影像監控系統資安標準草案
–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
V0.1.0	2017/9/5	陳聰杰	無	新建立
V0.1.1	2017/9/18	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. 2.17 節內容更新為通關密語。 4. 2.18 節內容更新為預設密碼。 5. 表 1 的級等內容調整。 6. 4.4.1.1 節與 4.4.1.2 節刪除初階及高階字眼。 7. 全文「安全保證等級」改為「安全等級」。 8. 實體安全增加實體儲存安全。 9. 系統安全增加系統儲存安全。 10. 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 2.20 銷售商加載軟體 2.21 無圖示軟體 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。
V0.1.3	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 3.1.3 節。 5. 修正 4.1.3 節。 6. 修正 4.1.5 節。 7. 修正 4.2.9 節。 8. 修正 4.4.1 節。 9. 修正 4.5.1 節。 10. 與「影像監控系統資安標準之測試規範草案-影像錄影機」格式調整一致。 11. 修改安全通道由 TLS1.1 改成 TLS1.2。
V0.1.4	2017/9/30	陳聰杰	依據	1. 前言內容調整。

			2017/9/29 網路攝影機公開說明會議討論內容修改	2. 修正 5.1.1,5.1.2 及 5.1.3 節實體安全之內容。 3. 修正 5.2.3 節更新安全之內容。 4. 修正 5.2.4 節韌體程式安全之內容。 5. 修正 5.2.7 節操控程式之 API 安全之內容。 6. 修正 5.2.8 節系統日誌檔與警示之內容。 7. 修正 5.3.1 節敏感性資料傳輸安全之內容。 8. 修正 5.4.1 節認證機制安全之內容。 9. 修正 5.5.1 節應用程式的程式安全之內容。
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. 新增 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「影像錄影機」。 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 安全分級。
V0.1.6	2017/10/18	陳聰杰	依據 2017/10/17 編審會議討論內容修改	1. 修正項目之條文內容「影像錄影機」改回「產品」。 2. 新增 4.3.4 影像傳輸安全。 3. 新增 4.3.4.1(a),4.3.4.2(a),4.3.4.3(a)。 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)。
V0.1.7	2017/10/22	陳聰杰	依據 2017/10/19 專家會議討論內容	1. 調整 4.6 節的安全等級至 4 節。 2. 調整原 4 節標準規範至 5 節。 3. 修正 5.1.5.3(c)。 4. 刪除 5.2.4.2(a)。

			修改	5. 刪除 5.5.1.3(b)。 6. 全文「密碼」更新為「通行碼」。

目錄

前言

本標準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。

本標準並未建議所有安全事項，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

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

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

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

本標準旨在建立網路攝影機於產品開發階段，產品資訊安全的評估及驗證時所遵循之共同標準，用以鑑別產品之安全等級。本標準之制定係參照國際物聯網相關資安標準/規範，例如：International Organization for Standardization (ISO) 27001 [2]、Underwriters Laboratories (UL) 2900 系列標準[7]、Groupe Speciale Mobile Association (GSMA) IoT Security Guideline [1]、Open Web Application Security Project (OWASP) Top IoT Vulnerabilities [6]、ONVIF Core Specification[11]及日本政府的物聯網安全指導方針[10]等，主要規劃從五大安全構面確保影像錄影機的資訊安全，包括實體安全、系統安全、通訊安全、身分鑑別與授權機制安全及應用程式安全；同時將安全要求劃分成三個等級，詳盡載明欲實踐每一個安全要求等級的必要條件，用以界定不同產品須具備之資安要求。

在確保影像錄影機的資安品質時，應同時考量整體影像監控系統的安全性，例如: 管理影像錄影機的雲服務被駭客入侵、操控影像錄影機的行動應用程式含有軟體漏洞及資訊安全等級不足的數位/影像錄影機等因素，皆可能對影像錄影機造成資安威脅，因此建議設置時

時須參閱所有相關產品之資安標準，達到整體網路影像監控系統的安全（Security Assurance）。

1. 適用範圍

本標準應用於影像監控系統的影像錄影機，且具連網功能者皆是，如圖 1 所示。

本標準為確保影像錄影機資安，訂定其產品之安全技術要求，依實體安全、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等五大評測要項訂定其產品之安全技術要求。

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與控制輸入信號，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。

