企業內網路與防火防毒牆應用在「遠端服務中心」之建置

彭麗貞　魏 廉 楊立達

國防部中山科學研究院

桃園縣龍潭郵政 90008 附 3 號信箱

TEL(03)4712201ext.351756,351824

FAX(03)4711494

摘要

這是一篇有關企業內網路(IntraNet)技術應用在國防事業之實務經驗論述。本單位正值大型主機系統適型化又面對系統整合等諸多困擾時，全球網路系統已在學術界已蔚爲風行　由於網際網路(InterNet)上擁有一致的主從架構標準　及瀏覽器提供一致的人機介面等諸多優點　成爲本院系統適型化的整合面選擇。經過成本及技術等相關考量及必要之實驗後，我們得到預期的成果並期待與人分享及交流經驗。

在本文**序論**中，我們談到對企業內網路的認知及導入 IntraNet 技術之原因，在**系統需求**中描述本院應用系統之需求及相關的組織及環境等背景因素。**相關技術**包括資料庫與網頁的連結技術　以及防火牆整合防毒牆技術。**系統建置**分爲系統架構及網頁實作兩部份分別探討其設計特性。最後則論述**系統成果**及**問題與發展**。

序論

隨著全球資訊網的快速發展，已經使得資訊地球村的理想得以實現，它不僅加速了國際文化與社會資訊的共享與互動，更重要的是它也逐漸改變企業的商業行爲。而類似全球資訊網路如此驚人成長的現象現在似乎又將再度重演，只不過現在的舞台是在各大企業組織內部，這就是越來越多公司已開始建造的企業網路(Intranet)，它將網際網路與全球資訊網技術所帶來的好處同樣的應用在公司內部，進而解決組織內部日益龐雜與快速變化的資訊問題。由於企業網路可以提供下列優點而被我們所採用：

1.節省成本

就硬體設備而言，如果組織內原來已有網路設備，則可以在不需購置額外 的硬體設備下就開始建構企業內部的網際網路。就軟體投資而言,全球資訊網的瀏覽器或伺服器等軟體的價格遠比其它軟體低廉。

2.開放式標準與架構

網際網路與全球資訊網的技術是一種跨越平台的開放式網路技術，這也表示採用企業網路架構將擁有大量的軟體可供選擇，可增加日後網路系統的擴充能力。

3.容易使用，學習曲線低

使用者而言，簡單易學主要來自於跨平台能力的統合使用者介面 瀏覽器所帶來的好處，同時也間接的節省員工的訓練時間與成本；另外就系統開發人員的觀點來看，超文件註記語言(HTML)及其附屬支援的描述語言顯然是一個較簡單的圖形使用者介面之設計方式。

系統需求

本單位內部所使用之各種管理資訊系統、地理資訊系統、決策支援系統、…等已有二十年歷史。除了有特殊需求的系統，執行在工作站上外，大部份的資訊系統均設計在大型主機上執行。並且由於單位組織較大、任務繁多、使用者人數都在數千人以上，因此以任務爲導向的各大型主機系統幾乎都在獨立運作。決策者有鑑於各單位間資訊交流日益迫切，各系統間整合需求之必要，再加上網路系統已臻成熟，除了積極展開光纖網路主幹鋪設、制定各類交換標準等各種網路基礎建設，並配合行政院 NII 政策，成立 CSII 小組，羅致人才，統籌運作及推廣相關事務。本院系統需求說明如下：

1.高度的安全需求

安全對國防事業而言是最重要的課題.因此投資於安全防護工作的人物力成本往往遠超過一般民間企業.安全的考量遠高於效率的考量。

2.分散式處理之開放型架構

本院爲分散式處理,集中管理之組織架構,各組織下之應用系統在適型化時必須符合開放型架構。

3.安全暢通的資料流通網

雖然資料作分散式處理,但在開放型架構下仍需彼此交換,形成一資料流通網。

4.一致的人機介面設計

畫面不因系統之不同,而有不同之操作方式,以提供一致的人機介面及單一窗口。

相關技術

在系統建置初期，我們針對設計需求考量所有相關技術，在衡量成本面、技術支援面以及人員學習面等相關問題後，選擇適當的產品及相關技術。系統建置主要技術可分爲下列兩點說明：

