Sociology Study, June 2017, Vol. 7, No. 6, 331-340
doi: 10.17265/2159-5526/2017.06.004

Impact of Cybercrime in Japan—Findings of Cybercrime Victimization Survey

Taisuke Kanayama[a]

Abstract

Although the threat of cybercrime is said to expand year by year recently, an actual impact of the threat has not estimated in Japan due to several reasons including inadequate statistics of cybercrime. The purpose of this study is to estimate the volume of cybercrime in Japan and identify its characteristics based on the result of cybercrime victimization survey conducted by the study group for cybercrime of Nihon University (NU) in 2016. The study group obtained a cybercrime victimization rate of 5.36% and concluded that cybercrime victimization in Japan is quite serious comparing with other survey results and crime statistics. Furthermore, the study group explored how to figure out cybercrime victimization more precisely based on characteristics of cybercrime obtained by this survey and proposed a couple of appropriate measures to cope with cybercrime.

Keywords

Cybercrime, victimization survey, victim's report

The annual number of Penal Code crimes has decreased consecutively in Japan from 2.8 million in 2002 to 1 million in 2016. On the other hand, the annual number of cybercrimes has constantly been increasing. According to police crime statistics [National Police Agency (Japan) 2017a], the number of cybercrimes was approximately 8,000 in 2016. When comparing the number of cybercrimes with Penal Code crimes, the former is too small to show a real impact. Therefore, in 2017, a comprehensive cybercrime victimization survey over the Internet was conducted. Based on the results of this survey, the actual volume of cybercrime and losses caused by it were estimated. This was followed by an analysis of why the hidden number of cybercrimes was larger than conventional crimes. Finally, a solution for reducing hidden cybercrime was explored. This study was conducted with the support of the Nikkoso Research Foundation for Safe Society.

CURRENT CRIME TRENDS IN JAPAN

Japan faced a sharp increase in crime in the late 1990s, such that the number of all recorded Penal Code crimes in 2002 represented a 160% increase over the number reported in 1996. As a result, the Japanese police took strong measures to reduce crime, focusing on both street crimes and break-ins at homes and offices. Additionally, in 2002, the police began to take steps to lead the crime prevention policy of the government. In 2003, the Japanese Government set up

[a]Nihon University, Japan

Correspondent Author:
Taisuke Kanayama, College of Risk Management, Nihon University, 1-34, 3-chome, Shimouma, Setagaya-ku, Tokyo 154-8513, Japan

a ministerial committee for crime reduction, which was composed of ministers from all branches of the government. In this meeting, a national action plan was set in motion that mobilized all possible resources to fight crime. This plan was designated the Action Plan to Create a Crime-Resistant Society (Cabinet Office 2003).

Since the inauguration of the national plan, the number of Penal Code crime recorded by the police has been consecutively decreasing for 14 years. On the other hand, the annual number of cybercrime has been increasing steadily since the year 2000 (see Figure 1).

Figure 1 shows the displacement of crime from Penal Code crime to cybercrime. However, the absolute number of cybercrime is far smaller than Penal Code crime at less than one percent. In a national poll[1] on the safety on the Internet, 56.3% respondents claimed to have a sense of fear on the Internet, for which the major reasons given were leaking of personal information and Internet fraud. The results of this poll are indicative of the impact of cybercrime that cannot be elucidated from crime statistics. As a result, a study group in Nihon University (NU) conducted a comprehensive cybercrime victimization survey through the Internet to clarify the impact of cybercrime. Hereafter, this survey is called "NU Survey".

SURVEY METHOD

The participants of this study were extracted among registered monitors of an Internet research company[2] (N = 13,000). They consisted of a comprehensive national sample of Japan based on population statistics, including age, gender, and prefectures. The survey questionnaire was composed of 25 questions that covered a wide range of cybercrimes and cybersecurity related issues. The survey was conducted in February 2017. The participants responded to the questionnaire over the Internet.

