影像監控系統資安標準之測試規範
草案–網路攝影機
(V0.1.0)

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

2017-09-02

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
V0.1.0	2017/9/2	高傳凱	無	新建立

目錄

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，計劃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，以協助台灣產業接軌國際。

「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」[5] 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，並具體規範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。

1. 適用範圍

泛指應用於影像監控系統的攝影機，且凡是攝影機本身具連網功能者皆是網路攝影機的一種，如圖 1 紅框處所示。

本標準為確保網路攝影機資安，訂定其產品之安全技術要求，擬分為五大面向做為評測要項，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護。

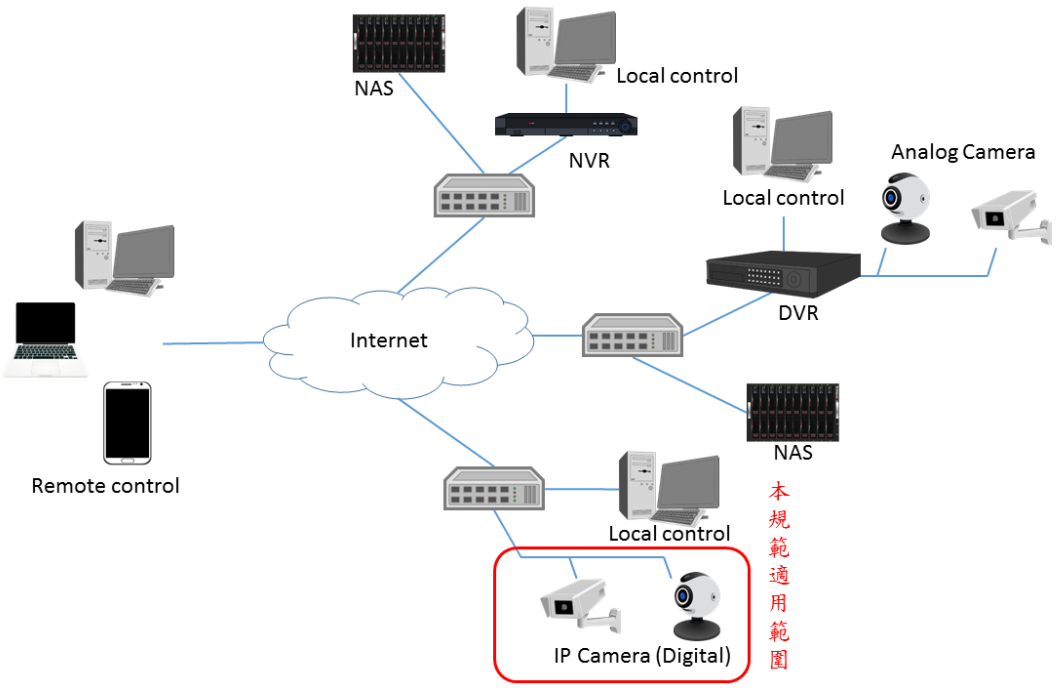

圖 1. 適用範圍示意圖

2. 用語及定義

下列用語與定義適用於本標準。

2.1. 網路攝影機 (IP Camera)

係指一種主要用於影像監控系統且具連網功能的攝影機，其應用類型包括：網路攝影機(IP camera)、智能家庭攝影機(smart camera)及 3D 攝影機(3D camera)等。

2.2. 資訊安全弱點 (Security Vulnerability)

指受測裝置安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。

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

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

2.4. 已知安全性弱點（Known Security Vulnerabilities）

係指 2.3 常見弱點與漏洞中各編號之漏洞。

2.5. 國家弱點資料庫 (National Vulnerabilities Database)

美國國家標準技術研究所（NIST）的國家弱點資料庫[3]，負責 2.3 常見弱點與漏洞資料的發布及更新。

2.6. 敏感性資料 (Sensitivity Data)

指依使用者行為或行動應用程式之運作，於裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限於個人資料、密碼、地理位置。

2.7. 個人資料 (Personally Identifiable Information)

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚

姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

2.8. 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。

2.9. 遠端管理介面 (Remote Control Management, RCM)

係指透過網路由遠端裝置上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。

2.10. 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。

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

係指軟體系統不同組成部分銜接的約定。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。

2.12. 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。

2.13. 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。

2.14. 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。

2.15. 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)。

2.16. 安全區域 (Secure Domain)

係指與正常作業環境隔離出的區域，僅用於執行安全性相關操作，如：加解密、金鑰管理、完整性檢查，並保存敏感性資料用。

2.17. 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。

2.18. 預設密碼 (Default Password)

係指產品在用戶初次將其連上網路，且在未更改任何設定的情況下，用以登入網路攝影機之密碼。

3. 測試項目分級

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：實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護共 5 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。

表 1. 實機測試項目分級總表

安全面向	安全要求分類	安全保證分級		
		一級	二級	三級
實體安全測試	4.1.1. 實體埠之安全管控測試	4.1.1.1	4.1.1.2	4.1.1.2
	4.1.2. 實體異常行為警示測試		4.1.2.1	4.1.2.1
	4.1.3. 實體防護測試		4.1.3.1	4.1.3.2
	4.1.4. 安全啟動測試			4.1.4.1
系統安全測試	4.2.1. 作業系統安全測試	4.2.1.1	4.2.1.2	4.2.1.3
	4.2.2. 網路服務連接埠的管控測試	4.2.2.1	4.2.2.1	4.2.2.1
	4.2.3. 網路服務安全測試	4.2.3.1	4.2.3.2	4.2.3.3
	4.2.4. 更新安全測試	4.2.4.1	4.2.4.2	4.2.4.2
	4.2.5. 韌體程式安全測試	4.2.5.1	4.2.5.1	4.2.5.2
	4.2.6. 敏感資料儲存安全測試	4.2.6.1	4.2.6.1	4.2.6.2

	4.2.7.網頁管理介面安全測試	4.2.7.1	4.2.7.1	4.2.7.1
	4.2.8.API 安全測試	4.2.8.1	4.2.8.1	4.2.8.2
	4.2.9.系統日誌檔與警示測試	4.2.9.1	4.2.9.2	4.2.9.2
通訊安全測試	4.3.1.資料傳輸安全測試	4.3.1.1	4.3.1.1	4.3.1.2
	4.3.2.網路介面通訊協定的安全設置測試	4.3.2.1	4.3.2.1	4.3.2.1
	4.3.3.通訊協定安全測試		4.3.3.1	4.3.3.1
身分認證與授權機制安全測試	4.4.1.認證機制安全測試	4.4.1.1	4.4.1.1	4.4.1.2
	4.4.2.密碼認證安全測試	4.4.2.1	4.4.2.1	4.4.2.1
	4.4.3.權限管控安全測試	4.4.3.1	4.4.3.1	4.4.3.1
隱私保護測試	4.5.1. 隱私資料的使用保護測試	4.5.1.1	4.5.1.1	4.5.1.1
	4.5.2. 隱私資料的傳輸保護測試	4.5.2.1	4.5.2.2	4.5.2.3

