企業對員工可攜式設備管理之研究

-以 H 公司為例

Bring Your Own Device Management at Enterprise -A Case Study for H Corporation

李仁鐘　潘季豪　林辰謎　楊明仁

Zne-Jung Lee　Ji-Hao Pan　Chen-Cheng Lin　Ming-Ren Yang

華梵大學資管系

Department of Information Management,
Huafan University

摘要

無線網路已經變成很多人工作或是生活的一部分。許多裝置都開始都內建無線網路存取功能，尤其以筆記型電腦（Notebook）、平板電腦（Tablet）以及智慧型手機（Smart Phone）最為普遍。現今企業體也因為無線網路普及化，終端設備支援良好；開始研究提升企業生產力的方法。於 2011 年攜帶自有設備終端設備到企業體工作（Bring Your Own Device, BYOD）概念開始成形。坊間有許多不同類型的解決方案。在企業體考量整體營運成本的前提下，有效整合既有投資與符合企業多樣化的服務需求；是現今企業追求的目標。本研究針對 H 公司所導入的 BYOD 架構為個案研究對象。實際架設一組測試用無線網路平台，透過實際架設與測試網路架構找出 H 公司所使用的管理邏輯。此管理邏輯須符合容易連線且方便管理的主要目標。期待能夠透過此研究協助企業體加速建置安全且簡易的無線網路環境，進一步提高企業整體生產力協助企業體再成長。

關鍵字：資訊安全、網路存取控管、BYOD

Abstract

Wireless network access is a part of our daily life. More and more devices support wireless access function by default. Most of popularly devices are Notebook, Tablet and Smart Phone. Wireless network access is really easy to deploy for company, because multiple devices support wireless access. Bring your own device concept (BYOD) started from 2011. There are a lot of BYOD solutions in the market. Enterprise customers are really concern about operation cost and maintained cost, so protecting existing IT investment is one of the key topics. This paper is a case study for H Corporation to build up a wireless platform for BYOD and find out the management concept of BYOD. This management concept of BYOD really protects IT investments. It does not need to allocate extra budgets and easy to management, and could improve the decision process of H Corporation and productivity.

Keywords: Information Security, Network Access Control, BYOD

1. 緒論

（一）研究背景

回顧二十年前，資訊產品剛開始蓬勃發展。進入資訊產業是大多數畢業生的夢想。當時一部個人電腦要價十萬元。且體積大攜帶不方便，如果能在學校或是特定單位使用電腦已經是不容易的事情。所以當時的情況，一般員工要自己帶設備進到工作崗位上；是極其不容易。第一是使用成本的問題，再來是體積大不方便攜帶；所以當時沒有需要管理員工攜入設備這類的問題。可是反觀現今趨勢，行動電話功能越來越強大；現今趨勢，網際網路發達，終端設備不斷推陳出新。平板電腦（Tablet）智慧型手機（Smart Phone）、筆記型電腦等體積都不斷縮小且功能越來越強大[12]。越來越方便攜帶，電池使用壽命也不斷在延長。當這些可以存取網路與攜帶資訊的裝置讓員工帶到企業內工作；存取企業內部資源，那就企業體就必須要仔細規劃與限制存取範圍，以避免出現資訊安全漏洞[9]。畢竟這些設備並沒有通過企業內部相關的檢查流程，軟體硬體相關更新；不一定符合企業內部安全控管規範。本文蒐集國內企業控管設備類型大約區分成三類；以個人電腦、智慧型手機以及平板電腦為主[12]。企業內部的資訊架構區分成很多不同的區域。其中包含硬體系統，軟體系統以及管理系統幾個大區塊[8]。且建置企業內部資訊系統目的在提供符合企業營運的需求。然而商場上快速且多變的需求通常是資訊管理人員最不能夠了解與體會的。

BYOD（Bring Your Own Device, BYOD）必須架構在有線與無線網路存取平台上，所以有只要有建置線網路存取平台的企業就可能有 BYOD 管理的需求。而在此類裝置中，有不同硬體平台以及不同作業系統。管理上比以前更不容易。雖然行動裝置帶來許多便利性，提高同仁資訊取得的速度。過去必須回到公司電腦系統端才能處理的事情；現在透過行動裝置有很多其實都已經可以做到。提升資訊傳遞的速度，相對上就可提高同仁產能，增加專案獲勝機率，進一步提高營業額增加獲利。看起來好像充滿光明面。事實上卻不是這樣美好的結局。制定網路存取範圍以及管理是一個大問題，再來數位資料與設備的安全性顧慮；加上行動裝置容易因為人為疏失遺落在各地。設備上面所存放的資訊，如果是企業併購的重大訊息，或者是交易憑證與相關資訊。有可能造成企業很大的損失。所以 BYOD 的安全問題是目前面臨到的問題之一[2][3][9]。

（二）研究動機

對一個企業或組織而言，良好的訊息傳遞是相當重要的一環。唯有良好的訊息透通。政策與業務執行方針才能讓所有同仁了解，也才有共同的營運目標以及方向。產品與報價訊息方便存取，才能夠讓業務同仁快速提供相關解決方案給用戶。所以容易存取的網路平台且兼顧安全性是非常重要的。當員工可以自行攜帶設備進入企業”工作”後企業必須要制定一個存取範圍。在此範圍內的資訊是可以開放讓同仁存取。企業可透過風險評估，了解目前所面臨的威脅以及現有的弱點為何。針對開放 BYOD 後的弱點則需要企業主再進一步改善[10][13]。

