行政院及所屬各機關出國報告
（出國類別：實習）

Internet Data Center
（網際網路資料中心）
服務與支援資訊技術出國報告

服務機關：中華電信研究所
出國人　職　稱：助理研究員
　　姓　名：張光宏

出國地點：美國
出國期間：91年11月17日至29日
報告期間：92年1月24日

系統識別號:C09200751

公 務 出 國 報 告 提 要

頁數: 14　含附件: 否

報告名稱:

實習Internet Data Center(網際網路資料中心)服務與支援資訊技術

主辦機關:

中華電信研究所

聯絡人／電話:

楊學文／03-4244218

出國人員:

張光宏　中華電信研究所　網路及多媒體應用技術研究室　助理研究員

出國類別: 實習

出國地區: 美國

出國期間: 民國 91 年 11 月 17 日 -民國 91 年 11 月 29 日

報告日期: 民國 91 年 01 月 24 日

分類號/目: H6／電信　／

關鍵詞: Internet,Data,Center,網際網路,服務

內容摘要: 網際網路已經成爲人們生活的一部份，在這個平台上所提供的服務也日益增多，相關傳輸及硬體設施的強烈需求因此應運而生，這也就是相當多廠商相繼建置網際網路資料中心(Internet Data Center, IDC)的原因，然而當相關服務陸續建置的同時，網路及系統安全的議題往往會被忽略，經過最近網路駭客及蠕蟲的攻擊，我們可以了解資訊安全在維護服務系統是相當重要的。 資訊安全議題的範圍可以說是相當廣泛，此次研習的重點著重在維護網路及系統安全的相關機制的建立，這部分的相關知識及策略皆可運用於IDC機房及企業內部安全機制的擬定；在本報告裡將包含以下安全議題的討論：防火牆安全機制、加密與認證、弱點掃描機制、入侵偵測機制和備援及復原機制

本文電子檔已上傳至出國報告資訊網

摘要

網際網路已經成為人們生活的一部份，在這個平台上所提供的服務也日益增多，相關傳輸及硬體設施的強烈需求因此應運而生，這也就是相當多廠商相繼建置網際網路資料中心(Internet Data Center, IDC)的原因，然而當相關服務陸續建置的同時，網路及系統安全的議題往往會被忽略，經過最近網路駭客及蠕蟲的攻擊，我們可以了解資訊安全在維護服務系統是相當重要的。

資訊安全議題的範圍可以說是相當廣泛，此次研習的重點著重在維護網路及系統安全的相關機制的建立，這部分的相關知識及策略皆可運用於IDC機房及企業內部安全機制的擬定；在本報告裡將包含以下安全議題的討論：防火牆安全機制、加密與認證、弱點掃描機制、入侵偵測機制和備援及復原機制等。

目　　錄

1. 目的

職等此次奉派出國研習網際網路資料中心(Internet Data Center, IDC, 以下簡稱IDC)相關建置及安全技術,出國時間自民國九十一年十一月十七日至民國九十一年十一月二十九日,含行程共十三日。其中十一月十八日至十一月二十七日於美國IBM接受IDC系統建置、管理及安全控制技術之訓練。

中華電信IDC機房的租用率一直是全國之冠，國內多數企業大多利用中華電信之系統及頻寬之優勢來提供相關網路服務，因此IDC相關網路及系統之安全性便相形重要。最近因為電腦病毒的技術已經從傳統的破壞電腦主機的行為，拓展成網路傳播的攻擊模式，其所造成的傷害也將從單一系統擴展至網路全面性的癱瘓，這樣的傷害除了服務將因此停止之外，對於企業的商譽的影響將是嚴重的打擊，所以維護系統的安全及網路的順暢是我們責無旁貸的責任。

資訊安全系統的建置是需要投入時間、預算及決心的，美國在很早以前就已經投入網路安全的領域，但相關技術基於戰略需求並未輸出到其他國家，與其等待先進國家發展相關網路安全技術，不如積極自行建立相關安全機制及組織一個具備資訊安全知識的團隊來維護及反應廣泛的資安危機。

