工作人都該懂的大數據實務運用

■ 法務部調查局資通安全處　雷喻翔

隨著通訊網路的爆炸性發展以及物聯網應用的普及性，大數據的應用一時之間成為顯學，產官學界也趨之若鶩，希冀能夠運用大數據的威力，提升整體業務效能。何謂大數據？其實也不是什麼嶄新的技術，數據分析早已行之有年，從最基本的統計分析到經由人工智慧演進的資料探勘、機器學習，相關領域都有專家學者競相投入研究。之所以近幾年大數據成為朗朗上口的話題是因為電腦處理速度的提升，使得原本需要耗費大量時間資源才得以獲得的分析結果，如今在短時間之內即可知道隱藏在茫茫資料海中細如針線的重要資訊。

2011 年，時任紐約市長的彭博為了改善頻傳的火警，除了政策面的訂定外，同時也決定從資料面著手，重新檢視消防局及建築部所有相關的建築資料，大數據一躍成為熄滅紐約市烈焰光火的利器。經由數據挖掘與分析，紐約消防隊發現高危險群的房屋數量從原本的 13% 竄升至 70%，有了更詳盡、更周全的目標之後，消防人員得以進一步針對需要檢驗的建築物進行分類，篩選出屬於高風險群而需要特別關注的建築物。透過大數據的著力，紐約市的火災數量確實獲得明顯的改進。

本篇文章不在數學統計等多加著墨，主要是探討大數據實際的應用，不需要龐大的資料庫亦無需多麼艱澀的數學模型，僅利用政府公開資料以及人人皆可使用的開放原始碼應用程式便可進行大數據的分析，進而激發工作上的新思維，資料俯拾即是，實作勝於一切。

資料蒐集及所用之工具

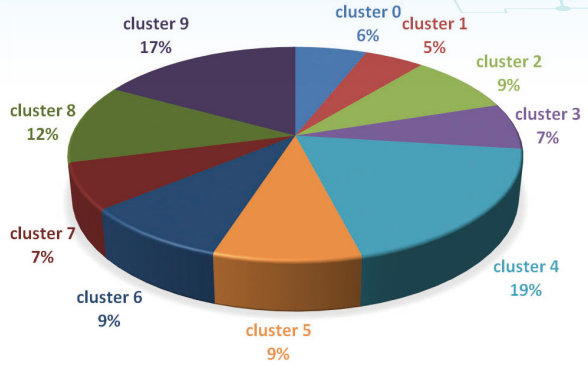
首先蒐集包含從臺北市政府開放資料及網路公開資料等 6 種不同的資料，其中包含臺北市 (1) 竊盜統計、(2) 里資訊、(3) 捷運站地址、(4) 公車站地址、(5) 百貨公司賣場地址及 (6) UBIKE 站地址，各資料表來源如表一所列，其中臺北市竊盜統計資料表又可分為房屋竊盜、汽車竊盜及腳踏車竊盜案件。

由於每個資料表擁有共通的屬性—地址，所以我們利用地址資訊將各資料表整合起來。考量臺北市的行政區域由大到小以區、里、鄰劃分，如圖一所示，共有 12 區、456 里、9,594 鄰，若是以一個區做為行政區域之劃分，其所涵蓋的區域面積過廣，對於在一個區內之東部或西部發生的犯罪案件並無太高的相關性，且行政區之面積大小也有很大的差異；而若是以鄰做為行政區域之劃分，其所涵蓋的面積又過於狹小，以鄰為歸類之所屬案件資料不足，各鄰之間的屬性（特徵）也較難有差異性。因此，我們取位於中間的里做為本專題之行政區域劃分，並以里為基準結合所有的資料表。在處理臺北市里資訊時，由於各個里的範圍不一，要找到里的實際中心較為複雜，因此我們採用里辦公室地址來代表每個里的中心座標。

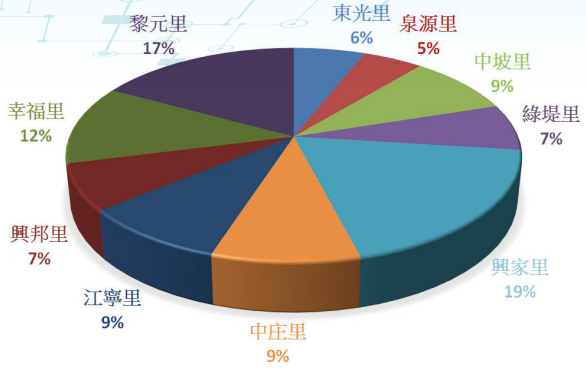
表一　本文蒐集之資料表統整

資料	資料來源	資料筆數
臺北市竊盜統計	臺北市政府公開資料 http://data.taipei/	1,012 / 177 / 607 房屋／汽車／腳踏車
臺北市里資訊	臺北市政府民政局 http://ca.gov.taipei	456
捷運站列表	臺北捷運公司 http://www.metro.taipei	108
公車站列表	臺北市公車資訊 http://5284.taipei.gov.tw/	5,026
大型商場資訊	OneLife 生活網 http://onelife.tw	46
UBIKE 站列表	UBIKE 網站 http://taipei.youbike.com.tw	274
實價登錄資訊	信義房屋	402

