行政院及所屬各機關出國報告
（出國類別：實　習）

配電業務電腦分散處理之網路應用與發展技術

服務機關：台灣電力公司
出 國 人 職　　稱：十一等電機工程監
姓　　名：陳淑惠(030395)
出國地區：美國
出國期間：90.09.10～90.09.25
出國計畫：90 年度第 33 號

行政院及所屬各機關出國報告審核表

出國報告名稱：配電業務電腦分散處理之網路應用與發展技術	
出國計畫主辦機關名稱：台灣電力公司	
出國人姓名/職稱/服務單位：陳淑惠／電機工程監／業務處	
出國計畫主辦機關審核意見	☑1. 依限繳交出國報告 ☑2. 格式完整 ☐3. 內容充實完備. ☑4. 建議具參考價值 ☑5. 送本機關參考或研辦 ☐6. 送上級機關參考 ☐7. 退回補正，原因： ☐(1)不符原核定出國計畫 ☐(2)以外文撰寫或僅以所蒐集外文資料為內容以 ☐(3)內容空洞簡略容 ☐(4)未依行政院所屬各機關出國報告規格辦理 ☐(5)未於資訊網登錄提要資料及傳送出國報告電子檔 ☐8. 其他處理意見
層轉機關審核意見	☐同意主辦機關審核意見 ☐全部 ☐部分＿＿＿＿＿＿＿＿（填寫審核意見編號） ☐退回補正，原因：＿＿＿＿＿＿＿＿（填寫審核意見編號） ☐其他處理意見：

說明：

一、出國計畫主辦機關即層轉機關時，不需填寫「層轉機關審核意見」。

二、各機關可依需要自行增列審核項目內容，出國報告審核完畢本表請自行保存。

三、審核作業應於報告提出後二個月內完成。

總經理：　　主管處：　　單位主管：　　報告人：

副總經理：

行政院及所屬各機關出國報告提要

出國報告名稱：配電業務電腦分散處理之網路應用與發展技術

頁數 20 含附件：□是■否

出國計畫主辦機關/聯絡人/電話：

台灣電力公司/陳德隆/(02)23667685

出國人員姓名/服務機關/單位/職稱/電話：

陳淑惠/台灣電力公司/業務處/十一等電機工程監/(02)23666688

出國類別：□1 考察□2 進修□3 研究■4 實習□5 其他

出國期間：90.09.10～90.09.25　　出國地區：美國

報告日期：90.11.20

分類號/目：電力

關鍵詞：網路

內容摘要：

本公司目前正積極建置業務單位之電腦骨幹網路計畫，同時電腦作業環境也由過去的大電腦集中處理方式漸漸走向開放的網路平台，在複雜的網路環境中，如何確保網路環境的安全及資訊安全，是一個必須全面考量的問題。擬定一有效適用的資訊安全政策，以降低威脅及弱點，減少損失，並了解現今網際網路中的攻擊方法與防護機制，雖然各種防禦措施並無法保證百分之百的安全，但亦提供了一道必要的防線，同時網路是面的分布，維護網路安全是企業內每個人的責任，任何一點不安全即會影響到整個企業網路。另在網路作業中資料的備份及相關設備的備援系統亦十分重要，有效掌握網路各點的安全，才能強化用戶服務與業務導向之應用。

行政院及所屬各機關出國報告
（出國類別：實　習）

配電業務電腦分散處理之網路應用與發展技術

服務機關：台灣電力公司
出 國 人 職　　稱：十一等電機工程監
姓　　名：陳淑惠(030395)
出國地區：美國
出國期間：90.09.10～90.09.25
出國計畫：90 年度第 33 號

目　　錄

壹、 實習任務：

配電業務電腦分散處理之網路應用與發展技術

貳、 實習行程

一、出國期間：90 年 09 月 10 日～09 月 25 日（計 16 天）

二、研習行程：

（一） 90/09/10：往程（台北→紐約）。

（二） 90/09/11～90/09/17：紐約，參訪 Con Edison Company。

（三） 90/09/18：往程（紐約→北卡）

（四） 90/09/19～90/09/23：北卡，參訪 Carolina Power & Light Company。

（五） 90/09/24～90/09/25：返程（北卡→紐約→台北）。

參、實習內容

一、前言：

本公司目前正積極建置業務單位之電腦骨幹網路計畫，所規劃之網路架構除整合區處與其所轄區處外部門（如配電中心、區域巡修股及服務所等），並能與本公司企業網路構成一完整之電腦資訊網路架構，瞭解國外網路發展與整合技術，作為規劃電腦網路及推動各項業務之參考。

