行政院及所屬各機關出國報告
（出國類別 ：實習）

「資料中心(IDC)備援服務新技術」報告

服務機關： 中華電信股份有限公司
數據通信分公司
出國人 ： 職　　稱　　姓　名
副工程師　　陳俊賢
出國地點： 美國
出國期間：92 年 11 月 30 日 92 年 12 月 13 日
報告日期：93 年 02 月 12 日

系統識別號:C09204906

公 務 出 國 報 告 提 要

頁數: 18　含附件: 否

報告名稱:

資料中心(IDC)備援服務新技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

陳俊賢　中華電信數據通信分公司　公眾數據處　副工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 11 月 30 日 -民國 92 年 12 月 13 日

報告日期: 民國 93 年 02 月 12 日

分類號/目: H6／電信　H6／電信

關鍵詞:　IDC, 異地備援, 資訊安全

內容摘要: 在政府訂定相關分級異地備援之要求下，近來陸續有許多政府機關執行異地備援之專案，在異地備援的服務中，國外目前的趨勢如何，有何新的技術或新的服務內容，IDC業者應該伴演什麼角色，在本出國實習報告中，將提一個建議方向與策略方法。整體的異地備援若僅只於傳統的資料備份、系統備援與網路切換是不夠的，現在異地備援的挑戰將是當資訊安全的災難發生時，如何復原？甚至於是否可以預防資訊安全事件的發生？因此資訊安全的管理將與異地備援息息相關，所以未來我們異地備援當思考如何整合資訊安全管理服務，提供一個完整的企業永續運作(Business Continuity)的解決方案。至於傳統的資料備份的解決技術，已經可以見到由光纖通道(Fibre Channel)慢慢地引進TCP/IP的技術，如iSCSI以及不同廠牌儲存管理的統一介面(不見得是像TCP/IP那樣的傳輸管理標準，但是已經是有幾個大廠開始相互交換內部資料格式)，所以未來的儲存管理甚至於異質平台的資料備份或許指日可待。

本文電子檔已上傳至出國報告資訊網

題要表

在政府訂定相關分級異地備援之要求下，近來陸續有許多政府機關執行異地備援之專案，在異地備援的服務中，國外目前的趨勢如何，有何新的技術或新的服務內容，IDC 業者應該伴演什麼角色，在本出國實習報告中，將提一個建議方向與策略方法。

整體的異地備援若僅只於傳統的資料備份、系統備援與網路切換是不夠的，現在異地備援的挑戰將是當資訊安全的災難發生時，如何復原？甚至於是否可以預防資訊安全事件的發生？因此資訊安全的管理將與異地備援息息相關，所以未來我們異地備援當思考如何整合資訊安全管理服務，提供一個完整的企業永續運作(Business Continuity)的解決方案。

至於傳統的資料備份的解決技術，已經可以見到由光纖通道(Fibre Channel)慢慢地引進 TCP/IP 的技術，如 iSCSI 以及不同廠牌儲存管理的統一介面(不見得是像 TCP/IP 那樣的傳輸管理標準，但是已經是有幾個大廠開始相互交換內部資料格式)，所以未來的儲存管理甚至於異質平台的資料備份或許指日可待。

目錄

第一章 前言

近年來台灣地區有許多的天災發生，如：民國 88 年 729 全台大停電、民國 88 年 921 集集大地震、民國 89 年 1031 象神颱風、民國 90 年 729 桃芝颱風、民國 90 年 917 納莉颱風、民國 91 年 331 花蓮強震等事件；同時近年來也有許多資訊安全事件，造成企業或政府機構的資訊系統服務中斷之情事，如 CodeRed、Nimda、SQL Slammer、Bugbear_worm、MS Support_worm、Passport 漏洞、信用卡偽造、金融資料外洩、中國網軍事件，以及疾風病毒（Blaster _worm）帶領變種軍團，聯手老大病毒（So-Big）等資安事件；綜合以上等因素，我們發現傳統的異地備援(Disaster Recovery)僅針對天然災害的災難來進行的備援措施是不夠的，因為為了企業永續營運(Business Continuity)的目標，所要面對的挑戰將不侷限於天然災難等意外事件，而是必須將病毒、蠕蟲、駭客攻擊等災難列入一併考量，方能做到新一代的異地備援目標。

