TAICS

TAICS TS-0015-2 v1.0 : 2017

影像監控系統資安標準之測試規範－網路攝影機

Video Surveillance System Security Test Specification - IP Camera

2017/12/26

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

影像監控系統資安標準之測試規範
—網路攝影機

Video Surveillance System Security Test Specification– IP Camera

出版日期: 2017/12/26
終審日期: 2017/12/15

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC 主席：安華聯網科技(股)公司 洪光鈞 總經理

TC 副主席：資訊工業策進會 蔡正煜 組長

TC 物聯網資安工作組組長：資訊工業策進會 高傳凱 博士

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

(行)國家中山科學研究院、(財)工業技術研究院、(財)台灣電子檢驗中心、(財)資訊工業策進會、(財)電信技術中心、中華電信(股)公司、友訊科技(股)公司、安華聯網科技(股)公司、宏達國際電子(股)公司、果核數位(股)公司、國立中央大學、晶復科技(股)公司、趨勢科技(股)公司。

本規範由經濟部工業局支持研究制定。

目錄

前言

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

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

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

網路攝影機，係藉由鏡頭採集圖像後，由攝影機內感光元件及控制元件處理影像並轉換成數位訊號，傳輸到電腦後再由軟體進行圖像還原，或透過內建處理器及網頁伺服器，以有線或無線網路連線檢視畫面。

鑑於近幾年網路攝影機資安事件頻傳，經濟部工業局為全面改善網路攝影機資安品質，計劃制定一系列影像監控系統相關之資安標準，並參考現行國際間物聯網資安相關標準與規範，協助台灣產業接軌國際，提升研發技術及保證產品質量。

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

1. 適用範圍

本規範為確保影像監控系統網路攝影機的資訊安全，依(1)實體安全、(2)系統安全、(3)通訊安全、(4)身分鑑別與授權機制安全、及(5)隱私保護等五項安全構面，訂定其產品安全技術要求。本規範適用於影像監控系統中具連網功能之嵌入式網路攝影機(如圖 1)。

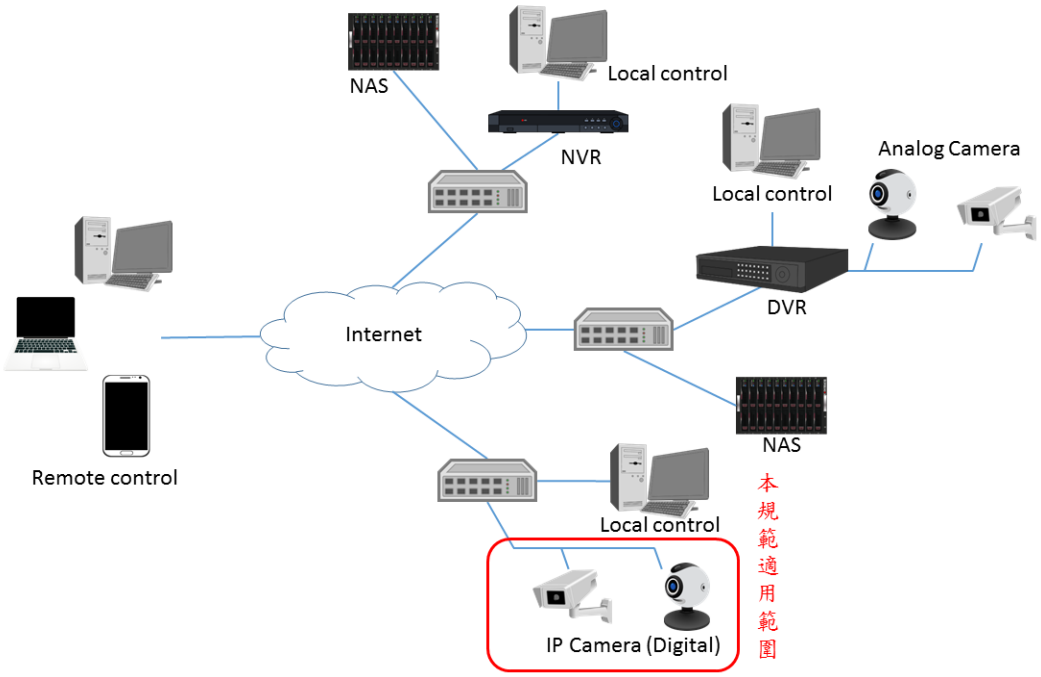

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。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。

TAICS TS-0014-2 影像監控系統資安標準-網路攝影機

3. 用語及定義

TAICS TS-0014-2 所規定之用語及定義適用於本規範。

3.1. 密碼套件 (Cipher Suite)

係指使用於安全通道(SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(MAC)和金鑰交換演算法。

3.2 除錯模式 (Debug Mode)

又稱工程模式(Engineer Mode)，一般於開發或修補階段，產品會處在此模式下，此模式可存取之系統資源不會受限，且還會顯示錯誤訊息提供工程人員除錯用。

3.3 網路埠掃描 (Port Scan)

網路埠，又稱為通訊埠或者連接埠，作為連網裝置與外部來源之間傳送/接收通訊資料，一般駭客使用網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，進一步探尋其漏洞，藉此找到未經授權的存取點。

4. 測試項目分級

本節依據影像監控系統資安標準-網路攝影機制定相對應之安全測試項目及測試標準。

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、隱私保護；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品須先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試標準等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
實體安全	5.1.1. 實體埠之安全管控測試	5.1.1.1	5.1.1.2	-
	5.1.2. 實體異常行為警示測試	-	5.1.2.1	-
	5.1.3. 實體防護測試	-	5.1.3.1	5.1.3.2
	5.1.4. 安全啟動測試	-	-	5.1.4.1
系統安全	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. 操控程式之應用程式介面安全測試	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	-
通訊安全	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. 通訊介面安全設置測試	5.3.2.1	-	-
	5.3.3. 通訊協定安全測試	-	5.3.3.1	-
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全測試	5.4.1.1	-	5.4.1.2
測	5.4.2. 通行碼鑑別機制安全測試	5.4.2.1	-	-
	5.4.3. 權限管控測試	5.4.3.1	-	-
隱私保護	5.5.1. 隱私資料的存取保護測試	5.5.1.1	-	-
	5.5.2. 隱私資料的傳輸保護測試	5.5.2.1	5.5.2.2	5.5.2.3

