影像監控系統網路攝影機資安標準之測試規範草案 (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

網路攝影機為一種可透過有線或無線網路，將數位化視訊流進行傳輸的攝影機。經由鏡頭採集圖像後，再由攝影機內感光元件及控制元件處理影像並轉換成數位訊號，傳輸到電腦後再由軟體進行圖像還原，或是透過內建處理器及網頁伺服器，以網路連線方式檢視畫面。近幾年來網路攝影機資安事件頻傳，經濟部工業局為全面改善網路攝影機資安品質，制定一系列影像監控系統相關之資安標準，並參考現行國際間物聯網資安相關規範，在考量台灣產業現況的同時接軌國際。

「影像監控系統網路攝影機資安標準之測試規範草案」，以下簡稱本測試規範，本測試規範以台灣資通產業標準協會(TAICS)所制定之標準「影像監控系統網路攝影機資安標準草案」[6] 為依據，俾作為網路攝影機製造商、系統整合商及物聯網資安檢測實驗室辦理檢測之依據，對於網路攝影機資安檢測之測試項目、測試條件、測試方法與測試標準等事項具體規範。

目錄

附圖表列

表格表列

1. 適用範圍

本規範適用於網路攝影機，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規範，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，皆不在本規範所規範之範圍內(見圖 1)。

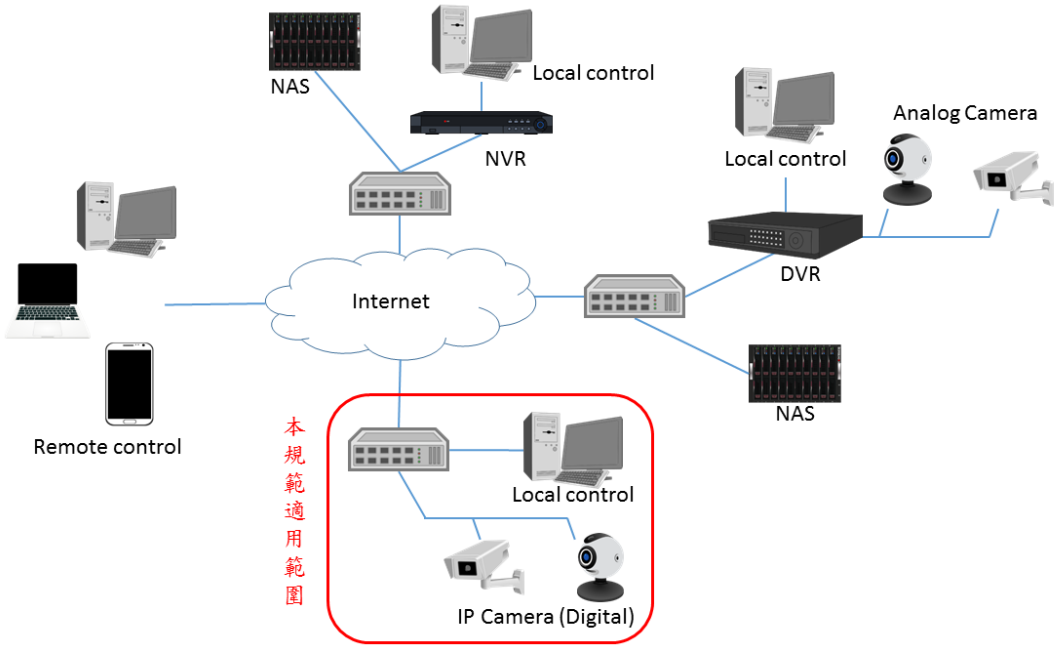

圖 1. 適用範圍示意圖

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[4]。

2.3. 漏洞評鑑系統 (Common Vulnerability Scoring System；CVSS)

一套公開評比企業資訊科技系統的安全性評鑑標準，CVSS 的判定標準，包括威脅所造成損害的嚴重性、資安漏洞的可利用程度、攻擊者不當運用該漏洞的難易度，都被列入評比。CVSS 的評分分數從 0 分到 10 分，0 代表沒有發現弱點，而 10 則代表最高風險[2]。

2.4. 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，本測試規範所指之機敏資料包括使用者帳號、密碼及敏感性資料。

2.5. 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。

2.6. 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，本測試規範所指之隱私包括網路攝影機所錄製之影音及用戶資訊。

2.7. 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。

2.8. 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、電腦版及網頁管理介面版。

2.9. 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。

2.10. 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。

2.11. 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。

2.12. 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。

2.13. 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。

2.14. 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. 網路攝影機資安測試規範

本節針對影像監控系統網路攝影機資安標準草案所制定之安全需求規範，包括：系統安全、通訊安全、身分認證與授權、隱私保護共 4 大面向，制訂相對應之測試項目；整體測試項目及判斷標準則綜整列於表 2。各測試項目之編碼原則說明如下：

- 測試項目編碼

  類別代碼，項目編碼。

- 說明:

(1) 類別代碼如下表：

表 1. 類別代碼

類別(中文)	類別(英文)	代碼
系統安全測試	System Security Testing	SYS
通訊安全測試	Communication Security Testing	COMM
身分認證與授權機制測試	Authentication and Authorization Testing	AUTH
隱私保護測試	Privacy Protection Testing	PV

- 範例：

  (1) 系統安全測試類別中的第一個測試項目「作業系統已知漏洞偵測」的測試編號為 SYS-1。

  (2) 隱私保護測試類別中的第 4 個測試項目「網路攝影機之隱私資料蒐集提示」的測試編號為 PV-4。

表 2. 實機測試之類別、項目及判定標準

主項目	測試項目	判定標準
SYS. 系統安全		
網路攝影機作業系統安全	1. 作業系統已知漏洞偵測	網路攝影機之作業系統，不得存在 CVSS 評分為最高風險 10 分之資安漏洞。
	2. 網路服務連接埠的管控	網路攝影機所開啟之網路服務連接埠必須與「廠商自我宣告表」中所宣告的「是否開啟網路埠」內容相符。
	3. 網路服務已知弱點偵測	網路攝影機所開啟之網路服務，不得存在 CVSS 評分為最高風險 10 分之資安漏洞。

