行政院第3574次會議

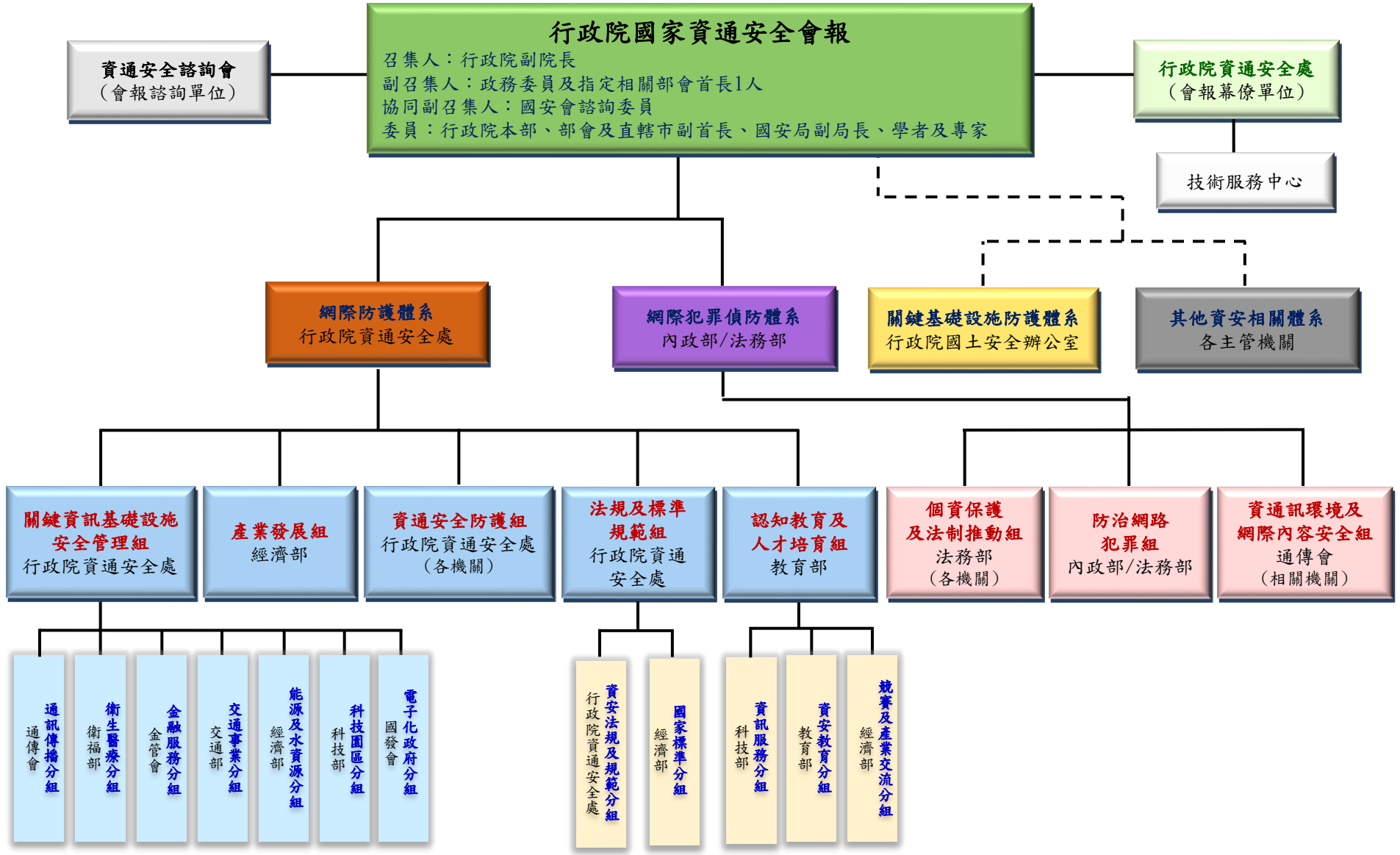
當前資安情勢分析

行政院資通安全處
報告人：簡處長宏偉
106年11月2日

大綱

- 政府資安推動機制
- 現階段資安情勢分析
- 未來策進作為

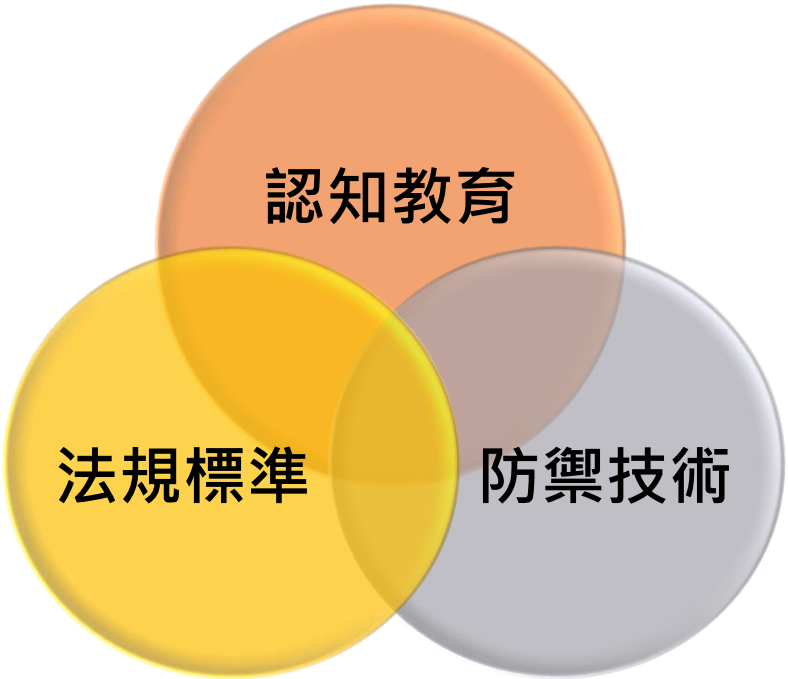
行政院國家資通安全會報組織架構圖



政府資安推動機制

✓各機關每年辦理1次通報演練及2次電子郵件社交工程演練
✓資安會報每年擇選30個機關(構)辦理資安外部稽核，持續改善並降低資安風險
✓政府機關(構)資安專責人力不足，擴大資安職能及教育訓練，培育所需資安人才

✓推動「資通安全管理法」立法，完善各項資安法制環境
✓訂定「國家資通安全發展方案(106至109年)」，奠基國家未來資安發展
✓新興資安標準規範部分，由經濟部、通傳會等發展IoT相關檢測標準及技術

