５　年　保　存
令和13年３月31日満了

ＦＮｏ．－01010802
崎務（企）第５９号
崎安（抑）第７８号
崎サ（企）第５９号
崎刑（企）第２８号
崎組（特詐）第39号
崎組（匿流）第12号
令和７年５月１４日

各　部　長
　　殿
各所属長

長崎県警察本部長

「国民を詐欺から守るための総合対策2.0」の決定について（通達）

警察においては、「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。以下「総合対策」という。）及び「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）に基づき、各種対策を強力に推進してきたところであるが、一層複雑化・巧妙化する詐欺等の手口の変化に応じて機敏に対策を改善するとともに、犯罪グループを摘発するための実態解明の取組や犯罪グループと被害者との接点の遮断といった抜本的な改革を強化するため、僚対策を統合する形で総合対策を改定し、令和７年４月22日、第42回犯罪対策閣僚会議において、別添「国民を詐欺から守るための総合対策2.0」が決定された。

各位にあっては、本総合対策の趣旨及び内容を踏まえ、関係機関・団体等とも連携しつつ、諸対策を強力に推進されたい。

担当	警務部警務課企画室企画第一係（2630・2633）

国民を詐欺から守るための総合対策 2.0

令和７年４月 22 日

犯罪対策閣僚会議

序　「国民を詐欺から守るための総合対策」の改定に当たって

令和６年中の財産犯の被害額は 4,000 億円を超え、これは刑法犯認知件数が過去最悪であった平成 14 年当時の被害を上回る額であり、極めて憂慮すべき状況にある。特に詐欺被害が急増しており、令和６年中の詐欺の被害額は 3,000 億円を上回った。詐欺は人の信頼を逆手に取り、これをだまして財産を奪い取る卑劣な犯罪であり、その急増によって、「国民が互いに寄せる信頼」という様々な社会・経済活動を円滑に行うに当たり不可欠な安全・安心な社会を支える基盤が揺らいでいる。また、組織的に詐欺を行う犯罪グループの拠点が東南アジア等の海外にも所在し、こうした拠点での詐欺に日本人が加担している事例が発生するなど、海外の犯罪動向が日本の治安に直結している。

政府はこれまで、令和６年６月に、詐欺全般に特化した初めての総合対策として「国民を詐欺から守るための総合対策」を策定し、詐欺等の被害を食い止め、信頼を基礎とする我が国社会の健全な発展、安全・安心な社会の実現を図るための施策を強力に推進してきた。

また、令和６年 12 月には、これまでの各種施策の進捗状況を点検した上で、更に一歩踏み込んだ対策を行うため、「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」を取りまとめ、ＳＮＳ等を使って実行犯を募集する、いわゆる「闇バイト」による強盗事件等への対策を講じてきた。

さらに、令和５年 12 月に開催されたＧ７茨城水戸内務・安全担当大臣会合や令和６年３月に英国で開催された国際詐欺サミットをはじめ、様々な国際会議を通じて、組織的な詐欺に対する各国との連携強化を推進してきた。

海外に所在する詐欺グループに対しては、外国当局による摘発への協力や、国連薬物・犯罪事務所（ＵＮＯＤＣ）等の国際機関と連携し、外国の法執行機関の取締能力を強化する支援を実施している。

しかしながら、こうした官民を挙げた対策が進むにつれ、犯人側は、それに応じて手口を巧妙に変化させている。

ＳＮＳ型投資詐欺では、著名人になりすます偽広告を含むバナー等広告の悪用は減少に転じたのに対し、ＳＮＳのダイレクトメッセージの悪用が増加し、バナー等広告を上回るようになっている。また、ＳＮＳ型ロマンス詐欺については、認知件数・被害額共に増加傾向にあるところ、特にマッチングアプリを利用した被害が目立っている状況にある。その結果、令和６年中のＳＮＳ型投資・ロマンス詐欺の被害額は約 1,268 億円と、前年の約３倍に増加している。

また、特殊詐欺では、警察官等をかたるオレオレ詐欺の被害が顕著であるほか、インターネットバンキングの利用による被害の高額化や固定電話のみならず携帯電話への国際電話番号による架電の増加がうかがわれる。その結果、令和６年中の特殊詐欺の被害額は約 722 億円と、平成 26 年の過去最高被害額（約 566 億

円）を超えている。
　さらに、キャッシュレス決済の利用の拡大等を背景に、正規の企業のサイトを模したフィッシングサイト等により、ＩＤ・パスワード等を不正に入手し、不正送金等を行うフィッシングによる被害も拡大しており、令和６年中のインターネットバンキングに係る不正送金事案による被害額は約 87 億円と高水準で推移したほか、クレジットカード不正利用被害額は約 555 億円[1]と過去最多となった。

　こうした情勢の中、一層複雑化・巧妙化する詐欺等について、立ち後れることなく、国民をその被害から守るためには、手口の変化に応じて機敏に対策をアップデートすることに加え、犯罪グループを摘発するための実態解明の取組や犯罪グループと被害者との接点の遮断といった抜本的な対策を強化する必要がある。そこで、今般、「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」を統合する形で「国民を詐欺から守るための総合対策」を改定し、政府を挙げた詐欺等に対する取組を抜本的に強化することとした。
　詐欺等の被害を食い止め、信頼を基礎とする我が国社会の健全な発展、安全・安心な社会の実現を図るため、各省庁等は、本総合対策に基づき、地方公共団体、民間事業者、外国当局や国際機関等国際社会とも連携・協力しながら、各種施策を一層強力に推進することとする。

[1] 一般社団法人日本クレジット協会の資料による

１　ＳＮＳ型投資・ロマンス詐欺対策

(1)　犯行準備段階への対策

ア　各種サービスやインフラの不正利用を防止するための取組

(ｱ)　利用者の本人確認強化等

①　ＳＮＳ事業者に係る本人確認の厳格化

総合対策[2]及び緊急対策[3]において、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推進してきたところ、一部事業者が運営するＳＮＳについては、依然メールアドレスのみでアカウント開設が可能であり、また、電話番号により認証を行っているＳＮＳについても、不正に取得された電話番号等を利用してＳＭＳ認証が行われている実態があることから、引き続き、ＳＮＳ事業者に対して、アカウント開設時に本人確認の厳格化を含む措置の検討を働き掛ける。

②　マッチングアプリ運営事業者に係る本人確認の厳格化

総合対策において、マッチングアプリアカウントの開設時の本人確認の強化を推進してきたところ、未だ本人確認が不十分であり、マッチングアプリアカウントが犯罪に悪用されていることから、アカウント開設時に、引き続き公的個人認証サービス等を用いたより厳格な本人確認を実施するよう働き掛ける。

③　音声通信ＳＩＭの契約時における本人確認の義務付け

総合対策において、携帯電話不正利用防止法に基づく携帯電話の契約時の非対面の本人確認手法を、マイナンバーカードの公的個人認証に原則として一本化し、運転免許証等を送信する方法や、顔写真のない本人確認書類等を使用する方法による本人確認は廃止するとともに、対面でもマイナンバーカード等のＩＣチップ情報の読み取りを義務付けることとしてきたところ、引き続き、所要の制度改正を実施する。

④　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

総合対策を踏まえ、データ通信専用ＳＩＭの不正利用の実態について調査を行った結果、契約時に本人確認書類を用いない本人確認手法を悪用し、不正に取得したログインＩＤやパスワードを用いて大量のデータ通信専用を含む通信用ＳＩＭを不正に契約した事例や、

---

[2]「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）

[3]「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）

通信アプリケーションソフトウェア等のアカウントの不正取得に悪用されているなどの事例が確認された。一部の事業者においては自主的な確認も行われている一方で、携帯電話不正利用防止法上、契約時の本人確認が義務化されていないデータ通信専用ＳＩＭの犯行ツールとしての悪用の可能性が今後も懸念されるため、データ通信専用ＳＩＭについても、引き続き悪用実態も把握しつつ、それらを踏まえ、電気通信事業者に対して、契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討する。

⑤　預貯金口座等の不正な開設、譲渡等への対策

総合対策において、警察から金融機関等に対し、不正な口座開設に係る手口等の情報を提供するなど、金融機関等と連携し対策に取り組んできたが、依然として預貯金口座等の不正な開設、譲渡が後を絶たないことや、新たな手口としてＳＮＳ等で勧誘を受けるなどし、他人に依頼されて送金を行う行為が増加していることから、こうした詐欺等に加担する行為について、広報啓発活動を推進する。

預貯金口座等の不正な譲渡等については、最近の手口や実務上の課題等を把握した上で、罰則の引上げを含めた法令の見直しを検討する。

また、帰国する在留外国人から不正に譲渡された預貯金口座の悪用を防止するため、在留期間が満了した外国人の預貯金口座からの現金出金及び他口座への振込が行われる場合には、在留期間の更新等の有無を確認し、確認できるまでの間は現金出金等が行われないことについて在留外国人に対する広報等を進める。

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、会社法や一般社団法人及び一般財団法人に関する法律により求められている定款の認証に際して行われる公証人への申告や、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する。

加えて、偽変造された本人確認書類により開設された架空・他人名義の預貯金口座等が詐欺等に利用されていることから、こうしたなりすまし等を防止するため、犯罪収益移転防止法に基づく口座開設時等の非対面の本人確認方法を、マイナンバーカードの公的個人認

