我國詐騙集團累犯特徵實證研究

王貴珠

中央警察大學圖書館講師

摘要：

資訊科技的進步，為人類生活帶來便利性，但詐欺(騙)集團往往透過各種通訊科技及金融服務，利用人性心理上的弱點，運用各種虛擬情境，在民眾防不勝防中謀取不法暴利，亦讓政府相關部門疲於奔命。因此，瞭解詐欺集團累犯特徵，以提供執法機關在研擬防制詐騙對策參考，是件刻不容緩之事。鑑此，本文擬從司法院「司法院法學檢索系統」取得研究用樣本。本研究透過內容分析法，結果發現：(一)從 2012 年 1 月起至 2016 年 6 月底止有效樣本 1,712 司法案件中，詐欺(騙)集團具有累犯紀錄的案件數達 597 件，占全部的 34.8%(逾 1/3)，即每 3 件詐欺(騙)案件中，就有 1 件是累犯案件，顯見國內詐欺(騙)集團累犯之嚴重程度。(二)詐欺(騙)集團累犯是存在著共通與差異之特徵。(三)詐欺(騙)集團累犯的共通的特徵為(1)2013 年與 2016 年詐欺(騙)集團累犯共通特徵為提款卡,機房,幫助及二線；(2)2013 年與 2015 年詐欺(騙)集團累犯共通特徵為簡易判決；(3)2014 年與 2016 年詐欺(騙)集團累犯共通特徵為大陸；(4)2013 年、2015 年與 2016 年詐欺(騙)集團累犯共通特徵為機房。(四)詐欺(騙)集團累犯的相異特徵表現出的特性為從 2012 年的第「一線」人員，發展到 2013 的二線人員利用電腦、行動電話來做群發，到 2015 年則出現詐騙教戰手冊，包括利用插有易付卡的手機提供車手使用，並作為日後機房人員便利聯絡前往指定地點收取被害人交付款項之用途，而到 2016 年則以偽卡在提款機鍵入密碼提領贓款。可見詐欺(騙)集團的詐騙手法,隨著資通訊科技變化而不斷在演進著。

關鍵詞：詐欺犯罪、文字採礦、資料採礦、詐欺(騙)集團

綱目：

壹、前言

一、研究動機

今(2016)年 4 月非洲肯亞電信詐騙案，陸方以電話詐騙受害人為大陸人民為由，在肯亞當地司法機關，針對遭扣押的兩岸華人詐騙嫌犯，以未觸犯該國相關

法律為由宣判無罪後，透過與肯亞的司法互助協定，將遭逮捕的兩岸嫌犯分批直接遣送大陸。由於這些遣回大陸遭拘留的嫌犯，其中包括了 37 名臺灣百姓，引發臺灣政府高層官員的高度關切和司法管轄權的爭議。[1]

加上最近常常發生 LINE 帳號被盜的情況，以臺灣人之愛用 Line 這個社交媒體來看[2]，帳號被綁架的問題，更不容忽視。

我國詐欺犯罪案件從 1997 年的 2,817 件至 2015 年的 38,913 件，成長幅度高達 12.81 倍。[3]

在「維基百科」中更有關於臺灣詐騙集團的記載，包括臺灣詐騙集團的歷史、組織、作案手法、案例分布、受害人及臺灣與中國大陸兩方面立場等面向。[4]

詐欺犯罪已從傳統單純的個人欺騙行為，跟著科技的進步與網路的便捷，演變成了智慧型、集團式的詐欺犯罪形態，而有越來越多的受害人，甚至造成了社會的恐慌，讓老百姓已分不清何者為真？何者為假？

由於詐欺犯罪造成民眾財產嚴重損害，如何阻止歹徒變本加厲觸犯法網，有效預防歹徒進行詐騙，是政府當局刻不容緩的課題。

二、研究目的

本研究擬從我國司法院「法學資料檢索系統」所提供的詐欺案件法院裁判書(.pdf 檔案)，從 2012 至 2016 年作為樣本，結合文字採礦、資料採礦等技術，試圖達到下列之研究目的：

(一) 採用內容分析法，透過文字採礦技術，來獲取詐欺案件詞語與文字歸類(Text Topics)。

(二) 以「詐騙集團累犯」或「詐欺集團累犯」為目標角色，產出詐欺(騙)集團累犯的特徵，以提供執法機關研擬防制詐騙對策之參考。

貳、文獻探討

一、文字採礦

文字採礦(Text Mining)又稱文字知識發現(Knowledge Discovery in Text)，係指將被處理的檔案資料或文件(Documents)視為字串資料型態來從事採礦的一種過程(Process)。此種過程常須借重資訊擷取、資料採礦、機械學習、統計學和電腦語言學等跨領域學科與技術之結合應用。資料大都以半結構性或非結構性來呈現之，並沒有特定實體與其屬性(Entity and Attributes)或格式(Format)，簡言之，就是文章段落(Paragraph)形式。它主要從多維度矩陣中去獲取它的特徵值(Eigenvalues)，其中文件即為矩陣，關鍵詞即為特徵值。因此，經由文字採礦的探索過程，企圖

[1] (1)引用資料來源：工商時報 2016 年 04 月 15 日 04:09 主筆室 http://www.chinatimes.com/newspapers/20160415000036-260202;(2)部分內容修改。

[2] 羅之盈，誰是你的雲端情人，天下雜誌，579 期(2015-08-18) http://www.cw.com.tw/article/article.action?id=5070178

[3] 法務部統計網 http://www.rjsd.moj.gov.tw/rjsdweb/book/Book_Detail.aspx?book_id=193

[4] https://zh.wikipedia.org/wiki/%E5%8F%B0%E6%B9%BE%E8%AF%88%E9%AA%97%E9%9B%86%E5%9B%A2

從大量的文件與其所切割的詞，來獲取少量的關鍵詞，目的在於擷取隱晦、有用、未被發掘，但具有潛在價值的資訊或知識，也是用來探索文件或網站內容的關鍵或核心詞語與意涵，以自動化或半自動化處理，來發現新的、有趣的訊息或關聯規則(Association Rules)，或是依賴人工解讀結果，使發現的訊息變成有用的資訊或知識。

在電腦儲存媒體和網際空間(Cyberspace)所存在的大量半結構性或非結構性電子文件中，如何去篩選和過濾出有用資訊及萃取有價值知識，成為文字採礦技術(Text Mining Techniques)的核心議題。實際上包括概念擷取(Concept Extraction)、文字摘要（Text Summarization）、資訊篩選（Information Filtering）、資料庫索引、命名實體標註或辨識（Named Entities Tagging or Identification）、意見分析（Opinion Analysis）、關係探索（Relation Discovery）、情感分析（Sentiment Analysis）、文字分類（Text Classification）、文字分群（Text Clustering）等議題。

文字採礦所提供的功能，包括各種檔案類型轉換到文字性檔案類型(Text File)、主記憶體位址配置結構之大尾端與小尾端(Big-Endian and Little-Endian)、特定編碼或內碼系統(Encoding or Internal Code System)轉換、自然語言處理 (Natural Language Processing, NLP) 、人工智慧之語意分解(Semantic Decomposition)與斷詞，關鍵詞之萃取、分類，獨立性關鍵詞(Independent Keyword)轉換成脈絡性(前後文)關鍵詞(Contextual Keyword)，以及建立脈絡詞語庫(Contextual Keyword Database)，最後轉換成結構化資料型態、權重與排序等；進階技術包括使用者自建詞語庫，多國語言詞語庫，網爬(Crawling Web Site)、時間事件(時框)分析，連結 (含社會網絡)分析，以及視覺化表達，例如，以不同顏色和關鍵詞字體大小來表示關鍵詞所出現的頻次等，類似文字雲(Word Cloud)的呈現方式。此外，文字採礦(Text Mining)所要處理的資料是具有半結構或非結構的特性(Semi-Structured or Unstructured Characteristics)，它所對應到資料採礦（Data Mining）處理的是詞語(Terms)(亦稱語彙)。資料採礦主要針對各種結構化資料進行量性分析，以擷取未被發掘、但具有潛在價值的資訊或知識。因此，如何在不失文件之原有「旨意」或「用意」情況下，以檔案名稱、關鍵詞和頻次(或權重值)等方式來呈現結構化資料，以利於進一步處理、分析與利用，包括採用統計、資料採礦或商業智慧(Business Intelligence, BI)等，則是文字採礦的發展重點與價值所在。