有鑒於異地備援不僅僅止於傳統的資料備份與系統備份，尚需要考量當資安事件類型的災害發生時，如何做相關的備援處理，以達到快速復原的目標，所以此次出國實習不僅是對傳統資料備援的新技術進行瞭解，並安排針對資安事件類型的災害的備援技術進行實習，期望能夠將兩個領域的技術整合引進我們的 IDC 機房，推出新一代的備援服務及其衍生相關的加值服務。

第二章 行程概要

一、十二月一、二日(星期一、二):至 NetScreen 公司研習,NetScreen 公司為一家資訊安全設備製造商,瞭解該公司在資訊安全的產品佈局,從 Firewall/VPN 到 IDP(Intrusion Detection & Prevention)以及 SSL VPN 設備,以及 Security Management 管理軟體的開發等等。

二、十二月三、四日(星期三、四):FalconStor 公司研習,包括新儲存技術與異地備援技術研習討論,以及其客戶美商藝電 EA(Electronic Arts)之異地備援實際案例探討等。

三、十二月五日(星期五):Extreme Networks 公司研習,實習在 Router 或 Switch 上如何進行 Intrusion 的偵測與阻隔(Access Control List),用以偵測可能的入侵行為與防止可能的駭客入侵,降低資安事件發生的機率。

四、十二月六、七日(星期六、日):整理資料及自由活動。

五、十二月八、九日(星期一、二):Network Associated 實習,實習 McAfee 產品之防毒技術,以及 IntruShield 產品之入侵預防技術。

六、十二月十、十一日(星期三、四):HDS(Hitachi Data System)公司實習,包括儲存服務之規劃、儲存空間配置、服務架構與維護管理之技術實習。

七、十二月十二、十三日(星期五):搭乘清晨零點十五分之班機由舊金山返回台北(十二月十三日上午六點抵達桃園機場)。

第三章 IDC 備援服務趨勢

企業或是機構的資訊系統考慮備援，主要是期望能夠做到災難復原(Disaster Recovery)，當發生災難時，資訊系統依舊能夠繼續運作或是在中斷後迅速回復運作。在傳統的備原或是災難復原的領域中，其所關注的焦點在於：Network Connectivity、Hardware、Operation Systems、Critical Data Structures、Mission-Critical Applications，如圖一左側所示。

Traditional disaster recovery site considerations	Additional recovery site considerations that address information security
• Network connectivity • Hardware • Operating systems • Critical data structures • Mission-critical applications	• Anti-virus protection • Firewalls and access control rules • Router control lists • Intrusion detection • VPN and authentication tokens • Content filtering • Forensics and diagnostic tools • Operating system and application security patches

圖一、傳統災難復原與新災難復原所需考量的範疇

目前我們的異地備援服務是已經都將這些部份涵蓋，我們 IDC 所提供的異地備援服務包括有：

1. 資料備份：目前已經投資有防火櫃做為客戶之備份磁帶的保存，以及網路儲存系統做為線上(On-Line)資料備份複製保存之服務。
2. 機房備份：目前主要以桃園富國機房做為異地備援的機房。

3. 系統備份：目前提供伺服主機租賃服務，供客戶重新安裝 Operation System 以及 Application 軟體，做為備份資訊系統。同時我們也提出 Windows 作業系統的線上備份的功能機制，讓客戶在復原時期省卻重新安裝作業系統與應用軟體的時間。
4. 網路備份：提供 X.25、Frame Relay、ATM、IP VPN 等網路之備援切換服務，以作為備援機房與使用者之間的備援通信網路。
5. 辦公室備份：提供客戶在災難發生後，緊急的備援辦公室，做為臨時辦公之用。
6. 人力技術支援：提供客戶在災難發生後，調度 IDC 相關的人力支援客戶加速復原時程，達到企業營運中斷時間縮短之目標。

而在圖一的右側部份，則是列出新的災難復原所需考量的範疇，也就是將資訊安全(Information Security)考量進去，包括有：Anti-Virus protection、Firewall and access control rules、Router control lists、Intrusion detection、VPN and authentication tokens、Content filtering、Forensics and diagnostic tools、Operation system and application security patches 等，這些資訊安全的議題在我們目前的 IDC 加值服務中，部份已經提供，但是卻沒有納入異地備援的服務中，如何整合進入異地備援服務中，提供出那一種類型的服務是目前急需規劃進行的工作。

為什麼異地備援要考慮資訊安全？其實我們講異地備援其實應該說是災難復原(Disaster Recovery)，而進行災難復原不外乎是要做到企業永續服務(Business Continuity)，所以如果我們能夠讓"災難"不發生，其實也就不需要進行災難復原；傳統的"災難"多指是天災，天然

