107 年第 2 季資通安全技術報告

Quarterly Technical Report


National Center for
Cyber Security Technology, NCCST

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 4
第二章　資安專題分享 6
2.1 資安法概要與重點摘錄 6
2.2 資安法因應重點與自我檢核 8
第三章　資安新興議題研討 10
3.1 DirtyAlphabet 新型態攻擊手法簡介 10
3.2 行動支付安全分析 13
3.3 掃碼換面紙 17
第四章　結論 19
資安相關活動 20
技服中心南部辦公室正式成立運作 20
學研合作交流會議 20
政府機關(構)資安稽核 20
國家資安資訊分享與分析中心(N-ISAC)技術交流會議 21
資安服務團 21
參考文獻 22

圖 目 次

圖 1　107 年第 2 季資安事件影響等級比率圖 2
圖 2　107 年第 2 季資安事件通報類型比率圖 3
圖 3　107 年第 2 季資安事件原因比率圖 4
圖 4　資安法章節 6
圖 5　DirtyAlphabet 族群之惡意程式分類 11
圖 6　行動支付運作架構圖 13
圖 7　QR Code 之支付流程 14
圖 8　Apple Pay 之支付流程 15
圖 9　Google Pay 之支付流程 16
圖 10　掃碼換面紙 18

表 目 次

表 1　資安法自我檢核表 9

摘要

隨著資通訊科技的日新月異，全球駭侵手法也越趨詭譎多變，為打造國家級資安機制，加速數位經濟發展，政府將資安提升至國安層次，宣示「資安即國安」的決心。行政院國家資通安全會報技術服務中心在行政院資通安全處指導下，期藉由每季出版之「資通安全技術報告」，從提供資安威脅現況與防護重點、分享資安專題及研討資安新興議題 3 個面向，掌握資安威脅趨勢，並落實資安防護措施，以降低資安風險，打造安全可信賴的數位國家。

「第 2 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

藉由彙整本季重要的資安事件，歸納本季全球主要的資安威脅以「物聯網設備資安弱點威脅升高」與「關鍵資訊基礎設施資安風險倍增」等 2 個面向為主。綜整分析本季政府機關(構)資安事件通報情形，主要面臨的資安威脅以「網站設計不當」與「弱密碼」等弱點為主。同時，針對「物聯網設備安全」、「關鍵資訊基礎設施安全」及「網站設計不當與弱密碼」等 3 方面，提出資安防護建議，以降低資安相關風險。

●第 2 章：資安專題分享

因應資通安全管理法施行後，公務機關與適用之特定非公務機關須落實執行相關法遵作業及配合事項，因此，本季資安專題從資通安全管理法的 5 個章節內容進行摘要介紹，並說明相關規定、適用對象及因應重點，同時，整理資通安全管理法之自我檢核表，協助適用單位進行自我檢視，以因應法規之遵循性。

●第 3 章：資安新興議題研討

本季針對「DirtyAlphabet 新型態攻擊手法簡介」、「行動支付安全分析」及「掃碼換面紙」等 3 個資安議題進行研討。在「DirtyAlphabet 新型態攻擊手法簡介」，說明駭客族群的相關背景、攻擊手法及惡意程式等，並提供防護建議。

在「行動支付安全分析」，探討行動支付之架構、支付流程、安全脆弱點及防範建議措施，以對行動支付之整體概觀與資安風險有初步的認識。最後，在「掃碼換面紙」，透過研析掃描 QR Code 資訊來換面紙之案例，說明使用者資訊的洩漏過程、資安風險及其因應之防護作為。

- 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，了解目前的資安威脅現況與因應之防護重點。藉由簡介資通安全管理法之相關規定、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，深入探討相關攻擊手法與資安風險，以掌握本季之資安威脅現況，並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

本報告藉由分析當季全球與政府之資安事件案例與統計數據，探討目前資安威脅現況，俾利政府機關(構)關注最新資安威脅趨勢，以了解其發生原因與攻擊手法，並檢視自我防護措施，進而有效因應與防範。

1.1 全球資安威脅現況

依據行政院國家資通安全會報技術服務中心(以下簡稱技服中心)所出版的「106 年資通安全技術年報」，近年來全球所面臨的資安威脅可歸納為 6 大面向，包括「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」。本報告係彙整本季全球重要的資安事件，以分析全球資安威脅現況。

在「物聯網設備資安弱點威脅升高」面向，技服中心發現組織型駭客利用「少爺殭屍網路」，針對家用路由器進行攻擊，並誘騙利用該路由器連網之使用者下載惡意 APP，以達竊取個人資料之目的。截至本(107)年 4 月止，已有 20 多萬台路由器被駭客掌控，至少 6,000 台行動裝置遭感染，該款 APP 不僅能取得手機型號、作業版本系統及應用程式列表等資訊，還能竊取受害者的 APP 帳號、聯絡人資料及簡訊內容，並可遠端撥號、接收及寄送簡訊，洩漏的個人資料超過 100 萬筆，感染範圍擴及全球 55 個國家。此外，美國國土安全部所屬之 US-CERT 於本年 4 月 16 日發布警訊，由俄羅斯政府資助的駭客正對路由器、交換器、防火牆及入侵檢測系統等網路基礎設備發動攻擊，駭客針對使用老舊協定、缺乏安全性、韌體或作業系統存在漏洞的裝置，違法獲取認證帳密進行入侵，主要目的在支援間諜行動、偷取智慧財產或持續對受害者進行網路監控，並對未來的攻擊行動奠定基礎。

