

# 流動技術保安

2011年7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. 管理人員的流動科技保安須知.....	3
簡介 .....	3
商業的趨勢及影響 .....	3
政府的政策及IT管治 .....	4
II. IT業界人員的流動技術保安須知 .....	5
無線網絡的分類 .....	5
實施策略 .....	7
企業的保安考慮及措施 .....	7
III. 終端用戶的流動技術保安須知 .....	9

## 摘要

現今科技一日千里，流動電話、平板電腦和手提電腦均愈趨普及，這些電子裝置的計算功能持續提高，同時又變得越來越細小和輕巧，甚至出現集多種功能於一身的流動電子產品。這些產品讓人類不論身處何方都能夠上網處理自己的數據，例如電子郵件及股票買賣等。

這些流動裝置為我們帶來很多方便，亦影響了傳統的商業運作，保安問題上的考慮是必要的。各機構需要關注流動裝置的保安情況，例如盜竊或遺失、由流動裝置洩漏的公司資料、導致的電腦病毒感染和未獲授權的網絡攔截等。因此，當我們享用新的流動通訊科技所帶來的快捷和便利時，亦要留意設計和執行適當的保安措施，以保障敏感資料不會外洩。

本文將介紹最常見的流動通訊科技以及使用時的保安缺點，此外還為終端用戶提供在使用流動裝置時的個人保安貼士。

## I. 管理人員的流動科技保安須知

### 簡介

桌上電腦和電話傳統上是兩種不同的裝置。現今科技一日千里，兩者的功能已不能清晰劃分。手提電腦和流動電話的結合，形成集運算和溝通功能於一身的手提裝置。流動電子裝置（或流動裝置）是易於攜帶，又能夠在不同地點輕易地儲存及處理大量資料的資訊系統。流動電子裝置的例子包括流動電話、智能電話、個人數碼助理（PDA）、平板電腦和手提電腦。

流動科技可以改變個人的日常生活，現在已可用流動電話來收發電子郵件，甚至通過3G及Wi-Fi的功能設備瀏覽互聯網。

### 商業的趨勢及影響

根據電訊管理局資料顯示，香港在2011年3月的流動電話服務用戶普及率高達194.3%，即有超過1370萬的流動電話服務用戶，以及超過680萬2.5G及3G流動電話服務用戶<sup>1</sup>。另外，資料亦顯示香港現時有超過9000個公共Wi-Fi熱點（2011年5月）提供免費Wi-Fi服務。無可置疑，這些數據表示香港已成為主要的無線城市。

用戶可方便地使用流動裝置接達公共服務和/或機構的應用系統資料，除了簡便快捷，更不受時間地點的限制。然而，有利必有弊，伺服器及客戶端分別受到保安方面的挑戰。本文只集中敘述客戶端，即流動裝置上的保安問題。一般流動裝置上的保安弱點包括：

1. 流動裝置一旦遺失或被盜，儲存在內的重要電子郵件或敏感的個人資料或會外洩。
2. 流動裝置輕巧又多用途（例如儲存及攝影功能），不誠實或未經許可的員工可利用它們作為盜竊公司敏感資料的工具。
3. 電腦病毒也可在流動裝置之間散播。跟桌上電腦軟件一樣，流動裝置應用系統亦有機會出現保安漏洞及錯誤。
4. GSM/GPRS的通訊規定欠缺嚴格的訊號保護，在網絡上較容易被截取。

雖然流動裝置所提供的流動性及網絡功能可增加生產力、縮短溝通時間，要在機構內推行流動科技必須審慎考慮保安問題，也應制訂關於使用流動裝置適當的保安政策。

---

<sup>1</sup> [http://www.ofta.gov.hk/en/datastat/key\\_stat.html](http://www.ofta.gov.hk/en/datastat/key_stat.html)

## 政府的政策及IT管治

香港政府的數碼21藍圖以及「GovWiFi」計劃的執行，顯示流動裝置在商業上的應用將無可避免地大幅提升。然而，使用電子郵件、短訊或話音傳輸等流動科技聯絡他人雖則輕易，但接收非應邀訊息的機會也相應提高。香港政府自2005年起便努力與業界合作，打擊非應邀訊息的問題。在2007年5月修訂「非應邀電子訊息條例」（UEMO），以規管商業電子訊息（CEMs）的發放。此條例涵蓋電子推廣產品或服務訊息，均以文字及預先錄製的話音訊息發放到傳真機或電郵地址<sup>2</sup>。