網路攝影機之韌體程式安全	4. 韌體程式的更新功能	網路攝影機之更新機制必須正常運行。
	5. 韌體程式更新 - 更新路徑的保護	測項 SYS-4 之測試結果為通過，網路攝影機之韌體線上更新機制，其更新路徑必須透過安全通道保護，同時安全通道版本需符合「附錄 C」的要求且加密演算法強度需符合「附錄 A」的要求。若無提供線上更新機制，本測試結果為通過。
	6. 韌體程式更新 - 更新檔案的保護	網路攝影機之韌體手動更新機制，其更新檔案必須加密保護，且加密演算法強度需符合「附錄 A」的要求。若無提供手動更新機制，本測試結果為通過。
網路攝影機之機敏性資料儲存安全	7. 機敏資料之儲存機制	網路攝影機之程式碼與安裝檔內其他檔案，不得被檢出帳號、密碼、身分認證因子或對稱式加解密演算法之金鑰。韌體若被加密導致無法被拆解，因機敏資料不會被洩露，本測試項為通過。
	8. 機敏資料的儲存保護	網路攝影機系統檔案內之使用者帳號與密碼必須經過加密儲存，加密演算法必須符合「附錄 A」的需求，以確保演算法之強度。產品若不具備系統層管理介面，則本測試結果為通過。
網路攝影機之遠端管理介面安全	9. 網頁管理介面常見資安風險檢驗	網頁介面操控程式，不可存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。
COMM. 通訊安全		
網路攝影機之資料傳輸安全	1. 機敏資料之傳輸保護	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。
通訊介面的安全設置	2. 網路攝影機之網路裝置資訊探詢功能	網路攝影機只要有提供 UPnP、SNMP 或 Bonjour 功能，則必須提供使用者可自行開/關功能之設置。
	3. 網路攝影機之 WiFi 防護設置	網路攝影機只要具備 WPS 功能，則必須提供使用者，WPS PIN 及 WPS Lock 開/關之功能，且功能預設要為關閉。
	4. 無線網路傳輸設定	網路攝影機之無線網路預設加密格式，需符合「附錄 A」加密演算法強度要求。

網路攝影機之通訊協定安全	5. 通訊協定異常輸入檢測	網路攝影機之通訊協定(見附錄 D)，必須經過異常輸入檢測，受測之產品不得發生程序崩潰(crash)到無法恢復，則本測試結果為通過。
AUTH. 身分認證機制		
網路攝影機認證機制安全	1. API 呼叫的身分認證機制	網路攝影機之 API 的使用，必須要有身分認證機制，且其身分認證機制具備抵抗重送攻擊的能力，則本測試結果為通過。網路攝影機若未提供 API，本測試結果為通過。
	2. 遠端管理介面認證機制	透過遠端管理介面存取網路攝影機時，必須經過身分認證程序，且其身分認證機制具備抵抗重送攻擊的能力，則本測試結果為通過。網路攝影機若未提供遠端管理介面，本測試結果為通過。
	3. 操控程式與網路攝影機之間的身分認證機制	透過操控程式存取網路攝影機時，網路攝影機必須要求身分認證，且其身分認證機制具備抵抗重送攻擊的能力，則本測試結果為通過。網路攝影機若未提供操控程式，則本測試結果為通過。
	4. API 呼叫之身分認證資訊傳輸安全	API 呼叫之身分認證資訊的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。網路攝影機若未提供 API，本測試結果為通過。
	5. 遠端管理介面之身分認證資訊傳輸安全	遠端管理介面身分認證資訊的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。網路攝影機若未提供遠端管理介面，本測試結果為通過。
	6. 操控程式與網路攝影機之間身分認證資訊傳輸安全	操控程式與網路攝影機之間身分認證資訊的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。網路攝影機若未提供操控程式，則本測試結果為通過。
網路攝影機密碼認證安全	7. API 之密碼認證機制 - 密碼強度	網路攝影機之 API 呼叫，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定[1]。網路攝影機若未提供 API，本測試結果為通過。
	8. API 之密碼認證機制 - 預設密碼唯一性	網路攝影機之 API 呼叫之預設密碼都需相異。網路攝影機若未提供 API，則本測試結果為通過。

	9. 遠端管理介面之密碼認證機制 - 預設密碼唯一性	廠商所出產之網路攝影機其遠端管理介面之預設密碼都需相異。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	10. 操控程式之密碼認證機制 - 預設密碼唯一性	操控程式採用密碼認證機制，則應用程式的預設密碼應該唯一。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	11. API 之密碼認證機制 - 密碼變更機制	網路攝影機之 API 呼叫，首次授權成功必須強制更改預設密碼。網路攝影機若未提供 API，則本測試結果為通過。
	12. 遠端管理介面之密碼認證機制 - 密碼變更機制	網路攝影機之遠端管理介面，首次登入必須強制更改預設密碼。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	13. 操控程式之密碼認證機制 - 密碼變更機制	操控程式採用密碼認證機制，則首次登入必須強制更改預設密碼。網路攝影機若未提供操控程式，則本測試結果為通過。
	14. 遠端管理介面之密碼認證機制 - 密碼強度	網路攝影機之遠端管理介面，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	15. 操控程式之密碼認證機制 - 密碼強度	操控程式採用密碼認證機制，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。網路攝影機若未提供操控程式，則本測試結果為通過。
	16. API 之密碼認證機制 - 密碼的輸入頻率及次數限制	網路攝影機 API 的使用，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提供 API，則本測試結果為通過。
	17. 遠端管理介面之密碼認證機制 - 密碼的輸入頻率及次數限制	網路攝影機之遠端管理介面，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	18. 操控程式之密碼認證機制- 密碼的輸入頻率及次數限制	操控程式採用密碼認證機制，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提

		供操控程式，則本測試結果為通過。
網路攝影機之權限管控	19. API 呼叫之權限管控機制	網路攝影機 API 的使用，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」。
	20. 遠端管理介面之權限管控機制	網路攝影機之遠端管理介面，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」。
	21. 操控程式之權限管控機制	網路攝影機之操控程式，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「操控程式帳號權限說明」。
	22. API 呼叫閒置時限	API 呼叫之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供 API，本測試結果為通過。
	23. 遠端管理介面閒置時限	遠端管理介面之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供遠端管理介面，本測試結果為通過。
	24. 操控程式閒置時限	操控程式之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供操控程式，則本測試結果為通過。
PV. 隱私保護		
隱私資料的蒐集保護	1. 網路攝影機之隱私資料蒐集提示	網路攝影機在執行錄影時，應點亮錄影指示燈。若網路攝影機沒有錄影指示燈，則本測試項目為不通過。
隱私資料的存取保護	2. 網路攝影機之隱私資料的存取控制	網路攝影機所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」相符。網路攝影機若未提供遠端管理介面，則本測試結果為通過。
	3. 網路攝影機隱私資料的儲存保護	網路攝影機所儲存的隱私資料應經過加密處理，且加密演算法強度需符合「附錄 A」的要求。
	4. 網路攝影機之隱私資	網路攝影機需提供刪除隱私資料的刪除功

