数字政策辦公室

資訊保安

物聯網保安

實務指引

第 1.2 版

2024 年 7 月

修改記錄				
修改次數	修改詳情	經修改頁數	版本編號	日期
1	更新物聯網裝置的定義一節、資產管理一節以及圖4.1、7.1和7.2	3-1，4-2，5-2，7-1，7-2	1.1	2021 年 6 月
2	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		1.2	2024 年 7 月

目錄

1. 簡介 1
   - 1.1 目的 1
   - 1.2 參考標準 1
   - 1.3 定義及慣用詞 2
   - 1.4 聯絡方法 2
2. 資訊保安管理 3
3. 物聯網概述 5
   - 3.1 物聯網裝置的定義 5
4. 物聯網保安介紹 7
   - 4.1 物聯網保安的挑戰 7
   - 4.2 物聯網部署中的組件 11
5. 物聯網的保安考慮因素和控制措施 13
   - 5.1 資訊科技保安政策 13
   - 5.2 資產管理 14
   - 5.3 接達控制 15
   - 5.4 加密方法 16
   - 5.5 實體和環境保安 16
   - 5.6 操作保安 17
   - 5.7 通訊保安 19
   - 5.8 系統購置、發展及維護 20
   - 5.9 遵行要求 22
6. 個人資料保護的考慮因素 25
7. 物聯網裝置的應用案例 26
   - 7.1 宏觀物聯網參考模型 27
   - 7.2 公共區域安裝的物聯網裝置（案例一） 28
   - 7.2.1 應用系統界面的保安建議 29
   - 7.3 辦公環境中安裝的物聯網裝置（案例二） 31
   - 7.3. 部署物聯網裝置的示例 32

1. 簡介

1.1 目的

本文件旨在協助各局及部門採用物聯網技術，並提供指引給多元的受眾，例如管理人員、資訊科技管理員、系統擁有者和資訊保安持份者，因他們負責評估在使用物聯網裝置儲存、處理或傳遞政府的資訊時，對政府資訊系統保安造成的影響。

本文件重點介紹採用物聯網時常見的保安考慮因素和良好作業模式，以加強對物聯網保安的基本理解。

由於每種物聯網裝置應用都有其特點和需要，建議決策局／部門採取風險為本的方法，實施適當的保安措施，以保護資料資產。

1.2 參考標準

以下參考文件對於本文件的應用是不可或缺的參考。

- 香港特別行政區政府基準資訊科技保安政策[S17]
- 香港特別行政區政府資訊科技保安指引[G3]
- Information technology – Security techniques – Information security management systems – Requirements (second edition), ISO/IEC 27001:2013
- Information technology – Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2013

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的定義及慣用詞。

縮寫及術語	
物聯網裝置	具有網絡連接和運算功能的裝置，通過感應或致動的方式自動與實體環境互動。

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資料資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，來迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資料資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下功能領域：

- 保安管理框架和組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；和
- 態勢感知和資訊共享。

<u>保安管理框架和組織</u>

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

<u>管治、風險管理和遵行要求</u>

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

各決策局／部門須定期和必要時對資訊系統和生產應用進行保安風險評估，以確定與漏洞相關的風險和後果，並為制定具有成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取協調行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。 若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並製定相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安每個人都有責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用威脅情報平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

3. 物聯網概述

3.1 物聯網裝置的定義

市場上所提供的物聯網裝置種類繁多，例如感應器、執行器等。 由於物聯網技術的不斷發展，物聯網裝置沒有一個全球都普遍接受的單一的定義。在本指引中，物聯網裝置是指有網絡連接和運算功能的裝置，這些裝置通過感應或致動方式自動地與實體環境互動。對於可以配置為與互聯網或企業網絡有網絡連接的裝置，無論它們是否連接到此類網絡，都被視為物聯網裝置。以下是物聯網裝置的一些例子：

- 具有網絡連接的感應器（例如空氣質量、溫度）;
- 具有網絡連接的智能計量錶（例如電、水）;
- 具有網絡連接的智能設備（例如雪櫃、電視、電燈）。

現今，很多資訊科技設備都內置了物聯網功能。本指引，將集中討論那些在政府會用作一般應用的物聯網裝置。 對於有專門工業用途的物聯網裝置，例如智能電機或智能泵等致動器，它們一般會集成於操作技術內，以監察和控制工業設備、過程和日常操作。操作技術不在本文件涵蓋的範圍。傳統的資訊科技設備，如流動裝置、網絡設備、工作站和伺服器不是本文件重點關注的裝置，因為《基準資訊科技保安政策》和《資訊科技保安指引》以及相關的實務指引已提及如何在這些設備推行保安措施。然而，如果傳統的資訊科技設備被用作為物聯網裝置，例如內置攝錄機的電腦被用作為監察系統，或流動裝置的全球定位系統/藍芽功能被用作為位置追蹤器，則本文件對物聯網裝置的保安措施亦同樣適用。此外，由於很多資訊科技設備是建立於不同的組件上，因此需要盡職覆檢審查組件的功能，並判斷這些組件的保安控制措施是否已被妥善實施或者在不需要的情況下其相關物聯網功能已被適當地停止使用。

由於局／部門可能已部署了一些物聯網裝置，局／部門可從以下角度對其物聯網裝置進行保安評估：

- 物聯網裝置所處理和儲存的資料；
- 物聯網裝置所連接的網絡與其他相連裝置；和
- 物聯網裝置自身的保護。

在評估辦公環境中使用物聯網裝置的保安時，應考慮以下因素：

- 物聯網裝置是否會處理或擷取敏感資料；
- 物聯網裝置是否會連接到部門網絡或決策局／部門擁有的設備；
- 在辦公環境中有否安裝物聯網裝置；
- 物聯網裝置是否會與互聯網或者其他外部設備連接以交換敏感資料；和
- 如果沒有妥善管理，物聯網裝置是否對保安有影響而影響政府形象。

決策局／部門應評估物聯網裝置所構成的風險，以及一旦發生保安事故，對政府運作和形象的影響。決策局／部門須界定和實施適當的措施，以確保物聯網裝置和數據的資訊保安與資料的保密分類相稱。

4. 物聯網保安介紹

4.1 物聯網保安的挑戰

在物聯網技術相關的系統中，智能裝置的數據保護面臨新的挑戰。與傳統資訊科技設備相比，物聯網裝置的攻擊面更廣、更多樣化。也就是說，物聯網裝置的保安威脅可能來自很多方面：設備、網絡、儲存以及與物聯網裝置相關的應用/服務，如雲端、網絡和流動服務。所有這些都可能受到網絡攻擊。

簡單而言，物聯網所面臨的主要威脅有以下幾方面：

<u>裝置</u>

裝置通常是發動攻擊的主要目標。裝置的漏洞可來自記憶體、固件、實體界面、網頁和網絡服務。攻擊者也可以利用不安全的預設設定、過時的組件和不安全的更新機制所產生的漏洞來攻擊裝置。缺乏設備管理和物理加固也是裝置的常見威脅。以下是裝置常見的威脅：

- 缺乏設備管理
  物聯網裝置可能缺乏妥善管理，包括資產管理、修補程式管理、安全退役和系統監控等。這種情況通常發生在低成本設計的感應器中。

- 不安全的預設設定
  由於一些物聯網裝置體積非常小和應用數量大，管理員可能通過使用裝置的預設設置來簡化操作。但是，預設設定一般容易受到外部攻擊，很容易被第三方利用，導致未經授權的系統接達。

- 缺乏實體強化
  對於物聯網裝置，特別是安裝在政府場地以外的物聯網裝置，並不足夠或有效落實埠限制或實體接達限制等強化措施。這使得攻擊者可以入侵實體設備以獲得控制權。

