影像監控系統資安標準之測試規範

草案-網路攝影機

(V0.9.0)

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

2017-09-25

目錄

前言

本規範係依台灣資通產業標準協會（TAICS）之規定，經技術管理委員會(理事會）審定，由協會公布之產業標準。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

網路攝影機，係藉由鏡頭採集圖像後，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，或透過內建處理器及網頁伺服器，以透過有線或無線網路連線檢視畫面。

鑑於近幾年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，協助台灣產業接軌國際，提升研發技術及保證受測物質量。

「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)，依據台灣資通產業標準協會(TAICS)所制定之「影像監控系統網路攝影機資安標準草案」[1] 所訂定，俾利網路攝影機製造商、系統整合商及物聯網資安檢測實驗室等作為相關受測物檢測技術的參考藍本。本測試規範中具體明列網路攝影機資安檢測之測試項目、測試條件、測試方法及測試標準等事項。

1. 適用範圍

泛指應用於影像監控系統的嵌入式攝影機，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，訂定其受測物之安全技術要求，擬依五個安全構面定義之，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。

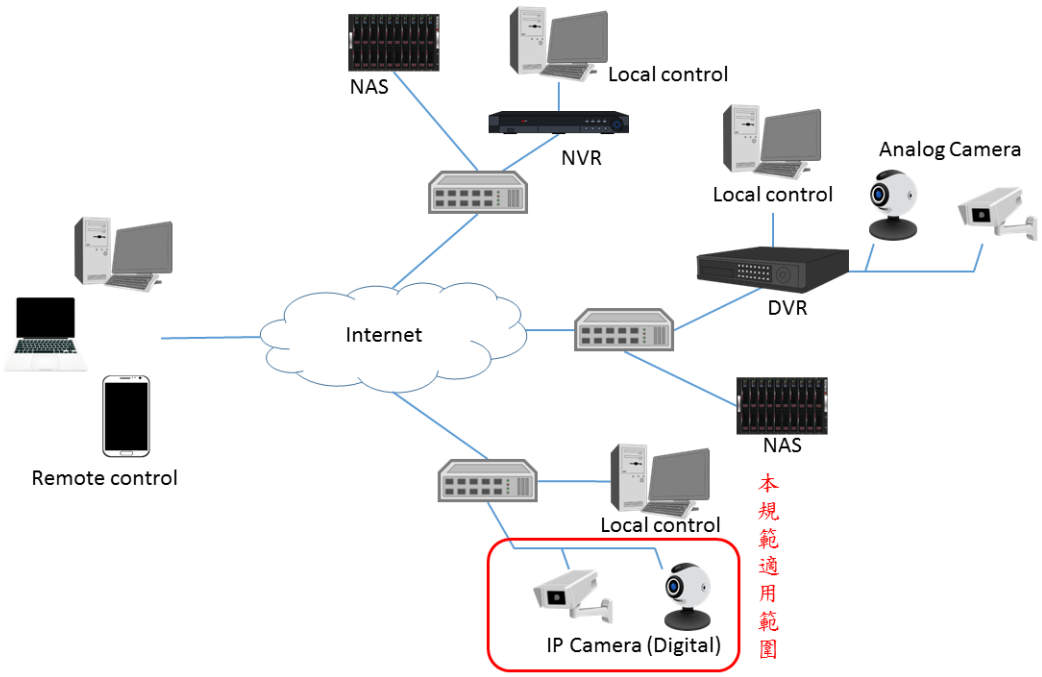

圖1. 適用範圍示意圖

2. 引用標準

下列標準因本標準所引用，成為本標準之一部份。下列引用標準適用最新版(包括補充增修)。

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

3. 用語及定義

下列用語與定義適用於本標準。

3.1 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。

3.2 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、完整性及可用性面臨威脅。

3.3 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。

3.4 國家弱點資料庫 (National Vulnerabilities Database)

係指美國國家標準技術研究所（NIST）提供的國家弱點資料庫[2]，負責 2.3 常見弱點與漏洞之資料的發布及更新。

3.5 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。評分分數從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險。

3.6 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，而該資訊之洩漏可能對使用者造成損害之虞，包括但不限於個人資料、

密碼或地理位置等。

3.7 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。

3.8 隱私 (Privacy)

係指私人資訊，此一資訊的全部或部份不可被公開，且資訊所有人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。

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

係指透過網路自遠端裝置上取得網路攝影機作業系統層的操控權，作業模式如下列：

(a) 工程師遠端維護受測物使用或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

(b) 進行系統設定，例如：設定網際協定位址(IP)。

3.10 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。

3.11 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。

3.12 第三方函式庫 (3rd Party Library)

係指系統程式設計者為加速開發，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。

3.13 加密 (Encryption)

係指法明文資訊透過數學演算法進行改變，使原來的資料不可讀而達到保密的目的。

3.14 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。

3.15 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)。

3.16 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。

3.17 政府組態基準 (Government Configuration Baseline, GCB)

規範資通訊終端設備(如：個人電腦) 的一致性安全設定[3](如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

3.18 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。

3.19 預設密碼 (Default Password)

係指受測物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。

3.20 裝置認證 (Device Authentication)

係指受測物為驗證相連裝置之身分，以確保傳輸對象身分是否可信賴，常用之認證方式可能是要求相連裝置提交使用者名稱及密碼，或者是相連裝置之數位憑證來確認裝置之身分。

4. 測試項目分級

本節依據影像監控系統網路攝影機資安標準草案所制定之標準規範，設計其相對應之安全測試項目及各安全等級之測試標準。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，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；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。而本實機測試標準等級總表中之各欄的關連性，須依循第 4 節之規定內容。

安全等級依(1)測試所需時間、(2)安全技術深度、(3)目前尚無通用測試方法、(4)受測物技術現況等驗證項目，共為三個等級，分為 1 級、2 級、3 級，與其對應之列代表的安全要求分項，識別一個特定的技術要求，且按等級順序排列，數字越大表示安全等級越高，且測試標準認定方式為：受測物須先通過較低安全等級之測試，始可進行較高等級之測試。

表 1　實機測試標準等級總表

安全測試構面	安全測試項目	安全等級測試標準		
		1 級	2 級	3 級
實體安全測試	5.1.1. 實體埠之安全管控測試	5.1.1.1	5.1.1.2	
	5.1.2. 實體異常行為警示測試		5.1.2.1	
	5.1.3. 實體防護測試		5.1.3.1	5.1.3.2
	5.1.4. 安全啟動測試			5.1.4.1

系統安全測試	5.2.1.作業系統安全測試	5.2.1.1	5.2.1.2	5.2.1.3
	5.2.2.網路服務連接埠的管控測試	5.2.2.1		
	5.2.3.更新安全測試	5.2.3.1	5.2.3.2	
	5.2.4.韌體程式安全測試(選測)	5.2.4.1	5.2.4.2	
	5.2.5.敏感資料儲存安全測試		5.2.5.1	5.2.5.2
	5.2.6.網頁管理介面安全測試	5.2.6.1		5.2.6.2
	5.2.7.API 安全測試	5.2.7.1		5.2.7.2
	5.2.8.系統日誌檔與警示測試	5.2.8.1	5.2.8.2	
通訊安全測試	5.3.1.資料傳輸安全測試	5.3.1.1		5.3.1.2
	5.3.2.網路介面通訊協定的安全設置測試	5.3.2.1		
	5.3.3.通訊協定安全測試		5.3.3.1	
身分認證與授權機制安全測試	5.4.1.認證機制安全測試	5.4.1.1		5.4.1.2
	5.4.2.密碼認證安全測試	5.4.2.1		
	5.4.3.權限管控安全測試	5.4.3.1		

