無線網路專題報告*

李 俊 勳 撰**

壹、前 言

隨著電腦的普及、網際網路應用的多元化，擁有多台電腦設備或資訊家電的家庭有越來越多的趨勢，為解決分享彼此資源（如印表機）、檔案及上網環境等問題，國際電腦大廠（如 IBM、康柏等）於 1998 年提出「家庭網路」的概念，在所提出的幾項解決方案中，由於無線傳輸訊息擁有易安裝與可移動性的優點，在近年相關技術、產品與價格均臻成熟之際，已逐漸成為家庭網路市場的主流。

去（2003）年 3 月，電腦大廠英特爾（Intel）結合無線寬頻上網產業廠商，大手筆的為該公司新一代筆記型電腦中央處理器 Centrino 行動運算技術，舉行造勢活動，積極推展建置無線上網熱點(Hot Spot)，更進一步將無線上網的運用推向隨時隨地與無所不在的地步。

雖然無線網路技術的發展，主要在解決「家庭網路」佈線及網際網路使用（俗稱行動上網）的問題，惟其技術的運用並非僅限制在此領域，隨著越來越多公司或企業亦應用無線網路技術佈建其區域網路環境，並作為傳輸機密資料的媒介之際，其原先設計作為一般家庭或上網使用的無線網路技術，其資料傳輸的安全機制是否完備，即引起廣泛的討論與爭議。

本篇報告將就我國無線網路的發展現況、我國金融機構的運用現況、無線網路風險管理措施，以及無線網路技術未來的發展趨勢等作介紹，並從中探討金融機構在引進此一技術時，所可能面臨的風險，以及所能採取的因應之道。

貳、我國無線網路的發展現況

無線網路（WLAN, Wireless Lane）是運用無線電波中未受法規限定的頻段（即其使

* 本文承蒙陳處長上程審閱並提供文章大綱意見，特致謝忱。惟本文觀點純屬作者個人意見，與服務單位無關，文中如有任何疏漏或謬誤，一律由作者自行負責。

** 作者為中央銀行金融業務檢查處科長。

用不須向政府申請使用執照）所發展出作為傳輸資料媒介的一種無實體網路。整個無線網路產業從上游至下游大概可區分為：技術規格制定、產品設備認證、晶片設計生產、產品製造及公眾無線網路服務等領域，本節將說明各領域的特性，分析我國產業在其中所扮演的角色，從而瞭解目前我國無線網路產業的發展現況。

一、技術規格制定機構

制定技術規格供各廠商作為設計產品依據的機構。無線網路的技術標準主要是由美國電子電機協會（IEEE）制定，目前最通用的標準規格為 802.11b、802.11a 及 802.11g 等，其主要的區別在於使用的無線電頻率與傳輸速率等的不同，其中又以 802.11b 為目前最成熟的技術規格。

IEEE 為非營利的國際技術專業公會，目前全球擁有 150 國 377,000 個以上的個人會員，我國教育部、國科會等為其經費贊助機構，而國內亦有多所大學教授或研究機構專家為其會員，對該組織技術規格的研訂，均可有效掌握其發展方向，並適時提供國內廠商所須的技術，對國內相關產品的研發皆有所助益。

二、設備認證機構

認證及測試各家廠商所生產的無線設備產品，是否符合一定標準技術規格的機構。無線網路領域，目前最主要的證認機構為 Wi-Fi 聯盟（亦有人將 Wi-Fi 視為無線網路的代稱），一般廠商生產的無線設備產品，均會送請 Wi-Fi 取得認證，以作為其能符合一定效率標準的保證。Wi-Fi 聯盟屬國際性的非營利組織，目前全球共計 206 個組織或個人加入其會員，幾乎包括所有資訊產業的重要廠商，我國多家廠商如：宏碁、華碩、技嘉、友訊、華邦、威盛等亦均為其會員，對所生產的無線產品設備是否能符合其認證程序，可適時掌握相關的技術環節。

三、晶片設計及或製造業

依據 IEEE 所制定的標準，設計電路圖作為製造無線網路晶片的公司，部分公司會自行生產晶片，亦有委託如台積電、聯電等專業代工生產者。

無線網路晶片組的核心是由控制與實體線連接部分（MAC/BB）的晶片與控制與無線電波發射接收部分（RF）的晶片兩種技術所組成，MAC/BB 屬數位技術，國內廠商在此方面均有良好的經驗，而 RF 技術則為類比技術，需較長的技術累積經驗，目前的關鍵技術仍由國外大廠所掌控。我國目前主要的 WLAN 晶片組設計與生產公司為：瑞昱半導體公司、上元科技公司等。

