以 BS7799 為基礎建構整合性醫院資訊安全架構之研究

A Study of the Integrated Architecture of Hospital Information and Communication Security based on the BS7799 Standard

陳瑞甫[a] 劉忠峰[a] 蕭如淵[b]

[a]國立中正大學資管所 [b]國立彰化師範大學資訊工程所

rafuchen@mis.ccu.edu.tw

摘要

隨著社會環境的變遷、全民健保的實施以及醫療院所間彼此的激烈競爭，醫療院所的經營面對前所未有的衝擊及挑戰。醫療院所為因應上述的挑戰，也紛紛導入資訊科技以期有效提升經營績效，並增加組織的競爭優勢。然而，由於大部份醫療相關的系統在開發時都缺乏良好的規劃設計，同時未能考量未來整合性、擴充性、管理性及整體安全性上的需求，因此，常常造成後續系統維護人員系統維護及管理上的困擾。此外，雖然病歷資料的數位化可有效的提升對於病患健康照護的品質，但另一方面也衍生出安全管理以及病患隱私權保護的問題。縱觀目前國內關於醫院資訊安全方面的相關研究還是相當的不足，且缺乏一個整體的安全架構設計，導致醫院組織對於各種威脅的承受度及應變能力非常的薄弱。因此，本研究的主要目的，是以英國國家標準協會(British Standard Institute, BSI)所制定之 BS7799 資訊安全規範標準規範作為本研究的基礎，同時考量現有有限資源、技術條件以及醫療產業特殊性的要求，主要針對醫療院所防毒、防駭(包含部份隱私權保護之議題)之需求，探討BS7799實際應用於國內醫療院所資訊安全評估作業的適用性，並依據現行學者專家所提出之安全管理機制與技術建置出一個適用於醫療機構整合性資訊安全的架構。冀望本研究之研究成果能提供實務界與學術界，醫療機構資訊安全議題上研究之參考。

關鍵字：BS7799、資訊安全、隱私權、醫院資訊系統

Abstract

Due to the rapid change in the health care industry and social environment, those health care enterprises are enforced to deal with all challenges and problems occurred in this specific industry. To quickly response those challenges mentioned above, those enterprises aggressively adopt information technologies to improve their management performance and competitive advantages. However, because the systems involved in the efficient improvement of hospital enterprise are not designed properly, it causes a lot of problems coming from the poorly design of the integration, extensibility, management and security issues. Besides, the privacy protection of the computerized medical records is another issue we have to pay our attention. Although it is extremely important to protect the hospital information security from being illegally modified or accessed, the development of hospital security is still in its infancy stage and lacks of an integrated security architecture. In this research, we hope to utilize the recommendations proposed by the BS7799 as the basis of this research to improve the security of the integrated hospital security. The purposes of this proposal focus on two major topics: first of all, according to the guidelines of BS7799, we develop some hospital security recommendations which are suitable for the improvement of hospital security especially for the threat of virus and hackers (including partial privacy issues). Secondly, we implement a security framework by using current security mechanisms and technologies to improve the global hospital security. This study cannot only provide a good reference for hospitals in developing security hospital framework but also provides valuable empirical data for further research.

Keywords: BS7799, Information Security, Privacy, Hospital Information Systems

壹、緒論

近來電腦病毒(Virus)肆虐[1]與駭客(Hacker)入侵 [2]猖獗，國內外各型企業都紛紛傳出嚴重災情，醫療產業亦不例外。由於醫院本身主要的職責在於提供病患良好且適當的照護，一旦資訊系統受到攻擊而無法正常運作時，勢必會影響醫療照護的品質，增加醫院的經營成本，間接亦可能造成客戶流失的問題。此外，由於醫院內部儲存有許多病患相關之數位化病歷資料，這部份的資料通常是敏感且與個人隱私息息相關，這部份的資料也是系統非法使用者所欲攻擊的目標[9]，而傳統防火牆對於這類攻擊所能提供的保護還是相當有限 [10]，因此，如何建置一個整合性的醫院網路資訊安全架構及相關的機制，來確保系統正常的運作並保護資料使用的安全性及機密性，便成為一個極為重要的議題，這部份除了相關技術層面需克服外，相關管理機制之建立更是關鍵所在[11]