二、網路設備發展趨勢

網際網路的革命，促使現有的網路架構發生結構性的變化，分別形成三波的衝擊，第一波的衝擊是骨幹網路走向高容量化，由於 Internet 時代的來臨，數據傳輸流量大增，導致既有的同步數位階層/同步光纖網路 (Synchronous Digital Hierarchy/ Synchronous Optical Network ; SDH/SONET 註一)系統容量，不足以因應未來之需求，而必須走向緊密分波多工(DWDM; Dense Wavelength Division Multiplexing 註二)系統；第二波的衝擊是上網方式由窄頻走向寬頻，過去的類比式數據機，上網速度為 33.6K、56Kbps，但在多媒體的需求下，窄頻的速度已不符合所需，導致各種寬頻上網技術興起，如 ADSL、Cable Modem 等，速度也大幅提升

到 512K、1.5Mbps 以上；第三波的衝擊則是都會網路的改變，身為骨幹網路與接取網路的橋樑，都會端網路不只要具有高容量特性，更要面對各種不同的接取技術，因此都會端核心網路將是走 DWDM 系統，都會接取網路則將走向光纖化發展，並需容納多種的電訊擷取技術。

目前整體通訊網路架構約可分為三層次：骨幹網路(Backbone Network)、都會網路(Metropolitan-Area Network；MAN)、接取網路(Access Network)，在整體網路中，骨幹網路是作為長途資料傳輸網路系統，都會網路則是用以連接骨幹網路以及接取網路，而接取網路則是一般用戶連接到整體網路的入口點，目前一般用戶連接到網路的方式則相當多樣，包括有打電話以及透過 ADSL、專線上網等。也由於接取端網路有不同服務，導致都會網路在整體網路扮演的橋樑角色就相形重要。

為了因應都會網中對於頻寬的需求，取代原有之專線連線(T1/E1)，Service Provider 提供更高速的連線給客戶已成為趨勢。WDM(註二)技術的成熟，也促使 Gigabit Ethernet Ring 逐步取代 SONET/SDH Ring，然而光纖乙太網路(Optical Ethernet)結合了光傳輸的高頻寬與乙太網路的普遍性，重新改寫了頻寬使用的規則。對於一個現代化企業而言，其資訊基礎建設的優劣

被視為具競爭力與否的重要指標，利用光纖乙太網路智慧型的通訊系統與高頻寬之傳輸環境，可由原本T1/T3專線轉型為都會網路環狀架構，大幅降低營運成本並提高整體營運效率。

展望未來，光纖纜線的建置成本將隨著消費需求大增而降價，也加速光纖取代銅纜線之速度；再者，Gigabit Ethernet之技術已成熟，10 Gigabit Ethernet之標準已大致底定，各網路設備廠商也將陸續推出相關產品，建構所謂光纖到大樓、光纖到街角甚至光纖到桌上之優質上網環境，也是各國資訊基礎建設之重要方向與努力目標。

註一：所謂 SONET(Synchronous Optical Network) 同步光纖網路，是由 Bellcore 在 1980 年代中期所提出在光纖網路上高速傳輸之同步規格，後來 CCITT(國際電話暨電報諮詢委員會，現更名為 ITU-T)訂定了所謂 SDH (Synchronous Digital Hierarchy)同步數位階層架構，其應用含蓋光纖及光纖以外網路之傳輸，應用於北美以外地區，因此我們通稱 SDH 為世界標準之規格，而 SONET 為北美標準之規格。

註二：所謂 WDM 技術，就是在現有的傳輸網路上做緊密分波多工 (Dense Wavelength Division Multiplexing；DWDM)，其原理就如同彩虹，依照光的不同波長分出，進而把多個不同波長之光信號在同一條光纖上傳輸，因此可提升傳輸容量並且互不影響，若採用 8 個波長之 WDM 技術，則可在同一條光纖上，提升傳輸容量為原來之 8 倍，目前每個波長能傳送 1 Gbps 的資料，將來陸續會朝 10 Gbps 甚至 40 Gbps、80 Gbps 發展；另外光傳輸因長距離而導致色散之問題因透過色散補償技術而獲得解決，並可利用光放大器、光再生器來延長傳輸距離至數千公里。

