影像監控系統資安標準之測試規範

草案–影像錄影機

（V0.1.7）

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

2017-10-22

文件修改記錄

版本	修改日期	修改人	修改依據	修改原因及說明
V0.1.1	2017/9/5	陳聰杰	無	新建立
V0.1.1	2017/9/14	陳聰杰	依據2017/9/12專家會議之專家意見彙總表	1. 圖 1 更新。 2. 2.15 節更新為安全隧道。 3. 2.18 節內容更新為預設密碼。 4. 表 1 的級等內容調整。 5. 3.x 節的「測試標準」更新為「測試細則」。 6. 刪除 4.3.1.2 節的初階、進階及高階字眼（同 4.4.1.1、4.4.1.2 及 4.5.2.x 等各章節）。 7. 全文「安全保證等級」改為「資訊安全等級」。 8. 在實體安全增加實體儲存安全。 9. 在系統安全增加系統儲存安全。 10. 在身分認證增加實體設備的身分驗證。 11. 新增章節： 2.19 出廠預載軟體 4.1.5 實體儲存安全 4.2.10 系統儲存安全 4.4.4 實體設備的身份驗證測試
V0.1.2	2017/9/21	陳聰杰	依據編審與專家會議討論內容修改	1. 修正前言與引言。 2. 2.18 節更新為裝置認證。 3. 修正 3. 安全等級說明。 4. 修正 4.1.5 節條文。 5. 合併 4.2.1 節和 4.2.3 節作業系統安全。 6. 修正 4.2.9 節。 7. 修正 4.4.1 節。 8. 刪除 4.5 隱私保護技術要求。 9. 修正 4.5 應用程式安全技術要求。 10. 修正各測試項目，調整如下： • 測試依據 • 測試標準 • 測試步驟 • 通過準則
V0.1.3	2017/9/27	陳聰杰	依據2017/9/22編審會議討論內容	1. 調整表 1~4。 2. 刪除 2.4 節已知安全性弱點。 3. 修正 2.20, 2.21 及 2.22 節。 4. 修正 3 節。

			修改	5. 修正 4.1.1 節。 6. 修正 4.1.2 節。 7. 修正 4.1.3 節。 8. 修正 4.1.5 節。 9. 修正 4.2.9 節。 10. 刪除 4.2.9.3(b)節。 11. 修正 4.3.2.1(d)節通過準則內容修改。 12. 刪除 4.2.9.3(b)節。 13. 修正 4.5.1 節。 14. 與「影像監控系統資安標準草案-影像錄影機」格式調整一致。 15. 修改安全通道由 TLS1.1 改成 TLS1.2。
V0.1.4	2017/9/30	陳聰杰	依據 2017/9/29 網路攝影機公開說明會議討論內容修改	1. 前言內容調整。 2. 修正 5.1.1,5.1.2 及 5.1.3 節實體安全測試之內容。 3. 修正 5.2.3 節更新安全測試之內容。 4. 修正 5.2.4 節韌體程式安全測試之內容。 5. 修正 5.2.7 節操控程式之 API 安全測試之內容。 6. 修正 5.2.8 節系統日誌檔與警示測試之內容。 7. 修正 5.3.1 節敏感性資料傳輸安全測試之內容。 8. 修正 5.4.1 節認證機制安全測試之內容。 9. 修正 5.5.1 節應用程式的程式安全測試之內容。
V0.1.5	2017/10/13	陳聰杰	依據編審與專家會議討論內容修改	1. 修正 3.1 節。 2. 調整 4 節的安全等級至 4.6 節。 3. 修正 4.2.1.1(a)。 4. 修正 4.2.1.2(a)/(c)。 5. 刪除 4.2.1.3(a)。 6. 刪除 4.2.3.2(a)。 7. 修正測試項目之條文為「產品」更改為「受測物」。 8. 修正測試項目之條文為「身分認證」更改為「身分鑑別」。 9. 新增附錄 D 測試項目分級。
V0.1.6	2017/10/19	陳聰杰	依據 2017/10/17 編審會議	1. 修正測試項目之條文內容「影像錄影機」改回「受測物」。 2. 新增 4.3.4 影像傳輸安全。

			討論內容修改	3. 新增 4.3.4.1(a),4.3.4.1(b),4.3.4.1(c)。 4. 修改 4.1.5.3(a)。 5. 修改 4.2.3.1(d)併入 4.2.3.1(c)。 6. 修改 4.2.9 系統備份安全。 7. 修改 4.2.9.2(b)至 4.2.9.3(b) 防竄改,等級調為 3 級。 8. 修改 4.3.1.2(a) 安全通道。 9. 修改 4.4.1.2(c)至 4.4.1.1(c) 憑證鑑別,等級調為 1 級。 10. 修改 4.4.2 通行鑑別機制。 11. 刪除 4.1.2.1(a)。 12. 刪除 4.2.3.2(a) 在測試標準已刪除。 13. 刪除 4.2.6.2(a)。 14. 刪除 4.2.7.2(a)。 15. 刪除 4.2.8.1(d)及(e)。 16. 刪除 4.2.8.2(a) 標準規範已刪除。
V0.1.7	2017/10/22	陳聰杰	依據 2017/10/19 專家會議討論內容修改	1. 調整 4.6 節的測試項目分級至 4 節。 2. 調整原 4 節資安測試規範至 5 節。 3. 修正 5.1.5.3(c)。 4. 刪除 5.2.4.2(a)。 5. 刪除 5.5.1.3(b)。 6. 全文「密碼」更新為「通行碼」。

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，使使用本標準前應適當建立影像監控系統之影像錄影機相關網路安全與正常運作，並且遵守相關法規之規定。

本標準之部分內容，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

影像錄影機，係包含兩類，（1）藉由前端攝影機的影像擷取處理，透過有線或無線訊號傳輸方式傳至影像錄影機，於影像錄影機進行影像編碼；（2）藉由網路整合型之前端攝影機，其功能整合影像編碼，並透過有線或無線訊號傳輸方式傳至影像錄影機。兩者皆可由影像錄影機集中式或分散式管理與儲存，並可透過影像錄影機的軟硬體解碼器將影像呈現檢視畫面，並融入人機互動之介面。

鑑於近幾年影像錄影機資安事件頻傳，經濟部工業局為全面改善影像錄影機資安品質，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。

「影像監控系統資安標準之測試規範草案-影像錄影機」（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「影像監控系統資安標準草案-影像錄影機」[1]所訂定，俾利影像錄影機製造商、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影像錄影機資安檢測之測試項目、測試標準、測試步驟及通過準則等事項。

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 所示。

本標準為確保影像錄影機資安，訂定其受測物之安全技術要求，擬依五大安全構面定義之，包括：實體安全、系統安全、通訊安全、身分鑑別與授權機制安全及應用程式安全。

其適用範圍包含影像錄影機之本實體，而前端攝影機與網路連接儲存裝置並不適用本規範。其中，影像錄影機之輸入介面包含有線與無線之影像及控制輸入信號，而輸出介面包含有線與無線之儲存與影像輸出信號，並且可以透過網路的方式進行管理操控。

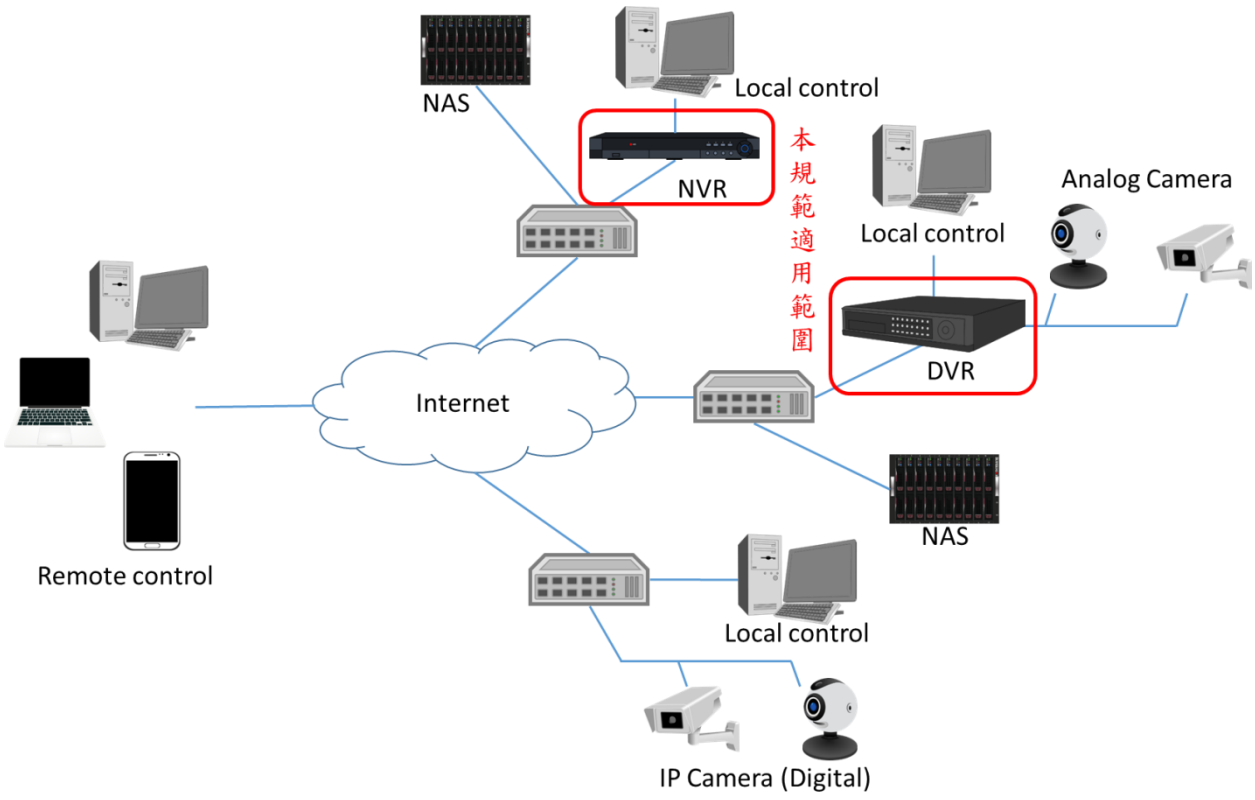

圖1. 適用範圍示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本（含補充增修）適用之。

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 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。

