TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資通安全查核重點及缺失案例分享

券商輔導部

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 大綱

- 資安查核重點
- 監理科技運用
- 資安通報案例

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

# 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

# 資安查核重點

## 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

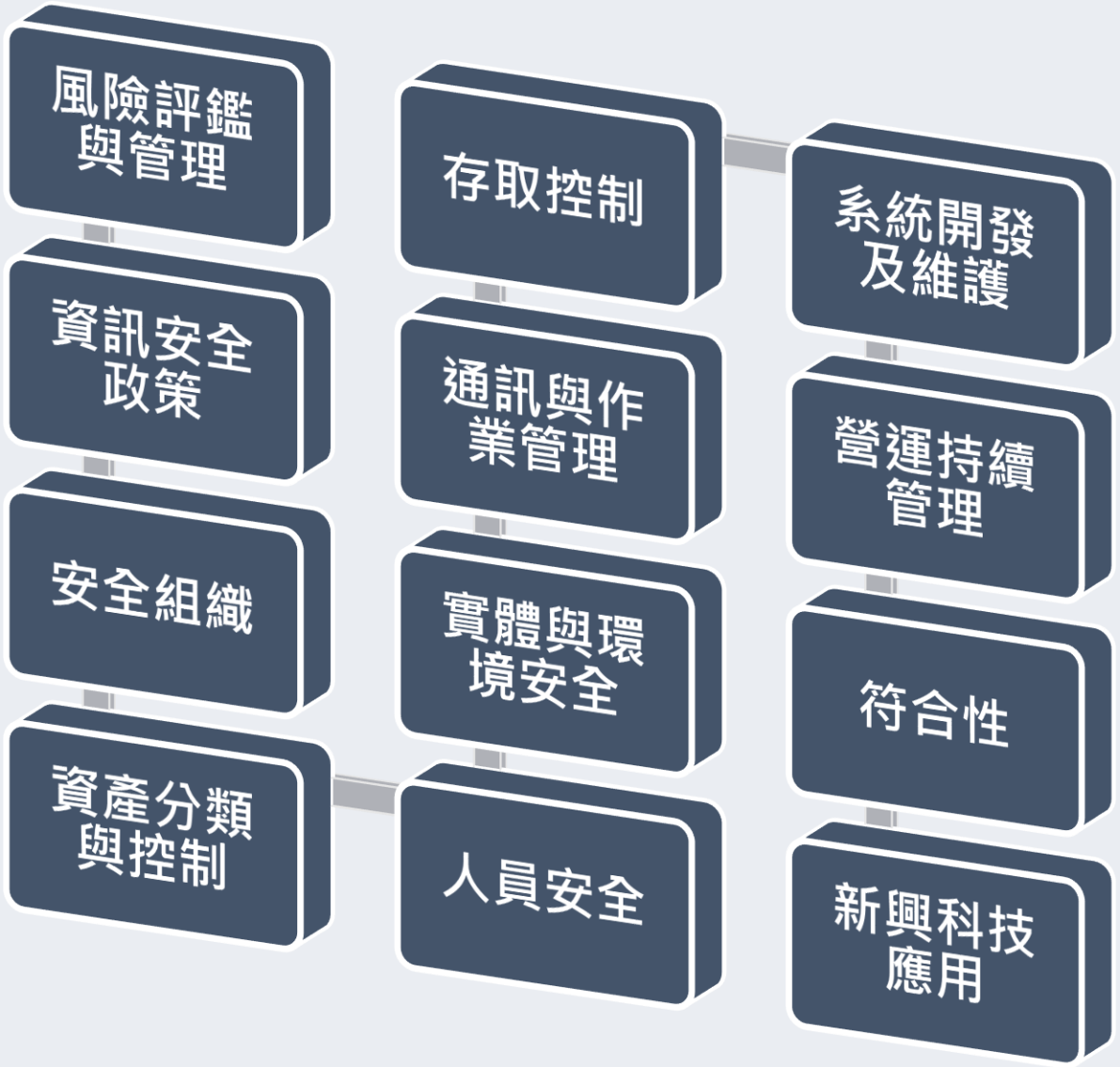
- 特定議題對市場之影響 或 檢視整體辦理情形

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 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



TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 風險評鑑管理

1. 評估可接受之資安風險等級
2. 風險評鑑報告、風險改善計畫(每年產出)

## 資訊安全政策

1. 定期評估資安政策
2. 發布員工、廠商知悉
3. 建立「資安、個資通報程序」

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 安全組織

1. 評估資安人力配置
2. 取得資安專業證照
3. 資安長設置 (13家)

