108 年國家資通安全情勢報告

行政院

中華民國 109 年 6 月

目次

壹、依據及目的

資通安全管理法(以下簡稱資安法)業於 108 年 1 月 1 日正式施行，本院依據資安法第 5 條規定，公布「國家資通安全情勢報告」。

本報告藉由研析 108 年全球資通安全威脅情勢及政府機關所遭受之資通安全威脅，研擬相關防護建議供各政府機關作為精進資安防護作為之參據，並增納關鍵基礎設施之資安情勢以強化其資通安全防護能量。本院期望藉由本報告之公布，除讓各界了解公部門所面臨之資安威脅外，亦期能提升各界之資安意識，透過公私協力，共同提升國家整體資安防護能量。

貳、108 年全球資安威脅情勢概要

依據世界經濟論壇(World Economic Forum， WEF)「2019 年全球風險報告」指出，在科技風險類別中，「資料欺詐或盜竊」與「網路攻擊」風險發生可能性分別高居第四名與第五名。相較於 107 年，資料欺詐或盜竊排名已超過網路攻擊，顯示機敏資料包含個人資料等成為攻擊目標的趨勢正日益增長。另就衝擊性而言，網路攻擊與關鍵基礎設施中斷，皆在排名前十名內，相關影響仍不容小覷。

經研析 108 年全球網路攻擊趨勢發現，目標式勒索軟體攻擊日益劇增，該攻擊手法預計在 109 年將有增無減，鑒於勒索軟體猖獗所帶來的嚴重影響，企業組織投保網路險意願亦隨之增加，此一趨勢將從 108 年延續到 109 年；在網路釣魚攻擊趨勢部分，其管道除藉由電子郵件外，109 年將會有更多駭客利用簡訊、社交媒體與遊戲平台來發動相關攻擊。在未來駭客只要願意付錢就能輕易買到最新行動惡意程式，且行動平台上網路釣魚攻擊也會越精細且越來越有效率；隨著 5G 時代來臨，市場上將出現越來越多的物聯網(Internet of Things, IoT)裝置，相關資安風險也會隨之升高；另一個 5G 相關議題則是因資料量爆增，所衍生之隱私保護與資料外洩風險，以下綜整 108 年全球重大網路攻擊事件如圖 1，並說明如下：

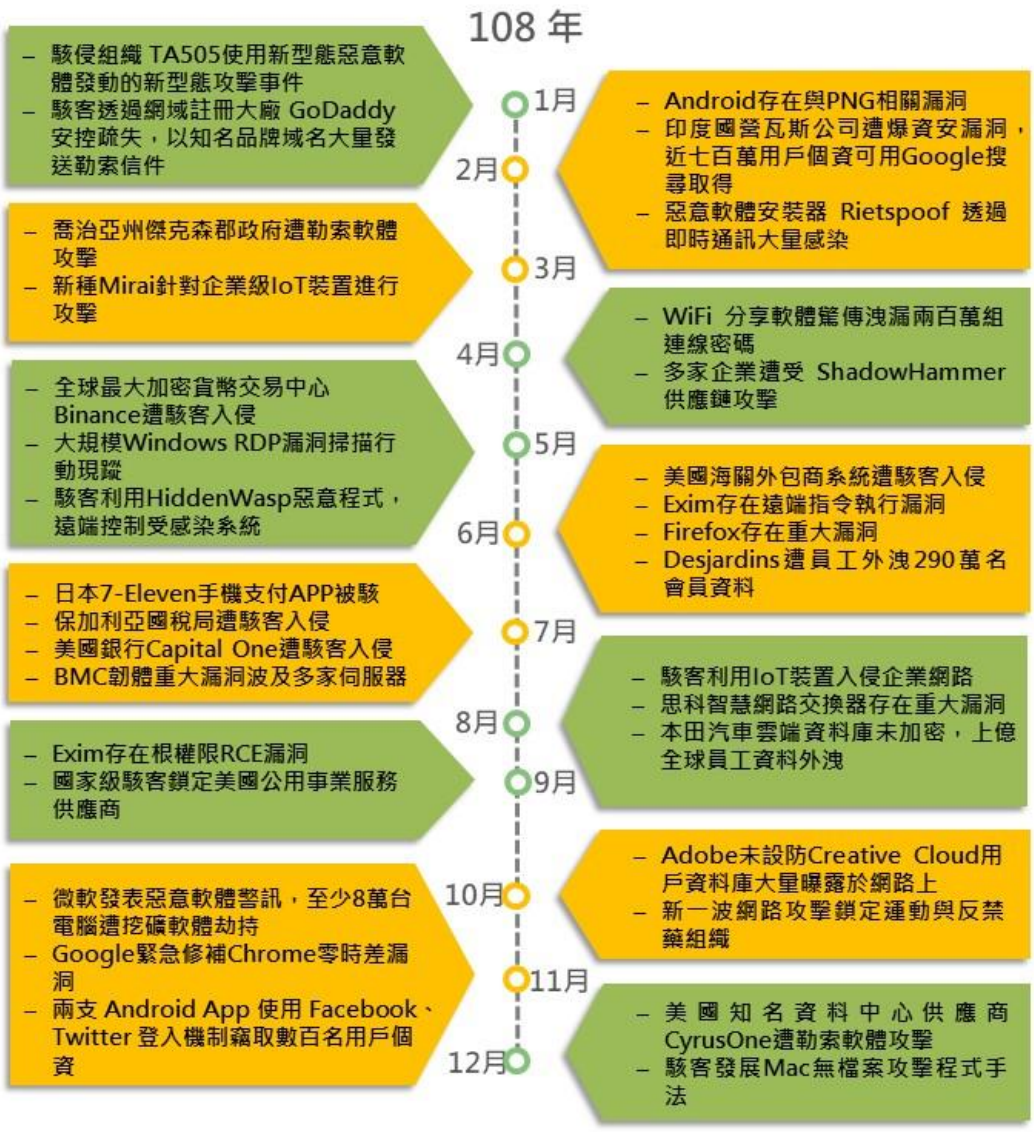

圖 1 108 年全球重大網路攻擊事件

一、個人資料外洩情形白熱化

個人資料外洩已成為現今資安事件相當普遍的狀況，由於使用者資安意識的不足，包含使用弱密碼、任意瀏覽或連結不明網站及開啟不明郵件檔案等，都造成資料外洩攻擊事件層出不窮。此外，現今有許多公司將系統移轉到雲端，惟未注意安全存取權限設定，意外洩露公司的資料庫或伺服器。因此個人資料外洩來源不僅可能來自於外部駭客惡意攻擊，更有些個人資料外洩來自於內部意外或惡意地洩露。