另外 BYOD 管理有許多層次，初階為人員存取授權、定義設備授權類型、設備存取範圍為基本的管理重點。進階的 BYOD 為行動裝置管理（Mobile Device Management, MDM）[15]，受納管的終端設備所安裝的軟體內容、軟體版本、設備離線時間控管、設備遺失資料如何銷毀等相

關管理議題。如何決定可接受風險值，做為接下來改善的依據，也是非常重要的一環。本研究主要研究範圍為初階的 BYOD 管理針對授權人員以及設備進行存取管制。行動裝置上面的軟體授權管理，對資訊人員來說也是一大挑戰[7]，主要原因是平台眾多、作業系統版本不一、授權與統計數量不容易，且如果企業體本身規模不夠大時相對上採購議價空間較小。

（三）研究目的

BYOD 的管理目標為區分設備類型以及存取區域，其管理邏輯在於有效區分設備所使用的網段。廠商在推廣產品及過度強調產品功能的前提下反而模糊使用者的焦點。所以每當與業界先進討論 BYOD 相關議題時，常發現大部分的使用者對於 BYOD 議題的範圍與架構十分模糊。本研究主要目的是透過現有企業型無線網路架構調整，達成簡易的 BYOD 管理目標；保障企業資訊投資，同時滿足企業對資訊安全性需求以及員工使用便利性需求。企業用的無線網路架構因為建置成本高達數十萬至數百萬元不等，一般民眾不容易接觸到， 本研究主要套用不同企業型無線網路控制器控管終端設備資料流(Traffic Flow)，達成管理 BYOD 管理目標。

（四）研究流程

在確認研究主題及研究方向後，本研究選定以H公司為研究目標，主要探討H公司導入之BYOD模型。研究此管理模型；確認H公司導入無線網路架構與相關存取規範。並透過實際測試確認此管理模型符合企業基本需求。研究流程圖如[圖1]所示。

圖1 研究流程圖

（五）研究限制

員工攜入式設備管理主要區分成幾個層面，人員辨識、設備辨識與設備管理[10][11][14]。BYOD 著重於使用者的認證與設備辨識，而行動裝置管理(MDM)、無線網路涵蓋範圍、無線網路訊號強度與無線容錯架構等不包含在本研究內。

本研究主要套用企業型無線網路控制器下的無線網路架構。透過控制器統一管理。如果使用簡易型無線分享器，不透過控制器管理的無線網路架構管理機制控制邏輯與本研究不同。控制機制落在網路交換器上面。但是整體管理邏輯相同。本研究主要參考 H 公司所導入的無線網路存取架構，在不增加企業的營運成本下面達成簡易的 BYOD 解決方案。由於研究有所使用之超高速乙太網路交換器以及無線網路控制器與無線存取基地台等相關設備，皆為 H 公司所提供之設備，其產品的相關使用特性並不代表其他廠商產品功能。且不同廠商在產品與解決方案規劃上有

其不同邏輯以及設定參數。但是針對 BYOD 管理邏輯基本上是相同的。另本研究方法統一 BYOD 的管理權限以方便資訊人員管理。

2. 文獻探討

本研究先探討行動裝置出貨狀況，探討目前市場成長趨勢[12]。接著探討網路存取控管，因為終端設備必須要連接網路才能夠存取網路上的資源，才能進一步處理相關資訊。研究 H 公司的無線網路管理邏輯，主要考量建置成本以及使用便利性。最後討論 ISO 27001 管理項目[2][3][6]。讓企業體根據 ISO 27001 控制項目去建置符合 ISO 27001 管理規範的安全網路存取架構。部分相關資訊整理如下：

（一）BYOD之興起

從產業的角度來看。目前智慧型手機的年出貨量已經超過個人電腦[12]。由此現象看來，使用者的習慣漸漸分成幾種。需要高效能與多樣化應用程式支援的用戶會選擇筆記型電腦。可是擁有筆記型電腦的使用者使用數位型手機的比例很高。在輕薄型的筆記型電腦（Ultra Book）上市前。使用者的選擇多數往平板電腦以及智慧手機這邊靠攏。

表1 2011年全球智慧型手機暨個人電腦出貨量資料表

Worldwide smart phone and client PC shipments

Shipments and growth rates by category, Q4 2100 and full year 2011

Category	Q4 2011 Shipments	Growth Q4'11/Q410	Full year 2011 shipment (Millions)	Growth 2011/2010
Smart Phones	158.50%	56.60%	487.7	62.70%
Total client PCs	120.2	16.30%	414.6	14.80%
Pads	26.5	186.20%	63.2	274.20%
Netbooks	6.7	-32.40%	29.4	-25.30%
Notebooks	57.9	7.30%	209.6	7.50%
Desktops	29.1	-3.60%	112.4	2.30%

智慧型手機以及個人電腦出貨統計資料。主要表現出智慧型手機出貨量以 60%以上的年度成長。反觀個人電腦只以 14.8%的年度成長。個人電腦成長力道很明顯趨緩。不過個人電腦整體出貨成長分類中，有一個特別的產品線"平板電腦"（PADs 或 Tablet）這個產品線的年度成長高達 274%。這結果顯示出使用者期望用到操作簡單、高效能、開機速度快且電池使用持久的平板電腦。也因為這樣的使用趨勢。開始有使用者帶自己的平板電腦或是智慧型手機到企業內工作。員工自攜行動裝置投入職場，企業體可節省員工設備之採購成本，並享受整體工作產能的提升。但另一方面，企業體也要及早制相關配套措施，包含個人行動裝置的身分識別、無線網路存取等級和客製化行動應用系統的管理措施，才能真正實現安全且高效率的虛擬企業。然而在企業建置相關配套措施的同時是否曾經仔細想過，BYOD 規劃是提供給高階主管還是給整體企業使用?這在規劃初期就應該制定出相關規範，以避免投資浪費[14]。現在各企業十分謹慎在資訊產品上面

