

# 城市無線網絡

2009 年 5 月

©香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 城市裡的無線網絡.....	3
促進城市無線網絡發展的要素 .....	3
II. 構建一個安全的城市無線網絡 .....	4
籌劃城市無線網絡系統 .....	4
保護城市無線網絡系統 .....	5
III. 訂立使用城市無線網絡和無線上網熱點接達企業網絡的政策 .....	8
IV. 終端使用者：城市無線網絡使用的最佳作業實務.....	9

## 摘要

現今，覆蓋城市的無線寬頻計劃受到廣泛的關注。越來越多在亞洲的大城市如台北和新加坡，已經部署了遍佈全市的無線網絡。在部署這些大型開放式網絡的過程中，所遇到的挑戰為數不少。城市無線網絡的業務模式（包括託管服務和公私合營模式）和基礎設施技術正快速地發展，本文主要介紹部署城市無線網絡常見的保安問題，也談及解決重大保安問題時所要考慮的措施。隨著城市無線寬頻計劃的發展，機構和公共部門也面臨資訊保安方面的新挑戰。此外，我們還談論機構和個人在資訊保安方面要面對的挑戰，並建議如何迎接這些挑戰。

## I. 城市裡的無線網絡

### 促進城市無線網絡發展的要素

城市無線寬頻計劃現今已得到越來越多的關注。許多大城市已宣佈部署覆蓋全市無線網絡的消息。以下是一些掀起現時城市無線網絡服務浪潮的主要發展動力：

#### 低成本部署

相對舊有的有線網絡而言，部署覆蓋全市無線網絡的成本便宜得多。首先，由於 Wi-Fi 晶片組的大量需求和生產，無線網絡設備的成本已顯著下降。其次，市政府可以利用市區現有的資產，如燈柱和政府建築物，充當無線上網接駁點極佳的天線場地。

#### 設備的互用性

通過 IEEE 和 Wi-Fi 聯盟，使業界主導的無線通訊技術標準化，確保各種設備的互用性更加廣泛。這推動了以標準設備整合而成的各種流動裝置，如手提電腦或個人數碼助理（PDAs），並刺激了無線技術應用的普及。

#### 數碼共融

隨著無線通訊技術變得更加普遍，城市無線網絡被視為數碼共融的催化劑。無線基礎設施能夠為那些低收入家庭提供廉價甚至免費的互聯網接入服務，並且向弱勢家庭提供電腦和互聯網接入服務的計劃。

正因如此，地方政府一直在積極推廣建立覆蓋全市無線網絡的計劃，使之能夠向市民和企業提供高速的互聯網接入服務。根據MuniWireless<sup>1</sup>的調查報告<sup>1</sup>，截至2007年8月1日，在美國有超過400個市鎮正在使用城市無線網絡，或正處於網絡部署/規劃階段。

---

<sup>1</sup> <http://www.muniwireless.com/article/articleview/6279/1/23>

## II. 構建一個安全的城市無線網絡

### 籌劃城市無線網絡系統

城市無線網絡一般是由地方政府當局，或公共部門與私人企業合作經營的。正因如此，公眾往往會覺得這類為廣泛使用者（包括小童）提供之無線網絡服務是安全的，所以，在一個大型的無線網絡項目的規劃階段，分析所有可能的資訊保安問題顯得尤為重要。以下所述範圍可能要加以考慮：

### 攻擊的類型

在規劃城市無線網絡項目時，應加以考慮一些必要的防禦層。城市無線網絡面對相關的威脅可分為三個方面：

1. 攻擊端點
2. 攻擊無線網絡本身
3. 來自無線網絡內部的攻擊

#### 攻擊端點

一旦使用者的手提裝置連接到城市無線網絡，該設備就很容易受到攻擊，如未獲授權的接達或病毒侵入。雖然使用者應該負責保護自己的流動設備，但人們普遍認為網絡提供者（即地方政府）應該有適當的保護措施，而不會遭惡意攻擊。因此，應在網絡上部署適當的基本保障作為第一道防線，以保護用戶的流動設備免受惡意攻擊。

#### 攻擊無線網絡本身

對那些犯罪者和有破壞傾向的人來說，城市無線網絡是一個很吸引人的攻擊目標。拒絕服務攻擊是其中一種可能的攻擊，能停止無線網絡的運作。攻擊者利用無線接駁點（Access Point, AP）的某些保安漏洞，把大量的惡意請求發送到目標無線網絡接駁點，並迫使網絡系統關閉，導致拒絕回應合法用戶的請求。因此，必須實施基本的保安措施，如在網絡邊緣設立防火牆和網絡入侵防禦系統（Intrusion Prevention Systems, IPSs），以防這種類型攻擊的入侵。