例如 108 年第 4 季某國際科技大廠發生員工竊取客服資料庫內容事件，顯示企業面臨更加險峻的內部威脅(Insider Threat)，該科技大廠於 11 月 5 日在官方部落格坦承，經查發現員工竊取客服資料庫內容，販賣給不知名犯罪組織牟利，影響近 12 萬名用戶。而此次事件引起內部注意的原因，係該公司於 108 年 8 月發現不少使用該公司家用安全解決方案的用戶，接到冒名該公司客服人員的詐騙電話，經推測應有內部人員配合。至 108 年 10 月底，該公司確定整起事件主因係 1 名員工屢次大量存取客服資料庫，該資料庫內含客服工單編號、用戶姓名、電子郵件信箱及部分客戶電話號碼等。該名員工將所竊得資料賣給外部犯罪組織，犯罪組織便利用相關資料進行詐騙行為。

二、 勒索軟體攻擊風險激增

駭客利用勒索軟體攻擊入侵手法眾多，包含使用社交工程郵件、惡意網站等，再加上使用者備份觀念明顯不足，讓駭客輕易利用此種攻擊，成功達到獲取金錢利益的目的。資安業者 Emsisoft 針對遭到勒索軟體攻擊的美國政府機構、學區及醫療服務供應商進行相關統計，於 108 年 10 月在官方部落格公布美國 108 年前 3 季勒索軟體調查結果，資料顯示至少有 621 個組織遭到勒索軟體攻擊。當美國各州、城

市或郡遭到勒索軟體攻擊時，很容易就會躍上新聞版面，但在遭到攻擊的 621 個組織中，只有 68 個組織為政府機關，代表有更多組織遭受勒索軟體攻擊卻祕而不宣。

位於美國佛羅里達州中只有 3.4 萬居民的小城市 Riviera Beach 於 108 年 5 月 29 日受到勒索軟體感染威脅，該市議會於 6 月 19 日投票表決，決定支付 65 個比特幣(約 63 萬美元)贖金予駭客。而此一資安事件源自於 1 名 Riviera Beach 市政府員工開啟電子郵件中所夾帶的惡意檔案，勒索軟體加密該市電腦系統重要檔案，造成該市電子郵件系統完全無法使用，造成負責 911 業務的調度員無法將來電輸入電腦系統，連支付薪水給員工或承包商都只能開支票，而無法透過電腦轉帳。

三、IoT 與行動式設備資安弱點威脅升高

隨著智慧家電及 IoT 應用興起，一般用戶也成為駭客下手目標。美國聯邦調查局 FBI 於 108 年 12 月 3 日呼籲大眾，勿將連網攝影機、遊戲機及智慧喇叭等 IoT 裝置與家用電腦連接於同一 Wi-Fi 網路。FBI 指出，新興家用資訊裝置不但可能藉由消費者不知道的方式蒐集資訊或傳到不明去處，還會讓駭客透過駭入上述 IoT 裝置入侵 Wi-Fi 網路，再經由家用路由器擴散到各個連網裝置，包括儲存隱私資訊與密碼的家用電腦等。

108 年新的 Mirai 變種再次捲土重來展開攻擊，包括利用無線投影系統及智慧電視等商務型聯網設備的漏洞，顯示駭客可能將目標轉向企業網路，藉以取得更大頻寬建立殭屍網路，方便日後發動分散式阻斷服務(Distributed denial-of-service，DDoS)攻擊。

四、APT 鎖定式攻擊竊取機敏資料

駭客採用的進階持續性威脅(Advanced Persistent Threat, APT)攻擊手法和傳統網路攻擊差別在鎖定專一或特定族群為目標對象。而會成為駭客的攻擊目標，多是擁有機敏性資訊或大量個人資料，如金融業者、國防、社群媒體，尤其是現在政府機關或企業高度仰賴之雲端服務皆是常被鎖定之攻擊目標。駭客鎖定目標後，便處心積慮蒐集各種可以使用的弱點和漏洞，包含各種社交工程手法與偵測所使用之資通系統漏洞、供應鏈等各種資安攻擊入侵手法等，藉以達到成功入侵組織內部的目的。

微軟威脅情報中心(Threat Intelligence Center)108 年 10 月 28 日於官方部落格揭露，在 109 年東京奧運前夕，偵測到來自 APT28 駭客集團新一波網路攻擊行動，駭客鎖定全球 16 個運動與反禁藥組織展開攻擊，但只有少數組織被成功入侵。另外，德國法蘭克福遭受 Emotet 惡意程式鎖定攻擊，致數個城市與學術網路關閉。Emotet 使用多種方法與規避技術來維護其持續性攻擊並逃避檢測。此外，更可透過夾帶惡意附件或連結的網路釣魚垃圾郵件進行傳播。

五、資安(訊)供應商持續遭駭破壞供應鏈安全

資安(訊)設備供應商容易成為駭客攻擊首要目標之一，係因供應商存在資安防護機制缺陷或是專注於業務成長而輕忽資安重要性，相對於駭客的真正攻擊目標，從供應商本身相對容易入侵。因此，駭客便利用資安(訊)設備供應商做為跳板進入目標內部網路以進行攻擊。

資安業者 Proofpoint 於 108 年 9 月 23 日在官網發布訊息，某國家級駭客集團持續鎖定美國公用事業服務供應商，展開魚叉式網路釣魚攻擊，藉機在受害者系統上植入 LookBack 惡意程式。至少有 17 個