災難當然非人為可以控制，但是現在的"災難"已經擴展到像是病毒、蠕蟲、駭客入侵/攻擊、人為錯誤等等資訊安全事件，其實是可以避免或控制的。因此消極地進行災難復原規劃，不如積極地進行風險控制，所以目前的異地備援/災難復原服務也將資訊安全的服務一併納入，以完整的業務永續(Business Continuity)為服務目標。就像我們對抗感冒一樣，在未感冒前可以採用"施打疫苗"的方式來避免感染，在感染感冒後採用"服用藥物"的方式來治療感冒；所以資訊安全的管理就像是"施打疫苗"的預防措施，而異地備援/災難復原則是"服用藥物"的補救方法，誠如我們常見的一句話「預防勝於治療」，所以資訊安全的管理服務是在企業進行業務永續(Business Continuity)時的最佳疫苗。

我們來比較一下資訊安全與災難復原/異地備援的不同，如同表一之比較表說明。

表一、資訊安全與災難復原的比較表

Information Security	Disaster Recovery
著重在確保資訊的可用度、保密性與一致性(Availability, Confidentiality, Integrity)，避免非授權的存取、使用與修改	著重在災難中復原(Recovery)，進行 resources redundant & backup, emergency response, and recovery
期望藉由許多程序管理降低安全威脅發生的機會(**降低風險**)	期望縮短災難發生對營業中斷的影響時間(**加速復原**)
為了做到高可用度(High Availability)，多數做法為進行 redundant & backup 及相對的復原計劃，因此 Information Security 計劃中多涵蓋 Disaster Recovery	

我們可以從表一中了解其實在資訊安全的領域中，災難復原是涵蓋其中的，因為資訊安全的目標是確保資訊系統的可用度、保密性與

一致性，在可用度方面來看，災難復原是確保高可用度的一種方法，所以當大家在重視災難復原的這些工作時，我們反省一下其問題來源我們會發現，其實我們需要重視的應該是資訊安全的議題。如果我們做好資訊安全的控制，就可以降低甚至於避免災難發生的機會，自然就無需啟用到災難復原計劃，這才是企業永續營運最佳的目標。

所以我們發現現在的 IDC 服務方向是朝資訊安全管理服務(Security Management Service)來發展，由資訊安全管理服務來涵蓋災難復原服務，達到服務面更廣更大更完整的方式來說服客戶委外由專業的 IDC 服務業者來負責。這些工作不外乎包括：防火牆架設與管理、入侵偵測與預防、弱點分析及修補、資訊的存取控制、事件的預警與告警通報作業、緊急應變計劃與程序、內外部稽核等等，我們分別依據各個服務內容來探討客戶需求以及服務業者所可能提供的服務方案：

1. 防火牆架設與管理：防火牆的架設與管理的工作主要是在於資訊安全政策上的訂定，確立內外部的通信開放部份與不開放部份以及開放對象等等政策。管理的部份包括資訊安全政策的異動管理以及防火牆的設備維運管理等等工作。目前在資訊安全管理服務(Security Management Service)裡面，多數委外服務的公司是以防火牆架設與管理委外部份為最多。國外的服務案例有的是防火牆由企業自備，而維運管理委外；也有是防火牆由資訊安全委外服務商(Security Service Provider)提供，包括軟硬體的維運管理。目前我們已經提供此類的服務，我們採用 NetScreen 的防火牆，並由我們統一提供維運與管理服務，定期產生報表供客戶參考資訊安全事件記錄。
2. 入侵偵測與預防：由於新的駭客入侵已經不是單純透過防火

牆就可以阻隔的，而是透過資訊系統本身的漏洞滲透進入，因此唯有透過入侵偵測(IDS, Intrusion Detection System)，或是入侵預防(IPS, Intrusion Prevention System)等設備，才能偵測出入侵事件或是阻隔入侵攻擊。早期的技術多半是採用網路型(Network-base IDS)或是主機型入侵偵測(Host-base IDS)，其作法只能偵測出可能的攻擊事件，並無法即時阻隔攻擊，因此目前比較新的技術都強調入侵預防的作法，然而入侵預防的技術的缺點是怕遭遇到誤判情形，將正常封包阻隔；另外一個缺點則是因為入侵預防其作法像防火牆一般，需要逐一封包檢視，因此效能是其瓶頸，如何提昇處理效能是入侵預防設備的挑戰。目前我們 IDC 機房也有提供入侵偵測服務，我們採用 ISS(Internet Security System)公司的產品來作網路型入侵偵測服務，入侵預防的產品與服務正在測試開發階段，預計與其他資訊安全的服務做一配套包裝後提出新服務。