1.資料庫與網頁連結技術

資料庫與網頁的連結是 IntraNet 中最重要的一環，由於企業的資料幾乎以資料庫的方式存放,並且原本 InterNet 上資料以目錄檔案管理的方式無法應付一般的企業行爲，例如交易買賣、人事薪資或庫存管理等。雖然以 CGI 程式可做一些雙向溝通，但仍無法像資料庫管理系統所提供的語言有效地查詢所需資訊。目前依市場上的各種解決方案，可粗分爲四大類：

- 撰寫 CGI 啓用資料庫
- 以範本檔案描述資料
- 以 API 連結

- SQL 嵌入 HTML 檔案

2.防火牆整合防毒牆技術

當電腦系統轉變到分散式的開放系統以後，重要資訊可以就近取得，就近處理，使電腦資料處理的成本降低了很多。然而，系統越開放，資訊越容易取得，安全上的潛在危機就越多。最常見的資料潛在危機有**「資料存取安全」**及**「資料內容安全」**,防火牆的架設通常用來防護資料存取安全,而掃毒程式則用來防護資料內容安全。針對以上兩大功能所設計之防火防毒牆，將是所有網路安全必須之裝置。

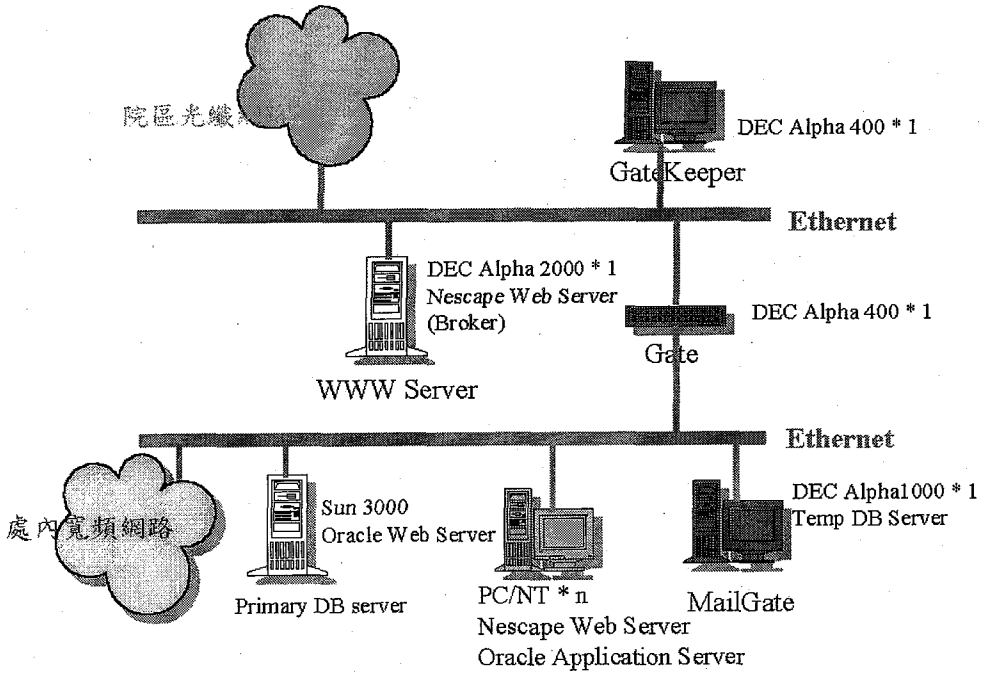
防火牆是由網路通道，網路保護者及郵件通道等三個系統所構成。網路通道負責封包之檢視及過濾內部網路與外部網路所有來往封包的功能，可有效控制其資料存取。網路保護者管制所有通訊軟體間對資料存取工作。郵件通道是爲網路安全管理的樞紐，記載所有在網路上各種活動記錄，並存有各種分析的工具。

