

青少年間におけるサイバー犯罪の加害と被害

: 広がり・リスク要因および防止戦略

Cybercrime Perpetration and Victimization among Adolescents: Prevalence, Risk Factors and Preventive Strategies

Keynote Speaker: **Dennis S. W. Wong**

Professor, Department of Social and Behavioural Sciences,

City University of Hong Kong, Hong Kong

キーワード: サイバー犯罪、日常活動理論、RAPID-IT-CRY、因子分析、加害と被害の相関関係

司 会: **笹倉 香奈** (甲南大学 法学部 教授)

日 時: 2021年6月20日(日) 13:00-14:30 セッション: Keynote Session

龍谷大学がホスト校となり、2021年6月18日(金)～21日(月)の4日間にわたり国際学会「アジア犯罪学会 第12回年次大会(Asian Criminological Society 12th Annual Conference, 通称: ACS2020)」をオンラインで開催しました。2014年の大阪大会に次いで国内では2回目の開催となる今大会では、アジア・オセアニア地域における犯罪学の興隆と、米国・欧州などの犯罪学の先進地域との学術交流を目的としています。

大会の全体テーマには『アジア文化における罪と罰: 犯罪学における伝統と進取の精神 (Crime and Punishment under Asian Cultures: Tradition and Innovation in Criminology)』を掲げ、「世界で最も犯罪の少ない国」といわれる日本の犯罪・非行対策と社会制度・文化に対する理解を広めることを目指しました。

LIVEで行われた本大会の基調講演(Keynote Session with Q&A Session)の概要を紹介します。

報告要旨

【はじめに】 インターネットやソーシャルネットワークが急速に普及し、情報通信技術 (ICT) は、教育、金融、社会、そして個人の活動に様々な機会をもたらした。デジタル時代における ICT の進歩は、私たちの日常生活に利便性とリスクの両方をもたらす諸刃の剣でもある。サイバー行動に関

するこれまでの研究においては、インターネットで多くの時間を費やす青少年は、通常よりネガティブなオンライン体験をする傾向があることが明らかになっている。

本報告では、まず、サイバー犯罪の定義と種類が示された後、青少年のサイバー犯罪被害の典型例を紹介が紹介された。これらを踏まえ、「日常活動理論 (routine activity theory)」を理論的基礎として、香港において1,533人の中高生を対象に行われた実証研究の成果に基づき開発されたサイバー犯罪リスクの簡易測定ツールである「青少年のためのサイバーリスクの反応速度 (RAPID) 識別ツール」“RAPID-IT-CRY”が紹介された。

【用語の定義】 サイバー犯罪は、国境のないサイバー空間で行われる。また、犯罪は組織的に行われることが多い。加害者と被害者が異なる国に所在することが多いのもその特徴である。犯罪類型は、プライバシー侵害犯罪、コンピュータ関連犯罪、データ関連犯罪および著作権侵害の4種類に分けることができる。国連薬物犯罪事務所 (UNODC) は①サイバー依存犯罪 (Cyber-dependant crime)、②サイバー無力化犯罪 (Cyber-enabled crime) および③児童に対する性的搾取・虐待 (Child sexual exploitation and abuse) の3つの分類している。犯罪の発生地であるサイバー空間は、①サーフェイス・ウェブ(誰もがアクセス可能)、②ディープ・ウェブ(特定の者のみがアクセス)および③ダーク・ウェブ(利用者の匿名化)の3つに分けることができる。

【香港におけるサイバー犯罪】 香港におけるサイバー犯罪には、①ビジネスメール詐欺、②ネットショッピング詐欺、③恋愛(ロマンス)詐欺、④ランサムウェアの使用による犯罪、⑤エレクトロニックバンキング詐欺、⑥チャットなどで交換した裸の写真・動画の悪用脅迫および⑦雇用詐欺があり、近年、増加傾向にある。

【少年が被害者となるサイバー犯罪】 少年の被害は、①ネット上のいじめ、②青少年の誘い込み (チャイルド・グルーミング)、③性的ゆすり行為 (セクストーション) などがある、ウォン教授は、これらの現象は、「日常活動理論 (routine activity theory)」によって最も適切に説明できる、と述べた。この理論は、犯罪は「動機付けられた加害者」「対象として適切な被害者」および「両者の接近を阻む障碍の不存在」という3つの要素が同時に存在する時に発生すると考える。現サイバー空間、とりわけ、青少年にとってのサイバー空間は、これらの3要素が準備されていると言える。