- 使用不安全或不支援的組件

  由於物聯網裝置可能會應用在廣泛的範疇，而很多設備都是以低成本為前提下設計的，因此，無論是硬件還是軟件，其組件都可能支援不足或存有不安全的設定。這令裝置很容易被入侵。

- 容易被修改的裝置

  由於裝置製造商可能未有採用設計層面的保安方式，物聯網裝置可能會無意中留下後門。

- 容易遭破壞的裝置

  由於物聯網裝置可能會安裝在公共區域，若裝置被盜或被破壞，可能會損壞裝置或相關系統並導致系統未能正常運作。

<u>數據</u>

物聯網裝置可能需要收集數據，並與對應裝置交換這些數據。使用者可能會低估收集的數據量，並收集不必要的數據。數據外泄是物聯網裝置常見的威脅之一，原因如下：

- 弱密碼或不可更改的密碼

  有些物聯網裝置可能不支援嚴謹的密碼設置，甚至不允許更改密碼。此外，如果用戶缺乏保安認知，他們可能會選擇一些容易被暴力攻擊破解的密碼。攻擊者就可能很容易進入這類系統。

- 缺乏保安更新機制

  一些物聯網裝置製造商可能缺乏資源為其設備（包括固件和軟件模組）提供保安更新，或可能無法及時提供保安更新。此外，物聯網裝置可能由沒有保安更新的第三方軟件/代碼組成。

- 不安全的數據儲存

  物聯網裝置或會儲存數據，但可能沒有保安措施或沒有加密功能來保護敏感資料。因此可能不足以防止未經授權的接達。

- 資訊外泄

  由於物聯網裝置可能安裝在限制區內，因此可能存在向未經授權方洩漏敏感環境資料的風險。此外，如果物聯網裝置與互聯網互連，攻擊者可能會通過惡意軟件感染、未經授權的接達或中間人攻擊等手段來獲取資料。

<u>網絡</u>

攻擊者可以透過通訊通道攻擊物聯網組件。此外，物聯網系統中使用的通訊規約可能存在會影響物聯網系統的保安漏洞。以下是一些常見的威脅：

- 不安全的網絡服務

  裝置本身運行不安全的網絡服務，特別是暴露在互聯網上的網絡服務，可能會危害物聯網的保安或允許未經授權的遠端控制。

- 不安全的數據傳輸

  一些物聯網裝置由於其效能有限，可能無法提供足夠的加密強度或敏感數據的接達控制。

- 通過網絡收集資料作惡意用途

  雖然互聯功能是物聯網裝置的優勢之一，但這也帶來了攻擊面。中間人或者會話劫持等攻擊可能讓攻擊者獲得敏感資料。

- 惡意攻擊

  與上述情況一樣，惡意攻擊者可能會通過網絡獲取物聯網裝置的接達權限，並在裝置上安裝惡意軟件。這將導致分散式拒絕服務攻擊，甚至將物聯網裝置變成僵屍網絡。

<u>私隱</u>

物聯網裝置可能安裝在辦公環境或公共區域。管理員可能沒有意識到物聯網裝置可能會收集過多的個人資料。如果不妥善管理，攻擊者可能會收集這些個人資料危及私隱。

<u>應用系統</u>

物聯網裝置的雲端服務、流動應用程式、網上應用系統和相關軟件的漏洞都可能導致系統受破壞。以下是一些常見的威脅：

- 不安全的應用程式界面

  物聯網生態系統中不安全的網址、後端應用程式界面、雲端或流動界面可能會讓物聯網裝置受破壞。常見的問題包括缺乏認證/授權，缺乏或弱加密，或缺乏輸入和輸出認證。

- 軟件漏洞

  軟件漏洞和配置錯誤是物聯網裝置的常見威脅。這些漏洞通常被攻擊者使用的攻擊工具入侵，例如，網上應用系統被利用作竊取用戶憑證或安裝惡意的固件更新。

4.2 物聯網部署中的組件

下圖說明建基於物聯網的部署中常見的組件。它由物聯網裝置、通訊、後台伺服器和儲存設備以及應用系統組成。這有助於我們識別威脅和推行相應的保安措施。部署模式將在第 7 節--物聯網裝置的案例中描述。取決於部署的可擴展性，有些組件是非必要的。例如，並非所有的物聯網部署都需要應用伺服器或資料庫。

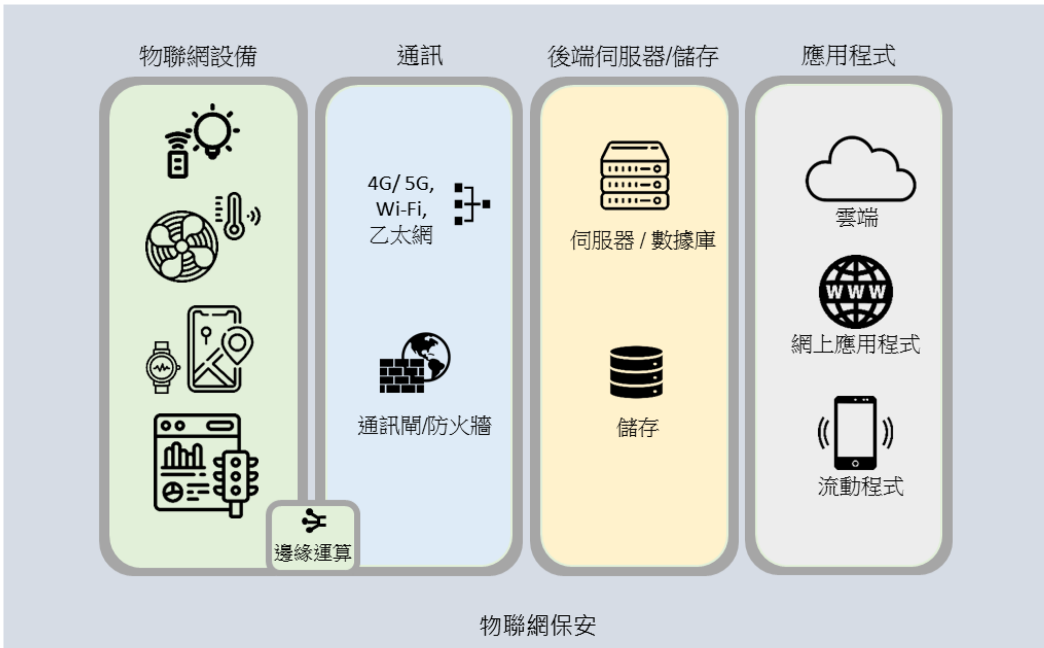

圖 4.1 建基於物聯網的部署中的常見組件

<u>物聯網裝置</u>

裝置層又稱端點，是物聯網技術系統的實體界面。物聯網裝置可以有各種操作系統、中央處理器類型、記憶體等。這些裝置可能位於辦公環境或公共區域，有些可能位於偏遠地區，這便需要遠端控制來保持正常操作。

邊緣運算是保護物聯網保安基礎架構的重要組成部分。由於物聯網裝置通常在提供保安功能方面有所局限，因此邊緣運算可充當抵禦潛在攻擊的角色。在這種情況下，邊緣裝置就是掌控那些物聯網裝置的看門人。

通訊

連接是物聯網裝置的關鍵。物聯網裝置可以相互連接，也可以直接連接到互聯網。網絡基礎設施包括傳輸資料數據、語音、圖像和視頻影片的局域網、廣域網絡或流動/無線連接（4G/5G、Wi-Fi 等）。

一些連接的例子包括：

- 4G/5G
- LTE
- Wi-Fi
- 乙太網絡
- 近距離無線通訊
- 低功耗藍牙
- 射頻識別

在技術方面，物聯網裝置支援多種通訊識別，如互聯網規約地址、媒體接達控制地址、電話號碼等，其中互聯網規約位址是比較常用的。互聯網規約位址可以通過無線連接(Wi-Fi、4G、5G、LTE 等)以及有線(乙太網等)通訊方式進行通訊。

