資通安全網路月報（112年4月）

資通安全網路月報（112年4月）

<近期政策重點>

- 近期發現機關刷卡機因暴露於外網，且未納入機關內部資安防護範圍內，導致該設備遭駭客非法入侵、植入惡意程式並連線至惡意中繼站，造成資安防護破口。請機關落實盤點物聯網設備(如刷卡機、影印機、CCTV等)，提供妥適資安防護措施，以降低資安風險。

- 政府組態基準(GCB)新增項目(如作業系統MicrosoftWindows Server 2019、瀏覽器Edge、應用程式Word 2019等)已公告於國家資通安全研究院網站，請資通安全責任等級A級與B級之公務機關導入前揭GCB項目，以持續強化資通設備之安全性設定。

<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55,091件，分析可辨識的威脅種類，第1名為資訊蒐集類(39%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵攻擊類(33%)，大多是系統遭未經授權存取或取得系統/使用者權限；以及入侵嘗試類(18%)，主要係嘗試入侵未經授權的主機。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，發現近期駭客偽冒某醫院郵件帳號，利用健康檢查報告相關主旨，寄送社交工程郵件攻擊政府機關人員。經分析，駭客註冊與某醫院網站相似的域名並放置惡意壓縮檔案，再以偽冒某醫院郵件帳號寄送檢查報告做為誘餌，誘導收件人點擊郵件內的連結並下載惡意壓縮檔，藉此達到植入後門程式以竊取機敏資訊的目的。相關情資已提供各機關聯防監控防護建議。

