

出國報告（出國類別：研習）

參加「第 12 屆新興智慧技術國際研習會(CEWIT 2015)」

服務機關：行政院環保署

姓名職稱：羅啓建管理師

徐嘉欣管理師

派赴國家：美國

出國期間：104 年 10 月 17 日~24 日

報告日期：105 年 1 月 13 日

目錄

壹、研習會背景與目的..... 3

貳、研習過程..... 4

參、心得與建議..... 12

肆、研習照片..... 15

附件1：第12屆新興智慧科技國際研習會論文摘要資料

附件2：Google for Work Security and Compliance Whitepaper - How

Google protects your data

附件3：Google’ s Carbon Offsets: Collaboration and Due Diligence

附件4：Mobile Solutions on Google Cloud Platform

附件5：Google’ s Green Computing: Efficiency at Scale

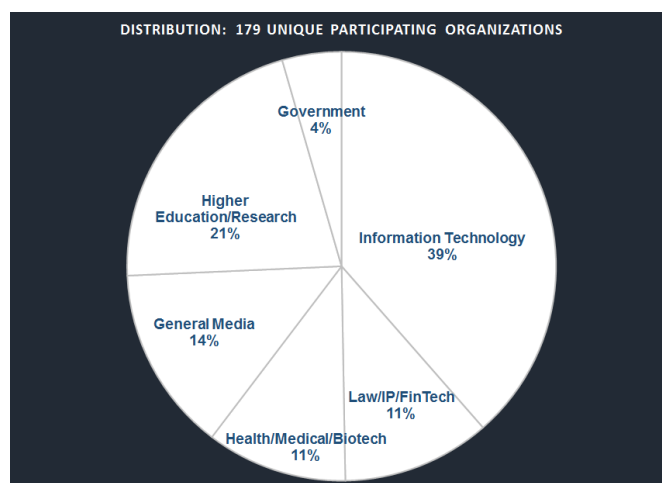
參加「第12屆新興智慧技術國際研習會(CEWIT 2015)」

出國報告

壹、研習會背景與目的

「第12屆新興智慧技術國際研習會(CEWIT 2015)」由無線網路與資訊技術卓越中心(Center of Excellence in Wireless and Information Technology (CEWIT))主辦，該中心於2003年成立於紐約石溪大學(Stony Brook University)的研究與開發園區內，希望成為新一代的研究與教育機構，其使命有三項，進行新興智慧科技研究，訓練專業資訊人才，與培育新的企業發展方向。

本次研習會以論文發表與實務操作之方式分享各界最新之研究成果，共計有500多位人員，12個國家參與此次研習會，參加人員如下圖，分布中約有39%為資訊技術人員，21%為高等教育與研究人員，14%為大眾媒體人員，11%為健康、醫療與生物技術人員，11%為法律與金融技術人員，最後4%則為政府機關人員（參與人員統計資料摘錄自研習會網站），研習會設置有網站（網址：<http://cewit.org/conference2015/>），網站提供有研習會相關資訊。



本次探討的議題主要為大數據分析與視覺化、網路安全、物聯網、資訊技術和資訊化社會、健康技術和醫療載具等新興資訊科技主題，研習會議程詳如附件1。另 (CEWIT)每年以不同主題辦理研習會，前一屆研習會議程無線網路與資訊技術為範疇（網址：<http://cewit.org/conference2014/>），提供參考。

貳、研習過程（含照片）

日期	工作內容概要
10月17日(六)	啟程臺北時間 19:05 抵達美國時間 22:05
10月18日(日)	自費參訪，避免因飛機誤點耽誤 19 日的研習會。
10月19日(一)	至長島區 Melville Marriot 飯店參加第 12 屆新興智慧科技國際研習會。 第 1 天議程，包括議題有報到、大數據分析與視覺化、網路安全與物聯網等。
10月20日(二)	至長島區 Melville Marriot 飯店參加第 12 屆新興智慧科技國際研習會。 第 2 天議程，包括議題有資訊技術和資訊化社會、健康技術和醫療載具與新興技術海報瀏覽等。
10月21日(三)	參訪紐約曼哈頓區彭博社紐約總部。
10月22日(四)	參訪紐約曼哈頓區 Google 紐約辦公室。
10月23日(五)	返程美國時間 1:25
10月24日(六)	抵達臺北時間 5:15