後端伺服器和儲存設備

一些物聯網系統需要應用後端伺服器或資料庫。在一些大規模的物聯網應用中，需要後端伺服器或資料庫來支援計算功能或數據儲存。後端伺服器或資料庫可以由數據中心或通過雲端平台來提供。

應用系統

物聯網可以與雲端、網絡或流動應用程式相結合。在某些情況下，雲端平台負責對收集的數據進行有效處理和管理。它還託管應用系統，以提供服務和管理整個物聯網架構。

5. 物聯網的保安考慮因素和控制措施

資訊保安是任何資料和通訊技術系統的主要關注點，物聯網系統也不例外。因此，資訊保安管理原則適用於物聯網保安。然而，物聯網系統為資訊保安帶來特殊的挑戰，因為物聯網裝置可以高度分散，亦可涉及大量不同的單位。使用物聯網裝置須全面檢視端對端保安，採取風險為本的方法為物聯網裝置識別保安風險、訂定風險的緩急次序和應對有關風險，包括但不限於資產管理、認證和授權、通訊網絡、軟件和應用系統、後端基礎設施、裝置保安、實體保安等。由於物聯網裝置和流動裝置的某些相似性，例如連接性，流動性和體積小，因此，在政府保安文件列出的流動裝置保安要求和原則應該同樣應用於物聯網裝置。

以下章節將介紹物聯網特定保安領域的挑戰和建議，重點介紹以下保安領域：

- 資訊科技保安政策
- 資產管理
- 接達控制
- 加密方法
- 實體及環境保安
- 操作保安
- 通訊保安
- 系統購置、發展及維護
- 遵行要求

5.1 資訊科技保安政策

決策局／部門須訂定並確實執行其資訊科技保安政策，根據業務和保安要求，就保護資訊系統和資產的工作提供管理方向和支援。當物聯網裝置部署或引入資訊系統時，決策局／部門須覆檢其部門的保安政策，以配合物聯網裝置的安全要求。此外，須設有正式的使用政策及程序，並採取適當的保安措施以防範針對物聯網裝置的風險。以下是一些對決策局／部門的建議：

- 覆檢資訊科技保安政策

  決策局／部門資訊科技保安政策應根據業務需要和保安要求，在必要時確實執行、定期覆檢和更新，以保護資訊系統和資產。特別是在資訊技術環境中引入物聯網時(如物聯網裝置、後端伺服器/儲存等)，更新各保安領域，引入新的或強化的保安要求，如接達控制、實體保安、通訊保安、資產管理等。

- 制定正式的物聯網裝置使用政策及程序

  須制訂正式的使用政策及程序，並採取適當的保安措施，以防範針對物聯網裝置的風險。使用政策及程序應包括但不限於以下要求：a.)實體保護，防範物聯網裝置和數據被盜或遺失；b.)接達控制，防範未經授權操縱設備和修改數據；c.)通訊保護，防範攔截數據或嗅探攻擊；d.)加密要求，提出基本和有效保護的最低標準；e.)日誌管理，跟蹤異常活動並識別其責任；f.) 保安漏洞管理，防止惡意軟件針對已知的保安漏洞，發起的惡意代碼和病毒的攻擊。

  使用政策及程序還應包括有關保護物聯網裝置之間連接以及連接到政府網絡的物聯網裝置的規則和建議，保護物聯網端點免受保安威脅，例如成為攻擊者操縱的僵屍網絡的一部分、惡意軟件傳播、分散式拒絕服務攻擊等。

5.2 資產管理

決策局／部門應確保和維持物聯網裝置和數據受到適當的保護。決策局／部門應備存和覆檢存有敏感資料或連接內部/外部網絡的物聯網裝置清單，並作出適當安排以確保按照政府的保安要求處理數據，以期減少對物聯網裝置、政府資料以及對資訊系統可能產生的影響的保安風險。

- 妥善記錄和管理物聯網裝置

  決策局／部門應從資產中識別出物聯網裝置，並在清單中標明、備存和定期覆檢清單，以確保清單是最新和準確的。應擬訂物聯網裝置清單，提供裝置資產資料，包括型號、獨有識別碼、固件、序號、擁有權等，並訂明會否處理、儲存或傳送任何敏感數據。決策局／部門應考慮使用電腦系統管理資產記錄，以有效促進資產管理和資訊科技保安。

- 對物聯網裝置處理的數據進行評估和分類

  應根據數據的敏感程度對其進行分類。在處理、儲存或傳輸數據過程中，應根據其類別予以相對應地保護。應明確界定和記錄數據所有權和處理程序。

- 當不再需要時，刪除儲存在物聯網裝置中的敏感數據

  為防止數據外泄、遺失或未經授權的接達，在處理或重用所有敏感數據前，須參照 G3 第 10.3(b)節的規定，以徹底清除或銷毀敏感數據。

5.3 接達控制

決策局／部門須界定和實施適當的保安措施，以確保物聯網裝置和數據的保安與資料類別相稱。這些措施應能有效防止物聯網裝置和數據在未經授權的情況下被入侵和操控。應考慮以下接達和管理物聯網裝置的常用保安措施、控制和作業模式，但並非詳盡無遺：

- 選擇設計上提供了保安功能（如識別、認證和授權）的物聯網裝置。
- 限制和控制對物聯網裝置和數據的接達，根據最小權限和職務分工的原則，向用戶授予接達權限。當不再需要這些權限時，撤銷這些權限。
- 確保充分的認證，使用嚴謹的密碼，定期更換密碼。
- 啟用雙重認證（如有）。
- 更改預設配置和設置，如用戶名稱和密碼。
- 啟用帳戶鎖定機制，防止過多的無效登入嘗試和暴力攻擊。
- 停用或刪除不必要的用戶帳戶（如訪客、演示戶口）。
- 只允許受信任的互聯網規約地址或/和獲授權的設備接達物聯網裝置或後台系統（如建基於雲端的伺服器）。
- 只允許經授權的人員實際接達物聯網裝置。
- 在傳遞和儲存過程中保護使用者憑證（如加密）。
- 在可行的情況下，禁用不必要的服務或邏輯埠（如遠程登入）和實體埠（如通用串列匯流排）。
- 在傳輸層保安和其他規約協商過程中，盡可能使用證書進行設備認證和保密，並在集成其他接達控制機制時，支援各種身份綁定。
- 確保支援公開密碼匙基礎建設的標準服務，如撤銷檢查、信任管理、程式註冊和登記，以及事故復原。

5.4 加密方法

在物聯網環境中，加密技術是不可或缺的，如果實施得宜，加密技術可以為認證性、機密性、完整性和不可否定性提供保安保證。加密技術被廣泛用於保護儲存或傳輸數據的機密性。如果敏感資料需要存儲在物聯網裝置中，必須進行加密。數碼簽署或訊息認證碼則用以核實儲存或傳送敏感或保密數據的真確性或完整性。決策局／部門應利用加密技術，以保護物聯網環境中的數據、系統、設備及它們之間的通訊。應考慮以下常見的保安措施、控制和做法，但並非詳盡無遺：

- 選擇在設計上已支援加密功能（如加密、公開密碼匙基礎建設等）的物聯網裝置。
- 使用加密規約來加密對等裝置、智能流動裝置應用程式、雲端服務和應用程式界面之間的任何通訊。
- 加密在不受信任的網絡上儲存和傳輸中的敏感資料。
- 使用標準的、可信任的、加密演算法以及嚴謹的密碼匙長度（如 AES -256）進行資料數據加密。
- 正確管理和使用加密密碼匙；避免在多個端點使用同一加密密碼匙。

5.5 實體和環境保安

對於物聯網裝置，須根據物聯網裝置儲存、處理和傳遞的資訊的保密分類實施保安控制，防止裝置遺失、被盜和損壞。

物聯網裝置和相關網絡設備應得到妥善管理、選擇適當的位址和保護，以降低不利環境和未經授權的實體接達的風險。攻擊者可能會利用物聯網裝置的實體漏洞對在同一網絡上的其他端點進行破壞。

