令和５年度 警察常任委員会
特定テーマ調査研究報告書

１　テーマ

「サイバー犯罪防止対策について」

＜テーマ選定の理由＞

スマートフォンなどのＩＴ機器が人々の日常生活と密接不可分の関係になるなどのＩＴ化の進展に伴い、生活に身近なサービスを介し、サイバー犯罪の被害に遭うケースが後をたたない状況が続いている。この状況の打開に向けて、子供から大人、高齢者にいたるまでのあらゆる年齢層の方々に、真に正しいインターネットの使い方や防犯知識を身に付けてもらう必要があるため、県警察の取組みについて調査研究する。

２　調査・研究の内容

(1)　当局の取組

ア　「サイバー犯罪防止対策について～警察庁と都道府県警察との連携した取組～」

〇開催日　令和５年 10 月 25 日

〇場　所　中会議室

〇報告者　左山サイバー企画課長

〇主な報告等

①　サイバー事案の特徴

②　サイバー捜査の困難性

③　警察庁と都道府県警察との連携した取組

〇主な意見等

・特定有害情報の区分について

・サイバーパトロールセンター等の詳細について

・一般の警察官に対するサイバー分野の人材育成について

・サイバー対策における公安部門の役割について

・サイバー空間における違法情報の増減傾向について

・サイバー犯罪に対する検挙方針について

・外国法制との相違等によるサイバー犯罪取締の制約について　等

イ　「サイバーセキュリティ対策の推進について」

〇開催日　令和５年 10 月 25 日

〇場　所　中会議室

〇報告者　野口サイバーセンター長

〇主な報告等

① サイバー空間をめぐる脅威の情勢
② サイバー空間の脅威に対する警察の対処体制等
③ サイバー空間の脅威に対する警察の取組
④ 全国警察が協働した取組
⑤ 実態把握と部門間連携の推進
⑥ 官民連携の推進
⑦ 広報啓発活動の推進
⑧ サイバー攻撃対策

〇主な意見等

・サイバー攻撃被害の暗数について
・ＳＮＳのプラットフォーマーに対する有害、違法情報の削除要請について
・ＳＮＳのプラットフォーマーの協力状況について
・特別採用のサイバー捜索区分に対する処遇改善について
・警察当局が目指す高度人材のレベルと採用について
・有害情報に対するフィルタリングの促進について
・県民に対するサイバー攻撃の分かりやすい広報について
・専門人材である任期付警察官のあり方（採用方法・権限・期間等）について
・サイバー犯罪対策の初動支援及び技術支援を行う第二拠点のあり方について
・ＡＩを用いた違法情報等捜査の成果について　等

(2) 学識経験者等の意見聴取について

〇開催日　令和６年１月 16 日
〇場　所　第３委員会室
〇講　師　神戸大学大学院　工学研究科　森井 昌克 教授
〇講義内容「今後の警察行政が取り組むべきサイバー犯罪防止対策
～サイバー犯罪の現状、病院、中小企業、一般県民、生徒学生、
そして公共サービスに対して～」

〇主な意見等

・現場の一般警察官（特に中年層）に求めるサイバーの具体的知識について
・警察や自治体のセキュリティ対策の実情について
・「サイバーセキュリティお助け隊」について、民間企業の既存セキュリティサービスとの棲み分けと、全国や本県の導入状況・課題について
・自分がだまされると自覚できないＩＱ70 少し上の境界値の方々、高齢者等の社会的弱者に対する、サイバー詐欺等の被害防止策について
・サイバー詐欺等の犯人が行う現金化の手口、特に最近の傾向について
・サイバー捜査におけるおとり捜査の有効性と国の方針、導入しない理由について
・サイバー社会の新常識と、未成年のサイバー犯罪防止のための対策について　等

