影像監控系統資安標準之測試規範
草案-影像錄影機
(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

2017-09-05

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	2017/9/5	陳聰杰	無	新建立

目錄

前言

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

物聯網的盛行，使日常用品皆朝向網路化邁進，影像錄影機也是其中之一，運用範圍包括：影音預覽、錄影錄音、影音回放、資料備份、遠端監控服務等，相當受到消費者青睞，但隨之而來的問題是網路攻擊事件，從 2014 年起網路資安事件日益頻繁、攻擊事件規模越來越大，2016 年底以 Mirai 為名的惡意程式，藉由影像錄影機為跳板，製造出前所未聞之網路攻擊的手法。

有鑑於此，藉由「影像監控系統資安標準草案-影像錄影機」之制定(以下簡稱本標準)，建立國內在確保影像錄影機資安品質的規範，期使設備商或系統服務商在產品研發上有所依據，促進國內產業整體優質化及產品競爭力，確保消費者在影像錄影機之運用上達到安全的目的。

本標準之制定係參照國際物聯網相關資安標準/規範，如 ISO 27001[2]、UL 2900 系列標準[7]、GSMA IoT Security Guideline[1]、OWASP Top IoT Vulnerabilities[6]及日本政府的物聯網安全指導方針[10]等，主要規劃從六大面向確保影像錄影機的資訊安全，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、隱私保護及應用程式安全；並分成三個安全需求等級，詳盡載明欲實踐每一個安全需求等級的必要條件，用以界定不同產品須具備之資安要求。

在確保影像錄影機的資安品質時，應同時考量整體影像監控系統的安全性，例如:管理影像錄影機的雲服務被駭客入侵、操控影像錄影機的行動應用程式含有軟體漏洞及安全等級不足的網路攝影機等因素，皆可能對影像錄影機造成資安威脅，因此建議設置時時須參閱所有相關產品之資安標準，達到整體網路影像監控系統的安全保證(Security Assurance)。

1. 適用範圍

泛指應用於影像監控系統的影像錄影機，且凡是影像錄影機本身具連網功能者皆是影像錄影機的一種，如圖 1 實線框處所示。

本標準為確保影像錄影機資安，訂定其產品之安全技術要求，擬分為六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、隱私保護及應用程式安全。

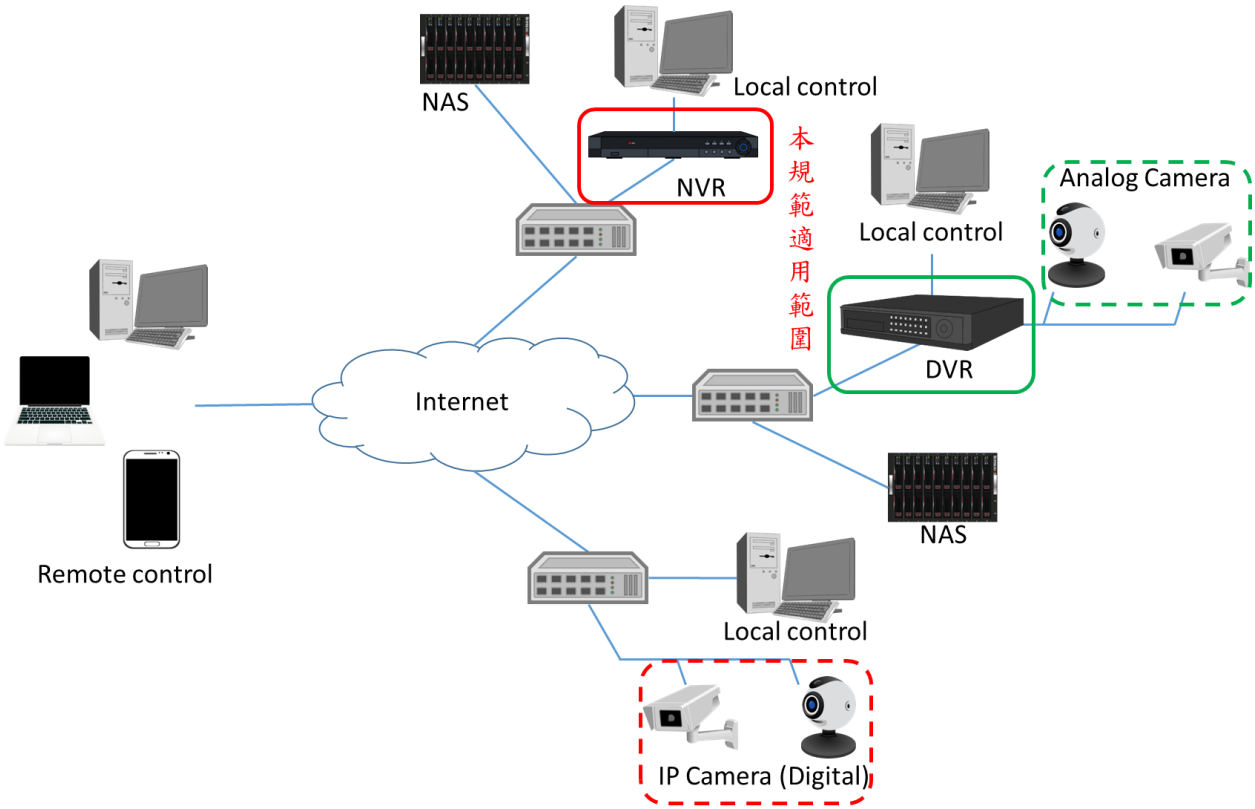

圖 1. 適用範圍示意圖

2. 用語及定義

下列用語與定義適用於本標準。

2.1. 影像錄影機 (Video Recorder)

係指一種主要用於影像監控系統且具連網功能的影像錄影機，其應用類型包括：數位影像錄影機(Digital Video Recorder，DVR)與網路影像錄影機(Network Video Recorder, NVR)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. 國家資安弱點資料庫 (National Vulnerabilities Database)

美國國家標準技術研究所（NIST）的國家資安弱點資料庫[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影像錄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影像錄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影像錄影機資源，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)

係指用於控制影像錄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。大部份影像錄影機皆提供 API 給操控端之應用程式呼叫，用戶可透過這些 API，撰寫實際實現影像錄影機相關操作(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，用以登入影像錄影機之密碼。

3. 測試項目分級

本節針對影像監控系統影像錄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、隱私保護及應用程式安全共 6 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 1。

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. 出廠之實體埠必須具備安全管控測試	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. 軟韌體程式安全測試	4.2.5.1	4.2.5.1	4.2.5.2
	4.2.6. 敏感性資料儲存安全測試	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. 操控程式之 API 安全測試			4.2.8.1
	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	4.3.1. 敏感性資料傳輸安全測試	4.3.1.1	4.3.1.1	4.3.1.2

測試	4.3.2. 通訊介面的安全設置測試	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. 認證資訊的傳輸保護測試	4.4.2.1	4.4.2.1	4.4.2.2
	4.4.3. 密碼認證機制測試	4.4.3.1	4.4.3.1	4.4.3.1
	4.4.4. 權限控管測試	4.4.4.1	4.4.4.1	4.4.4.1
隱私保護測試	4.5.1. 隱私資料的存取保護測試	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
應用程式安全測試	4.6.1. 應用程式的程式安全測試	4.6.1.1	4.6.1.2	4.6.1.3
	4.6.2. 應用程式的系統安全測試	4.6.2.1	4.6.2.2	4.6.2.3

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。 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。 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 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。
網路服務連接埠測試	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。
網路服務安全測試	4.2.3.1A 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 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。
更新安全測試	4.2.4.1A 軟韌體須具備更新機制。 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[4]。 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[4]。
軟韌體程式安全測試	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，不得出現於軟韌體之程式碼與安裝檔內其他檔案中。
敏感性資料儲存安全測試	4.2.6.1A 產品之敏感性資料須透過加密儲存，必須使用 FIPS 140-2 所核可之加密演算法[4]確保機密性。
網頁管理介面安全測試	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。
操控程式之 API 安全測試	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。 4.2.8.1B 認證錯誤訊息不能顯露出合法使用者名稱。 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 4.2.8.1D 廠商所生產之影像錄影機其預設密碼都須相異。 4.2.8.1E 首次成功取得影像錄影機 API 之認證，必須強制更改預設密碼。 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。 4.2.8.1G API 的存取，必須具備權限管控機制，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。

