# 107年第3季資通安全技術報告

Quarterly Technical Report

# 目　次

摘要 ..... i
第一章 資安威脅現況與防護重點 ..... 1
1.1 全球資安威脅現況 ..... 1
1.2 政府資安威脅現況 ..... 2
1.3 資安防護重點 ..... 5
第二章 資安專題分享 ..... 8
2.1 GDPR 概要與重點摘錄 ..... 8
2.2 GDPR 因應重點與自我檢核 ..... 11
第三章 資安新興議題研討 ..... 14
3.1 機器學習 HTTPS 加密流量分析 ..... 14
3.2 Android Root Bridge 漏洞利用 ..... 20
3.3 利用可變動資料串流(ADS)之進階持續威脅(APT)攻擊 ..... 23
第四章 結論 ..... 26
資安相關活動 ..... 27
公務人員資安職能訓練 ..... 27
安全系統發展生命週期(SSDLC)訓練研習 ..... 27
資安系列競賽 ..... 28
參考文獻 ..... 29

# 圖 目 次

圖 1　107 年第 3 季資安事件影響等級比率圖 ..... 3
圖 2　107 年第 3 季資安事件通報類型比率圖 ..... 4
圖 3　107 年第 3 季資安事件原因比率圖 ..... 5
圖 4　GDPR 章節 ..... 10
圖 5　惡意程式由 HTTP 轉移至 HTTPS 之趨勢 ..... 14
圖 6　類神經網路結構 ..... 16
圖 7　利用支持向量機建立分類邊界 ..... 16
圖 8　決策樹樹狀結構 ..... 17
圖 9　Entropy 值對決策樹分割節點的影響 ..... 17
圖 10　利用隨機森林判斷惡意流量示意圖 ..... 18
圖 11　利用學習曲線評估分類模型 ..... 19
圖 12　執行挖礦與企圖擴散的惡意程式樣本 ..... 21
圖 13　網路搜尋存在漏洞之聯網裝置 ..... 22
圖 14　駭侵手法說明 ..... 23
圖 15　使用 dir 指令檢視目錄與檔案大小 ..... 24
圖 16　壓縮檔內含 5 個行為相同之捷徑檔 ..... 25
圖 17　使用 dir /r 指令以檢視 ADS 檔案 ..... 25

# 表 目 次

表 1　GDPR 自我檢核表 ..... 12

# 摘要

世界經濟論壇(World Economic Forum, WEF)「全球風險報告」指出，無論是從網路安全風險發展現況或是相關潛在破壞力方面，本(107)年網路安全風險持續擴增，相關風險無所不在，如何掌握威脅發展趨勢，加強資安防護仍需持續。「第 3 季資通安全技術報告」除分析本季全球資安威脅、政府通報之資安事件外，並提供相對應之防範建議。同時，藉由資安專題之分享與精選資安新興議題之研討，提供政府機關(構)於資安風險的關注重點。

「第 3 季資通安全技術報告」分為以下 4 個章節。

●第 1 章：資安威脅現況與防護重點

從分析全球資安威脅現況開始，首先探討「資安(訊)供應商持續遭駭破壞供應鏈安全」相關案例，本年 8 月發生於科技公司之病毒感染事件，因為人為操作疏忽，協力廠商或內部操作人員在新機台安裝軟體過程時，並未依照 SOP 先進行防毒軟體的安裝與掃描，導致感染想哭(WannaCry)變種病毒。

另一起案例為 Timehop 遭駭，導致上千萬名用戶個資外洩，此為遭駭客鎖定的「進階持續威脅攻擊竊取機密資料」事件。Timehop 從去(106)年遭駭客使用具有管理員權限的員工帳密，登入其雲端供應商網路後，建立新的管理員帳戶，在本年被駭客入侵後，導致上千萬名用戶個資外洩，而且駭客也取得用戶存取臉書、推特及 IG (Instagram)等社交網站內容的憑證。

分析政府資安威脅現況可以發現通報之資安事件發生的主因，大部分為網站設計不當(占 24.34%)、應用程式漏洞(占 13.49%)及弱密碼(占 10.26%)等弱點。

●第 2 章：資安專題分享

歐盟 GDPR (General Data Protection Regulation)個資保護法規從本年起開始實施，其目的與主旨為規範個人資料處理與資料自由流通，保護個人基本權與自由，尤其是保護個人資料之權利。

我國已訂定「個人資料保護法」，惟 GDPR 的適用範圍因為網路世界資料無遠弗屆的特性，法規之適用性也變得沒有邊界與地域的限制。此次資安專題分享將說明 GDPR 相關規定，並從法規適用之範圍、相關定義、治理及技術面研析相關重點，最後整理相關檢核表，提供確認其法規遵循性之參考。

●第 3 章：資安新興議題研討

本季整理之資安新興議題，包括 3 大主題。

第 1 個資安新興議題為機器學習 HTTPS 加密流量分析，為確保資料加密之完整性且又能防堵惡意攻擊行為，機器學習技術逐漸被投入用來識別加密網路流量中的資安威脅，為建立最適合的分類模型，會藉由選擇不同的機器學習演算法，搭配所利用的特徵進行訓練，以判斷 HTTPS 連線是否存有惡意程式。分析 HTTPS 加密流量最常見的 4 種演算法，分別為類神經網路、支持向量機、決策樹及隨機森林。

第 2 個資安新興議題為 Android Root Bridge 漏洞利用，駭客利用 Root Bridge 漏洞入侵受害裝置後，即可在受害裝置上安裝惡意應用程式套件(APK)，使得受害裝置除了進行挖礦作業外，還會掃描網路上其他 ADB (Android Debug Bridge)裝置(連結埠 5555)，企圖擴散感染，受害裝置被植入負責執行挖礦與企圖擴散的惡意程式。

第 3 個資安新興議題為利用可變動資料串流(Alternate Data Streams, ADS)之進階持續威脅(APT)攻擊，此新興的攻擊手法，駭客結合社交工程郵

件、惡意捷徑檔及 ADS 等攻擊手法，進行進階持續威脅攻擊，此種縝密的攻擊手法除難以追縱外，更大幅提升案件分析的困難度。

- 第 4 章：結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅現況與因應之防護重點。同時，藉由簡介 GDPR 之相關規定、適用對象及因應重點，協助適用單位進行自我檢核。此外，透過 3 個資安新興議題的研討，深入探討技術主題、駭客攻擊手法及資安風險。在掌握本季之資安威脅現況時，亦說明下一季之資安專題重點。

# 第一章 資安威脅現況與防護重點

本報告藉由當季國內外所發生之重大資安事件與統計數據，研析主要發生原因與可能之衝擊與後果。透過本季的事件研析，在事件發生時，如何防止災害持續擴散與蔓延，為當下最需面對之事，如何快速且正確地應變與面對事件，則需仰賴事前的應變程序與演練。最後，本報告整理相關防護重點，提供組織相關資安風險或議題討論，並可依循防護重點規劃執行細節。

## 1.1 全球資安威脅現況

藉由統計與分析近年來全球資安事件，可將全球資安威脅趨勢歸納為「進階持續威脅攻擊竊取機密資料」、「分散式阻斷服務攻擊癱瘓網路運作」、「物聯網設備資安弱點威脅升高」、「關鍵資訊基礎設施資安風險倍增」、「網路與經濟罪犯影響電子商務與金融運作」及「資安(訊)供應商持續遭駭破壞供應鏈安全」等 6 大面向。政府機關(構)在面對這些類型的資安威脅時，應分析自身業務特性，了解可能遭遇之風險，即早提出應對之防範措施。

首先探討「資安(訊)供應商持續遭駭破壞供應鏈安全」面向之資安案例，本年 8 月國內的科技公司發生病毒感染事件，事件發生之原因，在於協力廠商或內部操作人員在新機台安裝軟體過程，並未依照 SOP 先進行防毒軟體的安裝與掃描，導致感染想哭(WannaCry)變種病毒；同時亦因新機台串連公司內部電腦網路，且相關作業系統又未全面更新，因而導致災情擴散。預估這次的機台中毒事件，將對該公司第 3 季營收造成重大衝擊。

