11015G0015

集合住宅類智慧建築資通訊安全應用之法制規定調查研究

受委託單位　：　財團法人資訊工業策進會

研究主持人　：　王自雄

研究員　　：　周晨蕙

研究期程　　：　中華民國 110 年 2 月至 110 年 12 月

計畫經費　　：　新臺幣玖拾捌萬肆仟伍佰元

內政部建築研究所委託研究報告

中華民國 110 年 12 月 3 日

（本報告內容及建議，純屬研究小組意見，不代表本機關意見）

目次

表次

圖次

摘要

關鍵詞：智慧建築、集合住宅、資訊安全

一、 研究緣起

進入 21 世紀後，人工智慧及資通訊技術取得突破性發展，帶動物聯網相關應用崛起。由於智慧家庭是建構智慧化社會的一環，產業界紛紛聚焦研發智慧家庭解決方案。資訊及隱私安全為智慧建築導入物聯網相關應用的重要課題，不僅民眾對於資安抱持疑慮，亦有半數以上企業認為聯網設備潛在的隱私風險將對業務和投資造成影響，阻礙業者投入相關市場之腳步。為解決上述問題，世界各國陸續推動相關政策、制定法律或指引、標準等。

我國於 2017 年通過《資通安全管理法》，並陸續針對不同領域制定資安標準和驗證制度，惟《資通安全管理法》規範對象為公務機關和關鍵基礎設施提供者，不及於一般建築物或住宅所有權人，且目前尚欠缺針對智慧建築領域之資安標準或指引。基於上述理由，應有調查分析國外相關法制規定，以及國內集合住宅類智慧建築導入資通訊應用時可能面臨之安全風險，研擬我國集合住宅類智慧建築導入資通訊安全應用注意事項草案，供主管機關參考之必要。

二、 研究方法與過程

在研究方法上，本研究將透過訪談了解國內集合住宅類智慧建築導入資通訊安全應用時可能產生之風險，以及國內相關法規及標準制定狀況，並收集國外集合住宅導入資通訊安全應用法法制規定和標準，作為研提我國於集合住宅內導入智慧建築資通訊安全應用注意事項草案之參考。

三、 重要發現

本研究經蒐集並整理我國、日本、美國、歐盟及英國等地區或國家，有關智慧建築或資通訊安全應用之法制規定，發現由於資通訊或聯網設備種類及態樣廣泛，故相關文件首先都會釐清適用對象和範圍，以利後續設想可能發生之意外事件，作為分析潛在威脅和風險之基礎。其次，各國在研擬相關規範時，日本從功能面和管理面出發，依序針對各利害關係人分別提出建議；歐盟則將建議分為「政策」、「組織、人員和流程措施」、「技術措施」3 類，而本報告進行訪談時，

亦有專家認為可軟硬體面和程序面（包含人員管理在內）著手研擬注意事項。

本研究依據上述研究成果，並參酌臺灣資通產業標準協會所制定之「消費性物聯網產品資安標準」及「物聯網場域資安防護評估指引」，根據本研究對於集合住宅類智慧建築之定義、發展狀況及國外法制調查整理等，提出我國集合住宅類智慧建築資訊安全應用情境，整理我國集合住宅類智慧建築架構及主要智慧化項目，以及各項智慧化服務可能涉及之利害關係人，並從功能面及管理面出發，分析我國集合住宅類智慧建築之可能發生之意外事件、資安威脅及弱點。最後，本報告針對我國集合住宅類智慧建築可能存在之弱點，比對各國針對智慧住宅或聯網設備提出之規範，研提我國集合住宅類智慧建築導入資通訊安全應用注意事項。

四、 主要建議事項

經過研究發現，本研究針對智慧建築之資訊安全，研提立即可行建議及長期建議如下：

建議一

加強我國智慧建築資訊安全之規範：立即可行建議

主辦機關：內政部建築研究所

協辦機關：財團法人資訊工業策進會

智慧建築為未來 5G 網路和物聯網之主要應用場域之一，內政部建築研究所自 2004 年建立候選智慧建築證書及智慧建築標章制度，目前智慧建築標章評估之八項指標：綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新，並未將資訊安全列為指標之一，雖具體評估內容中部份已納入資訊安全概念，如資訊通信指標之基本項目「2.3 區域網域」，其評估內容包括「適當的資訊安全保障設備」等，但仍應進一步檢視及精進，且有關資訊安全之評估內容散落在各項指標當中，故應有討論是否將資訊安全列為獨立評估指標，以及指標應包含之評估項目及具體評估內容等事項之必要。

本計畫已於 110 年度調查國外有關智慧建築和物聯網相關之規定，未來可以上述法制調查結果和國內現況為基礎，檢視我國智慧建築標章內有關資訊安全之規

定，並提出評估指標、評估項目及內容之調整建議。

建議二

強化公寓大廈管理服務人員資安意識與能力：中長期建議

主辦機關：內政部營建署

協辦機關：內政部建築研究所

集合住宅類智慧建築之資訊安全有賴於管理面執行與落實，管理單位必須選用合適之 IoT 設備，並建立資訊安全政策或標準作業流程，遵照一定程序選購、使用、管理、維護和更新、廢棄相關設備或系統，且管理人員亦須具備一定之資訊安全意識與能力，針對意外事件能即時應對處理，方能有效確保集合住宅類智慧建築之資訊安全。基於上述理由，建議未來主管機關可研擬是否加強公寓大廈管理服務人員之訓練，將資訊安全科目納入《公寓大廈管理服務人員管理辦法》第 20 條之管理服務人員訓練課程。

Abstract

keywords： smart building, Congregate housing, data security

Internet of Things (IoT) devices are being deployed in a wide variety of consumer applications at homes, offices, buildings, cities, and so on. Through IoT device, Smart building can gather information from the environment inside and outside to optimize temperature, lighting, and other elements. Because of this, Smart building can provide comprehensive, convenient, intelligent, and interactive services for both individuals and their surroundings. While IoT bringing numerous benefits, it also causes severe threats to privacy and security. Improper device updates, lack of security protocols, user unawareness, and active device monitoring are among the challenges that IoT is facing.

For above reason, California made laws requiring “reasonable security features” to be added to IoT devices. In addition, the United Kingdom asked IoT device manufacturers to meet security standards. For avoiding risk of IoT, this article research IoT cybersecurity legal issue, and focus on Congregate housing that using IoT technology. First of all, this article will interview related operator to understand actual situation, then analyze IoT cybersecurity regulation of the USA, EU, the United Kingdom and Japan. At last, this article will according the above research, and draft notice of Congregate housing use IoT device.

Research methods:

1. in-depth interview

   This research intends to learn about the problems that may be encountered in practice through interviews with industry experts, and to ask experts for their opinions and suggestions.

2. Document Analysis

   This research collects and analyzes relevant foreign standards as a reference.

Major outcomes:

1. Sort out and analyze the cybersecurity regulations related to the Internet of Things, connected devices, and smart buildings in the United States, the European Union, the United Kingdom, Japan and our country.
2. Develop a draft of precautions for the security application of smart buildings in our country's Congregate housing.

第一章 緒論

第一節 研究緣起

進入 21 世紀後，人工智慧及資通訊技術取得突破性發展，帶動物聯網相關應用崛起，典型之物聯網應用領域包括：智慧城市、智慧交通、智慧建築及智慧家庭等。由於智慧家庭是建構智慧化社會的一環，產業界紛紛聚焦研發智慧家庭解決方案，使 2019 年全球智慧家庭市場規模達到 1,055 億美元，雖然 2020 年受到新冠肺炎疫情影響，市場規模衰退 3.7%，但未來仍有機會再次成長，預估 2019～2023 年間，全球智慧家庭市場規模可望成長至 1,454 億美元，顯見智慧家庭及相關資通訊應用已成為人們日常生活不可或缺的一部份。

資訊及隱私安全為智慧建築導入物聯網相關應用的重要課題，不僅民眾對於資安抱持疑慮，根據調查顯示，亦有半數以上企業認為聯網設備潛在的隱私風險將對業務和投資造成影響，阻礙業者投入相關市場之腳步。為解決上述問題，美國加州於 2018 年 9 月制定、2020 年 1 月施行《SB-327 資訊隱私：連網裝置》（SB-327 Information Privacy: Connected Devices），要求設備製造商所提供之設備應提供「合理的安全功能」（reasonable security feature）；英國數位、文化、媒體和體育部（Department for Digital, Culture, Media and Sport,DCMS）宣示將強化聯網設備安全，確保出售給英國消費者之聯網設備符合有關密碼唯一性、提供聯繫窗口和明確規定設備安全性更新時間等要求。

上開法規和政策雖然已就聯網設備之資訊安全加以規範，但仍有專家認為不夠具體，而業界也希望能有更明確地規範加以遵循，在此背景下，日本於 2021 年 4 月 1 日提出「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン），其係專門針對智慧家庭制定之指引，深具參考價值。

我國於 2017 年通過《資通安全管理法》，經濟部工業局則自 2017 年起推動物聯網資安產業標準與檢測認驗證制度，針對影像監控系統、智慧巴士資通訊系統與智慧路燈系統制定產業資安標準和檢測規範標章；而內政部建築研究所於 2019 年 1 月出版「智慧住宅高齡照護設計指引」，供建築師和室內裝修專業人員參考，設計符合高齡照護需求之智慧住宅。

綜觀上述規定，可知我國雖然已制定《資通安全管理法》，並陸續針對不同領域制定資安標準和驗證制度，惟《資通安全管理法》規範對象為公務機關和關鍵基礎設施提供者，不及於一般建築物或住宅所有權人，而物聯網資安產業標準目前亦僅限於特定設備，綜上所述，可知我國目前仍缺乏針對集合住宅類智慧建築導入相關應用之規範。基於上述理由，應有調查分析國外相關法制規定，以及國內集合住宅類智慧建築導入資通訊應用時可能面臨之安全風險，就相關應用可能衍生之法律問題及因應對策，研擬我國集合住宅類智慧建築導入資通訊安全應用注意事項草案，供主管機關參考之必要。

第二節 研究目的

本研究之範圍僅限於集合住宅類之智慧建築，根據上述研究背景及範圍，本計畫之研究目的如下：

壹、 蒐集、整理集合住宅類智慧建築資通訊安全應用之國外法規或國際標準等規範，了解國外如何因應利害關係人導入資通訊安全應用時可能發生權益受損之風險，作為後續研究參考。

貳、 透過訪談或文獻分析等方式，調查並分析國內集合住宅類智慧建築導入資通訊應用時可能面臨之安全風險，以及國內集合住宅類智慧建築資通訊安全應用之法制規定。

參、 綜整上開導入資通訊安全應用之風險，以及各國法制對策，就智慧建築資通訊安全應用可能衍生之法律問題及對策，研提我國「集合住宅類智慧建築資通訊安全應用法制規定」注意事項草案。

第三節 研究方法與流程

壹、 研究採用之方法

一、 深度訪談法

本研究將透過訪談，了解國內集合住宅類智慧建築導入資通訊安全應用時可能產生之風險，以及國內相關法規及標準制定狀況。

貳、 文獻分析法

本研究將收集國外集合住宅導入資通訊安全應用法法制規定和標準，作為研提我國於集合住宅內導入智慧建築資通訊安全應用注意事項草案之參考。

參、 研究採用方法之原因

一、 深度訪談法

為制定集合住宅類智慧建築導入資通訊安全應用之注意事項，本研究擬透過訪談業界專家，了解實務上可能遭遇的問題，並請益專家看法和建議，以利編寫注意事項草案。

二、 文獻分析法

由於我國目前尚無針對集合住宅類智慧建築之規範或標準，故本研究擬透過蒐集、整理、分析國外集合住宅類智慧建築導入資通訊安全應用相關規範，作為編寫注意事項草案之參考。

肆、 預計可能遭遇之困難及解決途徑

為了解國內集合住宅類智慧建築導入資通訊安全應用狀況，以及實務上遭遇之困難，必須挑選合適對象進行訪談。本研究擬以智慧建築、物業管理等公協會，以及國內智慧住宅解決方案業者，或具有建造和維運智慧住宅經驗者，如台北市政府都市發展局為對象進行訪談。

伍、 研究步驟

圖 1-1 研究流程圖

（資料來源：本研究整理）

第四節 預期成果與效益

根據上述研究目的，本計畫預期成果與效益如下：

壹、 透過調查及訪談業者，瞭解國內集合住宅類智慧建築導入資通訊安全應用之狀況，以及可能產生的風險（如常見的攻擊方式、可能導致受損的權益等）。

貳、 蒐集及整理國內外法制規定和標準等資料，進行國內外集合住宅類智慧建築導入資通訊安全應用之法制分析，提供後續研究參考。

參、 透過編寫「集合住宅類智慧建築資通訊安全應用法制規定」注意事項草案，除可提供主管機關推動智慧建築相關計畫參考外，亦有助於推動智慧建築導入相關應用，以擴大智慧建築及相關智慧化應用市場。

第二章 集合住宅類智慧建築資通訊安全應用之法制規定

第一節、 我國集合住宅類智慧建築之定義及發展狀況

壹、 集合住宅類智慧建築定義與主要導入之智慧化項目

所謂集合住宅，根據《建築技術規則》第一條第一項第二十一款規定，係指「具有共同基地及共同空間或設備，並有三個住宅單位以上之建築物。」另根據《建築物使用類組及變更使用辦法》第二條規定附表二建築物使用類組使用項目舉例，可知集合住宅屬於 H 住宿類中 H-2「供特定人長期住宿之場所」。

惟我國法上雖有定義何謂集合住宅，但針對智慧建築（Intelligent Building,IB），目前卻尚未導入相關概念並予以法制化，主管機關僅配合智慧建築相關技術發展，修正《建築技術規則》建築設備篇第 136 條有關建築物電信設備之規定，並於上述規定內明定應引進光纜之建築物類型、應設置之電信設備與空間等，故尚無法在法律或命令層級上定義何謂智慧建築，只能參考其他文獻或規定釐清其概念[1]。

關於智慧建築，《智慧型公寓大廈自動化系統設計準則之研究》將其定義為『係指建築物及其基地設置建築自動化系統（Building Automation System，BAS），配合建築空間與建築體元件，從人體工學、物理環境、作業型態及管理型態角度整合，將建築物內之電氣、電信、給排水、空調、防災、防盜及輸送等設備系統與空間使用之運轉、維護管理予以自動化，使建築物功能與品質提昇，以達到建築之安全、健康、節能、便利與舒適等目的。其基本之構成要素需包括建築自動化系統裝置、建築使用空間、建築運轉管理制度』[2]。另外，《智慧建築標章申請審核認可及使用作業要點》第二點則將定義智慧建築為「指藉由導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物。」

在上述定義中，皆提到智慧建築構成要素之一為建築自動化系統裝置，而

1 監察院調查報告，《政府推動綠建築與智慧建築之成效案》，2019/12/17，https://twecoliving.blogspot.com/2019/12/108982.html（最後瀏覽日期：2021/06/22）。

2 內政部建築研究所，《智慧型公寓大廈自動化系統設計準則之研究》，頁 21（1996）。

建築自動化系統係指『建築物內一個以電腦為基礎之系統，具收集資料、數據，並據此做出動作之能力，亦可針對建築物各系統之性能狀況進行分析，以及資料、數據之編輯等。通常由現場處理裝置、中央處理裝置、感測裝置、動作裝置、配線所構成。』[3]。由於建築物有不同類型，故建築自動化系統裝置亦會依照需求而有不同類型，以智慧型公寓大廈為例，其自動化系統就包括中央監控系統、防災自動化系統、防盜自動化系統、通信自動化系統和環控自動化系統等[4]。

此外，智慧建築內通常會導入各種智慧化項目，針對建築物可能導入之智慧化項目，內政部建築研究所《既有建築物智慧化改善之研究-以集合住宅為例》報告以《智慧建築評估手冊》合格級門檻為基礎，建議既有集合住宅應導入之智慧化項目，如綜合佈線項目應包含：社區設置電信室或電信總箱、光纖到府、宅內配線箱；資訊通信項目應包含數位式電話交換功能須配置不斷電系統、公共區域設置無線區域網路等。

另根據統計，2008 年至 2013 年間辦理「既有建築物智慧化改善工作」之民間住宅類建築，申請補助之項目以安全防災最高，導入之項目側重門禁與監控管理系統；其次為便利舒適項目，偏重於網路佈建與社區管理智慧化入口網站之建設；然後為節能管理項目，大多為紅外線感應照明、智慧型監控管理系統與控制迴路系統之建置；最後為健康照護項目，以健康照護整合性管理平台為主[5]。

由上述建議項目和統計，可知既有建築物主要導入之智慧化項目。此外，內政部建築研究所於 2020 年出版《既有住宅社區導入智慧化改善指引》，說明既有住宅社區導入智慧化改善之步驟程序、相關注意事項、建置方式、實際案例之操作方式及可行之解決方案等，亦可作為了解既有集合住宅智慧建築樣貌之參考。

上述為有關既有集合住宅之討論，針對新建集合住宅主要導入之智慧化項目，由於近年我國中央及各縣市政府均積極推動社會住宅，希望能將社會

3 同前註，頁 21-22。

4 同前註，頁 24。

5 郭霖，〈住宅類既有建築智慧化之效益評估研究〉，中國文化大學建築及都市設計學系碩士論文，頁 3-4（2014）。

住宅作為智慧建築示範場域，故本報告擬參考目前我國社會住宅智慧社區架構及應用之智慧化服務。

根據台北市政府都市發展局出版之智慧社區建置規範手冊，智慧住宅架構包括建築自動化、通訊自動化、安全自動化、家庭自動化和能源管理系統，而智慧社區則進一步提供物業管理、智慧微電網、能源與節能、停車場管理、智慧生活服務、安全防災和智慧家庭照護等服務[6]。從上述架構出發，手冊指出所有公宅都應設置「智慧三表（水表、電表、瓦斯表）」並取得智慧建築標章，並建置基本智慧化設施，包括節能（智慧電網）、社區安全、智慧化停車管理、智慧管理雲、及相關智慧服務等[7]。此外，智慧社區建置規範手冊並針對安全防災、資訊通信、建築自動化、節能管理與智慧電網、智慧生活服務、物業管理等六種需求面向，提出必須建置項目之說明，包括設計通則、設計原則和設計標準等[8]。

6 台北市政府都市發展局，《臺北市公共住宅智慧社區建置規範手冊》，頁 2（2017）。

7 同前註，頁 8（2017）。

8 台北市政府都發局，〈台北市公共住宅智慧化執行策略〉，2017/11/03，https://tiba.org.tw/wp-content/uploads/dlm_uploads/2017/11/03_%E8%87%BA%E5%8C%97%E5%B8%82%E6%94%BF%E5%BA%9C%E6%99%BA%E6%85%A7%E5%85%AC%E5%AE%85%E6%99%BA%E6%85%A7%E5%8C%96%E5%9F%B7%E8%A1%8C%E7%AD%96%E7%95%A5%E5%BC%B5%E8%A3%95%E9%9A%86.pdf（最後瀏覽日：2021/09/29）。

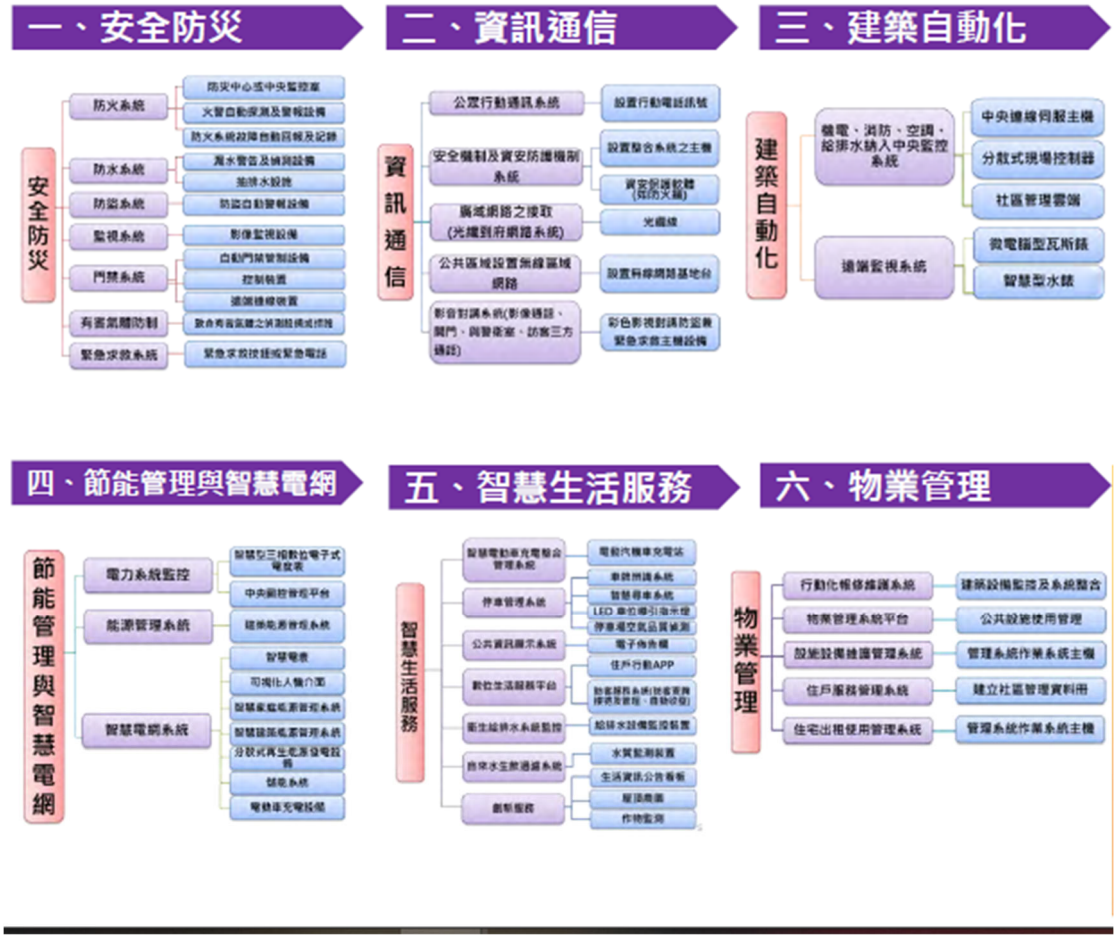

圖 2-1 台北市政府智慧社區建置規範手冊必須建置項目（資料來源：台北市公共住宅智慧化執行策略，2017）

另有研究比對各縣市所編寫之相關手冊，發現社會住宅包括「必須建置項目」及「選擇建置項目」兩類，必須建置項目以《智慧建築評估手冊》銀級門檻為主，並包含物業管理與基本生活服務等子項，例如安全防災、資訊通信、建築自動化、節能管理、智慧電網、智慧生活服務等；選擇建置項目則依據各社宅之定位，可選用各種生活輔助智慧項目，例如智慧圖書館、智慧托育、智慧商業零售以及智慧健康照護等[9]。由於上述選擇建置項目並非常態，故本報告將以必備建置項目，作為新建集合住宅主要導入之智慧化項目。

綜上所述，本文所稱之集合住宅類智慧建築，係指我國法上所稱導入資通

9 《社會住宅應用智慧化管理之研究》，內政部建築研究所委託研究報告，頁 23-25（2019）。

訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物，並屬於 H-2「供特定人長期住宿之場所」類別之「具有共同基地及共同空間或設備，並有三個住宅單位以上之建築物」。惟因集合住宅類智慧建築可能導入之智慧化項目甚廣，為進一步特定集合住宅類智慧建築之範圍，本文所稱之集合住宅類智慧建築，其所導入之智慧化項目，主要包括前述社會住宅必備建置項目，以及既有集合住宅進行智慧化改善時主要導入之項目，如安全防災相關項目（門禁與監控管理系統）、便利舒適項目（網路佈建與社區管理智慧化入口網站）、節能管理項目（紅外線感應照明、智慧型監控管理系統與控制迴路系統和健康照護項目等。

貳、 我國集合住宅類智慧建築發展歷程

住宅建築型態基本上可分為獨戶住宅和集合住宅兩種，前者擁有獨立建築基地和出入門戶，而後者則多戶共用建築基地、出入門戶和樓梯、電梯等設備空間，另依《建築技術規則》第 55 條規定，六樓以上建築物必須裝設電梯，故集合住宅又可分為無電梯公寓和電梯公寓兩種[10]。我國傳統住宅建築型態以獨戶住宅為主，如透天厝、三合院、四合院等，直到 60 年代初期，伴隨都市化進展，建築型態也從平面轉向立體垂直發展，惟當時仍以五樓以下無電梯公寓為主，及至 70 年代末期，因電梯工程技術進步，電梯公寓開始逐漸增加[11]。根據行政院主計處統計，各縣市以 2-5 層樓公寓為主要建築類型占 61.8%，6 樓以上建築物則分佈於中心都會縣市，顯見集合住宅已成為我國都市地區主要建築物型態[12]。

隨著新興科技發展和民眾對於生活品質的要求，智慧化設備或系統開始導入住宅內部或物業管理，智慧住宅逐漸成為未來住宅建設主流。為促進建築與資通訊科技之整合，內政部建築研究所於 2004 年建立候選智慧建築證書及智慧建築標章制度，申請候選智慧建築證書之對象為規劃設計階段

10 〈住宅類〉，內政部營建署，2001/12/04，https://www.cpami.gov.tw/index.php?option=com_content&view=article&id=98&Itemid=86（最後瀏覽日期：2021/05/27）。

11 林福展，〈從台灣傳統到現代住宅「起居空間」轉變之探討〉，中華大學碩士論文，頁 2-8（2007）。

12 〈台閩地區住宅狀況研析〉，行政院主計處，https://www.stat.gov.tw/ct.asp?xItem=1671&ctNode=548（最後瀏覽日期：2021/05/27）。

或施工中尚未完成領得使用執照之新建建築物，而申請智慧建築標章之對象則為已完成之新建建築物或既有建築物[13]。

根據統計，截止 2019 年 6 月為止，認可通過智慧建築標章共 417 件（包括智慧建築標章 114 件及候選智慧建築證書 303 件），而智慧建築普及率（每年認可通過候選智慧建築證書及智慧建築標章建築物之總樓地板面積，占當年核發建造執照及使用執照總樓地板面積之比率）亦逐年增高，在 2019 年 11 月來到 7.39%[14]；另根據臺灣建築中心網站公布資料顯示，截至 2021 年 4 月 30 日為止，已取得智慧建築標章或候選智慧建築證書之建築物共 666 件[15]。

雖然我國一直透過智慧建築標章制度引導建築物智慧化，惟根據內政部最新統計，我國住宅屋齡中位數為 29.8 年，全國住宅屋齡介於 20~40 年者占 47.7%，超過 40 年者占 28.9%，亦即我國近 8 成以上住宅為屋齡 20 年以上的老舊住宅[16]。針對老舊既有住宅，由於拆除或翻修改建不易，故為鼓勵既有建築物運用資通訊技術和設備系統，改善居住環境和提高生活品質，內政部建築研究所自 2008 年起辦理「既有建築物智慧化改善工作」，獎勵補助公有建築物及民間各級私立學校、社福機構和供住宅使用之建築物[17]。

綜上所述，可知我國一方面透過智慧建築標章制度鼓勵建築物與資通訊科技之整合，另一方面則透過獎勵補助方式，加強推動既有建築物智慧化改善工作，以提升居住空間品質。此外，配合行政院「數位國家•創新經濟發展方案(106~114 年)」政策，為發展我國 ICT 產業優勢，內政部建築研究所透過智慧化居住空間整合應用人工智慧科技發展推廣計畫(108~110 年)，積極整合人工智慧(AI)、物聯網(IoT)及大數據分析等科技，陸續完成研修我國智慧建築認證基準、建置及營運智慧化居住空間展示推廣中心、

13 內政部建築研究所，《智慧建築評估手冊》，頁 5、7（2016）。

14 〈108 年度智慧建築標章辦理成果〉，《建築研究簡訊》，第 107 期，2020/03/11，https://www.abri.gov.tw/PeriodicalDetail.aspx?n=861&s=2322&key=87&isShowAll=false（最後瀏覽日期：2021/06/10）。

15 〈核可案件公告〉，財團法人建築中心，http://ib.tabc.org.tw/modules/filelist/index.php/main/flist/3（最後瀏覽日期：2021/06/10）。

16 〈109 年第 46 週內政統計通報〉，內政部，2020/11/14/，https://www.moi.gov.tw/News_Content.aspx?n=2&s=198959（最後瀏覽日期：2021/06/10）。

17 林谷陶，《既有建築物智慧化改善之研究—以集合住宅為例》，頁 39（2015）。

出版「既有住宅社區導入智慧化改善指引」及「建築物智慧化系統規劃入門指引等成果，持續推動我國集合住宅類智慧建築之發展[18]。

參、 深度訪談重點整理

一、訪談對象

本計畫從集合住宅類智慧建築設計施工、管理角度出發，訪談產官學各界專家，包括建伸智慧綠建築公司（提供智慧建築及綠建築規劃設計顧問）黃健偉總經理（台灣智慧建築協會副理事長）、中國文化大學建築及都市設計學系溫琇玲副教授（台灣智慧建築協會名譽理事長）、台灣物業管理學會林世俊常務監事及台北市政府都市發展局張立人副工程司（社會住宅之規劃設計與施工），並訪談台灣資通產業標準協會陳曉強資深顧問請益我國資訊安全相關標準。整理上述各場訪談主題如下：

（一） 建伸智慧綠建築公司：我國集合住宅類智慧建築現況與導入資通訊設備之注意事項

（二） 台灣資通產業標準協會：我國物聯網設備資安標準及標章現況及結合集合住宅類智慧建築之可行性

（三） 台灣物業管理學會：從物業管理角度看集合住宅之資安注意事項

（四） 台北市政府都市發展局：從社會住宅經驗談集合住宅導入資通訊設備應注意事項

（五） 中國文化大學建築及都市設計學系：集合住宅類智慧建築導入資通訊安全應用應注意事項重點，及結合智慧建築標章之可行性

二、訪談大綱

在訪談大綱的擬定上，本計畫會依照訪談對象和主題調整內容，並圍繞以下主軸展開：

---

18 〈110 年度智慧化居住空間整合應用人工智慧科技發展推廣計畫(3/4)〉，內政部建築研究所，https://www.abri.gov.tw/cp.aspx?n=14048（最後瀏覽日期：2021/06/11）。

（一） 我國集合住宅類智慧建築發展狀況，以及主要導入之智慧化設備

（二） 確保集合住宅類智慧建築安全性之方法

鑒於資通訊或聯網設備可能有安全性疑慮，請教專家以了解目前可能透過哪些方式來確保集合住宅類智慧建築之安全性。如是否會針對硬體，在驗收時要求相關設備符合特定規範或規格（如取得資安標章）；在人員和程序方面，要求管理單位建立 SOP 等。

（三） 我國目前制定資訊安全相關標準或規範之狀況：

我國目前有針對物聯網設備研擬檢測標準和規範，並為落實檢測制度制定物聯網資安認驗證制度規章。惟上述制度係針對產品，未來如欲針對整棟建築物（特定場域）建立資通設備資安檢測標準或規範，就可能需要克服之問題請教專家意見。

（四） 參考國外作法研擬我國集合住宅導入資通訊安全應用注意事項之可行性：

日本國土交通省「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン），設想智慧建築內所遭遇之實體及虛擬風險，如人員未善盡保密義務或未遵守 SOP、硬體設備未定時維修、遭受網路攻擊等，並從管理面（組織、人、程序）和功能面（系統、資料、機器）盤點可能遭遇之風險及弱點，針對上述風險及弱點，參考國內外相關規範，針對 IoT 業者、服務提供者、服務供應者等，提出導入/提供相關設備或服務時之注意事項。