香港における1533人の中高生を対象とする調査研究の成果に基づいて、サイバー犯罪の発生リスクを簡易に測定するツールとして「ラピッド・イット・クライ (RAPID-IT-CRY)」が開発された。このツールは、8項目の尺度を用いた因子分析によって、内部的一貫性と併存的妥当性において良好な関係

を有することが確認された。このツールは、特に介入プログラムの現場実施者のために実務的に有用である。今後は、サイバー犯罪一般を予防するための認知行動的アプローチや実証研究のツールに応用されていく可能性もある。

【むすび】 実証研究の結果、インターネットに対する安全意識の欠如、自分は大丈夫だという根拠のない信念、道徳意識の欠如など、被害者のリスク要因が発見された。加害者と被害者との関係に一定の関係性があることも確認されている。少年をサイバー犯罪から護るための予防・介入対策としては、①潜在的加害者との接触制限、②少年の注意力の喚起および③オンライン保護者(online guardians)の増強と拡大がある。

質疑応答 (Q&A) 要旨

質問1: 「サイバー犯罪」にヘイトスピーチは含まれますか?

回答1: はい、含まれます。「サイバー犯罪」には、サイバー上での逸脱行為やサイバー上での加害行為が含まれます。迷惑なメッセージや卑猥なメッセージを送ることは、ヘイトスピーチに関連する可能性があります。

質問2: 香港では、子どもは何歳からコンピュータに触れるのですか?

回答2: 香港では、小学校では6歳からコンピュータの使用が許可されており、家庭学習や宿題を提出する際にもコンピュータやiPadを使用することが推奨されています。

COVID-19の流行時には、多くの学校が閉鎖され、ほぼ全ての子どもがコンピュータやiPadにアクセスできるようになっています。政府や地方団体が、子どもたちがコンピュータを利用できるように資金援助を行いました。多くの専門家は、居間にコンピュータを置き、子どもがインターネットを閲覧する様子を親が監視するように、とアドバイスしています。若い人たちはインターネット上の情報に対して脆弱で、サイバー犯罪被害を避けることはできません。

サイバー犯罪者は非常に巧妙ですが、若い人たちは彼らが使う手口に気付いていません。親は、インターネットの潜在的な危険性について子どもたちと話し合うべきです。また、世界中で起きている様々な事件を記憶し、子どもに共有して伝えていくべきです。

質問3: 香港では伝統的な犯罪が減少し、サイバー犯罪が増加しているのでしょうか?

回答3: 香港では、少年の非行件数は全体的に減少しています。子どもたちは家にいて、サイバースペースでコミュニケーションをとっています。街に出ることはほとんどないので、現在の主な非行犯罪はサイバー犯罪と薬物摂取です。

質問4: アジアや香港における、サイバー犯罪の特色は?

回答4: 他の国で発表された記事を読んだことがありますが、世界的に見てサイバー犯罪には大きな違いはないと思います。多くの若い人たちは、自分たちのことを「グローバル・シティズン」と呼んでいます。彼らがインターネットで遊んだり、コミュニケーションをとったりするとき、違いもあるものの、同じような文化を持っています。サイバー犯

罪における加害と被害も似ています。しかし、アジア人には道徳不活性化が見られ、そのためインターネットの利用が多く、被害者になりやすいのです。一方、欧米では親がリベラルで、サイバーセキュリティに対する意識が高いようです。

国によって文化的な偏りがあることは確かです。例えば、香港や台湾、中国本土では、人口のほとんどが中国人であるため、ヘイトクライムはあまり起こりません。いわゆる人種差別も、中国本土ではそれほど深刻ではありません。一方、アメリカやヨーロッパでは、文化的な移動があり、異なる人種が混在しているため、文化的な差別が多く見られるかもしれません。これは問題になるかもしれません。

東洋の文化は集団主義で、西洋は個人主義です。そのため、アジアでは介入や制限はより権威的なものとなります。文化の違いですね。サイバー犯罪は国境や文化を超えています。しかし、以上のような文化的な違いがあるため、国を超えた協力は非常に困難です。

質問5：香港ではネット上のグルーミングやセクスティングは違法ですか？日本では違法ではないのですが。

回答5：香港の法律は時代遅れです。香港には、オンラインやサイバー関連の法律はありません。従来 of 法律や条例があるだけです。そのため、サイバー犯罪に関する法律の制定を求める声が高まっています。例えば、ネット上でのグルーミングの場合、法律がないため、警察は「コンピュータの違法使用」で起訴します。すべてが「違法なコンピュータの使用」としてまとめられるのです。良い弁護士を雇ってこのことを主張すれば、起訴を免れることができるかもしれません。

文責：笹倉 香奈／協力：ドリス・ハラス