

有價證券全面無實體後
集保結算所資訊發展策略之探討

召集人：許 成

研究人員：陳鳳中、黃萬傳、黃治國、蕭傑元、
李 玲、梁碧雲、蘇鳳琪、姜文政、
朱靜怡、洪泰昌、張淑雅、蔣偉豪、
林志隆、林軒至、王志傑、張志偉、
張建明

臺灣集中保管結算所股份有限公司

中華民國 101 年 12 月

目錄

第一章 前言.....	1
第二章 資訊系統之基礎工程強化與更新.....	3
第一節 網路系統架構之整合與強化.....	3
第二節 電腦機房環境與機電設備之更新與強化.....	8
第三節 資訊系統備援機制研究.....	28
第四節 資料保存與備援機制.....	46
第五節 小結.....	57
第三章 應用系統之發展策略.....	59
第一節 業務系統之作業行為分類與整合.....	59
第二節 資料整合運用之研究.....	78
第三節 透過軟體工程提昇系統品質.....	90
第四節 中文字碼整合.....	98
第五節 資訊系統訊息交換方式之研究.....	112
第六節 資訊系統架構之發展策略.....	120
第七節 小結.....	175
第四章 資通安全機制之強化.....	177
第一節 內部資通安全機制之強化.....	177
第二節 外部資通安全機制之強化.....	203
第三節 小結.....	212
第五章 總結.....	214
參考文獻.....	217

第二章-第一節 圖表目錄

圖表 1.1.1	網路連線示意圖	4
圖表 1.1.3	IPv4 轉換 IPv6 之技術比較	7

第二章-第二節 圖表目錄

圖表 1.2.1	本公司機房實體環境設施現況之調查	12
圖表 1.2.2	實體環境設施與 TIA-942 標準對照	17
圖表 1.2.3	新版無風管冷氣機節能標章能源效率基準與標示方法表	25
圖表 1.2.4	舊版無風管冷氣機節能標章能源效率基準與標示方法表	25

第二章-第三節 圖表目錄

圖表 1.3.1	作業系統之備援情境	29
圖表 1.3.2	開放系統備援架構示意圖	32
圖表 1.3.3	DB2 HADR 示意圖	34
圖表 1.3.4	同地備援主機及 HyperSwap 示意圖	37
圖表 1.3.5	單主機平行處理架構示意圖	39
圖表 1.3.6	多主機平行處理架構示意圖	40
圖表 1.3.7	叢集式架構作業模式	42
圖表 1.3.8	DB2 PureScale 叢集式架構	43
圖表 1.3.9	雙中心同時作業示意圖	44
圖表 1.3.10	業界資訊系統備援機制架構	45

第二章-第四節 圖表目錄

圖表 1.4.1	大型主機備份架構示意圖	48
圖表 1.4.2	開放平台集中備份架構示意圖	50
圖表 1.4.3	光纖儲域網路示意圖	51
圖表 1.4.4	資料重複刪除示意圖	55

第三章-第一節 圖表目錄

圖表 2.1.1	本公司業務系統之範圍	60
----------	------------	----

圖表 2.1.2 各業務範圍對照之業務系統關聯	64
圖表 2.1.3 各業務系統使用單位與系統資料間之關係說明	74

第三章-第二節 圖表目錄

圖表 2.2.1 歷史資料調閱系統示意圖	79
圖表 2.2.2 IBM DB2 及 SYSDATABASE IQ 特性	83
圖表 2.2.3 異動資料擷取	84
圖表 2.2.4 資料複製：SQL Replicatio	85
圖表 2.2.5 資料複製：Q Replication	85
圖表 2.2.6 資料聯邦（Federation）	86
圖表 2.2.7 ETL/ELT（Extract，Transform & Load） ...	87
圖表 2.2.8 資料倉儲概念	88
圖表 2.2.9 資料倉儲概念	89

第三章-第三節 圖表目錄

圖表 2.3.1 IT 服務所面臨的新挑戰	91
圖表 2.3.2 IT 服務管理制度- ISO20000	92
圖表 2.3.3 IT 服務管理制度與程序及軟體工程應用對照 .	93
圖表 2.3.4 公司內部流程自動化現況	94
圖表 2.3.5 軟體工程應用	95
圖表 2.3.6 導入軟體工程自動化規劃策略	95

第三章-第四節 圖表目錄

圖表 2.4.1 台灣地區所使用的 BIG5 碼主要版本圖	98
圖表 2.4.2 各版本 BIG5 碼比較表	99
圖表 2.4.3 常見作業系統與編碼表	104
圖表 2.4.4 字型及字碼關係圖	107
圖表 2.4.5 開發平台架構圖	110

第三章-第五節 圖表目錄

圖表 2.5.1	「點對點式」的訊息交換	114
圖表 2.5.2	「點對點式」的優缺點	114
圖表 2.5.3	「EAI 式」訊息交換導入示意圖	116
圖表 2.5.4	「EAI 式」的優缺點	117
圖表 2.5.5	「EAI 式」的技術特性	117
圖表 2.5.6	「EAI 式」和「點對點式」訊息交換之差異	118

第三章-第六節 圖表目錄

圖表 2.6.1	IBM 大型主機發展大事紀	122
圖表 2.6.2	Unix/Linux 家族的發展	125
圖表 2.6.3	Windows 家族的發展年代圖	126
圖表 2.6.4	多工處理能力	128
圖表 2.6.5	多人使用環境	128
圖表 2.6.6	系統開放性	129
圖表 2.6.7	豐富的系統工具	130
圖表 2.6.8	程式可攜性高	131
圖表 2.6.9	網路環境	132
圖表 2.6.10	系統核心可變性	133
圖表 2.6.11	檔案格式一致性	133
圖表 2.6.12	核心系統轉換銀行列表	136
圖表 2.6.13	個案基本資料比較分析表	153
圖表 2.6.14	國外集保系統轉換經驗參考	154
圖表 2.6.15	資訊系統移轉人員問題及因應策略	156
圖表 2.6.16	個案資訊人員配置表	160
圖表 2.6.17	規劃示意圖	173
圖表 2.6.18	資訊服務導向	173
圖表 2.6.19	專案管理層面示意圖	174

第四章-第一節 圖表目錄

圖表 3.1.1	資通安全認證歷程	179
圖表 3.1.2	資通安全處理小組組織架構	183
圖表 3.1.3	資通安全事件通報及應變作業流程	184
圖表 3.1.4	資通安全處理小組通報程序	185
圖表 3.1.5	PDCA 循環	187
圖表 3.1.6	電腦主中心和異地備援中心資料的同步	188
圖表 3.1.7	BCP 組織圖	190
圖表 3.1.8	BCP 各組組織與權責	191
圖表 3.1.9	災害應變程序流程	193
圖表 3.1.10	資料外洩之諸多可能管道	196
圖表 3.1.11	端點型 DLP 的功能之一	197
圖表 3.1.12	端點型 DLP 的功能之二	198
圖表 3.1.13	區域網路傳輸加密示意圖	200
圖表 3.1.14	資料庫稽核工具	201

第四章-第二節 圖表目錄

圖表 3.2.1	本公司防火牆及入侵防禦配置	204
圖表 3.2.2	G-ISAC 交換情報種類與資安類型	211
圖表 3.2.3	本公司資安整體防護示意圖	213

第一章 前言

資訊科技發展與其他領域科技相比，是這五十年來發展最為快速的顯學，從真空管的電腦到積體電路的電腦，其運算速度成長可以說是完全按照摩爾定律，平均每二至三年成長一倍，以致於對人類文明產生的改變遠超過人類史上任何一階段，它成為人類有用的利器，運用在其它科學領域產生莫大助益，對於生活方便性與溝通性更是加速改善；而我們資訊人員不沉醉過去技術及經驗，對新知識及新技術永遠保持好奇和積極進取的心，在本次研究時以資訊使用與管理者角度進行探討，考量新技術如何運用於現行資訊環境，期望對於公司資訊未來發展能有所助益。

本次研究計畫參與同仁涵蓋集保公司資訊規劃部、金融資訊部及資訊作業部；適逢民國一百年台灣證券市場全面實施證券無實體化，雖然證券後台作業帳務處理早已資訊化，但因實體股票消失而全面以電子化方式儲存，對於大家心理面難免剛開始比較難適應，因此間接促使公司對於資訊品質的要求更勝以往，這是本次研究案起因，另公司資訊同仁亦借此機會對於公司整體資訊系統進行分類歸納，以此找出系統的差異性與共同性，並參酌資訊技術發展走向，來探討未來資訊方向，其原則不僅要符合使用者需求，更要探知新資訊技術如何加強資訊安全與提高系統穩定性。

此次範圍包含資訊系統基礎工程、資訊安全及應用軟體等三大範疇，已大致涵蓋所使用的電腦與周邊，該範圍就資訊管理者觀之，資訊系統建置因科技進步或廠商對產品中止維護而軟硬體更新外，主要是為配合市場業務發展需求進行

開發建置系統，在此狀況下資訊單位對於資訊建置步伐從未停止，隨著時間長河流逝，形成資訊系統陸續為處理不同商品，配合不同市場需要，在不同時間分別依不同作業機制建置不同系統，並提供多種類人機介面以便於使用者使用，就資訊管理者對整體系統與設備之觀察，已達到多種類多樣化狀況，但就維護而言亦是很大負擔，因此本次研究，我們針對現存各種系統與機制進行規納與分類，從當中選取有差異性或配合相關法規實施等因素，作為三大範疇之下各節研究之議題。

研究案參與同仁均在工作以外時間進行研究探討，或許有些研究內容比較不夠深入，但這份研究案目的是希望能藉由新技術降低人為疏忽機率、提昇異常狀況處理能力、加強資訊安全管理及提高資訊處理效能。可是在進行研究期間，適逢歐債風暴及美國財政懸崖問題，造成全球不景氣氛圍，對於研究結果是否要執行，可能需要考量成本效益及人力、物力、時間等調配問題，畢竟資訊運行與管理是長長久久，須全盤考慮以避免效益與成本不成比例造成財務負擔。

第二章 資訊系統之基礎工程強化與更新

第一節 網路系統架構之整合與強化

壹、研究目的與範圍

「資訊系統為現代企業營運之命脈」，自 2001 年 911 恐怖攻擊事件後，已經是企業的共識。但是資訊系統這個企業營運的大腦能否將有效的資訊提供給企業內外利害相關者，則有賴於正確安全的網路傳輸環境配合，方能長期順利運作。所以本案期望就本公司現有網路系統研究如何整合與強化，藉由新的技術與知識，讓整體資訊作業，達到“安全、效率、穩定”的企業目標。

貳、網路系統架構之現況

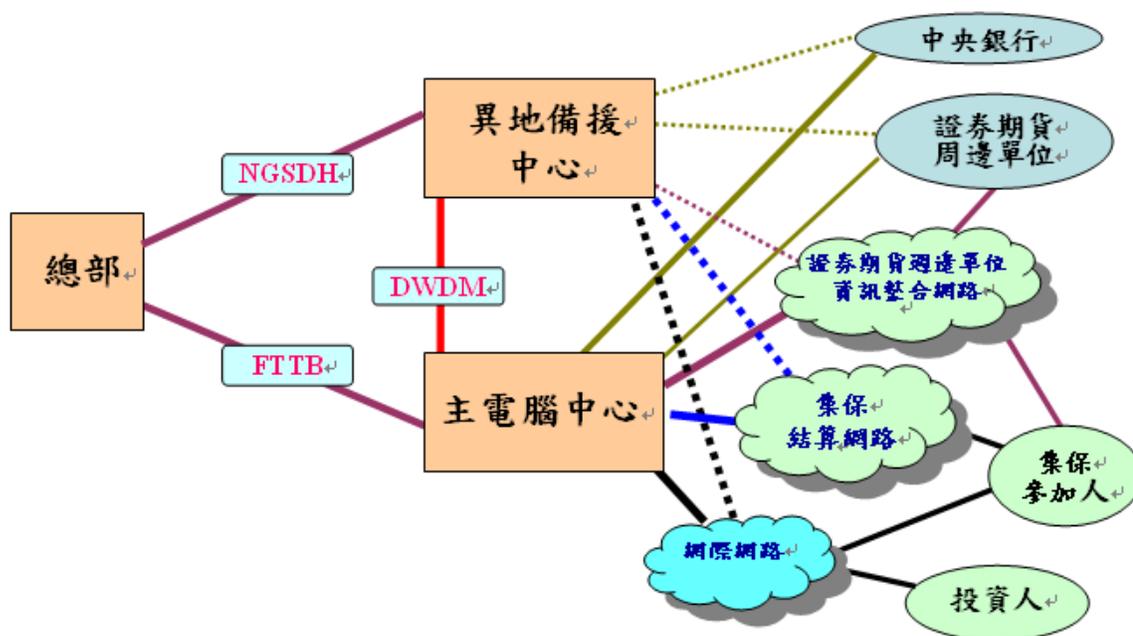
本公司有主電腦中心、業務與行政總部及異地備援中心等三個營運據點，三地分別租用電信業者提供之高速光纖網路連結，形成環狀網路架構，提供任一營運據點都有雙網路迴路，具備 IP 路由路徑備援之優點。

本公司主電腦中心對外備有多路加密寬頻光纖網路，供本公司參加人及周邊單位連結，辦理各項業務資訊系統連線作業。另外還建置網際網路(Internet)環境，提供網際網路相關系統連線服務，予投資人及本公司參加人連線使用。

異地備援中心為本公司各業務資訊系統之備援電腦中心，以 Dark Fiber (DWDM)與主電腦中心連結，滿足異地備援中心與主電腦中心各業務資訊系統，儲域及資料網路之橫向連結需求。除了是各業務資訊系統之備援電腦中心，同時

也提供各業務資訊系統研開測試環境暨業務演練環境，進行系統開發與測試。

本公司業務與行政總部主電腦主中心、異地備援中心三地連線及對外網路連線架構示意，詳見圖表 1.1.1



圖表 1.1.1 網路連線示意圖

參、未來發展策略之探討

一、網路拓樸優化

網路愈複雜導致交易資料流經網路節點愈多，對交易本身及網路系統效率有多項不利因素：

(一) 節點過多導致資料傳輸路徑增長，容易發生交易資料傳輸延遲，服務變慢的現象。

(二) 複雜網路不利於設備維運及連線障礙的除錯

網路拓樸愈複雜，一旦連線障礙發生，偵錯愈不容易，因為每一個網路設備節點都有失能的機率，然而障礙排除的時間過長，造成企業有形及無形的鉅大損失。

(三) 設備過多造成用電量增加，不合乎節能減碳的環保趨勢

如果優化網路拓樸，就成本效益考量有

1. 設備的整合集中化，提昇交易傳輸效率，縮短交易作業時間。
2. 參數設定和環境一致化，減少障礙影響因子。
3. 系統維運簡單化。
4. 維運費用降低。

但是就風險考量，需注意

1. 設備的備援，避免設備單點故障(single point failure)，導致網路系統失能。
2. 必須經過實際且審慎的實測評估，避免優化後之設備效能不足，反而成為網路傳輸的瓶頸，那就喪失優化的意義。

二、對外網路傳輸效率強化

現行本公司與參加人間連線傳輸電路規格以 ADSL 電路為主，ADSL 電路的下行速率高於上傳速率，適合資料查詢傳輸模式，為低速廉價電路，國內電信服務廠商提供的傳輸速率，最高為 8Mb/640kb，但是並未保證頻寬。

部分參加人使用專線電路(Leased Line)，因為使用大量資料交換傳輸交易，需要高速上傳速率，所以使用對稱式傳輸速率的專線電路，使用速率以 T1:1.544Mb 及 E1:2.048Mb 居多，費用較高，且無法彈性調整速率以因應臨時性的鉅量資料傳輸。

新一代的網路連線傳輸電路為 NGSDH 及 Metro-E (Ethernet over MPLS)，電路傳輸可靠度較專線電路及 ADSL 優，傳輸頻寬調整也比較有彈性。

未來本公司將持續推動新的應用服務，不管是頻寬或可靠度，這些新的應用服務會產生巨量資料的傳輸需求，比較不適合在 ADSL 電路上運作，而 NGSDH 或是 Metro-E 電路的可靠度及頻寬調整彈性都比專線電路更好，費用也相當，所以對外連線網路轉換為 NGSDH 或是 Metro-E 電路，是提昇傳輸效率的良好選擇。

三、IPv6通信協定導入

1980 年代初期 TCP/IP 標準確立，Internet 雛形出現，至今不過 30 餘年，Internet 連網運作關鍵元素，IP，已然耗盡，無法提供新的申請者使用，將衝擊產業與社會。為此，世界各大網路廠商、網路用戶與學術論壇聯手開發

新一代 IP 規格，IPv6，以替換舊有之 IPv4 定址規格，增加更多的網路位址讓有上網需求的使用者可以申請。

	優點	缺點
IPv4/IPv6 雙協定 (Dual Stack) 技術	<ol style="list-style-type: none"> 1. 設置容易 2. 維持原 end-end 連線模式 3. 雙協定主機可與 IPv4 主機、IPv6 主機、雙協定主機互連 	<ol style="list-style-type: none"> 1. 設備都須具備 IPv4 和 IPv6 位址，無法解決 IPv4 耗盡問題 2. 架構複雜，增加為運負擔 3. 純 IPv4 主機無法和純 IPv6 主機互通
穿隧 (Tunneling) 技術	<ol style="list-style-type: none"> 1. 維持 node-node 連線模式 2. 可利用原 IPv4 網路，成本低 	<ol style="list-style-type: none"> 1. 仍需要 IPv4 網路，無法解決 IPv4 耗盡問題 2. 增加網路負擔和維運複雜
轉換 (Translation) 技術	<ol style="list-style-type: none"> 1. 提供純 IPv4 主機和純 IPv6 主機互通 	<ol style="list-style-type: none"> 1. 轉換設備成為網路瓶頸點

圖表 1.1.2 IPv4 轉換 IPv6 之技術比較

第二節 電腦機房環境與機電設備之更新與強化

壹、研究目的與範圍

本公司之證券集中保管帳簿劃撥制度、期貨結算系統及票券保管結算交割系統實施之良窳，事涉數百萬投資人之權益，以及整體證券市場之運作秩序，且 100 年 7 月完成有價證券全面無實體化後本公司更逐漸轉型為資料中心，電腦作業系統是否正常運作，又為其中至為重要關鍵，提供高穩定及高效能之資訊運作環境實責無旁貸之責任，而電腦機房環境與機電設備需持續更新與強化更是必須持續辦理基礎作業。

95 年間因業務整併之作業需要，原票保公司與本公司整併為單一公司，於同年 6 月完成二個電腦主中心之整合作業，另同步規劃整併二異地備援中心，並於 96 年 2 月之農曆春節長假期間，將原有二個異地備援中心搬遷至主中心西南 70 公里 IDC(Internet Data Center)數據機房，作為本公司整合後之異地備援中心，至此開啟本公司對 IDC 機房建設之高規格要求及新一代機房基礎工程建設之認識。

稟承已往電腦機房建置經驗並期透過搜集本公司電腦機房實體環境現況，及因應綠色節能趨勢參酌現行業界在綠色科技之規劃與應用經驗，並利用新一代機房建設的策略對本公司電腦機房實體環境做現況分析與評估，提供本公司電腦機房相關實體環境設施運作檢討與改進措施，進一步更新與強化電腦機房環境與機電設備，以維持電腦系統穩定。

貳、機房環境現況說明

一、機房環境現況

100 年財團法人資訊工業策進會受本公司委託進行之「強化資訊系統因應重大災難之有效防禦評估與長期發展策略」研究時，曾對本公司主電腦中心與異地備援中心有關實體環境設施建置現況，進行了相關訪談與調查，其內容詳見圖表 1.2.1 本公司機房實體環境設施現況之調查。

項目名稱		主中心	異地備援中心
電力系統	市電系統	採電力需量契約容量 8200KW，由台電以特高壓 69KV 雙迴路方式供電。	由台電不同之兩變電所，提供雙迴路供電(FP23 饋線與 FQ09 饋線)，且互為備援，提高電力系統穩定安全。
	UPS 不斷電系統	1. 自備 UPS，採 N+1 雙套備援建置，備有 4 部 200KVA 等級之 UPS，兩兩互為備援之雙套備援建置，UPS 備載時間為滿載 30 分鐘以上。 2. 園區提供之 CPS 電力供應系統(1000KVA*2)。	採 N+1 架構建置，備有 200KVA UPS 2 部，電池組供電能力，可達滿載電量 30 分鐘以上。
	發電機組電力備援措施	1. 自備之 750KVA 發電機 1 部，儲油量 2700 公升，可連續運轉 30 小時。 2. 園區提供 2000KVA 發電機 3 部。 3. 機動型發電機租用。	採 N+1 架構建置，備有 750KVA 發電機 2 部，儲油量 12000 公升，可連續運轉 80 小時。

項目名稱		主中心	異地備援中心
	機架電源	採用雙迴路供應，每條電力迴路提供單相 120V、15A 電力	電力迴路具相互備援能力機櫃供應電源，採用雙迴路供應，每條電力迴路提供單相 120V、15A 電力，由發電機與不斷電系統提供備援電力。
	空調系統	採 N+1 架構建置，箱型冷氣 25 台，提供 24 小時恆溫恆濕之空調效果，冷房效果達 260RT。維持溫度攝氏 16-24 度及濕度 50%-70% 之機房環境。	機房提供 24 小時恆溫恆濕之空調系統，以無水機房理念建置，冷卻水系統隔絕於機房外部，採 N+1 架構建置，備有空調主機 4 部，冷房效果達 80RT。
	消防系統	採用 FM200 氣體消防系統，並採高架地板上下獨立分離，各自偵測啟動消防系統，並備有 16 個手提式氣體式滅火器。 早期偵煙系統安裝於機房天花板與高架地板下方，配有 20 個偵煙型感知器與 34 個偵熱型感知器。	保留大樓原有之 Inergen 消防系統，另建置機房專用 FE-13 高架地板上下獨立分離氣體消防系統。 建置 Vesda 極早偵煙系統，並於每個機櫃內設置取樣口。
	照明系統	採用每組 3 支 14W 之 T5 日光燈照明設備，並設有緊急停電狀況下之停電照明，及逃生指示燈，提供緊急狀況時使用。	採用每組 3 支 40W 之 T8 日光燈照明設備。各區之照明充足，並設有緊急停電狀況下之停電照明，及逃生指示燈，提供緊急狀況時使用。

項目名稱	主中心	異地備援中心
環控系統	<p>環境監控系統與機房內各安全系統結合，各安全系統之資訊及警訊，透過環控系統之網路與感測器，傳至環境監控電腦系統，提供機房維運人員由監控中心，對電力系統、UPS系統、發電機系統、空調系統、環境溫/濕度監控、漏水偵測系統、消防系統及機房門禁安全系統，進行遠端監控管理。</p>	<p>環控系統收納包含電力系統、UPS系統、發電機系統、空調系統、環境溫/濕度監控、漏水偵測系統、消防系統、極早偵煙系統及機房門禁安全系統。</p>
保全系統	<p>門禁管制電子卡片鎖與 CCTV 監控系統，24 小時監控機房全區的狀況。非機房人員進入，須登記進出資料，作為追蹤之用。</p>	<p>提供門禁管制及 CCTV 監控攝影，由 IDC 業主提供建物外圍 24 小時之保全服務。</p>
高架地板	<ol style="list-style-type: none"> 1. 每平方公尺可載重 500 公斤以上，並做斜支撐補強。 2. 蜂巢板之製作安裝，出風率達 10% 以上。 3. 高架地板下方有設備與通訊接地，來防止電磁干擾，高度在 30 公分以上。 	<ol style="list-style-type: none"> 1. 機房以鋁合金安裝，每平方公尺可載重 500 公斤以上，並做斜支撐補強。 2. 蜂巢板製作安裝，出風率達 10% 以上。 3. 高架地板下方有設備與通訊接地，來防止電磁干擾，高度在 30 公分以上(實際測量約 55 公分)。
防震系統	<p>藉由隔減震措施 ISO-BASE 防震設備，來降低地震輸入能量，並以螺栓等構件串連並排的機櫃，再以螺栓將上基座固定於高架地板的支柱，下基座底盤也同樣用螺栓固定於樓地板強化。</p>	<p>大樓為 RC 結構，防震係數達 6 級，重要系統主機與磁碟機之機櫃，裝設 ISO-BASE 防震設備，機櫃可因應芮氏 7.0-8.3 級地震，不致傾倒。</p>

項目名稱	主中心	異地備援中心
佈線方式	結構式佈線，資訊線路與電力線路皆於高架地板下方。	採結構式佈線方式，電力線架與資訊線架分開建置，電力線架建置於高架地板下方，資訊線架建置於機櫃上方。

圖表 1.2.1 本公司機房實體環境設施現況之調查

二、目前電腦機房建置之國際標準

隨著近年來機房實體環境相關的研究開發、規範標準、系統結構、功能應用、產品特性、材料工藝以及管理要求等諸多方面的衍變與發展，涉及機房工程的技術演變與發展趨勢呈現多維多態特性，另外隨著國際間環保意識抬頭，綠色機房就是在此節能風潮下衍生出來的機房概念，主要意指為符合低耗能、低碳排放、能源轉換效率等概念所設計的機房建置與管理方向等之新一代機房工程建設的理念與策略。

新世代機房設計以 TIA942 為基礎，針對電力、電信、建築、機械部份進行機房評估及改善檢討，輔以 Green Grid 聯盟及 LEED 評估標準作為綠色機房主要依循規範。

而機房的建置在 TIA-942 中隸屬於資料中心的子項目，其規範定義了空調、電力、消防、網路以及實體環境等各個層面，並且依據資料中心基礎設施的可用性（Availability）、穩定性（Stability）和安全性（Security）分為 4 個等級。第一級資料中心是最基礎的架構，不具有備援性（甚至沒有備用電源），而第四級資料中心架構具備多個通信、電源、空調設備系統及連接，擁有最高的容錯能力。

三、主中心及異地備援中心現況對應TIA-942標準之對照，詳見圖表

1.2.2 實體環境設施與TIA-942標準對照。

項目名稱		主中心	異地 備援中心	TIA942 作業要求	參照 條文
電力 系統	市電 系統	採電力需量契約容量 8200KW，由台電以特高壓 69KV 雙迴路方式供電。	由台電不同之兩變電所，提供雙迴路供電(FP23 饋線與 FQ09 饋線)，且互為備援，提高電力系統穩定安全。	提供雙迴路供電不同路由饋線的配置，並具有自動轉換電路斷路器或自動隔離旁路轉換開關。	5.3.6.1 5.4.8.12 G.5.2.3
	UPS 不 斷電 系統	1.自備 UPS，採 N+1 雙套備援建置，備有 4 部 200KVA 等級之 UPS，兩兩互為備援之雙套備援建置，UPS 備載時間為滿載 30 分鐘以上。 2. 園區提供之 CPS 電力供應系統 (1000KVA*2)。	採 N+1 架構建置，備有 200KVA UPS 2 部，電池組供電能力，可達滿載電量 30 分鐘以上。	<ul style="list-style-type: none"> 備援電源有兩種形式 UPS 和發電機。 UPS 系統需要能在停電時提供暫態切換，然後交由發電機繼續供電。 提供 100kVA 的 UPS 單元可以放置在機房內，但不能是加液型（需加水）的蓄電池，電池應該被詳細規定最少 5 至 30 分鐘的容量。 	5.3.6.2 G.5.1.5 5.4.8.1 3 G.5.1.3
	發電 機組 電力 備援 措施	1.自備之 750KVA 發電機 1 部，儲油量 2700 公升，可連續運轉 30 小時。 2. 園 區 提 供 2000KVA 發 電 機 3 部。 3. 機動型發電機租用。	採 N+1 架構建置，備有 750KVA 發電機 2 部，儲油量 12000 公升，可連續運轉 80 小時。	安裝的備用發電機系統，該備用發電機系統應該支援電腦房的加熱、通風和空調系統。備用發電機系統，機房之空調系統應該被連接到建築物的備用發電機系統。現場的燃料儲藏量應該是能提供發電機在設計負荷條件下運行最少 72 小時所需要的量。	5.3.5.2 .2 5.3.6.2 5.4.8.1 3 G.5.1.2

	機架 電源	採用雙迴路供應，每條電力迴路提供單相 120V、15A 電力	電力迴路具相互備援能力機櫃供應電源，採用雙迴路供應，每條電力迴路提供單相 120V、15A 電力，由發電機與不斷電系統提供備援電力。	提供雙迴路的排插座(120V 20A)，並自不同的 PDU 設備。	5.3.6.1
空調系統		採 N+1 架構建置，箱型冷氣 25 台，提供 24 小時恆溫恆濕之空調效果，冷房效果達 260RT。維持溫度攝氏 16-24 度及濕度 50%-70% 之機房環境。	機房提供 24 小時恆溫恆濕之空調系統，以無水機房理念建置，冷卻水系統隔絕於機房外部，採 N+1 架構建置，備有空調主機 4 部，冷房效果達 80RT。	資料中心必須維持空調系統的 24 小時運作保證，溫度應保持在攝氏 20 ~ 25 度之間，攝氏 22 度是最好的參考值。濕度必須控制在 40% ~ 55% 之間，露點不高於攝氏 21 度。	5.3.5.2 5.3.5.2 .1 5.3.5.2 .2 5.3.5.3
消防系統		採用 FM200 氣體消防系統，並採高架地板上下獨立分離，各自偵測啟動消防系統，並備有 16 個手提式氣體滅火器。早期偵煙系統安裝於機房天花板與高架地板下方，配有 20 個偵煙型感知器與 34 個偵熱型感知器。	保留大樓原有之 Inergen 消防系統，另建置機房專用 FE-13 高架地板上下獨立分離氣體消防系統，並建置 Vesda 極早偵煙系統，並於每個機櫃內設置取樣口。	必須按照 NFPA-75 來做消防系統和手執滅火器。機房的消防噴灑系統，應該是建物原有執行的系統。	5.3.7
照明系統		採用每組 3 支 14W 之 T5 日光燈照明設備，並設有緊急停電狀況下之停電照明，及逃生指示燈，提供緊急狀況時使用。	採用每組 3 支 40W 之 T8 日光燈照明設備。各區之照明充足，並設有緊急停電狀況下之停電照明，及逃生指示燈，提供緊急狀況時使用。	照明必須是在水平面最小 500 lux(50 footcandles)和在垂直面 200 lux(20 footcandles)，在機櫃之間的所有的通道中央，完成的地面以上 1m(3ft)處進行測量。	5.3.4.5 5.4.8.6 G.5.1.5

<p>環控系統</p>	<p>環境監控系統與機房內各安全系統結合，各安全系統之資訊及警訊，透過環控系統之網路與感測器，傳至環境監控電腦系統，提供機房維運人員由監控中心，對電力系統、UPS系統、發電機系統、空調系統、環境溫/濕度監控、漏水偵測系統、消防系統及機房門禁安全系統，進行遠端監控管理。</p>	<p>環控系統收納包含電力系統、UPS系統、發電機系統、空調系統、環境溫/濕度監控、漏水偵測系統、消防系統、極早偵煙系統及機房門禁安全系統。</p>	<p>機房門只提供給有授權的人員，所有的入口的監控措施應該提供測量功能，應該用微波探測系統和可視或紅外線閉路電視(CCTV)系統來防護。進入現場應該通過識別和授權系統來保證安全。</p>	<p>5.3.3 5.3.4.8 G.4.2.3</p>
<p>保全系統</p>	<p>門禁管制電子卡片鎖與 CCTV 監控系統，24 小時監控機房全區的狀況。非機房人員進入，須登記進出資料，作為追蹤之用。</p>	<p>提供門禁管制及 CCTV 監控攝影，由 IDC 業主提供建物外圍 24 小時之保全服務。</p>	<p>機房門只提供給有授權的人員，所有的入口的監控措施應該提供測量功能，應該用微波探測系統和可視或紅外線閉路電視(CCTV)系統來防護。進入現場應該通過識別和授權系統來保證安全。</p>	<p>5.3.3 5.3.4.8 G.4.2.3</p>
<p>高架地板</p>	<p>機房以合金鋼安裝，每平方公尺可載重 500 公斤以上，並做斜支撐補強。蜂巢板之製作安裝，出風率達 10% 以上。高架地板下方有設備與通訊接地，來防止電磁干擾，高度在 30 公分以上。</p>	<p>機房以鋁合金安裝，每平方公尺可載重 500 公斤以上，並做斜支撐補強。蜂巢板製作安裝，出風率達 10% 以上。高架地板下方有設備與通訊接地，來防止電磁干擾，高度在 30 公分以上(實際測量約 55 公分)。</p>	<p>最小的底板載重能力必須是 7.2 KPa(150 lbf/ft²)。推薦的底板載重能力是 12KPa(250 lbf/ft)</p>	<p>5.3.4.7 5.4.8.1 4</p>

防震系統	藉由隔減震措施 ISO-BASE 防震設備，來降低地震輸入能量，並以螺栓等構件串連並排的機櫃，再以螺栓將上基座固定於高架地板的支柱，下基座底盤也同樣用螺栓固定於樓地板強化。	大樓為 RC 結構，防震係數達 6 級，重要系統主機與磁碟機之機櫃，裝設 ISO-BASE 防震設備，機櫃可因應芮氏 7.0-8.3 級地震，不致傾倒。	電腦機房應考慮潛在的振動問題，並設計安全的措施來防止過多的振動。	5.3.5.5
佈線方式	結構式佈線，資訊線路與電力線路皆於高架地板下方。	採結構式佈線方式，電力線架與資訊線架分開建置，電力線架建置於高架地板下方，資訊線架建置於機櫃上方。	NA	NA

圖表 1.2.2 實體環境設施與 TIA-942 標準對照

從以上對照表來看，主電腦中心與異地備援中心其相關實體環境設施建置現況，經 TIA-942 標準評估後，為接近 Tier IV 之資料中心。

參、未來發展策略之探討

一、建立本公司電腦機房建置標準

在參考 TIA-942 資料中心建置要求及規範、本公司歷年來建置機房評估資料、中華電信 IDC 機房建置要求及 Green Grid 及 LEED 評估標準等。羅列出未來本公司進行「兩地三中心」電腦機房建設時規劃原則與方向，其分別為地點的選擇、建築物的要求、基礎建設的需求等，茲陳述於后：

(一)地點的選擇

1. 同地備援中心應與主中心位於相同都會區相距 10 公里內。
2. 同地備援中心應與主中心間交通應便捷，不易產生阻隔或斷絕，中心間車程半小時內。
3. 應遠離水災自然災害危險區，無淹水記錄。
4. 應遠離地震自然災害危險區，台灣地震危害度應為第一區。
5. 應遠離人為災害危險區，鄰近 1 公里內無軍事基地、化工廠、機場、車站等。
6. 遭受人為惡意攻擊或破壞致影響資訊作業安全之可能風險評估。

(二)建築物的要求

1. 應為電腦機房專用綠建築大樓自然光源充足、大樓產權應自有或獨立，並具專屬電信機房，大樓週遭環境單純。機房隔間採鋼板隔間，天花板則為金屬天花板，所有建材皆符合消防法規防火一個小時以上。
2. 大樓屋齡應為 15 年以內、建築物為 RC 混凝土或採 SRC(鋼骨+鋼筋混凝土)等以上結構等級，各樓層皆進行強化樑柱工程。
3. 建築物耐震度至少七級以上(在地震區 0、1、2，按地震區 3 的要求；在地震區 3 和 4，按地震區 4 的要求)。內部設備均加強定位設備(重要系統主機與磁碟機之機櫃，裝設 ISO-BASE 防震設備，機櫃可因應芮氏 7.0-8.3 級地震，不致傾倒)，以達防震效

果。

4. 樓高至少 4.5M 以上，可配合電腦設備高度、高架地板、消防、網路及電力線路等管線上下分離需求。
5. 樓板載重最好 7.2 KPa (150 磅/平方英尺，約為 732 公斤/平方公尺)。
6. 大樓供水狀況應有儲水量 14 天以上，並可提供緊急供水來源。

(三)基礎建設的需求

1. 機房門禁管制

- (1) 機房大樓產權必須自有，出入口設 24 小時專職保全人員，負責過濾人員進出及安全巡邏。
- (2) 電梯設置門禁卡管制，電腦紀錄出入人員及時間。
- (3) 機房入口獨立門禁管制(最好設有生物辨視系統)，並設專人管制機房進出人員身份及設備。
- (4) 必須至少四道門禁嚴格管控。
- (5) 於機房出入口、電信室及機房內部…等區域，設置無死角智慧照明 CCTV 監視點，24 小時進行監控錄影，CCTV 監控錄影以數位資料儲存、儲存期至少 90 天，可根據問題時間點進行調閱。
- (6) 機架上鎖，機架門鎖統一控管。

2. 機房電力

- (1) 台電供電採雙路由機制供電，且互為備援並與其他中心不同路由，提高電力系統穩定安全。
- (2) 需有發電機與備援發電機作為備援，採 N+1 架構，第二備援電力系統採用至少 1000KW(含)柴

油發電機N+1台並聯，儲油量可滿載運轉96小時以上。

(3)UPS採N+1套備援建置，且需採雙迴路高效率模組式UPS，在負載25%時即可達95%的高效運轉，輸入諧波電流也控制在3%以下，達到國際性綠色機房的水準。

(4)UPS備載時間為滿載30分鐘以上。

(5)電力需有自動切換系統。

(6)雙管道間可於單一管道間發生問題時提供備援方案。

(7)機房需有專職機電人員並提供專職機電值班人員7*24小時輪班。

(8)電源規劃依據美國電信產業協會TIA-942 Tier IV規範標準建置，提供雙迴路的電源。

3. 機房空調

(1)採用低能耗空調冷卻系統並有不同主機(水冷式、氣冷式)N+1套作為備援並提供恆溫恆濕下吹式系統。

(2)採用分區設置空調系統及搭配完整冷熱通道規劃，排除以往傳統冷熱通道混風造成降低冷房效果之狀況，達到節能減碳綠能機房目的。

(3)必須配置熱交換系統，將機房內熱氣與室外冷空氣對流。

(4)空調電源採雙路由，且所有空調系統均接至緊急電源(發電機)。

(5)中央電腦監控24小時專人監控，視當時環境溫

濕狀況進行遠端操作。

(6) 機房內最佳溫度攝氏 18°C - 27°C。

(7) 相對溼度 45% - 75%。

(8) 機房空調需達每坪一噸之標準。

4. 環境監控

(1) 環控系統範圍：須包含以下環境監控系統

- a. 電力
- b. 空調系統
- c. 消防
- d. 門禁
- e. 發電機
- f. 溫溼度
- g. 監視等系統

(2) 監控項目包括：只要在監控範圍內所有系統於發生故障時，皆必須能於管理中心之監控螢幕上產生告警通知，以確保電腦機房設備運作之安全。而其監控項目至少應包含以下三項…

- a. 異常告警
- b. 維修旁路
- c. 系統異常
- d. 系統告警通知：系統必須自動發送簡訊或電子郵件之方式，立即通知對應工程師處裡。

5. 消防設施

(1) 必須按照美國國家防火協會NFPA75規定來施做消防系統，機房內部皆備有FM-200海龍消防及自動排煙系統和手執滅火器。

- (2) 消防警報系統採用偵煙及偵熱雙迴路系統，以確保火警感知器正確性，並建置極早偵煙系統，於每個機櫃內設置取樣口。
- (3) 消防系統設備採用分區安裝及分區動作。
- (4) 滅火設備動作時需有延遲時間(~30sec)。

6. 高架地板

- (1) 採用鋁合金系列高架地板，樓地板荷重為1000Kg/m²，高壓地板載重約500Kg/m²。
- (2) 高架地板採蜂巢板製作按裝，蜂巢板出風率達16%。
- (3) 高架地板離樓地板高度60 CM以上，可配合消防、網路或電力線路等管線建置需求。
- (4) 防火要求：符合美國國家防火協會「NFPA-75」標準。

7. 其他硬體需求

- (1) 機櫃標準化依耗電負載高低分散機櫃設置。
- (2) 機房燈具採用CCFL或LED燈具，這類型燈所產生的熱能很低，溫度大約只有45度以下，不會帶給機房空調更多地負擔。
- (3) 每月定期提出機櫃電力使用報告，以避免使用過量造成電力超載跳電。
- (4) 機架電源提供雙迴路的排插座(120V20A)，並來自不同的PDU設備。

二、主電腦中心機房環境及機電設備之更新

主電腦中心自 90 年建置完成啟用至今，相關電腦機房環境之空調設備及機電設備使用時間已超過 11 年，設備漸邁入老化在運作上較易趨向不穩定且耗電越趨嚴重，然本公司電腦作業系統是否正常運作，事涉數百萬投資人之權益以及整體證券市場運作秩序致為重要關鍵，因此如何強化電腦機房環境與機電設備、節能減碳，持續提供本公司各業務資訊系統高穩定及高效能之資訊運作環境，實為重要課題。

為使重要機電設備都能恆久正常運轉，保障各項機電設備使用安全無虞。故洽請聯安機電顧問公司檢視目前本公司機房中建置之高壓、低壓機電設備，與相關零配附件、電力插座、電力線、配電盤、電容器、電力開關等有關設備，並提出「機電設備及電力電纜使用年限建議書」，本公司爰依建議增列各項機電設備與有關零配件之使用年限，除零配件原則上均須定期汰換外，當設備超過使用年限，但因保養得宜仍可正常使用者，將請專業廠商進行評估，評估合格且臨時故障不致有重大影響則續用，若經評估已不堪使用、或雖仍可使用但臨時故障，將造成重大影響者，則予以汰換，以確保本公司電腦機房機電作業之安全，其相關規劃項目如下：

(一) 規劃項目

1. 機電設備

(1) 緊急發電機

(2) 不斷電系統(UPS)

2. 機房環境

- (1) 空調系統
- (2) 熱顯影設備購置
- (3) 消防系統
- (4) 環境監控系統

(二) 效益分析

1. 機電設備的汰換更新效益

汰換更新發電機並將電壓提升至高壓系統供電此舉可減少線路損失，增加供電效率。而將發電機組之容量依現況及未來業務需求調整提升(750KVA=>1000KVA)，則可確保提供重要負載之緊急備用電力無虞。而增設之高壓同步自動切換開關具(C. T. T. S)功能，將能解決原ATS在切換回台電時會發生二次斷電之困擾，且當高壓自動切換開關盤或升壓變壓器故障時，可藉由新設的發電機組緊急備援迴路將電力送至5F機房，提升緊急備用電力之可靠度。另配合改善發電機室通風散熱系統後，可避免因通風量不足，導致發電機組過熱輸出容量下降或停機等問題發生，且同時將發電機房內部之狀態整合至中控中心的環控系統，使監控人員能完全掌控緊急備用系統之狀況。

2. 機房環境設備的汰換更新效益

(1) 空調系統

汰換過老的冷卻系統，投資效用最明顯，以汰換使用超過11年的機房冷氣系統預估電費將不增或減，而系統總冷卻能力可提高6成以供更多冷卻需求。因機房冷

氣系統設置的時間過久，其設備設置當時的效能基準業已提昇，例如最新的無風管冷氣機節能標章能源效率基準與標示方法於98年8月10日公告修正實施如圖表

1.2.3，前次的舊基準為96年7月10日公告修訂96年8月1日起實施如圖表1.2.4：

機種		冷氣能力分類 (kW)	能源效率比 (W/W)
氣冷式	單體式	2.2 以下	3.30
		高於 2.2，4.0 以下	3.35
		高於 4.0，7.1 以下	3.10
		高於 7.1，10.0 以下	3.05
	分離式	4.0 以下	3.85
		高於 4.0，7.1 以下	3.55
高於 7.1(冷氣能力 70 kW 以下機種)		3.40	
水冷式、蒸發式		全機種(冷氣能力 70 kW 以下機種)	4.80

圖表 1.2.3 新版無風管冷氣機節能標章能源效率基準與標示方法表

機種		冷氣能力分類 (kW)	能源效率比 (w/w)
氣冷式	單體式	2.2 以下	3.15
		高於 2.2，4.0 以下	3.20
		高於 4.0，7.1 以下	3.00
		高於 7.1，10.0 以下	2.95
	分離式	4.0 以下	3.45
		高於 4.0，7.1 以下	3.20
高於 7.1 (冷氣能力 70 kW 以下機種)		3.15	
水冷式、蒸發式		全機種 (冷氣能力 70 kW 以下機種)	4.25

圖表 1.2.4 舊版無風管冷氣機節能標章能源效率基準與標示方法表

一般而言以水冷式項目比較由舊基準4.25提昇為4.8，EER值提昇了0.55，以提供相同的冷氣能力時新基準冷氣空調在用電可以減少

11.4%(1-4.25/4.8)，因此選用EER高的新設備可以減少用電，當電腦機房設置很久的冷氣系統其EER值與新冷氣系統有顯著差異時，為求節能省電汰換更新冷氣空調系統成為要務，可以減少持續運轉的長期費用。

新採購R407C的制冷系統環保設計之精密電腦機房空調機組，除具高顯熱設計能提供理想的溫濕度環境(溫度20-25℃，相對濕度40%-55%)。採多種聯控模式可根據機房現場情況進行選擇，以實現節能和降低空調系統的總擁有成本；採用高效(EC)風機比普通風機節能8%-10%；內部設計”V”型蒸發器在有限的空間內增大換熱面積，可降低10%-15%的能耗，提昇冷房效能達成節能環保目的。

