公務出國報告

（出國類別：實習）

『寬頻網路客戶障礙處理管理資訊系統整合最新技術』實習報告

服務機關：中華電信台灣中區電信分公司

出國人　職　稱：助理管理師

姓　名：賴國榮

出國地區：美國

出國期間：92年9月21日至92年10月4日

報告日期：92年12月24日

系統識別號:C09203973

公 務 出 國 報 告 提 要

頁數: 37　含附件: 否

報告名稱:

寬頻網路客戶障礙處理資訊管理系統整合最新技術

主辦機關:

中華電信台灣中區電信分公司

聯絡人／電話:

呂鳳嬌／04-23442108

出國人員:

賴國榮　中華電信台灣中區電信分公司　資訊處　助理管理師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 09 月 21 日 -民國 92 年 10 月 04 日

報告日期: 民國 92 年 12 月 24 日

分類號/目: H6／電信　／

關鍵詞: DoS,Spoof,High-Availability

內容摘要: 本次奉派赴國外實習，所涵蓋範圍相當廣泛，內容也相當豐富；資訊系統要整體運作很順暢，提供不中斷的服務是很大的挑戰，不僅系統本身，系統管理人員，以及系統運作整體網路環境配合，均是很重要的，因此系統管理人員要充份了解系統及架構，熟稔災害復原程序，平常資料備份與保全，網路資訊安全重視與維護，緊緊相扣缺一不可，茲就其內涵摘要分述如下：第一部份係針對網路系統資訊安全作一概述，網路安全是一切整合資訊系統運轉順利的基石，茲就資訊安全內容、網路攻擊的種類、攻擊方法步驟、及網路攻擊的因應作介紹。第二部份則對寬頻網路資訊安全管理對策作介紹，說明寬頻網路資訊安全與做法、資訊安全管理的關鍵任務、存取控管、帳號管理、單點簽入、用戶端的管理、稽核機制、安全管理等。第三部份則就系統資料備份與保全作介紹，資料是企業最重要資產之一，資料備份是資訊安全的最後一道防線，因此就備份種類、資料備份與回存、資料保全、異地備援、及如何規劃完整備份作說明。

本文電子檔已上傳至出國報告資訊網

目 錄

摘要

本次奉派赴國外實習，所涵蓋範圍相當廣泛，內容也相當豐富；資訊系統要整體運作很順暢，提供不中斷的服務是很大的挑戰，不僅系統本身、系統管理人員以及系統運作整體網路環境配合，均是很重要的，因此系統管理人員要充份了解系統及架構，熟稔災害復原程序，平常資料備份與保全，網路資訊安全重視與維護，緊緊相扣缺一不可，茲就其內涵摘要分述如下：

第一部份係針對網路系統資訊安全作一概述，網路安全是一切整合資訊系統運轉順利的基石，茲就資訊安全內容、網路攻擊的種類、攻擊方法步驟及網路攻擊的因應作介紹。第二部份則對寬頻網路資訊安全管理對策作介紹，說明寬頻網路資訊安全與做法、資訊安全管理的關鍵任務、存取控管、帳號管理、單點簽入、用戶端的管理、稽核機制、安全管理等。第三部份則就系統資料備份與保全作介紹，資料是企業最重要資產之一，資料備份是資訊安全的最後一道防線，因此就備份種類、資料備份與回存、資料保全、異地備援及如何規劃完整備份作說明。

第一章 前言

為瞭解先進國家寬頻網路客戶障礙處理管理資訊系統整合最新技術，加強對資訊系統整合以提供服務不中斷之高服務性，以提高服務品質，經呈總公司核准，奉派赴ＨＰ科技公司美國丹佛、洛杉磯及舊金山等訓練中心實習，實習項目如下：

（１）、寬頻網路管理與資訊系統整合技術
（２）、物件導向語言與資訊系統整合技術
（３）、資訊系統資料庫管理與儲存設備整合技術

本次出國承蒙各級長官協助及ＨＰ台灣分公司之鼎力配合協助，尤其是 Charles Chang、Angel Chen 等幾位先生小姐精心安排課程及各位 Instructors 之熱心指導，使得本次出國實習收穫頗多，謹此表示由衷的感謝。本次出國案之課程及行程如下：

時間	課程
92/09/21（星期日）	去程（台北－舊金山－丹佛）
92/09/22（星期一～三）	研習（丹佛）
92/09/24（星期三）	行程（丹佛－洛杉磯）
92/09/25（星期四～五）	研習（洛杉磯）
92/09/27（星期六）	行程（洛杉磯－舊金山）
92/09/28（星期日）	整理資料（舊金山）
92/09/29（星期一～四）	研習（舊金山）
92/10/03（星期五～六）	返程（舊金山－台北）

第二章 網路資訊系統安全

2・1 資訊安全的定義與內容

資訊安全的範圍，包含網路安全、管理系統安全。網路提供了資訊系統運作的基楚平台，有健全的網路安全，傳送於其中的資料才得以受到保障，整體資訊系統運作才能順暢，提供高度服務。因此對於網路攻擊模式、手段、步驟等須有所了解，進而提出對策予以解決。

資訊安全在保護企業的資訊資產，尤其企業內各網路設備、主機服務系統，避免遭受各種威脅，降低對企業之傷害，進而提昇企業競爭力、增加商機，提高投資報酬率，確保企業永續經營。

資訊安全的重點在於保護資訊及其支援的處理設備、系統和網路的機密性（Confidentiality)、完整性（Integrity）和可用性（Availability)。

