警察常任委員会

平成 29 年度特定テーマに関する調査研究報告書

１　テーマ

サイバーセキュリティ対策について

２　調査・研究の内容

（１）　当局の取組

ア　サイバー攻撃対策について

〇開　催　日　平成２９年１０月２６日
〇場　　所　第６委員会室
〇報　告　者　塩井　　学　公安第一課管理官
〇主な報告等

① 官民連携の強化

・情報セキュリティに関する専門的な知識を有する研究者や技術者を「兵庫県警察サイバーセキュリティ対策アドバイザー」として委嘱
・高度な情報技術を保有する民間企業への警察官の派遣
・神戸大学との共同研究によるサイバー攻撃等検知システムの開発

② サイバー攻撃事件捜査による実態解明

・攻撃者(被疑者)及び発信元(ＩＰアドレス)の特定
・攻撃手口の解明
・攻撃手口の情報共有等の未然防止対策の推進

〇主な意見・提案等

・高齢者を含めたパソコン利用者に向けた水際対策としての、パソコン販売事業者等に店頭で啓発チラシ・リーフレットを配付してもらうような対策について

イ　サイバーセキュリティ戦略について

〇開　催　日　平成２９年１１月１７日
〇場　　所　第４委員会室
〇報　告　者　寺内　克元　サイバー犯罪対策課調査官
〇主な報告等

① サイバーセキュリティセンターの取組

・サイバー空間の脅威への対処能力の全体的な底上げ
・サイバー空間の脅威への対処能力と情報通信技術に係る知識等を備えた捜査員の育成
・民間の専門的知識、技能等の活用

② サイバー犯罪防犯センターの取組

・サイバー空間の脅威に対する兵庫県官民合同対策プロジェクト
・専従の警察官によるサイバー犯罪被害防止教室の開催

・企業対象の情報セキュリティセミナーの開催
・サイバー犯罪防犯センター専用ＨＰ等による広報・啓発
・サイバー防犯ボランティアの活動（違法情報・有害情報の通報、講演活動等）

③　検挙対策

・専従体制によるサイバー犯罪相談窓口の運用
・高度な知識を持つ捜査員で編成した初動捜査班の運用

○主な意見・提案等

・サイバー犯罪被害防止教室における警察独自の強みの周知の必要性について

ウ　サイバーセキュリティ対策の推進について（閉会中の継続調査事件）

○開　催　日　平成３０年１月１８日
○場　　所　第３委員会室
○報　告　者　有田　幸司　生活安全部長
齋賀　隆史　警備部長

○主な報告等

①　サイバー空間の脅威に対する警察の対処能力の強化

・兵庫県警察サイバーセキュリティ対策委員会の設置等によるサイバーセキュリティ対策の体制強化
・サイバー犯罪捜査検定や各種教養の実施による対処能力の全体的な底上げ
・サイバー捜査官・解析官の育成
・産官学の専門的知識・技能の活用

②　サイバー犯罪に対する検挙・抑止対策の推進

・サイバー犯罪対策課における相談窓口及び初動捜査班の運用
・インターネット・ホットラインセンターによる違法情報や有害情報の提供
・全国協働捜査方式による取締りの推進
・インターネットバンキングに係る不正送金事犯の取締りの推進
・サイバー防犯標語「あひルのおやコ」の策定等による青少年の適切なインターネット利用に関する取組の推進
・さまざま世代を対象としたサイバー犯罪被害防止教室の開催
・ホームページやフェイスブック等を活用した情報発信
・サイバー防犯ボランティアの活用

③　サイバー攻撃対策の推進

・サイバー攻撃特別捜査隊の設置
・サイバー攻撃の標的となるおそれのある重要インフラ事業者との連携
・兵庫県サイバー攻撃情報共有ネットワークを通じた情報共有
・情報窃取の標的となるおそれのある事業者等に対する注意喚起
・県内事業者等を対象としたサイバー攻撃対処セミナーの開催
・全国初の官学共同研究・開発によるサイバー攻撃等検知システムの運用
・サイバー攻撃を受けたコンピュータの解析による攻撃者及び手口の実態解明

