COVID-19居家隔離自動視訊人臉辨識管理(Home Quarantine Management)

前言：

Covid-19疫情日趨嚴重,居家檢疫人數倍增,目前疾管局採用”手機定位監控”,確實是非常方便準確的方法,但缺點是無法確認本人是否真的居家? 所以需要地方區里長協助電話訪談,這部分若能利用視訊人臉辨識自動化方式,可以大幅節省人力資源,如遇特殊情況再由人工介入輔助。

本計畫特色：

1.平台支援webrtc技術,目前主流瀏覽器皆已內建webrtc視訊核心,用戶端無須安裝軟體,透過簡訊或Line傳送視訊URL,即可帶起瀏覽器視訊功能.

2.系統可自動與居家用戶視訊互動, 完成管理功能, 用戶如有看診需要亦可轉為視訊診療.

3.平台全程錄影存證,以備發生爭議時,供調閱查證.

4.結合Microsoft 雲端人臉辨識,作為身分認證輔佐功能.

5.結合Google 影像文字辨識,作為證件資料輸入輔佐功能.

6.結合Google 語音辨識,作為居家地址輸入輔佐功能.

7.結合Google GPS定位,可偵測居家用戶目前所在地理位置.

以上簡介所有功能都可以實際測試, demo網址: https://rtc.tw/HQ.html

目錄：

前威有限公司 http://rtc.tw　　林志成 0928260333 lin260333@gmail.com

居家檢疫視訊管理名單建立

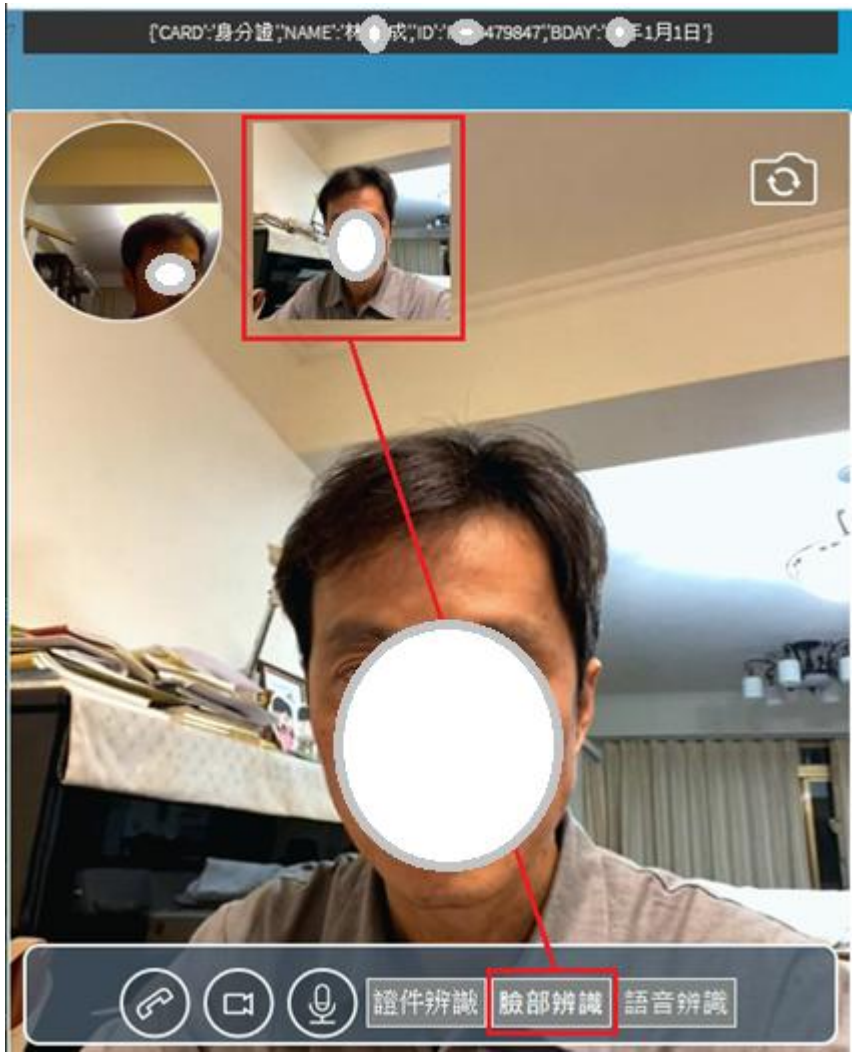
1. 工作人員透過瀏覽器(chrome)連上https://rtc.tw/HQ.html, 輸入自己的手機09yyyyyyyy
   以及居家用戶手機09xxxxxxxx
   =>系統送出視訊簡訊URL=>工作人員進入視訊畫面,等待居家用戶連上.
2. 居家用戶手機會立即收到簡訊URL,內容:
   "疾管局居家檢疫視訊邀請 https://rtc.tw/HQuser.html?roomkey=09xxxxxxxx&agent=09yyyyyyyy"
   用戶按下該簡訊連結=>進入視訊畫面,與工作人員開始進行視訊.

