

資訊安全期末報告

2024/06/18

「賣貨便假客服」網頁開發專案  
專案規劃書

S10959007 資工四 彭姿穎

S10959042 資工四 周巧晴

中華民國一一三年六月

## 目錄

|                      |    |
|----------------------|----|
| 圖目錄.....             | 3  |
| 壹、 專案背景與介紹.....      | 6  |
| 一、 專案的背景與動機.....     | 6  |
| 二、 原先詐騙手法.....       | 6  |
| 三、 目標與目的.....        | 6  |
| 貳、 需求分析.....         | 7  |
| 一、 使用者需求.....        | 7  |
| 二、 功能性需求與非功能性需求..... | 7  |
| 三、 使用流程.....         | 8  |
| 參、 系統設計.....         | 9  |
| 一、 前端程式設計.....       | 9  |
| 二、 後端資料庫程式設計.....    | 9  |
| 三、 使用的技術與工具.....     | 10 |
| 四、 使用者介面設計.....      | 11 |
| 肆、 成果與效能評估.....      | 14 |
| 一、 專案成果的展示與功能演示..... | 14 |
| 伍、 未來展望.....         | 20 |
| 一、 系統功能擴展.....       | 20 |

## 圖目錄

|   |    |
|---|----|
| 圖 1 密碼和鹽值 .....                                 | 7  |
| 圖 2 JSON Web Token .....                        | 7  |
| 圖 3 聊天室 id .....                                | 8  |
| 圖 4 render 可設置環境變數 .....                        | 10 |
| 圖 5 render 代理 postgresSQL.....                  | 10 |
| 圖 6 假賣貨便官網.....                                 | 11 |
| 圖 7 賣貨便假客服聊天室網頁-整體.....                         | 11 |
| 圖 8 賣貨便假客服聊天室網頁-點擊查看截圖方法 .....                  | 12 |
| 圖 9 賣貨便假客服聊天室網頁-切換成語音並點擊表情選擇.....               | 12 |
| 圖 10 賣貨便假客服聊天室網頁-點擊圖片 .....                     | 12 |
| 圖 11 賣貨便假客服登入網頁 .....                           | 13 |
| 圖 12 賣貨便假客服轉接客服網頁 .....                         | 13 |
| 圖 13 賣貨便假客服轉接客服網頁-已被轉接客戶 .....                  | 13 |
| 圖 14 賣貨便假客服轉接客服網頁-未被轉接客戶 .....                  | 13 |
| 圖 15 賣貨便假官網 .....                               | 14 |
| 圖 16 賣貨便假客服聊天室_客戶端 .....                        | 14 |
| 圖 17 賣貨便假客服聊天室_客服端 .....                        | 14 |
| 圖 18 賣貨便假官網.....                                | 15 |
| 圖 19 3 秒後跳轉賣貨便假客服聊天室 .....                      | 15 |
| 圖 20 客服進入賣貨便假客服登入網頁 .....                       | 16 |
| 圖 21 客服進入賣貨便假客服轉接客服網頁，客戶傳送第一則訊息後，會新增一個聊天室 ..... | 16 |
| 圖 22 鼠標移至客戶圖示有「轉接客服」按鈕.....                     | 16 |
| 圖 23 點擊按鈕後跳轉賣貨便假客服聊天室頁面，並可以觀看該聊天室先前的訊息 .....    | 16 |
| 圖 24 賣貨便假客服轉接客服網頁，更新為「回到客服」、「刪除」兩個按鈕 .....      | 16 |
| 圖 25 當該客戶已被轉接，則其他客服無法看到該客戶 .....                | 17 |
| 圖 26 選擇表情符號.....                                | 18 |
| 圖 27 表情符號會以[code]格式插入輸入框 .....                  | 18 |
| 圖 28 可傳送圖片 .....                                | 18 |
| 圖 29 點擊圖片可顯示全圖 .....                            | 18 |
| 圖 30 可同時傳送文字、表情符號 .....                         | 18 |
| 圖 31 可傳送檔案.....                                 | 18 |
| 圖 32 點擊發送按鈕右邊的^可以切換成語音 .....                    | 18 |
| 圖 33 需允許麥克風使用權限 .....                           | 18 |

