twcertcc 2020

資通安全年報

Information Security Annual Report

CONTENTS
目錄

圖目錄

表目錄

第一章、

前言

台灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC) 歷年來不斷增強資安事件處理能量，提升資安事件協處速度，並透過資安趨勢彙整分析、資安情資分享、資安事件與漏洞協處、國內外資安合作交流，以及資安活動參與及資安宣導，協助提升我國整體資安防護能量與機制，以達成維護乾淨安全的網路環境之願景。

近期，隨著大環境的變化，網際網路也產生了莫大的改變，而這些改變所影響的不僅僅只有一般使用者，許多企業也因此產生了相對應的改變與新興資安威脅。首先，由於遠距辦公模式逐漸興起，使得相關工具的安全性開始變得至關重要。因此，相較於過往的企業伺服器與內網之防護，遠距工作工具的選擇、防護機制設定，以及員工自身的資安意識，逐漸成爲影響企業資訊安全的重要因素之一。除了遠距辦公，許多企業也產生供應鏈以及工業 4.0 之轉變。供應鏈是由多家企業組合而成，每間企業的資安水準就相當重要，一旦其中的一或數間廠商資安防護薄弱，可能對整個供應鏈及其產品產生嚴重影響。爲避免供應鏈資安事件的發生，除了愼選具足夠安全防護的合作廠商外，其產品之生產製造過程，均應參照國內相關單位所提出之資安防範規範，進行檢測驗證，確保供應鏈中每個環節之安全無虞，以增加使用者對該產品之信任。工業 4.0 使得許多製造業逐漸改爲運用聯網設備及環境，但在增加其生產效率的同時，可能尚未或無法全面考慮相關的安全性，導致攻擊者得以透過網路對製造商進行攻擊。因此，我國重要的半導體產業，就配合國際半導體產業協會，針對該產業之資通訊安全，制定一系列規範，企盼透過此規範的建立與施行，達成在增加產業生產效益的同時，仍能保有足夠的安全性，杜絕攻擊者所帶來的所有資安威脅。

近年來，隨著科技發展，例如網通設備數量快速增加、網路域名及網站的普及、物聯網的興起等，都對網際網路產生了諸多變化，對一般使用者、企業及相關單位也都造成一定的影響。尤其隨著大量 IP 需求，IPv6 的發展勢在必行，但相較於使用已久的 IPv4，IPv6 在建置過程中，許多資安問題逐漸浮現，甚至還有諸多潛在威脅尚不得而知。因此，爲達成 IPv6 部署的最佳安全性，IPv6 Ready Logo 針對 IPv6 設備進行安全性檢測，設備需包含足夠的安全機制及功能才能獲取該標章，以及配合我國推行之 IPv6 發展相關計畫，能夠讓使用者或企業更加放心地進行 IPv6 建置。此外，越來越多的駭客濫用域名進行社交工程攻擊，再加上 COVID-19 疫情的發生，導致與之相關的域名濫用情形愈發嚴重，對關注疫情的使用者而言是種莫大的威脅。但除了相關單位的防範和通報外，使用者本身的安全意識更爲關鍵，必須在大量的疫情相關資訊中，得以分辨資訊的眞僞，並且隨時提高警覺，才能從源頭杜絕 COVID-19 相關之域名濫用及其所產生之嚴重威脅。最後，除了 IP 和域名的數量增加，網路相關設備的數量也隨之增加，導致 DDoS 攻擊的出現越發頻繁、攻擊類型及流量大幅上升，威脅也越發嚴峻。爲降低 DDoS 攻擊所帶來之嚴重威脅，越來越多防護或網通設備，會針對特殊攻擊方式或協定之 DDoS 攻擊進行過濾和防護，甚至越來越多業者推出流量清洗服務，協助企業區分惡意和合法流量，大幅減輕 DDoS 攻擊對企業的威脅程度，保護企業服務運行順暢無虞。

本年度期間，TWCERT/CC 持續進行資安情資通報與分享，總計分享逾 150 萬筆之資安情資予相關單位，包括來自國際，欲針對國內 IP 位址進行協處與警示的通報；以及來自國內，欲針對國內其他單位或國際 IP 位址進行協處與警示的通報。此外，TWCERT/CC 也與國內外資安組織進行系統介接，定期並即時地進行情資交流分享，提升情資警示及分享效率。同時，TWCERT/CC 爲遏止社交工程攻擊之威脅，建立我國本土之惡意檔案檢測系統 — Virus Check，透過靜態檢測模式與動態分析機制，全方位檢測檔案中是否潛藏惡意程式，進而達到降低社交工程惡意檔案攻擊之目的。並且，爲提升大衆對惡意檔案的防範敏銳度，以及收到可疑檔案時，能採取檢測等多重驗證的習慣，TWCERT/CC 於本年度進行相關推廣活動，鼓勵民衆多加利用 Virus Check 服務，減少因社交工程惡意檔案而受駭之機率。

而針對產品資安漏洞，TWCERT/CC 參與美國非營利組織 MITRE 之 CVE 計畫，擔任台灣區 CVE 編號管理者，負責接收、審核及發布資安漏洞 CVE 編號，同時將漏洞資訊公告於台灣漏洞揭露平台 (Taiwan Vulnerability Note, TVN)，讓更多單位了解並進行相關漏洞防護。TWCERT/CC 也會主動搜尋與該產品相關的組織、單位，並於蒐整之後個別告知，協助對資安漏洞進行適當防護，避免遭到惡意攻擊者利用後進行衍伸攻擊，提升國內資安漏洞防護之能量。在 2020 年期間，TWCERT/CC 總計接獲約 20 項產品，超過 50 個漏洞之資安通報，並透過這些漏洞發布的正確性，於 2020 年獲得美國國家弱點資料庫 (National Vulnerability Database, NVD) 評核在通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS) 檢測 3.1 版中，取得貢獻者 (Contributor) 等級之殊榮。

爲了強化大衆資安意識，TWCERT/CC 於今年度主辦、協辦及參與多場資安活動，透過面對面的演講與分享，達成更進一步的資安宣導成效。在本年度期間，爲提升資安聯防與應變效益，本中心主辦台灣通報應變年會，邀請國內各界資安重要人士進行分享與討論，透過經驗的共享與良好之互動，達成擴大我國企業資安認知與防護能量之目標。TWCERT/CC 亦與諸多資安組織、公協會及企業組織共同組成「台灣 CERT/CSIRT 聯盟」，並定期舉辦交流會議與教育訓練，除了透過此聯盟建立良好的資安聯繫與分享管道外，也希望能增進成員之間的交流互動，彼此互助攜手提升我國之資安防護能量。此外，爲提升與國際間的交流，TWCERT/CC 亦參與多場國際會議和活動，分享我國之資安現狀，以及進行網路安全攻防演練，企盼透過與國際接軌的交流活動，可以提升國際間的通報效率與情資共享。

在厚植資通安全意識方面，TWCERT/CC 於 2020 年期間持續發布國內外相關資安新聞、駭侵事件、漏洞資訊，以及相關資安研討會及活動等訊息，並且定期寄送資安電子報，積極提升大衆的資安知識與防護。這些定期發布之資安訊息，除了本中心官方網站外，亦可從 TWCERT/CC Facebook 粉絲團、Instagram 及 Twitter 等處取得相關資訊，企盼能透過全方位的資安訊息分享與宣傳，強化我國資安防範意識與能量。

在科技不斷發展、生活型態不斷變化的現代，在提升便利性的同時，更多的資安威脅也隨之而來。因此，TWCERT/CC 希冀透過資安趨勢分析、情資分享、資安事件與漏洞協處、國內外合作交流，以及資安宣導，提升我國資安聯防能量，共同維護台灣的整體網路安全。

第二章、
資安威脅與防護

爲提升我國企業與一般民衆之資安意識，以及國內各單位對資安相關議題的了解和關注，並與國外資安組織分享台灣重大資安事件及發展趨勢，TWCERT/CC 配合資安趨勢、資安政策、資安事件與重大駭侵等議題，收集國內外相關資安資訊，企盼藉此資安資訊彙整與分享，以增進國內民衆與組織之整體資安知識與防護能量。

第一節、企業組織之資安威脅與防護

一、遠距工作資安威脅與防護

1. 遠距工作資安威脅

隨著科技發展，許多企業爲減少員工交通時間與舟車勞累，以及辦公空間成本，開始提倡員工遠距工作。近期，更由於嚴重特殊傳染性肺炎 (Coronavirus Disease 2019, COVID-19) 疫情嚴峻，愈來愈多的企業及組織要求員工遠距工作，以降低接觸與感染風險。

根據統計，在 2019 年期間，有 40% 受訪者所在的企業依個人職務需求執行遠距工作，而有 31% 受訪者所在企業全體執行遠距工作之辦公方式[1]。從 2005 年以來，全球在家辦公的工作者數量增加了 159%，顯示遠距工作已成爲工作方式的發展趨勢[2]。

隨著遠距工作比例快速成長，爲達成員工遠距工作所需，諸多遠距工作工具推陳出新，而這些工具主要是針對五項遠距工作需求所開發而成[3]：

A. **計畫管理 (Project Management)**：讓計畫相關員工記錄並告知其執行進度，達成計畫在團隊中的同步和協作。

B. **即時通訊**：提供團隊溝通討論之管道，進行員工間的協調合作。

C. **團隊合作 (Collaboration)**：提供在組織間共享及同步相關資源之管道，讓成員得以順利取得資源後執行計畫相關作業。

D. **團隊管理 (Team Monitoring & Management)**：提供管理者即時檢視各成員的進度和貢獻，達到作業進度最適化和最佳的作業配置。

E. **遠距存取 (Remote Access)**：提供相關成員安全的存取存於企業中的相關資源，以順利完成工作上之所需。

因此，企業爲滿足員工遠距工作時的需求，最爲常見之遠距工作工具主要分爲底層工具和上層應用，兩者相互連結以達成遠距工作之所需。

1 Buffer. “State Of Remote Work”. Retrieved March 30, 2020, from the World Wide Web: https://buffer.com/state-of-remote-work-2019

2 MerchantSavvy. “Global Remote Working Data & Statistics”. Retrieved March 30, 2020, from the World Wide Web: https://www.merchantsavvy.co.uk/remote-working-statistics/

3 Splashtop. “Top 5 Software Tools for Remote Working from Home in 2020”. Retrieved March 30, 2020, from the World Wide Web: https://www.splashtop.com/top-5-software-tools-remote-working-from-home

遠距工作中重要底層工具如下：

A. **虛擬私人網路** (Virtual Private Network, VPN)：爲保障使用者連線時身分及數據的安全，企業會建立 VPN 供員工遠距工作時使用。

B. **通訊網路**：在資訊傳輸的過程中，需透過通訊網路進行連線及傳輸，因此員工爲連入企業內網或進行溝通及協同合作，企業或使用者都應使用足夠安全的通訊網路。

C. **家用網路** (Home Network)：當員工欲連入企業內網或存取共享資訊都需使用網際網路，因此員工往往會使用電信事業的行動通訊或固定通訊網路之家用路由器或 Wi-Fi 設備，提供網路予電腦或行動裝置進行連線作業。

遠距工作中重要上層應用如下：

A. **遠距會議** (Video Conference)：爲確保員工能與團隊成員討論、協調，以及和客戶進行業務溝通，企業需提供遠距會議工具供員工遠距工作時使用。

B. **遠端存取企業資源**：爲確保員工資訊、檔案及相關資源能與團隊或相關人員進行共享，並且可供多人處理或使用，企業會提供遠端存取機制及系統，供員工在遠距工作時使用。

然而，隨著遠距工作比例增加，員工使用的網路、裝置或相關工具，企業較難予以規範，導致因遠距工作所產生的資安威脅更加嚴重且普遍。對於遠距工作常見的工具，不論是底層工具或上層應用，都有產生資安威脅之可能，企業和員工均需小心防範。

(1). 遠距工作底層工具資安威脅

A. **虛擬私人網路 (VPN)**：於傳輸過程中加密以及隱匿使用者的位址，雖可提供足夠之安全性。然而，由於某些 VPN 設計或應用程式問題，可能產生相對應的漏洞。其可能產生的常見資安威脅如下：

I. **身分驗證漏洞**：使用者在使用 VPN 進行網路行爲前，VPN 會針對使用者身分進行驗證，在確認其身分後才會提供相關服務。但有些 VPN 系統存在安全性漏洞，並未確實驗證使用者所提交之資訊，或讓攻擊者可透過漏洞避過身分驗證過程，並取得系統管理員權限後，進行資料竊取或破壞等攻擊[4]。

II. **加密金鑰竊取**：對 VPN 系統而言，最爲重要也是使用者使用 VPN 的最大主因即爲其流量的加密，透過將使用者對外連接的封包流量進行加密，可以有效避免資訊遭第三者攔截後取得其中的機敏資訊。然而，VPN 系統是透過金鑰對流量進行加密，因此，若攻擊者透過各種方式取得 VPN 的加密金鑰後，極有可能可以對使用者的流量攔截後，以金鑰解密並取得其中的機敏資訊，對 VPN 的使用者產生莫大威脅[5]。

4 Cisco. “Cisco Adaptive Security Appliance Software SSL VPN Denial of Service Vulnerability”. Retrieved April 28, 2020, from the World Wide Web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ssl-vpn-dos

III. **VOracle 攻擊：**由於許多 VPN 系統在將通過的流量進行加密前，會將同一區域網路中的封包進行壓縮後再行加密，並傳輸給連線目標伺服器進行解密及解壓縮等行爲。然而，透過字符重複比例越多、壓縮成效越好之壓縮原理，攻擊者透過網路釣魚等方式，將使用者導入攻擊者可控之超文本傳輸協定 (HyperText Transfer Protocol, HTTP) 網站中，並且在使用者傳輸資訊時，將可能的字元同時傳至 VPN 伺服器中進行壓縮後加密並傳輸，而攻擊者可從其控制的 HTTP 網站中取得 VPN 系統壓縮後的大小，若攻擊者輸入的字元越接近其 VPN 的帳號或其中的重要資訊，則網站所收到壓縮後的封包大小會越小，攻擊者便可用類似暴力破解的方式，成功取得機敏資訊，甚至可順利截取使用者進行網路行爲的所有內容[6]。

圖 2-1：VOracle 攻擊示意圖　　資料來源：TWCERT/CC 整理

B. **家用網路：**由於家用網路設備是遠距工作者傳輸資訊的第一步，也是連線的重要設備之一，一旦家用網路設備遭到攻擊，其傳輸的訊息將輕易地外洩給第三方，這也導致家用網路設備成爲許多攻擊者的攻擊目標。其可能產生的常見資安威脅如下：

I. **弱密碼 (Weak Passwords)：**許多家用網路設備在初始時會使用出廠預設密碼，而使用者往往爲求便利或不知如何修改，而持續使用預設密碼作爲常用密碼，或設定低強度的密碼，導致攻擊者可透過搜尋該設備預設密碼或暴力破解方式在短時間內破解低強度密碼，並在取得權限後進行惡意行爲[7]。

5 VPNCompare. “NordVPN encryption key leak causes panic”. Retrieved April 28, 2020, from the World Wide Web: https://www.vpncompare.co.uk/nordvpn-encryption-server-security/

6 Nafeez. “Compression Oracle Attacks on VPN Networks”. Retrieved April 28, 2020, from the World Wide Web: https://i.blackhat.com/us-18/Wed-August-8/us-18-Nafeez-Compression-Oracle-Attacks-On-Vpn-Networks.pdf

7 Comparitech. “How to secure your home wireless network (Updated 2020)”. Retrieved April 13, 2020, from the World Wide Web: https://www.comparitech.com/blog/information-security/secure-home-wireless-network/

II. **家用網路設備漏洞利用：**隨著網際網路及設備的演進，家用網路設備往往因攻擊的方式及數目增加，過往未察覺的漏洞逐一浮出檯面。最爲常見的即爲讓攻擊者可繞過身分驗證要求，進而取得管理員權限後，進行資料竊取或破壞行爲。而使用者只能配合廠商執行初步緩解作業，或等待廠商漏洞修補完畢，難以在第一時間進行較完備的防護，導致一旦漏洞被發覺，可能造成使用者不小的威脅[8]。

III. **中間人攻擊 (Man-In-The Middle Attack, MITM)：**先透過位址解析協定 (Address Resolution Protocol, ARP) 欺騙或網域名稱系統 (Domain Name System, DNS) 欺騙方式，將使用者所傳輸的封包導至攻擊者端後再行送出，而攻擊者可透過封包截取工具，竊取其中資訊。雖然許多網路設備在進行網路連線時，會將其封包進行加密，但某些如有線等效加密 (Wired Equivalent Privacy, WEP) 或 Wi-Fi 存取保護 (Wi-Fi Protected Access, WPA) 等加密機制，都被證實爲不安全的保護機制，即便使用者使用 WEP 或 WPA，仍有資訊被竊取的風險[9]。

(2). 遠距工作上層應用資安威脅

A. **遠距會議：**針對遠距會議，雖然會議內容應僅限於參與者可見，但某些視訊會議的設計及防護措施不夠完整，導致有不在受邀名單中的人進入會議中，取得會議中的重要資訊。其可能產生的常見資安威脅如下：

I. **會議炸彈 (Meeting Bombing)：**許多遠距會議均以分享資訊的方式邀請他人參與，並無設定密碼等防護措施，使得攻擊者可隨意進入或透過目標的使用者帳號等資訊進入會議中，並且進行干擾及破壞等行爲[10]。

8 ThreatPost. “Cisco Patches 13 High-Severity Router and Switch Bugs”. Retrieved April 28, 2020, from the World Wide Web: https://threatpost.com/cisco-high-severity-bugs-2/148706/

9 Allot. “Home Router Vulnerability”. Retrieved April 28, 2020, from the World Wide Web: https://www.allot.com/resources/TB_Threat_Bulletin_Home_Router.pdf

10 Paloalto. “Best Practices for Video Conferencing Security”. Retrieved April 13, 2020, from the World Wide Web: https://blog.paloaltonetworks.com/2020/04/network-video-conferencing-security/

II. **竊取使用者登入資訊：**由於許多 Windows 主機會開啓伺服器訊息區塊 (Server Message Block, SMB) 協定，用以共享區域網路上的檔案、印表機或通訊等資源。然而，在遠距會議中，參與者所貼上的網址，許多軟體難以分辨爲網頁位址 (Uniform Resource Locator, URL) 還是存取區域網路資源的通用命名規範路徑 (Universal Naming Convention Path, UNC Path)，當使用者不小心點擊 UNC 路徑，並以 SMB 協定取得資源時，系統會將使用者 Windows 的帳號密碼傳輸至指定位址之伺服器，導致使用者的登入資訊外洩[11]。

III. **遠端執行惡意指令：**許多使用者會在遠距會議時，透過遠距會議軟體共享會議相關文件，供參與者自行下載。然而，攻擊者藉由遠距會議軟體會自動下載檔案，且下載至固定預設資料夾中之特性，上傳帶有惡意指令或惡意程式的檔案於其中，並在使用者自動下載後，透過 UNC 路徑方式執行惡意檔案，以散播惡意程式及進行破壞行爲[12]。

B. **遠端存取企業資源：**遠端存取的功能、方式繁多，某些遠端存取工具僅提供相關功能，無足夠的資安防護，導致員工在連線時遭受資安威脅。其可能產生的常見資安威脅如下[13]：

I. **阻斷服務攻擊 (Denial-of-Service, DoS)：**由於遠端存取需透過網路連接後進行資訊的傳輸，然而，一旦遠端存取伺服器遭受攻擊者大量的資訊，導致伺服器不堪負荷而中斷服務，將會導致所有的使用者都無法順利使用遠端存取資源。

II. **透過傳輸控制協定去同步 (Transmission Control Protocol Desynchronization, TCP Desynchronization)：**封包在進行傳輸時，會針對封包編列其序號，而裝置預設一旦收到序號不符合規範的封包，便會將其丟棄。因此，攻擊者便透過該機制，傳送一錯誤序號的封包給使用者及伺服器端，致使兩者通訊遭到影響，甚至攻擊者可趁機傳送惡意的正確序號封包，導致兩方接收攻擊者的惡意封包。

III. **遠端桌面協議中間人攻擊 (Remote Desktop Protocol Man-In-The-Middle, RDP MITM)：**許多人在進行遠端存取時，會通過便捷的遠端桌面協議連入企業內網的設備或伺服器中，透過圖形化介面直接進行操作。然而，由於 RDP 的使用者端不會針對其所連入的伺服器進行身分驗證，因此，攻擊者可透過如網路釣魚等各種方式，將使用者的流量導入攻擊者端後再行傳輸至伺服器，而該攻擊者便可從攔截流量封包的過程中，取得其中的機敏資訊。

隨著遠距工作愈發普及，許多企業並未考慮或落實資訊安全的防護，不論是使用工具之安全性或員工自身的安全意識不足，都可能造成企業因遠距工作而產生損失。根據研究統計，有 31% 的企業表示由於遠距工作之故，已經導致企業內部資訊遭到竊取或破壞，

11 Tom's Guide. "Zoom flaw could steal passwords and install malware: What to do now". Retrieved April 28, 2020, from the World Wide Web: https://www.tomsguide.com/news/zoom-password-malware-flaw

12 The Hacker News. "New Zoom Hack Lets Hackers Compromise Windows and Its Login Password". Retrieved April 28, 2020, from the World Wide Web: https://thehackernews.com/2020/04/zoom-windows-password.html

13 ESET. "[KB2907] Types of remote attacks". Retrieved May 5, 2020, from the World Wide Web: https://support.eset.com/en/kb2907-types-of-remote-attacks

並且只有一半的企業表示已針對遠距工作時，員工使用的工具、裝置及資料確實進行安全加密，避免遭攻擊者竊取後破解[14]。

2. 遠距工作資安防護

針對各種遠距工作常見工具的資安威脅，不論是底層工具或上層應用都需有相關防護機制，以提升企業資訊安全。

(1). 遠距工作底層工具資安防護機制

A. 虛擬私人網路 (VPN):

I. **使用者登入時進行多重認證：**應選擇提供多重認證之 VPN 系統，例如一次性密碼或生物辨識等方式，增加身分驗證的正確性及安全性[15]。

II. **定期更新 VPN 系統版本：**使用者應配合 VPN 廠商，定期檢閱並更新系統版本，方能在第一時間阻絕漏洞所帶來的資安威脅[16]。

III. **選擇足夠隱私性的 VPN 系統：**使用者應盡量選擇有足夠隱私性的 VPN 廠商，不記錄並保存任何使用者的活動紀錄，避免相關資訊外洩或被廠商販售賺取額外利益[17]。

IV. **選擇提供註銷金鑰的 VPN 系統：**使用者應選擇具有金鑰註銷功能的 VPN 系統，當發現金鑰遭外洩時能立即註銷，而非必須關閉帳戶或經長時間聯繫後才能變更金鑰[18]。

V. **連線時盡量使用超文本傳輸安全協定 (HyberText Transfer Protocol Secure, HTTPS) 網站：**使用者除了使用 VPN 進行網路行爲外，同時應使用有進行加密的 HTTPS 網站，替流量進行更多的防護，避免 VPN 金鑰或相關資訊遭竊取後，被輕易解密取得機敏資訊[19]。

14 Apricorn. “Security on the Go”. Retrieved March 31, 2020, from the World Wide Web: https://apricorn.com/blog/security-on-the-go-17a9c7/

15 Stronger. “Authentication Methods For VPNs”. Retrieved April 28, 2020, from the World Wide Web: https://stronger.tech/authentication-methods-for-vpns/

16 Norton. “What is VPN?”. Retrieved April 28, 2020, from the World Wide Web: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

17 SANS. “OUCH! Newsletter: Virtual Private Networks (VPNs)”. Retrieved April 13, 2020, from the World Wide Web: https://www.sans.org/security-awareness-training/resources/virtual-private-networks-vpns

18 OpenVPN. “Revoking Certificates”. Retrieved April 27, 2020, from the World Wide Web: https://openvpn.net/community-resources/revoking-certificates/

19 SAP. “VPN Losing It’s Security Over a New Threat VORACLE”. Retrieved April 28, 2020, from the World Wide Web: https://blogs.sap.com/2019/04/17/vpn-losing-its-security-over-a-new-threat-voracle/

B. 家用網路：

I. **應於家用網路設備使用強密碼：**使用者應針對家用網路設備密碼進行嚴格設定，例如不使用有意義的詞句，英文大小寫、數字及特殊字元隨機排列，且密碼長度應至少 12 個字元以上，並定期更換密碼，以保證密碼的強度及安全[7]。

II. **定期更新家用網路設備系統版本：**使用者應配合設備廠商，定期檢閱並更新，以避免設備已知的漏洞成爲防護破口[20] 。

III. **家用網路設備需使用足夠安全的加密類型：**使用者應選擇使用足夠安全加密類型的設備，例如較新穎的 WPA2 及 WPA3 的加密方式，以保障資訊傳輸中的安全[21]。

IV. **家用網路設備盡量設定禁用 SSID 廣播 (Service Set Identifier Broadcast, SSID Broadcast)：**SSID 是無線網路在供使用者連線時所顯示的名稱，然而，當攻擊者在搜索無線網路時，若接收到該無線網路的 SSID，即有可能將其作爲攻擊目標。因此使用者應將其功能關閉，以手動方式輸入無線網路的 SSID，不讓其他裝置可見，避免成爲攻擊的目標[22] 。

V. **選擇支援 VPN 功能之家用網路設備：**使用者應將網路設備搭配 VPN 進行網路行爲，除了 VPN 可確保除了使用者外不會收到解密後的封包外，更可依據其隱匿使用者眞實位址之特性，避免成爲攻擊者的攻擊目標，減少其安全威脅[23]。

(2). 遠距工作上層應用資安防護機制

A . 遠距會議：

I. **建立會議時需啓用遠距會議密碼：**爲避免不請自來的第三方進入個人會議中，應設定開啓會議密碼，避免不知名的第三者進入後，對會議進行惡意干擾等行爲[24] 。

II. **定期更新遠距會議系統版本：**使用者應定期檢閱其版本是否有更新，或啓用自動更新功能，以確保遠距會議系統的最新版本及最高的安全性[25]。

20 Wired. “How to Secure Your Wi-Fi Router and Protect Your Home Network”. Retrieved April 29, 2020, from the World Wide Web: https://www.wired.com/story/secure-your-wi-fi-router/

21 Norton. “Router security: How to setup Wi-Fi router securely”. Retrieved April 29, 2020, from the World Wide Web: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

22 NordVPN. “How to disable SSID broadcast to hide your Wi-Fi”. Retrieved April 29, 2020, from the World Wide Web: https://nordvpn.com/blog/how-to-disable-ssid-broadcast/

23 Professional Security. “VPN can prevent a man-in-the-middle attack”. Retrieved April 29, 2020, from the World Wide Web: https://www.professionalsecurity.co.uk/news/press-releases/vpn-can-prevent-a-man-in-the-middle-attack/

24 TechRepublic. “How to prevent Zoom bombing: 5 simple tips”. Retrieved April 29, 2020, from the World Wide Web: https://www.techrepublic.com/article/how-to-prevent-zoom-bombing-5-simple-tips/

25 McAfee. “How Secure Is Video Conferencing?”. Retrieved April 29, 2020, from the World Wide Web: https://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-secure-is-video-conferencing/

III. **關閉使用遠距會議裝置之 445 通訊埠：**由於主機的 port 445 是用於傳輸 SMB 訊息，允許主機共享網路上的文件、印表機等資源。然而，這樣的功能卻因爲機制上的弱點，產生將使用者的帳號密碼以弱加密方式傳輸給伺服器進行資源共享，若該伺服器爲攻擊者所控制之惡意伺服器，則使用者的帳號密碼有外洩的可能。因此，使用者應於系統中將 port 445 關閉，或透過防火牆阻擋進出於 port 445 的封包，避免導致使用者資訊外洩的問題[26]。

IV. **會議管理者應設定參與者權限：**遠距會議的管理者應針對所有的參與者設定功能權限，包括不讓非主持人的參與者共享螢幕、拒絕未知的參與者留言或上傳檔案，甚至拒絕允許清單外的參與者進入會議中，大幅降低不請自來的第三者，對遠距會議進行惡意行爲的威脅[27]。

V. **使用者盡量使用瀏覽器執行遠距會議：**隨著遠距會議所需的功能逐漸增加，應用程式會要求主機或系統更多的權限，導致許多權限允許後未能有足夠的防護能量。因此，使用者應盡量使用瀏覽器開啓其系統及服務，雖然較應用程式稍嫌不便，但藉由瀏覽器本身的防護機制和限制，可有效阻擋一些不適切的權限要求，避免產生資料外洩的問題[28]。

B. **遠端存取企業資源：**

I. **於遠端存取伺服器中建立入侵偵測與防禦系統 (Intrusion Detection and Prevention Systems, IDPS)：**對可能發生的異常流量、異常入侵及有害行爲等狀況，應透過 IDPS 進行防護，在第一時間進行確認、防護及紀錄，減少遠距存取功能因遭到攻擊而嚴重影響使用者的資安問題發生[29]。

II. **加密遠端伺服器中的資源：**爲保護在遠端伺服器中的資源，許多伺服器會將其中的資源和檔案進行加密。然而，除了將伺服器中資源加密外，其加密的金鑰應存於本機端或其他伺服器中，即便攻擊者截取使用者與伺服器連線的封包，也難以對其中的資源進行解密竊取機敏資訊[30]。

III. **對遠端存取使用者設定權限分級：**管理者應替遠端伺服器的資源存取設定權限，並將每一種權限所能存取的資源最小化，避免攻擊者在進入後，取得其不應存取的機敏資訊[31]。

---

26 Tom's Guide. "Zoom flaw could steal passwords and install malware: What to do now". Retrieved April 29, 2020, from the World Wide Web: https://www.tomsguide.com/news/zoom-password-malware-flaw

27 UCToday. "Video Conferencing Security: Four Key Considerations". Retrieved April 29, 2020, from the World Wide Web: https://www.uctoday.com/collaboration/video-conferencing/video-conferencing-security-four-key-considerations/

28 Kaspersky. "10 tips for Zoom security and privacy". Retrieved April 29, 2020, from the World Wide Web: https://www.kaspersky.com/blog/zoom-security-ten-tips/34729/

29 Rao, U. H., & Nayak, U. (2014). Intrusion detection and prevention systems. In The InfoSec Handbook (pp. 225-243). Apress, Berkeley, CA.