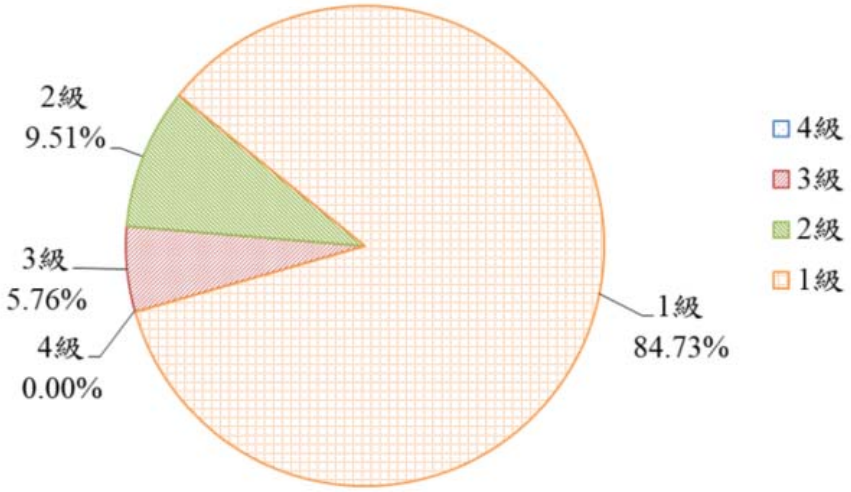
第二起案例為 Timehop 遭駭導致上千萬名用戶個資外洩，此為遭駭客鎖定的「進階持續威脅攻擊竊取機密資料」事件。Timehop 為提供臉書(Facebook)及推特(Twitter)過去貼文回顧的應用程式公司，本年 7 月 8 日在其官方網站公告，該公司於 7 月 4 日遭駭客入侵，導致 2,100 萬名用戶個

資外洩，而且駭客也曾取得用戶存取臉書、推特及 IG (Instagram)等社交網站內容的憑證。根據 Timehop 公布的內容，去年 12 月 19 日一名駭客使用具有管理員權限的員工帳密，登入其雲端供應商網路後，建立新的管理員帳戶。接著駭客接連在去年 12 月、本年 3 月及 6 月先後登入其雲端服務進行環境偵查。隨後在本年 7 月 4 日當天開始攻擊 Timehop 的主要資料庫並對外傳輸資料，從下午 2 點 43 分駭客觸動警報後，Timehop 人員花費 2 個小時才恢復正常服務。

總覽本季重大資安事件，主要的資安威脅以「資安(訊)供應商持續遭駭破壞供應鏈安全」與「進階持續威脅攻擊竊取機密資料」為主。資安(訊)供應商因為是組織的工作夥伴，彼此具有合作協同關係，已建立相當的信任度基礎，惟常常在很多便宜行事的狀況下，造成不可彌補的損失。而在進階持續性威脅攻擊方面，竊取機密資料向來都是駭客的主要目的，組織在評估自身風險時，對於駭客而言，有其利益、政治或軍事上之價值者，都應規劃與部署相對應的防護措施。

## 1.2 政府資安威脅現況

彙整本季所接獲之政府機關(構)通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關(構)之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。經彙整事件影響等級，第 3 季以 1 級事件占 84.73%為大宗，2 級事件占 9.51%次之，3 級事件則占 5.76%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

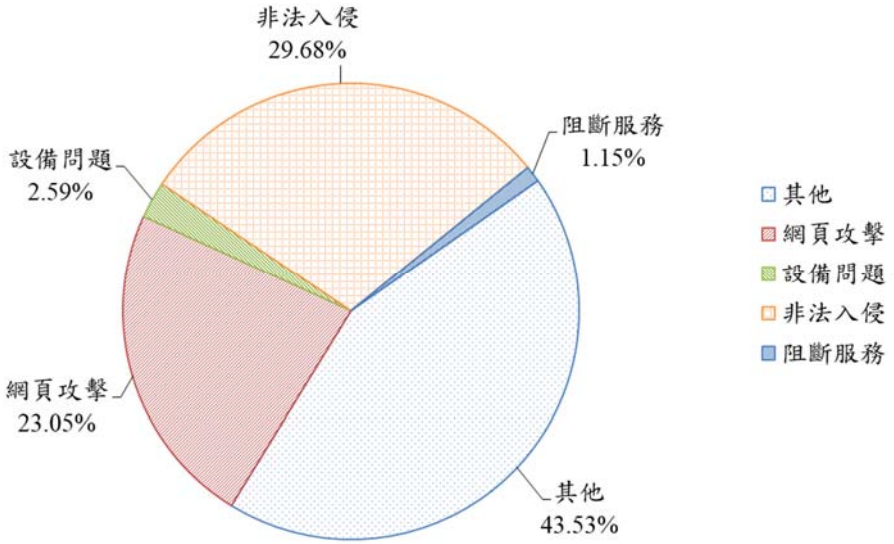



資料來源：本報告整理

圖1　107 年第 3 季資安事件影響等級比率圖

本季通報應變網站所接獲之資安事件通報，因進行網路攻防演練關係，其中將近八成是為攻防演練所通報之事件。資安事件發生原因，針對所通報之事件進行分析，發現部分政府機關網站或系統年代久遠，未確實掌握確切使用狀況，包括疏於定期維護或已經不再使用但又未下架，而遭駭客入侵；亦發生部分政府機關網站使用第三方元件，卻未即時更新安全性漏洞，而遭入侵上傳惡意程式。建議政府機關(構)應定期盤點資訊設備及系統之使用狀況，即時修補漏洞以降低資安風險。

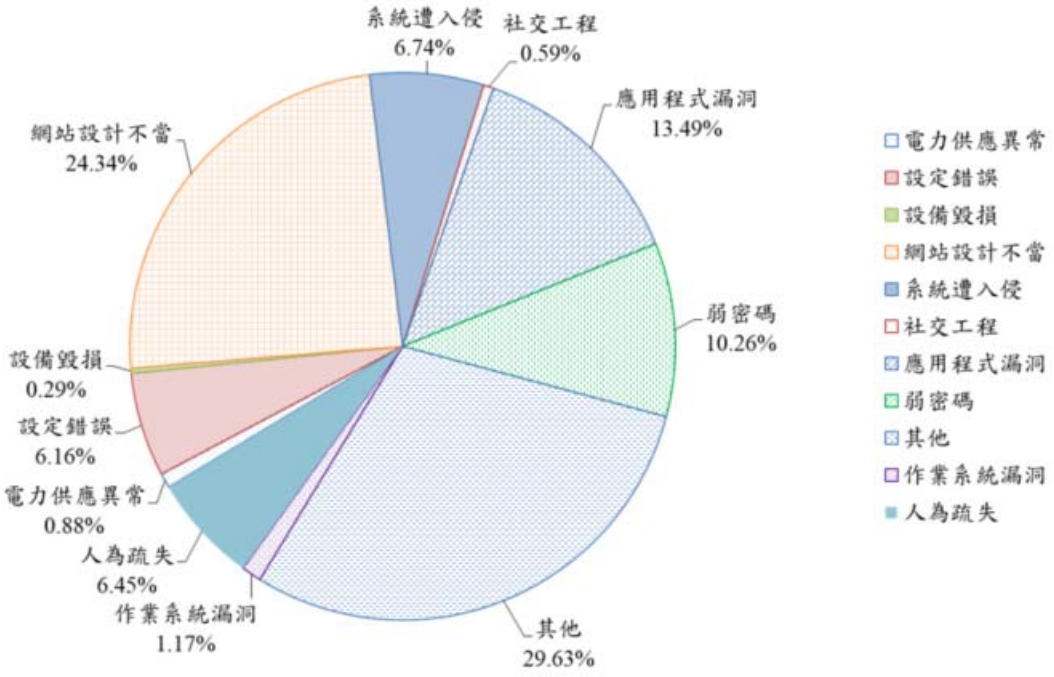
此外，資安事件通報類型依其發現之異常情形，分為網頁攻擊、設備問題、非法入侵、阻斷服務及其他，統計第 3 季資安事件通報類型(詳見圖2)，主要以「其他」占 43.53%為大宗，此類型為網路攻防演練遭攻擊成功所通報事件，由於攻防演練事件非屬實際發生之資安事件，故通報類型判定為「其他」。




