外国人犯罪、サイバー攻撃及び特殊詐欺等への対策に関する緊急提言
【治安・テロ・サイバー犯罪対策調査会　提言】

令和７年１２月１６日
自由民主党政務調査会

本調査会においては、昨年来、「闇バイト」対策、特殊詐欺対策、オンラインカジノ対策等について累次提言等を行ってきたところであり、先般の「闇バイト」指示役の検挙に見られるように、その成果も徐々に現れつつある。しかしながら、日々高まる我が国の治安への脅威に対処するため、早急に対策を講ずべき課題がなお存すると考えられる。

例えば、外国人による犯罪については、検挙件数が増加傾向にあり、犯罪の組織化も進んでいると見られるほか、社会の耳目を集める事案も発生しており、国民が不安を感じる状況が生じている。排外主義とは一線を画しつつ、我が国の規範の周知と犯罪の厳格かつ公正な取締りを推進することが急務であり、それが外国人との秩序ある共生社会を実現するための前提でもある。

また、最近、物流業や製造業を狙い撃ちしたランサムウェア[1]事案により、様々な製品の流通が停滞し、我が国の経済活動に大きな影響が生じている。一般的に、「サイバー攻撃」といえば、重要インフラを対象として国家の関与の下で行われるものが想起されることが多いと思われるが、身代金目的のランサムウェア被害は中小企業や医療機関に拡大しており、その報告件数は過去最高の水準となっている。さらに最近では、開発したランサムウェアを提供するサービス（ＲａａＳ：Ransomware as a service)が確認されるなど、ランサムウェア攻撃がビジネス化しており、攻撃者は、業種や事業規模を問わず、セキュリティ体制が脆弱な事業者を攻撃しているものとみられる。こうした状況を踏まえ、全ての国民がサイバー攻撃を受け得るとの危機意識を持つことが重要であり、官民を挙げてサイバー攻撃への対処能力を高める手立てを緊急に充実させなければならない。

さらに、本年４月、本調査会の組織的な詐欺への対策に関する提言に呼応する形で政府が「国民を詐欺から守るための総合対策２．０」を策定したものの、詐欺の増勢に歯止めがかからず、とりわけ特殊詐欺の被害額は、令和７年７月末の時点で、過去最悪であった令和６年の年間被害額を超えることとなった。こうした厳しい現実を重く受け止め、「国民を詐欺から守るための総合対策２．０」に

[1] 感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム。

盛り込まれた施策の着実な実施に加え、更なる対策を講ずるべきである。

本調査会においては、こうした課題への対応について有識者と関係省庁からヒアリングを行い、議論を重ねてきたところであり、以下のとおり、当面行うべき対策を緊急に提言する。

１　外国人による犯罪への対策

（１）警察における通訳体制の拡充

来日外国人犯罪は共犯事件の割合が41.1％（令和６年）と極めて高く、日本人の犯罪の当該割合（12.5％）の約3.3倍となっている。このため、検挙の際、同時に多数の通訳人が必要となることが多く、在留外国人数等が増加を続けていることを踏まえれば、十分な通訳体制を確保する必要がある。具体的には、警察における部内通訳人の育成及び部外通訳人の拡充に加え、同時に多数の通訳人が必要となった場合や、少数言語への対応が必要となった場合にも的確に捜査を行えるよう、警察庁の調整によって都道府県警察間における通訳人の情報共有・相互紹介等の取組を推進するほか、取調べにおいては、対面での通訳を原則としつつ、必要に応じ、遠隔地から電話等により通訳を実施する取組を推進すべきである。

（２）官民連携による広報啓発活動の実施

一部の訪日外国人旅行者による犯罪や迷惑行為が見られるが、その原因として、これらの旅行者が日本の法令やマナー等を十分に理解していないこと等が挙げられる。したがって、訪日外国人旅行者に対し、観光庁、外務省、出入国在留管理庁等の関係行政機関や民間事業者が連携して、査証取得時や入国時等の様々な機会を捉えて広報啓発活動を実施することにより、日本の法令やマナー等を周知すべきである。

また、技能実習生や留学生等に対しては、査証取得時、入国時等の広報啓発活動に加えて、その仲介事業者等からも、日本の法令やマナー等に関する情報提供を行うことが必要である。このため、出入国在留管理庁、厚生労働省等の関係省庁から仲介事業者等に対し、こうした情報提供について働き掛けるべきである。特に、技能実習生については、入国直後の入国後講習の機会を捉えて日本の法令やマナー等に関する啓発活動を励行することが重要であり、出入国在留管理庁、厚生労働省等の関係省庁は監理団体等と連携するなどして対応すべきである。

