資通安全網路月報（112年12月）

資通安全網路月報(112年12月)

<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4萬9,581件（較上月增加近500件），分析可辨識之威脅種類，第1名為資訊蒐集類(49%)，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(24%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(11%)，大多是系統遭未經授權存取或取得系統/使用者權限。另統計近1年情資數量分布詳見圖1。

經進一步彙整分析聯防情資資訊，發現近期駭客竊取受駭電腦之電子郵件資訊，包含民眾與某機關往來之電子郵件。駭客利用所竊取之民眾電子郵件內文或主旨做為誘餌，寄送含惡意附檔之社交工程郵件予機關人員，企圖誘騙機關收件人開啟惡意附檔以植入後門程式並竊取電腦資訊。相關情資已提供各機關聯防監控防護建議。

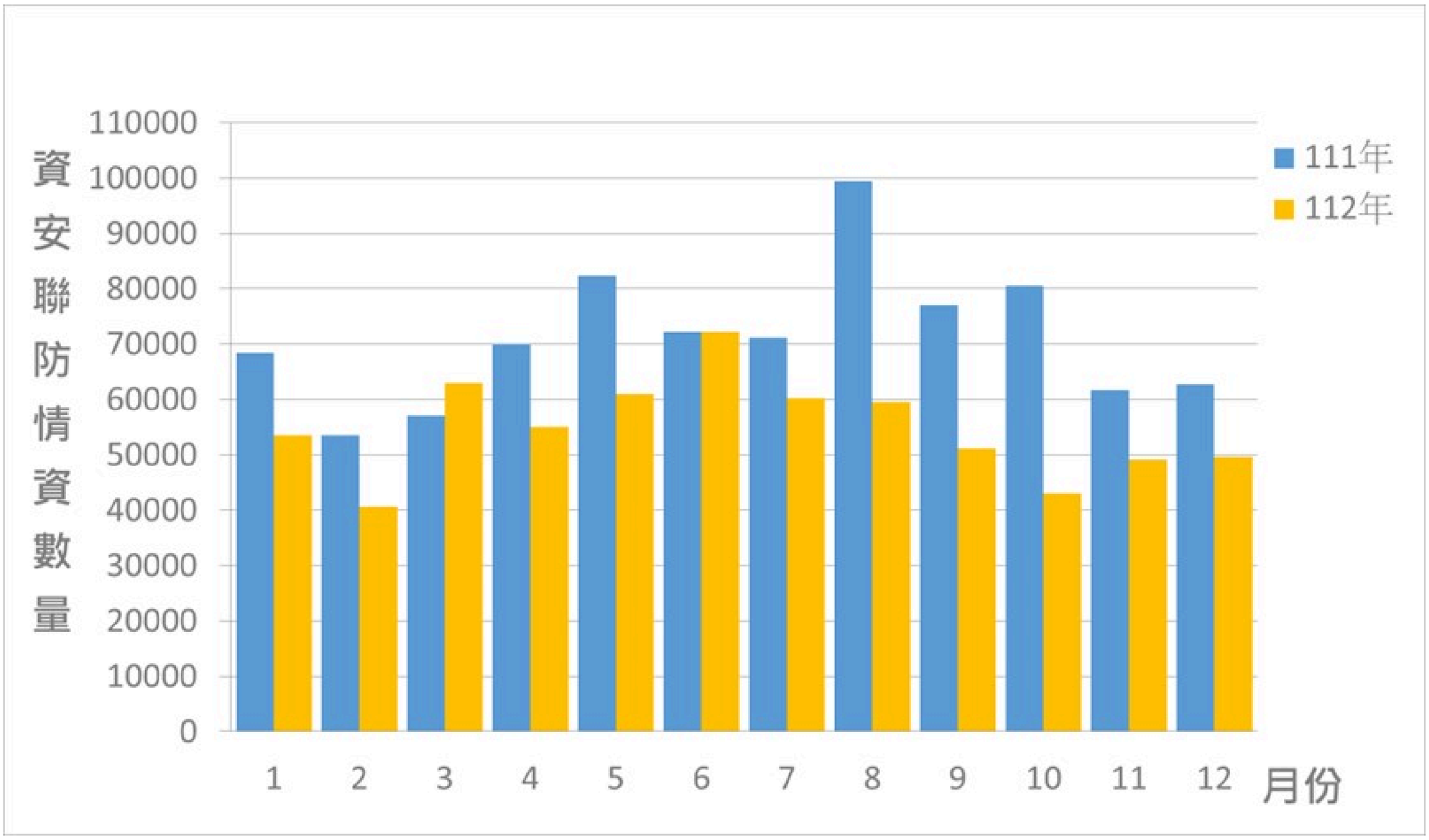

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共91件，較去年同月增加44.44%，研析偵測資訊發現，主要因多個機關資訊設備，嘗試下載惡意程式或產生符合惡意程式行為特徵之連線，占總通報數量49.45%。另近1年資安事件通報統計詳見圖2。

