

# サイバーセキュリティに関する警察の施策と 大学生によるサイバー防犯ボランティア活動

岡部 正勝

慶應義塾大学総合政策学部教授  
(前 警察庁長官官房参事官 (サイバーセキュリティ担当))

## 1. はじめに

### (1) サイバー空間をめぐる脅威の状況

警察庁が公表している「平成26年中のサイバー空間の脅威をめぐる情勢」<sup>(1)</sup>等の公表資料によれば、サイバー犯罪<sup>(2)</sup>の検挙件数は、平成26年は若干減少したものの、過去10年のスパンでみると4倍近くに増加している(その一方で、刑法犯の検挙件数は過去10年で4割以上減少しており、リアル空間に比べ、サイバー空間の治安が悪化している状況がうかがえる。)。また、都道府県警察の相談窓口で受理したサイバー犯罪に関する相談件数は、11万8,100件と前年より3万3,237件(39.2%)増加し、過去最高の件数を記録した。検挙件数や相談件数の内訳をみると、詐欺関連と、児童ポルノ等のわいせつ画像関連が多く、こうした情報がネット上にあふれている実態がうかがえる。また、後述のウイルス無力化作戦と関連するが、インターネットバンキング不正送金の被害額が、26年は前年比約2倍となる約29億円で過去最高となっている。

サイバー攻撃<sup>(3)</sup>関連では、平成26年は、我が国の事業者等からの情報窃取を企図したとみられるサイバー攻撃が大幅に増加した。26年中に警察が把握した標的型メール攻撃は、前年比約3.5倍となる1,723件となっている。平成27年に入っても、日本年金機構の事案をはじめ、サイバー攻撃による情報流出事案が相次いでいるところである。

また、警察庁では、インターネットとの接続点に設置したセンサーに対する不審アクセス件数を観測しているが、平成26年中は、1日・1IPアドレス当たり

491.6件(前年比+181.5件、+58.5%)とこれも大幅な増加を示している。

### (2) 青少年をめぐるインターネット環境の変化

青少年をめぐるインターネット環境については、これまでに国民的規模で進んできたインターネット普及に加え、ここ数年のスマートフォンの低年齢層への急激な普及<sup>(4)</sup>により、いわゆる「携帯」の時代とは状況が大きく変わってきており、これに見合った新たなリテラシー教育、情報モラル教育の必要性が増しているものと思われる。

そこで、本稿においては、まず、筆者の前職における経験等に基づき、警察におけるサイバーセキュリティに関する施策を概観する。次に、青少年に対するリテラシー教育の実践という観点から、大学教員という立場で筆者が主宰している研究会における、サイバー防犯ボランティア活動の概要を紹介することとしたい。

## 2. 警察の施策と課題

先に述べたとおり、サイバー犯罪の検挙件数は増加しているが、サイバー空間にあふれる違法行為に比べれば、検挙は氷山の一角でしかないというのが実情である<sup>(5)</sup>。検挙が困難な理由としては、匿名性が高く実行者の特定が困難であること、PCの感染等の被害が潜在しやすいこと、犯罪行為が容易に国境を越えるため、国際的な捜査協力という実務上の困難があることが挙げられる。

(1) [https://www.npa.go.jp/kanbou/cybersecurity/H26\\_jousei.pdf](https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf) (平成27年7月23日)

(2) 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をいう。

(3) サイバー攻撃は、要インフラの基幹システムを機能不全に陥れ、社会機能を麻痺させる電子的攻撃であるサイバーテロと、情報通信技術を用いた課(ちょう)報活動であるサイバーインテリジェンスとに分けられる。

(4) 例えば、内閣府に置かれた有識者会議である青少年インターネット環境の整備等に関する検討会が公表した「青少年インターネット環境の整備等に関する検討会報告書」(平成27年5月12日)によれば、高校生の携帯電話・スマートフォンの利用率は平成26年で95.2%となっており、うち、スマートフォンの占める割合は、ここ5年間で3.9%から94.3%に急増している。

(5) 通常の警察の統計は、「認知」件数と検挙件数を比較して検挙率を算出し、警察活動の効果のひとつの指標としているが、サイバー犯罪の場合は、そもそも違法行為の数が膨大である上に、認知件数を計測することが技術的に困難である。

そこで、警察としても、サイバー犯罪・サイバー攻撃の予防のために様々な施策を行っているが、本稿では、それらの中から、マルウェアに感染したPCを無力化する作戦、違法有害情報の通報を受けて削除する仕組みの構築、国際的な捜査協力の課題を取り上げ、簡単に紹介することとしたい。

### (1) マルウェアに感染したPCの無力化作戦

これまでに、2つの事例がある。ひとつめは、FBI、ユーロポール等との協力により行った「Game Over Zeus(GOZ)」というマルウェアのテイクダウン作戦というものである<sup>(6)</sup>。GOZは、インターネットバンキングに係る不正送金事犯に使用されているとみられる不正プログラムであるが、全世界で50万台から100万台のPCが感染し、うち約20%が日本にあるものと推定されている。そこで、日本を含む各協力国の法執行機関が連携し、当該不正プログラムのネットワークを崩壊させる(ボットネットのテイクダウン)作戦を実行している。この作戦においては、関連サーバを押収し、当該ネットワークの管理者を起訴するとともに、より多くの感染端末を特定し、プロバイダ等を通じて感染端末の利用者に対して不正プログラムの駆除を促すことにより、感染端末を減少させることとしている。

