RISK　MANAGEMENT　STUDIES

危機管理学研究

創刊号

サイバー犯罪被害実態調査（第１回）の結果について

日本大学危機管理学部　教授　金山　泰介

2017 年 3 月
日本大学危機管理学部
危機管理学研究所

サイバー犯罪被害実態調査（第１回）の結果について

日本大学危機管理学部　教授　金山　泰介

Ⅰ　調査の背景とその概要

1　調査の背景

サイバー犯罪等サイバー空間における危険は年々高まっているといわれているところであるが、その実態は判然としないというのが現実である。すなわち、警察が公表した 2015 年のサイバー犯罪の検挙件数は 8,096 件だが、刑法犯の検挙件数（約 36 万件）と比べて 45 分の 1 程度でしかない。海外の調査では、世界の成人インターネットユーザーの 41％が 1 年以内に被害に遭ったとの結果[1]もあり、我が国のインターネットユーザー数は 1 億人強であることから、サイバー犯罪の被害率が 0.008％であるとは考えにくいのである。そこで、サイバー空間の安全安心を守るための施策を推進するためには、サイバー犯罪の発生状況を把握することが不可欠であることから本調査を実施したものである。

2　調査の概要

本調査は、日本大学危機管理学部サイバー犯罪等調査研究チームが、警察庁サイバーセキュリティ対策担当参事官室及び日本サイバー犯罪対策センターの協力の下、インターネット調査会社（楽天リサーチ）に委託して平成 28 年 6 月に実施した。

包括的なサイバー犯罪に関する被害実態調査としては、おそらく日本では初めてのものである。

Ⅱ　調査結果の概要

1　回答者の属性

(1) 性別、年齢、地域

対象は、全国の 16 歳以上のパソコン、タブレット、スマートフォンユーザー 1 万 3,000 人で、男女比、年齢別（10 歳代から 60 歳以上）の人口比に概ね対応するように抽出した。

性別では、男性 6,439 人、女性 6,561 人、年齢別では 10 代 771 人、 20 代 1,656 人、

30 代 2,072 人、40 代 2,362 人、50 代 1,984 人、60 代以上 4,155 人であった。地域別では、各都道府県から 258 人～ 322 人のサンプルを抽出した。

(2) 職業別

職業別では、表 1 のとおりで就業者の割合は 60.6%で平成 26 年の 15 歳以上人口に占める就業者の割合 59.6%とほぼ一致している。

表 1　回答者の職業別割合

職業等	%
会社員（派遣社員も含む）	30.9
公務員、教職員、団体職員	6.8
専門職（医師、弁護士、会計士等）	2.5
自営業	6.2
自由業、フリーランス	1.9
パート、アルバイト	12.2
学生	6.3
専業主婦・主夫	18.4
現在は働いていない。	14.8

(3) IT の習熟度別

IT の習熟度別では、約 3 割が他者の支援を受けていることが判明した。

表 2　IT の習熟度別割合

IT 習熟度	%
IT について高度な知識・技能を有している。	5.4
IT について生活に必要な高度な知識・技能を有している。	64.8
他者から援助を受けながら IT を利用している。	29.8

2　サイバー犯罪被害状況

(1) 概況

本調査の設問においては、サイバー犯罪被害の有無といったような抽象的な聞き方ではなく、具体的な被害の類型に当たるか否かの回答を求めた（表 1)。したがって、「だます」等の違法要素は回答者の主観に基づくものであるが、具体的な被害・損害を被った者を抽出できるよう設問を作成した。

平成 27 年中何らかのサイバー犯罪被害を受けたと回答した者は、全体の 9.6%でその内女性が占める割合は、42.4%と平成 27 年の刑法犯被害者に占める女性の割合 33.1%に比べて高いことが判明した。

