資訊安全

因應惡意程式攻擊技術發展網路資訊安全管理探討

空軍備役上校 吳嘉龍

提要

資訊安全具三個特性，包括有機密性、完整性與及可用性。機密性在確保只有經授權的人方能允許存取資訊，完整性在於確保資訊內容及資訊處 方法正確且完整，可用性則確保經授權的使用者當需要時，能存取資訊及使用相關資產。資訊安全對組織而言相當重要，資訊是一種資產，就像其他的重要企業資產一樣，對單位組織具有價值，因此需要受到適當的保護。而資訊安全在於保障企業資訊資產免於 可承受的風險。個人資料保護法為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。近年來通訊、能源、水、電、交通系統等維繫民生與國家機器運轉的關鍵基礎設施成為駭客熱門的攻擊目標，如烏克蘭電廠被駭導致大停電、美國核電相關公司遭受駭客攻擊等，這些國家級基礎建設已成為駭客新攻擊目標，駭客透過偽造網址、分散式阻斷服務攻擊或癱瘓金流資訊系統等方式做為勒索的籌碼，一但淪陷將癱瘓民眾日常生活機能，造成經濟損失，衍伸出重大安全問題，甚至被有心人士利用來達成某些特定政治目的，所以因應惡意程式攻擊與完善資訊安全管理實為刻不容緩的議題。

關鍵字：網路管理、惡意程式攻擊、電腦緊急應變、資訊安全、分散式阻斷服務攻擊。

壹、前言

雲端與網路科技迅速發展，正將我們帶往一個與過去截然不同的數位世界，在數位生活裡，網路虛擬與真實世界的區隔會日漸模糊。英國標準協會台灣分公司總經理蒲樹盛分享世界經濟論壇(World Economic Forum, WEF)所發表的2018年全球風險研究報告，最嚴重的就是極端氣候所導致的天然災害，然後緊接著就是近來竄升最快的科技風險，其中網路攻擊排名第一。全球勒索軟體惡意程式肆虐，分散式阻斷服務攻擊(DDoS)不但頻繁，且流攻擊流量屢創新高，還有駭客攻擊的轉型迅速，除了以獲取商業利益為導向外，更進一步的將焦點鎖定在高價值的技術作為攻擊目標，因而衍生出例如虛擬貨幣的挖礦式攻擊。在未來的資安挑戰上，蒲樹盛舉例像Google發表的72量子位元電腦，能將原本需2個月破解的加密演算，縮短到數天，甚至是數小時，對現有加密機制的防護產生威脅。尤其值得注意的是，發展中的5G行動網路也是值得關注的趨勢。行政院國家資通安全會報因應我國特殊的政經情勢及全球複雜多元的資通訊變革，行政院國家資通安全會報(簡稱資安會報)於2016年11月提出「國家資通安全發展方案(106-109年)」以並作為國家推動資安防護策略與計畫之重要依據。面對網路安全管理與網路科技的迅速發展，美國非常重視資訊安全風險管控相關因應作為，2017年美國總統川普公布「強化聯邦網路與關鍵基礎設施網路安全」總統命令(Presidential Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)，要求各聯邦機關首長應使用改善關鍵基礎設施網路安全框架，管理該機構的網路安全風險[1-2]。

近年來，數位經濟帶動產業朝跨世代、跨境、跨領域、跨虛實等趨勢發展，促使全球產業格局翻轉，加上隨著數位經濟與物聯網(Internet of Things, IoT)時代的來臨，為建構完善的產業生態體系(ecosystem)及加速產業創新與優化產業結構，行政院提出「數位國家．創新經濟發展方案(2017-2025年)」(簡稱DiGi+)。作為下階段國家資通安全發展方案推動，需從資通安全的角度，確保數位國家安全，推動DiGi+方案「友善法制環境」、「跨域數位人才」以及「先進數位科技」三項數位國家基磐配套措施，進而打造安全可信賴的「數位創新基礎環境」及「網路社會數位政府」。行政院新聞傳播處指出為促進數位經濟創新發展、提高國人生活品質，邁向智慧國家是政府五大施政目標之一；為加速臺灣產業轉型升級，政府打造以「創新、就業、分配」為核心價值，及追求永續發展的經濟新模式，並透過「連結未來、連結全球、連結在地」三大策略，激發產業創新風氣與能量。政府提出「智慧機械」、「亞洲．矽谷」、「綠能科技」、「生醫產業」、「國防產業」、「新

農業」及「循環經濟」等5+2產業創新計畫，作為驅動台灣下世代產業成長的核心。行政院於105年底啟動「數位國家・創新經濟發展方案」(DIGI+方案)，作為引領數位發展、帶動創新的施政藍圖。期透過此方案，我國產業及生活能融入更多，如人工智慧、物聯網、大數據等智慧科技，發揮我們小而精與跨域整合速度快優勢，讓台灣成為智慧創新典範國度。「DIGI+方案」中定義D意指Development(發展)，發展堅固基磐；I意指Innovation(創新)，創新數位經濟；G意指Governance(治理)，治理智慧國家；I意指Inclusion(包容)，包涵容納公民社會，下列的表一為現階段「DIGI+方案」發展成果。科技會報辦公室指出，DIGI+方案亦推動多項貼近民眾的數位公共服務，包括積極打造空氣品質物聯網感測基礎建設，將國內空氣品質感測精度達鄉鎮等級，提供民眾即時空氣品質資訊；全國Gbps等級的寬頻網路涵蓋率已逾40%，並提升偏鄉衛生室及巡迴醫療點網路速度，完善偏鄉寬頻接取環境；建置災害訊息廣播系統可即時傳送10種災害警訊至民眾手機，透過一站式災害情報站提供民眾颱風資訊、停班停課、停(復)水/電力/電話、道路封閉等民生災害即時訊息服務[3-4]。

