SNSを通じたサイバー犯罪に関する青少年の意識調査
―Web調査から―

矢　作　由美子
（文教大学教育研究所客員研究員）

Investigation on Young People's Awareness of Cybercrimes through SNS: Based on Web Surveys

YAHAGI YUMIKO
(Guest Researcher of Institute of Education, Bunkyo University)

要　旨

本報告は、調査結果から得られた被害者の特性を明らかにするとともに、それを通じてサイバー非行解明の糸口を発見することを目的としている。

理論的観点としては、「日常活動理論（routine activity theory）」と「社会的学習理論（social learning theory）」を理論的基礎として、質問項目を検討し実施した。SNS上で悩み相談が行われているA団体の掲示板を活用し、18歳から23歳までとしWeb調査を実施した。その結果、回答数は138名得られ、その結果を報告する。

はじめに

インターネットとスマートフォンの普及により、誰もが手軽に情報を発信・受信できるようになった。しかし、スマートフォン利用においてトラブルも増えている。例えば、高額な請求が発生する課金トラブルや個人情報の流出などである。本調査でも「悪口」や「知り合った人」とのトラブルが多いことが分かった。そこで、本報告は、我が国のサイバー犯罪の実態について、ネット上で今の思いを匿名で語り、参加者が相互に悩みを相談するA団体の管理者の協力を得て、Web調査を実施した。その調査結果から得られた被害者の特性を明らかにするとともに、それを通じてサイバー非行解明の糸口を発見することを目的としている。

理論的観点としては、「日常活動理論（routine activity theory）」と「社会的学習理論（social learning theory）」を理論的基礎として、今回の調査の質問項目を検討し実施した。日常活動理論は、Cohen & Felsonによって提唱されたもので、「犯罪は、動機も持った犯罪者、適当な被害者、監視者の不在という３要件が満たされた場合に成立するとし」…「加害者も被害者もリスクの高いウエブサイト等を利用する機会が多いので、インターネット上の非行と被害者の相関関係は高いとされる」（四方、pp.21-22）。また、「社会的学習理論からは、犯罪者・非行少年は、インターネット上の非行仲間からサイバー犯罪の方法を習得することがみとめられる」（Lenkfekdt.2017, Holt. 2012, Shinner. 1997, 四方、p.17）また、インターネットの利用時間の長さや特定のウエブサイトの利用がサイバー犯罪被害に影響することが認められている（holt & Bossler. 2013, Bossler. 2012, 四方、p.22）とし、ネット上の情報掲示板から得た情報を利用して、独学で習得していく者が多い。こうした先行研究に基づき質問項目を作成した。

また、今回の調査質問のうち、対象者の中高時代を尋ねる回想項目がある。数年の違いではあるが、コロナ禍になる前の家庭でのネット環境での回答ということになる。承知の通り、文部科学省では新型コロナウイルス感染拡大による緊急事態宣言を受け、当初令和５年度にタブレット端末１人１台を達成するとしていたが、達成時期を前倒しして令和３年度中の実現を目指すなど、学校教育の在り方が一変し、かつ、家庭学習の時間が増え、インターネット利用については、自分用のパソコンやタブレットを持つ児童、生徒も増えた。その為、本調査の結果もまた違ってくることが予想されるが、今回の報告は、調査結果に従い中間報告とする。

１．対象

年間１万４～５千件を超える投稿（青少年からの投稿数が延べ１日、未成年者だけで40件程度）があるSNSサイトの管理者から協力を得ることが可能となった。オンラインアンケートの性質上、18歳未満にアンケートを取ることが困難を極めることから、対象者は、18歳から23歳までとした。

Web調査を実施した結果、回答数は138名（男 性24.4％、女性65.2％、その他9.4％）からの回答を得た。

２．調査方法

インターネット上で、年間１万４～５千件を超える投稿（青少年からの投稿数が延べ１日、未成年者だけで40件程度）があるSNSサイトの管理者から協力を得ることが可能となった。そのサイトの利用者の多くは、青少年であり、その方々に対し、非行・被害の経験の有無や、それら青少年の特性について、サイトの運営代表とスタッフの方々に協力を仰ぎつつ、質問項目を作成し、Webアンケート調査の実施に向け準備を進めた。

悩み相談が行われているＡ団体の掲示板を対象に、2021年１月１日から2021年４月末日までWeb調査を実施した。なお、回答者に対しては、Ａ団体のサポーター１年分を謝礼とした。

