# 客製化的 LDAP 驗證設計與應用

**楊志田、陳瑋昇**

輔仁大學資訊中心

## 摘　　要

以輕量級目錄服務(LDAP)來完成單一登入(Single Sign-On; SSO)的驗證方式已經行之有年，不論是帳密整合於單一入口網登入，或是根據帳密提供對應系統的功能權限、使用雲端空間等控制應用，不同架構可以有不同的管理模式與應用。

本文以本校第一代與第二代的 LDAP 建置經驗，說明為何採用 Open LDAP、建構帳密與個資分散的模式、統一驗證入口搭配多台不同功能需求的 LDAP 主機架構，以及如何達到客製化的驗證服務。

**關鍵詞：LDAP、SSO、單一入口網、Open　LDAP。**

# 壹、 前言

在電子化的服務中，系統安全絕對是首要任務，而身分認證就屬於在系統安全主要防護的六個項目當中[4]。每個單位對於所提供各眾多系統的單一入口帳密管控機制有所不同，其中以 LDAP[10]來處理單一登入(Single Sign-On; SSO)的驗證方式是很常見的，包含本校在內。不論是帳密整合於單一入口網登入[3]，或是根據帳密提供對應系統的功能權限[9]、使用雲端空間等控制應用[8]，不同架構可以有不同的管理模式與應用。但是，一般的 LDAP 建置，除了帳號密碼屬性之外，可能還包含了其他該帳號的個資屬性，例如：姓名、出生日、工作單位相關資訊，甚至包含其身分證字號等等。另外，驗證的機制可能是從帳號架構的根目錄開始，這樣的組合建置有其優缺點，也有其當時建置的客觀考量，本校的第一代 LDAP 大致就是如此。

隨著各系統端的驗證考量情況變得複雜，加上個資議題，針對個人其他資訊是否應該保存在 LDAP 內，是否只讓 LDAP 純粹處理帳密驗證，但如此的架構要如何解決各系統對該帳號的功能權限判定問題呢？以及如何建構客製化的驗證服務。本文提供本校第二代 LDAP 建置的相關經驗與考量之參考。

首先在第貳部分，提出一般 LDAP 建置與驗證機制問題，包含建置成本、驗證從帳號根目錄開始查詢之時間增加與管理者帳號被測試風險、提供系統驗證所需屬性皆存在 LDAP 當中的後續更新維護問題。並提供本校第一代 LDAP 實務運作上的問題。

在第參部分，介紹本校新一代 LDAP 設計方法，包含：為何採用 Open LDAP、在 LDAP 內只存帳號密碼與特定服務參數資訊，其他個資則存在學校學籍資料庫、人事資料庫，透過與資料庫驗證的方式確認帳號的目前角色，包含是否仍在職、在校生、畢業生等等身分，並提供各系統用以確認其所屬的功能權限，如此也減少了需要 LDAP 自己維護其他個資資料的問題。另外，建置 LDAP 群組，依照認證訴求分類為：完整同步、部分同步、帳密同步。並介紹統一驗證頁面機制、客製化不直接從全部帳號根目錄開始驗證之效益(時間、帳號安全)、且建置各不同訴求驗證功能的 LDAP 主機。

最後在第肆部分提出功能結果。並在第伍部分提出結論與未來展望。

# 貳、 一般 LDAP 建置與驗證機制問題

LDAP 的英文全名為 Lightweight Directory Access Protocol，中文翻譯為「輕量級目錄存取協定」，簡稱 LDAP。

LDAP 的目錄,是從所謂的根目錄開始往下,一層一層的分支形成樹狀圖的架構,可參考[10]。以往的建置與使用上有以下常見方式與情況。

一、 建置成本

(一) 以往，有業界提供的方案，如：Microsoft 的 Active Directory、Novell 的 eDirectory LDAP，但是這部分需要有預算採購。