(2)紅外線熱顯影設備

紅外線熱像儀主要用於電力相關設備的活線檢測與診斷，亦即在不斷電的狀態下，利用紅外線熱像的成像技術，進行電力設備的熱狀態檢測掃描，檢測電力設備接點有無過載或過熱之異常溫度升高情況，造成接點接觸不良或是絕緣材質正在破壞中，並依受測設備的構造特性解讀設備的發熱現象，以判斷設備是否異常、其異常位置與原因及可能的危害程度，進而能有計畫、有目的地進行維護工作。如此不僅能降低設備的檢修費用，減少設備過度維護衍生之問題，更可避免因設備非預期性失能所衍生的損失。

最終期望搭配機電設備、不斷電系統(UPS)及空調系統等汰換更新，能有效節約用電與費用支出，並能保障各項機電設備使用安全無虞，持續提供本公司各業務資訊系統高穩定及高效能之資訊運作環境。

第三節 資訊系統備援機制研究

壹、研究目的及範圍

考量公司的永續經營，當於發生天災、人為疏失或惡意破壞等相關情形而造成資訊系統損害時，能以最短時間快速回復正常營運作業，為當前刻不容緩的課題。因此各業務資訊系統同地暨異地備援機制之建置，及完整災害復原計畫，並持續的維護、管理與演練，以確保備援機制的有效性及正確性，為現階段企業重要之課題。

自 90 年於美國發生 9/11 恐怖主義攻擊事件、92 年全球 SARS 病毒侵襲事件及 99 年 12 月國內某公司資訊機房火災事件等相關事件，引起大家對「如何避免資訊中心同地備援設備與正式營運設備同時無法使用」議題之熱烈探討；為保障同地備援設備投資之有效性，資訊架構中長期應如何因應之研究，目前國內已有多家大型企業、金融機構正進行研議規劃建立其兩地三中心之機制，以另確保其資訊中心作業永續作業安全，並能提升對客戶服務品質，另強化現行資訊系統服務不中斷，研議兩地三中心資訊服務架構，為未來強化本公司資訊服務架構研議之方向。

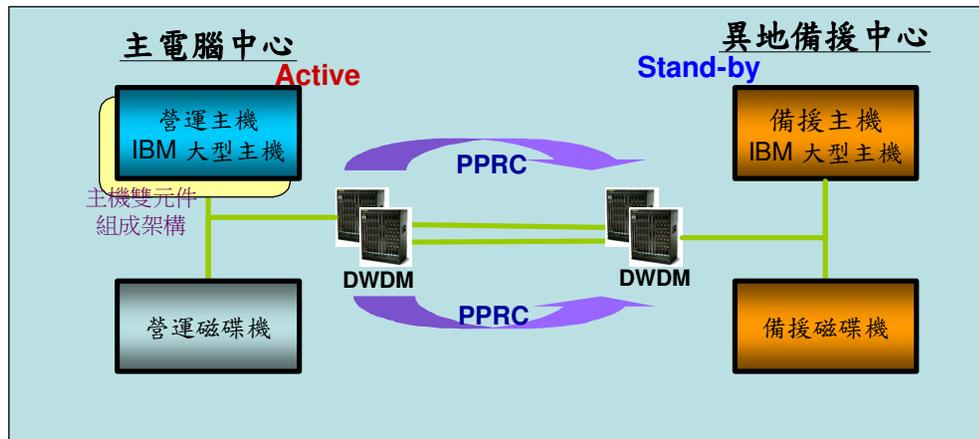
本次研究範圍以本公司各業務資訊系統為資料搜集對象，包括存託、SMART、Internet、基金、BCSS、風控、e_Report、交易所 TCPIP、Siris、Report、期貨、CRM、收費、MIS 等系統。

貳、資訊系統備援機制現況說明

一、大型主機現行架構

(一) 作業系統層面：

本公司現況之大型主機 z/OS 作業系統，係以 ACTIVE / STANDBY 模式 (A/S Mode) 作為系統備援機制；透過 DWDM 設備之高速光纖網路連線，及 PPRC 即時同步機制(詳如圖表 1.3.1)，可運作復原作業操作程序，完成下列作業系統之備援情境：



圖表 1.3.1 作業系統之備援情境

- 1、現況營運環境之大型主機，其重要硬體元件組係採用雙元件之組成架構，故當其中某一元件發生異常，或需要維修更換時，不致影響當下之系統正常運作。
- 2、主電腦中心端之營運主機(即 ACTIVE 主機)發生異常致作業系統無法運作時，可啟動異地備援中心端之備援主機(STANDBY 主機)，連結主電腦中心端之磁碟組，即可回復 z/OS 作業系統之運作。

- 3、主電腦中心端營運主機作業系統所使用之磁碟 (ACTIVE 磁碟)，發生異常致作業系統無法運作時，營運主機可啟動異地備援中心端之作業系統磁碟 (STANDBY 磁碟)，即可回復 z/OS 作業系統之運作。
- 4、主電腦中心端營運系統所使用之營運主機及營運磁碟 (即 ACTIVE SITE)，均發生異常致無法運作時，可啟動異地備援中心端之備援主機及備援磁碟 (即 STANDBY SITE)，即可回復 z/OS 作業系統之運作。

(二) 非作業系統層面：

現況「非作業系統」層面之備援機制，可針對大型主機之中介軟體 CICS、資訊庫軟體 IMS/DB，以及應用程式 (即 Application，以下簡稱 AP)……等三個部份來說明，分述如下：

1、中介軟體 CICS：

本公司運作於大型主機之應用系統為「證券存託系統」，而其線上交易 (OLTP; On Line Transaction Processing) 及交易運作所需之資源控制，係透過中介軟體 CICS 進行管控。

「中介軟體」係指介於「應用程式」與「作業系統」之間之軟體，故 CICS 的系統備援，亦可分為兩個部份；其偏向作業系統面之備援可直接與作業系統之備援方式結合，意即上述作業系統備援機制運作時，即包含中介軟體之系統層面備

援；另一部份則是與中介軟體本身運作有關之備援機制，例如：log、cold start、warm start……等，而這些則需仰賴中介軟體本身之備援啟動程序，例如：CICS 之 Emergency 啟動程序。

透過上述中介軟體兩個部份的備援機制，當系統面臨因故中斷之重新啟動，或是因災難發生而需啟動 STANDBY 環境時，即可進行相對應的備援程序，以回復中介軟體之運作，並確保交易狀態之一致性。

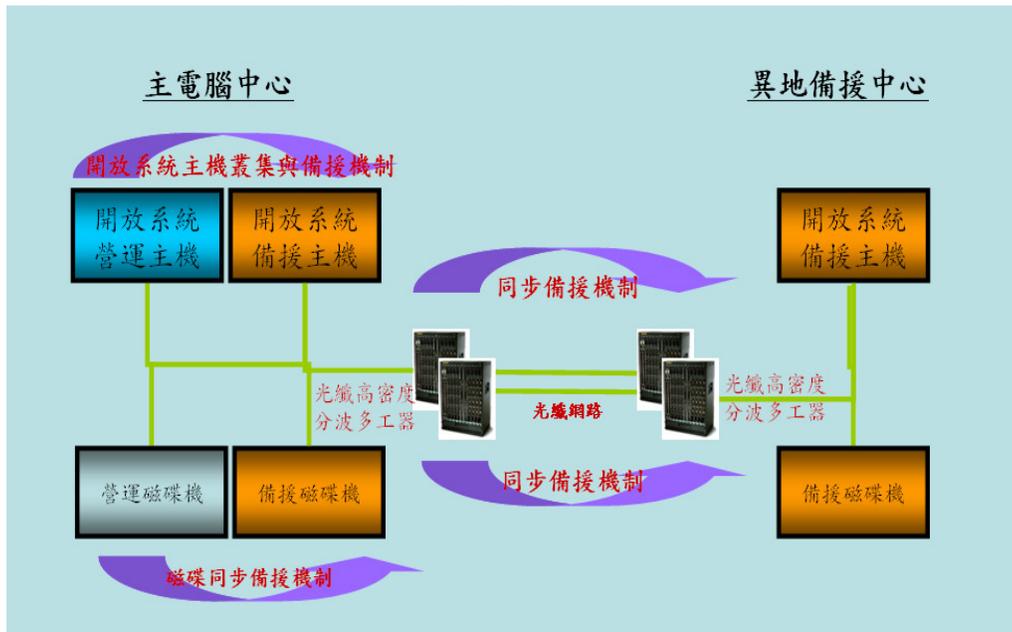
2、資料庫軟體 IMS/DB

「證券存託系統」之交易資料，除以 VSAM 檔案型式存放之外，亦有部分營運資料存放於階層式資料庫-IMS/DB 之中。

因階層式資料庫 IMS/DB 的資料結構，係以有之 ESDS 資料檔為 DATA 存放的基礎，再加上 RECON(即資料庫設定參數檔)、Active/Archive log、PSB GEN、DBD GEN……等重要核心檔案，均以標準 MVS 檔案存放於作業系統中，故資料檔部份之備援機制，直接搭配作業系統之備援機制即可；然而，當 IMS/DB 因任何異常原因，需重新啟動時，為確保資料庫中 DATA 與 archive log 紀錄之一致性，仍須進行相對應之啟動程序，例如：COLD START、EMERGENCY START……等。

二、開放系統主機現行架構

本公司現況之開放主機作業系統，同地備援機制係運用高可用性 HACMP 方式建置，異地備援機制係運用 PPRC 即時同步方式建置，AIX 作業系統資料則運用資料 MIRROR 機制達到備援目的(詳如圖表 1.3.2)，以上列備援機制完成下列作業系統之備援情境：



圖表 1.3.2 開放系統備援架構示意圖

- (一) 現況開放系統營運環境之主機，其重要硬體元件組係採用雙元件之組成架構，故當其中某一元件發生異常，或需要維修更換時，不致影響當下之系統正常運作。
- (二) 主中心端之開放系統營運主機(即 ACTIVE 主機)發生異常致作業系統無法運作時，系統自動偵測並啟動 HACMP 機制，同地備援主機(STANDBY 主機)接管正式

營運主機之網路及資源之設定，即可回復作業系統之正常運作。

- (三) 主中心端之開放系統營運主機作業系統所使用之磁碟機(ACTIVE 磁碟)發生異常時，由於開放系統之作業系統資料均為鏡像複製(MIRROR)，同時有二份資料運作，因此不影響系統之運作，待磁碟機修復完成後，重新複製 MIRROR 資料即可。
- (四) 主中心端之開放系統營運系統所使用之營運主機及營運磁碟(即 ACTIVE SITE)，因天災或其他意外事故發生異常致無法正常運作時，可啟動異地備援中心端之備援主機及備援磁碟機(即 STANDBY SITE)，即可回復開放系統平台作業系統之運作。

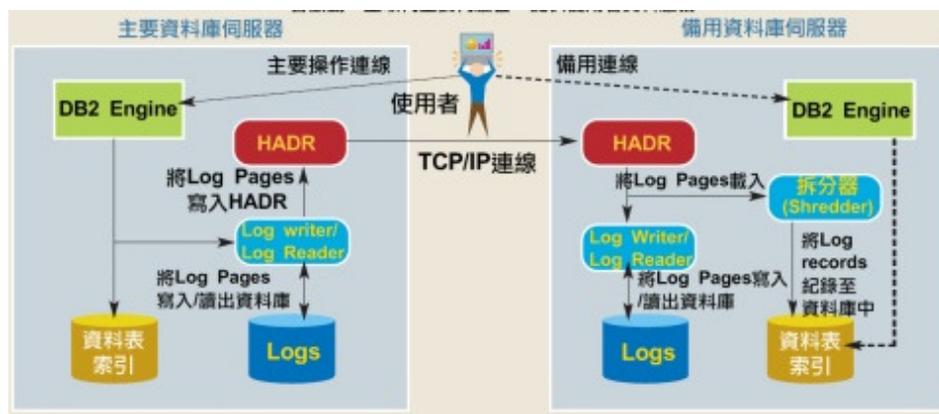
三、開放主機中介軟體

本公司現況之開放主機作業系統中介軟體備援方式，主要配合高可用性叢集式架構 HACMP(ACTIVE/STANDBY)備援方式，以及負載平衡叢集式架構 LOAD BALANCING CLUSTERS (ACTIVE/ ACTIVE)。

- (一) 現況本公司各業務系統所使用之中介軟體主要包括 WebSphere Application Server(WAS)、IBM Http Server (IHS)、WebSphere MQseries (MQ)、DB2、WebSphere Message Broker (MSB) 等，整體架構使用均配合各業務系統規劃架構配合建置。
- (二) 本公司各業務系統若使用 HACMP (ACTIVE /STANDBY) 備援方式，中介軟體備援機制將配合系統自動偵測並

啟動 HACMP 機制後，由同地備援主機 (STANDBY 主機) 接管正式營運主機，各中介軟體服務也同時切換至同地備援主機 (STANDBY 主機)，建置方式主要將中介軟體安裝於企業級磁碟機 (Enterprise DISK)，使啟動 HACMP 機制時，安裝於企業級磁碟機之中介軟體能確實由同地備援主機接管。

(三) 本公司業務系統採行負載平衡叢集式架構 Load Balancing Clusters (ACTIVE/ ACTIVE) 者，主要為 Web Service 類型之業務系統，其系統架構為三層式架構，更分為 Web、AP、DB，Web 伺服器主要藉由 IHS 提供 Http 的連結需求 (request)，Http 連結需求透過網路設備分流至不同的 Web 伺服器，Web 伺服器再將 Http 連結需求轉至 AP 伺服器，而 AP 伺服器配置方式主要將應用伺服器建置為 Cluster 架構，也就是將 AP 伺服器裡的 WAS 建置為 Cluster 架構，使 Cluster 架構下的應用系統能各自隨機接收前端 Web 伺服器的 Http 連結需求，最後 DB 部分則分為使用 DB2 HADR 機制 (參見圖表 1.3.3)



圖表 1.3.3 DB2 HADR 示意圖

DB2 HADR 架構中，應用程式存取資料庫是在主要伺服器上執行，而資料庫伺服器會透過 HADR 將 Log Page 傳至預備資料庫伺服器上，藉此同步資料庫內容，當主要伺服器停止運作時，預備伺服器就會啟動，並取代主要伺服器。現況採行負載平衡叢集式架構 Load Balancing Clusters (ACTIVE/ ACTIVE) 者，僅 SMART DB2 使用 HADR 機制。

參、未來發展策略之探討

建置本公司完整備援機制，中長期發展規劃，短期宜以提升本公司異地備援主機處理容量為目標，逐步提昇至與主電腦中心主機相當之處理容量（即達到等量備援之規模），以因應遇緊急狀況需啟動異地備援中心作業時，提供資訊系統正常服務；並規劃縮短各業務資訊系統啟動異地備援環境切換時間，另規劃建置各業務資訊系統雙活機制，縮短同地備援切換時間，未來可搭配資訊廠商於雙活機制(Active/Active)距離限制之技術發展，逐步擴展調整至「同城雙中心」或「兩地三中心」之雙活運作機制。惟建置「同城雙中心」或「兩地三中心」之雙活運作機制所需之時程較長，且整體硬體成本亦較高，故應一併考量公司未來整體發展政策，分階段建置並搭配應用程式之調整，逐步建置雙活相關運作機制環境，方可提高本公司資訊設備之投資效益。

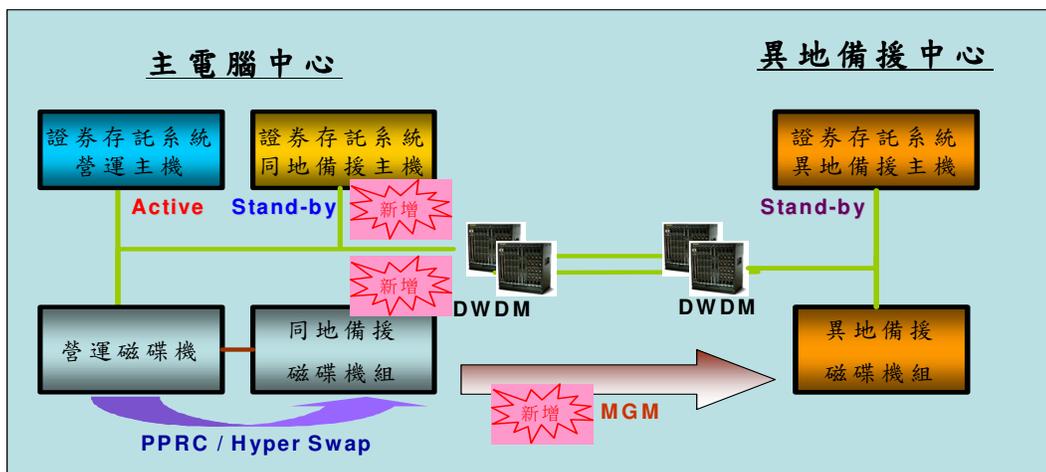
一、大型主機建置A/A雙活架構之執行策略

建置本公司大型主機 SYSPlex 平行處理架構，應要達到兩個目標，其一是建置主機 GDPS HyperSwap 功能，其二則是達到 Active-Active 作業處理架構；至於考量「同城雙中心」或「兩地三中心」之相關議題，本文後續將做詳細說明。以下將分成三個階段說明：

（一）階段一：建置同地備援主機及 GDPS HyperSwap

階段一之目標在建置大型主機同地備援主機，以及增購磁碟組以建置 GDPS HyperSwap 機制，並將原主電腦中心與異地備援中心間的

PPRC 模式改為 MGM 模式，如圖表 1.3.4；說明如下：



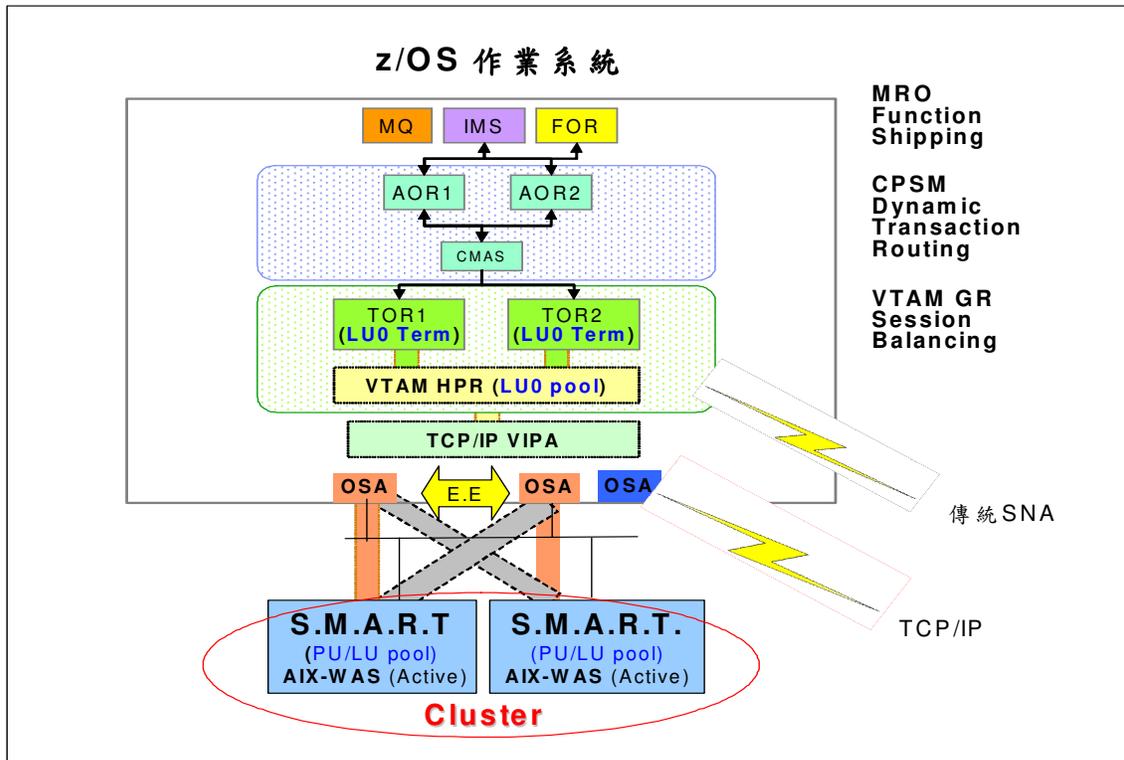
圖表 1.3.4 同地備援主機及 HyperSwap 示意圖

- 1、同地備援主機之建置可減少原本切換至異地備援主機時，在系統層所需耗費的時間(RTO自 2 至 4 小時，減少為 0.5 至 1 小時)。
- 2、應增購新的磁碟組以建置 GDPS 機制。GDPS 為 PPRC 之進階應用，可避免因磁碟機組故障，造成營運系統必須先中斷再切換至備援磁碟機組之問題；當磁碟發生障礙時，GDPS 以「Hyper Swap」的方式，讓營運中的系統，直接切換使用備援之磁碟機組，此時營運系統僅會發生數秒的「停頓」，即可繼續運作，且線上交易也不會發生中斷的狀況；如此即可解決磁碟故障所導致系統停頓無法提供營運服務的現象。
- 3、由於新增 GDPS HyperSwap 機制後所產生的限制，原本主電腦中心與異地備援中心間的

磁碟 PPRC 即時同步模式，則須調整為 MGM 非同步模式；在 MGM 模式下，資料可能會有 5 個 I/O 內的落失；然而真正發生大規模災害，致需啟動異地備援系統時，再由 AP 部門及業務單務介入補齊少許可能遺失的資料，應屬可被接受的範圍。

(二) 階段二：建置「單主機平行處理架構」

由於雙主機之 SYSPlex 運作必須搭配 CICSplex，且現有 CICS 對主機其它資源的存取方式，以及對外提供之連線服務機制……等均需逐步調整，故除系統層之修改外，仍需應用系統負責單位大力配合修改 UCPM 及相關程式邏輯，以符合 CICSplex 架構之運作，才可真正達到大型主機 A/A 雙活模式；建置「單主機平行處理架構」如圖表 1.3.5，說明如下：



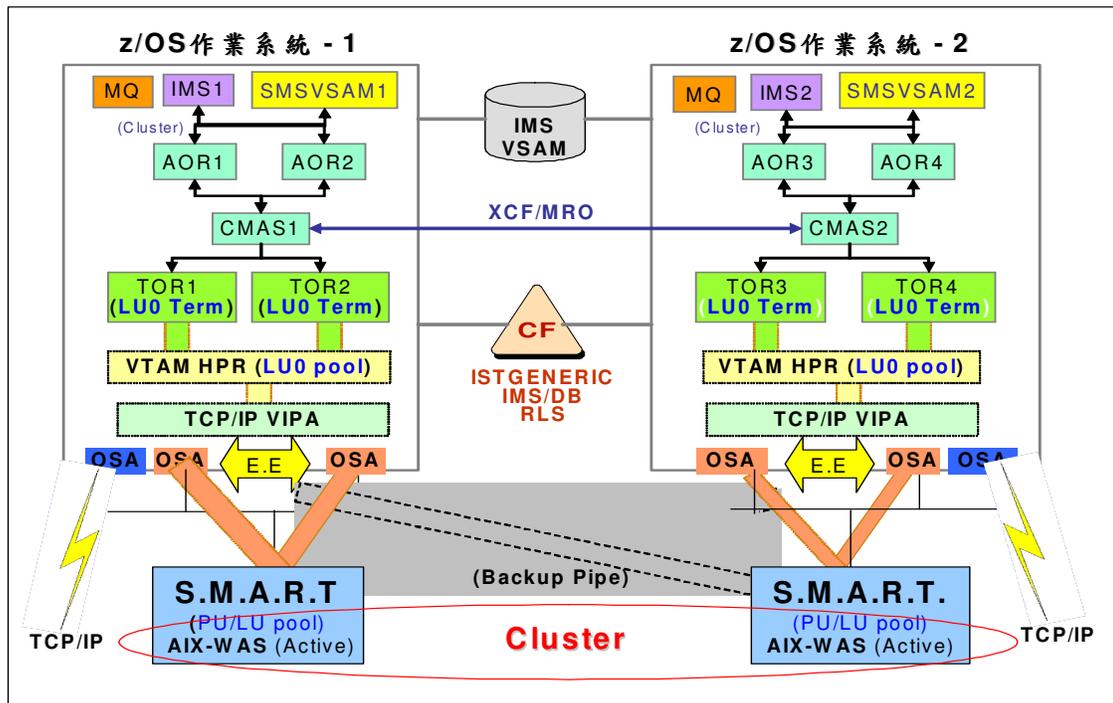
圖表 1.3.5 單主機平行處理架構示意圖

- 1、為建置 CICSplex，原本單一主機中 CICS 之「Single Region」運作模式，需改為單一主機 CICS 之「Multi Regions」運作模式，也就是建置 TOR、AOR 及 FOR，同時將現行的運作於 Single Region 之程式運作邏輯 (UCPM 及其它相關程式)，改寫為可運作於 Multi Regions 中。
- 2、將現行單一 CICS Region 存取階層式資料庫環境 (IMS/DB)，改變為多 CICS Regions 存取分享式階層式資料庫環境 (IMS/DB sharing)。

3、此階段中，「現行 CICS 對檔案(VSAM)及 MQ 的存取」、「單一主機之 TWS 批次排程」、「單一主機對外連線服務提供」，以及「現行異地備援切換機制」，均不改變。

(三) 階段三：建置「多主機平行處理架構」

建置雙主機組成之 SYSPlex 模式，並將階段二之「單主機平行處理架構」，轉換運作於此 SYSPlex 模式，達到完整之「多主機平行處理架構」，如圖表 1.3.6，說明如下：



圖表 1.3.6 多主機平行處理架構示意圖

1、建置 SYSPlex 模式後，即可達到「主機硬體及作業系統之 A/A 雙活架構」，Sysplex 平行作業之資料同步技術，保證效能正常

可用之距離限制為光纖距離 20 公里；而在階段二所完成之 CICPlex 之 Multi Region 模式，可達到「CICS 線上交易系統之 A/A 雙活架構」，故在將此 CICPlex 之 Multi Region，改運作於此 SYSplex 雙主機模式後，則可達到完整之大型主機 A/A 雙活運作架構，並達成「多主機對外連線服務」之目標。

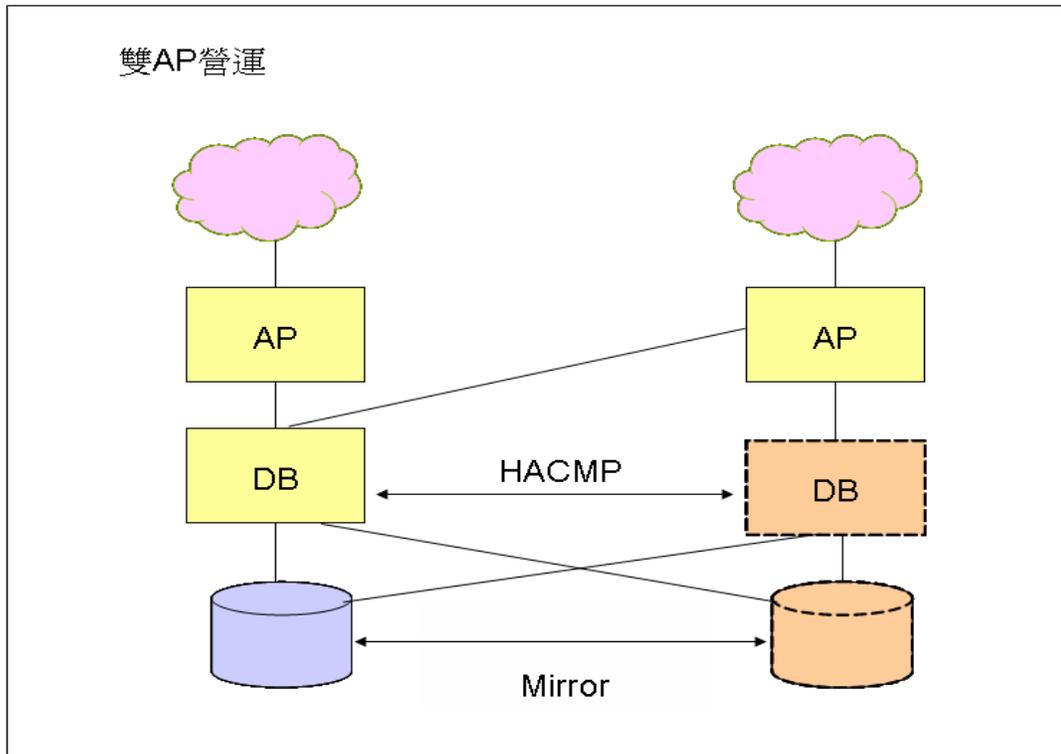
- 2、與階段二相同，CICS Regions 亦可存取分享式階層式資料庫環境(IMS/DB sharing)。
- 3、檔案(VSAM)之存取改為 VSAM RLS，而原本單一主機 MQ 改建置為 MQ Plex，而單一主機之 TWS 批次排程，則改為 TWS Plex，故可達成 CICSPlex 對上述資源之分享式存取目標。
- 4、現行異地備援切換機制仍不改變。

二、開放系統主機建置A/A雙活架構之執行策略

建置本公司開放系統主機 A/A 雙活架構，首先須先導入叢集式架構，其次依其建置難易度分階段建置達到 Active-Active 作業處理架構。

(一) 階段一：雙 AP 營運

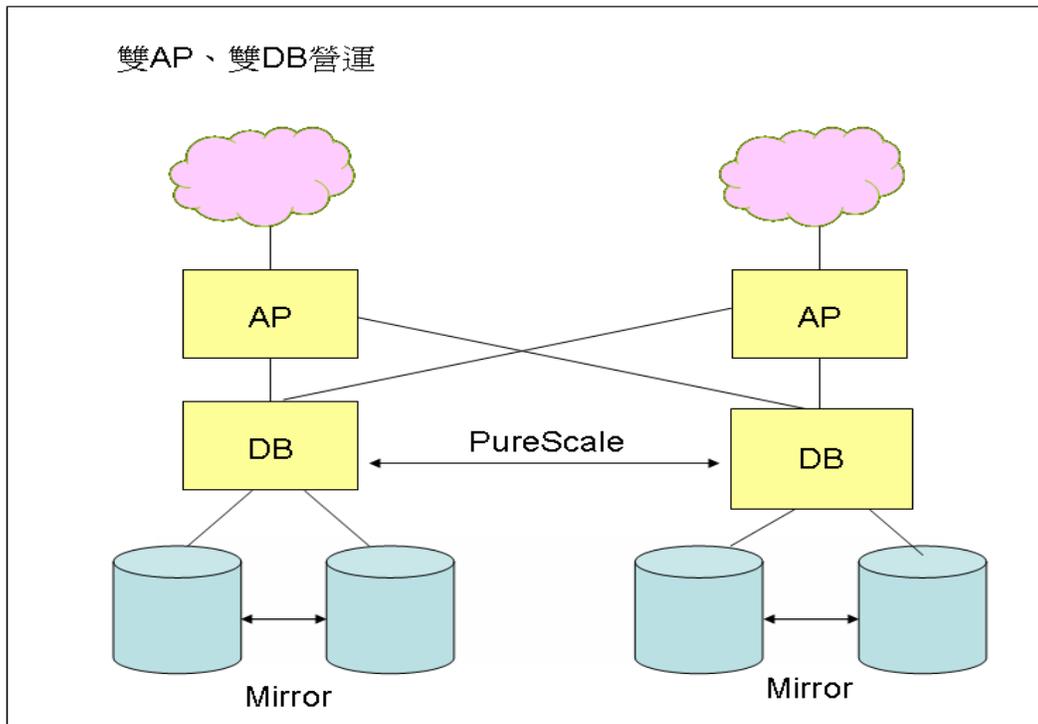
階段一之目標在所有開放系統導入叢集式架構，以雙主機雙 AP 機制營運，並將原主中心營運與備援主機改為叢集式架構作業模式，如圖表 1.3.7：



圖表 1.3.7 叢集式架構作業模式

(二) 階段二：雙 AP、雙 DB 營運

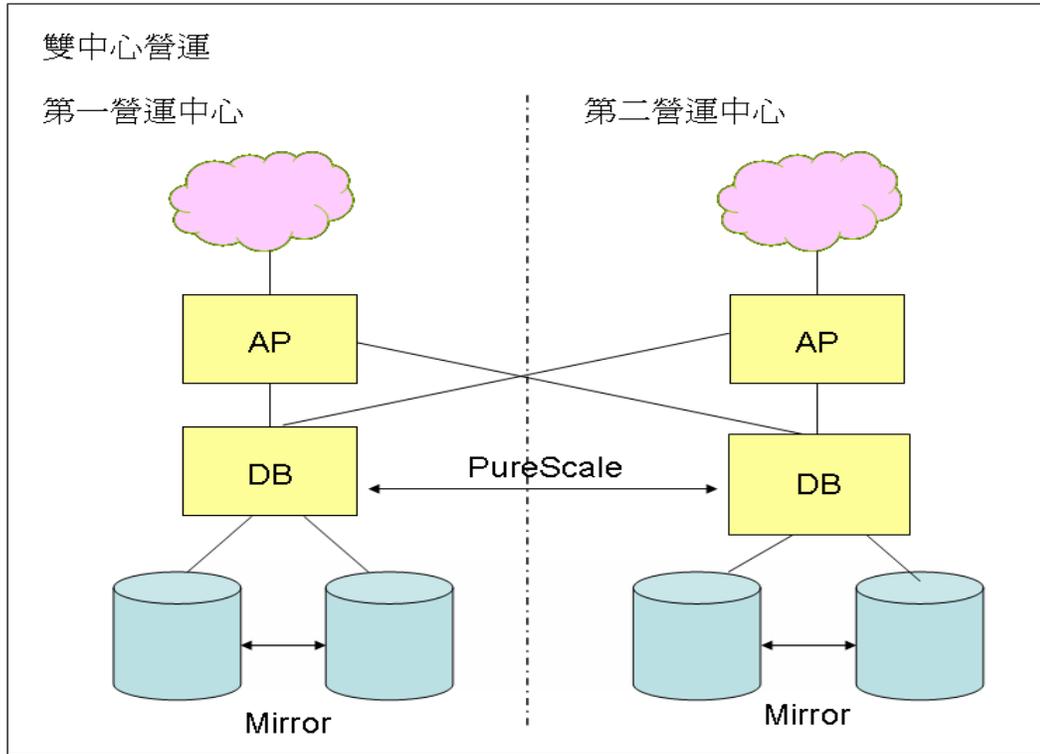
階段二之目標建置各業務資訊開放系統以雙主機雙 AP 及雙 DB 機制營運，導入 DB2 PureScale 或 Sybase Cluster 叢集式架構進行作業模式，資料庫 (DB2) 雙活機制之資料同步技術，保證效能正常可用之距離限制為光纖距離 10 公里，目前 IBM 實驗室與多家金融機構正在測試 20 公里資料同步技術之可行性，相關架構如圖表 1.3.8：



圖表 1.3.8 DB2 PureScale 叢集式架構

(三) 階段三：雙中心營運

階段三之目標建置雙主機雙中心營運模式，各業務資訊開放系統主機分置二地同時作業，如圖表 1.3.9：



圖表 1.3.9 雙中心同時作業示意圖

三、相關業界資訊系統備援機制架構

因應兩地三中心及雙活機制之運作模式，現已蔚為各國重要資訊中心資訊系統備援架構發展與中長期建設之主要趨勢，不論是為災備或提升對客戶服務品質與作業效率，相關企業之想法與作法漸趨於一致，故蒐集相關業界資訊系統備援機制架構規劃如下：

↻	同城雙中心↻	雙中心機制	異地備援中心↻	備援中心切換作業↻
新加坡↻ 交易所↻	無↻	無↻	1. 距離約 10 公里↻ 2. 主中心異常時切換至異地備援中心須於 2 小時內(包含公司決策時間)完成↻	每年依法令 <u>切換至備援中心營運</u> (至少 1 次)↻
馬來西亞↻ 交易所↻	無↻ (<u>同地備援採 HACMP</u>)↻	無↻	1. 距離約 10-12 公里，異地備援中心採 <u>HADR</u> ↻ 2. 主中心異常時切換至異地備援中心：交易系統 1 小時、結算系統 4 小時↻	無(僅每年測試演練 1 次)↻
中國工商↻ 銀行↻	有↻ (上海)↻	現況：A/S↻ 未來：A/A↻	有(北京)↻	無(僅演練)↻
<u>中證登公</u> 司↻	有↻ (北京)↻	現況：A/S↻ 未來：有需 要再進化至 A/A↻	無(計畫中)↻	無(僅演練)↻

圖表 1.3.10 業界資訊系統備援機制架構

第四節 資料保存與備援機制

壹、研究目的及範圍

一、研究目的

本公司目前保存各業務資訊系統資料的方式，雖然在技術與軟體版本上隨著資訊廠商所提供之版本逐年更新，但在磁帶備份、分儲及磁碟等硬體相關設備，仍屬舊有的資訊設備，為提升有效備份效率與分儲機制及磁碟效能等作業，須汰換舊有之相關設備，期能減少人為的介入所衍生之問題，將以更安全資料控管為前提，進而提升本公司資料保存及交易效能等作業。

另確保本公司各業務資訊系統能長期持續穩定運作，各業務資訊系統之系統資源管理備份工具，必須持續辦理版本更新或改建作業，以因應新種業務資訊系統使用需要，並能維持現行各業務資訊系統運作正常及穩定。

二、資料範圍及內容

(一) 蒐集範圍

以本公司各業務資訊系統為資料蒐集對象，結合各作業系統平台備份之特性及需求，備份之作業系統環境包括 Windows、Linux、AIX、z/OS 等，備份需求內容物包括前述之檔案資料備份、資料庫備份等備份內容；另蒐集本公司各業務資訊系統所使用之開放主機及大型主機系統所使用之相關磁碟機狀況。

(二) 搜集內容

除蒐集本公司備份資料實際現況等資料外，並蒐集及整理新一代備份功能，提昇備份效率，減少備份時間的理念與策略，包括：資料備份容量壓縮、備份資料傳輸機制、磁帶備份加密機制、磁帶備份管理機制、磁帶異地備援管理機制、磁帶備份分儲機制、磁帶備份之分類等級、磁帶備份保存機制，並蒐集現行使用之磁碟機，同、異地備援機制及新種磁碟機功能，俾便後續分析及整理。

（三）資料整理

訪談目前備份資訊廠商，蒐集最先進各種備份技術、了解各備份平台差異與優劣，結合目前實際作業需求，評估未來可行方案，協同備份資訊平台之資訊整合廠商，依現行整體實際環境，提出相關合宜之技術資料，以利本公司各項備份資料未來需求。

經蒐集、整理及分析相關磁碟機資訊後，將各種磁碟機備援機制技術，包含公司現行已使用之技術（如：PPRC、Mirror），考量其效能、安全性及對原營運系統之影響性，進而分析及評估適用之技術。

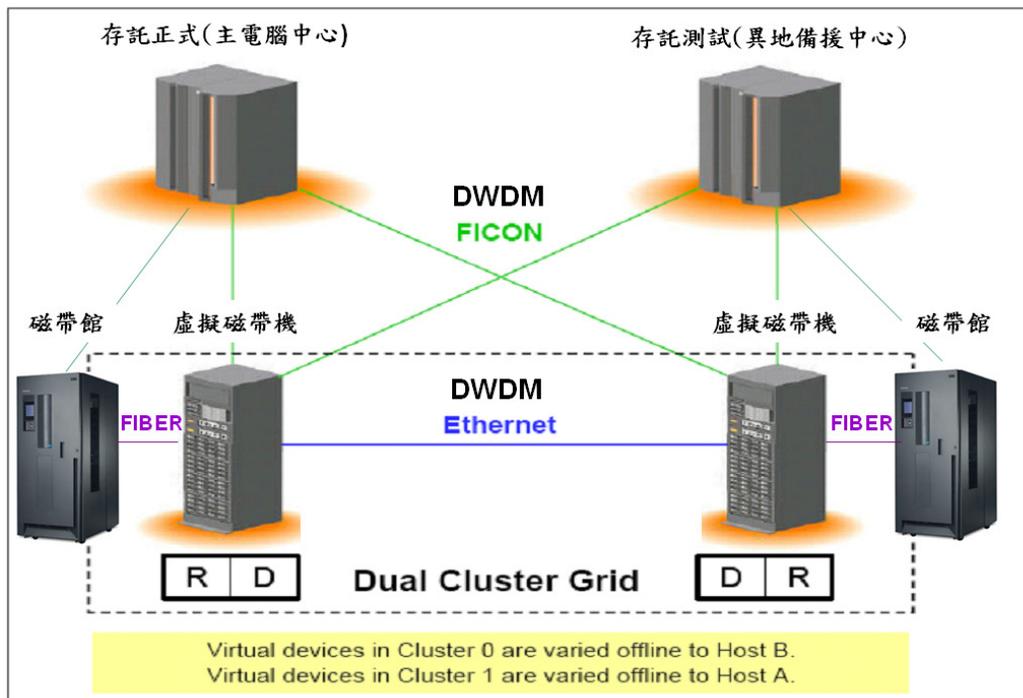
貳、現況

一、大型主機現行架構

- （一）現行備份採主從架構，主電腦中心與異地備援中心各有一台虛擬磁帶館及磁帶館，虛擬磁帶館，可模擬 256 台磁帶機，負責將資料寫入磁碟陣列中，並藉由實體磁帶機，將磁碟陣列中之資料寫入實體磁帶中，

磁帶館負責將資料直接寫入實體磁帶中。大型主機備份架構示意圖(詳如圖表 1.4.1)。大型主機之存託系統，依實際需求以光纖連線媒介方式，進行以下備份作業：

- 1、將資料寫入虛擬磁帶館之磁碟陣列中，並可依實際需求以網路方式將資料寫入串連之虛擬磁帶館之磁碟陣列，再由各自之虛擬磁帶館將資料透過實體磁帶機寫入實體磁帶中。
- 2、將資料直接透過磁帶館之實體磁帶機寫入實體磁帶中。



圖表 1.4.1 大型主機備份架構示意圖

(二) 資料備份模式：

- 1、資料備份共分為日、週、月與不定期四種備份模式，備份的內容與週期之需求，由各業務系統負責人提出，系統操作單位負責審核、記錄與過期資料刪除，系統工程單位負責環境建置與整體需求的驗證與確認。
- 2、所有備份完成之虛擬磁帶，目前均透過磁碟陣列再轉存於主中心磁帶館內，備份時運用 GRID 的技術同時寫入備援中心磁碟陣列中，再轉存於異地備援中心之磁帶館內，達到第二套異地備援中心儲存資料備援目的。
- 3、備份時並同時運用 Copy Export 技術，將備份完成之虛擬磁帶，寫入加密磁帶中，並透過加密管理機制 EKM(Encryption Key Manager)，達到資料加密需求。再由系統操作人員將磁帶從磁帶館退出後，送到第三地，達到第三套異地儲存資料備援目的。

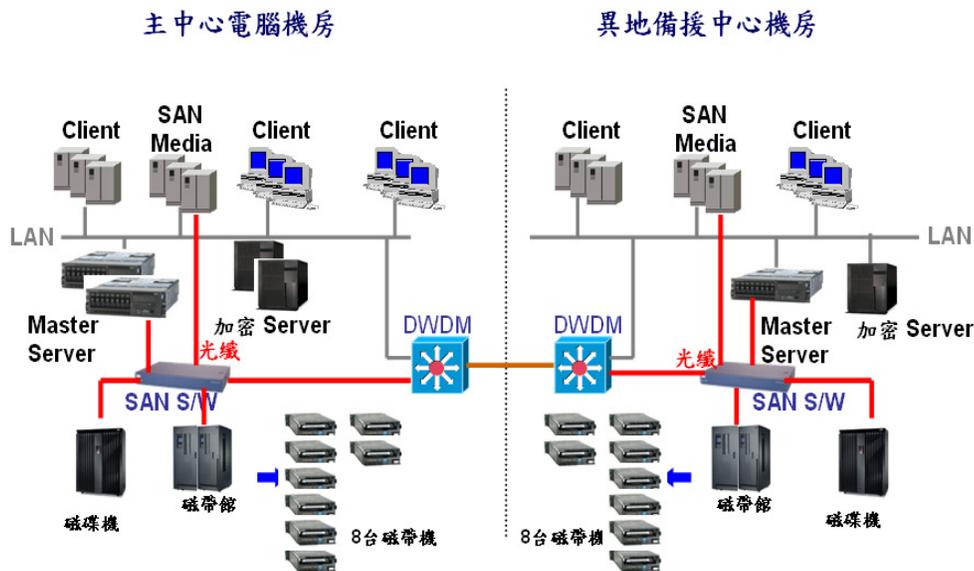
(三) 整體備份週期如下：

- 1、日備份：備份時間以交易之營業日備份為主(磁帶保留期限為 1 個月、30 代或永保)。
- 2、週備份：備份時間以每週之最後一個營業日備份為主(磁帶保留期限為 1 個月或 4 代)。
- 3、月備份：備份時間以每月之最後一個營業日備份為主(磁帶保留期限為一年、三年或永保)。
- 4、不定期備份：備份時間依業務系統負責人自訂(磁帶保留期限為 1 個月、4 代、30 代、一年、三年)