3.1. 安全保證第一級測試標準

表 2　第一級測試標準

測試類別	測試標準
實體安全測試	
實體埠之安全管控測試	4.1.1.1A 在實體埠的安全管控上，不得被利用來存取產品之作業系統，且原用於除錯和測試功能及外接儲存媒體用必須關閉 4.1.1.1B 除錯和測試及外接儲存媒體用功能必須關閉 4.1.1.1C 外接實體埠的插拔操作須提供日誌記錄
作業系統安全測試	
作業系統安全測試	4.2.1.1A 作業系統不得存在 CVSS 評分為最高風險 10 分之資安漏洞，則本測試項目結果為通過
網路服務連接埠的管控測試	4.2.2.1A 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，則本測試項目結果為通過
網路服務安全測試	4.2.3.1A 檢測網路服務是否存在 CVSS v3 評分為 10 分之常見資安弱點與漏洞
更新安全測試	4.2.4.1A 更新機制必須正常運行，則本測試項目結果為通過 4.2.4.1B 測項 4.2.4.1A 之測試結果必須為通過 韌體手動更新機制，其更新檔案必須加密保護，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。若無提供手動更新機制，則本測試結果為通過 4.2.4.1C 測項 4.2.4.1A 之測試結果必須為通過 韌體線上更新機制，其更新路徑必須透過安全通道保護，同時安全通道版本須符合「附錄 B」的要求，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。若無提供線上更新機制，本測試結果為通過
韌體程式安全測試	4.2.5.1A 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，本測試結果為通過
敏感資料儲存安全測試	4.2.6.1A 系統檔案內之使用者帳號、密碼、憑證及金鑰必須經過加密儲存，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]，以確保演算法

	之強度。產品若不具備系統層管理介面，則本測試項目結果為通過
網頁管理介面安全測試	4.2.7.1A 網頁管理介面操控程式，不得存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。若產品不具有網頁管理介面，則本測試項目結果為通過
API 安全測試	4.2.8.1A 產品之 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，則本測試項目結果為通過。或網路攝影機未提供 API，本測試項目結果亦為通過 4.2.8.1B 從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過 4.2.8.1C 網路攝影機之 API 密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過 4.2.8.1D 網路攝影機之 API 呼叫之預設密碼都須相異。網路攝影機若未提供 API，則本測試項目結果為通過 4.2.8.1E 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 4.2.8.1F 網路攝影機 API 的使用，其認證密碼的嘗試有輸入頻率及次數的限制，須與「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 4.2.8.1G 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須與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」相符，並且至少要有一般使用者與系統管理者二個不同權限之角色。網路攝影機若未提供 API，則本測試項目結果為通過 4.2.8.1H API 呼叫之閒置時限，須與「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，本測試項目結果為通過。若網路攝影機之每次 API 呼叫皆須重新認證授權，本測試結果為通過
系統日誌檔與警示測試	4.2.9.1A 安全事件日誌的資料應包含時間、使用者身分及操作行為。產品若不具有可檢視之安全事件日誌功能，則本測試項目結果為失敗 4.2.9.1B 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須與「廠商自我宣告表」所宣告之「日誌檔權限說明」相符，

	則本測試項目結果為通過
通訊安全測試	
資料傳輸安全測試	4.3.1.1A 敏感資料之網路傳輸必須經過加密保護，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]
網路介面通訊協定的安全設置測試	4.3.2.1A UPnP、SNMP 或 Bonjour 功能必須提供使用者可自行開/關功能之設置 4.3.2.1B 產品只要具備 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 4.3.2.1C 無線網路預設加密模式必須使用 WPA2
遠端管理介面與操控程式之身分認證與授權安全測試	
身分認證與授權機制安全	4.4.1.1A 透過遠端管理介面與操控程式存取網路攝影機時，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 4.4.1.1B 從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過
	4.4.2.1A 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過 4.4.2.1B 廠商所出產之網路攝影機其遠端管理介面與操控程式之預設密碼都須相異。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.2.1C 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，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 4.4.2.1D 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其授權密碼的嘗試有輸入頻率及次數的限制，須與「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
	4.4.3.1A 網路攝影機之遠端管理介面與操控程式，必須具備權限管控機制，該使用者的身分授權須與「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，並且至少要有一般使用者與系統管理者二

	個不同權限之角色。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.3.1B 產品之其它角色不能擁有系統管理者特權，則本測試項目結果為通過 4.4.3.1C 遠端管理介面之閒置時限，須與「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
隱私保護測試	
隱私資料的使用保護測試	4.5.1.1A 產品所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與「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 4.5.1.1B 必須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
隱私資料的傳輸保護測試	4.5.2.1A 影像類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 A」所列之公認弱加密演算法。非影像類隱私資料之傳輸加密演算法須使用 FIPS 140-2 所核可之加密演算法[3]

3.2. 安全保證第二級測試標準

表 3. 第二級測試標準

測試類別	測試標準
實體安全測試	
實體埠之安全管控測試	4.1.1.2A 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，必須移除
實體異常行為警示測試	4.1.2.1A 產品於實體操作出現異常時須提供警示機制，包括：鏡頭被異物遮敝時、實體設備遭竊取時或實體設備遭受破壞時，例如：機殼、元件被拆除
實體防護測試	4.1.3.1A 產品之外殼應該使用鐵殼來增加被暴力破壞的難度，或者是透過防盜螺絲來迫使拆解變得更加困難
作業系統安全測試	
作業系統安全測試	4.2.1.2A 作業系統不得存在 CVSS 評分為最高風險 9 分之資安漏洞，則本測試項目結果為通過
網路服務連接埠的管控測試	4.2.2.1A 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，則本測試項目結果為通過
網路服務安全測試	4.2.3.2A 網路服務不得存在 CVSS 評分為最高風險 9 分之資安漏洞，則本測試項目結果為通過
更新安全測試	4.2.4.2A 測項 4.2.4.1A 檢測結果必須是通過 更新機制僅可透過線上更新的方式，若提供使用者手動更新機制，則本測試結果為失敗 4.2.4.2B 測項 4.2.4.1A 檢測結果必須是通過 經過竄改之更新檔案不得被成功更新，則本測試項目結果為通過
韌體程式安全測試	4.2.5.1A 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，本測試結果為通過
敏感資料儲存安全測試	4.2.6.1A 系統檔案內之使用者帳號、密碼、憑證及金鑰必須經過加密儲存，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]，以確保演算法