對於使用中的物聯網裝置，決策局／部門應避免在這些物聯網裝置收集和儲存保密資料。如因為業務需要處理保密資料，應將數據加密並傳遞至保安控制措施符合相關政府保安要求的安全後端儲存。如因業務需要而無可避免地將保密資料儲存在沒有人員看管的物聯網裝置，則在偵測到並確認實體保護遭到嘗試入侵時，須實施適當的實體保護和輔助措施（如刪除數據、中斷網絡連接）。

應考慮以下與物聯網裝置實體保安相關的常見保安措施、控制措施和作業模式，但並非詳盡無遺：

- 為物聯網裝置和相關設備提供足夠的實體保護和檢測措施和控制（如鑰匙鎖、入侵偵測系統、警報或監控系統等），當特別安裝在公共區域或無人看管的位置時，可以檢測到實體竄改。
- 正確選址和妥善安裝物聯網裝置，並採取足夠的實體措施和控制措施，可以有效地保護物聯網裝置免受遺失、被盜、服務中斷、數據攔截或被實體攻擊或破壞。
- 保護電力和電訊導線不被攔截、干擾或損壞。
- 確保物聯網裝置和設備不容易被拆解。
- 限制通過實體界面或埠直接接達物聯網裝置。
- 啟用任何實體接達的詳細日誌，如通用串列匯流排埠。
- 禁用所有不必要的實體界面和埠，包括那些用於調試的界面和埠。

5.6 操作保安

決策局／部門須確保物聯網組件及其環境的操作保安。下列措施是必要和有效的保安措施，包括防範惡意軟件、記錄資訊科技流程和事件、監察可疑活動、防止技術性保安漏洞被利用等。以下為一些與物聯網操作有關的常見保安措施、控制措施和作業模式。這些措施和做法都應予以考慮，但並非詳盡無遺：

<u>操作程序和責任</u>

- 訂立和備存物聯網裝置、相關系統和網絡的操作程序。該程序是逐步的操作指令（如物聯網裝置和系統的安裝和配置、資料的演算和處理等）。
- 應用最少功能原則來管理物聯網裝置、相關系統和網絡。刪除和限制所有不必要的功能、服務或組件。

<u>防範惡意軟件</u>

- 啟用促使對所有物聯網端點的反惡意軟件保護，包括物聯網裝置、後端系統、流動裝置等。
- 須定期更新惡意軟件定義和偵測及修復保護引擎。

漏洞管理

- 及時在物聯網端點上安裝由產品供應商所提供最新的保安修補程式和更新固件，或實施其他補償保安措施。
- 在應用物聯網裝置之前，認證完整性和真實性，並測試製造商提供的保安修補程式和固件。
- 界定並維持一份授權軟件或應用程式的清單。
- 在使用開源軟件或代碼(如庫、資料庫和應用程式界面等)之前，核實和評估風險(如程式錯誤、保安性漏洞或後門)和影響。

雲端數據和通訊保安

- 加密儲存在雲端中的數據以及雲端與其他端點之間的通訊。
- 正確管理和保護加密密碼匙的整個生命週期。當儲存的數據被認為是敏感時，考慮使用硬體保安模組來保護加密密碼匙操作。

記錄和監察

- 根據其業務需要和保密類別，定義和覆檢與物聯網裝置和相關資訊系統活動記錄相關的政策。
- 保存活動記錄的時間應與其作為審計工具的時效相稱。
- 保護活動記錄，防止未經授權的接達和篡改。
- 定期檢查活動記錄的完整性。
- 持續不斷並即時監控物聯網端點和相關網絡通訊。這可以幫助及時檢測和跟進異常或可疑活動。

物聯網裝置保安

- 當需要高保安級別的物聯網裝置，保安晶片是首選組件。這能強制執行保安啟動，以防止未經授權的固件、引導載入器或引導映射更新。
- 使用包含保安功能的硬體，以加強對設備的保護和完整性。

5.7 通訊保安

由於物聯網裝置能夠通過有線或無線連接與其他設備和系統進行通訊，因此應採取充分有效的保安措施和控制措施來應對相關的保安威脅和攻擊。

對於連接到政府內部網絡的物聯網裝置，如果沒有採取適當的防禦措施，就能成為一個保安漏洞點，如泄露保密資料、向政府內部網絡傳播惡意軟件、或當被攻擊者感染時，發起分散式拒絕服務攻擊。

除非得到決策局／部門的適當批准，否則用戶不得將已連接到政府內部網絡的物聯網裝置連接到外部網絡。

應考慮以下與物聯網裝置通訊保安相關的常見控制措施和作業模式，但並非詳盡無遺：

- 網絡應盡量簡單和可靠（即把「安全」網絡與其他網絡的網絡界面點減至最低）。
- 設立物聯網裝置及相關網絡設備的網絡圖、邏輯位元址和實體位元址、配置等網絡資訊，以反映最新、全面的網絡環境，以便進行有效的保安控制措施和事故應變。
- 通過實體或邏輯手段將網絡劃分為獨立的網絡域，當保安性漏洞發生時，將影響降到最低。
- 確保組件/層級（即物聯網裝置、網絡設備、後端系統/儲存和應用）之間的通訊保安。
- 限制和控制所有的網絡通訊和連接（如通過防火牆規則、媒體接達控制地址過濾等），只允許獲授權的出入通訊以及連接到適當的網絡設備。
- 停用所有不必要和不安全的網絡服務（如遠程登入、檔案傳送規約等），並使用保安規約（如保密外殼、保密檔案傳送規約等）。
- 在有線和無線通訊中啟用加密功能。
- 在網絡傳輸前，用標準的、可信的加密演算法對數據進行加密。
- 在接達網絡服務和裝置到裝置的連接時，確實執行嚴謹的認證。
- 對於裝置與裝置之間的連接，在初始配對過程中需要使用者互動，以避免意外配對給未經授權的遠程方。在初始配對過程中，在提供正常服務之前，應將預設的無線密碼從出廠預設值更改，或重新設置密碼。

- 建立零信任網絡1和/或安全接達服務邊緣2的框架，以控制對物聯網系統的授權和安全接達。
- 考慮實施入侵偵測系統，以檢測異常活動、虛假設備和潛在的資訊保安事件，以及實施入侵防禦系統通過阻止可疑通訊來防止惡意攻擊。資料分析和深度資料包檢測有助從物聯網裝置產生的數據中識別威脅和異常情況。

5.8 系統購置、發展及維護

現今的資訊技術環境中，保安是不可或缺的。如果保安意識和措施不足，會嚴重影響資訊科技基礎設施、業務營運和聲譽。對於物聯網相關的應用、系統和裝置，保安應該是整個系統開發生命週期中不可或缺的一部分。在系統開發生命週期的早期階段就應該考慮保安問題，以便更好地管理保安風險和相關問題。設計層面的保安是實現這目標的一種方法。物聯網保安應有自己的需求，並納入系統需求中。應根據政府、法律和規管以及業務要求，正確和明確地定義這些要求，以確保系統、設備和資料的機密性、完整性和可用性。

政府資訊科技保安政策及指引所載的保安規定適用於與物聯網有關的系統和裝置。決策局／部門應遵守《基準資訊科技保安政策》和《資訊科技保安指引》第 16 節 - 系統購置、發展及維護的規定。