或永保)。

二、開放系統現行架構

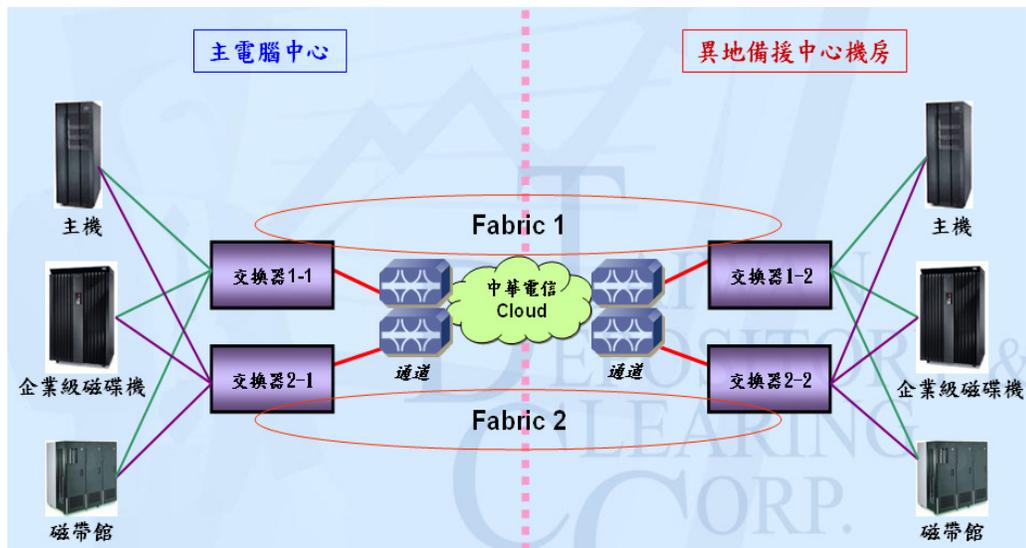
目前本公司集中備份主機環境，由一台 AIX 主機以作業系統邏輯虛擬主機(LPAR)機制建置，備份的對象除存託主機外，均為開放平台備份主要的範圍，並於主電腦中心以相同之邏輯虛擬主機(LPAR)機制建置同地備援環境，於異地備援中心建置異地備援環境，開放平台集中備份架構示意圖(詳如圖表 1.4.2)。



圖表 1.4.2 開放平台集中備份架構示意圖

- (一) 開放平台備份主機硬體環境內含 2 片光纖卡片，分別接上本公司兩組之儲域網路(Fiber1、Fiber2)，而每一組儲域網路包含主中心 3 台磁帶機與 1 台加密磁帶

機及備援中心機房 3 台磁帶機與 1 台加密磁帶機達到備援機制，光纖儲域網路示意圖(圖表 1.4.3)。



圖表 1.4.3 光纖儲域網路示意圖

- (二) 開放平台備份主機作業系統，已涵蓋加密管理機制 EKM(Encryption Key Manager)，EKM 負責磁帶館之加密磁帶機備份時產生加密功能，以達到資料加密需求。
- (三) 本公司以 Netbackup 軟體備份機制執行各開放平台系統資料備份，主中心機房與備援中心機房各有一座磁帶館，每台各有磁帶及加密磁帶，由於磁帶之數量及磁帶館容量限制保存模式，保留期限分為一個月與三年為主。
- (四) 資料備份模式：
 - 1、連線架構說明：現行備份採三層式連線架構，存託系統負責備份時間排程設定，觸發集中備份主機備份機制，集中備份主機透由備份主要程式與業務主機端之代理程式(Agent)溝通，資料以網路或光纖連線媒介方式，將資料寫入磁帶機中。

- 2、硬體設備說明：主中心機房與備援中心機房各有一座磁帶館，每座各有磁帶機及加密磁帶機，磁帶機負責各業務系統備份之需求，可允許同時六台主機備份之需求，加密磁帶機負責第三套異地儲存(證券交易所)加密磁帶之需求。
- 3、備份週期說明：硬體設備說明各業務資料備份共分為日、週、月、季四種備份模式，並於交易完成執行批次作業後執行，備份的內容與週期之需求，由各業務系統負責人提出，系統操作單位負責存託主機與自動排程系統中設定相關組態，系統工程單位負責集中備份主機備份內容之環境建置與整體需求的驗證與確認。
- 4、所有備份完成之磁帶，目前均存放於磁帶館內，備份時運用 In-Line Copy 的技術，同時寫入主電腦中心與異地備援中心磁帶機之磁帶機中，以確認資料同步寫入異地備援中心機房之磁帶館內，達到備援的目的。
- 5、A 級系統備份除上述資料主電腦中心與異地備援中心磁帶館資料備份份儲存方式外，另以 Netbackup Vault 技術將備份完成之主電腦中心磁帶內容讀取後，利用磁帶機密技術再次寫入加密磁帶機中，備份完成後系統操作人員將磁帶從磁帶館取出後，將加密磁帶送到第三地，達到第三套異地儲存資料備援目的。

(五) 整體備份週期如下：

- 1、日備份：備份時間以交易之營業日備份為主(磁帶

保留期限為 1 個月)。

2、週備份：備份時間以每週之最後一個營業日備份為主(磁帶保留期限為 1 個月)。

3、月備份：備份時間以每月之最後一個營業日備份為主(磁帶保留期限為三年)。

4、季備份：備份時間以每季之第一個月備份為主(磁帶保留期限為三年)。

三、磁碟機現行架構

(一) 磁碟機種類及數量：

本公司主電腦中心機房現有 IBM 系列磁碟機種類有四種企業等級磁碟機，於異地備援中心備援中心機房種類有兩種企業等級磁碟機，磁碟機內部之運作為採用 RAID 5 方式儲存以保護資料內容。

(二) 磁碟機備援模式：

於主電腦中心機房之各伺服器主機資料儲存為採用鏡射(MIRROR)方式，分別儲存於兩部實體不同之磁碟機中以達資料同地備援之目地；主電腦中心機房之磁碟機資料內容經由本公司 DWDM (Dense Wavelength Division Multiplexing) 線路，及使用 IBM PPRC (Peer to Peer Remote Copy) 之同步傳輸技術，將資料同步由主電腦中心機房傳送至異地備援中心機房之磁碟機內，以達資料異地備援之目地。

參、未來發展策略之探討

一、未來規劃方向分析

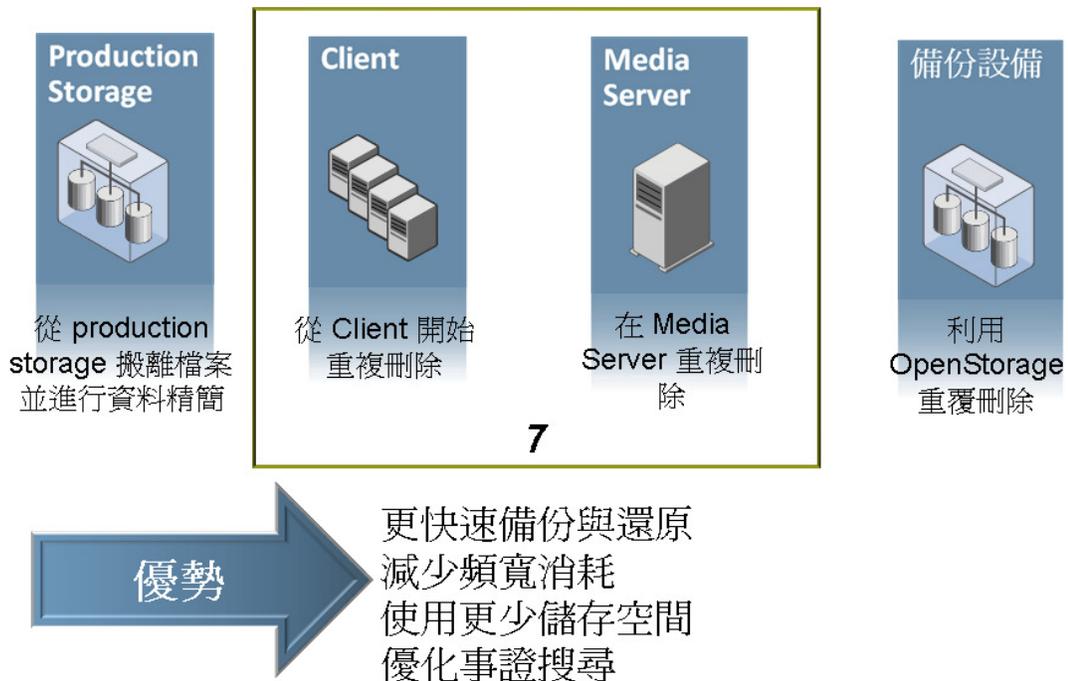
(一) 大型主機

倘大型主機需轉換至開放系統架構時，其資訊系統備份機制，將整合於現行開放主機資訊系統備份機制；反之未來保留部份現行大型主機架構，則可依下列規劃分析，研議未來之大型主機備份機制，其說明如下：

- 1、實體磁帶機：導入新款之加密磁帶機，除可提升整體備份寫入速度由原先 104MBps 提升至 250MBps，單卷儲存容量可由原先 700GB 提升為 4TB。
- 2、虛擬磁帶館：市場上暫無新備份技術發表，將持續追蹤是否有新備份技術可適用並加以導入。

(二) 開放系統：

- 1、規劃資料備份重複刪除(壓縮)機制架構：為求縮減備份資料量，引進資料備份壓縮備份機制，資料重複刪除示意圖(如圖表 1.4.4)。



圖表 1.4.4 資料重複刪除示意圖

資料壓縮機制可分為兩階方式資料壓縮後備份：

- (1) 方式一：可由原始需求主機(Client 端)將資料壓縮後送出，如此一來可從需求主機(Client 端)將資料送出至備份主機(Server 端)時減少網路頻寬需求，倘從需求主機(Client 端)至備份主機(Server 端)需經過許多之網路節點，這些網路的節點與網段均會因備份而受到影響。
- (2) 方式二：原始需求主機(Client 端)將備份資料完整送出至備份主機(Server 端)，備份主機(Server 端)再將資料壓縮，壓縮後才將資料寫入儲存媒體(磁帶或磁碟上)。

2、規劃導入虛擬磁帶館技術機制

建置虛擬磁帶館以磁碟虛擬磁帶方式，可避

免磁帶因長期重覆使用造成磁帶毀損磁帶上資料無法正常讀取，並加速資料備份作業效能。

(三)、磁碟機：

本公司未來磁碟機架構將採逐步整併暨更新主電腦中心與異地備援中心磁碟機，並採總量控管模式，彈性使用磁碟空間並避免資源過度佔據。

現有本公司之交易資料因受各項法規規定，需長期保存歷史交易資料內容，這些資料亦儲存於現有之舊型企業級磁碟機內，隨著資料成長，所需之空間亦需逐年增加。此種資料類型可隨舊型企業級磁碟機之汰換更新，轉換至較高存取速度符合本公司需求，但儲存空間更大之磁碟機種。

將現有單一儲存體機種改為兩種儲存體機種。一為追求儲存速度更快，供線上即時交易（如證券存託系統、期貨結算系統、票券保管結算交割系統等）類別系統使用；一為追求儲存容量但存取速度符合本公司需求，供歷史交易（如查詢資料庫系統等）資料儲存類別系統使用。

引進「虛擬化儲存技術」(Thin Provisioning)，使每一套系統認為有足夠空間可以使用，可以讓磁碟容量運用更有效率。另規劃建置全系統資料儲存設備控制架構(SVC, SAN Volume Controller)，依據各業務資訊系統作業環境及資料屬性，配置不同等級資料儲存設備（等級分為企業級、中/低階等級），不同業務資訊系統作業環境及資料屬性，分類儲存。

第五節 小結

完善之資訊系統基礎工程為企業永續經營之根本

整體資訊系統基礎工程涵蓋電腦機房環境及網路系統、伺服器主機與資料等面向，攸關企業永續運作計劃成敗，前述各類資訊設備與環境皆相互依存缺一不可，任何一個節點的不穩定或脆弱點皆可能造成整體或部分之資訊服務無法持續提供之風險。

電腦機房基礎建設與機電設施，係提供各類資訊設備運作之作業環境，電腦機房作業環境之任一異常或故障，將直接影響所有資訊設備運作順暢與否，故持續更新與強化電腦機房環境與機電設備，提供更穩定之基礎環境措施。

網路系統架構係資訊服務提供者與聯接使用者之橋樑，各類資訊服務可藉由多元化之連線管道及穩定之通道，提供不同類型之使用者，相關網路設備持續整合與強化，以提供更穩定之網路聯通介面。

伺服器主機係為各資訊服務之作業核心，其處理效能與備援能力直接反應在整體資訊服務水平上，具備多重備援機制與足夠之備援容量，可因應資訊設備異常時啟動備援機制亦可提供相同等級之資訊服務水平。

資料之完整性，涵蓋資訊儲存與備份等，必要的資料備份可支援資料因故毀損時進行資料回復作業，與資料備援可避免資料儲存設備故障導致資料無法使用之窘境。

綜合前述有關電腦機房與機電設備、網路系統、資訊系統備援機制與資料之完整性，皆存在相依相容缺一不可之特性，故為確保企業持續永續經營，持續辦理資訊系統之基礎

工程之整合與更新，直屬必要。

第三章 應用系統之發展策略

第一節 業務系統之作業行為分類與整合

壹、研究目的與範圍

一、為加強服務參加人，提供一致的作業介面，擬彙整各重要業務系統功能及使用介面，作為未來提昇系統之參考依據；以下臚列本公司各重要業務系統之發展及建置時程：

- (一)1995年2月14日市場實施「全面款券劃撥制度」。
- (二)1998年7月接受期交所委託，建置了期貨結算電腦系統，辦理期貨市場各項商品之交割結算事務。
- (三)2002年，本公司接下興櫃股票市場的結算交割業務。
- (四)2005年本公司建置「境外基金資訊觀測站」，並建置「境外基金款券收付平台」，提供完整境外基金服務。
- (五)2006年3月，本公司正式與票保公司合併，完成了證券市場與票券市場集中保管結算機制的整合。
- (六)自2006年因應證券市場需求，建置「證券場款券T+2日DVP帳簿劃撥交割作業」、「海外企業來台第一上市(櫃)、興櫃及第二上市(櫃)相關帳簿劃撥作業」、「指數股票型基金(ETF)跨國掛牌相關帳簿劃撥作業」、「國際債相關帳簿劃撥作業」、「法人對帳系統服務」、「股東會通訊投票平台建置」、「期信基金資訊申報及公告作業」、「股東會委託書查核」、「境外結構型商品申報及公告作業」等多項重大業務，提供證券市場及票券市場更精緻、安全、便捷、多元化的服務。

二、研究目的

- (一) 期望經彙整及分析公司重要業務系統架構，以提供未來系統間整合之參考，以提供參加人或使用單位更單純的作業流程或介面，更加強本公司對外服務及提昇作業效率。
- (二) 期望能藉由整理本公司各業務系統間之關聯，歸納及整合各業務系統間共通之作業模式，透過業務系統功能分類，以供未來建置新應用系統之參考，達到提昇管理及業務系統品質之目的。

三、研究範圍

本公司業務範圍涉及交易、結算及其他服務，依各市場及商品別分述如圖表 2.1.1 本公司業務系統之範圍

市場別	證券市場	櫃買市場	興櫃市場	基金	固定收益	期貨市場	股務
交易面	-	-	-	V	V	-	-
結算面	V	V	V	V	V	V	-
其他服務	V	V	V	V	V	-	V

圖表 2.1.1 本公司業務系統之範圍

(一) 證券、櫃買、興櫃市場：

1. 證券存託系統：辦理上市上櫃市場之帳簿劃撥作業，及辦理興櫃股票市場之結算交割作業，另包括無實體帳簿登錄作業，是本公司最重要業務系統。
2. S. M. A. R. T 系統：辦理使用單位與證券存託系統之操作介面處理。

3. 報表網路傳送查詢系統(E_Report)：提供所有參加人三年內之存託夜間批次報表線上查詢、列印、派送(e-mail)等功能

(二) 境內、外基金商品：

1. 境外基金交易平台系統：提供總代理人與銷售機構辦理境外基金之交易資訊傳遞及投資人交易款項之收付作業。
2. 境外基金申報公告系統：提供總代理人申報境外基金相關業務資訊，供投資大眾查詢。
3. 基金資訊傳輸平台系統：提供銀行信託部及國內投信公司辦理國內基金下單及交易確認資料之傳輸平台。
4. 期信基金申報公告系統：提供投信公司、保管銀行申報投資期貨基金相關業務資訊，供投資大眾查詢。

(三) 固定收益商品：

1. 票券結算系統(BCSS)：提供國內短期票券初、次級市場、兌償等相關作業之款券同步結算交割資訊服務。
2. 短票利率編製系統：依專營票券商當日短期票券初、次級市場牌告及成交利率資訊編製 SIRIS 短期利率，依報價利率資訊編製 TAIBIR 短期利率。
3. 款項收付服務平台系統(PSP)：以開放且標準的服務介面，提供各業務系統之進行款項收付服務。

4. 境外結構商品申報公告系統：提供總代理人申報境外結構型商品相關業務資訊，供投資大眾查詢。

(四) 期貨市場：

期貨結算系統：提供期貨商、結算會員登錄及查詢期貨結算交割業務資料，亦提供期交所執行期貨市場中期貨暨選擇權商品之各項結算、交割及風險控管相關作業。

(五) 股務作業：

1. 股東通訊投票平台系統：提供電子投票平台，鼓勵發行公司之股東參與公司經營，強化股東權益之保護。

2. 發行作業平台系統：提供股務代理機構登錄無實體、帳簿劃撥配發、轉換公司債及停止過戶相關資料，以及金融機構登錄短期票券、固定收益債券所有人名冊資料，蒐集後供業務單位及系統進行資料處理。

3. 辦理除權息、現金增資配發及還本付息作業：出具股東名冊及還本付息名冊與相關股務代理機構及代兌本息金融機構，保障股東權益。

四、研究項目

(一) 針對本公司所涉及業務範圍之相關資訊系統搜集其相關屬性，搜集項目包括：執行環境、連結方式、網路安控、系統安控、系統架構、操作介面、開發工具/程式語言、備援等級、市場參與者等項目，以彙整及分

析公司重要業務系統架構。

- (二) 針對與交割結算業務相關之系統，彙整其作業功能，包括：帳務架構、作業行為、業務特性、業務功能、作業時間等項目，以分類業務系統功能，並提供未來建置新應用系統之參考。

貳、業務系統之現況

一、各業務範圍對照之業務系統關聯

彙整各業務系統之服務市場、相關使用者、主要商品及業務功能之性質，整理如下：

- (一) 服務市場範圍包括上市、上櫃、興櫃市場、期貨市場、以及基金、固定收益商品等。
- (二) 所涉及之主要商品包括權益證券、債券、境、內外基金、期信基金、境外結構型商品、票券、期貨及選擇權等。
- (三) 主要使用者包括業務主管機關(金管會、央行)、交易所(證交所、櫃買中心、期交所)、參加人及交易商(證券商、期貨商、票券商、股代、發行公司、境外基金總代理、銷售機構、銀行)、相關單位(證金公司、相關公會、信託、投信、保管銀行)及投資大眾。
- (四) 主要功能於興櫃市場、基金、固定收益商品為交易申報及款券結算作業，於上市、上櫃、期貨市場為帳簿劃撥結算交割作業。

註：反白標示欄為本公司所屬業務系統

服務市場別		證券、櫃買、興櫃	基金	固定收益商品	期貨市場	股務處理	
主要商品		股票、債券、基金	境內、境外基金/境外結構型商品	債券、票券	期貨、選擇權	股票、債券、票券	
使用本公司系統之相關單位		證券商、證金公司、保管銀行、證交所、櫃買中心	總代理機構、銷售機構、銀行、央行、銀行局、證期局、投信投顧公會、證投公會、銀行公會、壽險公會、投信資大眾、期信基金、期貨公會	清算交割銀行、中央銀行、實券、保管銀行、外幣清算銀行、代理清算銀行、票券商、證券商、銀行局、期交所	期貨商、結算期會、期交所	股東、發行公司、股務代理機構、保管銀行、投信、信託業、還本付息機構、NCD發行銀行、市庫券經理行、保證人	
交易系統		證交所交易系統			期交所交易系統	-	
結算	前端系統	M1: SMART	F0: 境外基金交易平台	B0: 票券結算系統 (BCSS)	C0: 期貨結算系統	M1: SMART	
	帳務系統	M0: 證券存託系統					
	支援系統		F1: 境外基金申報公告 F2: 境外結構型商品申報公告 F4: 期信基金申報公告				M2: 報表網路傳送查詢系統 (E_REPORT)
			B1: 款項收付平台 (PSP)				
		F3: 基金資訊傳輸平台	B2: 短票利率編製系統 (SIRIS, TAIBIR)			F3: 基金資訊傳輸平台	
其他服務			-			S1: 股東通訊平台 S2: 發行作業平台	

圖表 2.1.2 各業務範圍對照之業務系統關聯

二、各業務系統之連線方式、安控及操作介面說明

本公司與外單位連線方式分為Internet及ADSL專線模式，於Internet傳輸資料若需加密係透過SSL處理，ADSL專線傳輸資料多經VPN加密處理，Internet連線利用CA憑證辨視使用者身分，ADSL專線連線則有CA、金鑰、帳號密碼等多種身分辨視方式，依各主要使用單位與各系統連線之作業說明如下：

(一) 業務主管機關

1. 金管會：包括銀行局、證期局，於Internet網頁登錄CA憑證後，可查詢「境外結構型商品申報公告」及「境外基金申報公告」、「期信基金申報公告」資訊。
2. 中央銀行：於Internet網頁登錄CA憑證後，可查詢「境外結構型商品申報公告」資訊；另於ADSL專線辦理「證券存託系統」之中央交換債轉帳及央行短期融通設質作業，並於Leased Line接收「票券結算系統」傳送之同資系統通知，以完成款項撥轉作業

(二) 交易所

1. 證交所、櫃買中心：於Internet以CA解密接收「報表網路傳送查詢系統」之證券市場、櫃買中心及興櫃股票報表；於ADSL專線以TCP/IP協定傳送證券市場、櫃買中心、興櫃成交資料；於ADSL專線以「SMART系統」辦理證券結算交割相關作業。

2. 期交所：於 ADSL 專線以 TCPIP 協定傳送期貨市場成交資料；及於 ADSL 專線以 PB 介面辦理期貨結算交割相關作業；並於 ADSL 專線以 MQ+金鑰方式接收「短票利率編製系統」SIRIS 資料。

(三) 參加人及交易商

1. 期貨商、結算會員(專營)

於 ADSL 專線透過 VPN 加密及身分確認機制，以 MTS 辦理「期貨結算系統」各項作業。

2. 票券商(專營)

於 ADSL VPN 專線及固定 IP(TCP/IP)連線方式，透過 MQ Server 辦理「票券結算系統」各項作業及以 MQ+金鑰方式接收「短票利率編製系統」SIRIS、TAIBIR 資訊。

3. 股務代理機構及發行公司

於 Internet 以 CA 憑證辦理「股東通訊平台」電子投票作業、辦理「發行作業平台」登錄作業、辦理「基金資訊傳輸平台」無實體登錄及配發作業、及接收「報表網路傳送查詢系統」之證券存託 e-mail 報表。

4. 境外基金總代理、銷售機構(投信、投顧、券商、銀行、信託業)

於 Internet 以 CA 憑證辦理「境外基金交易平台」之各項交易，「境外基金申報公告系統」之申報作業。

5. 證券商(可兼營期貨商、票券商、基金總代理、銷售機構或股務代理機構)

於 ADSL 透過「SMART 系統」辦理「證券存託系統」各項結算交割作業、及透過 FTP 辦理自動收檔、及接收「報表網路傳送查詢系統」之證券存託 e-mail 報表；另兼營各項業務者比照前述作業方式及內容。

6. 銀行(兼營證券商、期貨商、票券商、基金總代理、銷售機構或股務代理機構)兼營各項業務者比照前述作業方式及內容。

(四) 相關單位

1. 證金公司

於 ADSL 透過「SMART 系統」辦理「證券存託系統」各項信用交易作業。

2. 相關公會

投信投顧公會於 Internet 以 CA 憑證查詢「境外基金申報公告系統」資訊；境外結構債相關公會(包括投信投顧公會、證券公會、銀行公會、壽險公會等)於 Internet 以 CA 憑證查詢「境外結構型商品申報公告」資訊；期貨公會於 Internet 以 CA 憑證查詢「期信基金申報公告系統」。

3. 清算交割銀行

於 ADSL VPN 專線及固定 IP(TCP/IP)連線方式，透過 MQ Server 傳送交割確認，及接收「票券結算系統」通知進行交割作業。

4. 代理清算銀行

於 ADSL VPN 專線及固定 IP(TCP/IP)連線方

式，透過 HTTP 傳輸協定傳送交割確認，及接收「票券結算系統」通知進行交割作業。

5. 實券保管銀行

以 ADSL VPN 及固定 IP(TCP/IP)連線方式，透過 MQ Server 傳送交割確認，及接收「票券結算系統」通知進行交割作業。

6. 外幣清算銀行

以 ADSL VPN 及固定 IP(TCP/IP)連線方式，透過 MQ Server 傳送交割確認，及接收「票券結算系統」通知進行交割作業。

7. 保管銀行

於 Internet 以 CA 憑證辦理「期信基金申報公告系統」之申報作業；並於 ADSL 透過「SMART 系統」辦理「證券存託系統」各項結算交割作業、及透過 FTP 辦理自動收檔、及接收「報表網路傳送查詢系統」之證券存託 e-mail 報表。

8. 還本付息機構：於 Internet 以 CA 憑證辦理「基金資訊傳輸平台」之債券所有人名冊及短票登錄作業，及接收「報表網路傳送查詢系統」之證券存託 e-mail 報表。

9. 款項收付銀行

10. 境外結構商品總代理(國外投資銀行)：於 Internet 以 CA 憑證辦理「境外結構型商品申報公告」之申報作業。

11. 資訊廠商：以 ADSL VPN 及固定 IP(TCP/IP)連線方式，透過 MQ Client 接收「短票利率編製

系統」SIRIS、TAIBIR 資訊。

12. 期貨基金公司：於 Internet 以 CA 憑證辦理「期信基金申報公告系統」之申報作業

(五) 股東、投資大眾

於 Internet 以 CA 憑證辦理「股東通訊平台」電子投票作業，於 Internet 網頁查詢「期信基金申報公告系統」、「境外基金申報公告系統」、「境外結構型商品申報公告」、「短票利率編製系統」資訊。

連線方式	Internet			ADSL 專線										Leased line	
連線介面	IE 瀏覽器			PSP	SMART	MTS	PB 工作站	主機連線				傳檔工作站	瀏覽器工作站		主機連線
安控方式	CA+WAF+SSL/ISSL	SSL	無	VPN	VPN +帳號密碼	VPN +MAC	帳號密碼	TCPIP	FTP	MQ	VPN+MQ Server	VPN + MQ Client	VPN + Http	DES金鑰	SDLC + (SNA)MQ Server
證期局	F1_基金公告 F4_期貨基金公告														
銀行局 (境外結構商品主管機關)	F2_境外結構商品資訊														
中央銀行 (境外結構商品主管機關)	F2_境外結構商品資訊				M1_結算作業			MO_交換債 MO_融通設質							B0_撥款通知
證交所		M2_報表傳送			M1_結算作業			MO_證券成交	MO_證券成交	MO_證券成交					
櫃買中心		M2_報表傳送			M1_結算作業			MO_櫃買, 興櫃成交	MO_櫃買, 興櫃成交	MO_櫃買, 興櫃成交					
期交所						CO_期貨商備援	CO_結算作業	CO_期貨成交	CO_期貨成交			B2_利率指標			
期貨商 (結算會員)						CO_期貨交易									

連線方式	Internet			ADSL 專線										Leased line		
連線介面	IE 瀏覽器			PSP	SMART	MTS	PB 工作站	主機連線				傳檔工作站	瀏覽器工作站		主機連線	
安控方式	CA+WAF+SSL/ISSL	SSL	無	VPN	VPN +帳 號密碼	VPN + MAC	帳號密 碼	TCP/IP	FTP	NQ	VPN+NQ Server	VPN + NQ Clie nt	VPN + Http	DES 全鑰	SDLC + (SNA)NQ Server	
票券商					M1_ 結 算作業							B0_ 票 券成交 B2_ 利 率指標	B0_ 票 券成交 B2_ 利 率指標	B0_ 票 券成交 B2_ 利 率指標		
發行公司	S1_通訊投票 S2_通知登錄 F3_無實體登 錄及配發	M2_ 報 表傳送			M1_ 存 託交易											
股務代理機構	S1_通訊投票 S2_通知登錄 F3_無實體登 錄及配發	M2_ 報 表傳送			M1_ 存 託交易											
境外基金總代 理機構(投信、 投顧、券商)	F0_境外基金 交易 F1_基金申報															
境外基金銷售 機構(投信、投 顧、券商、銀 行、信託業)	F0_基金交易 F1_基金申報															
證券商 (兼營期商或票 券商、基金總代	F0_境外基金 交易 F1_基金申報	M2_ 報 表傳送			M1_ 存 託交易	CO_ 期 貨交易			MO_SID A 自動 收檔			B0_ 票 券成交 B2_ 利		B0_ 票 券成交 B2_ 利		

連線方式	Internet			ADSL 專線										Leased line	
連線介面	IE 瀏覽器			PSP	SMART	MTS	PB 工作站	主機連線				傳檔工作站	瀏覽器工作站	主機連線	
安控方式	CA+WAF+SSL/ISSL	SSL	無	VPN	VPN +帳號密碼	VPN +MAC	帳號密碼	TCP/IP	FTP	MQ	VPN+MQ Server	VPN +MQ Client	VPN +Http	DES 全鑰	SDLC + (SNA)MQ Server
理、銷售機構、股務代理機構)	S1_通訊投票 S2_通知登錄 F3_無實體登錄及配發											率指標	率指標		
銀行(兼營證券商、期貨商、票券商、基金總代理、銷售機構、股務代理機構)	F0_境外基金交易 F1_基金申報 S1_通訊投票 S2_通知登錄 F3_無實體登錄及配發	M2_報表傳送			M1_存託交易	CO_期貨交易			MO_SID A 自動收檔			B0_票券成交 B2_利率指標	B0_票券成交 B2_利率指標	B0_票券成交 B2_利率指標	
證金公司					M1_存託交易										
境外結構債相關公會(投信投顧、證券、銀行、壽險公會)	F2_境外結構債資訊														
投信投顧公會	F1_基金公告														
期貨公會	F4_期貨基金公告														

連線方式	Internet			ADSL 專線										Leased line	
連線介面	IE 瀏覽器			PSP	SMART	MTS	PB 工作站	主機連線				傳檔工作站	瀏覽器工作站		主機連線
安控方式	CA+WAF+SSL/ISSL	SSL	無	VPN	VPN +帳號密碼	VPN +MAC	帳號密碼	TCP/IP	FTP	MQ	VPN+MQ Server	VPN + MQ Client	VPN + Http	DES 全繪	SDLC + (SNA)MQ Server
清算交割銀行												B0_ 票 券交割 B2_ 利 率指標			
代理清算銀行													B0_ 票 券交割 B2_ 利 率指標		
實券保管銀行												B0_ 票 券交割 B2_ 利 率指標			
外幣清算銀行												B0_ 票 券成交 B2_ 利 率指標			
保管銀行	F4_ 期信基金 申報	M2_ 報 表傳送			M1_ 存 託交易										
款項收付銀行				F0_ 基 金款項 收付											F0_ 基 金款項 收付

連線方式	Internet			ADSL 專線										Leased line	
連線介面	IE 瀏覽器			PSP	SMART	MTS	PB 工作站	主機連線				傳檔工作站	瀏覽器工作站	主機連線	
安控方式	CA+WAF+SSL/ISSL	SSL	無	VPN	VPN +帳號密碼	VPN +MAC	帳號密碼	TCPIP	FTP	NQ	VPN+NQ Server	VPN + NQ Client	VPN + Http	DES 全鑰	SDLC + (SNA) NQ Server
NCD 發行銀行 市庫券經理行 保證人銀行	S2_NCD 登錄														
資訊廠商						CO_ 期貨交易						B2_ 利率指標			
期貨基金公司	F4_ 期信基金申報														
境外結構商品 總代理(國外投資銀行)	F2_ 境外結構債申報														
還本付息機構 (金融機構)	F3_ 債券所有人 名冊及短票登錄	M2_ 報 表傳送				M1_ 存 託交易									
股東/ 投資大眾	S1_ 通訊投票		F1_ 基金公告 F2_ 境外結構 債公告 B2_ 利率指標 F4_ 期信基金 公告 M1_ 網際網路 餘額查詢												

圖表 2.1.3 各業務系統使用單位與系統資料間之關係說明

二、各業務系統之帳務功能說明

本公司具結算交割帳務業務系統包括證券存託系統、期貨業務結算系統、票券結算系統、境外基金交易平台，茲就其作業處理說明如下：

- (一) 成交資料處理來源：證券市場、櫃買市場、興櫃市場、期貨市場皆以盤中即時自交易所接收方式處理，固定收益類商品、境外基金則逐筆自相對業務使用單位接收。
- (二) 帳務記載內容：各系統於券皆記錄至客戶明細帳；款項部分因票券結算系統、境外基金交易平台及證券存託系統中興櫃市場辦理與銀行間款項劃撥交割作業，款項紀錄至客戶明細帳；證券存託系統、期貨業務結算系統僅紀錄參加人及結算會員結算交割款項帳。
- (三) 結算交割方式：證券存託系統之上市櫃集中市場買賣以淨額方式交割款項，全額交割股及興櫃市場買賣以總額方式交割款項，券皆採總額方式交割；票券結算系統採款券同步即時總額交割(RTGS)、款券同步即時雙邊款項淨額交割；境外基金交易平台依成交資料每日整批交割款券；期貨結算系統依成交資料計算部位及應存有保證金，並每日進行盤中洗價，以記錄其相關損益數額。

參、未來發展策略之探討

一、本公司至2011年7月實施保管股票全面無實體化後，保管標的範圍涵蓋了證券及金融市場各種商品，服務市場及主要使用者亦日益眾多，如何妥適管理各業務系統，以更單純及一致之介面服務眾多使用者及連線單位，並提供穩定、安全、效率的作業系統，實是本公司資訊管理未來積極努力之目標。

二、使用單位流程或介面更單純及一致之考量

(一)安控方式一致性

1. Internet安控整合：

除公告性質資料無需加設安控處理，現行Internet各業務系統皆已整合至CA憑證+SSL作業，且各系統皆可接受工商憑證、證期憑證、公開資訊觀測站憑證、自然人憑證。

2. ADSL專線處理安控整合：各業務系統則依工作站及主機連線性質不同，尚存有多種安控作法，為方便使用者操作，同質性安控機制應逐步考慮某程度之整合，未來新開發之業務系統亦應參考現行安控作法，儘量以提供使用者一致性之作法為考量。

(二)作業介面單純性

1. 為提供使用者更單純作業介面，同質性系統可考慮整合作業介面，如境外基金申報公告、境外結構型商品申報公告、期信基金申報公告等。

2. 可依不同使用者需求，建立對照業務範圍，而非所有使用者皆操作同一主畫面，不同使用者可依其業務權責操作不同業務畫面，以單純化使用者介面。

三、業務系統間作業功能模組整合之考量

(一)彙整業務系統內部功能

進行各業務系統功能蒐集，以索引分類方式建立業務功能需求說明文件，除可釐清各業務系統細項功能特性，亦可依此進行整合系統功能模組討論，參酌未來業務發展性，進行系統共用功能模組整合，並預留可能彈性成長空間。

(二)分享系統功能建置經驗

彙總之各業務系統功能資料，亦可作為未來建置新系統之參考，其他諸如系統架構、主要功能模組及流程、開發技術及時程、測試及驗證方式皆可提供新系統建置參考，若有需要亦可考量將新系統整合入現行系統中。

第二節 資料整合運用之研究

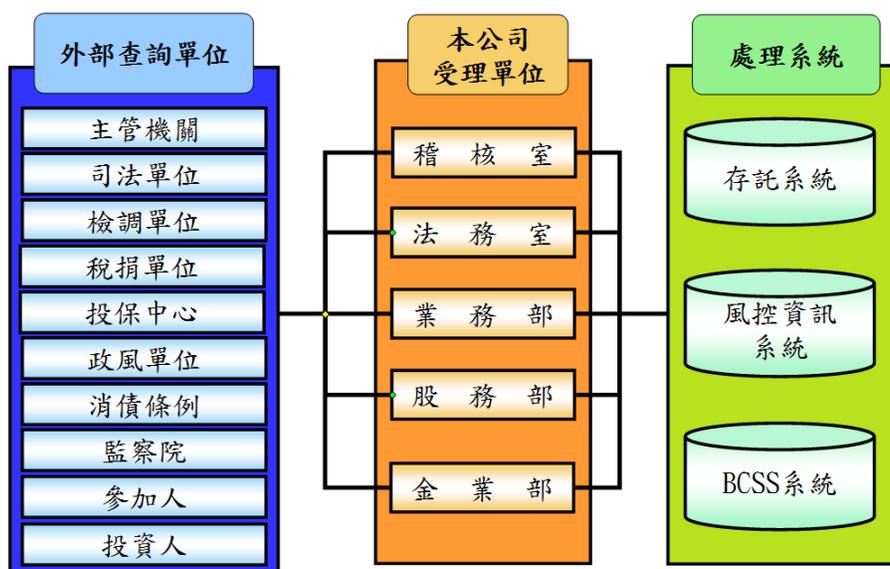
壹、研究目的與範圍

隨著本公司業務的拓展，保管商品越趨多元，商品面涵括證券、期貨、基金、票券、債券等，參加人涵蓋證券商、票券商、期貨商等，投資人亦包含各商品之投資人，因各業務之導入時序及商品屬性之差異，分別建置其各自獨立之業務系統，各業務系統使用技術亦有所不同，故各自運作及維護著不同來源(各應用系統的交易資料)或相同來源(參加人或客戶的基本資料)的資料，然而，若單一系統涵蓋所有業務的處理邏輯及資料，其維護之複雜度則會更為增加，因此本章節研究目的為如何整合組織中散佈的各種資料成有價值的資訊及跨不同異質系統、資料結構之複雜性與不同介面的差異性，可快速回應服務市場需求之探討。

本章節之研究範圍將著眼於目前本公司各種業務系統提供資料查詢作業為基礎，以業務系統歷史資料調閱整合為切入點，將具有調閱及分析價值之歷史資料整合於獨立資料庫，以不干擾日常作業之資料及應用系統資源為前提，提昇資料查詢調閱之效能及擴大服務範圍，並整合公司內部單位業務分析統計之資料建立整體資料倉儲。

貳、資料整合之現況說明

現行本公司受理外部單位之資料調閱種類甚多，提供之資料內容及報表格式亦多不同，所調閱之資料處理部份分別由「證券存託系統」(以下簡稱存託系統)、「票券保管結算交割系統(BCSS系統)」(以下簡稱票券系統)、「風險控管系統」(以下簡稱風控系統)三個系統進行產製，例如：法院及法務部行政執行署之專線電子函查作業，由「風控系統」提供其所需之查詢資料；集保帳戶(含證券及債券)及登錄帳戶之歷史交易資料調閱及其他有關單位之書函查詢，則於「存託系統」提供其所需之查詢資料；有關票債券帳戶歷史交易資料調閱，另由「票券系統」提供其所需之查詢資料。圖表 2.2.1 為查詢歷史資料調閱系統示意圖：



圖表 2.2.1 歷史資料調閱系統示意圖

由於「存託系統」目前使用 IBM 大型主機作業，調閱歷史資料作業因時效要求，常常需於白天營業時段處理，且其

處理之資料量亦較龐大，造成與存託系統日間證券市場作業對主機資源之使用相互排擠，進而影響存託系統運作。

「存託系統」與「票券系統」皆屬於線上交易處理系統（OLTP，On-Line Transaction Processing system），即將交易資料進行即時處理，其檔案及資料庫結構亦專為 OLTP 特性而設計，使用端之資料可以即時送到應用系統中進行處理，且能在很短的時間處理完畢並回覆處理結果，OLTP 系統著重即時的回應時間（Response Time），支援大量的使用者同時發送資料修改及新增等行為，也稱為即時系統（Real time system），有別於歷史資料調閱需求，則是以一段時間的大量資料作為存取主體，存取模式是以唯讀方式（Read Only）處理一項複雜查詢－（通常需對多個維度及彙整的資料進行複雜運算）。基於上述原因，未來之發展策略為將每日交易資料（Current Data）與龐大的歷史資料（Historical Data）分離，使 OLTP 系統專注於處理符合業務週期的交易資料，提升效能並縮短回應時間。另歷史資料調閱作業也能擁有其適合的資料庫結構，以符合其查詢需求並加速查詢效能。

參、未來發展策略之探討

一、整合外部單位資料調閱業務及內部單位業務分析統計之資料需求

(一) 建置交易歷史資料之查詢分析模型倉儲資料庫

本階段資料整合作業主要配合「查詢資料庫系統」專案，整合現行由「存託系統」維護及保存之集保帳戶交易歷史資料，移轉至開放系統平台，並建置查詢分析模型倉儲資料庫。由於「票券系統」現行已建置完整之調閱程序，因此專案建置規劃將由「票券系統」提供票債券帳戶歷史交易及餘額資料整合至查詢資料庫，故未來外部單位之資料調閱將統一由查詢資料庫提供。

(二) 整合歷史交易或其他業務分析需求之資料至查詢資料庫

整合現行由「境外基金系統」維護及保存之基金交易歷史資料及其他供業務分析統計需求之資料，轉置至倉儲資料庫。現行基金系統未建置歷史資料庫，其歷史交易資料維護及存放為定期將資料匯出，再以檔案格式壓縮保存於檔案系統，若遇有調閱需求，則再將保存於檔案系統之資料進行匯入資料庫作業，如此作業時間將隨資料增加而延長，未來規劃將歷史交易資料整合至查詢資料庫，以降低儲存成本並提高服務效能。若有其他業務分析需求之資料亦在此階段整合至查詢資料庫。

二、資料庫管理系統之特性探討

由於本資料整合係將線上交易處理（OLTP）系統產生之大量歷史資料彙整、整理及查詢運用，有別於線上交易處理）系統之交易務性處理，故往往整合後之資料為了完成擷取及

查詢分析目的，尚需大量的計算及篩選，本項特色正適用資訊系統之資料儲存理論－資料倉儲，作法是將存入資料庫之大量資料，利用特定分析方式（如：線上分析處理（OLAP）、資料採礦（Data mining））及資料模型設計（如：多維度方式（Dimensional approach）、正規方式（Normalized approach）），以提供大量資料儲存、快速分析能力，因此系統查詢及分析處理效率較佳。

由於資料倉儲之四個基本特性為主題導向（Subject-Oriented）、整合性（Integrated）、非暫存性（Nonvolatile）、時間變動性（Time-Variant）的資料累積，並以多維模型多層次的資料組織形成，故可預見其查詢效能及儲存容量將會為此類型資料庫一大瓶頸，若能選用針對分析、資料倉儲巨量資料而設計之資料庫管理系統，將可比傳統交易資料庫更能提昇查詢效能及有效壓縮資料存量。

本公司依實際測試驗證 IBM DB2 及 SYBASE IQ 之結果分別說明此二資料庫管理系統特性及效能，如下圖表 2.2.2，未來將依業務系統之特性作為選用資料庫管理系統之參考：

特性	DB2	SybaseIQ
資料儲存方式	row-base(水平儲存)	column-base(垂直儲存)
資料異動記錄	記錄每筆資料異動	記錄每個頁(Page)的異動
備份與回復	可回復至指定之任意時間點(配合 LOG)	僅可回復至前次備份完成的時間點

<p>產品特性</p>	<ol style="list-style-type: none"> 1. 支援線上交易處理 (OLTP) 或線上分析處理 (OLAP) 使用，管理者需透過參數設定及調整方式達到特定效能 2. 具資料儲存自動調整表空間之功能，壓縮後空間效能顯著 3. 具資源自主調整與動態管理能力，維護管理具彈性 4. 資料以「行」存儲 (Row-Base)，若為即席式查詢 (Ad-Hoc Query) 而未有適合之 Index 者，可能為 Table Scan 致使效能明顯下降 	<ol style="list-style-type: none"> 1. 專門為分析型應用與資料倉庫而設計，不需調整即可達到特定效能，維護管理較簡易 2. 採用資料壓縮及 FP 索引技術使壓縮比更大，空間效能更為顯著 3. 資料以欄位方式 (Column-Base) 垂直分割儲存，只存取查詢所需欄位，若查詢非為全欄位式查詢，則可有效降低 I/O 4. 保證至少存在一個索引，每個查詢組合皆為索引掃描 (Index Scan)，故可支援即席式查詢 (Ad-Hoc Query) 5. 採用 Bit-Wise Index，除 Bit-Wise 亦提供多種索引類型選用以提升查詢性能
-------------	---	---