與此同時，流動裝置亦為各界帶來其它保安問題及風險。舉例說，流動裝置通常有網絡接駁功能，可連接到企業的網絡。如該裝置未經檢查或管理便連接到網絡上，便會導致潛在的保安事故。因此，當企業要採用流動技術，必須制訂清晰的保安政策，針對在使用流動電話／平板電腦／PDAs／手提電腦的保安問題上最低限度的處理手法如下：

1. 流動裝置的實體保安問題：防止遺失及被盜；
2. 流動操作系統問題：採取防禦措施以防範及偵測電腦病毒或惡性程式碼；
3. 流動裝置儲存敏感資料問題：制訂明確的管理政策，平衡資料外洩的風險和便利的需要；
4. 其它技術上的措施：制訂保安程序及措施以保護流動商業應用系統及數據。

---

<sup>2</sup> <http://www.ofta.gov.hk/en/uem/main.html>

## II. IT業界人員的流動技術保安須知

這一節闡述主要的流動技術和通訊規定，包括1G、2G、2.5G、3G和4G、無線區域網絡與無線個人區域網絡（Wireless Personal Area Network, WPAN）。

### 無線網絡的分類

#### 無線寬廣區域網絡

第一代（1G）流動通訊技術於1970年代後期出現，最初是模擬系統，只適用於話音傳輸。80年代末至90年代初，第二代（2G）流動通訊系統面世<sup>3</sup>，話音訊號從此以數碼傳輸，以低成本提供高質素的通訊規定。基於Time Division Multiple Access（TDMA）<sup>4</sup>的技術，Global System for Mobile（GSM）<sup>5</sup>的通訊規定可歸類為2G的電話系統。

為了使話音傳輸服務進一步發展至資料收發，GSM營運商開始提供General Packet Radio Services（GPRS）<sup>6</sup>，即2.5G<sup>7</sup>；其後再推出Enhanced Data rates for GSM Evolution（EDGE）<sup>8</sup>，即2.75G<sup>9</sup>。EDGE可提供高達384 Kbps 的資料傳輸速率。

國際電訊聯盟（ITU）繼而發展第三代（3G）<sup>10</sup>流動通訊規定<sup>11</sup>，令流動技術再進一步至多媒體通訊（視像、圖片、文字、圖像和資料）。流動用戶的資料傳輸速率可達384kbit/s，在靜止狀態下的資料傳輸速率更高達2Mbps。3G Partnership Project（3GPP）<sup>12</sup>於1998年12月成立，其目標是以演進了的GSM核心網絡及其支援的無線電接達技術，為第三代流動通訊系統訂立全球認可的技術規格和技術報告。

---

<sup>3</sup> <http://www.itu.int/osg/spu/ni/3g/technology/index.html>

<sup>4</sup> <http://www.privateline.com/Cellbasics/hart-ch3IS-136.pdf>

<sup>5</sup> <http://www.etsi.org/WebSite/Technologies/gsm.aspx>

<sup>6</sup> <http://www.etsi.org/WebSite/Technologies/gprs.aspx>

<sup>7</sup> <http://en.wikipedia.org/wiki/2.5G>

<sup>8</sup> <http://www.etsi.org/WebSite/Technologies/edge.aspx>

<sup>9</sup> <http://www.mobileburn.com/term.jsp?term=2.75G>

<sup>10</sup> <http://en.wikipedia.org/wiki/3G>

<sup>11</sup> <http://www.itu.int/newsarchive/press/PP98/Documents/Backgrounder2IMT2000.html>

<sup>12</sup> <http://www.3gpp.org/About/about.htm>

當資料傳輸速率不斷提升，便出現一種新技術—High-Speed Downlink Packet Access (HSDPA)<sup>13</sup>，即3.5G<sup>14</sup>的降臨。HSDPA令資料傳輸速率大大提高至14.4Mbps。

第四代(4G)<sup>15</sup>通訊規定按計劃支援高質素多媒體服務，目標是在流動情況下資料傳輸速率標準可高達100 Mbps，在靜止狀態下則有1 Gbps。

