自然人憑證結合人事差假系統

何岳剛 蘇巨鋒 廖偉吏 鄭致瑋 湯媛喬 李封儒 丁德榮*
*國立彰化師範大學資訊工程學系
*E-mail: deron@cc.ncue.edu.tw

摘要

學校現有之人事差假作業主要是以人工方式進行遞交審核，請假人員必須親自將假單經過一層又一層的關卡遞送簽核，過程繁雜且耗時。有鑒於現今網路的發達，校園 E 化的普及，以及內政部大力推行自然人憑證的趨勢，特將自然人憑證與網際網路資料庫的技術，結合彰化師大現有之人事系統建立人事差假管理系統。以期能使請假手續的進行更快更方便且系統化，隨時隨地都可以辦理請假或簽核假單之手續。希望透過此系統的建置，可以節省人力資源，降低人為疏失且顧及資料的安全性。未來還可以將自然人憑證技術擴充至其他校內行政系統的整合與建置，以達到單一登入與校園 E 化之目標。

關鍵詞：自然人憑證，人事差假系統。

1. 簡介

隨著網路技術的蓬勃發展以及資訊技術的進步，人事室對於利用網路來處理請假資料的需求也逐漸增加。因應龐大的人事請假資料處理量和便利請假流程，推動網路請假系統的研發是不可免的趨勢。所以網路請假系統的發展將有助資料的存取、核對與保存；對人事室來說，可以增進效率並節省人力成本。對於教師、校務行政人員、人事室人員而言，透過網路進行網路請假，能使員工、人事室人員快速掌握完整的請假資料，有助於員工的請假、出差，人事室人員的維護與分析工作，進而提昇學校的請假服務品質。

網路請假的優點，除了假單資料儲存與傳遞便利外，網路請假系統可以根據使用者的角色(如教師、行政人員、長官、代理人、人事人員等)呈現個人之相關請假資訊與簽核管理的功能與介面。網路請假的流程有嚴謹的控制，較紙本假單傳遞易於進行，不需親自送往各階層主管，減少一層層簽核時間的耗費。請假網路化後，查詢人事差假資料極為便利，將可以提昇行政效率、服務品質及節省人事室的人力與空間。更重要的是，電子化的資料可以隨時做統計分析，將可協助校方及人事室人員做最適當的決策支援。

除此之外，並不會因網路化而使得人事資料，或各項私人機密資料外流，使用自然人憑證[8][9]，可確保其高度安全性及不可仿冒唯一性，讓使用者能安心使用本系統，而無其他顧慮。並希望能因使用 WEB 介面，使得使用者能更容易操作，不僅是已申辦自然人憑證者能使用，未申辦者也可以透過帳號密碼使用。

學校現有之人事差假作業主要是以人工方式進行遞交審核，請假人員必須親自將假單經過一層又一層的關卡遞送簽核，過程繁雜且耗時。有鑒於現今網路的發達，校園 E 化的普及，以及內政部大力推行自然人憑證的趨勢，特將自然人憑證與網際網路資料庫的技術，結合彰化師大現有之人事系統建立人事差假管理系統。以期能使請假手續的進行更快更方便且系統化，隨時隨地都可以辦理請假或簽核假單之手續。希望透過此系統的建置，可以節省人力資源，降低人為疏失且顧及資料的安全性。未來還可以將自然人憑證技術擴充至其他校內行政系統的整合與建置，以達到單一登入與校園 E 化之目標。

2. 背景知識

2.1 自然人憑證(Citizen digital certificate， CDC)

自然人憑證(Citizen digital certificate， CDC)[8][9]，就是電子身份證IC卡，以可以稱作是網路上的身分證，可以防範網路上常見的資訊安全攻擊(表1)。由表1可見，自然人憑證除了能夠用來確認網路上的身份之外(不可否認性)，還可確認資料的完整性及機密性，是當下維護資訊安全不可獲缺的重要技術與工具。

