醫療機構與企業遠端存取服務平台與管理機制之設計

陳政宏* 張克章+

*長庚大學企業管理研究所

+長庚大學資訊管理研究所

* m9340554@stmail.cgu.eru.tw

+ changher@mail.cgu.edu.tw

+聯絡人：長庚大學資訊管理研究所張克章教授

摘要

目前在醫療機構與企業遠端存取服務(Remote Access)的應用，普遍僅收發電子郵件的一般功能為主，缺乏深度層次連結醫療機構與企業營運攸關系統，也鮮少可靠而完整的使用者身份安全認證機制。本研究設計多層次、安全、完整的存取基礎架構平台，包括多重安全機制與使用者身份驗證，如 RSA SecurID Authentication 等認證措施，確保資訊存取安全。本設計建構一個以網頁為基礎的標準存取環境，讓近端、遠端、以及行動使用者，不受時空限制，透過網路便利而安全地存取醫療機構與企業營運關鍵應用程式和資訊。本論文研究成果，首創價值創新模式，並樹立醫療機構與企業遠端存取服務系統架構典範和業界學習標竿。

關鍵字：遠端存取、遠端辦公室、應用軟體部署、安全驗證機制

Abstract

Most of the hospital and corporate application in remote access are limited in email services and lack high-level, mission critical corporate processes, and there does not seem to have reliable and comprehensive tools for user authentication.

This study shows the design of a multi-level, secure, and comprehensive platform for remote access; including multiple security checking and user authentication systems. This design incorporates RSA, SecurID authentication techniques to ensure the security in information access. This web-based system tales the advantage of internet connection and provides a uniform operation environment to conduct mission-critical functions over wide-geographical area. The resulting increased efficiency and time savings come from the integration of corporate operational processes, workflow management, and remote manufacturing processes control – all through this highly efficient connectivity among different sites.

This paper provides an innovative value added model, and it provides an example for remote access application in the industry that is international and global in nature. It provides a total solution to today's multi-national and global corporations.

Keywords: Remote Access, Remote Office, Application Software Deployment, Security Verification Mechanism.

1、緒論

1.1 研究動機

設計一個安全的存取基礎架構平台與機制，讓分散在各地的遠端使用者，能夠不受時空的限制，在任何時間、任何地點，透過網路便利而安全地存取醫療機構與企業內部應用程式與資訊。

特別在面對 SARS 危機、或禽流感疫情爆發，必須進行人員隔離措施時；或職場及公共處所遭遇重大災變等突發情況，為維持醫療機構與企業持續營運，員工必須在家上班的狀況。完整的遠端存取服務系統機制，更突顯其不可或缺的重要性與價值。

目前醫療機構與企業在遠端存取服務的運用，主要採行 Web-based 型態，然在應用層次及安全的控管等方面，尚有可待加強之處。本研究擬建構一套完整的解決方案(Total Solution)，建立系統模式與樹立架構典範，希冀提供產業後續發展參考。

1.2 研究背景

1.2.1 醫療機構與企業外部環境

(1). 應用範疇

目前醫療機構與企業在遠端存取服務的應用，普遍以收發電子郵件的功能為主，缺乏再進展到文件管理、知識管理、規範管理、人員教育訓練、考勤簽核，以及營運或生產相關等工作流程簽核系統。也未深入發展到應用程式部署，以及營運系統或生產系統遠端控制的應用。

(2). 資訊安全

在資訊安全管理方面，目前醫療機構與企業的遠端存取服務系統，缺乏可靠而完整的使用者身份安全認證機制，經常無法滿足在快速變動與嚴苛的環境下的使用者需求。

(3). 存取權限

在遠端存取系統的存取權限管理方面，普遍缺乏有效的管控和良好的機制，時常無法克服便利性與安全性的選擇問題。

1.2.2 醫療機構與企業內部環境

面對國際化程度加深，需要在全球公務出差或工作旅

行的員工，經常缺乏一個標準、穩定而有效率的遠端存取環境，各地區 IT 人員也需進行繁複的 OA 作業環境與網路資源存取設定與維護。常因所處國際地域和辦公場所不同，而有不同的操作方式，影響工作效率與耗費時間甚巨。