|   |    |
|---|----|
| 圖 34 點擊紅色錄音按鈕開始錄音 .....                 | 18 |
| 圖 35 點擊綠色錄音按鈕結束錄音並傳送語音訊息 .....          | 18 |
| 圖 36 點擊即可下載檔案 .....                     | 18 |
| 圖 37 可播放語音訊息 .....                      | 18 |
| 圖 38 點擊截圖的圖示會出現「在輸入文字框中貼上圖片」 .....      | 18 |
| 圖 39 截圖後貼上即傳送截圖 .....                   | 18 |
| 圖 40 點擊常見問題/常見問題回覆選項，文字將會複製到文字輸入欄 ..... | 18 |

## 表目錄

|                |   |
|----------------|---|
| 表 1 客服 .....   | 9 |
| 表 2 聊天室 .....  | 9 |
| 表 3 聊天內容 ..... | 9 |

## 壹、 專案背景與介紹

### 一、 專案的背景與動機

本專案的背景與動機為因有在 Facebook 社團做交易買賣，而最常使用到的交易平台即為「賣貨便」、「交貨便」，且時常在社團內看到許多社員發文遇到諸如此類的詐騙手法，警惕其他社員注意這些使用者以及相似的詐騙手法。因此想透過這個機會實作、仿作看看這個賣貨便詐騙的詐騙網站。

### 二、 原先詐騙手法

1. 賣家上架商品至臉書社團
2. 詐騙私訊購買，並使用賣貨便平台交易
3. 詐騙聲稱賣家須辦理「三大保障」協議以認證金流，傳送詐騙網站網址，要求賣家與假的 7-ELEVEN 客服聯繫
4. 賣家上當，並提供給假客服自己的個資及銀行帳號
5. 假客服告知會以電話聯繫、操作相關手續
6. 轉帳介面中，假客服要求賣家在帳號輸入身分證數字部分，在金額輸入驗證碼並轉帳。
7. 確認目前餘額都沒有變，讓賣家卸下心防，但只是因為不存在該帳戶而轉帳失敗而已。
8. 第一次受騙時，假客服要求賣家輸入另一個帳戶(說是系統隨機產生)在驗證碼(金額的地方)輸入金額簽署成功(交易直接完成)錢直接轉出去
9. 第二次受騙時，假客服表示誤觸轉帳，自己無權限更改，需連絡主管復原，主管積極處(詐)理(騙)，以相同方式再次詐取更高的金額。
10. 後續即使報警凍結詐騙帳戶，錢也難以拿回。

### 三、 目標與目的

目標：

1. 仿作真正賣貨便官網之網頁介面
2. 實作跳轉至賣貨便假客服聊天室
3. 賣貨便假客服聊天室介面

目的：

為了解其網站背後所運用到的程式，實作並優化、增加其真實性。

## 貳、需求分析

### 一、使用者需求

1. 快速提問和回覆：客服端希望能夠快速回覆客戶的疑問以增加工作效率，騙更多錢；客戶端希望能夠快速詢問關於原先詐騙所述之無法下單的問題。因此我們新增常見問題和常見問題回覆等功能，提供使用者能快速詢問和回覆相關問題。
2. 人性化交流：客服和客戶期望互動的過程中，感受到人性化和個性化的對待，而非機器人般的冷淡回覆。  
因此我們保留原賣貨便詐騙網站之功能，諸如傳送表情、文字、檔案、圖片、截圖等功能，並新增傳送語音訊息的功能。

### 二、功能性需求與非功能性需求

1. 功能性需求：
  - I. 即時聊天功能：提供客服與客戶即時互動的能力，聊天室網頁須能即時更新最新內容。
  - II. 無須立即回覆：在無法立即轉接客服或客戶臨時有事時，能夠保留聊天室一段時間，讓客服和客戶能回來該聊天室。
2. 非功能性需求：
  - I. 安全性：保護客服的資料，客服的密碼用 sha256 結合 16 字節鹽值加密驗證(避免明文儲存)，登入成功後將利用客服 id 生成 9 小時有效的 JSON Web Token 供客服端儲存在 sessionStorage，在會話期間可以不必重複登入，而每當客服要進行操作時，都會對該 JSON Web Token 進行驗證，以降低未經授權登入或操作的機會。