	4.2.8.1H 產品之授權行為，應存在閒置時限供使用者設定。
系統日誌檔與警示測試	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。 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。 4.2.9.1C 產品之安全事件日誌檔紀錄檔須具備顯示功能機制。
通訊安全測試	
敏感性資料傳輸安全測試	4.3.1.1A 敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。
通訊介面的安全設置測試	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，且預設須為關閉狀態。 4.3.2.1B 產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。 4.3.2.1C 無線網路傳輸的安全機制必須支援 WPA2。
身分認證與授權機制安全測試	
認證機制安全測試	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。 4.4.1.1B 認證錯誤訊息不能顯露出合法使用者名稱。
密碼認證機制測試	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。 4.4.2.1B 廠商所生產之影像錄影機其預設密碼都須相異。 4.4.2.1C 首次登入產品必須強制更改預設密碼。 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。
權限控管測試	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。 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，此外，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。 4.4.3.1C 產品之授權行為，應存在閒置時限供使用者設定，一旦遠端連

	線已經遺失或結束，須要求新的認證。
隱私保護測試	
隱私資料的存取保護測試	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。 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。
隱私資料的傳輸保護測試	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，須使用 FIPS 140-2 所核可之加密演算法[4]。
應用程式安全測試	
應用程式的程式安全測試	4.6.1.1A 應用程式在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。 4.6.1.1B 應用程式應確認資料來源的安全。 4.6.1.1C 應用程式應可識別其發行資訊，以確保使用者瞭解其來源。 4.6.1.1D 應用程式所執行的行為，應取得使用者同意，並與其宣告之內容相符。 4.6.1.1E 應用程式所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路埠」相符。 4.6.1.1F 廠商需於文件中標明所使用之應用程式及引用之第三方函式庫。 4.6.1.1G 應用程式所引用之第三方函式庫，不得存在已揭露之重大資訊安全漏洞。 4.6.1.1H 應用程式必須具備應用程式更新機制。 4.6.1.1I 應用程式之敏感性資料不得出現於裝置應用程式程式碼中。
應用程式的系統安全測試	4.6.2.1A 應用程式所執行的程式行為，應取得使用者同意，必要時並提供風險提示。 4.6.2.1B 應用程式於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。 4.6.2.1C 應用程式應提供安全的身分辨識及保護機制。

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。 4.1.2.1B 實體設計之自動化硬體偵測機制，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。
實體防護測試	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。
作業系統安全測試	
作業系統安全測試	4.2.1.2A 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。
網路服務連接埠測試	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。
網路服務安全測試	4.2.3.2A 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。
更新安全測試	4.2.4.2A 除達到 4.2.4.1 要求外，軟韌體更新機制須一律採用線上更新。 4.2.4.2B 除達到 4.2.4.1 要求外，軟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。
軟韌體程式安全測試	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，不得出現於軟/韌體之程式碼與安裝檔內其他檔案中。

敏感性資料儲存安全測試	4.2.6.1A 產品之敏感性資料須透過加密儲存，必須使用 FIPS 140-2 所核可之加密演算法[4]確保機密性。
網頁管理介面安全測試	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。
操控程式之 API 安全測試	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。 4.2.8.1B 認證錯誤訊息不能顯露出合法使用者名稱。 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 4.2.8.1D 廠商所生產之影像錄影機其預設密碼都須相異。 4.2.8.1E 首次成功取得影像錄影機 API 之認證，必須強制更改預設密碼。 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。 4.2.8.1G API 的存取，必須具備權限管控機制，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。 4.2.8.1H 產品之授權行為，應存在閒置時限供使用者設定。
系統日誌檔與警示測試	4.2.9.2A 除達到 4.2.9.1 要求外，產品須提供異常警示功能。 4.2.9.2B 除達到 4.2.9.1 要求外，影像錄影機應提供當日誌紀錄檔無法儲存時之系統警示。
通訊安全測試	
敏感性資料傳輸安全測試	4.3.1.1A 敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。
通訊介面的安全設置測試	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，且預設須為關閉狀態。 4.3.2.1B 產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。 4.3.2.1C 無線網路傳輸的安全機制必須支援 WPA2。
通訊協定安全	4.3.3.1A 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

測試	協定屬性等欄位，避免關鍵之通訊協定(見附錄 A)因為任意或非法的輸入，造成產品異常行為的發生。
身分認證與授權機制安全測試	
認證機制安全測試	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。 4.4.1.1B 認證錯誤訊息不能顯露出合法使用者名稱。
密碼認證安全測試	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。 4.4.2.1B 廠商所生產之影像錄影機其預設密碼都須相異。 4.4.2.1C 首次登入產品必須強制更改預設密碼。 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。
權限控管測試	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。 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，此外，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。 4.4.3.1C 產品之授權行為，應存在閒置時限供使用者設定，一旦遠端連線已經遺失或結束，須要求新的認證。
隱私保護測試	
隱私資料的存取保護測試	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。 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。
隱私資料的傳輸保護測試	4.5.2.2A 隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[4]。
應用程式安全測試	
應用程式的程式安全測試	4.6.1.2A 應用程式不應在未取得使用者同意之情況下，於背景發送簡訊。 4.6.1.2B 應用程式於使用者設定關閉時，應停止該內建軟體所有相關程序。 4.6.1.2C 應用程式可能有程式設計上缺陷，內建應用程式應經過源碼掃描。

應用程式的系統安全測試	4.6.2.2A 應用程式應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。 4.6.2.2B 應用程式應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。 4.6.2.2C 應用程式之螢幕鎖定解鎖資料，不應以明文方式儲存，以避免遭未經授權的使用。 4.6.2.2D 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至少須 15 個字母。 4.6.2.2E 應用程式應提供回報安全性問題之管道。

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。 4.1.2.1B 實體設計之自動化硬體偵測機制，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。
實體防護測試	4.1.3.2A 除達到 4.1.3.1 要求外，晶片與功能編號不可存在於電路板。 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。
安全啟動測試	4.1.4.1A 確保產品於開機時，避免未經授權的軟韌體、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 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。
網路服務連接埠測試	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。
網路服務安全測試	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。
更新安全測試	4.2.4.2A 除達到 4.2.4.1 要求外，軟韌體更新機制須一律採用線上更新。 4.2.4.2B 除達到 4.2.4.1 要求外，軟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。
軟韌體程式安全測試	4.2.5.2A 產品的軟韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11]。
敏感性資料儲存安全測試	4.2.6.2A 敏感資料必須存放於產品的安全區域(Secure domain)中。
網頁管理介面安全測試	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。
操控程式之 API 安全測試	4.2.8.2A 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。
系統日誌檔與警示測試	4.2.9.2A 除達到 4.2.9.1 要求外，產品須提供異常警示功能。 4.2.9.2B 除達到 4.2.9.1 要求外，影像錄影機應提供當日誌紀錄檔無法儲存時之系統警示。
通訊安全測試	
敏感性資料傳輸安全測試	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。
通訊介面的安	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：

全設置測試	UPnP、SNMP 及 Bonjour，且預設須為關閉狀態。 4.3.2.1B 產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。 4.3.2.1C 無線網路傳輸的安全機制必須支援 WPA2。
通訊協定安全測試	4.3.3.1A 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，避免關鍵之通訊協定(見附錄 A)因為任意或非法的輸入，造成產品異常行為的發生。
身分認證與授權機制安全測試	
認證機制安全測試	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。 4.4.1.2B 除達到 4.4.1.1 要求外，產品之身分認證機制須採用雙向認證機制。
密碼認證機制測試	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。 4.4.2.1B 廠商所生產之影像錄影機其預設密碼都須相異。 4.4.2.1C 首次登入產品必須強制更改預設密碼。 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。
權限控管測試	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。 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，此外，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。 4.4.3.1C 產品之授權行為，應存在閒置時限供使用者設定，一旦遠端連線已經遺失或結束，須要求新的認證。
隱私保護測試	
隱私資料的存取保護測試	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。 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。
隱私資料的傳	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。