年齢別では、10 歳代が最も高く 15.3%、以下 20 歳代（14.1%)、30 歳台（11.1%）と年齢が高くなるにつれて低下している。

各サイバー犯罪被害の類型ごとにみると、性別では、いずれの類型においても男性の被害率が高く、年齢別では、10 代が最も高く年齢が高くなるにつれて低下している。

また､パソコン等の利用時間別及び IT 習熟度別で全体の被害率をクロス集計したところ、利用時間別では利用時間が長くなるほど被害率が高まる傾向にあり、「1 日当たり 30 分未満」が 6.3%、「7 時間以上」で 12.3%と倍近い開きがあった。IT 習熟度別では、習熟度が

高まると被害率も高まる傾向にあり、「IT について高度な知識・技能を有している」者 19.1%、「他者から援助を受けながら IT を利用している」者 7.8%と倍以上の開きがあった。

なお、「利用していたサイトから自分の情報が流出」、「迷惑メール」及び「OS のアップデート絡みによる動作支障」については、当初選択肢には含まれていなかったが、自由記載欄への記入が多い項目であったことから項目立てしたものである。また、「その他」の自由記載の中で明らかに他の選択肢の範疇に当てはまる回答については、該当する選択肢に移した。

表 3　サイバー犯罪等被害の類型別割合（複数選択）

サイバー犯罪被害の類型	%
現金をだまし取られた。	1.2
ID やパスワードをだまし取られた。	1.1
現金以外のものをだまし取られた。	0.5
名誉棄損、誹謗中傷、いじめをされた。	0.7
脅迫または恐喝された。	0.7
コンピューターまたはスマートフォンの情報を流出させられた。	1.2
コンピューターまたはスマートフォンの動作に支障が生じた。	4.6
利用していたサイトから自分の情報が流出	0.3
迷惑メール	0.6
OS のアップデート絡みによる動作支障	0.1
その他	0.9
サイバー犯罪被害には遭わなかった。	90.4

「サイバー犯罪被害には遭わなかった」と回答した者に対し、「被害を受けそうな機会に遭遇したか」と尋ねたところ、一回遭遇した者が 4.7%、2 回以上遭遇した者が 3.9%で、合計 8.6%であった。その機会の内訳は、表 4 のとおり、電子メールによるものが多くを占めた。

表 4　サイバー犯罪被害を受けそうな機会（複数選択）

手口	%
身に覚えのない請求メールが来た。	42.6
フィッシングメールが来た。	38.3
サイトを閲覧していたら入会金等を請求する文言が表示された。	26.2
マルウェアを含む電子メールが来た。	19.1
その他	7.1

(2) 現金被害

① 被害の手口

それぞれの被害の類型ごとに、その具体的な手口について回答を求めた。表 5 は、「現金をだまし取られた」手口についてである。インターネットオークションが現金被害の手口としては最も多いことが見て取れる。なお、パーセンテージは被害類型それぞれの中で占める割合である。

表５　現金被害の手口別割合（複数選択）

手口	%
インターネットオークションで代金を支払ったが品物が、届かなかった。	39.7
インターネットオークション以外のインターネットショップで代金を支払ったが、品物が届かなかった。	35.1
身に覚えのない請求なのに支払ってしまった（架空請求）。	24.5
他人に自分の ID、パスワードを使われ、口座から現金が引き出された。	17.9
クレジットカードを不正使用された。	14.6
恋愛感情に付け込まれて、現金を渡してしまった（結婚詐欺等）。	15.9
その他	7.9

②　被害額

現金被害額は、数百万円以上とする回答もあったが、10 万円を超える被害を受けた者が 17.8%、10 万円以下が、82.2%で、被害額の中央値は約 1 万 1,500 円であった。

(2) ID、パスワードの被害

ID、パスワードの被害については、表 3 のとおりでフィッシングサイトによるものが半数以上を占めた。

表６　ID, パスワード被害の手口別割合（複数選択）

手口	%
ネット銀行サイトを模倣したフィッシングサイトに誘導された。	34.2
ネットショップ、ゲームサイトを模倣したフィッシングサイトに誘導された。	38.9
虚偽内容のメールにだまされ、送付した。	32.9
その他	28.9

