IoT Security 的重要性與發展趨勢

TAcc+ 新創分析團隊

資安是發展物聯網（IoT）時必須做好的基本功，隨著物聯網裝置的快速擴散，新的資安防護破口也不斷增加。駭客們抓緊機會攫取利益，對政府、企業、個人所帶來的損失與風險不斷升高，連帶使得持續提升物聯網裝置的資安防護成為剛性需求，在防護上可分為硬體、安全的通訊、雲端安全、生命週期安全管理四個層次。主要的物聯網資安防護趨勢包括：透過設計強化安全性、零信任、增加 AI 在安全方面的使用、加強對物聯網安全的監管。隨著領導企業帶頭建立物聯網裝置標準規範，以及各國政府積極立法，廠商開發出的產品、服務是否跟得上產業、各國法規，將對其競爭優勢帶來顯著的影響。

物聯網資安防護

導入物聯網時，最大挑戰之一是資訊安全的問題。若沒有足夠的安全措施，情況就像車輛的防撞設計不堅固，無論車速或舒適度如何，都不會吸引人使用，這凸顯了其重要性。根據 IoTNOW 的研究，88%的企業認為需要加強物聯網的安全性，其中超過三分之一（37%）的受訪者指出需要進行重大改進，另有 60%的受訪者表示需要進行一定程度的改進。

物聯網安全的重要性和需求

根據 SonicWall 的網路威脅報告，全球針對物聯網裝置的惡意軟體攻擊數量呈現快速增長趨勢：

- 2019 年：至少 3,427 萬次
- 2020 年：5,690 萬次（年增 66%）
- 2021 年：6,010 萬次（年增 6%）
- 2022 年：1 億 1,230 萬次（年增 87%）
- 2023 年上半年：已達 7,800 萬次，顯示增長速度驚人。

報告中也指出造成 IoT 裝置容易遭受攻擊的主要原因：

- 98%的 IoT 資訊傳輸通道未加密：這使得駭客更容易攔截和竊取傳輸中的數據。

◆ 57%的 IoT 裝置防護能力極差：這些裝置缺乏基本的安全防護措施，容易被惡意軟體入侵。

◆ 83%的醫療影像裝置在不支援作業系統的環境下運行：這表示這些裝置難以進行安全更新和修補漏洞，增加了安全風險。

由於上述原因，醫院等機構經常成為駭客攻擊的目標，其中一個關鍵原因是醫院網路系統的安全性普遍較為脆弱。機敏數據（例如病患的個人資料、醫療記錄等）一旦洩露，將造成極高的損失，尤其是在醫療保健領域，平均每次資安事件會導致高達 710 萬美元的損失。因此，IoT 安全的重要性不言而喻。

根據網路安全公司 Palo Alto Networks 在 2020 年發布的《State of Enterprise IoT Security》報告，醫療影像系統是最容易遭受攻擊的物聯網裝置，被攻擊比例高達 51%。其次是監控攝影機，被攻擊比例為 33%。病患監控系統由於更新緩慢且安全性較差，遭受攻擊的比例為 26%。辦公室印表機的資訊安全往往被忽視，被攻擊比例達 24%。此外，在自動化過程中，路燈系統的資訊安全設計不夠完善，也成為容易遭受攻擊的公共系統之一。資訊包含機敏資料和具吸引力的財務誘因，加上缺乏資訊安全防護意識的環境及次要電子設備，造就了高動機與低駭客入侵門檻二大資安攻擊因素。大型機構像是公用設施、健康醫療機構及企業辦公室，被攻擊的比率極高。其他像是醫療裝置的閘道器（Medical Device Gateway）、能源管理裝置、消費性電子產品，以及家用電話，也有零星被攻擊比率。