第12屆新興智慧技術國際研習會(CEWIT 2015)」研習會，本次研習會舉辦地點位於相對偏遠的長島區Melville Marriot飯店，考量飛機抵達、返程時間及後續於曼哈頓區彭博社紐約總部及Google紐約辦公室參訪行程，選擇住宿靠甘迺迪機場較近的紐約皇后區，並以搭乘紐約大眾交通運輸地鐵(MTA)、長島鐵路(Long Island Rail Road, LIRR)等環保大眾交通方式，前往研習會及拜訪行程等地點，除學習資訊新知外，並以實際行為落實環保減碳。

一、 104 年 10 月 19 日研習會第 1 天：

第1天的研習會議程自上午9點開始，參與同仁於8點半抵達會場報到，會場接待人員利用先前同仁網路報名條碼資料（照片3），現場製作印製識別證，以便利於會場分辨身分使用。

參與同仁分別加大數據、網路安全與物聯網之研習，其中大數據共有6份論文分享，網路安全有7份論文分享，物聯網有7份論文分享，論文摘述如下。

（一）大數據 (Big Data)：

- 1、 Twitter Financial Community Sentiment and its Predictive Power to Market Movement：此主題講述 Twitter 為受歡迎社群網路之一，透由應用 Big Data 相關技術，建立相關使用者模組，探討 Twitter 使用者對於金融影響的預設關係。
- 2、 Cost and Machine Learning:An Application to Feature Selection for Hidden Markov Models：機器學習是種可發現隱藏的數據的方式，但大部分模型蒐集的數據不代表可推及預測未來的數據的結果，大部分的機器學習技術通常受限於資料量。而研究過程往往於資料蒐集、整理有許多對應的資料成本，此研究係探究選擇隱馬可夫模型 (Hidden Markov Model, HMM)的相對成本，馬可夫模型為於人工智慧的許多子領域有很強的應用，可描述具有隱含變數的隨機過程模型。
- 3、 RealTime LargeScale Big Data Networks Analytics and Visualization Architecture：大數據分析和可視化技術，是目前及未來資料處理的趨勢，然而目前大數據研究都圍繞大規模的數據傳輸，研究為以結合 Big Data 數據及網路技術的 XSimViz 模組，模組內部主要包含網路速度、系統設備效能、資料量等，探究動態即時的處理及操作過程，以提供更好的視決化技術協助使用者了解並與系統即時互動。
- 4、 The Data Sensorium: Multimodal Exploration of Scientific Data Sets：講者為本研習會紐約石溪大學(Stony Brook University)的副教授，講者亦具有為大提琴家和作曲家，研究主樣講述關於音頻數據的研究，透過大量的數據分析，進行資料整合，將統計數字，轉成聲波、頻率和功率，以聲音的型式顯現，進而可協助推測釐清不同的使用者可能喜歡的音樂類型、常聽歌曲，還可以偵測統計使用者在哪個地區收聽音樂，利用這些分析數據，能清楚描繪出使用者的個人行為圖像，更解析耳朵對於信息吸引甚於眼睛。
- 5、 Exploring the Feasibility of Heterogeneous Computing of Complex Networks

for Big Data Analysis：本研究為探究異構網路計算方式，對於巨量資料分析的益處，研究過程透過 KCMAX Bisection 相關演算法方式，結論推測可得提升效能至少 8%。

- 6、EP-SPARQL Complex Event Stream Processing System and its Applications：本研究為探討為了解大數據資料流在網路上的發展，開發了 EP SPARQL 系統，這個系統可應用於股票、社交網絡等。