需要解決的問題：

(1). 面對各種網路與設備的差異，如何讓支援與維護遠端辦公室的應用程式更有效率。

(2). 減少需要分派 IT 人員到各個遠端辦公室服務，應用程式集中化管理。

(3). 降低佈署與更新應用程式的人力成本，和簡化作業流程。

1.3 研究目的

(1). 遠端辦公室連線

安全地將分支機構、辦公室、委外合作夥伴、以及連絡中心連結在一起。建置一個安全的存取基礎架構平台，使醫療機構與企業便利且安全地提供應用程式與資訊給遠端使用者，並且在一個集中化的地點維護這些應用程式與資訊。建置一個安全的存取基礎架構與溝通管道，將遠端使用者應用程式與資訊的佈署與維護工作加以簡化、合理化，對於講求速度與效益的醫療機構與企業可帶來顯著的價值。

(2). 應用軟體部署

加速佈署工作、降低成本、並提升效率。設計一套安全的應用程式佈署存取基礎架構平台，簡化並加速以主機為主、網頁式、或是桌上型應用程式與資訊的佈署工作。可以快速、有效率地為佈署與更新營運關鍵應用程式和資訊。提供 IT 人員集中化應用程式的供應與管理功能。該解決方案可彈性擴充、同時具備穩定性、管理性、以及安全性。滿足醫療機構與企業快速地在整個醫療機構與企業佈署營運關鍵應用程式與資訊的需求(Citrix Technology Research Center, 2005) [2]，降低科技基礎架構的整體持有成本 (Total Cost of Ownership, TCO)。

2、文獻探討

2.1 RSA Authentication

RSA 加密演算法，應用於設計一個遠端存取服務系統上，所扮演的第一道安全把關的重要角色。賴溪松等(民 88) [5] 指出，RSA 加密演算法是一種非對稱加密演算法，在公鑰加密標準和電子商業中 RSA 被廣泛的使用。RSA SecurID 認證裝置要求使用者必須以兩種獨特的因素(Factors)進行認證(即用戶知道的因素和用戶具有的因素－Something they know & Something they have)，才能被授權進入網路(顧武雄，民 92)[6]。RSA SecurID Token 與 Architecture，分別如圖 1、圖 2 所示說明：

圖 1 RSA SecurID Token
(資料來源：Internet Security Systems, Inc., 2005)

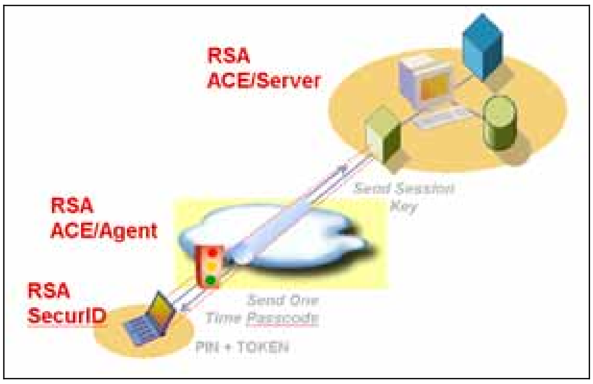


圖 2：RSA SecurID Token Architecture
(資料來源：RSA Security Inc., 2006)

2.2 Secure Sockets Layer

本研究設 Secure Sockets Layer 應用於網頁伺服器和瀏覽器間擔任安全把關的重要角色(Stephen Thomas, 2000) [14]。 以加解密方式溝通的安全技術標準，確保伺服器與瀏覽器間通過資料的私密性與完整性(Global Trust Inc., 2005) [9]。網站若未申請 SSL 憑證或憑證有問題，會顯示「此網站安全憑證有問題，建議不要繼續瀏覽此網站」的安全提示訊息(網際威信客戶服務中心，民 94)[4]，如圖 2-2 所示：

圖 3：一般系統 Web-based remote access portal
(資料來源：本研究)

