警察政策学会資料　第140号
令 和 7 （ 2 0 2 5 ） 年 2 月

サイバー捜査の課題と展望について

警察政策学会

刑事警察研究部会

まえがき

本資料は、令和６年 11 月 25 日、刑事警察研究部会の例会において、元警察庁サイバー警察局長　河原　淳平氏が、「サイバー捜査の課題と展望について」と題して講演された内容をまとめたものです。

同氏は、昭和 63 年に警察庁に入庁以来、警察庁警備企画課サイバー攻撃対策官、警察庁情報通信局情報技術解析課長等を歴任されたほか、石川県警察本部長、警察庁情報通信局長等の要職を経て、令和４年４月に新設された警察庁サイバー警察局長に就任され、令和６年１月まで創成期にある同局の責任者として、我が国に対するサイバー攻撃や多発するサイバー犯罪等への対応にご尽力された方です。

また、同氏は、令和６年９月に「匿名・流動型犯罪グループに対する戦略的取締り」をメインテーマとして開催された警察政策学会シンポジウムにおいてもコーディネータをお務めになるなど、退職後においてもこの種事犯の対策に積極的に取り組んでおられます。

こうした経験を踏まえた同氏の今回のご講演は、まさにこの分野の第一人者による時宜を得た総括となっており、従来断片的に語られるに過ぎなかったサイバー犯罪捜査の現状や課題について、初めて本格的にまとめられた貴重なものと言えましょう。極めて示唆に富む内容であり、警察政策学会資料として広く会員の皆さんのご参考に供することと致します。

令和７年１月

刑事警察研究部会長　小野　正博

目　次

講　　演

講師　　元警察庁サイバー警察局長
河　原　淳　平

はじめに

令和４（2022）年４月に関東管区警察局サイバー特別捜査隊が発足してから２年半になり、令和６（2024）年４月にはサイバー特別捜査部（以下「サイバー特捜部」という。）へ組織上の格上げがなされたところである。

サイバー特捜部では、これまで国際共同捜査への積極的参画を通じ、国際的なサイバー犯罪集団の摘発等において一定の成果を上げて来たが、本日は、そのバックボーンとなっている「情報の集約と横断的分析」及び「機動的な国際連携」について、その有効性を示すとともに、態勢の強化に関する取組をご紹介する。

また、目下最大の治安課題の一つである匿名流動型犯罪グループ（以下「匿流」という。）による犯罪については、昨今、サイバー空間における技術やサービスを悪用するものも多くみられ、サイバー特捜部ないしサイバー部門がその能力を生かして捜査に貢献するケースも出て来ている。

後半ではこのようなサイバー捜査のスコープの拡大についてお話しさせていただく。

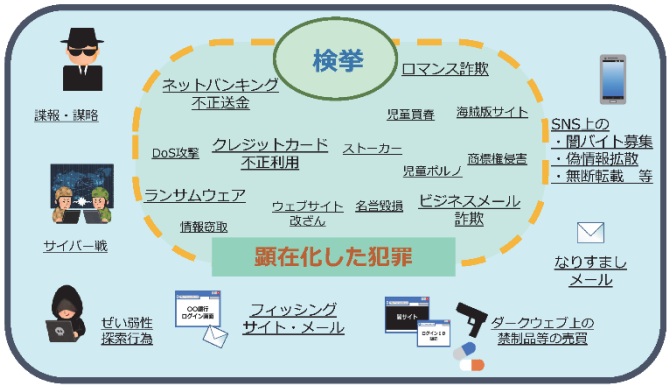
なお、本稿中、意見にわたる部分は筆者の個人的見解であることを申し添える。

１　増大するサイバー空間の脅威

(1) サイバー空間における脅威

サイバー空間は、多くの国民が参画し、重要な社会経済活動を営む公共空間となっているが、その一方で、匿名性を悪用した誹謗中傷や脅迫、偽情報・誤情報の氾濫、日常的に行われる禁制品の取引、ランサムウェア、フィッシング詐欺といった金銭目的犯罪の横行、渦巻く国家間の地政学的競争に基づく諜報謀略など、多様かつ膨大な脅威を内包している（図１）。

