2016 年度一般研究助成　研究報告書

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

研究代表者
日本大学危機管理学部　教授　金山泰介

共同研究者
日本大学危機管理学部　教授　美濃輪正行
日本大学スポーツ科学部　准教授　谷口郁生
日本大学危機管理学部　専任講師　宮脇健

まえがき

日本の刑法犯認知件数は、平成 14 年の 285 万件余をピークに毎年減少し、平成 28 年は 100 万件を下回るに至った。その一方で、サイバー犯罪（高度情報通信ネットワークを利用した犯罪やコンピューター又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪[1]）は平成 14 年の検挙件数 1,600 件余であったのが、平成 28 年には 8,000 件を上回っている。ただ、これは検挙件数であるので、そのまま刑法犯認知件数と比較するわけにはいかない。そこで、サイバー犯罪の認知件数を推定してみると、刑法犯では検挙件数は概ね認知件数の三分の一であることから、3 倍すると約 25,000 件となるが、これが果たしてサイバー犯罪の実態を反映していると言えるか疑問である。すなわち、サイバー犯罪について警察が受理した相談件数が平成 28 年は 13 万件を上回っているからである。

別の統計からは、さらに大きな被害が生じていることがうかがわれる。総務省が行っている通信利用動向調査[2]によれば、平成 28 年中にインターネット利用中に何らかの被害を受けた世帯は、65.3%に上っているのである。全国の世帯数にインターネットの普及率及び被害率を掛けると全国の約 2,740 万世帯がインターネット利用時に何らかの被害を受けていることなる。ただし、この調査の内容をみると、その内容をみると、「ウィルス発見したが感染なし」や「迷惑メール・架空請求メールを受信」が含まれていることから、これもサイバー犯罪の実態を反映していると言うには疑問が残る。

犯罪対策を的確に講じていくためには、通常は被害の実態を踏まえることが重要なのであるが、サイバー犯罪にあっては、上記のとおりその実態が十分把握されているとは言い難いので

ある。そこで、サイバー犯罪の実態を把握する方法として本調査研究を着想したところである。

第１　調査研究の目的

サイバー犯罪は、サイバー空間特有の匿名性や技術的な脆弱性を巧み利用し、かつ、不特定多数のインターネット利用者に対して極めて短い時間で敢行されているが、こうした特徴から、被害実態は必ずしも明らかにはなっていない。警察統計[3]では、サイバー犯罪の件数は、刑法犯のような認知件数ではなく、検挙件数で計上されていることから、刑法犯よりもその暗数は相当大きいものと推測される。その推移をみると、平成 16 年に初めて 2,000 件を超えてから急増し、平成 28 年まで 8,000 件前後で推移しているところである。その一方、刑法犯認知件数は平成 14 年をピークに平成 28 年まで 14 年連続減少していることから、刑法犯からサイバー犯罪への転移が生じている可能性が推認されるところであるが、把握されている件数が三桁以上異なっていることから、この統計のみでは具体的な検証は困難である。

こうした状況の下、サイバー犯罪対策を的確に講じていくためには、サイバー犯罪発生の実態を可能な限り明らかにするとともに、継続的にサイバー犯罪被害発生の把握を可能するようなシステムを構築することが必要と思料される。

本調査研究は、サイバー犯罪のほとんどがコンピューター、スマートフォン利用者を対象としていることから、インターネットを通じたサイバー犯罪被害実態調査を行うことにより、サイバー犯罪被害の全体像を浮かび上がらせるとともに、簡便なサイバー犯罪被害通報システム構築の可能性を探ることを目的とするものである。

第２　調査研究の方法

１　サイバー犯罪被害実態調査

インターネット経由のアンケート調査を平成 28 年 6 月及び 29 年 2 月に実施した。抽出方法は、有意抽出法でエリアサンプリング及び年齢、性別のサンプリングを行い、日本全国の男女比・年齢構成比に近いサンプルを得る試みを行った。調査実施機関は株式会社楽天リサーチで、サンプル数は、13,000 人である。

設問は、全 25 問でサイバー犯罪被害の内容に加え、警察等への被害届出・通報の有無、届出・通報しなかった理由等選択肢方式を用いて回答を求めた。

また、比較分析のため、法務省の犯罪被害実態（暗数）調査[4]、総務省の通信利用動向調査[5]、英国の犯罪被害実態調査（Crime Survey for England and Wales: CSEW）[6]及び英国のケント大学が行ったサイバーセキュリティ調査[7]について文献調査を行った。

２　サイバー犯罪被害通報システムに関する調査

英国が導入している Action Fraud を中心に、米国の Internet Crime Complaint Center(IC3)[8]及びオーストラリアの Australian Cybercrime Online Reporting Network(ACORN)[9]について文献調査を行った。

第3　結果

我が国におけるサイバー犯罪による被害実態調査については、法務省及び総務省が一部の罪種について行ったものがあるが（後述）、今回の調査はサイバー犯罪被害を包括的に対象とするもので、我が国ではおそらく初めてのものであった。

1　サイバー犯罪被害実態調査結果

(1) 回答者の属性

ア　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13,000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。この性別、年齢別の数字は、比較可能なように第1回及び第2回ともに同数となっている。

イ　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。職業別の割合は、第1回調査と第2回調査の間に大きな開きはない。

表1　回答者の職業別人数・割合

職業等	第1回		第2回	
	人数	割合(%)	人数	割合(%)
会社員（派遣社員も含む）	4,021	30.9	4,016	30.9
公務員、教職員、団体職員	878	6.8	942	7.2
専門職（医師、弁護士、会計士等）	320	2.5	368	2.8
自営業	809	6.2	844	6.5
自由業、フリーランス	249	1.9	264	2.0
パート、アルバイト	1,585	12.2	1,530	11.8
学生	813	6.3	905	7.0
専業主婦・主夫	2,397	18.4	2,325	17.9
現在は働いていない。	1,928	14.8	1,806	13.9

ウ　IT習熟度

IT習熟度については、表2のとおり第1回調査では3つのレベル、第2回調査では4つのレベルに分けて調査した。いずれも、習熟度と被害率はプラスの因果関係を示した（「第4考察1サイバー犯罪被害率の精度」参照）。

表 2　回答者の IT 習熟度別人数・割合

	第 1 回		第 2 回	
	人数	割合(%)	人数	割合(%)
IT について高度な知識・技能を有している	703	5.4	427	3.3
IT を業務で利用するに足りる知識・技能を有している	＊	＊	2,348	18.1
IT を生活で利用するに足りる知識・技能を有している	8,429	64.8	7,301	56.2
他者から援助を受けながら IT を利用している	3,868	29.8	2,924	22.5

エ　インターネット利用時間

サンプルの平均インターネット利用時間（オンライン時間）は、191.6 分であった。1 時間ごとに区切ったオンライン時間別の回答者の数は、表 3 のとおりである。

表 3　回答者のオンライン時間別人数・割合

オンライン時間	人数	割合(%)
0-1h	658	5.1
1-2h	2,929	22.5
2-3h	3,024	23.3
3-4h	2,710	20.8
4-5h	1,002	7.7
5-6h	1,241	9.5
6-7h	496	3.8
7-8h	130	1.0
8-9h	304	2.3
9-10h	48	0.4
10h-	455	3.5

(2) サイバー犯罪被害状況

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 4)。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・損害を受けた者を抽出できるよう設問を作成した。

第 1 回調査では、複数回答可としたが、第 2 回調査では複数回被害を受けた者については、被害が大きいと思われる方のみを回答するよう求めた。

ア　被害の類型

第1回調査では、8類型で設問を構成していたが、その他欄での自由記載で多かったものを抽出し、調査結果の表には「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」の3項目を追加した。第2回調査では、これ等の項目に「いじめ」、「ストーカー」、「不正アクセス」及び「知的財産権侵害」を加え、15類型とした。「迷惑メール」、及び「OSのアップデート絡みによる動作支障」は実質的な犯罪被害とは言えないが、第1回調査の自由記載で回答の多かった項目について、除外の便のため、あえて設問に盛り込んだところである。表における「＊」は、第1回調査では項目として設けなかった設問について記しているものである。

イ　被害率

回答者が、サイバー犯罪被害に遭っていないと答えた割合は、第1回調査が90.40％、第2回調査が87.52％で、総被害率は、第1回調査9.60％、第2回調査12.48％あった。その類型別の被害率の一覧が、表4である。ただし、上記実質的な被害と言えない項目及び各項目の自由記載欄から明らかに実質的な被害ではないとみられるものがそれぞれ1ポイント程度存在するので実際の被害率はその分低くなるとみられる。

表4　サイバー犯罪被害の類型別被害率

被害類型	割合(%)	
	第1回	第2回
現金、電子マネー等をだまし取られた	1.20	1.07
現金等以外のものをだまし取られた	0.50	0.28
脅迫又は恐喝された	0.70	1.07
名誉棄損、誹謗中傷された	0.70	0.66
いじめをされた		0.29
ストーカーをされた	＊	0.15
IDやパスワードをだまし取られた	1.10	0.39
コンピューター又はスマートフォンの情報を流出させられた	1.20	0.28
メールやSNSのアカウントに不正アクセスされた	＊	2.31
知的財産権を侵害された	＊	0.09
コンピューター又はスマートフォンの動作に支障が生じた	4.60	4.10
利用していたサイトから自分の情報が流出した	0.30	0.17
迷惑メール	0.60	0.96
OSのアップデート絡みによる動作支障	0.10	0.13
その他	0.90	0.28
サイバー犯罪被害には遭わなかった	90.40	87.52