○主な意見・提案等

・公衆無線ＬＡＮの利用者側に対する啓発活動の推進について

（２）　事例調査

ア　日本サイバー犯罪対策センター（ＪＣ３）の取組・調査結果

〇日　時　平成２９年８月３０日

〇主な取組及び調査内容

・インターネットバンキングの不正送金等、金融に関するサイバー犯罪被害状況を集約して犯罪手口の分析を行うとともに、攻撃者のプロファイリング等を通じた実効性のある金融犯罪対策を検討している。
・情報窃取型のサイバー攻撃の最新状況を分析し、サイバー攻撃の手法や対策について検討している。
・詐欺サイト被害等、ｅコマース事業を展開する企業を狙うサイバー犯罪に関する最新の情報を入手し、対策を検討している。
・マルウェアの通信先調査等の解析を行うことで、マルウェアの挙動を把握している。
・サイバー空間上の脅威情報を収集・蓄積し、脅威動向を分析している。
・米国ＮＣＦＴＡ、英国ＣＤＡ、国際刑事警察機構（インターポール）等の海外関係機関との間で、諸外国において流行が見られるマルウェアやサイバー犯罪の手口、実効性のあった対策等の情報共有を行っている。
・インターネットバンキングにおける不正送金の被害者は個人が多いが、法人が被害に遭うこともある。
・ランサムウェアによる被害では、ファイル等が勝手に暗号化され、暗号の解除を盾に金銭の要求をしてくるケースが多い。
・ランサムウェアの脅威としては、人間心理を利用するなど、ノウハウのつまった手法による攻撃がある。
・主に企業向けのサイバー攻撃として、ビジネスメール詐欺では、ＣＥＯ等のスケジュールを把握した上で（海外への出張中で電話がつながらないタイミング等）なりすまし、経理担当者へ至急送金するよう指示メールを送る手口もある。
・近年は、ストーカー規制法等の新しい法律による検挙が多い。
・昔の標的型メール等による外国からのサイバー攻撃では、日本語の文法がおかしいものが多かったため比較的見分けがつきやすかったが、現在は日本語の文法もまともなものが多いため、日本語を用いた標的型メールを用いたサイバー攻撃も多くなっている。
・ＪＣ３では、文面やファイル名を見ただけで標的型メールかどうかの判断ができるが、最近の手口では既存のウェブサイトを改ざんし、アクセスするだけでウイルス感染させるものもあるため、ＪＣ３がこういったサイバー空間上の犯罪インフラを発見し、警察が摘発している。
・不正送金事案において、暴力団が出し子等で関わっている可能性もあるが、不正プログラムをつくる主体は暴力団ではなく、外国の犯罪グループであると考えている。
・犯行グループも絶対にミスをしない訳ではなく、決まった時間に定期的に大量のデータを送りつけるなど、何かしらの形跡を残すことがあるので、そういったものを発見することで、犯人の特定や逮捕につながることもある。

〇主な意見

・サイバー犯罪と暴力団との関わりについて
・サイバー攻撃対策としての「おとり捜査」について
・ウイルス感染等を発見するための対策について
・犯行グループの特定や逮捕につながった事例について

イ　ＮＥＣの取組・調査結果

〇日　時　平成２９年８月３１日

〇主な取組及び調査内容

（サイバー攻撃の最新動向とＮＥＣの攻撃対策）

・サイバー攻撃の動機としては、情報窃取や操作妨害によって金銭を得るビジネスモデルの成立や、社会インフラ、重要インフラの国際的なＩＴ化に伴うセキュリティの政治利用の横行などが考えられる。

・これまでのサイバー攻撃は、個人の愉快犯によるものが主流であったが、現在は標的型攻撃メールをはじめとした巧妙化する攻撃や、プロのサイバー犯罪集団・国家組織による高度な攻撃が増えている。

