因應資通安全管理法之資安管理研究
－以物聯網安全為例
Research on Cyber Security Management of Cyber Security Management Act –Take Internet of Things as an Example

運輸資訊組 吳東凌 鄭志瑋

研究期間109年2月至109年12月

摘要

調研機構Gartner於108年預測，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，我國108年制定之「資通安全管理法」亦以資通系統為規範目標。本研究目標旨在探討物聯網之資安議題並研提資安防護建議，研究方式將參考我國資通安全管理法及其相關安全規範，分析我國現有物聯網安全標準，研提物聯網資安防護控制措施與實作建議，並應用於本所物聯網設備，做為本所在資安防護上之參考。

關鍵詞：
資通安全、物聯網

一、物聯網發展趨勢與我國資通安全法簡介

調研機構 Gartner 於 108 年預測，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，而這種新型應用環境也加劇了網路風險的曝露。隨著這幾年物聯網的快速發展，政府及所有產業紛紛跟上物聯網的發展，而網路環境從使用者及企業製造與營運的安全威脅逐漸擴大到個人電腦、網際網路及物聯網；攻擊的目標也是一樣，由人擴散到機器，手段愈來愈進階，從詐騙延伸至無人智慧攻防。

物聯網屬於 OT(Operational Technology)設備的一種，其安全性與 IT 設備相比易被忽略，主要原因在於物聯網的可見性較低，加上 IT 和 OT 間的互聯，以及 IT 與 OT 人員究竟誰負責 OT 資安工作，更易導致 OT 設備暴露在風險之中，因此容易遭受到駭客及惡意程式的攻擊；另 IT 與 OT 環境也有差異，IT 主要是用於管理和處理資訊技術應用，可包含軟體、硬體及應用等三個層次，涵蓋需要資訊服務、應用系統等各種產業，例如金融、電信、公務機關、電子商務、服務業等，而 OT 則是指可針對實體設備進行監測、控制及操作的軟硬體，主要包含製造業、醫療業、關鍵基礎設施、精密機械等產業。IT 應用重視機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，而 OT 應用則除上述的三項要求之外，應更重視安全性，包含人員安全、設備安全與資訊安全等多個面向。

國內「資通安全管理法」(以下簡稱資安法)於 108 年正式施行，主要規範對象為資通系統，更凸顯出物聯網設備在安全防護上之重要性與不足。本研究將依資安法及其相關安全規範為基礎，參考政府「關鍵資訊基礎設施防護基本政策」，彙整我國現有物聯網安全規範，研提「物聯網設備防護基準表」，並以本所物聯網設備為例進行分析，做為本所後續在資安防護上之參考。

二、資通安全管理法簡介

我國於 107 年 5 月經立法院三讀通過資安法，並於同年 6 月 6 日經總統公布，期望藉由法制化，有效管理資安風險，以建構安全完善的數位環境。其責任架構區分為「事前規劃」、「事中維運」及「事後改善」等三個階段，分述如下(如圖 1)：

(一)事前規劃

資安法要求各公務機關及特定非公務機關均應先規劃及訂定「資通安全維護計畫」，使各機關據此落實相關之資安防護措施，各機關並應依據資通安全責任等級分級辦法之規定，公務機關及特定非公務機關之責任等級目前分為 A、B、C、D、E 五級，各機關依據其資安等級從管理面、技術面及認知與訓練等面向，辦理其應辦事項，並納入資通安全維護計畫。此外，在機關所擁有之資通系統部分，各機關如有自行或委外開發資通系統，應依據分級辦法就資通系統進行分級（分為高、中、普三級），並就系統之等級採取相應之防護基準措施。