表1 電子認證技術之通訊安全服務

資訊安全服務項目	抵抗威脅	可採取防護技術
資料機密性服務(Confidentiality)	竊聽、非法取得資料、資料洩漏	加密系統、數位信封
資料完整性服務	竄改、重送、損壞	訊息認證碼、MAC、安全雜湊函數數位簽章、序碼(Serial)或時戳(Time)
資料來源認證服務(Authentication)	冒名傳送假資料	訊息認證碼、MAC、數位簽章
不可否認服務(Non-repudiation)	否認已接收資料、否認已傳送資料	數位簽章
存取控制服務(Access Control)	非法存取資料	可信賴作業環境、防火牆系統、身分卡

因為自然人憑證採用公開金鑰(Public Key Infrastructure，PKI)的架構[10]，所以需要一個公正的第三者(Certification Authority，CA)，以及註冊中心(Register Authority，RA)的建置。圖1為PKI架構

圖[10]，其中CA是指憑證管理中心(使用X.509 v3憑證格式)，負責執行憑證簽發、廢止、管理等核心作業，以及將簽發之憑證資料及憑證廢止清冊（Certificate Revocation List， CRL）公佈於目錄伺服器，以供外界查詢及下載。而RA為前端註冊管理中心，負責執行憑證申請、廢止及資料審核等作業。RA透過資料庫比對、臨櫃或書面資料審核等方式進行身分認證，以核發憑證。關於自然人所使用之密碼模組部分[9][10]包含：雜湊運算演算法、非對稱式加解密運算法、非對稱式加解密運算法。其中雜湊運算演算法部分，分別使用了MD5和SHA_1，雜湊運算後的長度分別為16(MD5)及20(SHA_1)個位元組長。非對稱式加解密運算法有RSA，對稱式加解密運算法有: DES CBC、DES ECB、3DES CBC、3DES ECB等四種。

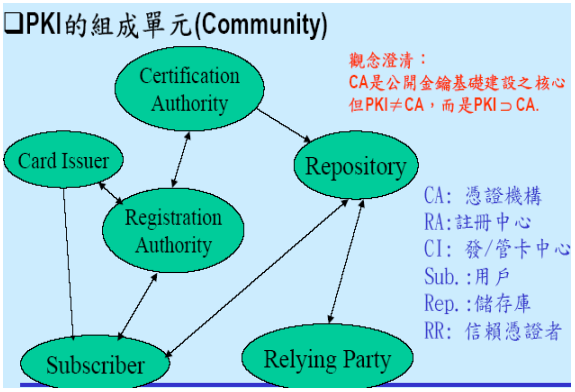


圖1 PKI的架構

自然人憑證的加解密的部分，方法參照 PGP 加解密的方法[10]來實作，使用數位簽章加數位信封的方式，非對稱式加密的私鑰長度 1024 bits，對稱式金鑰(session key)隨機產生 24 bits 的長度，很難被破解，且每次使用的 session key 皆不同，在安全性上有保障。其加密部分如下(圖 2)，解密部分如下(圖 3)。