	之強度。產品若不具備系統層管理介面，則本測試項目結果為通過
網頁管理介面安全測試	4.2.7.1A 網頁管理介面操控程式，不得存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。若產品不具有網頁管理介面，則本測試項目結果為通過
API 安全測試	4.2.8.1A 產品之 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，則本測試項目結果為通過。或網路攝影機未提供 API，本測試項目結果亦為通過 4.2.8.1B 從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過 4.2.8.1C 網路攝影機之 API 密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過 4.2.8.1D 網路攝影機之 API 呼叫之預設密碼都須相異。網路攝影機若未提供 API，則本測試項目結果為通過 4.2.8.1E 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 4.2.8.1F 網路攝影機 API 的使用，其認證密碼的嘗試有輸入頻率及次數的限制，須與「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 4.2.8.1G 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須與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」相符，並且至少要有一般使用者與系統管理者二個不同權限之角色。網路攝影機若未提供 API，則本測試項目結果為通過 4.2.8.1H API 呼叫之閒置時限，須與「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，本測試項目結果為通過。若網路攝影機之每次 API 呼叫皆須重新認證授權，本測試結果為通過
系統日誌檔與警示測試	4.2.9.2A 測項 4.2.9.1A 檢測結果必須是通過。 登入警示通知機制應與產品說明一致。產品若不具有登入警示功能，則本測試項目結果為失敗 4.2.9.2B 測項 4.2.9.1A 檢測結果必須是通過。

	警示通知機制應與產品說明一致。產品若不具有日誌紀錄檔無法儲存之異常警示功能，則本測試項目結果為失敗
通訊安全測試	
資料傳輸安全測試	4.3.1.1A 敏感資料之網路傳輸必須經過加密保護，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]
網路介面通訊協定的安全設置測試	4.3.2.1A UPnP、SNMP 或 Bonjour 功能必須提供使用者可自行開/關功能之設置 4.3.2.1B 產品只要具備 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 4.3.2.1C 無線網路預設加密模式必須使用 WPA2
通訊協定安全測試	4.3.3.1A 通訊協定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。
遠端管理介面與操控程式之身分認證與授權安全測試	
身分認證與授權機制安全	4.4.1.1A 透過遠端管理介面與操控程式存取網路攝影機時，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 4.4.1.1B 從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過
	4.4.2.1A 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過 4.4.2.1B 廠商所出產之網路攝影機其遠端管理介面與操控程式之預設密碼都須相異。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.2.1C 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，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 4.4.2.1D 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其授權密碼的嘗試有輸入頻率及次數的限制，須與「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

	4.4.3.1A 網路攝影機之遠端管理介面與操控程式，必須具備權限管控機制，該使用者的身分授權須與「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，並且至少要有一般使用者與系統管理者二個不同權限之角色。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.3.1B 產品之其它角色不能擁有系統管理者特權，則本測試項目結果為通過 4.4.3.1C 遠端管理介面之閒置時限，須與「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
隱私保護測試	
隱私資料的使用保護測試	4.5.1.1A 產品所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與「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 4.5.1.1B 必須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
隱私資料的傳輸保護測試	4.5.2.2A 隱私資料之傳輸加密演算法須使用 FIPS 140-2 所核可之加密演算法[3]

3.3. 安全保證第三級測試標準

表 4 第三級測試標準

測試類別	測試標準
實體安全測試	
實體埠之安全管控測試	4.1.1.2A 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，必須移除
實體異常行為警示測試	4.1.2.1A 產品於實體操作出現異常時須提供警示機制，包括：鏡頭被異物遮敝時、實體設備遭竊取時或實體設備遭受破壞時，例如：機殼、元件被拆除
實體防護測試	4.1.3.2A 測項 4.1.3.1A 之測試結果必須為通過 除達到產品不能被輕易破壞要求，晶片與功能編號不可存在於電路板 4.1.3.2A 測項 4.1.3.1A 之測試結果必須為通過 產品實體上不得存在可輕易一鍵還原回預設密碼的設計，即不須透過任何工具，可輕易在產品實體上一鍵還原回預設密碼須避免
安全啟動測試	4.1.4.1A. 確保產品於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，一旦系統的完整性及可信度獲得保證，產品始得開機
作業系統安全測試	
作業系統安全測試	4.2.1.3A 作業系統不得存在 CVSS 評分為最高風險 7 分之資安漏洞，則本測試項目結果為通過
網路服務連接埠的管控測試	4.2.2.1A 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，則本測試項目結果為通過
網路服務安全測試	4.2.3.3A 網路服務不得存在 CVSS 評分為最高風險 7 分之資安漏洞，則本測試項目結果為通過
更新安全測試	4.2.4.2A 測項 4.2.4.1A 檢測結果必須是通過 更新機制僅可透過線上更新的方式，若提供使用者手動更新機制，則本測試結果為失敗 4.2.4.2B 測項 4.2.4.1A 檢測結果必須是通過 經過竄改之更新檔案不得被成功更新，則本測試項目結果為通過

韌體程式安全測試	4.2.5.2A 韌體之原始碼掃描報告不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors，則本測試項目結果為通過
敏感資料儲存安全測試	4.2.6.2A 產品須具備安全區域，且敏感資料須存放於此，則本測試項目結果為通過。
網頁管理介面安全測試	4.2.7.1A 網頁管理介面操控程式，不得存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。若產品不具有網頁管理介面，則本測試項目結果為通過
API 安全測試	4.2.8.2A 測項 4.2.8.1 之測試結果必須為通過 產品所提供之 API 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，則本測試項目結果為通過
系統日誌檔與警示測試	4.2.9.2A 測項 4.2.9.1A 檢測結果必須是通過。 登入警示通知機制應與產品說明一致。產品若不具有登入警示功能，則本測試項目結果為失敗 4.2.9.2B 測項 4.2.9.1A 檢測結果必須是通過。 警示通知機制應與產品說明一致。產品若不具有日誌紀錄檔無法儲存之異常警示功能，則本測試項目結果為失敗
通訊安全測試	
資料傳輸安全測試	4.3.1.2A 與支援 AES-256 之伺服器連線並成功將資料正確還原，則本測試項目結果為通過
網路介面通訊協定的安全設置測試	4.3.2.1A UPnP、SNMP 或 Bonjour 功能必須提供使用者可自行開/關功能之設置 4.3.2.1B 產品只要具備 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 4.3.2.1C 無線網路預設加密模式必須使用 WPA2
通訊協定安全測試	4.3.3.1A 通訊協定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
遠端管理介面與操控程式之身分認證與授權安全測試	
身分認證與授權機制安全	4.4.1.2A 測項 4.4.1.1A 檢測結果必須是通過 認證機制須透過公開金鑰基礎建設才可以認證，若可採用其它認證方式

