# 資通安全網路月報（113年2月）

資通安全網路月報(113年2月)

**<近期政策重點>**

機關接獲資通訊產品漏洞資訊，應優先檢視是否使用受影響之資通訊產品，並參考CVSS等級及「已知被利用漏洞（Known Exploited Vulnerabilities，KEV）」列表，排定修補優先順序。（KEV係美國網路安全暨基礎設施安全局（CISA）公布被廣泛利用之資安漏洞）。上開資訊每週定期公布於國家資通安全研究院網站(https://s.moda.gov.tw/dc7RSEWgcvrQ)，請各機關逕行參考運用，尚未修補完成或因故無法修補時，應先運用如控制存取、隔離設定、降權及加強監控等控制措施，以維護資通安全。

跨機關協作使用共用檔案目錄時，應注意存取權限之安全性設定，請以最小揭露原則，設定僅特定帳號才可透過連結檢視及編輯該目錄之檔案，避免知道連結的所有人皆具存取權限，以降低資安風險。

**<整體威脅趨勢>**

事前聯防監控

本月蒐整政府機關資安聯防情資共4萬7,912件（較上月減少1萬4,666件），分析可辨識的威脅種類，第1名為資訊蒐集類(29%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(21%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(15%)，大多是系統遭未經授權存取或取得系統/使用者權限，統計近1年情資數量分布詳圖1。

經進一步分析聯防情資，發現近期駭客利用大學系所人員之電子郵件帳號，偽冒監察院名義，寄送含惡意附檔之社交工程電子郵件給政府機關人員，企圖誘騙收件人開啟惡意附檔以植入後門程式，並竊取電腦機敏資訊，相關情資已提供各機關聯防監控防護建議。

