

# 網路犯罪被害： 人口特性與情境機位的影響\*

陳玉書、簡鳳容、呂豐足、劉士誠\*\*

## 目 次

- 壹、前言
- 貳、網路犯罪被害相關研究
- 參、研究方法與研究對象
- 肆、研究發現
- 伍、結論與建議

## 摘 要

網路犯罪被害已成為犯罪學領域重要研究議題，網路犯罪被害預防亦逐漸引起民眾和政府關注；本研究運用 145,216 位警察官方資料庫樣本進行分析，主要目的在探討 2010-2019 年間網路犯罪被害趨勢與主要類型，觀察網路犯罪被害人口特性和情境機位的集中特性，分析人口特性與情境機位之關聯性，以及檢驗整合生活型態和日常活動理論(LRAT)為基礎的概念架構。研究結果顯示，網路犯罪被害主要型態為：網路詐欺、妨害電腦使用、侵害著作、妨害名譽/信用、財產犯罪、網路色情和其他等七大類型。無論網路犯罪被害人口特性或情境機位均存在集中特性；人口特性與情境機位間存在顯著關聯性，人口特性和情境機位對是否會造成網路犯罪被害損失具有顯

\* 本研究係根據本文以科技部委託陳玉書等於 2019-2020 年「網路生活型態、情境機位與網路被害之實證研究」資料為基礎資料整理而成，感謝審查委員在研究期間給予的寶貴建議，委託單位提供各項研究協助，以及所有研究成員的努力。

\*\* 陳玉書，美國杜克大學社會學博士，警察大學犯罪防治學系(所)副教授。

簡鳳容，中央警察大學犯罪防治研究所博士，臺北市立誠正國中教師。

呂豐足，中央警察大學犯罪防治研究所博士，通識教育中心兼任助理教授。

劉士誠，中央警察大學犯罪防治研究所博士生，刑事警察局偵查員，本文通訊作者：

k82\_5@yahoo.com.tw

著影響力，尤其以網路犯罪被害途徑、教育程度和加/被害人關係最具影響力；此項研究結果之持生活型態-日常活動理論(LRAT)的基本假設，並根據研究結果提出網路犯罪被害預防和未來研究之建議。

**關鍵字：**網路犯罪被害、生活型態-日常活動理論(LRAT)、人口特性、情境機會

# **Cyber Victimization: The Impact of Demographic Characteristics and Situational Opportunity**

## Abstract

Cybercrime victimization has emerged as a critical issue for criminology and a growing concern for cybercrime prevention policy. Using a sample of 145,216 cybercrime victims from the police official database, the current study attempts to describe the trend and types of cybercrime victimization from 2010 to 2019, to observe the concentration patterns of victim's demographic characteristics and situational opportunity, and examine the proposed model based on the Lifestyle-Routine Activity Theory (LRAT). Results indicate that major types of cybercrime victimization include fraud, infringement of computer usage, against copyright, against reputation/credit, property crime, online prostitution, and others. There exist concentration patterns of victim's characteristics and situation opportunity for different types of victimization. Victim's characteristics are significantly associated with situational opportunity. Demographic characteristics and situational opportunities have a significant influence on the victim's loss, especially the impact of cyber-path, education, and offender-victim relationship. Findings from this study provide empirical supports for the LRAT and suggestions for preventing cybercrime victimization and future study.

**Key Words: Cybercrime Victimization, Lifestyle-Routine Activity Theory, Demographic Characteristics, Situational Opportunity**

## 壹、前言

根據臺灣網路資訊中心 (Taiwan Network Information Center, TWNIC) 公布的「2019 臺灣網路報告」，推估臺灣地區 12 歲以上上網人數達 1,898 萬人；上網人數經推估已達 2,020 萬，整體上網率達 88.8%；使用行動電信網路者占 85.2%，顯示國人網路使用的普遍性與連網方式快速變化。民眾的生活與溝通方式更加依賴網路和通訊軟體，亦即有更多的人和機會暴露於網路犯罪被害的可能性；網路犯罪被害調查與統計分析刻不容緩。

國內曾經進行多次大樣本的犯罪被害調查 (許春金、陳玉書等，2000；許春金、陳玉書等，2005；許春金、陳玉書等，2010；蔡田木、許春金、陳玉書等，2015)，以及網路詐欺犯罪被害研究 (蔡田木、周文勇、陳玉書等，2009)，研究結果提供警政與犯罪被害保護具體建議，並逐步建立臺灣犯罪被害人研究與理論發展基礎。然上述研究大都聚焦於傳統犯罪被害類型，如住宅竊盜、汽機車竊盜、強盜、傷害和詐欺等類型，對於網路犯罪被害類型與被害人特性的探討，以及網路犯罪被害理論的建構仍相當不足。

綜觀國內有關網路偏差與被害相關研究，在犯罪者、法律、偵查技術方面的探討已相當豐碩多元，且偏向青少年及大學生為研究樣本 (如：盧浩權，2005；顏如佑，2005；吳峻豪，2008；楊垂青，2005；賴克宗，2005；許維維，2009；陳怡儒，2010；陳昭佑，2010；周愷嫻，2014；王茜，2014 等)；但對於被害人在虛擬世界中的人口特性、被害情境和被害類型等探討較少。Ngo 和 Paternoster (2011) 運用犯罪一般理論和生活方式 / 日常活動理論，從個人和情境因素解釋大學生網路犯罪被害；Leukfeldt 和 Yar (2016) 以日常活動理論為基礎，分析 9,161 名樣本被駭客入侵、被傳送惡意電腦病毒、被盜用身分、網購被騙、被網路跟蹤、被網路威脅等之被害經驗與影響因素。實有必要整合上述國內外網路犯罪被害研究成果，將研究樣本擴及不同人口屬性，以及多元型態的網路犯罪被害，期更完整的了解被害人特性、情境特性和網路犯罪被害型態之分布。

陳玉書等 (2006) 從事網路詐欺犯罪與被害研究時，即發現在網路情境中加、被害人的互動沒有時空限制，且可能相互轉換 (陳玉書、曾百川，2007；陳玉書、王秋惠；2011)。簡鳳容 (2018) 從事網路偏差行為與被害特性及其影響因素研究發現，網路偏差行為與網路犯罪被害有顯著正相關，二者存在重疊性，亦即網路犯罪被害人有可能轉變為網路加害人，而網路偏差者有較高機會成為網路犯罪被害人。國外研究亦發現被害與偏差多半有重疊現象 (Craig et al., 2009; Holt & Bossler, 2009; Vandebosch & Van Cleemput,

2009；Reyns, Henson, & Fisher, 2011；Van Wilsem, 2013；Hinduja & Patchin, 2014；Phillips, 2015；Kerstens & Jansen, 2016；Choi & Li, 2017）。因此，好的網路犯罪被害預防也是最佳的犯罪被害預防。

本文主要目的在彙整國內外有關網路犯罪被害相關文獻，以了解網路犯罪被害研究現況和主要發現，並透過2010-2019年官方網路犯罪被害資料分析網路犯罪被害型態（如：網路詐欺、妨害電腦使用、侵害著作權等犯罪被害型態）、被害人特性分布（如：性別、年齡、教育程度和職業類型等）和被害情境特徵，期盼根據研究結果提出對網路犯罪被害預防有幫助之建議。

## 貳、網路犯罪被害相關文獻

### 一、網路犯罪被害型態

內政部警政署2019年網路犯罪概況統計顯示，12,844件網路犯罪中主要類型以網路詐欺居首（30.2%），其次依序為妨害名譽（信用）占20.5%、妨害電腦使用占13.17%和侵害智慧財產權12.4%。美國聯邦調查局2019年網路犯罪報告（2019 Internet Crime Report）顯示，網路犯罪投訴中心（Internet Crime Complaint Center）於2019年接獲467,361件投訴案件，損失逾35億美元；主要的犯罪型態包括網路釣魚、網路詐騙、勒索和洩漏個人資料等。

賴克宗（2005）研究大學生網路被害發現，主要被害之類型依序為：被散播不實謠言、被外洩個人登錄資料、遭言語恐嚇、被盜賣網路虛擬寶物、被詐騙、被網友性侵害等。Ngo和Paternoster（2011）有關大學生網路犯罪被害研究顯示，主要的網路被害包括：收到電腦病毒、收到不想要的色情資訊、在性方面被索求、遭遇網路釣魚、被陌生人網路騷擾、被非陌生人網路騷擾、遭遇網路誹謗等。其中有54.8%曾遭遇網路釣魚，46.0%曾收到電腦病毒，而曾遭遇網路誹謗者僅占7.6%。Leukfeldt和Yar（2016）則發現六種主要的網路犯罪被害，包括：被駭客入侵、被傳送惡意電腦病毒、被盜用身分、被網路跟蹤、被網購詐騙和被網路威脅等。Reep-van den Bergh和Junger（2018）檢視瑞典、英國、荷蘭、德國、法國和盧森堡等國的網路犯罪被害調查，結果發現歐洲國家網路犯罪被害的主要類型為網路詐欺（含網路購物詐欺、網路銀行詐欺和預付款詐欺等）、網路恐嚇/騷擾、惡意程式和駭客入侵等。



由上述國內外網路犯罪被害研究或官方統計可知，網路犯罪與被害型態相當多元，如被動的被盜用身分、被盜取寶物、被駭客入侵、被傳送惡意程式、被洩漏個資等，或具互動性質的網路釣魚、被網路詐騙、被毀謗/勒索、被網路跟蹤/騷擾等，其中又以各種型態的網路詐欺最為普遍，而傳統的犯罪型態亦逐漸網路化，如竊盜、妨害名譽/信用、侵害智慧財產權、恐嚇/霸凌、跟蹤/騷擾等，並引起各國研究者的關注。

## 二、網路犯罪被害人特性

在性別方面，根據國家發展委員會 2019 年「性別數位機會發展現況」分析結果顯示，13,015 位受訪者中，男性上網率為 88.6%，女性曾使用網路比率則為 83.8%，男性較女性略高 4.8%；臺灣網路資訊中心 (TWNIC)「2016 年臺灣無線網路使用調查」結果顯示，男性與女性曾經上網的比例分別為 82.8% 和 76.4%，男性亦高於女性 6.4%，但在使用智慧型手機和行動上網則女性略高於男性；因此，男性在使用網路上的比率略高於女性，而上網方式或設備可能存在性別上的差異。

警政署 2019 年網路犯罪概況統計顯示，12,902 位網路犯罪被害人中，男性占 57.71%，女性則占 41.29%，雖然男性被害比率高於女性，但女性被害人數和比率有上升趨勢。葉雲宏 (2008) 研究顯示，男性的網路詐欺犯罪被害經驗顯著高於女性；Ngo 和 Paternoster (2011) 的研究發現，性別對網路犯罪被害的可能性無顯著影響；Ndubueze、Igbo 和 Okoye (2013) 在奈及利亞的研究發現，男性較女性有較高的網路犯罪被害率；Leukfeldt 和 Yar (2016) 則發現教育程度較高且有工作收入的女性，較有機會成為散播惡意軟體的受害者。然上述有關性別與網路被害研究，大都未將網路被害的型態做有效的區分，導致研究結果相當不一致。