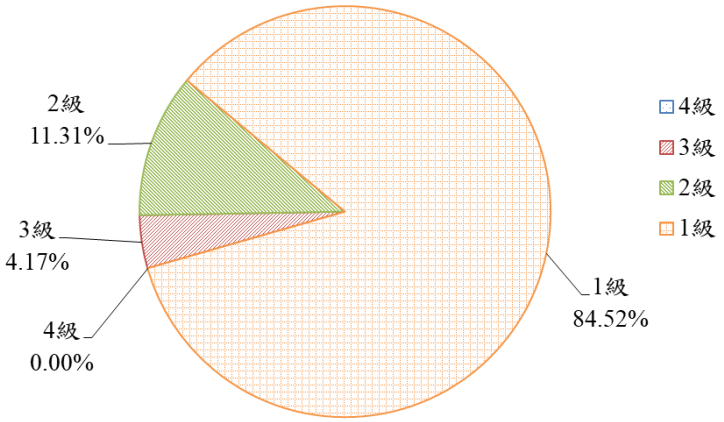
在「關鍵資訊基礎設施資安風險倍增」面向，思科(Cisco)旗下的 Talos 安全部門於本年 5 月 23 日揭露，一個已感染全球 50 萬台網路裝置的模組化惡意程式 VPNFilter。根據 Talos 的分析，VPNFilter 可長期進駐於受駭裝置上，

且對於 Modbus SCADA 協定的工業控制系統特別有興趣，它能監控裝置流量，竊取網站憑證，還能切斷裝置的連網能力或讓裝置無法使用。

觀察本季全球重要的資安事件，可發現本季的資安威脅以「物聯網設備資安弱點威脅升高」與「關鍵資訊基礎設施資安風險倍增」面向為主。物聯網的盛行，不僅代表資通訊科技的創新與應用，隨著越來越多的設備連上網路，這些創新又生活化設備的防護也成為資安的艱鉅挑戰。而在關鍵資訊基礎設施部分，因為只要關鍵資訊基礎設施發生資安事件，所影響的層面與衝擊都不容小覷，尤其在關鍵資訊基礎設施正面臨從封閉式系統逐漸轉型為開放式系統時，更多的資安風險也接踵而來。

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 2 季以 1 級事件占 84.52%為大宗，2 級事件占 11.31%次之，3 級事件僅占 4.17%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

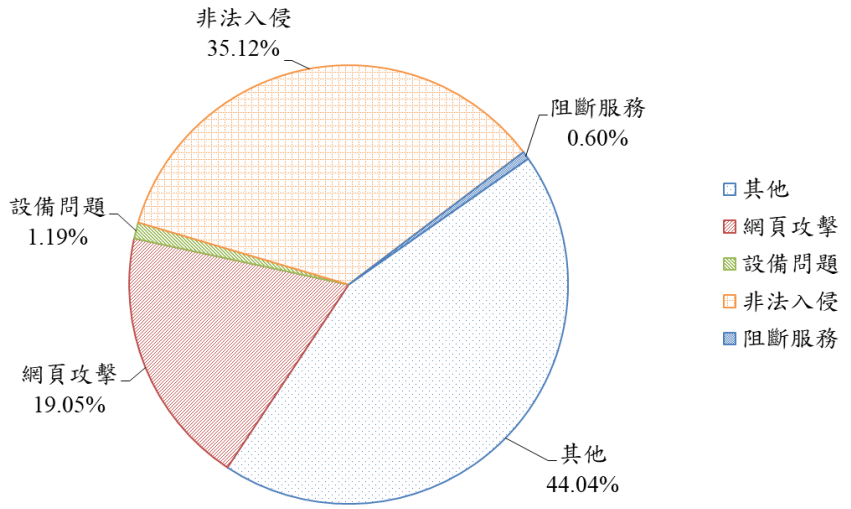


資料來源：本報告整理

圖1　107 年第 2 季資安事件影響等級比率圖

本季之通報事件以 3 級事件為最高影響等級，分析 3 級事件發生之原因，大部分為弱密碼導致系統被入侵，其次為因系統設計不當，造成個人資料外洩，再者因系統運作異常，導致核心業務運作無法於可容忍中斷時間內回復正常。

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 2 季資安事件通報類型(詳見圖 2)，發現主要以「其他」占 44.04%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」。

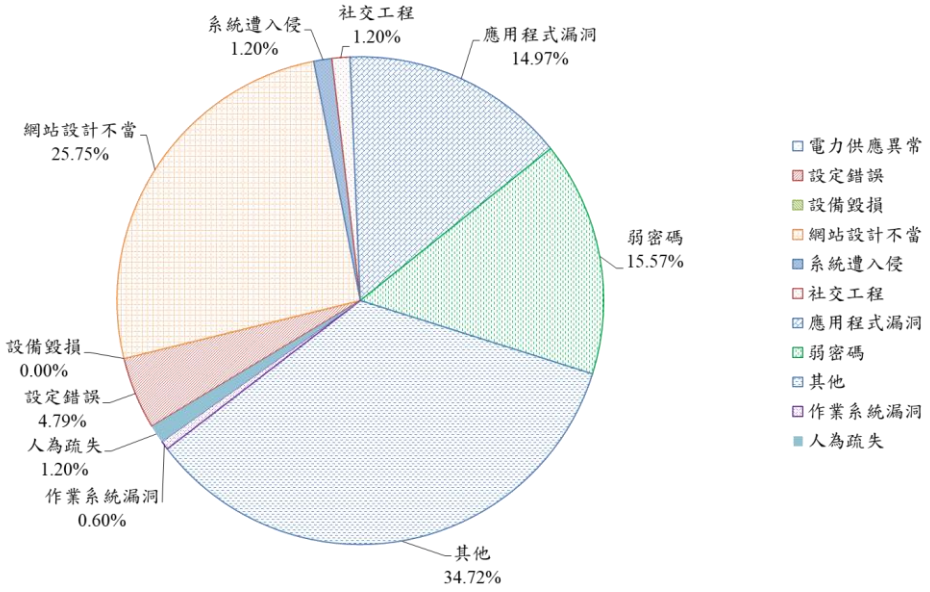


資料來源：本報告整理

圖2　107 年第 2 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，以其他(占 34.72%)、網站設計不當(占 25.75%)及弱密碼(占 15.57%)為主，詳見圖 3。在「其他」部分，以硬體設備不明原因異常，或因相關紀錄不足而無法確認事件原因為主。政府機關(構)應定期檢視系統是否有足夠的空間或資源，保存重要系統日誌且建立管理

