說明圖層座標系統或地理區域等資料。並可產生可下載圖資清單，供使用者選取。

4.3.3.3.5.2. 影音與文件資料管理

可儲存、查詢與取回二進位類型檔案格式。並可配合文件管理系統進行運作。

4.3.3.3.5.3. 數據資料管理

依據收集資料的資料特色，可建立適合的事實表(Fact Table)、維度表(Dimension Table)與度量(Measurement)。

4.4. 共同性服務管理

4.4.1. 帳號／權限管理

4.4.1.1. 帳號權限管理現況

全國消防系統及 EMIS 共用同一個 LDAP 單一簽入服務，惟無適宜之管理機制。系統縣市版與中央版之帳號及權限管理均由中央之系統管理人管理，並無分層授權予中央或地方之業管單位。縣市與中央之 LDAP 管理與同步更新模式為，中央可讀寫 LDAP，地方僅能讀取，故所有帳號權限均在中央修改，再更新至地方之 LDAP 伺服器。

署內各個人電腦與電子郵件帳號均透過 AD 管理，但與其他系統並未進行帳號權限整合。檔案管理／FTP 有至少三套，各自獨立管理，並未與 LDAP 或 AD 緊密整合。各科室與災害應變中心使用之 FTP，透過 AD 內之單位別區分，於登入時執行不同系統指令檔，以便使用該單位及個人之網路空間。

4.4.1.2. 單一簽入規劃目標

本規劃目標預計將署內全國消防系統、EMIS 系統、個人電腦帳號、電子郵件帳號，與 FTP 檔案管理等現有系統與帳號管理均能以一單一簽入機制整合為單一通行之帳號密碼。

規劃目標亦將規劃未來雲端平台之單一簽入機制，將所有現有系

統、外部介接系統，與研究機關資料交換憑證均透過此單一簽入服務進行自動登入與認證授權作業。

同時規劃整合行政院研考會之ｅ政府服務平台，整合民眾之自然人憑證，讓民眾或志工可透過ｅ政府認證後之憑證，註冊使用災害防救業務雲端服務之民眾或志工服務功能。

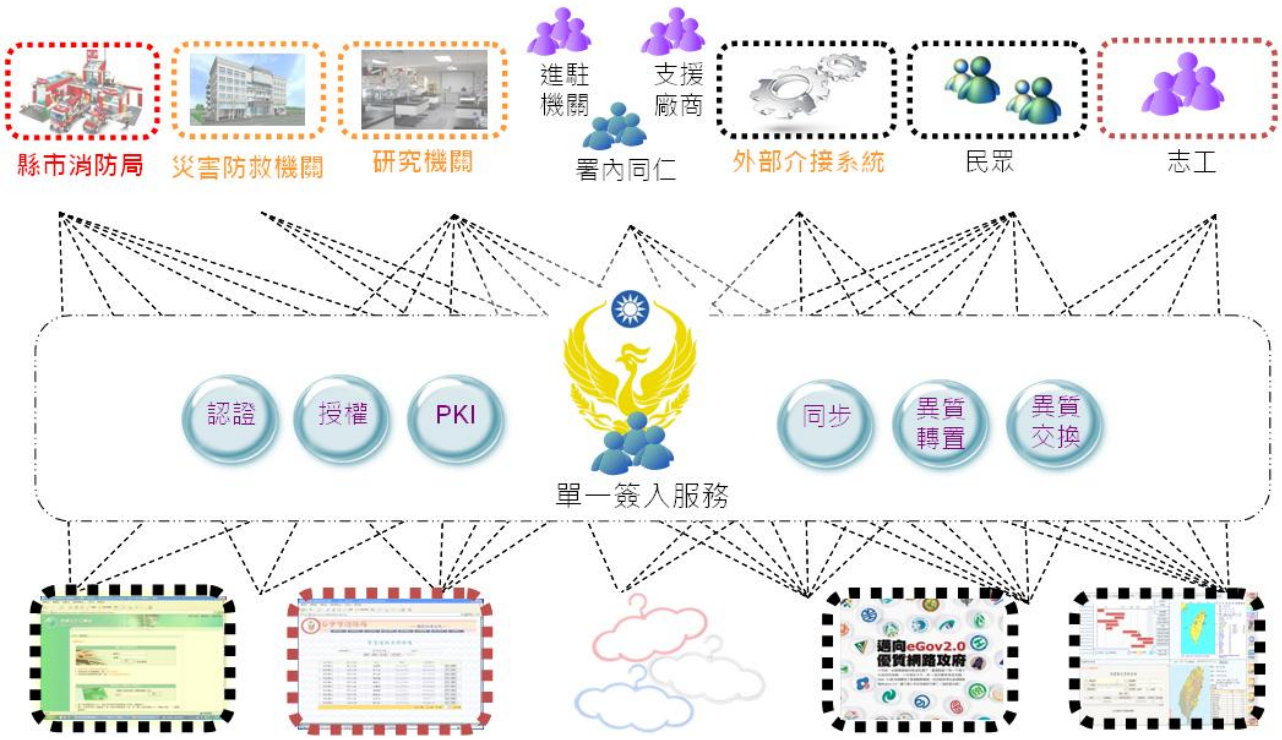


圖 369、單一簽入服務規劃目標

4.4.1.3. 單一簽入服務使用者

單一簽入服務預計有下列七種使用者角色：

- 進駐機關、支援廠商、署內同仁：此類角色主要均為在消防署內或中央災害應變中心，使用者透過本單一簽入服務進行系統操作運用。
- 研究機關：此類角色主要提供給研究機關做為外部資料交換或是系統元件嵌入應用為主，以機關憑證做認證授權依據。
- 災害防救機關：此類角色主要為中央其他災害防救機關，諸如經濟部水利署、農業委員會水土保持局、交通部中央氣象局等等，透過機關憑證做資料交換之認證授權依據。
- 縣市消防局：此類角色主要為地方消防與防災單位業管人員，