(二) 針對上述業界方案，使用單位通常無法自行針對所提供的整合性功能進行修改，造成單位服務發展應用的瓶頸，甚至可能在發生問題時無法自行解決。

二、 驗證程序從帳號根目錄開始查詢

(一) 驗證程序習慣從根目錄開始，聽起來是合理，但是如果帳號數量多的話，時間則會相對增多。

(二) 因為 LDAP 最大權限管理者帳號就位於根目錄，所以如果提供從根目錄開始查詢的話，也增加管理者帳號被測試的風險

三、 提供各系統驗證權限所需的非帳密屬性皆存在 LDAP 中

(一) 因為包含身分權限的個資也在其中，所以目錄結構較大

(二) 驗證屬性皆存在 LDAP 中,其實是合理,因為 LDAP 本身就是個目錄架構，但是現行服務系統愈來愈採分散架構，資料維護也會有需要分散更新與維護的考量。

(三) 負責 LDAP 帳密的管理，是否該負責維運該帳號的其他個資資料？這在權限分工上也是個考量的問題。

四、 各系統各自設計驗證的資料輸入頁面

(一) 因為驗證頁面設計在各自的系統內，當問題發生時候不一定是 LDAP 方面的原因，要再進行確認問題所在。

(二) 甚至有可能被各系統主機自行設計側錄資料的風險，尤其是針對委外開發的系統更需注意。

五、 本校第一代 LDAP 運作上的其他問題

(一) 當時採用 Novell eDdirectory，搭配的管理系統是委外負責

(二) 目錄架構採預設結構，且歷經長期增刪修訂，造成後來的目錄結構又多且亂，甚至有些不清楚的 OU 部分，如圖 1。

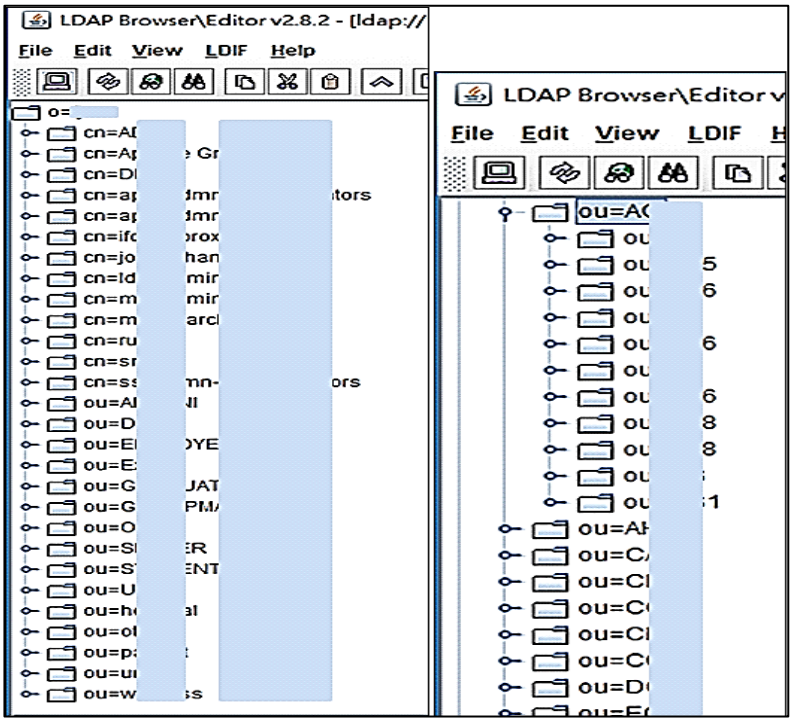



圖 1.　本校舊一代 LDAP 主機分類多層架構

(三) LDAP 與人事資料庫、學籍資料庫的同步，不是即時的。造成驗證空窗期。

(四) 委外的系統功能與 Novell eDirectory 版本有關，但無法自行修訂，造成之後一些異常問題，例如：同步程式、帳號搬移到其他目錄、刪除帳號等問題都曾經發生過但無法有效解決。

# 參、 本校新的 LDAP 設計方法

在規劃新的 LDAP 架構，除了針對上述過去所面臨的問題，也以全校各系統的客製化認證需求來考量以下。

一、 採用 Open LDAP

基於成本與自行修訂功能的需求，加上目前 Open LDAP 的功能與穩定，因此我們採用 Open LDAP 作為本校單一帳號驗證之用，安裝的版本是 ldapmodrdn 2.4.40，作業系統環境是 CentOS 6.7 release (64bit)。關於 eDirectory LDAP 與 Open LDAP 之間的差異比較可參考[2]。

二、 LDAP 內只存帳號密碼與特定服務參數資訊

我們的訴求是讓此 LDPA 主要只作帳密驗證功能，至於該帳號對應在各系統的權限所需判斷的其他屬性資料，則存在學校的學籍資料庫、人事資料庫，透過與資料庫驗證的方式確認帳號的目前角色，包含是否仍在職、在校生、畢業生等等不同身分，並回應該身分資訊提供各服務系統，使得各服務系統得以確認該帳號所屬的功能權限，如此分散架構也減少了需在 LDAP 主機維護其他個人資料的正確性與即時更新問題。

另外，為了因應某些服務主機有內部自建 LDAP，建置了資源配置屬性，所以我們在全校級的 LDAP 內存放一些服務參數，用以同步配置到該服務主機內的 LDAP，達到納管功能。但這不會影響其他服務系統驗證的複雜度與時間，原因是我們將 LDAP 分類如下。

三、 建置 LDAP 群組，依照認證訴求分類如圖 2，說明如下：

(一) LDAP 同步機制與實作可參考[1][6]。而我們的同步機制在概念上分為以下三種：完整同步、部分同步、密碼同步。

(二) 完整同步：完整同步帳號所有資訊。不提供驗證之用，作為備份用途。

(三) 部分同步：只同步帳號密碼、以及部分服務參數，提供上一段提到的特殊服務主機之用。

(四) 密碼同步：只同步帳號密碼資訊，提供給一般服務系統快速驗證之用。

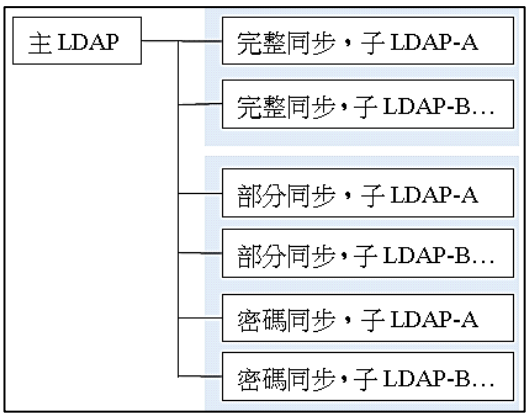



圖 2. 新 LDAP 各主機分類架構

(五) 以上的分類構想與客製化效能陸續陳述於下

四、 統一驗證頁面機制

如果帳密的輸入頁面是設計在各服務系統，透過各系統將帳密傳給 LDAP 作驗證的話，則在各系統有可能被側錄的風險，尤其是委外的開發系統。本案提供驗證用的介接程式給各服務系統，驗證頁面是在 LDAP 主機上，避免驗證資料被側錄。

五、 建置不同訴求驗證功能的 LDAP 主機

我們在既有的主 LDPA 之外，架設上述不同訴求分類的其他子_LDAP，可針對某特定子主機只開設特定服務的帳號，並且同步。因此，只要是介接到這一台驗證的系統，就只能提供給特定帳號群使用。各子_LDAP 的建置，也可用來分擔驗證的工作。另外，有些服務主機本身就有其自己的驗證目錄服務系統(例如：MAIL2000)，此法可以將該服務下的帳號納入統一管理 (即時的同步密碼或帳號停用)。

六、 客製化不直接從帳號根目錄開始驗證之效益

有些系統只開放給特定群組使用者，所以我們可針對該系統需求，只同步某子目錄架構到該子_LDAP 主機，如此等同直接從原始目錄中的某節點往下搜尋，節省時間。另外，該服務系統也因為無需使用 LDAP 管理者權限，所以從中間節點往下搜尋，避開根目錄管理者帳號被搜尋的風險，增加管理者帳號安全。

