兵庫県警察におけるサイバー戦略の実施について（一般甲）（要徹底）

令和８年８月18日
兵警サ企一般甲第63号

対号　兵庫県警察におけるサイバー戦略の継続実施について（令和６年８月９日兵警サ企一般甲第64号）

本県警察においては、深刻化するサイバー空間の脅威に適切に対処するため、対号に基づき各種対策を推進しているところであるが、社会情勢の変化を見据えた取組を一層推進するため、警察庁において警察におけるサイバー戦略が改定されたことを踏まえ、本県警察においても兵庫県警察におけるサイバー戦略（別添）を策定し、これに基づき各種対策を推進することとしたので、各所属長は、所属職員に周知徹底の上、その実効を上げられたい。

別添

兵庫県警察におけるサイバー戦略

第１　情勢認識

社会全体のデジタル化の進展に伴い、サイバー空間が、地域及び年齢を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げた一方、その匿名性が様々な犯罪で悪用されており、フィッシングに起因するとみられる証券口座に係る不正取引に加えて、匿名・流動型犯罪グループによって実行される、ニセ警察詐欺、ＳＮＳ型投資・ロマンス詐欺等の特殊詐欺、オンライン上で行われる賭博事犯、暗号資産を悪用したマネー・ローンダリング等が発生している。また、犯罪実行者募集情報等の違法情報及び爆発物の製造方法等の有害情報がＳＮＳを中心としたサイバー空間に氾濫しているほか、生成ＡＩ等の高度な技術を悪用した事案、企業・団体の事業活動に大きな影響を与えるランサムウェア事案等も発生している。

これらサイバー空間における事案は、公共の安全と秩序に対する挑戦であり、国民生活及び経済活動、ひいては安全保障及び危機管理に深刻かつ致命的な影響を及ぼすおそれがあることから、これらの事案に対処することは警察の責務である。

サイバー空間の匿名性を悪用した事案を認知した段階においては、国家を背景とする事案及び犯罪組織による金銭目的の事案のいずれに該当するか等は判然としないことが多いものの、国民の生命、身体及び財産の保護の任に当たる警察として、平時、有事を問わず間隙を生じさせず対処する必要がある。

そのために、警察は、事案の認知、実態解明、部門を越えた総合力に基づく横断的・俯瞰的分析、検挙等、あらゆる手段を駆使して対処に当たることが求められる。

第２　推進事項

１　検挙に向けた取組

(1)　事案認知の徹底

ア　事案の認知なくして検挙は達成されないところ、県民・事業者等からの通報及び相談（以下「通報等」という。）は、捜査の端緒となる上、サイバー空間をめぐる情勢の変化を把握する観点からも重要であることから、警察への通報等が積極的になされるよう、通報等がしやすい気運の醸成、環境整備等を推進した上で、被害の届出の迅速・確実な受理も含め、通報等に対して適切に対応する。また、こうした通報等を官民連携して促進するため、兵庫県サイバー攻撃情報共有ネットワーク等を通じた事業者等との平素からの信頼関係の醸成及びこれに基づく協力関係の構築を推進する。

イ　通報等の受動的な事案認知のみならず、能動的な事案認知も重要であることから、サイバーパトロール、能動的解明活動等を通じた積極的な端緒情報の入手に努める。

ウ　官民連携の軸となる一般財団法人日本サイバー犯罪対策センター（以下「ＪＣ３」という。）の知見及び情報を事案認知に活用するとともに、内閣官房等とも連携しつつ、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）の規定に基づく各種情報の把握及び認知に努める。

(2)　検挙に向けた捜査の推進

ア　サイバー部門は、国家を背景とする事案か否か、又は罪名にとらわれることなく、高度な専門的知識及び技術に基づき、サイバー攻撃、高度な技術的手法が用いられる事案等の他部門では対処困難なサイバー事案（警察法（昭和29年法律第162号）第

５条第４項第６号ハに規定するサイバー事案という。）を中心に、その捜査に果敢に取り組む。

イ　サイバー部門は、他部門が主管するサイバー事案の捜査に対しても積極的かつ主体的な支援を行い、被疑者の特定、暗号資産の形で隠匿された犯罪収益の解明等に貢献するなど、匿名性の打破に取り組む。

ウ　前記ア及びイの取組を通じて得られた情報を警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部（以下「サイバー特別捜査部」という。）に集約した上、サイバー特別捜査部と連携して横断的・俯瞰的分析を行うことで、これまで特定が困難であった複数事案同士の関連性、背景にある組織性、上位被疑者等を明らかにするとともに、更なる検挙を推進する。

(3)　国際連携の強化

国境を越えて実行されるサイバー事案の被疑者を検挙するためには、外国治安機関等との緊密な連携が不可欠であることから、警察庁を通じ、外国治安機関等からの共助要請に適切に対応するほか、被疑者が国内に所在しない場合であっても、警察庁を通じた国際共同捜査による検挙に向けた捜査を徹底する。

(4)　サイバー警察活動における適正性の確保

ア　サイバー事案においては発信元を隠蔽するための多種多様な手段が用いられているほか、これらの事案は国境を越えて実行され、その被害も広域かつ不特定の者に及ぶことから、多角的な証拠収集、裏付け捜査並びに電磁的記録の適正な取扱い及び解析・分析の徹底、ログの迅速な確保等のサイバー事案の捜査における基本的留意事項を徹底する。

イ　民間事業者又は他部門から提供を受けた情報等については、必要に応じて共有範囲を限定するなど、保秘の徹底を図るほか、各種法令等にのっとり、情報等の適正な管理を徹底する。

