國立交通大學

資訊管理與財務金融學系

資訊管理碩士論文

一個利用行動代理人解決企業外購系統服務安全問題的架構

A mobile agent based architecture to deal with the security problem on enterprise IT-Service outsourcing

研 究 生： 黃 振 瑋

指導教授： 羅 濟 群 教授

中華民國 103 年 1 月

一個利用行動代理人解決企業外購系統服務安全問題的架構

A mobile agent based architecture to deal with the security problem on enterprise IT-Service outsourcing

研 究 生：黃 振 瑋　　Student: Zhen-Wei Huang

指導教授：羅 濟 群　　Advisor: Chi-Chun Lo

國立交通大學

資訊管理研究所

碩士論文

A Thesis
Submitted to Institute of Information Management
College of Management
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science in Information Management
Jan 2014
Hsinchu, Taiwan, the Republic of China

中華民國　103 年　1　月

一個利用行動代理人解決企業外購系統服務安全問題的架構

研究生：黃振瑋　　指導教授：羅濟群 教授

國立交通大學

資訊管理研究所

摘要

企業中的許多資訊系統與資訊服務，例如 ERP 系統、郵件系統，伺服器服務等，由於自行開發成本高，時程長，且維護運作需有額外的金錢和人力，因此在導入資訊系統和資訊服務時，會考慮採用外購服務軟體的方式，來節省自行開發的投資。本篇論文著重在，企業將外購系統和服務導入之後，如何快速地處理錯誤，有效率地進行系統維護與管理，同時兼顧企業的網路安全性與資料機密性，這些都是讓系統能有效發揮其預期效益的關鍵。

本篇論文針對此管理問題，提出以行動代理人(Mobile Agent, MA)技術來管理，於安全通道(Secure Tunnel)上，做到錯誤資訊的自動化收集與處理。Mobile agent 具備的自主性(Autonomy)和行動性(mobility)，能獨立判斷所接收的資訊，並做出相對應的處置動作，可提高管理上的效率，大幅降低人員的工作量。同時又能在企業原有的網路環境下運作，不需大幅更動企業的網路配置與設定，一樣可以滿足企業對網路安全的要求。

關鍵字：行動代理人、虛擬私人網路、伺服器管理、企業外購

A mobile agent based architecture to deal with the security problem on enterprise IT-Service outsourcing

Student: Zhen-Wei Huang Advisor: Dr. Chi-Chun Lo

National Chiao Tung University

Institute of Information Management

Abstract

In the enterprises or companies, many information systems and IT-Services, such as ERP system, mail system, and server services, have higher cost and longer development time due to the self-development process. Extra money and labors are needed to maintain these systems. Therefore, enterprise IT-Service outsourcing would be adopted to save the investment of integrating the IT-Service. In this paper, we focus on the issues of maintenance, such as fixing the error more quickly, maintaining the system more efficiently, keeping the network security and the data confidentiality of the enterprise, which are the key points to meet the IT-Service performance expectation.

In this paper, we propose the mobile agent to manage these issues by automatically collecting the error info and error handling through a secure tunnel. The mobile agent, has the attributes of autonomy and mobility, can independently determine the receive information and taking the corresponding actions, that would improve the efficiency of management and reduce the labor burden. Meanwhile, it can be operated on the original enterprise network environment, without changing the network deployment and setting, to meet the need of enterprise network security.

Keyword ： Mobile Agent, VPN, Server Management, Enterprise Outsourcing.

誌謝

首先感謝指導教授羅濟群老師，給我學業上的指導和生活上的協助，諄諄教誨為我指引出方向並包容我的錯誤，使我在遭遇挫折時能繼續前行。感謝交大資管所陳安斌教授、中央資管所周世傑教授，在百忙之中擔任學生的碩士論文口試委員，提供寶貴意見，使論文能具有更完整的架構、指點出新的思考和未來研究方向，由衷地感謝指導老師和口試委員。

感謝泊寰學長，提供實務上的深厚經驗，帶領我進行專案的研究，耐心地協助我完成論文，與我分享許多進行研究的心得和學習心法，獲益良多。感謝鼎元學長和栩嘉學姐在課業上的指導和幫忙，也感謝志華同學，除了專案上的合作與協助，他認真的研究精神一直是我學習的榜樣。感謝淑惠助理，細心地處理我在所上這段時期大大小小的事務。感謝在交大這段時期的師長同學們，以及遇到的人們，每一次的交流往來，都點點滴滴地累積而成就著我。

也感謝我的家人，父母親和兩位弟弟一路地支持，讓我更有動力去面對挑戰、克服困難。最後，更要感謝並分享我最大的喜悅，給我的伴侶雯君，鼓勵著我，與我相伴扶持，讓我心靈上能持續地存有著溫暖。

目錄

圖目錄

表目錄

第一章 緒論

1.1 研究背景與動機

資訊科技對現在企業的營運，越來越重要。企業中常見的系統包括，從整合企業資源的企業資源規劃系統 ERP(Enterprise Resource Planning)、郵件系統，到一般性的辦公室自動化 OA(Office Automation)系統。企業在規劃資訊系統的建置時，會先以專案方式來做評估[2]，評估的面向包括：硬體、軟體、資訊服務，這三項。導入的方式會分為：自行建置和外購兩種。企業在資訊技術發展快速與競爭激烈環境中，在建置成本和時效的考量上，多採用外購系統服務的方式來導入資訊系統[3, 4]。

企業的外購系統服務的導入，可分為前中後三期：

一、前期的規劃：依照企業自身的需求和能力，決定外購系統服務的比例：是要百分之百，軟硬體全由資訊系統服務商包辦，或是部分由企業、部分由服務商。

二、中期的建置：包括與現有系統的整合、或是將整個舊系統汰換成新系統。人員的教育與訓練，系統的測試與修正等等。

三、後期的維護：導入後系統運作的維護，是以內部人員來負責，或外部服務商負責，還是兩者協同維護，若是兩者協同，其職責需做有明確的區分。

在各階段，企業都可以評估其所需投入的成本，來控制其外購服務的預算，但在後期的維護的階段，卻有很多的隱性成本，這包含了：一、持續的人員教育訓練成本，二、系統運作的水電成本，還有，三、佔了大部份的風險成本：很多系統是在上線之後，實際使用時，問題一個接一個冒出來。這些風險該要由誰來承擔，錯誤的發生又該如何修正，都是管理上要思考的問題。企業和服務商的關係並不在系統上線後就結束，後續的系統管理，更是兩者需合作解決的目標。

企業和服務商為了解決外購系統，在後期維護的管理問題，服務商考量成本和效益，多採用遠端安全管理的方式[5]。以企業的角度，當然希望系統維護的成本，是由服務商承擔，但服務商在有限的經費與資源下，除非企業願意持續付費，否則，多不願意承擔此責任。若企業的系統，建置後是保護在企業內網路，則外部服務商就必須進到內部去做維護，假設今天服務商賣出系統給數百家企業，在維護時，人員就需在這數百家企業間奔波，且各企業系統建置規格不一定相同，這又會造成管理上的困難，所以服務商多以遠端的方式，來實作系統的維護與管理，避免掉人員的移動上成本，並能集中管理，增加維護效益。

1.2 研究目的

本論文中提出一個利用行動代理人來遠端管理企業系統伺服器的架構，，以解決服務商和企業，在系統維護上，對企業伺服器的管理問題。行動代理人已被應用在許多領域中[4]，是一種達成網路管理自動化的有效方式[6-8]。本文提出的以行動代理人為基礎的架構，在企業外購系統服務上，可以克服的管理問題，包括：一、降低人員移動成本。二、整合不同企業系統規格[9]。三、協助企業內外部人員合作。四、保護企業內部資料的安全。五、克服企業防火牆的限制。六、錯誤事件的有效過濾和解決。

1.3 研究架構

第二章將針對相關的主題做文獻探討，其內容包括；第三章則對本論文所提出的研究方法做詳細介紹；第四章則介紹使用本論文提出的架構後所具有的效益分析；第五章為結論與未來研究方向

第二章 文獻探討

本論文的行動代理人之架構所考量到的因素，將在此章節分三部分探討：首先是行動代理人的介紹與運作機制。第二是虛擬私人網路(VPN)的介紹，及運作與管理問題；第三是安全通訊端層(SSL)的架構和比較

2.1 行動代理人(Mobile Agent)

行動代理人為一個可自主化，可獨立進行分散式運算與處理的程式，具有可在網路內各個電腦間移動的能力。其運作的基本原理為，當行動代理人在系統內被產生，並接受使用者所提出的任務後，於網路環境內任兩端點的電腦設施間移動，收集資訊、執行運算，並將最後的結果傳回。透過這樣的運作方式，行動代理人可提高分散式系統的運行效率，並減少電腦間資訊的傳遞次數和延遲，增進使用的便利性。

