# 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

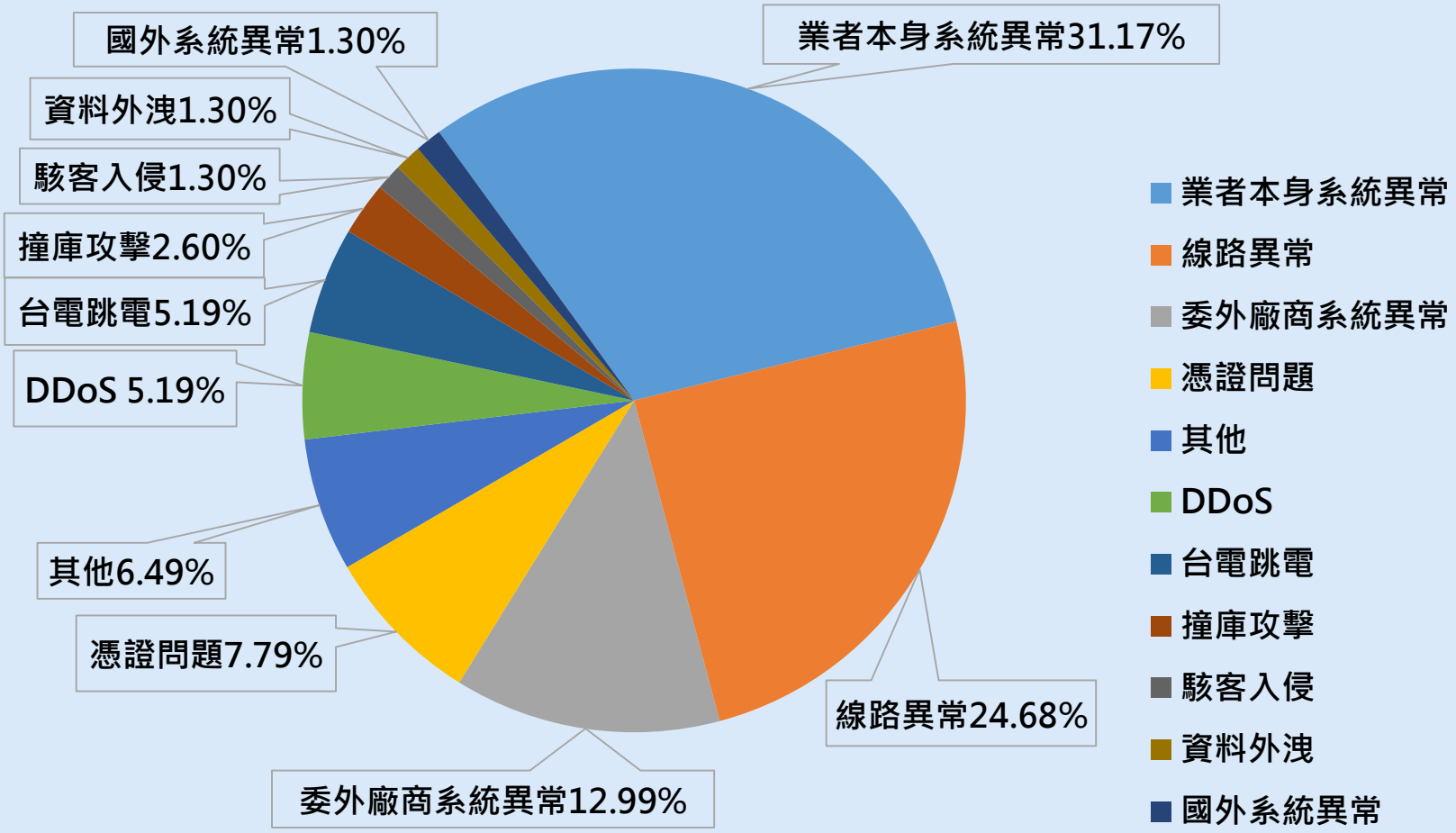
竭誠為您服務

- 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)