輸保護測試	
應用程式安全測試	
應用程式的程式安全測試	4.6.1.3A 應用程式應具備惡意字串輸入時的處理能力。 4.6.1.3B 應用程式應提供回報安全性問題之管道。 4.6.1.3C 應用程式可能被竄改，內建應用程式須具備數位簽章。
應用程式的系統安全測試	4.6.2.3A 應用程式應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。 4.6.2.3B 開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。 4.6.2.3C 應用程式須提供讓安全應用程式執行之安全區域。 4.6.2.3D 應用程式須具備應用程式異常操作之監控及防護。

4. 影像錄影機資安測試規範

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(供測試人員連線至影像錄影機之終端設備)、有線連線(乙太網路線或光纖纜線)、無線連線(WiFi)與受測之影像錄影機，用以測試受測裝置是否符合測試規範。

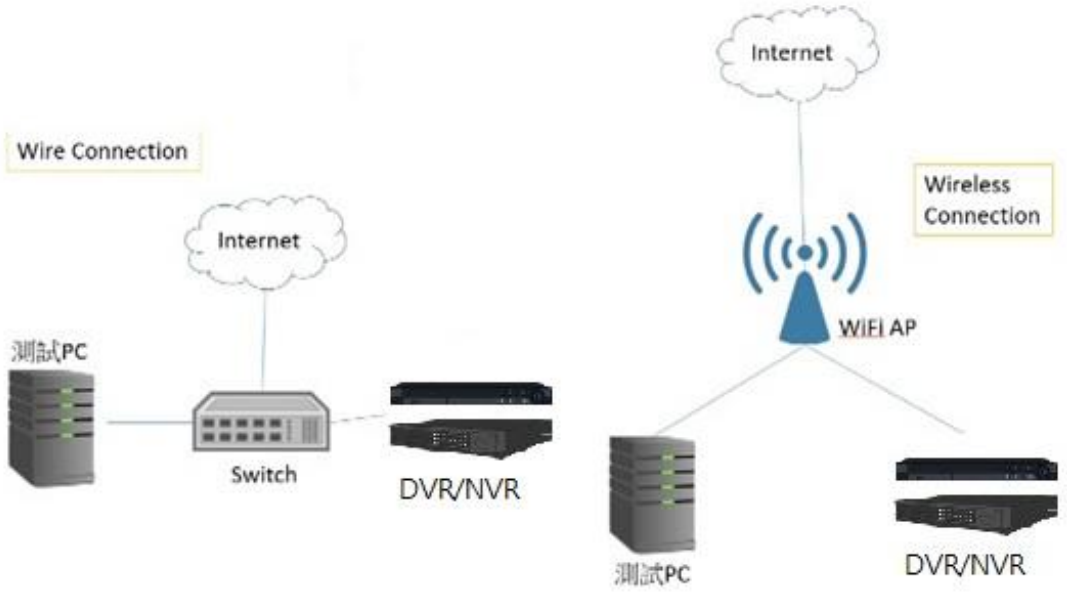

圖 2. 系統安全測試接續示意圖

4.1.1.1. 出廠之實體埠必須具備安全管控測試

A 除錯和測試功能必須關閉

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.1.1. 出廠之實體埠必須具備安全管控。

- 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 沒使用到的實體埠可以被關閉

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.1.1. 出廠之實體埠必須具備安全管控。

- 測試標準：

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。

- 測試方法：

依據廠商所提供之產品規格書，檢視是否有非必要功能的實體埠，例如：TTL、UART、JTAG、SWD 等，非使用者必要的實體埠須被關閉其功能，若必要之實體埠盡可能採最小數量使用原則，例如 SD、USB 等。

C 外接實體埠的操作機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.1.1. 出廠之實體埠必須具備安全管控。

- 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，其中需包含例如：日期與時間、主機名稱、服務名稱、顯示訊息、訊息等級、存放或顯示地點等。

4.1.1.2. 產品的外觀不得有實體埠存在測試

A 產品的外觀不得有實體埠存在

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.1.2. 產品不得有外接儲存用及除錯測試用之實體介面存在。

- 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，並於產品外觀

不得檢出具有除錯或測試用途之界面，例如：TTL、UART、JTAG、SWD、SD Card 等，其零件外觀不限於排母、排針、板對板連接器、板對線連接器、抽屜式連接器等。

4.1.2. 影像錄影機之實體異常行為警示測試

測試環境請參照圖 2。

4.1.2.1. 實體異常行為警示測試

A 異常時須提供警示機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.2.1. 影像錄影機之硬體設計須具備異常狀態之警示機制。

- 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，其警示機制包含例如：E- Mail 通知、訊息推播、蜂鳴器等。

B 實體設計之自動化硬體偵測機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.2.1. 影像錄影機之硬體設計須具備異常狀態之警示機制。

- 測試標準：

實體設計之自動化硬體偵測機制，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。

- 測試方法：

若實體裝置被破壞，應具有自動化硬體偵測之機制，檢視其異常動作時，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。

4.1.3. 影像錄影機之實體防護測試

測試環境請參照圖 2。

4.1.3.1. 影像錄影機之實體防護測試

A 產品之外殼不能被輕易拆除或破壞

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.3.1. 產品之外殼不能被輕易拆除或破壞。

- 測試標準：

產品在實體上要有防止被輕易拆除或破壞之設計護，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。

- 測試方法：

影像錄影機之機殼不能被輕易拆除或破壞，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. 影像錄影機之進階實體防護測試

A 晶片與功能編號不可存在於電路板

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.3.2. 避免不安全的實體設計。

- 測試標準：

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 不得存在可輕易一鍵還原回預設密碼的設計

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.1.3.2. 避免不安全的實體設計。

- 測試標準：

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. 影像錄影機之安全啟動測試

測試環境請參照圖 2。

4.1.4.1. 影像錄影機之安全啟動測試

A 產品須提供安全啟動(secure boot)功能

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.1.4.1. 產品須提供安全啟動(secure boot)功能。

- 測試標準：

  確保產品於開機時，避免未經授權的軟韌體、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

檢視影像錄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. 影像錄影機之作業系統安全測試

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 作業系統之 CVSS v3 評分為 10 分之安全機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.1.1. 作業系統不得存在 CVSS v3 評分為 10 分之資訊安全弱點。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 連線至影像錄影機，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 作業系統之 CVSS v3 評分為 9 分之安全機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.1.2. 作業系統不得存在 CVSS v3 評分為 9 分之資訊安全弱點。

- 測試標準：

  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。

- 測試方法：

由測試 PC 連線至影像錄影機，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 作業系統之 CVSS v3 評分為 7 分之安全機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.1.3. 作業系統不得存在 CVSS v3 評分為 7 分之資訊安全弱點。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 連線至影像錄影機，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. 網路服務連接埠測試

測試環境請參照圖 2。

4.2.2.1. 影像錄影機僅開啟必要之網路服務測試

A 影像錄影機僅開啟必要之網路服務

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.2.1 影像錄影機僅開啟必要之網路服務。

- 測試標準：

  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。

- 測試方法：

  開啟網路服務連接埠掃瞄工具，由測試 PC 連線至影像錄影機進行測試，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. 影像錄影機之網路服務安全測試

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 網路服務在 CVSS v3 評分為 10 分之安全機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.3.1 網路服務不得存在 CVSS v3 評分為 10 分之資訊安全漏洞。

- 測試標準：

  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 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。

- 測試方法：

  由測試 PC 連線至影像錄影機，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 網路服務在 CVSS v3 評分為 9 分之安全機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.3.2 網路服務不得存在 CVSS v3 評分為 9 分之資訊安全漏洞。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 連線至影像錄影機，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 網路服務在 CVSS v3 評分為 7 分之安全機制]

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.2.3.3 網路服務不得存在 CVSS v3 評分為 7 分之資訊安全漏洞。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 連線至影像錄影機，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. 影像錄影機之更新安全測試

