物聯網資通安全與國際標準應用

物聯網資通安全標準 ISO-27400將底定

IT 與 OT 在資通安全的標準遵循終於可以趨於一致，ISO/IEC 27400 的底定，將有助於確認 IoT 的資安標準，讓安全防護更上層樓。

文／梁日誠 (ISO/IEC JTC1/SC27及IEC/TC65加拿大對映技術委員會委員與TCIC環奧國際驗證公司全球營運總經理)

隨著物聯網(IoT)的應用在各個領域(如:製造、醫療、公務)漸被採用，資通安全(Cybersecurity)也成了各界關注的焦點，近日ISO組織公告了IoT資通安全之安全與隱私標準(草案DIS) ISO/IEC 27400(以下簡稱ISO 27400)，將物聯網資通安全與相關的國際標準做出關聯，也提供各界做為完善物聯網資通安全之參考及日後合規展現(如：資通安全管理法與個人資料保護法)之依據。

ISO組織在2018年推出了「ISO/IEC 30141 IoT Reference Architecture物聯網參考架構」，其中揭櫫了IoT須具備的Trustworthiness(可信賴度)以維持IoT架構的正常運作。「可信賴度」為跨領域能力的一環，貫穿物聯網參考架構的各個領域，包含了安全(Safety)、資安(Security)、隱私與個資保護(Privacy and PII Protection)、可靠性(Reliability)與韌性(Resilience)等特性，ISO 27400涵蓋了可信賴度中的資安及隱私與個資保護兩大面象，以物聯網的生命週期觀之，完整的涵蓋了資通安全(包含IT安全與OT安全)。ISO 27400藉由風險與控制措施的探討，將主要的國際資安與隱私標準做出關聯，讓各界可以基於已經建置的資安與隱私管理系統（如：ISMS與PIMS）進而延伸至物聯網的資通安全管理。

藉由以下主題的探討，來一窺ISO 27400的相關應用：

- 物聯網系統的利害相關者與物聯網服務的生命週期。
- 基於領域的參考模型。
- 風險與管理系統。
- 資安與隱私控制措施。
- 驗證與法遵。

物聯網系統的利害相關者與物聯網服務的生命週期

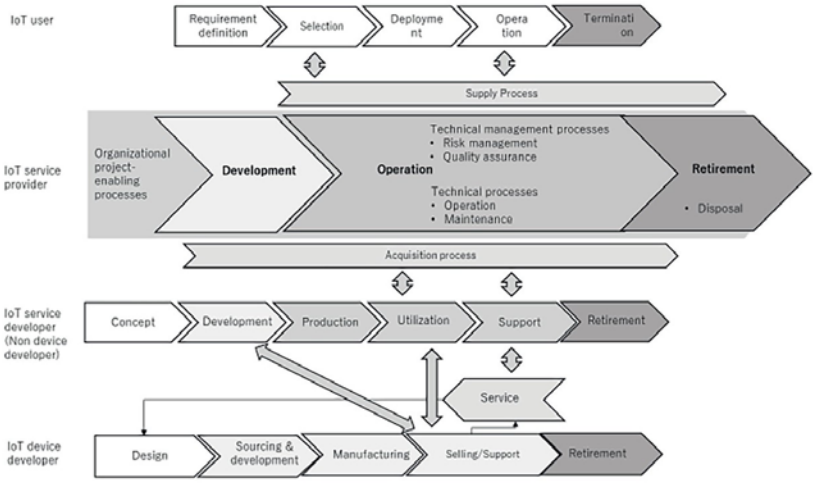
物聯網系統的利害相關者包含了物聯網服務提供者(Service provider)、物聯網服務開發者(Service developer)、物聯網使用者(Users)。

其中，物聯網服務提供者管理並營運提供給物聯網使用者的物聯網系統的相關服務，如: 連線服務、資料收集與管理服務、物聯網相關資產(如:物聯網設備)管理服務; 物聯網服務開發者負責物連網服務的設計、建置、整合，如: 物聯網設備開發者(是物聯網服務開發者的角色之一)，物聯網設備開發者執行使用於物聯網系統(特別是物聯網設備)之特定硬體設備的工程與製造;物聯網使用者是物聯網服務的終端使用者，分為人員使用者(Human user)與數位使用者(Digital user)，人員使用者為使用物聯網服務的個體，數位使用者為非人員使用者(Non-human user)並可能是代表人員使用者的自動化服務。

物聯網系統或服務的安全與隱私要求主要來自於物聯網使用者的期望或風險考量，然而物聯網

使用者通常不太了解物聯網科技的安全隱患。藉由ISO 27400，物聯網使用者可基於國際標準來了解並設定安全與隱私的要求等級，而物聯網服務提供者與物聯網服務開發者也可以ISO 27400作為共通語言，落實相關的控制措施來達到物聯網用戶的安全與隱私要求等級。

