第一章 緒論

本章主要的目的是要說明論文的著眼點，將分為五節，首先在 1.1 節中，將說明作此研究的動機，在瞭解研究動機後，於 1.2 節中進行此次研究的問題界定，在 1.3 節說明研究目的，在 1.4 節中說明研究方法，1.5 節則為研究架構。

1.1 研究動機

近年來，在各方大力倡導資訊科技所帶來的便利之情況下，許多的企業採用資訊科技來提升營運效率也變成一種因應時代變化的必要決策。在過去，企業向來以獨善其身的方式作為營運方針，但在現今強調亦敵亦友的「競合」關係中，也成為供應鏈中，一種新的現象。

在網際網路普及與蓬勃發展下，資訊的取得與傳遞變得更加便利，伴隨著資料庫與資料倉儲技術的成熟，資訊分享熱線也成為企業間競合關係的重要媒介。資訊分享熱線在資訊分享方面，可以作為企業夥伴間的資訊交換與交流，提升決策分析的準確度與減少資源的浪費。也可透過資訊分級制度，在競爭同業間，做資訊的分享，來達到資訊收集的最大效益，共創更進一步的產業環境。而從資訊安全的角度來看，資訊分享的傳遞過程，從以往單機的環境，轉為使用者可以透過網路來連線到遠端的伺服器，雖然提升了許多的營運效率，但是也隱藏了許多透過網路傳遞與接收所帶來的危險。因此網路安全性問題也成為資訊科技中，一項重要的課題。

資訊分享在帶來了透明與便利的互惠價值的同時，背後也被隨著不容忽視的安全性問題，因此如何在資訊分享、資訊分級與資訊安全間，取得最適當的平衡，是一項值得研究的課題。

對於四面環海的台灣而言，相較於全世界的漁業產量，台灣的年產量名列前茅，漁業產業每年都有幾千億的產值，在經濟上存在著舉足輕重的地位。漁業資訊的收集、分享與交換對於漁民或中央與地方行政管理單位而言都非常重要。以漁業署為例，目前所採取的方式是以書面的方式，根據各地方行政單位的回報進行統計與整理，每年定期出版裝訂成冊的漁業年報，以達到資訊分享的目的。

固然裝訂成冊的年報能夠讓使用者能夠瞭解漁業概況的資訊分享目的，在時間上，必須等待定期更新後的資訊；在空間上，資料必須取自於實體裝訂成冊的年報，在查詢上到受到限制。此時如果結合網際網路以及資料倉儲技術的特性，在時間及空間上，都可以有功能性的突破。

針對目前漁業署的三大異質性資料庫進行分析，結合資料倉儲以及網際網路的技術，突破傳統書面式年報所帶來的不便。而除了必須整合三大異質性資料庫以外，由於漁業署三大異質性資料庫的內容，大部分資料都屬於機密性較高的文件。對於所建立的資訊分享熱線之前端的檔案轉移服務與後端的存取控制也都是相當重要的環節。近年來，由於網際網路普及率越來越高，電子商務的經營模式也足見被世人所接受，也證明了資訊安全的觀念也越來越受到重視。有許多的資訊安全技術被提出來，除了增加了更多的安全性以外，也大幅的提升使用上的效率。因此希望能夠藉由最新的資訊安全技術，與三大異質性資料庫的資料倉儲，結合，作為資料倉儲的存取控制服務。

在漁業署中，署內組織的層級性，與內部檔案的機密性有部分的不對稱關係，意思是層級最高的長官不一定有權限存取機密性最高的檔案。因此，如果再進行資料倉儲的資訊分級需求規劃時，則不能夠利用組織層級來作為存取控制的權限層級。如果能夠利用在漁業署所擔任的角色來設定權限機制，將能夠大幅減低資訊分級規劃的時間。

1.2 問題界定

一直以來，我國漁船漁業相關人員與漁業行政單位之間的互動相當頻繁，但資訊分享則只能透過每一週期的定期漁業公報來傳遞。以漁業署為例，署內三大異質資料庫的整合，透過資料倉儲的建置，建立了漁業資訊分享熱線(Fishery Information Sharing Hotline, FISH)，成為了漁業資訊的線上資訊分享平臺。

線上資訊平台必須透過資料倉儲技術建立，而資料倉儲在建立的過程中，一開始就必須透過原始資料庫的資料來完成。在資訊分享平台建構完成後，定期透過資料庫軟體的資料轉換服務，將原始資料庫的資料，轉移到資料倉儲。這道程序就必須透過特定的連線方式來進行。

而資訊分享的實現必須以資訊安全為前提，尤其在面對機密性相對較高的漁業資訊，以及各方使用者的驗證工作與權限劃分之服務，也帶來了許多複雜而又不可忽視的存取權限安全控管機制之問題。因此，如何建立一套符合漁業資訊分享熱線需求的使用者存取機制與資訊分級權限控管制度，並改善因大量使用者登入資料倉儲系統存取資訊造成系統身份驗證效能降低的現象。

本研究主要針對三大異質性資料庫的整合，規劃漁業資料倉儲，進而建立漁業資訊分享熱線的前端與後端兩大服務作為此次研究的主要課題。

第一個服務為建構資料倉儲的前端的檔案轉移服務，目的在於將資料從異質性資料庫轉移到資料倉儲的檔案轉換服務。主要設計目標在網際網路的作業平台上，能夠藉由簡單的使用介面，建立自動化的轉移服務。為了突破作業平台的使用限制，本研究檔案轉移服務則利用爪哇程式語言進行實作。

第二個服務為存取控制服務，當中包含了認證、授權以及審計。利用存取控制服務的技術，針對三大異質性資料庫的資訊分級需求，利用 Cognos 中的 Access Manager 進行實作，建立漁業資訊分享熱線的權限控管機制。

1.3 研究目的

漁業資訊分享熱線權限控管機制主要是建構在線上分析處理（On Line Analytical Processing, OLAP）之前端使用者介面上。透過植基於角色式存取機制（Role-Based Access Control, RBAC）作為存取機制，再配合輕量級名錄存取協定（Lightweight Directory Access Protocol, LDAP）的名錄伺服器(Directory Server)建立此次之權限控管機制。漁業資訊分享控管機制是以密碼(Password Authentication)的模式來定義合法用戶端如何透過網路得到身份驗證的服務。名錄伺服器則是作為驗證使用者身份的後端資料庫，負責提供漁業資訊分享控管機制驗證合法使用者的依據。

透過上述的技術，將網路傳遞與資料倉儲的技術整合，結合身份驗證的機制以名錄伺服器的應用，以滿足不同資訊分享的需求。

本研究目的將針對以下問題提出解決辦法：

1. 實現漁業資訊分享熱線之使用者建立不同等級之存取權限。
2. 簡化漁業資訊分享熱線之管理者權限控管系統維護之工作內容。
3. 提升系統使用者登入系統驗證與存取之效率。

1.4 研究方法

本研究將從制度面、技術面、管理面與應用面四個面向來建立漁業資訊分享熱線之權限控管機制。

- 制度面：漁業資訊分享熱線的建構主要是透過三大異質性資料庫整合而成，而其資料庫原本各為不同使用者進行不同權限等級的存取，因此必須將原有的存取權限制度保留並沿用到整合後的漁業資訊分享熱線。
- 技術面：透過身份驗證、存取授權與開放審計等安全手法來完成漁業資訊分享熱線。
- 管理面：透過驗證與存取機制來提升系統維護者的管理效率。
- 應用面：利用已完成使用者分級存取的漁業資訊分享熱線，以實例說明各層級使用者的存取權限與資訊內容。

本論文的研究流程如圖 1.2 所示：

1. 訪談：此次研究的合作對象為漁業署，使用者主要為漁業署內部人員、各地方單位人員，經過訪談後，瞭解與釐清漁業資訊分享熱線之使用者的權限與功能需求。
2. 問題界定：歸納使用者的層級與存取權限。
3. 文獻回顧：參考過出發表的文章，找出適合的解決方法與模式。
4. 系統架構：藉由評估後，適當的方法來進行權限控管機制的架構設計。
5. 系統測試與操作：完成系統的建置後，則進行系統的操作與測試，進而瞭解實作與規劃前後是否有不符合。

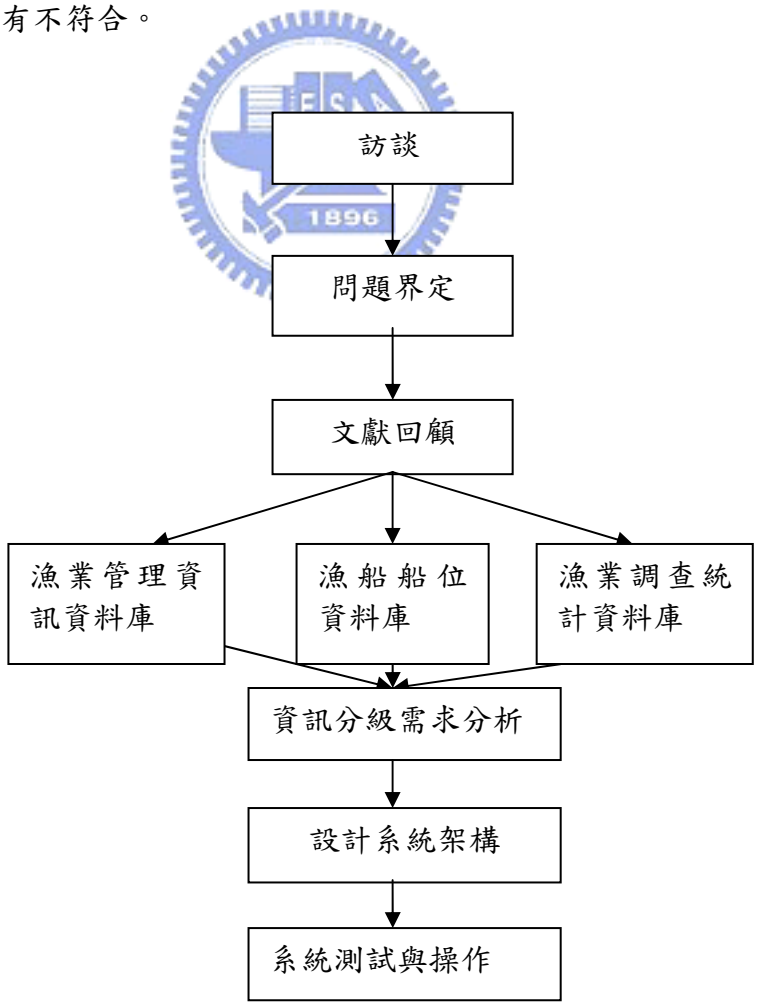


圖 1.2 研究方法與步驟

1.5 研究架構

本論文的研究架構編排如下：

緒論—說明本論文之研究動機、主題、方法、目的與背景等。

第一章　：文獻回顧—說明本論文所引用的機制與模式，包含身份驗證與名錄服務等。

第二章　：漁業資訊分享熱線之架構—介紹漁業資訊分享熱線之檔案轉移服務以及權限控管機制建立之規劃。

第三章　：檔案轉移服務系統之建置—說明檔案轉移服務系統的建置過程以及操作流程介紹。

第四章　：權限控管系統之建置--說明權限控管系統的建置過程以及操作流程介紹。

第五章　:權限開放審計之建置—說明利用 SQL server 的檔案轉換服務來建立查詢實作。

第六章　：結論及未來研究方向

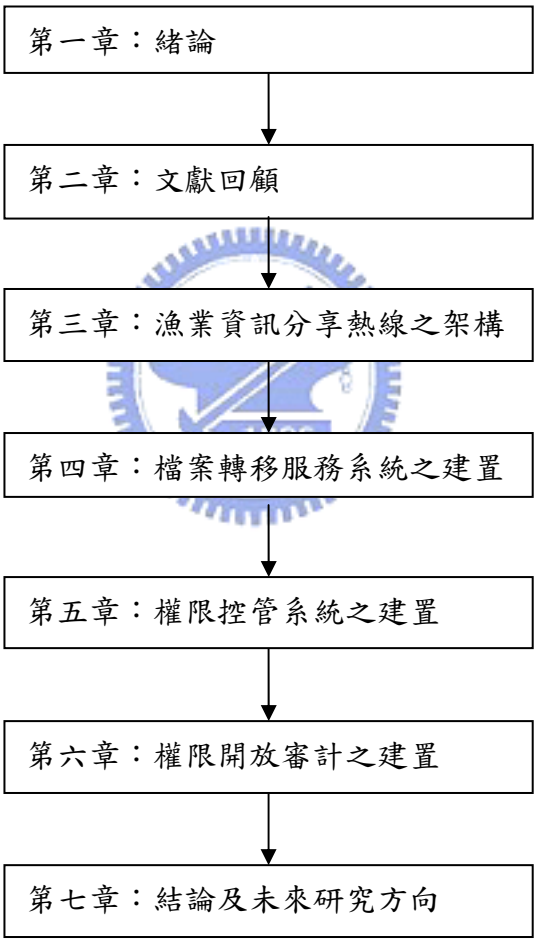


圖 1.3 研究架構

第二章 文獻回顧

本研究主要的目的是為了建構漁業資訊分享熱線中，前端的檔案轉移服務以及後端存取控制的部分。在文獻回顧中，將此兩部分所涉及的相關技術。在本章分成六小節來加以介紹，第 2.1 節介紹檔案轉移服務，第 2.2 節主要說明線上分析處理系統，第 2.3 節主要說明存取控制。

2.1 檔案轉移服務

檔案轉移服務所使用的協定為檔案傳輸協定（File Transfer Protocol,FTP）[3]，是 TCP/IP 的標準機制，主要目的是將一台電腦的檔案複製到另外一台電腦。在看似簡單的傳輸過程中，有許多問題仍須處理。如檔案的資料結構與命名方式等等，不過這些狀況在 FTP 中都已被克服。在 2.1.1 節說明服務模式。2..1.2 節說明 FTP 原理。2.1.3 節利用範例進行說明。

2.1.1 服務模式

針對網際網路之檔案資訊交換而言，最常見的傳遞模式除了 Http 模式之外；另一種技術就是檔案轉移協定（File Transfer Protocol,FTP）。透過 FTP 所提供對遠端伺服器的上傳與下載指令，可以迅速地將異端的檔案分享與交流。而在 Http 協定所整合功能的便利性高於 FTP 建制指令。但在簡易的 Clinet/Server 架構中，除了 Clinet 端繁複的流程操作，並且在機密性的文件上，還需建立使用者認證機制，略顯出 Http 協定在連結操作上的繁瑣[8]。

FTP 的用戶端有三個模組：使用者介面、用戶端控制程式及用戶端資料傳送程式。FTP 的伺服端有二個模組：伺服端控制程式及伺服端資料傳送程式。FTP 使用的是兩個公認阜，阜 21 做控制連線用，阜 20 做資料連線用，如圖 2.1 所示。

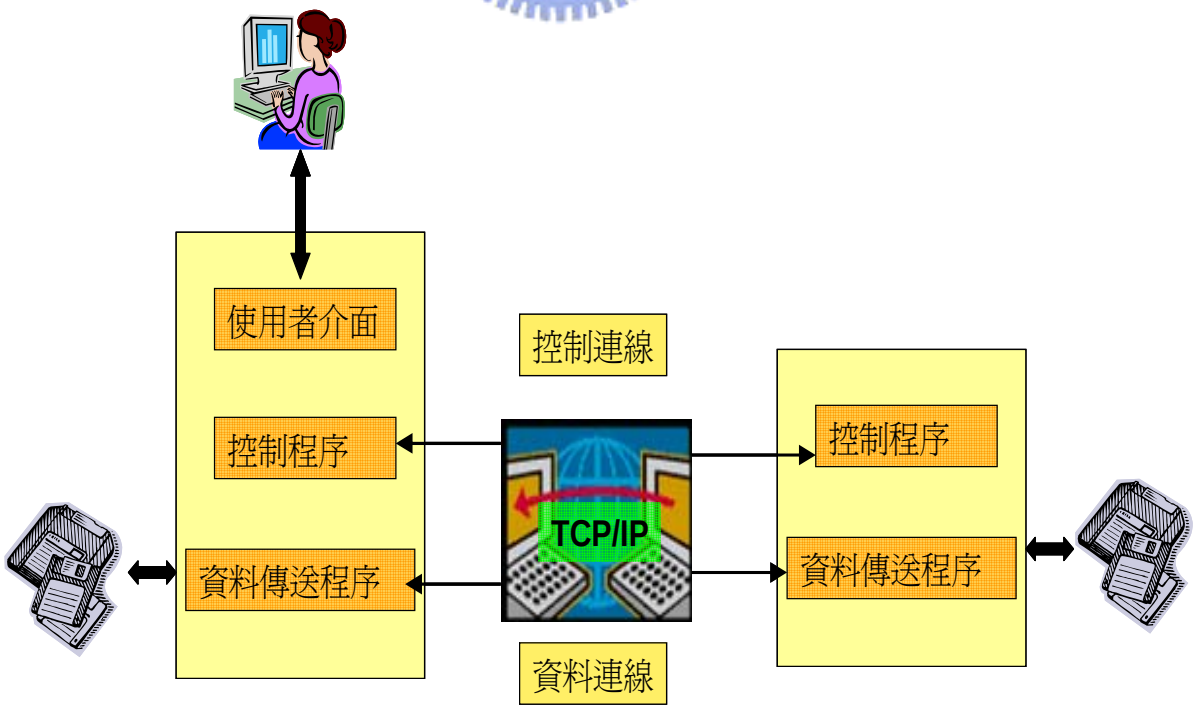


圖 2.1　FTP 架構圖[8]

2.1.2 FTP 原理介紹

FTP 運作的過程主要為連線（Connection）、通訊(Communication)、命令處理(Command Processing)、檔案傳輸(File Transfer)四個程式，下面將分別說明：

連線：首先伺服端的伺服程式會開啟 21 埠，等來使用者連線。當接收到使用者短暫埠發出 PORT 的命令後，伺服程式會開啟 20 埠建立資料連線，如圖 2.2 所示。

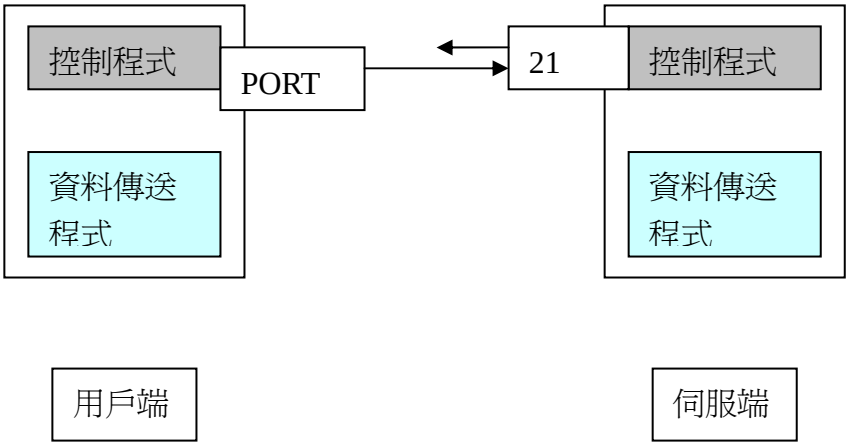


圖 2.2 連線程式[8]

通訊:在控制連線的通訊部分，FTP 使用的是 NVT ASCII 子元組。一個命令或回應都只是一短行字元，每行皆以二個行末端記號作結束，如圖 2.3 所示。

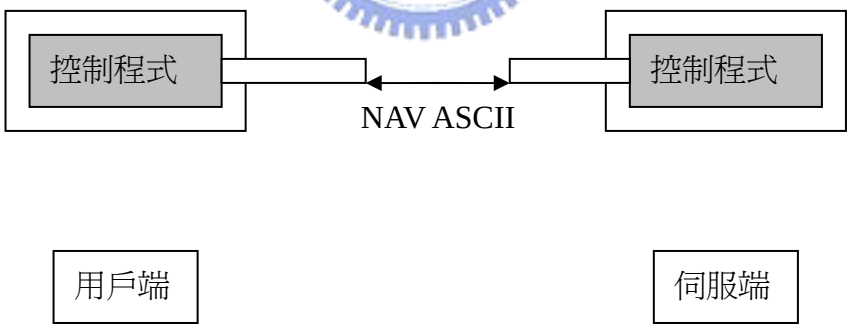


圖 2.3 控制連線通訊程式[8]

另外，在資料連線通訊部分，由於其目的是來傳送檔案，因此面對兩個系統不同性質的問題，需要透過定義通訊屬性來處理，分別包含檔案種類、資料結構及傳輸模式。

命令處理：FTP 使用控制連線來建立用戶端控制程式與伺服端控制程式的通訊。通訊期間，命令從用戶端送到伺服端，而回應由伺服端送到用戶端。

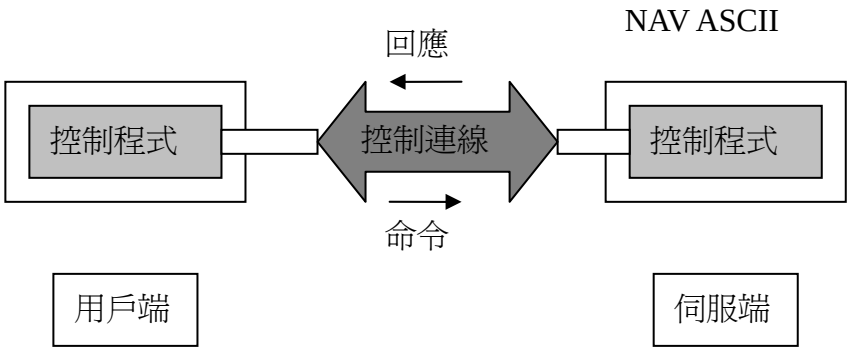


圖 2.4 命令處理程式[8]

檔案傳輸：檔案傳輸在資料連線上進行，由控制連線上所送出的命令所控制。檔案傳輸有三個動作，分別為：

收檔：檔案從伺服端複製到用戶端。由 RETR 命令來執行。

存檔：檔案從用戶端送到伺服端。由 STOR 命令來執行。

接收目錄：把資料夾或檔案名稱列表從伺服端送到用戶端。由 LIST 命令來執行。

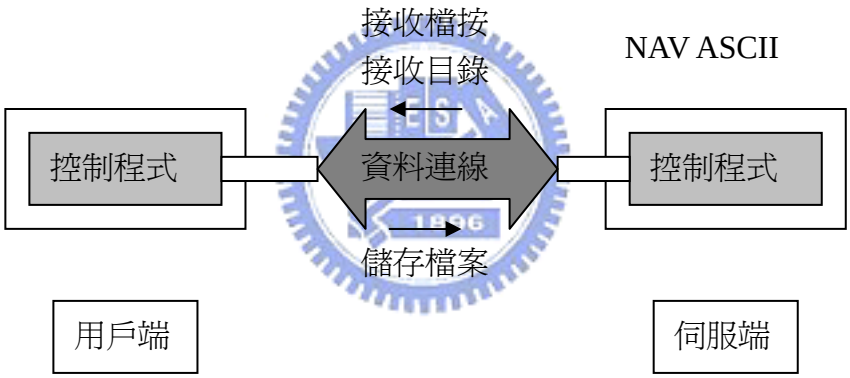


圖 2.5 檔案傳輸[8]

2.1.3 範例說明

以下之步驟將說明 FTP 的收檔過程，其過程如圖 2.6 所示。

1. 控制連線以 21 阜號建立後，FTP 伺服器送 220 的回應給用戶端。
2. 用戶端送 USER 命令。
3. 伺服端回應 331 代號(使用者名字正常，需要密碼）
4. 用戶端送出 PASS 命令。
5. 伺服端回 230(使用者登錄正常）
6. 用戶端以短暫阜做一個被動開啟以建立資料連線，透過控制連線送出 PORT 命令，將此短暫阜號送給伺服端。
7. 伺服器建立一條以 20 阜號與從用戶端短暫阜的資料連線，伺服器送出 150 回應。
8. 用戶端送出 LIST 訊息。
9. 伺服端回應 125 代碼且開啟資料連線。
10. 伺服器把檔案名稱或資料夾名稱，以檔案方式藉資料連線送出，當送出後伺服器

以控制連線回應 226 代號。

11. 用戶端下 QUIT 命令。
12. 伺服端收到 QUIT 命令後，回應 221 代號，並關閉連線。

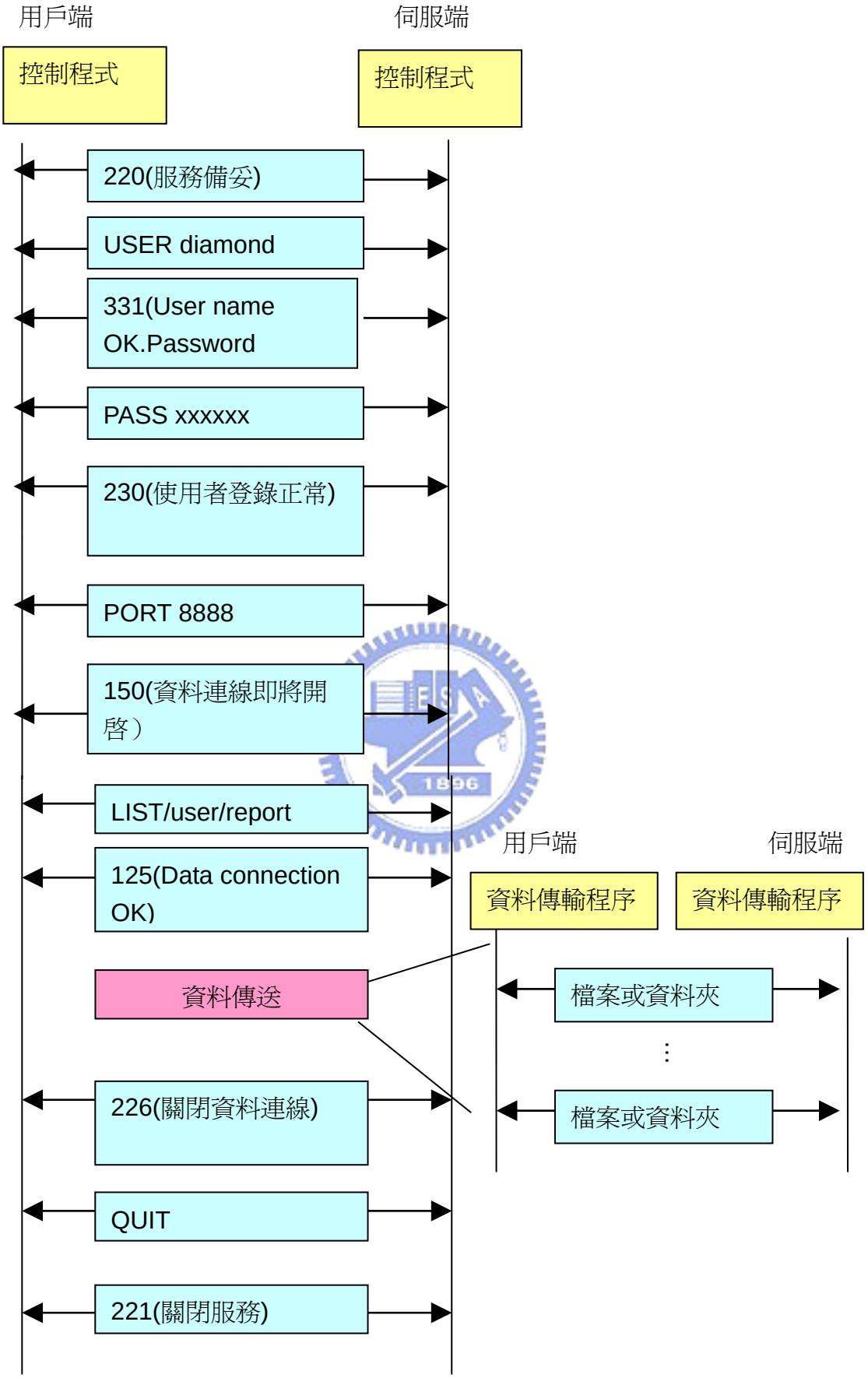


圖 2.6　FTP 範例流程[8]