	登入至網路攝影機，則此測試項目結果為失敗
	4.4.2.1A 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過 4.4.2.1B 廠商所出產之網路攝影機其遠端管理介面與操控程式之預設密碼都須相異。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.2.1C 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，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 4.4.2.1D 透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其授權密碼的嘗試有輸入頻率及次數的限制，須與「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
	4.4.3.1A 網路攝影機之遠端管理介面與操控程式，必須具備權限管控機制，該使用者的身分授權須與「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，並且至少要有一般使用者與系統管理者二個不同權限之角色。網路攝影機若未提供遠端管理介面，則本測試結果為通過 4.4.3.1B 產品之其它角色不能擁有系統管理者特權，則本測試項目結果為通過 4.4.3.1C 遠端管理介面之閒置時限，須與「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
隱私保護測試	
隱私資料的使用保護測試	4.5.1.1A 產品所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與「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 4.5.1.1B 必須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
隱私資料的傳輸保護測試	4.5.2.3A 與支援 AES-256 之伺服器連線並成功將資料正確還原，則本測試項目結果為通過

4. 資安測試規範

4.1. 實體安全測試

4.1.1. 實體埠之安全管控測試

圖 2 是作業系統安全測試架構，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。

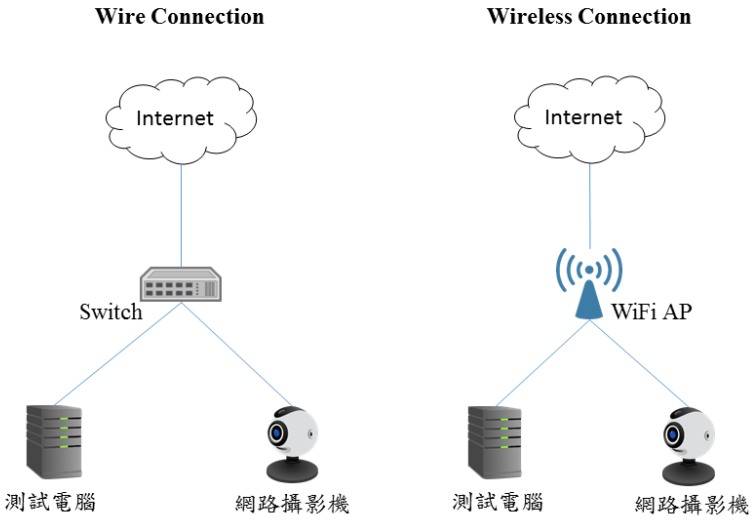

圖 2. 系統安全測試接續示意圖

4.1.1.1. 實體埠安全管控測試

A. 實體埠存取管控測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1A. 在實體埠的安全管控上，不得被利用來存取產品之作業系統。

- 測試標準：

在實體埠的安全管控上，不得被利用來存取產品之作業系統。

- 測試方法：

廠商須提供產品除錯、測試功能及外接儲存媒體的使用指南，檢視其功能為關閉狀態。

B. 實體埠功能管控測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1B. 實體埠採最小數量使用原則，沒使用到的實體埠可以被關閉，即用於除錯和測試及外接儲存媒體用功能必須關閉。

- 測試標準：

除錯和測試及外接儲存媒體用功能必須關閉。

- 測試方法：

依據產品規格之功能，檢視是否有非必要功能的實體埠，並符合產品規格書之規範。

C. 實體行為日誌功能測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1C. 外接實體埠的插拔操作須提供日誌記錄。

- 測試標準：

外接實體埠的插拔操作須提供日誌記錄。

- 測試方法：

廠商須提供實體埠的插拔之記錄檔位置，檢視是否有其日誌記錄。

4.1.1.2. 最小實體介面測試

A. 最小實體介面測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.2A. 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，必須移除。

- 測試標準：

所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，必須移除。

- 測試方法：

依據產品規格之功能，不得存在非必要之外接式儲存媒體使用的插槽，並於電路板不得檢出具有除錯或測試用途之界面。

4.1.2. 實體異常行為警示測試

測試環境請參照圖 2。

4.1.2.1. 異常狀態警示機制

A. 異常狀態警示機制

- 測試依據：

  「影像監控系統資安標準草案-網路攝影機」4.1.2.1A. 產品於實體操作出現異常時須提供警示機制，包括：鏡頭被異物遮敝時、實體設備遭竊取時或實體設備遭受破壞時，例如：機殼、元件被拆除。

- 測試標準：

  產品於實體操作出現異常時須提供警示機制，包括：鏡頭被異物遮敝時、實體設備遭竊取時或實體設備遭受破壞時，例如：機殼、元件被拆除。

- 測試方法：

  影像錄影機之前端攝影機，若鏡頭被異物遮敝時須提供警示機制。影像錄影機之前端攝影機，其實體設備應具備遭竊取之警示機制。影像錄影機之實體設備遭受破壞，例如：機殼、元件被拆除，須提供警示機制，例如：E-Mail 通知、訊息推播、蜂鳴器等。

4.1.3. 實體防護測試

測試環境請參照圖 2。

4.1.3.1. 實體保護測試

A. 實體保護測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.3.1A. 產品在實體上要有一定程度的防護，可能的做法是產品之外殼應該使用鐵殼來增加被暴力破壞的難度，或者是透過防盜螺絲來迫使拆解變得更加困難。

- 測試標準：

產品之外殼應該使用鐵殼來增加被暴力破壞的難度，或者是透過防盜螺絲來迫使拆解變得更加困難。

- 測試方法：

影像錄影機之機殼不能被拆除，可能的做法是產品之外殼應該使用鐵殼來增加被暴力破壞的難度，或者是透過防盜螺絲來迫使拆解變得更加困難。

4.1.3.2. 實體設計安全測試

A. 內部實體安全測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」除達到 4.1.3.1 要求外，晶片與功能編號不得存在於電路板。

- 測試標準：

測項 4.1.3.1A 之測試結果必須為通過。

除達到產品不能被輕易破壞要求，晶片與功能編號不可存在於電路板。

- 測試方法：

影像錄影機之晶片與功能編號不能存在於電路板，檢視其電路板是否存在晶片與功能編號之文字。

B. 密碼還原機制安全設計

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.3.2B. 除達到 4.1.3.1 要求外，產品實體上不得存在可輕易一鍵還原回預設密碼的設計，即不須透過任何工具，可輕易在產品實體上一鍵還原回預設密碼須避免。