圖一　臺北市行政區劃分。



圖二　各群所佔之里數量比例。



圖三　以離各群之中心最近距離之里作為代表。

資料歸納分析

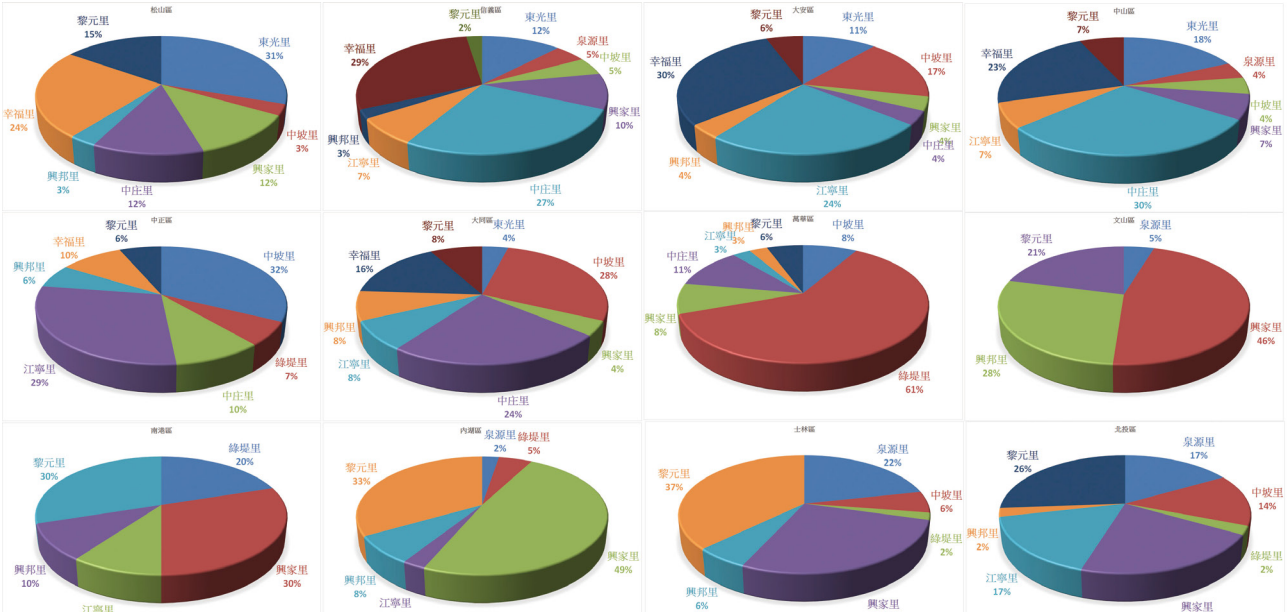
首先統計各個里所發生的竊盜案件次數、公車站總數、百貨公司總數以及里距離最近之捷運站名稱及其距離等資訊，接著先將全臺北市 456 個里分成 10 個群，進一步分析每個群的屬性。本文採用大數據領域中廣為使用的開放原始碼應用程式 WEKA 為分群工具，其結果如圖二所示。

從圖二可以看出各群中里數量的分布從最高 19% 到最低 5%，沒有特別集中於某一群，顯見臺北市的住宅環境並無明顯趨於一種型態。為了凸顯每個群的屬性，我們進一步在每一群中找出地理位置上距離中心點最近的里做為代表，其結果如圖三所示。

有了以上的轉換之後可以更明顯的看出群內的屬性關係，舉例而言，幸福里位於中正區善導寺捷運站旁邊，該位置不僅交通方便，離各大百貨也很近，同時房價亦居高不下，由此可知幸福里所代表的群其屬性較偏上述特徵。

接著再針對一些比較特殊的群來做分析，首先是以泉源里為代表的群組 1。檢視該群的特性，我們可以發現群組 1 距離捷運站最近，但是一公里內的捷運數反而不多，同時可能也因為人口數不多、非鬧區（MRT、公車站牌數、UBIKE 站數不多），所以竊盜次數最少；群組 0 及群組 4 的特性則是人口數較多、戶數較多；群組 8 則是房價較高，屬鬧區的型態，以大安區、信義區及中山區為主。