居家檢疫視訊管理名單建立(1-證件資料)

3. 工作人員建立用戶證件資料:
   1. 第一次[1]進入需建立用戶證照資料=>工作人員按右上方”鏡頭轉換”[2]=>請用戶出示證件
      [註1]: 第二次以後進入,如已建立過,畫面上方會自動出現用戶資料=>跳下一頁步驟4.
      [註2]: 鏡頭轉換目的:1.手機後鏡頭才有自動對焦能力,適合影像文字辨識.2.方便用戶手持證照
   2. 工作人員按下”證件辨識”=>辨識健保卡或身分證,並於上方顯示姓名,身分證號,生日,卡號
   3. 確認顯示資料無誤=>按下右上方”鏡頭轉換”鍵,切回前鏡頭臉部畫面.

居家檢疫視訊管理名單建立(2-人臉辨識)

4. 建立人臉辨識資料庫:
   1. 第一次[1]進入需建立人臉辨識資料=>工作人員待用戶臉部鏡頭出現=>適時按下”臉部辨識”
      [註1]:第二次以後進入,如已建立過,畫面上方會自動出現用戶頭像=>跳下一頁步驟5.
   2. 人臉辨識建立成功=>工作人員螢幕上方出現用戶頭像



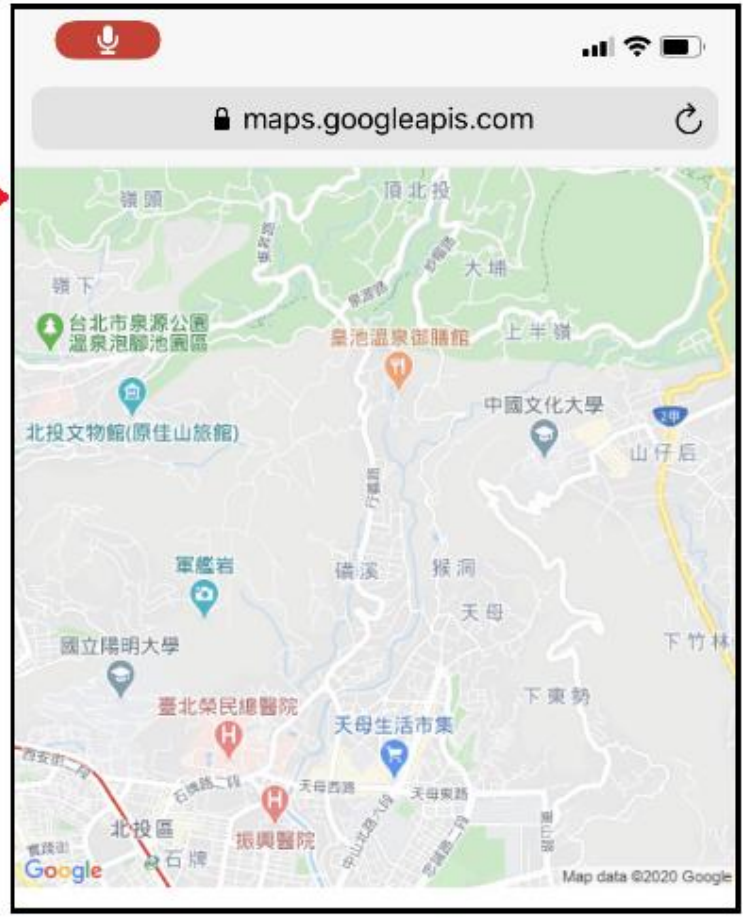
居家檢疫視訊管理名單建立(3-居家地址)