機制，以確認在需要時可用來做為追查之證據。其次，在「網站設計不當」部分，網站開發人員應從開發階段即將網站之安全性納入考量，同時定期進行網站弱點掃描，以即早發現弱點並強化網站之安全性。此外，目前政府機關(構)資訊系統設計與維護大多委託廠商辦理，必須符合安全的系統發展生命週期，確保程式在開發週期沒有系統弱點、交付時未含後門與惡意程式，亦應適時監督與檢視委外廠商之開發或維護行為。在「弱密碼」部分，除預設密碼須變更外，更應確保密碼長度、複雜度及定期更新密碼等項目符合資安要求。



資料來源：本報告整理

圖3　107 年第 2 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，主要集中於物聯網裝置與工業控制系統的防護不足，加上民眾無足夠的資安意識，導致少爺殭屍網路與 VPNFilter 惡意程式的擴散。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「弱密碼」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：

●物聯網設備安全之防護

–變更物聯網設備之預設帳號與密碼，強化密碼複雜度並定期更新密碼。

–確保連網之安全性，包括使用安全連線、傳輸加密及完整性驗證。

–定期更新並加強系統安全組態的設定。

●關鍵資訊基礎設施安全之防護

–加入各關鍵基礎設施領域之資安資訊分享與分析中心，以即時分享與交換與關鍵資訊基礎設施相關資安情資。

–隔離或嚴格控管網際網路與關鍵資訊基礎設施之連線。

–建置防火牆與入侵偵測防禦系統，並定期稽核所有連網的裝置與設備。

●網站設計不當與弱密碼

–導入安全資訊系統開發流程，確保程式開發流程在每一階段之資安要求。

–上線前與正式運作時，定期執行安全性檢測與漏洞修補。

–檢視與委外廠商之合約，是否包括資訊安全條款與要求，並定期監督與管理。

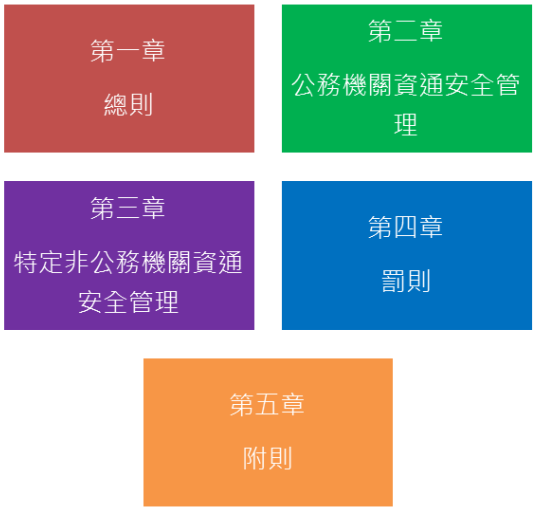
–變更預設密碼，並確保密碼長度、複雜度及定期更新密碼等項目符合資安要求。

第二章　資安專題分享

資通安全管理法(以下簡稱資安法)於本年 5 月 11 日立法院三讀通過，資安法的立法核心宗旨在積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。本季的資安專題分享將簡介資安法之相關規定、適用對象及因應重點，以了解資安法之相關重點。同時為使公務機關與適用之特定非公務機關清楚優先要務，亦整理資安法自我檢核表，協助先行自我檢視，進行差異分析後，規劃與排定相關資源，以因應法規之遵循性。

2.1 資安法概要與重點摘錄

在政府擘劃出「資安即國安」之策略目標後，資安法的通過更象徵政府積極在各個層面架構國家層級資安防護設施，亦成為我國資安發展眾所矚目的里程碑，更是重要的法規基礎。長期以來，在公務機關不餘遺力推動各項資安防護策略與措施外，此次資安法除公務機關外，更將關鍵基礎設施提供者、公營事業及政府捐助之財團法人等特定非公務機關納入適用範圍，以期透過法律強制之要求，達到重要資訊環境之安全完備度。資安法共分為 5 章(詳見圖 4)，各章之重點說明如下。



資料來源：本報告整理

圖4　資安法章節

第一章、總則。說明資安法之核心宗旨與主管機關為行政院，並透過名詞定義說明資通系統與資通安全事件等項目，同時介紹資安法之適用對象，包括公務機關與特定非公務機關(關鍵基礎設施提供者、公營事業及政府捐助之財團法人)。

再者，藉由主管機關應負之相關責任，以期達到平時情資分享與監督管理之責，相關責任包括訂定資通安全責任等級之分級與稽核特定非公務機關資通安全維護事項之完備度，並持續追蹤改善情形。鑒於資通系統與服務委外案件安全疑慮之新聞層出不窮，資安法亦針對委外辦理資通系統之建置、維運或資通服務之提供，要求委託機關應妥適選任及監督受託者。

第二章、公務機關資通安全管理。說明公務機關應訂定、修訂及實施資通安全維護計畫，並每年提出該計畫之實施情形，若經稽核有缺失或待改善者，則應提出改善報告。此外，亦明訂公務機關應置資通安全長，負責推動及監督機關內資通安全相關事務。為因應資通安全事件，除須訂定資通安全事件通報及應變機制外，亦須依規定辦理通報及應變。而為促進公務機關所屬人員對於資通安全工作之重視與投入，若該等人員踐行本法要求事項績效優良者，則應給予獎勵。

第三章、特定非公務機關資通安全管理。關鍵基礎設施提供者、公營事業及政府捐助之財團法人等特定非公務機關，應適用資安法之規定，並依其中央目事業主管機關之要求辦理資通安全相關事項。特定非公務機關均須善盡訂定、修正及實施資通安全維護計畫、辦理資通安全事件之通報、應變及訂定相關機制等義務，而考量關鍵基礎設施服務對我國資通安全環境之穩定性甚為重要，若關鍵基礎設施受影響而無法於可容忍中斷時間內回復運作，恐生社會公共利益之危害，更有甚者將影響國家安全。因此資安法課予關鍵基礎設施提供者較其餘特定非公務機關較高之資通安全義務，其應提交資通安全維護計畫實施情形，而其中央目的事業主管機關亦應稽核該計畫實施情形，而其餘特定非公務機關僅於其中央目的事業主管機關要求時，方須提交資通安全維護計畫實施情形，而其等之中央目的事業主管機關亦為得辦理該等計畫實施情形之稽核。