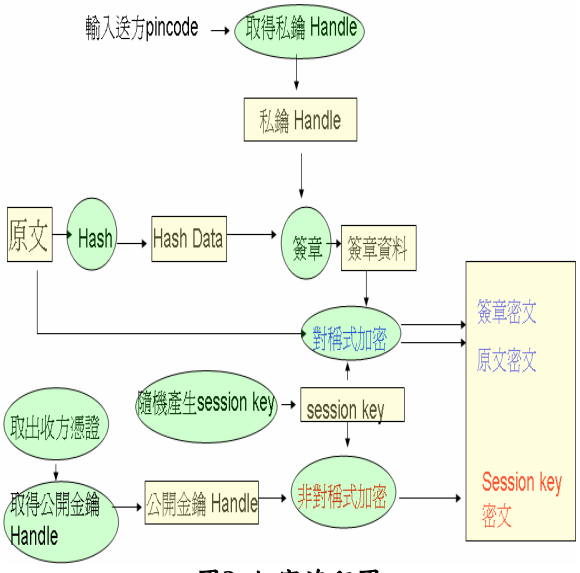


圖2 加密流程圖

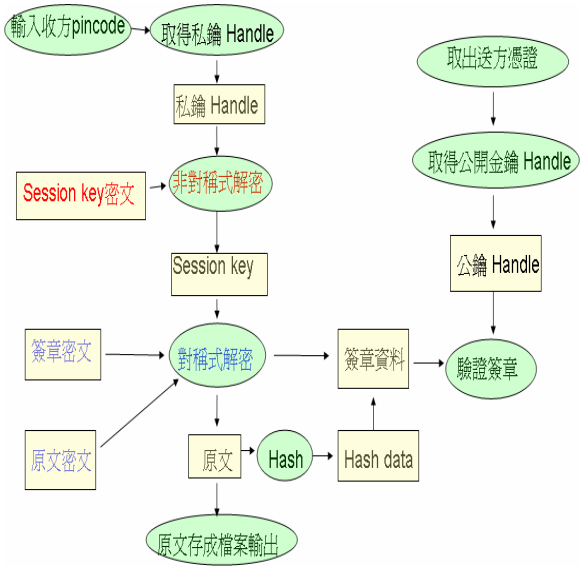


圖3 解密流程圖

2.2 PHP 技術

PHP[4][6]是網頁程式撰寫者常用的選擇，其功能強大、支援資料庫、網路連結，且具有跨平台的優點。支援多項的作業系統平台，包含：UNIX、Win32(NT/95/98/2000/XP)... 等；亦支援多種網站伺服器，如：Apache、CGI、FastCGI、JDBC API（Java Database Connectivity）…等，並擁有多種高發展性的應用程式特性：擴充性(Scalable)、高效能(Efficient)、安全性(Secure)、模組化(Modular)、多層式(Multi-tiered)，故以PHP語言設計本系統。

2.3 ORACLE 資料庫

網路服務系統的建置均以資料庫連結管理儲存資訊。在資料庫系統方面，我們選用ORACLE資料庫系統[7]作為系統後端資料庫。因為ORACLE能提供極高的安全性及強大的資料庫排程功能，使得系統資料能更有效更安全的運作與儲存。除此之外，ORACLE提供了PL/SQL語法，讓程式設計師能使用工具來強化資料庫系統存取。ORACLE資料庫可以安裝於不同的作業系統，具極佳的穩定性，提供很強的搜尋功能，與安全與管理的服務工具程式。另外，因為現有的校務行政系統也使用ORACLE作為資料庫，對於我們整合現有的校務行政系統的幫助上是一項很好的選擇。

2.4 人事差假行政系統

本校人事室現有之人事請假資料管理與維護的作業方式為：校內教職員工以書面方式遞交假單，經過各級主管審核通過後，滙整至人事室集中處理，再利用現有的電子表單，以人工作業登錄。主來以人工處理相關資料，再將資料彙整歸類，以紙本方式儲存收藏並輔以資料庫建立，便於未來查詢之用。

目前的請假審核方式主要是先經由直屬主管簽

核完畢，再送交單位主管簽核，最後呈送二級主管簽核完畢即可。除非請假超過 14 天以上或是二級主管請假，不需呈送一級主管(校長)簽核。目前管理審核仍須以人工方式一層一層上呈處理，且資料處理方面仍是以手動輸入建檔為主，費時且耗力，如需代請假或補請假則過程鎖繁雜，且有個人資料外流之疑慮，未符合個人資料保密的原則。

3. 系統設計

3.1 系統規劃

（1）系統實作功能說明

系統功能包含：

①使用者管理：對所有使用者做統一之管理，並結合現有之人事系統管理其差假資料。

②請假管理：將請假、補請假設計為簡單明白、易於使用，以 Web-base 系統簡化作業流程，加快請假處理速度，改善以往紙本請假耗費冗長時間之缺點。

③差假管理：對出差各項事宜：差費申請、加班費、不休假獎金…等，做好詳細管理。

④憑證管理：隨時更新、檢查憑證狀況，確保請假安全。並結合現有教職員之電子郵件、帳號密碼進行雙重登入工作。

⑤差勤管理：紀錄員工每日刷卡出勤狀況，隨時可補刷卡或調閱刷卡紀錄，並與差假系統做完整與一致性的查核。

⑥線上簽核：各級主管與其職務代理人能迅速且有效的線上簽核各項假單，當有相關的假單需要簽核時，均能以 e-mail 通知相關的人員，提供便利的連結供簽核，以節省行政上繁雜無謂的時間。