供應商遭到攻擊。駭客集團不斷地改善網路釣魚攻擊策略、技巧及程序，顯示該集團對美國關鍵基礎設施供應商的惡意企圖。

六、關鍵資訊基礎設施資安風險倍增

關鍵資訊基礎設施的建設範圍相當廣泛，且與民眾生活息息相關，包含能源、水資源、通訊傳播、交通、金融、醫療、高科技園區及政府機關等領域皆是重要防護範圍。隨著關鍵資訊基礎設施之資訊運作漸趨開放並與以網路進行串連，相關資安風險也隨之升高。

美國國家能源技術實驗室公布 108 年第 1 季 OE-417 電力緊急情況與干擾報告說明網路攻擊造成的電力系統運行中斷事件，該事件受害者是一家位於猶他州的可再生能源電力生產商，著力於風力與太陽能技術，該公司在事件發生後一天內便將系統恢復。

美國能源部指出該攻擊主要利用該公司所使用之防火牆已知漏洞，攻擊者可藉由在這些設備上觸發阻斷服務攻擊(DoS)指令，導致系統重新啟動，影響該公司控制中心與其他各個站點設備之間通訊中斷。

參、108 年政府資安威脅統計

一、政府機關資安事件通報

經彙整 108 年國家資通安全通報應變網站所接獲之 674 件通報事件，並依事件造成之機密性、完整性及可用性衝擊之嚴重度區分，由輕至重分為 1 級、2 級、3 級及 4 級，108 年通報事件影響等級比率(詳見圖 2)。

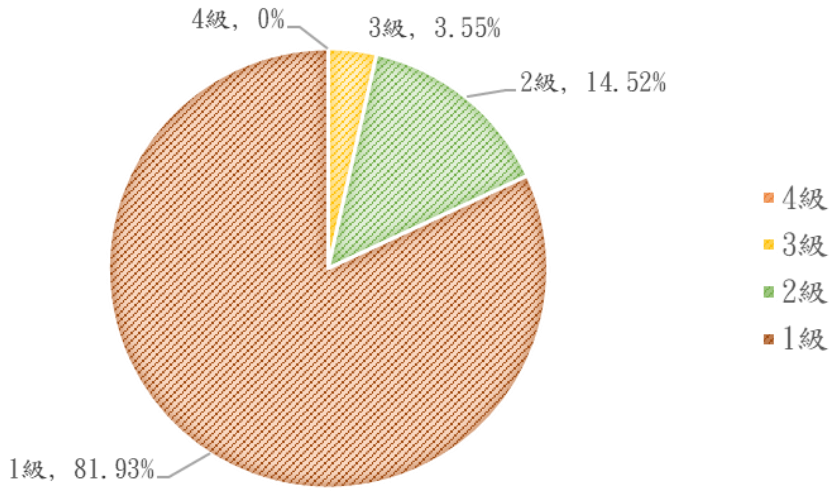

圖 2 108 年事件影響等級比率圖

資安事件通報類型可分為非法入侵、網頁攻擊、設備問題、阻斷服務(DoS/DDoS)及其他，經統計 108 年政府機關通報類型比率(詳見圖 3)，其中以「非法入侵」與「網頁攻擊」為大宗，「非法入侵」占事件通報類型 57.42%，相關事件主要係因主機未啟用作業系統自動更新功能，而遭植入多個惡意程式，或第三方產品或套件漏洞遭入侵，造成機關發生遭駭事件。此外，「網頁攻擊」占事件通報類型 17.74%，相關事件主要係因政府機關建置網站做為政令宣達或資訊公告管道，並開放民眾查詢點閱，惟因網站上傳功能未做好權限控管、檔案格式限制或第三方套件未更新等因素，成為駭客攻擊目標。

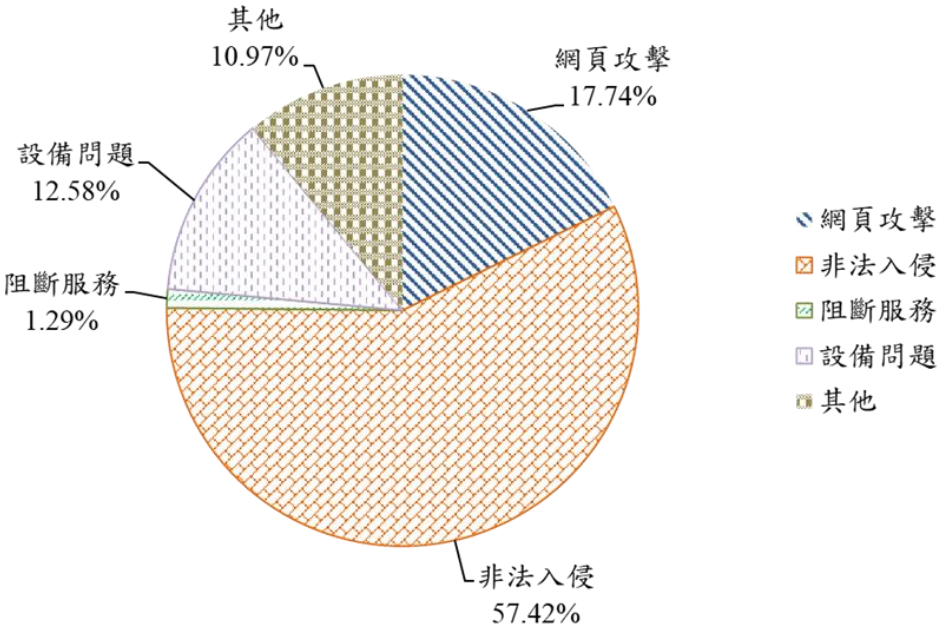

圖 3 108 年通報類型比率圖

二、資安攻防演練

本院為提升政府機關在面對網路攻擊之應處能力，每年針對政府機關辦理網路攻防演練，演練內容包括資通系統實兵演練及社交工程演練，108 年演練結果如下：

(一)資通系統實兵演練

資通系統實兵演練攻擊作業係由攻擊組以遠端資料蒐集、弱點掃描及滲透測試攻擊等方式，實際攻擊機關對外之資通系統與網路，演練機關依既有之資安監控機制，於發現被入侵後執行通報應變程序與弱點修補規劃作業。