防火牆基本上可以依各單位的機密等級需要可分成三種架構，其中最簡單之架構即利用一台伺服器作爲防火牆，此種方式是將網路通道、網路保護者及郵件通道等三個系統全部放在一台伺服器內，其能達到的功能有限，但具有其經濟性。第二種架構即利用二台伺服器作爲網路防火牆，此種方式可以較安全的保護網路的安全，因爲其中將網路通道及郵件通道二個系統放在同一台伺服器，有些功能無法達到。因此，對於機密等級要求較高之單位，則必須採取第三種架構,將各功能分別由不同的伺服器來執行以能真正保護到網路的安全。

並非所有系統均需全部功能，因功能愈多所需之電腦資源相對也是愈多，因此必須在安全及經濟上找到一最佳平衡點。

系統建置

本系統建置在一個以服務爲導向的子單位，必須提供全單位有關設施工程建造及維修、物料採購及管理等服務與諮詢，本系統則爲提高上述服務之品質而建置。因此我們將此系統命名爲**『遠端服務中心』**，定位在該子單位對全院之服務窗口，取其人性化之意，希望對使用者收親合力之效。以資料流的角度而言，『遠端服務中心』負責源自子單位外資訊的收集、來自子單位內各系統所提供之資訊的輸出，亦即子單位內外資訊之交流介面。『遠端服務中心』之系統架構如圖一，其中設計該架構特色有下列幾點：



圖一系統架構圖

I.防火防毒牆整合設計

爲整合電腦網路安全防護工作，我們在防火牆之第三層加入網路防毒功能，以使整個安全防護工作整合一致，便於使用及管理。建立一個完整的電腦網路安全防護系統工作可以從下列五個工作著手：

1.網路管理是整個安全防護之重點；

2.資料備份系統建立是最根本的資料安全防護的方法；

3.電腦系統及網路系統建立防毒系統；

4.資料加密在網路上傳輸；及

5.在網路上利用防火牆防止資料被竊取及防止非法進入系統破壞。

網路安全防護系統中含三個伺服器及防火牆軟體一套，整個系統架構如圖一所示。規格如下表：

1.	網路通道層	迷你主機(DEC α 400)
2.	網路保護者層	迷你主機(DEC α 400)
3.	郵件通道層	迷你主機(DEC α 1000)

	(內含防毒層)	
4.	防毒軟體	網路型防毒軟體 InterScan(趨勢科技公司產品)
5.	作業系統	最新版本 UNIX 作業系統 OSF/1
6.	網路安全軟體	高階防火牆軟體一套(Digital Firewall Service)
7.	防護功能	1.可隨網路環境的成長，使用者可彈性變動防火牆的設定。 2.支援 Hand-Held-Authentication 。該 Authentication 每次產生的密碼均不一樣 3.可定義其網路存取控制方式如下： 3.1 可規定內部網路與外部網路使用者均不能存取資料。 3.2 僅允許內部網路可存取外部網路的資源，而外部網路使用者不可進入內部網路。 3.3 可允許內部的網路使用者存取外部網路資源，而外部網路僅允許擁有 Authentication 的使用者方可進入內部網路存取資料。 4.模組化的設計，可依單位需求修改網路模組。 5.彈性的報表設計 6.本防火牆具有事件記錄功能(loggin)，並可將此事件記錄檔壓縮存放，使能節省其儲存空間。也可用時間限制或儲存空間百分比等方式來刪除其事件記錄檔。 7.具有將其事件記錄檔來產生報表(Report)的功能。報表上可看出 Total Connections 、資料傳輸量、 Connection 最長的使用者...等。 8.具有 Application Gateway 功能： Mail (SMTP), FTP, TELNET, WWW, NEWS,NNTP, Finger 。 9.具有 Name Service (DNS), Time Service (NTP) Service relays 的功能。