（a）數位影像錄影機（DVR）：為一種封閉式架構之影像儲存管理設備，支援 NTSC、PAL 等影像格式，並支援有線（例如：同軸電纜）之前端攝影機，其影像儲存支援內建儲存裝置。

（b）網路影像錄影機（NVR）：為一種開放式架構之影像儲存管理設備，支援 H.264、AVI 等影像格式，並支援有線（例如：網路線）及無線（例如：WiFi）之前端攝影機，其影像儲存支援本地端或遠端之儲存裝置。

3.2 資訊安全弱點（Security Vulnerability）

指影像錄影機安全方面之缺陷，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）

係美國國土安全部贊助之弱點管理計畫，該計畫針對每一弱點項目賦予其全球認可唯一共通編號[13]。

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）[2]提供的國家弱點資料庫[3]，負責 3.3 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）

一套企業資訊系統安全性評鑑標準，漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度，都被列入評比。評比從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險[6]。

3.6 嚴重性等級（Severity Rating）

係指漏洞評鑑系統之評比分數皆有其對應之嚴重性等級，分別是 0 分為無（None）嚴重性、0.1~3.9 分為低（Low）嚴重性、4.0~6.9 分為中（Medium）嚴重性、7.0~8.9 分為高（High）嚴重性及 9.0~10.0 分為重大（Critical）嚴重性。

3.7 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、通行碼或地理位置等。

3.8 個人資料（Personally Identifiable Information）

依「個人資料保護法」[7]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。

3.9 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影像錄影機所錄製之影像及用戶資訊。

3.10 操控程式（Control Program）

係指用於控制影像錄影機動態或瀏覽監控內容之應用程式，包括行動版及電腦版應用程式。

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

係指透過網路自遠端裝置取得影像錄影機作業系統的操控權，如：

（a）於遠端使用操控程式或透過網頁管理介面執行產品維護、存取影像錄影機資源、監看畫面或操控鏡頭。

（b）於遠端使用或透過網路管理介面進行系統設定，例如：網際協定位址（IP Address）。

3.12 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具備該介面操控端應用程式呼叫，用戶透過應用程式介面實現影像錄影機相關操作應用程式，例如：系統資訊擷取、監控影像擷取等。

3.13 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。

3.14 加密（Encryption）

係指利用數學演算法處理電子資料，使資料不會以原來的形式呈現，達到保密的目的，並且可透過解密方式取得加密資料原文內容。

3.15 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。

3.16 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（Secure Spckets Layer，SSL）和傳輸層安全性（Transport Layer Security，TLS）。

3.17 安全區域（Secure Domain，TrustZone）

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，並供敏感性資料保存用。

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

規範資通訊終端設備（例如：個人電腦）的一致性安全設定（例如：通行碼長度、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。

3.19 通行碼（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。

3.20 預設通行碼（Default Password）

係指影像錄影機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預設通關密語。

3.21 裝置鑑別（Device Authentication）

係指影像錄影機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通行碼，或者是相連裝置之數位憑證來確認裝置之身分。

3.22 安全事件日誌（Security Event Log）

係指記錄每個稽核規則所定義的活動，用以察覺威脅或攻擊事件的發生，本文之安全事件即是登入系統的嘗試。

3.23 通用隨插即用通訊協定（Universal Plug and Play，UPnP）

在區域網路環境下（例如：家庭網路或公司網路等），使各種裝置能夠直接互相連線，同時自行設定組態以進行資料分享。

3.24 簡單網路管理協定（Simple Network Management Protocol，SNMP）

SNMP 將網路設備區分為管理器（Manager）及代理器（Agent）2 個角色，代理器以變數呈現本身所收集之網域的網路狀態資料，而管理器透過 GET 等指令收集代理器所傳回的資訊。

3.25 零配置通訊協定（Bonjour）

在區域網路環境下（例如：家庭網路或公司網路等），提供自動搜尋網路設備的服務。Bonjour 使用 IP 通訊協定，在無須設定 IP 位址或 DNS 伺服器的情況下，設備即可自行發現彼此。

3.26 Wi-Fi 保護設置（Wi-Fi Protected Setup，WPS）

Wi- Fi 聯盟推出的一個通訊協定，得以簡化使用者在無線安全性方面的設定，一旦無線接入點進入 WPS 模式之後，使用者僅需要在用戶端（Client）無須任何繁複的安全性設定，按下按鈕便即可連線。

3.27 Wi-Fi 保護存取（Wi-Fi Protected Access，WPA）

用以保護網路安全之加密方式，分成 WPA 與 WPA2 兩個標準，基於改善有線等效加密（Wired Equivalent Privacy，WEP）所存在的網路弱點，而孕育而生。WPA 採用 Michael 訊息認證碼與 RC4 加密演算法，而 WPA2 採用的是 CCMP 訊息認證碼與 AES 加密演算法。

3.28 多因子鑑別(Multi-factor authentication，MFA)

係指身分鑑別須透過二種以上的認證機制後，得以獲得裝置之存取權限。

4. 測試項目分級

本節依據「影像監控系統資安標準草案-影像錄影機」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、身分鑑別與授權機制安全及應用程式安全；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聯性，須依循第 4 節之規定內容。

安全等級依（1）風險承受度綜合考量、（2）安全技術深度、（3）目前尚無通用檢測方法、（4）技術現況及（5）檢測所需時間，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	安全測試分項	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
	5.1.2. 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
	5.1.5. 實體儲存安全測試	5.1.5.1	5.1.5.2	5.1.5.3
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
	5.2.2. 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		
	5.2.5. 敏感性資料儲存安全測試		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		
	5.2.7. API 安全測試	5.2.7.1		
	5.2.8. 系統日誌檔與警示測試	5.2.8.1	5.2.8.2	
	5.2.9. 系統儲存備份安全測試	5.2.9.1	5.2.9.2	5.2.9.3
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. 通訊介面的安全設置測試	5.3.2.1		
	5.3.3. 通訊協定安全測試		5.3.3.1	
	5.3.4. 影像傳輸安全測試	5.3.4.1	5.3.4.2	5.3.4.3
身分鑑別與授權機制安全測試	5.4.1. 鑑別機制安全測試	5.4.1.1		5.4.1.2
	5.4.2. 通行碼鑑別機制測試	5.4.2.1		
	5.4.3. 權限管控測試	5.4.3.1		
	5.4.4. 實體設備的身分裝置鑑別測試	5.4.4.1		
應用程式安全測試	5.5.1. 應用程式的程式安全測試	5.5.1.1	5.5.1.2	5.5.1.3
	5.5.2. 應用程式的系統安全測試	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 2　第 1 級測試標準

安全測試分項	測試標準
實體安全測試	
實體儲存安全測試	5.1.5.1(a) 具備內部儲存備份 – 確保受測物具備有內部儲存備份之介面，例如：SATA 等。 5.1.5.1(b) 具備外部儲存備份 – 確保受測物具備有外部儲存備份之介面，例如：USB、eSATA 等。 5.1.5.1(c) 具備手動備份、排程自動備份 – 須提供「手動備份」與「排程自動備份」功能，則本測試項目結果為通過。
作業系統安全測試	
作業系統安全測試	5.2.1.1(a) 受測物之作業系統與網路服務不應存在高風險之常見弱點與漏洞 – 受測物之作業系統與網路服務不得存在漏洞評鑑系統 CVSS v3 嚴重性等級為重大以上之資安漏洞。
網路服務連接埠的管控測試	5.2.2.1(a) 檢測所啟用之網路服務與受測物宣告之一致性 – 受測物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) 韌體程式更新功能 – 受測物的韌體更新機制必須正常運行。 5.2.3.1(b) 韌體程式更新測試之更新檔案的保護 – 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) 韌體程式更新測試之更新路徑的保護 – 韌體線上更新機制，其更新路徑必須透過安全通道保護，安全通道必須使用加密套件(Cipher Suite)。
韌體程式安全測試（選測）	5.2.4.1(a) 韌體程式碼之敏感性資料外洩 – 受測物之程式碼與安裝檔內其他檔案，不得被檢出身分鑑別因子、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。
網頁管理介面安全測試	5.2.6.1(a) 網頁管理介面弱點檢測 – 網頁管理介面操控程式，不得存在 OWASP Web 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。
API 安全測試	5.2.7.1(a) API 呼叫的身分鑑別機制 – 透過遠端管理介面與操控程式存取受測物時，必須經過身分鑑別程序，且其身分鑑別機制具備抵抗重送攻擊的能力。

	- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。 5.2.7.1(b) API 呼叫之身分鑑別錯誤訊息 - 受測物須提供能驗證相連影像監控系統裝置身分的功能，且其裝置鑑別機制具備抵抗重送攻擊的能力。 - 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。 5.2.7.1(c) API 之通行碼鑑別機制之通行碼強度 - 通行碼鑑別之通行碼長度必須符合政府組態基準 CCE-33789-9。 - 通行碼鑑別之通行碼複雜度必須符合政府組態基準 CCE-33777-4。 - 通行碼鑑別之防止重複使用舊通行碼必須符合政府組態基準 CCE-35219-5。 - 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。 5.2.7.1(d) API 之通行碼鑑別機制之預設通行碼唯一性 - 預設通行碼都須相異。 - 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。 5.2.7.1(e) API 之通行碼鑑別機制之通行碼變更機制 - 首次取得授權後必須強制更改預設通行碼。 - 受測物中的所有通行碼鑑別機制皆使用同一組通行碼，則與本測項的通過準則一致。 5.2.7.1(f) API 之通行碼鑑別機制之通行碼的輸入頻率及次數限制 - 通行碼的輸入次數必須符合最高五次嘗試登入失敗次數導致帳戶鎖定的限制。 - 通行碼的輸入頻率必須符合帳戶鎖定計數器至少一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零次失敗。 - 通行碼的輸入頻率必須符合帳戶鎖定期間至少一分鐘以上，才會自動解除鎖定。 - 受測物中的所有通行碼鑑別機制皆使用同一組通行碼，則與本測項的通過準則一致。 5.2.7.1(g) API 呼叫之權限管控機制 - 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) API 呼叫之閒置時限 - 受測物必須提供 API 呼叫權限之閒置時限功能，提供閒置時限設定，例如：最長不得超過 10 分鐘。 - 受測物之每次 API 呼叫皆須重新鑑別授權，則本通過準則為通過。

系統日誌檔與警示測試	5.2.8.1(a) 安全事件日誌檔 - 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) 存取權限管控 - 受測物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) 日誌檔保存期限 - 受測物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。
系統儲存備份安全測試	5.2.9.1(a) 儲存的每週最少一次完整備份 - 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。確保受測物支援每週最少一次完整備份。 - 受測物若不具有每週最少一次完整備份的功能，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	5.3.1.1(a) 敏感性資料於傳輸過程中須加密保護 - 敏感性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]。
通訊介面的安全設置測試	5.3.2.1(a) 網路裝置資訊探詢功能 - 受測物須提供使用者得自行開/關「網路裝置資訊探詢」功能，例如：通用隨插即用通訊協定、簡單網路管理協定及零配置通訊協定。 - 該功能預設須為關閉。 5.3.2.1(b) 安全的 WiFi 組態設置 - 受測物只要具備 WPS 功能，則必須提供使用者可自行開/關「Wi-Fi 保護設置」之 WPS PIN 及 WPS Lock 功能。 - 該功能預設須為關閉。 5.3.2.1(c) 無線網路傳輸安全機制設置 - 無線網路傳輸的安全機制預設須採用「Wi-Fi 保護存取 2」。 5.3.2.1(d) 網路介面存取設置 - 使用者不得透過網路連線存取產品作業系統之除錯模式。
影像傳輸安全測試	5.3.4.1(a) 影像資料的傳輸機密性 - 影像資料之傳輸不得為明文，須使用 FIPS 140-2 所核可之加密演算法。
身分鑑別與授權機制安全測試	
鑑別機制安全測試	5.4.1.1(a) 鑑別機制強度 - 透過遠端管理介面與操控程式存取受測物時，必須經過身分鑑別程序，且其身分鑑別機制具備抵抗重送攻擊的能力。 5.4.1.1(b) 身分鑑別錯誤訊息 - 從錯誤訊息無法推斷出合法使用者名稱。 5.4.1.1(c) 憑證鑑別強度 - 透過遠端管理介面與操控程式存取受測物時，採用憑證鑑別須確保

	憑證有效性，例如：發證單位、有效期限、格式錯誤及憑證簽章等。
通行碼鑑別機制測試	5.4.2.1(a) 通行碼強度 - 通行碼鑑別之通行碼長度必須符合政府組態基準 CCE-33789-9。 - 通行碼鑑別之通行碼複雜度必須符合政府組態基準 CCE-33777-4。 - 通行碼鑑別之防止重複使用舊通行碼必須符合政府組態基準 CCE-35219-5。 5.4.2.1(b) 預設通行碼唯一性 - 預設通行碼都須相異。 5.4.2.1(c) 通行碼變更機制 - 首次取得授權後必須強制更改預設通行碼。 5.4.2.1(d) 通行碼的輸入頻率及次數限制 - 通行碼的輸入次數必須符合最高五次嘗試登入失敗次數導致帳戶鎖定的限制。 - 通行碼的輸入頻率必須符合帳戶鎖定計數器至少一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零次失敗。 - 通行碼的輸入頻率必須符合帳戶鎖定期間至少一分鐘以上，才會自動解除鎖定。
權限控管測試	5.4.3.1(a) 權限管控機制 - 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) 權限有效時間 - 受測物必須提供遠端控制權限之閒置時限功能，提供閒置時限設定，例如：閒置時限最多不可超過 20 分鐘。
實體設備的身分裝置鑑別測試	5.4.4.1(a) 身分驗證機制 - 廠商若未能提供管理者權限者，得提供足以證明符合本測試細項之詳細說明、畫面及截圖等佐證資料，確保受測物有提供使用者權限管理機制，開機後依管理權限執行相關作業。
應用程式安全測試	
應用程式的程式安全測試	5.5.1.1(a) 應用程式為最新之版本 - 應用程式須提供可識別其發行資訊，透過連網功能，提示系統內建之管理介面是否為最新之版本。 5.5.1.1(b) 應用程式之執行取得使用者同意 - 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。
應用程式的系統安全測試	5.5.2.1(a) 應用程式執行的程式行為，應取得使用者同意 - 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受測物自我宣告之內容相符，確認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。 5.5.2.1(b) 應用程式的身分辨識及保護機制 - 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，確認應用程式有提供安全的

	身分辨識及保護機制。

4.2 安全等級第 2 級測試標準

表 3 第 2 級測試標準

安全測試分項	測試標準
實體安全測試	
實體異常行為警示測試	5.1.2.1(a) 異常狀態警示機制 – 受測廠商須提供警示機制使用說明。 – 受測物之實體操作時，出現實體設備遭受破壞，例如：網路線與同軸電纜訊號中斷時，須提供警示機制。
實體防護測試	5.1.3.1(a) 實體保護 – 受測物須採用一體成形或防拆螺絲等機殼防拆除保護設計。
實體儲存安全測試	5.1.5.2(a) 具備有效儲存空間設定機制 – 確保受測物具備有效儲存空間設定機制，儲存空間小於設定值時，提供警告機制，例如：啟動燈號、發出警報聲。
作業系統安全測試	
更新安全測試	5.2.3.2(a) 韌體更新之完整性及可信度 – 經過竄改之更新檔案不得被成功更新。
敏感性資料儲存安全測試	5.2.5.1(a) 敏感性資料加密儲存 – 系統所儲存之身分鑑別因子、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) 日誌檔存取異常警示 – 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。
系統儲存備份安全測試	5.2.9.2(a) 備份影像檔案須加密保護以確保機密性 – 備份影像檔案須加密保護以確保機密性，且保護資料的加密方式不限定加密演算法。
通訊安全測試	
通訊協定安全測試	5.3.3.1(a) 通訊協定異常輸入 – 通訊協定必須經過異常輸入檢測，受測物於測試過程中不得發生因發生崩潰而無法恢復運作。
影像傳輸安全測試	5.3.4.2(a) 影像資料的傳輸機密性 – 影像資料之傳輸，須通過安全通道，且安全通道版本須符合「附錄 B」的要求。
應用程式安全測試	
應用程式的程式安全測試	5.5.1.2(a) 應用程式的關閉機制 – 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。

應用程式的系統安全測試	5.5.2.2(a) 支援螢幕解鎖保護機制 – 受測物本身之螢幕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。 5.5.2.2(b) 支援螢幕解鎖錯誤之強制鎖定保護機制 – 受測物本身之螢幕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。 5.5.2.2(c) 螢幕鎖定解鎖資料，須加密保護 – 受測物本身之螢幕鎖定解鎖資料，須加密保護以確保機密性，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。