108 年網路攻防演練針對 66 個演練機關 4,264 個對外資通系統進行演練，其中有 43 個機關之系統發現至少一個 Info 衝擊性以上弱點，占演練機關總數之 65.15%(詳見圖 4)。

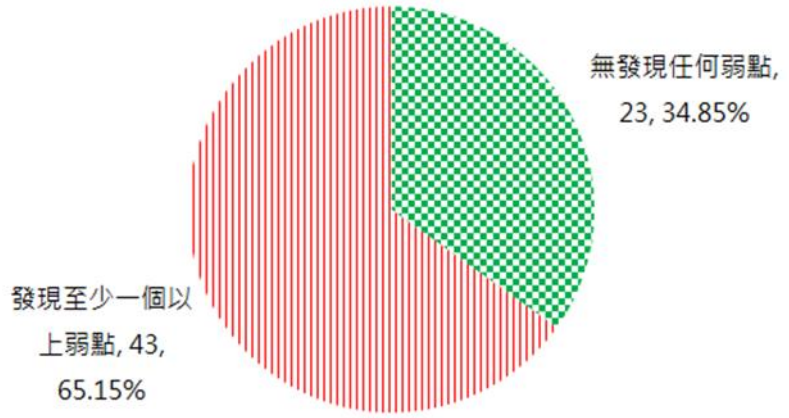

圖 4 發現弱點之機關比例

本次演練共發現 372 個弱點，其中高衝擊性弱點數量 179 個，占整體弱點數量之 48.12%；低衝擊性弱點數量 166 個，占整體弱點數量之 44.62%；Info 衝擊性弱點數量 27 個，占整體弱點數量之 7.26%(詳見圖 5)。

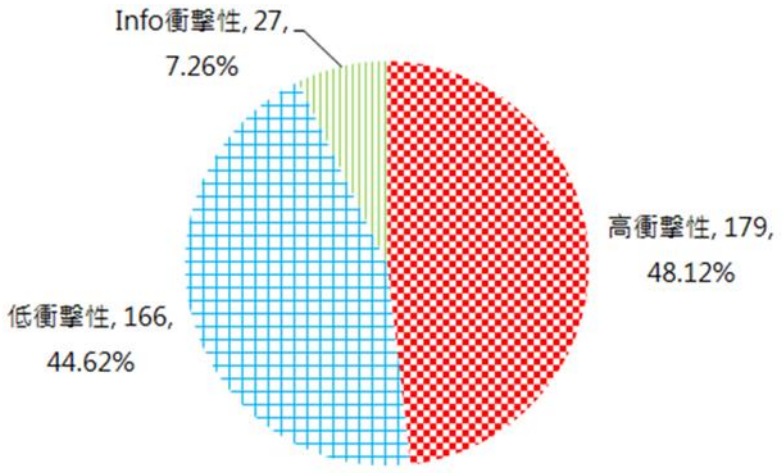

圖 5 弱點衝擊性比例分布圖

(二)社交工程演練

社交工程演練範圍共計 66 個機關，開啟郵件之機關有 52 個，占演練機關數量之 78.79%(詳見圖 6)；點閱連結/附件之機關有 48 個，占演練機關數量之 72.73%(詳見圖 7)。另社交工程簡訊演練範圍共計 60 個機關，點閱簡訊連結之機關有 45 個，占演練機關數量之 75%(詳見圖 8)。

