影像監控系統資安標準之測試規範草案
–影像錄影機
（V0.9.2）

推動單位：

台灣資通產業標準協會（TAICS）

制定單位：

台灣資通產業標準協會之網路與資訊安全技術工作委員會（TC5）

支持單位：

經濟部工業局、財團法人資訊工業策進會

2017-12-05

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
V0.2.0	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
V0.2.1	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
V0.3.0	2017/9/27	陳聰杰	依據2017/9/22編審會議討論內容修改	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。 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。
V0.4.0	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。
V0.4.1	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。
V0.5.0	2017/10/19	陳聰杰	依據 2017/10/17 編審會議討論內容修改	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。 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。
V0.6.0	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」。
V0.7.0	2017/10/31	陳聰杰	依據 2017/10/27 公開說明會討論內容修改	1. 新增用語及定義。 2. 調整 5.1.5.2 節至 5.2.9.1 節。 3. 新增 5.1.6 節。 4. 調整 5.2.4 節至 5.2.3 節。 5. 修正 5.2.8 與 5.2.9 節。 6. 調整 5.4.4.1 節。 7. 調整 5.5 節。
V0.8.0	2017/11/09	陳聰杰	依據 2017/11/3 編審會議討論內容修改	1. 增加 5.1.2.1(b) 儲存裝置須具備保護機制。 2. 移除 5.1.5.2(c) 支援電源備援機制。 3. 移除 5.1.6 實體設備的身分鑑別測試。 4. 增加 5.2.8.1(c) 影像檔案具備權限控管機制。 5. 移除 5.5.1.1(a) 識別程式來源要求測試。 6. 移除 5.5.2.1(b) 關閉應用程式的要求測試。 7. 調整 5.5.2.2(a) 回報安全性問題之管道到 5.5.2.1(c)。 8. 原表 2~表 4 的測試標準表移除。 9. 加入樣品條件。 10. 全文的受測物改為受測產品。

				11. 增加附錄 D。
V0.8.1	2017/11/23	陳聰杰	依據編審與專家會議討論內容修改	1. 調整 5.2.8.1(b) 確保影像檔案支援防竄改之警示機制。 2. 調整附錄 A 與附錄 C 之格式。
V0.9.0	2017/11/25	陳聰杰	依據 2017/11/24 專家會議之專家意見彙總表	1. 5.4.1.2(a)等級調整至 3 級。 2. 5.4.1.2(b)改為 5.4.1.1(d) 等級調整至 1 級。 3. 5.2.9.1(a) 建議修正確保產品支援完整備份影像檔案之能力。 4. 調整 5.2.9.3(a) 確保產品支援影像檔案異地儲存備份之功能。
V0.9.1	2017/11/28	陳聰杰	依據編審與專家會議討論內容修改	1. 修正測試項目之條文為「得」更改為「應」。 2. 修正測試項目之條文為「儲存裝置」更改為「儲存媒體」。 3. 修正表 1。 4. 修正 5.5.2 節。 5. 修改圖 2 測試示意圖
V0.9.2	2017/12/04	陳聰杰	依據編審與專家會議討論內容修改	1. 修正參考資料。 2. 刪除「附錄 A」及相關引用之章節。 3. 修改「附錄 B」至「附錄 A」及相關引用之章節。 4. 修改「附錄 C」至「附錄 B」及相關引用之章節。 5. 修改「附錄 D」至「附錄 C」。 6. 調整 5.1.2.1(b)、5.2.3.1(b)、5.2.3.1(c)、5.2.4.1(a)、5.3.1.1(a)、5.3.1.2(a)、5.3.4、5.2.9.2(a)的測試內容。

目錄

前言

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

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

本標準之部分內容，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。

0. 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、測試方法及測試結果等事項。

1. 適用範圍

本測試規範應用於影像監控系統中具連網功能之固定式影像錄影機皆屬之，如圖 1 紅框所示。

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，擬依五個安全構面定義之，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、應用程式安全。

本規範為確保影像監控系統影像錄影機符合「影像監控系統資安標準-影像錄影機」資訊安全水準要求，依（1）實體安全測試、（2）系統安全測試、（3）通訊安全測試、（4）身分鑑別與授權機制安全測試及（5）應用程式安全測試五項安全測試構面，訂定其產品之測試標準、測試方法及測試結果。本規範適用於影像監控系統中具連網功能之固定式影像錄影機（如圖 1）。