3. 弱點分析及修補：弱點分析(Vulnerability Assessment)服務主要是著眼於發現資訊系統所潛在的弱點或漏洞，並提供修補或加強的建議方法，以類似健康檢查的顧問諮詢來強化資訊系統的安全。目前我們 IDC 機房也有提供弱點分析及修補服務，我們採用 ISS(Internet Security System)公司的產品來作弱點分析及修補服務，如何有效的建立資訊資產資料庫以及弱點分析資料庫，以提昇弱點分析服務的正確性是本服務下一階段的挑戰。
4. 資訊的存取控制：所謂的資訊的存取控制主要是管制需要有經過授權的人方可依據其權限存取特定資料。此部份的技術多屬於應用系統上的認證授權，比較難以 ASP 模式委外，因

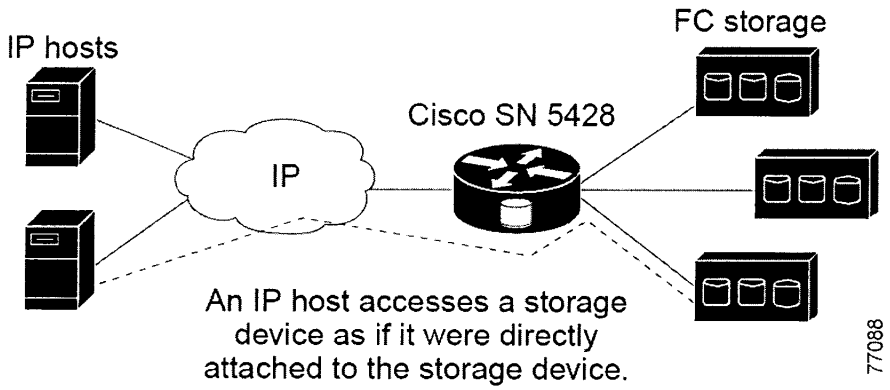
此此部份較少有服務的特定模式，僅有少部份是專案式客製化處理。除了應用系統上的認證授權外，資訊的存取控制也可以在前端的網路設備上進行控管，如 Access Control List (ACL)的設定，此部份倒是可以進行委外的部份；我們目前亦有提供路由器或交換器等網路設備上進行 ACL 的存取控制功能的設定。

5. 事件的預警與告警通報作業：資訊安全的預防以及即時偵測通報是非常重要的，一個是防範於未然，一個是即時的反應處理，所以事件的預警與告警通報作業是目前多數資訊安全委外服務的必要服務項目。事件的預警包括資訊系統新弱點/漏洞的通知，以及新的資訊安全攻擊手法的通知；告警通報則是包括遭受入侵/攻擊之事件通告，以及國際間其他最新入侵/攻擊之事件通告。目前我們 IDC 並沒有完整的此項服務，因為我們需要建立 SOC(Security Operation Center)方能做到即時的入侵/攻擊之事件通告，以及與其他國家的 SOC 連線方能取得最新的入侵/攻擊事件通告；目前我們的服務僅提供資訊系統新弱點/漏洞的通知，以及新的資訊安全攻擊手法的通知。
6. 緊急應變計劃與程序：有了即時的事件通報，還需要有一套完整的因應計劃與程序，才能在發生資訊安全事件時能不手忙腳亂，有條理的做出反應並加速處理，以降低事件影響時間與範圍。
7. 內外部稽核：資訊安全的各項工作是否落實，唯有藉由稽核來確保，方能達到資訊安全的各項政策之要求。稽核的方式有分內部稽核與外部稽核兩種，內部稽核是較經濟的一種作

法，至於外部稽核的成本較高，但是卻也可能發現更多的改善空間以更落實資訊安全的工作。目前我們IDC並沒有幫客戶進行稽核的工作，僅有是配合客戶的稽查人員進行答覆稽核的作業。

當然除了資訊安全的預防措施外，還是需要有事發後補救的措施，所以異地備援/災難復原還是需要的。然而目前的異地備援/災難復原的趨勢為何？主要還是以資料儲存技術的演進為主，主要的趨勢有：iSCSI的相關硬體陸續成熟上市、IDE硬碟陣列的推出、Windows NAS Server 的推出、以及跨廠牌的儲域網路系統(Storage Area Network, SAN)管理功能等等。