詳細な分析結果については、「第4考察1サイバー犯罪被害率の精度」で述べる。また、第1回調査では複数回答可能としたことから、その類型別のパーセンテージの合計は100とならない。

第2回の調査結果で大きく変動した類型は、ID、パスワードの窃取（1.1%→0.39%）及び情報流出（1.2%→0.28%）であるが、これは、アカウントの乗っ取りなど不正アクセスの項目を立てたことによるものとみられる。

ウ　各被害類型の手口

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。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が、第1回調査では複数回答であった。

（ア）現金等被害の手口

現金、仮想通貨等被害に係るサイバー犯罪の手口は、表5のとおりであるが、第1回、第2回両調査ともに「ネットオークション」による被害が最も多い。

表5　現金等被害の手口

被害手口	第1回(%)	第2回(%)
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	28.8
ネットオークション以外の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	21.6
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	6.5
アダルトサイト等を閲覧していたら、突然入会申込みを受け付けたなどの表示が現れ、会費等を支払ってしまった（ワンクリック詐欺）		3.6
他人に自分のID、パスワードを使われ、ネットバンク口座から現金を引き出された	17.9	0.0
他人に自分のID、パスワードを使われ、品物や電子マネーの購入に使われた	＊	8.6
クレジットカードを不正に使用された	14.6	10.8
懸賞金に当選したとのメールが来て、手数料等を支払ってしまった（懸賞金詐欺）	＊	3.6
SNS、出会い系サイト等で知り合った相手に恋愛感情に付け込まれて、現金等を渡してしまった（結婚・デート詐欺）	16.0	5.8
その他	7.9	10.8

（イ）　物品等詐欺の手口

現金、仮想通貨等以外の物品被害に係る詐欺の手口は、表6のとおりである。第1回調査では、ネットオークション、ネットオークション以外のネットショップ及びオンラインゲームでの被害が拮抗していたが、第2回調査では、「ネットオークション以外のネットショップでの被害」が筆頭であった。

表6　物品等詐欺の手口

被害手口	第1回(%)	第2回(%)
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	26.4	19.4
ネットオークション以外のネットショップで品物を送ったが入金されなかった	24.6	33.3
他人に自分のID、パスワードを使われ、ゲームのアイテムやポイントを失った	26.4	27.8
SNS、出会いサイト等で知り合った相手に恋愛感情に付け込まれて、指輪等を渡してしまった（結婚・デート詐欺）	16.0	13.9
その他	6.6	5.6

（ウ）脅迫等の手口

脅迫等の手口は表7のとおりである。第2回調査では「ランサムウェア」が増加し、「恋愛感情のもつれからの脅迫」が減少している。前者については、それまで「ランサムウェア」の感染を媒介するマルウェアスパムの多くは英文であったが、平成28年から和文のものが現れるなど脅威が大きく高まった結果であるとみられる。後者については、第2回調査から「ストーカー」の項目を新設したため、「恋愛感情のもつれからの脅迫」の項目への回答が減少したことによると考えられる。

表7　脅迫等の手口

被害手口	第1回(%)	第2回(%)
恋愛感情のもつれから脅かされた	31.5	4.4
恋愛感情以外の友人関係、取引関係等のもつれから脅かされた	35.4	13.9
ランサムウェアに感染させられたコンピューター等の復旧の代償に金銭を要求された	15.0	35.8
人に知られたくない写真や個人情報を公開すると脅され、金銭を要求された	＊	13.1
その他	35.4	32.8

（エ）誹謗中傷等の手口

インターネット上で行われる「誹謗中傷等」の手口は、表8のとおりであるが、第1回、第2回調査ともに、SNSでの被害が半数（以上）を占めている。第2回調査では、「いじめ」と「ストーカー」については別項目とした。

表8　誹謗中傷等の手口

被害手口	第1回(%)	第2回(%)
侮辱的な文言等を掲示板やSNS、ラインに書き込まれた	54.4	50.0
侮辱的な文言等を自分のブログ、ツイッターに書き込まれた	30.4	15.1
自分の名前を騙られて、書き込みやメール送信をされた	＊	7.0
人には知られたくない情報をネット上で公開された	12.4	16.3
人には見られたくない画像をネット上で公開された		7.0
その他	3.2	4.7

（オ）いじめの手口

いわゆるネットいじめの手口が表9である。第1回調査では誹謗中傷等に含められていたが、第2回調査では項目立てしたもので、「SNSでの書き込み」が筆頭手口であるが、次が「LINEはずし(LINEのグループから強制的に除外する又は該当者以外のもので新しいグループを作ること)」等のいわゆるネット上の仲間外れであった。

表9　いじめの手口

被害手口	第1回(%)	第2回(%)
侮辱的な文言等を掲示板やSNS、ラインに書き込まれた	＊	39.5
侮辱的な文言等を自分のブログ、ツイッターに書き込まれた	＊	10.5
自分の名前を騙られて、書き込みやメール送信をされた	＊	7.9
人には知られたくない情報をネット上で公開された	＊	5.3
人には見られたくない画像をネット上で公開された	＊	15.8
LINEはずし等仲間はずれにされた	＊	18.4
その他	＊	2.6

（カ）ストーカーの手口

いわゆるサイバーストーキングの手口が、表10である。これもいじめと同様、第2回調査で項目立てしたものであるが、直接のEメール送付が筆頭手口で、半数近くを占めている。

表 10　ストーカーの手口

被害手口	第 1 回(%)	第 2 回(%)
交際の再開を求める等のメールを何度も送り付けられた	＊	46.7
自分に関わる文言等を掲示板や SNS、ラインに書き込まれた	＊	23.3
自分に関わる文言等を自分のブログ、ツイッター等に書き込まれた	＊	16.7
自分の名前を騙られて、書き込みやメール送信をされた	＊	6.7
その他	＊	6.7

（キ）ID 窃盗の手口

サイトへのログオンアカウントの ID やパスワード等の窃取の手口が表 11 である。具体的な手口が分かっている被害においては、「フィッシング」が筆頭であるが、第 2 回調査では、「原因不明」が 6 割以上を占めており、被害者が気付かないままに窃取されている深刻な状況にあることが判明した。

表 11　ID 等窃盗の手口

被害手口	第 1 回(%)	第 2 回(%)
ネット銀行の HP そっくりのフィッシングサイトに誘導された	24.4	9.8
ネットショップやゲームのホーム頁そっくりのフィッシングサイトに誘導された	27.8	11.8
虚偽内容の電子メールにだまされて送ってしまった	28.2	9.8
原因は不明	24.4	62.7
その他		5.9

（ク）情報流出の手口

情報流出の被害手口は、表 12 のとおりであるが、「不正アクセス」を別項目としたことから、全体としては大きく減少している。

表 12　情報流出の手口

被害手口	第 1 回(%)	第 2 回(%)
電子メールを介してマルウェアに感染させられた	34.8	21.6
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	19.5	24.3
ハッキングによってコンピューターに侵入された	21.7	18.9
その他	24.0	35.1

（ケ）不正アクセスの手口

第 2 回調査から、別項目としたメール、SNS、オンラインゲーム等のアカウントへの不正アクセスの手口が、表 13 である。

表 13　不正アクセス手口

	第 1 回(%)	第 2 回(%)
自分に成りすまして書き込み等をされた	＊	34.3
自分に成りすましてゲームを利用された	＊	6.7
パスワード等を変更され利用できなくなり、アカウントを乗っ取られた	＊	26.7
その他	＊	32.3

（コ）知的財産権侵害の手口

第 2 回調査から著作権や商標権侵害被害を別項目としたが、その手口の内訳が表 14 である。手口の筆頭は、「投稿サイト等への無断アップロード」であった。

表 14　知的財産権侵害の手口

被害手口	第 1 回(%)	第 2 回(%)
著作権を保有する書籍、楽曲、映像が無断でネットオークションに出品された	＊	0.0
著作権を保有する書籍、楽曲、映像が無断でネットショップで販売された	＊	16.7
著作権を保有する書籍、楽曲、映像が無断で投稿サイト等にアップロードされた	＊	41.7
商標又は類似した商標を無断でネット上で使用された	＊	8.3
模倣品がネットオークションに出品された	＊	8.3
模倣品がネットショップで販売された	＊	8.3
その他	＊	16.7

（サ）マルウェア感染の手口

マルウェアに感染した経路についての手口別内訳が表 15 であるが、「サイトの閲覧による感染」が、第 1 回、第 2 回調査ともに筆頭であった。

表 15　マルウェア感染の手口

被害手口	第 1 回(%)	第 2 回(%)
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	21.0	20.6
サイトの閲覧によりマルウェアに感染させられた	34.6	38.6
電子メールを介してマルウェアに感染させられた	15.0	10.9
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	6.1	5.4
DoS 攻撃によりサーバーがダウンした	5.5	6.6
その他	17.8	17.8

（シ）その他の手口

第 1 回調査では自由記載であったが、第 2 回調査では、第 1 回調査で多かった項目をその他の小項目としたものが、表 16 である。「利用サイトからの情報流出」のほかは実質的な被害とは言えないが、除外の便のため、あえて項目としたものである。

表 16　その他の被害の手口

被害手口	第 1 回(%)	第 2 回(%)
利用していたサイトから自分の個人情報等が流出した	＊	9.8
迷惑メールを受信した	＊	55.8
アンチウィルスソフトがウィルスを検知した	＊	10.7
意に沿わずに OS やアプリがアップグレードした	＊	7.6
その他	＊	16.1