4.3 安全等級第 3 級測試標準

表 4 第 3 級測試標準

安全測試分項	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) 最小實體介面 - 所有不使用的介面應移除，包括電路板上除錯測試用之介面必須移除。 5.1.1.1(b) 實體行為日誌功能 - 外接實體埠的插拔操作須提供日誌紀錄。
實體防護測試	5.1.3.2(a) 內部實體安全 - 晶片上不得存在晶片編號，且電路板上不得存在功能編號。 5.1.3.2(b) 通行碼還原機制安全設計 - 受測物實體外部不得有徒手即可輕易還原預設通行碼的設計。
安全啟動測試	5.1.4.1(a) 支援安全啟動（Secure boot）功能 - 安全啟動必須正常運行，確保受測物於開機時，避免未經授權的韌體、驅動程式及作業系統的執行。
實體儲存安全測試	5.1.5.3(a) 儲存備份支援資料冗餘之能力 - 確保受測物儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上，具備將資料同時寫至第二個磁碟機之能力。 5.1.5.3(b) 支援硬碟熱備援 - 確保受測物儲存備份支援硬碟熱備援之功能，提升容錯能力。 5.1.5.3(c) 支援電源備援機制 - 確保受測物支援雙電源輸入之電源備援機制，電源異常時，提供警告機制，例如：啟動燈號、發出警報聲。
作業系統安全測試	
作業系統安全測試	5.2.1.2(a) 受測物之作業系統與網路服務不應存在高風險之常見弱點與漏洞 - 受測物之作業系統與網路服務不得存在漏洞評鑑系統 CVSS v3 嚴重性等級為高之資安漏洞。
敏感性資料儲存安全測試	5.2.5.2(a) 敏感性資料隔離保護 - 受測物須具備安全區域（Secure domain），且敏感性資料須存放於此。
系統儲存備份安全測試	5.2.9.3(a) 儲存的異地備份 - 廠商須提供測試指南，檢視其異地備份之技術是否存在，確保受測物儲存備份支援遠端儲存設備之功能，異地備份可提升影像儲存的完整性。 - 受測物若不具有異地備份的功能，則本測試項目結果為失敗 5.2.9.3(b) 儲存的資料防竄改 - 確保資料儲存支援影音資料防竄改的機制。 - 受測物若不具有影音資料防竄改的功能，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	5.3.1.2(a) 敏感性資料傳輸須採用安全通道 – 敏感性資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，並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[4]所核可，且同時支援前向安全(Forward Secrecy)之通行碼演算法。
影像傳輸安全測試	5.3.4.3(a) 影像資料的傳輸機密性 – 確保影像資料之傳輸加密演算法須採用 AES-256。 – 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。
身分鑑別與授權安全測試	
鑑別機制安全測試	5.4.1.2(a) 鑑別機制強度 – 驗證相連影像監控系統裝置身分的鑑別機制，是否透過多因子鑑別。 – 驗證遠端管理介面或操控程式與受測物之間的身分鑑別，是否透過多因子鑑別。 5.4.1.2(b) 裝置鑑別強度 – 受測物須提供能驗證相連影像監控系統裝置身分的功能，且其裝置鑑別機制具備抵抗重送攻擊的能力。
隱私保護測試	
應用程式的程式安全測試	5.5.1.3(a) 應用程式回報安全性機制 – 應用程式須提供回報安全性問題之管道。 5.5.1.3(b) 應用程式有標明所引用之第三方函式庫 – 廠商需於文件中標明所使用的應用程式所引用之第三方函式庫。
應用程式的系統安全測試	5.5.2.3(a) 應用程式的異常操作之監控及防護 – 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，確認應用程式有具備應用程式異常操作之監控及防護。

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

圖 2 是作業系統安全測試架構，包括測試用電腦（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。

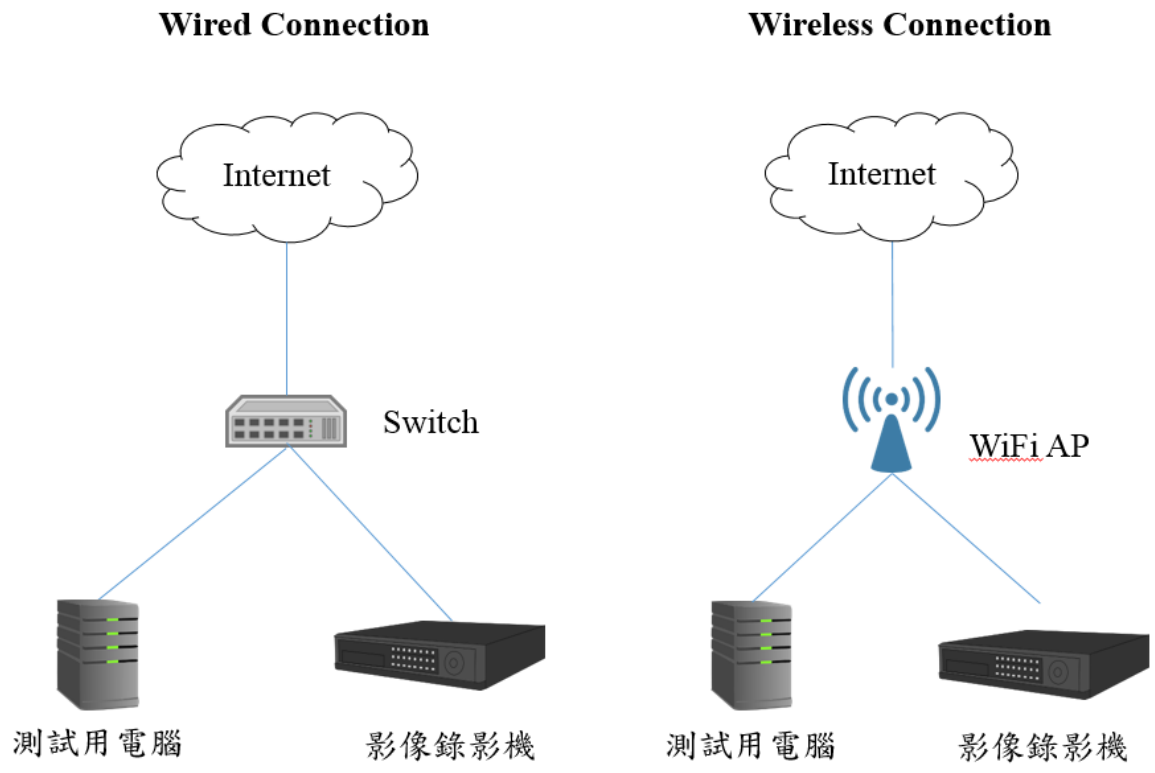

圖2 系統安全測試接續示意圖

5.1.1.1 除錯測試用之實體介面測試

(a) 最小實體介面

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.1.1(a)。

(2) 測試標準：

- 所有不使用的介面應移除，包括電路板上除錯測試用之介面必須移除。

(3) 測試步驟：

- 使用原廠所提供的特殊工具拆開外殼。
- 檢視受測物電路板外觀，不得存在具有除錯或測試用途之介面，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介面，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) 通過準則：

- 本測項為「通過」，測試步驟所列舉之實體介面皆不存在。
- 本測項為「不通過」，測試步驟所列舉之任一實體介面存在。

(b) 實體行為日誌功能

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.1.1(b)。

(2) 測試標準：

- 外接實體埠的插拔操作須提供日誌紀錄。

(3) 測試步驟：

- 插拔 USB 埠。
- 根據受測物說明，檢視插拔紀錄。
- 插拔網路埠。
- 根據受測物說明，檢視插拔紀錄。

(4) 通過準則：

- 本測項為「通過」，有提供 USB 埠與網路埠插拔日誌紀錄。
- 本測項為「不通過」，USB 埠與網路埠之任一種實體埠無提供實體埠插拔日誌紀錄。

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) 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-影像錄影機」5.1.2.1(a)。

(2) 測試標準：

- 受測物所提供之廠商，須提供「警示機制」之操作說明。
- 受測物之實體操作時，出現實體設備遭受破壞，例如：網路線與同軸電纜訊號中斷時，須提供警示機制，例如：E-mail 通知、訊息推播、發出警報聲等。

(3) 測試步驟：

- 將前端攝影機與受測物接上電源。
- 將網路線拔除或天線遮罩，使其斷訊。
- 檢視受測物是否依照使用說明達到告警效果。

(4) 通過準則：

- 本測項為「通過」，網路線與同軸電纜訊號中斷之異常警示功能皆可被證實。
- 本測項為「不通過」，網路線與同軸電纜訊號中斷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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.3.1(a)。

(2) 測試標準：

- 受測物須採用一體成形或防拆螺絲等機殼防拆除保護設計。

(3) 測試步驟：

- 檢視受測物之外殼是否透過防盜螺絲鎖住。

(4) 通過準則：

- 本測項為「通過」，受測物之外殼經由防盜螺絲鎖住。
- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.3.2(a)。

(2) 測試標準：

- 晶片上不得存在晶片編號，且電路板上不得存在功能編號。

(3) 測試步驟：

- 使用原廠所提供的特殊工具拆開外殼。
- 檢視其電路板是否存在晶片與功能編號之文字。

(4) 通過準則：

- 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) 通行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-影像錄影機」5.1.3.2(b)。