2.2 線上分析處理系統

線上分析處理系統(On Line Analytical Processing, OLAP)[9]是一項能從現存的資料中，組合出具有商業價值情報的一種分析技術。線上分析處理系統以資料倉儲中的多維度商業資料為基礎，進而呈現不同邏輯性的分析資料。而這些經過排列與維度轉換後的資料與原本存在於資料倉儲的資料是相互獨立的，無論線上分析處理系統的資料如何的進行 OLAP 十項操作，如上捲、下挖、切片與切丁等等，都不會影響儲存於資料倉儲原始資料的獨立性。

以分析的角度來看企業的本質也屬於多維度，因此一位分析家在對於不論是企業內部或外部的分析，其分析的概念轉化為線上分析處理系統時，也會是多維度的模式。而目前多維度架構的線上分析處理系統也已經提供使用者能夠容易想像與理解概念化商業資料。

商業資料是一種多維度的資料，除了環環相扣外且通常都是具有層級性的。而維度本身與層級性也有很大的關係，如縣市、鄉鎮縣市、區等，時間維度亦然，不過時間維度具有標準化的層級維度，如年、季、月、日、時等。

線上分析處理系統的資料皆儲存於矩陣中[5]，這些矩陣皆是邏輯化的商業維度。例如圖 2.7 顯示銷售資料的三個維度，而型態的顯示方式有稱為超方體(Cube)。

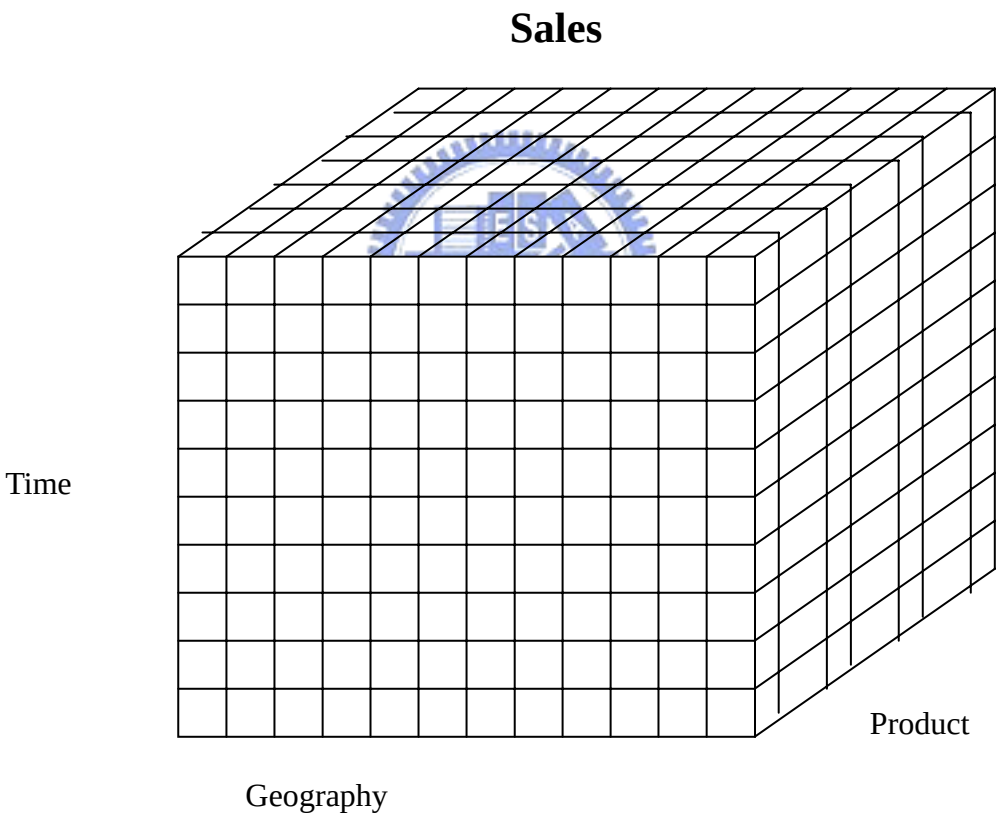


圖 2.7 超方體

2.3 存取控制

資訊安全的議題，在近來由於網際網路以及電子商務的蓬勃發展而備受重視，特別是當企業的資訊資源藉由網際網路來增加便利性的同時，企業資訊與系統資源的權限控管之安全問題即成為企業所關注的重要課題。

當使用者在通過系統的身份驗證取得相對應的驗證機制後，系統必須決定該名使用者可以獲得此服務系統所提供的服務與資源，以及這些資源的使用權限，並以政策與記錄的方式來規範使用權限資訊的機制，即為存取控制(Access Control)。在 2.3.1 節中說明身分認證。在 2.3.2 節中說明授權服務。在 2.3.3 節中說明權限開放審計。

2.3.1 身份認證

當要進入一個不公開的環境或者是使用設備時，會先透過許多的方法進行身份的鑑別，進而確認該使用者是否擁有該許可權。而在現實生活中，有許多的方法可以進行身份的鑑別，如長相、識別證、鑰匙和密碼等等。隨著科技的進步以及網路的普及，這世界也產生了另外一個無遠弗屆的網路空間，方便了許多資料與訊息的傳遞與交流。但是如何進行身份的鑑別，確認資料傳到擁有權限的使用者，因而產生了網路世界的身份驗證（Authentication）。

在 2.3.1.1 節中說明驗證需求。在 2.3.1.2 節說明驗證原件。在 2.3.1.3 節說明驗證方式。在 2.3.1.4 節說明驗證型態。在 2.3.1.5 節說明多頭狗驗證協定。

2.3.1.1 驗證需求

在實際生活中，經常會有不肖人士透過許多方式來盜用或偽造身份證的案例，進而取得非法的利益。同樣地，在網路環境中，類似的情況仍會層出不窮。以下將舉出幾點在網路上可能發生的情況，並說明為何在網路上有驗證之需求[1]：

1. 假冒(Masquerade)：第三者可以假造出某人的電腦 IP 位址所發出的封包傳送給欲攻擊的電腦，來擾亂正常連線。
2. 重送(Replay)：第三者可以藉由截取先前所傳送的資料，在後來的連線過程中又重送該資料使接收端產生混亂。
3. 修改內容(Content Modification)：第三者可以對網路上截取到的資料作修改，使資料失去正確性。
4. 修改次序(Sequence Modification)：第三者可以截取到資料後，搞亂傳送資料的先後次序，造成接收端的混亂。

否認(Repudiation)：對於傳送一些關鍵敏感的資料時，如果不做資料保密的驗證，則收送雙方將來可能會發生否認曾經送出或接收該資料的情況。

2.3.1.2 驗證元件

無論在何種系統，基本身份驗證元件應包含驗證的個體（使用者）、證明身份的工具（密碼）、驗證機制、管理的方式及系統擁有者等五種部分。說明如下：

1. 驗證的個體：該使用者為一欲登入系統，使用系統資源者。
2. 證明身份的工具：可以是一種密碼、金匙、生物特徵或含有證明身份的卡片等。
3. 驗證機制：為一驗證用者所提出證明工具的真偽之機制，在不同系統有不同的機制。

4. 管理的方式：將身份驗證機制驗證的結果送到此部分，由此來處理後續的動作，例如，產生一權杖(Token)、賦予其存取資源的權限等等。系統擁有者：有系統管理者的權限，可設定相關驗證原則，決定使用者帳號等功能。

2.3.1.3 驗證方式

隨著電腦網路的蓬勃發展，多種不同的身份驗證方法提供不同的安全等級。而目前較常用的身份驗證機制有以下各種方式[10][13]：密碼（Passwords）、標記（Tokens）、智慧卡（Smart Cards）、數位簽章（Digital Certificate）、生物辨識法(Biometrics)。其中，密碼是現今最通用的身份驗證方式，透過輸入使用者名稱及所設定的密碼來證明自己的身份。而系統藉由驗證使用者所提出名稱及密碼，與系統預先儲存的使用者資料比對來執行身份驗證工作。其優點是能完全以軟體實現且不需額外硬體支援，名稱及密碼透過加密後易於在網路中使用。其缺點是明文的名稱及密碼在網路上傳輸易被竊取偷用、易受重送攻擊、易受密碼猜測法攻擊、無效的密碼管理及控制、使用者缺乏警覺性及訓練以及易被木馬程式竊取密碼。

2.3.1.4 驗證型態

網路上的資料傳輸，幾乎都是以明文的方式傳送。因此，當一個使用者要求登入某台主機或使用其提供的服務時，其密碼很容易就會被第三者所竊得，侵入者只要在使用者及伺服器之間攔截網路上傳送的資料封包就可以輕易的偷取使用者的密碼。侵入者甚至可以在伺服器與伺服器中間線路竊聽這些以明文傳送的資料封包，直接或間接地竊取更多的資訊。因此許許多多的驗證方式提出，以型態類來看，大致是下列三種基本驗證型態[6]。

單向驗證(One Way Authentication)：這是最簡單的驗證方式，用戶端只需提供帳號和密碼給伺服端作存取確認，伺服端確認後就允許用戶端的登入。

雙向驗證(Two Way Authentication)：此方式為雙方相互驗證，雙方必須要提供帳號和密碼給對方才能通過驗證。不同於單向驗證，雙向驗證的用戶端還需要驗證伺服器的身份，如此一來用戶端就必須維護各伺服器所對應的帳號。

公正的第三方驗證(Trusted Third-party Authentication)：這也是一種通訊雙方相互驗證的方式，不過在驗證的過程中，必須透過一個雙方都能信任的公正第三者(Trusted Third Party)。在兩端連線之前，必須先通過公正第三者的驗證，然後才能互相交換金匙進行連線。其中最著名的例子就是多頭狗(Kerberos)驗證協定。

2.3.1.5 多頭狗驗證協定

遨遊於網際網路的過程中，其實有相當多的協定並沒有提供足夠安全的保護。目前也存在著許多破解與攔截密碼封包的軟體，因此在網路上傳遞未加密的密碼相當危險[6]。

多頭狗驗證協定主要是以 Needham and Schroeder 認證協定為基礎，目前在網路上被視為安全認證標準之一。它透過密碼學中安全金匙的應用提供客戶端與伺服端嚴謹的認證過程。利用嚴謹的加密技術，代替使用者的身份，而不需要傳送使用者的身份資料，使客戶端或伺服端能夠確保其身份能夠安全地通過網際網路，連線到另一端達到認證身份的目的。透過票券保證(Ticket Granting)[6]的技術，利用時間郵戳(Timestamps)來省去使用者利用相同身份重複登入的程序。

執行的流程如圖 2.8 所示。

- 步驟 1：使用者第一次登入時，連線到認證伺服器(Authentication Server)提出票券的請求。

- 步驟 2：認證伺服器回傳票券，此票券計錄用戶端的資料，還有與票券伺服器溝通的安全金匙。
- 步驟 3：利用安全金匙與票券伺服器進行連線。
- 步驟 4：票券伺服器在收到使用者安全金匙連線後，會回傳一份已加密的另外一張票券，票券中也包含了另一組新的安全金匙。
- 步驟 5：使用者可以利用舊的安全金匙解開新的安全金匙，並將新的安全金匙與新的票券一併送到系統伺服器。
- 步驟 6：系統伺服器在收到新的金匙與票券後，會驗證使用者身份，開啟使用者的使用權限。

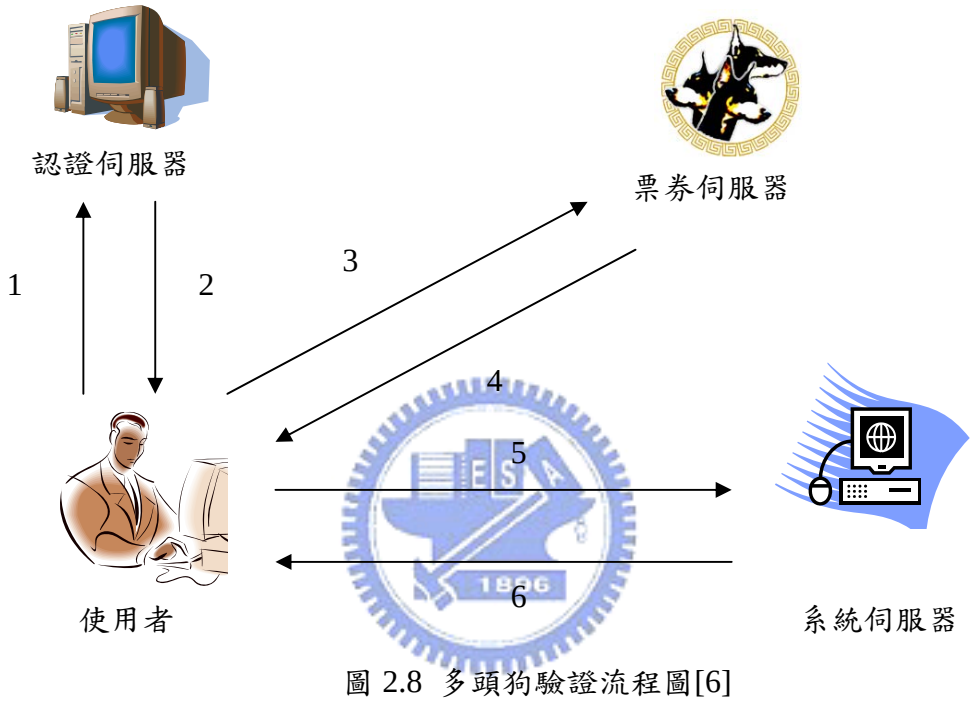


圖 2.8 多頭狗驗證流程圖[6]

2.3.2 授權服務

授權服務的功能主要是利用目錄服務的功能將使用者的身份資料以及其存取權限進行建檔並存放。接下來則針對以建立的身份進行存取權限的設定與管理。而在存取控制的部分，經過技術的演進，目前較普遍被採用的方式則是植基於角色式存取控制。在以下的內容，2.3.2.1 節會先說明名錄服務的功能，2.3.2.2 節則介紹輕量級名錄存取協定，在 2.3.2.3 節說明植基於角色式存取控制。

2.3.2.1 名錄服務

是一種資料儲存的結構與擷取的協定。也就是說名錄服務就像是一般的電話簿或是小型的資料庫所提共的資訊，而欲查詢的資料內容是放在網路上，可透過網際網路提供給全球使用者或是企業內部網路。提供企業內部相關人員查詢，使用者只需透過標準介面與語法來取得資訊。

名錄服務可視為一種特殊的資料庫，此資料庫存放的資料內容主要是在提供分散式系統中的其他應用程式或服務使用。利用名錄服務技術，將各式各樣的資料與資源做更具結構性的命名、說明、搜尋、存取與保護等。

2.4.2.2 輕量級名錄存取協定

隨著網路目錄服務的使用日漸普及，使用這套協定的機會也隨之增加。Lightweight Directory Access Protocol 的用途是對於網路目錄（例如 ND5，X.500，或 Active Directory）提出簡單的請求[15]。LDAP 的請求包括取得名字，位置，電話號碼，以及電子郵件位置等資訊。許多 WEB 瀏覽器（包括 Navigator 和 Internet Explorer）之中都包含了 LDAP 客戶程式，因此可以向目錄服務伺服器請求資訊[16]。輕量級名錄存取協定之所以被視為輕量級乃是因為他省略了 X.500 上許多不常用的操作，且能在「TCP/IP」上實作出名錄服務系統，提供用戶標準的名錄服務又具有與 X.500 名錄伺服器溝通的能力。而自從有支援輕量級名錄存取協定的資料庫後，輕量級名錄存取協定就不單單是閘道而是一個完整的名錄服務。

2.4.2.3 植基於角色式存取控制（Role-based Access Control, RBAC）

在說明植基於角色式存取控制之前，必須先介紹兩種存取控制，第一種是認定型存取控制(DISCRETIONARY ACCESS CONTROL, DAC)，此為系統維護者可以根據需求，自由設定授予不同人不同的權限，而並不會影響到其他使用者的權限。第二種為強制式存取控制(MANDATORY ACCESS CONTROL, MAC)，系統管理者會先對資料進行安全層級的區分，再對使用者設定其安全性權限，使用者本身不能夠對於其權限進行修改，透過此方式來限制使用者進入無權限的區域。

而在經過改良後，才產生了第三種存取控制，植基於角色式存取控制。植基於角色式存取控制[11]中是以角色來判斷其存取權限，系統管理者必須設定每個角色所能使用的系統資源及其使用資源的權限;每位使用者可屬於一個以上的角色，使用者只要屬於某個角色便能獲得這個角色所能存取的資源權限。其目的主要是由於一個使用者在不同的場合或時間點上可能會扮演不同的角色，另外，同樣的角色也會有不同的人來扮演，透過角色作為存取控制的判斷，可以避免上述之問題。植基於角色式存取控制而在 1990 年代被證實是能夠在大型的企業系統中管理與執行資訊安全的一項資訊技術。其基本元件包含了使用者（User）、角色(Role)、權限(Permission)及職位期間(Session)如圖 2.9 所示。使用者是代表真實環境欲執行或存取系統的人，每位使用者可分派給多種角色且同一角色也可由多人擔任;角色則是指組織團體中的某個角色，可視為權限的集合;權限則包含了系統操作、資源存取等;職位期間即為角色執行期，是使用者被指派為一個角色在執行或存取系統資源時所建立的，執行期包含了使用者使用中的角色集合以供使用者選擇所需的角色。

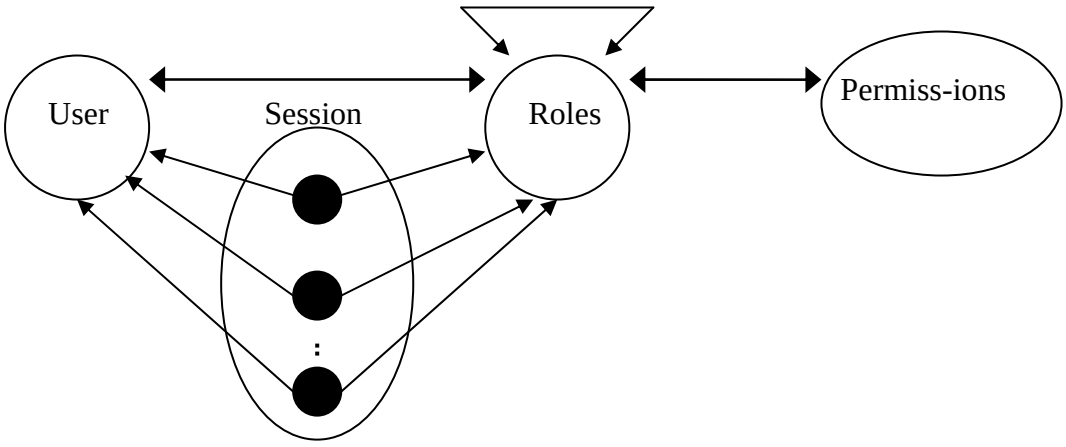


圖 2.9　RBAC 架構[11]

2.3.3 權限開放審計

資料及資訊的安全對於企業而言是非常重要的，因為大部分與電腦有關的犯罪行為都是透過一種簡單的進入方式，進而對於檔案作修改或使用的動作。如果在進行管理或是策略上的決策時，是根據這些被修改的資料的話，後果將不堪設想。所以資料的完整性將仰賴資料安全。另外，資料對於組織而言變得越來越重要，而特別是一些機密性高的文件，更不能輕易被其它人存取，尤其是競爭者。其次，新興的法律規定私密性資料的保護規範，如Gramm-Leach-Bliley Act(GLBA)等。

因此，對於存放於電腦中，而不時將會被存取的資料來說，這些資料是需要被受到監視的，監視的工作則透過審查員(Auditor)[10]來完成。資訊系統審查是一項跨領域的學科(discipline)，從網域外部到內部區域網路包含了傳統審查，資訊系統管理，行為科學以及電腦科學。

在安全審查的領域中包含了許多層面，如 IP 掃瞄與 Port 掃瞄、弱點掃瞄(Vulnerabilities Scan)、網路架構審查(Network Infrastructure Audit)、系統政策(System Policies)、遠端存取審查(Remote Access Audit)和密碼審查(Password Audit)[7]等。

1. 在 IP 掃瞄中，透過掃瞄軟體對於欲從外部的網路連進內部網域的所有 IP 進行掃瞄，而掃瞄軟體會自動將已知的 IP，列出其所屬的單位，方便進行辨識。
2. 弱點掃瞄則是將 IP 掃瞄的結果載入到另外一個更進階的掃瞄軟體，其會自動詳細的列出某連線的狀態、協訂和服務，監看每一個有可能對於安全規則有違反的連線。
3. 網路架構審查的第一步對外是透過防火牆，利用管理者所建立的規則來進行封包的過濾。對內則是監控所有有關的網路設備進行監控，如路由器、伺服器及調節器等。
4. 系統政策則是與電腦系統有關的一些政策文件，規定如電腦、軟體使用、電腦設備的採購、網路郵件等。
5. 遠端存取審查的目的是透過每一條遠端存取連線去審查有可能的漏洞以及存取使用者的數量。
6. 密碼審查主要是透過使用者帳號所對應的密碼來進行身份認證，進行審查動作。而為避免被使用暴力解碼或密碼目錄的攻擊，將設定每一組帳號在一段時間內的連續錯誤不能超過三次。

另外，當載入暫存區被使用時，其在載入時的程序應該要盡可能的減少，愈少的程序也表示有會影響資料完整性的可能性越低[13]。當然，此區必須受到權限存取的限制，建立查核涉及有關資料存取流程的程序，每一個存取的流程步驟都必須要被紀錄，包含流程號碼、主要欄位的總數等等。除此之外，記錄每一筆記錄也可以達到資料的獨立安全評估。

第三章 漁業資訊分享熱線架構

本章主要是介紹漁業資訊分享熱線之前端即為檔案轉移服務，以及後端之權限控管機制的架構，在 3.1 節則介紹資料倉儲的架構。在 3.2 節則介紹檔案轉移服務之部分，利用 JAVA 技術來開發檔案轉移服務的架構。在 3.3 節則介紹資訊分享熱線針對資料倉儲架構的資訊分級需求分析。在 3.4 節則介紹權限控管系統的設計架構。

3.1 資料倉儲架構

透過漁業署的三大統計資料庫:漁業調查統計資料庫、漁船船位資訊資料庫以及漁業管理資訊資料庫來建置「漁業資訊分享熱線」(Fishery Information Sharing Hotline , FISH)。漁業資訊分享熱線的建置包含三大流程，即資料輸入、資料轉換服務(Data Transformation Service , DTS)以及資料輸出。其做法是將三大統計資料庫的資料透過檔案轉換服務(File Transformation Service , FTS)轉到資料倉儲(Data Warehouse , DW)所在的伺服器上，在透過資料轉換服務將資料轉入資料倉儲中，接著將資料倉儲中的資料輸出以進行線上分析處理(On-Line Analytical Processing , OLAP)與圖形化的呈現，其架構如圖 3.1 所示。

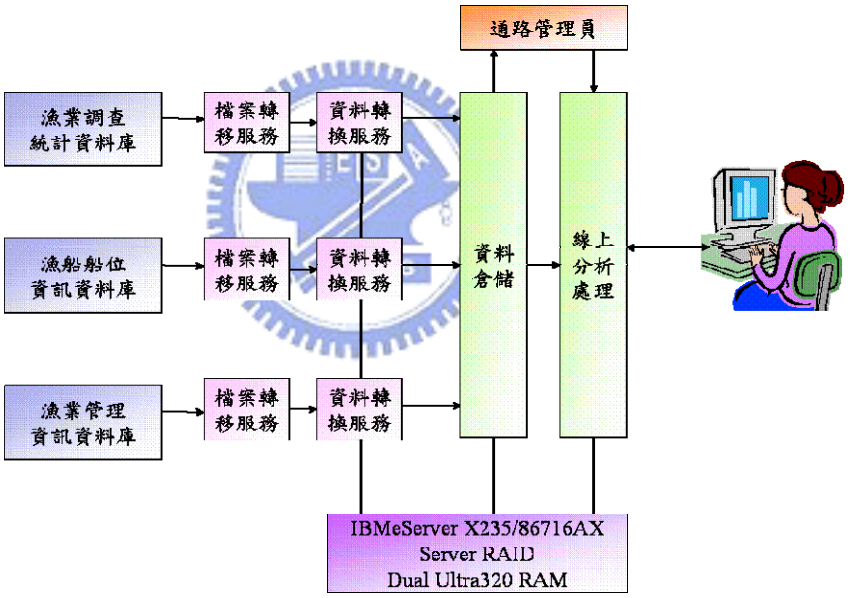


圖 3.1 漁業資訊分享熱線架構[5]

