鑑識調查(業者自費)
- 分享產業攻擊資訊
- 研擬產業對應策略
- 協調外部資源

事後檢討

- 檢討修訂「資安事件應變處理參考指引」
- 配合資安時事納入演練及教育訓練素材

SF-CERT通報應變服務(續)

發生資安事件
(資安通報系統接獲通報)

- 參照「資安事件應變處理參考指引」
- 7*24 電話關懷協助
- 7*24 電話顧問諮詢
- 現場事件應變、數位證據保全、鑑識調查(業者自費)

解除資安事件

發生重大資安攻擊事件

- 分享產業攻擊資訊
- 研擬產業對應策略
- 協調外部資源
- 擔任事件回應管道

重大資安攻擊事件：

1.單一類型資安攻擊/侵害事件，於10日內影響3家以上業者，且有影響業者交易之虞

2.其他主管機關指示事件

SF-CERT發揮良好成效

揭誠為您服務

DDoS攻擊事件	• 分享攻擊資訊及防護建議 • 要求ISP業者阻斷特定攻擊來源IP
業者資料外洩事件	• 分享攻擊資訊及防護建議 • 提供業者向AWS舉報下架資訊
憑證系統漏洞 老舊架構中台系統	• 要求供應商清查使用相關系統證券商，持續跟催改善 • 要求證券商落實定期源始碼安全性檢測、弱點掃描