SUMMARY OF THE FINDINGS

Victimization Rate

The number of participants who replied that they experienced victimization through cybercrime in 2016 was 1,623, or 12.48%. However, cybercrimes reported by 1,623 participants included crimes that were not related to obvious or substantial losses, such as the simple detection of malware. Therefore, the author estimated each report of cybercrime, which indicated that the number of participants who experienced substantial losses by cybercrime was 1,420, or 10.92%. The main types of cybercrime included damaging the function of computers, illegal access, threats or extortion, and fraud (see Figure 2). Table 1 shows the *modus operandi* of fraud (cash and property).

Monetary Losses

The number of participants that had experienced a monetary loss was 244, or 1.9% with the highest monetary loss reported as being five million yen (≒ $ 45,000), whereas the median loss was 15,000 yen, (≒ $ 140). The percentage of those that had experienced losses over 100,000 yen (≒ $ 9,000) was 19.5%.

Victims' Reports to the Police and Other Institutions

Victims that had reported a crime to the police or another institution were 32%. In other words, two-thirds of cybercrime victims did not report the crime (see Figure 3). Furthermore, the percentage of cybercrime victims that reported the crime was much lower than that for conventional crimes; consequently, the actual volume of cybercrime could be much larger than the figure indicated by police crime statistics.

PREVIOUS STUDIES ON CYBERCRIME VICTIMIZATION

Crime Victims Survey (CVS)[3]

The Research and Training Institute (RTI) of the

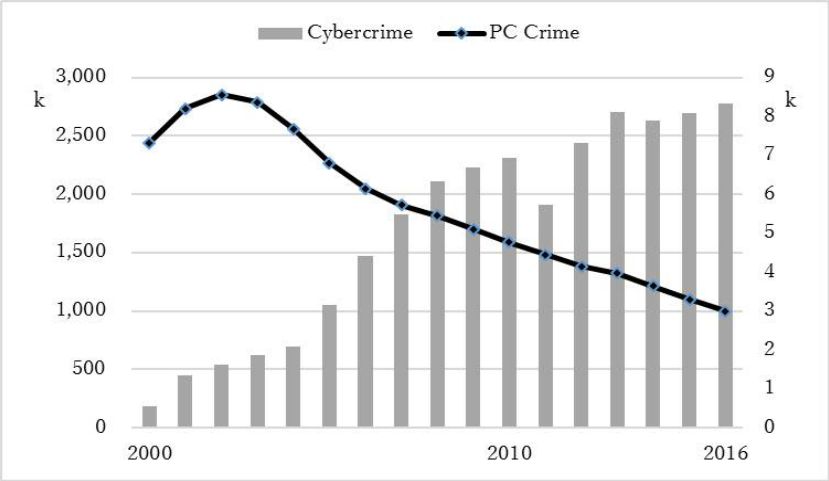

Figure 1. Annual Numbers of Penal Code Crimes and Cybercrimes in Japan.

Note: Author's original graph on police statistics.