⑦統計報表列印：可列印各相關人事差假統計資料，作為個人與人事室人員查閱、分析與存檔之用。

（2）系統軟硬體需求

本系統是以個人電腦為發展平台，其開發時所採用的硬體配備與軟體系統版本說明如圖 4 與表 2。

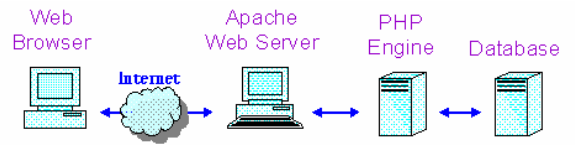


圖 4 系統使用環境

表 2 使用環境

瀏覽器端	ActiveX 搭配 VBScript，網頁部分使用 Xhtml，PHP，及 JavaScript 並使用 CSS 將版面一致化。
伺服器端	Windows NT 系統的 Apache Web Server。
資料庫端	Oracle 10g 教育版。

4. 系統設計

系統架構圖如下(圖 5)

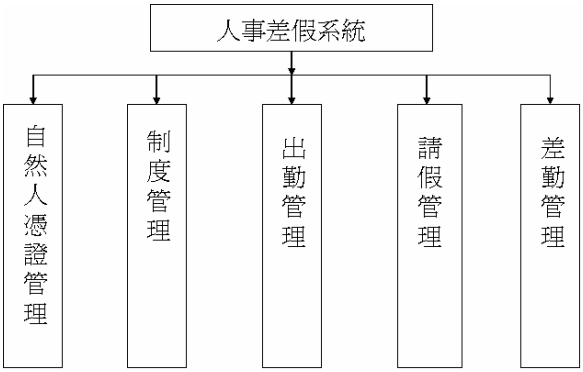


圖 5 人事差假系統

4.1 自然人憑證管理

4.1.1 用於登入部分

(1)使用者插入卡片後輸入 pincode 作為判斷依據。(2) Pincode 正確後使用私鑰對 Timestamp 作簽章，上傳至 Server 端做驗證，驗證正確即可登入。(3)使用者沒有自然人憑證則使用現有員工帳號密碼登入。

