【技術專欄-016】

檢測認證成物聯網產品研發依歸 網路攝影機資安標準出爐

文・台灣資通產業標準協會網路與資訊安全技術委員會 / 高傳凱&蔡正煜

物聯網(IoT)科技是全世界發展最快速的產業，相關應用不斷推陳出新，而物聯網科技成功與否，資訊安全是最主要的關鍵，因此經濟部工業局率先提出制定物聯網資安環境標準的目標，包括物聯網通用資安標準、輔助應用程式資安標準、影像監控系統資安標準、工控系統資安標準、車聯網系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準等，全面推升國內資安產業自主研發能量，提供穩定且安全的產業發展環境。

物聯網的盛行，使日常用品皆朝向數位化邁進，網路攝影機也是其中之一，運用範圍包括視訊通話、遠端監控、直播服務等，相當受到消費者青睞。但隨之而來的問題是網路攻擊事件，從 2014 年起，網路資安事件日益頻繁，攻擊事件規模越來越大，2016 年底以 Mirai 為名的惡意程式，藉由網路攝影機為跳板，製造出前所未聞之網路攻擊的手法。

有鑑於此，藉由「影像監控系統資安標準-網路攝影機」之制定，可建立國內在網路攝影機之資安品質的標準，期使設備商或系統服務商在產品研發上有所依據，藉以促進國內產業整體優質化及產品競爭力，並確保消費者在網路攝影機之運用上達到資訊安全的目的。

依據標準制定流程　有效提升資安品質

物聯網資安標準提供物聯網設備的資安需求，可作為設備設計與測試的依據。為使所訂定的資安標準能符合產業現況與需求，並讓依據此資安標準所設計的物聯網產品能有效提升資安品質，因此標準制定過程分成兩個主要階段，即資安威脅分析與標準草案研擬階段，以及標準諮議階段(圖 1)。

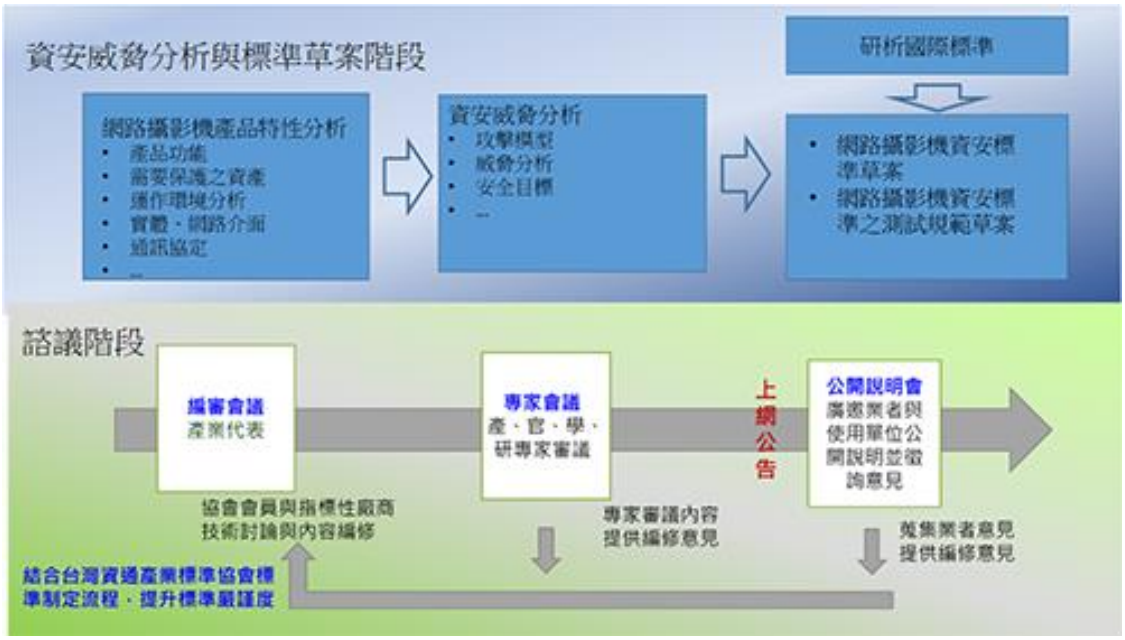

圖 1 標準制定過程分成「資安威脅分析與標準草案研擬」以及「標準諮議」兩個階段。

在資安威脅分析與標準草案研擬階段，主要分析網路攝影機產品特性，找出可能的資安攻擊面向，建立網路攝影機的資安威脅模型。依據此威脅模型找出有效的反制措施，進而訂定網路攝影機產品的資安要求。透過此系統化的資安威脅與資安需求的應對分析，並研析參考國際相關的資安標準形成此網路攝影機資安標準草案內容。