(二) 網路安全 (Cybersecurity)：

- 1、A digital envelop scheme for document sharing a private cloud storage：此主題講述在一個雲端儲存環境，我們可以數位信封的方式，將機敏文件加密，確保即使在雲端的儲存空間中，也只有被授權的人能夠閱讀文件。
- 2、Ensuring online data privacy and controlling anonymity：互動式社群網站蓬勃發展的現今，人們常不自覺的將個人隱私資料暴露在網路中，而且由於對隱私設定的不熟悉，造成無關的人也能接觸隱私資料，此主題講述如何確保線上資料的隱私，降低資料暴露的風險，以及如何控管匿名。
- 3、Predicting and protecting cross site request forgery attacks on contemporary web applications：依據 OWASP 調查現今網站 10 大弱點中，跨網站腳本攻擊一直名列其中，而且其變形攻擊手法也不斷推陳出新，此篇論文探討如何預測與保護網站應用系統遭受跨網站請求偽造攻擊，以降低網站遭受攻擊之風險。
- 4、Security challenges and data implications by using SmartWatch device in the enterprise：此主題由 IBM 介紹 SmartWatch 這個設備如何應用在企業中，以解決企業的資料安全與資料整合問題，在物聯網發展的時代，可以提供一個資料整合的方案。
- 5、Increasing privacy in a data-driven world：網路與大數據蓬勃發展的時代，藉由資料的彙整、分類與分析，人們可以發現許多隱藏的現象，也可針對個人發現許多隱私秘密，因此這篇論文描述了作者理想中新的具有隱私保護的網路世界，在這個世界中使用者會更清楚的知道他們在線上的行為會對他的隱私產生什麼作用，而且系統和應用程式再開發的階段就能將隱私保護的觀念納入，自然在這個理想的環境中，更能增進我們的隱私保護。
- 6、Investigating, categorizing, and mitigating malware download paths：網路上的惡意程式一直隨者資訊科技的發展不斷演化、更新，攻擊手法最常見的仍然是社交工程攻擊或網頁掛木馬攻擊，這篇論文將描述現

實網路環境中，使用者會如何連接到攻擊網頁，並經由研究其連接路徑，可以有較有目標的改善網路防禦能力，只要能在連接到攻擊網頁前，將路徑截斷，自然不會感染到惡意程式。

- 7、What you scan is not what I visit – Bypassing safe browsing lists：為了提升網路安全性，其實 Google 等搜尋引擎已導入許多新興技術，例如 Google Safe Browsing 在使用者搜尋時，會提供網站評價的建議，並預先診斷網站是否含有惡意程式，讓使用者不至於進入該網站而造成中毒，但是一種防禦方法的產生通常也會被人發現其破解方法，這篇論文討論如何避開此種防禦方法，讓使用者真正瀏覽的網頁，和系統診斷的網頁不一致，如此就能破解此防禦方法，期望藉由此破解方法再改善 Safe Browsing 機制，彌補相關漏洞。

(三) 物聯網 (Internet of Things)：

- 1、Spectral Partitioning Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks：物聯網技術透過無線傳輸感應器蒐集資料時，傳輸感應節點通常由電池供電，但通常電池的能源資源非常有限，本研究為並利用 FCM 計算每個區域的地理中心點，作為資料傳輸節點，研究發現在資料傳送上使用此方式較其他演算法好。
- 2、A New Circuit Design Framework for IoT Devices：傳統 Internet of Things (IoT)，在功能上有三個挑戰，設備能源、安全性及測試問題，使用電池有相關儲電問題，本研究將電池和使用無線做討論，以使用特斯拉線圈(Tesla Coil)，「特斯拉線圈」所發射出的高頻電波可免費源發射出高頻電來解決能源問題，但對應它有距離問題，本研究提出將電波由 DC signal 轉化成 AC signal，讓設備資料傳送更有效率。
- 3、Reliable Sensor Networks for Medical Applications：本研究為討在應用無線傳輸感應器和無線網路，將各項資料傳送給遠端系統透過遠端提供即時家庭醫療服務。
- 4、A Robust Low-cost and Robust Sensor for Smart Particulate Sensing for PM_{2.5} Applications：本研究探討使用成本但功能強大的感測器，在北京的空氣品質污染監測的研究，研究者贊助者 IBM 正在發展可高密度佈建 PM_{2.5} 監測器，且認為此監測器需要達成以下目標：精準、耐用（至少能使用 5 年）、可暴露於戶外、自動監測和傳輸與低成本，成本訂價約為美金 100 至 200 元。
- 5、Measuring Social Networks using Proximity Sensors：本研究為使用 Intel Edison IoT 技術，探究各設備距離及其效能情形，其中 IoT Intel Edison，是一個雙核心低耗電 CPU 配合 WiFi、Bluetooth 含低耗電藍牙 BLE