此外，保安覆檢應在設計階段進行，可以確保系統已分辨及納入必要的保安要求，評估和處理相關的保安風險和影響，以有效促進系統發展生命週期的後續階段。

對於物聯網相關的應用程式、系統和設備，須進行保安風險評估和審計，對保安審計中發現的風險進行核實，確保生產前採取適當、充分的保安措施。

應考慮以下與購置和發展物聯網應用相關的常見保安措施、控制和作業模式，但並非詳盡無遺：

[1] 零信任網絡所指的保安概念是指不會基於物理或網絡位置（即局部區域網絡或互聯網）就給予用戶、資產或服務的信任。 在授予接達權限之前必須嚴格執行授權和驗證。評估接達請求後，僅根據用戶身份和職務授予最小特權接達。在授予接達權限之前，必須嚴格執行授權和身份驗證。 評估接達請求後僅根據用戶身份和角色授予最小權限接達。

[2] 安全訪問服務邊緣是指結合了廣域網絡功能和網絡保安功能的網絡體系結構以提供服務，例如保安網頁通訊閘，雲端接達保安代理，防火牆即服務和零信任網絡接達。

- 根據保安政策和指引，以及部門的資訊科技政策，界定和覆檢保安要求，例如數據和系統接達控制(例如認證方法)、密碼管理(例如加密演算法、密碼匙保護)、保安漏洞管理(例如固件的可用性、服務供應商／製造商提供的保安修補程式)、通訊規約(例如保密外殼、TLS、HTTPS)、備份策略。
- 識別持份者(如資料擁有人、系統擁有人)，確定並記錄他們的角色和責任。
- 應實行更改控制。對系統配置或程式碼的更改應遵循規定的程序，以保持完整性和可靠性。
- 在規定的時間段(如在提供正式服務前，以及在進行大規模升級和變更前)對系統和應用程式進行保安風險評估。測試、覆檢和執行適當的保安措施，並確保其有效性。

<u>物聯網相關系統和裝置購置</u>

- 應開展調查研究，評估適合並滿足規定的保安要求的保安機制和功能。
- 選擇已設計、內置或已實現實體和邏輯保安功能的物聯網裝置或系統，如接達控制（如身份認證）、漏洞管理（如固件、保安修補程式）、反惡意軟件保護機制（如防火牆）、加密控制（如加密、可信平台模組），能有效加強對設備、系統和數據的保護。

<u>應用系統設計和開發保安</u>

- 考慮從收集/生成到棄置的整個資料生命週期的保安性。
- 確保並保持應用程式的完整性（如通過版本控制機制，分離開發、系統測試、驗收測試和實際運行的環境）。
- 避免收集和儲存不需要的敏感資料。
- 避免在物聯網裝置中收集和儲存保密資料。
- 在所有設計文件中記錄資料項目、保密類別級別及其保護機制。
- 根據全球認可的保安標準（如 OWASP）檢查網上應用系統和應用程式界面服務。
- 通過網上應用系統防火牆保護網上應用系統和應用程式界面服務。
- 認證網上應用系統和應用程式界面服務的數據輸入。
- 在網上應用系統和應用程式界面服務中使用加密技術來保護傳輸中的資料。
- 在網上應用系統中認證身份，並啟用會話超時的應用程式界面服務。
- 加密在流動應用程式與後台雲端應用系統或物聯網裝置的通訊。

- 當儲存的資料被認為是敏感資料時，加密資料並考慮雙重認證。

5.9 遵行要求

決策局／部門須避免違反與保安要求相關的法律、法定、規管或合約責任。決策局／部門除了考慮本地的法律及法定外，亦應考慮其他國家或地區的相關法律或法令的適用性，特別是在個人資料及私隱方面。如有需要，建議決策局／部門尋求專業或法律意見。保安措施須根據相關保安要求推行及操作。

就物聯網裝置部署而言，決策局／部門可考慮採用現成的雲端服務，以用於物聯網後端系統/儲存或應用。決策局／部門購置雲端服務前，應仔細研究和瞭解雲端服務的範圍、內容、合約條款和條件、責任和限制、使用政策等。決策局／部門在選擇解決方案時，應評估相應的保安措施和控制措施是否符合政府的保安要求，特別是處理保密/敏感的數據。此外，決策局／部門應注意雲端服務的資訊系統和儲存的資料可能位於香港以外的地區，亦因此受海外法律所規管。

關於雲端服務及相關保安考慮，請參考 ITG InfoStation 上的《雲端保安實務指引》
https：//itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml。

關於外判服務的保安性，請參考《基準資訊科技保安政策》和《資訊科技保安指引》第 17 節--外判資訊系統的保安。

<u>文件資料</u>

決策局／部門須保存記錄，以證明遵守保安要求的情況，並支援對有效執行相應保安措施的審計。保安風險評估和保安審計的報告或記錄結果，可視為適當和可接受的證明。由於保安風險評估和保安審計是持續進行的程序，有關記錄可作為參考，以便進行下一次評估或審計，以及採取進一步的跟進行動。

應檢查遵守保安的條例和政策的情況，並將其明確納入服務合同的規格和規約中。審計員為檢查遵守要求而提供的審計報告，應確保對資訊科技保安政策、資產管理、接達控制、密碼學、實體保安、操作保安、通訊保安、系統發展和遵守情況，已有適當控制。

數據保護、個人資料和私隱

決策局／部門須在資料資產的整個生命週期內，從產生或收集、儲存、處理、傳輸到銷毀，對其進行保護。

決策局／部門須根據保密類別對數據進行評估、分類和保護。應明確定義和記錄所有相關持分者的數據擁有權、角色和責任。物聯網的採用通常是由業務需要帶動的。因此，涉及物聯網裝置的資訊科技系統擁有者有責任管理相關的保安事宜。參考《基準資訊科技保安政策》 第 5.3.3 節 有關部門資訊科技保安組織，資訊科技系統的系統管理員可負責涉及物聯網裝置資訊科技系統的日常管理、運作和配置，包括保安監察，以防範保安威脅。另外，決策局／部門在實施物聯網之前，系統擁有人應該已經獲得部門資訊科技保安主任的批准。此外，如涉及物聯網裝置的資訊科技系統將連接到部門網絡，系統管理員可指定由負責監察決策局／部門網絡整體保安的網絡或局部區域網管理員負責監控物聯網裝置。

在處理保密數據方面，決策局／部門須遵守政府的保安規定（例如《實務守則》、《基準資訊科技保安政策》、《資訊科技保安指引》及部門的資訊科技保安政策）。在處理個人資料方面，除政府的保安規定外，決策局／部門亦須遵守本地的法律規定(例如《個人資料(私隱)條例》)及海外的資料保障法令或規例(例如《一般資料保護規範》)(如適用)。

為了保護物聯網運作或環境中的數據，決策局／部門應考慮採取全面的方法，根據其使用情況和業務環境，透過行政（例如部門的資訊科技保安政策及程式）、邏輯（例如加密、接達控制）或／及實體（例如位於上鎖的房間）的措施或控制，以及遵守政府的保安規定，保護數據免遭未經授權或有意圖的邏輯及實體接達、遺失或盜用。

有關個人資料和私隱的法例或問題，請參考本文件第 6 節--個人資料保護的考慮。

保安覆檢

物聯網相關資訊系統(如後端伺服器/儲存)或應用系統(如流動應用程式、網上應用系統)的保安風險評估和保安審計須按照政府的保安要求，每隔一段時間進行一次。

- 保安風險評估

  保安風險評估是一個識別、分析和評估保安風險的過程，並確定將風險降低到可接受水準的緩解措施。

  與傳統資訊系統和應用系統類似，與物聯網相關的資訊系統和生產應用系統至少須每兩年進行一次風險評估，並須在提供正式服務前，以及在進行大規模升級和變更前。決策局／部門應確保妥善評估和處理在風險評估期間發現的物聯網系統和應用系統的風險。

