資通安全網路月報（113年1月）

資通安全網路月報(113年1月)

<近期政策重點>

近來發現部分同仁使用公務信箱註冊於非公務網站，致遭帳密外洩案例，重申公務信箱勿註冊於非公務網站或外部服務，且不可使用相同通行碼，避免外部主機遭駭侵後，相關帳號、密碼及使用者個資等資料都將一起曝險；另使用者電腦系統及軟體亦應定期更新及掃毒，以維資通安全。

<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6萬2,578件（較上月增加1萬 2,997件），分析可辨識的威脅種類，第1名為資訊蒐集類(31%)，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(23%)，主要是嘗試入侵未經授權的主機；以及資訊內容安全類 (15%)，大多是系統遭未經驗證存取或影響資訊機敏性。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，發現近期駭客利用微軟 Outlook電子郵件服務，針對政府機關人員寄送主旨為「投訴政府人 員不作為」，內含惡意附檔之社交工程電子郵件，企圖誘騙收件人開 啟惡意附檔以植入後門程式，進而竊取機敏資訊，相關情資已提供各 機關聯防監控防護建議。

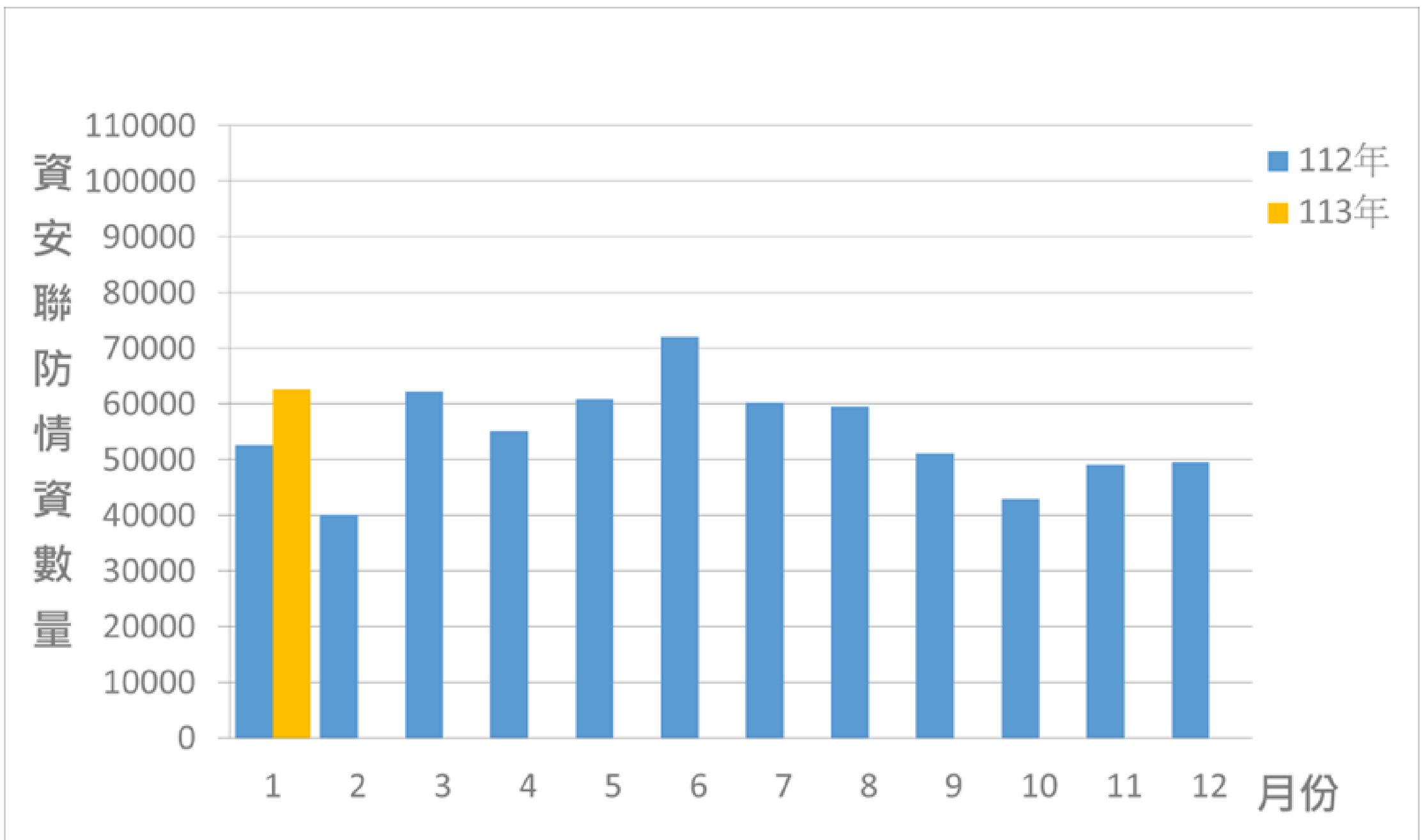

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共79件（較上月減少12件），主要為多個機關資訊設備符合惡意程式特徵之連線或疑似下載惡意程式，占總通報數量58.23%。另近1年資安事件通報統計詳見圖2。