就本計畫參考上述作法和我國現況，針對集合住宅導入資通訊應用研議注意事項之可行性，以及可以參考之國內外法規（含標準）等問題，請教專家意見。

（五） 我國集合住宅導入資通訊安全應用注意事項之研擬方向：

針對硬體設備之資訊安全，目前台灣資通產業標準協會

（TAICS）針對物聯網產品，已陸續發布之許多相關規範，或可作為注意事項內容之參考。惟符合前述規範之設備，價格可能較為昂貴，且一般住宅不一定需要太高等級之資安防護，故美國「IoT 設備資安能力核心基準」僅於基準中列出設備應具有哪些功能，未明確規定應符合或取得特定標準。

針對人員和程序方面，未來注意事項或可考慮要求管理單位建立規章、SOP 或規定相關人員必須進行教育訓練。然而，從管理面建立規範雖為確保資安之重要手段之一，惟集合住宅規模不一，該如何透過管委會或物業管理來落實相關規範，恐將成為問題。

最後，智慧建築內有大量資料，可作為後續利用之基礎，惟要促進資料流通利用，除透過制定資料標準格式，確保資料互通性外，尚須確保資料品質（可用性）和避免資料被竄改和資料完整性等。從注意事項角度出發，重點應會放在避免資料被竄改和確保資料完整性。本計畫將針對上述研擬方向，請益專家意見。

（六） 未來注意事項是否可能結合之智慧建築標章或其他規定：

注意事項研擬完成後，就後續是否有可能與智慧建築標章結合，或作為智慧建築標章指標項目調整之參考等問題，請教專家意見。

三、訪談紀錄重點整理

針對上述訪談大綱，本計畫依序整理專家訪談重點如下：

（一） 我國集合住宅類智慧建築發展狀況，以及主要導入之智慧化設備

目前有在發展智慧家庭的業者，如 Google、amazon 和小米所開發之設備，都可以連外網，以利後續提供更多加值服務，但 Apple 注意到資安問題，仍使用藍芽進行連接，未來研擬注意事項，可以建議安全等級高之住宅使用藍芽設備，避免資安風險。由於擔心資安問題，所以建築物大都只能連內網，但這樣

一來會限制後續發展。

過去認為理想的智慧建築應是一個大型的偵測站，可以蒐集和共享資料，但現在發展方向截然不同，對物聯網產業有很大影響。基於上述理由，有專家認為政府未來應協助釐清資料等級，以促進建築物互聯。如停車/瓦斯/求救/氣溫/空氣品質等資料，存取權限設定可以比較低，門禁和監視器資料的存取權限要設定較高，儲存期限較長，同時需要求進行異地備份。

（二） 確保集合住宅類智慧建築安全性之方法

集合住宅內最常討論監視器問題，由於建築物內監視器是長時錄影，住戶出入時間都會被記錄下來；此外，門禁系統也會紀錄住戶進出時間，可由此得知住戶的日常行動軌跡。惟目前系統架構建築物不連外網，被駭客入侵可能性較低，故問題比較可能發生在管理面，如有人複製檔案等，需要多加注意。此外，由於集合住宅資料的商業價值低，所以集合住宅的重點在於保護住戶的隱私。

（三） 我國目前制定資訊安全相關標準或規範之狀況

目前台灣資通產業標準協會（以下簡稱 TAICS）主要因應政府各部會需求推動資訊安全，由下而上針對個別產品制定相關標準，現在正規劃由上而下的資安指引，將每一個獨立個體，如將集合住宅、醫院等視為一個系統，建立一個模型，以這個模型分析系統風險和評估可能弱點，進行滲透性或破壞性測試攻擊系統，以評估系統的安全能力並分級。TAICS 目前擬規劃物聯網通用標準，未來可適用特定標準之設備（如 IP Camera）就適用特定標準，沒有的就可以適用通用標準。透過由下到上和由上到下制定標準，就可以將整體串連在一起。

針對智慧建築個別系統，目前監控設備已經有資安標準，業主可以依照需求和資安等級選用相應設備，但針對其他系統（如門禁系統）仍然缺乏相應規範。綜觀國際資安標準，主要分成針對系統進行管理（如 ISO27001）和針對硬體裝置/軟體運作

加以規範之兩大體系。針對監控設備，若智慧建築要求導入之設備必須符合 TAICS 所制定之標準應無問題；針對一般資訊管控，如防火、門禁系統之資料，或許可以參照既有國際標準進行管理。

（四） 參考國外作法研擬我國集合住宅導入資通訊安全應用注意事項之可行性

從地域來看，必須先從美國和歐盟開始蒐集相關法規，其他國家或地區大多也是遵循美國和歐盟標準，故可優先關注美國和歐盟規定；至於標準的結構，如前所述，主要分成規範硬體（產品）和系統（如 ISO27001），但最終兩者還是要結合在一起。另外在進行驗證時，由於專業不同，很難針對管理進行驗證，所以一般都是要求管理系統要符合特定標準，以及每個裝備必須取得特定標章等，並檢視申請驗證者所提供資料是否符合聲明。綜上所述，在規劃注意事項時，應分別針對業主本身，以及業主對於供應商的管理/驗收程序進行規範。

（五） 我國集合住宅導入資通訊安全應用注意事項之研擬方向

由於集合住宅規模不一，故應依照社區規模研擬不同的注意事項，將資安分級概念落實於集合住宅類智慧建築。針對集合住宅，有專家建議除限制設備是否可以連外網及設置位置外，亦須針對硬體設備進行定期測試、設定存取權限（如規定只有總幹事才能存取資料）和進行人員教育訓練。此外，由於小規模集合住宅缺乏人力，故管理重點應在於要求資料需要進行備份，甚至要求異地備援；而大型社區由於是交給物業管理，所以重點在於人員管理。

在注意事項研擬方向上，至少應區分軟硬體（設備面）和人員、程序面（管理面）加以規範。針對軟硬體設備，可以規範設備應具有哪些功能（如限制使用藍芽、具備反向紀錄功能等）、設置位置，以及需要定期檢測等；針對管理面，則可考慮要求制定作業流程和規範，如設定存取權限、定期教育訓練等。

有關設備面之規範，有專家進一步認為，目前智慧化或聯網設備皆有裝置網路 Switch+網路 Firewall+網路 Router 之軟硬體，為強化網路安全性及效能，可考慮要求軟體應即時更新及定期進行安全分析。在人員和程序方面，可考慮要求起造人制定 SOP，並由管理單位（如管理委員會）聘用合格資安證照人員，而為確保實際場域落實 SOP，未來可考慮由管委會督導，公協會或法人定期驗證物業管理公司、保全公司等單位是否落實 SOP/人員培訓。

此外，鑒於智慧建築資料保護和利用之重要性，未來亦應考慮加強資料防護。為落實資料管理，可考慮要求集合住宅將資料存在自己的伺服器或私有雲（近 5-10 年的新建築物其實都有預留空間存放伺服器，由於建築物內部資料量不大，不需要很大的伺服器，所以老舊建築物也可以將伺服器放在 DV 箱上）。

針對「異地備援」重點，有專家認為應針對「事件」，如闖空門、安全門被打開等進行儲存，並避免資料被竄改，如此一來，亦可解決資料量龐大問題。

（六） 未來注意事項或智慧建築標章是否可能結合之現有物聯網產品資安標準

目前我國主要係針對個別產品制定相關標準，如智慧建築欲導入相應設備，應可考慮要求其應符合相關標準。惟考量到集合住宅類智慧建築規模大小不一，對於資安需求程度亦有所不同，小規模集合住宅或老式公寓可能沒有資安需求，要求其使用的設備需符合特定標準，可能會衍生額外的成本，故研擬注意事項時應納入分級概念，或將取得物聯網標章或符合其他標準作為鼓勵得分項目，避免過度要求反而成為住戶或管理單位負擔。

第二節、 我國集合住宅類智慧建築資安相關規範

壹、 我國資訊安全及個人資料相關法令盤點

根據前述說明，可知我國推動智慧建築發展已具相當成效。然而，智慧建築雖然可以為民眾帶來便利並提升生活品質，卻也同時潛藏資訊安全方面之隱憂。為清楚掌握我國目前有關資訊安全之法規，以及其中有哪些規定適用於智慧建築，本計畫以資安、網路安全、資通安全或資訊安全為關鍵字，搜尋全國法規資料庫，盤點相關法律、行政規則、行政命令如下表 2-1：

表 2-1 我國資訊安全相關法令整理表

法規類別 (按主管機關)	法規名稱	相關條號 (條-項-款)
國家通訊傳播委員會	國家通訊傳播委員會組織法	3-1-8
	無線電頻率使用管理辦法	18-1-8
	無線廣播電視電臺設置使用管理辦法	18-1 20
	行動寬頻業務管理規則	12-2-2 40-1,5,7,11 42-2-1 43-1-3,4 55 之 1-1,2 83 之 1 83 之 4
	固定通信業務管理規則	70-4 71 之 1-1 74 之 2 74 之 5
	第二類電信事業管理規則	7-2-10 8-1-5 31 31 之 1 31 之 2-4 31 之 3-2
	專用電信網路設置使用管理辦法	6-2-6 7-1-4 8-2-9 9-1-7
	電信事業網路互連管理辦法	7-4-1
	電信事業重大事故無法提供電信服務通報辦法	3 6-3,4
	電信事業資通安全管理辦法	資通安全專法
	電信管理法	15-1,2,3 37-4-6,7 38-3-6,7 40-1-5 40-2-5 42-7 43-1 79-1-13 82-2-3
	申請經營有線廣播電視服務籌設辦法	14-1-5
	申請經營有線廣播電視服務審查辦法	4-1-4
	公眾電信網路設置申請及審查辦法	5-1-6,7 10-1-6,7 13-1-6,7

		17-1-5,6,7
	公眾電信網路檢驗辦法	2,3,10,12, 13,14,15,16
	公眾電信網路審驗辦法	11-1,2
	實驗研發專用電信網路設置使用管理辦法	6 10-1-11 12-1-8
	學術教育或專為網路研發實驗目的之電信網路設置使用管理辦法	17
	有線廣播電視系統經營者申請換發經營許可執照審查辦法	11-1-7
	憑證實務作業基準應載明事項準則	33
	關鍵電信基礎設施指定及防護管理辦法	5-1-5
	關鍵電信基礎設施資通設備測試機構及驗證機構管理辦法	3-3-1,2 5-2-2,4 10-1 14-1-5
	市場顯著地位者互連管理辦法	7-4-1
	國家通訊傳播委員會推動通訊傳播產業創新研究發展補助辦法	2
	國家通訊傳播委員會處務規程	6-1-2 8-1-4,8,10
國家發展委員會	國家發展委員會處務規程	13-1-7
	國家發展委員會檔案管理局處務規程	9-1-7
僑務委員會	僑務委員會處務規程	15-1-3
國家圖書館	國家圖書館處務規程	8-1-6
衛生福利部	全國性社會福利財團法人資料電子傳輸辦法	6-1-1
	全國性衛生財團法人及醫療財團法人資料電子傳輸辦法	6-1-1
	衛生福利部主管長期照顧服務機構財團法人資料電子傳輸辦法	6-1-1
	人體生物資料庫管理條例	5-2,3 13-1 24-1-4
	人體生物資料庫設置許可管理辦法	3-1-4 4-1-2 7-1-3
	防疫物資及資源建置實施辦法	2-1-2 5-1,2 6
	兒童及少年性剝削防制條例	4-2-4
	家庭暴力防治法	58-6
	家庭暴力電子資料庫建立管理及使用	7

	辦法	
	衛生福利部處務規程	19-1-3
	衛生福利部食品藥物管理署處務規程	16-1-3
	衛生福利部疾病管制署處務規程	17-1-3
	全民健康保險保險憑證製發及存取資料管理辦法	16-1-1
	老人福利法	12 之 1-3
	國民年金法	56-4
	兒童及少年福利與權益保障法	70-4
	社會救助法	44 之 3-2
	脆弱家庭之兒童及少年通報協助與資訊蒐集處理利用辦法	11-3
	特殊境遇家庭扶助條例	15 之 1-2
	身心障礙者權益保障法	71 之 1-2
金融監督管理委員會	外籍移工國外小額匯兌業務管理辦法	7-1-8
	電子支付機構業務管理規則	44-3-3 52-1-9
	電子支付機構資訊系統標準及安全控管作業基準辦法	17-1-6 21-1-1
	電子票證發行機構業務管理規則	24-1-6
	證券暨期貨市場各服務事業建立內部控制制度處理準則	10-1-10 14-2-5
	金融科技發展之輔導及協助辦法	2-1-6 10
	金融機構申請參加存款保險審核標準	4-1-6
	金融機構作業委託他人處理內部作業制度及程序辦法	18-2-5 18-5-1 18-6-3 19 之 1-1-4 19 之 2-1-5 19 之 2-2-1
	金融機構間資金移轉帳務清算之金融資訊服務事業許可及管理辦法	13 14
	金融控股公司及銀行業內部控制及稽核制度實施辦法	37-1-5 38-1-5 38 之 1-1~5
	金融科技發展與創新實驗條例	13 16-1
	金融科技創新實驗管理辦法	14-1-7 20-1-2-2 21-1-4
	公開發行公司建立內部控制制度處理準則	9-1-10 13-2-6
	金融監督管理委員會處務規程	11-1-5
	金融監督管理委員會檢查局處務規程	16-1-3

	金融監督管理委員會銀行局處務規程	16-1-3
	金融監督管理委員會證券期貨局處務規程	15-1-3
	金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法	10-1
	與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法	23-1-7
	保險代理人公司保險經紀人公司辦理網路投保業務及網路保險服務管理辦法	5-1-4 14-1-1-2
	保險業內部控制及稽核制度實施辦法	6-2 6 之 1-1~5
	信用評等事業管理規則	15-3-5
	人身保險及財產保險安定基金計提標準	2,3,4
	公開發行股票公司股務處理準則	44 之 1-2-2 44 之 1-5
中央銀行	中央銀行處務規程	12-1-6
	中央造幣廠組織規程	15-1-4
財政部	通關網路經營許可及管理辦法	6-1-1-5
	關務人員獎懲辦法	3-1-11 3-1-14 5-1-13 6-1-10 7-1-27 8-1-27
	財政部北區國稅局處務規程 財政部中區國稅局處務規程 財政部南區國稅局處務規程 財政部臺北國稅局處務規程 財政部高雄國稅局處務規程	7-1-5
	財政部財政資訊中心組織法	2-1-3
	財政部財政資訊中心處務規程	5-1-5 7-1-4 10-1-5 15-1-3
	財政部國有財產署處務規程	13-1-3
	財政部關務署處務規程	11-1-6
	財政部國庫署處務規程 財政部關務署高雄關辦事細則 財政部關務署基隆關辦事細則 財政部關務署臺北關辦事細則	15-1-3
	公益彩券發行機構個人資料檔案安全	17 之 1-1

	維護管理辦法	
審計部	審計部審計資訊委員會組織規程	2-1-4
經濟部	經濟部水利署各河川局辦事細則	7-1-7
	無人載具科技創新實驗管理辦法	18-1
	偏遠與原住民族及離島地區石油設施及運輸費用補助辦法	34-1-4
	公司法第二十二條之一資料申報及管理辦法	14-1
勞動部	勞動部處務規程	17-1-3
	勞動部勞工保險局處務規程	17-1-2
	勞動部勞動力發展署處務規程	15-1-2
	勞動部職業安全衛生署處務規程	12-1-2
文化部	文化部處務規程	17-1-3
	文化藝術獎助及促進條例	20
交通部	交通部公路總局各區監理所辦事細則	8-1-3
	交通部公路總局各區監理所組織準則	2-1-6
	交通部公路總局各區養護工程處辦事細則	10-1-8
	交通部公路總局材料試驗所辦事細則	6-1-4
	交通部公路總局處務規程	16-1-3
	交通部航港局辦事細則	15-1-3
	交通部高速公路局各區養護工程分局辦事細則	13-1-3
	交通部高速公路局各新建工程處辦事細則	6-1-6
	交通部高速公路局處務規程	16-1-3
	交通部高雄港務局布袋辦事處辦事細則	10-1-4
	交通部高雄港務局馬公辦事處辦事細則	10-1-4
	交通部基隆港務局辦事細則	12-1-10
	交通部臺中港務局辦事細則	11-1-7
	交通部花蓮港務局辦事細則	10-1-16
	交通部高雄港務局辦事細則	12-1-7
	交通部鐵道局各工程處辦事細則	5-1-6
	交通部鐵道局處務規程	16-1-3
	交通部觀光局辦事細則	4-1-6
	外籍旅客購買特定貨物申請退還營業稅實施辦法	19-2
	交通部民用航空局辦事細則	12-1-7
	交通部臺灣鐵路管理局資訊中心辦事細則	5-1-6
外交部	外交部處務規程	21-1-3

內政部	國民身分證及戶口名簿格式內容製發相片影像檔建置管理辦法	15-1-1 26 43-1-1 53
	大陸地區人民按捺指紋及建檔管理辦法	5-2
	內政部國土測繪中心辦事細則	9-1-5
	去氧核醣核酸樣本與紀錄監督管理辦法	8-2
	個人生物特徵識別資料蒐集管理及運用辦法	7-2
教育部	學校財團法人及所設私立學校內部控制制度實施辦法	12-1-10
	特殊教育行政支持網絡聯繫及運作辦法	8
	國民體育法	30-1-5
	國立公共資訊圖書館組織法	2-1-7
	國立自然科學博物館處務規程	10-1-6
	國家圖書館處務規程	8-1-6
科技部	科技部處務規程	18-1-2
考選部	公務人員特種考試國家安全局國家安全情報人員考試規則	9-2
	考選部處務規程	15-1-1-6 15-1-2-6 15-1-3-6
銓敘部	公教人員保險法	43-4
行政院人事行政總處	行政院人事行政總處處務規程	10-1-8
行政院主計總處	行政院主計總處處務規程	13-1-8
行政院農業委員會	行政院農業委員會水土保持局各分局組織準則	3-1-9
	行政院農業委員會水土保持局處務規程	5-1-7
	行政院農業委員會辦事細則	5-1-3-10 5-1-4-1,10
	行政院農業委員會農糧署中區分署辦事細則 行政院農業委員會農糧署北區分署辦事細則 行政院農業委員會農糧署東區分署辦事細則 行政院農業委員會農糧署南區分署辦事細則	5-1-10 14-1-6

	行政院農業委員會動植物防疫檢疫局辦事細則	9-1-2-7
	行政院農業委員會農業金融局辦事細則	5-1-2-10
中央選舉委員會	中央選舉委員會處務規程	5-1-8
客家委員會	客家委員會處務規程	6-1-6
國軍退除役官兵輔導委員會	高雄榮民總醫院處務規程	44-1-3
	臺中榮民總醫院處務規程	45-1-3
	臺北榮民總醫院處務規程	47-1-3
	臺北榮民總醫院玉里分院辦事細則	26-1-3
國立故宮博物院	國立故宮博物院處務規程	13-1-4
海洋委員會	海洋委員會海巡署各地區分署辦事細則	8-1-2
	海洋委員會海巡署偵防分署辦事細則	11-1-8
	海洋委員會海巡署教育訓練測考中心辦事細則	9-1-1
	海洋委員會海巡署處務規程	9-1-1,6
	海洋委員會處務規程	15-1-3
監察院	監察院處務規程	15-1-9
總統府	中華民國總統府處務規程	10-1-5-1,2
	國史館臺灣文獻館古文書閱覽複製辦法	7-2
	國史館辦事細則	10-1-4
國家安全會議	政府各機關協助國家情報工作應配合事項辦法	11
行政院-院本部	資通安全管理法	資通安全專法母法
	公務機關所屬人員資通安全事項獎懲辦法	資通安全專法(母法：資通安全管理法)
	資通安全管理法施行細則	同上
	特定非公務機關資通安全維護計畫實施情形稽核辦法	同上
	資通安全事件通報及應變辦法	同上
	資通安全情資分享辦法	同上
	資通安全責任等級分級辦法	同上
	特定非公務機關資通安全維護計畫實施情形稽核辦法	同上
	各機關訂定之「XX 部/院/委員會特定非公務機關資通安全管理作業辦法」，有訂定該辦法之機關共 23 個，包含：大陸委員會、中央銀行、內政部、文化部，司法院、外交部、交通部、行政院	同上

	原子能委員會、行政院農業委員會、行政院環保署、法務部、金融監督管理委員會、客家委員會、科技部、原住民族委員會、財政部、國防部、國軍退除役官兵輔導委員會、國家通訊傳播委員會、教育部、經濟部、僑務委員會、衛生福利部。	
	國民參與審判制度概要說明書及候選國民法官調查表應記載事項準則	7-1
	行政院處務規程	7-1-11 17 之 1 26-1-3
法務部	法務部調查局組織法	2-1-8 3
	法務部調查局處務規程	4-1-6 10-1-6,7
	法務部調查局桃園市調查處辦事細則	4-1-4 8-1-5
	法務部調查局高雄市調查處辦事細則	4-1-4 11-1-5
	法務部調查局臺北市調查處辦事細則	4-1-7 11-1-5
	法務部調查局新北市調查處辦事細則 法務部調查局臺中市調查處辦事細則 法務部調查局臺南市調查處辦事細則	4-1-5 9-1-5
	法務部調查局福建省調查處辦事細則	4-1-3 7-1-5
	法務部調查局航業調查處辦事細則	4-1-4 9-1-5
	監獄及看守所科技設備設置與使用及管理辦法	19-1
國家運輸安全調查委員會	國家運輸安全調查委員會處務規程	11-1-5
國防部	列管軍品廠商安全查核辦法	3-2-3
	國防部空軍司令部辦事細則	14-1-1
	國防部陸軍司令部辦事細則	14-1-1
	國防部參謀本部處務規程	8-1-1
	列管軍品廠商資格級別認證辦法	13
	悔過室設置辦法	8-2
	國防產業發展條例	4-2-7
	國家安全局處務規程	11-1-8 16-1-6
大陸委員會	大陸委員會處務規程	16-1-4,5

（資料來源：本研究整理）

貳、 可能與智慧建築資訊安全有關之法令

法規範依其表現形式可分為成文法與非成文法，前者如憲法、法律、行政命令等直接發生法效力之規定，而後者則如習慣法、一般法律原理原則等須經國家機關承認、闡釋與適用，始能間接產生法效力之規定。我國為成文法國家，以憲法作為根本大法，並以《中央法規標準法》規範中央法規之制定、施行、適用、修正及廢止。根據《中央法規標準法》第 11 條：「法律不得牴觸憲法，命令不得牴觸憲法或法律，下級機關訂定之命令不得牴觸上級機關之命令。」可知我國法律體系和位階，由上而下依序為憲法、法律和命令，故在討論我國法範圍時，原則上應限於憲法、法律和命令，合先敘明。

首先須說明，根據《中央法規標準法》第 2 條和第 3 條規定，法律得定名為法、律、條例或通則；而命令則得依其性質，稱規程、規則、細則、辦法、綱要、標準或準則，故法規名稱中未包含上述名稱者，理論上非法律或命令。

表 2-1 所整理之法規，位於法律層級者包括《國家通訊傳播委員會組織法》、《資通安全管理法》、《電信管理法》、《人體生物資料庫管理條例》、《兒童及少年性剝削防制條例》、《家庭暴力防治法老人福利法、國民年金法、兒童及少年福利與權益保障法、社會救助法特殊境遇家庭扶助條例、身心障礙者權益保障法、金融科技發展與創新實驗條例、財政部財政資訊中心組織法、國民體育法、法務部調查局組織法、國立公共資訊圖書館組織法、公教人員保險法等，其餘均為命令層級之規範。此外，我國主管機關亦常基於業務需求出版手冊、問答集或指引等，由於並非法律或命令，故無強制力，就性質上而言，較接近於《行政程序法》第 165 條之行政指導，亦即『行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為』。

表 2-1 所整理之法律或命令，就內容而言，大多為行政機關之組織法，或機關本身基於《資通安全管理法》對自身資訊安全規劃、推動、執行、監督，以及緊急應變計畫等職責之說明，如《國家通訊傳播委員會組織法》、「國家發展委員會處務規程」、「國家圖書館處務規程」、「國防部參謀本部

處務規程」、「國家運輸安全調查委員會處務規程」、「財政部財政資訊中心組織法」等。另外還有部份為各主管機關針對其所職掌業務，制定相關規範以確認資料傳輸之安全，如衛福部針對旗下法人之資料電子傳輸，制定《老人福利法》、《國民年金法》、「全國性社會福利財團法人資料電子傳輸辦法」、「全國性衛生財團法人及醫療財團法人資料電子傳輸辦法」、「衛生福利部主管長期照顧服務機構財團法人資料電子傳輸辦法」；金融監督管理委員會制定之「金融控股公司及銀行業內部控制及稽核制度實施辦法」、《金融科技發展與創新實驗條例》等。

在上述規範中，排除組織法或各機關針對其職掌業務所制定之規範，可能與智慧建築資訊安全有關之法律和法規命令，包括規範我國資訊安全政策之《資通安全管理法》及相關辦法，以及建築物導入或設置電信、聯網設備時需要注意之「固定通信業務管理規則」、「行動寬頻業務管理規則」、「專用電信網路設置使用管理辦法」、「建築物屋內外電信設備工程技術規範」、「建築物電信設備及空間設置使用管理規則」、「建築物屋內外電信設備設置技術規範」、「建築物電信設備審查及審驗機構管理辦法」等規定。此外，由於在談論資訊安全時往往也會一併談論個人資料保護，故規範個人資料蒐集、處理、利用之《個人資料保護法》和相關辦法，以及規範建築物設計施工、構造、設備之「建築技術規則」，亦為可能需要關注之對象。

首先，針對《資訊安全管理法》，我國於 2018 年通過該法以推動國家資通安全政策，惟該法規範對象為公務機關或特定非公務機關，並衡酌上開機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件進行分級，再依據等級制定有關義務內容、專責人員之設置及其他相關事項之辦法。由此可知，「集合住宅」除非是社會住宅，否則不會成為《資訊安全管理法》之規範對象。此外，由於資訊安全很難由正面或負面表列安全或不安全之行為，故《資通安全管理法》係從程序面進行規範，透過要求公務機關或特定非公務機關遵守一定程序來控管風險，實際上亦未針對建築物本身進行任何規範，故《資訊安全管理法》雖為我國主要資安法規，但非本計畫研析對象。

其次，雖然資訊安全措施是否完善，可能會影響到個資是否洩漏，但個資

或隱私並不等同於資訊安全。針對智慧建築資料相關法制議題，本計畫團隊已於 109 年執行「智慧建築安全監控資料應用之法制課題及對策」計畫，並提出問答集草案作為因應，故個資法亦非本計畫主要研究對象。

最後，「建築技術規則」規範建築物之設計、施工、構造及設備，設計施工篇針對建築物一般設計通則，以及建築物之防火、建築物安全維護設計、特定建築物、地下建築物、高層建築物等在設施施工時應遵守事項，如是否需留設空地、通道，通路之寬度、樓地板面積等加以規範；建築構造篇則就建築物構造之基本規則，如設計要求、施工品質、載重等，以及基礎構造、深構造、磚構造等之地基調查、基礎設計及施工加以規範；建築設備篇則針對建築物內設置之各項設備，如電氣設備、給水排水系統及衛生設備、消防設備等裝置方法和配件等加以規範。

如前所述，資訊安全很難透過正面或負面方式表列安全或不安全之行為，故大多從程序面進行規範，透過要求特定單位應制定資訊安全維護計畫，或要求進行資安宣導或定期針對系統進行弱點掃描等方式來降低資安風險。有鑑於此，規範建築物應如何設計、施工及建築物構造、建築物內設備應如何裝置等事項之「建築技術規則」，恐怕很難就建築物如何確保資訊安全一事加以規範。此外，鑑於內政部並非《資通安全管理法》主管機關，恐怕亦不適宜針對建築物在設計、施工，以及導入設備時應遵守哪些事項，進行明確地規範。

鑑於資訊安全對於智慧建築之重要性，在無法從法律層面由上而下訂定規範時，或可考慮由下而上制定應行注意事項，提供相關人士參考。內政部建築研究所為推廣智慧化居住空間概念，推動國內智慧建築之發展，於 2003 年訂定智慧標章制度，並於 2004 年起實施。根據 2016 年版智慧建築評估手冊，目前智慧建築標章分別從綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等八大指標，作為評估申請智慧建築標準之依據。

上述八大指標並未將資訊安全列為單獨的指標，似未將資訊安全作為評估項目之一。惟如進一步檢視各項指標之評估內容，可以發現部份項目與資訊安全有關，如資訊通信指標之基本規定評估項目中，2.3 區域網域評估內容包括「設置適當的資訊安全保障設備」；系統整合指標下 3.3 整合安

全機制項目之評估內容則有「各種應用系統之人機界面均需具備操作使用管理權限功能」、「各系統需具備電源備援之設備機制」、「提出整體整合系統之資安防護機制」；設施管理指標下 4.4 維運管理在基本規定要求訂定年度設備管理維護計畫，以及各項設施設備機能運作具備智慧化自主性作業管理，而在鼓勵項目則要求訂定智慧化設施設備危機處理與緊急應變計畫等[19]。

此外，如從實體及虛擬兩大方向來看資訊安全之維護，在實體面向上，為確保設備和系統之安全，必須避免因設備或環境問題，如斷電、設備故障等導致系統或設備無法運用。若從上述角度出發，則智慧建築標章各項指標中有關系統或設備應具備之功能的規定，如資訊通訊指標下 2.2 數位式電話交換要求具有不斷電設備，且於停電後能提供電話交換功能等，亦可視為與資訊安全有關之規定。

綜上所述，可知雖然我國智慧建築標章制度並未將資訊安全列為指標之一，但其實已經將資訊安全概念納入各項評估內容之中。然而，雖然智慧建築指標已經涵蓋資訊安全概念，但對於申請者而言，這些內容可能仍然不夠明確，如前述資訊通訊指標下區域網域項目，其評估內容為「設置適當的資訊安全保障設備」，但何謂「適當」資訊安全保障設備之標準？是否需要該設備符合一定資安規格、標準，或取得特定認證？仍無法從評估項目和說明中得知。

上述問題不只是申請者會面臨，對於一般住戶或是大樓管理單位而言，雖然不一定有申請智慧建築標章之需求，但也有可能會購買聯網設備或導入資通訊系統來管理集合住宅，從而產生需要確保系統或設備安全之需求。有鑑於此，本計畫擬參考國外作法，針對集合住宅類智慧建築提出注意事項，並擬從程序面和硬體面出發研擬具體內容。

參、 我國物聯網資安相關標準及測試規範

一、物聯網場域資安防護評估指引

根據物聯網場域技術範圍從底層感測設備物件技術，到最上應用層之

[19] 前揭註 13，頁 13-46。

服務，其應用情境包含智慧家庭、智慧醫療、公共安全、智慧建築、智慧交通、智慧能源、智慧農業、智慧物流、智慧停車等範疇，範圍十分廣泛，惟我國目前仍缺少從物聯網場域之系統面進行資安防護評估的準則，故台灣資通產業標準協會配合國家持續推動物聯網技術及5G 垂直應用之發展策略，研析國際物聯網資安評估指引或規範，從物聯網應用情境出發，建立適用於物聯網場域之資安評估機制[20]。

根據「物聯網場域資安防護評估指引」定義，物聯網場域係為物聯網系統所提供特定聯網應用的實體環境，該實體環境不限於同一地理位置，並包含應用層、網路層和感測設備層[21]。物聯網場域資安防護評估指引針對物聯網應用情境，以威脅建模（Threat Modeling）、漏洞檢測（Vulnerability Testing）、滲透測試（Penetration Testing）及衝擊分析（Impact Analysis）之評估報告等四道流程，進行資安防護評估[22]。