透過中央提供之系統與單一簽入帳號管理機制進行系統操作。

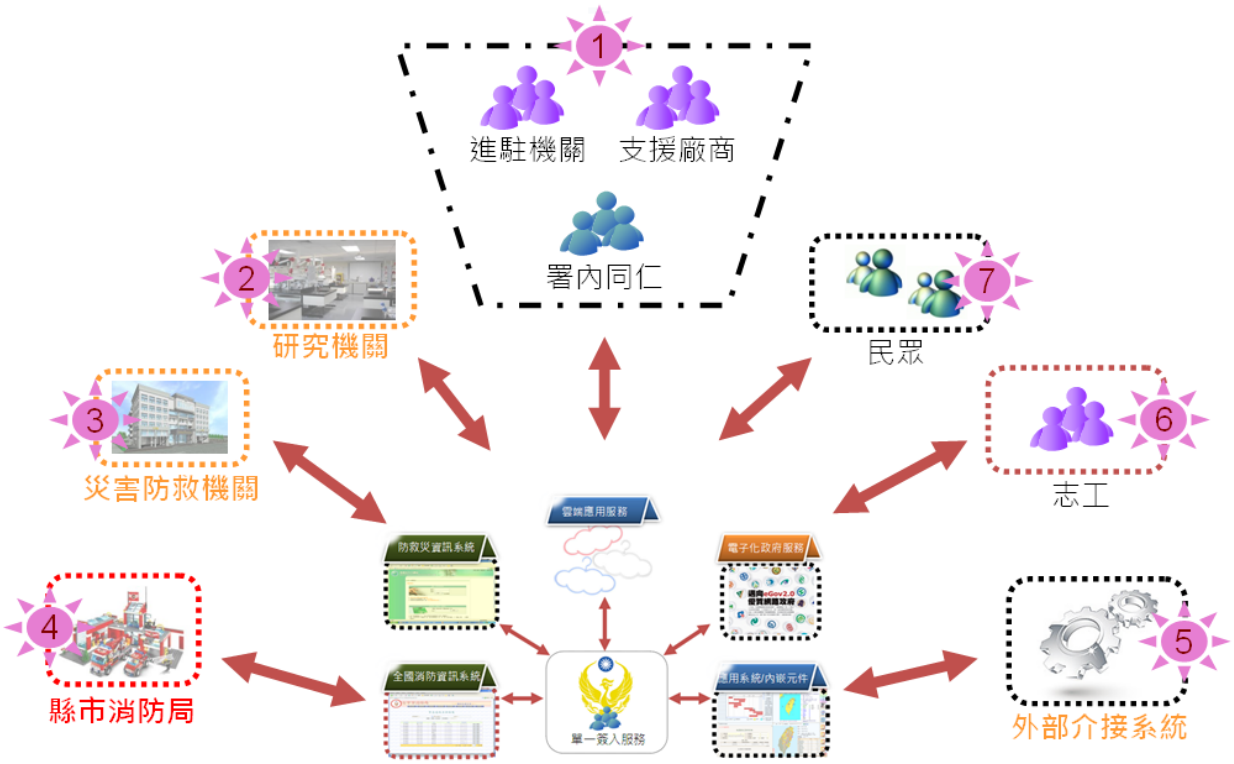


圖 370、單一簽入服務使用者示意圖

- 外部介接系統：此類角色主要為其他非機關單位之系統欲與消防署進行外部資料交換或是系統元件嵌入應用時，透過第三方信任單位之憑證做認證授權依據。
- 志工：此類角色主要透過自然人憑證做身份認證授權使用，因此志工須先申請自然人憑證，以利授權適當之系統使用權限。本單一簽入服務將與 e 政府平台進行黑白名單交換，確保憑證之有效與合法性。
- 民眾：此類角色主要透過自然人憑證做身份認證授權使用，因此民眾須先申請自然人憑證，本單一簽入服務將與 e 政府平台進行黑白名單交換，確保憑證之有效與合法性。