2・2 攻擊的種類

攻擊的種類有以下幾種：

(1)木馬程式

藉由侵入或設陷阱的方式，將後門程式(特洛伊木馬）送入對方伺服器中。

(2)電腦病毒

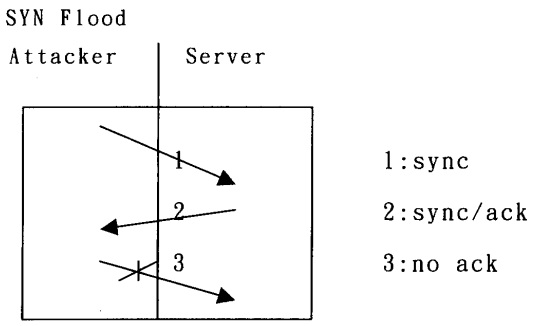
將有毒程式檔案資料，透過各種途徑如上網、電子郵件傳送等方式散播各種電腦病毒。

(3)封包攔截

利用執行監聽程式，捕捉在網路上傳遞的網路封包訊息資料，加以分析獲取有用資訊，就叫做 Sniffing（封包攔截）。

(4)DoS

Denial of Service 阻斷服務，藉由 OS 作業系統漏洞或 AP 應用程式的設計疏失，不斷送出無效資料進行攻擊，癱瘓目的主機或網路，使其無法正常提供服務，直到服務停止。例如 TCP 的 Three Way Handshaking，要建立一個 Connection，Client 端發出 Sync，而 Server 端發出 Sync/Ack 回應，等待 Client 端回應，但是攻擊的 Client 端就此停住不予回應，藉此消耗主機資源，若是此種攻擊大量發送封包，不多久系統資源耗盡，系統服務也就終止了。



DoS 攻擊可分為三種：

- 利用 TCP/IP Implementation Bug
  像 Ping of Death 在各 fragment 中夾帶其資料，當 packet 到達目的地，經由重組(Reassembly)後，它就產生攻擊威脅。
- 利用 TCP/IP Implementation Weakness
  此類攻擊像 SYN Flood，利用 handshaking 的過程，不回應 Ack，造成伺服主機的等待，若依此大量發送，將造成主機 Queue 的爆滿而中斷服務。另外 Land 攻擊，攻擊者送出大量 sync 封包，並

同時假冒 Source IP Address 為目標主機的 IP Address，使得目標主機自己回應(Response)到自己，而造成系統的無法使用。

暴力攻擊使網路塞滿沒有用的資料

它是網路頻寬攻擊，像 Smurf 利用 IP 定義的 broadcast addressing 攻擊，很快就把目標主機或網路擠爆。它發出 ICMP echo request 封包(ping)，並且把 destination 設定為網段的 broadcast address，造成路由器對該網段內的所有主機作廣播。若該網段內所有主機數目很多，大量 ping 要求及回應的封包，將擠滿整個網路。更有甚者，若是同時假冒來源 IP Address，那麼 ICMP 封包將去塞滿該被假冒 IP Address 的網段。

(5)Scan

掃描網路，搜尋網路上的可著力點，更有甚者可做破壞性的掃瞄。

(6)IP Spoofing

網址假造，假冒 IP Address，修改 Source IP Address，以隱藏入侵者自己。甚至假冒 IP Address 配合其它攻擊手段，讓目的主機或網路癱瘓。

(7)Social Engineering

社交工程，藉由與人員的社交活動接觸，以獲悉相關訊息。

2．3 攻擊方法與步驟

(1)尋找目標

知己知彼百戰百勝，為達到網路系統攻擊入侵，首先須尋找目標。方法有：

•網路列舉：連絡人、DNS 記錄查詢及 Zone Transfer…

・路徑勘查：traceroute…。

・收集相關的資訊：像公司名稱、電子郵件信箱、網頁、營業項目、股票資訊…。

(2)掃描網路

找出那些主機是存活的、提供了那些服務，以找出可能的攻入點。方法用 Ping，找出存活的主機；掃瞄 TCP、UDP 通信埠；ICMP 勘查，獲取更多系統資訊。

(3)列舉資源

了解目標網路架構及脆弱之處，利用 Windows 網域，使用者與群組 nbtstat、WFP、finger，作業系統偵測 nmap、xprobe 等，以了解目標主機是那一種作業系統，中間是否有防火牆擋住，目標主機的開關機時間，提供了那些服務，是那一種服務軟體及版本，最終目標就是主機的弱點，接著就是想辦法要獲得存取。

(4)入侵伺服器

獲得存取目標系統的能力。

利用未更新的伺服器軟體瑕疵，有瑕疵的 Web Application 輸入驗證，由 netBIOS 資訊進行密碼猜測，不當的設定與危險的預設安裝，SNMP 資訊及預設的 community string 等。

(5)入侵網路設備

獲得存取目標網路的能力。

方法有不安全的預設密碼，包含 telnet、Web 界面登入及 SNMP 的 community string 等。RIP（Routing Information Protocol）v1 沒有認證機制，而 v2 只有簡單的認證機制。

(6)入侵客戶端

存取目標客戶端的能力，客戶端通常因為缺乏防禦，

很容易得手。方法：

- 未受到保護的資源分享，暴力嘗試。
- 直接攻擊暴露出來的客戶端系統。
- 間接攻擊有瑕疵的瀏覽器(IE)、郵件軟體(OE)。
- 間接攻擊有瑕疵的多媒體播放軟體(WMP)。
- 透過瀏覽器竊取登入資訊(Cookie、Password)。
- 透過不安全瀏覽器存取檔案(IE)、安裝後門。

(7)獲得存取

利用一般性的軟體弱點及人員鬆散設定管理，讓入侵者有機可乘：

- 利用軟體弱點 Buffer Overflow、Format String、Race Condition、Input Validation。
- 預設的安裝，有些項目目前是尚未使用到。
- 預設的密碼未經變更，讓人很容易就猜測到。
- 不嚴謹的存取控制。

(8)權限提升

經由獲得存取後，就提昇其在目標主機設備中的權限，以供後續對系統的整體控制，以達到其最終目的。方法：利用本機軟體弱點，提升到 Administrator 權限，透過欺騙或木馬程式，盜取管理帳號密碼，取得密碼檔，對管理帳號進行密碼破解。