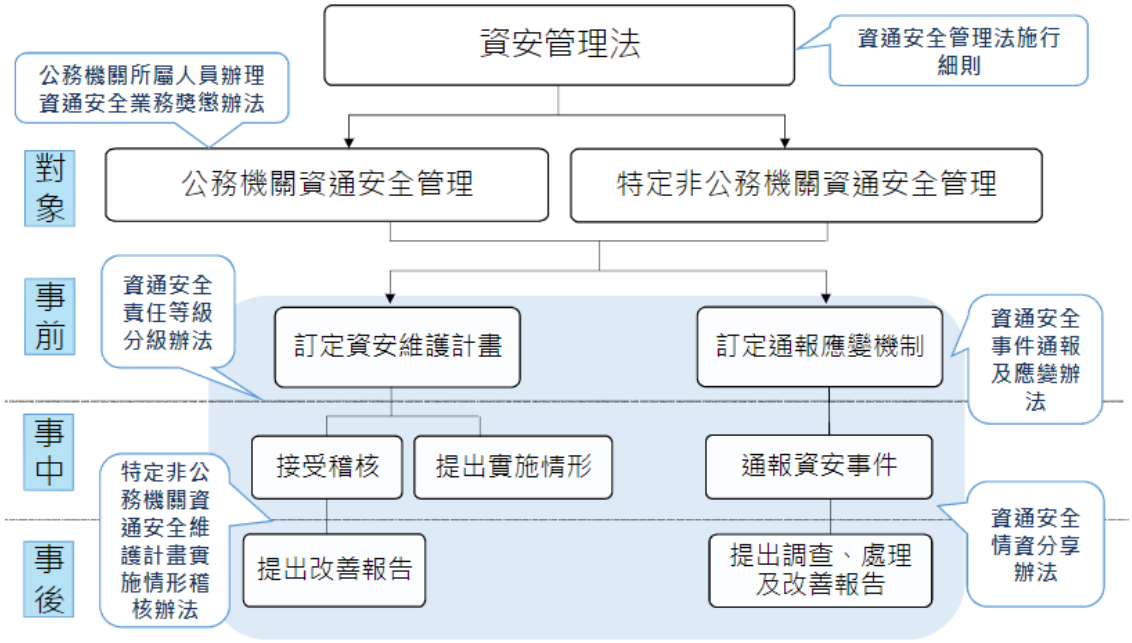
(二)事中維運

資安法要求各機關應定期提出「資通安全維護計畫」之實施情形，上級或中央目的事業主管機關並應定期進行各機關之實地稽核及資通安全演練作業。各機關如有發生資通安全事件，公務機關及特定非公務機關於知悉資通安全事件後，應於 1 小時內依規定進行資通安全事件之通報；如為第一、二級資通安全事件，並應於知悉事件後 72 小時內完成損害控制或復原作業；第三、四級資通安全事件，則應於知悉事件後 36 小時內完成損害控制或復原作業。

(三)事後改善

在事後改善部分，如各機關發生資通安全事件或於稽核時發現缺失，

則應進行相關缺失之改善，提出改善報告，並應針對缺失進行追蹤評估，以確認缺失改善之情形。



資料來源：行政院資通安全處，107 年 6 月

圖 1 資安管理法責任架構圖

三、關鍵資訊基礎設施防護基本政策簡介

關鍵資訊基礎設施防護基本政策(如圖 2)，包含「組織功能與權責」、「風險管理」、「CIIP 防護原則」、「資訊共享與合作」及「通報應變」5 個面向；其中，關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)由國家層級制定防護建議，各關鍵基礎設施領域層級依領域特性，訂定資安防護基準相關文件，以提升關鍵資訊基礎設施資安防護能力。

資料來源：行政院資通安全會報，108 年 1 月。

圖 2 關鍵資訊基礎設施防護基本政策

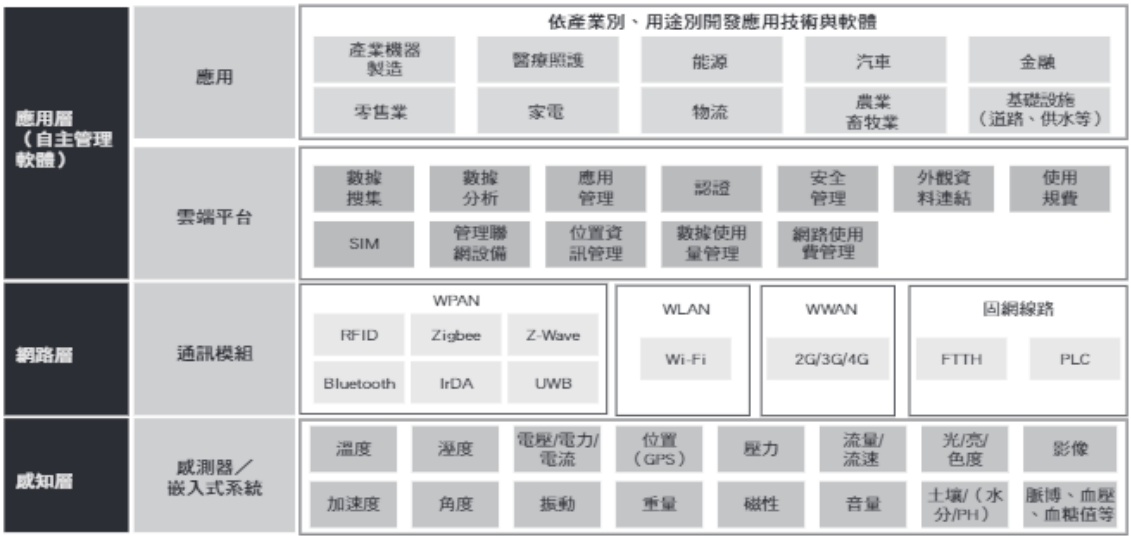
依「關鍵資訊基礎設施防護基本政策」定義，關鍵資訊基礎設施是架構於關鍵基礎設施(Critical Infrastructure, CI)之八大領域基礎上，包含能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關及高科技園區。關鍵資訊基礎設施(Critical Information Infrastructure, CII)係指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資通系統或調度、監控與數據擷取系統(Supervisory Control and Data Acquisition, SCADA)，亦屬關鍵基礎設施之重要元件。