サイバー空間の様々な脅威（図１）



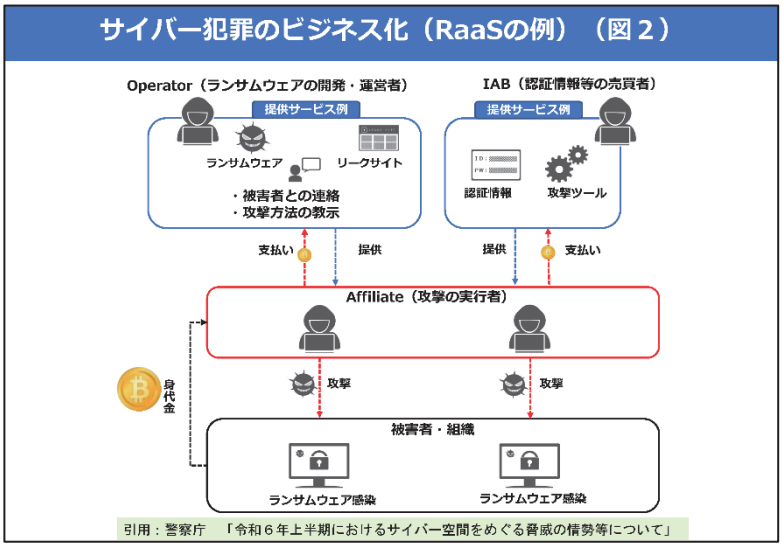
(2) サイバー空間の脅威の構造的特徴

ここで、サイバー犯罪やサイバー攻撃といったサイバー空間の脅威の構造に着目すると近年いくつかの特徴が挙げられる。

ア　サイバー犯罪のビジネス化

一つ目の特徴は、サイバー犯罪のビジネス化が進行しているということである。その中には攻撃組織の運営者と実行者の分業・棲み分けという現象も含まれている（図２）。

サイバー犯罪のビジネス化（RaaSの例）（図２）



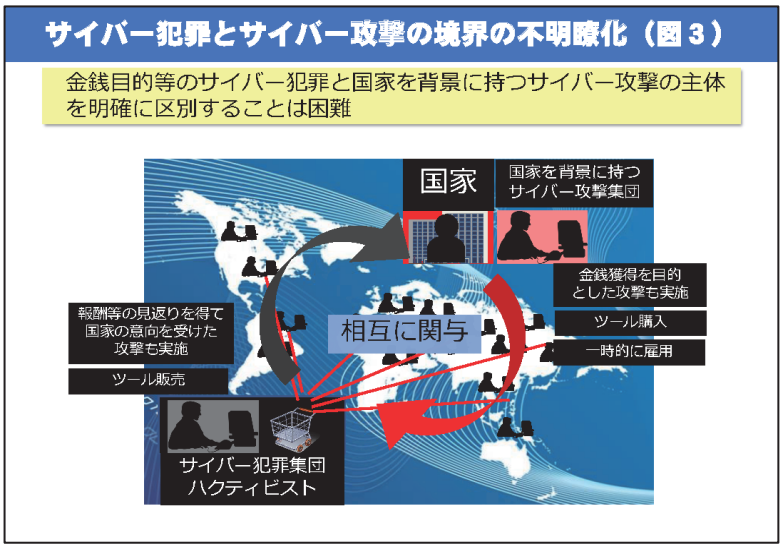
例えば、ランサムウェア攻撃グループでは、ソフトウェアの開発、標的の選定、暴露サイトの運用など役割が細分化され、リクルートや経理担当部門もあるなど、さながら企業といった様相を呈している。

また、近年はランサムウェアの開発・運営を行う大元の組織（オペレーター）からランサムウェアの提供を受けた別のグループ等（アフィリエイト）が実際の攻撃を実行し、犯行で得られた収益を按分するというスタイル（RaaS:ランサムウェア・アズ・ア・サービス）が定着している。このビジネスモデルには、必要に応じてシステムに侵入するための認証情報の売買を行うIAB（イニシャル・アクセス・ブローカー）という仲介業者も関与している。

大元の組織は仲間割れ等による離合集散や看板の付け替えを繰り返しながらも中核メンバーはある程度固定している。その一方で実行グループは事案ごとに入れ替わり、大元組織とのつながりは希薄である。このような関係性は匿名流動型犯罪グループの構造と一定の類似点を有している。

イ　サイバー犯罪とサイバー攻撃の境界の不明瞭化

もう一つの特徴は、金銭目的等で実行されるサイバー犯罪の主体と国家の指揮や支援の下に実行されるサイバー攻撃の主体を明確に区別できないということである（図３）。



中国及びロシアでは、軍・情報機関と、普段は金銭目的のサイバー犯罪を実行している在野のサイバー犯罪集団とが、各自の利害に応じて連携しているとされている。

ロシアは軍・情報機関が民間フロント企業（調査会社、報道機関等を標ぼう）、愛国的ハッカー、サイバー犯罪集団に、中国も普段は金銭目的のサイバー犯罪を行っている在野のブラックハッカーに、犯罪行為を見逃すのと引き換えに外国政府や外国企業等に対する DDoS 攻撃や情報窃取等を請け負わせる手法をとっているとの見立てがある。

ロシアや中国が、民間人や民間企業をサイバー攻撃の実行部隊として用いるのは、行為が発覚して国家の責任を追及されたときでも言い逃れができるからであると考える。

このように治安の問題で完結するのか国の安全保障につながるのか一見しただけでは判然としないこともサイバー空間の脅威の特徴といえる。

2　サイバー空間の脅威への対処に必要なこと

次に、サイバー捜査の要諦である「情報の集約と横断的分析」及び「国際連携」について見ていくこととする。

(1) 情報集約と横断的・俯瞰的分析体制の確立

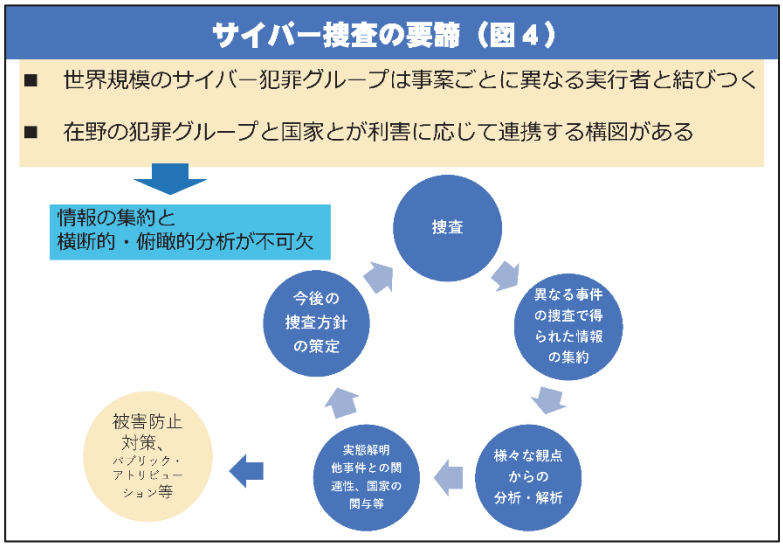
ア　サイバー捜査の要諦

先ほども述べたが、サイバー空間の脅威に関しては、

① 世界規模のサイバー犯罪グループは、匿流のように、大元の組織と実行者が事案ごとにアドホックに結びつくという側面がある。

② 在野の犯罪グループと国家とが双方の利害に応じて連携する構図があり、金銭目的の犯罪でもその実行者が間接的に国家につながる可能性がある。

という実態があるので、異なる事件（他部門主管のものもある）の捜査で得られた情報が適切に共有され、様々な観点からの分析を経て、他の事件との関連性、犯罪グループ相互のつながり、国家等の関与等の実態を解明し、次に、明らかになった他事件との関連性、犯罪グループ相互のつながり、国家等の関与等を踏まえ、今後の捜査方針を立てたり、次なる被害の防止対策の立案に活用したりするサイクルを回していくことが極めて重要である（図４）。