II.火線外的虛擬網站

我們認爲在開放式網路架構下，最安全的作法就是「將暴露在火線外的資料或程式降到最低」！因此我們在防火牆外利用一台主機以設置一個虛擬網站當作『遠端服務中心』之窗口，用來迎接到訪者。另外採取三個措施以維持正常的網頁服務：

1. 虛擬網站上，不放置任何有關使用者之資料庫或資料檔案，亦不放置任何網頁，以避免不當使用者或非法使用者之直接破壞。
2. 撰寫一支 Deaman，並安裝在虛擬網站上，配合主機一起運作。我們將該程式稱之爲「Broker」，專門負責接收到訪者之需求，通過防火牆的檢查並透過 DNS 找到真實的網頁網址，將網頁送達火線外的虛擬網站。
3. 將「Broker」備份在防火牆內，並定期重新載入，以確保真實的「Broker」正常運作。

III.火線內分散式實體網站

雖然網頁有美觀、易學易用的特性，但是存取效率往往受網路瓶頸及網站架構所影響。因此在建置時，我們不希望由於存取效率低落而將預期成果打折扣。在防火牆內的實體網站以實際業務區分，採分散式建置，每個實體網站上存有與該業務單位相關的網頁及應用程式，並且各網站又與共享之資料庫伺服器相連。利用這種分散式實體網站架構，可以將所有的到訪者按照其需求「虛擬安置」在網頁所在的網站上，而避免發生網頁服務過於集中在一個網站之壅塞情形。

火線內分散式實體網站是使用 PC/NT 爲 WEB 伺服器除了成本上的考量外易學易用易維護也是主要考量原因。PC/NT 亦擔任該業務單位的檔案伺服器 並負責 Printer Sharing 的工作。

IV.主要資料庫伺服器與暫存資料庫伺服器

防火牆內的資料庫伺服器是整體防護架構保護的重點。「安全」、「快速」與「穩定」是設計的重點。說明如下：

1.資料庫伺服器分爲主要資料庫伺服器(Primary DB Server) 與暫存資料庫伺服器(Temp DB Server),並分置於兩台獨立之主機。

暫存資料庫伺服器負責接收處外使用者尚未到案的業務申請資料，主要資料庫伺服器則負責貯存申請到案的資料,分置的原因是希望將龐大的申請者區隔以利主要資料庫伺服器的作業者順利執行業務。

2.主要資料庫伺服器擁有專用主機

由於在 IntraNet 中資料存取爲主要之交易行爲,爲避免將來大量的資料存取與過多的使用者人數引起資料庫伺服器的效率瓶頸。我們將主要資料庫伺服器所在的主機功能單一化,不負擔其他的伺服功能。

3.安裝安全等級爲 C2 之資料庫管理系統

在主要資料庫伺服器上安裝安全等級爲 C2 之資料庫管理系統是爲了防止合法人員的蓄意破壞或

資料庫管理系統本身突發性之意外發生。

在**網頁實作**部份，由於應用在 IntraNet 的網頁，其主要的功能仍然延續一般的資訊系統處理業務的特性，所以「快速」、「方便」仍是設計的主要訴求。因此，我們在製作網頁時，下列幾點是設計時考量的重點：