的投資，主要大多數企業體在過去投資資訊創新上有不佳的經驗；所以提供創新服務上會更謹慎小心。行動裝置銷售量持續成長，加上企業管理大師們的討論和鼓吹，推生出「帶自己的行動裝置上班（BYOD）」的新名詞。其中不乏大力鼓吹因為有助於增進工作生產力，透過雲端服務，可以快速取得資訊，轉寄以及加以處理；不少企業為之心動。現實中 BYOD 對企業體來說像是兩面刃[9]。由員工自攜行動裝置為企業體工作，好處是公司節省了員工設備硬體成本，整體工作產能也能因為雲端應用加上行動效率而有提升。但另一方面，這些裝置不一定符合企業資訊管理規範，簡而言之就是開啟資訊安全後門，讓企業的敏感資料面臨風險。所以本研究提供 BYOD 規範方向以及制定相關的管理辦法。

（二）網路存取控管

網路存取控管（Network Access Control, NAC）的由來主要是提高端點防護機制[1][7]。初期的目的是保護端點的安全，避免終端設備被病毒攻擊或是駭客入侵。這邊的端點設備主要以個人電腦為保護重點。使用的通訊協定以 TCP/IP（Transmission Control Protocol and Internet Protocol）[1]為主。TCP/IP 網路架構主要分成 OSI 7 層，請參考[圖二]。在此模型中，每一層各司其職，本文所探討的網路存取控管主要討論第四層（Transport Layer）與第三層（Network Layer）。網路存取控管在不同層級所管理與使用的方式不同，在第四層上的管理主要針對服務的埠作控管，可以不考慮來源與目的地[1]。針對通過的服務加以限制。在第三層的管理目的上主要管理來源地 IP 網段與目的地網段。網路存取控管可以啟動在路由器、三層交換器與防火牆等設備上面。現在市面上也有無線網路控制器具備此功能。不過在使用上面必須要針對安全需求來作相對應的設定，才能達到安全管理目標。[圖 2]主要為 OSI 參考模型。本研究所討論的服務在第四層 Transport Layer 以及第三層 Network Layer。簡單來說，第四層主要是針對特定 TCP 所使用的服務埠（Service Port）來作控管，常見的 TCP 服務如下：

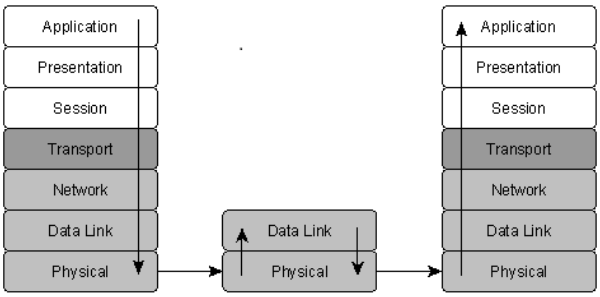

圖2 TCP/IP OSI 參考模型圖(資料來源：TCP/IP網路通訊協定第二版)

1. HTTP（Hypertext Transfer Protocol，超連結傳輸協定），用於網頁瀏覽。通常使用TCP 埠 80，企業內部通常會啟動快取服務（Proxy Service）並修改內定值；以提升企業內網安全。避免員工直接存取該埠，以提升安全防護等級。
2. HTTPS（Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL，安全超連結傳輸協定）用於網頁瀏覽，HTTP協定的安全版本。內定值使用TCP 埠443 ，可以依照網管人員實際需要修改使用埠。主要提升網際網路存取安全等級，在兩端使用加密機制，提升連線安全性。

3. FTP（File Transfer Protocol，檔案傳輸協定），用於檔案傳輸。使用的連接埠為TCP埠21、 20；使用上常會啟動認證機制，使用者必須要先申請帳號密碼方能存取該主機。匿名登入（Anonymous）通常只允許用戶下載資料，不允許上傳資料。在嚴謹度比較高的環境下，通常登入密碼會要求符合密碼長度以及複雜度；以提升FTP使用安全。
4. POP3（Post Office Protocol version 3，郵局協定），用於接收郵件。郵件伺服器與郵件端所使用的通訊協定。用於終端用戶收信使用。服務的埠為 TCP埠110與995。使用上也會有帳號密碼需要登入以提升資訊安全等級。
5. SMTP（Simple Mail Transfer Protocol，簡單郵件傳輸協定），用於發送電子郵件。服務的埠為TCP埠25。使用習慣上與POP3接近。
6. TELNET（Teletype over the Network），用於終端機存取，通過一個終端（Terminal）登陸到網路主機或是網路設備上。主要為文字模式在大型主機間設定或是執行程式使用。使用TCP埠23。
7. SSH（Secure Shell，用於替代安全性差的TELNET），用於加密安全登入用。通常提供網路設備遠端設定使用。

