影像監控系統網路攝影機資安標準草案 (V0.6.2)

推動單位：

台灣資通產業標準協會(TAICS)

制定單位：

台灣資通產業標準協會之網路與資訊安全技術工作委員會(TC5)

支持單位：

經濟部工業局、財團法人資訊工業策進會

2017-07-25

文件修改記錄

版本	修改日期	修改人	問題單流水號	修改原因及說明

前言

網路攝影機用途廣泛，包括視訊通話、遠端監控、直播服務等，造就公司或家庭設置網路攝影機的普及度上升，然而設備商、系統服務商未考慮連網後所造成的資安衝擊，導致從 2014 年陸續發生資安攻擊事件，不僅事態是越來越嚴重，2016 年底以 Mirai 為名的惡意程式，藉由網路攝影機為跳板，製造出空前未有的網路攻擊，經濟部工業局有鑑於此，致力於「影像監控系統網路攝影機資安標準草案」之制定(以下簡稱本標準)，以改善國內網路攝影機資安品質，並增加產品競爭力。本標準從四大領域來確保網路攝影機資訊安全，包括系統安全、通訊安全、身分認證與授權及隱私保護，並參酌國際物聯網相關資安規範，如 ISO 27001[4]、UL 2900 系列標準[8]、GSMA IoT Security Guideline[3]、OWASP Top IoT Vulnerabilities[7]及日本政府的物聯網安全指導方針[10]，製造商及消費者依循本標準之安全要求，得以降低私密影像外洩的風險，並確保網路攝影機之使用達到安全安心的目的。

目錄

附圖表列

1. 適用範圍

目前網路攝影機主要區分為兩種類型，一種是直接連接電腦用於視訊通話的消費型網路攝影機(Webcam)，另一種主要用於影像監控系統的連網監控攝影機(e.g., IP camera, Smart camera, 3D camera,…etc.)。網路攝影機係透過有線或無線網路進行傳輸的攝影機，因此只要有網路皆可進行遠端監控及錄影。網路攝影機根據視訊儲存方式又可分為以下兩種類型：

(1) 集中式網路攝影機：透過中央數位錄影主機(Digital Video Recorder, DVR)或網路錄影主機(Network Video Recorder, NVR)，集中處理視訊及管理。

(2) 分散式網路攝影機：攝影機內建記錄功能，可直接紀錄並儲存到標準儲存設備，例如 SD 卡、NAS(網路連接儲存設備)或是 PC/Server。

本標準適用於網路攝影機，不限定商業用或家庭用，僅依照攝影機之功能與規格，即是僅針對前端攝影機之安全性要求，而後端之數位錄影主機(Digital Video Recorder, DVR)或網路錄影主機(Network Video Recorder, NVR)、儲存設備以及前端攝影機與後端處理儲存設備之間傳輸過程，皆不在本標準所規範之範圍內(見圖 1)。