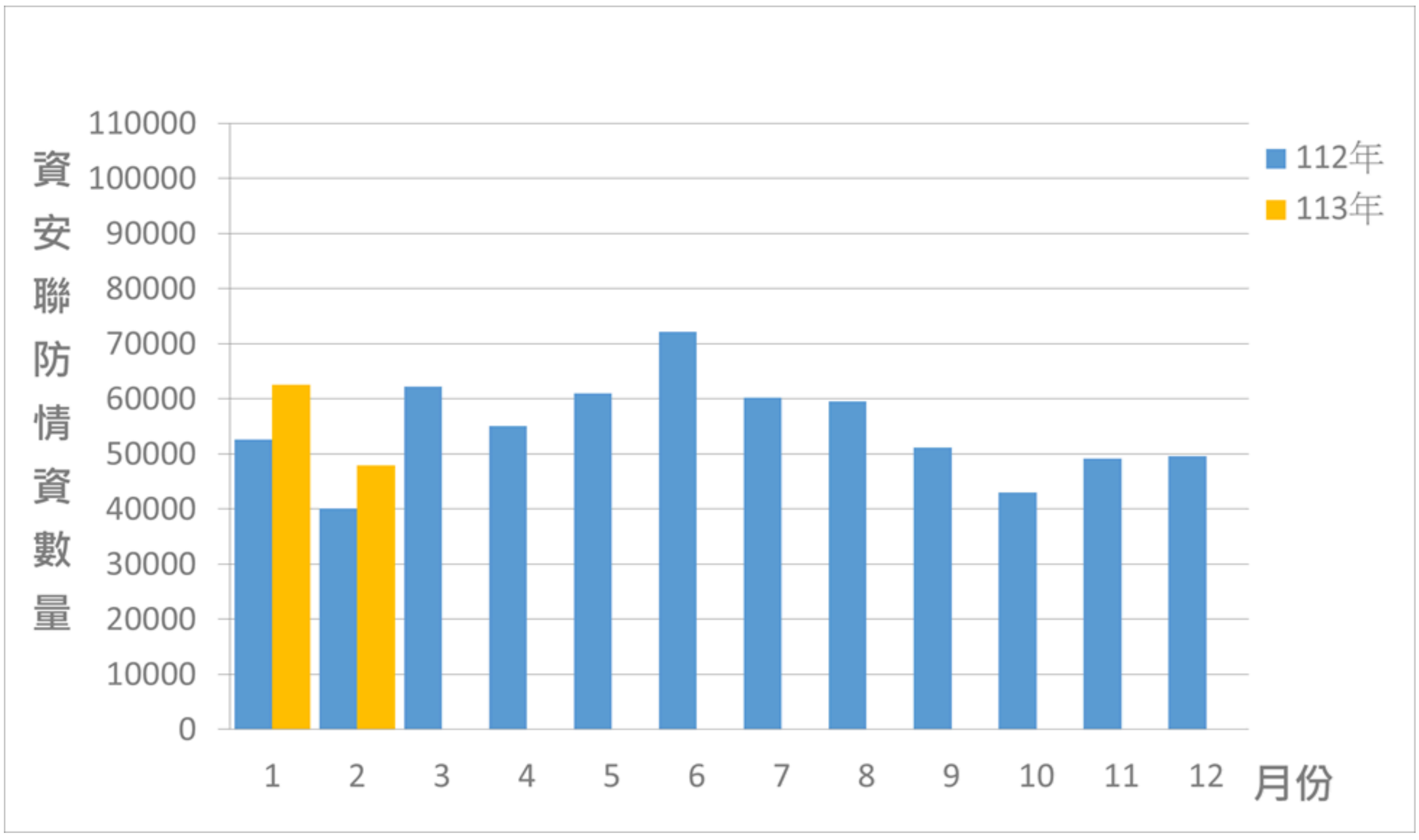


圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共73件（較上月減少6件），與去年同月通報件數無明顯差異。本月因某機關機房火警通報資安事件，造成自身與其部分相關機構對外網路中斷，其所致之服務影響事件佔本月「設備問題」類型之62.50%，近1年資安事件通報統計詳見圖2。

