國立科學工藝博物館

會員系統優化服務規劃設計

(案號 114026)

規劃設計報告書

目錄

第壹章 需求規格分析 3
一、 系統功能擴充 3
二、 大數據與分眾分析 9
(一) 綜合分析 9
(二) 館內活動軌跡 11
(三) 參觀行為分析 14
(四) 收入來源分析 16
(五) 會員忠誠度分析 17
(六) 教育活動成效分析 19
(七) 會員級別標籤 20
(八) 各式報表產出 21
(九) 訪客模式分析 21
第貳章 系統架構分析 22
一、 系統架構分析 22
(一) 現有系統整體架構 22
(二) 系統功能架構 23
(三) 系統技術框架 24
(四) 行為地點資訊架構 27
二、 系統功能擴充 30
(一) 註冊流程簡化 30
(二) 前台功能擴充 35
(三) 後台功能擴充 39
(四) 自動提醒功能 48
(五) 單一簽入驗證 49
三、 大數據與分眾分析 50
(一) 綜合分析 50

(二) 館內活動軌跡 53
(三) 參觀行為分析 59
(四) 收入來源分析 65
(五) 會員忠誠度分析 68
(六) 教育活動成效分析 71
(七) 會員級別標籤 73
(八) 各式報表產出 77
(九) 訪客模式分析 77
四、 API 功能擴充與介面規劃 78
(一) API 清單 78
(二) API 設計 78
(三) 會員系統軌跡資料紀錄 81
第參章 建置期程 82
一、 建置期程 82
(一) 會員系統 82
二、 交付文件 87
(一) 交付文件說明 87
(二) 雙向追溯表說明 88
第肆章 資訊安全法規及標準(資通系統防護基準) 90
一、 資通系統防護基準 SSDLC 檢核表 90
二、 資通系統防護基準控制措施 105

第壹章 需求規格分析

一、系統功能擴充

1、註冊流程簡化

(1)註冊必填簡化為以下欄位：姓名、電子郵件（唯一值）、身分證字號（唯一值）、性別、出生年月、居住地區（縣市）等 6 欄位。

(2)會員註冊功能需增加「個資宣告」之資訊（勾選同意後啟能註冊）。

(3)考量會員資訊有效性以及系統資訊完整性與一致性（避免重複、冒用），「電子郵件」資訊加入驗證機制。

(4)配合會員註冊必填欄位簡化，「申辦年卡」時需先填寫完原必填欄位後，始能繼續申辦流程。

(5)系統以工作階段（Session）機制保留民眾註冊時填寫之個人資訊，避免於收不到電子郵件驗證信或他情況而反覆操作系統時，需重複填寫。

(6)註冊流程依以下步驟優化：

A、民眾填寫註冊資訊(如上述 6 項必填欄位)

B、系統發送電子郵件確認信至民眾信箱

C、民眾點選電子郵件之確認信連結(系統狀態標示為註冊成功)

D、點選後，系統提示「電子郵件已確認，請確認您的下列註冊資訊是否正確」 (下接民眾已填寫之註冊資訊)。

E、民眾點選「確認無誤」後，完成註冊，並導至登入頁面並提示以剛剛輸入的帳密登入。

F、上述「電子郵件」填寫與驗證可透過 Google/FB 等第三方登入方式整合，直接代入不需額外填寫與驗證。

2、前台功能擴充

(1)前台設計原則為「行動優先」(Mobile First)，以資訊簡潔與設計簡化為方向。

(2)訊息功能(通知中心)增加圖文區塊功能，圖片應能自動擷取固定大小，設計風格以簡潔為主，以維持版本清爽。

(3)訊息功能(通知中心)增加短影音區塊，以單欄設計，資訊連結至本館 FB Reels 社群。

3、後台功能擴充

(1)會員資訊管理

A、會員資訊之查詢條件擴增為以下欄位：

(A)起迄日：查詢會員行為紀錄之起迄日；增加單選選項「註冊日」與「活動日」，以區分針對會員行為起迄日之狀態查詢。

(B)會員身分：選項為多選，包含：有效年卡、無效年卡、未辦年卡。

(C)五年未登入：以檢核項(Checkbox)選擇，勾選則列出五年未登入之帳號。

(D)性別：選項為多選（Checkbox），選項包含：男、女及其他；預設為「全選」。

(E)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區「北、中、南、東、其他」分類 (同大數據分析)

(F)年齡區間(上下限)：預設為空值(不限制)

(G)證件編號：以精確搜尋(Exact search)進行編號查詢。

(H)會員姓名：以模糊搜尋(Fuzzy search)進行姓名查詢。

(I)電子郵件：以模糊搜尋(Fuzzy search)進行查詢。

(J)團體會員：選項為多選，包含：是、否。

(K)訂閱電子報：，選項為多選，包含：是、否。

(L)紅利點數(上下限)：預設為空值(不限制)

B、查詢結果需包含以下欄位：會員編號、會員等級、會員姓名、現有點數、本年度到期點數、註冊日期、最後活動時間。

C、會員查詢結果中，點選各「欄位標題」可進行排序方式切換(正排版/反排版/預設排序)。

D、「到期點數」計算規則為當年度所累積點數，點數到期日為當年度 12 月 31 日(含)前使用完畢，若未使用將會自動歸零重新計算，恕無法展延使用。

E、會員之最後登入時間計算，應包含整合於 SSO 範圍內系統，所有會員之登入行為(現行會員系統無依此範圍記錄)。

F、「會員編號」改以「時序」進行編號：新註冊會員之會員編號應大於較早註冊會員之編號。

G、「查詢條件」區分精簡模式與進階模式，以開闔功能進行切換。預設為「精簡模式」。

H、會員資料查詢結果之「分頁導覽」(上下頁)功能，增加可直接輸入「頁碼」以導至該頁之功能。

I、後台編輯資訊時，若遇輸入特殊字元而系統阻擋時，應有提示文字說明與警示。

(2)信件發送功能

A、以所見即所得編輯器，進行發送內容之簡易編輯。

B、編輯內容後，以類同「會員資訊管理」之查詢條件篩選出欲發送之會員名單。

C、發送電子郵件給以上步驟指定之會員

(3)操作介面優化：以統一風格與 UI/UX 優化後台系統功能介面，包括後台新增功能與原有會員管理、紅利商品、系統管理、權限管理等功能。

4、自動提醒功能

(1)系統以電子郵件自動提醒一年未登入或未更新個資之會員。經提醒一次後，若一週後尚未登入或更新個資則再提醒一次。

(2)若會員五年未登入，系統以電子郵件提醒，並於確認五年未登入後自動刪除帳號（以資料隱碼處理）。提醒機制規劃為提早 1 個月提醒，若到期日仍未使用系統則逕行刪除。

(3)系統以電子郵件自動提醒會員點數即將到期。配合「點數到期」時間，提早 1 個月提醒，若到期日仍未使用自動歸零計算。

5、單一簽入驗證

(1)功能需求

(A)依 OAuth 2.0 (OpenID Connect) 以及已制定之程式流程架構，建置單一簽入功能。

(B)單一簽入使用系統之用戶編號 (client_id 與用戶金鑰 (client_secret) 由後台管理系統設定並取得。

(C)提供 C# 語言範例程式，供館方應用系統加入單一簽入機制參考與使用。

(D)可透過單一簽入由會員中心系統登入本館其他系統；若已於會員系統登入，於本館其他系統可自動登入，不需重複輸入帳密。

(E)支援第三方帳號登入，民眾透過 Google 或 FB 等帳號即可以登入，並與簡化後會員註冊與登入流程整合，登入後再補充資料即可。

(2)技術規格

A、建置遵循規範 OAuth 2.0 與 OpenID Connect。

B、實作機制依循《Google Identify OpenID Connect》之設計規範。

C、依「OAuth 2.0 與 OpenID Connect」規範建置之ＳＳＯ功能：

二、大數據與分眾分析

(一)綜合分析

建置大數據分析之「綜合分析」功能，籍由後台介面，可綜合統計與分析會員之行為次數、紅利點數、消費金額等面向。

1、系統可依下列條件進行分析：

(1)分析範圍：多選（Checkbox），選項包括：會員系統、掌握科工、推教系統、團約系統；預設為「全選」。

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類：

A、北部地區：臺北市、新北市、基隆市、新竹市、桃園市、新竹縣、宜蘭縣

B、中部地區：臺中市、苗栗縣、彰化縣、南投縣、雲林縣

C、南部地區：高雄市、臺南市、嘉義市、嘉義縣、屏東縣、澎湖縣

D、東部地區：花蓮縣、臺東縣

E、其他：包括金門縣、連江縣及境外地區。

【註】介面支援「收闔」設計，提供「全選/反選」區域操作功能。

(5)年齡區間(上下限)：預設為空值(不限制)

(6)紅利點數(上下限)：預設為空值(不限制)

(7)消費金額(上下限)：預設為空值(不限制)

(8)紅利給點：多選形式，選項包括：智慧展示、紅利活動、展品報修、意見回饋。

(9)會員編號或姓名：關鍵字查詢。

2、分析結果之「圖表輸出」可依下列條件選擇輸出資料與格式：

(1)Y 軸資料：單選，選項為：行為次數、紅利點數、消費金額

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳、年齡分布、居住地、會員等級

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

3、承上之「X 軸資料」，「年齡分布」分析之年齡分布區間如下：

(1)10 歲以上未滿 13 歲

(2)13 歲以上未滿 16 歲

(3)16 歲以上未滿 19 歲

(4)19 歲以上未滿 25 歲

(5)25 歲以上未滿 35 歲

(6)35 歲以上未滿 45 歲

(7)45 歲以上未滿 55 歲

(8)55 歲以上未滿 65 歲

(9)65 歲以上

(二)館內活動軌跡

系統大數據分析應具備「館內活動軌跡」分析功能，分析與輸出需求說明如下。

1、分析條件

(1)起迄日：查詢會員行為紀錄之起迄日。

(2)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(3)館內位置：選項多選，涵蓋館內可分析位置，預設為「全選」，並依樓層分類：

A、本館 B3：臺灣農業的故事

B、本館 B1：兒童科學園區、氣候變遷、開放式典藏庫、電影院、售票處

C、本館 1F：售票處、入口

D、本館 2F：動力與機械、烹調的科學、電信@臺灣、印象深刻、入口

E、本館 4F：交通夢想、衣技織長、健康探索廳、科學開門、科學桂冠、技職展區、電池小火車、地震體驗屋、智慧駕車遊高屏

F、本館 6F：希望·未來莫拉克風災紀念廳、太空飛行探索廳、臺灣工業史蹟廳、4D 太空飛行、月球漫步

【註】介面支援「收闔」設計，提供「全選/反選」樓層操作功能。

(4)年齡區間(上下限)：預設為空值(不限制)；年齡區間設定同「綜合分析」。

2、圖表輸出

(1)Y 軸資料：多選，選項為：行為次數、停留時間(分)、紅利點數

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

3、館內位置

館內「實體位置」資訊，應統一以下「展廳」名稱記錄與分析：

樓層	展廳	智慧展示	展廳導覽	展品報修	會員系統
本館 B3	臺灣農業的故事	V	V	V	
本館 B1	兒童科學園區(奇幻國/Fun 城市/夢想號)		V	V	V
	氣候變遷		V	V	
	開放式典藏庫		V		
	電影院				V
	售票處				V
本館1F	售票處				V
	入口				V
	東側入口				V
	西側入口				V
本館2F	動力與機械	V	V	V	
	烹調的科學	V	V	V	
	電信@臺灣		V	V	
	印象深刻				V
	東側入口				V
	西側入口				V
本館4F	交通夢想		V	V	
	衣技織長	V	V	V	
	健康探索廳	V	V	V	
	科學開門		V	V	
	科學桂冠		V	V	
	技職展區			V	
	電池小火車				V
	地震體驗屋				V
	智慧駕車遊高屏				V
本館6F	希望·未來莫拉克風災紀念廳		V	V	

	太空飛行探索廳		V	V	
	臺灣工業史蹟廳		V	V	
	4D 太空飛行				V
	月球漫步				V

會員系統「行為軌跡」之實體位置應以下表之「設備代碼」與「展廳」資訊代入並進行分析。

設備類型	設備代碼	設備名稱	樓層	展廳
體驗設施電子扣款機系統	E01	體驗設施電子扣款機 1 (6 樓太空廳)	6F	太空飛行探索館
體驗設施電子扣款機系統	E02	體驗設施電子扣款機 2 (4 樓智慧運輸)	4F	智慧駕車遊高屏
體驗設施電子扣款機系統	E04	體驗設施電子扣款機 4 (B1Fun 城市)	B1	兒童科學園區
體驗設施電子扣款機系統	E13	體驗設施電子扣款機 1 (2F 刻印)	2F	印象深刻
體驗設施電子扣款機系統	E14	體驗設施電子扣款機 4 (4F 長廊)	4F	電池小火車
體驗設施電子扣款機系統	E15	體驗式扣款機(B1Fun 城市 2)	B1	兒童科學園區
自動驗票系統	G01	自動驗票機_1F_東側入口	1F	東側入口
自動驗票系統	G02	自動驗票機_1F_西側入口	1F	西側入口
自動驗票系統	G03	自動驗票機_2F_東側入口	2F	東側入口
自動驗票系統	G04	自動驗票機_2F_西側入口	2F	西側入口
自動驗票系統	G05	自動驗票機_B1_劇院入口	B1	電影院
POS 系統	P01	售票窗口：P01 (1F-5)	1F	售票處
POS 系統	P02	售票窗口：P02(1F-6)	1F	售票處
POS 系統	P03	售票窗口：P03 (1F-8)	1F	售票處
POS 系統	P06	售票窗口：P06 (1F-備機)	1F	售票處
POS 系統	P04	售票窗口：P04 (B1-9)	B1	售票處
POS 系統	P05	售票窗口：P05 (B1-7)	B1	售票處
自動售票機系統	T01	自動售票機 1 (1F)	1F	入口
自動售票機系統	T02	自動售票機 2 (1F)	1F	入口
自動售票機系統	T03	自動售票機 3 (1F)	1F	入口
自動售票機系統	T04	自動售票機 4 (B1F)	B1	電影院
自動售票機系統	T05	自動售票機 5 (B1F)	B1	電影院

(三)參觀行為分析

1、觀眾入館頻率

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

B、資料範圍：全館、樓層(下拉式選單選擇樓層、展廳(下拉式選單選擇展廳)。

(2)圖表輸出

A、Y 軸資料：單選，選項為：行為次數

B、X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

(3)資料來源：由介接容留系統 API 取得資訊。

2、觀眾入館再訪率

(1)分析條件

A、起迄日：觀眾入館行為之起迄日。

(2)圖表輸出

A、Y 軸資料：單選，選項為：再訪率(%)

B、X 軸資料：單選，選項為：年度、季度、月份

C、圖表類型：單選，選項為：長條圖、折線圖

(3)定義再訪率與計算方式

再訪率 (%) = 再訪觀眾不重複人次 ÷ 入館觀眾不重複人次

A、再訪觀眾人次：同一人入館 2 次以上即算「再訪者」，同日多次入館僅計 1 次。

B、入館觀眾人次：所有入館觀眾不重複人次。

C、計算範圍涵蓋所有館內相關活動之入館記錄。

(4)資料來源：會員系統行為軌跡。

3、觀眾入館時段

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

(2)圖表輸出

A、Y 軸資料：單選，選項為：行為次數

B、X 軸資料：單選，選項為：小時

C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

(3)資料來源：由介接容留系統 API 取得資訊。

4、觀眾停留時間

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

B、資料範圍：全館、樓層選擇、展廳選擇。

(2)圖表輸出

A、Y 軸資料：單選，選項為：停留時間(分)

B、X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

D、資料分析

(A)以連續性行為分析觀眾停留時間

(B)可假設單次行為之「停留時間」。例如「紅利活動」可為 30 分鐘或 1 小時，亦或可於「紅利活動管理」功能，進行「活動時長」之設定，代入分析機制，以利後續分析。

(C)平均停留時間：總停留時間 ÷ 觀眾人數

藉由「容留系統」資訊，我們亦可透過以利特爾法則（Little's law），推算館內觀眾的平均停留時間：

$$\text{平均停留時間} = \frac{\sum \text{當前館內人數}}{\sum \text{每分鐘入館人數}} = \frac{\sum_{t=1}^{T} N_{\text{館內}}(t)}{\sum_{t=1}^{T} N_{\text{入館}}(t)}$$

其中：

- $N_{\text{館內}}(t)$ = 時間 t 的館內人數
- $N_{\text{入館}}(t)$ = 時間 t 的入館人數
- T = 觀察的時間長度（分鐘）

(3)資料來源：由介接容留系統 API 取得資訊。

（四)收入來源分析

1、分析條件

(1)收入來源分析：多選，包括：售票收入、商品收入、活動收入

(2)資料範圍：多選，包括：實體購票收入、線上購票收入（掌握科工）、商品收入（掌握科工）、科教活動

(3)起迄日：查詢會員行為紀錄之起迄日。

(4)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(5)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(6)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：營收金額

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、票種

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

（五）會員忠誠度分析

1、分析條件

(1)資料範圍：消費活動、紅利活動、體驗活動、教育活動

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(5)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：會員數

(2)X 軸資料：單選，選項為：忠誠度區分

(3)圖表類型：單選，選項為：長條圖、圓餅圖

3、分析模型

A、RFM 模型

以 RFM 模型計算會員忠誠度：

(A)Recency（R）：距離會員最近一次購買的時間（天數）。

(B)Frequency（F）：會員在特定時間內購買的次數。

(C)Monetary（M）：會員在特定時間內累積消費金額。

示例數據：

會員ID	最近購買天數 (R)	購買次數 (F)	總消費金額 (M)
A123	10	5	5000
B456	30	3	2000
C789	5	10	10000

B、計算方法

會員忠誠度計算方法：以分群方式分 5 群，分別給 1-5 級(分)：

(A)R：越小越好（最近購買的會員較忠誠）；最小的 20% 給 5 分，最大 20% 給 1 分。

(B)F：越大越好（購買頻率高表示忠誠度高）；最小的 20% 給 1 分，最大 20% 給 5 分。

(C)M：越大越好（高消費會員價值較高）；最小的 20% 給 1 分，最大 20% 給 5 分。

C、分級方法

例如依會員忠誠度，分為金、銀、銅三級。

其中，依據 RFM 總分，將會員劃分以下忠誠度群組：

(A)**金科工：RFM 總分 12～15**；忠誠會員，應提供特殊優惠。

(B)**銀科工：RFM 總分 8～11**；潛力客戶，可透過行銷活動強化關係。

(C)**銅科工：RFM 總分 3～7**；可能流失的會員，可用促銷或再行銷策略吸引回購。

D、消費金額計算

(A)票券購買

(B)商品消費

(C)課程消費

（六)教育活動成效分析

1、分析條件

(1)起迄日：查詢會員行為紀錄之起迄日。

(2)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(3)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(4)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：參與人數、消費金額、活動紅利、後續參與率

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、關鍵字分析

(3)關鍵字分析：夏令營、冬令營、週日閱讀、海外科學營、春季班、生活學堂、體驗活動、創客、其他

(4)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

3、後續參與率

(1)定義：「後續參與率」=

參與 2 次以上活動的學員數÷全體參與學員數×100%

(2)可作為評估學員忠誠度與活動吸引力的核心指標。

（七）會員級別標籤

1、分析條件

(1)資料範圍：消費活動、紅利活動、體驗活動、教育活動

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(5)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：會員數

(2)X 軸資料：單選，選項為：會員級別

(3)會員級別：全館會員級別、客制化會員級別 A、客制化會員級別 B……

(4)圖表類型：單選，選項為：長條圖、圓餅圖

3、客製化會員級別規則制定

(1)演算法：RFM 模型

(2)資料範圍：消費活動、紅利活動、體驗活動、教育活動等(多選)

(3)會員級別名稱

(4)級別組數：1-13

(5)級別命名：各組以文字輸入命名

(6)級別範圍：各組以「分數上限」設定級別範圍

4、客製化會員級別範例

(1)資料範圍：選擇「消費活動、紅利活動」

(2)會員級別名稱：消費紅利級別

(3)級別組數：5

(4)級別命名：博士、達人、大師、玩家、青銅

(5)級別範圍

A、博士 (不需選擇上限，預設 15)

B、達人 (上限 13)

C、大師 (上限 11)

D、玩家 (上限 8)

E、青銅 (上限 5)