(9)入侵其他系統

獲得其他系統的存取權限。

方法：透過信任關係，染指整個網域；列舉內部資源，對內部主機進行入侵。

(10)網路竊聽

由竊聽資訊進行後續入侵動作。

方法：透過網路竊聽盜取密碼或密碼雜湊；透過竊聽收集內部資源資訊、取得機密資訊；利用 spoofing

進行攻擊。

(11)竊取有價值資訊

獲得有價值的資訊，通常這也是入侵者最主要的目的之一。

方法：搜尋目標系統的儲存裝置。

(12)安置後門

入侵者為了日後能長期繼續控制目標設備，一個系統有時可能被安置不只一個的後門，以保障入侵者能繼續控制，這也是入侵者的主要目的之一，另外亦可能成為加害其他受害者的跳板。方法：

- 建立一般看似正常的帳號。
- 利用排程服務，如 cron、at 啟動額外程式。
- 變更啟動程序，如 rc 或 Startup Folder。
- 加入額外的服務，如 vnc 進行遠端控制。
- 利用系統既有的服務，如 remote.exe。
- 安裝鍵盤敲擊記錄器，記錄其輸入過程資料。
- 安裝監控程式－可能利用合法通道進行，如使用 ntdaddy.asp。
- 安裝其他後門或木馬，如 ntrootkit、lkm、rootkit、netbus。
- 使用隱藏工具，隱藏檔案、執行中的程序、進行中的連線－通常以後門的形式。

(13)掩蓋蹤跡

隱藏入侵的事實，煙滅證據。刪除或修改各種系統記錄檔：messages、utmp、temp、lastlog、.history、入侵偵測記錄、Web 存取記錄、檔案傳輸記錄。

此時入侵者已經完成整個入侵動作，完全掌握目標網路，控制目標系統，清除所有可疑記錄，建立長期控制機制。如果未能達成目的，還有另一阻斷服務的手

段－DoS & DDoS攻擊。

以上說明了駭客及入侵者對網路攻擊的方法與步驟。了解網路攻擊的步驟，可以預先防患截斷其可能的步驟，使其無法入侵，或入侵者無法再擴張。了解網路攻擊的結構，可以分析網路安全部署的問題，並加以補強。了解網路攻擊的手法，可以在適當的時機，以適當的工具應變。因此我們應當有一些作法，以資因應處理。

2・4 網路攻擊的因應

(1)設立監測工具

以便能找出入侵的事實，當入侵事件發生時能迅速反應。如門禁、登入限制、入侵偵測、記錄檔、錄影、安檢、稽核、證據保存等等。

(2)建立危機處理小組

・負責人員。

・系統管理人員。

・外部協助窗口：稽查人員、檢調人員、法律顧問。

(3)建立應變計畫

・監測工具的使用及其他可用資源。

・危機處理小組及可供諮詢的協助。

・當下的處理方式使能快速反應。

・證據保存及過程記錄供未來參考。

・系統災害復原計畫。

・將這個應變計畫放在一個安全且容易取得的地方。

(4)當下的因應對策

・能否研判入侵者類型，以找出相對應較佳的對策。

・切斷或是保持連線。

・追蹤、誘捕。

(5)應該準備的監測方式

- 事前

  良好的 Access Control List，包括資源及防火牆；良好的稽核記錄，安全測試計畫，輔以弱點測試工具，為你找出可能的弱點。

- 事發時

  須要一套能夠記錄網路封包的工具;能及時監控系統狀態的工具或能夠將系統記錄轉移到另一台機器的方法。

- 當下的應變方式

  入侵仍在進行中，持續的記錄與監控，是否能找到技術專家及檢調人員的支援？檢討持續入侵的原因，是否改變因應對策？

- 事後

  從記錄中分析可能的真實狀況，以確認入侵或遭受災害情形。

(6)從入侵者特徵分析其可能行為

- 對於外來的破壞狂而言，入侵只是為了破壞，最可能造成的結果是毀損系統，那麼及時阻斷可能是最好的應變方式。
- 對於商業間諜而言，目標設定在取得祕密的資訊，那麼引導到假的機密文件可能是不錯的誘餌，能增加誘捕的機會。
- 對於內部的使用者，目的可能是窺視或毀損資料，那麼備份可能的目標檔案並啟用稽核記錄，靜靜的進行蒐證可能是較佳的應變方式。

第三章 寬頻網路資訊安全管理對策

眾多的保全,並不能百分之百確保企業安全,輔以良好的資訊安全管理才可以確保企業更安全。從強化企業內部安全，Client 端安全管理著手。

3．1 未來我們所面臨的安全威脅包含

(1)病毒、Worm 攻擊將更快速、更具破壞力、影響程面及範圍更大。

(2)駭客攻擊的手法趨於多樣化及混和型的攻擊。

(3)阻斷服務攻擊手法更先進、更具破壞力、影響程面及範圍更大。

(4)安全漏洞增加的速度更快，修補時間縮短。

(5)駭客攻擊目標轉向企業內部的個人電腦及利用寬頻上網的個人電腦。

(6)具破壞力的工具被公開，且取得容易。

(7)攻擊後，資訊被竊聽與敏感性資料外洩，被有心人士利用而造成損失。

(8)無線網路與基礎網路成為下一波攻擊標的。

3．2 資訊安全管理的關鍵任務

(1)惡意碼與惡意攻擊的辨識困難。

(2)垃圾郵件激增。

(3)與組織任務無關的電子郵件行為。

(4)機密資料的外流。

(5)永遠不足的網路頻寬。

(6)不當的網路站台瀏覽與逛網行為。

(7)無限制的網路行為降低生產力。

(8)電子犯罪的證據蒐集困難。

(9)系統弱點的管制與補強耗費時日。

(10)與日俱增的網路安全管理問題。

(11)各項主機安全稽核報表提供困難。

(12)病毒常透過網路媒介在組織中流竄。

(13)各項主機系統資料 Log 檔案龐大不易讀取分析。

3．3 目前環境中的資訊安全

攻擊的主要目的是檔案與資料竊取、檔案與資料竄改與檔案與資料毀損。經由未經授權之違法存取、違法使用，以最高權限管理員、特定身分使用者身份欺騙，利用建置時的弱點、設計時的弱點或安裝設定時的弱點給予有機可乘。內部主要的威脅為拒絕服務攻擊、實體攻擊、不良的安全管理、錯誤或是不良的網路架構、人員之疏失等。