(3) 現金以外の財産被害

現金以外の被害では、オンラインゲームで主に用いられるゲームのアイテムやポイントが盗まれるような被害が、半数以上を占めた。

表７　現金以外の被害手口別割合（複数選択）

手口	%
インターネットオークションで品物を送ったが、入金されなかった。	45.9
インターネットオークション以外のネット販売で品物を送ったが入金されなかった。	42.6
ゲームのアイテムやポイントを失った。	50.8
恋愛感情に付け込まれて指輪等を渡してしまった。	27.8
その他	11.5

(4) 名誉棄損、誹謗中傷等被害

被害の約 4 分の 3 が掲示板、SNS、ラインへの投稿であった。また、リベンジポルノ型の被害も少なからず発生している。

表８　名誉棄損、誹謗中傷等被害の手口別割合（複数選択）

手口	%
侮辱的な文言等を掲示板、SNS、ラインに書き込まれた。	74.7
侮辱的な文言等を自分のブログ、ツイッター等に書き込まれた。	42.2
人には見られたくない画像を公開された。	16.7
その他	5.6

(5) 脅迫、恐喝被害

脅迫、恐喝においては、電子メールとそれ以外の SNS 等がほぼ同じ割合で用いられており、比較的新しい手口のランサムウェアによる被害も他の手口と同程度の発生している。「その他」では強迫的文言による架空請求が約 7 割を占めている。

表 9　脅迫、恐喝の手口別割合（複数選択）

手口	%
恋愛感情のもつれから電子メールにより脅かされた。	22.2
恋愛感情のもつれから電子メール以外の SNS 等により脅かされた。	22.2
恋愛感情以外の友人関係、取引関係等のもつれから電子メールにより脅かされた。	25.6
恋愛感情以外の友人関係、取引関係等のもつれから電子メール以外の SNS 等により脅かされた。	24.4
マルウェアに感染させられたコンピュータ等の復旧の代償に金銭を要求された。（ランサムウェア）	22.2
その他	25.6

(5) データ流出被害

「その他」に含まれていた「利用していたサイトからの自分の情報の流出」に該当する回答件数は、独立項目に移した。

表 10　データ流出被害の手口別割合（複数選択）

手口	%
電子メールを介してマルウェアを感染させられた。	51.3
ファイル共有ソフトを悪用するマルウェアを感染させられた。	28.7
ハッキングによってコンピュータに侵入された。	32.0
その他	18.7

(6) 機器の不具合被害

ホームページ閲覧による感染の手口が最も多く、電子メールを介しての感染の 2 倍以上であった。

表 11　機器の不具合被害手口別割合 (複数選択)

手口	%
ソフトウェアやアプリのダウンロードを介してマルウェアに感染させられた。	26.2
インターネットのホームページの閲覧によりマルウェアに感染させられた。	43.1
電子メールを介してマルウェアに感染させられた。	18.8
USB メモリ、DVD ロム等外部記録媒体によりマルウェアに感染させられた。	7.6
DoS 攻撃によりサーバーがダウンした。	6.9
その他	20.9

(7) その他

「その他」は、自由記載で回答を求めたが、回答者を被害者とするサイバー犯罪とは言い難い「迷惑メール」、「利用したサイト等からの自分の情報の流出」及び「OS のアップデート絡みの支障」に該当する回答が多く含まれていた。

2　被害通報の状況

(1) 通報の状況

警察へ届け出た割合は 10.4%、警察以外の機関へ通報した割合は 30.7%で、その警察以

外の機関では、クレジットカード会社が筆頭であった。

表 12　警察以外の通報先（複数選択）

通報先	%
クレジットカード会社	35.0
金融機関	21.9
ネットショップ運営会社	32.1
コンピュータセキュリティ会社	18.5
消費生活センター等公的機関	16.7
その他	12.3