このような広報啓発活動により、犯罪、事故、迷惑行為等の加害者にも被害者にもならないよう外国人に注意喚起し、秩序ある共生社会の実現に取り組むべきである。

（３）国内外の関係機関の連携による厳正な取締り

外国人による組織的窃盗等の違法行為が後を絶たないことから、国内関係機関が緊密に連携し、外国捜査機関等から協力も得ながら、こうした違法行為の厳正な取締りを推進すべきである。加えて、違法民泊など特別法犯についても、確実な対処を行うべきである。

また、技能実習生や留学生等が、悪質な仲介事業者等を介して来日する場合がある。出入国在留管理庁、厚生労働省及び外務省等の関係省庁は、悪質な事業者等を排除するため、事業者等の不適切な活動に関する情報を蓄積・共有するなど、省庁間の連携を推進すべきである。その上で、国内の仲介事業者等が悪質な活動をしている場合には、法令に基づき行政処分を行うとともに、必要に応じ、捜査機関において犯罪捜査を行うなど、適切に対処すべきである。また、特に技能実習生については、国外の送出機関等による悪質な活動を把握した場合には、二国間取決めに基づき、相手国の政府に対して速やかに情報を提供し、厳正な処分がなされるよう申入れ等を行うべきである。

（４）不法滞在者対策の推進

我が国における不法残留者数は、7万1229人（令和７年７月１日時点）に上り、不法滞在者と地域住民との間に軋轢が生じトラブルに発展した事例も散見されている。不法滞在は厳正に対処すべき犯罪であり、政府が策定する「国民の安全・安心のための不法滞在者ゼロプラン」に基づき、適切に対策を推進すべきである。

（５）外国人犯罪グループによるＳＮＳの不正利用への対策の推進

来日外国人による犯罪は、日本人によるものと比べて組織的に行われる傾向があるように見受けられ、ＳＮＳを利用して犯罪グループを形成している例もみられる。

「国民を詐欺から守るための総合対策２．０」に盛り込まれている

○　ＳＮＳアカウント開設時における本人確認の厳格化

○　ＳＮＳ事業者における捜査機関からの照会への対応の強化

○　日本法人のない海外事業者への迅速な情報提供の働きかけ

等の諸対策は、外国人犯罪の抑止・検挙にも資するものであることから、これらを着実に推進すべきである。

２　ランサムウェア等のサイバー犯罪への対処能力の強化

（１）サイバー攻撃を想定した業務継続計画の策定及び訓練の実施の促進

「暗号化したファイルを復号してほしければ身代金（ランサム）を支払え」などと企業等を恐喝するランサムウェア事案による被害が多発している。令和７年上半期におけるランサムウェアの被害報告件数は過去最多の116

件となっており、最近も、複数の企業がランサムウェアにより商取引の阻害、情報の流出等の深刻な被害を受けている。ランサムウェアの被害に遭った企業等においては、被害の調査や復旧、対外説明等に忙殺されることとなるほか、復旧するまで長期にわたって経済活動の停止を余儀なくされることも多い。また、被害の調査・復旧に要する費用は、年々増加している。このようなサイバー攻撃を防止するために、まずはＶＰＮ機器等のぜい弱性への対応、認証情報の適切な管理等の取組を着実に進めることが重要である。特に、サプライチェーンにおいて重要な事業者がサイバー攻撃を受けた場合には、国民の生活や国全体の経済に重大な影響が生じ得ることを考えると、基本的な対策を実施することは、企業の社会的責任と言っても過言ではない。一方、攻撃を行う犯罪者側が優位とされているサイバー攻撃について、その全てを未然に防ぐことは困難であることを踏まえれば、企業等においては、いつでもサイバー攻撃を受ける可能性があることを前提に、被害発生時に業務を適切に継続するための取組を推進していくことが重要である。

具体的には、ランサムウェア等のサイバー攻撃を受けた際に執るべき措置として、オフラインバックアップデータからの復元、各種ログの保全、あらかじめ設定した警察等関係機関の窓口への迅速な通報等の対応手順を整理した業務継続計画（ＢＣＰ：Business Continuity Plan）を策定した上で、具体的な状況を想定した訓練を実施することが重要であることから、こうした取組について、関係行政機関が連携して、所管業界等に対して広報啓発していくべきである。