為了提高漁業單位在行政管理上的執行效率與進行相關資訊的加值應用，於是建構了「漁業業務情報網」(Fishery Business Intelligence)以方便漁業單管理單位進行後續決策。「漁業業務情報網」(Fishery Business Intelligence)主要是由「漁業資訊分享熱線」(FISH)與「漁業資訊偵查器」(Vessel Information Monitor ,VIM)所組成，其架構如圖 3.2 所示。

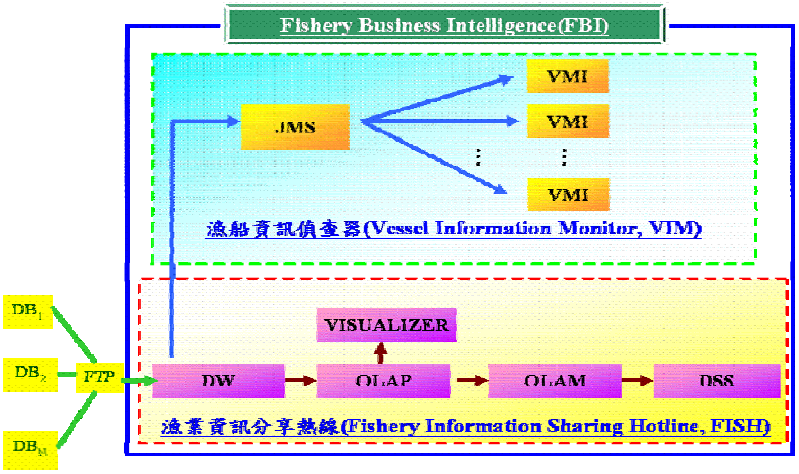


圖 3.2 漁業業務情報網[5]

3.2 檔案轉移服務架構

透過 Internet 傳輸資料的方式中，Socket 的觀念讓網路連線可視為另一種資料流，在建立 Socket 連線後，將寫入 socket 的資料傳送至遠端，簡易的 Socket 技術即廣泛運用到網路的層面上。

在檔案傳輸協定系統內，ServerSocket 類別為伺服器端所建立的 Socket，伺服器以 ServerSocket()建構式在主機內所提供的特定通訊埠，建立一個 ServerSocket 物件，並以 ServerSocket 的 accept()方法傾聽來自 Client 端的連線，在 Client 端達成與 ServerSocket 的連線後，才會建立聯繫兩端的 Socket 物件，並透過兩端 Socket 物件所提供的輸出入資料流，取得 Server 與 Client 端之間的 I/O 溝通管道，此模組內與 Server 端連結的兩端 Socket 物件(或通訊連結)，持續作用至 Client 或 Server 端提出 close()方法即結束，其作用在於負責檔案傳輸協定中連線的控制。在 FTP Server 端開啟一個埠後，經由 Client 端的 PI 以 open 的方式開啟，並向伺服器的預設埠進行連線動作，在連線正確完成時並進而要求 Client 端確認登入(login)的動作，Client 端順序輸入正確的 ID 與認證密碼後，通訊的連結才算建立成功，而後的指令則需經由此通訊連線得以傳輸[2]。

在通訊連線的狀態下，通訊的連結首先為 Server 端開啟其預定的埠以聆聽來自 Client 端的連線請求，但在資料傳輸的連結中(DTP 模組)，則為 Client 主動開啟預定檔案傳輸的埠，Server 經接收到來自於 Client 端的檔案處理指令，如 LIST(詳細列檔)、NLST(列檔) 、RETR(接收)、與 STOR(上傳)等時，Client 端首先會以 PORT 指令，傳送予 Server 端 Client 目前所使用的正確位址與埠號，告知 Server 需透過該 IP 位址與埠號，方可建立與 Client 端資料傳輸連結的資料傳輸插座(如圖 3.3，Data Transfer Socket)，即前小節所述的 DTP 模組。其中 PI 埠號若為 N，則 DTP 埠號則預設為(N-1)。主機間檔案的傳輸透過 DTP 模組的 Socket，與 Socket 所提供的 I/O 資料流進行檔案的傳遞處理，在此檔案傳輸的過程中，遇到 Client 端發出中斷的指令、連線埠號的異動、通訊連結的中斷、或檔案結尾的提示(EOF)種種情況下資料傳輸的連結將被終止。

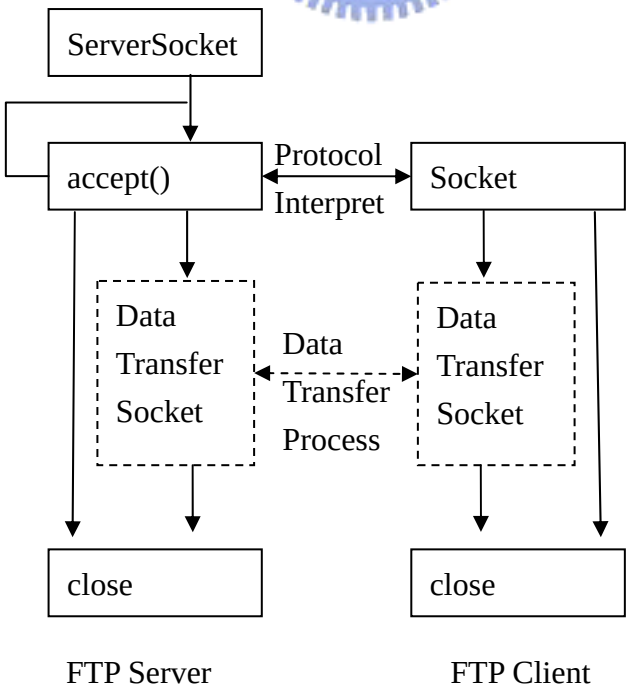


圖 3.3　FTP 程式開發架構[2]

在上述以 FTP 為主體的架構下，FTP 的檔案傳輸流程可簡化如圖 3.4，其中 FTP Client 端主要的傳輸步驟為(1)與 Server 端建立連線，(2)輸入使用者帳號指令，(3)傳送密碼驗證指令，(4)下達檔案傳輸指令，與(5)與 Server 中斷連線，而伺服器端也相對的給予 Client 端適當回應。其中在步驟(4)在下達檔案傳輸的請求指令時，Client 端會先透過通訊連結以 PORT 指令要求與 FTP Server 端建立資料傳輸連結[3]。

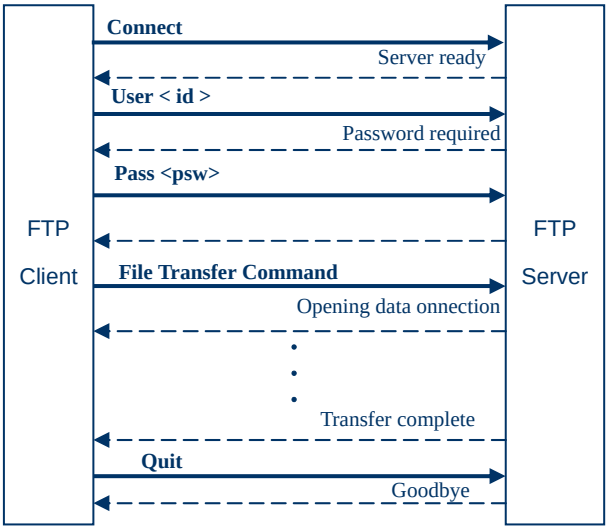


圖 3.4　FTP 檔案傳輸流程[2]

3.3 資訊分享熱線資訊分級需求分析

需求分析分為系統存取部分以及資訊存取的部分，系統存取的部分則如同驗證使用者，對存取的使用者做分級規劃。資訊存取的部分則如同授權的規劃，在對使用者進行分級的規劃後，再進行分級後的權限開放層度規劃。

3.3.1 系統存取

在系統使用者部分，根據與漁業署的聯繫以後，將使用者存取權限分為四個層級，按權限大小排列依序為第一級的資料管理人，第二級的為署內單位，第三級的為縣市政府或船公司，最後一級則為訪客，如表 3.1 所示。

表 3.1 系統存取權限

	漁調資料	漁管資料	船位資料
資料管理人	Mr.Wu	Mr.Wu	Mr.Chen
	Mr.Chen	Mr.Li	
署內單位	Mr.Wang	Mr.Wang	Mr.Chen
	Mr.Sun	Mr.Wang	業務主管
	Mrs.Wang		其他主管
	業務主管		
	其他主管		
縣市政府或船公司	臺北縣	臺北縣	臺北縣
	宜蘭縣	宜蘭縣	宜蘭縣
	桃園縣	桃園縣	桃園縣
	新竹縣	新竹縣	新竹縣
	苗栗縣	苗栗縣	苗栗縣
	台中縣	台中縣	台中縣
	彰化縣	彰化縣	彰化縣
	南投縣	南投縣	南投縣
	雲林縣	雲林縣	雲林縣
	嘉義縣	嘉義縣	嘉義縣
	台南縣	台南縣	台南縣
	高雄縣	高雄縣	高雄縣
	屏東縣	屏東縣	屏東縣
	台東縣	台東縣	台東縣
	花蓮縣	花蓮縣	花蓮縣
	澎湖縣	澎湖縣	澎湖縣
	基隆市	基隆市	基隆市
	新竹市	新竹市	新竹市
	台中市	台中市	台中市
	嘉義市	嘉義市	嘉義市
	台南市	台南市	台南市
	臺北市	臺北市	臺北市
	高雄市	高雄市	高雄市
	金門縣	金門縣	金門縣
	連江縣	連江縣	連江縣
訪客	一般彙整資料	一般彙整資料	一般彙整資料

3.3.2 資訊存取

漁業資訊分享熱線，共有三個異質性的資料庫，從這三個資料庫建立八個具有不同意義的資料倉儲，每一個資料倉儲中，分別建構出不同的維度，而不同存取權限的使用者，其能夠存取的資訊內容也不同。在表 3.3 中，所呈現的是在漁業調查統計資料庫中所建立的資料倉儲之一的平均價格，其所代表的意義則是魚貨的平均價格。在表 3.4 中則是呈現漁業的各魚生物的養殖面積。在表 3.6 中，呈現沿近海的資訊分級的維度開放權限內容。在表 3.7 中，呈現養殖的資訊分級的維度開放權限內容。在表 3.6 中，呈現遭難漁船的資訊分級的維度開放權限內容。在表 3.8 中，呈現進出口的資訊分級的維度開放權限內容。在表 3.9 中，呈現漁管的資訊分級的維度開放權限內容。在表 3.10 中，呈現從業人數的資訊分級的維度開放權限內容。

表 3.2 資料倉儲維度列表

資料倉儲名稱	所包含的維度
平均價格	時間、地區維度、魚或生物種類維度、漁業別
養殖面積	時間、地區、漁獲生物種類維度、漁業別種類維度、養殖方式
沿近海	時間、地區、漁獲生物種類維度、漁業作業種類維度
養殖	時間、地區、漁獲生物種類維度、漁業別種類維度
遭難漁船	時間、地區、遭難原因、噸位別
進出口	時間、水產別、國家別、進出口別、製品別
漁管	漁船別、漁期、漁船噸級、違規日期、主漁業、違規類別、漁船來源
從業人數	時間、地區、船員別、漁業別、專兼業別

表 3.3 平均價格

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
地區維度	地區	O	O	X	O
	縣市	O	O	O(自己縣市)	X
	鄉鎮	O	O	O(自己縣市)	X
	漁市場	O	O	O(自己縣市)	X
魚或生物種類維度	漁獲總計	O	O	O	O
	漁獲大類	O	O	O	O
	漁獲名稱	O	O	O	O
漁業別	漁業別	O	O	O	O

表 3.4 養殖面積

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
養殖方式	養殖方式	O	O	O	O
地區	地區	O	O	O	O
	縣市	O	O	O(自己縣市)	X
	鄉鎮	O	O	O(自己縣市)	X
漁獲生物種類維度	漁獲生物總計	O	O	O	O
	漁獲生物大類	O	O	O	O
	漁獲生物名稱	O	O	O	O
漁業別種類維度	漁業別總計	O	O	O	O
	漁業別大類	O	O	O	O
	漁業別名稱	O	O	O	O

表 3.5 沿近海

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
地區	地區	O	O	O	O
	縣市	O	O	O(自己縣市)	X
	鄉鎮	O	O	O(自己縣市)	X
	漁市場	O	O	O(自己縣市)	X
漁獲生物種類維度	漁獲總計	O	O	O	O
	漁獲大類	O	O	O	O
	漁獲名稱	O	O	O	O
漁業作業種類維度	漁業別總計	O	O	O	O
	漁業別大類	O	O	O	O
	漁業別名稱	O	O	O	O

表 3.6 養殖

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
地區	地區	O	O	O	O
	縣市	O	O	O(自己縣市)	X
	鄉鎮	O	O	O(自己縣市)	X
漁獲生物種類維度	漁獲總計	O	O	O	O
	漁獲大類	O	O	O	O
	漁獲名稱	O	O	O	O
漁業別種類維度	漁業別總計	O	O	O	O
	漁業別大類	O	O	O	O
	漁業別名稱	O	O	O	O

表 3.7 遭難漁船

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
地區	地區	O	O	O	O
	縣市	O	O	O(自己縣市)	X
遭難原因	遭難大類	O	O	O	O
	遭難原因	O	O	O	O
噸位別	噸位別	O	O	O	O

表 3.8 進出口

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
水產別	水產別	O	O	O	O
國家別	國家別	O	O	O	O
進出口別	進出口別	O	O	O	O

表 3.9 漁管

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
漁船別	漁船別	O	O	O	X
漁期	漁期	O	O	O	X
漁船噸級	噸級	O	O	O	X
違規日期	年	O	O	O	X
	季	O	O	O	X
	月	O	O	O	X
主漁業	主漁業	O	O	O	X
違規類別	違規種類	O	O	O	X
	違規型別	O	O	O	X
漁船來源	所屬縣市	O	O	O(自己縣市)	X
	漁船港	O	O	O	X

表 3.10 從業人數

維度別	下挖層數	資料管理人	署內及上級	縣市政府或船公司	Guest
時間	年	O	O	O	O
	季	O	O	O	X
	月	O	O	O	X
地區	地區	O	O	O	O
	縣市	O	O	O(自己縣市)	X
	鄉鎮	O	O	O(自己縣市)	X
船員別	船員別	O	O	O	O
漁業別	漁業別	O	O	O	O
專兼業別	專兼業別	O	O	O	O

3.3.3 驗證資料格式

在資訊分級中，必須透過通路管理員的使用者層級格勢將使用者分級，因為建立使用者層級與輸入使用者帳號密碼是有先後次序的。先規劃好使用這層級的架構，以使用者層級格式匯入如表 3.10，之後進行使用者驗證資料的新增作業時，才有可供參照的使用者層級。而使用者層級的格式內容包括：(1)命令（Command）、(2)使用者層級名稱(User Class)、(3)層級描述(User Class Description)以及(4)父層級名稱(User Class Parent)四個。

表 3.10 使用者層級格式[1]

指令: Command, User Class, User Class Description, User Class Parent				
參數	Command	User Class	Description	Parent
描述	A=新增使用者層級 D=刪除使用者層級	使用者層級名稱	層級描述	父層級 名稱
型態	字串	字串	字串	字串
註	必要	必要且唯一	選擇	必要
範例	A, The Matrix, Kung Fu, Root User Class			

有了使用者層級後，才可以進行使用者驗證資料的新增，表 3.11 是使用者格式，其內容格式為(1)命令（Command）、(2)使用者名稱(User Name)、(3)使用者名稱描述(Description)、(4)登入帳號(Basic Sign on Name)、(5)登入密碼(Basic Sign on Password)、(6)作業系統區功能變數名稱 (OS Sign on Domain)、(7)作業系統使用者名稱(OS Sign on User Name)、(8)使用者所屬層級(User Class, User)以及(9)使用者所屬的層級描述(User Class Description)九個。

表 3.11 使用者帳號、密碼格式[1]

指令: Command, User Name, Description, Basic Sign on Name, Basic Sign on Password, OS Sign on Domain, OS Sign on User Name, User Class, User Class Description									
參數	Command	User Name	Description	Basic Sign on Name	Basic Sign on Password	OS Sign on Domain	OS Sign on User Name	User Class	Class Description
描述	A=新增使用者 C=更改使用者 D=刪除使用者	使用者名稱	使用者描述	登入帳號	登入密碼	OS 領域	OS 使用者名稱	所屬層級	層級描述
型態	字串	字串	字串	字串	字串	字串	字串	字串	字串
註	必要	必要且唯一	必要	選擇	選擇	選擇	選擇	必要	選擇
範例	A, Keanu, Keanu Is a Movie Star, Holly Wood, Movie Star,,,The Matrix, Kung Fu								

以表 3.10 與表 3.11 的範例來說明，表 3.10 範例[A, The Matrix, Kung Fu, Root User Class]代表新增一個使用者層級，而其父層級名稱為權限最大的根目錄[Root User Class]。表 3.11 範例[A, Keanu, Keanu Is a Movie Star, Holly Wood, Movie Star,,, The Matrix, Kung Fu]代表新增一位使用者驗證資料。其使用者的階層式樹狀結構如圖 3.3 所示。

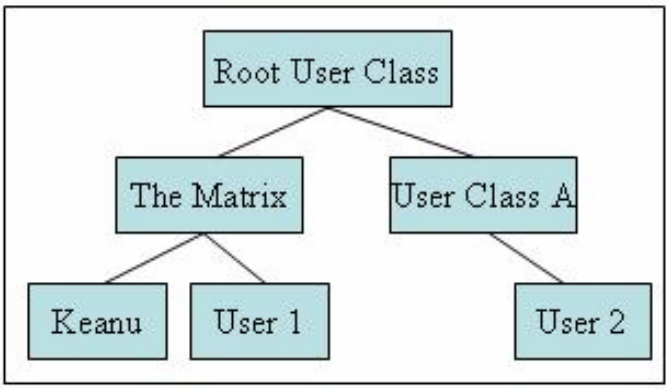


圖 3.5 使用者層級階層式架構[1]

3.4 權限控管系統

在多條供應鏈之間，交易資訊的分享，使得供應鏈的資訊成本大幅降低。

而線上分析處理系統在漁業資訊分享熱線中扮演著核心角色，在權限控管系統中，主要分為三大部分，分別為認證、授權與審計。而在以下的實作過程，將會依照此三大主題進行系統建置。權限控管系統機制是建立在資料倉儲的前端使用者環境線上分析處理(On Line Analytical Processing, OLAP)系統上，並引用植基於角色式存取控制模式作為本系統的安全控管機制。以角色存取控制來作為授權管理的理論基礎，再配合帳號與密碼的身份驗證以及輕量級名錄存取協定(Lightweight Directory Access Protocol, LDAP) 的名錄伺服器(Directory Server) 提出一套安全的權限控管機制。資訊分享控管機制是以密碼驗證(Password Authentication) 的模式定義合法用戶端如何透過網路得到身份驗證的服務。名錄伺服器則是作為驗證使用者身份的後端資料庫，負責提供資訊分享控管機制驗證合法使用者的依據並予以管理與管制。

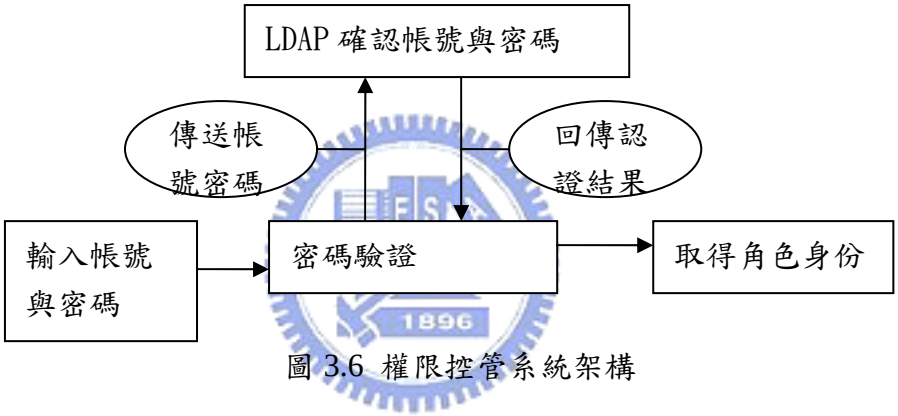


圖 3.6 權限控管系統架構

3.5 自動化排程

在 3.5 節將分三小節來介紹三大異質性資料庫的自動化作法，在 3.5.1 節介紹漁業定查統計資料庫，在 3.5.2 節介紹漁業管理資料庫，在 3.5.3 節介紹漁船傳位資訊資料庫的自動化排程。

3.5.1 漁業調查統計資料庫

開啟魚業調查統計資料庫該台電腦的 SQL Server 2000 ⇨開啟資料轉換服務⇨尋找本機封裝⇨執行刪除漁業調查統計資料庫⇨執行匯入資料⇨執行匯出 FIBASHD、FIFEEDD、FIFMARD、FIPRICD、FISEAFD、FITRAD、FIWORK。

開啟漁業調查統計資料庫該抬電腦桌面漁業資訊分享熱線 FTS，依序執行下列步驟:

設定其 IP 位址:172.18.34.213，使用者帳號:fish，使用者密碼:fish，如圖 3.7。

按漁業資訊分享熱線 mark 選取即時上傳，如圖 3.8。

依序按下連線⇨選檔(分別選取 D:|\漁業調查統計資料庫中的 FIBASHD、FIFEEDD、FIFMARD、FIPRICD、FISEAFD、FITRAD、FIWORK 等檔案)⇨上傳⇨斷線⇨結束。

圖 3.7 檔案轉移服務連線

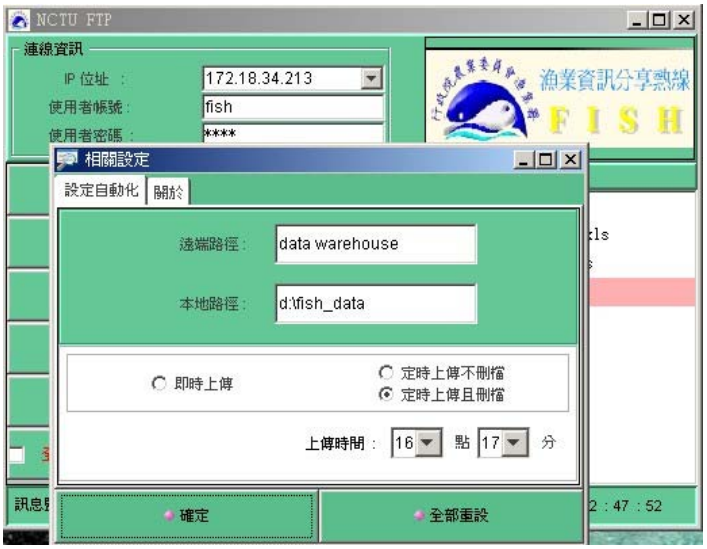


圖 3.8 設定自動化排程

3. 執行漁業資訊分享熱線所在電腦中 E:_漁業資料倉儲\DTS 中每個內部的 DTS 檔案(*.dts) (透過 SQL Server 的資料轉換服務加以執行)。

4. 執行 SQL Server 資料轉換服務中本機封裝中的自動化批次檔.dts。

3.5.2 漁業管理資料庫

請先將漁業管理資料庫中資料轉成以下的檔案名稱及格式，並傳送到資料倉儲所使用的主機上的 (E:\ _漁業資料倉儲 \ 更新文字檔)資料夾內。

表 3.12 詳細檔案列表

漁船違規數	930709 世華船明細.xls 930709 世華代碼明細.xls
漁船個數	930810 世華 112.xls 930810 世華 113.xls 930810 世華 114.xls 930810 世華 115.xls

傳檔的時間預定為每日的 AM 1:00，執行漁業資訊分享熱線所在電腦中 E:_漁業資料倉儲\DTS 中每個內部的 DTS 檔案(*.dts) (透過 SQL Server 的資料轉換服務加以執行)。

執行 SQL Server 資料轉換服務中本機封裝中的自動化批次檔。

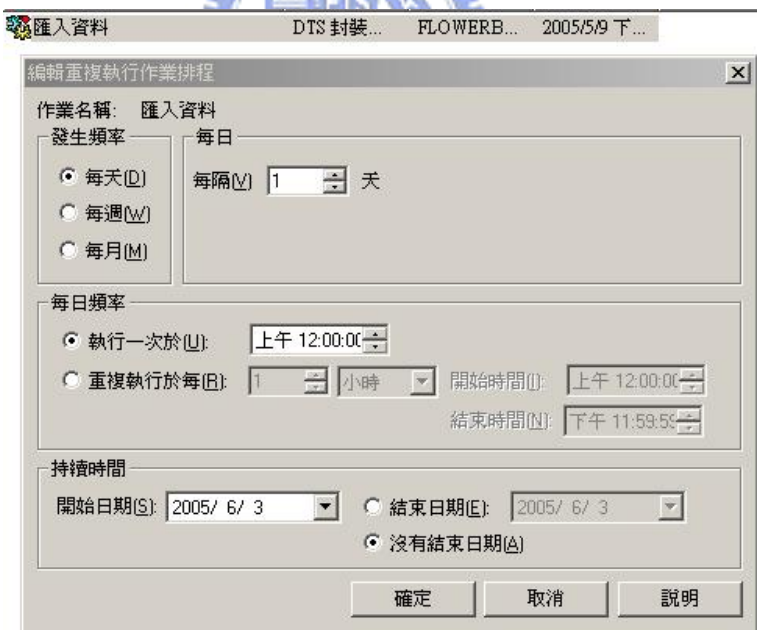


圖 3.10 自動化批次封裝

3.5.3 漁船船位資訊資料庫

1. 以 SQL Server 遠端連線的方式每天將資料傳到 Server 端的 SQL Server 資料庫中。
2. 執行漁業資訊分享熱線所在電腦中 E:_漁業資料倉儲\DTS 中個內部的 DTS 檔案(*.dts) (透過 SQL Server 的資料轉換服務加以執行)。
3. 執行 SQL Server 資料轉換服務中本機封裝中的自動化批次檔。