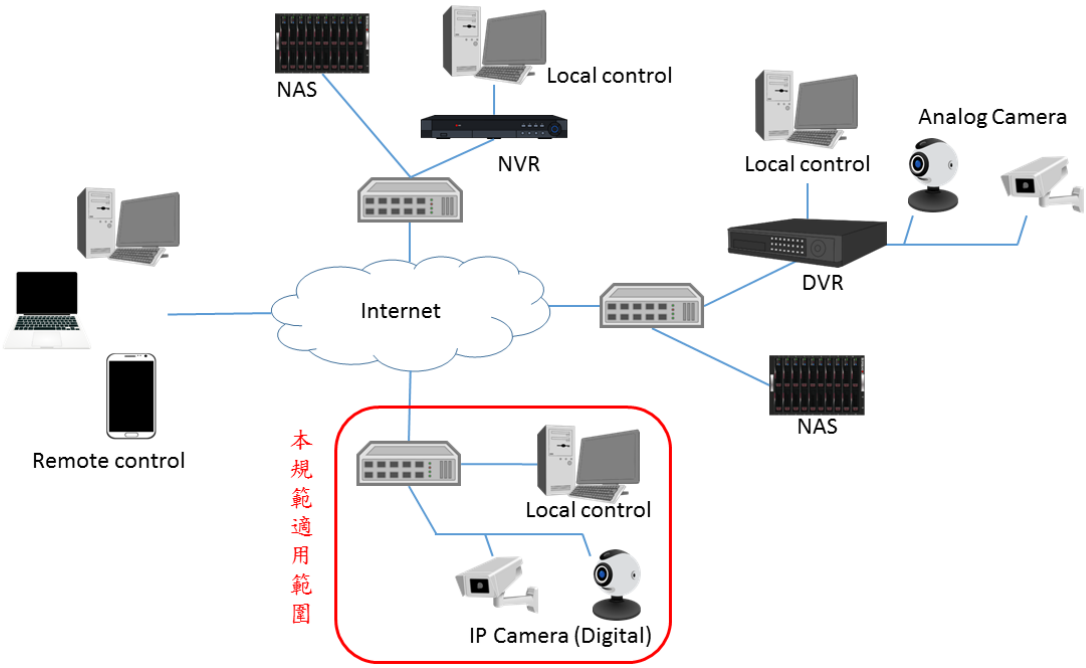

圖 1. 適用範圍示意圖

2. 用語及定義

2.1. 資訊安全漏洞 (Security Vulnerability)

指受測裝置安全方面之缺陷，包括受測裝置之系統、通訊及應用軟體等，威脅裝置之保密性、 完整性及可用性。

2.2. 常見弱點與漏洞 (Common Vulnerabilities and Exposures , CVE)

一個收集各種資安漏洞並且給予每個漏洞一個唯一編號，提供公眾查閱之資安漏洞資料庫[5]。

2.3. 機敏資料 (Private and Sensitivity Data)

因用戶的行為或網路攝影機之運作，所產生之機密或敏感資料，且該資料一旦遭外洩或竄改，勢必會造成該資料之擁有者的權益受損害，本標準所指之機敏資料包括使用者帳號、密碼及敏感性資料。

2.4. 敏感性資料 (Sensitivity Data)

因用戶的行為或網路攝影機之運作所產生之資料，一旦外洩可能對使用者造成損害，包括用戶資訊、地理位置、系統日誌。

2.5. 隱私 (Privacy)

係指私人資訊，此一資訊的全部或部份不想讓他人知道，且有權利去保護的部分，本標準所指之隱私包括網路攝影機所錄製之影像及用戶資訊。

2.6. 遠端管理介面 (Remote Command Control)

係指透過指令介面(例如: telnet, SSH 等)取得網路攝影機作業系統層的操控權，通常是作為工程師遠端維護產品使用，抑或是透過網頁管理介面遠端存取網路攝影機資源，例如：監看畫面、操控鏡頭，以及進行系統設定，例如：設定 IP 位址。

2.7. 操控程式 (Control Program)

係指用於控制網路攝影機行為或瀏覽監控內容之應用程式，目前可能的應用程式類型包括行動版及電腦版。

2.8. 應用程式介面 (Application Program Interface, API)

大部份網路攝影機皆提供 API 給操控端之應用程式呼叫，用戶可透過這些 API，撰寫實

際實現網路攝影機相關操作(例如：系統資訊擷取、監控影像擷取等)的應用程式。

2.9. 密碼 (Password)

係指一組字元串能讓系統辨識用戶身分，並可進一步控管用戶存取系統之權限。

2.10. 第三方函式庫 (3rd Party Library)

係指系統程式設計者為了加速開發，引用其他組織所製作具備某特定功能之函式庫，以滿足裝置所需提供的服務。

2.11. 加密 (Encryption)

係指透過數學演算法來對明文資訊進行改變，使原來的資料不可讀而達到保密的目的。

2.12. 數位簽章 (Digital Signature)

係指簽署人以私鑰簽名經由數學演算法處理過後產生一定長度之電子文件，形成電子簽章，並得以公開金鑰進行驗證，不僅可確保該文件的完整性，同時驗證文件作者的不可否認性。

2.13. 安全通道 (Security Tunnel)

目的是為網際網路通訊的端點與端點(End-to-End)之間，建立一條兼顧資料隱密性及完整性之通道，目前常見之實作通訊協定為安全通訊端層(SSL)和傳輸層安全性(TLS)。

3. 標準規範

本標準為確保網路攝影機安全，從四大面向訂定網路攝影機的安全技術要求，包括：系統安全、通訊安全、身分認證與授權、隱私保護。而以下技術要求又根據(1)檢測所需時間、(2)複雜度、(3)目前尚無通用檢測方法、(4)產品技術現況等因素，將每一要求分為必須達成的必要項(Mandatory, M)及需求單位依情況增減的參考項(Option, O)，必要項為受測網路攝影機必須遵守的要項，而參考項可視為網路攝影機廠商產品設計之建議，各個要求項的狀態見「附錄 D」。