縱觀國內目前關於醫院資訊安全方面相關的研究還是相當的不足，且缺乏一個整體的安全架構設計，導致醫院組織對於各種威脅的承受度及應變能力非常的薄弱，因此，本研究將採用英國國家標準協會(British Standard Institute, BSI)所制定的BS7799資訊

安全規範 [12, 13]，作為醫院組織現行資訊安全作業實施評估的參考依據，提供組織強化資訊安全之建議，以確保有效規範組織安全的重要性，優先執行項目以及資源分配的情況，此外，亦期望能將相關的結果應用於醫院整體系統架構之設計，並配合相關安全機制的建立[14, 15]，來設計出一個符合現行醫院資訊安全需求之整體系統安全架構。

因此，本研究之主要目的，希望以BS7799標準規範作為研究的基礎，同時在現有有限資源以及技術條件下，提出一個更安全且易於建置之醫療機構整合性網路資訊安全架構與安全管理機制。其次，探討BS7799實際應用於國內醫療院所資訊安全評估作業的適用性，並依據現行學者專家所提出之安全技術，提出適用於BS7799各控制要點的具體作法及措施，以期本研究之成果能提供實務界與學術界，醫療機構資訊安全議題上研究之參考。

貳、文獻探討

一、BS7799

BS7799 為英國國家標準協會(British Standards Institute, BSI, 1999)所制定之資訊安全標準，其主要目的在於確保企業資訊相關資產，包括實體、軟硬體設施、資料及資訊之安全，避免因為企業內外部之各種威脅及本身之缺失，而發生企業資訊安全相關事件。其本身標準設計的主要精神在於確保資訊之機密性、完整性及可用性的三大原則之下，建立完善的資訊安全系統，因此，BS7799包含了不同面向之企業安全政策，從安全政策的擬定、安全責任的歸屬、風險的評估、存取控制等均有所著墨，並廣泛的包含所有安全議題，且可適用於不同的產業及組織，是一個內容相當完整的資訊安全標準。雖然在資訊安全管理規範標準中尚包含其它的標準，如：COBIT以及TCSEC等標準 [3]，且其目標皆為確保資訊的機密性、完整性及可用性等特性，但是由於各標準彼此性質、處理資訊安全的方式及評量的方式皆不同，各標準皆有其各自適合之應用，但若以整體企業資訊安全管理的角度來思考，BS7799較能符合本研究之需求。

由於BS7799 I:1999[12]的內容已成為國際標準組織(International Standards Organization, ISO)所承認的ISO-17799國際標準，因此，資訊安全相關的規範也逐漸為企業及各國所重視，國外及國內均開始依照此標準來訂定適合於各國國情使用之標準規範。國內與BS7799相關的研究有陳祥輝(2000)[4]的“資訊系統的安全管理及鑑識軌跡設計－基於MIB與資料庫之探討”，該論文主要是利用BS7799提出一個安全管理模式及使用者對系統的存取軌跡測試，以防止駭客入侵，並利用稽核的方式來識別出危及系統安全之情事；李慶民(2000)[5]提出”以BS7799為基礎建構資訊安全評選模式之研究”，其主要是以BS7799為基礎，針對虛擬私用網路建立相關評選模式以得到資安相關客觀的結論；劉永禮(2002)[2]提出”以BS7799資訊安全管理規範建構組織資訊安全風險管理模式之研究”，其主要是利用BS7799所建立的控制要點及項目，作為組織資訊安全風險管理衡量的依據，並建立一個風險管理的模式。

BS7799 在醫療產業上應用之研究包含：Janczewski(2002)[11]使用BS7799於發展醫療資訊系統(Healthcare Information System, HIS)方面的研究，探討HIS發展的基本安全基礎，並獲得HIS發展中安全相關議題的基礎建議，但是由於此篇論文的重點著重於HIS方面安全性的探討，而本研究則是希望能以全面性及整合性的觀點來探討BS7799在醫療產業的適用性並提出我們的建議以供國內各醫療院所強化其本身資訊安全管理之參考，而此篇論文部份的研究成果，可做為我們在醫療資訊系統安全性驗證之依據；葉相妤(2002)[6]提出“運用BS7799檢測醫療院所資訊安全管理作業文件之研究”，該研究中，也是以BS7799為基礎針對各醫療院所上繳衛生署的資訊安全管理作業文件分析各醫院資訊安全的程度，並與國外的研究結果相比，探討國內外的差異情況，同時並歸納出不同的等級的BS7799規範以為醫院採用之標準。雖然這部份所達成的目標與本研究所欲進行的研究類似，但是由於該研究是採用各醫療院所上繳的文件作為資料分析的來源，這些資料若沒有經由詳細的求證程序，那麼很難確保文件記錄結果是否與目前各醫院的現況相符，而所得到的結論的信、效度也會降低。而本研究主要的研究重點，則是偏重於整合性醫院資訊安全架構之研究