  對於處理敏感資料並安裝在公共區域的物聯網裝置，須進行保安風險評估，評估資訊系統和數據資產的保安風險，並須採取足夠的保安控制措施，特別是實體保安措施，以保護數據。

  除資訊系統及應用系統的保安評估外，其他保安範疇(例如物聯網基礎設施、物聯網組件／層之間的連接等)也應採用保安評估，以覆檢和評估潛在的保安風險。因此，決策局／部門應考慮善用保安評估來發現和處理其業務環境和運作中的保安問題。此外，為物聯網組件進行保安評估的專業人士，應具備豐富的物聯網運作及保安實務經驗。

- 保安審計

  保安審計是認證過程或事件中遵守保安性原則或標準的程度，作為確定現有保護的整體狀態和認證現有保護是否正確執行的依據。

  應由足夠具備相關的物聯網保安運作、管治及合規方面的知識、技能及經驗的審計師定期進行保安評估。決策局／部門應確保其物聯網組件受到妥善保護，並符合政府和部門的資訊科技保安政策。

有關保安風險評估和審計的詳情，請參閱 ITG InfoStation 上的《保安風險評估與審計實務指引》
https：//itginfo.ccgo.hksarg/itcontent/itsecure/docs/Guidelines/DocRoadmap.shtml。

6. 個人資料保護的考慮因素

物聯網裝置可能會收集、監察或分析與個人有關的各種數據。建議決策局／部門在系統設計階段採用「設計層面的私隱」，以避免過度收集個人資料。決策局／部門應清楚通知用戶將會收集的個人資料的種類、收集的目的、個人資料的潛在受讓人，以及為保護個人資料而採取的保安措施。

決策局／部門在處理個人資料時，須確保遵守《個人資料(私隱)條例》，特別是保障資料原則 4(個人資料的保安)。決策局／部門亦應留意其他經濟體系的規管架構（例如歐盟公佈的《一般資料保護規範》）可能造成的影響。防止個人資料外泄及濫用的考慮因素包括但不限於：

- 盡量減少收集個人資料。
- 對物聯網裝置採用「設計層面的私隱」。
- 實施適當的保安措施，如加密個人資料並將其傳輸到安全的後端儲存，並執行嚴謹的密碼以防止帳戶被劫持。
- 對個人資料進行去身份識別或匿名化處理(如適用)。
- 當不再需要時，安全地銷毀個人資料。

7. 物聯網裝置的應用案例

物聯網裝置可以放置在廣闊而多樣化的領域。物聯網裝置收集和處理數據的位置是其保安性的關鍵，因為在辦公環境和在公共區域的保安控制措施是完全不同的，特別是在實體保安控制措施這範疇。 另外一個關鍵是涉及數據的保密分類。在購置前，決策局／部門應研究潛在供應商的物聯網裝置所具備的保安功能，以期得到最高保安水平的物聯網裝置。物聯網裝置應避免在設備本身儲存數據，尤其是敏感資料。應該有適當的保安保護數據收集和傳輸到後端儲存。為保護物聯網裝置中收集/處理/儲存的資料，應遵循相關政府保安規例、政策和指引，這些規例、政策和準則對保護保密資料有具體要求。