	料刪除功能	能，敏感性資料不以任何形式存在於網路攝影機中。
隱私資料的傳輸保護	5. 網路攝影機隱私資料的傳輸保護	網路攝影機的隱私資料不得以明文的方式傳輸，且保護資料的加密方式不得為「附錄 B」所列之公認弱加密演算法。

3.1. 系統安全測試

檢視網路攝影機之系統安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

3.1.1. 網路攝影機作業系統安全測試

3.1.1.1.測試環境

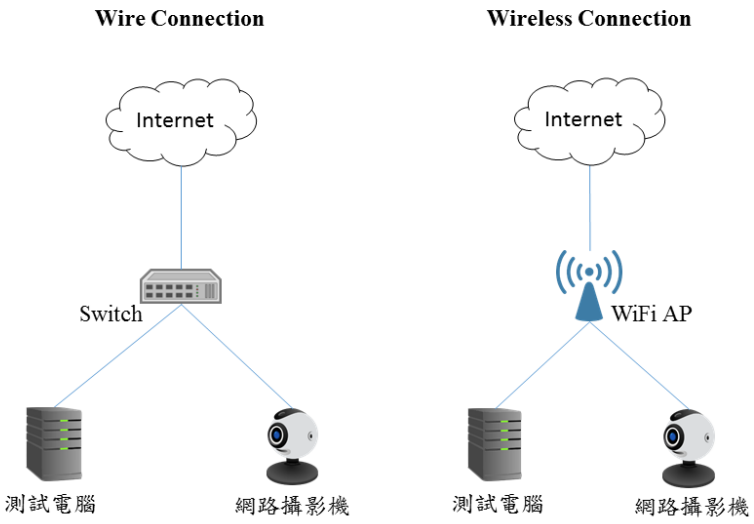

圖 2. 網路攝影機系統安全測試接續示意圖

圖 2 是網路攝影機系統安全測試架構，包括測試 PC(供測試人員連線至網路攝影機之終端設備)、有線連線(乙太網路線或光纖纜線)、無線連線(WiFi)與受測之網路攝影機，用以測試受測裝置是否符合測試規範。

3.1.1.2.SYS-1 [作業系統已知漏洞偵測]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.1.1.網路攝影機之作業系統，不得存在已揭露之重大 CVE 漏洞。

- 測試標準：

  網路攝影機之作業系統，不得存在 CVSS 評分為最高風險 10 分之資安漏洞。

- 測試方法：

  由測試 PC 連線至網路攝影機，使用弱點掃描工具對受測物之作業系統進行測試，確認檢查出之 CVE 漏洞風險級數。

3.1.1.3.SYS-2 [網路服務連接埠的管控]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.1.2.網路攝影機僅開啟必要之網路服務。

- 測試標準：

  網路攝影機所開啟之網路服務連接埠必須與「廠商自我宣告表」中所宣告的「是否開啟網路埠」內容相符。

- 測試方法：

  開啟網路服務連接埠掃瞄工具，由測試 PC 連線至網路攝影機進行測試，確認其開啟之連接埠與狀態是否和受測廠商自我宣告之內容相符。

3.1.1.4.SYS-3 [網路服務已知弱點偵測]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.1.3.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。

- 測試標準：

  網路攝影機所開啟之網路服務，不得存在 CVSS 評分為最高風險 10 分之資安漏洞。

- 測試方法：

  由測試 PC 連線至網路攝影機，使用弱點掃描工具對受測物之網路服務進行測試，確認檢查出之 CVE 漏洞風險級數。

3.1.2. 網路攝影機之韌體程式安全

3.1.2.1.測試環境

測試環境請參照圖 2。

3.1.2.2.SYS-4 [韌體程式的更新功能]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.2.1.網路攝影機必須具備韌體更新機制。

- 測試標準：

  網路攝影機之更新機制必須正常運行。

- 測試方法：

  受測廠商需配合提供測試版本之韌體更新檔案，測試人員根據產品之使用說明，進行韌體更新操作，確認韌體更新功能。

3.1.2.3.SYS-5 [韌體程式更新 - 更新路徑的保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.2.2.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。

- 測試標準：

  測項 SYS-4 之測試結果須為通過，而網路攝影機之韌體線上更新機制，其更新路徑必須透過安全通道保護，同時安全通道版本需符合「附錄 C」的要求且加密演算法強度需符合「附錄 A」的要求。若無提供線上更新機制，本測試結果為通過。

- 測試方法：

  將網路攝影機連網並啟動線上更新功能同時側錄封包，分析封包內容，確認傳輸路徑被加密保護。

3.1.2.4.SYS-6 [韌體程式更新 - 更新檔案的保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.2.2.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。

- 測試標準：

  測項 SYS-4 之測試結果為通過，網路攝影機之韌體手動更新機制，其更新檔案必須加密保護，且加密演算法強度需符合「附錄 A」的要求。若無提供手動更新機制，本測試結果為通過。

- 測試方法：

  廠商出示具備此功能證明之書面資料。當無充分資料證明具備此功能時，則請受測廠商實際示範。

3.1.3. 網路攝影機之機敏性資料儲存安全

3.1.3.1.測試環境

測試環境請參照圖 2。

3.1.3.2.SYS-7 [機敏資料之儲存機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.3.1.網路攝影機之機敏資料應避免出現於裝置韌體程式碼中。

- 測試標準：

  網路攝影機之程式碼與安裝檔內其他檔案，不得被檢出帳號、密碼、身分認證因子或對稱式加解密演算法之金鑰。韌體若被加密導致無法被拆解，因機敏資料不會被洩露，本測試項為通過。