二、醫療院所資訊系統安全的需求

近年來資訊安全事件的頻繁，使得安全的議題逐漸的受到重視。根據Loef et al.等人[16] 認為醫療院所安全保護範圍應使其免於(1)人或財產的實體損害(2)隱私權的侵犯(3)病歷資訊的遺失或破壞(4)操作完整性或一致性的危害。而在醫療組織安全的設計方面，Loef也建議第一步應仔細識別及分析目前對於人員，資產以及資訊存在那些潛在的威脅，以及抵抗弱點(Vulnerability)的評估。其次，在完成潛在威脅的評估後，將有助於制定安全的對策，因此，威脅分析是建立一個有效且安全系統的重要組成元素。以下將針對醫院目前常見的電腦病毒及駭客攻擊等兩大安全威脅，以及病患隱私權保護之議題，探討如下：

(一) 電腦病毒及防治措施

所謂「電腦病毒」，泛指一些能夠影響電腦正常運作之有害程式，通常是指一段刻意被寫作之可執行電腦程式碼。隨著資訊科技與網路技術之進步與普及，電腦病毒之設計愈來愈精緻，其威力也愈來愈強，造成之破壞也愈來愈嚴重，而「網路病毒(Cyber plagues)」已是電腦病毒發展的當代熱門產物。電腦病毒之防治與企業資訊安全政策有關，防毒之措施可從個人端與企業網路端來探討。就個人端而言，廖國銘等研究人員(2003)[1]提出以下具體準則：(1)定期備份資料、(2)定期更改密碼(3)不隨意開啟不明郵件附加檔、(4)不隨意開啟檔案資料夾之分享、(5)不隨意下載未經安全認證之軟體、(6)使用軟碟片或可攜式硬碟前應先進行掃毒、(7)事實更新版本或完成修補的動作、(8)安裝防毒軟體及定期更新病毒碼、(9)適度調高瀏覽器的安全性設定等級；至於企業網路端，其亦提出以下要點：(1)企業防火牆的建置及規劃、(2)伺服器端關閉無使用之通訊埠、(3)內部網路之區隔、(4)使用者權限管理、(5)

對企業之E-mail掃毒過濾、(6)建立代理人(Agent)制度、(7)建立入侵偵測系統。

(二) 網路入侵及防治措施

隨著網際網路的蓬勃發展，為人們帶來了生活極大的便利，但另一方面而言，由於企業的電腦設備透過Internet網路而彼此相連，因此，有心人士更可以利用目前企業資訊系統或是現有作業平台已知的一些安全性漏洞，進行入侵攻擊，以達成特定的目的(林秉忠, 2001)[7]。一般而言，系統入侵者的目的包含：（1）當作入侵其他機器的跳板、（2）盜用系統資源、（3）竊取機密資料以及（4）惡意攻擊。系統入侵者的身份可歸納為（1）系統外部的使用者、（2）越權的使用者以及（3）瀆職的管理者，其中以第二類越權的使用者發起之攻擊最常見[17]，因此，如何透過管理的機制來加強企業內部安全之控管，也是一個非常重要的議題。此外，若能針對組織本身的特性訂定適用的資訊安全政策，如：加強內部控管及稽核機制、資料的定期備份、建立緊急的應變計劃…等資訊安全管理相關的規範，除可增加入侵的困難度外，亦能有效降低入侵事件所造成的損害。

(三)隱私權保護

隨著資訊科技及網路技術的蓬勃發展，造成資訊流通的方便，而另一方面也使更多人擔心個人醫療資訊隱私保護的問題[6,16]，因為透過網路的影響，病人個人健康相關的電子化資訊會更容易遭受入侵及破壞，同時可能被大量的散佈，而侵犯到個人的隱私 [18]。在與個人醫療相關的隱私權保護中，以美國的HIPAA隱私權保護相關法規最具代表性，其隱私權的保護包含五大原則 [8,19]，內容如下：