(2) 警察に届け出た又は届け出なかった理由

①　被害を受けて警察に届け出た理由の筆頭は、「被害を少しでも取りもどすため(53.8%)」であったが、「再発を防ぐため」（44.6%）と公益的な理由の回答も多かった。被害を受けなかったと回答した者に対しても、「被害を受けたとすれば警察に届けたか」との質問を行った結果は、被害を受けた者とほぼ同様の傾向であった。

表 13　警察に届け出た（届け出る）理由 (複数選択)

理由	被害有り	被害無し
被害を少しでも取り戻すため。	53.8	55.1
犯罪は警察に届けるべきだから。	51.5	47.7
犯人を捕まえてほしいから。	46.9	48.7
再発を防ぐため（被害が広がらないように)。	44.5	58.8
その他	2.3	0.3
分からない。	2.3	1.3

②　被害を受けて警察に届け出なかった理由の筆頭は、「大した被害ではなかったから(53.4%)」であったが、被害を受けなかった者には、この設問はなかったため、「手続きが面倒で時間がかかりそうだから」が筆頭であった。

表 14　警察に届け出なかった（届け出ない）理由

理由	被害有り	被害無し
大した被害ではなかったから。	53.4	設問無し
手続きが面倒で時間もかかりそうだったから。	24.2	56.5
届け出ても検挙できそうにないから。	22.4	53.5
警察とは関わりたくないから。	7.5	13.1
その他	12.4	3.7
分からない。	11.6	6.9

③　サイバー犯罪被害について「ネット上だけで届け出られるシステムがあったら利用したか」との設問に対しては、被害の有無にかかわらず半数以上のものが利用又は匿名なら利用したと思うと回答した。

表 15　サイバー犯罪被害をネット上だけで届けられるシステムについての利用意思

利用意思の有無	被害有り	被害無し
利用すると思う。	39.9	46.9
匿名なら利用すると思う。	25.3	24.1
利用しないと思う。	10.9	6.2
分からない。	23.9	22.7

3　被害時の対処と被害後の変化

(1) 被害時の対処法

被害を受けた際の対処方法等をどのように調べたかを聞いたところ、コンピュータセキュリティ会社のウェブサイト閲覧が筆頭であったが、警察等公的機関のウェブサイトの利用率は低かった。

表 16　被害時の対処方法等の調査先

調査先	%
警察等公的機関のウェブサイト	9.6
コンピュータセキュリティ会社のウェブサイト	22.2
銀行やネットショップのウェブサイト	8.6
質問サイト	22.1
上記以外のウェブサイト	17.9
知人に尋ねた。	15.5
その他	3.8
調べなかった。	33.1

(2) 被害後の変化

被害を受けた後表のとおり様々な対策等を被害者は実施しているが、変わらないと回答した者が約 4 割に上っている。

表 17　被害後の行動や心境の変化の有無

行動や心境の変化	%
セキュリティ製品やサービスの導入	20.4
インターネットオークションの利用の停止	8.8
インターネットオークションの出品者情報の精査	10.6
ネットショッピングの支払い手段をクレジットカードにした。	6.3
クレジットカード利用明細のチェックの励行	20.1
サイバー犯罪の手口や対策等の情報の入手	15.2
その他	5.3
変わらなかった。	39.9

Ⅲ　先行調査研究

1　法務省第 4 回犯罪被害者実態（暗数）調査[2]

(1) 調査方法等

法務省が 4 年ごとに行っている総合的な犯罪被害実態調査の中で、平成 24 年の調査においてインターネットオークション詐欺について調査を行った。郵送による質問票調査で、対象者数 4,000 人中，回答が得られた者は 2,156 人（回答率 53.9%）であった。