威脅建模為一種用來識別及確認潛在威脅，使用列舉方式進行風險評估之結構化方法，而物聯網威脅建模包含盤點物聯網場域資產設備、建立物聯網場域架構圖、解析物聯網場域運作程序、識別並分析各種可能的威脅、紀錄所有可能的威脅等步驟；在完成威脅建模後，下一個步驟則是利用「物聯網場域資安防護評估指引」所制定的 8 項安全政策及 46 個安全控制項目進行漏洞檢測，作為後續滲透測試之依據；在滲透測試部份，物聯網滲透測試與傳統資訊領域針對單一系統不同，以著重於廣度並找出重大危害弱點為目標，並針對已經發現之威脅途徑與或各項漏洞與弱點，評估其對於使用者、場域、服務商之衝擊影響。最後，「物聯網場域資安防護評估指引」依據透測試結果進行物聯網場域應用於各種垂直應用領域的衝擊分析，瞭解該物聯網應用系統可能的風險，提供相關利益關係人制定資安應變計畫參考之依據[23]。

20 台灣資通產業標準協會，《物聯網場域資安防護評估指引》，頁 5（2021）。
21 同前註，頁 8。
22 同前註，頁 13。
23 同前註，頁 14-47。

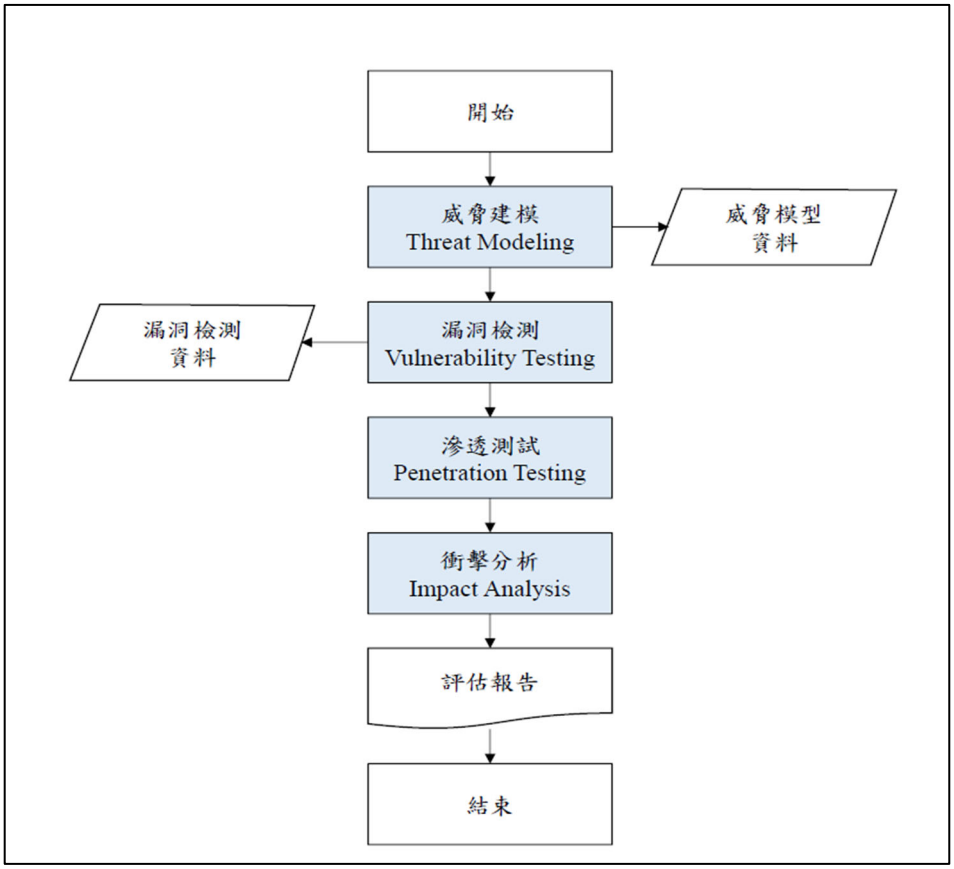

圖 2-2 物聯網場域資安防護評估流程圖

（資料來源：物聯網場域資安防護評估指引，2019）

二、消費性物聯網產品資安標準

消費性物聯網產品已逐漸普及應用於日常生活，目前常見容易遭駭客攻擊之七種物聯網裝置中，就有四種屬於消費性物聯網產品，其中家用網路路由器、機上盒、智慧家居產品等更是智慧建築或住宅內常見之設備[24]。台灣資通產業標準協會在國家通訊傳播委員會的支持下，以 ETSI EN 303 645 Cyber Security for Consumer Internet of Things：Baseline Requirements 為基礎，制定我國消費性物聯網產品資安產業標準，並於 110 年 11 月 25 日公布。

台灣資通產業標準協會所制定之消費性物聯網產品資安產業標準，其適用於與關聯服務所連接之連網設備，包括但不限於智慧家庭與人身穿戴應用之消費性物聯網產品，並將消費性物聯網產品定義為『指消

24 台灣資通產業標準協會，《消費性物聯網產品資安標準》，頁 4（2021）。

費性物聯網產品用於消費者可自行安裝設置或穿戴之連網設備，透過無線傳輸技術與關聯服務相互整合，消費者可監看與遙控消費性物聯網產品。例如：包括但不限於智慧家電、家庭閘道器、智慧手環等產品。』[25]

消費性物聯網產品資安產業標準包括：身分鑑別、漏洞安全、軟韌體更新、資料機密性與完整性、系統完整性、資源可用性、隱私保護及異常與警示等八大安全構面，每項構面都有進一步安全要求，而每項要求都包含一個或以上之安全要求項目。此外，消費性物聯網產品資安產業標準針對每個安全要求項目均設有安全層級，共分為強制性、建議、強制性且有條件、建議且有條件的安全要求。

[25] 同前註，頁 5。

表 2-2 安全要求總表（節錄）

安全構面	安全要求
身份鑑別	通行碼鑑別（2 項安全要求項目）
	身分認證機制（3 項安全要求項目）
安全漏洞	漏洞政策與安全設置（6 項安全要求項目）
	最小暴露攻擊面（9 項安全要求項目）
軟韌體更新	更新安全（16 項安全要求項目）
資料機密性與完整性	敏感性安全參數儲存（4 項安全要求項目）
	傳輸資料保護（8 項安全要求項目）
系統完整性	實體入侵防護（1 項安全要求項目）
	輸入驗證（18 項安全要求項目）
資源可用性	資源管理（3 項安全要求項目）
隱私保護	隱私保護能力（12 項安全要求項目）
異常與警示	安全事件警示（2 項安全要求項目）

（資料來源：消費性物聯網產品資安標準）

三、物聯網資安認驗證制度

面對物聯網資安挑戰，在行政院科技會報及行政院資通安全處指導下，我國目前由經濟部具有線介面之物聯網終端產品資安檢測；並由國家通訊傳播委員會主責具無線介面或電信/傳播終端設備介面。

針對無線網路攝影機，國家通訊傳播委員會參考台灣資通產業標準協會「影像監控系統資安標準—網路攝影機」及 ISO/IEC 15408、NISTSP 800-53、UL 2900-1 等國際標準，於 2018 年 8 月 29 日訂定「無線網路攝影機資通安全檢測技術指引」，適用於影像監控系統中具 Wi-Fi 連網功能之 IPCAM，亦適用同時具備有線及 WiFi 連網功能之 IP CAM（第二點參照）；針對有線網路攝影機，經濟部工業局財團法人資訊工業策進會與台灣資通產業標準協會，制定一系列資安標準及驗測規

範，包括影像監控系統、智慧巴士資通訊系統、智慧路燈、智慧音箱、空氣品質微型感測裝置等[26]。

在行政院科技會報與行政院資通安全處指導下，國家通訊傳播委員會與經濟部合作建立物聯網資安標章驗證制度，依據資安風險高低、資安技術防護複雜度，分為 1 級、2 級、3 級，給予符合物聯網資安測試規範與驗證規範之安全性要求，亦即通過台灣資通產業標準協會驗證之產品標章，以協助相關產品對外出口[27]。

26 〈關於物聯網資安認驗證〉，台灣資通產業標準協會，https://www.taics.org.tw/Validation04.aspx?validateType_id=14&Type=1010（最後瀏覽日期：2021/11/26）。

27 〈物聯網資安標章說明〉，台灣資通產業標準協會，ttps://www.taics.org.tw/Validation01.aspx?validateType_id=2（最後瀏覽日期：2021/11/26）。

第三節、 國外資通訊安全應用相關法制規定

我國透過智慧建築標章制度和獎勵補助既有建築物智慧化改善等方式，推動集合住宅類智慧建築發展，希望提升居住空間品質。惟當建築物導入資通訊設備或物聯網等最新科技時，資安問題亦隨之而來。在實體面，資通訊設備可能遭遇設備故障、訊號不良等問題，導致設備無法正常運作；在軟體面，資通訊設備則可能因作業系統、應用程式存在漏洞，洩漏所蒐集和儲存之資料，或因受到網路攻擊，使系統產生安全防護上隱憂。有鑑於此，世界各國陸續針對資通訊設備或物聯網產品加以規範，如美國加州於 2018 年 9 月制定、2020 年 1 月施行《SB-327 資訊隱私：連網裝置》（SB-327 Information Privacy: Connected Devices），要求設備製造商所提供之設備應提供「合理的安全功能」（reasonable security feature）[28]；英國數位、文化、媒體和體育部（Department for Digital, Culture, Media and Sport,DCMS）宣示將強化聯網設備安全，確保出售給英國消費者之聯網設備符合有關密碼唯一性、提供聯繫窗口和明確規定設備安全性更新時間等要求等[29]。

目前國際上有關資通訊設備或物聯網產品之政策、法規或標準，大多係針對所有聯網裝置之一般性規範，如前述美國加州訂定之《SB-327 資訊隱私：連網裝置》；或針對特定產品之標準，如我國台灣資通產業標準協會（TAICS）發布之 IP CAM 資安標準與測試規範、無線網路攝影機資通安全檢測技術指引、無線區域網路接取設備及路由設備資通安全檢測技術指引、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、以及智慧巴士資通訊系統系列資安標準與測試規範等，缺乏針對特定場域，如集合住宅類智慧建築導入資通訊設備或聯網裝置之資安規範或標準。

導致上述現象的原因，可能與建築物導入之設備差距較大有關，由於不同類型之建築物需求不同，即便同樣是集合住宅類智慧建築，伴隨規模大小和住戶需求不同，所導入的設備在種類和性能上也會存在不小差異，使分析相關產品潛在的風險變得困難，自然也很難據此制定相應規範或標準[30]。

---

28 〈加州通過第一個 IoT 裝置安全法〉，IThome，2018/10/1，https://www.ithome.com.tw/news/126165（最後瀏覽日期：2021/06/11）。

29 〈英國發布增強消費型智慧裝置安全性的新計畫〉，國際通傳產業動態觀測，2020/05/09，https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0K231386607692971161&sq=（最後瀏覽日期：2021/06/11）。

30 類似意見：Omar Alrawi, Chaz Lever, Manos Antonakakis, Fabian Monrose, *SoK: Security Evaluation of Home-Based IoT Deployments*, Presented at 2019 IEEE Symposium on Security and

即便可能存在上述問題，但鑑於智慧住宅是智慧生活的核心，而智慧生活是日本「Connected Industries」政策重點之一，日本經濟產業省成立智慧住宅工作小組，針對智慧住宅導入資通訊設備或聯網產品之資訊安全問題展開檢討，並於 2021 年 4 月 1 日公布「以安心、安全智慧住宅為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン）[31]。

綜觀國際趨勢，目前只有日本以智慧住宅為對象制定相關規範，故本文首先將介紹日本作法，作為研擬我國集合住宅類智慧建築導入資通訊安全應用之注意事項的參考。必須注意的是，日本所制定之指引範圍包括獨棟住宅和集合住宅，由於本報告係以集合住宅作為研究對象，故僅參考日本指引中有關集合住宅部份，合先敘明。

此外，雖非以特定場域為對象，但美國、歐盟、英國等先進國家和地區亦有針對消費性或家用物聯網設備制定相關標準，而日本在制定上開指引時亦將上開標準納入參考，故本報告亦將一併納入整理，以利後續參照。

壹、 日本

一、 以安心、安全智慧住宅為目標之虛實資安對策指引

日本政府近年提出「Society 5.0」願景，而為實現「Society 5.0」，必須串聯各式各樣的資料，創造新的產品和服務，形成「Connected Industries」之產業社會。「Connected Industries」包含不同領域，其中之一為智慧生活（スマートライフ），而智慧住宅（スマートホーム）則被認為是智慧生活核心概念，故為實現智慧生活從而達到「Connected Industries」和「Society 5.0」政策目標，日本認為必須

Privacy(SP), p.1(19-23 May 2019).該文章認為家用聯網產品（Home-Based IoT Deployments）核心功能類似，但特定功能卻有很大差距，較難進行分析。必須說明的是，上開文章係以家用聯網產品為研究對象，而本報告則係以集合住宅類智慧建築所導入之資通訊設備為主，並未將家用聯網產品納入討論。

31 〈スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました〉，経済産業省，https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html（最後瀏覽日期：2021/06/12）。

釐清智慧住宅在資訊安全層面上所需之技術、管理項目等對策[32]。基於上述理由，經濟產業省於 2018 年 3 月 13 日在產業資安研究會工作小組下設立智慧住宅工作小組，檢討實現智慧住宅之基本指引，並於 2021 年 4 月 1 日公布「以安心、安全智慧住宅為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，以下簡稱智慧住宅資安對策指引）[33]。

智慧住宅資安對策指引以智慧住宅 IoT 業者（如智慧家電或監視器）、遠距遙控 IoT 設備之業者（透過遠距方式提供服務之業者）、智慧住宅服務提供者（如電視和影音串流業者）、智慧住宅設備供應業者（如製造商、設備商）、智慧住宅維護業者（如提供維修、廢棄 IOT 設備服務之業者）、公寓大廈管理委員會、物業、住戶等為對象，針對在智慧住宅內透過 IoT 機器提供各項服務導致之資訊外洩、網路攻擊，以及實體空間受到侵害等問題提供建議作法，促進住宅導入相關智慧化設備[34]。

智慧住宅資安對策指引所稱之智慧住宅，係指『透過 IoT 實現育兒世代、高齡者、單身者等各種生活方式/需求相關服務之新生活』，為住戶和關係者提供便利，具備直接或間接透過通信網路連接 IoT 設備與服務等基本 IoT 系統特徵之住宅[35]。

必須注意的是，智慧住宅資安對策指引所稱住宅分為獨棟住宅和集合住宅兩種，由於上述兩種類型住宅所導入之 IoT 設備和服務有所差異，故本指引分別列出上述兩種類型住宅之通訊網路結構示意圖和關係者，作為後續討論基礎。

---

32 〈「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました〉，経済産業省，2021/04/01，https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html（最後瀏覽日期：2021/06/19）。

33 同前註。

34 産業サイバーセキュリティ研究会，《スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン》，頁 2-3（2021）。

35 同前註，頁 4。

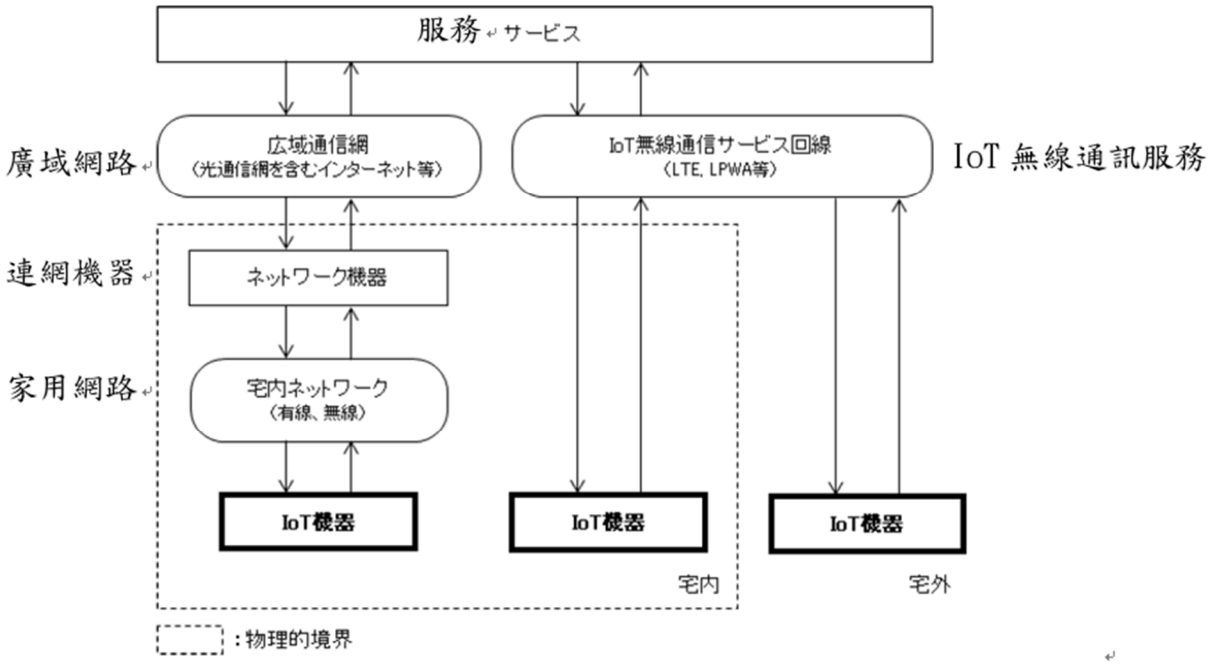

圖 2-3 獨棟住宅網路結構示意圖

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

表 2-3 獨棟住宅之關係者

服務、設備	關係者
服務	智慧住宅服務業者 智慧住宅維護業者
廣域網路、IoT 無線通訊服務	通訊設施業者
家用網路與網路設備	● 取得設備前： ➢ 智慧住宅供應業者 ● 取得設備後： ➢ 住戶 ➢ 智慧住宅維護業者
IoT 設備	● 從業者處取得或購入前 ➢ 智慧住宅供應業者 ➢ IoT 設備業者 ● 從業者處取得或購入後 ➢ IoT 設備業者 ➢ IoT 設備遠距遙控業者 ➢ 智慧住宅維護業者 ➢ 住戶

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

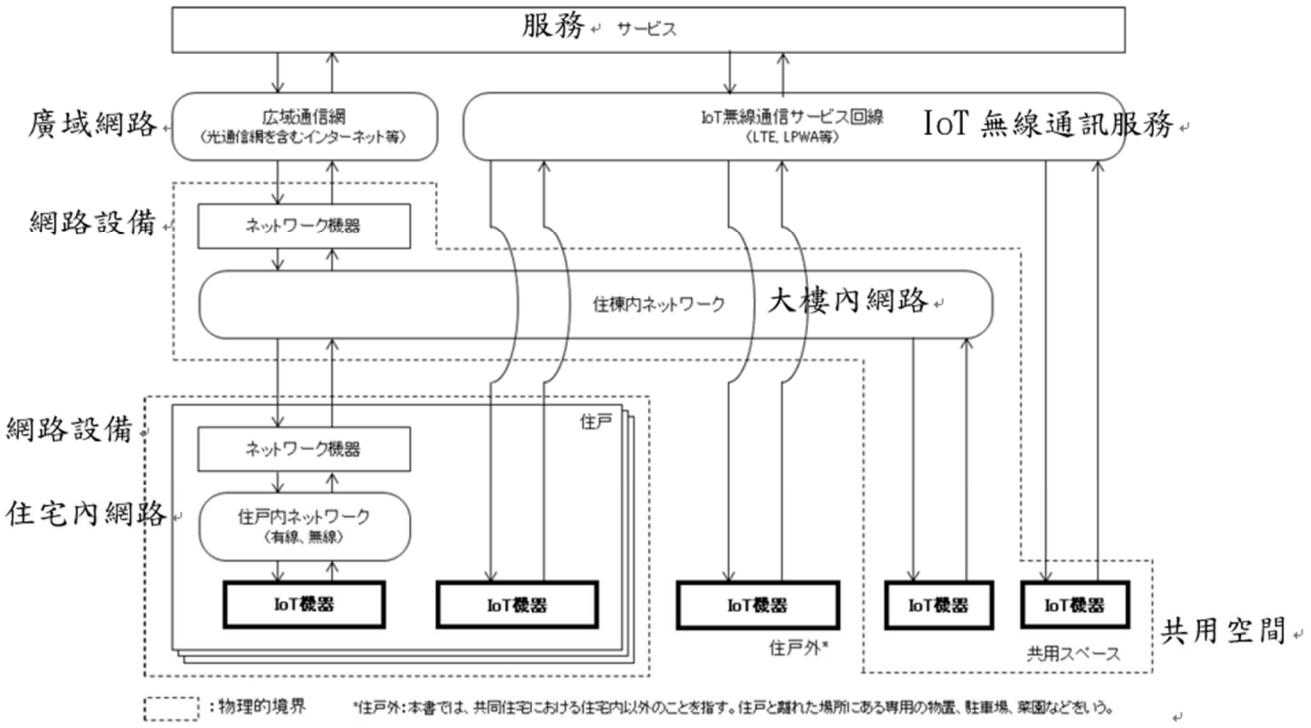

圖 2-4 集合住宅網路結構示意圖

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

表 2-4 共同住宅之關係者

服務、設備	關係者
服務	智慧住宅服務業者 智慧住宅維護業者
廣域網路、IoT 無線通訊服務	通訊設施業者
大樓網路與網路設備	● 大樓管理主體取得設備前： ➢ 智慧住宅供應業者 ● 大樓管理主體取得設備後： ➢ 分租住宅之管理單位和受託管理公司 ➢ 租賃住宅之所有者和受託管理公司
共用空間 IoT 設備	● 從業者處取得或購入共用空間 IoT 設備前： ➢ 智慧住宅供應業者 ➢ 智慧住宅 IoT 設備業者 ● 從業者處取得或購入共用空間 IoT 設備後： ➢ 智慧住宅 IoT 設備業者 ➢ IoT 設備遠距遙控業者 ➢ 智慧住宅維護業者 ➢ 分租住宅之管理單位和受託管理公司 ➢ 租賃住宅之所有者和受託管理公司
家用網路與網路設備	● 取得設備前： ➢ 智慧住宅供應業者 ● 取得設備後： ➢ 住戶 ➢ 智慧住宅維護業者 ➢ 租賃住宅之所有者和受託管理公司
家用 IoT 設備	● 從業者處取得或購入前

	➢ 智慧住宅供應業者 ➢ IoT 設備業者 ● 從業者處取得或購入後 ➢ IoT 設備業者 ➢ IoT 設備遠距遙控業者 ➢ 智慧住宅維護業者 ➢ 住戶 ➢ 租賃住宅之所有者和受託管理公司（住戶入住前）

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

智慧住宅資安對策指引基於前述智慧住宅定義，根據以下步驟，針對各利害關係人提出資安對策之建議：（1）以本指引所設定之智慧住宅範圍為基礎，設想智慧住宅可能產生之資安威脅及弱點；（2）將上述設想情境中危險源（威脅、弱點等）和事故抽象化，成為本指引所要檢討之要件；（3）整理上述要件和案例，與國際相關標準和規格進行比對；（4）針對上述（2）所抽出之各項要件，整理各利害關係人之應對措施；（5）在（4）所整理之應對措施上加以補充，提出智慧住宅最低應採取之資安對策[36]

在設想智慧住宅可能產生之威脅及弱點時，智慧住宅資安對策指引根據 2019 年 4 月 18 日制定之「虛實資安對策框架 1.0 版」（サイバー・フィジカル・セキュリティ対策フレームワーク，簡稱 CPSF）所提出之組織、人、物、資料、程序和系統等六大要素，並將上開要素分成管理面（組織、人、資料、程序）和功能面（物、系統、資料），檢討上開要素所涉之威脅及具體對策[37]。

智慧住宅資安對策指引指出，智慧住宅可能面臨資料相關及物理相

36 同前註，頁 11。
37 同前註，頁 12。

關（包含管理問題在內）之威脅。資料相關的威脅為資料傳送，無論是將資料從智慧住宅傳送到雲端，或從雲端將資料傳回住宅，在過程中都有可能發生設備被攻擊、感測器無法感應資料、資料無法傳送或讀取、傳送路徑暴露等問題，或存在設備本身安全性不足、無法依照既定方式使用、無法連接網路、未確認個人資料是否刪除等弱點；而物理相關威脅，如設備設定、更新、維修、移轉、廢棄等設備生命週期管理，以及委託外部業者維護管理 IoT 設備等過程中，也有可能發生資料外洩或被竄改等問題，或存在設備本身安全性不足，以及未依照標準作業流程處理設備等弱點[38]。

[38] 同前註，頁 14-25。

表 2-5 集合住宅資料傳送至雲端之潛在資安問題

可能發生的意外事件	● 因 IoT 設備被攻擊，利用感測器資料提供之服務，將無法正常分析和加工處理資料 ● 從設備端傳送至雲端空間之資料（含個資），如傳送途徑被竄改，利用感測器資料提供之服務，將無法正常分析和加工處理資料 ● 從設備端傳送至雲端空間之資料（含個資）外洩，進而導致個人資料或財產上損害
威脅	● IoT 設備受到攻擊，感測器無法進行測定、無法轉譯數位資料、無法傳送資料或資料於無意間傳送 ● 資料傳送路徑被暴露或竄改
弱點	● IoT 設備資安功能未徹底安裝 ● IoT 設備之弱點對策無法順利被執行 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、與網路連結之 IoT 設備以外之設備，及與集合內部網路連結之設備，未使其連結廣域網路進行管理 ● 智慧住宅相關設備信賴性低，受到攻擊時無法確實執行弱點對策 ● 更換或廢棄智慧住宅相關設備時，未確認是否有刪除資料或採取其他防止資料再利用措施 ● 更換智慧化服務和遠距管理系統等時，未確認是否有刪除資料或採取其他防止資料再利用措施 ● 使用智慧化服務時，未說明資料管理政策

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

表 2-6 雲端空間傳送資料至集合住宅之潛在資安問題

可能發生的意外事件	● 因集合住宅內 IoT 設備受到攻擊，無法依照預想方式處理從雲端空間接收之資料 ● 從雲端空間取得資料的路徑被竄改，可能使 IoT 設備被以不正方式連結，導致個資或財產等權利受到侵害 ● 從雲端空間取得資料的路徑被暴露，可能使智慧住宅之通信設備被以不正方式連結，增加被第三方攻擊之可能性
威脅	● IoT 設備受到攻擊，無法從雲端空間取得資料、無法處理資料等 ● 資料傳送路徑被暴露或竄改
弱點	● IoT 設備資安功能和安全功能（safty）未徹底安裝 ● IoT 設備與其他設備連接時，其他設備或系統資安功能或和安全功能（safty）未徹底安裝 ● IoT 設備之弱點對策無法順利執行 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、與網路連結之 IoT 設備以外之設備，及與集合內部網路連結之設備，未使其連結廣域網路進行管理

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

表 2-7 內部 IoT 設備之管理問題

可能發生的意外事件	● 利用業者所提供之服務未告知使用者資料政策，或未正確使用之不備，違反住戶意願使用個資 ● 因業者所提供之服務政策不備，以及資安對策之不足，導致業者端資料外洩 ● 利用業者所提供之安全相關服務未告知相關政策，或未正確使用之不備，導致 IoT 設備運作方式與住戶想像不同 ● 更換 IoT 設備時，被更換之設備資料外洩
威脅	● 業者所提供之服務或 IoT 設備，因未告知使用者安全性和隱私等政策或未正確被使用，導致使用者受有損害 ● 因操作錯誤使相關設備突然動作；或因設備未依照預定用途設置、使用，使其影響到建築物內其他設備 ● 搬家、販售或轉讓設備時，在未刪除前用戶資料狀況下，繼續使用 IoT 設備或服務
弱點	● 未提供服務及 IoT 設備相關政策，或未依照政策使用 ● IoT 設備資安功能和安全功能（safty）未徹底安裝 ● IoT 設備與其他設備連接時，其他設備或系統資安功能或和安全功能（safty）未徹底安裝 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 未注意到病毒感染或被以不正方式連結，繼續利用設備 ● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 提供服務之設備信賴性低，遭受攻擊時無法執行弱點對策 ● 更換或廢棄智慧住宅相關設備時，未確認是否有刪除資料或採取其他防止資料再利用措施 ● 遠距管理系統之管理端，保留設備設定資料及個資 ● 提供服務時未告知資料管理政策

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

表 2-8 外部 IoT 設備之管理問題

可能發生的意外事件	● IoT 設備被他人佔用導致意外動作，對於人體產生不良影響 ● IoT 設備干擾住家和共用空間內其他設備
威脅	● IoT 設備被佔用 ● 管理終端裝置與 IoT 設備間通信資料暴露 ● 管理終端裝置與 IoT 設備間通信資料被竄改
弱點	● IoT 設備允許經許可以外之管理終端裝置操作、設定 ● IoT 設備資安功能和安全功能（safty）未徹底安裝 ● IoT 設備與其他設備連接時，其他設備或系統資安功能或和安全功能（safty）未徹底安裝 ● 缺乏針對支援服務和維修時使用之設備，進行更換和廢棄之手續，或未依照手續採取一定措施

（資料來源：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン，2021）

針對上述智慧住宅內可能發生之威脅和存在的弱點，智慧住宅資安對策指引參考美國、歐盟、英國等先進國家或地區作法，以及日本獨立行政法人資訊處理推進機構和相關公協會所制定之標準等文件，分別針對智慧住宅 IoT 業者、遠距遙控 IoT 設備之業者、智慧住宅維護業者、智慧住宅服務提供者、智慧住宅設備供應業者、分讓住宅之管理單位或物業、住戶等對象，提出智慧住宅最低限度之資安對策。本報告整理概要如下[39]：

（一） 智慧住宅 IoT 業者

1. IoT 設備從出貨和初期化狀態時起就要確保防護機制（security）
2. 考慮安全性（safety）

[39] 同前註，頁 26-33。

3. 設備可更新軟體

4. 提供設備使用指南

（二） 遠距遙控 IoT 設備之業者/智慧住宅維護業者

1. 業者妥當運用、管理系統

2. 應根據服務與設備指南進行維護和管理

3. 應遵守相關政策/規定提供服務和進行管理

（三） 智慧住宅服務提供者

1. 妥當運用、管理服務提供業者之系統

2. 遵守相關政策/規定進行管理

（四） 智慧住宅設備供應業者

1. 選擇適合的 IoT 設備

2. 正確設置、設定 IoT 設備和服務

（五） 分讓住宅之管理單位、租賃住宅所有人或物業

1. 選擇共用空間和租戶設置之設備，並妥當管理、運用設備和網路

2. 遵守設備和服務用途及用法

（六） 住戶

1. 選擇可信賴之 IoT 設備和服務

2. 遵守 IoT 設備和服務之用途及用法

3. 保護個人資料

二、 其他參考指引

日本在制定智慧住宅資安對策指引時，參考許多國內外相關指引或報告，如前面提到智慧住宅資安對策指引根據「虛實資安對策框架 1.0 版」所提出之組織、人、物、資料、程序和系統等六大要素分析威脅和弱點，作為研擬資安對策之依據。在國內部份，日本主要參考以下指引：

（一） 虛實資安對策框架 1.0 版

日本經產省 2019 年 4 月 18 日以確保產業整體資訊安全為目的，制定「虛實資安對策框架 1.0 版」（サイバー・フィジカル・セキュリティ対策フレームワーク，以下簡稱 CPSF），內容分為概念、政策和方法三部份，第一部份概念從資安觀點出發，分析價值創造流程（バリュークリエイションプロセス）相關威脅模型，第二部份則根據上述模式提出因應威脅之對策要件，最後則依據對策要件提出具體資安對策[40]。