簡報完畢
敬請指教

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

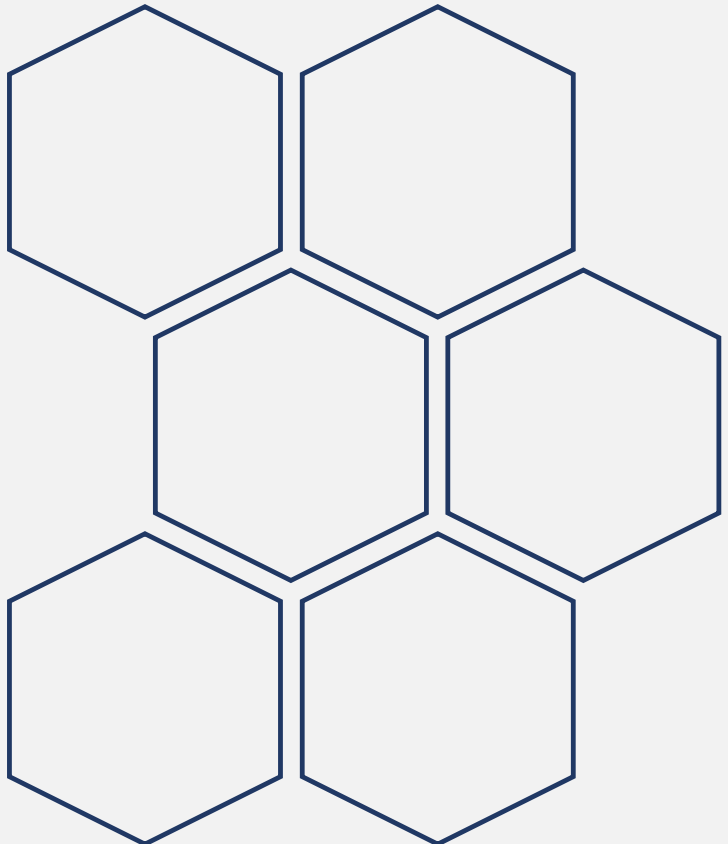
二、資安查核重點

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

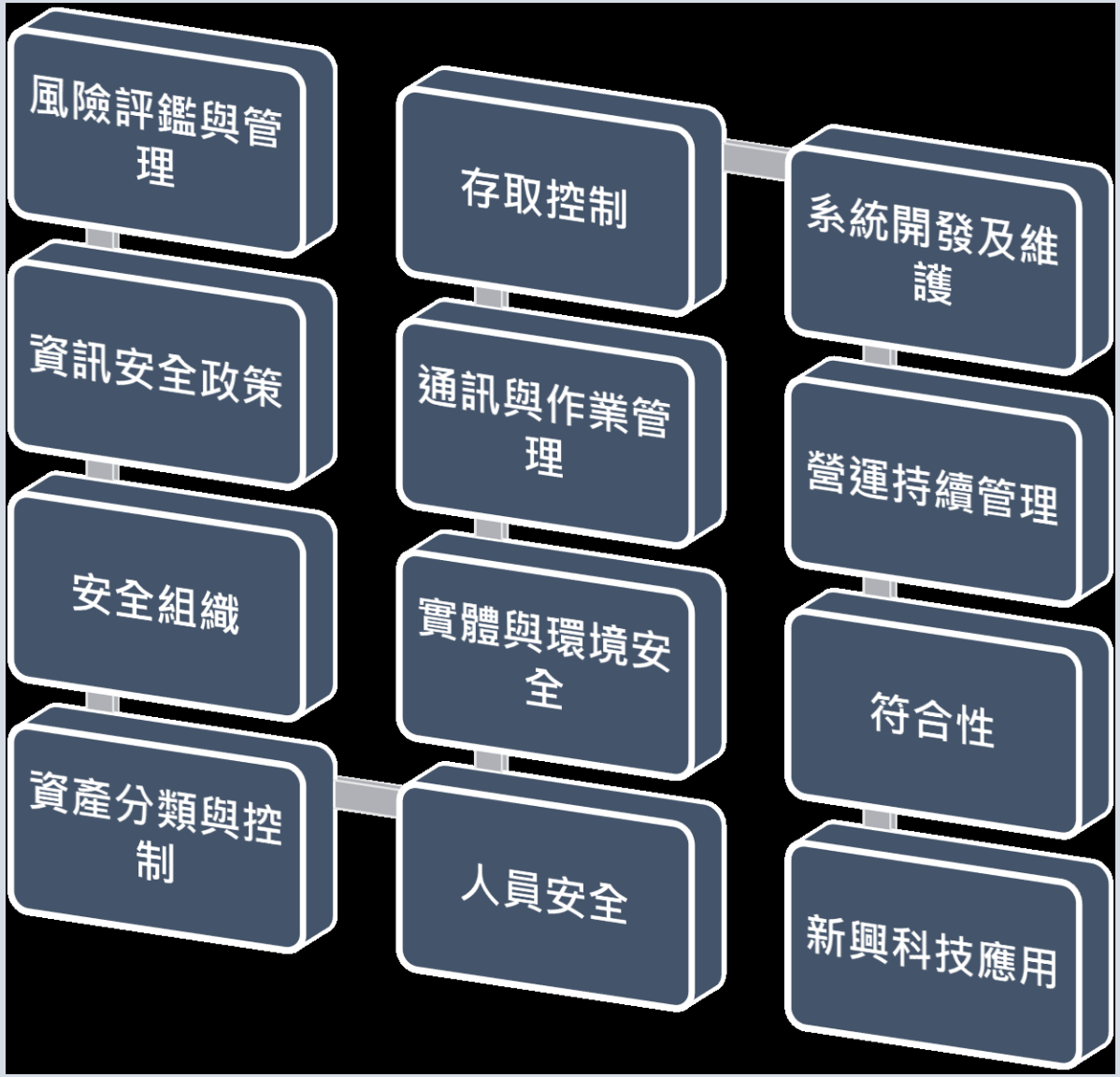

強化登入及憑證下載驗證
主機共置服務
資通安全檢查機制
資安防護彙總
個人資料保護
駭客攻擊防護
金檢年度查核重點

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