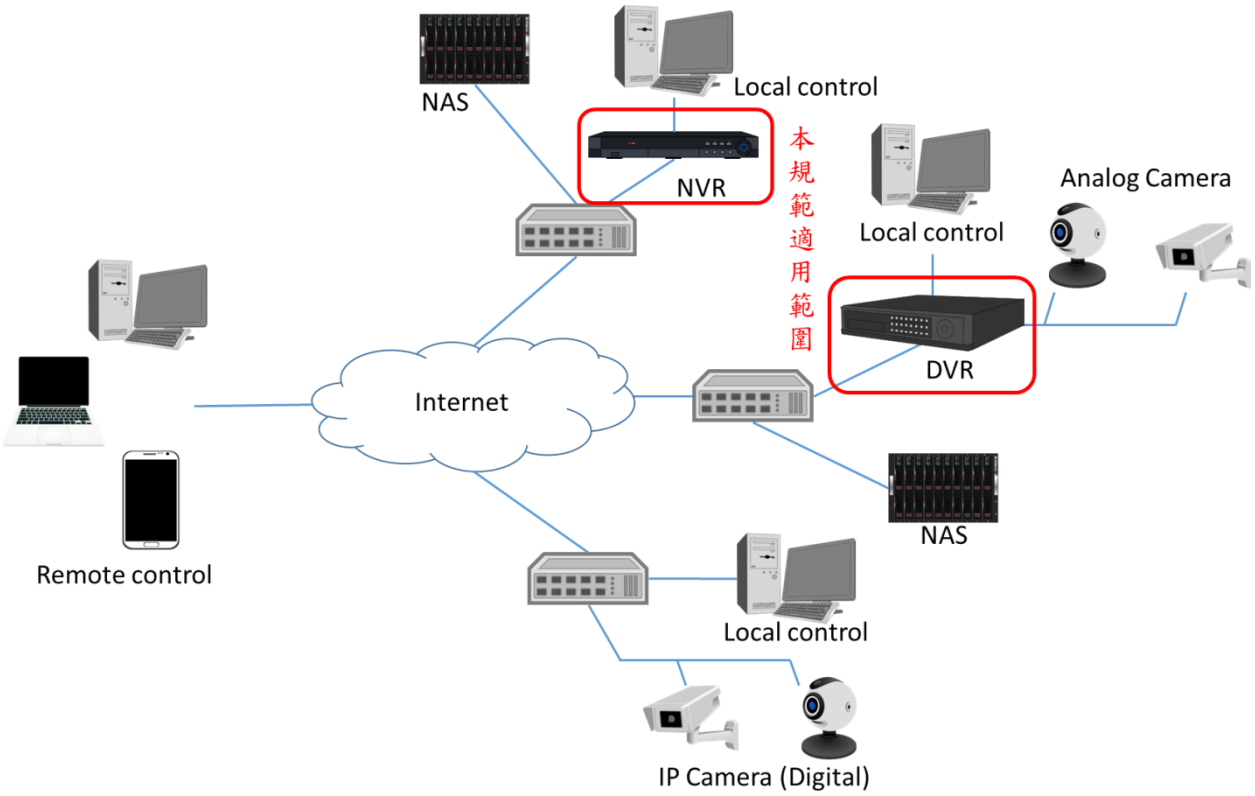

圖1. 適用範圍示意圖

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）

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號[12]。

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）[5]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）

一套公開評比企業資訊科技系統的安全性評鑑標準，CVSS 的判定標準，包括威脅所造成損害的嚴重性、資安漏洞的可利用程度、攻擊者不當運用該漏洞的難易度，都被列入評比。評分分數從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險[1]。

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）

指主要依「個人資料保護法」[19]上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.9 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行為或瀏覽監控內容之應用程式，目前可能的應用程式類型包括行動版及電腦版。

3.11 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，例如：

（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。部份影像錄影機皆提供 API 給操控端之應用程式呼叫，用戶可透過這些 API，撰寫實際實現影像錄影機相關操作（例如：監控資訊管理、遠端監控影像等）的應用程式。

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並經由數學演算法處理過後，所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）

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，例如：加解密、金鑰管理、完整性檢查，並保存敏感性資料用。

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，若無線接入點進入 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。

3.29 出廠預載軟體（Factory Preloaded Software）

影像錄影機出廠時已預設安裝之應用軟體，且使用者可透過圖示啟動。

3.30 銷售商加載軟體（The vendor loads the software）

影像錄影機銷售時預設搭載或首次連結網路後自動安裝之應用軟體，且使用者可透過圖示啟動。

3.31 無圖示軟體（No Icon Software）

於「出廠預載軟體」與「銷售商加載軟體」兩種情況所安裝之應用軟體，使用者無法透過圖示啟動，且該軟體會啟動通訊功能。

4. 安全等級

本標準旨在建立影像錄影機於產品發展階段的評估及驗證時所遵循之共同標準，用以鑑別產品之安全等級。

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

安全要求等級總表，如表 1 所示，第一欄為安全構面，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；第二欄為安全要求分項，係依第一欄安全構面設計對應之安全要求分項技術規範；第三欄為安全等級，依安全等級要求劃分成 3 個等級，按各安全要求分項規範之驗證結果，作為安全等級評估標準。且本安全要求等級總表中之各欄的關聯性，須依循第 5 節「標準規範」內容。

表 1 安全要求等級總表

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			5.1.1.1
	5.1.2. 實體異常行為警示		5.1.2.1	
	5.1.3. 實體防護		5.1.3.1	5.1.3.2
	5.1.4. 安全啟動			5.1.4.1
	5.1.5. 實體儲存安全	5.1.5.1	5.1.5.2	5.1.5.3
系統安全	5.2.1. 作業系統安全	5.2.1.1		5.2.1.2
	5.2.2. 網路服務連接埠的控管	5.2.2.1		
	5.2.3. 更新安全	5.2.3.1	5.2.3.2	
	5.2.4. 韌體程式安全（選測）	5.2.4.1		
	5.2.5. 敏感性資料儲存安全		5.2.5.1	5.2.5.2
	5.2.6. 網頁管理介面安全	5.2.6.1		
	5.2.7. API 安全	5.2.7.1		