四、無線網路設備製造業

應用無線網路晶片，設計組裝成無線網路卡或橋接存取點(Access Point)設備的公司。無線網卡是安裝在電腦設備上，存取點則是一端連結至實體網路線，一端接收傳送電波訊號，電腦設備將傳輸資料，透過無線

網卡轉換成電波廣播出去，存取點則在接到無線電波後轉送至實體網路線上的設備，從而讓電腦設備進入網路世界（架構如圖 1 所示）。

圖 1 :無線上網架構簡圖

註：取材自「HiNet 客戶服務 - 線上客服 - 無線網路」

台灣由於已擁有完整的電腦設備組裝技術及良好的成本管理能力，對於無線網路設備，台灣仍是全球的生產重鎮，2002 年台灣出貨量約已佔全球的七成，預估 2004 年應可達八成以上。

五、公眾無線區域網路服務業（PWLAN）

於公共場所佈建供大眾無線上網熱點(Hot Spot)的系統整合業者。台灣不只是無線網路設備的最大出口國，公共場所無線上網熱點的建置腳步也很快，目前國內主要的 PWLAN 有曜正科技、中華電信、蕃薯藤等，截至今(2004)年 4 月全台約有 700 多個可以無線上網的公共場所，包括關渡、墾丁、台北信義計畫區等景點，以及多處咖啡廳、餐廳、機場、學校、火車站等，均佈建上網熱點，隨時可提供無線上網服務。

由於台灣已成為無線區域網路（WLAN）產業的全球設備製造重鎮，目前無線網卡產品代工市佔率為全球第一，為結合系統整合業者共同開拓本土無線寬頻服務與應用之市場，進而延伸產業優勢，再創產業高峰，政府在總體國家發展策略上，將「推動無線寬頻網路計畫」納入「挑戰 2008 國發計畫」的第六個計畫「數位台灣計畫」

中，並將「行動－台灣計畫」也就是「M －台灣計畫」納入五年五千億「擴大公共建設投資計畫」中，計劃在 2008 年能達成五百萬全民無障礙雙網（無線網路與行動通信）整合上網目標，並將台灣打造成為全球第一的雙網應用服務環境，並藉此帶動通信產業，成為我國繼半導體以及影像顯示產業之後的第三個產值達到兆元以上的產業。

參、我國金融機構的運用現況

無線網路雖已普遍為大眾所接受，不過金融機構對新技術的引進向來比一般企業來的謹慎。本節所述內容，主要以中央銀行檢查 (註 1) 的金融機構為主，其中大部分由檢查人員以實地瞭解的方式取得資訊，部分則以電話方式訪詢，主要以下列三個議題作為瞭解金融機構運用無線網路的情形：

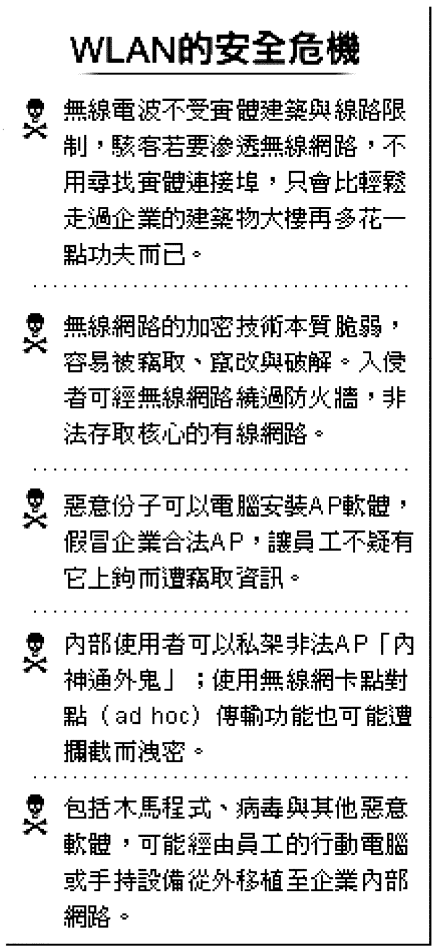
1.是否建置無線網路環境，其應用範圍為何？是否進行安全評估，其報告之陳核層級為何？稽核單位之參與情形？