30 HLN. "Encrypting Data at Rest on Servers: What does it get you?". Retrieved May 5, 2020, from the World Wide Web: https://www.hln.com/encrypting-data-at-rest-on-servers-what-does-it-get-you/index.html

31 BeyondTrust. "Privileged Remote Access Security". Retrieved May 5, 2020, from the World Wide Web: https://www.beyondtrust.com/remote-access/security

IV. **定期針對遠端存取伺服器進行漏洞掃描：**企業除定期檢閱設備廠商資訊外，亦需透過漏洞掃描工具，針對遠端存取伺服器進行漏洞掃描，檢測是否有已知的漏洞仍存在於設備中，讓管理者可透過漏洞報告，及時檢查及修復設備系統[32]。

二、企業供應鏈之資安威脅與防護

1. 供應鏈資安概述

產品供應鏈是指生產流通過程中，從產品原物料採購開始，直到將產品送達最終使用者的一系列企業活動[1]。供應鏈管理爲企業帶來許多創新，在物流、服務流、商流、資金流及資訊流等方面極大化地提升效率。而這些效益的背後，離不開供應鏈的資通訊安全。在供應鏈體系逐漸成爲諸多企業的運作模式，並且轉變成數位化之後，針對整個供應鏈薄弱的一環進行攻擊，讓受害目標無法輕易發現遭受破壞的部分，從而使企業和合作夥伴面臨資料外洩等資安威脅，是近年來備受關注的議題。

一般而言，企業供應鏈的資通安全威脅可分爲兩個層面[2]：

- **軟體供應鏈威脅：**利用受信任的管道散播惡意程式，間接入侵受害目標。例如將惡意程式碼植入網站，以及原始碼遭竄改導致惡意程式散布等，這些來自受信任的管道所造成的危害，認定爲軟體供應鏈威脅。

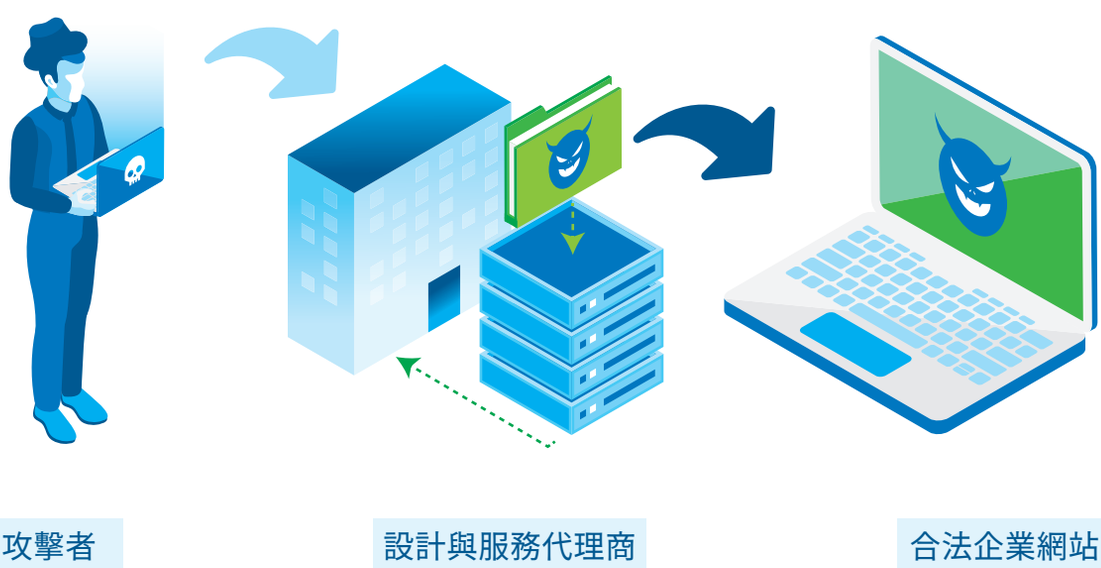


圖 2- 2：軟體供應鏈威脅示意圖　　資料來源：TWCERT/CC 整理

32 One Comodo. “Remote Access Attacks: Securing Your PC From Malware”. Retrieved May 5, 2020, from the World Wide Web: https://one.comodo.com/remote-access-attacks.php

1 張榮圳 . “供應鏈管理資訊分享模式之研究”： https://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi?o=dnclcdr&s=id=%22088NSYS5396022%22.&searchmode=basic (瀏覽日期：2020 年 11 月 22 日)

2 iThome. “【2020 十大資安趨勢 6：供應鏈安全】攻擊型態趨於多元，供應鏈防護需涵蓋 VPN 網路與外部服務”：https://www.ithome.com.tw/news/135178 (瀏覽日期：2020 年 11 月 22 日)

- **硬體供應鏈威脅：**從資通訊上游的積體電路 (Integrated Circuit, IC) 晶片設計開始，直到完成產品組裝賣給消費者的過程中，由不同的企業分工完成各項任務，因而造成不肖的廠商或人員得以在生產製造過程中引入資安威脅，例如在硬體設計中植入木馬，及在韌體程式中留有後門等。

圖 2-3：硬體供應鏈威脅示意圖　　資料來源：TWCERT/CC 整理

企業供應鏈的資安威脅目前以來自軟體類型方面的威脅較多，其中，近年來與臺灣最密切的，莫過於 2019 年國內知名科技公司的更新伺服器遭入侵一案。攻擊者在該公司的更新程式中藏入後門，讓原本用來向其生產之電腦提供基本輸入輸出系統 (Basic Input/Output System, BIOS)、統一可延伸韌體介面 (Unified Extensible Firmware Interface, UEFI) 和軟體更新的工具程式，在檢查是否有系統適用的最新程式時，下載並安裝了遭惡意程式感染的更新程式。由於該受感染的程式含有合法的數位簽章，並且是存放在用於更新的官方伺服器上，這使得它很長一段時間都未被發現。該公司所生產之電腦等設備遍及全球，因此可能使全球超過一百萬的使用者受到影響，而這起攻擊事件被稱爲 ShadowHammer(暗影之鎚)[3]。

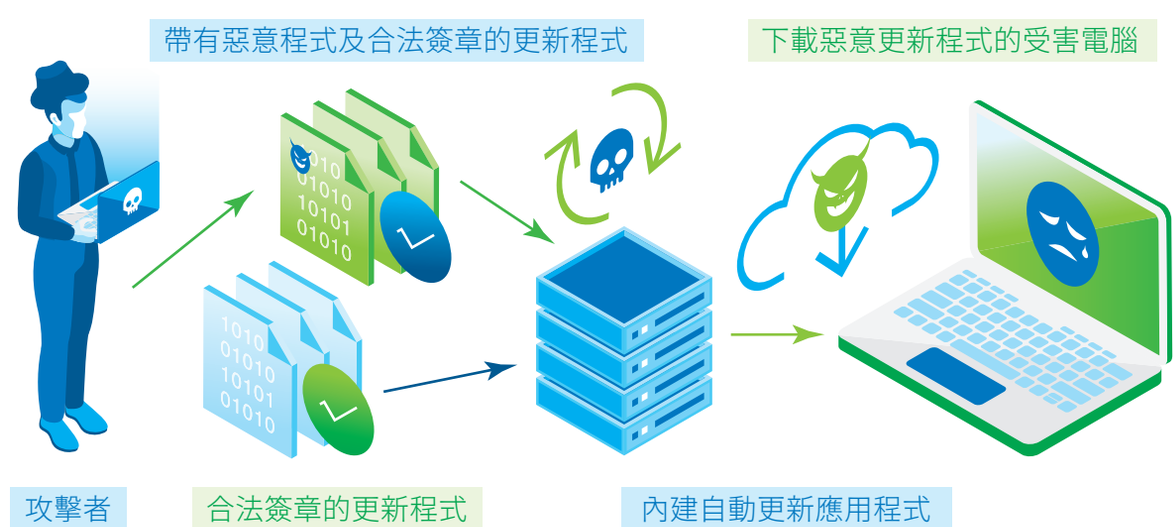


圖 2-4：ShadowHammer 事件示意圖　　資料來源：TWCERT/CC 整理

3 iThome. “華碩軟體更新伺服器竟成惡意後門派送幫兇”： https://www.ithome.com.tw/news/130415 (瀏覽日期：2020 年 11 月 23 日)

著名的硬體供應鏈資安事件，例如美國知名伺服器開發商之伺服器主機板疑似遭植入不明晶片一案。2018 年 10 月，《彭博商業周刊》(Bloomberg Businessweek) 在報導中指出[4]，被蘋果和亞馬遜等近 30 家企業所採用的美國知名資訊科技公司所生產之伺服器主機板，遭秘密植入間諜晶片，攻擊者得以透過該間諜晶片登入，以探查目標企業的機密資訊。此次事件主要是該伺服器委由三家製造商生產其主機板，兩間來自國內、另一間來自上海，但當這三間供應商無法負荷大量訂單時，會將部分工作分派給其分包商，經美國情報機關調查，是四間被外包的分包商。雖然相關單位都否認了該報導，專家也指出彭博商業周刊所描述的間諜晶片攻擊指控在技術上是不可能的[5]，但對於願意投入資源的對手來說，技術上不可能的說法並不存在。

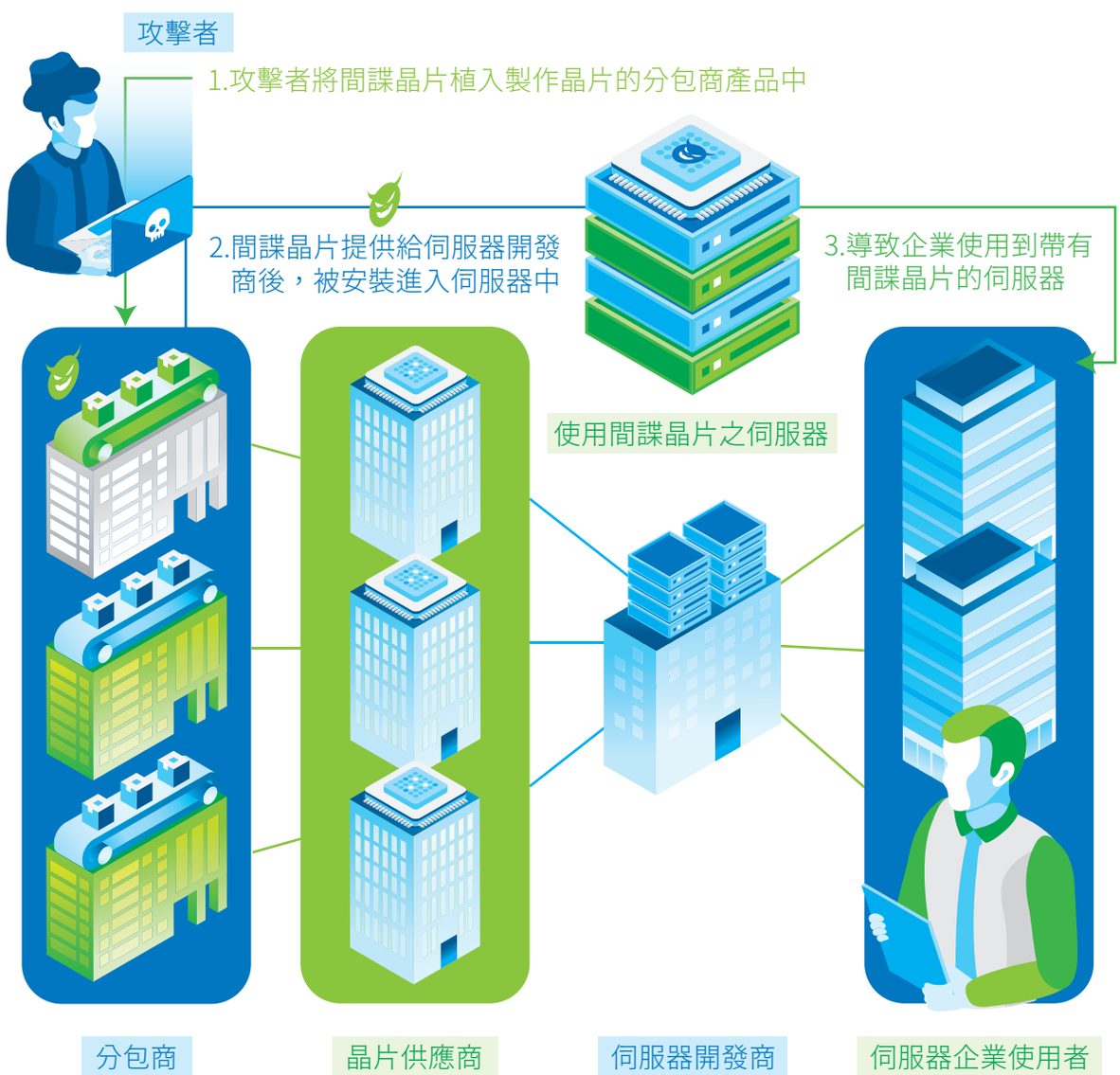


圖 2-5：伺服器開發商遭受間諜晶片攻擊示意圖　　資料來源：TWCERT/CC 整理

4 Bloomberg Businessweek. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”. Retrieved November 26, 2020, from the World Wide Web: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

5 Malcolm Owen. “Bloomberg's iCloud spy chip attack allegations technically impossible”. Retrieved November 26, 2020, from the World Wide Web: https://appleinsider.com/articles/18/10/23/bloombergs-icloud-spy-chip-attack-allegations-technically-impossible

在衆多供應鏈資安問題頻繁出現後，乾淨供應鏈將成爲各國的一大挑戰。例如常以供應鏈模式生產的半導體產業，其供應鏈安全將會對各個國家的基礎建設、國防、第五代行動通訊網路 (5th Generation Mobile Networks, 5G)、自動駕駛及工業系統等重要領域有關鍵性的影響，因此，供應鏈的防範與資安規範近年來也受到極大的重視。

2. 供應鏈資安規範發展現況

有鑑於攻擊型態趨於多元，供應鏈的安全對國內出口貿易及國家安全都十分重要，於是強韌的供應鏈及可信賴性遂成爲關鍵。目前我國與供應鏈資安相關的法規衆多[6]，較爲常見且重要的彙整如表 2- 1：

法規名稱	訂定單位	運作對象	目的
行動應用 App 基本資安檢測基準[7]	經濟部工業局、資策會	App 開發者	提升國內行動應用 App 基本安全防護能力。
智慧型手機系統內建軟體資通安全檢測技術規範[8]	國家通訊傳播委員會	智慧型手機製造商、經銷商及電信業者	智慧型手機系統及其系統內建軟體，以確保其符合現階段資訊安全要求。
影像監控系統資安標準測試規範[9]	經濟部工業局	影像監控系統裝置製造商、系統整合商	全面改善影像監控系統資安品質，協助國內產業接軌國際，提升研發技術及保證產品質量。
智慧巴士資通訊系統系列資安標準 & 測試規範[10]	經濟部工業局	國內智慧巴士車載資通訊系統相關業者	產品研發時之安全設計準則，以提升國內智慧巴士資通訊系統相關產品之品質及競爭力。
資通安全管理法[11]	行政院	公務機關或特定非公務機關	當機關委外辦理資通系統之建置、維運或資通服務時，必須確保受託者之相關資安品質。

表 2- 1：國內與供應鏈資安相關法規彙整表　　資料來源：[7], [8], [9], [10], [11]

6 張文村 . “後疫情時代全球資安市場趨勢與臺灣的機會”：https://s.itho.me/ events/2020/accs/1.%20III-CSTI_Dr.%20Chang.pdf (瀏覽日期：2020 年 11 月 26 日)

7 經濟部工業局 . “行動應用 App 基本資安自主檢測推動制度”：https://www.mas.org.tw/spaw2/uploads/files/03_1.pdf (瀏覽日期：2020 年 11 月 27 日)

8 國家通訊傳播委員會 . “智慧型手機系統內建軟體資通安全檢測技術規範”：https:// www.ncc.gov.tw/chinese/files/17030/566_37087_170303_2.pdf (瀏覽日期：2020 年 11 月 27 日)

9 經濟部工業局 . “影像監控系統資安標準測試規範”：http://www.tssia.org.tw/archive/file/ 影像監控系統資安標準測試規範 - 第一部 _ 一般要求 .pdf (瀏覽日期：2020 年 11 月 27 日)

10 經濟部工業局 . “智慧巴士資通訊系統系列資安標準 & 測試規範”：https://www.taics.org.tw/ LatestAssForm.aspx?Type=1&Ass_id=1055 (瀏覽日期：2020 年 11 月 27 日)

11 全國法規資料庫 . “資通安全管理法施行細則”：https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030303 (瀏覽日期：2020 年 11 月 28 日)

這些企業生產之產品或服務能從源頭交到終端使用者手中，有賴於供應鏈上下游各企業及供應商的通力合作。但在供應鏈中卻有太多規模大小不一、資安水準參差不齊的廠商參與其中，有諸多不確定且難以控制的因素，除了可能成爲資安威脅的破口，一旦發生資安事件，很難在第一時間找到肇事者。因此，爲避免供應鏈攻擊的發生，單一企業即便再努力防範也無法遏止，必須倚賴供應鏈中所有企業彼此合作、努力，方能杜絕在一系列供應鏈中所產生的資安威脅，建造一個乾淨、安全的供應鏈環境。

三、半導體產業工業控制系統資安概述

1. 半導體產業工業控制系統之資安威脅

德國政府於 2013 年提出以「智慧製造」爲革命重點之工業 4.0 計畫，其中，工業控制系統 (Industrial Control System, ICS，簡稱工控系統) 是半導體產業運作的核心，該系統會定期從現場設備中取得設備資訊並分析後，進行運行設備間的調整及事件的警示。

在半導體產業的運作中，資訊系統會對生產運作中產生的數據資料進行分析，提升生產過程的效率、透明性和靈活度。然而，這些圍繞數據建構的智慧工廠，其網路安全和資料安全將變得十分關鍵。一旦攻擊者進入企業內部，由於其系統相連，提供了跨越資訊科技 (Information Technology, IT) 和營運技術 (Operation Technology, OT) 系統進行惡意活動的機會。因此，預防工業控制系統安全事件的發生，已逐漸成爲全球關注的議題。

(1). 產業資安議題

製造業其產線，在生產效率極大化的重要考量下，資安一直不是工業企業所考慮的重點。但隨著工業 4.0 時代的來臨，產生了 IT 與 OT 融合後的安全挑戰，但製造業中機台運作時間可能長達 20 至 30 年，這些長期支援 (Long-Term Support) 的生產設備、系統在當初並沒有考慮到在複雜 IT 網路環境中的資安問題，如完整性 (Integrity)、身分驗證 (Authenticity) 等安全需求，也沒有預期到將會需要與 IT 環境進行資料互通，導致許多資安問題的產生[1] 。

2016 年，美國工業控制系統網路緊急應變小組 (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) 公布了 6 大影響工業控制系統 ICS 之安全性問題，彙整如表 2- 2[2]：

ICS 安全性問題	ICS 安全性問題描述	ICS 安全性問題防範建議
安全控制不足	工控系統往往對使用者存取安全控制不足，攻擊者可利用這些弱點，對 ICS 進行未經授權的存取。	系統或虛擬機應放置在嚴格且做好存取紀記錄的受管理網路內，並確保擁有適當安全控制。

1 iTHome. “【資安危機衝擊製造業拉警報】正視工廠生產線上的資安威脅，徹底改變防護概念爲當務之急” https://www.ithome.com.tw/news/126417 (瀏覽日期：2020 年 3 月 10 日)

2 Industrial Control Systems Cyber Emergency Response Team. “ICS-CERT Annual Assessment Report FY 2016”. Retrieved March 6, 2020, from the World Wide Web: https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

資料來源：[2]

ICS 安全性問題	ICS 安全性問題描述	ICS 安全性問題防範建議
不安全的遠端存取	透過遠端入侵及存取使用者帳戶，獲取使用者憑證或透操控擁有權限的裝置，以取得工控系統相關權限。	系統或虛擬機應放置在嚴格且做好存取紀錄的受管理網路內，並確保擁有適當安全控制。
不正確使用區域網路	若企業未確實設定虛擬區域網路 (Virtual Local Area Network, VLAN) 與建立安全規範，則攻擊者可能在入侵其中一個 VLAN 區段後，遍歷其他 VLAN 區段。	企業必須訂定遠端存取的權限標準，以及如何強化存取過程安全，例如使用多重身分驗證等，以降低這些風險。
自攜設備 (Bring Your Own Device, BYOD) 對工控系統的威脅	員工個人的行動裝置通常不會由企業管理，因此使用個人行動裝置存取企業相關資訊，對工控系統是高風險的行爲。	企業必須考慮此風險，並應採取使用行動裝置管理系統等措施，以將風險降低。
對雲端服務安全性和服務水平協議 (Security Level Agreement, SLA) 的強化不足	企業難以確保外部託管及雲端上的任何工控系統部分與內部工控系統的安全級別，避免讓外部託管之系統成爲資安漏洞。	企業可以簽署 SLA 協議，包括企業應確保雲端服務提供商足以維持與系統恢復 (Recovery)、事件管理 (Incident Management)，失效備援 (Failover)、鑑識支援 (Forensic Support) 及監控 (Monitor) 等功能。
未將工控系統網路監控作深度防禦 (Defense-in-Depth, DiD) 核心戰略	深度防禦戰略中，網路監控爲最基本之安全措施。然而，許多企業雖都有在 IT 網路中進行監控，卻很少監控工控系統網路。	企業須查閱工控系統運行紀錄，並使用資訊安全和事件管理類產品協助搜集、記錄並彙整來源資訊，當有異常或指定活動時發出警報，並即時分析，以利企業提早採取預防措施。

表 2- 2：ICS-CERT 提出之工控系統安全性問題及防範建議統整表

近年來，身爲製造業王國的台灣企業也積極將工廠朝向智慧製造邁進。但當工業控制系統逐漸地與企業內部資訊網路相融合，各種在 IP 網路所發生的資安問題及漏洞等潛在威脅逐漸浮上檯面[3]。尤其產業常見的併購、設備投資及擴廠等行爲，導致設備及廠區存在著不同的資訊基礎架構，或彼此間的資安水平不一。無法掌握各廠區的資安現況與弱點，是目前台灣半導體產業的主要問題之一。

3 李震華 . “全球資訊安全產業趨勢發展研究“： https://books.google.com.my/books?id=PxzBDwAAQBAJ&printsec=frontcover&hl=zh-TW&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (瀏覽日期：2020 年 1 月 16 日)

(2). 常見攻擊手法與防禦對策

工業控制系統是攻擊者極具價值的目標之一，攻擊者一旦獲得控制權，將會產生大量資料外洩與破壞等重大威脅。而針對工業控制系統的常見攻擊如表 2- 3[4]：

攻擊類型	攻擊手法	工控系統攻擊案例	防範建議
緩衝區溢位 (Buffer Overflow)	在暫存區存取超出容量的資料時引發的漏洞，是攻擊者常用來攻擊工業控制系統的手法。	2019 年某工業自動化廠商之軟體系統中，發現緩衝區溢位漏洞，無法正確驗證使用者身分。該廠商於兩個月內提出補丁程式解決問題[5]。	在程式撰寫時應實施程式碼檢查及完整性檢查，避免此問題發生[6]。
魚叉式網路釣魚 (Spear Phishing)	針對企業員工進行社交工程攻擊，再將受害者主機作爲跳板取得進入工控系統的機會。	2016 年，出現針對工控系統的魚叉式網路釣魚攻擊，假冒供應商、物流公司或銀行，且來源都是遭操控的合法來源，導致使用者下載含惡意程式的附件，讓攻擊者順利入侵工控系統進行惡意操作[7]。	收到相關訊息應立即查證寄送者身分，且企業應提供足夠的教育訓練予其員工。
SQL 注入漏洞 (SQL Injection)	複雜的工控系統應用程式可能擁有許多進入點，一旦程式開發人員沒有針對所有可能的輸入形式進行測試時，攻擊者就可能透過 SQL 注入漏洞進行攻擊。	一美國工程服務公司用於監控和管理現場設備狀態的軟體，在 12.5 及更早版本存在 SQL 注入漏洞。攻擊者透過輸入特殊格式，可成功取得系統管理員權限，該公司在知悉後，立即提出相關緩解方式及版本升級，避免該漏洞造成的資安威脅[8]。	企業應針對連線進行白名單規範，並且爲防範 SQL 注入攻擊，應設置當使用者欲取得特定功能時是直接呼叫資料庫取得，以避免受攻擊[8]。

表 2- 3：工業控制系統常見攻擊手法、案例與防範建議統整表

4 IBM. “Security attacks on industrial control systems. How technology advances create risks for industrial organizations”. Retrieved January 6, 2020, from the World Wide Web: https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-4573&S_PKG=ov39538&_ga=2.34200801.1303401921.1580475869-875586014.1580475869

5 Tenanble. “Multiple Advantech WebAccess Vulnerabilities”. Retrieved March 19, 2020, from the World Wide Web: https://zh-tw.tenable.com/security/research/tra-2019-28?tns_redirect=true

6 InfoSec. “Destructive Security Flaws in Industrial Control Systems”. Retrieved April 9, 2020, from the World Wide Web: https://resources.infosecinstitute.com/destructive-security-flaws-industrial-control-systems/#gref

7 Kaspersky Lab ICS CERT. “Spear phishing attack hits industrial companies”. Retrieved April 9, 2020, from the World Wide Web: https://ics-cert.kaspersky.com/alerts/2016/12/16/spear-phishing-attack-hits-industrial-companies/

8 CVE-2015-1008. “SQL injection vulnerability in Emerson AMS Device Manager before 13”. Retrieved March 19, 2020, from the World Wide Web: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1008

資料來源：[5], [6], [7], [8], [9], [10], [11], [12]

攻擊類型	攻擊手法	工控系統攻擊案例	防範建議
分散式阻斷攻擊 (Distributed Denial of Service, DDoS)	工控系統往往需要專用且獨立的訊息通道和網路進行通訊，因此攻擊者可透過 DDoS 攻擊，透過大量封包或資訊干擾以中斷其通訊網路。	戰略與國際研究中心 (Center for Strategic and International Studies, CSIS) 表明，DDoS 攻擊在能源、電力、水利部門數量較多，且通常針對電腦操作的工控系統，因爲當系統服務中斷，可能產生大規模停電等災難[9]。	透過入侵監測系統 (Intrusion Detection System, IDS) 提高網路安全，透過識別協定及異常流量，從而進行有效防禦[10]。
暴力破解 (Brute-Force Attack)	爲求便利，設備密碼往往不會過於複雜，甚至許多仍以預設密碼延續使用。這些強度較弱的密碼容易被暴力破解方式破解，甚至直接以預設密碼順利進入系統。	2014 年工控系統遭入侵事件中，發現用於管理控制系統的軟體能透過一台可連結網際網路的主機進行存取。由於該工控系統配置遠端存取功能和使用簡單的密碼原則，攻擊者便利用暴力破解技術成功入侵[11]。	廠商應修改設備預設密碼，或設備供應商使用唯一預設密碼。亦可添加多重認證機制，避免遭攻擊者入侵[12]。

2. 國內半導體產業相關資訊安全標準與指引

近年來，促進全球電子業供應鏈發展及建立產業技術標準之國際半導體產業協會 (Semiconductor Equipment and Materials International, SEMI)，在半導體、平面顯示器、太陽光電、奈米科技等領域的標準制定與推動已有顯著成果，但隨著全球半導體業資安威脅逐漸增加，SEMI 台灣技術委員會於 2019 年初成立晶圓廠及設備資訊安全任務小組 (Fab and Equipment Information Security Task Force)，建立半導體產業資安相關標準之訂定。

由於 SEMI 相關資安標準是將其範疇劃分後分別由國際各地區 SEMI 組織負責，而各 SEMI 組織在取得新標準提案表單 (Standards New Activity Report Form, SNARF) 案號後，將會針對該案號的標準範疇進行撰寫及制定。而台灣 SEMI 組織負責 SNARF 案號 6506，主要目標爲建立半導體業晶圓廠及其設備機台系統標準，企盼能增加系統的自我保護機制

9 McAfee. “In the Crossfire. Critical Infrastructure in the Age of Cyber War”. Retrieved January 24, 2020, from the World Wide Web: https://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf

10 NSFocus. “ICS Information Security Assurance Framework 19”. Retrieved April 9, 2020, from the World Wide Web: https://nsfocusglobal.com/ics-information-security-assurance-framework-19/

11 NCCIC. “ICS-CERT Monitor Jan - April 2014”. Retrieved January 26, 2020, from the World Wide Web: https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf

12 CISA. “Alert (TA13-175A) Risks of Default Passwords on the Internet”. Retrieved April 9, 2020, from the World Wide Web: https://www.us-cert.gov/ncas/alerts/TA13-175A

(Self-Protection Mechanism)[13]。在 SNARF 案號 6506 中，爲保障半導體晶圓廠設備資訊安全的有效性，國內 SEMI 提出了四個觀點，彙整如表 2- 4：

標準規範項目	欲解決之問題	防範建議	ICS-CERT 防範項目
電腦作業系統安全性 (Computer Operation System Security)	許多都屬於長期支援設備，且由於其配置的複雜性及廠商以生產作業爲重，使得設備無法定期更新，容易因版本老舊而產生資安問題。	該標準制定半導體廠商對長期支援設備的配置、維護及更新規範。設備廠商只能販售規定時間內的新作業系統設備。	安全控制不足不安全的遠端存取
網路安全性 (Network Security)	許多廠商在配置時，未能確實切割及隔離區域網路，因此當一設備遭到入侵，攻擊者便可透過網路入侵整個廠房甚至整個企業。且許多晶圓廠雖有意進行網路的配置和隔離，但因設備廠商未提供相關功能，難以自行實現。	該標準訂定相關網路配置規範，例如要求關閉易遭受攻擊的埠口 (Port)，或要求必須要裝設防火牆等防護設備。而設備廠商則需提供設備文件，將其網路連接、連接對象等詳細列出，並要求應包含一定的防護功能。	不正確使用區域網路
端點防護 (End-Point Protection)	由於晶圓廠設備多爲長期使用，難以定期進行系統更新，可能導致難以偵測新型態之惡意程式。且有些使用者爲增加便利性，安裝其他應用程式，卻可能致使惡意的應用程式進入機台中，卻因爲病毒碼及相關防護系統未能及時更新而無從察覺。	該標準認爲廠商在販售設備時便能包含安全防護功能。設備設計時也應將防護軟體的設置納入考量，使得晶圓廠容易安裝及更新。此外，晶圓廠更需建立應用程式白名單機制，避免員工或攻擊者將惡意應用程式安裝於機台中。	未將工控系統網路監控做深度防禦
安全監控 (Security Monitor)	對晶圓廠而言，過往記錄的資訊，大多都以運行的資訊爲主，鮮少記錄資安相關資訊以及進行後續統計分析，導致不論是即時警示、應急處理或事後鑑識，都相當不利，甚至可能導致資安事件影響層面擴大。	該標準建議晶圓廠商應修改其記錄項目，必須涵括可供事件分析之項目，如使用者、IP 位址等資訊，且應定期統整分析，即時提出警告。如此，便可在事件發生初期即收到警示，並根據彙整資訊進行後續處理。	未將工控系統網路監控做深度防禦

表 2- 4：SEMI 台灣技術委員會 SNARF 標準規範統整表　　資料來源：TWCERT/CC 整理

13 SEMI. “SEMI International Standards - Standards New Activity Report Form (SNARF)”. Retrieved January 27, 2020, from the World Wide Web: http://downloads.semi.org/web/wstdsbal.nsf/b8865fa87d9e7b57882579fb005c3cd7/749b1380634ba023882583dc0051a2b4!OpenDocument

在 2020 年 3 月，台灣 SEMI 組織已將 SNARF 6506 送交委員會審閱，後續若該標準獲得逾六成的票數後，便會成爲全球半導體產業的資安標準之一。該標準在半導體產業間彼此之共識下，將會影響全球所有半導體廠商之資安規劃，可降低資安威脅，提升資安防護能量。

第二節、網際網路之資安與防護

一、IPv6 資訊安全威脅與防護

1.IPv6 資安威脅

(1).IPv6 介紹

IP (Internet Protocol) 是用以分配給所有連網之主機，爲一種特定的標籤，讓資訊得以在一段期間內在兩個主機之間來回傳送及溝通。最初也是被使用最廣泛的網際網路協定爲網際網路通訊協定第四版 (Internet Protocol version 4, IPv4)，但近年不論是伺服器、個人電腦、行動裝置，甚至是物聯網裝置數量都急速增加，導致 IPv4 位址數量在 2011 年就已經被宣告即將用罄，而各區域網際網路註冊機構 (Regional Internet Registry, RIR) 針對 IPv4 位址缺少的狀況，都紛紛提出相關的限制措施，彙整如表 2- 5：

單位	地區	最後公告	相關措施
美洲網際網路位址註冊組織 (American Registry for Internet Numbers, ARIN) [1]	美國、加拿大及北大西洋群島地區	2015 年 9 月 24 日	• IPv4 位址已宣告耗盡。 • 僅接受關鍵基礎設施申請些微 IPv4 位址，以及用以促進 IPv6 部署之 IPv4 位址申請。 • 一般申請者僅能等待他人之 IPv4 位址釋出。
亞太網路資訊中心 (Asia-PacificNetwork Information Centre, APNIC) [2]	亞太地區	2019 年 7 月 2 日	• IPv4 已宣告耗盡。 • 刪除非保留區塊 (103 /8) 的 IPv4 位址等待清單，該清單爲成員自保留區塊取得 IPv4 位址後，額外申請之用，因此刪除該清單，將 IPv4 位址保留給新成員。 • 他人釋出的 IPv4 位址，都將回到保留區塊 (103 /8)，不提供已有 IPv4 位址成員申請。

1 ARIN. “IPv4 Addressing Options”. Retrieved January 30, 2020, from the World Wide Web: https://www.arin.net/resources/guide/ipv4/

2 APNIC. “IPv4 exhaustion”. Retrieved January 30, 2021, from the World Wide Web: https://www.apnic.net/manage-ip/ipv4-exhaustion/

單位	地區	最後公告	相關措施
歐洲網路資訊中心 (Réseaux IP Européens Network Coordination Centre, RIPE NCC) [3]	歐中、中東及中亞地區	2019 年 11 月 25 日	• IPv4 已宣告耗盡。 • 申請者僅能等待他人之 IPv4 位址釋出。 • 不再接受已有 IPv4 位址的申請者申請。
非洲網路資訊中心 (African Network Information Centre, AFRINIC) [4]	非洲地區	2020 年 1 月 13 日	• /8 的 IPv4 位址中，可用空間已小於 /11。 • 成員能取得的 IPv4 位址，最大限制爲 /22，最小爲 /24。 • 成員須證明其 IPv4 資源使用率高於 90%，才能額外取得更多 IPv4 位址。
拉丁美洲網域名稱註冊管理機構 (Latin American and Caribbean Internet Addresses Registry, LACNIC) [5]	拉丁美洲及加勒比海等地區	2020 年 8 月 19 日	• IPv4 已宣告耗盡 • 僅剩爲關鍵基礎設施保留的 IPv4 位址。 • 一般申請者僅能等待他人 IPv4 位址釋出。

表 2- 5：各地區 IPv4 狀態與相關措施彙整表　　資料來源：[1], [2], [3], [4], [5]

因此，爲因應需求量越來越高之 IP 需求，網際網路工程任務組 (Internet Engineering Task Force, IETF) 在 1998 年創建網際網路通訊協定第六版 (Internet Protocol version 6, IPv6)。IPv6 爲 128 位元之網路位址，除擴充所需 IP 數量外，也提供相較於 IPv4 的改善及優勢[6]：

