資料 10

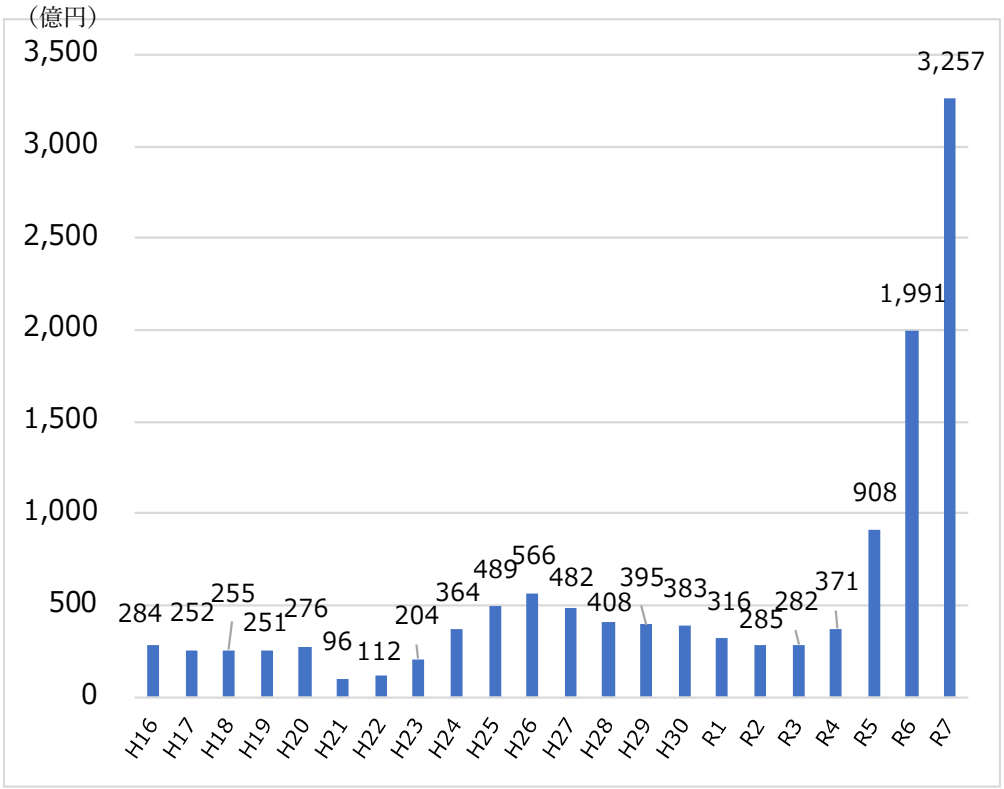
匿名・流動型犯罪グループによる犯罪の発生状況等（案）

１　特殊詐欺の被害状況

特殊詐欺の被害額は、この数年で爆発的に増加している。令和７年中は約 3,257 億円に達し、過去最悪を更新することとなったが、令和８年上半期は前年同期を更に上回る約 1,816 億円となっており、これは１日当たり約 10 億円の被害が発生している計算になる。また、個別の事案を見ると、９回にわたり総額約 12 億円がだまし取られるなど、長期間の巧妙な欺罔により、継続的に巨額の金銭が詐取される事例も発生している。

こうした特殊詐欺の多くに、匿名・流動型犯罪グループが関与しているとみられる。

【図１】特殊詐欺の被害状況



２　強盗等の被害状況

匿名・流動型犯罪グループは、凶悪な事件も多数引き起こしている。

令和６年には、南関東１都３県において、「闇バイト」を実行犯とする 18 件の強盗事件が２か月以上にわたって連続発生しており、このうち１件で被害者が殺害され、12 件で被害者が負傷している（令和８年２月までに 55 名（延べ 85 名）が検挙されている。）。

また、令和８年５月には、栃木県内で、高校生等を実行役とする強盗殺人事件が発生した。この事件では、実行役は現場指示役の指示に従い被害者を殺害したほか、現場指示役と上位指示役は秘匿性の高い通信アプリを使用していたことが判明している。