了解 ISO 第四層服務類型與服務埠，要控管相對上就容易許多。目前控管可以在路由器與防火牆設備設定，只允許特定服務的通過。接下來說明 ISO 第三層所定義的標準。第三層主要是針對特定目的地 IP 網段來控管（IP Network），並藉由此控管達到基本的安全防禦功能。IP 位址跟書信往來觀念相同；必須要有來源地址以及目的地址。全球 IP 派發統一由 IANA （The Internet Assigned Numbers Authority, IANA）管理。這樣才能統一規範避免派發 IP 重複。基於相同標準，網際網路上的服務才能正常執行。IP 位址計算有其計算基礎，通常透過子網路遮罩計算，來區分不同的 IP 網段。坊間有許多相關的文件以及書籍，本研究不探討 TCP/IP 規劃以及相關細節。指針對來源目的限制作簡單說明。

網路存取控管（NAC）必須要先通過人員認證，設備認證以及定義認證後的存取範圍。認證區分不同認模式與不同的密碼加密模式。設備認證可以透過網路卡號 (MAC Address)黑名單與白名單達成，黑名單代表限制存取，白名單代表允許存取。在資訊控管的目的是限制人員與設備去存取特定之設備、網段以及資料庫等。網路存取控管專注在於乙太網路架構下之存取。可以定義使用者之 IP 或是存取目的地網段，或是必須要透過特定之路由才能存取外網。定義網路封包所傳遞的路徑等等都是網路存取控管的一部分。無線網路控管等於是有線網路控管的延伸。可以把乙太網路上面的控管延伸到無線網路部分。當然整體規劃必須要能整合在一起。以避免使用上造成不方便。本文所提及的無線網路相關架構，基本上都是屬於開放式架構。並沒有使用廠商專屬之特殊私有協定。避免因設備屬性差異無法複製出整個管理模型。

（三）ISO27001:2005

有共同的標準才能讓組織內所有人有所依循。資訊業界有許多不同類型的標準規範，電機電子工程師學會（IEEE.Org）制定電子產品相關技術的主要研究單位。國際標準化組織（International Organization for Standardization,ISO）主要制定全世界工商業國際標準。目前資訊安全

ISO27001:2005 是全球最廣泛使用商業管理標準之一，ISO 27001:2005 主要採用”規劃-執行-檢查-行動”（Plan-Do-Check-Act, PDCA）模型參考[圖 3]所示。主要是針對建立資訊安全管理系統（Information Security Management System, ISMS）時，須做到運行的過程中相關操作流程、人員資訊設備等安全規範、導入系統操作、檢視稽核都需要建立相關的書面資料，並以此書面資料作為驗證的標準。一旦流程變更，需要重新修改相關書面文件以符合 ISO27001：2005 之相關規範。此規範的目的不在於增加相關人員負擔，主要在保障營運單位在資訊安全相關議題上面有其標準可依循。避免因為缺乏紀錄導致營運受到牽連與影響[2]-[5]。

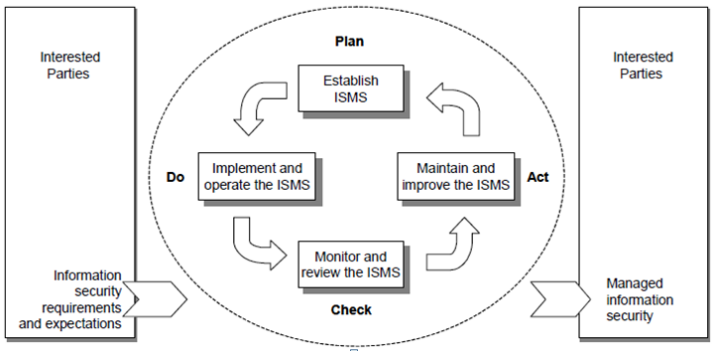

圖3 用於資訊安全管理過程之PDCA模型

資料來源：ISO/IEC 27001:2005

（四）ISO27002:2005

ISO 27002:2005 資訊安全管理作業要點（Code of Practice for Information Security Management），企業或組織在建立資訊安全系統時，會根據企業所在國家區域相關的主客觀情況或其經營屬性，對於所面臨的不同種類威脅及營運風險[5][6]，此管理作業要點包含合作對象以及上下游廠商皆須滿足的各項要求。不同企業體與組織都會發展出自己的特定原則或營運目標及要求，而 ISO27002:2005 列出了適用於大部分單位或組織所需注意的資訊安全控制點，此部分包括 11 個項目，39 個控制目標及 133 個控制措施[2][3][4][5]。作為各企業以及組織在施行資訊安全管理系統時之參考建議，本文只擷取 A.11 網路存取相關之章節，並未把所有章節列入。未列出之項目企業或組織應該視需求局部調整控管之項目。本研究主要探討的區域為 ISO27002:2005 章節之 A11.4。

表2 ISO27002控制項目、控制目標及控制措施表

Domain	控制目標	控制措施
A.11 存取控制	A.11.1 存取控制的營運要求	A.11.1.1 存取控制政策
	A.11.2 使用者存取管理	A.11.2.1 使用者註冊 A.11.2.2 特權管理 A.11.2.3 使用者通行碼管理 A.11.2.4 使用者存取權限的控制措施審查
	A.11.3 使用者責任	A.11.3.1 通行碼的使用 A.11.3.2 無人看管的使用者設備 A.11.3.3 桌面淨空與螢幕淨空政策
	A.11.4 網路存取控制	A.11.4.1 網路服務的使用政策 A.11.4.2 外部連線的使用者鑑別 A.11.4.3 網路設備識別 A.11.4.4 遠端診斷與組態埠保護 A.11.4.5 網路區隔 A.11.4.6 網路連線控制 A.11.4.7 網路選路控制
	A.11.5 作業系統存取控制	A.11.5.1 保全登入程序 A.11.5.2 使用者識別與鑑別 A.11.5.3 通行碼管理系統 A.11.5.4 系統公用程式的使用 A.11.5.5 會談期逾時 A.11.5.6 連線時間的限制
	A.11.6 應用系統與資訊存取控制	A.11.6.1 資訊存取限制 A.11.6.2 敏感性系統的隔離
	A.11.7 行動計算與遠距工作	A.11.7.1 行動計算與通信 A.11.7.2 遠距工作