3．4 存取控制

3．4．1 開放系統安全漏洞

(1)Superuser 的超級授權，如 Unix root 及 NT administrator 使用者。

(2)使用者 ID/Password 設定檔容易竊取，如 Unix /etc/passwd。

(3)檔案存取權限設定過於簡陋，如 Unix 之 owner、group 及 others。

(4)使用者授權設定管理不易，不同系統則有不同的管理方法。

(5)違反系統安全規定事件，沒有即時警訊。

3・4・2加強存取控制功能

(1)Superuser 控管

限制及管理 root 權限，可防止使用者變換身份(su)以侵入系統的行為，並提供稽核記錄。

(2)帳號/密碼安全控管

帳號密碼應妥善保管，提供圖形及命令列介面，方便快速的建立、更改、刪除。密碼依安全規則設定，至少六碼以上、英文數字及特殊符號混用，一段時間後強制更改密碼且不得與前幾次相同。

(3)系統資源安全控管

- 依照 Rule-Based 控管，以 What/Who/How/When/Where 規則制定 rules，控管所有系統資源，包含檔案、應用程式、device file、Host、TCP、Processes、Daemons 及稽核記錄。
- 依照日期及時間條件，管制檔案增加、刪除、讀出、寫入之允許時段。
- 攔截每個檔案開啟的要求，決定使用者是否有足夠權限存取該檔案。
- 保護重要 Process/Daemons，不被惡意或失誤停止。

(4)網路/登入安全控管

- 根據終端機、使用者、特定日期時間等，管制使用者進入系統。
- 設定是否允許使用同一使用者名稱簽入(Login)，並且可設定此使用者名稱同時連線的數目。
- 對以終端機模擬方式連線的使用者加以管制與稽核。

(5)集中安全管理功能

由中央控管所有伺服器，或將管理權限下放交由各部門、群組管理員。

3．5使用者帳號管理

由於不斷成長的內外部使用群與太多種類的主機及應用系統，員工轉換部門，員工流動率高等，使得使用者帳號管理愈形複雜，不易管理。

3．5．1加強帳號管理的安全

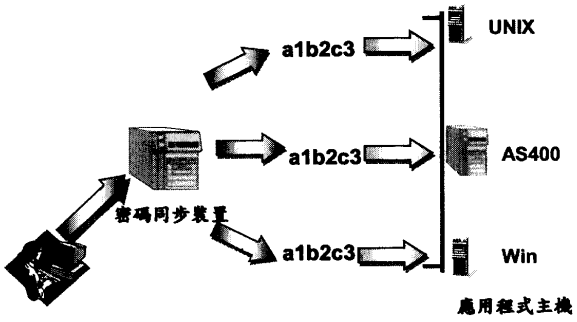
- 依據工作執掌自動產生帳號於不同系統。
- 使用者擁有正確的帳號及適當地權限。
- 與工作無關的帳號確實地被移除。
- 員工離職帳號確實地被移除。
- 帳號統一集中控管。
- 降低管理成本。

3．5．2單點簽入 (Single Sign On)

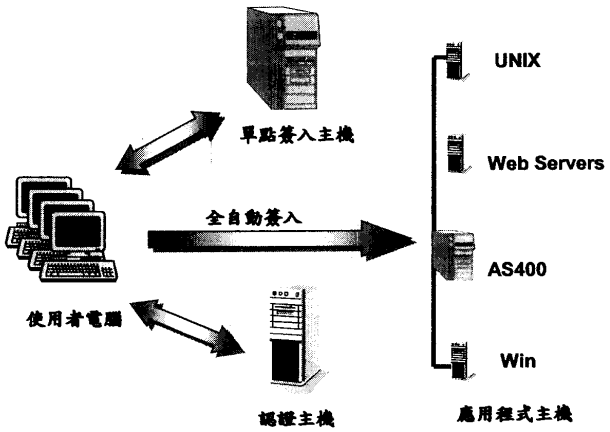
(1)密碼同步

由於系統越來越多，有太多密碼需要記憶，因此有單點簽入密碼同步的設置，但此種方式進入各主機的密碼均相同，也是有它不安全的地方。

密碼同步



安全的單點簽入



(2)安全的單點簽入

單點簽入，加上認證主機配合，以強化認證（Authentication）作業，提高安全性。

(3)認證的方式

- User ID & Password。
- Tokens
- SecureID
- Smart Cards
- PKI certificates
- 特徵辨識：指紋、聲音、瞳孔、臉部、掌紋、手寫筆跡的識別。

(4)單點簽入的好處

- 中央統一管理，利於安全稽核作業及報表。
- 符合現行 Web Services 作業方式。
- 降低企業資訊擁有及管理的總成本(TCO)。

3．6企業用戶端資訊安全管理

使用者端經常面臨的威脅來源，有 Hacker、DOS、DDOS、Virus、Worms、Web Services、E-Mail、非法存取資料、安全控管漏洞、系統漏洞等問題，因此若能就其設備等加以自動化管理，對於整體資源的安全、運用、控管等將有莫大的助益。

3．6．1用戶端設備管理問題

- User 數目多，PC 分散不易管理。
- 當系統異常、軟體安裝升級需求、中毒掃毒處理、軟體使用異常等，常須要 IT 人員協助處理。
- Hostname、IP 管理。
- 帳號及密碼管理。

- 作業系統安全管理漏洞。
- 行動設備(Notebook、PDA、Wireless)普及，管理不易。
- 行動儲存裝置普及(燒錄機、磁碟片、行動碟等)，外部資訊設備進出容易。
- 非法使用軟體。