3.1. 系統安全技術要求

3.1.1. 網路攝影機作業系統安全

3.1.1.1. 網路攝影機之作業系統，不得存在已揭露之重大 CVE 漏洞。

3.1.1.2. 網路攝影機僅開啟必要之網路服務。

3.1.1.3. 網路攝影機所開啟之網路服務，不得存在已揭露之重大 CVE 漏洞。

3.1.2. 網路攝影機之韌體程式安全

3.1.2.1. 網路攝影機必須具備韌體更新機制。

3.1.2.2. 網路攝影機之韌體更新機制，必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求。

3.1.3. 網路攝影機之機敏性資料儲存安全

3.1.3.1. 網路攝影機之機敏資料應避免出現於裝置韌體程式碼中。

3.1.3.2. 網路攝影機之機敏資料必須加密儲存，且加密演算法強度需符合「附錄 A」的要求。

3.1.4. 網路攝影機之遠端管理介面安全

3.1.4.1. 網頁管理介面不應該存在 OWASP (Open Web Application Security Project) top 10 [6]中所揭露之常見網站安全風險。

3.2. 通訊安全技術要求

3.2.1. 網路攝影機之資料傳輸安全

3.2.1.1. 機敏資料之網路傳輸必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求。

3.2.2. 通訊介面的安全設置

3.2.2.1. 網路攝影機需提供使用者，可自行開/關網路裝置資訊探詢功能。

3.2.2.2. 網路攝影機上不可存在不安全的無線網路設定。

3.2.3. 網路攝影機之通訊協定安全

3.2.3.1. 網路攝影機所使用之通訊協定(見附錄 B)，必須經過異常輸入檢測，且不得發生崩潰(crash)導致服務中止的情形。

3.3. 身分認證與授權技術要求

網路攝影機在不同的溝通介面上，包括網路攝影機之 API 呼叫、遠端管理介面、操控程式，皆需要應用到身分認證功能。

3.3.1. 認證機制安全

3.3.1.1. 遠端存取網路攝影機資源應經過身分認證機制，且必須為強認證機制。

3.3.1.2. 認證資訊的傳輸必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求。

3.3.2. 密碼認證安全

3.3.2.1. 網路攝影機之密碼認證機制，密碼強度必須遵守「附錄 C」的要求。

3.3.2.2. 廠商所出產之網路攝影機其預設密碼都需相異。

3.3.2.3. 首次登入網路攝影機必須強制更改預設密碼。

3.3.2.4. 網路攝影機在登入密碼的設計上必須有輸入頻率及次數的限制。

3.3.3. 網路攝影機之權限管控

3.3.3.1. 網路攝影機資源的存取，必須具備權限管控機制。

3.3.3.2. 網路攝影機之授權行為，應存在閒置時限。

3.4. 隱私保護技術要求

3.4.1. 隱私資料的蒐集保護

3.4.1.1. 網路攝影機在蒐集影音資料時，應給與適當的提示。

3.4.2. 隱私資料的存取保護

3.4.2.1. 網路攝影機所儲存的隱私資料，只有已被授權的個體才可以存取。

3.4.2.2. 網路攝影機所儲存的隱私資料必須受到加密保護，且加密演算法強度需符合「附錄 A」的要求。

3.4.2.3. 網路攝影機應具備使用者刪除其隱私資料之功能，提供對所儲存隱私資料的刪除權

限。

3.4.3. 隱私資料的傳輸保護

3.4.3.1. 網路攝影機隱私資料的傳送不得為明文。

註 1: 網路攝影機與其相對應之操控應用程式若涉及與雲端伺服端之互動，建議應由業者自我宣告或切結其伺服端資訊安全防護與管理措施。

註 2: 本標準僅針對網路攝影機本身制定安全要求，而遠端控制網路攝影機之行動 App，建議受測廠商檢測通過「行動應用 App 基本資安規範」[9]。

附錄 A
(規定)
加密演算法強度要求

加密演算法之強度必須支援以下幾個要求:

- NIST FIPS 140-2, Annex A: Approved Security Function. [2]