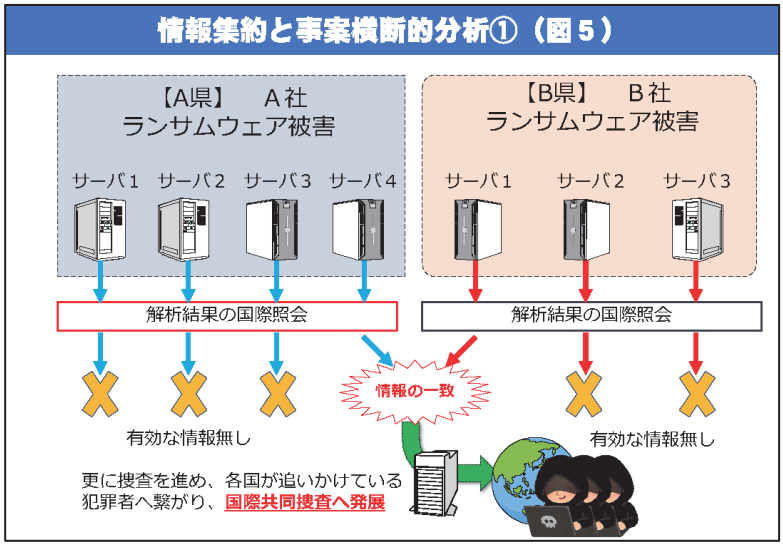


したがって、「事件単位の視点しか持たず、一つの事件が終結したらそこで終り」とか、「精緻な分析報告（プロダクト）を作り、上司や幹部に報告したらそれで満足（終わり）」というスタンスでは到底対応できない。

(2) 情報集約と事案横断的分析

このように、サイバー事案への対処に当たっては、ひとつの事件について「捜査を尽くせばそれで終わり」というわけではなく、個別の事件を超えた情報の集約と俯瞰的・横断的な分析体制が不可欠である。

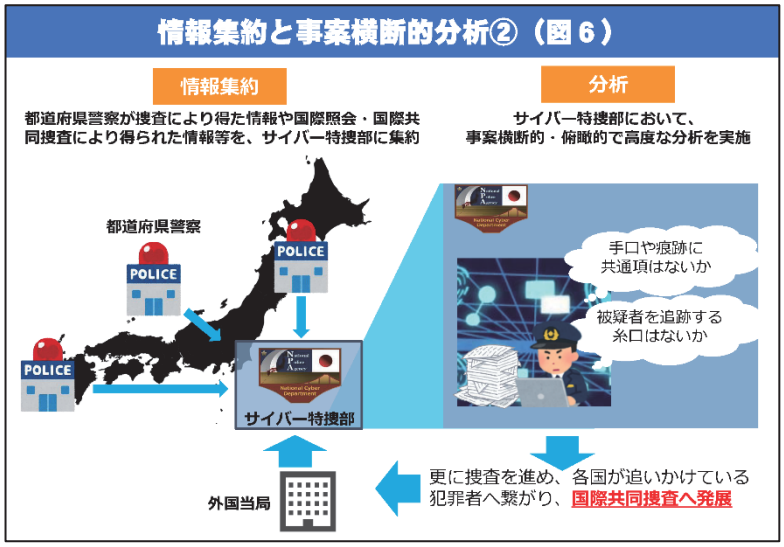
サイバー事案の捜査では、被害が発生した都道府県や踏み台サーバ（サイバー犯罪等を実行する際に中継ポイントとして利用されるサーバのこと。以下同じ。）の所在する都道府県など、関係する都道府県警察の捜査だけでは被疑者に直接つながるような有効な情報が得られることは稀である。そうであっても、各都道府県警察の捜査で得られた断片的な情報を集約し、別の都道府県で別の時期に発生した事件の捜査で得られた情報と突き合わせ、関連性を紡いで大きな絵を描くことが非常に重要である（図５）。



現在、サイバー特捜部には、俯瞰的・横断的分析等を行う「企画分析課」と重大サイバー事案に係る犯罪の捜査を行う「特別捜査課」が設置されている。

企画分析課に都道府県警察や特別捜査課の捜査で得られた情報を集約し、これに外国機関からの提供情報、OSINT 情報等を合わせて高度な分析、解析等を行い、結果を特別捜査課にフィードバックしている。