- 測試標準：

測項 4.1.3.1A 之測試結果必須為通過。

產品實體上不得存在可輕易一鍵還原回預設密碼的設計，即不須透過任何工具，可輕易在產品實體上一鍵還原回預設密碼須避免。

- 測試方法：

依據廠商提供之用戶指南，檢視其影像錄影機是否存在一鍵還原之功能。

4.1.4. 安全啟動測試

測試環境請參照圖 2。

4.1.4.1. 安全啟動測試

A. 測試產品是否支援安全啟動(secure boot)功能。

- 測試依據：

  「影像監控系統資安標準草案-網路攝影機」4.1.4.1A. 確保產品於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，一旦系統的完整性及可信度獲得保證，產品始得開機。

- 測試標準：

  安全啟動必須正常運行，則本測試項目結果為通過。

- 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。

4.2. 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。

4.2.1. 作業系統安全測試

測試環境請參照圖 2。

4.2.1.1. 作業系統常見弱點與漏洞的檢測-初階

A. 檢測作業系統是否存在 CVSS v3 評分為 10 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1A.受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 10 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

作業系統不得存在 CVSS 評分為最高風險 10 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.1.2. 作業系統常見弱點與漏洞的檢測-進階

A. 檢測作業系統是否存在 CVSS v3 評分為 9 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.2A.受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

作業系統不得存在 CVSS 評分為最高風險 9 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.1.3. 作業系統常見弱點與漏洞的檢測-高階

A. 檢測作業系統是否存在 CVSS v3 評分為 7 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.3A.受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

作業系統不得存在 CVSS 評分為最高風險 7 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.2. 網路服務連接埠的管控測試

測試環境請參照圖 2。

4.2.2.1. 網路服務的最小化檢測

A. 檢測所啟用之網路服務與廠商宣告之一致性。

- 測試依據：

  「影像監控系統資安標準草案-網路攝影機」4.2.2.1A.開啟之網路服務僅須為廠商提供必要服務之所需，透過最小化網路服務之啟用，即可降低產品的可入侵介面，廠商須於文件中標明所啟用之服務，以確保是否存在未宣告之網路服務連接埠被開啟。

- 測試標準：

  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，則本測試項目結果為通過。

- 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。

4.2.3. 網路服務安全測試

測試環境請參照圖 2。

4.2.3.1. 網路服務常見弱點與漏洞的檢測-初階

A. 檢測網路服務是否存在 CVSS v3 評分為 10 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1A.受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 10 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

網路服務不得存在 CVSS 評分為最高風險 10 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.3.2. 網路服務已知常見弱點與漏洞的檢測-進階

A. 檢測網路服務是否存在 CVSS v3 評分為 9 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.2A.受測產品之網路服務，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

網路服務不得存在 CVSS 評分為最高風險 9 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.3.3. 網路服務已知常見弱點與漏洞的檢測-高階

A. 檢測網路服務是否存在 CVSS v3 評分為 7 分之常見資安弱點與漏洞。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.3.3A.受測產品之網路服務，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

- 測試標準：

網路服務不得存在 CVSS 評分為最高風險 7 分之資安漏洞，則本測試項目結果為通過。

- 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。

4.2.4. 更新安全測試

測試環境請參照圖 2。

4.2.4.1. 韌體更新機密性測試

A. 韌體程式更新功能測試。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.4.1A.韌體須具備更新機制。

- 測試標準：

更新機制必須正常運行，則本測試項目結果為通過。

- 測試方法：

受測廠商須配合提供測試之韌體更新服務，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。

B. 韌體程式更新測試 - 更新檔案的保護。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.4.1B.產品支援離線手動更新，則更新檔案得確保機密性，且使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[3]。

- 測試標準：

測項 4.2.4.1A 之測試結果必須為通過。

韌體手動更新機制，其更新檔案必須加密保護，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。若無提供手動更新機制，則本測試結果為通過。

- 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。

C. 韌體程式更新測試 - 更新路徑的保護。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.4.1C.產品支援線上更新，則更新路徑得通過安全通道，且安全通道必須是 TLS 1.1 以上，以及使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[3]。

- 測試標準：

測項 4.2.4.1A 之測試結果必須為通過。

韌體線上更新機制，其更新路徑必須透過安全通道保護，同時安全通道版本須符合「附錄 B」的要求，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。若無提供線上更新機制，本測試結果為通過。

- 測試方法：

受測廠商須配合提供測試之韌體更新服務，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。

4.2.4.2. 韌體更新機制強度測試

A. 線上韌體更新保證測試。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.4.2A.除達到 4.2.4.1 要求外，韌體更新機制須一律採用線上更新。

- 測試標準：

測項 4.2.4.1A 檢測結果必須是通過。

更新機制僅可透過線上更新的方式,若提供使用者手動更新機制,則本測試結果為失敗。

- 測試方法：

受測廠商須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。

B. 韌體更新之完整性及可信度測試。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.4.2B.除達到 4.2.4.1 要求外，韌體更新必須透過數位簽章機制確保更新檔案的完整性及可信度。

- 測試標準：

測項 4.2.4.1A 檢測結果必須是通過。

經過竄改之更新檔案不得被成功更新，則本測試項目結果為通過。

- 測試方法：

擷取更新檔案，將該檔案透過 16 進制檢視是否含有簽章資訊，並竄改該檔案，提供竄

改過後的更新檔案供受測產品執行更新任務。

4.2.5. 韌體程式安全測試

測試環境請參照圖 2。

4.2.5.1. 敏感資料外洩測試

A. 韌體程式碼之敏感資料外洩。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.5.1A. 產品之帳號、密碼、身分認證因子或加解密用之金鑰，不得出現於韌體之程式碼與安裝檔內其他檔案中。

- 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，本測試結果為通過。

- 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。

4.2.5.2. 韌體程式安全性測試

A. 韌體程式碼之原始碼掃描。

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.5.2A.產品的韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11]。

- 測試標準：

韌體之原始碼掃描報告不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors，則本測試項目結果為通過。

- 測試方法：

受測廠商出示原始碼掃描報告供檢驗。

4.2.6. 敏感資料儲存安全測試

測試環境請參照圖 2。

4.2.6.1.敏感資料的儲存保護測試-初階

A. 敏感性資料加密儲存測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.6.1A.產品之敏感性資料須透過加密儲存，必須採用 FIPS 140-2 所核可之加密演算法[3]確保機密性。

