

Tashiro, Mitsuteru

Conference Paper

Assessing internet risks among high school students in Kanagawa Prefecture: A 2019 survey and the analysis of factors involving underage internet use

24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Tashiro, Mitsuteru (2024) : Assessing internet risks among high school students in Kanagawa Prefecture: A 2019 survey and the analysis of factors involving underage internet use, 24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/302532>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Assessing internet risks among high school students in Kanagawa Prefecture: A 2019 survey and the analysis of factors involving underage internet use

Mitsuteru TASHIRO*

*Chuo University¹

Keywords: luring minors, smartphones, Social Networking Service, Selfie.

Abstract

In order to mitigate the risk of luring minors using the internet, this study analyzed the current status of risk and its underlying factors based on responses in a questionnaire distributed among high school students in Kanagawa Prefecture, Japan. Results showed that the experience of receiving a message from a stranger saying "I want to meet you" is higher for female students who publish photographs of their face on social media or do not follow family rules on the use of the internet. The proportion of female students responding to a request of sending their photographs with "no" or "consult with a parent or teacher" was higher if they had experience in information literacy education within a year, had content filtering installed on their smartphones, or followed family rules.

Introduction

This study aims to explore preventive strategies against the luring of minors under the age of 18 on the internet (referred to as NET luring hereafter) and analyzes the risks caused by their internet use (NET risks hereafter). According to the WHITE PAPER Information and Communications

in Japan (2020), the household penetration rate of smartphones in 2019 was 83.4%; categorized by age group, 80.2% for those under 12 years old, 98.4% for those aged 13-19, and 99.1% for those aged 20-29. This spread of smartphones in our lives comes with the inevitable (but preventable) risk of an increase in NET luring. A survey by the National Police Agency of Japan (2018) reports that there were a total of 2,082 minors victimized on social networking services (SNS) in the fiscal year of 2019, with the number of serious crimes such as murder, indecent assault, and forcible sexual intercourse jumping from 26 in 2013 to 158.

To prevent NET luring, the Japanese government has legislated the Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use, and for smartphone use, telecommunication carriers such as DoCoMo (2023), KDDI (2023), and SoftBank (2023) offer free filtering as well as zoning services for protecting minors by verifying user age. In addition, telecommunication companies, service providers, and private foundations provide educational instructors to elementary, junior high, and high schools to offer classes on information ethics [LINE (2015), DoCoMo (2023b), KDDI (2023b),

¹ Specially Appointed Associate Professor, Chuo University.
E-mail: tmitsuteru001@g.chuo-u.ac.jp
Chuo UNIV. 742-1 Higashinakano, Hachioji-city, Tokyo
192-0393 Japan

SoftBank (2008)]. As a regulation by public sectors, the Tokyo Metropolitan Board of Education (2016) promotes the “SNS Tokyo Rule”, and the Cabinet Office of Japan (2017) as well as other organizations distribute leaflets on “What parents can do now”. As an outreach program of private companies and foundations, DoCoMo (2023c), KDDI (2023c), and SoftBank (2023b) implement regulations for smartphone use. Service providers such as LINE Mirai Foundation (2020) and Yahoo (2023) as well as their affiliated foundations and many other private organizations have launched outreach initiatives.

While one counter-approach against the NET risks may be to disallow or limit the minors’ use of smartphones or other devices, this practice would not be a fundamental solution to the problem as the penetration rate of smartphones is already high among minors and there are certainly social as well as educational advantages to using them. Against this background, this study investigates the current risks associated with minors’ internet use based on the concept of safety management. Mukaidono (2016) states that safety (of any kind) can be enhanced in three aspects: technical aspects, human aspects, and organizational aspects. In this study, I investigate effects of the following three control measures for securing safety: content filtering (or parental controls) as a technical aspect, information literacy education as a human aspect, and family rules on the use of the internet as an organizational aspect. Based on results from a survey, I examined the effectiveness of these control measures through statistical analysis of collected responses.