物聯網服務與利害相關者的生命週期示意圖如<圖一>。



<圖一>物聯網服務生命週期示意圖
資料來源: ISO/IEC 27400(DIS)

<圖一>的各組織內的系統與軟體生命週期流程宜與ISO 15288與ISO 12207分別校準，並參考ISO 24748系列生命週期管理標準。物聯網系統與產品安全生命週期參考模型(Security Life Cycle Reference Model)也於ISO30141中提出，強調物聯網系統與產品的設計時期(如: Security by Design，Privacy by Design)與營運時期的安全均不可偏廢。

基於領域的參考模型

物聯網系統與其營運的功能框架如ISO 30141中所定義之基於領域的參考模型，如<圖二>，<圖二>並顯示了與物聯網系統的利害相關者的對應關係。基於領域的參考模型提供了考量物聯網系統的安全與隱私的整體元件架構，風險來源可以依物聯網領域而識別，每個安全與隱私控制措施可以被關聯到一個或多個物聯網領域。

物聯網領域說明如下：

- 使用者領域(User Domain，UD)，包含人員與數位使用者。
- 實體個體領域(Physical Entity Domain，PED)，包含物聯網系統中的實體個體。
- 感應與控制領域(Sensing and Controlling Domain，SCD)，包含物聯網設備與物聯網閘道器。
- 營運與管理領域(Operations and Management Domain，OMD)，包含營運支援系統與業務支援系統。
- 資源存取與互換領域(Resource Access and Interchange Domain，RAID)，提供外部個體可存取物聯網系統能力的機制。
- 應用與服務領域(Application and Service Domain，ASD)，包含物聯網服務提供者所提供的應用與服務。

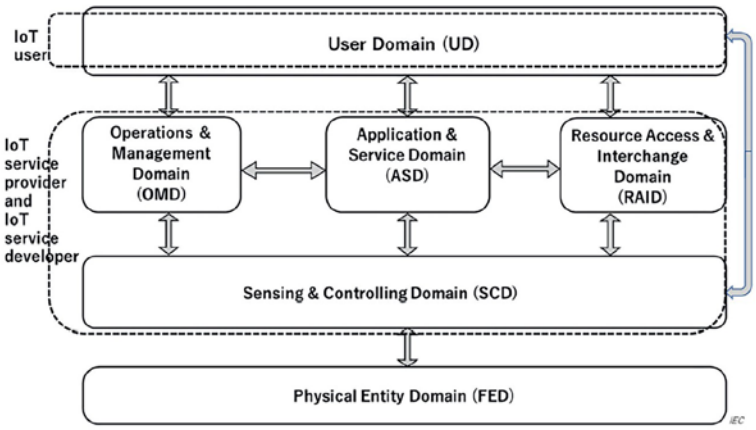
風險與管理系統

依各個物聯網領域而識別的風險來源可經由標準化的過程與方法執行風險管理，如以下風險管理相關國際標準：

- ISO 31000，提供一般性的風險管理指引。
- ISO/IEC 27005，提供資訊安全風險管理指引。
- IEC 62443-3-2，提供工業自動化控制系統(IACS)安全風險評鑑要求。
- ISO/IEC 29134，提供隱私衝擊評鑑。

當建置資訊安全管理系統(ISMS)與隱私資訊管理系統(PIMS)時，可以依據以下的國際資安管理系統標準與對應的風險管理及控制措施國際標準：

- ISO/IEC 27001，資訊安全管理系統(ISMS)，可選用ISO 27005(IT安全)與IEC 62443-3-2(OT安全)進行資安風險管理。進行風險處理時，可以選用ISO 27001附錄A的控制措施(IT安全)、



<圖二>基於領域的參考模型
資料來源: ISO/IEC 27400(DIS)

IEC 62443-2-1的安全控制措施(OT安全)與ISO 27400的安全控制措施(物聯網安全)。

- ISO/IEC 27701，隱私資訊管理系統(PIMS)，可選用ISO 29134進行隱私風險評鑑。進行風險處理時，可以選用ISO 27001附錄A的控制措施(IT安全)、ISO 27701附錄A與附錄B的控制措施(隱私保護) 與ISO 27400的隱私控制措施(物聯網隱私)。

安全與隱私控制措施

ISO 27400所列舉的物聯網安全與隱私控制措施依以下分類，並綜整如<表一>。

- 物聯網服務開發者與物聯網服務提供者的安全控制措施。
- 物聯網使用者的安全控制措施。
- 物聯網服務開發者與物聯網服務提供者的隱私控制措施。
- 物聯網使用者的隱私控制措施。