第四章、罰則。為促進公務機關所屬人員對於資通安全工作之重視與投入，

若該等人員違反資安法所定義務者，其所屬機關應按其情節輕重予以懲戒或懲處。而於特定非公務機關部分，資安法係針對其未依規定訂定、修正、實施資通安全維護計畫、提出資通安全維護計畫之實施情形、改善報告送交中央目的事業主管機關、訂定資通安全事件之通報及應變機制、通報資通安全事件、向中央目的事業主管機關提出資通安全事件之調查、處理及改善報告，或違反資通安全事件通報內容之規定等情形，課予金額不等之行政裁罰。

第五章、附則。說明資安法相關施行細則與施行日期，由行政院訂定。

2.2 資安法因應重點與自我檢核

資安法的通過所代表與象徵的意義，著重於如何在法規的要求下，檢視現行資安防護機制，以達到落實資安管理的目的。因此，歸納資安法的重點主軸包括以下 3 點：

- 資通安全長或資安專責人員，以負責推動及監督資通安全相關事項。
- 訂定、修訂及實施資通安全維護計畫，並定期以稽核等方式檢視該計畫之完備程度，若有缺失或待改善者，則應提出改善報告，並持續改善。
- 訂定資通安全事件通報及應變機制，並完備其通報及應變程序。

組織在面臨一個新法的通過，面對接踵而來的因應挑戰，勢必要規劃相當資源的投入。而因應上述摘錄之重點，參考目前規劃之資通安全維護計畫應備項目，擬定以下資安法自我檢核表(詳見表 1)，提供先行檢視與資安法之整體差異性，以逐步縮小適法性之差距。其中，僅適用於公務機關之項目以符號「▲」進行標示。

表1　資安法自我檢核表

項目	檢核項目
1	盤點與釐清核心業務及其重要性，落實資通系統之安全管理
2	訂定資通安全政策，並應於各內部單位建立與資通安全政策一致之資通安全目標
3	規劃資通安全推動組織，應配置資安專責人力及資源，以達成資通安全政策及目標 ▲公務機關應配置資安長
4	盤點資訊及資通系統，並標示核心資通系統及相關資產
5	依上述盤點結果之範圍評估資通安全風險，以了解如資訊儲存區域、組織面、實體面、技術及作業面等資通安全風險，並依風險評估結果，訂定適切之資通安全防護及控制措施
6	訂定資通安全事件通報、應變及演練相關機制，並完備其通報及應變程序
7	訂定資通安全情資之評估及因應機制，於收受資通安全情資後，應評估情資之內容，並據以決定是否就資通安全維護計畫、資通安全事件通報、應變方式或其他資通安全維護事宜為調整及因應
8	訂定資通系統或服務委外辦理之管理措施，若有委外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，並適時進行監督與管理
9	▲公務機關應建立機關所屬人員辦理業務涉及資通安全事項之考核機制，適時監督與管理資通安全事項辦理之成效
10	建立資通安全維護計畫及實施情形之持續精進及績效管理機制，資通安全維護計畫需提出實施情形報告，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

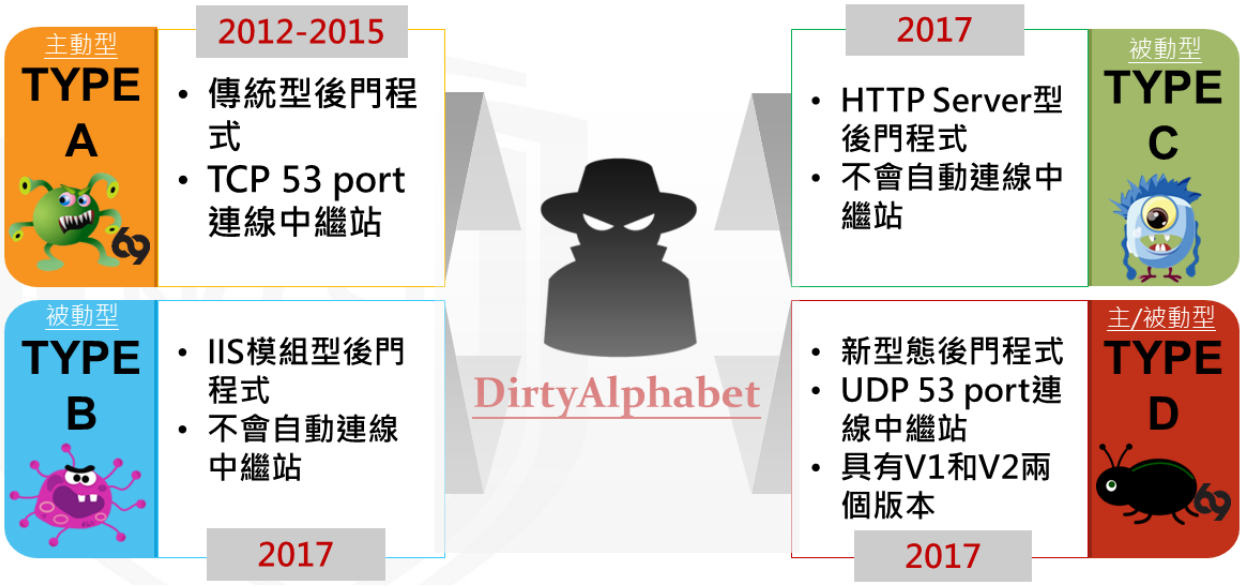
新興科技的崛起與應用，帶來另一波資安新興議題。面對無法預測與變化多端的攻擊手法，洞燭先機或知己知彼反而是正視資安威脅的方法。因此，資安新興議題將針對「DirtyAlphabet 新型態攻擊手法簡介」、「行動支付安全分析」及「掃碼換面紙」等議題進行資安研析，以了解新興攻擊手法所隱含的未知威脅，以及日常行為可能發生的資安風險，透過這些議題的研討，協助強化資安防護，同時宣導民眾在使用新興科技時，應有之資安意識。

