

# Epson 產品的網路安全措施

精工愛普生公司

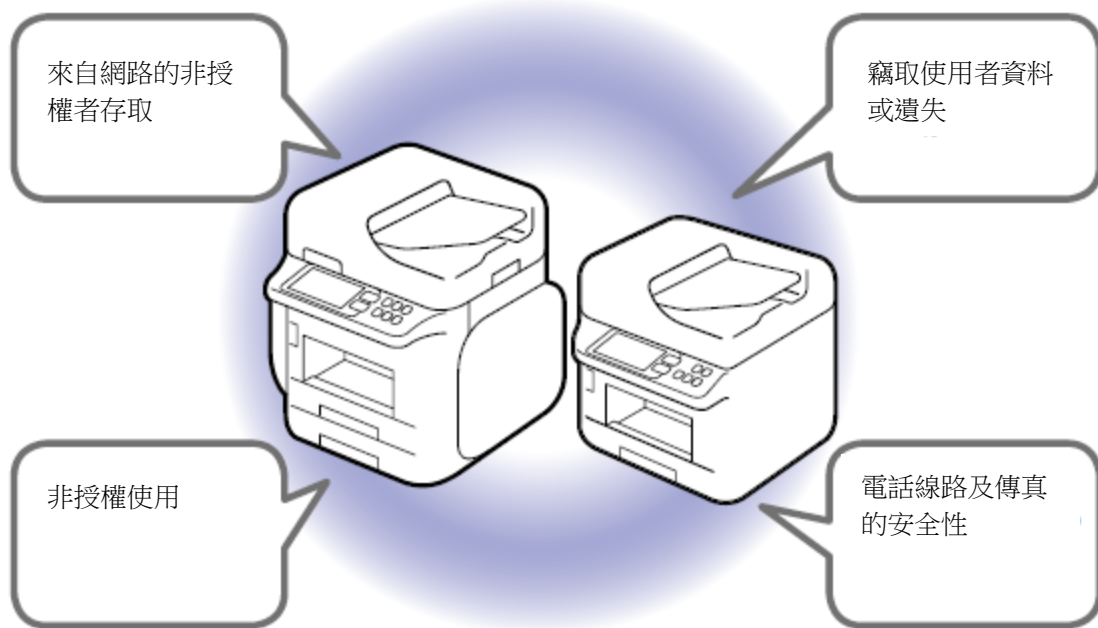
感謝您使用 Epson 產品。

目前 Epson 的多項產品，皆提供連接網路之功能。並且持續強化各式印表機、All-in-one 多功能產品、以及投影機的網路連接功能，藉此努力改善 Epson 客戶的使用便利性。

所有連接網路的產品都需要具有防護的網路環境和適當的安全性設定，以防止各式未經授權的存取及其他外來的威脅。

本文件將說明常見的安全性威脅、Epson 對安全性的處理方式以及重要的安全性措施。

請遵照本文件之說明，建立一個適當的網路環境並啟動安全性設定。



## Epson 對安全性的處理方式

我們針對 Epson 產品的安全性採取以下措施，確保您可以安全且安心地使用產品。

1. 將安全性視為產品品質的基礎。  
我們的產品設計是以提供整個產品壽命的安全性無虞。
2. 主動提供您相關的安全性資訊及專業知識。
3. 不斷地鑽研，建立對抗弱點的對策。
  - 採用業界的標準工具致力於弱點測試，且提供不具弱點的產品。
  - 從產品韌體所使用的開放來源軟體持續監視與弱點相關的資訊。
  - 當發現新的弱點時，我們會迅速對其進行分析並提供資訊與對策。