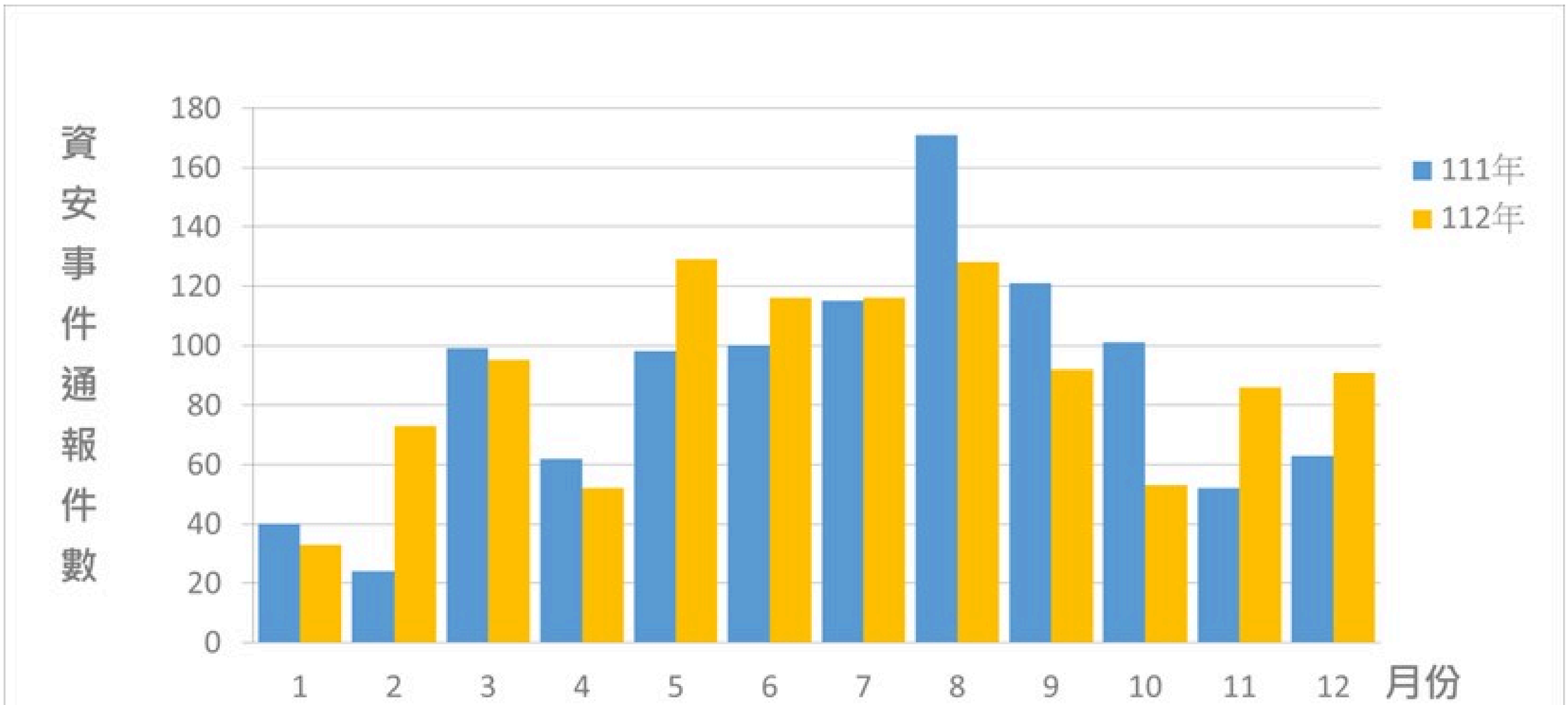

圖2 資安事件通報統計

事後資訊分享

上揭機關資安事件之通報，經查多為網路監視器之管理登入介面可於公開網路存取，使設備暴露於暴力破解與漏洞利用之風險，其中部分機關設備已受駭，對外連線至中繼站下載惡意程式；後續機關評估前述網路監視器無對外開放需求，故將設備斷網或限制僅供內部IP存取，以降低資安風險。

足資借鏡：

資訊設備管理介面對外開放，可方便管理人員即時遠端操控系統，惟設備存取權限未加以限制，駭客亦可透過暴力破解登入介面或利用漏洞入侵系統。此外，物聯網設備(如監視器與印表機等設備)易疏於更新，若對外開放存取，可能成為駭客主要攻擊的目標。建議機關在設定設備管理介面時，應加以限制其存取權限，僅允許內部IP存取，並評估搭配多因子驗證方式，以降低系統遭入侵之風險。

<國內外重點資安新聞>

1. 113年起高考三級新增「資通安全」類科

   鑑於資安業務需求迫切，考試院院會於112年12月28日通過公務人員高等考試三級考試暨普通考試規則修正案，自113年起高考三級新增「資通安全」類科，以滿足各機關對資安專業人才的需求，打造安全可信賴的數位國家，歡迎有志從事資通安全工作者踴躍報考。
   (資料來源：中央社，Yahoo，考試院官網)

2. 113年四技二專甄選納資安人才 名額增為136個

   行政院推動精進資通訊數位人才培育策略，逐步擴增國內公私立大專校院資通訊科系領域招生名額，113學年度共提供613名半導體、AI、機械領域系所擴充招生名額，包含136名資安人才，資安人才名額較112學年度增加12名。
   (資料來源：中央社)

<近期重要資安會議及活動>

1. 資安署於112年度12月25日召開「112年國家資安資訊分享與分析中心（N-ISAC）年會」，邀請相關會員分享近期資安威脅趨勢及事件實務案例，並安排模擬情資分享實作活動，以深化N-ISAC會員信任關係，促進各領域交流分享掌握情資，進而提高國家整體資安防護能量。
2. 資通安全管理法修正草案業於112年11月20日預告期滿，資安署刻彙整公共政策網路參與平臺（眾開講）及修法說明會獲得之回饋意見，調修法案相關內容，後續將送行政院進行法案審查後，送請立法院審議。

<資通安全長及資訊主管異動情形>

無

發布單位：資通安全署　　建立日期：2024-01-15　　更新日期：2024-01-11