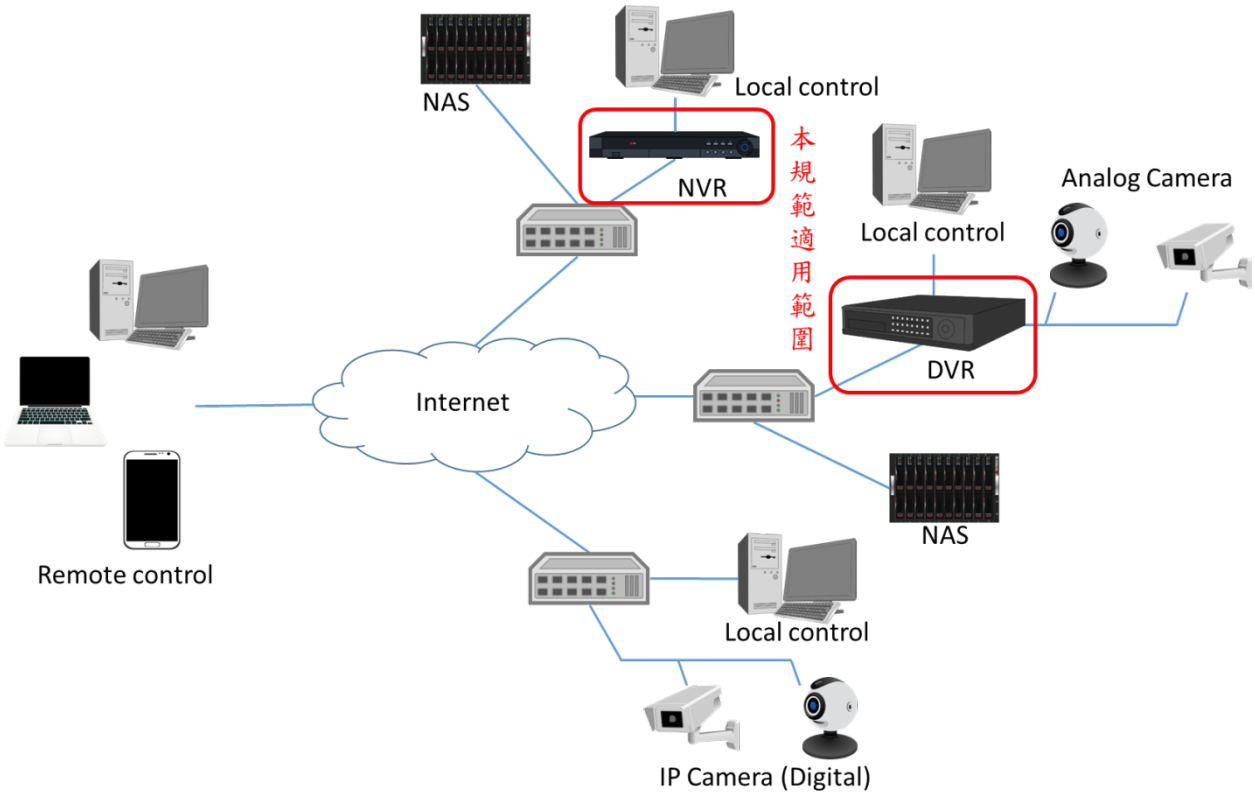

圖1. 適用範圍示意圖

2. 引用標準

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

TAICS TS 5100-2-2 影像監控系統資安標準-影像錄影機。

3. 用語及定義

TAICS TS 5100-2-2 所規定之用語及定義適用於本標準。

4. 測試項目分級

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

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、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連性，須依循第 4 節之規定內容。

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

表 1　實機測試標準等級總表

安全測試構面	安全測試項目	安全等級 測試標準		
		1 級	2 級	3 級
實體安全測試	5.1.1. 實體埠之安全管控測試	—	—	5.1.1.1
	5.1.2. 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. 實體備份測試	5.1.5.1	5.1.5.2	—
系統安全測試	5.2.1. 作業系統與網路服務安全測試	5.2.1.1	—	5.2.1.2
	5.2.2. 網路服務連接埠安全測試	5.2.2.1	—	—
	5.2.3. 更新安全測試	5.2.3.1	—	—
	5.2.4. 敏感性資料儲存安全測試	5.2.4.1	—	5.2.4.2
	5.2.5. 網頁管理介面安全測試	5.2.5.1	—	—

	5.2.6. 操控程式之應用程式介面安全測試	5.2.6.1	—	—
	5.2.7. 系統日誌檔與警示測試	5.2.7.1	5.2.7.2	—
	5.2.8. 系統儲存安全測試	—	5.2.8.1	—
	5.2.9. 系統備份安全測試	5.2.9.1	5.2.9.2	5.2.9.3
通訊安全測試	5.3.1. 敏感性資料傳輸安全測試	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	—
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. 通行碼鑑別安全測試	5.4.2.1	—	—
	5.4.3. 權限管控測試	5.4.3.1	—	—
應用程式安全測試	5.5.1. 程式信任來源測試	—	—	5.5.1.1
	5.5.2. 程式執行安全測試	5.5.2.1	5.5.2.2	—

5. 資安測試規範

5.1 實體安全測試

5.1.1 實體埠之安全管控測試

作業系統安全測試架構，如圖 2 所示，包括測試 PC（供測試人員連線至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。