資料來源：本報告整理

圖2　107 年第 3 季資安事件通報類型比率圖

最後，分析通報事件發生的原因，除網路攻防演練事件外，網站設計不當(占 24.34%)、應用程式漏洞(占 13.49%)及弱密碼(占 10.26%)為主，詳見圖 3。「網站設計不當」可能造成的後果，常常會導致網站無法正常運作，嚴重者亦可透過網站之管理權限，取得後台與相關連線之網路資源。而「應用程式漏洞」部分，不論應用程式為商用或客製開發，在上線前都應先執行程式弱點或漏洞檢測，以確保應用程式之安全。在「弱密碼」部分，相較於第 2 季的 15.57%，通報事件之比例已有下降趨勢，顯見政府在推動「資訊系統分級與資安防護基準作業規定」及「政府組態防護基準(Government Configuration Baseline, GCB)」已有一定之成效。




資料來源：本報告整理

圖3　107 年第 3 季資安事件原因比率圖

## 1.3 資安防護重點

分析本季全球資安威脅現況，組織被入侵的管道呈現多元化，一旦在資安環節有所疏漏時，特別是信任的委外供應商，造成的損害與後續的影響常常是無法估計的。另一方面，駭客入侵目之的，除透過攻擊行動可以帶來的獲利外，竊取大量個人資料與機密資料，仍是首要目標。被駭客虎視眈眈而目標式鎖定地的組織，應完善規劃資安事件通報與應變機制，以即早偵測發現並減緩損害擴大。

以此次國內的科技公司發生病毒感染事件為例，主要原因在於供應商提供的新機台本身就已感染想哭變種病毒，所以在科技公司檢討有無依照 SOP 操作之前，應先檢視與供應商之合約是否有相關之資安條款，確認已要求委外供應商所交付之設備或服務都無安全疑慮。SOP 絕對不是單一程序之

管理作業，就如此次案例，若在某一環節有落實資安作業，都不致讓此次事件造成如此嚴重後果。因此，在資安事件發生後，除進行根因分析外，亦應檢視整體之資安管理程序，設定資安檢核點。此外，針對社群網路眾多個人資料聚集的企業，如何從縱深防禦角度進行資安防護，且規劃資安方案與計畫。藉由 Timehop 個資外洩事件，可以看出具管理員權限者屬於特殊帳號權限，更應加強監督與管理，除平時應定期檢視相關管理員權限存在之必要性，並檢視其活動日誌是否有異常。同時，為了加強帳號登入之授權與識別，亦可採取雙因子驗證方式驗證。因駭客曾取得其他社交網站內容之憑證，更新密碼與金鑰亦是當下應立即進行之事，後續更需啟動客戶個資外洩之通報與應變程序。

另一方面，雖然政府機關(構)通報的資安事件以影響程度較低的「1 級」事件為主，惟分析事件的發生原因後，仍需注意「網站設計不當」及「應用程式漏洞」等所造成的資安風險。綜整以上資安威脅現況，提供資安防護重點建議如下：

●資安標準作業程序之防護

– 資安管理程序除需文件化外，應定期測試與檢視其落實程度。

– 建立資安事件之通報應變程序，包括事件分級應變與對外公開發言事宜。

– 檢視委外廠商之合約，並訂定工作事項檢核表，以定期稽核其執行狀況。

●社群網路安全之防護

– 訂定個人資料保護策略，規劃個人資料生命週期之保護程序。

– 定期檢視網站管理員之帳號，汰除閒置帳號，並檢視留存帳號之活動日誌。

– 資料庫後台應採取加密等防護機制，並檢視相關存取權限。

●網站設計不當與應用程式漏洞之防範

– 導入安全資訊系統發展生命週期(Secure Software Development Life Cycle, SSDLC)，確保程式開發流程遵循每一階段之資安要求。

– 上線前檢測是否有任何後門與漏洞；正式運作時，定期執行系統弱點掃描與漏洞修補。

– 檢視與委外廠商之合約，是否包括資安條款與要求，並定期監督與管理。

# 第二章 資安專題分享

歐盟一般資料保護規範(General Data Protection Regulation，以下簡稱GDPR)，於本年 5 月 25 日開始實施。GDPR 開宗明義敘及立法之目的與主旨為規範個人資料處理與資料自由流通，保護個人基本權與自由，尤其是保護個人資料之權利。另一方面，亦提到個人資料於歐盟境內之自由流通，不得以保護個人資料處理理由限制或禁止。

基於保護個人資料處理，但又需要資料自由流通的情況下，如何在隱私保護衝擊分析後，明確訂定組織管理階層與管理人員之責任，並規範相關保護措施，為 GDPR 法規遵循須逐一檢視之重點。本季的資安專題分享參考國家發展委員會之歐盟一般資料保護規則專區相關資料[1]，說明 GDPR 相關規定，並從法規適用之範圍、相關定義、治理及技術面研析相關重點，最後整理相關檢核表，提供組織確認其法規遵循性之參考。

## 2.1 GDPR 概要與重點摘錄

GDPR 號稱是史上最嚴格的個資保護法規，最主要原因是因為其所適用與涵蓋範圍，GDPR 雖然是適用歐盟的民眾，但因為網路世界資料無遠弗屆的特性，法規之適用性也變得沒有邊界與地域的限制，再加上對個人資料的定義包含虛擬的網路識別及其高額之違反法規的罰則，都使得組織在GDPR 的法規遵循更須戒慎恐懼。國內已訂定「個人資料保護法」，以下將就「個人資料保護法」與 GDPR 進行比較，主要用意在於若組織已符合個資法，可以再參考 GDPR 之管理重點，以持續加強個人隱私或資料之保護。本報告整理主要的差異點說明如下：

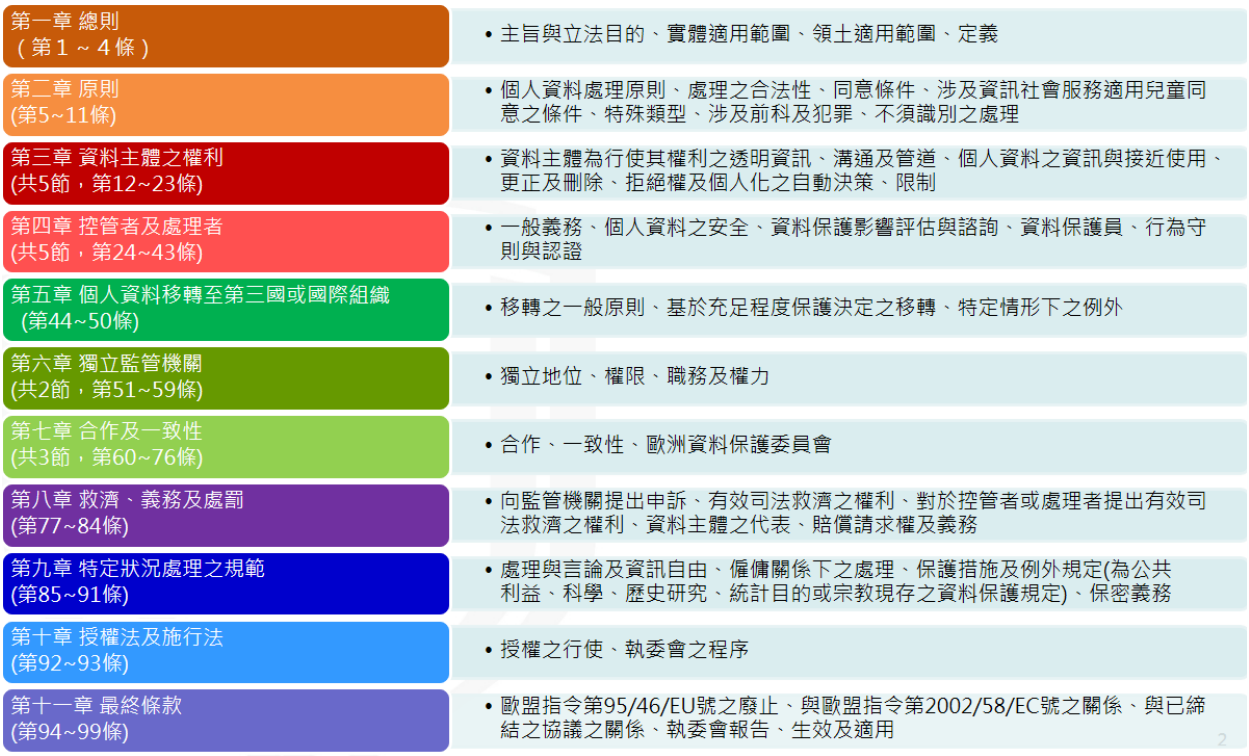
- 個人資料的定義廣泛：GDPR 之一般個人資料提及「網路識別碼」，透過網路識別碼，如 IP 位址所產生之數位軌跡，若得以識別特定當事人，則皆列為個人資料；另外，特別(種)個資亦新增種族或人種、政治意見、宗教、哲學信仰或貿易聯盟會員之個人資料等，皆是我國個資法比較沒