A. 高效路由：IPv6 較 IPv4 簡化其路由表，增加路由效率且明確分層，同時 IPv6 也允許網際網路服務供應商 (Internet Service Provider, ISP) 將其客戶的前綴 (Prefix) 聚合成單一前綴，並且將此前綴宣告給 IPv6 的網際網路做爲路由資訊。

B. 高效封包處理：IPv6 將其封包標頭 (Header) 進行簡化，使其封包處理效率增加。

3 RIPE NCC. “The RIPE NCC has run out of IPv4 Addresses”. Retrieved January 3, 2020, from the World Wide Web: https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses

4 AFRINIC. “AFRINIC enters IPv4 Exhaustion Phase 2”. Retrieved January 30, 2021, from the World Wide Web: https://afrinic.net/20200113-afrinic-enters-ipv4-exhaustion-phase-2

5 LACNIC. “IPv4 Depletion Phases”. Retrieved January 30, 2020, from the World Wide Web: https://www.lacnic.net/1039/1/lacnic/ipv4-depletion-phases#tabs-1

6 NetworkComputing. “Six Benefits Of IPv6”. Retrieved January 4, 2020, from the World Wide Web: https://www.networkcomputing.com/networking/six-benefits-ipv6

C. **定向資料流：**IPv6 可支援群播 (Multicast)，可將資料流同時發送至多個特定目標，較單點傳播 (Unicast) 解決多點傳輸問題，也較廣播 (Broadcast) 方式更加節省頻寬。

D. **網路設定簡化：**IPv6 內建自動位址指派技術 (StateLess Address AutoConfiguration, SLAAC)，路由器將會在其宣告中傳送其前綴資訊，並讓主機自動產生 Host ID 後，將其前綴資訊加上 Host ID，便可生成自身之 IP 位址[7]。

E. **支援更多服務：**透過移除網路位址轉換 (Network Address Translation, NAT)，IPv6 可以實現眞正的端到端 (End-to-End) 之連線，從而支援更多有價值的網際網路服務。

F. **安全性：**IPv6 協定中明確規範了網際網路安全協定 (Internet Protocol Security, IPsec)，用以確保傳輸時資料的機密性 (Confidentiality)、完整性 (Integrity) 及身分鑑別 (Authentication)，增強針對 IP 位址的安全性。

(2).IPv6 發展趨勢與分析

依據統計，2020 年 12 月，全球 IPv6 施行平均比例爲 28.18%，以 RIR 區分，其比例如表 2- 6[8]：

地區	IPv6 比例
全球	28.18%
ARIN	34.73%
APNIC	32.20%
LACNIC	25.23%
RIPE NCC	22.99%
AFRINIC	0.96%

表 2- 6：2020 年 12 月全球各地區 IPv6 建置比例　　資料來源：[8]

而台灣在全球 IPv6 施行比例中總計 50.68%，並於 APNIC 所統計之共 244 個國家中排名第 7、亞洲地區第 3，詳細資訊如表 2- 7。

全球排名	ccTLD	國家	洲別	IPv6 建置比例
1	IN	印度	亞洲	72.98%
2	BE	比利時	歐洲	63.05%
3	YT	馬約特島	非洲	62.95%

7 財團法人台灣網路資訊中心 . “IPv6 寬頻分享器介紹”： https://blog.twnic.net.tw/2019/02/27/2746/ (瀏覽日期：2021 年 2 月 1 日)

8 APNIC. “IPv6 Capable Rate by country (%)”. Retrieved February 1, 2021, from the World Wide Web: https://stats.labs.apnic.net/ipv6

全球排名	ccTLD	國家	洲別	IPv6 建置比例
4	BL	聖巴瑟米	美洲	57.33%
5	MY	馬來西亞	亞洲	54.86%
6	US	美國	美洲	52.82%
7	TW	台灣	亞洲	50.68%
8	GR	希臘	歐洲	50.57%
9	DE	德國	歐洲	50.49%
10	CH	瑞士	歐洲	46.73%
11	VN	越南	亞洲	45.70%
12	JP	日本	亞洲	44.37%
41	CN	中國	亞洲	20.62%
61	KR	韓國	亞洲	11.25%
96	HK	香港	亞洲	1.46%

表 2-7：2020 年 12 月全球 IPv6 建置比例排名　　資料來源：[8]

相對於 IPv4，IPv6 施行時間較短、成熟度也相對較低，較難大規模驗證 IPv6 的安全性及完整性。此外，導入 IPv6 時也較無明顯準則。因此，仍有許多的潛在威脅必須待 IPv6 愈發成熟，甚至經過多次資安問題的發現及修補後方能完善其機制。而其目前已知之資安威脅大約可分爲以下數種：

A. 洪水攻擊 (Flood Attack)：

I. **攻擊手法：**透過大量的封包傳輸及要求回應，造成受害者來不及處理相關作業，導致系統的服務中斷。

II. **IPv4 攻擊方式：**在 IPv4 中，經常使用的攻擊手法爲 IP Null Attack，攻擊者將封包的標頭設爲零或 Null，由於許多路由器或防火牆會將該封包認定爲未分類的數據封包並允許進入，導致無法有效阻擋大量的惡意封包。

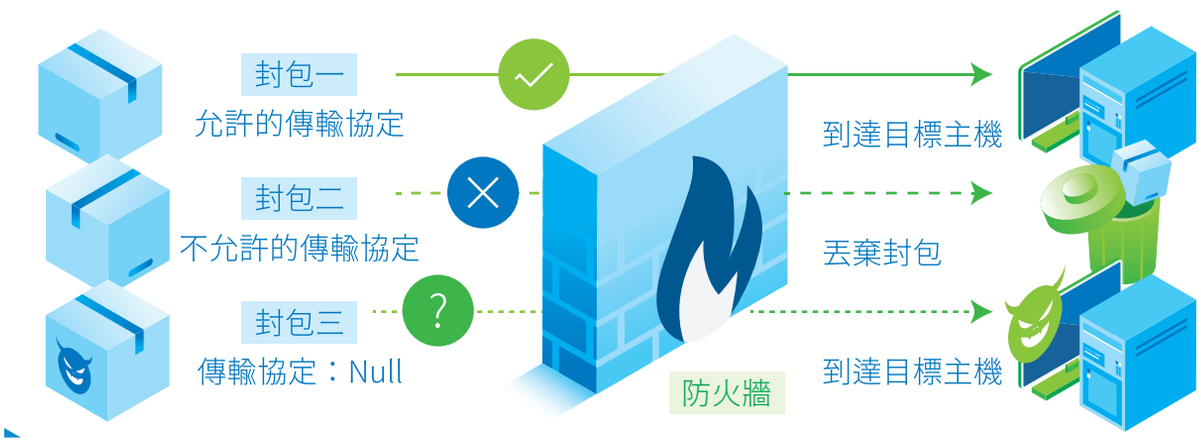


圖 2- 6：IPv4 洪水攻擊手法示意圖　　資料來源：TWCERT/CC 整理

III. **IPv6 解決方式：**IPv6 協定中已經將該標頭類型移除，使得封包所經之路由器不需特別解讀及處理，除了可增加路由器的處理速度外，也可避免 IP Null Attack。

IV. **IPv6 攻擊方式：**IPv6 簡化封包標頭，需額外資訊時再以擴充標頭 (Extension Header) 標示。然而，這也導致攻擊者將封包大小增加，更容易地達到阻斷服務之攻擊[9]。

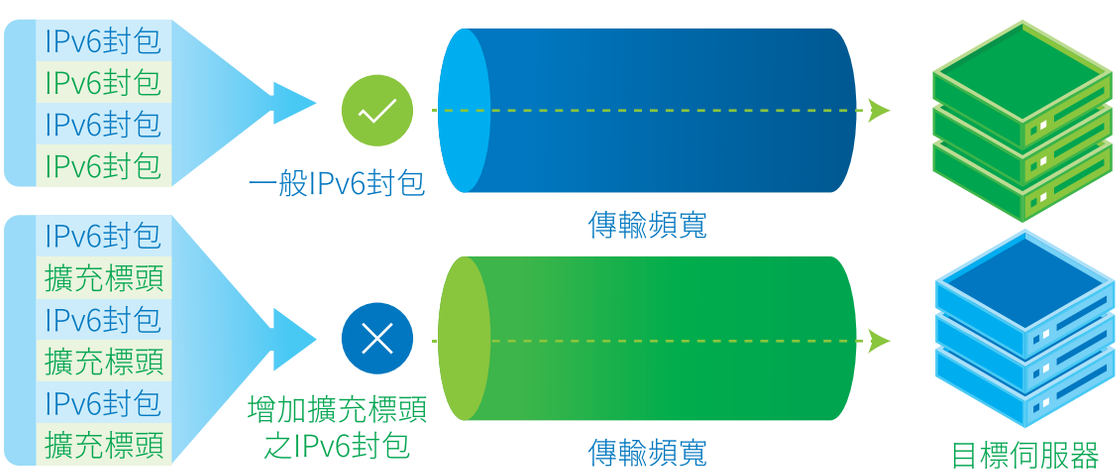


圖 2- 7：IPv6 洪水攻擊手法示意圖　　資料來源：TWCERT/CC 整理

9 Cisco. “IPv6 Extension Headers Review and Considerations”. Retrieved January 5, 2020, from the World Wide Web: https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

B. 分散式阻斷服務攻擊 (DDoS)：

I. **攻擊手法：**攻擊者會先偽冒成受害目標的 IP 位址，並透過大量的回覆訊息，使受害者服務中斷。

II. **IPv4 攻擊方式：**IPv4 支援廣播功能，可以 Ping 請求詢問所有範圍內裝置查找目標主機。卻導致攻擊者偽冒受害者 IP 發出大量 Ping 請求，讓收到的所有裝置回覆網際網路控制訊息協定 (Internet Control Message Protocol, ICMP) 的 Echo 訊息，導致受害者因大量封包湧入造成服務中斷。

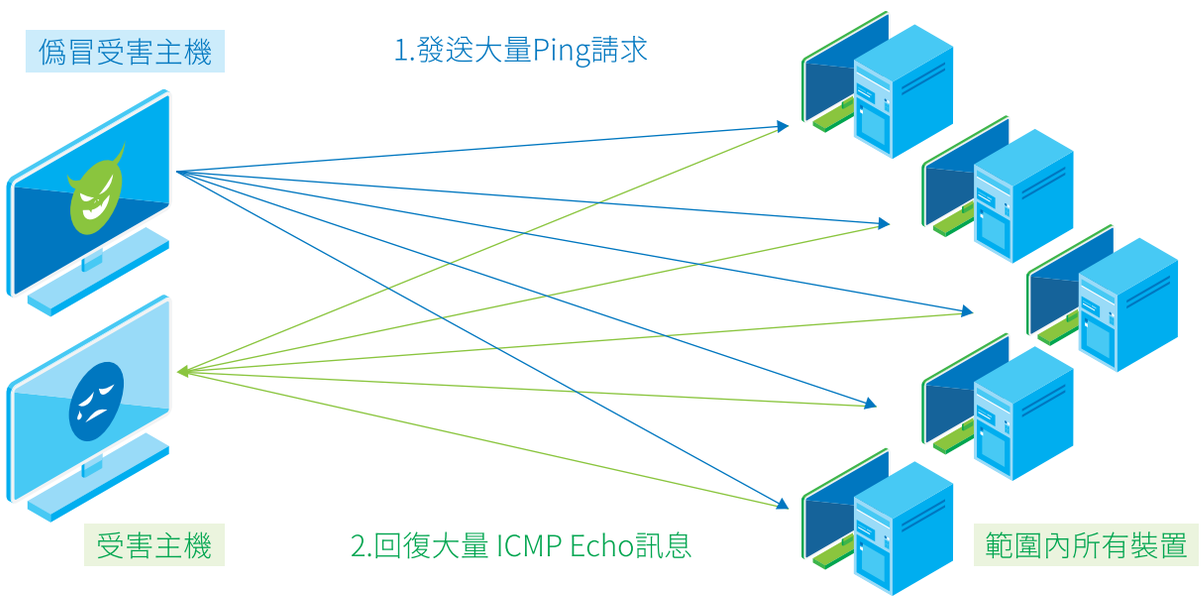


圖 2- 8：IPv4 DDoS 攻擊手法示意圖　　資料來源：TWCERT/CC 整理

III. **IPv6 解決方式：**IPv6 不支援廣播功能。

IV. **IPv6 攻擊方式：**IPv6 雖不支援廣播功能，但其群播功能與之相仿，攻擊者會先偽冒受害者 IP 後，對所有可連接的裝置進行群播，迫使該網段所有裝置或節點均回覆 ICMPv6 Reply 訊息，同樣致使受害者因突如其來大量的封包而中斷服務。

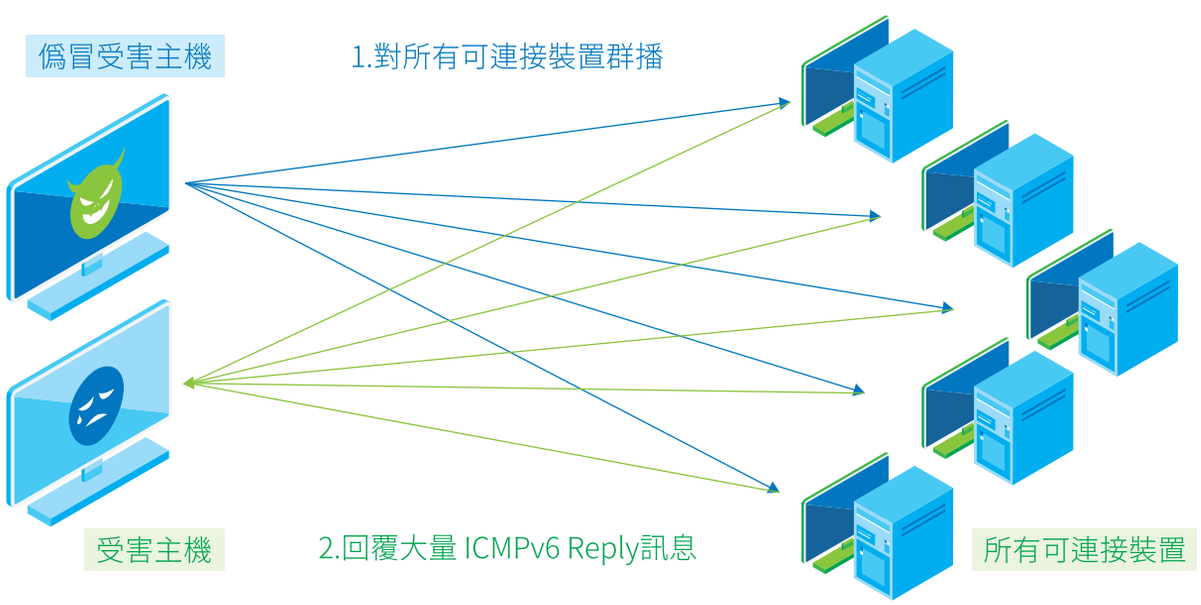


圖 2- 9：IPv6 DDoS 攻擊手法示意圖　　資料來源：TWCERT/CC 整理

C. 未經驗證或僞冒的裝置 (Rogue Devices)：

I. **攻擊手法：**攻擊者會僞冒受害主機必須連接的伺服器，致使受害主機所連接之節點被改爲攻擊者僞冒之惡意節點。

II. **IPv4 攻擊方式：**攻擊者僞冒動態主機設定協定 (Dynamic Host Configuration Protocol, DHCP) 伺服器，再將僞冒訊息發布給受害者，導致使用者無法聯網、流量遭到竊聽，甚至使受害主機連入惡意目標。

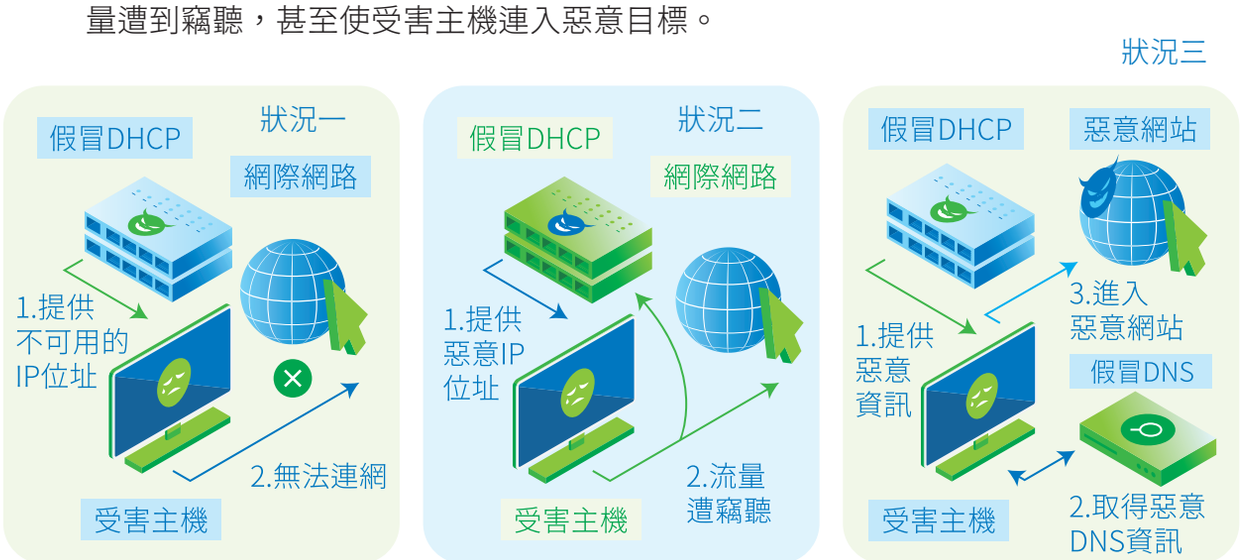


圖 2- 10：IPv4 僞冒裝置攻擊手法示意圖　　資料來源：TWCERT/CC 整理

III. **IPv6 解決方式：**IPv6 本身提供自動位址指派技術 (SLAAC) 的功能，不一定需要 DHCP 才能取得 IP 位址。

IV. **IPv6 攻擊方式：**攻擊者可透過僞冒路由，並在網路上發布其 IPv6 路由器公告 (Router Advertisement, RA)，讓使用者主機在收到該資訊後設定 IPv6 Route，導致該主機所連接之第一個節點即爲駭客所僞冒之惡意設備。

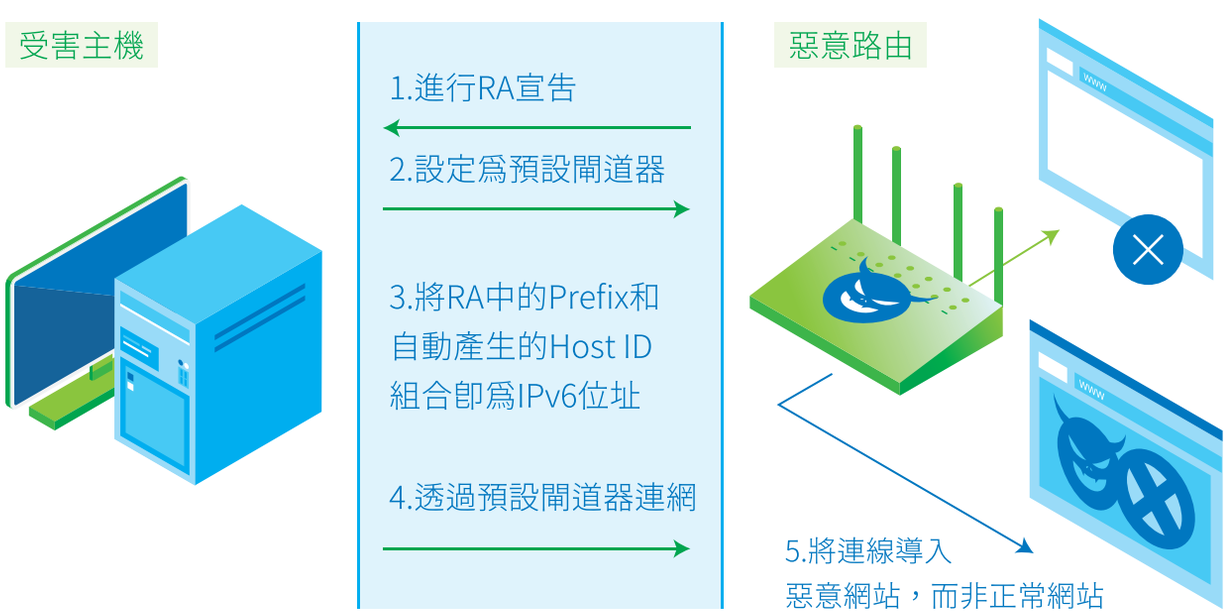


圖 2- 11：IPv6 僞冒裝置攻擊手法示意圖　　資料來源：TWCERT/CC 整理

D. 透過 NAT 將 IPv4 與 IPv6 轉換時弱點所造成之中間人攻擊：

I. **攻擊手法：**此爲 IPv4 與 IPv6 兩者相同之攻擊手法，主要是透過 IPv4 與 IPv6 轉換時的弱點所造成。

II. **IPv4 與 IPv6 攻擊方式：**NAT-PT(Network Address Translation–Port Translation) 爲一種 IPv4 與 IPv6 轉換技術，除了將其封包格式轉換外，透過 SLAAC 協定，在將 IPv4 轉換爲 IPv6 時，其前面 /96 會是來自路由器的固定 Prefix，再將 IPv4 的位址加於 /96 位址的後面，即爲轉換後的 IPv6 位址。

然而，這也導致只要攻擊者建立一惡意的 NAT-PT 路由器，且與使用者主機連線端僅使用 IPv6，與網際網路連線端僅使用 IPv4。此時，一旦使用者主機提出 DNS 查詢要求，惡意路由器會在收到 DNS 伺服器回覆後，將其以自己的 Prefix 加上目標網站的 IPv4 位址，成爲相對應的 IPv6 提供給使用者主機。

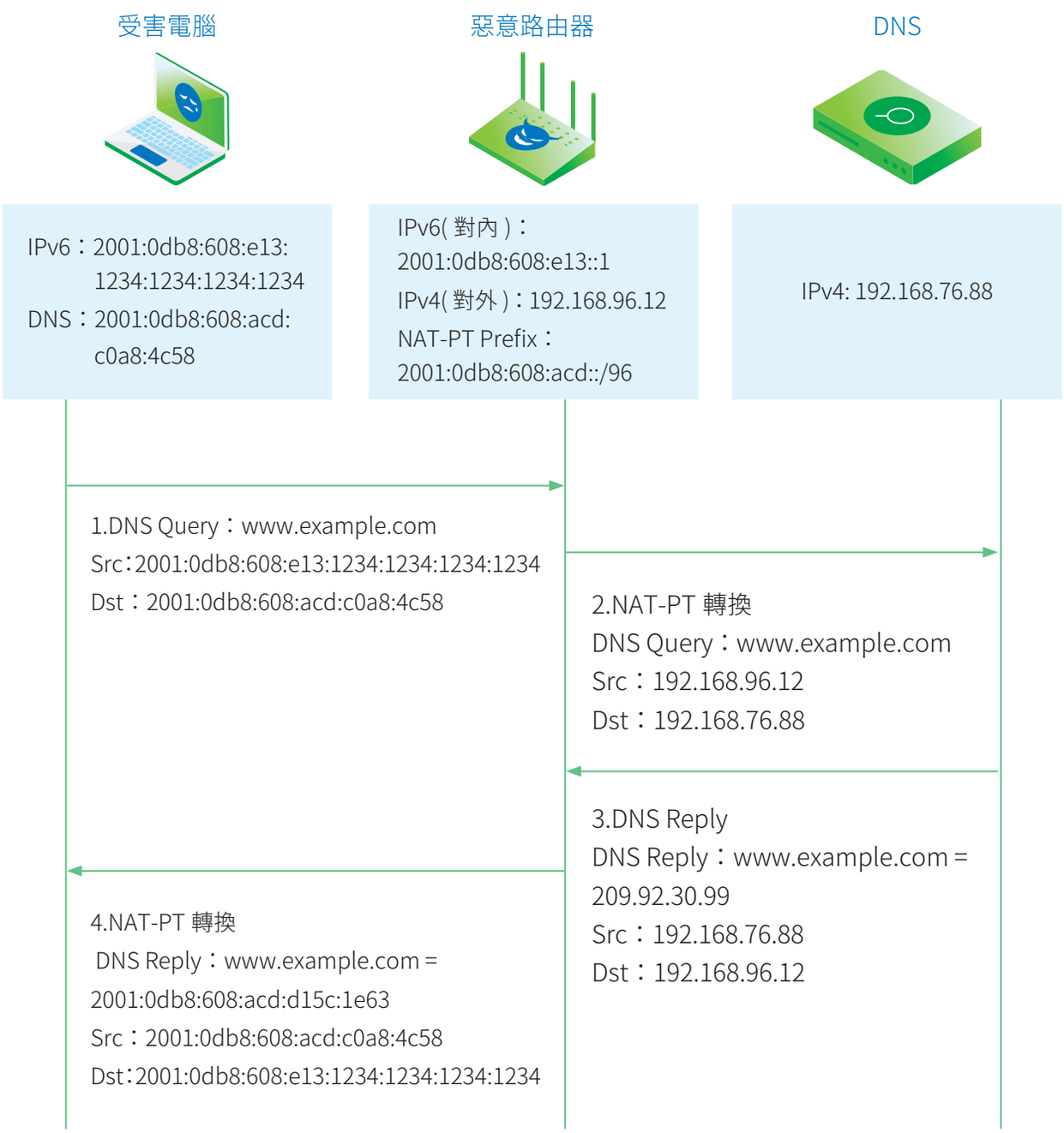


圖 2- 12：IPv6 中間人攻擊示意圖　　資料來源：TWCERT/CC 整理

如此一來，收到 IPv6 的主機僅目標網站的 IPv6 位址，使得每次主機要與目標網站連接時，會發現該 IPv6 位址前綴爲惡意伺服器的 NAT-PT 所有，使得主機必須將封包傳輸給惡意伺服器進行 NAT-PT 轉換爲 IPv4 位址，才能順利與目標網站進行連線，但也代表惡意伺服器能取得所有連線資訊[10] 。

2.IPv6 資安防護措施

(1).IPv6 資安威脅防護

由於 IPv4 即將用罄，發展並使用 IPv6 已經是未來必然的趨勢，但目前 IPv6 尚未成熟，且未能全面部署，尚不足以發現潛在的資安問題與漏洞。因此必須先針對目前已知的資安問題進行處理，如表 2- 8，以提升 IPv6 安全性：

防護項目	IPv4 防護	IPv6 防護
洪水攻擊 (Flood Attack) [11]	防火牆設置進行相關防禦。	• 防火牆進行封包的篩選及阻擋。 • 鄰居發現協議 (Neighbor Discovery, NDP) 偵測機制，將相鄰節點的 IPv6 位址、Port、Mac 位址等資訊綁定，以驗證眞僞。
分散式阻斷服務攻擊 (DDoS) [12]	防火牆或相關之防護軟體進行封包的辨識及阻擋。	• 針對攻擊門檻、阻擋時間以及保護目標進行設置，以減少 ICMPv6 訊息所造成之 DDoS 攻擊。
未經驗證或僞冒的裝置 (Rogue Devices) [13]	防火牆針對 IP 進行控管，並且透過白名單設定防止惡意裝置與之連接。	• 關閉 RA 功能，並手動設定相關之 IP 及 DNS。 • 在交換機執行 RA Guide 功能，過濾 RA 訊息。
中間人攻擊 (MITM)	• 透過 NDP 資訊驗證來源正確性。 • 透過 RA Guide 機制設定允許之 RA 資訊條件。 • 透過 IPsec 機制，針對傳輸的封包進行 Layer 3(網路層) 的資料傳輸加密。	

表 2- 8：IPv4 與 IPv6 安全性防護彙整表　　資料來源：[11], [12], [13]

10 ISC. “IPv6 MITM via fake router advertisements”. Retrieved January 10, 2020, from the World Wide Web: https://isc.sans.edu/forums/diary/IPv6+MITM+via+fake+router+advertisements/10660/

11 TP-Link. “Configuring IPv6 IMPB”. Retrieved January 10, 2020, from the World Wide Web: https://www.tp-link.com/us/configuration-guides/configuring_ipv6_impb/?configurationId=18225#_idTextAnchor001

12 SonicWall. “ICMP Tab”. Retrieved January 14, 2020, from the World Wide Web: http://help.sonicwall.com/help/sw/eng/6960/26/2/1/content/Firewall_Settings_Flood_Protection.066.5.html

13 NetworkLessons. “IPv6 RA Guard”. Retrieved January 14, 2020, from the World Wide Web: https://networklessons.com/cisco/ccie-routing-switching-written/ipv6-ra-guard

(2).IPv6 資安規範及標章推動

國家通訊傳播委員會 (National Communications Commission, NCC) 爲國內有意升級使用 IPv6 的組織和企業，提供相關業者升級時可依循之輔導手冊，並針對 IPv6 部分提出運行時所需檢測的裝置及需驗證項目，以確保最佳的 IPv6 資安品質[14] 。

而國際間亦有針對 IPv6 的部署及其安全性提出相關驗證計畫，迄今在國際上較知名且常被作爲標準之認證標章爲 IPv6 Ready Logo。根據統計，於 2003 至 2011 年開放檢測之第一階段銀質標章全球總計通過 480 個 IPv6 相關設備，國內則共有 75 個 IPv6 設備通過檢測，排名全球第三。而於 2005 年啓用迄今的第二階段金質標章，截至目前，全球共有 2,198 個 IPv6 相關設備通過檢測，國內則有 328 個 IPv6 設備通過檢測[15]。

爲提升 IPv6 的安全性，台灣網路資訊中心 (Taiwan Network Information Center, TWNIC) 執行 IPv6 計畫，分別爲「我國 IPv6 建置發展計畫」以及「新一代網際網路協定互通與認證計畫」，提供開發 IPv6 相關技術以及企業和組織實際導入時參考。而該計畫也在國內使用 IPv6 比例發展情形顯現出其功效，不論成長率或使用率都成爲國際間之佼佼者。也期盼在逐漸成熟的建置和發展之下，能夠達到最佳的檢測和防護能量，形成更加安全及穩定的網際網路。

二、網路域名濫用之影響、威脅與防護

1. 域名濫用與 COVID-19

網域名稱 (Domain Name，簡稱域名)，用以識別在網際網路中的伺服器名稱。針對網域名稱，對其註冊的使用者並無特殊規範，只要該域名並未被其他使用者註冊，並且未使用特殊保留字以及相關規範，基本上均可註冊後取得一定時間內的使用權[1] 。

然而，由於在進行域名註冊時，無法辨識域名的使用方式，也難以篩選註冊者，導致許多攻擊者透過註冊對其有利的域名後進行惡意行爲。此種將域名作爲惡意行爲用途之模式，被稱爲「域名濫用 (Domain Name Abuse)」。針對域名濫用，可分爲以下四種模式[2] ：

- **網路釣魚 (Phishing)：**將域名作爲網路釣魚之用，其域名註冊往往是與知名品牌相似的網域名稱，尤其是與金流相關的銀行及電子商務域名，在連入僞冒網站後，極有可能被竊取個資、機敏資訊，甚至造成財物損失。
- **惡意程式 (Malware)：**將域名作爲託管或傳播惡意程式之用，其域名往往是透過足夠吸引使用者的域名，在連入該網站後，遭受惡意程式攻擊。

14 國家通訊傳播委員會 . “推動 IPv4/IPv6 雙軌普行方案”：
https://www.ncc.gov.tw/chinese/files/19123/5138_42448_191231_8.pdf (瀏覽日期：2020 年 1 月 15 日)

15 IPv6Ready. “IPv6 Ready Logo Program”. Retrieved January 30, 2021, from the World Wide Web: https://www.ipv6ready.org/index.html

1 TWNIC. “域名公告”： http://www.twnic.org.tw/dnservice_announce_announce.php （瀏覽日期：2020 年 6 月 3 日）

2 ICANN. “Frequently Asked Questions: ICANN’s Domain Abuse Activity Reporting (DAAR) Project”. Retrieved June 3, 2020, from the World Wide Web: https://www.icann.org/octo-ssr/daar-faqs

- **殭屍網路與中繼站 (Botnet Command-and-Control, Botnet C&C)**：將域名用作中繼站位址，並且用以控制及識別受惡意程式感染的殭屍電腦，進行 DDoS 等攻擊。
- **垃圾郵件 (Spam)**：將域名作爲發送垃圾郵件之郵件系統所用，此種域名往往會使用足夠吸引使用者的字串，並且大量發送未經使用者同意的電子郵件。

隨著網際網路的發達，域名濫用的問題層出不窮，尤其近期隨著 COVID-19 疫情的發展，許多攻擊者以此傳遞不實資訊、進行詐騙及網路釣魚行爲，並註冊與之相關的網域名稱，誘騙大衆。因此，即便仍有許多新註冊的域名是用於正當的合法用途，但越來越多的域名濫用事件發生，逐漸成爲疫情時期的一大資安問題。