七、 重新設計精簡目錄架構

因為上述的設計概念，且不儲存個人帳密外之資訊，可以將原來數十個且多層次的目錄結構，如圖 3，修訂為在根目錄之下只剩下個位數目錄的結構，如圖 4。

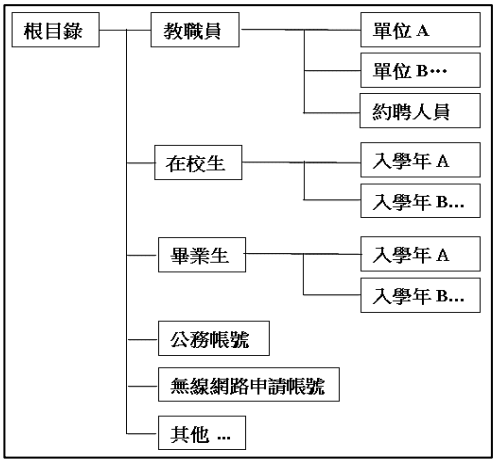



圖 3. 舊 LDAP 目錄架構

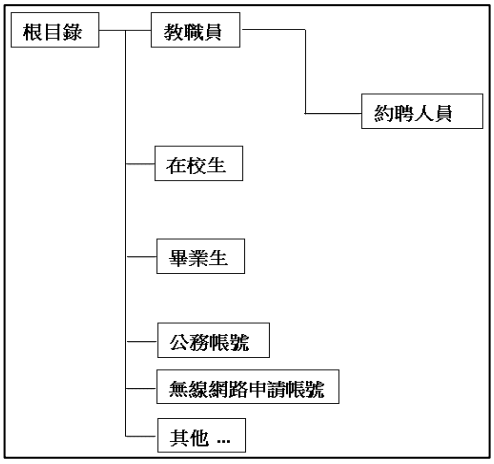



圖 4. 新 LDAP 目錄架構

八、 資料更新同步，這裡指的資料分為以下部分：

(一) 從統一驗證頁面向資料庫驗證的部分：因為各資料庫的維護不是在 LDAP 之內進行，所以當各單位更新相關資料庫之後，LDAP 驗證頁面去連結資料庫所對應的個人資料等同是最新同步過的。

(二) 子_LDAP 內資料的部分：依照上述圖 2，主_LDAP 資料異動成功時候，會進行對子_LDAP 的同步作業，分為完整同步、部分同步、密碼同步，且記錄同步失敗的紀錄，作為之後問題探討以及排程再執行的標的。

(三) 主_LDAP 這台機器只有在帳號增刪停用與帳密資訊修訂時候被存取，不提供一般驗證服務用。

九、 建置提供使用者關於 LDAP 帳號之相關業務網站，包含以下主題

(一) 重大訊息：主要針對新帳號使用者，提供帳號核發時程與使用說明

(二) 關於單一帳號：說明本校建置單一帳號(LDAP)之歷程與使用規範

(三) 帳號啟用與修改驗證資料：

1. 帳號啟用的最主要目的在於提供使用者設定自己的身分驗證資訊
2. 因應未來忘記密碼時的線上驗證程序所需。

(四) 相關申請：

1. 提供約聘人員帳號與單位公務帳號申請。
2. 正式聘任之專兼任教師、職員、工友、在學學生等的帳號是由權責單位（人事室及教務處）建立開設並管理，不須個人另外申請。

(五) 變更密碼：提供使用者進行變更密碼

(六) 忘記密碼查詢：

1. 提供使用者依據上述設定的資料驗證
2. 核對成功後，提供亂數臨時密碼用以登入並進行變更密碼。

(七) 帳號狀態查詢

1. 當使用者無法登入某系統之疑慮時，提供可自行查詢的機制。
2. 讓使用者可以知道目前該帳號是否停用、停用原因、帳號是否啟用、帳號使用期限等等情況。

十、 建置管理者功能網站

(一) 帳號申請審核：針對約聘人員帳號與單位公務帳號申請之線上審核與流程進度查詢。

(二) 帳號管理：可查詢該帳號的開設紀錄、屬性資料、異動紀錄、驗證紀錄，並且透過連結料庫查詢相關在校身分資訊、使用期限。

(三) 停用帳號 / 解除停用：可依據需要停止該帳號的部分服務，選擇停用部分子_LDAP 主機上的權限，避免帳號一停，所有的服務皆不能用。但是如果該帳號被盜用而發生危害整體資訊安全之行為時，則會進行停用全主機服務。

(四) 同步失敗紀錄：紀錄主_LDAP 與各個子_LDAP 同步失敗的紀錄。

# 肆、 功能結果

以上述設計方法之建制，檢視新環境，列述以下結果與功能。

一、 新 LDAP 目錄架構，精簡許多，如圖 5

二、 帳密驗證頁面申請

(一) 除了本單位自行開發維護的系統已經介接驗證頁面之外，針對其他單位自行管理的主機申請驗證帳號之需求，設定如下圖 6，主要設定是"認證完成回復網址"：該主機是以哪個網頁來接收驗證完成的回覆資料，以及"LDAP 搜尋目錄"：是從 LDAP 的哪個節點往下搜尋。當完成設定後，回復申請單位內容如圖 7，當中資訊包含：驗證程式網址、驗證完成回復資料的變數、查詢使用者登入驗證的紀錄網址。