第四章 檔案轉移服務系統之建置

在目前的許多產業間，分別存在著多條的供應鏈，因為合作的關係，而有資訊分享系統的建置，不過對於眾多提供情報的單位而言，如何將這些情報以低成本的方式從不同的電腦平臺匯總至資料倉儲內則成為一大挑戰。

在 4.1 節中說明檔案轉移服務設計。在 4.2 節中說明 4.2 原理與 JAVA 程式的對應。在 4.3 節中說明 4.3 檔案轉移服務功能與操作說明。

4.1 檔案轉移服務設計

在目前的許多產業間，分別存在著多條的供應鏈，因為合作的關係，而有資訊分享系統的建置，不過對於眾多提供情報的單位而言，如何將這些情報以低成本的方式從不同的電腦平臺匯總至資料倉儲內則成為一大挑戰。

目前本研究以漁業署之漁業資訊分享熱線作為研究平臺，而漁業資訊分享熱線的資料來源主要是來自三大資料庫：漁業調查統計資料庫、漁船船位資訊資料庫及漁業管理資訊資料庫，透過以爪哇技術(Java Technology) 為基礎的檔案轉移服務來進行三大資料庫情報匯集的功能，檔案轉移服務在漁業資訊分享熱線的位置如圖 4.1 所示。

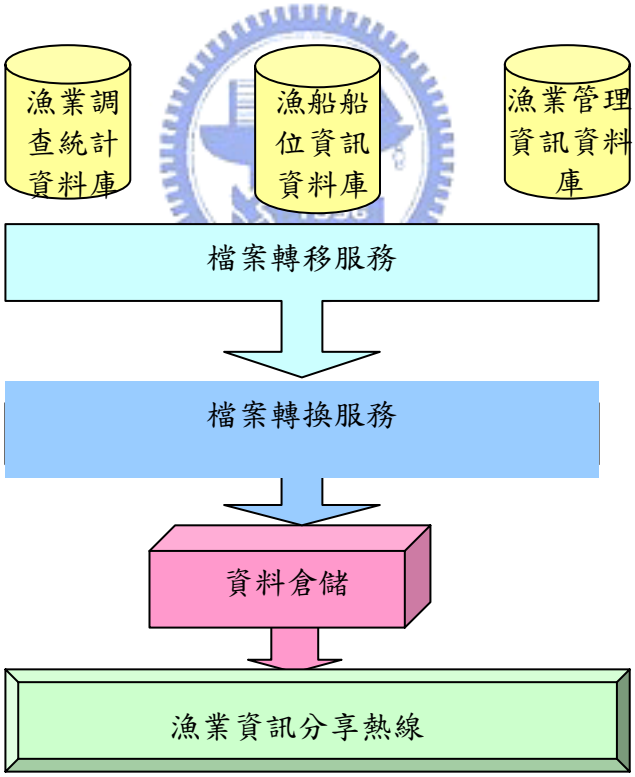


圖 4.1 檔案轉移服務於漁業資訊分享熱線的位置

對圖 4.1 的檔案轉移服務而言，其功能是將三大資料庫每日的資料檔即時地傳送至 FTP Server 處，接著再透過資料轉換服務將交易資料轉入資料庫與資料倉儲中。各使用者再透過網際網路進行線上分析處理及決策。檔案轉移服務的運作是建立在網際網路的檔案轉移協定 (File Transfer Protocol, FTP) 上。

4.2 原理與 JAVA 程式

在 4.2.1 中將說明利用 JAVA 語言建構 FTS 軟體的程序。在 4.2.2 中說明完成 JAVA 程式後，利用 JAR 指令做一個 JAR 檔，作為執行檔。

4.2.1JAVA 與原理的對應

在表 4.1 中，將列出檔案傳輸協定的原理以及所對應之 JAVA 程式碼。以下只針對在原理介紹所出現的幾個重要 FTP 動作，做 JAVA 程式碼的介紹。在表 4.1 的左邊欄位列出 FTP 的執行動作，右邊欄位則是利用 JAVA 語言所撰寫的相關指令。

- 在連線的部分，主要是利用 FtpClient 的物件來執行，此物件所要帶入的兩個值分別是 IP 位址以及阜號。
- 傳送帳號密碼則是用到 FtpClient 中的 Login 屬性來執行，此物件所要帶入的兩個值分別是帳號以及密碼。
- 傳送離開的指令則是用到 FtpClient 中的 CloseServer 屬性來執行。
- 列出遠端目錄則是利用 FtpClient 中的 List 屬性來執行，透過迴圈的方式來列出目錄。
- 選擇上傳檔案是利用利用 FtpClient 中的 setDirectory 屬性來執行，利用 s = s + 1 的方式，將目錄的字串列出。

表 4.1 FTP 原理與 JAVA 程式碼對應表

FTP 原理	JAVA 程式碼
連線	String ip_address = jComboBox1.getSelectedItem().toString(); ftpclient = new FtpClient(ip_address,port);
用戶端送 USER 命令	String user = jTextField1.getText(); String password = new String(jPasswordField1.getPassword()); ftpclient.login(user,password);
用戶端下 QUIT 命令	ftpclient.closeServer();

列出遠端目錄	try {String token = "";
	String allfile = "";
	DefaultListModel listModel = new DefaultListModel();
	listModel.addElement("..");
	TelnetInputStream input = ftpclient.list();
	BufferedReader br = new BufferedReader(new InputStreamReader(input)) ;
	while(allfile! = null){
	if(allfile.startsWith("d")){
	StringTokenizer st = new StringTokenizer(allfile);
	while(st.hasMoreTokens()){
	token = st.nextToken(); }
	if(!(token.equalsIgnoreCase(".")||token.equalsIgnoreCase("..")){
	listModel.addElement(token+" : \\");} }
	allfile = br.readLine(); }
	input.close();
	br.close();

選擇上傳檔案	String s="";
	try{BufferedReader br = new BufferedReader(new FileReader(new File("default_path.txt")));
	S = br.readLine();br.close();}catch(IOException ioe){
	error();}
	fd.setDirectory(s);
	fd.setVisible(true);
	filechosen += (fd.getDirectory()+fd.getFile()+"\n");
	jTextArea1.setText("已選取 :"+"\n"+filechosen);
	jLabel3.setText(" 訊息監控中心 : 請選取檔案 ");

4.2.3 Jar 壓縮檔製作過程

Java 程式語言中的 Jar 檔是一種壓縮的可執行檔，其可以將一個專案下的多個 Class 檔整合成一個壓縮檔。在需要執行時，亦可直接執行 Jar 檔，Jar 檔在被執行後，會根據所設定的路徑執行 main class。

利用 J Builder X 製作 Jar 檔過程如下：

步驟一：首先開啟 J Builder 後，點選下拉式選單「Files」開啟專案。

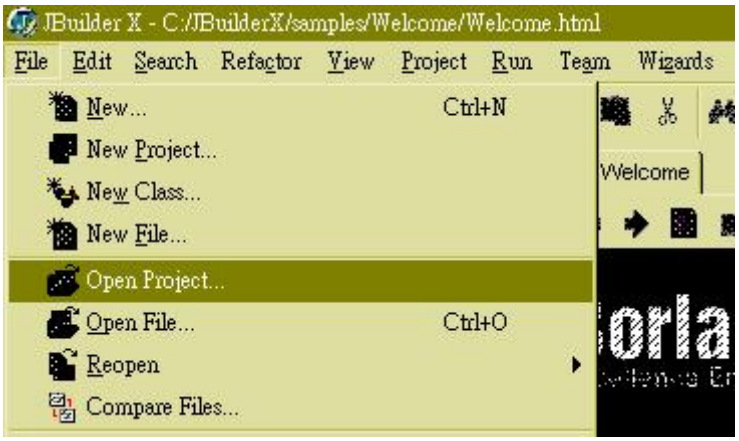


圖 4.2 開啟專案

步驟二：選擇要製作成 JAR 檔的專案。

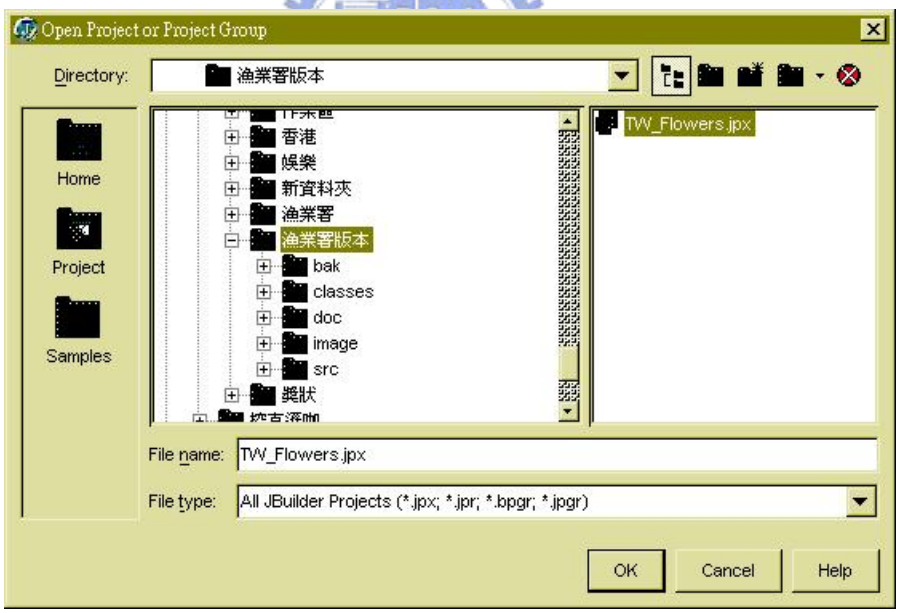


圖 4.3 選擇專案

步驟三：首先開啟 J Builder 後，點選下拉式選單「Wizards」並點選 Native Executable Builder 啟動 JAR 檔製作精靈。

圖 4.4 開啟精靈

步驟四：鍵入 JAR 檔的檔名與路徑，並按下 Finish 完成設定。

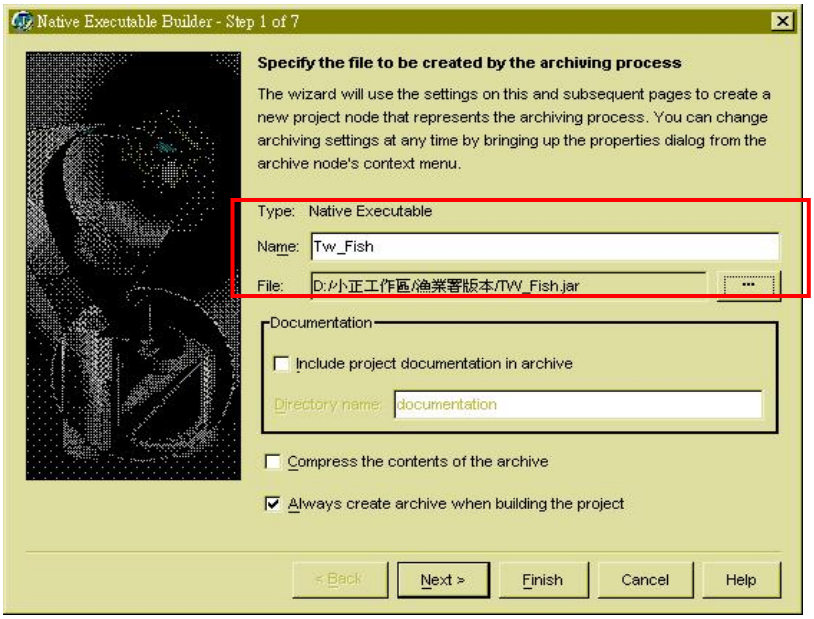


圖 4.5 製作精靈

步驟五： 按下執行完成 JAR 檔的製作，此時在資料夾內，如出現 JAR 檔即表示製作完成，點兩下 JAR 檔即可已執行程式。

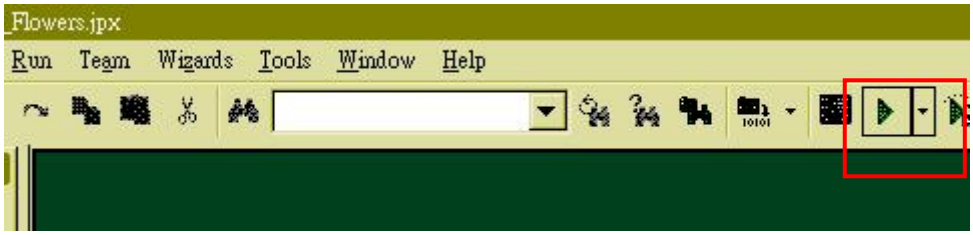


圖 4.6 執行按鈕


漁業署版本
請選取一個項目來檢視它的說明。
請參閱:
我的文件
網路上的芳鄰
我的電腦
名稱
大小
類型
bak 檔案資料夾
classes 檔案資料夾
doc 檔案資料夾
image 檔案資料夾
src 檔案資料夾
connect_address.txt 1 KB 文字文件
default_path.txt 1 KB 文字文件
FTP.iap_xml 49 KB InstallAnywhere Proj
last_upload_time.txt 1 KB 文字文件
remote_path.txt 1 KB 文字文件
TW_Fish.jar 106 KB Executable Jar File
TW_Flowers.exe 191 KB 應用程式
TW_Flowers.jpx 5 KB JPX 檔案
TW_Flowers.jpx.local 2 KB LOCAL 檔案
TW_Flowers.jpx.local~ 2 KB LOCAL~ 檔案
TW_Flowers.jpx~ 4 KB JPX~ 檔案
TW_Flowers-linux 319 KB 檔案
TW_Flowers-mac 221 KB 檔案
TW_Flowers-solaris 194 KB 檔案
TW_FlowersW.exe 194 KB 應用程式
tw_icon.gif 25 KB ACDSee6 GIF Image
upload_time.txt 1 KB 文字文件
user_id.txt 1 KB 文字文件

圖 4.7 檔案夾內容

4.3 檔案轉移服務功能與操作說明

此部分將說明利用爪哇技術所開發的檔案轉移服務之功能說明，而此服務主要分為自動與手動操作的部分，將分別說明如下。在 4.3.1 節中針對檔案轉移服務的功能說明。在 4.3.2 節中說明手動處理程式。在 4.3.3 節中說明自動處理程式

4.3.1 功能說明

該檔案轉移服務共分手動與全自動兩種操作模式；其中手動操作模式是指用人工一個步驟接一個步驟的操作方式來運作，而全自動操作模式則是每天會定時轉移交易檔案至資料倉儲。此檔案轉移服務的進入畫面如圖 4.2 所示，其右上方顯示出彰化花卉市場的標記，右下方則顯示操作日期與時間。市場標記下的左邊代表主端目錄，而其右邊則代表從端目錄。

圖 4.2 檔案轉移服務的進入畫面

4.3.2 手動處理程式

對手動操作模式而言，圖 4.2 左邊的「連線」、「選檔」、「上傳」、「斷線」與「結束」五個步驟則顯示其操作順序的流程，底下分別說明之。使用前，使用者可按下市場標記選擇主端與從端的路徑如圖八所示，設定後再按「確定」鈕已保證確認。

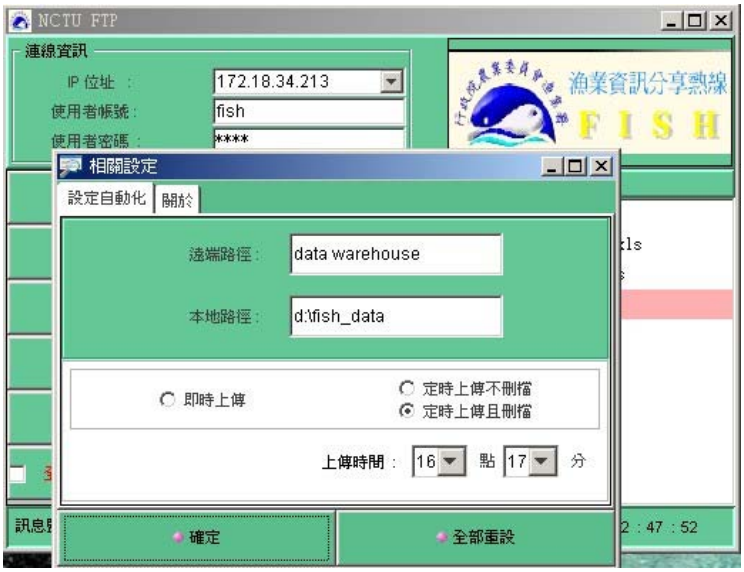


圖 4.3 設定路徑畫面

對「連線」步驟而言，這是使用者首先在圖 4.2 的左上方設定好連線位址、帳號與密碼後，再按「連線」按鈕以進行連線。設計此系統時，連線位址的設定採取下拉式選單方式進行；而選單內容則由外部的.txt 檔案動態匯入，例如使用者可事先將相關的連線位址放入.txt 檔案中。這樣的設計具有兩個特色，即操作容易且有使用上的彈性。建立連線後，這時可由訊息視窗得知最近成功上傳的紀錄，如圖 4.3 所示。

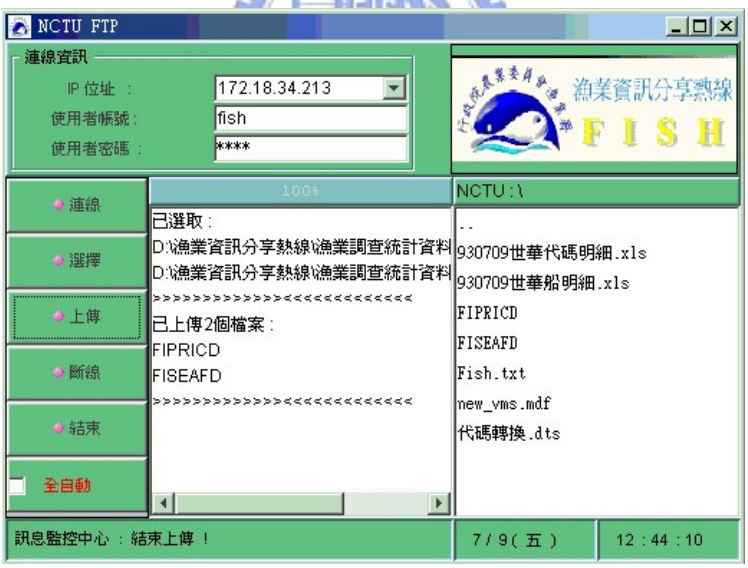


圖 4.4 上傳檔案成功畫面

對「選檔」步驟而言，這是在選取所要轉移的檔案。當按下「選檔」鈕後，這時會出現圖 4.5 的新視窗供使用者選擇要轉移的檔案。

圖 4.5 選擇檔案

對「上傳」步驟而言，這是指按下「上傳」鈕來轉移所選取的檔案。上傳檔案時，圖 4.6 的圈選處可看到進度條(Progress Bar)顯示出目前轉移檔案進度的百分比，而下方的訊息監控中心可得知上傳中的檔案名稱。

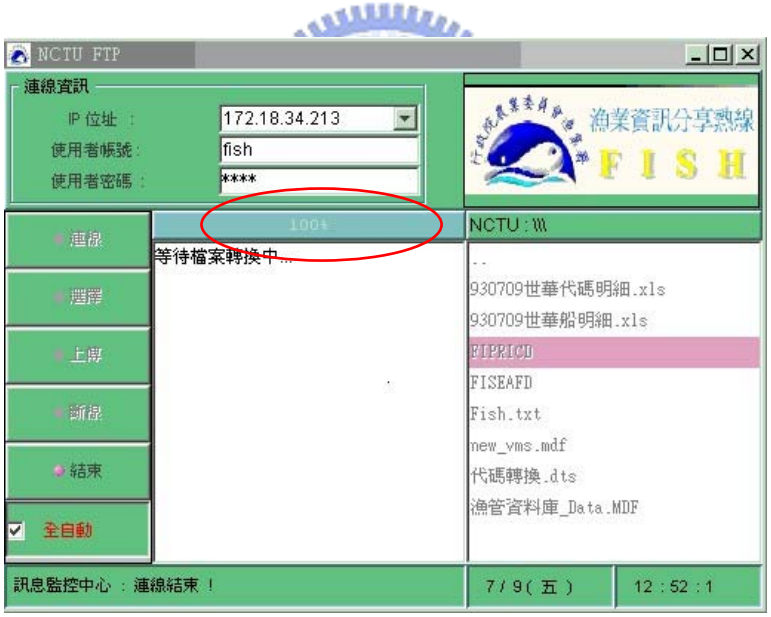


圖 4.6 上傳中的進度條狀態

對「斷線」與「結束」步驟而言，當確認完成檔案轉移後即可按下斷線按鈕以結束連線，這時在訊息列的地方可看到「已中斷連線！」的訊息；接著再按「結束」鈕以離開本系統。該處會顯示出上傳成功的檔案名稱；同時右方的檔案列表會將遠端已轉移檔案的名稱列出。

4.3.3 自動處理程式

對全自動操作模式而言，這是在圖 4.6 的「全自動」鈕處宣告，而其運作則可分為(1)即時上傳與(2)定時上傳兩種處理方式。前者是隨時偵測本地路徑是否有新的檔案準備上傳，如

有則馬上將檔案直接上傳。後者則是在每天固定的時刻進行檔案的轉移，故需要設定轉移的時間如圖 4.7 左下角所示。定時上傳又可依是否刪除已轉移的檔案而有兩種設定方式，如圖 4.7 中間右方所示。

圖 4.7 全自動操作模式的設定

圖 4.8 全自動化的功能設定

4.3.4 利用斐氏圖表示運作流程

利用斐氏圖可以清楚的說明整個系統的運作程序。因此在本節中，將利用透過 Visual Object 軟體來進行斐氏圖的繪製。在繪製過程中，主要分成兩個階段，第一個階段繪製檔案轉移服務在手動的運作程序；第二階段則繪製自動化的運作程序。

在第一階段的手動運作中，主要的動作則依照檔案轉移服務軟體的主要功能分別為：連線、選擇檔案、上傳、斷線與結束。這些主要功能則作為斐氏圖的轉移點(Transition)，另外，控制程序的開關、上傳檔案清單與資料傳送程序則作為(Place)，所繪製的斐氏圖如圖 4.9。

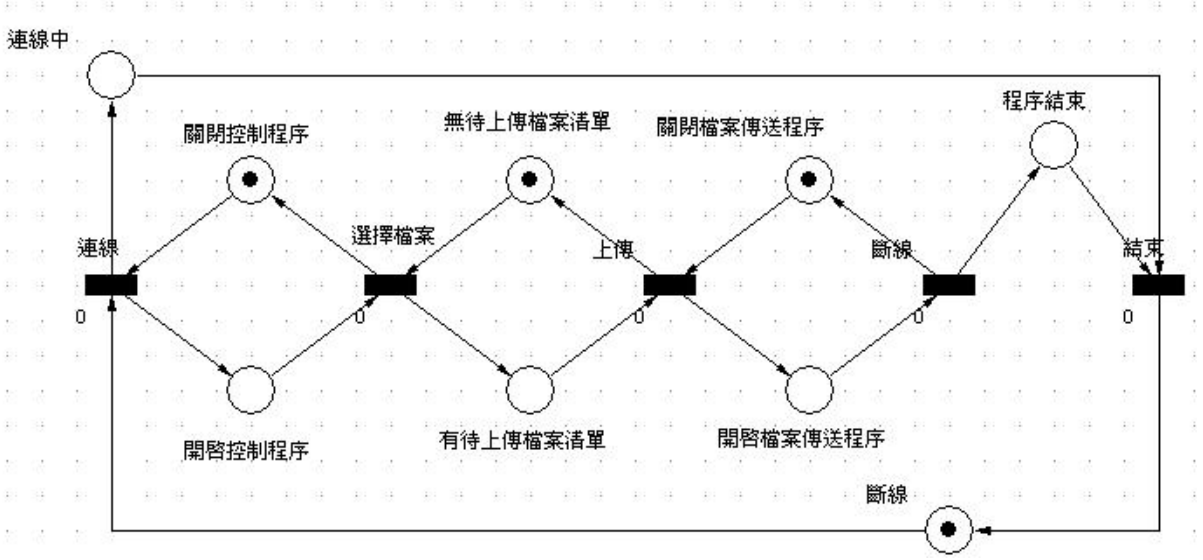


圖 4.9 斐氏圖-手動程序

在第二階段中則說明利用斐氏圖繪製自動化服務，主要的動作有啟動自動化、自動連線、載入上傳檔案清單、上傳、斷線以及結束。以上這些則作為斐氏圖的轉移點，在系統狀態、設定時間、控制程序、資料傳送程序上傳狀態以及程式狀態則作為 Place，所繪製的斐氏圖如圖 4.10。

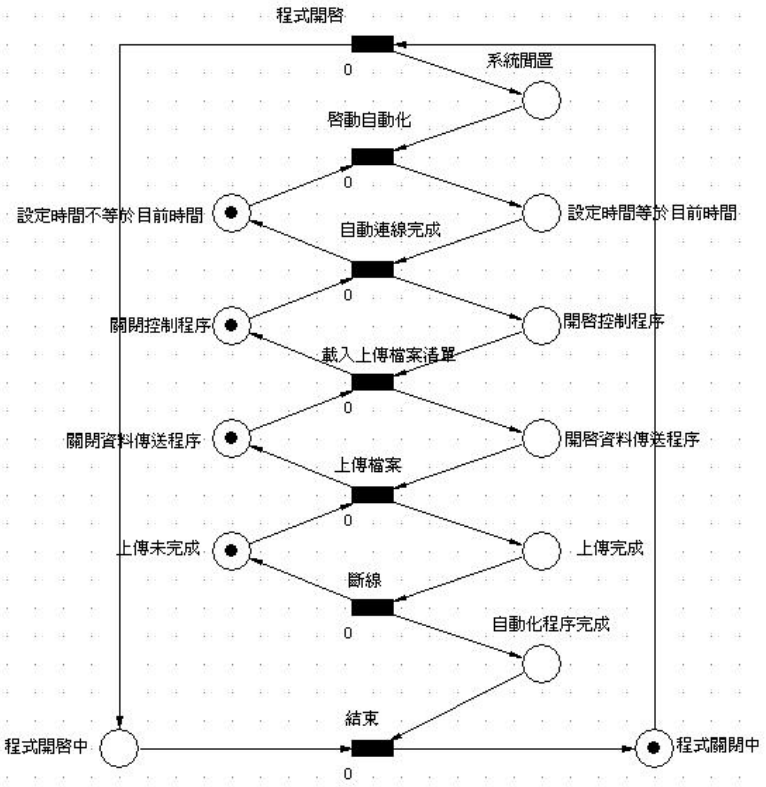


圖 4.10 斐氏圖-自動化程序

接下來的部份則是利用斐氏圖來表示 SOCKET 在整個檔案轉移服務的運作程序，在圖 4.11 的左半邊所代表的是用戶端的運作程序；而在圖右半邊則是伺服端的運作程序。圖中的運作過程主要是從連線的建立，經過目錄下載到檔案下載，最後連線結束的說明。