四、物聯網簡介

莊祐軒與羅乃維(2013)[1]研究指出物聯網顧名思義是指物體與物體之間互相聯結的網路，不論是有生命的動植物或是無生命的物件，皆可做為物聯網中互聯的載體。王文娟(2016)[2]指出物聯網強調所有物品的聯網，因此所有存在之物均需具備感測、邏輯與運算能力，以便透過資通訊技術之蒐集數據、監控、分析，再回饋機器或物品，促成設備的深度學習。物聯網其架構區分應用層、網路層與感知層三個部分(如圖 3)。

[1] 莊祐軒與羅乃維(2013)。物聯網安全的現況與挑戰。Communications of the CCISA, Vol. 19 No. 4 。

[2] 王文娟(2016)。物聯網概念及應用。經濟前瞻。線上檢索日期：2020 年 6 月 17 日。



資料來源：經濟前瞻，2016 年 11 月。

圖 3　物聯網架構

臺灣學術網路危機處理中心(TANet Computer Energency Response Team, TACERT)[3]指出隨著便利且智慧的物聯網設備日漸普及，安全挑戰也漸漸受到重視，許多針對智慧型設備(如：電視、監視器、遊戲機、交通號誌等)及與其相關的行動應用程式(APP)、雲端服務等的新興攻擊行為，也隨著物聯網的普及數量日益增加，但也同時間出現相關的風險，也逐漸的造成威脅，以下說明物聯網設備特性、面臨風險及我國安全規範。

(一)物聯網設備的特性

1. 成本低廉：物聯網設備多為單一功能之設備，因此在製作成本上相對低廉。
2. 可高度客製化：物聯網設備通常為單一機板加上附加功能元件所組成，可針對不同需求進行客製化。
3. 應用層面廣：物聯網設備的應用層面廣，如運輸物流、健康醫療、智慧環境或公共教育等應用。
4. 數量眾多：綜合上列特性，因此物聯網設備數量眾多。

(二)物聯網面臨的風險

[3] 臺灣學術網路危機處理中心(2019)， IoT 設備資安防護指南。

1. 系統更新及漏洞修補不易：物聯網設備通常會以公版方式客製化生產，且生產數量眾多。因此當發現物聯網系統有問題或是存在漏洞時，往往需要使用者進行手動修補，有時可能面臨無修補程式可修補的狀況。
2. 安全認證問題：物聯網設備為能連接網路及控制設備，因此除了有線網路介面外，可能還有像藍芽、無線網卡等介面。但有時因成本考量，可能使用較舊規格的產品進行設計組成，而這舊有規格產品所使用的安全認證可能較為簡易或存在漏洞，此時可能面臨有心人士透過這些不安全的通訊協定來進行入侵動作。
3. 遭受非法應用：當一種物聯網設備遭到破解入侵後，因物聯網設備的特性意謂著採取相同設計或硬體的設備皆存在此風險。而當有心人士取得足夠數量的物聯網設備之控制權限後，將可進行相關非法應用，如殭屍網路(Botnet)的組成、分散式阻斷服務攻擊(Distributed Denial-of-Service attack, DDoS)的攻擊及挖礦(Mining)的應用等。
4. 連接埠安全：物聯網設備通常會內建一些方便管理的功能，這些功能會有特定連接埠。然而一些管理裝置所用的連接埠，可能因為通訊協定本身的問題或是設定上的不良，導致駭客很容易透過這些連接埠來入侵這些設備，來進行上述的非法存取應用，或是用於入侵內部網路的跳板。

因此，可從前述特性及風險大致歸納物聯網三層架構(應用層、網路層與感知層)普遍存在的安全議題[4](如表 1)。

表 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。

[4] 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。

	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 年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[5](如表 2)：

表 2 開放網路軟體安全計畫之統計常見安全問題彙整表

項次	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
1	弱密碼、可猜測密碼，或固定式密碼值	●	●	
2	不安全的網路服務		●	
3	不安全的環境設定介面	●		
4	缺乏安全的更新機制	●		
5	使用不安全或已遭棄用的組件	●		●
6	隱私保護不充分	●		●
7	不安全的資料傳輸和儲存	●	●	●
8	缺乏設備管理	●	●	
9	不安全的預設設置	●	●	●
10	缺乏實體保護措施	●		