(八)各式報表產出

行為分析報告及票務等級報表之產出，其功能與介面整合於各大數據分析之「功能按鈕」中。每一組大數據分析功能皆有三種圖表輸出功能，包含：網頁輸出(HTML)、報表產出(Excel/ODS)、原始資料(Excel/ODS)。其中，「報表產出」即為以統計表格方式輸出大數據分析之結果。

(九)訪客模式分析

1、以數位存根(Http Cookie)鑑別訪客模式之使用者行為。以虛擬會員編號作為唯一值識別訪客行為足跡。

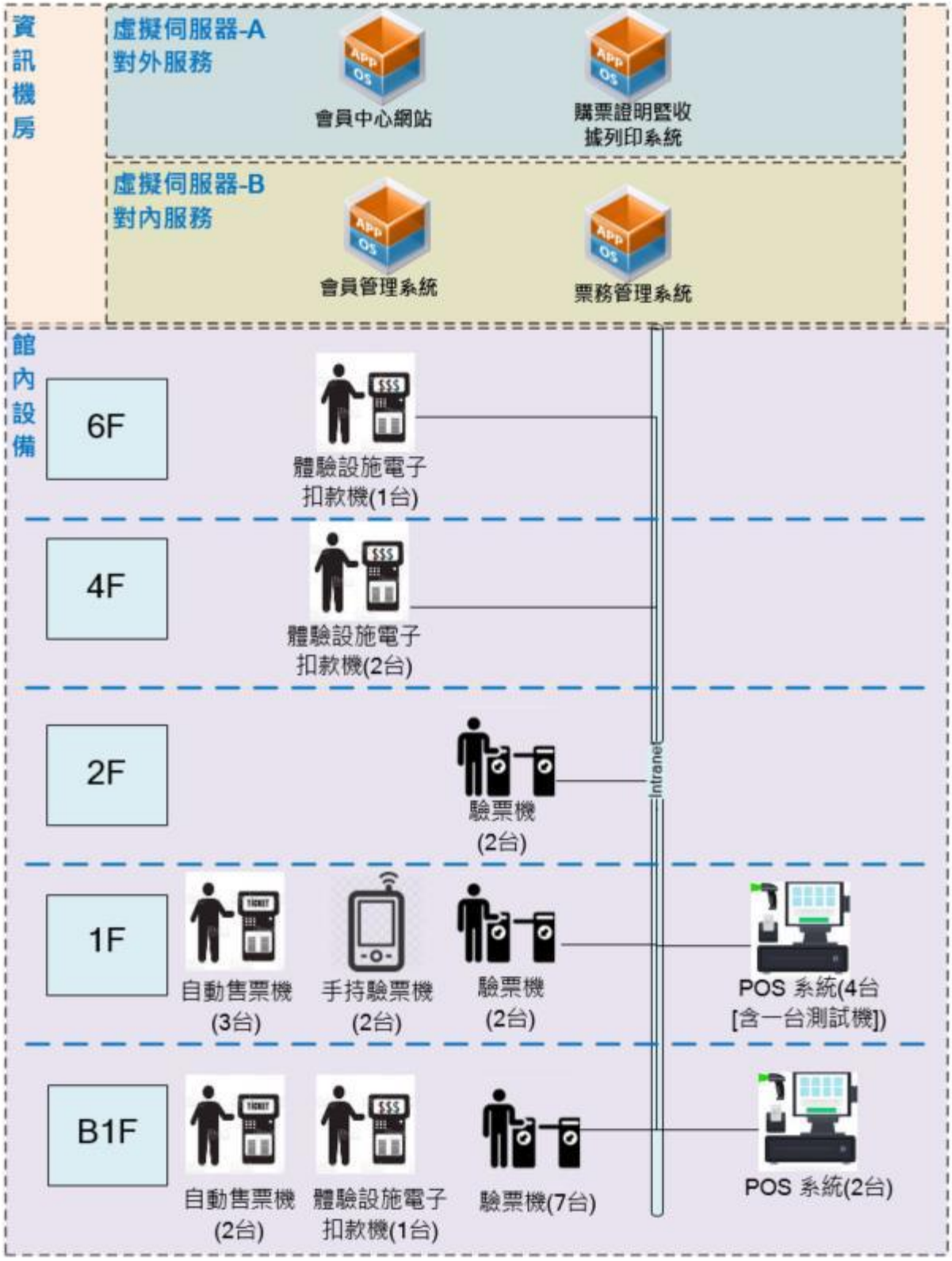
2、整合未來其他系統訪客模式之行為分析，例如訪客模式之線上購票、意見回饋、展廳導覽等行為。

3、整合訪客模式之實體行為足跡，例如訪客模式之展廳導覽(QR Code 掃描)等行為

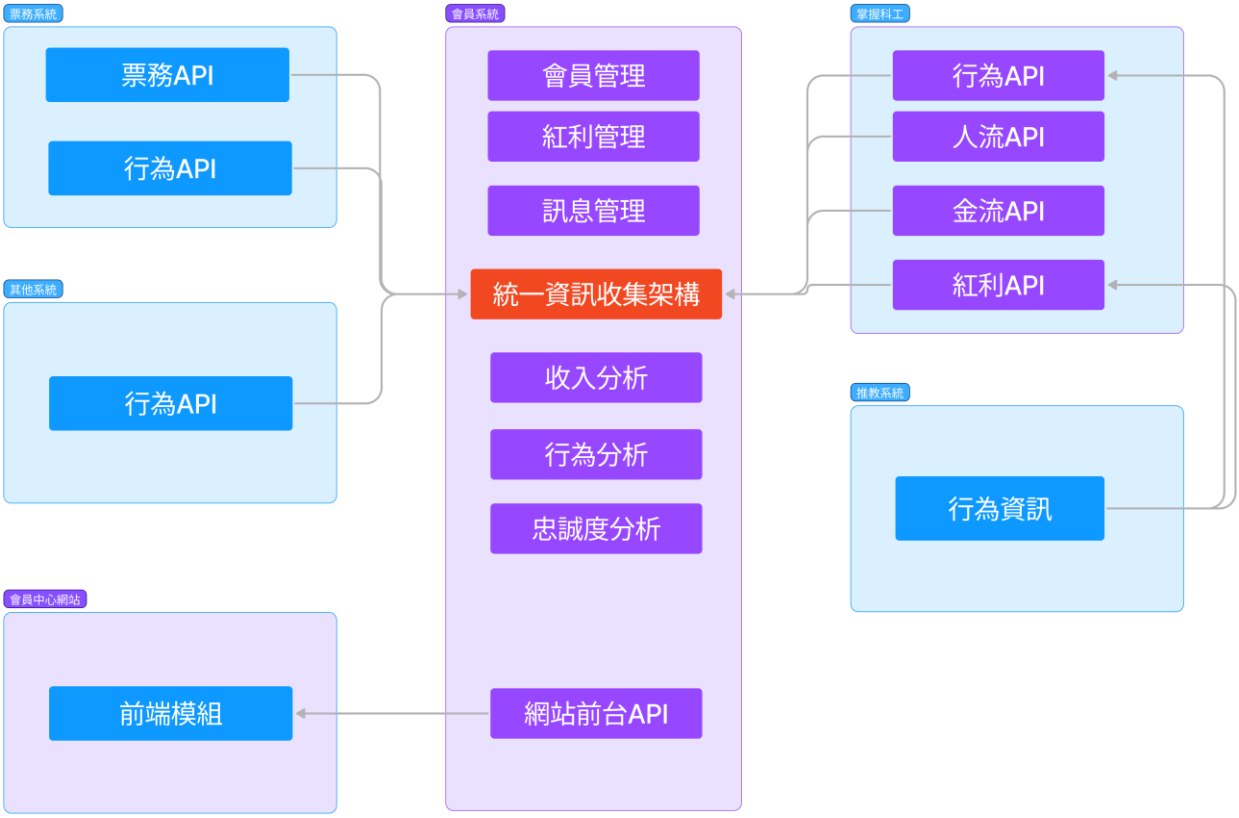
第貳章 系統架構分析

一、系統架構分析

(一)現有系統整體架構



(二)系統功能架構


票務系統
票務API
行為API
其他系統
行為API
會員中心網站
前端模組
會員系統
會員管理
紅利管理
訊息管理
統一資訊收集架構
收入分析
行為分析
忠誠度分析
網站前台API
掌握科工
行為API
人流API
金流API
紅利API
推教系統
行為資訊

(三)系統技術框架

1、原系統技術框架

系統	範圍	技術架構	版本
會員系統	前台	Next.js	11.1.2
	前台 API	.NET Core	5.0
	後台	.NET Framework	4.6.1
	後台 API	.NET Core	5.0
票務系統	後台	.NET Framework	4.7.2
團約系統	前台	.NET Framework	4.7.2

2、本案預計擴增程式範圍

系統	範圍	功能	子功能	原程式(API)主類別/編號	本案增修
會員系統	前台	會員中心	活動紀錄	Activities	擴增
			忘記密碼	ForgetPassword	
			友善連結	Links	
			載入中	Loading	
			登入	Login	
			虛擬會員卡	MemberCard	
			會員資料	Membership	擴增
			點數查詢	MyPoints	
			通知中心	Notification	擴增
			商品兌換	Redemptions	
			註冊	Register	擴增
			申辦年卡	RegisterCard	擴增
			修改密碼	ResetPwdLink	
	前台 API	會員管理	年卡購買	Member	
			會員登入	Login	
			第三方綁定	ThirdPartyAuth	擴增
			取得驗證碼	GetCaptcha	
	後台	會員管理	會員資料維護	MemberList	擴增
			紅利積點明細	PointInfo	擴增
			會員活動軌跡	Activity	擴增
			會員卡交易明細	CardReport	
		紅利商品	紅利商品維護	ProdData	
			紅利商品兌換	ProdTrans	

系統	範圍	功能	子功能	原程式(API)主類別/編號	本案增修
			紅利活動設定	PointEvent	擴增
		信件發送	信件撰寫		新增
			收件人管理		新增
			電子郵件發送		新增
			自動提醒功能		新增
		大數據分析	綜合分析		新增
			館內活動軌跡		新增
			參觀行為分析		新增
			收入來源分析		新增
			會員忠誠度分析		新增
			教育活動成效分析		新增
			會員級別標籤		新增
			報表產出		新增
		系統管理	訊息發布	Bulletin	擴增
			內容管理	Terms	
			友善連結管理	Links	
			系統特殊設定	CardConfig	擴增
			系統參數維護	CodeList	
			系統使用紀錄查詢	UserHistory	擴增
		權限管理	系統角色管理	Roles	
			使用者帳號維護	UserData	
	後台 API	會員管理	會員註冊	MEM_01	擴增
			會員資料更新	MEM_02	擴增
			紅利點數查詢	MEM_03	
			會員卡辦卡、續卡	MEM_04	擴增
			會員卡會員資料修改	MEM_05	
			會員卡綁卡	MEM_06	
			會員紅利兌換商品	MEM_07	
			紅利點數更新	MEM_08	擴增
			會員辦卡、續卡紀錄查詢	MEM_09	
			活動軌跡查詢	MEM_10	擴增
			會員查詢	MEM_11	
			活動軌跡新增	MEM_12	擴增
			單一登入串接	MEM_13	擴增
			會員登入	MEM_14	擴增

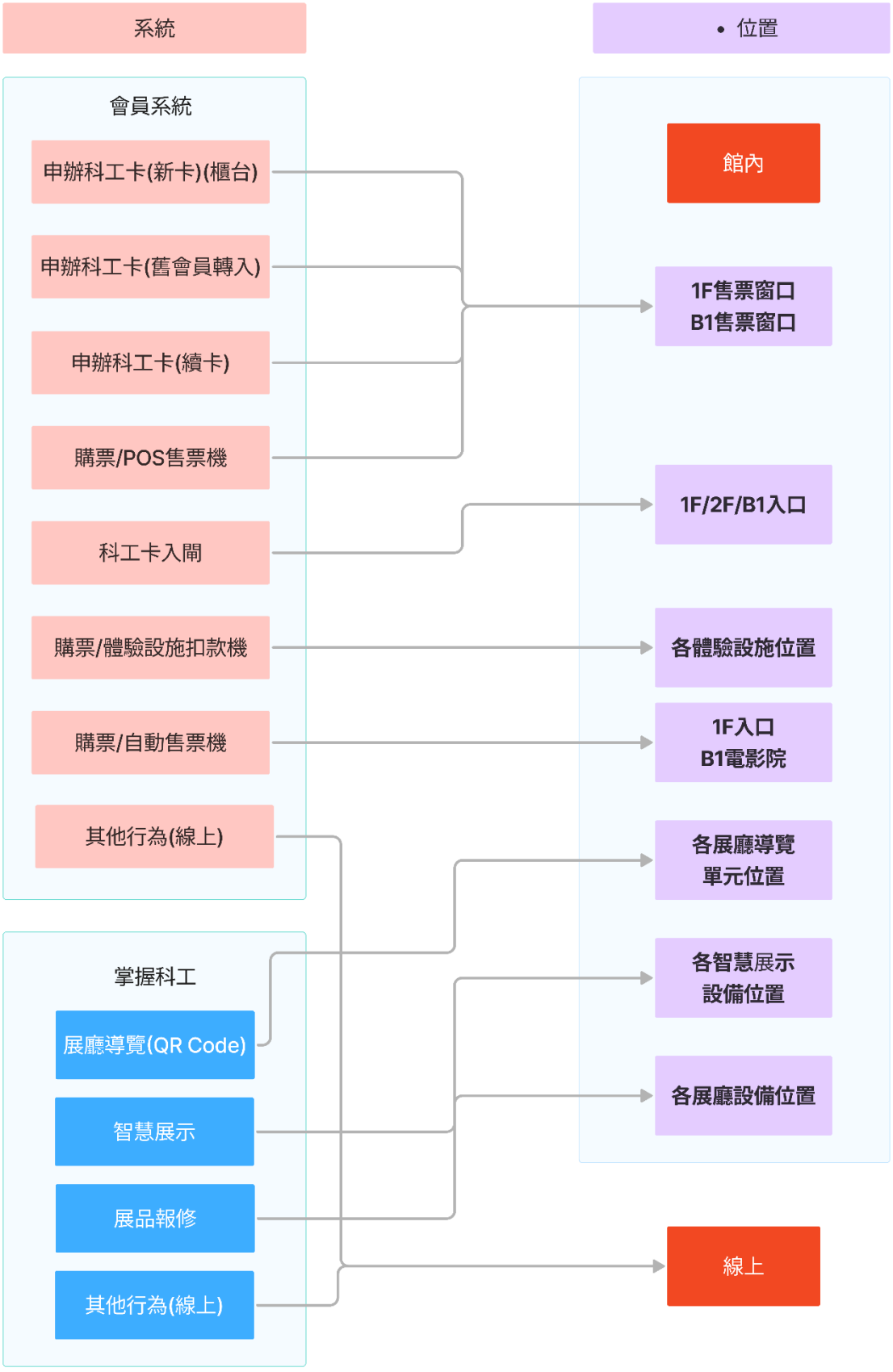
系統	範圍	功能	子功能	原程式(API)主類別/編號	本案增修
			密碼變更	MEM_15	
			紅利點數補登	MEM_16	擴增
			最新消息查詢	MEM_17	擴增
			紅利商品查詢	MEM_18	
			紅利商品兌換	MEM_19	擴增
			綁定第三方登入	MEM_20	擴增
			寄出重設密碼信	MEM_21	擴增
			重設密碼	MEM_22	
			友善連結查詢	MEM_23	
			使用條款查詢	MEM_24	
			會員卡查詢	MEM_25	

(四)行為地點資訊架構

1、行為地點鑑別架構

	行為	地點鑑別	位置
會員系統	申辦科工卡(新卡)(櫃台)	館內	1F 售票窗口 B1 售票窗口
	申辦科工卡(舊會員轉入)		
	申辦科工卡(續卡)		
	購票/POS 售票機		
	科工卡入閘		1F/2F/B1 入口
	購票/體驗設施扣款機		詳見「票務設備對照表」
	購票/自動售票機		1F 入口 B1 電影院
	申辦科工卡(新卡)(線上)	線上	
	科工卡續卡		
	紅利點數獲得(票券補登)		
	紅利點數獲得(掃描活動 QRCode)		
掌握科工	展廳導覽(QR Code)	館內	詳見「系統功能實體位置對照表」
	智慧展示		詳見「系統功能實體位置對照表」
	展品報修		各展廳設備
	紅利錢包	線上	
	線上購票		
	付費購買		
	展廳導覽(線上瀏覽)		
	開箱藏品		
	環境實況		
	意見回饋		
	版主推薦		
	尋位停車		

2、會員行為地點資訊架構



票務設備對照表

設備類型	設備代碼	設備名稱	樓層	展廳
體驗設施電子扣款機系統	E01	體驗設施電子扣款機 1 (6 樓太空廳)	6F	太空飛行探索館
體驗設施電子扣款機系統	E02	體驗設施電子扣款機 2 (4 樓智慧運輸)	4F	智慧駕車遊高屏
體驗設施電子扣款機系統	E04	體驗設施電子扣款機 4 (B1Fun 城市)	B1	兒童科學園區
體驗設施電子扣款機系統	E13	體驗設施電子扣款機 1 (2F 刻印)	2F	印象深刻
體驗設施電子扣款機系統	E14	體驗設施電子扣款機 4 (4F 長廊)	4F	電池小火車
體驗設施電子扣款機系統	E15	體驗式扣款機(B1Fun 城市 2)	B1	兒童科學園區
自動驗票系統	G01	自動驗票機_1F_東側入口	1F	東側入口
自動驗票系統	G02	自動驗票機_1F_西側入口	1F	西側入口
自動驗票系統	G03	自動驗票機_2F_東側入口	2F	東側入口
自動驗票系統	G04	自動驗票機_2F_西側入口	2F	西側入口
自動驗票系統	G05	自動驗票機_B1_劇院入口	B1	電影院
POS 系統	P01	售票窗口：P01 (1F-5)	1F	售票處
POS 系統	P02	售票窗口：P02(1F-6)	1F	售票處
POS 系統	P03	售票窗口：P03 (1F-8)	1F	售票處
POS 系統	P06	售票窗口：P06 (1F-備機)	1F	售票處
POS 系統	P04	售票窗口：P04 (B1-9)	B1	售票處
POS 系統	P05	售票窗口：P05 (B1-7)	B1	售票處
自動售票機系統	T01	自動售票機 1 (1F)	1F	入口
自動售票機系統	T02	自動售票機 2 (1F)	1F	入口
自動售票機系統	T03	自動售票機 3 (1F)	1F	入口
自動售票機系統	T04	自動售票機 4 (B1F)	B1	電影院
自動售票機系統	T05	自動售票機 5 (B1F)	B1	電影院

二、系統功能擴充

(一)註冊流程簡化

1、註冊欄位簡化

註冊必填欄位簡化為以下 6 項欄位：姓名、電子郵件（唯一值）、身分證字號（唯一值）、性別(男、女、其他)、出生年月、居住地區（縣市）等欄位。

2、電子郵件驗證

(1)「電子郵件」欄位資訊需加入驗證機制，以維持系統資訊完整性與一致性並避免重複、冒用。

(2)電子郵件完成驗證後需再次提示註冊已填寫之資訊以供確認；若有誤需提供再次編輯之功能。

3、申辦年卡配合調整

配合會員註冊之欄位簡化，「申辦年卡」時需先填寫完原必填欄位後(含國籍、聯絡電話、行動電話等)，始能繼續申辦流程。。

4、註冊流程優化

註冊流程依以下規範與步驟為原則優化：

(1)民眾填寫註冊資訊(如上述 6 項必填欄位)