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

5.1.1.1 實體埠安全管控測試

(a) 實體埠存取管控測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.1.1(a)。

(2) 測試目的：

- 驗證連接產品實體埠時，可否存取作業系統之除錯模式。 (3) 樣品條件：

- 產品須保持出廠預設環境狀態。
- 產品須提供進入作業系統除錯模式之方法。

(4) 測試佈局：

- 無

(5) 測試方法：

1. 根據產品所提供進入作業系統除錯模式之方法，開啟相應之管理介面連接工具。
2. 測試電腦連接產品之 USB 埠。
3. 確認可否透過 USB 埠存取作業系統之除錯模式。
4. 測試電腦連接產品之 RJ45 埠。
5. 確認可否透過 RJ45 埠存取作業系統之除錯模式。

(6) 預期結果：

- 使用者無法透過 USB、 RJ45 任一種實體埠存取作業系統之除錯模式。

- 產品若存在作業系統之除錯模式，須通過身分鑑別方可存取作業系統之除錯模式。
- 產品若不存在作業系統之除錯模式，則此測項為「通過」。

5.1.1.2 最小實體介面測試

(a) 最小實體介面測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.1.2(a)。

(2) 測試目的：

- 驗證是否可輕易從產品外部取得儲存媒體。

(3) 樣品條件：

無。(4) 測試佈局：

- 無。

(5) 測試方法：

- 目視產品外觀(不包括設計上須緊靠牆壁該面)，是否存在 SD card 插槽。

(6) 預期結果：

- 產品不存在外接式儲存媒體使用的 SD card 插槽。

(b) 實體埠插拔操作記錄功能

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.1.2(b)。

(2) 測試目的：

- 驗證產品實體介面之插拔是否有紀錄。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 由於產品之更新可能透過電腦或行動裝置上之操控程式，或者是網頁管理介面，因此測試架構如圖 2。

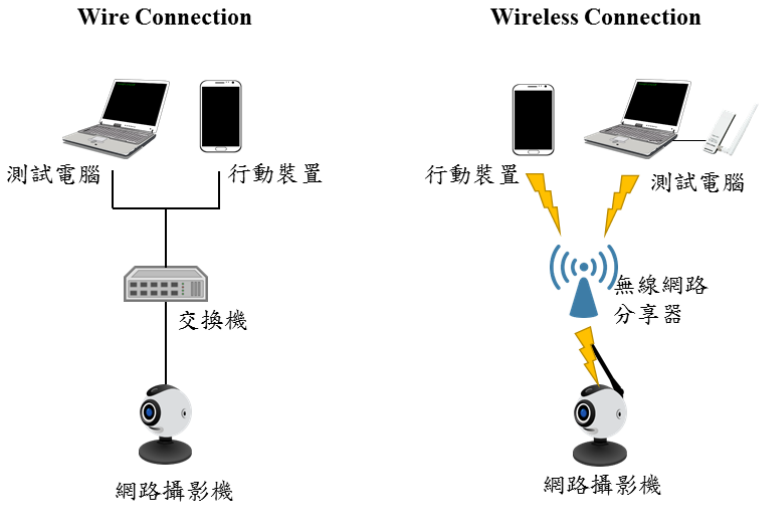

圖 2 測試示意圖

(5) 測試方法：

1. 根據產品使用說明，開啟相應之管理介面連接工具。
2. 插拔 USB 埠，檢視插拔紀錄。
3. 插拔 RJ45 埠，檢視插拔紀錄。

(6) 預期結果：

- 產品須具有實體埠插拔記錄功能，包括 USB 埠與 RJ45 埠。
- 該實體埠插拔記錄之時間須正確。

5.1.2 實體異常行為警示測試

5.1.2.1 異常狀態警示機制

(a) 異常狀態警示機制 (選測)

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.2.1(a)。

(2) 測試目的：

- 驗證產品遭受實體層之服務阻絕時，是否有相應之警示機制。

(3) 樣品條件：

- 產品應在通電的狀態下。

(4) 測試佈局：

- 無

(5) 測試方法：

1. 根據產品使用說明。
2. 將網路線拔除或天線遮罩，使操控主機因訊號中斷而無法存取產品。
3. 檢視產品是否依照使用說明達到警示效果。
4. 將產品電源拔除。
5. 檢視產品是否依照使用說明達到警示效果。

(6) 預期結果：

- 產品發生斷電與斷訊狀況時，產品須具備警示機制。

5.1.3 實體防護測試

5.1.3.1 實體保護測試

(a) 實體保護測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.3.1(a)。

(2) 測試目的：

- 驗證產品是否建立外殼拆除障礙。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 無

(5) 測試方法：

1. 目視產品之外殼是一體成型。
2. 目視產品之外殼經防拆螺絲鎖住。

(6) 預期結果：

- 產品採用一體成形或防拆螺絲等機殼防拆除保護設計。

5.1.3.2 實體設計安全測試

(a) 內部實體安全測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.3.2(a)。

(2) 測試目的：

- 驗證產品是否建立實體介面存取障礙。

(3) 樣品條件：

- 一體成型之產品不適用此測試項目。

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 卸除防拆螺絲以拆開產品外殼。
2. 目視晶片上是否存在編號。
3. 目視電路板上是否存在功能編號。

(6) 預期結果：

- 晶片編號不存在於晶片上與功能編號不存在於電路板上。

(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-網路攝影機」5.1.3.2(b)。

(2) 測試目的：

- 驗證產品實體層的通行碼還原設計，是否考量安全防護機制。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 目視產品外觀(不包括設計上須緊靠牆壁該面)，是否存在徒手即可輕易還原預設通行碼之設計。

(6) 預期結果：

- 產品外觀不存在徒手即可輕易還原回預設通行碼的設計。

5.1.4 安全啟動測試

5.1.4.1 安全啟動測試

(a) 測試產品是否支援安全啟動(secure boot)功能。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.1.4.1(a)。

(2) 測試目的：

- 驗證產品於開機階段是否檢驗產品之完整性。

(3) 樣品條件：

- 產品須提供安全啟動功能之設計文件。

(4) 測試佈局：

- 無。

(5) 測試方法：

- 審閱具備安全啟動功能證明之書面資料。

(6) 預期結果：

- 書面資料證實產品具備安全啟動之設計。

5.2 系統安全測試

檢視網路攝影機之系統安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.2.1 作業系統安全與網路服務安全測試