本章節將討論以下兩個部署物聯網裝置的例子，以提供一些有關物聯網保安的一般指引，供決策局／部門在不同的情況下作參考。

I. 在公共場所安裝的物聯網裝置（案例一）
II. 辦公環境中安裝的物聯網裝置（案例二）

7.1 宏觀物聯網參考模型

下圖展示了一個宏觀的物聯網參考模型，其中包括上述兩個部署案例。下文各節將對每個部署案例進行詳細說明。

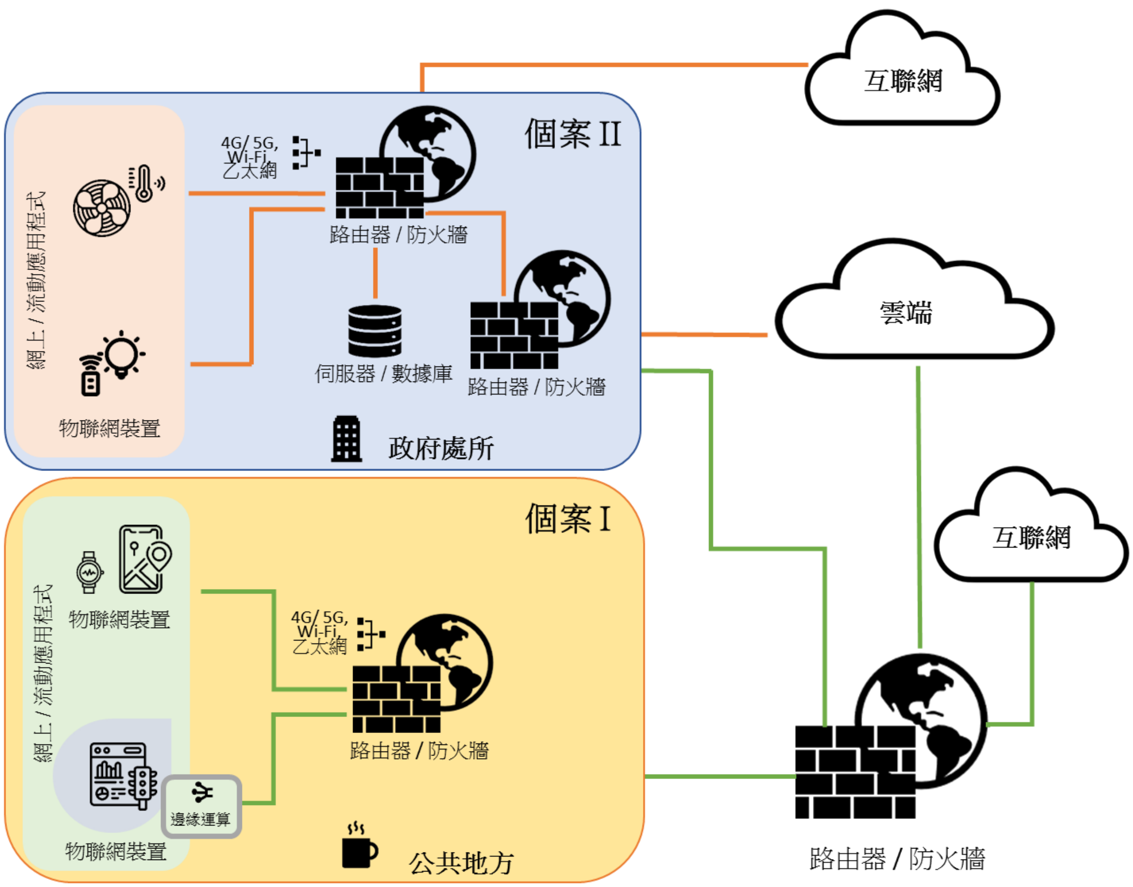

圖 7.1 宏觀物聯網參考模型

7.2 公共區域安裝的物聯網裝置（案例一）

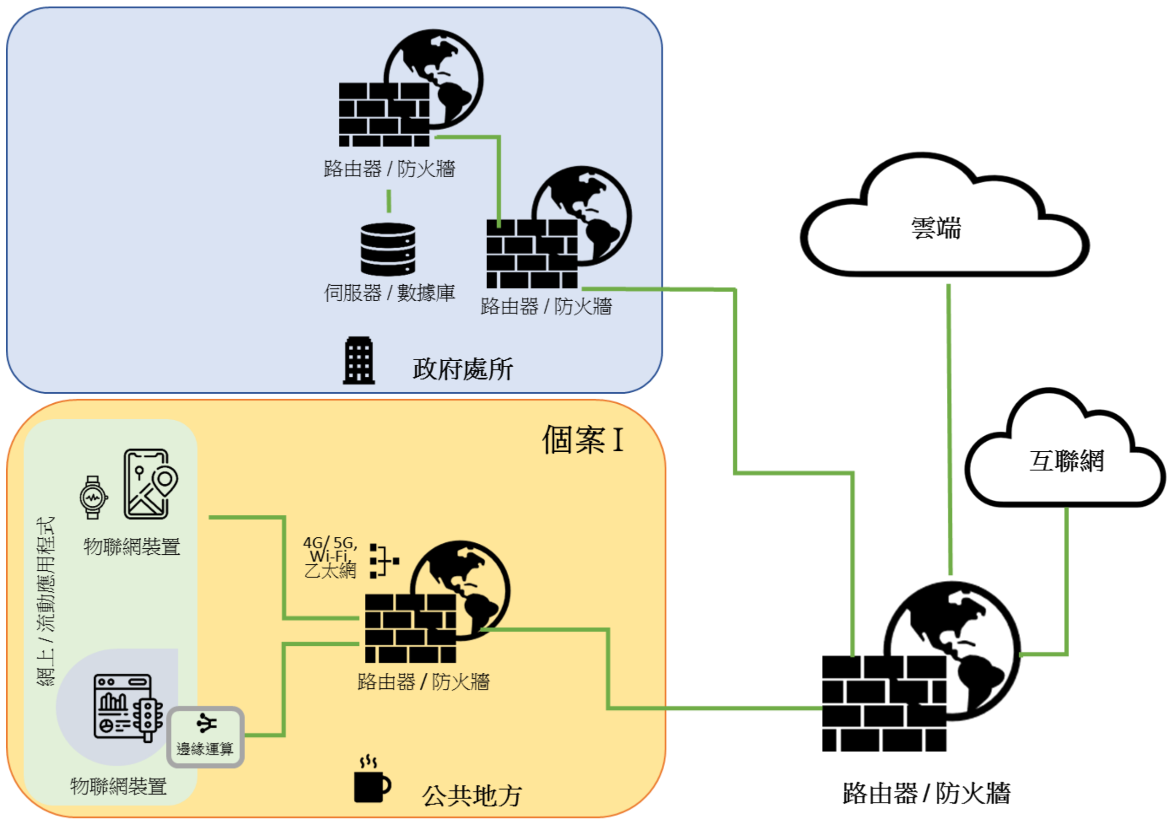

圖 7.2 物聯網部署案例一 – 公共區域

對於案例一，物聯網裝置安裝在公共區域。 它們相互連接或連接到路由器，以接達雲端或互聯網獲取服務或儲存數據。物聯網裝置也可能通過路由器、防火牆或雲端間接連接到政府內部網絡。

由於這類裝置，尤其是物聯網裝置產生的數據量增長得非常快，即時數據可能會出現延遲問題，影響應用的性能。在某些情況下，引入邊緣運算以提供對行動/資料的即時回應。邊緣運算的部署是為了使計算和儲存更接近設備和創建資料的位置，以提供高效的資料處理從而降低延遲。用於物聯網應用的邊緣運算在業界越來越受歡迎。數據處理，如聚合、複製和去識別化，以及一般的物聯網功能，如傳感和保安管理，都可能受益於邊緣運算，以提高物聯網系統的服務水準。

邊緣運算在物聯網系統中起著安全保護的重要作用。在邊緣設備上實施入侵偵測系統或入侵防禦系統可以抵禦分散式阻斷服務、暴力攻擊等可能的攻擊，方法是進一步提高攻擊的檢測率並增強對物聯網基礎設施的惡意企圖的防禦能力。應全面保障物聯網系統的保安，在邊緣結點施行資料認證、接達控制、修補程式更新、防止網絡攻擊等保安控制措施，並確保資料保護得到備存。必須遵守邊緣設備上的安全要求。

由於在這個部署個案中，物聯網裝置既沒有員工看管，也沒有安裝在有實體保安的地方，因此無法保證有效的實體保安保護。在這情況下，決策局／部門應避免收集敏感資料。如因業務需要無法避免，則決策局／部門不應把敏感資料儲存在物聯網裝置內，以減低資料外泄的風險。如需要儲存數據，則應將數據加密，並傳輸至安全的後端儲存庫，而該儲存庫的保安控制措施應符合政府的相關保安要求。如因業務需要而無可避免地在沒有員工在場的情況下把保密資料儲存在物聯網裝置中，決策局／部門須採取適當的實體保護措施，並在發現和確定有人試圖入侵實體保護時，採取輔助控制措施，例如遠端或自動刪除數據、中斷網絡連接等。

另外，設計良好的網絡對於保障物聯網的系統保安至關重要。一組物聯網裝置應該由一個具有適當接達控制的閘道進行分組和分段。物聯網裝置絕不應直接連接到內部網絡。應配置非軍事區，將內部網絡與外部網絡分開，藉此隱藏內部網絡的資料。應實施網絡分段，以降低來自物聯網裝置的違反保安事項的風險。

7.2.1 應用系統界面的保安建議

支持物聯網的解決方案通常建立在常見的應用系統界面上，如雲端、流動或網絡平台。這些常見的應用系統形成了一個物聯網生態系統。對物聯網生態系統的任何威脅都可能導致物聯網裝置或其相關組件受損。常見的問題包括缺乏認證/授權、缺乏或使用較弱加密等。下面的章節列出一些與這些應用系統界面有關的注意事項。

<u>雲端界面</u>

這類系統通常會用雲端資料庫、雲端儲存平台和雲端服務來構建物聯網解決方案。在採用物聯網技術的過程中，採用雲端服務會增加保安風險，如缺乏可視性和控制、共有的技術漏洞以及不安全的界面等。以下是保護雲端環境中物聯網裝置的保安控制措施，包括但不限於：

- 確保對所有雲端界面進行保安漏洞覆檢。
- 盡可能啟用 HTTPS。
- 加密儲存在雲端中的數據以及與其他端點之間的通訊。
- 妥善管理和保護密碼匙的整個生命週期。當儲存的數據被認為是敏感時，考慮使用硬體保安模組來保護加密密碼匙。
- 盡可能採用雙重認證方案。
- 盡可能啟用網上應用系統防火牆。
- 如果系統有本地或雲端的網上應用系統，將預設密碼改為嚴謹的密碼，預設用戶名稱也改為嚴謹用戶名稱。
- 啟用帳戶鎖定功能。
- 啟用嚴謹的密碼（如果提供）。
- 執行定期更改密碼，例如每九十天。

<u>流動界面</u>

物聯網應用系統負責提供應用服務。 在大多數情況下，使用者主要通過網上應用系統和流動應用程式與該應用系統進行互動，安排應用系統數據的收集、處理、分析和儲存。物聯網系統的流動界面需要有針對性的保安防禦，如：

- 使用個人辨認號碼或密碼來提供額外保安（在用戶端和伺服器上）。
- 盡可能使用雙重認證。
- 啟用帳戶鎖定功能。
- 啟用嚴謹的密碼（如果提供）。
- 強制定期更改密碼，例如每 90 天更改。
- 加密與後台雲端應用系統或物聯網裝置的通訊。
- 不要在流動應用程式中輸入非絕對需要的敏感資料，如地址、出生日期、信用卡等。
- 將敏感資料(如個人資料、使用者憑證、加密密碼匙等)存放在保安的儲存場所，並採取符合相關政府保安要求的保安控制措施。

<u>網頁界面</u>

與流動應用程式界面一樣，網頁界面是使用者與物聯網互動的另一個主要界面。網頁應用系統界面被認為是主要的攻擊面之一，需要實施有效的保安措施，如：

- 盡可能啟用 HTTPS。
- 盡可能使用雙重認證。
- 如果可能的話，啟用網上應用系統防火牆。
- 更改默認的用戶名稱和密碼。
- 啟用嚴謹的密碼（如果提供）。
- 啟用帳戶鎖定功能。
- 進行完善的網絡保安標準檢查，以降低風險。
- 如果系統有內部或雲端的網上應用系統，確保將預設密碼更改為嚴謹的密碼，如果可能，也更改預設用戶名稱。
- 如果系統具有帳戶鎖定功能，確保啟用該功能。
- 考慮採用防火牆等網絡分段技術，隔離物聯網系統與關鍵資訊科技系統
- 啟用會話超時。

