● 電子化政府資通安全推動現況與展望

一、政府資通安全威脅分析

隨著電子化政府的普及推動，政府機關應用資通訊科技的程度也越深。近年來政府機關電腦病毒、駭客入侵及個人資料外洩等資安事件迭有發生。政府資通安全不僅影響國家安全、社會安定及一般民眾權益，同時亦影響人民對於政府提供網路服務的信心，值得各界重視。

因應「個人資料保護法」修正通過後對政府機關造成的衝擊與影響，政府機關應依據個資法相關規定研擬配套措施，加強推動個人資料安全防護。今後，電子化政府推動工作必須在兼顧促進個人資訊合理流通及防止個人隱私權受到侵害情形下，提供安全及可信賴的便民服務，以提升民眾使用網路服務之信心。

針對政府資通安全威脅來源進行分析，可分爲外部威脅及內部問題，分別說明如下：

(一)外部威脅

1、組織型駭客針對性攻擊
2、鎖定特定對象或單位
3、攻擊形式變化快速

(二)內部問題

1、政府資安人力、經費及能量相對不足
2、資安事件通報意願不高
3、委外開發軟體及品質管理問題
4、資訊作業委外處理衍生資安管理問題
5、公務人員資安意識不足
6、各機關橫向聯繫機制尚待建立
7、資安相關法令尚未完備

二、國際資通安全發展趨勢

(一)爲提升網路安全，美國全面檢討網路安全整體策略

美國總統歐巴馬於 2009 年 5 月 29 日公布「網路政策評估(Cyberspace Policy Review)」報告指出，美國承諾建立起可靠且堅固的資通訊基礎建設。有鑑於網路安全問題的複雜性與重要性，於美國白宮設立網路安全政策官(Cybersecurity Policy Official)，負責統整與協調美國網路安全相關事務，並對美國國家安全委員會(National Security Council)與美國國家經濟委員會(National Economic Council)報告。

因應越來越多針對性的網路攻擊及駭客入侵，美國白宮於 2011 年 5 月提出網路安全計畫，以確保一般大眾使用網路之安全性、國家網路基礎架構防護及政府網路安全防護。同時並提出國際網路安全策略，以提升國家網路安全防護能量。

(二)DDOS 攻擊已成爲網路攻擊的主流

Arbor Networks 公司 2010 年全球網路基礎架構安全報告指出，DDOS 攻擊已經成爲目前網路攻擊的主流，報告重點說明如下：

1、DDoS 攻擊已成爲主流
2、DDoS 攻擊規模與頻率增快
3、DDoS 攻擊層面擴大
4、應用層的 DDoS 攻擊數量增多
5、DDoS 攻擊導致 IPS 與防火牆無法運作

6、IPv6 的資安問題

(三)個人隱私資料被竊與金融詐騙事件頻傳

駭客透過電子郵件社交工程或利用網站應用程式漏洞、網頁掛馬等方式，在受害電腦植入惡意程式，以竊取個人隱私資料，並與犯罪集團合作進行金融詐騙事件頻傳。

「個人資料保護法」於 99 年 4 月 27 日三讀修正通過，主要在規範個人資料之蒐集、處理及利用，以避免人格權受到侵害，並促進個人資料之合理利用。強化政府機關個人資料安全防護，將成爲電子化政府資通安全推動重點工作之一。

(四)關鍵基礎建設資安風險增加

在美國 911 恐怖事件後，關鍵資訊基礎建設保護措施(Critical Information Infrastructure Protection, CIIP)開始受到各國重視，尤其是關鍵基礎建設所隱藏的脆弱性，常爲恐怖份子最有興趣的攻擊目標。

2010 年起出現專門針對關鍵基礎建設的管理控制與資料擷取系統(Supervisory Control And Data Acquisition Systems, SCADA)設計的 Stuxnet Worm，會自行尋找 SCADA 系統，取得系統控制權限。Stuxnet Worm 之複雜度及針對性顯示，已有駭客針對關鍵基礎建設進行破壞行動。

(五)組織型駭客持續竊取政府資料

組織型駭客有計畫且針對性地入侵各國政府，鎖定特定單位與對象進行網路情蒐，以竊取政府機關機敏資料。美、英、法、德、紐及澳等國政府，均曾傳出疑似遭組織型駭客入侵事件。

(六)零時差攻擊造成資安防護困難

若軟體存在弱點，且未能及時修補，即讓駭客有機可乘。在軟體弱點尚未公布修補方式之前，出現的攻擊行爲即爲「零時差攻擊(Zero-day Attack)」。駭客結合電子郵件社交工程攻擊，利用假冒寄件者身分、與業務或時事相關郵件主旨等方式寄發電子郵件，其附件檔含零時差弱點，若使用者將郵件之附件檔開啓，將被植入含零時差弱點之惡意程式。

(七)網路犯罪重心已逐漸移至行動裝置平台

Cisco 2010 Annual Security Report 指出，網路犯罪的重心已經由 Windows 作業系統平台主機逐漸轉移至行動裝置平台。由於 Windows 7 作業系統更新修補程式時程縮短，入侵 Windows 系統已未如以往容易。近期由於智慧型手機與平板電腦盛行，已成爲網路犯罪下手的首要目標。