証に原則として一本化し、対面でもマイナンバーカード等のＩＣチップ情報の読み取りを義務付ける取組を早期に推進する。

⑥　犯罪収益移転防止法の適正な履行の確保

一部の特定事業者が、行政処分を逃れるために、処分前に廃業し、その直後に名ばかりの代表者を据えて起業するといった実態があり、犯罪収益移転防止法に基づく報告徴収、意見陳述、是正命令という一連のスキームによる是正が妨げられていることから、こうした事業者への対応策について検討する。

(ｲ)　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

総合対策において、預貯金口座や携帯電話等の各種サービスやインフラの不正利用を防止するための取組を推進してきたところ、ＳＮＳ上で「本人確認案件」等と称して、これらを不正に開設、売却させる犯罪実行者の募集行為が横行しており、それらに複数回応募し、多数の預貯金口座等を犯罪者グループに提供する者の存在も確認されていることから、１つの事業者で判明した不正利用者の情報を共有して、各事業者において関連する登録情報等の有無を確認し、不正利用防止に役立てるための枠組みの構築について検討する。

(ｳ)　犯行に利用されたアカウント等の利用停止措置の推進

総合対策において、犯行に利用されたＳＮＳアカウント等について、警察からＳＮＳ事業者等に情報提供を行い、速やかに利用停止を促すスキームの構築について検討し、一部ＳＮＳ事業者等との間で同スキームを構築し、運用を開始したところ、今後は、同スキームを構築するＳＮＳ事業者等を拡大する。

(ｴ)　犯行に利用された預貯金口座の凍結等

総合対策において、特殊詐欺やＳＮＳ型投資・ロマンス詐欺の犯行に利用された法人口座を含む預貯金口座について、金融機関に対する迅速な口座凍結依頼を実施してきたところ、引き続き、この取組を推進する。

また、引き続き、特殊詐欺等の犯行に利用されて凍結された預貯金口座の名義人のリストを警察庁が作成し、一般社団法人全国銀行協会等へ提供することにより、不正口座の開設の防止を推進する。

(ｵ)　在留外国人等に対する広報・啓発の実施

総合対策において、在留外国人に対する携帯電話・預貯金口座の不正譲渡の違法性に関する広報・啓発や、日本に新たに入国する技能実習生等及びその受入機関に対する携帯電話・預貯金口座の不正譲渡の防止

のための周知・啓発に取り組んできたところ、引き続き、これらの取組を推進する。

また、引き続き、在外公館においても上記広報・啓発資料を掲示及び配布、公館ウェブサイトに掲載するなど、未然防止に努める。

(ｶ) 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

緊急対策において、インターネットサービスの悪用の実効的排除に資する諸外国の法制度に関する調査・検討に取り組んできたところ、引き続き、総務省の有識者会議において調査・検討を行う。

イ 犯罪への加担を防止するための取組

(ｱ) 犯罪実行者募集情報の削除等の取組

① 「インターネット・ホットラインセンター」等の効果的な運用

総合対策において、犯罪実行者募集情報に関する情報収集、削除、取締り等を推進しているところ、緊急対策も踏まえ、令和７年２月、インターネット利用者等からの違法情報等に関する通報の受理、警察への通報、サイト管理者への削除要請等を行う「インターネット・ホットラインセンター」のガイドラインを改定し、犯罪実行者募集情報を違法情報としてサイト管理者等へ削除依頼を行うことが可能となった。その上で、同年３月から当該運用を開始するとともに、取り扱う情報の拡充に伴い、情報分析等のために「インターネット・ホットラインセンター」の体制を強化した。引き続き、国民に対し、「インターネット・ホットラインセンター」に対する情報提供を呼び掛けるとともに、「インターネット・ホットラインセンター」等の効果的な運用により、犯罪実行者募集情報の排除に向けた対策を推進する。

② リプライ機能を活用した個別警告等の更なる高度化

総合対策において、ＳＮＳ上で発信される犯罪実行者募集情報への対策として、ＡＩを活用し、返信（リプライ）機能を利用した投稿者等に対する個別警告等を推進してきたところ、犯罪実行者募集情報と検知されないよう、隠語や画像等を利用して巧妙に偽装する手口も見られることから、手口の変化に機動的に対応し、警告の対象となる投稿の抽出精度の更なる向上を目指すとともに、より効率的・効果的な運用方法を検討する。

③ 犯罪実行者募集情報に対するＡＩ技術等を活用した対策に係る検討

総合対策において、犯罪実行者募集情報の削除等の対策を推進してきたところ、犯罪者グループは複数のＳＮＳアカウントを用意し、連続的に投稿を行うなどすることで、アカウントの凍結や投稿の削

除への対抗措置を講じるなどしていることから、犯罪実行者募集情報に関して、ＡＩ等の先端技術等を活用したより一層高度な対策について検討する。

④　犯罪実行者募集情報に対する事業者による削除・掲載防止の推進

総合対策及び緊急対策において、犯罪実行者募集情報の実効的な削除に資する取組を推進してきたところ、引き続き、ＳＮＳ事業者及び雇用仲介事業者における、犯罪実行者募集情報の削除及び掲載防止等の取組を促進する。

(ｲ)　広報啓発の媒体や方法の拡充

総合対策及び緊急対策において、広報・啓発の内容の拡充を図るとともに、ターゲティング広告やアドトラック等を活用し、その媒体や方法の拡充に取り組んできたところ、依然としてＳＮＳ上及び求人サイト等において犯罪実行者募集情報に応募した者が犯罪に加担してしまう事例が確認されており、犯罪に加担させないための広報・啓発は、年齢層や地域等を考慮し、より効果的な手法によって実施される必要があることから、引き続き、訴求力の高い著名人の協力をはじめとした効果的な広報・啓発の内容並びに媒体及び方法の検討について、関係省庁が連携して取り組む。

加えて、知人等から仕事を紹介されるなどして海外に渡航した結果、東南アジアを中心とする海外において、特殊詐欺事件の「かけ子」等として犯罪に加担させられる事案も発生していることから、関係省庁・関係機関が連携し、国内外における注意喚起及び相談窓口の周知を徹底する。

(ｳ)　青少年の特性を踏まえた広報・啓発の推進

総合対策において、青少年が事の重大性を認識することなく、安易な考えからＳＮＳ等における犯罪実行者募集情報に応じた結果、自身や家族に危害を加えるなどと脅迫され、犯罪に加担してしまうことがないよう教育・啓発を推進してきたところ、児童・生徒等に加え、有職・無職少年等の学校に通っていない少年にもそのような危険性について浸透させる必要がある。加えて、青少年は知人等からの誘いに応じて犯罪に加担する場合も多いことを踏まえ、引き続き関係省庁・関係機関が連携し、防犯教室や非行防止教室等の様々な機会やＳＮＳ等の広報媒体を活用し、検挙事例・トラブル事例等を交えながら具体的な情報発信を行う。

また、引き続き、情報モラル教育の着実な実施を図るとともに、詐欺等の犯行に加担した少年の再非行防止の対策として、少年院等の関

係機関と連携した非行防止教室を開催するなど、少年の立ち直りに向けた再非行防止のための取組を推進する。

(ｴ)　犯罪グループの人的基盤となり得る非行集団等への対策

非行少年の緩やかなネットワークも含め、犯罪グループの人的基盤となり得る非行集団等に対する実態把握を強化し、違法行為の取締り、事件検挙等を通じて非行集団等からの少年の離脱に向けた取組を推進する。

(ｵ)　犯罪実行者募集情報に応募した者等の保護等

総合対策及び緊急対策において「犯行に加担させないための対策」を推進してきたところ、犯罪実行者募集情報に応募して犯罪に加担しようとする者の中には、自身や家族に危害を加えるなどと脅迫されていることを理由に犯罪に加担しようとする者もいることから、そのような者から相談があった場合には、状況に応じて、保護措置を講じること等により適切に対処する必要がある。警察では、犯罪に加担しようとする者に対する呼び掛けを実施し、相談者やその家族等の関係者を保護しているところ、引き続き、保護対策に間隙を生じさせないよう、体制を強化するとともに、必要な資機材の整備等を推進する。

(2)　着手段階への対策

ア　ＳＮＳ事業者・マッチングアプリ事業者等におけるスパム行為防止措置の強化

総合対策において、ＳＮＳ事業者等による実効的な広告審査等を行うよう働き掛けてきたところ、ＳＮＳ型投資詐欺の初期の接触手段としては、バナー等広告が減少する一方で、ダイレクトメッセージを悪用する被害が増加しており、ＳＮＳ型ロマンス詐欺においてはダイレクトメッセージを悪用した被害が依然多い。特に、ダイレクトメッセージにおいては、知らない人からのメッセージを契機とした詐欺行為が多いことから、詐欺に誘引するダイレクトメッセージ等が被害者等の端末に届く前に、事業者において、不審な者からのダイレクトメッセージ等をフィルターする取組や利用者が詐欺に誘引するダイレクトメッセージ等を受信した際に警告表示を行う取組を推進する。また、これらの取組は、常に手口の変化に対応した効果的な対策を推進していくとともに、被害防止に資する取組の実施が困難であれば実効性のある制度整備等を検討する。

イ　ＳＮＳ事業者等による実効的な広告審査等の推進

ＳＮＳ上のなりすまし型の偽広告については、バナー等広告から誘引する手口による被害が依然として発生していることから、総合対策を踏まえＳＮＳ事業者等に対して実施した要請に基づき、広告審査の強化、広