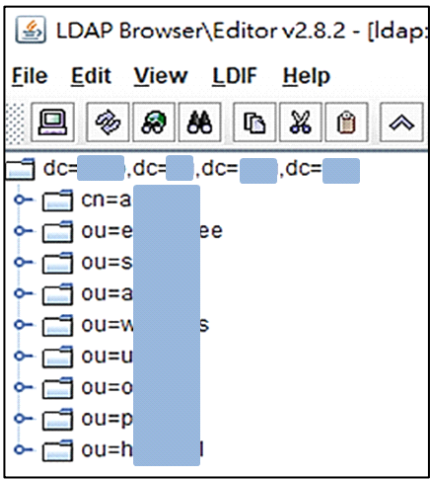



圖 5. 新 LDAP 目錄架構


圖 6. 驗證頁面設定

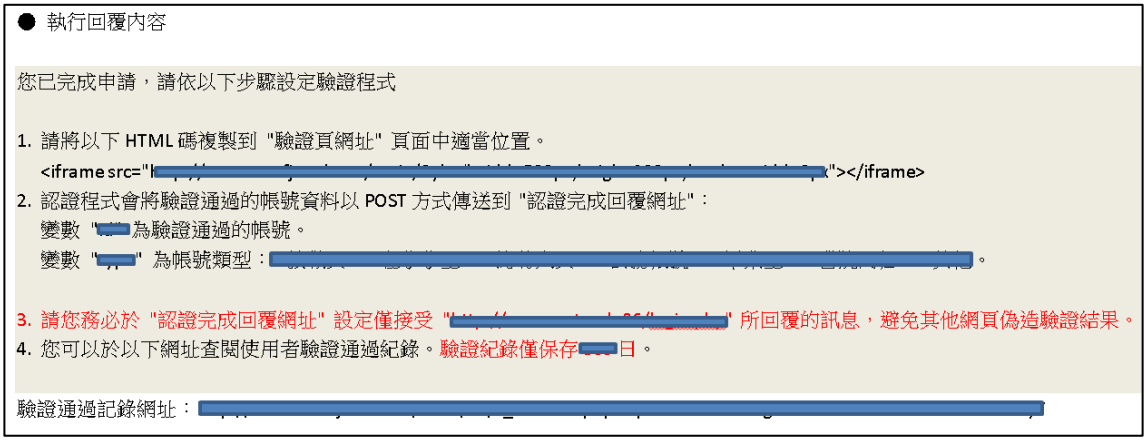
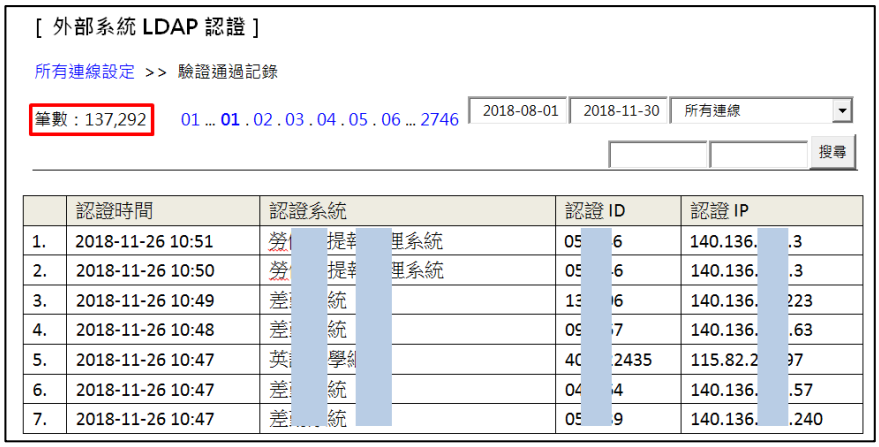



圖 7. 驗證設定完成回復

(二) 針對外單位系統，提供連線紀錄資訊，如圖 8，讓外單位自管主機可以知道系統使用連線的紀錄，包含：認證時間、使用者帳號、連線 IP 位址。圖中看到的是本單位管理系統能夠看到所有外單位系統驗證紀錄，如果是各單位主機管理系統則只能看到它們自己系統被連線驗證的紀錄。




| | 認證時間 | 認證系統 | 認證 ID | 認證 IP |
|---|---|---|---|---|
| 1. | 2018-11-26 10:51 | 勞 提 理系統 | 05 6 | 140.136. .3 |
| 2. | 2018-11-26 10:50 | 勞 提 理系統 | 05 6 | 140.136. .3 |
| 3. | 2018-11-26 10:49 | 差 統 | 13 6 | 140.136. 223 |
| 4. | 2018-11-26 10:48 | 差 統 | 09 7 | 140.136. .63 |
| 5. | 2018-11-26 10:47 | 英 學 | 40 2435 | 115.82.2 97 |
| 6. | 2018-11-26 10:47 | 差 統 | 04 4 | 140.136. .57 |
| 7. | 2018-11-26 10:47 | 差 統 | 05 9 | 140.136. .240 |

圖 8. 外部系統 LDAP 驗證紀錄

三、 提供給使用者針對 LDAP 帳號之相關線上服務網站，除了提供重大訊息、帳號使用規範之外，並提供相關功能，以下為當中的一部分。

(一) 修改驗證資料：如圖 9，使用者在輸入帳密無誤之後，進入設定備用信箱、忘記問題回答(包含自行設定的題目、答案)，以備之後如果忘記密碼之時，可利用後面提到的"忘記密碼"功能的驗證後，重新設定密碼。