2.1.1. 行動代理人的特性

行動代理人具有以下特性：

一、自主性(Autonomy)：

行動代理人可自主運作、自我控制，並根據其執行環境和執行結果，收集訊息，藉以決定下一個採取的動作，不會受其他使用者或系統的干涉。

二、行動性(Mobility)：

行動代理人可以在網路環境內的各個電腦間移動，這是行動代理人最主要的特色。

三、目標導向(Goal-Driven)：

使用者可在將行動代理人派發至網路前，設定行動代理人執行任務的特定目

標，交付其完成。

四、協同(Collaboration)：

行動代理人之間可透過程式語言的溝通或資料的交換達成任務的協同合作。

五、時間上連續(Temporally continuous)：

行動代理人在任務執行上，除了連續不間斷執行外，可以暫停一段時間後，再繼續執行任務，在控制上具有更多彈性。

六、學習能力：

行動代理人根據執行任務所收集的資料，可累積任務處理經驗，以利後續任務的完成。

2.1.2. 行動代理人的應用

基於行動代理人的特性，其主要的應用範疇為：

一、分散式系統的遠端處理：

在分散式系統上，可藉由行動代理人，攜帶壓縮後的程式碼，到遠端的電腦上執行，藉以降低網路上資料傳輸的通訊量。藉由行動代理人在遠端電腦上的移動和存取，降低網路流量負載的負擔，提升效率。

二、非同步處理

行動代理人在到達接收端的電腦後，發送和接收兩端的網路連線就不需要一直維持在連線狀態，行動代理人可自主地在接收端電腦運作，執行所賦予的任務，待連線恢復後，再傳送執行結果和收集訊息或攜帶程式碼回到發送端。

2.2 虛擬私人網路(Virtual Private Network, VPN)

目前，企業多採用虛擬私人網路來建構企業網路環境，虛擬私人網路對外部

網路使用了網際網路(Internet)架構來連結，大幅降低建構成本，同時又具有如同專用網路般的安全性。企業在架構虛擬私人網路時，為了保護企業內部網路(Intranet)的安全，防止內部機密資料的外流，或外部人員對企業內部網路資料的竊取與破壞，通常會以架設防火牆(Firewall)的方式，隔絕外部網路對企業內部網路的直接連結，所以在採用遠端管理的方式時，會遇到企業防火牆的問題。

2.2.1 以網路安全協定為基礎的虛擬私人網路(IP-Sec based VPN)

傳統上的作法，是以網路安全協定為基礎的虛擬私人網路(IP-Sec based VPN)，來達成內外部網路的連結[10]。若外部網路是使用行動裝置為連線裝置，則可再結合行動網際網路協定(Mobile IP)。

2.2.2 IP-Sec 介紹

私人虛擬網路(VPN)在應用上可透過網際網路(Internet)來連結，而網際網路是以 IP(Internet Protocol)為連線基礎，在 IP Layer 處理安全問題，在 IPv6 制定時，獨立為網際網路層安全協定(IP Security Protocol, IP-Sec)。

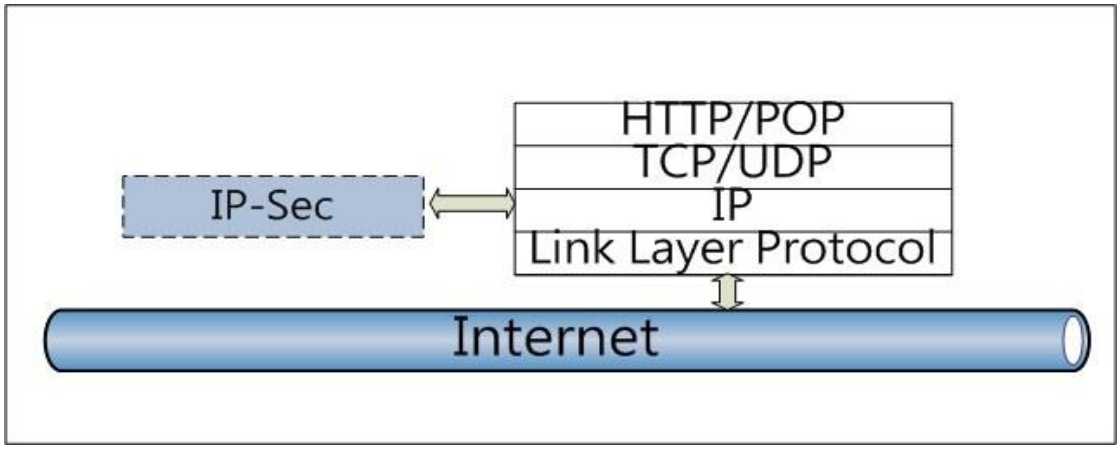

圖 1：IP-Sec 關係圖

IP-Sec 的安全協定：

AH（Authentication Header）

利用 Hash function，提供封包來源的驗證、檢查封包內容的一致性，若 IP 封包在網路上傳輸時，遭篡改或是偽裝，可依此查驗出來。

ESP（Encapsulating Security Payload）

ESP 結合加密演算法和 Hash function，對封包內容加密，可防止封包遭到竊取，亦具有類似 AH 的驗證能力。但 ESP 協定對於防止封包的篡改或偽裝的能力相較於 AH 仍較弱，因此 ESP 雖具有類似 AH 的驗證功能，但還未完全可取代 AH。

IP-sec 的封裝機制

Transport Mode

Host-to-Host 的封裝機制，由連線的兩端皆有 IP-Sec 實作的主機，對所交換的 IP 封包，採用 AH 或 ESP 的安全協定來達成保護，

Tunnel Mode

Gateway-to-Gateway（or Host），一端的主機先將尚未作安全保護的 IP 封包傳送至具有 IP-Sec 功能的 Security Gateway，Gateway 再將封包以 IP-Sec 保護後，傳送至遠端的 Gateway，接收端再將 IP-Sec 的保護機制解除並還原後，把 IP 封包發送至目的端的主機。

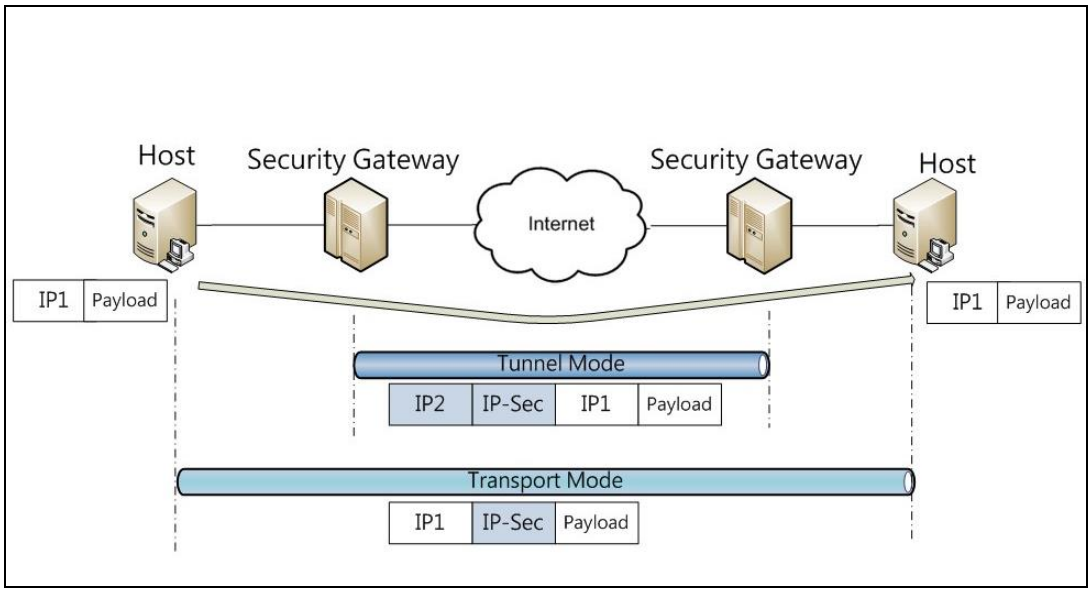

圖 2：IP-sec 的封裝機制

在實務上，當身處在公司外部網路的人員，不在公司的私人虛擬網路內時，想要由移終端(Terminal)，如個人電腦或筆記型電腦等，進入公司網路內的系統伺服器，做管理或資料存取，會產生如下的問題：由於這些資料是由企業網路內部的伺服器所管理，從防火牆外部存取資料，需先建立對企業內部網路伺服器的連結，才能夠互傳資料，而防火牆會限制外部網路的直接連結和資料存取。防火牆的主要功能是在控管內部網路以及外部網路之間的資料交換，阻絕不安全的連線，以避免未授權的網路連線，進入企業的網路安全協定的私人虛擬網路，而上述的 IP-Sec VPN 的設備應置於何處，是建置在防火牆的內部網路、外部網路，是另外開一個平行於防火牆的網路區域來放置，或是直接由防火牆來提供網路安全協定的服務。企業該採哪一種方式，才能提供安全可靠的虛擬私人網路服務，同時又不損害防火牆原有的保護機制？這個問題並沒有唯一的答案，也沒有絕對正確的答案，各項設置模式都有其優缺點，需視企業實際情況與需求而定。[11, 12]