資料來源：OWASP，2018。

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

(三)我國物聯網安全規範

我國在行政院科技會報辦公室及行政院資通安全處指導下，具有線介面之物聯網終端產品資安檢測，由經濟部負責推動；具無線介面或電信/傳播終端設備介面者則由國家通訊傳播委員會主責。雙方彼此合作制訂物聯網設備之資安測試標準、檢測環境，及輔導廠商產品進行資安檢測等業務等，以建置產品測試場域，協助產業進軍國際。其後經濟部以影像監控系統作為我國物聯網資安落實重點產業之領頭羊，於 106 年發布「影像監控系統資安標準（含一般要求、網路攝影機 V2.0、影像錄影機 V1.0、網路儲存裝置 V1.0）」；107 年制定「智慧巴士車載資通訊系統資安標準（含一般要求、車載機、智慧站牌）」；108 年新增「智慧路燈系統資安標準(含一般要求、智慧照明)」。茲將前述我國現有物聯網標準安全要求項目彙整如下表 3：

表 3 我國現有物聯網標準安全要求項目彙整表

項次	安全要求項目	智慧巴士	影像監控	智慧路燈
1	Wi-Fi 通訊安全	●	●	
2	日誌檔與警示	●	●	●
3	安全啟動	●		
4	作業系統與網路服務安全	●	●	●
5	更新安全	●	●	●
6	敏感性資料傳輸	●	●	●
7	敏感性資料儲存	●	●	●
8	軟韌體版本更新	●		
9	通行碼鑑別測試	●	●	

10	通訊協定與設置安全		●	
11	備份測試			●
12	雲端安全測試			●
13	傳輸對象限制	●		
14	資料完整性及來源驗證	●		
15	實體入侵防護測試			●
16	實體防護		●	
17	實體埠之安全管控		●	
18	實體異常行為警示		●	
19	網頁管理介面安全	●	●	
20	網路服務連接埠安全		●	●
21	網路服務管控	●		
22	網路管理介面安全測試			●
23	操控程式之應用程式安全		●	
24	應用程式安全測試			●
25	隱私保護能力安全測試			●
26	隱私資料的存取保護		●	
27	隱私資料的傳輸保護		●	
28	權限控管	●	●	
29	鑑別機制安全	●	●	

資料來源：本研究整理

五、研究方法

本研究參考政府「關鍵資訊基礎設施防護基本政策」及彙整我國現有物聯網安全規範，研提「物聯網設備防護基準表」，以符合資安法規範，並盤點本所物聯網設備，依設備名稱及廠牌分類整理(如表 4)，再針對這些設備進行資安等級評估，並參照研提之基準表資安控制措施，做為本所在資安防護上之參考。

表 4 本所物聯網設備分類表

項次	單位	設備名稱	設備廠牌	設備用途
1	所本部	事務機	Bizhub	公務使用
2		黑白印表機	FUJI	公務使用
3		彩色印表機	FUJI	公務使用
4		黑白印表機	HP	公務使用
5		彩色印表機	HP	公務使用
6		黑白印表機	Kyocera	公務使用
7		彩色印表機	Kyocera	公務使用
8		UPS1	DELTA UPS	備援電力
9		UPS2	DELTA UPS	備援電力
10		門禁卡機	SOYAL	環境監控
11		環境監控 IP CAM 主機	VACRON	環境監控
12		紅外線半球型 IP CAM	VACRON	環境監控
13		環境監控系統	WebAccess 圖控軟體	環境監控

14	港研中心	彩色印表機	HP	公務使用
15		彩色印表機	EPSON	公務使用
16		租用影印機	CANON	公務使用
17		多功能事務機	EPSON	公務使用
18		感應式讀卡機	璟德	公務使用
19		字幕機	C-Power	公務使用
20		溫溼度控制系統	執卓	環境監控
21		監視錄影主機	利凌	環境監控

資料來源：本研究整理

(一)驗證物聯網設備資安防護需求

以本所為例，依資訊資產盤點物聯網設備共計 21 類，運用「資通安全等級分級辦法－資通系統防護需求分級原則」(如表 5)以「機密性」、「完整性」、「可用性」及「法律遵循性」等四大構面，以災難性危害、嚴重危害及有限危害等 3 個高、中、普等級評估基準，作為本所物聯網設備安全等級標準。

表 5 資通安全等級分級辦法－資通系統防護需求分級原則

防護需求 / 等級構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生

	影響。		有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

資料來源：資通安全等級分級辦法

本所物聯網設備資安等級經評估後，其結果如表 6，計有所本部「環境監控 IP CAM 主機」、「紅外線半球型 IP CAM」、「環境監控系統」及港研中心「監視錄影主機」屬於中級防護需求，其餘設備屬於普級防護需求。

