因應資通安全管理法之資安管理研究

－以AI CAM為例

運輸資訊組 吳東凌 鄭志瑋

研究期間110年2月至110年12月

摘要

調研機構Gartner統計109年全球將有58億個物聯網(Internet of Things, IoT)裝置，其數量已超越傳統的IT(Information Technology)設備，物聯網常被歸類為OT(Operational Technology)設備，多在隔離和獨立的網路環境中執行，在資安防護及安全要求上相較IT設備常被忽略，在面對智慧運用等發展趨勢，OT環境無法再像以往封閉，必須連網與各個系統進行串聯，因此會將資安的風險帶入OT環境。本研究將依資通安全管理法相關資安規範為基礎，結合政府「關鍵資訊基礎設施防護基本政策」，分析物聯網特性、運用及發展，並以AI CAM為例，找出AI CAM與物聯網相關之資安防護控制措施與實作建議，以做為本所管理物聯網設備之參考依據。

關鍵詞：資通安全、AI CAM

一、物聯網發展趨勢

調研機構 Gartner 統計 2020 年全球有 58 億個物聯網(Internet of Things, IoT)裝置，其數量已經超越傳統的 IT(Information Technology)設備。隨著這幾年物聯網世代的快速發展，政府及所有產業紛紛跟上物聯網的發展；此外，在 2016 年 Google DeepMind 團隊開發人工智慧帶起 AI 新的發展趨勢，許多科技產業便朝向 AI 人工智慧與物聯網結合的 AIoT(Artificial IoT, 又稱智聯網)，並將 AIoT 視為未來各產業的 IT 系統主流架構，過去因為資訊傳輸頻寬受限，發展仍有瓶頸。然而，在 5G 逐漸普及後，解決過去頻寬問題，與 AIoT 結合運用於交通、醫療、工業等具獨立作業需求的領域。惟其架構仍屬前端的網路攝影機(Operational Technology, OT)與後端的運算裝置(IT)的互連，也易導致 OT 系統暴露在風險之中，加上 IT 安全系統不適用於 OT 系統，以及 IT 與 OT 人員究竟誰負責 OT 資安管理，都讓設備在連網環境下能否安全的運作造成困難，因為有諸多需要釐清、溝通與協調，這也讓空窗期或灰色地帶運作場域的系統下，容易遭受到駭客與惡意程式的攻擊。

在面對智慧運用等發展趨勢，OT 環境無法再像以往封閉，必須連網與各個系統進行串聯，因此會將資安的風險帶入 OT 環境。另 OT 與 IT 環境除在應用上有許多的差異外，同時也面臨被要求整合上的需求，這其中包括人員、流程與技術上的融合，目的之一也是希望能夠避免因為人為的疏失或遭遇蓄意攻擊的事件，導致企業或國家產生重大的損失。

自從 2020 年初起，全球受到 COVID-19 疫情席捲，企業為維持各項工作，多數改用遠距工作，甚至不在辦公室工作，而是各自在家工作，使得全世界更仰賴資訊技術與網際網路，與此同時各式各樣的詐騙郵件、勒索軟體、惡意程式、惡意網域、木馬程式等也如雨後春筍般大量暴增，隨之而來的風險與威脅日益嚴重。而隨著政府與經濟逐漸依賴網際網路，網

路安全所影響的層面擴及國家的關鍵基礎設施，包含醫療、金融、交通、通訊、能源等；因此，確保國家關鍵基礎設施運作安全，一直是政府關注的議題，各國亦研擬資安法規因應。

然而，任何安全管理對於工作效率必然產生影響，如何平衡須仰賴明確之法規規範與遵循，才能使得國家順利發展。我國資通安全管理法於2019 年施行後，明確界定資通系統、資通服務、資通安全、資通安全事件、公務機關、特定非公務機關、關鍵基礎設施、關鍵基礎設施提供者、政府捐助之財團法人等 9 類名詞定義，強化對資通安全政策與執行等管理層面規範，期能提升國家資通安全環境。此外，COVID-19 疫情爆發讓公眾運輸創新的目標聚焦於公眾健康，透過整合 AI、熱成像、視訊分析的系統能以非接觸方式辨識個人、偵測體溫與是否佩戴口罩，可望成為所有車站入口的關鍵安全配置，並整合至接觸追蹤等公眾健康照護系統，加速追蹤與找出個別受感染者、遏止病毒散播。由此可知，人工智慧結合影像偵測未來必然成為政府關鍵基礎設施重要的一環。