エ　被害内容

（ア）被害の形態

金銭的被害における形態は、表 17 のとおりであるが、第 2 回調査では、現金等、物品双方とも減少している。

表 17　被害の形態

被害の形態	第 1 回(%)	第 2 回(%)
現金	25.6	10.4
電子マネー、ビットコイン等：		3.3
物品	10.0	1.3
分からない	71.9	15.6
現金、物品等の被害はなかった		69.4

表 18 のとおり現金の被害者のうち約 18～19%が、10 万円以上の被害を訴えているが、その中央値は 1 万円台前半で、比較的少額な被害も多い。

表 18　現金被害額

	最高被害額	中央値	被害額 10 万円以上
第 1 回	5,000 万円	11,500 円	17.80%
第 2 回	500 万円	15,000 円	19.50%

（イ）被害時の使用機器

被害者が、被害を受けたときに使用していた機器は、表 19 のとおりであるが、第 2 回調査ではスマートフォンが増加している。

表 19　被害時の使用機器

使用機器	第 1 回(%)	第 2 回(%)
私有のコンピューター・タブレット	63.6	54.4
法人等が所有するコンピューター・タブレット	10.0	4.7
私有のスマートフォン	28.8	34.1
法人等が所有するスマートフォン	2.0	1.4
インターネットカフェ、ホテル等に備付けのパソコン	3.4	3.7
その他	3.8	1.7

(3) 被害の届出・通報の状況

ア　警察への届出・通報

警察への届け出た割合は、表 20 のとおり相談を含めても低いものの、実数を推計すると被害届だけでも 40 万件以上になるはずである。しかしながら、平成 28 年のサイバー犯罪に関する警察の統計[10]では相談を含めても 14 万件余りであることから、「社会的に望ましい行動」に係るバイアスが生じている可能性がある（「第 4 考察 2 捜査機関等への通報率について」参照)。

表 20　警察への届け出状況

	警察に被害届	警察で相談のみ	警察には届けなかった	警察以外の機関に届けた	どこにも届けなかった
第 1 回	10.4%		89.6%	30.7%	69.3%
第 2 回	6.7%	11.7%	81.5%	32.0%	68.0%

届け出た及び届け出なかった理由はそれぞれ表 21 及び 22 のとおりであるが、届け出なかった理由の筆頭が「大した被害ではなかったから」で、複数回答であるが、全体の 40～55％を占めている。

表 21　警察に届け出た理由

理由	第 1 回(%)	第 2 回(%)
被害を少しでも取り戻すため	26.7	36.3
犯罪は警察に届けるべきだから	25.6	32.7
犯人を捕まえて欲しいから	23.3	33.0
再発を防ぐため（被害が広がらないように）	22.1	34.7
対処方法が知りたかったから	＊	27.0
その他	1.1	1.0
分からない	1.1	3.7

表 22　警察に届け出なかった理由

理由	第 1 回(%)	第 2 回(%)
大した被害ではなかったから	40.6	55.9
手続きが面倒で時間もかかりそうだったから	18.4	21.2
届け出ても検挙できそうにないから	17.0	24.0
警察とは関わりたくないから	5.7	7.6
その他	8.8	10.7
分からない	9.5	10.8

イ　警察以外の機関への届出・通報

警察以外の機関への届出・通報状況は表 23 のとおりであるが、警察以外の機関への届出・通報も被害者の三分の一程度で、その多くが金融機関、インターネット関係企業と、公的機関への届出・通報は低調である。

表 23　警察以外の機関への届出・通報状況

警察以外の通報先	第 1 回(%)	第 2 回(%)
クレジットカード会社	9.7	10.4
銀行等金融機関	6.1	4.3
楽天、Yahoo 等ネットショップ運営会社	8.9	6.7
トレンドマイクロ等コンピューターセュキュリティ会社	5.1	3.4
ブログ、掲示板、SNS 等運営会社	＊	5.5
消費生活センター（ネット詐欺等）	4.6	4.7
インターネットホットラインセンター（違法有害メール）		2.6
情報処理推進機構情報セキュリティ安全相談（マルウェア）		1.5
法務省インターネット人権相談（いじめ等）		1.0
JPCERT／CC（マルウェア等）		0.5
フィッシング対策協議会（フィッシング）		1.2
政府模倣品・海賊版対策総合窓口		0.4
その他：	3.4	4.1
どこへも届けなかった	62.3	68.0

ウ　サイバー犯罪被害通報システムの利用

「サイバー犯罪被害をネット上だけで届出・通報できるシステムがあったとしたら利用したと思いますか」との問いについての回答状況は表 24 のとおりであるが、第 2 回調査では減少したものの「匿名なら利用したと思う」を含めると第 1 回、第 2 回両調査ともに 50%を越えているが、これも「社会的に望ましい行動」に係るバイアスが生じている可能性がある。

表 24　サイバー犯罪被害をネット上だけで届け出られるシステムについての利用意思

意思の有無	第 1 回(%)	第 2 回(%)
利用したと思う	46.9	36.7
匿名なら利用したと思う	24.1	19.7
利用しなかったと思う	6.2	8.9
分からない	22.7	34.7

(4) 被害後の被害者の変化

被害後の行動や心境の変化についての問いに対する回答の状況は、表 25 のとおりで、第 1 回、第 2 回調査ともに、「セキュリティ製品やサービスを新たに導入した」が筆頭であったが、約 4 割の被害者は何の対策も取っていなかった。

表 25　被害後の行動や心境の変化の有無

被害後の変化	第 1 回(%)	第 2 回(%)
セキュリティ製品やサービスを新たに導入した	20.4	21.6
ネットオークションの利用を止めた	8.8	4.7
ネットオークションでの出品者情報を念入りに確認するようになった	10.6	8.1
ネットショッピングでの支払い方法をクレジットカードに変えた	6.3	5.9
クレジットカードの利用明細をチェックするようになった	20.1	19.5
サイバー犯罪の手口や対策等の情報を入手するようになった	15.2	15.3
その他	5.3	10.0
特に何も変わらない	39.9	39.6

2　先行調査研究

（1）犯罪被害実態（暗数）調査

ア　調査方法

法務省は、平成 16 年以降 4 年おきに国連の国際犯罪被害実態調査（International Crime Victims Survey: ICVS）に参加する形で「犯罪被害実態（暗数）調査」を、全国から選んだ 16 歳以上の男女を対象としたアンケート調査等として実施している。犯罪全般を対象としているが、我が国独自の調査として、第 3 回調査[11]（平成 20 年）及び第 4 回調査[12]（平成 24 年）ではインターネットオークションに係る被害についても調査を行った。

平成 20 年の第 3 回調査は、同年 1 月から 3 月にかけて、層化二段無作為抽出法により全国から選んだ 16 歳以上の男女 6,000 人（男女同数）を対象として、平成 19 年以前の犯罪被害について、質問紙を用いた調査員による聞き取り方式及び調査対象者の自記式を併用して実施された。回答が得られた者は 3,717 人、回答率は 62.0％であった。

平成 24 年の第 4 回調査は、同年 1 月層化二段無作為抽出法により全国から選んだ 16 歳以上の男女 4,000 人を対象に郵送による質問票調査行い、回答が得られた者は 2,156 人、回答率は 53.9％であった。

イ　調査結果

第 3 回調査では、「昨年（平成 19 年）中に、あなたはインターネットオークション詐欺の被害に遭ったことがありましたか。」の問いに対し、3,717 人が回答し、第 4 回調査では、「過去 5 年間に，あなたはインターネットオークション詐欺の被害にあわれたことがありますか。」との問いに対し、2,156 人が回答した。結果は、表 28 のとおりである。

「捜査機関に届け出ましたか」との問いに対しては、第 3 回調査では「はい」が 3 人、「いいえ」が 25 人、「わからない」が 1 人であった。届け出なかった理由の筆頭は、「それほど重大ではない」14 人であった。第 4 回調査では、1 人が「届け出た」と回答した。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。

表 26　インターネットオークションによる被害（法務省調査）

	被害		捜査機関への通報	
	件数	割合(%)	件数	割合(%)
平成 19 年	29	0.78	3	10.3
23 年	6	0.28	1	5.0

（法務総合研究所研究部報告 41 及び 49 より著者が作成）

(2) 平成 28 年通信利用動向調査

ア　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 28 年度調査は、平成 28 年 1～2 月の間に全国の 20 歳以上の世帯主がいる 40,592 世帯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（E メール）によって 17,765 世帯から回答を得た。

イ　調査結果

過去 1 年間に自宅パソコン、PHS を含む携帯電話、スマートフォン及びその他の機器でインターネット利用をしたことのある世帯を対象に過去 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ごとの複数回答を求めた。集計世帯数は 2,030（比重調整後）で世帯員数は 6,043 人＋α である。＋α としたのは、統計表には単身から 7 人以上世帯まで個別に世帯数が記されており、これを積算して世帯員総数を算出したためである。7 人以上世帯は 29 であるのでαは、総世帯員数の 1%未満と推測されることから、表 27 においては総世帯員数を 6,043 人とした。

結果は表 27 のとおり、世帯を調査対象とし、かつ、実質的被害が生じていない「ウィルスを発見したが感染なし」及び「迷惑メール・架空請求メールを受信」を被害体験としていることとしていることから被害率は、65.3%と極めて高いものとなっている。