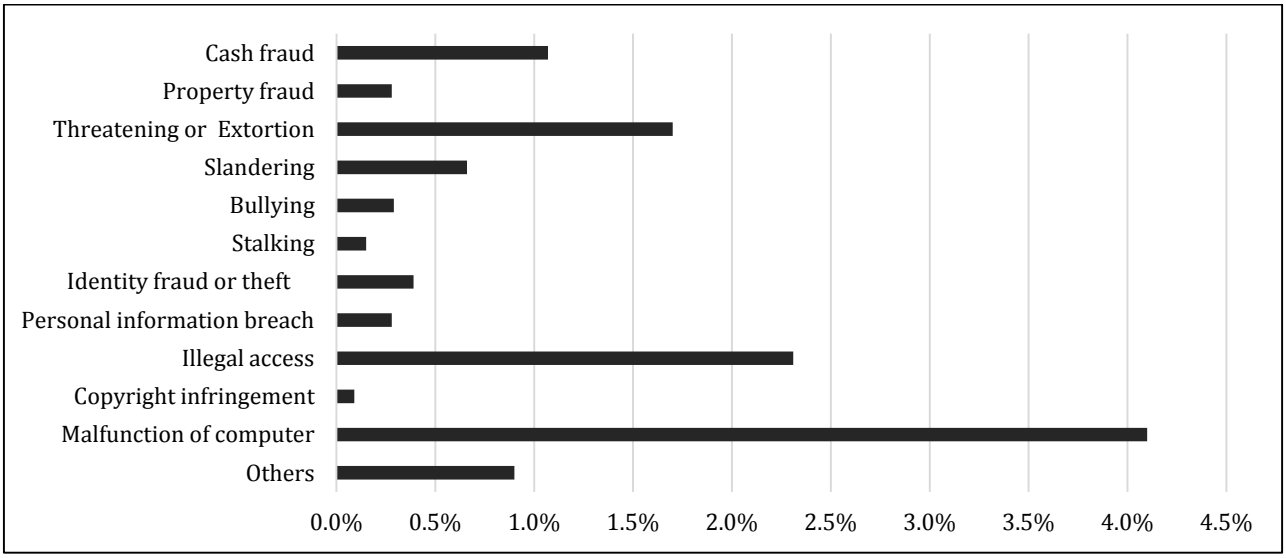

Figure 2. Types of Cybercrime.

Table 1. Modus Operandi of Fraud

Modus operandi	%
Internet auction fraud	.36
Online shopping fraud	.32
Credit card fraud	.12
Takeover of an account	.17
Payment fraud	.07
Romance fraud	.10
Lottery fraud	.04
Click fraud	.04
Other	.13

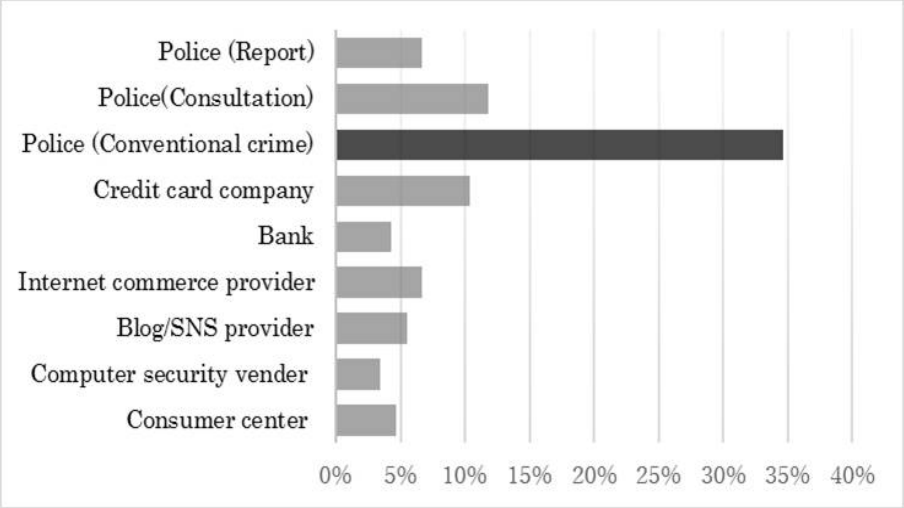

Figure 3. Victims' Reports.

Ministry of Justice in Japan had participated in the International Crime Victims Survey (ICVS) from 2000 and had conducted Crime Victims Surveys every four years: 2000, 2004, 2008, and 2012. A two-stage stratified random sampling method was used in each of these surveys conducted nationwide to select male and female participants aged 16 years old or older. The number of survey subjects varied such that it was 3,000 in 2000 and 2004 surveys, 6,000 in the 2008 survey, and 4,000 in the 2012 survey. The 2012 survey was based on a mail survey, in which a questionnaire was mailed to survey participants, who were asked to return it after completing their responses. It thus differed from the previous three surveys using interviews, which were mainly conducted by visiting interviewers (Japanese Ministry of Justice 2012). Moreover, the surveys conducted in 2008 (CVS 2008[4]) and 2012 (CVS 2012[5]) included an original question on Internet auction fraud. The number and percentage and the rate of auction fraud victimization indicated by these surveys are shown in Table 2.