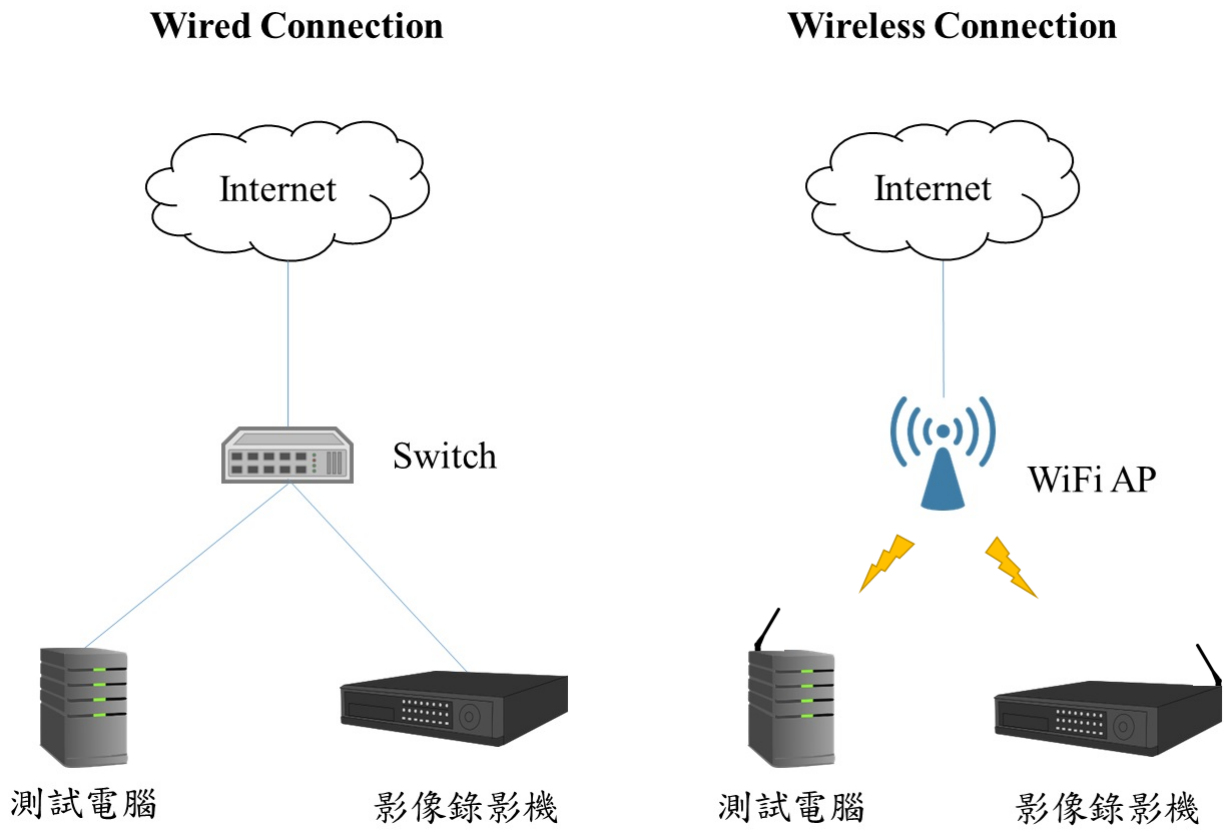

圖2 系統安全測試接續示意圖

5.1.1.1 產品之外接實體介面

(a) 最小實體介面測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.1.1.1(a)。

(2) 測試標準：

- 受測產品於電路板上除錯測試用之連接器須移除，例如：連接器等。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 使用原廠所提供的特殊工具拆開外殼。
- 檢視受測產品電路板外觀，不應存在具有除錯或測試用途之介面，包括 TTL Serial、UART、JTAG、SWD。
- 檢視受測產品內零件外觀，不應存在具有除錯或測試用途之連接器，包括排母、排針、板對板連接器、板對線連接器、抽屜式連接器。

(5) 測試結果：

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

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 硬體設計須具備異常狀態之警示機制

(a) 異常狀態警示機制測試

(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：

- 受測產品須具備相關警示機制於實體操作發生斷訊時，例如：網路線或同軸電纜訊號中斷時。

(3) 樣品條件：

- 受測產品須在通電的狀態下。

(4) 測試方法：

- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 將網路線拔除或天線遮罩，使其斷訊。
- 檢視受測產品是否依照使用說明達到警示效果。
- 將同軸電纜拔除，使其斷訊。
- 檢視受測產品是否依照使用說明達到警示效果。

(5) 測試結果：

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

(b) 儲存媒體須具備保護機制測試

(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(b)。

(2) 測試標準：

- 受測產品支援儲存媒體（例如：硬碟機）保護機制，且受測產品之儲存媒體不應在本機以外的機器被存取。

(3) 樣品條件：

- 儲存媒體支援更換之功能。

(4) 測試方法：

- 使用具儲存媒體拆解功能之工具，對受測產品之儲存媒體進行拆解。
- 重新裝上儲存媒體。

- 確認系統通行碼資料是否可識別。
- 確認金鑰是否可被擷取。
- 確認是否存在非公開之 E-mail 資料。
- 確認是否存在非公開之 IP Address 資料。
- 確認是否存在非公開之 URL 資料。

(5) 測試結果：

- 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。

(c) 實體埠插拔操作記錄功能測試

(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(c)。

(2) 測試標準：

- 受測產品須具有實體埠插拔操作記錄功能，例如：USB 埠、網路埠等。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 插拔 USB 埠，檢視插拔紀錄。
- 插拔網路埠，檢視插拔紀錄。

(5) 測試結果：

- 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。

5.1.3 實體防護測試

測試環境請參照圖 2。

5.1.3.1 產品之外殼須具不被輕易拆除的防護機制

(a) 實體保護測試

(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：

- 受測產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 目視受測產品之外殼是一體成形。
- 目視受測產品之外殼經防拆螺絲鎖住。

(5) 測試結果：

- 本測項為「通過」，受測產品之外殼為一體成形。
- 本測項為「通過」，受測產品經由防拆螺絲鎖住。
- 本測項為「不通過」，受測產品之外殼非一體成形或非由防拆螺絲鎖住。

5.1.3.2 避免不安全的實體設計

(a) 內部實體安全測試（選測）

(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：

- 晶片上不應存在晶片編號，且電路板上不應存在功能編號。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 使用原廠所提供的特殊工具拆開外殼。
- 目視晶片上是否存在編號。
- 目視電路板上是否存在功能編號。

(5) 測試結果：

- 本測項為「通過」，晶片與電路板上皆不存在編號。
- 本測項為「不通過」，晶片或電路板上存在編號。

(b) 通行碼還原機制安全設計測試

(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：

- 受測產品外部不應有徒手即可輕易還原預設通行碼的設計。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 根據受測產品使用說明，目視受測產品外觀是否存在徒手即可輕易還原預設通行碼之設計。

(5) 測試結果：

- 本測項為「通過」，徒手無法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 產品須提供安全啟動（Secure boot）功能

(a) 支援安全啟動（Secure boot）功能測試

(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：

- 受測產品不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。

(3) 樣品條件：

- 受測產品須提供安全啟動功能之設計文件。

(4) 測試方法：

- 審閱具備此功能證明之書面資料。

(5) 測試結果：

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

5.1.5 實體備份測試

測試環境請參照圖 2。

5.1.5.1 儲存備份機制初階要求

(a) 具備內部儲存備份測試

(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：

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

(3) 樣品條件：

- 無。

(4) 測試方法：

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

(5) 測試結果：

- 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) 具備外部儲存備份測試

(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：

- 確保受測產品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) 樣品條件：

- 無。

(4) 測試方法：

- 受測產品所提供之廠商，須提供「儲存備份」之操作說明。
- 檢查受測產品之實體是否具備外部儲存備份之裝置與連接器。

- 包含儲存媒體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。

(5) 測試結果：

- 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、排程自動備份測試

(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) 樣品條件：

- 無。

(4) 測試方法：

- 受測產品所提供之廠商，須提供「儲存備份」之操作說明。
- 檢查受測產品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。

(5) 測試結果：

- 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 儲存備份機制中階要求

(a) 儲存備份支援資料冗餘之能力測試

(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：

- 確保受測產品儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 受測產品所提供之廠商，須提供「儲存機制」之操作說明。
- 檢查受測產品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。

(5) 測試結果：

- 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) 支援硬碟熱備援測試

(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(b)。

(2) 測試標準：

- 確保受測產品儲存備份支援硬碟熱備援之功能，提升容錯能力。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 受測產品所提供之廠商，須提供「備援機制」之操作說明。
- 檢查受測產品的硬碟熱備援之技術是否存在。
- 當無充分資料證明具備此功能時，則請受測廠商實際示範。