今回、協力してくださった団体は匿名で悩みを語り合うサイトで、そこで投稿している方々に呼びかけてWeb調査を実施したものである。事前に質問項目の相談など、対象者についてもＡ団体へ聞き取りを行った。聞き取りから対象者には、『「家庭環境」「保護者との関係性」「虐待」「性被害」という複雑な事情を抱えている相談者が多く含まれていること。また、そのため親の監視の眼が行き届かない面があり、ネットマナーが低い傾向にあるのではないか』という意見をもらった。また、『中には「僕」という言葉を使うなど、性別がわからない人もいる。』とのことから、性別選択では「その他」の選択肢を加えた。

また、分析方法としては、単純集計、χ^2検定、及びFisherの正確性確率検定を行い、残差分析の結果は、値が－1.96より小さいか1.96より大きいのであれば、５％ P＜0.05未満水準で有意で、また、－2.58より小さいか2.58より大きいのであれば１％ P＜0.01未満水準で有意とする。

なお、字数の関係上、調整済み残差による頻度の差が見られなかった結果については、今回の報告に記述として反映していない箇所が多数あることをお断りしておく。

３．研究倫理

倫理委員会の承認を受けていないが、警察政策学会のプライバシーポリシーに基づき、倫理的な配慮と研究倫理上の課題の検討を以下の通り行った。

（１）対象者に与える影響について

Webアンケート調査は、対象者の非行経験や被害経験など、重要なプライバシーに関する調査であり、対象者に心理的影響を与

える可能性があり得るものといえる。そこで、①保護者の同意を得ることが困難で、これを求めることとすると調査の実施が不可能となることから本アンケートを18以上とし、未成年に対して実施していない。②Webを通じて行うものであり、対面調査ではないことから、対象者は心理的影響を受けにくいこと、③調査に当たっては、回答したくない質問に対しては回答する必要がないことを明記することにより、心理的影響を受ける可能性のある者からの回答を避けることができること、④対象者の心の深層に及ぶような質問は含まれないこと。

（2）プライバシーの保護について

①Web調査を実施するに当たり、本アンケート調査は、対象者の非行経験や被害経験など、重要なプライバシーに関する調査であることから、調査結果の秘密保持には万全を期すこと。②研究者において情報の管理を徹底するとともに、アンケートの委託業者との間では、契約において秘密保持条項を設定すること。③アンケートの結果は、利用目的である研究目的以外には使用しないこと。

4．結果

4－1　性別とインターネット利用方法の関連性

（1）インターネット利用方法（パソコン）と「性別」の関連性

インターネット利用方法については、スマホ、パソコン、ゲーム機、タブレットでパソコンでの利用（自分・家族共用・使用していない）の有無と性別の関連についてみた。

パソコンと性別の関連性についての分析は、χ^2検定（χ^2（4）=15.511, p<0.01, p=0.002, V＝0.233）、及びFisherの正確性確率検定を実施した。関連度を表す連関係数はV＝0.233で有意で、残差分析の結果はp<0.01だった。

パソコンでのネット利用については、「男子」は「自分」のを利用するが有意に多く、「女子」は、「自分」のを「利用する」が有意に少なかった。特に、「女子」は「パソコンを使用していない」が有意に多かった。

（2）ネットへの書き込み（友達ID・アカウント等）と性別の関連性

インターネットへの書き込み（友達ID・アカウント等）の有無と「性別」の関連についての分析は、χ^2検定（χ^2（2）=15.511, p<0.05, p=0.016, V＝0.244）およびFisherの正確性確率検定（5.923　P－0.032）を実施したところ、関連度を表す連関係数V＝0.244で有意で、残差分析の結果はp<0.05だった。

「男子」と「女子」ともに、頻度の差も見られなかったが、性別で「その他」を選択した人のうち、ネットに「友達のID・アカウント」の書き込みしたことが「ある」が有意に多かった。

（3）インターネットの書き込み（自分の写真）と性別の関連性

インターネット上の書き込み（自分の写真）の有無と性別の関連性の関連についての分析は、χ^2検定（χ^2（2）= 6.833, p<0.05, p=0.033, V＝0.223）、およびFisherの正確性確率検定（p＝0.31）を実施した。関連度を表す連関係数は、V＝0.223で有意で、残差分析の結果はp<0.05であった。

ネット上に自分の写真の書き込みをしたことの「ある」「男子」は、有意に少なく、「ない」が有意に多かった。「女子」は、書き込みをしたことが「ある」が有意に多く、「ない」は有意に少なかった。したがって、「女子」は、「男子」と「その他」に比べ、ネット上に「自分の写真」を書き込む頻度が有意に多かった。