CPSF 適用對象為所有參與價值創造流程之主體，包括企業資安部門主管、設備開發者、制定資安對策負責人等……在內，範圍十分廣泛[41]。CPSF 在分析價值創造流程潛在威脅時，係將整個流程分為三層構造及六大要素進行分析，三層構造分別為企業間串聯、實體與網路空間串聯、網路空間串聯；而六大要素則為組織、人、物、資料、程序和系統[42]。由於 CPSF 適用對象和範圍較廣，故智慧住宅資安對策指引僅參考該框架所提出之六大要素，作為分析威脅和弱點的最小單位。

（二） IoT 資安指引（IoT セキュリティガイドライン）

日本總務省和經產省共同於 2018 年 7 月制定「IoT 資安指引」（IoT セキュリティガイドライン），以 IoT 設備和系統、服務供應者及利用者為對象，希望能讓上述對象認識網路攻擊等風險，並促使其採取因應對策[43]。「IoT 資安指引」從方針、分析、設計、建構、運用/維護等面向出發，

---

40 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました，経済産業省，2019/04/18，https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html（最後瀏覽日期：2021/06/20）。

41 経済産業省，サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要，頁 4（2019）。

42 同前註，頁 7-9。

43 IoT 推進コンソーシアム、総務省、経済産業省，《IoT セキュリティガイドライン ver1.0 概要》，頁 2（2017）。

提出 5 大指針共 21 個要點，成為智慧住宅資安對策指引在研擬具體對策時之參考，本報告整理如下[44]：

1. 考慮 IoT 的性質制定基本方針

   (1) 經營者應考慮 IoT 性質，根據 IoT 資安指引，制定基本方針，並於公司內部公告周知，以及進行必要體制和人才整備。

   (2) 了解內部潛在問題並檢討對策，以防止失誤產生。

2. 認識 IoT 的風險

   (1) 從確保 IoT 設備安全觀點出發，確認設備應具有之功能，以及應保護之資訊。

   (2) 認識聯網功能、設備和系統之風險（包括遭受物理攻擊和設備廢棄後資訊洩漏等風險）

   (3) 參考過往案例學習

3. 思考如何設計

   (1) 從避免因發生異常影響其他聯網設備角度出發設計，如發生問題之 IoT 設備應立即斷網

   (2) 從確保不特定多數人聯網安全角度出發設計

   (3) 評價及驗證是否落實安心、安全之設計

4. 思考網路相關對策

   (1) 根據功能及用途，檢討網路結構和安全性能，建構 IoT 系統和服務，並檢討透過安全通路連網之對策

   (2) 建構和利用 IoT 系統和服務時，應留意初期設定。

44 同前註，頁 3-8。

(3) 導入認驗證功能

5. 維持安全且安心的狀況，資訊發信和共享

(1) 設備出貨/軟體釋出後，維持安心安全狀態

(2) 設備出貨/軟體釋出後也要掌握 IoT 風險，並將重要事項傳達給利用者

(3) 了解 IoT 系統和服務相關者之角色

(4) 掌握設備弱點，適當提醒 IoT 管理者注意

（三） 聯網世界之開發指針（つながる世界の開発指針）

日本獨立行政法人資訊處理推進機構 2016 年 9 月以滿足聯網世界(つながる世界)設備和系統之產品品質為目的，制定「聯網世界之開發指針」第一版，惟伴隨 IoT 服務進展，實際使用相關設備和系統時之產品「利用品質」重要性也與日俱增，故資訊處理推進機構再度於 2017 年 3 月發行第二版指針，將提高並維持利用品質相關內容加入指針內[45]。

「聯網世界之開發指針」一共有 17 項指針，並提供檢核表供企業使用，確認產品開發及利用是否符合指針。上述 17 項指針部份內容已納入前述「IoT 資安指引」，且同樣為智慧住宅資安對策指引參考之一，本報告整理 17 項指針內容如下[46]：

1. 制定安全安心之基本方針

2. 建立安全安心之體制和人才

3. 針對內部潛在問題預作準備

4. 釐清 IoT 設備應具有之功能

5. 設想可能因聯網導致的風險

45 独立行政法人情報処理推進機構，《つながる世界の開発指針》，頁 1（2017）。

46 同前註，頁 32-87。

6. 設想可能因聯網擴散的風險
7. 認識物理層面的風險
8. 從個別到整體都能保護之設計
9. 避免影響其他人之設計
10. 可以實現安心安全之整合性設計
11. 可確保不特定多數人安全安心之設計
12. 驗證、評價是否實現安全安心之設計
13. 設有可以掌握、紀錄自身狀態之功能
14. 設有即便經過一段時間也可維持安全之功能
15. 出貨後也要掌握 IoT 風險
16. 向出貨後關係業者傳達應遵守事項
17. 讓一般利用者知悉聯網風險

貳、 美國

一、 IoT 設備資安能力核心基準（IoT Device Cybersecurity Capability Core Baseline）

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）於 2020 年 5 月 29 日公布「NISTIR 8259 物聯網設備商之基本網路安全活動」（Foundational Cybersecurity Activities for IoT Device Manufacturers）和 8259A「IoT 設備資安能力核心基準」（IoT Device Cybersecurity Capability Core Baseline），後者定義組織在面臨物聯網挑戰時應考慮之設備基本資安功能，而前者則說明製造商如何依照「NISTIR 8259 物聯網設備商之基本網路安全活動」所制定之標準進行開發，將 IoT 設備應具備之核心功能導入開發過程[47]。

[47] Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, *IoT Device Cybersecurity Capability Core Baseline*, available at: https://doi.org/10.6028/NIST.IR.8259A (last visited 20. Jun 2021).

「IoT 設備資安能力核心基準」以表格整理核心基準，表格各欄依序列出設備資安能力、各能力通常具備之要素、需要具備這些能力和要素之理由如下：

表 2-9 IoT 設備資安核心能力基準

設備資安能力	通常要素	理由
設備識別（Device Identification）	1. 唯一的邏輯識別符（logical identifier） 2. 位於設備外部或內部之唯一實體識別符（physical identifier），可授權個體訪問	1. 此功能可以支援資料保護、弱點管理、訪問管理和事件檢測等 2. 唯一的邏輯識別符可區分設備與其他設備，以及進行驗證 3. 唯一的物理識別符可在邏輯識別符失效時使用 4. 識別能力可能會需要額外的非唯一之邏輯識別符，用於更具體之目的
設備配置（Device Configuration）	1. 可以變更設備軟體設定 2. 可以將限制更改為僅授權個體（entities） 3. 可授權實體恢復設備安全配置（該安全設定由個體定義）	1. 此功能可以支援資料保護、弱點管理、訪問管理和事件檢測等 2. 允許個體出於多種原因更改配置，否則將無法滿足個體需求 3. 多數資訊安全功能仰賴設備配置功能 4. 未經授權之個體可能出於各種原因想要變更配置，故必須具有可恢復原先安全配置之功能
資料保護（Data Protection）	1. 可將安全加密模塊用於標準化加密演算法，防止設備儲存和傳輸之機密	1. 此功能可以支援資料保護、弱點管理、訪問管理和事件檢測等

	性和完整性受到損害 2. 可以讓所有個體無法存取設備上所有資料，無論其之前是否獲得授權 3. 與設備設置功能一起使用之設置功能，如設定密碼長度	2. 個體通常希望保護資料機密性，避免未經授權個體存取或濫用資料 3. 個體通常希望保護資料完整性，避免被有意或無意地竄改
對介面之訪問（Logical Access to Interfaces）	1. 可以在邏輯上或物理上禁止任何本地或網路介面 2. 可以將網路介面之訪問權限限制為僅限授權個體（如設備身份驗證） 3. 與設備設置功能一起使用之設置功能，如啟用、禁用或調整有關鎖定或禁用帳戶，以及其他身份驗證	1. 此功能可以支援資料保護、弱點管理、訪問管理和事件檢測等 2. 限制訪問可減少被攻擊的機會 3. 根據設備狀況，應部份或完全限制訪問，如若設備沒有憑證，則在登錄時會受到限制
軟體更新（Software Update）	1. 可透過遠端或本地工具更新 2. 在安裝之前可驗證更新 3. 可以恢復更新前版本 4. 可以限制僅授權個體進行更新 5. 可啟用或禁用更新功能 6. 與設備設置功能一起使用之設置功能，如可以將更新設定為自動或手動	1. 此功能可以支援弱點管理 2. 軟體更新可以消除物聯網漏洞，降低被攻擊可能性 3. 更新可以修正設備運行問題，提高設備可用性 4. 個體可以透過更新滿足其需求 5. 某些組織或個體可能需

		要恢復到前一個版本的功能
資安狀態提醒（Cybersecurity State Awareness）	1. 能夠報告設備資安狀態 2. 可區分設備何時可以按照預期運行或需要降級處理 3. 可以限制只有個體才能查看狀態 4. 防止任何個體編輯狀態 5. 狀態訊息可用於其他設備，如事件日誌	1. 此功能可以支援弱點管理和事件檢測 2. 資安狀態提醒有助於調查危害、辨識誤用和排除操作問題 3. 設備如何讓其他個體了解資安狀態，將根據特定需求和目標而有所不同

（資料來源：IoT Device Cybersecurity Capability Core Baseline, 2020）

參、 歐盟

一、 物聯網基本安全建議（Baseline Security Recommendations for IoT）

歐盟網路和資訊安全局（The European Union Agency for Network and Information Security, ENISA）基於物聯網範圍涵蓋聯網服務和整個設備生態系統，如感測器、消費產品和智慧家電，而這些設備透過蒐集、交換和處理資料，一方面改變我們的生活狀態，另一方面卻也對安全帶來重大挑戰，於 2017 年 11 月發布「物聯網基本安全建議」（Baseline Security Recommendations for IoT）報告，以解決物聯網潛在的安全問題，確保產品和服務提供之安全性[48]。

ENISA 將物聯網定義為一透過可互相連結之感測器與起動器之生態系統，參考近年歐盟和美國針對物聯網安全所採取之措施，針對

[48] The European Union Agency for Network and Information Security (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, 7(2017), available at; https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a506-01aa75ed71a1/language-en (last visited 22. Jun 2021).

物聯網專家、軟體開發者和製造商、資安專家、IT/安全解決方案工程師、首席資訊安全官（Chief Information Security Officer, CISO）、關鍵基礎設施保護專家等對象，提出物聯網安全基本建議[49]。

「物聯網基本安全建議」分為 6 章，第 1 章說明本報告目的和研究方法，第 2 章定義本報告所稱之物聯網關鍵元素和環境，第 3 章分析物聯網主要風險、弱點和漏洞，第 4 章針對前面所提出之風險、弱點和漏洞提出因應措施，第 5 章進一步從兩大面向分析物聯網資安主要差異和未來挑戰，最後第 6 章則根據前面所提出之因應措施和差異分析，提出未來發展建議[50]。

針對物聯網可能產生之威脅，ENISA 將其分為惡意活動/濫用、竊聽/攔截/劫持、停電、損壞/損失（IT 資產）、故障、災難、物理攻擊等 8 類，並依照影響程度分為低中高不同等級[51]。ENISA 在報告中亦進一步針對上述 8 類威脅，以表格方式整理各類威脅樣態，以及可能受影響之設備。如在第一類「惡意活動/濫用」中，具體可能產生的威脅包括對隱私之攻擊（Attacks on privacy）在內，而此一威脅可能以想之設備則有 IoT 裝置、平台和後端（Platform & Backend）以及資訊[52]。

49 *id*, 12-15.
50 *id*, 16-17.
51 *id*, 32.
52 *id*, 34.

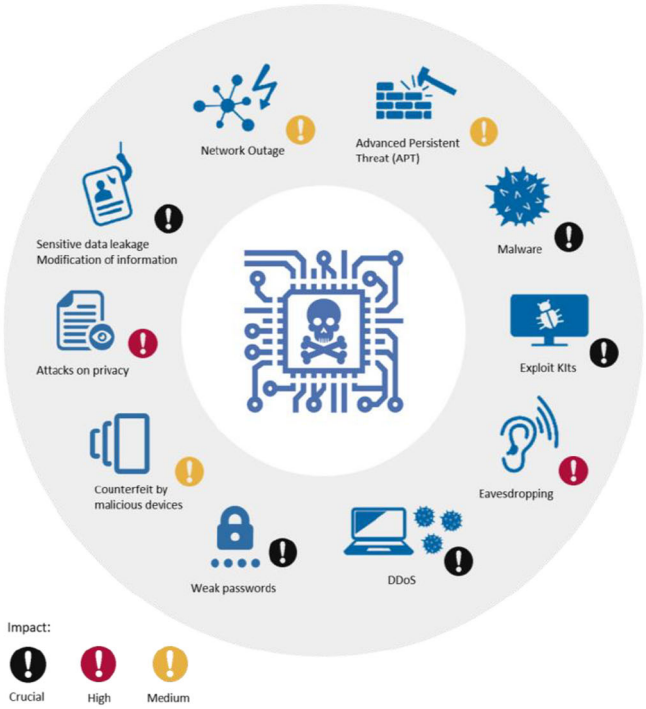

圖 2-5 物聯網可能產生之威脅

（資料來源：Baseline Security Recommendations for IoT, 2017）

上述第 4 章所提出之因應措施分為政策（Policies, PS）；組織、人員和流程措施（Organisational, People and Process measures,OP）；技術措施（Technical Measures, TM）3 類。第一類政策係指針對資訊安全之具體策略和目標，其通常會包括組織活動在內；第二類「組織、人員和流程措施」要求所有企業都必須有資訊安全標準，並確認員工可以落實流程管理及安全性操作，且企業應想辦法確保供應商和承包商可以負責，並準備好發生事故的因應措施；第三類「技術措施」則是確保物聯網安全之必要技術[53]。上述三類因應措施之具體內容如下[54]：

（一） 政策

1. 從安全出發設計（Security by design）：在整個設計和開發週期中，從整體角度出發考慮物聯網系統安全性

53 *id*, 46-52.
54 *id*.

2. 從隱私出發設計（Privacy by design）：從保護隱私角度出發，讓隱私成為系統一部份
3. 資產管理（Asset Management）：建立和維護關鍵網路資產管理程序及設定控制
4. 風險和威脅識別及評估（Risk and Threat Identification and Assessment）

（二） 組織、人員和流程措施

1. 臨終支援（End-of-life support）：發展物聯網產品之臨終支援策略
2. 經驗證之解決方案（Proven solutions）：導入經驗證之解決方案，避免使用某些自定義解決方案
3. 管理安全漏洞或事件（Management of security vulnerabilities and/or incidents）：建立分析及掌控安全事件之流程
4. 員工安全意識培養和訓練（Human Resources Security Training and Awareness）
5. 第三方關係（Third-Party relationships）：涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等

（三） 技術措施

1. 硬體安全（Hardware security）：如使用包含安全功能之硬體加強設備保護和完整性
2. 信賴與誠信管理（Trust and Integrity Management）：如簽名或密碼加密等措施，確保簽名或密碼不會被竄改
3. 默認安全和隱私（Strong default security and privacy）：在默認狀態下應啟用安全功能

4. 資料保護與合規（Data protection and compliance）：個人資料應依法蒐集、處理、利用
5. 系統安全及可靠性（System safety and reliability）：系統設計時應考慮到中斷可能性，並防止因中斷導致系統產生不可逆的損害
6. 安全軟體/框架更新（Secure Software / Firmware updates）：確認軟體可以透過空中下載（Over-the-Air, OTA）進行更新，以及透過安全管道進行更新。更新的檔案本身不包含敏感資料，並且經過加密，檔案在更新前會經過驗證。
7. 驗證（Authentication）：設計驗證及驗證機制；要求用戶更改初始帳號和密碼，且新設密碼必須使用強密碼或個人識別碼等
8. 授權（Authorisation）：設計時應將需要授權和不需要部份予以區分
9. 存取控制-物理和環境安全（Access Control - Physical and Environmental security）：透過存取控制確保資料完整性和機密性
10. 密碼（Cryptography）：確保正確有效地使用密碼，以保護資料機密性、真實性或完整性
11. 安全且可靠的通訊（Secure and trusted communications）：確保網路傳輸和儲存之完整性、機密性和真實性
12. 安全界面和網路服務（Secure Interfaces and network services）：如單獨設備受到攻擊或威脅，不會影響其他設備；避免整個產品系統使用相同密鑰；確認只有必要端口是公開且可使用……
13. 安全輸入和輸出處理（Secure input and output handling）：資料輸入前進行驗證，輸出時加以過濾

14. 日誌（Logging）：透過實施日誌記錄身份驗證、帳戶存取權限、修改安全規則以及系統功能等相關事件

15. 監控與稽核（Monitoring and Auditing）：定期監控以驗證設備行為，檢測是否有惡意軟體，即時排除措施

肆、 英國

一、 消費者物聯網資安實踐準則（Code of Practice for consumer IoT security）

英國數位、文化、媒體及運動部 2018 年 10 月 14 日公布「消費者物聯網資安實踐準則」，針對 IoT 製造商和其他利害相關者（設備製造商、IoT 服務提供商、應用程式開發商、零售商）提出 13 項準則，其中前 3 項準則應優先適用，以保護者隱私和安全，並降低被攻擊之風險[55]。上述準則如下[56]：

（一） 無預設密碼：許多聯網產品都有預設帳號和密碼，如用戶沒有更改帳號密碼，預設密碼將成為安全上隱憂，設備製造商應考慮取消此種作法。

（二） 實施弱點揭露政策：所有提供聯網設備和服務的公司，如 IoT 設備製造商、服務提供商、應用程式開發商等，應提供公開窗口，以便相關人員回報問題，即時處理發現的弱點。

（三） 保持軟體更新：聯網設備軟體應可更新，且更新必須即時且不影響設備功能。零售商應向用戶說明軟體支援之更新期限和條件。

（四） 安全儲存憑證及安全敏感資料：任何憑證應可安全地儲存於設備和服務上，應被安全儲存之敏感資料包括密鑰、設備標識符和初始向量。

---

55 *Code of Practice for consumer IoT security*, GOV.UK, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (last visited 21. Jun 2021).

56 *id*.

（五） 安全傳輸：安全敏感數據應在傳輸過程中加密，所有密鑰都應安全地管理。

（六） 最小化暴露的攻擊面：所有設備和服務都應遵循最小化原則，如關閉沒有使用的通訊埠等。

（七） 確保軟體完整性：聯網設備軟體應使用安全機制進行驗證。如果檢測到未經授權的變更，設備應提醒消費者/管理員。

（八） 保護個人資料：如所蒐集之資料涉及個人資料，則應根據歐盟一般資料保護規則（General Data Protection Regulation, GDPR)或 2018 資料保護法等個資相關規定處理。

（九） 系統可以有彈性地因應暫時中斷：應考慮網路斷線和停電等可能性，讓設備和服務更具備彈性，即便在中斷情況下也可運作並保持本地功能。

（十） 監控系統遙測資料：如果遙測資料是從 IoT 設備和服務蒐集而來，應對其進行安全監控。

（十一）讓其容易刪除個人資料：應讓消費者希望刪除或處理設備時，可以輕易刪除其個人資料。

（十二）容易進行設備保養和維護：聯網設備的安裝和維護步驟應最小化，並在可用性方面遵守最佳安全實踐，且應向消費者提供安全設置設備之指南。

（十三）驗證輸入資料：應驗證通過用戶界面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料。

第四節、 小結

本章爬梳我國集合住宅類智慧建築定義及發展狀況，並盤點我國集合住宅類資安相關規範，並整理國外資通訊安全應用相關法制規定。惟上述國內外相關規定其適用對象、範圍與重點等皆不盡相同，故整理表格如下，以更清楚掌握相關規範重點。

表 2-10 國內外資通訊安全應用相關法制規定

國別/地區	名稱	適用對象與範圍	規範重點
我國	物聯網場域資安防護評估指引	● 已開發完成之單一物聯網場域 ● 適用對象為物聯網設備製造商、系統整合商、軟體或硬體開發人員、系統規劃人員、服務供應商與使用者	從物聯網應用情境出發，以威脅建模、漏洞檢測、滲透測試及衝擊分析之評估報告等四道流程，進行物聯網場域資安防護評估。
	消費性物聯網產品資安標準	消費性物聯網產品，涵蓋消費性物聯網應用設備及其連接之無線網路環境	規範消費性物聯網產品之網路安全要求
日本	智慧住宅資安對策指引	● 具備直接或間接透過通信網路連接 IoT 設備與服務等基本 IoT 系統特徵之智慧住宅（包含獨棟與集合住宅） ● 智慧住宅 IoT 業者、遠距遙控 IoT 設備之業者、智慧住宅服務提供者、智慧住宅設備供應業者、智慧住宅維護業者、公寓大廈管理委員會、物業、住戶等	從管理面和功能面出發，分析具體運用情境中之潛在威脅和弱點，並據此針對智慧住宅 IoT 業者、遠距遙控 IoT 設備之業者、住戶等提出資安對策
美國	物聯網設備資安能力核心基準	物聯網設備	組織在面臨物聯網挑戰時，應考慮之設備基本功能
歐盟	物聯網安全基本建議	● 物聯網專家、軟體開發者和製造商、資安專家、IT/安全解決方案工程師、首席資訊安全官、關鍵基礎設施保護專家等	依據定義關鍵要件、分析主要風險與弱點、提出因應對策和未來發展建議等流程，提供解決物聯網潛在的安全問題，確保產品和服務提供安全性之建議
英國	消費性物聯網資安實踐準則	● 消費性物聯網設備 ● IoT 製造商和其他利害相關者（設備製造商、IoT 服務提供商、應用程式開發商、零售商）	提出 13 項準則，其中前 3 項準則應優先適用，以保護者隱私和安全，並降低被攻擊之風險

（資料來源：本研究整理）

第三章 我國集合住宅類智慧建築導入資通訊安全設備應注意事項

第一節、 從國外相關法制規定出發

伴隨時代進步和生活型態轉變，集合住宅已經成為我國主要建築物類型之一，且智慧化住宅亦成為未來建築物發展趨勢，而為發揮我國資通訊產業優勢，內政部建築研究所亦積極透過各項政策引導和推動建築物智慧化，發展迄今已略具成效。

然而，在建築物內導入資通訊設備和系統，雖然可以帶來便利，但新技術卻也同時存在安全上的隱憂。在實體面，物聯網裝置和資通訊設備可能遭遇設備故障、訊號不良、人員不會操作等問題，使設備無法正常運作；在軟體面，資通訊設備則可能因作業系統、應用程式存在漏洞，或遭受網路攻擊，洩漏所蒐集和儲存之資料，對安全防護造成威脅。針對上述問題，世界各國陸續透過立法或制定政策、指引、標準等方式，建議資通訊設備或物聯網裝置之設計和使用方式，而日本更進一步以智慧住宅為對象，針對智慧住宅關係人導入或使用相關設備可能產生之風險，提出因應對策和建議。

本研究在整理我國、日本、美國、歐盟和英國有關確保資通訊應用安全之規範後，歸納出以下重點：

壹、 應定義適用對象和範圍

綜觀各國所提出之指引或文件，由於資通訊或聯網設備種類及態樣廣泛，難以預測可能的應用情境，故相關文件首先都會釐清適用對象和範圍，以利後續設想應用情境，作為分析潛在威脅和風險之基礎。

在定義適用對象和範圍時，其他國家主要係說明何謂物聯網，但由於日本「以安心、安全智慧住宅為目標之虛實資安對策指引」係以智慧住宅為對象，故其則是定義智慧住宅，並分別設想獨棟住宅和集合住宅之聯網環境，以及可能涉及之利害關係人。

本研究之目的係針對我國集合住宅類智慧建築資通訊安全應用提出注意事項，故在提出注意事項上，亦須先釐清集合住宅類智慧建築之定義和範圍，方能設想在導入資通訊應用時可能會出現的問題，進而提出因應對策。基於上述理由，本研究於本章第一節討論名詞定義，以便確認討論範圍，後續也將以此為基礎，參考

日本作法設想可能之應用情境、風險和所涉及之利害關係人。

貳、 根據實際應用場域設想可能風險

日本智慧住宅資安對策指引從組織、人、物、資料、程序和系統等六大要素出發，並將上開要素分成管理面（組織、人、資料、程序）和功能面（物、系統、資料），檢討在實際場域中可能產生之風險。歐盟 ENISA 在提出安全建議前，也先分析物聯網的主要風險、弱點和漏洞等，將物聯網風險依照類型分為 8 類，並羅列各類風險下之具體威脅樣態，作為後續討論基礎。我國物聯網場域資安防護評估指引，亦從物聯網應用情境出發，以威脅建模、漏洞檢測、滲透測試及衝擊分析之評估等流程進行評估。由此可知，針對物聯網場域之資安，為能具體提出因應對策，根據實際應用場域情境設想潛在風險，為研擬注意事項之必經過程。

然而，上述指引歸納潛在風險的方式並不相同，日本是從管理面（組織、人、資料、程序）和功能面（物、系統、資料）出發，針對上述情況盤點可能面臨之威脅；歐盟則是直接將風險分類，從 8 種主要風險出發，整理各類型風險下之具體威脅及可能受其影響的設備；而我國則是識別物聯網場域之威脅類型與情境，其中包括身份冒用、資料竄改、否認性、資訊洩漏、阻斷服務、權限提升等類型。由於我國和歐盟指引係針對整個物聯網，故所設想的應用情境和威脅類型都較上位，而日本智慧住宅資安對策指引範圍限縮在智慧住宅，故指引直接從智慧住宅管理面和功能面出發，盤點可能發生之問題，讓指引所提出之建議更加貼近需求。然後，日本智慧住宅資安對策指引亦採取類似歐盟作法，將威脅本身進行分類，惟其僅將威脅分為物理和資料兩類。

由於本研究係針對集合住宅類智慧建築研提注意事項，或可參考日本作法，從智慧住宅管理面和功能面出發盤點可能發生之問題，再針對上述兩大面向問題提出對策。

參、 將因應對策分類

綜觀本報告所整理之指引，有些只是單純列出建議事項，而有些則進一步依照不同邏輯進行分類，如日本智慧住宅資安對策指引依序針對各利害關係人分別提出建議；歐盟「物聯網基本安全建議」則將建議分為「政策」、「組織、人員和流程

措施」、「技術措施」3 類；我國消費性物聯網產品資安標準則分從 8 大安全構面出發，研擬安全要求及安全要求項目。本研究進行訪談時，亦請益專家該從哪些角度研提注意事項，有專家認為可分別從軟硬體和程序面（包含人員管理在內）著手，軟體上要求即時更新資安軟體，硬體面則要求相關設備符合特定規範或規格，而在人員和程序方面，則要求管理單位建立 SOP，建議管理單位（如管理委員會）聘用合格資安證照人員，交給公協會訓練，而程序書（SOP&SMP）由起造人完成及資安第三方驗收合格再發給使用執照，然後每季進行驗證[57]；惟考量到集合住宅類智慧建築規模大小不一，對於資安需求程度亦有所不同，亦有專家建議在研擬注意事項時應納入分級概念，避免過度要求反而成為住戶或管理單位負擔[58]。針對上述意見，有專家進一步具體建議小規模集合住宅規範重點在於資料備份，而大型社區因是交由物業管理，故重點應放在人員管理[59]。本研究接下來將參酌國外作法及上述訪談結果，研擬因應對策。

肆、 提出資通訊設備應具備之基本功能

除針對應用情境可能產生之風險提出建議外，日本「聯網世界之開發指針」就產品開發及利用提出守則，美國「IoT 設備資安能力核心基準」則提出 6 種 IoT 設備應具備之核心能力，均從設備本身出發來確保後續使用上的安全性。此外，歐盟「物聯網基本安全建議」提出三大方向，其中之一亦為「技術措施」，故無論是否單獨規範物聯網設備應符合何種標準，或要求設備至少應具備哪些功能，在研擬注意措施時都應注意對軟硬體本身之要求。

第二節、 我國集合住宅類智慧建築資訊安全應用情境

壹、 集合住宅類智慧建築架構及主要智慧化項目

本報告於第二章第一節壹、「集合住宅類智慧建築定義與主要導入之智慧化項目」中，探討我國法上集合住宅類智慧建築之定義，認為所謂集合住宅類智慧建築，係指『透過導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，

57 計畫團隊親自訪談林世俊常務監事，台灣物業管理學會，台北市（2021/03/23）

58 計畫團隊親自訪談陳曉強資深顧問，台灣資通產業標準協會，台北市（2021/03/17）。類似意見者：計畫團隊親自訪談陳立人副工程司，台北市政府都市發展局，台北市（2021/04/27）

59 計畫團隊親自訪談黃健偉總經理，建伸智慧綠建築公司，台北市（2021/03/18）

以達到安全健康、便利舒適、節能永續目的之建築物』，並屬於《建築物使用類組及變更使用辦法》H-2「供特定人長期住宿之場所」類別之「具有共同基地及共同空間或設備，並有三個住宅單位以上之建築物」。

為更清楚掌握集合住宅類智慧建築架構及主要應用之智慧化服務，本報告於前文分別參考有關新建集合住宅及既有集合住宅之文獻，了解其主要架構及所導入之智慧化項目。由前文分析可知，無論是社會公宅或既有建築物智慧化改善，基本上都以符合《智慧建築評估手冊》之合格級門檻以上為目標，然後再依智慧住宅或智慧社區本身之需求，增加物業管理、智慧化生活服務（訪客服務和創新服務）或智慧健康照護、智慧停車場管理等項目。

基於上述理由，本報告擬參考《智慧建築評估手冊》之合格級門檻，亦即智慧建築標章基本規定評估項目（綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適），作為集合住宅類智慧建築之主要架構，並參考《台北市政府智慧社區建置規範手冊》有關社會公宅智慧社區之必備建置項目，以及既有建築物智慧化改善主要項目，規劃集合住宅類智慧建築之智慧化項目。

本報告所研擬之集合住宅類智慧建築基本架構和智慧化項目如下圖：

圖 3-1 集合住宅類智慧建築基本架構和智慧化項目

（資料來源：本研究製作）

上述智慧化服務會透過雲端系統或平台進行串聯，示意如下圖 3-2：

圖 3-2 以雲端系統串聯各項智慧化服務

（資料來源：本研究製作）

貳、 利害關係人

由於本報告係以集合住宅類智慧建築為研究對象，從其基本架構及所提供之智慧化服務出發，整理集合住宅類智慧建築之可能利害關係人（表 3-2）。

表 3-1 集合住宅類智慧建築利害關係人

智慧化服務	利害關係人
安全防災	● 安全防災系統（如防火系統、防震系統、防水系統、防盜系統、監視系統、門禁系統、停車管理、有害氣體防制、緊急求救系統）開發商 ● 安全防災系統維運商 ● 集合住宅類智慧建築管理單位
資訊通信	● 以固定通信網路架構提供電信服務之電信事業及系統經營者[60] ● 設計建築物電信設備及空間之建築物起造人
建築自動化	● 建築自動化子系統（如電力監控、能源管理系統、對講系統、電梯監控、監視系統等……）開發商 ● 建築自動化系統整合商 ● 建築自動化系統維運商 ● 集合住宅類智慧建築管理單位
能源管理	● 能源管理系統開發商 ● 能源管理系統維運商 ● 節能/儲能設備商（如智慧電錶、電動車充電設備） ● 綠能創電設備商（如太陽光電發電設備、風力發電設備等） ● 根據資訊進行公共區域能源管理之單位
智慧生活服務	● 訪客及創新服務提供商 ● 集合住宅類智慧建築管理單位 ● 住戶
物業管理	● 智慧化物業管理系統開發商 ● 智慧化物業管理系統維運商 ● 集合住宅類智慧建築管理單位 ● 住戶