	5.2.8. 系統日誌檔與警示	5.2.8.1	5.2.8.2	
	5.2.9. 系統儲存備份安全	5.2.9.1	5.2.9.2	5.2.9.3
通訊安全	5.3.1. 敏感性資料傳輸安全	5.3.1.1		5.3.1.2
	5.3.2. 通訊介面的安全設置	5.3.2.1		
	5.3.3. 通訊協定安全		5.3.3.1	
	5.3.4. 影像傳輸安全	5.3.4.1	5.3.4.2	5.3.4.3
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全	5.4.1.1		5.4.1.2
	5.4.2. 通行碼鑑別機制	5.4.2.1		
	5.4.3. 權限管控	5.4.3.1		
	5.4.4. 實體設備的身分裝置鑑別	5.4.4.1		
應用程式安全	5.5.1. 應用程式的程式安全	5.5.1.1	5.5.1.2	5.5.1.3
	5.5.2. 應用程式的系統安全	5.5.2.1	5.5.2.2	5.5.2.3

4.1.1 安全構面

(a) 實體安全：影像錄影機是否能輕易被拆解，或影像錄影機之儲存與測試除錯用之連接埠的管控，作為建立安全要求的標的。

(b) 系統安全：檢視影像錄影機之作業系統、網路服務、更新服務及韌體程式設計等，是否具備足夠之安全防護。

(c) 通訊安全：著重在機敏資料之通訊安全，和探查通訊服務是否存在未知之資安漏洞。

(d) 身分鑑別與授權機制安全：影像錄影機存在數種不同的溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，無論從那一類介面，皆須確保認證與授權機制的落實。

(e) 應用程式安全：影像錄影機之應用程式安全，包括出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，以確保其符合現階段資訊安全要求，但不包含使用者自行下載之非原廠軟體或附加服務。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項，而每一安全要求分項包含一個以上之安全要求。

4.1.3 安全等級

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，欲通過較高安全等級測試必須先通過較低安全等級測試方可。

4.2 安全等級詳述

4.2.1 安全第 1 級

係針對影像錄影機的功能及操作上主要以便利性為導向，安全威脅則是次要考量的應用環境，所以專注於必須保護的敏感性資訊及個人資料之管控，是開發商對於用戶提供最基本的安全。

表 2　第 1 級安全技術要求

安全構面	安全技術要求
實體安全	5.1.5.1(a) 具備內部儲存備份 – 確保產品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 – 確保產品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。
系統安全	5.2.1.1(a) 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 – 產品之作業系統與網路服務，不得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。
	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 – 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商須於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。
	5.2.3.1(a) 韌體程式更新功能 – 韌體須具備更新機制。 5.2.3.1(b) 韌體程式更新測試之更新檔案的保護 – 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。 5.2.3.1(c) 韌體程式更新測試之更新路徑的保護 – 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 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 [9]所核可，且同時支援前向安全（Forward Secrecy）之通行碼演算法。
	5.2.4.1(a) 韌體程式碼之敏感性資料外洩 – 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，不得出現於韌體之程式碼與安裝檔內其他檔案中。
	5.2.6.1(a) 網頁管理介面弱點檢測

	- 產品本機提供之網頁管理介面不得存在 OWASP Web Top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊[8]。
	5.2.7.1(a) API 呼叫的身分鑑別機制 - 透過管理介面存取產品資源前，須先經過身分鑑別機制，且不得因為重送攻擊而使鑑別被通過。 5.2.7.1(b) API 呼叫之身分鑑別錯誤訊息 - 鑑別錯誤訊息不能顯露出合法使用者名稱。 5.2.7.1(c) API 之通行碼鑑別機制之通行碼強度 - 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、及強制執行通行碼歷程記錄原則 CCE-35219-5。 5.2.7.1(d) API 之通行碼鑑別機制之預設通行碼唯一性 - 廠商所生產之產品其預設通行碼都須相異。 5.2.7.1(e) API 之通行碼鑑別機制之通行碼變更機制 - 首次成功取得產品 API 授權，必須強制更改預設通行碼。 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 - 產品在鑑別通行碼的設計上必須有輸入頻率及次數的限制。 5.2.7.1(g) API 呼叫之權限管控機制 - 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。 5.2.7.1(h) API 呼叫之閒置時限 - 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的鑑別。
	5.2.8.1(a) 安全事件日誌檔 - 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。 5.2.8.1(b) 存取權限管控 - 產品之安全事件紀錄須具備權限控管機制，該日誌檔不得允許未經授權的修改。 5.2.8.1(c) 日誌檔保存期限 - 須要求產品之日誌檔留存時間，且須符合 NIST SP 800-92[9]中，高影響系統 high impact systems 的日誌資料維護長度。
	5.2.9.1(a) 儲存的每週最少一次完整備份 - 確保產品支援每週最少一次完整備份。
通訊安全	5.3.1.1(a)敏感性資料於傳輸過程中須加密保護 - 敏感性資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[7]，以確保機密性。
	5.3.2.1(a) 網路裝置資訊探詢功能 - 產品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，而其預設值須為關閉狀態。 5.3.2.1(b) 安全的 WiFi 組態設置