・いまやサイバー空間の脅威は「海底から宇宙まで」といわれており、ＩＣＴを活用した社会基盤の全てがサイバー犯罪の対象領域となっている。

・サイバー攻撃は巧妙化しており、サイバー攻撃を行うためのパソコンを作る会社やそのパソコンをメンテナンスする会社など、ビジネス化あるいは分業化している状況にある。

・平成 27 年に経済産業省による「サイバーセキュリティ経営ガイドライン」が発表され、現在国内の民間企業において、このガイドラインを指針の参考としてセキュリティ対策を行っている。

・企業にとって、サイバーセキュリティは経営に直結する問題（例：ベネッセや日本年金機構における個人情報漏洩に伴う多額の損害賠償など）である。

・サイバーセキュリティ対策においては、まずウイルス対策ソフト等の機器を導入するのではなく、ＣＩＳＯといった情報管理の責任者を配置し、ＣＳＩＲＴ（いわゆるセキュリティ被害が発生した際に対応するチーム）をつくるなど、体制を整えた上で、何層もの防御対策を重ねる必要がある。

・ＮＥＣでは、未知マルウェア検知等の入口対策、外部不正通信検知等の出口対策を講じているほか、社内コミュニティや勉強会、ＣＴＦ（優秀な人材同士で争い互いの能力を高め合う手法）等を通じた技術者の育成や外部機関（ＩＰＡ、警察庁等）との連携による情報共有を図っている。

（官民連携したサイバー犯罪・攻撃対策）

・サイバーセキュリティ対策においては、官民の人的交流等により、互いの課題や取組をしっかりと共有する必要がある。

・民間企業は、犯罪グループからのサイバー攻撃から身を守るためにセキュリティを強化する。一方で警察は、サイバー犯罪の脅威の大もとに対して捜査や対策を行うという役割を果たしている。官民がこうした互いの強みを生かしながら連携をしていくことが重要である。

・サイバー犯罪・サイバー攻撃に対する官民連携においては、被害情報の共有や関連情報の分析が行える産業界、サイバー犯罪関連の専門的知見を有する学術機関、捜査等の権限を迅速に行使できる警察の３者の連携の中心で、ＪＣ３（日本サイバー犯罪対策センター）が役割を担っている。

・具体的に官民が直面するサイバー空間の主要な脅威としては、「ボットネット」「ランサムウェア」「ダークウェブ」「ビットコイン」などが挙げられるが、そのうち「ボットネット」は、さまざまなサイバー攻撃・サイバー犯罪の裏に潜んでおり、諸外国ではサイバーセキュリティ対策といえばボットネット対策と言われるほど、危険視されている。

・日本においては、犯罪者を特定するための先制的な捜査手法が限られたり、合法的に捜査に踏み切る法制度上の根拠がないケースがある。
・官民連携の中で、各主体が行うべきサイバー脅威への対策としては、インターネット運用者における顧客・インフラ保護対策、セキュリティ研究者やセキュリティ産業における脅威の研究と把握、政府や法執行機関における適切かつ迅速な捜査・被害防止が必要とされる。これらに加えて、インターネットユーザーのセキュリティ意識の向上が必要不可欠である。

〇主な意見

・官公庁との人事交流について
・同業他社との連携による事業への影響の有無について
・法制度上の困難について
・日本をサイバー攻撃の対象としている諸外国について

ウ　神戸大学大学院工学研究科森井教授及び研究生との意見交換会結果

〇日　時　平成２９年１１月２１日

〇主な調査内容

・サイバー攻撃の事例としては、丸川元大臣ＨＰの改ざんや日本年金機構の個人情報漏洩事件などがある。
・ランサムウェア等のサイバー攻撃は、ウイルス対策ソフトでは防ぎきれない。
・現在日本はマルウェア流行国であり、世界では減少傾向にあるのに対し、日本は増加傾向にある。
・マルウェアは被害に気づかないケースが多く、委員の中にも既に感染してしまっている可能性が高い。
・サイバー攻撃等検知システムは、約 150 事業者のウェブサイトを 24 時間巡回し、異常があれば警察が対応する、いわばお巡りさんのパトロールである。
・兵庫県を含む関西圏において実施した、大阪商工会議所とのアンケート調査によると、多数の企業がランサムウェア等の被害を受けており、そもそも被害に気づいていない企業も存在している。
・サイバーセキュリティには人材や経費の問題があるため、なかなか進展がない状態である。
・日本人はまじめなのでだましやすいことが、世界的に認知されることでサイバー攻撃の標的にされやすい状況になっている。