在年齡方面，警政署 2019 網路犯罪統計中，被害人的年齡以 30-39 歲為最多 (占 28.2%)，其次依序為 24-29 歲 (占 19.3%)、40-49 歲 (18.1%)、18-23 歲 (占 17.5%)，相較於 2018 年，未滿 12 歲的兒童和 50-59 歲被害人的被害人有顯著上升趨勢。葉雲宏 (2008) 研究發現，網路詐欺被害經驗者平均年齡為 20.3 歲，顯示網路犯罪被害人以青壯年居多。Ngo 和 Paternoster (2011) 研究發現，年齡為電腦病毒和網路誹謗被害的重要預測因子，年齡愈大者，電腦病毒被害和網路誹謗被害機率越低；Ndubueze、Igbo 和 Okoye (2013) 發現未滿 34 歲受訪者的網路犯罪被害率顯著高於年齡超過 35 歲者，Leukfeldt 和 Yar (2016) 研究則發現，年紀愈輕者被駭客入侵、被網路詐欺和網路人際威脅的風險愈高。上述官方資料與調查資料均顯示，年齡與網路

犯罪被害具有關聯性，年輕族群較年長者可能遭受網路犯罪被害，但年齡與網路犯罪被害的情境和型態是否有關，則須進一步分析。

在教育程度方面，黃祥益(2006)的研究發現，教育程度愈高受網路竊盜被害可能性較低，但被網路詐欺害的機會則較高；葉雲宏(2008)的研究則發現，教育程度為影響網路詐欺被害因素之一，網路詐欺被害人的教育程度大都為國中/小或高中(職)。Ddubueze、Igbo和Okoye(2013)調查研究發現，教育程度與網路犯罪被害並無顯著關聯性，但Leukfeldt和Yar(2016)的研究指出，教育程度高低對於被網路駭客入侵、網路纏擾和網路威脅沒有顯著影響；但教育程度愈高者較容易成為惡意軟體的被害人，而教育程度較低者為網路詐欺被害的高危險群。

在職業方面，警政署2019年網路犯罪概況中，網路犯罪被害人職業以服務業居多(占31.7%)，其次為無職業(13.4%)，再其次為學生(占12.1%)和專業人員(占11.2%)。Ddubueze、Igbo和Okoye(2013)研究發現，職業與網路犯罪被害有顯著關聯性，職業為學生或工商者有較高的網路犯罪被害率，而公務人員的被害率則較低。

上述實證研究與官方統計資料顯示，不同人口特性網路使用者遭受網路犯罪被害機會有所不同，而人口特性是否也會影響網路犯罪被害型態的分布呢？實有必要進行更進一步的分析，以了解人口特性與各類網路犯罪被害型態的關聯性。

### 三、情境機會與網路犯罪被害

Hindelang等人(1976)認為一個人會成為犯罪被害人是因為他的生活型態增加了他與犯罪者互動的機會，而從官方資料或被害人統計中可以發現，犯罪被害的風險與一個人的個人特性和生活型態有關。Hindelang等人的主張其實是來自於生活方式－暴露理論(A Lifestyle/Exposure Model of Personal Victimization)的啟示，個人若要從社會中順利地生存，就必須要適應角色期待和社會結構的約束，而這正和人口的特性有關，例如性別、年齡、教育程度(角色期待)和經濟、家庭、教育(社會結構)，而每個人也因為角色期待和所處的社會結構不同與約束，進一步影響其日常活動與生活方式，而暴露在犯罪被害的情境之中。

生活型態理論(Life-style Theory)強調的是：犯罪被害並非隨機的分佈(non-random distribution)，被害人與加害人之間的日常活動型態似乎有所關聯，生活方式包括職業活動(工作，學校，家管等)和休閒活動；日常生活型態與潛在違法者接觸的人更有可能遭受被害，亦即加害者與被害者在某個

生活上的時間和空間互動，促使犯罪發生之可能。

Vakhitova、Reynald 和 Townsley (2015) 認為在網路空間中暴露於風險和接近加害人的生活方式，與現實世界的研究類似；網路犯罪被害研究可透過測量在網上進行各種活動所花費的時間，來估計暴露的風險。上網時數愈久 (Pratt, Holtfreter, & Reising, 2010 ; Van Wilsem, 2013)、愈常在網路購物 (Van Wilsem, 2011 ; Reyns, 2013)；越常與人在網路上聯絡 (Reyns, Henson, & Fisher, 2016) 或較常使用網路工具與人互動 (Leukfeldt & Yar, 2016) 越容易遭受網路犯罪被害；簡鳳容 (2018) 有關網路偏差與網路犯罪被害研究結果顯示，網路生活型態對於網路犯罪被害除有顯著直接影響效果外，亦會透過網路情境機會或網路偏差行為，對網路犯罪被害造成間接影響。

Cohen 和 Felson (1979) 提出日常活動理論以解釋第二次世界大戰後美國總體犯罪率的變化，就日常活動理論觀點，生活方式的改變，犯罪標的物及監控型態的變化正反應了「日常活動」的變化，Cohen 和 Felson (1979) 認為日常活動可以反映在下列三個變項中：

#### (一) 有動機的加害人 (motivated offender)

日常活動理論以「機會」為核心來描述犯罪被害的發生，所謂有動機的加害人須透過適當犯罪機會的強化，方能成為「加害人」，如缺乏合適的標的物和監控者在場，則犯罪事件將不太可能發生。在網路社會中，可能的加害人到處潛藏伺機而動，科技扮演了使個人以最少的功夫而產生相當大負面影響的角色 (陳玉書、曾百川，2007)。Reyns (2010) 的研究發現，加、被害人在網路接近度與被害方面呈正相關，尤其是將陌生人作為加入社群網路中；當潛在的被害人與網路犯罪管道密切接觸，被害人不須與惡意軟體攻擊者進行互動，就會被感染電腦病毒 (Taylor, 2006)。而 Bossler 和 Holt (2009) 表示被害人在電腦上的特定活動中花費的時間更多，更易被惡意軟體感染。

#### (二) 合適的標的物 (suitable targets)

Felson (1998) 以 VIVA 辨識合適標的物特徵，(A) V (Value) 價值，係指標的物的價值，如在網路中所謂的熱門商品，對潛在的網路詐欺犯罪者是較具價值的，因此，從潛在加害人的觀點所做的評價則進一步影響標的物的合適性 (Yar, 2005 ; 黃俊祥，2007)，Ngo 和 Paternoster (2011) 發現標的吸引力是預測變項與網路被害的關鍵因子。(B) I (Inertia) 可移動性，係指標的物的可移動性 (慣性)；例如在網路購物或遊戲過程中進行交易，可能透過網路銀行或是線上刷信用卡交易完成，因此在網路上標的物的可移動性都很高，並且成為適合交易的標的物。而高科技的不法技術無所不在，可突破



所有網路安全設施，將網路中的資料快速下載、搬移(Yar, 2005；黃俊祥，2007)。(C) V (Visibility) 可見性，係指加害人可以接近被害人的途徑，隨著上網人數激增、各式社群網站蓬勃發展，網路資訊遍布每個角落，對潛在加害人而言，網路世界是一個標的物隨處可見的環境(黃俊祥，2007)。(D) A (Access) 可接近性，係指標的物的可接近性及是否易於逃脫，對網路犯罪者來說，網路移動的方式屬於非線性路線，可以輕易快速地從一個空間跳到另一個空間。他們可以在不同的網咖犯案，使用浮動IP很輕易的就可以躲避追緝，網路移動的方式非線性、網路無國界的特性，在這個方面表露無遺(王秋惠，2007)。

### (三) 有能力的監控者不在場 (absence of capable guardian)

監控指的是有能力防止犯罪發生的人、物或情境，Yar (2005) 認為在網路世界中，有能力的監控者比現實社會少很多，因為通常上網行為是一種私人的活動，即使同在一個環境上網，我們也很難去干涉或了解。而如何在網路空間中實施有效的監控，Choi (2008) 以電腦中是否有防毒軟體、防間諜軟體和防火牆軟體作為網路監控測量。Ngo 和 Paternoster (2011) 的測量包括：(A) 實體監控，如使用專用軟體，間諜軟體和防火牆軟體等；(B) 個人監控，如電腦技能和網路犯罪教育等。相關研究將個人的電腦或網路使用能力和技術(如：Bossler & Holt, 2009; Grzybowski, 2012)，使其有能力察覺網路犯罪被害風險或保護自己，而發揮網路上的監控力，並能保護個人避免被害(Grzybowski, 2012)。

由於網路與通訊軟體的便利性，個人在日常生活中有許多的活動已經逐漸被網路取代，在網路上的行為自然增加，久而久之，網路生活儼然成形，而網路犯罪被害的情境機會(如發生時間、途徑和加被害人關係等)亦是本研究所關心的焦點。

## 四、網路犯罪被害概念架構

在網路與數位年代，犯罪被害早已進入網路和虛擬空間，Yar (2005)、Choi (2008) 和 Reyns、Henson 與 Fisher (2011) 等人將 Hindelang 等人(1976) 的生活型態理論(Life-style Theory) 和 Cohen 和 Felson (1979) 的日常活動理論(Routine Activity Theory) 整合而成「生活型態-日常活動理論」(Lifestyle-Routine Activity Theory, 以下簡稱LRAT)。近年LRAT已被廣泛被運用於解釋網路犯罪被害(如：Vakhitova, Reynald, & Townsley, 2015; Holt, Bossler, Malinski, & May, 2016; Leukfeldt & Yar, 2016; 簡鳳容, 2018)，抑或檢驗標的吸引與監控缺乏對網路犯罪被害的影響(如：Reyns, 2010; Ngo &

Paternoster, 2011; 陳玉書、王秋惠, 2011)。

本研究致力整合人口結構和網路情境機會，以解釋網路犯罪被害所造成的損害；並主張完整的網路犯罪被害解釋模式須納入網路使用者的人口特性，因為不同人口特性的人會有不同的網路生活型態，暴露在不同風險的網路犯罪被害情境中，進而導致不同網路犯罪被害型態和損失。國內外官方網路犯罪被害統計與相關實證研究顯示，性別、年齡、教育程度和職業等個人特性與網路犯罪被害風險有關聯性，礙於抽樣調查不易，國內研究樣本大多以學生族群為主，如欲了解網路犯罪被害特性的完整圖像，實有必要就大樣本的官方資料進行分析。

本文藉由 2010 至 2019 年間官方網路犯罪被害資料進行分析，根據上述有關網路犯罪被害相關理論與實證研究，建構個人網路犯罪被害特性及其情境機會之研究架構圖(參見圖 1)。本研究的自變項為被害人人口特性、中介變項為網路情境機會、依變項則為網路犯罪被害；行為人因具有不同的人口特性(如：性別、年齡、教育程度、職業等)，而影響其網路生活型態(如使用網路時間、進入網路途徑和接觸對象等)，導致在不同網路情境中遭受被害；亦造成不同的被害型態和損失；因此，本研究假設(1)網路犯罪被害人的人口特性與被害情境為非隨機分布，具有集中特性(2)被害人特性與被害情境有顯著關聯性；(3)被害人特性與被害情境對網路犯罪被害損失有顯著影響力。