表 6 本所物聯網設備管理暨安全等級表

項次	單位	設備名稱	設備型號	設備用途	安全等級
1	所本部	事務機	Bizhub	公務使用	普
2		黑白印表機	FUJI	公務使用	普
3		彩色印表機	FUJI	公務使用	普
4		黑白印表機	HP	公務使用	普
5		彩色印表機	HP	公務使用	普
6		黑白印表機	Kyocera	公務使用	普
7		彩色印表機	Kyocera	公務使用	普
8		UPS1	DELTA UPS	備援電力	普
9		UPS2	DELTA UPS	備援電力	普
10		門禁卡機	SOYAL	環境監控	普
11		環境監控 IP CAM 主機	VACRON	環境監控	中
12		紅外線半球型 IP CAM	VACRON	環境監控	中
13		環境監控系統	WebAccess 圖控軟體	環境監控	中
14	港研中心	彩色印表機	HP	公務列印	普
15		彩色印表機	EPSON	公務列印	普

16		租用影印機	CANON	公務列印	普
17		多功能事務機	EPSON	公務列印	普
18		感應式讀卡機	璟德	公務使用	普
19		字幕機	C-Power	公務使用	普
20		溫溼度控制	執卓	環境監控	普
21		監視錄影主機	利凌	環境監控	中

資料來源：本研究整理

(二)訂定本所物聯網設備資安防護基準

分析我國「資通安全等級分級辦法－資通安全防護基準」、「關鍵資訊基礎設施資安防護建議」、「全球消費者物聯網標準 TS 103 645 V1.1.1」、「影像監控系統資安標準」、「智慧巴士車載資通訊系統資安標準」及「智慧路燈系統資安標準」等物聯網安全相關規範，多數針對特定物聯網設備訂定特定領域的防護基準，僅我國「資通安全等級分級辦法－資通安全防護基準」及「關鍵資訊基礎設施資安防護建議」從國家角度定義普遍適用基準；其中，又以「關鍵資訊基礎設施資安防護建議」從物聯網角度提出防護基準且安全構面考量較為全面，惟其考量之物聯網設備屬關鍵資訊基礎設施為主，相對某些安全需求較低之物聯網設備又不盡適用，而「資通安全等級分級辦法－資通安全防護基準」偏向資通系統安全著墨，對於不同的資安等級有明確的規範，可滿足組織掌握重點保護標的，並進行風險評鑑、有效運用資源，採行適當安全控制措施。

因此，本研究物聯網防護查核項目，結合兩者優點，針對相同部分分級，相異部分依風險分析予以訂定資安等級分級防護之控制措施，並增加「稽核與可歸責性(稽核事件、稽核紀錄內容、稽核儲存容量、稽核處理失效之回應、時戳及稽核資訊之防護)」、「識別與鑑別(內部使用者之識別

與鑑別、裝置之識別與鑑別、身分鑑別管理及鑑別資訊回饋)」及「系統與通訊防護(資料儲存之安全)」等控制領域或控制措施，以建構全面之物聯網設備資安防護基準(如表 7)。

表 7 物聯網設備防護基準表

1.網路架構(Network Architecture)				
項次	控制措施	普級	中級	高級
1	網段規劃	基於異質的裝置與網路封包，應在工業控制系統控制網路前，架設可過濾內部網路與工業控制電腦控制網路之不同異質網路封包之防火牆，並在內部網路對外連線架設處理網際網路封包防火牆。	1.在內部網路與工業控制電腦控制網路間架設DMZ，此區放置2個網路須共同存取資料之系統，讓內部網路系統或使用者不會直接存取到工業控制網路內的設備或機器。 2.防火牆須具有2種或以上之網路封包過濾功能，且防火牆須具備對工業控制電腦控制網路設備、DMZ間及內部網路進行網路連線過濾功能。	1.執行等級「中」之所有控制措施。 2.考量當組織遭受到大量攻擊或資料交換頻繁時，單一防火牆可能面臨功能喪失或效能降低等情況，為強化安全防護能量，在DMZ對外網路架設一對防火牆，分別對內部網路與工業控制電腦控制網路進行網路封包過濾。

2	邊界防護	1.監視與控制系統外部邊界，以及系統內關鍵內部邊界之通訊。 2.透過邊界防護設備，區隔出連接到外部的網路或非工業控制電腦之系統。 3.定期審查防火牆規則。		1.執行等級「中」之所有控制措施。 2.工業控制系統除以防火牆進行低中高等級防護外，組織亦需考量系統之重要性，以實體隔離或資料單向傳輸等方式實施最高等級之邊界防護。
2.存取控制(Access Control)				
項次	控制措施	普級	中級	高級
1	帳號管理	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	1.執行等級「普」之所有控制措施。 2.系統已逾期之臨時或緊急帳號應刪除或禁用。 3.禁用系統閒置帳號。 4.定期審核系統帳號之建立、修改、啟用、禁用及刪除動作。	1.執行等級「中」之所有控制措施。 2.當超過機關所規定之預期閒置時間或可使用期限時，系統應自動將使用者登出。 3.系統應依照組織所規定之情況及條件(如上班時間或指定 IP 來源)，使用系統。 4.監控系統帳號以發現違常使用，並於發現帳號違常使用時回報管理者。
2	遠端	對於每一種允許	1.執行等級「普」	1.執行等級「中」