2.是否計劃或規劃運用無線網路？預定建置時程及應用範圍？

3. 對全行各單位（含管理單位、營業單位）無線網路設備之使用（包括無線網卡、存取點設備 Access Point 等）是否明訂管理辦理？

截至 93.4.30 止中央銀行檢查的十六家本國金融機構運用無線網路情形，除 1 家銀行已在總行內部單位採用外，其餘使用情形或是與銀行業務無直接相關、及仍在評估中，不然就是尚未列入考慮，採用的情形尚稱謹慎。至於是否針對無線網路設備的使用，明訂各單位應遵循的管理規範乙節，大部分銀行仍付之闕如。

圖 2：WLAN 的安全危機

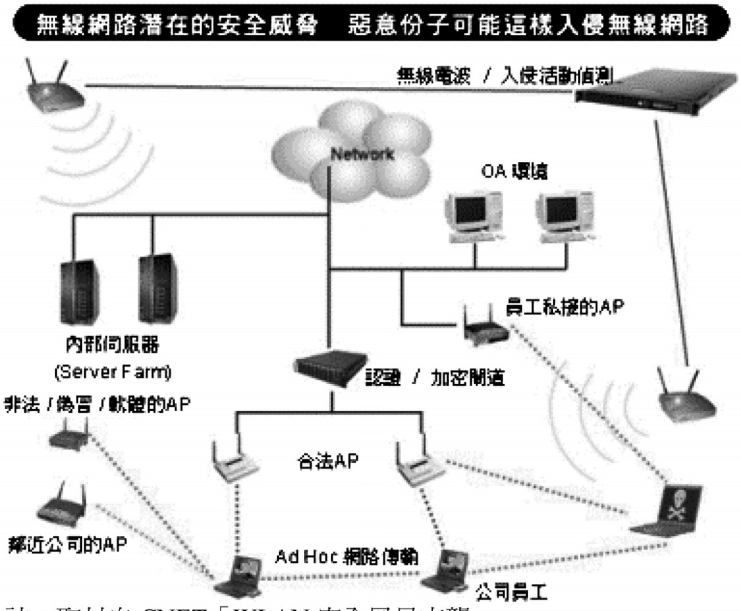


肆、無線網路風險管理措施

無線網路的設計類似於一般的無線通訊的原理，同樣的是利用電磁波以無方向性的廣播方式將訊號傳送出去，如同廣播電台、電視台一般，任何人只要將天線調對頻道，即可接收訊息（如同收聽廣播、收看電視），此點是與有線網路最大的不同點，加上電磁波具有高穿透力（可任意穿透天花板、門窗及水泥牆等），使得訊息傳輸遭截取的風險大增，加上目前普遍使用的無線網路訊息加密技術(WEP, Wired Equivalent Privacy)證明有其安全弱點，駭客極易取得破解工具，更增加無線網路訊息傳輸的不安全性。

無線網路另一個引起安全爭議的部分，是在連接至實體網路的橋接存取點(Access Point)。無線網卡是安裝在電腦設備上，存取點則是一端連結至實體網路線，一端接收傳送無線電波，扮演的角色是將無線電波訊號轉換成實體網路上的數位訊號，而電腦設備將輸送資料，透過無線網卡轉換成電波廣播出去，存取點則在接到無線電波後將訊號轉送至實體網路線上。倘若存取點的安控設定不當或未修改出廠時設備的預設值，任何裝有無線網卡的電腦設備即可輕易透過其存取點，使用內部網路的資源（包括存取網路訊息）。除此之外，如圖 3 所示，企業內部員工，利用二張無線網卡，一張連入公司網

圖 3　無線網路潛在的安全威脅



註：取材自 CNET「WLAN 安全風暴來襲」

路，一張連至外部，或私自架設無線網路的存取點(AP，Access Point)；以及駭客假冒公司合法AP架設伺服器以騙取員工合法的使用者資料等，均會使無線網路產生潛在的安全漏洞問題。

無線網路的安全真的這麼堪慮嗎？其實不然，根據市場研究組織Gartner指出，無線區域網路只要有適當的參數設定，就可避免大部分的網路入侵事件，亦是說，如果無線網路的存取點及用戶端軟體等設定得當的話，可減少約七成以上成功的無線區線網路攻擊。