二、有關詐欺(騙)相關的文獻

早期的詐欺(騙)集團自國內發跡後，即不斷運用市內電話、行動電話、市內溢波、節費器、網路電話等手段，加上犯罪使用的電信工具不斷換新，態樣也越來越推陳出新，犯罪手法的設計更讓人眼花撩亂，精彩的話術足以撼動人心，使得被害人輕易卸下心防，「言聽計從」將款項匯出至歹徒指定之帳戶，歹徒掌握時事、心理、法律知識發展出一套又一套新騙術，已成為智慧型犯罪，政府部門雖正視此問題，然則詐欺(騙)案件數仍居高不下，因而成為學者相關研究主題，諸如：通訊金融詐欺犯罪成因與防制、兩岸詐欺犯罪趨勢與防制對策、影響電話詐騙犯罪被害因素、政府防制詐騙犯罪政策行銷、海峽兩岸跨境電信詐欺集團犯

罪歷程、詐騙犯罪偵查措施、退休族群理財特徵與易受詐騙特徵、兩岸跨境詐欺犯罪手法之分析與其防制策略及電信詐欺犯罪模式與防制對策等之研究，參考表1。

表1：有關詐欺(騙)的相關文獻

年份	作者	研究主題	研究目的、方法	研究結果
2005	許清事[5]	通訊金融詐欺犯罪成因與防制－以臺北縣處理涉及人頭之詐欺案件為例	1. 探討1995－2004年詐欺犯罪在數量、型態及手法、性別、職業及教育程度等之資料分析，藉以瞭解整個詐欺犯罪之變遷。 2. 以2005年9月至2006年3月臺北縣受理通訊金融詐欺犯罪被害案1504件分析、比較。 3. 以臺北縣政府警察局已發生、破獲之新型態通訊金融詐欺犯罪中，採個案研究方法，分別就近年來所偵破之二件重大詐欺集團案例，針對被害人與資深偵辦員警進行訪談，並就被害、犯罪情境、加、被害人特徵、犯案標的等加以分析、研究。 4. 藉以瞭解影響通訊金融詐欺犯罪之成因，進而研擬出具體有效防制作為。	1. 被害人之被害歷程及加害人之騙局設計等犯罪特徵，進一步明瞭目前通訊金融詐騙案件氾濫之原因、詐騙集團犯罪模式、特性及透視歹徒如何運用人性心理弱點； 2. 瞭解目前仍無法加以根絕主要原因：「人頭電話、人頭帳戶仍未能有效加以根絕、現行法令之懲罰不足以嚇阻歹徒犯案之動機、兩岸仍未建立合作打擊犯罪之機制」。 3. 依據「情境犯罪預防策略」加以設計強化標的物、增加監控機制、提升犯罪風險、削弱犯罪者的動機等機制，並結合警察、電信、金融、司法及政府各相關部門，通力合作下，定能使目前反詐騙工作更具成效。
2009	蔡田木[6]	兩岸詐欺犯罪趨勢與防制對策之探討	隨著科技與網路時代帶來科技的便捷，不法分子利用各類詐騙手法以謀取不法利益之情 形必定層出不窮，如何阻止不法分子前仆後繼觸犯法網，有效預防歹徒進行詐 騙行為，實為一值得研究之重要課題。	詐欺犯罪近年來日趨嚴重，犯罪型態也不斷改變，由於調查局職司司法調查工作，面對詐欺亂象，有必要加強偵辦：(一) 比照重大經濟犯罪偵辦:由於不論是調查局或警方，對於偵辦詐欺案件，礙於現行績效制度，無法深入偵辦，或可考慮修改績效評比辦法，例如發掘線索即給予分數，以提高同仁偵辦意願。(二) 偵辦採取刨根方式:發揮綿密的情報系統網路，針對每個詐騙集團完整布線，並把犯罪首謀至各集團成員均予刨除。
2010	曾進忠[7]	資通訊詐欺犯罪特性及歷程之研究	1. 深入瞭解目前資通訊詐欺犯罪的特性； 2. 分析犯罪者利用資通訊服務及工具犯罪原因； 3. 剖析詐騙集團犯罪的歷程、模式及被害人被害主因，藉以策定更有效防制對策。	1. 詐騙集團利用資通訊科技之特性及漏洞，並透過資通訊業者提供之資通訊服務及工具從事詐欺行為，藉以規避警察機關的查緝； 2. 目前之資通訊詐欺犯罪詐騙手法與以往大同小異，以假冒電信費未繳為最大宗。 3. 網路購物等為主要型態，只是利用資通訊科技傳播詐欺訊息管道稍有改變，顯示利用工具的方法具高度替代性； 4. 政府相關單位、資通訊業者、金融業者及社會大眾對防制資通訊詐欺犯罪之能力與付出，顯然不足，仍有諸多缺失。
2010	黃珮如[8]	影響電話	以文獻探討法及電話問卷	1. 性別、年齡、教育、職業、婚姻狀

[5]許清事，2005，通訊金融詐欺犯罪成因與防制－以臺北縣處理涉及人頭之詐欺案件為例，國立臺北大學犯罪學研究所，碩士論文。

[6]蔡田木(2009)，兩岸詐欺犯罪趨勢與防制對策之探討，展望與探索 第七卷第七期，頁86-95。

[7]曾進忠，2010，資通訊詐欺犯罪特性及歷程之研究，國立臺北大學犯罪學研究所，碩士論文。

[8]黃珮如，2010，影響電話詐騙犯罪被害因素之研究，中央警察大學犯罪防治研究所，碩士論文。

		詐騙犯罪被害因素之研究	調查法，針對 165 數位資料庫內容為分析對象，抽取 2009 年 1 月至 6 月之曾經撥打電話進 165 反詐騙諮詢專線諮詢之被害者 19,152 名及未被害者 464,547 名做為抽樣母群體，共抽取被害組 252 人及未被害 97 人進行研究。	況、家庭結構及收入，對於個人是否被害、被害損失及他人監控間有影響，顯見個人特性會影響一個人是否會被害，而且也會影響到個人被害金額上之損失，以及受害時身邊有無他人陪伴； 2. 接觸訊息的種類、個人對訊息認知與個人對訊息接受的接受程度與否，影響個人是否被害； 3. 接觸訊息的種類與個人對訊息的認知，會影響個人的被害損失的高低；而接獲詐騙訊息時，有無他人陪伴或銀行監控下，與個人產生之詐騙結果、跟所遇到的詐騙模式間有關； 4. 個人針對訊息回應與否，與是否被害人之間、所遇到的詐騙模式種類與是否有他人陪伴或銀行監控間有關； 5. 投機型行為、網絡型購物、網路使用情形及與陌生訊息接觸四者與個人是否被害、或是否影響接獲訊息時有無他人陪伴或銀行監控及接獲何種詐騙模式三者間，有時支持本研究假設，有時無法支持假設； 6. 被害者在訊息接受時，以年齡較低者，網路使用情形較少者，較容易接受詐騙訊息； 7. 電話詐騙是否被害上，以不常使用網路、女性且年齡較低者，較容易被害； 8. 在假冒公務員、假借其他詐騙訊息與色情應召三類不同的詐騙類型的被害者間，其個人特性與生活習慣均有所不同。
2010	黃雪蘭[9]	政府防制詐騙犯罪政策行銷之研究－以「警政署 165 反詐騙諮詢專線」為例	針對 165 反詐騙專線之決策與執行單位，及線上直接服務民眾之基層員警為訪談對象，以及輔以次級資料分析法，利用官方統計資料、民調資料與 165 專線之現有資料庫之資料作檢視與分析，藉以瞭解 165 反詐騙專線之政策行銷策略與執行過程，以及執行之成效與未來之發展。	1. 165 專線從剛成立時之諮詢服務，為回應民眾之需求，服務項目一直在增加，除諮詢、檢舉、報案外，也增加攔阻匯款、執行異常電話停斷話務、詐騙情資分析與預防詐騙宣導等，增加使用率與攔阻成功率，進而減少民眾被騙。 2. 近年來 165 專線行銷策略亦趨多元，已創造了它的品牌，但宣導廣度與深度宜結合企業增進效果，未來可加強辦理。 3. 165 專線擁有大量詐騙情資資料庫，可將資料分析，提供外勤單位作偵防、查處或預防宣導。 4. 165 專線的服務，若由銀行端能加強關懷提問或電信業者能加裝偵測與標示系統，讓民眾可清楚辨識是來自境外詐騙電話，以及網路之安全管制等，以及跨部會的協調合作，仍待努力。 5. 165 專線功能與任務不斷的擴張，未來亦可能成為兩岸跨境反詐騙情資交換平台，惟目前仍為任務編組，人員亦均借調，應思考是否予以法制化。
2011	康健浚[10]	兩岸跨境詐欺犯罪	探討分析在 2009 年 4 月 26 日簽訂「海峽兩岸共同	台灣電信詐欺集團實施跨境犯罪盛行多年，在檢警機關不斷努力掃蕩之下，

[9]黃雪蘭，2010，政府防制詐騙犯罪政策行銷之研究－以「警政署 165 反詐騙諮詢專線」為例世新大學行政管理學研究所，碩士論文。

[10]康健浚，2011，兩岸跨境詐欺犯罪手法之分析與其防制策略之研究-以電信詐欺為例，中央警察大學外事警察研究所，碩士論文。

		手法之分析與其防制策略之研究-以電信詐欺為例	打擊犯罪和司法互助協議」，作為兩岸政府間推動共同打擊犯罪相關措施之準據。協議簽署後，在兩岸共同打擊犯罪合作策略及運作機制之現況為何，是否在執行上面臨困境，以及對打擊跨境犯罪之成效如何？	集團成員一一落網接受法律制裁，導致集團成員人力有限，而漸漸演變成車手集團與收購人頭帳戶集團結合為一團，車手、外務角色相同，領取贓款兼作收購人頭帳戶；車手集團須兼顧非法電信平台；收購人頭電話作業也漸與收購人頭帳戶集團分開，轉為獨立作業，一人跑單幫型態；詐欺組織也漸熟悉警方辦案方式，從使用電話上精進電信、用語技術，並實施話流管理，迫使警方難以追緝。
2012	何瑞玲[11]	詐騙集團是說故事高手？－從敘事理論解構詐騙集團的教戰手冊	在近幾年的台灣社會中，民眾對詐騙已經不再陌生了，政府除了成立 165 反詐騙專線之外，還砸下許多經費對民眾進行反詐騙的宣傳，但卻仍有上百億元的金錢被騙走，被害人除了有知識水準不高的民眾之外更不乏有高社經地位的科技新貴或是退休公務員等，可見詐騙案件與受害者的背景與教育程度無關。難道詐騙集團真的具有某種特殊能力，能讓受害者毫無警覺的付出大筆金錢?他們是如何突破受害者的心防，能夠不著痕跡的讓受害者越陷越深?	所有的詐騙案件，其實詐騙集團都有一本"教戰手冊"來做為詐騙成員和受害者聯繫的劇本，當我們將這本手冊視為一份故事腳本，透過敘事理論來分析這本「教戰手冊」，我們可以發現最後讓故事產生說服效果的其實是受害者本身的經驗投射，以及當下被詐騙集團所阻絕的情境所衍生出的結果，在這樣的狀況下，即便是政府在反詐騙文宣中極力宣導「檢察官不會監管帳戶或存款」或是「警察不會派人保管民眾的金錢」，由於受害者已經深深的陷入了詐騙情境，很難清楚的思考事件的真假，在這樣的狀態下，反詐騙的宣傳之所以沒有對受害者產生效應就不難理解了。政府要讓反詐騙宣傳有效果應改變方式，除了讓民眾能夠辨識事件真假之外，也應讓民眾知道當民眾捲入不法事件時可有哪些措施，同時再透過宣導短片將檢察官或是警察的辦案方式與正式流程讓民眾了解，不會因無知而繼續受騙，這樣才能真正的落實對民眾反詐騙的宣導。
2014	丁靖[12]	偵辦兩岸跨第三地電信網路詐欺犯罪之探討-以 0310 專案為例	以「0310」專案為個案研究的標的，探討專案中對於偵辦兩岸跨三地電信網路詐欺案件所觸及的學說理論，包括電信網路詐欺犯罪之演進、兩岸合作打擊犯罪及協議沿革、全球化及共同打擊犯罪理論、司法互助性質與類型等議題，蒐集、歸納、分析兩岸學者的研究著作，並提供偵辦實務上的問題綜合討論。	偵辦兩岸跨第三地電信網路詐欺案件，可依發起前置階段、調查取證階段、司法追訴階段，就各階段的主題、類別、重要概念以系統化整理方式，逐項闡述討論，並提出日後研究此類案件的討論方向，以及擴大詐欺罪刑之嚇阻效果及提升兩岸跨第三地案件證據規格及偵查能力之建議，希冀對偵辦跨境電信網路詐欺案件有所助益。
2013	紀延熹[13]	海峽兩岸跨境電信詐欺集團犯罪歷程之研究-以假冒機構詐欺模式為例	探討集團電信詐欺犯罪如何進化為跨境電信詐欺犯罪及其相關偵查、刑事(預防)政策之優劣利弊，希能對電信詐欺犯罪有更全面且深入之了解，並提出相關改進建議，以防杜該類犯罪於我國之猖獗盛行，維護我國內政之安定與經濟秩序之衡平。	1. 跨境電信詐欺集團吸收之成員普遍有教育程度不高、收入來源不穩定、收入低、以從事高勞力、低技術性質工作為主、有吸食毒品之惡習且嗜好前往酒店消費飲酒作樂等特性； 2. 集團成員之招募以透過近親團體介紹、拉進為主要來源，機房與宿舍通常距離鄰近，惟須分開承租以躲避警方查緝，據點之設立多在沿岸發達城市； 3. 詐騙成功與否，關鍵在於被害者身旁缺乏監控者； 4. 跨境詐欺集團成員無固定薪水，收

[11]何瑞玲，2012，詐騙集團是說故事高手？－從敘事理論解構詐騙集團的教戰手冊，國立政治大學傳播學院碩士在職專班，碩士論文。

[12]丁靖，2014，偵辦兩岸跨第三地電信網路詐欺犯罪之探討-以 0310 專案為例，中央警察大學刑事警察研究所，碩士論文。

[13]紀延熹，2013，海峽兩岸跨境電信詐欺集團犯罪歷程之研究-以假冒機構詐欺模式為例，國立臺北大學犯罪學研究所，碩士論文。

				入多寡係以詐騙業績比例分酬、流動率高，集團內部管理與處罰不講究、各集團成員間並無往來，社交地點以酒店場所居多，而成員若擁有資金、詐欺話術教戰手冊、經營模式，易脫離原集團另組詐欺集團等特性； 5. 跨境電信詐欺集團係一有組織結構、分層負責、廣泛運用科技、網路提升犯罪技術、日新月異之犯罪集團。
2014	吳秋宜[14]	全球化下建構兩岸共同打擊跨境犯罪機制之研究—以臺陸菲電信詐欺案為例	藉由研究跨境電信詐欺案例及深度訪談等方法來探討 1. 「海峽兩岸共同打擊犯罪及司法互助協議」的侷限。 2. 現行兩岸及東南亞國家打擊跨境犯罪的管道及模式。 3. 電信詐欺犯罪自大陸蔓延東南亞各國成因。 4. 案例研析實務運作所突顯之問題。 5. 現行兩岸與東南亞各國合作打擊跨境電信案件面臨之困境。 6. 兩岸合作與東協建立多邊打擊跨境犯罪機制之機會與挑戰等問題。	在全球化下建構兩岸共同打擊跨境犯罪機制，可以從加強及增訂兩岸跨第三地合作共同打擊犯罪協議、廣泛建立臺灣與東南亞國家之官方及非官方等多元聯繫管道、加強派駐聯絡官功能、兩岸攜手與東南亞國家建構多邊共同打擊跨境犯罪機制、深究跨境犯罪成因、律定各國共同偵查及調查取證程序、務實從單位對單位的個案合作推進到簽署正式司法互助協議等面向來推展與落實。
2015	賴明宏[15]	詐騙犯罪偵查措施之研究-以臺北市、基隆市為例	1. 藉由「文獻探討」與「官方次級資料」分析為何基隆市詐欺犯罪偵辦破獲率會比全國及臺北市高。 2. 藉由「文獻探討法」與「深度訪談法」等 2 種方式，針對基隆市與臺北市警察局偵查詐欺的個別作法作對照。 3. 分析歸納臺北市與基隆市警察局刑警大隊偵防詐欺犯罪的基層偵查人員及督導管理職級幹部人員等多方人士之訪談結果，提出我國警察機關詐騙犯罪偵查措施之改革策略與建議，以精準打擊詐欺犯罪及提升破案率。	1. 候用偵查人員甄試增訂電腦科目測驗。 2. 提高單位預算、充實軟硬體設備。 3. 補足專責隊人力，落實偵辦詐欺工作。 4. 建立專屬獎勵規範，激勵打擊詐欺意願。 5. 中央統一規劃詐騙偵查人員教育訓練。 6. 協調其他政府部門或民間單位加入共同防制詐騙。 7. 建立女警友善外勤工作環境。 8. 詐騙偵查單位納入正式編制。
2015	黃文喜[16]	退休族群理財特徵與易受詐騙特徵之研究	1. 探討 55 歲以上成年人之個人背景資訊、財務管理與詐騙經歷。 2. 分別深入探討其理財特徵、模式，與受詐騙族群之特徵。 3. 依據研究結果分別提出金融機構與退休族群接觸時的建議參	1. 理財特徵的部分退休族群中共可分為「保險理財型」、「積極投資型」、「多元投資型」、「儲蓄理財型」四種不同理財特徵之族群，「保險理財型」以投資保險為主，「積極投資型」偏愛股票投資，「多元投資型」使用較多的理財工具，「儲蓄理財型」則以儲蓄作為主要理財方式。 2. 易受詐騙特徵的部分，「基本金融行

[14]吳秋宜，2014，全球化下建構兩岸共同打擊跨境犯罪機制之研究—以臺陸菲電信詐欺案為例，國立中興大學國家政策與公共事務研究所，碩士論文。

[15]賴明宏，2015，詐騙犯罪偵查措施之研究-以臺北市、基隆市為例，國立臺灣大學政治學研究所，碩士論文。

[16]黃文喜，2015，退休族群理財特徵與易受詐騙特徵之研究，國立政治大學統計學系，碩士論文。

			考，與詐騙預防之建議。	為分數」為重要的判斷因素，分數較低的人有較高的機率被詐騙成功。「學歷」、「居住情況」、「年齡」能夠與「基本金融行為分數」共同作用，更詳細地找出易受詐騙之特徵。擁有較高「詐騙知識分數」的人未必會因為懂得較多的詐騙知識而降低被詐騙成功之機率。
2015	陳順和[17]	電信詐欺犯罪模式與防制對策之研究—以通訊網路匯流為核心	1. 探討前端電信詐騙機房的電信詐騙話務路由，尋求有效防制對策。 2. 採用質性與量化並重方式，以臺灣地區司法警察實務機關自 2009 年開始，與大陸地區各省公安廳共同破獲電信詐欺案件等官方資料抽樣樣本，以及刑事警察局 165 反詐騙諮詢專線統計資料分析。 3. 再針對電信詐騙集團主嫌與具有實務經驗的專家進行質性訪談，最後進行臺灣地區刑事專責偵辦新型態詐欺犯罪專責隊及科偵組等為抽樣對象，實施問卷調查。 4. 希望彙整出針對電信詐欺犯罪偵查與預防的實務經驗與困境，形成有效防制對策。	1. 通訊網路匯流的電信詐欺犯罪特性，電信詐騙機房是跨境詐欺犯罪成功關鍵，詐騙話務路由隨著匯流後呈現 IP 化、雲端虛擬化、跳台層轉化、委外分工細膩化、通訊多元化(Wi-Fi 機房、4G+ Wi-Fi 機房及洗錢機房)等情形，且有逐漸出現智慧型手機通訊軟體 LINE 詐騙新手法。 2. 整個電信詐騙機房架設關鍵在於系統商協助技術支援。 3. 兩岸合作共同打擊跨境電信詐欺犯罪各項專案具有壓制犯罪成效，但是 2014 年後呈現「犯罪飽和」現象。 4. 犯罪者及被害者與各種詐欺犯罪手法具有一定關聯性。 5. 受試的反詐騙專責刑事警察人員皆認為：2014 年元月份新修正「通訊保障及監察法」對於電信詐欺犯罪偵查有一定程度影響，電信網路匯流趨勢造成電信詐欺犯罪衝擊，增加警政署刑事警察局「165 反詐騙諮詢專線」再升級及跨國境司法互助具有偵查與預防效能，制定通訊與網路匯流管制政策法律，才能具體有效遏止跨境電信詐欺犯罪。
2015	李志祥[18]	通訊詐欺被害歷程之研究-以 ATM 解除分期付款為例	1. 利用官方資料中分析 ATM 解除分期付款詐欺模式之被害特性，進行犯罪學理論之檢證 2. 採取個案研究方式，選取具代表性之 ATM 解除分期付款被害個案進行實地訪談，分析被害人特性、標的及歷程。 3. 根據研究發現，提出防治建議。	1. ATM 解除分期付款詐欺被騙型態為一歷程。 2. ATM 解除分期付款詐欺犯罪與個人特性、金錢價值觀、防詐認識、ATM 功能認知有關。 3. ATM 解除分期付款詐欺犯罪類型與監督者缺席有關。

由表 1 歸納重點如下：

1. 近年詐欺犯罪類型中以資通訊方式的詐欺犯罪類型居多，而且隨著科技及網路的發達，詐騙的工具更不斷翻新。
2. 跨兩岸的詐欺犯罪案件偏多，因而引起更多研究者的興趣，大陸地區相關議題的研究也相對地比其他地區多。
3. 基於多數研究者提出政府對防制詐欺犯罪的建議，以及現實生活中，老百姓的生命財產受到嚴重威脅，因此內政部警政署刑事警察局於 105 年 8 月 24 日正式成立「打擊詐欺犯罪中心」，強調該中心的成立最主要目的，在於全力推展跨部會、跨機關及跨領域之合作，落實執行各項反詐工作，並積極查緝詐欺犯罪，以確保人民免於遭受詐欺犯罪，確保全民

[17]陳順和，2015，電信詐欺犯罪模式與防制對策之研究—以通訊網路匯流為核心，國立中正大學犯罪防治研究所，博士論文。

[18]李志祥，2015，通訊詐欺被害歷程之研究-以 ATM 解除分期付款為例，國立臺北大學犯罪學研究所，碩士論文。

財產安全。

三、詐欺(騙)集團

隨著時代的發展，詐欺(騙)集團已經出現跨國趨勢。「詐欺集團」係指三人以上意圖為自己或第三人之不法利益為宗旨，而結合從事各類詐欺之犯罪活動，並以犯罪所得來維持其生計與收入，具有集團性、常習性等特性之組織。

（一）詐欺(騙)集團組織架構

詐欺(騙)集團組織架構分為「集團首腦」、「車手」、「收購人頭帳戶與電話成員」、「建置非法電信平臺（機房）成員」等 4 大部分。[19]

1. 集團首腦：負責統籌指揮，並根據事先所編輯的詐騙劇本、模式，以接力撥打電話方式向不特定民眾詐騙。
2. 車手：負責提領贓款，並將贓款透過地下匯兌交付集團首腦。
3. 收購人頭帳戶與電話成員：負責將收購來的人頭帳戶、電話提供集團首腦、建置非法電信平臺成員，作為與被害人聯繫，規避警方查緝資金流向等工作。
4. 建置非法電信平臺成員：負責尋找有利建置地點，透過網路與通訊的大量性轉換傳輸增加隱密性，企圖規避警方查獲，並節省犯罪成本。

（二）詐欺(騙)集團常用詐騙方法及防範方法，詳如表 2。

表 2：詐欺(騙)集團常用詐騙手法及防範方法

詐騙方式	詐騙手法	防範方法
網路購物詐騙	被害人透過購物台或拍賣網站購買東西，然後接到「賣家」或「網站員工」來電，聲稱「因簽單登錄錯誤」，將會造成「買家」的帳戶每個月自動扣款，為避免「買家」損失，必須再去操作一次「自動提款機」，因而聽從歹徒指示按鍵操作，從「英文操作」開始，輸入所謂的代碼，該代碼其實是「匯款金額」與「歹徒帳號」，直到轉帳交易成功，帳戶內的存款被轉走，才發現被騙。	1. 養成查證習慣，勿聽信不明來電指示。 2. 自動提款機沒有取消約定扣帳功能，千萬不要依照電話指示操作自動提款機。 3. 來電顯示不能信，請掛斷來電撥打銀行客服電話查證，或撥 165 專線查證，勿聽信來電電話。 4. 0200、0800、0900、0204 起頭之電話都是虛擬碼，只能單方聽電話，無法撥出，亦不會顯示號碼於被害人手機上。
假冒警政、司法公務機關詐騙	假冒警察機關名義，以電話通知民眾，因查案時發現民眾遭冒名申辦帳戶，涉嫌洗錢詐欺，已將案件移送檢察官偵辦，稍後交由假冒檢察官，告知曾傳喚出庭，要求查清帳戶內資金流向，民眾必須將存款領出交給法院保管或匯款至歹徒所利用國家安全(人頭)帳戶，並告訴民眾於案情釐清後就退還，進而騙取錢財。	1. 法院或警察機關辦案，不會收取當事人現金、亦不會要求匯款。 2. 法院或警察機關不會監管當事人帳戶。 3. 法院不會用傳真方式，將傳喚書送給當事人，一定會以掛號信函送達。
網路援交詐騙	運用「援交」並結合「羞於告知外人」之心理，對民眾恐嚇方式如「找黑道擺平」、「電腦故障」等藉口，誘騙民眾去操作提款機，再不斷打電話騷擾、恐嚇被騙者，甚而再假藉國家金	1. 網路交友要謹慎，最好不要透露住址、學校、公司、家中電話等資料，以免成為歹徒恐嚇把柄。 2. ATM（自動提款機）已成為歹徒最佳詐騙工具，切勿聽從來電電話指示操

[19](1)引用資料來源：謝浚鋒，2009，電信詐欺犯罪模式與偵查之研究，國立臺北大學犯罪學研究所，碩士論文。(2) 部分內容修改。

	融機構以辦理「安全帳戶設定」名義，清空被害人所有存款。	作按鍵。 3. 一旦發現操作 ATM，存款遭轉走，應立刻報案，只有報案，才能終結歹徒恐嚇。
網路聊天室投資詐騙	於網路聊天室尋找詐騙對象，再自稱是海外投顧公司經理藉機與詐騙對象攀談，以建立感情與互信基礎，建立男女朋友或更親密關係，歹徒見時機成熟便投下「一本可萬利」投資的誘餌，同時製作假的海外投顧公司網頁，待取得被騙人信任後，再陸續掰出繳交手續費、保證金、公基金、帳戶管理費等名目詐騙錢財。	1. 近期網路投資詐騙手法愈加細膩、有耐心，從網路交友、談情一段時間，取得詐騙對象傾心愛慕。 2. 再將話題帶入「投資」、「中獎」，甚至以「合資」為誘因，讓人降低戒心，一再匯款。 3. 呼籲網路交友千萬勿涉及金錢借貸或投資，並可透過網路向海外網友徵詢，掌握正確資訊，以免遭詐騙血本無歸。
假綁架詐騙	歹徒掌握被害人親屬基本資料，更鎖定詳細之地域範圍，針對同一地區、同一學校或是同一班級的家長進行詐欺，並已初步以讓民眾無法判別其真實性而受騙，手法上運用匯款交付詐財。	1. 父母或家人應互相留下第二種聯絡方式，如同學、好朋友或學校導師電話，以備緊急聯絡。 2. 歹徒通常利用當事人緊張焦慮心理，以不准掛斷電話方式遙控，並要求家人出門領款，遇此情況，請先行掛斷電話，再透過撥打「104 查號台」、「165 反詐騙專線」或學校電話進行查證。 3. 165 反詐騙專線電話，可以協助聯絡疑似遭歹徒綁架之親人，切勿在尚未查明情況前匯款給歹徒。
假親友借錢詐騙	詐騙歹徒利用「妹妹」、「同學」、「朋友」、「客戶」等角色，以人際間的噓寒問暖，及「同情心」的操弄，以亂槍打鳥式的電話探詢，重要特徵就是「急需金錢調度或應急難」，從而詐騙接電話的人匯款。	1. 接到不明來電，特別是不願主動告知姓名時，切勿因「礙於情面」而任意猜測對方姓名，務必要求對方明確告知姓名。 2. 若遇到久未謀面之親友開口借錢的電話，最好回答：「對不起，我現在不方便說話，等一下再回你的電話」，然後將這通可疑電話掛斷。 3. 找出親友聯絡電話簿，用自己登錄的親友電話號碼，主動撥電話詢問是否真要借錢，以確認是否為詐騙電話。
假發放生活津貼，到家詐騙老人	詐騙歹徒透過不法管道，取得獨居高齡長者的個人資料，假冒社會局或退輔會人員撥打電話給被害民眾，偽稱目前正在發放老人生活津貼，並假冒工作人員到家協助申請，藉故填寫資料騙取存摺及印章，趕往銀行領出被害人存款。	1. 生活津貼發放被詐騙的對象多為獨居、高齡長者，主要利用老人家較少接收社會資訊，且年事已高，視力、警覺性較差，動作遲緩，較易受騙。 2. 公務人員證件容易偽造，如有配戴公務機關識別證的陌生人來訪，應先問對方姓名及服務單位，再打電話向所稱單位查證有無此人及來訪目的。 3. 家中有獨居年長者，對不明來訪者應提高警覺，勿輕易讓陌生人進入家中，更不可任意出示或交付銀行存摺、印章。
分類廣告求職、貸款遭騙提款卡	詐騙歹徒登報收買或於求職、貸款廣告中騙取人頭帳戶，將不知情民眾於應徵或申辦貸款時交出提款卡，同時告知歹徒密碼後，直到存摺中發現莫名其妙的進、出帳紀錄，不但工作、貸款沒著落，才發現已被利用成為詐欺人頭戶。	1. 報紙求職廣告暗藏陷阱，應徵時切記勿交出存摺、提款卡等重要證件，以免成為詐欺人頭戶，成為詐欺幫兇，必須面對司法，受到制裁。 2. 若因一時不察已經交出提款卡，應盡快以電話聯絡發卡銀行通知停用，並將廣告剪報、相關證件帶往就近派出所報案，以提供警方釐清案情。

網拍賣家詐騙	詐騙歹徒以賣家低於行情價網拍，並告知若不匯款將賣給別人等心理操作，不斷催促買家匯款，許多人受到「奇貨可居」的心理操作影響，匆促匯款後才發覺被騙。	1. 詐騙第一誘因是「低於行情價」，網友切勿因小失大，掉進歹徒所設陷阱。 2. 檢視賣家過去的拍賣評價，若原本是賣衣服、墨水匣、保養品，卻突然開始賣相機，就有問題。 3. 3、賣家過去交易紀錄「只有買、沒有賣」就有可能是透過小額交易來換取好評價，以騙取買家信任。 4. 如果賣家拒絕「當面交易」，並以住在屏東、花蓮、美國、日本等理由，表示不便「當面交易」，堅持只能先收款才寄貨。 5. 當拍賣商品具有「預訂性質」時，為求謹慎，應向有口碑店面或有信用商家訂購，以防預訂詐騙。
就業被騙投資	歹徒以人頭名義成立紙上公司，應徵並予錄用被害人，利用上班時間討論投資，製造投資國外期貨有良好利潤誘因，邀被害人加入投資，俟被害人陸續投資並被榨乾後，就以不適任為由開除，再透過同事私底下聯絡方式，降低被害人戒心，歹徒將錢騙到後，隨即惡性倒閉，被害人始知被騙。	1. 期貨交易法及相關法令，對於期貨商的設立、運作及從業人員等皆有嚴謹規範，合法期貨商的業務與財務運作，均須受主管機關監督，期貨交易一定要透過國內的外匯指定銀行，相關資訊可上行政院金管會網站查詢。 2. 求職時千萬不要相信他人耳語，就冒然投資，務必要花時間了解操作內容，認識詐騙案例，並將自己處境與案例相比較，凡是網路看盤、同事獲利、臺灣未開放的交易，都是詐騙陷阱，勿因一時貪念後悔無窮。

資料來源：臺北市政府法務局[20]。

資料整理：本研究。

參、研究方法

一、資料來源

本研究從我國「司法院法學資料檢索系統」（網址：http://nwjirs.judicial.gov.tw/Index.htm）所提供的【裁判書查詢】項目中，刑事裁判類別中，逐一選取各地方法院，利用【全文檢索詞語】功能，在欄位內輸入「(詐欺集團+詐騙集團)&詐欺罪」，判決日期為 2012 年 1 月起至 2016 年 6 月止的相關案件，透過立意抽樣法，共得 2,155 件樣本數，透過程式過濾排除無罪、羈押等無效案件後，有效樣本數為 1,712 件。

二、研究工具

為能順利完成研究目的，本研究所採用的軟體，包括如下：

(一)UniPDF.exe：將判決書(PDF 檔)轉為文字檔(TXT 檔)。

(二)SAS 預先處理 VBA 巨集程式(由本研究人員自行開發)：Excel 文字檔轉換成 UTF-8 編碼系統，及刪除雜訊詞和無作用的符號。

(三)透過 VBA 巨集程式產生「詐騙集團」或「詐欺集團」[21]的累犯二元屬性值。凡案件中有「累犯」為是者設定為 1，沒有者設定為 0。

[20] http://www.legalaffairs.gov.taipei/ct.asp?xItem=34033515&ctNode=56238&mp=120034

(四)SAS Text Miner 文字採礦模組：SAS Enterprise Miner 14.1 版，自動將文件內容歸類成數個主題(Topics)。

(五)SAS Enterprise Guide 7.1 版：從數個主題與累犯進行資料採礦，以獲得詐欺(騙)集團累犯之同質與異質特徵。

三、作業環境

在個人電腦 64 位元，Windows 7 作業系統下進行各項文書編輯，採礦之處理與分析等工作。

四、處理過程

在處理過程方面，可分為下列階段：

(一)蒐集與轉檔階段：

1. 透過「司法院法學資料檢索系統」網站取得本研究樣本，下載與詐欺相關之 PDF 檔裁判書(檔案)。
2. 當判決書中有出現(詐欺集團+詐騙集團) AND 詐欺罪」等關鍵詞者，歸屬詐欺(騙)集團案件。
3. 再經由 UniPDF.exe 將 pdf 檔案轉換成 txt 檔案，透過 Excel VBA 程式將它們分類與儲存在不同年份的資料夾內。提醒：在 Windows 作業系統環境下，SAS TM 文字採礦模組可接受中文字元的 ANSI、UNICODE(Little/Big-Endian)和 UTF-8 等編碼系統；提供資料處理用文件檔案數量至少 15 個。

(二)刪除控制與空白字元階段：利用自行撰寫之「SAS 預先處理 VBA 巨集程式」執行第一步驟-刪除空白及控制字元。另 SAS Text Miner 的每一個欄位容量最大值為 32KB。提醒：SAS EG 所稱的 32KB 是指半形字元而言，故被處理的文字檔案只能限於 32K/2 個中文字而已。

(三)檔案輸出：將處理後的檔案輸出以利後續的文字採礦及資料採礦處理。

(四)文字採礦處理：執行 SAS Text Miner 對裁判書進行同義字、忽略詞性、斷詞、詞頻等處理。SAS Text Miner 是 SAS Enterprise Miner (EM)的一個 plug-in，底下包含七個模組，其中「文字匯入」是做資料集處理的模組；「文字剖析」、「文字篩選」是根據自然語言處理的模組；「文字歸類」、「文字群集」、「文字規則產生器」、「文字設定檔」則是進行分析演算法的模組。有關文字採礦處理程序如圖 1 所示，其流程說明如下：

1.文字匯入階段：將分析用的判決案件內容彙總成一個檔案後，轉換成 SAS 資料集格式，再匯入至本階段，準備處理。

2.文字剖析階段：在屬性項下/剖析/語言/要選擇中文，剖析變數/TM_Contents，(角色：文字)，不同的詞性設定為否，名詞群組設定為否。

3.文字篩選階段：在屬性/詞語篩選/文字的最少數目設定為 1，次數加權設定為無，詞語權數亦設定為無。

4.文字歸類階段：屬性/學習歸類/多重詞語歸類的數目設定為 30。

[21]有些法官採「詐騙集團」一詞，另有些法官則採「詐欺集團」。

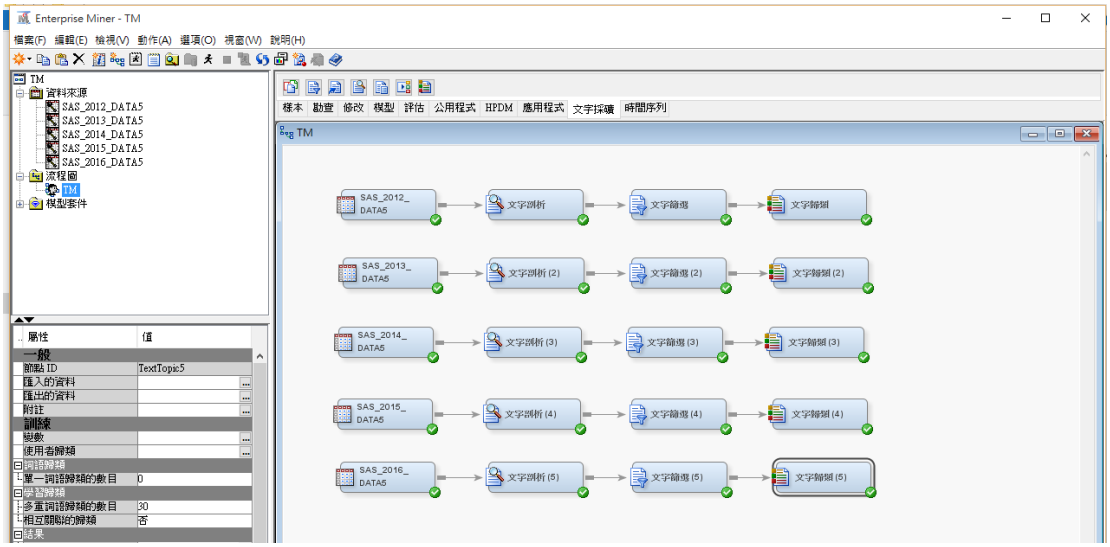

圖 1：詐欺(騙)集團累犯特徵文字採礦過程圖

(五)資料採礦流程：有關資料採礦處理程序如圖 2 所示，其流程說明如下：

1. 執行 SAS Enterprise Guide 7.1 版，由開啟欲採礦檔案(文字採礦結果檔案)，然後在工作選單下，點選迴歸項下的線性迴歸。
2. 分別將 2012-2016 年的 5 個檔案，進行線性迴歸，得到線性迴歸結果。
3. 線性迴歸結果中，若該類變數的參數估計值為負值，則此特徵就不是累犯特徵。

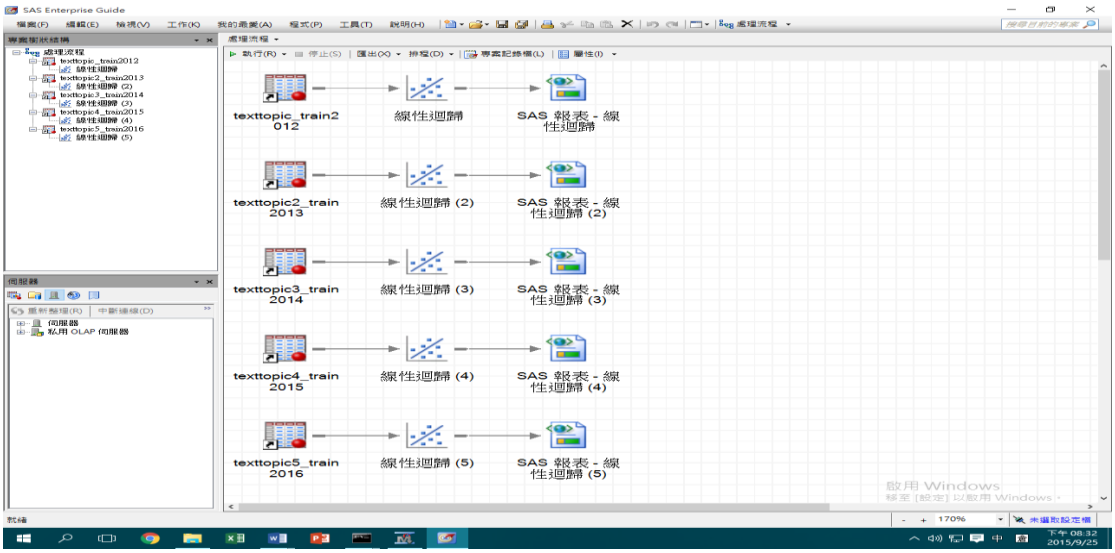

圖 2 詐欺(騙)集團累犯特徵資料採礦流程圖

五、研究限制

由於人力與時間限制，故本研究只針對 2012 年 1 月起至 2016 年 6 月底止的裁判書作為詐騙集團累犯研究對象，共 1,712 件裁判書(樣本數)。

肆、研究結果

一、敘述統計

本研究透過內容分析法，從 2012 至 2016 年有效樣本 1,712 個司法案件中，詐欺(騙)集團具有累犯紀錄的案件數達 597 件，占全部的 34.8%(逾 1/3)，即每 3

件詐欺(騙)案件中，就有 1 件是累犯案件，顯見國內詐欺(騙)集團累犯之嚴重程度，如表 3 所示。

表 3：臺灣地區從 2012 年 1 月-2016 年 6 月期間集團性詐騙案件統計(N=1,712)

年份別	詐欺(騙)集團案件數	詐欺(騙)集團累犯案件數	所占比例(%)
2012	237	109	45.99156
2013	347	132	38.04035
2014	331	116	35.04532
2015	437	130	29.74828
2016	360	110	30.55556
總計	1712	597	34.8715
月平均	30.57	10.66	34.87

二、詐欺(騙)集團累犯特徵採礦

本研究透過 SAS 資料採礦軟體，以前述 30 群歸類作為輸入角色(Input Role)，「詐欺集團」或「詐騙集團」累犯特徵作為目標角色(Target Role)，來針對 2012 年和 2016 年之裁判書詞語進行線性迴歸分析。詐欺(騙)集團累犯特徵資料採礦結果如下：

(一)從表 4 採礦結果得知，從事電話詐欺取財之分工合作模式：

(1) 取得筆記型電腦、數據機、教戰手冊、大陸電話號碼筆記等從事電話詐欺之設備及資料。

(2) 取得承租房屋、採購相關電話詐欺設備等所需資金。

(3) 俟前開電話詐欺機房先後成立後，即依前開詐騙集團所提供之資料對大陸地區人民進行詐騙，第「一線」(前線)人員便向該大陸地區人民佯稱有傳票未領、第二線(中線)人員便向該大陸地區人民佯稱其身分資料遭冒用，涉及金融刑事案件，必須配合刑事調查，其金融帳戶須接受國家監管云云，再將該通電話轉接至負責假冒金融監管局人員之第三線(後線)人員及第三線人員遂指示該大陸地區人民將其帳戶內之資金匯入某帳戶，然後詐騙得逞。

(二)2012 年詐欺(騙)集團累犯案件數為 109 件，占總樣本數的 46%，其中有 34 件是此種類型的累犯，佔了累犯案件數的 31%，即 10 件中就有 3 件。

表 4：2012 年對詐騙集團累犯特徵具顯著貢獻之採礦結果(N_1=237)

歸類(自變數)	參數估計值	標準誤	T 值	Pr>ltl
一線	0.75713	0.34217	2.21	0.0280
R 平方=0.3916；應變數平均值=0.45992；變異係數=90.66139；F=4.42；(Pr>F) < 0.0001。詐欺(騙)集團累犯案件數為 109 件，占總樣本數的 46%。				

(三)從表 5 採礦結果得知，「詐騙集團累犯的特徵」：有共犯是以提供「提款卡」供詐騙集團成員作為提領及匯出款項之用，幫助完成詐騙工作。以「馬來西亞」為首的跨國詐騙集團，透過某「牌行動電話」，指揮機房的第「二線」詐欺人員。另「法拉利」車手集團以「AMG」詐騙機房為中心，發送群呼，使大陸地區民眾陷於錯誤回撥，該回撥電話即經由設定路徑轉接至詐欺機房，第一線詐騙人員佯稱為大陸地區法院服務人員，經向大陸地區民眾謊稱確認有個資遭冒用或欠費未繳後，旋將電話轉予第二線詐騙人員接聽；該第二線詐騙人員即訛稱為大陸地區公安人員，要求民眾提供個人資料後，復將電話轉予第三線詐騙人員；該第三線詐騙人員詐稱係檢察官，向民眾騙稱其等涉

嫌洗錢案件，要求其等將錢存入指定帳戶內監管，致使民眾因而陷於錯誤，依照渠等之指示，將款項匯至大陸地區銀行帳戶內。亦有「機房」透過有犯意的「公關」小姐共同進行詐騙。

表 5：2013 年對詐騙集團累犯特徵具顯著貢獻之採礦結果(N_2=347)

歸類(自變數)	參數估計值	標準誤	T 值	Pr>ltl
簡易判決,提款卡,幫助	1.91178	0.47364	4.04	<.0001
交易明細資料	0.92161	0.19364	4.76	<.0001
AMG,法拉利	0.81544	0.26230	3.11	0.0020
筆記型電腦,行動電話	0.71631	0.22438	3.19	0.0016
公關	1.57742	0.31331	5.03	<.0001
機房,二線人員,群發,二線,電腦	1.49981	0.30015	5.00	<.0001
R 平方=0.3951；應變數平均值=0.38040；變異係數=104.01595；F=6.88；(Pr>F) < 0.0001。詐欺(騙)集團累犯案件數為 132 件，占總樣本數的 38%。				

(四)從表 6 採礦結果得知，「詐騙集團累犯的特徵」:「犀牛」詐騙集團使用的是「諾基亞」手機，成立的跨境詐騙集團，成員透過網路技術更改電信詐騙機房之網路顯號設定，偽裝為「大陸地區」公私部門之來電號碼，啟動網路平台自動撥號系統來進行詐騙操作。

表 6：2014 年對詐騙集團累犯特徵具顯著貢獻之關鍵詞採礦結果(N_3=331)

歸類(自變數)	參數估計值	標準誤	T 值	Pr>ltl
犀牛,諾基亞	0.49868	0.24628	2.02	0.0438
大陸地區	186.09845	52.14139	3.57	0.0004
R 平方=0.2938；應變數平均值=0.35045；變異係數=120.17637；F=4.16；(Pr>F) < 0.0001。詐欺(騙)集團累犯案件數為 116 件，占總樣本數的 35%。				

(五) 從表 7 採礦結果得知，「詐騙集團累犯的特徵」: 此詐騙集團發生地大部分來自「士林」，電話詐欺集團於機房內備有「教戰」守則，教導每個成員。詐騙集團成員將收購的「易付卡」，以上開行動電話號碼作為詐欺行為時之聯絡工具。又或者是詐騙集團成員誆稱投資港澳「運動」彩券或介紹投資「運動」網博奕公司「運動」堂口網站。

(六) 表 7：2015 年對詐騙集團累犯特徵具顯著貢獻之關鍵詞採礦結果(N_4=437)

歸類(自變數)	參數估計值	標準誤	T 值	Pr>ltl
簡易判決,門號	1.41790	0.69309	2.05	0.0414
機房,教戰	0.74494	0.25900	2.88	0.0042
運動,本金	0.69652	0.30323	2.30	0.0221
易付卡	0.71010	0.26711	2.66	0.0082
士林	1.00716	0.33236	3.03	0.0026
R 平方=0.2462；應變數平均值=0.29748；變異係數=138.42173；F=4.42；(Pr>F) < 0.0001。詐欺(騙)集團累犯案件數為 130 件，占總樣本數的 29.75%。				

(七) 從表 8 採礦結果得知，「詐騙集團累犯的特徵」: 歹徒以「大陸」地區為基地，指揮「機房」的第「二線」詐欺人員，以電話、手機簡訊通知中獎、刮刮樂、退稅費或其他類似之不法詐騙份子，為掩飾其等不法行徑，以避免執法人員

循線查緝，經常利用他人存款帳戶、印章、「提款卡」暨「密碼」，以確保犯罪所得免遭查獲。

表 8：2016 年對詐騙集團累犯特徵具顯著貢獻之關鍵詞採礦結果(N_5=360)

歸類(自變數)	參數估計值	標準誤	T 值	Pr>ltl
機房,二線,大陸	0.96091	0.34455	2.79	0.0056
幫助,密碼,提款卡	0.73826	0.34203	2.16	0.0316
R 平方=0.2388；應變數平均值=0.30556；變異係數=137.58331；F=3.44；(Pr>F) < 0.0001。詐欺(騙)集團累犯案件數為 110 件，占總樣本數的 30.56%。				

三、詐欺(騙)集團累犯特徵關鍵詞比較

本研究分別從 2012 至 2016 年的文字採礦中，分別獲得 30 群歸類，再透過資料採礦技術之線性迴歸模型，對「詐欺集團」或「詐騙集團」累犯特徵獲得具有顯著貢獻的關鍵詞。有關它們之間存在有共通與相異之特徵，如表 9。

表 9：2012-2016 年詐欺(騙)集團累犯特徵關鍵詞比較表

累犯特徵關鍵詞	2012 年	2013 年	2014 年	2015 年	2016 年
相同		提款卡,機房,幫助，二線、簡易判決	大陸	機房、簡易判決	機房,二線,提款卡,幫助,大陸
相異	一線	交易明細資料,AMG,法拉利,筆記型電腦,行動電話,公關,二線人員,群發,電腦	犀牛,諾基亞	門號、教戰,運動,本金,易付卡,士林	密碼

伍、結論

本研究結論如下：

(一) 在本研究從 2012-2016 年期間抽樣詐欺案件樣本總數為 1,712 件中，集團性詐騙累犯案件為 597 件，占總樣本數 34.87%。研究發現：100 件的詐騙案中就有近 35 件的累犯案件，所以詐欺(騙)集團累犯特徵是值得關注的。

(二) 2012-2016 年詐欺(騙)集團累犯案件數百分比各為 2012 年 46%，2013 年 38%，2014 年 35%，2015 年 29.75%，2016 年 6 月底止的 30.56%，近 4 年詐欺(騙)集團累犯案件數有逐年下降的趨勢，但今(2016)年 6 月底止又成長了一些。

(三) 隨著科技發展，詐騙集團詐騙管道開始透過網路遊戲、行動電話等等，而「幫助」關鍵詞的出現，可以得知有些人因為提供個人帳戶而被充當人頭帳戶，故被法官認定為詐欺罪的幫助犯。

(四) 詐欺 (騙)集團累犯共通特徵如下：

1. 2013 年與 2016 年詐欺 (騙)集團累犯共通特徵為提款卡,機房,幫助及二線。
2. 2013 年與 2015 年詐欺(騙)集團累犯共通特徵為簡易判決。
3. 2014 年與 2016 年詐欺(騙)集團累犯共通特徵為大陸。
4. 2013、2015 年與 2016 年詐欺 (騙)集團累犯共通特徵為機房。

(五) 詐欺(騙)集團累犯相異特徵：此相異特徵表現出來的特性為從 2012 年的第

「一線」人員，發展到 2013 的二線人員利用電腦、行動電話來做群發，到 2015 年更是有教戰手冊的出現，或是利用插有易付卡的手機交予車手，作為日後機房人員便利聯絡前往指定地點收取被害人所交付款項之用，而到 2016 年甚至已能用偽卡，在提款機鍵入密碼提領贓款，可見其詐騙手法不斷在演進中。

本研究從事詐欺(騙)集團累犯特徵的發掘，可以發現累犯使用的工具，大多與科技和網路結合，例如行動電話、電腦、機房、易付卡、提款卡及密碼等，詐騙工作人員分第一線、第二線及第三線，更用教戰手冊來從事訓練。另發生地區則以臺灣及大陸居多，亦即跨兩岸的案件相當多。本研究結果與表 1 的文章的研究結果不謀而合，皆是歹徒利用科技及網路的資通訊詐欺類型居多，而且也是以發生在臺灣與大陸兩岸之間為多數。因此希望藉由此研究為開端，將來從事更多相關案件的研究分析，以提供執法機關在研擬防制詐騙對策時之參考。

參考文獻

何瑞玲，2012，詐騙集團是說故事高手？－從敘事理論解構詐騙集團的教戰手冊，國立政治大學傳播學院碩士在職專班，碩士論文。

吳秋宜，2014，全球化下建構兩岸共同打擊跨境犯罪機制之研究—以臺陸菲電信詐欺案為例，國立中興大學國家政策與公共事務研究所，碩士論文。

李志祥，2015，通訊詐欺被害歷程之研究-以 ATM 解除分期付款為例，國立臺北大學犯罪學研究所，碩士論文。

紀延熹，2013，海峽兩岸跨境電信詐欺集團犯罪歷程之研究-以假冒機構詐欺模式為例，國立臺北大學犯罪學研究所，碩士論文。

康健浚，兩岸跨境詐欺犯罪手法之分析與其防制策略之研究-以電信詐欺為例，中央警察大學外事警察研究所，碩士論文，2011。

許清事，2005，通訊金融詐欺犯罪成因與防制－以臺北縣處理涉及人頭之詐欺案件為例，國立臺北大學犯罪學研究所，碩士論文。

陳順和，2015 電信詐欺犯罪模式與防制對策之研究—以通訊網路匯流為核心，國立中正大學犯罪防治研究所，博士論文。

曾進忠，2010，資通訊詐欺犯罪特性及歷程之研究，國立臺北大學犯罪學研究所，碩士論文。

黃文喜，2015，退休族群理財特徵與易受詐騙特徵之研究，國立政治大學統計學系，碩士論文。

黃珮如，2010，影響電話詐騙犯罪被害因素之研究，中央警察大學犯罪防治研究所，碩士論文。

黃雪蘭，2010，政府防制詐騙犯罪政策行銷之研究－以「警政署 165 反詐騙諮詢專線」為例世新大學行政管理學研究所，碩士論文。

蔡田木(2009)，兩岸詐欺犯罪趨勢與防制對策之探討。展望與探索 第七卷第七期，頁 86-95。

賴明宏，2015，詐騙犯罪偵查措施之研究-以臺北市、基隆市為例，國立臺灣大學政治學研究所，碩士論文。

謝浚鋒，2009，電信詐欺犯罪模式與偵查之研究，國立臺北大學犯罪學研究所，碩士論文。