そこで、1 世帯の被害を世帯員 1 人の被害である仮定して、被害率を算出してみたところ、26.12%との結果を得た。なお、この場合、世帯員 1 人の類型の異なる複数被害はそれぞれ 1 件として計上されるが、類型が同じ被害を複数の世帯員が受けた場合でも、1 件として計上されていることから、被害率を算出する際の分子である被害件数は実数より低く計上されている可能性がある。一方で、分母である世帯員総数は 6,043 人以上であるが、6,043 人を世帯員総数としているので、同じく低く計上されていることから、相殺され被害率はより実数に近い形で算出されていると考えられる。

その中で、実質的な被害とみられる、「ウィルスに 1 度以上感染（1.47%）」、「フィッシング（1.47%）」、「不正アクセス（0.91%）」及び「その他（個人情報の漏洩、誹謗中傷など）（0.48%）」を加え合わせると 4.33%という数値が得られた。

表 27　インターネット利用に伴う被害体験（総務省調査）

被害の類型		世帯割合(%)	世帯員割合(%)
何らかの被害を受けた		65.3	30.17
	ウィルスを発見したが感染なし	16.6	5.58
	ウィルスに１度以上感染	4.4	1.47
	迷惑メール・架空請求メールを受信	60.3	20.25
	フィッシング	4.4	1.47
	不正アクセス	2.7	0.91
	その他（個人情報の漏洩、誹謗中傷など）	1.4	0.48
特に被害はない		21.0	56.03
無回答		13.8	13.8

（通信利用動向調査平成 28 年報告書より著者が作成）

(3) Crime Survey for England and Wales (CSEW) [13]

ア　調査方法

CSEW とは、英国政府統計局（Office for National Statistics）が、毎年実施している犯罪被害実態調査のことで、2012 年までは British Crime Survey と称していた。英国のうち、England と Wales に所在する 35,000 世帯（2016-17 調査）の 16 歳以上の男女を対象として、過去１年間の犯罪被害について面接により実施されている。2009 年から、10～15 歳の少年も一部対象としている。

調査対象のサイバー犯罪は、詐欺及び不正アクセス、マルウェア等コンピューターの不正使用（Computer misuse）で脅迫、わいせつ図画頒布、知的財産侵害等は含まれていない。

イ　調査結果

2016 年 4 月～2017 年 3 月の 1 年間におけるサイバー犯罪による被害発生状況の推計は表 28 のとおりである 。詐欺とコンピューター不正使用犯罪の件数が、ほぼ拮抗している。

表 28　CSEW におけるサイバー犯罪被害の推計（2016 年 4 月～2017 年 3 月）

被害手口	件数	被害率(%)
銀行、クレジットカード口座詐欺：Bank and Credit account fraud	1,244,500	2.70
投資名目以外の詐欺：Non-investment Fraud	589,600	1.28
マルウェア：Computer Virus	1,138,150	2.47
不正アクセス：Unauthorized access to personal information	603,000	1.31
計	3,575,250	7.76

（Crime in England and Wales: year ending Mar.2017　Table 4 及び TableE-8 より著者が作成）

(4) 英国ケント大学第 2 回サイバーセキュリティ調査[14]

ア　調査方法

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。

調査内容は、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についてである。

イ　調査結果

（ア）サイバー犯罪被害の状況

過去 1 年間に回答者の 26%が Cyber Dependent Crime（サイバー固有犯罪：不正アクセス禁止法違反及びコンピューター・電磁的記録対象犯罪等）の被害を受け（表 29)、9.3%が Cyber Enabled Crime（ネットワーク利用犯罪）の被害を受けた（表 30)。金額的被害を受けた者のうち、1,000 ポンド（15 万円前後）以上の被害を受けた者が 28.8%、1,000 ポンド未満が 71.2%であった。

表 29　サイバー固有犯罪の手口

手口	割合(%)
マルウェア:Virus/Malware Attack	11.9
フィッシング:Phishing scam	7.3
アカウントに対する不正アクセス等:Online account attack (e-mail,SNS etc.)	6.2
ネット銀行口座に対する不正アクセス等:Online banking attack	3.9
DoS 攻撃:Denial of service attack	1.7
上記被害には遭わなかった:None of the above	74.0

（ケント大学第 2 回サイバーセキュリティ調査結果より著者が作成）

表 30　ネットワーク利用犯罪の手口

手口	割合(%)
インターネット詐欺:Online fraud or theft	4.1
誹謗中傷、いじめ:Online harassment/Bullying	2.9
ストーカー: Online stalking	2.3
性的嫌がらせ:Online sexual harassment	1.7
上記被害には遭わなかった:None of the above	90.7

（ケント大学第 2 回サイバーセキュリティ調査結果より著者が作成）

（イ）被害の届出・通報状況

被害者で捜査機関への届出・通報した者の割合は、表 31 のとおりであるが、警察等捜査機関 3.5%、Action Fraud 2.7%（重複あり）と低いものであった。

表 31　被害の届出・通報状況

通報先	割合(%)
銀行等金融機関:Financial services(Bank etc.)	5.0
インターネットプロバイダー:Your service provider	3.8
警察等法執行機関:Other law enforcement(e.g. police)	3.5
コンピューターセキュリティ会社:Your computer security provider	3.1
AF: Action fraud	2.7
上記には通報しなかった:None of the above	84.9

（ケント大学第 2 回サイバーセキュリティ調査結果より著者が作成）

届出・通報しなかった理由の筆頭は、「自分で処理できたから」で、次が「時間の無駄だから」であった（表 32)。

表 32　届出・通報しなかった理由

理由	割合(%)
自分で処理できたから:I fixed the problem myself	10.3
時間の無駄だから:Waste of time	7.6
通報先や方法が判らなかったから:I don't know who to or how to report it	5.1
犯罪かどうか判らなかったから:I don't know what the crime was	3.8
無回答/不明:N/A	73.3

（ケント大学第 2 回サイバーセキュリティ調査結果より著者が作成）

3　サイバー犯罪被害通報システムに関する調査結果

(1) Action Fraud

ア　経緯

Action Fraud(AF)はイギリス全土で発生した詐欺及びサイバー犯罪に関する事案を協調的かつ全国的に一貫した対応を提供するための通報窓口及び通報記録を統括するセンターとしてロンドンシティ警察(City of London Police)[15]によって運用されている。

英国では、2000 年代前半、耳目を集めるような複数の大型詐欺事件で有罪判決を得られなかったことなどを背景に、詐欺防止法(the Fraud Act 2006)が制定され、内務省(Home Office)に詐欺に関する情報を集約する National Fraud Report Center (NFRC)が、ロンドン

シティ警察には、詐欺情報を分析、捜査する National Fraud Intelligence Bureau(NFIB)がそれぞれ設置された。NFRC が、AF の前身である。2008 年には National Fraud Strategic Authority(NFSA)が Attorney General’s Office(検事局)の執行機関として設立され、2009 年には National Fraud Authority(NFA)と改名されるとともに、NFRC の名称も AF と改められた。

2010 年、AF の運用主体が内務省へ移管された後、国際組織犯罪等に対する国家捜査機関である Serious Organized Crime Agency(SOCA)が National Crime Agency(NCA)へと増強改編されたのを機に NFA も統合・廃止されたことから、AF の運用主体はロンドンシティ警察へと移管され現在に至っている。

2011 年以降、詐欺事件統計については、AF が担当することとされ、2013 年からは詐欺事件統計は警察ではなく AF がその全てを記録している。

イ　システムの内容

通報の対象となる犯罪は、NFIB 管轄の詐欺事案及びコンピューター不正使用法(Computer Misuse Act)に規定されているサイバー犯罪である[16]。

AF で受理した情報の犯罪性が明らかな場合は、管轄の警察に通報され捜査が開始される。それ以外の通報については情報として調査分析の対象となる。

受理の対象となる情報は、犯罪者又は被害者が英国に所在している場合に限られている。通報はオンライン又はコールセンターで受け付けられており、匿名の通報はオンラインでは受付けていないが、コールセンターで匿名通報も受理している。

ウ　被害通報受理状況

AF には月に平均して約 25,000 件の犯罪が通報され、さらに約 12,000 件の情報が寄せられている。情報報告は、一般市民又は企業からの通報で、犯罪としては成立しないものの詐欺行為として申し立てられた事案であるが、この情報通報も分析対象とされている。これにより作成されたデータベースは、「Know Fraud」システムと呼ばれ、英国内の捜査機関の利用に供されている。

表 33 は、AF が記録した詐欺及びサイバー犯罪手口の内訳である。CSEW の結果（表 28 参照）と比較すると、詐欺が 90%以上を占めマルウェアや不正アクセスなどのサイバー固有犯罪の件数が大幅に低くなっている。この種犯罪の届出・通報がいかに低調であるのかということが明確である。

表 33　AF が記録した詐欺及びサイバー犯罪手口の内訳（2016 年 4 月～2017 年 3 月）

手口	件数	割合(%)
銀行、クレジット詐欺:Banking and credit industry fraud	32,914	12.46
投資名目以外の詐欺:Non-investment fraud	107,213	40.60
投資詐欺:Financial investments	4,154	1.57
前払い金詐欺:Advance fee payments	44,408	16.82
保険金詐欺:Insurance fraud	1,809	0.69
その他の詐欺:Other fraud	57,016	21.59
マルウェア:Computer virus/malware	7,259	2.75
不正アクセス:Hacking	8,502	3.22
DoS 攻撃:Denial of service attack	781	0.30
計	264,056	100

（Crime in England and Wales: year ending Mar.2017 より著者が作成）

(2) Internet Crime Complaint Center[17] (IC3)

ア　概要

IC3 は、米国連邦捜査局（Federal Bureau of Investigation: FBI）の組織であるが、2000 年に発足し、当初は、捜査機関の支援等を行っている公益法人である National White Collar Crime Center と共同で運用されていた。発足時は、Internet Fraud Complaint Center と呼ばれていたが、サイバー犯罪の多様化に伴い、2003 年に現在の名称に改められた。