## 重要的安全性措施

產品出廠的預設值不一定能提供完美的防護。為了確保安全性，請於安裝時閱讀以下各項說明並針對您的使用環境進行必要的設定。

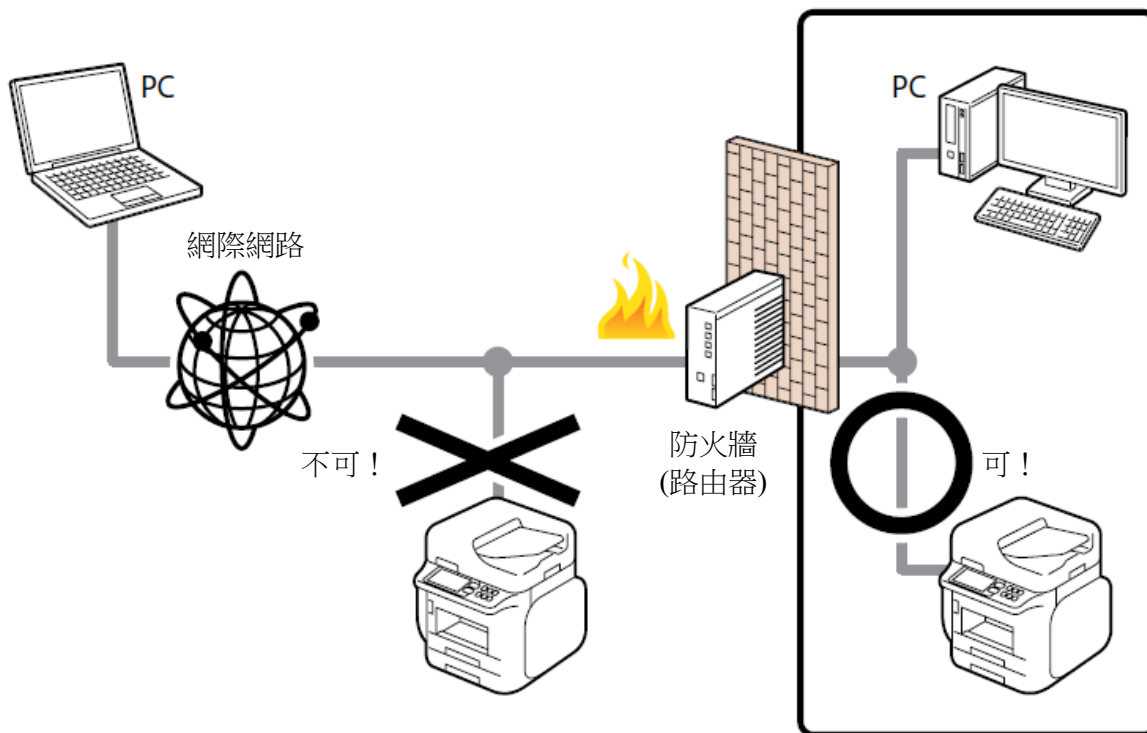
### 1. 管理員密碼

我們強烈建議您在產品上設定管理員密碼。

若您未設定管理員密碼，或您以出廠的預設值設定為管理員密碼，您的產品設定及網路設定可能會很容易被未經授權使用者進行存取，而此盜用者可能更改或盜取您的個人資料，以及如 ID、密碼及通訊錄等機密資料。

### 2. 連接至網際網路

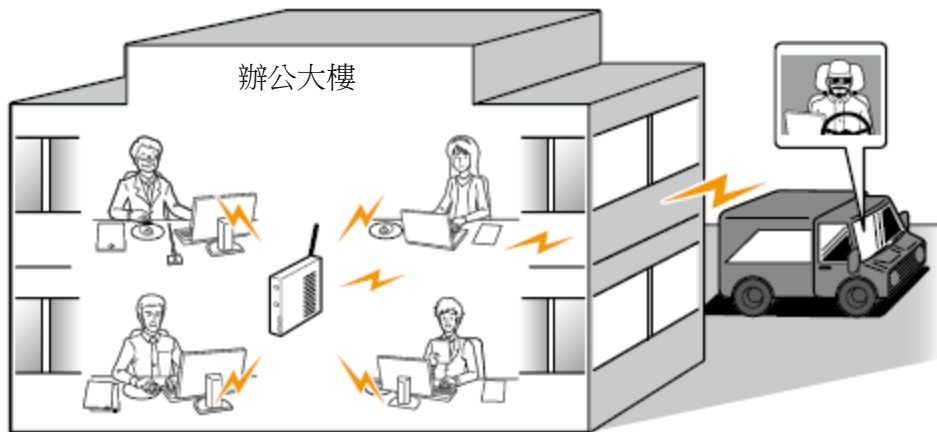
在設有防火牆、無線路由器或非直接連接至網際網路等其他方式保護的網路上安裝產品。當您這麼做時，我們建議您設置並採用私人的 IP 位址及網際網路防火牆（路由器）



Epson 連接網路的產品都包含 WebConfig 網頁型態等管理介面。我們執行弱點測試以藉此盡可能提供不具弱點的產品。然而，直接連接至網際網路的產品，則面臨未經授權者使用以及資訊外露等不可預見的安全性威脅。

### 3. 無線區域網路 (LAN)

無線區域網路的優點是，只要您在訊號範圍內，便可輕易連接網路並從電腦或智慧手機上進行列印。但另一方面，若未適當設置安全性，您將可能容易受到試圖攔截訊號並盜取身分的惡意第三方的安全性傷害。因此，當使用無線區域網路 (LAN) 時，請適當地啟動無線區域網路的安全防護。



請參閱產品手冊中設置區域無線網路的相關說明。  
詳細的網路安全措施，請參考附件《[安全指南](#)》。