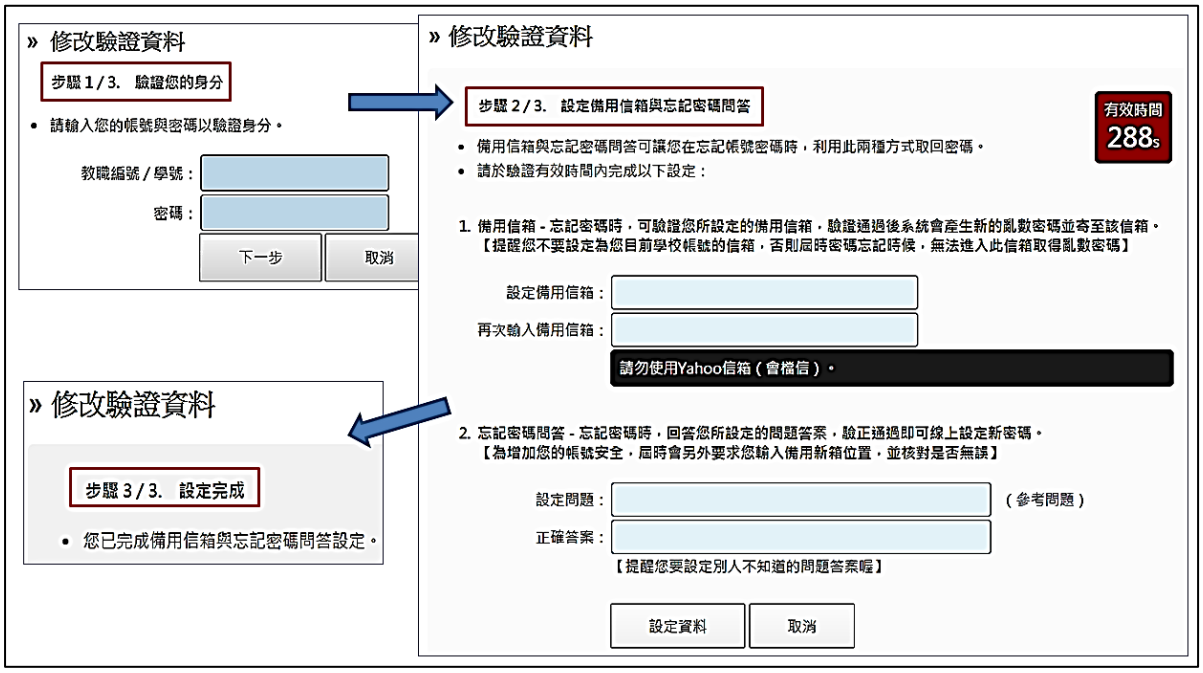



圖 9. 使用者修改驗證資料畫面

(二) 修改密碼：如圖 10，使用者在輸入帳密無誤之後，進入設定新密碼的頁面，依照密碼格式要求完成設定。

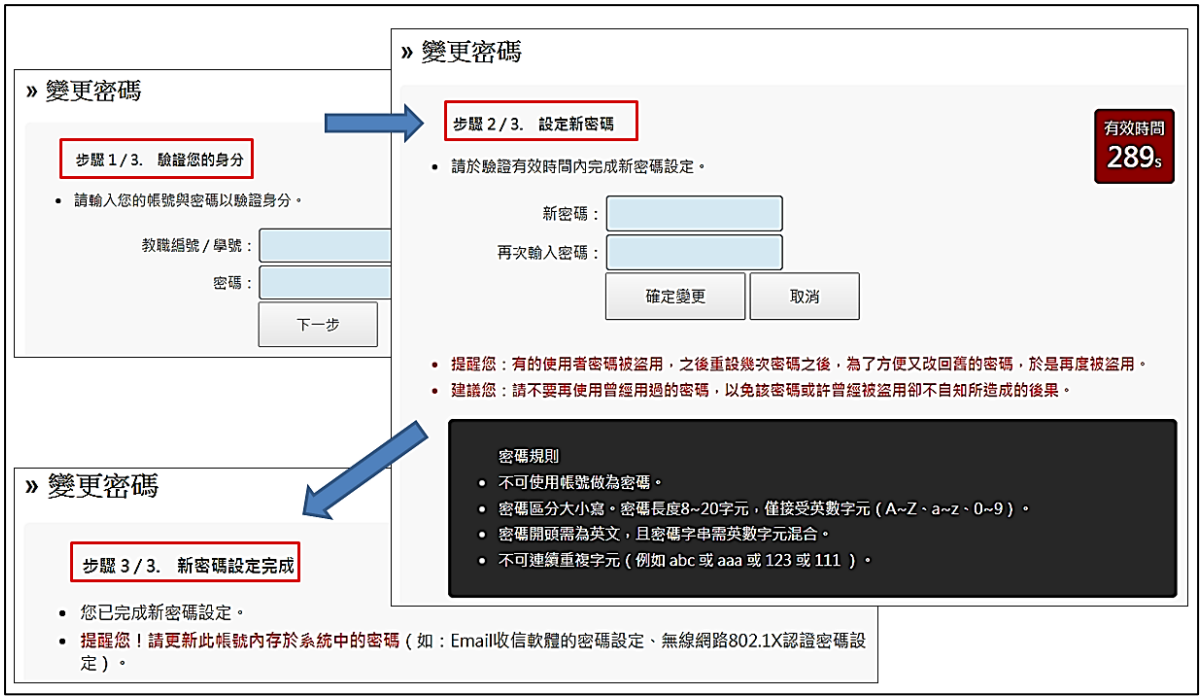



圖 10. 使用者修改密碼畫面

(三) 忘記密碼：如圖 11，提供使用者在忘記密碼時候，利用備用信箱取得亂數密碼，或是問題回答通過後線上重新設定密碼。圖中範例是以問題回答方式：使用者在輸入帳號，並選擇以忘記密碼問題方式之後，進入步驟 2 的問題與答案(為了嚴格起見，我們在系統中另外要求輸入備用信箱位址與驗證碼是否無誤)，資料正確後則進入步驟 3 的設定新密碼，完成後離開。