2.3 安全通訊端層(Secure Socket Layer, SSL) VPN

SSL VPN 是以瀏覽器為基礎的遠端存取安全機制，在用戶端使用瀏覽器連線 SSL VPN，以 HTTPS 協定建立兩端點之間的安全連線通道， SSL 所提供資訊傳輸安全保護，內部使用者只要能夠以瀏覽器開啟網頁，便能夠順利連線到企業的內部網路，而外部網路的使用者，使用瀏覽器與 SSL VPN Gateway 建立連線後，以帳號密碼登入，通過認證之後，便能進入企業內部網路，取用企業內開放的資源。SSL 提供加密演算法(RSA & DES, RC4 等)和 Hash Function(combined MD5 & SHA)，供網路通訊的安全服務，已達成以下幾項安全要求：身份識別(Authentication) ，識別通訊雙方的身份，防止遭偽裝的資料。資料隱密性(Confidentiality)，傳遞的資料為密文，防止通訊被竊聽。資料完整性(Integrity) : 保持資料完整，防止竄改。

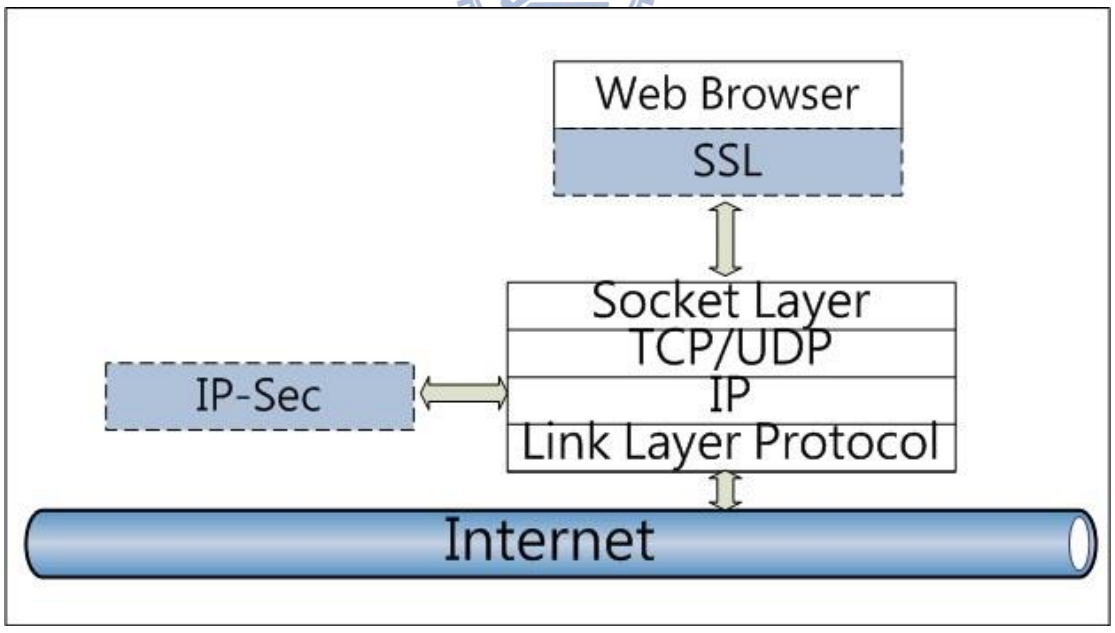

圖 3：SSL 關係圖

2.3.1.SSL 握手協定(Hand Shake)

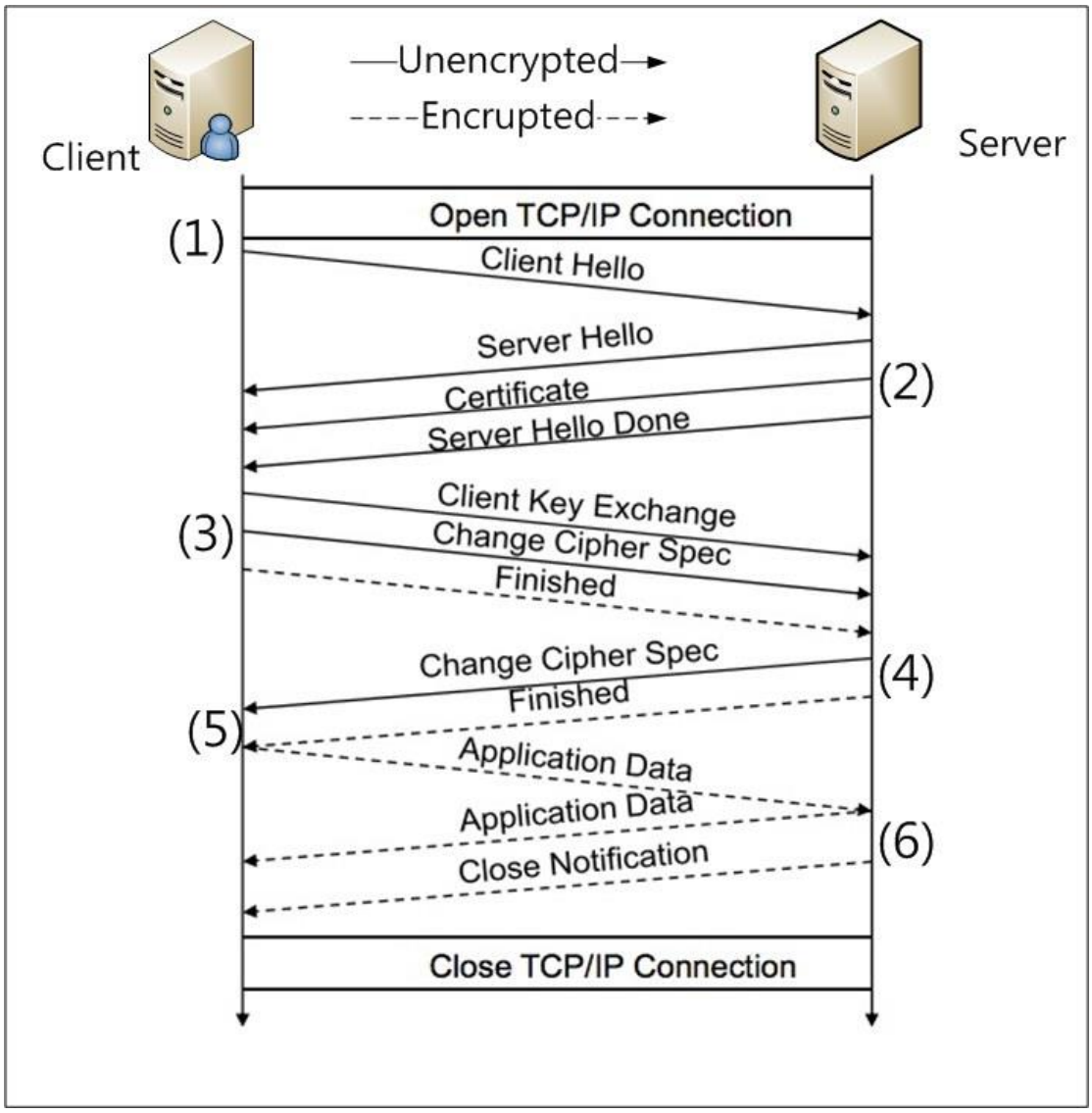

圖 4：SSL 握手協定

(1)用戶端利用 Client Hello 將本身的 SSL 版本、加密演算法、等資訊發送給伺服器端。伺服器端收到後，確定本次通訊所採用的 SSL 版本和加密演算法後，以 Server Hello 回覆給用戶端。

(2)伺服器端利用 Certificate 訊息將本身公鑰的數位憑證傳遞給用戶端，Server Hello Done 訊息告知用戶端自身的版本和加密相關訊息，協商結束，並開始進行

密鑰交換。

(3)用戶端驗證伺服器為合法之後，利用伺服器所給的公鑰來加密用戶端隨機生成的一組 46 位元亂數，以 Client Key Exchange 發送給伺服器。Change Cipher Spec 通知伺服器之後的內文將會採用協商後的密鑰和加密模組進行加密。用戶端計算已握手的 Hash 值，以協商後的密鑰和加密模組處理 Hash 值，以 Finished 發送給伺服器。伺服器以同樣的方式計算 Hash 值後和 Finished 的解密後的值比較，若相同，則協商成功。

(4) 伺服器端以 Change Cipher Spec 告知用戶端，後續的傳輸將會以協商成功的密鑰和加密模組進行加密。通知用戶端之後的內文將會採用協商後的密鑰和加密模組進行加密。伺服器端計算已握手的 Hash 值，以協商後的密鑰和加密模組處理 Hash 值，以 Finished 發送給用戶端。用戶端以同樣的方式計算 Hash 值後和 Finished 的解密後的值比較，若相同，且 MAC 值驗證正確，則協商成功。在用戶端接收到伺服器發送的 Finished，若能解密成功，則可驗證伺服器是數位證書的所有者，也就驗證了伺服器的身分。

(5),(6)雙方驗證完畢後，以協商好的加密方式加密傳送所需的 Application Data，最後伺服器端送出 Close Notification 結束這一次的通訊