(5) 測試結果：

- 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 作業系統與網路服務安全測試

測試環境請參照圖 2。

5.2.1.1 產品之作業系統與網路服務不應存在重大風險之常見弱點與漏洞

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

(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：

- 受測產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 啟動具作業系統及網路服務弱點掃描功能之工具，對受測產品執行弱點掃描。
- 目視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS v3 評分為 9 分以上之資安漏洞。

(5) 測試結果：

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

5.2.1.2 產品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

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

(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：

- 受測產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 啟動具作業系統及網路服務弱點掃描功能之工具，對受測產品執行弱點掃描。
- 目視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS v3 評分為 7 分以上之資安漏洞。

(5) 測試結果：

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

5.2.2 網路服務連接埠安全測試

測試環境請參照圖 2。

5.2.2.1 產品僅開啟必要之網路服務

(a) 所啟用之網路服務與受測產品自我宣告之一致性測試

(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：

- 受測產品開啟之網路服務須為廠商提供必要服務之所需，防止受測產品因啟用網路介面而被侵入的可能性，且廠商須於受測產品文件中標註應啟用之網路服務，避免未宣告之網路服務被開啟。
- 不包括 UPnP 所開啟之動態埠。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 開啟受測產品之操控程式或網頁管理介面。
- 啟動具網路埠掃描（port scan）功能之工具，對受測產品執行埠掃描。
- 目視掃描結果所呈現之網路埠開關狀態。
- 比對受測產品自我宣告中聲明之網路埠開關狀態。

(5) 測試結果：

- 本測項為「通過」，掃描結果之網路埠開關狀態與自我宣告內容相符。
- 本測項為「不通過」，掃描結果之網路埠開關狀態與自我宣告內容不符。

5.2.3 更新安全測試

測試環境請參照圖 2。

5.2.3.1 韌體更新機密性保證

(a) 韌體程式更新功能測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.3.1(a)。

(2) 測試標準：

- 韌體更新機制必須正常運行。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 若提供離線更新，目視操控程式或網頁管理介面是否具備檔案更新操作介面。
- 若提供線上更新，目視操控程式或網頁管理介面是否具備線上更新操作介面。

(5) 測試結果：

- 本測項為「通過」，離線或線上更新功能之驗證被認可。
- 本測項為「不通過」，無法證明具備離線或線上更新功能。

(b) 韌體程式更新測試之更新檔案的保護測試

(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：

- 受測產品支援離線手動更新，則更新檔案須加密保護以確保機密性，且須採用 FIPS 140-2 [3]所核可之加密演算法。
- 受測產品之身分鑑別因子、加解密用之金鑰（不含非對稱加密用之公鑰）及個人資料，不應出現於韌體之程式碼與安裝檔內其他檔案中。

(3) 樣品條件：

- 受測產品支援離線更新。

(4) 測試方法：

- 使用具韌體拆解功能之工具，對受測產品之韌體進行拆解。
- 檢視更新檔案是否可被解析。
- 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。

(5) 測試結果：

- 本測項為「通過」，韌體無法被拆解且加密演算法之驗證被認可。
- 本測項為「不通過」，韌體被拆解。
- 本測項為「不通過」，無法證明加密演算法採用 FIPS 140-2[3]所核可之加密演算法。
- 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。

(c) 韌體程式更新測試之更新路徑的保護測試

(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：

- 受測產品支援線上更新，其更新路徑須通過安全通道，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向安全功能（Forward Secrecy）。

(3) 樣品條件：

- 受測產品支援線上更新。

(4) 測試方法：

- 啟動安全通道掃描工具，對更新伺服器進行掃描。
- 比對掃描結果是否為「附錄 C」中所包含之 cipher suite。
- 檢視相同的線上更新頁面是否存在支援超文本傳輸協定之頁面。

(5) 測試結果：

- 本測項為「通過」，掃描結果為「附錄 A」中所包含之 cipher suite。
- 本測項為「不通過」，韌體更新未經過安全通道。
- 本測項為「通過」，掃描結果不為「附錄 A」中所包含之 cipher suite。

(d) 韌體更新之完整性及可信度測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.3.1(d)。

(2) 測試標準：

- 受測產品必須具備驗證韌體之正確性及完整性的功能。

(3) 樣品條件：

- 受測產品支援離線更新。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 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。

(5) 測試結果：

- 本測項為「通過」，竄改過的更新檔，及再簽章過的更新檔，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 敏感性資料儲存安全測試

測試環境請參照圖 2。

5.2.4.1 產品所儲存之敏感性資料須透過加密儲存

(a) 敏感性資料加密儲存測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.4.1(a)。

(2) 測試標準：

- 系統所儲存之身分鑑別因子、螢幕解鎖、加解密用之金鑰（不含非對稱加密用之公鑰）及個人資料不應明文儲存。
- 保護資料的加密方式須採用 FIPS 140-2 [3]所核可之加密演算法。

(3) 樣品條件：

- 受測產品須提供進入作業系統除錯模式之方法。

(4) 測試方法：

- 進入作業系統之除錯模式。
- 確認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。

(5) 測試結果：

- 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。

5.2.4.2 敏感性資料的存放，須從正常作業環境中隔離

(a) 敏感性資料隔離保護測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.4.2(a)。

(2) 測試標準：

- 敏感性資料必須存放於產品的安全區域。

(3) 樣品條件：

- 受測產品須提供此功能之設計文件。

(4) 測試方法：

- 審閱具備此功能證明之書面資料。

(5) 測試結果：

- 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。

5.2.5 網頁管理介面安全測試

測試環境請參照圖 2。

5.2.5.1 網頁管理介面不應存在 OWASP Web Top 10 常見網站安全風險

(a) 網頁管理介面弱點檢測測試

(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：

- 受測產品本機提供之網頁管理介面不應存在 OWASP Web Top 10[5]之 A1-Injection 及 A3-Cross-Site Scripting（XSS）攻擊。
- 受測產品不具網頁管理介面，則本測試項目結果為通過。
- 受測產品之網頁不應使用超文本傳輸協定。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 啟動具備網頁弱點掃描功能之工具，對受測產品網頁介面執行弱點掃描。
- 目視該弱點掃描工具所產生之報告，是否存在引發 Injection 及 XSS 之資安攻擊風險。