隱私保護測試	5.5.1. 隱私資料的使用保護測試	5.5.1.1		
	5.5.2. 隱私資料的傳輸保護測試	5.5.2.1	5.5.2.2	5.5.2.3

4.1 安全等級第 1 級測試標準

表 3　第 1 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	5.1.1.1(a) - 包括 USB、RJ45 及序列埠之實體埠可被關閉，使用者不得透過實體連結方式存取作業系統。
作業系統安全測試	
作業系統安全測試	5.2.1.1(a) - 作業系統與網路服務不得存在 CVSS 評分為最高風險 9 分以上之資安漏洞。
網路服務連接埠的管控測試	5.2.2.1(a) - 所開啟之網路服務連接埠必須與受測物自我宣告之內容相符。
更新安全測試	5.2.3.1(a) - 更新機制必須正常運行。 5.2.3.1(b) - 韌體更新檔案必須加密保護。 - 加密演算法不得為「附錄 A」所列之公認弱加密演算法。 5.2.3.1(c) - 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，且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 所核可之演算法[4]。
韌體程式安全測試（選測）	5.2.4.1(a) - 網路攝影機之程式碼與安裝檔內其他檔案，不得被檢出身分認證因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)及個人資料。

	- 韌體檔案若被加密，導致無法被拆解，因機敏資料不會被洩露，本測試項目結果為通過。
網頁管理介面安全測試	5.2.6.1(a) - 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。 - 若受測物不具有網頁管理介面，則本測試項目結果為通過。 - 採自動化測試手法。
API 安全測試	5.2.7.1(a) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果與測項 5.4.1.1(a)測試結果一致。 - 同 5.4.1.1(a)之測試標準。 5.2.7.1(b) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果與測項 5.4.1.1(b)測試結果一致。 - 同 5.4.1.1(b)之測試標準。 5.2.7.1(c) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果與測項 5.4.2.1(a)測試結果一致。 - 同 5.4.2.1(a)之測試標準。 5.2.7.1(d) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果與測項 5.4.2.1(b)測試結果一致。 - 同 5.4.2.1(b)之測試標準。 5.2.7.1(e) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果

	與測項 5.4.2.1(c)測試結果一致。 - 同 5.4.2.1(c)之測試標準。 5.2.7.1(f) - 受測物中的所有密碼認證機制皆使用同一組密碼,則本測項測試結果與測項 5.4.2.1(d)測試結果一致。 - 同 5.4.2.1(d)之測試標準。 5.2.7.1(g) - 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受測物自我宣告相符,並且至少要有二個以上不同權限的角色。 5.2.7.1(h) - 受測物必須提供 API 呼叫權限之閒置時限功能,最常不得超過 10 分鐘。 - 受測物之每次 API 呼叫皆須重新認證授權,則本測試結果為通過。
系統日誌檔與警示測試	5.2.8.1(a) - 安全事件日誌的資料應包含時間、使用者身分及操作行為。 - 受測物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。 5.2.8.1(b) - 產品須對安全事件日誌檔進行權限控管,該安全事件日誌檔的身分授權須與受測物自我宣告相符。 5.2.8.1(c) - 產品之日誌檔須具備保存期限的設計。 - 須符合 NIST SP 800-92[5]中 high impact systems 的日誌資料維護長度。
通訊安全測試	
資料傳輸安	5.3.1.1(a)

全測試	– 敏感資料之傳輸通道必須經過加密保護，且加密演算法須採用 FIPS 140-2 所核可之演算法[4]。
網路介面通訊協定的安全設置測試	5.3.2.1(a) – UPnP、SNMP 或 Bonjour 功能必須提供使用者可自行開/關功能之設置。 – 預設必須為關閉。 5.3.2.1(b) – 受測物只要具備 WPS 功能，則必須提供使用者，WPS PIN 及 WPS Lock 開/關之功能。 – 該功能預設須為關閉。 5.3.2.1(c) – 無線網路預設加密模式必須使用 WPA2。 5.3.2.1(d) – 使用者不得透過有線或無線連結的方式存取作業系統。
遠端管理介面與操控程式之身分認證與授權安全測試	
認證機制安全測試	5.4.1.1(a) – 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。 5.4.1.1(b) – 從錯誤訊息無法推斷出合法使用者名稱。
密碼認證安全測試	5.4.2.1(a) – 密碼認證之密碼長度必須符合政府組態基準 CCE-33789-9。 – 密碼認證之密碼複雜度必須符合政府組態基準 CCE-33777-4。 – 密碼認證之防止重複使用舊密碼必須符合政府組態基準 CCE-35219-5。

	5.4.2.1(b) - 預設密碼都須相異。 5.4.2.1(c) - 首次取得授權後必須強制更改預設密碼。 5.4.2.1(d) - 密碼的輸入次數必須符合最高 5 次嘗試登入失敗次數導致帳戶鎖定的限制。 - 密碼的輸入頻率必須符合帳戶鎖定計數器至少 1 分鐘以上的時間間隔，才會將失敗的登入嘗試計數器重設為 0 次失敗。 - 密碼的輸入頻率必須符合帳戶鎖定期間至少 1 分鐘以上，才會自動解除鎖定。
權限管控安全測試	5.4.3.1(a) - 透過遠端連線存取受測物，必須具備權限管控機制，該使用者的身分授權須與受測物自我宣告相符，並且至少要有二個以上不同權限的角色。 5.4.3.1(b) - 受測物必須提供遠端控制權限之閒置時限功能，且閒置時限最多不可超過 20 分鐘。
隱私保護測試	
隱私資料的使用保護測試	5.5.1.1(a) - 受測物所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與受測物自我宣告相符。 - 並且至少要有二個以上不同權限的角色。 5.5.1.1(b) - 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。

	5.5.1.1(c) - 受測物必須具備登入警示功能。
隱私資料的傳輸保護測試	5.5.2.1(a) - 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[4]。

4.2 安全等級第 2 級測試標準

表 3 第 2 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	5.1.1.2(a) - 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介面，必須移除。 5.1.1.2(b) - 外接實體埠的插拔操作須提供日誌記錄。
實體異常行為警示測試	5.1.2.1(a) - 攝影機鏡頭遭異物遮蔽、鏡頭遭調焦及鏡頭遭轉向之異常現象時，須主動發出警示通知。 5.1.2.1(b) - 受測物之實體遭受破壞時，例如：斷電、斷訊、機殼移除狀況，須提供警示機制。
實體防護測試	5.1.3.1(a) - 必須透過防盜螺絲鎖住外殼。
作業系統安全測試	
作業系統安全測試	5.2.1.2(a) 作業系統與網路服務不得存在 CVSS 評分為最高風險 8 分以上之資安漏

	洞。
更新安全測試	5.2.3.2(a) - 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。 5.2.3.2(b) - 經過竄改之更新檔案不得被成功更新。
韌體程式安全測試 （選測）	5.2.4.2(a) - 檢視受測物之原始碼掃描報告。 - 原始碼掃描報告不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors。
敏感資料儲存安全測試	5.2.5.1(a) - 系統所儲存之身分認證因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不得是明文。 - 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。 - 受測物若不具備作業系統管理介面，則本測試項目結果為通過。
系統日誌檔與警示測試	- 5.2.8.2(a)日誌紀錄檔無法正常儲存時，須發出警示。受測物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	
通訊協定安全測試	5.3.3.1(a) - 通訊協定必須經過異常輸入測試，受測之受測物於測試過程中不得發生程序崩潰(crash)到無法恢復運作。
隱私保護測試	
隱私資料的傳輸保護測試	5.5.2.2(a) - 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[4]。