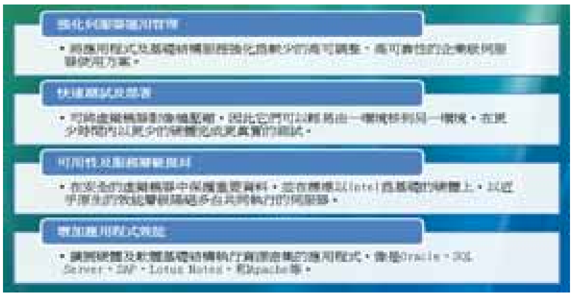
2.3 VMware Server

本研究設計 VMware Server 擔任伺服器資源整合、降低成本的任務(CGS Technology Center, 2006) [1]。其特點為：

1. 可彈性調整配置、可靠性高。
2. 實體系統轉換為邏輯電腦運算資源集區，簡化伺服器維護。
3. 作業系統及應用程式可在單一硬體標準化平台中多個虛擬伺服器加以隔絕(資訊與電腦期刊編輯部，民 94)[3]。

VMware Server 效益與說明，如表 1 所示：

表1：VMware 效益說明



(資料來源：VMware Inc. , 2006)

3、醫療機構與企業內部遠端存取系統設計與建置

本章節說明遠端存取服務系統應用於醫療機構與企業內部廣域網路之設計與建置。可快速、有效率地為近端、遠端、以及行動使用者佈署與更新營運關鍵應用程式和資訊。提供 IT 人員集中化應用程式的供應與管理功能。可彈性擴充、同時具備穩定性、管理性、以及安全性。

3.1 醫療機構與企業內部遠端存取程序

Intranet Remote Access Flow 如圖 4 所示說明：

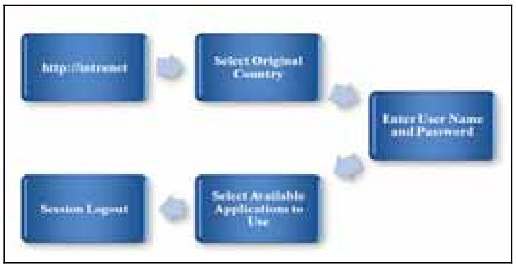


圖 4：Enterprise Intranet Remote Access Flow
(資料來源：本研究)

3.2 ICA(獨立運算架構) 組態設計

獨立運算架構(Independent Computing Architecture, ICA) 重要內容(金維訊科技研究中心，民 91)[1]：

(1). 高效網路傳輸：Citrix 的 SpeedScreen Technology (僅傳輸顯示界面變化的部分)，平均只佔用 10K 的網路頻寬。

(2). 終端設備靈活性：可在各種電腦裝置上正常運作。

(3). 普遍作業平台：可在許多作業系統平台正常運作應用軟體。

(4). 通用連接方式：可透過多種網路方式連接。ICA stream 及 Connection 如圖 5、圖 6 所示說明：

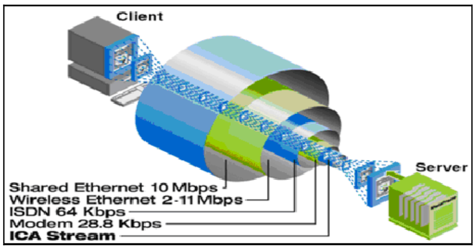


圖 5：ICA Stream 10 – 20 Kbps
(資料來源：Citrix Inc. , 2005)

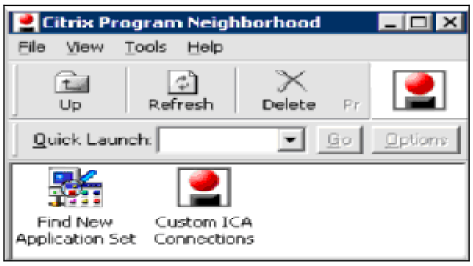


圖 6：ICA Connection (資料來源：本研究)

4、醫療機構與企業外部遠端存取系統設計與建置

本章節說明遠端存取服務系統應用於醫療機構與企業外部廣域網路之設計與建置。可快速、有效率提供 IT 人員集中化應用程式的供應與管理功能。具備穩定性、管理性、以及安全性。

4. 醫療機構與企業外部遠端存取程序

Extranet Remote Access Flow，如圖 7 所示說明：

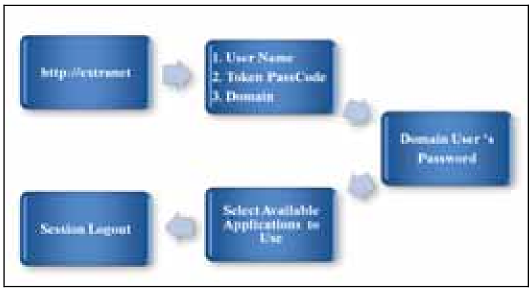


圖 7：Enterprise Extranet Remote Access Flow
(資料來源：本研究)