另外也比較臺北市 12 個行政區區內的差異度，從每個區內所屬不同群的比例可以了解該區內的差異性。從分析結果來看，萬華區及內湖區內的屬性較為集中，兩者皆有接近 50% 的里被分至同一群中；其餘的區皆無明顯的集中屬性，其中中山區更是被分類成 8 群，顯見其區內的分散性。



圖四　各群之間總結圖示。

這項分析提供另一種對於臺北市地區的傳統思維，一般而言，提到信義區、大安區時總讓人聯想到較為熱鬧、交通便利的區域，然而透過分析資料，得以更進一步地篩選出真正符合期待的區域及地點，總結分析結果如圖四。

本文之數據分析亦可做為後續研析的前導，文中打破臺北市 12 個行政區的分界，重新將區下轄的里重新分類，歸納出隱藏其中的關聯性。擁有同樣屬性的里，其人口組成及習性也有較高的機率偏向同一群，此種做法不侷限於臺北市，可套用至全臺各縣市地方。後續若能再整合更多的資料類型，例如貪瀆案件發生的地點、毒販常出沒的區域、經濟犯罪的熱點或人潮聚集軟目標，如此一來或可提供執法機關一種新的犯罪追查手法以弭禍於無形。

總結

處在被智慧網路包圍的社會，生活週遭無時無刻在產出數據。當然我們可以無視這些資訊，一如往常地執行日常工作，但是若能搭上這一波大數據熱潮，從中提升自己的工作能量，何樂而不為？

然而大數據並非百利而無一害，由於經手龐大的資料量，隨之而來的是資料隱私權的問題。在極為注重個人隱私的現今，

享受大數據所帶來的便利之餘，不得不注意個人資料的保護。現就公開資料和私有資料分別討論：公開資料既為公開，相關牽涉到個資的部分已去識別化，因此當無洩漏隱私權之疑慮，關鍵部分為政府私有資料。政府有關部門就各自職掌範圍蒐集民眾個資有其法律上之規範，稅捐部門就其稅捐稽查業務、衛生部門就健保業務等都早已行之有年。

然而大數據的應用可貴之處在於大量異質性資料的整合，如同前述所提紐約市於火警預防的研析就觸及不同部門間的資料，於此必然會產生跨業務資料使用權限的問題。對此，筆者認為若有適切的稽核規範，明確限定何人、何時、何地可以接觸整合後的資料，且有專職人員定期檢查使用情形，如此在個資運用上則無侵犯或洩漏個資之虞。

資訊技術是未來工作的趨勢，不用將它視為高不可攀的技術，畢竟我們不是鑽研統計數學的專家學者，所要做得是掌握概念、操作應用。藉由簡單的資料蒐集及分析，原本單純的結果便產生重要的附加價值，這正是大數據應用的精神所在。看完本文後，也一起來動手吧！

知識小學堂

一般而言，大數據的定義為 Volume（容量）、Velocity（速度）、Variety（多樣性）；商業分析和大數據分析之不同點在於：前者的資料分析方法為抽樣分析，且多以預定模型跑出期望結果；而後者則直接使用大數據的原始資料來進行統計分析，甚而視覺化。大數據最重要的是能爬梳資料，發現新模型，從探索過去進化至預測未來。

而「資料獨裁問題」為大數據分析值得關切的課題，需謹記勿盲目受到分析結果的制約，濫用或誤用資料，甚至將個體標籤化、汙名化。

共構金融資安聯防中心 打造高 CP 值防護網

■ 德明財經科技大學行銷管理系副教授　許建隆

金融機構因業務特性與經濟發展及社會安定緊密相連，在 2015 年行政院資安辦公室公告之「政府機關（構）資通安全責任等級分級作業規定」中，係歸類為 A 級單位（資安責任最高等級），並且定義為關鍵資訊基礎設施，相信在《資安管理法》推行後，公、民營行庫之核心系統仍將被列為關鍵資訊基礎設施，為因應此一趨勢，金融業資安從業人員宜儘早進行相關因應準備。

金融業依法架構資通安全維護計畫

根據《資安管理法》草案第 17 條要求，非公務機關應訂定通報及應變機制，並於發現資通安全事件時應向中央目的事業主管機關通報。目前，由金管會主導規劃推動金融界之資安資訊分享與分析中心（簡稱：金融資安中心，F-ISAC）預計於 2017 年第 2 季成立，可預見 F-ISAC 將成為各資安因應金融機構對主管機關通報資安事故或交換資安情資的平台。

前述法規條文與主管單位的動向勢將增加金融業資安從業人員的責任與工作，但若能有效、快速地交換威脅情資，也確實有可能在第一時間讓各金融業者快速應變最新的資安威脅與攻擊，有效避免或降低新攻擊手法所造成的實質或商譽損失。