特別捜査課においては、この分析、解析の結果を国際共同捜査等更なる捜査の方針策定や実施に活用している（図６）。

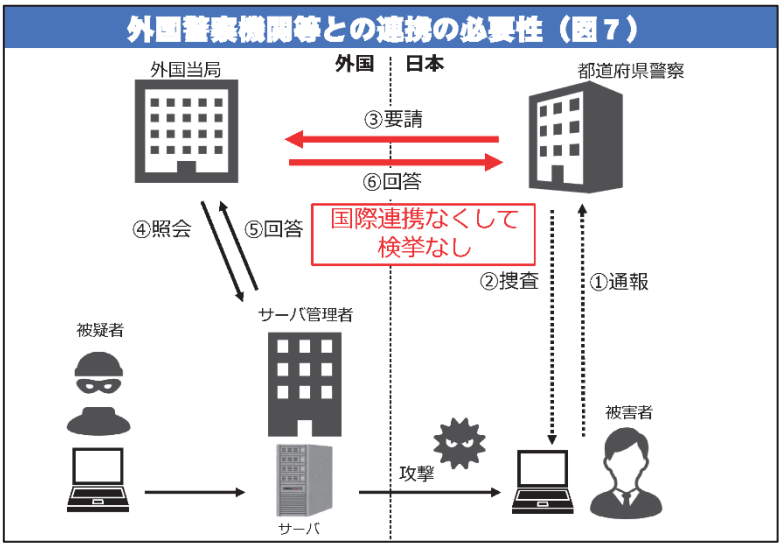


もちろん、サイバー部門で取り扱う情報の性格は様々であり、情報保全の観点から適切かつ厳格な運用を徹底した上で活用を図っていることを付言しておく。

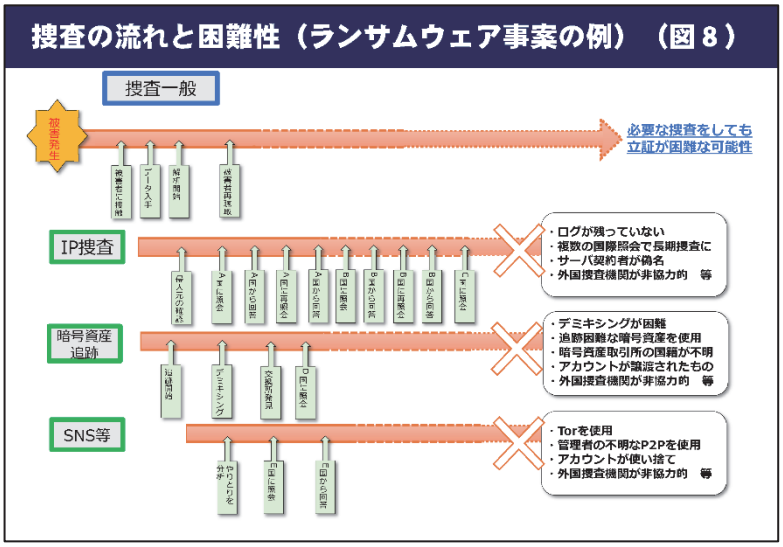
(3) 機動的な国際連携の推進

ア　外国警察機関等との連携の必要性

サイバー事案では、実行者が外国に所在するケースのほか、実行者が日本に所在する場合でも、踏み台サーバとして外国所在のサーバが悪用されたり、重要な証拠となりうるデータが外国所在のサーバに蔵置されていたりと、多かれ少なかれ国際捜査が必要となるケースが大半である（図７）。



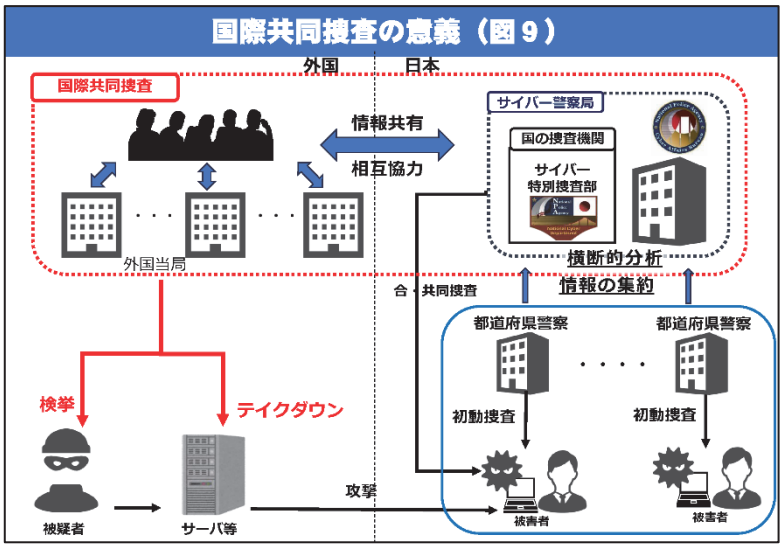
しかし、サイバー捜査の中核を構成する IP 捜査、暗号資産の追跡、SNS 等からの捜査はいずれも少なからざる困難を伴うものである。よって、以前は外国絡みの事案は、国際照会手続きに要する労力、時間といった捜査コストの高さの割に犯人の捕まる可能性が低いことが捜査着手へのモチベーションに影響していたことも否定できない（図８）。



イ　国際共同捜査の意義

このように、国際的なサイバー犯罪に関し、被害国の捜査機関はそれぞれ断片的な情報しか持ち合わせておらず、一国単独の捜査では全貌を把握することができないというのが一般的な構図である。これについては日本も他国も状況は同じである。

そこで、関係各国の捜査を通じて得られた情報を共有し、併せて捜査に関する知見を結集することで事案の全体像の解明、つまり国際的なレベルの情報の集約と横断的分析を行って犯人の検挙へと結びつけることが重要となる（図９）。



国際共同捜査の意義は正にこのようなところにある。

ウ　外国警察機関等との信頼関係の構築

国際共同捜査を推進する上で基盤となるのは各国との信頼関係であるが、これは一朝一夕

に作られるものではない。

強固な信頼関係を構築し、維持するため、警察庁では令和４年６月から、国際共同捜査のハブとなる欧州警察機構（ユーロポール）にサイバー専門の情報連絡官（リエゾンオフィサー）を常駐させ、関係国との間での情報交換や知見の共有に継続的に取り組んでいる（図 10）。

３　国際共同捜査への参画

(1) ユーロポールをハブとする国際共同捜査

サイバー特捜部は国の捜査機関として、ユーロポールをハブとする外国捜査機関と連携した複数の国際共同捜査に参画し、これまでランサムウェア被疑者の逮捕や関連する犯罪インフラの閉鎖（テイクダウン）を行うなどの成果が出ている。

外国警察から提供された情報については、内容を緻密に精査し、端緒を得るなどして、捜査に活用している。一般的には、外国警察から提供された情報を証拠化する場合、刑事共助条約・刑事共助協定に基づく手続きを要するが、この手続きには時間を要する場合もある。このため、各国捜査機関との協議等を通じ、手続きの迅速化等に努めている。

※　警察庁はユーロポールと「Working Arrangement（実務取決め）」を 2018 年に締結しており、国際共同捜査を実施する際、個人情報以外の情報については同取決めに基づいて警察庁とユーロポール加盟国との間で共有されている。他方、個人情報については、個々の加盟国と日本とが合意した上で、他の国際共同捜査参加国がこれに同意する形でやり取りする形をとっている。