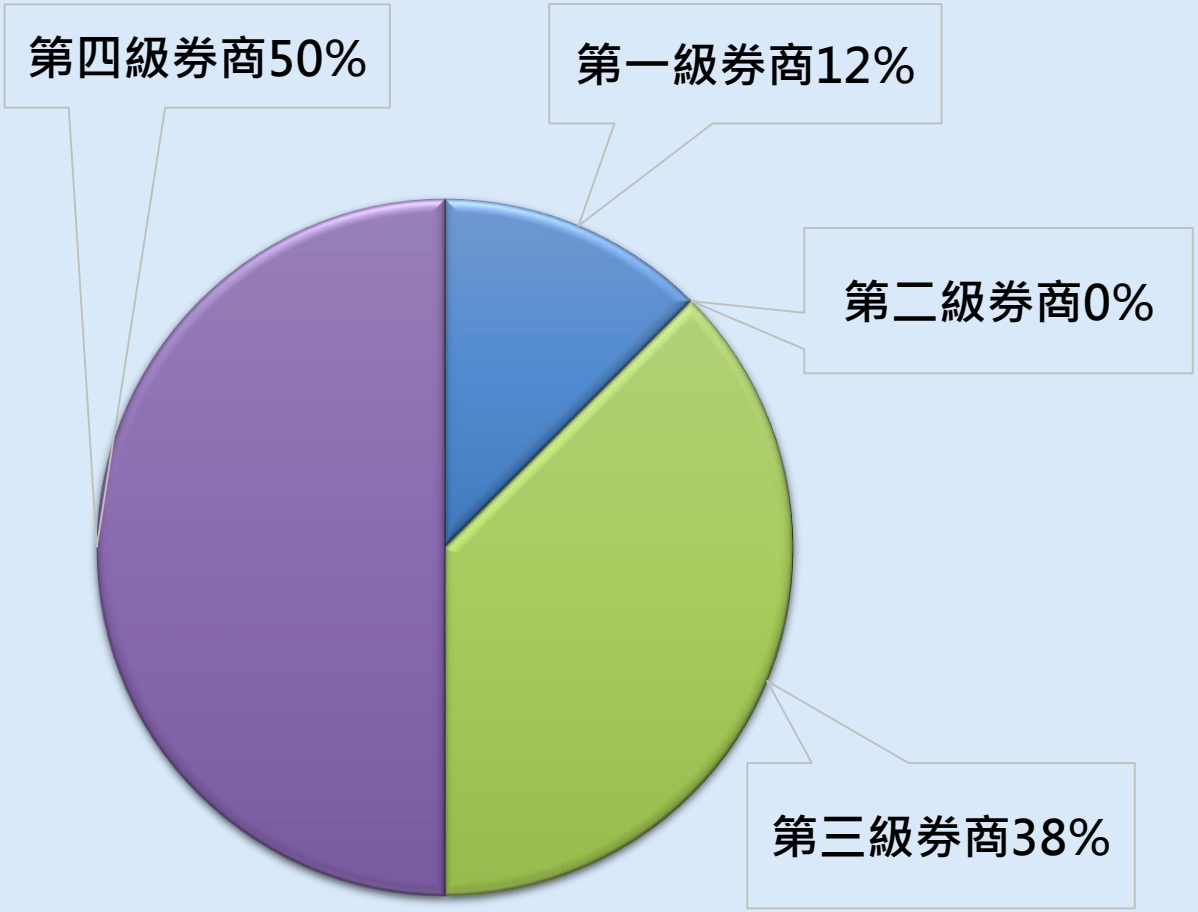
## 111年1-8月證券商通報事件統計



# 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

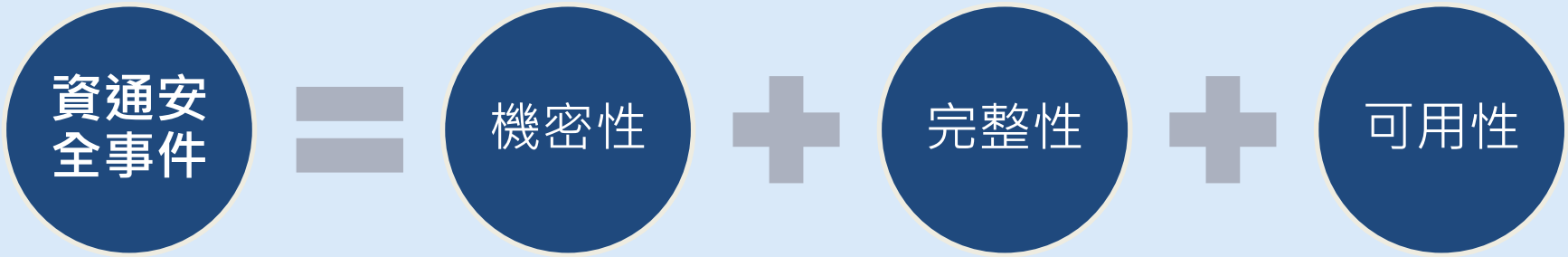


- 資通安全事件統計
- 資安事件處置與防護分享
- 資安事件通報應變辦法
- SF-CERT 通報應變服務

# 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<br>• 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<br>• 提供業者向AWS舉報下架資訊 |
| 憑證系統漏洞<br>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<br>• 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