圖表 2.2.2 IBM DB2 及 SYBASE IQ 特性

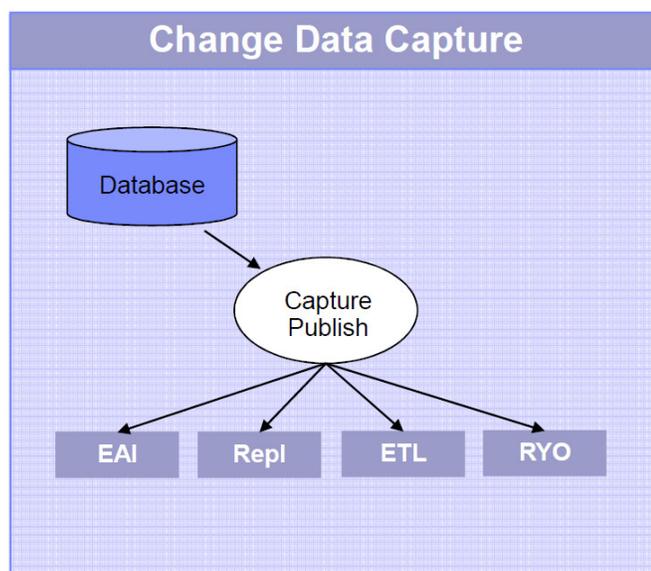
三、資料整合技術探討

資料倉儲建立後，即須持續不斷的將每營業日後之當日總結資料轉入資料倉儲，常見之資料整合技術約有四類：異動資料擷取 (Change Data Capture)、資料複製 (Data Replication)、資料庫聯邦 (Federation)、ETL (Extract,

Transform & Load) ，茲簡述如下：

(一)異動資料擷取 (Change Data Capture)

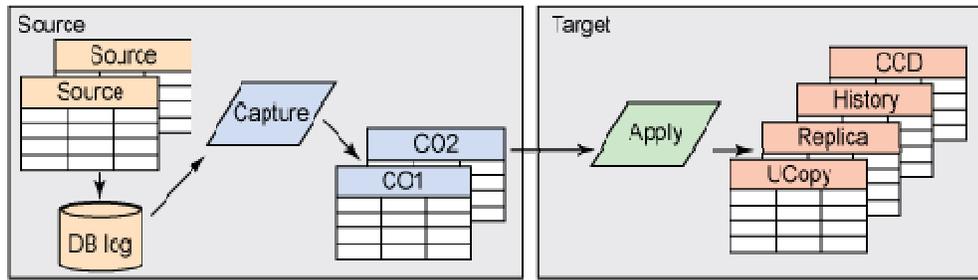
CDC (Changed Data Capture) 機制從字面上可知其著重於「異動資料」，即從來源資料庫中將「異動資料」以同步模式 (Synchronous Mode) 或非同步模式 (Asynchronous Mode) 發行 (Publish) 至目的資料庫，再進行後續資料使用及處理。



圖表 2.2.3 異動資料擷取

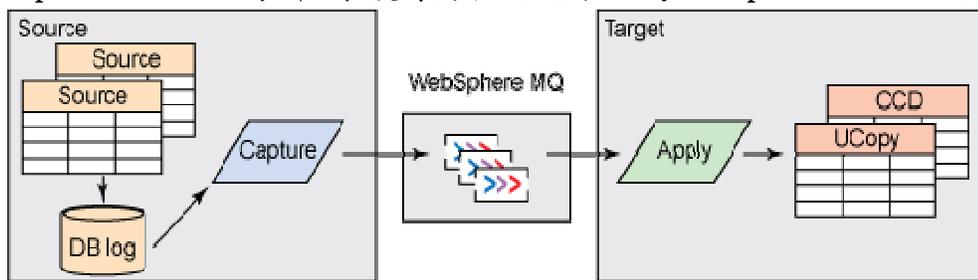
(二)資料複製 (Replication)

資料複製 (Replication) 主要分為 SQL Replication 及 Q Replication。SQL Replication 使用臨時表來保存從資料庫交易日誌中讀到的資料異動增量 (Incremental)，再以 SQL 將該增量寫到目標表中，其效能較慢。



圖表 2.2.4 資料複製：SQL Replicatio

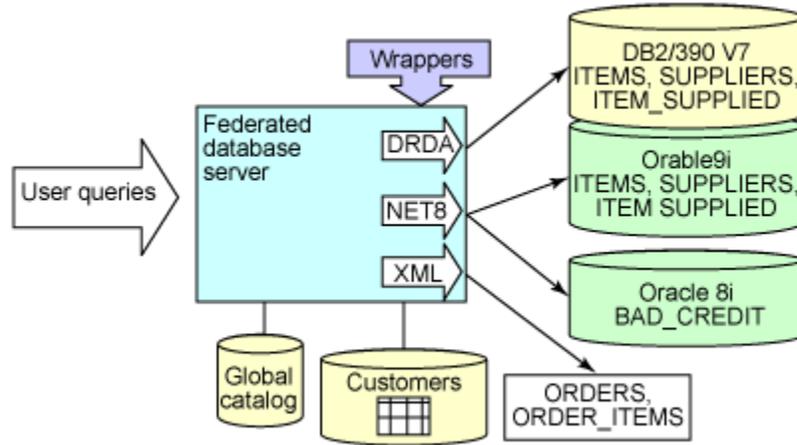
Q Replication 為將讀到的資料異動增量寫入 WebSphere MQ 佇列。MQ 佇列成為傳輸機制，而後運行在目的伺服器上之 Q Apply，從接收端佇列讀取資料，將重播 (Replay) 交易事務，並將異動寫入目標表。故 Q Replication 為即時複製其效能較 SQL Replication 佳。



圖表 2.2.5 資料複製：Q Replication

(三) 資料聯邦 (Federation)

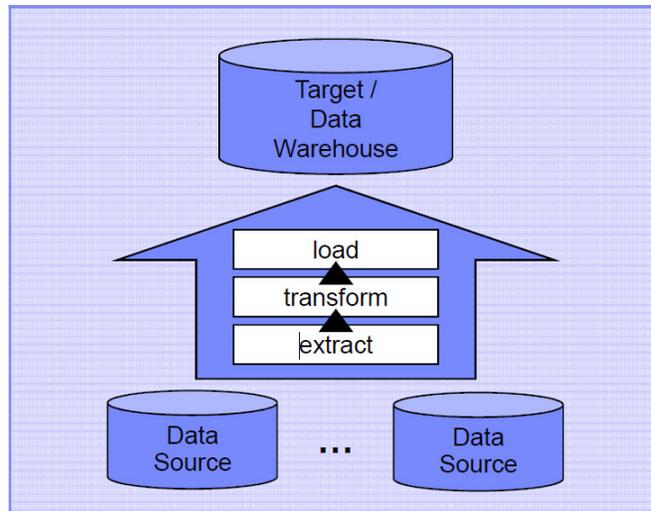
資料聯邦 (Federation) 是指將多個資料源以單一 個體方式管理，使應用程式能夠存取與整合分散各處的 資料源，又可維持各資料源的自主及完整性，在聯邦系 統上註冊遠端資料表後，可以像使用本地表格般使用這 些資料，從使用者角度就如同存取單一資料庫，而資料 並非實際整合，資料聯邦以效能來換取資料整合的好 處，因此在效能面，普遍比傳統資料倉儲工具低。



圖表 2.2.6 資料聯邦 (Federation)

(四) ETL/ELT (Extract, Transform & Load)

資料進入資料倉儲不僅僅只是彙總，尚需經過處理，而 ETL/ELT 即為將資料從來源端經過萃取 (extract)、轉置 (transform)、載入 (load) 至目的端的資料處理過程。由於 ETL 是極為複雜的過程，而手寫程式又不易管理，故多採用工具協助 ETL 的開發，並運用其內建的 Metadata 功能儲存來源資料與目的資料的對應 (Mapping) 及轉換規則，此外，ETL 工具亦可提供較強大的連接功能 (connectivity) 連接來源端及目的端，開發人員不需熟悉各種異質平台及不同的資料結構，亦能進行開發。



圖表 2.2.7 ETL/ELT (Extract, Transform & Load)

綜上，若需求為即時資料同步則可選用異動資料擷取 (Change Data Capture) 或資料複製 (Data Replication) 方式，若需求為即時資料存取且資料僅有一份不需彙集者，可選用資料聯邦 (Federation)，若為大量資料整合且可批次控制者，則可選用 ETL/ELT (Extract, Transform & Load)，除了資料聯邦 (Federation) 方式之外，異動資料擷取 (Change Data Capture) 或資料複製 (Data Replication) 方式皆可搭配使用 ETL/ELT。本項規劃之資料整合係將線上交易處理 (OLTP) 系統產生之大量歷史資料彙整、整理及查詢運用，故評估較適合採用 ETL/ELT。

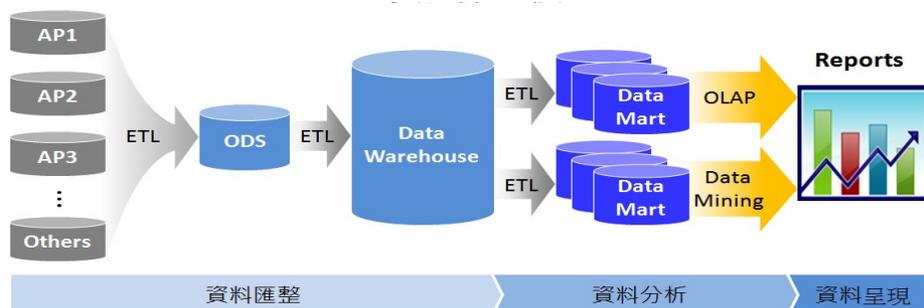
四、未來規劃之概念性架構

本公司無實體化之後，未來存券、結算交割都將全面進入電腦化時代，由於本公司提供多種商品保管登錄及結算交割等業務，故日常運作的資料庫系統資料涵括相當廣泛：

- (一)、商品資料面包括證券、期貨、基金、票券、債券等，
- (二)、參加人資料面涵蓋證券商、票券商、期貨商、銀行

等，（三）、發行人資料面包含有價證券無實體登錄、強制分戶保管、發行公司股務相關資料，（四）、投資人資料面包含各商品之交易性資料與非交易性資料等完整且大量的投資人歷史資料，這意謂著電子資料將與日俱增，為了讓電子資料的管理及存取更有效率，並確保日常作業之資料及應用系統資源不受干擾，整合公司內部資料建立整體資料倉儲是未來的規劃策略。

未來規劃資料倉儲的概念性架構將如下圖示：資料來源收集自日常運作的各資料庫系統，經過資料收集整合的過程（ETL/ELT）建立資料倉儲（Data Warehouse）或不同特定目的資料超市（Data Mart），再透過線上即時分析（OLAP）或資料挖掘（Data Mining）將資料提供給資料需求者作為資料分析（Data Analysis）、分析報表（Reporting）等其他應用。



圖表 2.2.8 資料倉儲概念

肆、小結

本公司無實體化之後，未來存券、結算交割都將全面進入電腦化時代，由於本公司提供多種商品保管登錄及結算交割等業務，故日常運作的資料庫系統資料涵括相當廣泛：

(一)、商品資料面包括證券、期貨、基金、票券、債券等，(二)、參加人資料面涵蓋證券商、票券商、期貨商等，(三)、發行人資料面包含有價證券無實體登錄、強制分戶保管、發行公司股務相關資料，(四)、投資人資料面包含各商品之交易性資料與非交易性資料等完整且大量的投資人歷史資料，這意謂著電子資料將與日俱增，為了讓電子資料的管理及存取更有效率，並確保日常作業之資料及應用系統資源不受干擾，整合公司內部資料建立整體資料倉儲是未來的規劃策略。

下圖為說明未來規劃企業資料倉儲的概念性架構：資料來源是自日常運作的資料庫系統收集而來，經過資料收集整合的過程（ETL/ELT，Extract、Transform & Load）建立資料倉儲（Data Warehouse）或不同特定範圍的資料超市（Data Mart），這些資料超市是資料倉儲的子集，再透過線上即時分析（OLAP）或資料挖掘（Data Mining）將資料提供給資料需求者作為資料分析（Data Analysis）或分析報表（Reporting）或其他應用。



圖表 2.2.9 資料倉儲概念

第三節 透過軟體工程提昇系統品質

壹、前言

依據研究¹，為了要符合企業對未來之靈活性、創新、降低成本、提升業務能力和提供豐富的使用者介面…等規劃方向，IT 服務在人員、流程和技術議題上面臨了一專業分工、管理複雜化、快速反應市場、兼顧安全與效能…等等挑戰，請詳圖表 2.3.1 IT 服務所面臨的新挑戰。

為了符合未來敏捷的企業服務需要，IT 資訊系統會日趨複雜，複雜的 IT 系統會提高風險：正確性風險－做對了嗎？效率性風險－來得及完成嗎？資安風險－夠安全嗎？IT 軟體開發部門正面臨的最大挑戰是：如何兼顧企業營運目標及降低日趨複雜所帶來的軟體品質風險？

本節主要在闡述，IT 軟體開發部門為確保服務品質及降低風險之導入軟體工程(Software Engineering)及自動化策略之研究。

構面	趨勢	企業營運目標	IT 面臨的挑戰
人員	專業分工	<ul style="list-style-type: none">●降低全球成本結構●靈活的人員配備●持續的生產力	<ul style="list-style-type: none">●整體計畫變得很複雜化●人力盤點要落實●複雜的管理結構
流程	有彈性	<ul style="list-style-type: none">●提高服務品質●降低專案風險●加速回應市場或客戶	<ul style="list-style-type: none">●強調快速交付優於品質●不一致的結果●降低完整性
技術	複合式技術	<ul style="list-style-type: none">●快速開發	<ul style="list-style-type: none">●失去 IT 服務交付應有

¹ *The Applications Handbook - A Guide to Mastering the Modern Application Lifecycle*, 2010, Hewlett Packard

	組合 豐富的網際 網路應用 雲端技術	●提供豐富的使用者介面 ●規模經濟，降低TCO	的要求標準(ALM 應用系統生命週期) ●如何兼顧安全與效能 ●增加系統間彼此的相依性
--	-------------------------------------	----------------------------	---

圖表 2.3.1 IT 服務所面臨的新挑戰

貳、軟體工程自動化與公司內應用現況

何為軟體工程？軟體工程為將系統化的、規範的、可度量的方法應用於軟體的開發、運作和維護的過程，即將工程化應用於軟體中(IEEE[IEE93])。軟體工程可稱之為軟體開發之品質管理機制，其目的為持續改善。

依據 IEEE SWEBOK²軟體工程知識體系，說明軟體工程之領域可包含：

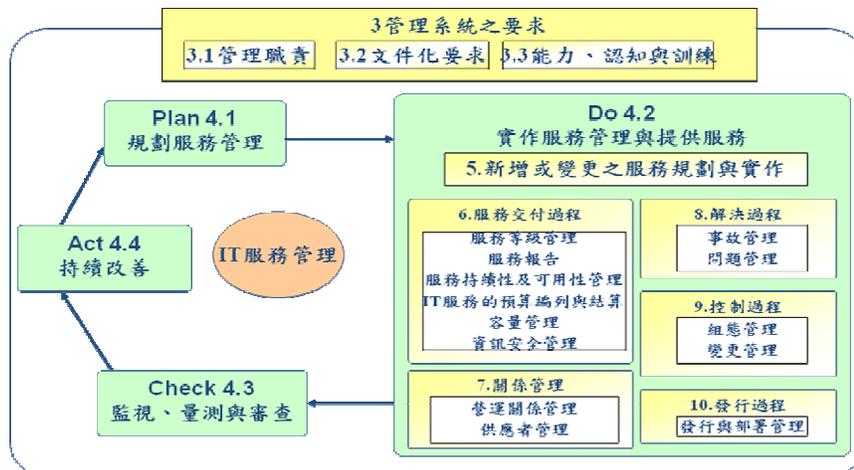
- Software requirements 軟體需求
- Software design 軟體設計
- Software construction 軟體建構
- Software testing 軟體測試
- Software maintenance 軟體維護
- Software configuration management 軟體組態
- Software engineering management 軟體工程管理
- Software engineering process 軟體工程流程
- Software engineering tools and methods 軟體工程工具與方法

² Software Engineering Body of Knowledge (SWEBOK),2004,IEEE

●Software quality 軟體品質

如同 SWEBOK 所述，軟體工程應包含該過程中應用的技術—技術方法和自動化工具及為建造高品質軟體提供一個可管理的架構(Framework)，其中又以自動化為主要的驅動力量，試問若沒自動化，軟體開發人員如何在被壓縮的時程內完成暨符合業務需求又兼具品質的軟體。像鞋匠孩子的故事：鞋匠總是忙於給其他人做鞋，他自己的孩子卻沒有鞋穿；在過去，很多軟體開發人員便是“鞋匠的孩子”，雖然建造了使其他人工作自動化的複雜系統，但自己卻幾乎很少使用自動化。

軟體工程可持續改善以確保品質，自動化機制可降低系統日趨複雜所帶來的風險以提高軟體交付之正確性、效率性及安全性；但如何透過管理機制以落實標準化？如何確定提升之軟體品質符合企業 IT 服務品質要求呢？IT 服務管理制度—ISO2000 國際標準可提供很好的應用參考，其範圍請見圖表 2.3.2 IT 服務管理制度—ISO20000。



圖表 2.3.2 IT 服務管理制度 - ISO20000

其中又以組態管理(Configuration Management)、變更管理(Change Management)、發行與部署管理(Release and Deploy management)及發行前之必要測試(Test)與服務品質息息相關，是導入軟體工程管理自動化最佳應用範圍，目前公司軟體開發程序與 ISO20000 標準及軟體工程應用之關連性，請見圖表 2.3.3 IT 服務管理制度與程序及軟體工程應用對照。

IT 服務管理制度 (ISO20000)	本公司內部相關程序	軟體工程應用
組態管理 Configuration Management 定義及控制服務與基礎建設之組件，並維護正確的組態資訊	資訊系統開發維護程序書 介面規格管理作業說明書	軟體版本控管 Software Configuration Management/Version Control (簡稱 SCM)
變更管理 Change Management 確保所有變更，在受到控制的方式下，受到評鑑、核准、實作及審查	資訊系統開發維護程序書 資訊系統變更管理作業說明書 資訊系統安全控管作業說明書 介面規格管理作業說明書	軟體生命週期管理 Application Life-cycle Management (簡稱 ALM)
發行與部署管理 Release and Deploy Management 對發行至實際環境版本變更(一或多個以上)之交付、分發及追蹤	資訊系統變更管理作業說明書	持續整合與交付—編譯與部署 Continuous Integration and Delivery—Build and Deployment (簡稱 CI&CD — B&D)
軟體測試 Software Test 受到控制之驗收測試環境，應在分發之前予以建立，並建置(Build)及測試所有的發項目	資訊系統開發維護程序書 資訊系統品質測試作業程序書	持續整合與交付—軟體測試 Continuous Integration and Delivery—Software Test (簡稱 CI&CD — TEST)

圖表 2.3.3 IT 服務管理制度與程序及軟體工程應用對照

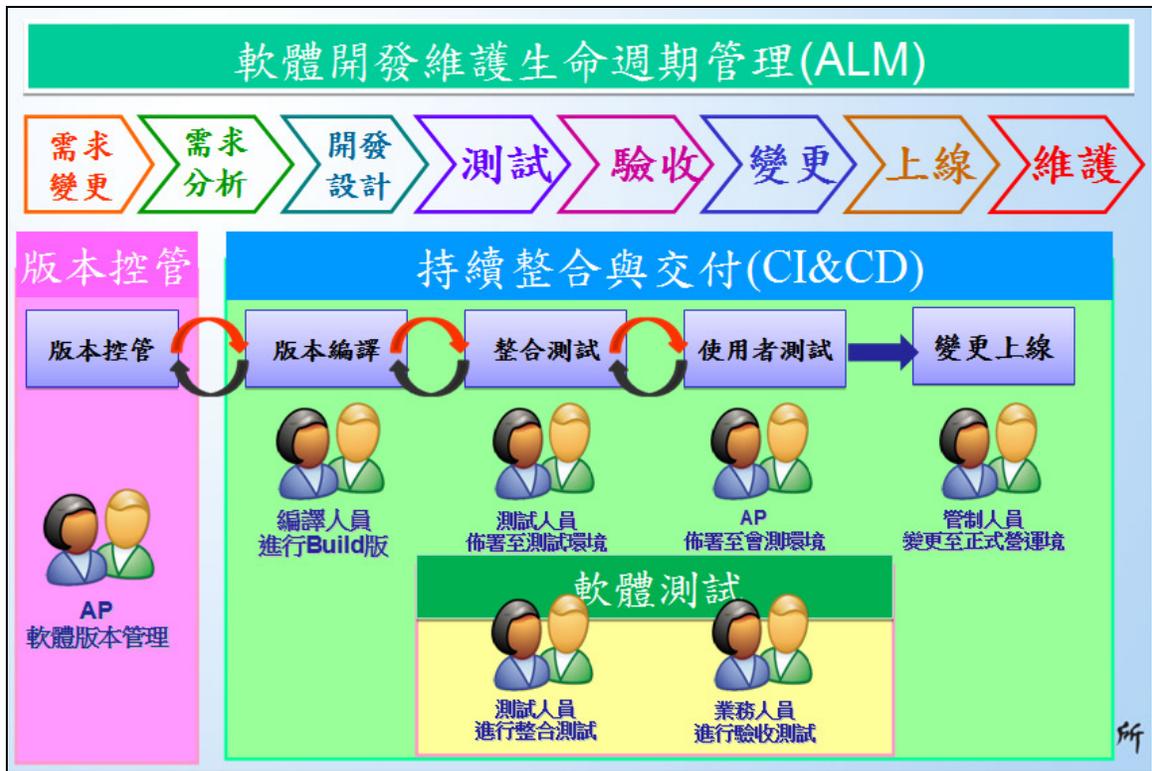
另整理公司內部與服務品質相關流程自動化情形，描述如圖表 2.3.4 公司內部流程自動化現況如下：

現況說明	資規部	金資部
軟體工程 (ISO2000)應用範圍	是否自動化	是否自動化
SCM 軟體組態/版本控管 (組態管理)	是	是
ALM 軟體生命週期管理 (變更管理)	否	是
CI/CD-B&D 持續整合與交付- 編譯部署 (發行與部署管理)	否	否
CI/CD-TEST 持續整合與交付- 軟體測試 (測試活動)	否	否

圖表 2.3.4 公司內部流程自動化現況

參、軟體工程自動化未來發展策略之探討

配合軟體工程於軟體服務品質相關之應用領域，參考如圖表 2.3.5 軟體工程應用，並依現況改善需要，規劃未來發展策略，請參考圖表 2.3.6 導入軟體工程自動化規劃策略。



圖表 2.3.5 軟體工程應用

階段	軟體工程自動化範圍				導入規劃內容
	ALM	SCM	B&D	TEST	
1	V				電子化軟體生命週期管理表單
2		V			提升軟體組態管理
3			V		自動化軟體發行與部署
4				V	提升軟體測試工具
5				V	導入軟體測試自動化機制

圖表 2.3.6 導入軟體工程自動化規劃策略

以下說明各階段之規劃內容：

- (一)第 1 階段，電子化軟體生命週期管理表單：將相關為進行軟體開發與維護所需表單電子化，並提供相關電子簽核流程。
- (二)第 2 階段，提升軟體組態管理系統：將現行軟體組態管理系統提升至新版本，以提供建立基準(Baseline)、軟體設計結構、支援軟體編譯建構與部署(Build and Deploy Management)...等新功能，並整合第 1 階段之資訊系統開發維護流程表單電子化系統，自動管理軟體從需求提出、分析、設計、測試及變更上線所需之原始碼版本控管作業。
- (三)第 3 階段，自動化軟體發行與部署：導入資訊應用系統自動化編譯與部署，整合第 1 階段之資訊系統開發維護流程，以提供自動編譯整合測試版本及正式營運版本，並提供自動佈署至整合測試及正式營運環境；另提供正式營運環境可回復至前一版本之自動部署機制及提供將變更紀錄或檔案異動紀錄，以附件型態回存至相關電子表單，以強化變更之稽核管理。
- (四)第 4 階段，提升軟體測試工具：提升或導入新工具，以配合軟體開發技術的更新及適當保護機敏資料，提供支援 Web 2.0、XPath、AJAX、.Net、機敏資料保護機制...等功能，並將現有已錄製之測試個案轉換至新版本或新工具；另整合第 1、3 階段完成之資訊應用系統自動化編譯與部署系統，於發佈及部署整合測試版本後自動執行功能回歸測試，並

將測試報告與結果，以附件型態回存至相關電子表單。

- (五)第 5 階段，導入軟體測試自動化機制：導入能整合於第 1-4 階段之工具，以軟體測試專業分工、建立測試管理流程、自動化軟體測試作業和進行軟體品質管理及確保持續改善。

預期透過導入與 IT 服務品質相關流程之軟體工程自動化機制，可達成之總體效益如下：

- (一)提升軟體品質以確保業務服務品質。
- (二)降低因業務需要造成 IT 系統日趨複雜所帶來的風險，以提高軟體產品之正確性、效率性及安全性。
- (三)縮短軟體發行時間，以快速反應市場或業務需要。

第四節 中文字碼整合

壹、研究目的與範圍

在資訊系統「中文亂碼」及「缺字」為中文電腦系統中常見之現象，尤其在以往中文並未有統一內碼的時代更是如此。而上述亂碼現象在資訊系統的實作上將會使原始資料發生漏失甚而發生資料錯誤或張冠李戴之現象，對資料正確性影響甚鉅。因此在未來資訊系統發展對中文編碼之整合規劃將是必須面對之重要課題。

西方系語言為拼音語言(英美語系)，因此只要極少數量之字母及符號即可表示完整語言。也因此其電腦系統大多使用 ASCII (American Standard Code for Information Interchange, 美國信息交換標準代碼) [7]表示。但中文世界或非拼音語系而言，中文字絕非 100 多個碼位可以容納，也就是說用一個位元組(Byte)已無法容納所有中文字，也因此發展出多位元組的編碼方式，來表達及容納更多的中文字，例如：Big5 碼等。

由於在 Big5 碼尚未產生前由於當時的個人 PC 並無通用的內碼，因此使得 Big5 碼幾乎成為臺灣地區中文電腦的標準內碼，目前台灣地區使用之各項版本資訊如圖表 2.4.1 所示：

	說明
BIG5-1984	最早由資策會所定的版本
BIG5-ETen	倚天版本
CP950	微軟所使用的版本
BIG5-2003	2003年由財團法人中文數位化技術推廣基金會接受經濟部標準檢驗局委託，召集國內業者代表、專家和學者，就BIG-5編碼字元表原始版本和各主要業界版本予以重整之最新版本
BIG5-IBM	IBM所使用的版本

圖表 2.4.1 台灣地區所使用的 BIG5 碼主要版本圖

由於各廠商對 Big5 標準不一致，在資訊系統實作資訊交換時也會產生所謂的「亂碼現象」。

除 PC 端之發展外狀況外，國內各大的行政資訊系統所使用之中文編碼發展也是需要我們注意，例如下表由主計處(97年)於統計整理之資訊^[9]如圖表 2.4.2：

資訊系統	中文編碼	字集數	編碼方式	預計新版字集數	新字申報	備註
MS Windows	BIG5/Unicode	2 萬以上	2~3 Bytes	70,195		
Linux	BIG5/Unicode	2.5 萬以上	1~4 Bytes	70,195		Utf-8 運作
戶政 EUC-CSIC	EUC-CSIC	7 萬以上	4 Bytes	92,038	700	
財稅	財稅/稅務碼	19,443/21,422	4 Bytes		2,422	
公路監理	電信碼	16,384	2 Bytes			
圖書館	CCCII	75,684	3 Bytes			
CNS 標準	CNS 11643	48,027 (81 年版)	3 Bytes	92,038 (94 年版) ³	國語會 4 萬多字 五大行政 約 8 千	交換碼
業界標準	BIG5/BIG5E	13,053/3,954	2 Bytes			BIG5-20 03
ISO 標準	ISO 10646 CJK+A+B ⁴	70,205	4 Bytes	我國提報 1 萬多字 至 IRG 會議 中	審查 CJK ext C1	CNS116 49

圖表 2.4.2 各版本 BIG5 碼比較表

³ 至 101 年 3 月共計 106,044 字數。

⁴ 至 101 年 3 月為 CJK+ExtA+ ExtB+ ExtC+ ExtD 版本為 Unicode 6.1，字數為 74,616 字數

由上列表可得知，全國五大行政資訊系統之中文編碼，戶政^[10]、財稅^[11]及公路監理^[12]編碼較為特殊，其餘仍以 Big5 為主。而值得注意的是在 100 年度財稅中心及移民署^[13] 皆改用 UCS-4(Universal Character Set-4 bytes)為其內碼基礎，同時字型則參考全字庫(CNS11643 中文標準交換碼全字庫)^[14] 為其標準。而正在實作中之新一代戶役政系統亦採用同財稅中心及移民署一樣之字碼及字型方案。

從以上整個的中文編碼發展來看，雖然有朝向 Unicode^[15] 編碼靠攏之趨勢，但中文編碼到目前為止仍可以說處於相當相當混亂時期，也因此不可避免衍生許多問題，在下面章節我們將對中文編碼現況及其面臨之問題作一較深入之探討。

貳、中文編碼現況

在上一章節對於本研究作一概述後，接下來在本章節中，我們將針對中文編碼現況尤其是現今所面臨之問題作一詳細介紹，對於中文編碼混亂所衍生之問題以下我們分為二個部份來加以說明：中文碼待克服問題及中文碼於資訊系統的實作中衍生之問題。

一、中文碼待克服問題

對於目前各有所依之中文編碼所衍生之問題已有許多研究提出，余保倫(2006)在其「中文數位化 Metadata 之探討」^[16] 研究報告指出資訊環境實作困擾及待克服之問題有下列幾項：

(一) 中文內碼缺一致性的標準

在上一小節敘述中我們可看到雖然 Big5 實質上成為國內中文內碼之標準，但各廠商在實作上各有不同之遵循標準，而這也將造成不同廠商實作之系統在資料交換上不可避免的產生問題。

(二) 國內完整字集彙整不易

在各政府機關言，各機關造字彙整外，民間單位之造字彙整將是一持續工作，如何建置涵蓋度夠，可作為所有單位(或個人)遵循之字集，並提供足夠字給所有人於業務使用，此工作困難度相當高。

(三) 國內與國際標準間之差異

如同第一點所言，目前 CNS11643 為最大及最完整之字集，但基於資訊系統發展之國際趨勢，將

Unicode 當成 CNS11643 之實作內碼已是不可避免之選擇，也因之我國目前盡力將 CNS11643 所有字納入 Unicode 標準，但仍有相當落差 (Unicode 6.0 74,616 字，CNS11643 106,044 字)。

(四)全面處理中文問題意願不高且成本頗高

中文問題在處理上除上述標準建立是一極龐大工程外，為了處理中文問題，系統有可能必須改變包含：作業系統、資料庫、程式需改寫、列印驅動程式及各種周邊工具產品須改變等，而這樣所花費時間及金錢成本與比率不高之中文缺漏字問題相比，最後導致願意全面處理中文問題的公司非常稀少。

(五)資訊產業界支持程度較為緩慢：

雖然各資訊廠商已將 Unicode 支援當成主要內碼為其發展產品之趨勢，但支援版本速度仍較為緩慢。

(六)整體性的中文方案較稀少

目前市場中對中文問題之解決方案仍是不多，很多廠商仍是著重於 Big5 造字管理，而對未來以 Unicode 為內碼之大字集解決方案仍不普遍。

(七)以音為主的語言直接引用內碼較為困難

在其第一問題敘述中我們亦已看到，由於缺乏一致性標準，故在系統資料交換中常發生資料錯誤甚至資料漏失狀況

發生，而這通常發生在較大內碼字集轉至較小內碼字集時發生。而其所提出之第 4、5 及 6 項問題，正是目前中文編碼所面臨最大問題。由於中文問題完整之解決方案通常成本相當高，而且中文字出現問題時比率不高，一般使用者多半選擇容忍不正確之中文字缺漏現象，而不願花費大量成本去實作較為完整之解決方案。

而除以上編碼標準眾多之問題外，目前採 Big5 編碼字集之資訊系統刻正面臨缺字及造字空間不足問題，所謂缺字在謝育平等(2004) [17] 「攜式字集資源-用以解決缺字問題」文中定義，「缺字」問題是指「電腦內碼對應文字的不完備造成無法順利瀏覽及輸入未收錄的文字，無法順利傳播及查詢內該文字的文件，難以在典藏過程是描述新遇到的缺字及完整統一造字的問題」。而這也是 Big5 編碼最大之問題之一，中文系統經過多年(自 1984 年以來)應用發展，其造字空間(5,809)已有將溢滿趨勢，可以想見當造字空間滿時。採用此編碼之中文系統將會無法再提供任何字造字服務。

而除上述問題外，我們也不可忽略中文問題在資訊系統的實作中衍生之問題。在本研究中我們將對此問題做一分析及探討。

二、中文碼在資訊系統的實作中衍生之問題：

資訊系統中資料經過之節點很多，而每節點對編碼的的實作及支援程度將會影響整個資料的正確及完整，甚而影響到呈現及列印。以下我們將針對資訊系統面臨的七項問題分別討論；作業系統、儲存、開發工具與程式、輸入、輸出、列印及交換等議題作一探討：

(一) 作業系統

各作業系統所支援及內定之編碼方式各有不同，從圖表 2.4.3 可以得知各作業系統編碼之不同。各作業系統支援之碼頁(code page)種類及其各種碼頁支援之規格版本在在都影響資料處理之正確性，亦同會影響在其上面運作之程式及各項產品。

作業系統	內定編碼	備註
Winsows 95	Big5	中文版(MS950)
Winsows 98	Big5	中文版(MS950)
Winsows 2000	Unicode(UCS2)	中文版內定使用MS950，但核心底層資料處理為Unicode (無法處理UCS4，亦即無法支援Unicdeo 3.0以上規格)
Winsows 2003	Unicode(UCS4)	中文版內定使用MS950，但核心底層資料處理為Unicode (可支援Unicode3.0以上之規格)
Winsows XP	Unicode(UCS4)	中文版內定使用MS950，但核心底層資料處理為Unicode (可支援Unicode3.0以上之規格)
Winsows 7	Unicode(UCS4)	中文版內定使用MS950，但核心底層資料處理為Unicode (可支援Unicode3.0以上之規格)
UNIX like	Extended Unix	AIX 繁體中文為 EUC-
zOS	EBCDIC	CP937(EBCDIC 繁體中文)

圖表 2.4.3 常見作業系統與編碼表

(二) 儲存

資料儲存除單純檔案外，最常見即為資料庫，各廠商實作資料當然支援之編碼方式各不相同，以 IBM 的 DB2 及 Microsoft SQL Server 為例：如果兩個資料庫皆設定為 Big5 編碼，那所代表的意義是 DB2 所使用的是 Big5-IBM 而 Microsoft SQL Server 則是使用 Microsoft-MS950，此兩種版本之 Big5 之差異我們在上一章節已介紹過，當資料在此兩種版本差異範圍內時，橫跨此兩種資料庫之資料就會發生錯誤。

(三) 開發工具與程式

開發工具及程式對各種編碼不同，例如 Java 或 .Net 開發環境，雖然兩種開發環境皆號稱支援 Unicode，但如要完整支援 UCS4 則，Java 2 SDK 需採用 1.6 Update18 以上版本，JRE 需採用 1.6 Update18 以上版本，而 .NET Framework 需採用 3.5SP1 以上版本。

(四) 輸入

輸入介面所提供及支援之編碼能力各有所不同，同時所採用或實作之輸入法也有所不同，可能發生所用之輸入法無法檢索出使用者所要之字型。例如 Windows 內建提供之輸入法並無法提供 CNS11643 所規範超過 10 萬字之輸入。

(五) 輸出

輸出是指在螢幕呈現，其中涉及應用程式對資料之解讀及解讀後資料之呈現。也因此如果解讀能力不

足或是呈現能力不足則輸出將無法正確呈現。例如：資料 0x0002F8E8 以 Unicode 編碼可正確解讀為「**植**」字，但如果顯示程式無法支援 UCS4 規範之能力，則縱使知道資料編碼格式仍無法解讀，若能正確解讀，但顯示使用之字形檔指定錯誤也無法顯示正確。

(六) 列印：

列印必須依賴正確程式對資料編碼之解讀，同時找出正確字型以驅動印表機做列印動作。而解讀錯編碼或字型無法使用正確將導致列印錯誤。

(七) 交換

在中文編碼中資料交換中為最嚴重之問題，如果資料解譯錯誤則原始資料將有可能永遠喪失。例如：傳送給 Java 所開發系統 0x0002F8E8 資料，Java 將其用 Big5 解讀，其結果可能變成「？」而非「**植**」字其原始資料將變成 0x3F，由 0x0002F8E8 轉變成 0x3F 原始資料之資訊可以說已完全喪失。

以上七點分析中可以得知，當我們將中文編碼落實在資訊實作面時，其中複雜及困難之程度並不亞於標準之統一與研訂，其中要考量之系統實作面議題非常廣泛，在目前許多中文編碼議題研究上我們並未看到對此方面依有較詳細且廣泛之研究，在本研究中我們將會對此議題作較為具體可行之規範及作法。

參、未來發展策略之探討

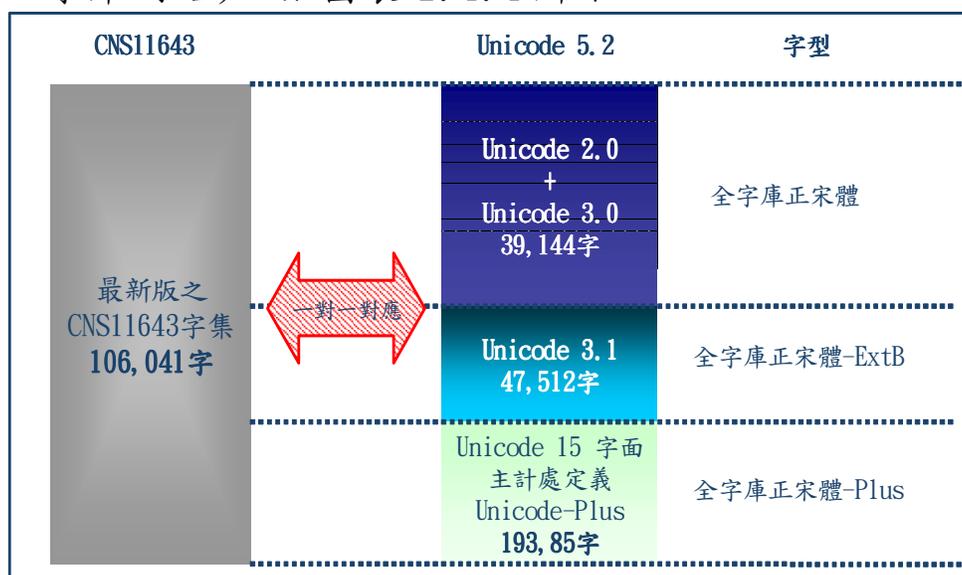
在本章節我們將針對未來中文碼發展策略原則及如何於資訊系統中實現解決方案作一說明。

一、建議之中文碼原則：

由於本公司在中文處理之需求較為固定，其需求包含中文名字、地址(戶籍與通訊)、公司名稱及基金名稱等。也因此我們在中文碼處理只要能達成與國內戶役政機關所用之中文相同之涵蓋範圍即可達成我們中文系統之需求，亦即是我們的中文系統設計必須以能涵蓋「全字庫」^[14]為範圍。我們分為編碼原則、字型原則及交換原則，詳述如下：

(一) 編碼原則：

採全字內碼法^[17]，亦即採用一足夠容納所需字型的編碼方式，又因目前唯一與「全字庫」有一對一對應，且可作為編碼之內碼系統之編碼為 Unicode (可參考全字庫網站)，如圖表 2.4.4 所示：



圖表 2.4.4 字型及字碼關係圖

因此在編碼原則我們建議以以 4-byte Unicode (UCS4)為基礎以作為中文編碼之內碼。我們採用 4-byte Unicode (UCS4) 理由如下：

- 1、可相容於 Unicode 規範並遵循 CNS11643 國家標準：
目前國際趨勢發展皆是以 Unicode 為主流，不論是作業系統、程式開發語言或是網際網路之傳輸等，相繼以 Unicode 為核心或是於相關規格中明定需支援 Unicode。
- 2、達到與 CNS11643 全字庫中文標準交換碼一對一對應：在「全字庫」網站所公佈資料中唯一與 CNS11643 交換碼有一對一對應關係即為 Unicode。

(二)字型原則：

字形原則以遵循全字庫標準為原則，以全字庫 CNS11643 網站 (<http://www.cns11643.gov.tw>) 提供之字型為基礎字型。因我們所需處理均為戶役政用字範圍，在全字庫規範之字型中應可處理，同是只要跟隨全字庫之更新，原則上就不會有缺字問題，若真是遇到缺字問題或狀況亦可依循申請程序向全字庫申請造字。

(三)交換原則：

在資料交換部份可以分為內部資料交換與對外資料交換兩部分來說明。

內部系統由於都為系統間之資料交換，故建議仍以 Unicode 為主，其編碼實作方式在通訊時可為 UTF-8，在做檔案交換時可為 UTF-8、UTF-16 或 UTF-32。

對外交換部份，統一採用 ISO2022 編碼格式之 CNS 字碼(簡稱 CNS 國際碼)作為對外交換字碼，而在未來推

廣期間輔以提供新/舊編碼資料：CNS11643(ISO2022 編碼實作)、BIG5，以為過渡期間之順利轉換。

二、未來實作方法之策略探討：

在規範中文編碼整合原則後，接下來必須要將各項原則落實於資訊系統之實作。以下分為作業系統及平台環境、資料庫系統、開發平台工具及相關開發作業規範四大部分來探討如何所擬定之原則落實於資訊系統實作中：

(一) 作業系統及平台環境：

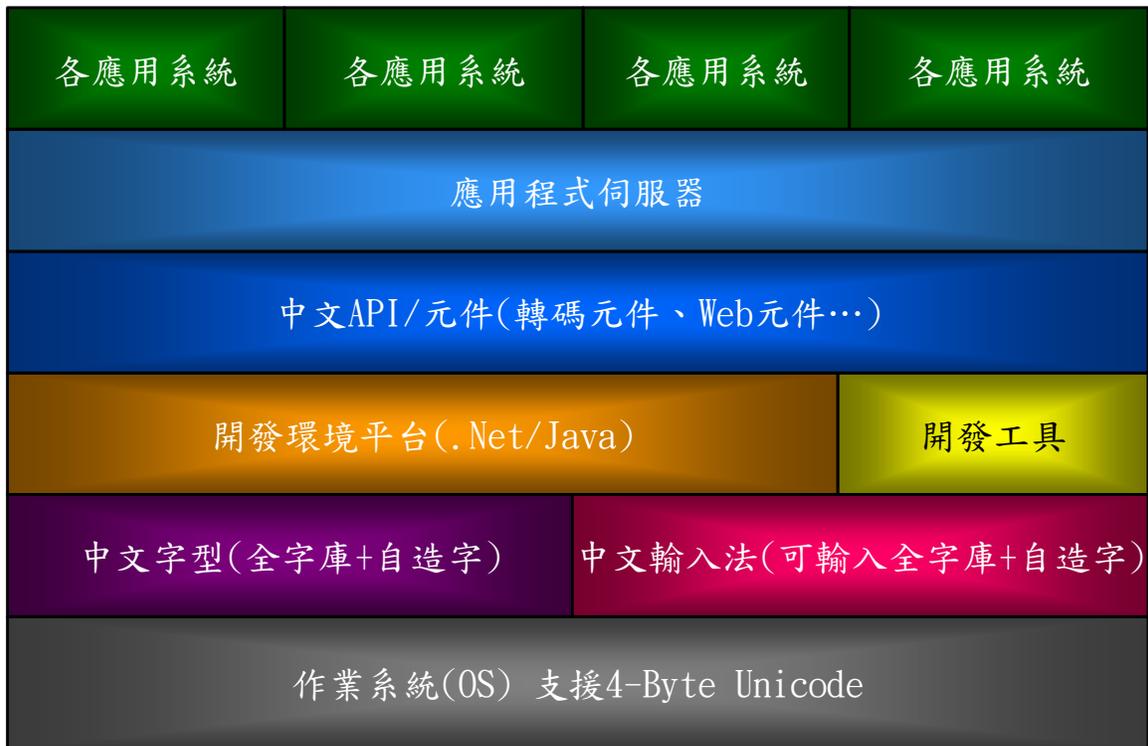
由於我們需要的編碼空間需要 4 byte 才能支援超過 10 萬字以上編碼空間，所以使用之作業系統需可支援 4-byte Unicode 格式(Windows XP、Vista、Windows 7 等皆可)，另 UNIX 或 Manframe 其他作業系統所要求亦同。瀏覽器部分需支援 IE8.x 版本與 Firefox3.x 版本以上。應用系統在此基礎上進行程式開發，才可達成支援 10 萬字以上正確之輸入、顯示及列印。

(二) 資料庫系統：

資料庫系統為應用系統建置中常用架構中的重要成員之一，大部分之應用程式資料儲存皆儲存於資料庫，因此資料庫支援之編碼格式就相當重要。如上面所述的編碼原則所採用之編碼為 4-byte Unicode，故資料儲存需要支援此種 4-byte Unicode 之實作，例如：DB2 需要 Version 7.2 FixPak 4 才完整支援 UCS4。

(三) 開發平台：

在在開發系統時須確認開發工具及其平台要能支援 Unicode 3.1 以上版本，例伽： Java 2 SDK 需採用 1.6 Update18 以上版本，JRE 需採用 1.6 Update18 以上版本。 .NET Framework 需採用 3.5SP1 以上版本。另外開發過程中有參予開發之第三方元件均需確保可支援 Unicode 3.1 以上版本，才可順利用來開發適用於此中文編碼方式之應用程式。