表一、促進數位經濟創新發展智慧國家現階段「DIGI+方案」發展成果(自行整理)

法規調適與政策規劃	1. 法規調適，完備前瞻科技應用的基礎環境。 2. 推動前瞻政策，強化5+2產業創新發展能量。
推動數位公共服務	1. 建置公共免費WiFi熱點。 2. 建置災害訊息廣播系統。 3. 打造空氣品質物聯網感測基礎建設。
加速寬頻基礎建設與推廣數位應用服務	1. 普及偏鄉及原民部落寬頻網路。 2. 升級偏鄉醫療頻寬。 3. 提升數位運用能力。 4. 擴大資料傳輸速率Gbps等級寬頻網路涵蓋率。

貳、個資保護風險評估與網路惡意程式攻擊安全威脅分析

本章節針對國家資通安全發展、資訊安全準則技術與風險管理相關理論角度切入，針對個資保護與網路惡意程式攻擊安全威脅分析作研究探討。2018年3月16日Facebook宣布停止英國數據分析公司「劍橋分析」(Cambridge Analytica)劍橋分析以及其母公司戰略溝通實驗室的臉書帳號，接著3月18日就被爆出5000萬使用者的個資遭遇不當使用，且「劍橋分析」劍橋分析將這些個資用於2016的美國總統大選上，美國麻州檢察長也宣布將對Facebook及劍橋分析公司展開調查，這起個資外洩事肇因分析為第三方合作夥伴的不當使用資料所引起[5]。全球晶圓代工龍頭台

資料來源：[7]

圖一、DIGI+5G應用產業創新策略規劃技術支援整合試煉平台

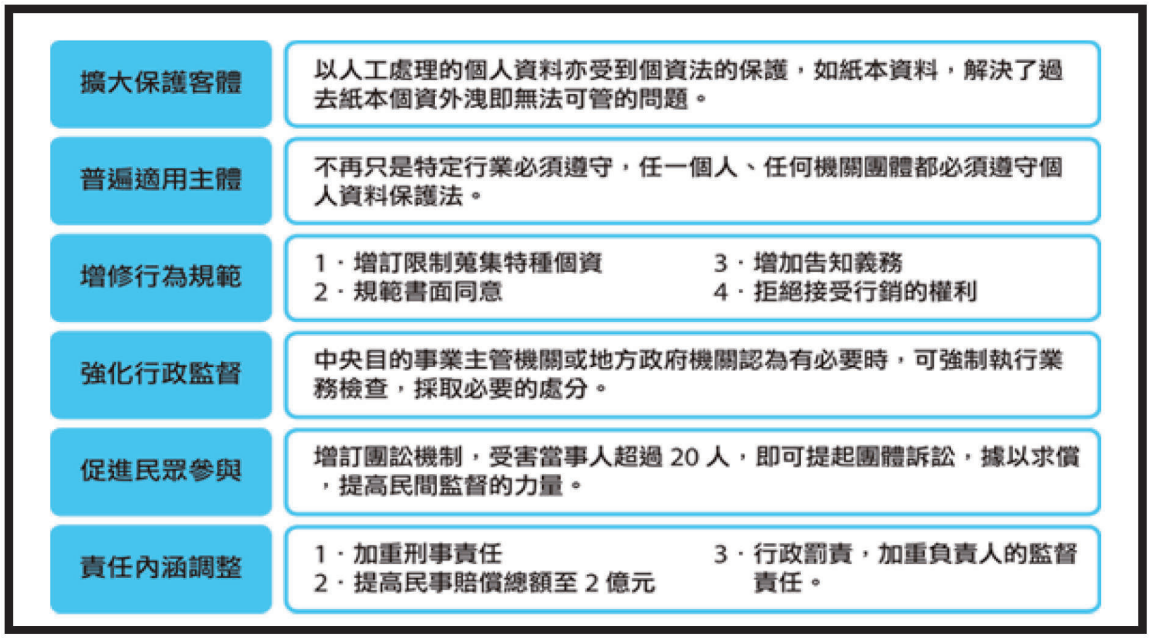
積電2018年8月3日晚間驚傳生產線遭WannaCry變種病毒入侵，影響所及，台積電竹科、中科與南科廠區相繼遭到感染，機台不斷重複開機，導致部份生產線停工。由於台積電向來有台股模範生的美譽，對資安防護的嚴謹也是眾所周知，所以此次發生病毒重大入侵後，引起媒體大幅報導，一開始更引起諸多揣測，甚至懷疑是內鬼或駭客攻擊所為。總裁魏哲家更親上火線於記者會中強調，此次重大資安事件純粹是安裝新機台時未按SOP，在進行網路連結前先隔離確保機台無毒。致使病毒進入公司網路，造成台積電停工1天，需報廢上萬片晶圓，預估損失高達78億元，此次資訊安全意外也為台積電史上最大資安事件[6]。