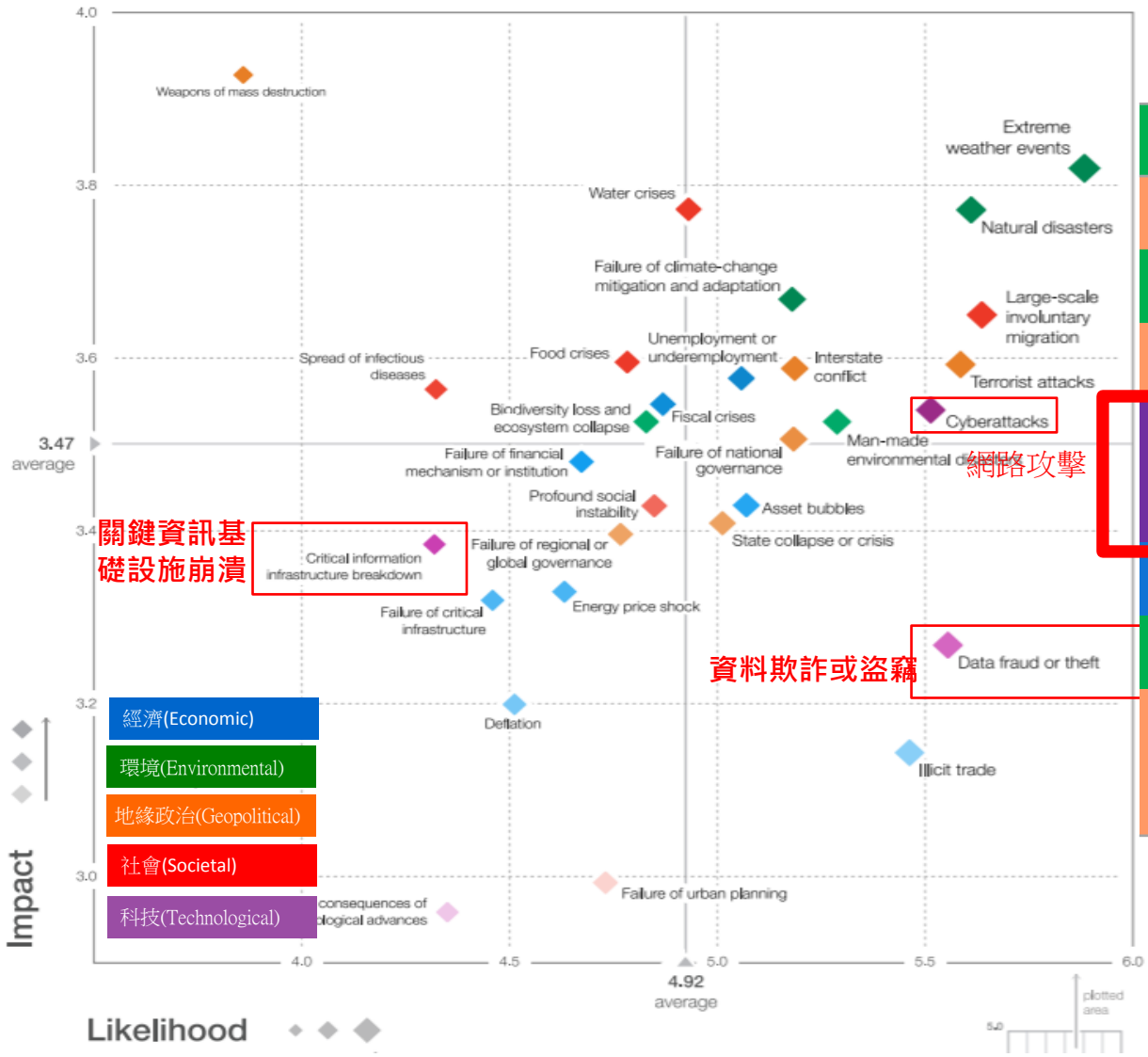


✓各政府機關網路防護監控、技服中心聯防監控及政府網際服務網(GSN)整體偵測防護形成縱深防禦
✓建置資安資訊分享平台(ISAC)、資安通報(CERT)及資安聯防監控(SOC)之資安聯防
✓透過攻防演練，主動發現網站系統弱點

大綱

- 政府資安推動機制
- 現階段資安情勢分析
- 未來策進作為

世界經濟論壇2017全球風險調查報告



10大可能風險

1. 極端氣侯
2. 大規模難民移民
3. 自然災害
4. 恐怖攻擊
5. 資料欺詐或盜竊
6. 網路攻擊
7. 非法貿易
8. 人為環境災害
9. 國家衝突
10. 國家治理失靈

Source: The Global Risks Report 2017 12th Edition, 2017.1.11

1.勒索軟體成長驚人

- 依據國外著名資安顧問公司之2017年資安威脅報告：勒索軟體成長167倍

  案例1：奧地利某知名飯店於2017年1月初遭勒索軟體攻擊，癱瘓所有電腦系統，無法確認訂房客戶，電子門鎖系統亦失去功能，為避免影響顧客權益，飯店支付贖金

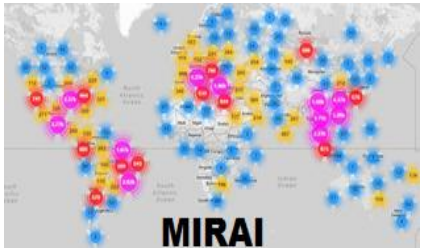
  案例2：美國華盛頓特區警用網路攝影機(CCTV)系統共187個網路影音儲存設備(NVR)中，有123台在其總統就職前8天(1/12)遭駭客植入勒索軟體，約占全特區NVR的70%