4.4.1.4. 單一簽入服務帳號管理流程

本節將依據前述之各使用者角色，依序規劃適當之帳號管理流程。各角色之帳號管理流程除依據業務管理流程外，對應之系統帳號管理生命週期亦做對應之規劃。

1. 署內同仁帳號管理流程

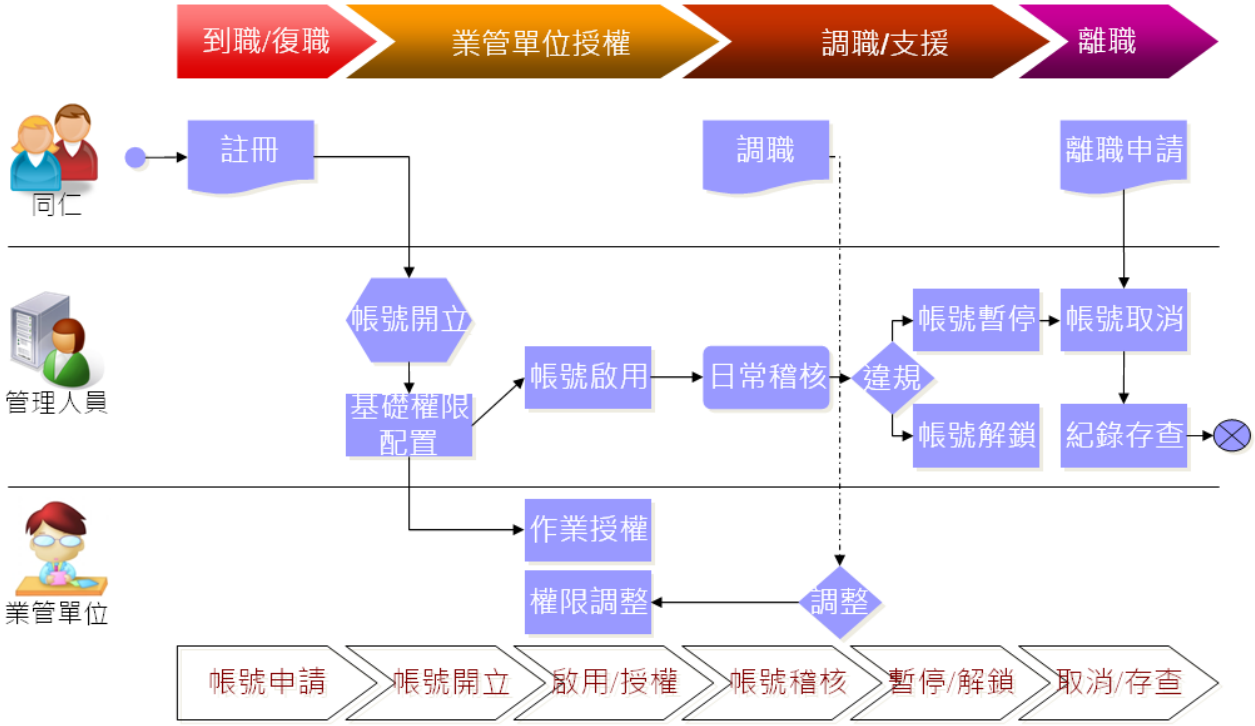


圖 371、署內同仁帳號管理流程

2. 進駐機關帳號管理流程

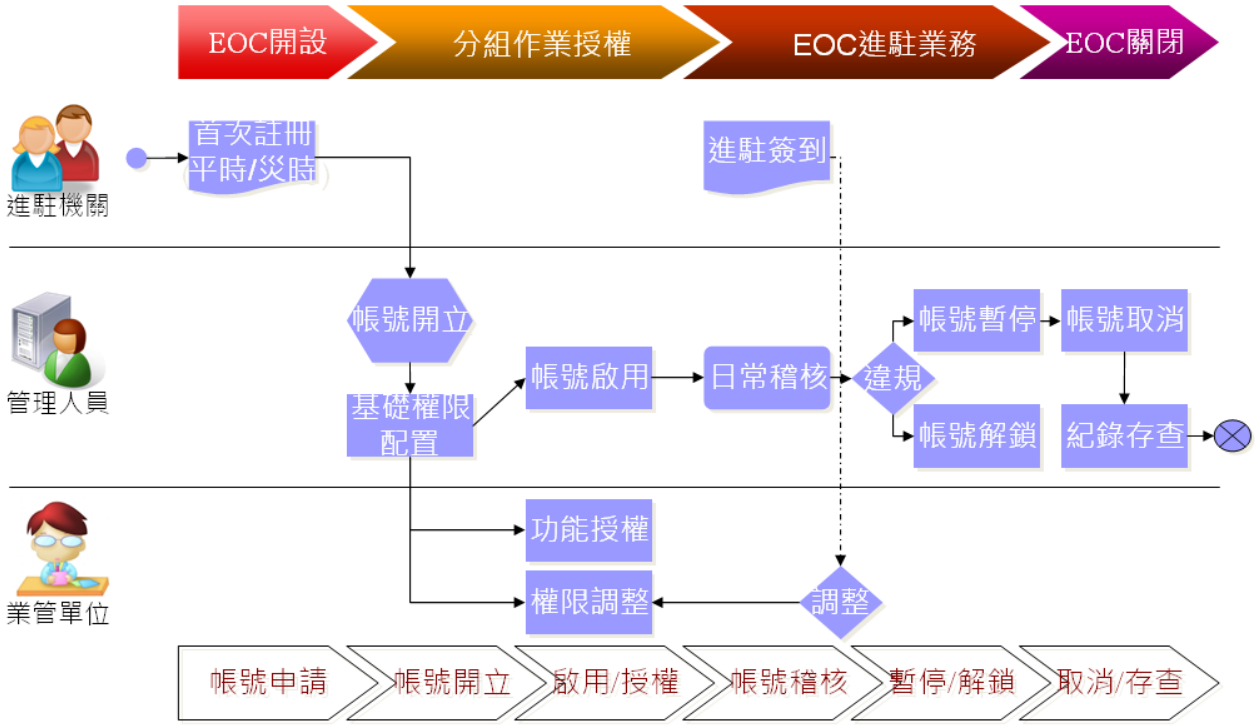


圖 372、進駐機關帳號管理流程

3. 支援廠商帳號管理流程

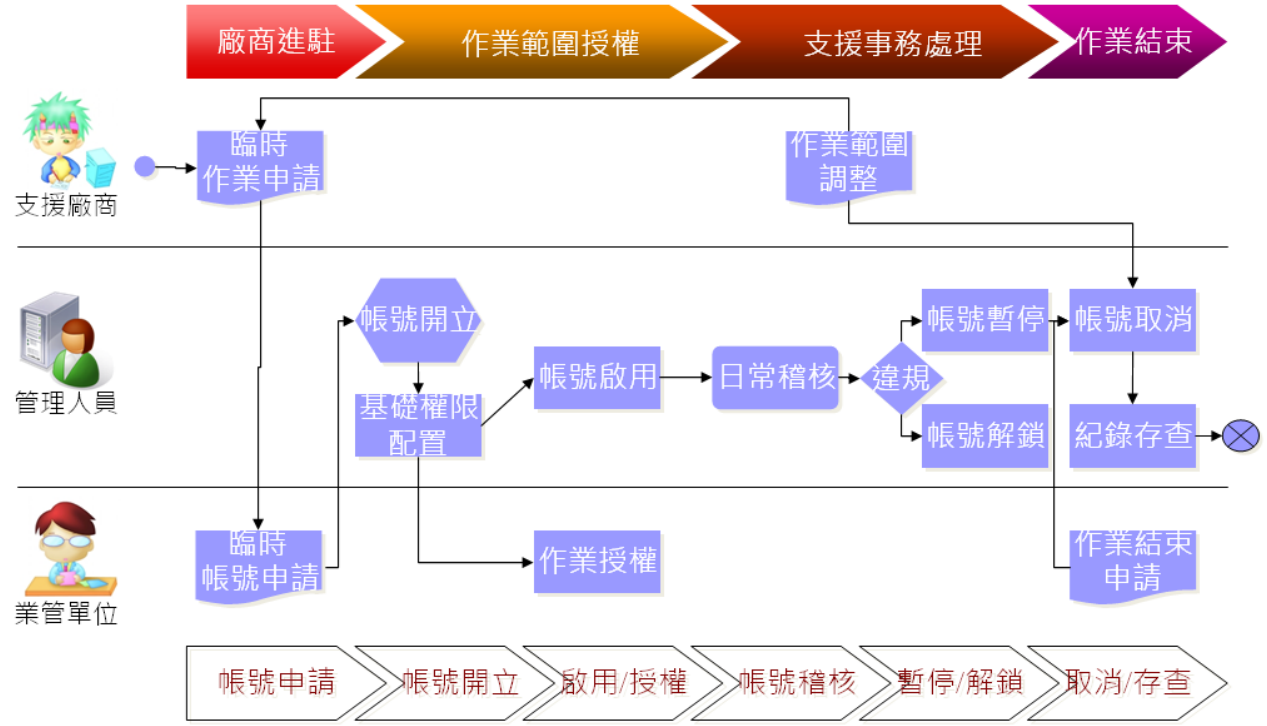


圖 373、支援廠商帳號管理流程

4. 研究機關帳號管理流程

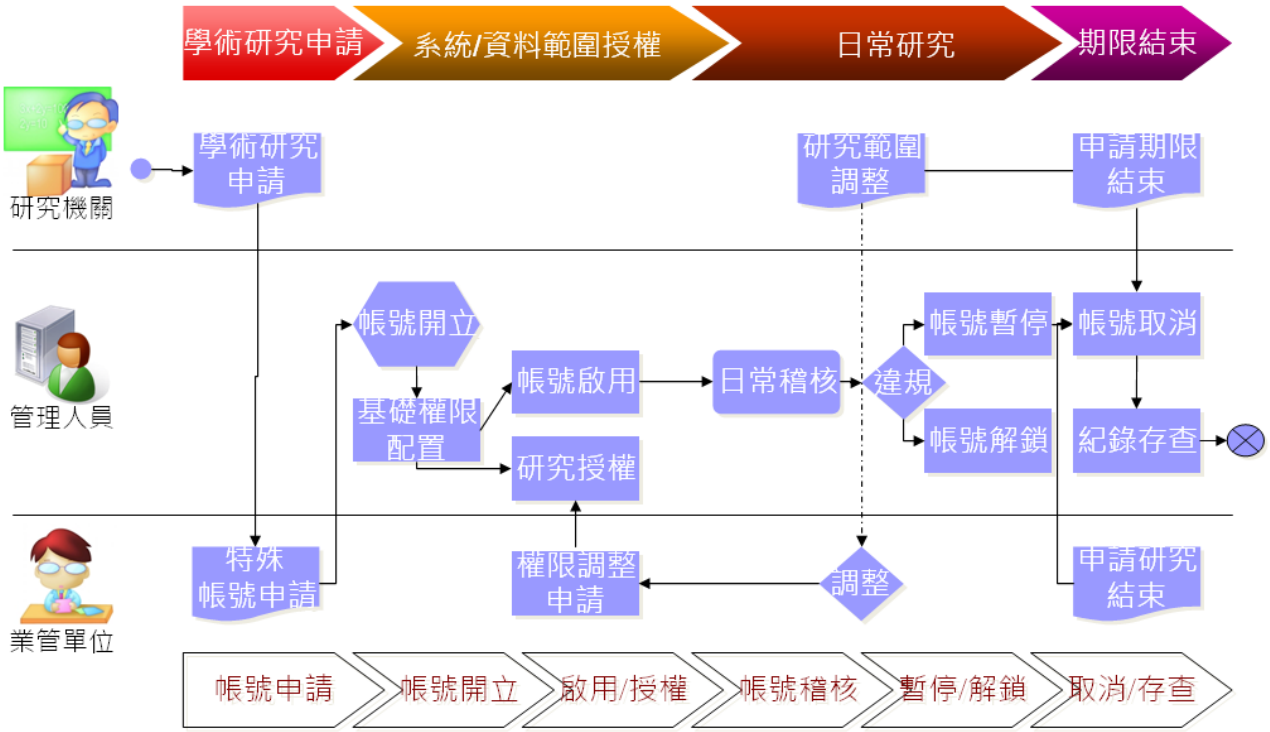


圖 374、研究機關帳號管理流程

5. 災害防救機關帳號管理流程

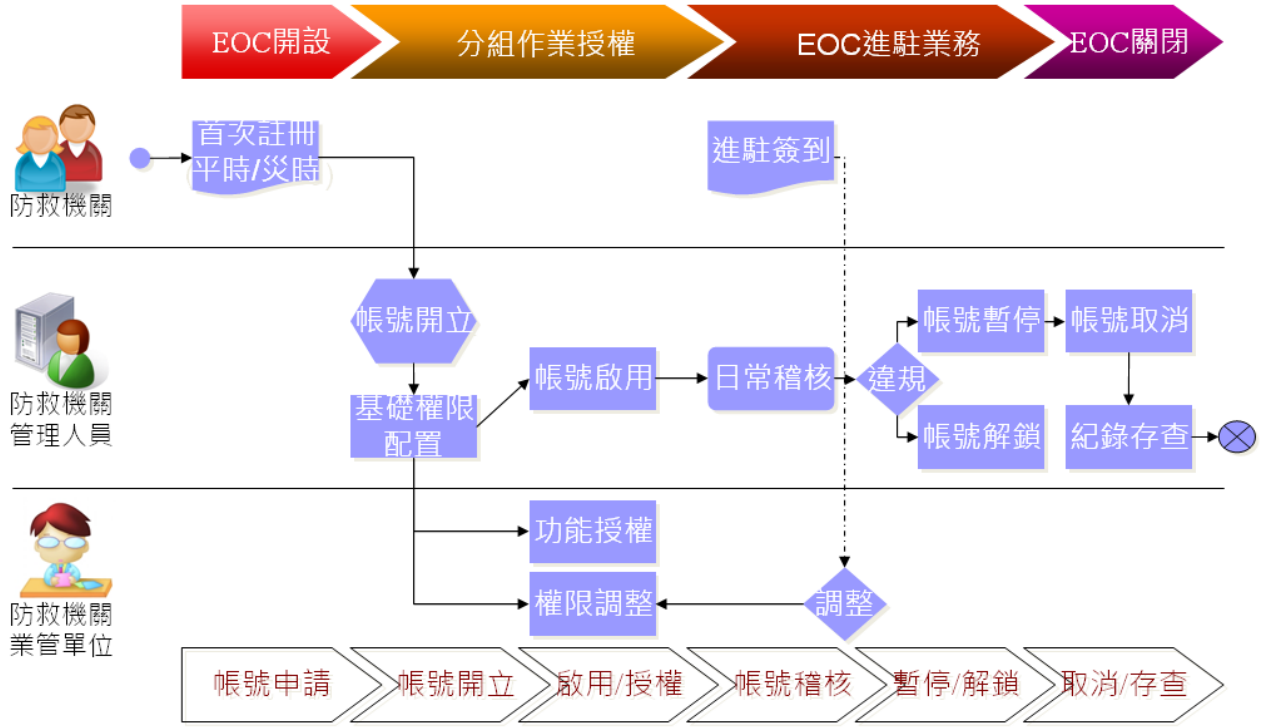


圖 375、災害防救機關帳號管理流程

6. 縣市消防局帳號管理流程