1. iSCSI的相關硬體陸續成熟上市：Intel的iSCSI網卡的上市，以Gigabit Ethernet的速度傳送資料，同時也簡化了網路儲存的架構，再搭配Cisco的SN 5000系列的Storage Router就可以讓前端的伺服主機存取位於TCP/IP網路後端的Storage，感覺就像是Direct Attach Storage一樣，如圖二。這樣就可以輕鬆地用主機端的單純Copy指令做到遠端資料備份，因為本機看到的磁碟區塊，已經是遠端的磁碟機。



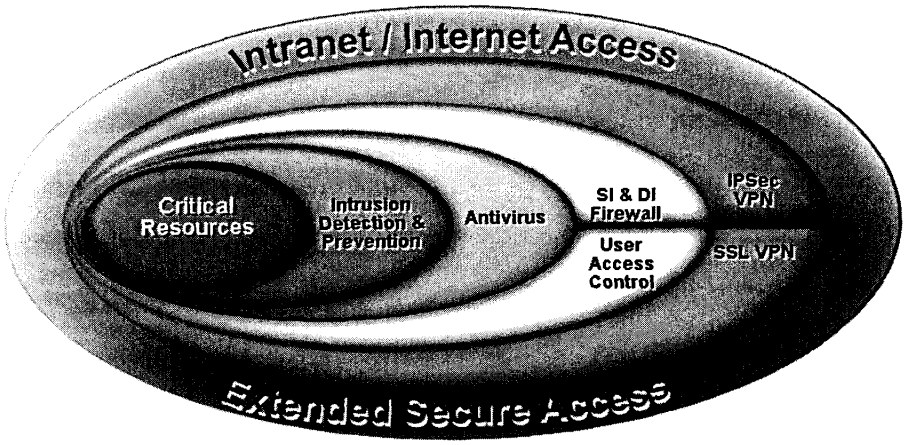
圖二、iSCSI Router介接使用架構圖。

2. IDE 硬碟陣列的推出：SCSI 硬碟成本較高，隨著 IDE 新傳輸介面標準的推出以及低成本的優勢，IDE 硬碟陣列的推出形成一個介於 SCSI 硬碟陣列與磁帶機之間的一種儲存媒體，也因此改變了許多儲存應用的架構，像是以往磁帶備份的時間過長的問題可以改為備份至 IDE 硬碟陣列中，以加速備份所需時間。另外一種應用為將較為少存取的資料由效能較佳的 SCSI 硬碟陣列中搬移至 IDC 硬碟陣列中，可以降低系統運作成本。
3. Windows NAS Server 的推出：軟體業界的巨人投入 NAS 的儲存領域中，使得原本比較廉價的 NAS 備份市場掀起了不小的漣漪，由於視窗式的圖像操作與為人熟悉的作業系統，造成一股使用 Windows NAS Server 進行資料備份的風潮。
4. 跨廠牌的儲域網路系統(SAN)管理功能：一直以來各廠牌的儲域網路系統(SAN)設備是採用不同的架構與技術來生產，因此不同廠牌間的儲域網路系統是無法對接管理，或是做相互的資料複製。目前幾家大廠如 EMC、HDS、HP(Compaq)已經取得共識，彼此交換管理的呼叫介面(API, Application Interface)來使用，因此可以達到初步的管理功能，可以監控不同廠牌的儲域網路系統狀態以及配發儲域網路系統的資源給前端伺服主機使用。

第四章 實習心得與建議

此次出國實習主要多專注在資訊安全新技術以及儲存網路系統服務方面之研習，針對資訊安全新技術以及儲存網路系統服務，分別說明實習的心得與看法於下：

1. 資訊安全新技術：在資訊安全方面，要保護的不外乎是 Critical Resources，而其保護的方法與技術包括有：Intrusion Detection & Prevention、Antivirus、Firewall、User Access Control、IPSec VPN、SSL VPN 等等，如圖三所示。



圖三、重要資訊系統的保護方法與技術

a. Intrusion Detection & Prevention：傳統的 Intrusion Detection 已經不足以立即處理入侵攻擊事件，目前是 Intrusion Prevention(或是稱為 In-line Mode Intrusion Detection)的天下，而現在市場上的最佳效能的產品是 Network Associated 公司的 McAfee IntruShield。其他產品像是 NetScreen IDP，Radware 等等都陸續推出 Prevention 產品。這一部份我們目前僅以合作案，推出 ISS 的 IDS 的方案，由於我們並沒