告出稿者の本人確認の強化、詐欺広告や詐欺に使用されたアカウントの削除等の適切かつ迅速な対応等に関する対応状況について令和６年10月にヒアリングを実施するとともに、同年11月にその評価を「ヒアリング総括」として公表した上で、各事業者に対して更なる対応の改善を求めた。当該改善状況について今後もモニタリング結果を踏まえ詐欺被害防止及び利用者保護に資する更なる対策を講じることを働き掛ける。

また、正規の広告主の利益が害されないようにする観点から、プラットフォーム事業者の広告審査の取組等についてデジタルプラットフォーム取引透明化法に基づく令和６年度のモニタリング・レビューの中で取り上げ、令和７年２月に公表された令和６年度の経済産業大臣評価において評価を行った。この論点に係る各プラットフォーム事業者の取組状況については、引き続き令和７年度の同モニタリング・レビューを通じて確認を行う。

ウ　投資詐欺サイトへの対策

総合対策において、投資詐欺サイトについて、閲覧者への注意喚起等を実施してきたところ、依然として、投資詐欺サイトを入口とした被害が認められることから、引き続き、注意喚起を実施していくとともに、フィルタリング機能を活用した海外の詐欺サイトの閲覧防止や、国内の詐欺サイトの確実な削除を推進する。

エ　金融商品取引法上の無登録業者への対策等

総合対策において、無登録業者等による広告の掲載等が違法となり得る場合の明確化など、金融商品取引法上の無登録業者の排除を推進してきたところ、引き続き、専用窓口にて利用者からの相談を受けるとともに、金融商品取引法に違反する可能性があるＳＮＳ上の偽広告等に関し、金融関係事業者等とも連携しながら情報収集等を行う。これらの取組を通じて収集した情報も活用しつつ、無登録業者については、警告書の発出、金融商品取引法に基づく裁判所への禁止又は停止命令の申立てを行うとともに、金融庁ウェブサイトを通じた業者名等の公表やＳＮＳ事業者への情報提供等、排除のための取組を積極的に推進するほか、金融庁や消費者庁が収集した無登録業者に関する情報を活用し、必要な取締りを推進する。また、利用者が無登録業者との取引を行わないよう、金融商品取引業等の登録の有無を利用者が容易に検索できる機能を開発・運用する。

オ　ＡＩ事業者ガイドラインの周知等

総合対策において、ＡＩ事業者ガイドラインの周知等を行うことでＡＩの安全安心な活用が図られるよう働き掛けてきたところ、引き続き、ＡＩ事業者ガイドラインを適時に更新するとともに、関連団体・組織、事業者等に対する説明や講演等を通じて普及・浸透を図る。

(3)　欺罔段階への対策

ア　変化する欺罔の手口の国民への迅速かつ実効的な広報・注意喚起

総合対策において、関係省庁が連携した広報等のほか、高い発信力を有する著名人や関係機関等と連携して特殊詐欺等に関する広報・啓発活動を展開してきたところであるが、常に変化する欺罔の手口に応じた主たる被害者層のセグメント分けや、具体的にとるべき対策を明確にしないまま、特殊詐欺等の抽象的な危険性を国民に訴えるにとどまっている部分も見られることから、変化する欺罔の手口について、迅速・的確にその特徴や被害者層、具体的に講じるべき対策等を明らかにした上で、訴求対象及び訴求内容と合致する広報啓発の手段を選定し、効果的な広報啓発を行う。

また、各関係機関等と連携した広報啓発活動に関しては、やみくもに連携を呼び掛けるのではなく、欺罔の手口に関係を有する事業者団体や、対策の働き掛けを効果的・効率的に行うことができると認められる事業者団体等に対し、各業を所管する省庁から、具体的に講じるべき対策を明らかにした上で連携を働き掛ける。

さらに、利用者が特に顕著な被害状況のサービス等を利用する際に適切な防犯意識を持つことができるよう、犯行に利用されるツールやプラットフォーム等に関しても、実効的な注意喚起を行うことを検討する。

(4)　金銭等の交付段階への対策

ア　被害の未然防止及び拡大防止のための取組

(ｱ)　金融機関と連携した被害の未然防止

総合対策において、金融機関と連携した被害の未然防止の取組として、高額の払戻し等を申し込んだ高齢の顧客に対する金融機関における声掛けを促進する取組や、各金融機関が定める一定の基準（顧客の年齢、払戻金額等）に基づき警察に全件通報する取組、高齢者のＡＴＭ振込・引出限度額を少額とすることの制度化に向けた検討を推進してきたところ、引き続き、同取組等を推進する。

(ｲ)　インターネットバンキングに係る対策の強化

総合対策において、金融機関と連携した被害の未然防止の取組として、ＡＴＭでの振込・引出制限等を推進してきたところ、インターネットバンキングの利用が被害の高額化の一つの要因になっていることがうかがわれることから、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、インターネットバンキングの申込みがあった際や利用限度額引上げ時の利用者への確認や注意喚起等の取組を推進する。

(ｳ)　預金取扱金融機関におけるモニタリングの強化

総合対策において、預金取扱金融機関と連携した検挙等を推進してきたところ、インターネットバンキングを利用した送金による被害が増加している状況を踏まえ、引き続き、関係当局が連携し、預貯金口座の不正利用に係る預金取扱金融機関の検知能力の強化を図るとともに、法人口座を含む不正な口座情報等について、警察と預金取扱金融機関における迅速な情報共有に係る取組を推進する。

(ｴ) 暗号資産交換業者による送金のモニタリングの強化

総合対策において、暗号資産を用いた詐欺被害の実態把握等を行ってきたところ、詐欺等の被害金には、マネー・ローンダリングの過程で、一定の暗号資産アドレスに集約されている実態もみられることから、暗号資産交換業者に対し、顧客の依頼により暗号資産を送金した後も、当該送金に係る取引の流れを適切にモニタリングするなど、取引モニタリングの強化を要請する。

(ｵ) 暗号資産交換業者への不正送金防止の更なる推進

総合対策を踏まえ、警察庁及び金融庁が連名で金融機関に対し要請している、口座名義人と異なる依頼人名による暗号資産交換業者への送金停止について、その実施状況を確認するなどのフォローアップを実施しているところであるが、依然として、詐欺等の被害金が暗号資産に交換されるなどのマネー・ローンダリングの実態がみられることから、引き続き、関係省庁や関係団体と連携し、金融機関における暗号資産口座への不正な送金に係る対策を推進する。

また、警察庁において、ＳＮＳ型投資・ロマンス詐欺等におけるマネー・ローンダリングについて、暗号資産交換業者と連携し、暗号資産口座凍結依頼等を実施するための枠組みを構築しており、引き続き、同枠組みを活用した被害拡大防止対策に取り組む。

(ｶ) 電子マネー発行事業者等における被害防止の推進

総合対策において、電子マネー発行事業者等における被害防止の取組として、一般社団法人日本資金決済業協会、電子マネー発行事業者、収納代行事業者等と連携し、顧客への注意喚起をはじめ、モニタリングによって、不正な方法で入手された電子マネーの検知及び利用停止、警察への速やかな情報提供等を推進してきたところ、引き続き、同取組を推進する。

(ｷ) コンビニエンスストア等と連携した被害の未然防止

総合対策を踏まえ、電子マネー型や収納代行利用型の手口の対策として、一般社団法人日本フランチャイズチェーン協会、各コンビニエンスストア事業者と連携し、同一人や同一機会での高額又は複数の電子

マネー購入希望者や収納代行利用者への声掛けのシステム化等を推進してきたところ、今後更なる連携を図るため、コンビニエンスストアの店舗ごとに担当警察官を指定し、担当警察官による店舗への定期的な立ち寄りや防犯訓練等を通じ、店舗と連携して詐欺が疑われる客への声掛け等を行う。

イ　被害金の追跡及び被害回復を容易にするための取組

(ｱ)　金融機関等の間における情報共有等の枠組みの創設

総合対策において、金融機関と連携した対策を推進してきたところであるが、犯罪者グループは複数の預金取扱金融機関の口座を保有し、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、被害金が犯罪者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、個々の金融機関において、取引のモニタリング等を行っ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と共有し、かつ、犯罪者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不正利用口座に係る情報を共有しつつ、速やかに口座凍結を行うことが可能となる枠組みの創設について検討する。

なお、犯罪者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、預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組を推進する。

(ｲ)　架空名義口座捜査等の新たな捜査手法の導入に向けた検討

総合対策において、預貯金口座等の不正利用防止対策並びに被害回復給付金支給制度及び振り込め詐欺救済法の効果的な運用を推進してきたところ、犯罪者グループは、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とから、犯罪者グループの上位被疑者の検挙、犯罪収益の剝奪等を図るとともに、口座の悪用を牽制するため、捜査機関等が管理する架空名義口座を利用した新たな捜査手法や関係法令の改正を早急に検討する。

(ｳ)　金融機関への照会・回答の迅速化

緊急対策を踏まえ、金融機関への照会・回答を迅速化するべく、照会・回答の利便性向上が期待できるオンライン照会を活用する取組を進めてきたところ、引き続き、捜査に関する既存のシステムのほか、民間システムの活用の拡大を検討するとともに、照会・回答の効率化に資する運用上の仕組みについて、関係団体等とも協議の上、検討する。