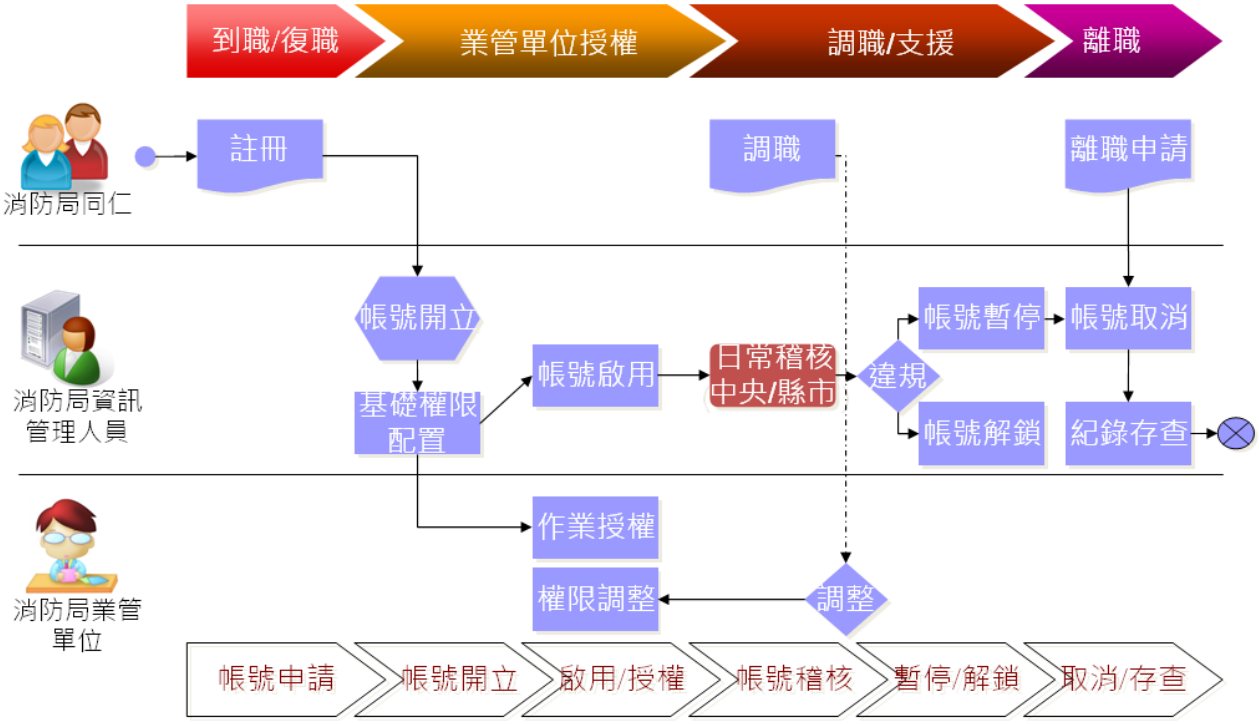


圖 376、縣市消防局帳號管理流程

7. 外部介接系統憑證管理流程

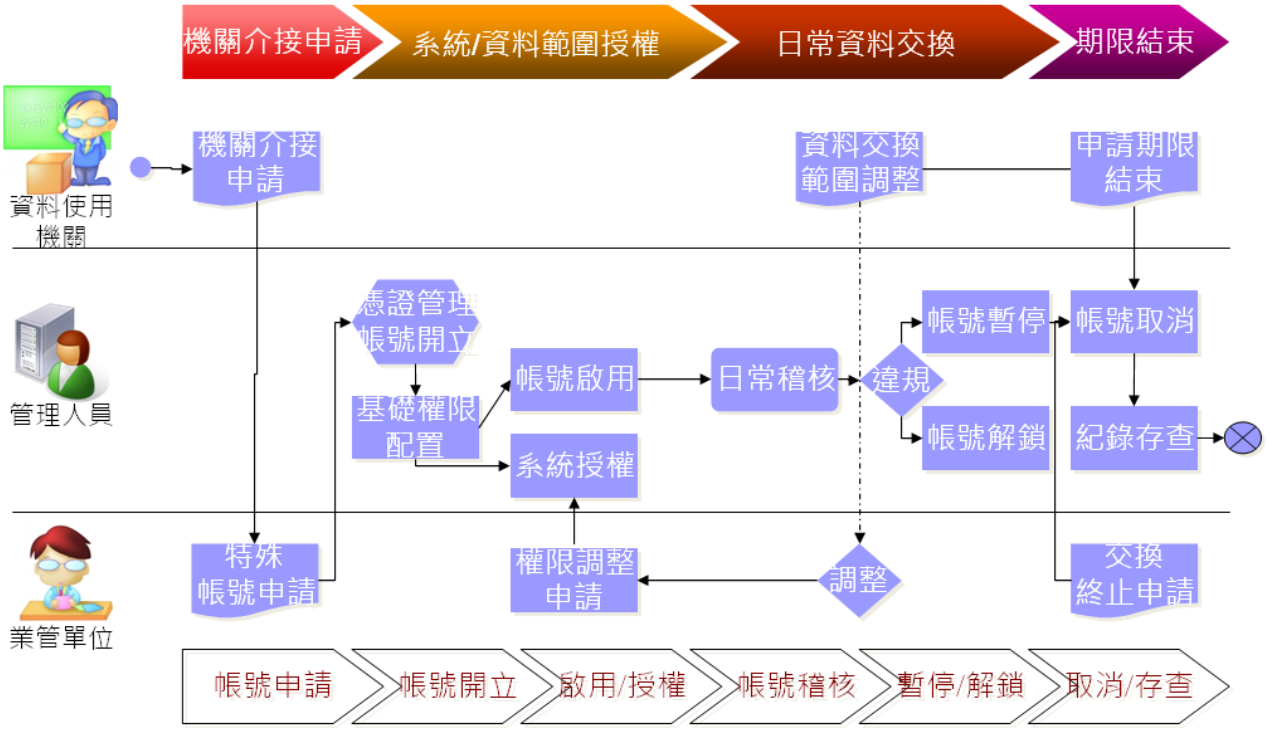


圖 377、外部介接系統憑證管理流程

8. 志工帳號管理流程

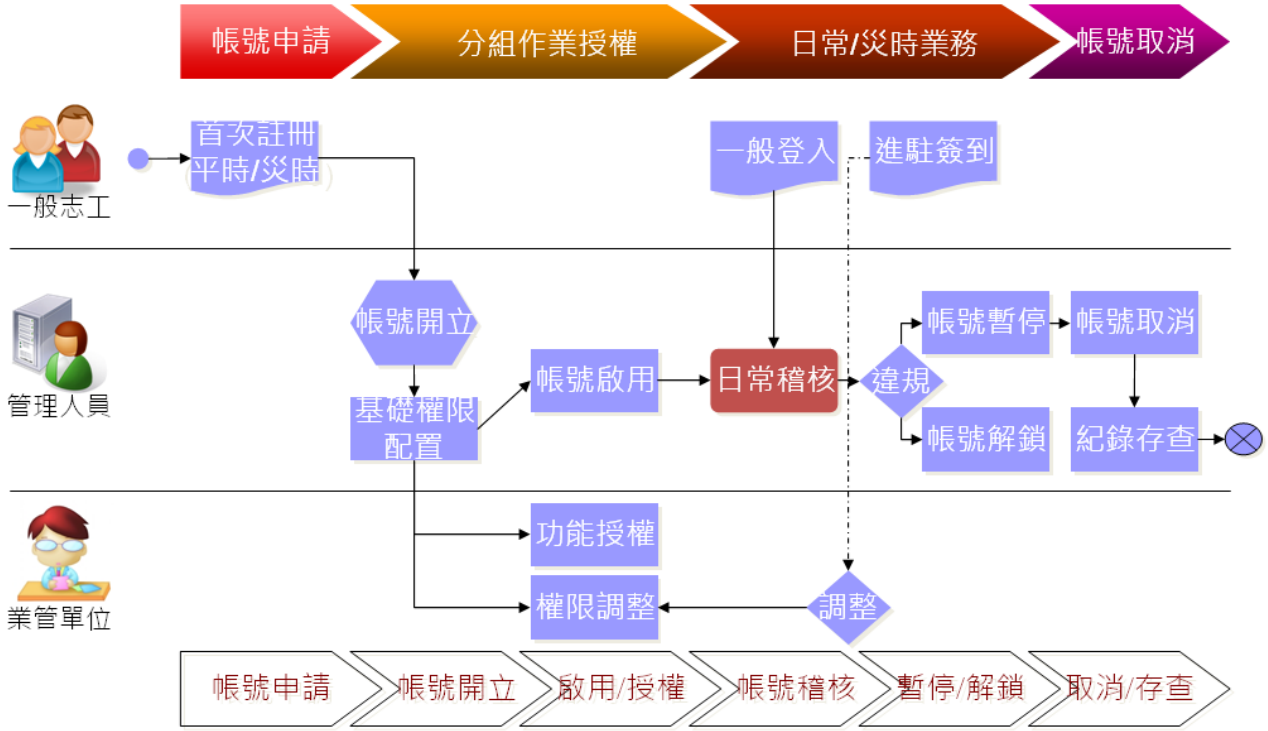


圖 378、志工帳號管理流程

9. 一般民眾帳號管理流程

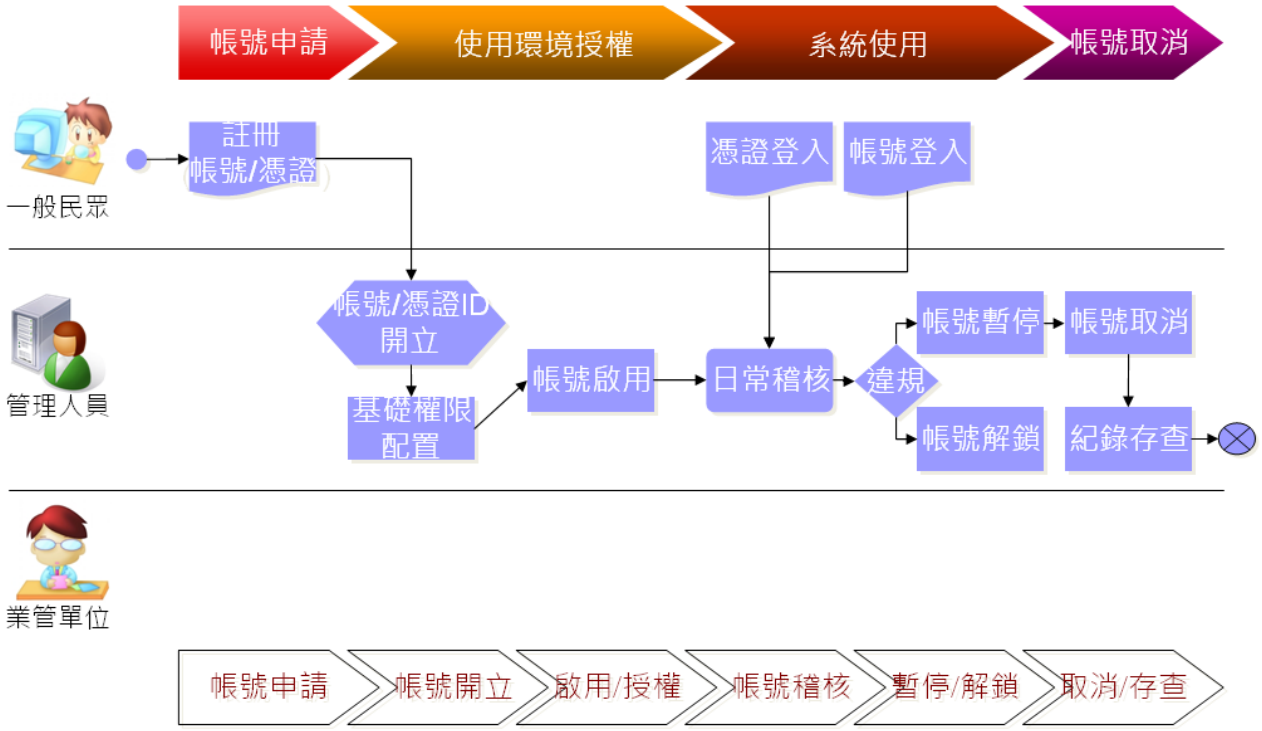


圖 379、一般民眾帳號管理流程

4.4.1.5. 單一簽入規劃服務架構



圖 380、單一簽入服務規劃架構

4.4.1.6. 帳號管理規劃

4.4.1.6.1. 帳號生命周期管控原則

單一簽入之帳號管理機制需對平台之使用者進行帳號生命周期之控管，提供使用者帳號申請介面，以茲使用者進行帳號申請作業。

帳號註冊後需透過平台管理人員進行帳號啟用，並給予基礎權限，帳號之授權需經由業管單位進行授權作業。