5.2.1.1 作業系統與網路服務常見弱點與漏洞初階測試

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

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.1.1(a)。

(2) 測試目的：

- 驗證產品之作業系統與網路服務是否存在已知重大資安風險之漏洞。

(3) 樣品條件：

- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 系統安全測試架構，如圖 3 所示，可採用有線或無線連線方式與產品建立鏈結，包括測試電腦(供測試人員連線至網路攝影機之終端設備)、有線連線(乙太網路線或光纖纜線)、無線連線與受測之網路攝影機，用以測試受測裝置是否符合測試規範。

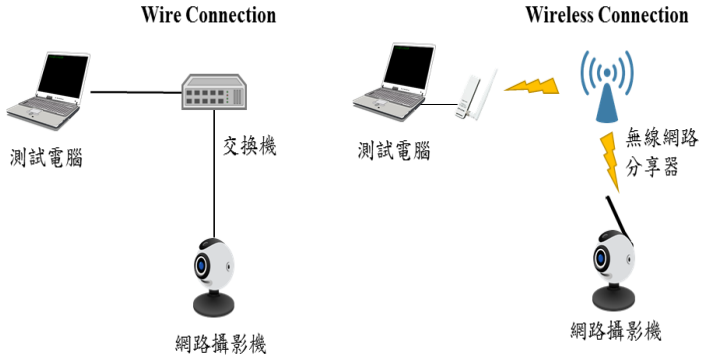

圖 3 測試示意圖

(5) 測試方法：

1. 將測試電腦連接產品。
2. 啟動具作業系統及網路服務弱點掃描功能之工具，對產品執行弱點掃描。
3. 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。

(6) 預期結果：

- 作業系統與網路服務不存在 CVSS v3 評分為最高風險 9 分以上之資安漏洞。

5.2.1.2 作業系統與網路服務常見弱點與漏洞中階測試

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

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.1.2(a)。

(2) 測試目的：

- 驗證產品之作業系統與網路服務是否存在已知高資安風險之漏洞。

(3) 樣品條件：

- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 參照圖 3。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 啟動具作業系統及網路服務弱點掃描功能之工具，對產品執行弱點掃描。
3. 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。

(6) 預期結果：

- 作業系統與網路服務不存在 CVSS 評分為最高風險 7 分以上之資安漏洞。

5.2.2 網路服務連接埠管控測試

5.2.2.1 網路服務最小化測試

(a) 測試所啟用之網路服務與產品自我宣告之一致性。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.2.1(a)。

(2) 測試目的：

- 驗證產品是否存在未知之網路埠。

(3) 樣品條件：

- 產品須保持出廠預設環境狀態。
- 產品須提供所啟用之網路服務與對應埠之宣告。

(4) 測試佈局：

- 參照圖 3。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 啟動具網路埠掃描功能之工具，對產品執行 TCP 埠、UDP 埠及埠 0 之掃描。
3. 目視掃描結果所呈現之網路服務與對應埠。
4. 比對產品自我宣告中所聲明之網路服務與對應埠。

(6) 預期結果：

- 產品所開啟之網路服務與對應埠，與產品自我宣告之內容相符。

5.2.3 更新安全測試

5.2.3.1 韌體更新機密性測試

(a) 韌體程式更新功能測試。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.3.1(a)。

(2) 測試目的：

- 驗證產品是否具備持續更新的能力。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 若提供離線更新，檢視操控程式或網頁管理介面是否具備檔案更新操作介面。
4. 若提供線上更新，檢視操控程式或網頁管理介面是否具備線上更新操作介面。

(6) 預期結果：

- 產品支援更新機制。

(b) 韌體程式更新測試 - 更新檔案的保護。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.3.1(b)。

(2) 測試目的：

- 驗證產品之韌體更新檔是否經過加密保護。

(3) 樣品條件：

- 產品須支援離線更新，否則不適用此測項。
- 產品須提供所使用之加密演算法書面資料作為審查依據。

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 使用具韌體拆解功能之工具，對產品之韌體進行拆解。
2. 檢視該韌體更新檔是否可被解析出檔案系統目錄。
3. 審閱可證明所使用加密演算法之書面資料。

(6) 預期結果：

- 韌體更新檔案無法被解析出檔案系統目錄。
- 加密演算法並無使用列於「附錄 A」之公認弱加密演算法。

(c) 韌體程式更新測試 - 更新路徑的保護。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.3.1(c)。

(2) 測試目的：

- 驗證產品的韌體線上更新是否具備傳輸加密。

(3) 樣品條件：

- 產品須支援線上更新，否則不適用此測項。
- 產品須提供所有相連伺服器之宣告。

(4) 測試佈局：

- 韌體線上更新之測試架構如圖 4，測試對象為產品更新所需要之更新伺服器。

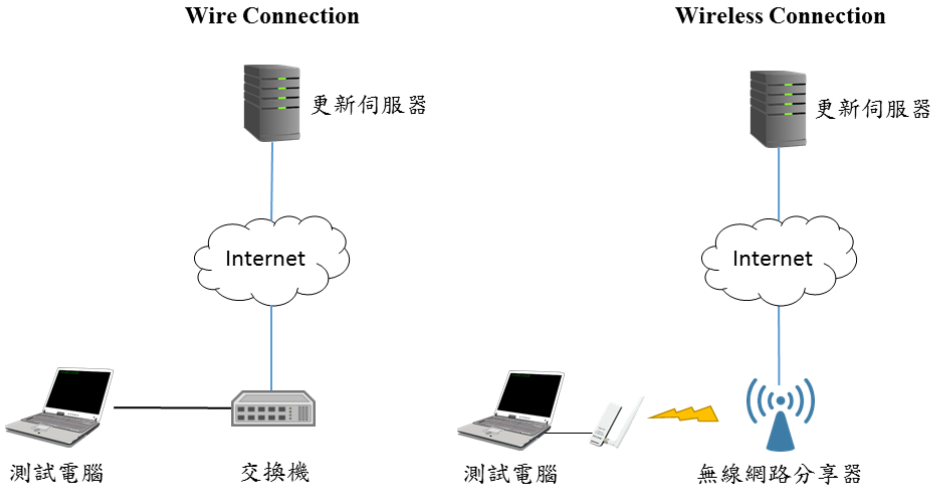

圖 4 測試示意圖

(5) 測試方法：

1. 啟動安全通道掃描工具，對更新伺服器進行掃描。
2. 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 B 之要求。
3. 檢視產品是否存在支援超文本傳輸協定(HTTP)之線上更新頁面。