接下來以一間企業的郵件伺服器與行動終端的連結為例，說明 SSL VPN 的應用和會遇到的問題，布建在網路環境上的設施包括：

公共伺服器(Corporate Server)：放在企業內部，負責企業系統的資訊處理與儲存。此設施依不同的企業狀況，可為 Mail Server、ERP Server、OA Server 等。

企業伺服器(Enterprise Server)：放在企業內部，負責讀取 Corporate server，將資料加密後傳送到使用者終端。

防火牆(Firewall)：分隔內外部網路環境，負責保護企業內的網路安全。

載體閘道器(Carrier Gateway)：放置在系統服務業者機房的閘道(Gateway)設備，負責將使用者終端與企業配對，建立安全通道，為網路設備。

終端裝置(Terminal Device)：使用者使用的設備，可以是個人電腦、筆記型電腦、甚至是無線裝置。

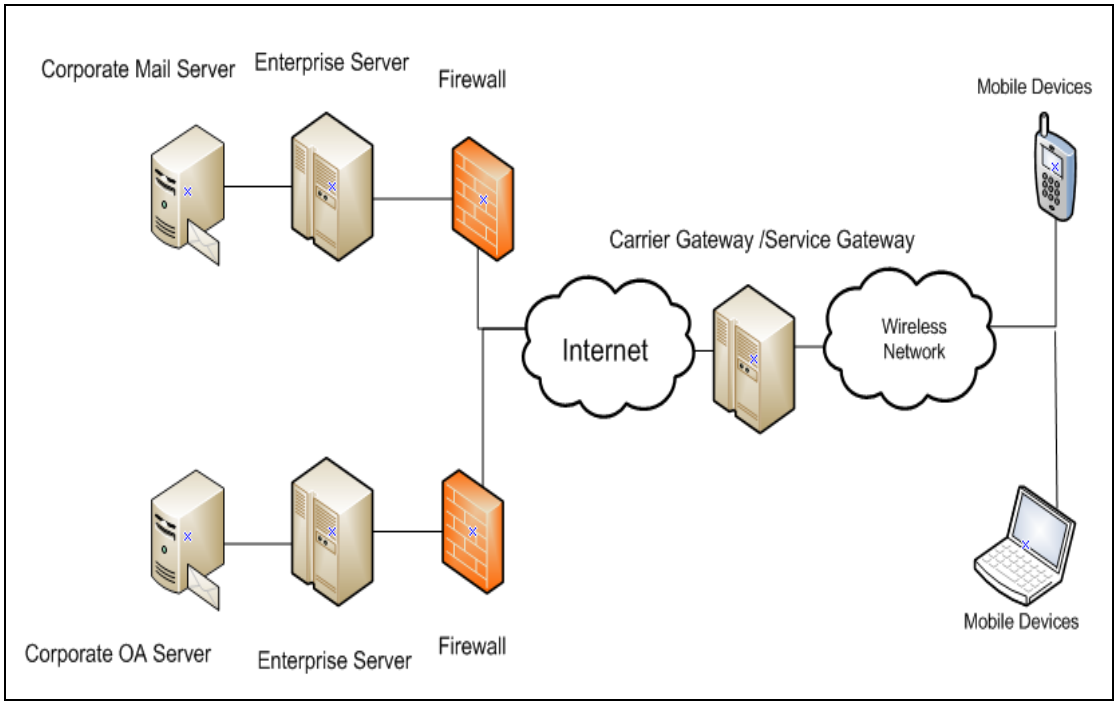

圖 5： SSL VPN of Push mail Services

當身處公司外的員工，要收發公司的郵件時。在這之前，需先建立一個安全通道(Secure Tunnel)，一般狀況下，安全通道的建立是由外部往內部，採用安全通訊端層的虛擬私人網路架構(SSL VPN)[13]，如上述所說明，SSL 具有很好的資料加密性，自由度也高，但高自由度同時也是他的缺陷，外部利用瀏覽器即可接觸到內部網路，此作法雖然方便，對防火牆內的企業網路會有潛在的安全威脅，而企業為強化內部網路的安全性，會提高防火牆的限制，這樣又會犧牲掉便利性。在便利性和安全性的權衡尚須找到一個合適的方式。

2.3.2.反向安全通訊端層(Reverse SSL)的架構

另一種作法是，由內而外建立安全通道[14]。企業內部網路內的企業伺服器(Enterprise Server)，主動連線到防火牆外的載體閘道器(Carrier Gateway)，在此將企業與移動式終端設備(Mobile Devices)做配對，建立安全加密通道(Secure Tunnel)，由於由內到外的連線建立，在通過防火牆時，情況較單純且好管理，防火牆開 port:80，走安全通訊端層(SSL)，如此一來，就可在不更改防火牆(Firewall)設定的前提下，讓移動式終端設備(Mobile Devices)可以和企業內部網路內的伺服器，進行具安全性的雙向資料傳輸。

2.3.3 反向安全通訊端層(Reverse SSL)、安全通訊端層(SSL)與網路安全協定（IP-Sec）在 VPN 上應用之比較

下表比較了 Reverse SSL VPN 和 IP-Sec VPN 的不同[15]。Reverse SSL VPN 在使用上比 IP-Sec VPN 更便利，也兼顧安全性，非常適合行動代理人的自動化的遠端管理運作。

項目	Reverse SSL VPN	IP-Sec VPN
連線建立	由內而外連線，可突破防火牆限制，同時避免來自外部的攻擊。	由外而內連線，不同的用戶端走不同的孔道受限於防火牆設定。
行動代理人適用性	適合行動代理人的自動化運行	行動代理人為配合 IP-Sec 架構，自動化設定會複雜。
遠端管理	可做到中央管理大量企業的遠端監控	可遠端連線，但不同企業有不同 IP-Sec 設定，不容易做到中央管理大量企業的遠端監控。
支援的應用	基於 web 的應用	所有支援 IP 協定的服務
安裝	安裝軟體較少，即插即用安裝。	安裝軟體較複雜，需長時間做硬體配置。
可擴充性	擴充時時，客戶端不需做大量設定與配置更動，依循標準 Web 設定即可通過 SSL 認證來連線	伺服器端易擴充，但用戶端須做複雜的軟體安裝和硬體配置更動。
費用	低	高

表 1 ：IP-Sec VPN，Reverse SSL VPN 之比較

Reverse SSL 是由 SSL VPN 所改良而來的，最主要的差別是在於連線方式，Reverse SSL 改用了由內而外的連線建立方式，繼承 SSL VPN 建置方便的最大優點，也確保了安全性。

項目	Reverse SSL VPN	SSL VPN
連線建立	由內而外連線，可突破防火牆限制，同時避免來自外部的攻擊。	由外而內連線，走單一孔道，較不受於防火牆設定，但也由於單一孔道，亦受外部攻擊。

表 2：Reverse SSL 與 SSL VPN 之主要差異

第三章

一個利用行動代理人解決企業外購系統服務安全問題的架構

在本章中，將以郵件系統伺服器的管理為例，就會遭遇的管理問題作探討，並介紹本論文所提出架構方式如何解決這些問題。

3.1 問題定義

在管理郵件系統伺服器的情境中，於反向安全通道架構下所會遭遇的問題如下：當企業位於外部網路的員工，無法正常地收發郵件，也就是錯誤發生時，企業內的 MIS 人員，會聯絡郵件服務的技術人員做修正，若錯誤發生在企業內部網路的共同郵件伺服器，會增加技術人員處理的難度。由於這項設備是被保護於企業虛擬私人網路所部屬的防火牆內，位於外部網路的技術人員，有幾個處理的方式。一個是技術人員，親自進到企業內部去檢測，這方式舟車勞頓，耗時費工。另一個作法，就是技術人員和內部 MIS 人員協調、來回溝通，找出錯誤，再由技術人員協助 MIS 人員在內部做處理。此方式在實務上，因業務責任劃分的問題，多不可行。最後一個方式，是以遠端方式進入伺服器做檢測，但從遠端進入，在防火牆顧及安全性的保護下，難以獲得詳細的錯誤訊息，無法作及時有效的處理。此外技術人員為了處理發生在不同企業、不同伺服器的不同錯誤，需花費許多時間與金錢的成本，大大降低管理的效率。基於以上幾點，我們尋求一個解決方案，能做到自動收集各個錯誤訊息，及時地處理，作定時的檢測，保持伺服器執行的效率，方便人員作錯誤處理和管理。

在此，提出行動代理人方式來改善這個問題，達成所預期的目標。在由內而外，建立反向安全通道的架構下，運用行動代理人，代替人力去處理網路狀況檢測，錯誤訊息收集，錯誤及時處理等動作，能提升網路管理效益，同時能達到企