(2) 測試標準：

- 受測物實體外部不得有徒手即可輕易還原預設通行碼的設計。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「安全設計」之操作說明。
- 受測物外殼是否存在不需工具即可還原預設通行碼之設計。

(4) 通過準則：

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

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) 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-影像錄影機」5.1.4.1(a)。

(2) 測試標準：

- 安全啟動必須正常運行，確保受測物於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，待系統的完整性及可信度獲得保證，受測物始得開機，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「安全啟動」之操作說明。
- 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) 通過準則：

- 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。

5.1.5 實體儲存安全測試

測試環境請參照圖 2。

5.1.5.1 實體儲存安全的備援機制之初級要求測試

(a) 具備內部儲存備份

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.1(a)。

(2) 測試標準：

- 確保受測物具備有內部儲存備份之介面，例如：SATA 等，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 檢查受測物之實體是否具備內部儲存備份之裝置與連接器。
- 包含儲存裝置（例如：SATA、PATA）與相對應之電源供應裝置（例如：SATA 電源連接器、PATA 電源連接器）。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

(b) 具備外部儲存備份

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.1(b)。

(2) 測試標準：

- 確保受測物具備有外部儲存備份之介面，例如：USB、eSATA 等，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 檢查受測物之實體是否具備外部儲存備份之裝置與連接器。
- 包含儲存裝置與相對應之電源供應裝置，例如：USB、eSATA 等。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

(c) 具備手動備份、排程自動備份。

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.1(c)。

(2) 測試標準：

- 須提供「手動備份」與「排程自動備份」功能，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 檢查受測物之實體是否具備手動備份、排程自動備份的功能。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

5.1.5.2 實體儲存安全的備援機制之中階要求測試

(a) 具備有效儲存空間設定機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.2(a)。

(2) 測試標準：

- 確保受測物具備有效儲存空間設定機制，儲存空間小於設定值時，提供警告機制，例如：啟動燈號、發出警報聲，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「備援機制」之操作說明。
- 檢查受測物之實體是否具備有效儲存空間設定機制。
- 儲存空間小於設定值時，有警告通知，例如：啟動燈號、發出警報聲。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

5.1.5.3 實體儲存安全的備援機制之高階要求測試

(a) 儲存備份支援資料冗餘之能力

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.3(a)。

(2) 測試標準：

- 確保受測物儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上，具備將資料同時寫至第二個磁碟機之能力，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「備援機制」之操作說明。
- 檢查受測物是否支援資料冗餘之能力，或支援獨立磁碟備援陣列之技術。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

(b) 支援硬碟熱備援

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.3(b)。

(2) 測試標準：

- 確保受測物儲存備份支援硬碟熱備援之功能，提升容錯能力，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「備援機制」之操作說明。
- 檢查受測物 RAID 之技術是否存在。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

(c) 支援電源備援機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.5.3(c)。

(2) 測試標準：

- 確保受測物支援雙電源輸入之電源備援機制，電源異常時，提供警告

機制，例如：啟動燈號、發出警報聲，則本測試項目結果為通過。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「備援機制」之操作說明。
- 檢查受測物之電源備援機制之技術是否存在。
- 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) 通過準則：

- 本測項為「通過」，有資料證明具備此功能。
- 本測項為「不通過」，無法證明具備此功能，廠商無法實際示範。

5.2 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。

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的檢測之初階測試

(a) 受測物之作業系統與網路服務不應存在高風險之常見弱點與漏洞

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.1.1(a)。

(2) 測試標準：

- 受測物之作業系統與網路服務不得存在漏洞評鑑系統 CVSS v3[12]嚴重性等級為重大以上之資安漏洞。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 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漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大以上之資安漏洞。

(4) 通過準則：

- 本測項為「通過」，作業系統與網路服務不存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大以上之漏洞。
- 本測項為「不通過」，作業系統或網路服務存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大以上之漏洞。

5.2.1.2 作業系統與網路服務常見弱點與漏洞的檢測之中階測試

(a) 受測物之作業系統與網路服務不應存在高風險之常見弱點與漏洞

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.1.2(a)

(2) 測試標準：

- 受測物之作業系統與網路服務不得存在漏洞評鑑系統 CVSS v3[12]嚴重性等級為高之資安漏洞。

(3) 測試步驟：

- 將測試用電腦連接受測物。

- 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漏洞評鑑系統 CVSS v3 嚴重性等級評比為高以上之資安漏洞。

(4) 通過準則：

- 本測項為「通過」，作業系統與網路服務不存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為高以上之漏洞。
- 本測項為「不通過」，作業系統或網路服務存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為高以上之漏洞。

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 網路服務的最小化檢測

(a) 檢測所啟用之網路服務與受測物宣告之一致性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.2.1(a)。

(2) 測試標準：

- 受測物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：

- 將測試用電腦連接受測物。
- 使用弱點掃描工具。
- 檢視所開啟之網路埠。

(4) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.3.1(a)。

(2) 測試標準：

- 受測物的韌體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) 通過準則：

- 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) 韌體程式更新測試之更新檔案的保護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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。
- 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) 通過準則：

- 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) 韌體程式更新測試之更新路徑的保護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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，安全通道必須

使用下述幾種加密套件(Cipher Suite)：

- 0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
- 0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
- 0xCC,0x14 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=ChaCha20(256) Mac=AEAD
- 0xCC,0x13 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=ChaCha20(256) Mac=AEAD
- 0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
- 0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
- 0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
- 0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
- 0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
- 0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256

(3) 測試步驟：

- 受測物於出廠預設環境狀態下。
- 將受測物連網並啟動更新。
- 啟動安全通道掃描工具。
- 檢視預設之安全通道是否符合測試標準所條列之加密套件。

(4) 通過準則：

- 本測項為「通過」，安全通道採用符合測試標準所條列之加密套件。
- 本測項為「不通過」，安全通道未採用符合測試標準所條列之加密套件。

5.2.3.2 韌體更新機制強度測試

(a) 韌體更新之完整性及可信度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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：

- 擷取受測物之更新檔案。
- 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) 通過準則：

- 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) 韌體程式更新測試之更新檔案的保護，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 敏感性資料外洩測試

(a) 韌體程式碼之敏感性資料外洩

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.4.1(a)。

(2) 測試標準：

- 受測物之程式碼與安裝檔內其他檔案，不得被檢出身分鑑別因子、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。
- 檢視系統通行碼資料是否可識別。
- 確認金鑰是否可被擷取。
- 檢查是否存在非公開之 E-mail 資料。
- 檢查是否存在非公開之 IP Address 資料。
- 檢查是否存在非公開之 URL 資料。

(4) 通過準則：

- 本測項為「通過」，通行碼、金鑰及非公開之 E-mail、IP Address 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：通行碼、金鑰及非公開之 E-mail、IP Address 及 URL 資料。

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測試-中階

(a) 敏感性資料加密儲存

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.5.1(a)。

(2) 測試標準：

- 系統所儲存之身分鑑別因子、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：

- 進入受測系統管理介面。
- 解析檔案系統目錄檢視系統通行碼資料是否可識別。
- 確認金鑰是否可被擷取。
- 檢查是否存在非公開之 E-mail 資料。
- 檢查是否存在非公開之 IP Address 資料。
- 檢查是否存在非公開之 URL 資料。

(4) 通過準則：

- 本測項為「通過」，通行碼、金鑰及非公開之 E-mail、IP Address 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：通行碼、金鑰及非公開之 E-mail、IP Address 及 URL 資料。

5.2.5.2 機敏性資料的儲存保護測試-高階

(a) 敏感性資料隔離保護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.5.2(a)。

(2) 測試標準：

- 受測物須具備安全區域（Secure domain），且敏感性資料須存放於此。

(3) 測試步驟：

- 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) 通過準則：

- 本測項為「通過」，敏感性資料存放於安全區域中。
- 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檢測

(a) 網頁管理介面弱點檢測

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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 Web 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。

(3) 測試步驟：

- 由測試用電腦連線至受測物進行測試。
- 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) 通過準則：

- 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 之鑑別功能測試

(a) API 呼叫的身分鑑別機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(a)。

(2) 測試標準：

- 透過遠端管理介面與操控程式存取受測物時，必須經過身分鑑別程序，且其身分鑑別機制具備抵抗重送攻擊的能力。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。

(3) 測試步驟：

- 由測試用電腦透過遠端連線與受測物建立連接。
- 檢視存取受測物前，受測物是否有要求身分鑑別。
- 若不具身分鑑別機制，本測試項目結果為不通過，則測試結束。
- 進行身分鑑別並側錄封包。
- 將側錄到的鑑別封包再重新送至受測物。
- 判斷鑑別結果是否成功。

(4) 通過準則：

- 本測項為「通過」，重送攻擊之封包未通過受測物之鑑別。
- 本測項為「不通過」，受測物不具備身分鑑別功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之鑑別。
- 本測項為「不通過」，每台受測物的通行碼皆相同。