IC3 の任務は、インターネット上の犯罪行為を FBI に通報するための信頼性が高く簡便なシステムを一般に提供するとともに、法執行機関と関係企業との効果的な協力関係の構築を図ることである。受理された通報は、分析され捜査等のため法執行機関に共有されるとともに、インターネット利用者等への注意喚起に用いられている。

イ　被害通報の受理状況

2016 年中 IC3 は、298,728 件のサイバー犯罪被害通報を、米国を含む世界 21 か国から受理しており、米国内からの通報は全体の 95.4%でその手口別内訳は表 34 のとおりである。

AF 同様詐欺被害が、多くを占めているが、個人及び企業の情報流出等侵害とその手段とみられるフィッシング及び ID 窃盗が 20%近くに上っている。

表 34　IC3 が受理したサイバー犯罪被害手口の内訳（2016 年）

被害手口	件数	割合(%)
代金不払い／商品不送:Non-payment/Non-delivery	81,028	21.8
個人情報侵害:Personal Data Breach	27,573	7.4
過大(架空)請求:419/Overpayment	25,716	6.9
フィッシング:Phishing/Vishing/Smishing	19,465	5.2
雇用詐欺:Employment	17,378	4.7
恐喝:Extortion	17,146	4.6
ID 窃盗:Identity Theft	16,878	4.5
脅迫:Harassment/Threats of Violence	16,385	4.4
カード詐欺:Credit Card Fraud	15,895	4.3
前払い金詐欺:Advanced Fee	15,075	4.1
恋愛詐欺等:Confidence Fraud/Romance	14,546	3.9
不動産詐欺:Real state/Rental	12,574	3.4
公的架空請求:Government Impersonation	12,344	3.3
送金詐欺:BEC/EAC	12,005	3.2
技術支援詐欺:Tech Support	10,850	2.9
不当表示:Misrepresentation	5,436	1.5
懸賞金詐欺:Lottery/Sweepstakes	4,231	1.1
企業情報侵害:Corporate Data Breach	3,403	0.9
マルウェア:Malware/Scareware	2,783	0.7
ランサムウェア:Ransomware	2,673	0.7
知的財産権侵害:IPR/Copyright Counterfeit	2,572	0.7
その他:Other	21,468	5.8
不明:No Lead value	13,794	3.7

（2016 Internet Crime Report[18]から著者が作成）

(3) Australian Cybercrime Online Reporting Network (ACORN)

ア　概要

Australian Cybercrime Online Reporting Network[19] (ACORN)は、2014 年にオーストラリア政府が設置した、連邦及び地方の警察機関(All Australian Police)、犯罪情報局 (Criminal Intelligence)、司法局 (Attorney General’s Department) 等の合同による機関 (National policing initiative) である。サイバー犯罪を簡便にオンラインで通報できるようにするとともに、犯罪予防等のための情報を提供するためのシステムで、受理された被害通報は、内容

に応じ適切な連邦、州警察等の捜査機関に転送される。また、匿名での被害通報も受理されている。

イ　被害通報の受理状況

ACORN は、2016 年中オーストラリア国内から 46,975 件の被害通報を受理しておりその内訳は表 35 のとおりである。

表 35　ACORN が受理したサイバー犯罪被害手口の内訳（2016 年）

被害手口	件数	割合(%)
ネット詐欺（売買を除く）:Scams or fraud	23,415	49.8
ネット売買:Purchase or sale	9,154	19.5
ネットいじめ:Cyber Bullying	3,510	7.5
その他:None of above	10,896	23.2

（ACORN statistics reports[20]より著者が作成）

第 4　考察

1　サイバー犯罪被害率の精度について

(1) 回答結果の精査

サイバー犯罪の被害率については、第 1 回調査 9.60%、第 2 回調査 12.48%との結果であった。設問については、具体的な被害を受けた者を抽出できるよう工夫するとともに、第 2 回調査では、犯罪被害ではないが、第 1 回調査の自由記載で回答の多かった項目について、分析する際の除外の便のため、あえて設問に盛り込んだところである。第 2 回調査結果から実質的被害と言えない「迷惑メール」及び「OS のアップデート絡みによる動作支障」の項目を除外するとともに、各項目のその他自由記載欄を精査し明らかに犯罪被害と認められないものを除外したところ、総被害率は、10.92%となった（表 41 参照)。

(2) サンプルの属性と被害率

性別では、平成 28 年中何らかのサイバー犯罪被害を受けた者の内女性が占める割合は、42.0%と平成 28 年の刑法（身体）犯被害者[21]に占める女性の割合 36.0%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 21.7%、以下 20 歳代 18.9%、30 歳台 14.1%と年齢が高くなるにつれて低下している。

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 26.93%、「他者から援助を受けながら IT を利用している」者 8.77%と 3 倍以上の開きがあった。また、オンライン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 1 時間未満」が 2.89%、「9～10 時間」で 27.8%と 10 倍近い開きがあった。

そこで、「被害に遭ったことがある」を「1」、「被害に遭ったことがない」を「0」とする、二項ロジット回帰分析を試みたところ、表 36 及び表 37 のとおり、サンプルの各属性（IT 習熟度、オンライン時間、性別）とサイバー犯罪の被害率にプラスの因果関係が認められた[22]。

表 36　被害の有無を従属変数とする二項ロジット回帰分析

	B	SE
定数	-0.63	0.268 ***
IT 習熟度	0.272	0.037 ***
オンライン時間	1.055	0.116 ***
性別	0.28	0.055 ***
年齢	-1.958	0.18 ***
対数尤度	9,406.001	
Nagelkerke R2 乗	0.055	
n	13,000	

***:p<0.001, **:p<0.01, *:p<0.05

表 37　サンプル属性と他の要因との相関分析の結果

		サイバー犯罪被害の有無	IT 習熟度	オンライン時間（対数）	性別
サイバー犯罪被害の有無	相関係数	1	.096**	.106**	.064**
	有意確率（両側）	.	0	0	0
	度数	13,240	13,000	13,000	13,240
IT 習熟度	相関係数	.096**	1	.219**	.199**
	有意確率（両側）	0	.	0	0
	度数	13,000	13,000	13,000	13,000
オンライン時間（対数）	相関係数	.106**	.219**	1	.075**
	有意確率（両側）	0	0	.	0
	度数	13,000	13,000	1,3000	13,000
性別	相関係数	.064**	.199**	.075**	1
	有意確率（両側）	0	0	0	.
	度数	13,240	13,000	13,000	13,240

***:p<0.001, **:p<0.01, *:p<0.05

つまり、サイバー犯罪被害を受ける確率は、IT の習熟度が高ければ高くなり、オンライン時間が長い方が高くなるということになる。また、そうした被害を受ける確率についても、男

性の方が女性よりも高く、年齢は若年層ほど、被害に遭いやすいという結果になった。ただし、結果としては説明力が高くないことから、その点に留意が必要である。なお、サイバー犯罪の類型を詐欺等の財産的犯罪、脅迫、ストーカー等の非財産的犯罪及びマルウェア感染等の情報技術的犯罪に分けて、同じく分析を試みたがいずれも、同様の結果であった。

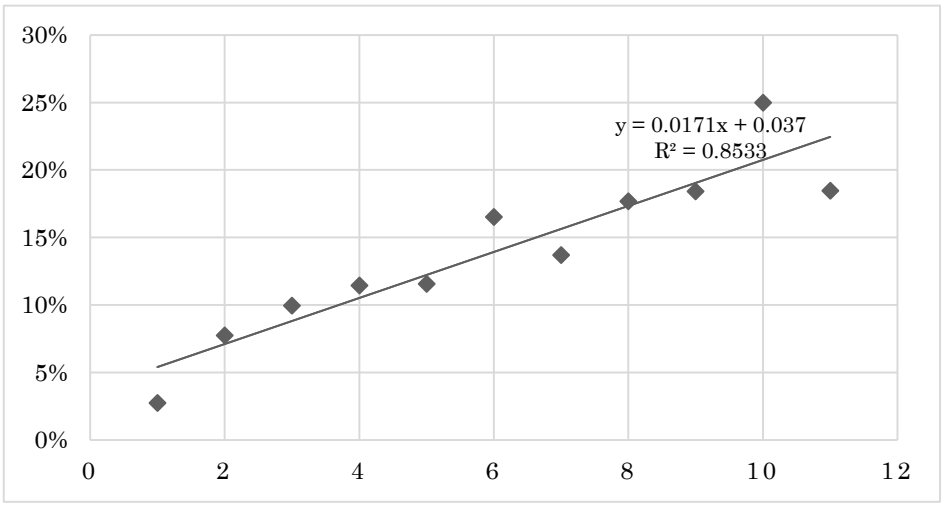
このサンプルの属性と母集団である全国のインターネットユーザーの属性を鑑みると、サンプルにあっては、インターネットリサーチ会社の登録モニターであることから、いわゆるインターネットのヘビーユーザーであると言える。したがって、母集団に比べて平均的にオンライン時間が長く、かつ、IT 習熟度が高いことが推認されることから、オンライン時間別の被害率を算出した結果は、表 38 のとおりである。

表 38　オンライン時間別のサイバー犯罪被害率

オンライン時間数	被害率(%)
0-1h	2.74
1-2h	7.75
2-3h	9.95
3-4h	11.44
4-5h	11.58
5-6h	16.52
6-7h	13.71
7-8h	17.69
8-9h	18.42
9-10h	25.00
10h 以上	18.46