相對在個資保護作為推動上，全國法規資料庫強調個人資料檔案指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。針對個資法研究指出個資法主要從蒐集、處理和利用等三個層面，來規範個人資料的合理利用，新個資法所保護的資料型態，也從原本的電腦處理之個人資料，延伸到電腦處理的數位個人資料，或是紙本的個人資料，皆適用於直接或間接識別之個人資料中。

表二、全國法規資料庫個人資料保護法定義表

（自行整理）

蒐集	指以任何方式取得個人資料。
處理	建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
利用	指將蒐集之個人資料為處理以外之使用。
國際傳輸	指將個人資料作跨國（境）之處理或利用。
公務機關	指依法行使公權力之中央或地方機關或行政法人。
非公務機關	指公務機關以外之自然人、法人或其他團體。



資料來源：[9]

圖二、新版個人資料保護法修法六大重點

表三、經濟部個資保護作業手冊風險情境表

（自行整理）

紙本類	處理：紙本文件於內部處理過程中，下班時收存於辦公室上鎖之資料櫃。
	保存：1.紙本文件之保存(含暫存區)地點具備進出管控措施；2.紙本文件歸檔、入倉(庫)或集中保管前，確實清點數量及內容；3.紙本文件存放地點有消防、滅火、溫度控制等設施。
	傳遞：1.紙本文件於內部傳遞過程中，具有簽收/點收等控管措施；2.紙本文件提供外部利用均有公文往返等使用紀錄。
	銷毀：1.包含個資之紙本文件均不進行回收使用；2.紙本文件於內部進行銷毀時，均銷毀致無法辨識；3.紙本文件交由受委託廠商銷毀前，已簽訂包含雙方權利義務及賠償條款之契約或保密協議；4.紙本文件交由受委託廠商進行銷毀時，妥善進行監銷並留存紀錄。
電子類	傳輸：1.同仁透過對外寄發、傳輸個資檔案均進行加密；2.同仁對外傳輸個資檔案均有傳輸記錄，如 Email 寄件備份、FTP 傳輸記錄、網路硬碟等。
	保存：存於電腦個資檔案，均有加密或存放於專用且安全之資料夾。
	銷毀：電子檔案保存期限屆滿後均進行刪除。
系統資料庫	存取權限：1.資訊系統之使用者帳號均定期審查；2.系統具備職務區隔機制，給予適當之存取權限。
	使用紀錄：1.資訊系統具有記錄使用者活動日誌功能；2.單位主管或其授權人員定期審查資訊系統使用者之活動日誌。

個資法規範個人資料蒐集、處理及利用，從資料蒐集開始，以至資料的處理、利用，整個過程都必須符合個資法的規定，確保不侵犯個人隱私權，以及合理使用個人資料。因此，除了配合政府所規定的個資法規，也要了解每個人能行使的權利。新版個資法擴大對於個人資料的保護，不論是經由電腦處理的個人資料，或是手抄記錄的個人資料，都受到規範，全國法規資料庫個資法相關定義整理如表二[7-8]。

個資法注重定期針對個人資料之作業流程進行風險評鑑，鑑別可承受之風險等級，並針對不可接受之風險進行風險處理。為落實尊重當事人意願之精神，新版個資法設有當事人書面同意之規定，並將其列為公務機關或非公務機關對個人資料之蒐集、處理或利用的合法要件之一。目前有兩種情況下不受個資法規範：為了個人或家庭活動的目的，而蒐集、處理、利用個人資料；及在公開場所或公開活動中所蒐集、處理、利用之未與其他個人資料結合之影音資料，新版個人資料保護法修法六大重點如圖二，經濟部個人資料保護作業手冊2018年3月版公告風險情境表如表三，風險評估作業表如表四[9]。

表四、經濟部個資保護作業手冊風險評估表

（自行整理）

評估個人資料風險	使用個人資料風險評估表就個人資料檔案內容進行價值識別。個人資料之價值識別得以個人資料之內容、個人資料之數量、個人資料檔案之識別程度，以及其他必要之項目為評估基準。於個人資料檔案內容價值識別後，應進行個人資料作業之具體風險類型識別。就識別出之風險，風險發生之衝擊程度及發生之可能性進行風險評估並區分等級。風險發生之衝擊程度得以損害高低以及其他必要之項目為評估基準。就風險發生之衝擊程度及發生之可能性進行識別後，應予以區分風險等級，並就高風險之個人資料檔案作業進行風險處理。
處理風險	處理個人資料風險依風險評估結果進行風險處理，擬定具體對策。
建立個資保護評估清冊	各單位及所屬機關應將風險評估結果製作個人資料風險評估清冊，妥善保管且定期維護該清冊。

參、新興資訊安全威脅與歐盟一般資料保護規章GDPR分析研究

此章節針對新興資訊安全威脅與一般資料保護規章加以分析探討，針對數位經濟科技發展與全球化影響，個人資料保護議題帶來許多新的挑戰，歐盟為提升個人資料保護規範密度，並建立歐盟境內一體適用之管理規範，通過「一般資料保護規則」。在此針對一般資料保護規章發展緣由加以探討與說明，歐盟個人資料保護法規原為「1995年資料保護指令」(Data Protection Directive)。該指令於1995年生效，為因應科技與網路之快速發展、全球化等外在環境變化，以及為消除各會員國