3．6．2 用戶端自動化資產管理

- 自動化清點企業內主機之硬體、軟體設備相關資訊。
- 列出企業內資產相關資訊。
- 硬體/軟體資產資訊報表。
- 資產異動警訊。
- 軟體版權控管。
- 報表/管理。
- 軟體資產清單。
- 那個使用者正在使用那些軟體以及其使用頻率。

3．6．3 用戶端設備管理自動化好處

- 監測資產、狀況異常。
- 作業系統 Hot Fix、Patch 同步升級。
- AP 同步化，版本、修補程式的一致。
- 病毒碼、掃毒引擎自動更新。
- 監測異常 Hostname、IP 管理。
- 監測異常自動通知管理者。
- 提供更精準的資產資訊。
- 易於稽核用。
- 減少非法軟體使用，減少潛在威脅。
- 偵測系統漏洞，以供加強修補，減少安全漏洞。
- 偵測病毒碼版本、強化更新，減少中毒機率。

・降低管理成本。

3・7安全管理解決對策

安全管理解決對策，可以由以下幾方面來處理。

3・7・1網路威脅防護管理

・防火牆，以區隔信任、DMZ、不信任區域，配合 Access Control List 的 Policy，以控管封包進出。對於各 Port 進出基本上先 Block 掉，再依需求打開特定的服務，以確保安全。

・防毒系統，建立防毒機制，減少資料受到病毒感染。

・入侵偵測系統，建立防駭安全網，即時辨識分析駭客入侵的攻擊，依控制規則，限制網路服務。

・傳送內容檢測，依特定字句過濾預警，自動攔檢告發不當收發信件，攔截有損生產力的垃圾郵件，列出前十大 Mail 用戶，對特定網頁可做 Block 或 Monitor。

・用戶網路流量調查，即時通訊頻寬使用分配。

3・7・2主機安全控管防護

・定期與不定期做主機弱點的掃瞄，找出弱點所在，並提供弱點修補，強化安全。

・主機存取控制，詳細記載主機存取紀錄，經由前述的權限適當授予及帳號控管，Log 存取記錄分析，了解主機存取之適當與否或異常發生。

3・7・3 Client端設備管理

・弱點偵測，定期與不定期做主機弱點的掃瞄，找出

弱點所在，通知加強修補，以確保安全。

- 加強存取控管，對螢幕應設定保護程式密碼。密碼不應該自動記憶在電腦設備上，以防他人的盜用。
- 導入 CMS（Client Management System）系統，針對 Client 端作業系統或應用程式未做 Hot Fix 或未上 Patches 者列管，通知改善，必要時阻斷其上 Internet。
- 全體納入防毒體系，依規定做好防毒工作。嚴禁將家裡等外接設備私自接入 Intranet 上。
- 依特定規則預警，查核過量的網頁瀏覽。
- 自動過濾或分級限制存取有礙生產力或不良網站。
- 分時分級禁止規則，某些時段才能上網或不能上網。
- 列出所有用戶使用網站資料量排行榜。

3．7．4 資訊安全稽核機制

當攻擊者是合法使用者時，其所為的存取資訊作為，就更需要藉助稽核機制來監督其行為是否符合安全政策規範。其範圍有：

(1)安全事件監控。

(2)定期與不定期對資訊安全作稽核。

(3)提供未符合預定安全政策之主機名單。

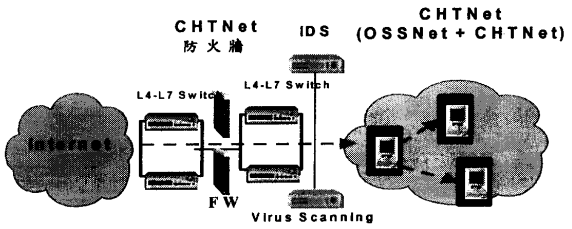
(4)各種具有法律依據的分析報表與事件還原機制。

3．8 本公司寬頻網路資訊安全與作法

(1)寬頻網路資訊安全

寬頻網路資訊安全是目前一大工作重點，使用雙網卡容易受到入侵攻擊，以本公司現況為例，目前 OSS 網路與公司內部企業網路 CHTNet 並未做隔離，OSS 網路的管理，有時經由 CHTNet Client 端以雙網卡的方式作業，有些 OSS Server 仍有需要與 CHTNet 其他資訊系統間做資料的交換傳送，因此將整體網路暴露在更高的風險中。當 CHTNet 網路受到駭客攻擊或病毒入侵（像 SQL Slammer），若沒有適當的阻隔，OSS 網路也將受到波及；若 OSS 網路受到入侵攻擊，由於雙網卡的使用，CHTNet 也將容易受到攻擊，而危害到整體企業資訊安全。因此將二者採取隔離是有其必要的。

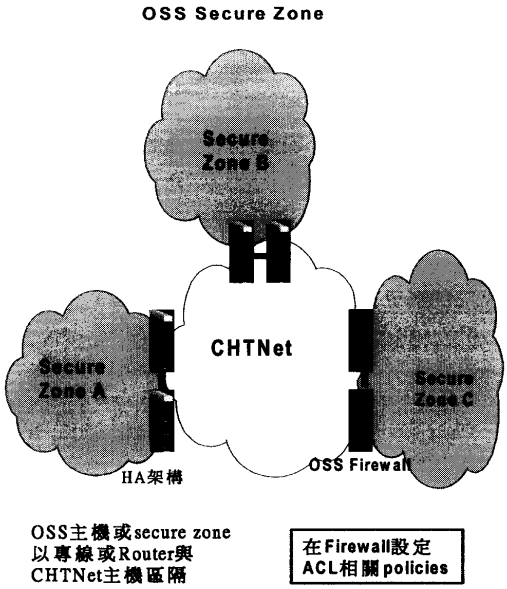
駭客攻擊病毒感染途徑



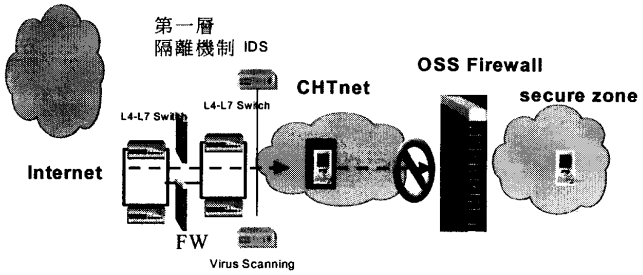
(2)安全作法

OSS 網路與 CHTNet 網路依存度高，為達到二者間更高安全性，可用下列方法：

- OSS 可形成 Secure Zone 方式，以減少與 CHTNet 之通道。
- 設置 OSS 防火牆，以加強與 CHTNet 網路通道之控管，利用 Firewall 以分隔 OSS 網路與 CHTNet 網路。
- 建立統一的安全控管機制，加強防火牆的 Access Control List（ACL）、頻寬管理，以管制使用通道，並訂定各 OSS 系統之駭客入侵的標準作業程序(SOP)，增進安全。