(1)病患掌握原則：病患有權看到並取得自己的病歷並有權要求更正不正確的病歷記錄，健康照護的提供者未取得病人同意不得揭露病患病歷資料。

(2)責任原則：儲存病患病歷資料的資料庫管理員須對其資料管理之政策、作業流程及系統負完全之責任。

(3)公共責任原則：為兼顧個人隱私及社會福祉，如為提升照護品質，減少照護危機，以維護公共衛生之使用，可不經過病患之同意，但資料之釋出應建立良好的規範。

(4)使用限制原則：使用者僅能取得最低之資料，個人健康資訊應只能用於健康照護目的，雇主不可以此作為人員聘用、解雇或升遷之參考，保險公司亦不可以此行銷其產品。

(5)安全保護原則：醫療機構應有防範資料不當使用或釋出的機制。在隱私的保護上應建立一定的流程，並應指派專人負責隱私保護的提醒與監控。

為確保資訊安全架構之完整，這些與病患隱私權相關的議題，也應在此架構設計時，一併納入考量。

叁、安全資訊系統架構之設計

一、現行醫療機構使用網路之需求

現行醫療機構使用網際網路之需求主要都為配合主管機關之行政命令或是法令規定，於規定的時間內，將資料上傳至主管機關，而資料傳送的方式有可能是由醫療院所採逐筆輸入的方式，或是傳送彙整檔案的方式來進行，傳送的時機大部份也是依據所轄業務機關所規定的期限內，將資料上傳，常見的資料上傳之需求，如：新生兒通報，老人檢健…等。此外，尚包含一些例外的狀況，如：SARS病患名單，是由主管機關視需求要求相關醫療院所傳送的資料。綜觀上述這些應用的需求，醫院內實際利用網際網路來傳輸資料的頻率較低且資料量很少，一般而言，醫院都是偏重於內部資料的處理，較少涉及外部資料的傳送，因此，在我們所提出的架構中，特別針對這種特性提出一個Internet上網區的規劃，並將其獨立於公司內部網路運作之外，彼此間若有資料傳遞的需求，則可透過另外設計的Intranet/Internet資料交換機制來完成。

未來配合健保IC卡的實施，病患的就醫及申報資料可能必須採取日結的傳送方式，這部份傳輸的資料量會較現行的需求為高，這部份也是我們在設計系統架構時必須納入的考量之一。此外，為加強對病患的服務品質，有愈來愈多的醫院，紛紛建置醫院的網頁系統，這個網頁系統除了提供病患健康相關資訊、醫院簡介及醫師內容外，其主要的功能在於提供網路掛號的服務，讓病患或其家屬可直接透過網頁系統，完成掛號的功能，減少病患等候掛號的時間，這個功能也是醫療機構在考量使用網際網路需求時，必須考慮的因素。此外，組織內部使用到網路的時機，除了對外作為訊息交換的媒介外，為加速組織運作的效能和經營績效，通常都是使用Intranet網路來完成醫院內部大部份的交易或作業流程，然而，Intranet的特性為高頻寬，資料傳送速度快以及使用頻率高等特性，這些剛好與Internet的特性相反，因此，在規劃系統架構時應特別予以注意。

二、安全策略規劃

規劃醫療資訊安全系統時必須要從整體安全防護的觀點來考量，考量因素包括：系統安全保護範圍之界定，風險評估，以及內部控管及稽核制度建立等管理面相關議題的探討，並架構出醫院整體資訊安全之需求，而這部份可配合BS7799所規範的10項控制要點，來重新審視現有的架構，並排定改善的時程及優先順序，再配合醫院的實際需求，並考量相關要素，修正出符合醫院需求的安全管理規範，將其落實至醫院的經營管理內。而其它的需求，如：隱私權保護相關的議題，也應納入系統安全規劃之中。其次，再來考量技術面之需求，這方面主要是針對防毒(Anti-virus)與防駭(Anti-hacker)兩大措施來進行，這部份可依據BS7799在存取控管控制要點之建議來設計，且根據許多學理與實務案例分析得知，駭客入侵之管道主要來自外部之網際網路，而電腦病毒之傳播，除了網際網路外，企業內部電腦之不當檔案存取、複製亦是主要傳染源，因此，有效區隔Internet與Intranet網路實體拓蹼(Topology)並制定完整且嚴謹的規範來限制同仁電腦文件之存取，才是杜絕電腦病毒與駭客入侵之根本解決方案。除了防範機制外，機動且完善的災害復原機制亦不可或缺，因此，選擇適當之防毒軟體並導入有效之軟體派送系統，將扮演災害復原之重要角色。綜合上述，「嚴格管制上網」、「杜絕任意檔案輸出