(Bluetooth Low Energy) 等無線通訊方式的 IoT Solution。

- 6、 Object Association and Identification through RFID Cluster Collaboration：無線射頻識別技術（簡稱 RFID，Radio Frequency Identification）是以基礎開發，所開發出來的無線感測(Wireless Sensor Network；WSN)技術，其功效為提供消費性市場物流資訊行動化與無縫連結，目前在物聯網應用為強調提供定位資訊。本研究為研究資訊傳送與距離空間之相關問題。
- 7、 Can Bandwidth Sharing be Truthful?：物聯網網路連接技術有 DDNS、Relay Server、UPnP 和 P2P 等，此研究為透過 P2P，探討在物聯網 IoT 上互相分享資源。

二、 104 年 10 月 20 日研習會第 2 天：

第二天的行程同樣自上午9點開始，參與同仁參加資訊技術和資訊化社會之研習，共有7份論文分享，並於研討會展場觀看現場發表論文內容，論文摘述如下。

(一) 資訊技術和資訊化社會 (Information Technology and Society)

- 1、 Identity Crisis in Teens: Role of Technology Addiction：在現今資訊化的社會中，人們隨時隨地都在接觸資訊技術，青少年自小就處在這個環境中，產生許多網路成癮、手機成癮與資訊科技成癮等現象，過去已有非常多相關研究文獻，本篇論文是採用多變量分析方式，研究此類資訊科技濫用對心理健康的結果，包括焦慮和自戀型人格障礙等的影響。
- 2、 Convergence: A Transformative Approach to Advanced Research at the Intersection of the Life, Physical and Engineering Sciences：此主題講述為了培育 2020 年所需要的人才，應該要將多個領域學科融合，增加未來員工的能力，使其能融合生命科學、物理學、資訊科技，甚至試行為科學等領域，這樣才是 2020 年所需要的人才。
- 3、 Understanding Transformation in Cyber-Human System：此主題講述資訊網路科技與人類的關係已經改變，我們應該使用更新的思維，理解資訊網路科技對我們社會的影響，在過去資訊網路科技主要使用在業務系統和嵌入式系統，例如薪資系統等，在系統設計當下，我們可以很清楚的規範使用者可以做什麼，以及他們行為所產生的影響，但是現今的資訊網路科技，例如 Google、Facebook 等，沒有人能知道這些系統對社會的最終影響將是什麼，人們可以使用這些系統做到遠超出原先設計者所意想不到的影響，因此現今進行系統開發時，

應更細緻的研究其所可能產生的影響，以免事態超出控制。

- 4、 IBM Research: STEM and Green IT: 環保議題為現今所有人類都關注的議題，且雲端資料中心在現行資訊科技中被廣泛的使用，包括金融服務，媒體，科技公司，大學和政府機構等，均大量使用雲端資料中心，依據 IBM 公司估計，在未來十年伺服器出貨量將成長 6 倍，資料存儲器出貨量則增長 69 倍，因此綠色節能的雲端資料中心將幫助我們減少溫室氣體排放，並有助於減緩全球暖化。
- 5、 Managing Remote Operation Teams: 依靠現今發達的資訊科技幫助，人們可以輕易進行遠距離通訊，因此公司中有越來越多的遠端團隊，這些團隊無論是在不同建築物、不同城市還是不同國家，均可經由資訊科技進行聯繫，但這些遠端團隊不同於現場人員，公司領導階層需要激勵和管理這些人時，無法使用傳統方式，這主題將討論遠端團隊的獨特管理方式、訓練與整合等。
- 6、 Ideas and Innovation at Stony Brook: 這次研習會議是由紐約石溪大學中的無線網路與資訊技術卓越中心主辦，此主題討論紐約石溪大學的創新實驗室開始一些新的研究主題，歡迎大家加入研究。
- 7、 Security Issues Surrounding the Use of Open Source Software by Online Students: 此主題探討有關線上教育活動中，使用開放原始碼軟體的安全問題。開放原始碼軟體主張共同研究學習與共同智慧，通過眾多線上專家的不斷更新，開放原始碼更安全，不容易黑客攻擊，且更快速地修補漏洞，此主題建議如進行線上學習，可使用開放原始碼軟體進行學習。