Review of Previous Survey and Research Related Surveys

The National Police Agency of Japan (2018) summarizes the current status of NET luring in *The current status of crimes due to the use of SNS* published in *The status of juvenile delinquency, child abuse, and sexual abuse in 2019*. According to the survey, there were a total of 2,082 cases of NET luring that led to victimizations, of which 844

pertained to the violation of the Child Welfare Act and the Youth Protection and Development Ordinance, 28 Violation of the Child Welfare Act, 482 concerned child prostitution, and 671 related to child pornography. Major crimes also included 1 murder, 49 forced sexual intercourse, 46 kidnaping, and 15 forced indecency. The survey also reported that among those cases, 1,867 were through the use of mobile phones (89.6%), of which 1,845 (88.6%) were via the use of smartphones. Among 1,722 cases that were subsequently investigated by police, there were only 13.4% of parents reporting to have installed filtering on their child’s mobile devices.

A similar report can be found in *The survey on internet use among youth in 2023* by the Children and Families Agency of Japan (2023). In the report, the use of filtering was 44.2% among elementary school students and 33.3% among high school students, presenting higher rates of filtering use than those reported by the National Police Agency. Additionally, when asked about rules at home regarding the use of the internet, 41.9% of high school students answered that they had some rules at home, whereas 47.5% did not. Among those family rules, 33.2% pertained to monitoring in-app purchases, 24% on the use of apps, and 16.4% related to how long and where one can use mobile phones. Regarding education on information literacy, 90.7% of high school students had taken a course, with 97.3% of those cases offered at school, 24.8% by parents, and 17.5% from other media such as television, books, and brochures.

Lastly, LINE MIRAI Foundation (2019) has an ongoing large-scale survey in collaboration with the Tama University Kumon Center and the Kanagawa Prefectural Board of Education. The survey shows that 33% of high school students who became friends on the internet were students from the same high school, and 42% were from different schools. Furthermore, 64% of males met males, and 80% of females met females. As a safety measure, 33% of respondents answered that they had some type of content filtering installed, 16% completely followed family rules on internet use, 24% mostly

followed the rules, and 45% had no rules. Additionally, the survey critically showed that those high school students who published photographs of their faces tended to receive messages from strangers more frequently, and elementary and junior high school students received messages from strangers less frequently if they followed family rules.

Previous Research

There has been some existing research on the three aspects of safety science (the technical, human, and organizational aspects) in relation to NET luring. The technical aspect mostly includes the use of age verification and content filtering. Analyzing data from LINE Play, Toriumi et al (2016). found that most direct messages involving NET luring first asked about the child's age and place of residence. Since most conversations were found to have ended at that point when the recipient turned out to be a minor or have a distant place of residence, it seems that the target of NET luring tends to be those over the age of 18 and/or those who live closer to the sender.

When it comes to the use of age verification systems, LINE Corporation (2015) prohibits minors from setting up LINE IDs and searching individuals by IDs through age verification provided by mobile phone companies, which can prevent minors and adults from being unnecessarily connected. For content filtering, the Ministry of Internal Affairs and Communications (2023) defines filtering as a service that protects juvenile generations from contact with illegal and harmful information and helps them use the internet safely and securely. The Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use also stipulates that, in principle, mobile phone operators are obliged to provide filtering services when the user of internet connection through mobile phones is a minor. Filtering includes such functions as parental controls, restrictions on app usage or usage time, as well as the ability to block access to harmful

websites. Mobile phone carriers such as DoCoMo (2023), KDDI (2023), and SoftBank (2023) provide these services free of charge. Regarding the effectiveness of filtering, the National Police Agency (2018) reported that 91.6% ($n = 1,540$) of victims of internet crimes did not use filtering functions. Since filtering is used by only 30% of mobile phone users, it can be predicted that filtering can make a difference in preventing those crimes. In this study, I examined the difference between age and the presence or absence of filtering to test the effectiveness of the technical aspect.

For the human aspect, education on information literacy can function to provide safety. Orita et al (2016). conducted research on developing teaching materials using manga, and their subsequent study managed to test the effectiveness of using those materials for information literacy education. However, these studies focused on the extent to which participants learned and retained knowledge about information literacy and did not investigate whether such knowledge actually resulted in the reduction of NET risks through changes in behavior. The current study directly examined the effectiveness of information literacy education in more pragmatic terms, Orita et al.(2010).