駭客攻擊方式中，佔比最高的是運用系統漏洞，達 41%。攻擊方以 AI 掃描 IoT 系統架構的弱點，趁虛而入。第二名是運用惡意軟體，佔比達 33%，讓使用方不慎下載惡意軟體，或是惡意軟體像是特洛伊木馬一般，透過其他看似安全的應用程式進入系統。利用使用者的習慣不佳（薄弱的資訊安全管理行為）進行攻擊的佔比達 26%，像是過於簡單的密碼、釣魚軟體等等。相較於電腦已建立一套完善的資訊安全防護系統，IoT 的安全系統至今尚未有一個統一的維護標準和專門維運廠商，致使駭客攻擊有機可趁。

駭客攻擊愈加猖獗，如何有效保護 IoT 裝置呢？首先，應建立完善的使用者認證系統。由於 IoT 裝置屬於機器設備，懂得網路運作原理的人可輕易複製網卡位址，這使得身份認證變得非常困難。因此，如何將設備裝置層控制（Device-Level Control）轉換成身份認證層控制（identity level control），成為資安管理的重要課題。其次，對每一個 IoT 裝置的追蹤與管理十分關鍵。與常見的電腦或手

機相比，追蹤電腦和手機相對容易，但各種型號與功能不同的 IoT 裝置，追蹤起來則要困難許多。再者，IoT 裝置的軟體升級問題也不容忽視。與電腦或手機有定期的軟體更新機制不同，許多 IoT 裝置缺乏螢幕和使用者介面，且品牌繁多，數量龐大，供應商如何進行定期的軟體升級與漏洞修補，成為一大挑戰。這三個問題顯著影響了 IoT 資安防護措施的實施。接下來將介紹物聯網安全元件的四個層面。

物聯網資安防護的四個層面

IoT 會發生資訊安全問題，分別在四個層面會有不同關注重點。第一層面-硬體。在硬體層面，最重要的是 IoT 設備的身份認證。 IoT 包括許多形形色色、裝上感測器的硬體，物理性的資訊安全管理是發展 IoT 資訊安全的方案之一。2021 年 10 月，美國 FDA 就頒布了醫療用器械「唯一設備認證（Unique Device Identification System, UDI System）」的指南草案，以期充分識別在美國銷售的醫療設備，從製造、分銷到患者使用都能夠知道其來源與身份。此舉之目的在於提高患者安全性，實現醫療設備銷售後的監控。

第二層面-安全的通訊：這一層面包含了防火牆、入侵偵測、入侵防護，以及端到端加密等。防火牆架設在 IoT 的內部網路及網際網路之間，架設一道可監控管理的閘門（Gateway），管制所有訊息封包的進出，允許或禁止網路上特定資料存取行為。其主要工作就是檢查所有通過的 IP 封包，藉由 IP 位址、連接阜（Port）及封包傳送方向來控制網路資訊封包傳播。入侵偵測系統主要功能在負責監聽、檢測網路封包，依據預先設定的安全策略，對網路與系統的運行狀況進行監測。當發現異常，自動發出警訊通報給網管人員，記錄各種攻擊企圖、攻擊行為或者攻擊結果。入侵防護系統則化被動為主動，當發現網路異常封包或行為時，系統除發送警訊通報給網管人員，也立即採取必要的處置措施，例如阻斷來源 IP。端到端加密，是一種安全通訊方法，目的是在防止潛在竊聽者。當一個終端設備傳輸數據到另一個終端設備時，可防止第三方獲取數據，只有終端雙方才可以讀取數據的通訊系統。IoT 設備由於數量龐大，且時常與各式不同 IoT 設備通訊，因此，端到端加密在 IoT 資訊安全的管理上是最重要且最主要的手段。

第三層面-雲端安全：雲端資訊安全保護，需要一套普遍適用的政策、技術、控制方法，以保護資料、應用程式與雲端運算的基礎設施。當數據或資訊送到以網路傳輸作為主要存取方式的雲端上，資訊安全的保護具有相當的挑戰性，需要考慮各式各樣的狀況，尤其實務上經常混合使用不同的雲端系統，使得資安保護更加困難。混合雲是指同時運用多個供應商，例如 AWS、Azure、Google Cloud，