入」、「導入專業之軟體派送系統」與「建置企業掃毒系統」，即是本研究提出且建置之安全資訊系統架構之主要精神。而在本系統架構的建構過程中，必須反覆的利用BS7799安全管理規範中的各種不同控管要點，持續評估及改善此系統架構並建置適當的機制來滿足資訊安全管理的需求。

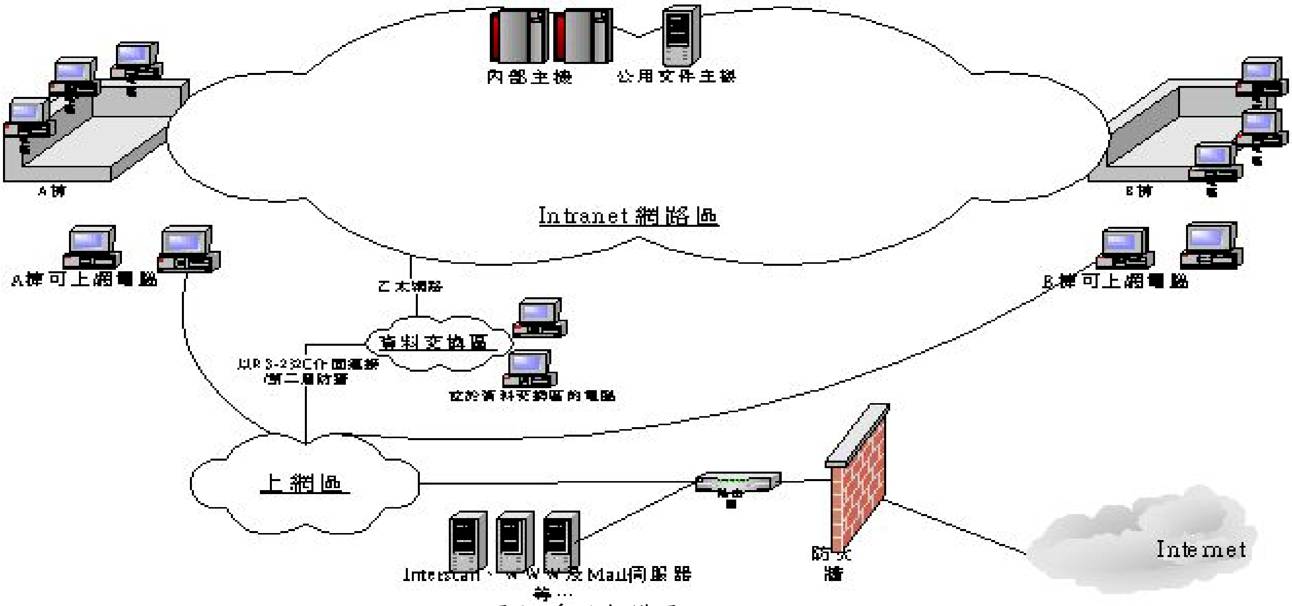

圖1:系統架構圖

三、安全資訊系統架構

在考量醫療機構作業特性與對Internet使用需求特性，本研究提出一個安全之資訊系統架構如圖1所示，其主要組成包含：隔離之Intranet網路區、隔離之Internet上網區、Internet防火牆、Intranet公用文件區、Intranet/Internet資料交換系統以及防毒與派送系統等。在此架構下，全院區分為Intranet(醫療系統區)與Internet(上網專區)兩個實體上互相獨立之網路，醫療系統區無法使用Internet，而上網專區無法使用醫療系統。以下說明之(個案醫院擁有兩棟大樓)。