Lastly, on the social aspect of safety assurance, Chiba et al(2014). surveyed 300 pairs of middle or high school students with their mothers. They found that while there was no correlation between whether or not junior high or high school students met strangers online and whether the students had rules at home, when there were no family rules, the students were more likely to be exposed to violent images or videos as well as abusive language. Additionally, children who were aware of the family rules of avoiding suspicious or potentially harmful websites were found to have less experience seeing harmful information.

The Current Study

Participants and Survey Period

I conducted a large-scale survey and

quantitatively analyzed the responses. I sent out questionnaire forms to public high schools in Kanagawa Prefecture, Japan, in collaboration with the Prefectural Board of Education. Individual teachers distributed the questionnaires to students in classrooms. After filling out the questionnaire, the student responses were sealed in a special envelope to prevent any spread of (potentially) personal information. The responses were sent to the KUMON Center at Tama University, Japan. Any personal information collected in the survey was handled in accordance with the ethics guidelines of the university. The survey took place between October and December of 2019, with a total of 3,465 people (2,144 valid responses) recruited from four public high schools.

Hypotheses based on Previous Surveys and Research

The Target of Analysis

Based on the results of previous surveys and research, this study investigated the effectiveness of drawing on the three aspects of safety science (technical, human, and organizational aspects) to prevent NET luring that involves minors. While existing research focused on only one aspect of safety science, this study simultaneously examined all three aspects. For the target of analysis, I selected two dependent variables: (1) the previous experience of receiving direct messages from a stranger for a meet-up and (2) whether one can appropriately respond to requests from a stranger for sending one's selfie. The justifications follow.

To quantify the incidents of NET luring, I chose to measure the experience of receiving solicitation messages over the past year (DM/Y hereafter). Annually, approximately 2,000 people experience assaults or other victimizations due to NET luring. While it is desirable to examine the incidents of assaults themselves, it is generally difficult to estimate the number of people with such experiences because asking to report the experience can be psychologically traumatic to recollect. Even if those questions adequately revealed the exact

degree of victimizations, the identification of victimizations must always be followed by police actions and psychological or clinical care for the victims. These hurdles make it challenging to directly examine the extent of victimizations caused by NET luring. The survey study by the LINE Mirai Foundation reported that 30.2% of respondents answered yes to the question "Have you experienced any of the following in the past year? A stranger sent me a message on SNS or via a messaging app saying they wanted to meet me." Compared to directly asking about the experience of victimizations, I believed that this question would yield a sufficient number of responses for analysis.

Additionally, I investigated whether respondents (high school students) can appropriately handle the situation when they are requested by a stranger to send their selfie. The National Police Agency of Japan confirms that requests for sending one's selfies are as frequent and risky as NET luring. Similar to the incidents of NET luring, however, it is also difficult to recruit a sufficient number of respondents through a questionnaire by asking such questions as "I have sent a nude picture of myself to a stranger." Additionally, police actions and psychological care will also be necessary after finding incidents of victimizations. Therefore, the current study instead focused on whether students respond appropriately to requests for a selfie, such as by refusing to send or consulting with a parent, teacher, or counselor (hereafter, this variable will be called SelfieRR: selfie request response).

Factors Affecting the Target of Analysis

Based on the previous studies, I hypothesized that the following five variables can influence the dependent variables (DM/Y and SelfieRR): gender, age, and the three aspects of safety assurance. For gender, most victims of NET luring are females. Hence, DM/Y, the experience of whether one has received solicitation messages, is predicted to be higher for women than men. As a predictor variable

in the subsequent multinomial logit analysis, gender was defined as a dummy-coded categorical variable, x_1 (0 for female, 1 for male). Furthermore, I hypothesized that if one has posted a photograph of his/her face on a SNS profile, the person will have a higher value of DM/Y because they would be more visible, especially if one is a woman. This variable was defined as face photo, x_2 , dummy-coded as 1 if one has posted a selfie and 0 if one has not.