ウ　捜査幹部による適時適切な指揮及び捜査主任官等による管理を通じて、緻密かつ適正な捜査を推進する。

2　未然防止・拡大防止に向けた取組

(1)　検挙による未然防止の推進

ランサムウェア事案等のサイバー事案に対しては、被疑者の検挙により大本を断つことが最も効果的であることから、国境を越えて実行されるサイバー事案についても、国家を背景とした事案を含め、積極的に事件化を図り、検挙を通じた抑止を推進する。

(2)　官民連携による情報発信の推進

限りある警察のリソースのみで地域社会全体のサイバーセキュリティの水準を向上させることは困難であることから、サイバー防犯ボランティア、学校、商工会議所等の地域に根ざした多様な主体と連携しつつ広報啓発活動等を推進するとともに、管理者対策及び兵庫県サイバー攻撃情報共有ネットワーク等を通じた事業者等への情報発信を推進する。

(3)　犯罪インフラへの対処の推進

ア　犯罪インフラの解体に向けた取組の推進

(ｱ)　サイバー空間の匿名性に起因するなりすましを助長したり、警察による追跡を阻害したりするような技術等について、関連法令を所管する省庁及び行政処分権限を有する監督官庁に対して情報提供を行う。

(ｲ)　サイバー空間の悪用を容易にする犯罪インフラを解体するとともに、不正に調

達した預貯金口座等を犯罪者グループに提供する者、暗号資産取引所等の市場を通さずに違法な取引を行う者等を事件検挙を通じて解体する。

(ｳ) サイバー攻撃の攻撃元であるサーバ等について、その管理者に情報提供を行うことにより、その閉鎖等を促進するほか、サイバー事案の踏み台とされている家庭用インターネット通信機器等の対策を推進する。

イ 違法・有害情報への対処の推進

(ｱ) 警察活動を通じて認知した違法・有害情報について、ＳＮＳ事業者等に情報提供を行うとともに、インターネット・ホットラインセンターの運用及び投稿者に対する個別警告等によりその削除を促進する。

(ｲ) フィッシングサイト等の実在の事業者のウェブサイト等を装った偽のウェブサイトについて、ＪＣ３、関係事業者等とも連携しつつ、閲覧防止措置等が講じられるよう取組を推進してサイバー空間の環境浄化を図る。

(ｳ) 不正な口座情報及び悪用のおそれのあるクレジットカード番号等を関係金融機関等へ提供するなど官民が連携してサイバー空間の犯罪インフラ化を防止する。

3 基盤整備に向けた取組

(1) 人材の確保・育成

社会全体においてサイバー分野における高度な専門的知識及び技術を有する人材（以下「高度サイバー人材」という。）の重要性が高まっている一方で、少子高齢化、人口減少等の進行により、社会構造が変化し、警察職員の採用情勢も厳しさを増していること等から、サイバー人材の確保・育成を総合的かつ一体的に推進する。

特に、あらゆる犯罪にサイバー空間が悪用されていることから、深刻化するサイバー空間の脅威に的確に対処するため、組織を挙げて全職員のサイバー対処能力の向上を図るとともに、アクセス・無害化措置をはじめとする能動的サイバー防御を担い得る高度サイバー人材の確保・育成及びキャリアパス管理を推進する。

(2) 計画的な資機材の整備

サイバー空間の匿名性を打破するためには、スマートフォン、コンピュータ等の解析を行う解析用資機材、暗号資産追跡ツール等の高度な資機材が不可欠である一方で、財政事情は厳しいことから、警察庁における取組と緊密に連携しつつ、真に必要な資機材の計画的な整備及び集約を推進する。

(3) 研究・開発の推進

警察のサイバー対処能力を更に高度化するとともに、被害の未然防止及び拡大防止を図るべく、警察における研究・開発を推進する。また、その推進に当たっては、政府が推進する各種プログラムを有効に活用する。

第３ サイバー戦略の推進体制

(1) 積極的かつ主体的な捜査の推進

サイバー部門は、事案に係る罪名を問わず、その高度な専門的知識及び技術に基づき、他の事件主管部門のみでは対処困難な事案について、積極的かつ主体的に捜査を推進するとともに、サイバー部門及び情報技術解析部門が一体となって各部門への支援を行い、これらを通じて得られた情報をサイバー特別捜査部に集約するなど、情報集約の結節点としての役割を果たす。

(2) サイバー部門と情報技術解析部門との緊密な連携

警察の限られた人的・物的リソースを効果的かつ効率的に利用し、サイバー部門と

情報技術解析部門との緊密な連携を確保する。

(3)　国家的背景が疑われるサイバー攻撃への対処

国家的背景が疑われる機微情報の窃取、選挙への干渉等又は重要インフラ等の機能妨害及び機能破壊を企図したサイバー攻撃への対処に当たっては、国家的背景に関する分析及び外国による諸工作を総体として捉えた対策を効果的に推進する観点等から、関係部門と緊密に連携して対処する。

(4)　警察本部及び警察署の連携

サイバー事案であっても、発生地における住民からの相談受理、初動捜査等、現実の空間における対処を伴うことから、警察本部及び警察署が緊密に連携して対処する。

(5)　サイバー部門における他部門との協力体制の推進

サイバー部門が、他部門の捜査への支援、本県警察全体のサイバー対処能力の底上げ等の部門横断的な性質の強い任務を負っていることを踏まえ、人事の柔軟性を確保するなど、縦割りを排した上で、他部門と必要な協力を推進できるよう十分に配意する。