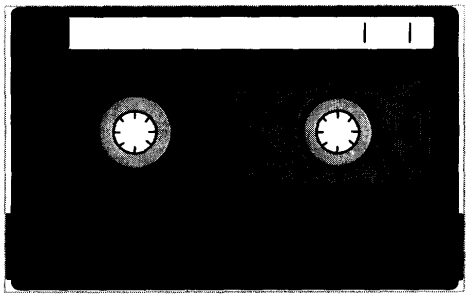
OSS Firewall隔離



第四章 系統資料備份與保全

4・1 系統資料備份

Backup提供企業資訊的保護及可取用性，提昇企業生產力。系統管理人員的職責之一就是系統資料備份，我們的資料面臨潛在威脅，由於災難或不可預期事件的發生，例如火災、颱風、水災、暴風雨、地震等天然災害或硬體設備的損壞、檔案系統的損壞、人為疏失檔案不小心誤殺或覆寫、電腦病毒入侵、硬碟資料毀損、停電、不滿的員工、網路駭客、恐怖活動等，都是造成資料毀損遺失的原因，因此如何讓資料損毀減至最小，讓使用者能夠信任、使用得愉快，提供穩定的服務，那麼備份是不可或缺的。全球每年因資料損毀，造成的損失高達美金數十億。當一個系統開始運作時，它的備份策略就應該擬定並且已經準備完成。



Backup是防止資料毀損的第一個步驟!

4・2 須要備份那些

4・2・1備份的作法可以是

(1)備份整個檔案系統或資料庫系統（Full Backup)。

(2)備份部份檔案系統或資料庫系統。

- 從上次備份點以後有改變的部份（Incremental Backup）。
- 一個檔案系統的次部份(Subtree of a File System)。
- 應用資料。
- 使用者資料。

(3)備份資料庫系統設定資料（Configuration）。

(4)備份系統開機設定資料（Configuration）。

4．2．2 Full Backup（完全備份）

完全備份是將根目錄下所有檔案及次目錄下檔案一起備份，資料庫則全部備份，在理想的環境中，Server應該作完全備份(full backup)。經常變化的重要資料文件和目錄，應每天備份，甚至是一天備份多次。基於安全的考量，Server在更新應用程式或更換硬體前後，必須執行一次完全備份。然而在一個大的系統中每日均作完全備份是不實際的：

(1)完全備份可能花費時間太長，也許一個晚上到次日上班時都還沒有完畢。

(2)完全備份未必所需，File Server上的大多數檔案均很少更改，有些檔案系統像是/tmp 、/cdrom等就不必包含進來。你可以仔細挑選評估，將必要備份的選擇進來，如此可以大大減少備份量。

(3)除了檔案系統與目錄外，也需要一些特別的程序，將資料庫系統及設定備份下來，最後系統開機程式設定也應一併備份下來，否則當系統毀損無法開機，此時該備份就是救星了，系統開得起來，資料備份也才倒得回去。

4・2・3 Incremental Backup（增量備份）

從上次備份點以後，針對有改變的部份加以備份。能更有效率地使用儲存媒體，只需要較少的資料儲存空間，相對的備份需要的時間較少。但災難復原時需使用多個媒體完成，回復需要更長時間。而且回復時媒體必須按照正確順序回復，才能將系統復原。

4・3 須要多久備份一次

要問這個問題，精確的說應是『多少的資料您經得起漏失？』評估應用程式在系統上之執行及用戶對於資料使用性的需求度，這可以引導出資料須要多久備份一次。以下因素可供考慮其備份頻率：

(1)檔案內容的改變是否很頻繁？

(2)檔案內容是否極其重要？

若說你能忍受一個月的資料漏失，那麼一個月備份一次也就夠了，若能忍受四個小時的資料漏失，那麼四個小時就應備份一次。就一般應用而言，每週作完全備份，而每天作增量備份是實際可行的。你應該建立一份對於系統備份的時程表，內容描述多久做完全備份及增量備份，而且在系統離峯比較少人作業時執行之。備份分級（Backup Level）是用來定義不同的備份程度方式之一。

4・4 資料保全

基於方便使用，備份的資料經常是存放在與機房同一個房間或同一棟建築物內，這樣雖然方便於資料拿取，但它其實是暴露在一個不可預期的風險中。一旦發生水災、火災、地震或類似 911 恐怖攻擊行動等災害，造成系統與資料同時在一個地點均毀損，那麼損失是無法估計的，甚者造成公司的倒閉是可能的。

安全的作法

(1)不同的資料備份存放到不同的地點，基本上應在不同的安全區域內。

(2)資料備份應標示完整清楚，包含下指令的參數等資訊、應有完整的備份策略、詳細載明日期、時間、方法。

(3)磁帶應避免潮濕及日曬，並應考慮水災、火災、風災、地震及避免失竊。

(4)磁帶有其一定的生命週期，應加註 Label、起始使用日期、有效期限等，並按預定表依序循環使用。

4・5 備份例子說明

假設有如下的備份排程（Schedule）：

- 每月月初，備份全部。
- 每星期五，備份月初以來有修改的部份。
- 每天，除了星期五以外，備份上星期五以來修改的部份，或備份月初以來修改的部份，（視二者何者先發生）。