在《資安管理法》（草案）中，要求公務機關與非公務機關須訂定、修正與實施資通安全維護計畫，也要求主管機關提供範本或施行辦法等資訊供業者參考。但在此之前，公務機關與非公務機關仍可先進行相關準備，檢視是否有不足或未涵蓋之處。首先，可從盤點目前的資安軟硬體設備的投資、資安服務的採購與實質效益、採用的資安制度標準以及相關流程作業，並參照近年的資安風險威脅，檢視現行資

安防護投資是否有不足或尚需補強深化之處，更重要的是避免各項資安投資流於僅有單點防護效果，宜透過作業流程將資安防護作業由點連成線，由線構成面，達到整體縱深防禦的資安防護。

資通安全維運作業的 3 大環節

為避免流程的設計僅是應付內部與外部稽核的查核活動、流於形式，建議金融業者可從「預警與強化作業」、「資安監控與通報作業」，以及「資安事故與情資應變作業」等 3 個相關聯的資安維運作業來檢視與調整現行作業流程。

從 2016 年上半年孟加拉中央銀行的環球銀行金融電信協會（SWIFT）金融電信網路遭駭客入侵跨國盜轉帳案例來看。當金

融業者收到此同業之威脅情資時，負責情資管理的資安人員將視情資等級進行內部通報，並針對可能受影響的工作站或主機，擬定對策，呈報決策主管，進行資安情資應變作業，或採行風險降低對策，例如限制工作站對 Internet 的直接存取、建立工作站專用機上的程式白名單管控機制，或加強對可能受影響之工作站電腦上的異常訊息與網路封包之監控通報等。

資安維運人員需要針對預警情資進行篩選、通報管理階層、盤點對應的資訊系統、判斷可能的影響，並擬定適當應變對策方案，快速取得決策階層同意後，投入資源進行對策所需的應變，並在資安情資應變完成後，重新檢視該個案應變過程，並思考是否可回饋到例常的資安強化作業。例如透過年度資安評估作業，檢查防火牆或代理伺服器（Proxy）是否有依照規劃對此類相關工作站正確設定對 Internet 的存取管控，避免該等工作站遭植入後門程式時傳送內部機敏資訊到駭客的中繼站；並因應該規劃設計資安監控規則，以監控該類工作站的網路連線活動是否有違反防火牆或代理伺服器（Proxy）對 Internet 的存取管控規則；再根據此規則確認資安事故通報與該類資安事故之應變作業程序。

如此從「預警與強化作業」、「資安監控與通報作業」與「資安事故與情資應

變」等活動循環落實資安維運作業，累積的資安經驗有助於提升金融業者面對相關資安情資的應變活動。

金融資安聯防中心功能何在？

若建立金融資安聯防中心，除了提供資安監控服務，宜提供以下功能，以強化其對於金融業者之效益：

一、提供針對性之資安弱點情資通報

未來金融資安中心（F-ISAC）雖然提供資安情資，但尚未規劃針對個別會員的需求在通報前事先過濾篩選情資，故預期其會員未來所收到之情資數量眾多，而與業者切身相關者寡少，業者自身之資安維運人員將需要花費許多工時用以過濾情資。因此，金融資安聯防中心若能對個別業者提供針對性之資安情資，並予以分類及建議風險因應之優先等級，將可節省業者相關人力工時，並提升因應作業之時效性。

二、提供事故處理經驗庫

金融業者間具有競爭關係，對於所遭受之資安攻擊事件與應變處理方法等詳情可能不宜與同業共享，但金融業者同為資安攻擊之熱門標的，各業者所遭遇之攻擊手法相似性高。因此，金融資安聯防中心若能將會員遭遇之攻擊事件與應變處理經驗予以匿名化處理，再提供給其他會員參考，將有助於提升個別業者事故因應之時效性，降低損失，並供部署強化措施之參考。

三、與國際資安組織接軌

金融業者拓展全球性業務時將面對國際化之資安防護要求，可能需要與多個國際性之資安資訊分享與分析中心介接，以提供自身之資安情資，或接收國際組織之資安情資。若資安聯防中心具備與國際資安中心（ISAC）之介接能力，將可免除金融業者自行開發與維運介接介面之負擔，順利與國際接軌。

全面升級資安防護，接軌國際

資安威脅、資安情資攻擊手法瞬息萬變，駭人的入侵新聞案例更令從業人員面對巨大的挑戰，《資安管理法》或許會更增加資安從業人員的責任與負擔，更直接增加企業營運成本，資安從業人員或許可藉此爭取更多的資源投入，重新檢視目前配置的資安軟硬體設備人力與組織架構，將現有投入或不足之處補強，由單點防護透過流程作業串聯成線，透過點線相連形成完整的資安防護面，最後構成整體防禦縱深，確實落實於資安維護維運計畫與作業。為使金融業者投入的資安投資更具效益，宜考量建立金融資安聯防中心，以收提升資安防護時效、降低損失，以及順利與國際接軌之綜效。