|   | 客服id<br>[PK] text | 密碼<br>character   | 鹽值<br>character varying (32)      |
|---|-------------------|---|-----------------------------------|
| 1 | s10959001         | f9421d49051e35083117d3041f3505f2672b3f8a731e406b88444d5ea4bf99... | df384116c510343870ef0a47b8944f7e  |
| 2 | s10959003         | 4daf9fdd97e189a97655559f3400d75a3b6157c577d3a8ea2597089cb9a3...   | fcf2994ef8548060d3b35e6b1ce7c8d   |
| 3 | s10959006         | 2a15b294f50562c8a00870ac6db351e89af20b2779ecff9cf99ecbbd7a1f673e  | 2ba8ee880e8c86edf9112e3b0c85feb   |
| 4 | s10959007         | d6614ec76677777c21d543a40959649cd9be1f5bcb23c3097787782479a6...   | 5f1820868fas23c74050c70d6cb91731  |
| 5 | s10959008         | c3b4fb86e70deb969a79c561a111420ef4505215c598a2cc51996553269c1...  | 6340955cd071610208514eab30ddcf    |
| 6 | s10959009         | 314cb438ec6757dadfbc28218629e6b5a5fe119d8d3798fb1555c5cf21378...  | d0386cbb71d5b9e69f1259926d1d2773  |
| 7 | s10959016         | 54ec22b33439b7f599eb365de7d16fa367b1c1ea94b1c7c85a5d37d519d79...  | 7425d44ef715c7268dfe15afcf631c    |
| 8 | s10959028         | c63c0f4d8d57519273876f0db437907e5b455091d56a4f6d6a33e04e141d4f... | 016bd0d4c8401ac91e7aac7296ef619d4 |
| 9 | s10959030         | a5bb4fd242e8115139cc8fe5c0b5f556c95b8839b009fa2bb2e3c035ba5e60... | 14097d9a624244f17e8586667108fa98  |

圖 1 密碼和鹽值

| 應用程式            | URL  |
|-----------------|--|
| Service workers | https://myship-7-11.onrender.com             |
| 儲存空間            | 來源 https://myship-7-11.onrender.com          |
| 本地儲存空間          | 金鑰 userId 值 eyJhbGciOiJIUzI1NiIsInR5cCI6I... |
| IndexedDB       |  |
| Cookie          |  |
| 私密狀態欄紋          |  |
| 興趣群組            |  |
| 共用儲存空間          |  |
| 存取儲存空間          |  |

圖 2 JSON Web Token

| 名稱          | 值               | D.   | Path | Expi... | 大小 | H... | S... | P... |
|-------------|-----------------|------|------|---------|----|------|------|------|
| _ga         | GA1.1.155347... | /    | /    | 202...  | 30 |      |      | M... |
| _ga_JHHQ... | GS1.1.171858... | /    | /    | 202...  | 52 |      |      | M... |
| userid      | fc5d0af3-532... | m... | /    | 202...  | 42 |      |      | M... |

圖 3 聊天室 id

客戶則是會被分配通用唯一識別碼 uuid 作為聊天室 id，並存在 cookie 中，維持 24 小時(通常能詐騙到都是短時間內)。

- II. 可靠性：系統應具有高可用性，減少系統停機和服務中斷時間。我們將伺服器架設在 render 上，一旦伺服器掛掉，就會馬上重新啟動並且寄信提醒我們，因此可用性很高。
- III. 易用性：界面設計應該直觀和易於導航，以提升使用者體驗。我們運用了大量圖示以讓使用者能一眼找到他們需要的功能。

### 三、 使用流程

1. 客戶進入假賣貨便官網，3 秒後跳轉到賣貨便假客服聊天室，啟動即時客服功能，假客服系統自動詢問使用者有何需求。
2. 客戶傳送第一則訊息後建立聊天室，假客服即可轉接客服。
3. 根據客戶的回應，假客服提供適當的導引，並騙取存款。