就以上情形來說可用三種分級來處理該備份，分別是每月備份、每週備份及每日備份，每月月初，做完全備份（Full Backup），其他則做增量備份（Incremental

Backup)，至於每週備份及每日備份，可用備份分級（Backup Level）來加以區分並完成作業，你可以定義十個備份分級(Level 0~9)，Level 0 是完全備份，Level 1 至 9 是增量備份，系統的備份策略則依應用系統作業情況、資料量、作業時間及儲存媒體等而決定。

4．6 資料回存

僅管資料均依預定的程序做好備份，但是一旦系統等發生問題，必須將資料回存到系統，不管是回存作業系統、系統檔案或資料庫系統資料等，則是另一個重要的議題，問題發生時是否很清處知道要回存的備份資料在那裡，資料可以讀出來否？回存備份資料的程序如何？要下的參數正確否？在在考驗系統管理人員沉著的應變處理能力，系統管理人員平時應經常演練，對於備份資料時也應確認是否作業完成、備份是否正確。一旦問題發生時不慌不亂，依預定的回復策略程序，按步就班一步一步的處理，如此才能不慌亂而於最短時間內將系統重新建置回復完成，繼續提供系統的服務。

4．7 資料備份回存例子－分三個Backup Level

如上述每月每週每日的備份例子中，為了實作它的備份，用了以下的備份分級：

Level 0：每月完全備份

Level 1：每週星期五備份

Level 2：每日備份，除了星期五以外

以下表格說明實作該例子的備份 Level

每月日期	1	2	3	4	5	6	7
每週星期	Sun	Mon	Tue	Wed	Thu	Fri	Sat
備份 Level	0	2	2	2	2	1	2

每月日期	8	9	10	11	12	13	14
每週星期	Sun	Mon	Tue	Wed	Thu	Fri	Sat
備份 Level	2	2	2	2	2	1	2

每月日期	15	16	17	. . .	. . .	31	1
每週星期	Sun	Mon	Tue	. . .	. . .	Tue	Wed
備份 Level	2	2	2	. . .	. . .	2	0

若資料於第 11 日毀損，你將使用下列的順序將資料回存到 10 日星期二備份的狀態：

(1)回存月初 1 日星期天的完全備份。

(2)回存第 6 日星期五每週的增量備份。

(3)回存第 10 日星期二每日的增量備份。

4．8 資料備份回存例子－分二個Backup Level

如上述每月每週每日的備份例子中，為了實作它的備份，用了以下的備份分級：

Level 0：每週完全備份

Level 1：每日備份，除了星期五以外

以下表格說明實作該例子的備份 Level

每月日期	1	2	3	4	5	6	7
每週星期	Sun	Mon	Tue	Wed	Thu	Fri	Sat
備份 Level	0	1	1	1	1	1	1

每月日期	8	9	10	11	12	13	14
每週星期	Sun	Mon	Tue	Wed	Thu	Fri	Sat
備份 Level	0	1	1	1	1	1	1

每月日期	15	16	17	．．．	．．．	31	1
每週星期	Sun	Mon	Tue	．．．	．．．	Tue	Wed
備份 Level	0	1	1	．．．	．．．	1	1

若資料於第 11 日毀損，你將使用下列的順序將資料回存到 10 日星期二備份的狀態：

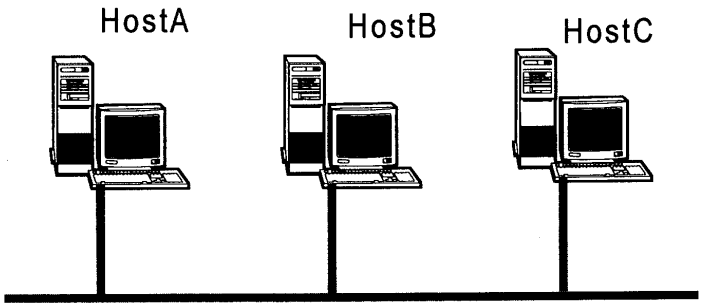
(1)回存第 8 日每週星期日的完全備份。

(2)回存第 10 日星期二的每日增量備份。

4．9 網路資料備份與回存

當本地系統沒有磁帶機以供儲存備份資料時，就必須利用網路，用 SAN 或 NAS 做資料的異地備份，或直接利用網路備份到遠端主機系統的磁帶機。

以下例子中有三台主機，其中只有 HostA 有磁帶機，而 HostB 及 HostC 則沒有磁帶機，必須備份到 HostA 磁帶機。



為了能讓 HostB 及 HostC 兩台主機資料寫入 HostA 磁帶機，必須於 HostA 主機上產生一個名叫 ~root/rhosts 的檔案，檔案內容必須包含 HostB 及 HostC 兩台主機，如此 HostB 及 HostC 才可以存取到 HostA 磁帶機。

.rhosts 的內容如下：

```
HostA# vi ~root/.rhosts
        HostB
        HostC
```

當 HostA ~root/.rhosts 產生後，HostB 及 HostC 就可以存取到 HostA 磁帶機，做資料的備份。

```
HostB# fbackup -f HostA:/dev/rmt/0m -u0g graph -I
index
HostC# fbackup -f HostA:/dev/rmt/0m -u0g graph -I
index
```

where

-f 目的輸出設備

-I 產生索引檔

-u 異動 /var/adm/fbackupfiles/dates 檔案內容，以記錄那個 graph file 及何時被使用過。graph 是一個檔案名稱，它包含要被備份檔案的名稱及其目錄資料。

僅管 HostB 及 HostC 可以備份資料到 HostA，但同一時間只能有一個使用者使用磁帶機，不能兩個同時使用它。同樣的，當資料要回存時，也可以透過網路方式回存，指令如下

```
HostB# frecover -f HostA:/dev/rmt/0m -rv
HostC# frecover -f HostA:/dev/rmt/0m -rv
```