附錄 B
(規定)
網路攝影機所使用之通訊協定

- 即時傳輸協定 (Real-time Transport Protocol, RTP)
- 即時傳輸控制協定 (Real-time Transport Control Protocol, RTCP)
- 即時串流協定 (Real Time Streaming Protocol, RTSP)
- 超文字傳輸協定(HyperText Transfer Protocol, HTTP)
- 超文字傳輸安全協定(HyperText Transfer Protocol Secure, HTTPS)

附錄 C
(規定)
密碼強度要求

- 政府組態基準(GCB) CCE-33789-9 最小密碼長度之規定[1]。

附錄 D
(參考)
資訊安全技術要求事項

下表綜整本標準之所有資安技術要求,狀態欄用來標示該項要求是必要項抑或是參考項。

- 系統安全技術要求

編號	技術要求	狀態
3.1.1.1	網路攝影機之作業系統，不得存在已揭露之重大 CVE 漏洞	M
3.1.1.2	網路攝影機僅開啟必要之網路服務	M
3.1.1.3	網路攝影機所開啟之網路服務，不得存在已揭露之重大 CVE 漏洞	M
3.1.2.1	網路攝影機必須具備韌體更新機制	M
3.1.2.2	網路攝影機之韌體更新機制，必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求	M
3.1.3.1	網路攝影機之機敏資料應避免出現於裝置韌體程式碼中	M
3.1.3.2	網路攝影機之機敏資料必須加密儲存，且加密演算法強度需符合「附錄 A」的要求	M
3.1.4.1	網頁管理介面不應該存在 OWASP top 10 中所揭露之常見網站安全風險	M

- 通訊安全技術要求

編號	技術要求	狀態
3.2.1.1	機敏資料之網路傳輸必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求	M
3.2.2.1	網路攝影機需提供使用者，可自行開/關網路裝置資訊探詢功能	M
3.2.2.2	網路攝影機上不可存在不安全的無線網路設定	M
3.2.3.1	網路攝影機所使用之通訊協定(附錄 B),必須經過異常輸入檢測，且不得發生崩潰(crash)導致服務中止的情形	O

- 身分認證機制安全技術要求

編號	技術要求	狀態
3.3.1.1	遠端存取網路攝影機資源應經過身分認證機制，且必須為強認證機制	M
3.3.1.2	認證資訊的傳輸必須經過加密保護，且加密演算法強度需符合「附錄 A」的要求	M
3.3.2.1	網路攝影機之密碼認證機制，密碼強度必須遵守「附錄 C」的要求	M
3.3.2.2	廠商所出產之網路攝影機其預設密碼都需相異	O
3.3.2.3	首次登入網路攝影機必須強制更改預設密碼	M
3.3.2.4	網路攝影機在登入密碼的設計上必須有輸入頻率及次數的限制	M
3.3.3.1	網路攝影機資源的存取，必須具備權限管控機制	M
3.3.3.2	網路攝影機之授權行為，應存在閒置時限	M

- 隱私保護技術要求

編號	技術要求	狀態
3.4.1.1	網路攝影機在蒐集影音資料時，應給與適當的提示	O
3.4.2.1	網路攝影機所儲存的隱私資料，只有已被授權的個體才可以存取	M
3.4.2.2	網路攝影機所儲存的隱私資料必須受到加密保護，且加密演算法強度需符合「附錄 A」的要求	M
3.4.2.3	網路攝影機應具備使用者刪除其隱私資料之功能，提供對所儲存隱私資料的刪除權限	M
3.4.3.1	網路攝影機隱私資料的傳送不得為明文	M

參考資料

1. CCE-33789-9, 政府組態基準(GCB)
2. Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
3. GSMA corp., IoT Security Guidelines for Endpoint Ecosystems
4. ISO 27001, 資訊安全管理系統認證
5. MITRE corp., Common Vulnerabilities and Exposures, https://cve.mitre.org/cve/cve.html
6. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
7. OWASP.org, Top IoT Vulnerabilities, https://www.owasp.org/index.php/Top_IoT_Vulnerabilities
8. UL 2900-1, Outline of Investigation for Software Cybersecurity for Network Connectable Products, Part 1: General Requirements
9. 行動應用資安聯盟, 行動應用 App 基本資安規範 V1.1
10. 總務省･經濟產業省, IoT セキュリティガイドライン ver 1.0