(ｴ)　暗号資産の没収・保全の推進

総合対策において、暗号資産の没収・保全を推進してきたところ、犯罪収益である暗号資産等の没収の裁判の執行・没収保全等の手続について、これを整備する法律案が国会に提出されたところであるが、今後、より一層円滑・確実に暗号資産を没収できるよう制度の具体的な運用について検討する。

(5) 犯行後の捜査段階における対策

ア 照会対応の強化等

(ｱ) ＳＮＳ事業者の照会対応の強化

総合対策において、ＳＮＳ事業者における照会対応の強化を求めてきた結果、一部の事業者については、照会対応の迅速化等の措置が講じられた。犯行に利用されるＳＮＳは随時変化していることから、その他の事業者についても照会への対応の円滑化に関する要請を実施したところ、引き続き、犯行実態も踏まえつつ、更なる働きかけを行い、なお協力が得られない事業者については、関係省庁において、照会に対する協力を得るためのより実効性のある方策を検討する。

(ｲ) 海外事業者の日本法人窓口の設置の働き掛けなど情報提供の迅速化のための環境整備

海外事業者による情報提供の迅速化を推進し、一部事業者との間では迅速化の取組を開始しているところ、関係省庁が連携し、日本法人のない海外事業者に対する日本国内の法人窓口設置など情報提供の迅速化のための環境整備に向けた更なる働き掛け等を推進する。

(ｳ) 通信履歴の保存の義務化

捜査機関が犯罪に関与している人物を特定するために通信事業者から所有する通信履歴を取得することが必要となる場面が多いことから、通信事業者に対する通信履歴等の円滑な差押えを可能とする取組を推進してきたところであるが、捜査機関が被害を認知した時点で通信履歴が残されていない場合が一定数存在している。通信事業者の通信履歴の保存の在り方について、通信履歴の保存の必要性や妥当性、保存期間や費用面の課題とともに、電気通信事業における個人情報等保護に関するガイドラインの改正や通信履歴の保存の義務付けを含め検討する。

(ｴ) 国際的な枠組みを通じた議論への参加

令和７年３月に英国及びＥＵが共催した「合法的アクセスに関する国際シンポジウム」に参加し、各国政府機関やテクノロジー業界等との継続的な対話等を構築するため、合法的なアクセスを維持する重要性、その課題等について議論を行った。引き続き、必要に応じて捜査機

関が一定の条件下で暗号化されたコンテンツ等に関するデータを取得できるよう、Ｇ７（ローマリヨングループ）等の国際的な枠組みを通じた議論に参加する。

(ｵ)　金融機関への照会・回答の迅速化＜再掲＞１⑷イ(ｳ)

イ　暗号化技術等に係る調査・研究、新たな法制度導入に向けた検討

犯罪者グループの壊滅のためには、シグナル、テレグラム等の匿名性の高い通信アプリをはじめとする犯罪に悪用される通信アプリ等について、被疑者間の通信内容や登録者情報等を迅速に把握することが重要であり、こうした被疑者間の通信内容等を迅速に把握するために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て検討する。

ウ　組織的詐欺や強盗等の実行犯に対する適正な科刑の実現に向けた取組の推進

総合対策において、ＳＮＳ型投資・ロマンス詐欺及び特殊詐欺事犯に係る組織的な犯罪の処罰及び犯罪収益の規制等に関する法律における犯罪収益等隠匿及び同収受罪の適用等を推進してきたところ、これらの詐欺の実行犯等に対して適正な科刑の実現を推進するため、引き続き、同法における組織的詐欺罪の適用を推進する。

また、引き続き、組織的詐欺や強盗等の事件捜査において余罪の積極的な立件を推進していくとともに、公判においても、悪質な事情について適切に主張・立証する。

エ　外国捜査機関等に対する捜査共助・協力結果を踏まえた海外にある犯罪収益等の剝奪

総合対策において、国境を跨いだ被害回復の充実に向けて関係機関や外国当局との協力関係を強化してきたところ、海外に流出した被害金の迅速な捜査・被害回復のため、ＩＣＰＯを通じた捜査協力、外国のＦＩＵとの情報交換、外交ルートや条約・協定を活用した国際捜査共助等により、当該事件に関する情報を早期に入手・分析し、没収・追徴を可能とすべく、海外に移転した犯罪収益等を特定する手段等について検討する。

オ　匿名・流動型犯罪グループの存在を見据えた取締りと実態解明の推進

総合対策において、匿名・流動型犯罪グループに対する取締りを強化するための取組として、警察において、部門の壁を越えた連携を推進し、あらゆる法令を駆使した効果的かつ多角的な取締りを行うとともに、積極的な情報収集を行うなどして、その活動実態や詐欺等への関与状況等の解明を推進してきたところ、引き続き、匿名・流動型犯罪グループの活動実態の変化に機動的に対応し、事件の背後にいる首謀者や指示役も含め

た犯罪者グループ等の弱体化・壊滅のため、部門の壁を越えた効果的な取締りを推進するとともに、匿名・流動型犯罪グループの資金獲得活動等に係る実態解明を進める。

また、緊急対策において、仮装身分捜査を導入することとされたところ、制定した実施要領に基づき、仮装身分捜査を適正に実施し、詐欺や強盗等の犯人を検挙し、被害を抑止する。

カ　不法行為に基づく損害賠償請求に関する裁判例の調査研究

不法行為に基づく損害賠償請求事案について、インターネット上の権利侵害事案等を中心に、慰謝料や弁護士費用等の損害額に関する司法判断の動向につき調査研究を実施してきたところ、引き続きその取組を継続するとともに、その結果が取りまとめられた時点で、損害賠償請求訴訟に携わる実務家等が参照することができるような形でこれを公表する。

２　特殊詐欺対策

(1)　犯行準備段階への対策

ア　各種サービスやインフラの不正利用を防止するための取組

１(1)アで掲げたＳＮＳ型投資・ロマンス詐欺に対する取組に加え、次の対策を推進する。

(ｱ)　闇名簿対策等の推進

総合対策及び緊急対策において、個人情報保護委員会と警察との連携や、個人情報保護に係る広報啓発を推進してきたところ、引き続き、警察は、特殊詐欺の捜査の過程で、悪質な「名簿屋」等の事業者を把握した場合に、個人情報保護法に基づいた行政上の措置の前提となり得る「名簿屋」等の事業者の実態把握に資するため、個人情報保護委員会に対して積極的な情報提供に努めるとともに、犯罪者グループ等にこうした名簿を提供する悪質な「名簿屋」、さらに個人情報を不正な手段により取得して第三者に提供する者に対し、あらゆる法令を駆使した取締り等を推進する。

個人情報保護委員会は、「名簿屋」等の事業者において、個人情報保護法上問題となる事態が確認された場合には、引き続き厳正に対処していく。さらに、引き続き、個人情報取扱事業者等に対して、安全管理措置の徹底等の個人情報の適正な取扱いの確保を図るべく、広報啓発を行う。また、個人情報を悪用する事業者等に対して、個人が個人情報を提供する事例も見受けられることから、警察からの情報提供を踏まえ、広く国民に対して個人情報に係る規律を周知するなど、国民が自らの個人情報を適切に取り扱うための広報啓発を更に推進する。

(ｲ)　犯行に利用される電話番号への対策

総合対策において、犯行に利用された電話に対して、繰り返し架電してメッセージを流すことで、電話を事実上使用することを不可能にする警告電話事業を実施してきたところ、今後は、電話番号の悪用防止のためのより効果的な方策の実施も含めて対策を検討する。

イ　犯罪への加担を防止するための取組＜再掲＞1(1)イ

(2)　着手段階への対策

ア　詐欺電話の防止等に係る取組

(ｱ)　国際電話サービスを悪用した詐欺等への対策

総合対策において、犯人からの電話を直接受けないための対策として国際電話不取扱受付センターにおける利用休止申込みを促進してきたところ、依然として国際電話番号が悪用されることが多く、契約者全体に国際電話利用休止について周知する必要があることから、国際電話サービスの休止について政府広報とも連携して一層強く国民に周知するとともに、固定電話の移転、切替え時をはじめとした契約変更等の機会に、国際電話を悪用した詐欺被害に遭う可能性があることを説明し、真に必要な者に限って国際電話サービスを利用できるようにする。

また、将来的には、こうした予防措置を推進する観点から、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人に対して利用休止を促すような効果的な対策の導入についての検討や国際電話をブロックする機能についてのニーズ調査の分析を実施する。

さらに、積極的な広報等により、今後国際電話の利用休止申込み件数が増加することが見込まれるため、国際電話不取扱受付センターの申請受付体制の更なる拡充を要請するとともに、総務省において、国際電話の悪用を含む詐欺電話への対策に関する相談受付体制を整備する。

(ｲ)　詐欺電話を遮断するサービスに係る支援措置等

総合対策において、犯人からの電話を直接受けないための対策として、通信事業者による 70 歳以上の固定電話契約者等に対するサービスの無償化を含む発信者番号表示サービス等の普及等を推進してきたところ、被害傾向の変化に伴い、高齢者以外の層が携帯電話への架電を受けて被害に合うケースも増加している。これまで一部の関係事業者において迷惑電話等の受信を防止又は受信した際の警告等を行うサービスを有料で提供しているところ、事業者に対し、幅広い利用者層への普及等のため、無償化を含めた効果的な措置を要請するとともに、被害防