4.2 Secure Gateway 設計與規劃

安全閘道(Citrix Secure Gateway, CSG)的功能，是在 Citrix MetaFrame 伺服器，與 SSL 的 Citrix 獨立運算架構(ICA)資料流程間所啟動的安全 Internet 閘道作用。SSL 技術用於加密，保證在網路中可以安全傳送資料。通過 Internet 在用戶端工作站和 CSG 伺服器間傳遞的資料都經過加密，以保證資訊流的安全性和完整性(Steve Kaplan, 2000) [13]。

本研究建置 CSG 伺服器於 VMware Server 平台，提供一個單點入口來安全地存取 Citrix 伺服器集群。為考量資訊安全需求，在 Secure Gateway、Proxy，及 MataFrame Server 建置，採行 Double-hop DMZ 架構 [14]：亦即區分 First Stage DMZ1 及 Second Stage DMZ2 兩層式架構，以提升系統的安全性。架構圖如圖 8 說明：

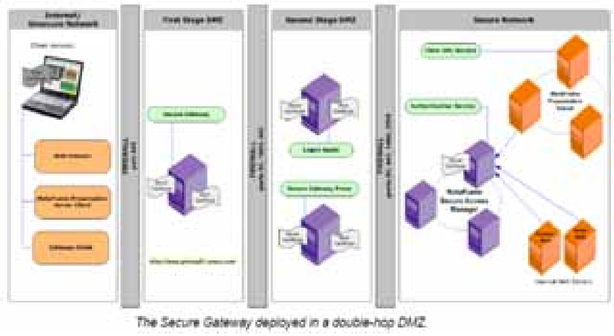


圖 8：Double-hop DMZ 架構
(資料來源：Citrix System Inc. , 2005)

4.3 Active Directory and GPO

群組原則設定儲存在網域控制站「群組原則物件 (Group Policy Object, GPO)」中(Microsoft Inc., 2006) [12]。GPO 與包含 Active Directory 站台、網域和組織單位 (OU) 容器連結。(吳翠鳳，劉聖路，民 94) [2] 指出，群組原則的 優先順序如圖 9 所示：

圖 9：群組原則優先順序
(資料來源： Windows Server 2003 群組原則)

4.4 Network Load Balancing

網路負載平衡(Network Load Balancing, NLB)，將 IP 輸送量分散到多個叢集主機(Microsoft Inc., 2004) [11]。藉由偵測主機失敗，及自動將輸送量重新分配到仍然存在的主機。完整分配的結構可提供錯誤後移轉的保護，可提供延展性及可用性。說明如圖 10 所示：

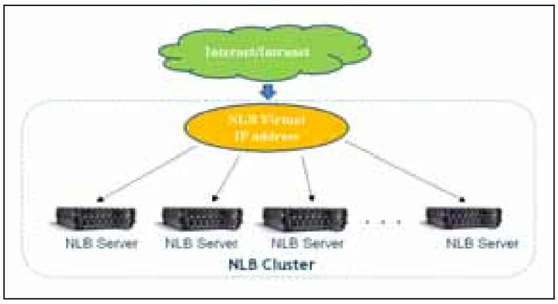


圖 10：NLB (資料來源：本研究)

4.5 Multi-Authentications

本研究設計多層次、安全且完整存取基礎架構平台，包括多重安全機制與使用者身份驗證措施，確保資訊存取安全。

- SSL encryption
- Firewall Access Control
- Citrix Secure Gateway
- RSA SecurID Authentication
- Active Directory and Group Management
- Group Policy Object

相對於不安全、且過於簡單的一般系統 Web-based Mail System 認證程序，比較如圖 11、圖 12 所示：

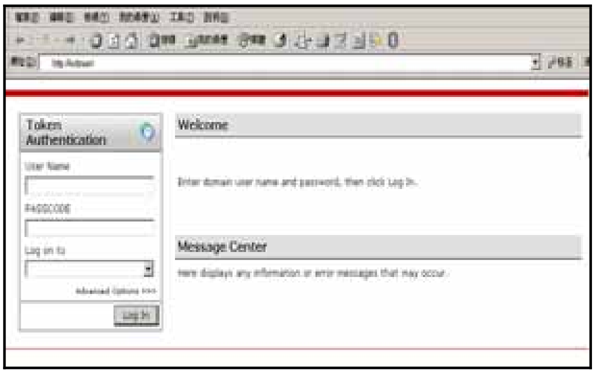


圖 11：RSA Token Authentication

(資料來源：本研究)