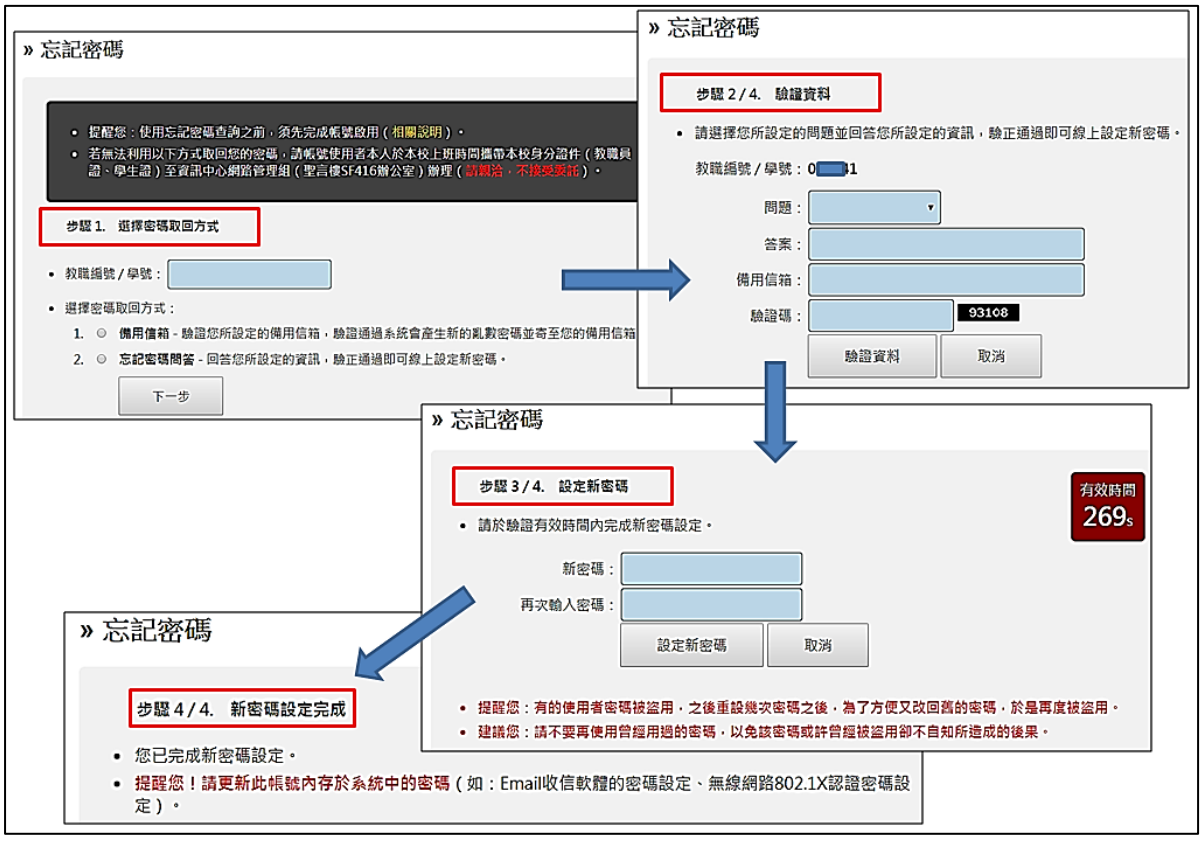



圖 11. 使用者忘記密碼畫面

(四) 帳號狀態查詢：提供使用者查詢自己帳號的狀態，如圖 12，使用者在輸入帳密無誤後，顯示其帳號狀態，包含是否正常或停用、停用原因、帳號是否啟用、帳號使用期限等等。

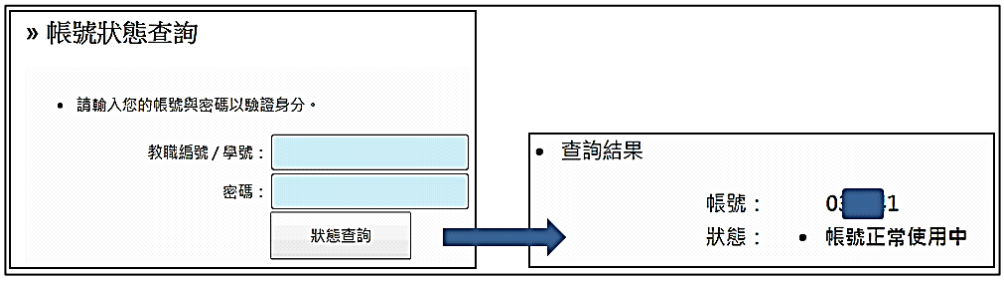
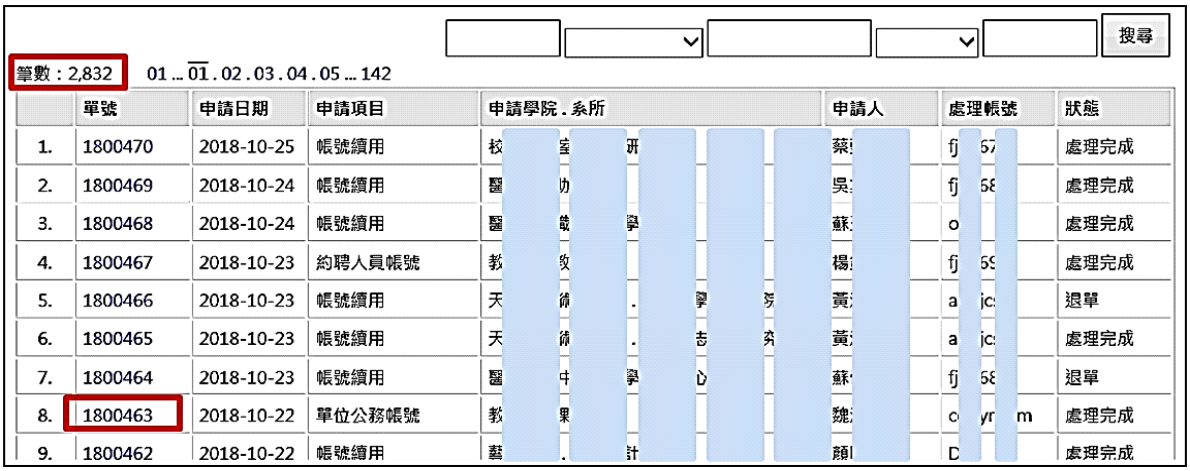