止機能向上のためのより効果的な方策を検討し、その普及や有効性の向上を図る。

また、固定電話については、国際電話不取扱受付センターにおいて利用休止の申込みを受け付けているところ、携帯電話への国際電話を悪用した詐欺も増加していることから、携帯電話についても、通信網上での受信防止措置も含めて国際電話を悪用した詐欺電話への対策を検討する。

また、総合対策において、犯人からの電話を直接受けないための対策として、公益財団法人全国防犯協会連合会と連携し、「優良防犯電話推奨事業」による機器の普及促進を推進してきたところ、引き続き、同事業による機器の普及促進を推進する。

(ｳ) 悪質な電話転送サービス事業者等の排除に向けた取組

総合対策を踏まえ、犯行に利用された固定電話番号等の利用停止や、新規番号の提供拒否、在庫番号の一括利用停止等の従来の対策を実施している。

また、令和６年６月から情報通信審議会電気通信事業政策部会の下で電気通信番号の犯罪利用対策に関するＷＧを開催し、電気通信番号制度の見直し（電気通信番号使用計画の認定に係る欠格事由への詐欺犯の追加等）について検討を重ね、同年 11 月に最終答申が取りまとめられた。同答申の内容を踏まえ、令和７年度に関係法令の改正作業や事業者への働き掛けを行う。

(ｴ) 発信者番号偽装への対策

発信者番号の表示が官公庁等の電話番号に偽装され、特殊詐欺等の犯罪に悪用されている事例が存在することから、関係事業者と連携して効果的な対策を検討し、速やかに実施する。

また、国民に対して電話番号を偽装する手口に関しての注意喚起を行う。

イ　詐欺メール、詐欺ＳＭＳによる被害防止等のための取組

(ｱ) 詐欺メール、詐欺ＳＭＳ等の送信防止・遮断措置

総合対策において、通信事業者によるメールやＳＭＳフィルタリングの活用の拡大等を行ってきたところ、詐欺に誘引するＳＭＳや電子メールについて悪用の実態が認められることから、ネットワーク上でこれらが利用者の端末に届くことを防止する対策を含めた取組を推進し、被害防止に資する取組の実施が困難であれば実効性のある制度整備等を検討する。

また、一部の関係事業者において、迷惑ＳＭＳ等を利用者の端末が受信した際に警告等を行うサービスを提供しているものについて、幅広い利用者層への普及等のため、無償化を含めた効果的な措置を要請するとともに、被害防止機能向上のための方策を検討し、その普及や有効性の向上を図る。

(ｲ)　送信ドメイン認証技術（ＤＭＡＲＣ等）への更なる対応促進

総合対策を踏まえ、総務省及び警察庁が連名で、金融機関、ＥＣ事業者、物流事業者等の事業を所管する省庁に対して、送信ドメイン認証技術（ＤＭＡＲＣ等）の周知を要請し、同要請を踏まえ、関係省庁から所管する事業者等への各種要請等を行っているところであるが、例えば、令和６年中のインターネットバンキングに係る不正送金事犯の手口をみると、フィッシングサイト等に誘導する手口のうち約 58 パーセントが電子メールであるなど、詐欺等にドメイン名のなりすましが用いられていることから、その対策を更に推進する必要がある。引き続き、利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関、EC 事業者、物流事業者、行政機関等のメール送信側事業者等に対して、導入状況も踏まえ、送信ドメイン認証技術（ＤＭＡＲＣ等）の導入推進を継続して実施するとともに、送信側事業者等に対してなりすましメールの受信拒否を要求するポリシーでの運用を検討するよう働き掛ける。また、関係省庁等が連携し、なりすましの対象となる事業者等に対して、必要に応じて、ＤＭＡＲＣ等の導入状況等を確認するなどのフォローアップを行う。

(ｳ)　犯行に利用される電話番号への対策＜再掲＞２(1)ア(ｲ)

(3)　欺罔段階への対策

１(3)で掲げたＳＮＳ型投資・ロマンス詐欺に対する取組に加え、次の対策を推進する。

ア　押収名簿を活用した注意喚起

総合対策において、特殊詐欺等の捜査の過程で入手した名簿の登載者に対し、警察官による戸別訪問や警察が民間委託したコールセンターからの電話連絡等を行い、注意喚起や具体的な予防対策等の周知を図る取組を推進してきたところ、引き続き、この取組を推進する。

(4)　金銭等の交付段階への対策

ア　被害の未然防止及び拡大防止のための取組

１(4)アで掲げたＳＮＳ型投資・ロマンス詐欺に対する取組に加え、次の対策を推進する。

(ｱ)　携帯電話を使用しながらＡＴＭを利用する者への注意喚起の推進

総合対策において、携帯電話を使用しながらＡＴＭを利用する者への注意喚起の取組を推進してきたところ、依然として被害者が犯人から携帯電話等で指示を受けながらＡＴＭを操作し被害に遭う事例が多数みられることから、金融機関その他の関係機関・団体と連携し、「ＡＴＭでの携帯電話の通話は、しない、させない」取組を推進していくとともに、より訴求力の高い注意喚起の方策を検討していくほか、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についても検討する。

(ｲ)　不動産業者等と連携した空き家等の不正な利用の防止

総合対策において、空き家、空室及び宅配ボックス（以下「空き家等」という。）の悪用防止の取組を推進してきたところ、引き続き、関係省庁が、地方公共団体等と連携し、悪用の実態や具体的な犯罪手口情報について、空き家等の所有者等に対して周知・啓発を実施するとともに、不審な利用を把握した場合は警察に情報提供するよう不動産業者等に周知を実施する。

(ｳ)　宅配事業者における被害防止の推進

総合対策において、宅配事業者と連携した被害の未然防止を推進してきたところ、引き続き、過去に犯行に使用された被害金送付先のリストを活用して、不審な宅配便の発見や警察への通報といった取組や、宅配事業者の荷受け時において、運送約款に基づく取扱いができない現金が宅配便に在中していないかどうかの声掛け等による注意喚起の取組等を推進する。

イ　被害金の追跡及び被害回復を容易にするための取組＜再掲＞１⑷イ

⑸　犯行後の捜査段階における対策＜再掲＞１⑸

３　ＩＤ・パスワード等の窃取・不正利用対策

⑴　フィッシングサイトへの対策

ア　フィッシングサイトの更なる閉鎖促進

総合対策において、フィッシングサイトの閉鎖促進対策として、金融機関、ＥＣ事業者、物流事業者等の事業を所管する省庁に対して、フィッシングサイトの閉鎖の促進等を要請し、同要請を踏まえ、関係省庁から所管する事業者等へ各種要請を行っているところであるが、令和６年中のフィッシング報告件数は、約 172 万件と右肩上がりで増加した[4]。

[4] フィッシング対策協議会の資料による。

そこで、フィッシングサイトの閉鎖を更に推進する必要があることから、なりすましの被害に遭った事業者等に対し、同事業者等からホスティング事業者等にフィッシングサイトの閉鎖依頼を実施するよう要請するとともに、関係省庁が連携し、特になりすましの被害が多い事業者等に対して、必要に応じて、フィッシングサイトの閉鎖依頼の実施状況を確認するなど、フォローアップを行う。また、都道府県警察が委嘱するサイバー防犯ボランティアは、サイバーパトロールを通じ、フィッシングサイトを発見し、ホスティング事業者等への閉鎖依頼を実施していることを踏まえ、こうした取組を積極的に後押しし、幅広い主体と連携したフィッシング対策を更に推進する。

イ　フィッシングサイトに係る情報の収集・分析及び提供による対策

総合対策において、警察庁では、フィッシングサイトへのアクセス時の閲覧防止措置や警告表示に活用させるべく、都道府県警察等から集約したフィッシングサイト等のＵＲＬ情報をウイルス対策ソフト事業者やフィルタリング事業者等に提供している。

そこで、引き続き、都道府県警察等から集約したフィッシングサイトに関する情報を基に、同一のＩＰアドレス上に構築されたサイトに関する情報を収集することで、未だ通報等がなされていないフィッシングサイトを先制的に把握し、ウイルス対策ソフト事業者等に提供する取組を推進するとともに、フィッシングサイト判定の高度化・効率化のために生成ＡＩを活用し、閲覧防止措置や警告表示によるフィッシングサイト対策の効率化を図る。

⑵　ＩＤ・パスワードやクレジットカード情報の不正入手対策

ア　フィッシングサイトに誘導するメールやＳＭＳへの対策

(ｱ)　ＳＭＳの不適正利用対策の推進

ＳＭＳ配信に関わる関係事業者において、ＳＭＳ配信元の明確化・透明化に係る取組や、ＳＭＳ認証代行事業者等の悪質事業者への対策等を盛り込んだ業界ルールの策定に向け、総務省と関係事業者において、引き続き協議を実施する。

警察庁においては、一般財団法人日本サイバー犯罪対策センター（ＪＣ３）と連携し、同センターが観測した、マルウェアによって送信される不正なＳＭＳに関する情報を都道府県警察へ共有し、先制的な注意喚起や広報啓発に活用している。引き続き、関係機関等と連携し、ＳＭＳ配信に関わる関係事業者に対する働き掛け等を推進する。

(ｲ)　詐欺メール、詐欺ＳＭＳ等の送信防止・遮断措置＜再掲＞２⑵イ(ｱ)