三、網路資訊安全

企業的資訊安全內容可分為設備、軟體、資料、個人及企業經營需求等部分，企業資訊系統的風險主要來自外在威脅及自身弱點，應擬定一有效適用的資訊安全政策，以降低威脅及弱點，減少損失。

企業資訊系統的風險主要來自外在威脅及自身弱點，威脅及弱點會損及資訊資源、系統及網路的可用性(Availability)、完整性(Integrity)或保密性(Confidentiality)。所以對每個資訊資源或事件的威脅或弱點，都須個別評估一旦發生時所可能造成的損失，包括資訊系統替換或維修的成本；將資訊系統重建為具智慧資產的成本；資訊系統停擺所損失的價值；以及其他(如顧客或協力廠商失去信心)。風險評估分析如下：

資訊資源	威脅或弱點	防範建議
企業經營需求	業務成長的需求、企業策略聯盟的形成、業務不斷的改變。	病毒防制、入侵偵測、安全稽核、使用者管理、身份認證、簽入驗證。
一般設備	水災、火災、颱風、地震	保險、保全系統、自動灑水系統。
資訊設備	火災、地震、安全管制不力、無權限者盜用。	保全系統、門禁系統、安全監視系統
軟體	意外修改或破壞、不安全	防火牆、病毒防

資訊資源	威脅或弱點	防範建議
	的新程式碼、不當備份。	制、入侵偵測、安全稽核、備份／恢復、備援系統、存取控制。
資料與資訊	儲存媒體安全性、駭客攻擊、遠端不安全資料取用、檔案被偷或遭破壞。	資料加解密、網路儲存記憶體、存取控制、使用授權、備份／恢復。
個人	員工偷竊資料、不滿的離職員工報復、為私利而複製資料、是否盡職管理系統、是否讓網路繼續正常執行。	使用者管理／群組管理、身分認證、單一簽入驗證、存取控制、使用授權。
其他	欺騙與偷竊、有惡意的駭客攻擊、商業間諜行為、電腦病毒感染及保護個人隱私權。	防火牆、資訊安全標準處理程序、病毒防制。

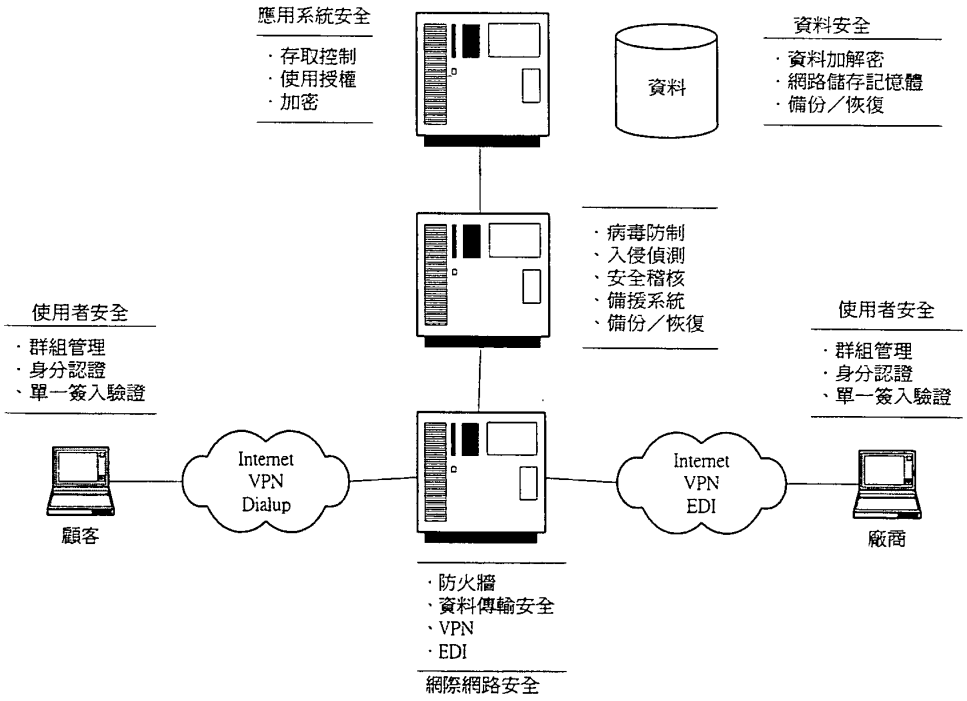
沒有百分之百絕對安全的資訊保全措施。既然風險沒辦法全部移除，就必須管理。有效的風險管理即是將資訊安全合格化、有效量化風險因子，並減低其發生的可能性。