【図２】　令和６年中に発生した一連の事件

３　匿名・流動型犯罪グループによる犯罪の被害防止に向けた取組

(1)　実態解明及び取締りのための取組

警察では、匿名・流動型犯罪グループの組織構造、内部統制の方法、資金の流れ等を解明し、その撲滅を図るため、

○　広域的な捜査連携や仮装身分捜査（令和７年１月に導入）による取締り

○　匿名・流動型犯罪グループ情報分析室（令和７年 10 月に警察庁に設置）における全国の情報の集約・分析

○　匿流ターゲット取締りチーム（略称「Ｔ３」。全国警察から捜査員を派遣し、令和７年 10 月に警視庁に設置。令和８年４月に体制増強）による取締り

○　外国の捜査機関との連携等国際捜査力の強化（令和８年６月からタイにリエゾンを派遣）

等に取り組んでいる。

(2)　広報啓発をはじめとした被害防止のための取組

警察では、自治体、自治会、関係団体・事業者等と連携し、

○　特殊詐欺の犯行に悪用されることが多い国際電話の利用休止を呼び掛ける活動（「みんなで止めよう!!国際電話詐欺 #みんとめ」）の推進

○　特殊詐欺の被害防止に資する警察庁推奨アプリ（令和７年 12 月に推奨制度を導入）の普及促進

○　金融機関と連携した被害拡大防止の推進

等に取り組んでいる。

(3)　犯罪インフラ対策のための取組

匿名・流動型犯罪グループにとって犯罪インフラが使いにくいものとなるよう、

○　犯罪収益の移転の阻止と被害者への返還を効果的に行うための「架空名義口座」に係る制度の整備（令和８年６月に立法措置済み）

○　「送金犯罪」（令和８年７月に罰則を導入）の取締り
○　不正に取得された携帯電話について携帯電話不正利用防止法に基づく役務提供拒否を促すための携帯音声通信事業者への情報提供
○　データ通信専用 SIM の契約締結時に本人確認を義務付ける制度の整備（令和８年５月に立法措置済み）

等に取り組んでいる。

４　匿名・流動型犯罪グループによる犯罪の被害防止に係る課題

前記３のとおり、警察等が匿名・流動型犯罪グループによる犯罪への対策を強化・推進しているにもかかわらず、期待される効果が十分に得られているとはいえない状況となっている。これには、以下の２点の課題があると考えられる。

(1)　匿名・流動型犯罪グループへの捜査の困難性

匿名・流動型犯罪グループの捜査は長期化する傾向にあり、具体的には以下のような例がある。

○　犯行グループの実行役は、「架け場」としてホテルを利用しており、繰り返し犯行拠点を移転させていた。また、警察の尾行への警戒心が極めて高かった。このため、ひとたび移転先を把握しても、直ちに行方をくらますということが繰り返され、詐欺事件の発生から「架け場」におけるかけ子の検挙までに約７か月を要することとなった。その間、当該犯行グループの標的とされた人々に対し、被害防止のための措置をとることができなかった。

○　犯行グループの実行役は、「架け場」として車両を利用し、移動しながら犯行を行っていた。このため、実行役の特定や居所の把握が難しく、詐欺事件の発生から「架け場」におけるかけ子の検挙までに約５か月を要することとなった。その間、当該犯行グループの標的とされた人々に対し、被害防止のための措置をとることができなかった。

また、匿名・流動型犯罪グループの被疑者のうち、「捨て駒」である実行犯を検挙しても、上位の指示役や次の標的を速やかに特定することは困難であり、新たな実行犯が補充されて犯行が継続されることとなる。