(2)系統發送電子郵件確認信至民眾信箱

(3)民眾點選電子郵件之確認信連結；確認信連結驗證無誤後，系統內部標示註冊狀態為註冊成功。

(4)驗證無誤後，前台介面提示「電子郵件已確認，請確認您的下列註冊資訊是否正確」 (下接民眾已填寫之註冊資訊)。

(5)民眾點選「確認無誤」後，完成註冊，並導至登入頁面並提示以剛剛註冊所填寫的帳密登入。

(6)上述電子郵件填寫與驗證(第 2~3 步驟)可透過 Google 與 Facebook 等第三方登入方式整合，直接代入不需額外填寫與驗證或綁定。

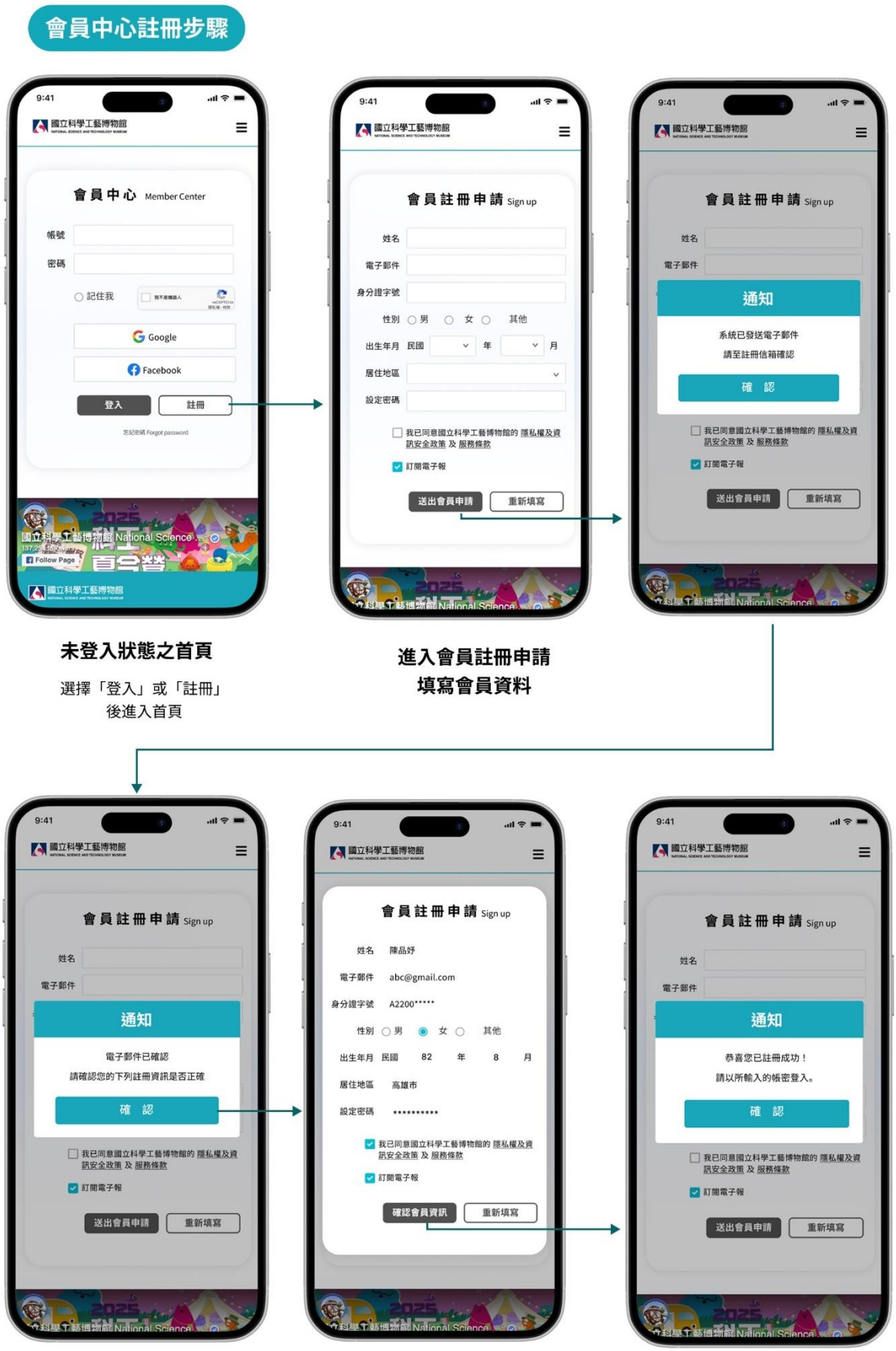
5、其他功能需求

(1)會員註冊功能需增加「個資宣告」資訊與檢核欄位（勾選同意後始能註冊）。

(2)系統以工作階段（Session）機制保留民眾註冊時填寫之個人資訊，避免於收不到電子郵件驗證信或他情況而反覆操作系統時，需重複填寫。

6、介面設計

(1)註冊流程優化



(2)中英文版註冊介面

會員中心註冊步驟
會員中心 Member Center
帳號 ID/Email
密碼 Password
記住我 Remember me
Google
Facebook
登入 Login
註冊 Register
會員註冊申請 Sign up
姓名 Name
電子郵件 Email
身分證字號 ID No.
性別 Sex
出生年月 Date of birth
居住地區 Address
設定密碼 Password
送出會員申請 Submit
重新填寫 Reset
通知 Notice
系統已發送電子郵件
請至註冊信箱確認
確認 Submit
電子郵件已確認
請確認您的下列註冊資訊是否正確
恭喜您已註冊成功！
請以所輸入的帳密登入
確認會員資訊
未登入狀態之首頁
選擇「登入」或「註冊」
後進入首頁
進入會員註冊申請
填寫會員資料

(3)註冊完成後針對「申辦年卡」等需求再填寫完整個資

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM

首頁｜資料設定｜申辦年卡

申辦年卡

國籍 ◉ 本國籍人士 ○ 外國籍人士 - 居留證

○ 外國籍人士 - 護照 Passport

聯絡電話

行動電話

送出年卡申請 重新填寫

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM

版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時 ｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM

首頁｜資料設定｜申辦年卡

申辦年卡

① 上傳照片 —— ② 信用卡付款

規格說明
1. 正面五官清晰照(自然不誇張)
2. 脫帽且不得佩戴有色眼鏡
3. 不能配戴大型髮飾或後製花邊、小圖
4. 不能無法辨識製卡人
5. 不能側臉照、不得使用合成照片

上傳照片參考範例：

購買須知
※ 本卡完成交易後即立刻開通年卡身分，且本卡一經開通後，恕不接受退卡。若有特殊退卡需求，請洽本館服務台辦理。
※ 年卡現不提供實體卡片，持卡人可利用下述方式於閘口查驗入館：
方式1：登入會員中心（https://member.nstm.gov.tw/Login）點選右上角虛擬會員卡
方式2：使用身分證背後條碼（居留證背面下方條碼）
方式3：綁訂電子票證卡片（如；悠遊卡、一卡通，如需綁定實體卡片， 請攜帶個人之電子票證至本館服務台辦理，同一時間內限綁定一張，如更換綁定之卡片，以最近一次綁定之卡片為主）
方式4：入口驗票機輸入身分證號

※ 年卡效期自繳費開通啟用日起算 365 天(含啟用當日)。
本人已詳閱各項注意事項及約定條款，並同意遵守科工館相關規定。

確認上傳 返回

(二)前台功能擴充

1、訊息功能擴充

(1)訊息功能(通知中心)增加圖文區塊功能，圖片應能自動擷取固定大小，設計風格以簡潔為主，以維持版本清爽。

(2)訊息功能(通知中心)增加短影音區塊，以單欄設計，資訊連結至本館 FB Reels 社群。

2、前台介面優化

(1)前台介面優化以「行動優先」(Mobile First)為原則，以資訊簡潔與設計簡化為方向。

(2)以統一 UI/UX 與識別系統、文字規範、色彩計畫等面向，重新設計與調整前台介面(含註冊、登入、通知中心、會員資料、活動紀錄、點數查詢、商品兌換等所有功能介面)。

3、介面設計

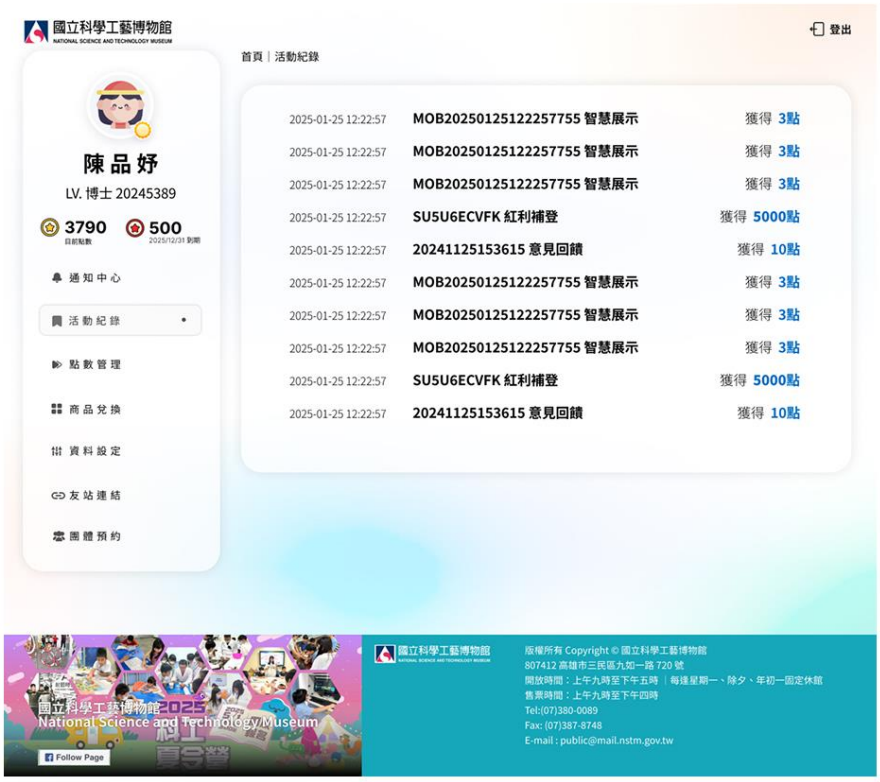
(1)通知中心

通知中心
國立科學工藝博物館
登出
首頁｜通知中心
最新消息
個人通知
陳品妤
LV. 博士 20245389
3790
500
通知中心
活動紀錄
點數管理
商品兌換
資料設定
友站連結
團體預約
於114年4月28日(週一)進行系統更新作業
於114年4月28日(週一)進行系統更新作業
於114年4月28日(週一)進行系統更新作業
希望×未來
Light up the Future
- 莫拉克解謎遊戲 -
科工夏令營
小小科學家從這裡出發！
科學躍動 高雄雄翔
2025.4.25-4.27
高雄市師生應援
免費參觀
國立科學工藝博物館2025
National Science and Technology Museum
Follow Page
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

國立科學工藝博物館
首頁｜通知中心
最新消息
個人通知
於114年4月28日(週一)進行系統更新作業
科學躍動 高雄雄翔
2025.4.25-4.27
高雄市師生應援
免費參觀
國立科學工藝博物館2025
National Science and Technology Museum
Follow Page
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

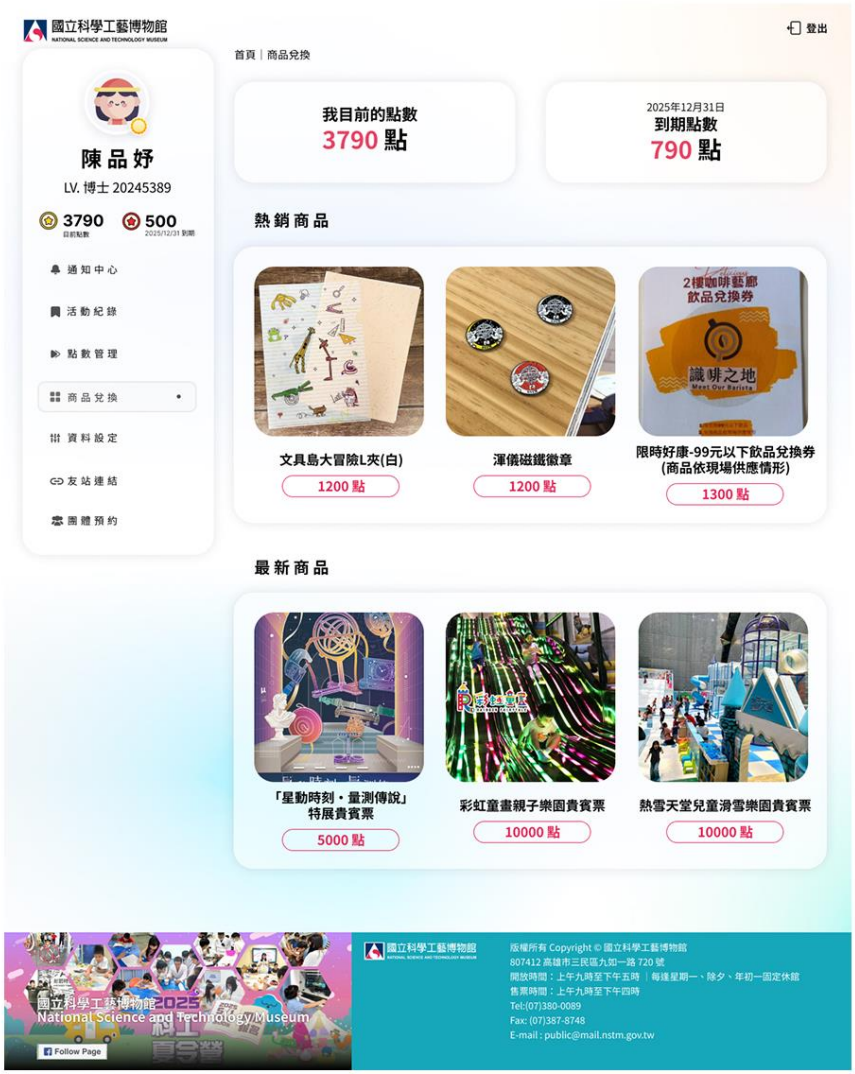
(2)活動紀錄

活動紀錄


國立科學工藝博物館
登出
首頁｜活動紀錄
陳品妤
LV. 博士 20245389
3790
500
通知中心
活動紀錄
點數管理
商品兌換
資料設定
友站連結
團體預約
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 SU5U6ECVFK 紅利補登 獲得 5000點
2025-01-25 12:22:57 20241125153615 意見回饋 獲得 10點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 SU5U6ECVFK 紅利補登 獲得 5000點
2025-01-25 12:22:57 20241125153615 意見回饋 獲得 10點
國立科學工藝博物館
National Science and Technology Museum
Follow Page
國立科學工藝博物館
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時 ｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

國立科學工藝博物館
首頁｜活動紀錄
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 MOB20250125122257755 智慧展示 獲得 3點
2025-01-25 12:22:57 SU5U6ECVFK 紅利補登 獲得 5000點
2025-01-25 12:22:57 20241125153615 意見回饋 獲得 10點
國立科學工藝博物館 National Science
Follow Page
國立科學工藝博物館
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時 ｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

(3)商品兌換


商品兌換
國立科學工藝博物館
登出
首頁｜商品兌換
陳品妤
LV. 博士 20245389
3790
500
通知中心
活動紀錄
點數管理
商品兌換
資料設定
友站連結
團體預約
我目前的點數
3790 點
2025年12月31日
到期點數
790 點
熱銷商品
文具島大冒險L夾(白)
1200 點
渾儀磁鐵徽章
1200 點
2樓咖啡藝廊
飲品兌換券
識啡之地
Meet Our Barista
限時好康-99元以下飲品兌換券
(商品依現場供應情形)
1300 點
最新商品
「星動時刻・量測傳說」
特展貴賓票
5000 點
彩虹童畫親子樂園貴賓票
10000 點
熱雪天堂兒童滑雪樂園貴賓票
10000 點
國立科學工藝博物館2025
National Science and Technology Museum
Follow Page
國立科學工藝博物館
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時 ｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

國立科學工藝博物館
首頁｜點數管理
我目前的點數
3790 點
2025/12/31 到期點數 790點
熱銷商品
文具島大冒險L夾(白)
1200 點
渾儀磁鐵徽章
1200 點
2樓咖啡藝廊
飲品兌換券
識啡之地
Meet Our Barista
限時好康-99元以下飲品兌換券
(商品依現場供應情形)
1300 點

Follow Page
國立科學工藝博物館
版權所有 Copyright © 國立科學工藝博物館
807412 高雄市三民區九如一路 720 號
開放時間：上午九時至下午五時 ｜每逢星期一、除夕、年初一固定休館
售票時間：上午九時至下午四時
Tel:(07)380-0089
Fax: (07)387-8748
E-mail : public@mail.nstm.gov.tw

(三)後台功能擴充

1、會員資訊管理功能擴充

(1)「查詢條件」欄位擴增為以下項目：

A、起迄日：查詢會員行為紀錄之起迄日；增加單選選項「註冊日」與「活動日」，以區分針對會員行為起迄日之狀態查詢。

B、會員身分：選項為多選，包含：有效年卡、無效年卡、未辦年卡。

C、五年未登入：以檢核項(Checkbox)選擇，勾選則列出五年未登入之帳號。

D、性別：選項為多選（Checkbox），選項包含：男、女及其他；預設為「全選」。

E、居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區「北、中、南、東、其他」分類 (同大數據分析)。

F、年齡區間(上下限)：預設為空值(不限制)。

G、證件編號：以精確搜尋(Exact search)進行編號查詢。

H、會員姓名：以模糊搜尋(Fuzzy search)進行姓名查詢。

I、電子郵件：以模糊搜尋(Fuzzy search)進行查詢。

J、團體會員：選項為多選，包含：是、否。

K、訂閱電子報：，選項為多選，包含：是、否。

L、紅利點數(上下限)：預設為空值(不限制)

M、「查詢條件」區分精簡模式與進階模式，以開闔功能進行切換。預設為「精簡模式」。

(2)「查詢條件」區分精簡模式與進階模式，以開闔功能進行切換。預設為「精簡模式」。

(3)查詢結果

A、查詢結果需包含以下欄位：會員編號、會員等級、會員姓名、現有點數、本年度到期點數、註冊日期、最後活動時間。

B、會員查詢結果中，點選各「欄位標題」可進行排序方式切換(包含正排版、反排版與預設排序)。

C、查詢結果之「分頁導覽」(上下頁)功能，增加可直接輸入「頁碼」以導至該頁之功能。

(4)其他功能需求

A、「會員編號」應以「時序」進行編號：新註冊會員之會員編號應大於較早註冊會員之編號。

B、後台編輯資訊時，若遇輸入特殊字元而系統阻擋時，應有提示文字說明與警示。

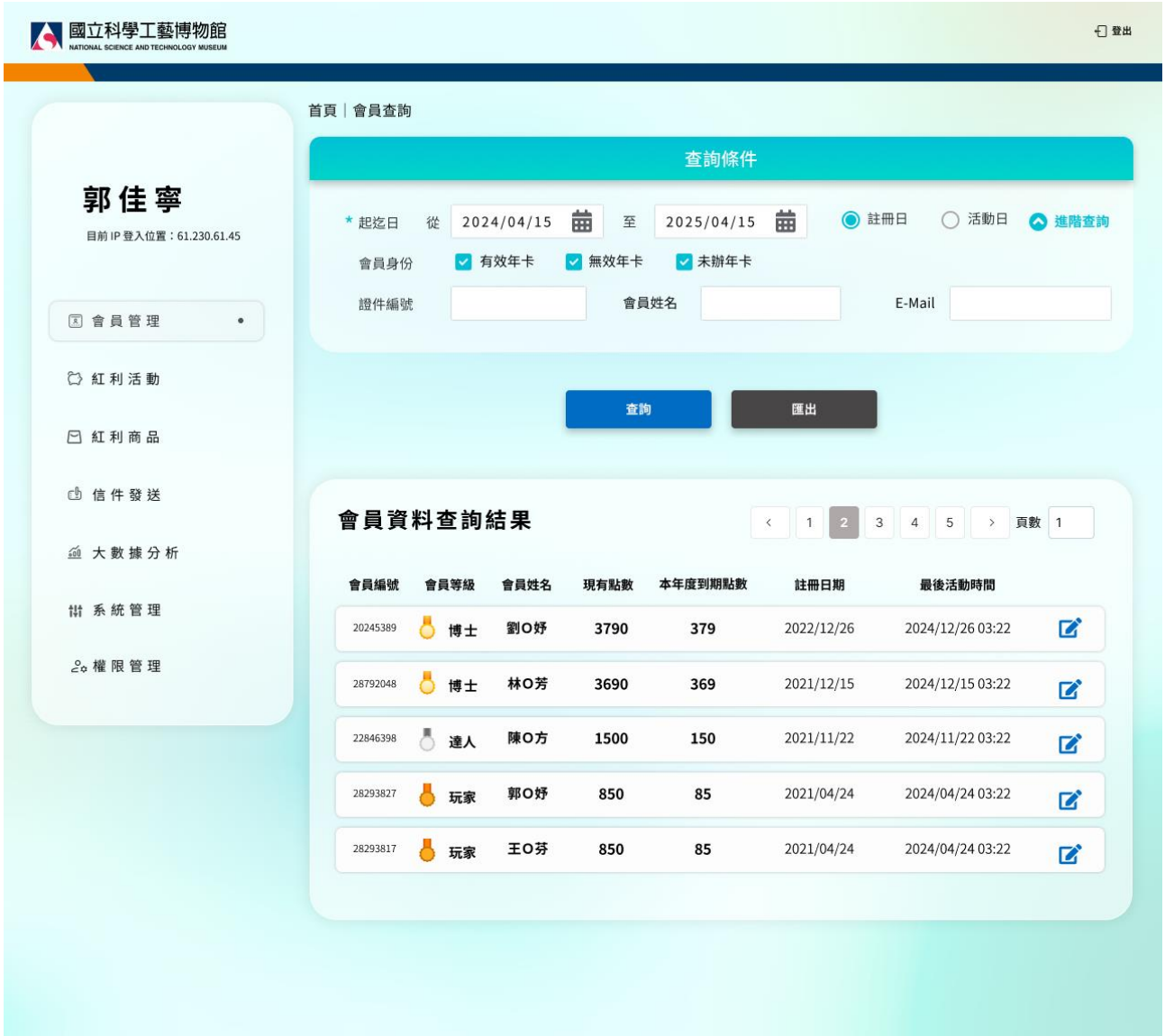
C、「到期點數」計算規則為當年度所累積點數，點數到期日為當年度 12 月 31 日(含)前使用完畢，若未使用將會自動歸零重新計算，恕無法展延使用。