法規差異以追求歐盟數位單一市場(Digital Single Market)目標，歐盟執委會於2009年開始推動修法，歐盟執委會隨後於2012年1月提出一般資料保護規章(General Data Protection Regulation，簡稱GDPR)草案，以取代1995年資料保護指令。其中與1995年資料保護指令差異在於，GDPR將可直接適用歐盟全境，不須經過轉換成歐盟會員國國內法程序。歐盟在GDPR中保留了1995年資料保護指令基本架構與核心原則，藉由GDPR改進現有個人隱私保護法律架構，達到調和並簡化境內資料保護規範以追求數位單一市場的目標、強化個人對自身資料的掌控能力、強化主管機關監理能力等目的[9-10]。

經過歐盟執委會、歐盟部長理事會與歐洲議會三方協商，歐盟於2016年4月完成GDPR立法程序並於5月生效，於2016年5月25日起正式施行。所以當大眾對個資防護的意識日益高漲後，勢必會要求擁有或使用這些個資的企業、組織對隱私資料能善盡更多管理責任。維護及落實資料管理制度，歐盟1995年資料保護指令GDPR

表五、資訊網路科技資訊安全威脅趨勢分析表

(自行整理)

個人資料以及憑證外洩攻擊激增	越來越多攻擊將鎖定員工家中連上網際網路裝置，此威脅與個人在企業使用自身裝置(BYOD)資訊安全風險極為類似。
針對帳號密碼攻擊更多	從消費者面向來看，最受關注威脅變化，有兩個最重要，一是網路釣魚案例在2019年將大幅增加，成為網路犯罪者主要惡意攻擊管道，另一是帳戶資料外洩，網路用戶遭盜用詐騙事件將不斷增加。
網路釣魚威脅再次攀升	根據趨勢統計以網路釣魚威脅態勢分析，所攔截網路釣魚相關網址數量逐年攀升，並從2017年的7千3百萬個，劇增到了2018年2億1千萬個。
注意帳密填充攻擊威脅	針對帳戶資料外洩所衍生的問題，趨勢特別引用了Ponemon Institute與Akamai報告內容指出帳密填充攻擊(Credential Stuffing)越來越嚴重，此撞庫攻擊手法，會利用大量外流的電子郵件地址和密碼，並透過自動化的方式來嘗試入侵。
工業控制系統漏洞被關注比例提升	很多工業控制系統漏洞是出現在管理SCADA(Supervisory Control And Data Acquisition)系統軟體的人機介面HMI(Human Machine Interface)，在此，具有系統監控和資料擷取功能的軟體，稱之為SCADA軟體。它是架構在PC之上的生產自動化及控制系統。此類型軟體的應用範圍很廣，舉凡電力、水利系統、石油、化工、汽車業都是其應用領域，趨勢預期將有更多關於HMI漏洞被揭露。
針對路由器、網路監視器、印表機、網路儲存系統(NAS)網路連線運作物聯網設備攻擊	2018年的Mirai變種VPNFilter，Cisco Talos首度於2018年5月揭露時，受害範圍遍及54個國家，約有50萬臺裝置受害。2018年最具代表性的物聯網裝置惡意軟體屬Mirai變種的VPNFilter，由俄羅期駭客集團Fancy Bear(或稱APT28)所採用，這個惡意軟體能夠感染的網路設備，包含了華碩、D-Link、華為、Linksys、MikroTik、Netgear，以及TP-Link等廠牌的路由器，還有QNAP的網路儲存設備。

中，便加入資料的「被遺忘權」，讓個人可要求企業組織抹除、使用其個人資料等，這些都是企業組織所需正視的資安議題。據趨勢科技2019年資安預測報告顯示，網路威脅者開始利用AI人工智慧發動目標式攻擊，透過AI預測判定企業管理階層和特定對象相關動向，進而取信周圍相關人士進行入侵威脅；資安廠商也已運用人工智慧模擬以偵測任何潛在網路威脅，提供企業與消費者多層式防護，2019年趨勢預測資訊安全威脅警示整理分析如表五[11-12]。

趨勢科技公布2019資安預測資料外洩攻擊迅速攀升、網路釣魚攻擊次數頻繁、工業控制系統(Industry Control System)威脅增加、企業與個人資安意識內化，採取跨世代防護技術多層式保護連網安全。事實上，在現今多元裝置以及操作系統趨勢下，駭客將不再透過以往單一軟體系統層面的漏洞攻擊套件模式，轉而利用社交工程鋪天蓋地式來進行網路釣魚攻擊。在此所指社交工程(Social Engineering)是指通過與他人的合法地交流，來使其心理受到影響，做出某些動作或者是透露一些機密資訊的方式。其中值得我們注意新興的資訊安全攻擊手法，包括，網路犯罪集團藉由入侵網路紅人的社群媒體帳號，藉此執行水坑式攻擊，藉由追隨者管道以及粉絲信任的心理，散布惡意程式(Malicious Codes)；利用聊天機器人(ChatBot，是經由對話或文字進行交談的電腦程式)來執行詐騙攻擊與互動式語音應答電話詐騙將成為網路攻擊威脅新趨勢。根據Kaspersky公布的2018上半年度報告，從物聯網裝置裡發現的惡意軟體共121,588種，比起2017年要多出將近3倍。雖然物聯網裝置使用量的增長，每年都以數十億的規模增加，駭客認為對物聯網裝置下手有利可圖而投入開發相關的惡意軟體，資安威脅也會因物聯網裝置數量增加而延續下去[12-13]。