〇主な意見

・サイバー攻撃の対象となる企業の業種別について
・世界的に見た日本のサイバー攻撃対策について
・県民のサイバーセキュリティ意識向上に向けた対策について
・安全なスマートフォンの利用方法について
・ウイルス感染の危険性があるアプリについて
・サイバー攻撃等検知システムで把握しているサイトの中での実際のウイルス感染被害について
・中小企業に向けた検知システムの拡充について

３　今後の方向性について（委員間討議の結果）

警察常任委員会では、深刻化するサイバー空間の脅威に対するサイバーセキュリティ対策について、当局からの現状報告・取組状況、管内・管外調査における調査や関係者との意見交換等を行い、これらの調査結果から、委員間で討議を行った。

兵庫県警では、サイバーセキュリティ対策のうち、サイバー犯罪対策を生活安全部が、サイバー攻撃対策を警備部がそれぞれ両輪で行っていることを踏まえ、サイバー犯罪対策（生活安全部門）」「サイバー攻撃対策（警備部門）」の２つの観点から、今後の方向性として以下のとおり提案する。

（１）サイバー犯罪対策の推進（生活安全部門）

インターネットの普及が進む中、警察に寄せられるサイバー犯罪に関する相談が年々増加傾向にあり、中でも実在する正規サイトを模した偽サイト等を利用し商品代金を騙し取る詐欺事案や、他人のＩＤ・パスワードを不正に取得し本来の利用者になりすましてサービスを悪用する不正アクセス事案など、県民生活の身近なところでの犯罪が発生しており、相談が多く寄せられている。

本県におけるサイバー犯罪検挙件数の約９割を占めるネットワーク利用犯罪では、詐欺や児童買春・児童ポルノ、青少年愛護条例違反など、少年が被害者となる事件が多い。また、インターネット掲示板で向精神薬（睡眠薬）の譲渡を求めた麻薬特例法違反事件や､平成 25 年から急増しているインターネットバンキングに係る不正送金事犯など、さまざまなサイバー犯罪が発生している。

こうした本県の情勢を踏まえ、今後のサイバー犯罪対策における課題として、以下２点挙げさせていただく。

ア　インターネット利用者への周知・啓発

ネットワークを利用した犯罪は、利用者のサイバーセキュリティ意識の高揚や事前の対策を講じることで多くの被害を防止することができる。そのためには、インターネット利用者へのサイバー犯罪情勢や最近手口の周知のほか、被害に遭わないためにどのような点に注意するべきか、どのような対策を講じるべきかをいかに警察から情報発信するかが課題である。また、近年のインターネット利用者の低年齢化に伴い、青少年に向けた周知・啓発活動を更に促進すべきである。

（主な提案）

・犯罪手口等の最新情報のメールでの配信
・マスメディアと連携した広報啓発活動の推進
・パソコンやスマートフォン販売事業者の店頭における啓発チラシ等の配付
・地域住民へのサイバー防犯講習等の更なる実施
・教育現場と連携したインターネット利用に関する講習の実施

イ　多様化するサイバー犯罪への体制整備

年々増加するサイバー犯罪に的確に対応するためには、サイバー対策課に設置されている相談窓口の充実やサイバー犯罪に関する高度な知識を有する捜査員の養成など、警察の捜査体制の整備を行う必要がある。また、児童ポルノ画像や覚せい剤等規制薬物の販売に関する情報など、インターネット上に掲載すること自体が違法となる事案や、インターネットバンキングに係る不正送金事犯など、都道府県警察の管轄が判別しにくいサイバー犯罪を取り締まるためには、都道府県を越えた取組が必要不可欠で