圖 12：一般系統 Web-based Mail 簡單認證程序比較

(資料來源：本研究)

4.6 Enterprise Remote Access Architecture

本研究設計 Enterprise Remote Access Architecture，包括內部及外部遠端存取系統，如圖 13 所示說明：

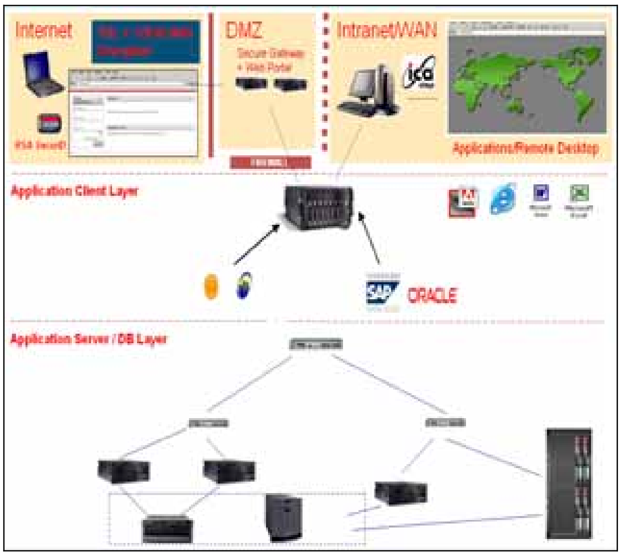


圖 13：Enterprise Remote Access Architecture

(資料來源：本研究)

5、效益評估

本章節為論述本論文研究成果，在設計一個遠端存取服務系統的應用推廣、使用者情境模擬，與效益評估說明。

5.1 應用推廣

(1). 讓應用程式存取透過一個集中的地點設定、管理，以降低醫療機構與企業資源配置的成本。

(2). 加速提供 ERP、工作流程軟體、電子郵件以及其他辦公室生產力應用程式，進而改善醫療機構與企業拓展的速度與效率 (Reeser et al., 2003) [15]。

(3). 設計安全的平台能讓分散在各地的員工安全地從任何地點，透過網路遠端存取他們所需的重要應用程式。

(4). 以集中化的應用程式管理，減少分派 IT 人員到各個遠端辦公室服務的需要。

(5). 以更少的頻寬，利用網際網路安全地佈署應用程式，能降低通訊與網路的成本。

(6). 一套使用者熟悉、一致性的桌面環境，讓員工從任何地點都能存取得到，進而鼓勵員工從任何地點工作都能具備高度生產力 。

(7). 特別在面對 SARS 危機、或禽流感疫情爆發，必須進行人員隔離措施時；或職場及公共處所遭遇重大災變等突發情況，為維持醫療機構與企業持續營運，員工必須在家上班的狀況，更突顯其不可或缺的重要性與價值。

5.2 使用者情境模擬

5.2.1 醫療機構與企業內部網路遠端存取情境模擬

(1). 員工 A 君在國外分公司出差，或在國內各分公司辦公地點開會或移動，需即時處理重要公務時。

(2). 可借用任一部辦公室電腦連上 intranet 網路，在 Web 瀏覽器輸入網址：http://intrant，點選全球地圖上原屬辦公室圖示。

(3). 完成使用者身份安全認證後，透過分公司與總公

司間的網路專線，快速跨越國際界限進入原屬所在國家辦公室「遠端存取伺服器主機」，在熟悉的使用者語系與桌面環境使用應用程式。

(4). 在日常熟悉的使用者界面下，使用電子郵件、工作流程軟體、ERP、其他辦公室生產力應用程式，以及簡報、遠程會議，甚至 e-Learning、近端文件列印等服務。