## 參、系統設計

### 一、前端程式設計

提供給使用者的網頁介面，包括客戶所需的假賣貨便官網和聊天室；客服所需的登入介面、轉接客服介面和聊天室介面。

### 二、後端資料庫程式設計

使用 Node.js 中的 Express 框架來架設 server，並用 WebSocket 監聽 port 中的 endpoint(端點)來接收、傳遞訊息，負責業務邏輯處理和資料交互，實現即時通知前端更新現有聊天室、聊天內容、客戶狀態等功能。使用 PostgreSQL 建構資料庫儲存假客服和賣家的對話紀錄。

資料庫的表如下，其中底線代表 primary key，斜線代表 foreign key：

表 1 客服

| <u>客服 ID</u> | 密碼 | 鹽值 |
|--------------|----|----|
|--------------|----|----|

表 2 聊天室

| <u>聊天室 ID</u> | 客服 ID |
|---------------|-------|
|---------------|-------|

表 3 聊天內容

| <u>聊天內容 ID</u> | 聊天室 ID | 訊息種類 ID | 訊息 |
|----------------|--------|---------|----|
|----------------|--------|---------|----|

訊息種類：

#### 0. 文字和表情

訊息會是純文字，表情會以"[表情代號]"表示，並找到`1f\${表情代號}.png`檔案呈現

#### 1. 圖片

訊息會以檔名表示

#### 2. 檔案

訊息會以檔名表示

#### 3. 音檔

訊息會以檔名表示

Github repository 中有三個資料夾專門存放使用者傳送的檔案(file)、圖片(img)、音檔(record)。

當有聊天室傳送任何檔案，將會在 file 中以聊天室 id 為名的資料夾(沒有的話會新建)，並存放在裡面，其中檔名與使用者提供時檔名相同；當有聊天室傳送任何圖片，將會在 img 中以聊天室 id 為名的資料夾(沒有的話會新建)，並存放在裡面，其中檔名會是`\${當下時間}.\${傳送檔案副檔名}`；當有聊天室傳送任何檔案，將會在 record 中以聊天室 id 為名的資料夾(沒有的話會新建)，並存放在裡面，其中檔名會是`\${當下時間}.opus`。

### 三、 使用的技術與工具

技術與工具：

1. 伺服器：node.js、express、websocket
2. 前端：websocket 連伺服器
3. 資料庫：postgresql、github repository

架設方式：

1. 建立一個 github repository，用 git 將寫好的程式碼 push 上去。
2. 用 render 代理 postgresql 資料庫以及連結 github repository，deploy server 的 node.js 檔案，之前設計的資料庫那些資料會存到代理資料庫中。

因為 git 不允許 push 含有敏感資訊的檔案到 github repository，因此可以利用 render 設置環境變數代替。

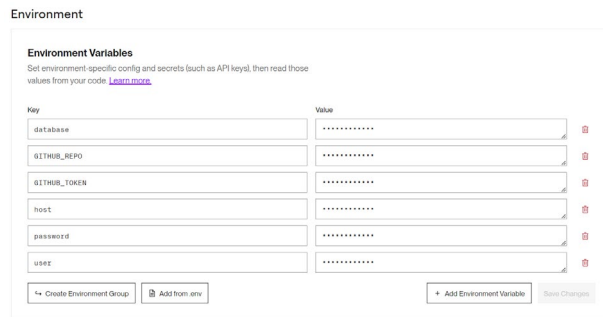


圖 4 render 可設置環境變數

Render 自動產生的 hostname 和密碼等等複雜度相當高，因此安全性不錯。

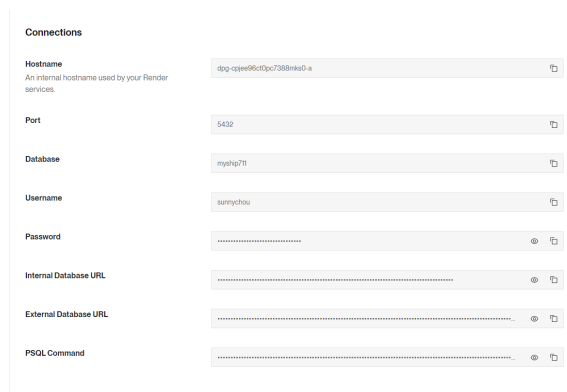


圖 5 render 代理 postgresql

3. 使用者上傳的檔案會用 personal access token push 到 github 中，並要呈現時用 github raw 連結呈現，提供使用者下載或直接觀看。