1. 網頁制式化

   捨棄一些動態圖形的展示或複雜的網頁背景,有別於 InterNet 上花俏的設計,呈現的是簡單清晰的作業畫面,並制定畫面之標準格式以供網頁維護人員持續發展。

2. 選擇適當的網頁製作工具

   由於在網頁設計上採取平實之風格設計,在網頁製作的工具上分爲兩類,

   其一爲不與資料庫連結的網頁製作工具,選擇簡單易用的流覽器編輯器,讓實體網站的維護人員容易上手製作該業務單位的網頁。

   其二爲與資料庫連結的網頁製作,因爲涉及與資料庫溝通及邏輯判斷等問題,我們必須從各種 WEB 應用程式語言中挑選其一。首先考量該語言與 WEB 伺服器軟體的整體運作再考慮開發人員對語言的熟悉度,因此我們配合 WEB 伺服器軟體選用該公司研發的第四代語言。該語言具有自動轉換成 HTML with Java Script 之程式碼之功能,可減少學習新語言之困擾。該語言亦用來開發其它非 WEB 之主從架構應用程式,預期將來能全面自動轉成 WEB 應用程式,而無重新撰寫之困擾。

3. 物件導向式資料輸入模式

   在設計與資料庫連結的網頁時,遇到要使用者輸入大量資料時,允許使用者暫存未完成的輸入資料。因此我們設計三個標準事件鈕(Event Button)於輸入畫面：

   一爲「暫存」,將輸入資料存入暫存資料庫,不作資料檢查動作。

   二爲「檢查」,僅對畫面上所輸入資料作檢查,不存入資料庫。

   三爲「完成」,先對畫面上所輸入資料作檢查,再將輸入資料存入暫存資料庫。

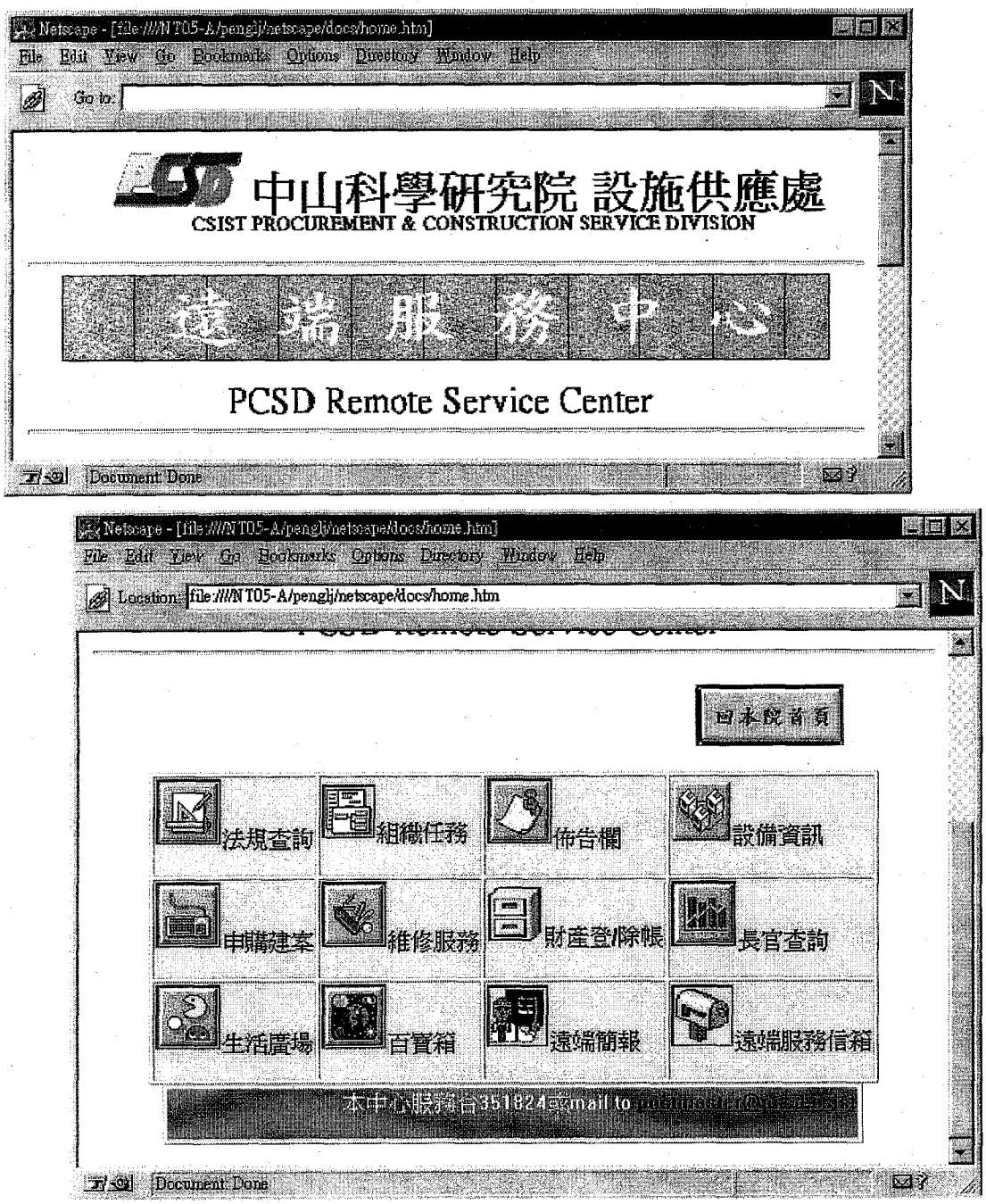
   如此設計可以讓使用者一次得到所有錯誤資料項(Data Item),並且予以暫存,以便有更多時間去尋找所需資料,而不必佔著一個客戶端(Client)之資源 。