測試環境請參照圖 2。

4.2.4.1. 軟韌體更新機制測試

A 軟韌體須具備更新機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.1. 軟韌體更新機密性保證。

- 測試標準：

軟韌體須具備更新機制。

- 測試方法：

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

B 產品支援離線手動更新

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.1. 軟韌體更新機密性保證。

- 測試標準：

產品支援離線手動更新，則更新檔案得確保機密性。

- 測試方法：

將影像錄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。

C 產品支援線上自動更新

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.1. 軟韌體更新機密性保證。

- 測試標準：

產品支援線上自動更新，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。

- 測試方法：

將影像錄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。

D 加密演算法須採用 FIPS 140-2

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.1. 軟韌體更新機密性保證。

- 測試標準：

使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[4]。

- 測試方法：

將影像錄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. 軟韌體線上更新機制測試

A 軟韌體更新機制須一律採用線上更新

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.2. 軟韌體更新機制強度。

- 測試標準：

除達到軟韌體更新機密性保證要求外，軟韌體更新機制須一律採用線上更新。

- 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。

B 軟韌體更新必須透過數位簽章機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.4.2. 軟韌體更新機制強度。

- 測試標準：

除達到軟韌體更新機密性保證要求外，軟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。

4.2.5. 影像錄影機之軟韌體程式安全測試

測試環境請參照圖 2。

4.2.5.1. 產品之敏感性資料在裝置軟/韌體程式碼的機制測試

A 產品之敏感性資料在裝置軟/韌體程式碼的機制測試

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.5.1. 產品之敏感性資料不得出現於裝置軟/韌體程式碼中。

- 測試標準：

產品之帳號、密碼、身分認證因子或加解密用之金鑰，不得出現於軟/韌體之程式碼與安裝檔內其他檔案中。

- 測試方法：

使用檢測工具拆解軟韌體，取出檔案系統目錄，確認加解密金鑰等機敏資料不得於影像錄影機軟韌體中被檢驗出來。

4.2.5.2. 敏感性資料在裝置軟/韌體程式碼的機制測試

A 敏感性資料在裝置軟/韌體程式碼的機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.5.2 除達到 4.2.5.1 要求外，產品的韌體不得存在因程式設計錯誤，而導致程式存在安全性弱點。

- 測試標準：

敏感性資料不得出現於裝置軟/韌體程式碼中。

- 測試方法：

使用檢測工具拆解軟韌體，取出檔案系統目錄，確認加解密金鑰等機敏資料不得於影像錄影機軟韌體中被檢驗出來。

B 產品的軟韌體之程式存在安全性弱點的機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.5.2 除達到 4.2.5.1 要求外，產品的軟韌體不得存在因程式設計錯誤，而導致程式存在安全性弱點。

- 測試標準：

  產品的軟韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11]。

- 測試方法：

  使用檢測工具拆解軟韌體，取出檔案系統目錄，確認加解密金鑰等機敏資料不得於影像錄影機軟韌體中被檢驗出來。

4.2.6. 影像錄影機之機敏性資料儲存安全測試

測試環境請參照圖 2。

4.2.6.1. 產品所儲存之敏感性資料須透過加密儲存測試

A 產品所儲存之敏感性資料須透過加密儲存

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.6.1. 產品所儲存之敏感性資料須透過加密儲存。

- 測試標準：

產品之敏感性資料須透過加密儲存，必須使用 FIPS 140-2 所核可之加密演算法[4]確保機密性。

- 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，並檢視其加密演算法是否符合 FIPS 140-2 所核可之演算法[3]。

4.2.6.2. 敏感資料的存放，須從正常作業環境中隔離測試

A 敏感資料的存放，須從正常作業環境中隔離

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.6.2. 敏感資料的存放，須從正常作業環境中隔離。

- 測試標準：

產品必須提供安全區域(Secure domain)功能。

- 測試方法：

廠商須提供測試指南，檢視其安全區域之功能是否存在。

4.2.7. 影像錄影機之網頁管理介面安全測試

測試環境請參照圖 2。

4.2.7.1. 網頁管理介面的網站安全機制測試

A 網頁管理介面的網站安全機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.7.1 網頁管理介面不得存在 OWASP top 10 [5]中所揭露之常見網站安全風險。

- 測試標準：

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。

- 測試方法：

開啟影像錄影機之網頁介面操控程式，由測試 PC 連線至影像錄影機進行測試，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. 影像錄影機之操控程式之 API 安全測試

測試環境請參照圖 2。

4.2.8.1. 操控程式之異常輸入檢測機制測試

A 操控程式之異常輸入檢測機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.8.1 操控程式之 API 必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

- 測試標準：

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。

- 測試方法：

由測試 PC 連線至影像錄影機，執行影像錄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。

4.2.9. 影像錄影機之系統日誌檔與警示測試

測試環境請參照圖 2。

4.2.9.1. 影像錄影機之系統日誌檔與警示測試

A 產品須提供安全事件日誌檔

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.9.1 產品須提供安全事件日誌檔。

- 測試標準：

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。

- 測試方法：

影像錄影機須提供登錄紀錄檔，並確認格式包含完整時間戳記與使用者身分。

B 安全事件日誌檔須具備權限控管機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.9.1 產品須提供安全事件日誌檔。

- 測試標準：

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。

- 測試方法：

影像錄影機之受測廠商需配合提供測試版本之更新檔案，測試人員根據產品之使用說明，並確認安全事件時，檢查系統警告通知，並具備權限控管機制。

C 安全事件日誌檔紀錄檔須具備顯示功能機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.9.1 產品須提供安全事件日誌檔。

- 測試標準：

產品之安全事件日誌檔紀錄檔須具備顯示功能機制。

- 測試方法：

影像錄影機須提供登錄紀錄檔之顯示方式，並可透過相關顯示畫面，確認其紀錄檔內容。

4.2.9.2. 產品須提供異常警示功能測試

A 產品須提供異常警示功能

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.9.2 產品須提供異常警示功能。

- 測試標準：

除達到產品須提供安全事件日誌檔要求外，產品須提供異常警示功能。

- 測試方法：

影像錄影機之受測廠商需配合提供測試版本之更新檔案，測試人員根據產品之使用說明，並確認用戶登入時，檢查系統警告通知。

B 應提供當日誌紀錄檔無法儲存時之系統警示

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.2.9.2 產品須提供異常警示功能。

- 測試標準：

除達到產品須提供安全事件日誌檔要求外，影像錄影機應提供當日誌紀錄檔無法儲存時之系統警示。

- 測試方法：

影像錄影機之受測廠商需配合提供測試版本之更新檔案，測試人員根據產品之使用說明，並確認儲存異常時，檢查系統警告通知。

4.3. 通訊安全測試

檢視影像錄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. 影像錄影機之敏感性資料傳輸安全測試

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 敏感資料於傳輸過程中須加密保護

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.1.1. 敏感資料於傳輸過程中須加密保護。

- 測試標準：

敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。

- 測試方法：

由測試 PC 連線至影像錄影機，開啟影像錄影機之操控程式，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，並檢視其加密演算法是否符合 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 敏感性資料傳輸須採用較嚴謹之加密演算法

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.1.2. 敏感性資料傳輸須採用較嚴謹之加密演算法，且須確保敏感性資料傳輸的完整性及不可否認性。

- 測試標準：

確保敏感資料之網路傳輸加密演算法必須支援 AES-256。

- 測試方法：

由測試 PC 連線至影像錄影機，開啟影像錄影機之操控程式，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，並檢視其加密演算法是否符合 FIPS 140-2 所核可之演算法[3]。

B 敏感性資料傳輸的完整性機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.1.2. 敏感性資料傳輸須採用較嚴謹之加密演算法，且須確保敏感性資料傳輸的完整性及不可否認性。

- 測試標準：

敏感性資料傳輸須支援數位簽章的功能。

- 測試方法：

廠商須提供測試指南，檢視其敏感性資料傳輸支援數位簽章之功能是否存在。

4.3.2. 通訊介面的安全設置測試

測試環境請參照圖 2。

4.3.2.1. 通訊介面的安全設置測試

A 影像錄影機之網路裝置資訊探詢功能

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.2.1 避免錯誤的通訊介面設置。

- 測試標準：

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，且預設須為關閉狀態。

- 測試方法：

由測試 PC 連線至影像錄影機，開啟影像錄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 影像錄影機之 WiFi 防護設置