(2) 国際共同捜査による検挙事例

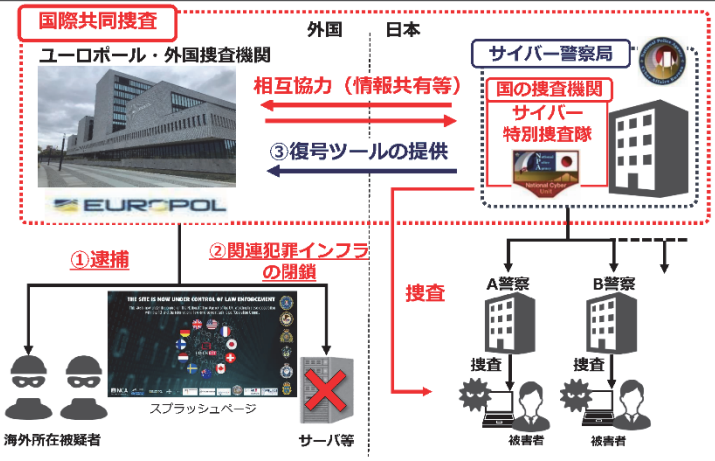
ア　世界規模で暗躍するランサムウェアグループの検挙

令和５年、名古屋港のコンテナターミナルシステムを攻撃し、経済活動に混乱を生じさせ

た国際的ランサムウェア攻撃グループ「ロックビット」に対する国際共同捜査のチャートを示す（図 11）。

我が国もユーロポール主催の国際捜査会議に出席し、サイバー特別捜査隊と関係都道府県警察の捜査によって得られた情報を提供するなど緊密に連携してきた。

国際共同捜査による海外ランサムウェア被疑者の逮捕等①（図11）

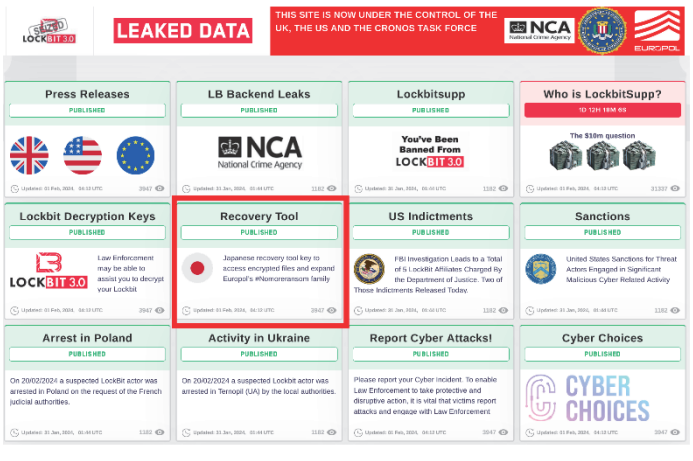


その結果、令和６年２月に関係各国の法執行機関が同グループの一員とみられる被疑者２名をウクライナ及びポーランド国内で逮捕するとともに、同グループの使用するサーバ等の犯罪インフラをテイクダウンした。

ランサムウェア攻撃グループが身代金の支払いに応じなかった被害者から窃取した情報を暴露するために運営していた「リークサイト」も閉鎖した。閉鎖後のページにアクセスすると、捜査機関側が用意したスプラッシュページ（「このサイトは法執行機関の管理下にある」旨の文言を示すウェブページ）が表示される。右側には捜査に参加した 12 カ国の国旗イメージと捜査機関のロゴが掲示されている。

この事案では、暗号化された被害データを復元することができるツールをサイバー特捜部が開発し、令和５年 12 月、ユーロポールを通じて関係国に共有するとともに、令和６年２月、世界中の被害企業の助けになるよう、ユーロポール等と共に情報発信するなど、国際場裏においても日本警察の存在感が増している（図 12）。

国際共同捜査による海外ランサムウェア被疑者の逮捕等②（図12）



引用：https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos?highlight=WyJjcm9ub3MiXQ==

その後も捜査は継続しており、令和６年５月には、英、米、豪当局が、同グループにおいてランサムウェアの開発・運営を行うロシア人被疑者の資産を凍結するとともに、同年９月にはグループの構成員４人

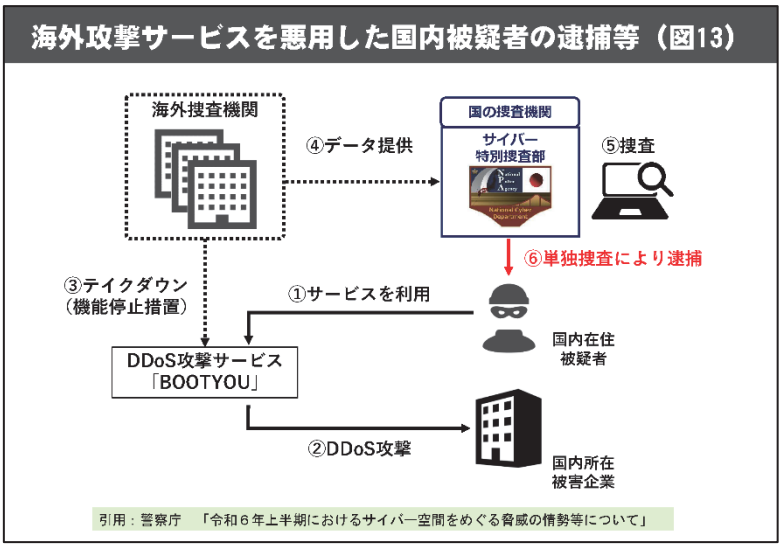
が英国、フランス及びスペインの当局に逮捕された。

イ　海外 DDoS 攻撃ウェブサービスを利用した国内攻撃事案被疑者の検挙

ユーロポール主導で米国と欧州の捜査機関が参画するサイバー攻撃の代行サービスを提供するような一連のサイトの封鎖を行う国際共同捜査が平成 30 (2018) 年以降継続している。

警察庁は令和５年９月からこの捜査に参加し、その中で日本に対する攻撃の情報が外国捜査機関からサイバー特捜部に提供された。

提供を受けた情報を分析したところ、国内居住の男が令和５年３月に都内の出版社のウェブサイトに攻撃を行い、一時閲覧不能状態にしていたことが判明したことから、令和６年８月、同人を電子計算機損壊等業務妨害の容疑で逮捕した（図 13）



このように、日本警察が参加した国際共同捜査において犯人が検挙される実績が積み上がると、犯罪者側に、国際共同捜査に参加するような国である日本に対してサイバー犯罪を敢行しようとした際に「検挙されるかもしれない」との心理的な効果がもたらされ、サイバー犯罪の抑止にもつながることが期待される。