（4）ネット上での個人情報・プライバシーの流失と性別の関連性

インターネット上で個人情報・プライバシーの流失のトラブルに巻きまれたことと、性別の関連性についての分析は、χ^2検定（χ^2（2）= 6.269, p<0.05, p=0.044）、およびFisherの正確性確率検定（p＝0.031）を実施した。関連度を表す連関係数は、V＝0.213で有意で、残差分析の結果はp<0.05であった。

「個人情報等の流失」トラブルは、「女子」は「男子」に比べ、「ある」が有意に多かった。したがって、「女子」は、「個人情報・プライバシーの流失」トラブルに巻き込まれやすいことが示された。

（5）コンピューターウイルスの作り方を調べたことと性別の関連性

コンピューターウイルスの作り方を調べたことの有無と「性別」の関連性の関連についての分析は、χ^2検定（χ^2（2）=10.336, p<0.01, p=0.009,）、およびFisherの正確性確率検定（p＝0.31）を実施した。関連度を表す連関係数は、V＝0.274で有意で、残差分析の結果はp<0.01であった。

ウイルスの作り方について調べたことの有無については、「男子」は、頻度の差は見られなかったが、「女子」は、ウイルスの作り方をしらべたことが「ある」は有意に少なく、「ない」は有意に多かった。

また、性別で「その他」を選択した人のうち、「ある」が有意に多かった。したがって、性別で「その他」の人のうち、コンピューターウイルスの作り方を調べたことが「ある」が多く示された結果から、ウイルスの作成を通して学べることはたくさんあるが、調べているだけで眺めて終われば良いが、場合によっては、違法行為へと繋がる結果は否めない。

（6）ネット上で他人に悪意を持って嫌な思いをさせたことと性別の関連性

ネット上で他人に悪意を持って嫌な思いをさせた有無と「性別」の関連についての分析は、χ^2検定（χ^2（2）=9.335, p<0.01, p=0.009）、およびFisherの正確性確率検定（p＝0.008）を実施した。関連度を表す連関係数は、V＝0.260で有意で、残差分析の結果はp<0.01であった。

他人に悪意を持って嫌な思いをさせたことについて、「男子」は「ある」が有意に多く、「ない」が有意に少なかった。「女子」は、「ある」が有意に少なく、「ない」は有意に多かった。したがって、「男子」は、ネット上で他人に悪意を持って他人に嫌な思いをさせた頻度が有意に多いことが示された。

その悪意が何かは不明であるが、先の結果で「男子」は、自分のパソコンを所持している割合が高く、様々な学習意欲も広がり得ることが容易になることから、学習次第では例えば、悪口程度から違法行為につながる可能性はあるといえる。

4－2　Twitter のアカウント数が複数と実際の出会いの関連性

（1）Twitter のアカウント数２個以上と、中高生時に実際に会うことの関連性

Twitterのアカウント数が２個以上の有無と中高の時に実際に会ったことの有無の関連性の分析は、χ^2検定（χ^2（1）=11.4839, p<0.001, p=0.001）、およびFisherの正確性確率検定（p＝0.001）を実施した。関連度を表す連関係数は、ϕ＝0.288で有意で、残差分析の結果はp<0.001であった。

Twitterのアカウント数２個以上「はい」の人のうち、中高の時に実際に会ったことが「ある」は有意に多く、「ない」は有意に少なかった。

したがって、Twitterのアカウントを複数所持している人は、SNS上で知りあった人と、

中高生時代に、様々な目的に合わせて興味関心から実際に出会いに繋がっていることが分かった。

4－3　トラブルの有無と危険性の認知の関連性

（1）「課金」でトラブルに巻き込まれたことと、危険性の認知との関連性

インターネット上の課金で、トラブルに巻き込まれた有無と危険性の認知の関連性の分析は、χ^2検定（χ^2（1）=10.543, p<0.01, p=0.005,）、およびFisherの正確性確率検定（10.198、p＝0.008）を実施した。関連度を表す連関係数は、V＝0.276で有意で、残差分析の結果はp<0.01であった。

課金でのトラブルに巻き込まれたことが「ある」人のうち、危険性を「知っている」は有意に少なかった。また、課金でのトラブルが「ない」と答えた人のうち、危険性を「知っている」が有意に多かった。したがって、課金でのトラブルがあった人が、危険性を十分理解していないことが示された。

（2）有料サイトでトラブルに巻き込まれたことと、危険性の認知との関連性

インターネット上の有料サイトでトラブルに巻き込まれた有無と危険性の認知の関連性の分析は、χ^2検定（χ^2（2）=8.403, p<0.05, p=0.015）、およびFisherの正確性確率検定（8.743、p＝0.014）を実施した。関連度を表す連関係数は、V＝0.247で有意で、残差分析の結果はp<0.05であった。