4.3 安全等級第 3 級測試標準

表 4 第 3 級測試標準

測試類別	測試標準
實體安全測試	
實體防護測試	5.1.3.2(a) - 晶片與功能編號不得存在於電路板。 5.1.3.2(b) - 受測物實體上不得存在不須透過任何工具，即可輕易在受測物實體上還原回預設密碼須避免。
安全啟動測試	5.1.4.1(a) - 安全啟動必須正常運行。
作業系統安全測試	
作業系統安全測試	5.2.1.3(a) - 作業系統與網路服務不得存在 CVSS 評分為最高風險 7 分以上之資安漏洞。
敏感資料儲存安全測試	5.2.5.2(a) - 受測物須具備安全區域，且敏感性資料須存放於此。
網頁管理介面安全測試	5.2.6.2(a) - 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。 - 若受測物不具有網頁管理介面，則本測試項目結果為通過。 - 採人工測試。
API 安全測試	5.2.7.2(a) - 受測物所提供之 API 必須經過異常輸入測試，受測之受測物於測試過程中不得發生程序崩潰(crash)到無法恢復運作。
通訊安全測試	

資料傳輸安全測試	5.3.1.2(a) - 敏感資料之傳輸通道必須經過加密保護，且加密演算預設必須採用 AES-256 之連線。
遠端管理介面與操控程式之身分認證與授權安全測試	
認證機制安全測試	5.4.1.2(a) - 測項 4.4.1.1 系列測試結果必須是通過。 - 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。
權限管控安全測試	5.4.3.1(a) - 透過遠端連線存取受測物，必須具備權限管控機制，該使用者的身分授權須與受測物自我宣告相符，並且至少要有二個以上不同權限的角色。 5.4.3.1(b) - 受測物必須提供遠端控制權限之閒置時限功能，且閒置時限最多不可超過 20 分鐘。
隱私保護測試	
隱私資料的傳輸保護測試	5.5.2.3(a) - 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。

5. 資安測試規範

5.1 實體安全測試

5.1.1 實體埠之安全管控測試

作業系統安全測試架構，如圖 2 所示，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。

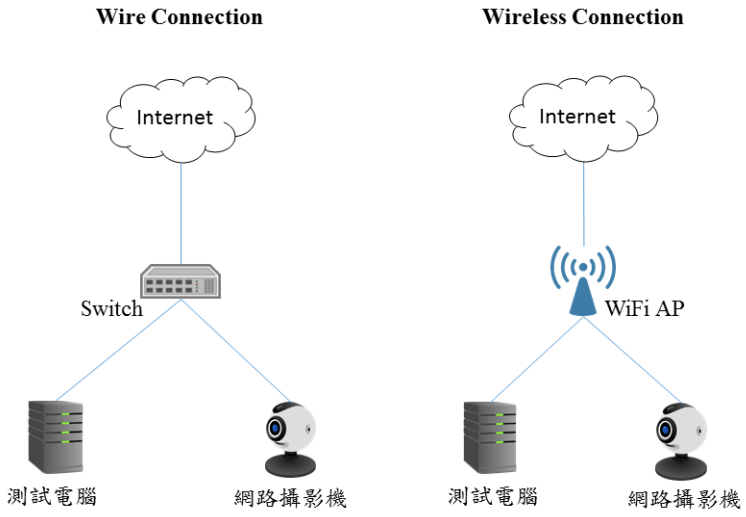

圖2 系統安全測試接續示意圖

5.1.1.1 實體埠安全管控測試

(a) 實體埠存取管控測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.1.1(a)。

(2) 測試標準：

- 包括 USB、RJ45 及序列埠之實體埠可被關閉，使用者不得透過實體連結方式存取作業系統。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 測試人員連接受測受測物之 USB 埠。
- 開啟管理介面連接工具。
- 檢視可否透過 USB 埠存取作業系統。
- 測試人員連接受測受測物之 RJ45 埠。
- 開啟管理介面連接工具。
- 檢視可否透過 RJ45 埠存取作業系統。
- 測試人員連接受測受測物之序列埠。
- 開啟管理介面連接工具。
- 檢視可否透過序列埠存取作業系統。

(4) 測試結果：

- 本測項為「通過」，無法透過 USB、 RJ45 及序列埠存取作業系統。
- 本測項為「不通過」，可以透過 USB、 RJ45 及序列埠之任一種實體埠存取作業系統。

5.1.1.2 最小實體介面測試

(a) 最小實體介面測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.1.2(a)。

(2) 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介面，必須移除。

(3) 測試步驟：

- 檢視受測物外觀，不得存在非必要之外接式儲存媒體使用的插槽，包括 USB 與 SD card。
- 檢視受測物外觀，不得存在具有除錯或測試用途之界面，包括 TTL、UART、JTAG、SWD。
- 檢視受測物內零件外觀，不得存在具有除錯或測試用途之界面，包括排母、排針、板對板連接器、板對線連接器、抽屜式連接器。

(4) 測試結果：

- 本測項為「通過」，測試方法所列舉之實體界面皆不存在。
- 本測項為「不通過」，測試方法所列舉之任一實體界面存在。

(b) 實體行為日誌功能測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」4.1.1.1(b)。

(2) 測試標準：

- 外接實體埠的插拔操作須提供日誌記錄。

(3) 測試步驟：

- 插拔 USB 埠。
- 根據受測物說明，檢視插拔紀錄。
- 插拔 RJ45 埠。
- 根據受測物說明，檢視插拔紀錄。
- 插拔序列埠。
- 根據受測物說明，檢視插拔紀錄。

(4) 測試結果：

- 本測項為「通過」，有提供 USB、 RJ45 及序列埠插拔日誌記錄。
- 本測項為「不通過」，USB、 RJ45 及序列埠之任一種實體埠無提供實體埠插拔日誌記錄。

5.1.2 實體異常行為警示測試

測試環境請參照圖 2。

5.1.2.1 異常狀態警示機制

(a) 鏡頭失效警示機制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.2.1(a)。

(2) 測試標準：

- 攝影機鏡頭遭異物遮敝、鏡頭遭調焦及鏡頭遭轉向之異常現象時，須主動發出警示通知。

(3) 測試步驟：

- 將攝影機接上電源。
- 將攝影機鏡頭用手遮敝。
- 檢視攝影機是否依照使用說明達到警示效果。
- 調整攝影機焦距使監控影像模糊。
- 檢視攝影機是否依照使用說明達到警示效果。
- 將攝影機鏡頭轉向。
- 檢視攝影機是否依照使用說明達到警示效果。

(4) 測試結果：

- 本測項為「通過」，鏡頭被異物遮敝、鏡頭遭調焦及鏡頭遭轉向之警示功能皆可被證實。
- 本測項為「不通過」，鏡頭被異物遮敝、鏡頭遭調焦及鏡頭遭轉向之任一個異常狀態未警示。

(b) 異常狀態警示機制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.2.1(b)。

(2) 測試標準：

- 受測物之實體遭受破壞時，例如：斷電、斷訊狀況，須提供警示機制。

(3) 測試步驟：

- 將攝影機接上電源。
- 將網路線拔除或天線遮罩，使其斷訊。
- 檢視攝影機是否依照使用說明達到警示效果。
- 將攝影機電源拔除。
- 檢視攝影機是否依照使用說明達到警示效果。