- 勒索軟體WannaCry於今年5月間全球肆虐，國內僅少部分的醫院、電力公司、學校及政府機關受影響(數量約185部電腦)

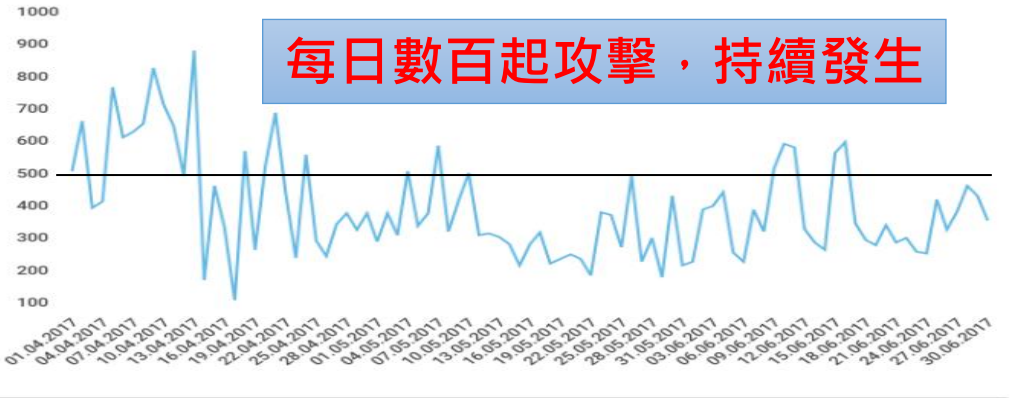
2.大型分散式阻斷攻擊加遽

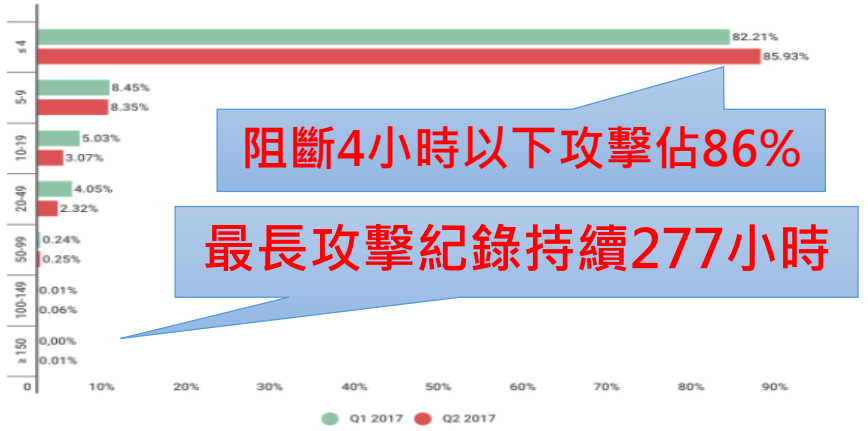
近期大型分散式阻斷服務(DDoS)攻擊案例大多為**混合式攻擊**，發動來源皆以**物聯網(IoT)設備**為主，所占比例與日俱增

- 駭客使用之Mirai殭屍網路活耀於2016年9月至10月，宣稱掌握**30萬部設備**，攻擊流量尖峰達**1Tbps**，阻斷網路正常流量
- 美國資安業者於2/24發布消息表示，全球最大殭屍網路(Botnet)，新增了DDoS攻擊模組**掌控了全球將近500萬台的殭屍電腦**