本份報告將分為：1.目的、2.過程、3.心得。

2. 過程

2.1. 行程概要

整個行程從11月17日出發，至11月29日返國，共計13天。其受訓過程如下表：

日期	主題
11/17	起程
11/18~11/22	IBM Security Training
11/23~11/24	假日資料整理
11/25~11/27	IBM Industry Solution Lab
11/28~11/29	回程

2.2. 受訓內容

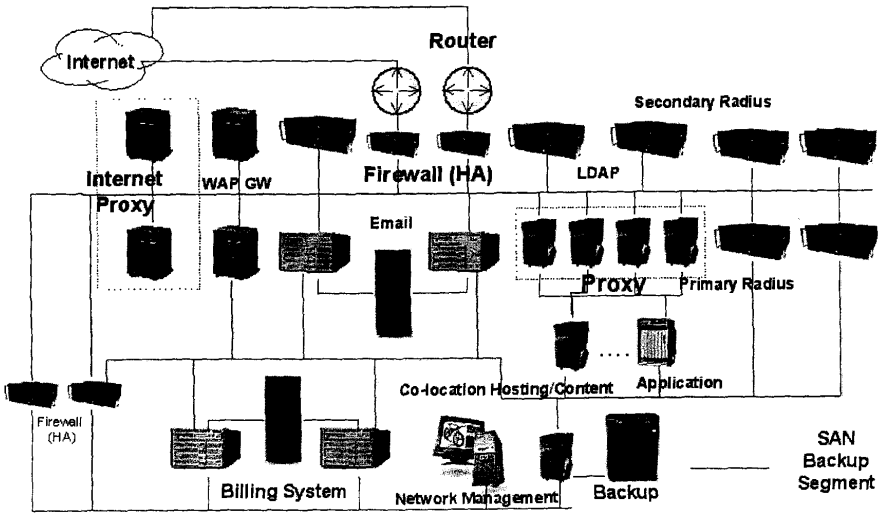
本次實習內容著重在於 IDC 的服務建置及安全性控制的討論，尤其網路安全的問題已經是全世界企業及一般用戶的共同話題，所以這次的課程討論大部分著重於安全性議題。

職將受訓內容分為以下幾個部分進行說明：

- IDC 服務內容簡介
- 網路安全機制
  - 防火牆安全機制
  - 加密與認證
  - 弱點掃描機制
  - 入侵偵測機制
  - 備援及復原機制

2.2.1. IDC 服務內容簡介

IDC 所提供的服務可分為硬體、軟體及管理三大部分，硬體設備部分包括空間、電力、主機及網路設備，軟體服務部分包括電子郵件、網頁伺服器、FTP Server、VoIP、Content Delivery 及 VPN 等，管理機制包括網路、設備監控及客服系統等等，由於 IDC 的建置均符合較高等級的軟硬體標準，可以提供企業、ISP 業者及個人用戶穩定、可靠、安全及高品質的作業環境，幫助企業掌握 e 時代經營優勢。



圖一　IDC 服務平台網路架構圖

以下就 IDC 服務平台之各項硬體設施、提供之服務及管理層面之功能特性分述如下:

(1). 硬體設施：

機房之建置需符合標準的電信環境規格，採高架地板，並具備防水防震功能，溫控空調系統來維持硬體系統之穩定性，消防系統持續監控及不斷電系統來維持系統服務之運作(Service Availability)。

網路設備需包含 Router、L2 Switch、L3 Switch、L4 Switch，主機設備包含 UNIX、Linux 及 Windows Server 主機，其他網路設備有防火牆、代理伺服器、頻寬管理器及撥接系統等。