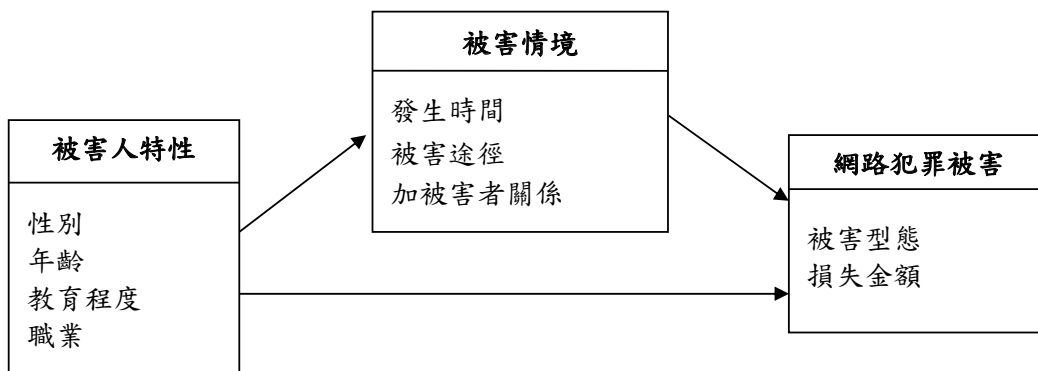


圖 1 網路犯罪被害之研究概念架構圖

## 參、研究方法與研究對象

### 一、研究方法

本研究主要在了解網路犯罪被害型態、被害人特性與情境機會分布，以及影響網路犯罪被害的人口與情境因素。為維護研究品質與研究倫理，在研究執行前即通過「國立成功大學人類研究倫理審查委員會」研究倫理審查(案件編號：108-171)。此項研究透過非介入性研究方法，蒐集2010至2019年警察機關現存有關網路犯罪被害之次級資料。研究進行時函請內政部警政署刑事警察局惠予同意提供「犯罪被害」資料庫中所需的樣本資料，如：被害人人口特性、被害情境(含時空特性)、被害類型、損失/傷害、加/被害人關係等。

由於警察犯罪被害資料的蒐集，係最接近網路犯罪被害發生時的報案或登錄資料，可避免樣本因記憶、隱瞞等因素而使研究資料偏誤，為對網路犯罪被害客觀的實證證據，研究者在進行官方資料蒐集時，必恪遵個人資料保護法之相關規範。為保護研究樣本個人資料與其權益，官方資料係由刑事警察局整合後，再將資料檔刪除足以辨識個人身分之關鍵變數(如：姓名、身分證字號、地址、出生月日等)，並簽署資料保密切結書，由專人負責妥善管理和保護所蒐集之官方資料。在個人資料去連結後，再提供研究者進行處理和分析，因此研究人員無法接觸原始資料或知悉樣本身分；而研究分析結果僅呈現整體特性、趨勢與變數關係，以保障犯罪被害人的隱私和權益。

由於每一件網路犯罪被害案件可能有一個以上被害人，無論被害人特性、情境特徵和被害型態均可能因被害人結構不同而異，因此本研究透過人工逐筆篩檢被害人數為2人以上的被害案件資料；由於案件數龐大且資料結構複雜，本文僅就被害人數為2人以下案件進行分析，以有效控制資料品質和研究概念測量，本文計有145,216位網路犯罪被害人。由於網路犯罪的匿名性與隱蔽性，被害人報案時往往不確定加害人特徵，形成大量的加害人遺漏值，分析時如包含加害人人口特性，將使樣本大量流失(約39%-44%)，造成現象描述和解釋的偏誤，因此本文僅聚焦於網路犯罪被害型態、被害人特性和案件發生的情境機會。

## 二、研究對象

本研究的研究樣本為2010至2019年警察接獲報案或破獲的網路犯罪被害資料，表1為本研究網路犯罪被害樣本之人口特性分佈，在性別方面，男性有62,204人(占55.2%)，女性有50,787人(44.8%)，男性高出女性10.4%。在年齡方面，以31歲至40歲所占比例最高(32,394人；占28.5%)，其次為18歲至25歲(26,202人；占23.1%)，26歲至30歲有19,453人(占17.2%)，顯示樣本以青壯年人口占大多數，。

在職業方面，以商業服務者最多(33,834人，占31.0%)，其次為農漁勞工(26,423人，占24.4%)，學生家管(20,461人，占18.8%)再次之，專業主管者有19,612人(占18.0%)，最後無業者為8,471人(占7.8%)。教育程度最多者為高中畢(肆)業(45,670人，占40.6%)，其次為大學畢(肆)業以上(42,388人，占37.6%)，國中畢(肆)業以下(12,827人，11.4%)再次之，最後為國中以下12,827人(占11.4%)，樣本之教育程度多集中於高中或大學。

表1 研究樣本特性分析

人口特性	人數	%	人口特性	人數	%
性別			職業		
男	62,204	55.2	無業	8,471	7.8
女	50,787	44.8	學生家管	20,461	18.8
合計	113,391	100.0	農漁勞工	26,423	24.4
年齡			商業服務	33,834	31.0
未滿18歲	4,304	3.8	專業主管	19,612	18.0
18-25歲	26,202	23.1	合計	108,801	100.0
26-30歲	19,453	17.2	教育程度		
31-40歲	32,394	28.5	國中以下	12,827	11.4
41-50歲	19,345	17.1	高中	45,670	40.6
51-60歲	9,209	8.1	專科	11,715	10.4
超過60歲	2,493	2.2	大學以上	42,388	37.6
合計	113,400	100.0	合計	112,600	100.0

### 三、研究概念測量

#### (一) 依變數：網路犯罪被害

本研究之依變數含網路犯罪被害類型和被害損失等2個變數；網路犯罪被害類型包括「詐欺犯罪」、「妨害電腦使用」、「侵害著作權」、「妨害名譽/信用」、「財產犯罪」、「色情犯罪」、「其他」等7大類型。網路犯罪被害損失金額則以被害人報案時之被害金額測量之，分為「無損失」、「1,000元以下」、「1,001~2,500元」、「2,501~5,000元」、「5,001~10,000元」、「10,001~25,000元」、「25,001~50,000元」、「超過50,000元」和「不確定損失金額」等8項；在進行羅吉斯迴歸分析時，則將損失分為「無損失」和「有損失」等二類，以觀察人口特性和情境對於網路犯罪被害損失之影響。

#### (二) 自變數：網路犯罪被害人特性

本研究之自變數包含網路犯罪被害人之主要人口特性，如：性別、年齡、教育程度和職業等4個變數。性別為類別變數，男性=1，女性=2；年齡為連續變數，以被害人報案時之年齡(報案年-出生年)測量之。教育程度為順序尺度，分為「國中以下」、「高中」和「大專以上」3個等級。職業為類別變數，包括：「無業」、「學生家管」、「農漁勞工」、「商業服務」和「專業主管」等5項類別。

#### (三) 中介變數：網路犯罪被害情境

本研究以被害人網路犯罪被害時間、被害途徑和與加/被害人關係等3個變數為中介變數，被害時間區分為「凌晨(00:00-05:59時)」、「上午(06:00-11:59時)」、「下午(12:00-17:59時)」和「夜晚(18:00-23:59時)」等4個時段。被害途徑為被害人報案時填報之網路犯罪被害管道，包括：「入口網站」、「拍賣網站」、「社群網站」、「論壇/聊天室」和「其他」等5項網路犯罪被害途徑。與加/被害人關係為類別變數，係以被害人報案時陳述是否認識加害人，包括：「陌生」、「認識」和「不清楚」等3個項目。



## 肆、研究發現

### 一、網路犯罪被害型態與損失

為深入了解2010至2019年網路犯罪被害的狀況與情境機會，以下針對網路犯罪被害特性(包括被害型態、趨勢和損失金額等)、被害人集中特性和網路犯罪被害的情境特徵進行分析。

#### (一) 網路犯罪被害型態

就整網路犯罪被害趨勢而言，本研究資料顯示，2010-2019年各類型網路犯罪被害人數的變化趨勢，從2011年的最高峰(18,831人)，其後略微下降，至2014年再度上升為17,495人，2019年則降為10,915人，呈現逐步下降趨勢<sup>1</sup>。網路犯罪被害類型非常多元，本研究主要分為詐欺犯罪、妨害電腦使用、侵害著作權、妨害名譽／信用、財產犯罪(如賭博、洗錢、重利等)、色情犯罪(如散播販賣陳覽猥褻物品、圖利引誘性交猥褻等)與其他(如偽造文書、洩密、賄選等)；2010至2019年間整體網路犯罪被害類型以詐欺犯罪居首(占29.5%)，其次依序為妨害電腦使用(占26.5%)、侵害著作權(占16.3%)、妨害名譽／信用(占11.9%)就超過了七成，因此對於網路犯罪被害之預防還是有一定的方向可循(參見表2)。

2010年前三類網路犯罪被害分別為詐欺犯罪(占38.7%)、妨害電腦使用(占24.4%)、侵害著作(占20.2%)。2019年由高至低依序為詐欺(占38.3%)、妨害名譽／信用(占21.2%)、妨害電腦使用(占14.4%)；2011年和2014年妨害電腦使用被害曾達7,500人以上(分別占45.8%和43%)，2014年以後則顯著下降；儘管近五年網路犯罪被害有趨緩的趨勢，網路詐欺被害案件大都高居首位，妨害名譽／信用所占的比率顯著上升，以網路侵害著作權、財產犯罪和色情犯罪的比率下降，但其他網路犯罪被害類型則顯著上升。人際互動而產生的妨害名譽／信用被害增加，是否與近年社群網站和網路聊天室／論壇盛行有關，尚須與網路犯罪被害途徑做進一步分析；而網路犯罪被害型態的多元化提高了其他網路犯罪被害的比率，亦值得關注(參見表2和圖2)。

<sup>1</sup> 本研究之樣本雖僅含被害人數為2人以下的網路被害案件，根據警政統計通報：105年和108年網路犯罪概況，2011-2019年電腦網路犯罪案件趨勢，亦以2011年的20,016件和2014年的18,728件呈現雙高峰趨勢一致。

表 2 網路犯罪被害件數變化

單位：人 / %

年別	被害類型							合計
	詐欺犯罪 (%)	妨害電腦使用 (%)	侵害著作權 (%)	妨害名譽 / 信用 (%)	財產犯罪 (%)	色情犯罪 (%)	其他 (%)	
2010	6,153(38.7)	3,869(24.4)	3,197(20.2)	1,091(6.9)	406(2.6)	730(4.6)	414(2.6)	15,860
2011	4,416(23.5)	8,642(45.8)	3,160(16.8)	1,178(6.3)	373(2.0)	663(3.5)	399(2.1)	18,831
2012	2,562(19.8)	4,362(33.7)	3,034(23.5)	1,103(8.5)	741(5.7)	675(5.2)	460(3.6)	12,937
2013	2,035(19.0)	3,225(30.0)	2,584(24.0)	1,197(11.2)	569(5.3)	619(5.8)	499(4.7)	10,728
2014	3,998(22.9)	7,536(43.0)	2,292(13.1)	1,500(8.6)	744(4.3)	629(3.6)	796(4.5)	17,495
2015	4,093(31.2)	2,886(22.0)	2,171(16.5)	1,543(11.7)	1,057(8.0)	563(4.3)	833(6.3)	13,146
2016	4,426(31.2)	2,394(16.9)	2,445(17.3)	2,043(14.4)	1,509(10.6)	496(3.5)	860(6.1)	14,173
2017	5,500(33.5)	2,112(12.9)	2,231(13.6)	2,548(15.5)	1,292(7.9)	1,371(8.3)	1,371(8.3)	16,425
2018	5,562(37.8)	1,850(12.6)	1,824(12.4)	2,734(18.6)	863(5.9)	344(2.3)	1,529(10.4)	14,706
2019	4,190(38.3)	1,574(14.4)	797(7.3)	2,312(21.2)	509(4.7)	250(2.3)	1,283(11.8)	10,915
合計	42,935(29.5)	38,450(26.5)	23,735(16.3)	17,249(11.9)	8,063(5.6)	6,340(4.4)	8,444(5.8)	145,216