國外防毒公司2017年第二季報告指出，於86國由駭客掌握殭屍網路參與DDoS攻擊





國內近期重大資安事件媒體報導

史上最大宗 6券商遭駭 勒索比特幣

鎖定頻寬小 瞬間癱瘓網站

2017年02月07日 傳送

【綜合報導】台灣爆發證券

爆員工個資外洩 190筆網路搜尋「全都露」

社會中心 / 台北報導 2017-01-11 13:00

新聞

民眾服務Email密碼規則遭破解！殃及117間外館，恐外洩上萬筆民眾個資

領務局與駐外使館聯繫信箱密碼遭駭客破解，因密碼具有規則性，所以全部117間外館的聯繫信箱內容恐遭外洩，估計有15,000筆曾利用出國登錄系統的民眾個資外洩。行政院資安處已前往領務局了解受害狀況，並已要求改用隨機密碼和雙因素認證。

文/黃泓瑜 | 2017-02-08發表

綁架印表機 46校遭勒索比特幣

2017-02-24

分享 Facebook Twitter

遠銀被駭盜18億 斯里蘭卡警逮2人

遠東商銀於106年10月3日上午發現電腦遭到惡意程式攻擊，目前合計美金5,800萬元已返回遠銀帳上，美金194萬8千元已被凍結，損失金額已降至美金15萬6千元。

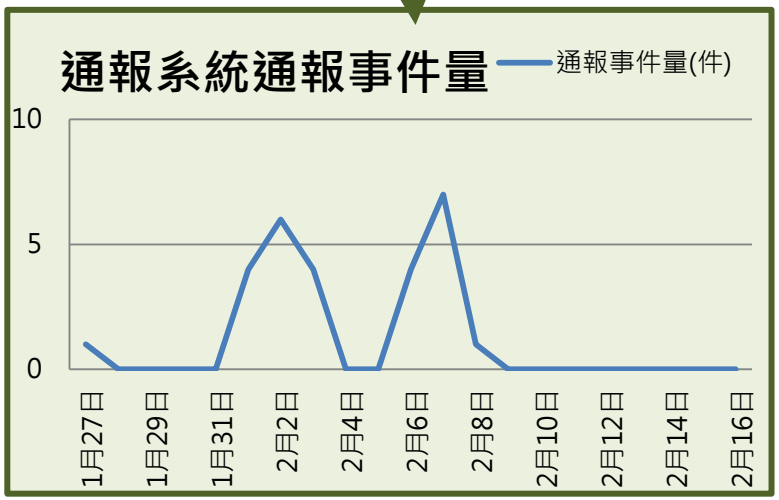
證券業者遭DDoS勒贖事件(1/2)

1月27日，凱基證券收到名為Armada Collective集團的DDoS勒索信件，要求支付比特幣，否則將於2月1日發動DDoS攻擊，但實際上未發動攻擊。2月2日，證交所接獲大展證券公司通報發生網路下單系統中斷情事，並收到相似勒索信件，正式拉開本次攻擊事件序幕。

由電信業者提供資訊顯示，DDoS攻擊跡象已趨緩；監控機制亦顯示證券期貨業者網站系統除例行維修外未發生大規模異常狀況；兼之業者陸續解除通報，均指出本次攻擊事件已逐漸平息。

警告階段(1/27-2/2) → **發起階段(2/3-2/8)** → **平息階段(2/9~)**

陸續接獲共21家證券期貨業者(包含：15家證券業者、4家期貨業者、1家投信公司、1家投顧公司)通報收到相似之勒索信件，部分業者之入口網站、電子下單系統遭受攻擊，致發生運作異常。



證券業者遭DDoS勒贖事件(2/2)