本研究將依資通安全管理法相關資安規範為基礎，結合政府「關鍵資訊基礎設施防護基本政策」，分析物聯網特性、運用及發展，並以 AI CAM 為例，找出 AI CAM 與物聯網相關之資安防護控制措施與實作建議，以做為本所管理物聯網設備之參考建議，以符合資通安全管理法規範。

二、AI CAM 趨勢發展

AI 技術結合影像監控系統是目前較為廣泛的 AIoT 應用之一，世界經濟論壇[1](World Economic Forum)在 2016 年世界工作報告中，亦認為 AI、遺傳學、奈米技術、3D 列印及生物技術，是推動世界第四次工業革

[1] World Economic Forum. “The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution” 2016 Global Challenge Insight Report (2016). Preface. https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security.

命的重要關鍵因素。由於 AI 是未來物聯網及工業 4.0 發展的核心，尤其在零售、交通運輸、自動化、製造業、醫療照護及農業等層面垂直領域具有巨大的潛力，其關鍵在於各種軟硬體的整合[2]。而 AIoT(智聯網)的發展，就是在 IoT 設備裝置上執行 AI 或機器學習運算工作，能直接套用 IoT 感測器串流資料用於大數據或機器學習模型推論，然而為達到上述 AIoT 運作架構，需具備感測晶片及網路、AI 演算法、雲端平台即服務 (Platform as a Service，PaaS)，與傳統物聯網最大的差別，在於傳統物聯網無法解決即時回應、資料隱私、離線處理等多元需求，而 AIoT 具備邊緣運算能力，以解決雲端架構所面臨的問題[3]；然而，也因為具備比過去傳統物聯網更多的運算及資料處理能力，其安全需要更嚴謹的管控作為。

(一)AI CAM 現況

網路監控攝影機(IP Camera/Network Camera)是目前常見的影像監控攝影機。有別於閉路電視、類比監控攝影機(CCTV)，網路監控攝影機是以電腦做為平台並利用網路做為傳輸架構，傳輸監控影像與聲音，而在運用上主要是搭配數位影像錄影機、網路影像錄影機及網路儲存裝置組成影像監控系統[4]，近年來網路監控攝影機透過儲存裝置與監控管理軟體的搭配創造出多種應用方案，並且透過發展自身的 IVS(Intelligent Video Surveillance)智能影像監控系統(如圖 2.1)來達成建置所需之目的。學者陳毅暉、林育樞、蘇苗彬(2020)[5]研發新型光學式立體視覺裝置利用雙相機光學原理之立體相對電腦視覺技術作相對計算左相機和目標物之相對距離，即時監測山坡地變位情形，形成監測崩塌地 3D 變位裝置。學者胡啟恩、郭雅諒、王元

[2] 國家實驗研究院科技政策與研究中心，〈未來 AI 發展八大新趨勢〉，2018 年 10 月 31 日，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13837

[3] 洪哲倫、張志宏、林宛儒(2019，12 月)。工業 4.0 與智慧製造的關鍵技術：工業物聯網與人工智慧。科儀新知，211 期，19-25。

[4] 財團法人台灣資通產業標準協會，影像監控系統資安標準-第一部。

[5] 陳毅暉、林育樞、蘇苗彬(2020)。應用 AIoT 立體視覺裝置於崩塌地距離量測之研究。技師期刊，91(7)，83-89。

凱(2018)[6]介紹視覺式行人偵測追蹤技術，並說明多物件追蹤系統的技術內容，除有系統方法的原理概念外，還包含如何調整行人偵測與多物件追蹤之參數，並透過參數最佳化，行人偵測器可給出更準確的效果及行人位置。