(5) 測試結果：

- 本測項為「通過」，不存在引發 Injection 及 XSS 之資安攻擊風險。
- 本測項為「通過」，受測產品不具網頁管理介面。
- 本測項為「不通過」，存在引發 Injection 及 XSS 之資安攻擊風險。
- 本測項為「不通過」，受測產品使用超文本傳輸協定之網頁。

5.2.6 操控程式之應用程式介面安全測試

測試環境請參照圖 2。

5.2.6.1 應用程式介面之鑑別機制強度

(a) 應用程式介面之認證機制測試

(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：

- 受測產品中的所有通行碼鑑別機制皆使用同一組通行碼，則本測項測試通過與否，同測項 5.4.1.1(a)與 5.4.1.1(c)測試結果一致。
- 同 5.4.1.1(a)與 5.4.1.1(c)之測試標準。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 同 5.4.1.1(a)與 5.4.1.1(c)之測試方法。

(5) 測試結果：

- 同 5.4.1.1(a)與 5.4.1.1(c)測試結果之判定描述。

(b) 應用程式介面之通行碼鑑別測試

(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(b)。

(2) 測試標準：

- 受測產品中的所有通行碼鑑別機制皆使用同一組通行碼，則本測項測試結果與測項 5.4.2.1(a)、5.4.2.1(b)、5.4.2.1(c)及 5.4.2.1(d)測試結果一致。
- 同 5.4.2.1(a)、5.4.2.1(b)、5.4.2.1(c)及 5.4.2.1(d)之測試標準。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 同 5.4.2.1(a)、5.4.2.1(b)、5.4.2.1(c)及 5.4.2.1(d)之測試方法。

(5) 測試結果：

- 同 5.4.2.1(a)、5.4.2.1(b)、5.4.2.1(c)及 5.4.2.1(d)測試結果之判定描述。

(c) 應用程式介面之權限管控機制

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.6.1(c)。

(2) 測試標準：

- 同 5.4.3.1(a)與 5.4.3.1(b)之測試標準。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 同 5.4.3.1(a)與 5.4.3.1(b)之測試方法。

(5) 測試結果：

- 同 5.4.3.1(a)與 5.4.3.1(b)測試結果之判定描述。

5.2.7 系統日誌檔與警示測試

測試環境請參照圖 2。

5.2.7.1 產品須提供安全事件日誌檔

(a) 安全事件日誌檔測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(a)。

(2) 測試標準：

- 須具備安全事件日誌檔之顯示功能，以記錄使用者的存取行為，用以察覺未授權或異常的登入操作及檔案的存取，該日誌檔內須包括完整時間戳記、使用者身分及操作行為等，供後續查閱之用。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具，瀏覽安全事件日誌。
- 檢視日誌內容是否記載使用者的登入紀錄。
- 檢視該日誌之登入紀錄是否提供時間與使用者身分資訊。

(5) 測試結果：

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

(b) 存取權限管控測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.1(b)。

(2) 測試標準：

- 受測產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的修改。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具，瀏覽安全事件日誌。

- 檢視帳號之身分類型對日誌檔的存取權限是否與受測產品自我宣告相符。

(5) 測試結果：

- 本測項為「通過」，日誌檔的存取權限與受測產品自我宣告相符。
- 本測項為「不通過」，日誌檔的存取權限與與受測產品自我宣告不符。

(c) 日誌檔保存期限測試

(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：

- 須要求產品之日誌檔留存時間。
- 須符合 NIST SP 800-92[4]中 high impact systems 的日誌資料維護時效。

(3) 樣品條件：

- 受測產品須提供日誌檔保存期限之說明文件。

(4) 測試方法：

- 測試人員根據受測產品之使用說明，檢視日誌檔的保存期限。

(5) 測試結果：

- 本測項為「通過」，保存期限符合 NIST SP 800-92[4]中 high impact systems 的日誌資料維護時效。
- 本測項為「不通過」，保存期限未符合 NIST SP 800-92[4]中 high impact systems 的日誌資料維護時效。

5.2.7.2 產品須提供異常警示功能

(a) 日誌檔存取異常警示測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.2.7.2(a)。

(2) 測試標準：

- 受測產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。

(3) 樣品條件：

- 受測產品須提供日誌檔保存期限之說明文件。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 將受測產品之日誌檔儲存空間填滿。
- 檢視受測產品是否依照使用說明達到警示效果。

(5) 測試結果：

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

5.2.8 系統儲存安全測試

測試環境請參照圖 2。

5.2.8.1 儲存機制安全要求

(a) 具備有效儲存空間設定機制測試

(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：

- 確保受測產品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。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 受測產品所提供之廠商，須提供「儲存機制」之操作說明。
- 檢查受測產品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。

(5) 測試結果：

- 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) 具備儲存的資料防竄改機制測試

(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：

- 確保影像檔案支援防竄改之警示機制。

(3) 樣品條件：

- 無。

(4) 測試方法：

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

(5) 測試結果：

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

(c) 影像檔案具備權限控管機制測試

(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：

- 確保存取影像檔案具備權限控管機制，且透過通行碼鑑別機制防護。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試用電腦連接受測產品。
- 受測產品所提供之廠商，須提供「權限控管機制」之操作說明。
- 根據受測產品之使用說明，存取影像檔案。
- 檢視權限控管機制的功能是否可以正常啟動。

(5) 測試結果：

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

5.2.9 系統備份安全測試

測試環境請參照圖 2。

5.2.9.1 影像檔案備份安全初階要求

(a) 受測產品支援完整備份影像檔案之能力測試

(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：

- 確保受測產品支援完整備份影像檔案之能力。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試用電腦連接受測產品。
- 受測產品所提供之廠商，須提供「儲存備份」之操作說明。
- 根據受測產品之使用說明，開啟完整備份功能。
- 檢視完整備份的功能是否可以正常啟動。