（資料來源：本研究整理）

參、 集合住宅類智慧建築潛在之風險

60 此處用語參考「建築物電信設備及空間設置使用管理規則」第 4 條。

本報告在調查與整理國外相關法制規定後，發現為能具體提出智慧建築之資安因應對策，大多會根據應用場域設想潛在風險，如日本從管理面（組織、人、資料、程序）和功能面（物、系統、資料）出發，針對上述情況盤點可能面臨之威脅，而歐盟則是直接將風險分為 8 種類型，依序整理各類型風險下之具體威脅及可能受其影響的設備。本報告以日本針對智慧集合住宅所盤點之資安風險為基礎，並參酌深度訪談及歐盟盤點之物聯網風險，分別從管理面和功能面出發，整理我國集合住宅類智慧建築之潛在資安風險如下表 3-3 至 3-6。

表 3-2 至 3-5 係以表 2-4 至表 2-7 為基礎，表 3-2 和表 3-3 係針對管理面相關規範不備，盤點可能導致之風險；表 3-4 和表 3-5 則是針對功能面問題，盤點設備可能產生之風險，並參酌專家訪談和歐盟規範所新增、調整和精簡內容，調整部份於文字下以底線加以標示。

表 3-2 資料從集合住宅傳送至雲端空間之風險

可能發生的意外事件	● 因 IoT 設備被攻擊，利用感測器資料提供之服務，將無法正常分析、加工處理資料並提供服務 ● 從設備端傳送至雲端空間之資料(含個資)，如傳送途徑被竄改，利用感測器資料提供之服務，將無法正常分析、加工處理資料並提供服務 ● 從設備端傳送至雲端空間之資料（含個資）被複製或外洩，進而導致個人資料或財產上損害
威脅	● IoT 設備受到攻擊，感測器無法進行測量、無法轉譯數位資料、無法傳送資料或執行未經用戶同意之動作(如傳送資料) ● 資料傳送路徑被暴露或竄改，使資料被複製、竊取、刪除或竄改
弱點	● IoT 設備資安功能未徹底安裝或未即時更新 ● IoT 設備無法順利執行弱點對策 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、與網路連結之 IoT 設備以外之設備，及與集合內部網路連結之設備，未使其連結廣域網路進行管理 ● 更換或廢棄 IoT 設備、智慧化服務系統等時，未確認是否有刪除資料或採取其他防止資料再利用措施 ● 使用智慧化服務時，未說明資料管理政策

（資料來源：本研究整理）

表 3-3 資料從雲端空間傳送至集合住宅之潛在資安風險

可能發生之意外事件	● 因集合住宅內 IoT 設備受到攻擊，無法依照預設方式處理從雲端空間接收之資料 ● 從雲端空間取得資料的路徑被竄改，可能使 IoT 設備被以不正方式連結，導致個資或財產等權利受到侵害 ● 從雲端空間取得資料的路徑被暴露，可能他人獲取有關網路設備、使用之協議、開放端口、使用之服務等資訊，增加被第三方攻擊之可能性
威脅	● IoT 設備受到攻擊，無法從雲端空間取得資料、無法處理資料等 ● 資料傳送路徑被暴露或竄改，使資料被竊取、刪除或竄改
弱點	● IoT 設備資安功能不足或未即時更新軟體 ● IoT 設備安全性（safty）不足 ● IoT 設備與其他設備連接時，其他設備或系統資安功能不足或未即時更新軟體；設備安全性（safty）不足 ● IoT 設備之弱點對策無法順利執行 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 集合住宅內部網路、與網路連結之 IoT 設備以外之設備，及與集合內部網路連結之設備，未使其連結廣域網路進行管理

（資料來源：本研究整理）

表 3-4 內部設備之潛在資安風險

可能發生的意外事件	● (他人)利用業者所提供之服務未告知使用者資料政策，或使用者未正確使用之不備，違反住戶意願使用個資 ● 因業者所提供之服務政策不備，以及資安對策之不足，導致業者端資料外洩 ● (他人)利用業者所提供之安全相關服務未告知使用者相關政策，或使用者未正確使用之不備，使硬體設備或軟體應用程式損壞，或使設備以不同於使用者想像方式運作，或執行未經用戶同意之動作（如竊聽、攔截信件、中斷服務等） ● 因天然或人為災害（如硬體設置錯誤或遭人故意破壞等）導致 IoT 設備損壞或無法正常運作 ● 更換 IoT 設備時，被更換之設備資料外洩
威脅	● 業者所提供之服務或 IoT 設備，因未告知使用者安全性和隱私等政策或未正確被使用，導致硬體設備或軟體應用程式損壞，或使用者受有損害 ● 因操作錯誤使相關設備突然動作；或因設備未依照預定用途設置、使用，使其影響到建築物內其他設備 ● 因天然或人為災害（如硬體設置錯誤或遭人故意破壞等）導致設備損壞或無法正常運作 ● 搬家、販售或轉讓設備時，在未刪除前用戶資料狀況下，繼續使用 IoT 設備或服務
弱點	● 未提供服務及 IoT 設備相關政策，或未依照政策使用 ● IoT 設備資安功能不足或未即時更新軟體 ● IoT 設備安全性（safty）不足 ● IoT 設備與其他設備連接時，其他設備或系統資安功能不足或未即時更新軟體；設備安全性（safty）不足 ● IoT 設備未依照預定用途、用法進行設置和運用 ● 未注意到病毒感染或被以不正方式連結，繼續利用設備

	● 集合住宅內部網路、及與網路連結之 IoT 設備以外之設備，住家內網路、及與網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用 ● 提供服務之設備信賴性低，遭受攻擊時無法執行弱點對策 ● 更換或廢棄智慧住宅相關設備時，未確認是否有刪除資料或採取其他防止資料再利用措施 ● 遠距管理系統之管理端，保留設備設定資料及個資 ● 提供服務時未告知資料管理政策

（資料來源：本研究整理）

表 3-5 外部設備之潛在資安風險

可能發生的意外事件	● IoT 設備被他人佔用擅自動作，對於人體產生不良影響 ● IoT 設備干擾住家和共用空間內其他設備
威脅	● IoT 設備被佔用 ● 管理終端裝置與 IoT 設備間通信資料暴露 ● 管理終端裝置與 IoT 設備間通信資料被竄改
弱點	● IoT 設備允許經許可以外之管理終端裝置操作、設定 ● IoT 設備資安功能不足或未即時更新軟體 ● IoT 設備安全性（safty）不足 ● IoT 設備與其他設備連接時，其他設備或系統資安功能不足或未即時更新軟體；設備安全性（safty）不足 ● 缺乏針對支援服務和維修時使用之設備，進行更換和廢棄之手續，或未依照手續採取一定措施

（資料來源：本研究整理）

第三節、 注意事項草案內容

在完成集合住宅類智慧建築架構及提供之智慧化服務分析，整理各項服務可能涉及之利害關係人，以及分析集合住宅類智慧建築潛在之資安風險後，本報告將同時參酌第二章專家訪談及國外法制調查結果，從功能面和管理面出發研擬注意事項草案。

本報告首先綜整日本、美國、英國、歐盟相關規範，發現功能面主要從：系統默認安全、實體安全、軟體更新、識別功能、設定功能、資料保護、網路傳輸、介面連接和存取、紀錄功能、系統彈性、操作指南等出發；管理面則從政策、組織、流程、人員、資料等出發，研擬注意事項。本報告更進一步參考國外規定，針對上述功能面和管理面應考量重點，整理各國相關規定如下表 3-6 及 3-7。

表 3-6 集合住宅類智慧建築功能面應注意事項

	功能面（設備、系統、資料）注意事項	參考規定
系統默認安全	● IoT 設備從初期起就要有保全機制（security） ● 默認安全和隱私功能（在默認狀態下啟用安全功能）	日本智慧住宅資安對策指引 歐盟物聯網基本安全建議 英國消費性物聯網資安實踐準則
實體安全	● 設備應考慮安全性（safety） ● 產品宜支援安全啟動(Secure boot)機制 ● 產品之使用者介面應驗證輸入的語法和內容	日本智慧住宅資安對策指引 我國消費性物聯網產品資安標準
軟體更新	● 軟體可透過空中下載（Over-the-Air, OTA）、遠端或本地工具更新，且更新時不影響設備功能。如更新時會中斷產品功能，宜於更新前告知使用者 ● 當產品支援線上安全更新，產品應鑑別更新伺服器身分之真實性，且應於更新檔傳輸過程中確認真實性與完整性 ● 更新軟體應不包含敏感資料且經加密 ● 軟體更新應使用安全機制進行驗證，確保更新軟體真實性與完整性 ● 可以限制僅特定人可更新軟體 ● 可以決定是否啟用更新功能，或將更新功能改為手動 ● 更新後可恢復到前一版本 ● 產品宜以清楚識別的方式通知使用者進行更新	日本智慧住宅資安對策指引 歐盟物聯網基本安全建議 美國 IoT 設備核心能力基準 我國消費性物聯網產品資安標準
識別功能	● 設備應可以與其他設備區別（實體或邏輯識別符號）	美國 IoT 設備核心能力基準

	● 產品型號及名稱應標示在包括但不限於產品標籤、實體介面，讓使用者能清楚辨識 ● 當產品出於安全為目的將產品唯一識別碼以硬編碼方式儲存，應防止實體或軟體等方式篡改	我國消費性物聯網產品資安標準
設定功能	設備可以授權用戶更改軟體設定，並具有恢復原廠設置功能	美國 IoT 設備核心能力基準
資料保護	● 設備具有資料保護功能，如加密、設定密碼長度、可以讓其他人無法存取資料，避免資料被竄改，保持資料完整性和機密性 ● 產品持久性儲存器(persistent storage)中的敏感性安全參數應加密儲存，或存放於產品的安全區域，從正常作業環境中隔離 ● 產品的關鍵安全參數不應使用於軟體原始碼 ● 敏感資料在傳輸過程中應加密 ● 盡量不要使用預設密碼 ● 應要求要求用戶更改初始帳號和密碼，且新設密碼必須使用強密碼或個人識別碼等 ● 安全輸入和輸出處理：資料輸入前應經驗證、輸出應經過濾 ● 產品用於更新及與關聯服務間傳輸所使用之關鍵安全參數應具唯一性	美國 IoT 設備核心能力基準 英國消費性物聯網資安實踐準則 歐盟物聯網基本安全建議 我國消費性物聯網產品資安標準
網路傳輸	● 產品之安全傳輸應使用符合國際標準要求或公認之資安產業慣例之最佳傳輸加密技術 ● 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道 ● 產品所有之網路與安全功能於交付前宜通過審查(review)或評估(evaluate) ● 產品之密碼演算法及密碼基元	歐盟物聯網基本安全建議 英國消費性物聯網資安實踐準則 我國消費性物聯網產品資安標準

	(cryptographic primitives)宜可被更新，或產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限 ● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 應驗證通過用戶界面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料 ● 產品之身分認證因子傳輸應加密傳輸	
介面連接和存取	● 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份認證機制、帳號啟用和禁用） ● 存取產品資源前，宜透過身分鑑別機制 ● 變更產品安全相關設定之功能應具備身分認證機制 ● 產品宜支援硬體等級的記憶體存取控制機制 ● 注意介面安全，如單獨設備受到攻擊或威脅，不會影響其他設備 ● 避免所有產品使用相同密鑰；廠商所生產之裝置，其預設通行碼都應相異 ● 當產品採用預設通行碼，通行碼生成機制應足夠隨機 ● 確認設備只有必要端口是公開且可使用	美國 IoT 設備核心能力基準 歐盟物聯網基本安全建議 我國消費性物聯網產品資安標準
紀錄功能	● 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態。狀態訊息可用於其他設備。 ● 當偵測到產品有未經授權的軟體變更時，產品宜向管理者或使用者發出警示 ● 產品所收集之遙測數據宜檢查是否存	美國 IoT 設備核心能力基準 歐盟物聯網基本安全建議 我國消費性物聯網產品資安標準

	在安全異常，以作為監控安全事件之用	
系統彈性	● 設備和系統應具備彈性，可因應網路斷線和停電等中斷系統設計時應考慮到中斷可能性，並防止因中斷導致系統產生不可逆的損害 ● 產品宜在網路中斷時仍可保持本地端運作，且在網路恢復後，產品能回復正常運作 ● 產品宜具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線	美國 IoT 設備核心能力基準 歐盟物聯網基本安全建議 我國消費性物聯網產品資安標準
操作指南	● 設備安裝和維護步驟應最小化，便利後續使用和維護，並提供設備使用指南 ● 廠商宜提供如何檢查產品是否具備安全設置的指南 ● 廠商宜提供產品安全開發說明文件 ● 廠商應提供關鍵安全參數之安全管理程序說明文件	日本智慧住宅資安對策指引 英國消費性物聯網資安實踐準則 我國消費性物聯網產品資安標準

（資料來源：本研究整理）

表 3-7 集合住宅類智慧建築管理面應注意事項

	管理面（組織、人、程序、資料）注意事項	參考規定
政策	建立和維護關鍵網路資產管理（Asset Management）程序及設定控制等政策	歐盟物聯網基本安全建議
政策	應建立風險和威脅識別及評估政策	歐盟物聯網基本安全建議
組織	組織應導入經驗證之解決方案，避免使用某些自定義解決方案	歐盟物聯網基本安全建議
組織、流程	組織應建立分析及掌控安全事件之流程，以及時處理安全漏洞或事件	歐盟物聯網基本安全建議 我國消費性物聯網產品資安標準
組織、人	應培養和訓練員工安全意識	歐盟物聯網基本安全建議
組織、流程	應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等	歐盟物聯網基本安全建議
人	業者、管理單位等應妥當運用、管理系統	日本智慧住宅資安對策指引
流程	業者根據設備操作說明維護和管理設備	日本智慧住宅資安對策指引
流程	業者應遵守相關政策/規定，提供服務和管理系統	日本智慧住宅資安對策指引
流程	● 業者、管理單位應定期監控以驗證設備行為、檢測是否有惡意軟體，並即時採取排除措施	歐盟物聯網基本安全建議

	● 業者提供使用者的產品支援期限聲明應淺顯易懂 針對無法軟體更新之受限制設備產品，廠商宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法	
人	業者應正確設置、設定 IoT 設備和服務	日本智慧住宅資安對策指引
人	管理單位應選擇適合的 IoT 設備	日本智慧住宅資安對策指引
組織	廠商應提供產品之漏洞揭露政策，包括提供聯絡資訊或窗口，以便相關人員回報問題，即時處理發現的弱點	英國消費性物聯網資安實踐準則 我國消費性物聯網產品資安標準
資料	依個資法規定處理個人資料 個人資料應可以刪除	英國消費性物聯網資安實踐準則
資料	監控來自 IoT 設備之遙測資料	英國消費性物聯網資安實踐準則
流程	● 所有設備和服務都應遵循最小化原則，產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需 ● 確保產品執行所需之特權控制與廠商所宣告的一致	英國消費性物聯網資安實踐準則 我國消費性物聯網產品資安標準

（資料來源：本研究整理）

本報告以表 3-2 至表 3-5 所分析之我國集合住宅類智慧建築弱點為基礎，比較上述各國注意事項和規範，從避免因弱點產生資安威脅及意外事件角度出發，整理對應之規範如下表 3-8：

表 3-8 集合住宅類智慧建築弱點及對應之注意事項

弱點	對應之注意事項	
IoT 設備資安功能未徹底安裝，或未即時更新軟體	功能面	● IoT 設備/系統應有默認安全和隱私功能 ● 軟體可透過空中下載（Over-the-Air, OTA）、遠端或本地工具更新，且更新時不影響設備功能。如更新時會中斷產品功能，宜於更新前告知使用者 ● 更新之軟體應不包含敏感資料且經加密 ● 軟體更新應使用安全機制進行驗證，確保軟體真實性和完整性（設備應鑑別更新伺服器身分之真實性，且應於更新檔傳輸過程中確認真實性與完整性） ● 可以決定是否啟用更新功能，或將更新功能改為手動 ● 可以限制軟體更新權限 ● 軟體更新後可恢復到前一版本 ● 設備宜以清楚識別的方式通知使用者進行更新 ● 產品所有之網路與安全功能於交付前宜通過審查(review)或評估(evaluate) ● 產品之密碼演算法及密碼基元(cryptographic primitives)宜可被更新，或產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限
	管理面	● 管理單位應選擇適合的 IoT 設備 ● 業者應正確設置、設定 IoT 設備和服務 ● 業者應遵守相關政策/規定，提供服務和系統 ● 業者根據設備操作說明維護和管理設備 ● 業者和管理單位應妥當運用、管理設備和系統 ● 廠商提供使用者的產品支援期限聲明應淺顯易懂 ● 無法軟體更新之受限制設備產品，廠商宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法 ● 業者宜提供產品安全開發說明文件
IoT 設備安全性（safty）不足	功能面	● 設備應考慮實體安全性（safety） ● 設備應支援安全啟動（Secure boot）機制 ● 設備之使用者介面應驗證輸入的語法和內容 ● 設備應可以與其他設備區別，產品型號及名稱應標示

		在包括但不限於產品標籤、實體介面，讓使用者能清楚辨識 ● 當設備出於安全為目的將產品唯一識別碼以硬編碼方式儲存，應防止實體或軟體等方式篡改 ● 設備和系統應具備彈性，可因應網路斷線和停電等中斷，並防止因中斷導致系統產生不可逆的損害 ● 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態
	管理面	● 管理單位應選擇適合的 IoT 設備 ● 業者根據設備操作說明維護和管理設備 ● 業者宜提供如何檢查產品是否具備安全設置的指南 ● 業者宜提供產品安全開發說明文件
IoT 設備與其他設備連接時，其他設備或系統資安功能不足或未即時更新軟體；設備安全性（safty）不足	功能面	● IoT 設備/系統應有默認安全和隱私功能 ● 軟體可透過空中下載（Over-the-Air, OTA）、遠端或本地工具更新，且更新時不影響設備功能 ● 更新之軟體應不包含敏感資料且經加密 ● 軟體更新應使用安全機制進行驗證，確保軟體完整性 ● 可以決定是否啟用更新功能，或將更新功能改為手動 ● 可以限制軟體更新權限；軟體更新後可恢復到前一版本 ● 設備應考慮實體安全性（safety） ● 存取產品資源前，宜透過身分鑑別機制 ● 變更產品安全相關設定之功能應具備身分認證機制 ● 設備應可以與其他設備區別 ● 設備和系統應具備彈性，可因應網路斷線和停電等中斷，並防止因中斷導致系統產生不可逆的損害 ● 設備宜在網路中斷時仍可保持本地端運作，且在網路恢復後，產品能回復正常運作 ● 設備宜具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線 ● 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態 ● 確保產品執行所需之特權控制與廠商所宣告的一致

	管理面	● 管理單位應選擇適合的 IoT 設備 ● 業者和管理單位應妥當運用、管理設備和系統 ● 業者應正確設置、設定 IoT 設備和服務 ● 業者應遵守相關政策/規定，提供服務和系統 ● 業者應根據設備操作說明維護和管理設備 ● 業者宜提供如何檢查產品是否具備安全設置的指南 ● 業者提供使用者的產品支援期限聲明應淺顯易懂 ● 針對無法軟體更新之受限制設備產品，廠商宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法
IoT 設備允許經許可以外之管理終端裝置操作、設定	功能面	● IoT 設備/系統應有默認安全和隱私功能 ● 可以限制軟體更新權限 ● 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態 ● 設備具有資料保護功能，如加密、設定密碼長度、可以讓其他人無法存取資料，避免資料被竄改，保持資料完整性和機密性 ● 產品持久性儲存器(persistent storage)中的敏感性安全參數應加密儲存，或存放於產品的安全區域，從正常作業環境中隔離 ● 產品的關鍵安全參數不應使用於軟體原始碼 ● IoT 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用） ● 避免所有 IoT 設備使用相同密鑰；廠商所生產之裝置，其預設通行碼都應相異；當產品採用預設通行碼，通行碼生成機制應足夠隨機 ● 確認 IoT 設備只有必要端口是公開且可使用 ● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 產品之安全傳輸應使用符合國際標準要求或公認之資安產業慣例之最佳傳輸加密技術 ● 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道
	管理面	● 管理單位應培養和訓練員工安全意識 ● 業者和管理單位應妥當運用、管理設備和系統 ● 業者應正確設置、設定 IoT 設備和服務 ● 業者應遵守相關政策/規定，提供服務和系統

		● 業者根據設備操作說明維護和管理設備 ● 所有設備和服務都應遵循最小化原則,產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需
未注意到病毒感染或被以不正方式連結，繼續利用 IoT 設備	功能面	● IoT 設備/系統應有默認安全和隱私功能
	管理面	● 管理單位應培養和訓練員工安全意識 ● 業者和管理單位應妥當運用、管理設備和系統
IoT 設備無法順利執行或被執行弱點對策	功能面	● 設備和系統應具備彈性，可因應網路斷線和停電等中斷，並防止因中斷導致系統產生不可逆的損害 ● 設備宜在網路中斷時仍可保持本地端運作，且在網路恢復後，產品能回復正常運作 ● 設備宜具備保持連線穩定與功能正常運作之能力 ● 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態 ● 當偵測到產品有未經授權的軟體變更時，產品宜向管理者或使用者發出警示 ● 設備所收集之遙測數據宜檢查是否存在安全異常，以作為監控安全事件之用
	管理面	● 管理單位應建立分析及掌控安全事件之流程，以管理安全漏洞或事件 ● 管理單位應培養和訓練員工安全意識 ● 業者和管理單位應妥當運用、管理系統 ● 業者和管理單位應定期監控以驗證設備行為，檢測是否有惡意軟體，並即時採取排除措施 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 廠商應提供產品之漏洞揭露政策，包括提供聯絡資訊或窗口,以便相關人員回報問題,即時處理發現的弱點 ● 所有設備和服務都應遵循最小化原則，產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需
IoT 設備未依	功能面	● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 產品之安全傳輸應使用符合國際標準要求或公認之資

照預定用途、用法進行設置和運用		安產業慣例之最佳傳輸加密技術 ● 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道 ● 應驗證通過用戶介面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料 ● 產品之身分認證因子傳輸應加密傳輸 ● 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用） ● 避免所有產品使用相同密鑰;廠商所生產之裝置,其預設通行碼都應相異,當產品採用預設通行碼,通行碼生成機制應足夠隨機 ● 如設備單獨受到攻擊或威脅，不會影響其他設備 ● 設備可以授權用戶更改軟體設定，並具有恢復原廠設置功能
	管理面	● 業者和管理單位應妥當運用、管理系統 ● 業者應正確設置、設定 IoT 設備和服務 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者應根據設備操作說明維護和管理設備 ● 所有設備和服務都應遵循最小化原則，產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需
與集合住宅內部網路連結之 IoT 設備以外之設備，及與住家內網路連結之 IoT 設備以外之設備，未依照預定用途、用法進行設置和運用	功能面	● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 應驗證通過用戶介面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料 ● 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用） ● 避免所有 IoT 設備使用相同密鑰;廠商所生產之裝置,其預設通行碼都應相異,當產品採用預設通行碼,通行碼生成機制應足夠隨機 ● 如設備單獨受到攻擊或威脅，不會影響其他設備 ● 確認設備只有必要端口是公開且可使用 ● 設備可以授權用戶更改軟體設定，並具有恢復原廠設置功能
	管理面	● 業者和管理單位應妥當運用、管理系統 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者應根據設備操作說明維護和管理設備

		● 所有設備和服務都應遵循最小化原則，如關閉沒有使用的通訊埠等
集合住宅住戶IoT 設備以外之設備，及與內部網路連結之 IoT 設備以外之設備，沒有使其連結廣域網路進行管理		● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 應驗證通過用戶介面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料 ● 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用） ● 避免所有產品使用相同密鑰;廠商所生產之裝置,其預設通行碼都應相異;當產品採用預設通行碼,通行碼生成機制應足夠隨機 ● 如設備單獨受到攻擊或威脅，不會影響其他設備 ● 確認設備只有必要端口是公開且可使用
	管理面	● 業者、管理單位等應妥當運用、管理系統 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者應根據設備操作說明維護和管理設備 ● 所有設備和服務都應遵循最小化原則，產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需
更換或廢棄IoT設備、智慧化服務系統等時，未確認是否有刪除資料或採取其他防止資料再利用措施	功能面	● 設備安裝和維護步驟應最小化,便利後續使用和維護,並提供設備使用指南
	管理面	● 業者和管理單位應妥當運用、管理系統 ● 業者應根據設備操作說明維護和管理設備 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者或管理單位應依個資法規定蒐集、處理、利用個人資料 ● 業者或管理單位應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等
遠距管理系統之管理端，保留設備設定資料及個資	功能面	● IoT 設備/系統應有默認安全和隱私功能 ● 確保網路傳輸和儲存之完整性、機密性和真實性 ● 應驗證通過用戶介面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料 ● 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用） ● 避免所有產品使用相同密鑰;廠商所生產之裝置,其預設通行碼都應相異;當產品採用預設通行碼,通行碼生

		成機制應足夠隨機 ● 產品所收集之遙測數據宜檢查是否存在安全異常，以作為監控安全事件之用 ● 確認設備只有必要端口是公開且可使用
	管理面	● 管理單位應培養和訓練員工安全意識 ● 業者和管理單位應妥當運用、管理系統 ● 業者應根據設備操作說明維護和管理設備 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者或管理單位應依個資法規定蒐集、處理、利用個人資料 ● 業者或管理單位應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等 ● 業者或管理單位應監控來自 IoT 設備之遙測資料
缺乏針對支援服務和維修時使用之設備，進行更換和廢棄之手續，或未依照手續採取一定措施	功能面	● 設備安裝和維護步驟應最小化，便利後續使用和維護，並提供設備使用指南
	管理面	● 業者和管理單位應妥當運用、管理系統 ● 業者應遵守相關政策/規定，提供服務和管理系統 ● 業者應根據設備操作說明維護和管理設備 ● 業者宜提供如何檢查產品是否具備安全設置的指南 ● 業者宜提供產品安全開發說明文件 ● 業者應提供關鍵安全參數之安全管理程序說明文件
使用智慧化服務時，未說明資料管理政策	功能面	無
	管理面	● 業者應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等 ● 業者應遵守相關政策/規定，提供服務和管理系統
未提供住戶服務及 IoT 設備相關政策，或未依照政策使用設備或提供服務	功能面	無
	管理面	● 管理單位應建立分析及掌控安全事件之流程，以管理安全漏洞或事件 ● 業者應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等 ● 業者應遵守相關政策/規定，提供服務和管理系統

（資料來源：本研究整理）

在完成上述比較及整理後，本報告將根據上述表格，分別從功能面和管理面歸納我國集合住宅類智慧建築導入資通訊安全應用設備之注意事項：

壹、 功能面

一、 資訊安全

（一） IoT 設備/系統應有默認安全和隱私功能。

（二） IoT 設備具有資料保護功能，如加密、設定密碼長度、可以讓其他人無法存取資料，避免資料被竄改，保持資料完整性和機密性。

（三） 產品持久性儲存器（persistent storage）中的敏感性安全參數應加密儲存，或存放於產品的安全區域，從正常作業環境中隔離。

（四） 產品的關鍵安全參數不應使用於軟體原始碼。

（五） 避免所有 IoT 設備使用相同密鑰；廠商所生產之裝置，其預設通行碼都應相異當產品採用預設通行碼，通行碼生成機制應足夠隨機。

二、 軟體更新

（一） 軟體可透過空中下載（Over-the-Air, OTA）、遠端或本地工具更新，且更新時不影響設備功能；如更新時會中斷產品功能，宜於更新前告知使用者。

（二） 更新之軟體應不包含敏感資料且經加密。

（三） 軟體更新應使用安全機制進行驗證（如鑑別更新伺服器身分之真實性），確保軟體真實性與完整性。

（四） 當偵測到有未經授權的軟體變更時，宜向管理者或使用者發出警示。

（五） 用戶可以決定是否啟用軟體更新功能，或將更新功能改為手動。

（六） 設備可以限制誰具有軟體更新權限

（七） 軟體更新後可恢復到前一版本。

（八） 設備宜以清楚可識別的方式，通知使用者進行更新。

（九） 產品所有之網路與安全功能於交付前宜通過審查（review）或評估（evaluate）。

（十） 產品之密碼演算法及密碼基元（cryptographic primitives）宜可被更新；產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限。

三、 實體安全

（一） IoT 設備應考慮實體安全性（safety）。

（二） IoT 設備應支援安全啟動（Secure boot）機制。

（三） IoT 設備之使用者介面應驗證輸入的語法和內容。

（四） IoT 設備應可以與其他設備區別（具識別性），產品型號及名稱應標示在包括但不限於產品標籤、實體介面，讓使用者能清楚辨識。

（五） 當設備出於安全為目的，將產品唯一識別碼以硬編碼方式儲存，應防止被以實體或軟體等方式篡改。

四、 軟硬體設定

（一） IoT 設備和系統應具備彈性，可因應網路斷線和停電等中斷，並防止因中斷導致系統產生不可逆的損害（系統彈性）。

（二） IoT 設備宜具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線等。

（三） IoT 設備具有可紀錄和報告設備狀態之功能，可限制只有特定人才能查詢設備狀態，並防止其他人編輯狀態（紀錄功能）。

（四） IoT 設備可以授權用戶更改軟體設定，並具有恢復原廠設置功能。

（五） IoT 設備具有可控制存取權限之能力（如禁止本地或網路存取、身份驗證、帳號啟用和禁用）。存取產品資源前，宜透過身分鑑別機制；變更產品安全相關設定之功能應具備身分認證機制。

（六） 確認 IoT 設備只有必要端口是公開且可使用。

（七） 避免所有 IoT 設備使用相同密鑰，如設備單獨受到攻擊或威脅，不會影響其他設備。

五、 網路傳輸

（一） 確保網路傳輸和儲存之完整性、機密性和真實性。

（二） 應驗證通過用戶介面或 API 輸入的資料，或在服務和設備網路之間傳輸的資料。

（三） 產品之安全傳輸應使用符合國際標準要求或公認之資安產業慣例之最佳傳輸加密技術。

（四） 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道。

六、 其他

（一） 所有設備和服務都應遵循最小化原則，產品啟用之網路埠與網路服務、實體介面、軟體服務、原始碼等應為廠商提供必要服務之所需提供 IoT 設備使用指南、產品安全開發說明文件、檢查產品是否具備安全設置指南等文件。

貳、 管理面

一、 業者及管理單位共通事項

（一） 業者和管理單位應妥當運用、管理設備和系統。

（二） 業者和管理單位應定期監控以驗證設備行為，檢測是否有惡意軟體，並即時採取排除措施。

（三） 所有設備和服務都應遵循最小化原則，如關閉沒有使用的通訊埠等。

（四） 業者或管理單位應依個資法規定蒐集、處理、利用個人資料。

（五） 業者或管理單位應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等。

（六） 業者或管理單位應監控來自 IoT 設備之遙測資料。

二、 管理單位

（一） 管理單位應建立分析及掌控安全事件之流程，以管理安全漏洞或事件。

（二） 管理單位應選擇適合的 IoT 設備。

（三） 管理單位應培養和訓練員工安全意識。

三、 業者

（一） 業者應制定涉及第三方資料之處理、顧客資料之共享等資料應用規範，以及供應鏈之風險管理政策等。

（二） 業者應正確設置、設定 IoT 設備和服務。

（三） 業者應遵守相關政策/規定，提供服務和系統。

（四） 業者應根據設備操作說明維護和管理設備。

（五） 廠商應提供產品之漏洞揭露政策，包括提供聯絡資訊或窗口，以便相關人員回報問題，即時處理發現的弱點。

（六） 業者應以淺顯易懂方式聲明產品支援期限；無法軟體更新之受限制設備產品，業者宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法。