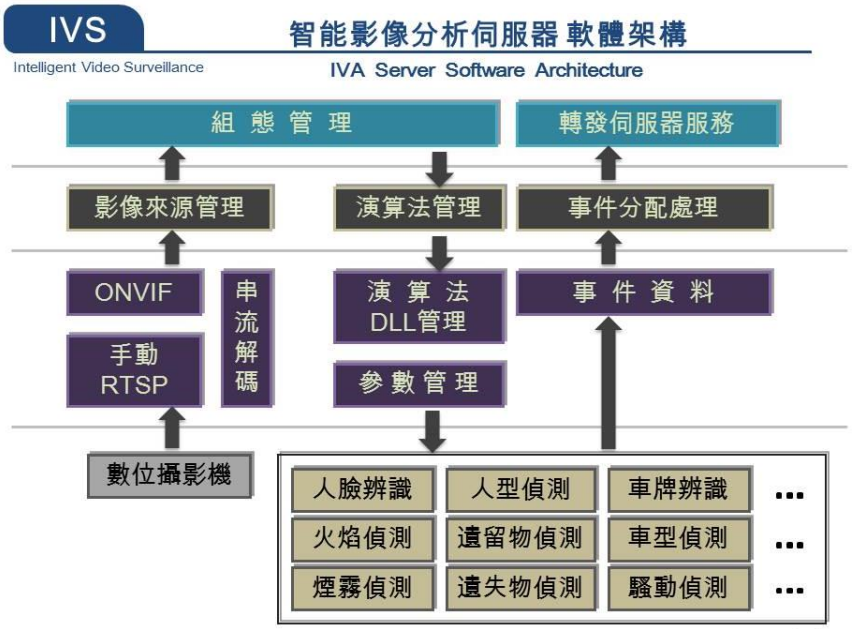
資料來源：https://www.tdv.com.tw/productd-34-34。

圖2.1 IVS平台架構

(二)AI CAM 特性

IVS 智能影像監控系統等於是主動將儲存畫面同時進行同步分析(如圖 2.3)，當畫面出現異狀，系統即透過預先條件發出警示訊息，讓相關人員可在問題發生的當下，即掌握並處理當前狀況，與傳統監控系統需要人工監視、發掘問題有極大的不同。而要能達到主動發掘的分析能力，需要幾個部分來配合：

[6] 胡啟恩、郭雅諒、王元凱(2018)。視覺式行人偵測追蹤技術之發展。科學新知，215 期，34-45。



資料來源：https://www.tdv.com.tw/productd-34-34。

圖2.2 IVS智能影像分析伺服器軟體架構

1. 透過場域變數與演算法分析

智慧影像監控的大數據訓練，目前市面上已有開放資料集可供使用，但企業因為各家應用場景不同，會以此為基礎再傳給AI特定應用場域，例如百貨商場、大賣場的電腦影像數據，便可更快開發出符合自家商業模式的機器學習模型(Machine Learning Model)，以此不斷修正演算法參數，再透過準確率(Accuracy Rate，ACR)、真陽性率(True Positive Rate，TPR)、真陰性率(True Negative Rate，TNR)、偽陽性率(False Positive Rate，FPR)、偽陰性率(False Negative Rate，FNR)、陽性預測值(Positive Predictive Value，PPV)、陰性預測值(Negative Predictive Value，NPV)、幾何平均評估指標(Geometric Mean，GM)、接收者特徵操作曲線(Receiver Operating characteristic Curve，ROC)及曲線下方面積(Area Under the Curve，AUC)等幾種評估指標[7]，計算AI是否有效。

2. 提升硬體設備蒐集暨處理能力

要達到辨識率、準確率的提升，從硬體架構的角度，關鍵就在攝錄畫面

[7] 科學 Online(2019) 。AI 的表現好嗎？十種常見的評估指標，2019 年 2 月 18 日。https://highscope.ch.ntu.edu.tw/wordpress/?p=80752

的解析度；當 IP CAM 的解析度越高，在 IVS 系統服務端可供其分析、判斷的資料相對較多，自然可降低其誤判問題[8]。另外，目前部分產品整合智慧前端設備(Smart End Point，SEP)將原有交付後端的影像分析工作，部份轉移至前端進行處理，例如，IP CAM 透過高效能資安監測整合後，在影像未壓縮前隨即針對影像內容進行物件移動、遺留物偵測等關鍵分析，藉此由前端攝影機即可實現錄製畫面是否觸發的關鍵角色，使得畫面儲存需求，精省到可能僅需要以前的十分之一，且監控端點本身也具備動態分析功能，這也代表攝影機可在最短的時間內將異常訊息傳回中控單位，增進整體安控系統的維安效率[9]。

3. 縮短影像傳輸處理時間

由於 IVS 系統監控端使用高解析影像攝影機，當然網路的頻寬也會因大量的畫面資訊傳輸而變得更加吃緊。目前高階攝影機幾乎都採行 H.264 壓縮技術，處理監控畫面高階影像的壓縮與傳輸需求，而 H.264 對比原有的 Motion JPEG 與 MPEG-4 壓縮格式而言，有其規格上的實質優勢，可針對影像採大比例的壓縮處理，藉此降低檔案容量同時也能減輕頻寬負荷，一般而言 H.264 壓縮方式，可以較 MPEG-4 減少 50% 檔案大小，相較 Motion JPEG 甚至可以減省近 8 成空間。