有述及之部分。

- 當事人權利新增：GDPR 新增個資可攜權、強調拒絕權及個人化之自動決策，如組織以「建檔」形式對個人資料任何形式之自動化處理，包括使用個人資料來評估與該當事人有關之個人特徵，特別是用來分析或預測當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵，以法規遵循性而言，在未徵得當事人同意的情況下，都有違反法規的疑慮。

- 組織治理責任：GDPR 需要進行資料保護影響評估，分析個資保護之風險與衝擊，評估現行組織對資料保護之狀況；另外在權責部分亦應設立個資保護員，主責個資保護之相關管理與聯絡事宜。組織之治理責任的另一個重點是隱私保護之設計(privacy by design)及預設(privacy by default)，隱私保護之設計與預設，要求組織在不論任何業務、技術及運作的整個流程都應有隱私保護的設計，且不逾越當事人的預設同意與應用範圍。

GDPR 共有 11 章(詳見圖 4)，以組織之觀點整理，GDPR 法規的核心領域共 3 項，分別為隱私權(亦即當事人權利)、資料安全與控制及治理。因此以下將概述第 1~4 章之重點，以協助組織快速了解 GDPR 之管理方案。




資料來源：本報告整理

圖4　GDPR 章節

第一章(總則)：說明實體適用範圍包括全部或部分以自動化方式處理之個人資料；領土適用範圍包括控管者或處理者在歐盟境內之分支機構所為之個人資料處理活動，若設立於歐盟境外，但對歐盟境內之資料主體提供商品或服務。

第二章(原則)：說明個人資料處理原則，如合法性、公正性、透明度、資料最少蒐集、儲存限制、完整性及保密性等處理原則，以及個資當事人之同意條件。另外，涉及兒童、特種個資、前科及犯罪等處理原則。

第三章(資料主體，意指當事人之權利)：說明當事人欲行使其權利所需之透明資訊、溝通及管道，蒐集當事人之個人資料時所提供之資訊，尚未自資料主體取得個人資料時所應提供之資訊，個人資料之資訊與存取、更正及刪除(被遺忘權)、限制處理、資料可攜性、拒絕權及個人化之自動決策

等權利。

第四章(控管者及處理者)：說明控管者(controller)之責任、設計及預設之資料保護、共同控管者、處理者(processor)、處理活動之紀錄；個人資料之安全、向監管機關進行個人資料侵害之通報、向當事人為個人資料侵害之溝通、資料保護影響評估；資料保護員(data protection officer)之指定、資料保護員之職位與職務；行為守則與認證。

## 2.2 GDPR 因應重點與自我檢核

前述章節已界定 GDPR 適用範圍與個資的相關定義，接續組織需逐步檢視再結合法規的核心領域，就隱私權(亦即個當事人權利)、資料安全與控制及治理等方面進行符合性之遵循與確認。本報告特別針對這 3 個面向整理出下列幾項因應重點，提供組織參考並落實相關作法：

- 隱私保護衝擊分析(Data protection impact assessment)，以即時分析相關風險，並規劃安全之防護機制。隱私保護衝擊分析從整個組織業務流程，辨識涵蓋在法規遵循範圍內的個人資料與其生命週期，評估現行保護機制後，辨識風險未被減緩或機制不足處。

- 設計及預設之資料保護(Data protection by design and by default)，考量現有技術、成本、處理之性質、範圍、內容、目的及處理對當事人之權利等可能發生之風險，控管者均應提出適當之科技化且具組織的措施，如在委外、產品研發或程式設計的專案初始，就應納入隱私保護的設計，像假名化、去識別化或資料蒐集最小化等原則；在資料保護預設原則下，謹守個資當事人同意之資料被處理等原則。

- 整合組織內部已運作之相關管理制度或技術防護，如 ISO 27001, BS 10012, ISO 29100, NIST SP 800-53 等，以多層次之縱深防禦方式，降低來自不同面向之風險，同時可收資源整合之效。

- 規劃與確保處理系統及服務持續之機密性、完整性、可用性及彈性(resilience)之能力，並定期測試，評估並衡量確保個人資料處理安全性之科技化且具備組織化措施之有效性。
- 防護技術之更新，如假名化之處理、加密技術之運用、對於資料之控管與處理者要求處理活動之紀錄、刪除不同類別之個人資料之預設時間及個人資料外洩之偵測等，皆應有整體防護技術的方案。
- 訂定個資外洩事件通報及應變機制，定期演練以完備其通報及應變程序。在實體(physical)或技術性事件中，建立即時回復個人資料可用性及可接近性之能力。
- 架構持續改善之運作機制，包括以指導(direct)為核心，建立評估(evaluate)、控制(control)、維運(maintain)及回應(react)等各個循環管理工作事項，以達法規遵循與業務流程持續變動管理之效。

法規的遵行雖無法一蹴可幾，但組織需在有限資源的情況下，對法規明顯要求符合之事進行改善。本報告針對 GDPR 法規整理之重點，提供建議之自我檢核表(詳見表 1)，組織可逐步檢視與 GDPR 之整體差異性，以期縮小適法性之差距。

表1　GDPR 自我檢核表

| 項目 | 檢核項目 |
|---|---|
| 1 | 以風險、法規遵循為基礎，發展完整性的資料保護策略，並訂出相關政策與行動方案，透過與各內部單位良善溝通管道與教育訓練，建立與政策一致之個人資料安全防護目標。 |
| 2 | 定期盤點與釐清業務流程，依據個人資料之生命週期，發展維運與持續改善方案。 |

| 項目 | 檢核項目 |
| --- | --- |
| 3 | 規劃資料保護之核心推動管理委員會，同時可配置資料保護員一職，得適當且即時涉入所有有關個人資料保護之業務，俾資料當事人就所有與其資料處理及行使本規則權利之有關事項得聯繫資料保護員。 |
| 4 | 定期實施隱私保護衝擊分析，以即早辨識相關風險；同時於相關流程加入設計及預設之資料保護的防護管理機制。 |
| 5 | 當事人權利之定期檢視，特別是針對資料可攜權、拒絕權或個人化之自動決策及被遺忘權，應從管理與技術面著手，以嚴謹且完整程序確認。 |
| 6 | 控管者應實施適當科技化且有組織的措施，以確保並得證明其處理符合法規規定。該等措施應得予審視，且必要時應予更新。 |
| 7 | 個人資料處理活動之紀錄責任，若有需要時控管者或處理者及控管者應依監管機關之要求提供紀錄。同時，若要進行任何當事人資料權利之回應與處理，個人資料處理活動之紀錄，亦可考量列為必要之工作事項。 |
| 8 | 訂定個人資料業務相關系統或服務委託辦理之管理措施，若有資料管理者辦理資通系統之建置、維運或服務之提供，應選任適當之受託者，並從合約(協議)與實際業務執行時，適時進行監督與管理。 |
| 9 | 訂定個人資料事件通報、應變及演練相關機制，定期演練以完備其通報及應變程序；控管者發現個人資料侵害發生，即應向監管機關通報，通報機制應於發現後 72 小時內啟動。 |
| 10 | 建立法規遵循性之個人資料安全維護案及實施情形之持續精進及績效管理機制，定期提出實施情形報告，若有缺失或待改善者，則應提出持續改善報告。 |