Annual Communication Usage Trend Survey of Japan in 2016[6]

The Ministry of Internal Affairs and Communications in Japan has conducted the Annual Communication Usage Trend Survey (MIC survey) since 1990, targeting households (households and household members) and enterprises. The 2016 survey was conducted by mail, and it requested participants to return their responses by mail or online. The questionnaires including questions on damage incurred by using the Internet were sent to 40,592 households, and 17,765 responses were returned (Ministry of Internal Affairs and Communications 2016). The MIC survey included claims of victimization that were not recognized as causing substantial damages, such as the simple detection of malware and the reception of junk email. After excluding claims resulting in non-substantial damages, the survey identified a substantial victimization rate of 4.33%.

Crime Survey for England and Wales

Crime Survey for England and Wales (CSEW) is a systematic victim study conducted by the Office for National Statistics in the UK Government by using face-to-face interviews in which people are asked about their experiences of crime in the 12 months prior to the interview. The total sample size includes 35,000 households and approximately 50,000 people

Table 2. Victimization by Internet Auction Fraud

	Victims		Report to police	
Year	N	%	N	%
2008	29	.75	3	10.3
2012	6	.28	1	5.0

Note: Author's original table on RTI reports[7].

Table 3. Types of Damage Caused by Internet Use

Types of damage	Household (%)	Individual (%)*
Damage	65.3	30.17
Detection of malware but no infection	16.6	5.58
Infected by malware	4.4	1.47**
Reception of junk mail or fraudulent mail	60.3	20.25
Phishing	4.4	1.47**
Illegal access	2.7	.91**
Others (personal data breach, slander, etc.)	1.4	.48**
No damage	21.0	56.03
N/A	13.8	13.8

Notes: Author's original table on the Annual Communication Usage Trend Survey 2016. * Damaged rate per individual was calculated based on the tables in the Annual Communication Usage Trend Survey 2016; ** Indicates cases of substantial victimization.

aged 16 and over (as of March 2017). Until 2015, CSEW did not cover fraud such as online fraud, or the misuse of computers, including the detecting computer viruses, or unauthorized access to personal information[8]. Table 4 shows number of victimizations by online fraud and computer misuse.

ONLINE CYBERCRIME REPORTING SYSTEMS

Action Fraud[9]

Action Fraud (AF) is the national reporting center for fraud and cybercrime in the UK, which receives reports and information about crime on behalf of the police. AF also gives advice and guidance on fraud prevention measures, although it does not have investigative powers. However, the reports compiled by AF are sent to the National Fraud Intelligence Bureau (NFIB), which is run by the City of London Police and consists of the national lead force for fighting fraud. The NFIB collates and analyzes intelligence on fraud, identifies viable lines of inquiry, and develops a case, which is submitted to the police for investigation (Action Fraud 2017). AF received 264,056 reports between April 2016 and March 2017.

Internet Crime Complaint Center[10]

The Internet Crime Complaint Center (IC3) in the US is intended to provide the public with a reliable and convenient reporting mechanism for submitting information to the FBI concerning suspected Internet-facilitated criminal activity, and for developing effective alliances with industry partners. Information is analyzed and disseminated for investigative and intelligence purposes, as well as for law enforcement and public awareness (Internet Crime Complaint Center 2017). IC3 received on average

Table 4. Estimated Number of Victimizations by Online Fraud and Computer Misuse in the CSEW of 2016-2017[11]

Types of cybercrime	N	%
Bank and credit account fraud	1,244,500	2.7
Non-investment fraud	589,600	1.28
Computer viruses	1,138,150	2.47
Unauthorized access to personal information	603,000	1.31
Total	3,575,250	7.76

Note: Author's original table on CSEW.

over 280,000 complaints per year during 2012 to 2016.