(5) 測試結果：

- 本測項為「通過」，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 影像檔案備份安全中階要求

(a) 備份影像檔案須加密保護以確保機密性測試

(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，且須採用 FIPS 140-2 [3]所核可之加密演算法。

(3) 樣品條件：

- 無。

(4) 測試方法：

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

(5) 測試結果：

- 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。

5.2.9.3 影像檔案備份安全高階要求

(a) 儲存的異地備份測試

(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：

- 確保受測產品支援影像檔案異地儲存備份之功能。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試用電腦連接受測產品。
- 受測產品所提供之廠商，須提供「儲存備份」之操作說明。
- 根據受測產品之使用說明，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。

(5) 測試結果：

- 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。

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 敏感性資料傳輸安全測試

測試環境請參照圖 2。

5.3.1.1 敏感性資料於傳輸過程中須加密保護

(a) 敏感性資料於傳輸過程中須加密保護測試

(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：

- 敏感性資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向安全功能（Forward Secrecy）。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 使用安全通道掃描工具。
- 比對掃描結果是否為「附錄 C」中所包含之 cipher suite。
- 檢視相同的網頁管理介面是否存在支援超文本傳輸協定之身分鑑別相關頁面。
- 根據產品使用說明，開啟相應之管理介面連接工具。
- 執行身分鑑別操作，檢視操控程式之身分鑑別過程是否採用安全通道。

(5) 測試結果：

- 本測項為「通過」，掃描結果為「附錄 C」中所包含之 cipher suite。
- 本測項為「不通過」，掃描結果不為「附錄 C」中所包含之 cipher suite。

5.3.1.2 敏感性資料傳輸須採用安全通道

(a) 敏感性資料傳輸須採用安全通道測試

(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：

- 安全通道所使用之加密演算法須支援 AES-256 同等或以上加密強度的演算法。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 由測試用電腦連線至受測產品進行封包側錄。
- 檢查測試程式回報結果。

(5) 測試結果：

- 本測項為「通過」，測試程式回報可使用 AES-256 加密傳輸。
- 本測項為「不通過」，測試程式回報不可使用 AES-256 加密傳輸。

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 避免錯誤的通訊介面設置

(a) 網路裝置資訊探詢功能測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(a)。

(2) 測試標準：

- UPnP、SNMP 及 Bonjour 服務必須提供使用者可自行開/關功能之設置。
- SNMP 服務預設應為關閉。
- Bonjour 服務預設應為關閉。

(3) 樣品條件：

- 產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 目視受測產品之操控程式或網頁管理介面，UPnP 是否存在供使用者操作的開/關介面。
- 透過具 UPnP 掃描功能之工具以確認受測產品是否支援 UPnP 服務，同時確認使用者是否可自行開/關 UPnP 服務。
- 目視受測產品之操控程式或網頁管理介面，SNMP 是否存在供使用者操作的開/關介面。
- 透過具 SNMP 掃描功能之工具以確認受測產品是否支援 SNMP 服務，同時確認使用者是否可自行開/關 SNMP 服務。
- 目視受測產品之操控程式或網頁管理介面，Bonjour 是否存在供使用者操作的開/關介面，且預設為關閉。
- 透過具 Bonjour 掃描功能之工具以確認受測產品是否支援 Bonjour 服務，同時確認使用者是否可自行開/關 Bonjour 服務。

(5) 測試結果：

- 本測項為「通過」，UPnP、SNMP 及 Bonjour 可供使用者進行開/關操作，且 SNMP 及 Bonjour 預設都必須關閉。
- 本測項為「不通過」，SNMP 及 Bonjour 任一服務預設未關閉。
- 本測項為「不通過」，UPnP、SNMP 及 Bonjour 任一服務不可供使用者進行開/關操作。

(b) 安全的 WiFi 組態設置測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.2.1(b)。

(2) 測試標準：

- 受測產品具備 WPS 功能，則必須提供使用者 WPS PIN 開/關之功能。
- 該功能預設須為關閉。
- 受測產品不支援 WPS 功能，本測試項目為通過。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據產品使用說明，開啟相應之管理介面連接工具。
- 目視產品之操控程式或網頁管理介面,WPS PIN 是否存在供使用者操作的開/關介面，且此開/關功能是否有效。

(5) 測試結果：

- 本測項為「通過」，WPS PIN 皆存在供使用者操作的開/關介面，且預設都必須關閉。
- 本測項為「通過」，產品不支援 WPS 功能。
- 本測項為「不通過」，UPnP 功能預設未關閉。
- 本測項為「不通過」，UPnP 功能未存在供使用者操作的開/關介面。

(c) 無線網路傳輸安全機制設置測試

(1) 測試依據：

「影像監控系統資安標準草案-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) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據產品使用說明，開啟相應之管理介面連接工具。
- 目視產品之操控程式或網頁管理介面，無線網路預設加密模式是否為「Wi-Fi 保護存取 2」。
- 側錄 Wi-Fi 封包，確認傳輸是否採「Wi-Fi 保護存取 2」加密。

(5) 測試結果：

- 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) 網路介面存取設置測試

(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：

- 預設不應透過網路連線存取受測產品作業系統之除錯模式。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 檢視可否透過受測產品所開啟之網路服務連接埠存取作業系統之除錯模式。

(5) 測試結果：

- 本測項為「通過」，可透過網路服務連接埠存取作業系統之除錯模式。
- 本測項為「通過」，存取作業系統之除錯模式應經過身分鑑別。
- 本測項為「不通過」，不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 產品所使用之關鍵通訊協定，必須經過異常輸入檢測

(a) 通訊協定異常輸入測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.3.3.1(a)。

(2) 測試標準：

- 受測產品之關鍵通訊協定（參考附錄 B），不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致受測產品因發生崩潰而服務中止的情形。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 由測試用電腦連線至受測產品。
- 啟動具模糊測試功能之工具
- 執行受測產品之影像傳輸功能。
- 執行對「附錄 B」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。