進行數據託管、儲存，和執行應用程式堆疊（Application Stacks）。

第四層面-生命週期安全管理：在 IoT 中，不只是硬體、通訊安全、雲端安全值得重視，整體生命週期的安全管理亦非常重要。簡單來說，就是何時補丁（Patch）、升級與更新，如何更新、升級與維修。這些問題涵蓋在整個 IoT 設備從製造後到銷售通路、消費者手上，直到設備安全退役後的整個生命周期的安全性管理。例如，多數人可能會忽略了設備生命週期安全管理的安全報廢（Secure Decommissioning）。硬體即使被破壞，大多數都能夠再進行還原，所以用過的記憶體不能隨便亂丟，而需要有一個安全銷毀的程序。確保 IoT 設備能夠安全退役，且內部的數據都已經清空，應納入重要的資訊安全管理方針。

物聯網資安防護趨勢

IoT Security 市場 2022 年有 179 億美元，2023 年有 209 億美元，預計至 2028 年達 592 億美元，年複合成長率高達 23.1%，屬於高度成長的領域（MarketsandMarkets，2023）。IoT 資訊安全管理方面的趨勢包括：

1.透過設計強化安全性：開發團隊在設計之初，就要把「安全考量」一併考慮進去，因為事後補救的資訊安全效果事倍功半。包括使用具安全設計的硬體和軟體，實施確實的身份驗證和授權機制，以及使用最新的安全補丁使設備保持最新狀態。

2.零信任（zero trust）安全性的日益普及：沒有人或任何設備預設為可被信任。此方法通過根據使用者身份和設備狀態，限制對資源的訪問來防止資安攻擊。

3.增加 AI 在安全方面的使用：AI 可用於識別可疑活動、檢測惡意軟體和回應安全事件。

4.加強對物聯網安全的監管

物聯網硬體資安防護

IoT 資訊安全管理的第一層-硬體層，旨揭如何做到 IoT 設備的身份認證。以車子為例，過去傳統油車最貴的部件是引擎，因此引擎製造商就會在引擎上刻上編號，即使車子被偷或被解體，也有機會透過引擎編號來找到失竊的車子。未來電動車是由一堆電池與電腦等電子產品組成，如何對電動車進行身份認證？電動車的馬達、控制系統、CPU，與電腦的組合，就形成了車體新的身份認證。其中，IoT 設備，或者晶片的身份認證有不同模式，目前主流是透過

物理不可複製函數（Physical Unclonable Function，PUF），記錄在實體晶片上。

PUF 是一個具體化的物理結構函數，是半導體最新的安全認證技術之一。透過製造矽晶片時，由製程產生有限度的物理誤差，使得每個晶片具有稍為不同的物理特徵，作為該晶片的 DNA 或者稱之為晶片的指紋。PUF 具有幾個重要特性，包含隨機性、不可複製性和穩定性。它提供了一個具體的物理性特徵以識別各個晶片的差異。PUF 解決了目前 MAC 位址（Media Access Control Address）可以輕易地以編碼的方式刪除，破壞其晶片之間的數位辨識與認證。

數據型的身份認證應用之科技是公開金鑰基礎建設（Public Key Infrastructure，PKI）：一組由硬體、軟體、參與者、管理政策與流程組成的基礎架構，用來創造、管理、分配、使用、儲存，以及復原「數位憑證」。PKI 藉著數位憑證認證機構，將使用者的 IoT 身份跟公開金鑰鏈結在一起，讓每個憑證中心 IoT 的身份保持唯一性。透過物理性的身份認證，例如 PUF，以及數據型的身份認證，雙管齊下，確保 IoT 在硬體方面的資訊安全性。

2021 年，PKI as a Service 的新創先驅 Key Factor 公司，合併 Prime Key（頒發憑證的公司），此結合帶來的好處是提供 End to end 的 IoT 設備的身份管理，並能夠靈活地發布證書。Key Factor 在 2024 年營收已超過 1 億美元，且過去三年收入成長達 525%，顯示企業在物聯網趨勢下迫切的資安需求，反映在其市場的快速成長。