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.2.1 避免錯誤的通訊介面設置。

- 測試標準：

產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。

- 測試方法：

由測試 PC 連線至影像錄影機，開啟影像錄影機之操控程式，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 無線網路傳輸設定

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.3.2.1 避免錯誤的通訊介面設置。

- 測試標準：

無線網路傳輸的安全機制必須支援 WPA2。

- 測試方法：

  由測試 PC 連線至影像錄影機，開啟影像錄影機之操控程式，確認其預設啟用之無線網路傳輸加密機制。

4.3.3. 影像錄影機之通訊協定安全測試

測試環境請參照圖 2。

4.3.3.1. 通訊協定異常輸入測試

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-影像錄影機」4.3.3.1 影像錄影機所使用之關鍵通訊協定，必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

- 測試標準：

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 A)因為任意或非法的輸入，造成產品異常行為的發生。

- 測試方法：

由測試 PC 連線至影像錄影機，執行影像錄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. 身分認證與授權測試

檢視影像錄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。

4.4.1. 影像錄影機認證機制安全測試

測試環境請參照圖 2。

4.4.1.1. 認證機制強度測試

A 認證機制強度

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.1.1 認證機制強度-初階。

- 測試標準：

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，例如認證機制加入隨機數(nonce)及時戳(timestamp)來抵禦重送攻擊等。

- 測試方法：

由測試PC連線至影像錄影機進行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影像錄影機，判斷認證結果是否成功。

4.4.1.2. 嚴謹之認證機制要求測試

A 嚴謹之認證機制要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.1.2 認證機制要求-高階。

- 測試標準：

產品之身分認證機制須採用公開金鑰基礎建設。

- 測試方法：

廠商須提供測試指南，檢視其公開金鑰基礎建設之功能是否存在。

B 認證機制須採用雙向認證

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.1.2 認證機制要求-高階。

- 測試標準：

  產品之身分認證機制須採用雙向認證機制。

- 測試方法：

  廠商須提供測試指南，檢視其認證機制的雙向認證之功能是否存在。

4.4.2. 影像錄影機認證資訊的傳輸保護測試

測試環境請參照圖 2。

4.4.2.1. 認證資訊於傳輸過程加密保護測試

A 認證資訊於傳輸過程中須加密保護

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.2.1. 認證資訊於傳輸過程中須加密保護。

- 測試標準：

認證資訊包括：帳密、金鑰、憑證等，其網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。

- 測試方法：

由測試 PC 連線至影像錄影機進行 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。

B 認證機制須採用公開金鑰基礎建設

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.2.1. 認證資訊於傳輸過程中須加密保護。

- 測試標準：

認證錯誤訊息不能顯露出合法使用者名稱。

- 測試方法：

由測試 PC 透過遠端管理介面連線至影像錄影機進行測試，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。

4.4.2.2. 認證資訊傳輸用較嚴謹之加密演算法測試

A 認證資訊傳輸須採用較嚴謹之加密演算法

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.2.2. 認證資訊傳輸須採用較嚴謹之加密演算法。

- 測試標準：

  除達到認證資訊於傳輸過程中須加密保護要求外，確保認證資訊之網路傳輸加密演算法預設必須採用 AES-256。

- 測試方法：

  由測試 PC 透過操控程式連線至影像錄影機進行測試，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。

B 認證資訊具備防竄改的檢查機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.4.2.2. 認證資訊傳輸須採用較嚴謹之加密演算法。

- 測試標準：

  除達到認證資訊於傳輸過程中須加密保護要求外，確保認證資訊之網路傳輸具備防竄改的檢查機制。

- 測試方法：

  廠商須提供測試指南，檢視其具備防竄改的檢查機制之功能是否存在，例如：在傳輸資料的 bitstream 裡放入 watermark、在 check checksum 加上由硬體產生的獨一 hashcode、數位憑證等，在程式碼編譯之前整合混淆、加密、防竄改等機制。

4.4.3. 影像錄影機密碼認證安全測試

測試環境請參照圖 2。

4.4.3.1. 影像錄影機密碼認證安全測試

A 密碼認證機制強度

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.3.1 密碼認證機制強度。

- 測試標準：

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至少須 15 個字母。

- 測試方法：

由測試 PC 連線至影像錄影機進行 API 授權密碼輸入，確保影像錄影機之密碼長度是否符合政府組態基準的最小密碼長度原則 CCE-33789-9。

B 預設密碼的唯一性

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.3.1 密碼認證機制強度。

- 測試標準：

廠商所生產之影像錄影機其預設密碼都須相異。

- 測試方法：

準備 2 台以上影像錄影機，由測試 PC 連線至影像錄影機進行 API 授權密碼輸入，比對每台影像錄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-影像錄影機」4.4.3.1 密碼認證機制強度。

- 測試標準：

首次登入產品必須強制更改預設密碼。

- 測試方法：

由測試 PC 連線至影像錄影機進行 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。

D 登入次數限制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.3.1 密碼認證機制強度。

- 測試標準：

產品在登入密碼的設計上必須有輸入頻率及次數的限制。

- 測試方法：

由測試 PC 連線至影像錄影機，進行 API 授權密碼輸入頻率與次數限制測試。

4.4.4. 影像錄影機之權限管控測試

測試環境請參照圖 2。

4.4.4.1. 影像錄影機之權限管控測試

A 影像錄影機資源的存取管控機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.4.4.1. 影像錄影機資源的存取，必須具備權限管控機制。

- 測試標準：

  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。

- 測試方法：

  由測試 PC 獲取影像錄影機之 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。

B 管理介面之權限管控機制

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.4.4.1. 影像錄影機資源的存取，必須具備權限管控機制。

- 測試標準：

  透過存取控制表(ACL)，得以新增/移除/中止使用者帳戶，或者是憑證的新增/廢止/更新，並對所有合法授權之帳戶強制實施最小權限(least privilege)原則，此外，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。

- 測試方法：

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

C 閒置時間之機制

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.4.1. 影像錄影機資源的存取，必須具備權限管控機制。

- 測試標準：

產品之授權行為，應存在閒置時限供使用者設定。

- 測試方法：

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

D 遠端管理介面閒置時間

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.4.4.1. 影像錄影機資源的存取，必須具備權限管控機制。

- 測試標準：

遠端通訊會議連線已經遺失或結束，須要求新的認證，且前一個會議連線所儲存的資料不得被新的會議連線所使用。

- 測試方法：

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

4.5. 隱私保護測試測試

檢視影像錄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，隱私資料泛指從影像錄影機端或操作界面端所收集到的影音或使用者資訊。

4.5.1. 隱私資料的存取保護測試

測試環境請參照圖 2。

4.5.1.1. 隱私資料的存取保護測試

A 隱私資料的權限管控

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.5.1.1 隱私資料的權限管控。

- 測試標準：

產品所儲存的隱私資料，只有已被授權的個體才可以存取。

- 測試方法：

開啟影像錄影機之服務，登入後查詢身分類型與權限是否與廠商自我宣告相符。

B 隱私資料的刪除權限管控

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.5.1.1 隱私資料的權限管控。

- 測試標準：

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。

- 測試方法：

檢視影像錄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. 隱私資料傳輸機密性之基本要求測試

A 隱私資料傳輸機密性之基本要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.5.2.1 隱私資料傳輸機密性之基本要求。

- 測試標準：

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，須使用 FIPS 140-2 所核可之加密演算法[4]。

- 測試方法：

開啟影像錄影機之服務，由測試 PC 連線至影像錄影機進行測試，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。

4.5.2.2. 隱私資料傳輸機密性之進階要求測試

A 隱私資料傳輸機密性之進階要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.5.2.2 隱私資料傳輸機密性之進階要求。