D、會員最後登入時間之計算，應包含整合於 SSO 範圍內系統，所有會員之登入行為(現行會員系統無依此範圍記錄)。

(5)介面設計

A、會員查詢

(A)精簡模式



(B)進階模式(展開查詢條件)

B、會員明細資料

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜會員查詢
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
紅利商品
信件發送
大數據分析
系統管理
權限管理
關於 20245389 會員資料
劉 O 妤
LV. 博士 00245389
3790
目前點數
500
2025/12/31 到期
發信提醒會員點數到期
手動發送
會員活動行為分析
消費
紅利
體驗
瀏覽
教育
服務
智慧分析 AI
該會員在消費與紅利累積方面較活躍，顯示她主要關注購物與回饋，但對教育、服務與館內探索的參與度較低。
建議透過專屬優惠與個人化推薦，提高她對展覽、館內活動及會員服務的興趣，以增強該會員的忠誠度與互動……
詳細活動資訊
註冊國立科學工藝博物館新會員 免費獲得1000點
有效期限：2025/03/20至2025/04/18
1000點
紅利點數轉移
轉移日期：2025/01/03 轉移至：00245389
-250點
接收到來自 00245389 紅利點數轉移
有效期限：2025/03/20至2025/04/18
2410點
會員基本資料
姓名 劉O妤
地區 高雄市
上次登入 2025/02/03 13:25:35
性別 女
會員編號 20245389
通訊地址 807044 高雄市三民區＊＊＊＊＊＊
Email 帳號 the＊＊＊＊＊@gmail.com
身分證字號 F240＊＊＊＊＊＊
綁定 Google 否
手機號碼 0919＊＊＊007
出生年月日 2000/11/22
綁定 FB 否
此動作需要輸入您的密碼，系統會記錄您登入時間與位置
查看詳細資訊

2、信件發送功能

(1)功能說明

A、以所見即所得編輯器，進行發送內容之簡易編輯。

B、編輯內容後，以同「會員資訊管理」之查詢條件篩選出欲發送之會員名單。

C、發送電子郵件給以上步驟指定之會員

(2)介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM

登出

首頁｜信件發送

郭佳寧

目前 IP 登入位置：61.230.61.45

- 會員管理
- 紅利活動
- 紅利商品
- 信件發送
- 大數據分析
- 系統管理
- 權限管理

狀態：尚未發送（草稿）

Normal text

館慶日特別活動｜入館即享 500 點回饋！

為慶祝國立科學工藝博物館館慶日
特別推出限時回饋活動！
活動地點：國立科學工藝博物館
活動內容：當日入館即贈 500 點回饋點數，可用

於館內指定消費！快來共襄盛舉，一起探索科學的樂趣，領取專屬回饋吧！

- 點數使用規則請見官網或館內公告
- 本活動最終解釋權歸國立科學工藝博物館所有

儲存　捨棄

查詢條件

* 註冊日　從 2024/04/15　至 2025/04/15

居住地　居住地分類

年齡區間　從 35歲　至 40歲

會員帳號　　會員姓名

性別　男　女　其他　　E-Mail

查詢

會員資料查詢結果

‹ 1 2 3 4 5 › 頁數 1

會員編號	會員等級	會員姓名	現有點數	本年度到期點數	註冊日期	最後活動時間	
20245389	博士	劉O妤	3790	379	2022/12/26	2024/12/26 03:22	
28792048	博士	林O芳	3690	369	2021/12/15	2024/12/15 03:22	
22846398	達人	陳O方	1500	150	2021/11/22	2024/11/22 03:22	
28293827	玩家	郭O妤	850	85	2021/04/24	2024/04/24 03:22	
28293817	玩家	王O芬	850	85	2021/04/24	2024/04/24 03:22	

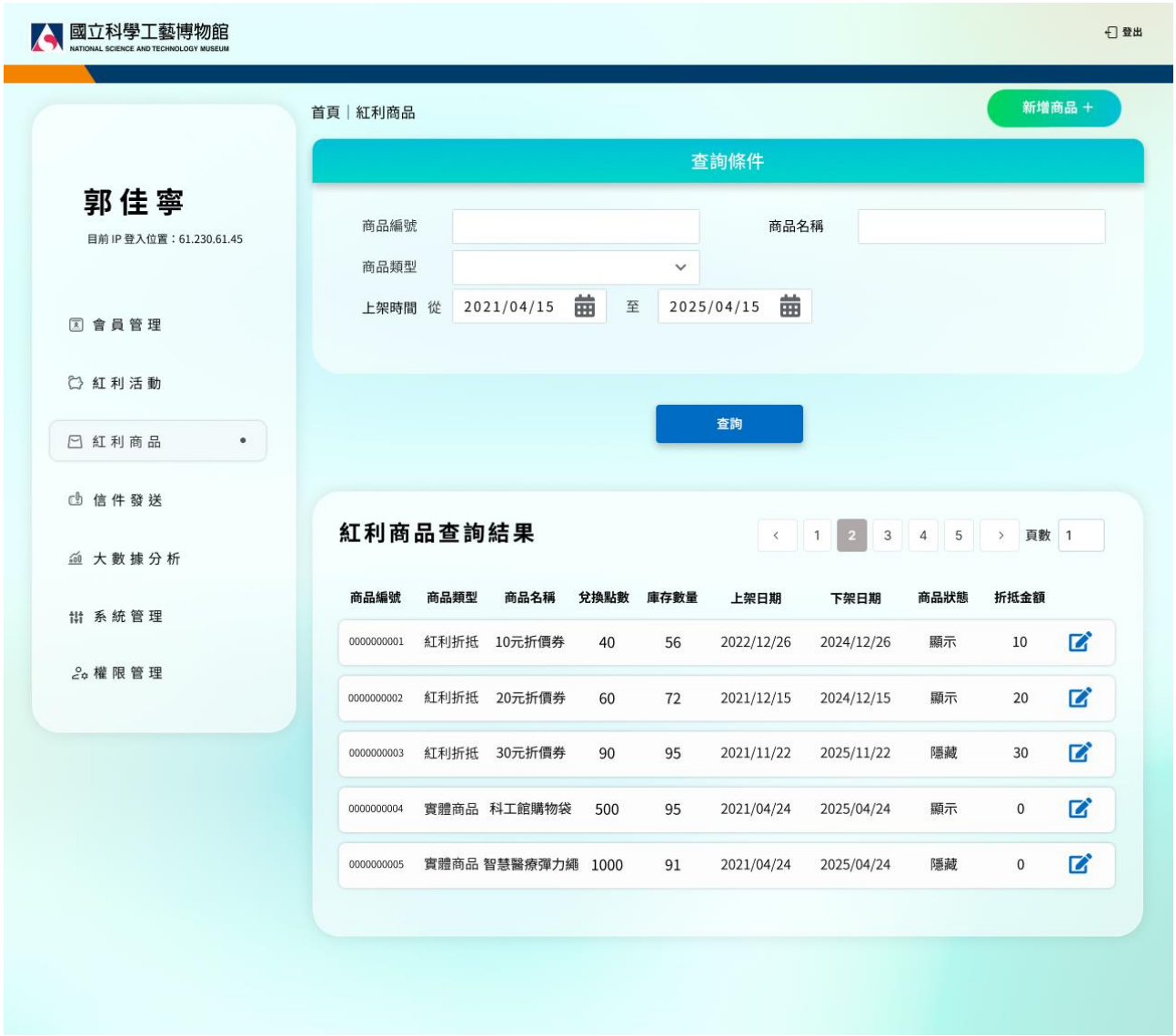
發送

3、操作介面優化

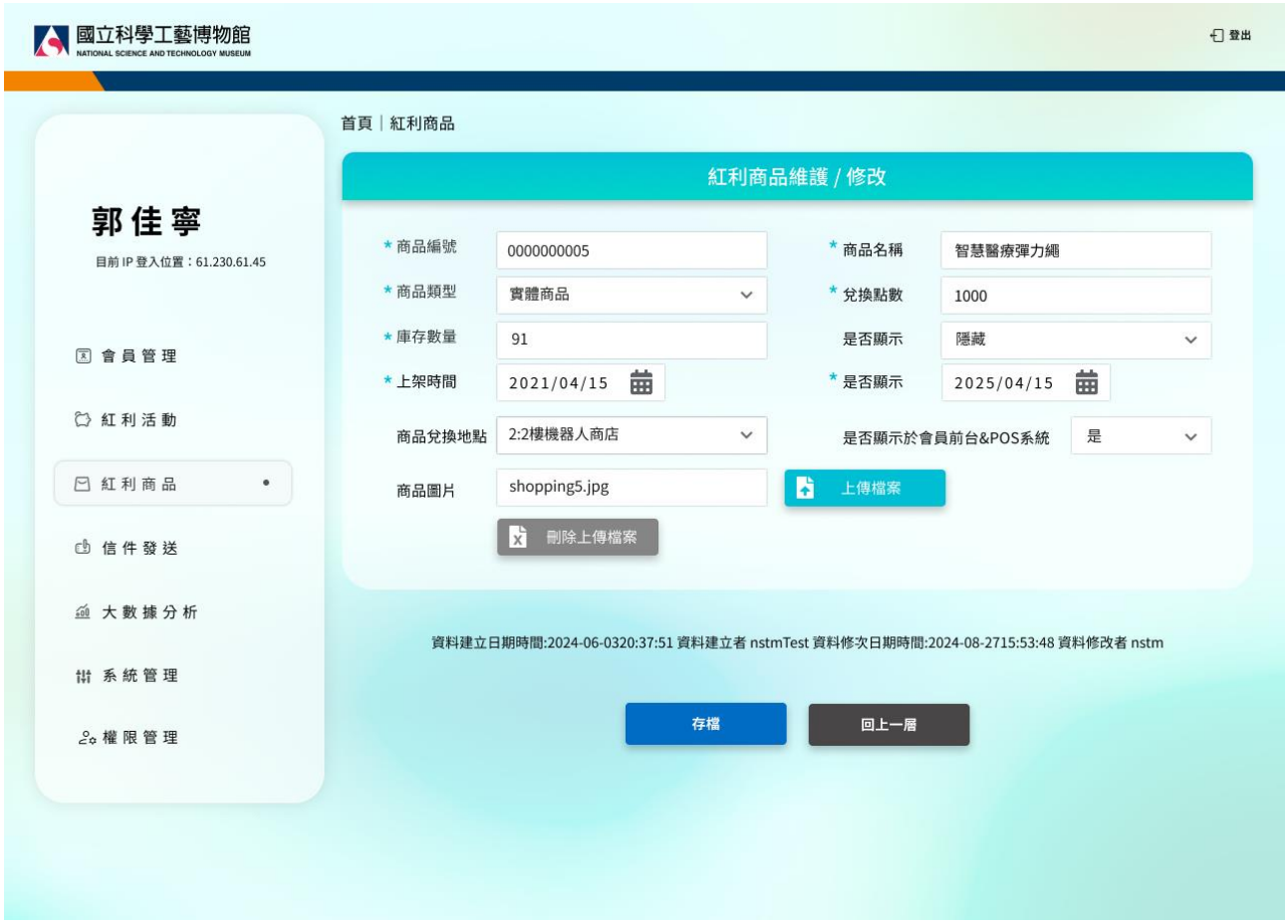
以統一風格與 UI/UX 優化後台系統功能介面，包括後台新增功能與原有會員管理、紅利商品、系統管理、權限管理等功能。

4、介面設計

(1)紅利商品查詢



(2)紅利商品編輯


國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜紅利商品
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
紅利商品
信件發送
大數據分析
系統管理
權限管理
紅利商品維護 / 修改
* 商品編號
0000000005
* 商品名稱
智慧醫療彈力繩
* 商品類型
實體商品
* 兌換點數
1000
* 庫存數量
91
是否顯示
隱藏
* 上架時間
2021/04/15
* 是否顯示
2025/04/15
商品兌換地點
2:2樓機器人商店
是否顯示於會員前台&POS系統
是
商品圖片
shopping5.jpg
上傳檔案
刪除上傳檔案
資料建立日期時間:2024-06-0320:37:51 資料建立者 nstmTest 資料修次日期時間:2024-08-2715:53:48 資料修改者 nstm
存檔
回上一層

（四）自動提醒功能

1、個資更新提醒

(1)系統以電子郵件自動提醒一年未登入或未更新個資之會員。

(2)經提醒一次後，若一週後尚未登入或更新個資則再提醒一次。

2、帳號刪除提醒

(1)若會員五年未登入，系統以電子郵件於1個月前，提醒若五年未登入將刪除帳號。

(2)產出會員五年未登入清冊(電子檔)以利後續進行資安稽核作業；帳號刪除作業應以資料隱碼方式處理。

3、點數到期提醒

(1)系統以電子郵件自動提醒會員點數即將到期。

(2)配合「點數到期」時間，提早1個月提醒。

(3)若超過到期日仍未使用，點數自動歸零。

（五）單一簽入驗證

1、功能需求

(1)依 OAuth 2.0 (OpenID Connect) 以及已制定之程式流程架構，建置單一簽入功能。

(2)單一簽入使用系統之用戶編號 (client_id) 與用戶金鑰 (client_secret) 由後台管理系統設定並取得。

(3)提供 C# 語言範例程式，供館方應用系統加入單一簽入機制參考與使用。

(4)可透過單一簽入由會員中心系統登入本館其他系統；若已於會員系統登入，於本館其他系統可自動登入，不需重複輸入帳密。

(5)支援第三方帳號登入，民眾透過 Google 或 FB 等帳號即可以登入，並與簡化後會員註冊與登入流程整合，登入後再補充資料即可。

2、技術規格

(1)建置遵循規範 OAuth 2.0 與 OpenID Connect。

(2)實作機制依循《Google Identify OpenID Connect》之設計規範。

(3)依「OAuth 2.0 與 OpenID Connect」規範建置之 SSO 功能：

三、大數據與分眾分析

於後台建置「大數據與分眾分析」功能，包括綜合分析、館內活動軌跡、參觀行為分析、收入來源分析、會員忠誠度分析、教育活動成效分析、會員級別標籤、各式報表輸出、訪客模式分析等功能與面向。

(一)綜合分析

建置大數據分析之「綜合分析」功能，籍由後台介面，可綜合統計與分析會員之行為次數、紅利點數、消費金額等面向。

1、分析條件

系統可依下列條件進行分析：

(1)分析範圍：多選（Checkbox），選項包括：會員系統、掌握科工、推教系統、團約系統；預設為「全選」。

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類：

A、北部地區：臺北市、新北市、基隆市、新竹市、桃園市、新竹縣、宜蘭縣

B、中部地區：臺中市、苗栗縣、彰化縣、南投縣、雲林縣

C、南部地區：高雄市、臺南市、嘉義市、嘉義縣、屏東縣、澎湖縣

D、東部地區：花蓮縣、臺東縣

E、其他：包括金門縣、連江縣及境外地區。

【註】介面支援「收闔」設計，提供「全選/反選」區域操作功能。

(5)年齡區間(上下限)：預設為空值(不限制)

(6)紅利點數(上下限)：預設為空值(不限制)

(7)消費金額(上下限)：預設為空值(不限制)

(8)紅利給點：多選形式，選項包括：智慧展示、紅利活動、展品報修、意見回饋。

(9)會員編號或姓名：關鍵字查詢。

2、圖表輸出

分析結果之「圖表輸出」可依下列條件選擇輸出資料與格式：

(1)Y 軸資料：單選，選項為：行為次數、紅利點數、消費金額

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳、年齡分布、居住地、會員等級

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

(4)承上之「X 軸資料」，「年齡分布」分析之年齡分布區間如下：

序號	區間
1	10 歲以上未滿 13 歲
2	13 歲以上未滿 16 歲
3	16 歲以上未滿 19 歲
4	19 歲以上未滿 25 歲
5	25 歲以上未滿 35 歲
6	35 歲以上未滿 45 歲
7	45 歲以上未滿 55 歲
8	55 歲以上未滿 65 歲
9	65 歲以上

3、資料來源

(1)會員系統會員活動軌跡資料

(2)會員系統紅利積點軌跡資料

(3)掌握科工行為紀錄 API

4、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜綜合分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
分析範圍 會員系統 掌握科工 推教系統 團約系統
* 起迄日 從 2024/04/15 至 2025/04/15
性別 男 女 其他
居住地 居住地分類
年齡區間 從 35歲 至 40歲
紅利點數 0 點 至 10000 點
消費金額 從 0 元 至 10000 元
紅利給點 智慧展示 紅利活動 展品報修 意見回饋
會員編號或姓名
圖表輸出
Y軸資料 行為次數 紅利點數 消費金額
X軸資料 年度 月份 季度 日期 樓層 展廳 年齡分布 居住地 會員等級
圖表類型 長條圖 圓餅圖 折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）
科工會員消費行為分析(月份)
40k
30k
20k
10k
0
17500
18000
20000
15000
6000
6000
16000
25000
24000
10000
20000
30000
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
月份

(二)館內活動軌跡

系統大數據分析應具備「館內活動軌跡」分析功能，分析與輸出需求說明如下。

1、分析條件

(1)起迄日：查詢會員行為紀錄之起迄日。

(2)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(3)館內位置：選項多選，涵蓋館內可分析位置，預設為「全選」，並依樓層分類：

A、本館 B3：臺灣農業的故事

B、本館 B1：兒童科學園區、氣候變遷、開放式典藏庫、電影院、售票處

C、本館 1F：售票處、入口

D、本館 2F：動力與機械、烹調的科學、電信@臺灣、印象深刻、入口

E、本館 4F：交通夢想、衣技織長、健康探索廳、科學開門、科學桂冠、技職展區、電池小火車、地震體驗屋、智慧駕車遊高屏

F、本館 6F：希望·未來莫拉克風災紀念廳、太空飛行探索廳、臺灣工業史蹟廳、4D 太空飛行、月球漫步

【註】介面支援「收闔」設計，提供「全選/反選」樓層操作功能。

(4)年齡區間(上下限)：預設為空值(不限制)；年齡區間設定同「綜合分析」。

2、圖表輸出

(1)Y 軸資料：多選，選項為：行為次數、停留時間(分)、紅利點數

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

3、館內位置命名

館內「實體位置」資訊，應統一以下「展廳」名稱記錄與分析：

樓層	展廳	智慧展示	展廳導覽	展品報修	會員系統
本館 B3	臺灣農業的故事	V	V	V	
本館 B1	兒童科學園區(奇幻國/Fun 城市/夢想號)		V	V	V
	氣候變遷		V	V	
	開放式典藏庫		V		
	電影院				V
	售票處				V
本館1F	售票處				V
	入口				V
	東側入口				V
	西側入口				V
本館2F	動力與機械	V	V	V	
	烹調的科學	V	V	V	
	電信@臺灣		V	V	
	印象深刻				V
	東側入口				V
	西側入口				V
本館4F	交通夢想		V	V	
	衣技織長	V	V	V	
	健康探索廳	V	V	V	
	科學開門		V	V	
	科學桂冠		V	V	
	技職展區			V	
	電池小火車				V
	地震體驗屋				V
	智慧駕車遊高屏				V
本館6F	希望·未來莫拉克風災		V	V	