有料サイトでのトラブルに巻き込まれたことが「ある」人のうち、インターネットの危険性について「よく知っている」は有意に多く、「知っている」は有意に少なかった。また、有料サイトでトラブルに巻き込まれたことが「ない」人のうち、ネット上の危険性を「よく知っている」が少なく、「知っている」は有意に多かった。

したがって、危険性を「よく知っている」ことで自分は大丈夫と過信しているのか、トラブルに巻き込まれており、逆に、危険性を「知っている」程度の方が、トラブルを回避している結果であった。

（3）電話番号の書きこみと、危険性の認知との関連性

ネット上に「電話番号」の書き込みしたことの有無と、危険性の認知の関連性の分析は、χ^2検定（χ^2（2）=15.373, p<0.05, p=0.032）、およびFisherの正確性確率検定（7.707、p＝0.032）を実施した。関連度を表す連関係数は、V＝0.334で有意で、残差分析の結果はp<0.05であった。

ネット上に「電話番号」の書き込みしたことが「ある」人のうち、インターネットの危険性について「知らない」は有意に多かった。

また、ネットに「電話番号」の書き込みしたことが「ない」人は、危険性についてはある程度知っていた。

今回の調査結果から、危険性を認知しないまま「電話番号」を書き込んでいる人が一定数いることから、電話番号は、家の特定や携帯電話にSNSで架空請求などの被害につながりかねない結果といえる。

（4）メアドの書きこみと、危険性の認知との関連性

ネット上に「メアド」の書き込みの有無と、危険性の認知に関連性の分析は、χ^2検定（χ^2（2）=19.253, p<0.01, p=0.005）、およびFisherの正確性確率検定（9.959、p＝0.008）を実施した。関連度を表す連関係数は、V＝0.374で有意で、残差分析の結果はp<0.01であった。ネット上に「メアド」の書き込みしたことが「ある」人のうち、ネットの危険性について「知らない」は有意に多かった。

また、ネット上に「メアド」の書き込みをしたことが「ない」人のうち、危険性につい

てはある程度知っていた。したがって、電話番号と同様に、メアドを書き込んだ人のうち、危険性を認知しないまま書き込んでいる人が一定数いることが分かった。

４－４　利用時間との関連

（１）平日の一日の利用時間と Twitter のアカウント数との関連性

平日の一日の利用時間とTwitterのアカウント数との関連性について、分析は、χ^2検定（χ^2（１）=11.973, p<0.01, p=0.001,）を実施。関連度を表す連関係数は、V＝0.374で有意で、残差分析の結果はp<0.01であった。

平日のインターネット利用時間が「３時間以内」の人のうち、Twitterのアカウントが２個以上「ある」は有意に少なかった。

また、利用時間が「４時間以上」の人のうち、Twitterのアカウントが２個以上「ある」人は有意に多く、「ない」は有意に少なかった。

したがって、ネットにつなげている時間が長い人ほど、Twitterのアカウントが2個以上になるが、他のSNSを利用しながら長時間ネット利用していると考えられる。

（２）平日の一日の利用時間と他人の ID・パスワードでログインとの関連性

平日の一日の利用時間と他人のID・パスワードでログインしたことの有無の関連性について分析は、χ^2検定（χ^2（２）=6.607, p<0.01, p=0.010）及びFisherの正確性確率検定（p＝0.020）を実施した。関連度を表す連関係数は、ϕ＝0.219で有意で、残差分析の結果はp<0.05であった。

平日のインターネット利用時間が「3時間以内」という人が、他人のID・パスワードでログインしたことが「ある」は有意に多く、したことが「ない」は有意に少なかった。また、ネット利用時間が「４時間以上」という人が、他人のID・パスワードでログインしたこと「ある」は、有意に少なく、「ない」は有意に多かった。したがって、他人のID・パスワードでログインした人のうち、ネットにつなげている時間は３時間以内という結果が示された。

（３）平日の一日のネット利用時間と、一月当たりの利用金額の関連性

質問項目では、平日の一日のネット利用時間について（①60分以内、②１－３時間以内、③４－５時間以内、④－９時間、⑤10時間以上）尋ねた。

それを、２分割にして、「３時間以内」と「４時間以上」とし、一月当たりの利用金額「１円～３千円未満」、「３千円～１万未満」、「１万～５万未満」、「５万以上」、「なし」との関連性をみた。