三、政府資安推動策略

行政院爲積極推動國家資訊通信安全政策，加速建構國家資訊通信安全環境，提升國家競爭力，於 90 年設立國家資通安全會報，開始推動我國資通訊安全建設。爲了保護政府資訊系統與網路之正常運作，資安會報訂頒「國家資通訊安全發展方案(98 年至 101 年)」，以加速進行國家資通安全優質環境之建構，提升電子化政府安全及國家競爭力。

爲提供安全及信賴的電子化政府服務，政府資通安全工作必須以全方位觀念永續推動，政府資通安全 3E 策略說明如下：

(一)技術工程(Engineering)：利用入侵偵測系統、防火牆系統、郵件過濾系統、數位簽章、加密技術等建構第一道防線。

(二)執行管理(Enforcement)：落實資訊安全管理政策、資安事件通報處理機制、內外部資安稽核制度、資訊安全標準及規範、產品及系統品質檢驗機制

等。

(三)教育宣導(Education)：強化資訊安全警覺訓練、資訊安全宣導、資安人才培訓、網路使用倫理等。

四、政府資安防護措施

自行政院國家資通安全會報成立以來，政府資安防護及應變機制已逐步建立，但是隨著資訊科技的普及應用，以及電子化政府應用日益深化，面對網路安全的威脅與風險，仍有必要對目前資安相關工作進行檢討，以強化政府資安整體防護能量。以下謹就資通安全之事前安全防護、事中預警應變、事後復原鑑識等不同階段，說明如下。

(一) 事前安全防護

1、 資安監控與防護

建立多重防護縱深(Defend in Depth)資安監控機制，建置政府資通安全監控平台(Government- Security Operation Center, G-SOC)，提供政府機關網路監控服務，以及早發現資安事件，降低資安風險。

2、 資安情蒐與分析

(1) 蒐集來自政府網際服務網(Government Service Network, GSN)、台灣學術網路(Taiwan Academic Network, TANET)及民間網際網路服務業者(Internet Service Provider, ISP)等網路攻擊資訊，分析駭客攻擊手法與工具，掌握資安威脅趨勢。

(2) 研究殭屍網路(Robot Network, Botnet)議題，提升Botnet偵測分析能力，並採自動化方式追蹤Botnet資訊，掌握我國Botnet散布情況，降低我國Botnet數量。

3、 資安認知與品質提升

(1) 建立政府機關資安檢測與評鑑機制

參考國際資通安全相關標準，訂定政府資安規範整體發展藍圖架構，發展政府資安相關規範及參考指引，並建立政府機關資安檢測與評鑑機制。

(2) 推動重點機關通過資訊安全管理系統驗證

為強化政府資安防護能力，提供安全及便捷的網路服務，強化民眾使用政府網路服務的信心，保護民眾隱私權益，推動資安等級 A、B 級機關通過資訊安全管理系統(ISMS)驗證。

(3) 提升公務人員資安知識與能力

為提升公務人員資安知識與能力，辦理資安技術講習、資安證照訓練、資通安全防護巡迴研討會等訓練課程，並發展資安數位學習課程。為發掘校園優秀人才，辦理「資安技能金盾獎」、「資安動畫金像獎」等競賽活動，並辦理「資安週」系列活動，以提升全民資安認知。

同時進行公務人員資安職能規劃，依據其職務與角色，規劃執行業務應具備之資安知識與技能，並建立公務人員資安能力評量制度。

(二) 事中預警應變

1、 資安事件及時發現

透過 GSOC 進行資安事件監控作業，包括資安事件管理系統、整合性惡意程式監看、使用者端警示系統、蜜網(Honeynet)與內部網路警示系統等。

2、 資安通報與應變

(1) 建立政府資通安全通報應變作業程序，協助政府機關處理及應變資安事件。

(2) 建置政府資安資訊分享與分析中心(Government- Information Sharing and Analysis Center, G-ISAC)，整合資安相關情資，進行資安訊息分享。

3、 資安健診服務

推動資安健診評量架構與追蹤管理機制，提供政府機關資安健診服務，強化政府機關資安防護能量，掌握資安防護情形。

(三) 事後復原鑑識

1、 事後系統回復

(1) 結合產官學研資源與技術能力，建立國家資通安全區域聯防運作機制，提供受駭機關資安事件處理與諮詢服務，並提升其資通安全防護能力。

(2) 規劃政府重要資訊系統異地備援機制，以提升資安事件「事後」存活能力。

2、 資安事件鑑識

(1) 研究資通安全鑑識相關技術。

(2) 協助並訓練政府機關相關人員執行資安事件鑑識作業。

五、結語

因應政府組織改造、個人資料保護法修正通過及雲端運算、行動服務等創新發展趨勢，電子化政府面臨之資安威脅與挑戰，將更為複雜與嚴峻。為持續強化國家資通安全防護能量，行政院研考會將運用雲端運算發展技術，依據「第四階段電子化政府計畫」整體發展策略，規劃「雲端資安防護整合服務計畫(101年至 105 年)」，打造新世代的政府雲端資安防護體系。本計畫將結合產、官、學、研各界資源與能量，以資安「情資、防護、職能、確保 (Intelligence、Defense、Education、Assurance, IDEA)」四個面向，提供政府雲端資安整合服務，達成「掌握資安情報價值」、「精進資安監控防護」、「強化通報應變能量」、「確保應用系統強度」及「提升資安訓練推廣」。

(本文由行政院研究發展考核委員會資訊管理處主任吳啓文 提供)