圖表 2.4.5 開發平台架構圖

(四) 相關開發作業規範：

由於內部各系統間傳遞資訊採用 UTF-8/UTF-16 編碼，故各系統開發系統時內部可自由選擇實作之編碼，但必須確保中文字碼進出各系統時可維持字碼與資料完整。

以上為我們對各種可能之中文碼解決方案作詳細分析，

並歸納出未來最適之發展策略及解決方法，同時對如何實現之策略亦有詳細說明，期以此策略分析可作為未來逐步解決中文碼問題之方向指引。

中文字由於天性使然，在資訊系統處理中相對困難，不論在輸入、顯示、列印或資料交換上，在資訊系統皆是一大挑戰。也由於發展的歷史原因也衍生出許多資訊系統不得不面對之問題，最常出現的例如：造字空間不足問題、同字不同碼、同碼不同字、找不到要輸入的字(缺字)、無法顯示特定的字、出現亂碼及資料交換時資料錯誤等問題。

因此未來中文字碼整合工作勢在必行，因為今日不作就將面對隨之而來之問題。利用全字庫之標準及 Unicode 編碼作為內碼將有機會解決目前編碼亂象問題。使中文在資訊處理上不論字型、編碼及交換上都能標準化，亦能解決長久以來存在中文資訊處理上之問題。

第五節 資訊系統訊息交換方式之研究

壹、研究目的與範圍

本公司自民國 79 年 1 月正式營運至今已發展出將近七十多個大小不同的相關系統，包括證券、票券、期貨、庫存及各種業務系統等。各系統開發初期可能只為了某項服務或業務而各自獨立發展，接著可能由於某些特殊因素進而與其他資訊系統做了接觸。但是隨著時間的發展及業務的推廣，各資訊系統不再只是「點對點式」的做資訊溝通，而是「點對面式」的做資訊交換；即一個系統可能面對 2 個以上其他的系統，不論是即時、非即時、單向或雙向的做資訊交換。對資訊系統而言，這裡的環境已由單純轉變成複雜，而且系統工作日趨繁重，因此為避免產生不必要的問題、提昇公司整體資訊交換的品質與系統開發的效率，是本案研究的重點。

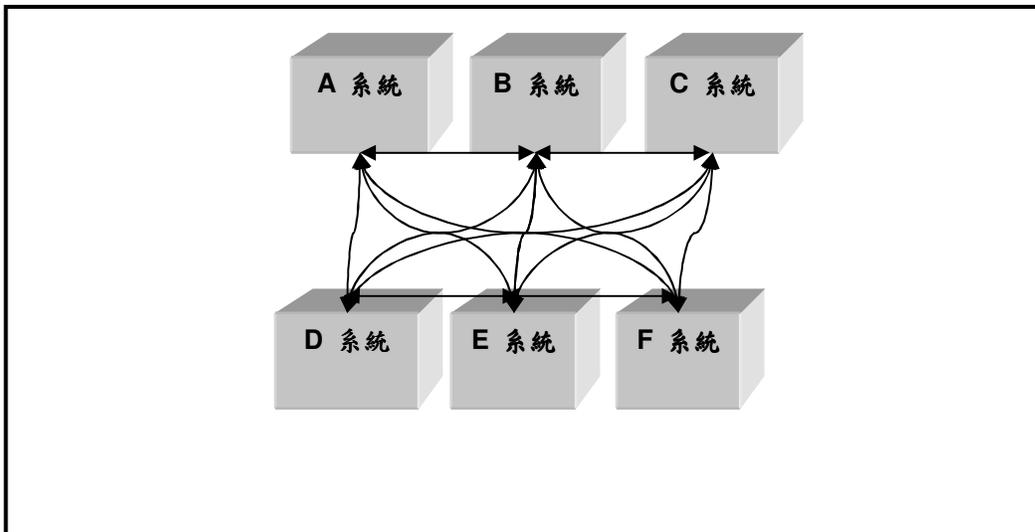
貳、系統現況

本公司內的系統相當多，本案挑選具重要性、指標性的系統納入調查。經洽詢各系統負責人取得相關資料後彙總分析現況如後，相關蒐集資訊包括：

- (1)系統名稱：說明各系統中文名稱。
- (2)傳遞方向(單向或雙向)：說明該系統與傳遞的對象兩者互動關係，資料是雙向互傳或者是單向傳送情形。
- (3)傳遞的對象：說明對象系統的名稱。
- (4)傳遞內容：簡述資料傳遞內容。
- (5)傳遞時間：說明傳遞時間為何，(譬如：每日 18:30；每月 1 日 06:00；每日 09:00~19:00 即時等..)。
- (6)傳遞方式：簡述資料傳遞方式，(譬如：每日由 OP

- 人員啟動傳遞；每日由某某系統自動傳遞等..)。
- (7)傳遞時是否加密：說明資料是否有進行加密。
 - (8)傳遞格式：說明資料格式，(譬如：PDF、TXT(文字檔)、HTML、CSV(利用特殊字區格欄位，譬如：逗號)、DOC、HttpRequest/HttpResponse、test/html 等..)。
 - (9)使用何種服務進行傳遞：簡述傳遞雙方所使用的協定服務，(譬如：FTP、TELNET、Java Socket、rsh、rcp、SMTP、MQ、Http、SOAP 等..)。
 - (10)中文內碼：對於資料內容，傳遞雙方所使用的中文內碼方式，(譬如：Big5、CNS11643、主機碼等..)。

依照現況調查的結果，公司各系統採用的是傳統訊息交換的做法－「點對點式」的方法進行訊息交換如圖表 2.5.1，也就是當 A 系統需要與 B 系統做訊息交換，其兩組或一組系統開發人員必須針對此一需求各自依 A、B 系統的特性，完成開發設計及整合與測試；但當 A 系統又需要與 C 系統做訊息交換時，一樣的情景又再次重演，但是 A 系統必須要重新整合與測試 B 系統，看看是否可以正常運作。由此類推，這種做法，由於各系統間資料不一、系統特性不一、物件標準不一、整合測試難度高、介面紊亂、尤其是各系統都有一些歷史及資料包袱等問題，造成系統間整合成本過高，整合成功機率過低，而且通常是修改系統基礎工程的成本大於處理訊息交換的成本(含時間與人力)。無法有效提昇系統整體品質與效率，對系統開發人員造成不少困擾與問題。圖表 2.5.6 說明目前點對點式的優缺點。



圖表 2.5.1 「點對點式」的訊息交換

項目	說明
優點	具自由、方便、成本低廉，各系統依不同需求目的自行設計連接達成資訊交換。
缺點	<ol style="list-style-type: none"> 1. 公司內部資訊交換無統一標準，包括系統開發方式、訊息格式、中文內碼等。 2. 針對同一事情系統可能被重覆開發或資料重覆，浪費人力及時間，資源無法有效運用。 3. 資訊系統互相連接，形成雜亂無序的網路架構，浪費網路成本，且維護成本較高。 4. 沒有統一管理監控的程序或作法，較易產生資訊安全上的缺口，若發生異常將不易查覺與防堵。 5. 資訊系統開發各自為政，系統開發人員無法深入了解訊息交換內容及任務交接時也會困難許多。 6. 單一系統若做重大系統變更，相關資訊系統必須同時做變更。 7. 需要花許多時間處理傳檔的失敗(重傳、找問題)。 8. 許多資料交換倚賴人力檢查或啟動。 9. 缺少完整的資料交換記錄。

圖表 2.5.2 「點對點式」的優缺點

參、未來發展策略之探討

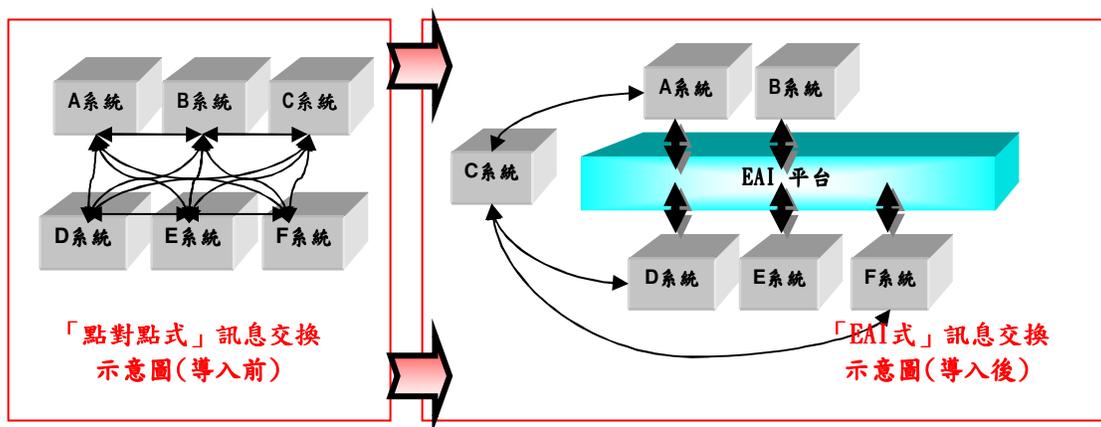
為取代目前「點對點式」訊息交換。通常可用下列兩種方案解決，即「Make them one system」和「Make them work together」，說明如下：

「Make them one system」：就是將各個系統變成一個系統，但這類方式的各系統間同質性要很高。在規劃上，通常會選擇一個功能較完整的做為存續系統，然後再加入其他系統不可或缺的部份。處理過程中，資料的轉移、差異性的調整是不可避免的，系統架構和程式修改部份，會依實際業務需求而有不同幅度的調整。另一種方法是，重新建置一套新的系統，再將原有資料重新導入。但是，對同質性不高的資訊系統而言，這種方式並不適宜。尤其是業務整合及系統規劃設計就是非常吃力的整合工作。

「Make them work together」：不同資訊系統有不同的 Know-How，在進行不同業務性質的資訊系統訊息整合時，首先要考量目的是什麼？加速新產品開發？業務流程的整合？顧客資訊的充份掌握？或是成本的降低？這個方案是保留各個資訊系統的自主性，思考彼此要如何協同運作。主要的目標是當執行一個跨系統資訊交換時，需先設計定義各系統執行先後的順序和例外狀況的處理，並回覆處理的結果，同時訂定訊息規範、建立訊息交換機制，再配合流程的設計和交易安全的控管等。

通常若選擇 Make them one system，則對公司現存系統的變更及軟硬體系統工程過於艱難，費用高昂，非常不智。故建議採用 Make them work together，建設一個中介系統

平台處理來自各系統的訊息交換工作及作業流程，同時導入較為成熟的企業級應用資訊技術-「EAI」(Enterprise Application Integration)，中文稱為「企業應用系統整合」。即引用單一的軟體作業平台的多元應用系統整合，期望能將不同應用系統、不同作業平台的資訊加以集合，相互溝通，對各項相關資訊能流暢的進行擷取、彙整、傳遞，達到提昇資訊系統投資的效益目標。將公司內各資訊系統統一向 EAI 平台連結，不論是 R6 AIX、IBM 主機、PC 等等，連結後訊息交換工作透過 EAI 平台的流程機制進行處理。圖表 2.5.7~2.5.9 分別說明「EAI 式」訊息交換方式導入、優缺點及技術特性。



圖表 2.5.3 「EAI 式」訊息交換導入示意圖

項目	說明
優點	<ol style="list-style-type: none"> 1. 降低 try and error 成本。 2. 降低各系統整合成本(包括人力、物力、財力及軟硬體資源)。 3. 有效監控及管理各系統聯結狀況。 4. 系統人員可專注在業務需求的開發工作。

缺點	<ol style="list-style-type: none"> 1. EAI 並不是萬靈丹，任何程式或流程的整合都可能需要工程師做適度的程式碼修正。 2. 需要改變網路架構與原先設定。 3. 以後需有專人維護此技術。 4. 初期建置成本高。 5. EAI 並不能將所有聯結全部納入。因為若干系統的特殊規格或先天限制等原因，而無法導入 EAI。
----	---

圖表 2.5.4 「EAI 式」的優缺點

1. EAI 技術有助於組織內的「業務流程」及「資料」的整合。
2. EAI 技術可以重覆使用。
3. EAI 技術通常不會大幅要求改變現有的硬體架構。
4. EAI 技術不需要深入瞭解各系統功能面。
5. EAI 技術不會對各系統要求原始程式碼管理權。

圖表 2.5.5 「EAI 式」的技術特性

現有的 EAI 技術(如 Tibco, webMethods 等軟體工具)，以各種 Adaptor 解讀並轉換來自異質系統間不同應用程式或資料庫的資料。譬如 Tibco, 以一個訊息集結點(Message Hub)的架構，各系統皆單獨與之連接。在此架構下的訊息交換模式稱為事件驅動(event-driven)，即預先設計好一個事件，當有被需要的時候，就會在適當的時機被觸發，觸發時會將訊息發佈(Publish)給有訂閱(subscribe)此事件的各系統。因此這種驅動模式會更即時、更具流程自動化(process automation)。

同時每個 EAI 的軟體工具都有一特殊的訊息骨幹架構，上有商業流程邏輯引擎、商業安全匣道、連向各種應用及系

統的 API，可完成整合過程中的文件取得、交易作業 (transaction)、資料映射 (data mapping)、工作流程 (workflow)、安全加密、運作監控等。採用 Message Hub 的好處是 EAI 平台內具有工作流程 (workflow) 引擎及規則 (rule)，可使訊息傳遞或交換更為流暢。以往「點對點式」的連接模式，每次新連接，系統人員都得重新再設計及測試，而 Message Hub，可以先設定好，然後依據規則再執行，系統人員不需重新設計。圖表 2.5.10 說明「EAI 式」和「點對點式」兩者訊息交換之間的差異。

差異點	EAI 式	點對點式
資訊架構	中介系統平台、HUB 架構	點對點架構
整合性	業務流程及資料導向	資料導向
重覆使用性	業務流程及資料均可重覆執行或運用	單一運用
IT 人員	對整合應用程式細節可以不需瞭解	自行撰寫應用程式，同時需瞭解開發細節
效益性	整合彈性高、成本較低、效率高	整合僵化、成本較高、效率低

圖表 2.5.6 「EAI 式」和「點對點式」訊息交換之差異

倘若公司對系統間訊息資料的同步性、一致性、即時性非常需要的話，那麼可以考慮導入 EAI，以下說明：

本公司的跨系統作業可以被真正實踐，同時可提昇服務品質及作業效率。導入 EAI 後，不論是銀行、證券商、票券商及各類金融同業的作業可在同一個 EAI 資訊窗口辦理，再由數個交易流程跨系統的完成，讓整體訊息充分發揮。系統間的資料即時同步更新，公司內的各種不同的流程都能快速整合。

藉由 EAI 管理作業流程，降低作業疏失，增強稽核控管的能力。有些業務流程繁雜，譬如跨系統、跨部門或跨日期等，容易造成人為的缺失，事後需投入大量人力或財力進行補救。若透過 EAI 導入相關交易流程或機制，整個繁雜的作業可以被縮短，時間更可以被掌握，錯誤機率更能夠降低。

新的系統能快速的整合，不論是新種業務平台或新採購的系統，透過 EAI 的設定將可快速的融入公司的 EAI 架構。介面開發與維護更省經費，統一的 EAI 介面管理，在未來的系統開發與維護都較以往更容易。

第六節 資訊系統架構之發展策略

壹、研究目的及範圍

本研究案藉由分析開放式主機平台及傳統大型主機平台之特性、金融業選擇新核心系統平台趨勢、銀行新核心系統移轉成功因素探討、存託業務需求發展現況，進行資訊系統未來架構之研議及擬定發展策略。

貳、系統現況

一、IBM大型專屬主機平台及開放式主機平台特性說明

(一) IBM 大型專屬主機平台特性

1. 大型主機的歷史：

大型主機(Mainframe)是在 1970 年代迷你電腦(Mini Computer)誕生之後，才出現的相對名詞，意指集中式控管、大型、昂貴又很可靠的大型電腦。

1964 年 IBM 推出世界上第一臺普及化的商用大型主機 System 360，在市場上獲得極大的成功，奠定藍色巨人在計算機工業的霸權。數十年來，大型主機一直都是 IBM 在金融市場的主力，也是藍色巨人的金雞母。

從 1950 至 1970 年代，大型主機市場「由一個藍色巨人搭配七個小矮人所組成」的熱鬧局面，歷經數十年，今日大型主機市場被市佔率超過九成的 IBM 所統治，由 Sperry 和 Burroughs 合併而來的 Unisys 是唯一碩果僅存者。IBM 大型主機四十多年來輝煌的發展史，可說是近代電腦技術發展的縮影。

在 1960 年代高階語言編譯器技術剛處於起步階段，為了縮短高階語言與處理器指令集之間的語意隔閡(Semantic Gap)，讓指令集本身更接近高階語言，使得指令集架構變得非常的複雜。對普遍使用 COBOL (Common business Oriented Language)語言的商用大型電腦來說，提供豐富的字串與十進位數字處理指令，已成為一種常態。IBM 大型主機嚴謹定義的必備條件為需包含專屬 CISC 指令集，與大量執行 COBOL 或其他第四代程式語

言(大型主機的程式約有 85%是 COBOL),因此 IBM 定義的大型主機係指 S/360 家族體系,不包括 AS/400、RS/6000 等系統。

1964 年	IBM 開發出新的商業電腦系統 System/360
1971 年	IBM System/370 問世
1972 年	SAP 公司為 System/360 開發了革命性的「企業資源計劃」(ERP)系統
1980 年	首創 S/370 第一個美國核心銀行系統
1990 年	IBM S/390 問市
2005 年	IBM 推出第九代大型主機 z9
2010 年	IBM 宣布推出 zEnterprise

圖表 2.6.1 IBM 大型主機發展大事紀

2. 大型主機的特性：

(1) 可靠性 (Reliability)

大型主機的最大特性為極高之可靠度，大型主機擁有強大的容錯能力，故能廣泛在公眾事務、金融、商業、醫療、國防、學術、航太等領域獲各企業採用，尤其是金融產業。財星雜誌全球 500 大中，有 7 成的公司，以及全球 25 大銀行的核心運算平台即是採用 IBM 大型主機。

(2) 可使用性 (Availability)

根基於大型主機優越的系統設計，包含記憶體 (Memory chips)、匯流排 (memory busses)、輸出／輸入通道 (I/O channels)、及電源供應 (power supplies) 等元件皆設計為成對 (或更多) 以互相備援，從而確保了大型主機系統高達 99.99% 的可使用性。

(3) 可維護度 (Serviceability)

大型主機允許在替換大多數元件的同時，仍能維持系統的正常運作。

(4) 高安全性

因大型主機的平台與作業系統並不開放，封閉式特性很難被惡意入侵，系統的安全性極強。大型主機內含密碼加速器(cryptography accelerator)，可提供系統每秒鐘完成 6,000 次安全線上交易。

(5) 高效能的輸出／輸入(Input/Output, I/O)性能

大型電腦並不單以 MIPS (millions of instructions per second)來衡量性能，I/O 系統的設計才是大型主機的技術重心。大型主機具備強大的 I/O 效能，可進行大規模的數據輸入輸出處理，在支援大量使用者與交易量時，依然保持穩定輸出的表現，及高度的可靠性。

(6) 向後兼容性

因客戶核心系統的業務程式碼不易更動，大型主機具備完整的指令集回溯相容能力，可確保現有的程式可穩定的在新版本系統上執行。此外，大型主機也是最早實作虛擬化技術(1972)，並提供邏輯分割(Logical Partition)功能和工作流量管理、提供服務隨需應變(Capacity on Demand)技術等先進科技的電腦。

3. 大型主機的缺點

(1) 硬體費用及軟體使用費昂貴

因其特殊的市場特性與歷史背景，大型主機市場有著非常強烈的封閉特性，作業系統無法買斷，必須按期

繳交「軟體授權月租費」，無論作業系統、應用程式、處理器、指令集、系統架構與週邊設備都是專屬規格，幾無替代產品選擇，造成系統建置的硬體費用及軟體使用費十分昂貴。

(2) 系統維護人才斷層

大型主機的應用系統絕大部分仍為 COBOL 程式，COBOL 的設計理念就是要讓「不懂電腦的商務人士也會寫」，缺乏結構化的規畫，使得程式碼疊床架屋，且舊時欠缺整理系統設計文件、說明文件的觀念，程式設計師普遍忽略於程式碼加以註解，導致這些核心系統程式難以理解，更難以改寫。目前學校教育皆為教授開放式系統及程式語言，懂 COBOL 程式、會操作大型主機的人才逐漸凋零，將造成系統維護人力的斷層，亦是企業管理的一大難題。

(3) 無法即時滿足業務需求

大型主機提供之程式開發環境不佳、測試工具少，且操作介面缺乏親和力(User friendly)，導致應用系統開發時間長，無法配合業務發展以達到 Time To Market 的需求，限制了企業新業務推展的速度。

(4) 與開放系統連結之整合能力較差

封閉式系統固然能提升安全性，但也提高與其他開放系統整合的難度。大型主機需與其他系統功能連結時，可供選擇的解決方案少且價格高昂。

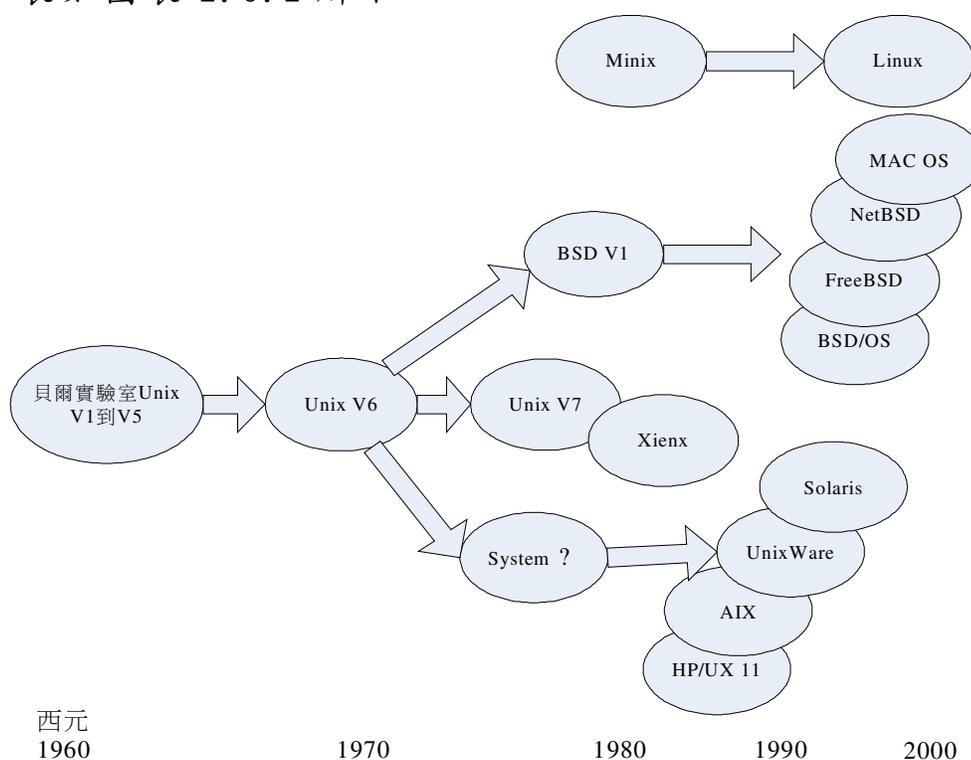
(二) 開放式主機平台特性

1. 開放式主機平台簡史：

1963 年，奇異公司與貝爾實驗室合作以 PL/I 語言建立的 Multics，是激發 1970 年代眾多作業系統建立的靈感來源，尤其是由 AT&T 貝爾實驗室的丹尼斯·里奇與肯·湯普遜所建立的 Unix 系統。

當使用 Unix 需要收費時，荷蘭 Andrew S. Tanenbaum 教授（即是 Computer Network 的作者，Prentice Hall）便利用 Unix 的相關技術，發展一個稱之為 Minix 的作業系統，它的雛型是 Unix-like 作業系統。

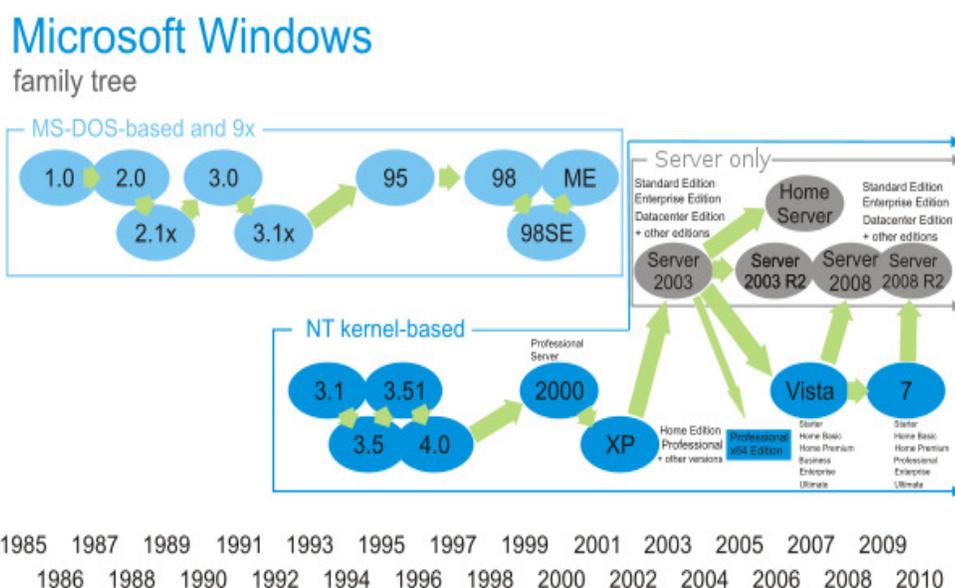
直到 1990 年，在芬蘭的 Helsinki 大學裡，有一位叫 Linus Torvalds 的大學生發展出新的作業系統稱之為『Linux 作業系統』，Unix/Linux 家族的發展年代表如圖表 2.6.2 所示：



圖表 2.6.2 Unix/Linux 家族的發展

1980 年，西雅圖電腦產品公司（Seattle Computer Products）的一名 24 歲的程式師蒂姆·派特森（Tim Paterson）編寫出了 86-DOS 作業系統。1981 年 7 月，微軟以五萬美元的代價向西雅圖公司購得本產品的全部版權，並將它更名為 MS-DOS。隨後，IBM 發佈了第一台個人電腦，當時採用的作業系統是西雅圖公司的 86-DOS 1.14，但微軟很快改進了 MS-DOS，並使它成功地成為 IBM PC 採用的作業系統。並於 1981 年 8 月 12 日，正式發佈 MS-DOS 1.0 和 PC-DOS 1.0。

1990 年代初，微軟與 IBM 的合作破裂，微軟從 OS/2 專案中抽身，並且在 1993 年 7 月 27 日推出 Windows 3.1，一個以 OS/2 為基礎的圖形化作業系統。並在 1995 年 8 月 15 日推出 Windows 95，最新的 Windows 7 則是於 2009 年 10 月 22 日發售，Windows 家族的發展年代表如圖表 2.6.3 所示：



圖表 2.6.3 Windows 家族的發展年代圖

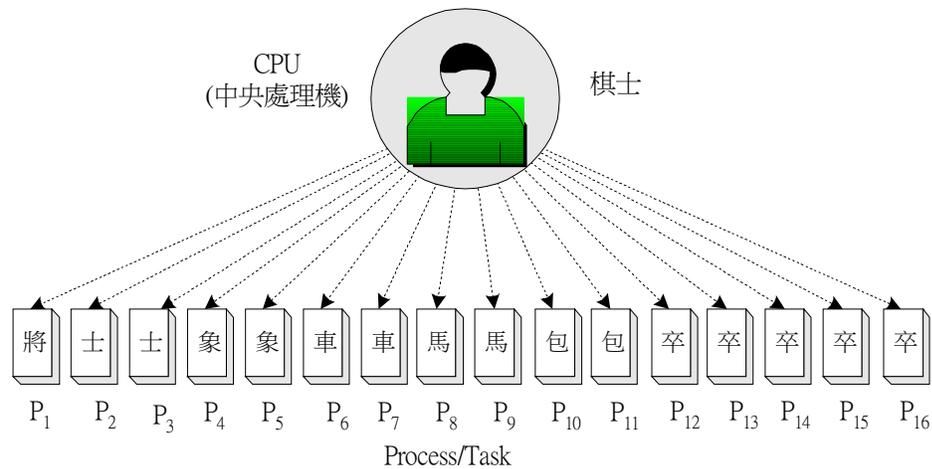
2. 開放式主機平台特性

為何二十幾年來，Unix/Linux/Windows 系統一直保持著重要的地位，許多地方都可以看到他的蹤影；尤其近年來網際網路的盛行，更少不了 Unix/Linux/Windows 系統，他到底有何特性，我們以下分幾個重點來探討：

(1) 多工處理能力

『多工處理』(Multi-task) 是 開放式主機平台最基本的功能。在 開放式主機平台上同時可以產生多個『行程』(Process)，每一個行程都有其獨立的執行環境（或稱獨立的記憶體空間），並處理其專屬的任務。

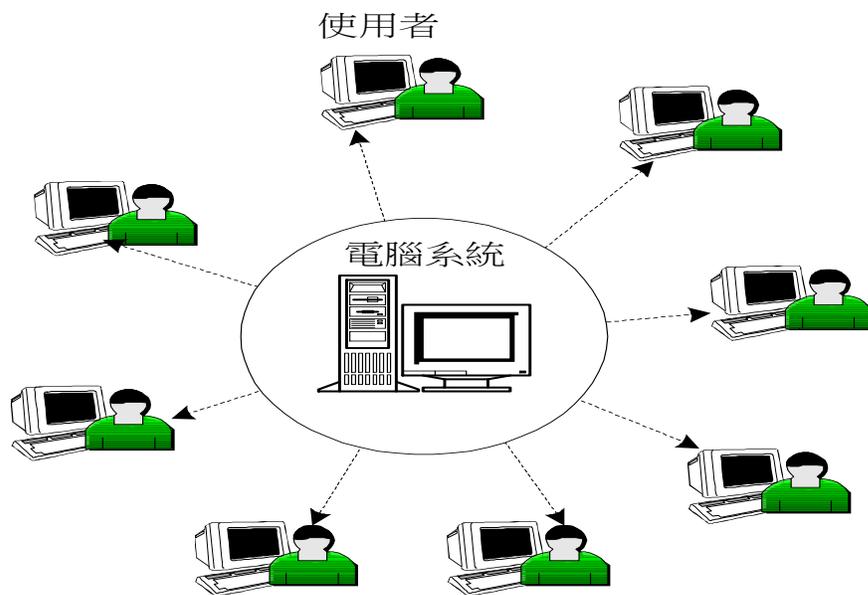
我們以圖表 2.6.4 來說明作業系統的多工處理能力。作業系統的運作就好像下（玩）象棋一般，象棋中有許多棋子（Process），每一棋子都有其特殊功能（Task）；棋盤中雖然有許多棋子，但只有一個人（CPU）可以下棋，每次也僅可以移動一顆棋子。如果雙方棋士都下得很快的話，整個棋盤的棋子就好像同時在移動，猶如千軍萬馬作戰一般。同樣的，CPU 執行速度很快的話，所有行程就好像同時在運作，正如同許多工作人員共同完成任務一般。



圖表 2.6.4 多工處理能力

(2) 多人使用環境

『多人環境』(Multi-user Environment) 是開放式主機平台另一個重要的特性(如圖表 2.6.5 所示)。系統上每一個行程都可以將其當作一個使用者，當系統輪流到某一個行程執行時，該行程便可掌控所有資源；也就是說，該行程可以使用系統上所有資源(依權限範圍而定)。

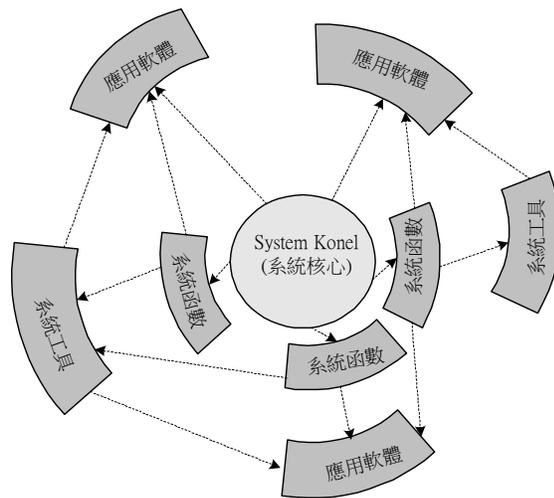


圖表 2.6.5 多人使用環境

(3) 開放性系統

在 Unix/Linux 系統上不但可以任意下載系統執行檔，連原始程式也可以下載使用，並提供有系統編譯及修改工具，讓其他使用者重新修訂系統程式。簡單的說，Unix/Linux 系統上沒有任何秘密可言，所有技術資料都是公開的；尤其近年來網際網路的盛行，再加上自由軟體基金會的鼓吹，許多人都願意將它所研究的成果在網路上發表，造成短時間內開放式主機平台成長非常快速，許多免費軟體也都非常容易取得。早期免費軟體大多被開發在 Linux 系統上（因為 Unix 系統必須收費），但隨著系統開發工具的發展，這些免費軟體大多可以容易地被移植到 Unix 或 Windows 系統上，尤其移植到 Unix 系統更是容易。

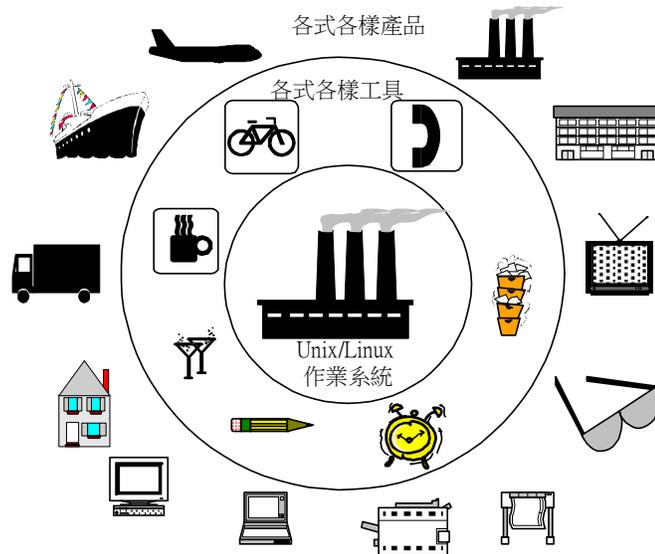
既然是開放性的系統，許多有心人士除了可以在開放式主機平台上開發各式各樣的工具，之間的工具其共通性也很高，極容易由現有工具整合或開發出另一新工具，如圖表 2.6.6 所示。



圖表 2.6.6 系統開放性

(4) 豐富工具與公用程式

一部作業系統擁有各式各樣的工具，就好像一座工廠擁有多種生產工具。具備了各式各樣工具之後，再給予不同生產程序，便可以製造出不同的產品。如圖表 2.6.7 所示，一座擁有完善設備的工廠，依照多樣性的生產程序，便可以製造出多樣性的飛機、汽車、機車或腳踏車等等產品。



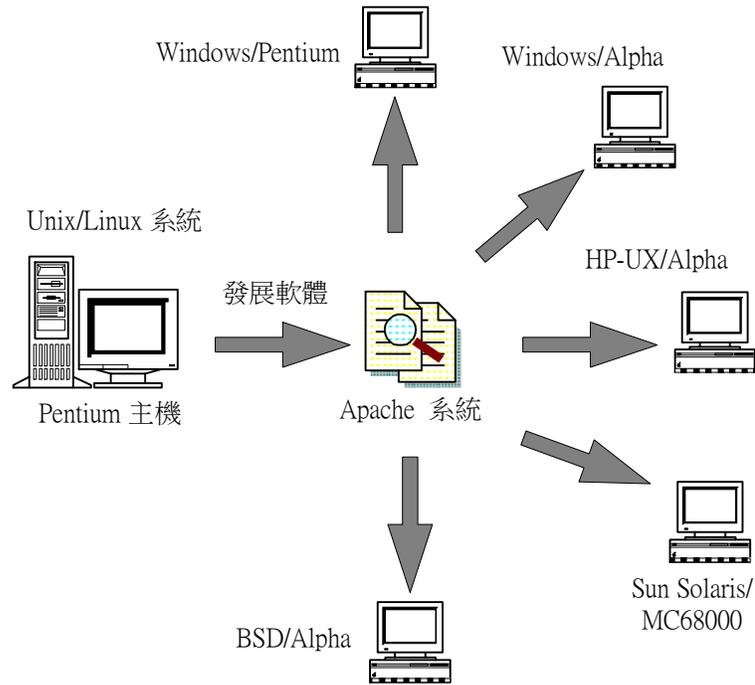
圖表 2.6.7 豐富的系統工具

(5) 程式的高可攜性

所謂『可攜性』(Portability)，即是某一系統（或主機）上的程式是否可以輕易的被移植到其他系統上。首先我們來看看作業系統本身，開放性主機平台的系統程式絕大部分都是利用 C 語言所編寫而成，只有極少部分與硬體較有關係的程式利用『組合語言』編寫。希望移植到其他電腦上時，只要重新編寫極少數的組合語言程式，再重新編譯 C 語言所寫的程式即可。

目前應用軟體（如圖表 2.6.8，Apache 系統）大多是利用高階語言所發展出來（C 或 Java 語言），一般系

統大多有類似的編譯器，只要將軟體重新編譯即可。但發展軟體時大多會呼叫系統函數，問題就發生在這些系統函數是否有一致性。目前開放式作業平台的系統函數也漸漸標準化。

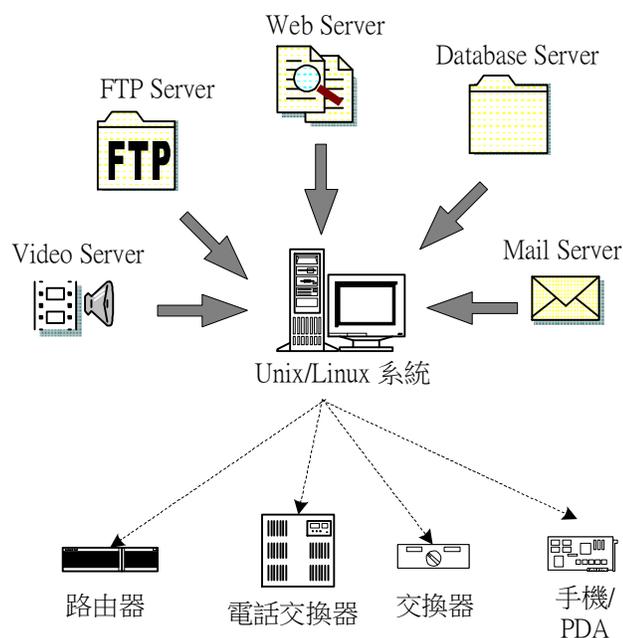


圖表 2.6.8 程式可攜性高

(6) 優良的網路環境

除了開放性條件之外，優良網路環境可說是開放式主機平台廣泛風行的因素之一。早期 Ethernet 與 TCP/IP 網路的萌芽裝置就是 Unix 作業系統；經過幾十年的演進，不論由軟體（應用系統）或硬體（網路設備）來看，Unix 系統上也擁有豐富的網路套件，『網路』這個名詞幾乎與 Unix 名稱離不開。以目前使用開放式主機平台大多離不網路應用，因此許多情況都將網路系統模組植入核心之內，不但可嵌入更多的應用程式，又可以增加網路處理的速度。

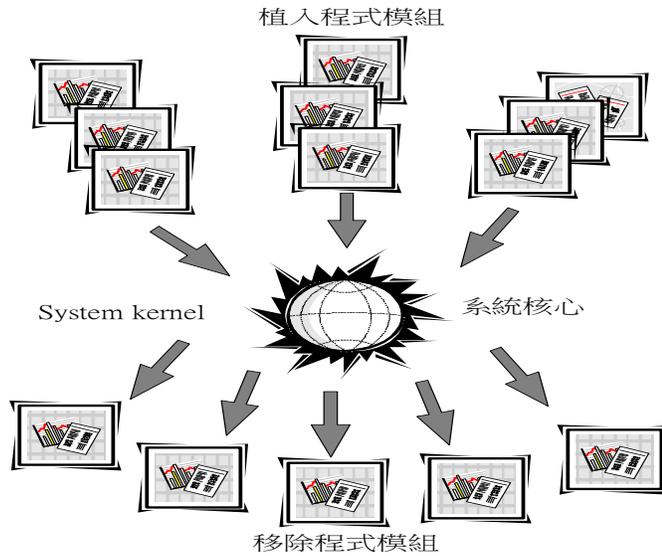
簡單的說，優良網路環境不但可以植入多種伺服器軟體，也可利用它來開發各種的網路設備，譬如電話交換機、路由器、交換器或行動手機等等，如圖表 2.6.9 所示。



圖表 2.6.9 網路環境

(7) 系統核心的可變性

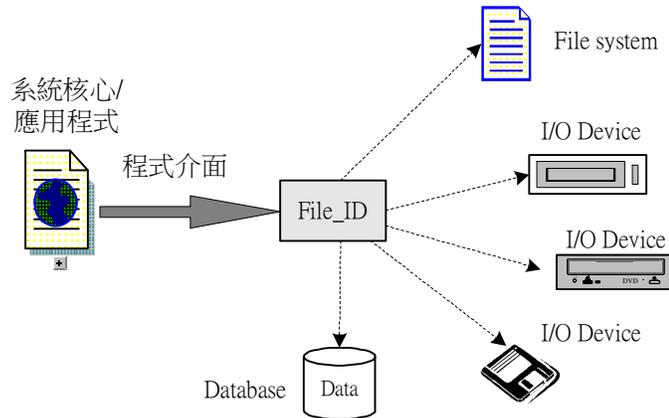
為了達到『小而美』的『Unix 哲學』(Unix Philosophy)，系統核心被設計成可變動性的。系統管理可依照環境需求，重新規劃組態系統核心，一方面移除系統較不常用的系統函數，另一方面可植入較常用的系統函數。如此一來，一部 Unix 系統可擴充成一部非常龐大的應用系統(如網路伺服器)，也可以將其縮成很小的系統(如路由器或橋接器)。通常我們都將這些系統函數模組化，可依照需求植入某些模組或移除，如圖表 2.6.10 所示。



圖表 2.6.10 系統核心可變性

(8) 檔案格式的一致性

在 Unix 系統上，無論是檔案系統或任何週邊裝置都是以一個檔案結構來表示，因此，系統上有一般檔案或裝置檔案 (Device file)。採用同樣的檔案結構表示，目的是為了統一所有存取介面 (或函數呼叫)。對使用者的觀點而言，它存取週邊設備就如同存取檔案一般，不但方便也可以整合所有的存取介面。目前其他作業系統 (如 Windows) 也採用這種模式，如此一來，之間所發展的軟體互通性也提高了許多 (如圖表 2.6.11 所示)。



圖表 2.6.11 檔案格式一致性

二、金融業選擇新核心系統平台趨勢說明

台灣金融機構的核心系統大約從六十年代開始發展，因業務需求變更及業務種類不斷增加，加上銀行核心系統普遍呈現老舊現象，無法即時有效支援業務發展需要，核心資訊系統的更新是件刻不容緩的事情，然而早年銀行核心系統多半採用大型且封閉的主機系統（如：IBM Mainframe），但隨著資訊科技的創新，無人銀行、網路銀行的發展及競爭環境日趨複雜多元，中央銀行總裁彭淮南就曾表示：「觀察歐美國家發展經驗，網際網路除了破除了種族、距離的限制之外，並且加快且加速全球資訊科技的流通，已經徹底顛覆了大家習以為常的交易方式。」，因此許多銀行藉由發展新一代核心系統，負責支援及整合其他銀行資訊系統的運作，而開放式資訊架構較符合現今的競爭環境，下表為銀行核心系統由封閉系統轉為開放系統的銀行金融機構。

銀行名稱	專案時程	採用系統	過程
A 銀行	2001-03 2004-02	FNS_Unix	<ol style="list-style-type: none"> 1. 1999 年開始評估導入新系統，並找 Anderson 顧問公司檢視所有的資訊平台、擘畫資訊藍圖，經過長達二年的準備時間，於 2001 年三月正式推動這項計劃。 2. 從 2004 年 2 月 13 日(星期五)下午 6 點各分行全部關帳那刻開始，將舊系統的資料做當日帳務批次處理、從舊系統轉出資料、轉至新系統上，大約花費 13 個小時，比原先預估的 15 個小時還要順利。 3. 於 2007/11 贏得 Asian Banking & Finance 肯定，榮獲亞洲區「最佳銀行核心系統」大獎。