## 無線城市區域網絡及無線區域網絡

當手提電話系統不斷提升傳輸速率技術，其它具競爭性的技術例如Wi-Fi（或無線LAN或WLAN）及WiMAX（Worldwide Interoperability for Microwave Access）也向這目標進發，為綜合多媒體服務提供更高帶寬。Wi-Fi無線技術是依據IEEE802.11的標準，雖然有某程度上的限制，卻能夠提供達54Mbps的資料傳輸速率，比HSDPA的14.4Mbps更快。

WiMAX亦稱為無線城市區域網絡（或無線MAN），是WiMAX論壇的商標。WiMAX論壇是一間非牟利機構，以IEEE 802.16標準<sup>16</sup>為業界證實及推廣寬頻無線產品的互通和互相兼容的特性。WiMAX比WLAN（Wi-Fi）支援更寬頻譜，在有線的寬頻如cable及DSL<sup>17</sup>等服務外提供另一無線網絡的選擇。對於固定的應用系統，WiMAX可提供達40Mbps的傳輸容量；至於流動用戶在3000米距離之內則可享受高達15Mbps的傳輸速率。

WiMAX網絡的接達控制提供數碼證書或預設的共用密碼匙認證機制，並支援嚴格的AES加密算法，其密碼匙管理規約的設計包含內置保護，可防止中繼攻擊。然而，WiMAX還未被大規模推行，其防禦能力仍處於評估階段。

## 無線個人區域網絡（Wireless Personal Area Networks, WPAN）

除了以上提及的通訊規定，流動裝置還支援無線個人區域網絡（WPAN），例如藍芽（Bluetooth）及紅外線，可在短距離內（以米計算，例如1米之內）連接及控制不同的產品及裝置。

---

<sup>13</sup> [http://en.wikipedia.org/wiki/High-Speed\\_Downlink\\_Packet\\_Access](http://en.wikipedia.org/wiki/High-Speed_Downlink_Packet_Access)

<sup>14</sup> <http://en.wikipedia.org/wiki/3.5G>

<sup>15</sup> <http://en.wikipedia.org/wiki/4G>

<sup>16</sup> <http://www.wimaxforum.org/about/>

<sup>17</sup> <http://www.wimaxforum.org/technology/>

藍芽的技術規格是開放的，由藍芽Special Interest Group (SIG) 監管。藍芽提供低帶寬的無線連接功能，在約10米的距離內支援資料（非同步）及話音（同步）通訊，總帶寬可達1 Mb/sec<sup>18</sup>。

紅外線連接是短程的無線訊號，像一條電線以建立通訊網絡，檔案及資料可在約1米距離之內雙向傳輸。然而，若紅外線的視線受阻，便會失去連接。

## 實施策略

流動裝置被廣泛使用，包括流動文字通訊和瀏覽網頁等，最普遍是流動用戶收發電子郵件。一些商業網站更特別開發相應的網頁以滿足使用這類流動技術的用戶。

當商業機構決定使用流動技術，便需要制訂清晰的保安政策，以防止因流動用戶的活動而引致內部網絡入侵、病毒感染和資料外洩。

## 企業的保安考慮及措施

企業實施流動技術時或會出現以下的保安問題：

1. 小型流動裝置被竊或遺失
2. 員工不誠實或未經許可使用流動裝置而引致資料外洩
3. 病毒散播或其它修補程式管理的問題
4. GSM通訊可能發生的窺視及截取

在准許員工使用手提裝置工作前應考慮裝置可能會遺失或被竊。要避免因而資料外洩，其中一個方法是事前替裝置啟動密碼保護功能，要認證才可以使用该裝置。這個方法需要明確的密碼管理政策。另一個方法是用裝置的遙距資料毀滅功能，當該裝置遺失或被竊時，裝置內所有的資料便可被遙距毀滅。此外，應維護一份獲准使用於工作上的流動裝置清單，並且定期核對清單。若要在裝置內儲存敏感資料，則必須加密予以保護。

因員工不誠實或未經許可使用流動裝置而引致資料外洩是機構的一大隱憂。當員工獲授權接達敏感資料，不論蓄意或人為錯誤，資料外洩是有機會的。因此必須實施防禦方法，包括要求所有員工簽署一份保密聲明及協議。有些工作環境例如客戶中心，員工需要接觸大量客戶的個人資料，機構或有需要採取措施，例如不准員工攜帶手提電話等個人物品進入工作範圍。