	- 產品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，而其預設值須為關閉狀態。 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 - 預設不得透過網路連線存取產品作業系統之除錯模式。
	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[7]。
身分鑑別與授權機制安全	5.4.1.1(a) 鑑別機制強度 - 透過管理介面存取產品資源前，須先經過身分鑑別機制，且不得因為重送攻擊而使鑑別被通過。 5.4.1.1(b) 身分鑑別錯誤訊息 - 鑑別錯誤訊息不能顯露出合法使用者名稱。 5.4.1.1(c) 憑證鑑別強度 - 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。
	5.4.2.1(a) 通行碼強度 - 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、強制執行通行碼歷程記錄原則 CCE-35219-5。 5.4.2.1(b) 預設通行碼唯一性 - 廠商所生產之產品其預設通行碼都須相異。 5.4.2.1(c) 通行碼變更機制 - 首次登入產品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 - 產品在登入通行碼的設計上必須有輸入頻率及次數的限制。
	5.4.3.1(a) 權限管控機制 - 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。 5.4.3.1(b) 權限有效時間 - 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的鑑別。
	5.4.4.1(a) 身分驗證機制 - 確保產品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	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，須取得使用者同意，並與其宣告之內容相符。
	5.5.2.1(a) 應用程式執行的程式行為，應取得使用者同意 - 應用程式所執行的程式行為，須取得使用者同意，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 – 應用程式須提供安全的身分辨識及保護機制。

4.2.2 安全第2級

主要針對組織考量營運規劃上資安之重要性，且欲於良好商業發展活動上，積極發展安全工程技術，期望獲得最大安全，具準備付出額外的安全工程之意願，但不須大幅度重新設計開發。

表 3　第 2 級安全技術要求

安全構面	安全技術要求
實體安全	5.1.2.1(a) 異常狀態警示機制 – 產品於實體操作時，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。
	5.1.3.1(a) 實體保護 – 產品須採用一體成形或防拆螺絲等機殼防拆除保護設計，例如：使用防盜螺絲增加拆解的困難。
	5.1.5.2(a) 具備有效儲存空間設定機制 – 確保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。
系統安全	5.2.3.2(a) 韌體更新之完整性及可信度 – 產品必須具備驗證韌體之正確性及完整性的功能。
	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）及個人資料不得明文儲存，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。
	5.2.8.2(a) 日誌檔存取異常警示 – 當安全事件日誌檔無法儲存時，產品須提供系統警示功能。警示功能設計例如：E-mail 通知、訊息推播、發出警報聲等。
	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	5.3.3.1(a) 通訊協定異常輸入 – 產品之關鍵通訊協定（參考附錄 A），不得存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。
	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，且預設啟用之加密演算法與訊息完整性校驗須採用 Federal Information Processing Standards（FIPS）140-2 [7] 所核可，以及同時支援前向安全（Forward Secrecy）之通行碼演算法。
應用程式安全	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，須停止該內建軟體所有相關程序。

	5.5.2.2(a) 支援螢幕解鎖保護機制 – 產品本身之螢幕須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 – 產品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 – 產品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。

4.2.3 安全第 3 級

應用環境屬於高風險情況，認為保護資產之價值使額外付出顯得正當時，以保護高價值資產對抗高風險為最終目的。因此開發者為獲得較高安全，需透過安全工程技術應用，且大幅度的重新設計開發。

表 4 第 3 級安全技術要求

安全構面	安全技術要求
實體安全	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，例如：連接器等。 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，例如：USB 埠、網路埠等。
	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 - 產品外部不得有徒手即可輕易還原預設通行碼的設計。
	5.1.4.1(a) 支援安全啟動（Secure boot）功能 - 產品不得以未經授權的韌體、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。
	5.1.5.3(a) 儲存備份支援資料冗餘之能力 - 確保產品儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上。 5.1.5.3(b) 支援硬碟熱備援 - 確保產品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 - 確保產品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。
系統安全	5.2.1.2(a) 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 - 產品之作業系統與網路服務，不得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。
	5.2.5.2(a) 敏感性資料隔離保護 - 敏感性資料必須存放於產品的安全區域（Secure domain）中。
	5.2.9.3(a) 儲存的異地備份 - 確保產品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。 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。
通訊安全	5.3.1.2(a) - 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 [7]所核可，且同時支援前向安全（Forward Secrecy）之通行碼演算法。
	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。
身分鑑別與授權機制安全	5.4.1.2(a) 鑑別機制強度 – 產品之身分鑑別機制須採用多因子鑑別。 5.4.1.2(b) 裝置鑑別強度 – 支援影像監控系統身分之裝置鑑別，且不得因為重送攻擊而使鑑別被通過，以確保相連裝置的可信度。
應用程式安全	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 – 廠商須於文件中標明所使用的應用程式所引用之第三方函式庫。
	5.5.2.3(a) 應用程式的異常操作之監控及防護 – 應用程式須具備應用程式異常操作之監控及防護。

