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
【治安・テロ・サイバー犯罪対策調査会　提言】

令和７年２月２５日
自由民主党政務調査会

本調査会としては、昨年末にいわゆる「闇バイト」対策の強化に関する緊急提言を行ったところであるが、最近の犯罪情勢をみると、令和６年中の財産犯の被害額は約4,000億円（前年比約1,500億円増）に上り、刑法犯認知件数が戦後最悪だった平成14年の被害額を上回るという極めて憂慮すべき状況にある。その増分の大半を特殊詐欺・SNS型投資・ロマンス詐欺を始めとする詐欺による被害額（前年比約1,400億円増）が占めており、これらの詐欺への対策が急務である。

犯行グループは巧妙に手口を変化させているところ、これに対応するためには、緊急提言において示した対策を徹底することはもとより、犯行グループが利用している金融･通信に関するサービスやインフラについて、悪用を防止するための仕組みを設けるなどの対策について早急に検討を進め、実施可能なものから速やかに実施することが必要である。

また、更なる被害を抑止するためには犯行グループの中枢を検挙することが肝要であり、そのためには新たな捜査手法の導入に向けて、技術的･法的な検討を進めなければならない。

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提言する。

１　金融関係
（１）インターネットバンキングの申込み時における審査の強化等

最近の被害事例の中では、犯行グループが被害者にインターネットバンキングの利用を申し込ませ、インターネットバンキングで被害金のやり取りをさせる手口が確認されている。従来の特殊詐欺の手口とは異なり、被害者を金融機関等の窓口に行かせることなく犯行が完結するため、警察や金融機関等の職員による水際での被害防止が困難であるほか、インターネットバンキングは利用限度額が高額であり、被害額が増加しやすいといった課題がある。

これに対応するため、政府から金融機関に対し、インターネットバンキングの申込みがあった際の審査の強化や注意喚起、インターネットバンキングの初期利用限度額の適切な設定、利用限度額引上げ時の利用者への確認

の徹底等を依頼し、被害の抑止に努めるべきである。

（２）預金取扱金融機関等の間における情報共有等の枠組みの創設

犯行グループは複数の預金取扱金融機関の口座を保有していると思われ、被害金を次々に移動させることによって、その追跡を困難にさせているほか、被害金が犯行グループの手に渡る前に口座凍結を行うことを困難にさせている。現状は、個々の金融機関内部において、不審な口座の情報をモニタリングするなどしているところであるが、犯行に使用される口座の情報を迅速に捜査機関が取得し、かつ、犯行グループによる被害金の出金を防ぎ被害回復を図るため、預金取扱金融機関間において取引情報を共有しつつ、不正取引を検知し速やかに口座凍結を行うことが可能となる枠組みを創設するべきである。

なお、犯行グループが集約した被害金を暗号資産に変換し、海外の暗号資産交換業者の口座に移転させるなどの事例も確認されていることから、将来的には、預金取扱金融機関間のみならず、暗号資産交換業者を始め金融インフラに関連する事業者全体における情報共有等の枠組みを創設することを視野に入れつつ、その在り方について検討すべきである。

（３）「架空名義口座」を利用した捜査

犯行グループは口座の名義から人定事項を特定されることを防ぐため、他人名義の口座等を違法に取得し、犯行に利用している。これを逆手に取り、金融機関・捜査機関が管理する「架空名義口座」を犯行グループの手に渡らせ、その利用状況を把握することによって犯行グループの上位被疑者の検挙、犯罪収益の剥奪等に必要な情報を取得できると考えられる。また、これによって、全体として口座の悪用を牽制する効果があるものと考えられる。

「架空名義口座」を利用した捜査を実施するには関係法令の改正が必須になると考えられることから、政府において早急に検討すべきである。

２　通信関係

（１）データ通信専用SIMの契約時における本人確認の義務付け

データ通信専用SIMについては、通信アプリを利用することによって音声通話SIMと同様に通話等をすることができるにもかかわらず、音声通話SIMと異なり、契約時の本人確認が法令によって義務付けられていない。

契約時の本人確認は犯行の未然防止・犯行後の追跡可能性の確保に有効と考えられることから、データ通信専用SIMについて、その悪用実態を踏まえ、契約時の本人確認の義務付けを検討すべきである。

（２）固定電話の国際電話サービスを悪用した詐欺等への対策

特殊詐欺に利用された電話番号の多くが国際電話番号となっており、そ

の接続を防ぐことが国際電話番号を利用した犯行の未然防止につながると考えられる。

そのため、国際電話サービスを利用しない設定があることを政府広報等を利用して国民に広く周知するとともに、固定電話の移転、切替え時等の契約変更等の機会をとらえて、とりわけ高齢者に国際電話サービスの必要性を判断する機会を提供するなど、予防的な対応を取れるようにするべきである。

また、国際電話サービスを利用しない者に対して料金等で優遇するなど、予防措置をしやすくする仕組みも検討すべきである。

（３）詐欺電話・詐欺SMSを遮断するサービスに係る支援措置等

一部の関係事業者において迷惑電話や迷惑SMSを防止するサービスを提供しているところ、同様のサービスを詐欺電話・詐欺SMS対策として普及させることによって、自主的な被害防止を促進することができると考えられる。

前述のサービスには有料のものもみられるところ、これについて、無償化を含めた支援の措置とともにより効果的な方策を検討し、その普及や有効性の向上に努めるべきである。

（４）不特定多数の者に対する詐欺に誘引するSMS等の送信防止・遮断

詐欺に誘引するSMS、SNSのダイレクトメール、電子メールについては、不特定多数の者に大量に送信されている実態がうかがえる。

これらが被害者の端末に届く前に通信事業者において送信を防止し、又は遮断することによって、被害の未然防止につながると考えられることから、現行法の範囲内でこうした取組が実施可能であるかを検討し、可能であれば、通信事業者と連携し早期に実施すべきである。また、それが困難であれば法改正等を検討すべきである。

（５）犯罪に悪用される通信アプリ等の通信内容等を把握するための措置の検討

シグナル、テレグラム等匿名性の高い通信アプリを始めとする犯罪に悪用される通信アプリ等について被疑者の通信内容や登録者情報等を迅速に把握することは、犯行グループの壊滅に必須である。

しかしながら、そのために必要な技術や法制度については十分な検討がなされていない状況にあることから、ある種のソフトウェアを利用して犯行グループの端末から犯罪に悪用される通信アプリ等の通信内容等を迅速に把握するなどの効果的と考えられる手法について、諸外国における取組を参考にしつつ、技術的アプローチや新たな法制度導入の可能性も含め検討すべきである。

（６）通信履歴の保存の義務付け

通信履歴は、本来、通信事業者が業務を遂行する上で必要な範囲内で保存するものであるが、犯罪のオンライン化が進んだ現下の状況においては、犯罪に関与している発信者を特定するために、捜査機関が通信事業者から通信

履歴を取得することが必要不可欠である。

捜査機関が被害を認知した時点では通信履歴が残されていない場合が少なくないことから、通信履歴を捜査に利用するためには、通信事業者に一定期間の通信履歴の保存を義務付けることが有効と考えられるところ、義務付けに係る保存期間や費用面の課題についても、海外の例も参考にしながら検討すべきである。

3　総合的な対策

国民を詐欺から守るための総合対策が策定されたにもかかわらず、詐欺被害が過去最悪となっている現状を踏まえ、以上の項目を含め、政府においてあらゆる方向から対策を検討し、可能なものから速やかに実行すべきである。

以上