Where

-r recover everything on a backup volume

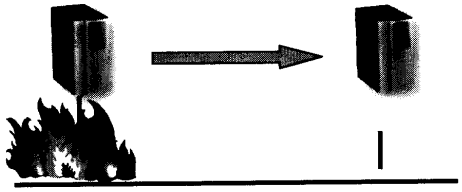
-v verbose

4・10 資料複製

應用程式(資料庫)主機每年的成長，每台主機每一年的資料量成長，電子商務、公司內部網路、IT管理系統都需要24x7的運作效率，因此提高資料的高可用性乃當務之急。

(1)不停止的高可用性

一個能夠提供自動且高效率的將資料複製到第二台備援的主機上，並能在主要服務主機發生問題時自動將服務轉移至備援的主機，提昇資料的容錯功能。



(2)資料的高可用性方案

- 硬體解決方案可用 Redundancy (UPS，ECC memory)、Replication (RAID，Mirroring)。
- 軟體解決方案可用 Replication、Server failover、Clustering。

(3)High-Availability

即為整合硬體及軟體使資料的使用性更具安全性及延續性的解決方案，保持最新的資料於備援的主機，保持企業重要的伺服主機正常運作。

4・11 異地備援分類

依災難發生時備援處理的優先順序，備援程序希望達到的回復時間(Recovery Time Objective)、以及資料

的回復點(Recovery Point Objective)，可將備援分為三類。

(1)第一類是專屬系統熱備援

對於重要對外服務的系統，在異地備援中心，除了須同步資料的更新，另外須備妥提供服務的同機型備援主機群(AP Server)，及資料庫伺服器(DB Server)。一旦災難發生就可以馬上切換到備援中心，由備援中心主機接替提供服務。

(2)第二類是異地資料同步備援

平時系統資料(含作業系統、檔案系統及資料庫系統)同步複製到遠端異地備援中心，在遠端異地備援中心提供可彈性調度的備援主機供使用。

(3)第三類是批次資料定期備份

平時利用伺服器所提供的自動定時備份功能，以批次方式，定時將資料拷貝至遠端異地備援中心。

4．12異地備援網路架構

異地備援中心，可以採用 SAN(Storage Area Network)架構，將原本分散於各系統的直接存取空間(Direct Access Storage)內資料，集中到 SAN Storage，以收好的效益。例如空間的管理、運用、維運作業，能統一集中管理、彈性運用、節省人力、達到集中化，並透過 Host-based、Network-based 及 Storage device 方式，可以將儲存空間跨越不同廠牌實體裝置，以達到邏輯的儲存空間。

4．13異地備援解決方案

依照遠端資料鏡射(Remote Mirror)及資料複製(Remote Replication)所用的技術，異地備援解決方案可分為以下四類：

(1)應用程式等級類(Application based)

此為傳統以資料庫廠商所提供的遠端資料複製(replication)工具的備援方式，須對個別主機做資料複製機制之組態設定，無法跨越異質資料庫平台。

(2)主機系統軟體等級類(Host based)

此種備援方式必須在每部被納管的伺服主機加裝Volume Manager及Volume Replicator管理程式。

(3)儲存設備等級類(Storage based)

由儲存設備廠商提供的備份軟體，符合SAN Storage備援，是目前異地備援主要技術。為了系統備援的速度、穩定度、整體效能，一般會採用此技術。

(4)儲存伺服器等級類(Storage Server based)

它是介於Host based及Storage based間的產品，提供異質儲存設備虛擬化的功能，但將每部Server的磁碟管理軟體集中在一台Storage Domain Server，同時扮演資料備援時對外Gateway的角色。當伺服器本身受到病毒感染或受到攻擊，或資料傳輸量伺服器本身處理能力無法負荷時，就會產生瓶頸，這將對整體備援產生重大影響。

4．14如何規劃完整備份

一份周全的備份計劃應力求詳盡，包含各個應考慮到的層面與因素，例如了解您的網路環境，資料的重要性，資料系統回復的迫切性，資料的回復點忍受度，確

定要備份的伺服器及資料型態，欲備份的資料量，了解您的備份時段及時間，備份的方式架構，決定硬體、軟體規格，異地備援中心選擇的考量，災難復原重建計劃等等；同時最重要的一點是演練，演練，再演練，以確保資料能有效、正確的回存並重建完整，以提供繼續的服務。

第五章 心得與建議

資訊系統要整合運作很順暢，提供不中斷的服務是很大的挑戰，不僅系統本身，包含系統管理人員，以及系統運作環境整體配合等均是很重要的因素，因此管理人員充份了解系統架構，熟稔系統災害復原操作程序，平常資料備份與保全，網路資訊安全維護與重視，緊緊相扣缺一不可。網路安全是一切整合資訊系統運轉順利的基石，對於網路駭客攻擊入侵方法與步驟的充份瞭解，將有助於網路系統入侵的因應處置及資訊安全的防護，進而對寬頻網路資訊安全採取機極作為與管理，並採取對策，諸如有關管理的關鍵任務、系統安全漏洞的修整補強、使用者帳號管理、加強存取控管、使用者單點簽入、用戶端的加強管理、稽核機制的啟用等，均是相當重要的項目。再者，資料是一個企業重要的資產，資料備份則是企業資訊安全的最後一道防線，因此規劃一份完整周詳的備份作業，做好異地備援工作，管理人員恪遵備份的規則，才能確保企業資訊安全，立企業於不敗之地。

若公司全體人員朝此目標前進，則整體系統高效能的運轉，提供良好的服務當可實現。公司訂定資訊安全最高指導政策（Policy），在此政策下有關網路系統安全的規劃、管理權的訂定、系統安全規則、實行計劃步驟、用戶 Client 端設備使用存取管理等，全體同仁依此安全政策共同遵守，創造一個網路資訊安全的環境，則運作其間的系統，亦較無後顧之憂，節省

人力、物力的大量投入，進而提高系統的服務度，為企業帶來較高的競爭力與商機，為公司股東員工創造三贏，獲致更高報酬利潤。