5. 標準規範

5.1 實體安全

5.1.1 實體埠之安全管控

5.1.1.1 產品不得有除錯測試用之實體介面存在

(a) 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，例如：連接器等。

(b) 外接實體埠的插拔操作須提供日誌紀錄，例如：USB 埠、網路埠等。

5.1.2 實體異常行為警示

5.1.2.1 產品之硬體設計須具備異常狀態之警示機制

(a) 產品於實體操作時，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。

5.1.3 實體防護

5.1.3.1 產品之外殼須具不被輕易拆除或破壞的防護機制

(a) 產品須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 避免不安全的實體設計

(a) 晶片上不得存在晶片編號，且電路板上不得存在功能編號。

(b) 產品外部不得有徒手即可輕易還原預設通行碼的設計。

5.1.4 安全啟動

5.1.4.1 產品須提供安全啟動（Secure boot）功能

(a) 產品不得以未經授權的韌體、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。

5.1.5 實體儲存安全

5.1.5.1 備援機制之初級要求

(a) 確保產品具備有內部儲存備份之介面，例如：SATA 等。

(b) 確保產品具備有外部儲存備份之介面，例如：USB、eSATA 等。

(c) 須提供「手動備份」與「排程自動備份」功能。

5.1.5.2 備援機制之中階要求

(a) 確保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。

5.1.5.3 備援機制之高階要求

(a) 確保產品儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上。

(b) 確保產品儲存備份支援硬碟熱備援之功能，提升容錯能力。

(c) 確保產品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。

5.2 系統安全技術要求

5.2.1 作業系統安全

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) 產品之作業系統與網路服務，不得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。

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) 產品之作業系統與網路服務，不得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。

5.2.2 網路服務連接埠的控管

5.2.2.1 產品僅開啟必要之網路服務

(a) 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商須於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。

5.2.3 更新安全

5.2.3.1 韌體更新機密性保證

(a) 韌體須具備更新機制。

(b) 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。

(c) 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 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 **錯誤! 找不到參照來源。**]所核可，且同時支援前向安全（Forward Secrecy）之通行碼演算法。

5.2.3.2 韌體更新機制強度

(a) 產品必須具備驗證韌體之正確性及完整性的功能。

5.2.4 韌體程式安全（選測）

5.2.4.1 產品之敏感性資料不得出現於裝置韌體程式碼中

(a) 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，不得出現於韌體之程式碼與安裝檔內其他檔案中。

5.2.5 敏感性資料儲存安全

5.2.5.1 產品所儲存之敏感性資料須透過加密儲存

(a) 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）及個人資料不得明文儲存，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。

5.2.5.2 敏感性資料的存放，須從正常作業環境中隔離

(a) 敏感性資料必須存放於產品的安全區域（Secure domain）中。

5.2.6 網頁管理介面安全

5.2.6.1 網頁管理介面不得存在 OWASP Web Top 10 [8] 常見網站安全風險

(a) 產品本機提供之網頁管理介面不得存在 OWASP Web Top 10 之 A1-Injection 及 A3-Cross-Site Scripting（XSS）攻擊。

5.2.7 API 安全

5.2.7.1 API 之鑑別機制強度

(a) 透過管理介面存取產品資源前，須先經過身分鑑別機制，且不得因為重送攻擊而使鑑別被通過。

(b) 鑑別錯誤訊息不能顯露出合法使用者名稱。

(c) 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、及強制執行通行碼歷程記錄原則 CCE-35219-**5**。

(d) 廠商所生產之產品其預設通行碼都須相異。

(e) 首次成功取得產品 API 授權，必須強制更改預設通行碼。

(f) 產品在鑑別通行碼的設計上必須有輸入頻率及次數的限制，即：

- 最高五次嘗試登入失敗即鎖定帳戶。
- 帳戶鎖定期間至少一分鐘以上，始可自動解除。
- 帳戶鎖定計數器至少一分鐘以上的時間間隔，始可將失敗的登入嘗試計數器重設為零次。

(g) 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

(h) 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的鑑別。

5.2.8 系統日誌檔與警示

5.2.8.1 產品須提供安全事件日誌檔

(a) 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。

(b) 產品之安全事件紀錄須具備權限控管機制，該日誌檔不得允許未經授權的修改。

(c) 須要求產品之日誌檔留存時間，且須符合 NIST SP 800-92[9] 中，高影響系統（high impact systems）的日誌資料維護長度。

5.2.8.2 產品須提供異常警示功能

(a) 當安全事件日誌檔無法儲存時，產品須提供系統警示功能。警示功能設計例如：E-mail 通知、訊息推播、發出警報聲等。

5.2.9 系統儲存備份安全

5.2.9.1 備份安全之初階要求

(a) 確保產品支援每週最少一次完整備份。

5.2.9.2 備份安全之中階要求

(a) 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。

5.2.9.3 備份安全之高階要求

(a) 確保產品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。

(b) 確保資料儲存支援影音資料防竄改的機制。

5.3 通訊安全技術要求

5.3.1 敏感性資料傳輸安全

5.3.1.1 敏感性資料於傳輸過程中須加密保護

(a) 敏感性資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[7]，以確保機密性。

5.3.1.2 敏感性資料傳輸須採用安全通道

(a) 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 [7]所核可，且同時支援前向安全（Forward Secrecy）之通行碼演算法。