Regarding age, Toriumi et al. reported that solicitation emails often asked one's age and the place of residence as the first question. This is probably because the sender wants to avoid minors due to the influence of the Youth Protection and Development Ordinance. Since one's age and date of birth can be highly personal information and difficult to manage, I instead focused on the school grade at the time of the survey. It was predicted that the frequency of DM/Y would be lower in the first and second grades and higher in the third grade because students in the first two grades are minors (i.e., less than 18 years old). Being in the 3rd grade was defined as x_3 and coded as 1 if one was in the 3rd grade (or part-time 4th grade) and 0 if one was in the 1st or 2nd grade.

Lastly, the three aspects of safety science were expected to have an inhibitory effect on the dependent variables. The technical aspect referred to the use of content filtering, the human aspect pertained to the experience of information literacy education, and the organizational aspect concerned the status of compliance with family rules on the internet use. The experience of information literacy education was hypothesized to reduce the risk of NET luring, defined by education, x_4 , and dummy-coded as 1 if one had experienced any information literacy education and 0 if not. For filtering, the National Police Agency of Japan reported that more than 90% of the victims of NET luring did not make use of any filtering services. In this study, it was hypothesized that the use of filtering would prevent potential risks of NET luring. Filtering was defined as x_5 and coded as 1

if one had installed filtering on his/her devices and 0 if one had not. For family rules, the Tokyo Metropolitan Government reported that even if students have rules at home on their internet use, a high percentage of them do not follow the rules. I hence hypothesized that actually following the rules (rather than having the rules) would reduce the risk of NET luring. It was defined as a dummy-coded variable, x_6 , with 1 if one followed family rules and 0 if one did not.

Formulating the Hypotheses

The hypotheses discussed in the previous section were formalized by the following equations (Equation 1-3). Defining the dependent variables, DM/Y and SelfieRR, as y_1 and y_2 , respectively, as well as the independent variables of gender, face photo, age, education, filtering, education, and rules as x_{1-6} , the odds of DM/Y can be defined as $y_1 = f(x_e)$ and those of SelfieRR as $y_2 = f(x_p)$ with the constant terms as b and a_n . The combined influence of the predictors (x_{1-6}) can be defined as $g(x)$:

$$g(x) = b + \sum_{n=1}^6 a_n x_n$$

Hence, the odds ratio of the two dependent variables in connection to the predictor variables can be expressed as follows:

$$y_1 = \frac{e^{g(x_e)}}{1 - e^{g(x_e)}}$$

$$y_2 = \frac{e^{g(x_p)}}{1 - e^{g(x_p)}}$$

Results

Descriptive statistics of data from this survey were already reported and presented by the LINE MIRAI Foundation (2019) In this chapter, I tested the hypotheses using inferential statistics. Table 1 presents the proportion of students having some experience of receiving a direct message from a

stranger (DM/Y) as well as being able to appropriately handle a request to send a selfie. Table 2 shows similar statistics but for the predictor variables (gender, face photo, 3rd grade, education, and filtering). Table 3 displays the proportion of participants with different levels of following family rules.

Table 1 : Percentage of Yes to the Dependent Variables

	Proportion
DM/Y (y_1)	20.0%
SelfieRR (y_2)	74.2%
n = 2,144	

Table 2: Percentage of Yes to the Predictor Variables

	Proportion
Gender (x_1)	50.9%
Face photo (x_2)	31.0%
3rd grade (x_3)	27.6%
Education (x_4)	58.9%
Filtering (x_5)	30.7%
n = 2,144	

Table 3: Percentage on Different Levels of Following Rules

Rules	Proportion
Not followed	48.6%
Somewhat not followed	4.0%
Neither	7.4%
Somewhat protective	24.0%
Protective	16.1%
n = 2,144	

To formally test the hypotheses, I conducted a multinomial logit analysis based on Equation 2 and 3 using the *mlogit* package in the statistical software *R*, created by Yves (2020). Table 4 presents the results for DM/Y. First, there was a difference between male and female students ($b = -0.439$, $SE = 0.115$) with males reporting less experience than females (who had higher values of DM/Y). DM/Y was also significantly higher for those who published the photograph of their face ($b = 0.262$, $SE = 0.119$), which can further increase the frequency of experience for women. However, those who followed any rules at home had significant a lower chance of receiving messages ($b = -0.079$, $SE = 0.035$). 3rd grade, education, and

filtering did not seem to have any influence on DM/Y.