(6) 預期結果：

- 產品之線上更新，其更新路徑須通過安全通道，且安全通道只可支援「附錄 B」中所建議之密碼套件。

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測試。

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.3.2(a)。

(2) 測試目的：

- 驗證產品是否具備完整性與不可否認性之韌體更新檔案驗證功能。

(3) 樣品條件：

- 產品須支援離線更新，否則不適用此測項。

- 產品須提供所使用之數位簽章書面資料作為審查依據。

(4) 測試佈局：

- 無。

(5) 測試方法：

. 審閱可證明所使用數位簽章之書面資料。

(6) 預期結果：

- 書面資料證實產品具備驗證韌體完整性與不可否認性之設計。。

5.2.4 韌體程式安全測試

5.2.4.1 敏感性資料外洩測試 (選測)

(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-網路攝影機」5.2.4.1(a)。

(2) 測試目的：

- 驗證產品之韌體檔案是否洩露敏感性資料。

(3) 樣品條件：

- 若韌體檔案經過加密處理，則廠商須提供解密工具。
- 產品須提供所有相連伺服器之宣告

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 使用具韌體拆解功能之工具，對產品之韌體進行拆解。
2. 取出檔案系統之路徑目錄。
3. 確認系統通行碼資料是否可識別。
4. 確認金鑰是否可被擷取。
5. 確認是否存在非公開之 email 資料。
6. 確認是否存在產品所宣告之相連伺服器外之 IP 資料。
7. 確認是否存在產品所宣告之相連伺服器外之 URL 資料。

(6) 預期結果：

- 產品之程式碼與安裝檔內其他檔案，無檢出身分鑑別因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)。
- 若韌體檔無法被拆解，此測項為「不通過」。

5.2.5 敏感性資料儲存安全測試

5.2.5.1 敏感性資料的儲存保護初階測試

(a) 敏感性資料加密儲存測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.5.1(a)。

(2) 測試目的：

- 驗證產品之敏感性資料於儲存狀態下是否加密保護。

(3) 樣品條件：

- 產品須提供敏感性資料保存方式之書面資料作為審查依據。
- 產品須提供敏感性資料儲存加密演算法之書面資料作為審查依據。

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 審閱能證明符合此安全要求之書面資料。

(6) 預期結果：

- 身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不是明文儲存。
- 保護資料的加密方式不為「附錄 A」所列之公認弱加密演算法。

5.2.5.2 機敏性資料的儲存保護中階測試

(a) 敏感性資料隔離保護測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.5.2(a)。

(2) 測試目的：

- 確認產品敏感性資料之存放與正常作業系統隔離。

(3) 樣品條件：

- 產品須提供敏感性資料保存方式之書面資料作為審查依據。
- 產品須提供支援安全區域功能之書面資料作為審查依據。

(4) 測試佈局：

- 無。

(5) 測試方法：

1. 審閱具備此功能證明之書面資料。

(6) 預期結果：

- 書面資料證實產品之敏感性資料存放於安全區域。

5.2.6 網頁管理介面安全測試

5.2.6.1 網頁管理介面常見資安風險測試

(a) 網頁管理介面弱點測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.6.1(a)。

(2) 測試目的：

- 驗證產品之網頁管理介面是否存在已知資安漏洞。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 3。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。
3. 啟動具備網頁弱點掃描功能之工具，對產品網頁介面執行弱點掃描。
4. 檢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。

(6) 預期結果：

- 產品之網頁管理介面，不存在引發 OWASP web Top 10 [**2**]之 Injection 及 Cross-Site Scripting (XSS)資安攻擊風險。
- 產品之網頁管理介面不支援超文本傳輸協定。
- 產品不支援網頁管理介面，則此測項為「通過」。

5.2.7 操控程式之應用程式介面安全測試

5.2.7.1 應用程式介面之鑑別機制強度測試

(a) 應用程式介面之鑑別機制

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.7.1(a)。

(2) 測試目的：

- 驗證產品的應用程式介面呼叫是否經過身分鑑別程序。

(3) 樣品條件：

- 產品須具備電腦或行動裝置之操控程式介面，否則此測項不適用。
- 若應用程式介面之身分鑑別與授權機制和 5.4 身分鑑別與授權機制為同一組時，此項不測。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟電腦或行動裝置之操控程式。
3. 透過操控程式與產品建立連線，同時側錄封包。
4. 呼叫資源存取相關之應用程式介面，檢視封包側錄結果是否要求身分鑑別。
5. 若產品要求身分鑑別，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。
6. 檢視鑑別結果是否成功。
7. 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。

(6) 預期結果：

- 呼叫資源存取相關之應用程式介面時，須經過身分鑑別。
- 針對應用程式介面之身分鑑別發動重送攻擊失敗。

- 從鑑別錯誤訊息無法推斷出合法使用者名稱。

(b) 應用程式介面之通行碼鑑別

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.7.1(b)。

(2) 測試目的：

- 驗證產品的應用程式介面通行碼鑑別機制強度是否足夠。

(3) 樣品條件：

- 產品須具備電腦或行動裝置之操控程式介面，否則此測項不適用。
- 產品應用程式介面之呼叫應要求通行碼鑑別，否則此測項不適用。
- 若應用程式介面之身分鑑別與授權機制和 5.4 身分鑑別與授權機制為同一組時，此項不測。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟電腦或行動裝置之操控程式。
3. 透過操控程式與產品建立連線，同時側錄封包。
4. 呼叫資源存取相關之應用程式介面。
5. 於產品要求通行碼鑑別時，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。
6. 於產品要求通行碼鑑別時，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。
7. 於產品要求通行碼鑑別時，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。