(1). 國際 COVID-19 域名註冊

在 2020 年 COVID-19 疫情開始大量爆發以來，大衆的關注急速上升。然而，許多攻擊者卻藉由這些恐慌與關注，透過相關網域，發送相關的垃圾郵件，或建立相關的釣魚網站及散播惡意程式。根據統計報告，從 2020 年 1 月至 2 月底期間，全球總共已註冊逾 4,000 多個與 COVID-19 相關的新網域名稱，並且在這些網域中，有約 3% 是被確認爲遭濫用的惡意域名，另有 5% 的網域爲可疑域名，與 COVID-19 相關網域爲遭濫用的惡意網域之可能性高於其他網域 50%。然而，截至 3 月中，整體新註冊與 COVID-19 相關網域，已經超過 16,000 筆的新網域，在近三週期間，其註冊數量較前幾週增長了近 10 倍，並且有約 0.8% 確認爲受濫用的惡意域名，以及有約 19% 的可疑域名[3&4]。

由於與 COVID-19 相關域名數量快速增加，世界智慧財產權組織 (World Intellectual Property Organization, WIPO) 所執行的統一域名爭議解決政策 (Uniform Domain Name Dispute Resolution Policy, UDRP)，也接獲大量相關域名註冊爭議案件[5]。例如 2020 年 3 月 13 日註冊之 coronagileadsciences.com 域名，在 3 月 31 日時被國際製藥公司 Gilead 提出爭議訴訟，認爲註冊者透過 Gilead 提升名氣，也影響其商譽，認爲是惡意註冊，最終判決爲將該域名轉讓給投訴人[6]。另一起爭議案件爲於 2020 年 4 月 1 日時申請註冊之 facebookcovid19.com 域名，在 4 月 10 日，Facebook 投訴註冊爭議，認爲 Facebook 商標明顯，且被投訴者並無合法使用商標之權益。甚至當投訴者聯繫註冊方要求終止域名時，對方竟回覆該域名正在販售，價格爲 2,000 美金，因此被認爲此爲惡意註冊行爲。最終，網域被判將此有爭議之域名移交給投訴者 Facebook 處理，並且該域名將所有權轉至 Facebook 手中[7]。

3 Check Point. “COVID-19 Impact: As Retailers Close their Doors, Hackers Open for Business”. Retrieved June 5, 2020, from the World Wide Web: https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/

4 Check Point. “Update: Coronavirus-themed domains 50% more likely to be malicious than other domains”. Retrieved June 5, 2020, from the World Wide Web: https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

5 WIPO. “WIPO Cybersquatting Case Filing Surges During COVID-19 Crisis”. Retrieved June 8, 2020, from the World Wide Web: https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html

6 WIPO. “WIPO Arbitration and Mediation Center Case No. D2020-0776”. Retrieved June 9, 2020, from the World Wide Web: https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2020-0776

7 WIPO. “WIPO Arbitration and Mediation Center Case No. D2020-0885”. Retrieved June 9, 2020, from the World Wide Web: https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2020-0885

(2). 國內 COVID-19 域名註冊

隨著 COVID-19 疫情的加劇，全球註冊與 COVID-19 相關之域名數量大增，而屬於台灣地區的 .tw 域名也不例外。根據台灣網路資訊中心統計，透過 COVID、CORONA 及 VIRUS 三組字串，對 .tw 新註冊域名進行分析，從 2020 年 1 至 2 月底期間，符合此條件的域名僅有約 5 組，但從 3 月開始，其相關域名註冊快速上升，到 4 月已有約 20 組，截至 2020 年 6 月 1 日，已經共有 30 組相關域名[8]。

針對所查詢的 COVID、CORONA 及 VIRUS 字樣，註冊者根據上述關鍵詞及其衍伸進行域名註冊，因此，分析與之相關的域名字詞，使用最多的爲 coronavirus 字樣，約有 26.67% 之域名使用，使用 virus 字樣的域名數量次之，約 23.33% 之域名使用，接著依序爲 COVID19、COVID-19 及 COVID 字樣，詳細資訊如圖 2- 13[8]：

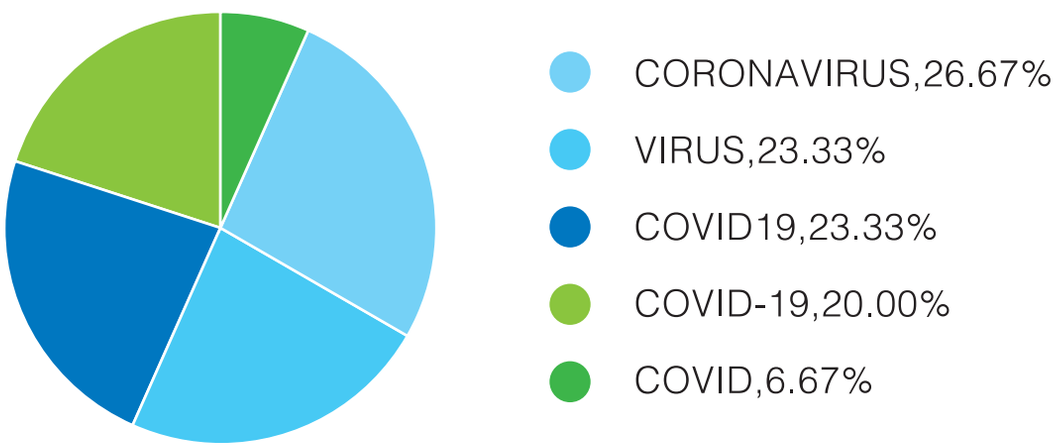


圖 2- 13：COVID-19 相關網域註冊字樣　　資料來源：[8], TWNIC

此外，在所有與 COVID-19 相關的域名中，經過 TWNIC 對網域的實際使用情形回應資訊量測，其中有 30% 的網域爲正常使用之網站，有 23.33% 是爲了保護品牌商標或防止他人濫用的域名，回應顯示域名保護訊息。但有 16.67% 顯示 DNS 設定錯誤，無法與之連線，更有 6.67% 的域名顯示出售訊息。詳細資訊如圖 2- 14[8]：

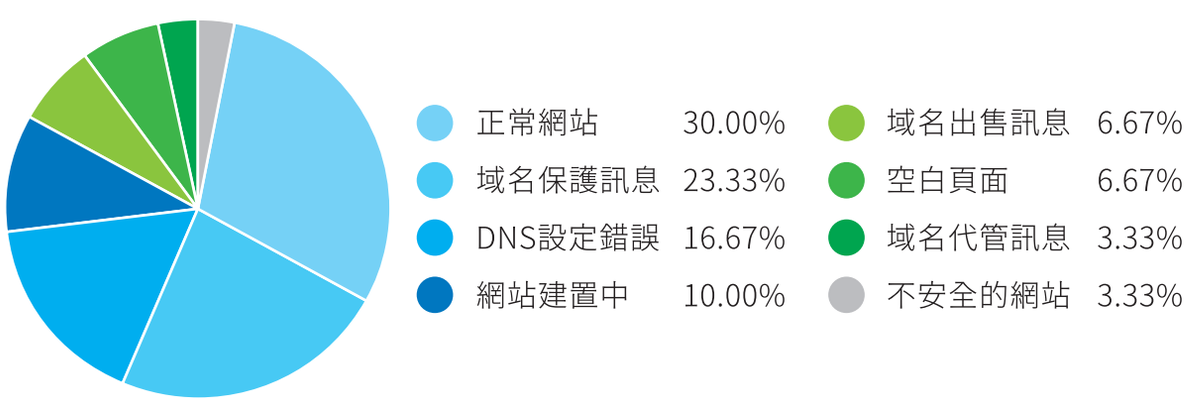


圖 2- 14：COVID-19 相關網域回應資訊量測結果　　資料來源：[8], TWNIC

8 TWNIC. “新冠病毒 COVID-19 對網域名稱之影響”： https://blog.twnic.net.tw/2020/05/22/7227/ （瀏覽日期：2020 年 6 月 8 日）

(3).COVID-19 相關域名濫用案例

針對全球域名的濫用情形，根據國內資安公司趨勢科技的統計，與 COVID-19 相關之域名數量在 2020 年 1 至 3 月間大幅上升[9] 。可明顯知道，域名濫用問題隨疫情大幅增加，其著名案例如表 2- 9：

惡意域名	國家	使用工具	惡意目的	攻擊手法
uk-covid-19-relieve[.]com [10]	英國	• 釣魚簡訊 • 釣魚網站	• 騙取個資與金融資訊	• 誘騙 • 假冒英國政府告知發放 258 歐元疫情救濟金，並要求進入惡意網站取得資金。 • 網站中顯示英國政府「gov.uk」字樣，要求輸入郵遞區號與金融卡等資訊。
Corona-virus-Map[.]com.exe [11]	美國	• 釣魚網站 • 惡意應用程式	• 感染惡意程式 • 竊取主機資訊 • 下載其他惡意程式	• 誘騙 • 偽冒約翰霍普金斯大學疫情地圖，要求下載惡意執行檔。 • 啓動後會受惡意程式 AZORult 攻擊，該惡意程式會竊取受害主機的相關資訊，以及將其他惡意程式下載至受害主機。
coronavirus app[.]site [12]	美國	• 釣魚網站 • 惡意 APP	• 感染勒索病毒	• 誘騙 • 連入網站後鼓勵下載與疫情相關的惡意 APP。 • 下載安裝後，將會受到勒索病毒 CovidLock 的攻擊。

9 Trend Micro. “Developing Story: COVID-19 Used in Malicious Campaigns”. Retrieved June 11, 2020, from the World Wide Web: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

10 Computer Service Centre. “A new wave of phishing during COVID-19”. Retrieved June 15, 2020, from the World Wide Web: https://www.computerservicecentre.com/news/article/a-new-wave-of-phishing-during-covid-19

11 Reason Security. “COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report”. Retrieved June 16, 2020, from the World Wide Web: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

12 DomainTools. “CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware”. Retrieved June 16, 2020, from the World Wide Web: https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware

惡意域名	國家	使用工具	惡意目的	攻擊手法
@cdc.gov.tw [13]	台灣	• 垃圾郵件 • 惡意附件	• 感染惡意程式 • 竊取個資	• 威脅 • 自稱國內衛生福利部疾病管制局 (Centers for Disease Control, CDC) 署長，用 @cdc.gov.tw 網域寄送垃圾郵件，增加眞實性。 • 信件表示收件者所在地區出現 3 名確診病患，其中有患者爲其接觸者，要求收件者進行疫情測試，並開啓附件取得相關資訊，否則會遭到逮捕起訴。 • 信件中的惡意附件爲惡意程式 RoboSki，會竊取受害主機中的資訊，以及安裝後門程式，操控受害主機。

表 2- 9：COVID-19 域名濫用案例彙整表　　資料來源：[10], [11], [12], [13]

除上述案例外，仍有諸多潛在風險存在於網際網路中，例如包括使用混淆字元的網域，像是使用 c0vid 或 c0v1d 等字樣取代 covid，以及特意的拼寫錯誤，像是以 carona 或 corrona 字詞取代 corona 以混淆大衆，使用者需更加小心，避免成爲域名濫用的受害者[14]。

2. 域名濫用監測與防護

隨著疫情嚴峻，諸多攻擊者藉由與疫情相關的網域名稱及內容，博取信任，以取得不法利益。根據研究，與 COVID-19 相關之域名濫用問題的惡意網域比例，較過往季節性或節日主題的網域高 50%[4]。因此，針對 COVID-19 與域名濫用問題，使用者應提高警覺加強防護[15]：

- 不明來源的郵件，即便內容很吸引人，也不要隨意點擊連結或下載附件，必須確認該連結及附件的安全性後再行動。
- 諸多自稱是政府、國際組織或知名企業的訊息，務必確認寄送者的身份、郵件位址等資訊，避免誤信而遭受損失。

13 Telefonica. “Vendetta Group and the COVID-19 Phishing Emails”. Retrieved June 20, 2020, from the World Wide Web: https://business.blogthinkbig.com/vendetta-group-covid-19-phishing-emails/

14 DomainTools. “Free COVID-19 Threat List - Domain Risk Assessments for Coronavirus Threats”. Retrieved June 19, 2020, from the World Wide Web: https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats

15 Trustwave. “COVID-19 and Your Cybersecurity: We're Here to Help”. Retrieved June 20, 2020, from the World Wide Web: https://www.trustwave.com/en-us/covid-19/

- 許多應用程式及 APP 會藉由 COVID-19 名稱吸引大衆下載，因此使用者應從合法可信來源或知名應用程式商店中下載應用程式，減少受惡意應用程式攻擊的風險。
- 許多資安單位或企業都會針對諸多的網路域名進行監測，一旦該域名出現惡意行爲，將會納入黑名單，甚至會推出相關的防護軟體，避免使用者受害，減少對使用者帶來的威脅。
- 不論是個人或組織及企業使用者，都應提升安全意識，多加參與或舉辦許多相關資安教育訓練，只有提升使用者習慣及安全意識，才能確實有效阻絕資安威脅的發生。

三、分散式阻斷服務攻擊之威脅與防護

1. 分散式阻斷服務攻擊威脅概述

分散式阻斷服務 (DDoS) 攻擊，是阻斷服務 (DoS) 攻擊的進階版，透過發送大量的封包或請求，使受害主機因無法負荷而癱瘓，導致中斷服務。DDoS 攻擊之模式，主要分爲頻寬消耗及資源消耗兩種[1] ：

- **頻寬消耗型攻擊：**攻擊者透過傳送大量無效、甚至惡意放大流量的服務請求給受害主機或伺服器，使得網路頻寬壅塞，導致一般使用者無法順利登入或連線，產生主機或伺服器癱瘓之後果。
- **資源消耗型攻擊：**攻擊者透過大量的服務請求，但不讓服務請求完成，導致主機或伺服器資源都被用來處理攻擊者的大量無效請求，無資源可回應一般使用者。

兩種類型之 DDoS 攻擊，又可分爲多種手法。雖攻擊者利用之工具或協定不盡相同，但均會造成受害主機或伺服器無法負荷，嚴重影響其運行。頻寬消耗型手法衆多，大多爲透過特殊協定之放大攻擊，包括[2&3] ：

- **Memcached 放大攻擊：**Memcached 是一種分散式之高速資料庫緩衝系統，提供高效率存取及高擴展性，但本身缺乏認證及安全管理機制，容易被操控爲進行 DDoS 攻擊的利器。

1 Gaia.“DDoS 攻擊是什麼？ 弄懂常見 DDoS 攻擊手法與防禦措施”: https://www.gaia.net/tc/gaia-trend/ddos-ddos (瀏覽日期：2020 年 11 月 20 日)

2 CloudFlare. “什麼是 DDoS 攻擊？”：https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-attack/ (瀏覽日期：2020 年 11 月 20 日)

3 US-CERT. “UDP-Based Amplification Attacks”. Retrieved November 26, 2020, from the World Wide Web: https://us-cert.cisa.gov/ncas/alerts/TA14-017A

攻擊者會將大量數據植入暴露於網際網路中的 Memcached 伺服器中，並偽裝成受害主機之身分提出請求，而被植入大量資料的 Memcached 伺服器便會將這些資料傳送給受害主機。大量的資料傳輸導致受害主機無法順利收到一般使用者的正常請求並回應。

圖 2- 15：Memcached 攻擊示意圖　　資料來源：TWCERT/CC 整理

此攻擊放大係數爲 10,000 至 51,000，爲所有 DDoS 放大攻擊中倍率最高者。

- **NTP 放大攻擊：**網路時間協定 (Network Time Protocol, NTP) 是一種允許主機之間透過封包交換進行系統時間同步之網路協定。在 NTP 協定中，有一個 monlist 指令，讓 NTP 伺服器回傳多筆近期與之通訊的列表，該列表最高限制爲 600 筆。

  攻擊者利用此機制，以偽冒之 IP 位址寄送 monlist 請求給 NTP 伺服器，則 NTP 伺服器便會將至多 600 筆之數據傳送給遭偽冒的 IP，導致遭偽冒之受害主機因一次大量的數據傳輸，造成其網路頻寬難以負荷，而無法順利提供服務。

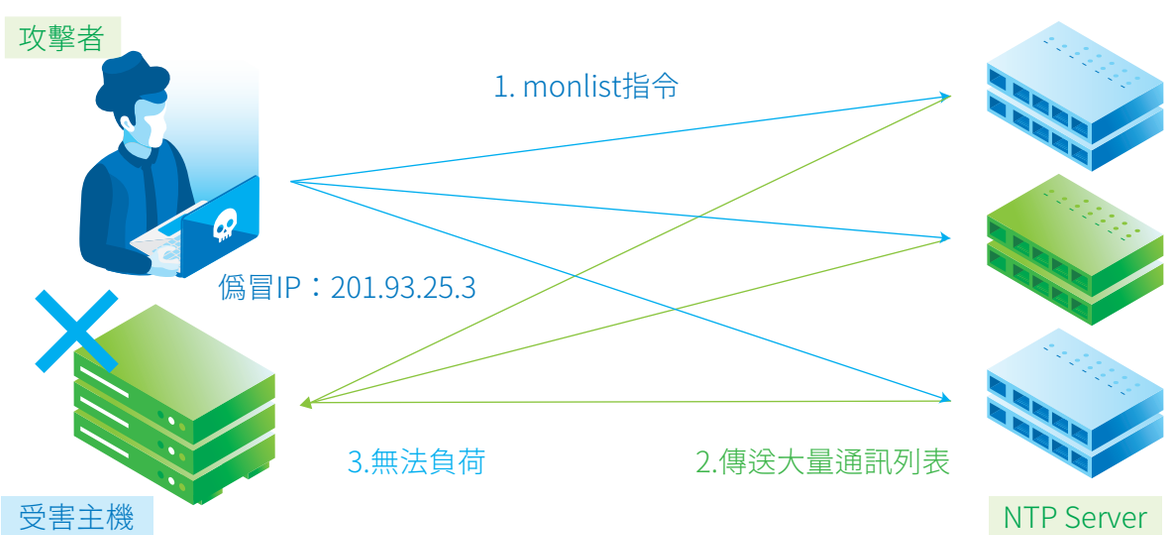


圖 2- 16：NTP 放大攻擊示意圖　　資料來源：TWCERT/CC 整理

此攻擊放大係數爲 556.9，爲所有 DDoS 放大攻擊中倍率次高者。

- **DNS 放大攻擊：**在某些特殊的請求中，例如 Any 請求，讓 DNS 伺服器回傳關於目標網域的所有訊息，導致 DNS 伺服器回傳的封包大小放大，回應比請求封包更大的封包給請求發起方。

  攻擊者利用此機制，僞冒受害主機，向 DNS 伺服器發起放大封包的請求，並且讓 DNS 伺服器回傳大量的放大封包給受害主機，導致受害主機頻寬壅塞，一般使用者無法順利連線。

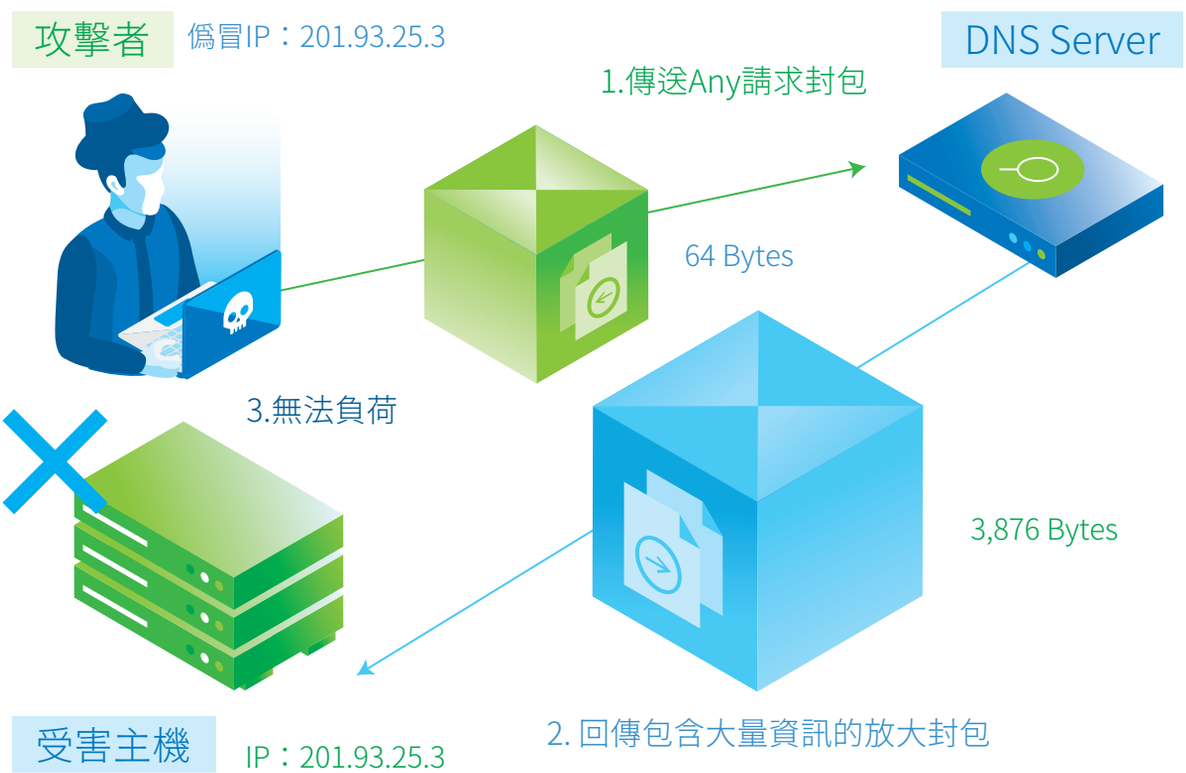


圖 2- 17：DNS 放大攻擊示意圖　　資料來源：TWCERT/CC 整理

此種攻擊手法相當常見，其放大倍率爲 28 至 54。

除上述頻寬消耗型攻擊外，亦有針對伺服器資源之資源消耗型攻擊，其攻擊模式包括[2]：

- **SYN Flood 攻擊：**TCP 連線時，伺服器端在收到 SYN 封包後，會回應並保留一通信埠提供請求端連線之用，在收到請求端 ACK 訊息後開始後續連線作業。

  攻擊者利用此機制，傳送僞冒來源 IP 位址之 SYN 請求封包給受害伺服器，受害伺服器會回應給遭僞冒主機並保留連接埠，然而，在伺服器等待回應的期間，攻擊者仍會大量持續傳送 SYN 請求，且這些封包因僞冒來源 IP 讓伺服器無法收到回覆，使其連接埠因 SYN 請求而分配完畢，導致無其他連接埠可供一般使用者使用。

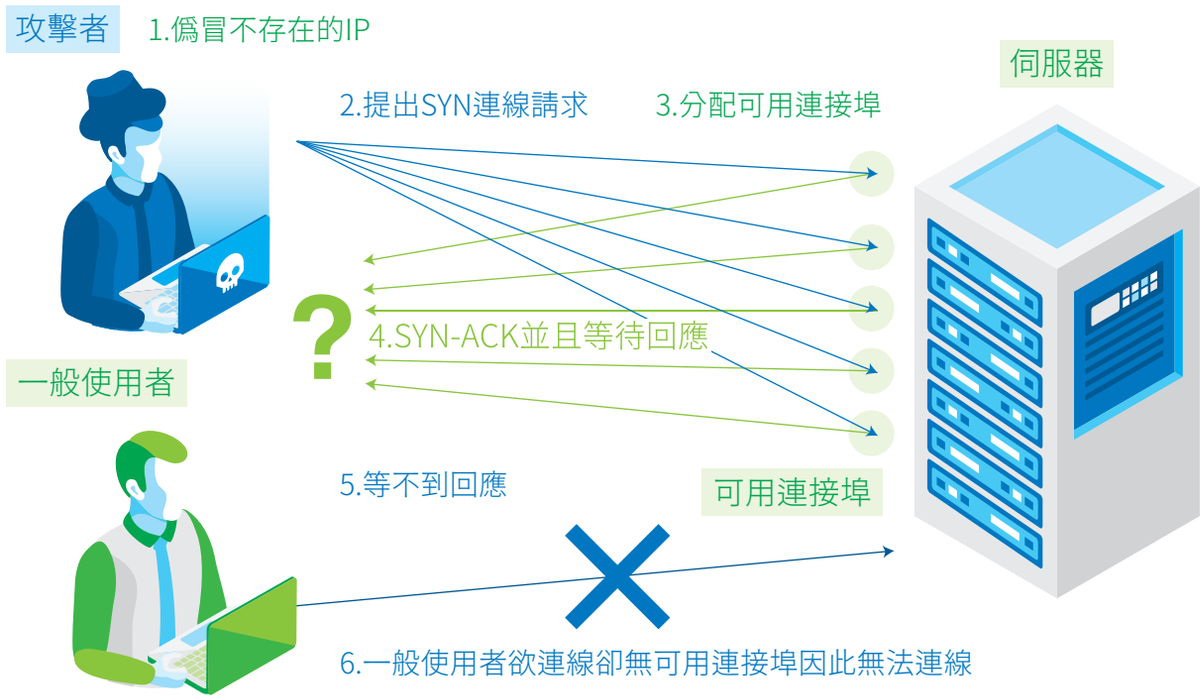


圖 2- 18：SYN Flood 攻擊示意圖　　資料來源：TWCERT/CC 整理

- **應用層 DDoS 攻擊：**應用層爲提供使用者完整的服務，伺服器回應請求所進行的動作、會較其他層來得更多，因此會消耗更多資源，例如使用者一個簡單的網頁存取請求，伺服器就必須先進行資料庫的查詢、應用程式介面 (Application Programming Interface, API) 的調動，才能生成網頁，甚至可能還需驗證請求端的憑證，其所需耗費的資源較請求端多出許多。

  攻擊者透過此機制，以殭屍網路大量傳送應用層之請求封包給受害伺服器，導致受害伺服器不堪負荷而中斷服務。

- **低速緩慢攻擊 (Low and Slow Attack)：**此種攻擊主要是透過相當冗長的請求過程，佔據受害伺服器之服務資源，拉長服務時間，卻又保持其速率不讓連線超時，使得受害伺服器無法對一般使用者提供服務。低速緩慢攻擊所需之頻寬較小，且難以與一般流量區分，相較於大規模流量之 DDoS 攻擊，此種攻擊不容易被發現，卻仍會導致受害伺服器服務被拖慢，甚至導致服務中斷之問題。

著個人電腦、行動裝置，甚至物聯網裝置的數量大量增長，攻擊者在植入惡意程式後可操縱的設備數量大量增加，雖然越來越多的伺服器或主機所能負荷的流量也越來越大，但仍不及攻擊者所惡意傳送的大量封包，因此 DDoS 攻擊之資安事件仍常有所聞。國內外相關案例彙整如下：

(1). 國內企業 / 組織遭受 DDoS 攻擊案例 :

A. 國內政府機關遭 Op Taiwan 活動之 Anonymous Asia DDoS 攻擊[4&5] ：

2015 年 7 月，當時學生課綱之相關爭議不斷，而駭客組織 Anonymous Asia 在 Facebook 專頁表態支持反課綱學生，並透過 DDoS 方式陸續攻擊我國諸多政府機關以及相關民間組織。此次攻擊活動被命名爲 Op Taiwan，且同時也號召菲律賓、加拿大、香港、中國大陸及美國等各地匿名者團體，於 2015 年 8 月 1 日對我國政府機關及相關組織共同發動 DDoS 攻擊。在遭受攻擊的一週期間，各機關採取阻擋攻擊來源、新增阻擋設備以及限制頻寬等方式緩解攻擊產生之影響，並且藉由網際網路接取服務業者獲得通報單位處理國內攻擊來源，以及透過 TWCERT/CC 針對他國攻擊來源進行通報及處理。此次事件，Anonymous Asia 宣稱其已經成功攻擊 14 個政府機關以及數間民間組織，所幸此次攻擊並未造成嚴重損失及後果。

B. 國內多家券商遭 DDoS 攻擊勒索虛擬貨幣[6]：

在 2017 年 2 月，國內逾十間證券公司收到署名爲 Armada Collective 寄送之勒索信件，要求該證券公司支付七至十個比特幣，當時市價換算爲約新臺幣 27 至 30 萬元，否則便會進行 DDoS 攻擊癱瘓證券公司之網站。實際上，在一月底股市休市沒多久便出現零星災情，在開春交易首日更出現達 800Mbps 之攻擊流量，而攻擊者揚言此僅爲試探性攻擊，若證券公司不支付款項，便會在 4 日後之 2 月 7 日發動 TB 等級之攻擊。金管會立即出面協調 NCC、國內三家網際網路接取服務業者以及行政院資安處，嚴密監控相關網際網路流量，以減少相關損害。在預告日前一天，證券公司出現第二波災情，一直持續至預告當日，另有三家證券公司成爲 DDoS 新的攻擊受害者，但當日並未出現攻擊者預告之 TB 級攻擊，最大僅出現 GB 等級攻擊，並且大多數證券公司在受到攻擊後，於半小時內便都恢復正常運作，並未產生嚴重的損失。雖然此次攻擊未出現嚴重受害者，但也顯示著新興勒索攻擊的出現，讓 DDoS 攻擊成爲企業所需防護的主要目標之一。

4 財金資訊季刊 . “淺談匿名者網路攻擊事件與防範作爲”： https://www.fisc.com.tw/Upload/37d8e425-0bce-4e17-a7af-e3dca5fc39d7/TC/8508.pdf (瀏覽日期：2020 年 11 月 23 日)

5 行政院國家資通安全會報 技術服務中心 . “DDoS 攻擊簡介與案例分享”： https://lic.tumt.edu.tw/ezfiles/25/1025/img/16/232000252.pdf (瀏覽日期：2020 年 11 月 23 日)

6 iThome. “臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件”： https://www.ithome.com.tw/news/111875 (瀏覽日期：2020 年 11 月 23 日)

7 iThome. “臺灣多家主機託管商遭 DDoS 攻擊，元兇是國內 IP 疑大量 DVR 設備遭入侵”： https://www.ithome.com.tw/news/140158 (瀏覽日期：2020 年 11 月 23 日)

C. 國內多家主機代管商遭大規模 DDoS 攻擊使得網站服務受影響[7] ：

2020 年 9 月，國內多家主機代管商遭大規模 DDoS 攻擊，最早出現於 9 月 19 日傍晚，第一間受害廠商證實遭受攻擊，並且攻擊狀況於隔日開始逐漸增長，一天可能會遭遇三波攻擊、每次持續約 1 至 2 小時，導致諸多網站服務受到影響。但攻擊事件尚未結束，另有兩間廠商分別在 22 日及 23 日表示正遭受嚴重 DDoS 攻擊。此次攻擊較爲特殊之處，是攻擊來源 IP 位址均來自於國內，因此許多針對國外 IP 位址進行 DDoS 防護之機制無法順利運行。此外，此次攻擊來源 IP 位址多爲視訊監控錄影主機 (Digital Video Recorder, DVR)，且大部分 DVR 設備爲使用弱密碼及開啓 Telnet 服務之設備，導致攻擊者入侵難度大幅降低，遂成爲殭屍網路方便利用之設備。

(2). 國內裝置 / 設備遭利用對外進行 DDoS 攻擊 :

A. 國內大量網路攝影機遭駭以對他國進行 DDoS 攻擊[8&9] ：

在 2016 年 10 月，美國網路效能管理公司 Dyn 遭到極爲大量之 DDoS 攻擊，此事件主要是由受 Mirai 惡意程式感染之殭屍網路進行攻擊，涉及數千萬個 IP 位址，其攻擊流量最高達到 1.2 Tbps，成爲 DDoS 攻擊歷史中數一數二大規模之攻擊事件。在攻擊期間，使用 Dyn 域名服務之諸多網站，如 Twitter、Amazon、Spotify、Netflix 以及華爾街日報等知名網站，都無法順利提供服務。在此事件中，殭屍網路主要由逾五十萬臺的網路攝影機所組成，然而，在其中卻有近三萬台之網路攝影機之 IP 位址來自國內，數量爲全球第四多之國家。其原因爲這些網路攝影機提供 Telnet 連網功能，加上預設帳號密碼並未強制要求使用者修改，導致攻擊者透過遠端操縱這些網路攝影機，進行此次極大流量之 DDoS 攻擊。

B. 國內大量裝置遭用以對他國金融機構進行 DDoS 攻擊[10&11] ：

在 2016 年 11 月，俄羅斯 5 間銀行遭到大量 DDoS 攻擊，這 5 間銀行分別於不同時間點遭受攻擊，平均攻擊時間爲 1 小時，最長的攻擊則持續了 12 個小時之久。根據統計，此次事件中，攻擊者是透過遭受特定惡意程式感染之殭屍網路進行攻擊，這些殭屍網路包含逾 2 萬 4 千台以上不同的設備，並且在這些大量的殭屍網路設備中，有一半以上的設備來自美國、台灣、印度及以色列，一部分爲使用弱密碼之物聯網裝置，導致國內諸多使用弱密碼的裝置，成爲攻擊者利用工具。

8 iThome. “【資安周報第 47 期】傀儡網路氾濫，臺灣成爲全球 DDoS 攻擊幫兇”： https://www.ithome.com.tw/news/109354 (瀏覽日期：2020 年 11 月 23 日)