樓層	展廳	智慧展示	展廳導覽	展品報修	會員系統
	紀念廳				
	太空飛行探索廳		V	V	
	臺灣工業史蹟廳		V	V	
	4D 太空飛行				V
	月球漫步				V

4、實體位置與設備代碼對應

會員系統「會員活動軌跡」之實體位置應以下表之「設備代碼」與「展廳」資訊代入並進行分析。

設備類型	設備代碼	設備名稱	樓層	展廳
體驗設施電子扣款機系統	E01	體驗設施電子扣款機 1 (6 樓太空廳)	6F	太空飛行探索館
體驗設施電子扣款機系統	E02	體驗設施電子扣款機 2 (4 樓智慧運輸)	4F	智慧駕車遊高屏
體驗設施電子扣款機系統	E04	體驗設施電子扣款機 4 (B1Fun 城市)	B1	兒童科學園區
體驗設施電子扣款機系統	E13	體驗設施電子扣款機 1 (2F 刻印)	2F	印象深刻
體驗設施電子扣款機系統	E14	體驗設施電子扣款機 4 (4F 長廊)	4F	電池小火車
體驗設施電子扣款機系統	E15	體驗式扣款機(B1Fun 城市 2)	B1	兒童科學園區
自動驗票系統	G01	自動驗票機_1F_東側入口	1F	東側入口
自動驗票系統	G02	自動驗票機_1F_西側入口	1F	西側入口
自動驗票系統	G03	自動驗票機_2F_東側入口	2F	東側入口
自動驗票系統	G04	自動驗票機_2F_西側入口	2F	西側入口
自動驗票系統	G05	自動驗票機_B1_劇院入口	B1	電影院
POS 系統	P01	售票窗口：P01 (1F-5)	1F	售票處
POS 系統	P02	售票窗口：P02(1F-6)	1F	售票處
POS 系統	P03	售票窗口：P03 (1F-8)	1F	售票處
POS 系統	P06	售票窗口：P06 (1F-備機)	1F	售票處
POS 系統	P04	售票窗口：P04 (B1-9)	B1	售票處
POS 系統	P05	售票窗口：P05 (B1-7)	B1	售票處
自動售票機系統	T01	自動售票機 1 (1F)	1F	入口
自動售票機系統	T02	自動售票機 2 (1F)	1F	入口
自動售票機系統	T03	自動售票機 3 (1F)	1F	入口

設備類型	設備代碼	設備名稱	樓層	展廳
自動售票機系統	T04	自動售票機 4 (B1F)	B1	電影院
自動售票機系統	T05	自動售票機 5 (B1F)	B1	電影院

5、資料來源

(1)會員系統會員活動軌跡資料

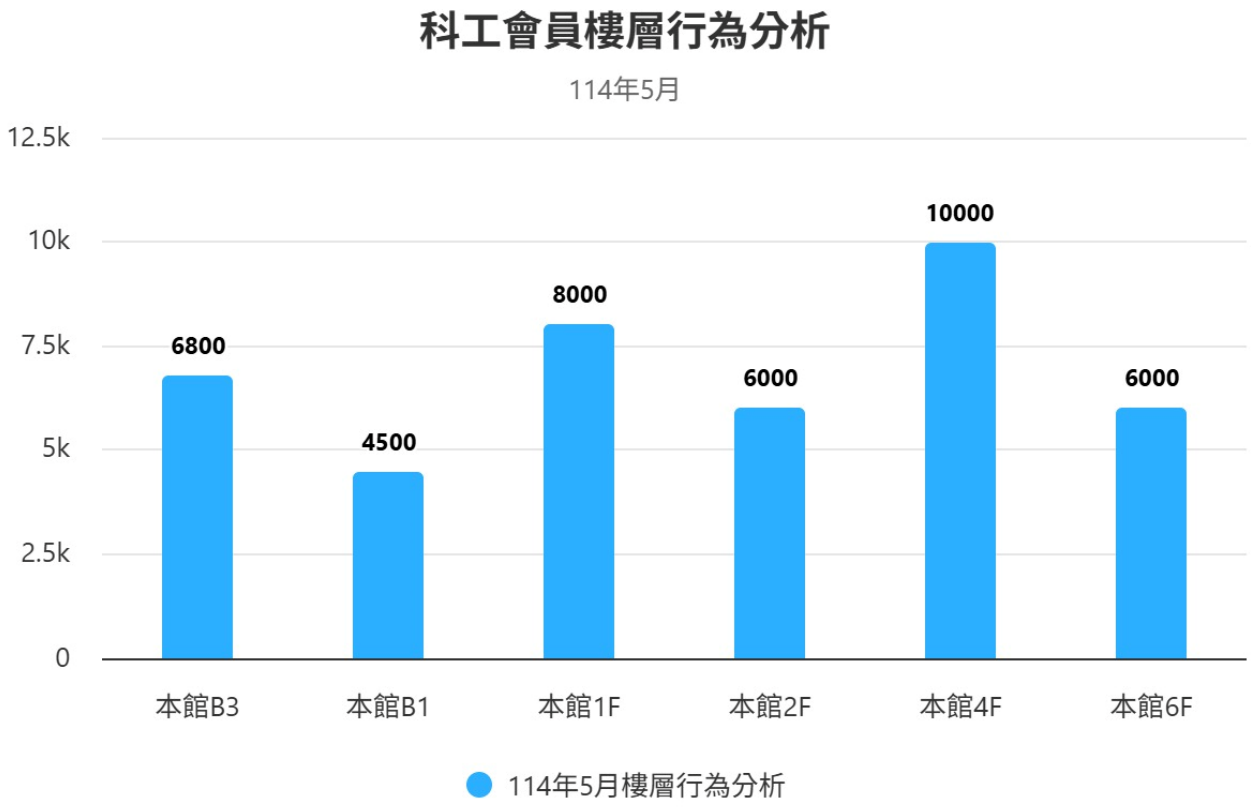
(2)掌握科工行為紀錄 API

(3)其他具實體位置資料來源

6、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜綜合分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
起迄日 從 2024/04/15 至 2025/04/15
性別 男 女 其他
館內位置
樓層分類
本館B3 臺灣農業的故事
本館B1 兒童科學園區 氣候變遷 開放式典藏庫 電影院
本館2F 動力與機械 烹調的科學 電信@臺灣 印象深刻
本館4F 交通夢想 衣技織長 健康探索廳 科學開門 科學桂冠 技職新視界 電池小火車 地震體驗屋 智慧駕車遊高屏
本館6F 希望・未來莫拉克風災紀念廳 太空飛行探索廳 台灣工業史蹟廳 4D太空飛行 月球漫步
年齡區間 從 35歲 至 40歲
圖表輸出
Y軸資料 行為次數 停留時間(分) 紅利點數
X軸資料 年度 月份 季度 日期 樓層 展廳
圖表類型 長條圖 圓餅圖 折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

7、圖表分析


科工會員樓層行為分析
114年5月
12.5k
10k
7.5k
5k
2.5k
0
6800
4500
8000
6000
10000
6000
本館B3
本館B1
本館1F
本館2F
本館4F
本館6F
114年5月樓層行為分析

(三)參觀行為分析

1、觀眾入館頻率

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

B、資料範圍：全館、樓層(下拉式選單選擇樓層、展廳(下拉式選單選擇展廳)。

(2)圖表輸出

A、Y 軸資料：單選，選項為：行為次數

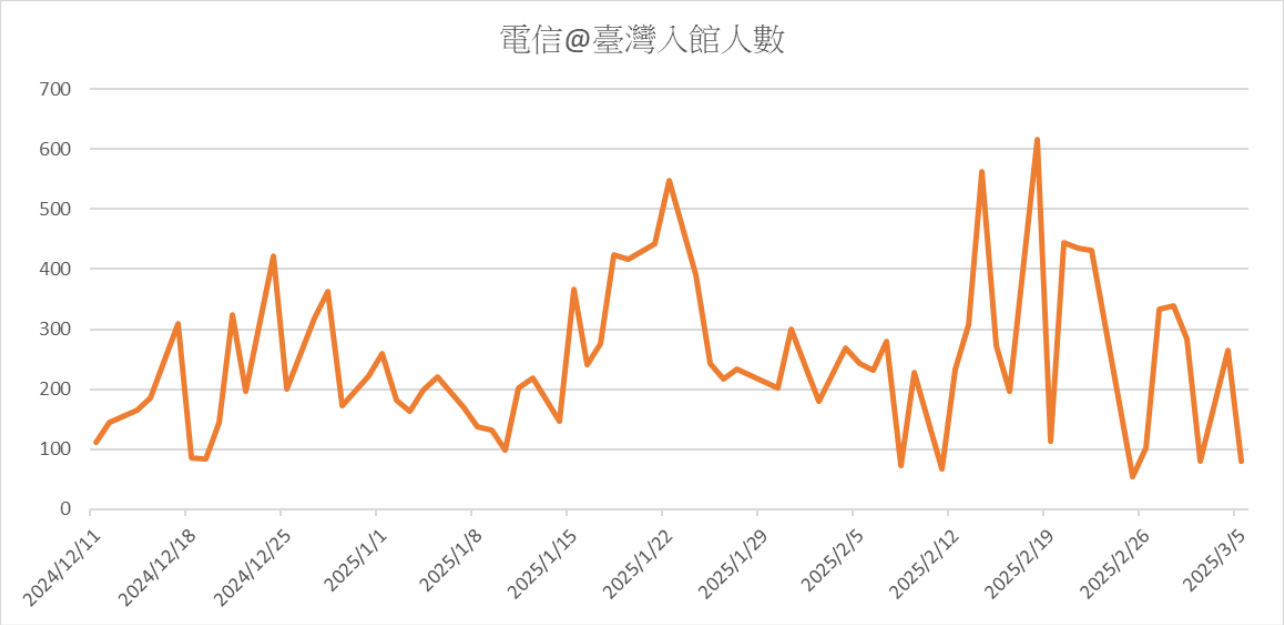
B、X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

(3)資料來源：由介接容留系統 API 取得資訊。

(4)介面設計

(5)圖表分析



2、觀眾入館再訪率

(1)分析條件

A、起迄日：觀眾入館行為之起迄日。

(2)圖表輸出

A、Y 軸資料：單選，選項為：再訪率(%)

B、X 軸資料：單選，選項為：年度、季度、月份

C、圖表類型：單選，選項為：長條圖、折線圖

(3)定義再訪率與計算方式

再訪率 (%) = 再訪觀眾不重複人次 ÷ 入館觀眾不重複人次

A、再訪觀眾人次：同一人入館 2 次以上即算「再訪者」，同日多次入館僅計 1 次。

B、入館觀眾人次：所有入館觀眾不重複人次。

C、計算範圍涵蓋所有館內相關活動之入館記錄。

(4)資料來源：會員系統行為軌跡。

3、觀眾入館時段

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

(2)圖表輸出

A、Y 軸資料：單選，選項為：行為次數

B、X 軸資料：單選，選項為：小時

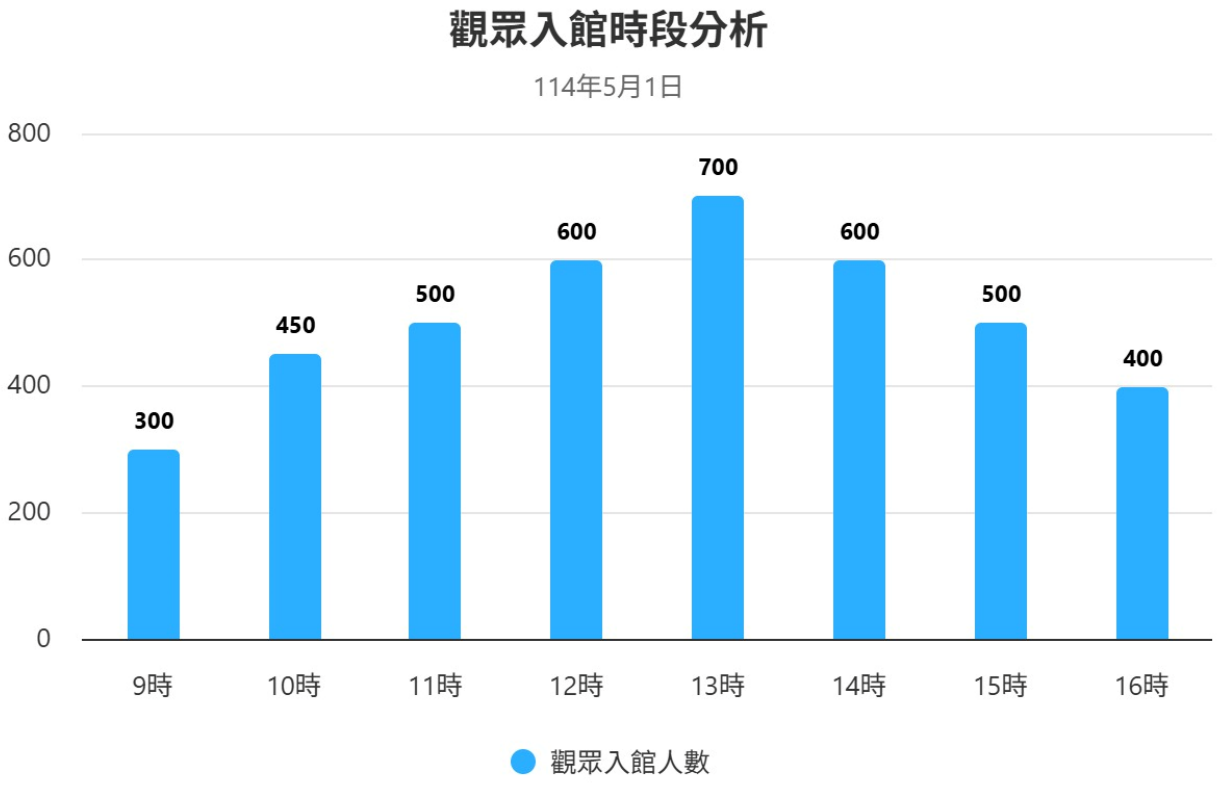
C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

(3)資料來源：由介接容留系統 API 取得資訊。

(4)介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁 | 大數據分析 | 參觀行為分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
參觀行為分析
觀眾入館頻率
觀眾入館再訪率
觀眾入館時段
觀眾停留時間
起迄日
從
2024/04/15
至
2025/04/15
圖表輸出
Y軸資料
行為次數
X軸資料
小時
圖表類型
長條圖
圓餅圖
折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

(5)圖表分析


觀眾入館時段分析
114年5月1日
800
600
400
200
0
300
450
500
600
700
600
500
400
9時
10時
11時
12時
13時
14時
15時
16時
觀眾入館人數

4、觀眾停留時間

(1)分析條件

A、起迄日：觀眾入館行為紀錄之起迄日。

B、資料範圍：全館、樓層選擇、展廳選擇。

(2)圖表輸出

A、Y 軸資料：單選，選項為：停留時間(分)

B、X 軸資料：單選，選項為：年度、季度、月份、日期、樓層、展廳

C、圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

D、資料分析

(A)以連續性行為分析觀眾停留時間

(B)可假設單次行為之「停留時間」。例如「紅利活動」可為 30 分鐘或 1 小時，亦或可於「紅利活動管理」功能，進行「活動時長」之設定，代入分析機制，以利後續分析。

(C)平均停留時間：總停留時間 ÷ 觀眾人數

藉由「容留系統」資訊，我們亦可透過以利特爾法則（Little's law），推算館內觀眾的平均停留時間：

$$\text{平均停留時間} = \frac{\sum \text{當前館內人數}}{\sum \text{每分鐘入館人數}} = \frac{\sum_{t=1}^{T} N_{\text{館內}}(t)}{\sum_{t=1}^{T} N_{\text{入館}}(t)}$$

其中：

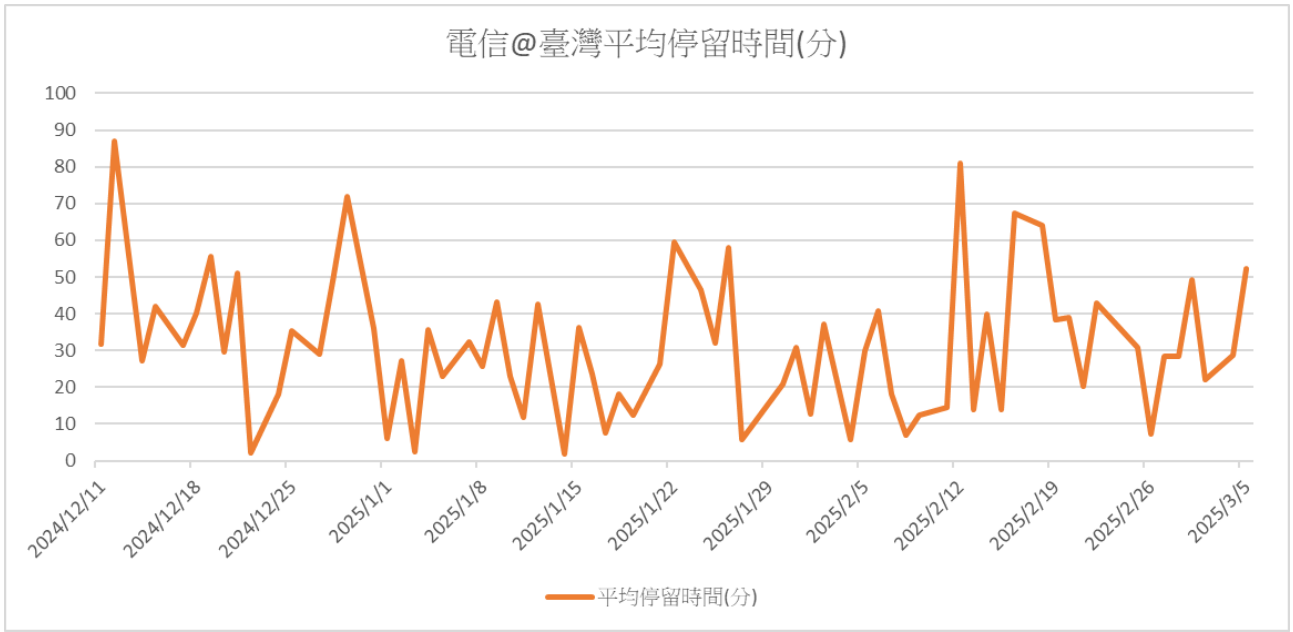
- $N_{\text{館內}}(t)$ = 時間 t 的館內人數
- $N_{\text{入館}}(t)$ = 時間 t 的入館人數
- T = 觀察的時間長度（分鐘）

(3)資料來源：由介接容留系統 API 取得資訊。

(4)介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜參觀行為分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
參觀行為分析
觀眾入館頻率
觀眾入館再訪率
觀眾入館時段
觀眾停留時間
起迄日
從
2024/04/15
至
2025/04/15
資料範圍
全館
本館2F
動力機械廳
圖表輸出
Y軸資料
停留時間(分)
X軸資料
年度
季度
月份
日期
樓層
展廳
圖表類型
長條圖
圓餅圖
折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

(5)圖表分析


電信@臺灣平均停留時間(分)
100
90
80
70
60
50
40
30
20
10
0
2024/12/11
2024/12/18
2024/12/25
2025/1/1
2025/1/8
2025/1/15
2025/1/22
2025/1/29
2025/2/5
2025/2/12
2025/2/19
2025/2/26
2025/3/5
平均停留時間(分)

（四）收入來源分析

1、分析條件

(1)收入來源分析：多選，包括：售票收入、商品收入、活動收入

(2)資料範圍：多選，包括：實體購票收入、線上購票收入（掌握科工）、商品收入（掌握科工）、科教活動

(3)起迄日：查詢會員行為紀錄之起迄日。

(4)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(5)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(6)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：營收金額