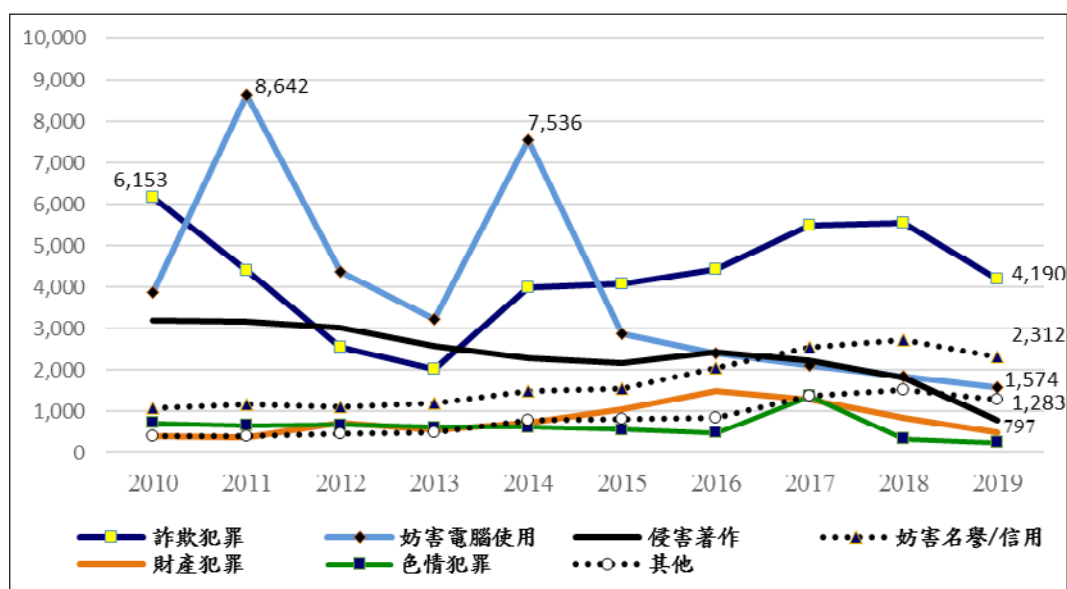


圖 2 2010-2019 年網路犯罪被害型態與趨勢

## (二) 網路犯罪被害損失

圖 3 為網路犯罪被害損失狀況值分布，在被害人報案或案件登錄時，有高達 82,581 位被害人（占 56.9%）無法確定被害損失，其次則為無損失者有 11,118 人（占 7.7%），51,517 位有被害損失（約占 35.4%）；有損失者中，多

數損失在 1 萬元以下，但有 379 人損失達 1 百萬以上，損失千萬以上者有 26 人。

進一步分析網路犯罪被害類型與損失值關係，結果顯示，85% 的網路詐欺犯罪受害者表示有金錢損失，其次為妨害電腦使用被害有 34.4% 表示有金錢損失；而 89.3% 的網路財產犯罪被害，逾 90% 的侵害著作、妨害名譽/信用、網路色情和其他犯罪等類型被害人無法確定其損失；此亦顯示出網路犯罪被害的標的往往較難衡量其金錢價值，如：軟體受損、檔案被竊、名譽信用受損、傳遞假訊息、張貼色情等，與傳統犯罪以人身或財物為標的有顯著不同，因此，網路犯罪被害人的權益更不易受到保護(參見表 3)。

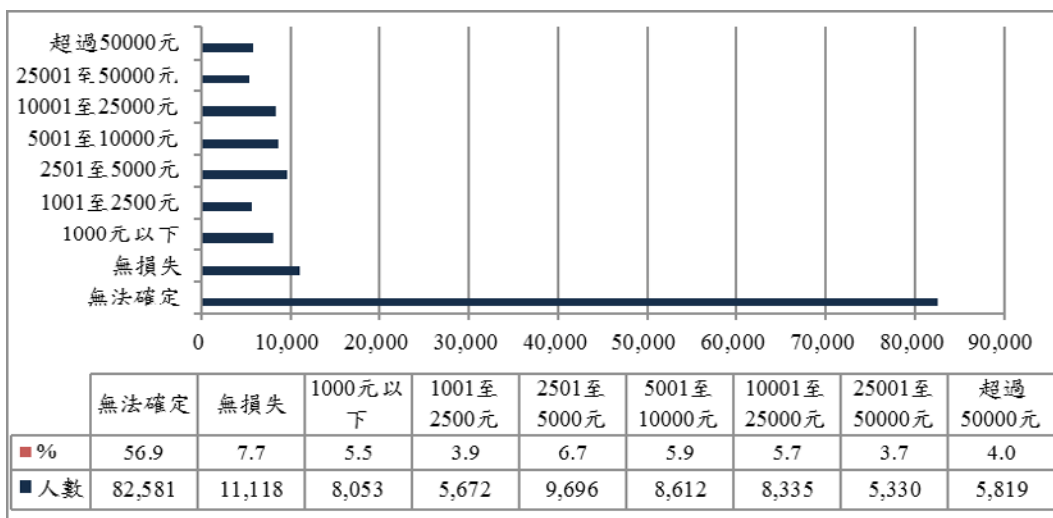


圖 3 網路犯罪被害損失狀況之分布

表 3 網路犯罪被害類型與損失值分布

損失狀況		犯罪被害類型							總和
		詐欺犯罪	妨害電腦使用	侵害著作	妨害名譽/信用	財產犯罪	色情犯罪	其他	
無損失	人數	1,391	9,051	335	102	109	12	118	11,118
	(%)	(3.2)	(23.5)	(1.4)	(0.6)	(1.4)	(0.2)	(1.4)	(7.7)
有損失	人數	36,494	13,215	484	15	753	3	553	51,517
	(%)	(85.0)	(34.4)	(2.0)	(0.1)	(9.3)	(0.0)	(6.5)	(35.4)
無法確定損失金額	人數	5,050	16,184	2,2916	17,132	7,201	6,325	7,773	82,581
	(%)	(11.8)	(42.1)	(96.6)	(99.3)	(89.3)	(99.7)	(92.1)	(56.9)
合計人數	人數	42,935	38,450	23,735	17,249	8,063	6,340	8,444	145,216
	(%)	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)

## 二、網路犯罪被害人與情境機會的集中性

### (一) 網路犯罪被害人的集中特性

本研究假設網路犯罪被害人的人口特性為非隨機分布，具有集中特性；本研究根據被害人人口特性次數分布結果(參見表1)，針對性別、年齡、教育程度與職業等4個變數進行綜合分析，以觀察各類型網路犯罪被害人在人口特性上之集中趨勢。在進行綜合分析時為避免此4變數之分布細格太多，而無法觀察到網路犯罪被害人在人口上的集中特性，因此將年齡分為「35歲以下」和「36歲以上」2組，教育程度分為「高中職以下」和「專科以上」2組，職業類別分為「無業/學生/商業服務」和「其他」(含農/漁/牧/公/專業主管等)2組；結合性別、年齡、教育程度和職業類別等4個變數(2\*2\*2\*2)共16個組合。

由表4中可觀察到各類型網路犯罪被害人人口特性之集中性，如就排序前五項(5/16 = 31.25%)人口特性組合占各類網路犯罪被害的比率觀之，則網路色情被害前五項的人口特性組合的集中率最高為90.7%，其次為侵害著作權的67.7%，再其次為網路詐欺被害占58.5%；妨害電腦使用被害(占44.4%)、妨害名譽/信用被害(占48.9%)和財產犯罪被害(占48.9%)等被害人口特性集中性較不明顯。

以人口特性組合集中率最高的網路色情被害為例，「女性、35歲以下、高中職以下、無業/學生/商業服務者」被害比率最高(占73.8%)；而侵害著作被害以「男性、36歲以上、專科以上、其他職業」被害比率最高(占32.1%，其中職業為專業主管占31%被害率)；詐欺犯罪被害比率最高的人口組合則為「男性、35歲以下、高中職以下、無業/學生/商業服務者」被害比率最高(占16.4%)。顯示不同類型網路犯罪被害人的人口組成並非隨機分布；性別和職業類型影響網路色情集中於女性的無業/學生/商業服務者，侵害著作則集中於36歲以上和職業為專業主管；此項研究結果支持本研究之假設1，以及LRAT理論有關人口結構影響犯罪被害的主張，至於人口特性與網路情境機會之關聯性則有待進一步分析。

表 4 各類型網路犯罪被害人人口特性之集中性 單位：%

性別 (A)	年齡 (B)	教育 程度 (C)	職業 (D)	網路犯罪被害類型 <sup>1</sup>												
				詐欺犯罪		妨害 電腦使用		侵害著作		妨害 名譽/信用		財產犯罪		色情犯罪		
				%	排序	%	排序	%	排序	%	排序	%	排序	%	排序	
男	35歲 以下	高中職 以下	無業/學生/ 商業服務	16.4	1	9.5	3	1.1		9.7	3	11.7	2	4.7	3	
			其他	9.4	4	6.9		1.6		5.9		7.4		0.4		
		專科 以上	無業/學生/ 商業服務	9.5	3	10.2	2	2.3		13.5	1	9.2	3	0.9		
			其他	5.2		6.9		7.2		6.2		4.7		0.8		
	36歲 以上	高中職 以下	無業/學生/ 商業服務	4.6		4.1		6.4		7.6	5	6.8		0.7		
			其他	4.7		4.6		9.4	2	5.9		7.1	5	1.1		
		專科 以上	無業/學生/ 商業服務	1.9		3.3		8.1	5	4.4		3.1		0.0		
			其他	2.9		5.3		32.1	1	7.6	5	6.5		0.8		
	女	35歲 以下	高中職 以下	無業/學生/ 商業服務	15.2	2	8.5	4	0.7		10.3	2	11.8	1	73.8	1
				其他	4.2		2.8		0.7		2.0		2.9		2.0	
			專科 以上	無業/學生/ 商業服務	8.0	5	11.3	1	1.2		7.8	4	7.0		7.5	2
				其他	3.9		7.9	5	5.4		3.2		3.7		2.2	5
36歲 以上		高中職 以下	無業/學生/ 商業服務	7.0		6.5		2.3		7.2		9.1	4	2.5	4	
			其他	2.8		2.6		9.3	3	2.3		2.6		1.1		
		專科 以上	無業/學生/ 商業服務	2.3		4.4		3.3		2.8		3.3		0.6		
			其他	1.9		5.1		8.8	4	3.4		3.2		0.6		
前五名人口組合 %				58.5%		44.4%		67.7%		48.9%		48.9%		90.7%		

註 1：表中各類犯罪被害樣本數為：詐欺被害 n=37,260；妨害電腦使用 n=35,589；侵害著作 n=13,072；妨害名譽/信用 n=15,144；財產犯罪 n=1,032；色情犯罪 n=1,012。

## (二) 網路犯罪被害的情境機會與集中特性

網路犯罪被害發生的情境機會主要包含發生的時間、網路途徑和加/被害人關係等 3 個變數；在被害時間方面，本研究將一天分為 4 個時段：凌晨 (00:00-05:59 時)、上午 (06:00-11:59 時)、下午 (12:00-17:59 時) 與夜晚 (18:00-23:59 時)；被害案件發生最多的在「下午」(占 35.4%)，其次為「夜