資料來源：ISO27002

3. 研究方法

本研究為了加速找出 BYOD 之管理邏輯，參考 H 公司導入 BYOD 的建置模型；透過實際建置出一套無線網路架構。此架構必須兼顧安全與使用便利性。所有存取皆須要通過認證，差別在於認證的方式以及加密程度不同。導入 BYOD 方案前企業體必須要先確定 BYOD 管理目標以及管理方法，明訂出可以企業內可使用設備之類型清單，如開放平板電腦存取，管制智慧型手機存取。然後再管理平台上作限制，雖然使用者可以透過無線網路架構登入，因為設備類型不在管理清單內；無法使用企業內之無線網路。BYOD 管理流程示意圖請參考[圖 4]人員存取流程。人員在使用網路資源前，必須通過相關認證。確定身分後，依照企業或組織所訂定的存取原則給予使用權限。

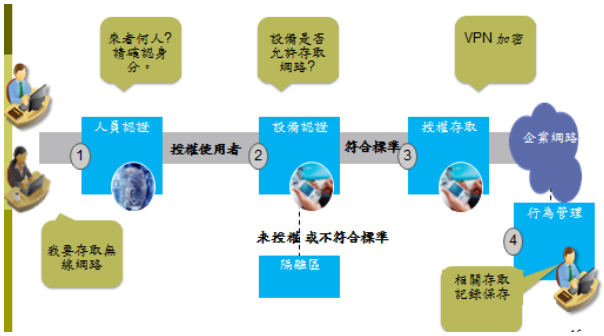

圖4人員存取流程圖

（一）H公司BYOD方案研究

H 公司目前所導入的解決方案邏輯十分簡單，區分兩個不同的無限存取識別（Service Set Identifier, SSID）一個用於公司資產的設備，另一個供 BYOD 設備與訪客使用。不同設備透過不同認證方式，認證後可存取範圍不同。透過這樣的邏輯達到簡易的 BYOD 管理。據了解 H 公司自行研發行動裝置管理解決方案尚在研發中。預計在不久將來導入。如果導入成功，可以成為下一個研究目標。[表 3]為 H 公司所制定的基本管理邏輯。

表3 H公司無線管理邏輯

	BYOD 管理邏輯		Windows,Andriod Smart Phone /Tablet ,iOSiPhone,iPAD 裝置
A.11 存取控制	A.11.4 網路存取控制	A.11.4.1 網路服務的使用政策	使用者認證
		A.11.4.2 外部連線的使用者鑑別	需要
		A.11.4.3 網路設備識別	現階段不考慮
		A.11.4.4 遠端診斷與組態埠保護	現階段不考慮
		A.11.4.5 網路區隔	套用特定 VLAN
		A.11.4.6 網路連線控制	當存取內部資料時
		A.11.4.7 網路選路控制	需要透過 ACL 隔開

本研究參考 H 公司導入之 BYOD 管理方案。員工自行攜帶裝置或訪客使用企業內部無線網路。使用前必須要先閱讀相關使用規範，使用者同意此規範後，才能申請帳號存取 H 公司的無線網路系統。不過此網路只允許存取網際網路；不允許存取企業內網。

1. 首次連線用戶

當使用者第一次拜訪 H 公司或是員工首次使用無線網路時。開啟個人設備無線網路，連線到 SSID:mobile-net。自動取得 IP 後，開啟瀏覽器後，會出現登入畫面，如下[圖 5]所示。如果首次使用，請閱讀相關說明。說明文件包含使用使用者限制以及服務條款。主要服務對象，包含 H 公司往來上下游廠商與 H 公司員工。使用 H 公司的無線網路，必須符合 H 公司全球商業行為準則，不可以透過 H 公司網路做非法行為。且 H 公司不保證所有網際網路服務皆可使用。另無線網路存取之涵蓋範圍因各分公司無線網路基礎建設之差異;H 公司不保證無線網路連線之穩定性以及連線速度。因為直接存取網際網路，H 公司不保證

訪客設備之使用安全性，如有資料遺失損毀，H 公司不負擔相關責任。另訪客必須有 H 公司內部員工代為申請臨時使用帳號。申請時必須要提供員工編號以及相關使用資訊包含訪客人數、預估使用時間、訪客單位資訊等。以作為日後稽核用途。

