證券商
資安作業說明

臺灣證券交易所
券商輔導部

大綱

一、證券商資安風險

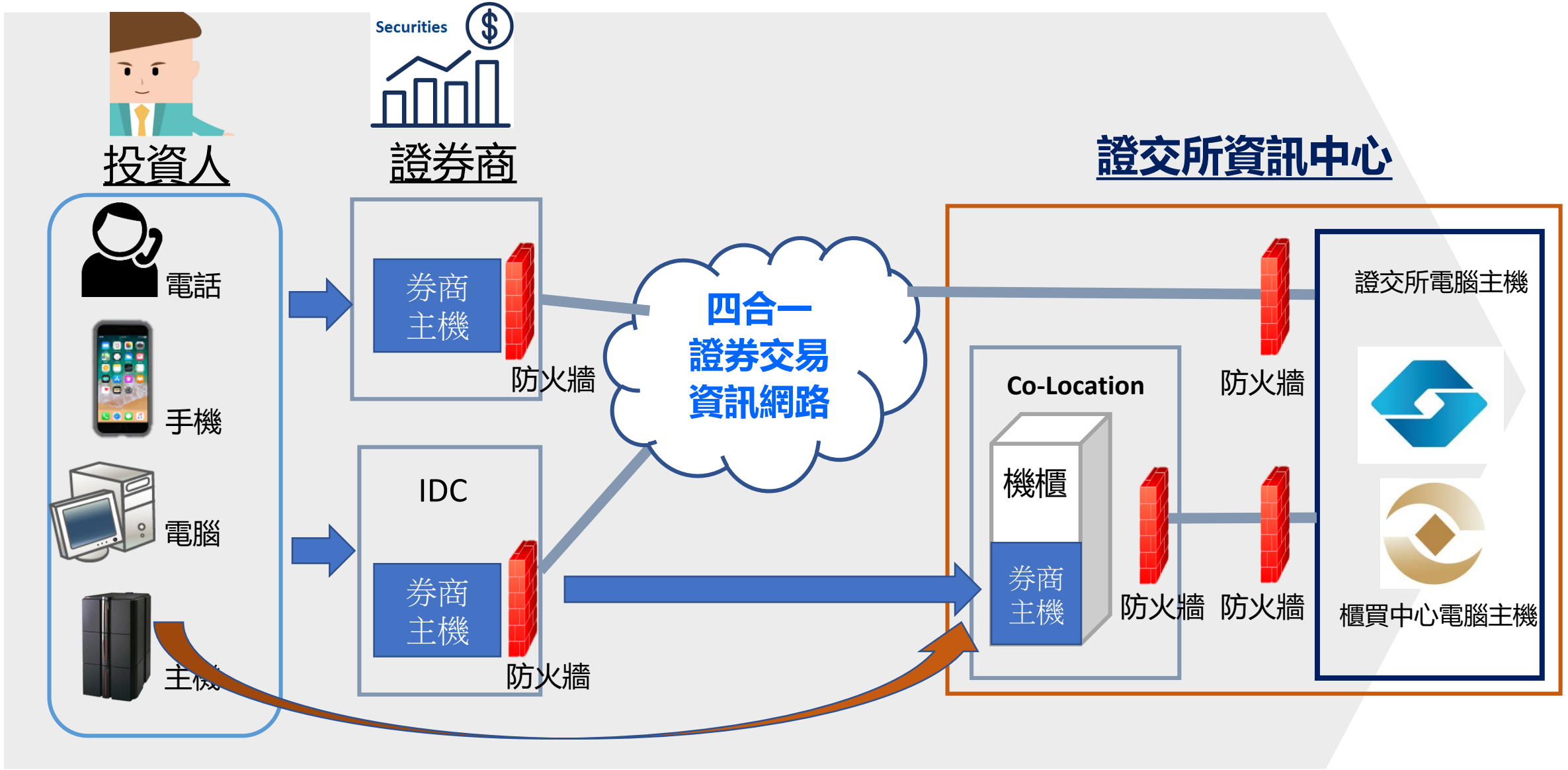
二、證券商資安規範及認證

三、證券商分級管理

四、資安案例分享

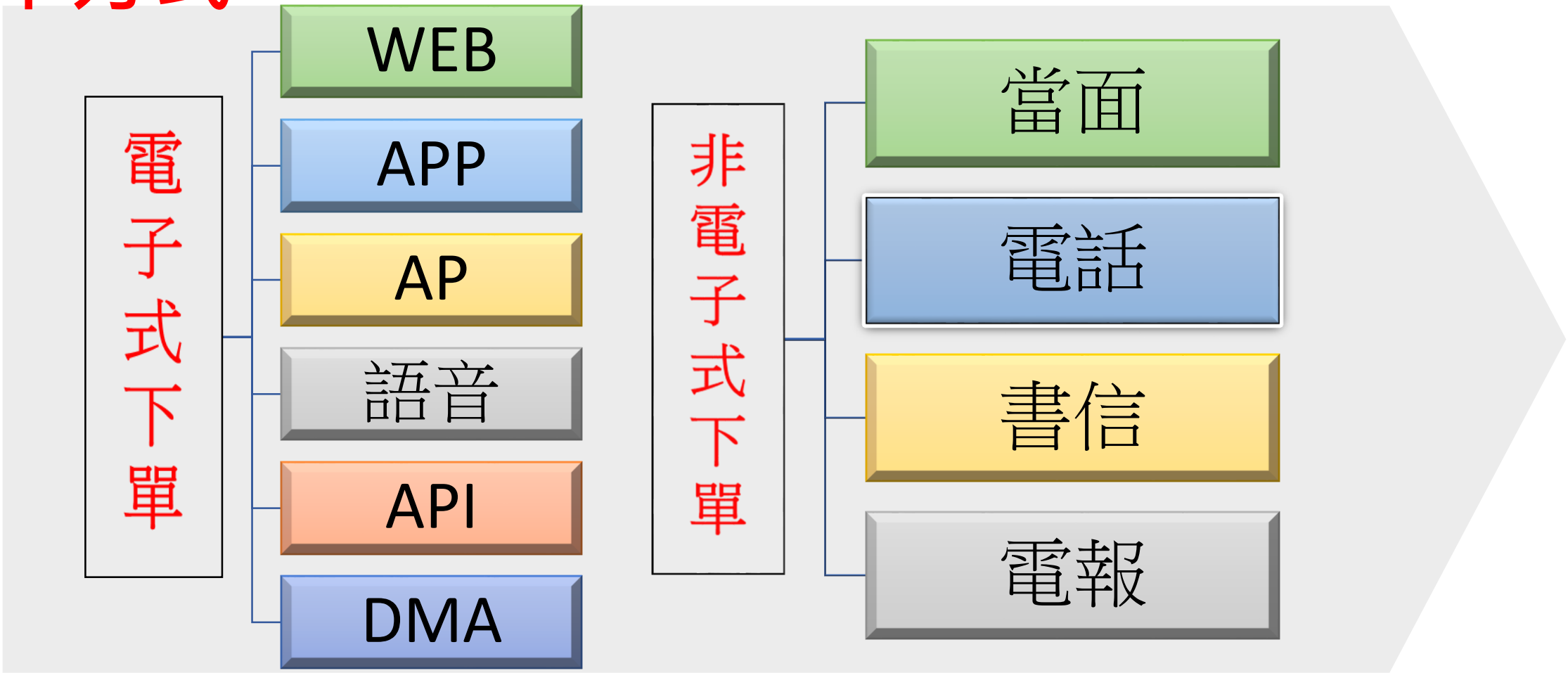
五、結語

一、證券商資安風險



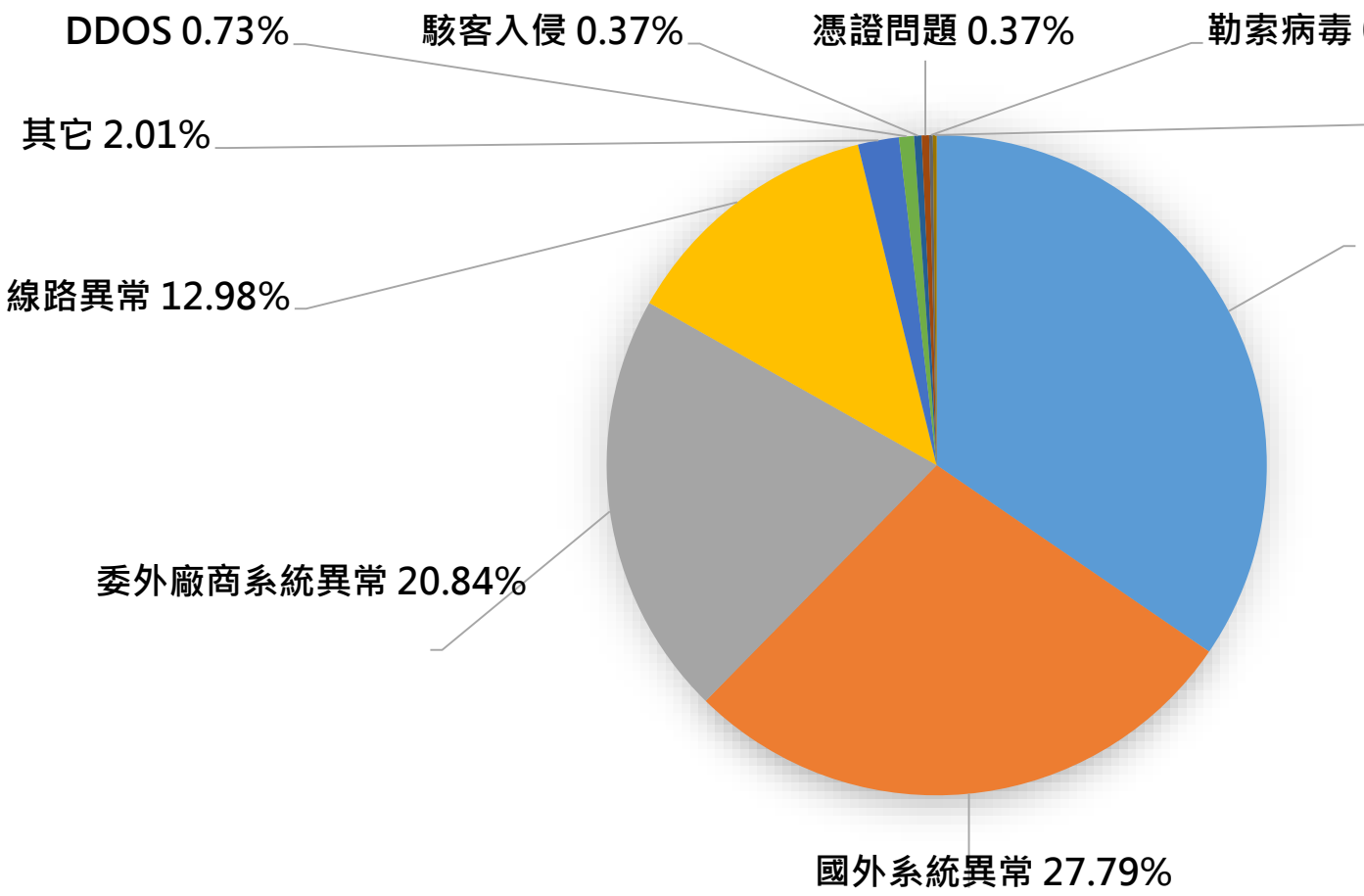
一、證券商資安風險

下單方式



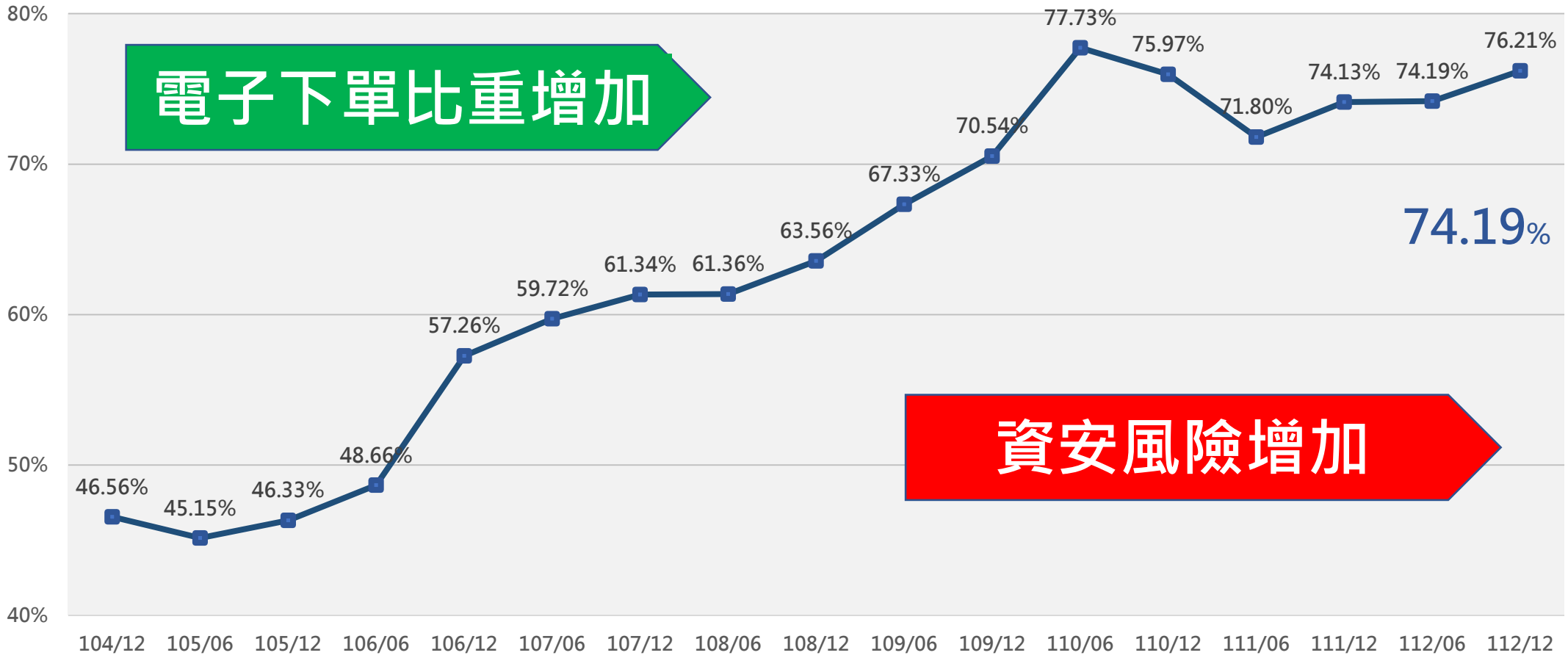
一、證券商資安風險

112年資安通報統計



業者本身系統異常	189	件
國外系統異常	152	件
委外廠商系統異常	114	件
線路異常	71	件
其它	11	件
DDOS	4	件
駭客入侵	2	件
憑證問題	2	件
勒索病毒	1	件
個資洩漏	1	件
總計	547	件

一、證券商資安風險



一、證券商資安風險

- 駭客（Hacker、 Cracker）：研究如何智取電腦安全系統的人員
- 常見方式：
  - 假冒熱點、免費WiFi