帳號之日常行為均需受到資訊安全管理人員之帳號稽核。進入黑名單後或是違反平台安全原則時，系統能自動根據安全原則進行帳號暫停作業。使用者帳號之解鎖需透過申請解鎖介面由平台管理人員或權限管理人員進行帳號之解鎖作業，系統同時也須提供帳號取消與存查等功能。



圖 381、帳號生命周期管控原則示意圖

4.4.1.6.2. 帳號行為稽核管理

單一簽入服務之帳號管理服務，需紀錄所有使用者之登入、授權、系統使用等各項使用狀態紀錄，以進行使用者行為分析稽核作業。系統需提供自行設定分析與稽核範圍，包含使用者之使用狀況，權限之授與及登入情形等，並產生異常帳號與事件清單。

對於特定使用者，帳號管理服務需提供帳號追蹤與列管功能，

以方便查閱指定帳號之狀態。列管清單追蹤之使用者進行登入、授權及使用各種服務時,系統自行進行單一使用者行為追蹤動作，必要時將送出警示訊息或郵件予管理者。針對使用方式異常的使用者，需制定黑名單。

違反特定安全規範或行為時,系統將自行暫停該帳號之權限，並產生資安事件清單列管。超過特定期限或違反特殊事件時，系統管理者將可進行帳號取消作業。



圖 382、帳號行為稽核管理示意圖

4.4.1.6.3. 帳號密碼管理