5. 居家用戶地址資料:
   1. 第一次[1]進入需建立用戶居家地址

      [註1]: 第二次以後進入,如已建立過,畫面上方會自動出現用戶居家地=>跳下一頁步驟6.
   2. 工作人員按下”語音辨識”=>請用戶口說出居家地址=>系統自動將語音地址轉成文字地址
   3.工作人員判斷地址辨識結果正確(若失敗可重複2.) => 完成地址輸入=>跳下一頁步驟6.

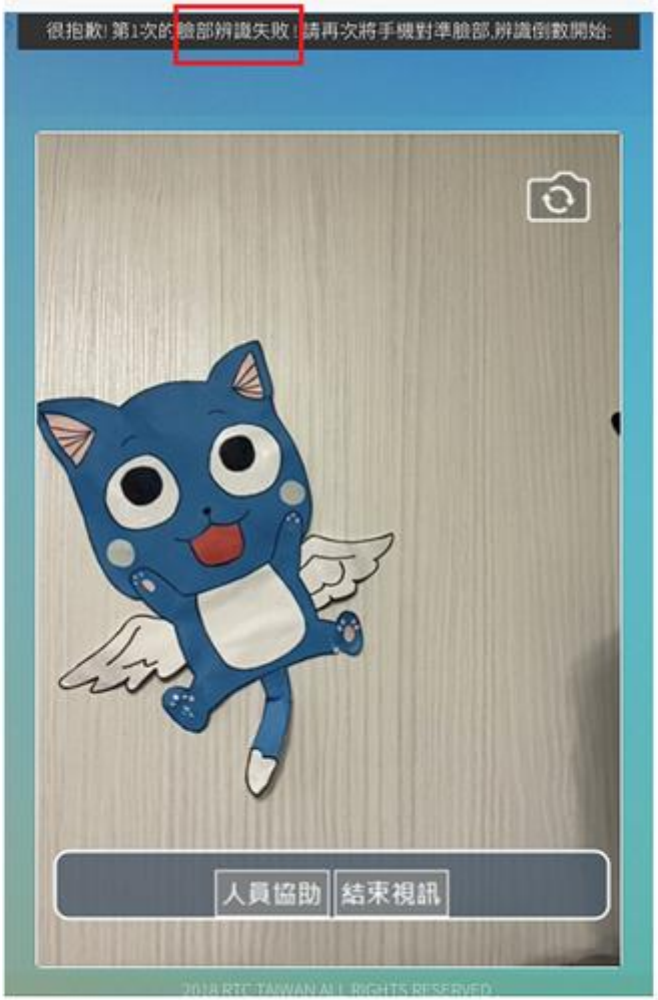
居家檢疫視訊管理名單建立(4-地理位置)

6. 居家用戶地理位置:
   1. 工作人員按下"地理位置"，居家用戶第一次會先彈出"是否允許Google地理位置取得？“ =>居家用戶必須允許. [註]:第二次以後系統會自動擷取居家用戶地理位置.
   2. 居家用戶允許後=>工作人員畫面最上文字會出現=> GPS：…地址... , 同時右上方出現方形小地圖,點擊該小圖=>彈出另一大地圖視窗,這時候工作人員的攝影機會暫時變黑,而聲音還是可正常對話,關閉大地圖後,攝影機恢復正常.



系統自動執行視訊管理居家用戶

1. 系統依設定(例如:每天08:00~20:00 隨機5通),自動發出視訊簡訊給居家檢疫用戶.
2. 居家用戶手機收到簡訊,按下連結 https://rtc.tw/HQuser.html?roomkey=09xxxxxxxx&agent=09yyyyyyyy
3. 用戶接通後,系統會以聲音跟文字方式導引用戶完成"人臉辨識", 如果人臉辨識3次失敗, 自動會轉接服務人員協助.
4. 用戶如有看診需求,可以隨時按下方"人員協助"鈕, 系統立即以簡訊通知工作人員上線協助.
5. 系統可自動抓取居家用戶GPS定位資訊,比對居家地址計算偏離距離,判斷是否發出告警?