  - 假冒網站、APP
  - DDoS攻擊(分散式阻斷服務攻擊)
  - 撞庫攻擊
  - 社交工程
  - ……

二、證券商資安規範及認證

證券商資安查核重點

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

二、證券商資安規範及認證

證券商資安查核

年度資安例查

- 檢視證券商整體資安防護 及 法規落實情形

選案查核

- 投資人檢舉、主管機關指示、主機共置服務

專案查核

- 特定議題對市場之影響 或 檢視整體辦理情形

二、證券商資安規範及認證

資安認證

公司認證

- ISO27001、ISO27701、ISO22301

個人證照(全體證券商)

- 管理類證照、技術類證照

三、證券商分級管理

證券商資安分級

第一級(2家)	>200億
第二級(7家)	100~200億
第三級(9家)	40~100億
第四級(49家)	<40億

經紀業務市占率

電子下單比率

分級應用

- 資通安全查核頻率
- 資安長設置標準
- 導入國際資安管理標準
- 專責資安單位及資安人員數量配置
- 資安防禦設備投入時程

資安案例1：委外廠商系統異常

憑證系統驗章回應緩慢，造成電子交易平台無法登入

- 經查資料庫資源使用正常，係因憑證系統應用程式無法提供連線服務
- 將憑證系統主機重開機、重啟服務之後，連線即恢復正常

資安案例1：委外廠商系統異常

強化措施

- 系統整體資源評估(前中後台與憑證系統)
- 落實營運持續計劃

資安案例2：委外廠商控管問題

廠商系統中毒，病毒轉傳至證券商

- 經查廠商系統中毒，經由線上維護將病毒傳送至證券商
- 證券商採獨立網段並有監控，尚無造成損害

資安案例2：委外廠商控管問題

強化措施

- 加強異常行為監控(如登入失敗)
- 落實網段區隔
- 禁止使用預設高權限帳號使用及簡易密碼

資安案例3：委外廠商控管問題

證券商未將測試與正式系統隔離

- 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
- 造成1.4億元鉅額錯帳，回補後證券商虧損113萬，並被課35萬元違約金

資安案例3：委外廠商控管問題

強化措施

- 落實網段區隔
- 帳號控管應依職掌配置妥適權限
- 測試計劃應完整(目的、方法、紀錄、結果)