三、 104 年 10 月 21 日**彭博社紐約總部參訪**：

10月21日的行程同樣自上午9點開始，參與同仁搭乘紐約大眾交通運輸地鐵至彭博社紐約總部參觀，彭博社主要為一個經濟資訊的平臺，該公司開發有經濟資訊分析工具與平臺，並販賣此平臺，提供世界各地的使用者交換資訊，同時該公司也經營媒體，提供權威性的經濟評論及觀點，且為分析未來的經濟動態，該公司使用許多先進技術進行分析，例如大數據分析等。

在進入該公司前，我們在門禁處進行登記和換證作業，該公司運用條碼結合列印識別證之功能，能立即製作訪客專屬的識別證，避免因沿用識別證導致冒充混入之風險，在參訪中發現彭博社為提升同仁的開放性與活躍思維，他們在公司中設有許多聚會場合，可供同仁在輕鬆的環境下討論工作、激發創意，

並且該公司的辦公室與會議室均採用開放性設計，辦公室中無任何隔屏，會議室則使用透明玻璃，外面很容易就能看到內部的開會狀況。

彭博社同時也經營媒體，因此我們時常可以在電視上看到彭博社的新聞，彭博社中除了有專屬的播報空間，同時他們也在公司內部的聚會空間設置有開放主播臺，將播報融入辦公環境，背景不時可以看到人員行走，讓播報較為生動活潑。

另外我們也發現該公司所使用之杯子、碗、衛生紙等日用品，均採用環保產品或再生產品，以身體力行的方式支持環保工作。最後有關該公司的經濟資訊平臺設計架構因為涉及供公司核心競爭力，因此未提供相關文件資料供本署參考。

四、 104 年 10 月 22 日 Google 紐約參訪：

10月22日的行程同樣自上午9點開始，參與同仁搭乘紐約大眾交通運輸地鐵至Google紐約辦公室參訪，並瞭解 Google現行如何推動環保與資安相關工作，以下簡述本次參訪瞭解之主題。

(一) Google for Work Security and Compliance Whitepaper - How Google protects

your data：Google目前是最為普遍的雲端服務提供商之一，全世界有眾多的公務機關、公司與個人使用Google App服務，本署目前也使用許多Google的雲端服務，例如信箱、雲端硬碟、表單、Youtube等，因此在資安方面Google投入許多資源與作法，保障使用者資料隱私。

就人員面 Google針對員工背景、教育訓練與資安作為均有相關規範，並成立專門的資訊安全小組、隱私保護小組、審計與法規專家，並與資訊安全研究者共同協作，如果發現系統漏洞，即給予獎勵金，鼓勵資深資安研究者共同改善系統。

作業面則會執行漏洞管理、惡意程式預防、意外管理與監控，例如Google會針對內部網路流量進行監控，有專門的資安分析師來發現是否有可疑行為出現，並由各個管道蒐集可能造成資安危害的資訊。

技術面則導入最先進的科技，成立大型資料中心，導入各項資安設備與技術保護系統或個人資料，如2階段驗證、Single sign-on、OAuth 2.0 與

OpenID等，並建立硬體追蹤管理，Google硬碟利用如FDE（全磁盤加密）和驅動加密等以保護資料。當一個硬碟停止服務時，被授權的個人經由驗證，才能將0寫入至硬碟，並進行多步驗證程序，以確保所有訊息均被移除。如果硬碟不能移除訊息，則將使用切碎機物理破壞方式切成小塊，以保護資料不會被洩漏。