	存取	之遠端存取類型，都應先取得授權，建立使用限制、組態需求、連線需求及文件化。	之所有控制措施。 2.監控資訊系統遠端連線。 3.系統應實作加密機制來保護遠端存取連線的機密性。 4.系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	之所有控制措施。 2.依維運需求，授權透過遠端執行特定之功能與存取相關資訊。 3.採用伺服端的集中過濾機制檢查系統使用者授權。
3	最小權限		採用最小權限原則，只允許使用者(或代表使用者行為的程序)依據任務與業務功能，完成指派任務所需之授權存取。	
4	無線網路管理	1.建立無線存取使用限制、組態/連線需求及實作指引。 2.使用無線存取系統需先取得授權。		
3.稽核與可歸責性(Audit and Accountability)				
項次	控制措施	普級	中級	高級
1	稽核事件	1.依規定之時間週期及紀錄留存政策，保留稽核紀錄，並滿足法規要求。 2.確保資訊系統有稽核特定事件(如更改密碼、登錄失敗、資訊系統存取失敗)之能力，並決定有哪些特定事件在資訊系統中應該被稽核。	1.執行等級「普」之所有控制措施。 2.應定期審查稽核事件。	

2	稽核紀錄內容	1.稽核類別需包含存取控制、要求錯誤、作業系統事件、控制系統事件、備份與儲存事件、組態變更及稽核日誌事件等。 2.稽核紀錄至少需包含事件類型、何時發生、何處發生及任何與事件相關之使用者之身分識別等資訊，並採用日誌記錄機制。	
3	稽核儲存容量	1.依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量(工業控制系統稽核儲存容量需求可能大於資通系統)。 2.依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。配置足夠的稽核儲存容量可減少因容量不足，所造成的潛在損失或降低無法稽核之發生率。	
4	稽核處理失效之回應	系統應在稽核處理失效(如儲存容量不足)之 情況下，採取適當之 行動，例如：關閉系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。	1.執行等級「普」之所有控制措施。 2.當組織規定需要即時通報的稽核失效事件發生時，系統應在組織規定之時效內，對組織特定之人員、角色提出告警。
5	時戳	使用系統內部時鐘產生稽核紀錄所需時戳，並可對映到世界協調時間(UTC)或格林威治標準時間(GMT)。	1.執行等級「普」之所有控制措施。 2.系統內部時鐘應具備定期同步機制。
6	稽核資訊之防護	1.對稽核資訊與稽核工具進行防護，以防止未授權的存取、修改及刪除。 2.對稽核紀錄之存取管理，僅限於有權限之使用者。	1.執行等級「普」之所有控制措施。 2.定期備份稽核紀錄到與原稽核系統不同之實體系

				統(如 Log 伺服器等)。 3.應防護稽核資訊之完整性。
4.營運持續計畫(Contingency Planning)				
項次	控制措施	普級	中級	高級
1	營運持續計畫	1.確認必要任務、維運功能及相關營運持續需求。 2.計畫內容需包含電力、燃料、淨水及汙水等相關支援系統，並以恢復必要功能或業務為首要目標。 3.提供復原目標、復原優先事項及度量標準。	1.執行等級「普」之所有控制措施。 2.定期審查工業控制系統營運持續計畫。	
2	安全模式		1.當危及安全的條件被偵測時，系統需限制只能進入安全模式操作。 2.安全模式操作可以自動或手動啟動，如在有限的電力或減少通訊頻寬下，只允許某些功能進行。	
3	控制系統備援		1.重要的控制系統應具有備援系統。 2.備援系統應與時俱進。 3.評估備援系統時，應將事件鑑識(如稽核日誌)與加密功能，列入系統備援考量。 4.執行等級「中」之所有控制措施。	
5.識別與鑑別(Identification and Authentication)				
項次	控制措施	普級	中級	高級

1	內部使用者之識別與鑑別	1.系統應具備唯一識別及鑑別組織使用者(或代表組織使用者行為之程序)，不應有共用帳號之行為。 2.系統應採用實體安全措施進行識別。	1.執行等級「普」之所有控制措施。 2.對帳號之網路或本機存取採取多重認證技術(如鎖IP)。
2	裝置之識別與鑑別	1.應識別與鑑別連接至工業控制系統裝置，以及其限制連線數量與類型。 2.應識別組織所屬裝置與非個人裝置(如委外廠商所屬裝置與行動裝置等)。	
3	身分鑑別管理	使用預設密碼登入系統時，應於登入後要求立即變更。	1.執行等級「普」之所有控措施。 2.基於密碼之鑑別系統應強制最低密碼複雜度；強制新的密碼最少變更之字元數；強制密碼最短及最長之效期限制。 3.使用者更換密碼時，組織內應訂定異於使用過密碼相同之次數(如不可以與前3次使用過密碼相同等)。 4.具備帳戶鎖定機制，組織應訂定帳號登入進行身分鑑別失敗次數(如登入失敗5次等)，以及不允許該帳號繼續嘗試登入之時間(如至少15分鐘等)。 5.身分鑑別相關資訊不以明文傳輸。 6.身分驗證機制需防範自動化程式之登入或密碼更換嘗試。

