資通安全查核重點及缺失案例分享

台灣證券交易所
券商輔導部

大綱

一、資安查核簡介

二、資安通報案例

三、法規宣導說明

證券商電腦稽核之法源

臺灣證券交易所股份有限公司查核證券商作業辦法

- 第1~11條說明辦理查核依據及方式

建立證券商資通安全檢查機制

•91.2.21台證（九一）稽字第003551號，修訂「建立證券商資通安全檢查機制」檢查項目，並自91.4.1日起實施。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

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

- 特定議題對市場之影響 或 檢視整體辦理情形

TAIWAN STOCK EXCHANGE
臺灣證券交易所

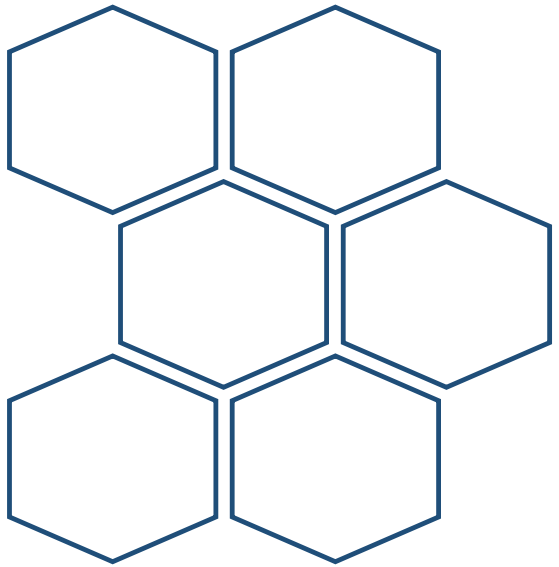
資安查核簡介

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

TAIWAN STOCK EXCHANGE
臺灣證券交易所

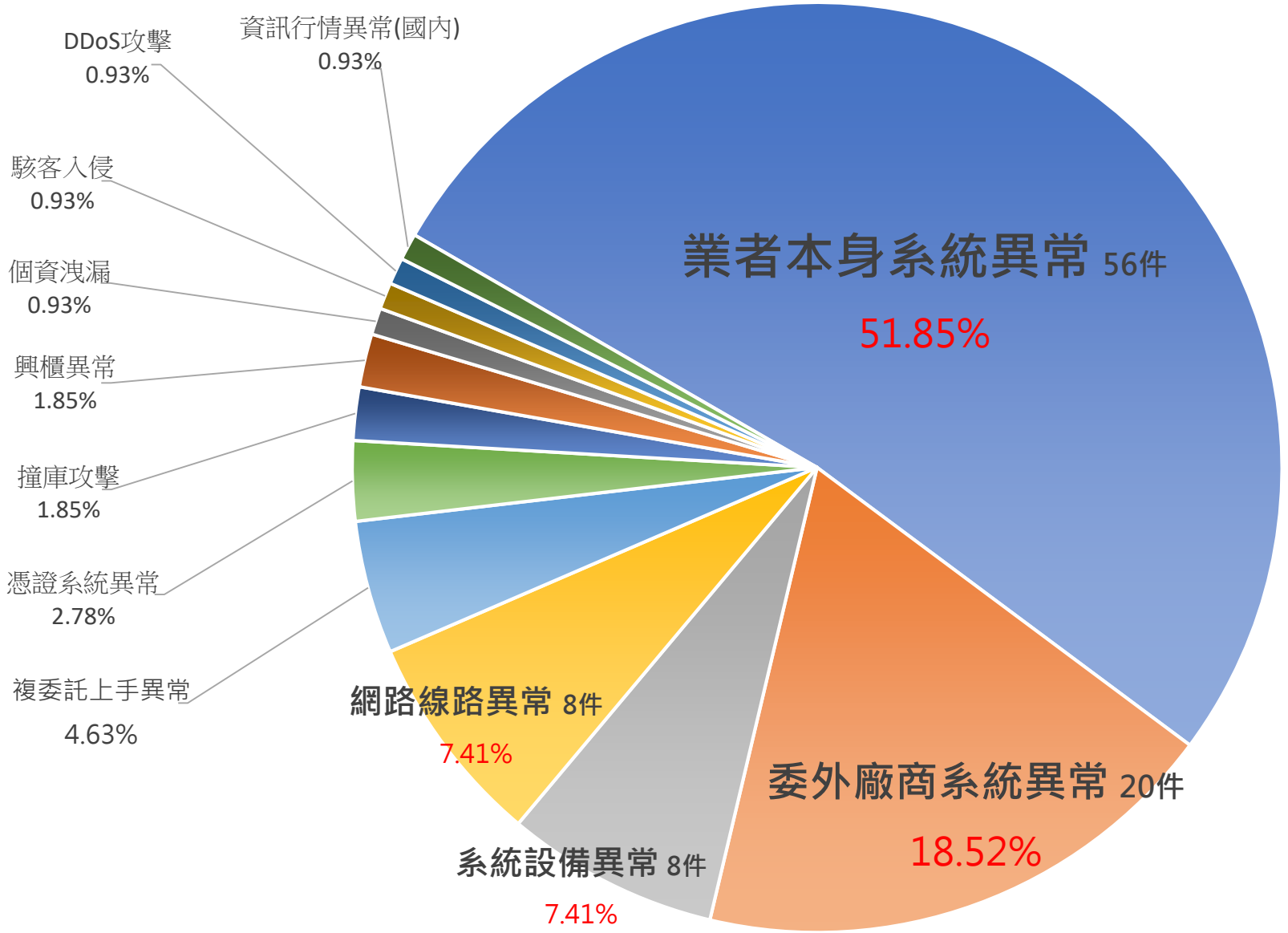
資安通報案例



TAIWAN STOCK EXCHANGE
臺灣證券交易所

112年 資安通報 分析(共108件)

資安通報案例



「系統異常」通報
合計占比 70 %

案例
電子平台無法登入下單
交易功能異常
系統服務緩慢

原因
程式上線前測試不足
作業系統更新前未完整測試
資源配置不足
持續營運及壓力測試未完善

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

分散式阻斷服務(DDoS)攻擊

事件原因：發生DDoS攻擊事件，已導入流量清洗，同時封鎖所有來自國外IP之連線。

影響範圍：造成部分投資人無法正常下單。

處理措施：分析攻擊來源，精準封鎖高風險區域IP。
透過官網公告，或email、簡訊方式通知投資人，使用替代服務方案。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

電子下單平台無法登入

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