B 銀行	2006-04 2009-06	1. 核心系統採用 IBM 與 FNS 2. 財會系統採用 Oracle 3. 前端系統(通路整合)為慶燁科技 4. DB 為 Oracle	1. 歷經四、五年以上的評估、開發、測試，B 銀行的核心系統，將於 2009 年第二季結束之前完成轉換。 2. ATM、MyATM、電話銀行、官方網站、網路銀行、MyB2B、FEDI... 其實整個服務全部都會停機一輪。轉換的時間從 5/28 凌晨開始，一直到隔天凌晨 2:00 才恢復。
C 銀行	2001 年底 2004-09	台灣優利(Unisys) CleverPath Windows 系統	1. C 銀行的核心系統轉換，其實是在一個被迫的情況下開始，因為大約在 2000 年左右，彰化銀行知道原本正在使用的核心系統，即將在不久後停止生產，而相關的服務支援最多也只能延續到 2005 年。 2. 終於在 2001 年底正式啟動，將近 3 年的系統建置過程中，C 銀行總共投入了 100 多個人力，2003 年 8 月中旬第一個系統終於上線，然後再慢慢從外匯系統延伸到所有系統，並且在 2004 年 9 月 6 日正式完成銀行核心系統轉換的作業。
D 銀行	2005	i-flex	1. 耗資 1500 萬美元(折合新台幣 5 億元)，導入新核心系統，採用號稱全球最大銀行核心系統廠商 i-flex 合作，預估二年內完成。
E 銀行	2011-08 2012-06	IBM 四方金創	1. 2009-03 曾採用 Temenos .NET 平台進行轉換。
F 銀行	2009-02	主要是以 Unix 搭配 BANCS	

G 金控	2003-02 2005-02	Windows 的作業平台	1.G 金控於 2003 年 2 月，宣佈與 TEMENOS、凌群電腦公司及台灣微軟等廠商合作，進行為期 2 年的核心系統暨週邊設備系統再造工程，該計劃案採用 Windows 的作業平台為最大特色，新的銀行核心系統是將原本銀行、證券及投信各自獨立的金融服務逐步整合，將核心金融業務集中統一調度與管理。
------	-------------------------	------------------	--

圖表 2.6.12 核心系統轉換銀行列表

三、存託業務需求發展現況

(一) 系統架構

1. 電腦主機配置

- (1) 現行本公司證券存託系統正式營運硬體設備，主要在南港主中心之 IBM z114 大型主機 (2818-V01) 上。
- (2) 另於竹北異地備援中心設置一台 IBM z9 主機 (2096-Y01)，此異地備援配備平時作為存託系統異地熱備援使用，如遇正式作業主機 2096-Y01 故障無法使用之緊急狀況，則切換作為正式作業主機。
- (3) 兩地機房透過 DWDM 網路通訊設備，使用光纖通道相互連結營運。並各裝置一套 DS8300 磁碟機 (4.6 TB)，使用 IBM 同步遠程備份功能 (PPRC)，確保達到兩地機房主機系統上的儲存、更正資料之即時同步與保持一致性。

2. 電腦主機配置

- (1) 目前在主機上所使用的作業系統軟體，係 IBM 主機系統軟體 ZOS，版本為 1.8。
- (2) 各參加人與本公司連線作業，使用 SMART 系統工作站透過 CICS 連線控制系統軟體，提供外界各使用單位辦理線上交易執行。
- (3) 主機端儲存參加人與客戶帳務資料之資料庫，則使用階層式架構之 IMS/DB。

(二) 系統功能

以業務面來看，目前證券存託系統之資訊服務功能如下：

1. 集中保管

- (1) 客戶基本資料維護
- (2) 客戶存券帳務異動服務
- (3) 客戶查詢服務
- (4) 證券商存券帳務異動服務
- (5) 無實體證券帳簿劃撥處理
- (6) 股務處理
- (7) 保管機構查詢服務
- (8) 第一手股票委賣申報
- (9) 信用交易帳務處理

2. 帳簿劃撥

- (1) 議價買賣
- (2) 設質交付帳務處理
- (3) 認購／售權證帳簿劃撥
- (4) 私人間讓受／繼承／贈與帳務處理

- (5) 公開收購作業
- (6) 私募有價證券帳簿劃撥服務
- (7) 個股選擇權履約撥轉
- (8) 全權委託
- (9) 開放式受益憑證作業

3. 結算交割

- (1) 證券商當期買賣有價證券之交割結算服務
- (2) 證交所／櫃檯買賣中心交割結算服務
- (3) 部分地區休市交割結算服務
- (4) 錯帳／更正帳號／違約／瑕疵補正帳務處理
- (5) 有價證券借貸帳務處理
- (6) 興櫃股票給付結算
- (7) 鉅額買賣作業

4. 其他

- (1) 證券上市（櫃）、下市（櫃）之建檔作業
- (2) 證券商開業、停業、復業
- (3) 證券商合併、讓與
- (4) 證券合併
- (5) 證券減資
- (6) 證券掛失
- (7) 颱風天自動化作業

（三）連線程式

證券存託系統提供之線上交易，共約 944 個連線交易，交易種類依交易作業功能、條件及資料處理內容，歸類如下：

1. 帳務類交易

(1) 客戶基本資料異動類

客戶開戶基本資料建檔，基本資料變更、解約、保管機構往來登記、款項基本資料建檔等。

(2) 存摺資料異動類

新發存摺、換發存摺、補登存摺、餘額登摺、存摺掛失等。

(3) 送存類

現券送存、補足送存、零股送存、零股補足送存、連號送存、連號補足送存、債券補足送存、未領送存等。

(4) 領回類

存券領回、本日提領、權證屆期轉銷、存券領回代轉、有價證券兌回、收回、買回、贖回等。

(5) 配發類

發行或增資配發、證券合併或轉換、強制轉換、減資、無實體發行登錄或交付設定、承銷中籤配發、公開收購交付撤銷轉發等。

(6) 限制動用類

設質交付申請、留置申請、暫存申請、借出或標借申請、借出或標借撤銷、法院扣押、扣押解除等。

(7) 交割匯撥類

集中市場或 OTC 交割、興櫃交割、借券轉帳、標借轉帳、外資買賣轉帳、補正撥轉等。

(8) 更正撥轉類

更正帳號申請、更正帳號撤銷、錯帳申報或刪除、申報違約處理、存券更正扣帳、存券更正轉帳、債券成交帳號變更等。

(9) 客戶帳撥轉類

存券匯撥、現償轉帳、興櫃違約沖轉、登錄存券撥轉、登錄專戶或管理式保管帳轉入集保劃撥帳、登錄專戶或管理式明細調整等。

(10) 繼承／贈與／私人間讓受類

私人間直接讓受申請或撤銷、繼承及贈與申請或撤銷、讓受繼承贈與之過戶審核及撥轉、非市場交易撥轉等。

(11) 附條件買賣撥轉

櫃檯股票議價或附條件議價、債券買賣或附條件買賣、附條件存券匯撥等。

2. 查詢類交易

(1) 客戶資料查詢作業

客戶資料查詢、存券異動明細查詢、證券所有人名冊資料查詢、控管資料查詢、設質資料查詢等。

(2) 存券異動彙計查詢及日結作業

存券異動彙計查詢、存券交易日結資料查詢、存券交易日結資料總結、匯撥轉入交易明細查詢、送存清冊查詢、零股領回資料查詢、設質異動資料彙計查詢、設質交付轉入明細資料查

詢、私人間讓受轉帳申請資料查詢等。

(3) 一般資料查詢

掛失股票號碼查詢、買賣未開戶資料查詢、領回股票號碼清冊查詢、權證發行基本資料查詢、擔保品撥轉明細查詢、承銷中籤查詢、信用交易過戶查詢、保管機構集保戶結算資料查詢、出借證券申請查詢、單式存摺資料查詢、全權委託現金增資認股資料查詢等。

3. 集中交易對帳類

(1) 委託變更類

委託買進成交明細變更、委託賣出成交明細變更等。

(2) 查詢類

信用交易明細查詢、劃撥買賣明細查詢、交割清單資料查詢、劃撥轉帳存券不足查詢、劃撥戶交割不足查詢等。

4、興櫃市場類

(1) 資料通知類

推薦券商成交資料通知，經紀／自營商成交資料通知、成交資料取消通知等。

(2) 查詢類

興櫃股票資料查詢、成交明細資料查詢、給付結算資料查詢、興櫃股票送存及控管數額查詢等。

5. 錯帳、更正帳號／違約申報處理類

(1) 錯帳申報作業

錯帳申報、處理申報、錯帳彙總查詢、互抵資料查詢、錯帳申報明細資料查詢、錯帳處理明細資料查詢等。

(2) 更正帳號作業

更正帳號申報、更正帳號申報明細查詢等。

(3) 違約申報作業

違約申報、違約處理申報、違約結清申報、違約申報明細查詢等。

(4) 借券作業

借券專戶帳號維護、借券明細資料查詢、還券查詢、新借查詢等。

(四) 批次程式

證券存託系統批次作業主要目標是完成集中市場／櫃檯買賣市場之帳簿劃撥轉帳、買賣交割。就投資人而言，將投資人所買進之股票，依證交所通知，將其買進數額轉進該投資人之集保帳戶，將投資人所賣出之股票，依證交所通知，將其賣出數額自其集保帳戶轉出，辦理賣出股票交割。對證券商而言，將證券商當期之買賣，依證券別、買賣別、委託類別（普通、信用）彙總，計算其各種股票之總買賣股數、應收應付金額。並彙總全體證券商之買賣資料產出交割計算表，以供全體證券商對證交所／櫃檯買賣中心交割之用。此外，在批次作業中尚有交割轉帳以外的業務，以及系統本身系統維護的作業。概述如下：

1、試算作業

每一交易日收盤後，證券存託系統接收證交所及櫃檯買賣中心之成交資料後作試算處理。試算作業分別在每一交易日約下午 13 時 45 分及下午 14 時 48 分執行，其主要功能如下：

- (1) 彙整證券商當期買賣資料，供證券商與證交所對帳。
- (2) 計算證券商當期買賣所有股票之股數、金額。
- (3) 計算證券商每一種股票對交易所為淨收或淨付。
- (4) 計算證券商當期買賣總金額，並計算對交易所為淨收或淨付。
- (5) 計算投資人賣出，存券不足股數，以供證券商通知投資人儘早補足。

2、交割結算作業

每個交易日，當證券商日中完成證交所、櫃檯買賣中心對帳，確認所有買賣之交易股數金額後，系統依據上述資料計算每家證券商對證交所及櫃檯買賣中心之證券總買、總賣、淨收、淨付，並計算每家證券商對證交所及櫃檯買賣中心交割金額之淨收、淨付；產生交割計算表給證交所及櫃檯買賣中心，產生淨收、淨付檔案傳送給證交所。

3、買賣轉帳作業

依據對帳確認後之成交紀錄，計算每一投資人帳號對每一種股票之總買、總賣後進行轉帳。先處理賣出資料，於客戶餘額中扣除當日賣出資料，若不足扣除則紀

錄存券不足資料檔，供證券商次日查詢並通知投資人儘早補足。對投資人買進資料，則加入其餘額。另外，對買進或賣出資料分別記錄於補登檔，供投資人次日補登存摺之用。對證券商另行加總其客戶當日每種股票之買賣股數記錄於日結總帳中，供其核對帳務之用。總結買賣轉帳作業功能如下：

(1) 對投資人

- A. 買進轉帳：買進股數加入其餘額。
- B. 賣出轉帳：由其餘額中扣除賣出數額。
- C. 記錄補登資料。

(2) 對證券商

- A. 記錄存券不足資料，供其次日查詢。
- B. 加總其每種股票之當日買進、賣出股數，並記錄於日結檔中，供證券商次日核對帳務。

4、配發作業

依據發行公司或其股務代理機構所提供之配發名冊，於夜間進行配發轉帳作業。作業內容如下：

- (1) 自配發專戶餘額中扣減本次成功配出之股數。
- (2) 加計配發股數至投資人帳戶。
- (3) 配發失敗者，其配發股數仍留在配發專戶。
- (4) 配股率大於百分之二十者，再由投資人帳戶扣減後轉至融資融券專戶。
- (5) 記錄日結檔、匯入檔，以供證券商次日核對帳務。

5、證券所有人名冊作業

- (1) 遇發行公司除權、除息及開股東大會時，系統依據前置作業所輸入之控制資訊(作業日期、證券代號)自動啟動證券所有人名冊作業。以最後過戶日投資人帳上餘額加計前一營業日賣出之股數為其持有之股數。
- (2) 因同一投資人可於多家證券商開立帳戶，故同一投資人以其身分證字號或營利事業統一編號進行歸戶，將其持有股數彙總後並歸入該投資人通訊地址為最新異動之帳戶。
- (3) 將集中保管之所有投資人歸戶後之資料製作成媒體(光碟片)，提供給發行公司或其股務代理機構。
- (4) 所提供之資料有：投資人戶名、身分證字號／營利事業統一編號、戶籍地址、通訊地址、電話、集中保管帳號、持有股數、款項劃撥帳號等。

6、報表作業

將日中所有線上帳務性交易(送存、領回、匯撥、轉帳、設質、繼承、贈與、私人間讓受……等)之交易明細、流水記錄，將其帳號、證券代號、交易類別、交易股數、交易日期等資料自流水記錄中摘取，加計當日買賣成交資料並依帳號別排序後列印交易明細表，提供給證券商核對帳務使用。

7、網路報表傳送作業

將參加人(證交所、櫃檯買賣中心、證券商、發行

公司、股務代理機構)之各種報表，依參加人代號彙整，即同一參加人之所有報表併為一份，利用網路，將報表傳送至參加人電子郵箱。傳送前，先將報表資料，利用參加人之公開金鑰加密，加密後再傳送，以確保傳輸資料之安全。

8、資料交換作業

本公司與證交所、櫃檯買賣中心業務往來密切，許多作業皆靠電腦系統互相傳遞資料來完成。

- (1) 本公司收檔作業計有：證金標借作業、收盤價、成交紀錄、標購紀錄、拍賣紀錄、可轉債債息、權證發行、借券作業、ETF 作業、券商交割價款等共 53 種。
- (2) 本公司傳檔作業計有：外資轉帳餘額、證金標借圈存、避險專戶餘額、權證履約明細、錯帳／違約更正申報、應收付擔保價款、交割款項、委託變更明細資料、ETF 圈存資料、外資額度控管明細資料、中央交換公債額度控管資料等共 60 種。

9、核帳作業

本公司處理集中市場及櫃檯買賣市場之交割轉帳作業，故每日買賣轉帳完成後並對其結果作交叉驗核，作業如下：

- (1) 檢驗投資人餘額總和與證券商帳簿餘額總數是否相符。
- (2) 檢驗投資人交易明細總和與證券商帳簿之異動總

數是否相符。

- (3) 檢驗證券商當日買賣交易確認後之成交資料與本公司夜間批次轉帳之資料是否相符。

10、系統維護作業

本公司管理超過 1,600 萬戶投資人帳戶資料，1,300 多個連線單位。為確保系統正確且迅速有效之運作，系統平日之維護作業非常重要。維護工作計有：

- (1) 證券商開業、停業、合併之建檔及帳務移轉作業。
- (2) 證券上市（櫃）、下市（櫃）、合併、減資等之建檔及帳務移轉作業。
- (3) 系統操作流程管理及自動化流程安排等作業。
- (4) 系統變更管理作業。
- (5) 檔案重整及資料庫重整作業。
- (6) 磁碟空間管理及檔案空間管理作業。

11、檔案備份作業

- (1) 每一交易日，當所有參加人結束連線作業後，會先做一次資料備份作業，遇執行批次作業發生異常時，資料能回復到異動前之狀態。
- (2) 在批次執行完成後，系統會再作一次備份，以供隔日線上交易發生異常時能回復到異常前之狀態。
- (3) 備份之檔案包括線上所有之檔案及資料庫，如存券主檔、日結檔、結算檔、客戶基本資料檔、交易流水檔、買賣明細檔……等，目前系統約 1,190 個檔案，需辦理備份作業。

(五) 系統重要數據參考

項次	系統描述項目
1	本系統自民國 79 年元月上線使用迄今，已逾 20 年。
2	相關程式共約 5683 支，連線交易程式約 805 支。
3	系統資料量共約 1TB，資料包括參加人及投資人基本資料及帳戶餘額、交易明細等資料。
4	參加人連線家數約：約 1300 家，總計約 4000 台工作站。
5	投資人開戶數：約 1470 萬戶。
6	連線交易量：約 26.5 萬筆交易/日平均(不含成交)。
7	成交回報交易量約 110 萬筆/日平均；歷史最大量：268 萬筆；30MSU 限縮下約可處理：270 萬筆。
8	批次處理量：累計約 3 億筆紀錄/日平均。
9	傳送參加人報表：每日寄出約 1600 份電子報表郵件，合計報表份數約 1 萬 2 千份。
10	交易累計量：約 44.7 億筆，約 536G GB。
11	未登褶資料量：約 8 億多筆，約 80GB。

四、銀行新核心系統移轉成功因素探討

臺灣金融業更換銀行新核心系統選擇趨勢，放棄原大型主機的升級計劃，走向開放式主機平台，本章節探討不同之核心系統移轉策略，並以國內政府組織或臺灣金融業為個案，瞭解其資訊系統移轉過程中管理面及技術面之問題與解決方式，作為未來證券存託系統移轉之參考借鏡。

(一)核心系統移轉策略

系統移轉有三種基本方式：一次全部移轉(big bang)、按階段移轉(phase-in approach)、按漸進式移轉(evolutionary approach)(使用者導向之企業資源規劃系統移轉方法，蔡春智，東海大學工業工程學系碩士論文，2000)。

1、一次全部移轉 (big bang)

目標系統完全取代既有系統，將所有既有系統的使用者介面、應用軟體、組合物件及資料庫，依可用性移轉至目標系統，同時需做企業流程再造。一次全部移轉至目標系統，可達全面性整合資訊系統與企業流程之效。對於重要性高且嚴重影響組織競爭力的資訊系統，應採取此策略。但此法最大的缺點為整個導入過程必須鉅細靡遺的完整規劃整體資訊系統與管理流程，且依企業維運目標，需投入大量專案人力進行規劃、管理及參與專案建置。若導入失敗將浪費太多資源、成本與時間甚至失去企業本身的競爭優勢。

2、按階段移轉 (phase-in approach)

當系統移轉專案本身存在著技術無法克服的困難

點，如目標系統太過龐大、需整合之既有系統過多，超出企業之人力資源或機器設備所能負荷時，可借由按階段導入，也就是模組化方式，一部份一部份的轉換新系統，以降低專案困難的程度。

依系統功能模組按階段移轉，視企業需求，保留部份模組功能及資料於既有系統，按階段逐步移轉模組至目標系統。以降低移轉風險，提高系統移轉之彈性；惟本項作業需按步就班，每一階段完成需停、看、聽，思考下一階段作業需修正下一階段工作項目及方針，確保每一階段作業之完成度與可靠度。

3、漸進式移轉 (evolutionary approach)

以使用者需求漸進式移轉系統，並透過使用者的回饋，逐步發展新系統。此策略雖破壞性最低，使用者適應度最高，但容易造成移轉時程拉長且效果不彰。

(二) 研究個案說明

由於國內資訊系統移轉為近幾年才逐漸被重視，故截至目前為止，有關此領域之研究仍屈指可數。由於研究時間有限，本研究在初級資料方面，以國內已完成之相關個案研究為主要參考的資料來源。本研究參考的個案包含：

1、個案 A 稅務資訊作業平台移轉計畫

本個案以公共行政部門為對象，探討公共行政部門在進行系統移轉時的關鍵成功因素。於目前國內政府機關資訊組織人力普遍不足，故其有關係統移轉所需之應用程式、使用者介面及資料庫常委託廠商進行開發，機關除擔任委外專案監督角色外，相關資訊部門人員則隨

時參與及支援專案各項任務，使專案得以順利執行。個案 A 與一般政府機關不同之處在於，其所處理之資料為較隱密性之資料，且需配合政府之政策，即時規劃並建置符合全國性需求之國稅資訊系統。

由本案例可充份瞭解，逢專案委外時，廠商扮演一極為重要之角色，舉凡與外包單位之使用者訪談、溝通，業務領域知識及流程之瞭解與改造，及配合使用者對於系統使用回饋之應對，對於專案之成功與否，亦佔有舉足輕重之角色與地位。

2、個案 B 核心資訊系統(FNS)

個案 B 開啓銀行核心系統走向開放架構的先例，是全臺灣第一家核心系統採用開放性架構的銀行。本個案得以瞭解個案 B 對於業務面之需要而產生既存資訊系統移轉之需求，系統移轉前，單位內資訊人員必須對其既存資訊系統進行分析、設計與目標系統規格之訂定等工作，交由委外廠商開發後，進行後期之測試與移轉上線工作，移轉期間，使用者全程參與並即時提供資訊資源，如此才得以將前端之介面與需求充份導入目標系統。為縮短目標系統移轉上線時間，除使用者積極參與外，實際採用直接上線之導入方式，為降低風險，其做法為強化測試過程與加長測試期程，以要求目標系統移轉後所發生之狀況減至最低。

3、個案 C 新銀行核心系統

高達 7.29 億元的新銀行系統專案，是個案 C 營運數十年來，第一次翻新核心系統。雖非國內第一家從大

型主機系統走向開放架構的銀行企業，但是，由於個案 C 的營運規模大，業務複雜度高，其 IT 組織原本就是整合性的組織，不是個別獨立的組織，所以，藉由本個案得以瞭解組織文化、組織策略，以及資訊科技等因素上，對系統開發的過程產生影響。亦可由本個案得知，雖然個案 C 最後成功的進行了系統轉換，但其中仍有可能導致轉換失敗的風險存在，或是轉換過程中應注意而未進行的工作事項。

各個案之基本資料，分析比較如圖表 2.6.13；於系統移轉的過程中所面臨之問題及關鍵成功因素，詳見下頁《三、系統移轉關鍵成功因素》。

個案名稱	個案 A 稅務資訊作業平台移轉計畫 (簡稱個案 A)	個案 B 核心資訊系統(FNS) (簡稱個案 B)	個案 C 新銀行核心系統 (簡稱個案 C)
資料來源	既存資訊系統移轉模式之研究(蔡志雄，世新大學資訊管理所碩士論文，2004)		拋去 20 年包袱重新打造銀行系統架構，楊惠芬，iThome 媒體報導，2009
移轉原因	硬體年限已達汰換階段、系統老舊維護成本過高、組織與流程變動、政府政策需求	既存資訊系統已老舊、無法繼續進行維護或因新需求之產生而被迫進行移轉工作	銀行合併後，系統包袱倍增，考量到長遠發展的需求而進行移轉工作
專案人力	委外 (使用者介面部份由中心資訊人員與	委外 (系統分析、設計及移轉則由	委外

	廠商共同撰寫)	銀行資訊人員負責)	
專案期間	1998~2003	2002~2005	2006~2009
既存資訊系統架構	專屬系統資料庫 網路式資料庫 COBOL	IBM DL1 之階層式資料庫	大型主機架構
目標資訊系統架構	RMDB Oracle (9i)	Unix RMDB Oracle (8i)	IBM R6 RMDB Oracle
移轉方式	大部份採用一次移轉上線之方式另少部份採用平行處理方式進行移轉	採用一次上線及移轉之方式	階段上線(ATM等先行建置系統上線一段時間後，帳務處理系統才上線)

圖表 2.6.13 個案基本資料比較分析表

(三) 國外集保系統轉換經驗參考

於參考新加坡及馬來西亞集保系統轉換為新一代系統架構經驗發現，基於不同目的及考量，各自有不同的作法，表述如下：

	新加坡	馬來西亞
目的	汰換老舊 IBM 主機、降低系統維運成本	降低系統維運成本、開放式系統之擴充性及整合性高
策略	為降低系統轉置風險及費用、縮短專案時程，移植原系統之 COBOL 程式，新程式則採 Java 開發	為降低系統轉置風險及費用、縮短專案時程，移植原系統之 COBOL 程式，不變更業務處理邏輯
執行	專案委外廠商為 Clarity 公司，將主機 COBOL 程式以工具轉換，在 Clarity 的主機模擬軟體 UniKix 上執行	專案委外廠商為 IBM Malaysia 1. 連線交易程式及批次程式維持 COBOL，程式修改幅度約 20% 2. 使用者介面以 Java 重新開發 3. 批次作業控制程式以 Unix shell 重新開發 4. 查詢類交易以 JAVA 開發直接讀取資料庫，不經 COBOL 程式處理

圖表 2.6.14 國外集保系統轉換經驗參考

(四) 關鍵成功因素

組織因為既有系統功能或資料容量無法應付迅速變化的科技環境，為提昇競爭優勢及營運績效，組織應視既有系統

的現況，配合組織的願景及組織文化，選擇一個最適合的移轉策略，進行系統移轉。在根據本研究所引用的個案，並參配其他相關研究，整理在系統移轉的過程中所面臨之問題及關鍵成功因素，歸納分述如後。

1、非科技因素

(1)組織文化之整合

政府機關或企業進行既存資訊系統合併移轉時，往往使得非系統之因素(即人員問題)，阻礙系統移轉工作之執行，除此之外，業務人員與資訊人員間之衝突問題亦時有所聞。因此，若能在系統移轉專案前，加強組織文化與人員達成共識，對系統移轉之貢獻亦不可忽視。例如個案 C 是以業務導向的概念在規畫專案，故其專案經理是由曾經擔任過分行經理的主管出任。其系統規劃也是以業務導向思考，讓系統思維更貼近市場，業務與 IT 的整合效益才因此提高。

(2)流程再造與員工抗拒

配合新系統調整工作流程，對於資訊系統移轉成功與否有正向的影響。因新的資訊系統的使用，勢必會衝擊原有的作業流程，很多原本人工作業或判斷的部份，改由系統處理；當新系統上線，可能導致員工地位降低或造成利益衝突；在組織方面，可能因管理者之投資報酬理念及守舊的態度而影響系統移轉的成功；而在群體方面，則可能因系統移轉產生權利結構的破壞而抗拒；而員工強烈的抗拒

心態常是導致組織變革遲遲無法推展的主要原因。

在這種系統移轉過程中，原本的作業流程勢必得配合新系統作調整才能發揮效益，而這種組織再造的變革過程中，對於有技術障礙的同仁，儘早安排教育訓練及調整工作內容，可以降低抗拒。依國內相關研究(黃明乾，我國大型製造業從事資訊系統轉型策略之個案研究，國立中山大學資訊管理研究所碩士論文，1997)，整理資訊系統移轉人員問題及因應策略如圖表 2.6.15：

人員問題	因應策略
<ul style="list-style-type: none"> ●資訊人員對系統轉型之恐懼 ●資訊部門控制權之影響 ●對新系統信心不足 ●平行作業帶來之阻力 ●系統轉型之時間壓力問題 ●配合系統轉型之分析，帶來之作業困擾 ●對系統之轉換信心不足 ●操作方式不同，造成排斥心理 ●教育訓練困難，作業負荷過重，使用單位抱怨 	<ul style="list-style-type: none"> ●建立資訊部門同仁之共識 ●資訊部內部人員任務之重新編組 ●藉總管理處之力量，逼使各使用單位配合系統轉型計劃 ●與軟體公司合作開發後，加強資訊人員之信心 ●藉由決策主管之策動和充份溝通，達成使用者充份配合系統轉型之意願 ●重新招募新資訊人員 ●採工作輪調，避免使用者有新舊系統之操作環境比較

圖表 2.6.15 資訊系統移轉人員問題及因應策略

(3)高階主管的支持及決心

在個案中，一致認為「高階主管的支持及決心」是影響系統移轉的一個很重要的因素。在政府部門中，資訊部門係屬於與業務科室平行的單位，在系統移轉的過程中，面臨到的組織成員的抗拒及組織

流程再造等衝擊的壓力，實非資訊部門可以獨立承擔，久而久之，資訊部門由主導單位，變成了被動的配合單位，這對於機關的發展及系統移轉的成敗，都是負面的影響。在這樣的情況下，高階主管的支持與變革的決心，不僅對於資訊部門是一個重要的支持的力量，面對組織成員的反彈，也具有一定程度的安撫力量。而系統移轉對組織的影響甚鉅，除了投入資源之外，作業流程的改變更需要高階管理者的全力支持，才能貫徹流程再造，面對組織抗拒等阻力時，做為主導團隊之後盾。

個案 C 中，營運高層給予專案團隊非常大的支持，多次強調「不要為了上線而上線，一定要系統穩定才能上線」、「穩定、安全，是個案 C 對新核心系統的基本要求」、「新的核心系統不一定要急著上線，但是，系統上線之後，一定要很穩定」。這樣的態度是從上而下凝聚的共識，讓專案團隊猶如吃下定心丸，毫無後顧之憂地專心投入各個階段的系統轉換工程。使用者端的 170 多個單位，也在邁入測試階段之後，密切配合。

個案 B 中，訪談結果亦顯示，高階主管之決心，為考量市場競爭力、效率、速度及產品皆應具競爭力，對於移轉參與人員應該適時激勵，系統才得以完整開發。

(4) 充足預算

政府部門的預算編列方式，係依預期（計畫）二年後所發生的經費而編列。這種編列方式對於行

政業務費用可能適用，但是，對於進步快速的資訊科技而言，影響系統重建或移轉的因素，往往不是二年前可以預見的；而且，二年後所可以運用的資訊科技及經費亦非預算編列時可以預見。

但是礙於預算執行績效，勢必得執行。在經費不充裕的情況下，貿然進行系統移轉，不僅無法提供完整的功能協助使用者提高工作效率，而且，採用過時的資訊設備或科技，會降低系統的使用壽命，增加系統移轉的機率。屆時，組織又必需承擔下一次系統移轉所帶來的不適應及工作績效的降低等成本，長時間下來的內耗，對組織而言會產生負面的影響。所以，在經費不充裕的情況下，不要輕易決定系統移轉。

(5)使用者參與

在政府公共行政部門中，最基層的使用者無法參與政策的制定，對於組織策略及目標的相關訊息，均透過口耳相傳，得到片面或不盡真實的消息；而一個組織系統移轉策略的訂定，如果能夠提高透明化程度，讓使用者在最短的時間之內知道，可提高使用者對於新系統的接納度與使用的意願。個案 A 中，系統移轉前皆與稅務資訊作業相關使用者進行深入之訪談，除了瞭解既存系統之基本功能外，更希望使用者能將業務流程一併考量於新系統中，並於開發及測試過程中持續不斷修改與更正。

個案 B 中，使用者於移轉專案初期即積極參與，即參與進行需求訪談、系統測試與回饋等工作，

因此對於目標系統有相當程度之瞭解，協助設計出更符合使用者需求及與使用者工作密切相關的系統功能及操作介面，對降低系統上線後之排斥感及衝擊，提高使用者的使用意願等方面，有很大的助益。

(6) 內部資訊人員之人力配置

政府機關或企業之資訊資源與人員有限，當面臨既存資訊系統移轉時，為維持營運系統仍正常運作，系統移轉人員之調配成為相當重要之因素，配置得當，則系統移轉得以順利進行，配置不妥，則將直接影響企業系統之正常運作。

主導單位可能是資訊部門或非資訊部門，這關係到組織對資訊科技的重視程度，及資訊部門在組織內的定義，若組織定義資訊科技是主導企業流程的主要競爭力，則其資訊部門應具規模，且由資訊部門主導系統移轉；反之，若組織將資訊部門視為較被動的支援單位，其屬性僅支援其他部門之活動，則其資訊單位規模較小，而系統移轉的主導單位可能為非資訊部門。然而，不論主導單位是資訊部門或非資訊部門，主導系統移轉的團隊應同時具備流程面及技術面的專業人員，其質量的優劣會直接影響到系統移轉的成敗。主導單位應先尋求組織內部資源整合，當主導系統移轉能力的質或量缺乏時，則應尋求外部資源，並成立專案小組，以利重新組合成員。茲整理個案人力配置情形如圖表 2.6.16：

個案名稱	個案 A 稅務資訊作業平台移轉計畫	個案 B 核心資訊系統 (FNS)	個案 C 新銀行核心系統
資訊團隊成員	n/a	200 人	450 人
系統移轉專案人員	所有人	60 人	150 人
既存資訊系統維護人員	相關稅務系統皆分配固定之承辦人進行維護工作，較大或難以維護之專屬系統則委外辦理	80 人	300 人

圖表 2.6.16 個案資訊人員配置表

(7) 委外廠商的專業能力與控管

政府公共行政部門因受限於法令的規範及服務的目的，組織文化及行政程序較刻板，政府公共行政部門係以預算及民眾期待為資訊科技採行之主要原因。而資訊科技的應用，往往處於經費及資訊不對稱的情況下，資訊科技的採用通常來自合作夥伴的建議。系統建置及移轉時，非常仰賴合作夥伴的專業技術能力。此外，部份作業委外情況時，直接面臨即為廠商與業主間之溝通協調問題，一般而言，委外專案合約若無明確規定廠商與業主彼此間之權利與義務，或對於系統需求不明確時，極易產生彼此認知上之不協調。因此，本研究個案 A 中，個案 A 於進行需求規格書之訂定時，即要求嚴謹以降低日後發生問題之機率。後續於需求訪談階段，

要求廠商系統分析人員需與使用者進行長時間之溝通以確實瞭解使用者需求；其他於移轉過程新需求產生之問題，亦依委外合約之規定，於訂定之範圍內要求廠商進行系統修改。

個案 C 中，系統計畫雖然是由 IBM 承包，但為了縮短接手維護的學習曲線，相關專案成員都直接與 BANCS 原廠建立良好溝通管道。第二階段的修改與調整，個案 C 甚至要求原廠派遣人力來臺灣，並且完成後續的客製化調整。

2、科技因素

(1) 資料庫一致性與資料純化工作

既存資訊系統背後皆連結一龐大之資料庫，系統移轉必將遭遇資料格式訂定、轉換、檢核、測試等過程；另系統移轉時資料庫亦無法容忍錯誤情況之發生。因此，系統移轉前應盡力做好資料純化、檢核之工作，以降低錯誤發生之機率。

個案 A、B、C 中，其共通性為將既存資訊系統之資料庫移轉至關聯式資料庫中，完全依賴關聯式資料庫之架構而運作，個案中所共同遭遇之問題為資料庫格式之整合與轉換等問題，由於不同資料庫之欄位、格式不盡相同，又原始資料庫中之資料亦有錯誤存在，雖個案皆傾向將資料庫移轉委外辦理，但資料庫格式之需求、規劃，及後續之移轉仍需由機關及企業全程參與。

個案 A 中，由於既存於資訊系統之資料相當重要，相關稅務系統之資料格式又不盡相同，故需額

外撰寫轉檔程式將諸多稅務系統之資料庫予以檢核與合併；而稅務系統又具備不可停滯之特性，故於必須審慎規劃資料庫移轉之時段及一致性之問題。

個案 C 中，系統的歷史包袱是資料的正確性及合理性。因個案 C 於過去的整併過程中，為了快速完成系統面的整合，所以，就會放寬部分資料的把關標準，時間久了，不合理的資料也就跟著多了。例如，個案 C 的系統是以「帳戶」為主來設計，基本上，每個帳戶都會有一個聯絡地址，但這樣的情況，可能會出現一種現象，就是同一位客戶總共開了 5 個帳戶，而 5 個帳戶的聯絡地址都不一樣，這樣的情況，有可能是櫃員的疏失，也可能是這位客戶真的有很多聯絡地址，但要怎麼做才能掌握到正確資料，而且又把對客戶的影響減到最小，於專案進行時，資訊部門就必須跟業務單位共同規劃討論，制定資料轉換規則。

(2)系統測試及修改

整體而言，機關或企業中仍應建立系統及使用者介面測試區域，供使用者或系統開發人員於平日即不斷進行系統測試，並透過測試回饋機制，分別回饋至使用者與系統開發人員，惟如採委外方式辦理，則業主與委外廠商之權利義務關係應於合約中詳細敘明。各企業所進行之測試雖然不盡相同，但一般會進行單元測試、功能測試、壓力測試或整合測試，其目的在於強化目標系統之穩定性，故系統移轉測試工作為既存資訊系統移轉專案中之一個關

鍵成功因素。

個案 B 中，於進行系統移轉專案時，原業務之新需求仍不斷產生，其解決作法為針對業務需求將目標系統及資料儲存於另一新的環境與設備上，並不斷持續修正移轉之介面，而前端之介面與作業仍正常進行。另移轉採用目標系統直接上線與非同步方式進行移轉，惟上線前亦需經過如單元測試、功能測試及整合測試等工作，以降低問題產生之機率。

個案 C 中，因為系統轉換，不只是翻新系統而已，整個資訊架構都徹底改變了，所以，個案 C 用了一年的時間進行系統測試，除一般情境外，亦針對月初日、月底日、發薪日等情境做過測試。而當系統面、功能面的測試都完成之後，動員全行進行模擬演練測試，第一次測試於 5 分鐘內即宣告失敗。幸好，第八次後續的模擬演練測試每一次都成功，系統最後才能如期上線。

(3) 縮短移轉期程

移轉期程可長可短，雖受限於既存資訊系統大小程度不同，而有不同之移轉期程，因此，政府機關或一般企業應於移轉前即進行系統移轉期程之評估，並配合單位內適合之系統運作週期，選定適當之時間點進行系統移轉之工作，如此便能縮短移轉期程。

個案 A 中，部份稅務資訊系統移轉時通常仍需進行一至二個星期之平行移轉作業，以確保系統移轉後之正確性，無論資料或系統之移轉皆需具備即

時上線之能力，故系統移轉之排程對專案進行而言，具有舉足輕重之地位。

個案 C 中，採取分次中斷系統的做法，盡量縮短服務中斷時間。相較於其他銀行的核心系統轉換，個案 C 還必須克服的問題，包括捷運沿線的 ATM 服務絕對不能中斷。然而，為了因應核心系統轉換，服務不中斷幾乎是不可能的任務，個案 C 所能做的，是把影響降到最低，因此，最終採取分次中斷的做法，進而縮短每一次服務中斷的時間。個案 C 原本的核心系統在 5 月 28 日零點正式走入歷史，新的核心系統也在 5 月 29 日凌晨 1 點鐘啟動，中間只有停機 25 個小時，遠低於個案 C 合併時，停機 40 個小時的記錄，也比原訂目標提早了 1 小時完成。

新系統上線的第一個營業日，因為是在 4 天連假結束之後，而且又適逢月底轉換月初，所以交易爆增至 70 萬筆，相較於平日的交易至少增加了 3 成，對於系統造成的負擔無庸置疑。過程中，為了讓分行臨櫃作業順暢執行，不得不短暫停止自動化交易等局部服務，進而調整硬體資源配置，並且把資源集中在分行等第一線交易系統上。在經過適當的調整之後，自動化交易服務等問題都在半小時內得到解決。

參、未來發展策略之探討

一、證券存託系統未來架構之研析

證券存託系統改善未來架構究竟要在原來 Mainframe 主機環境下，或於開放式系統環境下進行新系統之開發建置，主要評估研析項目如下：

(一) 資訊系統一致性

本公司 A 級系統當中除證券存託系統使用傳統大型主機外，其餘皆使用開放式主機，考量資訊系統維護人員、開發工具、監控軟體避免雙重投資，建議本公司資訊系統能朝一致方向規劃設計。

(二) 穩定性

大型主機的最大特性有著極高之穩定度，及強大的容錯能力，故能廣泛在公眾事務、金融、商業、醫療、國防、學術、航太等領域獲各企業採用，開放式主機在穩定性以叢集(Clustering)技術，鏡射備份(Mirroring)技術彌補，使開放式主機能具備不停頓機制，來盡量達到大型主機所具有系統運行之穩定性。

(三) 安全性

大型主機過去因為封閉系統，駭客不容易侵入並造成危害，但現在由於網際網路蓬勃發展，相對業務服務必須對外開放服務；故無論在大型主機或者開放式主機本公司皆投入完整可靠的安全機制，例如在大型主機使用 RACF，而開放式主機則使用 A-MOS 來落實本公司安全政策。

(四) 維護成本

Mainframe 主機系統與開放式系統之長期軟、硬體營運維護成本之整體考量：

1. 參考某金融機構現況，Mainframe 主機的硬體維護費用每年約新台幣四百萬元外，需再每年支付軟體授權費約新台幣二千六百萬元，每年總計花費維護費用約三千萬元；以相當處理效能之開放系統主機的硬體維護費用每年約新台幣一百六十萬元，需再每年支付軟體維護費概估約新台幣四百萬元，故將傳統大型主機(Main Zframe)轉置到開放式主機每年維護費用則約省二千四百萬元。
2. IBM 大型主機的硬體費用 z9 入門價大約 100 萬美元(臺幣 3 千 2 百萬元)外，光是一年 16 顆處理器作業系統的授權費，企業就要花費 1.17 百萬美元(約臺幣 3 千 7 百萬元)，再加上每年業務量的需求，每增加一個處理器，就得花費 3~5 萬美元(約 1.28 百萬臺幣)，再加上應用程式的費用，企業一年花在大型主機的金額非常可觀。

(五) 人才尋求及養成

系統開發人員在 Mainframe 主機系統與開放式系統開發的人才找尋及養成難易度之考量。

1. 大型主機應用系統的開發，由於受限於主機運作環境的不開放，COBOL 語言造成程式異動及維護的不易，業務需求變化很大，但如果從封閉系統中，進行撰寫 COBOL 語言，往往要花費許多開發時間才能完成系統功能。
2. 大型主機的系統開發多半使用 COBOL 語言，但相對

於開放式架構的程式語言而言，目前懂得開教程式語言的人才較多，懂 COBOL 語言的人少，企業必須透過培訓的方式，來培養 COBOL 的人才，對於企業而言，造成管理上的問題且懂得 COBOL 語言的人才，將逐漸退休，且目前學校教育已經沒有教授，將造成人力的斷層。

(六) 業務開發時間

1. 以目前存託業務需求發展現況，本公司證券存託系統業務功能種類繁多，相關連線及批次作業程式甚巨；為快速服務證券期貨市場需求，必須有效率化之電腦系統及開發工具。
2. 大型主機程式開發工具過於老舊且在維護上十分沒有效率，一個簡單的需求便須花上數周或數月來進行修改開發及測試的工作，而在開放式主機中具備了參數化、模組化的開發方式對所有業務種類、業務項目、作業項目、作業程序、資訊產生流程中、所涉及檔案更新、參數異動、相關檢核、功能特性以及邏輯架構，可建立適用之應用系統模組，來提升相關業務系統之開發效率。

(七) 技術發展趨勢

目前國內外金融業逐漸以關聯式資料庫技術 (Relational Data-Base)，替代現有 Mainframe 主機系統之傳統循序檔案 (VSAM) 及舊式資料庫 (IMS-DB)，可以有效加速新種業務之開發及整體系統運作效率：

1. 以 Mainframe server 上的主要開發語言：COBOL、PL/1 這類 procedure language，生產力很難"再"提

高，因為程式中的 business logic 與 db manipulate logic 很難分開，programmer 必須兼顧兩者而不能只專注在 business logic，加上不是 interpreter type 開發-測試很浪費時間。

2. 使用關聯式資料庫在程式中的 business logic 與 db manipulate logic 是分開的，business logic 由程式邏輯層處理，db manipulate logic 由資料操作層處理，可以有效加速新種業務之開發及整體系統運作效率。
3. 近年來，電腦科技之發展，開放系統處理大量資料已證明可行，而開放系統之特色是使用者對系統有更多之選擇機會和應用者有更多之控制權，亦即能因應新功能在較短時間內，以較低成本取得最新技術，實現業務需求服務功能。
4. 本公司向來以主機為主之封閉系統，固然建構了一個相當穩定、可靠且安全之資訊系統。但面對外在資訊技術資源、人力資源、設備資源之發展以開放系統為主之環境。應改變原來 One Size Fits All 之觀念，提供彈性化、差異化、處理多樣少量之系統，並與原主機系統結合，是本公司均必須面對之課題。
5. 近年來，由於開放式 Unix 伺服器的衝擊下，部份金融業者因銀行兼併或本身業務因素等影響下，放棄了大型主機的升級計畫，走向了開放式的伺服器環境中，目前包含了國泰世華銀行、元大銀行、台新銀行、上海銀行、板信銀行、中華郵政、聯合信用卡中心等正在進行或已完成大型主機走向開放的伺服器環境

之中。

(八) 比較項目表列

項次	比較項目	傳統大型主機	開放式主機
1	資訊系統一致性	證券存託系統使用	除證券存託系統使用傳統大型主機外,其餘皆使用開放式主機
2	穩定性	具有不停頓容錯機制	具有不停頓機制
3	安全性	兩者均具備完整可靠的安全機制,可落實本公司安全政策 1. RACF(傳統大型主機) 2. A-MOS(開放式主機) 3. 防火牆建置	
4	維護成本	高(依初次建置、人員養成、硬體成本逐年降低、軟體成本逐年升高之變動而有不同結果)	
5	維護人才尋求及養成	1. 使用 COBOL 語言開發, 程式異動及維護較不易。 2. 懂 COBOL 語言的人越來越少, 企業必須透過培訓的方式, 培養 COBOL 的人才。	1. 使用 Java、C++(C)、SQL 語言開發, 程式異動及維護較容易。 2. 人才找尋容易。
6	業務開發時間	較慢(程式開發較難以模組化)	較快(開發語言具模組化特性)
7	技術發展趨勢	1. COBOL、PL/1 這類 procedure language, 生產力很難“再”提高。 2. 廠商投入開發新軟體工具較少 3. 測試較費時間(較無好用測試工具)	1. 使用各式各樣軟體工具, 可以有效加速新種業務之開發及整體系統運作效率。 2. 新資訊技術之使用已趨成熟與普及化, 處理大量連線或批次作業資料, 已經驗證可行, 金融業已陸續轉置。