因此，對一般企業所言，如何降低無線網路安全風險，管理應是最重要議題。至於金融機構，由於是處理及保管與社會大眾切身相關的財務及個人私密資料，因此必須採取更嚴謹慎密的安全評估及防範措施，美國財政部金融局（OCC）於92.12.9發布「無線網路的風險管理」，其內容所提供的一些風險管理準則，應可作為金融機構建置無線網路環境的參考。以下謹就文章所提的主要風險管理準則做一介紹：

1.由於無線網路有眾所周知的潛在安全風險，銀行是否有能力降低此風險，將取決於：

- 董事會與管理階層監督的有效性；
- 管理階層對建置與管理無線網路專案，其政策與程序的有效性；
- 跟得上技術演進的能力；
- 網路的可靠性與其容量；
- 緊急應變計畫的妥適性；
- 銀行安全規章執行的有效性；以及，
- 監控偶發事件與採取減低風險步驟的措施。

2. 至於如何降低無線網路所衍生的風險，可採取下列步驟：

- 採行無線網路前，應進行安全風險評估，並建置適當的政策與內部控制。
- 採行的安全措施應能保護銀行網路與無線網路上的設備，避免遭非法存取、傳輸攔截、洩露客戶資料，及其他弱點的威脅等。
- 注重無線網路的安全測試計畫。
- 檢視委外服務契約中所述能提昇效能水準的指標，以確保採取無線網路的有效性。
- 建置與維護網路的投資總成本或其收益，包括有關安全部分須投入的遞增成本（如：授權、督控、更新、測試等），應被視為決定專案成功與否的要項之一。

3. 對於如何確保無線網路的安全，建議可採取下列措施：

- 制定使用者的使用政策與管理程序。對無線網路的安裝與使用訂定有效的政策與程序，可助於強化整體系統的安全性。
- 明訂可經由無線網路傳輸的訊息類別。

- 留存經申請核准建置的無線網路架構圖、存取點位置，及可使用無線網路的設備的文件。
- 採行必要的措施，以控制無線廣播的範圍。
- 依據無線網路安全評估結果，採取適當的資料加密方式。
- 針對無線網路環境的使用，建置使用者適當的辨識控制機制。
- 對無線網路相關的實體及非實體設備，採取適當的防護措施。
- 建置適時有效的系統瑕疵及弱點更新程序。
- 將無線網路系統納入銀行整體的安全測試環結，並進行完整的安全測試，以確保銀行所建置的政策、程序與控管仍為適當。

4. 對於建置無線網路的專案管理，建議應：

- 完整的審慎評選。由於無線網路有其潛在的安全威脅，當計劃委外處理時，對廠商應進行完整的審慎評選，尤其是確保其能提供符合銀行需求的技術支援能力（於風險評估時即應確認）。
- 進行成本效益分析。對無線網路進行總成本法(total cost of ownership)或投資報酬率法(return on investment)的成本效益分析，會有助於專案管理評估其效益及預期目標的成效。

5. 為確保無線網路能提供預期的效能，建議應：

- 預估網路容量。於發展階段確認無線網路所能提供的效能，瞭解可供選擇的網路協定與其資料傳輸量，將有助於研訂符合營運目標與服務水準的計畫。
- 瞭解無線網路可使用性。對無線網路的無線電頻率使用，及其可能受其他設備（如微波爐、無線電話）的干擾，應確實認知，並預先規劃適當的因應措施，以維持網路之正常運作。
- 訂定緊急應變計畫。緊急應變計畫必須能因應銀行重要業務及系統的需求，所採取的解決方案亦應符合業務需求與所提供的服務水準。

文章最後的結論再次強調董事會與管理階層的有效率監督與管理，對金融機構是否能有效的降低無線網路所衍生風險的重要性，OCC 並要求董事會與管理階層，在建置無線網路前，應先配合檢討修改銀行的安全規章，並監督其執行情形，以確保能達成有效的風險管理目標。

綜觀 OCC 所發布的「無線網路的風險管理」內容，如同該機構以前所發布的其他風險管理準則般，作為如何管理無線網路已相當週詳，不過對於如何禁止員工私自架設存取點，或防制駭客以偽裝公司合法存取點方式騙取員工合法識別碼及密碼乙節，似乎未提醒銀行應予特別注意；美商無線管理解

決方案供應商 Cirond 的執行長 Nick Miller 就對其應注意的重要性舉一個簡單例子：「企業花了許多銀子與人力在網路安全上，不過只要一台 30 美元的無線基地台（存取點）就可讓這一切投資通通破功。」。至於如何解決，除了教育員工瞭解其行為對企業網路安全可能造成的影響，以及應隨時注意四週環境是否有異常設備並通報外，配備掃描無線訊號的「探測器」定時派專人巡視探測，及安裝無線入侵偵測器亦是無可避免的人力與金錢投資。