影響範圍：投資人登入異常、查詢帳務資料回應緩慢。

強化措施：評估整體資源配置（前、中、後台、憑證系統）
優化程式效能
加強故障復原程序與壓力測試

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

委外廠商開發之「AP/Web下單系統」登入異常

事件原因：該廠商之「商品轉檔」新程式於上午8:30上線，造成大量投資人登入後，同時下載新商品檔，系統出現壅塞，導致部分投資人登入異常，無法下單交易。

影響範圍：共16間證券商受影響，投資人登入需等候10~15分鐘影響時間為08:30~09:50，共80分鐘。

處理措施：緊急將新程式退版，協助下單系統恢復正常登入，未來盤前有上線需求，將進行瞬間大量壓力測試。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

資訊廠商「行情報價系統」異常

事件原因：因當天開盤爆量，行情傳輸需求爆增，造成行情主機資源滿載，報價服務異常，影響使用該報價資訊之證券APP/Web。

影響範圍：共4間證券商受影響，投資人無法取得行情報價，影響時間為09:05~09:35，共30分鐘。

處理措施：資訊廠商緊急增加報價服務機組數量、預計汰換並升級原機房之報價機組、啟用新機房之新機組

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

資訊廠商「行情報價系統」異常

事件原因：因期貨市場爆量造成頻寬滿載，影響使用該報價資訊之AP平台發生投資人登入緩慢之情形。

影響範圍：共13間證券商受影響，投資人無法取得行情報價，影響時間為09:00~10:14，共74分鐘。

處理措施：已擴增資訊廠商機房對外頻寬，加速汰換主機設備

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

資訊廠商「行情報價系統」異常

強化措施：1.要求供應商改善負載監控機制

2.落實供應商簡訊通報機制

3.要求供應商定期提供系統效能監控及壓力測試報告

4.要求供應商提出汰換/升級計畫時程，必要時協助進行效能測試及功能測試。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重大資安事件通報案例