比較分析の手がかりを調査したところ、総務省が主要メディアの平均利用時間を調査していることが判明した[23]。これによると、平成 28 年における、平均オンライン時間は、平日で 99.8 分間、休日で 120.7 分間である。これを、平成 28 年中の土、日曜及び祝日の総数 121 日を休日として、加重平均したところ、平成 28 年の平均オンライン時間は、106.7 分となった。そこで、本調査結果のサイバー犯罪被害率を y 軸に、オンライン時間を x 軸とした散布図から近似式 y=0.0171x+0.037 を得（グラフ 1)、この x に 1.78（時間）＝106.7（分）を代入すると、6.74%という被害率が得られた。R^2値は、0.8533 で相関度は高い。ちなみに、オンライン時間が 6 分増えると、0,171 ポイント被害率(%)が高まる計算となる。

グラフ 1　サイバー犯罪被害率とオンライン時間



この調査分析結果の 6.74%という被害率は、インターネット利用者についてのものであるので、下記数式のとおり全国民ベースで換算すると、5.36%という数字が得られた。これが、平成 28 年中のサイバー犯罪の推計被害率なのである。

6.74%×100,840,000（インターネット利用者総数）÷126,933,000（総人口）＝5.36%

(3) 被害率の検証

この推計被害率の数値を先行調査研究と比較して、その信頼性の検証を試みた。

全体の被害率としては、総務省調査のうち、本調査では被害として取り扱わなかった「ウィルスを発見したが感染なし」(5.58%) 及び「迷惑メール・架空請求メールの受信」(20.25%) を除外した世帯員ベースの被害率は、4.33%であった（表 27 参照)。これは、インターネット利用者を対象とした調査であるので、本調査の被害率は、オンライン時間補正後の 6.74%と比較することになる。2 ポイント以上異なっているが、この 4.33%の被害率には、本調査の項目にある詐欺 (0.83%)、脅迫/恐喝 (0.64%)、いじめ (0.18%)、ストーカー (0.14%) 及び知的財産権侵害 (0.06%) は含まれていないとみられることから、これらを 6.74%から差し引くと 4.89%と近似する数値が得られた。総務省調査には、「架空請求メールを受信」の項目がありこの中に詐欺の実被害が含まれている可能性があるが、いずれにしてもこれは除外されているので本調査との比較に当たっての問題とはならない。

また、CSEW (2016-17) におけるサイバー犯罪被害率は 7.76%(表 28 参照)であるので英国の統計には詐欺以外の脅迫等一部罪種が含まれていないことを勘案しても、英国の犯罪認知件数 (police recorded crime) が 3,788,269 件 (2016－17) と日本の刑法犯認知件数の 3 倍以上であり、犯罪率が全体的に高いとみられることから、類似した結果であると言えよう。

また、個別の手口では、総務省調査の不正アクセス、フィッシング及びその他（個人情報の漏洩、誹謗中傷など）並びに法務省調査のインターネットオークションついて比較した。

まず、総務省調査との比較結果が表 39 である。フィッシングについては第 2 回調査結果で大きく異なっているが、個人情報の流出、誹謗中傷では近似する結果となった。

表 39　総務省調査との比較

被害類型	本調査:オンライン時間補正後(%)	総務省調査(%)
不正アクセスされた	1.35	0.91
フィッシング	0.08 第 1 回調査:0.55	1.47
個人情報の流出、誹謗中傷	0.58	0.46

インターネットオークションについての比較が、表 40 である。法務省調査結果については、全国民を対象としたものであることから、本調査結果（28 年）を総人口比で補正した結果（0.29%）で比べると、平成 23 年法務省調査結果（0.28%）とほぼ一致したが、平成 19 年法務省調査結果（0.78%）は 2 倍以上高くなっている。そこで、警察庁の統計[24]をみるとインターネットオークション被害に関する相談の受理件数は、平成 23 年 5,905 件、平成 28 年 5,440 件であるが、平成 19 年は 12,707 件と 2 倍以上にのぼっていることから、同年は被害が多かったとみられ、それが法務省調査結果に反映したものと推認される。

表 40 インターネットオークション被害率

	被害年	件数	割合(%)
本調査	平成 28 年	47	0.36 0.29（総人口比）
法務省調査	平成 19 年	29	0.78
	平成 23 年	6	0.28

以上から、本調査結果の被害率は、他の複数の統計と比較しても信頼に足る精度を有しているものと考える。この 5.36%という数値は、法務省の第 4 回犯罪被害実態（暗数）調査では平成 23 年中の全犯罪による被害率が 11.9%であるので、その約半分に当たり、相当高いと言えると考えられる。また、算出された被害率にインターネット利用者数を掛けると、推計被害者総数は、679 万 8,531 人となる。類型別サイバー犯罪被害率及び推計被害者数の総括表が、表 41 である。

表 41　類型別サイバー犯罪被害率

被害類型	当初補正後(%)	オンライン時間補正後	総人口比	推計被害者数
現金、電子マネー等をだまし取られた	1.07	0.66	0.52	665,490
現金等以外のものをだまし取られた	0.28	0.17	0.14	172,357
脅迫又は恐喝された	1.04	0.64	0.51	646,339
名誉棄損、誹謗中傷された	0.66	0.41	0.32	411,742
いじめをされた	0.29	0.18	0.14	181,933
ストーカーをされた	0.23	0.14	0.11	143,631
ＩＤやパスワードをだまし取られた	0.39	0.24	0.19	244,173
コンピューター又はスマートフォンの情報を流出させられた	0.28	0.18	0.14	177,145
メールや SNS のアカウントに不正アクセスされた	2.18	1.35	1.07	1,359,706
知的財産権を侵害された	0.09	0.06	0.05	57,452
コンピューター又はスマートフォンの動作に支障が生じた	3.98	2.46	1.95	2,480,028
利用していたサイトから自分の情報が流出	0.17	0.10	0.08	105,329
その他	0.25	0.15	0.12	153,206
総被害率／総被害者数	10.92	6.74	5.36	6,798,531
サイバー犯罪被害には遭わなかった。	89.08	93.26	94.64	

2　捜査機関等への通報率について

サイバー犯罪被害に関する警察等捜査機関への通報率について英国及び法務省の調査結果と比較したのが、表 42 である。

サイバー犯罪被害に関しては、日本、英国ともに捜査機関への届出・通報率が相当低いことがわかる。ちなみに、一般犯罪と比べても、法務省の第 4 回犯罪被害実態（暗数）調査では、自動車等や車上盗の通報率は 50%を超えており、一般的に低いといわれている性的犯罪においても、18.5%である[25]。

届出・通報しなかった理由の筆頭は、「大した被害ではなかったから」が、第 1 回、第 2 回とも半数以上を占めており、「手続きが面倒で時間もかかりそうだったから」が約 2 割を占めている（表 22 参照）。被害額 10 万円以上の被害届出率が 45.9%であるのに対し、被害額 1 万円以下では 19.1%に過ぎない。届出・通報にかける時間や手間を考えると、被害金額の多寡

によって通報率が上下することはある意味当然とも考えられるのであるが、低コストで不特定多数に犯罪企図を可能とするサイバー犯罪の特性がまさに悪用されていると言えるのである。

表 42　捜査機関への届出・通報率の比較

	捜査機関への通報率(%)	備考
本調査	8.33	2 回の調査の平均
	14.98	警察への相談のみを含む
法務省調査	8.16	2 回の調査の平均
CSEW	7.38	AF の受理数を推計値で除したもの
ケント大学調査	3.50	
	6.20	AF を含む

次に、調査結果の届出・通報率の数字自体その信ぴょう性を検証する必要がある。すなわち、推計被害件数に届出・通報率を掛けて届出・通報件数を推計すると、56 万件余あるいは 101 万件余という大きな数字が得られるのであるが、現実に警察が把握している数字は、検挙件数 7,448 件、相談件数 131,518 件であり、これを単純に加えた 138,966 件と比較すると 4～7 倍もの違いが生じているのである。

これは、本選択肢の回答において、「社会的に望ましい行動」に係るバイアスが生じているのではないかとみられる。この「社会的に望ましい行動」に係るバイアスとは、アンケート調査において社会的に望ましい回答と望ましくない回答を選択させる場合、望ましい回答をより選択する傾向があるというものである。本調査においては、警察への届出が望ましい行動で、届け出ないことは望ましくない行動ということになる。本調査では、届け出たか出なかったかの事実を聞いているのではあるが、これだけ大きく調査結果の数字と実際の統計数字と異なっていることを鑑みれば、「社会的に望ましい行動」に係るバイアスが生じていると考えざるを得ない。

また、警察以外の通報先としては、クレジットカード会社が 2 回の調査ともに筆頭であり、以下金融機関、ネットショップ運営会社等が続き、複数回答ながら消費生活センター等公的機関への通報率は、全体としてもさほど高くはないのである（表 23 参照)。これは、サイバー犯罪の罪種や手口別に通報・相談の窓口が細分化されており、分かりにくいことが理由の一つと考えられる。

さらに、サイバー犯罪被害についてネット上だけで警察に届けられるシステムがあったら利用したかの問いに対しては、「匿名なら」という条件付きも含めると半数を大きく超えているのであるが、ここでも、「社会的に望ましい行動」に係るバイアスが生じている疑いがある。（表 24 参照)。