工作人員手動視訊管理居家用戶

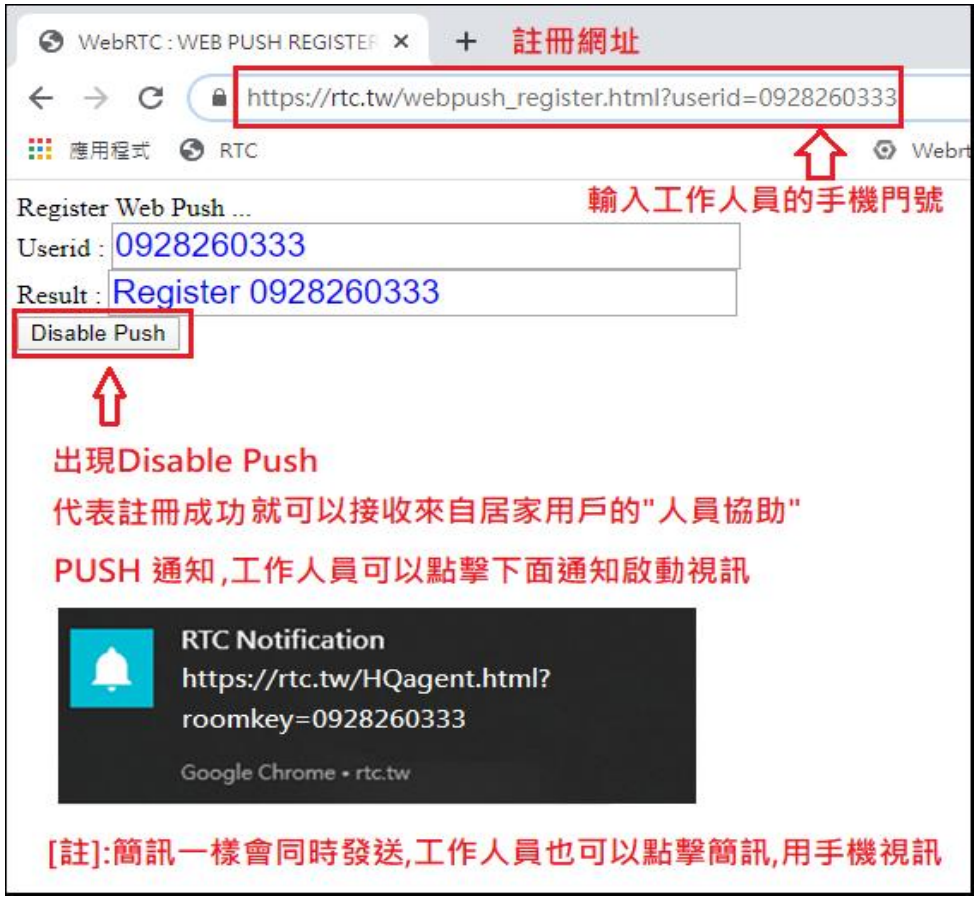
1. 工作人員透過chrome連上https://rtc.tw/HQ.html,輸入自己及用戶手機09xxxxxxxx
   =>系統送出簡訊：“疾管局居家檢疫視訊邀請 https://rtc.tw/HQuser.html?roomkey=09xxxxxxx&agent=09yyyyyyyy”
2. 工作人員視訊等待畫面上方自動出現’用戶頭像’,’證件資料’,’居家地址’ ,’GPS位置’
3. 居家用戶收到簡訊連結=>進入視訊畫面,與工作人員開始進行視訊訪談.

工作人員設定電腦版視訊通知

當居家用戶人臉辨識3次失敗,或用戶按下"人員協助",系統除了立即簡訊通知工作人員,也會以web-push方式通知,要啟動web-push請依照下面程序進行:

1. 工作人員透過桌機chrome連上https://rtc.tw/webpush_register.html?userid=0928260333
   (上面userid=09xxxxxxxx => 請輸入工作人員的手機號碼)
2. 進入網頁後,先按下"Enable Push"=> 變成"Disable Push"=>表示註冊成功,參考下面畫面.
3. 註冊成功後,當用戶來電時,電腦桌面右下角會彈出"通知視窗",按一下該視窗即可啟動視訊

[註]:手機簡訊也會同步發送,工作人員也可以選擇使用手機視訊.