圖 12. 使用者帳號狀態查詢畫面

四、 管理者系統網站，此網站是提供內部管理使用，提供部分說明如下。

(一) 帳號申請審核：針對約聘人員帳號與單位公務帳號申請之線上審核與流程進度查詢，如圖 13，當中有目前為止申請的筆數在左上角，以及申請單號與申請日期、項目、單位、申請人、申請人帳號、目前處理狀態。在點選某單號之後，可進一步看到該筆申請單內容，如圖 14，當中除了申請料內容之外，還包含主管簽核流程，以及業務承辦紀錄。




| | 單號 | 申請日期 | 申請項目 | 申請學院 . 系所 | 申請人 | 處理帳號 | 狀態 |
|---|---|---|---|---|---|---|---|
| 1. | 1800470 | 2018-10-25 | 帳號續用 | 校 | 蔡 | fj 57 | 處理完成 |
| 2. | 1800469 | 2018-10-24 | 帳號續用 | 醫 | 吳 | fj 58 | 處理完成 |
| 3. | 1800468 | 2018-10-24 | 帳號續用 | 醫 | 蘇 | o | 處理完成 |
| 4. | 1800467 | 2018-10-23 | 約聘人員帳號 | 教 | 楊 | fj 59 | 處理完成 |
| 5. | 1800466 | 2018-10-23 | 帳號續用 | 天 | 黃 | a jcs | 退單 |
| 6. | 1800465 | 2018-10-23 | 帳號續用 | 天 | 黃 | a jcs | 處理完成 |
| 7. | 1800464 | 2018-10-23 | 帳號續用 | 醫 | 蘇 | fj 58 | 退單 |
| 8. | 1800463 | 2018-10-22 | 單位公務帳號 | 教 | 魏 | c yr m | 處理完成 |
| 9. | 1800462 | 2018-10-22 | 帳號續用 | 藝 | 顏 | D | 處理完成 |

圖 13. 特殊帳號申請審核總表畫面

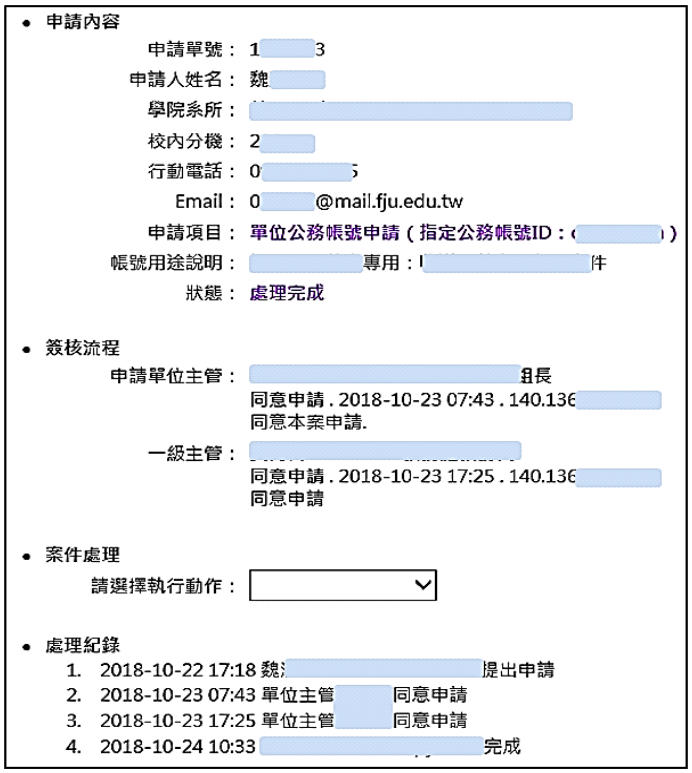



圖 14. 特殊帳號申請審核流程畫面

(二) 帳號管理：除了以上提到的帳號開設紀錄、驗證紀錄之外，還有 LDAP 屬性資料、異動執行紀錄，並且透過連結料庫查詢相關在校人事身分資訊、使用期限。如圖 15。

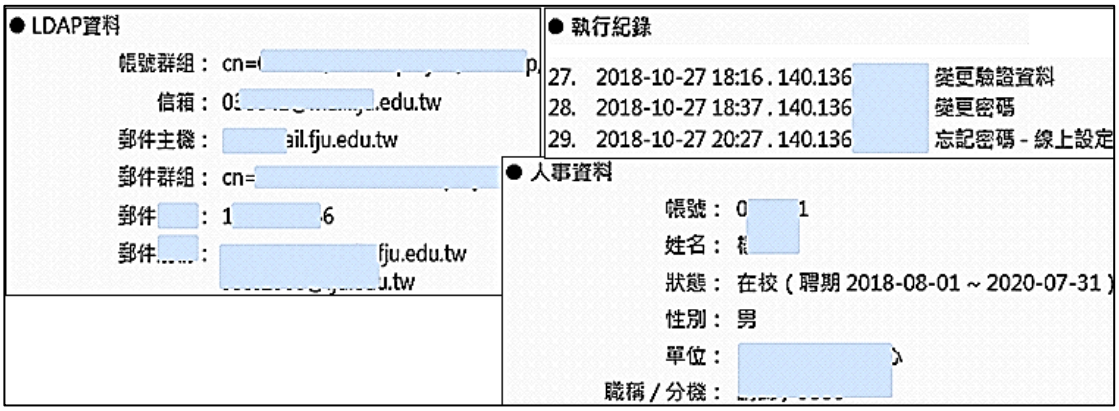



圖 15. 帳號 LDAP 資料、執行紀錄、人事資料畫面

(三) 停用帳號 / 解除停用：圖 16 是帳號停用列表，當中顯示該帳號停用的時間、停用的認證 LDAP 主機範圍、停用原因等等。如果點選該帳號，就可進入解除停用的功能。