由於有員工私自架設存取點的問題，衍生所致企業所面對的議題是「未引進無線網路的企業是否應制訂無線安全政策?」，答案很明顯是肯定而應該的。企業的資訊安全政策與管理並不會因不採用或引進新技術，而仍可確保整體企業資訊的持續安全與正常運作，資訊安全高階管理階層，應隨時注意科技的發展，並定期檢討對企業所可能造成的衝擊，預先擬訂安全防範措施，以確保企業資訊安全的正常運作。

本篇報告所蒐集到的國內金融機構對無線網路的使用情形，雖運用層面尚屬有限，惟似仍未將無線網路所可能導致的風險及對銀行的衝擊，預為檢討並修訂相關安全政策。檢查人員於辦理實地檢查時，應提醒銀行相關人員注意檢討辦理。

伍、無線網路技術未來的發展趨勢

人類永遠追尋及嚮往著無拘無束的生活。網際網路的發明，如同人類發明電力般的，將會對人類生活造成重大影響，而因應而生的無線網路世界，亦是人類追尋的目標。無線網路雖有前述所提的安全問題，不過隨著安全技術使用的日趨成熟，IEEE 協會已於 2004.6.24 通過可確保無線網路內傳送資料更安全的加密技術(802.11i)，如此將可有效解決資料中途遭欄截甚至解密所造成的安全問題。

無線網路另一個待突破的問題：訊號可廣播的距離與傳輸速率。目前由英特爾(Intel)主推的技術 WiMax 預計將於 2005 年 5 月成為另一項技術標準(802.16d)，其訊號可廣播的範圍達 48 公里，比目前使用的技術 Wi-Fi 至多僅數百公尺擴大很多，而最快傳輸速率每秒 70Mb，亦比 Wi-Fi 每秒傳輸 11 至 54Mb 快上許多。

無線網路目前還有一個待克服的問題：無法滿足行動中的電腦無間斷的上網問題，亦俗稱網路漫遊問題。由於目前 Wi-Fi 技術可提供傳送與接收訊息的範圍較短，因此民眾僅可在公眾無線區域網路服務業者（PWLAN）佈建的上網熱點(Hot spot)可接收的範圍內，以定點方式無線上網，如此將無法滿足一般行動商務民眾的要求。未來

WiMax 技術成熟後，由於傳輸的範圍較廣，或許可解決目前的問題，不過屆時可能又必須解決漫遊在不同 PWLAN 所建置的熱點間訊息交換與上網費的拆帳問題。目前業者推出的解決方案，大都是整合手機的 GPRS 技術（俗稱的 3G），即是行動電腦在熱點範圍內使用 Wi-Fi 上網，範圍外則自動切換至利用手機上網，不過相對也影響傳輸速率。

至於無線網路有關私自架設（或遭盜裝）存取點及駭客偽裝合法存取點的問題，前項問題僅得以無線入侵偵側方式解決，未來此技術將會整合至網路安全管理設備中，以減少額外的成本投入；對於駭客偽裝問題，可利用無線設備間相互認證的技術解決。

看起來未來的無線網路世界似乎一切美好，不過如同各種工具都應該有正確的使用方法才能發揮其功能，未來有關無線網路的安全設計仍有賴人們的正確使用，而其中良好的管理才是最重要的議題。

陸、結　語

無線網路由於擁有低成本、易安裝的特性，隨著安全議題一一被克服及使用技術的愈臻成熟，無可避免將會廣為社會大眾所接受。金融機構在計劃引進此項技術前，應確實瞭解其所可能衍生的風險及產生的衝擊，從而修改安全政策並擬訂良好的管理措施，隨時注意科技的進展適時調整因應對策，以符合金融機構安全與穩健的經營原則，為達此目標，董事會及高階管理應投入必要的關注及監督。

此外必須注意的是，藉由網際網路所發展的網路銀行通路，使金融機構的營業據點延伸至不特定的任何地點與任何對象，而隨時隨地可上網的無線網路更加深其不確定性（如同手機預付卡，無法確定發話人般），因應此一技術廣為大眾所接受之際，金融機構必須重新審視網路銀行的安全機制，以防範其可能導致之風險。

附　註

(註 1) 自民國 93 年 7 月起，中央銀行已不再對金融機構辦理一般業務檢查。