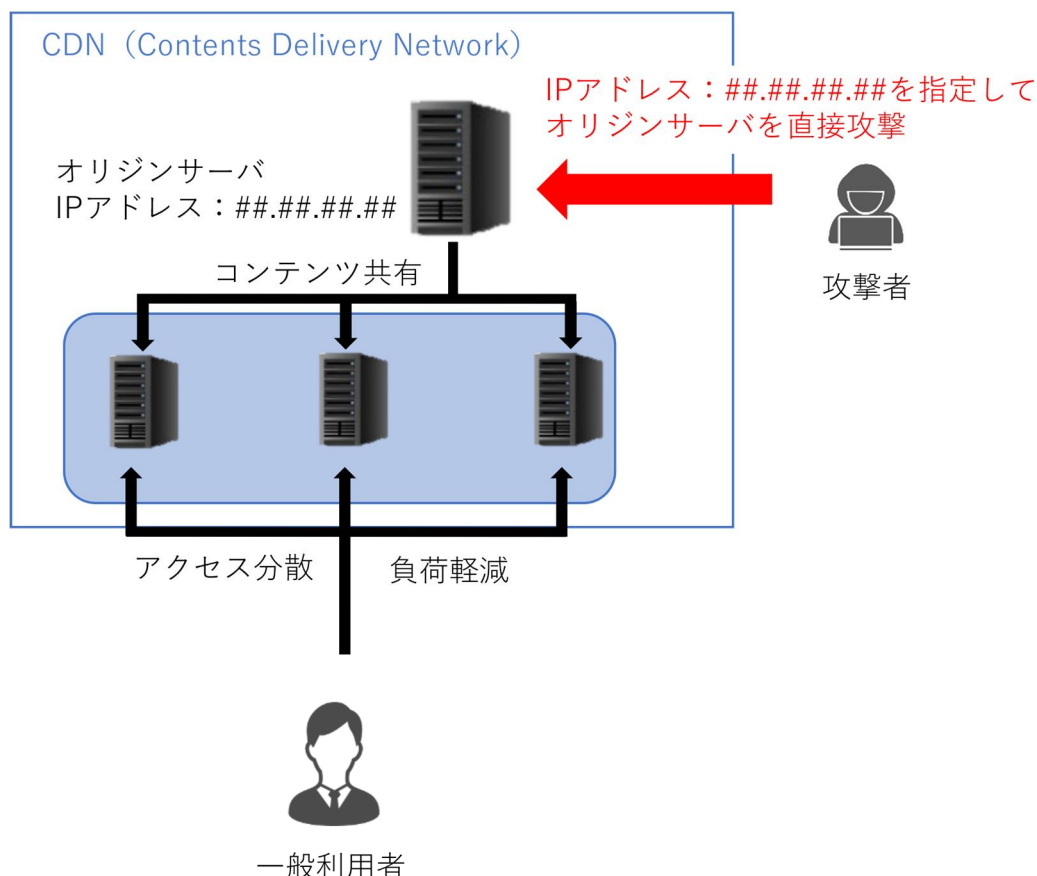


令和7年における
サイバー空間をめぐる脅威の情勢等について

令和8年3月
警察庁サイバー警察局

の通信の遮断、アクセスを監視し攻撃を検知・遮断する機能を持つような対策装置やサービスの導入、サーバ装置、端末、通信回線装置及び通信回線の冗長化等が求められる。

【図表 16：DDoS 攻撃におけるオリジンサーバへの攻撃のイメージ】

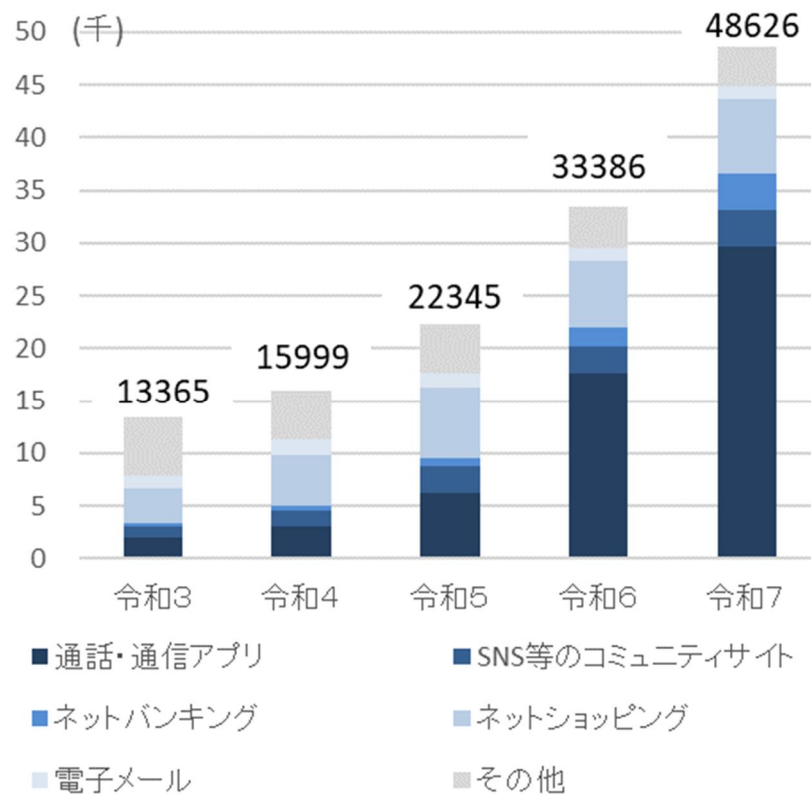


2 インターネット空間を悪用した犯罪に係る脅威情勢

情報通信技術の著しい発展や、日常生活や経済活動へのサイバー空間の浸透は社会に様々な便益をもたらす反面、サイバー空間を舞台とした犯罪をはじめ、新たな治安課題を生み、また深刻化させており、このような情勢は、令和7年中のサイバー関係の警察に対する相談数が約 18 万 5,000 件に達するなどしていることから見てとれる。

また、インターネットを利用した詐欺事案の発生が右肩上がり増加しており、令和7年においては、通話・通信アプリを使用した詐欺が約6割を占める。

【図表 17：インターネットを利用した詐欺の認知件数と内訳】



インターネット上で提供される技術・サービスの中には、犯罪インフラとして悪用され、犯罪の実行を容易にし、あるいは助長するものも存在している。例えば、SNS や匿名性の高いメッセージングアプリは犯罪実行者の募集や、犯罪グループ間の連絡手段として使われ、SMS やメールはフィッシングに悪用されている。また、インターネットバンキングや暗号資産は、特殊詐欺等における被害金の送金先やマネー・ローンダリングなどに悪用されている。さらに、ペイメントサービスのアカウント作成等に利用される SMS 機能付きデータ通信専用 SIM は、契約時の本人確認の義務付けがないことから、犯罪インフラとして悪用されている。