Australian Cybercrime Online Reporting Network[12]

The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of the commonwealth, state, and territorial governments. It is a national online system that allows the public to securely report instances of cybercrime. ACORN also provides advice to help people recognize and avoid common types of cybercrime (Australian Cybercrime Online Reporting Network 2017). This organization received 46,975 reports in 2016.

RESULTS AND DISCUSSION

Verification of Victimization Rates

In order to verify the victimization rate indicated by the NU Survey, the author examined the nature of samples and compared the victimization rate between all types of cybercrime and specific types of cybercrime.

Firstly, because 13,000 participants were registered monitors of an Internet research company, it could be assumed that they are heavy Internet users. Indeed, the average online time of the participants was 191.6 minutes (3.19 hours) which looks longer than average Internet users' online time. Therefore, the author examined the relationship between the victimization rate and the length of online time using a scatter gram, which indicated that the number of online hours was correlated with the victimization rate as shown in Figure 4. Its approximation was y = .0185x + .0435.

MIC survey. The average online time of Internet users in Japan according to the MIC survey was 106.7 minutes (1.78 hours) in 2016. If we substitute this average time for "x", the victimization rate ("y") in Japan could be calculated as 6.74%. However, 6.74% was victimization rate among Internet users and the author converted this rate to the complete population base of 2016 by using the numerical formula below.

$$6.74\% \times 100{,}840{,}000^{*} \div 126{,}933{,}000^{**} = 5.36\%$$

* Number of Internet users in 2016

** The total population in 2016

Table 5 shows the converted table of victimization rate for the type of cybercrime.

Then, the author compared the above victimization rates with those of certain previous surveys: The MIC survey indicates that the substantial victimization rate of individuals is 4.33% (see Table 3) and the total percentage of corresponding types of Internet user based victimization rate is 4.89% (see Table 6). Therefore, the results of both surveys indicate identical findings regarding the substantial cybercrime victimization.

CVS. The raw data on victimization rate for Internet auction fraud in the CVS was .36% (see Table

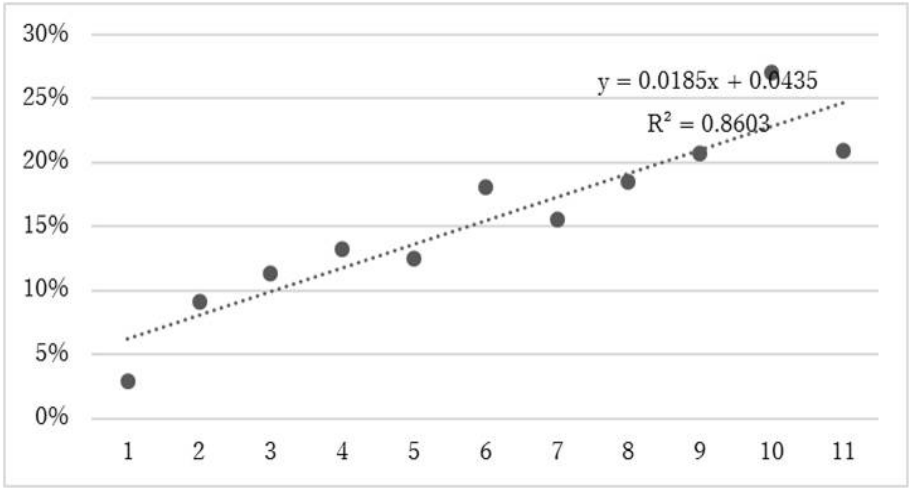

Figure 4. Victimization Rate and Online Time.