(5). 輕易的跨越國際語言藩籬及所在環境的限制，增進醫療機構與企業發展的速度與卓越的效率。

5.2.2 醫療機構與企業外部網路遠端存取情境模擬

(1). 員工 A 君在國內外旅行，或在家辦公，或出差，需即時處理重要公務。

(2). 使用任一部電腦連上 internet 網路，在 Web 瀏覽器輸入網址：http://extrant。

(3). 完成使用者身份安全認證後，透過網路，快速跨越國際界限進入醫療機構與企業內部「遠端存取伺服器主機」。

(4). 在熟悉的使用者環境下，使用電子郵件、工作流程軟體，甚至醫療機構與企業營運、生產資料庫系統、或遠端系統控制等生產力應用程式。

(5). 讓分散在各地的員工安全地從任何地點，透過網路遠端存取他們所需的重要醫療機構與企業營運攸關的應用程式與資訊，具備即時與高度生產力。

5.3 效益評估

在瞬息萬變的商業環境中，如何自由存取最新的資訊將是一個重要的關鍵。電腦環境比以前來的複雜許多，如何使存在多樣地使用，將是今日醫療機構與企業的重要課題。本研究設計能透過使用同一平台，對員工而言不論在任何的環境，都能夠任意地透過網路環境安全地傳送資料，並且能夠有效地控制費用並把金額降到最低，不論何時何地都能夠持續地為提供最新且即時的資訊及服務，提升醫療機構與企業的競爭能力。本研究設計醫療機構與企業內部及外部遠端存取系統，與一般醫療機構與企業應用比較，分別整理如表 5-1 及表 5-2，分析差異與效益。

表 5-1：醫療機構與企業內部遠端存取系統效益分析（資料來源：本研究）

指標分析	本研究設計	一般設計
應用範疇	1. 全球一致化、標準、穩定而有效率的遠端存取環境。 2. 滿足醫療機構與企業快速地在國際佈署營運關鍵應用程式與資訊的需求，降低科技基礎架構的整體持有成本。	沒有一致、標準、穩定而有效率的全球一致遠端存取環境。
流程改善	1. 透過應用程式與作業集中化，發揮 IT 人員的生產力，改善作業流程。 2. 降低佈署與更新應用程式的人力成本，和簡化作業流程。 3. 只需 5~10 秒鐘即可到達原屬國家之遠端服務主機。	1.IT 人員需進行繁複的 OA 作業環境，與網路資源存取設定與管理維護。 2.建立連線至少需 10 分鐘以上，並需長期承受緩慢的網路速度下工作。
降低成本	1. 需要分派 IT 人員到各個遠端辦公室服務。 2. 加速應用程式的佈署與更新。運用端對端的可見度，讓整個醫療機構與企業的軟體授權利用率最佳化。	面對所處國際地域和辦公場所不同，而有不同的操作方式，影響工作效率與耗費時間與成本。
醫療機構與企業營運攸關	1. 不受時空的限制，在任何時間、任何地點，透過網路便利而安全地存取醫療機構與企業內部應用程式與資訊。 2. 延長現有技術投資的使用壽命，提升投資報酬率，降低成本達 5 倍以上。 3. 透過對整個醫療機構與企業的應用程式強化的控管與安全性，以支援符合法規規範的計劃。	無

表 5-2：醫療機構與企業外部遠端存取系統效益分析（資料來源：本研究）

指標分析	本研究設計	一般設計
應用範疇	1. 收發電子郵件。 2. 文件管理、 知識管理、規範管理、人員教育訓練、考勤簽核，以及營運或生產相關等工作流程簽核系統。連結醫療機構與企業內部超過 1000 個資料庫系統。	僅有收發電子郵件功能。缺乏各種工作流程與資料庫系統連結。
醫療機構與企業營運攸	1. 應用程式部署，以及營運系統或生產系統遠端控制應用。 2. 應付職場及公共處所遭遇重大災變等	無

關	突發情況，為維持醫療機構與企業持續營運，員工必須區隔或在家上班的狀況。完整的遠端存取服務系統機制。	
資訊安全	多層多重使用者身份安全驗證機制。包括至少下列安全機制：SSL、Firewall Access Control、Secure Gateway Double-hop、RSA SecurID、AD Authentications	缺乏可靠而完整的使用者身份安全驗證機制。如圖 2-2 所示，顯示不安全的網站憑證問題。
存取權限	完整的應用程式與資訊存取控制管理機制。	普遍缺乏有效的管控和良好的機制。例如群組原則管理等。