(b) API 呼叫之身分鑑別錯誤訊息

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(b)。

(2) 測試標準：

- 受測物須提供能驗證相連影像監控系統裝置身分的功能，且其裝置鑑別機制具備抵抗重送攻擊的能力。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。

(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，是否要求裝置鑑別。
- 若不具裝置鑑別機制，本測試項目結果為不通過，測試結束。
- 進行身分鑑別並側錄封包。
- 將側錄到的鑑別封包再重新送至受測物。

- 判斷鑑別結果是否成功。

(4) 通過準則：

- 本測項為「通過」，重送攻擊之封包未通過受測物之鑑別。
- 本測項為「不通過」，受測物不具備裝置鑑別功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之鑑別。
- 本測項為「不通過」，每台受測物的通行碼皆相同。

(c) API 之通行碼鑑別機制之通行碼強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(c)。

(2) 測試標準：

- 通行碼鑑別之通行碼長度必須符合政府組態基準 CCE-33789-9。
- 通行碼鑑別之通行碼複雜度必須符合政府組態基準 CCE-33777-4。
- 通行碼鑑別之防止重複使用舊通行碼必須符合政府組態基準 CCE-35219-5。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。

(3) 測試步驟：

- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 根據政府組態基準 CCE-33789-9 之 GCB 設定值，檢視受測物通行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通行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通行碼歷程記錄。

(4) 通過準則：

- 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。
- 本測項為「不通過」，每台受測物的預設通行碼皆相同。

(d) API 之通行碼鑑別機制之預設通行碼唯一性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(d)。

(2) 測試標準：

- 預設通行碼都須相異。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼時，則與本測項的通過準則一致。

(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。
- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 比對每台受測物的預設通行碼是否相異。

(4) 通過準則：

- 本測項為「通過」，每台受測物的預設通行碼相異。
- 本測項為「通過」，受測物登入要鑑別，但不存在預設通行碼，則本測試項目結果為通過。
- 本測項為「不通過」，每台受測物的預設通行碼皆相同。

(e) API 之通行碼鑑別機制之通行碼變更機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(e)。

(2) 測試標準：

- 首次取得授權後必須強制更改預設通行碼。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼，則與本測項的通過準則一致。

(3) 測試步驟：

- 受測物為出廠預設環境狀態。
- 由測試用電腦連線至受測物。
- 進行 API 鑑別通行碼輸入。
- 確認首次取得授權後，是否強制要求更改預設通行碼。

(4) 通過準則：

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

(f) API 之通行碼鑑別機制之通行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-影像錄影機」5.2.7.1(f)。

(2) 測試標準：

- 通行碼的輸入次數必須符合最高五次嘗試登入失敗次數導致帳戶鎖定的限制。

- 通行碼的輸入頻率必須符合帳戶鎖定計數器至少一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零次失敗。
- 通行碼的輸入頻率必須符合帳戶鎖定期間至少一分鐘以上，才會自動解除鎖定。
- 受測物中的所有通行碼鑑別機制皆使用同一組通行碼，則與本測項的通過準則一致。

(3) 測試步驟：

- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 不斷輸入錯誤的通行碼進行 API 鑑別。
- 檢視受測物被鎖定的嘗試登入失敗次數最多不可超過五次。
- 檢視受測物重設帳戶鎖定計數器的時間間隔至少要為一分鐘。
- 檢視受測物之帳戶鎖定期間至少一分鐘以上。

(4) 通過準則：

- 本測項為「通過」，同時符合帳戶鎖定限制最多五次、帳戶鎖定計數器時間間隔至少一分鐘及帳戶鎖定期間至少一分鐘。
- 本測項為「不通過」，帳戶鎖定限制高於五次。
- 本測項為「不通過」，帳戶鎖定計數器時間間隔不到一分鐘。
- 本測項為「不通過」，帳戶鎖定期間不到一分鐘。

(g) API 呼叫之權限管控機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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：

- 將測試用電腦連線至受測物。
- 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 的鑑別授權。
- 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) 通過準則：

- 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：

「影像監控系統資安標準草案-影像錄影機」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，提供閒置時限設定，例如：最長不得超過十分鐘。
- 受測物之每次 API 呼叫皆須重新鑑別授權，則本通過準則為通過。

(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。
- 依設定之閒置時限，檢視 API 呼叫是否需要重新鑑別。

(4) 通過準則：

- 本測項為「通過」，依設定之閒置時限，需重新鑑別方可再存取 API 呼叫。
- 本測項為「通過」，每次 API 呼叫皆須重新鑑別授權。
- 本測項為「不通過」，不支援 API 呼叫之權限閒置時限。

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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.8.1(a)。

(2) 測試標準：

- 安全事件日誌的資料應包含完整時間戳記、使用者身分及操作行為等。
- 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：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「安全事件日誌」之操作說明。
- 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) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.8.1(b)。

(2) 測試標準：

- 受測物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：

- 受測物所提供之廠商，須提供「安全事件日誌」之操作說明。
- 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) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.8.1(c)。

(2) 測試標準：

- 受測物之日誌檔須具備保存期限的設計。
- 須符合 NIST SP 800-92[5]中高影響系統 high impact systems 的日誌資料維護長度。

(3) 測試步驟：

- 受測物所提供之廠商，須提供「安全事件日誌」之操作說明。
- 檢視日誌檔的保存期限是否與受測物自我宣告相符。

(4) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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：

- 受測物所提供之廠商，須提供「安全事件日誌」之操作說明。
- 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告警效果。

(4) 通過準則：

- 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」，測項 5.2.8.1 系列任一檢測結果為不通過。
- 本測項為「不通過」，日誌檔無法儲存時，未收到警示。

5.2.9 系統儲存備份安全測試

測試環境請參照圖 2。

5.2.9.1 備份安全之初階要求測試

(a) 儲存的每週最少一次完整備份

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.9.1(a)。

(2) 測試標準：

- 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。確保受測物支援每週最少一次完整備份。
- 受測物若不具有每週最少一次完整備份的功能，則本測試項目結果為失敗。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 根據受測物之使用說明，開啟備份功能。
- 檢視每週最少一次完整備份的功能是否可以正常啟動。

(4) 通過準則：

- 本測項為「通過」，每週最少一次完整備份可以正常運作。
- 本測項為「不通過」，未提供完整備份功能。
- 本測項為「不通過」，完整備份無法正常運作。

5.2.9.2 備份安全之中階要求測試

(a) 備份影像檔案須加密保護以確保機密性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.9.2(a)。

(2) 測試標準：

- 備份影像檔案須加密保護以確保機密性，且保護資料的加密方式不限定加密演算法。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 根據受測物之使用說明，開啟備份影像檔案。
- 檢視備份影像檔案是否被加密保護。

(4) 通過準則：

- 本測項為「通過」，備份影像檔案有被加密保護。
- 本測項為「不通過」，備份影像檔案沒有被加密保護。
- 本測項為「不通過」，加密演算法不支援 AES-256。

5.2.9.3 備份安全之高階要求測試

(a) 儲存的異地備份

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.9.3(a)。

(2) 測試標準：

- 廠商須提供測試指南，檢視其異地備份之技術是否存在，確保受測物儲存備份支援遠端儲存設備之功能，異地備份可提升影像儲存的完整性。
- 受測物若不具有異地備份的功能，則本測試項目結果為失敗。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「儲存備份」之操作說明。
- 根據受測物之使用說明，開啟異地備份功能。
- 檢視異地備份的設定是否可以正常啟動。

(4) 通過準則：

- 本測項為「通過」，異地備份可以正常運作。
- 本測項為「不通過」，未提供異地備份功能。
- 本測項為「不通過」，異地備份無法正常運作。

(b) 儲存的資料防竄改

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.9.3(b)。

(2) 測試標準：

- 確保資料儲存支援影音資料防竄改的機制。
- 受測物若不具有影音資料防竄改的功能，則本測試項目結果為失敗。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「防竄改機制」之操作說明。
- 根據受測物之使用說明，開啟影音資料防竄改功能。
- 檢視影音資料防竄改的功能是否可以正常啟動。

(4) 通過準則：

- 本測項為「通過」，影音資料防竄改可以正常運作。
- 本測項為「不通過」，未提供影音資料防竄改功能。
- 本測項為「不通過」，影音資料防竄改無法正常運作。

5.3 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。

5.3.1 資料傳輸安全測試

測試環境請參照圖 2。

5.3.1.1 敏感性資料之傳輸保護初階測試

(a) 敏感性資料於傳輸過程中須加密保護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.1.1(a)。

(2) 測試標準：

- 敏感性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：

- 由測試用電腦連線至受測物。
- 開啟受測物之操控程式，進行敏感性資料之傳輸測試。
- 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) 通過準則：

- 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 敏感性資料之傳輸保護中階測試

(a) 敏感性資料傳輸須採用安全通道

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.1.2(a)。

(2) 測試標準：

- 敏感性資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，並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[4]所核可，且同時支援前向安全（Forward Secrecy）之通行碼演算法。

(3) 測試步驟：

- 由測試用電腦連線至受測物。
- 開啟受測物之操控程式，進行敏感性資料之傳輸測試。
- 側錄封包，檢視封包是否經過安全通道。
- 透過測試程式與支援「附錄 B」的要求之伺服器連線，檢查測試程式回