資訊安全範圍包含系統項目及資訊安全設備與技術，如圖所示。

・設備：保險、保全系統、門禁系統、安全監視系統、自動灑水系統。

・網際網路安全：防火牆考量、資料傳輸安全控制、VPN／EDI（如病毒防制、入侵偵測、安全稽核、備援系統、備份／恢復）。

・使用者安全：使用者管理／群組管理、身分認證、單一簽入驗證（資料加解密、網路儲存記憶體、存取控制、使用授權、備份／恢復）。



與營運相關的資料或資訊，是企業相當重要的資產。針對資料與資訊取用的安全等級可分成：非限制性（員工、協力廠商都可取用）、限制性（限高階主管或特定主管）、限制分送（功能導向，因應業務需求而設定）三種方式。各種使用者取用企業資料或資訊，須確認資料的安全等級及其使用權限。

非限制性	限制性	限制分送
會議通知	機密會議記錄	銷售資料及個人資料
網路電話目錄	組織內部員工薪資資料	顧客資料庫或相關隱私資料
公司公開資料	財務報告	潛在需求資料
USER ID	系統管理者密碼	一般性密碼、加密金鑰
大部份網際網路的政策與程序	敏感事件的反應計劃	風險評估結果
主要應用系統的功能資訊	主要應用系統的原始碼	主要應用系統的產品資訊

另企業常有疑問，為何安裝了防火牆，網站還是被入侵。以網路安全來說，防火牆只是一個警衛、一個大門管理員，通常它只管讓誰去哪裡、去幾樓、找誰，並未深入管理，防火牆不是萬靈丹，不能事事靠它，適時修正伺服器上的系統漏洞（如安裝 Services Pack 等）

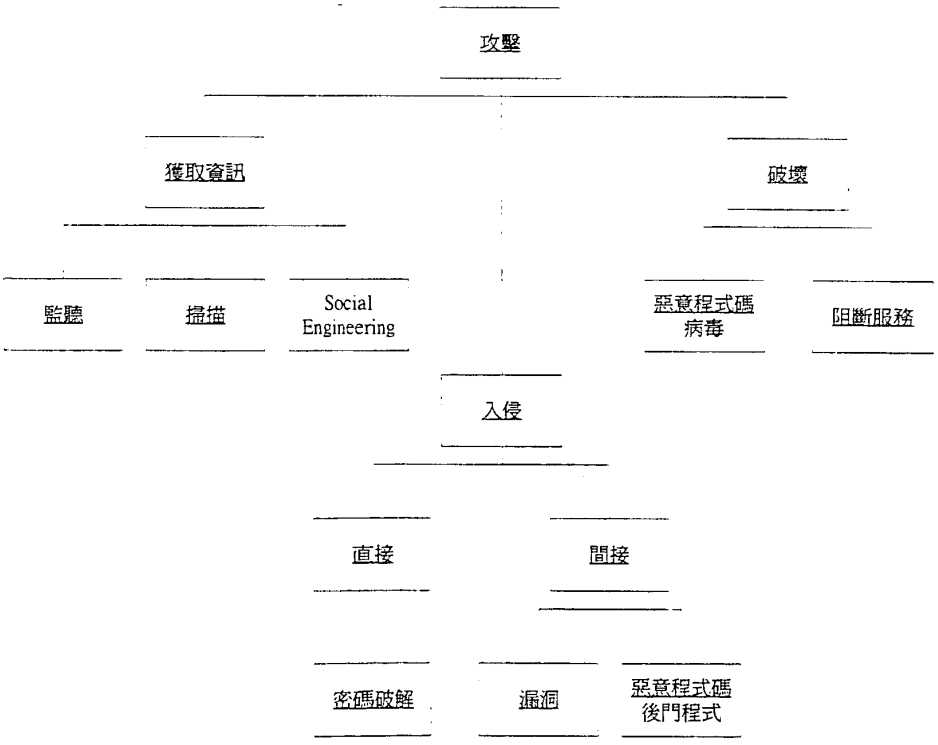
實有必要，在安裝防火牆時僅開放必要的服務，少開一個洞就多一份保障，養成良好的 Log、Backup 習慣，在所有追蹤駭客的文件中，一定是按部就班的一站一站查，且目前硬碟如此的便宜，用點空間來作 Syslog，絕對是值得的投資。