3.1 DirtyAlphabet 新型態攻擊手法簡介

技服中心經由長期的追蹤與分析，近期掌握組織型駭客 DirtyAlphabet 所使用的新型態攻擊手法。有別於一般後門程式，DirtyAlphabet 族群善於使用 DNS 服務來做為後門主動報到與被動等待命令的途徑。由於在一般網路環境中，防護設備並不會特別將 DNS 流量納入偵測與監控的範圍，故駭客可將惡意程式藉由 DNS 的通訊過程植入受害主機，以達成隱匿行跡與後續操控之目的。

本次發現的新型態攻擊手法以社交工程郵件與網站入侵為主，同時由於 DirtyAlphabet 族群對反鑑識手法十分熟悉，在入侵後即會主動隱藏蹤跡並抹去相關跡證，更利用獨創的 DNS 查詢手法進行遠端遙控並規避偵測，所使用之反鑑識手法包括修改檔案建立日期、以空白增大惡意程式大小、刪除系統日誌、用相黏鍵[1]跳過登入、建立酷似系統內建的帳號、偽造網頁存取 IP 等。

經深入研析，DirtyAlphabet 族群所使用之惡意程式，包括「DirtyAlphabet Type A」、「DirtyAlphabet Type B」、「DirtyAlphabet Type C」及「DirtyAlphabet Type D」4 大類(詳見圖 5)，以下說明這 4 類惡意程式之攻擊手法與特徵。



資料來源：本報告整理

圖5　DirtyAlphabet 族群之惡意程式分類

●DirtyAlphabet Type A

DirtyAlphabet Type A 屬於較傳統的後門程式類型，在植入惡意程式後會連線至中繼站，再從中繼站下載並執行惡意模組。程式啟動時，除會定時向中繼站報到外，也會檢測系統是否已有惡意模組，若無則連線至中繼站下載惡意模組並執行。但由於該惡意程式僅能運行於 32-bit 系統，故此類型活動跡象僅至 2016 年為止。歸納此類惡意程式具有以下特徵：

–與中繼站進行連線時，均透過 TCP 53 port 報到。由於 TCP 53 port 是 DNS server 間進行同步時所使用的通訊埠，故防火牆通常不會阻擋。

●DirtyAlphabet Type B

DirtyAlphabet Type B 之惡意程式是透過入侵受害電腦後，在特定的系統模組內加入惡意模組，再利用修改工具，將瀏覽器所送出的請求檔頭修改為特定格式，以遠端操控受害者電腦。歸納此類惡意程式具有以下特徵：

–攻擊目標為 IIS 的 ISAPI 模組。

–不會主動連線至中繼站。

–以類似 Webshell 方式接受駭客指令，並可隱藏來源 IP，增加追查難度。

●DirtyAlphabet Type C

DirtyAlphabet Type C 之惡意程式執行後會模擬一個 HTTP Server，並接收外部傳來的封包，若封包內容符合特定格式則執行相關指令。與 Type B 類似，駭客可利用一些修改工具，將瀏覽器所送出的請求檔頭修改為特定格式，以遠端操控受害者電腦，但此類型有 URL 限制，需要存取特定網址才可進行操控。此外，Type C 較 Type B 泛用型高，由於 Type B 僅能用於已安裝 ISAPI 模組功能的網頁伺服器，而 ISAPI 模組又非預設安裝，因此 Type B 相容性不高。歸納此類惡意程式具有以下特徵：

–為 HTTP Server 型之後門程式。

–使用時會帶特定網址。

–不會主動連線中繼站。

●DirtyAlphabet Type D

DirtyAlphabet Type D 之惡意程式為 Type A 的改良版，故有部分相似的特徵。惟此類型的惡意程式使用多種新型手法，導致傳統方式難以偵測。此外，此類型的惡意程式又有 V1 與 V2 等 2 種版本，V2 版本甚至有自毀功能，可於某些條件下自動抹除。歸納此類惡意程式具有以下特徵：

–所有連線均利用 UDP 53 進行報到與操控，且格式完全符合 DNS 協定，因此除欲查詢 DN 外沒有其他可供偵測之資訊。

–惡意程式回報時僅使用單向連線，且中繼站通常無回應，部分網路設備會視為失敗連線故不記錄於日誌中，因此難以察覺。

依目前相關資安事件與情資顯示，與 DirtyAlphabet 族群相關的受害範圍與影響並不大，惟其攻擊手法之持續精進值得關注與追蹤。若要防範遭受 DirtyAlphabet 族群攻擊，須注意社交工程郵件與網站入侵等 2 種攻擊途徑。針對社交工程郵件的防範，除使用惡意郵件偵測系統輔助外，亦應透過定期執行社交工程郵件演練來強化人員的資安意識。另一方面，針對網站入

侵的防範，則應加強伺服器的漏洞修補並搭配入侵偵測機制，以即早發現，並阻絕其惡意連線。

3.2 行動支付安全分析

行動支付代表無現金社會的正式來臨，更是一場未來支付的重大變革，了解行動支付的安全性將是推動與使用行動支付的關鍵因素。從早期的實體信用卡、網路電商發展到現在的行動支付，陸續衍生出許多不同角色，詳見圖 6。

資料來源：本報告整理

圖6　行動支付運作架構圖

- 相關標準：藉由標準的制定與規範，加速行動支付的推動與發展，主要標準包括支付代碼化標準(EMVCo Payment Tokenization)、EMV QR Code 國際共通支付標準及 PCI-DSS 安全認證。
- 整合服務：為避免商家必須面對多家支付業者與銀行而降低導入行動支付的意願，金管會開放「整合傳遞交易訊息服務」業務，以簡化商家與後端系統介接之複雜度。