4	鑑別資訊回饋	系統應遮蔽在鑑別過程中之資訊(如密碼等)，以防止未授權之使用者可能之窺探或使用。		
6.系統與通訊防護(System and Communications Protection)				
項次	控制措施	普級	中級	高級
1	傳輸之機密性與完整性		盡其可能使用加密機制(如數位簽章或加密雜湊函數等)，以防止資訊揭露。	
2	資料儲存之安全		1.靜置資訊指資訊位於系統特定元件，如儲存設備上之狀態。與系統相關需要防護的資訊，如系統組態設定等資訊應予以防護。 2.機密資訊應加密儲存。	
7.系統與服務獲得(System and Services Acquisition)				
項次	控制措施	普級	中級	高級
1	外部系統服務	外部系統屬於組織系統授權範圍外實作的服務，但不是組織系統的一部分(如供應商維修系統等)，應要求外部服務供應商遵守與符合組織的安全要求。		
2	系統文件	1.組織應建立 ICS 系統、系統元件及系統服務相關安全措施的實作與運作，相關之管理文件。 2.組織應定期確認管理文件內容的品質與完整性。		
8.實體與環境防護(Physical and Environmental Protection)				
項次	控制措施	普級	中級	高級
1	實體存取授權	1.應建立系統所在的設施實體存取授權之使用者清單，並定期審查存取清單。 2.當使用者不再需要存取時，應由設施存取清單移除該使用者。		
2	實體存取控制	1.ICS 應考量實體安全之相依性，並考量電子與機械設備室的進出管制。		

		2.緊急事件發生時，工業控制設備應進行限制授權管制。	
3	實體存取監控		1.組織應監控系統設施的實體存取，並監控、偵測及警示實體安全事件。 2.監控範圍應包含備援系統與遠距離終端設備等。
4	緊急電源		1.應建立能供應最小業務負載量之長時間電力備援。 2.建議可採用替代電力供應，做為緊急備源電源。
5	溫溼度控制		系統環境的溫溼度控制系統(如冷暖氣系統、照明系統等)，也屬於工業控制系統重要一環，須定期維護溫溼度控制系統。
6	水損防護		在關鍵基礎設領域類別所使用的工業控制系統運作時，水的供應狀況會影響系統運作。應確保工業控制系統周邊設備，如火災防護、緊急照明及備援系統等，建議具有水偵測防護管理，避免漏水造成系統損害。
7	第三方/陪同者的存取	1.篩選、執行及文件化第三方人員的安全控制，並監控服務提供者的行為與承諾。 2.在相關合約與協議文件中明確包含人員安全控制。	
9.系統與資訊完整性(System and Information Integrity)			
項次	控制措施	普級	中級 / 高級
1	漏洞修補	系統的漏洞修復應測試有效性及潛在影響，並依律定之時間週期更新。	1.多數系統與相關軟體，常需藉由供應商進行軟體更新，需定期追蹤與驗證漏洞修復。若因技術限制、個別資通系統之設計、結構或性質等因素，致系統漏洞無法修復時，應實作降低弱點暴露因應對策。 2.工業控制系統進行漏洞修補後，應進行測試。
2	惡意程		1.系統應具有偵測惡意程式防護機制。

	式碼防護		2.防護工具應具有針對工業控制系統防護，如流量監控與稽核等。
3	系統監控		1.使用監控工具等相關技術，須確認不會影響工業控制系統操作。 2.當既有之工業控制系統不能監控出入流量時，應單獨對相關資通系統進行監控。
4	可預測之故障預防		1.參考系統之平均故障時間(Mean Time To Failures, MTTF)，做為系統可靠度與潛在故障考量基準。 2.依據平均故障時間、維修與運作紀錄及產品生命週期等資訊，定義系統使用期限，以降低元件故障可能造成潛在危害。
5	故障容許度		定義系統裝置故障容許度標準，並進行相關防護措施。
10.組態管理(Configuration Management)			
項次	控制措施	普級	中級	高級
1	組態變更控制	1.系統相關組態變更應予以文件化，並保留系統組態控制變更紀錄。 2.依規定的時間週期，保留系統組態控制變更紀錄。 3.稽核與審查系統組態控制變更紀錄。		
2	最基本功能	1.設定系統僅提供業務必要的功能。 2.系統僅提供必要的功能，關閉不須使用之功能、埠、協定及服務。 3.系統應將獲得授權執行的軟體程式列入白名單。 4.應定期審查必要的功能內容與白名單。		
11.組織管理(Organization Management)				
項次	控制措施	普級	中級	高級
1	委外管理	委外管理對於供應商與承包商的資通安全要求，相關詳細管理可參考「政府資訊作業委外安全參考指引」。		
2	人員管	1.應建立人員資安政策之目的、範圍、角色、責任、管理承		