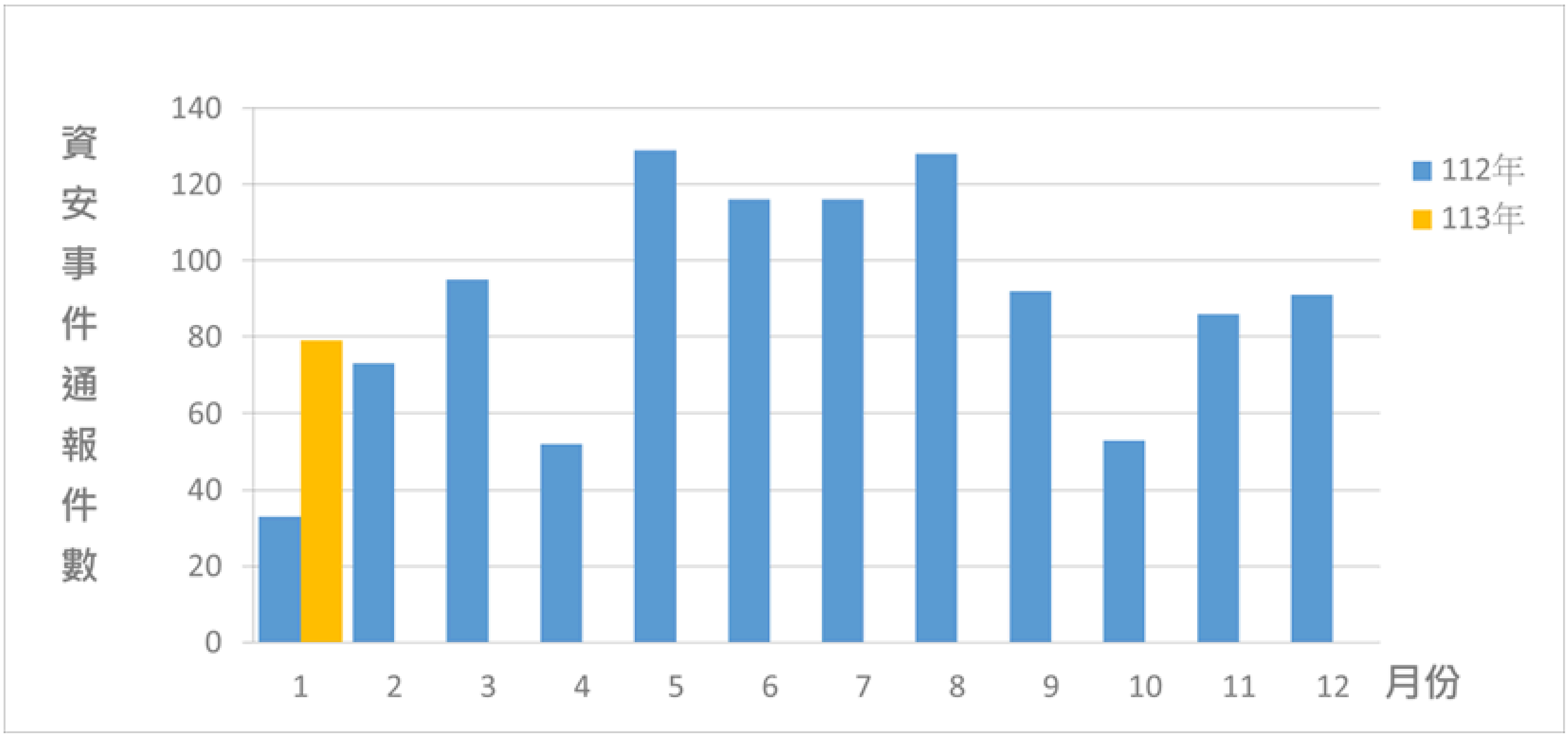

圖2 資安事件通報統計

事後資訊分享

某機關端點偵測軟體(EDR)偵測發現其對外服務網站遭嘗試上傳後門程式，經機關調查發現網站後台帳號密碼為弱密碼，以致遭駭客破解後成功登入，並嘗試上傳惡意程式。調查過程中亦發現，該帳號密碼自廠商交付後，未曾執行密碼變更作業；機關已停用該帳號，並另行建立新帳號，採用複雜性密碼(長度至少8碼，含英文大寫、小寫、數字及特殊符號)，同時設置僅限單位內部可存取之管理介面。