報結果。

(4) 通過準則：

- 本測項為「通過」，測試程式確認受測物可使用 FIPS 140-2 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 FIPS 140-2 加密傳輸。

5.3.2 通訊介面的安全設置測試

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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(a)。

(2) 測試標準：

- 受測物須提供使用者得自行開/關「網路裝置資訊探詢」功能，例如：通用隨插即用通訊協定、簡單網路管理協定及零配置通訊協定。
- 該功能預設須為關閉。

(3) 測試步驟：

- 受測物於出廠預設環境狀態下。
- 由測試用電腦連線至受測物。
- 開啟受測物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) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(b)。

(2) 測試標準：

- 受測物只要具備 WPS 功能，則必須提供使用者可自行開/關「Wi-Fi 保護設置」之 WPS PIN 及 WPS Lock 功能。
- 該功能預設須為關閉。

(3) 測試步驟：

- 受測物於出廠預設環境狀態下。

- 由測試用電腦連線至受測物。
- 開啟受測物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) 通過準則：

- 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

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(c)。

(2) 測試標準：

- 無線網路傳輸的安全機制預設須採用「Wi-Fi 保護存取 2」。

(3) 測試步驟：

- 受測物於出廠預設環境狀態下。
- 由測試用電腦連線至受測物。
- 開啟受測物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) 通過準則：

- 本測項為「通過」，無線網路預設之加密模式為「Wi-Fi 保護存取 2」。
- 本測項為「不通過」，無線網路預設之加密模式不為「Wi-Fi 保護存取 2」。

(d) 網路介面存取設置

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(d)。

(2) 測試標準：

- 使用者不得透過網路連線存取產品作業系統之除錯模式。

(3) 測試步驟：

- 受測物於出廠預設環境狀態下，測試用 PC 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之除錯模式。

(4) 通過準則：

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

5.3.3 通訊協定安全測試

測試環境請參照圖 2。

5.3.3.1 通訊協定異常輸入檢測

(a) 通訊協定異常輸入

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.3.1(a)。

(2) 測試標準：

- 通訊協定必須經過異常輸入檢測，受測物於測試過程中不得發生因發生崩潰而無法恢復運作。

(3) 測試步驟：

- 由測試用電腦連線至受測物。
- 執行受測物之影音傳輸功能。
- 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) 通過準則：

- 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。

5.3.4 影像傳輸安全測試

測試環境請參照圖 2。

5.3.4.1 影像資料的傳輸初階保護

(a) 影像資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.4.1(a)。

(2) 測試標準：

- 影像資料之傳輸不得為明文，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。
- 由測試用電腦連線至受測物進行封包側錄。
- 同時分析封包是否加密，並檢視其加密演算法。

(4) 通過準則：

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

5.3.4.2 影像資料的傳輸中階保護

(a) 影像資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.4.2(a)。

(2) 測試標準：

- 影像資料之傳輸，須通過安全通道，且安全通道版本須符合「附錄 B」的要求。

(3) 測試步驟：

- 由遠端管理介面進行受測物各種功能操作。
- 由測試用電腦連線至受測物進行封包側錄。
- 同時分析封包是否加密，並檢視其加密演算法。

(4) 通過準則：

- 本測項為「通過」，影像資料之傳輸通過安全通道，且安全通道版本符合「附錄 B」的要求。
- 本測項為「不通過」，影像資料傳輸不是使用通過安全通道，或安全通道版本不符合「附錄 B」的要求。

5.3.4.3 影像資料的傳輸高階保護

(a) 影像資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.4.3(a)。

(2) 測試標準：

- 確保影像資料之傳輸加密演算法須採用 AES-256。
- 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：

- 於受測物中啟動測試程式。
- 由測試用電腦連線至受測物進行封包側錄。
- 檢查測試程式回報結果。

(4) 通過準則：

- 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。

5.4 身分鑑別與授權安全測試

檢視影像錄影機之身分鑑別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 鑑別機制安全測試

測試環境請參照圖 2。

5.4.1.1 鑑別機制強度初階測試

(a) 鑑別機制強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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受測物時，必須經過身分鑑別程序，且其身分鑑別機制具備抵抗重送攻擊的能力。

(3) 測試步驟：

- 由測試用電腦透過遠端連線與受測物建立連接。
- 檢視存取受測物前，受測物是否有要求身分鑑別。
- 若不具身分鑑別機制，本測試項目結果為不通過，測試結束。
- 進行身分鑑別並側錄封包。
- 將側錄到的鑑別封包再重新送至受測物。
- 判斷鑑別結果是否成功。

(4) 通過準則：

- 本測項為「通過」，重送攻擊之封包未通過受測物之鑑別。
- 本測項為「不通過」，受測物不具備身分鑑別功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之鑑別。

(b) 身分鑑別錯誤訊息

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.1.1(b)。

(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：

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

(4) 通過準則：

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

(c) 憑證鑑別強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.1.1(c)。

(2) 測試標準：

- 透過遠端管理介面與操控程式存取受測物時，採用憑證鑑別須確保憑證有效性，例如：發證單位、有效期限、格式錯誤及憑證簽章等。

(3) 測試步驟：

- 由測試用電腦透過遠端連線與受測物建立連接。
- 監聽連線建立封包。
- 檢視存取受測物前，是否有要求身分鑑別。
- 測試人員自簽一個憑證去測試鑑別是否成功。

(4) 通過準則：

- 本測項為「通過」，通過受測物之憑證鑑別。
- 本測項為「不通過」，未通過受測物之憑證鑑別。

5.4.1.2 鑑別機制強度中階測試

(a) 鑑別機制強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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鑑別機制，是否透過多因子鑑別。
- 驗證遠端管理介面或操控程式與受測物之間的身分鑑別，是否透過多因子鑑別。

(3) 測試步驟：

- 審閱具備此功能證明之書面資料。

(4) 通過準則：

- 本測項為「通過」，受測物之身分鑑別透過多因子鑑別。
- 本測項為「不通過」，受測物之身分鑑別未透過多因子鑑別。

(b) 裝置鑑別強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.1.2(b)。

(2) 測試標準：

- 受測物須提供能驗證相連影像監控系統裝置身分的功能，且其裝置鑑別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，是否要求裝置鑑別。
- 若不具裝置鑑別機制，本測試項目結果為不通過，測試結束。
- 進行身分鑑別並側錄封包。
- 將側錄到的鑑別封包再重新送至受測物。

- 判斷鑑別結果是否成功。

(4) 通過準則：

- 本測項為「通過」，重送攻擊之封包未通過受測物之鑑別。
- 本測項為「不通過」，受測物不具備裝置鑑別功能。
- 本測項為「不通過」，重送攻擊之封包通過受測物之鑑別。

5.4.2 通行碼鑑別機制測試

測試環境請參照圖 2。

5.4.2.1 通行碼鑑別機制

(a) 通行碼強度

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.2.1(a)。

(2) 測試標準：

- 通行碼鑑別之通行碼長度必須符合政府組態基準 CCE-33789-9。
- 通行碼鑑別之通行碼複雜度必須符合政府組態基準 CCE-33777-4。
- 通行碼鑑別之防止重複使用舊通行碼必須符合政府組態基準 CCE-35219-5。

(3) 測試步驟：

- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 根據政府組態基準 CCE-33789-9 之 GCB 設定值，檢視受測物通行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通行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通行碼歷程紀錄。

(4) 通過準則：

- 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) 預設通行碼唯一性

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.2.1(b)。

(2) 測試標準：

- 預設通行碼都須相異。

(3) 測試步驟：

- 準備 2 台以上受測物。
- 受測物於出廠預設環境狀態下。
- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 比對每台受測物的預設通行碼是否相異。

(4) 通過準則：

- 本測項為「通過」，每台受測物的預設通行碼相異。
- 本測項為「通過」，受測物登入要鑑別，但不存在預設通行碼，則本測試項目結果為通過。
- 本測項為「不通過」，每台受測物的預設通行碼相同。

(c) 通行碼變更機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」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通行碼。

(3) 測試步驟：

- 受測物於出廠預設環境狀態下。
- 由測試用電腦連線至受測物。
- 進行 API 鑑別通行碼輸入。
- 確認首次取得授權後，是否強制要求更改預設通行碼。

(4) 通過準則：

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

(d) 通行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-影像錄影機」5.4.2.1(d)。

(2) 測試標準：

- 通行碼的輸入次數必須符合最高五次嘗試登入失敗次數導致帳戶鎖定的限制。
- 通行碼的輸入頻率必須符合帳戶鎖定計數器至少一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零次失敗。
- 通行碼的輸入頻率必須符合帳戶鎖定期間至少一分鐘以上，才會自動解除鎖定。

(3) 測試步驟：

- 由測試用電腦連線至受測物進行 API 授權通行碼輸入。
- 不斷輸入錯誤的通行碼進行 API 鑑別。
- 檢視受測物被鎖定的嘗試登入失敗次數最多不可超過五次。
- 檢視受測物重設帳戶鎖定計數器的時間間隔至少要為一分鐘。
- 檢視受測物之帳戶鎖定期間至少一分鐘以上。