(2). 服務提供：

IDC 之基本服務包括：主機代管 (Co-Location)、虛擬主機 (Virtual

Hosting)、DNS 申請及代管、虛擬網站、虛擬郵件信箱、虛擬網站流量分析。加值應用服務包括：資料儲存、防火牆租用、伺服器快取加速、內容傳送(Content Delivery)、伺服器負載平衡、虛擬私有網路、Voice over IP、專案規劃諮詢、應用服務提供等。

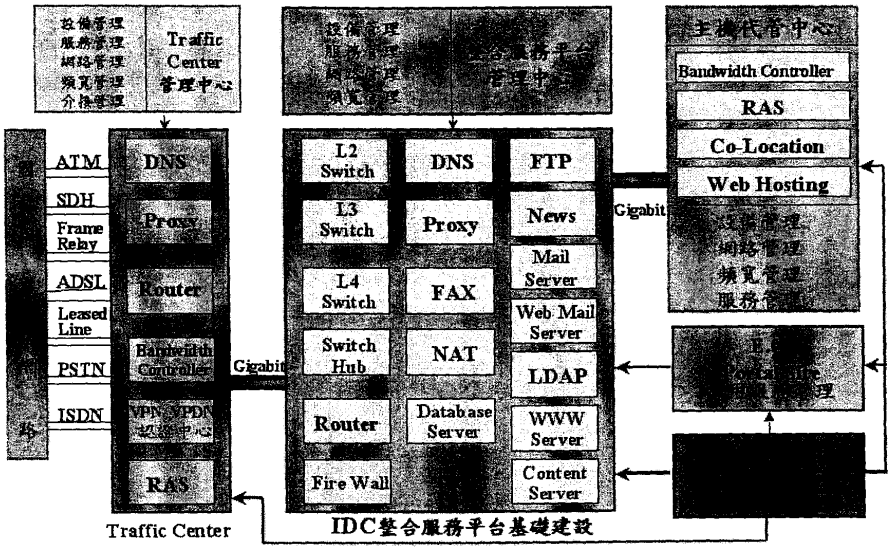
(3). 維運管理服務：

維運管理機制可提供用戶對於其設備及服務品質之掌握，一般 IDC 業者提供以下維運管理服務：

- 主機設備預警及故障監控
  - CPU
  - Memory
  - Disk
  - Application
- 網路設備及流量監視預警
  - 流向特定的資料流
  - 不同封包之流量
- 訊務報表
  - 日報表
  - 週報表
  - 月報表
  - 年報表
- 客戶專業服務

IDC 服務平台之設計及規劃必須符合相當的標準及規範，建置一個符合穩定、安全及高效率的服務平台必須具備以下幾個需求：

- 高標準安全穩定之電信機房
- 備援網路架構及設備
- 高頻寬網路架構
- 伺服器設備 HA 架構
- Server Load Balance
- 安全之網路及伺服器系統
- 充分連接國內外其他各大交換中心及 ISP
- 完整的網路運轉中心 (NOC)
- 24 小時警衛、網管、技術支援



圖二　IDC 整合服務及管理平台架構

2.2.2. 網路安全機制

網際網路已經深入到每一個家庭中，在這個平台上的交易行為日益頻繁，在這樣開放的平台上，資料的安全及網路設備是否可以正常運作是我們必須考量的重點，在本節網路安全機制部分將就以下五個部分來探討網路安全機制的建立：

(1). 防火牆安全機制
(2). 加密與認證
(3). 弱點掃描機制
(4). 入侵偵測機制
(5). 備援機制

2.2.2.1.防火牆安全機制

防火牆(Firewall)是目前網路存取控制最有效率的解決方案之一，一般企業或者是網路服務提供者都會將防火牆當作維護企業內部安全的第一道防線，IETF正式將防火牆列為資訊安全的機制(RFC1636)，其重要性可見一般，內部重要資源根據既定的安全政策及封包的過濾可以對進出的行為加以監控及紀錄，可遏止部分惡意行為的破壞。