5.3.2 通訊介面的安全設置

5.3.2.1 避免錯誤的通訊介面設置

(a) 產品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，而其預設值須為關閉狀態。

(b) 產品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，而其預設值須為關閉狀態。

(c) 無線網路傳輸的安全機制預設須採用「Wi-Fi 保護存取 2」。

(d) 預設不得透過網路連線存取產品作業系統之除錯模式。

5.3.3 通訊協定安全

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

5.3.4 影像傳輸安全

5.3.4.1 影像資料傳輸機密性初階要求

(a) 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**錯誤! 找不到參照來源。**7]。

5.3.4.2 影像資料傳輸機密性中階要求

(a) 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，且預設啟用之加密演算法與訊息完整性校驗須採用 Federal Information Processing Standards（FIPS）140-2 **錯誤! 找不到參照來源。**7]所核可，以及同時支援前向安全（Forward Secrecy）之通行碼演算法。

5.3.4.3 影像資料傳輸機密性高階要求

(a) 確保影像資料之傳輸加密演算法須採用 AES-256。

5.4 身分鑑別與授權機制安全技術要求

5.4.1 鑑別機制安全

5.4.1.1 鑑別機制強度初階要求

(a) 透過管理介面存取產品資源前，須先經過身分鑑別機制，且不得因為重送攻擊而使鑑別被通過。

(b) 鑑別錯誤訊息不能顯露出合法使用者名稱。

(c) 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。

5.4.1.2 鑑別機制要求中階要求

(a) 產品之身分鑑別機制須採用多因子鑑別。

(b) 支援影像監控系統身分之裝置鑑別，且不得因為重送攻擊而使鑑別被通過，以確保相連裝置的可信度。

5.4.2 通行碼鑑別機制

5.4.2.1 通行碼鑑別機制強度

(a) 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、強制執行通行碼歷程記錄原則 CCE-35219-5。

(b) 廠商所生產之產品其預設通行碼都須相異。

(c) 首次登入產品必須強制更改預設通行碼。

(d) 產品在登入通行碼的設計上必須有輸入頻率及次數的限制，即：

- 最高五次嘗試登入失敗即鎖定帳戶。
- 帳戶鎖定期間至少一分鐘以上，始可自動解除。
- 帳戶鎖定計數器至少一分鐘以上的時間間隔，始可將失敗的登入嘗試計數器重設為零次。

5.4.3 權限管控

5.4.3.1 產品資源的存取，必須具備權限管控機制

(a) 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

(b) 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的鑑別。

5.4.4 實體設備的身分裝置鑑別

5.4.4.1 產品須提供身分驗證機制

(a) 確保產品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。

5.5 應用程式安全技術要求

5.5.1 應用程式的程式安全

5.5.1.1 應用程式的程式安全之初級要求

(a) 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。

(b) 應用程式所執行的行為，須取得使用者同意，並與其宣告之內容相符。

5.5.1.2 應用程式的程式安全之中階要求

(a) 應用程式於使用者設定關閉時，須停止該內建軟體所有相關程序。

5.5.1.3 管理介面的程式安全之高階要求

(a) 應用程式須提供回報安全性問題之管道。

(b) 廠商須於文件中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

5.5.2.1 應用程式的系統安全之初級要求

(a) 應用程式所執行的程式行為，須取得使用者同意，必要時並提供風險提示。

(b) 應用程式須提供安全的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

(a) 產品本身之螢幕須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。

(b) 產品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。

(c) 產品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。

5.5.2.3 應用程式的系統安全之高階要求

(a) 應用程式須具備應用程式異常操作之監控及防護。

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）[16][17]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，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[14]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）[15]

定義在 RFC 2326 規範中，用來控制具有即時性需求的資料，如影音多媒體資料的播放、錄製及暫停，可達到用戶端到媒體伺服器之間的即時影音控制。

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

定義在 RFC 7540 規範中，超文本傳輸協定之全名為 HypertText Transfer Protocol（簡稱為 HTTP），是目前網際網路上應用最廣泛的一個網路協議（protocol），其主要目的是為了提供網頁的發佈與取得。

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

定義在 RFC 2818 規範中，是一種經由 HTTP 進行通訊傳輸，且傳輸是建立在 SSL/TLS 安全通道之上，以保護傳輸中之資料。HTTPS 的主要應用是對網站伺服器進行身分認證，確保傳輸中資料的隱密性與完整性。

C.6 檔案傳輸協定（File Transfer Protocol，FTP）[18]