在網際網路的世紀裡，網路安全的領域極為廣泛，不論從網路層面、系統層面、應用層面，都有許多問題。這些問題包括了病毒、廣告郵件、資源濫用、道德問題、駭客破壞等，每一個環節都十分重要。關於防制駭客，只能說先把自己的系統漏洞補好，再使用防火牆系統，如此即使不能保證不被攻擊，但是至少可以將損失減到最輕。

四、網路安全防護機制

由於資訊科技(Information Technology；IT)和網際網路(Internet)的快速發展，參與網際網路的人數日益增加且複雜，電腦主機上和在網際網路間傳送的資料愈來愈重要，Internet 上的網站提供之服務也愈來愈關鍵(Critical)；然而網路安全的發展速度卻沒有跟上，常常因為效率或方便性的考量而被忽略掉。

為了確保企業內部網路在網際網路的安全，我們先了解現今在網際網路中的攻擊方法。一般來說，攻擊依類型可以分為三類：獲取資訊、入侵和破壞。



・監聽：這類型的攻擊是指監聽電腦系統或網路封包以

獲取資訊;監聽實質上並沒有進行眞正的破壞性攻擊或入侵，但卻通常是攻擊前的準備動作，攻擊者利用監聽來獲取他想攻擊對象的資訊，如網址、使用者帳號，甚至直接拿到使用者密碼。

- 掃描：這類型的攻擊是指掃描電腦系統以獲取資訊；攻擊者利用掃描來獲取他想攻擊對象的資訊，如開放的服務、提供服務的程式甚至利用已發現的漏洞樣本(Pattern)做比對直接找出漏洞。

- Social Engineering：這個類型是指不透過電腦或網路的攻擊行為；一個 Social Engineering 的例子是攻擊者自稱是系統管理者，發電子郵件或打電話給使用者，要求使用者提供密碼，以便測試程式或其他理由;其他像是躲在使用者背後偷看他的密碼也屬於Social Engineering。

- 密碼破解：這類型的攻擊是指使用程式或其他方法來破解密碼;破解密碼主要有兩個方法式，猜出密碼或是一個一個嘗試所有可能的密碼。

- 漏洞：是指程式或軟體在設計、實作或操作上的錯誤，而被攻擊者用來獲得資訊、取得系統管理者權限或破壞系統。

- 惡意程式碼：這個類型的攻擊是攻擊者透過外部裝置和網路把惡意程式碼安裝到系統內，外部裝置可能是軟碟機、光碟機、抽取式硬碟機或甚他可攜式媒體的裝置。這個類型的攻擊通常是攻擊者成

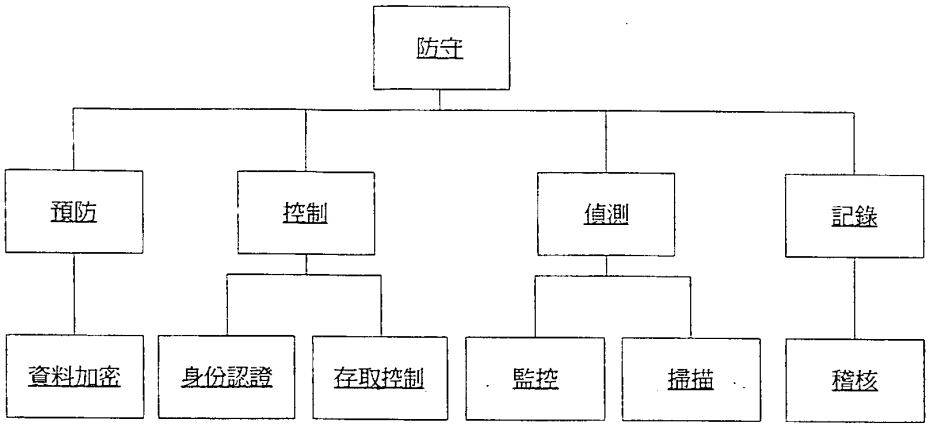
功入侵後做的後續動作，可以分成兩個子類別：病毒(Virus)和後門程式(Backdoor)。

-病毒有兩個特性，自我複製性(Self-replicating)和破壞性(Destruct)，這類別的攻擊就是把病毒安裝到系統內，利用病毒的特性破壞系統和感染其他系統。