- 測試方法：

  使用檢測工具拆解韌體，取出檔案系統目錄，確認加解密金鑰等機敏資料不得於網路攝影機韌體中被檢驗出來。

3.1.3.3.SYS-8 [機敏資料的儲存保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.3.2.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。

- 測試標準：

  網路攝影機系統檔案內之使用者帳號與密碼必須經過加密儲存，加密演算法必須符合「附錄 A」的需求，以確保演算法之強度。產品若不具備系統層管理介面，則本測試結果為通過。

- 測試方法：

  廠商應提供作業系統層管理介面之存取權限，解析檔案系統目錄，確認使用者帳號與密碼經過加密儲存，並檢視確認其加密演算法符合「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.測試環境

測試環境請參照圖 2。

3.1.4.2.SYS-9 [網頁管理介面常見資安風險檢驗]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.1.4.1.網頁管理介面不應該存在 OWASP top 10 [5]中所揭露之常見網站安全風險。

- 測試標準：

  網頁介面操控程式，不可存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。

- 測試方法：

  開啟網路攝影機之網頁介面操控程式，由測試 PC 連線至網路攝影機進行測試，使用網頁弱點掃描工具對受測物之網頁介面進行測試，檢視受測網頁介面是否存在引發 Injection 及 XSS 攻擊之資安風險。

3.2. 通訊安全測試

檢視網路攝影機之通訊安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

3.2.1. 網路攝影機之資料傳輸安全

3.2.1.1.測試環境

測試環境請參照圖 2。

3.2.1.2.COMM-1 [機敏資料之傳輸保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.2.1.1.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。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 連線至網路攝影機，開啟網路攝影機之操控程式，進行機敏資料之傳輸測試，同時側錄封包，確認封包經過加密保護，並檢視確認其加密演算法符合「附錄 A」的要求。

3.2.2. 網路介面通訊協定的安全設置

3.2.2.1.測試環境

測試環境請參照圖 2。

3.2.2.2.COMM-2 [網路攝影機之網路裝置資訊探詢功能]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.2.2.1.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。

- 測試標準：

  網路攝影機只要有提供 UPnP、SNMP 或 Bonjour 功能，則必須提供使用者可自行開/關功能之設置。

- 測試方法：

  由測試 PC 連線至網路攝影機，開啟網路攝影機之操控程式或網頁管理介面，根據「廠商自我宣告表」中所宣告的「是否開啟網路埠」內容，確認是否存在 UPnP、SNMP 或 Bonjour 的開/關操作。

3.2.2.3.COMM-3 [網路攝影機之 WiFi 防護設置]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.2.2.2.網路攝影機上不可存在不安全的無線網路設定。

- 測試標準：

  網路攝影機只要具備 WPS 功能，則必須提供使用者，WPS PIN 及 WPS Lock 開/關之功能，且該功能預設須為關閉。

- 測試方法：

  由測試 PC 連線至網路攝影機，開啟網路攝影機之操控程式，根據「廠商自我宣告表」中所宣告的「是否支援 WPS」，確認是否存在 WPS PIN 及 WPS Lock 的開/關操作，並確認預設狀態是在關閉的設定。

3.2.2.4.COMM-4 [無線網路傳輸設定]

- 測試依據：

「影像監控系統網路攝影機資安標準草案」4.2.2.2.網路攝影機上不可存在不安全的無線網路設定。

- 測試標準：

  網路攝影機之無線網路預設加密格式，需符合「附錄 A」加密演算法強度要求。

- 測試方法：

  由測試 PC 連線至網路攝影機，開啟網路攝影機之操控程式，確認其預設啟用之無線網路傳輸加密機制。

3.2.3. 網路攝影機之通訊協定安全

3.2.3.1.測試環境

測試環境請參照圖 2。

3.2.3.2.COMM-5 [通訊協定異常輸入檢測]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.2.3.1.網路攝影機之通訊協定(見附錄 D)，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。

- 測試標準：

  網路攝影機之通訊協定，(見附錄 D)必須經過異常輸入檢測，受測之產品於測試過程中不得發生程序崩潰(crash)到無法恢復運作，則本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機，執行網路攝影機之影音傳輸功能，在網路攝影機之傳輸介面上，執行對某一協定所有欄位至少 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。檢查通訊傳輸技術介面或受測系統是否仍正常運作。

3.3. 身分認證與授權測試

檢視網路攝影機之身分認證機制測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

3.3.1. 網路攝影機認證機制安全

3.3.1.1.測試環境

測試環境請參照圖 2。

3.3.1.2.AUTH-1 [API 呼叫的身分認證機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.1.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。

- 測試標準：

  網路攝影機之 API 的使用，必須要有身分認證機制，且其身分認證機制具備抵抗重送攻擊的能力，若符合上述要求，則本測試結果為通過。或網路攝影機未提供 API，本測試結果亦為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機進行 API 存取測試，確認 API 存取是否有身分認證機制，同時側錄封包，將側錄到的相關認證資訊再重新送至網路攝影機，判斷認證結果是否成功。

3.3.1.3.AUTH-2 [遠端管理介面認證機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.1.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。

- 測試標準：

  透過遠端管理介面存取網路攝影機時，必須經過身分認證程序，且其身分認證機制具備抵抗重送攻擊的能力。網路攝影機若未提供遠端管理介面，本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，觀察建立連線時，網路攝影

機是否有要求身分認證，同時側錄封包，將側錄到的相關認證資訊再重新送至網路攝影機，判斷認證結果是否成功。

3.3.1.4.AUTH-3 [操控程式與網路攝影機之間的身分認證機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.1.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。

- 測試標準：

  透過操控程式存取網路攝影機時，網路攝影機必須要求身分認證，且其身分認證機制具備抵抗重送攻擊的能力，若符合上述要求，則本測試結果為通過。或網路攝影機未提供操控程式，本測試結果亦為通過。

- 測試方法：

  由測試 PC 透過操控程式連線至網路攝影機進行測試，觀察建立連線時，網路攝影機是否有要求身分認證，同時側錄封包，將側錄到的相關認證資訊再重新送至網路攝影機，判斷認證結果是否成功。

3.3.1.5.AUTH-4 [API 呼叫之身分認證資訊傳輸安全]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.2.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。

- 測試標準：

  API 呼叫之身分認證資訊的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。網路攝影機若未提供 API，本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機進行 API 呼叫之身分認證機制，同時側錄封包，確認封包是否經過加密保護。