8	改善轉置風險	兩者皆有風險 須研議執行策略(例如分階段)，來降低風險
9	金融業選擇趨勢	放棄了大型主機的升級計畫，走向了開放式的伺服器環境中： 1. 台新銀行 銀行核心資訊系統(FNS) 2004-02 2. 國泰世華銀行 新銀行核心系統 2009-06 3. 彰化銀行 核心系統轉換 2004-09 4. 元大銀行 新核心系統開發 2009-02 5. 聯合信用卡中心 信用卡系統 2009-10 6. 兆豐金控銀行 信用卡系統 2004-05 7. 其它:日盛金控、台電核能電廠、血液基金會、基隆港務局、財政部海關空運系統

綜觀前述章節各方面主、客觀因素考量，本研究案建議證券存託系統未來架構可朝開放式主機方向規劃及開發設計，在策略上為降低系統轉換風險及有效人力運用應進行全面架構規劃並仔細估算考量，規劃原則及策略分述如下。

二、規劃原則

因應證券存託系統面臨改善之必要性與迫切性，系統改善考慮層面需涵蓋業務觀點（Business View）及技術觀點（Technical View），除就現有業務功能逐一分析外，尚須就資訊面整體考量平台整合、資料庫設計管理、開發工具、模組化工程、系統安全管理、對外連線機制及系統改善相關設備外，更須將未來業務發展目標一併於規劃時納入考量，使改善後之系統兼具業務擴充彈性及技術延展性，茲將改善規劃原則分述如下：

（一）改善應用系統支援未來業務發展策略

本公司未來業務發展，除了目前提供的所有功能，其他如股票發行市場股務事項、國外基金發行買賣帳務處理、保險業證券市場進出帳務處理、其他特別參加人帳務處理、國內外投資證券相關業務……等，提供有效之金流、券流、資訊流等資訊服務，業務上尚有非常廣闊空間，但亦有賴應用系統之改善，能帶來一個效率高、成本低、品質好之資訊系統支援。

（二）建立標準的系統開發及維護環境

引入系統開發工具，建立標準化系統開發程序、自動產生標準化之文件、建立資料間之關聯性，除了有助於系統開發品質外，對同仁辦理系統分析、系統開發、系統維護之時效亦有助益，工作成果亦容易檢驗評估。

（三）採行模組化分析

就現有系統中，所有業務種類、業務項目、作業項目、

作業程序、資訊產生流程中、所涉及檔案更新、參數異動、相關檢核、功能特性以及邏輯架構等因素，建立適用之應用系統模組，以利未來相關業務系統之開發效率。

(四) 強化測試機能

引進適當測試工具，增加測試範圍、廣度及深度，建置完整測試環境增加壓力測試功能，提高系統開發品質。

(五) 整合網際網路開放系統之運用

因應資訊技術之進步，及證券市場參與者業務需求，藉由系統改善建構一個整合開放式資訊系統環境，以利未來業務之推展。

(六) 善用人力資源

透過系統改善之進行，使資訊人力資源之進用、訓練、運用、調整及備援，易於適當規劃與彈性運用。

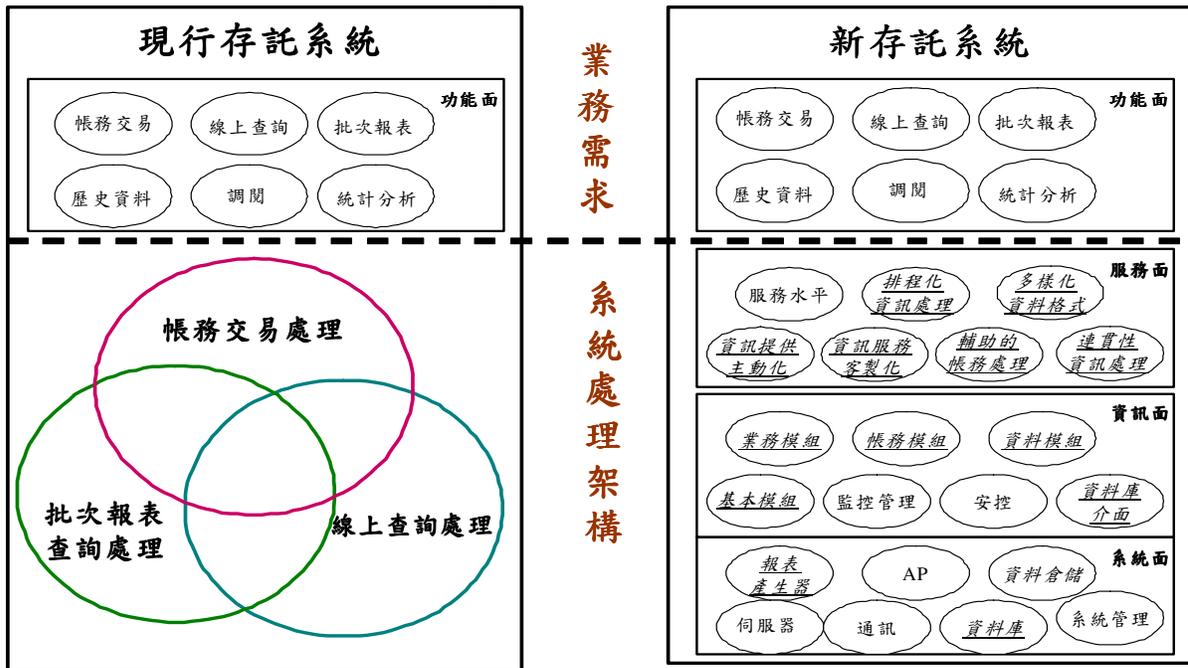
三、執行策略

(一) 本專案以系統架構、程序及人力與設施三個面向進行規劃，規劃示意如圖表 2.6.17



圖表 2.6.17 規劃示意圖

(二) 以資訊服務導向進行專案改善如圖表 2.6.18

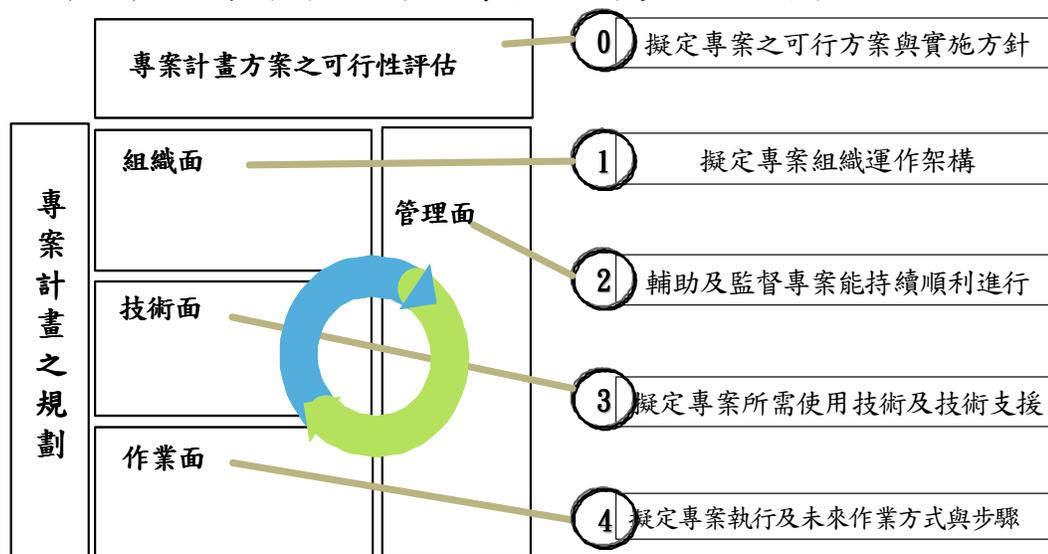


圖表 2.6.18 資訊服務導向

上圖為現行存託系統處理架構，因應 20 年來之業務需求變動，帳務交易、線上查詢、批次報表處理已出現疊床架屋，新增業務或維護系統常牽一髮動全身，規劃難以周全之窘

境，未來新系統規劃設計將以資訊服務導向，系統架構朝模組化、參數化彈性設計，以提高應用系統維護方便性，進行本專案之改善。

(三) 以專案管理層面考量執行步驟如圖表 2.6.19



圖表 2.6.19 專案管理層面示意圖

四、結語

- (一) 綜觀各方面主、客觀因素考量，本研究案建議未來架構可朝開放式主機方向規劃及開發設計。
- (二) 為降低系統轉換風險、減少業務需求凍結時間及有效人力運用，應協同專家顧問進行架構全面規劃並仔細估算系統架構、程序、人力及設施後決定推展策略。
- (三) 推展策略建立後，應以無比決心及勇氣朝目標邁進。

第七節 小結

應用系統是資訊的靈魂，程式人員撰寫程式就是賦予電腦生命，而整體資訊環境中其核心是資料庫，無論程式人員所撰寫成千上萬程式，目的就是改變或查詢資料庫內容，所以資料庫的應用是資訊發展之重點，換個方向就程式觀之，其程式均是人所撰寫，自然會有疏漏或錯誤或未考慮事項，如何減少程式問題成為軟體發展上努力方向，也是資訊廠商開發不同產品以降低人為疏失；在本應用系統研究探討之章節，可看出此次研究結果主要朝向標準化與自動化兩大方向，也符合因應公司內部系統多樣化之考量，期能發展出標準化與自動化以減少人力物力成本。

在第一節依集保各項業務系統，就各項目如傳輸方式、安控方式、使用者對象、結算機制等進行分類，一則提供資料給後續各章節研究使用，另一則提供給資訊規劃開發參考使用，以避免資源浪費。接著再就目前軟體發展趨勢，分別探討資料整合、軟體工程提昇系統品質、中文標準化、資息交換之統合方式及資訊架構之發展予以分別研究，以提出未來軟體走向之輪廓。

從軟體整體發展路徑來看，現今主要朝向資料運用與軟體工程兩大區塊，雖然大家熱中討論大量資料運用(Big Data)，但在運用時必須架在資料彙總基礎上，因此資料整合運用這一節偏重於將不同資料庫，如何萃取每日異動資料以彙總成為資料倉儲之技術探討，並參考相關案例再針對業務考量，研究如何建置一個資料超市，以配合線上分析與資料挖掘(Data Mining)供使用者分析使用，其目的為擴大服務市場，提供市場風險控管，協助市場發展；另於透過軟體工程

提昇系統品質討論，將程式開發流程共同性部分，提出研究自動化可行性，以減少不必要人為疏失，該節注重在流程表單自動化、軟體版本控管及稽核軌跡、自動化編譯和部署、自動化測試等方向，雖然這些功能均有資訊產品配合，但需考量現行組織、業務系統交易流程及全體同仁確實長久執行，如此才能達到期望效果。而中文碼整合與訊息交換之研究，其所涉及範圍包含公司內部各獨立系統及外部連線單位，因此研究結果也必須要取得各系統負責人及外部單位資訊人員共識，不僅要克服系統問題，也要涉及推廣的問題，所以此二節討論的內容如實施，則溝通技巧大於資訊技術；最後資訊發展策略，強調電腦主機的未來走向，雖然目前很多金融機構，規劃將專屬性主機轉置到開放性主機，也有一些成功案例，但在成本考量上需思考未來十年期間成本，以及同仁資訊技術範疇等等，這些考量之後再進行轉置規劃，如此比較容易達到預期效果。

本次應用系統之發展研究，雖未涉及目前熱門海量資料(Big Data)及雲端等議題，但我們主要從現行運作資訊系統深入研究，化繁為簡找出共同性建立標準化，也許不是當今熱門項目，卻是資訊發展之根本，可由此研究探討加強資訊軟體基礎，未來才可進一步走向新資訊領域。

第四章 資通安全機制之強化

第一節 內部資通安全機制之強化

壹、研究目的及範圍

一、研究目的

近幾十年來資訊科技日新月異，資訊樣貌亦由傳統式專屬主機與封閉式專屬網路，逐漸演進到開放式網際網路的 E 世代，隨著網際網路熱潮擴散至全世界，上網人數急速增長，帶動了網際網路形形色色的商業活動，網際網路到處衝斥著大量的金流、資訊流，電子交易成為人們生活中不可或缺的一環，惟在大規模使用金流、資訊流的同時，直接造成了資訊系統面臨各種安全上的威脅，諸如電腦病毒、駭客入侵、電子資料的竄改、刪除、非法複製、未經授權的資料存取、冒名或匿名傳送、非法網路監聽、惡意破壞、甚至意外天然災害等等，皆衍生了許多管理面、技術面、法律面等多層面的問題，資訊安全的問題，遂成為注目的焦點。

二、研究範圍

藉由本公司內部整體資通安全管理制度、各類資訊系統所採行之相關各項資通安全管理機制，由內而外由使用者端、主機端、內部網路端至連外網路端之資通安全防護，逐一檢視各項資通安全防護機制，確認各項機制之適當性，對應現行最新資安主張與技術，期能找出可加強之處。

本節將針對內部資通安全機制逐一分析，次節將針對外部資通安全機制逐一分析。

貳、現況說明

一、整體資通安全概述

本公司資訊安全政策開宗明義，「充分運用資訊及通訊安全科技，建構兼具有效性及完整性之資訊安全防護機制，以確保資訊資產之機密性、完整性及可用性。」。本公司自成立以來即利用電腦處理龐大的證券與期貨結算及集中保管資料，資通安全為首要要求目標，故自民國 93 年即通過 BS7799 資通安全認證，並一直維持認證之有效性，BS7799 於民國 94 年 10 月為 ISO 國際組織採用，成為 ISO27001 資通安全認證，ISO27001 除要求組織需建立 ISO27001 認可之資通安全管理系統 (Information Security Management System, 簡稱 ISMS) 外，尚需持續維持 ISMS 的有效性，並接受發證機構每半年一次的發證後稽核，以確認其有效性，發證 3 年期滿，需接受發證機構全面重新稽核，通過後再頒予為期 3 年之認證證書，且組織需配合 ISO27001 之改版，同步修改組織的 ISMS。本公司一直維持 ISO27001 認證之有效性，歷次稽核發證機構從未發現任何不符合之缺失，本公司資通安全認證歷程詳如圖表 3.1.1。

年月	認證活動	說明
93年10月	取得資通安全認證 BS7799 證書	為全國第 26 家通過驗證的機構
94年12月	取得擴大認證範圍證書	為證券周邊單位第 1 家取得全部資安等級系統驗證
95年11月	合併票保 BS7799 證書並改版為 ISO27001	將票券保管相關系統納入認證範圍
98年10月	ISO27001 驗證三年期滿，重新認證	順利通過認證，無不符合事項
迄今	ISO27001 持續有效	

圖表 3.1.1 資通安全認證歷程

二、資通安全組織及其運作

本公司「資通安全處理小組」為常態任務編組，負責有關資通安全預防及危機處理相關事宜，建立蒐集稽核線索及入侵活動偵測資料，並加以分析與闡釋，以確保資訊基礎建設之安全性，提供完整不中斷的資訊系統運作，遇資訊及網路系統遭受破壞或不當使用等緊急事件發生時，能迅速作必要之應變處置，期能於最短時間內完整回復系統功能，有效降低事件損害之影響範圍。

「資通安全處理小組」組織架構及其運作方式說明如下：

(一) 組織架構

「資通安全處理小組」設召集人及執行長，其下設置安全預防分組、危機處理分組及稽核分組，其組織架構圖詳圖表 3.1.2。

(二) 工作職掌

1. 召集人：

- (1) 主持資通安全會議。
- (2) 資通安全相關問題處理之決策。
- (3) 安全配套措施之決策。

2. 副召集人：

- (1) 代理主持資通安全會議。
- (2) 資通安全相關問題處理之決策。
- (3) 安全配套措施之決策。

3. 執行秘書

- (1) 襄助召集人資通安全事宜。
- (2) 協助召集人召開資訊資產評估、資訊安全風險評鑑及資訊安全政策評估等資通安全會議。
- (3) 協調資通安全相關問題之處理及人力之調配。
- (4) 協調安全配套措施之執行。
- (5) 向召集人、副召集人及首長報告資通安全事件狀況及處理情形。

4. 安全預防分組：

- (1) 訂定系統安全等級及權責區分。
- (2) 審視資通安全相關文件規範。
- (3) 檢視資訊資產價值及風險評鑑作業等資通安全機制。
- (4) 檢討資通安全事件，訂定預防措施。
- (5) 監督資通安全監控作業。

(6) 蒐集資通安全新知與趨勢，培訓資通安全技術。

(7) 小組幕僚作業。

5. 危機處理分組：

(1) 規劃危機處理程序。

(2) 查明安全事件原因。

(3) 確定影響範圍並作損失評估。

(4) 執行緊急應變措施。

(5) 辦理安全事件通報。

(6) 執行解決辦法。

(7) 檢視資訊資產價值及風險評鑑作業等資通安全機制。

6. 稽核分組：

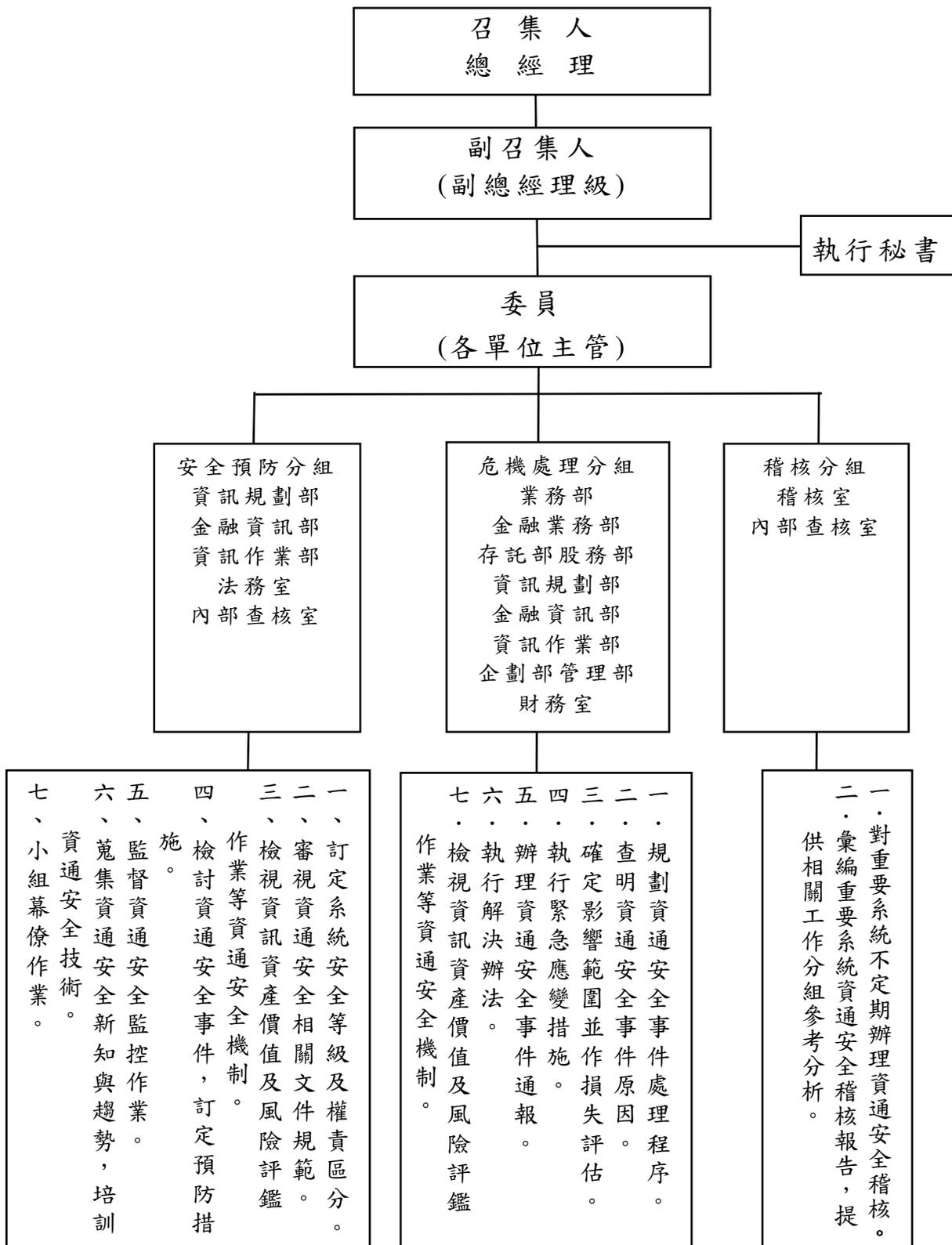
(1) 對重要系統不定期辦理資通安全稽核。

(2) 彙編重要系統資通安全稽核報告，提供相關工作分組參考分析。

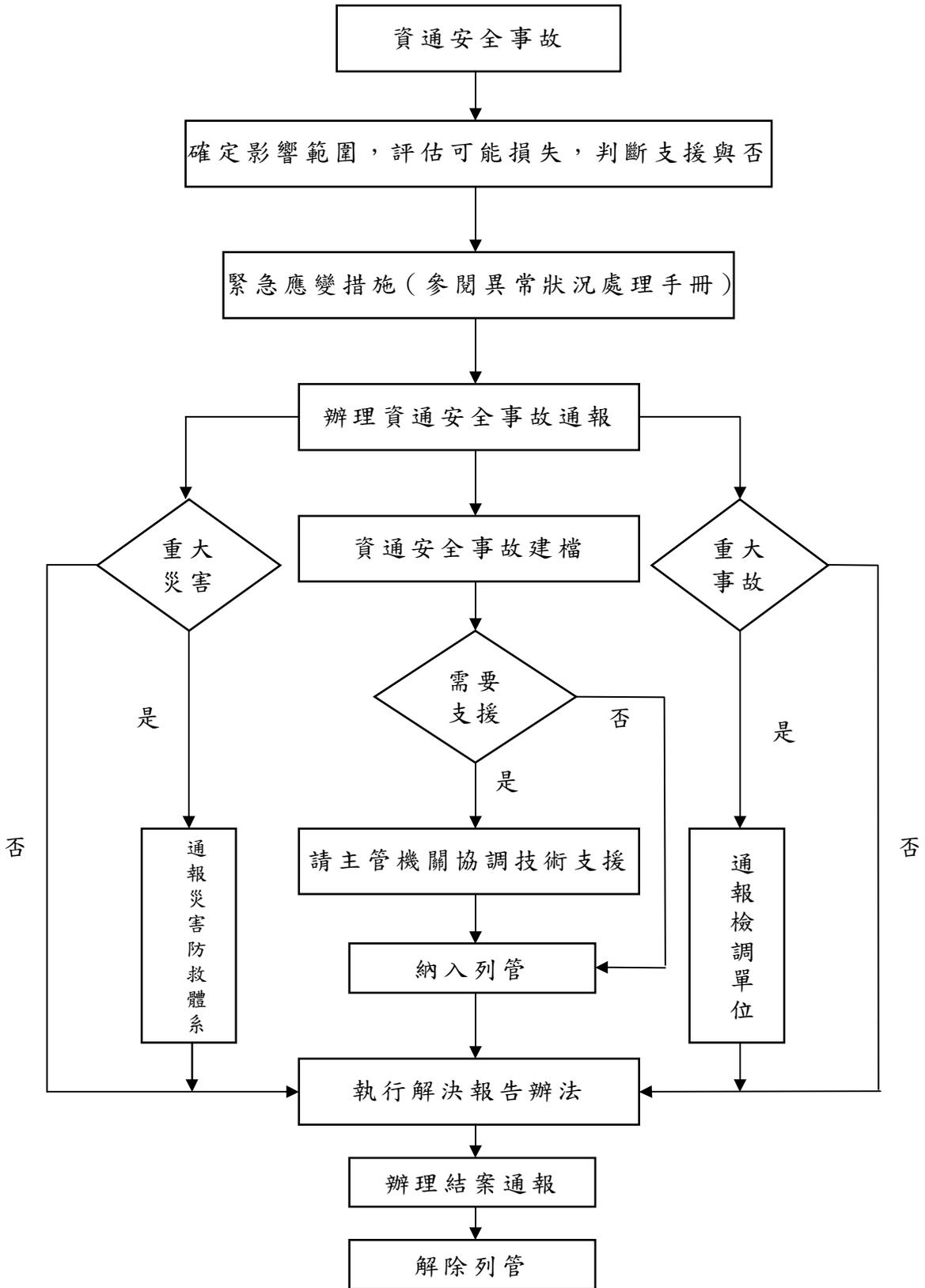
(三) 資通安全事件通報及應變作業

1. 資通安全事件發生時，資通安全處理小組依據本公司資通安全事件通報及應變作業流程(如圖表 3.1.3)及異常狀況處理手冊及相關作業規定，有效率的排除異常，將系統回復正常運作，倘該項資訊安全事件危及人員生命或設備遭到破壞等涉及民刑事案件時，亦及時通報檢調單位請求處理；如引發重大災害時，同時向現行災害防救體系通報，請求支援處理。

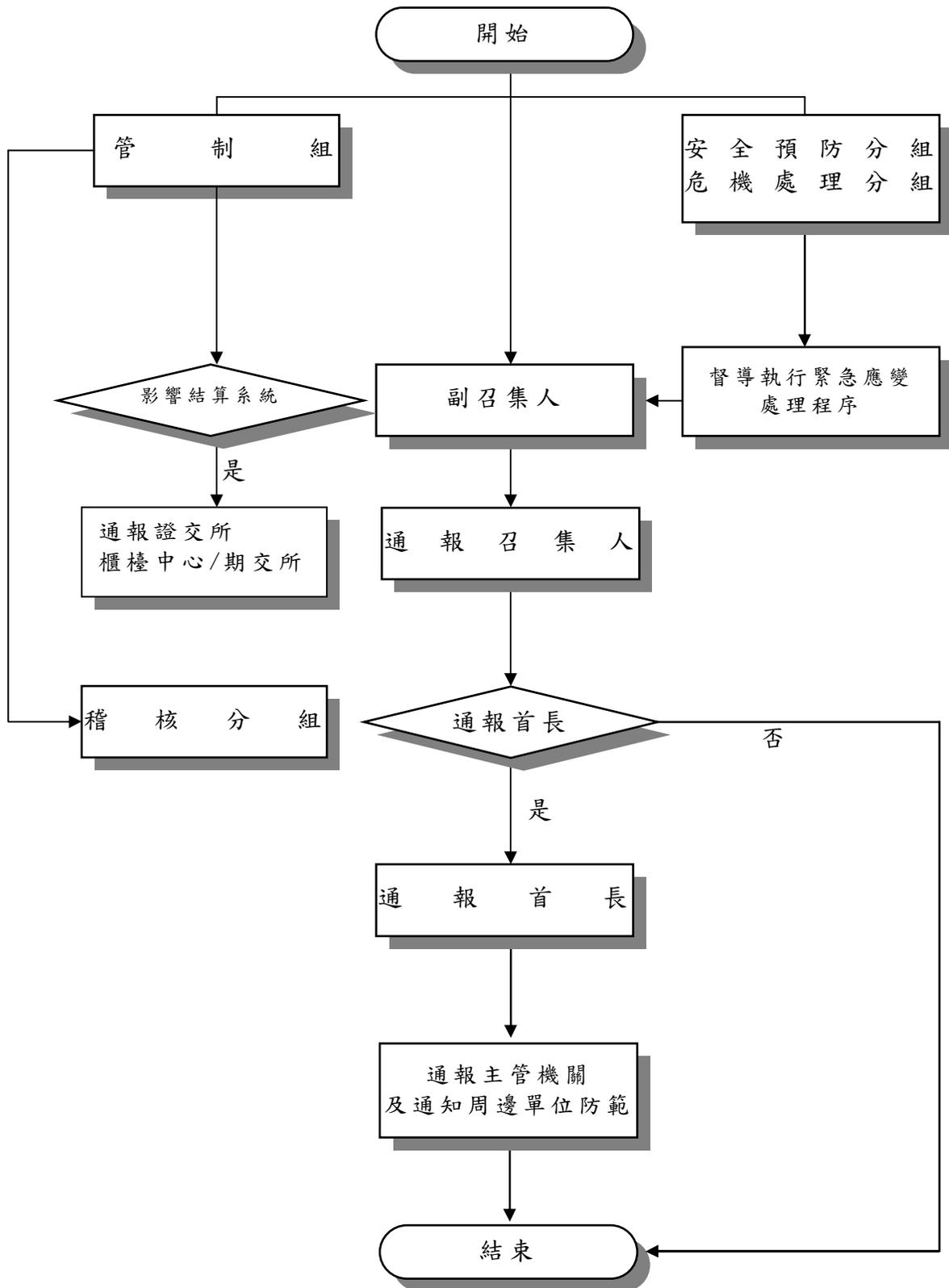
2. 即時將發生資訊安全事件之事實、可能影響之範圍、採取之應變措施等事項，填具「資通安全事件通報單」通報主管機關，並通知業務相關單位，當系統回復正常運作時，亦需將解決辦法透過「資通安全事件通報單」傳送，以解除列管，資訊安全事件通報作業流程(如圖表 3.1.4)。



圖表 3.1.2 資通安全處理小組組織架構



圖表 3.1.3 資通安全事件通報及應變作業流程



圖表 3.1.4 資通安全處理小組通報程序

三、本公司資訊安全管理系統

資訊對組織而言就是一種資產，和其他重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運、將營運損失降到最低。資訊存在的方式有許多種，可以列印或書面表示、可以用電子方式儲存、可以用郵寄或是電子郵件傳送、也可以用影片播放或以口頭說明。然而，無論資訊的形式為何，何種方式與他人共享或儲存，都應以適當的方式加以保護。資訊安全之目的為達成：

－機密性 (Confidentiality)

確保只有經授權的人才能存取資訊；

－完整性 (Integrity)

確保資訊與處理方法的正確性與完整性；

－可用性 (Availability)

確保經授權的使用者在需要時可以取得資訊及相關資產。

本公司早已於民國 93 年建立資訊安全管理系統 (Information Security Management System, 簡稱 ISMS)，並取得 ISO27001 國際資通安全標準驗證，依標準要求，持續進行規畫(Plan)、執行(Do)、監控 (Check)、矯正與改善 (Action) 的 PDCA 循環(如圖表 3.1.5)，維持 ISMS 有效性並符合 ISO27001 標準。與 ISMS 相關之程序書共計 48 本，茲就本公司採取之措施簡述如下：

資訊安全管理系統 (ISMS) Information Security Management



ISMS目的在於保護資訊資產的機密性、可用性與完整性。

圖表 3.1.5 PDCA 循環

(一) 本公司為確保資訊安全管理持續有效，針對資訊系統之資料存取管理、開發與維護管理、實體環境安全管理、通訊與作業管理、管制區域安全管理等，製定詳細控制程序，記載於本公司 ISO 體系程序文件，由全體員工一體遵行，控制程序細節在此不贅述。

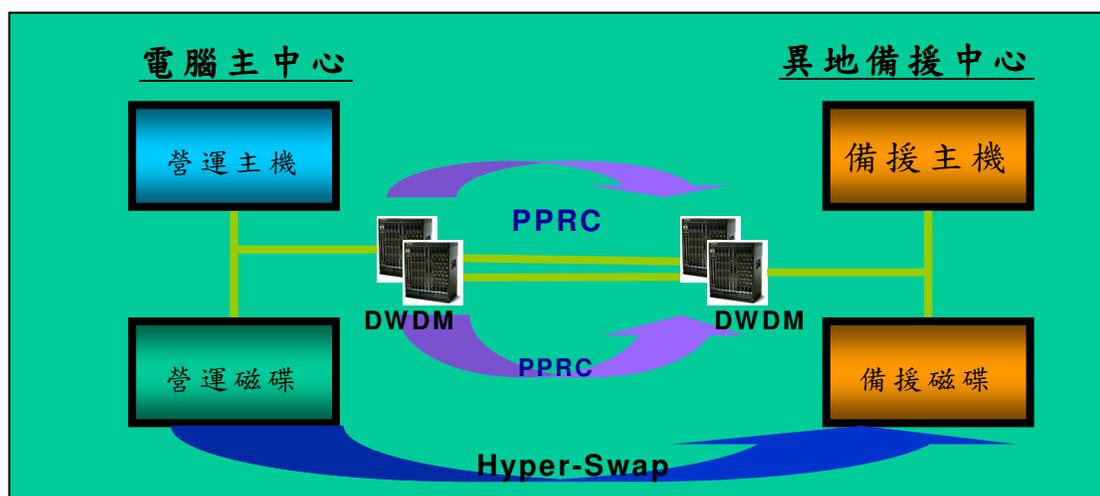
(二) 異地備援機制 DRP 與業務永續運作 BCP

本公司為有效降低營運風險，建置有完善的異地備援機制及業務永續運作計畫，每半年定期演練乙次，期使每位同仁熟悉應變程序，並持加強程序檢討，說明如下：

異地備援機制，是將重要的資料分開兩地存放，並即時同步資料，當電腦主中心的設備發生問題，異地備援中心的

設備可以立即接手取代繼續運作，提供的資訊服務不會因地理位置所發生的天災人禍等不可抗拒事件而中斷。

本公司異地備援中心與電腦主中心分別設置於不同的地理區域，其間相隔約 100 公里之遙，經由 PPRC(Peer to Peer Remote Copy) 技術可具體實現電腦主中心和異地備援中心資料的同步(如圖表 3.1.6)，透過 DWDM(Dense Wavelength Division Multiplexer)光纖通訊高密度波長多工分工器機制可快速傳送，隨時保持兩地資料的一致性，並確保每一線上交易同步修改兩地的資料庫檔案。



圖表 3.1.6 電腦主中心和異地備援中心資料的同步

業務永續運作計畫(Business Capacity planning，簡稱 BCP)的制定是一件複雜的工作，不論災害發生前的預防準備、災害發生時的緊急應變及災害發生後的復原重建，都需要本公司各部室的通力合作才能確保本公司營運的持續。本計畫著重於統合各部室的作業，成為本公司面對災害之預防準備、緊急應變及復原重建工作的依據。

本計畫明確規定本公司主要營運功能的場所無法運作時

之備援處所，並特別強調業務永續運作小組的功能與職責，對於會對本公司所提供之服務、資訊系統及組織功能造成衝擊之災害的預防準備、緊急應變及復原重建，將統由該小組負責。

1. 概述

(1)、目的

為確保本公司主要作業能於預期的時間內復原，本計畫明確鑑別本公司關鍵作業及重要作業以及所需的人力及資源，以確保有足夠的人力及資源來進行災害的預防準備及緊急應變，另本計畫明確規範業務永續運作小組的職責，該小組的主要職責之一是建立公司層級的程序規定，以確保本公司營運持續。

(2)、範圍

為鑑別出本公司主要業務，本公司進行業務營運衝擊分析，依據營運衝擊分析的結果，本公司的作業可分成：

- a、關鍵作業（4小時內回復），共 37 項作業。
- b、重要作業（4-12 小時內回復），共 6 項作業。
- c、一般作業（12-24 小時內回復），共 4 項作業。
- d、影響較小作業（24 小時以後回復），共 20 項作業。

本計畫之目標是要於 4 小時內使關鍵作業（如集中市場劃撥交割作業）能回復運作，重要作業（如帳務日結作業）能於 12 小時內回復運作。另為有效評鑑本公司資訊資產風險，將上述業務營

運衝擊分析之結果，做為評鑑資訊資產風險之依據。

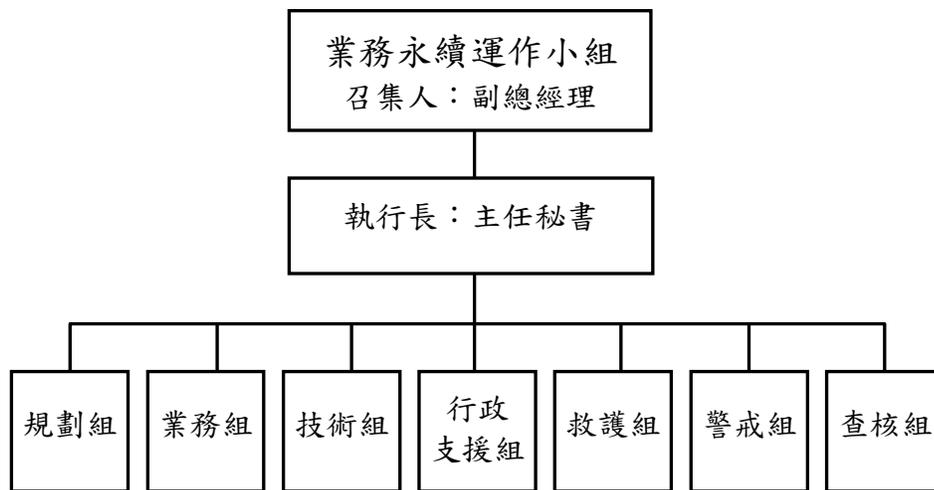
(3)、災害範圍

- a、主要辦公場所或主要機房場所損毀。
- b、主要辦公場所及主要機房場所同時遭受損毀。

(4)、業務永續運作小組(簡稱 BCP 小組)組織

BCP 小組為一常態性任務編組，主要職責為負責業務永續運作計畫及危機處理相關事宜，執行事前預防、事中應變及事後復原的工作。

a、組織圖



圖表 3.1.7 BCP 組織圖

b、各組組織與權責

角色	負責人	職 責	編 制
召集人	副總經理	1. 負責宣布啟動業務永續運作計畫 2. 宣布復原工作完成切換回原營業場所營業 3. 調度備援場所的資源 4. 負責統一對外發言	
執行長	主任秘書	1. 負責監控整個情況及指揮調度各組進行應變及復原工作	

角色	負責人	職 責	編 制
		2. 每年須啟動一次對本計畫的全面檢討或更新 3. 將年度總檢討或更新的結果向本公司 BCP 小組召集人報告 4. 負責召開災害事後檢討會議	
規劃組	組長	擬訂演練計畫及制修訂業務永續運作計畫	由企劃部同仁組成，企劃部部門主管擔任組長
業務組	組長	負責確認技術組所備援及回復的設備及系統符合業務單位的需要	由業務部、股務部、存託部、財務室及金融業務部同仁組成，業務部部門主管擔任組長
技術組	組長	負責資訊設備及資訊系統的備援及回復	由資訊規劃部、資訊作業部及金融資訊部同仁組成，資訊規劃部部門主管擔任組長
行政支援組	組長	負責備援及復原階段相關行政支援工作(如調派車輛及人力、保險理賠等)	由管理部及法務室同仁組成，管理部部門主管擔任組長
警戒組	組長	在備援及復原階段對公司的人員及資產提供足夠的安全防護	由管理部管理組同仁(警衛)組成，管理部部門副主管擔任組長
救護組	組長	搶救災害現場並向BCP小組報告損害狀況	由稽核室同仁組成，稽核室部門主管擔任組長
查核組	組長	針對災害事件之因應及檢討改善措施，進行追蹤管制	由內部查核室同仁組成，總稽核擔任組長

圖表 3.1.8 BCP 各組組織與權責

(5)、測試及演練

本計畫須每年進行測試及演練，依據「異常狀況處理手冊」所訂狀況屬嚴重至不能控制且有危及公司營運中斷之虞者，每年的測試演練項目可包括：

- a、針對各種情況進行沙盤推演(利用暫時停止營運，以狀況的範例討論災害復原程序)，例如

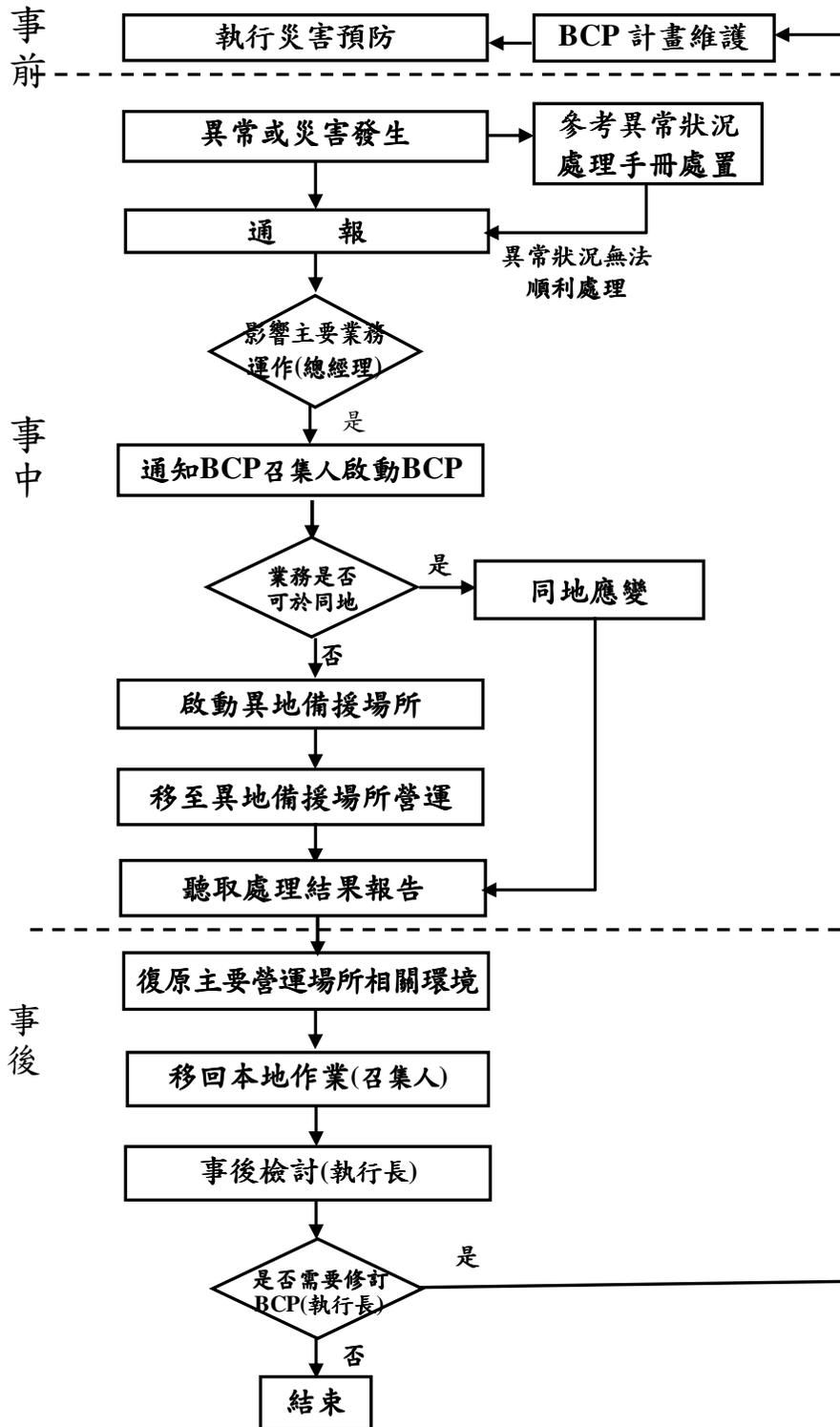
流程演練(Walkthrough & Tabletop)。

- b、狀況模擬(尤其在意外事件或危機範例後,用以訓練員工的定位管理),例如通報演練和疏散演練。
- c、復原測試(以確保資訊系統可有效復原),例如支援關鍵作業之所有資訊系統的復原演練。
- d、測試供應商的設施和服務(以確保廠商提供的服務和產品符合合約中的規定)。
- e、完整演練(測試組織、人員、設備、設施和作業是否能夠妥善處理中斷情況),例如選定「異常狀況處理手冊」之A級狀況進行演練。

為達到預期的測試演練效果,技術性測試由技術組執行,業務演練的部分由每年演練計畫之主辦部室撰寫年度詳細的演練計畫並加以執行;演練過程中的監督及演練計畫執行之確認由查核組擔任。演練完成後,主辦部室與規劃組共同根據每一次演練的檢討結果修正業務永續運作計畫內容,並將修正後的計畫內容向執行長報告。查核組人員要針對災害事件之因應及檢討改善措施進行追蹤管制,並供業務永續運作計畫測試演練或修正之參考。

2、災害應變程序

(1)、流程圖



圖表 3.1.9 災害應變程序流程

3、災害應變策略

本公司發生災害後之應變及復原時期的主要工作說明如下：

(1)、緊急應變階段

緊急應變階段的起始工作以保護生命及財產安全為首要目標，如果主要辦公場所無法使用，應建立臨時指揮中心，供首長及 BCP 小組成員指揮調度；並在災害現場建立安檢界線及管制措施。

(2)、備援階段

備援階段的起始工作以回復主要業務為首要目標，主要業務將視設備及建築物損害程度決定於原場所或指定之備援場所復原。

在備援階段，支援主要作業之系統需能維持運作至原場地復原或永久性場址重建完成為止，在時間及資源許可的情形下，應儘量維持一般及影響較小作業之系統之運作，數量愈多愈好。

(3)、復原階段

儘速回復至正常作業狀態是本階段的主要目標，不論回復至正常作業狀態所需時間的長短，本階段的工作可由災害發生之後立即開始，與備援階段同時展開。

四、本公司其他相關內部資通安全機制

(一) 源碼檢測、弱點掃描、社交工程演練及滲透測試

本公司每半年進行一次源碼檢測、弱點掃描及社交工程演練，滲透測試則為每年進行一次，期能持續加強防護。

源碼檢測使用 Fortify SCA 自動檢測工具，可找出開放式應用系統弱點，防止外界針對網頁應用程式之惡意攻擊，如 SQL Injection 與 Cross-site Scripting 等。