4. 整合現有辦公室文書處理工具

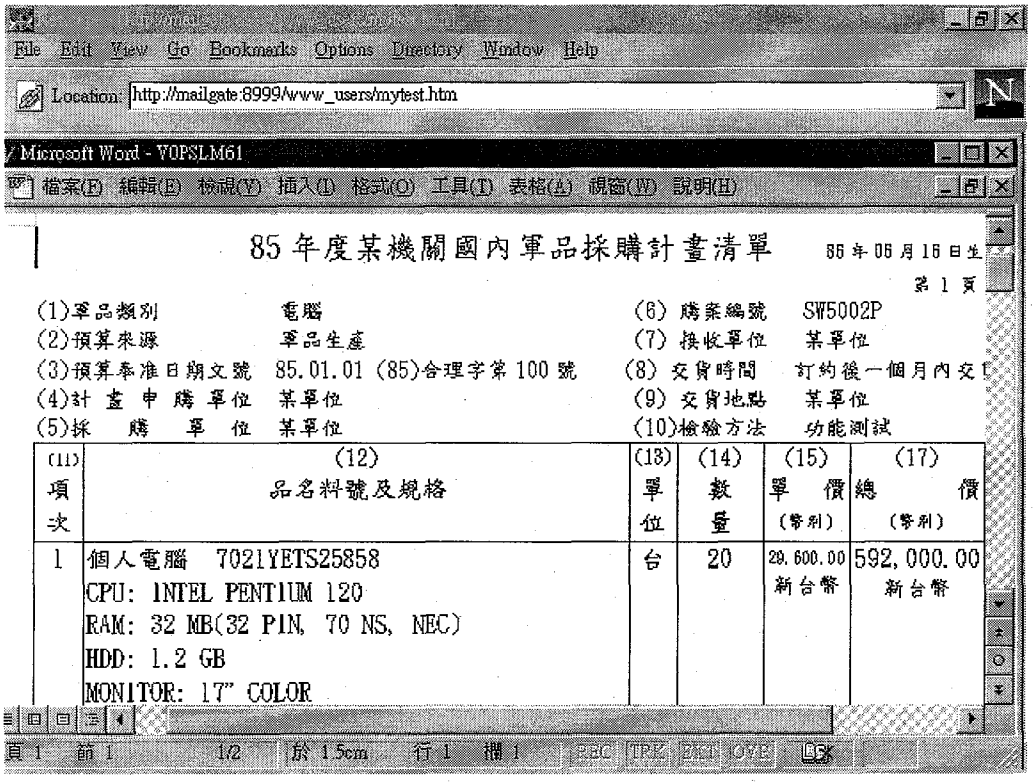
   由於國防事業仍使用許多複雜表格,因此將現有辦公室文書處理工具整合在網頁設計,並自動擷取後端資料庫之資訊作爲表格內容(如圖三)。一則保障現有投資,使用者仍然面對熟悉之辦公室文書處理工具,二則可減少開發項目。