9 iTWire. “DDoS attack on Dyn costly for company: claim”. Retrieved November 23, 2020, from the World Wide Web: https://www.itwire.com/security/76717-ddos-attack-on-dyn-costly-for-company-claim.html

10 Kaspersky. “DDoS attack on the Russian banks: what the traffic data showed”. Retrieved November 23, 2020, from the World Wide Web: https://securelist.com/ddos-attack-on-the-russian-banks-what-the-traffic-data-showed/76728/

11 BBC News. “Russian banks hit by cyber-attack”. Retrieved November 23, 2020, from the World Wide Web: https://www.bbc.com/news/technology-37941216

2. 分散式阻斷服務攻擊之防護

爲避免企業因遭受 DDoS 攻擊而對其服務產生嚴重影響，企業應設立相關防護機制及設備，從最初的異常流量偵測、流量分析，以及後續的攻擊處理及回應等，使企業在不阻擋正常流量的情況下阻絕惡意流量的攻擊，方能維持企業系統順利運行。而針對 DDoS 攻擊之頻寬消耗和資源消耗兩種類型，其所需之系統、設備及機制卻不盡相同，因此，彙整兩種類型之 DDoS 攻擊所需防護相關工具如表 2- 10[12]：

	工具	防護機制	防護方式	防護目標
頻寬消耗 DDoS 攻擊	交換器 (Switch)	速率限制與存取控制 (Access Control List, ACL) 機制	控制欲流入伺服器之流量，進行相關限制	• Memcached DDoS 攻擊 • NTP DDoS 攻擊 • DNS 放大攻擊
		Bogon Filter 與 Deep Packet Inspection	過濾有問題封包	
	路由器 (Router)	速率限制與存取控制 (ACL) 機制	控制欲流入伺服器之流量，進行相關限制	• Memcached DDoS 攻擊 • NTP DDoS 攻擊 • DNS 放大攻擊
		入口過濾 (Ingress Filtering) 機制	對封包之來源 IP 位址進行檢測和過濾	
	網路流量清洗 (Flow Cleaning)	常駐型防禦	企業所有流量都導入其中分析後，透過其監測設備和防護系統，將合法流量及惡意流量區隔，再導回企業本身提供服務。	• Memcached DDoS 攻擊 • NTP DDoS 攻擊 • DNS 放大攻擊
		動態防禦	攻擊事件發生時立即將流量導入分析，透過監測設備和防護系統，將合法流量及惡意流量區隔，再導回企業本身提供服務。	

12 國家資通安全會報 技術服務中心 . “DDoS 攻擊手法與防護策略重點摘要”： http://download.icst.org.tw/attachfilearticles/DDoS 攻擊手法與防護策略重點摘要 .pdf (瀏覽日期：2020 年 11 月 24 日)

	工具	防護機制	防護方式	防護目標
資源消耗 DDoS 攻擊	防火牆 (Firewall)	阻擋特定網路協定、Port 及 IP 位址等資訊	辨識及過濾惡意封包	• SYN Flood 攻擊 • 應用層 DDoS 攻擊
		大數據或人工智慧	辨別網際網路流量是否異常，並針對異常流量進行阻擋和示警	
	交換器 (Switch)	速率限制以及存取控制 (ACL) 機制	控制欲流入伺服器之流量，進行相關限制	• 低速緩慢攻擊 • SYN Flood 攻擊 • 應用層 DDoS 攻擊
		Traffic Shaping 機制	避免封包延遲問題	
		Delay Binding 功能	防禦應用層惡意請求	
	路由器 (Router)	速率限制以及存取控制 (ACL) 機制	控制欲流入伺服器之流量，進行相關限制	• SYN Flood 攻擊
		入口過濾 (Ingress Filtering) 機制	對封包之來源 IP 位址進行檢測和過濾	
	入侵防禦系統 (Intrusion-Prevention Systems, IPS)	特殊特徵比對	針對特殊性質以及特定通訊協定方式之 DDoS 攻擊進行防禦	• SYN Flood 攻擊 • 應用層 DDoS 攻擊
	網路流量清洗 (Flow Cleaning)	由提供服務之廠商所建立之設備和機制所定	大多數提供流量清洗之廠商，都可針對常見 DDoS 攻擊進行防護	• SYN Flood 攻擊 • 應用層 DDoS 攻擊 • 低速緩慢攻擊

表 2- 10：兩種 DDoS 攻擊防護工具、機制與目標彙整表　　資料來源：[12]

對於 DDoS 攻擊，越來越受到企業和資安單位的重視，因爲一旦企業服務中斷，容易產生業務損失及聲譽受損等問題，因此爲避免 DDoS 攻擊所帶來的嚴重影響，是諸多企業所欲解決之目標。許多資安單位及網際網路接取服務業者也紛紛推出相關防護機制和設備，讓企業得以透過與之合作，大幅降低 DDoS 攻擊所帶來之威脅，從而提升整體網際網路之安全。

第三章、

情資分享與漏洞協處概況

資安威脅無所不在，爲防止資安事件發生及造成企業營運風險，TWCERT/CC 接受資安事件通報、協助處理及提供情資分享等服務，以降低企業受到資安事件的危害；同時深入了解資安威脅型態，防止擴散波及其他企業。此外，TWCERT/CC 協助國內廠商維護產品安全，接受我國產品相關資安漏洞通報，並協助溝通、修補和發布 CVE 編號，強化台灣資安漏洞處理防護系統，提升台灣產品安全性。

第一節、TWCERT/CC 資安情資分享

在 2020 年 1 月至 12 月期間，TWCERT/CC 總計分享逾 150 萬筆之資安情資予相關單位，包括來自國際，欲針對國內 IP 位址進行協處與警示的通報，以及來自國內，欲針對國內其他單位或國際 IP 位址進行協處與警示的通報。TWCERT/CC 分享之情資來源主要爲國際資安交流組織、國內資安相關組織，以及各國電腦緊急應變小組 (Computer Emergency Response Team, CERT) 組織等相互交流的訊息。

在收到資安通報後，TWCERT/CC 會依據通報中之對象進行情資分享。依國內外對象區分，國內分享對象主要包括政府單位、網路業者、金融單位、學術單位、台灣駭客協會 HITCON 等資安組織，以及諸多國內企業；國外分享對象爲逾百個國家的 CERT/CSIRT 單位及相關資安組織。此外，爲提升情資警示及分享效率，TWCERT/CC 通報系統與國家資安資訊分享與分析中心 (National Information Sharing and Analysis Center, N-ISAC)、美國自動化資安威脅情資共享計畫 (Automated Indicator Sharing, AIS)、反釣魚工作小組 (Anti-Phishing Working Group, APWG) 等國內外資安組織介接，定期並即時地進行情資互通交流，提升情資分享效能。

圖 3-1：TWCERT/CC 資安跨域聯防與情資分享　　資料來源：TWCERT/CC 整理

情資交流分享中，除了持續接收現有情資來源之外，更積極與國外組織進行情資交流合作。因此，在 TWCERT/CC 積極推廣下，本年度共增加了五個國際組織之合作，以提升情資分享廣泛度。而國內部分，主要是透過國家資安資訊分享與分析中心 N-ISAC 平台，與國內各大資安資訊分享與分析中心 (ISAC) 建立情報交流網絡，快速蒐整相關資安情資，以及積極主動檢索並分析網路上國內資安資訊，即時分享給國內相關受駭單位，並持續以電子郵件、電話方式進行後續追蹤，以掌握國內資安受害情況，強化我國整體網路安全。

在 TWCERT/CC 所接獲並進行分享的情資中，以接收國際情資後分享至國內相關單位之數量爲大宗。而接收國內情資，將國內發現或資安資訊分享至國外的情資數量中，以 RIR 管理區域區分，最多的爲屬於北美、南極洲、部分加勒比地區之國家，其次爲屬於歐洲、中東、中亞地區之國家，第三則爲屬於拉丁美洲、部分加勒比地區之國家，其詳細比例如圖 3- 2：

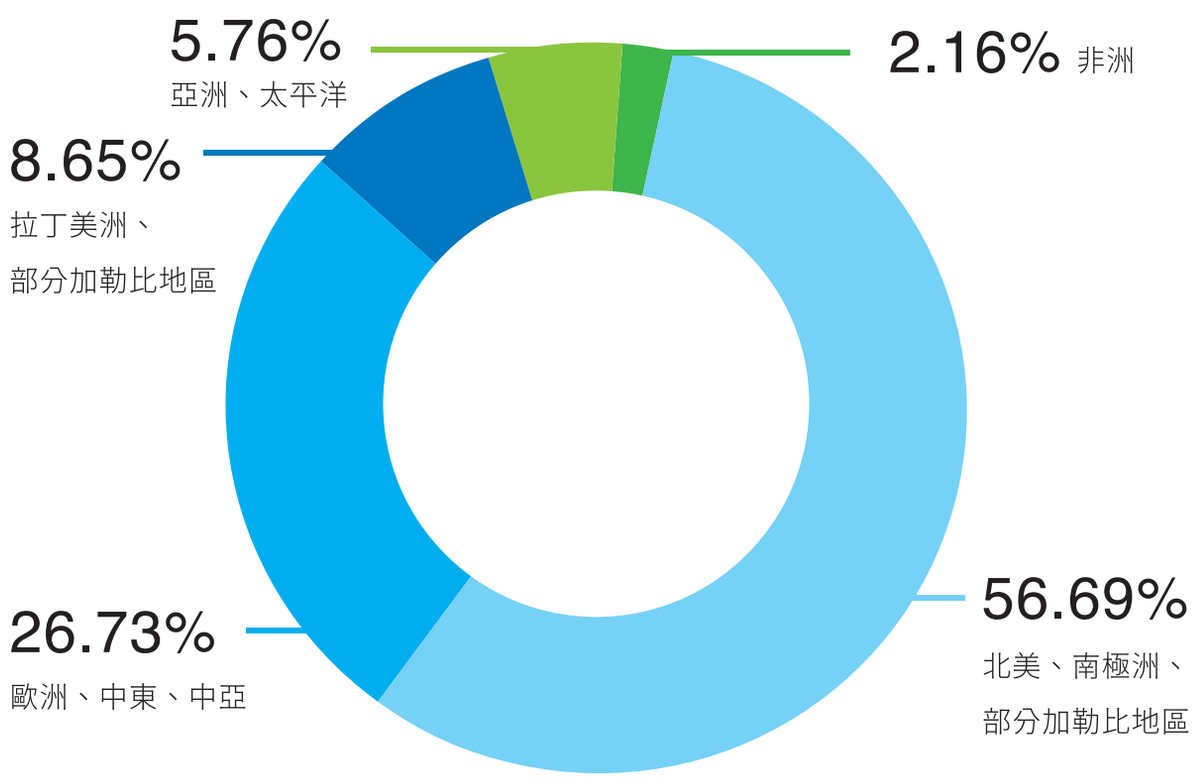


圖 3- 2：TWCERT/CC 國際資安事件情資分享比例　　資料來源：TWCERT/CC 整理

在衆多類型中，接獲並通報國內組織機構的資安事件類型比例最高者爲殭屍電腦 (Bot)，主要爲受害主機因感染惡意程式，遭到攻擊者利用，作爲殭屍電腦對外進行惡意行爲。比例次高者爲系統疑存在弱點，主要爲針對國內企業組織系統，被發現存有可作爲攻擊捷徑或工具之弱點，可能因此對組織本身產生資安威脅，因此予以通報以減緩其威脅。第三爲系統疑發起對外攻擊，主要爲系統可能被攻擊者入侵，或遭惡意程式感染後被攻擊者操縱，對外進行攻擊行爲，因此予以通報，除了減緩受攻擊單位之受害程度外，更避免受操縱系統內之機敏資訊外洩或破壞。本年度對境內分享之情資威脅類別詳細比例如圖 3- 3：

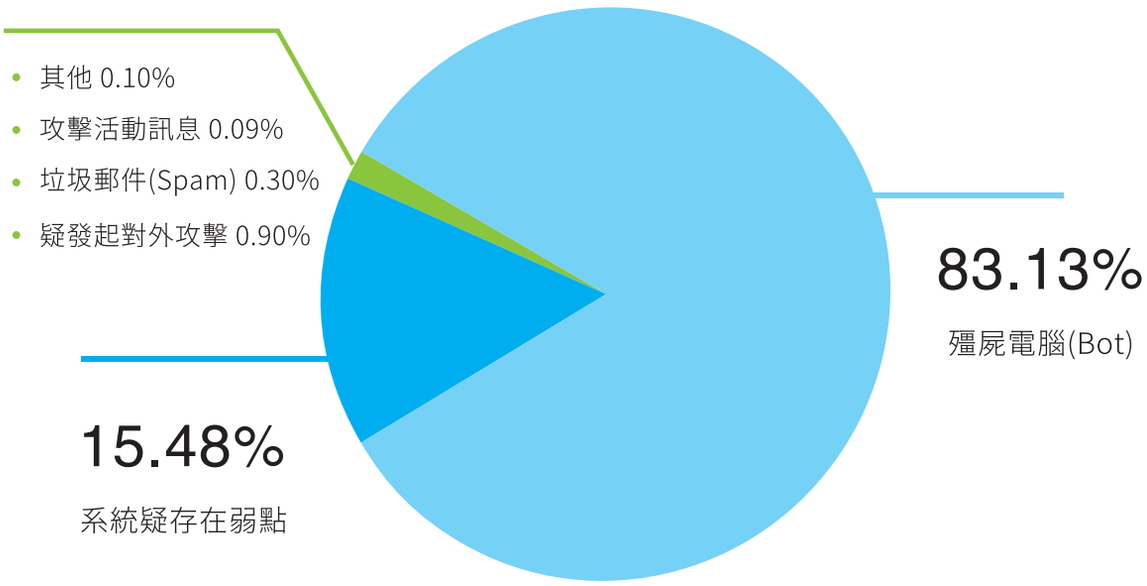


圖 3- 3：TWCERT/CC 境內情資分享威脅類別比例　　資料來源：TWCERT/CC 整理

除針對境內進行之分享作業，TWCERT/CC 亦接收國內通報後分享與國際單位。本年度中，接獲並通報國際組織機構的資安事件類型比例最高者爲系統疑存在弱點，主要爲國際間之企業組織系統，被發現可能存有能作爲攻擊者攻擊工具或捷徑之弱點，增加該企業組織系統受攻擊之風險。比例次高者爲系統疑發起對外攻擊，主要爲國際企業組織之系統或主機因受攻擊者操控，導致其被利用對外發起惡意攻擊行爲。第三爲垃圾郵件 (Spam)，主要爲電子郵件系統遭攻擊者操控，對外寄送未經允許之垃圾郵件。本年度對境外分享之情資威脅類別詳細比例如圖 3- 4：

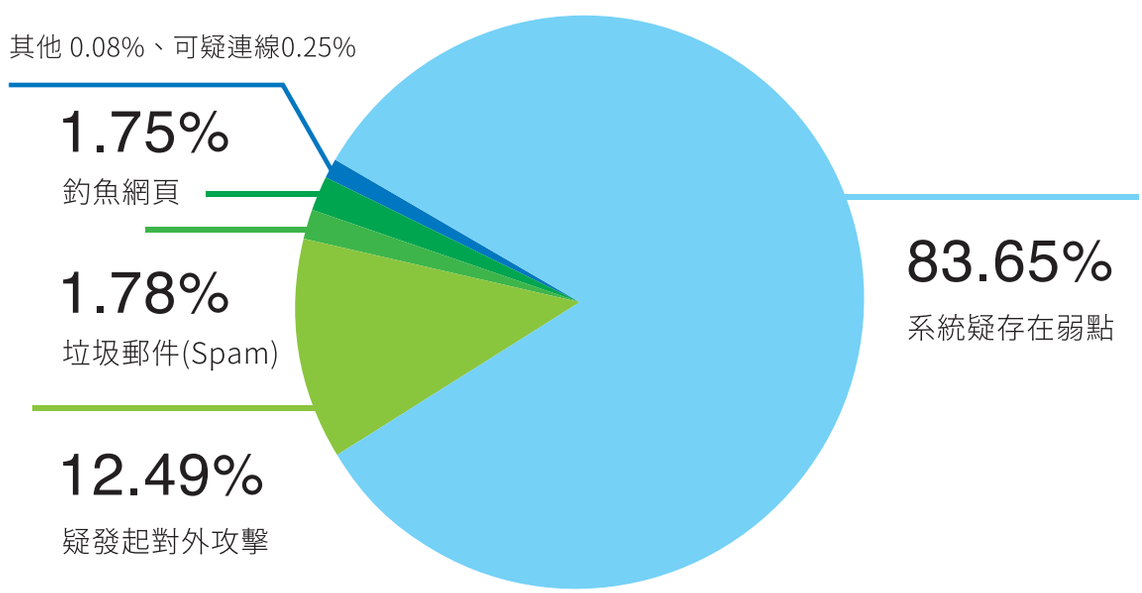


圖 3- 4：TWCERT/CC 境外情資分享威脅類別比例　　資料來源：TWCERT/CC 整理

第二節、Virus Check 惡意檔案分析

隨著近年來社交工程攻擊日益嚴峻，攻擊者爲達到傳播惡意程式之目的，往往會將其隱藏於檔案中，透過社交工程方式，誘騙使用者自釣魚郵件或釣魚網站等處，下載惡意檔案，以此作爲攻擊者入侵及進行惡意行爲之媒介。爲遏止社交工程攻擊造成之威脅擴大，TWCERT/CC 與相關單位合作，建立國內本土之惡意檔案檢測系統 — Virus Check，整合防毒軟體之靜態檢測模式與沙箱動態分析機制，透過以惡意程式病毒碼特徵快速找出惡意程式，搭配在隔絕沙箱環境中偵測未知檔案之惡意行爲，以全方位檢測檔案中是否潛藏惡意程式，進而達到降低社交工程惡意檔案攻擊之目的。

惡意檔案檢測服務系統 Virus Check 服務，於 2019 年 7 月中旬上線開放予大衆使用，該年度至 2019 年 12 月，共計達 2,651 之檔案檢測數量。而本年度爲提升系統之易用性及友善性等考量，以及進行與外部相關單位合作之未來規劃，進行介面之優化作業，優化後之系統平台已於今年 7 月正式提供服務。

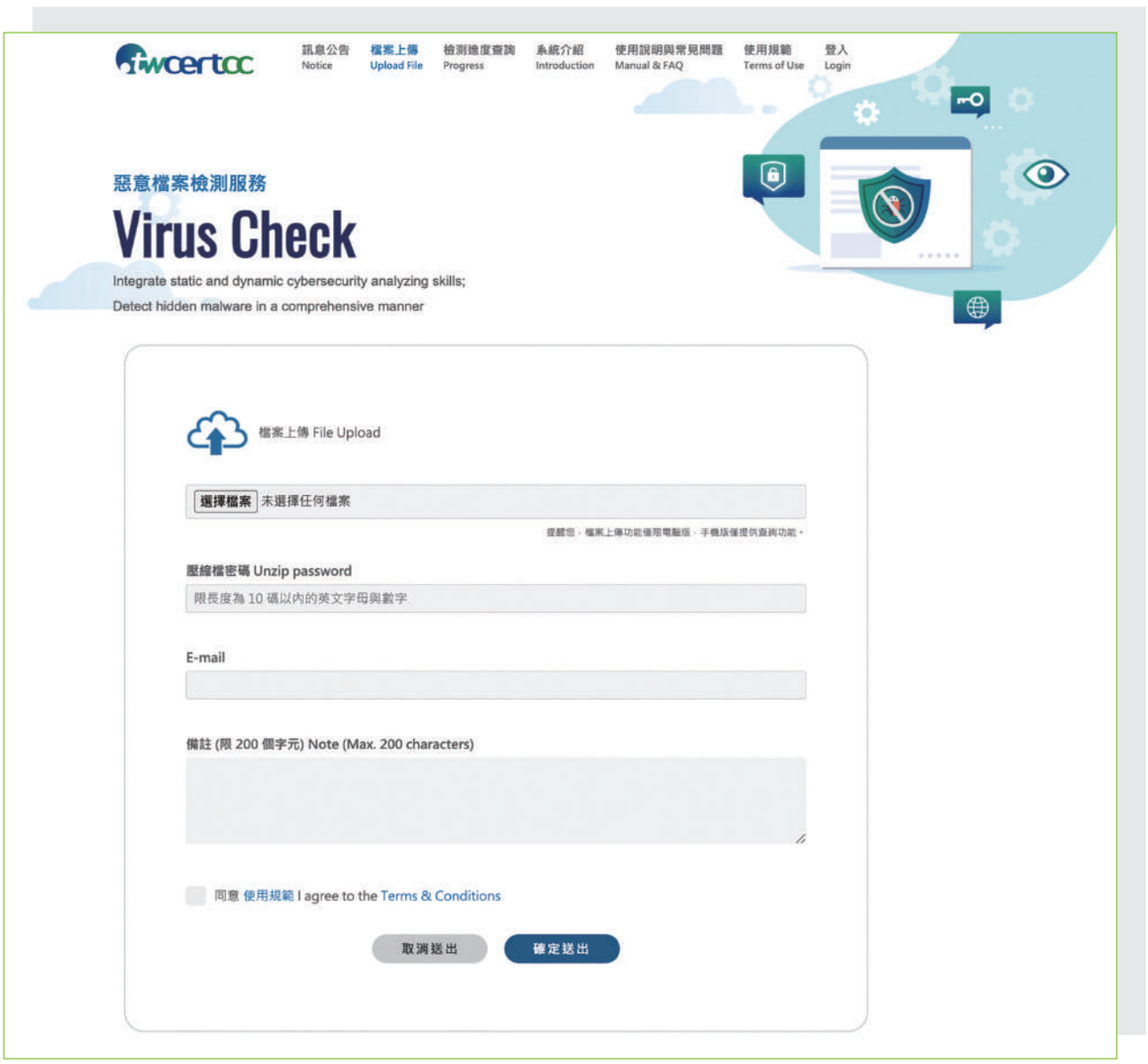


圖 3- 5：惡意檔案檢測服務 Virus Check

本年度之統計中，該系統總計檢測逾兩千個檔案，其中包含約 10.4% 之檢測檔案爲高風險檔案，約 9.2% 檢測爲中風險檔案，剩餘之 80.4% 檢測檔案爲低風險檔案，2020 年每月之檢測檔案數量與風險比例如圖 3- 6：

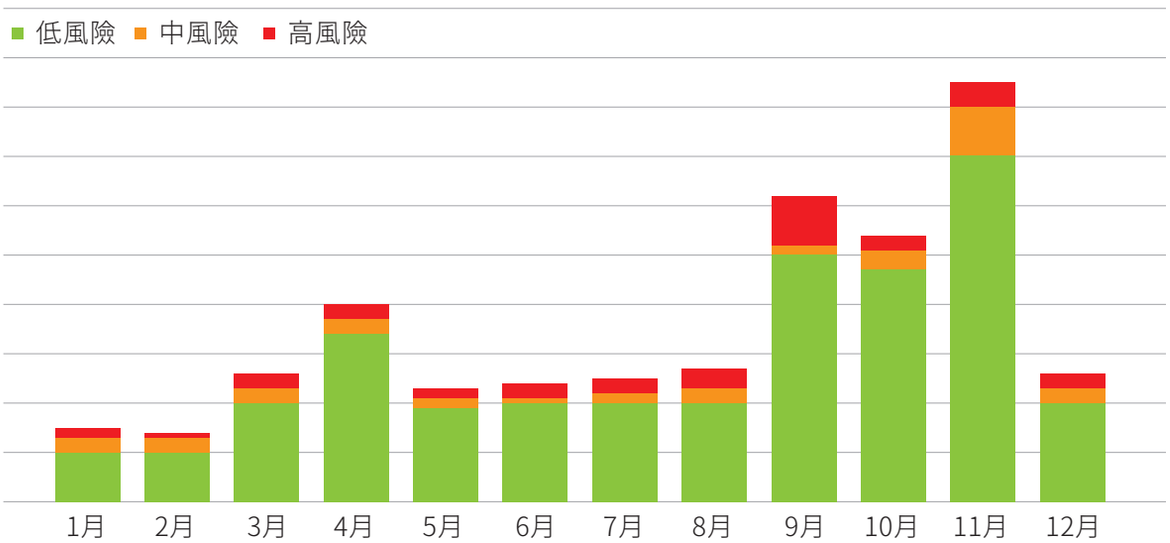


圖 3- 6：2020 年 1 至 12 月 Virus Check 檢測檔案數量與風險比例　資料來源：TWCERT/CC 整理

其中，若 Virus Check 系統檢測爲中風險與高風險之檔案，TWCERT/CC 會評估防毒軟體與合作檢測資安廠商之檢測結果，針對中高風險卻鮮少防毒軟體或資安廠商檢測到，則可能爲新樣式之惡意程式，將會提供給相關合作單位進行深度檢測，以確認該檔案中是否存有新樣式之惡意程式。在 2020 年期間，TWCERT/CC 共計傳送 49 個中高風險檔案給合作廠商，但並未發現新樣式之惡意程式。

而針對中高風險檔案之檔案類型，2020 年 1 至 12 月期間，逾 400 個檔案中，數量最多者爲可執行檔 exe 檔案，次多者爲動態連結函式庫 DLL 檔案，第三多者爲 Word doc 檔案。詳細比例如圖 3- 7：

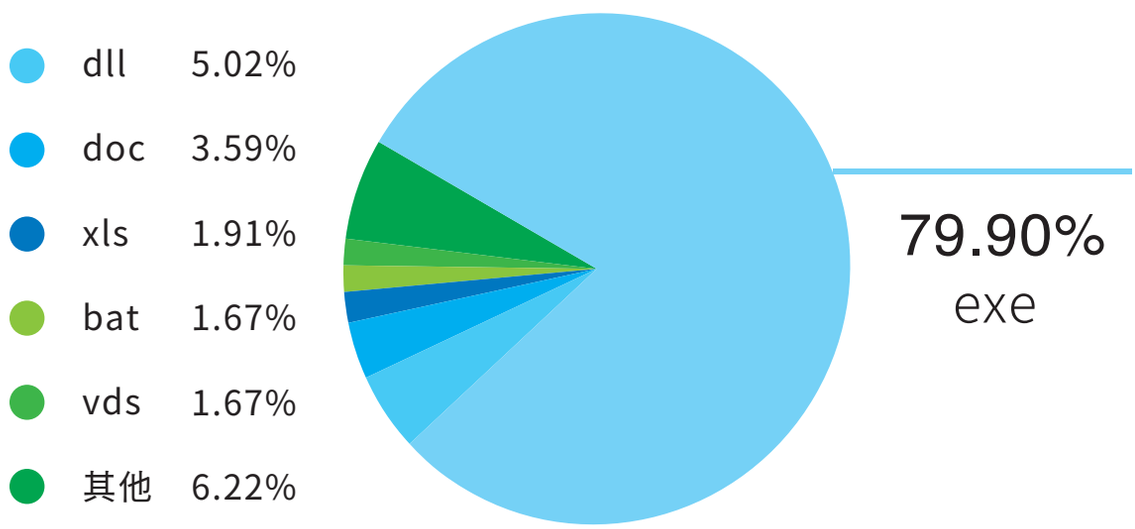


圖 3- 7：Virus Check 檢測檔案中高風險檔案類型比例　資料來源：TWCERT/CC 整理

除此之外，爲提升大衆對檔案檢測之資安意識以及降低惡意程式受害風險，TWCERT/CC 於本年度進行兩波惡意檔案檢測服務之推廣活動，鼓勵民衆多加利用 Virus Check 服務。第一波活動於 2020 年 9 月期間舉行，透過社群媒體及 google 關鍵字進行推廣宣傳，第二波則是於 2020 年 10 月舉行，依據第一波活動數據之分析，將關鍵字著重於「檔案檢測」、「Virus Check」以及「線上掃毒推薦」等字句進行進一步之曝光，也讓有相關需求之使用者能查找並順利使用該服務。除了 2020 年期間的兩波活動，未來亦會不定期舉辦相關推廣活動，讓越來越多的民衆能夠對惡意檔案有更高之敏銳度，以及培養其收到可疑檔案時，能採取檢測等多重驗證的行動，減少因社交工程惡意檔案而受駭之機率。

第三節、資安漏洞協處

一、全球發布之產品漏洞概況

美國網路安全非營利組織 MITRE，於 1999 年發布通用漏洞揭露計畫 (Common Vulnerabilities and Exposures, CVE)，主要目的爲識別、定義及分類那些遭公開揭露的資安漏洞，針對每個資安漏洞提供 CVE 編號，確保漏洞描述之一致性。截至 2020 年 12 月，已有國家 CERT 組織、產業 CERT 組織、研究機構及廠商等共 25 個國家、148 個組織成爲 CVE 編號管理者 (CVE Numbering Authority, CNA)，可進行產品漏洞審核及 CVE 編號發布，以利大衆查閱與引用。而 TWCERT/CC 在 2018 年成爲台灣區 CNA 成員，協助國內組織及企業審核及發放相關資安漏洞之 CVE 編號。

在 2020 年期間，全球總計發布了逾 1.8 萬筆 CVE 編號。依據 CVE 漏洞內容，由美國國土安全部 (Department of Homeland Security, DHS) 旗下之科學暨技術局 (Science and Technology Directorate, S&T) 管理以及由 MITRE 經營之通用缺陷列表 (Common Weakness Enumeration, CWE) 清單，會分析這些 CVE 漏洞內容及漏洞形成之原因，制定相關漏洞類型列表，除了建立一溝通便利之通用語言外，更可作爲漏洞識別、緩解及預防的基準。

除了 CWE 之外，美國國家標準暨技術研究院 (National Institite of Standers and Technology, NIST) 的國家弱點資料庫 (National Vulnerability Database, NVD) 亦會針對每個 CVE 漏洞進行嚴重性與影響程度的通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS) 檢測。CVSS 會對 CVE 漏洞之內容進行多面向的評鑑，除了綜合之 CVSS 風險評分外，尚包括漏洞攻擊向量 (Attack Vector, AV)、攻擊複雜度 (Attack Complexity, AC)、使用者操作 (User Interaction, UI)、所需權限 (Privileges Required, PR)、影響範圍 (Scope, S)、機密性影響 (Confidentiality Impact, C)、完整性影響 (Integrity Impact, I)，以及可用性影響 (Availability Impact, A) 等八個面向[1]，詳細資訊如表 3- 1：

1 FIRST. “Common Vulnerability Scoring System v3.1: User Guide”. Retrieved January 20, 2021, from the World Wide Web: https://www.first.org/cvss/v3.1/user-guide

面向	漏洞評分項目
攻擊向量 (AV)	• High(H)：可透過網際網路進行攻擊 • Adjacent(A)：可透過受限的網路進行攻擊，如區域網路或藍芽等 • Local(L)：僅透過本地端進行攻擊 • Physical(P)：僅透過實體訪問方式進行攻擊
攻擊複雜度 (AC)	• Low(L)：攻擊者可在隨時隨地進行攻擊 • High(H)：攻擊者須滿足其無法控制的條件，才能進行攻擊
使用者操作 (UI)	• None(N)：無需使用者執行特定行爲便能進行攻擊 • Required(R)：需使用者執行特定行爲才能進行攻擊
所需權限 (PR)	• None(N)：未經權限的攻擊者可進行攻擊 • Low(L)：需取得一般使用者權限，才能進行攻擊 • High(H)：需取得管理員權限，才能進行攻擊
影響範圍 (S)	• Changed(C)：該漏洞會影響除存有漏洞的元件外的其他元件 • Unchanged(U)：該漏洞僅會影響存有漏洞的元件本身
機密性影響 (C)	• High(H)：所有的資訊或一些機敏資訊都被洩漏給攻擊者 • Low(L)：攻擊者可以獲得部分資料，但無法控制資料的類型和機敏程度 • None(N)：無資料被洩漏
完整性影響 (I)	• High(H)：攻擊者可竄改所有資料或一些機敏資訊 • Low(L)：攻擊者可竄改部分資料，但無法控制資料的類型和機敏程度 • None(N)：無資料被竄改
可用性影響 (A)	• High(H)：受影響的資源完全無法使用，或關鍵服務 / 系統被降低效能，甚至中斷服務 • Low(L)：受影響的資源並非關鍵服務 / 系統，但仍產生降低效能或中斷服務的問題 • None(N)：無可用性影響

表 3- 1：CVSS 八面向與評分項目　　資料來源：[1]

爲了協助大衆了解安全漏洞的類型及趨勢，MITRE 的 CWE 團隊，透過各 CWE 類型於 NVD 中的數量頻率，以及各 CWE 類型之平均 CVSS 分數，以此計算出 CWE 整體危險等級。計算公式如下 ：