#### 來自無線網絡內部的攻擊

城市無線網絡可提供廉價甚至免費的互聯網接達服務，使電腦和互聯網服務供更多人使用。如果網絡系統的資訊保安做得不夠完善，那些存有惡意的攻擊者會利用這些網絡為所欲為。攻擊者把免費使用的無線網絡服務作為一種工具，不但可攻擊沒有適當保護設備的無線網絡服務使用者，還可以採用多種形式攻擊正在使用互聯網的用戶。

## 不正當地使用無線網絡

不正當使用無線網絡是一個值得關注的問題，尤其是通過 Bit-Torrent (BT) 服務 (或類似服務) 獲取色情內容或侵犯版權的作品，都需要予以處理。

## 通訊保密

在沒有任何加密系統的公共無線網絡裡，網絡竊聽是一種讓人不安的資訊保安問題。沒有加密系統，資料通常是以原文的形式傳發，惡意用戶使用簡單易用的小包偷窺工具，就可以在毫無問題下快速地獲取這些被傳送到網絡的資訊。可考慮以加密系統來解決這些問題。然而，在使用者的電腦或流動裝置中啟動加密功能，使人覺得複雜性，可能會減低人們使用無線網絡的興趣。因此，安全與便利兩者之間必須取得平衡。

## 匿名使用者

服務提供者為了充分利用他們的公共無線熱點，很可能允許匿名使用者接達其網絡。有一些城市無線網絡的無線網絡配置細節是公開的，並且沒有用戶的認證要求。這可能使惡意使用者更容易利用無線網絡進行不正當行為。沒有使用者身份的認證，網絡審計追蹤的能力將受到嚴重限制。

## 保護城市無線網絡系統

為了確保城市無線網絡的安全，行政和技術管制是必要的。以下是一些最重要的行政和技術保安措施，用於保護任何城市無線網絡：

## 訂立可接受使用政策

可接受使用政策是訂立一系列的規則，用戶隨著可接受的慣例來使用無線網絡服務，並以聲明概述了違反這項政策的後果。違反政策者通常會被撤銷其享有網絡接達服務的權利，如果他們的活動涉及非法行為，須通知有關當局，例如警方。這項政策還應配合任何資訊保安政策的要求。以下是一些可接受使用政策聲明的普遍元素：

1. 禁止使用

2. 用戶承擔的責任
3. 暫停或終止服務的條件
4. 私隱

## 中央保安和偵測措施

部署必要的網絡安全措施，如防火牆、防病毒解決方案、網絡入侵偵測系統（IDS） / 網絡入侵防禦系統（IPS）、虛假無線接駁點偵測、以及無線的 IPS，以保障使用者免受網絡入侵。設置一個內容過濾機制可以是另一個考慮。為避免使用者自由而不受控制地接達互聯網，服務提供者有必要控制或過濾不雅網站、色情或淫穢內容和提供非法下載的網站。

## 捕獲門戶（Captive portal）

作為一種威懾機制，服務提供者也可以考慮設立一個捕獲門戶，每當用戶透過無線網絡在自己的設備啟動一個新的瀏覽器對話時，登陸頁面便會顯示出來。可接受使用政策會顯示在登陸頁上，以提醒人們正確使用此項服務。

## 用戶認證服務

在設計無線網絡服務時，服務提供者需要為使用者設立一個啟動和停止服務設定識別碼（Service Set Identifier 或 SSID）的認證機制，而此機制亦應有能力追蹤城市無線網絡內入侵者的位置。在 Wireless@SG（新加坡無線網絡），所有使用者的服務在被啟動之前均需要註冊，並輸入自己的姓名、地址和手機號碼。

## 無線加密

為了用戶得到無線界面上的保護，應為他們提供可供選擇的基本無線加密功能如 WPA 及高級加密標準 (AES) 或 WPA2 及 AES 加密。由於部份較舊的網絡設備不支援 AES 加密，因此服務提供者在設計無線網絡服務時應考慮同時提供加密或不加密的無線網絡服務以迎合不同用戶的安全需求。

## 無線網絡接達控制

無線網絡服務的接達控制應被視為網絡的第一層防禦，服務提供者可進行遠端批准或阻止任何無線用戶端設備的接達。這可以幫助遏制發生任何不良影響的保安事故。

## 用戶端隔離

現今大多數已安裝的無線網絡是以「基建模式」(infrastructure mode) 運行，必須利用一個或多個無線接駁點。在此配置模式下，所有的網絡交通都經過這些無線接駁點，通過監測控制這些無線接駁點上的用戶間之通訊，服務提供者可以防止惡意攻擊對易受攻擊的用戶端設備進行接達。