(5) 測試結果：

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

5.3.4 影像傳輸安全測試

影像資料傳輸安全測試同「5.3.1 敏感性資料傳輸安全測試」之內容。

5.3.4.1 影像資料傳輸機密性初階要求

(a) 影像資料傳輸須通過安全通道測試

(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：

- 影像資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 A」的要求，同時應支援前向安全（Forward Secrecy）之加密演算法。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 使用安全通道掃描工具。
- 比對掃描結果是否為「附錄 C」中所包含之 cipher suite。
- 檢視相同的網頁管理介面是否存在支援超文本傳輸協定之身分鑑別相關頁面。
- 根據產品使用說明，開啟相應之管理介面連接工具。
- 執行身分鑑別操作，檢視操控程式之身分鑑別過程是否採用安全通道。

(5) 測試結果：

- 本測項為「通過」，掃描結果為「附錄 C」中所包含之 cipher suite。
- 本測項為「不通過」，掃描結果不為「附錄 C」中所包含之 cipher suite。

5.3.4.2 影像資料傳輸機密性高階要求

(a) 影像資料傳輸加密演算法須支援 AES-256 測試

(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：

- 安全通道所使用之加密演算法須支援 AES-256 同等或以上加密強度的演算法。

(3) 樣品條件：

- 無。

(4) 測試方法：

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

(5) 測試結果：

- 本測項為「通過」，測試程式回報可使用 AES-256 加密傳輸。
- 本測項為「不通過」，測試程式回報不可使用 AES-256 加密傳輸。

5.4 身分鑑別與授權機制安全測試

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 鑑別機制初階強度要求

(a) 鑑別機制強度測試

(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：

- 透過管理介面存取受測產品資源前，須透過具備防止重送攻擊之身分鑑別機制。

(3) 樣品條件：

- 受測產品之用戶帳號已經建立。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具。
- 執行身分鑑別操作，同時側錄封包。
- 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至受測產品。
- 檢視認證結果是否成功。

(5) 測試結果：

- 本測項為「通過」，重送攻擊之封包未通過受測產品之身分鑑別。
- 本測項為「不通過」，受測產品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產品之身分鑑別。

(b) 身分鑑別錯誤訊息測試

(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：

- 鑑別錯誤訊息不能顯露出合法使用者名稱。

(3) 樣品條件：

- 受測產品之用戶帳號已經建立。

(4) 測試方法：

- 將測試電腦連接受測產品。

- 根據受測產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。
- 輸入錯誤的通行碼，檢視鑑別錯誤訊息是否透露合法使用者名稱。

(5) 測試結果：

- 本測項為「通過」，錯誤訊息未明確指出是帳號錯誤還是通行碼錯誤。
- 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) 憑證認證有效性測試

(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：

- 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) 樣品條件：

- 受測產品之用戶帳號已經建立。
- 受測產品須支援憑證鑑別機制。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。
- 竄改憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
- 檢視憑證鑑別是否成功

(5) 測試結果：

- 本測項為「通過」，竄改憑證鑑別失敗。
- 本測項為「不通過」，竄改憑證鑑別成功。

(d) 裝置鑑別測試

(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(d)。

(2) 測試標準：

- 受測產品支援影像監控系統裝置身分鑑別功能，且須具備防止重送攻擊之能力，確保相連裝置之可信度。

(3) 樣品條件：

- 受測產品之裝置帳號已經建立。
- 受測產品具備與其相連之前端攝影機。

(4) 測試方法：

- 將受測產品與其它影像監控系統裝置建立連線。
- 檢查成功建立連線前，是否要求裝置鑑別。
- 若不具裝置認證機制，本測試項目結果為不通過，測試結束。

- 執行身分鑑別操作，同時側錄封包。
- 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至受測產品。
- 檢視認證結果是否成功。

(5) 測試結果：

- 本測項為「通過」，重送攻擊之封包未通過產品之身分鑑別。
- 本測項為「不通過」，受測產品不具備裝置鑑別機制。
- 本測項為「不通過」，重送攻擊之封包通過產品之身分鑑別。

5.4.1.2 鑑別機制高階強度要求

(a) 認證機制強度測試

(1) 測試依據：

「影像監控系統資安標準草案-影像錄影機」5.4.1.2(a)。

(2) 測試標準：

- 受測產品之鑑別機制須採用多因子鑑別。

(3) 樣品條件：

- 受測產品之用戶帳號及相關認證因子（如通行碼）已經建立，且多因子認證功能已經啟用。
- 須提供具多因子認證操作之受測產品說明文件。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據受測產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別
- 執行多因子身分鑑別操作，檢查是否每次的身分鑑別都採用不同種類之認證因子。
- 檢查認證過程中是否採用 SMS 簡訊獲取通行碼。
- 檢查認證過程中，使用行動裝置作為 what you have 認證因子時，檢視是否能同時在 2 台以上的行動裝置上獲取認證因子。

(5) 測試結果：

- 本測項為「通過」，透過多因子鑑別應以存取受測產品。
- 本測項為「不通過」，未透過多因子鑑別即可存取受測產品。
- 本測項為「不通過」，每一次身分鑑別皆採用相同種類的認證因子。
- 本測項為「不通過」，當使用 what you have 認證因子時，採用 SMS 簡訊獲取通行碼。
- 本測項為「不通過」，當使用 what you have 認證因子時，同時可從 2 台以上行動裝置的 App 獲取通行碼。

5.4.2 通行碼鑑別安全測試

測試環境請參照圖 2。

5.4.2.1 通行碼鑑別機制強度

(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[2]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[2]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[2] CCE-35219-5。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 從網頁管理介面或操控程式建立或變更通行碼。
- 輸入小於 8 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。
- 輸入含使用者的帳戶名稱全名中，超過兩個以上的連續字元，檢查通行碼是否能成功建立或變更。
- 輸入不含英文大寫字元(A 到 Z)、英文小寫字元(a 到 z)、10 進位數字(0 到 9)或非英文字母字元(例如：!、$、#、%)之任一種類字元之通行碼，檢查通行碼是否能成功建立或變更。
- 從網頁管理介面或操控程式變更通行碼，輸入與現行相同之通行碼，檢查通行碼是否能成功變更。

(5) 測試結果：

- 本測項為「通過」，同時符合政府組態基準[2] 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[2] CCE-33789-9。
- 本測項為「不通過」，不符合政府組態基準[2] CCE-33777-4。
- 本測項為「不通過」，不符合政府組態基準[2] CCE-35219-5。