第四章 結論與建議

第一節 結論

本報告依據規劃時程，完成訪談大綱之研擬和訪談行程。迄今為止，研究團隊已經拜訪台北市政府都市發展局、台灣資通產業標準協會、台灣物業管理學會、台灣智慧建築協會和建伸智慧綠建築公司，就（1）可以透過哪些方式確保集合住宅類智慧建築之安全性，如在硬體方面，要求相關設備符合特定規範或規格（如取得資安標章）；在人員和程序方面，要求管理單位建立 SOP 或人員需要取得證照等；（2）我國目前只有針對特定設備之標準，為何會缺乏針對物聯網或以建築物整體為對象之資安檢測標準或規範；（3）未來注意事項是否有可能結合智慧建築指標及導入方式.....等議題，請教專家意見，並依照期中審查委員意見，將訪談結果獨立整理於「第二章第一節參、深度訪談重點」。

本報告於期中前已經完成我國集合住宅類智慧建築定義、發展狀況及資訊安全相關規範之整理與初步分析，期末報告則全面性盤點我國可能涉及資訊安全和個資之法律和命令（第二章第二節壹、我國資訊安全及個人資料相關法令盤點），並整理成表格，然後再從中找出可能與智慧建築有關之法令。

由於資訊安全很難由正面或負面表列安全或不安全之行為，而《資通安全管理法》亦是從程序面進行規範，透過要求公務機關或特定非公務機關遵守一定程序來控管風險，故《資訊安全管理法》及相關辦法雖為我國主要資安法規，但非本計畫所要研析之對象。此外，雖然資訊安全措施是否完善，可能會影響到個資是否洩漏，但個資或隱私並不等同於資訊安全，故個資法亦非本計畫主要研究對象。我國目前並無在法律或命令層級，針對智慧建築之資訊安全加以規範，惟內政部建築研究所為推動國內智慧建築之發展，於 2003 年訂定智慧標章制度，分別從綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等八大指標評估智慧建築。上述指標並未將資訊安全列為評估項目之一，雖然細究各別項目，部份項目已經涵蓋資訊安全概念，但對於申請者而言，這些內容可能仍然不夠明確，故本報告蒐集並整理日本、美國、歐盟及英國規範，將其作為研擬我國集合住宅類智慧建築導入資通訊安全應用注意事項之參

考。

本報告已於期中完成蒐集日本、美國、歐盟和英國等國家和地區，有關智慧建築或資通訊安全應用之法制規定，發現由於資通訊或聯網設備種類及態樣廣泛，故相關文件首先都會釐清適用對象和範圍，以利後續設想可能發生之意外事件，作為分析潛在威脅和風險之基礎。其次，各國在研擬相關規範時，日本從功能面和管理面出發，依序針對各利害關係人分別提出建議；歐盟則將建議分為「政策」、「組織、人員和流程措施」、「技術措施」3 類，而本報告進行訪談時，亦有專家認為可軟硬體面和程序面（包含人員管理在內）著手研擬注意事項。

本報告依據上述研究成果，並參酌臺灣資通產業標準協會所制定之「消費性物聯網產品資安標準」及「物聯網場域資安防護評估指引」，根據本研究對於集合住宅類智慧建築之定義、發展狀況及國外法制調查整理等，於期末報告第三章提出我國集合住宅類智慧建築資訊安全應用情境，整理我國集合住宅類智慧建築架構及主要智慧化項目，以及各項智慧化服務可能涉及之利害關係人，並從功能面及管理面出發，分析我國集合住宅類智慧建築之可能發生之意外事件、資安威脅及弱點。最後，本報告針對我國集合住宅類智慧建築可能存在之弱點，比對各國針對智慧住宅或聯網設備提出之規範，研提我國集合住宅類智慧建築導入資通訊安全應用注意事項。

第二節 建議

針對本計畫所進行之研究與分析，研提立即可行建議及長期建議如下：

建議一

加強我國智慧建築資訊安全之規範：立即可行建議

主辦機關：內政部建築研究所

協辦機關：財團法人資訊工業策進會

智慧建築為未來 5G 網路和物聯網之主要應用場域之一，內政部建築研究所自 2004 年建立候選智慧建築證書及智慧建築標章制度，目前智慧建築標章評估之八項指標：綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新，並未將資訊安全列為指標之一，雖具體評估內容中部份已納入資訊安全概念，如資訊通信指標之基本項目「2.3 區域網域」，其評估內容包括「適當的資訊安全保障設備」等，但仍應進一步檢視及精進，且有關資訊安全之評估內容散落在各項指標當中，故應有討

論是否將資訊安全列為獨立評估指標，以及指標應包含之評估項目及具體評估內容等事項之必要。

本計畫已於 110 年度調查國外有關智慧建築和物聯網相關之規定，未來可以上述法制調查結果和國內現況為基礎，檢視我國智慧建築標章內有關資訊安全之規定，並提出評估指標、評估項目及內容之調整建議。

建議二

強化公寓大廈管理服務人員資安意識與能力：中長期建議

主辦機關：內政部營建署

協辦機關：內政部建築研究所

集合住宅類智慧建築之資訊安全有賴於管理面執行與落實，管理單位必須選用合適之 IoT 設備，並建立資訊安全政策或標準作業流程，遵照一定程序選購、使用、管理、維護和更新、廢棄相關設備或系統，且管理人員亦須具備一定之資訊安全意識與能力，針對意外事件能即時應對處理，方能有效確保集合住宅類智慧建築之資訊安全。基於上述理由，建議未來主管機關可研擬是否加強公寓大廈管理服務人員之訓練，將資訊安全科目納入《公寓大廈管理服務人員管理辦法》第 20 條之管理服務人員訓練課程。

附錄一：「集合住宅類智慧建築資通訊安全應用之法制規定調查研究」委託研究計畫案審查意見及廠商回應一覽表

項次	審查委員意見（依發言順序）	廠商回應
1	1. 研究主題為物聯網對建物及居住空間所扮演關鍵角色，並整合智慧化居住空間以及帶動經銷發展為目標。其中研究團隊對於目前台灣建物智慧化及空間面向對物聯網台灣發展現況是否掌握，納入此研究之結果內容。 2. 研究人員皆為法律背景，但針對研究目標之建物、居住空間以及智慧建築如何了解現況與進行？ 3. 過去已有「智慧建築安全監控法則」，本研究計畫針對「集合住宅為對象」，請補充說明「台灣集合住宅對象現況發展」並納入研究結果。 4. 預期成果如何落實物聯網實際應用之具體說明。國外皆以「報告」、「原則」、「對策」「指引」，本研究以應用之「注意事項」是否具體？請補充改進說明。	1. 研究團隊將參酌委員意見，將我國建物智慧化及物聯網發展現況納入研究內容。 2. 謝謝委員垂詢，由於研究團隊均為法律背景，故本計畫將透過訪談和舉辦座談會等方式，請益建物、居住空間及智慧建築等領域專家意見。 3. 研究團隊將參酌委員意見，於確定承接本計畫後，在研究報告內補充說明「台灣集合住宅對象現況發展」並納入研究結果。 4. 謝謝委員垂詢，服務建議書係因配合本案需求說明書而使用「注意事項」。研究團隊最終所繳交之成果會配合委託單位需求。
2	1. 服務建議書中人事費，第 2 頁 458,200 元與第 13 頁 433,200 元不一致。	1. 謝謝委員垂詢，服務建議書第 2 頁人事費為研究費和座談會出席費之總和，433,200 元為人事

	2. 服務建議書第 13 頁在本計畫內工作月數 12 應改為 10 個月。 3. 服務建議書第 16 頁研究進度表 12 個月應改為 10 個月。 4. 研究團隊鄧佩琳，職稱副研究員，學歷為師範學院初等教育系是否有符合團隊需求。 5. 透過台灣智慧建築協會中協調挑選合適業者。	費中之研究費。 2. 服務建議書內人事費之工作月數，於確定承接本計畫後，將依照實際執行月數調整。 3. 服務建議書內之研究進度，於確定承接本計畫後，將依照實際執行月數調整。 4. 鄧珮琳副研究員於本案負責行政管理；因其工作年資較長，故於本案職稱為副研究員。 5. 謝謝委員建議，研究團隊將聯繫台灣智慧建築協會，以利挑選合適業者進行訪談。
3	1. 109 年有智慧建築安全監控法則課題研究，然今年課題針對智慧建築資通訊安全建議宜有 2011，2016 年版推動智慧建築熟悉人員。 2. 智慧建築資通訊全未來宜包括監控系統、監控人員、法則化項目、規範內容予以進行。 3. 研究目的之(一)國外相關資料、案例可增加國內之瞭解。可透過國內實際案例瞭解予以進行。 4. 預期助益中有提及可降代智慧建築導入相關應用之風險，或許可調整說法。	1. 謝謝委員建議，研究團隊將透過訪談和舉辦座談會等方式，請益熟悉 2011，2016 年版智慧建築標章專家之意見。 2. 研究團隊將參酌委員建議，規劃注意事項內容。 3. 謝謝委員建議，研究團隊將透過訪談和舉辦座談會等方式，蒐集國內案例。 4. 謝謝委員建議，研究團隊會調整服務建議書用語，避免使用較為負面之詞彙。

	1. 本案應與進行智慧建築相關保全業者、物業管理業及共住宅或社會住宅管理單位訪談。針對所要、所需擬取資料。如何在隱私保護下能夠放心取得數據進行分析應用。 2. 有關國際資安法治觀測有哪些實際項目，建議加強。歐盟GDPR、APEC、CBPR 之比較說明以利廠商向外推動輸出。 3. 此外相關新興資訊技術如區塊鏈與國內正在制訂之標準亦應加強探討。 4. 人力部分應與貴會如多媒體、資通所等跨部門合作，瞭解政府推動建築數位轉型的高度需求。能夠了解本所推動目的。	1. 謝謝委員建議，研究團隊將透過訪談和舉辦座談會等方式，拜訪智慧建築相關保全業者、物業管理業及共住宅或社會住宅管理單位等，俾使研究成果符合委託單位需求。 2. 謝謝委員建議，於確定承接本計畫後，研究團隊會加強有關國際資安法制觀測之說明，以及歐盟GDPR、APEC、CBPR 之比較說明，以利國內廠商向外輸出。 3. 謝謝委員建議，研究團隊將參酌委員意見，將新興資訊技術與國內智慧家庭技術標準等納入研究內容。 4. 謝謝委員建議，研究團隊會加強與本會其他部門之合作，補強研究團隊主要人員均為法律背景之不足。

附錄二：「集合住宅類智慧建築資通訊安全應用之法制規定調查研究」委託研究計畫案期中審查意見及廠商意見回覆表

委員	審查委員意見	執行團隊意見回覆說明
1.朱教授曉萍	1. 期中報告已針對各國集合住宅類智慧建築資通訊安全應用之法制規定進行資料蒐集，但以陳述國外的制度作法為主，較未見國內相關制度與國外作法之對應比較，宜予調整。 2. 簡報檔對於研究進行的邏輯與脈絡說明較為清晰，可考慮將其納入期中報告內容。尤其是期中研究成果第三章的陳述過於簡略，應將主要成果及目前的建議重新整理納入。 3. 訪談紀錄之日期誤植為 109 年，應予修正。	1. 謝謝委員建議，關於國內制度與國外作法之比較，會於期末報告內加以補充。 2. 謝謝委員建議，期末報告會將期中審查會議簡報內容納入，並補充主要成果及建議。 3. 謝謝委員建議，訪談紀錄日期誤植等問題，將於期末報告內統一修正。
2.何教授明錦	1. 本研究相關主題已邁入第二或第三年的研究，資訊及隱私安全確為智慧建築導入 AIoT 等相關資通訊技術應用的重要課題。 2. 期中報告對美國、日本、英國、歐盟等國家或地區的系統性的安全指導原則措施均有所收集分析，值得肯	1. 謝謝委員肯定。 2. 謝謝委員肯定。

委員	審查委員意見	執行團隊意見回覆說明
	定。	
	3. 期中簡報歸納已界定的使用對象範圍主要以智慧住宅為主，也分別考慮獨棟與集合住宅的聯網及可能涉及的利害關係人，並將針對互聯網的主要風險弱點和漏洞加以分類及提出解決對策，尤其在相對應的既有法規應用或制修訂，若有具體成效，對智慧建築尤其住宅類之資通訊安全應用更有保障，建議成果應更為深入具體，而非僅止於注意事項草案。	3. 謝謝委員肯定，本年度計畫要求為提出注意事項草案，研究團隊會再思考如何深化研究成果，為我國現行法規提供建議。
	4. 研究方向及目標均非常正確，但實質的成果應在期末報告展現，才能夠真正達成目標。	4. 謝謝委員建議，研究團隊會於期末報告內提出具體建議。
3.周董事長光宙	1. 本研究蒐集國內外智慧建築資通訊安全相關法規或標準，並藉由業界訪談了解我國集合式住宅型態之現況需求，後續成果值得期待。	1. 謝謝委員肯定。
	2. 現階段著重於意見蒐集與文獻回顧，尚未明確描述未來「導入資通訊安全應用之	2. 謝謝委員建議，研究團隊將於期末報告內補充說明注

委員	審查委員意見	執行團隊意見回覆說明
	注意事項草案」之架構，建請補充說明。	意事項草案規劃架構及內容。
	3. 由於集合住宅類智慧建築規模不一，例如有/無管理委員會、社會住宅、無人化管理住宅等需求均不一致，建議後續擬定注意事項時，可分別針對適用對象設定不同應用情境，並據以擬訂因應對策。	3. 謝謝委員建議，研究團隊於規劃注意事項草案時，將參酌不同集合住宅需求，針對不同應用情境研擬因應對策。
	4. 期中報告 P.6 圖 2-1「既有集合住宅導入智慧化檢討架構」解析度較差無法辨識內容，建請予以修正。	4. 謝謝委員建議，關於圖片解析度等問題，將於期末報告內統一修正。
4. 梁教授漢溪	1. 現有法規之整理，建議從法規面先予以區分，如設備、系統、管理、個資等加以探討期中報告 P.18-P.19 之內容。	1. 感謝委員的建議，由於目前我國並未於法規層面規範智慧建築，故期中報告內僅探討智慧建築標章。研究團隊會於期末報告盤點集合住宅有關設備、管理、保全等相關法規，以及智慧建築標章內有關資安部份。至於個資及資安法，目前我國個資法和資安法規範對象為公務機關和非公務機關，而資安法所規範之非公務機關為關鍵基礎設施，一般集合式住宅應非資安法規範
	2. 智慧建築中有關資安之相關內容應先釐清運作狀況。	
	3. 訪談部份針對資安問題，建議整理及未來進行方向。	

委員	審查委員意見	執行團隊意見回覆說明
		對象。 2. 感謝委員的建議，有關智慧建築內資安之運作狀況，研究團隊會再透過訪談等方式進一步了解。 3. 感謝委員建議，針對訪談紀錄，會再進一部整理並摘要重點。
5.廖建築師慧燕	1. 本研究蒐集美國、日本及歐盟相關資料，並綜整分析後提出之對策及分類，針對本研究之研究標的進行分析，值得肯定。惟本研究探討法制面，並未進行國內相關法令之蒐集分析，建議應增加國內相關法令，並說明本研究在相關法令架構之層級與關係，以臻完整。 2. 本研究題目為法制規定，但是目前提出未來研究後將提出「注意事項」，請問到底未來之成果其與相關法令之關係為何，提供給誰使用，建議應該於報告中說明清楚。 3. 究竟目前國內集合住宅之資安風險為何？個資外洩、	1. 謝謝委員建議，研究團隊將於期末報告內補充國內法制之分析，以及本研究在相關法令架構之層級與關係。 2. 謝謝委員建議，惟本計畫僅為法制規定調查研究，計畫目標為透過調查國內外相關規定，提出注意事項草案，並非針對法律或命令層級之法規提出立法或修正建議。 3. 謝謝委員建議，資安風險可能包括硬體面，如設備故障；或管理面，如人員管理不當、操作錯誤等問題。研究團隊將於期末報告內依據集合住宅類智慧建築之應用情境，歸納各種潛在資安風險和威脅，以研提因應

委員	審查委員意見	執行團隊意見回覆說明
	駭客或是硬體故障等軟硬體的問題，建議以文獻蒐集及訪談方式調查分析後，提出應該包括軟硬體之注意事項，且為免造成規模小的集合住宅對於資安之需求不同，建議依據報告中提出之分級機制，區分提出哪些為最基本要求的核心項目，哪些是可達到提升安全的選擇性項目。	對策。
	4. 為了解國內目前集合住宅之資安風險，以對症下藥，建議加強實務面之訪查，目前或因疫情關係做的不多，建議應就所欲了解之問題，包括不同規模之集合住宅等（以配合報告中所謂分級制）先規劃訪查對象，盡可能完整掌握國內目前資安風險問題，與未來如何落實加強資安之可行性，建議可考量以獨立章節說明調查之設計、訪談重點與歸納分析之結果	4. 謝謝委員建議，研究團隊將於下半年度加強訪談規劃，並於期末報告內以專章或專節分析訪談結果。
6.練協理文旭	1. 建議於報告中提醒建築具備聯網功能的設施，需符合各項資安法規。	1. 謝謝委員建議，研究團隊將於期末報告內補充說明。

委員	審查委員意見	執行團隊意見回覆說明
	2. 除 TAICS 現有 ZP-COM、CVR、NVR，無線路由器等有明確規範外，目前正研訂「消費性物聯網資安規範」及「門禁系統資安規範」，建議可一併參考。	2. 謝謝委員建議，研究團隊將參考現正研訂之規範，作為研擬注意事項之參考。
	3. 本研究相關成果可提醒業主及設計規劃者，作為要求各設備商、整合商需提供產品及設備系統漏洞更新機制之參考。	3. 謝謝委員建議，研究團隊將以業主、設計規劃者、設備商、整合商等利害關係人為對象，規劃注意事項之內容，以利提供參考。
	4. 除基本防火牆外，宜建議及提醒各系統應提供網路、網頁、網站等弱點掃描報告(不得申請中、高階以上風險)。	4. 謝謝委員建議，研究團隊會將提供弱點掃描報告等要求，納入注意事項草案。
7.劉理事長國隆	1. 資安的探討建議分三個部份來考量。 (1) 對外資訊的傳輸方式：a.傳輸線 b.wifi(無線)。 (2) 內部資料管理的資安設定等級如何明確化。 (3) 設備損壞、電力中斷、傳統式的安全控管方式。a.資安替代方案的建構 b.網路、電力穩定性的資安處理方式？	1. 感謝委員的建議，研究團隊將納入作為研擬注意事項之參考。

委員	審查委員意見	執行團隊意見回覆說明
	2. 內部資安的控管方式請研究外包、資安人員、資訊使用、弱點分析等，另期中報告 P.35 第 5 行在建造工程不宜加入資安驗收的程序，建議加註在使用執照取得前，應在物聯網或物管公司選定後，再核發智慧標章。 3. 建議能訪談各縣市政府社會住宅之主管單位，並將訪談的內容與回饋問題，提出應對之方向。 4. 期中報告中 P.59 訪談臺北市都市發展局時，使用主管單位提出維運成本很高，如何使其規格符合我們的需求，而讓使用管理單位能夠繼續使用智慧建築的設備，建請提出補充說明。	2. 感謝委員的建議，研究團隊將納入作為研擬注意事項之參考。 3. 4. 感謝委員的建議，研究團隊將於疫情緩和後，規劃於下半年進行訪談。 5. 感謝委員的建議，研究團隊將於期末報告內，針對如何平衡導入智慧化設備與維運成本進行補充說明。
台灣物業管理學會(林監事世俊)	1. 智慧建築資通訊安全應用著重應變、減災政策、計畫、驗證、實施管理等。 2. 智慧建築資通訊安全資料著重安全等級分類、屬性分類、備份等級分類等，併請納入期末階段分析參考。	1. 謝謝委員建議，研究團隊將納入作為研擬注意事項之參考。 2. 謝謝委員建議，研究團隊將納入作為研擬注意事項之參考。
財團法人	1. 建議後續可針對集合住宅	1. 謝謝委員建議，研究團隊將

委員	審查委員意見	執行團隊意見回覆說明
台灣建築中心(江專案經理友直)	類建築分別擬訂公、私領域之資通訊安全利用注意事項，以利各管理單位參考。 2. 建議後續可訪談不同類型及規模之集合住宅類建築物管理操作人員或所有權人，以進一步了解實際執行難處並據以分析擬定後續對策。 3. 建議將期中報告 P.24 表 2-4 標題欄位設定跨頁重複出現，以利閱讀。	作為後續研究方向之參考。 2. 感謝委員的建議，研究團隊將於疫情緩和後，規劃於下半年挑選適合對象進行訪談。 3. 謝謝委員建議，關於報告格式等問題，將於期末報告內統一修正。
羅組長時麒	1. 本研究除蒐集國際智慧建築資通訊安全應用法規外，建議釐清國內資安相關法令之層級，以利智慧建築導入 IoT 時，能夠了解需遵循哪些法令規定。	1. 謝謝委員建議，研究團隊將於期末報告內補充國內資安法規，以利智慧建築導入 IoT 時參考依循。

附錄三：「集合住宅類智慧建築資通訊安全應用之法制規定調查研究」委託研究計畫案期末審查意見及廠商意見回覆表

委員	審查委員意見	執行團隊意見回覆說明
1.朱教授曉萍	1. 注意事項草案之內容和面向皆已完成，惟尚未能依正式文件之格式呈現，建議於最終報告中提出。 2. 國內外作法的比較，建議能以一頁式圖表予以對照整理，可以更清楚了解各自的重點及差異。	1. 謝謝委員建議，執行團隊將於成果報告中調整草案呈現方式。 2. 謝謝委員建議，執行團隊將於成果報告中新增國內外法規對照表。
2.周董事長光宙	1. 本研究完整提出集合住宅在相關系統法條導入應用時，所涉及到資安各層面之影響及相關風險評估，並分析國內外相對應的法規應用參考，完全符合預期研究成果。 2. 建議請依本研究成果基礎，研議後續研究項目作為本研究延續性之應用目標。 3. 建議於智慧建築標章手冊改版內容時，將相關系統設備，應用 Iot 技術服務可導入資安應注意或鼓勵之項目。	1. 謝謝委員肯定。 2. 謝謝委員肯定。 3. 謝謝委員建議，執行團隊已於本年度與台灣智慧建築協會就智慧建築標章手冊有關資安項目進行討論。
3.梁教授漢溪	1. 從功能與管理層面探討相關風險，涉及層面廣，如何得到最有效之分類，可再加以考量，且如何結合法條，可作為後續研究參考。 2. 我國資安相關法令整理相當多，如何歸納到智慧建築後續研究可再進行，以利智慧建築推動之安全。 3. 建議事項，可再明確些如公	1. 謝謝委員肯定，執行團隊將規劃後續深化研究成果，將項目進行更細緻的分類。 2. 謝謝委員建議，關於我國資安法令該如何與智慧建築扣合，可作為後續深入研究主軸。 3. 謝謝委員建議，本年度僅初

	寓大廈管理服務人員管理辦法，可能不僅人員訓練課程，實質規範事項亦相當重要。	步提出注意事項草案，執行團隊將思考如何深化各項內容，使注意事項草案更加具體且可操作。
4.練協理文旭	1. 國外文獻詳實，惟對國內文獻部分，雖無完整建築資安，但對於智慧建築主要項目，如門禁、影像監控、空氣品質、無線路由器、行動 APP 等已有 CNS 或經濟部推動中之資安標準。建議有國家 CNS 標準者(如 CNS16120)或有資安標章者(如 APP)，政策上應列為必要要求。如尚無檢測機構，可量整個標準、供利害關係人尊循參考。 2. 分級部分，不宜以案場規模分級，建議以風險、安全需求及可負擔性考量。 3. BA 或需端管理平台，建議應出具公正第三方網路、網站(頁)弱點掃描報告(不得出現中、高風險)。 4. 無特定資安標準之聯網設施，建議提醒符合“消費性物聯網資安標準”。	1. 謝謝委員建議，執行團隊將於成果報告中補充國內文獻，並參考 CNS 或經濟部推動中之資安標準。 2. 執行團隊將參酌委員建議及注意事項草案定位，進一步思考如何進行分級。 3. 執行團隊將參酌委員意見，於注意事項草案中適度納入相關建議。
5.劉理事長國隆	1. 資通訊安全應用之法則：同意應加強對資料處理人員、樓管人員的加強訓練。 2. 資通訊安全應用方面，應於收集資料之時即思考未來資料運用時如何合於個人資料保護法的規範。建議未來資通訊安全應用需加以納入考量。 3. 各縣市主管單位對資通訊安全應用反應的彙整如此	1. 謝謝委員肯定。 2. 謝謝委員建議與肯定。執行團隊目前所提出之注意事項草案，已將遵守個人資料保護法相關規定納入。

	即可協助，台灣法治規定的考量。	
6.財團法人台灣建築中心(連組長俊傑)	1. 本研究完整提出集合住宅在相關系統設備導入住宅應用時，所涉及到資通訊安全各層面之影響及相關風險評估，並分析國內外相對應的法規應用參考，符合預期研究成果。 2. 為增加本研究成果應用性，建議可於應注意事項草案中補充相關名詞解釋或範例說明，如敏感資料之定義、何謂「實體安全性」…等，以利非專業者參考運用。	1. 謝謝委員肯定。 2. 謝謝委員建議，執行團隊後續將考慮針對專有名詞，於注意事項草案內新增名詞解釋。

附錄四：建伸智慧綠建築公司訪談紀錄

一、 建伸智慧綠建築公司訪談紀錄

（一） 會議資訊

會議時間：110 年 03 月 18 日 10：00 至 11：00

會議地點：建伸智慧綠建築公司

受訪談人：黃健偉總經理

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：我國集合住宅類智慧建築現況與導入資通訊設備之注意事項

（二） 訪談提綱

1. 內政部建築研究所 104 年「既有建築物智慧化改善之研究-以集合住宅為例」研究報告，曾根據智慧建築評估手冊，建議建築物導入之智慧化項目，並指出由於集合住宅規模不一，在導入智慧化設備時往往會依照住戶需求，優先導入節能或安全相關設備，惟「系統整合」仍是智慧化關鍵。**請教黃總經理我國集合住宅智慧化發展狀況，以及主要導入之智慧化設備。**

   （1） 承上，智慧化或聯網設備可能有安全性疑慮，**請問目前可以透過哪些方式來確保集合住宅智慧化之安全性？如在硬體方面，可能在驗收時要求相關設備符合特定規範或規格（如取得資安標章）；在人員和程序方面，要求管理單位建立 SOP 等。**

2. 日本國土交通省「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン）草案，設想智慧建築內所遭遇之實體及虛擬風險，如人員未善盡保密義務或

未遵守 SOP、硬體設備未定時維修、遭受網路攻擊等，並從管理面（組織、人、程序）和功能面（系統、資料、機器）盤點可能遭遇之風險及弱點，針對上述風險及弱點，參考國內外相關規範，針對 IoT 業者、服務提供者、服務供應者等，提出導入/提供相關設備或服務時之注意事項。**研究團隊擬參考日本作法和我國現況，針對集合住宅導入資通訊應用研議注意事項。針對集合住宅類智慧建築內可能遭遇之資安風險、應考慮之規範項目，以及可以參考之國內外法規（含標準）等，請教黃總經理之建議。**

3. 我國目前針對智慧建築有智慧建築標章，分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等指標，缺乏資訊安全指標；智慧建築評估手冊中所列智慧建築評估項目亦無資訊安全項目。**請教黃總經理當時規劃智慧建築標章指標及評估項目之想法，以及未來是否或有可能將資訊安全納入指標或評估項目？**

4. 承上，如不適合將資訊安全納入智慧建築標章指標或評估項目，針對集合住宅可能導入之聯網或智慧化設備，台灣資通產業標準協會（TAICS）針對物聯網產品，已發布：IP CAM 資安標準與測試規範、無線網路攝影機資通安全檢測技術指引、無線區域網路接取設備及路由設備資通安全檢測技術指引、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、智慧巴士資通訊系統系列資安標準與測試規範，並建立物聯網資安標章。**未來是否可能將上述資安標準或認證驗機制納入智慧建築標章或相關法規，如建議在指標內新增導入之設備必須取得資安認證？**

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，本次訪談希望能了解（1）我國集合住宅導入資通訊安全應用之現況；（2）國內外資通訊安全應用相關法制規定，作為研提我國集合住宅類智慧建築導

入相關應用注意事項之參考。首先請教黃總經理當初智慧建築標章為何沒有資安指標，以及目前集合住宅類智慧建築狀況。

2. 黃總經理：現行智慧建築標章之「設施管理指標」鼓勵項目，4.4 維運管理鼓勵訂定智慧化設施設備危機處理與緊急應變計畫，後者內容包括資安、當機、駭客入侵等，故雖然智慧建築標章沒有獨立之資安指標，但其實早已將資安納入，只是目前僅作為鼓勵加分項目。

3. 黃總經理接著說明集合住宅內較關注之資安問題：針對住戶隱私，最常討論的是監視器問題，由於建築物內監視器是長時錄影，住戶出入時間都會被記錄下來；此外，門禁系統也會紀錄住戶進出時間，可由此得知住戶的日常行動軌跡。由於住戶可能會在意上述問題，故以現在的系統架構來看，所有建築物都不連外網，所以不太會被駭客入侵，故問題比較可能發生在管理面，如有人複製檔案等。另外，從開發業者和使用者角度出發，我們也很重視個人信箱的隱私問題，避免他人偷拆信或信件投錯等狀況發生。我們公司幫台北市政府做老舊社區之智慧化改造，主要就遭遇到上述問題，所以我們會針對信箱進行設計，改採電子信箱。

4. 周晨蕙研究員：請問當初在設計智慧建築標章時，為何會將資安放到設施管理指標的鼓勵項目？由於鼓勵項目是針對制定應變計畫，則針對硬體的部份，未來是否有可能考慮結合物聯網標章或其他針對設備之規範和智慧建築標章？如要求所導入之聯網設備應取得物聯網標章。

5. 黃總經理：目前智慧建築標章只鼓勵申請人制定相關計畫，而在制定應變計畫後，未來管委會或管理公司是否能落實也是一個問題，故在資安方面還有很多努力空間。硬體設備主要規範在智慧建築標章之系統整合指標，可能可以將取得物聯網標章或符合其他標準作為鼓勵得分項目，但若列為基本項目，業者可能很難在這一項拿到分數，不利於鼓勵業者創新。

6. 周晨蕙研究員：請教黃總經理，目前智慧家庭內導入資通訊設備的狀況，以及在訂定注意事項之前，有哪些問題需要先釐清？

7. 黃總經理：目前有在發展智慧家庭的業者，如 Google、amazon 和小米所開發之設備，都可以連外網，這樣後續才可以提供更多加值服務，只有 Apple 注意到資安問題，使用藍芽進行連接，未來研擬注意事項，可以建議安全等級高之住宅使用藍芽設備，避免資安風險。由於現在擔心資安問題，所以建築物大都只能連內網，但這樣一來會限制後續發展。另外，還需注意設備位置問題，如監視器擺放位置是對著住家拍，還是對外拍？拍攝公共區域還是走廊？由於監視器都是長時攝影，可以持續紀錄，所以需要注意上述問題。一般而言，社區的防護重點是由內而外，避免私人空間（住宅）被外人入侵；根據我們接觸民眾經驗，多數民眾在意的是鄰近環境的安全，擔心有外人進來社區、網路被攻擊等，由於集合住宅資料的商業價值低，所以集合住宅的重點在於保護住戶的隱私，故監視器設置的位置或監控重點不會針對內部，住宅內部的資訊量通常較少。

8. 黃總經理繼續分享：過去認為理想的智慧建築應是一個大型的偵測站，可以蒐集和共享資料，但現在因為害怕資料外洩所以都封閉起來，對物聯網產業也有很大影響。有鑑於此，我認為政府未來應協助釐清資料等級，以促進建築物互聯。如停車/瓦斯/求救/氣溫/空氣品質等資料，存取權限設定可以比較低，門禁和監視器資料的存取權限要設定較高，儲存期限較長，同時需要求進行異地備份。