(三)AI CAM 資安風險

依前述 AI CAM 現況及特性，大致可以將其資安風險區分「網路監控攝影機(IP CAM/Network CAM)和「人工智慧(Artificial Intelligence)」兩部分探討：

1. 網路監控攝影機(IP CAM/Network CAM)

網路監控攝影機定義上屬於物聯網應用之一，其主要資安風險歸納物聯網三層架構(應用層、網路層、感知層)普遍存在的安全議題[10](如表

[8] DIGITIMES(2009)。智慧影像監控系統發展應用，2009 年 8 月 6 日。
https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000145711_bnl69iz32f8hxe05f5ty5
[9] DIGITIMES(2009)。IP 化監控系統的架構策略，2009 年 8 月 6 日。
https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000145616_8fc71o3h0i2xeq7l
[10] 江榮倫、廖伯侖(2014，11 月)。潛談物聯網的安全隱憂與挑戰。勤業眾信通訊，43-47。

2.1)：

表 2.1 物聯網普遍安全議題彙整表

物聯網架構層	普遍安全議題
應用層	裝置設定的隱私資料保護
	裝置身分認證及存取權限管控
	軟體漏洞與保護機制
網路層	資料傳輸加密及保護
	裝置的網路安全管控
感知層	底層的感知設備攻擊

資料來源：資訊安全通訊，19 卷 4 期，2013。

OWASP(Open Web Application Security Project，開放網路軟體安全計畫)2018 針對物聯網裝置安全問題進行統計，歸納出物聯網常見的十項安全性問題，對應物聯網三層架構[11](如表 2.2)：

表 2.2 OWASP 統計常見安全問題彙整表

OWASP 統計常見十項安全問題	對應物聯網架構		
	感知層	網路層	應用層
弱密碼、可猜測密碼或固定式密碼值	•	•	
不安全的網路服務		•	
不安全的環境設定介面	•		
缺乏安全的更新機制	•		
使用不安全或已遭棄用的組件	•		•

[11] OWASP IoT Top 10，https://www.owasp.org/index.php/OWASP Internet of Things Project.

隱私保護不充分	•		•
不安全的資料傳輸和儲存	•	•	•
缺乏設備管理	•	•	
不安全的預設設置	•	•	•
缺乏實體保護措施	•		

資料來源：OWASP，2018。

趨勢科技(2020)[12]針對 ZKTeco FaceDepot-7B、Hikvision DS-K1T606MF、Telpo TPS980 與 Megvii Koala 等四款臉部辨識門禁裝置中導入邊緣運算能力直接可以對使用者的影像進行驗證之設備進行資安檢測實驗，發現「裝置硬體弱點」、「系統管理權限濫用」、「透過 USB 連接埠植入惡意檔案」、「無加密也無安全機制的網路流量」、「傳輸遭到竄改」等問題。顯見影像分析裝置安全問題仍與物聯網安全問題重疊。

三、AI CAM 安全相關規範

我國參照國際物聯網相關資安標準規範[13]，ISO 27001、ANSI/CAN/UL 2900-1：2017 標準、Groupe Speciale Mobile Association (GSMA) IoT Security Guideline 、 Open Web Application Security Project(OWASP) Top 10 Vulnerabilities 及日本政府的物聯網安全指導方針等， 建立國內在影像監控系統上資安品質的標準，包含實體安全、系統安全、通訊安全、身分鑑別與授權機制安全、及隱私保護，從此五大安全構面針對影像監控裝置詳盡載明應採取的共通方法。其資安標準區分「一般要求」、「網路攝影機」、「影像錄影機」及「網路儲存裝置」等四部分。

四、研究分析

[12] 趨勢科技(2020)。臉部辨識裝置爆資安漏洞。https://blog.trendmicro.com.tw/?p=65908
[13] 同註 4。

(一)威脅分析

本研究中指的 AI CAM 為影像監控系統增加 IVS(Intelligent Video Surveillance)智能影像監控裝置，功能上具有影像分析的能力，也就是說現行影像監控系統資安標準規範，並未針對具有人工智慧分析能力之設備進行規範。雖然如此，但人工智慧之安全問題仍無法脫離實體安全、系統安全、通訊安全、身份鑑別與授權機制安全、隱私保護及應用程式安全等安全構面。因此，本研究彙整分析現有影像監控系統資安標準要求事項，針對影像分析設備的安全問題「隱私保護」及「應用程式安全」兩項安全構面上提出建議：