(4) 測試結果：

- 本測項為「通過」，斷電、斷訊之異常警示功能皆可被證實。
- 本測項為「不通過」，斷電、斷訊之任一個異常狀態未警示。

5.1.3 實體防護測試

測試環境請參照圖 2。

5.1.3.1 實體保護測試

(a) 實體保護測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.3.1(a)。

(2) 測試標準：

- 必須透過防盜螺絲鎖住外殼。

(3) 測試步驟：

- 檢視受測物之外殼是否透過防盜螺絲鎖住。

(4) 測試結果：

- 本測項為「通過」，受測物經由防盜螺絲鎖住。
- 本測項為「不通過」，受測物之外殼經由一般螺絲鎖住。

5.1.3.2 實體設計安全測試

(a) 內部實體安全測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.3.2(a)。

(2) 測試標準：

- 晶片與功能編號不得存在於電路板。

(3) 測試步驟：

- 使用特殊工具拆開外殼。
- 檢視其電路板是否存在晶片與功能編號之文字。

(4) 測試結果：

- 本測項為「通過」，電路板不存在晶片與功能編號。
- 本測項為「不通過」，電路板存在晶片與功能編號。

(b) 密碼還原機制安全設計

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.3.2(b)。

(2) 測試標準：

- 受測物實體上不得存在未經由任何工具，即可輕易在受測物實體上還原回預設密碼須避免。

(3) 測試步驟：

- 根據受測物說明文件，檢視受測物外殼是否存在不需工具即可還原預設密碼之設計。

(4) 測試結果：

- 本測項為「通過」，須使用工具才可觸發還原預設密碼功能。
- 本測項為「不通過」，徒手即可觸發還原預設密碼功能。

5.1.4 安全啟動測試

測試環境請參照圖 2。

5.1.4.1 安全啟動測試

(a) 測試受測物是否支援安全啟動(secure boot)功能。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.1.4.1(a)。

(2) 測試標準：

- 安全啟動必須正常運行。

(3) 測試步驟：

審閱具備此功能證明之書面資料。

(4) 測試結果：

- 本測項為「通過」，安全啟動功能之驗證被認可。
- 本測項為「不通過」，無法證明具備安全啟動功能。

5.2 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。

5.2.1 作業系統安全測試

測試環境請參照圖 2。

5.2.1.1 作業系統與網路服務常見弱點與漏洞初階測試

(a) 測試作業系統是否存在 CVSS v3 評分為 9 分以上之常見資安弱點與漏洞。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.1.1(a)。

(2) 測試標準：

- 作業系統與網路服務不得存在 CVSS 評分為最高風險 9 分以上之資安漏洞。

(3) 測試步驟：

- 將受測 PC 連接網路攝影機。
- 使用弱點掃描工具。
- 檢視弱掃報告之作業系統與網路服務是否存在 CVSS v3 評分為 9 分以上之資安漏洞。

(4) 測試結果：

- 本測項為「通過」，作業系統與網路服務不存在 CVSS v3 評分為 9 分以上之漏洞。
- 本測項為「不通過」，作業系統或網路服務存在 CVSS v3 評分為 9 分以上之漏洞。

5.2.1.2 作業系統與網路服務常見弱點與漏洞中階測試

(a) 測試作業系統與網路服務是否存在 CVSS v3 評分為 8 分以上之常見資安弱點與漏洞。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.1.2(a)

(2) 測試標準：

- 作業系統與網路服務不得存在CVSS 評分為最高風險8分以上之資安漏洞。

(3) 測試步驟：

- 將受測 PC 連接網路攝影機。
- 使用弱點掃描工具。
- 檢視弱掃報告之作業系統與網路服務是否存在CVSS v3評分為8分以上之資安漏洞。

(4) 測試結果：

- 本測項為「通過」，作業系統與網路服務不存在 CVSS v3 評分為 8 分以上之漏洞。
- 本測項為「不通過」，作業系統或網路服務存在 CVSS v3 評分為 8 分以上之漏洞。

5.2.1.3 作業系統與網路服務常見弱點與漏洞高階測試

(a) 測試作業系統與網路服務是否存在 CVSS v3 評分為 7 分以上之常見資安弱點與漏洞。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.1.3(a)。

(2) 測試標準：

- 作業系統與網路服務不得存在CVSS 評分為最高風險7分以上之資安漏洞。

(3) 測試步驟：

- 將受測 PC 連接網路攝影機。
- 使用弱點掃描工具。

- 檢視弱掃報告之作業系統與網路服務是否存在CVSS v3評分為7分以上之資安漏洞。

(4) 測試結果：

- 本測項為「通過」，作業系統與網路服務不存在CVSS v3評分為7分以上之漏洞。
- 本測項為「不通過」，作業系統或網路服務存在CVSS v3評分為7分以上之漏洞。

5.2.2 網路服務連接埠的管控測試

測試環境請參照圖 2。

5.2.2.1 網路服務的最小化測試

(a) 測試所啟用之網路服務與受測物自我宣告之一致性。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.2.1(a)。

(2) 測試標準：

- 所開啟之網路服務連接埠必須與受測物自我宣告之內容相符。

(3) 測試步驟：

- 將受測 PC 連接網路攝影機。
- 使用弱點掃描工具。
- 檢視所開啟之網路埠。

(4) 測試結果：

- 本測項為「通過」，受測物所開啟之網路埠與受測物自我宣告之內容相符。
- 本測項為「不通過」，受測物所開啟之網路埠與受測物自我宣告之內容不符。

5.2.3 更新安全測試

測試環境請參照圖 2。

5.2.3.1 韌體更新機密性測試

(a) 韌體程式更新功能測試。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.3.1(a)。

(2) 測試標準：

- 更新機制必須正常運行。

(3) 測試步驟：

- 根據受測物之使用說明，檢視韌體更新操作。
- 若提供離線更新，則檢視離線更新是否具備檔案更新操作介面。
- 若提供線上更新，則檢視線上更新是否具備線上更新操作介面。

(4) 測試結果：

- 本測項為「通過」，更新功能之驗證被認可。
- 本測項為「不通過」，無法證明具備更新功能。

(b) 韌體程式更新測試 - 更新檔案的保護。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.3.1(b)。

(2) 測試標準：

-

- 韌體更新檔案必須加密保護。
- 加密演算法不得為「附錄 A」所列之公認弱加密演算法。

(3) 測試步驟：

- 確認更新檔案是無法被韌體拆解工具拆解。

- 審閱具備此功能證明之書面資料。

(4) 測試結果：

- 本測項為「通過」，韌體無法被拆解且加密演算法之驗證被認可。
-
- 本測項為「不通過」，韌體被拆解。
- 本測項為「不通過」，無法證明加密演算法採用 FIPS 140-2 所核可之加密演算法。

(c) 韌體程式更新測試 - 更新路徑的保護。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.3.1(c)。

(2) 測試標準：

- 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，預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 所核可之演算法[4]。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 將受測物連網並啟動更新。
- 啟動安全通道掃描工具。
- 檢視預設之加密方式是否是 TLS 1.1 以上。
- 檢視預設啟用之加密演算法是否採用 FIPS 140-2 所核可之加密演算法。

(4) 測試結果：

- 本測項為「通過」，加密方式採用 TLS 1.1 以上且預設啟用之加密演算法採用 FIPS 140-2 所核可之加密演算法。
-
- 本測項為「不通過」，加密方式採用 SSL 或 TLS 1.0。

- 本測項為「不通過」，預設啟用之加密演算法未採用 FIPS 140-2 所核可之加密演算法。

5.2.3.2 韌體更新機制強度測試

(a) 線上韌體更新保證測試。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.3.2(a)。

(2) 測試標準：

- 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。

(3) 測試步驟：

- 根據受測物之使用說明，檢視韌體更新操作。
- 若提供離線更新，則檢視離線更新是否具備檔案更新操作介面。
- 若提供線上更新，則檢視線上更新是否具備線上更新操作介面。