ある。

（主な提案）

・インターネット掲示板の運営事業者に対する周知

・相談窓口の対応時間の見直し

（２）サイバー攻撃対策の推進（警備部門）

情報通信技術が浸透した現代社会においては、生活に不可欠な電力、ガス、水道等の重要インフラも情報システムによって支えられており、いまや「海底から宇宙まで」ＩＣＴを活用した社会基盤のすべてがサイバー攻撃の対象領域となっている。これらの要因としては、情報窃取や操作妨害によって金銭を得るビジネスモデルの成立や国際的なＩＴ化に伴うセキュリティの政治利用の横行などが考えられる。

サイバー攻撃は、重要インフラの基幹システムに対する電子的な攻撃である「サイバーテロ」と情報通信技術を用いた諜報活動である「サイバーインテリジェンス」に分類される。国内におけるサイバーテロの発生はないが、サイバーインテリジェンスの事例としては、三菱重工に対する情報窃取を目的とした標的型メール攻撃や、日本年金機構に対する個人情報の窃取を目的とした標的型メール攻撃などが発生している。近年のサイバー攻撃の動向としては、個人の愉快犯によるもの以外に、プロのサイバー犯罪集団・国家組織による高度なものが増えている。

また、本県においても、遠隔操作が可能な不正プログラムを作成するための不正プログラムを保管していた県内の高校生をウイルス保管罪で検挙した事例があり、今後もサイバー攻撃の発生の可能性は否めないことから、被害の未然防止、攻撃手口の徹底した分析が求められる。

こうしたサイバー攻撃への対策を講じていく上で、以下の２つの課題を挙げさせていただく。

ア　サイバー攻撃被害の未然防止

サイバー攻撃対策としては、被害の未然防止が大前提であり、発生してからでは遅い。被害の未然防止においては、被害情報の共有や関連情報が行える産業界、サイバー犯罪関連の専門的知識を有する学術機関、捜査等の権限を迅速に行使できる警察の３者と、ＪＣ３（日本サイバー犯罪対策センター）がそれぞれ互いの強みを生かしながら連携を図る必要がある。特に、サイバー攻撃の対象とされやすい重要インフラ事業者や先端科学技術事業者等との情報共有を行うなど連携を図るほか、県内事業者に対する最新のサイバー攻撃に関する情勢説明やセキュリティ対策についての講習を行うなど、事業者のサイバー攻撃被害の未然防止が課題である。

また、全国初の官学共同研究・開発によるサイバー攻撃等検知システムを活用し、引き続き県内の重要インフラ事業者が構築するウェブサイトを監視し、サイバー攻撃の早期発見に努める必要がある。

（主な提案）

・サイバー攻撃の対象となりやすい企業の顧客に向けた注意喚起

・マスメディアとの連携による攻撃手法の周知

・中小企業を対象としたサイバーセキュリティ対策の講習会の実施

・サイバー攻撃等検知システムの監視対象事業者の拡大

イ　サイバー攻撃対処能力の更なる向上

現在、兵庫県警においては、兵庫県警察サイバーセキュリティ対策委員会のほか、

本部と警察署にサイバー犯罪対策のプロジェクトを設置するなど、サイバーセキュリティ対策の体制強化を図っているが、日進月歩のサイバー攻撃に対処するためには、更なる対処能力の底上げが求められる。特に、専門性の高いサイバー攻撃の対処のためには、「情報処理区分」の採用枠を拡大など、ＩＴ関連企業での勤務経験や情報処理技術に関する資格を有する人材を積極的に登用することが効果的であると考えられる。

（主な提案）

・サイバー攻撃の捜査に特化した専従捜査機関の設置
・海外の捜査機関との連携の強化
・ホワイトハッカー等の外部人材の登用
・民間事業者との更なる人事交流の推進
・捜査資機材整備のための更なる予算確保