弱點掃描使用 McAfee FoundScan 自動掃描工具，可找出伺服器相關網路及作業系統弱點(木馬、後門程式、病毒及惡意軟體(Trojan , Backdoors, Viruses, and Malware)及作業系統(UNIX / Windows)、Web 程式) 等加以修復。

社交工程演練係由外界寄電子郵件給每位員工，誘使員工開啟該郵件，用以確認員工資通安全警覺性，主管機關所訂目標為惡意郵件開啟率、點閱率須分別低於之 10%及 6%，本公司迄今皆符合標準。

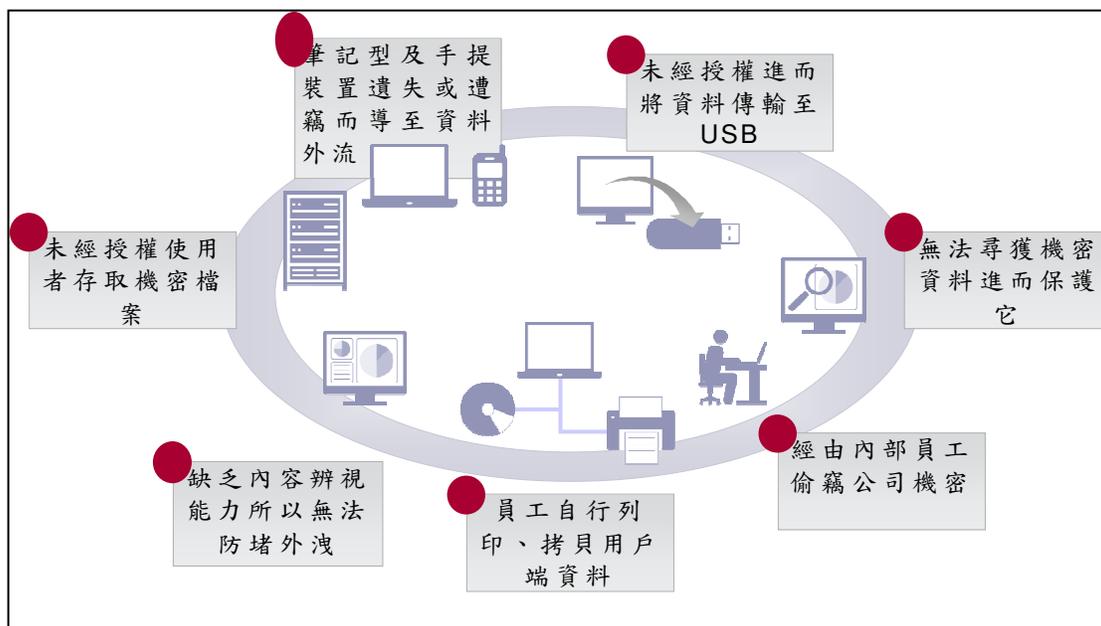
滲透測試係模擬外界駭客之攻擊手法，找出本公司對外服務系統之弱點而加以修復，滲透測試進行各種服務類型之弱點測試，包括作業系統、網站服務、應用程式及密碼強度 4 種類型。

(二) 個資外洩防護系統(Data Loss Prevention)

隨著新版個資法的通過，業界對於資料外洩保護的需求不斷的增溫，而報章媒體時有報導國內外某些單位發生資料洩外事件，造成實質損失及商譽損害，雖然本公司從未發生過資料外洩事件，惟持續不斷加強資安之原則從未改變，遂於近年將資安防護重點聚焦於個資保護。

目前業界對於個資保護的解決方案多採用資料外洩防護系統(Data Loss Prevention, 簡稱 DLP), 並將其分為端點型 DLP(Endpoint DLP)及網路型 DLP(Network DLP)二大類, 端點型 DLP 防止該端點電腦將正式資料或個人資料外洩, 網路型 DLP 防止經由「對外上網」與「寄發外部電子郵件」將正式資料或個人資料外洩。

本公司經檢視資料外洩之諸多可能管道(如圖表 3.1.10), 經考量 DLP 之市場佔有率及訪查業界 DLP 之功能, 並於本公司環境 POC(Proof of Concepts)實測, 選擇出適合本公司需求之 DLP。



圖表 3.1.10 資料外洩之諸多可能管道

DLP 的功能簡述如下：

1. 可依關鍵字 (Key Word) 與正規表示式 (Regular Expression, 如身分證字號最後一碼之檢查方式) 來識別受保護資料(如個人資料、機密資料)。

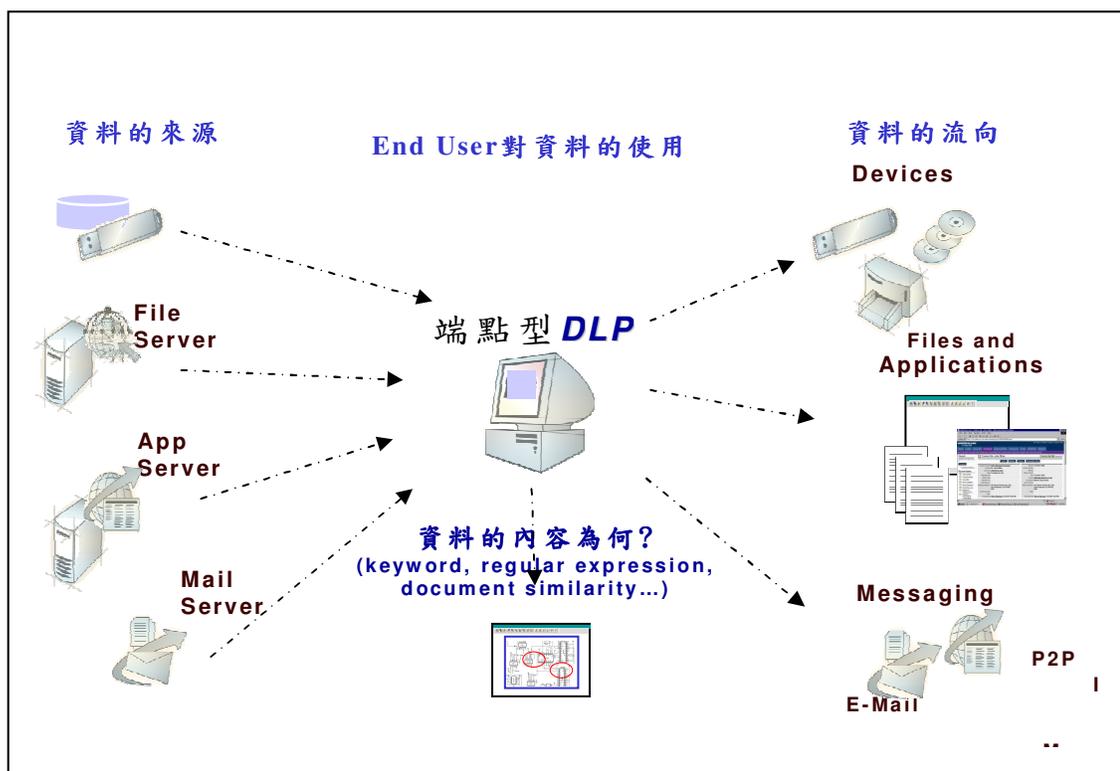
2. 可以指紋特徵(Fingerprint)或標籤(Tag)功能，辨視受保護資料或檔案。

3. 受保護資料控制：

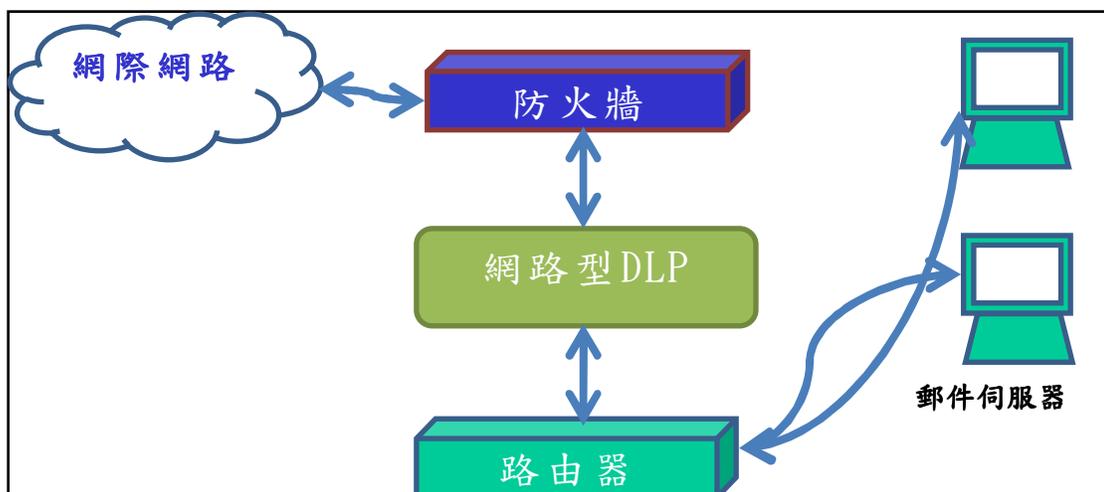
(1) 可禁止資料之複製貼上、剪下貼上、列印、畫面擷取(Print Screen)、上傳至 HTTP/HTTPS 網站、複製檔案及以 eMail 寄出，並可顯示違反資訊安全之警告訊息。

(2) 可禁止複製到卸除式存放裝置(如隨身碟、外接硬碟等)，若允許使用，能記錄特殊資料寫至卸除式存放裝置之資訊內容，並將資料加密(Encrypt)，於裝置 Agent 之電腦始能解密讀出資料。

(3) 可禁止透過 MSN 或 SKYPE 等將檔案傳送出去。



圖表 3.1.11 端點型 DLP 的功能之一



圖表 3.1.12 端點型 DLP 的功能之二

本公司端末型 DLP 已正式運作，網路型 DLP 將於 101 年底前完成建置。

(三) 內部網路 IP 管理工具

目前本公司辦公室(OA)網路之資訊設備，係以安裝「神網軟體」，作為對每一電腦工作站之各項監控與管理，惟對於未安裝「神網軟體」之其他資訊設備，自行使用網路插座連接至本公司 OA 網路時，則不易控管，故藉由 IP 管理工具，以有效強化資訊設備連線之管理，杜絕非法工作站進入本公司 OA 網路，不致產生資安問題與風險。

IP 管理工具可監控並自動蒐集 OA 網路中之資訊設備的實體位址 MAC (Media Access Control)、IP 和使用者帳號，並將以上資訊與預先設定之白名單比對，倘比對結果不正確，代表該資訊設備並未被授權登入本公司 OA 網路中，經由該 IP 管理工具即時告警機制之通知，IP 管理工具管理人員可立即採取因應措施，將該

不合法之資訊設備阻絕，不可連接至本公司 OA 網路，進一步保護 OA 網路安全。

(四) 內部網路傳輸 VPN 加密

虛擬私有網路 VPN (Virtual Private Network) 係利用通道 (Tunneling) 技術、加解密等安全技術，在公眾網路 (例如 Internet) 上，建構出虛擬的私有網路 (Private Network)，以達到私有網路的安全與便利性，並為業界廣泛採用之資通安全機制。

依照本公司目前資料傳輸過程中之路徑類別區分兩項：

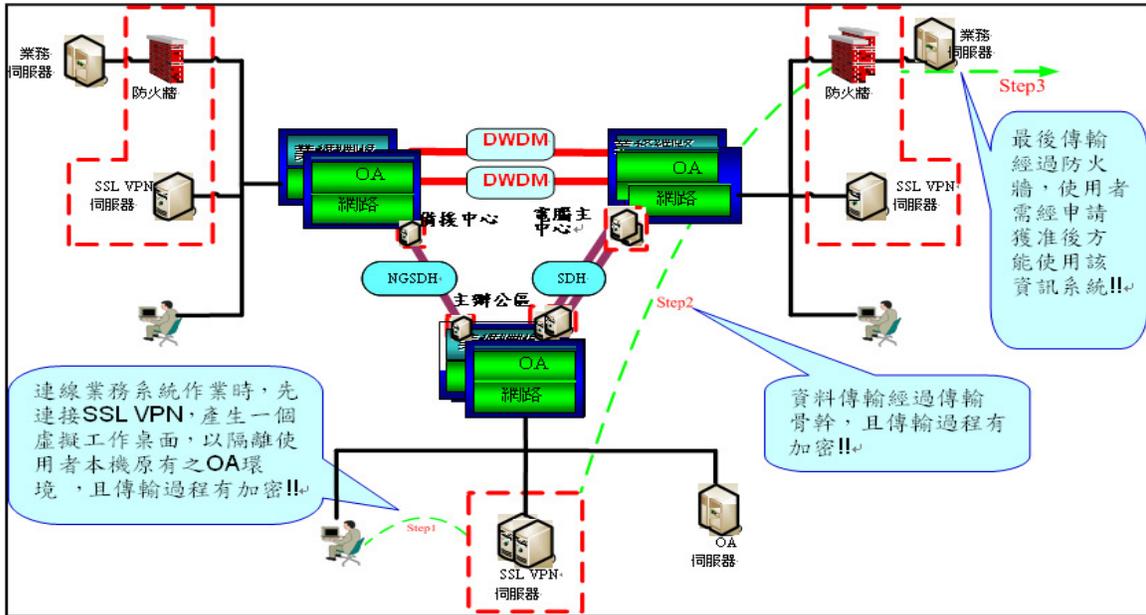
1、主幹傳輸加密：

主辦公區、主機房辦公區及異地備援機房辦公區，主幹網路全程加密，以保護本公司辦公室自動化作業傳輸資料之安全。

2、個人電腦傳輸加密：

工作專區內建置 VPN 加密機制，收容該專區內各專機之傳輸資訊做加解密收送至機房，連線方式採用 VPN 加密通道機制，可達到連線資料加密傳輸之作業安全保護目的。

無論工作專區專機連線至各資訊系統作業環境，及主辦公區連接主機房、異地備援機房，皆能達到全程傳輸加密之成效，如圖表 3.1.13 所示。



圖表 3.1.13 區域網路傳輸加密示意圖

(五) 大型主機稽核軌跡系統

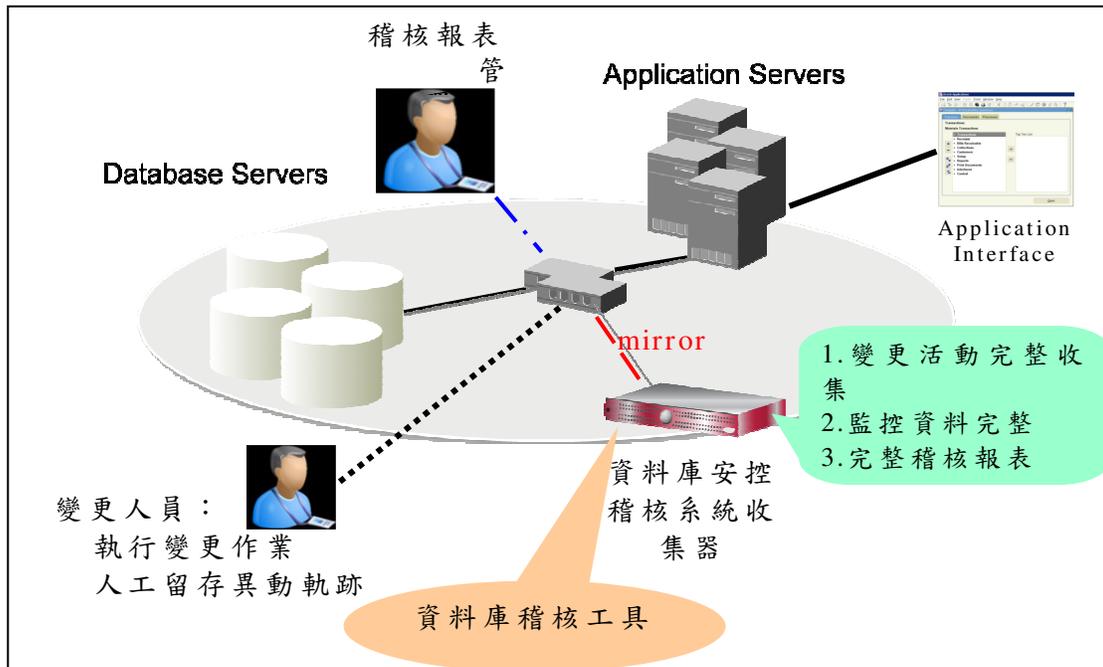
因應新版個資法之即將實施，大型主機稽核軌跡系統可紀錄使用者操作 IBM 3270 終端機之所有行為，將其加密存放於資料庫供稽核檢索，每日出報表(修改檔案紀錄、執行程序紀錄及使用個資檔案紀錄)由專人檢核，符合新版個資法對於舉證之要求。

(六) 資料庫稽核工具

以自動化工具，確保資料庫異動軌跡之完整留存，取代以人工留存異動軌跡時，無法確保未執行其它資料庫或資料異動操作之弊端，又可加強對資料庫存取之人、事、時、地、物，提供完整的稽核與管理。

本公司資料庫稽核工具如圖表 3.1.14 所示，係採網路層方式收集變更軌跡，不影響資料庫效能，並收集和監聽有關 *who*、*what*、*where*、*when*、*how* 五項重要的資料，將使用者和資料庫間的存取行為完整保存

與呈現，符合新版個資法對於舉證之要求。



圖表 3.1.14 資料庫稽核工具

(七) 資料遮罩 (DATA MASK)

內部人員資料外洩是資料外洩之主要途徑，其中包含企業本身的員工或外包廠商人員，透過合法權限有意或無意將資料外洩或帶出。資料遮罩工具之資料偽裝功能將可識別之真實資料遮罩至測試之假資料，兼顧提供完好的測試資料及安全性。

本公司應用系統測試資料遮蔽工作，早先係由各單位自行撰寫程式自正式系統資料庫(或檔案)下載正式資料至測試環境，所使用之程式不一，資料遮蔽處理邏輯亦不盡相同，易造成程式維護及交接問題，現行使用資料遮罩自動化工具，經由圖形化介面操作即可達到準備及建立所期望之測試資料，並藉由產品管理功能，讓測試資料可重複使用，同時提供資料遮蔽效益及完整稽核軌跡，資料保護更周全、更有效率。

參、未來發展策略之探討

一、維護資通安全管理系統(ISMS)持續有效

本公司資通安全管理系統係經 ISO27001 國際資通安全標準驗證通過，經由驗證機構每半年實地稽核一次，確認本公司資通安全管理系統持續有效，並應隨 ISO27001 改版調整本公司資通安全管理系統，除此之外，持續了解資通安全最新趨勢，掌握市場最新技術，適時導入新種資通安全技術及工具，以持續加強資通安全管理系統。

二、建立個人資料管理系統，強化個人資料保護

因應新版個人資料保護法之即將實施，為有效管理個人資料，確保個人資料不外洩，本公司將規劃建置個人資料管理系統(Personal Information Management System，簡稱 PIMS)，強化個人資料管理，執行步驟簡述如下：

- (一) 本公司個資現況與個資標準之差異分析
- (二) 個資作業流程分析與個資盤點
- (三) 個資衝擊分析與個資風險評鑑
- (四) 個資安全控制措施分析及規劃
- (五) 個資相關程序及表單設計
- (六) 個資稽核作業
- (七) 外部稽核驗證

個人資料管理系統建置完成後，將以個人資料管理標準驗證，以確認管理系統之有效性。

第二節 外部資通安全機制之強化

壹、研究目的及範圍

一、研究目的

近年來，政府大力推動 E 化，政府機關、大型企業、金融機構以及軍事單位都相繼採用電腦化資訊作業，運用電腦系統與網際網路來進行資訊處理與交換，以減少人力、物力、財力之投資，許多重要的資料諸如商業機密、國防機密、客戶個人資料、帳務資料及交易紀錄等，都儲存於電腦系統或利用電腦通訊網路來傳遞，因此如何有效的防範電腦及網路世界的非法犯罪行為，維護資訊系統的恆常安全性，已成為電腦世界必須立即面對的迫切課題。

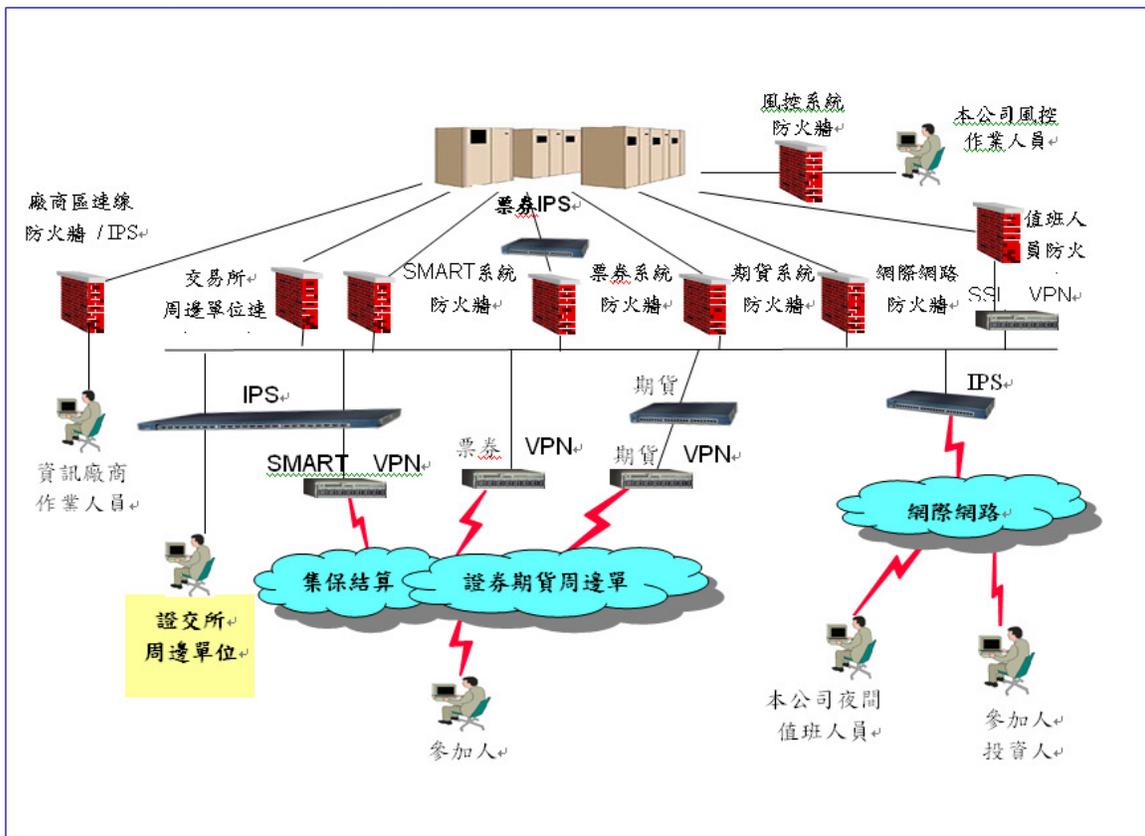
二、研究範圍

檢視本公司對外提供服務各類資訊系統所採行之相關各項資通安全管理機制，由主機端、連外網路端之資通安全防護，逐一檢視各項資通安全防護機制，確認各項機制之適當性，對應現行最新資安主張與技術，期能找出可加強之處。

貳、現況說明

一、防火牆、入侵防禦系統及防毒系統

本公司針對重要資訊系統入口、參加人與廠商之外來連線，配置各型防火牆、入侵防禦設備 (Intrusion Protection System, 簡稱 IPS)，以防禦來自外界之網路攻擊，確保資訊系統運作正常與資訊之合法使用，防火牆及入侵防禦設備現行共 70 餘台，其配置詳如下圖，由本公司網路安全技術人員負責防火牆政策 (Policy) 之擬定、修改與管理，定期檢視防火牆政策，並每日檢查防火牆及入侵防禦設備之運作狀況。



圖表 3.2.1 本公司防火牆及入侵防禦配置

本公司於每一台個人電腦及筆記型電腦上皆安裝防毒軟體，以有效防治電腦病毒，電腦病毒特徵碼可隨時檢查更新，另防毒軟體之掃描引擎亦隨時檢查更新，並設定每台電腦每週完整掃描一次。

二、網頁監控

網頁監控系統(NetIQ)可防範網頁被惡意竄改，藉由監控網頁檔案的檔案修改時間、檔案大小及屬性的資訊，並與上一監控的結果作比較，綜合判斷網頁是否被異動，當有異動發生時，會依設定的條件判斷是否為正常的異動，若為不正常的異動，則啟動回復機制，並即時警示，其監控項目及即時警示說明如下：

(一) 監控項目

1. 網頁內容字串是否被更動。
2. 網頁物件是否被更動。
3. 網頁連結是否被更動。
4. 網站相關檔案之修改日期及大小是否被更動。
5. 檔案是否被新增或刪除。

(二) 即時警示

1. 語音：通知機房值班人員。
2. 簡訊：通知網站系統相關負責人員。
3. email：通知網站系統相關負責人員。

三、網路內容安全管理

網路內容安全管理系統(Content SQR) 可攔截網路不當資訊，系統具有 Email、Webmail、Web、IM、P2P、FTP、

Telnet 及遠端桌面管理等應用層服務(Layer 7)的內容管理與流量分析，過濾分析涵蓋網路層到應用層，功能如下：

- (一) 即時通訊軟體交談訊息記錄。
- (二) 即時通訊軟體使用管理與傳檔管制。
- (三) 即時通訊管理警示。
- (四) WebMail 通訊記錄與附件管控。
- (五) 網頁瀏覽記錄、網址關鍵字過濾。
- (六) P2P 使用管控、傳檔管制。
- (七) Web 影音串流管理。
- (八) FTP、Telnet 及遠端桌面記錄。

四、垃圾郵件管理

垃圾郵件管理過濾系統(SPAM SQR) 可過濾垃圾郵件，即時更新垃圾信特徵、設定過濾條件，以攔截惡意郵件。系統架構於企業內部郵件伺服器前，有效降低企業受到各式郵件攻擊和威脅，如釣魚郵件、病毒郵件、郵件炸彈等攻擊、內部異常濫發郵件。

五、網頁應用程式防火牆

網頁應用程式防火牆 (Web Application Firewall, WAF) 顧名思義，是用來保護網頁應用程式，對抗各式各樣針對網頁應用程式的攻擊，當攻擊對象從網路轉向伺服器、再轉向應用系統，攻擊內容從網路層擴大到應用層時，防禦措施也從防火牆、IDS 逐步演進為 AP Firewall、IPS 等，而隨著 WWW 佔了極大量的網際網路服務比重與惡意攻

擊比重，既有的對抗措施又不足以聚焦與回應針對 Web 的攻擊，遂衍生出 WAF 資安設備。

本公司於民國 100 年建置網頁應用程式防火牆(Web Application Firewall，以下簡稱 WAF)，以有效防範針對本公司網頁應用系統弱點之攻擊。

(一) WAF 阻擋針對應用系統程式弱點之攻擊(應用層)、一般防火牆阻擋 IP + PORT SERVICE 網路層之攻擊。

(二) WAF 防範攻擊種類：

OWASP 組織(Open Web Application Security Project) 為世界夙負盛名的資安機構，其所公布之網頁應用程式潛在漏洞，為業界公認之資安漏洞標準，本公司 WAF 即以防範此類資安漏洞為主，如 SQL Injection 即攻擊者利用 GET / POST 在參數裡塞入部份程式，取得不允許存取的資料；Cross-Site Scripting 則以變更連結方式，將使用者導向惡意網站或假網站，駭客常運用此種漏洞轉址到釣魚網站，騙取使用者輸入帳號、密碼等個人重要資料或植入木馬。

(三) WAF 維運

本公司每日由專人檢視 WAF 運作狀況，每月檢視更新新的攻擊手法。

六、網路傳輸VPN加密

虛擬私有網路 VPN (Virtual Private Network) 係利用通道 (Tunneling) 技術、加解密等安全技術，在公眾網路 (例如 Internet) 上，建構出虛擬的私有網路 (Private Network)，以達到私有網路的安全與便利性，並為業界廣

泛採用之資通安全機制。

本公司之對外服務系統諸如證券存託 SMART 端末系統、期貨結算系統、基金傳輸平台及台銀分割債連線系統等，皆採 VPN 安全傳輸機制，傳輸資料全程加密。

另本公司同仁下班後，倘因資訊作業緊急需要，可使用本公司夜間值班專用筆記型電腦，利用家中 ADSL 與公司資訊系統連線，其連線方式為目前廣泛使用之網際網路，連線架構上採用 SSL VPN 設備結合終端伺服器(Terminal Server)，在夜間值班專用筆記型電腦上搭配虛擬工作平台軟體，以達到身分驗證、資料全程加密、使用者無法將資料下載至個人磁碟儲存設備等機制。

七、使用CA身分鑑別機制

CA 憑證(Certificate Authentication) 為目前廣泛採用且可靠的身分鑑別機制，本公司資訊安全政策規定身分鑑別機制應優先考量使用 CA 憑證，舉凡近期新增應用系統(如股東會通訊投票平台、境外基金交易平台、境外結構型商品申報公告平台等)，其身分鑑別機制皆使用 CA 憑證。

八、資訊安全監控中心SOC

行政院於 91 年 5 月通過「挑戰 2008：國家重點發展計畫」，其中第六項「數位台灣計畫」中，將資通安全列入「資通安全環境建置」之子計畫，其中資安監控中心 (Security Operation Center，簡稱 SOC) 建置被列為重點工作項目，用意在建立針對重要政府資訊系統、民生系統之資訊安全監控機制。各單位需要成立資訊安全監控中心 (SOC)，以建立完整之預警及通報機制作業，透過各項

資訊安全相關的資訊分析研判、預警、及追蹤，確實掌握最新的病毒、漏洞及駭客資訊，使資訊安全事件之損害降至最低。本公司因應國家資通安全會報要求及「影響國家安全、社會安定之重要資安作業系統」納管作業規範，於民國 94 年建置資訊安全監控中心（SOC），以整合網路安全設備及建立資安事件集中管理機制等方式，取代原有著重網路可用性監控之 NOC（Network Operation Center）。以下略述本公司資訊安全監控中心建置內容及系統架構。

（一）技術及平臺

將防火牆以及入侵偵測防禦系統（IDS/IPS）等異質系統的資安事件整合至資訊安全管理 SIM（Security Information Management）平台，而此平台具備對監看的事件進行即時分析以及事件處理功能。

（二）組織及人員

對 SOC 設立明確的組織，將正式組織人員對應至此任務編組內。定義組織內各職位人員的角色及責任，並依職掌建立第一線人員負責即時監控單位環境的資安事件，並進行事件的分析及研判作業，第二線人員負責進階資安事件研判，並協助案件追蹤，第三線人員負責資安事件分析並持續更新知識庫，SOC 主管負責 SOC 整體系統的正常運作，持續改善 SOC 作業品質，並協助資安案件追蹤。

（三）營運綜效

SOC 之建置不僅可有效降低資安風險、簡化事件管理流程及減少設備管理成本，更提升對投資人網路交易及資料保護之安全保障，確保資訊安全防護之無虞。

參、未來發展策略之探討

一、建置資訊分享與分析中心 ISAC

(一) 在網路的世界中，無論是學術、政府及企業網路都易受到先進持續威脅 (Advanced Persistent Threat, 簡稱 APT)，面對不斷改變的網路攻擊模式，早期通報和預警功能是將災害降至最低的兩大關鍵，目前證券期貨相關周邊單位已建立跨市場資訊互換作業通報 (四方通報) 機制，對於影響證券期貨市場之重大事件會相互通報以為因應。

(二) 行政院國家資通安全會報為建立政府資通安全防護管理中心，推動國內相關機關建立「資訊分享與分析中心」(ISAC)，期能有效防範相關資安事件滋生，除建立政府資訊分享與分析中心(G-ISAC)外，目前已有經濟部電子商務資安通報服務中心(EC-CERT)，教育部學術資訊分享與分析中心(A-ISAC)及國家通訊傳播委員會資訊分享與分析中心(NCC-IASC)等已建立相關 ISAC 機制。

(三) G-ISAC 交換情報種類與資安類型

情報種類	事件類型
資安訊息	漏洞預警、攻擊活動預警、公告資訊、中繼站黑名單、資安事件處理結果統計資料、惡意程式網路偵測規則、特定 IP 詳細連線紀錄、每日病毒郵件紀錄、每日病毒郵件附檔、每日病毒郵件詳細資訊、IP 對應政府機關列表、所轄 IP、中繼站阻擋統計資料等
網頁攻擊	網頁置換、惡意留言、惡意網頁、釣魚網站等

資安預警	系統弱點、可疑連線、資訊洩漏、可疑程式、對外攻擊、網頁攻擊事件等
入侵攻擊	系統入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、社交工程攻擊、Spam、C&C、Bot 等
回饋	資安事件通報結果、錯誤通報、刪除情報、更新情報

圖表 3.2.2 G-ISAC 交換情報種類與資安類型

(四) 目前本公司已建置資訊安全監控中心 SOC，如有發現重大網路攻擊之資安事件，會立即通報其他周邊單位以為因應，但鑑於各周邊單位互通之資安資訊缺乏較完整機制，宜建置 ISAC 以強化各單位間之資安資訊之分享及通報作業，俾及早發現資安事件並採取預防措施，降低資安風險，並可作為未來建立證券期貨周邊單位或證券期貨市場資通安全防護管理中心之基礎。

第三節 小結

台灣市場於去年進入有價證券全面無實體時代，集保結算所身為證券市場後台作業中心，打造更安全、更可靠的資訊環境，是本公司應盡的責任，新版個資法已於今年10月1日正式生效，金融市場擁有許多個人基本資料，以本公司為例，現行接受證券商委託管理約有八百六十多萬位投資人的資料，本公司一直以來也以最高安全規格來維護這些資料的安全性，不斷探討資訊安全議題，了解最新發展趨勢，採用最新資訊安全技術與資訊安全管理新觀念與做法，以持續維持資訊安全的強度。

在投資人的個人資料保護方面，本公司規定資訊部門的人員，必須在有錄影監控與資安設備保護的工作專區內，進行個人資料電腦處理作業；業務部門與管理部門則必須在專用電腦上處理個人資料，專用電腦只限有權人員方能使用，並以資安設備保護。

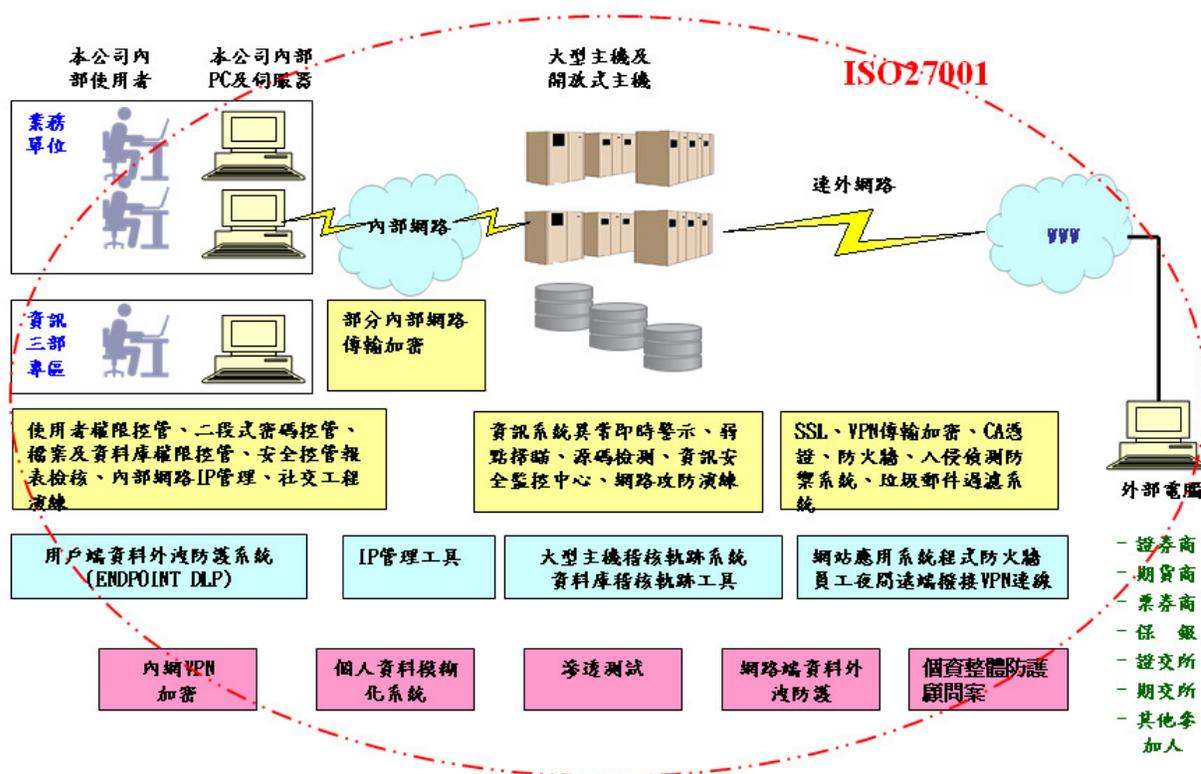
在個人資料保護制度方面，目前本公司已經獲經濟部同意，就本公司建置之個人資料管理系統（PIMS），以台灣個人資料保護與管理制度(TPIPAS)為標準進行驗證；預計明年年底前可順利通過。

在分享資安資訊方面，早期通報和預警功能將是將災害降至最低的兩大關鍵，本公司未來也會配合主管機關，著手建置證券期貨周邊單位的資訊分享與分析中心(ISAC)，以促進證券業間的資安資訊分享。

就集保結算所的實務經驗而言，做好資安管理需要幾個要素來共同配合：第一是一定要有高階管理者的支持，很幸運的，本公司的高階管理者十分重視資安並非常支持資安

相關的投資，第二是要了解資安最新趨勢，善用市場最新資安技術，第三是要持續加強員工的資安教育，深化員工的資安意識，最後是以規劃/執行/查核/行動 PDCA 循環，不斷精進資通安全管理系統。

落實資安管理，可防範企業「實質」及「無形商譽」的損害，而外界的資安威脅不斷的衍生及變化，惟有持續落實資安管理，方能有效解決外界資安威脅，確保投資人資料的安全，故資安管理可說是「永無止境」。



圖表 3.2.3 本公司資安整體防護示意圖

第五章 總結

本公司成立已逾 20 年，隨者業務不斷的成長及新種商品陸續增加，為滿足內外利害關係人(Stakeholder)的需求，同時配合資訊科技技術的演化與進步，集保的資訊系統也日益擴大及複雜，主要系統包括證券存託系統、庫存系統、票券結算交割系統、期貨結算系統及基金系統等，當然也建置了公文、人力資源、財務會計及 EIP 等內部支援系統。

民國一百年台灣證券市場全面實施證券無實體化後，本公司在證券後台作業的角色，也由結算、交割、帳簿劃撥及實體集中保管，轉為以結算、交割、帳簿劃撥為主，實體保管就只剩下下市櫃股票，因此也將庫存系統從大型主機轉置至成本較低之 X86 伺服器上，表面上看來，有人認為集保本業是從【倉儲業】轉為【資訊業】，但實際上對資訊系統而言，以提供的功能來看，並沒有太大的改變(本公司目前除存託及庫存系統外，票券、期貨及基金等資訊系統與證券無實體化較無相關)，只是因實體股票消失而全面以電子化方式儲存，對於大家心理面難免剛開始比較難適應，覺得電腦帳無法以實體再做比對，因此間接促使公司對於資訊品質的要求更勝以往，這是本研究案的起因。

【穩定、效率、安全】是集保資訊系統設定的目標，為達成此目標，集保資訊部門同仁從資訊系統的規劃、設計、建置及維運，皆以此為主軸。前述之重要系統都已根據相關之需求訂定量化之服務等級，足可滿足市場可預見之龐大交易量需求；至於未來的資訊發展策略，可從機房、網路、主機、儲存體及系統軟體等系統架構基礎工程(Infrastructure)、應用軟體與資訊安全等三大範疇加以說

明。

機房是所有資訊系統之建置基礎，目前本公司已擁有符合國際標準 TIA-942 近 Tier 4 主機房及異地備援機房(DR)各一座，主機房建置已超過 10 年，未來將逐步更換發電機、UPS 及空調等設備，惟宥於樓板高度及無法長時間停機，因此無法改建為冷熱通道隔離之環保新式機房，以符合 Green Grid 及 LEED 等標準，滿足 PUE 1.5 之節能減碳需求，將來若政策確定，可在證交所 105 年預計落成之板橋新建機房，重新建置本公司符合 TIA-942 Tier 4 及 Green Grid 及 LEED 等標準之下一代機房，以提供資訊系統更佳之營運基礎。

為滿足各種業務參加人與投資大眾需求，集保提供 Internet、ADSL、專線及四網合一 NGSDH 等不同網路連線方式，配備多樣且複雜之網路及安控設備，為便於維運管理及提升效率，未來將朝設備整合及網路拓樸優化方向做改善，另外逐漸汰換 ADSL 為四網合一 NGSDH 線路，而導入 IPv6 通信協定亦是未來策略重點。

應用系統是資訊的靈魂，程式人員撰寫程式就是賦予電腦生命，早期的程式因為功能單純且較無後續維護的觀念，程式人員常常各憑功力，使得軟體的品質無法掌握，後因為大型軟體的需求，往往需數百人協同開發，因此有了軟體工程的標準，期望軟體跟硬體的製造一般，能將各個模組就如同生產線上之零件，可作組裝檢驗，達成標準化及自動化之目標；本研究案試著就各項業務系統，從傳輸方式、安控方式、使用者對象、結算機制等進行整理歸類，同時亦以各系統提供外部單位之資料查詢內容為切入點，找出共通模組及相同資料，為後續系統的改善整合奠定基礎，達成軟體工程

【Reuse 多、Redo 少】的終極目標。

在本年新版個資法實施之前，本公司已依據電腦處理個資法要求，完成相關之資安佈署及制度，並已取得 ISO27001 之 ISMS 國際認證，配合新版個資法亦建置 WAF、DLP、專機專區及內網加密等強化機制，未來除維持此認證之有效性，並將取得 TPIPAS 個資管理系統認證，同時，配合主管單位建置 ISAC 資訊分享與分析中心。

【技術、程序、人員】是構成有效且完善資訊系統之三大要素，因此，除前述之各個技術構面外，本公司之 ISO9001、ISO27001 及異常處理手冊內所制定之標準作業程序亦是資訊作業必須時刻遵循之要件，而完整的異地備援及 BCP 例行性演練，更是確保業務不中斷之保證。

人是所有工作之核心，如何做好資訊人員之選才、訓才、用才及留才工作，是集保提供完善資訊服務及永續經營之不二法則。

參考文獻

1. 財團法人資訊工業策進會-臺灣集中保管結算所(Taiwan Depository & Clearing Corporation- TDCC)強化資訊系統因應重大災難之有效防禦評估與長期發展策略研究報告。
2. ANSI T1.413-1998 "Network and Customer Installation Interfaces - Asymmetric Digital Subscriber Line (ADSL) Metallic Interface." (American National Standards Institute 1998)。
3. *ITU-T Rec. G. 707/Y. 1322, Network node interface for the synchronous digital hierarchy (SDH).*, Geneva: International Telecommunications Union, 2007-01, retrieved 2010-11-03
4. *ITU-T Rec. G. 783, Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.*, Geneva: International Telecommunications Union, 2006-03, retrieved 2010-11-03
5. 100年12月行政院「網際網路通訊協定升級推動方案」。
6. 美國可用性研究中心2002年提出-網路關鍵物理基礎設施 NCPI (Network Critical Physical Infrastructure) 研究報告。
7. ASCII, <http://zh.wikipedia.org/wiki/ASCII>.
8. 邱菊梅(2002),「中文電腦缺字研究」,玄奘人文社會學院中國語文研究所碩士論文。
9. 余保倫、周智禾(2008),「中文字碼標準化及互轉機制之探討」,行政院主計處研究報告

10. 內政部戶政司，<http://www.ris.gov.tw>。
11. 財政部財稅資料中心，<http://www.fdc.gov.tw>。
12. 公路監理，<http://www.thb.gov.tw>。
13. 移民署，<http://www.immigration.gov.tw>。
14. 全字庫，<http://www.cns11643.gov.tw>
15. Unicode, <http://unicode.org/>
16. 余保倫(2006), 「中文數位化 Metadata 之探討」, 行政院主計處研究報告
17. 謝育平、吳政泓、項潔, 「可攜式字集資源-用以解決缺字問題」, 第三屆數位典藏技術研討會論文集, 2004年8月, 頁71~78
18. 王韋翔(2012), webMethods BPM 簡報, 怡康軟體股份有限公司。
19. 黃信嘉(2007), 「企業應用整合系統成功模式之研究-以某企業物流整合資訊系統為例」, 銘傳大學。
20. 何元榕(2004), 參加「企業應用整合(Enterprise Application Integration)技術」實習心得報告, 中華電信研究所。
21. 鄧國廷(2003), 「運用 EAI 作為提升企業資訊技術價值之研究」, 國立台灣科技大學。
22. 黃明乾, 我國大型製造業從事資訊系統轉型策略之個案研究, 國立中山大學資訊管理研究所碩士論文, 1997
23. 蔡志雄, 既存資訊系統移轉模式之研究, 世新大學資訊管理所碩士論文, 2004
24. 蔡春智, 使用者導向之企業資源規劃系統移轉方法, 東海大學工業工程學系碩士論文, 2000