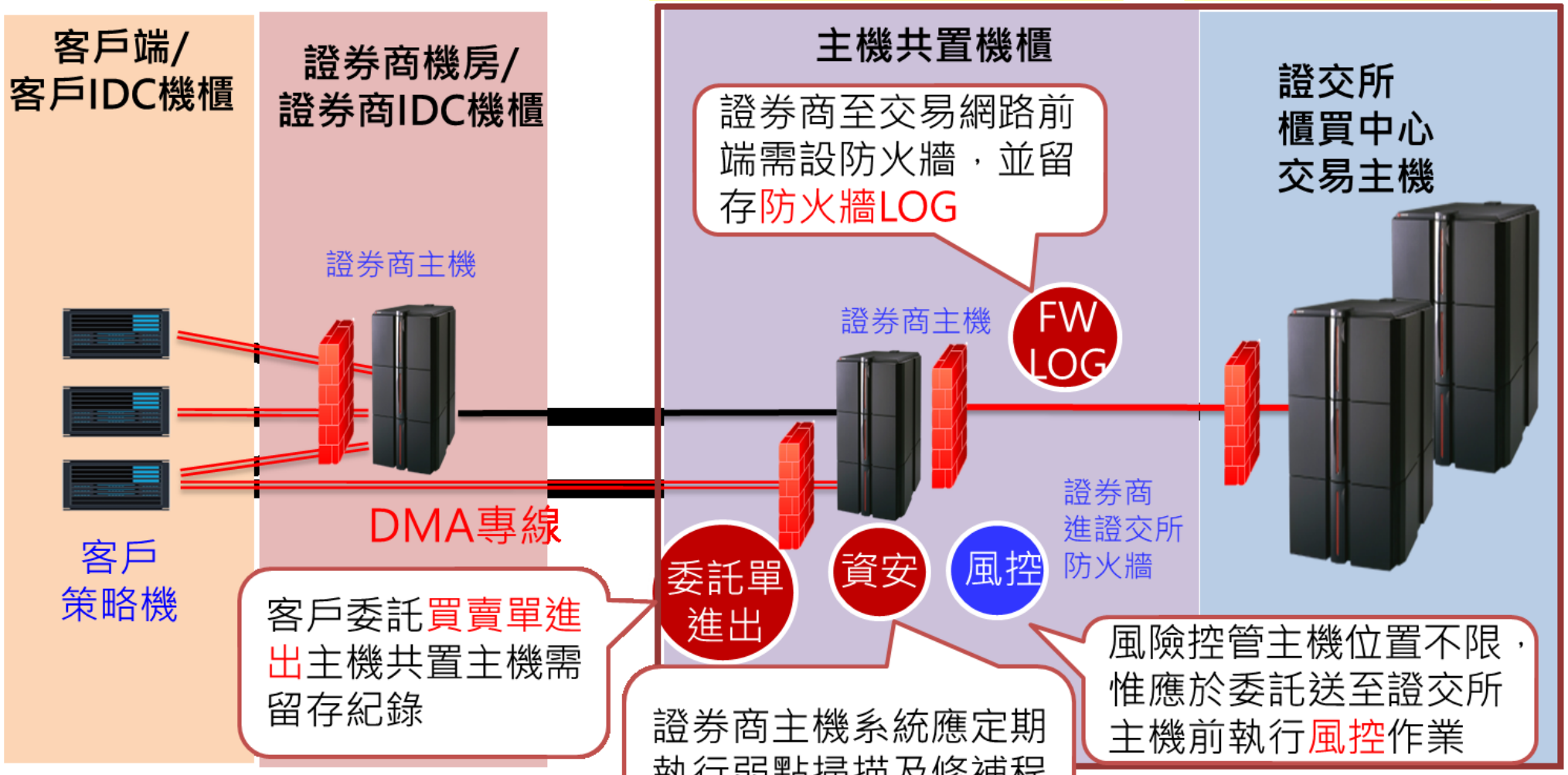
資安查核重點

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

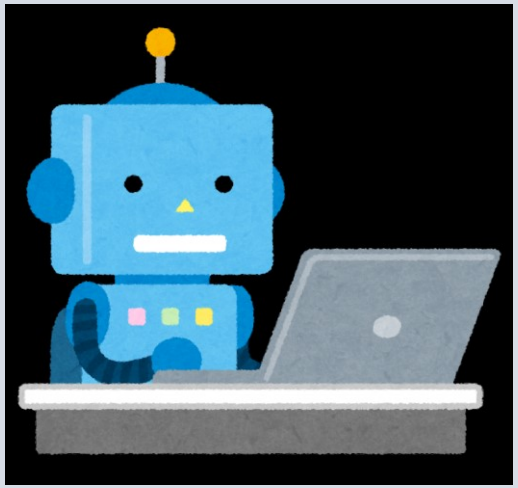
案例說明-撞庫攻擊

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

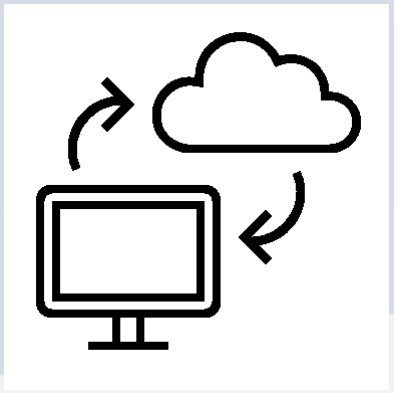
複委託偽冒下單



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