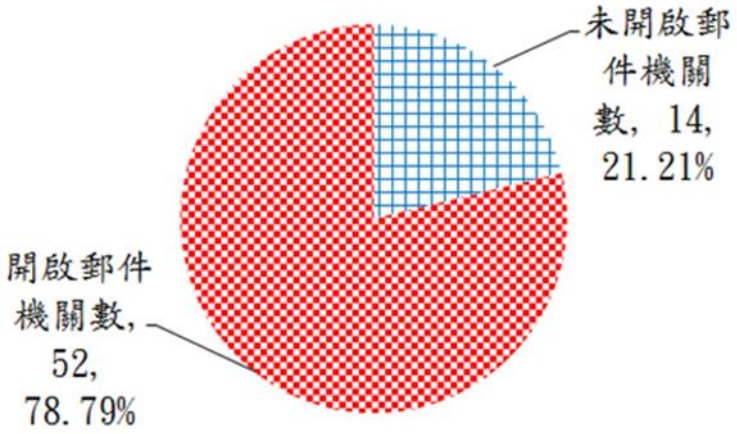

圖 6 開啟郵件機關比例圖

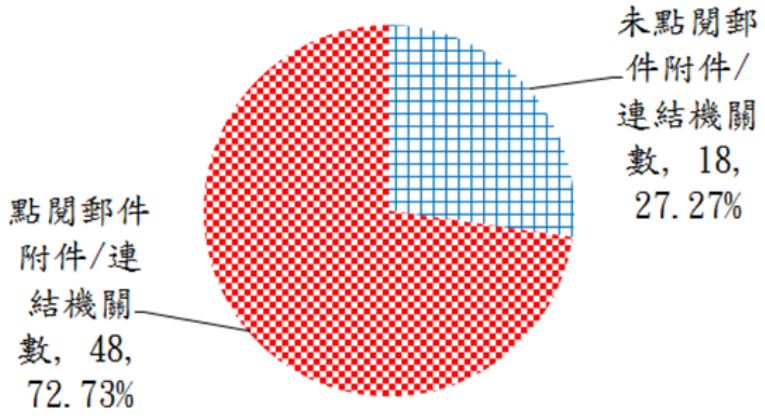

圖 7 點閱郵件附件/連結機關比例圖

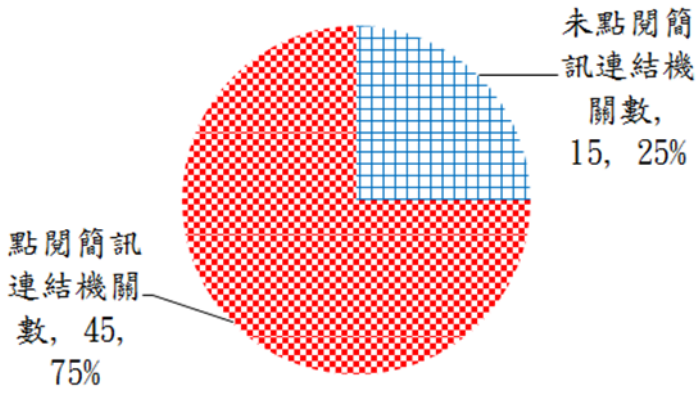

圖 8 點閱簡訊機關比例圖

三、資安稽核作業

本院為協助政府機關提升資安防護之完整性及有效性，108 年稽核公務機關係以上級/監督/中央目的事業主管機關為稽核對象，特定非公務機關則以政府補助之財團法人與公營事業為主，共選擇 10 個公務機關與 5 個特定非公務機關進行稽核，辦理情形如下：

(一) 實地稽核

實地稽核分「策略面」、「管理面」及「技術面」3 個構面進行稽核，「策略面」稽核項目包括：「導入資訊安全管理系統範圍之適切性」、「機關首長對資安業務之支持度」、「資源投入資安業務情

形」及「資安業務運作規劃及落實」；「管理面」稽核項目包括：「資產管理及風險評鑑」、「人力資源管理」、「資訊委外安全管理」、「所屬機關監督管理」;「技術面」稽核項目包括:「電子資料保護」、「通訊及作業安全」、「資安事件通報及處理」、「資通系統開發及維護安全」。實地稽核共 12 個稽核項目，108 年公務機關各稽核項目之表現統計情形詳見圖 9。

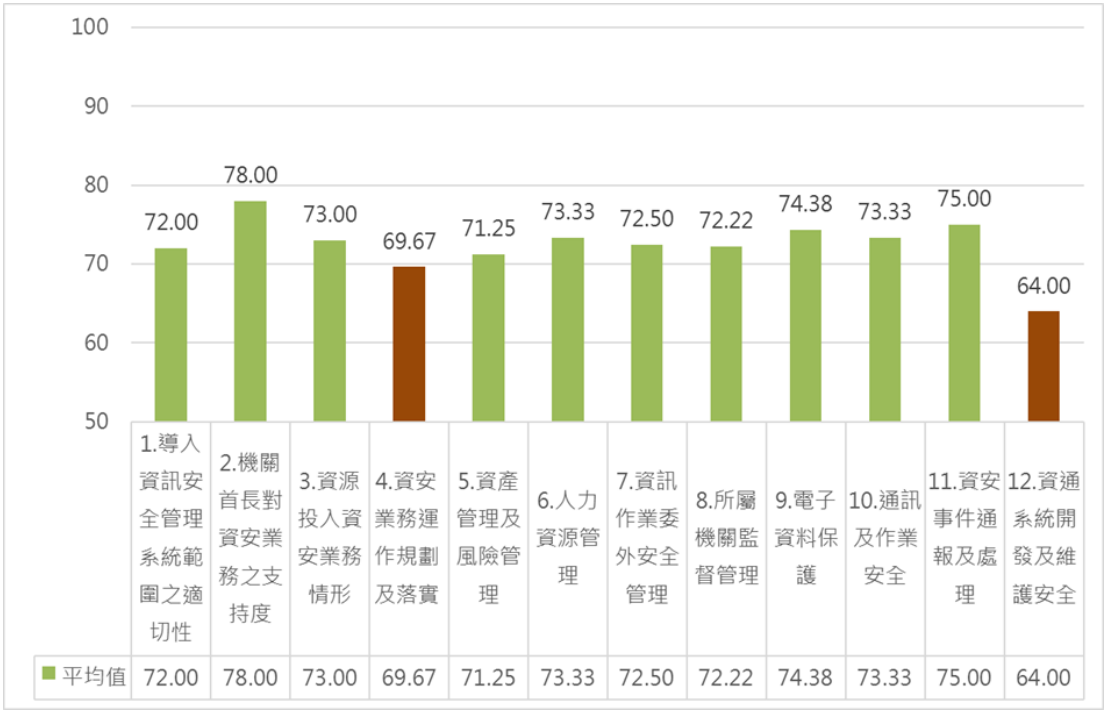

圖 9 公務機關實地稽核項目整體表現分析圖

(二)技術檢測

技術檢測分為「使用者電腦安全檢測」、「網路惡意活動檢視」、「核心資通系統安全檢測」、「網路架構檢測」、「網域主機安全防護檢測」、「物聯網設備檢測」及「組態設定安全檢測」7 大檢測項目，108 年公務機關技術檢測各項目之整體表現情形詳見圖 10。