晚」(占32.7%)，在凌晨仍有8,213件(占5.7%)的被害比率，顯示網路犯罪發生的時段與被害人的生活作息可能有關(參見圖4)。

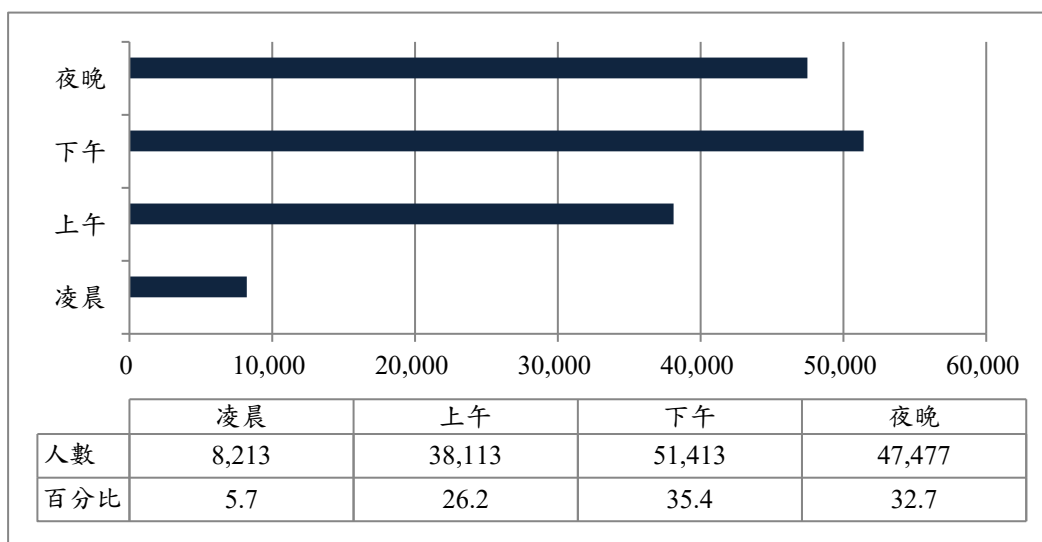


圖4 網路犯罪被害時段之分布

被害的途徑與上網的網站、目的及功能有所關聯，本研究將被害途徑分為入口網站(如Google、雅虎奇摩等)、拍賣網站(如露天拍賣、eBay等)、社群網站(如Facebook、Twitter等)、論壇聊天室(如BBS、痞客邦、愛情公寓等)與其他(如網路銀行等)。被害人進入網路途徑最多的是「入口網站」計40,263人，其次為「論壇聊天室」計29,012人，二者合計逾一半。加/被害人關係則與被害人的交友範圍有關，本研究將關係分為：陌生、認識(包含親戚、朋友、鄰居等)與不清楚(製作筆錄當下未能確認加/被害人關係，事後破案亦未能補登錄者屬之)，其中最多的是「不清楚」(占67.9%)，其次為「陌生」(占27.3%)，「認識」者僅占4.8%(參見表5)。

從加/被害人關係亦能顯示網路情境不受時空限制的特性，也讓素昧平生的兩端千里一線牽；網路的便利與普及，使國人在生活、工作和人際互動更為仰賴網路，犯罪被害機會隨之增加。進一步觀察網路犯罪被害途徑與加/被害人關係之關聯性，二者存在顯著關聯性( $\chi^2=11551.65$ ;  $p<.001$ )；整體而言，95.2%的加/被害人關係是陌生或不清楚加害人，僅4.8%的被害人認識加害人；其中以社群網站有較高的認識比率(占14.7%)，其次為論壇聊天室占8.0%；拍賣網站認識的比率最低僅0.6%。網路情境存在人際不確定的高風險狀態，尤以拍賣網站和入口網站為甚。

表 5 網路犯罪被害途徑與加/被害人關係之關聯性

被害途徑	加/被害人關係						合計
	陌生	%	認識	%	不清楚	%	
入口網站	7,344	18.2	475	1.2	32,444	80.6	40,263
拍賣網站	6,654	34.2	109	0.6	12,695	65.2	19,458
社群網站	7,209	38.6	2,744	14.7	8,719	46.7	18,672
論壇聊天室	8,863	30.5	2,334	8.0	17,815	61.5	29,012
其他	6,073	24.4	701	2.8	18,099	72.8	24,873
合計	36,143	27.3	6,363	4.8	89,772	67.9	132,278

$\chi^2=11551.657$ ;  $df=8$ ;  $p<.001$

本研究假設網路犯罪被害情境為非隨機分布，具有集中特性；本研究根據被害情境分析結果（參見圖 4 和表 5），針對時段、加/被害人關係和被害途徑等 3 個變數進行綜合分析，以觀察各類型網路犯罪被害在情境機會之集中趨勢。在進行綜合分析時為避免此 3 變數之分布細格太多，而無法觀察到網路犯罪被害情境的集中特性，因此將被害時段為「凌晨/上午」和「下午/夜晚」2 組，加/被害人關係分為「認識」和「不認識/不清楚」2 組，被害途徑分為「入口/拍賣網站」、「社群/論壇/聊天室」和「其他」3 組；結合被害時段、加/被害人關係和被害途徑等 3 個變數（2\*2\*3）共 12 個組合。

由表 6 中可觀察到各類型網路犯罪被害情境之集中性，如就排序前 4 項（4/12 = 33.3%）情境組合占各類網路犯罪被害的比率觀之，則侵害著作前 4 項的情境機會集中率最高為 92%，其次為詐欺被害的 86.2%，再其次為妨害電腦使用的 84.2% 和財產犯罪被害的 83.6%；而妨害名譽/信用和色情犯罪被害的集中率亦超過 75%；顯示網路犯罪被害的情境機會有相當高的集中特性，顯示不同類型網路犯罪的情境機會並非隨機分布，此項結果支持本研究假設 1。

以情境機會集中率最高的侵害著作被害為例，「下午/夜晚、加被害人 不認識/不清楚、入口/拍賣網站者」被害比率最高（占 40.8%）；而詐欺犯罪（占 36.5%）和妨害電腦使用被害（35.6%）亦在相同情境下有最高的被害率；但妨害名譽/信用與色情犯罪被害最常發生在「下午/夜晚、加被害人 不認識/不清楚、社群/論壇/聊天室」，被害率分別為 36.1% 和 27.1%，而財產犯罪被害率最高的組合則為「下午/夜晚、加被害人 不認識/不清楚、其他網路場域」。網路和虛擬空間的無遠弗屆和多元管道，提供加害人接觸

被害者的可及性，而網路使用者的隱蔽性，亦使被害人在使用網路時無法知悉潛在加害人的存在，而成為犯罪標的物。

表 6 各類型網路犯罪被害情境機會的集中性 單位：%

時段	加/ 被害人 關係	被害 途徑	網路犯罪被害類型 <sup>1</sup>											
			詐欺犯罪		妨害 電腦使用		侵害著作 名譽/信用		財產犯罪		色情犯罪			
			%	排序	%	排序	%	排序	%	排序	%	排序		
凌晨 / 上午	認識	入口/拍賣 網站	0.1		0.2		0.0		0.4		0.2		0.2	
		社群/論壇/ 聊天室	0.5		0.3		0.0		5.4		0.6		1.6	
		其他	0.1		0.2		0.0		0.6		0.2		0.2	
	不認識 / 不清楚	入口/拍賣 網站	<b>10.8</b>	<b>3</b>	<b>15.6</b>	<b>3</b>	<b>30.3</b>	<b>2</b>	5.7		7.7		<b>9.1</b>	<b>4</b>
		社群/論壇/ 聊天室	<b>9.5</b>	<b>4</b>	8.5		3.5		<b>19.4</b>	<b>2</b>	6.2		9.0	
		其他	3.1		5.5		<b>9.2</b>	<b>4</b>	3.8		<b>24.8</b>	<b>2</b>	8.6	
下午 / 夜晚	認識	入口/拍賣 網站	0.2		0.2		0.0		0.8		0.3		0.4	
		社群/論壇/ 聊天室	1.0		0.6		0.0		<b>9.9</b>	<b>4</b>	1.1		3.2	
		其他	0.2		0.2		0.0		0.8		0.2		0.6	
	不認識 / 不清楚	入口/拍賣 網站	<b>36.5</b>	<b>1</b>	<b>35.6</b>	<b>1</b>	<b>40.8</b>	<b>1</b>	<b>9.9</b>	<b>3</b>	<b>15.1</b>	<b>3</b>	<b>20.8</b>	<b>2</b>
		社群/論壇/ 聊天室	<b>29.4</b>	<b>2</b>	<b>21.5</b>	<b>2</b>	4.4		<b>36.1</b>	<b>1</b>	<b>12.7</b>	<b>4</b>	<b>27.1</b>	<b>1</b>
		其他	8.5		<b>11.5</b>	<b>4</b>	<b>11.7</b>	<b>3</b>	7.3		<b>31.0</b>	<b>1</b>	<b>19.3</b>	<b>3</b>
前五名人口組合 %			86.2%		84.2%		92%		75.3%		83.6%		76.3%	

註 1：表中各類犯罪被害樣本數為：詐欺被害 n=33,677；妨害電腦使用 n=36,733；侵害著作 n=23,420；妨害名譽/信用 n=16,909；財產犯罪 n=7,516；色情犯罪 n=6,078。

### 三、被害人特性與情境機會的關聯性

根據 LRAT 理論，網路犯罪被害的發生係被害標的在網路情境中聚合，而提供網路犯罪的機會所致；本研究進一步分析網路犯罪被害人的入口特性與情境機會的關聯性。表 7 顯示被害人的性別與被害發生時間 ( $\chi^2=359.055$ :  $p<.001$ )、被害途徑 ( $\chi^2=1156.264$ :  $p<.001$ ) 與加/被害人關係 ( $\chi^2=196.003$ :

p<.001)之關聯性皆達顯著水準。無論男、女其被害主要發生時間大多以下午為主、夜晚次之，但女性被害發生在下午的比率高於男性(39.9% vs. 35.7%)，而男性被害在凌晨的比率則高於女性(11.7% vs. 8.8%)。在被害途徑方面，無論男性或女性其被害途徑主要為入口網站和論壇/聊天室，但女性在入口網站和社群網站的被害比率高於男性(35.9% vs. 29.3%; 17.2% vs. 14.7%)，而男性在論壇/聊天室被害比率則高於女性(26.7% vs. 18.7%)。在加/被害人關係方面，女性認識加害人比率略高於男性，但亦有較多的女性被害時不清楚加害人是誰。

表 7 被害人性別與被害情境之關聯性分析

被害情境	被害人性別		$\chi^2$ ; df; Sig.	
	男性 (%)	女性 (%)		
發生時間	凌晨	7,304(11.7)	4,485(8.8)	$\chi^2=359.055^{***}$ df=3
	上午	10,902(17.4)	8,847(17.4)	
	下午	22,379(35.7)	20,260(39.9)	
	夜晚	22,019(35.2)	17,195(33.9)	
	合計	62,604(100.0)	50,787(100.0)	
被害途徑	入口網站	16,693(29.3)	16,417(35.9)	$\chi^2=1156.264^{***}$ df=4
	拍賣網站	7,442(13.1)	5,526(12.0)	
	社群網站	8,376(14.7)	7,910(17.2)	
	論壇聊天室	15,226(26.7)	8,597(18.7)	
	其他	9,260(16.2)	7,414(16.2)	
合計	56,997(100.0)	45,864(100.0)		
加/被害人關係	陌生	21,729(34.7)	15,788(31.1)	$\chi^2=196.003^{***}$ df=2
	認識	3,363(5.4)	3,272(6.4)	
	不清楚	37,512(59.9)	31,727(62.5)	
	合計	62,604(100.0)	50,787(100.0)	