單一簽入系統需規範密碼安全性原則。密碼安全性原則至少包含嚴禁設定之密碼、應該避免的密碼、密碼強度、密碼長度、密碼組成，以及輔助密碼提示。

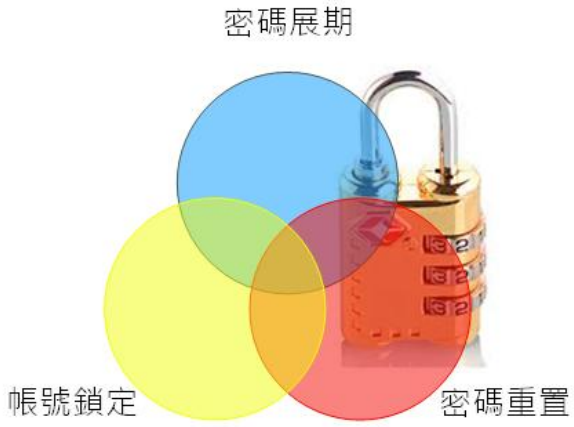


圖 383、帳號密碼管理示意圖

當使用者註冊時，系統需依據密碼安全性原則確認密碼之安全性，包含密碼展期、密碼重置及連續輸入錯誤密碼之帳號鎖定功能，同時也要提供自動發送密碼安全性原則調整通知郵件。



圖 384、帳號註冊申請介面範例

此外系統需提供密碼忘記之輔助密碼提示作業，以及帳號解鎖介面，以供取回密碼與申請帳號解鎖作業。



圖 385、密碼提示申請介面範例

4.4.1.7. 整合應用規劃

4.4.1.7.1. 異質帳號整合

系統需提供 LDAP 異質轉置遷移服務，讓整合後之應用系統其帳號、密碼、系統功能權限表、Profile 等資訊，轉置遷移至本 LDAP 服務內。

對於不同 LDAP 之帳號同步交換作業，系統需提供 LDAP 異質交換服務，讓 LDAP 無法完全遷移之應用系統其帳號、密碼、系統功能權限表、Profile 等資訊得儲存於 LDAP 內，並進行同步作業。