●支付服務：結合行動支付技術、相關標準及銀行金融系統，提供消費者與商家便利的支付方式，分為電子支付、電子票證、第三方支付及國際支付。

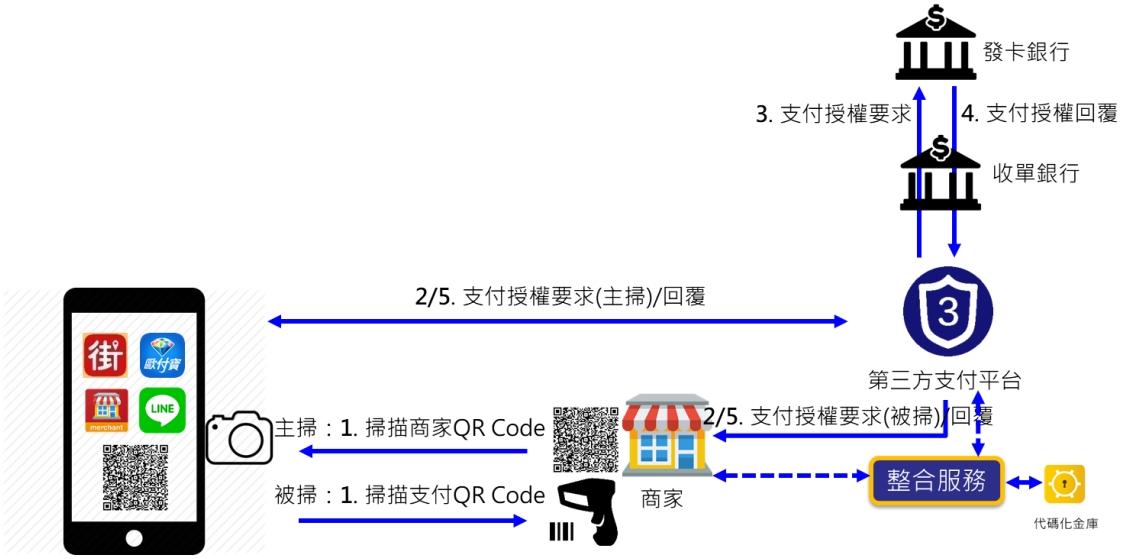
●標準服務：代碼化服務業者(Token Service Provider)可將信用卡卡號轉換為無意義的代碼，避免真實卡號在交易過程曝光，以降低盜刷風險，負責代碼的產生、儲存及轉換。

●卡務/帳務：由銀行、信用卡組織、發卡機構、收單機構及清算機構等形成之金融系統，處理信用卡發行與運作、銀行帳戶管理、銀行帳戶轉帳、銀行間清算等業務。

目前行動支付服務業者百家爭鳴，惟依使用者的支付介面主要可歸類為「掃碼支付」(以 QR Code 為例)與「感應支付」(以 Apple Pay 與 Google Pay 為例)等方式，以下簡介 QR Code、Apple Pay 及 Google Pay 之支付流程。

●QR Code

主要技術以掃描 QR Code 方式進行支付，由於不需要特定廠牌手機與通訊功能，目前業者與配合的商家最多。惟目前各業者 QR Code 規格尚未一致化，所以國內外正積極推動共通標準，其支付流程詳見圖 7。

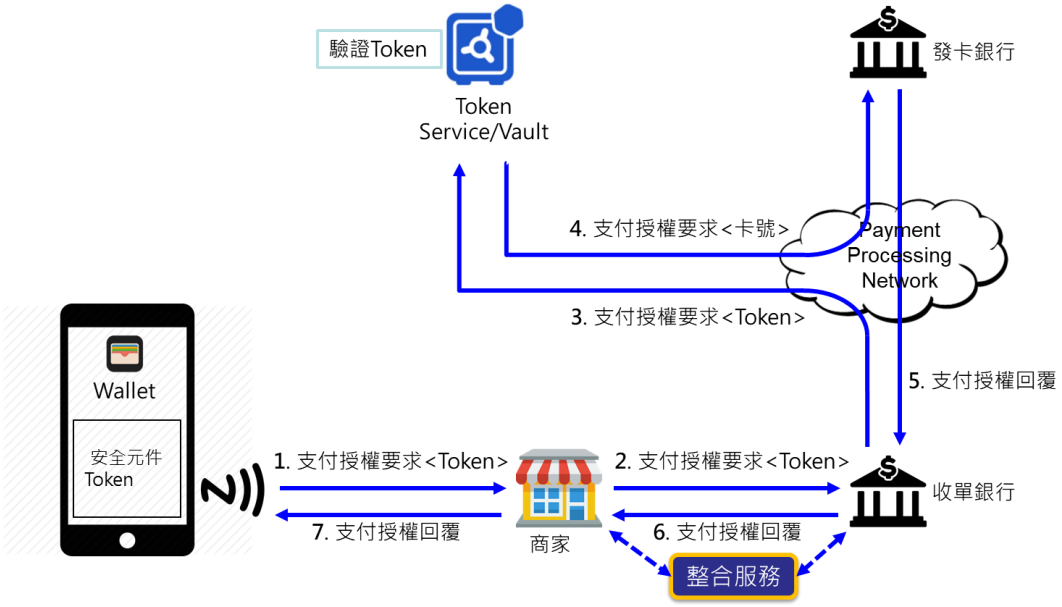


資料來源：本報告整理

圖7　QR Code 之支付流程

●Apple Pay

主要技術採用近距離無線通訊(Near Field Communication，以下簡稱 NFC)與代碼化技術(Tokenization)，透過 TSP 將卡號轉換成代碼(Token)，降低因卡號洩漏而導致被盜刷的風險，並利用手機具備硬體的安全元件(Secure Element，以下簡稱 SE)，儲存代碼及金鑰，Apple Pay 支付流程詳見圖 8。