(b) 預設通行碼唯一性測試

(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：

- 廠商所生產之產品其預設通行碼都須相異
- 在未經設定新通行碼前無法存取產品。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 準備兩台以上受測產品。
- 透過網頁管理介面或操控程式，根據產品使用說明輸入預設通行碼。
- 比對每台網路攝影機的預設通行碼是否相異。

(5) 測試結果：

- 本測項為「通過」，兩台受測產品的預設通行碼相異。
- 本測項為「通過」，受測產品不存在預設通行碼之設計。
- 本測項為「不通過」，兩台受測產品的預設通行碼相同。

(c) 通行碼變更機制測試

(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：

- 首次成功取得受測產品存取之授權，須強制更改預設通行碼。

(3) 樣品條件：

- 受測產品須保持出廠預設環境狀態。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 從網頁管理介面或操控程式輸入通行碼。
- 確認首次取得授權後，是否強制要求更改預設通行碼。

(5) 測試結果：

- 本測項為「通過」，首次取得授權後，強制要求更改預設通行碼。
- 本測項為「通過」，產品不具備「預設通行碼」之功能。
- 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測試

(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) 樣品條件：

- 受測產品之用戶帳號及相關認證因子（如通行碼）已經建立。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。
- 不斷輸入錯誤的通行碼。
- 檢視受測產品被鎖定的嘗試登入失敗次數最多不可超過五次。
- 檢視受測產品重設帳戶鎖定計數器的時間間隔至少要為一分鐘。
- 檢視受測產品之帳戶鎖定期間至少一分鐘以上。

(5) 測試結果：

- 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 產品資源的存取，必須具備權限管控機制

(a) 權限管控機制測試

(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產品，必須具備權限管控機制，該使用者的身分授權須與受測產品自我宣告相符。
- 至少要有二個以上不同權限的角色。

(3) 樣品條件：

- 受測產品之用戶帳號及相關認證因子（如通行碼）已經建立。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 透過網頁管理介面或操控程式，分別以不同角色登入受測產品。
- 存取受測產品資源，同時檢視該帳號之身分類型與其對應之權限是否與受測產品自我宣告相符。

(5) 測試結果：

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

(b) 權限有效時間測試

(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：

- 受測產品之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試電腦連接受測產品。
- 透過網頁管理介面或操控程式登入受測產品。
- 目視受測產品之操控程式或網頁管理介面，閒置時限是否存在供使用者設定的操作介面。
- 閒置受測產品直到超過閒置時限值。
- 檢視是否需要重新認證才可存取受測產品。

(5) 測試結果：

- 本測項為「通過」，閒置超過閒置時限值，需重新認證方可再遠端控制/存取受測產品。
- 本測項為「不通過」，閒置超過閒置時限值，無需重新認證方可再遠端控制/存取受測產品。

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 程式信任來源測試

測試環境請參照圖 2。

5.5.1.1 函式庫引用安全要求

(a) 引用之第三方函式庫測試

(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：

- 應用程式須於文件中標明所引用之第三方函式庫，則本測試項目結果為通過。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 開啟受測系統。
- 確認已符合檢測條件。
- 受測產品所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測產品說明，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產品自我宣告的相符。

(5) 測試結果：

- 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 程式執行安全測試

測試環境請參照圖 2。

5.5.2.1 執行機制安全要求

(a) 應用程式回報安全性機制測試

(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：

- 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，則本測試項目結果為通過。

(3) 樣品條件：

- 無。

(4) 測試方法：

- 將測試用電腦連接受測產品。
- 受測產品所提供之廠商，須提供「應用程式」之操作說明。
- 根據受測產品之使用說明，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。

(5) 測試結果：

- 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。

5.5.2.2 起動機制安全要求

(a) 應用程式的異常啟動機制測試

(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：

- 應用程式須具備未授權或遭竄改之應用程式不應被啟動，則本測試項目結果為通過。

(3) 樣品條件：

- 無。

(4) 測試方法：

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

(5) 測試結果：

- 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）
安全通道版本使用要求

係指超文本傳輸協定結合安全性通訊層協定或傳輸層安全性協定，建立安全通道以保護傳輸中資料不被竊取之技術，然而安全性通訊層協定在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布將全面禁用，所以已經完全由傳輸層安全性協定取代安全性通訊層協定，但傳輸層安全性協定 1.0 存在可以降級到安全性通訊層協定 3.0 的功能，使得傳輸層安全性協定 1.0 同樣不被信任，因此目前本標準強烈建議使用的版本如下：

- 傳輸層安全性協定 1.2

附錄 B
（規定）
影像錄影機所使用之通訊協定

B.1 即時傳輸協定（Real-time Transport Protocol，RTP）&即時傳送控制協定（Real-time Transport Control Protocol，RTCP）

定義在 RFC 3550 規範中[6]，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。定義在 RFC 3550 規範中[6]，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）。

B.2 即時串流協定（Real Time Streaming Protocol，RTSP）

定義在 RFC 2326 規範中[7]，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。

B.3 超文本傳輸協定（Hyper Text Transfer Protocol，HTTP）

定義在 RFC 7540 規範中[8]，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。

B.4 傳輸層安全協定（The Transport Layer Security，TLS）

定義在 RFC 5246 規範中[9]，在兩個應用程式之間，透過網路建立起安全通道，於交換資料時可防止遭受到竊聽及篡改。

B.5 檔案傳輸協定（File Transfer Protocol，FTP）

定義在 RFC 959 規範中[10]，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。

附錄 C
（規定）
影像錄影機建議使用之 Cipher Cuite

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

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] 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）.

[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] NIST, NIST Special Publication 800-92: Guide to Computer Security Log Management, Sep, 2006.

[5] OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project.

[6] RFC 3550, RTP: A Transport Protocol for Real-Time Applications.

[7] RFC 2326, Real Time Streaming Protocol（RTSP）.

[8] RFC 7540, Hypertext Transfer Protocol Version 2（HTTP/2）.

[9] RFC 5246, The Transport Layer Security（TLS）Protocol Version 1.2.

[10] RFC 959, File Transfer Protocol（FTP）.