3.3.1.6.AUTH-5 [遠端管理介面之身分認證資訊傳輸安全]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.2.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。

- 測試標準：

  遠端管理介面身分認證資訊的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。網路攝影機若未提供遠端管理介面，本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，於連線建立階段要求身分認證時，同時側錄封包，確認封包是否經過加密保護。

3.3.1.7.AUTH-6 [操控程式與網路攝影機之間身分認證資訊傳輸安全]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.1.2.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。

- 測試標準：

  操控程式與網路攝影機之間身分認證資訊的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。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過操控程式連線至網路攝影機進行測試，於連線建立階段要求身分認證時，同時側錄封包，確認封包是否經過加密保護。

3.3.2. 網路攝影機密碼認證安全

3.3.2.1.測試環境

測試環境請參照圖 2。

3.3.2.2.AUTH-7 [API 之密碼認證機制 - 密碼強度]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.1.網路攝影機之密碼認證機制，密碼強度必須遵守「附錄 E」的要求。

- 測試標準：

  網路攝影機之 API 呼叫，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定[1]。網路攝影機若未提供 API，本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機進行 API 授權密碼輸入，確保網路攝影機之密碼長度遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。

3.3.2.3.AUTH-8 [遠端管理介面之密碼認證機制 - 密碼強度]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.1.網路攝影機之密碼認證機制，密碼強度必須遵守「附錄 E」的要求。

- 測試標準：

  網路攝影機之遠端管理介面，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，確保網路攝影機及相應之實體主控裝置之遠端管理介面之密碼長度，遵守政府組態基準（GCB）CCE-33789-9 最小密碼長度之規定。

3.3.2.4.AUTH-9 [操控程式之密碼認證機制 - 密碼強度]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.1.網路攝影機之密碼認證機制，密碼

強度必須遵守「附錄 E」的要求。

- 測試標準：

  操控程式採用密碼認證機制，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  開啟網路攝影機之操控程式，由測試 PC 連線至網路攝影機進行認證測試，確認密碼強度遵守政府組態基準(GCB) CCE-33789-9 最小密碼長度之規定。

3.3.2.5.AUTH-10 [API 之密碼認證機制 - 預設密碼唯一性]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.2.廠商所出產之網路攝影機其預設密碼都需相異。

- 測試標準：

  網路攝影機之 API 呼叫之預設密碼都需相異。網路攝影機若未提供 API，則本測試結果為通過。

- 測試方法：

  準備 2 台以上網路攝影機，由測試 PC 連線至網路攝影機進行 API 授權密碼輸入，比對每台網路攝影機的預設密碼是否唯一。

3.3.2.6.AUTH-11 [遠端管理介面之密碼認證機制 - 預設密碼唯一性]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.2.廠商所出產之網路攝影機其預設密碼都需相異。

- 測試標準：

  廠商所出產之網路攝影機其遠端管理介面之預設密碼都需相異。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  準備 2 台以上網路攝影機，由測試 PC 透過遠端管理介面連線至各網路攝影機進行測試，比對每台網路攝影機的預設密碼是否唯一。

3.3.2.7.AUTH-12 [操控程式之密碼認證機制 - 預設密碼唯一性]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.2.廠商所出產之網路攝影機其預設密碼都需相異。

- 測試標準：

  操控程式採用密碼認證機制，則應用程式的預設密碼應該唯一。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  準備 2 台以上網路攝影機，開啟網路攝影機之操控程式，由測試 PC 連線至網路攝影機進行測試，比對每台網路攝影機的預設密碼是否唯一。

3.3.2.8.AUTH-13 [API 之密碼認證機制 - 密碼變更機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.3.首次登入網路攝影機必須強制更改預設密碼。

- 測試標準：

  網路攝影機之 API 呼叫，首次授權成功必須強制更改預設密碼。網路攝影機若未提供 API，則本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機進行 API 授權密碼輸入，確認首次授權成功是否強制要求更改預設密碼。

3.3.2.9.AUTH-14 [遠端管理介面之密碼認證機制 - 密碼變更機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.3.首次登入網路攝影機必須強制更改預設密碼。

- 測試標準：

  網路攝影機之遠端管理介面，首次登入必須強制更改預設密碼。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，採用之認證方

式為使用預設的管理者帳密登入，則登入後必須要求更改預設密碼。或是不使用預設管理者帳密，必須自行創建一個遠端管理的帳號。

3.3.2.10.AUTH-15 [操控程式之密碼認證機制 - 密碼變更機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.3.首次登入網路攝影機必須強制更改預設密碼。

- 測試標準：

  操控程式採用密碼認證機制，則首次登入必須強制更改預設密碼。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  開啟網路攝影機之操控程式，由測試 PC 連線至網路攝影機進行測試，確認首次登入是否強制更改預設密碼。

3.3.2.11.AUTH-16 [API 之密碼認證機制 - 密碼的輸入頻率及次數限制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.4.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。

- 測試標準：

  網路攝影機 API 的使用，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提供 API，則本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機，進行 API 授權密碼輸入頻率與次數限制測試。

3.3.2.12.AUTH-17 [遠端管理介面之密碼認證機制 - 密碼的輸入頻率及次數限制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.4.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。

- 測試標準：

  網路攝影機之遠端管理介面，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠

商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，進行遠端連線密碼輸入頻率與次數限制之測試。

3.3.2.13.AUTH-18 [操控程式之密碼認證機制- 密碼的輸入頻率及次數限制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.2.4.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。

- 測試標準：

  操控程式採用密碼認證機制，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  開啟網路攝影機之操控程式，由測試 PC 連線至網路攝影機進行測試，進行連線密碼輸入頻率與次數限制之測試。

3.3.3. 網路攝影機遠端管理介面之權限管控

3.3.3.1.測試環境

測試環境請參照圖 2。

3.3.3.2.AUTH-19 [API 呼叫之權限管控機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.3.1.網路攝影機資源的存取，必須具備權限管控機制。

- 測試標準：

  網路攝影機 API 的使用，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」。網路攝影機若未提供 API，則本測試結果為通過。

- 測試方法：

  由測試 PC 獲取網路攝影機之 API 使用權限，查詢身分類型與權限是否與廠商自我宣告相符。

3.3.3.3.AUTH-20 [遠端管理介面之權限管控機制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.3.1.網路攝影機資源的存取，必須具備權限管控機制。