物聯網設備身分識別標準建立

傳統上，大多數的物聯網裝置或設備都會使用預設密碼，同時為了方便管理維運，也常設定通用密碼，這些密碼經常被設定的過於簡單，例如 0000、1234、admin…。當使用者買來這些設備後，多數人不會主動更改密碼，使得惡意者可輕易猜出這些密碼，成為資安保護上的破口。此外，在部署 IoT 設備時，必須依靠專業技術人員手動操作進行實體裝置安裝，以及設置密碼憑證，花費時間長。若遇到負責人員更動也會影響維運，使得整體運作成本居高不下。

以 Paypal、Google、Apple、VISA、Intel、LINE 等頂尖大廠為首建立的國際身分識別標準組織 FIDO 聯盟（Fast IDentity Online Alliance），針對 IoT 設備的身分識別推出 FDO（FIDO Device Onboard）標準規範，於 2021 年 4

月發布初版，以期降低運作成本、管理複雜度、部署和維運的時間，提高安全性。FDO 規範在設備製造過程中就確定裝置的所有權，透過自動化簡化驗證程序，讓 IoT 裝置在不修改的情況下，仍可安全連上不同的 IoT 平台。

過往產業界一直都有發展類似的技術，但欠缺統合的標準，FDO 做為一個開放的產業標準，自規範推出後，持續獲得越來越多的廠商支援。2023 年 9 月 FDO 認證計畫啟動後，已有多家廠商的產品申請認證。業界普遍認知到，隨著 FDO 的推廣與擴散，有助於資訊科技（IT）與運營科技（OT）的融合，以及解決物聯網裝置跨領域、跨產業、跨組織統合使用的需求，並期望透過此規範，解決產業界共同面對的挑戰。

物聯網資安立法

隨著駭客針對物聯網裝置的攻擊越演越烈，各國政府也積極立法。舉領跑者歐盟為例，歐盟於 2019 年發布的「歐盟網路與資訊系統安全指令（NIS2 Directive），適用範圍包括物聯網設備，該法要求各成員國於 2024 年前將指令轉化為國內法規，並於同年正式生效。2024 年 10 月 10 日，歐盟理事會通過資安韌性法案（Cyber Resilience Act，CRA），藉此強化數位產品的安全性，法案已生效，且要求 2027 年底前，相關軟體、硬體與服務的業者，必須完全合規。物聯網產品、設備及服務須在供應鏈和生命週期內做好相關資安要求。

越來越嚴謹的法規，要求製造商在產品的設計、開發與維運之全生命週期，保持足夠的安全性以確保聯網裝置的使用可靠。對於想要進軍海外市場的業者而言，開發出的產品、服務是否跟得上各國法規，將對銷售量帶來重大影響。同理，產品、服務能夠符合越多國家的法規要求，競爭優勢也會更明顯。

參考資料：

- 【資安月報】2024 年 4 月。iThome。2024。
- 2025 年「物聯網」將會暗潮洶湧 安全法規與駭客威脅成關鍵。科技島。2024。
- Appier 全線產品整合生成式 AI 創新應用，驅動智慧商業策略升級。經濟日報。2024。
- FIDO 聯盟推 IoT 設備身分識別 FDO 標準，紅帽 RHEL、Fedora 開始支援。iThome。2022。
- StartUp 創辦人對生成式 AI 的 6 項提問。AWS。2024。

- 生成式 AI 的產業應用與發展趨勢。數位發展部。2024。
- 最新 IoT 設備身分識別 FDO 標準，即將有 4 家廠商取得首波認證，臺灣工業電腦廠也包括在內。iThome。2024。
- 新法令力促工控 IoT 資安防護　企業迎向全生命週期合規挑戰。網管人。2024。
- 歐盟網路韌性法案 CRA 將於 2027 年強制執行。德國萊因 TÜV。2024。