

英國政府公布物聯網設備安全設計報告及製造商應遵循之設計準則草案



英國數位文化媒體與體育部於2018年3月8日公布「安全設計：促進IoT用戶網路安全（Secure by Design: Improving the cyber security of consumer Internet of Things）」報告，目的在於讓物聯網設備製造商於製程中即採取具有安全性之設計，以確保用戶之資訊安全。此報告經英國國家網路安全中心(National Cyber Security Centre, NCSC)、製造商及零售商共同討論，並提出了一份可供製造商遵循之行為準則（Code of Practice）草案。

此行為準則中指出，除設備製造商之外，其他包含IoT服務提供者、行動電話軟體開發者與零售商等也是重要的利益相關人。

其中提出了13項行為準則：

1. 不應設定預設密碼（default password）；
2. 應實施漏洞揭露政策；
3. 應持續更新軟體；
4. 應確保機密與具有安全敏感性的資訊受到保護；
5. 應確保通訊之安全；
6. 應最小化設備可能受到網路攻擊的區域；
7. 應確保軟體的可信性；
8. 應確保設備上之個資受到妥善保障；
9. 應確保系統對於停電事故具有可回復性；
10. 應監督設備自動傳輸之數據；
11. 應使用戶可以簡易的方式刪除個人資訊；
12. 應使設備可被容易的安裝與維護；
13. 應驗證輸入設備之數據。

此草案將接受公眾意見至2018年4月25日，並規劃於2018年期間進一步檢視是否應立相關法律與規範，以促進英國成為領導國際之數位國家，並減輕消費者之負擔並保障其隱私與安全權益。

本文為「經濟部產業技術司科技專案成果」

相關連結

[DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, Secure by Design](#)

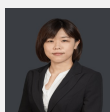
相關附件

[DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, Changing driving laws to support automated vehicles: discussion paper \[pdf \]](#)

你可能會想參加

- 零售業個資安全宣導暨安全維護計畫規劃說明會
- (已額滿)114年「企業營業秘密保護實務座談會」(北部場)-營業秘密因應數位環境之保護風險及管理對策
- 2025科技研發法制推廣活動—科專個資及反詐騙實務講座(實體)
- 2025科技研發法制推廣活動—科專個資及反詐騙實務講座(直播)

- 【台北場1】 通訊傳播事業個資法遵教育訓練
- 【台中場】 通訊傳播事業個資法遵教育訓練
- 【新北場】 通訊傳播事業個資法遵教育訓練
- 【高雄場】 通訊傳播事業個資法遵教育訓練
- 【台北場2】 通訊傳播事業個資法遵教育訓練
- 114年「企業營業秘密保護實務座談會」（南部場）
- 114年「企業營業秘密保護實務座談會」（中部場）
- 114年資訊服務業者個資安維辦法宣導說明會
- 【線上】 資訊服務業個資安維計畫說明會
- 【實體】 資訊服務業個資安維計畫說明會暨交流工作坊
- 【台北場1】 通訊傳播事業個資保護實務專題講座
- 【台北場2】 通訊傳播事業個資保護實務專題講座
- 【台北場3】 通訊傳播事業個資保護實務專題講座
- 金融相關資服業者線上個資安維宣導說明會



柯亦儒

組長 編譯整理

上稿時間：2018年04月

資料來源：

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, Changing driving laws to support automated vehicles: discussion paper (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf (last visited Apr. 13, 2018).

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, Secure by Design (Mar. 7, 2018), <http://www.ntc.gov.au/about-ntc/news/media-releases/ntc-seeks-feedback-on-changing-driving-laws-to-support-automated-vehicles/> (last visited Apr. 13, 2018).

文章標籤

物聯網

資訊安全

推薦文章