- 測試標準：

系統檔案內之使用者帳號、密碼、憑證及金鑰必須經過加密儲存，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]，以確保演算法之強度。產品若不具備系統層管理介面，則本測試項目結果為通過。

- 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、密碼、憑證及金鑰經過加密儲存，並檢視其加密演算法是否採用 FIPS 140-2 所核可之演算法[3]。

4.2.6.2.機敏資料的儲存保護測試-高階

A. 敏感性資料隔離保護測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.6.2A.敏感資料必須存放於產品的安全區域(Secure domain)中。

- 測試標準：

產品須具備安全區域，且敏感資料須存放於此，則本測試項目結果為通過。

- 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。

4.2.7. 網頁管理介面安全測試

測試環境請參照圖 2。

4.2.7.1.網頁管理介面常見資安風險檢測

A. 網頁管理介面弱點檢測

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.7.1A.確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊。

- 測試標準：

網頁管理介面操控程式，不得存在引發 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。若產品不具有網頁管理介面，則本測試項目結果為通過。

- 測試方法：

開啟網路攝影機之網頁管理介面，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。

4.2.8. API 安全測試

測試環境請參照圖 2。

4.2.8.1.API 之認證功能測試

A. API 呼叫的身分認證機制

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.8.1A. API 之身分認證機制，不得因為重送攻擊(Replay Attack)而使得認證被通過。

- 測試標準：

產品之 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，則本測試項目結果為通過。或網路攝影機未提供 API，本測試項目結果亦為通過。

- 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。

B. API 呼叫之身分認證錯誤訊息

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.8.1B. 認證錯誤訊息不能顯露出合法使用者名稱。

- 測試標準：

從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過。

- 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，藉由輸入錯誤的帳號、密碼，檢視錯誤訊息。

C. 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」4.2.8.1C. 參照 FIPS SP 800-63-3[8] 密碼強

度原則，密碼認證機制之密碼長度必須支援 15 個字母長度。

- 測試標準：

網路攝影機之 API 密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過。

- 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，輸入達 15 個字母長度之密碼，檢視密碼設定是否成功。

D. 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」4.2.8.1D.廠商所生產之網路攝影機其預設密碼都須相異。

- 測試標準：

網路攝影機之 API 呼叫之預設密碼都須相異。網路攝影機若未提供 API，則本測試項目結果為通過。

- 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。

E. 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」4.2.8.1E. 首次成功取得網路攝影機 API 之認證，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。

F. 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」4.2.8.1F. 產品在認證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，其認證密碼的嘗試有輸入頻率及次數的限制，須與「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 認證密碼輸入頻率與次數限制測試。

G. 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」4.2.8.1G. API 的存取，必須具備權限管控機制，即須將使用者角色切割成數個不同權限之使用者環境，例如：一般使用者、特權使用者、系統管理者等，並於文件中標明現存角色與其對應的權限，以確保產品之角色權限與廠商所宣告相符。

- 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須與「廠商自我宣告表」所宣告之「裝置 API 帳號權限說明」相符，並且至少要有一般使用者與系統管理者二個不同權限之角色。網路攝影機若未提供 API，則本測試項目結果為通過。

- 測試方法：

受測廠商須於文件中標明現存角色與其對應的權限，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。

H. 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」4.2.8.1H.產品之授權行為，應存在閒置時限。

- 測試標準：

API 呼叫之閒置時限，須與「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，本測試項目結果為通過。若網路攝影機之每次 API 呼叫皆須重新認

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。

4.2.8.2.API 異常輸入測試

A. API 異常輸入測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.8.1A.透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免 API 因為任意或非法的輸入，造成產品異常行為的發生。

- 測試標準：

測項 4.2.8.1 之測試結果必須為通過。

產品所提供之 API 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，則本測試項目結果為通過。

- 測試方法：

由測試 PC 連線至網路攝影機，執行對產品每一 API 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。

4.2.9. 系統日誌檔與警示測試

測試環境請參照圖 2。

4.2.9.1.安全事件日誌檔測試

A. 安全事件日誌檔測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.9.1A.須具備安全事件日誌檔之顯示功能，以記錄用戶的存取行為，用以察覺未授權或異常的登入操作，產品須提供完整時間戳記、使用者身分及操作行為之安全事件日誌檔供查閱。

- 測試標準：

安全事件日誌的資料應包含時間、使用者身分及操作行為。產品若不具有可檢視之安全事件日誌功能，則本測試項目結果為失敗。

- 測試方法：

測試人員根據產品之使用說明，開啟安全事件日誌，檢視內容是否記載所有使用者的存取紀錄。

B. 存取權限管控測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.9.1B.產品之安全事件日誌檔須具備權限控管機制，該紀錄檔不得允許未經授權的修改，以防止被竄改的可能。

- 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須與「廠商自我宣告表」所宣告之「日誌檔權限說明」相符，則本測試項目結果為通過。

- 測試方法：

測試人員根據產品之使用說明，存取安全事件日誌，檢視身分類型與權限是否與廠商自我宣告相符。

4.2.9.2.異常警示功能測試

A. 登入警示功能測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.9.2A.除達到 4.2.9.1 要求外，產品須提供登入警示功能。

- 測試標準：

測項 4.2.9.1A 檢測結果必須是通過。

登入警示通知機制應與產品說明一致。產品若不具有登入警示功能，則本測試項目結果為失敗。

- 測試方法：

測試人員根據產品之使用說明，成功與網路攝影機建立連接，並檢視是否依照產品使用說明接收到登入警示。

B. 日誌檔可用性測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.2.9.2B.除達到 4.2.9.1 要求外，網路攝影機應提供當日誌紀錄檔無法儲存時之系統警示。

- 測試標準：

測項 4.2.9.1A 檢測結果必須是通過。

警示通知機制應與產品說明一致。產品若不具有日誌紀錄檔無法儲存之異常警示功能，則本測試項目結果為失敗。

- 測試方法：

測試人員根據產品之使用說明，成功與網路攝影機建立連接，製造安全事件紀錄檔無法儲存之情境，包括：更改存取權限與填滿儲存空間，並檢視是否依照產品使用說明接收到登入警示。

4.3. 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。

4.3.1. 資料傳輸安全測試

測試環境請參照圖 2。

4.3.1.1.敏感資料之傳輸保護測試-初階

A. 敏感資料之傳輸保護測試-初階

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.1.1A.敏感資料之網路傳輸必須採用 FIPS 140-2 所核可之加密演算法[3]，以確保機密性。

- 測試標準：

敏感資料之網路傳輸必須經過加密保護，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。

- 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，進行敏感資料之傳輸測試，同時側錄封包，確認封包經過加密保護，並檢視其加密演算法是否採用 FIPS 140-2 所核可之演算法[3]。