8. 於產品要求通行碼鑑別時，輸入與現行相同之通行碼，檢查通行碼是否能成功變更。
9. 比對任二台網路攝影機應用程式介面的預設通行碼是否相異。
10. 確認在未設定新通行碼的情況下，是否可存取產品資源或行使產品任一功能。
11. 確認首次取得應用程式介面的授權後，是否強制要求更改預設通行碼。
12. 於產品要求通行碼鑑別時，不斷輸入錯誤的通行碼。
13. 檢視產品被鎖定的嘗試登入失敗次數最多不可超過 5 次。
14. 檢視產品重設帳戶鎖定計數器的時間間隔至少要為 1 分鐘。
15. 檢視產品之帳戶鎖定期間至少 1 分鐘以上。

(6) 預期結果：

- 資源存取相關之應用程式介面，其通行碼鑑別之通行碼長度必須符合政府組態基準 CCE-33789-9。
- 資源存取相關之應用程式介面，其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。
- 資源存取相關之應用程式介面，其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。
- 資源存取相關之應用程式介面，其 2 台產品的預設通行碼相異或者未經設定新通行碼前無法存取產品。
- 資源存取相關之應用程式介面，於首次取得授權後，產品強制要求更改預設通行碼。
- 資源存取相關之應用程式介面，其通行碼輸入次數必須符合最高 5 次嘗試登入失敗即鎖定帳戶。
- 資源存取相關之應用程式介面，其通行碼輸入頻率必須符合帳戶鎖定計數器至少 1 分鐘以上的時間間隔，失敗的登入嘗試計數器方可重設為 0 次失敗。
- 資源存取相關之應用程式介面，其通行碼輸入頻率必須符合帳戶鎖定期間至少 1 分鐘以上，系統方可解除鎖定。

(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-網路攝影機」5.2.7.1(c)。

(2) 測試目的：

- 驗證產品的應用程式介面是否存在權限控管。

(3) 樣品條件：

- 產品須具備電腦或行動裝置之操控程式介面，否則此測項不適用。
- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。
- 若應用程式介面之身分鑑別與授權機制和 5.4 身分鑑別與授權機制為同一組時，此項不測。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟電腦或行動裝置之操控程式。
3. 透過操控程式與產品建立連線，分別以不同角色呼叫資源存取相關之應用程式介面。
4. 同時檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(6) 預期結果：

- 資源存取相關之應用程式介面，必須具備權限管控機制，該使用者的身分授權須與產品自我宣告相符。
- 至少要有二個以上不同權限的角色。

5.2.8 系統日誌檔與警示測試

5.2.8.1 安全事件日誌檔測試

(a) 安全事件日誌檔測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.8.1(a)。

(2) 測試目的：

- 驗證產品是否有安全事件紀錄供查詢。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具，瀏覽安全事件日誌。
3. 檢視日誌內容是否記載使用者的登入紀錄。
4. 檢視該日誌之登入紀錄是否提供正確時間與使用者身分資訊。

(6) 預期結果：

- 產品具有可供使用者檢視之安全事件日誌功能。
- 安全事件日誌的資料應包含正確時間、使用者身分及登入行為。

(b) 存取權限管控測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.8.1(b)。

(2) 測試目的：

- 驗證產品之安全事件日誌紀錄是否具備權限控管。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。
- 產品須提供日誌檔存取權限說明。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具，瀏覽安全事件日誌。
3. 檢視帳號之身分類型對日誌檔的存取權限是否與產品自我宣告相符。

(6) 預期結果：

- 安全事件日誌檔的身分授權與產品自我宣告相符。

(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-網路攝影機」5.2.8.1(c)。

(2) 測試目的：

- 驗證產品是否有控管日誌紀錄的保存期限。

(3) 樣品條件：

- 產品須提供日誌檔保存期限之說明文件。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 測試人員根據產品之使用說明，檢視日誌紀錄的保存期限。

(6) 預期結果：

- 產品之日誌檔具備日誌紀錄維護期限之設計。
- 須符合 NIST SP 800-92[**3**]中 high impact systems 的日誌紀錄維護期限。

5.2.8.2 異常警示功能測試

(a) 日誌檔存取異常警示測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.2.8.2(a)。

(2) 測試目的：

- 驗證產品是否具有確保日誌紀錄檔可用性之功能。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 將產品之日誌檔儲存空間填滿或者修改權限使日誌檔不可寫入。
4. 檢視產品是否依照使用說明達到警示效果。

(6) 預期結果：

- 日誌紀錄檔無法正常儲存時會發出警示。

5.3 通訊安全測試

檢視網路攝影機之通訊安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.3.1 資料傳輸安全測試

5.3.1.1 敏感性資料之傳輸保護初階測試

(a) 敏感性資料之傳輸保護初階測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.3.1.1(a)。

(2) 測試目的：

- 驗證產品之敏感性資料於傳輸過程是否具備加密保護。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 執行身分鑑別操作，同時側錄封包。
4. 檢視所側錄之封包是否採用 FIPS 140-2 所核可之對稱金鑰加解密演算法[**4**]。

(6) 預期結果：

- 敏感性資料之網路傳輸須經過加密保護，且加密演算法須採用 FIPS 140-2 所核可之對稱金鑰加解密演算法。

5.3.1.2 敏感性資料之傳輸保護中階測試

(a) 敏感性資料之傳輸保護中階測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.3.1.2(a)。

(2) 測試目的：

- 驗證敏感性資料之傳輸通道，是否經過加密保護。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 使用安全通道掃描工具。
3. 比對掃描結果是否為附錄 B 中所包含之密碼套件。
4. 根據產品使用說明，開啟相應之管理介面連接工具。
5. 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。

(6) 預期結果：

- 敏感性資料之傳輸須採用安全通道。
- 安全通道所支援之密碼套件全部皆符合附錄 B 的要求。

5.3.2 網路介面通訊協定的安全設置測試

5.3.2.1 通訊介面組態設置測試

(a) 網路裝置資訊探詢功能測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.3.2.1(a)。

(2) 測試目的：

- 確認產品是否運行在具安全風險的網路設定。

(3) 樣品條件：

- 產品須支援通用隨插即用通訊協定、簡單網路管理協定、零配置通訊協定之任一個網路服務，否則本測項不適用。
- 產品須保持出廠預設環境狀態。
- 產品須提供所支援網路服務之說明文件。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 若產品支援通用隨插即用通訊協定，目視產品之操控程式或網頁管理介面，通用隨插即用通訊協定是否存在供使用者操作的開/關介面。
4. 透過具通用隨插即用通訊協定掃描功能之工具以確認產品是否支援通用隨插即用通訊協定服務，同時確認使用者是否可自行開/關通用隨插即用通訊協定服務。
5. 若產品支援簡單網路管理協定，目視產品之操控程式或網頁管理介面，簡單網路管理協定是否存在供使用者操作的開/關介面。
6. 透過具簡單網路管理協定掃描功能之工具以確認產品是否支援簡單網路管理協定服務，同時確認使用者是否可自行開/關簡單網路管理協定服務。