1. 計算 NVD 中包含的每種 CWE 類型數量，並且針對每種類型進行數量比例計算其頻率值。

$$Freq=\{count(CWE'_x \in NVD) \text{ for each } CWE'_x \text{ in } NVD\}$$

$$Fr(CWE_x)= \frac{count(CWE_x \in NVD)-min(Freq)}{max(Freq)-min(Freq)}$$

2. 透過每種 CWE 之平均 CVSS 分數，計算每種 CWE 類型之嚴重等級。

$$Sv(CWE_x)= \frac{(average\ CVSS\ for\ CWE_x)-min(CVSS)}{max(CVSS)-min(CVSS)}$$

3. 透過每種 CWE 之頻率值與嚴重等級，計算出各種 CWE 的危險程度。

$$Score(CWE_x) = Fr(CWE_x) \times Sv(CWE_x) \times 100$$

透過上述公式，可以計算出每一種 CWE 類型在當年度對資安所產生的危險程度。其危險程度並非單純倚賴出現次數或影響程度進行判斷，而是除了於當年所有 CVE 出現次數越多之外，該漏洞類型所帶來的影響程度也需越大，其危險程度數字才會越高，如此方能進行全面性的危險程度了解與分析。在計算出各 CWE 類型的漏洞危險程度分數後，MITRE 的 CWE 團隊會以此進行年度的漏洞危險程度排序，並以此作爲研究分析以及企業組織防護的重點目標。

根據上述公式，CWE 團隊公布了 2020 年危險程度最高的前 25 名 CWE 類型漏洞。在排名前 10 的漏洞中，危險程度分數最高者爲 CWE-79：跨網站指令碼 (Cross-site Scripting, XSS)、第二高者爲 CWE-787：越界寫入 (Out-of-bounds Write)、第三爲 CWE-20：不適當輸入驗證 (Improper Input Validation)。接著，第四至第十名依序爲 CWE-125：越界讀取 (Out-of-bounds Read)、CWE-119：記憶體緩衝區內不當的操作限制 (Improper Restriction of Operations within the Bounds of a Memory Buffer)、CWE-89：SQL 隱碼 (SQL Injection)、CWE-200：向未經授權的使用者暴露機敏資訊 (Exposure of

2 CWE. “2020 CWE Top 25 Most Dangerous Software Weaknesses”. Retrieved January 19, 2021, from the World Wide Web: https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Sensitive Information to an Unauthorized Actor)、CWE-416：使用已釋放記憶體 (Use-After-Free, UAF)、CWE-352：跨站僞造請求 (Cross-site Request Forgery, CSRF)，以及 CWE-78：OS 命令注入 (OS Command Injection) [2]。

在 CVE 漏洞資訊中，除了上述之 CVSS 等級、分數和 CWE 漏洞類型外，爲提升每個漏洞修補之精準度，NIST NVD 建立通用平台評估 (Common Platform Enumeration, CPE) 標準規範，用以描述及識別相關產品的類型、使用平台及版本等資訊。CPE 資訊主要分爲三大類型：應用程式 (Application,“a”)、硬體 (Hardware,“h”) 及作業系統 (Operating Systems, “o”)。並在區分類型後，提供包含廠商名稱 (Vendor)、產品名稱 (Product)、產品版本 (Version)，以及更新套件中的產品更新 (Update)、產品版次 (Edition)，和語言 (Language) 等詳細資訊。

因此，彙整 2020 年度所有 CVE 編號之 CPE 資訊，可發現作業系統 (o) 的數量最多，佔總體 CPE 類型的 43.07%；其次爲應用程式 (a)，佔總體 CPE 類型的 36.86%；最後則爲硬體 (h)，佔總體 CPE 類型的 20.07%。而針對每種不同的 CPE 類型，結合 CVSS 等級，可分析每種 CPE 中 CVSS 等級之百分比，詳細資訊如圖 3- 8：

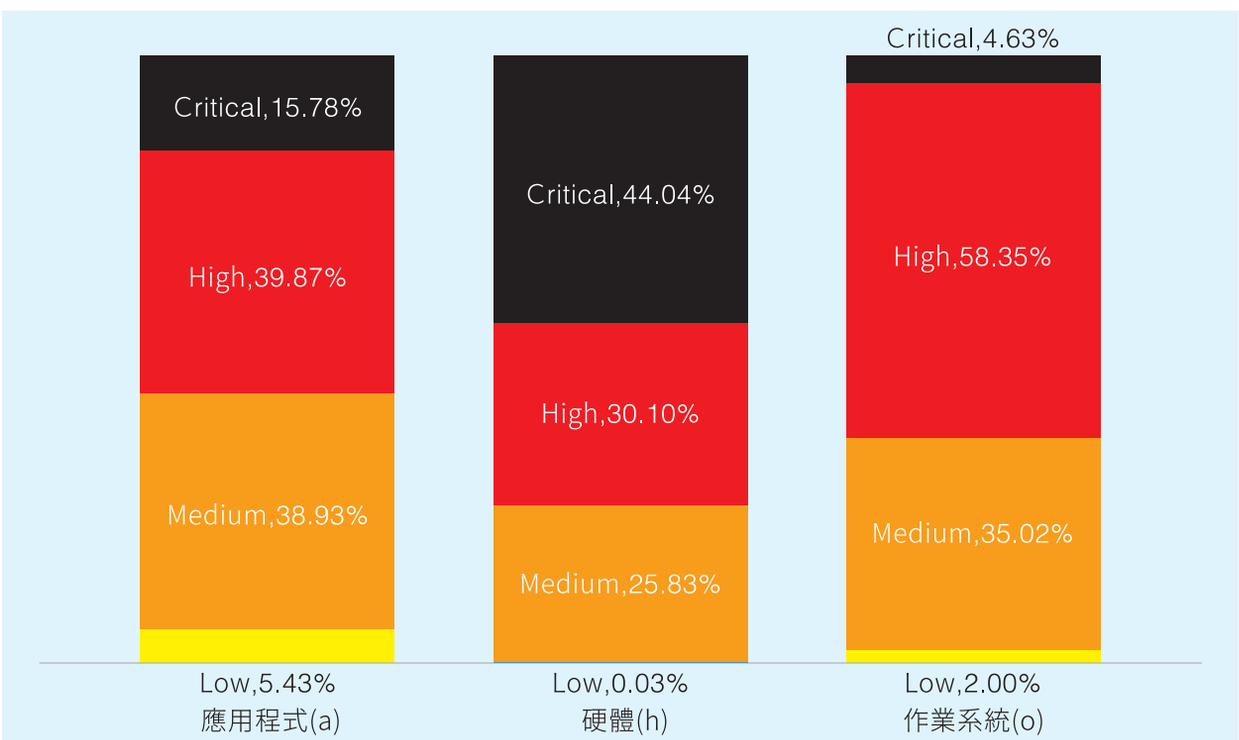


圖 3- 8：2020 年期間 CVE 編號之各 CPE 類型的 CVSS 等級比例　　資料來源：TWCERT/CC 整理

從圖 3- 8 可知，每種不同 CPE 類型的資訊產品一旦發生漏洞，容易產生的安全性 CVSS 等級也不盡相同。其中，可以明顯見得，硬體部分的 CVSS 等級比例中，對產品影響程度最爲嚴重的 Critical 比例最高，代表只要硬體設備或對硬體設備產生影響的漏洞發生，就有可能產生較爲嚴重的影響和威脅，須小心防範。

除此之外，透過 2020 年期間，各 CPE 產品與 CWE 類型數據進行交叉比對，以了解每種 CPE 產品出現的 CWE 漏洞類型排行及其比例。首先，針對應用程式 (a) 所發生的漏洞類型進行統計，詳細資訊如圖 3- 9：

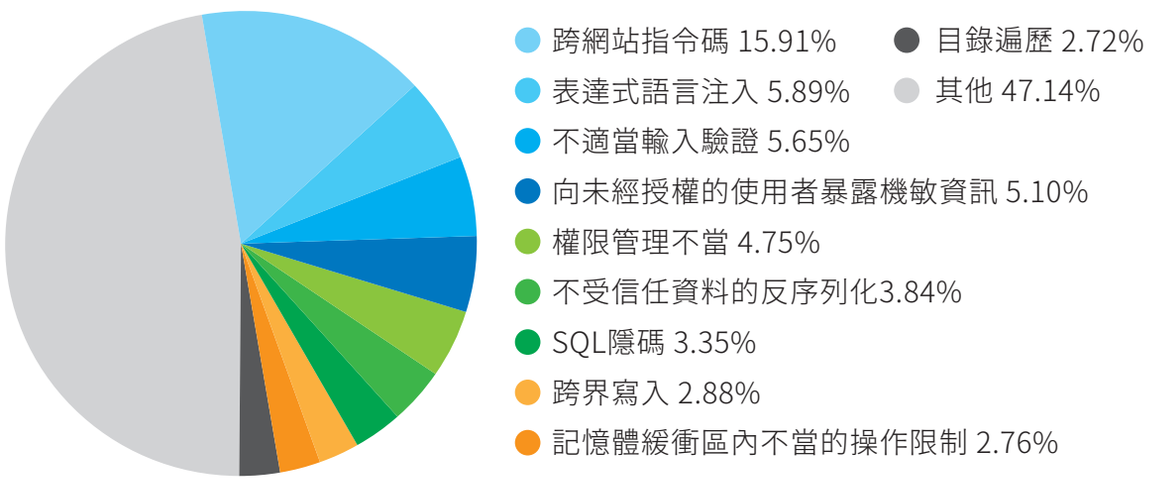


圖 3- 9：2020 年應用程式 (a) 類型中之資安漏洞類型比例　　資料來源：TWCERT/CC 整理

從圖 3- 9 可見，應用程式類型中，其 CWE 類型較爲多樣，且其每種漏洞類型比例相差無幾，亦即無法僅針對特定幾種漏洞類型進行防禦，仍需將諸多漏洞威脅作爲防範目標。

此外，應用程式前 10 名的漏洞大多數均爲 2020 年危險程度最高之前 25 名 CWE 漏洞類型中，唯有排名第二的 CWE-917(表達式語言注入 , Expression Language Injection) 不在其中，除了因應用程式在三種 CPE 類型中佔比較高，使得類型較爲相仿外，其所產生的漏洞也有一定之嚴重程度，方能進入前 25 名最危險的漏洞類型中。

因此，雖然應用程式的漏洞類型相當多樣，但其中比例較高的漏洞類型，仍可作爲警示目標之用。對欲針對應用程式類型的資訊系統進行防護者，可依此進行更爲精確之防範。

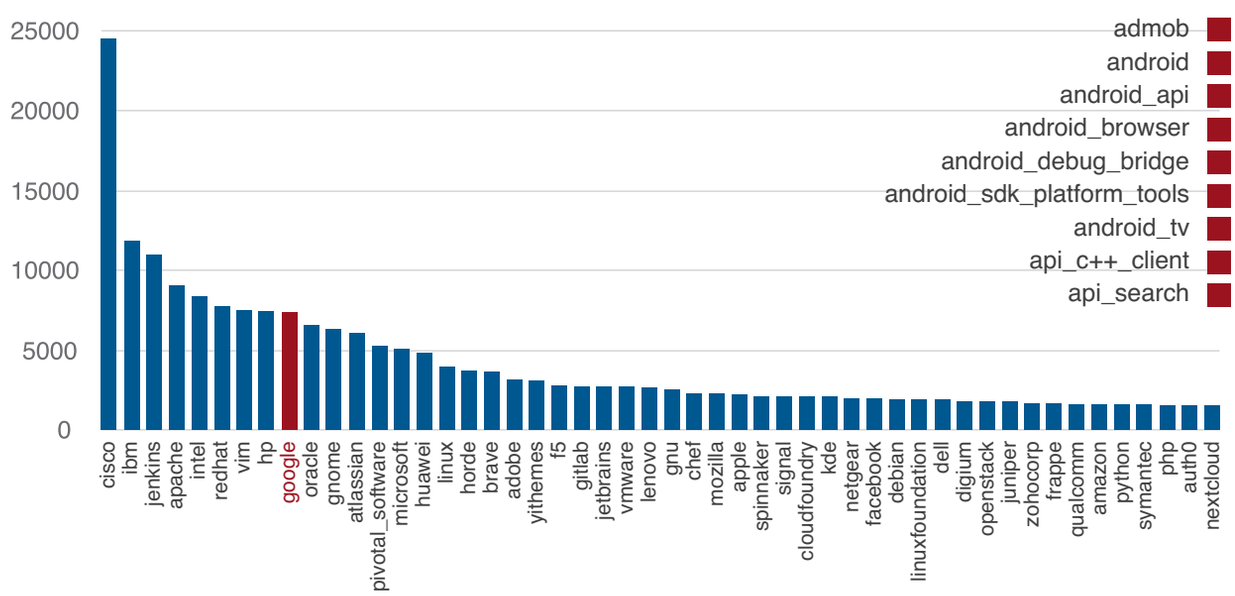


圖 3- 10：全球 CPE 廠商及產品分佈　　資料來源：NVD

所圖 3- 10 爲全球 CPE 統計分佈圖，從中可見，CPE 清單中涵蓋了大量的產品資訊，而這些產品包含了 CPE 的應用程式、硬體與作業系統三種類型。其中，雖然許多漏洞是發生於應用程式，但卻可能會對其運行的作業系統，甚至硬體，產生影響。尤其許多大型企業從硬體、作業系統到應用程式都有生產，使其軟體與硬體之間緊密且關聯性高，但若其中的應用程式或作業系統發生漏洞，則很有可能對其運行的作業系統或硬體產生影響。以圖 3- 10 中的 Google 爲例，在 CVE-2008-7298 中，其 android_browser 因沒有對 Cookie 修改進行確實限制，除應用程式 android_browser 本身外，其運行的作業系統 android 也受漏洞影響，成爲同樣容易遭受攻擊的目標。

最後，CPE 中的作業系統 (o) 所發生的漏洞類型進行統計，詳細資訊如圖 3- 11：

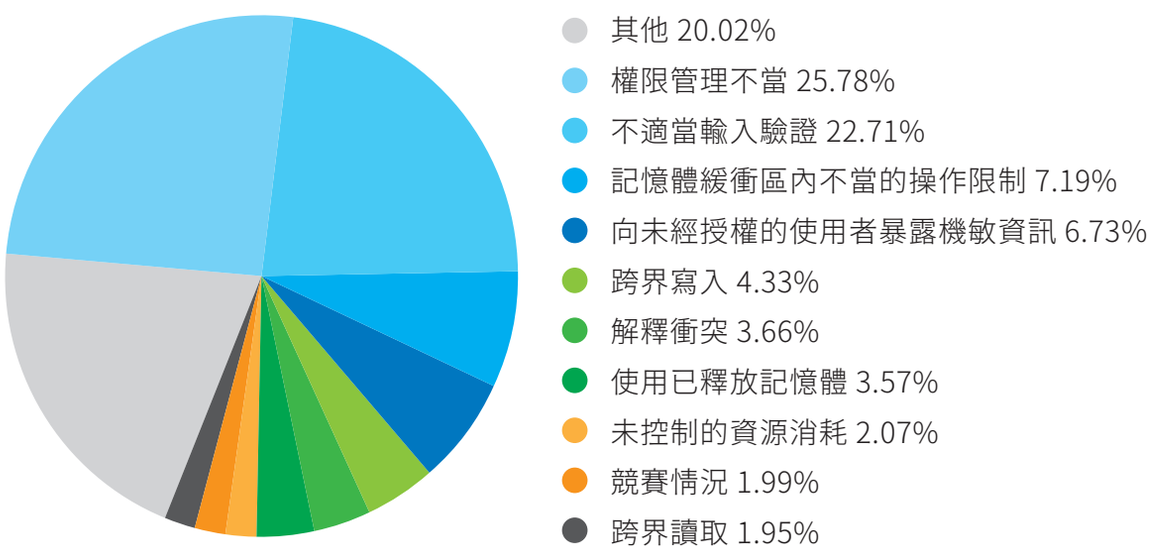


圖 3- 11：2020 年作業系統 (o) 類型中之資安漏洞類型比例　　資料來源：TWCERT/CC 整理

從圖 3- 11 可見，作業系統類型之漏洞類型數量居中，但有幾種漏洞類型佔比相當高，尤其排名第一的 CWE-269：權限管理不當 (Improper Privilege Management) 數量已超過總數量的四分之一，顯示作業系統所發生或對其產生影響的漏洞類型都集中在特定幾個漏洞類型中。因此，這些較常發生的漏洞類型，將會是在作業系統產品中，首要進行防範的對象及目標。

此外，在作業系統排名前 10 的漏洞中，大部分都包含在 2020 年危險程度最高之前 25 名 CWE 漏洞類型中，僅有兩個漏洞類型並不屬於其中，包括 CWE-436：解釋衝突 (Interpretation Conflict) 和 CWE-362：競賽情況 (Race Condition)，這兩個漏洞雖然並未在全體產品的危險程度中上榜，但對於針對作業系統的防範者而言，亦是需多加留意且著重防禦的對象之一。

而另一以 CPE 和 CWE 進行比對之統計資訊，得以見得每種類型所產生或受影響的 CWE 漏洞之數量和比例。其中，應用程式部分，雖然其 CWE 類型較多，因此，相關防護者必須針對應用程式之產品，進行全方位的漏洞檢視和防禦，避免發生任何一種損害企業產品安全及對使用者造成威脅的資安漏洞。而硬體和作業系統部分之 CWE 類型都爲數量較少或集中於特定漏洞類型，是作爲防範對象的良好目標，相關人員可針對這些集中且佔比較高的漏洞類型，進行加強的資安防禦。但針對硬體和作業系統，也並非單純針對那些常見資安漏洞進行防禦即可，仍需注意其他可能產生之漏洞，甚至，由於那些佔比相當高的漏洞類型極爲常見，導致容易成爲攻擊者的攻擊目標，因此，要完全杜絕這些漏洞所帶來的威脅，還需進行進一步且深度防護，以達到保障資訊產品安全性之目標。

二、我國發布之產品漏洞概況

TWCERT/CC 參與美國非營利組織 MITRE 之 CVE 計畫，在共計 26 個國家、156 個組織的 CVE 編號管理者 (CNA) 中，擔任台灣區 CNA，負責接收、審核及發布資安漏洞 CVE 編號，並同時將漏洞資訊公告於台灣漏洞揭露平台 (Taiwan Vulnerability Note, TVN)，讓更多相關單位了解並依此進行進一步的資安漏洞防護。

在擔任台灣區 CNA 的角色中，TWCERT/CC 除進行產品資安漏洞確認、審核、作爲通報者與廠商之間的協調者之外，同時也會主動搜尋有該產品使用及相關的組織、單位，並於蒐整之後個別告知，並協助其針對該產品之資安漏洞進行適當防護，避免遭到惡意使用者利用進行攻擊，也能讓產品廠商在修補完畢後，讓更多的使用者與使用單位配合更新，達成全面之產品漏洞修補防護，大幅提升國內資安漏洞防護之能量。

在 2020 年期間，TWCERT/CC 總計接獲約 20 項產品，超過 50 個漏洞之資安通報，其 CVE 產品類別與編號統計如表 3- 2：

	產品類型	數量	CVE 編號
硬體	智慧監控	7	CVE-2020-10513、CVE-2020-10514、CVE-2020-3920、CVE-2020-3921、CVE-2020-3923、CVE-2020-3924、CVE-2020-3936
	設備控管	4	CVE-2020-3928、CVE-2020-3929、CVE-2020-3930、CVE-2020-3931
	網路通訊	4	CVE-2020-12773、CVE-2020-12774、CVE-2020-24552、CVE-2020-3932
系統	電子郵件	15	CVE-2020-10511、CVE-2020-10512、CVE-2020-12782、CVE-2020-17384、CVE-2020-17385、CVE-2020-17386、CVE-2020-25848、CVE-2020-25849、CVE-2020-25850、CVE-2020-35740、CVE-2020-35741、CVE-2020-35742、CVE-2020-35743、CVE-2020-35851、CVE-2020-3922
	企業管理	14	CVE-2020-10505、CVE-2020-10506、CVE-2020-10507、CVE-2020-10508、CVE-2020-10509、CVE-2020-10510、CVE-2020-12777、CVE-2020-12778、CVE-2020-12779、CVE-2020-12780、CVE-2020-12781、CVE-2020-3933、CVE-2020-3934、CVE-2020-3935
	設備控管	1	CVE-2020-25847
平台	金融資訊	3	CVE-2020-3937、CVE-2020-3938、CVE-2020-3939
	企業管理	1	CVE-2020-24551
	電子郵件	1	CVE-2020-12776
應用程式	網路安全	8	CVE-2020-25842、CVE-2020-25843、CVE-2020-25844、CVE-2020-25845、CVE-2020-25846、CVE-2020-3925、CVE-2020-3926、CVE-2020-3927
總累計 CVE 數量：58 個			

表 3- 2：TWCERT/CC 審核發布之 CVE 類別與編號統計表　　資料來源：TWCERT/CC 整理

在國內，除了 TWCERT/CC 外，QNAP Systems, Inc. 與 Synology Inc. 亦爲台灣區之 CNA，針對其產品發布及修補漏洞。經統計，台灣區三間 CNA 於 2020 年期間所發布之 CVE 漏洞，總計 103 個，並以此進行國內資安漏洞之統計分析。

針對國內本年度發布之所有 CVE 編號，每個漏洞均有其針對的 CWE 類型，因此，以 CVE 編號作爲母體進行統計，出現次數最多者爲 CWE-79(跨網站指令碼)，佔總漏洞數量 21%。第二高者爲 CWE-89(SQL 隱碼)，佔總漏洞數量約 10%。第三高者包含 CWE-77(命令注入 , Command Injection)、CWE-78(OS 命令注入) 及 CWE-200(向未經授權的使用者暴露機敏資訊)，均佔總體數量之 6%。

此外，同樣以 CVE 作爲母體進行統計，平均 CVSS 分數最高者包含 CWE-74(注入漏洞)、CWE-120(緩衝區溢位)、CWE-434(沒有限制危險類型的檔案上傳 , Unrestricted Upload of File with Dangerous Type)、CWE-522(憑證防護不足 , Insufficiently Protected Credentials) 以及 CWE-787(越界寫入) 這五種漏洞類型，每種類型之平均 CVSS 分數均爲 9.8，是嚴重等級最高的 Critical 等級，代表在國內產品中，一旦上述漏洞發生，便會對其與相關產品產生嚴重影響，是首要且主要防範之漏洞類型。

然而，爲瞭解每種 CWE 類型的危險程度，並非僅依據漏洞的發生次數或其影響程度，而是需將兩者相輔相成，一旦此漏洞類型出現次數多，以及每次出現後的影響程度大，才會被認爲該漏洞於本年度擁有高危險度。

因此，透過國內於 2020 年所發布之 CVE 資訊，以各 CVE 漏洞之次數、CVSS 分數等數據，計算我國本年度危險程度最高之前 10 名 CWE 漏洞類型，詳細資訊如表 3- 3：

排名	CWE 編號	漏洞類型
1	CWE-79	跨網站指令碼 (Cross-site Scripting, XSS)
2	CWE-77	命令注入 (Command Injection)
3	CWE-78	OS 命令注入 (OS Command Injection)
4	CWE-89	SQL 隱碼 (SQL Injection)
5	CWE-74	注入漏洞 (Injection)
6	CWE-863	不正確的授權 (Incorrect Authorization)
7	CWE-798	將驗證的機密性資料直接寫入 (Use of Hard-coded Credentials)
8	CWE-120	緩衝區溢位 (Classic Buffer Overflow)
9	CWE-522	憑證防護不足 (Insufficiently Protected Credentials)
10	CWE-22	目錄遍歷 (Path traversal)

表 3- 3：我國 2020 年危險程度最高前 10 名 CWE 漏洞類型彙整表　　資料來源：TWCERT/CC 整理

根據表 3- 3 可以見得，這些漏洞類型與單純的發生次數和平均 CVSS 分數排名迥異，必須其發生次數與影響程度均爲高，方被認爲擁有較高的危險程度。然而，從表中亦可發現，國內產品之 CVE 漏洞類型與其危險程度，與國際間有所差異，在前十名漏洞類型中，有四個並未成爲全球最危險前 25 名之一，可能因全球與這些資訊產品與其使用之硬體、系統及程式等不同，造成發生的漏洞類型有所差異。雖然這些數據僅針對國內三間 CNA 所發布之國內資通訊產品漏洞，但仍是國內廠商用以加強自家產品資安防護的良好參考資訊及目標。

在了解國內產品漏洞危險分數後，再將發生該漏洞之產品或該漏洞影響的產品進行區分，依據 CPE 類型，可將其區分爲應用程式 (a)、硬體 (h) 及作業系統 (o)。根據統計，數量最多者爲應用程式 (a)，佔總受影響產品數量的 51.76%；第二高者爲作業系統 (o)，佔總數的 34.96%；最後爲硬體 (h)，佔總數之 13.28%。並且爲了瞭解各種 CPE 類型中，發生或受到影響的漏洞影響程度，再以其 CVSS 進行統計，詳細資訊如圖 3- 12：

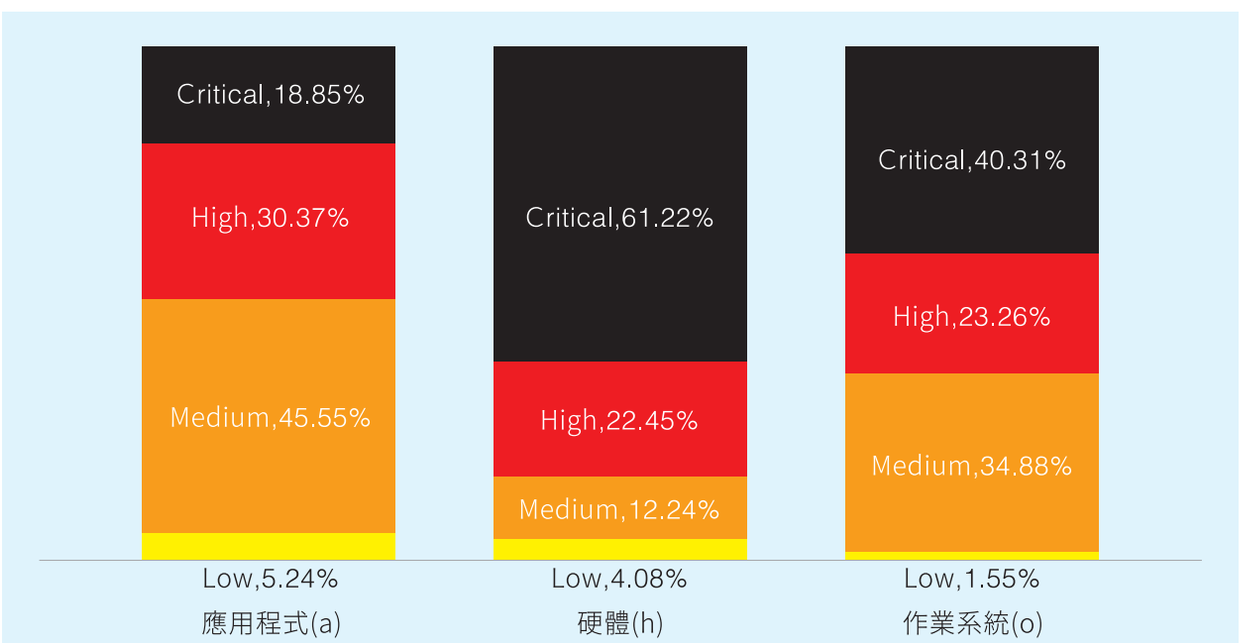


圖 3- 12：2020 年期間我國各 CPE 類型的 CVSS 等級比例　　資料來源：TWCERT/CC 整理

從圖 3- 12 可知，不論是國內或國際發布的 CVE 漏洞，每種 CPE 類型，其容易產生的安全性 CVSS 等級也不盡相同。但在國內產品 CVE 的統計中，除硬體外，作業系統的 CVSS 等級，也都以 Critical 佔比最高，因此，國內相關廠商應同樣針對作業系統進行謹慎防範，避免產品發生漏洞問題時，對作業系統產生嚴重影響。

除此之外，亦針對國內漏洞之 CPE 類型和其 CWE 類型進行交叉比對，呈現每種 CPE 中最爲常見的 CWE 類型。首先，針對應用程式 (a)，資訊如圖 3- 13：

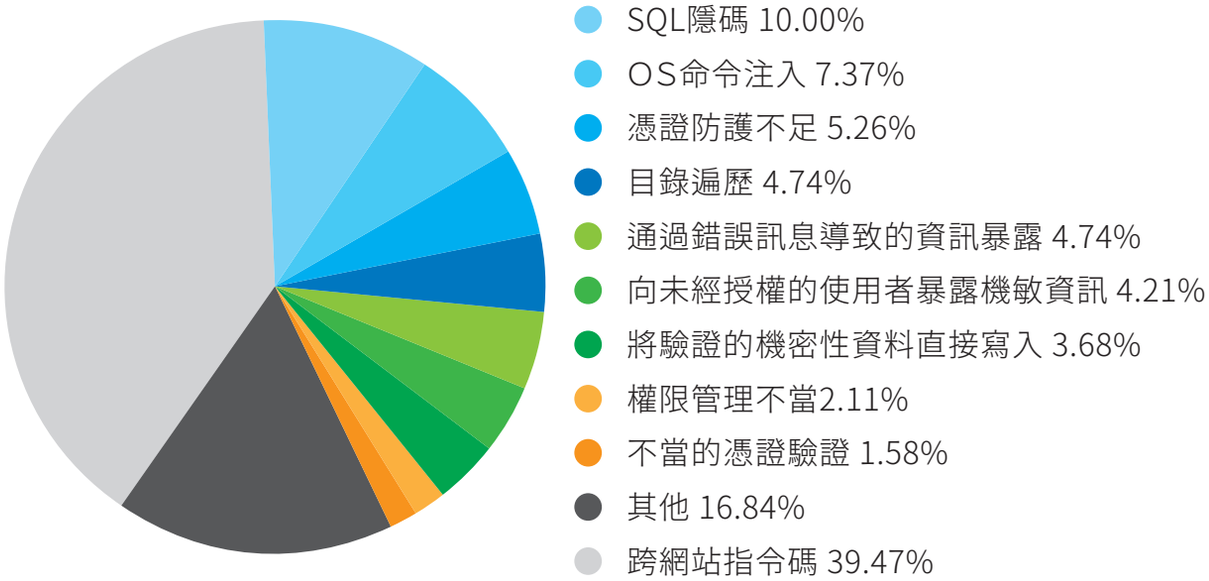


圖 3- 13：2020 年我國 CVE 應用程式 (a) 類型中資安漏洞類型比例　資料來源：TWCERT/CC 整理

從圖 3- 13 可見，應用程式類型中，其 CWE 類型較多且分散，僅有排名第一的 CWE-79：跨網站指令碼，佔全體數量近 40%，但在剩餘的漏洞類型中，其數量與比例相差不大。而這樣類型較多的情況中，較難鎖定特定漏洞類型進行應用程式的防範，應用程式廠商與相關企業都必須針對所有可能的漏洞類型進行防範，甚至這些資安防範會涉及其運行的作業系統及硬體，才能有效隔絕從硬體面和作業系統入侵應用程式之攻擊。

在前 10 名的漏洞類型中，80% 爲全球排名中之 CWE 類型，僅有排名第六的 CWE-209：通過錯誤訊息導致的資訊暴露 (Generation of Error Message Containing Sensitive Information) 與第十的 CWE-295：不當的憑證驗證 (Improper Certificate Validation)，但卻有四項並未列於國內 CWE 排名中，亦即應用程式類型於全球不論是發生次數還是影響程度的比例都較國內高，因此其危險程度漏洞類型也較爲相仿。但雖如此，並非國內相關產品對其應用程式就不需多加防護，僅是許多漏洞除了發生或影響應用程式之外，同時還影響了硬體及作業系統，導致硬體及作業系統的比例相對提升，因此，相關產品除了仍須針對應用程式多加防護外，還需針對與其相關的硬體與作業系統一併進行檢驗及防護，避免因應用程式本身的漏洞，對商品的作業系統和硬體安全性，以及相關商家的聲譽產生嚴重損害。