(4) 測試結果：

- 本測項為「通過」，不得支援離線更新。
- 本測項為「不通過」，支援離線更新。

(b) 韌體更新之完整性及可信度測試。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.3.2(b)。

(2) 測試標準：

- 經過竄改之更新檔案不得被成功更新。

(3) 測試步驟：

- 擷取更新檔案。
- 竄改更新檔案，檢視是否仍可成功更新。
- 對更新檔案再行簽章，檢視是否可成功更新。

(4) 測試結果：

- 本測項為「通過」，經竄改及再簽章後，更新不成功。
- 本測項為「不通過」，經竄改或再簽章後，更新會成功。

5.2.4 韌體程式安全測試(選測)

此小節之測項為選測，一旦受測物通過測項 5.2.3.1(b)，則廠商須提供解密工具，作為韌體程式檔解密之用，測試環境請參照圖 2。

5.2.4.1 敏感資料外洩測試

(a) 韌體程式碼之敏感資料外洩。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.4.1(a)。

(2) 測試標準：

- 網路攝影機之程式碼與安裝檔內其他檔案，不得被檢出身分認證因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)及個人資料。
- 韌體檔案若被加密，導致無法被拆解，因機敏資料不會被洩露，本測試項目結果為通過。

(3) 測試步驟：

- 使用韌體分析工具拆解韌體。
- 取出檔案系統之路徑目錄。
- 檢視系統密碼資料是否可識別。
- 確認金鑰是否可被擷取。
- 檢查是否存在非公開之 email 資料。
- 檢查是否存在非公開之 IP 資料。
- 檢查是否存在非公開之 url 資料。

(4) 測試結果：

- 本測項為「通過」，密碼、金鑰及非公開之 email、IP 及 url 資料未被檢出。
- 本測項為「不通過」，檢出任一敏感資料，包括：密碼、金鑰及非公開之 email、IP 及 url 資料。

5.2.4.2 韌體程式安全性測試

(a) 韌體程式碼之原始碼掃描。

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.4.2(a)。

(2) 測試標準：

- 檢視受測物之原始碼掃描報告。
- 原始碼掃描報告不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors。

(3) 測試步驟：

- 檢視原始碼掃描報告。

(4) 測試結果：

- 本測項為「通過」，韌體之原始碼掃描報告不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors。
- 本測項為「不通過」，韌體之原始碼掃描報告存在 CWE/SANS TOP 25 Most Dangerous Software Errors。

5.2.5 敏感性資料儲存安全測試

測試環境請參照圖 2。

5.2.5.1 敏感性資料的儲存保護初階測試

(a) 敏感性資料加密儲存測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.5.1(a)。

(2) 測試標準：

- 系統所儲存之身分認證因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不得是明文。
- 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。
- 受測物若不具備作業系統管理介面，則本測試項目結果為通過。

(3) 測試步驟：

- 進入作業系統管理介面。
- 解析檔案系統目錄檢視系統密碼資料是否可識別。
- 確認金鑰是否可被擷取。
- 檢查是否存在非公開之 email 資料。
- 檢查是否存在非公開之 IP 資料。
- 檢查是否存在非公開之 url 資料。

(4) 測試結果：

- 本測項為「通過」，密碼、金鑰及非公開之 email、IP 及 url 資料未被檢出。
- 本測項為「不通過」，檢出任一敏感性資料，包括：密碼、金鑰及非公開之 email、IP 及 url 資料。

5.2.5.2 機敏性資料的儲存保護中階測試

(a) 敏感性資料隔離保護測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.5.2(a)。

(2) 測試標準：

- 受測物須具備安全區域，且敏感性資料須存放於此。

(3) 測試步驟：

- 審閱具備此功能證明之書面資料。

(4) 測試結果：

- 本測項為「通過」，敏感性資料未存放於安全區域中。
- 本測項為「不通過」，無法證明具備安全區域之功能。
- 本測項為「不通過」，敏感性資料未存放於安全區域中。

5.2.6 網頁管理介面安全測試

測試環境請參照圖 2。

5.2.6.1 網頁管理介面常見資安風險測試之初階測試

(a) 網頁管理介面弱點測試之初階測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.6.1(a)。

(2) 測試標準：

- 網頁管理介面操控程式，不得存在引發 OWASP Top 10[6]之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。
- 若受測物不具有網頁管理介面，則本測試項目結果為通過。
- 採自動化工具測試手法。

(3) 測試步驟：

- 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。
- 檢驗測試報告是否存在引發 Injection 及 XSS 攻擊之資安風險。

(4) 測試結果：

- 本測項為「通過」，不存在引發 Injection 及 XSS 攻擊之資安風險。
- 本測項為「不通過」，存在引發 Injection 及 XSS 攻擊之資安風險。

5.2.6.2 網頁管理介面常見資安風險測試之中階測試

(a) 網頁管理介面弱點測試之中階測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.6.2(a)。

(2) 測試標準：

- 網頁管理介面操控程式，不得存在引發 OWASP Top 10[6]之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之資安風險。

- 若受測物不具有網頁管理介面，則本測試項目結果為通過。
- 採人工測試。

(3) 測試步驟：

- 由測試 PC 連線至網路攝影機進行測試。
- 使用人工測試手法對受測物之網頁介面進行測試。
- 檢驗測試報告是否存在引發 Injection 及 XSS 攻擊之資安風險。

(4) 測試結果：

- 本測項為「通過」，不存在引發 Injection 及 XSS 攻擊之資安風險。
- 本測項為「不通過」，存在引發 Injection 及 XSS 攻擊之資安風險。

5.2.7 API 安全測試

測試環境請參照圖 2。

5.2.7.1 API 之認證功能測試

(a) API 呼叫的身分認證機制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.7.1(a)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.1.1(a)測試結果一致。
- 同 5.4.1.1(a)之測試標準。

(3) 測試步驟：

- 同 5.4.1.1(a)之測試步驟。

(4) 測試結果：

- 同 5.4.1.1(a)之測試結果。

(b) API 呼叫之身分認證錯誤訊息

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.7.1(b)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.1.1(b)測試結果一致。
- 同 5.4.1.1(b)之測試標準。

(3) 測試步驟：

- 同 5.4.1.1(b)之測試步驟。

(4) 測試結果：

- 同 5.4.1.1(b)之測試結果。

(c) API 之密碼認證機制 - 密碼強度

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(c)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.2.1(a)測試結果一致。
- 同 5.4.2.1(a)之測試標準。

(3) 測試步驟：

- 同 5.4.2.1(a)之測試步驟。

(4) 測試結果：

- 同 5.4.2.1(a)之測試結果。

(d) API 之密碼認證機制 - 預設密碼唯一性

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(d)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.2.1(b)測試結果一致。
- 同 5.4.2.1(b)之測試標準。

(3) 測試步驟：

- 同 5.4.2.1(b)之測試步驟。

(4) 測試結果：

- 同 5.4.2.1(b)之測試結果。

(e) API 之密碼認證機制 - 密碼變更機制

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(e)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.2.1(c)測試結果一致。
- 同 5.4.2.1(c)之測試標準。

(3) 測試步驟：

- 同 5.4.2.1(c)之測試步驟。

(4) 測試結果：

- 同 5.4.2.1(c)之測試結果。

(f) API 之密碼認證機制 - 密碼的輸入頻率及次數限制

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(f)。

(2) 測試標準：

- 受測物中的所有密碼認證機制皆使用同一組密碼，則本測項測試結果與測項 5.4.2.1(d)測試結果一致。
- 同 5.4.2.1(d)之測試標準。

(3) 測試步驟：

- 同 5.4.2.1(d)之測試步驟。

(4) 測試結果：

- 同 5.4.2.1(d)之測試結果。

(g) API 呼叫之權限管控機制

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(g)。

(2) 測試標準：

- 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受測物自我宣告相符，並且至少要有二個以上不同權限的角色。

(3) 測試步驟：

- 將測試 PC 連線至網路攝影機。
- 根據宣告表所宣告之「裝置 API 帳號權限說明」所提供之帳號，進行 API 的認證授權。
- 進行 API 呼叫的測試。
- 檢視該帳號之身分類型與權限是否與受測物自我宣告相符。