4.1.2 用於加解密部分

(1)使用者可選擇需加密的檔案。(2)使用數位簽章與數位信封方式，需使用對方憑證內公鑰。(3)使用者沒有自然人憑證則使用 PHP 製作的加密函式。

4.1.3 私鑰簽核

(1)主管使用自己的私鑰於請假時做簽核動作，上傳至伺服器端儲存。(2) 使用者對於自己的假單有疑惑，可以查詢簽核檔，即可知道請假記錄是否正確。

4.1.4 憑證狀況查詢

(1)憑證管理者專用功能。(2)系統每日固定下載 CRL 檔，並且檢查各憑證，是否有廢止，或到期。

4.2 制度管理

制度管理功能架構圖如(圖 6)所示。

4.2.1 年度假日行事曆資料維護：

以行事曆的模式進行新增、刪除、修改國定假日、臨時補假(如颱風假)。

4.2.2 員工基本差勤資料維護：

新增、刪除、修改以及查詢員工(教師、職員或兼任)之休假出差資料記錄。

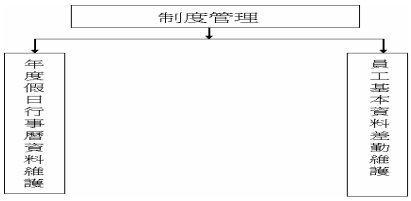


圖 6 制度管理

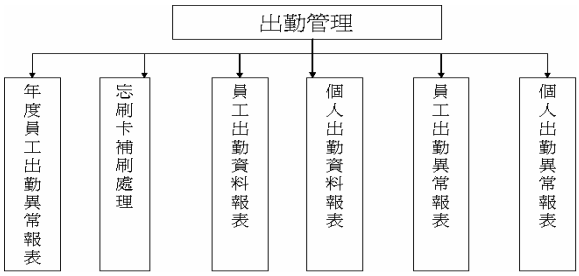


圖 7 出勤管理

4.3 出勤管理

出勤管理功能架構圖如(圖 7)所示。分述如下：

(1)非固定差勤規定組別人員資料：非固定差勤規定組別人員資料的維護功能，新增、刪除、修改、查詢等。

(2)忘刷卡補刷處理：線上申請補刷卡動作，主管審核後自動建檔，完成補刷卡動作。

(3)員工出勤資料報表：查詢特定員工或全部員工於某一時間區間內的出勤資料。

(4)個人出勤資料報表：查詢個人於某一時間區間內的出勤資料

(5)員工出勤異常報表：查詢特定員工或全部員工於某一時間區間內的出勤異常資料，有三種輸出可供選擇，全部列出(依日期)、刷卡未達二次、遲到早退等。

(6)個人出勤異常報表：查詢個人於某一直間區間內的所有異常資料，包含刷卡未達兩次以及遲到早退等。

(7)年度員工出勤異常資料報表：功能同員工出勤異常報表，查詢某一年度間特並員工或全部員工的出勤異常資料。

4.4 請假管理

請假管理功能架構圖如(圖 8)所示。分述如下：

(1)請假資料維護：員工請假資料的維護功能，增加、刪除、修改和查詢。

(2)員工請假資料報表：由管理員輸入請假資料的查詢時間，會顯示出員工請假資料報表。

(3)個人請假資料報表：使用者登入後，輸入報表查詢時間，會顯示出自己的請假資料報表。

(4)員工休假累計表：此報表會顯示出學年開始到目前時間，員工的休假累計報表及各項假別的累計請假天數。

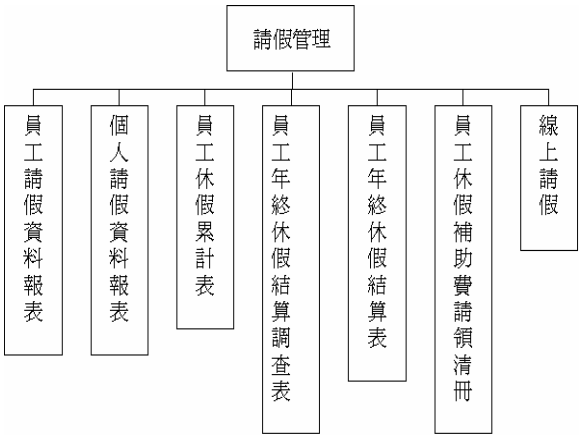


圖 8 請假管理

(5)員工年終休假結算調查：此報表顯示出某個學年度，員工各種假別的休假累計天數，及休假天數。用來給員工確認有沒有錯誤的。

(6)員工年終休假結算表：此報表顯示出某個學年度，員工各種假別的休假累計天數，及總休假天數。

(7)員工休假補助費請領清冊：算出某個學年度，員工的休假補助費，以報表呈現。

(8)線上請假：以自然人憑證卡登入後，填寫線上假單，來線上請假。

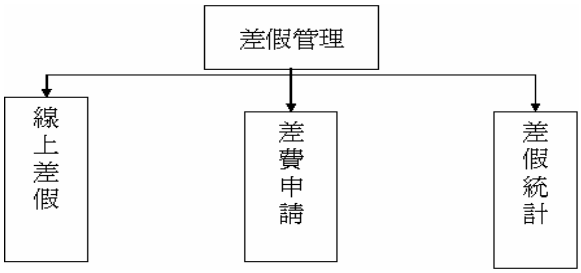


圖 9 差假管理

4.5 差勤管理