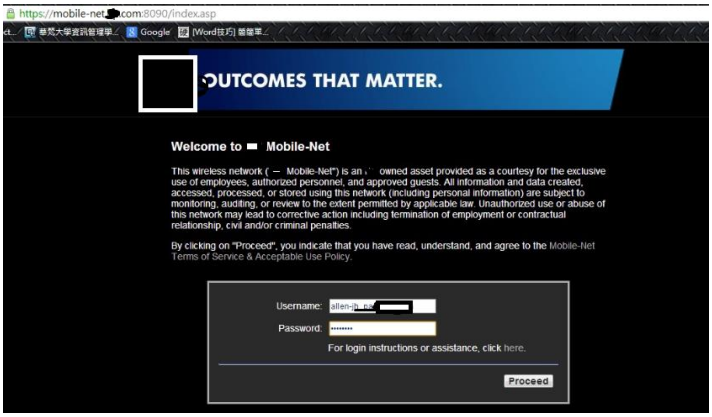

圖5 訪客線上協助系統

2. 已申請帳號用戶

已經申請帳號密碼的使用者，使用攜帶的設備連線無線 SSID： mobile-net ；自動取得 IP 之後，開啟瀏覽器使用網頁認證。員工可使用員工郵件帳號以及職工編號登入。訪客則使用申請的帳號密碼進行登入動作。如下[圖 6]所示：

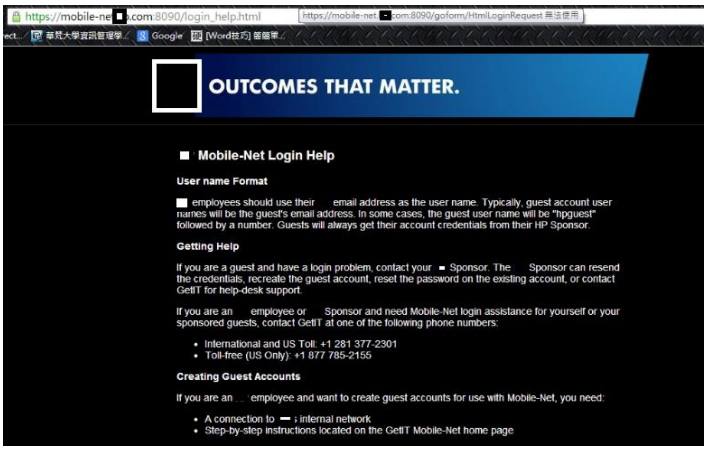

圖6 使用者登入畫面

登入完畢後的使用者，系統會自動開啟一個瀏覽器使窗。顯示使用者登入名稱以及使用 IP 與連線相關訊息。使用者如果沒有登出，則可以持續使用到申請時間終了。如果使用者中途關機，或是關閉該瀏覽器視窗；則需要重新登入方可存取無線網路。

3. 使用限制

使用者雖然透過 H 公司無線網路存取網際網路，可是不能存取 H 公司內網。使用者如果發現無線訊號不良或所在區域無線訊號不好;H 公司不保證使用頻寬與使用者行動範圍。另並非所有的網際網路服務皆可以存取。不保證使用者自行安裝的軟體可以使用正常；例如臉書遊戲（Facebook Gaming）、協同作業軟體（Unified Communications）以及需要特定頻寬管理的軟體（Quality of Service）、特定的廣播服務（Protocol Independent Multi-cast）等，H 公司不保證可以存取上述幾種類型服務。

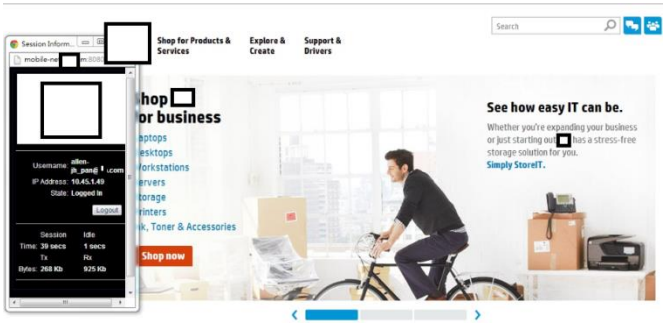

圖7 使用者登入後畫面

實際使用 PING 測試連線狀態，發現可以 PING 8.8.8.8 （Google 之 DNS 服務主機）可是無法 PING 到 H 公司內部之主機。實際使用後發現此架構可以有效區分內網以及外網的網路存取。

（二）建置測試平台與基本測試

建置一個無線網路測試平台，三層交換器負責路由以及對外網路連線設定、無線網路控制器負責控制與管理無線基地台，無線基地台負責傳廣播與遞無線訊號，傳遞訊號至認證主機等設備。本研究主要測試架構如[圖 8]所示:

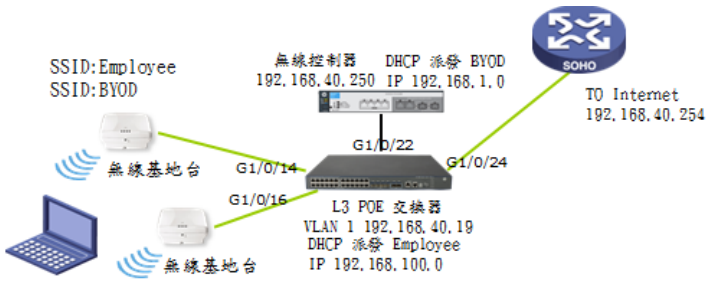

圖8 主要測試平台示意圖

本研究主要測試項目，建構一個無線控制器的無線網路環境；啟動兩個 SSID 無線網路服務，讓不同的 SSID 使用不同的認證方式，模擬 H 公司無線網路架構。本研究測試將所有認證帳號統一集中在無線控制器中，簡化整體帳號管理。但是企業實際建置上通常會區分成不同的認證主機。能夠控制存取範圍讓不同的使用者群組存取不同的網段。企業用認證伺服器主要提供員工認證使用，通常企業體會透過 Active Directory 統一做認證管理。訪客帳號則建立在無線控制器中方便管理，避免 Windows 主機中過多使用者帳號。因為 Microsoft 軟體授權在伺服器端是針對 Windows Active Directory 所開立帳戶數。也避免建立一般訪客帳號時存取主機造成資安問題。所以本研究測試將所有認證帳號統一集中在無線控制器中，簡化整體帳號管理。