有 24 小時的資訊安全人員來監控分析即時偵測，所以僅是將偵測的 log 每週交付給客戶參考，因此服務無法吸引真正需要入侵偵測服務的客戶。建議我們 IDC 服務可以採購或是尋找合作廠商提供 IDP 的硬體設備，一如我們之前提供的防火牆租賃服務一般，由我們掌握管理權負責組態設定以及監控事件記錄 log，IDP 設備將有問題的攻擊或入侵阻擋下來，可以有效地降低以往 IDS 需要大量人力監控分析 log 記錄的工作；唯目前的 IDP 設備是否有誤判情形而將正常的連線當成攻擊或入侵而阻擋之情形，並未有成熟的市場經驗，因此尚待我們再進一步的分析設備的功能與特性，方能尋覓出適當的品牌與型號來提供本項服務。不過雖然如此，我們依舊可以預見，IDP 服務將是下一階段非常重要的服務之一。

b. Antivirus：防毒的解決方案已經多年的產品，但是目前的新的駭客攻擊手法是結合病毒與資訊系統漏洞而成為自發性傳播感染的蠕蟲(Worm)攻擊，這些蠕蟲感染已經非以往的防毒軟體可以阻擋清除的。新的防毒策略包括非常多的部份來進行處理，有防毒牆的方式來阻擋過濾蠕蟲感染的散播，或是路由器、交換器的 Pattern Matching 的方式將蠕蟲感染比對後阻擋掉，另外就是郵件掃毒，以避免蠕蟲透過郵件預覽或是附件，甚至是利用特定 URL 來感染並植入後門程式等等；還有為了讓駭客無法利用系統的漏洞而進入資訊系統取得管理權或是植入後門程式的方法是：弱點分析(Vulnerability Assessment)與漏洞修補，定期的發現系統弱點與漏洞而加以補強，使得駭客無從發現漏

洞而進行入侵或植入後門。

像防火牆公司 NetScreen，其新的產品方向也整合與 Trend Micro 的病毒功能整合，在其小的防火牆 NS-5XP 就採整合進入其韌體的方式來一併提供防火與防毒牆；至於其他大型的防火牆因為考慮效能問題，而是採用通信協定方式配合防毒牆來分工合作。我們 IDC 已經提供有 NetScreen 的防火牆服務，建議接下來我們可以著手來研究搭配何種品牌的防毒牆來進行防毒服務，補強我們在防毒服務上的不足。

另外 Extreme Networks 的下一階段 Router/Switch 產品也將新增針對病毒或蠕蟲 Access Control 功能，可以對於固定 Pattern 來過濾或是進行異常流量或封包的阻擋，我們可以看到防毒功能是很多不同領域產品公司的共同努力方向，以因應近年來日益增加資訊安全事件的趨勢。我們也確實在這幾年發現很多資訊安全事件的解決並無法在後端的伺服主機或是防火牆來阻擋，而可能需要在更前面的路由器或是交換器先將攻擊封包攔阻，才能有效阻檔大量的攻擊封包，如 DDoS(Distributed Deny of Service) 攻擊。所以我們 IDC 下一階段的路由器或是交換器的採購或擴充，必須考量這方面的規格，將它們加入規格中，以提昇未來處理資訊安全事件的能力。

c. Firewall：防火牆已經是多年來成熟的產品市場，但是目前面臨的最大挑戰就是效能問題，因為儘管可能你所採用的防火牆可以阻擋入侵，但是未必能夠承受大量的 DDoS 封包攻擊；所以如何避免阻斷服務情形的發生，必然是要增