(3)　事例調査　～ 特定テーマに関する主なもの ～

ア　県民との意見交換（ソーシャルメディア研究会）

〇開催日　令和５年８月 29 日

〇場　所　兵庫県立大学姫路新在家キャンパス内

〇概　要　ソーシャルメディア研究会代表の竹内和雄教授、及び研究会メンバーより、子供とネット社会の現状と、研究会の取組について説明を受け、意見交換を行った。

イ　兵庫県警察本部サイバーセンター

〇開催日　令和５年 10 月 30 日（管内調査）

〇場　所　兵庫県警察本部内

〇概　要　県警察における今後のセキュリティ人材育成、警察庁等との連携による捜査の高度化・効率化について

〇主な意見等

・警察業務が多忙化・複雑化する中で、既存の警察職員全員にサイバー犯罪初級資格を求めることの妥当性について

・各警察署においてサイバー犯罪捜査を行うよりも、警察本部直轄化するべき（提案）について

・秘匿性の高いアプリ、国際犯罪のマネーロンダリングにおける都道府県警察の限界と警察庁の役割について

・県警察における復号化技術レベルについて

・任期付専門人材の採用状況、人材確保が難しい理由について

・サイバー犯罪捜査部門の今後の増員等の予定・必要性等について

・サイバー人材のスキル維持の取組について

・新規採用時にサイバー犯罪初級資格を要件とすること（提案）について　等

ウ　株式会社インターネットイニシアティブ

〇開催日　令和５年 11 月６日（管外調査）

〇場　所　社内会議室等

〇概　要　サイバーセキュリティ対策について（デジタルに依存する社会、サイバー犯罪の事例等について（オペレーションセンター見学含む））

〇主な意見等

・サプライチェーン上で大企業と取引する上で要求される情報セキュリティレベル、そしてそれに必要なコストについて

・セキュリティ対策人材を育成する傾向について（内部育成か外部招聘か）

・フィッシング詐欺防止のため、プロバイダー等において、ネットワーク上から詐欺サイトを遮断することの可能性について

・ネットワーク上で遮断することの国際合意について

・企業等のサイバーセキュリティ認証制度について

・サイバー犯罪者の人物像について

・企業グループにおけるセキュリティ部門の職員の特徴、給与水準、勤務態勢や在宅勤

務率、職場での使用言語、部門収益等について
・個人のセキュリティが甘い部分（特に位置情報等）について
・スマートフォンのセキュリティについて
・ハッカーを追い詰める、逆攻撃を事業化する可能性について　等

エ　グローバルセキュリティエキスパート株式会社

〇開催日　令和５年 11 月６日（管外調査）

〇場　所　社内会議室

〇概　要　中小・中堅企業へのサイバー犯罪防止対策について（2022 年の事故実例から学ぶ～サイバーセキュリティとはつまり防犯対策～）

〇主な意見等

・特殊詐欺が今後サイバー分野に移行する恐れがあり、個人への啓発活動について

オ　情報通信機構サイバーセキュリティ研究所（ＮＩＣＴ）

〇開催日　令和５年 11 月７日（管外調査）

〇場　所　研究所内会議室

〇概　要　最新の研究状況及び人材育成等について

〇主な意見等

・攻撃感知用の未使用アドレスの入手について
・攻撃元を逆襲する可能性について
・実践的サイバー防御研修（ＣＹＤＥＲ）で防衛が成功した事例について
・攻撃回避策としてのアドレス変更について
・外国製品や古い機種のセキュリティ面での穴について
・研究所の成果の民間への開放と対価徴収について
・自衛隊等との連携について
・攻撃情報サービスを自治体の半数が希望しない理由について、また自治体へのアラート情報以上のサポートを機構が行わない理由について
・青少年、若者が悪に流れない倫理対策について
・機構の予算の確保状況について　等

３　今後の方向性について

サイバー空間は、地域や老若男女を問わず、全県民が参加し、重要な社会経済が営まれる公共空間へと変貌を遂げ、あらゆる場面で実空間とサイバー空間が融合した社会の到来が実現しつつある。こうした中、県民の日常生活に不安を与えるサイバー犯罪や重要インフラ事業者及び先端技術を有する企業等へのサイバー攻撃等のサイバー関係事案が続発している。

警察常任委員会では、サイバー関係事案の取締りや被害の未然防止対策及び官民連携による総合的な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・取組状況の聴取、管内・管外調査における調査や県民や学識者との意見交換等を行った。

兵庫県警では、令和２年９月に、サイバー空間の脅威に対する対処の司令塔として、既存各部に属さない警察本部長直轄の所属であるサイバーセキュリティ・捜査高度化センターを新たに設置し、令和３年３月には生活安全部サイバー犯罪対策課を移管し、サイバー企画課及びサイバー捜査課を設置する等、体制の強化が行われている。