- 測試標準：

  網路攝影機之遠端管理介面，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」相符。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，登入後查詢身分類型與權限是否與廠商自我宣告相符。

3.3.3.4.AUTH-21 [操控程式之權限管控機制]

- 測試依據：

「影像監控系統網路攝影機資安標準草案」4.3.3.1.網路攝影機資源的存取，必須具備權限管控機制。

- 測試標準：

  網路攝影機之操控程式，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「操控程式帳號權限說明」相符。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  開啟網路攝影機之操控程式，由測試 PC 連線至網路攝影機進行測試，登入後查詢身分類型與權限是否與廠商自我宣告相符。

3.3.3.5.AUTH-22 [API 呼叫閒置時限]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.3.2.網路攝影機之授權行為，應存在閒置時限。

- 測試標準：

  API 呼叫之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供 API，本測試結果為通過。若網路攝影機之每次 API 呼叫皆需重新認證授權，本測試結果為通過。

- 測試方法：

  由測試 PC 連線至網路攝影機進行 API 呼叫之身分認證機制，在成功取得網路攝影機 API 授權後，閒置超過「閒置時限」，再透過操控程式操作網路攝影機，觀察是否有發出重認證之要求。

3.3.3.6.AUTH-23 [遠端管理介面閒置時限]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.3.2.網路攝影機之授權行為，應存在閒置時限。

- 測試標準：

  遠端管理介面之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供遠端管理介面，本測試結果為通過。

- 測試方法：

  由測試 PC 透過遠端管理介面連線至網路攝影機進行測試，在經過對網路攝影機認證完成後，閒置超過「閒置時限」，再透過操控程式操作網路攝影機，觀察是否有發出重新認證之要求。

3.3.3.7. AUTH-24 [操控程式閒置時限]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.3.3.2.網路攝影機之授權行為，應存在閒置時限。

- 測試標準：

  操控程式之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。網路攝影機若未提供操控程式，則本測試結果為通過。

- 測試方法：

  由測試 PC 透過操控程式連線至網路攝影機進行測試，在經過對網路攝影機認證完成後，閒置超過「閒置時限」，再透過操控程式操作網路攝影機，觀察是否有發出重新認證之要求。

3.4. 隱私保護測試

檢視網路攝影機之隱私保護需求是否符合書面送審資料，並依下列各測試項目進行實機測試。在本測試規範中，隱私資料泛指從網路攝影機端或操作界面端所收集到的影音或使用者資訊。

3.4.1. 隱私資料的蒐集保護

3.4.1.1.測試環境

測試環境請參照圖 2。

3.4.1.2.PV -1 [網路攝影機之隱私資料蒐集提示]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.4.1.1.網路攝影機在蒐集影音資料時，應給與適當的提示。

- 測試標準：

  網路攝影機在執行監控時，應點亮狀態指示燈。若網路攝影機沒有指示燈，則本測試項目為不通過。

- 測試方法：

  網路攝影機執行影像監控，檢視網路攝影機使用指南或外觀，確認指示燈的運作。

3.4.2. 隱私資料的使用保護

3.4.2.1.測試環境

測試環境請參照圖 2。

3.4.2.2.PV-2 [網路攝影機之隱私資料的存取控制]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.4.2.1.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。

- 測試標準：

  網路攝影機所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」相符。網路攝影機若未提供遠端管理介面，則本測試結果為通過。

- 測試方法：

  開啟網路攝影機之服務，登入後查詢身分類型與權限是否與廠商自我宣告相符。

3.4.2.3.PV-3 [網路攝影機隱私資料的儲存保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.4.2.2.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。

- 測試標準：

  網路攝影機所儲存的隱私資料應經過加密處理，且加密演算法強度需符合「附錄 A」的要求。

- 測試方法：

  開啟網路攝影機之服務，由測試 PC 連線至網路攝影機進行測試，確認隱私資料檔案經過加密保護。如有外接記憶體，則取出放入讀卡機，檢視是否隱私資料經過加密。

3.4.2.4.PV-4 [網路攝影機之隱私資料刪除功能]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.4.2.3.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。

- 測試標準：

  網路攝影機需提供刪除隱私資料的刪除功能，確保敏感性資料不以任何形式存在於網路攝影機中。

- 測試方法：

  檢視網路攝影機是否提供刪除隱私資料之指令或圖形化操作元件，並確認執行刪除功能後裝置中之隱私資料能被移除。

3.4.3. 隱私資料的傳輸保護

3.4.3.1.測試環境

測試環境請參照圖 2。

3.4.3.2. PV-5 [網路攝影機隱私資料的傳輸保護]

- 測試依據：

  「影像監控系統網路攝影機資安標準草案」4.4.3.1.網路攝影機隱私資料的傳送不得為明文。

- 測試標準：

  網路攝影機的隱私資料不得以明文的方式傳輸，且保護資料的加密方式不得為「附錄 B」所列之公認弱加密演算法。

- 測試方法：

  開啟網路攝影機之服務，由測試 PC 連線至網路攝影機進行封包側錄，同時分析封包是否加密，並檢視其加密演算法。

附錄 A
(規定)
加密演算法強度需求

- NIST FIPS 140-2, Annex A：Approved Security Function. [3]

附錄 B
(規定)
公認之弱加密演算法

- BASE 64 Encode and Decode
- Data Encryption Standard, DES
- Message-Digest Algorithm, MD5
- Rivest Cipher 4, RC4
- Secure Hash Algorithm 1, SHA-1

附錄 C
(規定)
安全通道版本使用要求

- Transport Layer Security (TLS) 1.1
- Transport Layer Security (TLS) 1.2

附錄 D
(規定)
網路攝影機之通訊協定

- 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 E
(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 F
(參考)
測試項目與資安要求對應總表

下表狀態欄中的 M 是 Mandatory 的縮寫，為本測試規範之強制項，而 O 則是 Option 的縮寫，為本測試規範之選擇項。

- 系統安全技術要求

編號	測試項目	狀態	技術要求
SYS-1	作業系統已知漏洞偵測	M	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
SYS-2	網路服務連接埠的管控	M	3.1.1.2.網路攝影機僅開啟必要之網路服務
SYS-3	網路服務已知弱點偵測	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
SYS-4	韌體程式的更新功能	M	3.1.2.1.網路攝影機必須具備韌體更新機制
SYS-5	韌體程式更新 - 更新路徑的保護	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
SYS-6	韌體程式更新 - 更新檔案的保護	M	
SYS-7	機敏資料之儲存機制	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
SYS-8	機敏資料的儲存保護	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
SYS-9	網頁管理介面常見資安風險檢驗	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