肆、全球資安規範發展與資訊安全風險管理理論技術探討

此章節針對全球資訊安全規範發展與資訊安全風險管理理論技術分析探討，歐盟提出號稱史上最嚴個資法GDPR實施後，全球企業都在努力適應，美國為了抗衡GDPR推出加州隱私法案和物聯網法案，擴大個資保護範圍，而美國財經雜誌《財星》(FORTUNE)全球500大企業並投入了80多億美元做合規技術。目前的合規方案，通常都是基於國際資通安全標準，但仍可能被歐盟資料保護委員會(EDPB)認定為不符合GDPR標準。因此，EDPB正在規劃推出GDPR認證標準，並發布認證機制。我國對於資通安全管理法的施行，重點在於資安是持續精進的風險管理，每個機關都應做落實資安風險的辨別並強化辨別資安風險的能力。值得一提的是，過去偏重在公務機關，現在納管範圍擴大，增加特定非公務機關，也是比較不同之處，此外，還有在

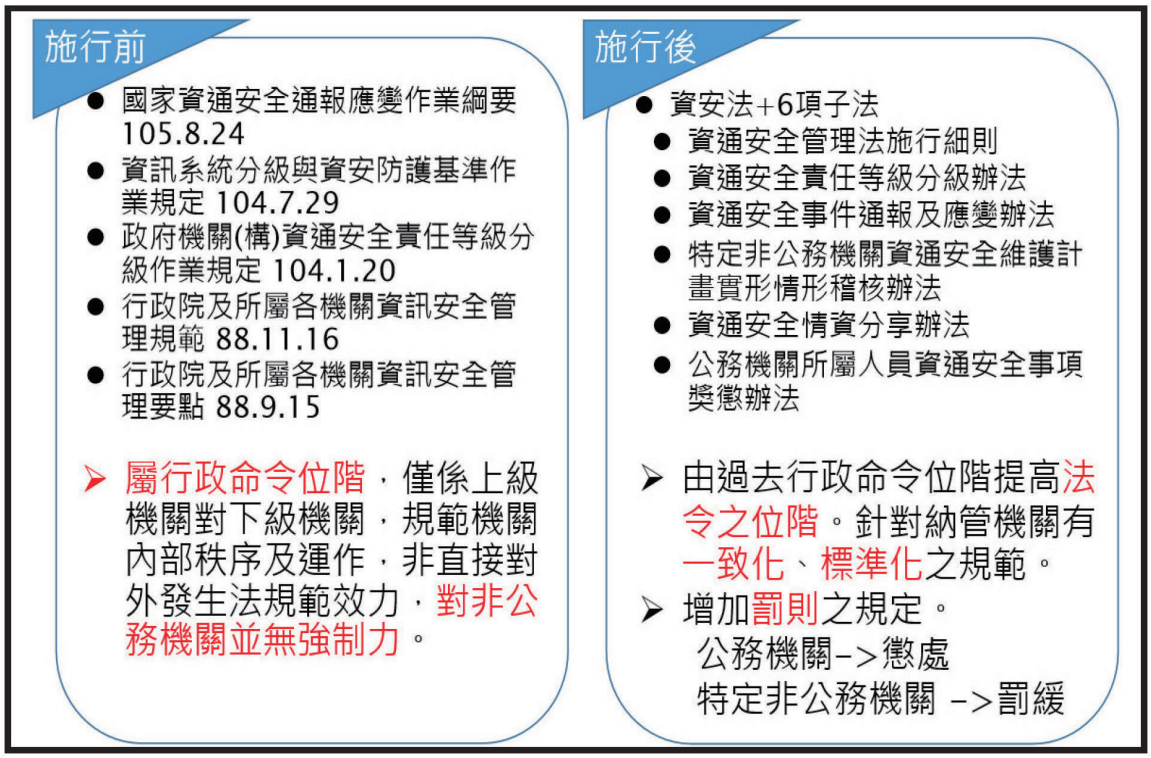
表六、影響我國組織或企業的法遵議題表

（自行整理）

我國資通安全管理法	全國法規資料庫於2018年06月06日公布，2019年1月1日正式實施「資通安全管理法」。關於通訊軟體安全，在資安管理法訂定之後，目前資安處也正重新檢討整個政府機關內部資訊與相關的規範，通訊軟體就是焦點之一。隨著國際間針對華為與中國製造設備爭議持續延燒，期盼促進網路、資安設備自主研發腳步，並獲取躍上國際舞臺的機會。
加州隱私法與物聯網(IoT)裝置資訊隱私法	美國加州議會2018年6月通過的「加州隱私法」，預計在2020年7月實施，而這項法案可能會影響到美國「聯邦隱私法」制定。美國加州2018年9月通過，預計2020年1月1日實施的「物聯網(IoT)裝置資訊隱私法案」(SB-327 Information Privacy: Connected Devices)。加州議會於今年9月通過全美第一個物聯網(Internet of Things, IoT)裝置的資訊隱私法案(Information Privacy: Connected Devices)，待加州州長Jerry Brown簽署之後預計於2020年的1月生效，成為美國第一個IoT法案。該法案主要規定IoT裝置的製造商必須提供合理的安全功能，明確規範任何可自區域網路之外登入的連網裝置都必須符合以下兩者之一的身分認證規定，一是若裝置使用的是預設密碼，那麼每個裝置所配置的預設密碼都必須是獨特的，二則是在使用者首次設定該裝置時，必須提醒使用者設定自己的密碼。
歐盟第二次支付服務指令(PSD2)監理技術標準(RTS)	歐盟第二次支付服務指令(Second Payment Services Directive，PSD2)與監理技術標準(Regulatory Technical Standards，RTS)，在2018年1月13日正式生效的歐盟第二次支付服務指令(Second Payment Services Directive，PSD2)，強調金融銀行業者要開放API給第三方服務業者或外部人員，使其可以存取資料，其中，PSD2的監理技術標準(Regulatory Technical Standards，RTS)預計要在2019年9月才會推出。