在諮議階段，則透過邀請產官學研各界專家與產業代表辦理專家會議與公開說明會擷取各方意見，從各種不同面向探討標準的嚴謹度與實施的可行性並凝聚共識。以下說明流程中各項工作內容：

網路攝影機產品特性分析

了解物聯網產品的資安威脅之前，必須深度了解其特性與功能及其運作環境。拆解其技術框架，解析聯網產品的對外連接介面包含實體介面、網路介面，還有使用的網路通訊協定，這些都是外部威脅的可能攻擊面，分析的結果可作為後續資安威脅分析的依據。

資安威脅分析

經過前一個步驟的產品特性分析，了解系統需要保護的重要資產，以及駭客可以利用的攻擊面。在這個步驟中主要的工作即是分析在這些可入侵的介面是否可能存在哪些弱點與威脅來源，而威脅來源可以利用這些弱點破壞或取得哪些

重要資產，造成產品使用者的損失。透過此分析過程了解網路攝影機的資安威脅來源與攻擊型態。最後，並定義需要達到的資安目標與威脅反制措施。

蒐集/研析國際及區域組織之資安標準

本標準雖為國內標準，但是台灣為高度開放的經濟體，科技產業更是以商品出口為主，必須參考融合國際標準內容，使制定之資安檢測機制符合國際需求。

本標準參照國際物聯網相關資安標準/規範，如 International Organization for Standardization(ISO) 27001、Underwriters Laboratories(UL) 2900 系列標準、Groupe Speciale Mobile Association(GSMA) IoT Security Guideline、Open Web Application Security Project(OWASP) Top IoT Vulnerabilities 以及日本政府的物聯網安全指導方針等。

訂定網路攝影機資安標準/測試規範

網路攝影機資安標準，提供了網路攝影機產品在設計時須達到的資安需求。利用前面步驟所產出的資安威脅模型，研析反制威脅措施與資安風險管理目標，訂定網路攝影機產品的資安要求。因此，當網路攝影機產品的設計以此標準為依據，即可具備預防這些已知之資安威脅能力。

除資安標準外，也制定了對應之檢測規範作為實驗室測試的依據，檢測實驗室可以扮演第三方公正測試者的角色，按照測試規範所定的測試步驟，驗證產品是否符合資安標準的要求。

諮議階段

在諮議階段須辦理編審會議、專家會議與公開說明會，主要目的在凝聚產業對此份標準的共識。本系列標準共舉辦 8 場編審會議、6 場專家會議及 4 場公開說明會。標準草案內容在凝聚各方共識，並修改後成為正式公告發行標準文本。

專家會議集合產官學研不同領域之專家提供不同面向的見解，從技術、法規、政策提供標準的可行性與合理性意見及修訂方項，提升未來使用者端與業者端對標準的支持。

維護影像監控安全　資安標準列舉說明

物聯網科技的核心--網路攝影機，無論是車聯網、家聯網、醫聯網、社區聯網都須要影像資訊的輔助，作為能滿足民生、工業、軍事及政府需求的設備，可以說是科技生活的必需品。從設備自身的架構來說，具有影像這種高價值資

料、長時間聯網、常見的作業系統等，是功能相當齊全的嵌入式裝置，因此本標準從實體、系統、通訊、身分鑑別與授權、隱私保護這五個面向，來確保網路攝影機資安品質。

影像監控系統，又稱安控系統，目的是監看特定場所以達到維安目的，主要是由網路攝影機、數位影像錄影機、網路影像錄影機及網路儲存裝置組成。除此之外，監控所有攝影機畫面的監控中心，包括本地端或遠端電腦設備、行動裝置與雲端伺服器，以及連接監控設備之網路環境，包括 Wi-Fi 存取點、路由器和交換機等，構成整個影像監控系統。