足資借鏡：

機關應建立密碼變更機制，並套用至內部所有系統，首次登入系統時，應立即執行密碼變更作業，採用複雜性密碼，避免使用預設密碼，導致外洩風險。此外，網站後台未加限制存取來源，恐利駭客透過工具找到後台登入頁面，執行暴力破解作業。機關應針對後台登入頁面限制存取來源，僅允許內部IP存取，並套用政府組態基準(Government Configuration Baseline，GCB)之帳戶原則，如定期變更密碼、採用複雜性密碼及設定帳戶鎖定閾值(嘗試登入錯誤次數)等，以降低系統遭入侵風險。

<國內外重點資安新聞>

1. 某公司旗下的半導體設備廠網頁遭到攻擊

   國內某半導體設備廠傳出遭到網路攻擊，駭客直接竄改該公司的網站並公布此事，揚言若不付錢，將公布所有客戶資料。

   該公司表示部分資訊系統遭到攻擊，初步評估對運作無重大影響。在偵測到攻擊行動的當下，已全面啟動相關防禦機制及復原作業，並協同外部資安公司進行全面掃描、檢測、資料復原，但未進一步說明遭遇之攻擊類型。

   (資料來源：iThome)

2. 112年代發統一發票獎金入帳異常，某銀行因系統轉換作業不夠完善遭罰400萬元

   某銀行112年6月中進行統一發票獎金入帳，因資訊系統轉檔時，金額欄位移位入帳金額多2個零，造成3萬5,952筆異常入帳，受影響客戶共142戶。金融監督管理委員會針對該銀行未對資訊系統轉換作業建立完善客戶權益保護措施、未確實執行資訊系統轉換作業、未落實重大偶發事件通報程序，以及查核報告未能完整提供事件過程等4項缺失，依銀行法核處罰鍰。

   (資料來源：iThome)

3. 通訊診察治療新辦法113年7月1日實施，強化資安為醫療照護服務要項

   衛生福利部於113年1月22日發布修正通訊診察治療辦法，擴大特殊情形病人適用範圍，增加得以通訊方式提供的醫療服務項目，運用通訊及數位科技來提升醫療照護效能及可近性，並同時強化資通安全規範等事宜。

   (資料來源：CTIMES)

4. 俄羅斯駭客入侵！某公司證實：領導層電郵帳戶遭駭

   某公司在113年1月19日證實被俄羅斯駭客組織Midnight Blizzard使用密碼噴灑（password spraying）攻擊手法成功入侵，致該駭客組織可以存取該公司部分電郵帳戶。該公司仍在聯繫帳戶遭到存取的員工，不過並未對外透露，有多少帳戶受到影響。

   password spraying攻擊通常針對擁有大量使用者帳戶的大型企業組織，攻擊者可以透過各種方式獲取用戶帳名列表，例如購買黑市數據或網路釣魚攻擊。如果該些帳戶使用常見的密碼，則攻擊成功的可能性就會增加，或組織沒有限制使用弱密碼或使用多因素身份驗證機制，亦會提升攻擊成功的可能性。

   (資料來源：INSIDE)

<近期重要資安會議及活動>

1. 數位發展部資通安全署業於113年1月15日、22日辦理「資安主管資安治理研習」，邀請專家學者分享新興資安威脅與防護思維及資安政策與治理相關資訊，並邀請財政部資訊中心及臺北市政府資訊局分享紅隊演練經驗，期透過本次活動提升資訊（資安）主管資安知能，強化政府資安防護及應變能力。
2. 為協助政府機關導入優質民間資安服務，強化資安防護能力，數位發展部資通安全署委由國家資通安全研究院辦理112年度針對18家資安服務廠商之服務能量及專業技術進行評鑑，結果已公布於該院官網，提供各機關作為遴選資安服務廠商之參考。

<資通安全長及資訊主管異動情形>

外交部資通安全長於113年1月22日起，原由李淳政務次長兼任，改由謝武樵政務次長兼任。

客家委員會資訊主管於113年1月2日起，原由吳克能處長兼任，改由陳瑞榮處長兼任。

衛生福利部資訊主管於113年1月17日起，原由龐一鳴處長兼任，改由李建璋處長兼任。

發布單位：資通安全署　　建立日期：2024-02-15　　更新日期：2024-02-07