管理面、技術面與政策及整合面的改變。在資安管理法納管對象中，分為公務機關與特定非公務機關，其中後者又分為三類，包括關鍵基礎設施提供者、公營事業，以及政府捐助的財團法人。在資通管理法細節的子法於2018年11月發布後，2019年1月1日已經正式施行。施法前後的差異如下，過去政府在資安防護的要求上，規範屬行政命令位階，在資安管理法施行後，現在提高為法令之位階，因此針對納管機關有一致化、標準化之規範，影響我國組織或企業的法遵議題分析如表六，我國資通安全管理法的施行前後比較說明如圖三[14-15]。

美國歷經從國家弱點資料庫(National Vulnerability Database)到國家查檢表計畫(National Checklist Program)，更進而整合規範安全內容自動協定(Security Content Automation Protocol)並且加以實作，之後美國正式提出以資訊安全護理為基石的「人員支援技術操作執行(People Executing Operations Supported by Technology)」之資訊安全管理實作並進行一連串之軟體保證的標準化工作項目。為落實前述計畫，2002年1月23日，美國參眾兩院通過數位安全研究與發展法(Cy-



資料來源：行政院資通安全處[14]

圖三、我國資通安全管理法的施行前後比較說明

ber Security Research and Development Act)，**經由國家弱點資料庫(Vulnerability Database)**與國家查檢表計畫建立資訊產品弱點管理、安全性測量及其遵循之自動化致能標準，並經由2002年11月14日公布的聯邦資訊安全管理法(Federal Information Security Management Act)，責付美國國家標準與技術研究院(National Institute of Standards and Technology，簡稱NIST)制定相關標準系統[16-17]。

英國標準協會(British Standards Institution; BSI)為世界上第一個國家標準化機構，ISMS是由英國標準協會所提出國際資訊安全管理標準BS 7799-2發展而來，**ISO/IEC27001是ISO國際標準組織驗證規格。資訊安全管理系統(Information Security Management System**，簡稱ISMS)是一套有系統地分析和管理資訊安全風險的方法。對內讓企業組織具備安全管理能力建立「安全等級」資訊管理制度並且為資訊架設一套安全防護機制，有效對外防範電腦病毒、蠕蟲、木馬程式惡意程式(Malicious Codes)攻擊及駭客入侵，當遭受資訊安全威脅與攻擊時，系統仍可維持正常運作能力。新版ISO標準發行及時的提供對資訊安全管理系統(ISMS)的整體概念，為整體管理系統的一部份，以營運風險方案為基礎，用以建立、實施、操作、監

表七：資訊安全管理系統(ISMS)資訊安全管理制度建置規劃階段表

(自行整理)

安全需求分析	1.專案執行計畫書。 2.專案啟始會議簡報資料。 3.資安需求與現況分析。
資安與流程教育	1. ISMS 建置課程教材。 2. ISO27001 介紹。 3.資訊安全管理系統介紹及建置。
安全政策/架構	1.資訊安全政策第一階與第二階文件。 2.資安組織建議報告。
風險評鑑	1.風險評鑑工具。 2.風險評鑑報告。 3.風險處理計畫書。
風險處理	1.資訊安全政策第三階與第四階文件。 2.適用聲明書。 3.資安管理文件與管理工具。

督、審查、維持及改進資訊安全。行政院國家資通安全會報技術服務中心指出資訊安全管理的目標是透過控制方法，把資訊風險降低到可接受的程度內進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保資訊蒐集、處理、傳送、儲存及流通之安全。以上表七為資訊安全管理制度建置規劃階段表[18-20]。

伍、結語與因應作為

解析資訊安全的定義與重要性，可以從人、科技、流程等三個方向來思考，跟人有關的部分包括對人的訓練與認知上的建立、認證、實體安全、人員安全、資訊系統安全監督等，在科技方面則有科技的層次、安全的準則、IT/IA(Information Technology /Information Assurance)的獲得、風險評估、驗證與鑑定等，與流程相關的則有評估、監督、入侵偵測、警告、應變、回復等流程。以醫療隱私資訊安全為例說明，醫療產業具高度醫療專業、精密儀器設備及巨量病患隱私等特性，在日益提高的資訊化與儀器設備逐步聯結網路趨勢下，網際安全與隱私保護已成為醫療產業面對的重大挑戰。我國醫療的發展面向包括在醫療服務內容上，未來醫療將由急重症的醫治擴及到日常的健康促進工作上。隨著網路與穿戴式裝置的崛起，配合適當個資保護下，醫療專業將在疾病發生前就可以開始提供醫療服務。具備聯網能力醫療器材的弱點管理分析，醫療產業為關鍵基礎設施之一，國內醫療院所配置