加防火牆的處理效能。目前許多廠商是致力於 ASIC 的開發，使得硬體處理效能能夠加速，但是隨著日新月異的攻擊手法與技術演進，硬體 ASIC 又有其限制，因此目前的趨勢是開發 Programmable ASIC 來增加變更的彈性，我們必須留意未來再採購的防火牆設備，確實是朝這個方向開發設計的。

d. User Access Control：在 Access Control 方面，無非是朝著針對攻擊封包或是蠕蟲感染封包進行阻擋，以及對於某一類型封包流量的管制(或稱 Rate Shaping)，以避免如 SQL Slammer 事件那般大量的 Multicast 封包流，造成交換器當機的情形發生，或是大量的 ICMP、TCP 或 UDP Flooding 造成網路壅塞。這些 Access Control 的趨勢也是我們在買下一梯的路由器或是交換器時所需考慮的功能之一。

e. IPSec VPN：IPSec VPN 技術主要是用於 Internet VPN 架構下，國外網際網路頻寬費用較為廉價，因此許多企業採用 Internet 來架構其企業內部網路(Intranet)，其所仰賴的安全機制即是 IPSec VPN。目前非常多的路由器或是防火牆皆支援 IPSec VPN 功能，只是國內的 Internet 環境還是不像國外那般比 Intranet VPN 網路低廉許多，所以還是較少客戶採用。唯目前的兩岸間的 Intranet VPN 頻寬費用昂貴，因此存在著採用 IPSec VPN 的市場，我們 IDC 倒是可以考慮提供多部 NetScreen 防火牆租賃來構成 IPSec VPN 的服務，以較為經濟的費用滿足台商兩岸的通信需求。

f. SSL VPN：SSL VPN 是一個極新的技術，主要的應用面是在於提供企業員工以非常簡易且快速地透過 Internet 來安

全地存取企業內部的資訊系統。它強調只是透過 Https 方式，即可非常安全地進行各項傳統的資訊系統應用連線，不像以往需要安裝 Tunnel 軟體來做安全連線。我們 IDC 的維運網路倒是可以考慮建置 SSL VPN 設備，以方便維運人員於非上班時間安全地進入 IDC 維運網路，進行遠端遙控障礙修復等工作。

除了以上各別的資訊安全領域以外，其實整體資訊安全的管理才是資訊安全服務的關鍵，雖然目前有資訊安全的管理產品，但是大多數的產品不過是一個集中管理設定的介面系統罷了，它們並無法管理不同廠牌的設備，多半只能管理同一廠牌的各項設備產品。唯目前的市場上並沒有一家公司可以跨越到各個領域並同時都有對應的產品，所以我們無法有一個良好的工具來掌握資訊安全的全盤狀況，這將是我們 IDC 在未來要推出一個完整的資訊安全管理服務最大的挑戰。

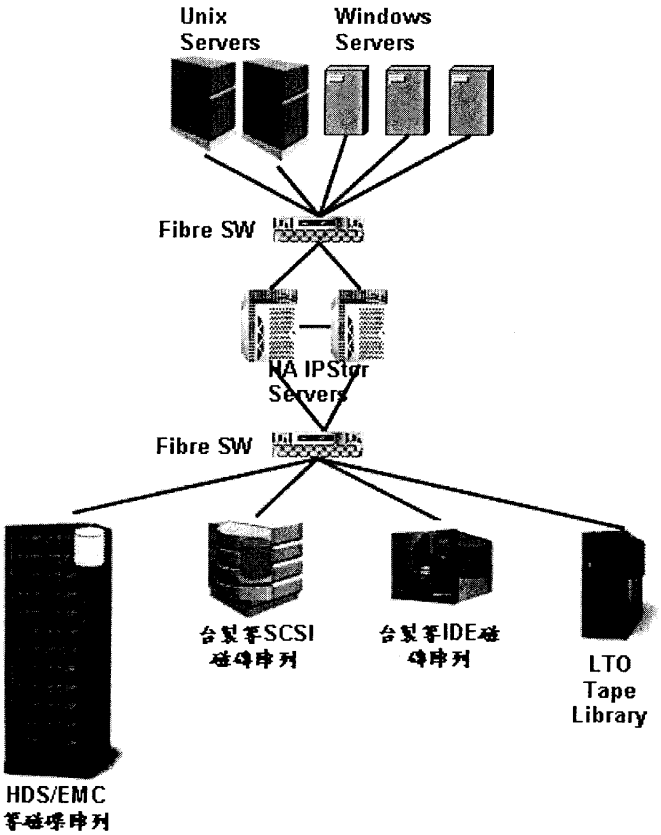
2. 儲存網路系統服務方面：在儲存網路服務方面的技術而言，因為已經是成熟的市場服務，所以目前所見到的服務趨勢比較著重於前面資訊安全我們所提的管理功能部分。和資訊安全領域的情形一樣，各家儲存網路系統產品多是以功能面來相互競爭，而其背後的技術卻是大相逕庭，所以面臨跨廠牌的管理時往往是 IT 維運管理人員心中的痛，因為不同廠商的儲存網路系統，各自有其管理的系統與介面，很難做到整合監控與管理。而這些問題已經存在已久，所以我們已經看到部份的成果。目前幾家大廠如 EMC、HDS、HP(Compaq)已經取得共識，彼此交換管理的呼叫介面(API, Application Interface)來使用，因此可以達到初步的整合管理功能，可以監控不同