## 資產分類與控制

1. 編列資訊資產清冊
2. 每年評估資訊系統妥適分級
   (核心、非核心)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 人員安全

1. 完成資安教育訓練(含物聯網)
2. 取得訓練時數證明

## 實體與環境安全

1. 制定「資訊設備報廢」規範、留存報廢紀錄
2. 制定「機房門禁管制」規範、定期審查權限

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 網路安全管理

1. 依用途區分網路
   (DMZ區、營運環境、測試環境、其它環境)
2. 適當區隔機制(防火牆、區域網路、實體隔離)
3. 核心系統應建置於防火牆內
4. 不使用危害國家資通安全產品

## 網路安全管理

5. 遠端連線應使用安全連線機制、登入應採多因子驗證
6. 適時修補網路設備、作業系統之安全漏洞
7. 評估已停止支援服務(EOS)設備的汰換、升級計畫
8. 評估防火牆管控規則、進出紀錄保存3年

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 網路安全管理

9. 伺服器及個人電腦應安裝防毒軟體、更新病毒碼、定期掃描

10. 偵測系統內「網頁及程式」異動紀錄、通知相關人員

11. 制定「電子郵件安全」規範、設定安全性規則(以純文字檢視、關閉自動下載圖片)、過濾惡意軟體

## 網路安全管理

12. 建置「入侵偵測 (IPS) 防禦機制」、
建置「網站應用程式防火牆 (WAF)」

13. 制定「網路下單服務品質標準」，包含「交易安全性、穩定性、系統可用性、提供給客戶的服務」；
並對可用性進行評估(壓力測試報告)

# 資安查核重點

## 網路安全管理

14. 防範撞庫攻擊：每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄進行監控及分析
15. 對於嘗試登入帳號之異常及不明來源IP，建立警示機制，進行監控分析及留存紀錄
16. 建立通知客戶機制(簡訊、APP 或 Email)，確認是否為客戶本人登入

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 電腦系統及作業安全管理

1. 制定「軟體安裝作業程序」
2. 建立軟體白名單、黑名單

## 存取控制

1. 制定「最高權限帳號管理辦法」，管控使用，留存紀錄
2. 定期盤點帳號使用情形、檢討久未使用之帳號
3. 人員異動應即時更新帳號權限、不可共用帳號
4. 設定密碼複雜度、密碼長度、使用期限 ( 文數字、符號、6碼以上、90天 )

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 存取控制

5. 核心系統稽核日誌(log)應紀錄使用者識別碼、登入日期時間(供日後稽核使用、鑑識)
6. 管控機敏資料，防止外洩；妥善管理 測試環境中的 正式資料 (依規定申請、適當遮蔽個資)
7. 網路登入、下單應採多因子驗證

## 存取控制

8. 線上交付憑證應採多因子驗證，且需與登入時使用之因子不同
9. 定期盤點帳號使用情形、檢討久未使用之帳號
10. 盤點個資、留存操作軌跡、加密傳輸機制
11. 電子式專屬線路下單（DMA）使用合規，交易及稽核紀錄保存五年

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 系統開發及維護

1. 委外合約應包含「資訊安全協定」及「委外稽核權」
2. 資訊服務供應商之選定過程，應留下風險評估紀錄(如財務狀況、專業能力)
3. 程式變更之管控程序，應包含日常及緊急作業
4. 每半年辦理一次資訊系統「弱點掃瞄作業」

## 系統開發及維護

5. 評估系統已知弱點之修補方式，留存紀錄；修補完成後再次掃描
6. 每年將APP交付合格檢測實驗室，並通過資安驗證，針對報告進行覆核
7. 訂定API服務規範，投資人首次使用API委託下單前，應進行連線測試

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 系統開發及維護

8. APP如涉及「下單交易」、「帳務查詢」、「身份辨識」之功能異動，上架前應再次自行或委外通過檢測
9. 委外開發之APP應檢視資料傳送對象之適當性，並留存相關紀錄
10. 核心系統上架及更新時，應執行源碼掃描安全檢測
11. 使用第三方服務時，應制定相關規範進行管控

## 持續營運管理

1. 建立DDoS防護機制
2. 主備線路導入流量清洗機制
3. 訂定核心系統可容忍中斷服務時間
4. 訂定持續營運應變計畫
5. 備援程序演練、故障復原程序演練
6. 建立資料保存及備份機制，防範勒索病毒