表4 測試設備說明與IP分配表

設備名稱	設備用途	設備 IP
網路閘道器	對網際網路連接	192.168.40.254/24
L3 POE 交換器 HP5500-24G POE 交換器	提供無線基地台供電與 L2/L3 存取，與不同 VLAN 間路由	192.168.40.19/24 192.168.100.254/24
無線控制器 HP MSM760	管理無線基地台與派送相關設定到基地台，同時具備 DHCP Server 以及訪客認證	192.168.40.250/24
無線基地台 HP MSM4xx	廣播無線訊號以及服務終端設備	192.168.100.x/24
筆記型電腦或 iPAD	連線測試	依照不同 SSID 取得不同網段
VLAN 1	管理 IP	192.168.40.0/24
VLAN 100 SSID:Employee	員工網段	192.168.100.0/24
SSID:BYOD	訪客與 BYOD 存取	192.168.1.0/24

1. 設定三層交換器

電腦的終端管理軟體透過串列介面，連線到三層交換器上。啟動管理介面 IP 創建好虛擬網路(Virtual Area Network, VLAN)；啟動路由；並開啟交換器介面上網路供電功能 (Power Over Ethernet, PoE)

2. 設定無線控制器

首先設定電腦網路介面 IP 位址為 192.168.1.2/24，連線開啟電腦瀏覽器連線到無線控制器，重置過後的 HP 無線控制器網路介面 IP 位址為 192.168.1.1。

3. 設定網際網路閘道器

設定閘道器的目的在於三層資料交換，透過路由設定才能讓不同網段可以互通本研究架構之網段。192.168.1.0/192.168.100.0 透過閘道器轉換彼此互通。

4. 設定測試用終端設備

5. 進行基本測試

實際使用筆記型電腦或平板電腦進行連線測試。分別連線到不同的 SSID.並確認該 SSID 正常運作。檢查是否可以取得相對應的 IP 分配。並且可以存取網路

經過測試結果請參考下表 5 相關資訊。連線不同無線訊號，確實有不同的連線結果。BYOD 套用存取控管只能存取網際網路不能存取內網。主要差異在於透過網路存取控管(NAC)可以有效限制來源以及目的地。套用網路存取控管可以套用在兩的地方。一種是套用在交換器上面，另外一種解決方式套用在無線控制器上面。因為無線網路透過網頁認證的流量都會集中在無線控制器上面。所以可以透過無線控制器設定達成管理目標。在實際導入中，大多套用在無線控制器端。主要原因是避免交換器設定過於繁雜簡化交換器管理。整個控制器設定參數相當多，且各廠牌無線控制器設定方式不盡相同。實際運用請參考各廠牌使用手冊與各相關參考資訊。

表5 測試結果

存取 SSID 名稱	取得 IP 資訊	內網存取	外網存取
Employee	192.168.100.x/24	可	可
BYOD	192.168.1.x/24	不可	可

6. 測試驗證方式

實際測試的時候要確認終端設備連線到不同 SSID，通過認證後，達到 H 公司的管理需求。所以必須要確認終端設備所連線的無線基地台，讓終端設備透過無線網路有持續的流量產生，再透過封包擷取軟體；去收集封包確認測試架構符合 H 公司規劃邏輯。所以實際測試必須要針對兩個不同的測試架構下各收集資料一次次以做比對。比對後找出最接近的架構，並將相關測試結果紀錄於後。

7. 驗證測試SSID:Employee網路流量

電腦連線 SSID:Employee，確認取得 IP 網段資訊；並開啟 Ping 視窗同時 Ping 網際網路 8.8.8.8 -t 以及內網閘道器 192.168.40.254 -t 並記錄結果。

透過交換器鏡射功能(Mirroring)，擷取封包確認可由交換器端發現終端設備封包，代表該封包未透過控制器數位通道。

8. 連線測試SSID:BYOD 網路流量

電腦連線 SSID:BYOD，確認取得 IP 網段資訊；並開啟 PING 時 PING 網際網路 8.8.8.8 以及內網閘道器 192.168.40.254 並記錄結果。

透過交換器鏡射功能(Mirroring)，擷取封包確認封包轉發方式。

4. 結果與分析

經由本研究參考 H 公司所導入 BYOD 解決方案的測試結果。發現 H 公司的管理邏輯相當簡易。但是實際要模擬出整個架構，卻有相當難度。主要原因在於一般網路架構通常規劃二層與三層的網路存取，透過網路存取控管（NAC)達成。可是 H 公司的架構卻是使用數位資料通道的方式（Data Tunnel)。筆者期初對無線網路架構不甚熟悉。也花許多時間收集資料。所有訪客與員工攜入式設備線網路全部 Tunnel 在無線網路控制器上面。這樣的架構與之前筆者所接觸到的無線架構不同，相對上在收集資料與實際測試花費許多時間。其實業界有許多不同網路廠商在無線網路控制器上都支援數位資料通道的方式，建置上可以請廠商協助。