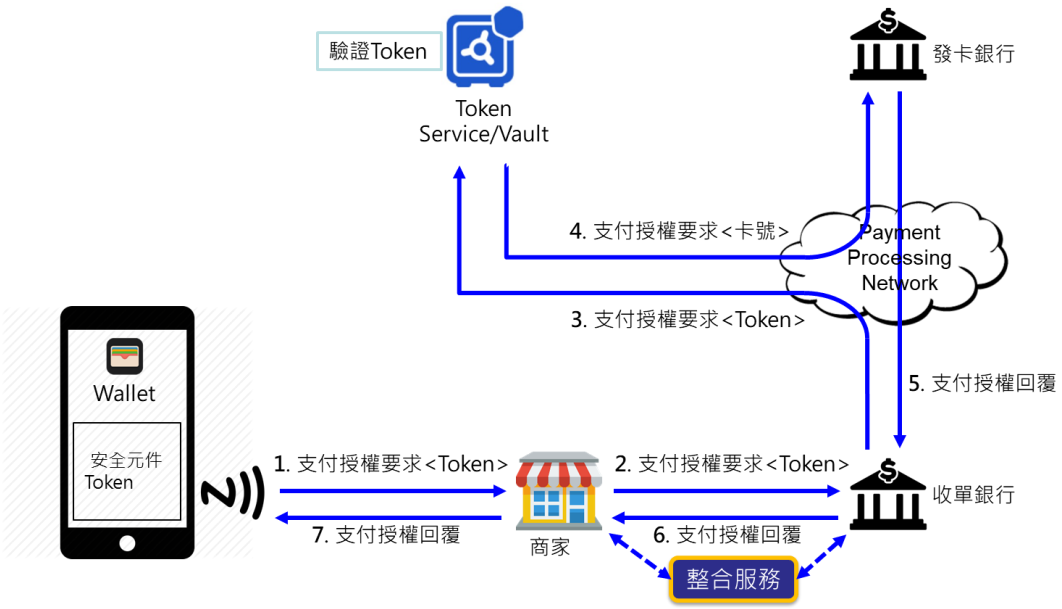


資料來源：本報告整理

圖8　Apple Pay 之支付流程

●Google Pay

與 Apple Pay 相似，主要技術採用 NFC 與代碼化技術，但與 Apple Pay 不同的是，Google Pay 是由主機卡模擬(Host Card Emulation，以下簡稱 HCE) Cloud 搭配手機支付 APP 來模擬 SE，代碼與金鑰儲存在 Google Pay APP 中，但金鑰有使用限制，需不斷從 HCE Cloud 下載更新，Google Pay 支付流程詳見圖 9。



資料來源：本報告整理

圖9　Google Pay 之支付流程

由於行動支付帶來便利也面臨越來越多的資安威脅，以下針對「行動載具端點」、「商家」、「整合服務提供者」、「支付服務提供者」及「標準服務提供者」等面向，提出其安全脆弱點與建議措施。

●行動載具端點

–脆弱點：身分認證機制不完備，有被盜刷的疑慮、消費者使用偽造 QR Code 付款，導致異常交易及小額支付允許無需輸入支付密碼，有被盜刷的疑慮等。

–建議措施：使用多因子身分認證機制、避免使用靜態的 QR Code，建立 QR Code 驗證機制(QR Code 共用平台)及預設為不啟動小額支付功能。

●商家

–脆弱點：商家 QR Code 可能被偽造 QR Code 置換導致異常交易、支付 APP 與後端伺服器可能存在安全漏洞及商家掌握部分卡號與交易紀錄。

–建議措施：避免使用靜態 QR Code，建立 QR Code 驗證機制(QR Code 共用平台)、規範行動支付軟體與系統之安全檢測及加強資安防護通報。

●整合服務提供者

–脆弱點：支付 APP、系統介接函式庫及後端伺服器可能存在安全漏洞、整合服務系統掌握個資、卡號及交易紀錄並提供介接服務。

–建議措施：規範行動支付軟體與系統之安全檢測與落實 PCI-DSS 驗證稽核，透過法規與罰則進行管控。

●支付服務提供者之脆弱點與建議措施

–脆弱點：支付 APP 與第 3 方支付平台之通訊協定缺乏安全驗證，有安全漏洞的疑慮、第 3 方支付平台存有未代碼化的卡片完整資訊，有洩漏的疑慮及第 3 方支付平台掌握個資、卡號及交易紀錄；HCE 掌握卡號與交易紀錄；Apple Server 掌握卡號。

–建議措施：依「金融機構提供 QR Code 掃描支付應用安全控管規範」發展相關通訊協定標準，提供業者遵循、規範採用代碼化技術標準及落實 PCI-DSS 驗證稽核，透過法規與罰則進行管控。

●標準服務提供者

–脆弱點：TSP 系統儲存卡片完整資料並提供驗證服務。

–建議措施：落實 PCI-DSS 驗證稽核，透過法規與罰則進行監管。

3.3 掃碼換面紙

相關報導指出，在大陸的「共享紙巾」潮流即將引入台灣，民眾僅須透過手機掃描面紙機上的 QR Code，就能領取免費面紙，詳見圖 10。目前「共享紙巾」主要透過微信社群軟體進行推廣，民眾掃描 QR Code 後會關注「共享紙巾」上的廣告商公眾號，即可使用「共享紙巾」服務，相關服務包括搜索附近機台及與好友分享紙巾等。

機台後端除可取得民眾的微信個人帳號公開資訊，而且若由微信公眾號尋找附近的「共享紙巾」機台，則機台後端亦可取得民眾的 GPS 定位資訊；同時民眾若將微信公眾號轉傳給其他聯絡好友，聯絡人好友關注該公眾號後(病毒式行銷)，透過此手法，機台後端將可建立民眾的社群帳號關聯。

資料來源：[2]