4.3.1.2. 敏感資料之傳輸保護測試-高階

A. 敏感資料之傳輸保護測試-高階

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.1.2A.確保敏感資料之網路傳輸加密演算法必須支援 AES-256。

- 測試標準：

與支援 AES-256 之伺服器連線並成功將資料正確還原，則本測試項目結果為通過。

- 測試方法：

於網路攝影機中啟動測試程式，透過測試程式與支援 AES-256 之伺服器連線，檢查測試程式回報結果。

4.3.2. 網路介面通訊協定的安全設置測試

測試環境請參照圖 2。

4.3.2.1. 通訊介面組態設置測試

A. 網路裝置資訊探詢功能測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.2.1A. 產品須提供用戶可自行開/關「網路裝置資訊探詢」功能，例如：UPnP、SNMP 及 Bonjour。

- 測試標準：

UPnP、SNMP 或 Bonjour 功能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。

B. 安全的 WiFi 組態設置測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.2.1B. 網路攝影機上不得存在不安全的無線網路設定。

- 測試標準：

產品只要具備 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。

C. 無線網路傳輸安全機制設置測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.2.1C. 無線網路傳輸的安全機制預設必

須採用 WPA2。

- 測試標準：

無線網路預設加密模式必須使用 WPA2。

- 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安全機制。

4.3.3. 通訊協定安全測試

測試環境請參照圖 2。

4.3.3.1. 通訊協定異常輸入檢測

A. 通訊協定異常輸入檢測

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.3.3.1.透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免關鍵之通訊協定(見附錄 C)因為任意或非法的輸入，造成產品異常行為的發生。

- 測試標準：

通訊協定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。

4.4. 遠端管理介面與操控程式之身分認證與授權安全測試

檢視網路攝影機之身分認證與授權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。

4.4.1. 認證機制安全測試

測試環境請參照圖 2。

4.4.1.1. 認證機制強度測試-初階

A. 認證機制強度測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.1.1A.產品之身分認證機制，不得因為重送攻擊而使得認證被通過。

- 測試標準：

透過遠端管理介面與操控程式存取網路攝影機時，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。

- 測試方法：

由測試 PC 透過遠端連線登入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。

B. 身分認證錯誤訊息

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.1.1B.認證錯誤訊息不能顯露出合法使用者名稱。

- 測試標準：

從錯誤訊息無法推斷出合法使用者名稱，本測試項目結果為通過。

- 測試方法：

由測試 PC 透過遠端連線至網路攝影機進行測試，藉由輸入錯誤的帳號、密碼，檢視錯誤訊息。

4.4.1.2. 認證機制強度測試-高階

A. 認證機制強度測試

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.1.2A.除達到 4.4.1.1 要求外，產品之身分認證機制須採用公開金鑰基礎建設。

- 測試標準：

測項 4.4.1.1A 檢測結果必須是通過。

認證機制須透過公開金鑰基礎建設才可以認證，若可採用其它認證方式登入至網路攝影機，則此測試項目結果為失敗。

- 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。

4.4.2. 密碼認證安全測試

測試環境請參照圖 2。

4.4.2.1. 密碼認證機制

A. 密碼強度

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.2.1A. 參照 FIPS SP 800-63-3[8] 密碼強度原則，密碼認證機制之密碼長度必須支援 15 個字母長度。

- 測試標準：

透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其密碼長度可達 15 個字母長度，則本測試項目結果為通過。

- 測試方法：

由測試 PC 透過遠端連線至網路攝影機進行授權密碼輸入，輸入達 15 個字母長度之密碼，檢視密碼設定是否成功。

B. 預設密碼唯一性

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.2.1B.廠商所生產之網路攝影機其預設密碼都須相異。

- 測試標準：

廠商所出產之網路攝影機其遠端管理介面與操控程式之預設密碼都須相異。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 透過遠端連線登入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。

C. 密碼變更機制

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.2.1C.首次登入產品必須強制更改預設密碼。

- 測試標準：

透過遠端管理介面與操控程式登入網路攝影機之密碼認證，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 透過遠端連線登入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。

D. 密碼的輸入頻率及次數限制

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.2.1D.產品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：

透過遠端管理介面與操控程式登入網路攝影機之密碼認證，其授權密碼的嘗試有輸入頻率及次數的限制，須與「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 透過遠端連線登入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。

4.4.3. 權限管控安全測試

測試環境請參照圖 2。

4.4.3.1. 權限管控機制

A. 權限管控機制

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.3.1A. 產品須將使用者角色切割成數個使用者環境，例如：一般使用者、特權使用者、系統管理者等，並於文件中標明現存角色與其對應的權限，以確保產品之角色權限與廠商所宣告相符。

- 測試標準：

網路攝影機之遠端管理介面與操控程式，必須具備權限管控機制，該使用者的身分授權須與「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，並且至少要有一般使用者與系統管理者二個不同權限之角色。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。

B. 存取控制清單

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.3.1B. 對所有合法授權之帳戶強制實施最小權限(least privilege)原則，即系統管理者有其專門的特權，其它角色不能擁有這樣的權限。

- 測試標準：

產品之其它角色不能擁有系統管理者特權，則本測試項目結果為通過。

- 測試方法：

由測試 PC 透過遠端連線至網路攝影機進行測試，登入後確認非系統管理者之權限。

C. 權限有效時間

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.4.3.1C. 產品之授權行為，應存在閒置時限，一旦遠端連線已經遺失或結束，須要求新的認證。

- 測試標準：

遠端管理介面之閒置時限，須與「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。

4.5. 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所收集到的影音或使用者資訊。

4.5.1. 隱私資料的使用保護測試

4.5.1.1. 隱私資料權限管控測試

測試環境請參照圖 2。

A. 網路攝影機之隱私資料的存取控制

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.5.1.1A.產品所儲存的隱私資料，只有已被授權的個體才可以存取。

- 測試標準：

產品所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與「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。

B. 隱私資料刪除功能

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.5.1.1B. 具備使用者刪除其隱私資料之功能，及對所儲存隱私資料的刪除權限。

- 測試標準：

必須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。

4.5.2. 隱私資料的傳輸保護測試

測試環境請參照圖 2。

4.5.2.1. 隱私資料的傳輸保護-初階

A. 隱私資料的傳輸機密性

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.5.2.1A. 影像類隱私資料之傳輸不得為明文，非影像類隱私資料之傳輸，須採用 FIPS 140-2 所核可之加密演算法[3]。

- 測試標準：

影像類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 A」所列之公認弱加密演算法。非影像類隱私資料之傳輸加密演算法須採用 FIPS 140-2 所核可之加密演算法[3]。