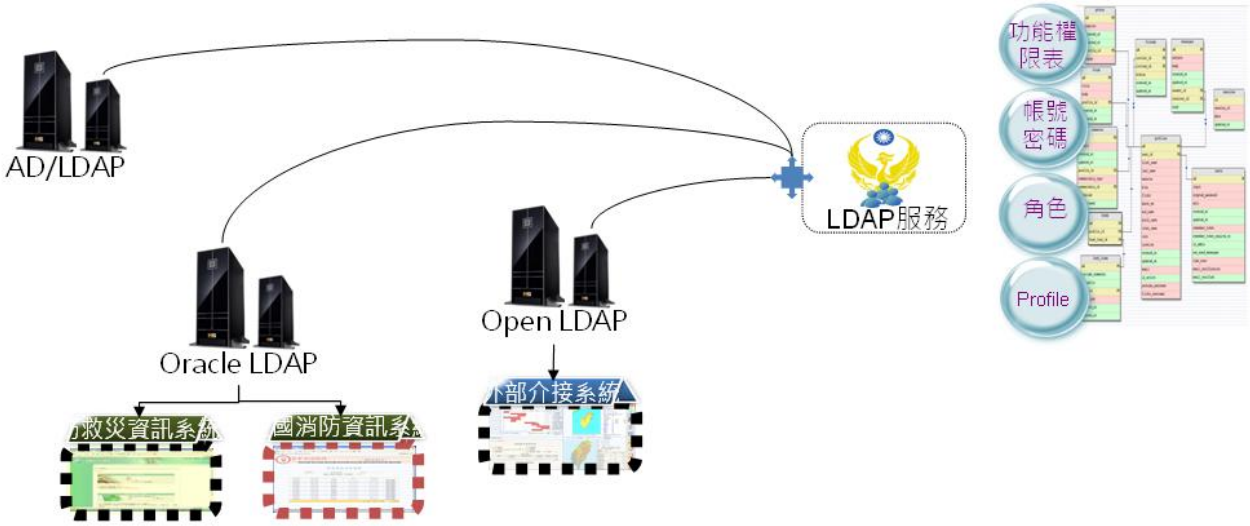


圖 386、異質帳號整合

4.4.1.7.2. 標準單一簽入管理 API 介面

系統需提供標準單一簽入管理 API 介面，讓未來新開發系統及暨有系統均能透過此介面取得帳號權限資訊。此標準單一簽入管理 API 須具備群組管理、帳號管理、密碼管理、安控管理、認證授權、關聯性管理、目錄管理等標準介面。

未來新開發系統均需在授權下，依照此標準 API 進行帳號權限管理作業，以建立帳號角色之 Profile Schema，並依據此設定設定應用服務之權限。

暨有系統需於 LDAP 資訊遷移完畢後，在授權下，建立帳號角色之 Profile Schema，並以此標準 API 進行帳號資訊讀取作業。

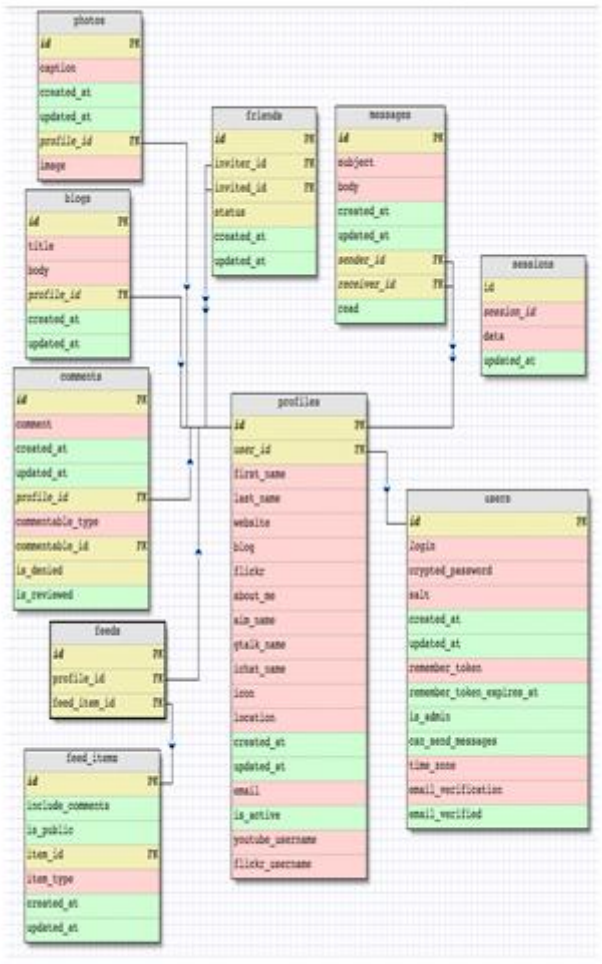


圖 387、標準單一簽入管理 API 示意圖

4.4.1.7.3. 服務整合

1. 一般應用服務整合

欲整合之系統需依據標準單一簽入管理 API 介面，將暨有應用系統之帳號資訊設定於 LDAP 中，並透過系統之角色權限對應，進行權限管理。

2. 元件整合

欲整合之軟體元件需依據標準單一簽入管理 API 介面，將授權配發之帳號紀錄於 LDAP 內，並於每次使用元件時，自動進行登入授權作業。

3. 研考會自然人憑證整合

系統需能提供同時使用 1024 及 2048 位元之憑證管理作業，並與研考會平台進行黑白名單之交換作業，讓使用者能於

首次登錄後即能將憑證資訊儲存於 LDAP 中，並配對至 LDAP 帳號，並於後能直接運用憑證或帳號登入，其餘管理依照一般應用服務之帳號管理進行。

4. 智慧卡整合

系統需能提供同時使用 1024 及 2048 位元之智慧卡管理作業，系統須能將智慧卡晶片 ID 儲存於 LDAP 伺服器內，並配對至 LDAP 帳號，並於後能直接運用智慧卡或帳號登入，其餘管理依照一般應用服務之帳號管理進行。

4.4.2. 資料庫管理

運用累積的天然災害歷史資料，與現行的分析需求為基礎，設計不同新的資料模型，經由線上多維分析機制，可建立各項動態分析報表，成為輔助各機關進行決策的參考。

4.4.2.1. 歷史資料查詢

1. 歷史災害資料與警戒資料查詢

可用日期區間查詢過去曾發生的災害與警戒狀況。

- 資料內容

曾發生或發佈的颱風警報、地震測報、土石流警戒、淹水警示、水位警戒、海嘯警報等等所收集的相關災害與與警戒資料。

2. 歷史災情資料查詢

可用日期區間、災害名稱(如颱風名稱)或雨量站累計雨量、水位站水位資料等。查詢過去曾發生的災情狀況。

- 資料內容

資料時間，災情說明。並顯示關連災害名稱（如地震震度、颱風名稱） 與顯示關聯測站資料（如雨量站、水位站）

3. 測站監測歷史資料

依所收集各測站（包括氣象站、雨量站、水位站與其他已收

集測站） 觀測資料，顯示歷史統計資料。

- 資料內容

可依日、旬、月、季、半年、年、3 年、5 年、10 年等不同統計區間。顯示平均值、最高值、最低值與其他具統計參考觀察意義資料。

4.4.2.2. 多維度分析

依所收集資料，建立各式多維度分析模組，包括颱風警報、豪雨特報、雨量、河川水位、淹水警戒、土石流警戒與災情等多個模組。並可依分析需求，自行組合、重整與計算各模組，來呈現不同的分析結果。且提供提供表格與圖形報表，圖形至少需要包括長條圖、折線圖、圓餅圖以及散布圖等常見圖表。