3　オンラインによるサイバー犯罪被害通報システムについて

（1）導入の必要性

ア　サイバー犯罪被害実態把握の重要性

冒頭述べたように、警察統計上のサイバー犯罪の件数としては検挙件数が用いられている。そのためサイバー犯罪の件数が、増加傾向にあることは認識できるのであるが、実数は、8,000 件前後と刑法犯認知件数と比較するに極めて小さいものとなっている。それは、サイバー犯罪検挙件数の半数以上を占める不正アクセス防止法違反、児童買春、児童ポルノ法違反事件等の特別法犯は、そもそも送致件数で計上されており、認知件数という概念がないためである[26]。

また、刑法犯サイバー犯罪の多くを占める詐欺罪の場合は、特殊詐欺等外見的に欺罔行為が明確なものを除いて、単なる債務不履行なのか詐欺であるのかは、捜査を遂げてみないとわからないことが多いことから、その認知件数は他の刑法犯に比べても検挙件数に近いものとなっているのである。すなわち、成りすましなど外見的に欺罔行為が明らかな振り込め詐欺等の特殊詐欺が急増する以前の平成 12 年の詐欺犯の認知件数は、44,384 件、検挙件数 35,255 件である。ちなみに特殊詐欺の認知件数が、14,000 件を超えている平成 28 年の詐欺犯では、認知件数 40,990 件、検挙件数 18,582 件となっている。このような理由から、従来から警察ではサイバー犯罪の件数として認知件数ではなく、検挙件数を用いているのである[27]。

その一方、上述のとおり第 2 回サイバー犯罪被害実態調査結果から平成 28 年中全国のインターネット利用者の 6.74％、680 万人が何らかの被害を受けたとの結果が出ている。警察が把握している検挙件数との比較では百分の一以下、サイバー犯罪等に関する相談件数（平成 28 年 131,518 件）と比較しても 16.9％とサイバー犯罪に関する警察への通報率は極めて低いのである。

確かに、本調査はこの通報率の低さを補うべく実施したものであり、犯罪被害実態調査の先進国である英国では、「犯罪被害実態調査（Crime Survey）は、信じがたいほど有用（incredibly valuable）[28]」と評価しているが、犯罪被害実態調査では、被害者を助け、被疑者を検挙することは、困難なのである。もちろん、被害を申告しない被害者は、国家による救済に値しないとの考え方もできるのであるが、従来型の犯罪とは異なるサイバー犯罪の特性を鑑みるとき、国家としてはより積極的な対応が必要であると考えられる。

イ　被害者支援の充実の必要性

サイバー犯罪の主な特性は、①インターネットバンキングの不正送金事案や情報の窃取事案等被害者が、被害を受けた事実に気が付きにくいものが多いこと、及び②メールによる架空請求やワンクリック詐欺等極めて低いコストで、かつ、不特定多数に対し短時間で犯罪を企図することが可能であることである。

この特性のため、被害者は被害の発生に気付くのが遅れ、短時間に大量の犯罪が企図されることから、被害は広範囲に拡散してしまうのである。これを少しでも防ぐためには、サイバー犯罪ごとの具体的な手口をインターネットユーザーに情報提供して注意喚起することが必要な

のであるが、そのためには、新たな手口に関する被害等をいち早く把握することが肝要なのである。すなわち、マルウェアやOSの脆弱性等に関してJPCIRTコーディネーションセンター[29]が発信している緊急情報のようなシステムを、サイバー犯罪全般に広げていくことが必要なのである。そのためには、簡便で迅速なサイバー犯罪被害通報を可能とするようなシステムを整備しなければならないと考えられる。

(2) 導入すべきモデル

上記で述べたような、簡便で迅速なサイバー犯罪被害通報を可能とするようなシステムとしては、どのようなものが考えられるのであろうか。

まず、運用主体であるが、調査した3か国のシステムにあっては、法執行機関が英国（ロンドンシティ警察）及び米国（FBI)、中央と地方政府の合同機関がオーストラリア（National Policing initiative）といずれも、法執行機関又は政府機関が運用している。犯罪被害に関する情報であること及びその後の捜査の便宜を考慮すれば、法執行機関が対応することが望ましいと言える。しかしながら、オーストラリアのACORNは、受理情報に関する捜査管轄を持たず、英、米においても受理する情報の多くは受理機関であるロンドンシティ警察又はFBI以外の法執行機関の管轄であることから、運用主体が必ずしも捜査管轄を有している必要はないと考えられる。

次に通報の方法については、サイバー犯罪はその多くがインターネット利用中に発生、あるいは被害を受けたことに気付くものであるから、被害者の便宜を考えればインターネットで通報できるものが望ましいことは言うまでもない。ここで問題となるのは、インターネットでの被害通報を「被害届」として受理できるか否かという点である。我が国の現状では、通報サイトへの入力やメールでのやりとりが行われたとしても、本人確認の点から、原則的には困難であるといわざるをえない。

現在、我が国の警察において「被害届」のほかに被害通報を受理する手段として用いられてものとして「相談」及び「情報提供」があるのでこれについて検討する。

「相談」については、警察安全相談として、全国の警察本部、警察署等に窓口が設けられ、神奈川県警察等電子メールでの受付も行われているが、主に面接で行われており、原則として匿名での相談は受け付けられていない。

「情報提供」については、様々な形態で行われているが、不特定多数から情報を募る手段として、匿名での提供を推奨する「匿名通報ダイヤル[30]」がある。これは、暴力団が関与する犯罪等、犯罪インフラ事犯、薬物事犯、拳銃事犯、特殊詐欺、また、少年福祉犯罪、児童虐待事案、人身取引事犯等の潜在化しやすい犯罪の検挙、また、被害者となっている子どもや女性の早期保護等を図るため、犯罪情報の提供を募るサイトである。「匿名通報ダイヤル」という名称であるが、電話だけでなく電子メールでの通報を受け付けており、警察庁が民間企業に委託して行われている。

インターネットによるサイバー犯罪通報システムは、英（AF)、米（IC3)、豪（ACORN）で導入されており、最近導入されたACORNでは、匿名での通報も可能としている。英のAFにおいても電話通報では匿名での通報が可能となっている。

いずれも、政府機関が運営しているが、通報を直ちに捜査の端緒なる被害届ではなく、犯罪情報として受理し、その後の調査分析により捜査に着手するか否かは担当すべき捜査機関の裁量に委ねられているが、具体的な捜査に着手しない場合でも調査分析の結果は、被害防止や他の事件捜査のための情報として活用されるのである。

次に、サイバー犯罪を含むサイバー空間でのトラブル対処については、現在警察を始めとして多くの行政機関、公的機関、民間組織がそれぞれの必要に応じて相談や被害軽減のための活動を展開している実態にある（表23参照)。そこで、こうした組織が受理したサイバー犯罪情報を警察に伝達されるような仕組みを構築する可能性について検討する。

現状では、公務として行われているものついては、その過程で犯罪ありと思料した公務員には告発義務（刑事訴訟法第239条第2項）が課せられているところであるが、告訴告発は、捜査機関に捜査を義務付ける法的効果を有し、また、原則個人で行うものであることから、公務所間の情報提供等の協力関係に用いることはなじまないと考えられる。

したがって、警察と各組織との間でサイバー犯罪に関する情報提供の申し合わせ等をそれぞれの組織と行うなどの協力体制を構築すれば可能と言えそうであるが、各組織は、それぞれの目的に沿った対応が中心であり、情報通信企業にあっては、憲法上「通信の秘密」の保持義務があり、そうでない組織にあっても個人情報保護方針が異なっていることなどから、各組織が把握したサイバー犯罪をシステマチックに警察に伝達されるような仕組みを構築することは相当な困難が見込まれる。

最後に、サイバー犯罪被害の届出・通報を促進するための方策を検討する。被害者へのフィードバックとなる被害対応措置等の情報を個別に提供するようなサイバー犯罪被害診断システムについては、警察に届け出た者の27.0%が「対処方法が知りたかったから」を挙げているように明らかにそのニーズは存在する（表21参照)。したがって、低調な届出・通報を促進する手段として、被害者が求める対処方法を個別具体に提供できるシステムが、届出・通報受理システムに付随していれば、確実にサイバー犯罪被害の届出・通報が促進されると見込まれる。既に電子メールでの相談を受け付けている警察本部も存在していることから、予算と人員を確保できれば、実現可能と考えられる。

また、サイバー犯罪被害をネット上だけで届け出られるシステムの利用意思に関する問いでは、「社会的に望ましい行動」に係るバイアスが生じている可能性があるものの、20%前後の回答者が「匿名なら利用したと思う」と回答しており、匿名性も届出・通報の促進に資すると考えられるのである（表24参照)。

以上検討の結果を整理すると、運用主体にあっては、情報に基づく捜査を効果的に進めるためには、直接的な管轄の有無は別にしても、法執行機関であることが必要であると考える。た

だし、具体的な運用については、「匿名通報ダイヤル」のように民間に委託することも可能であろう。

通報方法であるが、サイバー犯罪の特性を鑑みると、情報提供の迅速性、簡便性に重点を置くべきであると考えられることから、「被害届」ではなく、「サイバー犯罪情報」として受理することが現実的であると考えられる。さらに、届出・通報を促進するためには、匿名での通報を認めるとともに、届出・通報者が、被害対処のための個別具体的な情報を得られるようにシステムが設計されるならば、効果的であると考えられる。