---

<sup>18</sup> <http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html>

電腦病毒日漸威脅流動裝置，2004年第一隻被證實的蠕蟲Cabir可感染流動電話及使用Symbian操作系統的裝置<sup>19</sup>。蠕蟲在受感染的操作系統上利用藍芽技術不斷散播，解決方法卻於稍後才出現。因此，企業必須考慮制訂保安政策以保護流動電話，包括安裝防毒軟件並更新病毒識別碼定義，以及實施並定期更新適當的修補程式管理政策。

因應早期的模擬話音傳輸而出現的GSM，其設計目的是建立安全的通訊渠道，然而GSM通訊並非如理想般安全，有被截取的可能性<sup>20</sup>。美國一群研究員發現這問題，並破解了用於GSM認證及加密的COMP128算法<sup>21</sup>。因此，企業要在商業應用系統使用流動裝置，必須考慮使用更先進的通訊規定（例如3G、Wi-Fi等）。

---

<sup>19</sup> <http://news.bbc.co.uk/2/hi/technology/3809855.stm>

<sup>20</sup> <http://www.gsm-security.net/papers/securityingsm.pdf>

<sup>21</sup> <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>

### III. 終端用戶的流動技術保安須知

終端用戶使用流動裝置時須符合一些保安措施，例如美國國防部曾要求員工將所有儲存在「容易移走的電腦裝置」的資料全部加密，包括手提電腦及個人數碼助理<sup>22</sup>。

一個未加適當保護的流動裝置一旦被盜或遺失的話，歹徒就可以輕易取得裝置上的資料。如果裝置感染了惡意軟件，有可能偷偷地被利用而使用了一些高消費的服務，或者泄露敏感資料。以下是給用戶在使用流動裝置時的一些保安提示。

#### 當你設定流動裝置時

- 在許可的情況下，應啟動開機密碼或其它裝置密碼管理工具。
- 配置你的流動裝置，使它在一段指定的非活動狀態時間內自動鎖定。
- 應在流動裝置上安裝手機保安軟件，如防毒軟件和防火牆。
- 應安裝最新流動裝置作業系統和相關的備份／同步軟件的修補程式，替軟件升級至最新版本。
- 應徹底審察應用程式／服務的所有權限要求，特別是一些涉及特權的存取。
- 應替儲存在流動裝置或抽取式媒體內的敏感資料進行加密。
- 應在許可的情況下，設定遠端清除功能。
- 在不使用時，應關閉無線連接，像 Wi-Fi、藍芽和／或紅外線無線通訊。
- 如沒有必要使用基於位置為本的應用程式，應關掉流動裝置內的定位服務設定。
- 不應破解流動裝置以解除其使用或存取限制。

#### 當你使用流動裝置時

- 應小心看守你的流動裝置，一時疏忽都有被竊的可能。
- 不應在流動裝置上處理敏感資料，除非使用具有加密功能的或安全的端到端連接。
- 不應打開或點擊在 SMS/MMS 或電子郵件上可疑或不可靠的連結。

---

<sup>22</sup> [http://www.gcn.com/print/26\\_22/44923-1.html](http://www.gcn.com/print/26_22/44923-1.html)

- 不應下載或接受不明或不可靠的程式或內容。
- 連接公共的 Wi-Fi 熱點時要謹慎。應避免存取敏感資料，除非採取了足夠的保安措施。

#### **當你備份流動裝置內的資料時**

- 應在許可的情況下，開啓備份／同步軟件之加密選項。
- 應確保儲存在桌面電腦或抽取式媒體上的備份都經過加密。

#### **當你棄置流動裝置時**

- 應確保流動裝置內的數據和設定在棄置前已被完全地刪除。

#### **任何時候**

- 應把流動裝置放置在安全的地方，尤其是在不使用時。
- 應時刻留意與流動裝置有關的保安漏洞，並安裝最新的修補程式。
- 不應在流動裝置上安裝非法或未經授權的軟件。
- 不應接受不明或不可靠的無線連接要求。

當享受流動技術為我們帶來的方便時，緊記採取適當的保安措施。流動用戶必須留意有關風險，以享受香港作為無線城市所帶來的益處及方便。