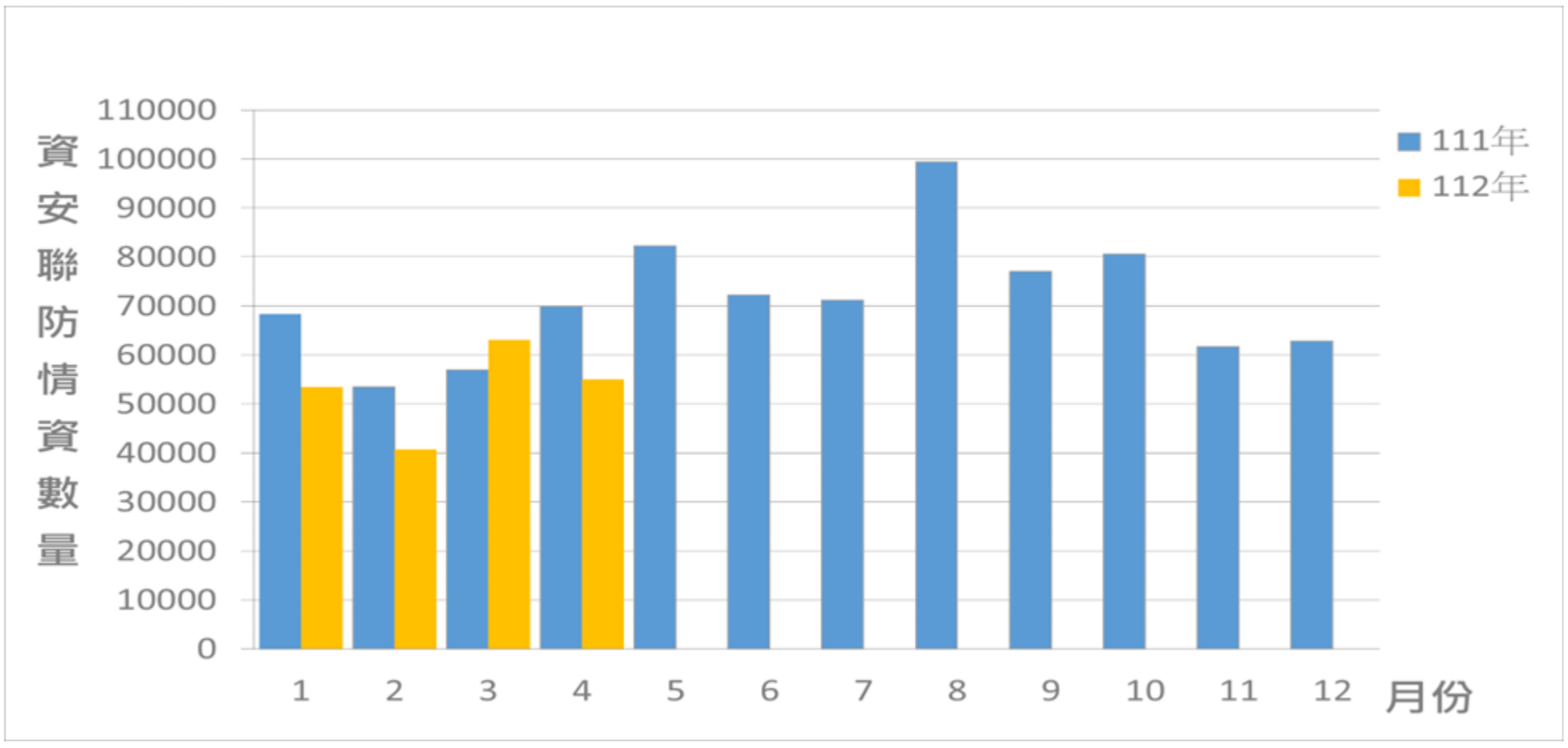

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共52件，較上個月減少45.26%，主要是上個月通報阻斷服務事件較多，本月則以非法入侵事件為主，占總通報數量55.77%。另近1年資安事件通報統計詳見圖2。