また、サイバーセキュリティに関する適切なサービスの提供を受ける中小企業や小規模事業者に対して「ＩＴ導入補助金」を活用した支援を行う「サイバーセキュリティお助け隊サービス」事業や、サイバー攻撃を想定した業務継続計画に基づき定期的に訓練を行う病院等に対する診療報酬の加算、医療機関におけるサイバーセキュリティを確保するための補助金等の施策も、既に存在している。関係省庁においては、こうした施策を更に推進するとともに、所管業界ごとの実情を踏まえ、各事業者から必要とされている支援を丁寧に把握し、サイバー攻撃の未然防止や被害拡大防止のための措置を促進する取組を強化していくべきである。

（２）検挙を通じた犯罪の抑止に向けた官民連携の推進

ランサムウェア等のサイバー攻撃は、我が国の社会・経済活動や国民生活の安定を脅かす重大な犯罪であり、被疑者の検挙を通じた犯罪の抑止が極めて重要であることは論を俟たない。

警察においては、攻撃手法や攻撃者の解明、攻撃の無力化や被害回復等の

能力を更に高めるべく、サイバー人材の確保・育成や各種資機材の整備等の取組を推進すべきである。また、サイバー攻撃の被疑者は国外にいることが多いと見られることから、警察においては、外国捜査機関等との連携を強化しつつ、国際共同捜査を通じた被疑者の検挙に取り組む必要がある。

サイバー攻撃への対処に当たっては、被害企業等から協力を得ることが肝要である。これまで警察が達成してきた国際共同捜査による検挙や警察庁サイバー特別捜査部が独自開発した復号ツールによる被害回復の成果についても積極的に広報し、被害企業からの協力を得られるよう努めていくべきである。また、本年５月、サイバー対処能力強化法が制定されたところであり、同法に基づく協議会を活用して官民の情報共有を深化させることが重要である。さらに、各都道府県警察において設置されたサイバーテロ対策協議会等の枠組みを通じた官民連携を更に強化すべきである。被害企業の中には、警察に通報することなく、「データを復旧する」などと称して犯罪グループと交渉する「復旧業者」や「コンサルタント」に依頼して間接的に身代金を支払っている実態があるとも指摘されている。このような犯罪グループへの利益供与を阻止する観点からも、警察から企業等に対する平素からの情報提供、具体的事案を想定した警察と企業等の合同対処訓練等を通じて、サイバー攻撃に屈しない業務継続計画の策定の促進や警察への通報の機運の醸成に一層取り組むべきである。

加えて、サイバー保険は、事案発生時の各種対応を支援するなど企業活動の迅速な復旧を可能にする役割を果たしていることから、適切な保険業者が提供するこうした保険の有用性について周知を図るなど、その普及を促進するための取組を行う必要がある。あわせて、検挙による抑止を一層推進する観点や保険加入によるモラルハザードを防止する観点から、保険金の支払いを受けるためには警察への通報が必要である旨を保険の約款に明記すべきである。その上で、早期に通報がなされなかった場合には保険金の支払額を減額したり、ＢＣＰの整備等高度なセキュリティ体制を構築している事業者に対しては掛金を割り引いたりするなど、一層有用なサイバー保険の在り方を検討すべきである。

３　特殊詐欺等対策

（１）金融機関等における取組の強化

依然としてインターネットバンキングを通じた高額な詐欺被害が発生していることを踏まえ、インターネットバンキングの振込限度額の引き下げや限度額変更のタイミングの制限等の取組を加速すべきである。また、近年、フィッシングの報告件数やクレジットカード不正利用被害額が増加し

ていることに加え、二段階認証が突破されるなど手口が巧妙化しているところであり、こうした被害を未然に防ぐため、送信ドメイン認証技術（ＤＭＡＲＣ）の普及、フィッシングサイトの閉鎖活動、金融機関等によるパスキーの導入を更に加速すべきである。

さらに、実態のない法人が設立され、当該法人が詐欺等の犯罪収益の隠匿等に悪用される実態があることから、犯罪収益移転防止法により求められている取引時確認といった法人の実質的支配者情報を確認する制度を確実に運用するほか、より実効性のある取組について検討を加速すべきである。