業網路的安全性，確保資料隱密性。

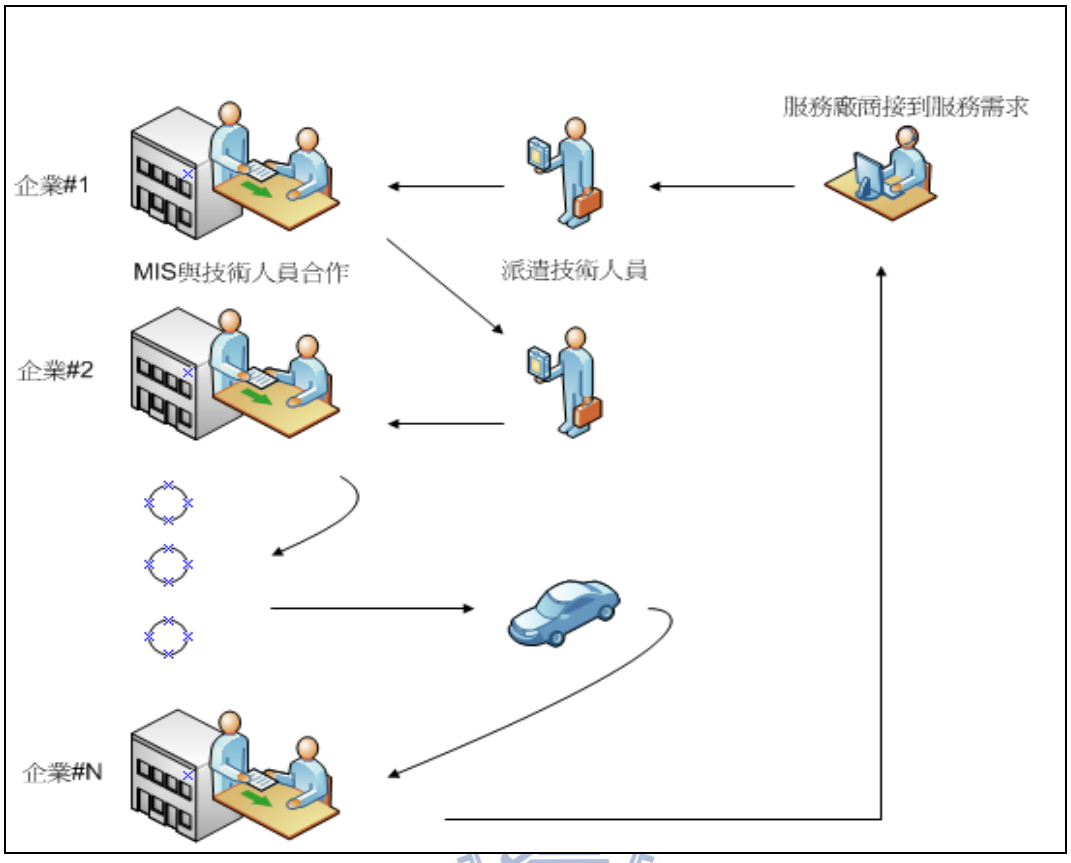

圖 6：未使用行動代理人的維護方式

圖二中顯示，在未使用行動代理人前，技術人員必須往來於不同的企業之間，和企業的 MIS 人員共同維護企業伺服器，耗時，費工，效率低。

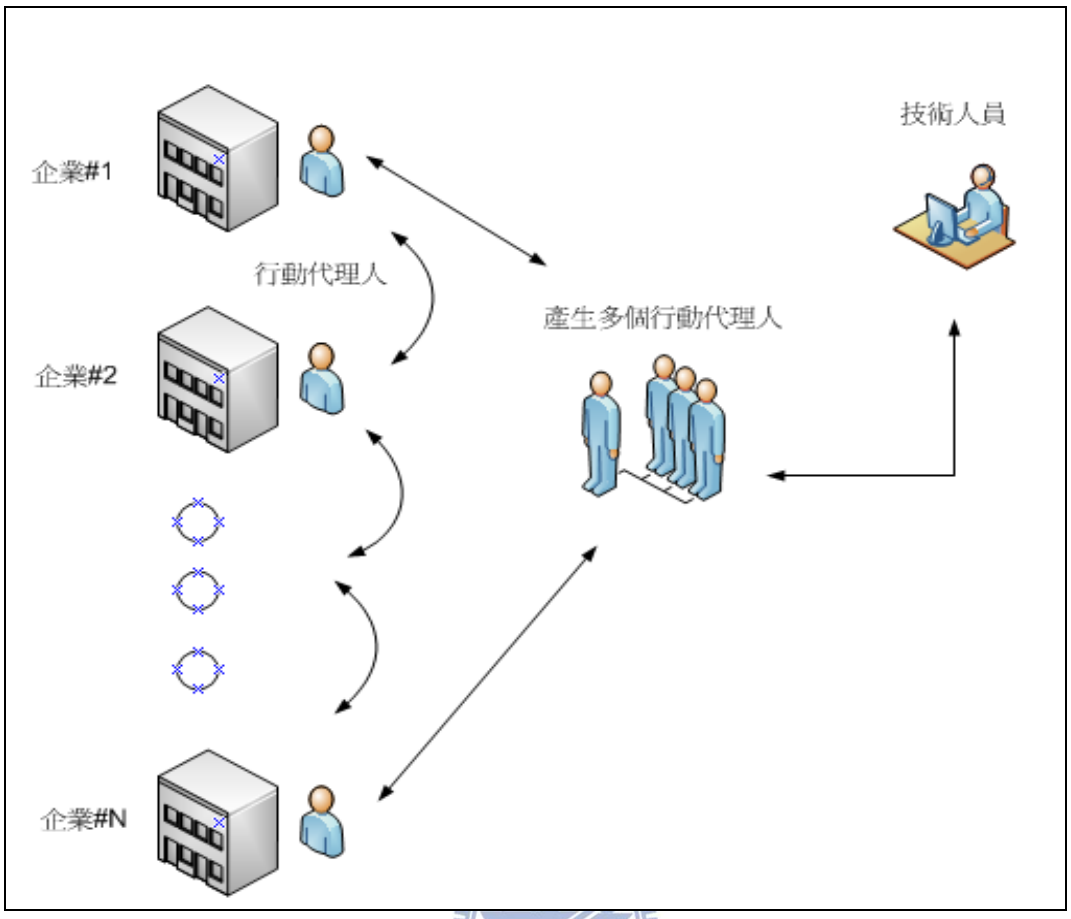

圖 7：使用行動代理人的維護方式

技術人員用行動代理人來管理，可發射多個代理人，至各企業的伺服器做系統維護，或是發射單一行動代理人於企業間做輪詢式的伺服器維護。[16, 17]

3.2 反向安全通訊端層上的行動代理人運用(Mobile Agent on Reserve SSL VPN)

3.2.1 行動代理人運作架構

本論文提出一個以行動代理人為基礎的架構，來解決企業外購系統服務後，外部公司的技術人員和企業內部 MIS 在企業伺服器上的管理問題。

本架構中的人員角色有以下三種：企業內資訊系統管理人員(MIS)，外部的技術支援人員(Technical supporter)和開發人員(Developer)。後兩者也可合稱為技術人員。

企業資訊管理人員：

負責擔任企業與技術人員的聯絡，維護企業伺服器的正常運作，當與發生與郵件服務相關的問題與錯誤時，會尋求技術人員的協助與解決。

開發人員：

依據企業資訊管理人員所提出的管理功能需求，設計出具有不同功能行動代理人程式，並以 Python 開發撰寫行動代理人的實作程式。

技術支援人員：

撰寫好的行動代理人，存放於電信業者的管理伺服器(Management Server)中，由技術支援人員負責維護，管理伺服器與各項功能的正常運作。

各個具有不同功能的行動代理人程式，由存放於管理伺服器中的行動代理人發射器(Mobile Agent Launcher) 透過建立好的安全通道，發射至企業內，位於企業伺服器中(Enterprise Server)中的行動代理人接收器(Mobile Agent Receiver)，做各項檢測和錯誤修正，以及收集相關資訊。由於各項運作是在企業內部完成，資料收集也是在內部完成，回傳至外部的資訊只有錯誤訊息(Error Log)，不包含企業內的相關資訊，並透過 SSL 加密，確保了資料的安全性與機密性。技術支援人員則透過回傳的錯誤訊息，來做後續的處理動作。