調査結果を踏まえた今後の方向性については、サイバーセキュリティ対策のうち 、サイバー犯罪対策はサイバー捜査課、サイバー攻撃対策は警備部サイバー攻撃対策隊、県警察全体のサイバーセキュリティ対策の企画・立案やサイバー人材の育成など司令塔の役割はサイバー企画課が、それぞれ担当していることを踏まえ、 サイバー犯罪対策 、サイバー攻撃対策、サイバーキュリテイ対策の３つの視点から提案する。

（１）サイバー犯罪対策について

サイバー空間の公共空間化が加速し、あらゆるサービスにインターネットが活用される一方で、インターネットが犯罪インフラとして様々な犯罪に利用されている。また、警察本部や警察署に寄せられるサイバー犯罪等に関する相談は高水準に推移しており、とりわけ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するフィッシング、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関係に関する相談が多く寄せられている。

特にフィッシング等に伴うインターネットバンキングに係る不正送金事犯の県下の発生件数は令和５年６月末時点で１２６件（＋１１４件)、被害額は約１億６，２００万円（＋約１億３００万円）と前年に比べ大幅に増加している。

また、本県におけるサイバー犯罪検挙件数の８割以上を占めるネットワーク利用犯罪では、詐欺やストーカー、脅迫、児童ポルノなど、高齢者や青少年などの社会的弱者が被害者となる事件が多い傾向がある。

（現状における課題・問題点）

・会社や個人レベルでのサイバー犯罪に対する認識がまだ低いレベルにあるので、どのようなリスクがあるのか、具体的な犯罪手口や被害の実態を今以上に広く周知し、啓発することが重要である。

・県民に対する、犯罪手口の公開の広報不足が課題であると思う。

・便利な生活を求めると、そこには必ず犯罪がつきまとう。ＩＴ機器等の利用者（所有者）本人が分からないうちに、悪質な知識を持ち巧みに侵入し、大きな被害をもたらす。
経済的、精神的な損失となる背景には、機器やシステムにおいて１００％のガードが出来ていない事や利用者側の意識や知識が十分高くないことが考えられる。利用者の年齢や必要な情報等をもとにした最低限の情報範囲内のみでの利用や規制が出来たらよいが、人により程度は様々であり、情報の分類や切り分けなどの判別ができない課題がある。

（今後の方向性と期待される将来像）

・次々と新たな手口で迫ってきているにも関わらず、あまりにその手口に対し無知であるため、細やかで徹底した手口などの広報（ＳＮＳでのシュートビデオ等）と教育の強化を求める。

・サイバーパトロールでの「職務質問」の強化を図る必要がある。

・オンライン警告については、警告対象が限定されすぎており、投資詐欺等はカバーされていない。取締対象をさらに拡大する必要がある。

・日本で多大な収益を上げているＧＡＦＡＭを中心としたＳＮＳ等のプラットフォーマーに対して、投資詐欺等のサイバー犯罪対策に対し、コストを払って、しっかりと対策をするべきということを警察庁と一緒になって、対応を求めていく必要がある。

・インターネット等を利用した覚醒剤等の販売など、悪質化・巧妙化する薬物事犯の徹底検検挙を行う必要がある

・覚醒剤や大麻等の薬物乱用防止対策について、摘発、取締りを強化するとともに、ネット上の取引など密売・購入手法について潜在化・巧妙化が進行していることから、サイバーパトロールの推進など監視体制を強化する必要がある。

・サイバー犯罪の被害未然防止のためのセミナーや広報啓発等の取組みを推進する必要がある。

・サイバー犯罪に的確に対応できるよう、サイバー犯罪の取締り能力を強化するとともに、ランサムウェア、フィッシング、不正アクセス、有料サイトの料金請求やインターネット上の誹謗中傷など典型的なサイバー犯罪事例の内容や対策について広報啓発活動を強化する必要がある。

・県民に対して世代別に犯罪事例の周知、対策の広報の推進を国の「サイバーセキュリティ月間」を活用する等、意識を高めることが喫緊の課題である。

（２）サイバー攻撃対策

サイバー攻撃とは、生活に欠かせない重要インフラ（情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油の各分野における社会基盤）の基幹システムに重大な障害を引き起こす電子的攻撃である「サイバーテロ」と情報通信技術を用いた諜報活動である「サイバーインテリジェンス」に分類され、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おり、被害の未然防止、攻撃手口の徹底した分析が求められている。