多項新進器材，因應技術進步，其中絕大多數器材均具備聯網能力，但具備聯網能力之醫療器材，在醫療體系中多為醫學工程部門管理，而非資訊部門，2019資安法年施行後，在管理範圍中若能將此部分納入，可大幅提升醫療產業整體資訊安全。面對未來連網技術、物聯網、雲端與跨平台連網趨勢，單位組織不應僅依靠單一資安工具，應採取跨世代的威脅偵測技術，在正確時刻採取有效防護策略；我們尤其更應培養資安意識，對於電子郵件或是通訊軟體上的訊息提高警覺，降低遭受社交工程攻擊網路釣魚詐騙風險，或可透過安裝防毒軟體協助保護個人資料與交易安全，此外，除了定期更新密碼，使用多重認證的帳密保護措施，以及密碼管理工具以保護相關憑證資訊，也可幫助個人機密資料的保護[21-23]。

針對網路惡意程式威脅分析，去年數位勒索攻擊是網路犯罪集團獲利的主要模式，同時也將促使歹徒朝各種可能帶來龐大獲利的詐騙手法發展。物聯網(IoT)裝置的漏洞將擴大歹徒可利用的打擊面，因為未來將有更多這類裝置出現在各種智慧型環境。變臉詐騙(Business Email Compromise，亦稱「商務電子郵件入侵」，簡稱BEC)，將使得更多企業機構陷入騙局，遭受嚴重的財務損失。假新聞和網路宣傳的時代將與傳統網路犯罪技巧並存。機器學習和區塊鏈(Block chain)技術的應用，既是機會、也是潛在陷阱。GDPR條款多達99條，其中與台灣製造業息息相關的是第25條，要求企業從設計及預設機制著手保護隱私資料(PbD)，如擬匿名化和資料最小化等安全控制措施。繼《歐盟通用資料保護規則》(EU General Data Protection Regulation，GDPR)在2018年5月實施，以及美國加州於去年6月通過了有輕量版GDPR之稱的隱私法案之後，Google並於2018年9月24日發表《負責任的資料保護規定框架》，以期作為未來美國立法的參考依據。Google隱私長Keith Enright表示，《負責任的資料保護規定框架》是基於既有的隱私框架及Google對全球資料保護法案的經驗，框架中的準則有助於評估新的立法，同時倡導負責任、互動與適用的資料保護規定。相關的準則涉及蒐集與使用個人資訊的規範、允許使用者控制個人資訊的使用、允許使用者存取/修改/刪除/下載個人資訊、區隔消費者服務與企業服務、採用符合國際規範地理範圍及鼓勵全球互通性等[24-26]。

就個人資料保護角度探討，隱私工程組成元件，很大一部分來自於各種法令的要求，尤其是單位組織針對使用者提供各種產品和服務，需要滿足隱私需求時，都會跟法令有關。再者，依照各種使用情境不同，進行風險評鑑後，便會導引出不同的風險模型，也經常會出現需要重新再識別的風險；當依照不同風險模型做風險評估後，所設定提供服務須有對應系統能力與需求，同時，也要確保資訊系統可以滿足需求並對應風險。對於資訊安全議題的重視，國家安全會議2018年9月14日發布

我國首部資通安全戰略報告，推強調資安即國安策略方針，對內凝聚政府推動資安政策量能，促進資安產業發展；對外則達成資安策略宣導，同時促成國際合作之目的。為落實此三大目標，行政院則在106年通過4年期的「國家資通安全發展方案」，為有效強化我國資通電能力，國防部也結合國防戰力成立資通電軍指揮部。資訊安全防護作為需要做到即時性、簡易性，須提供高可視度與防護性，來涵蓋來自多面向的資訊威脅，並整合多樣化的技術以防護偵測進階威脅的入侵攻擊，經由持續性的自動化檢測評估，確保資安系統自身維持最優化配置。網路科技發展迅速讓我們正面臨著各種內部威脅、進階威脅偵測、關鍵資產保護、事件回應、合規檢查、管理弱點風險、雲端安全等議題，應有效地識別與資料相關的安全和合規風險，落實弱點掃描來識別資料庫以避免稽核失敗，並將風險降至最低，強化資訊緊急應變作為，以期達到永續完善的資訊安全管理目標[27-30]。