1. 隱私保護

我國影像監控系統資安標準對於隱私保護係針對「隱私資料的存取保護」與「隱私資料的傳輸保護」等兩項要求，其內容要求使用上隱私資料必須經過授權，且存取均須警示；傳輸上依不同安全等級使用不同等級加密機制，雖然已經大部分杜絕隱私資料使用上的問題。然而透過片段影像，將知識抽取分析的人工智慧技術，卻可識別出影像特徵進而組合成有意義的資訊。

2. 應用程式安全

審視我國影像監控系統資安標準，並未對「網路攝影機」要求執行「應用程式安全」構面安全措施，然後目前已有部分市售攝影機機體本身具有資安監控能力，同時搭載基礎影像分析功能，故本研究將「網路攝影機」資安標準內容新增安全構面－「應用程式安全」。

(二)建立資安防護建議基準

本研究結合我國台灣資通產業標準協會－「影像監控系統資安標準測試規範－第一部:一般要求」、「影像監控系統資安標準測試規範－第二部:網路攝影機」、「影像監控系統資安標準測試規範－第三部：影像錄影機」及「影像監控系統資安標準測試規範－第四部：網路儲存裝置」，並且依據AI CAM 概念之資安標準，對於「智能影像監控裝置」、「網路攝影機」、「影

像錄影機」之資安標準提出部分新增安全措施建議；另以 IVS(Intelligent Video Surveillance)智能影像監控裝置為例，研提資安防護建議基準(如表 4.1)。

表 4.1 IVS 系統資安防護建議基準

<table>
<tr><td colspan="6">IVS 系統資安防護建議基準</td></tr>
<tr><td colspan="6">實體安全</td></tr>
<tr><td>項次</td><td>控制措施</td><td>1 級</td><td>2 級</td><td>3 級</td><td>說明</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">實體埠之安全管控</td><td colspan="3">產品預設不應透過實體介面存取產品作業系統之除錯模式。若需經實體介面存取，則應通過身分鑑別作業始得執行。</td><td></td></tr>
<tr><td></td><td colspan="2">支援儲存媒體例如：硬碟保護機制，且產品之儲存媒體不應在本機以外的機器被存取。</td><td></td></tr>
<tr><td>2</td><td>實體異常行為警示</td><td></td><td colspan="2">(1)具有實體埠插拔操作記錄功能。
(2)具備相關警示功能於實體操作發生斷訊時。</td><td></td></tr>
<tr><td>3</td><td>實體防護</td><td colspan="3">外部不應有徒手即可還原預設通行碼的功能。</td><td></td></tr>
<tr><td>4</td><td>安全啟動</td><td colspan="2"></td><td>支援安全啟動(Secure Boot)功能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。</td><td></td></tr>
<tr><td>5</td><td>實體備份</td><td>具備外部儲存備份之介面，例如：USB、eSATA 等。</td><td>儲存之影像，支援資料冗餘之能力，例如：RAID 1 等</td><td>支援硬碟熱備援之功能，提升容錯能力。</td><td></td></tr>
</table>

			級以上。		
系統安全					
項次	控制措施	1 級	2 級	3 級	說明
1	作業系統與網路服務安全	作業系統與網路服務，不應存在美國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。			
				作業系統與網路服務，不應存在美國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。	
2	最小化網路與服務安全	開啟之網路服務應為必要服務之所需，防止因啟用網路介面而被侵入的可能性，且應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。 產品所收集之遙測資料應告知使用者，且未告知之遙測資料不應被收集。			
3	更新安全	韌體應具備更新機制。 支援離線手動更新，則更新檔案 應加密保護以確保機密性，且應採用 NIST SP 800 140C，CMVP Approved Security Functions (所核可之同等或以上加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中不應存在明文或甚至可被解密回復之敏感性資料。 支援線上更新，其更新路徑應通過安全通道，且安全通道版本應符合傳輸層安全性協定 v 1.2 同等或以上之版本的要求同時金鑰交換協議應支援前向安全功能(Forward Secrecy)其中於身分			