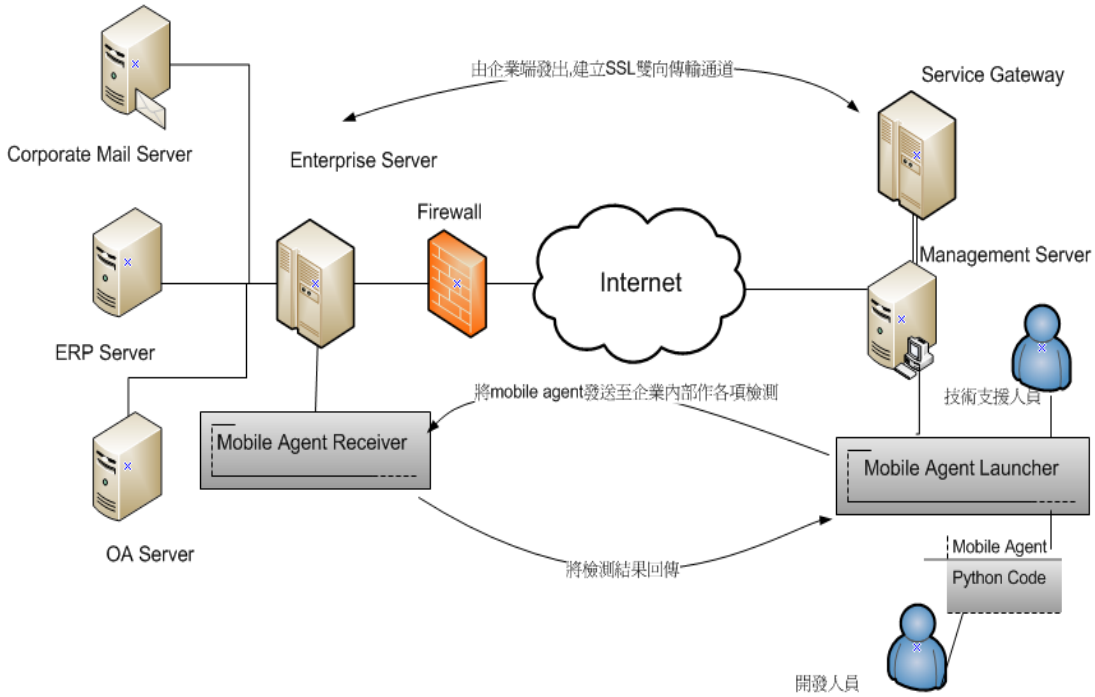

圖 8： Mobile Agent 運作架構

3.2.2. 行動代理人運作流程

安全通道的建立是透過雙向握手協定，透過防火牆的 port:80 和 443 建立以 SSL 加密的安全通訊。連線建立流程如下圖：

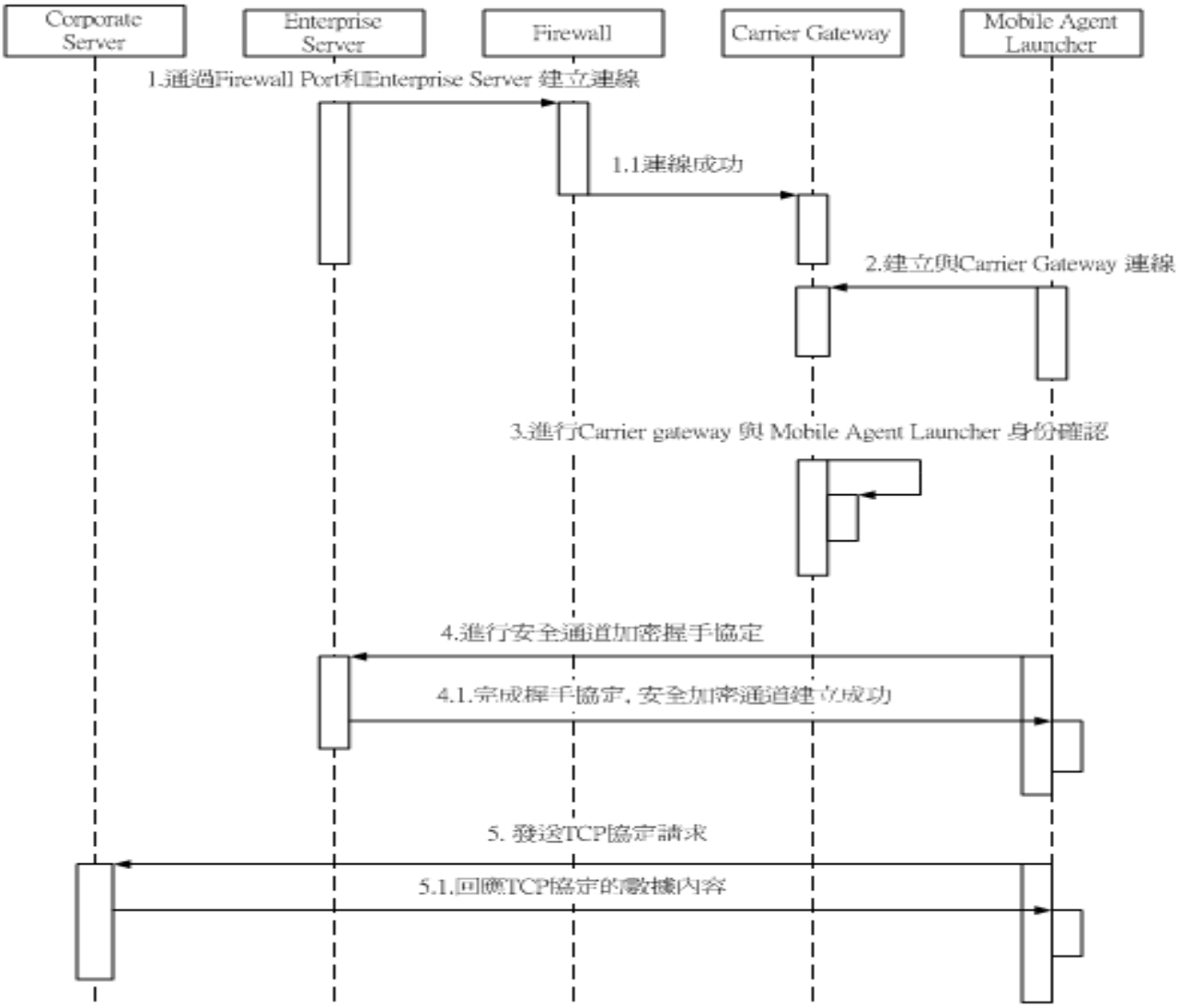

圖 9：反向安全通訊端層建立流程圖

安全通道建立完成後，行動代理人發射模組，便會在此通道上發射行動代理人至企業內部。行動代理人回傳訊息之後，此通道會持續存在，除非企業端主動斷線。

3.2.3 錯誤與問題處理流程

企業內發生問題時，資訊系統管理人員與技術支援人員接洽，技術支援人員針對問題，利用現有的行動代理人功能來處理，若無法處理，與資訊管理人員溝通後，開出功能需求，由開發人員撰寫具新功能的行動代理人來解決問題。其運

作流程入如下圖。

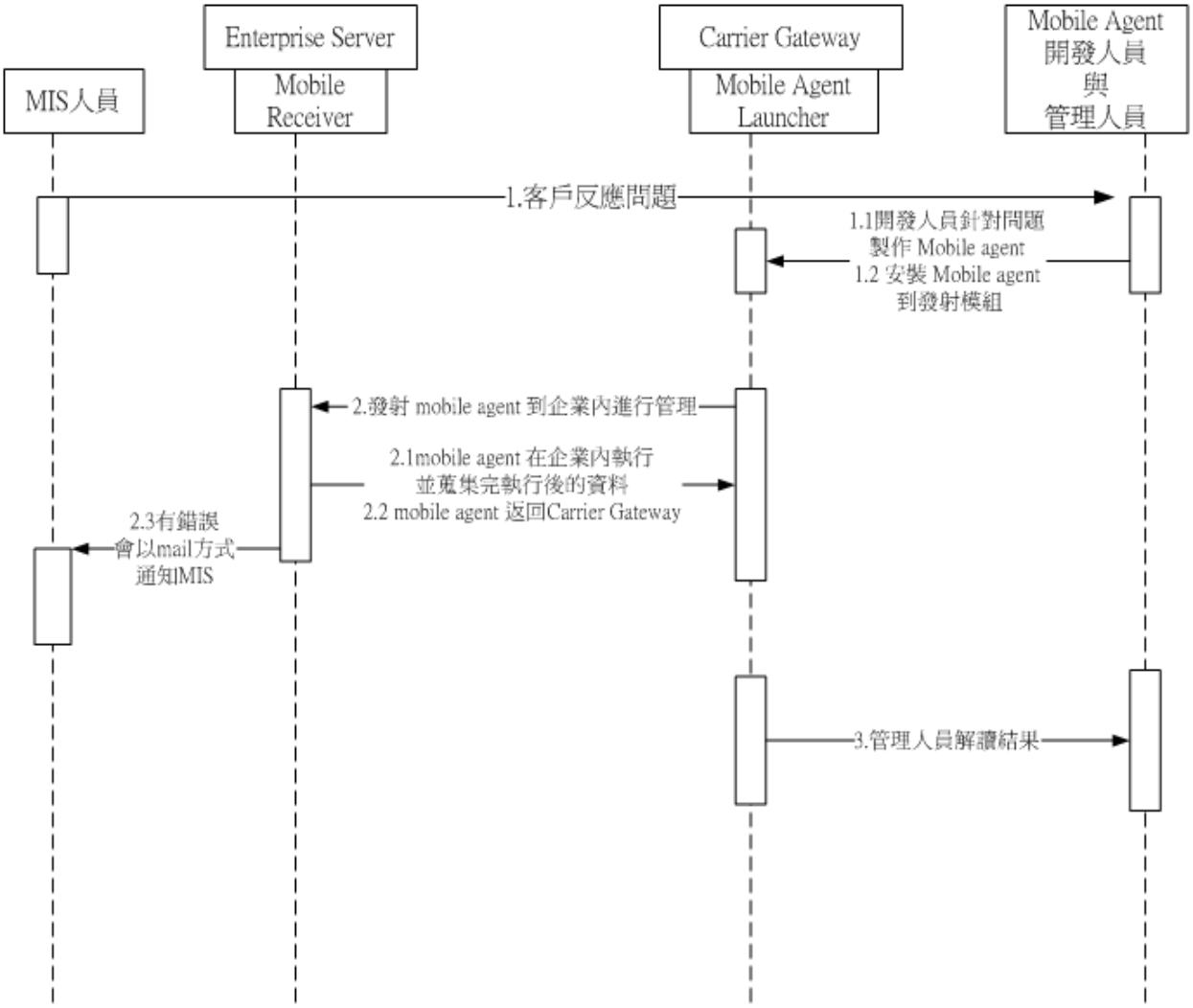

圖 10：服務流程圖

錯誤會以 Mail 方式通知 MIS 和管理人員，讓兩邊的人員能有溝通的依據。資料收集和運算會在企業伺服器內完成，回傳的僅為錯誤訊息和處理結果，不會有企業內部機密資料外洩的疑慮，確保機密性。