(2) 調査結果

① 「過去 5 年間にインターネットオークション詐欺に遭ったか」との問いに対し、2,156 人中 20 人が「被害に遭った」と回答した（0.9%）。

② 「捜査機関に届け出たか」との問いに対しては、1 人が「届け出た」と回答した（5%）。届け出なかった理由で最も多かったのは、「損失がない、大したことではない」（6 人）であった。

2　総務省通信利用動向調査[3]

(1) 調査方法等

総務省では、毎年行っている通信利用動向調査の質問項目に平成14年から「インターネットの利用の際受けた被害」を盛り込んでいる。

平成27年調査は、平成28年１～２月の間に全国の20歳以上の世帯主がいる世帯40,592を対象に質問票を郵送する形で行われ、郵送及びオンライン（メール）によって14,765世帯から回答を得た。

(2) 調査結果

過去１年間に自宅パソコン、携帯電話PHSを含む、スマートフォン及びその他の機器でインターネットを利用したことのある世帯11,526を対象に、過去１年間にインターネットを利用する際に被害を受けたか否か利用手段毎の複数回答を求めた。

結果は表18のとおりであるが、設問にあるとおり、迷惑メール等の受信自体を被害ととらえていること及び世帯を調査対象としていることから被害率が高くなっている。

表18　インターネット利用の際に受けた被害

被害の態様等	%
コンピュータウィルスを発見したが、感染はしなかった。	15.8
コンピュータウィルスを発見し、少なくとも１度は感染した。	6.6
迷惑メール・架空請求メールを受信した。	67.1
フィッシング	3.5
不正アクセス	1.9
その他（個人情報の漏洩、誹謗中傷）	1.4
特に被害はない。	26.2
不詳	9.7

3　英国ケント大学第２回サイバーセキュリティ調査[4]

(1) 調査の概要

ケント大学セイバーセキュリティ総合研究所（Kent University’s Interdisciplinary Research Centre for Cyber Security）が、インターネット調査会社（Google　Consumer Survey）に委託し、2014年２月に実施し、英国全土の1,502人から回答を得た。

調査の対象は、過去12か月間にサイバー犯罪とサイバーセキュリティにかかわった経験の有無を調査した。

(2) 主な調査結果

本稿に関連性のある調査結果としては次のようなものである。

①　過去１年間に26％がCyber Dependent Crime（不正アクセス禁止法違反及びコンピュータ・電磁的記録対象犯罪等）の被害を受けた。

②　過去１年間に9.3%がCyber Enabled Crime(ネットワーク利用犯罪)の被害を受けた。

③　金額的被害を受けた者は、1,000ポンド以上が28.8%、1000ポンド未満が71.2%であった。

④　被害者で捜査機関への申告した者は、警察等捜査機関3.5%、Action Fraud[5]2.7%（重複あり）と低いものであった。通報しなかった理由の首位は、「自分で解決した（10.3%）

であったが、次が「時間の無駄（7.6%）」であった。

Ⅳ　検討

1　サイバー犯罪被害の実態は明らかになったのか。

サイバー犯罪の被害者のほとんどは、インターネットユーザーであることから、インターネット経由で調査を行うことは合理的かつ有効であると考えられる。ただし、本調査で対象としたインターネットユーザーは、インターネット調査会社のモニターに登録しているものであることから、ネット利用頻度は全国平均よりも高くなっている。

調査結果では、1 日のインターネット利用時間の平均は、最小で 143 分、最大で 240 分であった。ちなみに、平成 27 年総務省調査によれば、1 日平均のネット利用時間は平日で 90.7 分、休日で 113.7 分であることから、本調査対象は、全国平均よりも 1.5 ～ 2.2 倍程度長くインターネットを利用していることになる。

ネット利用時間別の被害率は、利用時間の長さと正の相関にあることから、全国平均の利用時間を調査結果に当てはめると、全国のインターネットユーザ―の平均被害率は 8.5% 以上と推計できる。