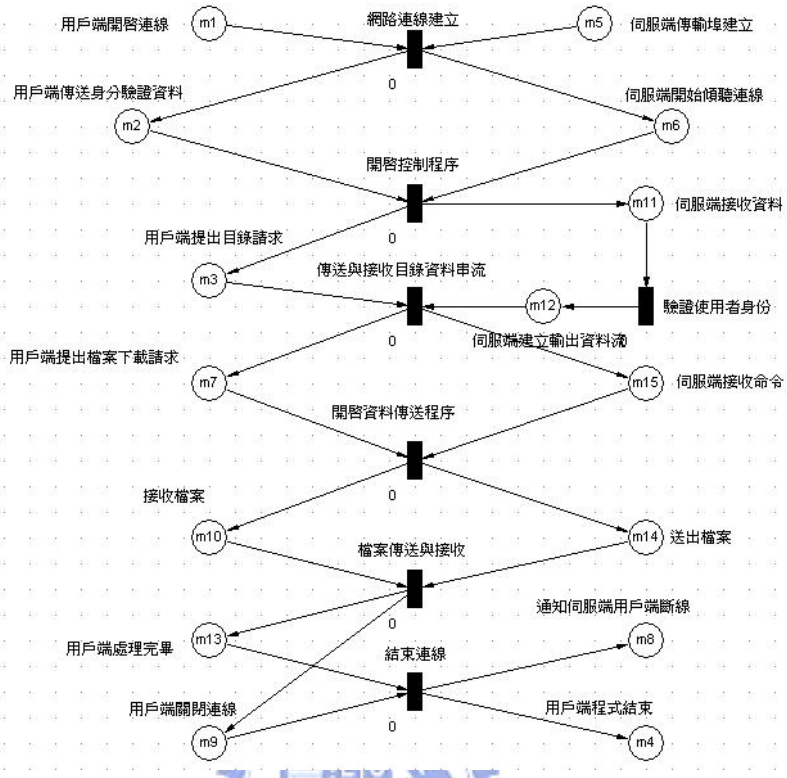


圖 4.11 斐氏圖-Socket 運作程序

第五章 權限控管系統之建置

在權限控管系統建置的部分，首先介紹所使用到的系統元件，其中包含驗證系統與名錄服務，再來則介紹驗證機制，最後則介紹此次研究在全縣控管系統建置所使用的軟體，並分別針對驗證與授權的部分加以說明。在 5.1 節中說明系統原件。在 5.2 節中說明驗證機制。在 5.3 節中說明 5.3 權限控管系統設定。

5.1 系統元件

漁業資訊分享熱線主要是建構在密碼驗證系統與輕量級名錄存取協定名錄服務上，為瞭解釋漁業資訊分享熱線的架構，以下則會說明漁業資訊分享熱線驗證機制的主要角色，並介紹資訊安全原理在漁業資訊分享熱線中所使用的應用軟體之對應關係。在 5.1.1 節中說明驗證系統與名錄服務。在 5.1.2 中說明系統元件與安全原理。

5.1.1 驗證系統與名錄服務

漁業資訊分享熱線中的運作元件主要分為三類，分別是驗證授權中心、安全政策(Security Policy)和帳號資料庫。以下介紹這三種元件所包含的角色：

A. 驗證授權中心：

在本系統中，驗證授權中心即為通路管理員。驗證授權中心提供兩種服務，分別是通路管理員驗證伺服器以及票券伺服器。通路管理員的主要功能是讓使用者在得到進入線上分析處理伺服器的票券之前，讓使用者從通路管理員驗證伺服器得到「TGT」，利用「TGT」可以連線票券伺服器請求服務。票券伺服器會產生一張票券讓使用者連線至網域內的線上分析處理伺服器。當使用者欲連線至目標電腦時，使用者需先出示「TGT」，並要求獲得票券後才能連上目標電腦。

B. 安全政策：

安全政策相當於植基於角色式存取控制模式的規劃。安全政策包含了存取控制裡每個角色所對應的權限關係。在漁業資訊分享熱線中，安全政策是定義在預設網域群組物件中，並由網域的驗證授權中心實現。安全政策儲存在名錄服務中成為網路安全原則屬性的子集合。系統預設只有系統管理員（Administrator）群組可以設定原則，包括在票券伺服器設定票券最長的使用時間、最大連線人數等。

C. 帳號資料庫：

儲存在名錄服務的帳號資料庫所提供的，就是驗證授權中心所需的安全政策資料，名錄內的每一物件代表一個政策，安全政策帳號物件的屬性代表一個加密金鑰。只有網域伺服器是名錄服務伺服器，每一網域伺服器皆有一可寫入及可拷貝的名錄，其中帳號可被產生、登入密碼可被重置並可被網域伺服器改變群組成員，當網域伺服器的名錄服務內容改變時，會將該名錄拷貝並傳送至網域內所有伺服器。

5.1.2 系統元件與安全原理

通路管理原是一個將安全資訊做集中式管理的一套軟體，主要功能是設定並維護加拿大

Cognos 公司的業務情報（Business Intelligence, BI）相管產品的安全資訊。通路管理員驗證伺服器的安全資訊來源包括輕量級名錄存取協定名錄伺服器、本機驗證輸出(Local Authentication Export, LAE)檔以及[AUT]檔三種驗證資訊服務。使用輕量級名錄存取協定名錄伺服器作為安全資訊來源的好處是能夠快速查詢且能供多種應用程式取用，適合使用者人數較多的系統使用;當沒有網路環境而又需要存取受使用層級保護的多為度資料模型時，本機驗證輸出檔可以發揮其可攜帶的特性，提供通路管理員作為驗證來源;[AUT]檔則是 Cognos 舊版產品的驗證來源。

票券伺服器則除了能產生目標伺服器的服務通行證之外，也包含了控制連線人數與通行證的生命週期。並提供單一簽入（Single Sign On）的服務，只要使用者的通行證在生命週期內，存取其他網域伺服器的服務時，則不需再次登入驗證，只需到票券伺服器更換通行證即可。

圖 5.1[1]為漁業資訊分享熱線的構成元件與多頭狗、輕量級名錄存取協定的對應關係

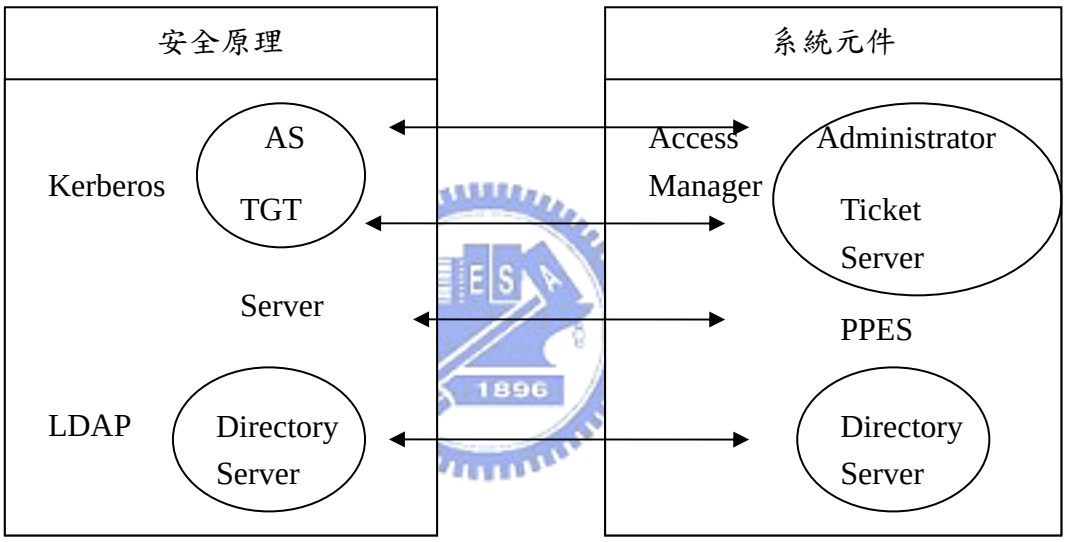


圖 5.1 安全原理與系統元件之對應關係[1]

5.2 驗證機制

漁業資訊分享熱線對使用者進入「線上分析處理系統」所做的驗證過程約可分六個步驟，如圖 5.2[1]所示。以下說明使用者從用戶端的瀏覽器連上「線上分析處理系統」後之驗證過程。

步驟一：使用者輸入帳號與密碼後，通路管理員驗證伺服器進行身份驗證，根據通路管理員驗證伺服器儲存在輕量級名錄存取協定名錄伺服器或本機驗證輸出檔所定義的安全原則來進行身份確認。

步驟二：經驗正確認為合法使用者後，通路管理員核發「TGT」給使用者至票券伺服器要求服務的通行證。

步驟三：使用者經由用戶端傳送方才獲得的「TGT」通行證給票券伺服器。

步驟四：確認「TGT」通行證是有效的生命週期內之後，則有票券伺服器核發可以識別使用者身份的票券分享給業務情報軟體如「Power Play」、「Visualizer」或「Impromptu」使用。並將這張票券的索引以 Cookie 的資料形式儲存在 Web User 的瀏覽器中。

步驟五：使用者提供由伺服器儲存在客戶系統中的資料用來使線上分析處理伺服器能餞別用戶身份，只是伺服器依照用戶的請求發送 WEB 頁面。

步驟六：依照存取原則提供使用者所需的業務情報。

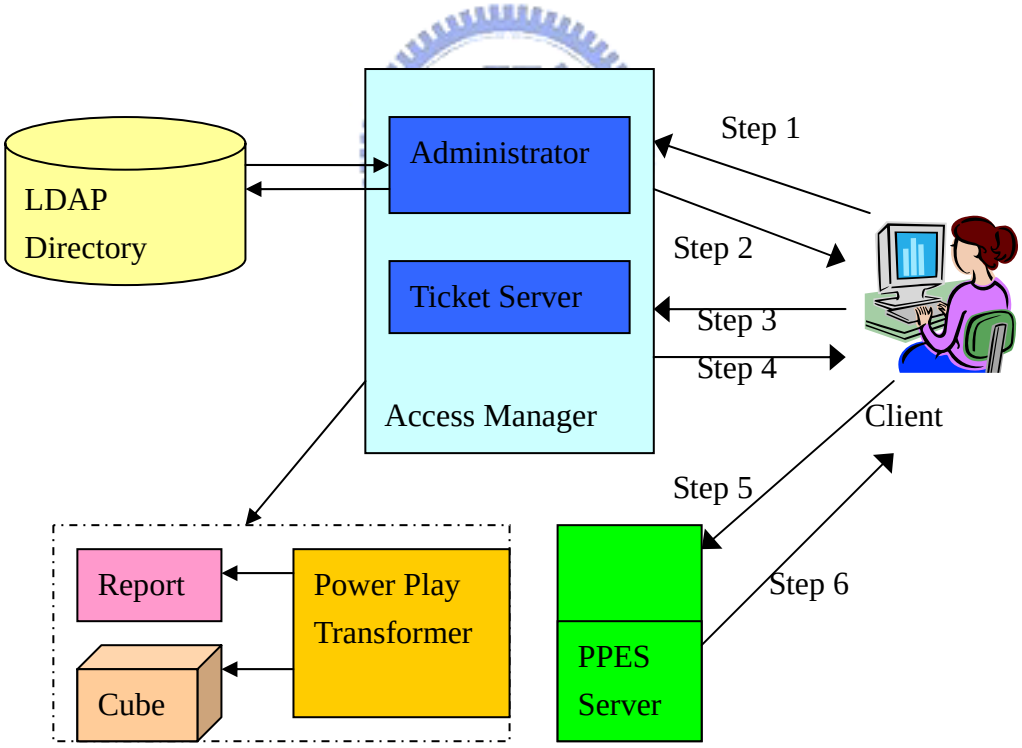


圖 5.2 漁業資訊分享熱線的驗證機制[1]

5.3 權限控管系統設定

在權限控管系統中，主要分成三大部分：認證(Authentication)、授權(Authorization)以及審計(Accounting)。而此研究針對此三大部分進行深入的探討。在 5.3.1 節中說明認證部分，在 5.3.2 節中說明授權的部分，而在審計的部分則到第六章獨立說明。

5.3.1 認證部分

使用者驗證是交易資訊分享系統安全的第一道防線，利用通行密碼驗證(Password Authentication)防止非法使用者進入交易資訊分享系統。在輸入使用者層級與使用者之前，必須先定義 Access Manager 所使用的驗證資訊來源。Access Manager 主要支援名錄伺服器、LAE 檔及 AUT 檔三種驗證資訊服務。以本研究為例，彰化花市交易資訊分享系統是以 Netscape 公司的商業產品 LDAP 名錄伺服器作為存取驗證資訊的來源，而以 LAE 檔作為驗證資訊的備份與維護。以下將介紹 Access Manager 新增連線 LDAP 伺服器的步驟，以及匯入使用者驗證資訊的過程。

首先將票卷伺服器(Ticket Server)啟動，並設定票卷伺服器的連線參數。包括票卷伺服器的埠號(Port Number)、系統允許的最大連線人數以及票卷伺服器所核發的票卷時效，如圖 5.3。隨後在 Access Manager 的名錄伺服器新增一個連線，輸入主機名稱、名錄伺服器的埠號以及區別名稱(Distinguished Name, DN)，其中名錄伺服器的埠號以不和其他網路服務的埠號衝突為原則，區別名稱則通常是輸入主機所在的網功能變數名稱稱，如圖 5.4。接著測試票卷伺服器與憑證中心是否連線正常，如圖 5.5、5.6 所示。

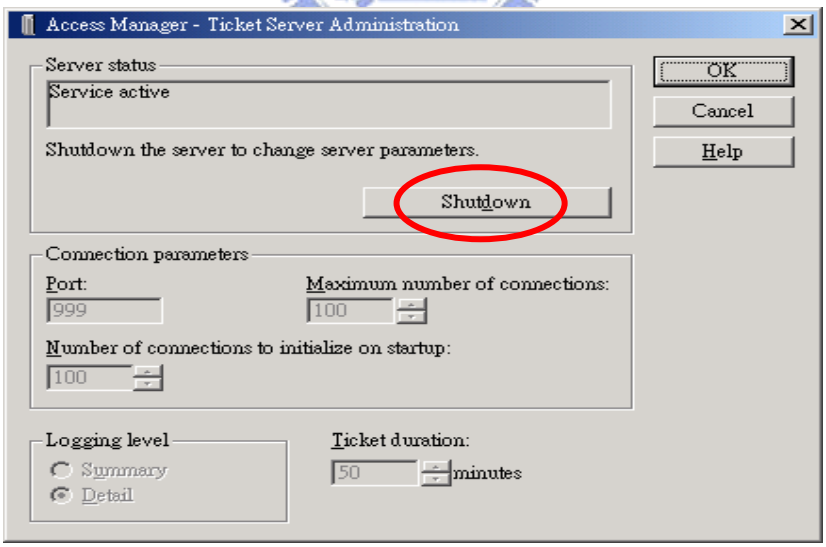


圖 5.3 啟動票卷伺服器

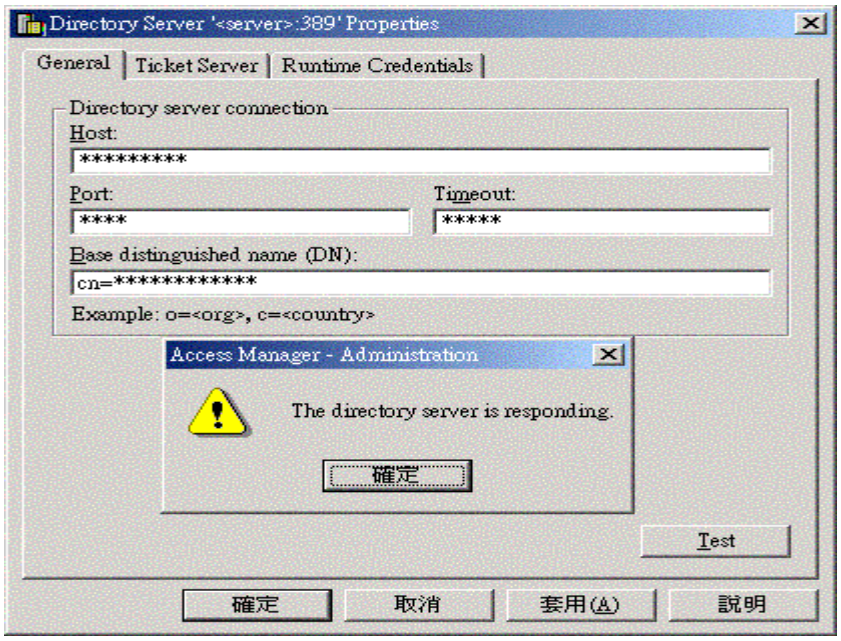


圖 5.4 輸入名錄伺服器主機名稱

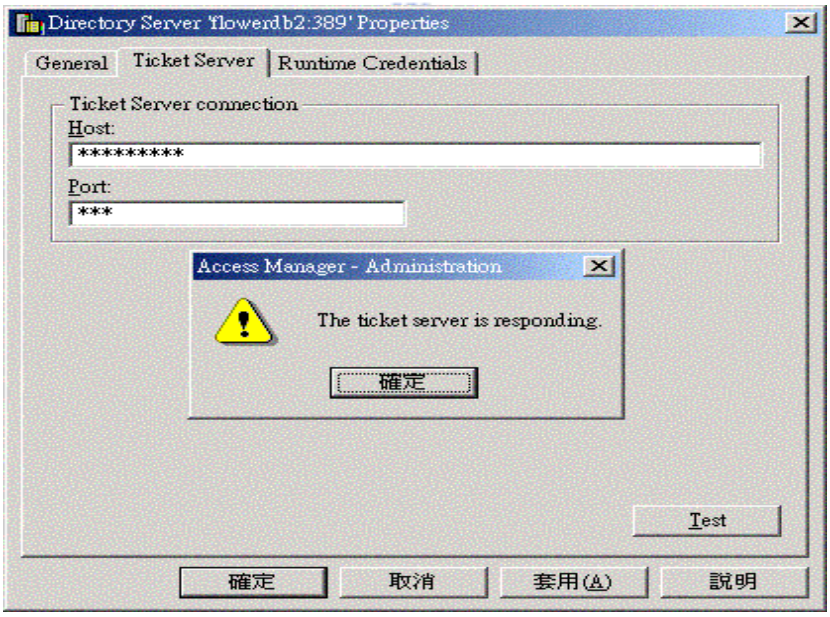


圖 5.5 測試票卷伺服器連線

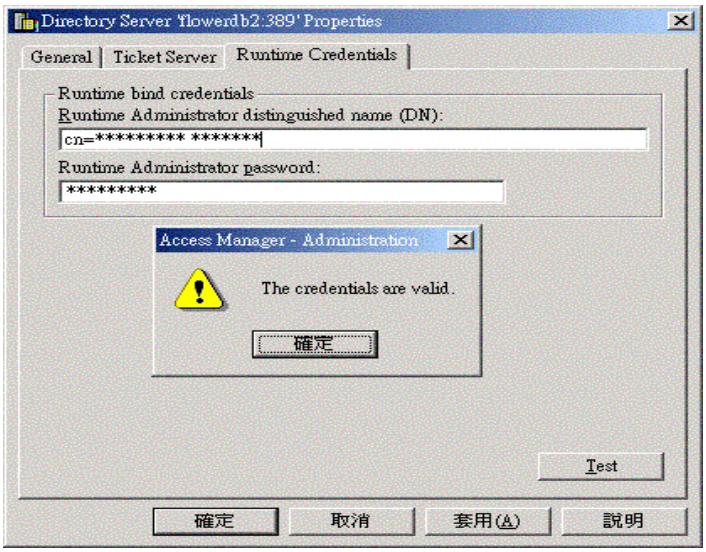


圖 5.6 測試憑證中心連線

Access Manager 連線名錄伺服器成功後，名錄伺服器會產生一個名稱空間(Namespace)。在名稱空間下的所有使用者層級與使用者都會繼承此名稱空間的屬性設定。圖 5.7 是名稱空間帳號登入的設定，設定的項目包括帳號登入的方式、帳號登入錯誤時可容許的次數、帳號登入錯誤後封鎖帳號的時間、帳號的字母長度以及是否區分大小寫。圖 5.8 是名稱空間密碼輸入的設定，設定的項目包括使用者密碼的長度與是否區分大小寫，以及是否要求使用者定期更新密碼。圖 5.9 則是名稱空間的時區與語系的設定。

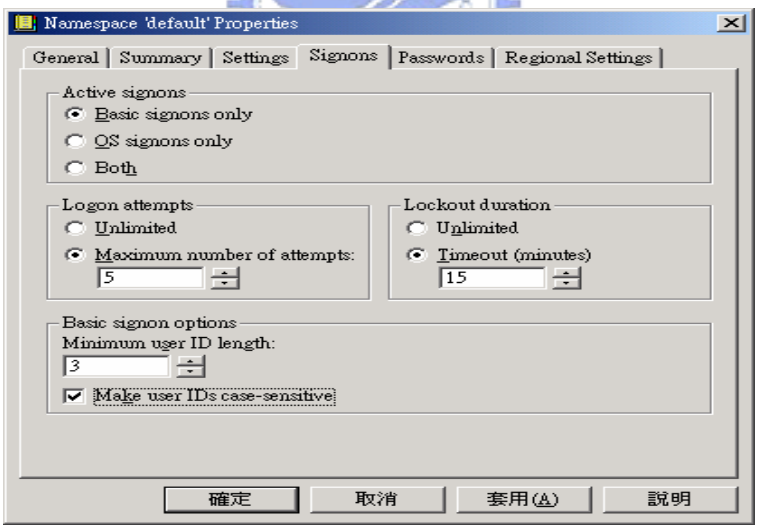


圖 5.7 設定登入帳號時的行為屬性

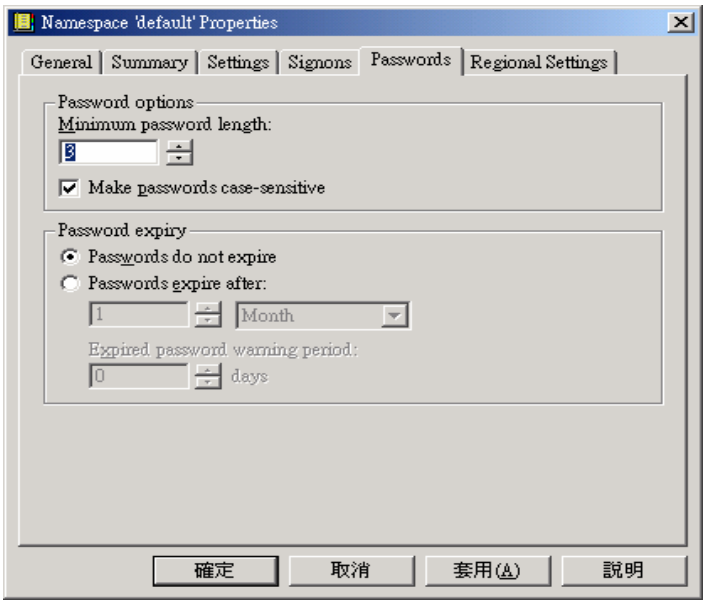


圖 5.8 設定密碼時的行為屬性

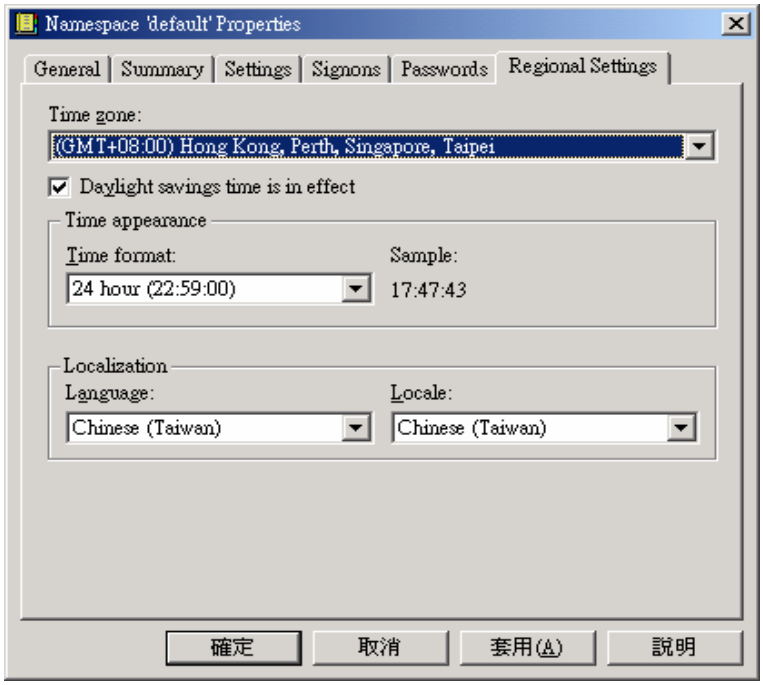


圖 5.9 設定時區與語系

設定完名稱空間的屬性之後，點選執行配置(Runtime Configuration)將名錄伺服器配置為 Access Manager 預設的驗證資料來源。首先選擇 Access Manager 可配置的驗證來源，同時點選名錄伺服器與 LAE 檔為 Access Manager 的驗證來源，如圖 5.10。然後確認名錄伺服器的設定環境無誤，如圖 5.11。接著選擇名錄伺服器要預設的名稱空間，如圖 5.12。圖 5.13 為 LAE 檔的路徑名稱，圖 5.14 則為 LAE 檔預設的名稱空間。最後選擇名錄伺服器為 Access Manager 預設的驗證資料來源，如圖 5.15。如此設定，一旦名錄伺服器無法正常連線時，LAE 檔會替代名錄伺服器成為 Access Manager 驗證資料來源以維持系統的驗證運作。