- 測試標準：

隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[4]。

- 測試方法：

開啟影像錄影機之服務，由測試 PC 連線至影像錄影機進行封包側錄，同時分析封包是否加密，並檢視其加密演算法。

4.5.2.3. 隱私資料傳輸機密性之高階要求測試

A 隱私資料傳輸機密性之高階要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.5.2.3 隱私資料傳輸機密性之高階要求。

- 測試標準：

確保隱私資料之網路傳輸加密演算法預設必須採用 AES-256。

- 測試方法：

  開啟影像錄影機之服務，由測試 PC 連線至影像錄影機進行封包側錄，同時分析封包是否加密，並檢視其加密演算法。

4.6. 應用程式安全測試

檢視影像錄影機之實體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。在本測試規範中，實體安全泛指從影像錄影機端或操作界面端所收集到的使用者資訊。

4.6.1. 應用程式的程式安全測試

測試環境請參照圖 2。

4.6.1.1. 應用程式的程式安全測試-初階

A 應用程式的初次存取之要求

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

  應用程式在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。

- 測試方法：

  檢查受測軟體是否提供使用者登入確認並取得授權之機制。

B 應用程式的資料來源之要求

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

  應用程式應確認資料來源的安全。

- 測試方法：

  受測軟體透過網路傳輸資料至遠端伺服器，檢查伺服器端提供給受測軟體之憑證資料是否過期。

C 應用程式應可識別其發行資訊

- 測試依據：

  「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式應可識別其發行資訊，以確保使用者瞭解其來源。

- 測試方法：

檢查受測軟體或廠商自我宣告表是否提供受測軟體的發行商和版本資訊。

D 應用程式的執行行為之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式所執行的行為，應取得使用者同意，並與其宣告之內容相符。

- 測試方法：

執行及操作受測軟體，並列舉受測軟體所使用的功能及存取權限。比對列舉之內容是否與廠商自我宣告之內容相符。

E 應用程式的網路連接埠之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路埠」相符。

- 測試方法：

執行受測軟體，並取得受測軟體開啟之網路埠號。檢查取得之網路埠號是否與廠商自我宣告表相符。

F 應用程式的引用之第三方函式庫之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

廠商需於文件中標明所使用之應用程式及引用之第三方函式庫。

- 測試方法：

依據廠商所提供之技術文件，須標明所使用之應用程式及引用之第三方函式庫。

G 應用程式的資訊安全漏洞之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式所引用之第三方函式庫，不得存在已揭露之重大資訊安全漏洞。

- 測試方法：

由測試 PC 連線至影像錄影機，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。

H 應用程式的更新機制之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式必須具備應用程式更新機制。

- 測試方法：

受測廠商需配合提供測試版本之應用程式更新檔案，測試人員根據產品之使用說明，進行應用程式更新操作，確認應用程式更新功能。

I 應用程式的敏感性資料之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式之敏感性資料不得出現於裝置應用程式程式碼中。

- 測試方法：

影像錄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。

4.6.1.2. 應用程式的程式安全測試-中階

A 應用程式的發送訊息之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式不應在未取得使用者同意之情況下，於背景發送訊息。

- 測試方法：

透過比對訊息資料檔案之檔案時間戳記等方式，檢查是否有背景發送訊息等紀錄。

B 應用程式的內建軟體之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式於使用者設定關閉時，應停止該內建軟體所有相關程序。

- 測試方法：

關閉執行之受測軟體，並再次以管理者權限取得所有執行中的應用程式清單，檢查清單是否相同。

C 應用程式的源碼掃描之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式可能有程式設計上缺陷，內建應用程式應經過源碼掃描。

- 測試方法：

廠商須提供測試指南，檢視其源碼掃描之功能是否存在。

4.6.1.3. 應用程式的程式安全測試-高階

A 應用程式的處理惡意字串輸入之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式應具備惡意字串輸入時的處理能力。

- 測試方法：

執行受測應用程式，並輸入資料隱碼攻擊字串，檢查之受測軟體是否執行隱碼攻擊字

串。

B 應用程式的回報安全性之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式應提供回報安全性問題之管道。

- 測試方法：

應用程式應提供回報安全性問題之管道，包括：E-Mail 通知、訊息推播等。

C 應用程式的具備數位簽章之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.1.1 應用程式的程式安全之基本要求。

- 測試標準：

應用程式可能被竄改，內建應用程式須具備數位簽章。

- 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。

4.6.2. 應用程式的系統安全測試

測試環境請參照圖 2。

4.6.2.1. 應用程式的系統安全測試-初階

A 應用程式的系統安全之基本要求]

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式所執行的程式行為，應取得使用者同意，必要時並提供風險提示。

- 測試方法：

透過受測系統內建作業系統更新功能執行作業系統更新，取得作業系統更新之連線目的地位址，檢查目的地位址是否與廠商自我宣告之內容相符。

B 應用程式的下載或安裝更新作業之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。

- 測試方法：

檢查受測系統或官網是否提供作業系統更新資訊，並告知使用者更新之內容或未更新可能造成安全風險之資訊。

C 應用程式的安全的身分辨識之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式應提供安全的身分辨識及保護機制。

- 測試方法：

應用程式應提供安全的身分辨識及保護機制,須包含所有資料在使用、儲存及傳輸時，皆可被安全保護。

4.6.2.2. 應用程式的系統安全測試-中階

A 應用程式的系統安全之進階要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。

- 測試方法：

開啟受測系統之螢幕鎖定設定功能介面，並設定螢幕鎖定方式及解鎖資料。鎖定受測系統(包含關閉螢幕及關閉受測系統),喚醒受測系統(包含開啟螢幕及開啟受測系統)，並操作解鎖方式，檢查是否可以所設定的解鎖資料喚醒受測系統。

B 應用程式的強制鎖定保護機制之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。

- 測試方法：

開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料，鎖定受測系統，喚醒受測系統，並重複輸入數次錯誤的解鎖資料，檢查受測系統是否顯示強制鎖定的訊息。

C 應用程式的螢幕鎖定解鎖資料之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式之螢幕鎖定解鎖資料，不應以明文方式儲存，以避免遭未經授權的使用。

- 測試方法：

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至少須 15 個字母。

D 應用程式的密碼強度之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式的密碼強度之要求。

- 測試方法：

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至少須 15 個字母。

E 應用程式的回報安全性問題之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式應提供回報安全性問題之管道。

- 測試方法：

應用程式應提供回報安全性問題之管道，包括：E-Mail 通知、訊息推播等。

4.6.2.3. 應用程式的系統安全測試-高階

A 應用程式的系統安全之高階要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。

- 測試方法：

依書面資料審查是否具備此功能。當無充分資料顯示具備此功能時，則請申請者做功能示範。

B 應用程式的自我測試機制之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。

- 測試方法：

依書面資料審查是否具備此功能。當無充分資料顯示具備此功能時，則請申請者做功能示範。

C 應用程式的執行安全區域之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式須提供讓安全應用程式執行之安全區域。

- 測試方法：

廠商須提供測試指南，檢視其安全區域之功能是否存在。

D 應用程式的異常操作之要求

- 測試依據：

「影像監控系統資安標準草案-影像錄影機」4.6.2.1 應用程式的系統安全之基本要求。

- 測試標準：

應用程式須具備應用程式異常操作之監控及防護。

- 測試方法：

應用程式須具備未授權之應用程式不得被啟動，遭竄改之應用程式不得被啟動。

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)
影像錄影機之通訊協定

- 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。

- 乙太網路點對點通訊協定(Point-to-Point Protocol Over Ethernet, PPPoE)：

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。

- 動態功能變數名稱服務(Dynamic Domain Name Server, DDNS)：

定義在 RFC 2136 規範中，是一種自動更新名稱伺服器（Name server）內容的技術，提供浮動 IP 或非固定(DHCP)IP 的主機可以動態 IP 地址映射之功能。