総務省によると平成 27 年のインターネットユーザーの推計は 1 億 46 万人であることから、概算すると約 850 万人が何らかの被害を受けたと推計される。

さらに、警察への申告率 10.4%をサイバー犯罪発生件数の推計に当てはめると 85 万件以上申告が行われていることになるが、警察の検挙件数、相談受理件数を合わせても 13 万件余であることから [6]、矛盾が生じている。その理由としては、犯罪についての警察への届け出が社会的に望ましい行動であることから、その回答にバイアスが生じているのか、被害推計が大きすぎるのか、あるいはその両方なのか不明である。

被害率は、英国ケント大学調査の半分以下であったが、インターネットオークション詐欺被害では、0.67%（1 年間）と法務省調査 0.9%（5 年間）を大きく上回っている。ただ、法務省調査では対象がインターネットユーザーだけではないので、平成 23 年当時のインターネットの利用率（79.1%）及び利用頻度（毎日 1 回以上 59.1%）を勘案してもその差は大きなものである。

本調査の精度については第 2 回調査との比較等により引き続き分析する必要がある

2　捜査機関への通報率の低さについて

先行調査と今次調査で共通するのは、警察等捜査機関への通報率の低さである。今次調査では、10.4%と法務省調査（5%）や英国ケント大学調査（6.2%）よりも高い結果が出ているが、法務省の犯罪被害実態調査にある自転車盗（42.7%）や不法侵入（47.9%）の申告率に比べて大幅に低く、申告率が低い性的事件（18.5%）をも下回っているのである [7]。

届けなかった理由の過半数は、「大した被害ではなかったから（53.4%）」であった。ち

なみに、法務省の調査で自転車盗を届けなかった理由の筆頭も「それほど重大ではない（30.3%）」であったがその割合をみると、サイバー犯罪被害は自転車盗被害よりも軽く扱われているのである。

しかしながら、「被害をネット上だけで届けられるシステムがあったら、利用したか」との問に対しては、「利用すると思う。（46.9%）」、「多分利用すると思う。（24.1%）」約 3 分の 2 の被害者が回答していることから、サイバー犯罪被害の実態をより明らかにするためには、英国で実施されている類似のシステム[8]等を参考に、簡便な被害申告システムを構築する必要があると考える。

おわりに

本調査研究結果は、日工組社会安全研究財団社会安全に関する研究助成を受けた「サイバー犯罪実態及びサイバー犯罪被害通報・診断システムの可能性に関する調査研究」の一部である。また、クロス集計については、日本大学危機管理学部専任講師宮脇健が担当した。

---

[1] Norton Report p11, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013（平成 28 年 9 月 25 日参照）

[2] 法務総合研究所研究部報告 49　80-81 頁　http://www.moj.go.jp/housouken/housouken03_00066.html（平成 28 年 9 月 25 日参照）

[3] 総務省　平成 27 年通信利用動向調査　http://www.e-stat.go.jp/SG1/estat/List.do?bid=000001074098&cycode=0（平成 28 年 9 月 25 日参照）

[4] http://www.cybersecurity.kent.ac.uk/Survey2.pdf（平成 28 年 9 月 25 日参照）

[5] 英国の詐欺とサイバー犯罪にかかるオンラインでの被害通報システム http://www.actionfraud.police.uk/（平成 28 年 9 月 25 日参照）

[6] 平成 27 年におけるサイバー空間をめぐる脅威の情勢　9-11 頁 http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf（平成 28 年 9 月 25 日参照）

[7] 法務総合研究所研究部報告 49　14 頁　http://www.moj.go.jp/housouken/housouken03_00066.html（平成 28 年 9 月 25 日参照）

[8] Action Fraud 英国の詐欺とサイバー犯罪にかかるオンラインでの被害通報システム http://www.actionfraud.police.uk/（平成 28 年 9 月 25 日参照）