資料來源：本報告整理

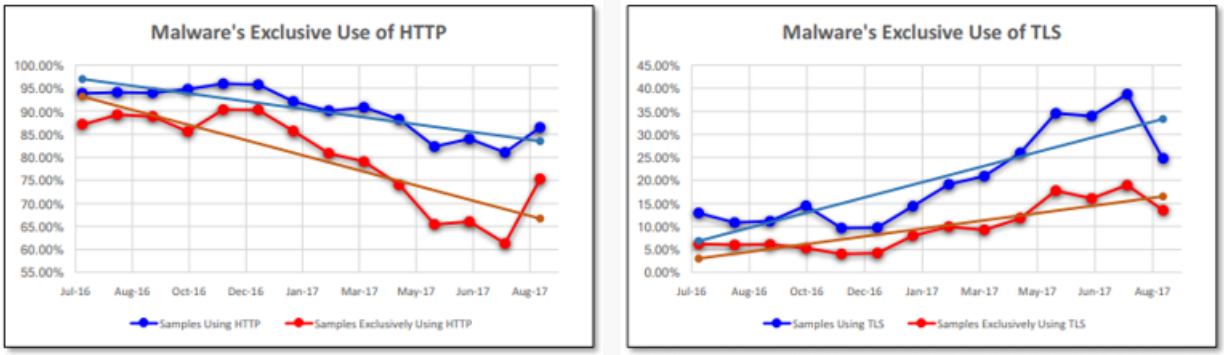
# 第三章 資安新興議題研討

本報告所探討的資安新興議題，類型包括機器學習的資安技術研究與駭客之新興攻擊手法等，分別為機器學習 HTTPS 加密流量分析、Android Root Bridge 漏洞利用及利用可變動資料串流(ADS)之進階持續威脅(APT)攻擊等議題。

透過這些新興技術議題的研討，使技術人員了解未來資安技術的可能運用與發展，新興的資安技術可以視為未來的武器運用，端視這些技術掌握在正義或暗黑的一方。

## 3.1 機器學習 HTTPS 加密流量分析

根據網路瀏覽器的統計數據顯示，目前已超過 70%的網頁採用 HTTPS 通訊協定，以保障資料隱私與完整性[2][3]。惟加密流量保障用戶隱私的同時，也成為不法份子攻擊的管道，透過將惡意程式隱藏在加密流量內逃避偵測的攻擊手法，使得惡意程式有由 HTTP 轉移至 HTTPS 之趨勢，詳見圖 5。




資料來源：[4]

圖5　惡意程式由 HTTP 轉移至 HTTPS 之趨勢

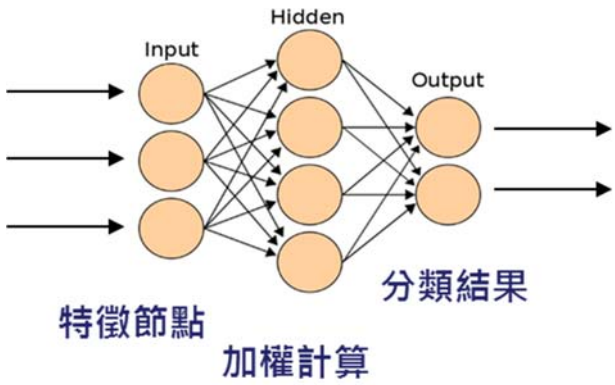
面對大量湧入的加密流量，傳統識別威脅的方法(如封包檢測等)已無法使用。為了防止加密流量中的惡意攻擊行為，目前常見的檢測方法為設置代理(Proxy)，透過 Proxy 先解密接收到的通訊數據，再利用傳統識別威脅的方法分析其中的行為與內容後，再加密進行發送。惟此方法雖可套用傳統檢測方法，卻也可能曝光用戶的隱私。

因此，為確保資料加密之完整性且又能防堵惡意攻擊行為，機器學習技術逐漸被投入用來識別加密網路流量中的資安威脅，藉由分析網路流量特徵，在不解密的情況下識別惡意流量找出潛在威脅。

機器學習是利用演算法來分析資料與學習，並對事件做出決定或預測。為建立最適合的分類模型，會藉由選擇不同的機器學習演算法，搭配所利用的特徵進行訓練，以判斷 HTTPS 連線是否存有惡意程式。目前在分析 HTTPS 加密流量中，最常見的演算法為類神經網路、支持向量機、決策樹及隨機森林，以下將簡介這 4 種機器學習演算法的特性。

●類神經網路

類神經網路是藉由模擬人類神經的傳遞方式來達到複雜的學習成效，透過對各個 HTTPS 連線的特徵做加權計算與訓練後，最終輸出是否為惡意流量的分類結果(詳見圖 6)。其中，深度學習即是此類型最著名的學習方法，它透過多層的加權計算與訓練，來強化學習能力。

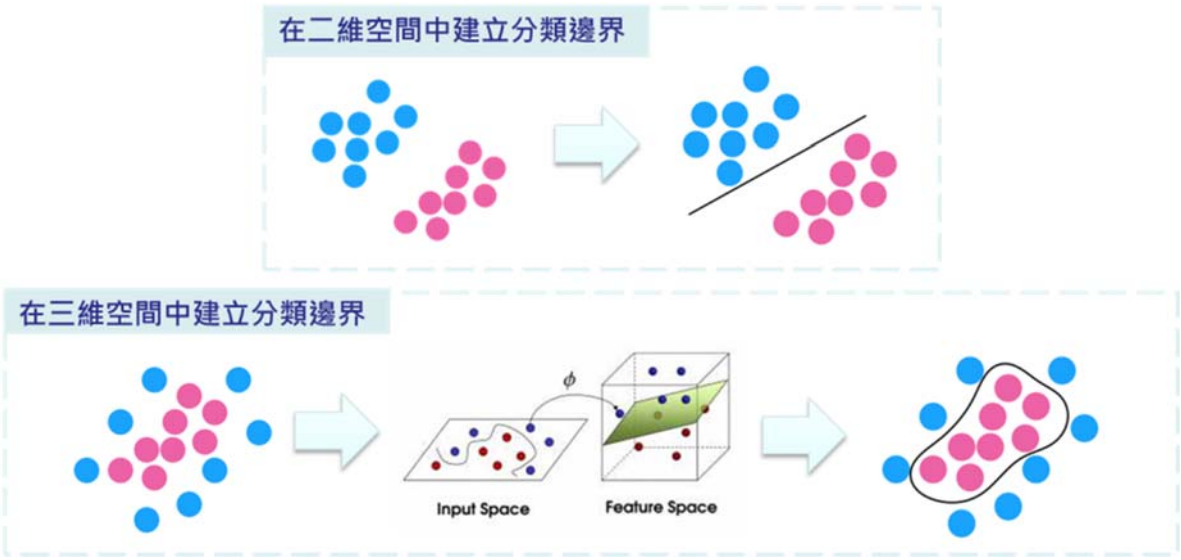



資料來源：本報告整理

圖6　類神經網路結構

●支持向量機

支持向量機的訓練過程是利用連線特徵建立出多維空間，再利用訓練樣本找出與正常或惡意資料間隔最大的分類邊界，並以此來分類資料(詳見圖 7)。

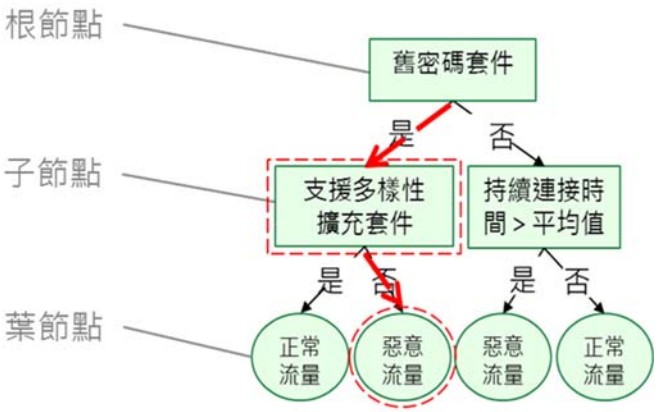



資料來源：本報告整理

圖7　利用支持向量機建立分類邊界

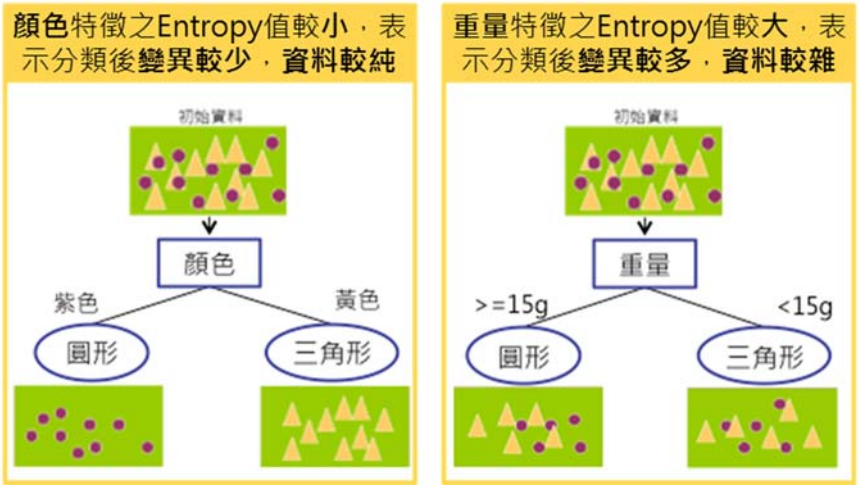
●決策樹

決策樹是利用樹狀結構來處理分類問題，根節點與子節點代表所使用的特徵，葉節點代表分類的結果(詳見圖 8)。通過計算各特徵節點的熵(Entropy)值[5]來建構樹狀結構，決定優先使用哪個特徵作為分割節點，使分類後能讓相似的資料盡可能的分於同一類，以降低資料的變異程度。