		鑑別過程應驗證憑證合法性，以及有效性(如：發證機構、有效期限、憑證格式及憑證簽章等)。具備驗證韌體之完整性及真確性的功能。具備備援更新功能，即發生更新失敗時，系統能回復至更新前之狀態。	
4	敏感性資料儲存安全	儲存的敏感性資料，應僅由獲授權個體存取。 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)不應明文儲存，而保護資料的方式應採用 NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。 提出金鑰管理程序以確保金鑰管理的品質。 敏感性資料應存放於產品的安全區域(Security Domain)，與正常作業環境隔離。	
5	網頁管理介面安全	產品之網頁管理介面不應存在引發 Injection 及 Cross Site Scripting (XSS)攻擊之漏洞。	
6	操控程式之應用程式介面安全	ONVIF(Open Network Video Interface)應用程式介面應具備身分鑑別機制，錯誤訊息不會造成敏感性資料的洩漏；另身分鑑別程序具備重送攻擊抵抗能力。 應用程式介面通行碼遵循「通行碼鑑別安全」安全標準。 應用程式介面權限遵循「權限管控」安全標準。	
7	日誌檔與警示	應具備安全事件日誌與顯示功能，確實記錄使用者的存取行為，得以查核未授權或異常的登入操作。其內容應包括完整時間戳記、使用者身分及執行結果，供後續查閱之用。 安全事件日誌應具備權限控管機制，該日誌檔不應允許未經授權的存取。 安全事件日誌檔應具備日誌滾動(Log Rotate)機制。 安全事件須確實記錄影像檔案寫入行為內容應	

		包括完整時間戳記、使用者身分及執行結果供後續查閱用。			
通訊安全					
項次	控制措施	1 級	2 級	3 級	說明
1	敏感性資料傳輸安全	敏感性資料之網路傳輸預設應通過安全通道，且安全通道版本應符合傳輸層安全性協定 v 1.2 同等或以上之版本的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。			
			接收敏感性資料傳輸之安全通道，其中於身分鑑別過程應 驗證憑證真確性及有效性，如：發證機構、有效期限、憑證格式及憑證簽章等。		
				傳輸敏感性資料之安全通道，應支援 AES 256 同等或以上加密強度的演算法。	
2	通訊協定與設置安全	提供使用者得自行開關「網路裝置資訊探詢」功能包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。 預設不應透過網路連線存取產品作業系統之除錯模式。			
			影像監控裝置所使用之通訊協定不應存在錯誤處理漏洞，包括訊息長度、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。		
3	Wi-Fi 通訊安全	提供使用者得自行開關「Wi Fi 保護設置(WPS)」之 WPS PIN 功能，而其預設值應為關閉狀態。Wi Fi 的安全機制預設應採「Wi Fi 保護存取			

		(WPA)」，且 Wi Fi 保護存取之版本應符合 Wi-Fi 保護設置 v2 同等或以上之版本的要求 。			
			支援 Wi Fi 協定則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，導致產品因發生崩潰而服務中止的情形。		
				Wi Fi 認證安全機制應支援 802.1X 基於埠的網路存取控制。	
身分鑑別與授權機制安全					
項次	控制措施	1 級	2 級	3 級	說明
1	鑑別機制安全	存取設備資源前，應透過具備防止重送攻擊之身分鑑別機制。 鑑別錯誤訊息不應顯露出合法使用者名稱。			
			設備應具備置換憑證之功能以增加憑證鑑別機制之可信度。 設備每次還原出廠設定時 憑證之金鑰(包括 SSH 及 TLS)都應改變確保每台產品金鑰之唯一性及降低金鑰外洩可能引發之資安風險。		
				(1) 產品之鑑別機制應採用 PKI 或多因子鑑別(例：token, FIDO 等強鑑別機制。	

				(2) 相連之影像監控產品應支援雙向鑑別確保相連裝置之可信度。	
2	通行碼鑑別機制安全	裝置預設通行碼都應相異；抑或首次成功取得產品存取之授權，應強制更改預設通行碼。 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元；抑或警示使用者其採用之通行碼強度不足。 通行碼強度原則參照政府組態基準之通行碼原則類別， 通行碼中之字元應符合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：!、@、#、%)；抑或警示使用者其採用之通行碼強度不足。 設備在登入通行碼的設計上應有輸入頻率及次數的限制。			
				(1) 通行碼不得存有連續字元。 (2) 是否執行通行碼歷程記錄功能	
3	權限管控	(1)是否具有權限控管機制。 (2)是否存在有限的授權時間長度			
隱私保護					
項次	控制措施	1 級	2 級	3 級	說明