- 通訊安全技術要求

編號	測試項目	狀態	技術要求
COMM-1	機敏資料之傳輸保護	M	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
COMM-2	網路攝影機之網路裝置資訊探詢功能	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
COMM-3	網路攝影機之 WiFi 防護設置	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
COMM-4	無線網路傳輸設定	M	
COMM-5	通訊協定異常輸入檢測	O	3.2.3.1.網路攝影機之通訊協定，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

- 身分認證機制安全技術要求

AUTH-1	API 呼叫的身分認證機制	M	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
AUTH-2	遠端管理介面認證機制	M	
AUTH-3	操控程式與網路攝影機之間的身分認證機制	M	
AUTH-4	API 呼叫之身分認證資訊傳輸安全	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
AUTH-5	遠端管理介面之身分認證資訊傳輸安全	M	
AUTH-6	操控程式與網路攝影機之間身分認證資訊傳輸安全	M	
AUTH-7	API 之密碼認證機制 - 密碼強度	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 E」的要求
AUTH-8	遠端管理介面之密碼認證機制 - 密碼強度	M	
AUTH-9	操控程式之密碼認證機制 - 密碼強度	M	

AUTH-10	API 之密碼認證機制 - 預設密碼唯一性	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
AUTH-11	遠端管理介面之密碼認證機制 - 預設密碼唯一性	M	
AUTH-12	操控程式之密碼認證機制 - 預設密碼唯一性	M	
AUTH-13	API 之密碼認證機制 - 密碼變更機制	O	3.3.2.3.首次登入網路攝影機必須強制更改預設密碼
AUTH-14	遠端管理介面之密碼認證機制 - 密碼變更機制	O	
AUTH-15	操控程式之密碼認證機制 - 密碼變更機制	O	
AUTH-16	API 之密碼認證機制 - 密碼的輸入頻率及次數限制	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
AUTH-17	遠端管理介面之密碼認證機制 - 密碼的輸入頻率及次數限制	M	
AUTH-18	操控程式之密碼認證機制-密碼的輸入頻率及次數限制	M	
AUTH-19	API 呼叫之權限管控機制	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
AUTH-20	遠端管理介面之權限管控機制	M	
AUTH-21	操控程式之權限管控機制	M	

AUTH-22	API 呼叫閒置時限	M	3.3.3.2.網路攝影機之授權行為，應存在閒置時限。
AUTH-23	遠端管理介面閒置時限	M	
AUTH-24	操控程式閒置時限	M	

- 隱私保護技術要求

編號	測試項目	狀態	技術要求
PV-1	網路攝影機之隱私資料蒐集提示	O	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
PV-2	網路攝影機之隱私資料的存取控制	M	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
PV-3	網路攝影機隱私資料的儲存保護	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
PV-4	網路攝影機之隱私資料刪除功能	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
PV-5	網路攝影機隱私資料的傳輸保護	M	3.4.3.1.網路攝影機隱私資料的傳送不得為明文

附錄 G
(規定)
廠商自我宣告表-1

<table>
<tr><th colspan="5">受測物基本資訊</th><th>SYS-2</th><th>AUTH</th><th>SYS-4</th><th>AUTH</th><th>AUTH-22</th></tr>
<tr><td>項次</td><td>受測物名稱及型號</td><td>製造廠商</td><td>受測物作業系統版本</td><td>受測物韌體版本</td><td>是否開啟網路埠</td><td>是否提供API</td><td>是否支援韌體更新</td><td>支援遠端管理介面</td><td>裝置 API 帳號權限說明</td></tr>
<tr><td rowspan="4">1</td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4">☐ 否
☐ 是
固定埠號(服務)：
_____
_____
動態埠號範圍(服務)：
_____
_____</td><td rowspan="4">☐ 否
☐ 是</td><td rowspan="4">☐ 否
☐ 是，線上更新
☐ 是，手動更新</td><td rowspan="4">☐ 否
☐ 是</td><td></td></tr>
<tr><td>AUTH-23</td></tr>
<tr><td>遠端管理介面帳號權限說明</td></tr>
<tr><td></td></tr>
</table>

附錄 H
(規定)
廠商自我宣告表-2

受測物基本資訊					AUTH	AUTH-24	COMM-3	AUTH-19 AUTH-20 AUTH-21	AUTH-7 AUTH-8 AUTH-9
項次	受測物名稱及型號	製造廠商	受測物作業系統版本	受測物韌體版本	是否提供操控程式	操控程式帳號權限說明	是否支援 WPS	登入錯誤次數與對應之鎖定時間	閒置時限
1					□ 否 □ 網頁版 □ 行動 App 版 □ 電腦版 □ 其他： _____		□ 否 □ 是		

附錄 I
(規定)
廠商自評檢核表

評估類別與項目：SYS. 系統安全		自我評估				註記
		完全實施	部份實施	尚未實施	不適用	
網路攝影機作業系統安全	1. 網路攝影機之作業系統，不得存在 CVSS 評分為最高風險 10 分之資安漏洞					
	2. 網路攝影機所開啟之網路服務連接埠必須與「廠商自我宣告表」中所宣告的「是否開啟網路埠」相符					
	3. 網路攝影機所開啟之網路服務，不得存在 CVSS 評分為最高風險 10 分之資安漏洞					
網路攝影機之韌體程式安全	4. 網路攝影機之更新機制應正常運行					
	5. 網路攝影機之韌體線上更新機制，其更新路徑必須透過安全通道(Security Tunnel)保護，同時安全通道版本需符合「附錄 C」的要求且加密演算法強度需符合「附錄 A」的要求。					
	6. 網路攝影機之韌體手動更新機制，其更新檔案必須加密保護，且加密演算法強度需符合「附錄 A」的要求。					
網路攝影機之機敏性資料儲存安全	7. 網路攝影機之程式碼與安裝檔內其他檔案，不得被檢出帳號、密碼、身分認證因子或對稱式加解密演算法之金鑰					
	8. 網路攝影機系統檔案內之使用者帳號與密碼必須經過加密儲存，加密演算法必須符合「附錄 A」的需求，以確保演算法之強度。					
網路攝影機之遠端管理介面安全	9. 網頁介面操控程式，不可存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險					
評估類別與項目：COMM. 通訊安全		自我評估				註記
		完全實	部份實	尚未實	不適用	