3.2.4 行動代理人(Mobile Agent, MA）功能

--以郵件伺服器管理為例

行動代理人所能提供的功能可區分為六大類：

項次	功能分類	功能說明	MA 數量
1	網路管理	檢測網路狀況，安全通道是否暢通。	2
2	資源管理	檢測硬碟、作業系統資源使否足夠使用。	3
3	異常處理	監控異常狀況。	4
4	服務功能	提供各項郵件寄送相關服務。	6
5	資料庫連結管理	檢測與資料庫存取是否異常。	3
6	批次(Patch)管理	檢查與操作批次檔。	2

表 3：行動代理人(MA) 功能列表

以下依照各大類，詳述各行動代理人的細部功能：

一、網路管理：檢測網路狀況，安全通道是否暢通。

1. 每 10 min 偵測企業 enterprise server 是否有網路斷線的情況, 若斷線則發出警告

2. 檢查安全通道是否暢通，允許 mobile agent 在 enterprise server 進行簡單的加法運算任務，再回傳運算結果到中華電信，以便確認 mobile agent 執行環境是正

確可以運行。網路斷線的情況有可能是：企業當中有管理者修改了防火牆設定，阻隔 80/443 port 由內到外的連線，但忘了通知管理 push mail server 的 MIS

二、資源管理：檢測硬碟、作業系統等資源是否足夠使用。

1. 監控是否硬碟爆滿，沒有多餘的空間可以使用了

2. 監控 RAM 的記憶體使用情況，若 garbage collection 失效導致記憶體耗用過多，則自動重新啟動相關 process 以便釋放記憶體

3. 檢查作業系統的 file descriptor 資源是否耗盡，若異常則先嘗試自動恢復，若自動恢復失敗則警告

三、異常處理：監控異常狀況。

1. 監控 push mail windows service 是否異常停止，若異常則先嘗試自動恢復，若自動恢復失敗則警告

2. 監控行事曆同步 windows service 是否異常停止，若異常則先嘗試自動恢復，若自動恢復失敗則警告

3. 監控通訊錄同步 windows service 是否異常停止，若異常則先嘗試自動恢復，若自動恢復失敗則警告

4.取得 enterprise server 上的錯誤日誌內容，以便判讀問題

四、服務功能類：提供各項 push mail 相關服務。

1. 檢查 enterprise server 的 mail 在指定時間內的傳送流量報告，發給企業管理者

2. 檢測企業單封郵件是否發生編碼問題(例如日文編碼)，造成手機無法接收該封郵件，將發生問題的郵件 mime 格式回報給企業 mis 管理者,以便分析原因

3. 檢測企業內的資訊系統，機器所產生的自動發送郵件（管理用途的郵件），因為格式不符合 Lotus 指定欄位格式，而造成手機無法接收問題，將問題回報 MIS 管理者

4. 從 lotus server 取出單一郵件，檢驗該郵件的所有欄位格式的值是否正確，並

且將結果發給 MIS 管理者檢測

5. 檢測是否發生使用者的 mail 帳號密碼異常，導致手機無法接收 mail，若異常則發出警告通知管理者

6. 檢查是否過去 4 小時之內，無任何郵件傳遞到手機，若異常則發出警告通知管理者

五、資料庫連結管理：檢測與資料庫存取是否異常。

1. 檢查 enterprise server database 是否發生 database schema 格式異常，若異常則先嘗試自動恢復，若自動恢復失敗則警告

2. 檢查系統對資料庫的連線操作是否過多 (通常只會發生在大型企業，連線數很多時)，若異常則先嘗試自動恢復，若自動恢復失敗則警告

3. 檢查 enterprise server 資料庫的欄位是否塞入空白資料，若發生資料內容為空白，則有可能發生異常，需要對管理者發出警告

六、patch 管理：檢查與操作 patch 檔。

1. 檢查 patch 過後的檔案大小是否正確，是否成功的覆蓋檔案，並完成 patch 任務

2. 將修正的 patch 檔案傳遞到企業 enterprise server，並且進行自動 patch 任務，遠端升級

3.2.5. 軟硬體部屬架構

以下介紹為軟硬體部屬的實際架構，並詳述架構中每個模組的角色和功能

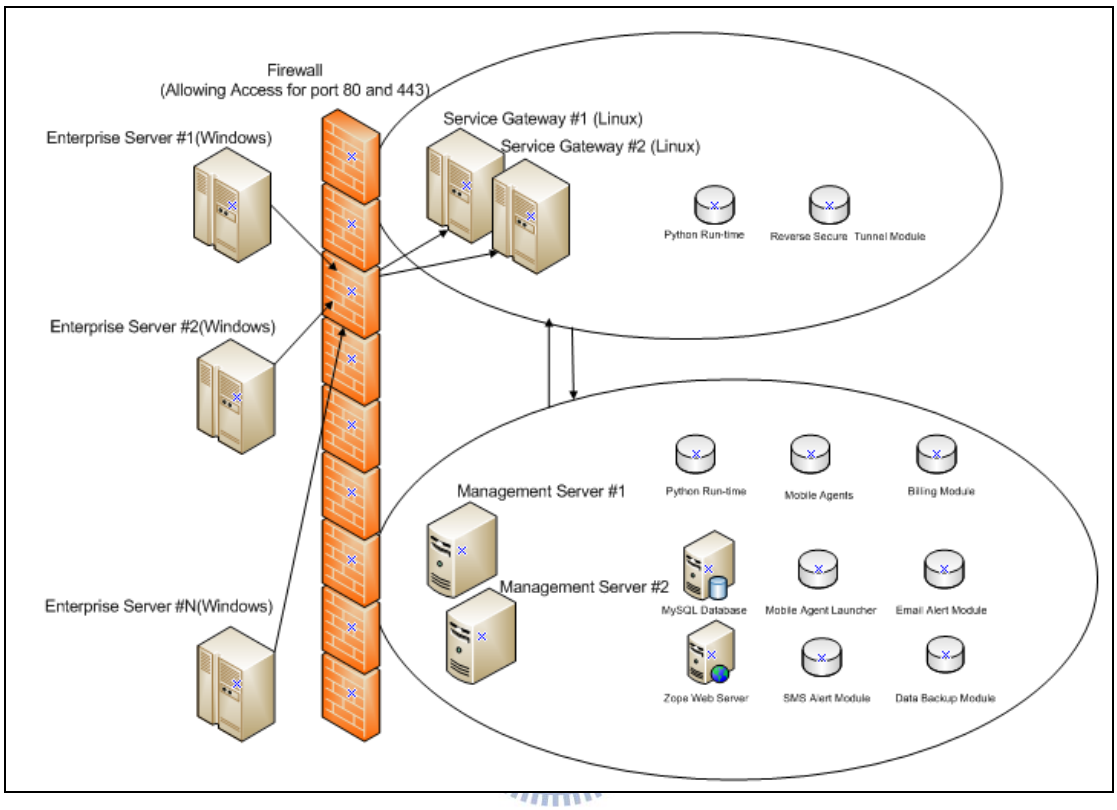

圖 11：軟硬體實際部屬圖

Service gateway 與 Management server 在實際部署時，都有兩台彼此支援，可以達到 Load Balance 與 Fault Tolerance 的效果，以下分別介紹模組的用途。

Python run-time：

由於所有的程式模組都是採用 Python 語言開發，所以必須安裝 Python run-time，目前採用的是 Python 2.3 版本

Reverse SSL module：

當企業的 Enterprise server 連接到 Service gateway 的時候，由此模組負責建立反向安全通道，並以 Keep alive 協議維持連線的通暢