圖10 掃碼換面紙

以下提供 QR Code 掃碼應注意之相關資安作為：

- 廠商、相關廣告業主或相關 QR Code 服務提供者，應隨時檢查機台的 QR Code 是否有遭誤用，並在機台與相關廣告文宣上，主動告知欲連結的網址為何，如此一般民眾可交叉比對網址是否如文宣所示。
- 使用者方面，若執行手機掃碼後看到一串怪異網址，建議不要在沒有確認下直接使用瀏覽器打開相關連結。若掃描 QR Code 後發現有 APP 下載行為，務必確認只能透過官方的 Google Play 或 APP Store 下載。另外，若民眾發現相關 APP 軟體與社群頁面出現任何授權請求訊息，則應詳細確認相關資訊，避免讓自己與好友陷入資訊外洩的風險。

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，並歸納出「物聯網設備資安弱點威脅升高」與「關鍵資訊基礎設施資安風險倍增」等 2 大面向，在本季有資安威脅升高之趨勢。此外，在政府資安威脅現況中，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弱密碼等弱點加以關注。針對本季全球與政府所面臨的主要資安威脅，本報告針對「物聯網設備安全」、「關鍵資訊基礎設施安全」及「網站設計不當與弱密碼」等 3 方面提出資安防護建議。另一方面，因應資安法施行在即，本報告藉由資安專題分享，說明資安法之相關規定、適用對象及因應重點，相關單位可審視自我資安環境之完備度並落實資安管理制度。在資安新興議題研析，「DirtyAlphabet 新型態攻擊手法簡介」揭露組織型駭客使用 DNS 進行攻擊之新興手法。而「行動支付安全分析」及「掃碼換面紙」等 2 個議題，則提供在行動支付逐漸盛行的今日，各界需注意的資安作為。

資安能量的建立是需要日積月累，且謹慎以對。下一季「資通安全技術報告」，將持續分析全球與政府機關(構)之資安威脅現況，以及探討資安新興議題並提供防護建議。而資安專題分享則將針對歐盟 GDPR 進行研析探討，主要會在分析適用範圍、與 GDPR 法規要求之差異性分析及提供自我檢核表，提供政府機關(構)與民間企業檢視內部法規遵循性之符合程度。

資安相關活動

為提升資安防護能量，本季舉辦多項資安相關活動，說明如下：

◆ 技服中心南部辦公室正式成立運作

為平衡資安區域發展，加強學研合作，技服中心自 106 年起規劃於南部科學園區台南園區設立南部辦公室，經相關籌劃與資源整合，於本年 6 月 29 日正式揭牌運作。南部辦公室主要任務包括結合中南部地區學研資源、強化資安合作交流、加強對中南部政府機關(構)資安防護服務及提升整體資安防護能量。因此，定位是以學研合作與資安事件技術服務為主，核心與機敏業務仍由技服中心本部負責。

◆ 學研合作交流會議

為推動資安核心技術需求導向的學研合作、強化資安核心技術研發的場域驗證及儲備資安核心技術的研發人才，技服中心於本年 6 月 29 日舉辦學研合作交流會議，以鏈結資安研發能量與實務需求、強化資安核心技術自主研發能量、提升資安人才質量及帶動資安產業發展。整體合作方式藉由技服中心提供的議題、場域、資料及技術支援，由學研單位進行研發、人才培訓及回饋相關成果。

本次會議除分享 106 年學研合作成果外，並規劃本年學研合作計畫，合作議題包括「惡意程式分析與檢測系統」、「關鍵基礎設施之互動式蜜網系統」、「資安情資交流合作」、「工業控制模擬平台與區塊鏈資安應用」及「資訊設備探勘端點之開發與部署技術」等。

◆ 政府機關(構)資安稽核

政府機關(構)資安稽核之目的在落實資安稽核制度，協助政府機關(構)強化資安防護之完整性及有效性，並透過持續改善降低資安風險，提升資安防護與認知意識。

本年資安稽核技術檢測增加物聯網設備檢測，包括網路攝影機(IP CAM)、網路印表機及門禁系統等。此外，建立資安稽核員培訓與遴選機制，並協助主管機關對所屬機關(構)進行第二方稽核。

◆ 國家資安資訊分享與分析中心(N-ISAC)技術交流會議

為因應關鍵資訊基礎設施成為駭客攻擊趨勢，行政院資通安全處規劃於每季定期召開國家資安資訊分享與分析中心(以下簡稱 N-ISAC)技術交流會議，期透過相關議題的交流與討論，提升我國關鍵資訊基礎設施之資安防護能力。

本季於 4 月共邀請 26 個一般會員進行討論，會議內容主要為各領域 ISAC 說明運作執行情況，同時就 N-ISAC 情資交流規劃、電腦緊急事故處理及通報平台共用性評估說明及關鍵資訊基礎設施防護建議等議題，進行討論交流。此外，6 月召開技術會員會議，共邀請 6 個技術會員與會交流，會議內容為針對 N-ISAC 情資交流項目進行規劃說明與討論，並分享近期資安事件案例。

◆ 資安服務團

資安服務團成立的主要目的為因應資安法施行，政府機關(構)新增資安業務，規劃短期間由資安服務團協助推動及落實各項政策及措施，並建立相關標準作業與檢核基準。預期效益包括輔導與協助機關(構)落實資安防護，同時於事件發生時，組成跨機關應變小組，進而強化跨機關聯防及資安防護網路。

資安服務團作業規劃分為「資安防護輔導訓練」與「資安防護實地輔導」，安排受輔導機關(構)參加策略面、管理面及技術面之資安輔導訓練，以提升資安相關知識與技能，俾利與實地輔導有效銜接；實地輔導進行策略面、管理面及技術面之實地檢視，並提出對受輔導機關(構)資安防護措施之整體建議，協助推動與落實資安政策。

參考文獻

[1]台灣數位有聲書推展學會，相黏鍵說明，取自：
http://www.tdtb.org/information_nvda_view.aspx?nid=20130915111816

[2]自由時報，個資只值一包面紙，取自：
http://news.ltn.com.tw/news/life/breakingnews/2420852