いまひとつは、本年に入り、警視庁が行っている「ネットバンキングウイルス無力化作戦」というものである。技術的な詳細は公表されていないが、PCに感染してインターネットバンキングの不正送金を指示する新型ウイルスと海外の指令サーバを突き止め、国内外の8万2千台のウイルスの無力化を始めたと発表されている<sup>(7)</sup>。一部報道によれば<sup>(8)</sup>、「警視庁が指令サーバになりかわり、同庁の監視コンピュータから感染PCに接続、セキュリティ会社「セキュアブレイン」(東京)と共同開発したプログラムを「解毒剤」として働かせ、ウイルスを無力化しており、この手法は今後新たに現れるウイルスにも応用できるとみている」という。この報道が事実とすれば、捜査機関が直接指令サーバを「乗っ取り」、ウイルスを無力化するという点で、これまでにない新しい手法であり、積極的な犯罪対策の好事例といえよう。

### (2) 違法有害情報対策

インターネットに接続すれば、誹謗中傷、児童ポル

ノ、わいせつ画像などが氾濫していることは周知の事実であるが、こうした違法・有害情報対策のひとつとして、インターネット・ホットラインセンタ(IHC)による通報受理・削除要請という制度がある<sup>(9)</sup>。平成26年にIHCが受理した通報件数は150,352件(前年比+19,632件)と大幅に増加しており、うち違法情報は35,013件(+4,642件)、有害情報は3,874件(+446件)であった。警察への通報件数は17,189件、IHCからサイト管理者等に対して削除を依頼した違法情報8,303件のうち、7,890件が削除され、削除率95.0%となっている。この制度は、公が直接コンテンツを削除することができないという制約の下、事業者の自主的措置を前提として、表現の自由と、ネット空間の安全や被害者救済とのバランスを図ったものであるが、削除に応じない悪質業者の存在など、課題も多い。

### (3) 国際的な捜査協力

サイバー犯罪・サイバー攻撃は、容易に国境を越えるものであるため、事後的な追跡においては、国際的な協力が必須である。サイバー攻撃の発信地が外国であった場合には、その国の当局に、発信されたPCの所有者、使用者情報などを照会しなければならない。また、違法情報が海外サーバに蔵置されている場合、違法情報自体を我が国でダウンロードして証拠化することは可能であるが、サーバ設置者等に関する情報は外国当局に協力を要請せざるを得ない。しかし、国際的な照会には時間を要することが多く、その間にログ等の情報が消滅する可能性があるほか、そもそも照会にはほとんど回答をしない国も存在する。

この点では、各国との信頼関係構築が重要であるが、そもそも、国際的なサイバー犯罪捜査においては、何を犯罪とするのか、どのような捜査手法を各国が採り得るのか、といった点につき、グローバルスタンダードがなければうまく機能しない。これについては、EUのイニシアチブで、既にサイバー犯罪条約(ブダペスト条約)というものが存在するが<sup>(10)</sup>、批准している国は、欧州諸国、米国、日本等に限られており、アジアでは日本しか批准していない。

サイバー空間をめぐる国際的な秩序の形成については、既存の国際法を適用するべきという日米欧と、新たな枠組みを作るべきという中露の立場が大きく対立し、IT途上国のうち独裁的国家や宗教的国家の多く

(6) <https://www.npa.go.jp/cyber/goz/> (平成27年7月24日)

(7) <http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku504.htm> (平成27年7月24日)

(8) [http://www.nikkei.com/article/DGXLASDG09HA2\\_Q5A410C1MM0000/](http://www.nikkei.com/article/DGXLASDG09HA2_Q5A410C1MM0000/) (平成27年7月24日)

(9) 平成26年中のIHC運用状況につき、<https://www.npa.go.jp/cyber/statics/h26/pdf03-2.pdf#search=%E8%AD%A6%E5%AF%9F%E5%BA%81+IHC> (平成27年7月24日)

(10) [http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159\\_4.html](http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html) (平成27年7月24日)

は、中露の立場に近いものとみられている。この背景として、中露等には、政治的表現を含むコンテンツ規制を強化したいとの真意があるとみられており、合意への道は遠いだろう。

### 3. 慶應義塾大学SFCサイバー防犯ボランティア研究会<sup>(11)</sup>による実践活動

慶應義塾大学総合政策学部には、官学の人事交流の一環として、警察庁から現役の職員が出向し<sup>(12)</sup>、社会安全に関する講義等を行っている。これに加え、2年前(筆者の前任者の在任中)から<sup>(13)</sup>、研究会活動の一環として、小中高の児童生徒に対するサイバー防犯ボランティアの実践活動を行っている。これまで、既に十数校における活動実績があり、概ね好評で、報道にも取り上げられた<sup>(14)</sup>。

当該実践活動は、児童生徒と同じデジタル・ネイティブ世代の大学生たちが、児童生徒に近い目線で、同じ言葉遣い<sup>(15)</sup>も用いて語りかけるために、児童生徒も真

剣に耳を傾けており、グループワークを行う場合にも積極的な参加がみられる。これに加え、最近では、筆者単独あるいは筆者と学生による保護者対象の講演を実施する例があり、児童生徒に対する啓発活動と相俟って、適切なペアレンタル・コントロールに貢献しているものと自負している。

---

(11) 研究会ホームページ <http://cyberlab.sfc.keio.ac.jp/>

(12) 警察庁からの出向者は、筆者で5代目となる。

(13) 活動開始の趣旨や当初の状況については、四方光『サイバー犯罪対策概論』(立花書房、平成26年)150頁以下参照。

(14) 平成27年6月5日付け毎日新聞(神奈川版)「スマホ利用注意 慶大生ら20人がサイバー教室」、同日付け神奈川新聞「ネットの注意点大学生から学ぶ」等。

(15) 例えば、LINEの使用における「既読無視(スルー)」、「未読無視」といった用語や、SNSやYouTubeの機能に関する知識の豊富さも、児童生徒の心を惹きつけることに役立っているようである。