分析は、χ^2検定（χ^2（４）=14.743, p<0.01, p=0.005）及びFisherの正確性確率検定（15.283, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.327で有意で、残差分析の結果はp<0.01であった。

一日利用時間が「３時間以内」では、「１～３千円」が有意に少なく、「０円」が有意に多かった。「４時間以上」では、「１～３千円」が有意に多く、「０円」は有意に少なかった。

詳細にみると、一日利用時間60分以内が「１万～５万未満」と有意に多く、「１時間から３時間以内」は「０円」が多かった。また「１～３千円」は有意に少なかった。これらの結果から、平日一日の利用時間の長さに比例して、月平均の利用金額が上がっておらず、お金をかけずに「０円」、つまり「無料」をうまく活用しているということだろう。

５．ハッキングの知識と危険性の関連性から

（１）ハッキングの知識と、ネット上の危険性の認知の関連性

インターネット上の危険性の認知と、他人のコンピューターやサーバーをハッキングす

る知識との関連性についてみていく。分析は、χ^2検定（χ^2（４）=27.711, p<0.01, p=0.001）及びFisherの正確性確率検定（18.296, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.317で有意で、残差分析の結果はp<0.01であった。

危険性を「知っている」人のうち、ハッキングが「できる」が有意に少なかった。逆に、危険性について「わからない」と回答した人のうち、ハッキングが「できる」が有意に多く、「できない」が有意に少なかった。

つまり、ネット上の危険性について「わからない」と曖昧に回答する人の中に、ハッキングが「できる」人が一定数いることから、「危険性を分かっている」と答えたくない心理が働いたものと考えられる。

（２）ハッキングの知識と、有料サイトでのトラブルの関連性

インターネット上のハッキングの認知と、有料サイトでトラブルに巻き込まれた有無の関連性についてみていく。その分析は、χ^2検定（χ^2（２）=11.729, p<0.01, p=0.003）及びFisherの正確性確率検定（7.887, p＝0.014）を実施した。関連度を表す連関係数は、V＝0.292で有意で、残差分析の結果はp<0.05であった。

ハッキングすることが「できる」人のうち、「有料サイト」のトラブルに巻き込まれたことが「ある」は有意に多く、「ない」が有意に少なかった。

したがって、ハッキングが「できる」知識がある人の中で、有料サイトで何らかのトラブルに巻き込まれていることが示された。

（３）ハッキングの知識と、ネット上の売買トラブルとの関連性

ハッキングの知識と、ネット上の売買でのトラブルの有無との関連性についてみていく。χ^2検定（χ^2（２）=15.263, p<0.01, p=0.001）及びFisherの正確性確率検定（8.751, p＝0.01）を実施した。関連度を表す連関係数は、V＝0.333で有意で、残差分析の結果は、p<0.01であった。

ハッキングすることが「できる」人のうち、「ネット上の売買」のトラブルに巻き込まれたことが「ある」は有意に多く、「ない」は有意に少なかった。

したがって、他人のコンピューターやサーバーをハッキングすることが「できる」人のうち、ネット上の売買トラブルに巻き込まれたことが「ある」人がいることから、技術的な知識があっても、ネットの売買では何らからのトラブルに巻き込まれていることが示された。

（４）ハッキングの知識と、「その他の犯罪」トラブルとの関連性

他人のコンピューターやサーバーをハッキングすることが出来る知識と、「その他の犯罪」でトラブルに巻き込まれた有無の関連性についてみていく。χ^2検定（χ^2（２）=28.152, p<0.01, p=0.001）及びFisherの正確性確率検定（8.751, p＝0.01）を実施した。関連度を表す連関係数は、V＝0.333で有意で残差分析の結果は、p<0.01であった。

ハッキングすることが「できる」人のうち、ネット上で「その他の犯罪」に巻き込まれたことが「ある」は有意に多く、「ない」は有意に少なかった。

したがって、上記同様、技術的な知識があるのに、「その他の犯罪」で何らからのトラブルに巻き込まれる人が一定数いることが示された。

（５）ハッキングの知識と、一月当たりの利用金額の関連性について

ハッキングの知識と、一月当たりの利用金額は、「１円～３千円未満」、「３千円～１万未満」、「１万～５万未満」、「５万以上」、「な

し」の関連性についてみていく。

χ^2検定（χ^2（８）=53.171, p<0.01, p=0.001）及びFisherの正確性確率検定（28.848, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.439で有意で残差分析の結果は、p<0.01であった。