硬體也會受應用程式與作業系統漏洞影響：

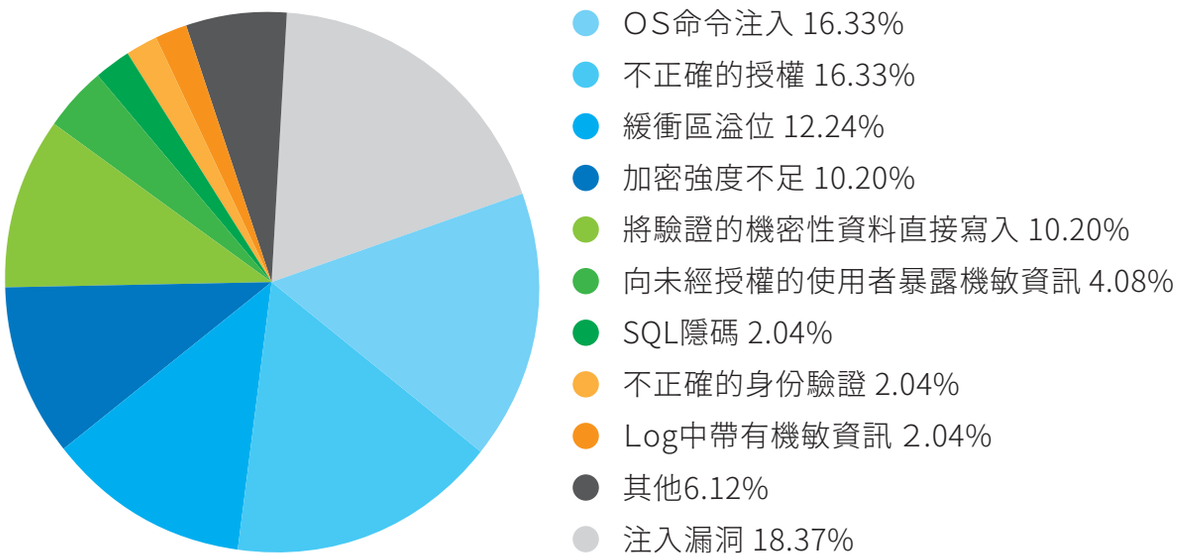


圖 3- 14：2020 年我國 CVE 硬體 (h) 類型中之資安漏洞類型比例　　資料來源：TWCERT/CC 整理

從圖 3- 14 可見，會影響到硬體之漏洞類型中，其前十項類型便佔據整體數量的近 94%，相較於應用程式和作業系統類型，硬體部分的漏洞防範目標較爲精確。且雖在其十項漏洞類型中，有約一半的 CWE 並未包含於全球危險排行榜中，包含 CWE-74：注入漏洞、CWE-863：不正確的授權 (Incorrect Authorization)、CWE-120：緩衝區溢位、CWE-326：加密強度不足 (Inadequate Encryption Strength) 以及 CWE-295：不當的憑證驗證；亦有 40% 的項目未包含在國內的排行榜中，包括 CWE-326：加密強度不足、CWE-200：向未經授權的使用者暴露機敏資訊、CWE-287：不正確的身份驗證，以及 CWE-295：不當的憑證驗證。這表示在三種 CPE 類型中，硬體類型的佔比都不高，因此類型與全部 CPE 類型的統計中有較大的差異。但正因其差異較大，將三者數據進行交集後所重疊的漏洞類型，將是於漏洞類型中常見，且其嚴重程度也足以進入國際及國內排行中的 CWE 類型，是國內相關廠商針對硬體時，首要進行防範的對象及目標。

但即便硬體發生或受到影響的漏洞類型數量少且精確，也並非僅針對這些漏洞類型即可，這些漏洞類型僅爲廠商及相關企業首要的防禦項目，其餘的漏洞類型仍需進行防範，甚至這些重要漏洞類型，因其較爲常見且影響嚴重，因此不能僅進行基本防護，必須建立深入且全面的防禦機制，甚而必須包含該硬體所運行的應用程式和作業系統，方能大幅降低資安漏洞所帶來的威脅。

CPE 中的作業系統 (o) 類型統計資訊如圖 3- 15：　　資料來源：TWCERT/CC 整理

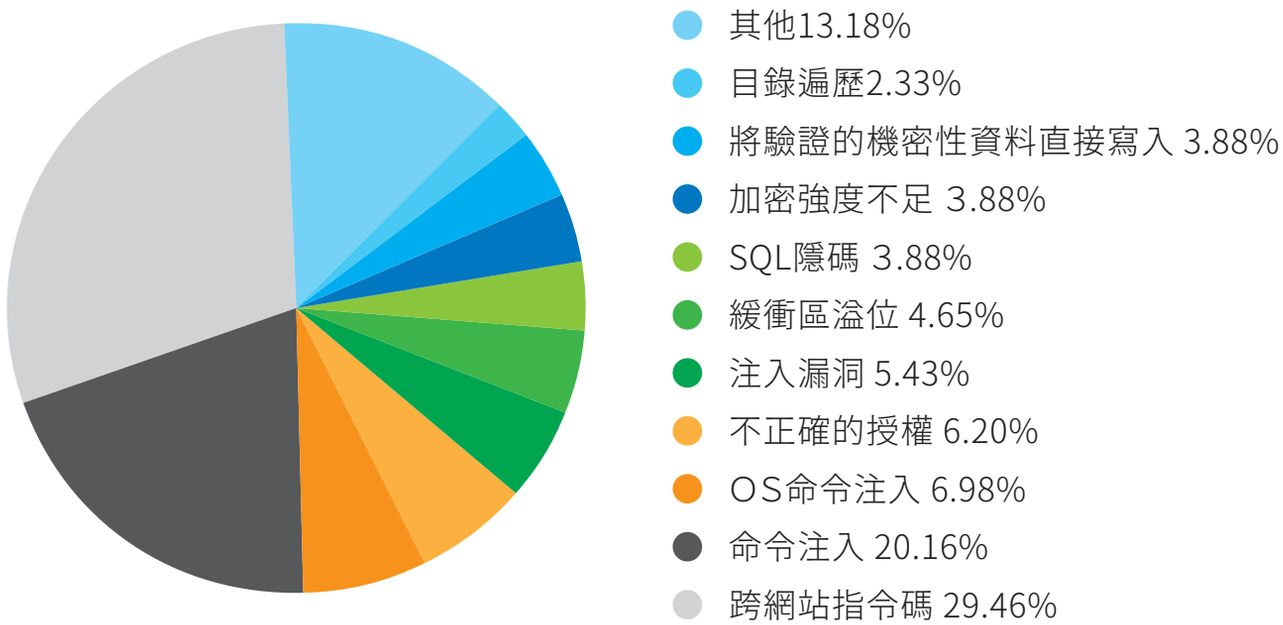


圖 3- 15：2020 年我國 CVE 作業系統 (o) 類型中之資安漏洞類型比例

從圖 3- 15 可見，作業系統類型中，其類型較多，雖其前兩名漏洞類型之佔比已經接近 50%，是國內作業系統應著重防禦的漏洞類型，但整體而言，僅僅兩種漏洞類型的防範在安全性上遠遠不足，因此，作業系統需防禦之目標漏洞類型仍多。而其前十名的漏洞類型中，有一半的類型並未包含於全球前 25 名最危險漏洞類型中，包括 CWE-77：命令注入、CWE-863：不正確的授權、CWE-74：注入漏洞、CWE-120：緩衝區溢位及 CWE-326：加密強度不足。但卻有 90% 位於國內 CVE 最危險漏洞類型中，僅有 CWE-326：加密強度不足，未包含其中。此種狀況下，可分析國內的 CVE 漏洞，在作業系統上，不論是出現次數或嚴重程度，都較國際間更高，因此其類型才會與國內排行較爲相符。

此外，正因其漏洞類型也較爲多且平均，除了比例最高的前兩種類型外，其餘的漏洞類型中較難鎖定特定對象進行作業系統的防範，作業系統廠商與相關企業都必須針對所有可能的漏洞類型進行防範，甚至這些資安防範會涉及其中的應用程式以及其運作的硬體，才能有效隔絕從硬體面和應用程式入侵之攻擊。

TWCERT/CC 爲台灣區之 CNA 角色，會針對台灣區的資通訊產品進行資安漏洞確認、審核，並發布相對應的 CVE 編號和其資訊。透過分析國內 CNA 於 2020 年發布的漏洞資訊，希望以此提供國內資安防護的一個方向與目標，達成提升台灣整體資安防護能量之願景。

三、TWCERT/CC 發布之 CVE 資安漏洞品質，獲美國 NIST NVD 評核爲 Contributor

TWCERT/CC 在 2018 年取得 MITRE 授權成爲 CNA 成員，協助國內組織及企業審核及發放 CVE 編號。自 2019 年至 2021 年 2 月，TWCERT/CC 已審核並發布共 84 個產品漏洞之 CVE 編號，其漏洞產品涵蓋國內 DVR 產品、智慧家電、語音設備、網通設備與軟體服務系統。

針對發布之 CVE 漏洞，NIST NVD 會依據 CNA 所通報之 CWE 漏洞類型及 CVSS 漏洞風險與影響程度進行評核，以確保 CVE 漏洞資訊的正確性及一致性。NVD 也會針對 CNA 提供的 CWE 與 CVSS 資訊和 NVD 審核的 CWE 與 CVSS 資訊進行比對和評分，並以該評分從低至高將 CNA 成員分成參考者 (Reference)、貢獻者 (Contributor) 及提供者 (Provider) 三個等級。其中，Provider 等級必須與 NVD 審核結果達到 95% 以上的匹配率，而 Contributor 等級則必須達到 70% 以上之匹配率，由此可見 Provider 及 Contributor 等級的 CNA 均必須具備高度之技術水準方能得此殊榮。

TWCERT/CC 爲 MITRE 授權之 CNA，致力於我國產品漏洞之 CVE 審核與發布，在多年積極努力下，於 2020 年獲得美國 NVD 評核在 CVSS 3.1 取得貢獻者 (Contributor) 等級之殊榮！此殊榮除了肯定 TWCERT/CC 的貢獻外，更彰顯國內企業對其產品漏洞修補配合度相當高，透過 TWCERT/CC 協助國內廠商處理產品漏洞，儘快完成漏洞緩解及修補，以避免駭客利用產品漏洞造成使用者遭駭之情況發生，並提升我國產品之資安防護能力。

四、國際資安事件與漏洞協處案例

1.UPnP 網路協定之資安弱點

TWCERT/CC 接獲國際情資指出，UPnP Subscribe 功能存在資安弱點，影響不局限於單一產品，採用 UPnP 協定之設備或系統皆可能受到影響。當攻擊者存取 UPnP 終端設備，進行以下攻擊：

(1) 攻擊者可利用網際網路開放之 UPnP 設備，來進行反射放大 TCP DDoS 攻擊。
(2) 攻擊者可透過 UPnP Subscribe 的功能，使 UPnP 設備向外部網域洩漏資料。

建議使用者處置方式如下：

(1) 限制 UPnP 裝置暴露於 Internet 上。
(2) 監控 UPnP 類型的 DDOS 流量。

TWCERT/CC 確認資訊後將此弱點及相關處置建議告知相關單位與企業，請其進行相關處理，避免受駭。

2.Thunderbolt 3 漏洞

TWCERT/CC 接獲國際情資指出，廣泛內建於高階主機和筆記型電腦的高速傳輸界面 Thunderbolt 3 存在嚴重的硬體安全漏洞，允許攻擊者輕易地於數分鐘內，破解電腦安全加密並竊取使用者資料。

TWCERT/CC 接獲通報確認後，隨即與國內硬體相關廠商聯繫，提供漏洞資訊請其防範。建議使用者應依照 Microsoft 的說明，正確設定 Thunderbolt 3 的內核 DMA 保護，

若無法自行設定相關安全措施，應聯絡製造商或其他技術支援服務來確保設備安全。切勿將不信任的周邊設備連接電腦，並且在 Thunderbolt 3 介面已啓用的情形下，勿讓電腦設備離開視線或借予他人，以避免遭受攻擊。

3.F5 BIG-IP 漏洞

TWCERT/CC 接獲國際通知，F5 BIG-IP ADC 產品具高風險漏洞。F5 Networks 的知名網路及安全產品 BIG IP 應用遞送控制器 (Application Delivery Controller，ADC) 存在一個重大安全漏洞 (CVE-2020-5902)，可讓不具授權的遠端攻擊者執行指令，並取得系統完整控制權，包括攔截流經該設備的應用流量。根據收到受影響的 IP 情資，分別通知受影響的 228 個 IP 單位，告知相關漏洞資訊。

4.Fortinet SSL VPN 漏洞情資

12 月初 TWCERT/CC 接獲國外資安機構資安專家揭露，有關 Fortinet SSL VPN 2018 年遭揭露之漏洞 CVE-2018-13379，全球仍有近 5 萬個 IP 裝置尚未更新，仍有其資安風險。TWCERT/CC 根據該研究人員揭露受影響之 IP 單位，通告台灣相關受影響未更新的單位及企業，分別告知逾 40 個企業單位相關資安漏洞資訊，並請企業單位盡速更新，避免受駭。

五、國內資安事件與漏洞協處案例

1. 國產晶片漏洞事件

TWCERT/CC 接獲國際情資表示：某國內廠商生產之網通產品晶片有資安漏洞，攻擊者可以透過預設帳密，使用該晶片預設開啓的 netlog 功能，取得終端介面執行任意指令，我國有多家業者受此漏洞影響。TWCERT/CC 確認漏洞後，立即透過該廠商設立之產品資安通報窗口進行情資通報與聯繫受影響之業者多加注意。目前該漏洞已完成修補，並於 6 月 8 日公告 CVE。

2. 網通儲存設備 (NAS) 勒索攻擊事件

TWCERT/CC 接獲通報，在 5 月 23 日至 5 月 29 日之間，約發生 20 起 NAS 勒索攻擊。深入了解後，發現該起攻擊事件與 2019 年 11 月發生的勒索攻擊事件爲同一資安漏洞所致，使用者只要進行韌體更新即可避免受駭。因此相關廠商再次提供漏洞和更新資訊，請 TWCERT/CC 進行相關資安消息發布，請各政府、企業單位和民衆注意，並且應儘速修補及更新以避免遭受攻擊。

3. 郵件防護系統案例

TWCERT/CC 官網接獲企業主動通報，旗下郵件防護系統存有命令注入漏洞，且陸續有相關受駭狀況。爲避免使用者產生資安威脅，該廠商已儘速完成漏洞修補，並主動提供相關漏洞資訊供 TWCERT/CC 進行資安消息發布，已請各政府、企業單位和民衆注意，小心防範以及儘速配合廠商修補漏洞。

4. 仿政府單位釣魚郵件

TWCERT/CC 官網接獲企業通報，有一假冒政府單位「免費分發 COVID-19 防護設備」的釣魚信件，信件要求下載含惡意程式之附檔並回傳。收到通報後，TWCERT/CC 立即針對此一釣魚信件附件進行分析，並提供相關資訊提醒政府單位和企業等應多加留意此社交攻擊。

5. 某科技公司遭駭侵攻擊

TWCERT/CC 官網接獲民眾通報收到釣魚郵件，從通報郵件中發現該連結確實屬於釣魚網站的連結，但寄送人確是該企業正確的郵件主機位置名稱和 IP 範圍，因此主動聯繫企業瞭解狀況，證實 8 月初該企業有發生駭侵事件，並於 8 月底收到相關勒索信件。而後 TWCERT/CC 與其簽定 NDA，協助分析此駭侵行動之惡意檔案和系統漏洞狀況，加強該企業之資安防護。

6. 某電商平台遭駭以致資料外洩

TWCERT/CC 接獲民眾通報某女裝電商有個資外洩之事件並接獲詐騙電話。向該電商承包的網站平台詢問後了解狀況如下：目前已知共有 8 間電商平台受害，訂單資料與聯繫資訊，如姓名、電話、email 等個資外洩。經查證後，發現問題爲網頁存有 SQL 隱碼資安漏洞，導致客戶資料外洩。在溝通與協助後，該電商已於事件發生後兩周內修補完畢，並全數以簡訊提醒客戶防範詐騙。

第四章、

合作交流與資安推廣

為提升大眾之資安意識與資安事件通報意願，TWCERT/CC 做為我國企業資安事件通報及協處之首要窗口，每年舉辦相關資安通報應變研討會，並積極參與國內外知名資安會議與活動，提升 TWCERT/CC 之國際知名度，以建立國內外良好暢通之資安情資交流管道，強化國內整體資安防護能量。

第一節、主辦活動

一、台灣資安通報應變年會

隨著全球資訊環境的瞬息萬變，在物聯網、AI、5G 技術快速發展下，資訊安全議題已成為數位經濟下重要顯學。TWCERT/CC 於 10 月 27 日主辦 2020 台灣資安通報應變年會，本次年會主題為「超前部署，掌握資安聯防與應變先機」，讓與會者了解如何透過資安聯防與應變，達到最佳之資安防範與部署。

本次年會中，邀請到國內產官學各界的資安重要人士來分享與討論資安相關議題。TWCERT/CC 做為協助企業面對、處理和解決資安問題的合作夥伴，我們致力於幫助企業盡速解決資安問題，同時避免事件擴大影響範圍，降低資安事件發生的衝擊，也於會中分享資安相關情報給不同產業別的企業，以達到資安聯防之目的。

圖 4-1：2020 年台灣資安通報應變年會活動現況　　資料來源：TWCERT/CC 整理

本次年會持續對企業宣導資安意識和資安通報的重要性，並分享各產業別之企業資安解決方案與防護措施，透過資安案例的分享，從中汲取相關產業面對資安威脅的應變措施，建立具有完善資安應變流程的產業生態，進而擴大台灣企業的資安認知與防護能量。

依年會參與者統計分析，本次與會者以資訊服務業爲大宗，占總人數 27%，其次爲製造業、金融單位，再其次則爲高科技產業及政府單位，詳如圖 4- 2：

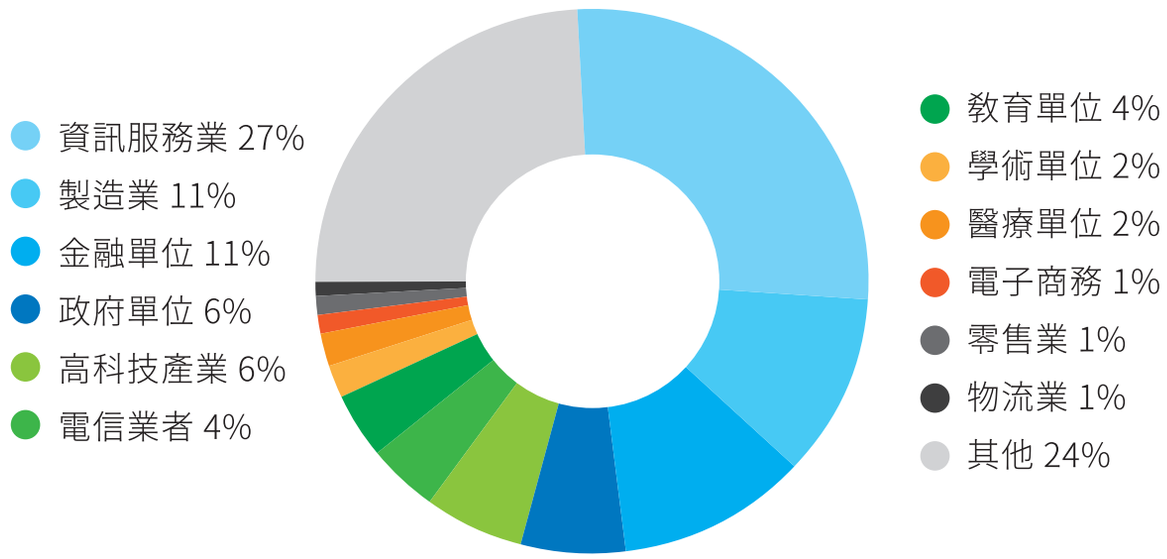


圖 4- 2：活動與會者行業別分析　　資料來源：TWCERT/CC 整理

依滿意度調查，高達 99% 的民眾感到滿意；全數之參與者均表示此會議對其有所幫助；並且有 99.4% 的活動參與者，願意再參加下次的年會活動。

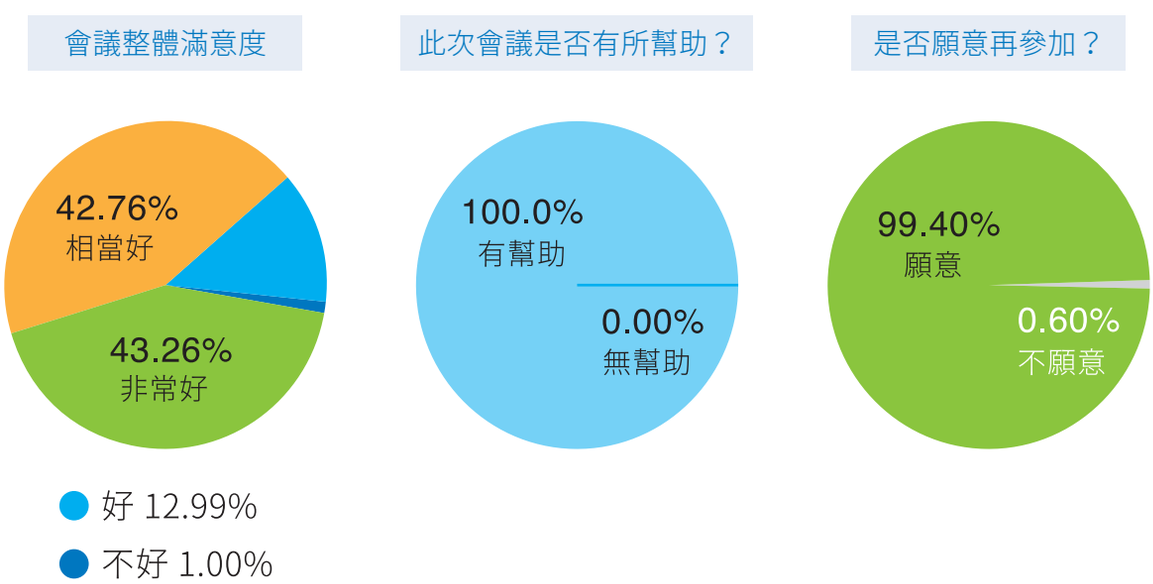


圖 4- 3：與會者回饋問卷統計分析　　資料來源：TWCERT/CC 整理

整體而言，此次台灣資安通報應變年會已確實達到宣傳資安意識、提升品牌認知，以及增添資安通報意願之目的。未來，TWCERT/CC 亦會持續定期舉辦相關資安活動，希望能藉此達成強化全國資安防護能量之目標。

二、台灣 CERT/CSIRT 聯盟交流會議

爲讓台灣各 CERT/CSIRT 和企業單位有固定聯繫管道、互通國內資安情資交流，由 TWCERT/CC 整合國家電腦事件處理中心 (Taiwan National Computer Emergency Response Team, TWNCERT)、國家通訊傳播委員會電腦危機處理中心 (National Communications Commission Computer Emergency Response Team, C-CERT)、台灣學術網路危機處理中心 (TANet Computer Emergency Response Team, TACERT)、經濟部商業司及民間企業等單位，共同組成「台灣 CERT/CSIRT 聯盟」，定期提供資安情資，舉辦資安交流活動與相關教育訓練，以強化資安防禦體系，增加我國資安資訊交流管道及效益。

在 2020 年期間，台灣 CERT/CSIRT 聯盟共新增 75 個單位成員，總累計已達 100 個會員單位。會員類型包括資安公司、法人單位、相關公協會，以及一般企業單位等，都希望藉此機會提升共同的資安防護能量。

本年度共召開兩次台灣 CERT/CSIRT 聯盟會議，第一次聯盟會議在 7 月 16 日於台北文創舉辦，共計 29 個單位、51 個成員參與。本次會議中，首先由 HITCON Zeroday 的翁浩正總召進行演講，分享國內資安漏洞趨勢及案例，提升成員對產品的資安漏洞防範意識。接著，由聯盟成員威聯通科技 (QNAP) 講述其產品資安事件應變小組 (PSIRT) 之組織、運作流程，並分享相關產品的資安處理實例，讓更多成員了解並提升相關資安組織的建立意願。再接續，由果核數位分享 OWASP API Security top10 相關的弱點案例與處理狀況，讓相關企業及成員能藉此了解 API 的資安趨勢，並進行更爲精確的防範作業。最後，TWCERT/CC 林克容資深工程師與大家介紹本年度的工作項目，以及相關的資安通報和資安服務內容，希望透過與成員的分享交流，達成強化國內整體資安防護能量之宏願。

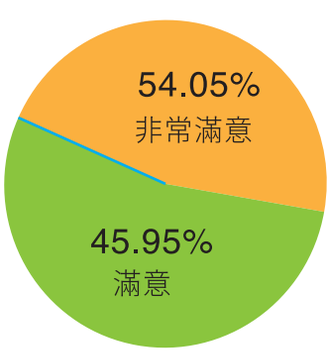
台灣 CERT/CSIRT 聯盟第二次聯盟會議在 12 月 3 日於台北文創舉辦，共計 37 個單位、51 個成員參與。本次會議首先由中華資安國際的林峰正經理，從紅藍攻防實戰視角分享對於 2021 資安趨勢的觀察，除分析大量的統計數據和相關案例外，亦從紅隊角度講述攻擊者攻擊的面向及案例，讓成員得以從如此全方位的分析中，了解如何更進一步增加自身組織的資安防護。接著，由聯盟成員合勤科技游政卿資安長，針對 PSIRT 之建立、運作和資安事件處理，從自身經歷出發，提供成員對資安組織建立的必要與其發展方向，讓成員能更加深刻地了解並重視資安組織的重要性。第三場，由如梭時代分享如何透過電子商務網站進行駭侵攻擊與資安防禦的運作實例，透過對逐漸興起之電子商務產業攻擊的詳細內容及深度分析，讓成員得以從中學習如何避免類似事件重演。最後，由 TWCERT/CC 鄭意璇管理師，說明 110 年度的預計工作項目內容及 TWCERT/CC 所提供之資安服務，希望藉此讓更多企業和成員在 TWCERT/CC 的引導下，合力建構我國安全之網路環境。

除了定期舉辦之聯盟會議外，台灣 CERT/CSIRT 聯盟亦定期辦理資安教育訓練。台灣 CERT/CSIRT 聯盟於 8 月 6 日在集思交通部會議中心舉辦聯盟教育訓練，本次訓練主題爲「攻擊檢測實務」，共有 23 個單位、52 個成員參與。課程內容主要爲剖析 Kali Linux 2020，以及其內的必要攻擊工具，如 Nmap, Metasploit, Burp Suite 等。希望透過本次教育訓練，共同提升聯盟成員及相關企業之資安能量。

在兩次聯盟會議以及教育訓練中，均取得極高的滿意程度，同時也接獲諸多良好回饋。希望能透過此聯盟成員間的交流合作，持續發展並讓台灣CERT/CSIRT聯盟變得更好、更完善，達成提升台灣整體網路環境安全品質之夙願。

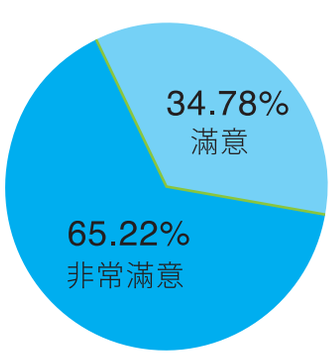
圖 4-4：台灣 CERT/CSIRT 聯盟會議盛況　　資料來源：TWCERT/CC 整理

第一次聯盟會議滿意度



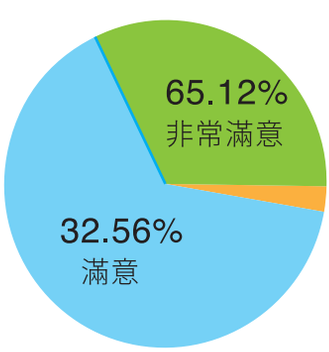
- 非常不滿意 0.00%
- 不滿意 0.00%

第二次聯盟會議滿意度



- 非常不滿意 0.00%
- 不滿意 0.00%
- 普通 0.00%

聯盟教育訓練滿意度



- 不滿意 2.33%
- 非常不滿意 0.00%
- 普通 0.00%

圖 4-5：與會者回饋問卷統計分析　　資料來源：TWCERT/CC 整理

第二節、國際交流

一、APNIC 50 線上論壇

亞太網路資訊中心（Asia-Pacific Network Information Centre，APNIC）主辦之 APNIC 論壇，爲結合全世界網路專家、政府代表、產業領導者、以及對資安議題有興趣之機構，進行當下資安議題探討與分享。

APNIC 50 論壇於 2020 年 9 月 9 日舉辦，今年因疫情影響改以線上論壇的方式進行。TWCERT/CC 參與本次 APNIC 50 論壇，並於 Security 2 場次中針對全球疫情與資安樣態進行探討與案例分享。報告內容包括駭客組織廣泛利用疫情所引起之恐懼、好奇心理進行多樣化的社交工程攻擊，例如提供疫情救濟金或威脅曾接觸過確診者，必須下載帶有惡意的檔案等，藉著疫情的嚴峻提升駭侵行爲成功率。其中也分享本年度發生於台灣的資安案例，供各國參考，希望藉著相關資訊的分享，提升國際間的警戒，避免因同樣的攻擊手法持續出現受害者。

本次 APNIC 50 論壇線上會議，TWCERT/CC 準備了台灣遭遇之 COVID-19 相關資安事件案例與成員分享討論，獲得 APNIC 與媒體的青睞，國外媒體爭相報導[1&2]。可見扣緊時事相關的資安議題是具有媒體能見度的，也能協助 TWCERT/CC 提升國際知名度。

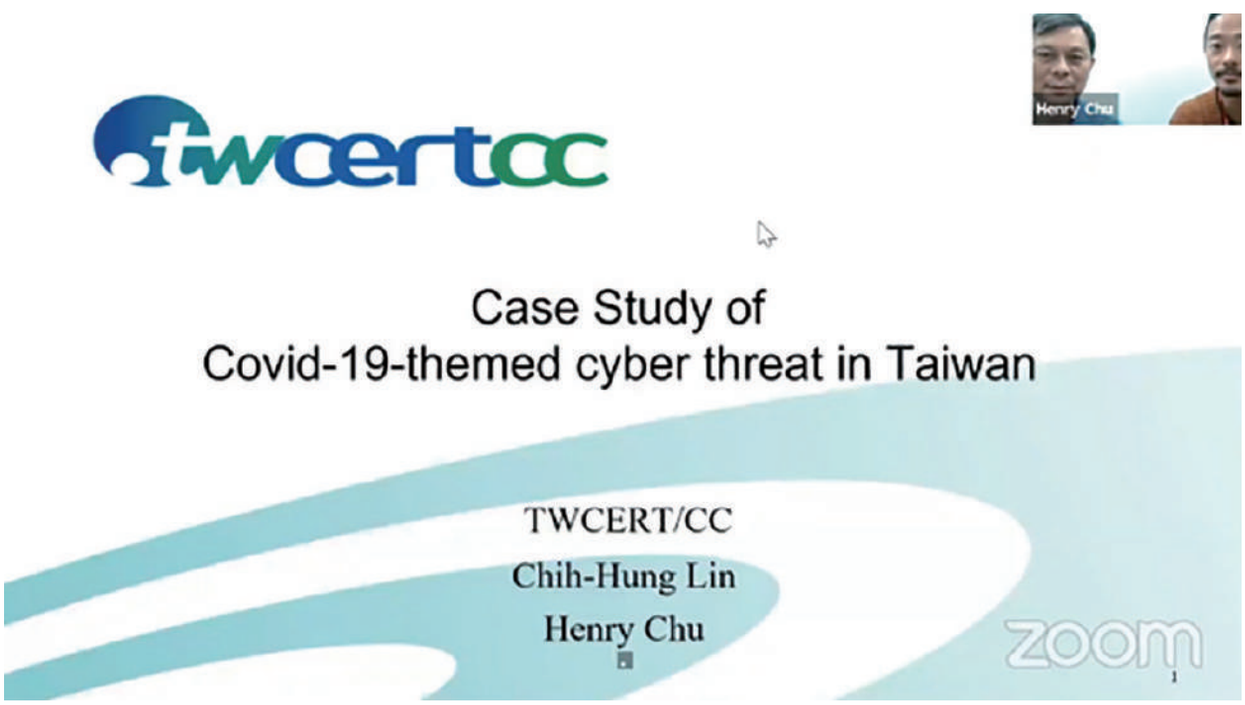


圖 4- 6：TWCERT/CC 林志鴻組長和曲承則工程師線上分享實況　　資料來源：TWCERT/CC 整理

1 APNIC. “How COVID-19 changed the cyber threat landscape in Taiwan”. Retrieved January 15, 2021, from the World Wide Web: https://blog.apnic.net/2020/09/16/how-covid-19-changed-the-cyber-threat-landscape-in-taiwan/

2 Theergister. “Fake Zoom alerts and dodgy medical freebies among COVID-cracks detected by Taiwan's CERT”. Retrieved January 15, 2021, from the World Wide Web: https://www.theregister.com/2020/09/17/taiwans_cert_analsyes_covid_hacks/

二、APCERT 年會

亞太區電腦網路緊急應變處理小組 (Asia Pacific Computer Emergency Response Team, APCERT) 每年定期舉辦一次全體性之年會 APCERT Annual Conference，是亞太地區相關資安組織 CERT 單位彼此交流討論的資安盛會，目的在於協同合作建立一個安全、乾淨且可靠的網路環境。本年度 APCERT Annual Conference 於 2020 年 9 月 29 日舉辦，本屆由斯里蘭卡 CERT 主辦，也因疫情關係，改透過 Webex 進行線上討論與交流。會議內容主要爲 APCERT 各個工作小組的運作討論、明年規劃，以及交流分享各會員國近期資安狀態。

圖 4- 7：APCERT 年會與會者線上合影　　資料來源：TWCERT/CC 整理

APCERT 組織中，爲了維護一個乾淨、安全且可信任的網路空間，成立了諸多不同主題之工作小組 (Working Group)，包含清除網路威脅、教育訓練、情資分享及網路攻防演練等，希望藉此爲多個經濟體的資通訊安全提供更好的防護。TWCERT/CC 亦參與其中多個工作小組，包含進行國際網路安全攻防演練的 Drill Working Group。