7. 若產品支援零配置通訊協定，目視產品之操控程式或網頁管理介面，零配置通訊協定是否存在供使用者操作的開/關介面，且預設為關閉。
8. 透過具零配置通訊協定掃描功能之工具以確認產品是否支援零配置通訊協定服務，同時確認使用者是否可自行開/關零配置通訊協定服務。

(6) 預期結果：

- 若產品支援通用隨插即用通訊協定服務，該服務提供使用者可自行開/關功能之設置。
- 若產品支援簡單網路管理協定服務， 該服務提供使用者可自行開/關功能之設置。
- 若產品支援零配置通訊協定服務，該服務提供使用者可自行開/關功能之設置。
- 若產品支援簡單網路管理協定服務， 簡單網路管理協定服務預設應為關閉。
- 若產品支援零配置通訊協定服務，零配置通訊協定服務預設應為關閉。

(b) 安全的 Wi-Fi 組態設置測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.3.2.1(b)。

(2) 測試目的：

- 驗證產品是否存在錯誤的 Wi-Fi 設定。

(3) 樣品條件：

- 產品須支援 Wi-Fi 保護設置功能，否則此測項不適用。
- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。

3. 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。

(6) 預期結果：

- 有提供使用者 WPS PIN 開/關之功能。
- WPS PIN 功能預設為關閉。

(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-網路攝影機」5.3.2.1(c)。

(2) 測試目的：

- 驗證產品是否存在不安全的 Wi-Fi 通道保護設定

(3) 樣品條件：

- 產品需支援 Wi-Fi 功能，否則此測項不適用。
- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 與產品建立連線，同時側錄 Wi-Fi 封包。
4. 根據側錄結果確認傳輸是否採用「Wi-Fi 保護存取 2」加密方式。

(6) 預期結果：

- Wi-Fi 預設加密模式為「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-網路攝影機」5.3.2.1(d)。

(2) 測試目的：

- 驗證產品不提供遠端存取作業系統除錯模式之設計。

(3) 樣品條件：

- 產品須保持出廠預設環境狀態。
- 產品須提供進入作業系統除錯模式之方法。

(4) 測試佈局：

- 參照圖 3。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 檢視可否透過產品所開啟之網路服務連接埠存取作業系統之除錯模式。

(6) 預期結果：

- 使用者無法透過有線或無線之網路連結方式存取作業系統之除錯模式。
- 產品若存在作業系統之除錯模式，存取作業系統之除錯模式應經過身分鑑別。
- 產品若不存在作業系統之除錯模式，則此測項為「通過」。

5.3.3 通訊協定安全測試

5.3.3.1 通訊協定異常輸入測試

(a) 通訊協定異常輸入測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.3.3.1(a)。

(2) 測試目的：

- 驗證產品之通訊協定是否存在未知之資安漏洞。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 3。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 啟動具模糊測試功能之工具。
3. 執行對「附錄 C」中每一種類之通訊協定所有欄位至少 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。
4. 對產品執行影像監控之操作，檢查產品是否仍正常運作。

(6) 預期結果：

- 通訊協定必須經過異常輸入測試，產品於測試過程中不應發生程序崩潰(crash)到無法恢復運作。

5.4 身分鑑別與授權機制安全測試

檢視網路攝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

5.4.1.1 鑑別機制強度初階測試

(a) 鑑別機制強度測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.1.1(a)。

(2) 測試目的：

- 驗證產品是否具備可靠之身分鑑別機制。

(3) 樣品條件：

- 產品之用戶帳號已經建立。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 執行身分鑑別操作，同時側錄封包，並檢視是否確實執行身分鑑別。
4. 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。
5. 檢視鑑別結果是否成功。
6. 執行產品登出並再次登入，檢視身分鑑別功能是否正常執行。

(6) 預期結果：

- 無論透過網頁管理介面或操控程式存取網路攝影機時，皆須經過身分鑑別程序。

- 身分鑑別機制具備抵抗重送攻擊的能力。
- 使用者可以成功登出產品。
- 使用者成功登出後，可以再次手動登入產品。

(b) 身分鑑別錯誤訊息

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.1.1(b)。

(2) 測試目的：

- 驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。

(3) 樣品條件：

- 產品之用戶帳號已經建立。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦連接產品。
2. 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。
3. 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。

(6) 預期結果：

- 從鑑別錯誤訊息無法推斷出合法使用者名稱。

(c) 裝置鑑別測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.1.1(c)。

(2) 測試目的：

- 產品須提供能鑑別相連之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) 樣品條件：

- 產品須具備與網路影像錄影機相連之能力，否則此測項不適用。
- 產品之用戶帳號已經建立。
- 產品須提供與其相連之網路影像錄影機。

(4) 測試佈局：

- 此測試須搭配網路影像錄影機，測試架構如下圖。

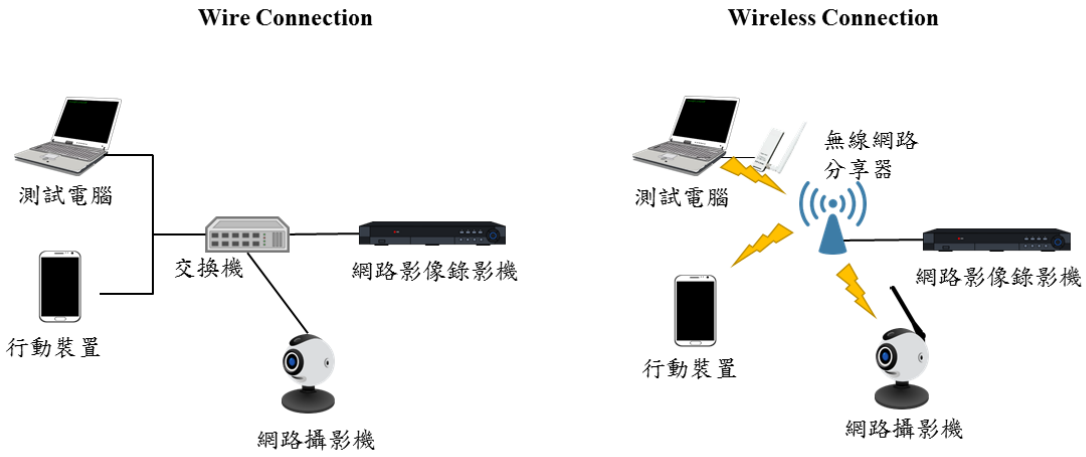

圖 5. 測試示意圖

(5) 測試方法：

1. 將產品與其它影像監控系統裝置建立連線。
2. 將測試電腦或行動裝置連接其它影像監控系統裝置。
3. 檢查是否要求對連裝置之身分鑑別。
4. 執行身分鑑別操作，同時側錄封包。
5. 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。
6. 檢視鑑別結果是否成功。