1	隱私資料的存取保護	儲存的隱私資料，應被授權的個體始可存取。每次發生新的隱私存取事件時，產品應主動發出警示。			
2	隱私資料的傳輸保護	隱私資料之網路傳輸預設應通過安全通道，且安全通道版本應符合傳輸層安全性協定 V1.2 同等或以上之版本的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。			
			接收隱私資料傳輸之安全通道，其中於身分鑑別過程應驗證憑證真確性及有效性(如：發證機構、有效期限、憑證格式及憑證簽章等)。		
				傳輸隱私資料之安全通道，應支援 AES 256 同等或以上加密強度的演算法。	
應用程式安全					
項次	控制措施	普級	中級	高級	說明
1	應用程式安全	未授權或遭竄改之出廠預載應用程式(如：bin 檔、exe 檔及網頁原始碼)不應被啟動。 應用程式須於文件中標明所引用之第三方函式庫，確保引用來源是安全的。			
			應用程式須於文件提出智慧影像分析技術測試方法及辨識率		

資料來源：本研究整理。

五、結論

隨著物聯網技術日趨成熟，讓安控產業應用有了廣大的延伸空間，尤其在 AI 融入物聯網架構，雖然是將 IT 與 OT 能力極大化；然而，卻也使得原先的資安問題更顯複雜，雖然 AI 的「技術濫用引發安全問題」、「技術

或管理缺陷導致的安全問題」、「超級智能引發安全問題」、「隱私保全疑慮」、「雲端存儲的隱私疑慮」及「資料探勘的隱私疑慮」等項安全問題，因網路架構上的變化極小，在安全構面上與原有的架構沒有太多差異，但在本質上是功能面的翻新，且在應用上所賦予的責任與意義均與過去物聯網設備迥異，例如：近期「鐵路行車安全改善六年計畫」，其預警系統就是運用 AI 技術來實現預警的目的，但 AI 的測試卻被要求要在短期內完成，測試覆蓋率根本無法有效達到預警功能，這也是未來持續運用 AI 技術的一項隱憂。雖然 IT 應用重視機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，然而 AI 的技術的應用，更使得這三項特性難以達成。

因此，本研究從資通安全管理法的角度，試圖從目前應用較為廣泛的視覺 AI 技術探討資安構面與控制措施如何滿足與面對未來 AI 技術應用的安全挑戰，期使各機關應用 AI 技術時，縮短認識該領域資安概念的時間，進而提出更加完善的資安管控措施，不斷精進我國資安環境。

參考文獻

1. World Economic Forum. “The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution” 2016 Global Challenge Insight Report (2016). Preface. https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security.
2. 國家實驗研究院科技政策與研究中心，〈未來AI 發展八大新趨勢〉，2018年10月31日，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13837。
3. 洪哲倫、張志宏、林宛儒(2019，12月)。工業4.0與智慧製造的關鍵技術：工業物聯網與人工智慧。科儀新知，211期，19-25。
4. 財團法人台灣資通產業標準協會，影像監控系統資安標準-第一部。
5. 陳毅暉、林育樞、蘇苗彬(2020)。應用AIoT立體視覺裝置於崩塌地距離量測之研究。技師期刊，91(7)，83-89。
6. 胡啟恩、郭雅諒、王元凱(2018)。視覺式行人偵測追蹤技術之發展。科學新知，215期，34-45。
7. 科學Online(2019) 。AI的表現好嗎？十種常見的評估指標，2019年2月18日，https://highscope.ch.ntu.edu.tw/wordpress/?p=80752。
8. DIGITIMES(2009)。智慧影像監控系統發展應用，2009年8月6日，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000145711_bnl69iz32f8hxe05f5ty5。
9. DIGITIMES(2009)。IP化監控系統的架構策略，2009年8月6日，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000145616_8fc71o3h0i2xeq7l。
10. 江榮倫、廖伯侖(2014，11月)。潛談物聯網的安全隱憂與挑戰，勤業眾信通訊，43-47。
11. OWASP IoT Top 10，https://www.owasp.org/index.php/OWASP Internet of Things Project。
12. 趨勢科技(2020)。臉部辨識裝置爆資安漏洞，https://blog.trendmicro.com.tw/?p=65908。
13. 同註4。