一般來說，防火牆如架設於介接內部及外部網路之間，稱之為外部防火牆，如果架設於內部網路則稱之為內部防火牆，外部防火牆作為內部網路與外部網路區隔之用，達到隔離的作用；而內部防火牆可作為內部網路相互監控之用。在任何狀況下，防火牆的規劃不應該因方便而留有任何後門，這個後門往往會成為日後安全的漏洞。

防火牆分為兩大類型：封包過濾型防火牆及進階型防火牆。

- 封包過濾型防火牆
  是一種較為簡單的防火牆類型，透過檢查通訊協定之網路層、傳輸層和會話層封包，過濾其來源位址、目的地址、通訊協定、目的埠等資訊，其運作方式較為有效率，且價格較低廉，但其功能性仍較不足，對於較複雜的安全政策並無法支援。
- 進階型防火牆
  目前市面上的產品大多為這種類型，除了具備封包過濾的功能外，可檢查應用層部分，配合安全政策對於進出的封包加以管制。

目前市面上防火牆產品有軟體式及硬體式兩種，其功能及執行效率各有優缺點，其一般的功能包含以下幾個部分：

- 封包檢查
  可檢查 HTTP、FTP、SMTP 等通訊協定的封包內容，針對其封包特定的格式加以改寫來達到阻絕或隔離的目的；在 HTTP 通訊協定中可改寫其內容，阻絕特定之 Java Plug-in 或 ActiveX 程式；在 FTP 通訊協定中可根據檔名及其內容來進行病毒之掃描。
- 負載平衡
  可利用隨機、Round-robin 或是時間延遲等方式來分配網路流量到不同伺服器上。
- 使用者認證
  一般大多支援 Radius、LDAP、及 Kerberos 等認證方式。

- 網路位址轉譯(Network Address Translation, NAT)
  將內部位址對應至 Internet IP 位址，可進行多對一的對應模式，也就是所謂的 Dynamic Mapping，也可進行一對一的對應模式也就是所謂的 Static Mapping。
- 圖形化介面
  提供圖形化(GUI)介面來顯示所有的即時訊息，並可設定相關告警訊息，以提供管理者處理。

防火牆的配置可視實際需要建置，包括內部網路、對外介接的網路等地方均可視需要建置，以下提出部分需要加強建置的位置及方式：

- 在對外網路連結的部分必須建置防火牆以進行隔絕的作用，並視需要規劃所謂的"非戰區(DMZ)"，將可暴露於 Internet 與必須保護的部分加以分類，並制定相關安全政策，落實於防火牆存取安全控制中。
- 內部網路中之重要伺服主機資料必須加以保護時，應架設防火牆來控制資料之存取。
- 利用防火牆所提供之虛擬私人網路功能(VPN)來控制從外部必須存取內部資源的連線。
- 不同位置的內部網路需要利用 VPN 來加強其資料及存取的安全性。
- 必須開啟日誌(Log)的功能，並定時檢查是否有異常行為的發生。

由於防火牆攸關資訊安全的重責大任，選擇防火牆功能時應該將以下幾個重點列入考慮：

- 可支援的最大網路流量
- 同時可容納的 Session 數目
- 可設定最大的 Policy 數目
- 支援的通訊協定及服務項目是否合乎需求

2.2.2.2.加密與認證

資訊加密的目的在於防範於資料傳輸過程中被有心人監聽而竊取重要資料，加密方式是利用加密演算法對資料加密，目前已經公佈的加密演算法已經上百種，主要分為對稱（私鑰）演算法和非對稱（公鑰）演算法。

對稱演算法中加解密均透過同一把私鑰來完成，具有較高的保密等級，較著名的演算法有：DES、3DES、IDEA、RC4、RC5 等，因為加解密均透過同一把私鑰，相對地，私鑰的保存及傳遞的安全性相形重要。