差勤管理功能架構圖如(圖 9)所示。分述如下：

(1)線上差假：使用者在登入後，可在線上請假部分請差假，若是申請差假必須要確認使用者身份：

①教師：請差假有課必須通知課務組，若是接受外部專案計畫，必須填寫“出差請示單”。

②職員：除非地點為國外，不需送給校長直接在單位主管便可以核准。

③主管：只要主管請差假，皆需要送至校長核准，才算準假。

(2)差費申請：使用者登入後，可以在線上填寫申請差費表格，附上所需的資料上傳到系統，系統再以 e-mail 的方式傳給各個層級簽核，若有一個層級被拒絕，就被退回且 e-mail 通知申請人與已簽核核准之層級。

(3)差假統計：使用者在線上之“請假部分”選擇“差假統計”即可以列出目前為止差假部分休

假的時數統計。

5. 系統主要畫面

茲將開發完成之系統主要頁面擷取說明如下：(1) 登入介面：員工登入畫面，可選擇使用自然人憑證或帳號密碼登入。(如圖 10)

圖 10 登入畫面

(2) 憑證管理：檢查憑證狀態，每天自動進行更新。(如圖 11)

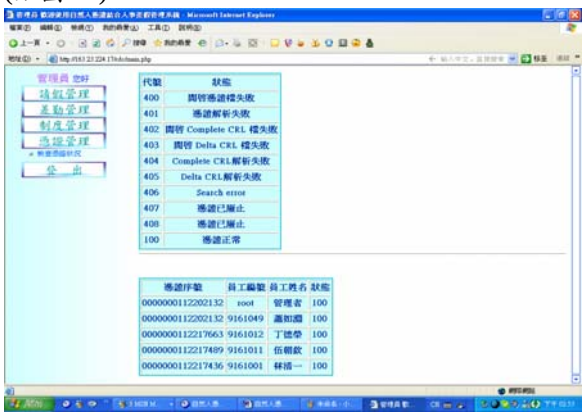


圖 11 憑證管理

(3) 制度管理：管理員工資料、行事曆。(如圖 12)

圖 12 制度管理

(4) 簽核系統：包含主管簽核、職務代理人、補刷卡等簽核頁面。(如圖 13、14)

圖 13 簽核頁面(一)

圖 14 簽核頁面(二)

(5) 線上請假：各種線上請假假別、包含補請假功能。(如圖 15)

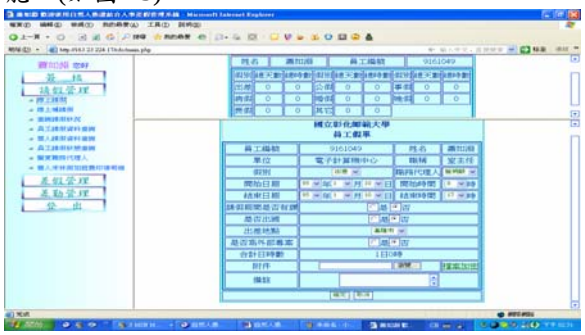


圖 15 請假頁面

(6) 檢查假單：查詢假單狀態，包含已取消、審核中、已完成假單。(如圖 16)

圖 16 查詢假單

(7) 差費申請：出差後 14 天可申請各項出差費用。

(如圖 17)

圖 17 差費申請

(8) 各項報表：各種出差、請假、刷卡紀錄…等，報表明細。(如圖 18)

圖 18 各項報表

6.實作經驗

關於自然人憑證的實作部分，乃是使用中華電信提供的 HiSECURE 函式介面 5.1 版[8][9]，主要是包裝成 C++ 的函式元件，將 C/C++的程式放在網頁上執行，目前較常見的方法是將 C/C++ 的程式製作成 DLL 檔，再透過 Visual Basic(VB)程式去呼叫。再利用 VB 內建的 Package and Deployment Wizard 工具，將所需的 DLL 檔以及相關的程式碼製作成一個 cab 檔。除此之外，亦嘗試過使用其他的方法(如 COM 及 JNI)來實作，但最後使用 Visual C++(VC++)的 MFC 技術，將先前用自然人憑證函式作的程式製作成 ActiveX 控制項[1][3]，而不再經由 VB 多作一層包裝如此，執行速度較快。對於非對稱式加解密部分的實作，則先製作測試憑證，再使用測試憑證對控制項簽章，如此可達到初步的安全性，不會直接被瀏覽器封鎖，之後再用 cab 封裝工具將控制項、inf 檔以及所需的 DLL 檔封裝起來。值得注意的是，需要加入 MSDN[1][3]提供的 mfc42.cab ，才能夠正確的執行 MFC，讓 ActiveX 控制項[1][3]正確的執行。