參考文獻

[1]資安人科技網，網路科技帶來的連鎖效應，2018年07月09日，編輯部-Information Security資安人科技網焦點新聞，https://www.informationsecurity.com.tw/article/。
[2]行政院國家資通安全會報，國家資通安全發展方案(106-109年)，行政院國家資通安全會報，2019年05月01日存取，第1-58頁。
[3]行政院新聞傳播處，「DIGI＋方案」推動成果一朝智慧國家邁進，2018年7月31日，取自https://www.ey.gov.tw/Page/。
[4]全國法規資料庫，個人資料保護法，2015年12月30日，法務部全國法規資料庫，法規類別：行政院國家發展委員會，公告取自https://law.moj.gov.tw/ LawClass/LawAll.aspx?PCode=I0050021。
[5]資安人科技網，透過網路科技的應用所帶來的個資風暴，2018年07月23日，編輯部-Information Security資安人科技網焦點新聞，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=8651。
[6]資安人科技網，國家安全與經濟發展重要的基石，2018年10月08日，編輯部-Information Security資安人科技網焦點新聞，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=8673。
[7]行政院新聞傳播處，政院：盼跨界合作迎接5G世代實現「智慧生活」，行政院DIGI+小組會議，2018年10月3日。
[8]經濟部，個人資料保護作業手冊107年3月版，經濟部法規委員會，取自https://www.moea.gov.tw/MNS/colr/content/SubMenu.aspx?menu_id=7783。
[9]吳其勳，圖解個資法，2012年12月25日，iTHome電週文化事業，取自https://www.ithome.com.tw/article/87965。
[10]羅正漢，2019資安預測趨勢提七大重點:資料外洩通報與網路釣魚將大增，2019年1月5日，iTHome電週文化事業，取自https://www.ithome.com.tw/ news/127899。
[11]iTHome電週文化事業編輯部，【iThome企業資安大調查】企業今年資安投資重點為何？，2019年4月1日，iTHome電週文化，取自https://ithome.com.tw/article/129708。
[12]趨勢科技，趨勢科技公布2019資安預測，2018年12月19日，趨勢科技Trend Micro官網,取自https://www.trendmicro.com/zh_tw/about/newsroom/press-releases/2018 /2018-12-19。
[13]周峻佑，【2019資安十大趨勢2】大規模攻擊橫跨多廠牌物聯網裝置，受害範圍持續擴張，2019年1月7日，趨勢科技官網,取自https://www.ithome.com.tw/news/127995。
[14]羅正漢，臺灣資通安全管理法上路一個月，行政院資安處公布實施現況，2019年2月15日，iTHome電週文化事業，取自https://www.ithome.com.tw/news/128789。
[15]黃彥棻，【2019資安十大趨勢4】臺灣政府組織受資安法規範，美國提加州隱私法與物聯網法案保護個資，2019年1月8日，iTHome電週文化事業，取自https://www.ithome.com.tw/news/128789。
[16]林祝興、張明信，資訊安全概論(第三版)，旗標文化，台北，2017年，第10-22頁。

[17]樊國楨、黃健誠，ICT產業風險管理標準：ISO/IEC 27036，2012年10月12日，Information Security資安人科技網，取自https://www.informationsecurity. com.tw/article/article_detail.aspxaid=7095。
[18]蔡昀臻、樊國楨，個人資料管理系統驗證要求事項標準化進程初探：根基於ISO/IEC JTC 1/SC 27在2017-01公布的框架，2017年10月1日，資訊安全通訊，23卷4期，第1-36頁。
[19]行政院國家資通安全會報技術服務中心，ISMS風險評估手冊，2003年12月25日公告取自https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1206。
[20]SGS管理學院，歐盟GDPR全面啟動SGS提對策邀請歐盟專家來台解析，2018年6月28日，經濟日報，取自https://www.sgs.com.tw/zh-tw/news/2018。
[21]黃彥棻，【GDPR施行後的法遵議題】深度剖析隱私工程，2018年11月26日，iTHome電週文化事業，取自https://www.ithome.com.tw/news/127226。
[22]邱述琛、廖彥鈞，2019資安法施行後醫療產業如何具體強化資訊安全，2019年03月14日，Information Security資安人科技網，取自https://www.informationsecurity. com.tw/article/article_detail.aspx。
[23]劉士成，不用再瞎禁中國通訊設備先看各國的資安防護安全標準，2019年1月27日，奇摩轉載NOWnews今日新聞，取自https://tw.news.yahoo.com/amphtml。
[24]陳曉莉，美國政府擬徵詢Amazon、蘋果、Google等科技巨頭，準備打造自家版的GDPR，2018年9月26日，iTHome電週文化事業，取自https://www.ithome.com.tw/news/126091。
[25]財團法人台灣智庫，國會政策研究中心，關鍵基礎設施安全條例(CIIP)—國家資通安全的第一哩路，2017年3月10日存取。
[26]行政院研考會，資訊系統風險評鑑參考指引(修訂)v2.0，2019年05月21日存取。
[27]行政院國家資通安全會報技術服務中心，美國NIST發布網路安全事件回復指引，國家資通安全會報資通安全資訊網，2019年5月20日存取，http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf。
[28]黃彥棻，【GDPR施行後的法遵議題】深度剖析隱私工程，2018年11月26日，iTHome電週文化事業，取自https://www.ithome.com.tw/news/127226。
[29]Information Security資安人科技網編輯部，製造業所面臨的資安管理挑戰及趨勢，2019年5月20日，Information Security資安人科技網專題訪問，取自https://www.informationsecurity.com.tw/article/article_detail.aspx。
[30]中華民國總統府，國家資通安全戰略報告-資安即國安，總統：今年國家安全會議提出了我國首部資安戰略報告，為數位國家、創新經濟奠定堅實基礎，政府資訊公開，2018年9月14日，https://www.president.gov.tw。

作者簡介

空軍備役上校　吳嘉龍

學歷：中正理工學院48期電機系電子組、美國空軍理工學院電腦工程碩士、國防大學理工學院國防科學研究所電子工程組博士。經歷：電子官、區隊長，教官、講師、助理教授、科主任、校教評秘書、副教授、教授、系主任、圖書館館長、資圖中心主任。現職：日月光半導體製造股份有限公司資訊處顧問、危機管理學會理事兼資訊安全主任委員。