9. 周晨蕙研究員：由於集合住宅規模不一，許多小型社區可能沒有請保全，只能靠住戶自己管理，故想要求小規模住宅採取跟大型社區相同的資安對策可能有所困難。針對小型社區之資安，黃總經理有何建議？

10. 黃總經理：除限制設備是否可以連外網及設置位置外，針對硬

體設備進行定期測試和進行人員教育訓練，設定存取權限（如規定只有總幹事才能存取資料）等都十分重要。小型住宅雖然較缺乏人力，但住戶自己管理不一定比較不安全。針對小型住宅，我認為管理重點在於要求資料需要進行備份，甚至要求異地備援；而大型社區由於是交給物業管理，所以重點在於人員管理。

11. 周晨蕙研究員：針對硬體設備之注意事項，如果不建議要求業主應取得標章或符合特定標準，怎樣在注意事項內規範會比較好？

12. 黃總經理：針對硬體設備，可以考慮在注意事項內要求特定設備需具備之功能，如要求在存取資料時可以反向紀錄等。綜言之，注意事項大約分成硬體設備和管理兩大面向，前者可以規範設備應具有哪些功能（如限制使用藍芽、具備反向紀錄功能等）、設置位置，以及需要定期檢測等；後者則制定作業流程和規範，如設定存取權限、定期教育訓練等。

13. 黃總經理繼續針對資料防護功能分享看法：一般住宅主要都是擔心住戶個資外洩，尤其是社會住宅等出租型大樓，會比較重視住戶個資的管理。為落實資料管理，台灣要推動的是將資料存在自己的伺服器或私有雲，近 5-10 年的新建築物其實都有預留空間存放伺服器，由於建築物內部資料量不大，不需要很大的伺服器，所以老舊建築物也可以將伺服器放在 DV 箱上，老舊建築物的問題是佈線改善。

14. 資策會科法所感謝黃總經理寶貴的經驗分享。

附錄五：台灣資通產業標準協會訪談紀錄

一、 台灣資通產業標準協會訪談紀錄

（一） 會議資訊

會議時間：110 年 03 月 18 日 10：00 至 11：00

會議地點：台灣資通產業標準協會

受訪談人：陳曉強資深顧問

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：我國物聯網設備資安標準及標章現況及結合集合住宅類智慧建築之可行性

（二） 訪談提綱

1. 我國目前針對智慧建築有智慧建築標章，分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等指標，缺乏資訊安全指標；智慧建築評估手冊中所列智慧建築評估項目內（參下表），亦無資訊安全項目。基於上述理由，目前若要討論智慧建築之資訊安全，是否僅能從智慧建築內所導入之設備出發，看特定設備是否符合資安標準或取得標章？

2. 承上，台灣資通產業標準協會（TAICS）針對物聯網產品，已發布之資安相關規範包括：IP CAM 資安標準與測試規範、無線網路攝影機資通安全檢測技術指引、無線區域網路接取設備及路由設備資通安全檢測技術指引、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、智慧巴士資通訊系統系列資安標準與測試規範等，上開部份針對特定設備之規範，或可作為檢視智慧建築資安之標準，惟有以下問題想請教 TAICS 意見：

（1） 目前我國係針對物聯網設備研擬檢測標準和規範，並為落實檢測制度制定物聯網資安認驗證制度規章，惟上述制度係針對產品，若從建築觀點出發，上開制度恐難涵蓋所有面向。僅針對產品制定標準並進行認驗證，是否有何特殊考量？

（2） 承上，從建築角度出發，研擬針對整棟建築物之資通設備資安檢測標準或規範，必須克服哪些問題？如需要先釐清規範對象和可能產生之安全風險等。

（3） 針對我國物聯網設備之資安標準或認證驗機制納入智慧建築標章，如建議在指標內新增導入之設備必須取得資安認證，請教 TAICS 看法。

3. 日本國土交通省「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン）草案，設想智慧建築內所遭遇之實體及虛擬風險，如人員未善盡保密義務或未遵守 SOP、硬體設備未定時維修、遭受網路攻擊等，並從管理面（組織、人、程序）和功能面（系統、資料、機器）盤點可能遭遇之風險及弱點，針對上述風險及弱點，參考國內外相關規範，針對 IoT 業者、服務提供者、服務供應者等，提出導入/提供相關設備或服務時之注意事項。研究團隊擬參考日本作法，研擬我國集合住宅類智慧建築導入資通訊安全應用注意事項。針對智慧建築內可能遭遇之資安風險、應考慮之規範項目，以及可以參考之國內外法規（含標準）等，請教 TAICS 之建議。

4. TAICS 技術工作委員會今年起推動制定智慧建築資通訊標準，作為日後建築興建時期所需之資通訊整合規範及驗收準則。智慧建築資通訊標準預計產出「智慧建築能源管理資料格式標準」、「安全監控系統資料格式標準」和「智慧建築設施管理系統資料格式標準」。

（1） 上述預計產出仍是針對特定系統制定之資料格式標準。由此觀之，鑑於智慧建築可能涵蓋面向甚廣，針對特定設備或系統制定標準，或許是較好的作法。未來 TAICS 是否可能規劃進一步針對智慧建築制定資安標準或規範？

（2） 根據內政部建築研究所「既有建築物智慧化改善之研究-以集合住宅為例」研究報告，建議建築物導入之智慧化項目如下圖所示。由於集合住宅規模不一，在導入智慧化設備時往往會依照住戶需求，優先導入節能或安全相關設備，惟「系統整合」仍是智慧化關鍵。從上述建議導入項目和需求出發，如後續要針對智慧建築內導入之設備或系統等制定資安標準，可能規範對象為何？

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，本次訪談希望能了解（1）我國集合住宅導入資通訊安全應用之現況；（2）國內外資通訊安全應用相關法制規定，作為研提我國集合住宅類智慧建築導入相關應用注意事項之參考。首先想請問台灣資通產業標準協會（以下簡稱 TAICS），目前所制定之資安標準為何大多針對特定設備？是否針對智慧建築（場域）制定標準有所困難？

2. 陳曉強資深顧問：台灣資通產業標準協會（以下簡稱 TAICS）主要因應政府各部會需求推動資訊安全，而各部會在推動資安時會比較關注業務職掌相關的設備，加上監控系統涉及隱私、個資外洩等風險，故 TAICS 目前所制定之資安標準或規範才會聚焦在設備或特定需求（如智慧巴士）上。

3. 陳曉強資深顧問繼續說明：TAICS 之前是由下而上制定相關標準，現在正規劃由上而下的資安指引，將每一個獨立個體，如將集合住宅、醫院等視為一個系統，建立一個模型，以這個模型分析系統風險和評估可能弱點，進行滲透性或破壞性測試

攻擊系統，以評估系統的安全能力並分級，看使用者需求適用不同等級。在制定上述指引後，可能會有人因此質疑由下而上制定的標準沒有意義，但如果我們要求整個系統應達到 2 級，結果系統內所使用的設備只有 1 級，這樣最後整體可能還是無法達到 2 級。目前 TAICS 所制定的個別標準，如果能夠作為採購驗收之標準，可以作為拼圖的一部份，日後只要補足目前沒有標準，或針對系統特性需特別處理的部份。針對聯網設備，TAICS 也希望日後可以慢慢補足相關標準，或透過制定一般性原則來規範。TAICS 目前擬規劃物聯網通用標準，未來可適用特定標準之設備（如 IP Camera）就適用特定標準，沒有的就可以適用通用標準。透過由下到上和由上到下制定標準，就可以將整體串連在一起。

4. 周晨蕙研究員：以現況而言，由於目前智慧建築標章並無資安指標，為確保智慧建築之資訊安全，未來是否有結合智慧建築標章/候選證書和物聯網資安標章之可能？如要求未來欲取得標章或證書之建築物所使用之設備，必須取得物聯網資安標準？

5. 陳曉強資深顧問：TAICS 技術工作委員會之 TC7 為「智慧建築資通訊」，聚焦於智慧建築之設施管理、系統整合等議題，有關資訊安全部份則係由 TC5「網路與資訊安全」討論。針對智慧建築，TC7 主席溫琇玲老師曾提出系統相互之間連結有資安問題；此外，針對個別系統，目前監控設備已經有資安標準，業主可以依照需求和資安等級選用相應設備，問題可能較小，但針對建築物內其他系統（如門禁系統），仍然缺乏相應規範。綜觀國際資安標準，主要分成針對系統進行管理（如 ISO27001）和針對硬體裝置/軟體運作加以規範之兩大體系，沒有任何一個國際標準能兩者兼顧，而目前協會所提供之標準，亦大多是針對實體進行規範。根據上述說明，針對監控設備，若智慧建築要求導入之設備必須符合 TAICS 所制定之標準應無問題；針對一般資訊管控，如防火、門禁系統之資料，

或許可以參照既有國際標準進行管理，這部份 TAICS 不會另外訂定。

6. 周晨蕙研究員：鑑於智慧建築內還有很多設備並未制定資安標準，未來如要繼續完善物聯網資訊安全，可能針對哪些設備制定標準？

7. 陳曉強資深顧問：TAICS 比較關注 IP camera 等設備，一來是配合政府單位需求，二來亦是回應產業需求。智慧建築內無論是門禁系統、智慧停車、防火系統等都有資安需求，但以 TAICS 立場，我們比較不會主動制定標準，還是要受到政府或民間委託。上述聯網設備，廣義來看都是感測器，如前所述，TAICS 今年預定發布可以適用於所有感測器之物聯網資安標準，不管這些感測器具體功能為何，其所應具備之資訊安全都是一樣的。由此觀之，不能說沒有針對某個設備制定標準，只是要確認是否有適用之標準，以及其適用範圍是否包含特定設備；如果特定設備不完全適用該標準，再檢討是否根據該設備之特性，新增相應規範。

8. 陳曉強資深顧問進一步提到智慧停車發展趨勢：公有停車場越來越少，釋放私有停車場是未來趨勢，但老建築無法提供相關資訊（如是否有空車位）。集合住宅白天住戶出門上班，就可以將空車位租借給上班族停車。如果以後針對智慧停車制定標準，未來亦可直接導入集合住宅。

9. 周晨蕙研究員：由於本計畫目的是調查國內外相關法制規定，作為研擬注意事項之參考，故想請問陳顧問可以參考哪些規定，以及研擬注意事項時應考量之重點。

10. 陳曉強資深顧問：從地域來看，必須先從美國和歐盟開始蒐集相關法規，其他國家或地區大多也是遵循美國和歐盟標準，故可優先關注美國和歐盟規定；至於標準的結構，如前所述，主要分成規範硬體（產品）和系統（如 ISO27001），但最終兩者還是要結合在一起。另外在進行驗證時，由於專業不同，很難

針對管理進行驗證，所以一般都是要求管理系統要符合特定標準，以及每個裝備必須取得特定標章等，並檢視申請驗證者所提供資料是否符合聲明。綜上所述，在規劃注意事項時，應分別針對業主本身，以及業主對於供應商的管理/驗收程序進行規範。

11. 周晨蕙研究員：簡言之，一方面可從業主在管理上是否有制定並遵守 SOP、是否有對人員進行訓練；另一方面，則從業主向供應商所採購之硬體設備是否符合特定標準出發，研議注意事項內容。最後請教陳顧問，集合住宅規模大小不一，對於小規模集合住宅而言，想要落實資安防護可能有所困難，該如何解決這個問題？

12. 陳曉強資深顧問：資安最容易有漏洞的地方是人，硬體要求只能盡量降低人為風險，資安本身沒有完美，重點只在於我們是否能夠承擔風險。集合住宅可以透過分級加以控管，小規模集合住宅或老式公寓可能沒有資安需求，不用負擔額外的成本，所以注意事項內亦可將分級概念納入。

13. 資策會科法所感謝陳曉強資深顧問寶貴之經驗分享。

附錄六：物業管理學會訪談紀錄

一、 台灣物業管理學會訪談紀錄

（一） 會議資訊

會議時間：110 年 03 月 23 日 15：00 至 16：00

會議地點：台灣物業管理學會

受訪談人：林世俊常務監事

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：從物業管理角度看集合住宅之資安注意事項

（二） 訪談提綱

1. 內政部建築研究所 104 年「既有建築物智慧化改善之研究-以集合住宅為例」研究報告，曾根據智慧建築評估手冊，建議建築物導入之智慧化項目，並指出由於集合住宅規模不一，在導入智慧化設備時往往會依照住戶需求，優先導入節能或安全相關設備，惟「系統整合」仍是智慧化關鍵。**請教我國集合住宅智慧化發展狀況，以及主要導入之智慧化設備。**

   （1） 承上，智慧化或聯網設備可能有安全性疑慮，**請問目前可以透過哪些方式來確保集合住宅智慧化之安全性？如在硬體方面，可能在驗收時要求相關設備符合特定規範或規格（如取得資安標章）；在人員和程序方面，要求管理單位建立 SOP 等。**

2. 日本國土交通省「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン）草案，設想智慧建築內所遭遇之實體及虛擬風險，如人員未善盡保密義務或未遵守 SOP、硬體設備未定時維修、遭受網路攻擊等，並從管

理面（組織、人、程序）和功能面（系統、資料、機器）盤點可能遭遇之風險及弱點，針對上述風險及弱點，參考國內外相關規範，針對 IoT 業者、服務提供者、服務供應者等，提出導入/提供相關設備或服務時之注意事項。**研究團隊擬參考日本作法和我國現況，針對集合住宅導入資通訊應用研議注意事項。請教有關針對集合住宅類智慧建築內可能遭遇之資安風險、應考慮之規範項目，以及可以參考之國內外法規（含標準）之建議。**

（1） 承上，雖然從管理面建立規範為確保資安之重要手段之一，**惟集合住宅規模不一，該如何透過管委會或物業管理來落實相關規範？**

3. 我國目前針對智慧建築有智慧建築標章，分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等指標，缺乏資訊安全指標；智慧建築評估手冊中所列智慧建築評估項目亦無資訊安全項目。**未來注意事項是否有可能納入指標或評估項目，以確保智慧建築之資訊安全？如要將注意事項納入指標，哪些面向可能不適合放入指標（如有關管理面之規範可能難以放在設計建造階段作為指標或評估項目）？**

4. 針對集合住宅可能導入之聯網或智慧化設備，台灣資通產業標準協會（TAICS）針對物聯網產品，已發布：IP CAM 資安標準與測試規範、無線網路攝影機資通安全檢測技術指引、無線區域網路接取設備及路由設備資通安全檢測技術指引、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、智慧巴士資通訊系統系列資安標準與測試規範，並建立物聯網資安標章。**未來是否可能將上述資安標準或認證驗機制納入智慧建築標章或相關法規，如建議在指標內新增導入之設備必須取得資安認證？**

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，本次訪談希望能了解（1）我國集合住宅導入資通訊安全應用之現況;（2）國內外資通訊安全應用相關法制規定,作為研提我國集合住宅類智慧建築導入相關應用注意事項之參考。首先請教林常務監事，我國集合住宅智慧化發展狀況,以及確保集合住宅智慧化設備安全之方式。

2. 林常務監事：目前智慧化或聯網設備皆有裝置網路 Switch+網路 Firewall+網路 Router 之軟硬體，但網路相關設備之互通性差、延展性差、擴展性差、備援性差導致網路安全及性能效益低，故建議就有關每個網路結點的安全及性能效益提昇，必須強化網路管理平台軟體即時更新資安軟體[含 ATP(Advanced Threat Prevention) 及安全分析 SA(Secure Analytics)]，以防止駭客植入惡意程式。其次，就資安硬體方面，可能在驗收時要求相關設備符合特定規範或規格（如取得資安標章），故建議採購資安的軟/硬體必須有資安標章，且在驗收時要求就有每個網路結點(網路 Switch+網路 Firewall+網路 Router)的安全及性能效益進行第三方驗收。最後，在人員和程序方面，應要求管理單位建立 SOP 等，故建議管理單位（如管理委員會）聘用合格資安證照人員（證照等級由政府規定），交給公協會訓練，而程序書（SOP&SMP）由起造人完成及資安第三方驗收合格再發給使用執照，然後在每季進行驗證。

3. 周晨蕙研究員：請問為何由起造人制定管理規範？

4. 林常務監事：因為起造人負責建築物設計、營建和交屋，其中包括系統和設備購買等，所以只有起造人有能力負擔，且管委會、住戶等是消費者，消費者購買之住宅應具備完善的防護功能，而非將資安管理責任轉嫁到消費者身上，要求住戶在購買房屋後，還要另外處理資安問題。此外，未來還可以考慮要求起造人一定要制定相關規範，否則不予核准建照。

5. 周晨蕙研究員：雖然從管理面建立規範為確保資安之重要手

段之一，惟集合住宅規模不一，該如何透過管委會或物業管理來落實相關規範？

6. 林常務監事：若能要求起造人完成前述硬體符合特定規格，以及建立 SOP 等工作，則管理單位日後只要聘用具有合格資安證照人員即可。此外，日後也可以由第三方執行程序書（SOP&SMP）之每委稽核工作，以落實資安管理。實際場域是否落實 SOP 由管委會督導，公協會或法人定期驗證物業管理公司、保全公司等單位是否落實 sop/人員培訓。初期政府推動可以列為補助或獎勵項目，以鼓勵產業發展。如果我們不這樣要求，以後不動產管理業會越來越貶值。

7. 周晨蕙研究員：由於目前智慧建築標章沒有獨立之資安指標，未來注意事項是否有可能納入標章，以確保智慧建築之資訊安全？如要將注意事項納入標章，哪些面向可能不適合放入？

8. 林世俊常務監事：未來就採購資安的軟/硬體必須有資安標章，且在驗收時要求就有每個網路結點(網路 Switch+網路 Firewall+網路 Router)的安全及性能效益進行第三方驗收。相關規定可納入智慧建築標章資訊通信指標之基本需求項目。另外，資安的設備管理面之規範，可由起造人在設計階段申請智慧建築候選證書提送審查。

9. 周晨蕙研究員：將相關要求列為基本項目，是否會影響業界創新和導入資通訊設備之意願？另外，針對人員受訓及取得證照之要求，由於需要目前已在現場工作之保全回訓，是否會額外造成現場負擔？

10. 林世俊常務監事：起造人申請智慧建築證書或標章可以申請容積獎勵，對起造人來講，既然可以享受容積獎勵，自然可以要求它負擔一定成本。另外，一般保全其實不會接觸後台，所以需要管理的是後台管理人員或總幹事，故要驗證的對象亦是委外廠商或物管公司，不會影響到現場和第一線保全。

11. 周晨蕙研究員：在其他訪談中，有專家建議可針對集合住宅資

料之保存方式、期間，以及是否需要異地備援等進行規範，就此請教林常務監事建議。

12. 林世俊常務監事：聯網或智慧化設備之資料量龐大要確保資料安全必須實施資料動態分流，並以網路管理平台軟體即時更新資安軟體[含 ATP(Advanced Threat Prevention)及安全分析 SA(Secure Analytics)]，以防止駭客植入惡意程式，而且可即時自動阻隔已知惡意程式的 domains&IPS、偵測已知&Zero-Day 的惡意程式、受感染的聯網或智慧化設備被標識並自動更新防禦。此外，為確保資料完整性，防止遭篡改或外洩，須實施資料量異地備援性，並自動警示資料被篡改事件或資料被外洩事件。

13. 林世俊常務監事繼續分享：異地備援未來是一個新的商業模式，集合住宅資料可以委外儲存管理，而為確保相關資料安全，只要針對保全公司或委外單位進行驗證即可。異地備援的重點應在於針對「事件」，如闖空門、安全門被打開等進行儲存，並避免資料被竄改，如此一來，亦可解決資料量龐大問題。另外，監視器平時可以要求平時低畫質錄影，有事件發生時才改高畫素，這樣可以減少 32%資料量，一天下來資料量差 6GB。

14. 林世俊常務監事最後說明建築物智慧化目的：建築物導入智慧化設備，最大的目的在於減低保養、維護和營運費用，是否衍生其他服務是額外的，未來建研所推動既有建築物智慧化改善，可以改從資安著手。

15. 資策會科法所感謝林常務監事寶貴的經驗分享。

附錄七：台北市政府都市發展局訪談紀錄

一、 台北市政府都市發展局訪談紀錄

（一） 會議資訊

會議時間：110 年 04 月 27 日 17：00 至 18：00

會議地點：台北市政府都市發展局

受訪談人：張立人副工程司

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：從社會住宅經驗談集合住宅導入資通訊設備應注意事項

（二） 訪談提綱

1. 我國近年積極推動公共住宅相關政策，為推動公共住宅，台北市政府於 2018 年訂定「台北市政府公共住宅智慧社區建置參考手冊」，說明智慧社區從採購、設計、施工、驗收到營運管理等各階段之原則。「台北市政府公共住宅智慧社區建置參考手冊」在設計階段，依序針對安全防災、資訊通信等六大面向，提出必須建置項目，並將「安全機制和資安防護機制系統」列為「資訊通信」的主要項目之一。由此可知，資安為公共住宅設計時應考量的因素之一，惟從內容觀之，目前主要係要求規劃緊急電源、不斷電系統、系統備援及設置防火牆等，**請問日後是否會考慮透過其他方式來確保集合住宅智慧化之安全性？如在硬體設備方面，可能在驗收時要求相關設備符合特定規範或規格（如取得資安標章）；在軟體方面，要求網路管理平台定期更新及安全分析；在人員和程序方面，要求管理單位建立 SOP，或要求聘用具有相關證照人員等。**

   (1) 針對硬體設備是否要求需符合特定規範或取得標章，有認

為這樣可能會增加廠商負擔，且目前國內尚無通用之物聯網產品資安標準，建議可以在注意事項內描述硬體設備應具備之功能即可；亦有認為可在注意事項內提出硬體設備應符合特定規範或規格，並在驗收時就每個網路結點（網路 Switch+網路 Firewall+網路 Router）的安全及性能效益進行第三方驗收。**針對上述問題，請教都發局從實際經驗來看，如未來要研擬注意事項，比較適合採用何種作法？有明確的標準，是否會比較方便驗收？**

(2) 在軟體和人員、程序之管理等方面，可能需要求制定 SOP 和管理計畫。目前「台北市政府公共住宅智慧社區建置參考手冊」針對物業管理之設計標準，提到應就智慧化設備之管理維護及修繕制定計畫，並規定建築物內之人員服務必需以人機系統提供服務等。**請教未來如需在規劃設計階段制定 SOP 和管理計畫，由誰（如起造人、物業或管委會等）來制定較為合適？如明確要求應定期更新軟體、進行弱點掃描、管理人員必須受訓或取得相關證書等，是否有困難？後續又要如何確保遵守 SOP？**

2. 日本國土交通省「以安心、安全智慧家庭為目標之虛實資安對策指引」（スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン），設想智慧建築內所遭遇之實體及虛擬風險，如人員未善盡保密義務或未遵守 SOP、硬體設備未定時維修、遭受網路攻擊等，並從管理面（組織、人、程序）和功能面（系統、資料、機器）盤點可能遭遇之風險及弱點，針對上述風險及弱點，參考國內外相關規範，針對 IoT 業者、服務提供者、服務供應者等，提出導入/提供相關設備或服務時之注意事項。**研究團隊擬參考日本作法和我國現況，針對集合住宅導入資通訊應用研議注意事項。請教有關針對集合住宅類智慧建築內可能遭遇之資安風險、應考慮之規範項目，以及可以參考之國內外法規（含標準）之建議。「台北市政府公共住宅智慧社區建置參考手冊」有哪些部份可**

納入注意事項？

3. 我國目前針對智慧建築有智慧建築標章，分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等指標，缺乏資訊安全指標；智慧建築評估手冊中所列智慧建築評估項目亦無資訊安全項目。**未來注意事項是否有可能納入指標或評估項目，以確保智慧建築之資訊安全？如要將注意事項納入指標，哪些面向可能不適合放入指標？**

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，本次訪談希望能了解（1）我國集合住宅導入資通訊安全應用之現況；（2）國內外資通訊安全應用相關法制規定，作為研提我國集合住宅類智慧建築導入相關應用注意事項之參考。本研究已經拜訪台灣資通產業標準協會、物業管理學會和智慧建築協會等公協會，由於台北市政府都市發展局近年積極推動資通訊設備導入社會住宅，故想先請教目前社會住宅推動狀況及經驗。

2. 張立人副工程司：關於社會住宅資訊通信設備之設計原則和標準，可以參考台北市政府都發局公布之公共住宅智慧社區建置參考手冊。針對資訊安全之維護，原則上公共住宅係要求個系統之對外網路應統一設置防火牆，若智慧社區有多基地之情形且有網路分別設置之情形，則應於各對外網路接口設置防火牆。

3. 周晨蕙研究員：目前公共住宅在資安方面僅要求設置防火牆，未來是否可能會考慮新增硬體設備應符合特定規格，或要求公宅管理需建立 SOP，以及物管人員需取得證照等要求？

4. 張立人副工程司：目前公宅在資安方面，主要是規定設置防火牆和防毒軟體；硬體方面則有要求設備要有電腦機殼鎖，具體設計標準可參考手冊內容。由於公宅目前是採用功能驗收方式，所以並未要求廠商一定要採購符合特定規範或標準之設備，而是看該設備或系統是否具有相應功能。

5. 張立人副工程司補充說明：如果要求一定要採購符合特定規格之設備，或要求物業管理人員需具備一定能力，都會增加公宅維運成本。此外，目前公宅所要求之防火牆等級很高，相當於一般企業防護等級，但從公宅建造目的和入住民眾需求來看，公宅的智慧化程度其實不需要這麼高。目前公宅是要求建造應符合智慧建築標章合格級，即便如此維運成本也很高，如果還要再提昇規格，維護管理可能會有問題，所以目前市府考慮的其實是降低規格，以減少日後維護成本。

6. 周晨蕙研究員：剛剛提到維護的問題，請問現在合約是否會要求廠商協助軟體定期更新？

7. 張立人副工程司：合約只要求廠商要負保固責任，目前要求 5 年。無論是硬體設備故障，或是軟體因更新後無法使用，都算在保固的範圍內。但合約不會要求廠商要協助軟體升級，畢竟軟體升級通常都需要另外花錢，所以無法寫在合約內，否則廠商會無法預估成本。

8. 張立人副工程司補充說明：目前公宅遇到最大的問題，其實是公宅住戶以弱勢族群為主，如喑啞人、老人、殘障人士等，太過複雜的 ICT 設備對他們來說反而不會使用，所以公宅應該要依照住戶需求設定不同等級，資安等級也應該隨之調整。目前公宅是採用功能驗收，由於並非所有功能住戶都有使用需求，所以也會要求廠商要設計可以選擇是否使用該功能。如影像辨識功能，公宅管理單位可以關閉該功能，直到住戶都同意蒐集、分析其影像。

9. 周晨蕙研究員：最後請教張副工程司，從北市府建置公宅經驗出發，在導入 ICT 設備時最應注意的問題是什麼？

10. 張立人副工程司：以公宅來講，最重視的都是住宅安全問題，故導入的設備，如空氣品質偵測、緊急求救系統、CCTV、電子圍籬、影像保全等，都是跟安全有關之系統。由於合約能要求之保固期間有限制，不可能一直讓廠商負擔保固責任，所以

系統和設備是否安全可靠，成為最重要的問題。另外，智慧住宅也應注重弱電系統品質，還有配管配線等問題。

11. 周晨蕙研究員：資策會科法所感謝張副工程司寶貴的經驗分享。

附錄八：中國文化大學建築系溫琇玲教授訪談紀錄

一、 台北市政府都市發展局訪談紀錄

（一） 會議資訊

會議時間：110 年 07 月 16 日 10：00 至 11：00

會議地點：線上訪談

受訪談人：溫琇玲教授

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：我國集合住宅類智慧建築現況與導入資通訊設備之注意事項

（二） 訪談提綱

1. 鑑於智慧化或聯網設備可能有安全性疑慮，請問目前可以透過哪些方式來確保集合住宅智慧化之安全性？如在硬體方面，在驗收時要求相關設備符合特定規範或規格(如取得資安標章)；在人員和程序方面，要求管理單位建立 SOP 或人員需要取得證照等。

   （1） 針對硬體設備之資訊安全，目前台灣資通產業標準協會（TAICS）針對物聯網產品，已發布之資安相關規範包括：IP CAM 資安標準與測試規範、無線網路攝影機資通安全檢測技術指引、無線區域網路接取設備及路由設備資通安全檢測技術指引、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、智慧巴士資通訊系統系列資安標準與測試規範等，上述指引或可作為參考。**惟符合指引之設備，價格可能較為昂貴，且一般住宅不一定需要太高等級之資安防護，故訪談時有專家認為毋需於注意事項內明定設備應符合特定規範，僅列出設備應具有哪些功能即可，而美國「IoT 設備資安能力核心基準」便是採取類似作法。就上述想法，請教老師意見。**

（2） 美國「IoT 設備資安能力核心基準」列出六項核心能力：設備識別(Device Identification)、設備設置(Device Configuration)、資料保護(Data Protection)、對介面之訪問(Logical Access to Interfaces)、軟體更新(Software Update)、資安狀態提醒(Cybersecurity State Awareness)。研究團隊考慮於注意事項內建議集合住宅類智慧建築內所導入之設備，應注意是否具備上述能力，且**訪談時有專家具體建議，不僅採購的軟/硬體必須符合特定規格或認證，且在驗收時尚須要求針對每個網路結點(網路 Switch+網路 Firewall+網路 Router)的安全及性能效益進行第三方驗收。就上述想法，請教老師意見。**

（3） 在人員和程序方面，除要求管理單位建立規章、SOP 或規定相關人員必須進行教育訓練等外，**訪談時有專家具體建議，管理單位(如管理委員會)必須聘用合格資安證照人員(證照等級由政府規定)，交給公協會訓練，而程序書(SOP&SMP)可由起造人完成及第三方驗收合格再發給使用執照。就上述想法，請教老師意見。**此外，雖然從管理面建立規範為確保資安之重要手段之一，**惟集合住宅規模不一，該如何透過管委會或物業管理來落實相關規範？**

2. 資料經濟為近年重要趨勢，智慧建築內有大量資料，可作為後續利用之基礎，惟要促進資料流通利用，除透過制定資料標準格式，確保資料互通性外，尚須確保資料品質（可用性）和避免資料被竄改和資料完整性等。**從注意事項角度出發，重點應會放在避免資料被竄改和確保資料完整性，針對建築資料之利用，老師是否還有其他建議？**

3. 我國目前智慧建築標章，分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、節能管理、健康舒適、智慧創新等指標。**未來注意事項研擬完成後，後續是否有可能與智慧建築標章結合，或作為智慧建築標章指標項目調整之參考？**

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，本次訪談希望能了解（1）我國集合住宅導入資通訊安全應用之現況；(2)國內外資通訊安全應用相關法制規定，作為研提我國集合住宅類智慧建築導

入相關應用注意事項之參考。首先請教溫老師，我國集合住宅智慧化發展狀況，以及確保集合住宅智慧化設備安全之方式。

2. 溫琇玲教授：想要確保智慧建築之資訊安全，最快的作法就是要求智慧建築標章符合相應規範，但問題是要如何符合資安規範才能執行與落實。現在修正中之新版智慧建築標章有一個很重要的概念，是從性能/功能出發，研擬指標的評估項目。如果指標內要求建築物所使用之設備應取得特定標章，可能會面臨擁有特定標章之產品不夠多或成本較高等問題；此外，有些設計師想要進行彈性的設計，其所選用的產品可能也不是有節能標章的產品。如果在智慧建築標章內要求使用經認證之產品，一方面可配合政府政策，同時也正面鼓勵業者選用該些產品，大家一起合力推動相關產品發展。

3. 溫琇玲教授延續上面看法：我們可以從情境出發，如果今天要蓋智慧建築大樓，業主需求只有一定要考量資訊安全，但建築物內具體要考量哪些項目，評估手冊是沒有辦法詳細說明的，評估手冊只能就最基本的項目，比較籠統地加以規範，確定智慧建築資安基本核心功能，要求個別產品符合/具備這些功能。但如果是已經建立資安標準之產品（如監視器等），就可以考慮在評估手冊內鼓勵使用這類產品。必須注意是的事，上述標準都非強制性規範。