サイバー攻撃対策は、被害の未然防止が大前提であり、発生してからでは遅い。ランサムウェアによる暗号化による恐喝などの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っている。

（現状における課題・問題点）

・公安等警察組織の権限により情報セキュリティが確保できることが前提となるが、国によって情報統制の考えが違い、規制する側の態度が異なるため困難である。

・現状把握と分析だけに終わっているのではないか。

（今後の方向性と期待される将来像）

・具体的に企業の規模や扱う情報の種別等に応じた対策のモデルや認証制度を具体的に示し、対策の行動に繋げていく取り組みを強化する。

・犯罪検挙まで実行されてこそ有効な防止対策になると思われる。

・サイバー攻撃に対する防御システムが、世界基準（国際基準）の統一化と共通のネットワークセキュリティにより守られるのなら良い。その為に様々な情報に対する共通で的確な対応システムを構築すべきと考える。

・うちは関係ないと思いがちな、中小企業へのアプローチを強化し、未然に防ぐ体制を構築する必要がある。

・証拠が残りやすいという点から、完全犯罪をあきらめさせ、無効化させる段階まで進めてもらうことが究極の理想の将来像である。少なくともサイバー犯罪は割に合わないと実行犯に思わせるところまで取組をすすめていただきたい。

（３）サイバーセキュリティ対策・サイバー人材の育成

サイバー犯罪は「匿名性が高い」「犯罪の痕跡が残りにくい」「不特定多数の者に被害が及びやすい」「距離的、時間的制約が少ない」「被害の潜在化」「組織的に敢行される」などの特徴があり、通信履歴が保存されていない国外からの犯行やダークウェブや匿名性の高い通信アプリケーションの存在などがサイバー捜査を困難にさせているなどの特徴がある。

県警察のサイバーセキュリティ対策の向上のためには、技術的な側面からの対策だけでなく、捜査などで必要となる人的サポート能力、そしてそれを支える組織的な体制の充実が必要不可欠であり、違法・有害情報等対策や偽サイト等対策、国境を越えて行われるサイバー犯罪への対策などにおいて、警察庁との連携や官民連携を進める必要がある他、警察庁及び都道府県警察が実施する教養研修などを通じサイバー人材を育成する必要がある。

（現状における課題・問題点）

・各道府県本部での個別の対応には限界がある。

・ＩＴ技術者を雇うには多大の予算が必要である。

・学生のうちから精通している人材を採用するのなら、獲得に向け警察官採用時点から、通常の採用基準や警察学校の訓練基準が適しているのか疑問である。

（今後方向性と期待される将来像）

・サイバー犯罪の手口はその道のプロが編み出し、ダークウェブ等を通じ世界中で情報共有されながら進化していることから、その対策を一県警で適切に対処するため、専門人

材の育成や体制整備を今以上に強化する必要がある。

・専門人材の育成や体制強化にも限界があると思われるので、地域性のないサイバー空間の犯罪対策は警察庁等国が主導して取り組むことが重要である。

・セキュリティ対策は国で行うべき。

・ＡＩなどのツールの活用や、民間の専門事業者に一定程度の業務委託体制が取れるよう検討する必要がある。

・便利なものは、誰もが有効に利用し、快適な社会ツールの一つとして危険を意識することなく利用できるようになれば良い。機器の設定面、システム面で、危険から守られるようになればと考える。

・今の社会ルールを守る為の規制の強化は利便性の向上と相反する可能性がある。公安等警察の規制は現実的な自由の保障と裏腹な関係にあることは同様である。国際基準、国際管理システムが地球上で共通認識として成立することが必要と考える。

・サイバーセキュリティ・捜査高度化センターによる部局横断的な解析技術の活用、全国警察との協同や民間も含めた人事交流・派遣等による優秀な人材の育成を推進し、適切な人材確保を進める必要がある。

・サイバー犯罪を完全に防御することは不可能との見解があった。まずはこの認識を県民に伝える必要があると思う。県の対策として、巧妙化する犯罪に追いつくため情勢に対応できる人材･育成が重要である。