非對稱演算法之加解密方式是透過兩把不同的 keys 來完成(私鑰及公鑰)，其演算法較為複雜，執行效率較差，較著名的演算法有：RSA、Diff-Hellman 等，這種演算模式較符合現今網際網路的開放性架構，是目前網路傳輸安全重要的技術之一。

由於網際網路在發展之初並未將網路傳輸的安全性加入其通訊協定中，造成在網路上傳輸的資料多為明文，有意竊取密碼或重要資訊的有心分子，往往透過網路監聽的方式便可輕易獲取，因此網路傳輸加密與認證方式是另一項重要的議題：

- SSH：對 Telnet 之傳輸資料加密，包括帳號及密碼。
- SSL：SSL 提供網路資料傳輸的安全性，其作用在 TCP/IP 之傳輸層，因此不管在上層之通訊協定為何都可以使用 SSL 加密傳輸，所以 SSL 經常使用在 HTTP 及 SMTP 的傳輸當中。
- SET：是一種為提供網際網路電子交易安全性的機制，消費者、網路商店、信用卡發卡銀行、網路商店銀行四者在各自的交易機制下透過私鑰再加密，彼此都不會看到對方的交易內容。

2.2.2.3.弱點掃描機制

弱點掃描是另一項維護網路安全重要的機制，透過某些已存在的弱點樣板模式(Pattern)對於重要的系統主機進行弱點掃描比對，可提早發現弱點的存在，進而修復這些弱點，是一種主動式的網路安全稽核動作。

雖然弱點掃描是一項很好的網路安全機制，但是由於其運作原理是根據弱點的模式比對及某些系統內部資訊的猜測動作，常常造成弱點資訊的誤報，形成管理人員的困擾，因此，弱點掃描報表的研讀及分析是必要的，並可透過資訊安全人員協助，確實定位出弱點的發生位置。

市面上有一些免費的弱點掃描軟體，像 Nessus 等，可以做到初步弱點的確認，其缺點是弱點比對 Pattern 的管理問題，無法確定是否有即時更新；另外像 ISS 之 Internet Scanner 是一套商業軟體，可以有較高的判讀率，弱點比對 Pattern 有專人在收集及撰寫，但購買成本是一項重要的因素。

以下就評估弱點掃描軟體所必須考慮的因素加以說明：

- 弱點資料庫是否有專人收集及維護，及其更新速度是否夠迅速。
- 執行效率問題。
- 執行時對目標系統的影響程度。
- 掃描程式的穩定性。
- 是否可以自訂弱點比對 Pattern？
- 掃描結果分析報表的準確度。

2.2.2.4.入侵偵測機制

入侵偵測系統(Intrusion Detection System, IDS)是一種檢視及分析網路流量，透過 Pattern 比對來偵測進出之封包是否為惡意攻擊之封包，包括外來的攻擊或非法擷取內部資訊的行為，及後門程式的攻擊行為；另一種檢視及分析行為是透過系統主機的日誌檔的紀錄來比對所有對系統主機的動作，藉以查出異常行為的發生，交叉比對的結果可以降低入侵行為的誤報率。

入侵偵測系統在網路卡之混雜模式(promiscuous)收集該網段的封包，即時分析封包內容並比對 Pattern 資料庫，再根據先前之設定進行特定的反應，例如發送簡訊、電子郵件或者是其他警示訊息，甚至可以切斷網路的服務，除了封包比對之外，目前多數的入侵偵測系統也可以針對特定的 Port 偵測特定的入侵行為，

對於多數後門程式透過特定 Port 來進行攻擊行為，有相當好的監測功能。

這種網路型的入侵偵測系統的安裝只需在需要偵測的網段安裝一部入侵偵測系統，便可即時監控及分析網路流量，建置成本較低；在建置入侵偵測系統的主機時應該將其放置在較隱密的地點，並且不要提供任何服務，以免造成駭客攻擊的目標，這樣的偵測方式攻擊者的行為不易被隱藏。另外，對於某些不成功的惡意的嚐試性攻擊可以提早被監控，進而提供適當的處置。