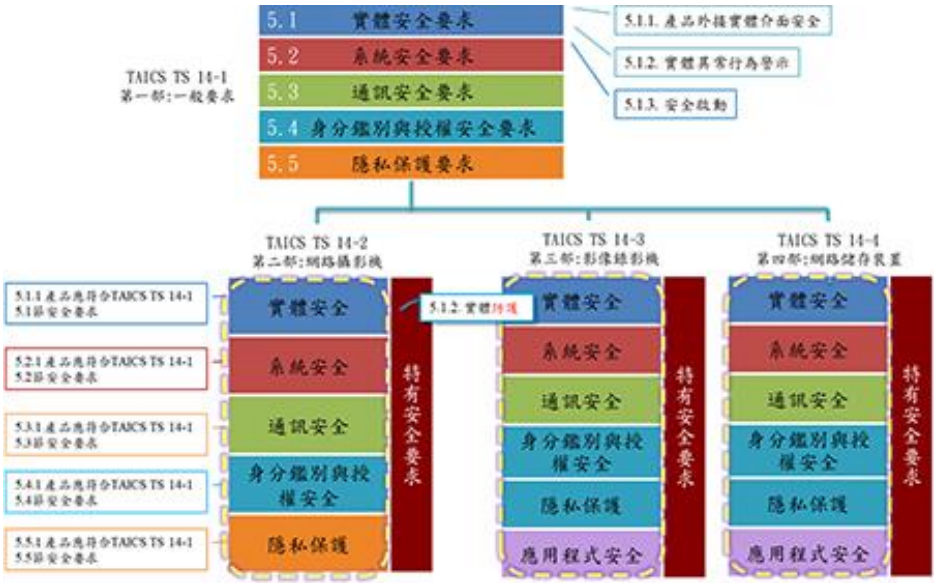

圖 2 影像監控系統系列資安標準框架

TAICS TS-0014 系列標準為影像監控系統相關(圖 2)，包括網路攝影機、影像錄影機及網路儲存裝置。TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求，為其他 TAICS TS-0014 系列標準的參照，因此網路攝影機的資安需求涵蓋第一部和第二部，再根據標準所提出之安全構面，即可掌握網路攝影機的安全需求與欲保護的目標，下述則是網路攝影機之五大安全構面：

• 實體安全

著重在裝置是否可輕易被拆解，或產品資料存儲與測試用連接埠的處置，包括實體埠之安全管控、實體異常行為警示、實體防護、安全啟動。

• 系統安全

確保裝置之作業系統、網路服務及韌體程式設計等，須具備足夠的安全防護，以及警示及日誌功能是否齊全，包括作業系統與網路服務安全、網路服務連接

埠安全、更新安全、敏感性資料儲存安全、網頁管理介面安全、操控程式之應用程式安全、日誌檔與警示。

・通訊安全

敏感性資料之通訊安全，和通訊服務存在未知之資安漏洞與否，包括敏感性資料傳輸安全、通訊協定與設置安全、Wi-Fi 通訊安全。

・身分鑑別與授權機制安全

與使用者及其他裝置之間的溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，須確保身分鑑別與授權相關機制，包括鑑別機制安全、通行碼鑑別機制、權限控管。

・隱私保護

影像監控裝置之隱私，包括使用者的影像資料，於存取與傳輸的保護及權限管控等，確保隱私資料不應外洩，包括隱私資料的存取保護、隱私資料的傳輸保護。

產品實測重點說明　資安測試手法逐項確認

為驗證裝置是否符合安全要求，必須藉由實驗室透過資安測試手法來確認，這裡將舉例幾個重點測試項目，分析測項的測試目的及通過標準，使讀者在閱讀此份標準時可以明瞭每個安全要求背後的意義。

5.1.1.1 實體介面安全管控

此測項的目的是為了驗證是否可透過產品實體介面，存取作業系統之除錯模式，因此測試人員首先要確認電路板上是否有通用異步收發器(UART)用的針腳。除此之外，有些裝置是可以透過通用序列匯流排(USB)進入除錯模式，甚至廠商連除錯模式都閉鎖住也是有可能的，因此各家會有不同的方式，必須先請受測廠商告知。