	理	諾及組織間之協調。 2.對系統使用者(包含管理人員、高階管理者等)提供基本的資安認知教育訓練，進行教育訓練時間應包含當系統有新使用者、系統功能變更及定期實施等。 3.人員離職時，應於規定時間禁止存取資通系統。
3	風險政策	1.應對資訊與系統分級，且建立相關安全分級政策。 2.應訂定期審查風險評鑑結果。
4	事件應變	1.應建立事件應變政策與計畫。 2.應定期進行事件應變演練與訓練。 3.應定期檢視事件處理程序。

資料來源：本研究整理

六、研究座談會

本研究分別於109年7月30日及12月28日召開期中及期末座談會，邀集資安領域專家就本研究提出建議，其審查意見及辦理情形如下(如表8)：

期中座談會		
專家人員簡介	審查意見	審查意見辦理情形
蔡嘉志 大同世界科技股份有限公司網路資安暨物聯網事業處工程師	物聯網設備因種類眾多，先天上具有較多安全性問題，建議「表1物聯網普遍安全議題彙整表」臚列之資安議題外，可加入網頁介面漏洞修補、後臺安全管理、強化加密與認證機制、最小化存取及韌體更新需認證等議題。	因表1係引用參考文獻，該建議相關議題將納入表3修訂。
王煜詔 財團法人臺灣商品檢測驗證中心資訊與通信技術服務部組長	「表3我國現有物聯網標準安全要求項目彙整表」參考之文獻引用僅有資安標準第一	已將第二、三部納入參考，並配合修訂表3。

	部，但該文獻還包含第二、三部，建議納入參考。	
劉向榮 聯準科技服務有限公司資安顧問	物聯網設備傳輸時應加密，關於「表 7 物聯網設備資通系統防護基準表」建議加入此項檢核項目。	已配合修訂。
期末座談會		
專家人員簡介	審查意見	審查意見辦理情形
吳文進 聯準科技服務有限公司	建議本案後續可朝智慧運輸、車聯網設備繼續探討。	納入後續研究參考議題。
翁明義 聯準科技服務有限公司	本所部分物聯網設備置於所外，未來可將此類設備納入 ISMS 稽核範圍。	配合辦理。

資料來源：本研究整理

七、結論與建議

(一)物聯網雖然使周遭設備連結成網路，便利了生活，也因投入物聯網發展為臺灣資通訊產業帶來產業發展，卻也成為個人隱私外洩的媒介、網路犯罪的工具，更可能損害大眾利益或危及國家安全。因此，各國開始重視影響人民生活、國家經濟及健康等關鍵基礎設施所屬之工業控制系統之資通安全。

(二)一般 IT 設備較重視機密性，與物聯網設備在功能設計理念具有相當大的差異。本研究針對物聯網安全提出研究，再參酌資安法及相關法令規範，將本所物聯網設備進行資安等級分級及對應研提之防護基準表，除可強化本所資安防護之外，更能利用不同領域之物聯網設備，提供資安防護參考。

(三)本研究彙整我國物聯網安全相關規範，分析各法規、標準之差異，並

結合各標準相關優點歸納物聯網防護檢核項目，有助於建構全面之物聯網安全防護基準，可以有效滿足組織掌握重點保護標的，並促使進行風險評鑑、有效運用資源，採行適當安全控制措施。

(四)本研究盤點本所物聯網設備共計 21 類，運用「資通安全等級分級辦法－資通系統防護需求分級原則」區分「機密性」、「完整性」、「可用性」及「法律遵循性」等四大構面，以災難性危害、嚴重危害及有限危害等 3 個高、中、普等級為評估基準，做為本所物聯網安全等級評估之參考標準；經評估所本部計有「環境監控 IP CAM 主機」、「紅外線半球型 IP CAM」、「環境監控系統」及港研中心「監視錄影主機」屬於中級防護需求，其餘設備屬於普級防護需求。

(五)本研究後續可運用研提之「物聯網資通安全控制措施防護基準」及「關鍵資訊基礎設施資安防護建議」，賡續探討交通領域物聯網之資安議題，以強化本研究成果，並提升本所資通安全防護。

參考文獻

1. 莊祐軒與羅乃維(2013)。物聯網安全的現況與挑戰。Communications of the CCISA, Vol. 19 No. 4 。
2. 王文娟(2016)。物聯網概念及應用。經濟前瞻。線上檢索日期：2020年6月17日。
3. 臺灣學術網路危機處理中心(2019)。 IoT設備資安防護指南。
4. 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。
5. OWASP IoT Top 10，https://www.owasp.org/index.php/OWASP Internet of Things Project.