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。

附錄 D

（參考）

技術要求事項與各標準規範對照表

技術要求	OWASP IoT Top 10 對應項目[5]	ONVIF 對應項目[13]
5.1.1.1(a) 最小實體介面	I10: Poor Physical Security	N/A
5.1.1.1(b) 實體行為日誌	I10: Poor Physical Security	N/A
5.1.2.1(a) 異常狀態警示機制	I10: Poor Physical Security	N/A
5.1.3.1(a) 實體保護	I10: Poor Physical Security	N/A
5.1.3.2(a) 內部實體安全	I2: Insufficient Authentication/Authorization	N/A
5.1.3.2(b) 通行碼還原機制安全設計	I2: Insufficient Authentication/Authorization	N/A
5.1.4.1(a) 支援安全啟動功能	I9: Insecure Software/Firmware	N/A
5.1.5.1(a) 具備內部儲存備份	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.1.5.1(b) 具備外部儲存備份	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.1.5.1(c) 具備手動備份、排程自動備份	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.1.5.2(a) 具備有效儲存空間設定機制	N/A	N/A
5.1.5.3(a) 儲存備份支援 RAID 1 等級以上	N/A	N/A
5.1.5.3(b) 支援硬碟熱備援	N/A	N/A
5.1.5.3(c) 支援電源備援機制	N/A	N/A
5.2.1.1(a) 檢測作業系統是否存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大	I3: Insecure Network Services	N/A
5.2.1.2(a) 檢測作業系統是否存在漏洞評鑑系統 CVSS v3 嚴重性等級評比為高	I3: Insecure Network Services I6: Insecure Cloud Interface	N/A
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	I3: Insecure Network Services I6: Insecure Cloud Interface	Core Spec. – Ver. 16.12 4.5.2 Network
5.2.3.1(a) 韌體程式更新功能	I9: Insecure Software/Firmware	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade
5.2.3.1(b) 韌體程式更新測試 - 更新檔案的保護	I9: Insecure Software/Firmware	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade
5.2.3.1(c) 韌體程式更新測試 - 更新路徑的保護	I9: Insecure Software/Firmware	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade
5.2.3.1(d) 韌體程式更新測試 - 加密演算法的機制	N/A	N/A
5.2.3.2(a) 韌體更新之完整性	I9: Insecure Software/Firmware	4.5.3 System

及可信度		
5.2.4.1(a) 韌體程式碼之敏感性資料外洩	I9: Insecure Software/Firmware	N/A
5.2.5.1(a) 敏感性資料加密儲存	N/A	Advanced Security Service Spec. – Ver. 1.3 5.2 Keystore
5.2.5.2(a) 敏感性資料隔離保護	I10: Poor Physical Security I8: Insufficient Security Configurability	Advanced Security Service Spec. – Ver. 1.3 5.2 Keystore
5.2.6.1(a) 網頁管理介面弱點檢測	I1: Insecure Web Interface	N/A
5.2.7.1(a) API 呼叫的身分鑑別機制	I2: Insufficient Authentication/Authorization I3: Insecure Network Services	N/A
5.2.7.1(b) API 呼叫之身分鑑別錯誤訊息	I2: Insufficient Authentication/Authorization I3: Insecure Network Services	N/A
5.2.7.1(c) API 之通行碼鑑別機制 - 通行碼強度	I2: Insufficient Authentication/Authorization I3: Insecure Network Services	N/A
5.2.7.1(d) API 之通行碼鑑別機制 - 預設通行碼唯一性	I2: Insufficient Authentication/Authorization	N/A
5.2.7.1(e) API 之通行碼鑑別機制 - 通行碼變更機制	N/A	N/A
5.2.7.1(f) API 之通行碼鑑別機制 - 通行碼的輸入頻率及次數限制	N/A	N/A
5.2.7.1(g) API 呼叫之權限管控機制	I8: Insufficient Security Configurability	N/A
5.2.7.1(h) API 呼叫之閒置時限	I8: Insufficient Security Configurability	N/A
5.2.8.1(a) 安全事件日誌檔	I8: Insufficient Security Configurability	Core Spec. – Ver. 16.12 4.5.3 System
5.2.8.1(b) 存取權限管控	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.2.8.1(c) 日誌檔保存期限	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.2.8.2(a) 登入警示功能	N/A	N/A
5.2.8.2(b) 日誌檔存取異常警示	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.2.9.1(a) 儲存的每週最少一次完整備份	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.2.9.2(a) 儲存的安全加密機制必須支援 AES-256	N/A	N/A
5.2.9.3(a) 儲存的異地備份	N/A	N/A
5.2.9.3(b) 儲存的資料防竄改	N/A	N/A
5.3.1.1(a) 敏感性資料之傳輸	I1: Insecure Web Interface I2: Insufficient	N/A