#### 四、使用者介面設計

##### 1. 假賣貨便官網(<https://myship-7-11.onrender.com/Home/Main>)



圖 6 假賣貨便官網

如上，仿冒賣貨便官網，過3秒跳轉賣貨便假客服網頁。但除了圖片展示外，無其他功能，以避免客戶不小心點到其他東西，導到其他網頁，沒有直接前往賣貨便假客服網頁，而減少被騙可能。

此外，網頁上圖片沒有顯示出來是因為3秒有時不足以將所有圖片載入。

##### 2. 賣貨便假客服聊天室網頁

(客服端：<https://myship-7-11.onrender.com/chat.html>)

客戶端：<https://myship-7-11.onrender.com>)



圖 7 賣貨便假客服聊天室網頁-整體



圖 8 賣貨便假客服聊天室網頁-點擊查看截圖方法



圖 9 賣貨便假客服聊天室網頁-切換成語音並點擊表情選擇



圖 10 賣貨便假客服聊天室網頁-點擊圖片

### 3. 賣貨便假客服登入網頁(<https://myship-7-11.onrender.com/cslogin.html>)



圖 11 賣貨便假客服登入網頁

### 4. 賣貨便假客服登入(<https://myship-7-11.onrender.com/transfer.html>)



圖 12 賣貨便假客服轉接客服網頁

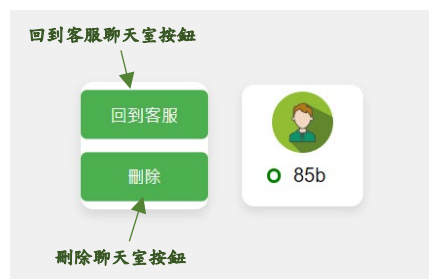


圖 13 賣貨便假客服轉接客服網頁-已被轉接客戶



圖 14 賣貨便假客服轉接客服網頁-未被轉接客戶

