資通安全網路月報（112年3月）

資通安全網路月報（112年3月）

<近期政策重點>

一、完善法規實務運作，數位發展部已初步擬具資通安全管理法草案，於112年3月20日請各機關彙整所屬、所轄及所管提供草案修正建議，請各機關於文到14日內提供意見，以利修法更臻周延完善。

二、請各機關112年5月26日前至資通安全作業管考系統(https://spm.nat.gov.tw/)完成111年資通安全維護計畫實施情形提報作業，後續並就所屬公務機關(含學校)之資通安全維護計畫實施情形進行檢視及審閱。

<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63,034件，分析可辨識的威脅種類，第1名為入侵嘗試類(34%)，主要是嘗試入侵未經授權的主機；其次為入侵攻擊類(28%)，大多為系統遭未經授權存取或取得系統/使用者權限；以及資訊蒐集類(26%)，主要係透過掃描、探測及社交工程等攻擊手法取得資訊。另統計近1年情資數量分布詳圖1。

經進一步彙整分析聯防情資資訊，發現近期駭客利用高風險漏洞CVE-2022-3995進行攻擊活動，該漏洞為網通設備存在任意文件寫入漏洞(Arbitrary Write Vulnerability)，攻擊者無需通過身分認證即可攻擊該設備。國家資通安全研究院已觀察到外部惡意IP持續對政府機關設備進行攻擊，主要分布在綜合行政類與內政衛福勞動類機關。相關情資已提供各機關聯防監控防護建議。