委外資訊服務供應商合約內容

落實執行合約內容：

1. 定期稽核權
2. 罰則與損害賠償條款
3. 定期提交服務水準報告

重新評估可容核心系統可容忍中斷時間

依「分級防護應辦事項附表」辦理 (已於7月底完成)

1.第一級(A級)證券商：市占率1%以上　且
(共16家)　　自然人客戶數達公司客戶數50%以上
核心系統可容忍中斷時間：1小時

2.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
核心系統可容忍中斷時間：2小時

TAIWAN STOCK EXCHANGE
臺灣證券交易所

預告修訂法規

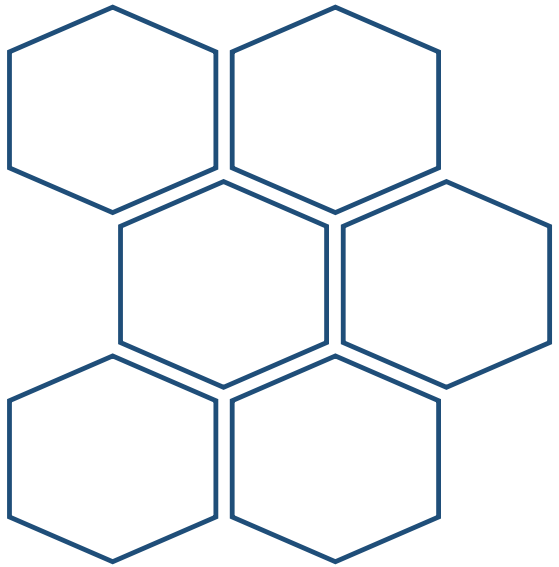
委外管理加強落實

修正草案：供應鏈風險管理參考指引

法條內容：在「資訊服務供應商合約安全控管」中，要求供應商配合進行**壓力測試**及**調整服務負載量**，當市場交易量、業務變化及客戶屬性等發生顯著異動時，**應對系統資源進行調配或擴增**。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

法規宣導說明



TAIWAN STOCK EXCHANGE
臺灣證券交易所

證券期貨市場資通安全事件
通報應變作業注意事項

通報時機

1.發生重大影響客戶權益 或 正常營運之資訊服務異常事件
（影響投資人下單、成交回報等功能）

2.發生資通安全事件

TAIWAN STOCK EXCHANGE
臺灣證券交易所

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 分鐘內至通報系統。
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。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

證券期貨市場資通安全事件
通報應變作業注意事項

通報應變

因網路或電力中斷等事由，無法於系統通報時，
改以電話方式向主管機關證期局及證交所通報
待網路通訊恢復正常後，再於系統補申報。

報案紀錄

1.保存相關事證　　2.向刑事警察局報案
3.提醒投資人誤上當　　4.檢舉下架

證券商通報重大資安事件之範圍申報程序及其他應 遵循事項

重大資安事件範圍

1.第一級至第三級證券商 或 經紀業務成交金額市占率前 20 名證券商之「核心系統」。

2.開盤期間影響交易達 2 小時以上未能恢復

3.於 10 日內就同一資安、系統異常事件， 通報次數達 3 次以上者

證券商通報重大資安事件之範圍申報程序及其他應 遵循事項

重大資安事件範圍

4.同一資安或系統異常事件(例如同一委外資訊廠商系統異 常、同一基礎設施異常等)，自首家證券商通報日起 10 日 內，影響達 3 家以上證券商者。

證券商通報重大資安事件之範圍申報程序及其他應 遵循事項

重大資安事件範圍

5.新型態資安攻擊或駭客攻擊事件(例如撞庫攻擊、DDoS 攻 擊、勒索病毒等)。

6.其他重大資安事件：包括但不限於指定案件、重大輿情案件、客戶資料等敏感資料外洩、其他重大影響投資人權益 案件等。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

證券商通報重大資安事件之範圍申報程序及其他應 遵循事項

初步通報	1.於通報系統輸入資料。 2.或30 分鐘內填具「證券商重大資安事件通報單-初步(正式)通報作業。
結案通報	應於通報重大資安事件之次日起七個營業日內函報詳細資料，填寫結案通報單。
納入內控	將「重大資安事件之通報機制」納入證券商內部控制制度標準 規範。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

簡報結束
敬請指導