## 肆、 成果與效能評估

### 一、 專案成果的展示與功能演示

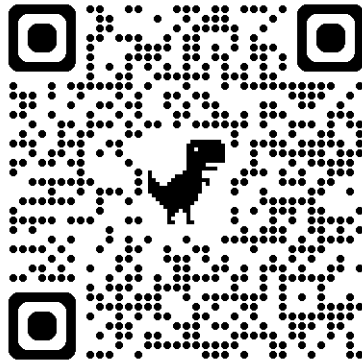


圖 15 賣貨便假官網

<https://myship-7-11.onrender.com/Home/Main>

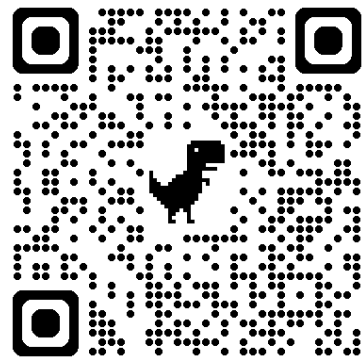


圖 16 賣貨便假客服聊天室\_客戶端

<https://myship-7-11.onrender.com>



圖 17 賣貨便假客服聊天室\_客服端

<https://myship-7-11.onrender.com/cslogin.html>

## 1. 客戶端

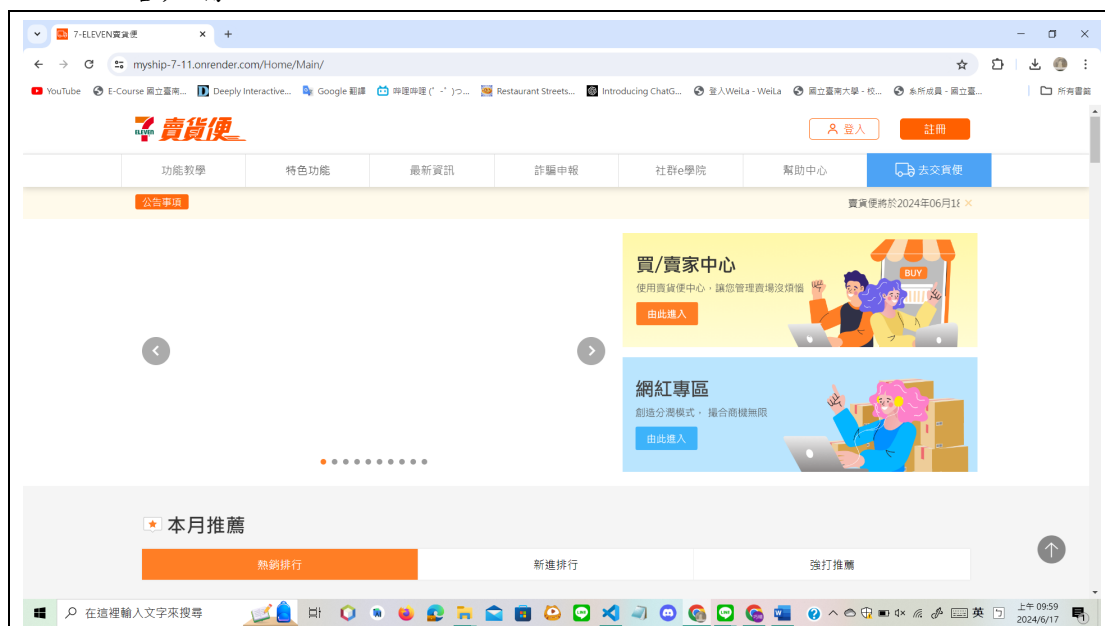


圖 18 賣貨便假官網



圖 19 3 秒後跳轉賣貨便假客服聊天室

首先會先進入賣貨便假官網，3 秒後跳轉至賣貨便假客服聊天室

## 2. 客服端

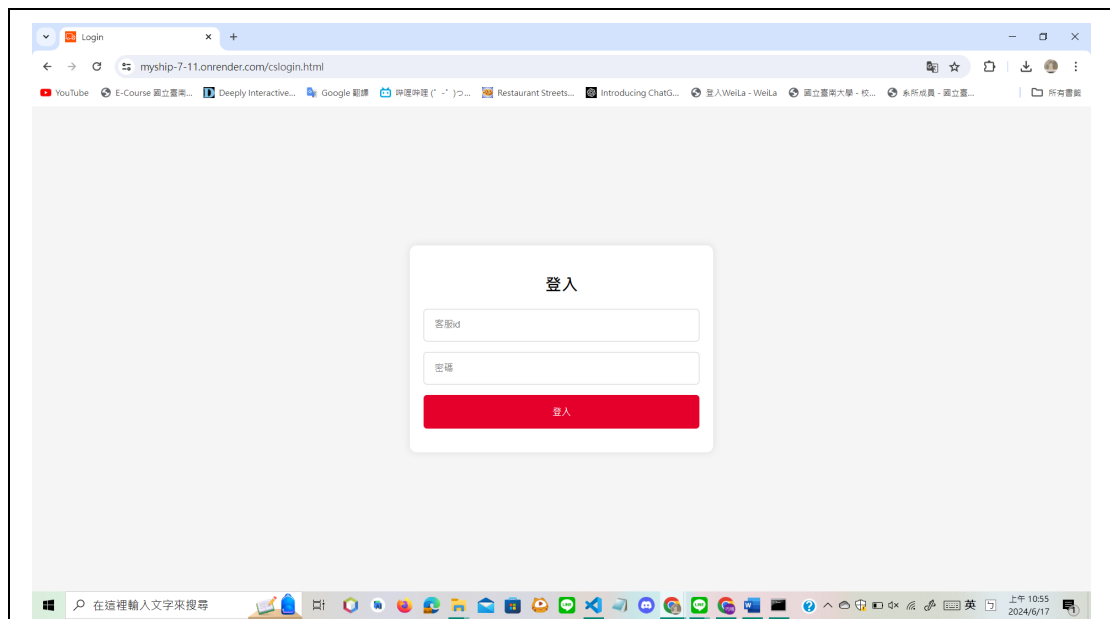


圖 20 客服進入賣貨便假客服登入網頁

客服端會先進入此畫面登入

帳號：s10959007、s10959042

密碼：0429、0526

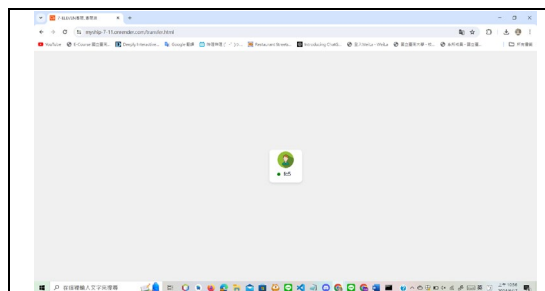


圖 21 客服進入賣貨便假客服轉接客服網頁，客戶傳送第一則訊息後，會新增一個聊天室

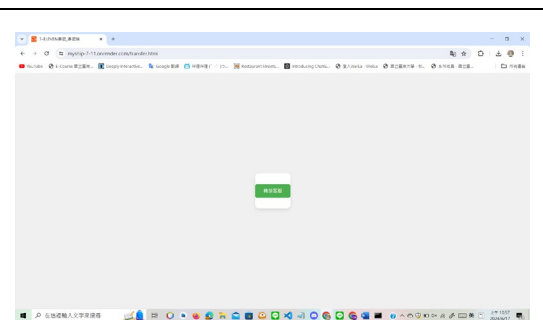