(4) 測試結果：

- 本測項為「通過」，API 呼叫的身分權限與宣告表中「裝置 API 帳號權限說明」相符。
- 本測項為「不通過」，API 呼叫的身分權限與宣告表中「裝置 API 帳號權限說明」不符。

(h) API 呼叫之閒置時限

(1) 測試依據：

「影像監控系統網路攝影機資安標準草案」5.2.7.1(h)。

(2) 測試標準：

- 受測物必須提供 API 呼叫權限之閒置時限功能，最常不得超過 10 分鐘。
- 受測物之每次 API 呼叫皆須重新認證授權，則本測試結果為通過。

(3) 測試步驟：

- 成功取得 API 呼叫之存取權限後。
- 停止進行任何 API 之呼叫。
- 閒置 10 分鐘以上，檢視 API 呼叫是否需要重新認證。

(4) 測試結果：

- 本測項為「通過」，閒置 10 分鐘以上，需重新認證方可再存取 API

呼叫。

- 本測項為「通過」，每次 API 呼叫皆須重新認證授權。
- 本測項為「不通過」，不支援 API 呼叫之權限閒置時限。

5.2.7.2 API 異常輸入測試

(a) API 異常輸入測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.7.2(a)。

(2) 測試標準：

- 受測物所提供之 API 必須經過異常輸入測試，受測之受測物於測試過程中不得發生程序崩潰(crash)到無法恢復運作。

(3) 測試步驟：

- 使用模糊測試工具。
- 由測試 PC 連線至網路攝影機。
- 執行對受測物每一 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) 測試結果：

- 本測項為「通過」，未發生程序崩潰到無法恢復運作。
- 本測項為「不通過」，發生程序崩潰到無法恢復運作。

5.2.8 系統日誌檔與警示測試

測試環境請參照圖 2。

5.2.8.1 安全事件日誌檔測試

(a) 安全事件日誌檔測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.8.1(a)。

(2) 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。
- 受測物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。

(3) 測試步驟：

- 將受測 PC 連接網路攝影機。
- 根據受測物之使用說明，開啟安全事件日誌。
- 檢視日誌內容是否記載使用者的登入紀錄。
- 檢視該登入紀錄是否提供時間與使用者身分資訊。

(4) 測試結果：

- 本測項為「通過」，安全事件日誌須提供時間與使用者身分之登入行為之資訊。
- 本測項為「不通過」，未提供使用者登入行為之安全事件日誌功能。
- 本測項為「不通過」，安全事件日誌功能無提供時間與使用者身分之登入行為之資訊。

(b) 存取權限管控測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.8.1(b)。

(2) 測試標準：

- 產品須對安全事件日誌檔進行權限控管，該安全事件日誌檔的身分授權須與受測物自我宣告相符。

(3) 測試步驟：

- 測試人員根據受測物之使用說明，存取安全事件日誌。
- 檢視身分類型與對日誌檔的存取權限是否與受測物自我宣告相符。

(4) 測試結果：

- 本測項為「通過」，日誌檔的存取權限與「日誌檔權限說明」內容相同。
- 本測項為「不通過」，日誌檔的存取權限與「日誌檔權限說明」內容相異。

(c) 日誌檔保存期限測試

(5) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.8.1(c)。

(6) 測試標準：

- 產品之日誌檔須具備保存期限的設計。
- 須符合 NIST SP 800-92[5]中 high impact systems 的日誌資料維護長度。

(7) 測試步驟：

- 測試人員根據受測物之使用說明，檢視日誌檔的保存期限。

(8) 測試結果：

- 本測項為「通過」，保存期限符合 NIST SP 800-92[5]中 high impact systems 的日誌資料維護長度。
- 本測項為「不通過」，保存期限未符合 NIST SP 800-92[5]中 high impact systems 的日誌資料維護長度。

5.2.8.2 異常警示功能測試

(a) 日誌檔存取異常警示測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.2.8.2(b)。

(2) 測試標準：

- 日誌紀錄檔無法正常儲存時，須發出警示。受測物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。

(3) 測試步驟：

- 將受測物儲存空間填滿。
- 反覆登入/登出直到日誌檔無法儲存。
- 檢視受測物是否依照使用說明達到警示效果。

(4) 測試結果：

- 本測項為「通過」，日誌檔無法儲存時，收到警示。
- 本測項為「不通過」，日誌檔無法儲存時，未收到警示。

5.3 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。

5.3.1 資料傳輸安全測試

測試環境請參照圖 2。

5.3.1.1 敏感資料之傳輸保護初階測試

(a) 敏感資料之傳輸保護初階測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.1.1(a)。

(2) 測試標準：

- 敏感資料之傳輸通道必須經過加密保護，且加密演算法須採用 FIPS 140-2 所核可之演算法[4]。

(3) 測試步驟：

- 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。
- 側錄封包，檢視封包是否經過加密保護。
- 確認加密演算法是否採用 FIPS 140-2 所核可之演算法[4]。

(4) 測試結果：

- 本測項為「通過」，機敏資料之傳輸採用 FIPS 140-2 所核可之演算法。
- 本測項為「不通過」，機敏資料明碼傳輸。
- 本測項為「不通過」，機敏資料之加密傳輸未採用 FIPS 140-2 所核可之演算法。

5.3.1.2 敏感資料之傳輸保護中階測試

(a) 敏感資料之傳輸保護中階測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.1.2(a)。

(2) 測試標準：

- 敏感資料之傳輸通道必須經過加密保護，且加密演算預設必須採用 AES-256 之連線。

(3) 測試步驟：

- 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。
- 側錄封包，檢視封包是否經過加密保護。
- 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) 測試結果：

- 本測項為「通過」，測試程式確認受測物可使用 AES-256 加密傳輸。
- 本測項為「不通過」，機敏資料明碼傳輸。
- 本測項為「不通過」，測試程式確認受測物不可使用 AES-256 加密傳輸。

5.3.2 網路介面通訊協定的安全設置測試

測試環境請參照圖 2。

5.3.2.1 通訊介面組態設置測試

(a) 網路裝置資訊探詢功能測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.2.1(a)。

(2) 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。
- 預設必須為關閉。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 由測試 PC 連線至受測物。
- 開啟網路攝影機之操控程式或網頁管理介面。
- 檢視受測物是否支援 UPnP。
- 確認 UPnP 預設是否關閉。
- 檢視 UPnP 是否存在供使用者操作的開/關介面。
- 檢視受測物是否支援 SNMP。
- 確認 SNMP 預設是否關閉。
- 檢視 SNMP 是否存在供使用者操作的開/關介面。
- 檢視受測物是否支援 Bonjour。
- 確認 Bonjour 預設是否關閉。
- 檢視 Bonjour 是否存在供使用者操作的開/關介面。

(4) 測試結果：

- 本測項為「通過」，UPnP、SNMP 及 Bonjour 預設都必須關閉，且是否都存在供使用者操作的開/關介面。

- 本測項為「不通過」，UPnP、SNMP 及 Bonjour 任一功能預設未關閉。
- 本測項為「不通過」，UPnP、SNMP 及 Bonjour 任一功能未存在供使用者操作的開/關介面。

(b) 安全的 WiFi 組態設置測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.2.1(b)。

(2) 測試標準：

- 受測物只要具備 WPS 功能，則必須提供使用者，WPS PIN 及 WPS Lock 開/關之功能。
- 該功能預設須為關閉。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 由測試 PC 連線至受測物。
- 開啟網路攝影機之操控程式或網頁管理介面。
- 確認 WPS PIN 與 WPS Lock 的預設狀態是在關閉的設定。
- 檢視是否存在 WPS PIN 與 WPS Lock 的開/關操作。