附錄 D
(參考)
測試項目與資安要求對應總表

- 實體安全技術要求

測試項目	分級	技術要求
4.1.1.1A 除錯和測試功能必須關閉	1~3 級	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必須關閉、外接儲存媒體用。
4.1.1.1B 沒使用到的實體埠可以被關閉	1~3 級	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。
4.1.1.1C 外接實體埠的操作機制	1~3 級	外接實體埠的插拔操作須提供日誌記錄
4.1.1.2A 產品的外觀不得有實體埠存在	1~3 級	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。
4.1.2.1A 異常時須提供警示機制	2~3 級	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。
4.1.2.1B 實體設計之自動化硬體偵測機制	2~3 級	實體設計之自動化硬體偵測機制，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。
4.1.3.1A 產品之外殼不能被輕易拆除或破壞	2~3 級	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。
4.1.3.2A 晶片與功能編號不可存在於電路板	3 級	除達到產品之外殼不能被輕易拆除或破壞要求外，晶片與功能編號不可存在於電路板。
4.1.3.2B 不得存在可輕易一鍵還原回預設密碼的設計	3 級	除達到產品之外殼不能被輕易拆除或破壞要求外，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。

4.1.3.2C 電路板上用於除錯或測試用途之界面機制	3 級	除達到產品之外殼不能被輕易拆除或破壞要求外，電路板上用於除錯或測試用途之界面，必須移除。
4.1.4.1A 產品須提供安全啟動(secure boot)功能	3 級	確保產品於開機時，避免未經授權的軟韌體、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。

- 系統安全技術要求

測試項目	分級	技術要求
4.2.1.1A 作業系統之 CVSS v3 評分為 10 分之安全機制	1~3 級	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。
4.2.1.2A 作業系統之 CVSS v3 評分為 9 分之安全機制	2~3 級	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。
4.2.1.3A 作業系統之 CVSS v3 評分為 7 分之安全機制	3 級	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。
4.2.2.1A 影像錄影機僅開啟必要之網路服務	1~3 級	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。
4.2.3.1A 網路服務在 CVSS v3 評分為	1~3 級	受測產品之網路服務，不得存在國家弱

10 分之安全機制		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。
4.2.3.2A 網路服務在 CVSS v3 評分為 9 分之安全機制	2~3 級	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。
4.2.3.3A 網路服務在 CVSS v3 評分為 7 分之安全機制	3 級	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。
4.2.4.1A 軟韌體須具備更新機制	1~3 級	軟韌體須具備更新機制。
4.2.4.1B 產品支援離線手動更新	1~3 級	產品支援離線手動更新，則更新檔案得確保機密性。
4.2.4.1C 產品支援線上自動更新	1~3 級	產品支援線上自動更新，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。
4.2.4.1D 加密演算法須採用 FIPS 140-2	1~3 級	使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[4]。
4.2.4.2A 軟韌體更新機制須一律採用線上更新	2~3 級	除達到軟韌體更新機密性保證要求外，軟韌體更新機制須一律採用線上更新。
4.2.4.2B 軟韌體更新必須透過數位簽章機制	2~3 級	除達到韌體更新機密性保證要求外，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。
4.2.5.1A 產品之敏感性資料在裝置軟/韌體程式碼的機制	1~3 級	產品之帳號、密碼、身分認證因子或加解密用之金鑰，不得出現於軟/韌體之程式碼與安裝檔內其他檔案中。
4.2.5.2A 敏感性資料在裝置軟/韌體程式碼的機制	3 級	敏感性資料不得出現於裝置軟/韌體程式碼中。
4.2.5.2B 產品的軟/韌體之程式存在	3 級	產品的軟/韌體不得存在 CWE/SANS

安全性弱點的機制		TOP 25 Most Dangerous Software Errors [11]。
4.2.6.1A 產品所儲存之敏感性資料須透過加密儲存	1~3 級	產品之敏感性資料須透過加密儲存，必須使用 FIPS 140-2 所核可之加密演算法[4]確保機密性。
4.2.6.2A 敏感資料的存放，須從正常作業環境中隔離	3 級	產品必須提供安全區域(Secure domain)功能。
4.2.7.1A 網頁管理介面的網站安全機制	1~3 級	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。
4.2.8.1A 操控程式之異常輸入檢測機制	3 級	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。
4.2.9.1A 產品須提供安全事件日誌檔	1~3 級	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。
4.2.9.1B 安全事件日誌檔須具備權限控管機制	1~3 級	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。
4.2.9.1C 安全事件日誌檔紀錄檔須具備顯示功能機制	1~3 級	產品之安全事件日誌檔紀錄檔須具備顯示功能機制。
4.2.9.2A 產品須提供異常警示功能	2~3 級	除達到產品須提供安全事件日誌檔要求外，產品須提供異常警示功能。
4.2.9.2B 應提供當日誌紀錄檔無法儲存時之系統警示	2~3 級	除達到產品須提供安全事件日誌檔要求外，影像錄影機應提供當日誌紀錄檔無法儲存時之系統警示。

- 通訊安全技術要求

測試項目	分級	技術要求
4.3.1.1A 敏感資料於傳輸過程中須加密保護	1~3 級	敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。

4.3.1.2A 敏感性資料傳輸須採用較嚴謹之加密演算法	3 級	確保敏感資料之網路傳輸加密演算法必須支援 AES-256。
4.3.1.2B 敏感性資料傳輸的完整性機制	3 級	敏感性資料傳輸須支援數位簽章的功能。
4.3.2.1A 影像錄影機之網路裝置資訊探詢功能	1~3 級	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，且預設須為關閉狀態。
4.3.2.1B 影像錄影機之 WiFi 防護設置	1~3 級	產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。
4.3.2.1C 無線網路傳輸設定	1~3 級	無線網路傳輸的安全機制必須支援 WPA2。
4.3.3.1A 通訊協定異常輸入檢測	2~3 級	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 A)因為任意或非法的輸入，造成產品異常行為的發生。

- 身分認證機制安全技術要求

測試項目	分級	技術要求
4.4.1.1A 認證機制強度	1~3 級	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，例如認證機制加入隨機數(nonce)及時戳(timestamp)來抵禦重送攻擊等。
4.4.1.2A 嚴謹之認證機制要求	3 級	產品之身分認證機制須採用公開金鑰基礎建設。
4.4.1.2B 認證機制須採用雙向認證	3 級	產品之身分認證機制須採用雙向認證機制。
4.4.2.1A 認證資訊於傳輸過程中須加密保護	1~3 級	認證資訊包括：帳密、金鑰、憑證等，其網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。
4.4.2.1B 認證機制須採用公開金鑰基礎建設	1~3 級	認證錯誤訊息不能顯露出合法使用者名稱。
4.4.2.2A 認證資訊傳輸須採用較嚴謹之加密演算法	3 級	除達到認證資訊於傳輸過程中須加密保護要求外，確保認證資訊之網路傳輸

		加密演算法預設必須採用 AES-256。
4.4.2.2B 認證資訊具備防竄改的檢查機制	3 級	除達到認證資訊於傳輸過程中須加密保護要求外，確保認證資訊之網路傳輸具備防竄改的檢查機制。
4.4.3.1A 密碼認證機制強度	1~3 級	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至少須 15 個字母。
4.4.3.1B 預設密碼的唯一性	1~3 級	廠商所生產之影像錄影機其預設密碼都須相異。
4.4.3.1C 密碼變更機制	1~3 級	首次登入產品必須強制更改預設密碼。
4.4.3.1D 登入次數限制	1~3 級	產品在登入密碼的設計上必須有輸入頻率及次數的限制。
4.4.4.1A 影像錄影機資源的存取管控機制	1~3 級	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。
4.4.4.1B 管理介面之權限管控機制	1~3 級	透過存取控制表(ACL)，得以新增/移除/中止使用者帳戶，或者是憑證的新增/廢止/更新，並對所有合法授權之帳戶強制實施最小權限(least privilege)原則，此外，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。
4.4.4.1C 閒置時間之機制	1~3 級	產品之授權行為，應存在閒置時限供使用者設定。
4.4.4.1D 遠端管理介面閒置時間	1~3 級	遠端通訊會議連線已經遺失或結束，須要求新的認證，且前一個會議連線所儲存的資料不得被新的會議連線所使用。