APCERT 除了每年固定舉辦之年會外，Drill 工作小組也會每年固定舉辦資安通報演練。本年度的演練於 3 月 11 日舉行，由澳大利亞 AusCERT 主辦，共有來自 APCERT 亞太經濟體、伊斯蘭合作組織電腦網路緊急應變處理小組 (OIC-CERT)，以及非洲電腦網路緊急應變處理小組 (Africa CERT)，總計 33 個團隊參與。此次演練，TWCERT/CC 有三名成員分別擔任 Player 以及 Observer 之角色[3]。

本次演練主題爲「Banker doubles down on Miner」，是依據眞實存在的資安事件進行編修及調整之主題。此主題中，參與團隊需協助一間企業，處理因數據洩漏而導致企

業受到惡意軟體感染的資安事件。演練共分八個階段，由參與者小組與國內、國際的電腦網路緊急應變處理小組 (CSIRTs/CERTs)，以及受影響的機構，演練資安事件的處理與協調，包括通知相關單位及要求使用者停止使用受影響的設備、分析惡意程式碼，以及聯繫並協處受影響之機構，方能全方位地解決問題。最終，此次活動共有 9 個團隊順利於時間內完成所有的任務，TWCERT/CC 即爲其中之一。

參與 APCERT Cyber Drill 網路安全攻防演練，目的在於累積 TWCERT/CC 成員的資安協處經驗，並將參與演練時所遇到的問題、想法，回饋至 TWCERT/CC 組織資安事件通報協處流程，進而提升整個協處流程的品質與效率。同時 TWCERT/CC 也期許未來能帶領台灣的企業內部資安團隊，一起進行相關的資安演練，培養我國企業的資安事件應變能力，提升整體環境的資安防護。

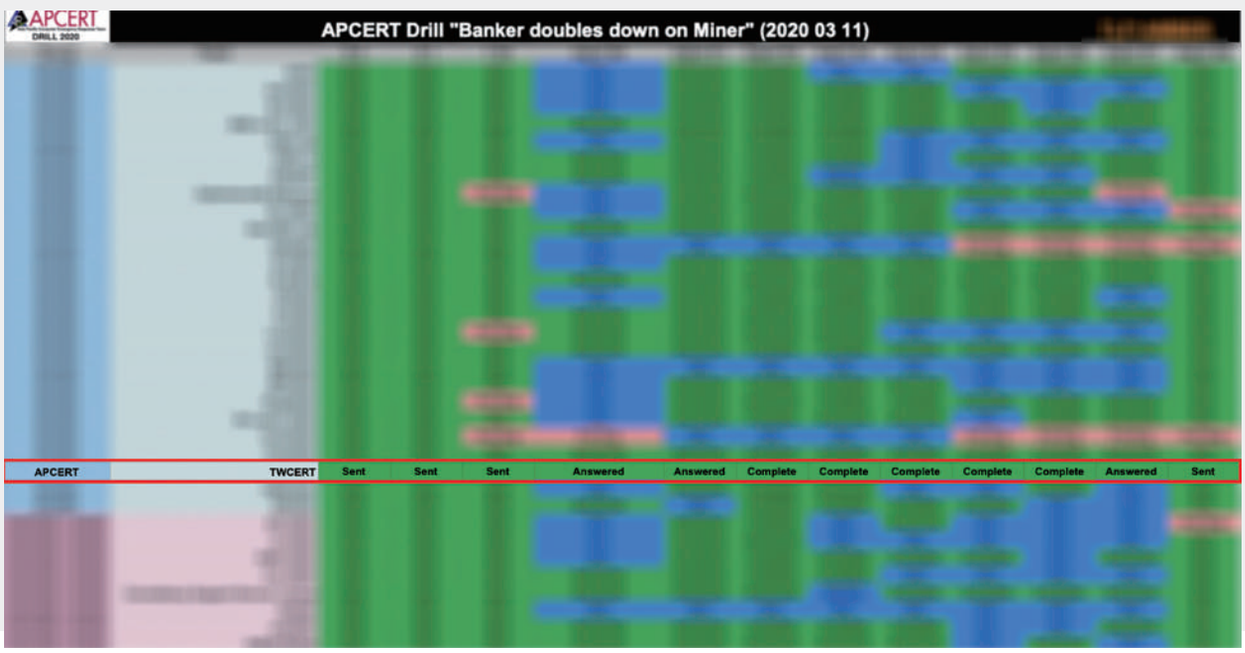


圖 4- 8：TWCERT/CC 於 APCERT Cyber Drill 活動成果　　資料來源：TWCERT/CC 整理

三、FIRST 2020 年會

國際資安事件應變小組論壇 (The Forum of Incident Response and Security Teams, FIRST) 之 2020 年會，也因疫情影響取消六月份的實體會議，改於 2020 年 11 月 16 日至 18 日舉辦線上會議。

FIRST 爲國際非營利組織，致力於促進全球各資訊安全應變小組及各領域資安人員之間的合作與技術交流。探討議題包括資安政策、技術工具、通報應變流程處理等。本年度之會議內容，包含建置威脅情資分享平台之經驗學習、透過 AI 偵測資安威脅之機敏資料與個資考量、以及區域性通報應變處理小組經驗分享與全球聯防等議題。

3 AusCERT. “AusCERT and the APCERT CYBER DRILL 2020”. Retrieved January 20, 2021, from the World Wide Web: https://www.auscert.org.au/blog/2020-03-12-auscert-and-apcert-cyber-drill-2020

本次會議主要爲了解 FIRST 國際組織之資安發展趨勢與現況，包含國際間針對通報應變所採取之政策措施、個資與機敏資訊濫用、及威脅情資平台分享相關之技術等，皆與 TWCERT/CC 之業務關連。藉參加此會議提升國際聯防與 TWCERT/CC 資安通報之分析與處理能量。

圖 4- 9：參與 First 2020 online Conference 相關畫面　　資料來源：TWCERT/CC 整理

第三節、國內交流

一、TWCERT/CC 資安服務宣導

在 2020 年期間，TWCERT/CC 參與了諸多國內資安相關會議及活動，並於許多場次中進行演講分享。而每一參與之活動類型及對象不盡相同，其中，許多大型資安活動是開放給所有民眾及企業參與的，且涵蓋主題廣泛，通常不限於資安類型之主題，但這也是接觸各領域民眾的絕佳機會。因此，TWCERT/CC 亦受邀並於會中進行相關演講，希望藉此提升大眾資安防護意識。

首先，TWCERT/CC 參與由台灣數位安全聯盟主辦之國際資安大會 (InfoSec Taiwan)。此活動主要以資安相關產業別，進行六個分軌議程，進行全方位產業應用之資安議題探討。

TWCERT/CC 以協辦角色參與活動，並於防禦與偵測主題系列議程中，進行「掌握情資 超前應處資安威脅」專題演講，透過資安資訊的統計分析，和與會者分享如何運用資安情資進行資安威脅防禦，並再次強調資安通報交流情資的重要性，藉此提升國內資安通報與情資交流之意願及比例，達成攜手增進國內整體資安防護能量之目標。

圖 4- 10：TWCERT/CC 於 2020 國際資安大會演講現況　　資料來源：TWCERT/CC 整理

除國際資安大會外，TWCERT/CC 也參與由資安人主辦的亞太資訊安全論壇 (Info Security 2020)，由丁綺萍副執行長於其中的高科技資安論壇系列議程中，進行「資安威脅防護暨應變復原」專題演講。此專題演講主要爲傳達資安事件通報應變與情資交流之重要性，希望藉此機會提升國內企業資安通報意願及比例，並與相關企業進行資安情資交流，以達到資安聯防之目的。

圖 4- 11：TWCERT/CC 於高科技製造資安論壇演講現況　　資料來源：TWCERT/CC 整理

圖 4- 12：台中資訊月 TWCERT 攤位

資料來源：TWCERT/CC 整理

TWCERT/CC 參與的另一開放予一般大眾的活動，爲於台中國際展覽館舉辦的 2020 台中資訊月。此活動以「數位催化 智連未來」爲主題，希望透過展出最新智慧科技及應用，成爲民眾學習最新科技的絕佳機會。但除了精彩的最新科技和應用外，資訊安全也是其中的一大重點，因此 TWCERT/CC 參與其中，並進行攤位擺設，藉由第一線面對面的宣導和溝通，藉此提升大眾資安防護意識，加強國內整體資安防護。

除了攤位擺設外，TWCERT/CC 亦於展覽館內會議室舉辦網路資訊安全論壇，透過演講將更多的資安訊息內容傳達予民眾，爲增進大眾資安知識與防護能量盡一份心力，達到雙贏互惠的良好合作成果。

二、TWCERT/CC 社群資安分享

TWCERT/CC 參與之活動眾多，除了面對一般大眾的活動外，亦參與特定社群的資安會議。這些會議往往是針對特定領域之資安相關議題進行演講交流。TWCERT/CC 受邀前往進行演講或交流，藉此提升各領域之資安意識與能量。

首先，TWCERT/CC 以協辦之角色，參與由數位鑑識協會主辦的 2020 Cyberspace 研討會活動。此活動今年以數位治理爲主題，邀請政府、企業界與學術界之專家先進，分享數位治理之相關議題與發展趨勢。

本次活動，TWCERT/CC 由林志鴻組長與會並參加「智慧城市與資安治理」專題論壇，與其他四位與談人談論關於我國智慧城市之資安議題。同時，林志鴻組長亦應邀於另一場次之資安綜合座談會上擔任與談人，談論我國於後疫情時代之數位戰略及資安治理，和與會者一同話資安、護台灣。

圖 4- 13：TWCERT/CC 參與智慧城市與資安治理專題論壇　　資料來源：TWCERT/CC 整理

WORKSHOP

此外，TWCERT/CC 參與由臺灣學術網路 (TANET) 舉辦之 2020 台灣網際網路研討會。此次研討會中，除了有智慧計算與資訊工程兩大領域相關優質學術論文的發表外，亦邀請專家學者進行專題演講和網路資安重要主題之 Workshop 分享。

TWCERT/CC 代表 TWNIC，由林志鴻組長於 Workshop 中進行「掌握資安情資，強化威脅應處」主題演講，分享當前資安威脅的嚴峻現況並說明資安事件通報、情資分享對於整體資安防禦的重要性，透過數據分析及相關實際案例，宣導並提升與會人員之通報意願。

圖 4- 14：TWCERT/CC 於 TANET 2020 台灣網際網路研討會演講現況

TANET

資安本身有諸多主題可以探討，例如上述之數位治理議題；此外，資安亦是眾多領域的組織或使用者都應了解並學習的，例如上述學術類型之活動，亦包涵資安議題之演講。因此，爲擴展資安宣導之主題與領域，TWCERT/CC 參與社交工程防護及案例分享研討會，希望藉此機會提升公益社會團體之資安知識與防護意識。

本次社交工程防護及案例分享研討會由 TWNIC 主辦，台中市電腦商業同業公會執行。活動中，除了邀請專業講師進行社交工程防護與案例之議題分享外，TWCERT/CC 亦於活動中介紹服務內容，希望公益社會團體可充分使用 TWCERT/CC 服務資訊，並藉此研討會提升公益社會團體人員資安意識，降低遭受駭客攻擊風險。本次活動根據問卷調查統計，研討會內容、講師專業度、場地滿意度以及整體表現等皆具高滿意度，未來還會積極舉辦相關資安活動，希望能藉此機會達成強化國內資安防護能量之目標。

圖 4- 15：TWCERT/CC 分享推廣資安服務　　資料來源：TWCERT/CC 整理

三、TWCERT/CC 企業資安研討

資安議題範圍相當廣泛，但就特定對象而言，卻又相當專精。因此，許多企業或組織會舉辦與其產業相關之資安活動，除了提升員工的一般資安知識外，同時亦可明確接收關於其產業的資安資訊，更精確地提升產業資安防護能量。而 TWCERT/CC 亦常受邀針對特定產業領域，進行演講或交流，藉此提升該產業成員及組織之資安意識與能量。

首先，TWCERT/CC 協辦並參與由 Digitimes 主辦之 2020 DForum 物聯網技術與應用論壇。此活動主要針對物聯網及智慧製造相關產業，爲了提升該產業之資安意識，TWCERT/CC 受邀於活動中進行「超前部署跨域資安聯防」專題演講，透過數據統計分析以及實際案例，傳達資安事件通報應變與情資交流之重要性，並藉此提升物聯網相關產業成員之資安意識及通報意願。

圖 4- 16：物聯網技術與應用論壇分享現況　　資料來源：TWCERT/CC 整理

除物聯網與智慧製造產業外，TWCERT/CC 也參與由社團法人安防產業協會舉辦之「後疫時代」系列座談會－決勝策略會議。此活動的目標群眾以安防設備製造商爲主，TWCERT/CC 受邀於此活動中進行服務範疇及案例專題演講。在此活動中，TWCERT/CC 透過專題演講與安防產業分享企業關注之資安案例，以及 TWCERT/CC 的服務範疇，傳達資安事件通報應變與情資交流之重要性，希望藉此活動提升國內安防產業相關之整體資安能量。

圖 4- 17：TWCERT/CC 分享推廣資安服務　　資料來源：TWCERT/CC 整理

除了物聯網、智慧製造及智慧安防產業外，貼近民衆生活且越來越普及的電子商務亦需嚴格的資安防範。因此，TWCERT/CC 以協辦之角色參與由 EC-CERT 舉辦之電商業者與資安專家溝通交流會議。此活動中，TWCERT/CC 進行「跨域資安聯防」專題演講，傳達資安事件通報應變與情資交流之重要性，尤其電子商務產業逐漸蓬勃的現在，更容易成爲資安攻擊目標，因此，希望透過專題演講與電商業者分享企業關注之資安案例，並推廣 TWCERT/CC 的服務範疇，提供更多相關資安防護資訊給電商業者，期能達成提升國內電商資安能量之目的。

圖 4- 18：ECCERT 電商資安座談分享現況　　資料來源：TWCERT/CC 整理

除了上述特定的產業之外，許多中小企業本身也需增加自身及其員工的資安意識。根據統計，有 35.7% 資安事件的觸發來源是企業內部員工，只要增添其員工資安知識，便可大幅減低企業資安破口問題。

TWCERT/CC 分別與桃園市中小企業協會、台南市中小企業協會、台北市中小企業協會，以及台中市電腦商業同業公會合作，於四個縣市各舉辦一場資訊安全防護及案例分享研討會。

首先，TWCERT/CC 與桃園市中小企業協會合作，進行資訊安全防護及案例分享，主要宣導對象爲桃竹苗地區之中小企業相關人員。活動中，主要介紹 TWCERT/CC 之資安服務內容及相關案例，除了提供與會者相關資安知識外，更讓其充分了解目前在資安事件協助上可運用的資源，以便中小企業在資安事件發生的第一時間，便能即時尋求並獲得協助，降低資安事件帶來的影響及威脅性。此外，爲提升與會者對於社交工程的資安防護意識，邀請安侯建業汪文淵資安顧問，進行一場社交工程資安講座，以提高中小企業員工之資安警覺，避免因社交工程攻擊造成企業損失。

圖 4- 19：桃園場研討會資安專題講座分享現況　　資料來源：TWCERT/CC 整理

第二場爲 TWCERT/CC 與台南市中小企業協會合作，舉辦資訊安全防護及案例分享研討會，主要宣導對象爲南部中小企業資訊人員。此次研討會議程內容分爲兩部分，第一部分，由 TWCERT/CC 介紹服務內容，提供與會者在資安事件協助上可運用的資源，一旦資安事件發生，便可利用此資源，將其受害程度降至最低。第二部分，特邀科諾資訊股份有限公司黃俊文創辦人，於活動中進行企業資安部署與效益研討分享，提升與會人員資安意識，提高資安警覺並超前部署，大幅降低資安攻擊所帶來的威脅。

圖 4- 20：台南場研討會資安專題講座分享現況　　資料來源：TWCERT/CC 整理

第三場次爲 TWCERT/CC 與台北市中小企業協會合作，舉辦資訊安全防護及案例分享研討會，主要宣導對象爲北北基地區的中小企業相關人員。此次研討會亦分爲兩部分，第一部分由 TWCERT/CC 介紹服務範疇與通報方式，提供與會者在資安事件通報和協處上可運用的資源，避免中小企業發生資安事件時無相關資源協助，導致受害企業蒙受嚴重損失。第二部分是特邀中華電信資安產品負責人吳明峰組長，在本次活動中進行社交工程實務分享，透過實際案例讓與會者對社交工程有更深的了解，並以此提升與會人員的資安防範意識，避免因缺乏防範而受騙上當，造成損失。

圖 4- 21：新北場研討會資安專題講座分享現況、圖 4- 22：台中場研討會資安專題講座分享現況

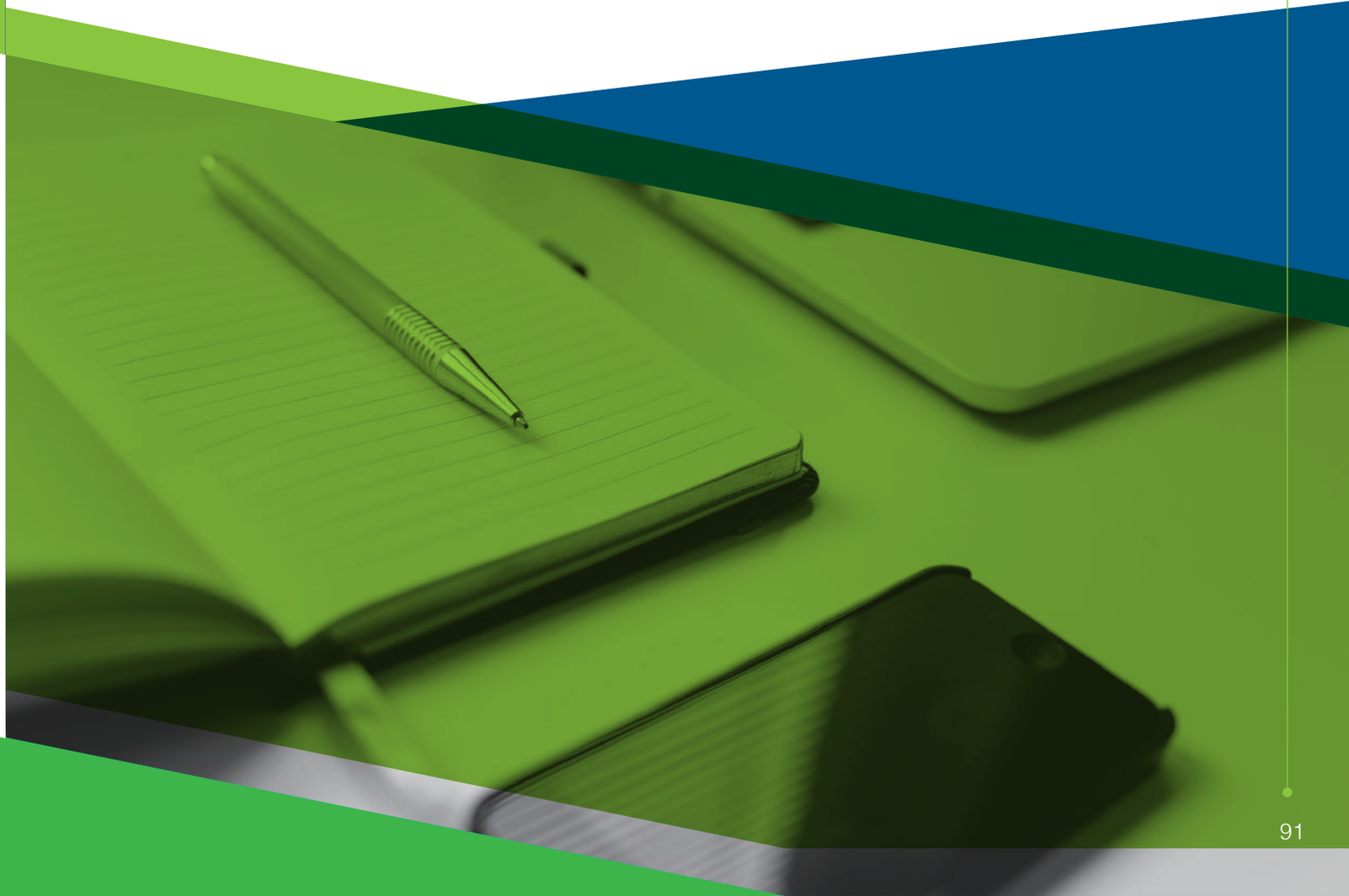
本年度最後一場次爲 TWCERT/CC 與台中市電腦商業同業公會合作，舉辦資訊安全防護及案例分享研討會。此次活動亦分爲兩部分，首先介紹 TWCERT/CC 之服務內容，希望企業能充分利用此一資源，推動企業資安事件通報、產品資安漏洞通報，以及惡意檔案檢測服務等，除了替中小企業增添更多的資安防護資源外，更可透過與會者及其單位的推動，讓更多人了解及使用這些服務，以此提升國內的資安防護能量。第二部分則爲邀請中華電信林經理探討「企業因應勒索軟體的資安策略」，針對越來越多的勒索要挾，應從源頭開始防範，透過強健的員工資訊安全培訓，企業可大幅降低員工爲惡意程式敞開大門的風險，以此提升企業整體資安防護能量。

資料來源：TWCERT/CC 整理

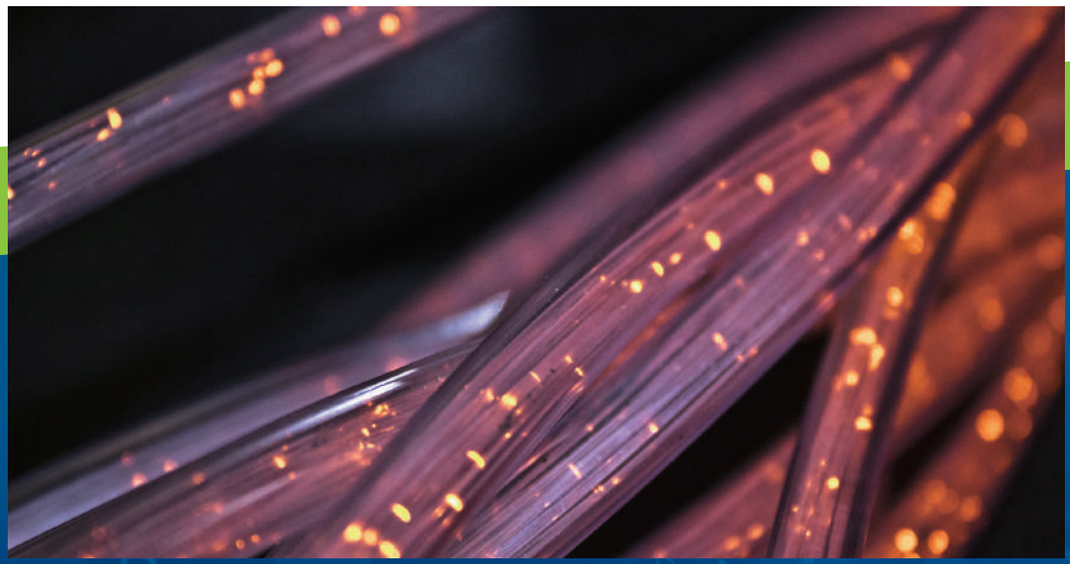
第五章、
結語

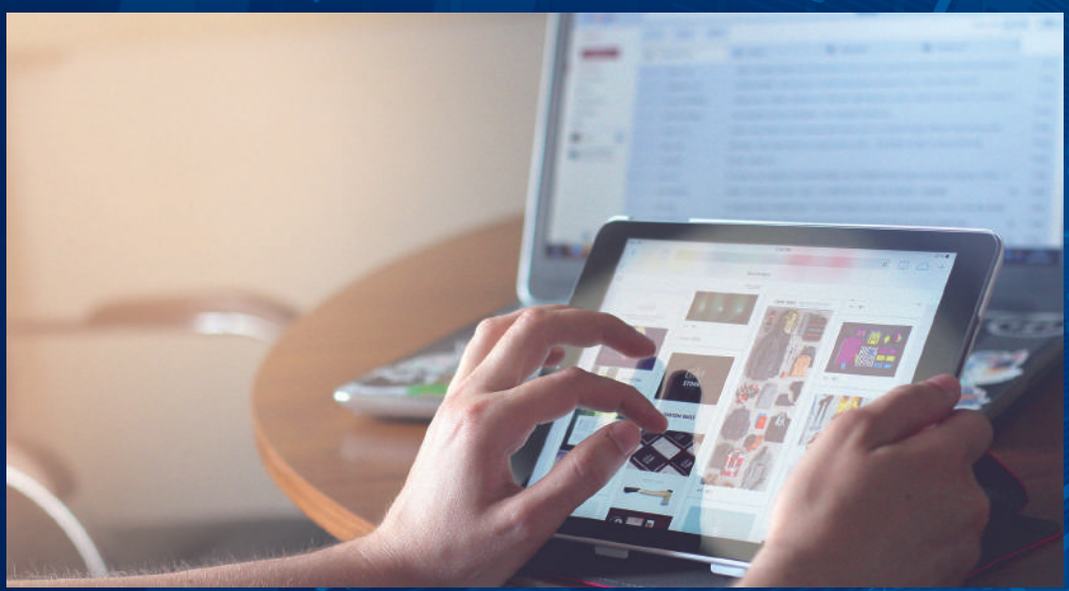
隨著網際網路及科技技術的蓬勃發展，除了增添生活中的便利性之外，相關的網路安全問題亦日益嚴重。尤其遠距工作逐漸成爲一種作業趨勢，不論是企業、組織、家庭或個人都可能是受駭目標，因此，提升大衆的資安意識、加強資通訊產品的安全性，以及資安事件的防範與處理，都是爲達成維護我國安全網路環境所必須之努力目標。

2020 年，全球不論是企業或民衆的生活，都產生了巨大的變化。隨著新冠疫情的發展，網際網路的使用比例和設備大量增加，雖然提供了諸多的便利性，卻同時也產生了許多資安問題。變化最爲明顯的是企業遠距辦公比例的大幅上升，而這些爲了維持企業營運的遠距辦公工具數量衆多，安全性卻參差不齊。因此除了確保遠距辦公工具本身具足夠安全性外，員工亦需維持網路良好使用習慣，以及充分的資安意識，才能達成全方位的遠距工作安全防護。除員工的工作模式外，企業近年來的生產及營運模式，逐漸以供應鏈形式爲主。但供應鏈中一旦有一廠商資安防護薄弱，除了易遭攻擊之外，更會對其供應鏈中的其他廠商及產品產生嚴重影響。因此，除需愼選合作廠商外，亦應要求供應鏈上的所有廠商均需遵守產業供應鏈資安相關法規，強化供應鏈的資安防護。工業 4.0 的出現也造成了企業極大的變化，從過往的 OT 到連接網路的 IT，使得攻擊者可透過網路進行攻擊。然而，許多仍以生產作業爲重的產業，尚未意識到這些潛在的資安威脅，或是還未能全面進行防禦，導致企業因此受到嚴重的駭侵攻擊。因此，國際半導體產業協會 (SEMI) 針對半導體業者提出一系列資安標準，希望能藉此提升半導體產業的資通訊安全，避免那些運用資通訊科技提升生產效率的智慧工廠，反而成爲被駭客攻擊的對象。



然而，資安問題並非僅因爲使用者及企業的改變而發生，某些新的規範或制度也會帶來新的資安威脅。隨著網際網路的普及與設備數量快速增加，IPv6 的發展就是一個例子。由於 IPv6 的施行時間尚短，導致許多新資安威脅在建制過程中逐漸浮出檯面。爲防範這些新興資安威脅，除了增添相關防護設備和機制外，在部署 IPv6 時亦需選擇具足夠安全性之設備及環境，如通過 IPv6 Ready Logo 標章之設備，以及參考我國 IPv6 相關發展計畫等，以增加 IPv6 之安全性。此外，域名濫用也是近期較爲嚴重的資安問題。隨著疫情愈發嚴峻，越來越多攻擊者透過註冊與疫情相關之域名，藉此取信於使用者。不論在國內或全球都層出不窮，與疫情相關字詞組合的域名註冊數量及濫用之比例大幅增加。因此，爲避免遭受詐騙，唯有維持良好的網路使用習慣，以及對可疑的訊息保持警惕，方能配合相關單位，完全阻絕域名濫用所帶來的威脅。隨著網路設備的大量增長，DDoS 攻擊也愈發常見，導致許多企業因此被迫中斷其服務。因此，爲了降低 DDoS 攻擊對企業及組織所帶來的威脅，越來越多的安全設備可以針對特定的 DDoS 進行流量識別與防範，甚至許多業者都推出了流量清洗服務，替企業隔絕惡意流量，達成我國企業通訊安全強化之目標。





在網際網路的發展之下，不論是聯繫或威脅都早已無國界之分。因此，身為我國企業資安事件通報協處及國際資安窗口，TWCERT/CC 主動積極擴大國際合作管道，並與企業、各資安組織和 CERT/CSIRT 組織進行資安情資交流，以利在資安全球化的同時，仍能攜手維護我國的資通訊安全。然而，在這些大量的資安事件中，雖然許多資安威脅的手法及類型往往隨著科技的變遷而改變，但仍有許多攻擊模式使用已久，如透過社交工程散播惡意程式等，是極為常見的攻擊手法。因此，為避免惡意檔案所帶來的威脅，惡意檔案檢測服務系統 Virus Check，透過結合靜態與動態檢測模式，提供使用者全方位的惡意檔案檢測，並且除了降低因惡意檔案的受害機率外，更可從這些惡意檔案中發現新型態之惡意程式，得以建立我國的惡意程式資料庫，達成更為精確且安全的惡意程式防護目標。除了惡意程式，資通訊產品之資安漏洞也是極大的威脅來源。TWCERT/CC 參與 MITRE 的 CVE 計畫，成為台灣區之 CNA，接收國內產品的資安漏洞情資，並作為通報者與廠商之間的協調角色，協助產品漏洞之確認及修補，在確認該漏洞修補完畢後，才會進行 CVE 編號之發放，讓更多產品相關的使用者或企業了解並配合進行緩解和修補，從而阻絕攻擊者欲利用資安漏洞進行惡意攻擊的威脅。

為了降低資安事件發生之機率，TWCERT/CC 已針對自身資訊產品的漏洞進行修補、防護，並對相關單位進行情資分享和通知；也透過 Virus Check 系統阻絕惡意程式透過社交工程攻擊的入侵。然而，在網際網路中的任何行為都取決於使用者，不論建立了多強的防護設備，或是提供了極佳的資安資源，都可能因使用者不願意使用而毫無用武之地。因此，要增進整體資安防護能量，使用者的資安意識提升是不可或缺的。TWCERT/CC 便透過多方管道進行資安宣導，以提升使用者的資安知識，包括按月發行的資安電子報，分享上百則國內外資安新聞，同時也透過如 Facebook、Instagram 及痞客邦等社群媒體提升其能見度，以便觸及更多的使用者。並且為了配合大環境之變化，亦於本年度提供諸多如遠距辦公資安小錦囊，以及翻譯分享美國國土安全部 (DHS) 網絡安全和基礎設施安全局 (CISA)，針對 COVID-19 網絡犯罪的威脅分析與建議等文章，以及如疫情相關之社交攻擊、口罩實名制詐騙簡訊、外送 APP 資安議題等宣導，以利大眾在經歷生活及工作模式改變的同時，仍能維持網際網路的安全。此外，為確保資安資訊的確實傳達，TWCERT/CC 參與諸多相關活動，透過面對面的現場演講及溝通，確保資訊安全防範意識的有效傳達。

在 2020 年期間，由於環境的重大變化，使得網際網路的運作及使用模式亦隨之改變，這些改變除了在疫情中帶來便利之外，卻也可能帶來相對應的資安威脅。尤其諸多的資安事件都是透過與疫情相關之議題或改變進行攻擊，導致許多使用者或企業措手不及而受害。因此，提升我國整體資安意識及資安防護能量之作業已刻不容緩，TWCERT/CC 積極進行資安宣導、情資分享、國際交流，以及針對產品、系統甚至企業及組織的資安防護，也希望不論是使用者或企業都協助配合，透過彼此之間的攜手合作，方能達成維護我國乾淨、安全的網際網路環境之願景。

資通安全年報 2020

Information Security Annual Report

出版者：財團法人台灣網路資訊中心

書名：2020 資通安全年報

主編：台灣電腦網路危機處理暨協調中心

指導單位：國家通訊傳播委員會

地址：105412 台北市松山區八德路四段 123 號 3 樓

電話：(02)2528-6786

版次：初版

出版日期：2021 年 4 月

定價：新台幣 1,000 元整

ISBN ：

根 植 臺 灣 • 展 望 世 界

台灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Team / Coordination Center

105台北市松山區八德路四段123號3樓

3F., No. 123, Sec. 4, Bade Rd., Songshan Dist., Taipei City 105035, Taiwan (R.O.C.)

https://www.twcert.org.tw/tw　T +886-2-2528-6768

ISBN 978-986-992-391-0