並且所有流程均通過第三方資安相關驗證，如ISO27001、SOC2/3、FISMA等，Google保證將以最佳的資安水準，提供顧客服務。

（二）Google's Carbon Offsets: Collaboration and Due Diligence：為了減少Google的碳足跡產生，他們通過提高效率、使用現場太陽能發電和購買綠色電力的方式減少碳足跡。而且為了減少碳足跡到零，他們購買碳抵消，也就是投資環保項目，例如投資於減少禽畜產生的甲烷或是垃圾填埋分解氣體收集來減少碳足跡，依靠大量研究，協作，標準化和調查，通過以上作為Google嘗試將自己的碳足跡減為零，降低自身發展而對地球產生的衝擊。

（三）Mobile Solutions on Google Cloud Platform：在現今有超過數十億的人正在使用智慧型手機，針對智慧型收機的網路服務也在蓬勃發展中，例如本署的Opendata服務，因其上的資料具有高使用價值，因此被大量引用，每個小時都有百萬人次使用，但也因為如此嚴重的影響到本署其他網路服務的提供，以及平常公務的使用，Google為了解決這個問題，提供一個雲端的解決方案，因為智慧型手機的用戶增長非常迅速，公司內部的資訊資源有限，且無法迅速的增長，因而此時就需要藉助雲端平臺協助解決，在此解決方案中，Google可以提供完整的運算引擎、資料庫、儲存空間，以及許多附加服務，例如搜尋引擎、記錄功能、巨量資料查詢分析等，本署也於104年12月測試該雲端平臺儲存空間之功能，測試導入後，果然能極大緩解本署資訊網路資源的壓力，

（四）Google's Green Computing: Efficiency at Scale：在雲端服務蓬勃發展與環保意識抬頭的現在，人們會詢問雲端機房是環保且符合效益的解決方案嗎？我們都知道大規模生產時比較容易降低成本，這個觀念是否能適用

於雲端機房，在提供龐大數量資訊服務的同時，能更有效的利用能源？這個研究就是針對這個主題而產生，並以電子郵件服務為研究標的，Google在這個研究中發現，在小型公司（50個使用者）自建電子郵件時，每年每個使用者將使用能源175 kWh，中型公司（500個使用者）28.4 kWh，大型公司（10,000個使用者）7.6 kWh，而Gmail只需要不到2.2 kWh；而每年每個使用者碳排放在小型公司為103kg，中型公司16.7kg，大型公司4.1kg，而Gmail只排放不到1.23kg，因此Google發現在資訊資源密集的雲端機房，能夠更有效與更環保的使用資源。

參、心得與建議

一、心得

- (一)研究發現，資訊科技爆發性發展的現在，資訊科技所產生之全球溫室氣體排放量約佔2%，其中雲端資料中心佔大部分之能量消耗，因此如何發展綠色機房（綠色運算）是未來發展重點，在享受科技的同時，也能保護環境不受衝擊。
- (二)現今醫療科技在行動與穿戴式載具上蓬勃發展，有56%的人們相信藉由醫療穿戴式科技監控人體健康狀況，能增加10年的平均壽命；46%的人們相信藉由醫療穿戴式科技監控飲食與運動可有效降低肥胖；42%的人們相信由醫療穿戴式科技監控與微調運動計畫，可大幅提升人們的運動能力。目前美國已經有21%的顧客開始使用穿戴式科技產品，未來各行各業的穿戴式科技應用值得我們關注。
- (三)本次參加研習會與參訪2間公司，發現在報到與門禁時，已大量運用條碼結合列印識別證之功能，能立即製作訪客專屬的識別證，避免因沿用識別證導致惡意人士冒充混入之風險，雖然會增加設備建置與耗材之成本，但能有效管控訪客之出入，惟在臺灣有個資法爭議，如在製作識別證時，保留訪客相片、姓名等相關訊息，是否會違反個資法，是尚待討論之議題。
- (四)本次行程中發現美國已大量使用玉米或馬鈴薯等可分解材質製作杯子，其中玉米杯裝冷飲，馬鈴薯杯裝熱飲，已很少見到使用塑膠杯子；另外並使用未漂白紙張製作餐巾紙，可減少漂白時造成的環境污染，為了保護臺灣的環境，減少不可分解垃圾，未來可朝此方向發展。
- (五)本署規劃運用Data Cloud，於建構環境資源資料廣深並俱，加強歷史性資料之蒐