資料來源：本報告整理

圖8　決策樹樹狀結構

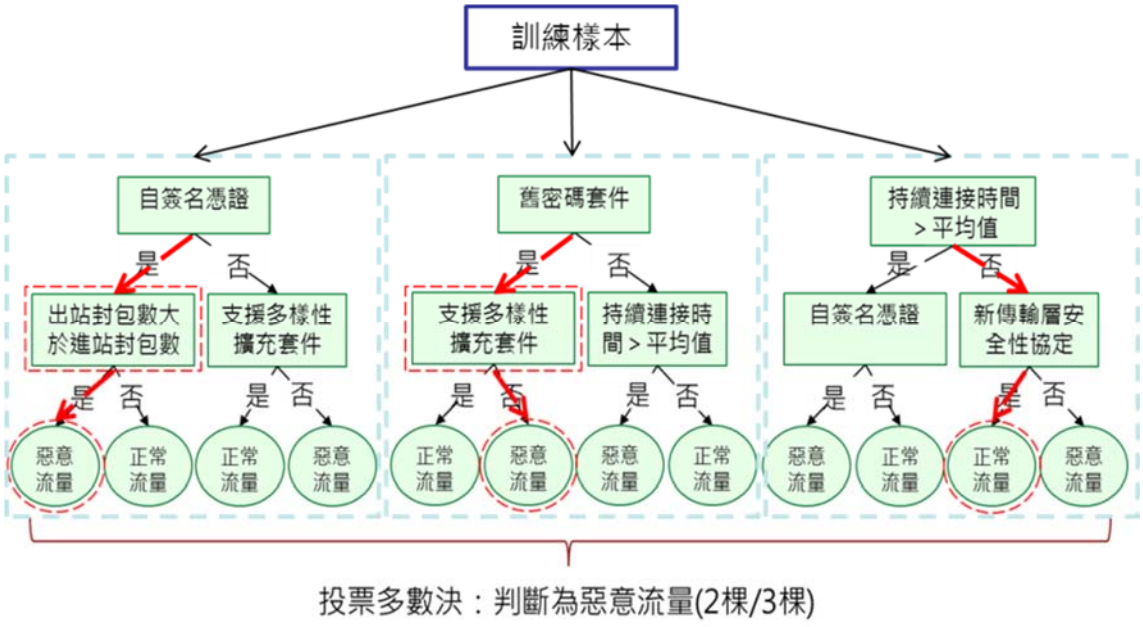



資料來源：本報告整理

圖9　Entropy 值對決策樹分割節點的影響

●隨機森林

隨機森林是由多個決策樹所組成的整合學習技術，能提供很好的效能與預測能力，且在實務上非常容易使用，只需要決定決策樹的棵數與每棵樹所選擇的特徵個數，即可進行資料的分析，再基於每一棵樹的分類結果，採取「多數決」方式做為最終分類結果(詳見圖 10)。隨機森林為目前判斷加密流量是正常/惡意的問題上，最常使用的機器學習演算法。

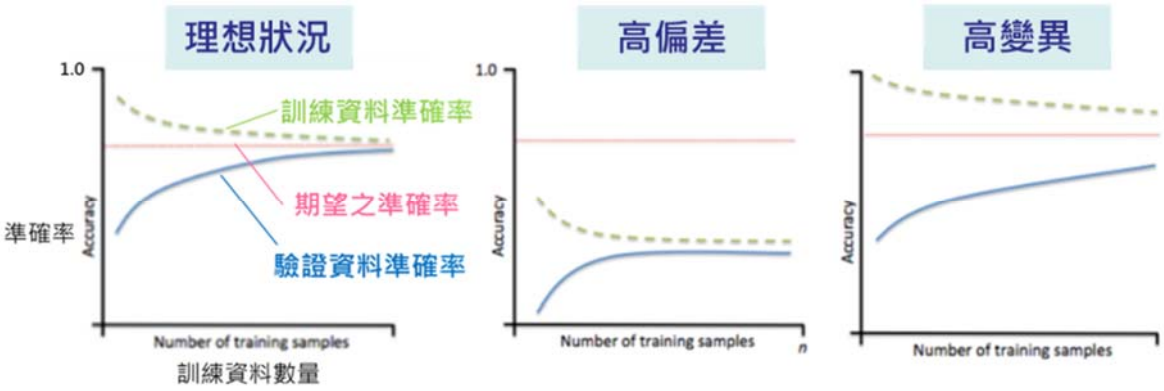



資料來源：本報告整理

圖10 利用隨機森林判斷惡意流量示意圖

利用機器學習演算法建立出分類模型後，可透過學習曲線做為評估分類模型好壞的依據。當訓練資料與驗證資料的誤差收斂且與期望之準確率誤差較小，此時為理想狀況，則無須再進行參數調整，成功建立分類模型。若訓練資料與驗證資料的誤差收斂但準確率卻很低，此情況稱為「高偏差」，則可以透過增加模型參數，如建立更多的特徵來改善。而當訓練資料與驗證資料的準確率相差太多，此情況稱為「高變異」，則可以透過增

大訓練集，或者減少特徵數來改善(詳見圖 11)。




資料來源：本報告整理

圖11 利用學習曲線評估分類模型

透過訓練好的分類模型，利用事先準備好的測試集檢測其分類結果，並計算準確率。若準確率已達預期目標，則保留模型供實際使用，並持續追蹤模型情況以判斷是否需調整。若沒有達預期目標，則可使用不同的機器學習演算法、數據集或特徵集以訓練其他的分類模型。

目前的研究成果顯示，使用類神經網路所訓練出來的分類模型，其準確率介於 76.42%至 99.63%間[6][7][8]，使用支持向量機的準確率介於 39.9%至 99.98%間[6][7][8]，使用決策樹的準確率介於 95.87%至 99.98%間[7][8]，使用隨機森林的準確率介於 70.41%至 99.99%間[6][7][8]。雖然上述 4 種演算法的分類結果，最高準確率皆可達 99%以上，但類神經網路在訓練過程需要較多在設定架構或調整參數等專業知識；支持向量機在訓練過程需消耗較多的記憶體空間，因此效能不佳；決策樹容易在訓練數據中生成複雜的結構樹而造成高偏差現象；因此，在目前加密流量分析議題中，多數會使用隨機森林演算法來訓練分類模型。隨機森林改善了決策樹會產生的高偏差問題，無論對大或小的訓練樣本也能提供較高的準確率與效能，調整的參數也相對容易，並且在實務上非常容易使用，可做為實作加密流量分析優先考量的演算法。

### 3.2 Android Root Bridge 漏洞利用

由近期事件案例發現，透過安卓(Android)系統建置的公車站電子看板，存在 Root Bridge 漏洞。此漏洞的存在，易遭駭客入侵散佈惡意程式，並發動分散式阻斷服務(Distributed Denial of Service，以下簡稱 DDoS)攻擊，進而被植入挖礦程式，以賺取虛擬貨幣。經研究分析發現，除北韓駭客利用這個漏洞，植入挖礦程式以獲取利益外，亦有中國網路犯罪集團利用相同漏洞，植入殭屍程式控制智慧裝置，並針對特定購物網站發動 DDoS 攻擊，讓購物網站無法正常提供服務，藉以對商家進行金錢勒索。