## **實體保安**

無線接駁點或無線界面卡通常含有配置資訊，一旦被竊取，便會對無線網絡服務構成重大威脅。穩妥地把網絡設備，如無線接駁點，安裝在常人不能觸及到有嚴格實體保安控制的地方，這可減少被盜竊的危險。

## **記錄和審計功能**

服務提供者應考慮實行記錄和審計功能，以記錄所有網絡連接的資料，尤其是未經授權的接達。持有授權人員應該定期檢查記錄。

## **保安風險評估及審計**

保安風險評估及審計是檢查無線網絡安全程度的重要方法，用以確定所需的修正措施，維持可接受的保安水平。這些方法有助於識別無線網絡的漏洞，例如使用預設或易猜的密碼和簡單網絡管理規約 (SNMP) 的社群字串的無線接駁點，以及偵測是否已啓動加密功能等。然而，保安風險評估只能揭示資訊系統於某一段時間的部份風險，故在無線網絡運作後，應定期進行風險評估及審計。

此外，應制訂最佳作業實務，包括建立明確的事故應變程序。因為在安全鏈上，互聯網個人用戶往往是最薄弱的環節，所以應該定期向公眾灌輸安全上網的知識和方法。

### III. 訂立使用城市無線網絡和無線上網熱點接達企業網絡的政策

由於 Wi-Fi 熱點的普及和城市無線網絡服務遍及全球，旅客很可能在旅途上也能利用這些服務來連接企業網絡。如果這種遠端接達的保安措施做得不足，這可能會對企業網絡造成一定的保安風險。惡意攻擊者可能會通過某個不知情僱員的帳號，侵入企業網絡，獵取敏感資訊。

機構應加以界定針對使用城市無線網絡服務或公共無線熱點接達企業網絡的保安政策，經常外出工作的員工使用這些服務進入企業網絡時，應該提高警覺。

## IV. 終端使用者：城市無線網絡使用的最佳作業實務

雖然城市無線網絡服務提供方便、甚至免費的互聯網接達，用戶應該採取必要的保安措施，以保護自己免受潛在的破壞和攻擊。以下是給個人使用者的一般性提示：

1. 把城市無線網絡服務視作為不可信賴的網絡，在沒有加密通道（如保密插口層(SSL)）上不要登入敏感的網站。在沒有虛擬私有網絡(Virtual Private Network, VPN)保護或類似的加密機制，不能確保通訊保密的前題下，使用城市無線網絡服務接達公司伺服器是不明智的。在使用VPN時，應該停止使用分割通道技術(分割通道允許用戶在連接到互聯網的同時，也保持另一個VPN的連接)。
2. 當連接到一個公共無線熱點時，用戶可能被導向至一個捕獲門戶的網頁。攻擊者可能會設置虛假的捕獲門戶網頁，以獲取敏感資料。因此，通過核實網站的證書，鑒別捕獲門戶網頁的真偽顯得尤為重要。
3. 有些作業系統可讓用戶創造一個首選無線網絡清單。一旦這份清單確定後，該系統將不斷尋找清單裡的首選網絡，並嘗試自動連接到首選網絡。通過獵取這種個人設備發送出來的資訊，攻擊者可以設置一個虛假的無線接駁點來回應受害者連接首選網絡的請求。這樣，用戶會自動連接到入侵者的無線網絡。為防止這種類型的攻擊，應關閉或移除首選網絡清單功能。
4. 應避免電腦與電腦之間的對等無線聯網。臨機操作模式(Ad-hoc Mode)能使個人無線設備與其它電腦以無線方式直接連接，但這種方式對未授權的連接只提供最低限度的保安。為防止攻擊者獲取資訊，應該關閉這個在個人無線設備的功能。此外，網絡資源分享功能也應該關閉。
5. 在連接到城市無線網絡服務時，為了保護自己的電腦，個人用戶應該安裝和執行帶有最新電腦病毒識別碼的防病毒/防間諜軟件、使用最新的系統修補程式、以及開啓個人防火牆。儲存在任何無線設備裡的敏感和機密資料，應以嚴格的加密演算法進行加密。在公共場所連接到互聯網時，常用的保安措施如開機密碼或系統登入認證、和有密碼保護的螢幕保護裝置程式等也應該使用。