		施	施	施		
網路攝影機之資料傳輸安全	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					
通訊介面的安全設置	2. 網路攝影機只要有提供 UPnP、SNMP 或 Bonjour 功能，則必須提供使用者可自行開/關功能之設置					
	3. 網路攝影機只要具備 WPS 功能，則必須提供使用者，WPS PIN 及 WPS Lock 開/關之功能，且功能預設要為關閉					
	4. 網路攝影機之無線網路預設加密格式，需符合「附錄 A」加密演算法強度要求					
網路攝影機之通訊協定安全	5. 網路攝影機之通訊協定，應具備通訊協定內容的錯誤處理能力，即經過異常輸入檢測不會發生程序崩潰(crash)到無法恢復的情形					
評估類別與項目：AUTH. 身分認證與授權		**自我評估**				**註記**
		完全實施	部份實施	尚未實施	不適用	
網路攝影機認證機制安全	1. 網路攝影機之 API 的使用，必須要有身分認證機制，且其身分認證機制具備抵抗重送攻擊的能力					
	2. 透過遠端管理介面存取網路攝影機時，必須經過身分認證程序，且其身分認證機制具備抵抗重送攻擊的能力					
	3. 透過操控程式存取網路攝影機時，網路攝影機必須要求身分認證，且其身分認證機制具備抵抗重送攻擊的能力					
	4. API 呼叫之身分認證資訊的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。					
	5. 遠端管理介面身分認證資訊的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。					
	6. 操控程式與網路攝影機之間身分認證資訊的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。					
網路攝影機密碼認證安全	7. 網路攝影機之 API 呼叫，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。					
	8. 網路攝影機之 API 呼叫之預設密碼都需相異。					
	9. 網路攝影機之 API 呼叫，首次授權成功必須強制更改預設密碼。					
	10. 網路攝影機 API 的使用，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。					
	11. 網路攝影機之遠端管理介面，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。					
	12. 廠商所出產之網路攝影機其遠端管理介面之預設密碼都需相異。					
	13. 網路攝影機之遠端管理介面，首次登入必須強制更改預設密碼。					
	14. 網路攝影機之遠端管理介面，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。					
	15. 操控程式採用密碼認證機制，密碼強度必須遵守政府組態基準（GCB） CCE-33789-9 最小密碼長度之規定。					
	16. 操控程式採用密碼認證機制，則應用程式的預設密碼應該唯一。					
	17. 操控程式採用密碼認證機制，則首次登入必須強制更改預設密碼。					
	18. 操控程式採用密碼認證機制，其授權密碼的嘗試有輸入頻率及次數的限制，需與「廠商自我宣告表」中所宣告之「登入錯誤次數與對應之鎖定時間」相符。					
網路攝影機遠端管理介面之權限管控	19. 網路攝影機 API 的使用，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」。					
	20. 網路攝影機之遠端管理介面，必須具備權限管控					

	機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」。					
	21. 網路攝影機之操控程式，必須具備權限管控機制，該使用者的身分授權需與「廠商自我宣告表」所宣告之「操控程式帳號權限說明」。					
	22. API 呼叫之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。。					
	23. 遠端管理介面之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。					
	24. 操控程式之閒置時限，需與「廠商自我宣告表」中所宣告之「閒置時限」相符。					
評估類別與項目：PV. 隱私保護		**自我評估**				**註記**
		完全實施	部份實施	尚未實施	不適用	
隱私資料的蒐集保護	25. 網路攝影機在執行監控時，應點亮狀態指示燈。若網路攝影機沒有指示燈，則本測試項目為不通過。					
隱私資料的存取保護	26. 網路攝影機所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權需與「廠商自我宣告表」所宣告之「遠端管理介面帳號權限說明」相符。					
	27. 網路攝影機所儲存的隱私資料應經過加密處理，且加密演算法強度需符合「附錄 A」的要求。					
	28. 網路攝影機之隱私資料刪除功能。					
隱私資料的傳輸保護	29. 網路攝影機的隱私資料不得以明文的方式傳輸，且保護資料的加密方式不得為「附錄 B」所列之公認弱加密演算法。					

附錄 J
(規定)
網路攝影機資安測試申請表

<table>
<tr><td colspan="8">網路攝影機資安測試申請表</td></tr>
<tr><td rowspan="6">廠商資料</td><td colspan="5">公司名稱：</td><td colspan="2" rowspan="6">(請蓋公司章)</td></tr>
<tr><td colspan="5">公司地址：</td></tr>
<tr><td colspan="5">負責人：</td></tr>
<tr><td colspan="5">申請人：　　申請日期：</td></tr>
<tr><td colspan="5">電話：　　傳真：</td></tr>
<tr><td colspan="5">Email：</td></tr>
<tr><td rowspan="4">受理單位</td><td colspan="7">單位名稱：</td></tr>
<tr><td colspan="7">聯絡人：</td></tr>
<tr><td colspan="7">電話：　　傳真：</td></tr>
<tr><td colspan="7">Email：</td></tr>
<tr><td rowspan="4">送測設備</td><td>模組型式</td><td colspan="6"></td></tr>
<tr><td>設備型號</td><td>軟體版本</td><td>韌體版本</td><td>設備日期</td><td>數量</td><td colspan="2">備註</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="4">審查報告</td><td>文件編號</td><td colspan="3">文件名稱</td><td>數量</td><td colspan="2">備註</td></tr>
<tr><td></td><td colspan="3"></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2">申請測試內容</td><td colspan="3">☐新申請案件</td><td colspan="3">☐補申請案件</td></tr>
<tr><td colspan="8">送測廠商簽名:_____</td></tr>
</table>

參考資料

1. CCE-33789-9, 政府組態基準(GCB)
2. First.org, Inc., Common Vulnerability Scoring System, V3 Development Update, https://www.first.org/cvss
3. Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
4. MITRE corp., Common Vulnerabilities and Exposures, https://cve.mitre.org/cve/cve.html
5. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
6. 台灣資通產業標準協會(TAICS), 影像監控系統網路攝影機資安標準草案