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、票種

(3)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

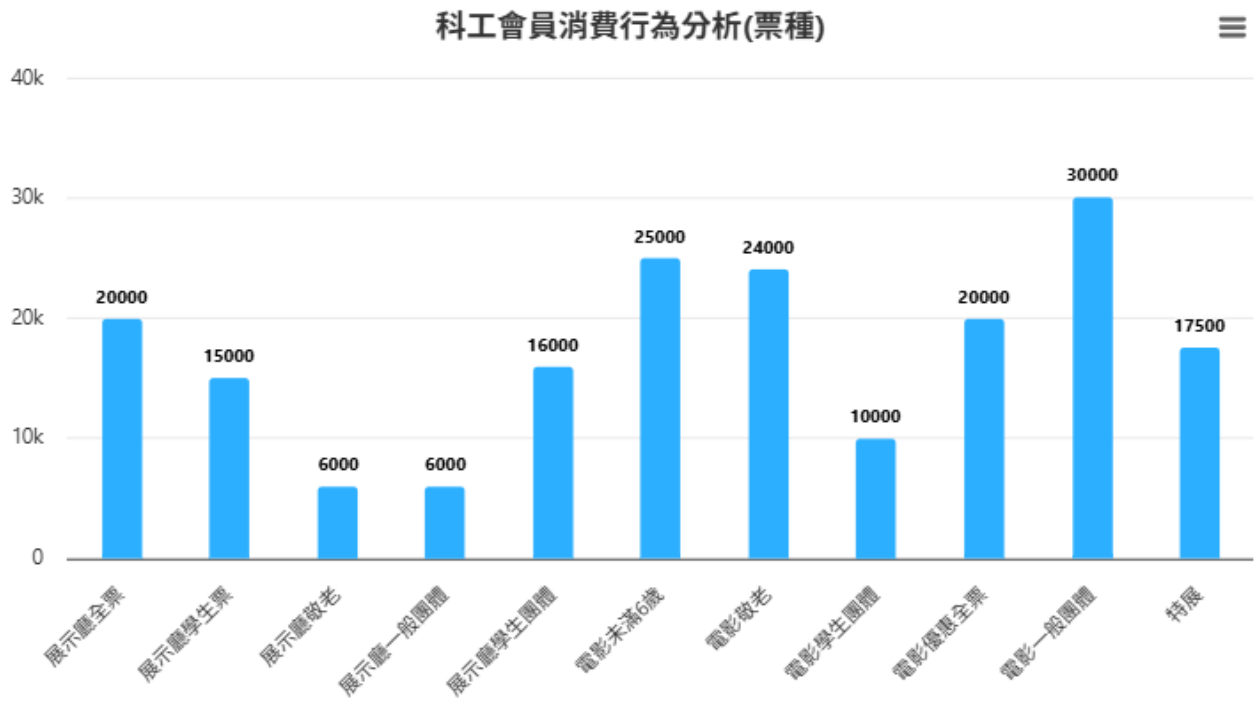
3、資料來源

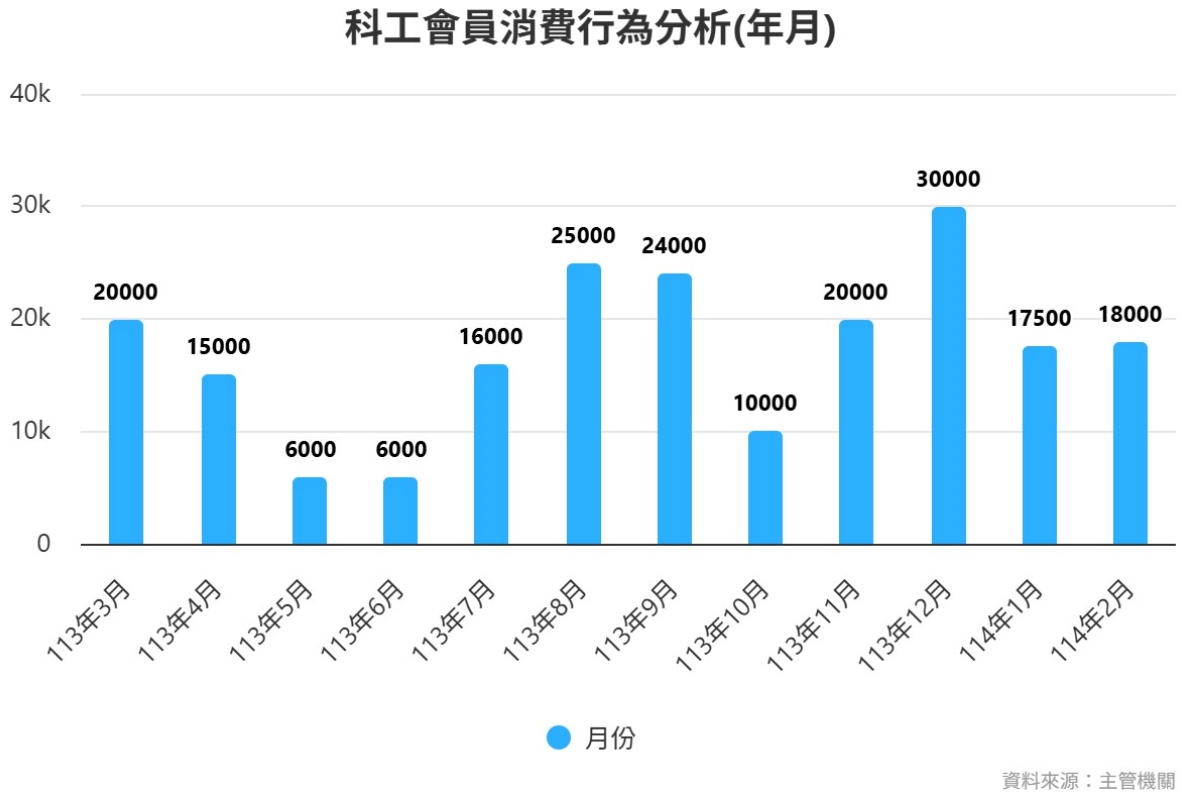
(1)會員系統紅利積點軌跡資料

4、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜收入來源分析
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
分析條件
收入來源分析 售票收入 商品收入 活動收入
資料範圍 實體購票 線上購票（掌握科工） 付費購票（掌握科工） 科教活動
* 起迄日 從 2024/04/15 至 2025/04/15
性別 男 女 其他
居住地
居住地分類
北部地區 臺北市 新北市 基隆市 新竹市 桃園市 新竹縣 宜蘭縣
中部地區 臺中市 苗栗縣 彰化縣 南投縣 雲林縣
南部地區 高雄市 臺南市 嘉義市 嘉義縣 屏東縣 澎湖縣
東部地區 花蓮縣 臺東縣
其他 金門縣 連江縣 境外地區
年齡區間 從 35歲 至 40歲
圖表輸出
Y軸資料 營收金額
X軸資料 年度 月份 季度 日期 票種
圖表類型 長條圖 圓餅圖 折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）
科工會員收入來源分析(票種)
50k
40k
30k
20k
10k
0
20000
15000
6000
6000
16000
25000
24000
10000
20000
20000
10000
7500
39000
展示廳全票
展示廳學生票
展示廳敬老
展示廳一般團體
展示廳學生團體
電影未滿6歲
電影敬老
電影學生團體
電影優惠全票
電影一般團體
臺測特展成人
臺測特展學生
科工會員
月份
資料來源：主管機關

5、圖表分析





資料來源：主管機關

(五)會員忠誠度分析

1、分析條件

(1)資料範圍：消費活動、紅利活動、體驗活動、教育活動

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(5)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：會員數

(2)X 軸資料：單選，選項為：忠誠度區分

(3)圖表類型：單選，選項為：長條圖、圓餅圖

3、分析模型

A、RFM 模型

以 RFM 模型計算會員忠誠度：

(A)Recency（R）：距離會員最近一次購買的時間（天數）。

(B)Frequency（F）：會員在特定時間內購買的次數。

(C)Monetary（M）：會員在特定時間內累積消費金額。

示例數據：

會員ID	最近購買天數 (R)	購買次數 (F)	總消費金額 (M)
A123	10	5	5000
B456	30	3	2000
C789	5	10	10000

B、計算方法

會員忠誠度計算方法：以分群方式分 5 群，分別給 1-5 級(分)：

(A)R：越小越好（最近購買的會員較忠誠）；最小的 20% 給 5 分，最大 20% 給 1 分。

(B)F：越大越好（購買頻率高表示忠誠度高）；最小的 20% 給 1 分，最大 20% 給 5 分。

(C)M：越大越好（高消費會員價值較高）；最小的 20% 給 1 分，最大 20% 給 5 分。

C、分級方法

會員忠誠度分為金、銀、銅三級。其中，依據 RFM 總分，將會員劃分以下忠誠度群組：

(A)**金科工：RFM 總分 12～15**；忠誠會員，應提供特殊優惠。

(B)**銀科工：RFM 總分 8～11**；潛力客戶，可透過行銷活動強化關係。

(C)**銅科工：RFM 總分 3～7**；可能流失的會員，可用促銷或再行銷策略吸引回購。

D、消費金額計算

會員忠誠度主要由「消費活動」計算忠誠度。消費活動主要來自以下幾類行為：票券購買(含線上與實體)、商品消費、課程消費等。

4、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜會員忠誠度分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
資料範圍
消費活動
紅利活動
體驗活動
教育活動
* 起迄日
從
2024/04/15
至
2025/04/15
性別
男
女
其他
居住地
居住地分類
北部地區
臺北市
新北市
基隆市
新竹市
桃園市
新竹縣
宜蘭縣
中部地區
臺中市
苗栗縣
彰化縣
南投縣
雲林縣
南部地區
高雄市
臺南市
嘉義市
嘉義縣
屏東縣
澎湖縣
東部地區
花蓮縣
臺東縣
其他
金門縣
連江縣
境外地區
年齡區間
從
35歲
至
40歲
圖表輸出
Y軸資料
會員數
X軸資料
忠誠度區分
圖表類型
長條圖
圓餅圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

（六)教育活動成效分析

1、分析條件

(1)起迄日：查詢會員行為紀錄之起迄日。

(2)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(3)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(4)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：參與人數、消費金額、活動紅利、後續參與率

(2)X 軸資料：單選，選項為：年度、季度、月份、日期、關鍵字分析

(3)關鍵字分析：夏令營、冬令營、週日閱讀、海外科學營、春季班、生活學堂、體驗活動、創客、其他

(4)圖表類型：單選，選項為：長條圖、圓餅圖、折線圖

3、後續參與率

(1)定義：「後續參與率」=

參與 2 次以上活動的學員數÷全體參與學員數×100%

(2)可作為評估學員忠誠度與活動吸引力的核心指標。

4、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜教育活動成效分析
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
資料範圍
推廣教育活動報名與紅利資訊
起迄日
從
2024/04/15
至
2025/04/15
性別
男
女
其他
居住地
居住地分類
北部地區
臺北市
新北市
基隆市
新竹市
桃園市
新竹縣
宜蘭縣
中部地區
臺中市
苗栗縣
彰化縣
南投縣
雲林縣
南部地區
高雄市
臺南市
嘉義市
嘉義縣
屏東縣
澎湖縣
東部地區
花蓮縣
臺東縣
其他
金門縣
連江縣
境外地區
年齡區間
從
35歲
至
40歲
圖表輸出
Y軸資料
參與人數
消費金額
活動紅利
後續參與率
X軸資料
年度
月份
季度
日期
關鍵字分析
關鍵字分析
夏令營
冬令營
週日閱讀
海外科學營
春季班
關鍵字管理
生活學堂
體驗活動
創客
其他
圖表類型
長條圖
圓餅圖
折線圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

（七）會員級別標籤

1、分析條件

(1)資料範圍：消費活動、紅利活動、體驗活動、教育活動

(2)起迄日：查詢會員行為紀錄之起迄日。

(3)性別：多選（Checkbox），選項：男、女及其他；預設為「全選」。

(4)居住地：選項多選，涵蓋所有縣市，預設為「全選」，並依地區分類(選項與介面設計同「綜合分析」)。

(5)年齡區間(上下限)：預設為空值(不限制)

2、圖表輸出

(1)Y 軸資料：單選，選項為：會員數

(2)X 軸資料：單選，選項為：會員級別

(3)會員級別：全館會員級別、客制化會員級別 A、客制化會員級別 B……

(4)圖表類型：單選，選項為：長條圖、圓餅圖

3、客製化會員級別規則制定

(1)演算法：RFM 模型

(2)資料範圍：消費活動、紅利活動、體驗活動、教育活動等(多選)

(3)會員級別名稱

(4)級別組數：1-13

(5)級別命名：各組以文字輸入命名

(6)級別範圍：各組以「分數上限」設定級別範圍

4、客製化會員級別範例

(1)資料範圍：選擇「消費活動、紅利活動」

(2)會員級別名稱：消費紅利級別

(3)級別組數：5

(4)級別命名：博士、達人、大師、玩家、青銅

(5)級別範圍

A、博士 (不需選擇上限，預設 15)

B、達人 (上限 13)

C、大師 (上限 11)

D、玩家 (上限 8)

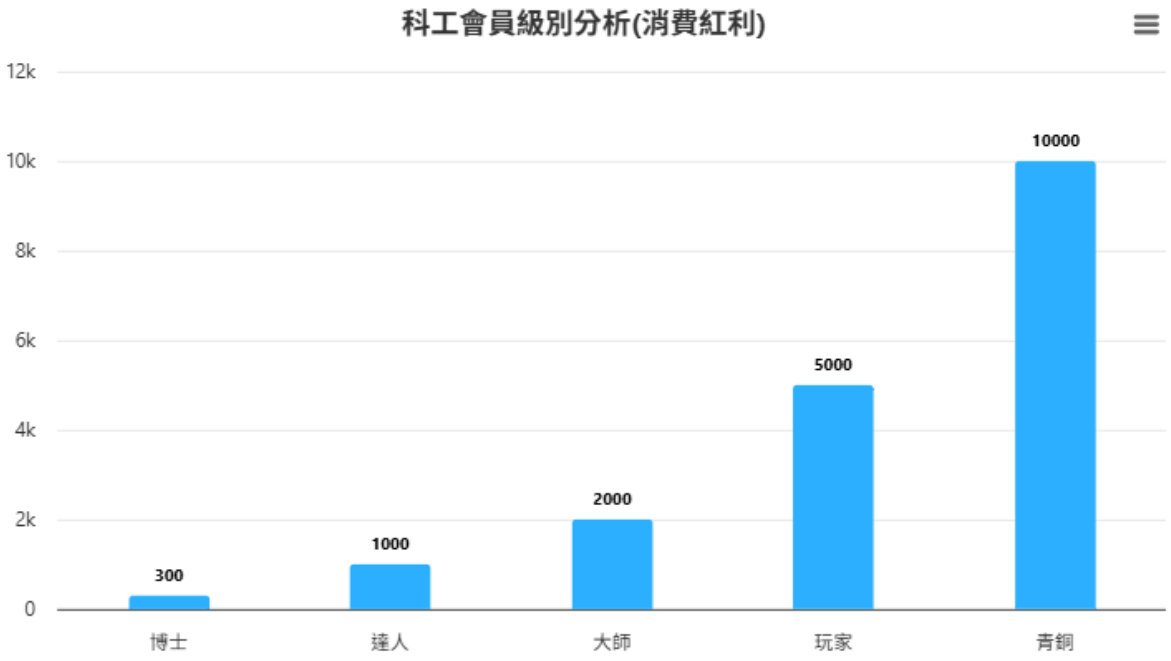
E、青銅 (上限 5)

5、介面設計

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜會員級別標籤
新增會員級別 +
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
分析條件
資料範圍
消費活動
紅利活動
體驗活動
教育活動
* 起迄日
從
2024/04/15
至
2025/04/15
性別
男
女
其他
居住地
居住地分類
北部地區
臺北市
新北市
基隆市
新竹市
桃園市
新竹縣
宜蘭縣
中部地區
臺中市
苗栗縣
彰化縣
南投縣
雲林縣
南部地區
高雄市
臺南市
嘉義市
嘉義縣
屏東縣
澎湖縣
東部地區
花蓮縣
臺東縣
其他
金門縣
連江縣
境外地區
年齡區間
從
35歲
至
40歲
圖表輸出
Y軸資料
會員數
X軸資料
會員級別
會員級別
全館會員級別
消費紅利級別
圖表類型
長條圖
圓餅圖
圖表標題
網頁輸出
報表產出
原始資料（Excel）

國立科學工藝博物館
NATIONAL SCIENCE AND TECHNOLOGY MUSEUM
登出
首頁｜大數據分析｜會員級別標籤
新增會員級別 +
綜合分析
館內活動軌跡
參觀行為分析
收入來源分析
會員忠誠度分析
教育活動成效分析
會員級別標籤
郭佳寧
目前 IP 登入位置：61.230.61.45
會員管理
紅利活動
信件發送
大數據分析
系統管理
權限管理
會員級別編輯
資料範圍
消費活動
紅利活動
體驗活動
教育活動
會員級別名稱
消費紅利級別
級別組數
5
級別命名與範圍
博士 14 ~ 15
達人 12 ~ 13
大師 9 ~ 11
玩家 6 ~ 8
青銅 3 ~ 5
儲存

6、圖表分析


科工會員級別分析(消費紅利)
12k
10k
8k
6k
4k
2k
0
300
1000
2000
5000
10000
博士
達人
大師
玩家
青銅

(八)各式報表產出

行為分析報告及票務等級報表之產出，其功能與介面整合於各大數據分析之「功能按鈕」中。每一組大數據分析功能皆有三種圖表輸出功能，包含：網頁輸出(HTML)、報表產出(Excel/ODS)、原始資料(Excel/ODS)。其中，「報表產出」即為以統計表格方式輸出大數據分析之結果。

(九)訪客模式分析

1、以數位存根(Http Cookie)鑑別訪客模式之使用者行為。以虛擬會員編號作為唯一值識別訪客行為足跡。

2、整合未來其他系統訪客模式之行為分析，例如訪客模式之線上購票、意見回饋、展廳導覽等行為。

3、整合訪客模式之實體行為足跡，例如訪客模式之展廳導覽(QR Code掃描)等行為

四、API 功能擴充與介面規劃

(一)API 清單

項次	API 名稱	端點	新建	所屬系統	方法/格式
1	掌握科工行為紀錄	https://mobilemgr.nstm.gov.tw /v1.0/behavior	V	掌握科工	GET/JSON
2	信件發送訂閱會員	https://mms.nstm.gov.tw:23489/api/member	V	會員系統	GET/JSON
3	容留資訊	https://mobilemgr.nstm.gov.tw /v1.0/footfall	V	掌握科工	GET/JSON

(二)API 設計

1、掌握科工行為紀錄 API

(1)查詢欄位

序號	欄位名稱	中文名稱	必填	說明	實例與備註
1	DateStart	行為起日	V	查詢結果包括起日	2025-01-01
2	DateUnil	行為迄日	V	查詢結果包括起日	2025-03-31
3	Class	行為分類		六大行為分類 多選，以「逗號」(,)區隔 輸入 0 為不限制	1,2,3
4	Type	功能種類		多選，以「逗號」(,)區隔	智慧展示,展品報修
5	PointLower	紅利點數下限		正整數	0
6	PointUpper	紅利點數上限		正整數	10000
7	AmountLower	消費金額下限		正整數	0
8	AmountUpper	消費金額上限		正整數	10000
9	Floor	樓層		單選 B3/B1/1F/2F/4F/6F	B1
10	Hall	展廳		單選，輸入展廳名稱	開放式典藏庫

(2)輸出欄位

序號	欄位名稱	中文名稱	說明	實例與備註
1	System	系統名稱	系統/網站名稱	掌握科工、票務系統
2	Date	行為時間	yyyy-MM-dd HH:mm:ss	2025-03-24 20:34:14
3	UserId	會員編號	會員中心 8 碼會員編號	24334213
4	Class	行為分類	六大主分類： 1 消費 2 紅利	行為分類記錄 1-6 數字 有購票之行為優化列入消費分類

序號	欄位名稱	中文名稱	說明	實例與備註
			3 體驗 4 瀏覽 5 教育 6 服務	
5	Type	功能種類	線上購票 付費購買 智慧展示 …… 課程紅利	
6	Action	動作	● 線上購票：加入購物車、選擇購物車、線上刷卡、交易成功、票券使用 ● 課程活動：活動分類	
7	Detail	詳細資訊	說明商品名稱、票種、動作明細等資訊 ● 線上購票：票種 ● 課程活動：活動名稱	
8	Location	實體位置	以展廳為單位；後續可再細緻標注詳細位置 實體位置名稱回傳值需符合《系統功能實體位置對照表》	B1 氣候變遷 2F 動力與機械 4F 健康探索廳
9	Point	紅利點數	紅利增加與減少數量	+10 / -20
10	Amount	消費金額	購票或商品交易之金額	300
11	IP	IP 位置		123.123.123.123