Table 4: Results of the Multinomial Logit Analysis on

	DM/Y			
	Estimate	Std. Error	AMPE	
Intercept	-1.119	0.138	-0.176	***
Gender (x_1)	-0.439	0.115	-0.069	***
Face photo (x_2)	0.262	0.119	0.041	*
3rd grade (x_3)	-0.137	0.128	-0.022	
Education (x_4)	0.091	0.115	0.014	
Filtering (x_5)	-0.152	0.123	-0.024	
Rule (x_6)	-0.079	0.035	-0.012	*

*** $p < 0.001$ ** $p < 0.01$ * $p < 0.05$ and “.” for $p < 0.1$

Similarly, Table 5 presents the summary of results for SelfieRR. The analysis showed that SelfieRR was significantly higher for those who had some experience of information literacy education (education: $b = 0.289$, $SE = 0.104$), indicating that knowledge of information literacy can help students more appropriately respond to a request for sending selfies. The same pattern of results was also observed for filtering ($b = 0.387$, $SE = 0.117$) and rules ($b = 0.096$, $SE = 0.032$), suggesting that those who had installed filtering on their mobile device or followed family rules had a higher chance of appropriately responding to the requests. Lastly, male students were found to be less likely to deal with the requests with appropriate responses.

Table 5: Results of the Multinomial Logit Analysis on

	SelfieRR			
	Estimate	Std. Error	AMPE	
Intercept	1.176	0.132	0.215	***
Gender (x_1)	-0.739	0.109	-0.135	***
Face photo (x_2)	-0.212	0.116	-0.039	
3rd grade (x_3)	-0.190	0.113	-0.035	
Education (x_4)	0.289	0.104	0.053	**
Filtering (x_5)	0.387	0.117	0.071	***
Rule (x_6)	0.096	0.032	0.018	**

*** $p < 0.001$ ** $p < 0.01$ * $p < 0.05$ and “.” for $p < 0.1$

In summary, for gender differences, DM/Y was found to be higher for female students. This was further the case if those female students published

a photograph of their face, which made it possible for strangers to identify that they were a woman. Hence, being a woman and being identified as a woman can lead to the internet troubles such as NET luring. In terms of school grades, there was no significant difference between 3rd grade students and 1st and 2nd grade students. Hence, there was no indication in data that 3rd grade high school students were more likely to be targeted by strangers. With respect to the three aspects of safety science, DM/Y was significantly lower when students followed a family rule on the internet use; SelfieRR was significantly higher when students had received any information literacy education, installed filtering on their device, or followed a rule at home.

Discussion

In this study, I examined high school students' experiences in receiving direct messages from a stranger (DM/Y) and whether they can appropriately respond to requests from a stranger to send their selfies (SelfieRR). For DM/Y, considering that many victims of online kidnapping are women, publishing a photograph of one's face can be thought to increase the risk of NET luring (as reflected in the increase in DM/Y, see Table 4) because the picture allows strangers to identify one as a woman. Unfortunately, providing information literacy education or using the filtering functions did not seem to mitigate the risks. This may be attributed to the fact that DM/Y is a type of passive experience; that is, there is usually no way but to receive direct messages (unless one blocks the sender's account, which is impossible to do preemptively). This can also mean that senders usually send messages indiscriminately to people who they can identify as women. For this reason, it is necessary to take control measures such as encouraging women not to let their female identity be visible, and information literacy education and setting household rules can be used to raise their awareness. Additionally, one should also avoid unnecessarily registering and disclosing one's

gender on SNS. Lastly, results showed that DM/Y did not differ between 3rd and 1st-2nd graders. This may be due to the fact that there is actually not much age difference between those two grade groups. Since DM/Y was the reported experience in the past one year, there may not have been any significant difference in the grades. Analysis of the effects of age hence would require a much wider range of ages to be sampled.