4.4.2.3. 歷史資料統計

可使用日期或災害為查詢條件，查詢已定義的統計報表包括人員傷亡、維生管線、交通設施通阻、農林漁牧災損、環保除疫、學校災損、淹水情形、水利設施災情與其他有用統計報表。或可自行組合已定義的統計欄位，動態產生新的統計報表。已定義的統計欄位除前述報表之欄位外，應包括各測站監測歷史資料，如雨量、河川水位等。

4.4.3. 圖資服務管理

4.4.3.1. 整合 SOA 平台

SOA（Service-Oriented Architecture），以服務為基礎的分散式處理架構，由服務提供者、服務需求者、及服務仲介者來達成任務需求，以 GIS 來說實作的方式即是提供 GIS Web Service。

GIS Web Service 是軟體元件，它透過 Web 通訊協定及資料格式的開放式標準來為其他的應用程式提供服務，使用者在任何地方都可以使用瀏覽器發出服務需求並獲得服務。

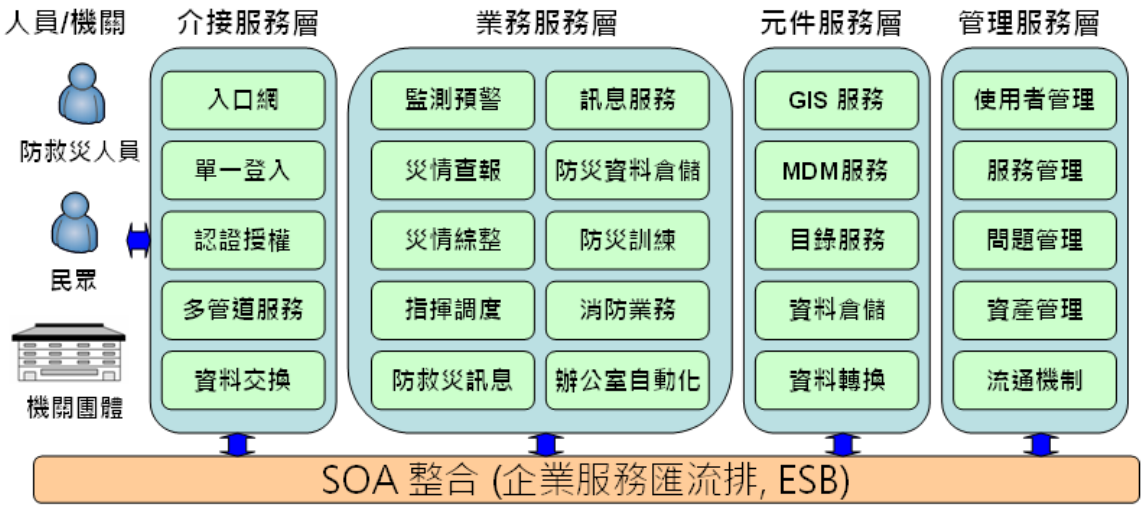


圖 388、防救災雲端之 SOA 架構圖

4.4.3.2. GIS 網路服務架構

- 應用服務（Application Services）
- 目錄服務（Catalog Service）
- 資料服務（Data Services）
  - - Feature Access Service （WFS）
  - - Coverage Access Services （WCS）
  - - Sensor Collection Services （SCS）
  - - Image Archive Services
  - - Location Services （OLS）
  - - GML （geography markup language）
- 功能服務（Processing Services）

  從網路上獲得事先程式化的 GIS 功能，對 GIS 資料進行處理或分析，處理或分析所需的資料可以從網路上獲得，或與功能包裹在一起。
- 繪圖服務（Portrayal Service）
  - - Map Portrayal Service （WMS）
  - - Coverage Portrayal Services （CPS）
  - - Mobile Presentation Services

4.4.3.3. 圖資服務內容

對各項網路服務（如 ESRI map service、web service、WMS、WFS、KML service）提供資料開放狀態設定，可新增、修改、刪除各類服務，並細分為以下二類，並需建置服務內容，說明如下：

4.4.3.3.1. 資料服務

可對外發佈 GIS 網路服務（包括 WMS，WFS），依需求新增資料服務，至少提供災情分佈 WMS 及 WFS。

4.4.3.3.2. 功能服務

4.4.3.3.2.1. 定位查詢類

（1）門牌地址定位：提供輸入門牌地址文字查詢，結果若為 1 筆以上，會將 N 筆結果回應給使用者。定位提供完全比對及模糊比對兩種不同方式，其比對邏輯，完全比對針對輸入文字至門牌資料庫搜尋，需一模一樣找到結果；模糊比對之門牌定位，若完整輸入找不到門牌，依序回頭找弄、巷、段、路名，查詢後結果為 1 筆以上時，提供查詢結果清單，由使用者選擇取最佳及最適之門牌。

（2）交叉路口定位：請參考【定位查詢】章節。

（3）道路 K 數定位：請參考【定位查詢】章節。

（4）高速公路 K 路定位：請參考【定位查詢】章節。

（5）座標定位（經緯度或 67、97 都要能夠被轉換定位）：請參考【定位查詢】章節。

（6）南北島圖號定位：請參考【定位查詢】章節。

（7）重要地標定位：請參考【定位查詢】章節。

（8）簡易定位：：請參考【定位查詢】章節。

4.4.3.3.2.2. 應用查詢類

需針對各業務應用系統依需求製定修改相關服務，至少提供以下項目：

（1）依座標點位找到最近的 POI（醫院、消防分隊、警察局及學校）。

（2）依座標點位找到最近的避難場所。

（3）依座標點位是否落在警戒區（淹水警戒及土石流警戒）內。

（4）路徑規劃考量避開交通通阻路段及淹水災情，選擇安全性較高之路線。

4.4.3.4. 服務權限控制

GIS 空間服務需與 SOA 平台整合，服務取用之權限也依 SOA 平台權限管理之規則。

5. 災害防救業務雲端之平台服務規劃

5.1. 災害防救平台服務架構

災害防救平台服務規劃主要是針對防救災雲端整體架構中的 PaaS 進行說明。平台服務層為整體雲端架構中界於「應用服務層」及「基礎服務層」之中間層軟體，為組合及支持上層應用服務，提供所需之共用軟體組件及底層基礎服務，並利用下層之基礎服務層所提供之網路、硬體、存儲設備等實體資源，以達最佳使用效率。以水平橫向由下往上堆疊展開之層次來看，包括中介軟體層、服務層、服務整合層以及入口層等層，越接近上層越由系統軟體偏向領域應用之軟體組件;為求平台服務層之整體軟體組件運作效率及資訊安全之考量，需考量規劃縱向橫跨水平層次之服務件管理以及資訊安全之管理工具導入。

「平台服務層」為未來持續堆疊建構上層創新服務之重要軟體基礎。其整體設計架構以 SOA(服務導向架構)概念貫穿。服務層級間鬆散耦合，獨立運作但又可彼此間串聯成服務使用。SOA 架構下的服務開發，都是引用資訊業界所共同定義的標準，未來不論是開發、整合、維護、尋求外界人力或服務，都能輕易將系統透過此一標準將所有系統及資源整合起來。平台服務模塊如下圖：



圖 389、防救災雲端平台服務範圍