\*\*\* p<.001

被害人的年齡可能會影響個人使用網路的情境，而使其暴露在網路犯罪被害的風險有所不同；表 8 為在不同網路情境被害者的年齡差異分析，結果顯示，網路犯罪被害發生時間(F=582.714; p<.001)、被害途徑(F=322.484; p<.001)和加/被害人關係(F=119.400; p<.001)不同者，其年齡的平均數有顯著差異。

就網路犯罪被害發生時間而言，在夜晚被害者的平均年齡最低

( $M=32.297$ )，且顯著低於其他三個時段被害人的平均年齡，上午被害者的平均年齡最高( $M=36.354$ )，且顯著高於凌晨和下午的被害人，而下午被害人平均年齡亦顯著高於凌晨的網路犯罪受害者。

在被害途徑方面，以在網路論壇/聊天室被害者的平均年齡最為年輕( $M=32.579$ )，且顯著低於其他網路場域被害人的平均年齡；其次為在社群網站被人( $M=33.020$ )，其平均年齡顯著低於入口網站/拍賣網站/其他，其他或拍賣網站的被害人平均年齡則顯著高於入口網站。在加/被害人關係方面，以陌生關係的年齡平均數為最高( $M=34.833$ )，且顯著高於不確定和認識二組，惟不同加/被害人關係者的年齡平均數差異性較被害發生時間和被害途徑強。

整體而言，在不同網路情境被害者的年齡確有顯著差異，白天被害者的平均年齡較長，而夜晚或凌晨受害者則較年輕；具人際互動性質的網路場域被害人(社群網站或論壇/聊天室)，其被害人的平均年齡較為年輕；而具消費性質的拍賣網站被害人的平均年齡較長；加/被害人關係為陌生者的平均年齡最高；顯示年齡的確會影響被害人的網路生活型態(參見表8)。

表 8 不同網路情境被害人之年齡差異分析

被害情境	被害人年齡			F; Sig.
	n	M	SD	
發生 時間	凌晨(A)	11,783	34.099	11.79106
	上午(B)	19,755	36.354	11.96272
	下午(C)	42,633	34.620	11.82775
	夜晚(D)	39,198	32.297	11.38809
	合計	113,369	34.065	11.78738
被害 途徑	入口網站(A)	33,104	34.502	11.20786
	拍賣網站(B)	12,968	35.678	12.20175
	社群網站(C)	16,283	33.020	11.46415
	論壇/聊天室(D)	23,815	32.579	12.11402
	其他(E)	16,666	36.089	11.76031
合計	102,836	34.228	11.75272	
加/ 被害人 關係	陌生(A)	37,512	34.833	12.09996
	認識(B)	6,638	33.605	12.44303
	不清楚(C)	69,219	33.693	11.52816
	合計	113,369	34.065	11.78738

\*\*\*  $p < .001$



表 9 為被害人教育程度與被害情境之關聯性，結果顯示教育程度與發生時間 ( $\chi^2=186.892$ ;  $p<.001$ )、被害途徑 ( $\chi^2=3563.423$ ;  $p<.001$ ) 與加/被害人關係 ( $\chi^2=1207.092$ ;  $p<.001$ ) 之關聯性均達顯著水準，因此，教育程度會影響研究樣本被害時之情境。

在發生時間方面，無論被害人教育程度為何，被害時間在下午或夜晚的比率逾 75%，但教育程度為國中以下者在下午或夜晚被害的比率高於教育程度為高中或大專以上；而教育程度在高中或大專以上在凌晨被害比率則高於國中以下者。在被害途徑方面，國中以下大多為論壇聊天室或社群網站被害，二者合計占 55%，高中或大專以上則在入口網站被害比率較高（分別占 28.6%、38.1%）。在加/被害人關係方面，雖然加/被害人關係以「不清楚」居多，但國中以下者之加害人為「陌生」達 43.3%，顯著高於高中或大專以上者。由此可發現在網路生活中，使用者教育程度會影響其被害情境，兩者具有顯著關聯性（參見表 9）。

表 9 被害人教育程度與被害情境之關聯性分析

被害情境	教育程度			$\chi^2$ ; df; Sig.	
	國中以下 (%)	高中 (%)	大專以上 (%)		
發生 時間	凌晨	995 (7.8)	4,976(10.9)	5,677(10.5)	$\chi^2=186.892^{***}$ df=6
	上午	2,032(15.8)	7,761(17.0)	9,789(18.1)	
	下午	5,023(39.2)	16,949(37.1)	20,408(37.7)	
	夜晚	4,777(37.2)	15,984(35.0)	18,229(33.7)	
	合計	12,827(100.0)	45,670(100.0)	54,103(100.0)	
被害 途徑	入口網站	1,882(18.3)	11,580(28.6)	19,547(38.1)	$\chi^2=3563.423^{***}$ df=8
	拍賣網站	1,339(13.0)	4,532(11.2)	7,057(13.8)	
	社群網站	2,349(22.8)	7,449(18.4)	6,201(12.1)	
	論壇聊天室	3,304(32.2)	10,782(26.6)	9,496(18.5)	
	其他	1,412(13.7)	6,156(15.2)	8,983(17.5)	
合計	10,286(100.0)	40,499(100.0)	51,284(100.0)		
加/ 被害人 關係	陌生	5,560(43.3)	14,532(31.8)	17,087(31.6)	$\chi^2=1207.092^{***}$ df=4
	認識	886 (6.9)	3,222 (7.1)	2,289 (4.2)	
	不清楚	6,381(49.8)	27,916(61.1)	34,727(64.2)	
	合計	12,827(100.0)	45,670(100.0)	54,103(100.0)	

\*\*\*  $p<.001$

表 10 為被害人職業類型與被害情境之關聯性，結果顯示被害人職業類型與其被害發生時間 ( $\chi^2=954.341$ ;  $p<.001$ )、被害途徑 ( $\chi^2=3292.143$ ;  $p<.001$ ) 與加/被害人關係 ( $\chi^2=286.755$ ;  $p<.001$ ) 之關聯性皆達顯著水準。在發生時間方面，無業者近 40% 在下午被害，學生家管之被害發生時間以晚上占大多數 (40.6%)，而專業主管在上午被害的比率為 22.6%，高於其他職業類型的被害者。在被害途徑方面，無業/學生/家管在論壇/聊天室被害比率高於其他職業類型 (約占 29%)，農漁勞工、商業服務和專業主管則以有較高比率在入口網站被害，專業主管在拍賣網站被害的比率為 19.7%，高於其他職業類型的被害人。在加/被害人關係方面，儘管被害人認識加害人的比率偏低，但無業者認識加害人的比率高於其他職業類型，專業主管認識加害人的比率則最低，僅占 3.9%；此或與不同職業類型被害人的網路犯罪被害途徑有關，例如：相較於其他職業，無業者有較高比率在社群網站或論壇聊天室等人際互動的場域接觸加害者，而專業主管則大都在入口網站或拍賣網站接觸加害者，不同網路場域的人際互動模式和隱蔽性有所不同，會影響被害人對加害人的了解程度 (參見表 10)。

表 10 被害人職業類型與被害情境之關聯性分析

被害情境	被害人職業類型					
	無業 (%)	學生家管 (%)	農漁勞工 (%)	商業服務 (%)	專業主管 (%)	
發生時間	凌晨	892(10.5)	1,934 (9.5)	2,715(10.3)	3,603(10.6)	2,156(11.0)
	上午	1,479(17.5)	2,633(12.9)	4,611(17.5)	5,809(17.2)	4,442(22.6)
	下午	3,379(39.9)	7,580(37.0)	9,886(37.4)	12,890(38.1)	7,123(36.4)
	夜晚	2,721(32.1)	8,314(40.6)	9,211(34.8)	11,532(34.1)	5,891(30.0)
	合計	8,471(100.0)	20,461(100.0)	26,423(100.0)	33,834(100.0)	19,612(100.0)
$\chi^2=954.341^{***}$ ; df=12						
被害途徑	入口網站	1,901(25.7)	5,529(30.0)	8,453(35.2)	9,743(32.0)	6,041(32.9)
	拍賣網站	690 (9.3)	2,171(11.8)	2,791(11.6)	3,543(11.7)	3,624(19.7)
	社群網站	1,463(19.8)	3,192(17.3)	3,525(14.7)	5,462(18.0)	2,001(10.9)
	論壇聊天室	2,200(29.7)	5,281(28.6)	5,921(24.7)	6,774(22.3)	2,582(14.0)
	其他	1,144(15.5)	2,267(12.3)	3,308(13.8)	4,877(16.0)	4,136(22.5)
	合計	7,398(100.0)	18,440(100.0)	23,998(100.0)	30,399(100.0)	18,384(100.0)
$\chi^2=3292.143^{***}$ ; df=16						
加/被害人關係	陌生	2,724(32.2)	6,491(31.7)	8,837(33.4)	11,055(32.7)	6,919(35.3)
	認識	706 (8.3)	1,278 (6.2)	1,495 (5.7)	2,069 (6.1)	757 (3.9)
	不清楚	5,041(59.5)	12,692(62.1)	16,091(60.9)	20,710(61.2)	11,936(60.8)
	合計	8,471(100.0)	20,461(100.0)	26,423(100.0)	33,834(100.0)	19,612(100.0)
$\chi^2=286.755^{***}$ ; df=8						

\*\*\* $p<.001$

#### 四、網路犯罪被害損失影響因子

本研究假設被害人特性與被害情境對被害損失有顯著影響力，為檢驗此項假設，以網路犯罪被害有無損失為依變數，並以二元羅吉斯迴歸 (Binary Logistic Regression) 進行分析；首先以被害人人口特性為自變數進行分析，檢驗被害人性別、年齡、教育程度和職業類型對網路犯罪被害有無損害之影響 (模式一)。其次加入情境機會因素，含被害時間、被害途徑和加被害關係等變數，以觀察研究概念架構中所有變數對網路犯罪被害損失的影響 (模式二)。

表 11 為網路犯罪被害損失之二元羅吉斯迴歸分析，模式一中自變數含被害人性別、年齡、教育程度和職業、年齡、教育程度和職業類別等對網路犯罪被害有無損失均具有顯著影響力。在性別方面，如以被害者損失較低的女性做為參考組別，男性被害者損失風險為女性的 1.368 倍，性別對損失有無具顯著影響力 ( $B=.313$ ,  $Wald=178.737$ ,  $p<.001$ )。年齡對損失有無具顯著影響力 ( $B=-.012$ ;  $Wald=110.218$ ;  $p<.001$ )，被害人年齡越年輕者，其網路犯罪被害的損失風險越高。就教育程度而言，大專以上被害者之損失較低做為參考組別，高中組損失風險為大專以上的 1.448 倍 ( $B=.370$ ,  $Wald=214.277$ ,  $p<.001$ )；國中以下組損失風險為大專以上的 3.129 倍 ( $B=1.141$ ,  $Wald=622.123$ ,  $p<.001$ )，教育程度對損失有無具顯著影響力 ( $Wald=703.945$ ,  $p<.001$ )。職業類型方面，職業類別仍對損失有無具顯著影響力 ( $Wald=117.946$ ,  $p<.001$ )，以專業主管被害者之損失較低做為參考組別，學生家管組損失風險為專業主管的 1.448 倍 ( $B=.370$ ,  $Wald=75.196$ ,  $p<.001$ )；相較於專業主管，其他職業類別則無統計上顯著影響。