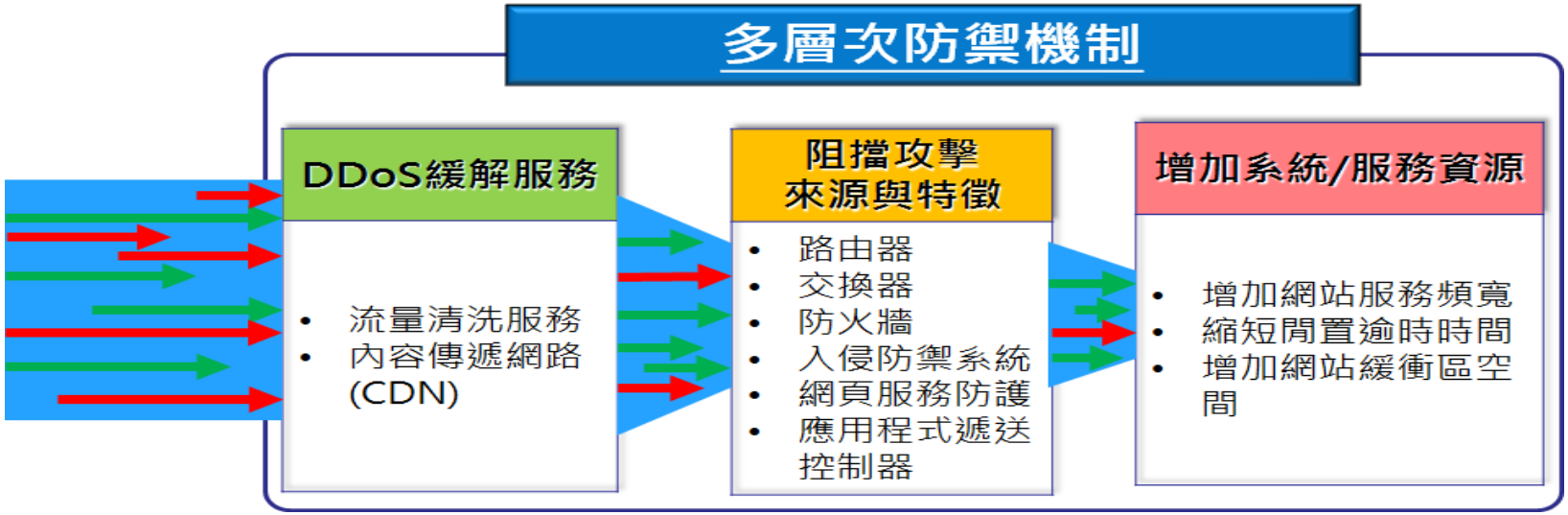
應變與改善

成立緊急應變專案小組

「證券期貨市場資通安全通報系統」

- 機關應檢視內部網路架構與需求，設置**多層次防禦機制**

建議



遠東商銀SWIFT入侵事件

- 遠東商銀於106年10月3日上午發現電腦遭到惡意程式攻擊，駭客假冒遠銀名義透過SWIFT(環球銀行金融電信協會)組織系統發出7個電文，使遠銀境外分行之外幣帳戶依據電文內容，執行付款至斯里蘭卡、柬埔寨及美國等地銀行帳戶，遭駭金額計有美金6,010萬4,000元，折合新臺幣約18億餘元
- 經由迅速通報、聯合防護等措施，目前合計美金5,800萬元已返回遠銀帳上，194萬8,000元已被凍結，損失金額已降至美金15萬6,000元(約新台幣468萬餘)，實際損失不到0.3%，並於駭客提款當地緝捕人犯到案
- 本院於106年10月18日邀集遠銀、金管會及刑事警察局召開本案第1次專案會議，充分掌握本案應處作為，近期將召開第2次專案會議研商持續防範措施

大綱

- 政府資安推動機制
- 現階段資安情勢分析
- 未來策進作為

未來策進作為-三度防護

- 廣度
  - 透過資安旗艦計畫及前瞻基礎建設計畫，建構政府機關、關鍵基礎設施及地方政府區域治理等多重資安聯防體系
  - 結合大數據分析及人工智慧技術(AI)，預測資安攻擊趨勢
- 深度
  - 強化內外網縱深防禦，持續提升人員資安防護意識，減少誤開郵件及駭客入侵情事
  - 擴大資安稽核及資安健診之檢測方式，主動發現並改善問題
- 速度
  - 各機關策訂資安計畫，落實辦理各項資安應辦事項，提升資安事件偵測及反應速度
  - 透過資安通報及網路攻防等各項演練，提升資安事件應變速度

報告完畢
敬請指教