(一) 隔離之Intranet網路區

在網路佈建上，將醫院日常作業所在之網路區域完全規劃成獨立之區域網路，此區域網路上包含所有支援醫院作業之個人電腦、資料庫系統主機，以及所有其他設備。使用者使用連接於Intranet網路之個人電腦來進行所有醫院相關之內部應用系統(例如：醫師使用之門診醫囑系統、行政人員使用之人事系統…)，以及電腦文件製作(例如：衛教文件編製、門診人次分類試算結果存檔…)。在此網路之個人電腦完全無法連上Internet，其若真有連上Internet之必要，則其必須親至「Internet上網區」上網。此部份強調之隔離，在於網路拓蹼上實際與連上Internet之網段絕對區隔沒有任何互連之網路線路，亦即不使用Virtual LAN等網路技術所作之邏輯劃分(實體上Internet與Intranet彼此仍共用相同網路傳輸媒體)，此外，針對Intranet內部系統的使用，必須強化權責區分，以及系統的存取控制，唯有授權的使用者才有存取及使用系統的權利，此外，對於系統的使用情況亦必須加以記錄，以作為系統稽核之依據。

(二) 隔離之Internet上網區

Internet上網區之目的在於提供一特定地點，供醫院同仁連線上網。醫院需選定特定集中之地點(例如：醫院之電腦教室)來建置一上網區域。考量使用上之特殊需求，上網區之電腦可透過較長距之網路佈線配置於醫院之任何地點以方便人員使用。此部份強調之隔離，在於上網區網路與Intranet完全隔絕，上網區之電腦無法進入Intranet區域。一旦此區域之Internet主機或其他電腦遭受駭客破壞或病毒肆虐，由於其與Intranet獨立，因此不會影響醫院日常之內部作業。

(三) Internet防火牆

隔離之Internet上網區與Internet間仍需架設高效能之防火牆系統，以保護上網區內之醫院WWW、DNS與Mail等Internet主機之安全。為確保重要主機運作的正常，企業亦可視需求添購入侵偵測系統(Intrusive Detection System, IDS)，藉以提升安全防護的等級。

(四) Intranet公用文件區

此部份在開發或導入一管理全院各式電腦文件之應用系統，人員在電腦編輯完成之文件需上傳至此公用文件區，並且可經由權限設定機制來規範何人或何部門可讀取該文件。此系統之目的除可統一管理醫院文件外，另一重要目的則在提醒人員，其使用之個人電腦隨時可能因中毒與其他原因而被資訊部門重新安裝或收回，屆時存於其內之文件將招到破壞或刪除而無法救回。使用者若需將檔案複製至外部媒體(如：軟碟、隨身碟等)，亦需透過公用文件區之機制來完成(例如：在資訊部門之某台電腦配備外部儲存裝置可將外來檔案存至公用文件區或將自公用文件區將檔案輸出至磁碟片)，因為所有一般個人電腦之外部儲存裝置(軟碟機、USB連接阜等)皆已被拆除。

(五) Intranet/Internet資料交換系統

此系統之開發為本架構得以順利運作之關鍵。在實務上，醫院仍無法完全避免 Internet 上提供之服務不存取醫院內部之資料(例如：網路掛號)。因此，如何建立安全性高之 Internet 與 Intranet 傳輸管道又可免於駭客入侵之威脅，則是本交換系統設計之重點。一般醫

院通常只建置一套防火牆系統來保護 Internet 與 Intranet 之資料互動，然而，許多的國內外案例告訴我們，即使採購任何高效能之防火牆，皆仍無法保證網路駭客之入侵，由近年發生之中華民國總統府網站及美國國防部網站皆曾被駭客入侵之事件即可得到驗證。基於安全考量，部份醫院或單位會建置第二層或多層之防火牆來因應，然而這些安全設備仍建置於現有開放性網際網路通訊協定之上，因此潛在之安全威脅並無法保證消除。