如果攻擊者的行為在系統主機上進行，並未透過網路方式傳輸，那麼監測網路流量的偵測系統並無法確實取得該惡意行為的證據，面對這樣的惡意行為可以審視系統主機的所有日誌紀錄來發現異常行為的發生，成功或非法登入的用戶進入系統後的所有行為將會被紀錄，設定更嚴密的稽核原則將可以取得更多的系統行為資訊，掌握系統的動態。

結合在網段的流量監測及系統主機日誌的分析，可以掌握多數的攻擊行為，並可即時反應，以免系統遭受更大的破壞，然而，誤報率一直是入侵偵測系統的最大弱點，經由更縝密的監視分析往往會將某些正常的行為視為攻擊行為，造成管理者的困擾，因此，管理人員對於入侵偵測的判讀也是一件重要的工作。

2.2.2.5.備援及復原機制

資料備份及復原機制永遠是資訊安全不可或缺的一環，不管服務系統是遭受天災或是惡意的攻擊行為而造成資料的流失，資料是否即時備份是服務可否繼續的關鍵，擬定一套嚴格及周密的備份計劃是必要的，且應嚴格督導執行。

備份計劃應該包含以下規範：

- 備份負責人的歸屬及責任。
- 事先規劃系統主機資料備份的深度及廣度。
- 完全資料備份的時間及部分資料備份的時間，需仔細規劃避免資料遺漏。
- 定期檢視備份資料的完整性及正確性。
- 備份資料的保全。

在談論資料備份及復原機制之餘，對於備份資料的保全應該格外注意，由於備份的資料大多是重要的資料，我們需更加防範備份資料被竊取，當我們花費很多心力來防範來自網路攻擊或惡意存取的同時，常常忽略備份資料已經集合所有重要資料的大全，若遭有心人竊取後果將不可預料。另外，在定期檢視備份資料的完整性及正確性的方面是另一項管理者經常忽略的部分，卻是在最危急的狀況

下經常出錯的環節，定期檢視是根本解決之道。

3. 心得

隨著最近幾年來資安事件層出不窮地發生，每次都帶給國家、社會及企業相當程度的傷害，所謂"沒有絕對安全的系統"，系統或網路本身都存在著原創或是人為所造成的漏洞，需要企業本身針對個別需求進行資訊安全的規劃及建置，一個具備高度安全的網路及主機一定所費不貲，基於成本考量，首先先分析所管轄的系統及網路最脆弱及最需要加強的部分在哪裡，再根據本文所討論的資訊安全技術配合安全政策的制定及落實，建構一個全面性的安全體系，才有可能實現資訊安全的境界。

IDC機房的建置已經漸漸步入成熟期，而管理及安全的議題正考驗著服務提供者，由於IDC業者必須肩負著網路及主機系統的穩定性及可靠性，所以在資訊安全的規劃及建置格外重要，以制定一套符合實際需要的資訊安全策略為第一優先工作，再培養一組精通網路安全的人才，時時監控安全狀態，再由上而下確實落實資訊安全政策，配合持續性的管理機制，達到一個相對安全的作業環境。

綜觀此次研習，資訊安全已經是所有企業及服務提供者未來的重點工作，連微軟的軟體開發策略也從功能導向轉換成安全性導向，可見安全已經是未來大家努力的方向，然而在成本及時間因素的考量下，從最有可能出問題及最脆弱的位置下手，是一個不錯的方向，既可以解決目前的嚴重問題，又可以將投資成本分散，若一開始就佈建所有的安全設備，不是一項符合經濟效益的做法。

資訊安全的目的不外乎提供主機系統資訊的可用性、完整性及機密性，為達到這個目的，除了以上所提之相關技術及方法之外，最後也是最重要的就是安全政策及管理機制是否可以落實，透過由上而下的決策，傳達到每一位員工，建立起資訊安全的觀念，就可以減少很多潛在問題的發生。