4. 周晨蕙研究員：未來除可能要求採購的軟/硬體必須符合特定規格或認證外，是否有可能要求由第三方進行驗收，以確保符合標準。就上述想法，請教老師意見。

5. 溫琇玲教授：針對智慧建築之資料格式，我們曾經手過一個案子，該按將資料格式標準寫入招標文件，因為業主不懂無法驗收，所以委請第三方（智慧建築協會）進行驗測。對於智慧建築資訊安全而言，可能有兩個方面來確保，一個是要求使用之產品通過資安驗證（選購合適設備），另一個則是由認證單位發給證照，證明該建築通過資訊安全認證。然而問題在於，就算我們可以針對建築物、設備和人進行認證，但究竟要如何進行認證呢？從國外經驗當中，我國可以學習到哪些作法？首先，從產品、系統、人到機構，所在空間之資訊安全認證，應視規模大小而定；其次，人員資安訓練的內容應包含什麼？課程內容、時數、是否要參訪、考試內容等，可能都要進一步仔

細思考。

6. 周晨蕙研究員：智慧建築會蒐集到很多資料，而資料安全也是資訊安全的一環，新版智慧建築標章會如何處理這一塊，並兼顧資料活用呢？

7. 溫琇玲教授：資料安全並非資訊安全，兩者並非同一個概念，且資料安全還可能涉及個資問題，目前智慧建築評估手冊並未將資料安全納入。智慧建築內應蒐集哪些資料、蒐集後如何應用等等，是未來的重要課題。

8. 周晨蕙研究員：資策會科法所感謝溫教授寶貴的經驗分享。

附錄九：智慧建築安全監控資料應用法制對策問答集座談會

（一）會議資訊

會議時間：110 年 11 月 3 日下午 2 時 00 分至 4 時 00 分

會議地點：內政部建築研究所

與會人員：林谷陶、林煒郁、黃健瑋、王文楷、李政綸、吳榮華、張浤則、張偉倫、盧勝斌、張育偉、練文旭、劉建宗、張裕隆、潘志朋、連俊傑、賴怡伶、周晨蕙、蔡淳宇（職稱略）

記　　錄：蔡淳宇、蘇香榕

（二）會議記錄

1. 內政部建築研究所林谷陶研究員說明今日座談會目的，希望與會各位專家惠賜意見。

2. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理進行引言簡報，本次議題主要報告計畫執行狀況，以及根據訪談結果和參考國外文獻後提出之注意事項草案規劃，並針對草案內容請專家給予建議。

3. 中華民國全國建築師公會林煒郁主任委員

   各位好，針對此議題我一些看法分享給大家。首先，今天討論的主題是一個很新的東西，目前我們國內應該都還沒有相關規範，所以會蒐集日本、歐洲等其他國家相關的研究去做參考。我過去在做一些相關研究案，他們也會做一些案例的參考研究，但最怕的一件事情就是台灣與國外習慣、既有法規、實務執行上不一樣，卻直接把規範複製過來。建議往後如果要參考國外法規，最好還是先看我國民情及實務執行狀況再決定，才不會使得在國外行得通的法規到了台灣卻行不通，因為我國在建築法規上與國外有相當大的落差。

   另外，在制度分級的部分，可能還是要等待以後資料齊備後再進行。

   以上是我簡單的意見，給大家參考，謝謝。

4. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝林主委的建議。很多部份是我們還要再去加強的，因為目前我們進行研究時，大部分還是會先從國外狀況去做了解。國內而言，剛好台灣資通產業標準協會（TAICS）今年也針對物聯網發布相關標準「物聯網應用資安評估指南」(Security assessment guidelines for IoT-enabled field applications)，這部分也是我們應該納入並做補強的。

5. 台灣智慧建築協會黃建偉副執行長

各位好，首先我針對本次資安研究給予讚賞，因為資安議題嚴重影響台灣智慧建築的發展。就我所知目前有部分設備已經在進行資安驗證的工作，剛剛有看到一些注意事項是想探討未來的資訊運用會影響到產業發展，那是不是可以區隔出一個範圍，限制什麼樣的資料可以被直接運用？剛剛看得的某些設備項目，目前廠商已有基本功能，所以現在要做的是比較原則性的注意事項。希望未來可以就此議題持續發展有關資料的運用，例如環境資料中的溫溼度、或是其他資料是可以不受資安法規的控管，因為這些內容會影響到未來資料的取得和應用。

另外一個議題是，關於資安的應用，除了上述提及的設備面，是不是能有類似授權書的部分，授權使用者資料的取得；或者是資料在運用上是不是能有一個法定簽署條款，讓業者和未來集合住宅的住戶有一個使用範疇。因為剛剛我們看到的是有關設備控管的資安，現在其實很多台灣的硬體研發，為了符合國外標準，大致上都有在往這個方向努力。

有關資安設備，建議可以將 IoT 設備做區分，因為不同 IoT 設備差異性極大、面向極廣，所以注意事項的適用範圍可以再做討論，例如 IoT 可能是一個感測器、門禁管制設備、或者監視器，可見其廣度，建議後續可以先鎖定特定設備。

最後，集合住宅類導入資訊、通訊安全後，營運管理者可能會接觸到一些硬體設備的資料。所以在管理面上，或許能有像是保密協定的措施。建議未來營運商要有相關約束文件，否則其取得資料容易，

會拿來做為什麼用途我們不得而知。所以了硬體面外，其實還有許多環節都有資安問題存在。以上是我的初步發言，謝謝。

6. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝黃副執行長給了我們後續研究相當具體的建議。首先針對資料，這部分是科法所不管在建築上、或是其他議題上，一直都有在做討論的。目前資料定性的發展、如何促進資料流通與應用，一直是熱門議題。可惜我國缺乏像是歐盟制定的整體資料政策。在法規方面，國發會研擬中的開放資料專法暫時擱置中，所以我國目前尚無促進資料利用的法規。要如何填補此漏洞，是未來在整個法制方面需要去做努力的。目前開放資料專法還沒有下文的話，針對個別具體領域的資料要如何運用和流通，是我們可以努力的方向。而針對個別具體領域的資料，我們也比較好說明它的價值以及範圍，有很多資料其實和個資無關，像是建築資料，它既跟個資無關也不是所謂的營業秘密，並不會受到營業秘密的保護，這些資料真正的問題是我們沒有去想到它可能是有流通價值的。未來這部分要如何釋出、讓它做更有效的應用是未來我們可以好好研究的方向。在設備面，我們要如何去細緻化注意事項的整體規範？因為目前注意事項確實停留在比較大面向的部分，這也是未來研究可以加強的部分。最後在營運管理面，這次在注意事項當中也有針對管理提出建議，但還是停留在較粗淺的部分，像是建議其提出相關 SOP、組織政策，未來實際在執行時，像是物業要如何跟集合住宅簽訂契約；或是未來我們可以做什麼樣的機制確保營運商可以遵守其自訂的SOP，是不是要有一些驗證機制去確保他們有確實執行、物業管理人員是否有充足的資安素養，未來這整套機制的完善會是非常需要努力的方向。

7. 社團法人台灣物業管理產業協會王文楷理事長

很榮幸能成為此座談會的參與者。針對此議題我提供一些個人看法。不論是從疫情、後疫情時代，隨全球資訊通訊科技發達，我們物業管理從 2004 年就定調了以科技協助管理的一個主軸，只不過台灣近幾十年的發展，勞務歸勞務、科技歸科技，現在終於有一個

整合機會,這是一個很好的研究部署,這裡面也包括了整個不動產、物業管理的環境及消費型態的變革。在此研究下，未來可能帶動不動產產業結合資訊通訊科技的智慧化，這可能會產生新的商業模式。

今天討論的注意事項可能是比較偏向行政指導的性質,剛剛也分析了美國、英國、日本及歐盟的做法，有些是比較概括性的綱要、綱領。我國相關規範未來會像國外一樣制定綱要，或者是延續目前團隊於本研究所擬定的「注意事項」是我第一個問題，可以提供研究團隊思考。

集合住宅既已提到是建築技術規則中分類型態的一個名詞,而去了解整部建築藝術規則，可發現住宅、集合住宅、連棟住宅經常被合體規範，代表其法令整體強度及要求寬鬆。且在技術規則中很清楚的顯示，集合住宅是對三個住宅建築單位，我們會面臨到例如住商共融、住辦共融、住商辦共融，或工業區的建築有些也能容許居住，在此情況下，技術規則只談建築物興建的指導。在建築技術規則裡面，興建完成使用的使用，可能是同一個權利主體大家共同使用，抑或是不同所有權人有共同行為規範並一起使用,那便回到國內公寓大廈管理條例。研究時要注意是否對於法規有所偏解，例如此草案中利害關係人有「起造人」,但當房屋興建完成後我認為裡面還缺少了一個很重要的利害關係人,也就是公寓大廈管理條例所稱的「住戶」。

剛剛聆聽簡報，分為兩個面向，分別是管理面及功能面。而在此兩面向共有九項指標，可能需要整合。不管是哪個面向，其共同追求的都是實體安全。影片裡面提出的實體安全底下的管理面還有使用者、管理單位、業者，透過使用者將資料傳輸到管理單位，管理單位再傳輸到業者，而這中間透過網路的傳輸就存在資訊安全問題。這就回到一開始講的，到底本次要擬定的是實體的注意事項，抑或是上位性的綱領？可以先把智慧化初步定位在門禁保全、緊急呼叫系統、火警監控、環境感測、燈光控制等，在國外研究中，我們也都可看見這些。要整合物聯網，在應用、管理、通訊、感知層面，

這是我們一直以來的研究，大家也做了一個初步整合。就高雄發生的城中城事件可以發現，地方副首長到消防局、工務局之間互相推諉責任，所以未來我們要先跟政府間做層級整合。且不單只是政府行政部門的整合、公用事業的整合。

至於分級方面，我個人覺得可以參考是要用工程規模抑或是經濟規模來談，像是先鎖定固定金額以上的智慧建築，或是回歸到技術規則。以上報告，謝謝。

8. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

非常謝謝理事長給我們的寶貴建議。跟理事長說明一下我們目前所研擬的注意事項還沒有規劃要做出版或是給大家參考的標準，主要是先整理並給主管機關作參考，針對國外法規規定做調查研究。剛剛理事長提及的面向都是我們未來完善整個研究需要注意的，也希望之後有機會與您請教細節。很多目前所遇到的問題都是要做轉型，傳統的物業管理在現在的物聯網時代，在智慧住宅管理甚至人員訓練都會面臨到轉型，需要注意到方方面面複雜的問題，尤其台灣的建築物，講到集合住宅，大家都會先想到的就是一些單純的住戶，但實際上的狀況不見得如此，所以要如何管理會是非常複雜的問題，也都是我們之後要再去更注意的部分。

9. 台北市政府都市發展局張裕隆正工程司

台北市政府都發局在興建社會住宅有一些經驗跟大家分享。簡報及研究中有提及社會住宅有訂立智慧社區參考手冊，針對標章的幾大面向做為未來社宅興建的標準。這次的研究也會使我們日後增列資安這部分。在討論此議題有分應用及管理層面。社會住宅於應用層面，在設定智慧社區資安軟體部份會著重在預防、偵測軟體的設置，以及出現特殊狀況時會有報警機制；硬體方面會設置防火牆，以及在網路的管理措施方面會有一些電子郵件相關的處理，儲存空間會進行密碼保護。在管理層面，機關管理兩萬戶的社會住宅也會建立一個叫做社宅雲的平台，受都發局管理。我們跟資訊局合作，這個管理方面有照市府資安的 SOP。我們在做的 SOP 有七項工作要進

行，分別是系統弱點掃描、網頁弱點掃描、滲透測試、原始碼測試、行動應用程式、資安庫的稽核、資安的建整。因為社宅是由我們委託物業做管理，因此物業公司可能也要做數位轉型，勢必要進行跨領域的整合，必須要操作社宅的語音平台及每個營建廠商所建置的軟硬體設施、資安設備，因此這些也需要做教育訓練。我們每次在點交屋給物業管理業者前都會對於物業管理人員進行教學，也會做教學手冊，甚至把過程錄製成影片以保存教學。以上供大家參考，謝謝。

10. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝張正工程司的分享，北市府在這方面腳步非常快，也在前期幫制度做了非常多的建立與完善。不管是在軟體層面需要有哪些要求、或是管理層面要如何進行。管理面，北市府已經建立了他們的SOP，甚至針對如何去做物業管理人員的教育訓練，都已經有了非常完善的規劃。希望有機會可以再向北市府請教。

11. 中興保全科技股份有限公司練文旭協理

各位先進大家好，此研究中對國外文獻的探討相當完整，但對國內部分較為欠缺，國內雖然沒有智慧建築相關資安標準，但是就智慧建築個個設備例如門禁、監控 APP 等等，經濟部工業局已有很多文獻可以參考。智慧建築其實也就是一個物聯網的資安場域，但台灣資通產業標準協會（TAICS）在今年六月左右，有提出一個物聯網場域資安評估指引，這指引便是可參考之文獻。它針對物聯網場域的威脅部分提了六大項，身分冒用、資料竄改等等，每一個威脅再產生三個威脅情境跟防護，所以這個資料其實相當完整、健全。

剛剛張正工程司也提到台北市標準裡面包含行動 APP，我覺得必須要做一個資安的提醒，但不見得要去訂資安指引，可以參考現有可用部分就好，行動 APP 資安檢測也已經到了第三版，相當完整。

所謂分級不代表其規模大小，而是以它的威脅程度，例如有無密碼、有無使用者身分確認，如果沒有使用者身分確認便是等級一，有則是等級二，如果用到交易和金流就進到等級三，所以我不建議從規

模大小去看，因為在小規模，以國內來講草案已經完成，尤其在 12 月底大概就會推出一版消費性物聯網資安標準。各位可以想像就連消費性物聯網都有資安標準，那裝在住宅裡這麼重要的設備至少也要符合最基礎的標準。比較進階一點的標準，針對智慧建築會用到的設備再去做細分，提醒業者在採用不同子系統時可以要求設備商遵循此標準。另外，門禁系統又分為五大標準，今年 12 月底大概就會完成，建議這塊可以多參考工業局的資料，雖然它是智慧建築的資安，但是其實還是物聯網相關的資安標準，只是用在建築場域而已。

分級部分，最起碼應該普及化，所有的東西都需要符合最基本的要求。但當然也有些需要特別高規格的部分，針對一個廣大的平台服務商，它要去執行網路掃描、滲透測試等等，應該具備這樣的資安水平。資安其實沒有百分之百的安全，特別提醒很多相關業者最重要的是備份，現在很多備份工作都要求管理者執行，但物業管理者和保全其實都相當缺乏這部分的知識，所以應該要求系統整合商做自動化備份會比較理想。我還是建議針對國內既有規範，去萃取關係人比較了解的部分。比如在消費性物聯網資安標準中，有一條「隨系統整合產品的服務商，應該揭露其漏洞政策的對策時間。」意思是我推出一個 A 產品，假設 A 產品未來被通報在漏洞平台上，那廠商應該要有責任跟客戶承諾其在幾天內會對策完畢並提供更新，這時候才有 OTA 軟體更新的程序出來。這其實是一個很完整的流程，但如果沒有去提醒，很多物業管理業者或社區建商，它可能不太懂得去要求服務商，所以應該提醒簽約時，請對方承諾若有漏洞時，多久要更新。這便是我想要求的把深奧專業用句轉成白話。例如針對密碼，預設密碼在國內是普遍現象，應該提醒消費者感變預設密碼。一個很簡單的提醒就能避免掉一大部分的工期，以上簡單的報告，謝謝。

12. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝協理。確實我們目前研究較缺乏國內的部分，我們會再把它補充到整個報告裡面，也將其相關內容統整到草案，讓注意事項整體

更貼近國內狀況。另外在分級概念上謝謝協理的提醒，我們當初的想法比較單純，沒有想到較小的社區可能會連保全都沒有請。分級可能還是要從本身的威脅程度去做處理，謝謝協理的建議。備份部分，注意事項比較沒有去強調這點，但這其實也是非常重要的，可以放到管理面去做比較詳細的規定。

13. 中興保全科技股份有限公司李政綸襄理

各位好，針對現場中看到的實際狀況分享我的經驗。大概 2018 年就有物聯網資安標準，那陣子在一個成果發表會有相關監控廠商參與。在資安標準裡面，一些相關的廠商事實上有很多應用了，但我們所遇到的困難是如何將複雜資安標準的用語，用可以讓現場設備安裝設備廠商人員所理解的方式向他們說明，目前已有的如 CNS12160 標準。

無論是從很重要的門禁系統，或者是對講機系統，又或者已經有在執行的監視系統，能夠讓我們明白如何去執行，我也較好去跟我們身邊的設備廠商去提相關的依循方式。不然像是一般的社宅，我也無法跟他們溝通在這類型的案子你就必須要給我用這類型的產品。有關於相關基準是否可以更加白話可以讓現場人員遵循時更加清楚。這是我遇到的問題，謝謝。

14. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝襄理。這也是實際上比較容易遇到的問題，從法規制定的層面來講，我們其實很難訂的明確，因為過於明確可能導致執行上的困難。但從實務的角度而言，可能會希望訂的明確，在實際執行時才方便跟廠商溝通。我想這是實務面跟法規面比較大的落差，需要我們去弭平。

15. 新光保全股份有限公司盧勝斌經理

跟各位做個報告，集合住宅智慧建築跨越了智慧家庭，甚至到智慧社區、智慧城市，智慧建築裡有許多資訊通訊系統產品，因為其東西多，要整合的東西、相關標準也就多，對系統整合商來說整合風險就較難以掌控。雖然說注意事項的草案裡在功能面上有區分，有

軟體更新、實體安全、軟硬體設定、網路傳輸等等，但是我的想法是我們是否可以建立 ICT 系統相關標準、規範，甚至建立一個共同平台，讓系統整合商有具體的依據去遵循。

16. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝經理，其實實務工作者想要的是具體、清楚的規範，才能使人有所依循。那這部分如何更具體地去規範，我想我們還要去了解更進一步的需求才能有所制定。

17. 良福保全股份有限公司張育偉經理

非常高興認識大家。我們目前在林口社會住宅有 ABC 幾個案場。我們面對比較大的問題是商業智慧系統導入的問題，林口社會住宅四區是四個不同建商所興建，在系統整合上，因為要將四間不同的商業智慧系統整合起來，因此困難會比較大。所以其實社會住宅這部分在國內並沒有明確的規範，從我們目前接觸到社宅資安方面而言，目前良福雖然有 ISO27001 的認證，但是似乎有點難以適用到保全業上面。往往 ISO 相關人員到我們公司稽核，會覺得大家都在不同認知上去規範資訊安全標準。或者我們認為應該更特別的去做處理，但稽核公司卻跟我們抱持不同見解，這是我們目前遇到較難以去做處理的方向。

目前業界一直有針對資安進行更新，但是往往在新舊系統上會有落差，像是保全系統，設備一放就是放好幾年的舊機器，新型機器資安方面可能就比較完整，那系統整合時就會面臨新的缺口。希望未來可以成立一個平台讓業者在進行相關工作的時候能有地方諮詢。以上是我的見解，謝謝。

18. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝張經理，其實系統新舊問題，或是廠商所使用的系統不相同時要如何去整合，對我們而言是非常難以處理的。那在此部分，想跟各位請教，整個建築體壽命非常長，但設備是需要一直換新的，這

些設備的淘汰率高，新產品問世快，其規格可能會不斷改變。為了確保資安，可能設備要一直去做更新，那在實務上這是不是一個比較難做到的事情？是不是我們比較難去要求場域在設備的管理跟維護上面讓管理單位不斷更新？這是我個人會想再跟各位請教的。

19. 安華聯網科技股份有限公司劉建宗研發長

第一點：就我的認知，集合住宅應該會有一些共用的設備或系統，但智慧住宅是每個人在家裡都可以導入智慧設備而建立的，所以它們有一些基本上的差異。如果要論這個議題，應該聚焦在一些比較共用的方面，或者說是在建築過程中就導入的一些資訊系統。以智慧住宅而言，像是一些鄉下的老房子本身也可導入一些資訊系統。目前報告就資安方面蒐集了日本、歐盟、美國，日本參考的部分就比較像是社會住宅。談智慧住宅大家會比較聚焦在物聯網上，像是歐盟、美國就比較會去制定物聯網資安的相關法規。我認為物聯網資安是比較大的議題，如果拿物聯網跟集合住宅的應用情形來看的話，依物聯網的定義，只要連網設備它一開始生產、或是說在銷售之後其整個生命都應該涵蓋。但是集合住宅應該聚焦在「公用」，它的影響也不太一樣。智慧住宅可能針對公用物會有一些影響，但集合住宅它一個外洩可能就會影響到整棟大樓，所以這些標準我個人覺得偏向智慧住宅跟物聯網，較不像是集合住宅的議題。在集合住宅的部分，國際間沒有針對它的相關法規。智慧城市倒是比較多相關資訊，從智慧城市的角度去看的話就會比較多國外的規範、議題可以參考。

第二點：這份報告有談到兩點相當重要。其一，要訂定相關規範，其二是加強人員的資安素養。除了這兩點很重要，資安是與時俱進的，今天安全不代表明天安全，所以持續改善的觀念是要去思考的。像是集合住宅的安全性，它不會是我們今天這個時間點測完它可以它就以後都可以，資安必須是持續性的。怎麼從管理制度去發現問題，改善問題是非常重要的。

第三點：關於分級的部分，「美國國家標準和技術研究院網路安全框架」（NIST CSF）理論上可以適用在各種情境，當然他會比較上

位一點，就會遇到剛剛許多先進提到的，在某個場域它並不能直接解決遇到的問題，這是後續團隊要再努力的。「美國網際網路安全中心關鍵網路安全控制」（CIS Critical Security Controls）目標是協助公司去進行優化，它分為三個類別，分別從小型企業、重型企業、大型企業來看待。也許集合住宅可以從戶數，依據戶數多寡去做分級。

20. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝劉研發長的建議。應如何定義本研究中的智慧建築與聚焦我們這份研究的範圍，並使我們的問題更突顯，方便日後研擬對策，也是未來需要努力的目標。國際間關於智慧城市的相關標準，雖然其層級較高，但也會有一些基礎設備、措施是我們可以參考的，這部份我們也會納入研究。

21. 財團法人台灣建築中心連俊傑組長

各位好。分享一下業務執行上我們會遇到的一些資安議題。在資通訊指標有談到，有關智慧建築要取得標章，會談到網路管理系統及資訊安全保障設備，基於手冊上功能性的評定，其實其強度還是會依照管理者、申請人的使用管理需求為主。所以只要達到功能即可，強度要求並沒有說一定要提高到什麼樣的等級，因此集合住宅可能會較其他住宅的安全薄弱，因為其他種類的住宅可能都已經有專屬的資訊安全中心協助做專業管理。那在手冊中有關網路管理系統，它其實是做為一個管理的應用，也就是說取得智慧建築標章的建築物，它必須要有網路管理軟體來掌握其內部各連網設備之狀態。它也有規定一個資訊安全的保障設備，這是屬於外網的防護，在電信業者連進來時必須有一個硬體防火牆作為第一線資安防護。系統整合方面，手冊也有規定人機介面要有使用管理權限的功能，也要提出在系統整合資安的防護機制。這都是一些性能上的要求，並沒有細部規定它要達到什麼樣的程度。所以此研究某部分有補足這些細部項目。在使用管理端，我們有注意到其實集合住宅對於資安防護，主要在於註明管理單位或管委會本身並沒有像資安管理人員，或是居民本身對這樣的資安防護意識並沒有那麼重視，所以在管理階段

可以納入一些有關專業管理人員的培訓機制，來提升社區對整體資安方面的重視。

原有社區在納入智慧建築系統時，原則上它並沒有能力研判其所採購的東西有沒有符合基準，可能在分級上要有一個簡單的綱領，讓社區管理者方便依循。但這涉及到的系統又會非常複雜，以集合住宅而言，可能涉及到空調系統、照明系統、門禁系統，這些都是子系統本身的服務，那整合性的系統之介面就非常多，資料的防護的重要性就可能會依其需求而不同。所以在應用類別可能就可以做一些優先性的區分。再者，研究中有提到 IoT 設備，這樣的名詞真的比較廣泛，可以再做限縮。現在危老建案越來越多，其特性為基地小，可能只有六戶、八戶，其無完整監控中心，所以一些雲端服務慢慢地被推出，資訊可能只有末端的設備，一些主計可能都在雲端上處理，這也是一種服務模式。以上，謝謝。

22. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝連組長分享，有幾個重點是未來我們需要再去注意的。首先是我們要如何去收斂我們注意事項的範圍，像是各位先進有提到的，IoT 設備的範圍實在太廣，集合住宅比較常使用到的 IoT 設備，像是門禁、監視器等等，我們應該先針對這些設備在導入時應該注意的事項去做研究，這樣產業界也才能以較方便執行。另外集合住宅最大的問題可能是人的問題，畢竟資安也是比較新的概念，不管是住戶或者負責管理的單位，都需要時間培養資安意識。

23. 財團法人資訊工業策進會資安科技研究所賴怡伶專案經理

各位長官先進好，有兩點針對剛剛的議題做出回應。首先，關於這部導入旨意，參考許多國際標準，討論面向相當足夠，但是智慧建築布建的應用種類不是單一的，因此這部指引裡面的要求都是比較通用的，可能會定的稍微粗略，業者在應用的時候可能會需要的是具體針對智慧建築各項設備的相關標準。至於國內，如各位提及，工業局已推行蠻多物聯網相關產業標準，相關資安產業標準其實在工業局的 ACW 網站都可以下載的到，在這幾年我們已經制定了像

監控空氣品質探測器、無線寬頻分享器這些。集合住宅類的智慧建築，除了可以透過指引的方式了解要布建怎樣的資安設備，實際上建議直接納入現有的資安產業標準，除了條文外它亦有制定一些測試規範，在條文過於概括時，測試規範可以讓廠商具體了解。現有標準管理面有小篇幅做了一些規範，但不太足夠，建議可以對管理面多做規範，功能面的部份建議參考既有相關規範。

第二點是未來可能面臨草案分級這部分，最根本的管理面項目外，比較有爭議的是公務面的分級，要確定的是草案的角色定位，到底是資安基本準則還是資安規範。如果只是基本準則，那可能就不需要做分級了。如果未來要做更深入的安全要求的話，思考的方向可以針對應用情境跟智慧化導入程度及威脅程度來做參考依據。門禁系統的部分，12 月會公告，11 月會有草案推出。主要是參考 NIST303245、ISO62443-4-2 部份去制定。

24. 財團法人資訊工業策進會科技法律研究所周晨蕙專案經理

謝謝賴經理的分享。總結來講，目前注意事項的確是比較基本準則，我們想對比較共通性的事項先做基本定義，所以還處在比較粗略的階段，要細緻化可能需要再去更聚焦研究的對象跟範圍。如何針對不同設備做更細部的規範，這也是我們需要再去做深入研究的。國內其實已經有不少現行標準，我們也會再去做一個參考，或者是直接去做扣合，這樣一來，在注意事項上我們也可以不用去規定得那麼清楚，讓廠商依其需求參考現行的標準。在管理面上，如何確保流程上的安全性可能才會是最重要的，因此可能是要去做多一點規範的，甚至是怎麼去落實管理人員的素養，都可能會是我們在實務面上需要重視的問題。謝謝各位今天的出席。

參考書目

1. 林谷陶（2015），《既有建築物智慧化改善之研究—以集合住宅為例》。
2. 內政部建築研究所（1996），《智慧型公寓大廈自動化系統設計準則之研究》。
3. 內政部建築研究所（2016），《智慧建築評估手冊》。
4. 監察院調查報告（2019），《政府推動綠建築與智慧建築之成效案》，https://twecoliving.blogspot.com/2019/12/108982.html。
5. 臺灣資通產業標準協會（2021），《消費性物聯網產品資安標準》，https://www.taics.org.tw/Publishing.aspx?PubCat_id=2。
6. 臺灣資通產業標準協會（2021），《物聯網場域資安防護評估指引》，https://www.taics.org.tw/Publishing.aspx?PubCat_id=2。
7. 林福展（2007），〈從台灣傳統到現代住宅「起居空間」轉變之探討〉，中華大學碩士論文。
8. 郭霖（2014），〈住宅類既有建築智慧化之效益評估研究〉，中國文化大學建築及都市設計學系碩士論文。
9. 〈108 年度智慧建築標章辦理成果〉，《建築研究簡訊》，第 107 期，2020/03/11，https://www.abri.gov.tw/PeriodicalDetail.aspx?n=861&s=2322&key=87&isShowAll=false（最後瀏覽日期：2021/06/10）。
10. 〈109 年第 46 週內政統計通報〉，內政部，2020/11/14/，https://www.moi.gov.tw/News_Content.aspx?n=2&s=198959（最後瀏覽日期：2021/06/10）。
11. 〈110 年度智慧化居住空間整合應用人工智慧科技發展推廣計畫(3/4)〉，內政部建築研究所，https://www.abri.gov.tw/cp.aspx?n=14048（最後瀏覽日期：2021/06/11）。
12. 〈台閩地區住宅狀況研析〉，行政院主計處，https://www.stat.gov.tw/ct.asp?xItem=1671&ctNode=548（最後瀏覽日期：2021/05/27）。

13. 〈住宅類〉，內政部營建署，2001/12/04，https://www.cpami.gov.tw/index.php?option=com_content&view=article&id=98&Itemid=86（最後瀏覽日期：2021/05/27）。

14. 〈加州通過第一個 IoT 裝置安全法〉，IThome，2018/10/1，https://www.ithome.com.tw/news/126165（最後瀏覽日期：2021/06/11）。

15. 〈英國發布增強消費型智慧裝置安全性的新計畫〉，國際通傳產業動態觀測，2020/05/09，https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0K231386607692971161&sq=（最後瀏覽日期：2021/06/11）。

16. 〈核可案件公告〉，財團法人建築中心，http://ib.tabc.org.tw/modules/filelist/index.php/main/flist/3（最後瀏覽日期：2021/06/10）。

17. 〈スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました〉，経済産業省，https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html（最後瀏覽日期：2021/06/12）。

18. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました，経済産業省，2019/04/18，https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html（最後瀏覽日期：2021/06/20）。

19. IoT 推進コンソーシアム、総務省、経済産業省（2017），《IoT セキュリティガイドライン ver1.0 概要》。

20. 独立行政法人情報処理推進機構（2017），《つながる世界の開発指針》。

21. 経済産業省（2019），サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要。

22. 産業サイバーセキュリティ研究会（2021），《スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン》。

23. *Code of Practice for consumer IoT security*, GOV.UK, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (last visited 21. Jun 2021).

24. Omar Alrawi, Chaz Lever, Manos Antonakakis, Fabian Monrose, *SoK: Security Evaluation of Home-Based IoT Deployments*, Presented at 2019 IEEE Symposium on Security and Privacy(SP).

25. Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, *IoT Device Cybersecurity Capability Core Baseline*, available at: https://doi.org/10.6028/NIST.IR.8259A (last visited 20. Jun 2021).

26. The European Union Agency for Network and Information Security (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, 7(2017), available at; https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a506-01aa75ed71a1/language-en (last visited 22. Jun 2021).

集合住宅類智慧建築資通訊安全應用之法制規定調查研究

出版機關：內政部建築研究所

電話：（02）89127890

地址：新北市新店區北新路 3 段 200 號 13 樓

網址：http://www.abri.gov.tw

編者：王自雄、周晨蕙

出版年月：110 年 12 月

版次：第 1 版

ISBN：978-986-5456-46-7(平裝)