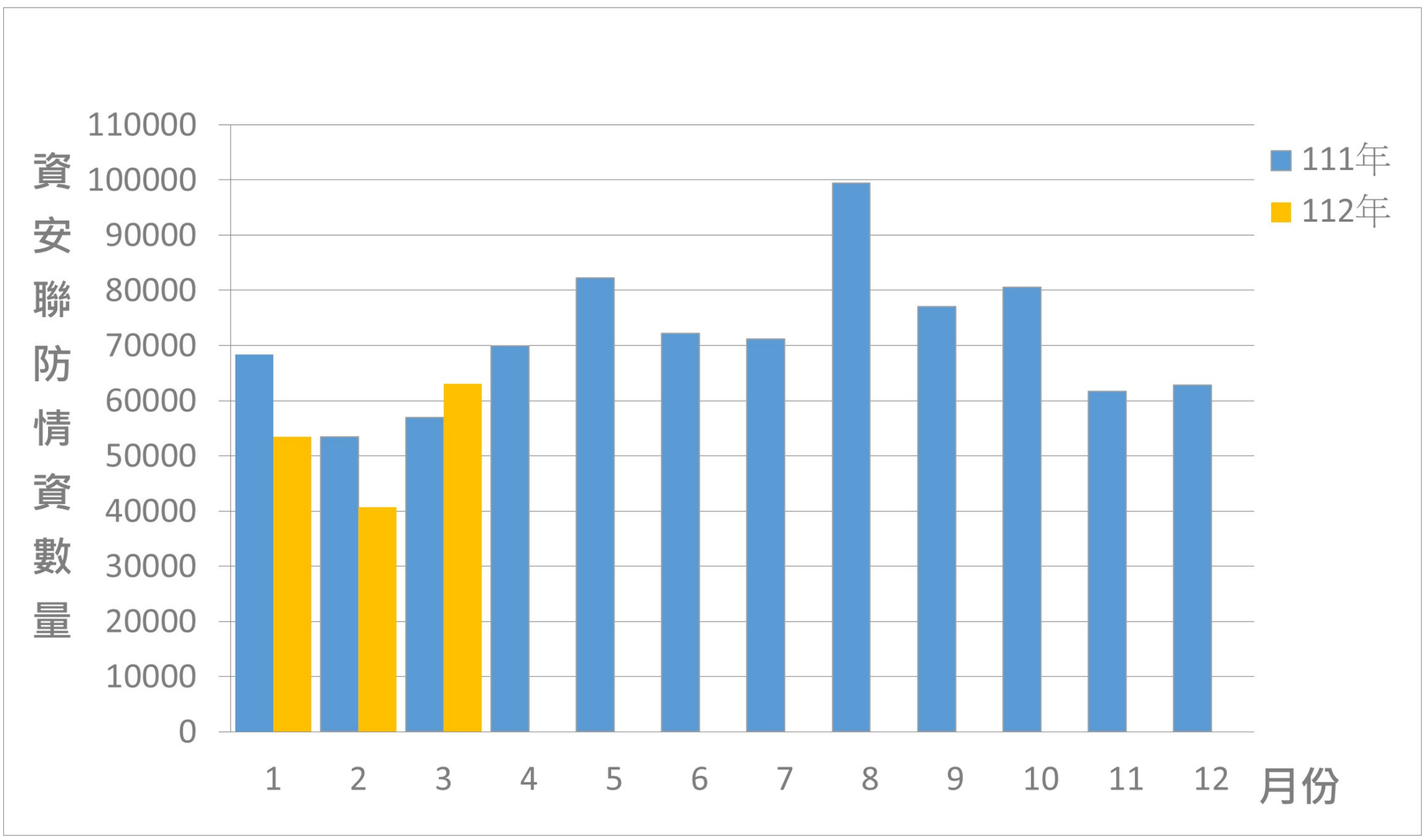

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共95件，較上個月增加30.14%，因本月多個機關遭阻斷服務攻擊，影響對外服務緩慢或中斷，占總通報數量17.89%。另近1年資安事件通報統計詳見圖2。