(ｳ)　送信ドメイン認証技術（ＤＭＡＲＣ等）への更なる対応促進＜再掲＞
２⑵イ(ｲ)

イ　ＩＤ・パスワード等の窃取対策

(ｱ)　パスキーの普及促進

総合対策において、次世代認証技術の１つであるパスキー[5]の普及のため、金融機関やＥＣ事業者等の事業を所管する省庁に対して、その導入等の促進を要請し、同要請を踏まえ、関係省庁から所管する事業者等へ各種要請を行っているところ、フィッシングによる被害の中には、送金時等の二段階認証に必要なＳＭＳ認証コードをリアルタイムに盗み取って行う手口が発生していることから、引き続き、関係省庁と連携し、関係事業者等が参加する各種講演会等の機会を捉え、パスキーの有用性について説明を行うなど、その普及に向けた取組を実施する。

(ｲ)　ＥＣサイトの脆弱性を悪用したクレジットカード情報窃取対策

クレジットカードの不正利用の被害の中には、ＥＣサイト構築用ソフト[6]の脆弱性が悪用され、クレジットカード情報が窃取されている事例もみられる。経済産業省は、捜査等により把握した当該窃取の手口等に関する情報を関係省庁や関係団体に提供している警察庁と連携するとともに、脆弱性対策等の情報窃取対策の実施について、カード会社がＥＣ事業者に対して適切に指導等を行うよう監督する。

⑶　ＩＤ・パスワードやクレジットカード情報の不正利用対策

ア　事業者等との情報連携による対策の強化

(ｱ)　ＥＣ加盟店等との情報連携

総合対策において、ＥＣ加盟店等においては、不正取引に関するアカウント情報等をそれぞれの個人情報の取扱いに関する指針等に基づき被害防止対策に活用しているため、ＥＣ加盟店等と警察との連携を進めてきたところであるが、こうした連携をより強化するため、利用者の個人情報の保護と被害防止対策が両立されるべく、ＥＣ加盟店等における不正取引等に関する個人データの警察への提供に係る整理を「『個人情報の保護に関する法律についてのガイドライン』に関するＱ＆Ａ」等に追加する。その上で、当該Ｑ＆Ａ等を通じ、ＥＣ加盟店等における提供情報の範囲を明確化し、その適切な運用と情報提

---

[5] ＦＩＤＯ　ＡｌｌｉａｎｃｅとＴｈｅ　Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ　Ｃｏｎｓｏｒｔｉｕｍにより規格化されているパスワードが不要な認証技術。フィッシングサイト等の正規サイト以外のウェブサイトにおいては認証が機能しないといった観点から認証情報の漏えいリスクを低減できる効果があるとされている。

[6] 専門知識がなくても手軽にＥＣサイトを構築することができるソフトウェア

供の充実化を働き掛ける。

また、警察庁においては、令和６年 12 月に各都道府県警察が捜査等を通じて把握した悪用のおそれのあるクレジットカード番号等を集約し、カードの利用停止等の対策に活用するため、国際ブランド各社に一括して提供する枠組みを構築したところ、引き続き、同枠組みを活用した被害拡大防止対策に取り組む。

(ｲ)　コード決済に関する被害防止

総合対策において、フィッシング等により窃取されたコード決済サービスのアカウントがコンビニエンスストアの店舗で不正に利用されている実態を受け、同様の犯罪手口が確認されている薬局等に対しても同様の取組を推進するとしていたところ、令和６年 11 月、一般社団法人日本チェーンドラッグストア協会に対し、コード決済の悪用に関する対策の強化を依頼した。引き続き、コード決済を悪用したマネー・ローンダリングや現金化への対策に取り組む。

(ｳ)　金融機関におけるモニタリングの強化＜再掲＞１⑷ア(ｳ)

(ｴ)　暗号資産交換業者による送金のモニタリングの強化＜再掲＞１⑷ア(ｴ)

イ　不正アクセス行為の事後追跡性確保等

(ｱ)　踏み台とされている家庭用インターネット通信機器[7]の実態把握及び対策

インターネットバンキングに係る不正送金事案の中には、不正送金等を実行する際に一般家庭のＩＰアドレスからのアクセスに偽装するための踏み台として、不正プログラムに感染している家庭用インターネット通信機器を不正利用する事例が認められることから、こうした踏み台に利用される機器の実態を調査・分析し、その悪用実態を踏まえ、国民に対し注意喚起や広報啓発をするなどの対策を実施する。

(ｲ)　通信履歴の保存の義務化＜再掲＞１⑸ア(ｳ)

⑷　マネー・ローンダリングや現金化への対策

ア　音声通信ＳＩＭの契約時における本人確認の義務付け＜再掲＞１⑴ア(ｱ)③

イ　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＜再掲＞１⑴ア(ｱ)④

ウ　預金取扱金融機関におけるモニタリングの強化＜再掲＞１⑷ア(ｳ)

---

[7] 主に一般家庭においてインターネットに接続して利用される、パーソナルコンピュータやスマートフォン、ＩｏＴ機器等

エ　暗号資産交換業者による送金のモニタリングの強化＜再掲＞１⑷ア(ｴ)

オ　暗号資産交換業者への不正送金防止の更なる推進＜再掲＞１⑷ア(ｵ)

カ　ＥＣ加盟店等との情報連携＜再掲＞３⑶ア(ｱ)

キ　コード決済に関する被害防止＜再掲＞３⑶ア(ｲ)

⑸　犯行後の捜査段階における対策

ア　金融機関への照会・回答の迅速化＜再掲＞１(4)イ(ｳ)

イ　通信履歴の保存の義務化＜再掲＞１⑸ア(ｳ)

ウ　暗号化技術等に係る調査・研究、新たな法制度導入に向けた検討＜再掲＞１⑸イ

エ　踏み台とされている家庭用インターネット通信機器の実態把握及び対策＜再掲＞３(3)イ(ｱ)

オ　ＥＣ加盟店等との情報連携＜再掲＞３(3)ア(ｱ)

カ　上位被疑者の検挙を見据えた捜査の推進

インターネットバンキングに用いられるＩＤ・パスワードやクレジットカード情報を窃取するためのフィッシングを敢行する上位被疑者については、匿名性の高い犯罪インフラや通信手段を利用していることから、この匿名性を打破するため、情報の横断的・俯瞰的な分析を実施するなど、上位被疑者の特定に資する捜査を積極的に推進する。

４　治安基盤の強化等

⑴　体制の充実強化

ア　首謀者等を検挙するための取締り・実態解明能力・体制の強化

総合対策において、匿名・流動型犯罪グループの存在を見据えた取締りと実態解明のための取組として、警察庁及び各都道府県警察における部門横断的な取締り及び実態解明を行うための体制の整備を行ってきたところであるが、匿名・流動型犯罪グループは、匿名性の高い通信手段の悪用や不正に開設・譲渡された預貯金口座や暗号資産口座を用いて巧妙にマネー・ローンダリングを行っており、首謀者等の検挙が困難となっている実態がある。また、匿名・流動型犯罪グループによる資金獲得活動の中には、特殊詐欺やＳＮＳ型投資・ロマンス詐欺のように、国内外の犯行拠点から広域的に敢行される実態が認められるものがある。こうした実態を踏まえ、犯罪者グループに関する情報の集約・分析や、外国当局及び金融機関等の関係機関と緊密に連携した取締りを推進するなど、全国警察が一体となって更に効果的な実態解明を推進するため、体制の強化や分析システムの高度化を行う。

さらに、匿名・流動型犯罪グループは、ＳＮＳ等で犯罪の実行者を募集し、応募してきた者に身分証を送付させるなどした後に、応募者自身や家族に危害を加えるなどと脅迫し、犯罪に加担させている実態があることから、犯罪実行者募集情報に応募した者等の保護対策に間隙を生じさせないようにするための資機材の整備等を行う。

イ　サイバー人材の体系的な育成の推進のための態勢の充実強化

緊急対策において、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充実強化のための取組を推進してきたところ、匿名・流動型犯罪グループによる犯罪においては、犯罪収益の暗号資産への交換や匿名性の高い通信手段の利用、ＳＮＳ上での犯罪実行者募集等が行われるため、その取締りにサイバー事案への対処に係る能力が必要とされ、警察官や技術系職員を含む警察職員のサイバー事案対処能力の底上げが必要不可欠であることから、警察学校におけるサイバー教育及び都道府県警察等のサイバー人材の育成の更なる推進のための態勢の充実強化を図る。

また、検察においても、捜査公判において、サイバー事案対処能力の向上が必要不可欠であることから、研修等を通じて、サイバー捜査に関する専門知識を有する検察官を含む検察庁職員の育成に努めるとともに、推進のための態勢の充実強化を図る。

ウ　サイバー空間における情報集約・分析及び取締りのための態勢の充実強化

総合対策において、暗号資産の追跡を実施する専従の体制を構築するなど、暗号資産追跡を含む高度な専門的知識及び技術に基づくサイバー捜査体制や情報の横断的・俯瞰的な分析体制を強化してきたところであるが、サイバー空間上では、引き続き、警察の捜査に支障をきたすような犯罪インフラが利用されている実態があり、匿名・流動型犯罪グループの上位被疑者に対しては高度な専門的知識及び技術に基づく取締りが必要不可欠であることから、警察庁及び都道府県警察間の連携強化並びに犯罪インフラ等の実態解明を含めた更なる情報集約・分析及び取締りのための態勢の充実強化を図る。