圖 22 鼠標移至客戶圖示有「轉接客服」按鈕

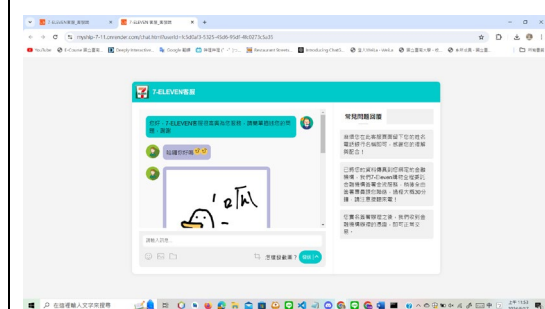


圖 23 點擊按鈕後跳轉賣貨便假客服聊天室頁面，並可觀看該聊天室先前的訊息

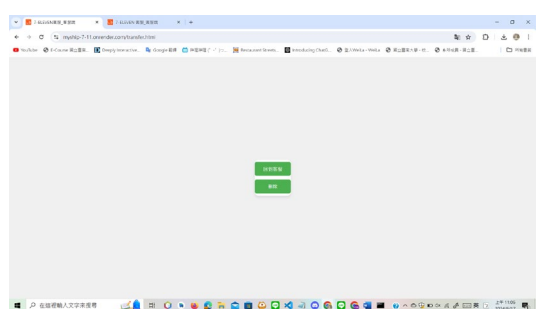


圖 24 賣貨便假客服轉接客服網頁，更新為「回到客服」、「刪除」兩個按鈕



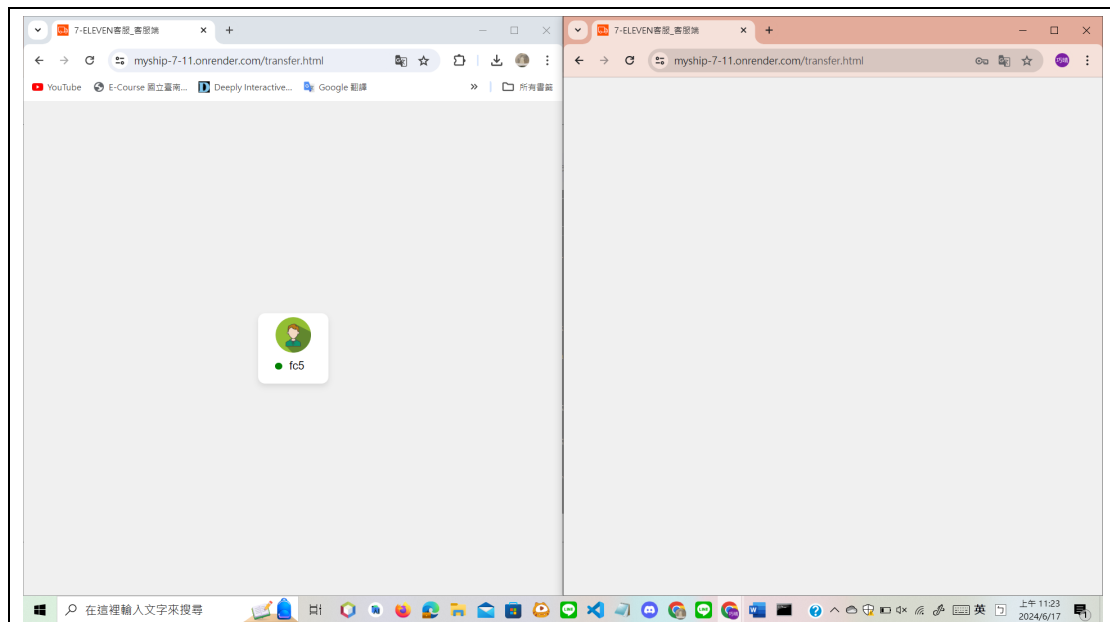





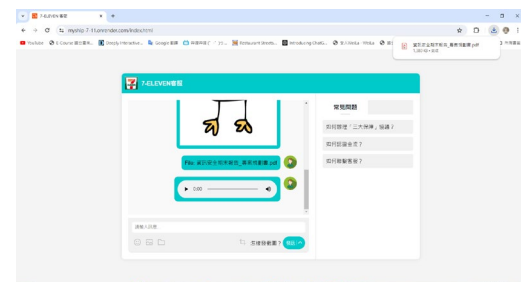

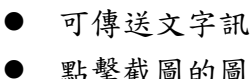


圖 25 當該客戶已被轉接，則其他客服無法看到該客戶

- 當客戶傳遞第一則訊息則客戶向客服則新建立一個聊天室
- 客服端即可點擊「轉接客服」
- 跳轉新分頁正式進入聊天室擔任客服角色回覆客戶訊息
- 客服可傳遞文字訊息、語音訊息、表情符號、圖片、檔案
- 客服端介面會將該客戶更新成「回到客服」、「刪除」兩個按鈕，點擊前者即可跳轉至客服聊天室回覆頁面，點擊後者則可直接刪除此聊天室

### 3. 聊天室功能

|   |   |  |
|---|---|--|
|    |  |  |
| 圖 26 選擇表情符號   | 圖 27 表情符號會以[code]格式插入輸入框  | 圖 28 可傳送圖片   |
|    | 圖 29 點擊圖片可顯示全圖  |  |
| 圖 30 可同時傳送文字、表情符號   |   |  |
|   | 圖 31 可傳送檔案  |  |