第5　結論

我が国における平成28年中のサイバー犯罪の被害実態は、推計被害者数6,798,531人被害率5.36%、詐欺、脅迫等のネットワーク利用犯罪だけでも推計被害者数2,221,492人被害率1.74%と平成28年の刑法犯認知件数996,120件と比較するまでもなく深刻な実態にあることは明白である。さらに、考察で明らかになったように、サイバー犯罪の被害率は、全体としても包括的な犯罪類型別でも、オンライン時間の長さ及びIT習熟度の高さとプラスの因果関係がある。すなわち、国民のオンライン時間が長くなればなるほど、あるいは国民のIT習熟度が高まれば高まるほど被害が拡大するのである。

平成27年の平均オンライン時間は、97.8分であるので、平成28年と比べて、被害率では0.26ポイント、被害者数にして約260,000人増加したことになるのである。ちなみに、平成27年から平成28年にかけての刑法犯認知件数は102,849件減少しているが、CSEWの犯罪申告率40%[31]を我が国に当てはめてみると、暗数も含めて102,849件÷0.4=257,122件の刑法犯が減少した計算となるが、まさにサイバー犯罪被害者数の増加分とほぼ一致しているのである。

本調査により我が国におけるサイバー犯罪被害の深刻な状況が明らかになったところであるが、被害実態調査では、個別の事件の解決は困難である。したがって、被害者の積極的な届出・通報が求められるところであるが、その被害の届出・通報率も一般犯罪と比べてかなり低いことが判明している。被害を届出・通報しなかった理由の筆頭は、「大した被害ではなかったから」で、これは、まさにサイバー犯罪者の思うつぼにはまっていると言える。すなわち、ITの発展は、架空請求詐欺、ワンクリック詐欺に代表されるように不特定多数者に対して低コストで犯罪を企図することを可能としたのである。この種犯罪は、1件当たりの被害額が僅少であっても、ITの悪用で多数の犯罪を敢行することによって大きな犯罪収益をもたらしているのである。いいかえれば、寸借詐欺[32]のようなローリスクローリターンの犯罪を、ITの発展は、ローリスクハイリターンの犯罪に変化させてしまったのである。

この種犯罪を把握、検挙するためには被害者の積極的な被害の届出・通報が不可欠であることは言うまでもないが、被害が僅少であると被害回復の欲求及び犯人への処罰意識が一般的に低く、手続きの煩瑣性も加わって、届出・通報が低調なのである。これを打開し、サイバー犯罪被害の届出・通報を促すためには、被害者の認識を改めるとともに簡便な届出・通報システムの整備が必要なのである。

具体的には、英、米、豪で導入されているようなインターネット上だけで完結するサイバー犯罪被害通報システムを導入することである。その場合、現在の手続き上オンラインで被害届を受理することは困難であるが、サイバー犯罪情報として受理し、犯罪捜査に活用することは十分可能であると考えられる。既に、「匿名通報ダイヤル」という一定の犯罪に対する匿名通報システムが導入されていることから、サイバー犯罪被害にあっても匿名での通報を可能とするとともに、届出・通報者が求める被害対処のための個別具体的な情報が提供されれば、さらに届出・通報が促進されると考えられる。

最後に本調査結果から新たに得られた調査研究の課題を二つ指摘することとする。

一つは、犯罪の転移についてである。本調査からは刑法犯認知件数が、平成 15 年以降 14 年連続減少する一方で、平成 27 年から 28 年にかけては、暗数を含めると刑法犯の減少数とサイバー犯罪の増加数がほぼ一致しているとの結果が明らかになり、刑法犯からサイバー犯罪への犯罪の転移が大規模に生じている疑いが生じたところである。ただ、ここでは犯罪全体の英国の統計に基づく届出・通報率を用いて試算したものであることから、サイバー犯罪だけではなく、我が国の犯罪全体の被害実態調査を行い、犯罪の転移の実態を明らかにする必要である。

二つ目は、IT 習熟度とサイバー犯罪被害率との関係である。分析によれば、IT 習熟度とサイバー犯罪被害率がプラスの因果関係にあることが明らかになった。サイバー犯罪被害を減少させるためには、インターネット利用者一人一人が、サイバー犯罪に対する抵抗力を高める必要があることから、これまでも様々な IT 教育や広報啓発が行われているのであるが、本調査結果を見る限り、その効果は疑わしいものとなっているのである。したがって、サイバー犯罪対策の中核であるインターネット利用者のサイバー犯罪への抵抗力を高めるためには、IT 習熟度とサイバー犯罪被害率に関しより詳細な調査を行い、効果的なサイバー犯罪予防のための教育訓練手法を開発する必要があると考えられるのである。

---

[1] 平成 28 年警察白書 120 頁
[2] 通信利用動向調査平成 28 年報告書（世帯編）
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b1.html (平成 29 年 9 月 15 日参照)
[3] 警察庁「サイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/(平成 29 年 9 月 15 日参照)
[4] http://www.moj.go.jp/housouken/houso_houso34.html (平成 29 年 9 月 15 日参照)
[5] 総務省情報通信政策研究所「平成 28 年情報通信メディアの利用時間と情報行動に関する調査」
http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000064.html (平成 29 年 9 月 15 日参照)
[6] http://www.crimesurvey.co.uk/ (平成 29 年 9 月 15 日参照)
[7] http://www.cybersecurity.kent.ac.uk/Survey2.pdf（平成 29 年 9 月 25 日参照）
[8] https://www.ic3.gov/default.aspx (平成 29 年 9 月 15 日参照)
[9] https://www.acorn.gov.au/ (平成 29 年 9 月 15 日参照)
[10] 注 3 参照
[11] 法務総合研究所研究部報告 41 221 頁
[12] 法務総合研究所研究部報告 49 80-81 頁
[13] 注 6 参照
[14] 注 7 参照
[15] ロンドンの中心部の一部を管轄する警察本部。ロンドンの他の地域を管轄するいわゆるロンドン警視庁（Scotland Yard）とは別の独立した組織。

[16] 通報対象犯罪のコード・分類は 62 種からなり、「詐欺事案における刑法犯件数内務省集計規則」(Home Office Counting Rules For Recorded Crime - Fraud)によって詳細に記載されている。

[17] 注 8 参照

[18] https://pdf.ic3.gov/2016_IC3Report.pdf (平成 29 年 9 月 15 日参照)

[19] 注 9 参照

[20] https://www.acorn.gov.au/resources (平成 29 年 9 月 15 日参照)

[21] 「平成 27 年の犯罪」53 表

[22] インターネットによるアンケート調査においてインターネット利用時間に関するの問いでは、正確な時間数を分単位で記述してもらったが、前述の結果のように利用時間に大きな差があるため、一番小さい数字を基準とした対数変換を行った数字値に変換を独立変数として投入して 2 項ロジット分析を行った。また、性別に関しては男性を 1、女性を 0 とするダミー変数を用いた。そのため、犯罪に遭ったと性別の結果で B がプラスの数値になっていることから、男性が被害に合いやすいという結果になる。IT 習熟度は質問項目の「1．IT について高度な知識・技能を有している」という回答を 4、「2．IT を業務で利用するに足りる知識・技能を有している」を 3、「3．IT を生活で利用するに足りる知識・技能を有している」を 2、「1．他者から援助を受けながら IT を利用している」を 4 と逆転させた順序尺度を変数として投入した。そのため、B の結果がプラスであることから習熟度が高い方が被害に合いやすいということになる。

[23] 注 5 参照

[24] 注 3 参照

[25] 法務総合研究所研究部報告 49 14 頁

[26] 警視庁の統計平成 28 年第 56 表脚注
http://www.keishicho.metro.tokyo.jp/about_mpd/jokyo_tokei/tokei/k_tokei28.files/ktd056.pdf (平成 29 年 9 月 15 日参照)

[27] 平成 10 年頃から検挙件数のみを用いるようになっている。それ以前は、認知、検挙両方を用いていたがその差はほとんどなかった。ちなみに、平成 9 年の認知件数は 263 件、検挙件数は 262 件である。

[28] http://www.crimesurvey.co.uk/AboutTheSurvey.html （平成 29 年 9 月 15 日参照）

[29] https://www.jpcert.or.jp/（平成 29 年 9 月 15 日参照）

[30] http://www.tokumei24.jp/gaiyo.html（平成 29 年 9 月 15 日参照）

[31] CSEW と警察統計を比較したところ警察への申告率は 10 件中 4 件と記載。
http://www.crimesurvey.co.uk/AboutTheSurvey.html （平成 29 年 9 月 25 日参照）

[32] 財布を紛失したなどの理由で交通費等小額の金銭を他人から騙し取ること。

参考文献

Doyle, Charles ‘Cybercrime: An overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal laws” Congressional research Service （2014）

Goodman,Mark “Future Crime” 松浦俊介訳 青土社（2016）

岡部正勝「サイバー空間における危機管理」『現代危機管理論 現代の危機の諸相と対策』立花書房（2017）

岡部正勝「サイバー犯罪の捜査と課題」刑事法ジャーナル Vol.51 成文堂（2017）

金山泰介「サイバー犯罪被害実態調査（第 1 回）の結果」危機管理学研究創刊号 101-111 頁（2017）

金山泰介「刑法犯の減少と犯罪の転移」早稲田大学社会安全政策研究所紀要第 8 巻 17-41 頁（2016）

法務総合研究所研究部報告 41「第 3 回犯罪被害実態（暗数）調査」（2008）
http://www.moj.go.jp/housouken/housouken03_00011.html(平成 29 年 9 月 15 日参照)

法務総合研究所研究部報告 49「犯罪被害に関する総合的研究 - 安全・安心な社会づくりのための基礎調査結果（第 4 回犯罪被害者実態（暗数）調査結果） - 」（2012）
http://www.moj.go.jp/housouken/housouken03_00066.html(平成 29 年 9 月 15 日参照)