為了免除外來駭客透過網路入侵 Intranet 之危險，其一勞永逸的方式就是不使用網路來作兩者傳輸之媒介，亦即基於 TCP/IP 網路協定之各種潛在危險將不會發生。考量開發便利性與成本效益，透過低層之 RS232C 串列傳輸方式或是其它可替代的傳輸方式來作為 Internet 與 Intranet 溝通橋樑將是極佳之選擇。其做法是：資訊人員開發主從式(Client/Server)RS232C(Null modem 傳輸)傳輸系統(包含 Client 端與 Server 端兩種程式)，分別安裝於醫院 Internet(Server 端程式)與 Intranet(Client 端程式)之各一台電腦中，此二電腦以 RS232C(Null modem)傳輸線連接著。一旦 Internet 網站服務需存取 Intranet 資訊時，Internet 之電腦 Server 端程式會透過 RS232C 線與 Intranet 電腦之 Client 端程式建立連線(Connection)，並將需求資訊傳給 Client 端程式；Client 端程式收到資訊後進行相關處理後將結果回傳給 Server 端程式，進而呈現結果於 Internet 網站上。如此一來，使用本「資料交換系統」既可達到 Internet 與 Intranet 互傳之目的，又可免除被駭客入侵之危險，相信是醫院網路安全防治上優於防火牆之有效方式。然而，RS232C 傳輸線之傳輸速度不高，並不適合於大量資料資料之交換，然而，以醫院網站應用服務之需求(例如：網路掛號)，通常並不需進行大量資料之傳送。

(六) Intranet/Internet資料交換系統

完整資訊安全措施除了上述之預防措施外，亦需包含有效之偵測(Detecting)與回復(Recovering)之機制。因此，對於病毒防範與偵測，醫院可導入口碑佳之防毒系統來因應，而災害復原則採用專業軟體派送系統來進行。

四、系統發展

實現本安全資訊系統架構之發展，除採購並導入防毒系統、軟體派送系統、防火牆外，資訊部門另需進行相關應用系統開發與修改與網路電腦佈建重整工程(此些工作亦可委外進行)，最後則進行使用者教育訓練與推行，相關步驟受限於篇幅限制，則不在此詳述。

肆、討論

本研究主要是希望以現由BS7799資訊安全之規範作為醫療院所制定相關安全管理規則之參考依據，並以此檢視現有醫院安全防範上可能之漏洞及威脅，同時針對醫療院所常見病毒及駭客之產生安全之顧慮，提供一個整合性的資訊安全架構。本研究與南部某區域級醫院合作，實際在醫院環境中建構此安全資訊系統架構。本研究實際發展RS232C之傳輸交換系統並應用於醫院網站提供之網路掛號系統中，經過實際評估，完成一筆網路掛號之時間與從前透過網路方式相同(並無明顯延遲現象)。因此，本研究所提之架構，經實作之驗證後，可歸納出以下之特性、限制以及導入此架構決策之考量，相關內容說明如下：

一、安全資訊系統架構之特點

1. 駭客無法入侵，安全性高：利用 RS232C 實體線路將醫院的 Intranet 及 Internet 網路做一有效區隔，駭客不得其門而入，因此有較高的安全性。
2. 電腦病毒不易感染、傳播與發作：不當的檔案存取或是使用來源不明的程式最易受到電腦病毒的危害，本研究是採用集中管理的方式，僅允許使用者使用上網區的電腦與外界進行互動，這些電腦本身就會安裝個人版的防毒軟體，並且定期更新病毒碼之內容，其受感染的機會相對變小。
3. 高安全性之電子文件存取：由於上網區的規劃，電子文件的存取相對較有保障，不怕受到病毒的威脅，因此，電子文件的存取具有高安全性。
4. 公用電子文件控管容易：公司內部經常有一些共用的電子文件必須進行分享，因此可透過公用文件區的建置，來達成資訊分享的目的，每一份文件都會由資料上傳者嚴格的設定允許讀取者的權限，故亦能輕易的進行文件的存取控管。
5. 建置成本低廉：對醫院而言，採用我們所提出的整合性資訊安全架構，其本身在成本支出方面僅需添購上網區所需的電腦軟硬體設備以及 RS232C 傳輸線路，其他所需的軟體功能，皆可由內部資訊室人員進行開發，因此，此架構在成本方面，相較於醫院其他的支出而言，相當的低廉。

二、安全資訊系統架構之限制

1. Internet 與 Intranet 間資料交換之速度較一般網路慢：受限於 Internet/Intranet 網路間使用 RS232C 傳輸線路既有傳輸速度的限制，其速度較一般網路慢。為改善傳輸速度上的限制，爾後可能會針對其他傳輸速度較快的傳輸線路進行研究，並開發相對應的資料上傳/下載系統。
2. 無現成套裝軟體，程式需另外發展：目前並無現有的套裝軟體可資利用，因此，所需使用的軟體還需另外開發。