在分析 Root Bridge 漏洞之前，必須先介紹 Android Debug Bridge(ADB)。ADB 是用於 Android 開發使用的指令工具，可以直接控制 Android 模擬器或真實的 Android 裝置，進行除錯、測試、上傳及下載等工作，一般開發多使用實體 USB 進行連結，但也可以開啟網路連線管理功能(預設連結埠為 5555)，透過網路同時連結多個裝置進行除錯。

這個管理介面通常是開發商用來進行系統管理與應用程式開發使用，在非開發者版本應該被停用。惟部分聯網裝置卻因管理失當或錯誤使用 ADB 功能，導致受害裝置能透過 5555 連結埠進行連線，使任何人在不需認證的情況下，即可獲得系統最大權限(Root shell)操作該聯網裝置。

一旦駭客利用 Root Bridge 漏洞入侵受害裝置後，即可在受害裝置上安裝惡意應用程式套件(APK)，使得受害裝置除了進行挖礦作業外，還會掃描網路上的其他 ADB 裝置(連結埠 5555)，企圖擴散感染。技服中心在事件調查中，發現受害裝置被植入負責執行挖礦與企圖擴散的惡意程式樣本，詳見圖 12。


| 樣本名稱 | MD5 | 類型 | 功能 |
|---|---|---|---|
| sss | 6a22c94d6e2a18acf2377c994d0186af | ELF_ARM | 惡意程式主體，負責釋放樣本及啟動droidbot |
| nohup | 9a10ba1d64a02ee308cd6479959d2db2 | ELF_ARM | 啟動sss及droidbot的指令集 |
| bot.dat | bc84e86f8090f935e0f1fc04b04455c6 | data | 釋放其他8個樣本 |
| droidbot.apk | 914082a04d6db5084a963e9f70fb4276 | apk | 基於coinhive的挖礦app |
| droidbot | 412874e10fe6d7295ad7eb210da352a1 | ELF_ARM | 連結到開啟5555埠的Android裝置，並感染 |
| config.json | 27c3e74b6ddf175c3827900fe06d63b3 | json | 礦池及設定駭客錢包位址 |
| invoke.sh | 48fdf98e12cb7d8f963c5c8a616150c3 | shell | 安裝及啟動挖礦app |
| install-recovery.sh | 6cc2f496aa1ce87ae802a0e570fd62f8 | shell | 輔助安裝挖礦app |
| ddexe | 53ff82c3b5aa126eb16bf282a1f8bf4c | shell | 輔助安裝挖礦app |
| debuggerd | c8bbb31dae834b2224565de1933c9a70 | shell | 輔助安裝挖礦app |
| xmrig32 | ac344c3accbbc4ee14db0e18f81c2c0d | ELF_ARM | arm-32上的CPU挖礦 |
| xmirg64 | cc7775f1682d12ba4edb161824e5a0e4 | ELF_ARM | arm-64上的CPU挖礦 |
| botsuinit_1_1.txt | cd37d59f2aac9101715b28f2b28b7417 | txt | 安裝成功後由invoke.sh產生出來 |

資料來源：本報告整理

圖12 執行挖礦與企圖擴散的惡意程式樣本

進一步以網路引擎進行搜尋與統計，目前存有 Root Bridge 漏洞的 Android 聯網裝置已遍布全球，其中台灣位居全球第二，這些聯網裝置的類型包括智慧家電與個人的行動裝置，詳見圖 13。分析並推測造成漏洞的最主要原因，在於使用者自行使用 Root 權限開啟 ADB 連線功能。一般民眾可能參考網路上的教學文章，自行使用坊間流傳的權限提升(俗稱 Root)工具並參照教學流程，對 Android 系統的手機、平板、智慧電視及電視盒進行權限提升，以達到自行安裝非官方的 APP 或盜版程式的目的，但卻也因此造成許多智慧電視與電視盒在提高權限的過程中被開啟 Root Bridge 漏洞，導致智慧家電遭受入侵。

TOTAL RESULTS

45,013

TOP COUNTRIES

| | |
|---|---|
| Korea, Republic of | 10,841 |
| Taiwan | 10,036 |
| China | 7,554 |
| United States | 4,260 |
| Hong Kong | 2,442 |

TOP ORGANIZATIONS

| Device Name | Model Name | Device Type | Count |
|---|---|---|---|
| Samsung Galaxy Note 3 | SAMSUNG-SM-N900A | Android Smart Phone | 2904 |
| Motorola Moto X (Europe) | XT1052 | Android Smart Phone | 2886 |
| Google Pixel XL | Pixel XL | Android Smart Phone | 472 |
| Google PIXEL 2 XL | PIXEL 2 XL | Android Smart Phone | 454 |
| Samsung Galaxy S5 | SM-G900F | Android Smart Phone | 436 |
| OnePlus 3T | ONEPLUS A3010 | Android Smart Phone | 360 |
| OnePlus 5 | ONEPLUS A5000 | Android Smart Phone | 358 |
| Samsung Galaxy S8 Plus | SM-G955F | Android Smart Phone | 337 |
| Samsung Galaxy S8 | SM-G950F | Android Smart Phone | 335 |
| Samsung Galaxy S4 | GT-I9500 | Android Smart Phone | 100 |
| EVPAD PRO 電視卡盒 | EVPAD-PRO-T | Android TV box | 56 |
| EVPAD PRO 電視卡盒 台灣版 | EVPAD-TW-MAX | Android TV box | 46 |
| Asus ZenFone 5 | ASUS T00J | Android Smart Phone | 44 |
| MXQ PRO 4K s905 p201 | Android p201 | Android TV box | 43 |
| EVPAD PRO 電視卡盒 | EVPAD-PRO-MAX | Android TV box | 33 |
| Sunchip TV box | CX_A39 | Android TV box | 33 |
| Unblock Global Edition S800 | Global_Edition_S800 | Android TV box | 30 |
| RockTek A2V | RT_A2V | Android TV box | 24 |
| Askey Set-top box | STI6030 | Android TV box | 24 |
| JVC 65T | 65T | Smart TV | 21 |

資料來源：SHODAN

圖13　網路搜尋存在漏洞之聯網裝置

為降低 Root Bridge 漏洞所帶來的威脅，針對聯網裝置之安全防護，提供以下 5 點建議：

- 勿隨意對裝置進行權限提升動作，以避免開啟不必要功能。
- 若無使用上的需求，應關閉裝置的遠端管理功能，減少裝置被攻擊的途徑。
- 勿隨意在裝置上安裝來路不明之應用程式(含 APP)，並留意應用程式所要求之存取權限。
- 若需使用遠端管理功能，應避免將裝置管理介面曝露於網際網路，並完備權限存取控制。
- 若裝置有被植入惡意程式的疑慮，可使用回復出廠設定的方式，以清除惡意程式。

### 3.3 利用可變動資料串流(ADS)之進階持續威脅(APT)攻擊

由近期事件案例分析發現新興的攻擊手法，駭客結合社交工程郵件、惡意捷徑檔及可變動資料串流(Alternate Data Streams，以下簡稱 ADS)等攻擊手法，實施進階持續威脅(APT)攻擊。其縝密的攻擊手法除難以追縱外，更大幅提升案件分析的困難度。以下將介紹此新型態的 APT 攻擊手法，並提供簡易的檢查方法，讓使用者對 ADS 檔案進行基本的防範。

ADS 主要的設計目的是在檔案中允許存放多個額外的資訊，以便程式技術人員後續的應用，此為 Windows NTFS 檔案格式的特性。惟由於 ADS 的附加資訊除必須以特定的指令才能顯示外，在寫入資料後，原始檔案的大小並不會因此而改變。因此，駭客運用 ADS 的隱蔽性與特殊性將惡意檔案隱藏在捷徑檔(*.lnk)中，再設計業務相關議題發送社交工程郵件，誘使相關人員點擊捷徑檔(*.lnk)以執行惡意程式，即可成功攻擊目標使用者，駭侵手法詳見圖 14。