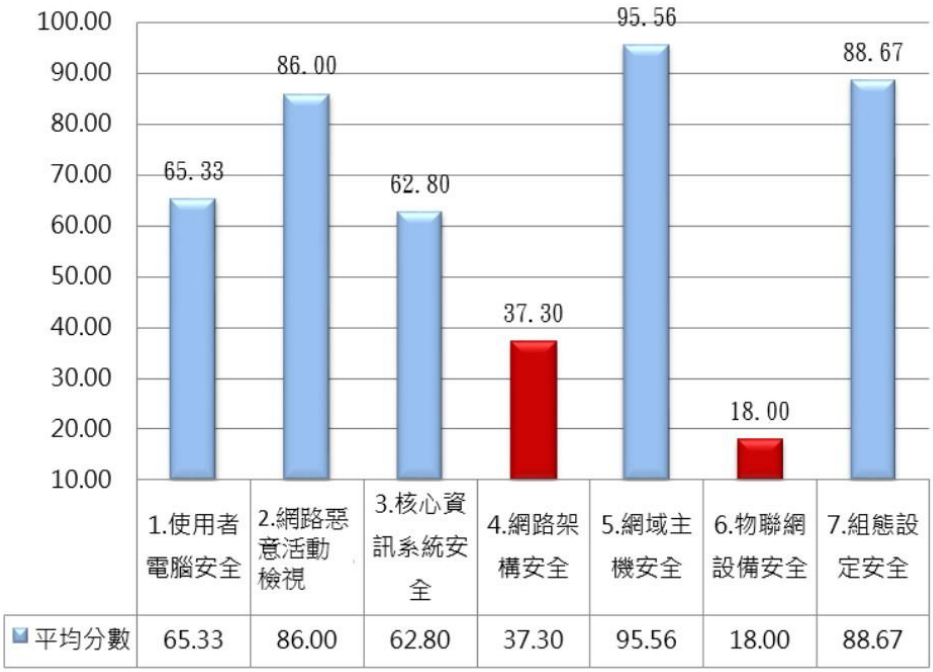

圖 10 公務機關技術檢測項目整體表現分析圖

(三)資安稽核共同發現事項

1. 策略面

(1) 未有效落實機關核心業務及核心資通系統之界定。

(2) 資安維護計畫與內部 ISMS 規範文件不一致，且未納入資安法規要求。

(3) 資通安全相關法遵及技術知能要求與日俱增，惟受稽機關常因資安人力資源缺乏未配置專職/責人力。

2. 管理面

(1) 受稽機關人員與委外廠商對於資安相關法規認知仍顯不足。

(2) 未依資安法等規範事項規劃與落實資訊委外作業。

(3) 上級機關未依所屬或監督機關之資通安全責任等級，規劃適當之稽核整體計畫（包含明訂受稽機關遴選原則、依機關資安責任等級需求規劃檢核表等），以致影響稽核執行

成效。

3. 技術面

(1) 網路架構安全性仍顯不足，未確實進行網段區隔及存取控管。

(2) 資通系統安全開發程序未納入資通系統防護需求且未落實。

(3) 未針對核心資通系統定期進行弱點掃描、系統滲透測試，機關資安健診作業應訂定內部資安作業程序，且應確實改善追蹤。

(4) 未就 GCB 套用之例外管理，提出可行方式及改善時程，並定期追蹤改善情形。

(5) 未將 IoT 設備納入資訊資產盤點範圍，並建立適當防護措施。

四、聯防預警情資

為有效掌握政府機關的潛在資安威脅，國家資訊安全防護中心(簡稱 N-SOC)定期彙整政府機關資安預警情資與事件，掌握資安威脅類別及趨勢。經分析 108 年所彙整之情資，計分為系統服務、入侵攻擊、阻斷服務、惡意程式、政策規則、掃描刺探及尚需調查等 7 類。108 年資安威脅類型前 3 名分別為入侵攻擊類(占 39.96%)、掃描刺探類(占 33.07%)及惡意程式類(占 14.84%)，各類威脅分布情形詳見圖 11。

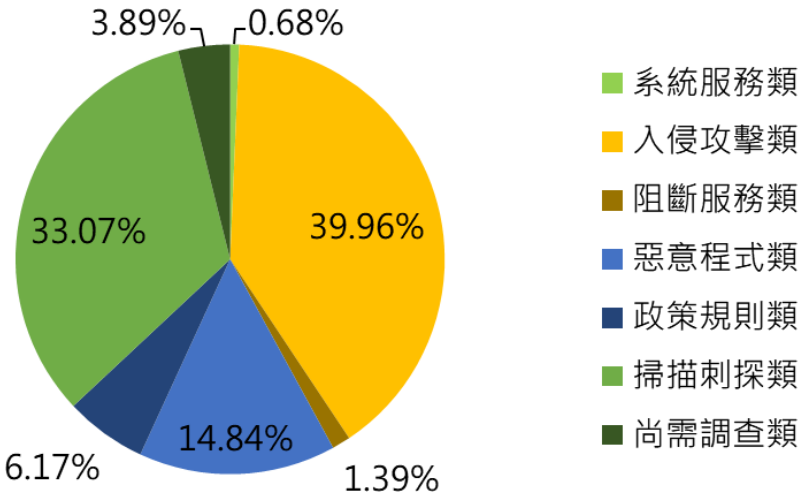

圖 11 各類資安威脅分布圖

五、惡意電子郵件

觀察 108 年針對政府機關之電子郵件社交攻擊趨勢，其攻擊數量較 107 年上升，分析 108 年惡意電子郵件夾帶之惡意檔案，係以 RAR 與 ZIP 壓縮檔類型為主，比較 107 年與 108 年檢測出惡意檔案數量與類型詳見圖 12。經查 108 年 11 月之惡意電子郵件比率相對較高(詳見圖 13)，分析後發現有較多 Emotet 惡意程式嵌附於電子郵件附件。進一步研析全球重大資安事件，自 108 年下半年起歐洲出現多起 Emotet 殭屍網路攻擊事件，推估該攻擊與惡意程式散布活動可能已蔓延至亞洲。