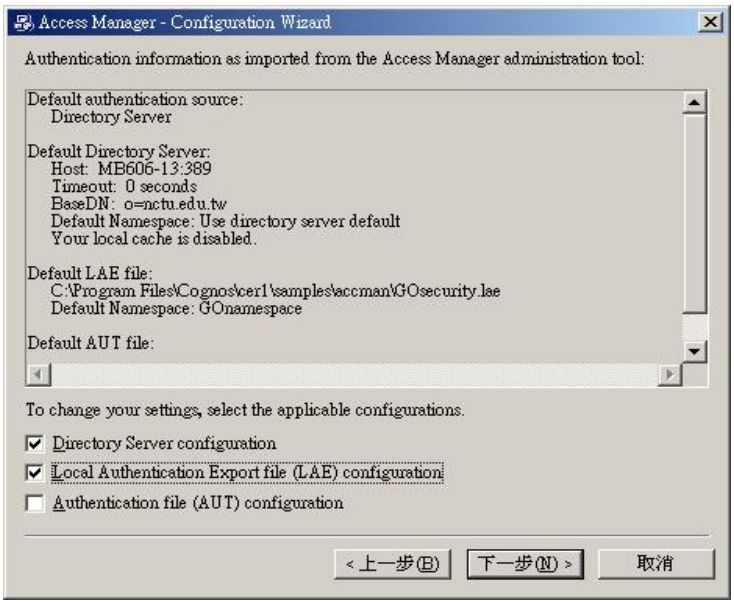


圖 5.10 選擇 Access Manager 的驗證來源

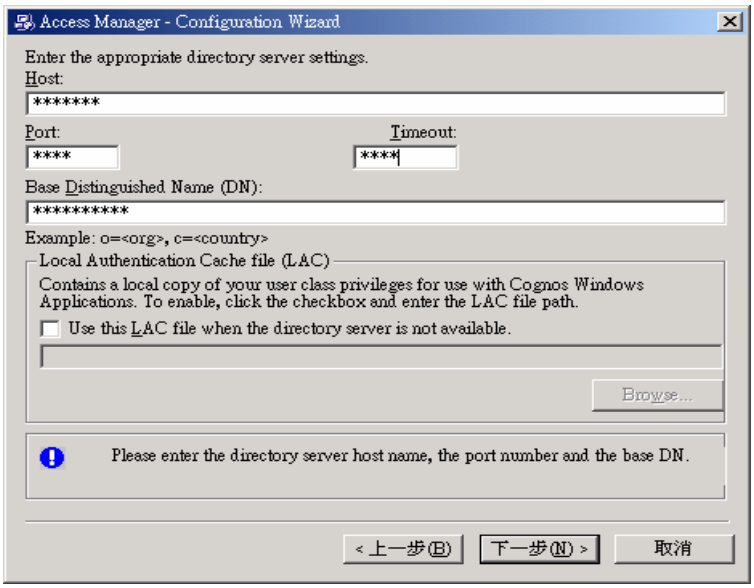


圖 5.11 確認名錄伺服器的環境

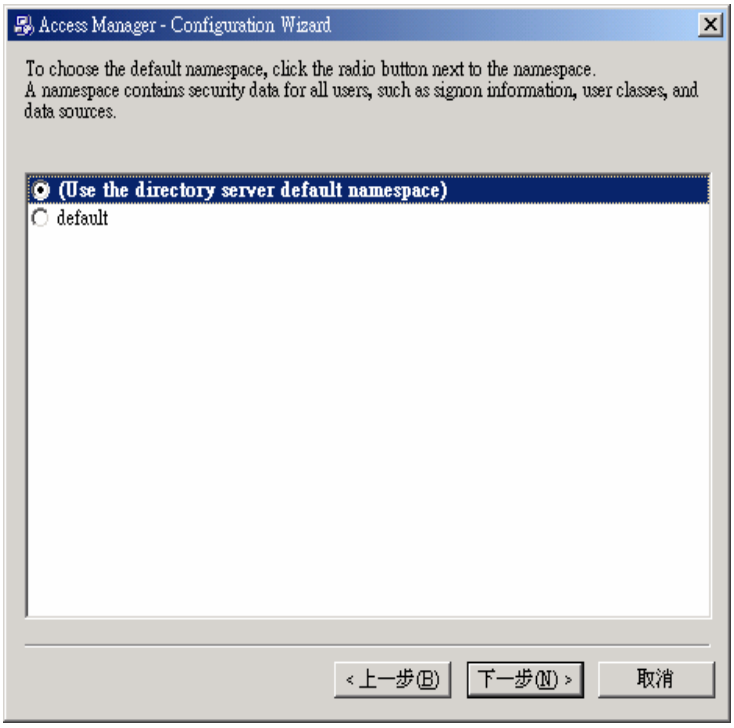


圖 5.12 選擇名錄伺服器預設的名稱空間

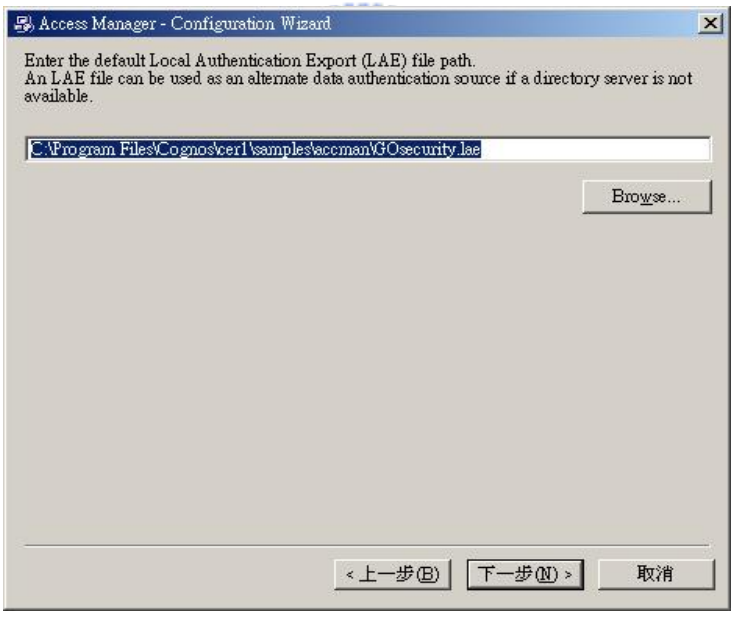


圖 5.13 確定 LAE 檔的路徑

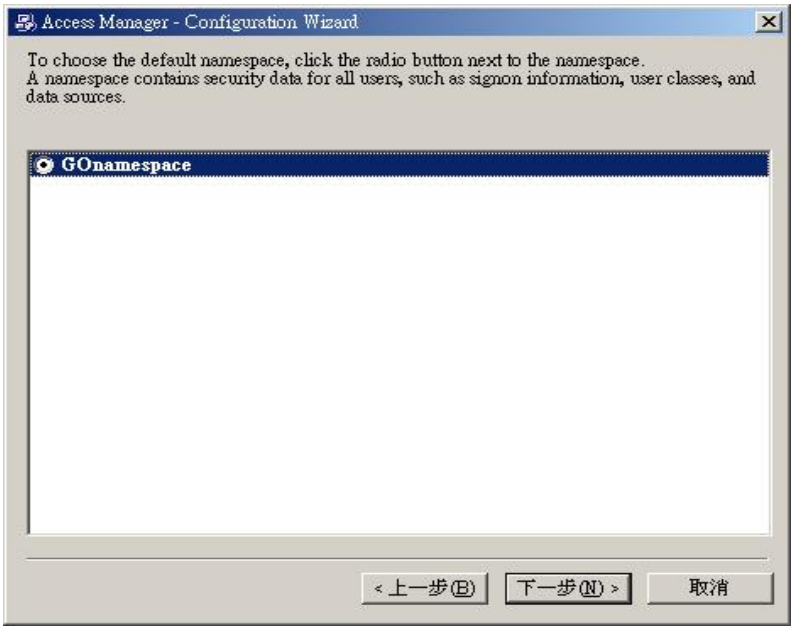


圖 5.14 選擇 LAE 檔預設的名稱空間

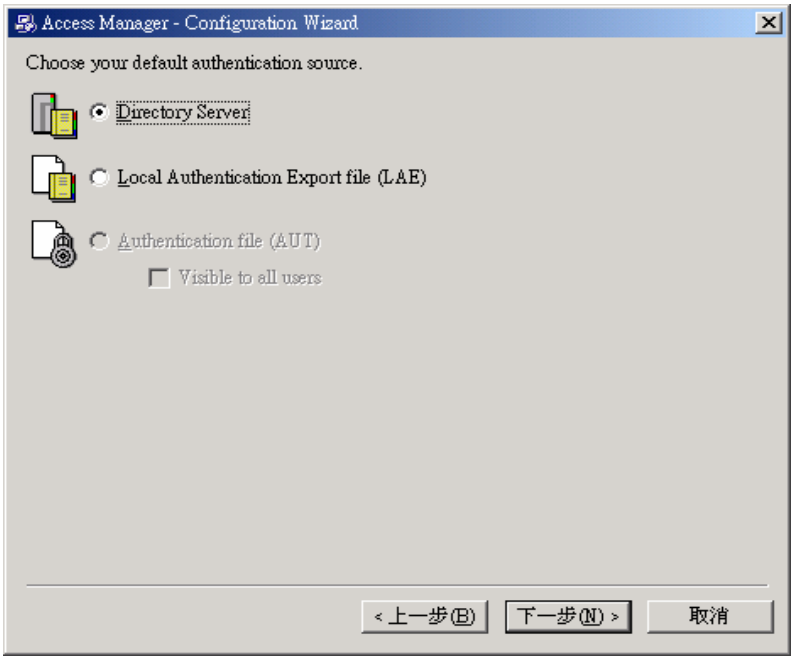


圖 5.15 選擇名錄伺服器為預設的驗證資料來源

接著依照交易資訊分享的分級內容來新增使用者層級，輸入使用者層級名稱後並設定允許使用者層級存取資訊的日期與時間，如圖 5.16 所示。圖 5.17 則為使用者層級與使用者的行為設定，定義使用者層級是否能新增或刪除所存取的資訊內容，以及使用者能否有修改密碼的權力。

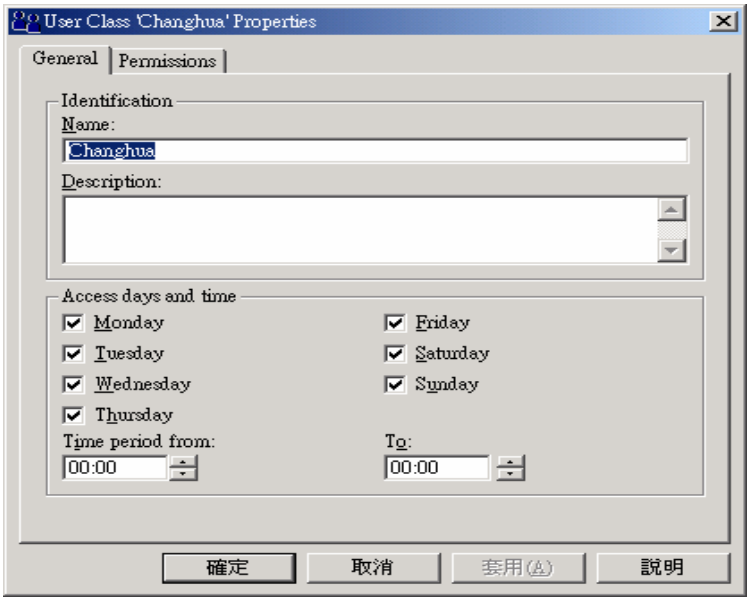


圖 5.16 設定使用者層級存取的日期與時間

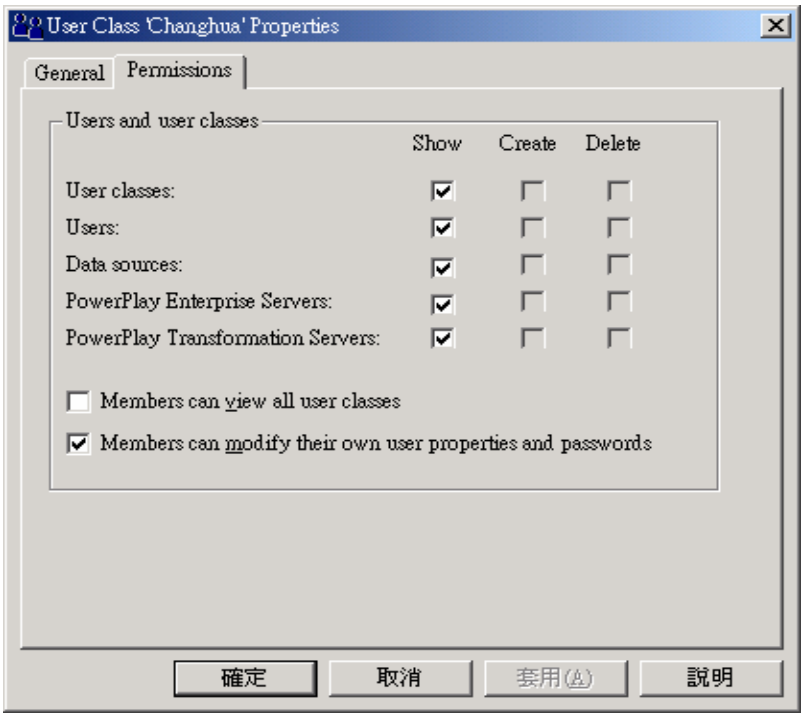


圖 5.17 設定使用者層級與使用者的行為

接著新增使用者，圖 5.18 是輸入使用者的名字、電子信箱及電話號碼等個人資料，圖 5.19 是輸入使用者帳號與密碼，圖 5.20 是選取使用者所屬的使用者層級，圖 5.21 則是設定使用者個人化的資料夾。

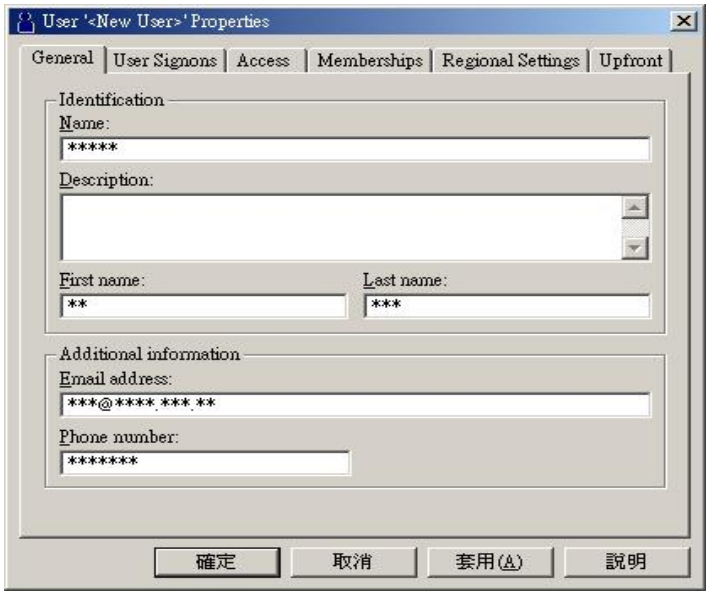


圖 5.18 輸入使用者名稱

圖 5.19 輸入使用者帳號與密碼

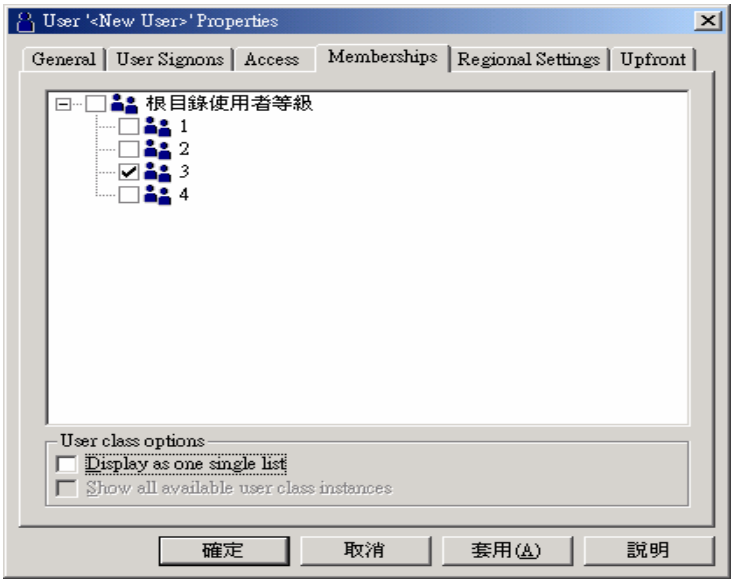


圖 5.20 選取使用者所屬的使用者層級

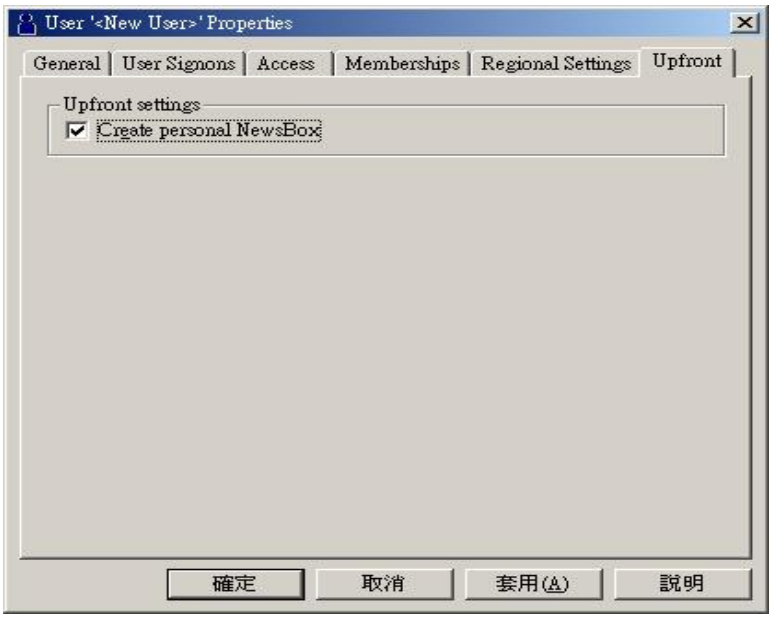


圖 5.21 Upfront 個人化資料夾

依照上述方法新增訪客的帳號，並在名稱空間的屬性裡將訪客帳號 Guest 設定為免輸入帳號與密碼即可登入，如圖 5.22 所示。建立使用者層級與使用者之後，Access Manager 的驗證架構即已建置完成，如圖 5.23。

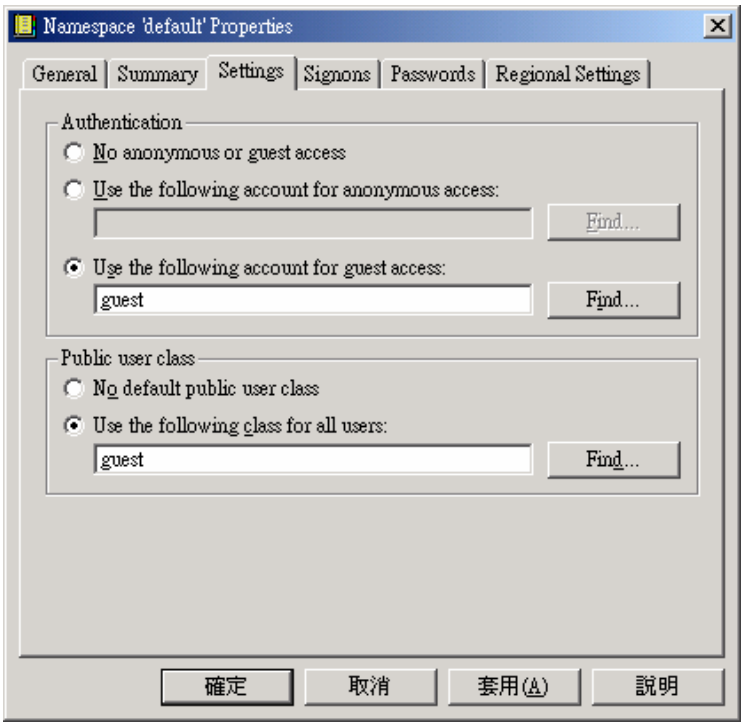


圖 5.22 設定訪客為公用帳號

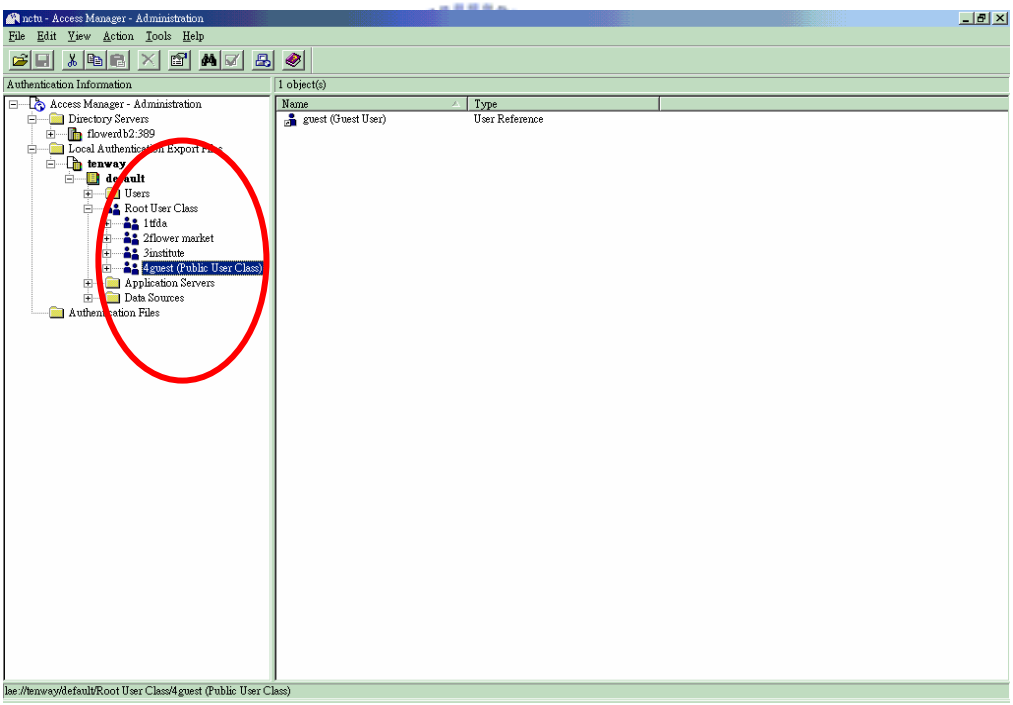


圖 5.23 完成 Access Manager 的架構

5.3.2 授權部分

完成 Access Manager Administrator 使用者層級與使用者的匯入之後，接下來便是存取控制的部分。存取控制是基於將資訊分享內容分級的安全政策，來規範合法的使用者在安全範圍內存取資訊。例如，訪客只能合法存取相關的大宗交易資料，而不能隨意存取單筆的交易資料。由於 Power Play Transformer 是建構多維度資料模型的商業軟體，主要功能是篩選與分

類資料倉儲的資料並設計出 OLAP 的架構。因此，必須在 Power Play Transformer 中加入多維度資料模型的使用者層級並配合分級原則，使得使用者在 OLAP 上只能存取合法的維度與衡量值。

首先將在 Access Manager Administrator 中架構好的使用者層級套用到 Power Play Transformer 產生的 Power Cube 裡，在 Transformer 中點選 Model Properties 如圖 5.24，勾選「Include Access Manager user classes in the model」與「Include Access Manager auto-accesses in the model」按下確定後，畫面即出現使用者層級的小視窗，如圖 5.25。將所需要設定權限的層級拖曳到 Power Cubes 的視窗中，即完成多維度資料模型使用者的匯入作業。

圖 5.24 點選 Model Properties

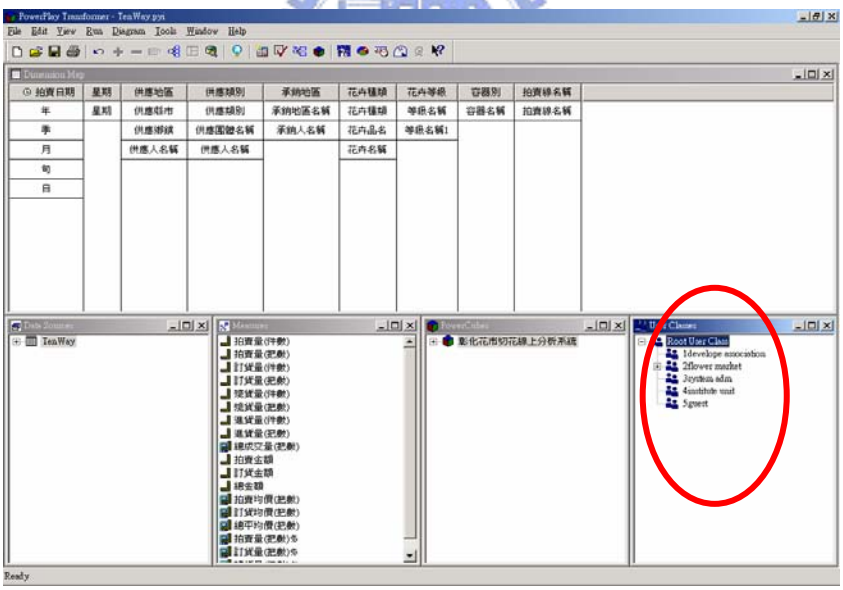


圖 5.25 產生使用者層級視窗

在衡量值方面，在 Power Cubes 下所屬的使用者層級按右鍵點選層級的屬性，出現如圖 5.26 多維度資料模型衡量值的視窗，在 Status 處設定該使用者層級在 OLAP 中是否能觀看到此衡量值。