7.3 辦公環境中安裝的物聯網裝置（案例二）

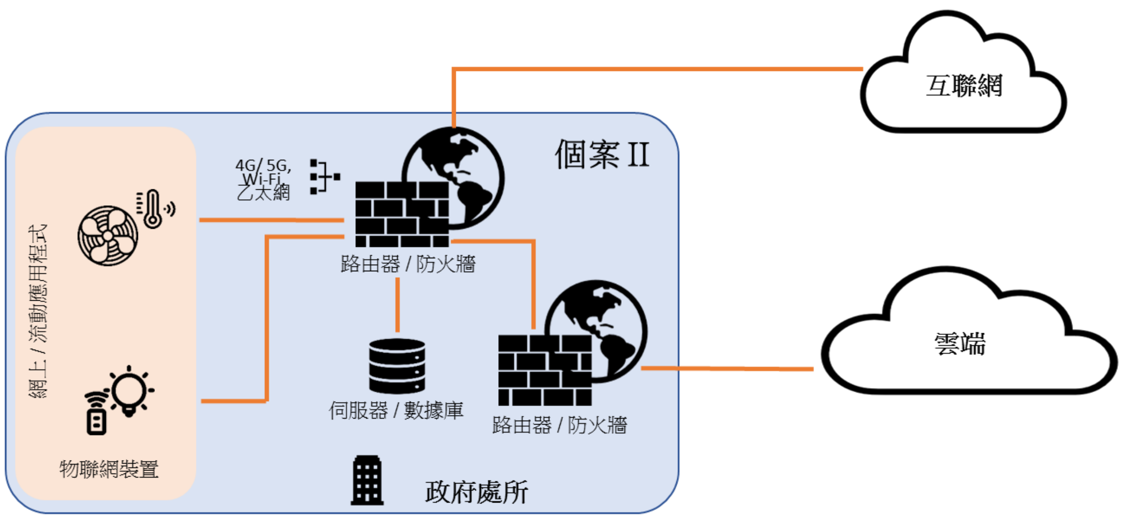

圖 7.3 物聯網部署案例二 – 辦公環境

對於案例二，物聯網裝置部署在辦公環境中，用於支援業務營運。物聯網裝置可以連接到部門網絡。物聯網裝置可以通過防火牆連接到雲端進行數據處理或儲存。由於物聯網裝置安裝在辦公環境中，須加以保護，避免收集敏感資料或被入侵成為攻擊內部網絡的跳板。辦公環境中的工作站和端點應考慮的因素包括但不限於實體保護、接達控制、網絡分段、加密保護、

記錄管理、裝置管理（例如使用保安修補程式和固件升級、惡意軟件偵測和預防），以及數據保護（尤其是個人資料）方面的要求。

從保安的角度來看，應盡可能採用最少功能和最少權限的原則，並設有防範惡意軟件的保護機制。決策局／部門需要評估所需的功能，並停用任何不必要的功能和連接埠，以避免收集敏感資料和連接未經授權的設備或網絡。如果可能的話，應將允許的服務／連接列為白名單。由於物聯網裝置與流動裝置有某些相似之處，例如連接性、流動性和體積細小，政府保安文件中對流動裝置的保安要求和原則，應同樣適用於物聯網裝置。

此外，由於物聯網裝置即使在辦公環境中也可能無人看守，因此應實施實體保安控制措施，防止遺失、盜竊和損壞。使用者應該明白，他們的設備只允許連接到批准的網絡和設備。應確保連接寬頻或 Wi-Fi 的網絡是安全的。

與個案一相似，決策局／部門應避免收集敏感資料。如因業務需要而無可避免，決策局／部門不應把敏感資料儲存物聯網裝置內，以減低資料外泄的風險。如需要儲存數據，則應將數據加密，並傳輸至保安的後端儲存庫，而後台儲存庫的保安控制措施應符合政府的相關保安要求。

7.3.1 部署物聯網裝置的示例

以下是在不涉及敏感資訊的情況下通過 Wi-Fi 網絡連接到互聯網來安裝物聯網裝置的示例。首先，應採取整體和深層防禦的方法。一般來說，應考慮以下三個部分：

- 寬頻路由器
- Wi-Fi 路由器
- 智能裝置

<u>寬頻路由器</u>

寬頻路由器位於本地網絡和互聯網之間，是抵禦駭客、惡意軟件和病毒的第一道防線。在網絡層面上，決策局／部門應確保物聯網裝置不會連接到辦公室網絡，並應考慮在互聯網通訊閘(例如寬頻路由器)限制所有對本地網絡(例如 Wi-Fi 網絡)的存取。除了將寬頻路由器放置在保安區域外，建議正確配置和利用寬頻路由器的保安功能，包括但不限於：

- 改變出廠預設設置（如用戶名稱、密碼、服務設定識別碼等），使用嚴謹的密碼進行認證。
- 保持固件的更新，並從製造商網站下載更新的固件。
- 啟用防火牆功能。
- 啟用媒體接達控制地址過濾功能，限制可以加入網絡的設備。
- 啟用劃一資源定位址過濾，防止用戶接達特定網站。
- 停用已知保安問題的服務/功能，如
    - WPS (Wi-Fi Protected Setup)，允許在沒有密碼的情況下連接網絡。
    - 遠端系統管理。
    - 通用隨插即用，允許自動連接未經授權的設備。
    - 不安全的規約（遠程登入、檔案傳送規約等）。
    - 網絡服務。
- 關閉服務設定識別碼廣播。
- 啟用拒絕服務保護功能，停用支援埠掃描服務。
- 啟用記錄，並進行定期檢查。

<u>Wi-Fi 路由器</u>

決策局／部門應注意，Wi-Fi 網絡會被其他端點共用，以接達寬頻。一旦端點或智能設備受到感染，便會有保安風險。惡意程式碼會在同一網絡內傳播，而其他端點亦會受到感染。因此，建議將智能設備與其他端點設備隔離在一個與部門網絡隔離的網絡（例如訪客 Wi-Fi 網絡）中，該網絡可配置不同的服務設定識別碼、認證方法，並只允許接達互聯網，但不允許連接至內部網絡。隔離的網絡可以有效防止或減低感染的影響。可以的話，這個分離智能設備的 Wi-Fi 網絡以及服務設定識別碼不應廣播，以減少對智能設備以及 Wi-Fi 網絡的攻擊面。 此外，我們亦建議使用最新的 Wi-Fi 標準/規約(例如 Wi-Fi 保護接入 3 (WPA3))及適當的接達控制(例如認證、嚴謹的密碼等)進行 Wi-Fi 通訊，因為據知 WPA2 容易受到 KRACK(Key Reinstallation Attack)的攻擊。

<u>智能設備</u>

為保護端點（如智能設備），應採用最少功能和權限原則，並實施防止惡意軟件的保護機制和防止遺失、被盜和損壞的實體保安控制措施。如果可行，建議：

- 停用未使用或不需要的功能 。
- 停用實體和邏輯埠或服務（如通用串列匯流排埠、局部區域網絡埠、藍牙、從互聯網遠端存取智能設備等）。
- 為智能設備提供固件和作業系統，及安裝應用程式的保安修補程式，使其保持在最新的保安狀態。
- 從可信的程式商店下載並安裝授權的流動應用程式 。
- 只連接已授權的設備到智能設備。
- 不使用時關閉電源。
- 在不需要的情況下，停止互聯網的連接。

最後，建議決策局／部門進行保安風險評估，以識別和評估潛在的保安風險（例如未經授權進入 Wi-Fi 網絡或智能裝置、傳播惡意軟件、 顯示非預期的內容）和影響，然後根據業務需要，決定和實施適當的保安措施和配置，以符合相應的政府保安要求。

完