また、被疑者検挙の具体的なイメージを持ちながら捜査を進めるようになったことで、我が国の捜査員の士気の高揚と練度の向上につながっている側面もある。

4　サイバー捜査のスコープの拡大

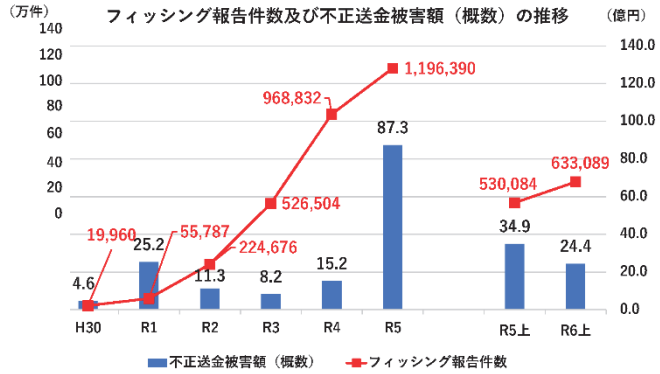
(1) サイバー空間への匿流の進出

「警戒の空白を生じさせないための組織運営の指針」等では、事件主管課のみでは対処が困難な捜査事項について、サイバー部門において的確な支援体制を確保することが求められている。これを踏まえ、サイバー特捜部はその分析、解析等の能力を活かし、部門を問わず様々な犯罪捜査に貢献している。

最近の特徴として、サイバー特捜部の捜査のスコープが拡大していることが挙げられる。

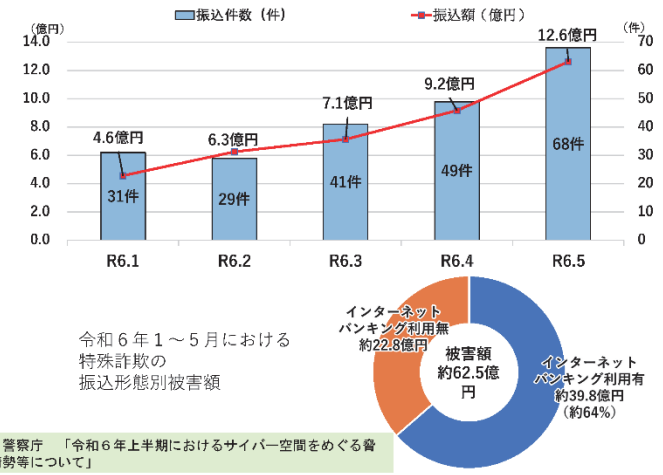
現下最大の治安課題である匿流による犯罪においても、サイバー空間や新たな技術が悪用されている実態があり、匿流に対する捜査においてサイバー捜査の知見や手法が有効となるケースも多い。まず注目したいのがインターネットバンキングの不正送金の被害増加である。同事犯の令和５年の被害件数は 5,578 件、被害額は約 87.3 億円と前年から急増し、いずれも過去最悪となった（図 14､図 15）。以前は中国の犯罪グループによる犯行が目立っていたが、ここまで被害が急増した背景には匿流の進出が窺われる。

インターネットバンキングに係る不正送金被害（図14）



引用：警察庁　「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

特殊詐欺におけるインターネットバンキングを利用した振込被害（図15）



引用：警察庁　「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

このように匿流による犯罪においても、サイバー空間や新たな技術が悪用されている実態がある。

(2) 暗号資産追跡の取組

ア　暗号資産による犯罪収益の隠匿

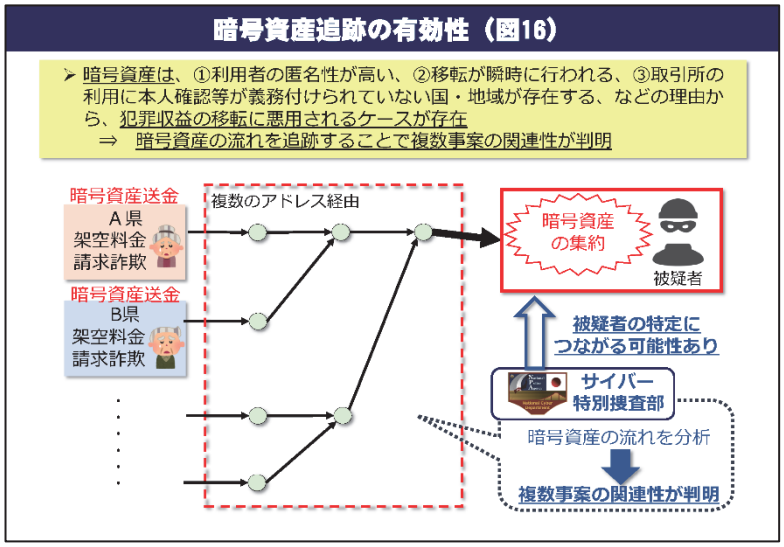
暗号資産は取引の匿名性が高く、移転が瞬時に行われること等の理由から、近年は特殊詐欺やネットバンキング不正送金事犯で得た収益を匿名性の高い暗号資産に移転して隠匿する手口が見られる。

サイバー警察局では暗号資産の追跡能力の重要性を認識しており、ミキシング（複数種類のコインアドレス群を経由させて追跡を困難にする手法）のような移転状況の追跡を困難にする技術・手法に対抗するため、追跡技術の研究を推進するとともに、国際連携を通じた追跡能力の強化に継続して取り組んでいる。具体的には、民間企業等（JC3 や Chainalysis 社）の各種研修に加え、ユーロポールやインターポール主催のフォーラム等への参加、海外捜査機関との情報交換等を通じて追跡能力の強化を図っている。

イ　暗号資産追跡の有効性

サイバー事案に限らず、様々な犯罪収益の隠匿に暗号資産が悪用される中、サイバー特捜部では、個々の事件捜査における移転状況の追跡にとどまらず、その追跡結果を罪種、部門を問わず集約し、横断的・俯瞰的な分析を実施している。分析においては、資金の送金先や被疑者の特定だけでなく、別の時期に別の場所で発生した他事案との関係性の解明を進めており、その結果は都道府県警察と適切に共有されている。

こうした取組により、例えば、インターネットバンキングに係る不正送金事犯と別の特殊詐欺事案に関して同一被疑者の関与が判明するなど、従来の捜査では必ずしも明らかにならなかった複数事案相互の関連性や、背景にある組織性が浮き彫りになっているところである（図 16）。



(3) 検挙事例

暗号資産の追跡及び横断的・俯瞰的分析が特殊詐欺被疑者の検挙に結びついた事例を２つ取り上げる。

ア　サイバー保険名目の架空請求詐欺事犯

令和５年、愛知県内の女性がサイバー保険名目の架空請求詐欺に遭い、約 1,760 万円を騙し取られた事案が発生し、愛知県警察が捜査を開始した。（同グループでは被害者を欺罔する架け子、口座の調達係、マネロン担当などの分業化が進み、指示役の統率下、組織的な犯行を行っていた。）