(2)　装備資機材等の充実強化

ア　スマートフォン端末等の解析能力の強化

総合対策及び緊急対策において、証拠品として押収されたスマートフォン端末等の解析の円滑化に向けた、最新の電子機器やアプリケーションの解析のための技術力の向上、パスワードが不明なスマートフォン端末の解析等を行う解析用資機材の充実強化を行ってきたところ、匿名・流

動型犯罪グループによる犯罪の捜査及び実態解明のために解析の更なる円滑化が必要であることから、引き続き、警察、検察における解析用資機材の充実強化を推進するとともに、捜査員や検察庁職員等に対する研修等を推進し、情報技術解析に関する態勢を強化する。

イ　捜査に必要な情報の収集の効率化

匿名・流動型犯罪グループによる犯罪においては、ＳＮＳを通じて詐欺等の犯行や実行者の募集が行われている実態があることから、サイバー空間上の膨大な情報から捜査に必要な情報を効率的に収集・分析し、警察、検察において、匿名・流動型犯罪グループの実態の解明やサイバー事案に対処するための資機材の充実強化を推進する。

⑶　新たな捜査手法の導入に向けた検討

ア　架空名義口座捜査等の新たな捜査手法の導入に向けた検討＜再掲＞１⑷イ(ｲ)

イ　暗号化技術等に係る調査・研究、新たな法制度導入に向けた検討＜再掲＞１⑸イ

⑷　国際連携の推進

ア　外国当局との連携体制の構築による摘発の推進

総合対策において、海外拠点の摘発の推進等のための取組として、国際捜査の徹底・外国当局等との連携等を推進してきたところ、特殊詐欺等の拠点が引き続き海外にも存在していることがうかがわれることに加え、ＳＮＳ等で実情を知らされずに海外拠点へおびき寄せられ、詐欺等の犯罪に加担させられる事例も確認されていることから、引き続き、ＩＣＰＯ等を通じた捜査協力の推進、外交ルートや条約・協定を活用した国際捜査共助等の円滑・迅速化や、国連薬物・犯罪事務所（ＵＮＯＤＣ）を始めとする国際機関と連携し、外国の法執行機関の取締り能力を強化する支援に継続的に取り組む。また、外交ルートも含めた政府のハイレベルからの働きかけにより、関係諸国と協働した詐欺等対策や特殊詐欺等の拠点にいる邦人の保護の取組を推進するほか、外国当局とより緊密に情報共有等が可能となる連携体制の構築を検討する。

イ　被疑者移送体制の強化

総合対策において、海外拠点の摘発の推進等のための取組として、国外被疑者の身柄移送体制の強化を推進してきたところであるが、外国当局により大規模な海外拠点が摘発され、多数の被疑者を日本へ移送しなければならないものの、複数回に分けて日本に移送せざるを得ない事例が生じており、関係被疑者の移送時期が異なることにより、移送後の捜査に支障を生じさせる懸念もあることから、関係省庁において、海外拠点摘発

時の身柄移送に係る方策について協議するほか、民間の航空会社にも協力を得るなど、海外で摘発された被疑者の移送体制の強化を図る。

ウ　海外に流出した犯罪収益等の確実な剝奪

総合対策において、海外に流出した犯罪収益等の実態把握や海外当局との協力関係の強化を図っているところ、実態を踏まえつつ、国境を跨いだ被害回復を確実にするため関係省庁と協議していく。

エ　外国捜査機関等との連携の推進

総合対策において、国際捜査の徹底・外国当局等との連携、海外拠点の摘発を推進しているところであるが、海外に所在する組織犯罪グループによって日本国内でＳＮＳ型投資・ロマンス詐欺が行われている実態があることから、インターポール等と連携し、都道府県警察による捜査に加え、サイバー捜査に関する高度な専門的知識及び技術に基づく横断的・俯瞰的な分析を行うことで得られた被疑者情報を関係国捜査機関に提供することによって、複数の関係被疑者の検挙に貢献するなどしている。また、警察庁では、サイバー空間における脅威への諸外国の対処能力の向上を図るとともに、外国捜査機関等との協力関係を強化することを目的として、外務省や独立行政法人国際協力機構（ＪＩＣＡ）と連携した外国捜査機関に対する支援を行っている。引き続き、海外に所在する犯罪グループによる犯罪の実態解明及び取締りに向けた外国捜査機関等との連携の強化を推進する。

オ　情報技術解析の高度化のための外国機関との連携の推進

総合対策及び緊急対策において、情報技術解析の高度化のために外国関係機関との連携を行うこととしているところ、引き続き、情報技術解析に関する国際会議等への参画を通じた外国関係機関との情報共有や連携を推進し、最新の技術動向の把握に取り組む。

⑸　防犯対策の強化等

ア　防犯カメラの設置に係る支援

総合対策及び緊急対策において、防犯カメラの整備を推進してきたところ、特殊詐欺や強盗等の広域に発生する事件は、社会における重大な脅威となっており、社会全体で防犯対策を強化する必要があることから、犯罪の発生状況等を踏まえた防犯カメラの増設が必要な場所の整理、地域社会の多様な関係者への保存期間の十分な防犯カメラの増設の働き掛けを行うほか、自治体と連携し、地方創生の交付金を活用した防犯カメラの設置等の地域防犯力の強化への支援を行う。

イ　防犯性能の高い建物部品、宅配ボックス等の設置等に係る支援

総合対策において、侵入犯罪対策を推進してきたところ、強盗等の事件の手口を踏まえ、引き続き、防犯性能の高い建物部品（ＣＰ部品）をウェブサイトで公表するなどして、その普及に努めるほか、侵入犯罪対策の広報・啓発を推進するとともに、ＣＰ部品として登録されたドア・窓への交換や、宅配ボックスの設置等への支援により、防犯性の高い住宅への改修を促進する。

ウ　現金を自宅に保管させないための対策

総合対策において、自宅に保管する現金を狙った「現金手交型」の特殊詐欺や強盗等の対策を推進してきたところ、引き続き、高齢者等に対して具体的な犯行手口について注意喚起を行うとともに、高額の現金を自宅に保管することの危険性を訴え、金融機関への預貯金等を活用するなどの予防対策を推奨する。

エ　宅配事業者等を装った強盗を防ぐための対策

総合対策において、宅配事業者を装った強盗を防ぐための対策を推進してきたところ、強盗等の事件では、宅配事業者の訪問を偽装するなどの手段で一般住宅等に侵入する手口がみられることから、強盗等を企図する者が住居等に不法に侵入する機会を低減するため、引き続き、宅配事業者と連携して非対面形式による宅配方法の普及に関する取組を推進するとともに、宅配事業者等を装って事前に下見活動を行う可能性もあることを踏まえ、引き続き、防犯情報の発信による注意喚起を図る。

オ　匿名・流動型犯罪グループの資金源への対策

匿名・流動型犯罪グループが詐欺等の犯行に関与している実態が見られるところ、これらグループの資金獲得活動は、詐欺等のほかに、組織的な窃盗や強盗、違法・悪質なホストクラブ営業やスカウト行為、薬物密売、オンラインカジノ等、多岐にわたっている。こうした資金獲得活動に着目した取締り等を推進し、匿名・流動型犯罪グループに対して効果的に打撃を与え、弱体化を図る。

また、近年、匿名・流動型犯罪グループが関与していると認められる悪質なリフォーム業者による犯罪行為が確認されており、こうした手口による犯罪の被害者が特殊詐欺や強盗等の二次被害に遭う危険性があるところ、このような悪質な営業を行うリフォーム業者の排除に向けた取組を推進するため、刑事手続等において把握したリフォーム業者に関する情報等を監督官庁へ提供する仕組みを設けることで、こうした悪質な営業を行うリフォーム業者に対し、当該監督官庁が適切な行政処分等の措置を講じられるように検討するとともに、関係省庁において、リフォーム業界の協力も得つつ、消費者に対する注意喚起等の広報・啓発を実施する。

カ　パトロール等による警戒

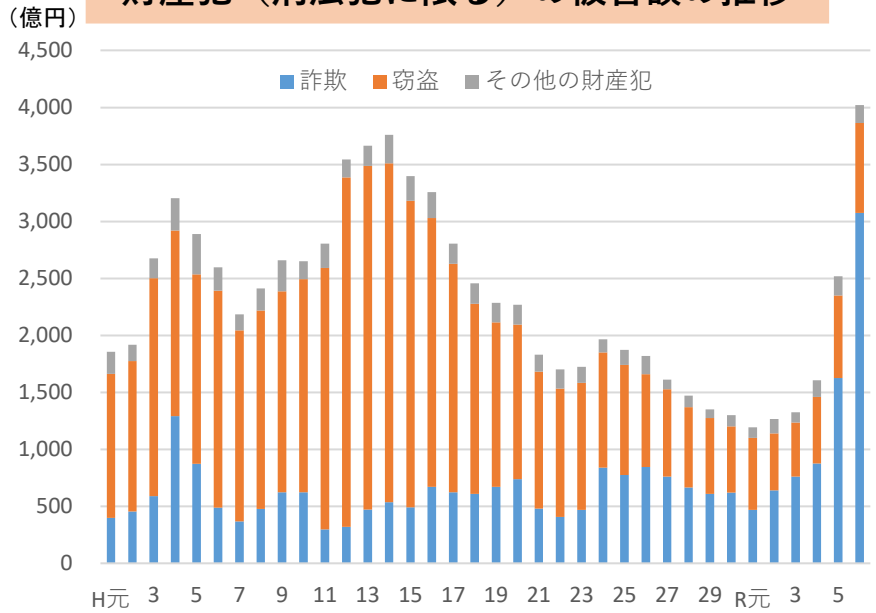
総合対策において、職務質問や防犯指導等の効果的な実施を通じて、事件等の発生を防ぐとともに、犯罪を取り締まるため、警察によるパトロール等による警戒を推進しているところ、引き続き、犯罪の多発する時間帯・地域に重点を置くなどしたパトロールを推進する。加えて、様々なステークホルダーによる青色回転灯等装備車（いわゆる「青パト」）を用いたパトロール活動の推進等、地方創生の交付金も活用し、地域防犯力の強化への支援を行う。