As with DM/Y, men had a significantly lower chance of responding to requests to send a selfie appropriately (see results for SelfieRR in Table 5). This may be because female students tend to be the victims of NET luring, and they may have more experience in dealing with the situation, whereas males were less aware of the issue due to their smaller chance of victimization. However, this does not mean that men are not victimized in NET luring. Information literacy education can be critical in this respect to provide opportunities for male students to become aware of the issue. In this connection, results showed all three aspects of safety science (education, filtering, and family rules) are effective in increasing the chance of SelfieRR. This contrasting difference from that of DM/Y may be because SelfieRR by nature is an active response to engage with the trouble, which contrasts with DM/Y, which is a passive incident. However, it is also possible to project that the three aspects of safety science themselves are effective in controlling trouble such that minors who receive literacy education, install filtering, and follow family rules do not engage in such risky behaviors. In the future, it is critical to focus on what factors may encourage students to follow the three aspects of safety science.

Conclusion

With the spread of the internet and smartphones, the web environment surrounding minors has changed significantly. In particular, due to the rapid spread of SNS, there are many unknown risks associated with the use of the internet for minors. In this study, I analyzed the frequency

of receiving direct messages from a stranger and one's ability to appropriately respond to a request from a stranger by distributing a questionnaire survey among high school students. I focused on the impact of the following three aspects: gender, age, and safety science. As a result, I found that DM/Y was significantly higher among women who disclosed their face photos, significantly lower when they followed household rules on the internet use; SelfieRR was lower among men, and significantly higher when there were three elements of safety science in place. These results indicated that the three aspects of safety science, namely information literacy education, installation of filtering, and adherence to household rules, may be effective in reducing NET risk.

On the other hand, it can be predicted that while women had a higher rate of getting direct messages from a stranger, men were less able to appropriately respond to requests for sending a selfie, and probably, they should exhibit a higher proportion of actually sending the picture. As information literacy education, installation of filtering, and following domestic rules were found to be effective, it is necessary to set up profiles (in SNS) that do not disclose one's gender and this can be discussed in family rules as well as in literacy education.

References

Ministry of Internal Affairs and Communications , JAPAN (2020), 'Information and Communications in Japan WHITE PAPER2 2019 ',
<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nb000000.html>, access:2023/12/1.

National Police Agency(2018), '平成 30 年における SNS に起因する被害児童の現状',
https://www8.cao.go.jp/youth/kankyau/internet_to_rikumi/kentokai/41/pdf/s4-b.pdf,
access:2023/12/1.

NTT DOCOMO, INC. (2023), 'filtering service',
<https://www.docomo.ne.jp/service/filtering/>,

access:2023/12/1.

KDDI CORPORATION (2023), 'filtering service',
<https://www.au.com/mobile/service/filtering/>,
access:2023/12/1.

SoftBank Corp. (2023), 'filtering service',
<https://www.softbank.jp/mobile/service/filtering/>,
access:2023/12/1.

LINE Corporation (2015), '年齢認証を用いた機能制限',
<https://linecorp.com/ja/csr/newslit/ja/2015/6>,
access:2023/12/1.

NTT DOCOMO, INC. (2023b), 'スマホ・ケータイ安全教室',
<https://www.docomo.ne.jp/corporate/csr/social/safety/educational/>., access:2023/12/1.

KDDI CORPORATION (2023b), 'KDDI の情報モラル講座',
<https://www.kddi.or.jp/kyoshitsu/>.,
access:2023/12/1.

SoftBank Corp. (2008), '青少年の安心・安全な携帯電話利用を目指す考えよう、ケータイ～情報モラル授業プログラム～の開始について',
https://www.softbank.jp/corp/group/sbm/news/press/2008/20081210_01/., access:2023/12/1.