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 符合性

1. 每年辦理資訊安全查核作業1次
   （內部辦理 或 委託外部專業機構）
2. 針對資安查核報告，確實辦理追蹤改善

## 新興科技應用

1. 使用雲端服務時，應制定「雲端運算服務運作安全規範」
2. 訂定「社群媒體管理辦法」(內容過濾與監視)
3. 訂定「員工使用自攜行動裝置管理規範」
4. 訂定「物聯網安全規範或管理辦法」
5. 每年更新「物聯網設備管理清冊」

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 前三級證券商適用

1. 核心系統導入國際資安標準 (ISO 27001)
2. 建立「防範網路釣魚機制」
3. 辦理滲透測試，評估修補作業流程
4. 辦理資安健診，包含「網路架構、網路惡意活動、伺服器主機、防火牆設定檢視」

( 一級 證券商 「每年」 辦理1次
二三級 證券商 「每兩年」 辦理1次 )

## 前三級證券商適用

5. 妥善處理線上開戶之客戶資料
(婉拒開戶、未前往開戶，應有資料刪除機制)
6. 建立資通安全威脅偵測管理機制
(建置資安監控中心)
7. 核心系統辦理原始碼檢測作業
(包含掃描週期、掃描工具及後續修補情形)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安查核重點

## 一二級證券商適用

1. 建立「進階持續性威脅(APT)」防禦系統(可自行或委外)
2. 依據F-ISAC情資，進行資安強化作業
3. 定期辦理社交工程演練，並針對未通過之人員進行資安教育訓練

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 監理科技運用

# 導入大數據分析工具

## 「資安風險現況」 儀表板

- 以風險為導向，依據證券商「電子交易比重」及「查核缺失扣分」，定義風險區塊，找出需要關懷的證券商，加強輔導，協助改善。

## 「風險趨勢分析」 儀表版

- 分析證券商家數占比最高的「缺失類型」及「增減趨勢」，關注重要資安議題，找出「隱藏風險」，精準輔導，提升防護能力。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安通報案例

# 資安通報案例

## 通報案例1：委外廠商系統異常 (1日內發生2起同類型)

### 1.APP電子下單主機異常，無法登入

- 經查下單主機相關設定均無異常，最後將主機中內建的「Windows Defender防火牆」關閉後，連線即恢復正常。

### 2. APP電子下單系統，連線異常

- 因中台主機作業系統更新後，內建的防毒軟體導致連線異常，後續將作業系統回復舊版，連線即恢復正常。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安通報案例

## 分析原因

- 應是微軟在當日發布系統更新，維護廠商安裝更新檔後，系統上原本已開通之連線服務，被更新後的預設值給覆蓋掉（預設值為「封鎖」），導致連線異常、服務中斷，影響客戶下單交易。

## 對應作為

- 應謹慎評估作業系統升級或程式更新後的影響，並經過完整測試後再進行升級，同時應有效掌握維護廠商所提供之服務內容。

# 通報案例2：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。

# 通報案例2：委外廠商系統異常

## 分析原因

- 憑證伺服器與資料庫連線之程式存在設計瑕疵，當使用者完成憑證驗章後無法順利結束連線並釋出連線資源，造成系統資源被持續占用，當達到系統承載上限後，即無法再提供資源給下一位使用者，造成憑證驗章服務中斷。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安通報案例

## 應變方式

### 營運持續計畫

業務持續運作演練(BCP)

| 執行 | 切換 |
| --- | --- |
| 故障復原程序 | 備援系統 |

RTO 復原時間目標

### 客戶服務不中斷

| | |
| --- | --- |
| 1.第一時間公告 | 1.妥善處理客訴 |
| 2.引導投資人採用替代方式下單 | 2.統計受影響人數<br>預估受影響金額 |

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安通報案例

## 後續處理

### 依規定通報

| 資通安全通報系統 | MIS公告 |
| --- | --- |
| 30分鐘 初步通報<br>24小時 正式通報<br>3 天內 解除通報 | 即時公告<br>(涉及 影響交易、影響投資人權益 ) |

### 系統開發及維護

| 程式開發 | 壓力測試 |
| --- | --- |
| 1.掌握核心架構<br>2.Code review<br>3.優化程式效能 | 1.擴大壓力測試<br>2.系統資源分配<br>(應用程式主機、資料庫主機、憑證主機) |

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 資安通報案例

## 諮詢服務

| 證券業者資安應變與諮詢服務 | |
|---|---|
| 資安事件<br>電話關懷服務<br>協助於30分鐘內完成初步通報 | 全天候(7X24小時)<br>應變處理電話諮詢<br>協助於24小時內轉為正式通報 |

TAIWAN STOCK EXCHANGE
臺灣證券交易所

# 簡報結束
# 敬請指導