|   |   |  |
|  | 圖 32 點擊發送按鈕右邊的^可以切換成語音  | 圖 33 需允許麥克風使用權限  |
| 圖 34 點擊紅色錄音按鈕開始錄音   | 圖 35 點擊綠色錄音按鈕結束錄音並傳送語音訊息  |  |
|   |   |  |
|  | 圖 36 點擊即可下載檔案   |  |
| 圖 37 可播放語音訊息  |   |  |
|   |   |  |
|  | 圖 38 點擊截圖的圖示會出現「在輸入文字框中貼上圖片」  |  |
| 圖 39 截圖後貼上即傳送截圖   |   |  |
|   |   |  |
|  | 圖 40 點擊常見問題/常見問題回覆選項，文字將會複製到文字輸入欄   |  |
|   |   |  |

- 可傳送文字訊息、語音訊息、表情符號、圖片、檔案
- 點擊截圖的圖示會出現「在輸入文字框中貼上圖片」，截圖後貼上即傳

- 可傳送文字訊息、語音訊息、表情符號、圖片、檔案
- 點擊截圖的圖示會出現「在輸入文字框中貼上圖片」，截圖後貼上即傳

送截圖

- 右側有常見問題/常見問題回覆，點擊選項，文字將會複製到文字輸入欄，點擊發送才會傳送文字給對方

## 伍、 未來展望

### 一、 系統功能擴展

1. 多語言支援：引入多語言功能，支援更多國家的用戶，擴展國際市場。
2. 自動回覆：當客戶傳送訊息後，並不是隨時客服都在線，故提供自動回覆，或者在客戶傳送常見問題時，客服能即時傳送對應回覆訊息。
3. 截圖功能：真正實現及時部分畫面螢幕擷取功能。
4. 引進 AI 智能回覆：不須人工一個一個回覆。