Table 5. Victimization Rate for the Type of Cybercrime

Types of cybercrime	Raw data (%)	Internet user base (%)	Population base (%)
Cash fraud	1.07	.66	.52
Property fraud	.28	.17	.14
Threatening or extortion	1.04	.64	.51
Slandering	.66	.41	.32
Bullying	.29	.18	.14
Stalking	.23	.14	.11
Identity fraud or theft	.39	.24	.19
Information theft or disclosure	.28	.18	.14
Illegal access	2.18	1.35	1.07
Copyright infringement	.09	.06	.05
Damaging the function of computers	3.98	2.46	1.95
Others	.42	.25	.2
Total victimization	10.92	6.74	5.36

Table 6. Victimization Rate of Common Types of Cybercrime Indicated by MIC and NU Surveys

MIC substantial victimization (Internet user based)	4.33%	Internet user based victimization	4.89%
Infected by malware	1.47%	Damaging the function of computers	2.46%
Phishing	1.47%	Identity fraud or theft Information theft	.24%
Illegal access	.91%	Illegal access	1.35%
Others (personal data breach, harassment, etc.)	.48%	Slandering	.41%
		Others	.25%

Table 7. Rate of Reporting a Crime in the Surveys

	Reported rate (%)	Notes
NU survey	6.7	
	18.4	Including consultations
CVS	8.16	Internet auction
CSEW	7.38	

Table 8. Reasons for not Reporting a Crime

Reasons	%
The loss is small	55.9
Reporting procedure is troublesome	21.2
Little possibility of an arrest	24.0
Reluctant to be involved with the police	7.6
Others	10.7
DK	10.8

1), and the converted victimization rate for Internet auction fraud based on the population would be:

.36% × 100,840,000* ÷ 126,933,000** = .29%, which is very close to the 2014 CVS result (.28%) shown in Table 6.

CSEW. In 2016-2017, the victimization rate for online fraud and computer misuse in the CSEW is 7.76% after excluding other cybercrimes such as slandering and breaches of intellectual property (see Table 4). The percentage of corresponding types of cybercrime victimization rate in the NU Survey is 4.01%, which is nearly half of the victimization rate of the CSEW. Nevertheless, considering differences in the general crime victimization rate between the UK and Japan, it could be appropriate that the rate in the UK is double of that of Japan[13] and it was concluded that the results of the NU Survey correspond with the results of CSEW.

Victim's Reports

Table 7 is a comparative table of victim report rates for cybercrime in the three surveys. It can be seen that all the rates are considerable lower than the rate for conventional crime. For example, the reported rate of burglaries is more than 50% in the 2012 CVS, and the average reported rate of crime in the UK is 40%[14]. Reasons for not reporting crime victimization to the police are shown in Table 8.

CONCLUSIONS

A cybercrime victimization rate of 5.36% in the NU Survey was obtained, which corresponded to that of certain previous surveys. The rate of 5.36% has considerably large impact compared with the rate for general crime victimization in the CVS 2014, which is 11.9%.

It is not difficult to conduct an online survey on cybercrime victimization as was done in this study. However, it is very difficult to lead a specific investigation and arrest of criminals by those surveys. Therefore, it is necessary to improve the reported rate of cybercrime to lead investigations and arrest of criminals. How can we encourage victims to report their losses?

The main reason for not reporting a crime is "the small loss (55.9%)". This reflects exactly what cybercriminals are expecting. IT technology enables good people, as well as criminals to make contact with the general public without any cost. For example, a

criminal can send fraudulent e-mails to millions of people and defraud considerable amounts of money, even though there is a low success rate. Moreover, only a small loss is incurred by each individual. Thus, many criminals commit these crimes with wide speared victimization and minimal damages. These criminals escape from the police because only a few victims report the crime to the police. Therefore, it is important to change the victims' mindset through education and by providing a simple and easy reporting system. It is obvious that an online reporting system would be suitable to encourage cybercrime victims to report crimes to the police, because cybercrime usually happens or is noticed when people are online.

The NU Survey inquired, "Would you have reported your loss to the police if an online reporting system were available?". Approximately, 36.7% of the respondents replied yes to this question. Moreover, 19.7% of the respondents replied that they would report a crime if an anonymous reporting system were available.