Tokyo Metropolitan Board of Education, JAPAN (2016), 'SNS Tokyo Rule',
https://www.kyoiku.metro.tokyo.lg.jp/administration/pr/files/tokyo_no_kyoiku201601_es/1071e.pdf,
access:2023/12/1.

Cabinet Office. JAPAN (2017), 'What parents can do now',
https://www8.cao.go.jp/youth/kankyau/internet_us_e/h29/pdf/leaf-2.pdf, access:2023/12/1.

NTT DOCOMO, INC (2023c), '子どもにスマートフォンを持たせる前に保護者が知っておきたいこと',
<https://www.docomo.ne.jp/corporate/csr/social/safety/parents/>, access:2023/12/1.

KDDI CORPORATION (2023c), 'スマホ・ケータイファミリーガイド (ルールを考かんがえよう!)', <https://www.kddi.com/family/rules/>, access:2023/12/1.

SoftBank Corp. (2023b), '親子で作るスマホルールリスト',
<https://www.softbank.jp/mobile/special/sumaken/rulelist/>, access:2023/12/1.

LINE MIRAI. Foundation (2020), 'SNS ノート',
https://scdn.line-apps.com/stf/linecorp/ja/csr/sns_note_20200301.pdf, access:2023/12/1.

Yahoo Japan Corporation (2023), 'インターネットを上手に使おう',
<https://kids.yahoo.co.jp/study/integrated/information/inf002.html>, access:2023/12/1.

Mukaidono M. (2016), '入門テキスト安全学', TOYO KEIZAI INC...

Children and Families Agency, JAPAN(2023), '令和5年度「青少年のインターネット利用環境実態調査」報告書',
https://www.cfa.go.jp/policies/youth-kankyoku/internet_research/results-etc/r05, access:2023/12/1.

LINE MIRAI. Foundation (2019), '青少年のネット利用実態把握を目的とした調査 平成30年度最終報告書',
<https://linecorp.com/ja/csr/newslist/ja/2019/205>, access:2023/12/1.

Toriumi F., Nakanishi T., Tashiro M., Eguchi K.

(2016), 'Encounters between Predators and Their Targets in Private Chat', *Journal of transformation of human behavior under the influence of infosociomics society*, 1, pp 23-28.

Ministry of Internal Affairs and Communications, JAPAN (2023), 'フィルタリング (有害サイトアクセス制限サービス) をご存じですか?', https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html, access:2023/12/1.

Orita A., Tashiro M., Yoshikawa A., Eguchi K.(2016), 'オリジナルマンガ教材による中学生向け情報リテラシー教育の実践', *IPSJ SIG Technical Report Vol.2016-EIP-72 No.12*, pp1-6.

Orita A., Yoshikawa A., Yamamoto H. (2010), 'Preliminary Report of Privacy Education by a MANGA Case', *IPSJ SIG Technical Report Vol.2010-EIP-50 No.30*, pp1-7.

Chiba N., Seki Y., Horikawa Y., Hashimoto Y. (2014), 'A Study of Home Measures for Children's Safe Internet Use', *Journal of Information Processing Society of Japan*55(1), pp311-324.

Yves C. (2020), 'Estimation of Random Utility Models in {R}: The {mlogit} Package', *Journal of Statistical Software*95(11), pp1-41.

Attachment

Questions used in this study

(1) In the past year, have you ever received a message from a stranger asking you to meet them?

- 1 Yes
- 2 None

(2) What would you do if someone you became close to online asked for a photo of you?

1. Send because you trust
2. Send a photo that does not identify you
3. Decline
4. Talk to an adult, such as a parent or teacher
5. Others
6. I don't know

(3) Gender

man

woman

I don't want to answer

(4) Do you disclose your personal information on social networking sites or messaging services?

1. Yes
2. No

(5) Grade

Freshman

2nd Grade

3rd Grade

Part-time 4th grade

(6) Have you taken any courses on mobile phones or the Internet at school in the past year?

1. Yes
2. No

(7) Is filtering set up on your phone?

1. Yes
2. No

(8) Do you follow the rules for using mobile phones and computers at home?