5. 結論與建議

任何改變對企業與組織都一定會有相對上的衝擊。不過相對上也會有帶來其效益。極大化組織維運的績效是現今許多企業與組織追求的目標。而且現今社會演變之快速已經超過十倍速時代。筆者認為每個人都應該具備適度的適應性以及學習力；以符合現今社會的挑戰與衝擊。導入可攜式設備的管理（BYOD）對企業與組織而言，不能只看到產能增加與期初資訊費用的節省；必須要能夠更宏觀的去了解。開放後潛在資訊安全風險以及管理的問題[14]。

本研究了解現今企業所面臨的窘境，所以未了達到 BYOD 的管理目標。透過 H 公司的個案研究發現。有下列兩點發現：

1. 保障既有投資，開放BYOD不必額外添購設備
2. 調整暨有無線網路可建置基礎的BYOD解決方案

其實相同的資訊產品，在不同的管理與設定邏輯下；有許多不同的彈性；並非需要再投資新設備或是導入新的解決方案才能夠達成目標。在本研究中，終端設備的辨識不在考慮範圍內。主要原因是 H 公司只開放網際網路存取，對於企業內網是採用完全隔離機制。這樣的好處是架構簡單容易維運與管理。不過這些終端設備如果需要存取內網就必須要透過虛擬私有網路（Virtual Pravite Network, VPN）來達成。這樣的話所有存取的網路流量會透過網際網路再傳回企業體，等於是占用兩次網際網路頻寬，加上一般 VPN 計費標準是看終端用戶的人數來計算。整體使用成本需要精算過；才能決定是否導入該專案。期待透過本研究，可以有效幫助國內企業與相關單位；在導入 BYOD 解決方案時，可以參考本架構節省建置成本。本研究 BYOD 主要在於區分設備存取網路達成存取分流，但未針對應用程式與終端設備相容性作討論。EMM 的概念主要探討行動設備所使用的企業體應用軟體整合方案[16]；而導入 WIPS 可以避免因為內部員工異常無線網路，避免駭客使用相同 SSID 騙取公司同仁帳號密碼造成資安問題[17]。未來組織再擴充新解決方案時，建議可把下列兩個部分列入考慮：

1. 企業可攜式設備管理(Enterprise Mobile Management, EMM）

2. 無線入侵防禦系統（Wireless Intrusion Prevention System, WIPS）

6. 參考文獻

[1] 陳祥輝，TCP/IP 網路通訊協定第二版，博碩文化，2012：頁 10-5。

[2] 中華民國經濟部標準檢驗局，資訊技術-安全技術-資訊安全管理系統-要求事項，CNS-27001:2007。

[3] 中華民國經濟部標準檢驗局，資訊技術-安全技術-資訊安全管理之作業規範，CNS-27002:2007。

[4] 中華民國經濟部標準檢驗局，資訊技術－安全技術－資訊與通訊技術安全管理－第 1 部: 資訊與通訊技術安全管理概念與模型，CNS-14929-1:2008。

[5] 中華民國經濟部標準檢驗局，風險管理－原則與指導綱要，CNS-31000:2009。

[6] 李美雯，“你的單位 ISMS 了沒”，*國立臺灣大學計算機及資訊網路中心電子報*，第七期，2008：http://www.cc.ntu.edu.tw/chinese/epaper/0007/20081220_7005.htm。

[7] 無線網路安全白皮書，台灣電腦網路危機處理既協調中心，民 92 http://www.cert.org.tw/docfile/Wireless_Security.pdf

[8] 推動 BYOD 的 3 大安全控管作法 2012-05-06 http://www.ithome.com.tw/itadm/article.php?c=73587&s=1

[9] 員工自帶設備上班:BYOD 的兩難，黃彥棻 2012-05-06 http://www.ithome.com.tw/itadm/article.php?c=73696

[10] 經理人月刊 BYOD，帶自己的行動裝置來上班! http://www.managertoday.com.tw/?p=12359

[11] 思科新聞稿:企業擁抱 BYOD 趨勢 2012-05-31 http://www.cisco.com/web/TW/about/news/news_20120531.html

[12] Canalys Press release 2012-3-21 Feburuay 2012 Smart phone overtake client PCs in 2011 http://www.canalys.com/static/press_release/2012/canalys-press-release-030212-smart-phones-overtake-client-pcs-2011_0.pdf

[13] Don’t count on BYOD cost savings, experts say 2012-07-02 http://searchconsumerization.techtarget.com/news/2240159031/Dont-count-on-BYOD-cost-savings-experts-say

[14] BYOD woes:Appmanagement,licensing’compliance http://searchconsumerization.techtarget.com/guide/BYOD-issues-App-management-licensing-compliance-and-more

[15] Sampson Lisa, Mobile device security best practices for BYOD http://searchnetworking.techtarget.com/feature/Mobile-device-security-best-practices-for-BYOD

[16] Stacy K. Crook Stephen D. Drake Benjamin Hoffman IDC Market Analysis Worldwide Mobile Enterprise Management Software 2012-2-16 Forecast and Analysis and 2011 Vender Shares http://idcdocserv.com/236835e

[17] Seltzer Larry 2012 Oct 4 MDM is Dead , Long Live EMM http://www.informationweek.com/byte/personal-tech/mobile-applications/interop-mdm-is-dead-long-live-emm/240008495

[18] Phifer Lisa, Wireless IPS Buyer's Guide 2012 http://www.wi-fiplanet.com/reviews/ST/wireless-ips-buyers-guide.html