-後門程式通常是攻擊者在入侵成功後，為了方便下次入侵而安裝的程式。

• 阻斷服務：這類型攻擊的目的不是要入侵系統或是取得資訊，而是阻斷被害主機的某種服務，使得正常使用者無法接受網路主機所提供的服務。這類型主要是把稀少的資源用盡，讓服務無法繼續，例如 TCP 同步訊號洪水型攻擊(TCP SYN Flood Attack)是把被害主機的等待佇列填滿，而 ICMP 洪水型攻擊(ICMP Echo Reply Flood Attack)是把被害主機的網路頻寬用盡。

在了解現有攻擊方法後，我們可依防守特性將防守模式分為四個類別：預防、控制、偵測和記錄。



- 資料加密：使得攻擊者即使取得加密過的資料，也無法獲取正確的資料內容，所以資料加密可以保護資料，防止監聽攻擊。這個防守類型可以分為兩個子類別：對稱式加密（Symmetric Encryption）和非對稱式加密（Asymmetric Encryption），不過目前比較多的應用是結合對稱式及非對稱式的加密。

- 身分認證：身分認證用來判斷某個身分的確實性，例如使用者、網路主機、檔案或資料，確認身分後，系統才可以依不同的身分給予不同的權限。密碼是最常被用來確認使用者身分的方法，但它可能會遭受到破解或監聽；加密主要是用來確認資料擁有者的身分，即所謂的數位簽章。

- 存取控制：是利用確認身分方法獲知使用者的確實性

後，根據不同身分給予不同的存取控制權限，控制使用者存取系統資源或資料。防火牆(Firewall)的過濾封包(Packet Filtering)功能也是屬於這類型的防守方法。

- 稽核：這一類型的防守是把系統中和安全有關的事件記錄下來，例如使用者登入來源與登入系統失敗次數及各種重要的網路活動。當受到攻擊時，這些資料可以用來幫助調查攻擊者的來源，或分析攻擊的方法，以思考可能的方式來預防下次的攻擊。現在的作業系統都有提供稽核的功能。

- 監控：這一類型的防守是監控系統或網路是否有異常的活動，可分為網路監控程式(Network-based Monitor)和主機監控程式(Host-based Monitor)。網路監控程式可以監控網路中主機是否有異常的網路活動，它藉著開啟網路卡的promiscuous mode來攔截網路中的封包，分析這些封包及流量對網路內主機是否有不正常影響，再做出適當的反應；主機監控程式可以監控主機對外的網路活動和內部的異常行為。

- 掃描：這裡的掃描指的是使用已知的樣本，來掃描系統內是否有惡意程式碼，也就是病毒或後門程式。一般所謂的防毒軟體就是屬於這種類，由於掃描程式是靠已知樣本來找到惡意程式碼，所以使用者必須時常更新已知樣本，也就是防毒軟體中的病毒碼，掃描程式才能發現較新的惡意程式

碼。

網路安全是一個必須全面考量的問題，就使用者來說，由於使用者大多是使用 Windows 系統，所以必須安裝掃描程式和隨時取得最新的已知惡意程式碼樣本來確保自己的主機不被病毒感染和被安裝後門程式，注意自己的密碼不被竊取，不要認為自己的主機上並沒有存放重要資料就認為無所謂，卻不知本身雖無重要資訊外流的危險或損失，但是卻可能成為攻擊的攻擊進入點或是分散式阻斷服務攻擊的常駐程式，造成企業內網路主機被攻擊；就系統管理者來說，系統管理者必須經常注意系統漏洞及修補漏洞，架設防火牆來過濾外來的封包，經常性使用監控程式來偵測系統有無異常現象，使用稽核程式來記錄系統的各種有關安全的活動，使用複雜度較高的密碼，儘可能不讓系統被入侵。

肆、 實習心得及建議

隨著電子商務時代的到來，越來越多企業與個人的重要資訊在網路上傳輸，使資訊安全的議題日益受到重視。本公司的電腦作業環境也由過去的大電腦集中處理方式漸漸走向開放的網路平台，在複雜的網路環境中，如何確保網路環境的安全及資訊安全，不僅是資訊部門的責任，也是每個同仁的責任，網路是面的分布，任何一點不安全即會影響到整個企業網路。另在網路作業中資料的備份及相關設備的備援系統亦十分重要，雖然各種防禦措施無法百分百的防止入侵，但有完善的備援措施卻可在短時間內回復系統，不僅可以提供持續不間斷的服務，提高客戶的滿意度，更可以得到客戶的信賴，讓整個業務蒸蒸日上。

伍、參考資料

1. Con Edison environment, health and safety annual report 2000。
2. Con Edison 2000 annual report。
3. http://www.cplc.com。
4. 網路通訊雜誌。