- 隱私保護技術要求

測試項目	分級	技術要求
4.5.1.1A 隱私資料的權限管控	1~3 級	產品所儲存的隱私資料，只有已被授權的個體才可以存取。

4.5.1.1B 隱私資料的刪除權限管控	1~3 級	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。
4.5.2.1A 隱私資料傳輸機密性之基本要求	1~3 級	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，須使用 FIPS 140-2 所核可之加密演算法[4]。
4.5.2.2A 隱私資料傳輸機密性之進階要求	2~3 級	隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[4]。
4.5.2.3A 隱私資料傳輸機密性之高階要求	3 級	確保隱私資料之網路傳輸加密演算法預設必須採用 AES-256。

- 應用程式安全技術要求

測試項目	分級	技術要求
4.6.1.1A 應用程式的初次存取之要求	1~3 級	應用程式在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
4.6.1.1B 應用程式的資料來源之要求	1~3 級	應用程式應確認資料來源的安全。
4.6.1.1C 應用程式應可識別其發行資訊	1~3 級	應用程式應可識別其發行資訊，以確保使用者瞭解其來源。
4.6.1.1D 應用程式的執行行為之要求。	1~3 級	應用程式所執行的行為，應取得使用者同意，並與其宣告之內容相符。
4.6.1.1E 應用程式的網路連接埠之要求	1~3 級	應用程式所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路埠」相符。
4.6.1.1F 應用程式的引用之第三方函式庫之要求	1~3 級	廠商需於文件中標明所使用之應用程式及引用之第三方函式庫。
4.6.1.1G 應用程式的資訊安全漏洞之要求	1~3 級	應用程式所引用之第三方函式庫，不得存在已揭露之重大資訊安全漏洞。
4.6.1.1H 應用程式的更新機制之要求	1~3 級	應用程式必須具備應用程式更新機制。
4.6.1.1I 應用程式的敏感性資料之要求	1~3 級	應用程式之敏感性資料不得出現於裝置應用程式程式碼中。
4.6.1.2A 應用程式的發送簡訊之要求	2~3 級	應用程式不應在未取得使用者同意之情況下，於背景發送簡訊。

4.6.1.2B 應用程式的內建軟體之要求	2~3 級	應用程式於使用者設定關閉時，應停止該內建軟體所有相關程序。
4.6.1.2C 應用程式的源碼掃描之要求	2~3 級	應用程式可能有程式設計上缺陷，內建應用程式應經過源碼掃描。
4.6.1.3A 應用程式的處理惡意字串輸入之要求	3 級	應用程式應具備惡意字串輸入時的處理能力。
4.6.1.3B 應用程式的回報安全性之要求	3 級	應用程式應提供回報安全性問題之管道。
4.6.1.3C 應用程式的具備數位簽章之要求	3 級	應用程式可能被竄改，內建應用程式須具備數位簽章。
4.6.2.1A 應用程式的系統安全之基本要求	1~3 級	應用程式所執行的程式行為，應取得使用者同意，必要時並提供風險提示。
4.6.2.1B 應用程式的下載或安裝更新作業之要求	1~3 級	應用程式於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。
4.6.2.1C 應用程式的安全的身分辨識之要求	1~3 級	應用程式應提供安全的身分辨識及保護機制。
4.6.2.2A 應用程式的系統安全之進階要求	2~3 級	應用程式應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
4.6.2.2B 應用程式的強制鎖定保護機制之要求	2~3 級	應用程式應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。
4.6.2.2C 應用程式的螢幕鎖定解鎖資料之要求	2~3 級	應用程式之螢幕鎖定解鎖資料，不應以明文方式儲存，以避免遭未經授權的使用。
4.6.2.2D 應用程式的密碼強度之要求	2~3 級	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至少須 15 個字母。
4.6.2.2E 應用程式的回報安全性問題之要求	2~3 級	應用程式應提供回報安全性問題之管道。
4.6.2.3A 應用程式的系統安全之高階要求。	3 級	應用程式應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。
4.6.2.3B 應用程式的自我測試機制之要求	3 級	開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。
4.6.2.3C 應用程式的執行安全區域之	3 級	應用程式須提供讓安全應用程式執行

要求		之安全區域。
4.6.2.3D 應用程式的異常操作之要求	3 級	應用程式須具備應用程式異常操作之監控及防護。

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>受測物軟/韌體版本</td><td>是否開啟網路埠</td><td>是否提供 API</td><td>是否支援軟韌體更新</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="2">1</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">☐ 否
☐ 是
固定埠號(服務)：
_____
_____
動態埠號範圍(服務)：
_____
_____</td><td rowspan="2">☐ 否
☐ 是</td><td rowspan="2">☐ 否
☐ 是,線上更新
☐ 是,手動更新</td><td rowspan="2">☐ 否
☐ 是</td><td></td></tr>
<tr><td>AUTH-23
遠端管理介面帳號權限說明</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	軟韌體版本	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	
影像錄影機作業系統安全	1. 影像錄影機之作業系統，不得存在 CVSS 評分為最高風險 10 分之資安漏洞					
	2. 影像錄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. 影像錄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					
影像錄影機之軟韌體程式安全	4. 影像錄影機之更新機制應正常運行					
	5. 影像錄影機之軟韌體線上更新機制，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，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。					
	6. 影像錄影機之軟韌體手動更新機制，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]。					
影像錄影機之機敏性資料儲存安全	7. 影像錄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. 影像錄影機系統檔案內之使用者帳號與密碼必須經過加密儲存，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]，以確保演算法之強度。					
影像錄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**
		完全實	部份實	尚未實	不適用	

		施	施	施		
影像錄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，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]					
通訊介面的安全設置	2. 影像錄影機只要有提供 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. 影像錄影機只要具備 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. 影像錄影機之無線網路預設加密模式，須符合 FIPS 140-2 所核可之加密演算法[3]					
影像錄影機之通訊協定安全	5. 影像錄影機之通訊協定，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**				**註記**
		完全實施	部份實施	尚未實施	不適用	
影像錄影機認證機制安全	1. 影像錄影機之 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影像錄影機時，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. 透過操控程式存取影像錄影機時，影像錄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，且加密演算法須符合 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，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。					
	6. 操控程式與影像錄影機之間身分認證資訊的網路傳輸必須經過加密保護，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。					

影像錄影機密碼認證安全	7. 影像錄影機之 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. 影像錄影機之 API 呼叫之預設密碼都須相異。					
	9. 影像錄影機之 API 呼叫，首次授權成功必須強制更改預設密碼。					
	10. 影像錄影機 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. 影像錄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. 廠商所出產之影像錄影機其遠端管理介面之預設密碼都須相異。					
	13. 影像錄影機之遠端管理介面，首次登入必須強制更改預設密碼。					
	14. 影像錄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。					
影像錄影機遠端管理介面之權限管控	19. 影像錄影機 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」。					
	20. 影像錄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. 影像錄影機之操控程式，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. 影像錄影機在執行監控時，應點亮狀態指示燈。若影像錄影機沒有指示燈，則本測試項目為不通過。					
隱私資料的存取保護	26. 影像錄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. 影像錄影機所儲存的隱私資料應經過加密處理，且加密演算法須符合 FIPS 140-2 所核可之演算法[3]。					
	28. 影像錄影機之隱私資料刪除功能。					
隱私資料的傳輸保護	29. 影像錄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)
影像錄影機資安測試申請表

<table>
<tr><td colspan="7">影像錄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>(請蓋公司章)</td></tr>
<tr><td colspan="5">公司地址：</td><td rowspan="5"></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="6">單位名稱：</td></tr>
<tr><td colspan="6">聯絡人：</td></tr>
<tr><td colspan="6">電話：　　傳真：</td></tr>
<tr><td colspan="6">Email：</td></tr>
<tr><td rowspan="4">送測設備</td><td>模組型式</td><td colspan="5"></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>備註</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">審查報告</td><td>文件編號</td><td colspan="2">文件名稱</td><td>數量</td><td colspan="2">備註</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2">申請測試內容</td><td colspan="2">☐新申請案件</td><td colspan="3">☐補申請案件</td></tr>
<tr><td colspan="7">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), 影像監控系統影像錄影機資安標準草案