物聯網安全控制措施可與其他安全控制措施，如：ISO 27001附錄A合併使用; 物聯網隱私控制措施可與其他隱私控制措施，如：ISO 27701附錄A與附錄B合併使用。

驗證與法遵

物聯網系統，依其不同應用，可能涉及驗證或法遵議題，如：個人資料保護法、資通安全管理法。以某個適用於資通安全管理法的機關為例，ISO 27400對於物聯網系統可能的驗證與法遵考量如下：

- 依資通安全管理法施行細則第七條，識別物聯網系統是否為核心資通系統。
- 依資通安全責任等級分級辦法附表一至六(若適用)，辦理物聯網系統之資通系統分級及防護基準。
- 若為核心資通系統，將物聯網系統納入資訊安全管理系統之導入(A/B/C級)及通過公正第三方之驗證(A/B級)。
- 對於物聯網系統相關之受託者(如:服務提供者、服務或設備開發者)，依資通安全管理法施行細則第四條要求受託者辦理受託業務之相關程序及環境(如:物聯網)，應具備完善之資通安全管理措施或通過第三方驗證，所稱第三方，係指通過我國標準法主管機關委託機構認證之機構，其驗證標準可為國際、國家或團體標準。第三方核發之驗證證書應有前開委託機構(即TAF)之認證標誌。
- 依據ISO 27001 Clause 6.1.3 c)備考2.附錄A中所列之各項控制目標及控制措施並未盡列，故可能需要額外之控制目標及控制措施。可選擇除了ISO 27001附錄A以外所適用的其他國際(如: ISO 27701、IEC 62443-2-1、ISO 27400)或國內自行發展的控制措施，並納入適用性聲明6.1.3 d)。
- 依據ISO 27006/AMD1:2020，組織依據ISO 27001選擇其適用的控制措施，驗證文件(如：證書)可以註明組織除了ISO 27001附錄A以外前項所述的控制措施。
- 當物聯網系統相關之受託者(如：服務提供者、服務或設備開發者)發生資安疑慮時，委託機關應依資通安全管理法施行細則第四條，於知悉受託者發生可能影響受託業務之資通安全事件

物聯網服務開發者與物聯網服務提供者的安全控制措施 Security controls for IoT service developer and IoT service provider	
Policy for IoT security	Protection of logs
Organization of IoT security	Use of suitable networks for the IoT systems
Asset management	Secure settings and configurations in delivery of IoT devices and services
Equipment and assets located outside physical secured areas	User authentication
Secure disposal or re-use of equipment	Provision of software and firmware updates
Learning from security incidents	Sharing vulnerability information
Secure IoT system engineering principles	Security measures adapted to the life cycle of IoT system and services
Secure development environment and procedures	Guidance for IoT users on the proper use of IoT devices and services
Security of IoT systems in support of safety	Determination of security roles for stakeholders
Security in connecting varied IoT devices	Management of vulnerable devices
Verification of IoT devices and systems design	Management of supplier relationships in IoT security
Monitoring and logging	Information security in IoT devices
物聯網使用者的安全控制措施 Security controls for IoT user	
Contacts and support service	Deactivate unused devices
Initial settings of IoT device and service	Secure disposal or re-use of IoT device
物聯網服務開發者與物聯網服務提供者的隱私控制措施 Privacy controls for IoT service developer and IoT service provider	
Prevention of privacy invasive events	Fail-safe authentication
IoT privacy by default(共2個)	Minimization of indirect data collection
Collection and use of personal data(共2個)	Communication of privacy preferences
Verification of IoT functionality	Verification of automated decision
Consideration of IoT users	Accountability for stakeholders
Management of IoT privacy controls	Unlinkability of PII
Unique device identity(共2個)	PII protection in IoT devices
物聯網使用者的隱私控制措施 Privacy controls for IoT user	
User consent	Certification/validation of PII protection
Connecting with other devices and services	

<表一>物聯網安全與隱私控制措施

時，以稽核或其他適當方式確認受託業務之執行情形，以展現良善的管理作為與法遵。

藉由以上的考量事項，各組織可以經由第三方驗證展現法遵，物聯網服務提供者、物聯網服務開發者也可經由採用ISO 27400來展現與其他業者對於資安與隱私保護的承諾與差異性。

在發展ISO 27400的同時，IoT security and privacy — Device baseline requirements的國際標準ISO 27402也正在發展中(技術組草案CD)，對於物聯網設備的基線要求提供規範，將更進一步強化物聯網生態系的資通安全，也將使物聯網方案所支撐的智慧應用更加的強固。