6、結論與建議

本論文研究成果，首創價值創新模式，並樹立醫療機構與企業遠端存取服務系統架構典範和業界學習標竿。整合資源與應用，跨越國際疆界與藩籬。運用理論與實務的結合，不僅是處理單一個案，更提供醫療機構與企業整體的解決方案(Total Solution) 。如表 6-1 所示說明：

表 6-1：醫療機構與企業遠端存取平台設計與建置成果(資料來源：本研究)

目前在醫療機構與企業遠端存取服務(Remote Access)的應用，普遍僅收發電子郵件的一般功能為主，缺乏深度層次連結醫療機構與企業營運攸關應用，也鮮少可靠而完整的使用者身份安全認證機制。本研究設計多層次、安全、完整的存取基礎架構平台，包括多重安全機制與使用者身份驗證：SSL、Firewall Access Control、安全閘道(Citrix Secure Gateway, CSG)、RSA SecureID Authentication、Active Directory 認證與群組管理、群組原則物件(Group Policy Object, GPO)等措施，確保資訊存取安全。

本論文研究建構一個標準、而穩定的 Web-based 存取環境，整合伺服器資源管理與降低成本，運用伺服器虛擬化技術，透過網路便利而安全地存取醫療機構與企業應用程式與資訊，並可連線遠端辦公室及應用軟體部署，深度結合醫療機構與企業流程與工作簽核系統，連結內部資料庫與營運或生產系統遠端控制，大幅提升工作效率與節省時間。

運用本研究設計，可達成快速、有效率地為近端、遠端、以及行動使用者佈署與更新應用程式和資訊，亦包括簡報以及會議的服務。滿足快速地佈署營運關鍵應用程式與資訊的需求，達到「天涯若比鄰」的效益，對於講求速度與成效的醫療機構與企業可帶來顯著而重要價值。

建議後續研究者，可在本論文研究設計架構後，在外部遠端存取系統持續增強系統管理性及安全性。在內部遠端存取系統佈建更綿密、更廣泛，更延伸與醫療機構與企業營運攸關流程與系統緊密結合的全球網路，擴充服務範圍與水準。期能繼續擴大「任何時間、任何地點都能便利存取所需應用程式與資訊」的願景與卓越發展。

參考文獻

[1] 金維訊科技研究中心，獨立運算架構，金維訊公司，北京，民國九十一年。
[2] 吳翠鳳，劉聖路，Windows Server 2003 群組原則技術探討與建置，Microsoft 百日維新研討會特輯(12)，頁3-8，台北，民國九十四年。
[3] 資訊與電腦期刊編輯部，VMWare Server虛擬伺服器，資訊與電腦期刊，民國九十三年。
[4] 網際威信客戶服務中心，憑證實務作業基準，網際威信公司，台北，民國九十二年。
[5] 賴溪松等著，近代密碼學及其應用，松崗電腦圖書資料公司，頁135-168，台北，民國八十八年。
[6] 顧武雄，ISA 2004整合RSA安全應用指引，旗標資訊期刊，卷132，頁125-131，民國九十四年。
[7] CGS Technology Center, “VMware Technology” , CGS International Inc., 2006.
[8] Citrix Technology Research Center, http://www.citrix.com/, Citrix System Inc., 2005.
[9] Global Trust Service Division, Secure Sockets Layer, Global Trust Inc., 2005.
[10] ISS Support Division, “RSA SecurID”, Internet Security Systems, Inc., 2005.
[11] Microsoft Technology Center, “Network Load Balancing White Paper”, Microsoft Inc., 2004.
[12] Microsoft Technology Center, “Understanding the Group Policy Feature Set White Paper”, Microsoft Inc., 2006.
[13] Steve Kaplan, “Citrix Metaframe for Windows Terminal Services: the official guide”, McGraw-Hill, New York, 2000.
[14] Stephen Thomas, “SSL and TLS Essentials”, Wiley, New York, 2000.
[15] Tim Reeser, Steve Kaplan and Alan Wood, “Citrix MetaFrame Access Suite for Windows Server 2003: The Official Guide”, McGraw-Hill, 2003.
[16] VMware Technology Center, “Virtualization Solution”, VMware Inc., 2006.
[17] RSA Technology Center, ACE and SecurID , RSA Security Inc., 2006.