資料來源：本報告整理

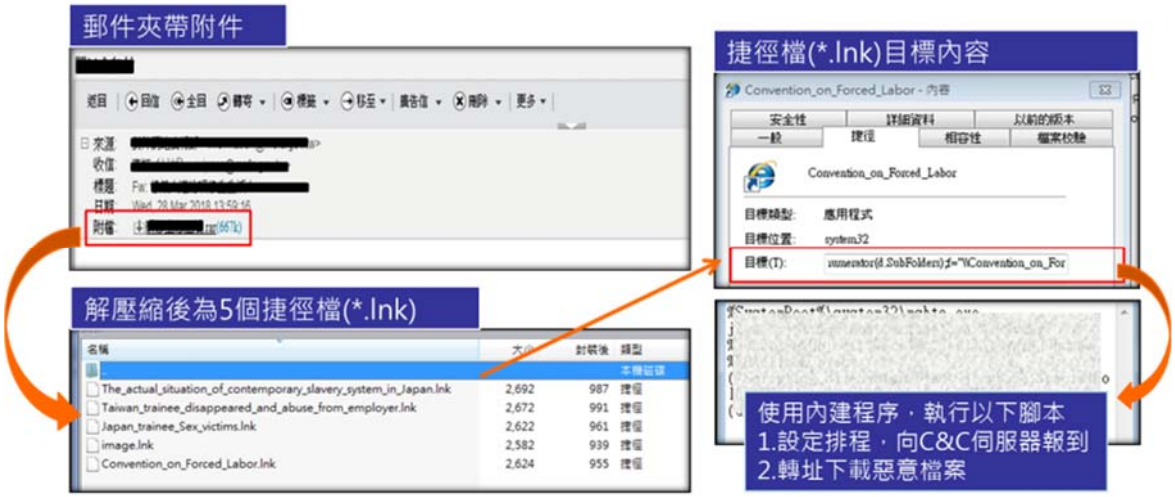
圖14　駭侵手法說明

為執行攻擊，駭客會準備惡意程式相關檔案 Zone.AM、Zone.CM 及 Zone.SPE。其中，Zone.AM 包含執行惡意程式的相關排程、Zone.CM 為排程中所觸發的惡意程式、Zone.SPE 包含中繼站短網址。接著駭客使用指令，將惡意檔案寫入至捷徑檔的 ADS 中。由於 ADS 的特性，即便利用檔案總管查看目錄與檔案大小，亦無法發覺有惡意檔案的存在，詳見圖 15。駭客再利用與業務相關議題的社交工程郵件，誘使人員點擊惡意捷徑檔(*.lnk)，即可啟動惡意程式的相關排程達到攻擊之目的。


資料來源：本報告整理

圖15　使用 dir 指令檢視目錄與檔案大小

此外，技服中心深入調查後發現，於本次案例中，駭客利用的壓縮檔夾帶多個行為相同的惡意捷徑檔(*.lnk)，推測駭客為達到成功攻擊之目的，可能使用多個功能相同但名稱不同的捷徑檔，以增加點擊觸發惡意程式的機率，詳見圖 16。




資料來源：本報告整理

圖16　壓縮檔內含 5 個行為相同之捷徑檔

整理上述攻擊手法後，若要防範此類的攻擊，使用者勿隨意點擊來路不明的郵件與附件檔案，若必須檢視附件內容，則可在掃毒後，進一步在命令提示字元模式(command line)下利用 dir /r 指令來檢視附件內容中是否含有不明的 ADS 資訊(詳見圖 17)，以確認附件檔案是否有夾帶不明程式。


資料來源：本報告整理

圖17 使用 dir /r 指令以檢視 ADS 檔案

# 第四章 結論

本報告透過 6 大面向研析本季之全球資安威脅現況，並針對「資安(訊)供應商持續遭駭破壞供應鏈安全」與「進階持續威脅攻擊竊取機密資料」等 2 大面向，以本季發生的重大資安事件來探討供應商管理不善與機敏資料防護不周所可能帶來之資安風險。另一方面，在政府資安威脅現況，本季所通報的資安事件雖以影響等級最輕微之「1 級」事件為主，惟分析通報事件之原因後，仍需針對網站設計不當及應用程式漏洞等弱點加以關注。針對本季全球與政府所面臨的主要資安威脅，本報告針對「資安標準作業程序」、「社群網路安全」及「網站設計不當與應用程漏洞」等 3 方面，提出資安防護建議。

資安專題的分享，因應 GDPR 範圍為網路世界，可能衝擊到台灣組織的管理程序，本報告藉由說明 GDPR 之相關規定及因應重點，相關單位可審視自我資安環境之完備度，並落實個人資料保護管理制度。

本季探討的資安新興議題，除了「機器學習 HTTPS 加密流量分析」之資安技術研討，另外亦包括 2 個新興駭客手法的介紹，分別為「Android Root Bridge 漏洞利用」及「利用可變動資料串流之進階持續威脅攻擊」。期能透過資安技術的介紹與駭客手法的說明，逐步提升技術人員之資安防護能量。

下一季「資通安全技術報告」，持續分析全球與我國政府機關之資安威脅現況，以及從蒐集新興資安議題，國內外情資與相關研究人員角度提供防範的重點。另外，「資通安全管理法」預定於明(108)年 1 月 1 日施行，因此第 4 季之資安專題分享，將分享該法及其子法之管理與準備之重點。

# 資安相關活動

本季行政院資通安全處亦辦理多項資安相關活動，說明如下：

## ◆ 公務人員資安職能訓練

公務人員資安職能訓練為提升政府機關(構)資安(訊)業務承辦人員資安專業知識與技能，期透過職能訓練培訓更多公務人員成為資訊、資安專業人才；同時也協助政府機關(構)透過專班之開設，可以遴選合宜人才受訓，並符合「政府機關(構)資通安全責任等級分級作業規定」要求。

本年共辦理 8 梯次之資安職能訓練，主題包括電子郵件安全、雲端服務安全管理、資訊安全通識及電子資料暨個資保護管理等，分別於台北、桃園、台中及台南等地辦理。公務人員資安職能訓練不僅只有課程訓練與小組練習，更於課後設計相關測驗題進行評量，以測試受訓人員之理解與應用程度。

## ◆ 安全系統發展生命週期(SSDLC)訓練研習

本年 SSDLC 研習共分為 2 大主軸，首先開辦安全資訊系統開發研討會，介紹資訊系統安全發展生命週期基礎觀念與各階段流程強化安全之相關作業，以提升政府機關(構)資訊系統之安全性。

接續辦理安全資訊系統開發實作研習，主要在介紹安全資訊系統發展生命週期基礎概念、開發階段安全實務介紹及實作練習，著重在政府機關(構)人員之實際操作與練習。課程內容包括 SSDLC 基礎概念簡介、威脅建模(Threat Modeling)介紹與實作練習及部署與維運階段之系統組態管理等實機操作。共辦理 8 個梯次，每梯次共 2 天的實作課程。

## ◆ 資安系列競賽

為推廣全民資安認知意識與加強學生資安技術能力，舉辦資安系列競賽活動，提升我國資安認知與技術能量。自 95 年開始辦理資安系列競賽活動，目前為全國最具規模之資安系列競賽活動之一。

資安系列競賽活動之主題皆會參考資安趨勢，本年以「電子支付安全」為主題，藉由與民眾生活息息相關之主題提升社會大眾資安意識。競賽活動以資安技能金盾獎為活動核心，旨在發掘資安人才，提升資安技術能力；同時亦透過徵件競賽(海報、漫畫、微電影及動畫)等資安作品，推廣大眾之資安認知。

## 參考文獻


[1]國家發展委員會，歐盟一般資料保護規則專區，取自：
https://www.ndc.gov.tw/Content_List.aspx?n=1DE9FB38844DDC8D

[2]Google，網站的 HTTPS 加密實行狀況，取自：
https://transparencyreport.google.com/https/overview

[3]Let’s Encrypt, Let's Encrypt Stats，取自：
https://letsencrypt.org/stats/#percent-pageloads

[4]Cisco, TowardsGeneralizableNetwork ThreatDetection，取自：
http://statisticalcyber.com/talks/Towards%20Generalizable%20Network%20Threat%20Detection.pdf

[5]維基百科，熵(資訊理論)，取自：
https://en.wikipedia.org/wiki/Entropy_(information_theory)

[6]Czech Technical University in Prague, Detection of HTTPS Malware Traffic，取自：https://dspace.cvut.cz/bitstream/handle/10467/68528/F3-BP-2017-Strasak-Frantisek-strasak_thesis_2017.pdf

[7]IEEE, Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity，取自：
https://dl.acm.org/citation.cfm?id=3098163

[8]ACM, Deep learning for malicious flow detection，取自：
https://ieeexplore.ieee.org/abstract/document/8292316/