資安案例4：程式測試不完整(本身系統異常)

證券商上版程式測試不完整

- 下單程式上版後未詳細檢查正式上線結果
- 出現測試資料、對帳單寄錯對象、程式有問題無法及時下架

資安案例4：程式測試不完整(本身系統異常)

強化措施

- 程式應有完整測試計劃
- 強化個資管理 (非公務機關個人資料檔案安全維護辦法)

資安案例5：證券商下單程式遭冒用

網路商店出現非證券商上架之APP

- 平台上出現非證券商提供之APP
- 於網站警示公告並申訴APP下載平台下架偽冒APP

資安案例5：證券商下單程式遭冒用

強化措施

- 防範詐騙釣魚並積極通知客戶
- 於官網揭露相關訊息並提供軟體服務下載點
- 向警察局報案及軟體平台提報下架偽冒程式

五、結語

精進監理措施

- 優化查核品質、掌握市場脈動、新興議題善用專家職能

強化改善防禦能量

- 確保證券商改善計畫合理可行、提升證券商資安聯防能力、增加預警選案指標

五、結語

加重事件處置措施

- 強化經理人問責制度、提高違約金額度

資安監理科技運用-導入大數據分析工具

- 分析資安風險現況 、資安風險趨勢

簡報結束
敬請指導