Mobile agent launcher：負責發射 mobile agent 的模組

Mobile agents：這是提供各種監控用途以及管理用途的 mobile agent

MySQL database：

儲存企業註冊資料，用戶註冊資料，以及計費相關資訊，目前採用的是 MySQL Ver 14.7 Distrib 4.1.11 版本

SMS alert module：

異常狀況發生時，本模組負責採用手機簡訊的方式通知管理者，簡訊模組實際運作時，會連接到行動電信業者的 SMSC 中心傳遞訊息。

Email alert module：異常狀況發生時，本模組負責採用 Email 的方式通知管理者

Billing module：負責記錄每個企業的計費情況

Zope web server：

提供服務供應商的管理者可以使用 Web 介面進行企業基本資料維護與管理的 GUI

Data backup module：

全自動進行資料備份，當系統意外毀壞時，可以將備份資料復原

Firewall

打開 80, 443 兩個 ports ，允許企業連接到 Service gateway 建立反向安全通道，並且封鎖其他 ports 以保護主機的安全性。

第四章 功能與分析

4.1.功能比較

採用舊的處理方式雖也能達成行動代理人的功能,但因其管理方式分散且非自動化，同時仰賴人力，在效率上較行動代理人差很多

在未使用行動代理人前,當位於企業虛擬私人網路內部的郵件伺服器發生問題時，資訊系統管理人員會透過電話或電子郵件方式來與技術人員聯絡，技術人員的處理方法大致上分為兩種，一是遠端連線方式進入內網處理，一是人員直接進到企業內部，在內網中做處理，而企業為了保護內部網路，對外部進入內網的連線，或是外部人員進入企業內，都會做許多層的安全管制與驗證，雖然在安全性上有一定強度，但卻犧牲掉管理的效率，花費許多安全驗證上的成本。此外，從技術人員的角度來看，一次能處理的錯誤和服務的企業數有限，必須花費時間從企業內部的錯誤記錄中找出問題所在並處理，錯誤處理的方法通常無法有效模組化，也就無法重複利用，很大部分都倚賴人員的經驗，在人員離職或工作交接時，需花費額外的訓練成本，在處理效率和重複使用度上都很差。

使用行動代理人以多重執行緒(Multi-Thread) 的方式去發射行動代理人進入企業內部，一次管理很大量的企業伺服器(Enterprise Server)，可以有效提昇效率[18]。同時集中式的行動代理人，功能模組化的管理方式[19]，方便人員在交接時，能清楚逐項列出各個管理功能，能避免重複開發，管理功能重複使用度高，發生過的管理問題，已有對應的行動代理人處理，新接手人員僅需作行動代理人的瞭解與維護，使其能正常運作，正常解決問題，而不需在老問題發生時，因缺乏經驗的傳承，必須從頭開始思考解決方法。

下表就行動代理人所能做到的的六大類功能和處理效率、重複使用性[20]，兩項性質，比較使用前和使用後的差別。

	未使用行動代理人	使用行動代理人
網路管理	技術人員需以遠端連線和現場檢測兩種方式來執行工作，管理分散且異質性的企業網路服務	定時自動偵測連線，並測試執行環境
資源管理		可自動釋放資源避免資源耗盡
異常處理		Alert Module
Push Mail 服務功能		各項服務功能可自動化
資料庫連線管理		監測異常存取和欄位格式的確保
Patch 管理		可進行遠端升級

表 4：功能比較表

4.2.效益評估方法

當發生錯誤時，企業資訊管理人員會與技術人員聯絡，要求將錯誤修正，此時技術人員會寄發一分問卷，說明將採用行動代理人解決方案，徵求企業同意安裝此服務所需的相關元件，並請資訊管理人員和系統服務使用者就使用行動代理人的架構後的狀況進行滿意度評分，以對行動代理人的運作情況做追蹤。

4.3.效益分析

在未採取行動代理人方式下，以傳統的方式解決企業內部問題時，平均處理一個狀況的時程，需一至三工作天，當中包含人員的移動和協調溝通的時間；採用行動代理人後的平均處理時間可縮短至半天至一天，並減少了人員移動的耗費。企業內部資訊人員的投訴狀況也獲得降低。。

	未使用行動代理人	使用行動代理人
處理效率 (每一個狀況排除)	一至三個工作天	半天至一個工作天
重複使用性	因人員和任務而變動處理方式	行動代理人可自動進行多次的任務執行
使用者投訴比率	12 次/月	4 次/月

表 5：效益比較表

企業 MIS 專業人員使用後評估問卷：

使用 Push mail 服務的企業共 11 家，共寄發 22 份問卷，每一家提供兩份，一份為企業內部 MIS 人員，一份為系統服務的使用者，回收 18 份，同意使用共 9 家，比例為 81.8%；不同意使用共 2 家，比例為 18.2%。不使用的原因，最多為其系統的規劃上不能配合。並依處理效率、便利性、錯誤處理妥善度、持續使用意願、推薦意願五個項目作一至五分的滿意度評估，一分為最不滿意、二分為不滿意、三分為無感、四分為滿意、五分為非常滿意。平均得分如下：

處理效率	3.8
便利性	2.8
錯誤處理妥善度	4.0
持續使用意願	4.5
推薦意願	3.8

表 6：企業使用滿意度

由以上滿意度評分，可看出企業的使用後滿意度高，而在便利性得分較低，分析其原因是在於，要求在 Enterprise Server 上額外安裝 Mobile Receiver 這項動作，被 MIS 人員視為不便利的主要因素之一。

第五章 結論與未來研究

5.1 結論

利用行動代理人的架構來做企業系統的管理維護，達成自動化管理，解決前述的系統維護問題，降低人員成本，減少錯誤，提升維護效率。這個方式於實務上，應用於郵件服務商的對企業郵件伺服器的服務，這架構不僅限於郵件伺服器，或是其他種類的伺服器管理，更可廣泛用於企業外購系統的遠端管理上，提供更方便操作和更完善的服務，以發揮企業外購系統的最大效益。

5.2 未來研究

目前所實作出的行動代理人是在 Linux 上的 python code，以命令列(Command Line)的方式來供管理者操作，需要較為專業的人員來處理。未來可增加圖形化界面(GUI)來提供管理者有更方便使用的中央控管畫面。另外行動代理人有可能會被執行端的電腦所破壞，或更動當中的訊息，因此在資料加密和認證機制上可再作加強，以確保安全性和可靠性。以人工智慧為方向，來改進行動代理人的學習能力，也是未來可研究的方向之一。

參考文獻

1. Eid, M., et al., *Trends in Mobile Agent Applications.* Journal of Research and Practice in Information Technology, 2005. 37(4): p. 323-351.
2. Osei-Bryson, K.-M. and O.K. Ngwenyama, *Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts.* European Journal of Operational Research, 2006. 174(1): p. 245-264.
3. Park, S., *IT Outsourcing: Strategic Implications.* The Review of Business Information Systems–First Quarter, 2006. 10(1).
4. Sabherwal, R. and V. Choudhury, *Governance of remotely outsourced software development: A comparison of client and vendor perspectives.* Information systems outsourcing: Enduring themes, new perspectives, and global challenges, 2006: p. 187-222.
5. Persona, A., et al., *Remote control and maintenance outsourcing networks and its applications in supply chain management.* Journal of Operations Management, 2007. 25(6): p. 1275-1291.
6. Vieira-Marques, P.M., et al., *Secure Integration of Distributed Medical Data Using Mobile Agents.* Intelligent Systems, IEEE, 2006. 21(6): p. 47-54.
7. Huy Hoang, T., K. Shonali, and S. Bala, *Mobile agents for network management: when and when not!*, Proceedings of the 2005 ACM symposium on Applied computing. March,2005,Santa Fe, New Mexico.
8. Satoh, I., *Building and Selecting Mobile Agents for Network Management* Journal of Network and Systems Management, 2006. 14,Number1 p. 147-169.
9. Rayan Stephan, P.R.N.P., *Network management platform based on mobile agents.* International Journal of Network Management, 2004. 14(1): p. 59-73.
10. Berioli, M. and F. Trotta. *IP mobility support for IPsec-based virtual private networks: an architectural solution*. 2003.
11. Hole, K.J., E. Dyrnes, and P. Thorsheim, *Securing Wi-Fi Networks.* Computer, 2005. 38(7): p. 28-34.
12. Adeyinka, O. *Analysis of problems associated with IPSec VPN Technology*. 2008.

13. Chen, J., F. Miao, and Q. Wang. *SSL/TLS-based Secure Tunnel Gateway System Design and Implementation*. 2007.
14. Bicakci, K., B. Crispo, and A.S. Tanenbaum, *Reverse SSL: Improved Server Performance and DoS Resistance for SSL Handshakes.*
15. Rowan, T., *VPN technology: IPSEC vs SSL*. Network Security, 2007. 2007(12): p. 13-17.
16. Gavalas, D., G.E. Tsekouras, and C. Anagnostopoulos, *A mobile agent platform for distributed network and systems management.* Journal of Systems and Software, 2009. 82(2): p. 355-371.
17. Ching-hang Fong, Gerard Parr, and Philip Morrow, *A Comparison of Mobile Agent and SNMP Message Passing for Network Security Management Using Event Cases* in *Autonomic Principles of IP Operations and Management*. 2006, Springer Berlin / Heidelberg. p. 156-167.
18. Timon, C.D., Y.L. Eldon, and C. An-Pin, *Mobile agents in distributed network management.* Commun. ACM, 2003. 46(7): p. 127-132.
19. Autran, G. and L. Xining. *Large Scale Deployment a Mobile Agent Approach to Network Management*. in *Networking, 2008. ICN 2008. Seventh International Conference on*. 2008.
20. Satoh, I., *Building reusable mobile agents for network management.* IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2003. 33(3): p. 350-357.