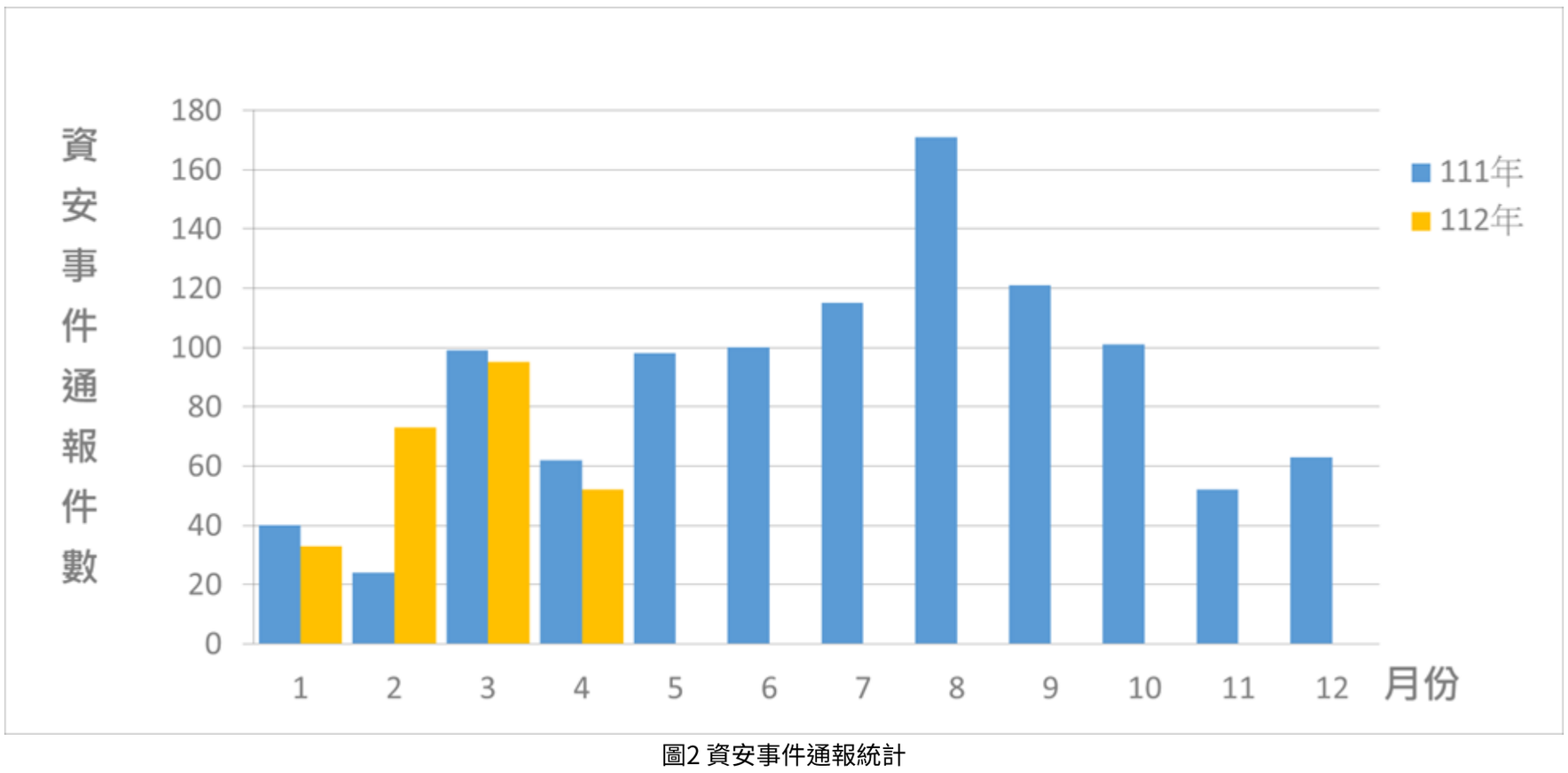

圖2 資安事件通報統計

事後資訊分享

本月發現某機關資訊設備對外進行異常連線，經機關調查後發現其受駭設備是舊版網站，該網站未於新版網站上線後下架，且未妥善管理與維護，致遭駭客利用SQL Injection漏洞入侵成功。機關現已將舊版網站下架，亦清查內部網站使用情況，降低可能的潛在資安風險。
足資借鏡：
資通系統有其生命週期，可能因資通環境或業務需求等議題改版更新，惟舊版系統下架常遭忽略，尤其是委外建置於供應商處的系統，有可能因此潛藏資安風險，建議機關訂定並落實網站上/下線相關作業程序，定期稽查機關對外服務網站使用情形，檢視與移除未使用的網站資料，避免衍生相關資安疑慮。

<國內外重點資安新聞>

- 一、行政院通過個人資料保護法修正草案，設置個資保護獨立監督機關並提高個資外洩罰責

行政院於112年4月13日通過國家發展委員會擬具的「個人資料保護法」第1條之1、第48條、第56條修正草案，將函請立法院審議。修正內容包含增訂個人資料保護法的主管機關「個資保護委員會」，並提高罰款的金額，如屬情節重大，最高可處1千萬元罰鍰，並令其改正，如未改正可按次處罰。

在個資保護獨立監督機關成立前，行政院請各中央目的事業主管機關加強執法，並呼籲企業、民間提升資安及個資保護，共同努力維護國人的個資安全。

(資料來源：行政院官網)

- 二、某機關火警初判機器負載量過大釀災

某機關112年4月24日晚間8時許傳出火警，係因內部機器設備負載量過大釀災，該機關表示相關資料都有電子備份，不影響工作運行。
(資料來源：公視新聞網)

- 三、金融機構供應鏈風險自律規範112年4月上路

銀行公會日前就銀行資訊系統委外作業，發布「金融機構資通系統與服務供應鏈風險管理規範」，明定五大類銀行資訊系統委外時，對銀行資訊系統開發、建置或維運委外作業規範，及銀行雲端委外服務之新規範等。
ATM等顧客自動化服務或營運重大影響的第一類系統，從112年4月10日開始適用，其餘第二、三類系統則有1年緩衝期，113年4月開始適用。
(資料來源：iThome)

<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4月17日聯合辦理第2梯次「資安長共識營」，邀請專家對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從駭客思維談資安等議題，並透過座談強化資安風險管理作業。

<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：2023-05-15　　更新日期：2023-05-23