模式二中增加被害情境變數，結果顯示發生時間 ( $Wald=58.922$ ,  $p<.001$ )、被害途徑 ( $Wald=839.401$ ,  $p<.001$ )、加被害關係 ( $Wald=283.170$ ,  $p<.001$ ) 對網路犯罪被害損失均達統計顯著水準。如以「上午」的損失較低做為參考組別，下午損失風險為上午的 1.212 倍 ( $B=.193$ ,  $Wald=31.460$ ,  $p<.001$ )；夜晚損失風險為上午的 1.308 倍 ( $B=.269$ ,  $Wald=57.941$ ,  $p<.001$ )；凌晨損失風險則為上午的 1.160 倍 ( $B=.149$ ,  $Wald=8.302$ ,  $p<.01$ )。在被害途徑方面，以入口網站的損失較低做為參考組別，拍賣網站損失風險為入口網站的 2.443 倍 ( $B=.893$ ,  $Wald=432.105$ ,  $p<.001$ )；社群網站損失風險為入口網站的 1.253 倍 ( $B=.226$ ,  $Wald=26.694$ ,  $p<.001$ )；論壇聊天室損失風險為入口網站的 2.204 倍 ( $B=.790$ ,  $Wald=560.164$ ,  $p<.001$ )；「其他」損失風險為入口網站的 1.185 倍 ( $B=.169$ ,  $Wald=24.618$ ,  $p<.001$ )。就加被害關係而言，如以被害人「不清楚」加害人狀況的損失較低做為參考組別，「陌生」損失風險

為「不清楚」的 1.645 倍 (B=.498, Wald=277.825,  $p<.001$ ) ; 「認識」損失風險為「不清楚」的 1.480 倍 (B=.392, Wald=16.020,  $p<.001$ ) 。

表 11 網路犯罪被害損失之二元羅吉斯迴歸分析 (n=50,852)

自變數	模式一		模式二	
	B	Exp(B)	B	Exp(B)
<b>人口特性</b>				
性別 (女=2)	.313(178.737)***	1.368	.233(94.536)***	1.262
年齡	-.012(110.218)***	.988	-.013(127.887)***	.987
教育程度 (專科以上=3)	(703.945)***		(435.449)***	
國中以下	1.141(622.123)***	3.129	.933(396.650)***	2.542
高中	.370(214.277)***	1.448	.286(121.436)***	1.331
職業類別 (專業主管=5)	(117.946)***		(82.840)***	
無業	.065(1.573)	1.067	.033(.387)	1.033
學生家管	.370(75.196)***	1.448	.320(54.249)***	1.378
農漁勞工	.075(3.745)	1.078	.062(2.414)	1.064
商業服務	.014(.125)	1.014	.024(.381)	1.024
<b>被害情境</b>				
發生時間 (上午=1)			(58.922)***	
下午			.193(31.460)***	1.212
夜晚			.269(57.941)***	1.308
凌晨			.149(8.302)**	1.160
被害途徑 (入口網站=1)			(839.401)***	
拍賣網站			.893(432.105)***	2.443
社群網站			.226(26.694)***	1.253
論壇聊天室			.790(560.164)***	2.204
其他			.169(24.618)***	1.185
加 / 被害關係 (不清楚=3)			(283.170)***	
陌生			.498(277.825)***	1.645
認識			.392(16.020)***	1.480
常數	1.328(622.350)***	3.775	.842(182.464)***	2.320
Chi-Square	1411.387		2872.101	
Cox & Snell R <sup>2</sup>	.027		.055	
Nagelkerke R <sup>2</sup>	.044		.089	
正確 %	81.5%		81.5%	

註：自變數括弧內為參考組別；B 值弧內為 Wald 值。 \*\*  $p<.01$ ; \*\*\*  $p<.001$

模式二的 Chi-Square 為 2872.101，Cox & Snell  $R^2$  為 .055，Nagelkerke  $R^2$  為 .089，解釋正確率為 81.5%，優於模式一，顯示被害情境為導致有無損失之關鍵因子；如以 Wald 值比較模式二中各因子影響力，各因子對於網路犯罪被害損失的影響力依序為：被害途徑、被害人教育程度、加/被害人關係、年齡、性別、教育程度和發生時間。

## 伍、結論與建議

本研究屬探索性之研究，試圖透過大樣本的官方犯罪被害資料，描述 2010 至 2019 年間網路犯罪被害型態與損失狀況，分析網路犯罪被害人與情境機會的集中特性，進而檢驗造成網路犯罪被害損失的影響因子。國內外官方資料與網路犯罪被害研究均顯示，網路犯罪被害類型相當多元(吳嫦娥，2004；賴克宗，2005；內政部警政署，2020；Ngo & Paternoster, 2011；Leukfeldt & Yar, 2016；Reep-van den Bergh & Junger, 2018；Federal Bureau of Investigation, 2020)。由於網路犯罪被害種類繁多，本研究歸納出詐欺犯罪、妨害電腦使用、侵害著作權、妨害名譽／信用、財產犯罪、色情犯罪與其他等七類網路犯罪被害。

研究結果發現，2010 至 2019 年間網路犯罪被害趨勢雖有波動，近五年呈現逐漸下降趨勢。2010 年盛行之網路犯罪被害類型為詐欺犯罪、妨害電腦使用、侵害著作，2019 年網路詐欺和妨害電腦使用仍為主要網路犯罪被害類型，但侵害著作被害顯著下降，而妨害名譽／信用和其他網路犯罪被害所占比率顯著上升；顯見因網路的普及、使用習慣和互動模式等，使網路犯罪被害的類型不斷變化。由於網路犯罪被害標的物的除金錢外，有許多屬於軟體、資訊和信用／名譽等難以金錢衡量其價值，而使被害人無法估計其實際損失，56% 的被害人無法確定損失，且有損失者的變異量大(標準差為 519,671.826)；因此，無論在犯罪被害類型或被害損失上，網路犯罪被害與傳統犯罪被害均有明顯不同。

網路犯罪被害相關研究與 LRAT 理論顯示，被害人的人口特性並非隨機分布(黃祥益，2006；葉雲宏，2008；警政署，2020；Ngo & Paternoster, 2011；Ddubueze, Igbo, & Okoye, 2013；Leukfeldt & Yar, 2016)；上述官方統計或實證研究大都分析人口特性對特定的網路犯罪被害的影響，較少同時觀察主要人口結構在各類網路犯罪被害的集中特性。本研究綜合被害人的性別、年齡、教育程度和職業在各類網路犯罪被害的集中特性；結果顯示，網路色情和侵害著作被害人的人口綜合集中性較高，網路詐欺被害人的人口集中性



中等，妨害電腦使用、妨害名譽/信用和財產犯罪被害人的人口特性多元，較不具集中特性；不同的網路犯罪被害類型有不同的集中特徵；如女性、35歲以下、高中職以下、無業/學生/商業服務者即占73.8%網路色情被害；約三分之一的侵害著作被害者為男性、36歲以上、專科以上、其他職業；此項結果部分支持本研究假設一。

在被害情境方面，Vakhitova、Reynald 和 Townsley (2015) 發現被害人暴露於加害人的網路生活空間時，將提高其被害風險；使用網路的途徑也會影響被害風險 (Van Wilsem, 2011; Reyns, 2013; Reyns, Henson, & Fisher, 2016; Leukfeldt & Yar, 2016; 簡鳳容; 2018)；本研究綜合網路犯罪被害人被害時段、被害途徑和加/被害人關係等網路使用情境，觀察網路犯罪被害情境機會的集中性；結果發現各類型網路犯罪被害情境的綜合集中性均超過75%，其中侵害著作集中率為92%，網路詐欺集中率為86.2%，因此，網路犯罪的情境機會並非隨機分布，且以犯罪被害類型不同，被害情境也有所不同；本研究有關網路犯罪情境集中特性假設獲得支持。針對不同的網路犯罪被害型態，了解被害人與情境機會之集中特性和差異，有助於於網路犯罪被害預防與偵查。

根據LRAT理論，人口特性會影響個人的網路生活型態，使其暴露於被害風險情境，而成為合適標的物，在監控缺乏情況下導致犯罪被害 (Vakhitova, Reynald, & Townsley, 2015; Holt, Bossler, Malinski, & May, 2016; Leukfeldt & Yar, 2016)；因此，網路犯罪被害人的入口與情境特性存在顯著關聯。本研究資料分析結果顯示，性別、年齡、教育程度和職業類型與被害發生時間、被害途徑與加/被害人關係之關聯性皆達顯著水準；例如：女性在下午、入口網站/社群網站或認識加害人的比率高於男性，但男性在凌晨、論壇/聊天室被害比率則高於女性；發生在夜晚或論壇/聊天室的網路犯罪被害人平均年齡較低，但加/被害人關係為陌生者的平均年齡較高；教育程度為國中以下者在論壇聊天室或社群網站被害比率高於高中或專科以上；而專業主管則大都在入口網站或拍賣網站接觸到加害人；因此，網路犯罪被害人的入口特性確實會影響其被害情境的分布，此項結果支持本研究的假設二；因此，預防網路犯罪被害對策仍需因時制宜，針對不同族群之生活型態而有分眾宣導措施。

本研究另一項目的在觀察人口特性和情境機會是否會影響網路犯罪被害損失；二元羅吉斯迴歸分析結果顯示，人口特性與情境機會對於網路犯罪被害損失均具有顯著影響力，各影響因子中以被害途徑對網路犯罪被害損失影響力最為顯著，其次為被害人的教育程度，再其次為加/被害人關係。整體而言，男性、年紀越輕、職業類型為學生/家管、被害時段在夜晚、被害

途徑為拍賣網站或論壇聊天室和與加害人為陌生人等狀態下遭受網路犯罪被害，則有損失的比率較高。

就性別而言，本研究的結果與葉雲宏(2008)、Ndubueze、Igbo和Okoye(2013)等人研究發現相似，男性網路犯罪被害損失風險顯著高於女性；因此，未來研就可致力於網路犯罪被害的性別差異分析，並探究此種性別差異產生的原因。此外，本研究以官方資料為基礎，樣本年齡以31-40歲居多，其次為18-25歲，二者合計占51.6%，樣本之年齡結構與陳玉書、王秋惠(2011)網路詐欺被害調查結構相似。進一步觀察年齡與網路犯罪被害之關係，結果顯示年齡與被害損失風險有顯著關聯性，被害人年齡越大者，其損失風險越小；未來研究可進一步觀察不同年齡層樣本的網路犯罪被害類型與損失金額多寡的關聯性，以及加害人年齡是否與被害人之年齡有所互動。

過去研究顯示被害人教育程度、職業與網路犯罪被害存在顯著關聯性(黃祥益, 2006; 葉雲宏, 2008; Leukfeldt & Yar, 2016); 本研究發現大專以上被害人損失風險最低，高中組損失風險為大專以上的1.448倍；國中以下組損失風險為大專以上的3.129倍。在職業方面，由於國內多數網路犯罪被害調查以學生或青少年居多，因此有關網路被害人職業類別的訊息相當有限；本研究結果顯示專業主管被害人損失最低，學生家管組損失風險為專業主管的1.448倍；其他職業類別則無統計意義。Yar(2005)認為在網路世界中有能力的監控者較現實社會少很多；Bossler和Holt(2009)、Grzybowski(2012)、Ngo和Paternoster(2011)認為個人的網路與電腦使用技術和知識，可以協助察覺和辨識網路風險，而將之視為網路個人監控力(personal guardianship)。本研究發現在被害人中，教育程度較高與職業為專業主管者，網路犯罪被害時較不易有損失；因此，提供網路使用者良好的使用電腦、網路或通訊軟體安全訊息和知識，以及提升使用能力，亦可降低網路犯罪被害或減少被害損失。