被害金の全てが国内の暗号資産取引所の振込用口座に送金され、その後、暗号資産に換えて移動している状況が認められたことから、サイバー特別捜査隊（当時）が暗号資産の追跡を支援。この結果、他都道府県警察で捜査中の事案との関係性が判明。調整の結果、５県警察からなる合同捜査本部が設置される。サイバー特別捜査隊による暗号資産の分析支援等により、被疑者らが経営する会社法人名義のアカウントに再度収束し、現金化されている状況

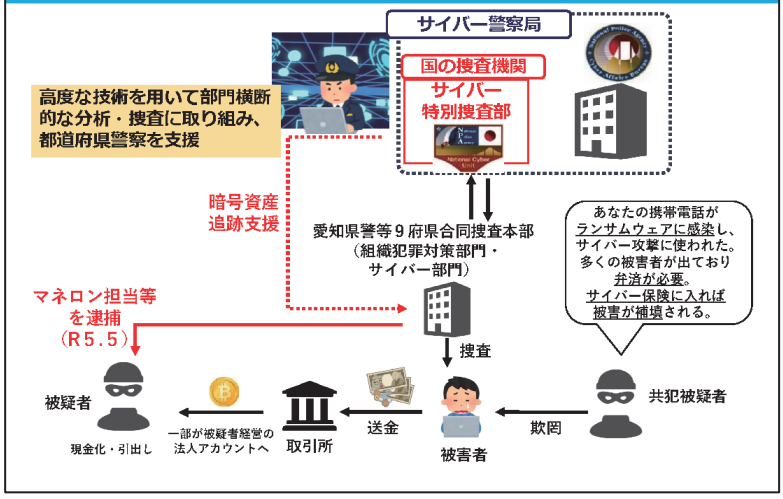
を特定。令和５年５月、合同捜査本部が法人代表及び実質的経営者の男２名を検挙した（図 17）。

イ　組織的インターネットバンキング不正送金事犯

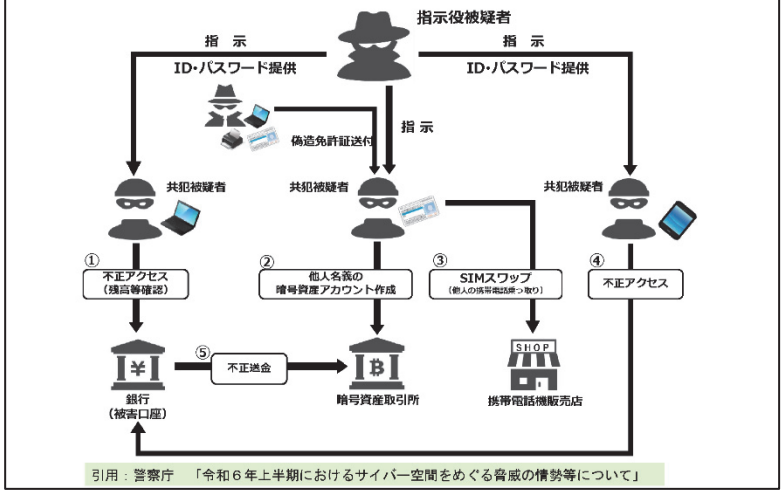
令和 4 年から 5 年にかけて発生した複数のインターネットバンキングに係る不正送金事件について指示役を含む被疑者を検挙した事例である（図 18）。

関係都道府県警察の捜査で得られた情報をサイバー特捜部に集約し、暗号資産の追跡捜査や関係被疑者の SNS アカウントに係る捜査等を実施したところ、複数の都道府県警察が捜査していた事案は同一の犯行グループが組織的に不正送金を敢行している実態が判明した（被害件数及び被害額は少なくとも 20 件・1 億 2,000 万円）。

暗号資産追跡等による特殊詐欺事件被疑者の逮捕（図17）



組織的インターネットバンキング不正送金事犯の概要（図18）



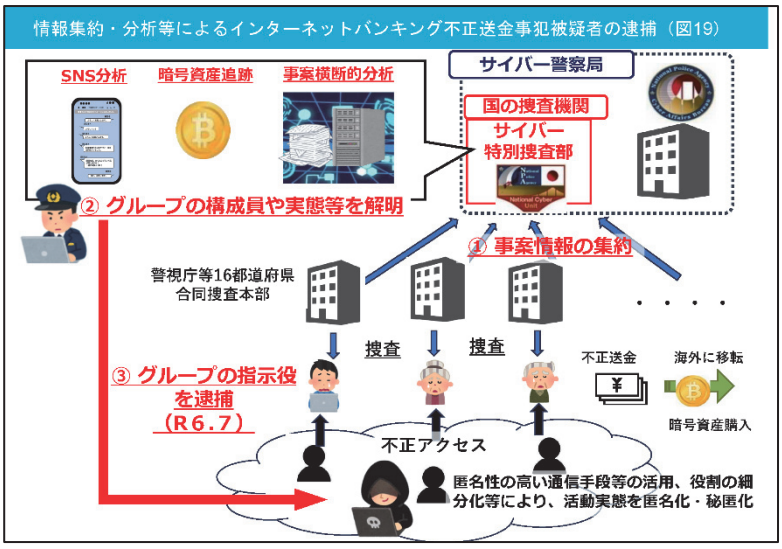
このため、当初、個別に捜査していた１６都道府県警察とサイバー特捜部との合同捜査本部を設置して捜査を行ったところ、解明された犯行の構図は以下のとおりであった。

指示役の被疑者は、何らかの方法（フィッシング、マルウェアによる窃取、ダークウェブでの取引等）により入手した正規利用者の ID/パスワードを使ってインターネットバンキングに不正アクセスし、氏名、生年月日、携帯電話番号等の個人情報を入手。それを使って SNS で募集した共犯者の顔写真を使って正規利用者名義の免許証を偽造。本人が契約する携帯電話事業者の店舗に共犯者が赴いて正規利用者になりすました偽造免許証を提示しつつ、携帯電話の紛失を口実に SIM カードの再発行を受け、携帯電話を乗っ取る。