集、整理及資料化(datafication)時，在運用規劃透過導入物聯網(Internet of Things, IOT)等工具技術時，可藉由本次研討會經驗在相關器材、能源及佈點時，多加注意，以擴大資料蒐集層面及規模，提升本署空氣污染資料蒐集，進而提升本署開放資料品質。

(六)地球系統中「大氣、水、林、地及生態」等各個環境面向彼此間環環相扣、緊密關聯，如何有效掌握環境資料，解析環境現況，對環境治理及自然保育工作至為重要。然而因環境資料具有數量龐大且格式異質的特性，運用新的資料處理方法及適當的計算資源，尋求資料分析的新型態詮釋方式，探究跨越原始資料項目的交叉分析，探索資料原始目的以外的解讀意涵，以提出契合科學論據之環境治理政策措施，相顯重要，目前本署針對這部分已導入大數據(Big Data)技術，並以近年來，許多流行病理學研究已確立PM_{2.5}對於健康造成影響，包括：支氣管炎、氣喘、心血管疾病、肺癌等，無論長期或短期暴露在空氣污染物的環境之下，皆會提高呼吸道疾病及死亡之風險，在104年度以PM_{2.5}議題為研究主題，進行全臺空氣品質時空特徵相關性與長期趨勢的探索研究、以及相似性與相關性的挖掘，已有交通污染物CO和NOX等相關性佳等初步成果，目前研究仍是以空間推估為主，後續持續應用大數據(Big Data)技術時，參考研討會各研究建議納入其他因素，如納入時間因素進來，並於蒐集資料時，考量即時風向、雨量等氣象資料、道路上之車流資料、POI之間的人流資料等與時間相關的資料，即可進一步與此模型結合，精進為同時考量到時間與空間的預測模型，以精進空氣品質預報，提升施政透明。

二、建議事項

(一)現今惡意軟體下載攻擊大多發生在網路瀏覽器下載，典型攻擊方式為社交工程攻擊或網頁掛木馬攻擊，其中社交工程攻擊因為較具有目標性，且能直接導向下載惡意軟體，因此攻擊成功率較高，發現如已遭受社交工程攻擊，被安裝惡意軟體成功率高達95%；而網頁掛木馬攻擊，因為現行瀏覽器或防毒軟體會提醒網頁安全性，因此被安裝惡意軟體成功率約53%，現行有部分技術例如URL阻擋、進階持續性滲透攻擊防禦等，雖能阻擋部分攻擊，但仍未有一種技術能完全防禦，仍需使用者保持良好使用網路習慣，以減少被攻擊的風險。

- (二)為達到即時監控都會區之空氣污染，IBM正在發展可高密度布建之PM2.5監測器，且他們認為此監測器需要達成以下目標：精準、耐用（至少能使用5年）、可暴露於戶外、自動監測和傳輸與低成本（大約100~200美金），目前IBM與中國大陸政府有針對北京的空氣污染監測在合作，建議本署再導入IOT時，可向IBM瞭解此空氣監測解決方案，以多方學習，達到智慧國土之目標。
- (三)本署的資訊資源有限，且機房規模只能算是中等規模，為了提供民眾一個更高品質的網路服務，以及追求更環保的能源使用效率，建議本署在開發系統時，能考量系統性質，如系統內的資料較無資安疑慮時，可考量導入雲端系統的開發方法，使用雲端資源，以服務日益增加的使用需求。

肆、研習照片

照片1：研習會會場



照片2：研習會會場俯視圖



照片3：報到



照片4：識別證



照片5：討論情形



照片6：討論情形



照片7：參與同仁



照片8：彭博社



照片9：講解情形



照片12：Google 參訪



照片13：Google六邊形工作區