加えて、本年２月に本調査会が策定した「組織的な詐欺から国民の財産を守るための対策に関する緊急提言」において、預貯金取扱金融機関等の間における不正利用口座の情報共有等の枠組みの創設を提言したところであるが、その枠組みを更に発展させた新たな取組として、諸外国の詐欺対策センターも参考に、被害金の即時の追跡・凍結・回復を実現するための官民協働の「金融犯罪対策センター」（仮称）を構築し、金融機関等におけるモニタリング能力の底上げや、被害情報の共有と口座凍結の迅速な実施を促進すべきである。

（２）通信事業者等における取組の強化

詐欺へ誘引する手段としてＳＮＳのダイレクトメッセージ等が多く用いられていることを踏まえ、ＳＮＳ事業者において、詐欺に誘引するダイレクトメッセージ等を利用者が受信した際に警告表示を行う取組を更に推進すべきである。

また、特殊詐欺の中で、国際電話を端緒とするものが圧倒的多数を占めていることを踏まえ、各種機会を通じて国際電話の利用休止について強く国民に周知するとともに、国際電話サービスを利用しない者に対する優遇措置等、国際電話を真に必要としない者に対して利用休止を促すような効果的な対策の導入を引き続き検討すべきである。

さらに、新たな取組として、民間の高度な知見等を活用し、国際電話を拒否することができるような携帯電話向けの被害防止アプリについて、その普及を促進すべきである。加えて、著名人なりすまし型偽投資広告については、当該広告情報を発信する行為が一定の場合には刑法に触れることを明確化し、これを法令違反情報として位置付けた上で、「違法情報ガイドライン」に記載することにより、情報流通プラットフォーム対処法上の大手プラットフォーマーに削除を促す取組を推進すべきである。

（３）「国民を詐欺から守るための総合対策２．０」に基づく検討の加速

詐欺の増勢に歯止めがかからない現状に鑑み、（１）及び（２）に掲げた施策のほか、「国民を詐欺から守るための総合対策２．０」において検討す

ることとされている以下の施策については、可能な限り早期に結論を得るべく、検討を加速させるべきである。

○　ＳＮＳアカウント開設時における本人確認の厳格化
○　データ通信専用ＳＩＭの本人確認の義務付け等
○　預貯金口座等の不正な譲渡等に係る罰則の引上げ
○　犯罪収益移転防止法の適正な履行の確保
○　事業者間における不正利用に係る名義情報等の共有の促進
○　インターネットサービスの悪用の実効的排除に資する法制度の調査等
○　犯罪実行者募集情報に対するＡＩリプライ警告の高度化
○　犯罪実行者募集情報に対するＡＩ技術等を活用した対策
○　犯行に利用されるツールやプラットフォーム等への実効的な注意喚起
○　高齢者のＡＴＭ振込・引出限度額を少額とすることの制度化
○　架空名義口座を利用した新たな措置や関係法令改正
○　金融機関への照会の迅速化
○　暗号資産の確実な没収・保全の推進
○　ＳＮＳ事業者における捜査機関からの照会への対応の強化
○　通信履歴の保存の義務付け等
○　匿名性の高い通信アプリによる被疑者間の通信内容等の把握手法
○　海外に移転した犯罪収益等を特定する手段等
○　電話番号の悪用防止のためのより効果的な方策の実施等の対策
○　発信者番号偽装への効果的な対策
○　迷惑ＳＭＳ等に係る被害防止機能向上のための方策
○　携帯電話を使用しながらＡＴＭを利用した場合のＡＴＭの利用中断措置を含めた対策
○　外交ルートの活用も含めた外国当局とより緊密な情報共有等が可能となる連携体制の構築
○　悪質リフォーム業者に対し、監督官庁が適切な行政処分等の措置を講じるための対策

（４）警察における取締りの強化

国民を詐欺被害から守るためには、匿名・流動型犯罪グループを壊滅することが肝要であることは言うまでもないが、警察庁・警視庁に設けられた新たな体制の下、匿名・流動型犯罪グループの中核の検挙に向けて更に取組を強化すべきである。

また、特殊詐欺事犯が、海外を拠点として敢行されるケースが多いことから、外国の関係機関との連携を強化すべきである。

このほか、先般発生した匿名・流動型犯罪グループへの捜査情報の漏洩

は、匿名・流動型犯罪グループの壊滅に向けた各種捜査に影響を及ぼしかねない重大な事案であることをしっかりと認識し、警察において再発防止に万全を期すよう、対策を講じるべきである。

以上