ハッキングすることが「できる」人のうち、一月当たりの利用金額は、「１万～５万未満」と、「５万以上」が有意に多かった。また、ハッキングが「できない」人のうち、一月当たりの利用金額が、「なし」が有意に少なかった。

また、ハッキングすることが「わからない」と答えた人のうち、一月当たりの利用金額が「３千円～１万未満」が有意に多かった。

したがって、ハッキングすることが「できる」人のうち、一月当たりの利用金額が５万円以上という人もいれば、ハッキングが「できない」人は、お金をかけずに無料の範囲で留まっている人が多いことが示された。

（６）ハッキングの知識と、ネット上の情報掲示板等でアイテム等を売買する知識の関連性

ハッキングの知識と、ゲームの情報掲示板などでアイテムやキャラクターを売買する知識との関連性についてみていく。χ^2検定（χ^2（４）=36.263, p<0.01, p=0.001）及びFisherの正確性確率検定（35.192, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.362で有意で、残差分析の結果はp<0.01であった。

ハッキングすることが「できる」人のうち、ネット上の情報掲示板などを活用し、アイテムやキャラクターを売買するやり方が「できる」が有意に多かった。また、ハッキングできるか「わからない」と回答した人のうち、「できない」は有意に少なく、「わからない」が有意に多かった。

したがって、ハッキングすることが「できる」人のうち、キャラクター等を売買することは容易に行っているといえる。

また、ハッキングができるか「わからない」と回答した人のうち、キャラクターなど売買ができるか「わからない」と答えている人がいるが、少なからず、潜在的には、いずれの知識もある人がいるものと思われる。

（７）ハッキングの知識と、海賊版のマンガ・動画をみる知識の関連性

ハッキングの知識と、インターネットの海賊版のマンガや動画をみる（ダウンロードする）知識の関連性についてみていく。χ^2検定（χ^2（４）=26.847, p<0.01, p=0.001）及びFisherの正確性確率検定（25.296, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.312で有意で、残差分析の結果はp<0.01であった。

ハッキングすることが「できる」人のうち、海賊版のダウンロードのやり方が「できる」人は有意に多かった。したがって、他人のコンピューターやサーバーをハッキングすることが「できる」人は、海賊版のダウンロードは、容易なことだろう。ただし、ハッキングができるか「わからない」人のうち、アイテム等の売買同様に、海賊版のダウンロードができても「わからない」と答えている人のうち、少なからず、潜在的には、いずれの知識もある人がいるものと思われる。

（８）ハッキングの知識と、ウイルスの作り方を調べたことの関連性

ハッキングの知識と、ウイルスの作り方を調べたことの有無について関連性をみていく。χ^2検定（χ^2（２）=19.183, p<0.01, p=0.001）及びFisherの正確性確率検定（12.415, p＝0.001）を実施した。関連度を表す連関係数は、V＝0.258で有意で、残差分析の結果はp<0.01であった。

ハッキングすることが「できる」人のうち、

ウイルスの作り方を調べたことが「ある」人は有意に多く、調べたことが「ない」は有意に少なかった。

また、ハッキングは「できない」人は、ウイルスの作り方を調べたことが「ある」は有意に少なく、「ない」は有意に多かった。

したがって、他人のコンピューターやサーバーをハッキングすることが「できる」人は、ウイルスの作り方を調べることが容易といえ、実際に作ってみた経験のある人が含まれているかは不明であるが、学習意欲が高まれば試してみたくなる人がいないとは限らない結果といえる。

（9）ハッキングの知識と、不正にお金を得る方法を調べたことの関連性

他人のコンピューターやサーバーをハッキングすることの知識と、不正にお金を得る方法を調べたことの有無について関連性をみていく。

χ^2検定（χ^2（2）=21.221, p<0.01, p=0.001）及びFisherの正確性確率検定（14.701, p=0.001）を実施した。関連度を表す連関係数は、V=0.392で有意で、残差分析の結果はp<0.01であった。

ハッキングすることが「できる」人のうち、不正にお金を得る方法を調べたことが「ある」は有意に多く、「ない」は有意に少なかった。

また、ハッキングすることが「できない」では、不正にお金を得る方法を調べたことが「ある」は有意に少なく、「ない」は有意に多かった。

したがって、他人のコンピューターやサーバーをハッキングすることが「できる」人は、不正にお金を得る方法を調べることは容易といえ、実際に不正行為へとエスカレートしていく可能性は否定できない結果といえる。