(6) 預期結果：

- 其它影像監控系統裝置與產品建立連線時，須經過裝置身分鑑別。
- 該裝置鑑別機制具備抵抗重送攻擊的能力。

(d) 憑證鑑別有效性測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.1.1(d)。

(2) 測試目的：

- 驗證產品是否具有鑑別憑證有效性之能力。

(3) 樣品條件：

- 產品之用戶帳號已經建立。
- 產品須支援憑證鑑別機制。

(4) 測試佈局：

- 參照圖 5。

(5) 測試方法：

1. 將產品與其它影像監控系統裝置建立連線。
2. 將測試電腦或行動裝置連接其它影像監控系統裝置。
3. 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。
4. 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。
5. 檢視憑證鑑別是否成功。

(6) 預期結果：

- 採用憑證鑑別須確保憑證有效性。

5.4.1.2 鑑別機制強度中階測試

(a) 鑑別機制強度測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.1.2(a)。

(2) 測試目標：

- 驗證裝置之身分鑑別機制是否支援多因子認證之強認證機制。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，且多因子鑑別功能已經啟用。
- 須提供具多因子鑑別操作之產品說明文件。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 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。
3. 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鑑別因子。
4. 檢查鑑別過程中是否採用短訊服務(Short Message Service, SMS)獲取通行碼。
5. 檢查鑑別過程中，使用行動裝置作為所持之物(what you have)之鑑別因子時，檢視是否能同時在 2 台以上的行動裝置上獲取鑑別因子。

(6) 預期結果：

- 網頁管理介面或操控程式與產品之間的身分鑑別，透過多因子身分鑑別。
- 每一階段身分鑑別皆採用不同種類的鑑別因子
- 當使用所持之物作為鑑別因子時，沒有採用短訊服務獲取通行碼。
- 當使用所持之作為鑑別因子時，不可同時從 2 台以上行動裝置的應用程式獲取通行碼。

5.4.2 通行碼鑑別安全測試

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-網路攝影機」5.4.2.1(a)。

(2) 測試目的：

- 驗證產品的通行碼鑑別機制強度是否足夠。

(3) 樣品條件：

- 產品須支援通行碼鑑別機制，否則此測項不適用。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 從網頁管理介面或操控程式建立或變更通行碼。
3. 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。
4. 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。
5. 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。
6. 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。

(6) 預期結果：

- 通行碼鑑別之通行碼長度符合政府組態基準 CCE-33789-9。
- 通行碼鑑別之通行碼複雜度符合政府組態基準 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-網路攝影機」5.4.2.1(b)。

(2) 測試目的：

- 驗證產品是否有相同的預設通行碼。

(3) 樣品條件：

- 產品須支援通行碼鑑別機制，否則此測項不適用
- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 準備 2 台以上產品。
2. 將測試電腦或行動裝置連接產品。
3. 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。
4. 比對 2 台網路攝影機的預設通行碼是否相異。
5. 確認在未設定新通行碼的情況下，是否可存取產品資源或行使產品任一功能。

(6) 預期結果：

- 2 台產品的預設通行碼相異。
- 未經設定新通行碼前無法存取產品。
- 以上二項預期結果滿足其中一項即可。

(c) 通行碼變更機制

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.2.1(c)。

(2) 測試目的：

- 確保上線之產品不存在預設密碼。

(3) 樣品條件：

- 產品須支援通行碼鑑別機制，否則此測項不適用
- 產品須保持出廠預設環境狀態。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 從網頁管理介面或操控程式輸入通行碼。
3. 確認首次取得授權後，是否強制要求更改預設通行碼。

(6) 預期結果：

- 首次取得授權後，產品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-網路攝影機」5.4.2.1(d)。

(2) 測試目的：

- 驗證通行碼鑑別機制是否有防止暴力破解之能力。

(3) 樣品條件：

- 產品須支援通行碼鑑別機制，否則此測項不適用
- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。

2. 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
3. 不斷輸入錯誤的通行碼。
4. 檢視產品被鎖定的嘗試登入失敗次數最多不可超過 5 次。
5. 檢視產品重設帳戶鎖定計數器的時間間隔至少要為 1 分鐘。
6. 檢視產品之帳戶鎖定期間至少 1 分鐘以上。

(6) 預期結果：

- 通行碼輸入次數符合最高 5 次嘗試登入失敗即鎖定帳戶。
- 通行碼輸入頻率符合帳戶鎖定計數器至少 1 分鐘以上的時間間隔，失敗的登入嘗試計數器方可重設為 0 次失敗。
- 通行碼輸入頻率符合帳戶鎖定期間至少 1 分鐘以上，系統方可解除鎖定。

5.4.3 權限管控測試

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-網路攝影機」5.4.3.1(a)。

(2) 測試目的：

- 驗證產品資源的存取是否具有權限控管機制。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。
- 產品須提供角色存取權限之宣告。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 透過網頁管理介面或操控程式，分別以不同角色登入產品。
3. 存取產品資源，同時檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
4. 若為網頁管理介面，嘗試以同一頁面讓不同權限的角色存取。

(6) 預期結果：

- 具備權限管控機制，該使用者的身分授權須與產品自我宣告相符。
- 至少擁有二個以上不同權限的角色。

(b) 權限有效時間

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.4.3.1(b)。

(2) 測試目的：

- 驗證產品是否存在有限的授權時間長度。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 透過網頁管理介面或操控程式登入產品。
3. 目視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。
4. 閒置產品直到超過閒置時限值。
5. 檢視是否需要重新鑑別才可存取產品。