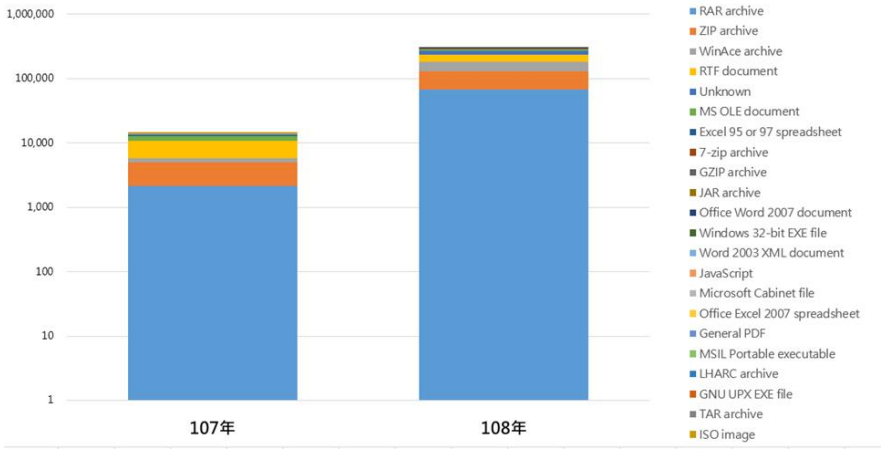

圖 12 惡意檔案數量與類型

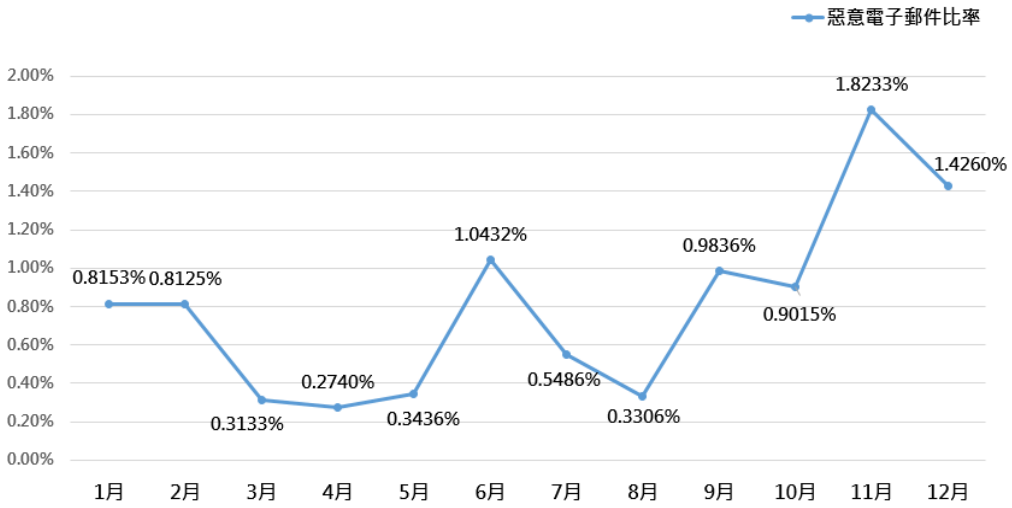

圖 13 惡意電子郵件比率

另一方面，透過惡意電子郵件的 APT 攻擊為近幾年駭侵組織常用的手法之一，有別於一般廣泛散播之惡意程式較容易被防毒軟體等偵測防護，組織型駭客持續發動針對性社交工程電子郵件攻擊(Spear-phishing Attack)，做為入侵政府機關電腦，竊取公務、國防及商業機密並布建情蒐網路之主要手段，107 與 108 年惡意電子郵件攻擊趨勢與 APT 威脅詳見圖 14。

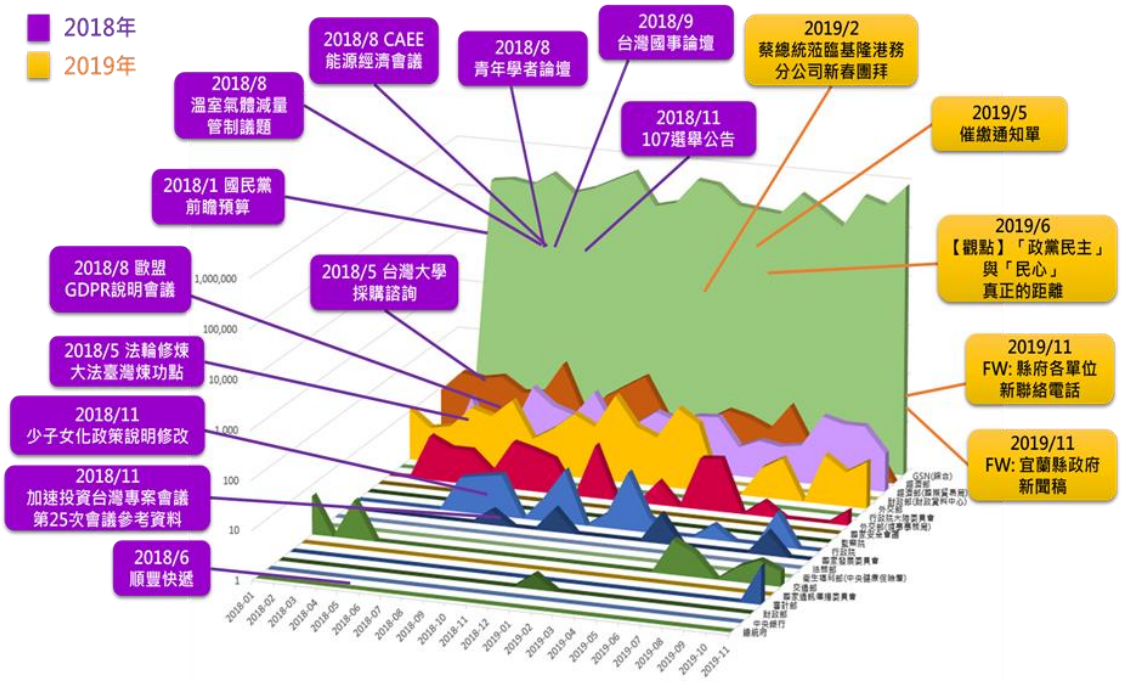

圖 14 惡意郵件趨勢與進階持續性威脅

肆、政府機關資安威脅情勢

經綜整 108 年國內外資安威脅情資，歸納政府機關面臨之資安威脅如下：

一、個人資料外洩威脅持續存在

比較 107 年與 108 年事件等級通報情況，3 級事件通報件數比率由 107 年的 2.29%提升到 108 年的 3.55%，分析相關攻擊主要以資料外洩事件居多。個人資料外洩事件頻傳，最主要係駭客可以利用個人資料進行詐騙、身分盜用，同時個人資料在市場上可被轉賣以獲取利益，讓駭客集團對個人資料長久以來具備高度興趣。

108 年曾發生比較大量的公務人員個人資料外洩，經追查主要為機關未落實資通安全管理相關作業，如未針對檢測結果落實改善作業、系統日誌的檢視及留存等，再加之導入之資通安全管理制度輔導及驗證機制未確實發揮監督制衡效果。此外，個人資料外洩不僅可能來自於外部駭客惡意攻擊，也可能因網頁設計不良存在安全性漏洞或內部人員操作不當洩露等，都是資料外洩常見的發生原因。

二、勒索軟體攻擊風險激增

108 年政府機關發生勒索軟體攻擊事件占總通報件數之比率為 8.39%，有鑑於勒索軟體攻擊事件在國內外頻傳，政府機關已逐步建立系統備援與資料備份機制，雖然有因存在系統弱點被成功入侵，但多能在短時間內恢復系統正常運作。

以某機關之全球資訊網傳出被勒索病毒入侵為例，包含全球資訊網及部份內部系統等受到影響無法正常運作，系統癱瘓數天後便先恢復外部服務網站與系統，後續逐步回復內部網路相關系統。勒索病毒犯罪集團之所以鎖定政府或醫療機關，推論主要係因這些機關所提供的服務較不能忍受長時間服務中斷的狀況，對其所服務的對象也會深

受到影響，各政府機關需詳加防範。

三、IoT 與行動式設備資安弱點威脅升高

隨著 IoT 與行動式設備的普及，IoT 相關設備已成為駭客首選的入侵目標，108 年國內所蒐錄之 Mirai 殭屍網路族群攻擊達近 6 千萬次，該殭屍網路族群持續有新的變種出現，並持續散布感染各種 IoT 設備。

以 108 年發現某款 NVR(Network Video Recorder)遭駭侵為例，該 NVR 被駭客利用來寄發社交工程電子郵件，攻擊政府機關或進行內部資通系統弱點掃描探測，該設備因系統功能豐富且易於管理，被廣泛應用於銀行、醫院、學校或購物中心等。全球約有 5,000 台該款 NVR 設備公開於網際網路，其中約 100 餘台位於台灣，經分析發現多數遭駭客利用之設備主要原因為預設密碼太簡單且未修改、或軟體及韌體未進行安全性更新所致。

四、APT 鎖定式攻擊竊取機敏資料

透過惡意電子郵件進行 APT 攻擊為組織型駭客常用手法之一，目標對象則鎖定政府機關電腦，竊取公務、國防及商業機密，透過入侵特定目標對象，布建情蒐網路以展開進一步攻擊。

經分析某機關社交工程惡意郵件時，藉由關聯分析發現，不同月份之社交工程郵件所夾帶之 2 個惡意文件皆為相同作者，使用者點擊開啟附檔後，該惡意文件會透過 Gmail 郵件服務送回受害電腦相關資訊，因此，使用者未注意便開啟不明來源郵件之附檔或連結，將導致惡意程式進入機關公務作業環境，進行提權及擴散，提高公務資料外洩或業務運作受影響之風險。

五、資通系統委外供應鏈遭駭

由 108 年通報資安事件發現，維護廠商提供機關之資通設備，因

未落實適當檢查與管制，導致存有惡意程式之資通設備，利用機關網路進行中繼站連線，或委外廠商遭感染勒索軟體，透過遠端存取擴散至機關等事件。

駭客不直接對政府機關展開攻擊，研判主要是因為政府機關長期在資安防護部署上有一定的作業基準與防護強度，要成功入侵需耗費更多時間與資源，因此，駭客嘗試轉向攻擊各機關資通系統之委外廠商，例如藉由入侵委託廠商的作業環境，透由其協助機關維運途徑進入機關，或利用系統開發商之系統設計缺陷，入侵使用該共同性系統之機關。

伍、資安防護建議

針對本報告前述資安威脅，提供防護建議如下：

(一)各機關實行資訊安全管理制度時應落實相關要求事項，依照資通系統防護基準，進行資料傳輸儲存之加密機制、漏洞修復、資通系統監控及日誌保留期間與管理等防護措施，並辦理技術性檢測及追蹤改善作業。

(二)為降低資通系統遭受勒索軟體攻擊的風險，各機關應依資料重要等級，規劃備份週期，並建立離線備份與異地備份機制。另可藉由調整網路架構確保內外網隔離，將伺服器與使用者電腦進行網段區隔，以強化對外防護。

(三)針對政府機關面臨 IoT 設備攻擊威脅之情形，應加強辦理如下防護作為：

1、 在購置 IoT 設備時，應要求廠商提供該設備之安全性檢測證明，在使用 IoT 設備前，應修改預設密碼。

2、 應定期進行官方軟體及韌體之安全性更新。

3、 針對無法更新之設備，建議透過防護設備或系統設定限制存取來源。

(四)為避免惡意電子郵件攻擊造成機敏公務資料外洩，各機關應持續提升機關人員之資安意識，宣導使用者注意郵件來源之正確性，勿開啟不明來源郵件之附檔或連結，勿使用公務郵件帳號註冊外部服務，並應定期更新作業系統弱點修補程式以及防毒軟體病毒碼。

(五)針對政府機關委外供應鏈遭受攻擊之情形，除應依「資通安全管理法施行細則」第 4 條各款規定辦理對委外廠商之資安要求及監督管理外，針對資通系統部分應定期進行系統更新、源碼檢測及弱點掃描，並配合系統開發廠商之漏洞修補程式，即時進行修補。

陸、結語

網路攻擊無遠弗屆，鑒於國內政府所面臨的資安威脅與全球資通安全事件與日俱增，期藉由殭屍網路威脅、聯防監控、電子郵件及通報事等情蒐分析，了解駭客攻擊與資安事件發生之根因與脈絡，並進而接軌國際之資安情資，以達知己知彼、防患於未然之效。

資安法自 108 年實施後，政府資通安全防護策略奠基在資安法的基礎，持續發展防護策略與縱深防禦方案，包含政府資安技術的諮詢服務、日常維運的組態基準設定及系統安全發展生命流程導入後之成熟度評量機制。同時，本院藉由年度定期之資安稽核、技術檢測及攻防演練，期能兼具深度與廣度檢視政府機關資安防禦之完備度與韌性。另本院透過研析新興資安議題與資安攻擊手法，以預見資安威脅之發展與趨勢，同時洞悉未來資訊科技應用之資安風險，俾利及早提供防範作為。