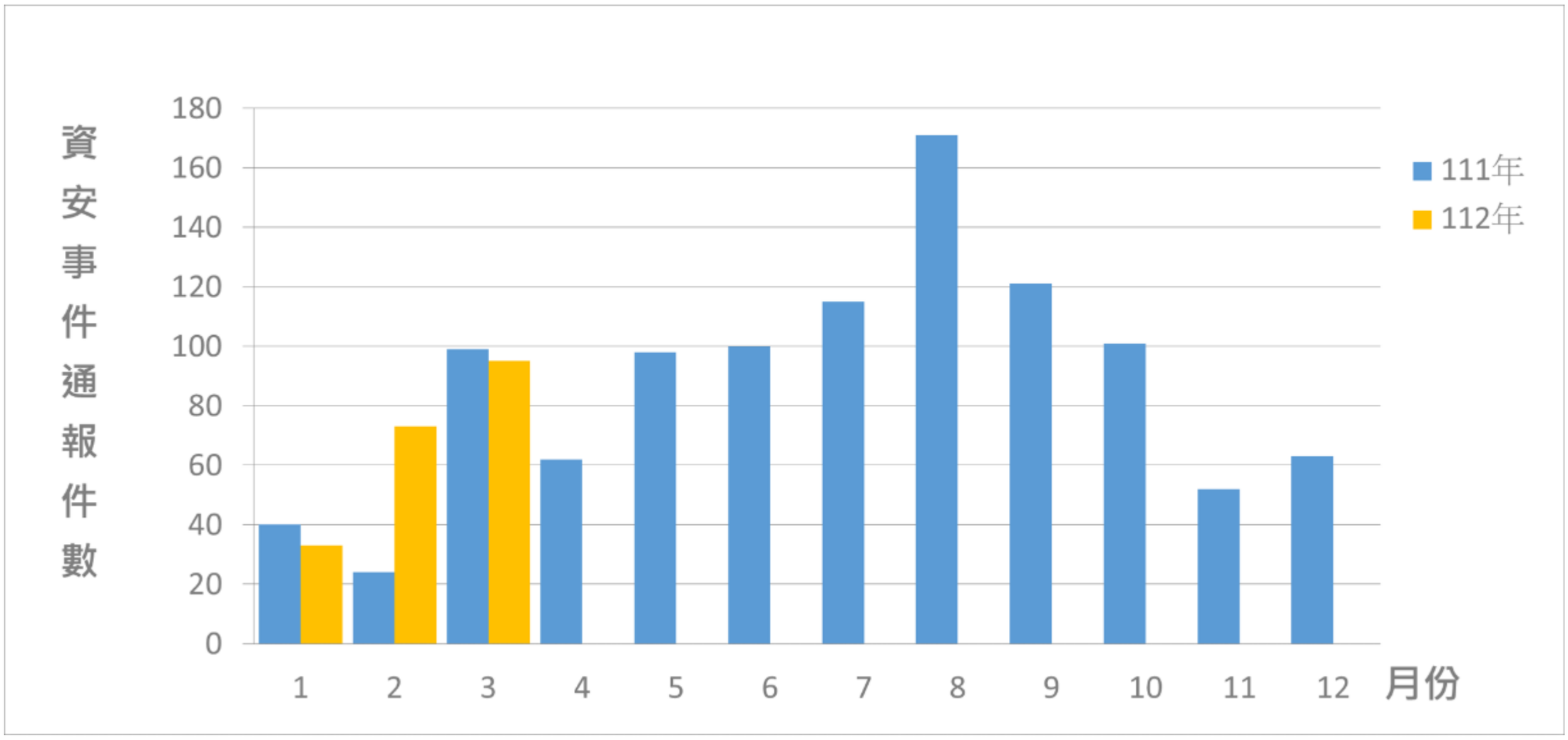

圖2 資安事件通報統計

事後資訊分享

本月某機關發現網站WordPress Plugin目錄遭植入惡意程式，經查係因網站維護商為方便維護網站，於維護當日調整該目錄權限設定為所有人皆可寫入，惟完成維護作業後，未將該目錄權限復原，造成當日晚間遭駭客逕行存取並植入惡意程式。機關已恢復目錄限制存取、清查確保未有其他惡意程式殘留，並加強監督廠商維運作業，以避免類似情形再次發生。

足資借鏡：
機關網站委由廠商維運已成普遍趨勢，然而廠商若為求維運方便，將網站或環境設定調整為未符資安規範，可能導致網站存在資安疑慮。機關應依資通安全管理法施行細則第4條落實委外監督管理之責，確保資安防護措施之有效性；同時依資通安全責任等級分級辦法附表十資通系統防護基準，規範存取控制採最小權限原則，僅依機關業務需求，開放指派任務所需之授權存取，降低因廠商疏忽所肇生之資安風險。

<國內外重點資安新聞>

一、政府全民普發6千元，傳出有詐騙集團架設冒牌網站行騙
我國政府實施全民普發現金6千元政策，但傳出有人註冊名稱相似網域，架設名稱雷同之網站，意圖騙取民眾個資的情況。
財政部於3月18日發布臉書貼文表示，正確網址應為https://6000.gov.tw，並呼籲民眾要提高警覺。
（資料來源：iThome、財政部官網）

二、館藏數位圖檔傳出遭到中國盜賣，起因是將檔案存放在對外提供服務的伺服器
機關表示本案係肇因於承辦人建檔過程，將資料儲存於可提供對外服務之伺服器中，致有心人士得以使用工具軟體，讀取局部的高階圖檔加以拼接存取，致數位圖檔被盜取。
機關於111年底已改採內部封閉式儲存設備，阻絕人為操作可能外流之風險，並打算透過法律途徑要求淘寶網、書格網等平臺下架，或是提出訴訟以維護權益。
（資料來源：鏡週刊）

<近期重要資安會議及活動>

行政院人事行政總處與數位發展部資通安全署，於112年3月27日聯合辦理第1梯次「資安長共識營」，邀請專家跟機關資安長們分享從烏克蘭得到的啟示、資安長的自我定位及威脅角度看防禦框架等議題，交流機關強化資安風險管理作業。

<資通安全長及資訊主管異動情形>

中央銀行資通安全長於112年3月6日起，原由陳南光副總裁兼任，改由嚴宗大副總裁兼任。

發布單位：資通安全署　　建立日期：2023-04-13　　更新日期：2023-04-13