廠牌的儲域網路系統狀態以及配發儲域網路系統的資源給前端伺服主機使用。

像此次參訪實習的 FalconStor 公司就可以跨廠牌的管理不同廠牌的儲存網路系統，然而它所強調的是採兩種方式來介接，一個是單純地當不同廠牌的儲存網路系統為一個磁碟陣列，另外一個做法是以 SED(Service Enable Disk)將原本的儲存切割資訊轉址方式(Redirect)來做整合再利用，所以它能夠以側面角度來與其他品牌來介界接(非正統做法)，而且也可以順利地與多家廠商介接，而不用取得該公司的內部運作架構或細節。不像其他 EMC、HDS、HP(Compaq)等廠商間以交換控制介面來相互連線。但是其缺點就是因為它們採側面方式來介接，有些客戶比較不能接受這種類似走後門的方式，所以這也影響了部份市場的開拓。不過我們倒是可以善加利用這個好處於客戶首次進行的 Data Migration 的過程中，因為這只是一次性工程，客戶應該可以接受這種介接方式，完成後會再恢復為原先架構或是一個嶄新的架構。

至於此次 HDS 的行程中，我們也發現像 HDS 與 EMC 等儲存網路系統大廠，皆推出中低階的產品，並且將原本高階產品的異地備份/複製功能移植到中階產品上，因此具備異地備援的儲存網路系統之費用已經大幅下降。我們可以利用此一現象再投資世界大廠 HDS 或 EMC 的中階儲存網路設備，做為我們儲存服務的儲存空間，將原本舊的儲存空間投資設備(台灣製的 SilverShine 磁碟陣列)做為第二階之儲存空間，或是以效能區隔為 Level 1 與 Level 2，客戶要求高效能的儲存空間服務我們以 HDS 或 EMC 的設備提供，如果中小型客戶所

需的僅是尚可的效能空間，那我們就以台灣製的 SilverShine 磁碟陣列做因應，如此以不同的成本經營，也給客戶不同的費用來租賃，相信可以區隔出市場定位，各別在不同的客戶群中尋得目標客戶。再加上可以考慮引進 IDE 的磁碟陣列，來做為 Level 3 的儲存空間服務，定位在做資料備份空間碟，以 IDE 硬碟效能高於磁帶機的宣傳方式，吸引需要快速備份的高階客戶；因為 IDE 硬碟取得成本並不會較磁帶機與磁帶來得高出許多，所以這也是一個可以嘗試的新服務。



圖四、hiStorage 未來服務架構示意圖

所以我們可以利用高階 SCSI 硬碟設備、中階 SCSI 硬碟設備、IDE 硬碟設備、以及磁帶機與磁帶，這四種儲存空間設

備來透過 IPStor 的集中管控，進行不同服務等級的儲存空間租賃服務，當然再配合 IPStor 本身的功能可以自動將 I/O 讀取率較低的資料由高階效能的儲存設備搬移至較低階效能的儲存設備，如此一來也可以將各不同效能的儲存設備可以達到有效利用，如圖四。

至於磁碟機上異地備份/複製的部份，在技術方面倒是不見有何新的創新，反而看到的現象是原本廠商專注的高階備援市場轉戰中低階備援客戶市場，因此也見到的有很多異地備份/複製的軟體直接於 Host 端安裝，然後備份至異地的儲存空間存放。而目前的簡易做法即是用 iSCSI 來達到透過 TCP/IP 網路進行存取異地端的儲存設備。而我們原本合作的 FalconStor 公司的 IPStor 軟體也推出像 FileSafe 與 DataSafe 等軟體，可以直接將 Host 端的資料或作業系統資料進行異地備份/複製。還有另外我們即將推出的 DataSAFE 服務也是同樣的精神，在客戶端的主機上安裝一個 Agent 程式，然後該程式會定期將所定義的資料或系統資料備份至我們 IDC 機房內的伺服主機上，達到異地備份的功能。我想我們在這一部份的技術趨勢中，倒是已經跟上腳步或是可以說已經領先國內的許多廠商。