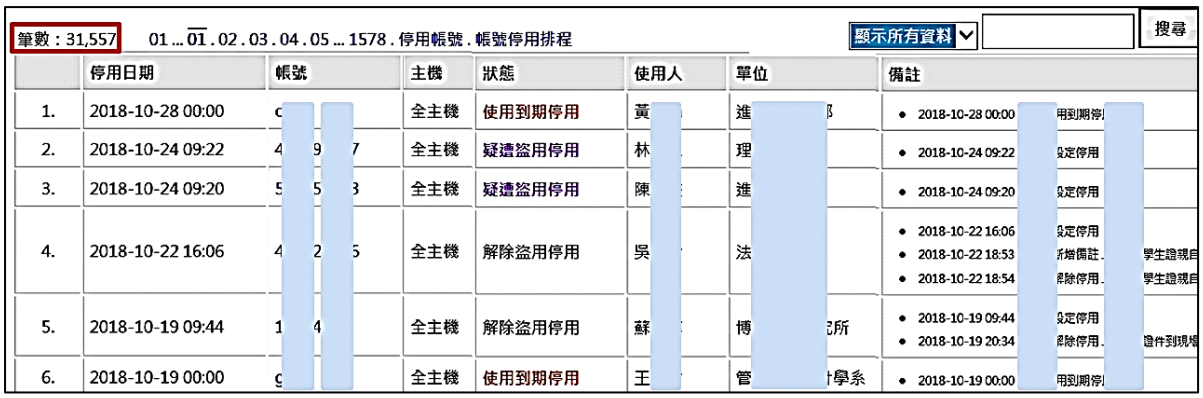



圖 16. 帳號停用列表

# 伍、 結論與未來展望

一、 對於委外開發系統，須有心理準備在未來之服務是否得以延續。尤其是長期的服務系統，最好要確定能完全掌控系統未來升級、改版、修訂等情況所需具備之能力與資源。

二、 系統開發各有創意巧思，我們以不同訴求類型的多台 LDAP，配合不同需求的系統服務，來執行資料分散管理的驗證架構，也可納管特殊服務的權限資訊。由本文陳述之內容，可確信本單位自行架構設計開發的帳密驗證系統，確實可以解決本校目前的系統身分驗證需求，並可彈性客製化。

三、 Google 在近期宣布將推出客戶和合作夥伴的雲端身份（Cloud Identity for Customers and Partners，CICP），以及 Secure LDAP 功能，可以幫助使用者統一雲端、本地端和傳統應用程式的身份管理[5]，將也會是個之後研究的主題。

四、 未來，將進一步整合相關措施，以保障使用者帳號的安全

(一) 結合 OTP (One Time Password)機制：讓使用者除了登入系統需要的帳密之外，並需要輸入個人行動裝置(或其他配套方式)產生的一組驗證碼[7]，以確定為本人使用。以因應網路釣魚信件或是詐騙網頁的猖狂之下，讓使用者即使不小心可能洩漏了帳密之後，仍能保護其帳密的使用範圍。而針對某系統可能要一天登入數次使用的情況下，可能造成另類麻煩(因為每次登陸都要輸入 OPT 驗證碼)，這方面的問題我們已經研究了因應方式：將 OPT 認證結合裝置來源的判斷，以過濾在有效期間已經驗證過的裝置來源，相信如此可以讓安全與便利得以兼顧。

(二) 增加使用者可自行查詢本身帳號的認證紀錄：目前認證紀錄的查詢只提供管理者使用，我們正將進行將此功能修訂讓使用者可自我查詢，希望可以藉此讓使用者觀察是否有不對的驗證時間，得以在有疑問之時盡快做必要處理，例如：更改密碼相關資訊、檢查是否安裝防毒軟體或是升級更新情況，並持續追蹤或與本單位連繫協助研究問題來源。

(三) 推廣納入尚未結合此認證方式的其他各單位系統：因為目前的驗證系統只確定在本單位自行研發或維運的主機服務當中，其他各單位自行管理開發的系統不一定都結合了本單位的驗證頁面。希望在推廣及各單位使用後，讓本校使用者的單一 LDAP 帳密更加安全 。

(四) 教育訓練：縱使有再多的軟硬體防護措施來保護我們的網路資源安全(包含帳密)，但是最無法掌握的則是人為的疏失，這需要提升校內使用者的資訊素養，以正確觀念來了解與使用網路資源，以免害了自己帳密被盜用可能造成的隱私曝光或是因此在某些服務的資源(例如：選課內容)被竄改，甚至被利用帳密進行造成危害大家的事件(例如：濫發詐騙信件、網路攻擊行為)所造成的困擾。

# 參考文獻


1. skypeGNU1 (2017)。OpenLDAP Master-Slave 同步複製。取自：http://blog.51cto.com/skypegnu1/1939505，2018 年 10 月 29 日下載。
2. 王筱君、陳欽鑑(2016)。eDirectory LDAP 快速輕易無縫接軌至 Open LDAP。TANET2016 臺灣網際網路研討會論文集，第 1124～1128 頁。2016/11/01。
3. 李明坤、楊中皇(2005)。基於安全 LDAP 伺服器之整合服務認證系統設計與實現。2005 年第十一屆資訊管理暨實務研討會，下載網址為 http://dx.doi.org/10.6679/TANET.2016.200。2005/12/10。
4. 李宗翰(2012)。提升系統安全防護的 6 種產品。取自 https://www.ithome.com.tw/tech/88125，2018 年 10 月 30 日下載。
5. 李建興(2018)。Google 推出身分和存取管理服務 CICP，還以 Secure LDAP 支援傳統應用程式。取自 https://www.ithome.com.tw/news/126400，2018 年 10 月 29 日下載。
6. 宗士強、林劍檸、朱雙華(2010)。LDAP 目錄服務同步。計算機與現代化，第 2010 年第 10 期，第 150～153 頁。中國，2010/10/01。
7. 周峻佑(2016)。當單一密碼認證不再安全。輔助密碼的身分認證機制，你了解多少？取自 https://www.ithome.com.tw/news/106955，2018 年 10 月 30 日下載。
8. 徐振庭(2013)。一個以 LDAP 為基礎的雲端儲存系統。國立交通大學資訊科學與工程研究所碩士論文。
9. 陳能海(2011)。單一簽入系統與帳號管理之個案研究。國立中央大學資訊管理學系碩士在職專班碩士論文。
10. 楊中皇(2008)。Open LDAP 目錄服務。網路安全的理論與實務，第 17 章，金禾圖書。取自：http://security.nknu.edu.tw/textbook1ed/CHAP17-OpenLDAP.pdf，2018 年 10 月 29 日下載。