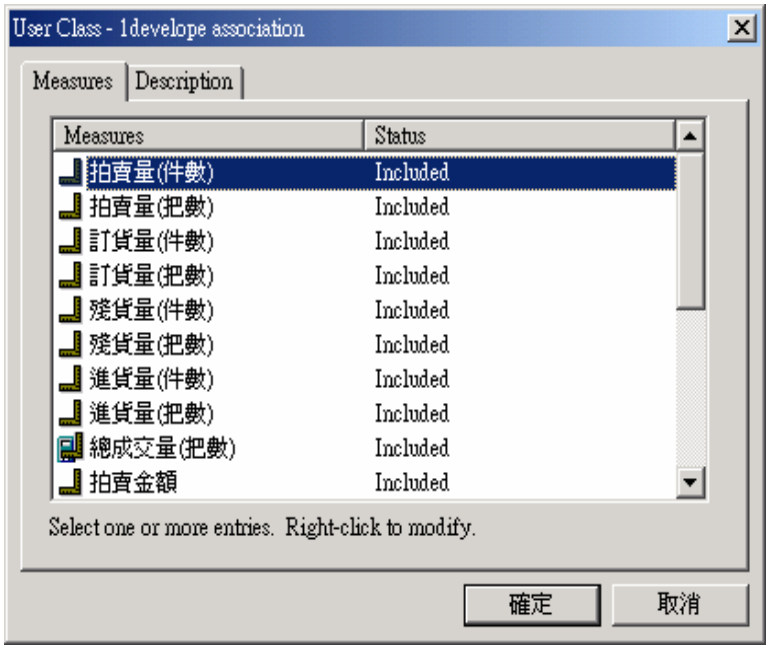


圖 5.26 設定使用者層級之衡量值

在維度方面，開啟 Tool Bar 的 Show Diagram 功能選項進入 User Class 設定多維度資料模型所屬的使用者層級可觀看的維度。設定選項為 Use Customer View 如圖 5.27 與 Omit Dimension 如圖 5.29。Use Customer View 包含加總(Summarize)的功能如圖 5.28，其主要的目的是讓使用者在 OLAP 上只能下挖到某一欄維度中的某個階層。Omit Dimension 的功能則是刪除維度選項，使用者在 OLAP 上將無法存取此一維度以及其中的任何階層。維度與衡量值的設定完成之後，將 Transformer 的資料倉儲架構存檔並重新轉換出一個多維度資料模型，如此便完成存取控制的工作。

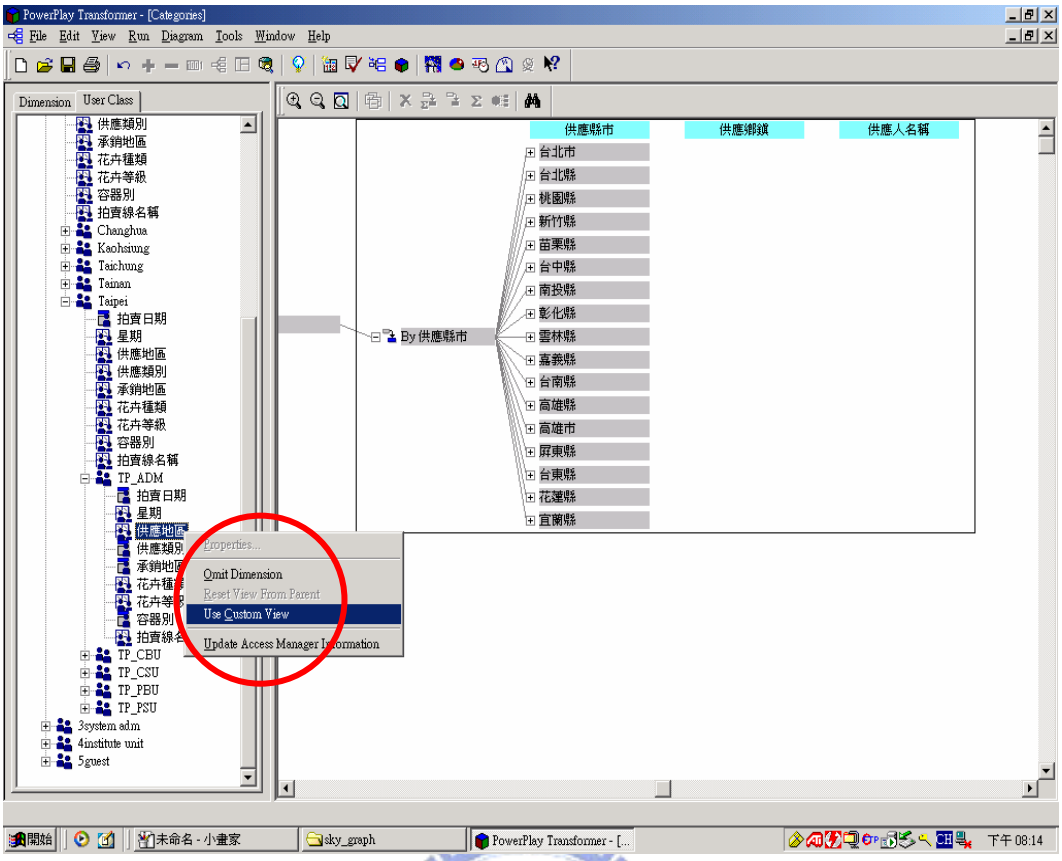


圖 5.27　Use Customer View 選項

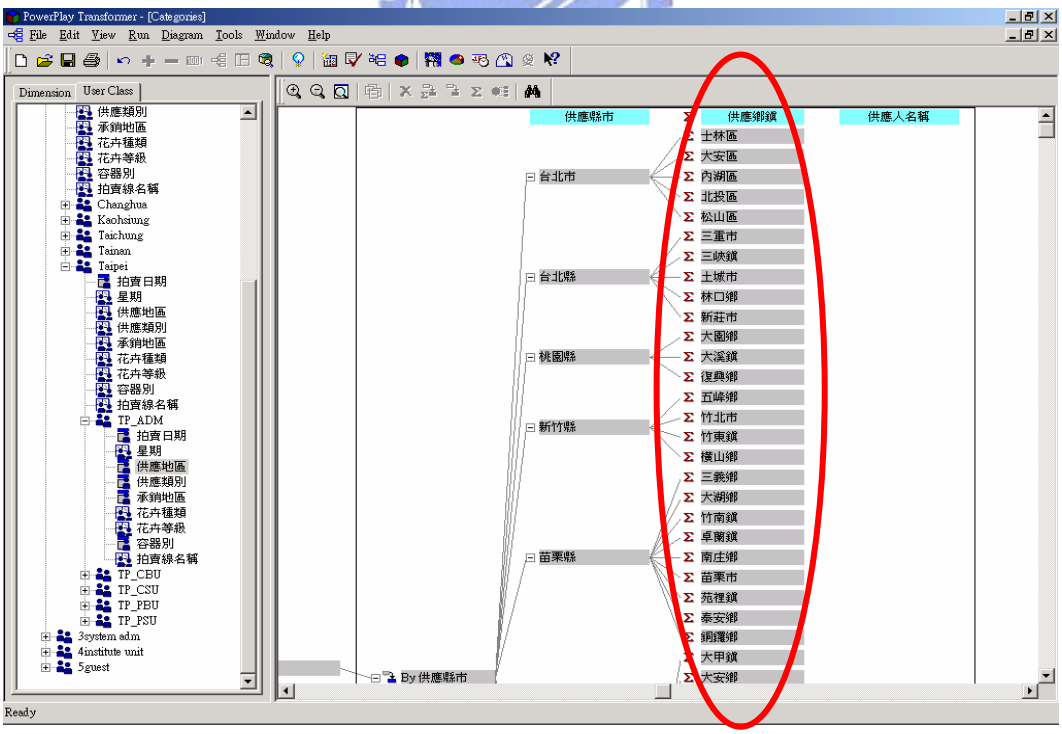


圖 5.28　加總功能

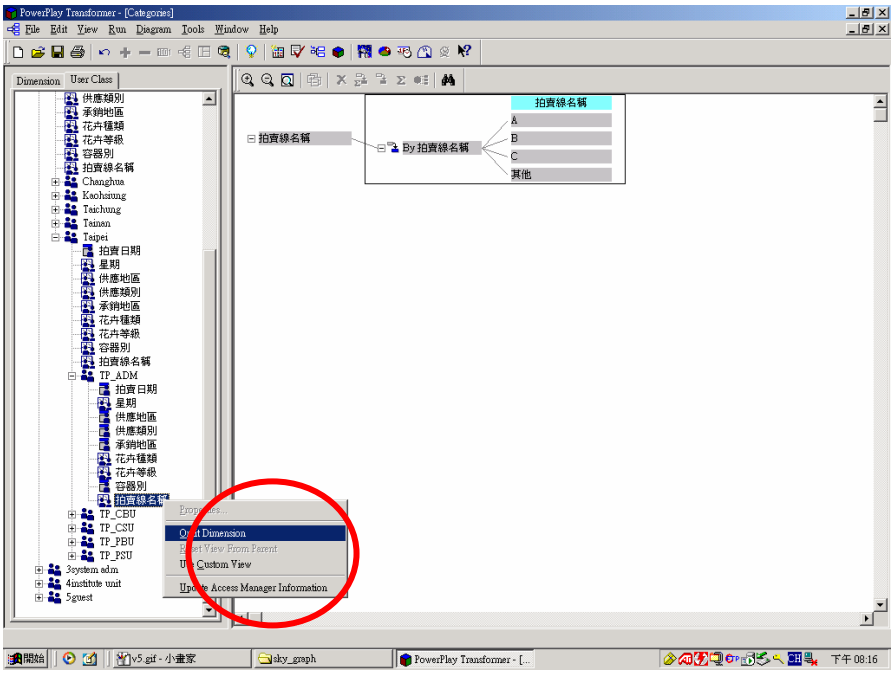


圖 5.29 刪除使用者層級之維度

5.3.3 權限控管系統之操作

在完成權限控管系統的簡略介紹以後，以下的部分，則透過流程的方式來示範系統的操作。

一、認證部分

Step 1. 開啟位於程式集 Cognos 資料夾中的 Access Manager –Administrator，進入系統主畫面。

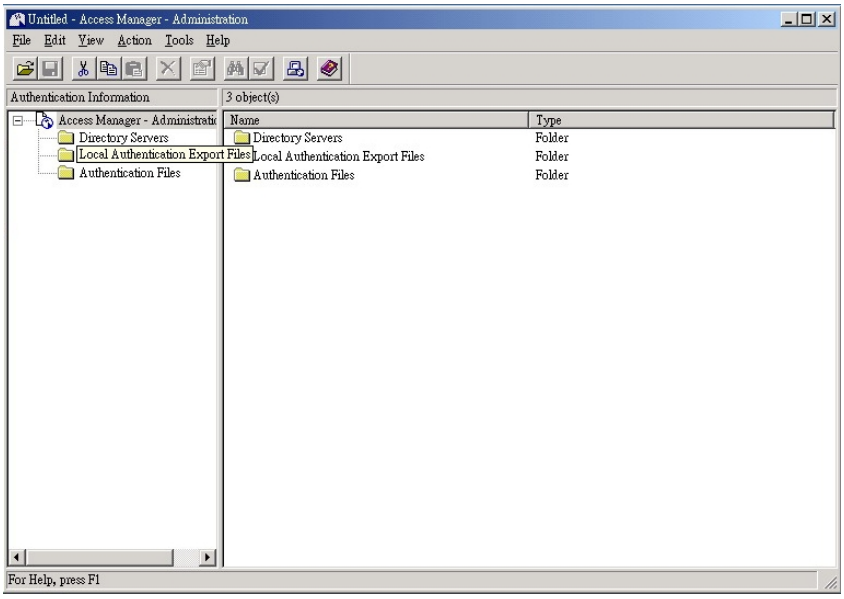


圖 5.30 Access Manager –Administrator 主畫面

Step 2. 按下開啟舊檔按鈕，載入先前已完成的設定檔。

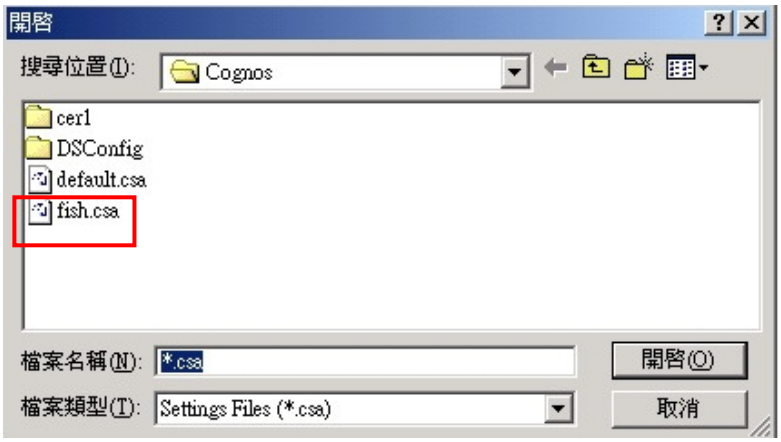


圖 5.31 開啟舊檔畫面

Step 3. 完成載入舊檔後，展開選項功能。

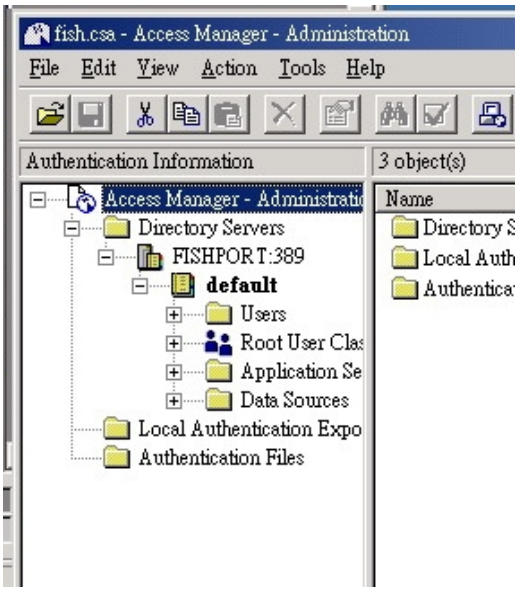


圖 5.32 載入後的設定

Step 4. 進入使用者層級列表，在欲建立使用者層級的父層級上按滑鼠右鍵，Add User Class。

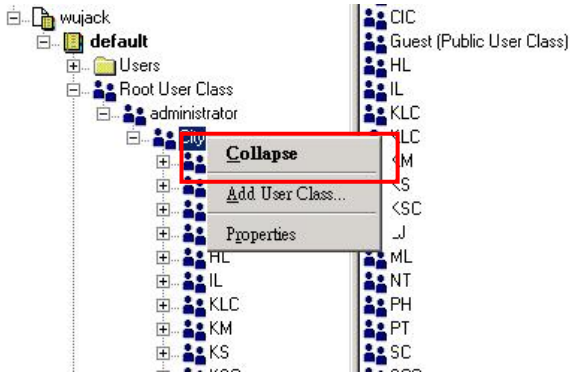


圖 5.33 新增使用者層級

Step 5. 進入新增使用者層級畫面後，設定此角色的名稱與可使用的時間或期間以及功能。

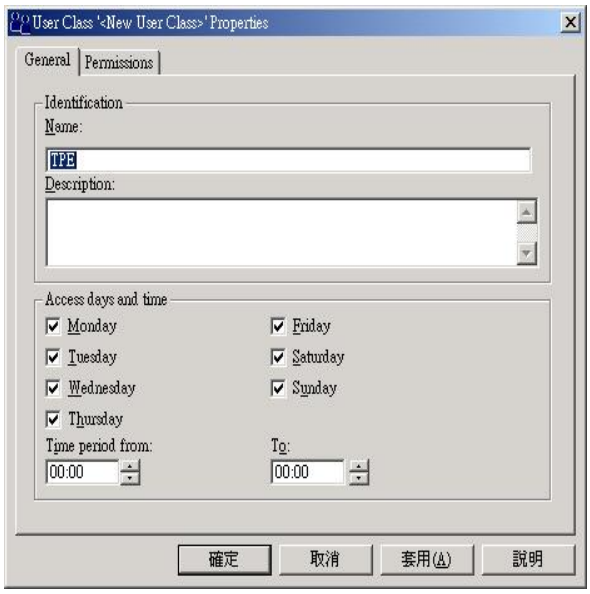


圖 5.34 新增使用者層級設定

圖 5.35 新增使用者層級設定-2

Step 6. 在 User 上按右鍵，此時點選 Add User，進入新增畫面。
Step 7. 設定新增使用者的帳號與密碼，以及所繼承的角色。

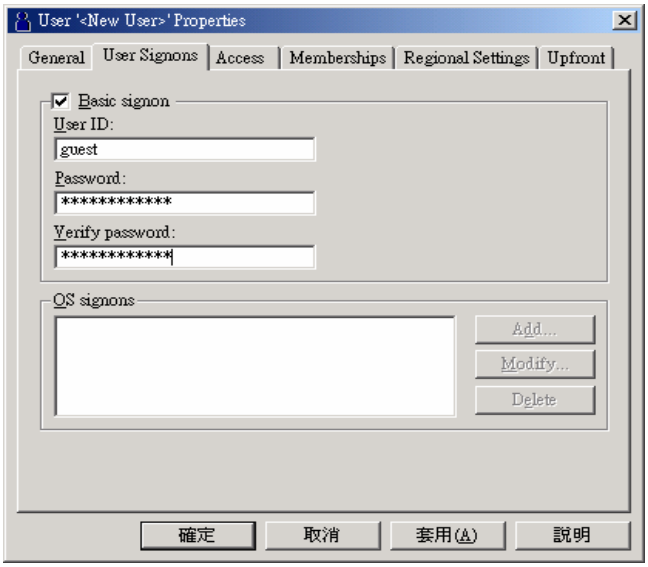


圖 5.36 新增使用者的設定畫面

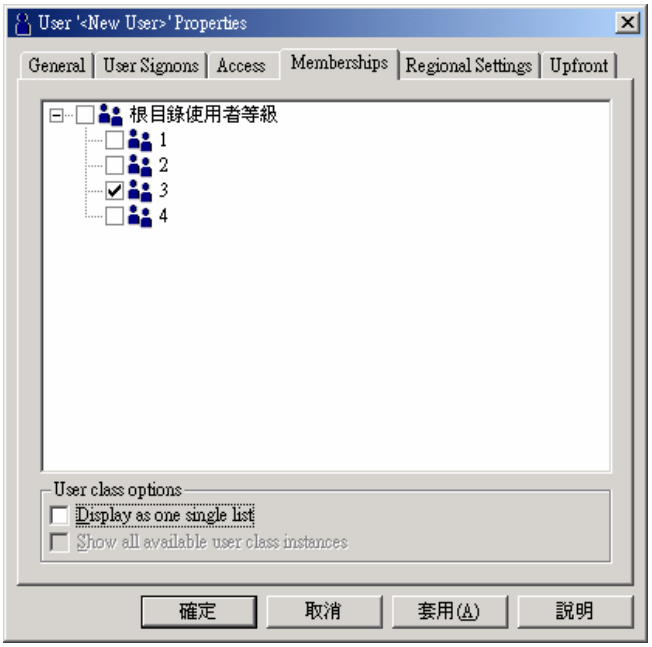


圖 5.37 新增使用者的設定畫面-2

Step 8. 完成認證部分。

二 授權部分

Step 1.開啟位於程式集 Cognos 資料夾中的 PowerPlay transformer，進入系統主畫面。

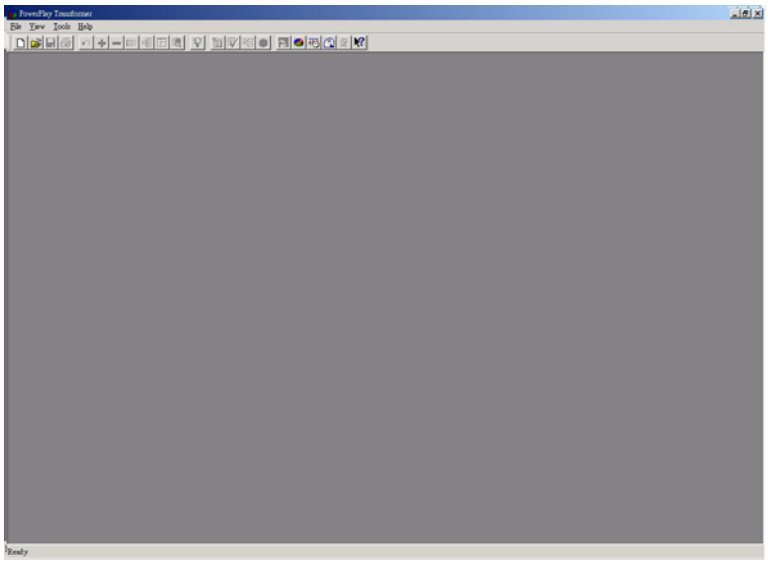


圖 5.38　PowerPlay transformer 系統主畫面

Step 2. 載入以製作完成的超方體。

圖 5.39 開啟超方體畫面

Step 3. 載入超方體後，接下來則要載入以建立的權限使用者名單，點選 File/Model Properties 在 Authentication 的兩個選項打勾。