乗っ取った携帯電話を用いてインターネットバンキング取引時の二要素認証である SMS 認証を突破し、不正送金を実行する。得られた犯罪収益は暗号資産に移転して隠匿するという

もの（図 19）。

都道府県警察から集約された情報の横断的分析、不正送金の被害金の追跡捜査等によって判明した事実に基づく国際照会等により、犯罪組織の活動実態を解明するとともに、犯行グループの指示役を特定し、令和６年７月、不正アクセス禁止法違反で逮捕した。



ウ　今後の捜査体制の更なる強化に向けて

このほかにも組織的なクレジットカード情報不正利用事犯やリバトングループによるマネロン事犯等でサイバー特捜部による暗号資産の追跡及び事案横断的分析が犯人検挙に貢献している。

現在、サイバー特捜部では、刑事・組織犯罪対策部門からの人材を積極的に受け入れている。サイバー特捜部の任期を終えて出身都道府県警察に帰任した後は、サイバー特捜部での勤務で得られた知見、人脈等を活用、還元し、部門・分野を問わず第一線における対処能力の底上げに裨益してもらうことを期待している。

5　今後の課題と展望

最後に、サイバー捜査に関する今後の課題及び展望について簡潔に触れる。

いずれも本研究部会のテーマとして今後取り上げるべきものと考えている。

端的に言うと、我が国の現状は、技術の進化やサービスの進展に法制度等が追いついていないというものである（図 20）。

今後の課題と展望（図20）

安全・安心なデジタル社会実現のための環境整備

- 生成AI等の高度な技術、新たなサービスを悪用した犯罪への対応
- 犯罪収益の剥奪、本人確認等に関する制度整備
- 新たな捜査手法の導入

(1) 生成AI等新たな技術・サービスを悪用した犯罪への対処

生成AIが、巧妙な標的型メール攻撃やディープフェイクによるなりすまし詐欺、影響工作等に悪用される可能性など、技術の進歩に伴い新たに出現するリスクにも目を向けていく必要がある。民間事業者等とも連携しながら新しい技術やサービスをキャッチアップして、対処能力を身につけていくことが重要と考えている。

また、警察においてもAI技術に関する専門人材の確保・育成に取り組んでいく必要がある。

(2) 犯罪収益の剥奪、本人確認等に関する制度の整備

犯罪収益を犯罪活動への再投資に利用されることを防止し、犯罪の実行を割の合わないものとするためには、犯罪収益の剥奪が非常に重要である。

我が国では、没収は付加刑として刑事裁判での有罪認定がないと実施できない一方、警察では判決前に犯罪収益の隠匿や消費等が行われることがないよう、組織的犯罪処罰法及び麻薬特例法に定める起訴前の没収保全措置を積極的に活用することで実効性を確保している。令和５年改正された組織犯罪処罰法では暗号資産も没収対象になったことから、犯罪収益の剥奪を積極的に進めていく必要がある。

また、検挙事例で見たように、データ通信用携帯SIMカードが多数の犯罪に悪用されている実態があるのに、SIMカード販売時の本人確認がいまだに任意であり、それすら身分証の券面を目視確認するだけの形式的なものとなっている。その結果、精巧な偽造免許証などを提示されて担当者が簡単に騙されるケースが跡を絶たないところ、関係省庁が連携してデジタル技術による公的個人認証基盤の活用等を進めていくことが求められる。

(3) 新たな捜査手法の導入

囮捜査の実施や通信傍受法の適用拡大についても他の民主主義国家の取組を研究し、導入に向けた検討を進める必要がある。

AI技術については、違法・有害情報検索の効率化等において警察活動への導入が既に開始されている。

今後、捜査をはじめとする犯罪対策へのAI技術の導入は不可欠であると考える。透明性を確保した運用の在り方も含めて研究・検討していくべきであろう。

【追記】第 41 回犯罪対策閣僚会議の開催

令和６年 12 月 17 日、第 41 回犯罪対策閣僚会議が開催された。同会議では、同年８月以降、SNS 等を使って実行犯を募集するいわゆる「闇バイト」による強盗事件等が相次いで発生したことを受け、「国民を詐欺から守るための総合対策」（令和６年６月 18 日犯罪対策閣僚会議決定）に基づき推進してきた各種対策のフォローアップも含め、「いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策」（令和６年 12 月 17 日犯罪対策閣僚会議決定）が取りまとめられた。具体的には、

① 「被害に遭わせない」ための対策

- SNS 等を利用した犯罪の捜査上の課題に対応するための SNS アカウントの開設時の本人確認の強化を含む措置について検討を行うほか、事業者に対して本人確認の厳格化を要請する　等

② 「犯行に加担させない」ための対策

- 検討中の違法情報ガイドラインにおいて、「闇バイト」を募集することや、募集者の氏名等が含まれていない募集広告等が職業安定法等に違反する旨の記載を盛り込む方向で検討を進める。あわせて、プラットフォーム事業者に対し、同ガイドラインにおける記載内容を各者の削除等に関する基準に盛り込むよう求める　等

③ 「犯罪者のツールを奪う」ための対策

- 被害金の追跡を行うに当たって、金融機関への照会・回答の迅速化を図る　等

④ 「犯罪者を逃がさない」ための対策

- 現行法の範囲内で実施可能な仮装身分捜査の在り方を検討し、ガイドライン等で明確化した上で、早期に仮装身分捜査を実施する
- 警察におけるサイバー犯罪対策部門の更なる体制強化、各種装備資機材の充実強化、幹部警察官や技術系職員を含む警察職員に対するサイバー教育の更なる充実強化に取り組むほか、更なる情報技術解析の高度化に向け、外国機関との連携等を行う
- 諸外国の例を参考にした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・検討を行う　等

の施策を強化・拡充することとされた。

（引用元：いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策（抜粋）https://www.kantei.go.jp/jp/singi/hanzai/kettei/241217/kinkyu_taisaku.pdf

警察政策学会資料　第 140 号

サイバー捜査の課題と展望について

令和 7（2025）年 2 月

編集　警察政策学会
　　刑事警察研究部会

発行　警察政策学会

〒 102-0093
東京都千代田区平河町 1-5-5　後藤ビル 2 階
電話（03）3230-2918・(03-3230-7520)
FAX（03）3230-7007