2、信件發送訂閱會員 API

(1)查詢欄位

序號	欄位名稱	中文名稱	必填	說明	實例與備註
1	RegisterStart	註冊起日		查詢結果包括起日	2025-01-01
2	RegisterUntil	註冊迄日		查詢結果包括起日	2025-03-31

(2)輸出欄位

序號	欄位名稱	中文名稱	說明	實例與備註
1	MB_CODE	會員編號		
2	MB_EMAIL	電子郵件		

3、容留系統資訊 API

(1)查詢欄位

序號	欄位名稱	中文名稱	必填	說明	實例與備註
1	DateStart	行為起日	V	查詢結果包括起日	2025-01-01
2	DateUnil	行為迄日	V	查詢結果包括起日	2025-03-31
3	Floor	樓層		單選 B3/B1/1F/2F/4F/6F	B1
4	Hall	展廳		單選，輸入展廳名稱	開放式典藏庫

(2)輸出欄位

序號	欄位名稱	中文名稱	說明	實例與備註
1	DateStart	紀錄起始時間	yyyy-MM-dd HH:mm:ss	2025-03-24 20:34:14
2	DateStart	紀錄終止時間	yyyy-MM-dd HH:mm:ss	紀錄終止時間多起始時間 5 分鐘
3	Floor	樓層		4F
4	Hall	展廳		健康探索廳
5	In	累積入場人數		250
6	Out	累積出場人數		100
7	Sum	場內人數		150

(三)會員系統軌跡資料紀錄

1、行為軌跡資料表增加欄位「實體位置」(TR_LOCATION)，資訊以現行「活動備註」資訊(例如 E15、T02、P03 等)轉譯為文字說明格式(例如：2F 兒童科學園區)。

2、紅利軌跡資料表增加欄位「票種」(TRANS _TICKET)，資訊以現行「交易備註」欄位(票號)，查詢「訂單明細查詢 API」而得。票種資料格式為：「展示廳全票 1/電影敬老 2/量測特展成人 1」。

3、上述兩項資訊取得以「排程方式」查詢後定期寫入會員系統資料庫。

4、紅利軌跡於現行系統或外部系統之會員「消費行為」之紀錄需律定加註「付費」，以區分紅利來源之屬性。例如會員參與「紅利活動」中有付費者，需加註「付費」。

第參章 建置期程

一、建置期程

(一)會員系統

1、系統優化

建置期程以決標日為專案啟動日進行規劃。

項次	期程	工作項目	交付項目	交付時程
1	第一期	1. 召開專案啟動會議 2. 專案工作計畫規劃	專案工作計畫書	決標後 20 日曆天內
2		1. 需求訪談 2. 系統分析與設計規劃	1. 系統分析及設計規格書 2. 需求雙向追溯表 3. SSDLC 檢核表(含需求與設計階段)	決標後 40 日曆天內
3		協助驗證掌握科工系統「容留資訊」與「掌握科工行為紀錄」API	驗證測試報告書	民國 114 年 10 月 19 日前
4		完成以下功能開發與測試： 1. 註冊流程簡化(含第三方整合登入) 2. 會員資訊管理 3. 信件發送功能 4. 大數據與分眾分析 (1) 館內活動軌跡 (2) 參觀行為分析 (3) 收入來源分析 (4) 會員忠誠度分 (5) 各式報表產出	1. 驗證測試報告書 2. 需求雙向追溯表 3. 資訊安全檢測報告(含系統軟體弱點檢測報告與源碼安全檢測報告等) 4. SSDLC 檢核表(含開發與測試階段)	民國 114 年 10 月 27 日前
5		完成系統建置並部署至本館環境	SSDLC 檢核表(部署階段)	民國 114 年 11 月 07 日前
6		教育訓練	教育訓練計畫書及實施實錄報告	
7		整合測試作業	系統問題反應暨處理單	民國 114 年 11 月 21 日前
8		第一期查驗後上線	1. 系統測試結果報告書 2. 系統操作手冊	民國 114 年 11 月 28 日前

項次	期程	工作項目	交付項目	交付時程
			3. 資訊安全檢測報告（含系統軟體弱點檢測報告、源碼安全檢測報告等），並附「防護基準佐證報告」 4. SBOM 表 5. 緊急回復計畫書 6. 授權證明書 7. 第三方軟體使用授權書（如開發過程中有使用到第三方軟體時，須提供永久無償使用授權書） 8. 系統程式原始碼及執行碼光碟片	
9	第二期	1. 召開第二期專案啟動會議 2. 專案工作計畫規劃	專案工作計畫書(第二期)	民國 115 年 1 月 16 日前
10		1. 第二期需求訪談 2. 系統分析與設計規劃	1. 系統分析及設計規格書 2. 需求雙向追溯表 3. SSDLC 檢核表(含需求與設計階段)	民國 115 年 3 月 6 日前
11		完成下列功能開發與測試： 1. 前台功能擴充 ● 訊息功能擴充 ● 前台介面優化 2. 後台功能擴充 ● 操作介面優化 ● 自動提醒功能 ● 單一簽入驗證 3. 大數據與分眾分析 ● 綜合分析 ● 教育活動成效分析 ● 會員級別標籤 ● 訪客模式分析 4.「信件發送訂閱會員」API	1. 驗證測試報告書 2. 需求雙向追溯表 3. 資訊安全檢測報告(含系統軟體弱點檢測報告與源碼安全檢測報告等） 4. SSDLC 檢核表(含開發、測試與部署階段) 5. 系統測試結果報告書	民國 115 年 06 月 12 日
12		完成系統建置並部署至	SSDLC 檢核表(部署階段)	民國 115 年 06 月 26 日

項次	期程	工作項目	交付項目	交付時程
		本館環境		前
13		教育訓練	教育訓練計畫書及實施實錄報告	
14		整合測試作業	系統問題反應暨處理單	民國 115 年 07 月 10 日前
15		系統驗收後上線	交付文件 1. 系統測試結果報告書 2. 系統安裝與管理維護手冊 3. 系統操作手冊 4. 資訊安全檢測報告（含系統軟體弱點檢測報告、源碼安全檢測報告等），並附「防護基準佐證報告」 5. SBOM 表 6. 緊急回復計畫書 7. 授權證明書 8. 第三方軟體使用授權書（如開發過程中有使用到第三方軟體時，須提供永久無償使用授權書） 9. 結案報告書 10. 系統程式原始碼及執行碼光碟片 11. 保固證明書	民國 115 年 07 月 24 日前
16	保固期	系統保固維護 (保固範圍包括會員系統前後台全系統以及第一、二期建置功能)	1. 定期保養檢測單(包含系統程序/作業調整之事項) 2. 至保固期滿時之最新版文件（包含：資料庫架構文件、系統安裝與管理維護手冊、系統操作手冊、程式原始碼及執行碼光碟片等）	自驗收合格日起算保固 2 年。

2、系統維護

本案自 114 年 12 月 9 日起提供會員系統全系統(含系統前台、前台 API、系統後台、後台 API)以及團約系統之系統保固維護服務。

(1)系統維護包含有關會員系統之保養維護服務、技術諮詢、故障修復、每 6 個月定期保養檢測等保固服務，廠商須指派專責人員為各項應用系統之維護及諮詢窗口。

(2)維護工作事項

1. 確保本系統既有功能持續正常運作。
2. 本系統運作異常時之測試與檢修。
3. 本系統運作維護之諮詢。
4. 落實本系統資訊安全防護作業。
5. 每半年交付定期維護工作紀錄表。
6. 如有專案需求時，應提供各項數位博物館網站與本館文物典藏系統資料庫介接之技術支援及問題排除。
7. 當功能無法持續作業時，得標廠商應負責問題排除、修正及除錯，於接獲機關通知後4個工作小時內回覆；如本案功能無法正常運作，得標廠商應於接獲告知起4個工作小時內派員檢修，並於1個工作日內完成修復，但機關同意者，不在此限。

(3)維護內容

1. 確保本案標的持續正常運作。
2. 保固期間若系統執行發生錯誤，廠商應免費修正。

3. 因專案需求修改本案系統程式時，廠商應先檢視其修改項目，並提出修改項目之所需作業天數，待與承辦人確認無誤後， 即進行系統程式增修作業。
4. 協助安裝本系統及資料復原工作，使系統恢復正常運作，不另行收費。

二、交付文件

（一）交付文件說明

文件名稱	建議內容
專案工作計畫書	含履約範圍、目標、工作項目、預定時程規劃、各階段文件函送、相關人員工作分派等。
系統分析及設計規格書	含整體架構、功能摘要、環境架構、系統功能需求、系統相關參數、作業流程圖、資料流程圖、軟硬體架構圖、界面規格設計、相關系統介接介面及資料庫設計等。
需求雙向追溯表	依雙向追溯(向前追蹤/向後追蹤)原則，編擬雙向追溯編號原則；內容含 1)雙向追溯之需求規格與設計規格，2) 程式模組、測試方案與驗證結果雙向追溯架構與編號原則。
驗證測試報告書	含系統測試環境、測試執行方式、雙向追溯測試方案與測試結果等。
SBOM表	系統使用各式非自行開發之第三方元件、套件、模組、編譯引擎等，須詳列於 SBOM 表中經本機關同意。內容需含第三方套件名稱、授權(License)、版本、發布時間、CVSS威脅分數、風險指數(低、中、高、重大)，並不得使用威脅分數 7 分以上指數套件。
系統測試結果報告書	含測試環境、測試執行方式、壓力與負載測試、單元測試與整合測試結果、問題解決等。
教育訓練計畫書及實施實錄報告	含教育訓練計畫書（訓練地點、時程、課程內容講義、建議講師等）出席人員簽到表、訓練手冊、照片等。
系統問題反應暨處理單	由館方業務同仁進行系統實際使用及測試。測試期間本館反饋之問題或建議及後續處理。
系統安裝與管理維護手冊	含系統安裝、伺服器開關機、例行維護、注意事項、異常排除及日誌研判、網站移轉、資料備份及還原等。
系統操作手冊	含網站概述、軟硬體環境要求、網站架構說明、功能說明、網站操作說明、功能畫面操作指引與說明、常見範例說明等。
緊急回復計畫書	含系統緊急回復計畫等。
程式原始碼及執行碼	含資料庫結構表、網站原始碼、元件、各應用系統原始程式碼（source code）、相關編譯安裝程序文件及專案使用圖文原始檔等。
資訊安全檢測報告（系統軟體弱點檢測報告、源碼安全檢測報告等）	含檢測時間、檢測方式、檢測工具說明、弱點摘要及分析說明、安全強化建議等，並附「防護基準佐證報告」。

文件名稱	建議內容
結案報告書	含本案所有成果、過程紀錄、達成之效益等。
維護紀錄單	含維護問題描述、處理方式、時間等說明。

(二)雙向追溯表說明

1、編碼說明

(1)系統代碼：SER_MBR (代碼意義：公共服務組_會員系統)

(2)業務需求編號：以《需求說明書》之專案需求編列。編碼為系統代碼後接業務需求(Business Requirements)縮寫「BR」，並以三位數字依序編列。例如：SER_MBR_BR_001。

(3)功能需求編號：以《系統分析及設計規格書》之系統功能需求編列。編碼為系統代碼後接功能需求(Functional Requirements)縮寫「FR」或非功能需求(Non-Functional Requirements)縮寫「NFR」，並以三位數字依序編列。例如：SER_MBR_FR_001、SER_MBR_UFR_001等。非功能需求可包括例如「系統應於 4 秒內回應查詢請求」(效能需求)或「第三方元件不得使用 CVSS 威脅分數 7 分以上指數套件」(資安需求)等非功能性規範。

(4)測試方案編號：測試方案編碼方式為系統代碼後接測試方案(Test Case)縮寫「TC」，並以三或四位數字依序編列。例如：SER_MBR_TC_001 或 SER_MBR_TC_0001 等。測試方案以及編號應於《雙向追溯驗證測試報告書》詳細撰寫。

2、雙向追溯表建議欄位：

需求編號、需求描述、來源(需求說明書、需求訪談等；可加註提出人)、功能需求編號、功能需求摘要、測試方案編號、測試狀態(通過、失敗、未測試等)、確認時間(甲方驗證通過時間與簽章)、備註等。

3、雙向追溯表建議格式

業務需求			功能需求		測試與驗證		
需求編號	需求描述	來源	功能需求編號	功能需求摘要	測試方案編號	測試狀態	確認時間
SER_MBR_BR_001	系統以電子郵件自動提醒會員點數即將到期	需求說明書	SER_MBR_FR_001	點數到期前 1 個月以電子郵件提醒	SER_MBR_TC_001 SER_MBR_TC_002	通過	114.09.10
			SER_MBR_FR_001	到期日後點數歸零	SER_MBR_TC_003	未測試	
SER_MBR_BR_002	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入	需求說明書	SER_MBR_NFR_001	同一帳號登入連續失敗達 3 次後鎖定該帳號不得登入	SER_MBR_TC_004	通過	114.09.05
			SER_MBR_UNR_001	最後一次登入失敗後 15 分鐘內不得換入	SER_MBR_TC_005	未通過	114.09.05

第肆章 資訊安全法規及標準(資通系統防護基準)

依《資通安全責任等級分級辦法》資通系統防護基準「中級」規定，應辦事項(SSDLC)與控制措施設計如下說明。

一、資通系統防護基準 SSDLC 檢核表

1、存取控制

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
1-1. 帳號管理	1-1-1. 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	【資安需求項目查檢】資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、建立、修改、啟用、停用或刪除之行為。	V	V	V		
	1-1-2. 已逾期之臨時或緊急帳號應刪除或禁用。	【資安需求項目查檢】若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。	V	V	V		
	1-1-3. 資通系統閒置帳號應禁用。	【資安需求項目查檢】宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。	V	V	V		
	1-1-4. 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	【日常維運管理需求】定期審核資通系統帳號使用現況，檢視是否存在帳號被異常建立、竄改或啟用等行為，並禁用或刪除閒置帳號與臨時帳號。					V
1-2.最小權限	1-2-1. 採最小權限原則，僅	【日常維運管理需求】使用者(或代表使用者行為之程序)應	V	V	V		V

	允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	以完成該工作所需的最小權限操作系統功能，避免過度授權而增加系統資源被不當存取的風險。因此在進行授權決定時，應考量該使用者(或代表使用者行為之程序)之業務性質與範圍，限制其所能存取的系統功能及資料。					
1-3. 遠端存取	1-3-1. 對於每一種允許之遠端存取類型(如遠端桌面連線、ssh、網路芳鄰或FTP)，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	【資安需求項目查檢】機關應明確訂定資通系統之存取限制、組態需求、連線需求，並將這些資訊文件化，以供日後查檢。 開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，至少辦理下列防護措施： (一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。 (二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。 (三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼。					V
	1-3-2. 使用者之權限檢查作業應於伺服器端完成。	【資安需求項目查檢】應於伺服器端實作權限檢查機制，並預設禁止任何未通過權限檢查之存取行為，以避免被使用者繞過。					V
	1-3-3. 應監控	【日常維運管理需求】資通系					V

	資通系統遠端連線。	統所允許之遠端連線活動，應使用監控設備或其他可偵測未經授權使用的設備，在發現異常連線或存取行為時提出警告，以防止資通系統被不當使用。					
	1-3-4. 資通系統應採用加密機制。	【資安需求項目查檢】遠端存取資通系統時，應以加密機制保護機敏資料傳輸時之機密性。常見作法如採用 HTTPS 加密傳輸等，並選擇高強度之協定版本及演算法。					V
	1-3-5. 資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	【日常維運管理需求】遠端存取行為應經過適當授權後始可放行，若有必要允許外部遠端存取之系統功能，應限制資通系統遠端存取之來源(如機器、網路位址等)，預先定義合法來源並進行管理，避免全面性開放存取。					V

2、事件日誌與可歸責性

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
2-1. 紀錄事件	2-1-1. 訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。	【資安需求項目查檢】應依機關規定之時間週期及紀錄留存政策，保留系統事件日誌(Audit Logs)，目的包含程式除錯、行為歸責、稽核取證及法規要求等。 保存範圍如下： A 級機關：應保存全部資通系統與各項資通及防護設備最近 6 個月之日誌紀錄。 B 級機關：應保存全部核心資通系統與相連之資通及防護設備最近 6 個月之日誌紀錄。 C 級機關：應保存全部核心資	V	V	V		V

		通系統最近 6 個月之日誌紀錄。 保存項目如下： 作業系統日誌 (OS event log) 網站日誌 (web log) 應用程式日誌 (AP log) 登入日誌 (logon log)					
	2-1-2. 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	【資安需求項目查檢】資通系統應實作記錄特定事件之功能，如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等。	V	V	V		V
	2-1-3. 應記錄資通系統管理者帳號所執行之各項功能。	【資安需求項目查檢】系統管理者為資通系統內具有最高權限之帳號，對系統及資料極具影響力，記錄所有管理者帳號執行之各項功能，有助於定期記錄系統行為及資安事件追查。	V	V	V		V
	2-1-4. 應定期審查機關所保留資通系統產生之日誌。、建立、修改、啟用、停用及刪除。	【日常維運管理需求】機關應訂定日誌審查時程，由負責人員檢視日誌紀錄內容，以掌握是否在期間內曾發生重要的資安事件，如異常的存取行為、重大的系統錯誤等。					V
2-2.日誌紀錄內容	2-2-1. 資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致	【資安需求項目查檢】日誌應詳細描述所觸發的事件，包含人、 事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。盡可能採用單一的 Log 機制，如不得同時混用兩種以上日誌產生	V	V	V		V

	性，並應依資通安全政策及法規要求納入其他相關資訊。	套件(如 Log4Net 與 Nlog 等)，並應確保日誌內容格式之可讀性，以便於事件比對與追查。日誌應依據資通安全政策及其他法規要求，納入任何有必要留存之資訊，如憑證資訊、日誌層級、會談識別碼等。					
2-3.日誌儲存容量	2-3-1. 依據日誌紀錄(Audit Logs)儲存需求，配置所需之儲存容量。	【資安需求項目查檢】資通系統應配置日誌紀錄所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。					V
2-4.日誌處理失效之回應	2-4-1. 資通系統於日誌處理失效時，應採取適當之行動。	【資安需求項目查檢】日誌處理失效時，應訂定相對應的處理措施(如覆寫最舊的稽核紀錄、停止產生稽核紀錄或對特定人員提出警告等)，避免危害系統可用性，或是當資安事件發生時無稽核紀錄可比對追查之情況。					V
2-5.時戳及校時	2-5-1. 資通系統應使用系統內部時鐘產生日誌紀錄(Audit Logs)所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	【資安需求項目查檢】使用系統內部時鐘產生日誌所需時戳，採用全系統一致的時間標準，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。					V
	2-5-2. 系統內部時鐘應定期與基準時間源進行同步。	【資安需求項目查檢】日誌紀錄必須維持使用精確的時間，以利事件追蹤及稽核取證等用途，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統及網路設備與校時伺服器進行同步，如國家標準時間伺服器					V

		(time.stdtime.gov.tw)或使用機關自建之伺服器。					
2-6.日誌資訊之保護	2-6-1. 對日誌(Audit Logs)之存取管理，僅限於有權限之使用者。	【資安需求項目查檢】應施行日誌存取控管，避免未經授權使用者惡意讀取、竄改或刪除稽核紀錄。					V
	2-6-2. 應運用雜湊或其他適當方式之完整性確保機制。	【資安需求項目查檢】日誌紀錄以安全雜湊演算法產生，並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。其他保護方式如加密、唯讀保存及即時監視檔案異動行為等。	V	V	V		V

3、營運持續計畫

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
3-1.系統備份	3-1-1. 訂定系統可容忍資料損失之時間要求。	【日常維運管理需求】機關應訂定可容忍資料損失之時間要求，若資安事件發生造成資料損失時，需使用最接近的備份資料進行復原，資料損失與備份資料之間的時間間隔，亦稱為復原點目標(Recovery Point Objective, RPO)。 RPO 一旦訂定完成，則可協助系統維護人員選擇適合的備份機制及頻率。如若訂定為 1 小時，則至少每小時必須進行一次資料備份，所選擇的儲存媒體可能為磁碟；但若 RPO 訂定為一週(168 小時)，則至少每週進行一次資料備份，使用磁帶或光碟片等媒體即可滿足備份需求。					V
	3-1-2. 執行系統源碼與資料	【日常維運管理需求】應備份系統源碼與資料，備份時機如					V