圖 5.40 載入權限

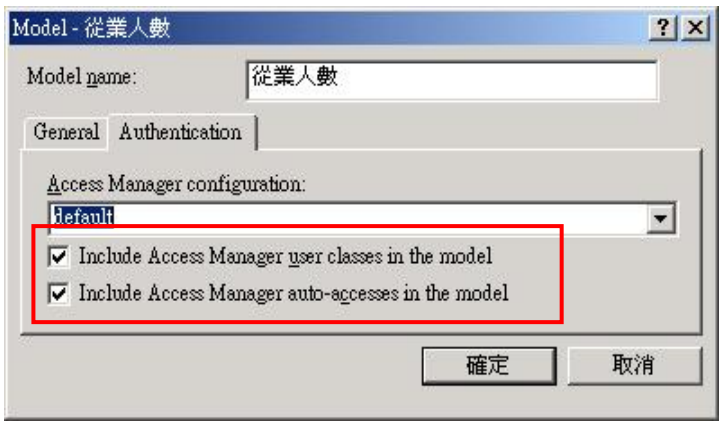


圖 5.41 載入權限-2

Step 4. 再右下角的視窗會出現在 AccessManager 的使用層級權限名單。

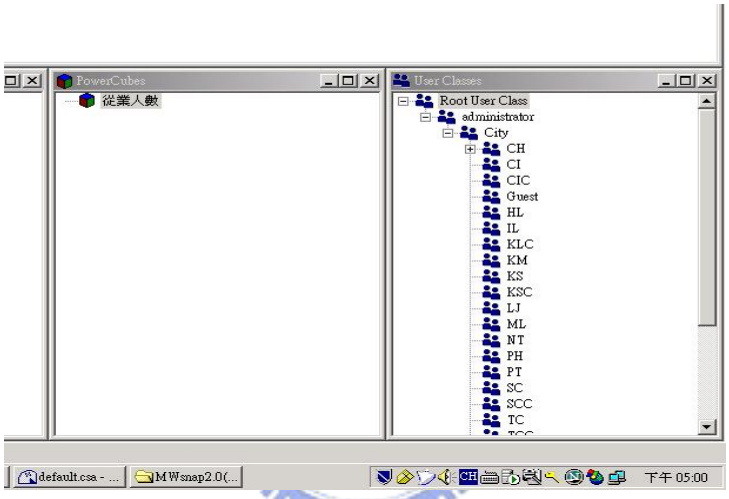


圖 5.42 完成使用層級名單載入

Step 5. 將此超方體欲開放的使用層級拖曳到左邊超方體的視窗，作為超方體授權的權限名單。

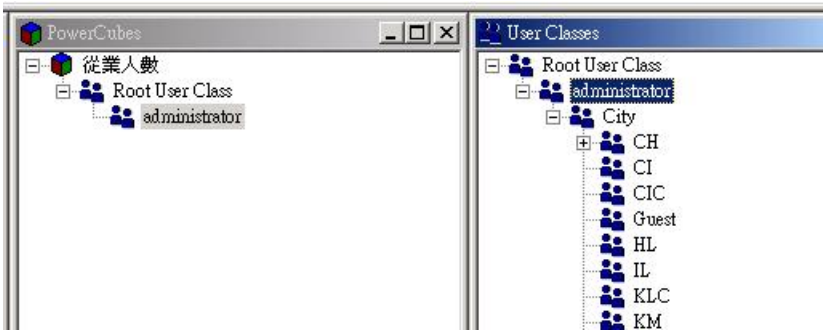


圖 5.43 拖曳使用層級

Step 6. 在完成授權名單後，接下來點選框選的圖示，建立權限的範圍。

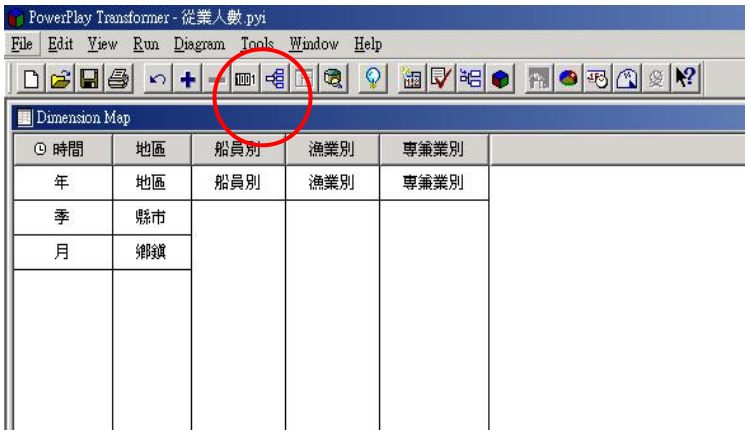


圖 5.44 建立權限範圍

Step 7. 將權限名單展開，在欲設定權限的維度按滑鼠右鍵，點選 Use Custom View 設定維度的開放程度。

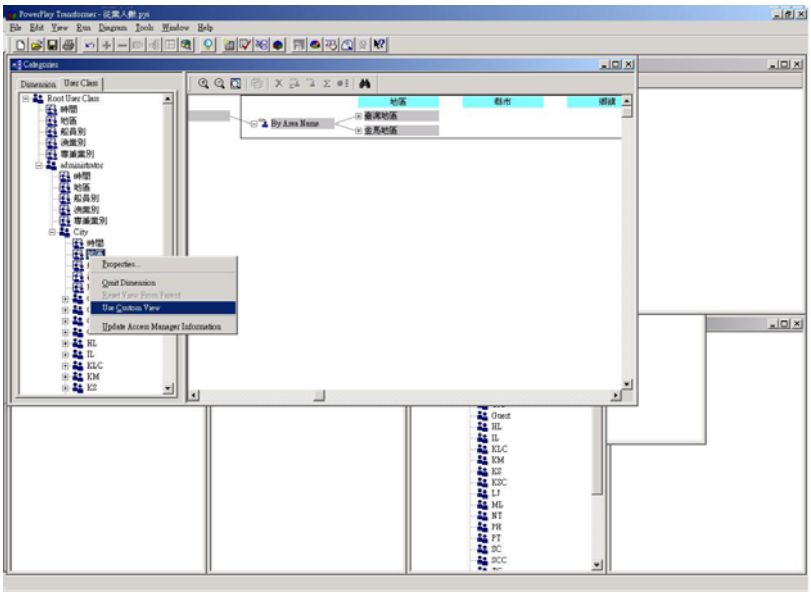


圖 5.45 維度開放設定

Step 8. 在展開的維度上，選取欲限制的方式，Apex 為只開放此地區的權限，其他地區則不會顯示。

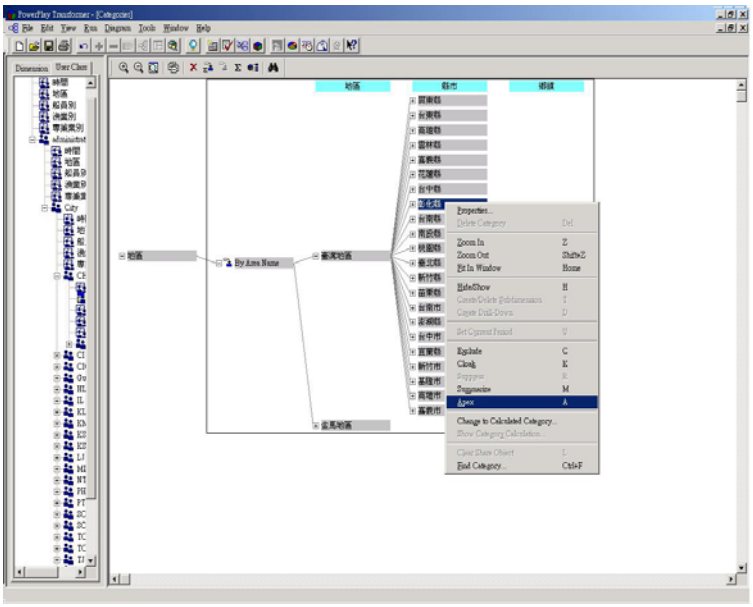


圖 5.46　Apex 限制功能

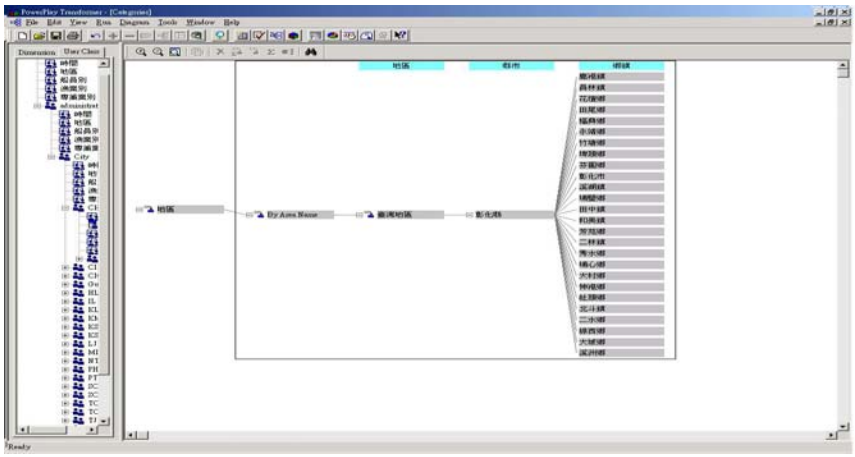


圖 5.47　Apex 限制功能-2

Step 9. 而 Summarize 則是將只顯示到設定的下探深度，此維度更深層的資料都不顯示，只顯示加總的結果。

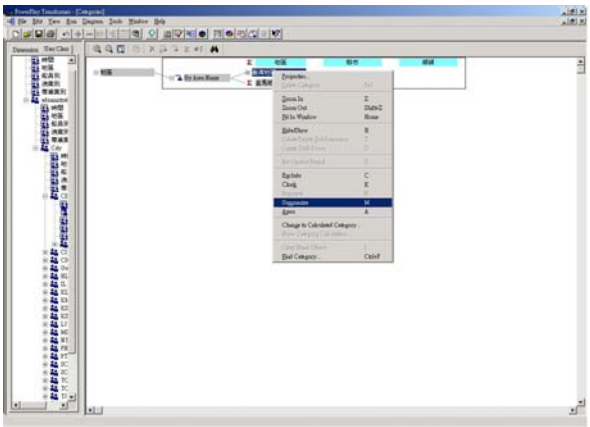


圖 5.48　Summarize 限制功能

Step 10. 完成設定後，按下建立超方體按鈕，開始進行超方體的自動設定處理。

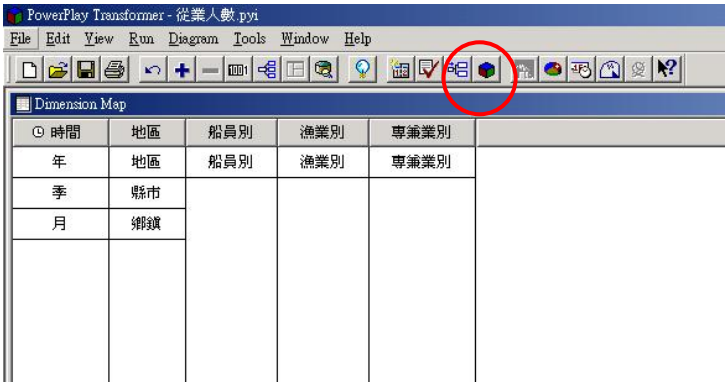


圖 5.49 產生超方體

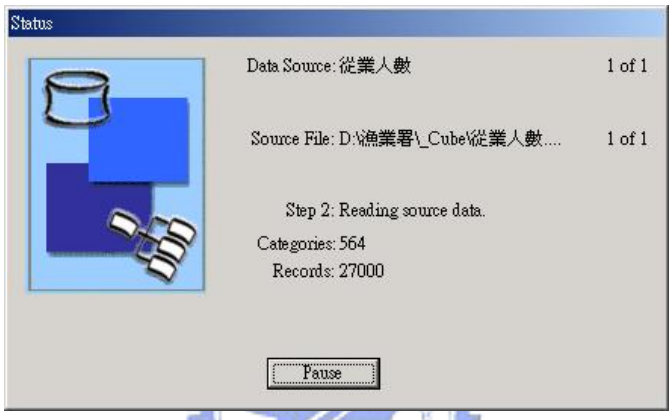


圖 5.50 產生超方體過程

第六章 審計查詢系統

在存取控制中，最後一個階段為審計，漁業資訊分享熱線的審計系統建置將在此章節進行介紹。在 6.1 節會介紹的審計系統的架構，6.2 節將介紹漁業資訊分享熱線審計系統的建置流程。

6.1 漁業資訊分享熱線審計系統的架構

為了能夠紀錄每一位使用者登入以及使用的存取狀況，將會利用 Cognos 的 PPES 中，開啟 Auditing 的功能，系統即會每日產生一個 ppes_audit.log 記錄檔。此紀錄檔包含了登入時間、登入使用者層級、使用之維度以及使用者帳號等資訊，透過這些紀錄即可作為查詢的來源檔。

首先將這些來源紀錄檔藉由檔案轉移服務傳送到審計伺服器，接著利用審計伺服器的 SQL server 所提供的檔案轉換服務，進行資料的篩選以及格式的統一與資料整理，在完成資料的整理以後，即將完成的資料匯入資料庫，完成審計資料的建置與存放。最後則利用動態網頁程式語言撰寫動態查詢網頁，在動態網頁的部份，本系統選擇利用 ASP 的語法，連結資料庫，建構審計查詢系統。圖 6.1 說明了整個漁業資訊分享熱線審計系統的架構。

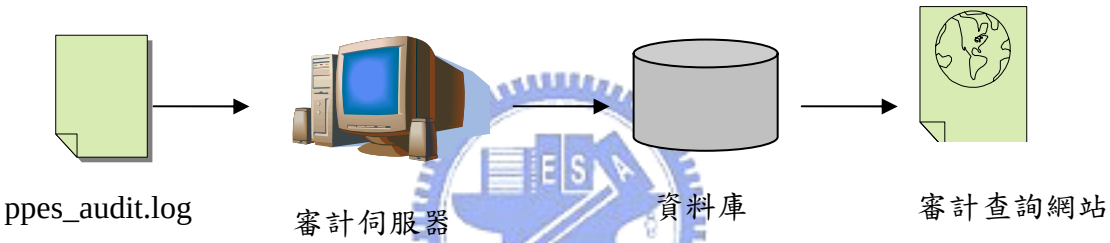


圖 6.1 漁業資訊分享熱線審計系統架構

本系統的設計架構是屬於主從式架構，主從式架構屬於一種分散式的架構，透過分散式的概念，將系統處理所產生的部份負荷，分散至客戶端。客戶端則是提出服務的一端，伺服端則為提供服務的一端。主從式架構則有別於以往的檔案伺服器，取而代之的是資料庫伺服器，資料庫伺服器中，包含了資料庫管理系統，集中管理系統的所有資料。

在主從式架構中，有分二層式架構與三層式架構，本系統屬於三層式架構。在三層式架構中，主要包含客戶端為最前端，中間則為應用程式伺服器，最後端則是資料庫伺服器。

在本系統中，應用程式伺服器則為審計伺服器，當客戶端連線進入審計伺服器後，在客戶端提出服務的請求後，審計伺服器則會與資料庫伺服器建立連線，取得相關的資料，再經由審計伺服器以網頁的方式呈現到客戶端。

6.2 漁業資訊分享熱線審計系統的建置

在 6.2 節將介紹審計系統的建置過程，分為兩個小節，在 6.2.1 節介紹來源紀錄檔的處理，6.2.2 節介紹審計系統的建置與設計。

6.2.1 來源紀錄檔的處理

在進行審計系統建置之前，必須先針對 PPES 所產生的紀錄檔進行前置處理，此紀錄檔的名稱為 ppes_audit.log 檔案，此檔案於每日都會新增一筆。下圖為紀錄檔轉入 Excel 後的詳細內容。

	A	B	C	D	E	F	G	H
1		TimeStemp	TimeZone	SessionID	RequestID	ComponentID	MessageForma	Message
2	I	2005-05-04:18:46:14.484	台北標準時間	62093	3a8	PPRQ	-	PWQ,/從業人數,D:/漁業署/_Cube/從業人數.mdc
3	I	2005-05-04:18:46:15.328	台北標準時間	62093	3a8	PPDS	USR	Administrator
4	I	2005-05-04:18:46:15.328	台北標準時間	62093	3a8	PPDS	UC	All User Classes
5	I	2005-05-04:18:46:15.343	台北標準時間	62093	3a8	PPRQ	-	The request has completed.
6	I	2005-05-04:18:46:21.468	台北標準時間	62093	3a9	PPRQ	-	PWQ,/從業人數,D:/漁業署/_Cube/從業人數.mdc
7	I	2005-05-04:18:46:21.500	台北標準時間	62093	3a9	PPDS	USR	Administrator
8	I	2005-05-04:18:46:21.500	台北標準時間	62093	3a9	PPDS	UC	All User Classes
9	U	2005-05-04:18:46:21.500	台北標準時間	62093	3a9	PPDS	PPUH	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,
10	U	2005-05-04:18:46:21.500	台北標準時間	62093	3a9	PPDS	PPUD	48,34,0,0,0,0;36,12,0,34,0,0,0,0,0;51
11	I	2005-05-04:18:46:21.500	台北標準時間	62093	3a9	PPRQ	-	The request has completed.
12	I	2005-05-04:18:46:24.937	台北標準時間	62093	3aa	PPRQ	-	PWQ,/從業人數,D:/漁業署/_Cube/從業人數.mdc
13	I	2005-05-04:18:46:25.046	台北標準時間	62093	3aa	PPDS	USR	Administrator
14	I	2005-05-04:18:46:25.046	台北標準時間	62093	3aa	PPDS	UC	All User Classes
15	U	2005-05-04:18:46:25.046	台北標準時間	62093	3aa	PPDS	PPUH	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,
16	U	2005-05-04:18:46:25.046	台北標準時間	62093	3aa	PPDS	PPUD	115,115,0,0,0,0;23,92,0,5,110,0,0,0,0;115
17	I	2005-05-04:18:46:25.046	台北標準時間	62093	3aa	PPRQ	-	The request has completed.
18	I	2005-05-04:18:46:26.421	台北標準時間	62093	3ab	PPRQ	-	PWQ,/從業人數,D:/漁業署/_Cube/從業人數.mdc
19	I	2005-05-04:18:46:26.453	台北標準時間	62093	3ab	PPDS	USR	Administrator
20	I	2005-05-04:18:46:26.453	台北標準時間	62093	3ab	PPDS	UC	All User Classes
21	U	2005-05-04:18:46:26.453	台北標準時間	62093	3ab	PPDS	PPUH	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,
22	U	2005-05-04:18:46:26.453	台北標準時間	62093	3ab	PPDS	PPUD	25,25,0,0,0,0;5,20,0,0,5,20,0,0,0;25
23	I	2005-05-04:18:46:26.453	台北標準時間	62093	3ab	PPRQ	-	The request has completed.
24	I	2005-05-04:18:46:27.828	台北標準時間	62093	3ac	PPRQ	-	PWQ,/從業人數,D:/漁業署/_Cube/從業人數.mdc
25	I	2005-05-04:18:46:27.859	台北標準時間	62093	3ac	PPDS	USR	Administrator
26	I	2005-05-04:18:46:27.859	台北標準時間	62093	3ac	PPDS	UC	All User Classes
27	U	2005-05-04:18:46:27.859	台北標準時間	62093	3ac	PPDS	PPUH	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,
28	U	2005-05-04:18:46:27.859	台北標準時間	62093	3ac	PPDS	PPUD	20,20,0,0,0,0;0,5,15,0,4,16,0,0,0;20
29	I	2005-05-04:18:46:27.859	台北標準時間	62093	3ac	PPRQ	-	The request has completed.

圖 6.2　ppes_audit.log 檔案內容

由上圖可了解在每一位使用者登入後，將會記錄使用者瀏覽的詳細資訊，下表將解釋每個格式的主要意義。

表 6.1 PPES_AUDIT.LOG 欄位說明

欄位名稱	欄位說明
TimeStemp	記錄登入日期及時間
TimeZone	地域時間的區別
MessageFormat	訊息格式：說明 Message 的欄位資訊
Message	訊息內容：資料倉儲名稱、使用者帳號與類別、瀏覽維度

6.2.2 審計系統之設計

首先利用檔案轉移服務的自動化程序中的排程上傳功能，此功能可以事先設定本端資料夾路徑，並於每日固定時間進行傳送。而在 SQL server 則設計檔案轉換服務，並設定排成為每日執行，將經由檔案轉移服務所送入的檔案進行匯入的動作，在匯入的過程中，就先將匯

入的欄位設定，達到篩選的目的。下圖為檔案轉換服務的設定。

圖 6.3 檔案轉換服務

在完成匯入後，開始進行動態網頁的建置，本研究採用 ASP 語法來撰寫動態網頁連結資料庫的程式。在網頁中如圖 6.4，主要提供日期區間查詢、資料倉儲查詢、使用者層級查詢，查詢條件為:

一、日期區間查詢：查詢者可利用下拉式選單來選擇所要查詢的日期。

二、資料倉儲查詢：由於漁業資訊分享熱線包含了九個資料倉儲，此查詢可選擇九個資料倉儲的詳細讀取內容。

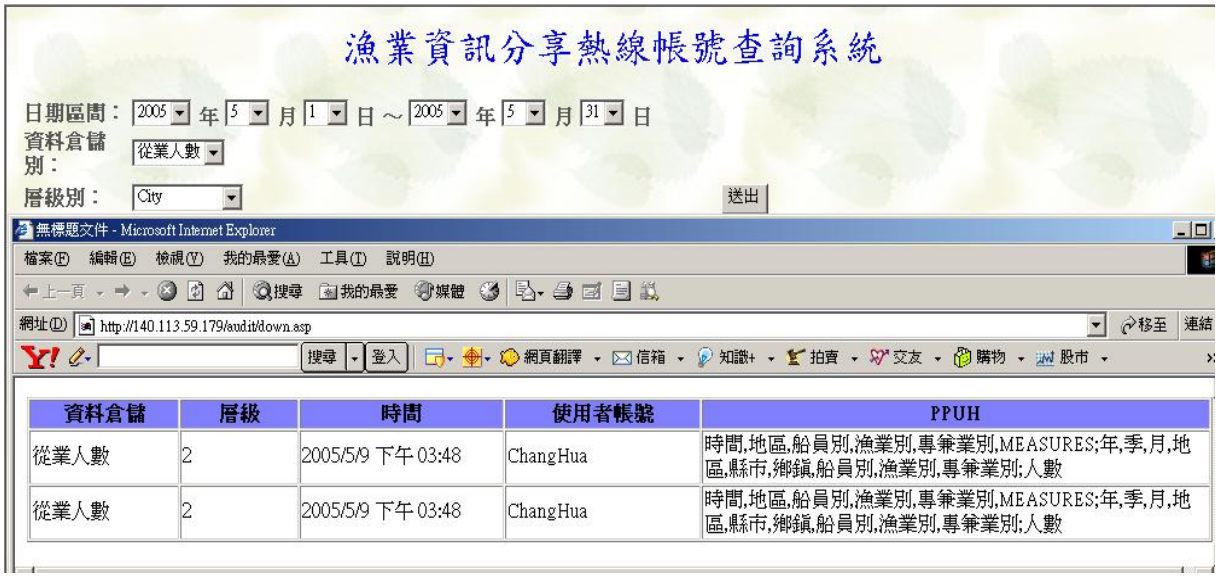
三、層級別：在本系統，主要層級分為四層，選擇四個不同層級來查詢。

資料倉儲	層級	時間	使用者帳號	PPUH
沿近海	0	2005/5/9 下午 03:48	Administrator	時間,地區,漁獲生物種類維度,漁業作業種類維度,MEASURES;年,季,月,地區,縣市,鄉鎮,漁市場,漁獲總計,漁獲大類,漁獲名稱,漁業別總計,漁業別大類,漁業別名稱;交易量,自用及其他估計量,總產量
沿近海	1	2005/5/19 下午 03:4	Manager	時間,地區,漁獲生物種類維度,漁業作業種類維度,MEASURES;年,季,月,地區,縣市,鄉鎮,漁市場,漁獲總計,漁獲大類,漁獲名稱,漁業別總計,漁業別大類,漁業別名稱;交易量,自用及其他估計量,總產量
沿近海	2	2005/5/9 下午 03:48	ChangHua	時間,地區,漁獲生物種類維度,漁業作業種類維度,MEASURES;年,季,月,地區,縣市,鄉鎮,漁市場,漁獲總計,漁獲大類,漁獲名稱,漁業別總計,漁業別大類,漁業別名稱;交易量,自用及其他估計量,總產量
從業人數	0	2005/5/4 下午 06:46	Administrator	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,縣市,鄉鎮,船員別,漁業別,專兼業別;人數
從業人數	2	2005/5/9 下午 03:48	ChangHua	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,縣市,鄉鎮,船員別,漁業別,專兼業別;人數
從業人數	2	2005/5/9 下午 03:48	ChangHua	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,縣市,鄉鎮,船員別,漁業別,專兼業別;人數
進出口	0	2005/5/12 下午 03:4	Administrator	時間,水產別,國家別,進出口別,製品別,MEASURES;年,季,月,水產別,國家別,進出口別,製品別;當月數量,當月重量,當月價值,累積數量,累積重量,累積價值

圖 6.4 審計資訊網

6.2.3 審計系統之使用說明

在審計系統的使用說明中，將透過例子的操作，進一步的深入介紹此系統的功能。在本系統可查詢的項目有日期區間、資料倉儲、以及層級別。假設此時系統管理者欲透過本系統查詢五月份從業人數的城市層級使用者，此時使用者進到此系統後，可以透過本系統的查詢項目，在日期區間選擇 2005 年 5 月 1 日到 2005 年 5 月 31 日的資料，在資料倉儲別可選擇從業人數資料倉儲，而在層級別可以選擇 CITY 層級。選取完畢後，按下送出，就可以透過動態網頁顯示出查詢的結果。以下圖片就是查詢的結果。



資料倉儲	層級	時間	使用者帳號	PPUH
從業人數	2	2005/5/9 下午 03:48	ChangHua	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,縣市,鄉鎮,船員別,漁業別,專兼業別;人數
從業人數	2	2005/5/9 下午 03:48	ChangHua	時間,地區,船員別,漁業別,專兼業別,MEASURES;年,季,月,地區,縣市,鄉鎮,船員別,漁業別,專兼業別;人數

圖 6.5 查詢系統結果

第七章　結論及未來研究方向

7.1 結論

漁業署內部的資料大部分都是每日進行更新，分別存放在三大異質性資料庫中。全省有許多的單位對於資料庫中的資料都相當的倚重。在漁業署的三大異質性資料庫尚未整合之前，漁業署在每年年報的分享上，無論是在資訊擷取的面向或者是權限控管的面向上，都存在著許多的不便。在三大異質性資料庫進行整合並建立漁業資訊分享熱線後，除了解決了傳統年報上的不便外，也提供了許多附加的價值，並大幅的提升了漁業署的資訊效率以及安全機制，這些優點也都一再的凸顯了資料倉儲化對於不論是公司行號或是企業團體，都將帶來許多正面的價值。

在本研究中，針對資料倉儲建置過程的兩大階段進行研究與實作。透過檔案轉移服務，將原本分散在三個異質性資料庫的資料，能夠集中到一台資料倉儲伺服器中，進行檔案轉換服務的處理。在這過程中，為了要克服三個異質性資料庫所使用的作業平台之不同，而利用 JAVA 程式語言來撰寫，達到服務跨平台的目的。資料倉儲建置的後端部分為存取控制，在整各資料倉儲系統中，扮演了非常重要的角色。當三大異質性資料庫在完成整合後，資料倉儲伺服器的資料庫，包含了各種層級不同權限的資料。資料倉儲的建置與漁業資訊分享熱線的目的在於資訊分享，資料權限有層級之分，就產生資訊分級的必要性。因此資料倉儲的最後一個階段就是透過存取控制的觀念，達到資訊分級的目標。

存取控制的部份主要建立在三個基礎之上:認證、授權以及審計。在認證的部份，本研究引用了多頭狗認證的技術，透過第三方認證以及安全金匙的方式，避免密碼在通訊協定間進行傳遞，大幅提高認證過程的安全性。在授權的部份，利用名錄存取伺服器的原理，將使用者的權限資料特別存放到名錄伺服器，當資料倉儲伺服器在完成使用者認證後，須進行權限索取時，可以透過 SSL 安全機制與名錄伺服器連線讀取，名錄伺服器的資料庫特殊的排列模式可以大幅的提升權限存取的效率，達到降低系統負荷的目標。最後於審計的部份，主要目的是對於系統存取的使用者與動作能夠進行監督，進而確保資料的完整性、安全性與正確性。在使用者帳號的編制則是利用植基於角色式存取協定，打破以往使用者帳號與權限的直接關聯，兩者之間加入角色因子，透過角色間接達到使用者帳號與權限的關聯。其好處在於能夠省去相同權限帳號的重複建置，取而代之的是利用繼承的方式讓使用者帳號直接取得角色的權限。在利用植基於角色式存取協定達到使用者帳號負荷的降低後，藉由資料倉儲軟體 Cognos 中的 PPES 來啟動紀錄檔的方式，透過紀錄檔藉由篩選、萃取與淨化的檔案轉換服務，將紀錄檔轉入資料庫，並藉由 ASP 動態網頁的方式來進行查詢的動作，達到資料存取追蹤的目的。

本研究在針對漁業署漁業資訊分享熱線的建置過程，首先克服跨平台的障礙，進而能夠將三大異質性資料庫的資料統一整合到單一資料倉儲資料庫。引用存取控制的新技術，建立了漁業資訊分享熱線的權限層級存取，並大幅降低系統負荷，提高系統整體運作效率，也減低管理者在進行安全性審查管理的複雜度。

在完成檔案轉換服務後，完成漁業三大資料庫的整合後，大幅的降低漁業署的資訊分享成本，從原本需要大批人力編輯彙整以及大量印刷成冊的龐大花費，減低到只需要定期維護，就可以及時的提供資訊分享服務，不論在時間上或成本上都提供了非常實質的貢獻。

7.2 未來研究方向

在本研究中，實作了資料倉儲的檔案轉移服務以及存取控制，透過檔案轉移服務能夠將檔案在不同的電腦間進行傳送，並利用存取控制來管制使用者的存取動作，在存取控制的認證以及授權都引用了目前最新的技術來作為建構的基礎。在審計的部分，則只進行了初步的建構，簡單的提供記錄以及查詢的功能。透過 PPES 所建立的紀錄檔，萃取當中的資訊，可以監控目前漁業資訊分享熱線的使用情形，既然是監控，審計系統在接續的研究中，建議能夠設計為及時傳訊的方式，如此一來才能夠做到事先預防，在出現異狀的同時就能夠馬上終止服務，而不需每次按查詢功能來更新存取情況。

如果能夠做到及時的更新內容的話，可以再配合專家系統的技術，事先將有可能存取異常的動作列出，藉由及時更新內容的方式，透過專家系統自動比對，如果有出現異狀，就可以提出警告。而在異狀條件可以依照可能性先分級，如果此異狀條件先前有發生過，表示此異狀條件的可信度很高，亦即出現存取異狀的可能性也相對高，就能夠將此條件的可能性等級調高，慢慢更新專家系統的資料庫，達到審計系統自動化的目標。