根據目前筆者所測試過的結果顯示，網路攝影機能進入除錯模式的實體介面多半是 UART，而大部分對 UART 的保護強度不足，沒密碼或弱密碼的情形是很常見的，因此測試步驟中還有要求實體介面的通行碼認證。透過此測項的驗證，可確保使用者無法經由實體介面進入作業系統模式。

5.2.3.1 韌體檔案安全測試

此測項的目的是為了驗證設備之韌體更新檔是否會洩露敏感性資料，韌體常存在著 Hardcode 敏感性資料的資安問題，不只如此，大多數網路攝影機之韌體更是唾手可得，駭客往往會把韌體拆解甚至逆向工程，因此測試的手法須以駭客思維來執行，利用類似 Binwalk 這類的韌體拆解工具，再到拆解出來的檔案系統中檢視是否存在密碼、金鑰等敏感性資料。此外，目前國際上普遍開始對韌體檔案加密，因此也可以透過對韌體進行加密來滿足測項的通過條件。

5.2.6.1 應用程式介面(ONVIF API)之鑑別機制測試

其測試目的是為了驗證產品的應用程式介面呼叫是否經過身分鑑別程序，且該身分鑑別程序具備重送攻擊抵抗能力。ONVIF API 是一個不具認證機制的通訊協定，也是導致網路攝影機影像資料外洩的主因，因此這個測項也同樣要以駭客思維執行。

先以第三方具 ONVIF API 的應用程式直連網路攝影機，此時若不具身分鑑別功能，即可存取該設備，若具備身分鑑別功能，則透過 Man-in-the-Middle 攻擊，從中擷錄 ONVIF API 的認證封包，於下次連線時再轉發，看是否可以經由 Replay 攻擊導致認證成功。

5.3.1.1 敏感性資料之傳輸保護初階測試與 5.5.2.1 隱私資料的傳輸機密性初階保護測試

本項確認在測試關鍵資料的傳送是否透過安全通道的保護，除此之外，還要求網路攝影機要具驗證此安全通道憑證有效性及合法性之能力，這是指網路攝影機要接受憑證時，亦即當裝置為資料的接收方時，要必須具備防 Man-in-the-Middle 攻擊的能力，因此才會在「樣品條件」的地方加入「若與產品對連之影像監控裝置採用自簽發憑證，則產品須提供可編輯中繼憑證之介面」這樣的條件，配合實驗室可能採用自簽發憑證來做測試。

測試時，則是先將裝置與其他影像監控裝置(如 NVR)連接，並啟動安全通道之建立程序，當其他影像監控裝置發送憑證予產品之同時，攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。接著，發送已竄改之憑證予產品，於安全通道建立的交握過程中監聽封包，檢視產品是否接受此憑證。

5.3.2.3 通訊協定異常輸入測試

此測項的目的是為了驗證設備之通訊協定是否存在未知之資安漏洞，要檢查設備的通訊協定是否存在非邏輯性的程式漏洞，唯有透過自動化模糊測試軟體，將變異過的封包一一送入裝置，才能有機會找到通訊協定漏洞。

然而，模糊測試所耗時間甚鉅，每個裝置對於各封包的回覆時間不同，所以在測試方法中有註明：「測試對通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試」，是透過時間限定，來避免萬一受測設備測 10 萬筆花費相當長時間的情況發生。 此外，測試的主要目的是為了判斷通訊協定的崩潰是否因為變異的封包而發生，所以若系統崩潰是因為攻擊頻率太高而導致，將不會影響測試結果。

標準協會負責運作　全力推動檢測制度

本標準的認證制度架構規畫如圖 3 所示。整體認證制度由台灣資通產業標準協會負責運作，包含實驗室的管理與通過檢測之物聯網設備標示作法等部分。另外，包含第三方公正機關全國認證基金會(TAF)對檢測實驗室進行品質認證，以確保實驗室之檢測能力品質符合標準的要求，有效提升物聯網設備資安品質。

圖 3 認證制度架構規畫

面對資安的威脅，沒有任何措施可以保證百分之百的安全，只能將風險降低在可以接受的程度。最重要的是，產業須建立資安意識，不以通過標準檢測為目的，而是隨時注意資安威脅提升防護能力，才能建立可信賴的物聯網應用環境，蓬勃物聯網應用的發展。

(本文同步刊載新通訊元件雜誌 2018 年 7 月號 209 期《技術前瞻》)