(4) 測試結果：

- 本測項為「通過」，WPS PIN 與 WPS Lock 預設都必須關閉，且是否都存在供使用者操作的開/關介面。
- 本測項為「不通過」，UPnP、SNMP 及 Bonjour 任一功能預設未關閉。
- 本測項為「不通過」，UPnP、SNMP 及 Bonjour 任一功能未存在供使用者操作的開/關介面。

(c) 無線網路傳輸安全機制設置測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.2.1(c)。

(2) 測試標準：

- 無線網路預設加密模式必須使用 WPA2。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 由測試 PC 連線至受測物。
- 開啟網路攝影機之操控程式或網頁管理介面。
- 確認其預設啟用之無線網路傳輸安全機制。

(4) 測試結果：

- 本測項為「通過」，無線網路預設之加密模式為 WPA2。
- 本測項為「不通過」，無線網路預設之加密模式不為 WPA2。

(d) 網路介面存取設置測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.2.1(d)。

(2) 測試標準：

- 使用者不得透過有線或無線連結的方式存取作業系統。

(3) 測試步驟：

- 受測物為出廠預設環境狀態，測試人員透過網路連接受測物。
- 開啟管理介面連接工具。
- 檢視可否透過受測物所開啟之網路服務連接埠存取作業系統。

(4) 測試結果：

- 本測項為「通過」，可透過網路服務連接埠存取作業系統。
- 本測項為「不通過」，不可透過網路服務連接埠存取作業系統。

5.3.3 通訊協定安全測試

測試環境請參照圖 2。

5.3.3.1 通訊協定異常輸入測試

(a) 通訊協定異常輸入測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.3.3.1(a)。

(2) 測試標準：

- 通訊協定必須經過異常輸入測試，受測物於測試過程中不得發生程序崩潰(crash)到無法恢復運作。

(3) 測試步驟：

- 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。
- 執行對「附錄 C」中每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) 測試結果：

- 本測項為「通過」，未發生程序崩潰到無法恢復運作。
- 本測項為「不通過」，發生程序崩潰到無法恢復運作。

5.4 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。

5.4.1 認證機制安全測試

測試環境請參照圖 2。

5.4.1.1 認證機制強度初階測試

(a) 認證機制強度測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.1.1(a)。

(2) 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。

(3) 測試步驟：

- 由測試 PC 透過遠端連線與受測物建立連接。
- 檢視存取受測物前，網路攝影機是否有要求身分認證。
- 若不具身分認證機制，本測試項目結果為不通過，測試結束。
- 進行身分認證並側錄封包。
- 將側錄到的認證封包再重新送至網路攝影機。
- 判斷認證結果是否成功。

(4) 測試結果：

- 本測項為「通過」，重送攻擊之封包未通過受測物之認證。
- 本測項為「不通過」，受測物不具備身分認證功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之認證。

(b) 裝置認證測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.1.1(b)。

(2) 測試標準：

- 產品須提供能驗證相連影像監控系統裝置身分的功能，且其裝置認證機制具備抵抗重送攻擊的能力。

(3) 測試步驟：

- 將受測裝置與其它影像監控系統裝置建立連線。
- 監聽連線建立封包。
- 檢查成功建立連線前，是否要求裝置認證。
- 若不具裝置認證機制，本測試項目結果為不通過，測試結束。
- 進行身分認證並側錄封包。
- 將側錄到的認證封包再重新送至網路攝影機。
- 判斷認證結果是否成功。

(4) 測試結果：

- 本測項為「通過」，重送攻擊之封包未通過受測物之認證。
- 本測項為「不通過」，受測物不具備裝置認證功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之認證。

(c) 身分認證錯誤訊息

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.1.1(c)。

(2) 測試標準：

- 從錯誤訊息無法推斷出合法使用者名稱。

(3) 測試步驟：

- 由測試 PC 透過遠端連線至受測物進行測試。
- 輸入錯誤的帳號、密碼。
- 檢視錯誤訊息是否透露合法帳號的存在。

(4) 測試結果：

- 本測項為「通過」，錯誤訊息未明確指出是帳號錯誤還是密碼錯誤。
- 本測項為「不通過」，錯誤訊息明確指出是帳號錯誤還是密碼錯誤。

5.4.1.2 認證機制強度中階測試

(a) 認證機制強度測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.1.2(a)。

(2) 測試標準：

- 驗證相連影像監控系統裝置身分的認證機制，是否透過雙因子認證。
- 驗證遠端管理介面或操控程式與網路攝影機之間的身分認證，是否透過雙因子認證。

(3) 測試步驟：

審閱具備此功能證明之書面資料。

(4) 測試結果：

- 本測項為「通過」，產品之身分認證透過雙因子認證。
- 本測項為「不通過」，產品之身分認證未透過雙因子認證。

5.4.2 密碼認證安全測試

測試環境請參照圖 2。

5.4.2.1 密碼認證機制

(a) 密碼強度

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.2.1(a)。

(2) 測試標準：

- 密碼認證之密碼長度必須符合政府組態基準 CCE-33789-9。
- 密碼認證之密碼複雜度必須符合政府組態基準 CCE-33777-4。
- 密碼認證之防止重複使用舊密碼必須符合政府組態基準 CCE-35219-5。

(3) 測試步驟：

- 由測試 PC 連線至網路攝影機進行 API 授權密碼輸入。
- 根據政府組態基準 CCE-33789-9 之 GCB 設定值，檢視受測物密碼輸入長度至少要求 8 個字元以上。
- 根據政府組態基準 CCE-33777-4 之 GCB 設定值，檢視受測物建立或變更密碼時是否會強制執行複雜性需求，包括：
  - 不得含使用者的帳戶名稱全名中，超過兩個以上的連續字元。
  - 包含下列四種字元中的三種：
    - 英文大寫字元(A 到 Z)。
    - 英文小寫字元(a 到 z)。
    - 10 進位數字(0 到 9)。
    - 非英文字母字元(例如：!、$、#、%)。
- 根據政府組態基準 CCE-35219-5 之 GCB 設定值，檢視受測物是否執行密碼歷程記錄。

(4) 測試結果：

- 本測項為「通過」，同時符合政府組態基準 CCE-33789-9、CCE-33777-4 及 CCE-35219-5。
- 本測項為「不通過」，不符合政府組態基準 CCE-33789-9。
- 本測項為「不通過」，不符合政府組態基準 CCE-33777-4。
- 本測項為「不通過」，不符合政府組態基準 CCE-35219-5。

(b) 預設密碼唯一性

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.2.1(b)。

(2) 測試標準：

- 預設密碼都須相異。

(3) 測試步驟：

- 準備 2 台以上受測物。
- 受測物為出廠預設環境狀態。
- 由測試 PC 連線至受測物進行 API 授權密碼輸入。
- 比對每台網路攝影機的預設密碼是否相異。

(4) 測試結果：

- 本測項為「通過」，每台受測物的預設密碼相異。
- 本測項為「通過」，受測物登入要認證，但不存在預設密碼，則本測試項目結果為通過。
- 本測項為「不通過」，每台受測物的預設密碼相同。

(c) 密碼變更機制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.2.1(c)。

(2) 測試標準：

- 首次取得授權後必須強制更改預設密碼。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 由測試 PC 連線至受測物。
- 進行 API 認證密碼輸入。
- 確認首次取得授權後，是否強制要求更改預設密碼。