Certain countries have already introduced online cybercrime reporting systems, such as "AF" in the UK, "IC3" in the USA, and "ACORN" in Australia. In order to solve the problem of cybercrime, it would be necessary to establish a system for encouraging cybercrime victims to report their losses to the police, by following the examples of online cybercrime reporting systems in other countries.

Funding

The author's study was supported by the Nikkoso Research Foundation for Safe Society from April 2016 to October 2017.

Notes

1. Retrieved 20 October, 2017 (http://survey.govonline.go.jp/h27/h27-net/index.html).
2. Rakuten Research Co. Tokyo Japan.
3. Retrieved 20 October, 2017 (http://www.moj.go.jp/housouken/houso_houso34.html).
4. RTI report 41. Retrieved 20 October, 2017 (http://www.moj.go.jp/housouken/housouken03_00011.html).
5. RTI report 49. Retrieved 20 October, 2017 (http://www.moj.go.jp/housouken/ousouken03_00066.html).
6. Retrieved 20 October, 2017 (http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b1.html).
7. See notes 1 and 2.
8. Retrieved 20 October, 2017 (http://www.crimesurvey.co.uk/).
9. Retrieved (https://actionfraud.police.uk).
10. Retrieved 20 October, 2017 (https://www.ic3.gov/default.aspx).
11. Crime in England and Wales: Year ending Mar 2017. Retrieved 20 October, 2017 (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017).
12. Retrieved 20 October, 2017 (https://www.acorn.gov.au).
13. 20.1% in CSEW 2016-2017, 11.9% in CVS 2012.
14. Retrieved 20 October, 2017 (http://www.crimesurvey.co.uk/AboutTheSurvey.html).

References

Action Fraud. 2017. *What Is the Action Fraud Remit?* Retrieved 20 October, 2017 (https://actionfraud.police.uk/about-us-frequently-asked-questions).

Australian Cybercrime Online Reporting Network. 2017. *About the ACORN*. Retrieved 20 October, 2017 (https://www.acorn.gov.au/about-acorn).

Cabinet Office. 2003. *Hanzai Taisaku Kakuryou Kaigi (The Ministerial Meeting Against Crime)*. Retrieved 20 October, 2017 (http://www.kantei.go.jp/jp/singi/hanzai/).

Crime in England and Wales: Year Ending Mar 2017. Retrieved 20 October, 2017 (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017).

Internet Crime Complaint Center. 2017. *IC3 Mission Statement.* Retrieved 20 October, 2017 (https://www.ic3.gov/about/default.aspx).

Japanese Ministry of Justice. 2012. *White Paper on Crime 2012 Part5/Chapter3/Section1*. Retrieved 20 October, 2017 (http://hakusyo1.moj.go.jp/en/61/nfm/n_61_2_5_3_1_0.html).

Ministry of Internal Affairs and Communications. 2016. *2016 White Paper on Information and Communications in Japan*. Retrieved 20 October, 2017 (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/whitepaper.html).

National Police Agency (Japan). 2017a. *Annual Statistics of Crime*. Retrieved 20 October, 2017 (https://www.npa.go.jp/publications/statistics/sousa/year.html).

——. 2017b. *The White Paper on Police (Digest Edition 2016)*. Retrieved 20 October, 2017 (https://www.npa.go.jp/hakusyo/h28/english/WHITE_PAPER_ON_POLICE_2016/Contents_WHITE_PAPER_on_POLICE2016.htm).

——. 2017c. *Heisei 28 nen chu ni okeru cyber kukan wo meguru kyoi tou no jousei ni tsuite (Security Situation in Cyberspace in Japan 2016)*. Retrieved 20 October, 2017 (http://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf).

Bio

Taisuke Kanayama, LL.B., professor of Criminal Justice, College of Risk management, Nihon University, Japan; research fields: criminal justice, policing, crime displacement, cybercrime.