7. 結論

本論文主要為設計以自然人憑證技術結合人事差假之系統。希望透過此系統的建立，改善請假流程，同時並提供使用上之便利性，進而提高校園 E 化環境的品質。本系統使用中華電信提供的 HiSECURE 函式介面 5.1 版[8][9]，主要是包裝承 C++ 的函式元件，將 C/C++的程式放在網頁上執行以達到驗證、加密等功能。目前此系統正測試中，預期教育訓練完畢可以正式推展於校內應用。未來還可以將自然人憑證技術擴充至其他校內行政系統的整合與建置，以達到單一登入與校園 E 化之目標。

參考文獻

[1] 周世雄，“Active X 技術大公開”，臺北市，初版，第三波，1997，民 86。

[2] 陳會安，“JavaScript 網頁製作徹底研究”，旗標出版股份有限公司，台北市，台灣，民 94。

[3] 彭明柳，“Active X 玩家技術手冊”，臺北市，初版，博碩，民 86。

[4] 施威銘研究室，“PHP 網頁模組隨學隨用”，臺北市，台灣，旗標，民 93。

[5] Kazuhiro Furuhata 著，柯志杰 譯，“最新 JavaScript 完整語法參考辭典”，臺北市，台灣，旗標，民 93。

[6] 小企鵝，小忠忠，“PHP 之戀”，臺北市，台灣，上奇，民 94。

[7] 劉漢山，“Oracle Database 10g PL/SQL 程式設計經典 (Oracle Database 10g PL/SQL Programming)”，臺北市，台灣，學貫，民 94。