（10）ハッキングの知識と、他人に嫌な思いをさせたことの関連性

他人のコンピューターやサーバーをハッキングすることの知識と、インターネットで他人に悪意を持って嫌な思いをさせたことの有無について関連性をみていく。

χ^2検定（χ^2（2）=8.667, p<0.05, p=0.013）及びFisherの正確性確率検定（9.003, p=0.016）を実施した。関連度を表す連関係数は、V=0.251で有意で、残差分析の結果はp<0.05であった。

ハッキングすることが「できる」人のうち、他人に悪意を持って嫌な思いをさせたことが「ある」は有意に多く、「ない」は有意に少なかった。

また、ハッキングの技術は「わからない」人のうち、他人に悪意を持って嫌な思いをさせたことが「ある」は有意に少なく、「ない」は有意に多かった。したがって、他人のコンピューターやサーバーをハッキングすることが「できる」人のうち、「ネットで他人に悪意を持って嫌な思をさせたこと」が「ある」が少なからずいる結果が示された。

（11）ハッキングの知識と、他人のID・パスワードでログインしたことの関連性

他人のコンピューターやサーバーをハッキングすることの知識と、他人のID・パスワードで勝手にSNS・ゲーム・サイトにログインしたことの有無について関連性をみていく。

χ^2検定（χ^2（2）=15.263, p<0.01, p=0.001）及びFisherの正確性確率検定（8.751, p=0.01）を実施した。関連度を表す連関係数は、V=0.333で有意で、残差分析の結果はp<0.01であった。

ハッキングすることが「できる」人のうち、他人のID・パスワードでログインしたことが「ある」は有意に多く、「ない」は有意に少なかった。

したがって、ハッキングすることが「で

きる」人のうち、他人のID・パスワードで、勝手にSNS・ゲーム・サイトにログインしたことがある人が一定数いることから、不正行為へとエスカレートしていく可能性は否定できない結果である。

6．考察

（1）トラブルについて

今回の結果からもスマートフォン利用においてトラブルも増えている。ネット上での出逢いと繋がりは広がるばかりである。ツールとしては、Twitterのアカウントを２個以上持っている人は、他のSNS を使い分けながら、興味関心が増え、直接出会うことに抵抗感も薄れているといえる結果であった。それだけに、監視の眼と十分なリテラシー教育が必要と言えるだろう。

今回の調査結果で、Twitterのアカウントを複数所持している人は、SNS上で知りあった人と、特に、女子が、中高生時代に、様々な目的に合わせて興味関心から実際の出会いに繋がっていることが分かった。また、女子に多いのが、安易に「自撮りの写真」を送っていることである。

個人情報の流出との関連で、危険性を認知しないまま「電話番号」、「メアド」を書き込んでいる人が一定数いることが調査結果でも示されている。こうした行為は、家の特定や、携帯電話番号やメールアドレスが危険な業者にわたるなど、後々、SNSに架空請求が頻繁に来ることを招きかねない。同様に、「課金」についてもトラブルを抱えることになった人がいる。自分が考えている以上に、返済トラブルに巻き込まれたことは推測できる。これまでは、保護者を通して課金の支払いがあれば、注意の機会もあったといえるが、18歳以上は成人扱いになった以上、その目が届かないことも増大するだろう。責任もって、使い方をどう正しく理解させていくかが鍵といえる。

ただし、今回の調査で、不正行為につながる技術力の習得に優れている人ほど、自分は大丈夫と過信している人が一定数いた。特に、「有料サイト」、「ネット上での売買」でトラブルに巻き込まれていた。その様な人たちには、報復に繋がらないようにするためにも、事前に相談できる窓口を周知させ、相談する勇気が必要なことを伝えていくしかない。

あるいは。本調査の対象者が、支払いなど基本的な処理能力に幾分弱いところがあるためトラブルに巻き込まれている可能性も否定できない。例えば、本人が、どのような契約かを正しく理解していたのか、契約内容を誤って認識しているかいないか。あるいは、無料期間中に解約手続きを忘れていたため無料期間中に解約手続きができなかった、あるいは解約したつもりが、解約できていなかったといったところだろう。

（2）月の利用金額と海賊版のダウンロードの行為について

ネット上の情報掲示板など活用すれば、有料を無料で楽しめる方法も関連するキーワードを入力し検索すれば、容易に入手できる。例えば、お金の稼ぎ方や売買のやり方、あるいは、海賊版のマンガや動画のダウンロードのやり方など見つけることは容易といえる。そこから実際に、どこまで試行する気になるかである。今回の調査結果でも、月額金額を抑えながら得た情報を使い、違法すれすれのサイトから上手く無料で楽しめる方法を見つけていると思われる。