	備份。	廠商交付或內容變更時，或依機關規定定期備份。					
	3-1-3. 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	【日常維運管理需求】常見之儲存媒體如磁碟、磁帶、光碟等，因使用方式及保存環境之差異，可能影響儲存媒體壽命而造成備份資料損毀。機關應訂定週期性測試時間表，並依時間表進行備份資料還原測試，以確保備份資料處於可用狀態。					V
3-2.系統備援	3-2-1. 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	【日常維運管理需求】機關應考量服務需求、使用現況、相關資源項目，以及資安事件發生之風險，訂定資通系統從中斷後至重新恢復服務之可容忍時間要求，亦可稱為復原時間目標(Recovery Time Objective, RTO)。					V
	3-2-2. 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。	【日常維運管理需求】機關應準備適當及足夠的備援設備或其他有效恢復服務運作之方式(如還原虛擬機器快照等)，以便在發生災害時，可於所訂定之容忍時間內讓服務回復正常運作。					V

4、識別與鑑別

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
4-1. 內部使用者之識別與鑑別	4-1-1. 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	【資安需求項目查檢】資通系統應具備唯一識別及鑑別機關使用者之功能，如替內部使用者建立個別帳號，以強化系統之可歸責性(Accountability)。若多人共用同一個帳號登入系統，則難以從稽核紀錄識別確切的使用者身分。	V	V	V		
4-2. 身分驗證管理	4-2-1. 使用預設密碼登入系統時，應於登入後要求立即變更。	【資安需求項目查檢】使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。	V	V	V		
	4-2-2. 身分驗證相關資訊不以明文傳輸。	【資安需求項目查檢】身分驗證相關資訊於網路傳輸時，不可直接傳輸明文(如密碼原始字串)，避免被惡意攔截網路封包而外洩。	V	V	V		
	4-2-3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次，至少15分鐘內不允許該帳號繼續嘗試或使用機關自建之失敗驗證機制。	【資安需求項目查檢】系統應實作帳戶鎖定機制，於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。	V	V	V		
	4-2-4. 使用密碼進行驗證時，應強制最低密碼複雜度、強制密碼最短及最長之效期限制。(但對於非內部使	【資安需求項目查檢】應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，目的在避免因使用安全性不足之密碼而被人輕易破解。強制密碼最短效期目的在防止使用者規避3次密碼歷程之限制，而於短期內頻繁變換密碼後又改回	V	V	V		

	用者可依機關自行規範辦理)	原始密碼。強制最長之效期之目的在避免固定使用同一組密碼。實務上，可參考政府組態基準 GCB 之建議值，設定密碼複雜度及密碼使用效期限制。					
	4-2-5. 密碼變更時，至少不可以與前三次使用過之密碼相同。(但對於非內部使用者可依機關自行規範辦理)	【資安需求項目查檢】使用者前 3 次舊密碼應被保留(以雜湊值形式)，於設定新密碼時，比對新密碼與舊密碼之雜湊值，若雜湊值相同則拒絕此次密碼設定。	V	V	V		
	4-2-6. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	【資安需求項目查檢】系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。如圖形驗證碼(CAPTCHA)為常見的防範方式，透過將驗證碼以圖形方式呈現於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(如勾選特定選項等)，防堵自動化程式之嘗試行為。	V	V	V		
	4-2-7. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	【資安需求項目查檢】密碼重設機制設計不良可能造成安全問題，常見錯誤是系統自行產生隨機密碼後以電子郵件寄送給使用者，此問題在於無法確保傳輸過程經過加密保護，故提高資安風險。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，如電子郵件或手機號碼等，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性符記(如簡訊驗證碼、電子郵件驗證連結	V	V	V		

		等)，一般會由亂數產生的英數字所組成，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳符記之有效性後，才允許使用者進行重設密碼動作。					
4-3. 鑑別資訊回饋	4-3-1. 資通系統應遮蔽鑑別過程中之資訊。	【資安需求項目查檢】資通系統身分鑑別頁面 中，資料輸入欄位(如密碼等)應設定不以明文顯示方式，如以*取代真實輸入字元，以避免他人從旁窺視而盜取密碼。	V	V	V		
4-4. 加密模組鑑別	4-4-1. 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	【資安需求項目查檢】密碼不可以明文方式儲存，應經過加密或雜湊處理，使得系統管理者或是惡意入侵的攻擊者皆無法輕易取得使用者原始密碼，以降低密碼外洩風險。實務上，當使用者設定密碼時，應針對該帳號產生一個亂數值(Salt)，將密碼結合亂數值，再以雜湊函式處理產生雜湊值後，分別於不同欄位儲存亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。	V	V	V		
4-5. 非內部使用者之識別與鑑別	4-5-1. 資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	【資安需求項目查檢】資通系統若開放給外部使用者(含其他機關、委外開發與維護廠商、臨僱人員及一般民眾等)存取使用，應具備識別及鑑別之能力，如利用帳號、憑證或來源 IP 位址等方式，識別與鑑別使用者。	V	V	V		

5、系統與服務獲得

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
5-1. 系統發展生命週期需求階段	5-1-1. 針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	【資安需求項目查檢】使用此自評工具進行系統安全需求檢核。 需求階段的所有檢核項目都完成填答後，即可勾選此項。	V				
5-2. 系統發展生命週期設計階段	5-2-1. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	【資安需求項目查檢】可參照「安全軟體設計參考指引」之第 3 章安全軟體設計階段實務活動，包含「安全設計原則」，進行系統設計時應參考使用的設計原則；「執行攻擊面分析」，進行攻擊面的定義、識別與對應方式，包含如何進行攻擊面的衡量與評估，並進行管理等；「執行風險分析」，軟體設計過程中，如何透過使用威脅建模與架構風險分析，進行系統架構與威脅的分析，並使用通用性的安全設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連安全軟體設計的實務活動之後，應確保安全設計符合需求階段提出的相關安全需求。		V			
	5-2-2. 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	【資安需求項目查檢】系統發展生命週期需求階段發展之安全需求檢核項目，可能未能充分符合系統之所有安全需求，故應依據風險評估結果進行修正。 設計階段的所有檢核項目都完成填答後，即可勾選此 2 項。		V			
5-3. 系統發展生命	5-3-1. 應針對安全需求實作	【資安需求項目查檢】應於系統開發階段，針對安全需求實			V		

週期開發階段	必要控制措施。	作必要之控制措施，輔以檢核表方式進行確認，可減少遺漏之可能。 開發階段的所有檢核項目都完成填答後，即可勾選此項。					
	5-3-2. 應注意避免軟體常見漏洞及實作必要控制措施。	【資安需求項目查檢】軟體開發時應避免常見漏洞，如 OWASP TOP 10 或 CWE/SANS TOP 25 等，這些錯誤容易被惡意攻擊者利用，造成資料被竊取、竄改或使軟體無法運作，故需實作必要控制措施，以降低資安風險。			V		
	5-3-3. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	【資安需求項目查檢】系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯 示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的 try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的 finally 陳述，確保將該段功能程式碼所使用的資源正確釋放。			V		
5-4. 系統發展生命週期測試階段	5-4-1. 執行「弱點掃描」安全檢測。	【資安需求項目查檢】弱點掃描係利用自動化工具，對受測目標進行安全性掃描，以找出系統潛在弱點。				V	
5-5. 系統發展生命週期部署與維運階段	5-5-1. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服	【資安需求項目查檢】就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評估，正面表列需要開啟					V

	務及埠口。	該服務及埠口之理由，並關閉不必要之項目。					
	5-5-2. 資通系統相關軟體，不使用預設密碼。	【資安需求項目查檢】系統相關軟體元件或組態設定若有使用預設密碼，應於系統正式上線前變更完畢。					V
	5-5-3. 於系統發展生命週期之維運階段，應執行版本控制與變更管理。	【日常維運管理需求】在維運階段可能因需求變更、系統除錯、功能精進等原因而需要變更系統組態，而版本控制之目的，即在記錄系統組態在某段時間內的變更行為，使得使用者在需要時可取回特定的版本，嚴謹的版本控制(如 git、svn)與變更管理(如應用系統維護紀錄單)可強化系統的安全性與可用性。					V
5-6. 系統發展生命週期委外階段	5-6-1. 資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	【日常維運管理需求】機關委外開發資通系統時，可參考本文件之內容，並依據不同之安全等級(高、中、普)制定適用之安全需求，明確納入委外契約以做為驗收時之依據。	V				
5-7. 獲得程序	5-7-1. 開發、測試及正式作業環境應為區隔。	【日常維運管理需求】開發環境、測試環境與正式作業環境可區隔成不同的設備及網段，限制所能存取的應用程式及資料庫，以保護正式作業環境系統及資料。實務上，開發人員常以本機電腦為開發環境，並連結使用本機端之資料庫進行應用程式開發。俟開發完畢則將應用程式部署至測試主機，並連結至測試用資料庫，供測試人員進行測試使用。俟測試			V	V	V

		完畢，再將應用程式部署至正式環境，並連結至正式資料庫提供上線服務。					
5-8. 系統文件	5-8-1. 應儲存與管理系統發展生命週期之相關文件。	【日常維運管理需求】系統發展生命週期之相關文件如系統需求書、系統規格書、系統發展計畫、系統測試計畫及測試報告等，應書面或電子化形式進行文件保存，並被納入管理程序。 各階段的所有檢核項目都完成填答後，即可勾選該階段此項。	V	V	V	V	V

6、系統與資訊完整性

措施	檢核項目	實施方式參考建議	需求階段	設計階段	開發階段	測試階段	部署階段
7-1. 漏洞修復	7-1-1. 系統之漏洞修復應測試有效性及潛在影響，並定期更新。	【資安需求項目查檢】針對系統所使用的外部元件與軟體進行表列，包含其版本資訊，定期關注元件版本更新訊息及安全漏洞通告，若有相關之安全漏洞，評估系統元件更新之必要性，並於系統測試環境進行更新測試驗證後，才於正式環境進行更新。					V
	7-1-2. 定期確認資通系統相關漏洞修復之狀態。	【日常維運管理需求】注意相關之安全漏洞訊息(透過 CVE 相關訊息網站、廠商安全通告等)，若發現採用之軟體或元件具有安全漏洞，應設法修復漏洞並定期追蹤修復之狀態。					V
7-2. 資通系統監控	7-2-1. 發現資通系統有被入侵跡象時，應通報機關特定人員。	【日常維運管理需求】應指派人員負責處理資通系統入侵攻擊相關資安事件，並於發現資通系統有被入侵跡象時，通報相關人員進行處理。					V
	7-2-2. 監控資通系統，以偵	【日常維運管理需求】機關應具備監控資通系統之能力，如					V

	測攻擊與未授權之連線，並識別資通系統之未授權使用。	指派專業人員或使用監控設備，用以偵測資通系統連線行為，當發現未授權之連線或存取行為應向系統維護人員提出告警。					
7-3. 軟體及資訊完整性	7-3-1. 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	【資安需求項目查檢】提供完整性驗證工具以驗證軟體或資訊在儲存或傳輸過程中未被人惡意竄改，如網站可在檔案下載連結處，提供以安全雜湊演算法產生之雜湊值，並說明使用的雜湊演算法為何，供使用者取得資料後自行計算雜湊值進行比對。另外，為確保系統程式之完整性，可對系統程式檔案留存雜湊值，並進行監控比對，以偵測未授權之惡意變更。	V	V	V		V
	7-3-2. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。	【資安需求項目查檢】對於使用者輸入欄位資料應檢查是否符合預期之邏輯規則，實務上以正規表示式(Regular Expression)驗證內容之合法性。檢查機制若於客戶端實作，容易被使用者繞過檢查機制，故應於應用系統伺服器端實作始視為有效。 如採用 Prepared statements, Stored procedures,Input Validation 等措施防範 SQL Injection 攻擊；如採用黑名單過濾跳脫特殊字元、白名單正規表示式驗證、輸出編碼等措施防範 XSS 跨站腳本攻擊；網站若提供頁重導(Redirects)或導向(Forwards)之功能，必須確認使用者輸入欲重導向的網頁在合法白名單內，以避免重導向至惡意網頁。	V	V	V		V

	7-3-3. 發現違反完整性時，資通系統應實施機關指定之安全保護措施。	【日常維運管理需求】機關應訂定相關安全保護措施，在發現資通系統完整性遭到破壞時採取適當之行動。如當發現資料庫或檔案被不當竄改、站台被植入惡意指令碼或元件等資安事件時，應通知系統管理者進行緊急應變處置，並依規定之通報流程進行資安事件通報作業。					V

二、資通系統防護基準控制措施

(1)存取控制

措施內容	控制措施	控制措施設計
帳號管理	一、建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、資通系統閒置帳號應禁用。 四、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	一、帳號管理機制 1. 申請：依機關現行辦法申請之。 2. 建立：由「系統管理者」權限建立帳號；預設密碼為 12 碼大小寫英數混合亂數。 3. 修改：「系統管理者」權限可修改所有帳號；其他權限可修改個人帳號。 4. 啟用：限「系統管理者」可啟用帳號。 5. 停用：限「系統管理者」可停用帳號。 6. 刪除：限「系統管理者」可刪除帳號。 二、上述帳號管理機制從帳號建立、修改、啟用、停用至刪除等程序皆記錄於「系統操作記錄」，供未來稽核。 三、已逾期之帳號無法使用。 四、每月檢查閒置帳號。 五、每年檢視帳號管理之設計功能。
最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。	以「角色管理」功能，詳細指定各角色於各子功能可「讀取」與「寫入」之權限。 角色中無設定之功能，不具該功能存取權限。
遠端存取	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用	一、授權管理 1. 通過帳號驗證之使用者，依系統設定組態，配發一式「角色權限」，限制於該角

措施內容	控制措施	控制措施設計
	限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後臺之連線。 四、應採用加密機制。 五、遠端存取之來源應為機關已預先定義及管理之存取控制點。	色之存取權限。 2. 使用連線限於為 HTTPS (TLS 1.2)。 3. 角色權限之組態設定規範於《系統需求規格書》 二、使用者權限檢查作業於伺服器端完成。 三、系統後台連線記錄於 IIS 日誌。 四、加密機制採 TLS 1.2。

(2)事件日誌與可歸責性

措施內容	控制措施	控制措施設計
記錄事件	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。 四、應定期審查機關所保留資通系統產生之日誌。	一、應用系統日誌保留二年。 二、應用系統記錄以下事件： 1. 使用者帳號相關各式事件，含帳號登入、登出、建立、修改、啟用、停用、刪除。 2. 案件管理相關事件，含分派、處理、結案等修改記錄。 3. 報表匯出、圖表下載。 三、「系統管理者」權限之所有功能執行。 四、配合機關定期審查機關所保留資通系統產生之日誌。
日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	應用系統日誌格式如下： 1. 事件類型：INFO、WARN、ERROR 2. 發生時間：yyyy-MM-dd HH:mm:ss 3. 發生位置：IP 4. 登入角色 5. 登入帳號 6. 事件內容
日誌儲存容量	依據日誌儲存需求，配置所需之	日誌每日預估產生量不超過 1MB，

措施內容	控制措施	控制措施設計
	儲存容量。	儲存一年期間需要容量不超過 1GB。
日誌處理失效之回應	資通系統於日誌處理失效時，應採取適當之行動。	應用系統日誌處理失效時，寄發電子件通知系統管理者。
時戳及校時	一、資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 二、系統內部時鐘應定期與基準時間源進行同步。	1. 應用系統日誌時戳使用作業內部時鐘。 2. 應用系統日誌時間採 UTC+08:00 時間。 3. 應用系統自動與機關指定時間伺服器同步系統時間。
日誌資訊之保護	一、對日誌之存取管理，僅限於有權限之使用者。 二、應運用雜湊或其他適當方式之完整性確保機制。	應用系統日誌存取僅限作業系統之系統管理者與 IIS_USER。 每日產生之日誌檔，以 SHA256 計算雜湊值並儲存於檔案與資料庫。

(3)營運持續計畫

措施內容	控制措施	控制措施設計
系統備份	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。 三、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	一、系統可容忍資料損失之時間要求訂定為「24 小時」。以每 24 小時為頻率進行資料備份。 二、系統源碼於每次上版(含測試機與正式機)時上傳至「D:\upload」並以日期區分。 三、系統執行檔於每次上版(含測試機與正式機)時備份於「D:\backup」並以日期區分。 四、資料庫以「工作排程器」於每日 08:00PM 進行備份，資料庫檔案備份於「D:\dbbackup」；資料保留期限為 30 天。 五、每季於測試機匯入備份檔以驗證其正確性。
系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。	一、中斷後至重新恢復服務之可容忍時間訂為 4 小時。 二、系統服務以「測試機」作為備援。

(4)識別與鑑別

措施內容	控制措施	控制措施設計
內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	一、作業系統各使用者使用獨立帳號。 二、應用系統各使用者使用獨立帳號。
身分驗證管理	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。 七、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 八、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	一、使用預設密碼登入系統時，於登入後要求立即變更。 二、長度限 12 碼以上、需至少含數字、大寫與小寫英文。 三、網站系統所有資料以 HTTPS 傳輸。 四、密碼最長效期為 3 個月，超過效期強制更新。 五、密碼最短效期為 1 日，密碼於 1 日內不得重設。 六、密碼不得與前 3 次相同。 七、身分驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入。 八、身分驗證失敗達三次後，以「WARN」等級記錄於日誌。 九、系統內建 Google reCAPTCAH v2 (或 v3)防範自動化程式之登入。 十、以 TOKEN 機制重設密碼，效期預設為 1 小時。
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	輸入密碼或其他代替密碼之通行碼時，以顯示「·」號方式遮蔽。
加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	密碼以 SHA256 儲存於資料庫。
非內部使用者	資通系統應識別及鑑別非機關	應用系統以「機關外部權限」角色區分

措施內容	控制措施	控制措施設計
之識別與鑑別	使用者(或代表機關使用者行為之程序)。	使用者。

(5)系統與服務獲得

措施內容	控制措施	控制措施設計
系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認。	由機關之評估為確認基準。
系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	依 ISO 27001:2013 風險分析、評估與鑑另之程序，提出檢核項目與安全需求修正。
系統發展生命週期開發階段	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	一、開發避免 OWASP TOP 10 弱點。 二、錯誤訊息改呈現 HTTP 404 Not Found。
系統發展生命週期測試階段	執行「弱點掃描」安全檢測。	配合機關之網頁弱點掃描，修正弱點。
系統發展生命週期部署與維運階段	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統不使用預設密碼。 三、於系統發展生命週期之維運階段，應執行版本控制與變更管理。	一、作業系統定期執行 Windows Updates。 二、只開放 Port 443 與作業連線所需埠口並留存記錄。 三、更新作業系統與資料庫預設密碼並留存記錄。 四、以 Git Engine 作為程式版本控管機制。
系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	配合機關辦理。
獲得程序	開發、測試及正式作業環境應	本公司作業區分為「開發」與「測試」

措施內容	控制措施	控制措施設計
	為區隔。	環境」。 機關系統區分為「測試」及「正式」環境。
系統文件	應儲存與管理系統發展生命週期之相關文件。	交付並保存以下文件： 1. 系統需求規格書 2. 測試報告 3. 各項教育訓練教材 4. 使用者操作手冊 5. 系統管理操作手冊

(6)系統與資訊完整性

措施內容	控制措施	控制措施設計
漏洞修復	一、系統之漏洞修復應測試有效性及潛在影響，並定期更新。 二、定期確認資通系統相關漏洞修復之狀態。	一、執行定期弱點掃描之漏洞修復。 二、於測試機驗證弱點修復不影響正式運作中的系統，並留有測試紀錄；經機關查驗後於正式機上版。 三、每季認資通系統相關漏洞修復之狀態。
資通系統監控	一、發現資通系統有被入侵跡象時，應通報機關特定人員。 二、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用 。	系統出現以下情事通報機關人員： 一、應用系統有出現非正式運作之檔案。 二、異常登入記錄。 三、備份或日誌檔之目錄或檔案有異常。 四、其他異常入侵跡象。 以四層雙向技術以及登入模組、權限模組，偵測與記錄攻擊與未授權之連線與使用。
軟體及資訊完整性	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊 。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	一、系統檔案以雜湊計算值記錄系統程式狀態，並每日自動偵測是否被竄改。 二、應用系統每則輸入欄位皆具有資料驗證規則。 三、發現違反完整性時，依機關指定之安全保護措施進行處置或通報。