[8] http://moica.nat.gov.tw/html/index.htm，“內政部自然人憑證管理中心”。

[9] 中華電信 HiSECURE 函式介面 5.1 版版本 A.doc。

[10] william stalling, ”Network security Essentials”，Prentice Hall。

附錄

系統流程圖：

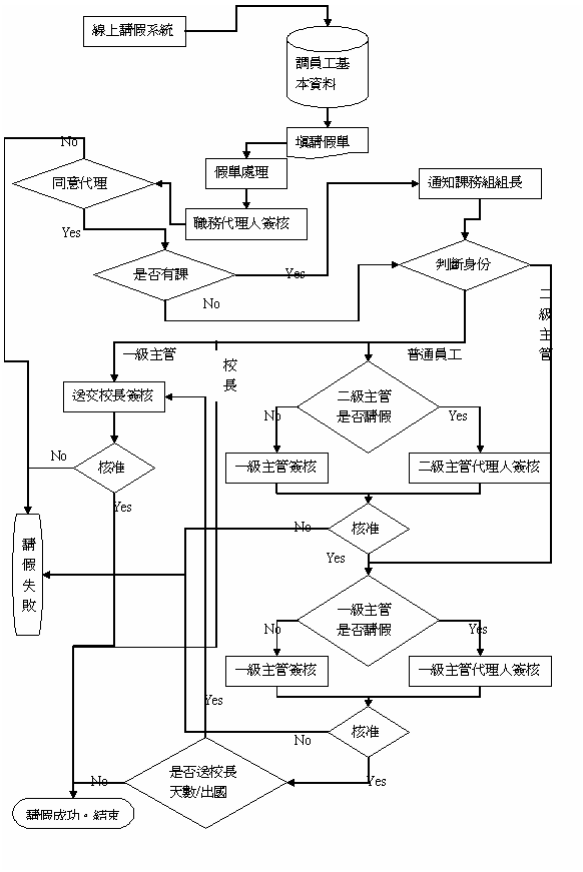


圖 19 線上請假流程圖

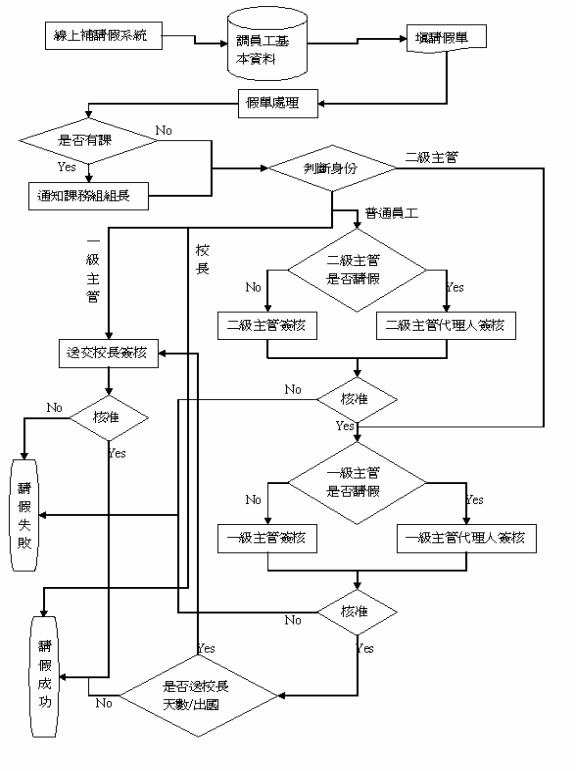
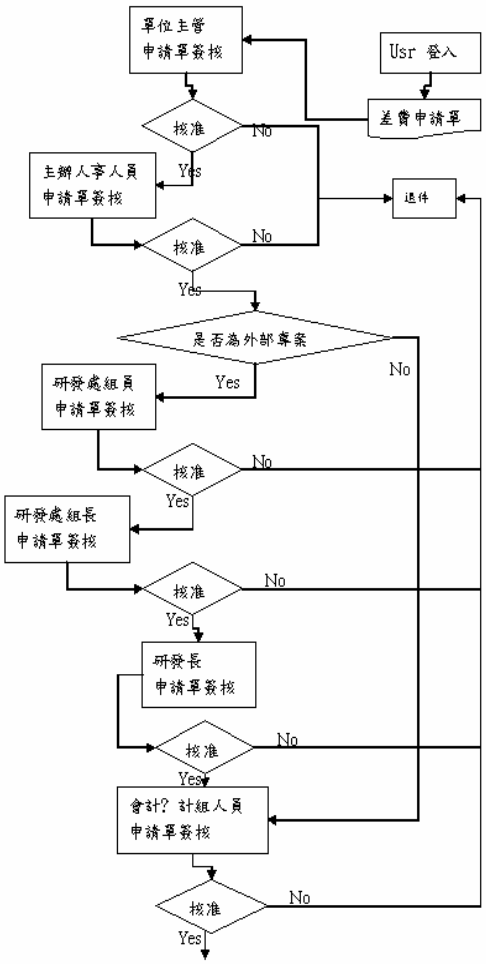


圖 20 線上補請假流程圖



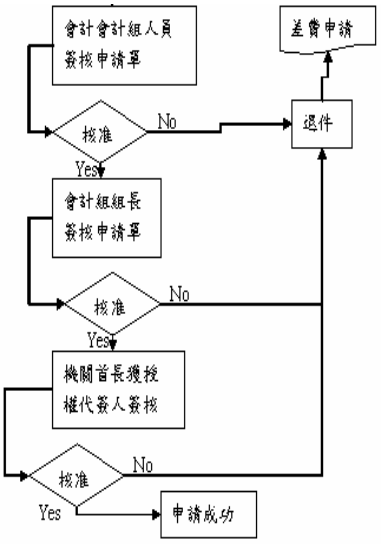


圖 21 差費申請流程圖