分析では、月平均の利用金額と、インターネットの海賊版のマンガ・動画を見る（ダウンロードする）知識の関連に有意差はみられなかったが、月額平均が「０円から3000円以内」で、海賊版の知識について「わからない」が有意に多かった。

本調査において、犯罪にかかわる質問については、どうしても回答が、「わからない」

と曖昧な答えは増えてしまう傾向が見られる。

改めて、著作権法をみれば、海賊版コンテンツのダウンロードは、正規版が有償か無償であるかを問わず、原則として違法とされている（著作権法30条１項３号参照）。その一方で、海賊版コンテンツのダウンロードが刑事罰（犯罪）の対象とされているのは、正規版が有償で提供・提示されている場合のみとなっている（同法119条３項）。したがって、こうしたわかりづらい規制があるために、回答者からの正確な回答は得づらくなる。

（３）ハッキングの知識とＳＮＳの利用との関連について

今回の調査結果で、SNSの内、Twitterのアカウントが２個以上あると回答した人、または、Facebookの利用があると、回答した人のうち、ハッキングの知識が「ある」で関連性が多くみられた。

調査結果では「男子」は、自分のパソコンを所持している割合が高く、ハッキングができ、学習意欲がある者のうち、実際に不正行為へとエスカレートしていく可能性は否定できない。彼らを、潜在的な犯罪予備軍ともいえるのではないだろうか。また、性別で「その他」の人のうち、コンピューターウイルスの作り方を調べたことが「ある」が多く示されている。彼らのように、技術的に知識のある者のうち、ネット上で悪意を持てば、様々な方法で嫌な思いをさせることは容易にできる。やった本人は、「悪ふざけのつもり」と言い訳しても、相手にとっては度を超えた行為や、世間を驚かすような事件につながることが懸念される結果といえる。

また、他人のコンピューターやサーバーをハッキングすることが「できる」人は、「他人のアカウントを利用したことがある」や「不正にお金を得る方法を調べること」で有意に多かった。不正なプログラムの作り方を学習する動機については、勉強や好奇心、悪意のいたずら程度に考えている人も多いが、この行為は、なりすまし行為に当たり、不正アクセス禁止法という法律にも違反する行為といえる。

今回、特に、学習意欲が高くハッキング出来る層のうち、ウイルスの作り方を調べるだけにとどまらず、相手に対して悪意を持てば、ウイルスを自作し実際にウイルスを拡散する行為へと進む可能性は否定できない。今回の調査結果からも、動機の解明にもつながる点も見えてきた。

それは、悪意といっても技術的に未熟なハッカーは、個人や組織を困らせたり、復讐したり、混乱させたりしようとするが、特別な目的があるわけではなく、あくまでも相手を困らせることだけが目的になる場合も多いということである。ただし、聞き取り調査から、動機の解明をして行く必要はあるだろう。

おわりに

以前であれば、高度な攻撃を実行するほどの技術はなくても、腕試しや、名声欲しさのような犯罪行為もみられた。しかし、最近では金銭目的につながるケースも増えているのが現状である。SNSを活用し楽しむ若者が増える半面、青少年によるサイバー犯罪については、ここ数年、特に中学生、高校生がマルウェアを作成、さらに感染させたり、不正アクセスを行って金品を強奪したりとサイバー社会でも凶悪な犯罪に手を染める事件を目にする機会が増えている。しかし、我が国における先行研究は、情報モラル教育の観点からのものがほとんどで、犯罪学の観点からの調査はほとんどなされていないため、青少年によるサイバー犯罪とその被害の実態は明らかになっていない。今後も、調査計画に沿って、アンケート調査結果を踏まえた聞き取り調査を実施していく予定である。

参考文献

・四方光「第２章　サイバー犯罪の犯罪学」中野目善則・四方光編著『サイバー犯罪対策』成文堂、2021年、pp.16-35.

・Cohen. L. E. & Felson. M. “Social change and crime rate trends: A routine activity approach”. America Sociollgical Review 44, 1979, pp.588-608.

・Holt. T. J. Bossler. A. M. & May, D. C. 2012, Low self-control, deviant peer association, and juvenile cyberdeviance. American Journal of Crimimal Justice, 37, pp.378-395.

・Leukfeldt. E. R. Kleemans. E. R. & Stol. W. P. 2017, Cybercriminal networks,social tise and online forums: Social ties versus digital ties within phishing and malware networks, British Journal of Criminolgy, 57, pp.704-722.

・Skinner. W. F., A. M. 1997, A social leaning theory analysis of computer crime among college students. Journal of Research in Crime and Delequency. 34, pp.495-518.