このため、刑事手続により、これらの犯罪を一つ一つ立件して対処するだけでは、同種犯行の反復・拡散に迅速に歯止めをかけることができない状況にある。

(2)　秘匿性の高い通信アプリの悪用等

特殊詐欺の被害者に連絡が行われていた拠点において、当該連絡用のスマートフォンとして 84 台が差し押さえられた例や、投資詐欺事件に係る実行犯のリクルーターであった者が、１名で 12 台のスマートフォンを所持していた例があるなど、匿名・流動型犯罪グループがスマートフォンやタブレット等の犯行ツールを活用して犯罪を敢行している実態が把握されている。

また、上記のような犯行拠点で差し押さえたスマートフォンやタブレットに、標的となる人物の詳細な情報（氏名、住所、電話番号、生年月日、性別、家族構成、学歴、所得、保有銀行口座、使用するスマートフォンのメーカー、やり取りした際の状況（通信アプリを使えるか、文字入力によるやり取りができるか等））が掲載された「闇名簿」

が、エクセルファイル、画像ファイル等として記録されていた例があり、こうした情報が犯人間で通信アプリを介して共有されている実態が把握されている。

現行制度の下で、警察が犯行グループの通信内容等を解明するためには、主に

① 通信事業者の協力の下、その保管・管理する通信ログ等の情報を取得する手法

② 通信経路上の通信を捕捉する手法

③ 犯行グループのスマートフォン等を押収し、その保存データを解析する手法

が考えられる。

しかし、匿名・流動型犯罪グループ等は、エンド・トゥー・エンド暗号化技術が用いられた通信アプリを使用することが常である。その場合、送信者の端末で暗号化された情報が受信者の端末で復号されることから、通信経路の途中段階（通信事業者のサーバーや通信経路）の情報は常に解読不能な暗号文の状態となっている。このため、仮に、通信を媒介する通信事業者の協力を得て前記①又は②の手法をとったとしても、その内容を復号・解明することは技術的に不可能であり、こうした情報を警察が被害防止に活用することができない状況となっている。また、前記③の手法については、そもそも押収に至るまでに相当長期間の捜査を要するとともに、仮に押収できたとしても、被疑者が画面ロックの解除に応じないことや、自動的に情報が消去されていくことが多いことから、情報を迅速な被害防止に活用できる可能性は低い。

５　被害防止に必要な情報を入手することにより警察が果たし得る責務

犯人が通信アプリを利用して行う犯人間の相互連絡や被害者への連絡においては、これから敢行しようとしている犯罪の標的となる人物に関する情報等、切迫する犯罪被害に関する情報が記録されていると考えられる。

警察がこうした情報を把握することができれば、犯人を直ちに特定・検挙できない場合であっても、切迫した犯罪被害を防止する責務を果たすことが可能となると考えられる。

具体的には、入手した情報に基づき、

○　標的となっている人物の所在の特定

○　犯罪の切迫性の見極め

○　実行され得る犯罪の罪種、実行犯の人数、手口・凶器等に応じた態勢の整備

等を行った上で、適切な警察活動（重点的な警備・警ら、防犯指導等）を通じて犯罪被害の未然防止を図ることとなる。

６　小括

匿名・流動型犯罪グループが実行する特殊詐欺や強盗等の被害は極めて憂慮すべきものであり、警察等が取組を強化しているが、匿名・流動型犯罪グループの捜査をめぐっては、前記４(1)のような課題があり、直ちにその組織全体を検挙し、刑罰法令の適用により継続する犯行を止めることは、極めて困難と言わざるを得ないことから、十分な被害抑止効果が得られていない状況にある。

他方で、犯人間でのやり取り等に含まれている情報の中には、前記４(2)のとおり、犯罪の標的となる人物の特定等に資する情報が含まれており、こうした情報が入手できれば、

警察による効果的な被害防止措置が期待できるものの、従来の手法では当該情報を警察が入手することは難しい。

こうした状況を踏まえれば、匿名・流動型犯罪グループによる犯罪の被害を防止するためには、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し、犯罪の被害が切迫する者に対して警察が直接的かつ積極的に被害防止措置を講じる制度を導入することが急務である。