Leukfeldt和Yar(2016)認為，網路特性提供LRAT理論中有價值、可移動、可見和可及的標的物，並符合VIVA條件；然加害人需要藉由可以接觸被害人的途徑，方能達到犯罪的目的；本研究發現，被害途徑對於網路犯罪被害損失最具影響力，儘管52%被害途徑為入口網站和論壇聊天室，然相較於被害途徑為入口網站，拍賣網站造成損失風險最高，其次為論壇聊天室，再其次為社群網站。相關研究顯示，個人進入網路世界的途徑深受網路文化和生活型態的影響(Pratt, Holtfreter, & Reising, 2010; Van Wilsem, 2011; 2013; Reyns, 2013; Vakhitova, Reynald, & Townsley, 2015; Reyns, Henson, & Fisher, 2016; Leukfeldt & Yar, 2016; 簡鳳容, 2018)。本研究

結果應證個人網路犯罪被害的途徑，反映出其在網路世界的生活型態（如人際互動、消費、學習和娛樂等），以及被害損失的風險。

就加/被害人關係而言，加害人如為「陌生」的被害損失風險最高，「認識」者次之；本研究受限於官方資料對於概念的測量，僅能觀察到現象的狀況，無法知悉加/被害人關係形成的原因。具高風險的生活型態可能使被害人無法知悉加害人訊息，而產生大量的陌生加害人或不清楚加害人狀況。Choi (208) 研究顯示，風險生活型態（如下載免費軟體/音樂/影片、開啟任何附加檔案）為影響網路犯罪被害的顯著因子；Leukfeldt 和 Yar (2016) 亦以避免打開來路不明的郵件/附檔測量網路風險知覺，並發現網路風險知覺可以降低駭客入侵和網路詐欺。因此，提供網路使用者辨識風險連結和訊息，以及養成安全的網路生活型態和使用習慣，應為降低網路犯罪被害的關鍵。

本文分析資料係採用刑事局 2010 至 2019 年刑案資料庫中網路犯罪被害人原始資料進行分析，資料取得相當不易，立基於大樣本的被害資料，對於網路犯罪被害趨勢、型態、被害人人口特性和主要情境特徵，能夠有較完整的描述，並找出變數之間可能存在的關聯性與影響力。然受限於官方資料特性，研究變數測量僅能採用資料建立時分類和測量方式，研究者雖儘可能找出符合研究目的與理論概念的測量變數，仍無法完整的檢驗 LRAT 理論中的概念。目前國內對於大樣本的網路犯罪被害之相關研究仍在累積當中，網路犯罪被害不僅態樣多元，被害人特性與被害情境的互動方式都有很多不同之處，後續研究者亦可針對不同網路犯罪被害型態做深入的觀察，可能發現更豐富完整的資訊。如能結合國內外相關研究文獻，設計完整的調查問卷進行調查，則可進一步檢驗 LRAT 理論。

刑案資料庫中有關犯罪與被害人資料，大都建立在報案時狀態，因而無法窺知報案以後實際結果，例如加/被害人關係中「不清楚」占相當比率，顯示被害人報案當下未能確認是否認識加害人；如將「不清楚」排除，則遺漏值過多，影響統計分析。建議官方能在破案後確認加/被害人關係，以利未來研究者可持續觀察官方資料所呈現之訊息，並提供更新的網路犯罪被害特性與趨勢。

本研究樣本來源為警察機關官方資料庫，樣本特性與自陳報告或被害調查有所不同，研究結果較適宜推論有實際報案紀錄之網路犯罪被害人；另由於被害人 3 人以上之資料較為龐雜，為使統計分析維持穩定結果，同時有助於觀察個人特性與被害情境之關聯性，在整理樣本時僅篩選被害人人數 2 人以下之案件，是以解釋被害人特性與被害情境關係時，無法完全推估 3 人以上的集團性網路犯罪被害母體。

最後，我國目前官方資料之網路犯罪被害數據散見各處，經檢視2010至2018年之法務部《犯罪狀況及其分析》，均未有探討網路犯罪之完整單元；相較於美國聯邦調查局之全國犯罪報告（Uniform Crime Reports）與國家犯罪被害調查（National Crime Victimization Survey）均有網路犯罪（Cyber Crime）專欄資料可稽；英國國家統計辦公室（Office for National Statistics）出版「英格蘭與威爾斯犯罪狀況（Crime in England and Wales）」則將網路犯罪歸類為「電腦濫用（Computer Misuse）」；日本法務省犯罪白書（以令和元年版為例）其第5章亦有闡釋網路犯罪（サイバー犯罪）之專章。根據臺灣網路資訊中心（TWNIC）每年公布的「臺灣網路報告」，網路已成為國人日常生活不可或缺之一部分，在人手一機、連網天涯之今日，犯罪被害之型態亦隨之轉型，我國之《犯罪狀況及其分析》實有將網路犯罪與被害成立專文討論之必要，以與時俱進、順應國際潮流。



## 參考文獻

### 中文文獻

- 王秋惠(2007)。網路詐欺被害特性與被害歷程之研究。中央警察大學犯罪防治研究所碩士論文。
- 王茜(2014)。網路成癮，網路偏差及網路被害者之關係：人的聚合還是網路活動場域的聚合？。臺北大學犯罪學研究所碩士論文。
- 吳峻豪(2008)。國中學生網路使用行為、網路成癮和自我概念之研究-以台中縣為例。中華大學科技管理研究所碩士論文。
- 吳嫦娥(2004)。台北市少年網路成癮傾向及網路被害現況調查。青少年國際網路使用相關問題與防治對策學術研討會論文集，47-48。
- 周憐嫻(2014)。青少年網路虛擬身份與網路被害、不當行為。犯罪與刑事司法研究，(22)，45-73。
- 許春金、陳玉書、莫季雍等(2000)。臺灣地區犯罪被害經驗調查研究。法務部、內政部警政署委託研究。
- 許春金、陳玉書等(2005)。臺灣地區犯罪被害調查。內政部警政署委託研究。
- 許春金、陳玉書等(2010)。99年臺灣地區犯罪被害調查。內政部警政署。
- 許維維(2009)。國中生網路虛擬財物竊盜之加害人與被害人特性分析。臺北大學犯罪學研究所碩士論文。
- 陳玉書、王秋惠(2011)。網路詐欺被害特性分析。執法新知論衡，7(2)，11-31。
- 陳玉書、邱炫棉(2006)。犯罪被害恐懼感影響因素之分析。犯罪防治學報，7，1-42。
- 陳玉書、曾百川(2007)。網路詐欺犯罪理性選擇歷程之質性分析。中央警察大學犯罪防治學報，8，115-146。
- 陳怡儒(2010)。少年網路霸凌被害因素研究-以日常活動理論分析。國立中正大學犯罪防治所碩士論文。
- 陳昭佑(2010)。臺北市國小學童家庭環境對網路成癮影響之研究。臺北市立教育大學社會科教育學系碩士論文。
- 黃俊祥(2007)。少年網路偏差與犯罪行為成因之研究。中央警察大學犯罪防治研究所博士論文。
- 黃祥益(2006)。臺灣地區少年網路犯罪與被害特性之研究。中央警察大學犯罪防治研究所碩士論文。



- 楊垂青(2005)。少年網路沉迷之研究-子女與父母管教之觀點。國立中正大學犯罪防治所碩士論文。
- 葉雲宏(2008)。網路詐欺犯罪被害影響因素之研究。中央警察大學犯罪防治研究所碩士論文。
- 蔡田木、周文勇、陳玉書等(2009)。詐騙犯罪被害人屬性之研究。刑事警察局委託研究。
- 蔡田木、許春金、陳玉書(2015)。104年臺灣地區犯罪被害調查。內政部警政署委託研究。
- 盧浩權(2005)。青少年網路沉迷現象與生活壓力、負面情緒之相關研究，靜宜大學青少年兒童福利研究所碩士論文。
- 賴克宗(2005)。大學生網路犯罪被害研究-以國立中正大學學生為例。國立中正大學犯罪防治所碩士論文。
- 簡鳳容(2018)。網路偏差行為與被害特性及其影響因素之研究。中央警察大學犯罪防治研究所博士論文。
- 顏如佑(2005)。青少年網路成癮相關因子之研究。高雄醫學大學行為科學研究所碩士論文。

#### 外文文獻

- Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3 (1), 400.
- Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, 73, 394-402.
- Choi, Kyung-Shick (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2 (1), 308.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.
- Craig, W., Harel-Fisch, Y., Fogel-Grinvald, H., Dostaler, S., Hetland, J., Simons-Morton, B., & Pickett, W. (2009). A cross-national profile of bullying and victimization among adolescents in 40 countries. *International journal of public health*, 54, 216-224.
- Felson, M. (1998). *Crime and everyday life*. Thousand Oaks, CA: Sage.
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal*

- crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.
- Hinduja, S., & Patchin, J. W. (2014). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* Corwin Press.
- Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32* (2), 108-128.
- Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth’s on-Line victimization and perpetration. *Deviant Behavior, 37* (5), 585-600.
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37* (3), 263-280.
- Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber crime victimization among internet active Nigerians: An analysis of socio-demographic correlates. *International Journal of Criminal Justice Sciences, 18* (2), 225-234.
- Ngo, F. T. & R. Paternoster. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5* (1), 773-793.
- Phillips, E. (2015). *Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending.* Bridgewater State University.
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47* (3), 267-296.
- Reep-van den Bergh, C. M. M. & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7* (1).
- Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers. *Crime Prevention & Community Safety, 12* (2), 99-118.
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50* (2), 216-238.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization.

- Criminal justice and behavior*, 38 (11), 1149-1169.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, 32 (2), 148-168.
- Taylor, T.L. (2006). *Play between Worlds: Exploring Online Game Culture*. Cambridge, MA: MIT Press.
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32 (2), 169-188.
- Van Wilsem, J. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review*, 29 (2), 168-178.
- Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29 (4), 437-453.
- Yar, M. (2005). The Novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, 2 (4), 407-427.

#### 網址

- 內政部警政署 (2020)。警政統計通報：108 年網路犯罪概況。網址：<https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=95821&ctNode=12594&mp=1>。
- 臺灣網路資訊中心 (TWNIC) (2019)。2019 臺灣網路報告。網址：<https://report.twNIC.tw/2019/>。
- 國家發展委員會 (2019)。108 年性別數位機會發展現況 (手冊)。網址：<https://www.ndc.gov.tw/cp.aspx?n=55c8164714dfd9e9>。
- Federal Bureau of Investigation (Ed.) (2020). 2019 Internet crime report. <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.
- Grzybowski, M. K. (2012): An Examination of Cybercrime and Cybercrime Research: Self-control and Routine Activity Theory. Arizona: Arizona State University. Available at [http://barrettdowntown.asu.edu/wpcontent/uploads/2012/05/Grzybowski\\_An-Examination-of-Cybercrimeand-Cybercrime-Research\\_-Self-control-and-Routine-ActivityTheory](http://barrettdowntown.asu.edu/wpcontent/uploads/2012/05/Grzybowski_An-Examination-of-Cybercrimeand-Cybercrime-Research_-Self-control-and-Routine-ActivityTheory).