居家檢疫視訊管理後台作業(需整合)

1. 用戶沒有點擊邀請簡訊URL後續處理:
   不論工作人員手動或視訊系統自動發出邀請簡訊,用戶都有可能沒有回覆,這種case可以由視訊系統再度撥打傳統電話至用戶手機,提醒用戶打開簡訊連上系統. 如果傳統電話依舊不通,那就先標記"一次失聯紀錄",當累積N次失聯紀錄,就要發告警給相關人員.
2. 聲音影像側錄存證管理:
   視訊雙向聲音影像側錄存證(檔案size約每分鐘5MB),
   查詢調閱介面…….

3. 工作人員管理與登入作業…

視訊平台規格需求

1. 視訊平台主機

OS : windows 2016含以上
實體核心: 4xCPU , 3.0 GHz含以上
RAM : 32 GB
HD : 200 GB
以上規格一部主機可以同時運作120路視訊,用戶&工作人員視訊占用2路.
可多部視訊平台主機堆疊
[註]: 建議視訊主機以實體機為主,VM主機雖然也可以但能力遜色許多,相同規格VM只能同時運作40路視訊.

2. 視訊儲存空間容量

假設每天1000人,每人每天 5通 , 每通 2分鐘, 預估如下 :
1000人/每天 x 5通/每人x 2分鐘/通 x 5MB/分鐘 = 50000 MB/每天 x 365天/年 ~= 1.8TB/年

3. 網路頻寬需求

視訊頻寬 audio-bitrate ~ 35 kbits/second , video-bitrate ~ 1000 kbits/second 合計1035 kbits/sec
假設同時有100對P2P視訊 : 網路頻寬需求約 200 Mbits/second
網路防火牆需開通TCP: 443,4433,1701,8080 ; UDP:30000-33000

用戶端與工作人員端視訊設備規格

1. 用戶端使用一般手機,主要分為android , ios 兩類:

   1.1 android手機 – 預設瀏覽器必須是chrome,當用戶點擊簡訊URL時能自動帶起瀏覽器進入視訊網頁 , 第一次進入視訊網頁時因為開啟攝影機,麥克風緣故,會彈出”是否同意視窗?”,必須在同意之後才能啟用視訊. 第二次以後就可以自動進入視訊.

   [註] : 有些大陸製手機預設瀏覽器不是chrome, 瀏覽器不支援webrtc無法視訊.

   1.2 ios手機 –瀏覽器固定為 safari 沒有問題. 但稍微麻煩的是safari每次進入視訊網頁都會彈出”是否同意視窗?” 必須在同意之後才能啟用視訊.

2. 工作人員端一般使用桌機或平板(windows or mac)

   2.1 需安裝chrome瀏覽器,加裝攝影機與喇叭麥克風.

   2.2 工作人員也是可以使用手機來操作,以增加移動性.

個資與系統平台安全性探討

1. 個資問題: 本計畫涉及5項用戶個資揭露:
    1. 證件(身分證/健保卡)資料
    2. 人臉資料
    3. 居家地址資料
    4. GPS地理位置
    5. 錄影錄音 – 必須落地加密

    以上個資的建立必須取得用戶同意.

    以上個資的存/查必須有加密與認證程序.
2. 系統平台安全性: 所有資料流動與儲存必須限制在台灣內部區域.
    1. 網站Web-Server安全性
    2. WebRTC-Media-Server安全性 - 必須排除Zoom被詬病的資安問題

        [註]:Zoom主要有3項資安問題:
        1. 有大陸認證主機參與其中． 2.視訊會議ID與會議密碼設定問題
        3. 使用AES-128 ECB金鑰加密及解密視訊

        https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
    3. 用戶資料庫安全性
    4. 用戶個資儲存安全性
    5. Google雲端:證件辨識,語音辨識,GPS位置等資訊保密,必須取得Google保證
    6. Microsoft雲端:人臉資料資訊保密,必須取得Microsoft保證.