5. 網頁設計生活化

提供與工作無關的生活化網頁,例如提供「中午訂便當」的網頁,以及「百寶箱」網頁提供個人之健康小偏方,正式書信用語及範例等。一方面可以吸引不願接觸電腦的人員,一方面由於輕鬆活潑的網頁設計,有舒緩工作壓力的作用。



圖二 遠端服務中心首頁



圖三 瀏覽器,文書處理與資料庫整合網頁

系統成果

整個系統的主要功能如圖二的網頁所示，可區分爲三大類：

1. 政令宣導類。包括法規查詢,組織任務,佈告欄,設備資訊等子類。
2. 資訊存取服務類。包括申購建案,維修服務,物料管理及長官查詢等子類。
3. 生活類。包括生活廣場,百寶箱,遠端簡報及服務信箱等子類。

預期的系統成果，說明如下：

1. 達成資料流通網目的。
   本系統因具有標準之主從架構及統一之文件格式(HTML),全院各單位之資訊窗口符合標準建置,即能利用此 IntraNet 網路系統達成資料交換的目的.
2. 提供安全的資料存取環境。
   防火防毒牆的整合架設,符合了國防事業對安全的高度要求.被授權的合法人員將在本院之資訊高速公路上合法暢行並各取所需。
3. 統一的人機介面。
   雖然不同的應用系統產生不同的資訊,但是本系統提供一致的服務窗口,使用者不再面臨多系統多操作的困擾。

4. 順暢的資料輸入方式。

網頁與資料庫連結後,由於畫面具有彈性化的設計,比一般視窗畫面更容易滿足需求,加上超鏈結(Hyperlink)的功能使得資料的存取更順暢。

5. 提高整體資訊化程度。

由於系統設計人性化,本系統除了提供方便的業務處理工具,取代紙面電話簿,行事曆,以Mail 取代留言錄,…,以及生活化的網頁,本系統已成爲員工之最佳工作伙伴。

問題與發展

可預期的是子單位間頻繁的資料交換及網頁服務勢必造成網路壅塞,因此良好的網路主體(NetWork Backbone)設計架構是系統成功的前提之一。

速率是層層的安全防護網所付出的代價。如何在高度安全需求下能將系統處理速率達到最佳化是本系統將來面臨的重要課題。我們希望隨著網際網路技術之日益精良,配合政府 NII 總體建設時程及各項標準,成爲國防軍事網及政府事業網之一環。

參考文獻

Simson Garfinkel and Gene Spafford, "Practical UNIX and Internet Security", O' Reilly & Associates, Inc. 1996.

Karanjit Siyan, Ph. D., and Chris Hare, "Internet Firewalls and Network Security", New Riders Publishing Indianapolis, Indiana. 1995.

王清佑，" 動悉 UNIX 網路與系統安全篇"，和碩科技文化有限公司， 1995.

沈碧容，" 網路安全手冊—企業應用篇" ， 和碩科技文化有限公司， 1996.

楊吳泉，" 現代密碼學入門與程式設計" ， 全華科技， 1996.

劉國昌、劉國興， "資訊安全" ， 儒林出版社， 1995.

張盛益、許美鈴， "電腦安全的威脅與對策" ， 資策會， 1995.

作者簡介

彭麗貞,元智工學院電機與資訊工程研究所碩士,中山科學研究院技士

魏 廉,前任中山科學研究院設施供應處處長,現任榮工處副處長

楊立達,中山科學研究院設施供應處處長