- 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。

4.5.2.2.隱私資料的傳輸保護-進階

A. 隱私資料的傳輸機密性

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.5.2.2A. 隱私資料之傳輸須採用 FIPS 140-2 所核可之加密演算法[3]。

- 測試標準：

隱私資料之傳輸加密演算法須採用 FIPS 140-2 所核可之加密演算法[3]。

- 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。

4.5.2.3.隱私資料的傳輸保護-高階

A. 隱私資料的傳輸機密性

- 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.5.2.3A. 確保隱私資料之網路傳輸加密演算法預設必須採用 AES-256。

- 測試標準：

與支援 AES-256 之伺服器連線並成功將資料正確還原，則本測試項目結果為通過。

- 測試方法：

於網路攝影機中啟動測試程式，透過測試程式與支援 AES-256 之伺服器連線，檢查測試程式回報結果。

附錄 A
(規定)
公認之弱加密演算法

- BASE 64 Encode and Decode

  Base64 是一種能將任意 Binary 資料用 64 種字元組合成字串的方法，而這個 Binary 資料和字串資料彼此之間是可以互相轉換的，此機制的目的是在保證效率的情況下，不讓處理過的資料被輕易識別，因此演算法的複雜度相對也就不能太高。

- Data Encryption Standard, DES

  是一種基於使用 56 位元金鑰之對稱式加密演算法，此加密演算法在 1999 年已被公開破解，也有一些分析報告提出了演算法理論上的漏洞。

- Message-Digest Algorithm, MD5

  是一種雜湊函式(hash function)，可以產生出一個 128 位元的雜湊值(hash value)，用於確保傳輸中資料的完整性，此方法在 1996 年已被證實存在漏洞，可以被破解。

- Rivest Cipher 4, RC4

  是一種密鑰長度可變的對稱加密演算法，同時也是無線加密協定(WEP)所採用的加密演算法，在 2015 年被公告已破解，並禁止在所有版本的 TLS 中使用。

- Secure Hash Algorithm 1, SHA-1

  是一種雜湊函式(hash function)，可以產生出一個 160 位元的雜湊值(hash value)，用於確保傳輸中資料的完整性，2005 年 SHA-1 被發現含有理論上漏洞，會造成碰撞攻擊(collision attack)。

附錄 B
(規定)
安全通道版本使用要求

HTTPS 是超文本傳輸協定(HTTP)結合 SSL/TLS 安全通道的傳輸中資料保護技術，然而 SSL 在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布將全面禁用，到此已經完全由 TLS 替代 SSL，然而 TLS 1.0 存在可以降級到 SSL 3.0 的功能，使得 TLS 1.0 同樣不被信任，因此目前本規範建議使用的版本如下：

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

附錄 C
(規定)
網路攝影機之通訊協定

- 即時傳輸協定 (Real-time Transport Protocol, RTP)：

定義在 RFC 3550 規範中，常應用於影音串流(Video Streaming)系統、視訊會議及一鍵通(Push to Talk)系統，其定義了在網際網路上傳遞音訊和影片的標準封包格式。

- 即時傳送控制協定 (Real-time Transport Control Protocol, RTCP)：

定義在 RFC 3550 規範中，RTCP 並不用於資料傳輸，而是支援 RTP 將多媒體資料封裝並發送，RTCP 會週期性地在一個 RTP 會議連線上以帶外(out-of-band)的方式提供統計及傳輸控制資訊，此協定之主要功能是為 RTP 提供服務品質(Quality of Service)的反饋(feedback)。

- 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中，用來控制具有即時性需求的資料，如影音多媒體資料的播放、錄製及暫停，可達到用戶端到媒體伺服器之間的即時影音控制。

- 超文本傳輸協定(HyperText Transfer Protocol, HTTP)：

定義在 RFC 7540 規範中，超文本傳輸協定之全名為 HypertText Transfer Protocol（簡稱為 HTTP），是目前網際網路上應用最廣泛的一個網路協議（protocol），其主要目的是為了提供網頁的發佈與取得。

- HTTPS 加密協定(HyperText Transfer Protocol Secure, HTTPS)：

定義在 RFC 2818 規範中，是一種經由 HTTP 進行通訊傳輸，且傳輸是建立在 SSL/TLS 安全通道之上，以保護傳輸中之資料。HTTPS 的主要應用是對網站伺服器進行身分認證，確保傳輸中資料的隱密性與完整性。

附錄 D
(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	網路服務已知漏洞偵測	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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]
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不得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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]
SYS-9	網頁管理介面常見資安風險檢驗	M	3.1.4.1.網頁管理介面不得存在 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，且加密演算法須採用 FIPS 140-

			2 所核可之演算法[3]
COMM-2	網路攝影機之網路裝置資訊探詢功能	M	3.2.2.1.網路攝影機須提供使用者，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.網路攝影機上不得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

- 身分認證與授權機制安全技術要求

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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]
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須相異
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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]
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 E
(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>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 F
(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	名稱及型號	製造廠商	作業系統版本	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： _____	日誌檔權限說明	□ 否 □ 是		

附錄 G
(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，同時安全通道版本須符合「附錄 B」的要求，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					
	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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					
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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]，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，不得存在引發 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	部	尚	不	

		全實施	份實施	未實施	適用	
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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]					
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模式，須採用 FIPS 140-2 所核可之加密演算法[3]					
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. 身分認證與授權機制		**自我評估** 完全實施	部份實施	尚未實施	不適用	**註記**
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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					
	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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					

	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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					
網路攝影機密碼認證安全	7. 網路攝影機之 API 呼叫，其密碼長度必須符合政府組態基準[6]的最小密碼長度原則 CCE-33789-9。					
	8. 網路攝影機之 API 呼叫之預設密碼都須相異。					
	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，須與「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，其密碼長度必須符合政府組態基準[6]的最小密碼長度原則 CCE-33789-9。					
	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須相異。					
	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，須與「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，其密碼長度必須符合政府組態基準[6]的最小密碼長度原則 CCE-33789-9。					
	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，須與「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	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須與「廠商自我宣告表」					

面之權限管控	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須與「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須與「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，須與「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，須與「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，須與「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須與「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，且加密演算法須採用 FIPS 140-2 所核可之演算法[3]。					
	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 A」所列之公認弱加密演算法。					

附錄 H
(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. First.org, Inc., Common Vulnerability Scoring System, V3 Development Update, https://www.first.org/cvss
2. MITRE corp., Common Vulnerabilities and Exposures, https://cve.mitre.org/cve/cve.html
3. National Institute of Standards and Technology, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017.
4. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
5. 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