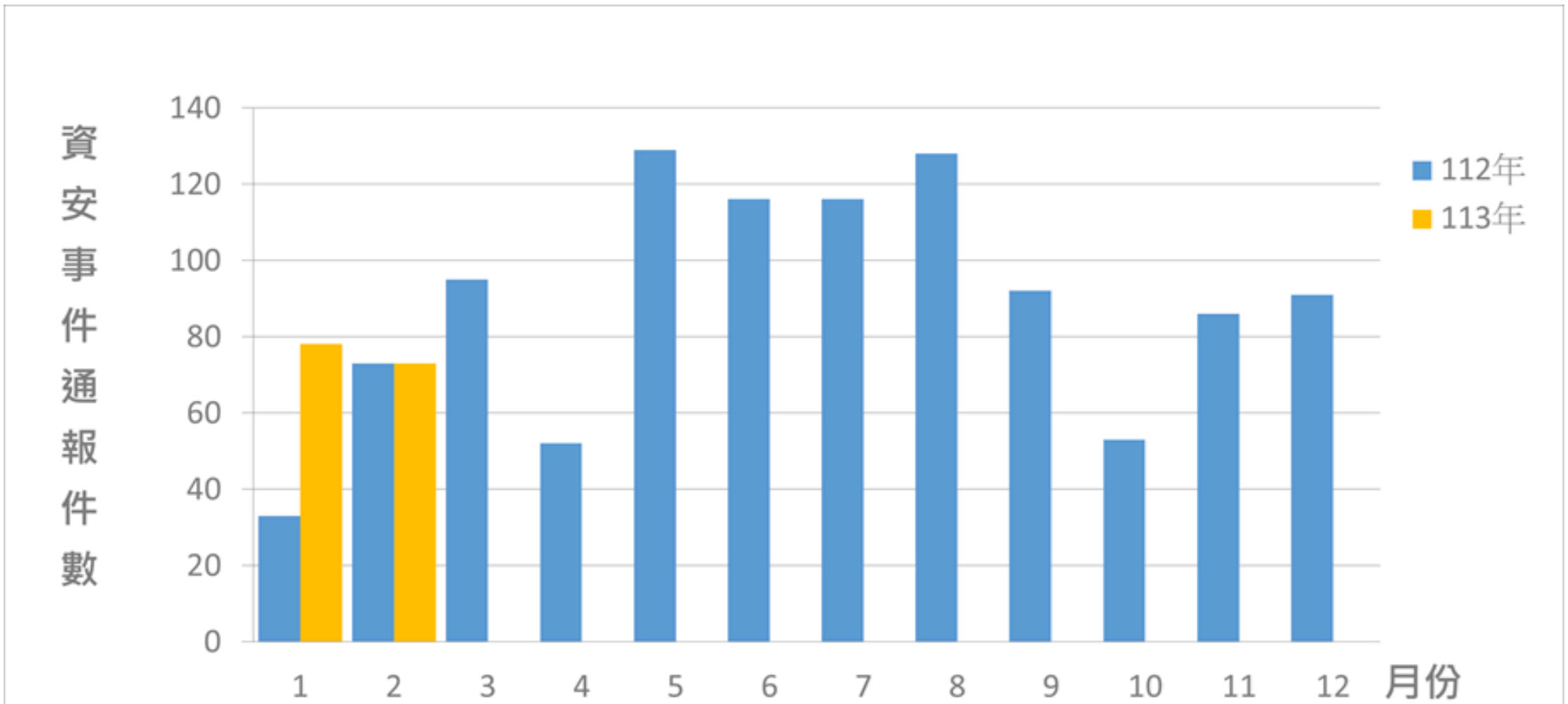


圖2 資安事件通報統計

事後資訊分享

部分政府機關之網域名稱系統(Domain Name System,DNS)採用向上集中方式，因其網路與DNS服務主機之共構機房發生火警，導致內/外部網路服務中斷，切換至備援網路後，官方網站仍無法對外提供服務，經查係因服務提供機關之備援DNS未具有變更DNS指向功能，無法指定成其他DNS主機，故網站無法正常顯示，後續應檢討DNS備援機制，以避免類似情況發生。

**足資借鏡：**

政府機關為資源有效運用，多採用資訊向上集中架構，上級機關除提供資訊服務外，亦應確認備援機制之有效性，建議可辦理業務持續運作演練，採複合式演練情境，並納入與資通系統或服務相關之利害關係人，以全面檢視系統相關機制之完整性，同時確保在緊急狀況發生時，相關人員可快速採取因應作為。

**<國內外重點資安新聞>**

1. 滑手機也要顧資安 資安署：掌握4不6要就安心

   數位發展部資通安全署指出，手機及網路已深入日常生活，使用便利服務的同時，也要注意資安防護，掌握「四不六要」：不瀏覽可疑網站、不亂掃QR code、不連接可疑的Wi-Fi、不下載來路不明的軟體；要定期更新密碼、要備份資料與更新軟體、要關閉未使用的Wi-Fi等介面、要開啟加密防護連接、要刪除機敏資料、要對網路資訊存疑。

   此外，資安署已於「e等公務園＋學習平台」提供「行動裝置安全」、「使用APP安全」兩門課程，歡迎民眾線上學習，充實資訊安全知識。

   (資料來源：聯合新聞網)

2. 某廠商資訊系統遭加密攻擊，評估資料無外流疑慮

   某上市櫃大廠再爆資安事件，某廠商2月19日公告，資安系統遭到加密攻擊，第一時間阻斷加密源頭，資料無外流疑慮，也沒有遭到勒索，對營運無重大影響。該廠商立刻與外部資安諮詢公司合作，全面強化相關防禦機制、復原作業及資安政策，以保護資料安全及完整性。

   (資料來源：Yahoo 經濟日報)

3. 三、 釣魚簡訊誘入假網站，美日台45國萬筆個資外洩，警逮17人

   詐騙集團涉嫌架設假網站，發送釣魚簡訊，將被害人導入假網站輸入信用卡資訊，美、日、台等45個國家總計有1.2萬多筆信用卡個資外洩，其中台灣外洩個資有300多筆，35人被盜刷200多萬元。

   刑事局呼籲，「釣魚簡訊」詐欺手法行之有年，民眾收到此類簡訊時，應保持「零信任」警覺態度，若有任何疑問，可撥電話至警政署165反詐騙諮詢專線進行查證。

   (資料來源：自由時報)

**<資通安全長及資訊主管異動情形>**

彰化縣政府資訊主管於113年2月1日起，原由許宏基科長兼任，改由陳昌茂副處長兼任。

---

發布單位：資通安全署　　建立日期：2024-03-15　　更新日期：2024-03-19