(4) 測試結果：

- 本測項為「通過」，首次取得授權後，強制要求更改預設密碼。
- 本測項為「不通過」，首次取得授權後，未強制要求更改預設密碼。

(d) 密碼的輸入頻率及次數限制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.2.1(d)。

(2) 測試標準：

- 密碼的輸入次數必須符合最高 5 次嘗試登入失敗次數導致帳戶鎖定的限制。
- 密碼的輸入頻率必須符合帳戶鎖定計數器至少 1 分鐘以上的時間間隔，才會將失敗的登入嘗試計數器重設為 0 次失敗。
- 密碼的輸入頻率必須符合帳戶鎖定期間至少 1 分鐘以上，才會自動解除鎖定。

(3) 測試步驟：

- 由測試 PC 連線至網路攝影機進行 API 授權密碼輸入。
- 不斷輸入錯誤的密碼進行 API 認證。
- 檢視受測物被鎖定的嘗試登入失敗次數最多不可超過 5 次。
- 檢視受測物重設帳戶鎖定計數器的時間間隔至少要為 1 分鐘。
- 檢視受測物之帳戶鎖定期間至少 1 分鐘以上。

(4) 測試結果：

- 本測項為「通過」，同時符合帳戶鎖定限制最多 5 次、帳戶鎖定計數

器時間間隔至少 1 分鐘及帳戶鎖定期間至少 1 分鐘。

- 本測項為「不通過」，帳戶鎖定限制高於 5 次。
- 本測項為「不通過」，帳戶鎖定計數器時間間隔不到 1 分鐘。
- 本測項為「不通過」，帳戶鎖定期間不到 1 分鐘。

5.4.3 權限管控安全測試

測試環境請參照圖 2。

5.4.3.1 權限管控機制

(a) 權限管控機制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.3.1(a)。

(2) 測試標準：

- 透過遠端連線存取受測物，必須具備權限管控機制，該使用者的身分授權須與受測物自我宣告相符，並且至少要有二個以上不同權限的角色。

(3) 測試步驟：

- 將測試 PC 連線至受測物。
- 根據受測物之宣告說明，對受測物所有的遠端管理介面進行操作。
- 檢視該帳號之身分類型與其對應之權限是否與受測物自我宣告相符。

(4) 測試結果：

- 本測項為「通過」，帳戶身分與其對應之權限與受測物宣告相符。
- 本測項為「不通過」，帳戶身分與其對應之權限與受測物宣告不符。

(b) 權限有效時間

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.4.3.1(b)。

(2) 測試標準：

- 受測物必須提供遠端控制權限之閒置時限功能，且閒置時限最多不可超過 20 分鐘。

(3) 測試步驟：

- 成功取得遠端連線之存取權限後。

- 停止進行任何遠端控制。
- 閒置 20 分鐘以上，檢視再次遠端控制受測物時是否需要重新認證。

(4) 測試結果：

- 本測項為「通過」，閒置 20 分鐘以上，需重新認證方可再遠端控制/存取受測物。
- 本測項為「不通過」，閒置 20 分鐘以上，無需重新認證方即再遠端控制/存取受測物。

5.5 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。

5.5.1 隱私資料的使用保護測試

5.5.1.1 隱私資料權限管控測試

測試環境請參照圖 2。

(a) 隱私資料的存取控制

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.1.1(a)。

(2) 測試標準：

- 受測物所儲存的隱私資料，必須具備權限管控機制，該使用者的隱私存取授權須與受測物自我宣告相符。
- 並且至少要有二個以上不同權限的角色。

(3) 測試步驟：

- 將測試 PC 連線至受測物。
- 根據受測物說明，以不同身分之使用者進行隱私存取。
- 檢視該帳號之身分類型與其對應之權限是否與受測物自我宣告相符。

(4) 測試結果：

- 本測項為「通過」，帳戶身分與其對應之權限與受測物宣告相符。
- 本測項為「不通過」，帳戶身分與其對應之權限與受測物宣告不符。

(b) 隱私資料刪除功能

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.1.1(b)。

(2) 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。

(3) 測試步驟：

- 根據受測物說明，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。
- 執行刪除功能後，確認受測物之隱私資料已被移除。

(4) 測試結果：

- 本測項為「通過」，隱私資料可被移除。
- 本測項為「不通過」，隱私資料不可被移除。

(c) 登入警示功能測試

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.1.1(c)。

(2) 測試標準：

-受測物必須具備登入警示功能。

(3) 測試步驟：

1. 開啟遠端管理介面。
2. 登入網路攝影機成功。
3. 根據受測物使用說明，確認是否接收到登入警示。
4. 登入網路攝影機失敗，包括未授權的使用者登入與帳密輸入錯誤。
5. 根據受測物使用說明，確認是否接收到登入警示。

(4) 測試結果：

-本測項為「通過」，登入成功及失敗，皆收到登入警示。

-本測項為「不通過」，登入成功或失敗，未收到登入警示。

5.5.2 隱私資料的傳輸保護測試

測試環境請參照圖 2。

5.5.2.1 隱私資料的傳輸初階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.2.1(a)。

(2) 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使用 FIPS 140-2 所核可之加密演算法[4]。

(3) 測試步驟：

- 由遠端管理介面進行受測物各種功能操作。
- 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) 測試結果：

- 本測項為「通過」，影像類的隱私資料不得以明文的方式傳輸。
- 本測項為「通過」，非影像類隱私資料之傳輸使用 FIPS 140-2 所核可之加密演算法。
- 本測項為「不通過」，影像類的隱私資料以明文傳輸。
- 本測項為「不通過」，非影像類的隱私資料傳輸不是使用 FIPS 140-2 所核可之加密演算法。

5.5.2.2 隱私資料的傳輸中階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.2.2(a)。

(2) 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[4]。

(3) 測試步驟：

- 由遠端管理介面進行受測物各種功能操作。
- 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) 測試結果：

- 本測項為「通過」，隱私資料之傳輸使用 FIPS 140-2 所核可之加密演算法。
- 本測項為「不通過」，隱私資料傳輸不是使用 FIPS 140-2 所核可之加密演算法。

5.5.2.3 隱私資料的傳輸高階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-網路攝影機」5.5.2.3(a)。

(2) 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。

(3) 測試步驟：

- 於網路攝影機中啟動測試程式。
- 檢查測試程式回報結果。

(4) 測試結果：

- 本測項為「通過」，測試程式回報可使用 AES-256 加密傳輸。

- 本測項為「不通過」，測試程式回報不可使用 AES-256 加密傳輸。

附錄 A

(規定)

公認之弱加密演算法

A.1 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。

A.2 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。

A.3 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。

A.4 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。

A.5 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，所以已經完全由 TLS 取代 SSL，但 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，因此目前本規範強烈建議使用的版本如下：

- Transport Layer Security (TLS) 1.2

附錄 C

(規定)

網路攝影機所使用之通訊協定

C.1 即時傳輸協定 (Real-time Transport Protocol, RTP)：

定義在 RFC 3550 規範中[7]，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。

C.2 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)。

C.3 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中[8]，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。

C.4 超文本傳輸協定(HyperText Transfer Protocol, HTTP)：

定義在 RFC 7540 規範中[9]，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。

C.5 HTTPS 加密協定(HyperText Transfer Protocol Secure, HTTPS)：

定義在 RFC 2818 規範中[10]，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。

參考資料

1. 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
2. NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing
3. 行政院國家資通安全會報技術服務中心, 政府組態基準 Microsoft Windows 8.1 (V1.3)
4. National Institute of Standards and Technology, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017.
5. NIST, NIST Special Publication 800-92: Guide to Computer Security Log Management, Sep, 2006
6. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
7. RFC 3550, RTP: A Transport Protocol for Real-Time Applications
8. RFC 2326, Real Time Streaming Protocol (RTSP)
9. RFC 7540, Hypertext Transfer Protocol Version 2 (HTTP/2)
10. RFC 2818, HTTP Over TLS