(6) 預期結果：

- 產品之授權行為，存在閒置時限供使用者設定。
- 遠端連線逾時、遺失或結束，須要求新的身分鑑別。

5.5 隱私保護測試

檢視網路攝影機之隱私保護需求是否符合書面送審資料，並依下列各測試項目進行實機測試。在本測試規範中，隱私資料泛指從網路攝影機端所收集到的影音或使用者資訊。

5.5.1 隱私資料的存取保護測試

5.5.1.1 隱私資料權限管控測試

(a) 隱私資料的存取控制

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.1.1(a)。

(2) 測試目的：

- 驗證產品隱私權的存取是否具有權限控管機制。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。
- 產品須提供隱私存取權限之宣告。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 透過網頁管理介面或操控程式，以不同角色登入產品。
3. 存取影像資料，同時檢視該帳號之身分類型與其對應之隱私存取權限是否與產品自我宣告相符。

4. 當產品提供網頁管理介面時，以一般使用者角色瀏覽僅供系統管理者角色存取之頁面，檢視該帳號之身分類型與其對應之隱私存取權限是否與產品自我宣告相符。

(6) 預期結果：

- 產品所儲存的隱私資料，具備權限管控機制，該使用者的隱私存取授權須與產品自我宣告相符。
- 至少擁有二個以上不同權限的角色。

(b) 隱私資料刪除功能

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.1.1(b)。

(2) 測試目的：

- 驗證使用者擁有刪除自身隱私權的權限。

(3) 樣品條件：

- 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。
- 每一角色已建立所屬之影像及用戶資訊。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 透過網頁管理介面或操控程式，以不同角色登入產品。
3. 目視產品之操控程式或網頁管理介面，影像資料是否存在供使用者刪除的操作介面。
4. 執行刪除功能後，確認產品之隱私資料已被移除。

(6) 預期結果：

- 提供使用者刪除隱私資料的功能。
- 隱私資料確實刪除。

(c) 登入警示功能測試

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.1.1(c)。

(2) 測試目的：

- 驗證產品是否具有防止隱私外洩之功能。
- 產品設計上須緊貼牆壁該平面，不被視為外觀。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 透過網頁管理介面或操控程式，以不同角色登入產品。
3. 根據產品使用說明，無論登入成功與否，確認是否接收到登入警示。
4. 若收到登入警示，則本測試項目通過，測試結束。
5. 根據產品使用說明，目視產品外部是否設置狀態指示燈。
6. 目視產品外觀之狀態指示燈是否亮起。

(6) 預期結果：

- 每次發生新的產品存取事件時，產品必須主動發出警示。
- 只要有人登入產品則外殼之狀態指示燈亮起。
- 以上二項預期結果擇一通過，本測試項目結果為通過。

5.5.2 隱私資料的傳輸保護測試

5.5.2.1 隱私資料的傳輸初階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.2.1(a)。

(2) 測試目的：

- 驗證產品隱私資料的傳輸是否經過加密保護。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 根據產品使用說明，開啟相應之管理介面連接工具。
3. 啟動影像監控功能，同時側錄封包。
4. 檢視所側錄有關影像資料之封包是否採用「附錄 A」之公認弱加密演算法。
5. 於管理介面輸入用戶資訊，同時側錄封包。
6. 檢視所側錄有關用戶資訊之封包是否採用 FIPS 140-2 所核可之演算法。

(6) 預期結果：

- 影像類隱私資料不以明文的方式傳輸，且保護資料的加密方式不應使用列於「附錄 A」之公認弱加密演算法。
- 非影像類隱私資料之傳輸加密演算法須支援 FIPS 140-2 所核可之加密演算法。

5.5.2.2 隱私資料的傳輸中階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.2.2(a)。

(2) 測試目的：

- 驗證產品隱私資料於傳輸過程中是否有加密保護。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 對產品使用安全通道掃描工具。
3. 比對掃描結果是否為附錄 B 中所包含之密碼套件。
4. 啟動影像監控功能，同時側錄封包。
5. 檢視所側錄之封包是否採用安全通道。
6. 於管理介面輸入用戶資訊，同時側錄封包。
7. 檢視所側錄之封包是否採用安全通道。

(6) 預期結果：

- 影像資料與用戶資訊之傳輸皆須採用安全通道。
- 安全通道所有支援之密碼套件須符合附錄 B 的要求。

5.5.2.3 隱私資料的傳輸高階保護

(a) 隱私資料的傳輸機密性

(1) 測試依據：

「影像監控系統資安標準-網路攝影機」5.5.2.3(a)。

(2) 測試標準：

- 驗證產品隱私資料之傳輸保護，是否支援強加密演算法。

(3) 樣品條件：

- 無。

(4) 測試佈局：

- 參照圖 2。

(5) 測試方法：

1. 將測試電腦或連接產品。
2. 對產品使用安全通道掃描工具。
3. 比對掃描結果是否為附錄 B 中所包含之密碼套件，且支援 AES-256 加密演算法。
4. 啟動影像監控功能，同時側錄封包。
5. 檢視所側錄之封包是否採用安全通道。
6. 於管理介面輸入用戶資訊，同時側錄封包。
7. 檢視所側錄之封包是否採用安全通道。

(6) 預期結果：

- 確保隱私資料之網路傳輸加密演算法須支援 AES-256。

附錄 A
(規定)
公認之弱加密演算法

A.1 BASE 64 Encode and Decode

Base64 是一種能將任意二位元資料，用 64 種字元組合成字串的方法，而這個二位元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，同時也是有線等效加密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傳輸層安全性協定中使用。

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)
安全通道建議使用之密碼套件

安全通道應使用下述幾種密碼套件：

- 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

附錄 C
(規定)
網路攝影機所使用之通訊協定

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

定義在 RFC 3550 規範中[**5**]，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[**6**]，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[**7**]，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 傳輸層安全協定(The Transport Layer Security, TLS)：

定義在 RFC 5246 規範中[**8**]，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。

參考資料

[1] TAICS TS-0014-2 影像監控系統資安標準-網路攝影機

[2] OWASP, OWASP Top 10 – 2017, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

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

[4] NIST, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017

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

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

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

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

版本修改紀錄

版本	時間	摘要
v1.0	2017/12/26	出版

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw