線上遊戲犯罪手法與偵查模式之研究

林宜隆　　林文龍
中央警察大學資管所教授　　宜蘭縣警察局

網際網路（Internet）的快速興起，創造出了新的網路資訊社會（Cyber Society）生活模式，上網咖打連線遊戲戰，已成了許多青少年學生的最愛。然而，在享受網路帶來便利的同時，亦產生了許多新興的犯罪問題亟待解決；各種新興的網路犯罪類型如線上遊戲犯罪（On-line Game Crimes），是過去未曾發生的，沒有案例可循，也沒有偵查模式等機制可參照，讓這些新興的網路犯罪案件成了偵查人員的燙手山芋。

目前線上遊戲犯罪在學術界及實務界中，亦尚未有較成熟的研究成果或偵查機制，因此本文擬以文獻探討法來針對網路犯罪及偵查犯罪理論等相關文獻進行探索，次由內容分析法將所蒐集的64件線上遊戲犯罪之官方文件[1]進行分析，得到線上遊戲犯罪的各項犯罪因子量化結果，及其分布的現況解析；進而推導出線上遊戲之犯罪模式，並建構出各類型線上遊戲犯罪偵查模式，再藉由專家意見指導及專業人員的深入訪問來檢視及修正犯罪模式和偵查模式，使提出之偵查模式更具完整與可行性。

壹、前言—犯罪事實認定

犯罪事實依證據認定，因此犯罪偵查工作最主要目的就是蒐集證據。在刑事證據法則中，具有證據價值者分為下列三類[2]：

一、供述證據：就是以人之供述為證據，稱之為供述證據，係以人之知覺經驗而陳述其思想內容證據方法，在實務上證據法則之「人的證據方法」應分為：被告（共同正犯）、共犯、證人（包括鑑定證人）、鑑定人（包括鑑定機關）、被害人、告訴人（或自訴人）。如被告、被害人筆錄等。

二、物的證據：物的證據係以物之狀態或存在，或以文書之意義等為證據方法，亦即以人之五官感覺作用而獲得認識之事物（證物與文書），稱其為證物或物證，物又分為一般之物及文書二種。如兇刀、書面契約等。

三、情況證據：集合得以推測犯罪事實存在或不存在之事實，即情況事實，本推理作用而為事實之認定，亦即為推理主要事實存否之事實，因其材料不同，大別分為內部徵象與外部跡象二種，又因情況事實與犯罪行為發生之時間關係的不同，乃有行為前情況與行為時情況及行為後情況之分。

貳、網路犯罪偵查程序

網路犯罪偵查最主要困難點在於偵查方向擬定、犯罪者身分確認、犯罪證據之證據力等，案情內容的迅速掌握，釐清犯

1 官方文件資料來源：內政部警政署刑事局、宜蘭縣警察局。

2 鄭厚旋，犯罪偵查學（桃園縣：中央警官學校，1988年），頁21、603-606。

罪類型及偵辦方向，往往是能否破案的關鍵。對於一直以偵辦傳統犯罪的警察人員而言，偵辦網路犯罪時難免有茫然不知所措之窘境，而以警察單位本身專業能力不足而無法受理偵辦。因此須將網路犯罪各類基本型態與犯罪偵查程序互相整合，以科學化實證研究之犯罪分析，而非以傳統犯罪偵查之經驗累積為基石[3]。

由網路犯罪之案例分析及偵查程序可以發現，網路犯罪偵查程序可分為三個階段[4]：

一、確認網路犯罪模式，藉由受害者的描述、網路的基本資料（作業系統、網路拓撲等）、偵測追蹤工具掃描（掃瞄Port之開啟狀態、稽核紀錄檔、網路基線Baseline異常行為追蹤等）解析網路犯罪者是使用何種手法攻擊或入侵網路系統。

二、清查網路犯罪者身分，可由連線登入來源追查、系統使用者資料過濾、電子郵件來源等去追蹤清查犯罪者身份。

三、逮捕犯罪者偵辦，適用一般犯罪偵查程序。

參、線上遊戲犯罪手法

從犯罪主體的範疇來看，「人」才是犯罪的主因，就線上遊戲犯罪模式的建立角度而言，除了人的因素之外，尚需考慮因素如：犯罪動機、犯罪目的、犯罪手法等等，方可有較完整模式的建立。

一、線上遊戲犯罪因子探討

剖析線上遊戲的犯罪行為，其犯罪因子類型與網路犯罪並無不同，均可歸類為犯罪動機、犯罪標的、犯罪目標及犯罪手法四類[5]，但再深入探究各犯罪因子所包含項目時則發現，線上遊戲的犯罪行為在犯罪動機部分，僅有金錢、利益、好奇心及虛榮心四項、犯罪標的部分，有虛擬寶物(電磁記錄)、金錢、服務及權限四項、犯罪目標的部分，則有角色ID（虛擬人物）、個人及遊戲公司三項，如表1所示。

表1：網路犯罪與線上遊戲犯罪之犯罪因子比較

犯罪因子	網路犯罪（林宜隆、黃明凱，2001）	線上遊戲犯罪（本研究整理）
犯罪動機	金錢與利益	金錢
		利益(金錢除外)
	好奇心	好奇心
	虛榮心	虛榮心
	報復	無
	商業競爭	無
	愛國情操	無
	其他	無
犯罪標的	資料	虛擬寶物(電磁記錄)
		金錢
	服務	服務
	權限	權限
犯罪目標	個人	角色ID(虛擬人物)
		個人
	公司	遊戲公司
	政府	無
	軍事	無
	學術	無
犯罪手法	入侵或攻擊手法	社交工程法詐騙
		傳統竊盜、詐欺手法
		偽造遊戲網站進行不法集資
		使用鍵盤記憶程式詐取
		利用遊戲管理漏洞竊取

3 許春金，犯罪學（桃園縣：中央警官學校，1996年），頁237-238。

4 林宜隆，網際網路與犯罪問題之研究（桃園縣：中央警官學校，2001年），頁71。林宜隆、黃明凱，「網路犯罪模式與偵查模式之探討」，在第六屆資訊管理學術暨警政資訊實務研討會論文集（桃園縣：中央警官學校，2002年），頁34。

5 林宜隆、黃明凱，「網路犯罪模式分析及案例探討」，在第三屆網際空間學術研究暨實務研討會論文集（桃園縣：中央警官學校，2001年），頁160-161。

二、犯罪手法

本文採以犯罪手法作為犯罪類型分類的依據，依其犯罪手法的特徵與普及性，將所蒐集案例分析後，共歸納出五種犯罪手法類型，即「社交工程類」、「傳統竊盜類」、「偽造集資類」、「工具詐騙類」及「員工自盜類」等五項作為犯罪類型之分類，分別於下說明。

1、社交工程類：社交工程（Social Engineering）是一種攻擊行為，攻擊者利用人際關係間的互動特性所發展出來的攻擊法；通常攻擊者若無法直接取得主機內部資料時，會利用電子郵件或者電話，謊稱是某家網際網路服務供應商的工程師，以維修測試系統的理由，騙取總機的重要資料，再利用這些資料取得主機的最高權限，利用該台主機對其他系統發動攻擊，或者乾脆將主機內部資料佔為己有[6]。而利用社交工程法犯罪，更具體言之，即係利用人性之弱點與無知，藉由各種詐騙方式來達到所要得到的標的物[7]。利用社交工程手法來進行線上遊戲犯罪者，常見的犯罪型態如「猜猜我是誰？」「我是某人的朋友？」「我是某人，記得嗎？」「可否幫我…？」「我要做…，請幫助我？」「我有寶物要賣…，有誰要？」等，均係藉由人性與天俱來的憐憫心及惻隱心，或對某事物認知的不足，而以各種障眼手法或花言巧語來達到詐騙目的。

2、傳統竊盜類：本類型為真實社會中，觸犯刑法竊盜罪刑者。常見的竊盜行為如趁被害人疏於防範或注意時，將被害人所使用遊戲之帳號及密碼暗中記下後，再伺機進入遊戲中竊取虛擬寶物。

3、偽造集資類：犯罪人藉由網路架設網站並偽裝成遊戲公司的網站，於網站上偽稱以「集資」、「付費下載服務等」各項詐騙方式進行牟取不當利益。

4、工具詐騙類：犯罪人先設計買賣交易假象來取信於被害人後，進行虛擬寶物的現金交易，並藉由使用「鍵盤記憶程式」等具有相似功能的工具程式，取得被害人之帳號及密碼，再進入遊戲中取回虛擬寶物。

5、員工自盜類：本類為員工自盜類型，如犯罪人係線上遊戲公司的遊戲管理者，利用軟體設計的漏洞而取得他人帳號密碼後，伺機進行竊取虛擬寶物。

肆、線上遊戲犯罪偵查模式

一、線上遊戲歷程相關紀錄檔(Log Files)分析及偵查

對於線上遊戲犯罪之偵查，遊戲公司伺服器之遊戲歷程相關紀錄檔案的分析，可視為物證取得之主要管道。對於數量龐大的記錄資料，如何在有效的時間內，過濾出重要的物證或找出與案情有關連的線索，則是偵查的重要步驟之一。其分析及偵查步驟應依「因果關係」以科學推理法則，主要朝「人」、「時」、「地」及「物」四方面進行偵查，即可達到破案所需的各項證據；另在「事」的方面，因遊

6 「社交工程」，檢索自智匯館華文百科，http://www.cnpedia.com/result/Eword.Asp?Eword=Social%20Engineering，上網日期2003年2月8日。

7 資料來源為內政部警政署刑事局新聞稿，2002年9月11日。

戲歷程過於細微且次數太多，通常已無需作比對舉證部分，而如特殊個案需要，可再行深入舉證來與犯罪過程作比對，進行案情重建。

線上遊戲歷程相關紀錄檔偵查詳細步驟，可就「人」、「時」、「地」及「物」等四方面進行，如圖1 所示。為求簡扼明確，綜合說明如下。

1、 線上遊戲相關紀錄檔之選擇：通常在線上遊戲公司伺服器之遊戲各項紀錄檔中，常提供的項目有遊戲歷程、IP位置、道具接收者遊戲歷程、道具接收者IP位置、會員資料、道具接收者會員資料、道具流向等多項紀錄檔供偵查使用，而其中多項紀錄檔均有重複的紀錄資料，反而會造成資料太多而不易分析、釐清，而耗時甚久，故為縮短偵查期程，以其中之遊戲歷程、道具接收者IP位置及會員資料三項紀錄檔進行分析即可。

2、 發生犯罪之起訖時間：

(1)能預估犯罪時間者：經報案人告知或其他線索得知犯罪時間者，比對道具撿拾者及遊戲歷程的紀錄檔作分析，取得犯罪當時使用電腦之IP位址。

(2)無法預估犯罪時間者：彙整各項情資，研判可能之犯罪時間為何。

3、 ID核對無誤：因道具撿拾者、遊戲歷程及會員資料等紀錄檔中，對ID之編碼有所不同，故須對紀錄檔審慎核對ID確實無誤。

4、 IP位置之分析與偵查：

(1)過濾出犯罪過程所使用之IP位置及數量（共使用哪些IP位址）。

(2)運用TWNIC WHOIS IP/ASN 網站查出該用戶網段及ISP公司為何。

(3)向ISP 公司調出該帳號申請人，並運用邏輯推理方法釐清可能之嫌疑人。

5、 寶物（道具）接收者進行偵查：由寶物（道具）接收者ID之會員資本資料記錄中，進行基本資料的查核，先以警政連線系統之戶政資料查詢輸入該筆資料，若該資料正確無訛，則採用並進行人的追查；若為錯誤資料，則朝其他方面偵查。

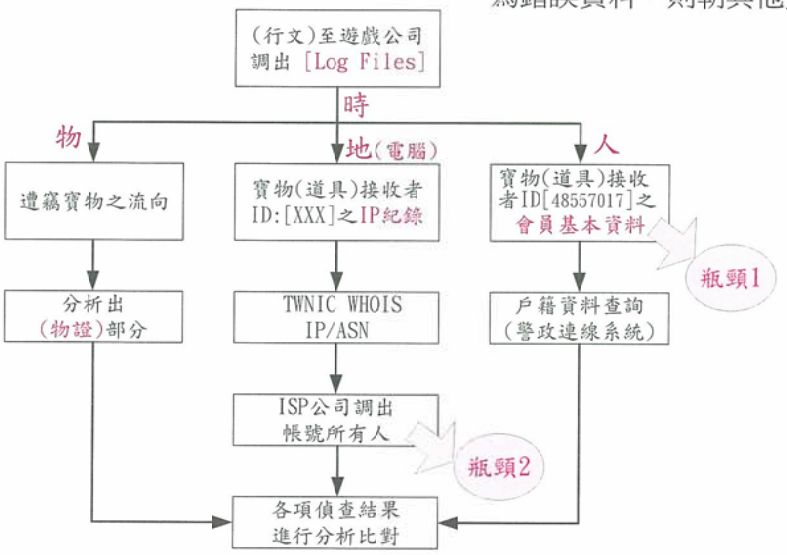

圖1：線上遊戲歷程相關紀錄檔偵查詳細步驟

6、 遭竊寶物（道具）之流向：
(1)遭竊寶物（道具）移轉方式：如丟下、撿取、交換、存放、領出等各種方式。
(2)遭竊寶物（道具）之清點統計。

7、 其他事證之蒐集：如寶物（道具）接收者ID的等級為何？進入遊戲實施犯罪行為時，係從何處（遊戲中的地點）進入？等，與案情有相關的事證或跡證進行蒐集或記錄，以利後續與供述證據作推判，進而確認犯罪事實真相。

8、 偵查瓶頸：
(1)偵查瓶頸一，線上遊戲玩家(使用者)，如果一開始加入線上遊戲公司會員，於登錄基本資料時，就登錄假資料，會造成紀錄檔中寶物（道具）接收者之會員基本資料是假資料，則當偵查至此時，該偵查即告中斷（斷線），需循其他管道進行偵查。本項盲點，對於線上遊戲虛擬世界中的秩序規範之責任，線上遊戲公司應對該類事項做更綿密之規範，以確保絕大多數玩家的權益。
(2)偵查瓶頸二，於ISP 公司調出IP帳號申請人（或所有人）的基本資料後，如該IP 帳號係為網咖（網路咖啡店）時，則該偵查即告中斷，因目前網咖管理辦法中，並無明訂網咖店須對消費者使用電腦的情形做一詳細的記錄或對照資料，如登記使用者身分、時間與店內陳設電腦位置等記錄資料來釐清使用責任。主管機關應儘速立法或以行政命令明確加以規範，遏止不法。

二、同類型案例之偵查模式

以犯罪手法為依據，將所有案件分析歸納出同類型犯罪手法之案件，共得到五種犯罪手法分別為「社交工程」、「傳統竊盜」、「偽造集資」、「工具詐騙」及「員工自盜或其他類」等五類犯罪手法。接著以犯罪手法與偵查範疇為歸類依據，分別建立出四類個案偵查步驟，即「社交工程」、「偽造集資」、「工具詐騙」及「員工自盜或其他類」等四類型偵查步驟，本文囿於篇幅限制，茲節錄社交工程類與偽造集資類偵查步驟作說明。

(一)社交工程類

利用社交工程手法來進行線上遊戲犯罪者，常見的犯罪型態如「猜猜我是誰?」「我是某人的朋友?」「我是某人，記得嗎?」「可否幫我…?」「我要做…，請幫助我?」「我有寶物要賣…，有誰要?」等，均係藉由人性天生具備的憐憫心及惻隱心，或對某事物認知的不足，而以各種障眼手法或花言巧語來達到詐騙目的。

1、個案分析
(1)案情摘要：張ＯＯ於電腦網路上利用網友提供洪ＯＯ先生之密碼及帳號，進入遊戲ＯＯ數位科技股份有限公司之伺服器內，先後分別登入被害人李ＯＯ、林ＯＯ兩人基本資料（身分證字號）來申請遊戲帳號，並在遊戲中將被害人洪ＯＯ先生所擁有的虛擬物品竊取使用。
(2)發生時間：90年8月間。
(3)犯罪者基本資料：
a.犯罪者身份：學生。
b.犯罪者性別、年齡：男、22歲。
(4)犯案手法：略。

(5)觸犯法條：涉嫌偽造文書、竊盜等罪嫌。

2、個案犯罪流程，略。

3、社交工程類偵查模式（如圖2所示）

(1)被害人須先向線上遊戲公司申請取得遊戲購買證明（或會員登記資料）及受害期間遊戲歷程記錄等資料，再前往警察機關報案（參照：民國91年4月1日內政部警政署刑事局與線上遊戲公司舉辦「研商網路遊戲業者如何因應及配合警方查緝網路線上遊戲犯罪會議討論紀錄」之決議事項）；如民眾未準備是項資料，請其前往遊戲發行公司提供相關資料後，再進行製作筆錄程序。

(2)筆錄之內容，應詳載下列事項：

a.報案事由為何？

b.確認線上遊戲公司及伺服器為何？（何時何地申請）

c.確認帳號及角色（ID）為何？

d.寶物（道具）遭竊之時間、地點、遭竊物數量、等級？發生過程詳述？

e.寶物換算成新台幣之價值為多少？兌換比例為何？

f.所使用之帳號、密碼有無其他人知道或共用？

g.案發前後該類犯罪有無與他人有過糾紛或其他跡象？

(3)進行遊戲歷程記錄偵查，參閱本文「線上遊戲歷程相關紀錄檔分析及偵查部分」。

(4)視案情決定是否須前往案發現場之電腦進行勘查；另該案如有知情者（證人或關係人），可考慮是否須進行探訪查證。

(5)經步驟(3)(4)偵查後，綜合並檢視所掌握之證據，依供述證據（被害人、證人之供述內容）、物證及情況證據檢視其證據力是否足夠。經紀錄檔分析得嫌疑人之職業、年齡等條件，與該犯罪行為之各犯罪因子作一客觀之分析，推測犯罪事實存在或不存在。

(6)當所掌握之證據力足以合理推測嫌疑人涉有犯罪時，即可進行傳喚或拘提（報請檢察官）到案，並進行偵訊事宜；如所掌握證據力尚不足時，則須重回(3)(4)步驟再深入蒐集相關事證。

(7)經訊問後嫌疑人之供述內容與所掌握之證據作一完整比對，是否符合先前之推斷，以避免錯漏。若出現與先前推斷不符時，則考量是否為員工自盜類型之犯罪，推斷過程應細心求證比對。

(8)移送地檢署。

(二)偽造集資類偵查模式（如圖3所示）

於受理被害人筆錄後，即就「人、事、時、地、物」等之必然性或可能性進行偵查，進而發現犯罪事實真相。本類偵查步驟如下：

1、蒐集網站及網頁之相關跡證部分：

(1)對可能犯罪事證進行蒐集，並解析犯罪之過程，完整加以紀錄建檔。

(2)在蒐集網站及網頁之相關犯罪事證時，可注意嫌疑人有無留下通訊聯絡方式，如大哥大、電子郵件等，再調出通聯紀錄或電子郵件伺服器之紀錄檔，進行過濾偵查。

(3)取得涉嫌（不法）之網址後，以 Ping 等指令查出所在 IP 位址，

接著進入TWNIC/WHOIS網站查出用戶網段之基本資料，向 ISP 公司調出該帳號之申請人或所有人，最後進行清查可能涉嫌人。

2、清查金融機構可疑帳戶部分：

(1)確定不法之匯款帳戶部分，清查銀行帳戶所有人的基本資料後，再就嫌疑人近期的交往對象加以了解，釐清有無涉嫌犯案的可能性。

(2)清查該金融機構有無裝設錄影監視器，進行過濾偵查。

3、有無事前糾紛情事或內部員工犯案的可能性部分，這部分為結合傳統刑案偵查的重點方向，主要可分為下列幾個偵查項目進行過濾：

(1)所蒐集得到的情報（線索）進行查證。

(2)交往對象為何?（必要時調出通聯紀錄清查）。

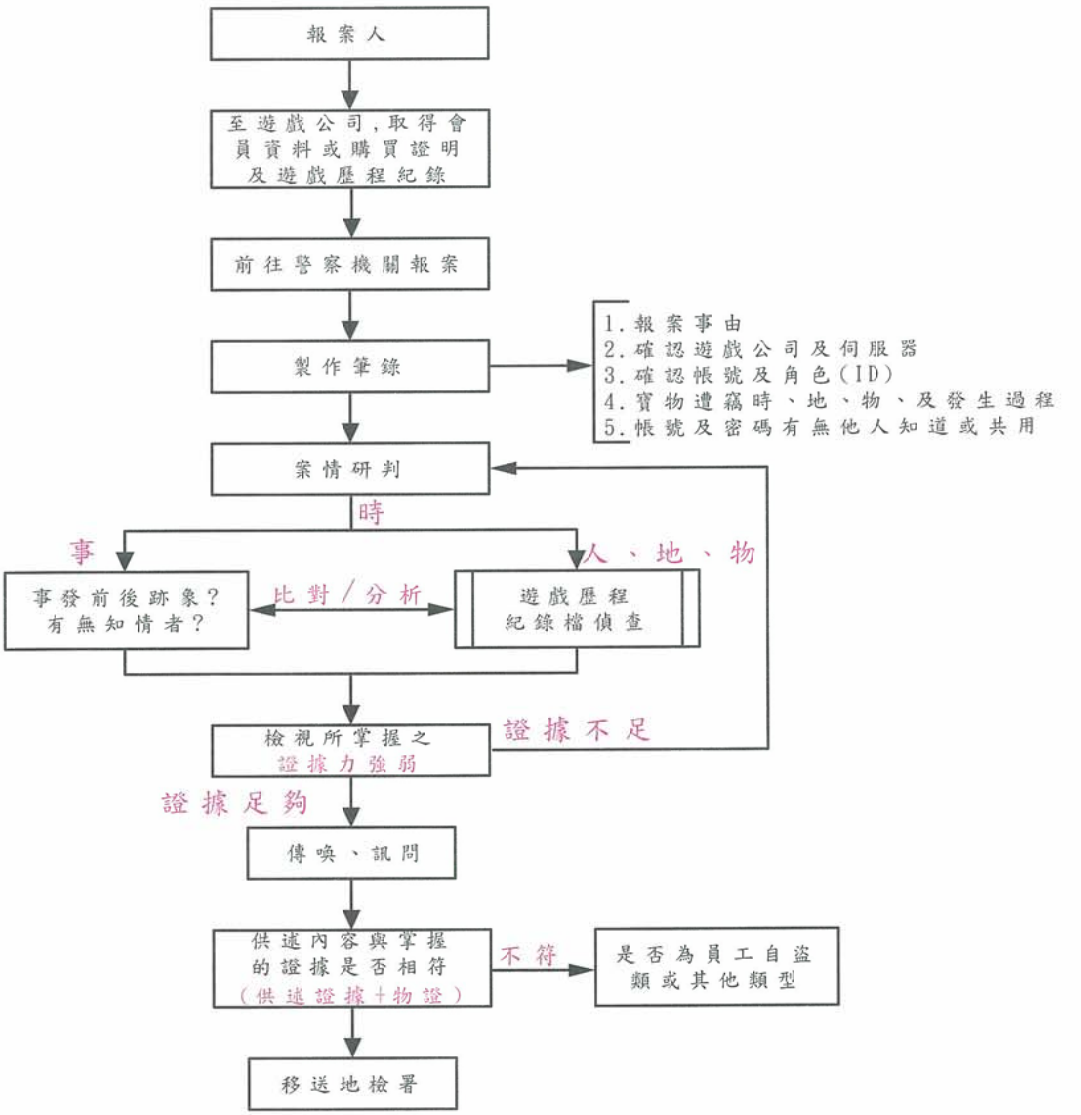

圖2：線上遊戲社交工程類偵查模式

(3)試著突破涉嫌人之心防。
(4)檢視或分析各種不在場證明的可信度。
(5)就涉嫌人的財務狀況深入瞭解、分析。
(6)本案是否為感情或愛情糾紛？
(7)其他可能衍生犯罪動機之因子，如謀財、報復等。

4、經上述步驟偵查後，綜合並檢視所掌握之證據，依供述證據（被害人、證人之供述內容）、物證及情況證據檢視其證據力是否足夠。經紀錄檔分析得嫌疑人之職業、年齡等條件與該犯罪行為之各犯罪因子作客觀之推測犯罪事實存在或不存在。

5、當所掌握之證據力足以合理推測嫌疑人涉有犯罪時，即可進行傳喚或拘提（報請檢察官）到案，並進行偵訊事宜；如所掌握證據

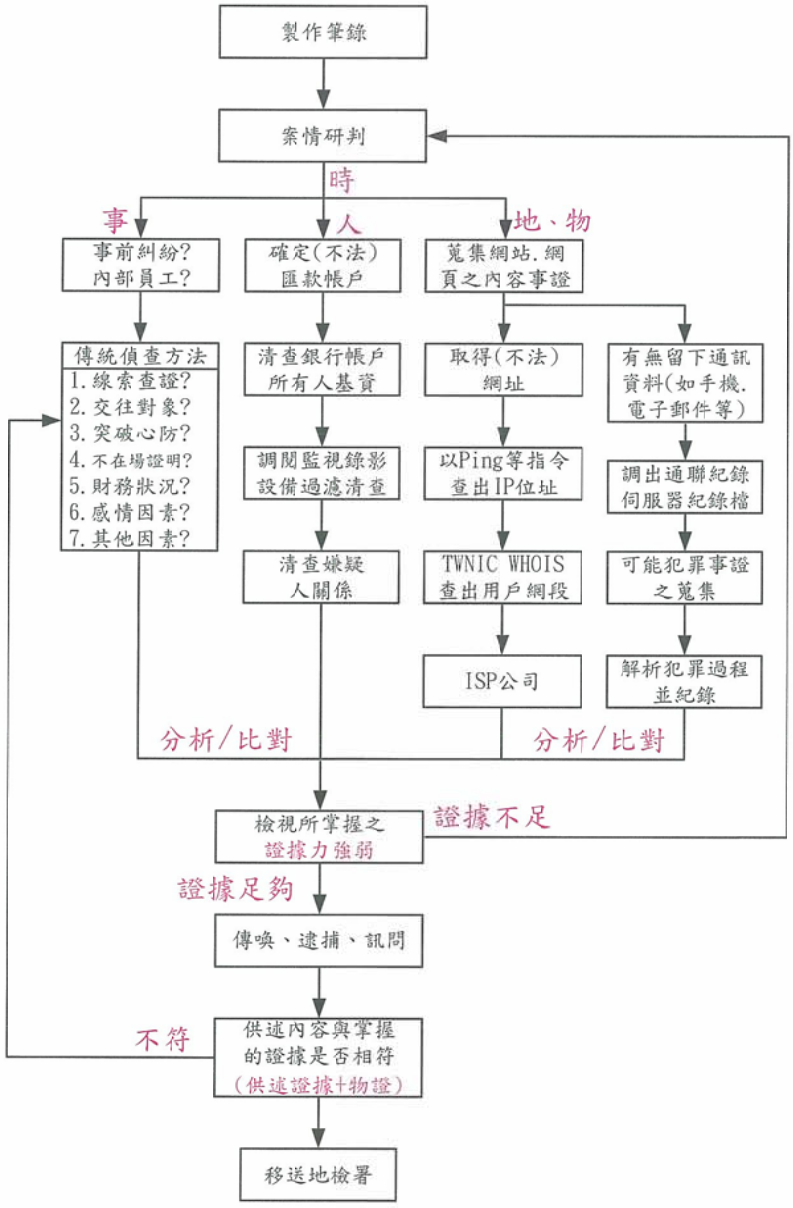

圖3：線上遊戲偽造集資類偵查模式

力尚不足時，則須重回案情研判階段重複偵查。

6、經訊問後嫌疑人之供述內容與所掌握之證據作一完整比對，是否符合先前之推斷，以避免錯漏。如不符時，則須返回步驟3再深入重新偵查。

7、移送地檢署。

伍、結論

網路資訊社會已然成形，而網路資訊社會文化正在逐漸形成中。網際網路具有供個人創造、發揮空間的特性，因而擄獲不少不願面對殘酷現實世界的人陶醉其中，甚而成癮；然而，一旦受外在環境影響，本身規範束縛力崩解，則產生犯罪傾向進而實施犯罪行為、危害他人[8]。因此，一個新的資訊社會生活型態的誕生，新的秩序建立將是首要的課題，而警察在新秩序的建立上扮演著重要的角色，因此如何提升執法機關之偵防能力及人力，將是當前及未來打擊網路犯罪之基礎。

線上遊戲衍生之犯罪，近來，手法不斷翻新，而大多數外勤警察人員並未有充裕的時間來了解線上遊戲是如何進行、如何衍生犯罪、犯罪手法為何等，使得該類案件，多數外勤警察人員並未能立即著手偵辦，而須透過少數專業偵查人員才具有偵辦該類案件能力。在面對推陳出新的各種網路犯罪，一直以來著重於傳統犯罪偵查之警察，將需要有一整體的網路犯罪偵查模式做執勤知能的後盾，才能在未來網路世界中發揮執法的功能，並有效率地完成各項任務。

8 Stuart McClure and Joel Scambray and George Kurtz, Hacking Exposed Second Edition: Network Security Secret & Sclution, Berkley: McGraw-Hill, 1999.