保護初階	Authentication/Authorization I4: Lack of Transport Encryption I8: Insufficient Security Configurability	
5.3.1.2(a) 敏感性資料傳輸須採用安全通道	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization I4: Lack of Transport Encryption I8: Insufficient Security Configurability	Core Spec. – Ver. 16.12 5.12.1 Authentication
5.3.2.1(a) 網路裝置資訊探詢功能	I3: Insecure Network Services	Core Spec. – Ver. 16.12 4.5.2 Network
5.3.2.1(b) 安全的 WiFi 組態設置	I3: Insecure Network Services	N/A
5.3.2.1(c) 無線網路傳輸安全機制設置	I3: Insecure Network Services	N/A
5.3.2.1(d) 網路介面存取設置	I3: Insecure Network Services	N/A
5.3.3.1(a) 通訊協定異常輸入	I3: Insecure Network Services	Core Spec. – Ver. 16.12 4.5.2 Network
5.3.4.1(a) 影像資料之傳輸不得為明文	I4: Lack of Transport Encryption I5: Privacy Concerns	N/A
5.3.4.2(a) 影像資料之傳輸須使用 FIPS 140-2	I4: Lack of Transport Encryption I5: Privacy Concerns	N/A
5.3.4.3(a) 影像資料之傳輸加密演算法須採用 AES-256	I4: Lack of Transport Encryption I5: Privacy Concerns	N/A
5.4.1.1(a) 鑑別機制強度	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization	Core Spec. – Ver. 16.12 5.12.1 Authentication 5.12.3 Username token profile
5.4.1.1(b) 身分鑑別錯誤訊息	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization	Advanced Security Service Spec. – Ver. 1.3 4.2 Certificate-based Client Authentication
5.4.1.1(c) 憑證鑑別強度	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization	Core Spec. – Ver. 16.12 5.12.1 Authentication 5.12.3 Username token profile
5.4.1.2(a) 多因子鑑別機制	I2: Insufficient Authentication/Authorization I7: Insecure Mobile Interface	N/A
5.4.1.2(b) 裝置鑑別強度	I7: Insecure Mobile Interface	N/A
5.4.2.1(a) 通行碼強度	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization I8: Insufficient Security Configurability	N/A
5.4.2.1(b) 預設通行碼唯一性	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization I8: Insufficient Security Configurability	N/A

5.4.2.1(c) 通行碼變更機制	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization I8: Insufficient Security Configurability	N/A
5.4.2.1(d) 通行碼的輸入頻率及次數限制	I1: Insecure Web Interface I2: Insufficient Authentication/Authorization I8: Insufficient Security Configurability	N/A
5.4.3.1(a) 權限管控機制	I2:Insufficient Authentication/Authorization I8: Insufficient Security Configurability	Core Spec. – Ver. 16.12 5.12.2 User-based access control
5.4.3.1(b) 權限有效時間	I2:Insufficient Authentication/Authorization I8: Insufficient Security Configurability	Core Spec. – Ver. 16.12 5.12.2 User-based access control
5.4.4.1(a) 身分驗證機制	I2	Core Spec. – Ver. 16.12 5.12.1 Authentication
5.5.1.1(a) 應用程式為最新之版本	I7: Insecure Mobile Interface	Core Spec. – Ver. 16.12 5.12.1 Authentication
5.5.1.1(b) 應用程式之執行取得使用者同意	N/A	Core Spec. – Ver. 16.12 4.5.3 System
5.5.1.2(a) 應用程式的關閉機制	N/A	N/A
5.5.1.3(a) 應用程式回報安全性機制	I8: Insufficient Security Configurability	Core Spec. – Ver. 16.12 4.5.7 Security 5.12 Security
5.5.1.3(b) 應用程式有標明所引用之第三方函式庫	N/A	N/A
5.5.2.1(a) 應用程式執行的程式行為，應取得使用者同意	N/A	Core Spec. – Ver. 16.12 4.5.7 Security 5.12.2 User-based access control
5.5.2.1(b) 應用程式提供更新通知	I9: Insecure Software/Firmware	N/A
5.5.2.1(c) 應用程式的身分辨識及保護機制	I2: Insufficient Authentication/Authorization	N/A
5.5.2.2(a) 支援螢幕解鎖保護機制	N/A	Core Spec. – Ver. 16.12 4.5.7 Security
5.5.2.2(b) 支援螢幕解鎖錯誤之強制鎖定保護機制	N/A	Core Spec. – Ver. 16.12 5.11 Error handling
5.5.2.2(c) 螢幕鎖定解鎖資料，須加密保護	N/A	N/A
5.5.2.3(a) 應用程式的異常操作之監控及防護	N/A	Core Spec. – Ver. 16.12 5.11 Error handling

參考資料

[1] UL 2900-1, Outline of Investigation for Software Cybersecurity for Network Connectable Products, Part 1: General Requirements

[2] GSMA corp., IoT Security Guidelines for Endpoint Ecosystems

[3] OWASP.org, Top IoT Vulnerabilities, 取自 https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[4] 總務省經濟產業省, IoT セキュリティガイドライン ver 1.0

[5] NIST, National Vulnerability Database, 取自 https://nvd.nist.gov/vuln/full-listing

[6] 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）

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

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

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

[10] 行動應用資安聯盟, 行動應用 App 基本資安規範 V1.1

[11] 國家通訊傳播委員會, 智慧型手機系統內建軟體資通安全檢測技術規範, March 2016.

[12] MITRE, 2011 CWE/SANS Top 25 Most Dangerous Software Errors, 取自 http://cwe.mitre.org/top25/

[13] ONVIF, Core Specification Version 16.12, December 2016.

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

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

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

[17] RFC 2818, HTTP Over TLS

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

[19] 個人資料保護法, 取自 http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021