「国民を詐欺から守るための総合対策」の改定に当たって

現在の情勢

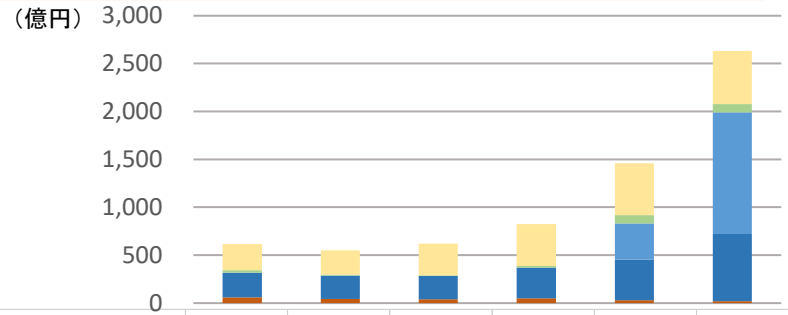
ＳＮＳやキャッシュレス決済の普及等が進む中で、これらを悪用した詐欺等の被害が加速度的に拡大する状況を受け、令和６年６月、「国民を詐欺から守るための総合対策」を策定し、官民一体となった対策を講じてきたところ、令和６年中の財産犯の被害額は4,000億円を超え、これは平成元年以来最も高かった平成14年当時の被害を上回る額であり、極めて憂慮すべき状況。その増分の大半を詐欺による被害額が占めており、詐欺への対策が急務。

財産犯（刑法犯に限る）の被害額の推移



	R元	R2	R3	R4	R5	R6
詐欺	469.5	640.1	763.0	876.8	1,625.8	3,074.7
窃盗	633.2	501.6	474.0	585.3	725.8	789.3

特殊詐欺、SNS型投資・ロマンス詐欺、不正送金事犯、クレジットカード不正利用事犯の被害額の推移



		R元	R2	R3	R4	R5	R6
合計		615.1	549.5	620.3	822.7	1,536.0	2,631.4
カード不正利用		274.1	253.0	330.1	436.7	540.9	555.0
詐欺	不正送金	25.2	11.3	8.2	15.2	87.3	86.9
詐欺	SNS型投資・ロマンス詐欺					455.2	1268.0
詐欺	特殊詐欺（その他）	256.7	242.6	242.5	323.9	422.8	704.4
詐欺	小計	281.9	253.9	250.7	339.1	965.3	2,059.3
特殊詐欺（詐欺盗）		59.1	42.6	39.5	46.9	29.8	17.1

※　令和６年の特殊詐欺及びＳＮＳ型投資・ロマンス詐欺の被害額は暫定値。
※　カード不正利用の被害額は、日本クレジット協会が集計したもの。

総合対策の改定

○　一層複雑化・巧妙化する詐欺等の被害から国民を守るためには、手口の変化に応じて機敏に対策をアップデートすることに加え、犯罪グループを摘発するための実態解明、犯罪グループと被害者との接点の遮断等の取組が必要。

○　令和６年12月に決定した「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」と統合するとともに、金融・通信に関するサービス・インフラの悪用を防止するための対策や、架空名義口座を利用した新しい捜査手法の検討等の新たな取組を追加して従来の総合対策を改定し、政府を挙げた詐欺等に対する取組を抜本的に強化。

「国民を詐欺から守るための総合対策2.0」における主な施策

1 SNS型投資・ロマンス詐欺対策 ／ 2 特殊詐欺対策

（1） 犯行準備段階への対策

○ 携帯電話不正利用防止法上、契約時における本人確認が義務付けられていないデータ通信専用SIMについて、悪用実態を踏まえ、電気通信事業者に対して契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討。

○ 犯罪実行者募集情報の削除等の取組を促進するほか、犯罪グループの人的基盤となり得る非行集団等からの少年の離脱に向けた取組等犯罪への加担を防止するための取組を推進。

（2） 着手段階への対策

○ 詐欺に誘引するダイレクトメッセージ等が被害者等の端末に届く前にフィルターする取組や利用者が詐欺に誘因するダイレクトメッセージ等を受信した際に警告表示を行う取組を推進。

○ 契約変更等の機会も活用しながら、国際電話サービスを利用しない設定があることを一層強く国民に周知。また、将来的には、国際電話サービスを利用しない者に対する優遇措置等、国際電話を必要としない人への利用休止を促すような効果的な対策の導入を検討。

○ 迷惑電話、迷惑SMS等の受信を防止又は受信した際の警告を行う有料のサービスについて、事業者に対し、無償化を含めた効果的な措置を要請するとともに、被害防止機能向上のためより効果的な方策を検討し、その普及や有効性の向上を図る。

○ 発信者番号の表示が官公庁等の電話番号に偽装されている手口について、国民に注意喚起を実施するとともに、関係事業者と連携して効果的な対策を検討し、速やかに実施。

（3） 欺罔段階への対策

○ 変化する欺罔の手口について、迅速・的確にその特徴や被害者層、具体的に講じるべき対策等を明らかにした上で、訴求対象・訴求内容と合致する広報啓発の手段を選定するなど、効果的な広報啓発を実施。

（4） 金銭等の交付段階への対策

○ 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、インターネットバンキングの申込みがあった際や利用限度額引上げ時の利用者への確認や注意喚起等の取組を推進。

○ 預金取扱金融機関や暗号資産交換業者によるモニタリングの強化や、暗号資産交換業者への不正送金防止に係る取組を推進。

○ 預金取扱金融機関間において不正利用口座に係る情報を共有しつつ、速やかに口座凍結を行うことが可能となる枠組みの創設について検討。預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組を推進。

○ 犯罪者グループの上位被疑者の検挙、犯罪収益の剥奪等を図るとともに、口座の悪用を牽制するため、捜査機関等が管理する架空名義口座を利用した新たな捜査手法や関係法令の改正を早急に検討。

（5） 犯行後の捜査段階における対策

○ 匿名性の高い通信アプリをはじめとする犯罪に悪用される通信アプリ等について、被疑者間の通信内容や登録者情報等を迅速に把握するために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て検討。

○ 通信履歴の保存の在り方について、電気通信事業における個人情報等保護に関するガイドライン改正や保存義務付けを含め検討。

○ 仮装身分捜査を、令和７年１月に制定した実施要領に基づき適正に実施し、詐欺や強盗等の犯人の検挙、被害の抑止を推進。

3 ID・パスワード等の窃取・不正利用対策

（1） フィッシングサイトへの対策

○ フィッシングサイト判定の高度化・効率化のために生成AIを活用し、閲覧防止措置や警告表示による対策の効率化を図るなど、フィッシングサイトへの対策を推進。

（2）・(3) ID・パスワードやクレジットカード情報の不正入手・利用対策

○ 悪用のおそれのあるクレジットカード情報を国際ブランド各社に提供する枠組みを活用するほか、ECサイトの脆弱性を悪用したクレジットカード情報窃取対策の実施について、カード会社がEC事業者に対して適切に指導を行うよう監督。

○ なりすましメールの対象となる事業者に対し、関係省庁が連携し、メールのなりすまし防止技術（DMARC）の導入推進のため、必要に応じたフォローアップや受信拒否を要求するポリシーでの運用の働き掛けを実施。

（4） マネー・ローンダリングや現金化への対策

預金取扱金融機関等によるモニタリングの強化、EC加盟店等との情報連携等(1･2(4)等再掲)

（5） 犯行後の捜査段階における対策

○ インターネットバンキングに係る不正送金等の実行時に、一般家庭からのアクセスに偽装するための踏み台として家庭用インターネット通信機器が悪用されていることから、その実態を調査・分析し、悪用実態を踏まえた対策を実施。

4 治安基盤の強化等

○ 犯罪グループの首謀者等の検挙、警察・検察におけるサイバー人材の育成の更なる推進、警察庁・都道府県警察間の連携強化等のため、態勢の充実強化を推進。

○ スマートフォン端末等の解析能力の強化、捜査に必要な情報収集の効率化のため、警察・検察の装備資機材の充実強化を推進。

○ 外国機関と連携し、詐欺等対策や邦人保護の取組のほか、情報技術解析の高度化を推進。

○ 地方創生の交付金を活用した防犯カメラの設置等地域防犯力の強化に資する取組への支援を行うなど、防犯対策の強化を推進。

○ 詐欺等のほか、組織的な窃盗や強盗、違法・悪質なホストクラブ営業やスカウト行為、薬物密売、オンラインカジノ等多岐にわたる資金獲得活動に着目した取締り等を推進し、匿名・流動型犯罪グループの資金源への対策を推進。