(4) 通過準則：

- 本測項為「通過」，同時符合帳戶鎖定限制最多五次、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一分鐘。
- 本測項為「不通過」，帳戶鎖定限制高於五次。
- 本測項為「不通過」，帳戶鎖定計數器時間間隔不到一分鐘。
- 本測項為「不通過」，帳戶鎖定期間不到一分鐘。

5.4.3 權限管控測試

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-影像錄影機」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：

- 將測試用電腦連線至受測物。
- 受測物所提供之廠商，須提供「遠端管理介面」之操作說明。
- 根據受測物說明，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) 通過準則：

- 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-影像錄影機」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，提供閒置時限設定，例如：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。
- 依設定之閒置時限，檢視再次遠端控制受測物時是否需要重新鑑別。

(4) 通過準則：

- 本測項為「通過」，依設定之閒置時限，需重新鑑別方可再遠端控制/存取受測物。
- 本測項為「不通過」，依設定之閒置時限，無需重新鑑別方即再遠端控制/存取受測物。

5.4.4 實體設備的身分裝置鑑別測試

測試環境請參照圖 2。

5.4.4.1 受測物需提供身分驗證機制

(a) 身分驗證機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.4.1(a)。

(2) 測試標準：

- 廠商若未能提供管理者權限者，得提供足以證明符合本測試細項之詳細說明、畫面及截圖等佐證資料，確保受測物有提供使用者權限管理機制，開機後依管理權限執行相關作業。

(3) 測試步驟：

- 將測試用電腦連線至受測物。
- 受測物所提供之廠商，須提供「遠端管理介面」之操作說明。
- 根據受測物說明，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) 通過準則：

- 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。

5.5 應用程式安全測試

檢視影像錄影機之應用程式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，應用程式安全泛指從影像錄影機端或操作介面端所收集到的使用者資訊。

5.5.1 應用程式的程式安全測試

測試環境請參照圖 2。

5.5.1.1 應用程式的程式安全之初級要求測試

(a) 應用程式為最新之版本

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.1.1(a)。

(2) 測試標準：

- 應用程式須提供可識別其發行資訊，透過連網功能，提示系統內建之管理介面是否為最新之版本。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物說明，開啟受測軟體之應用程式。
- 檢視該應用程式是否與受測物宣告的最新之版本相符。

(4) 通過準則：

- 本測項為「通過」，應用程式為最新之版本。
- 本測項為「不通過」，應用程式與最新之版本不符。

(b) 應用程式之執行取得使用者同意

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.1.1(b)。

(2) 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。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物說明，檢查受測系統之隱私權政策或使用聲明中，是否提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。
- 如未符合，則執行受測軟體，並存取使用者敏感性資料。
- 檢查受測軟體是否提供相對應的使用者同意機制。
- 檢視該應用程式執行的行為是否與受測物自我宣告相符。

(4) 通過準則：

- 本測項為「通過」，應用程式之執行取得使用者同意。
- 本測項為「不通過」，應用程式之執行未取得使用者同意即執行。

5.5.1.2 應用程式的程式安全之中階要求測試

(a) 應用程式的關閉機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.1.2(a)。

(2) 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。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 以管理者權限取得所有執行中的應用程式清單。
- 執行並操作受測軟體。
- 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。
- 檢查上述兩個步驟之清單相同。

(4) 通過準則：

- 本測項為「通過」，應用程式可以正常關閉。
- 本測項為「不通過」，應用程式無法關閉。

5.5.1.3 應用程式的程式安全之高階要求測試

(a) 應用程式回報安全性機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.1.3(a)。

(2) 測試標準：

- 應用程式須提供回報安全性問題之管道，包括：E-mail 通知、訊息推播等。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物之使用說明，是否有回報安全性的功能。
- 檢視回報安全性的功能是否可以正常啟動。

(4) 通過準則：

- 本測項為「通過」，回報安全性機制可以正常運作。
- 本測項為「不通過」，未提供回報安全性機制。
- 本測項為「不通過」，回報安全性機制無法正常運作。

(b) 應用程式有標明所引用之第三方函式庫

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.1.3(b)。

(2) 測試標準：

- 廠商需於文件中標明所使用的應用程式所引用之第三方函式庫。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物說明，是否標明所使用的應用程式所引用之第三方函式庫。
- 檢視該應用程式是否與受測物自我宣告的相符。

(4) 通過準則：

- 本測項為「通過」，應用程式有標明所使用的應用程式所引用之第三方函式庫。
- 本測項為「不通過」，應用程式未標明所使用的應用程式所引用之第三方函式庫。

5.5.2 應用程式的系統安全測試

測試環境請參照圖 2。

5.5.2.1 應用程式的系統安全之初級要求測試

(a) 應用程式執行的程式行為，應取得使用者同意

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.1(a)。

(2) 測試標準：

- 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受測物自我宣告之內容相符，確認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。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物說明，開啟受測軟體之應用程式。
- 檢視該應用程式執行時是否取得使用者同意，必要時並提供風險提示。

(4) 通過準則：

- 本測項為「通過」，應用程式執行前取得使用者才執行。
- 本測項為「不通過」，執行前未徵求使用者之同意。
- 本測項為「不通過」，即使使用者不同意也可以執行。

(b) 應用程式的身分辨識及保護機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.1(b)。

(2) 測試標準：

- 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，確認應用程式有提供安全的身分辨識及保護機制。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物說明，資料在使用、儲存及傳輸時有提供安全的身分辨識及保護機制。
- 檢視該身分辨識及保護機制是否與受測物自我宣告的相符。

(4) 通過準則：

- 本測項為「通過」，廠商有提供身分辨識及保護機制。
- 本測項為「不通過」，廠商沒有提供身分辨識及保護機制。

5.5.2.2 應用程式的系統安全之中階要求測試

(a) 支援螢幕解鎖保護機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.2(a)。

(2) 測試標準：

- 受測物本身之螢幕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。

(3) 測試步驟：

- 開啟受測系統。
- 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。
- 檢查是否可以進入螢幕鎖定模式後，依所設定的解鎖資料喚醒受測系統。

(4) 通過準則：

- 本測項為「通過」，應用程式支援螢幕解鎖保護機制。
- 本測項為「不通過」，應用程式不支援螢幕解鎖保護機制。
- 本測項為「不通過」，應用程式支援螢幕解鎖保護機制，但是功能無法正常運作。

(b) 支援螢幕解鎖錯誤之強制鎖定保護機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.2(b)。

(2) 測試標準：

- 受測物本身之螢幕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。

(3) 測試步驟：

- 開啟受測系統。
- 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。

(4) 通過準則：

- 本測項為「通過」，應用程式的螢幕解鎖錯誤之強制鎖定保護機制可以正常運作。
- 本測項為「不通過」，未提應用程式的螢幕解鎖錯誤之強制鎖定保護機制。
- 本測項為「不通過」，應用程式的螢幕解鎖錯誤之強制鎖定保護機制無法正常運作。

(c) 螢幕鎖定解鎖資料，須加密保護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.2(c)。

(2) 測試標準：

- 受測物本身之螢幕鎖定解鎖資料，須加密保護以確保機密性，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。

(3) 測試步驟：

- 開啟受測系統。
- 確認已符合檢測條件。
- 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。
- 以管理者權限身分確認解鎖資料是否以明文方式儲存於受測物上；若未能提供管理者權限者，得提供足以證明符合本測試細項之詳細說明、畫面及截圖等佐證資料，必要時檢測實驗室得要求申請者做功能示範。

(4) 通過準則：

- 本測項為「通過」，螢幕鎖定解鎖資料，有加密保護。
- 本測項為「不通過」，螢幕鎖定解鎖資料，未加密保護。

5.5.2.3 應用程式的系統安全之高階要求測試

(a) 應用程式的異常操作之監控及防護

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.5.2.3(b)。

(2) 測試標準：

- 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，確認應用程式有具備應用程式異常操作之監控及防護。

(3) 測試步驟：

- 將測試用電腦連接受測物。
- 受測物所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測物之使用說明，執行異常操作的動作。
- 檢視異常操作是否被監控及防護。

(4) 通過準則：

- 本測項為「通過」，異常操作後即有警示通知回報。
- 本測項為「不通過」，異常操作後應用程式並無任何警示。

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，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，因此目前本規範強烈建議使用的版本如下：

- Transport Layer Security（TLS）1.2

附錄 C
（規定）
影像錄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。

C.6 檔案傳輸協定（File Transfer Protocol，FTP）[11]

定義在 RFC 959 規範中，是一種用於網路檔案傳輸的一套標準協議，具有可靠性和高效率的傳輸資料，並促進檔案的共享之模式。

參考資料

[1] 台灣資通產業標準協會（TAICS），影像監控系統資安標準草案-影像錄影機

[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

[11] RFC 959, File Transfer Protocol（FTP）

[12] First.org, Inc., Common Vulnerability Scoring System, V3 Development Update, https://www.first.org/cvss

[13] MITRE corp., Common Vulnerabilities and Exposures, https://cve.mitre.org/cve/cve.html