三、導入安全資訊系統架構之決策衡量

1. 醫院內部對於即時與Internet連線並作資料交換之需求較低。
2. 配合現行BS7799資訊安全規範之控制要點，規劃醫院整體安全系統架構。

陸、結論與建議

本研究主要著重於整合性醫院網路資訊安全架構的研究，由於目前鮮少有專家學者針對醫院之需求提出一個良好的解決方案，而醫療院所也是在此次疾風病毒的影響之下，才開始深切體會資訊安全對於企業經營所扮演之重要性，而透過本研究所提架構之實作，

除可確保醫院內部資訊系統之正常運作外，同時亦可達到內部文件分享及系統建置成本低廉的優點，因此可提升醫療院所導入的意願。此外，本研究之主要貢獻不僅提供一個整合性安全系統架構發展之準則，讓醫療院所有所遵循的依據，同時並在此架構之下提出一個符合現行醫院需求、低成本、易於建置且安全性高的防毒防駭系統。此一架構亦可提供醫院導入BS7799 安全管理規範及整合性安全架構發展準則，作為其他醫院或是其他產業規劃之參考。同時，並可讓有意願提升醫院整體安全防護的同業，瞭解導入此一架構的重要因素，以減少系統建置時的障礙。

柒、參考文獻

1. 廖國銘、仝興倫、劉順德、張光宏、蔡雨龍、鍾佩芳、施君熹、孫三為(2003)，企業機構之網路病毒防治與管理，電信研究雙月刊，33(2)，pp307-321。
2. 何全德(2000)，從駭客入侵淺談網路安全防護策略, 資訊與教育雜誌，78， pp2-7。
3. 劉永禮(2002)，以 BS7799 資訊安全管理規範建構組織資訊安全風險管理模式之研究，元智大學工程與管理所碩士論文。
4. 陳祥輝(2000)，資訊系統的安全管理及鑑識軌跡設計－基於 MIB 與資料庫之探討，文化大學資管所碩士論文。
5. 李慶民(2000)，以 BS7799 為基礎建構資訊安全評選模式之研究－以虛擬私有網路系統為例，國防大學國防資訊所碩士論文。
6. 葉相妤(2002)，運用 BS7799 檢測醫療院所資訊安全管理作業文件之研究，陽明大學衛生資訊及決策所碩士論文。
7. 林秉忠(2001)，2001 年台灣 Web 伺服器安全性調查，資訊安全雜誌，7(2)， pp. 76-90。
8. 吳昊(2000)，由醫療資訊隱私之觀點論全民健保IC 卡政策，台灣大學法律研究所碩士論文。
9. E. Smith, J.H.P. Eloff (1999), “Security in health-care information systems-current trends,” International Journal of Medical Informatics, 54, pp 39-54,.
10. Allen Householder, Kevin Houle, and Chad Doubherty (2002), “Computer attack treads challenge internet security,” Security & Privacy, pp 5-7.
11. Lech Janczewski and Frank Xinli Shi (2002), “Development of Information Security Baselines for Healthcare Information Systems in New Zealand,”Computer & Security, 21(2), pp172-192.
12. BSI (1999), “Information Security Management – Part I: Code of practice for information security management”, BS7799-1:1999, BSI (British Standards Institute).
13. BSI(1999), “Information Security Management – Part II: Specification for information security management systems”, BS7799-2:1999, BSI (British Standards Institute).
14. Dimitris Gritzalis (1997), “A baseline security policy for distributed healthcare information systems,” Computers and Security, 16(8), pp709-719.
15. Peter Ward and Clifton L Smith (2002), “The Development of Access Control Policies for information Technology Systems,” Computer & Security, 21(4), pp356-371.
16. C. Loef, N. J Mankovich and M. Rosner (2002), “Standards and security for medical information technology,” MEDICAMUNDI, 46(2), pp41-46.
17. Richard Power (2000), “Tangled Web: Tales of the Digital Crime from the Shadows of Cyberspace,” Que/Macmillian Publishing.
18. Gary Kurtz (2001), “EMR confidentiality and information security, ” Journal of Healthcare Information Management, 17(3), pp 41-48.
19. David Baumer, Julia Brande Earp, and Fay Cobb Payton(2000), “Privacy of medicine records: IT implications of HIPPA ,”ACM SIGCAS Computers and Society , 30(4), pp 40-47.