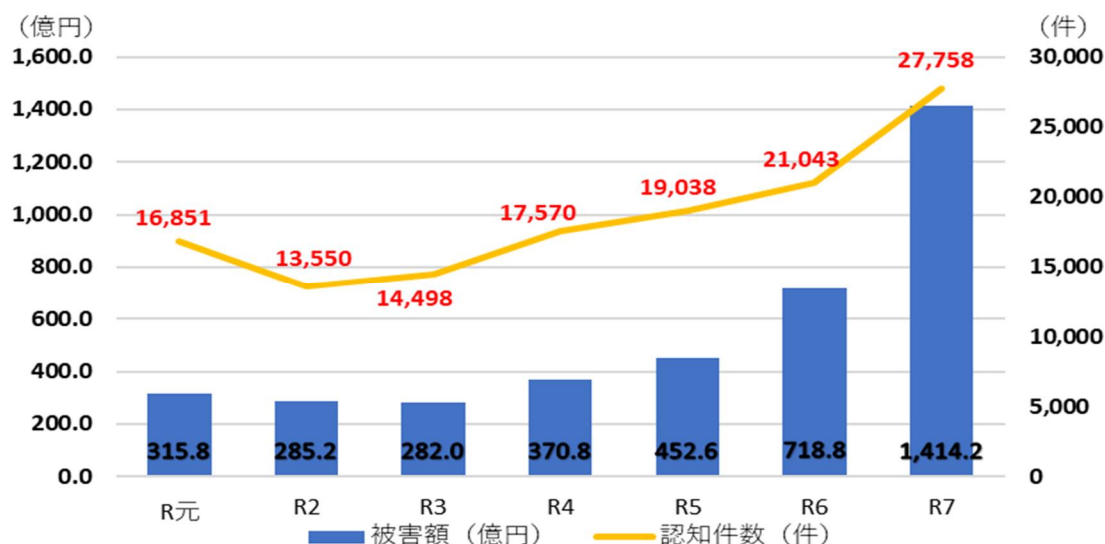
(1) SNS・メッセージングアプリ等を悪用する犯罪

多くの国民が利用する SNS は、犯罪インフラとして悪用されている実態がみられる。例えば、各種犯罪により得た収益を吸い上げる中核部分が匿名化され、SNS を通じるなどしてメンバー同士が緩やかに結び付くなどの特徴を有する「匿名・流動型犯罪グループ」が、SNS で仕事の内容を明らかにせず、「高額」「即日即金」「ホワイト案件」等、「楽で、簡単、高収入」を強調する表現を用いるなどして、犯罪実行者を募集し、特殊詐欺等を敢行していることが確認されている。その際、首謀者、指示役、犯罪実行者の間の連絡手段には、匿名性が

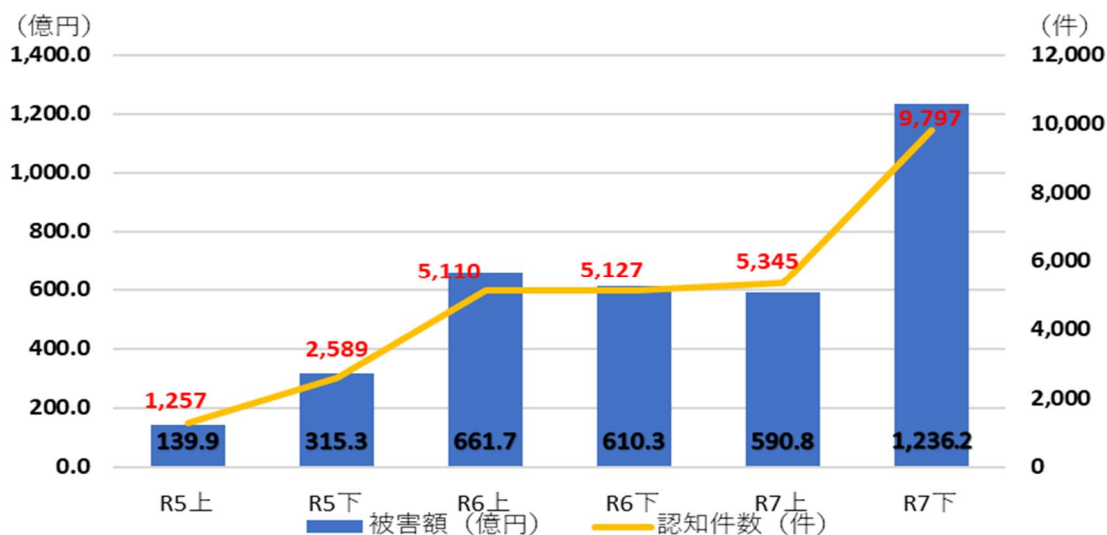
高くメッセージが自動的に消去される仕組みを備えた通信手段が悪用されている実態がみられる。このほか、匿名・流動型犯罪グループの関与が認められるものとして、SNSを通じて対面することなく、やり取りを重ねるなどして関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭をだまし取る又は恋愛感情や親近感を抱かせて金銭をだまし取る SNS 型投資・ロマンス詐欺があり、まさに SNS が犯罪インフラとして悪用されている。

令和 7 年の特殊詐欺の被害額は約 1,414 億 2,000 万円（前年同期比 96.7%増と、過去最悪となった令和 6 年の被害額を上回り、SNS 型投資・ロマンス詐欺の被害額についても約 1,827 億円（前年同期比 43.6%増）と昨年を上回った。

【図表 18：特殊詐欺の認知件数・被害額】



【図表 19：SNS 型投資・ロマンス詐欺の認知件数・被害額】



ムページ上で公開している。

アンケート結果からは、オンラインゲームに関するトラブルに巻き込まれたことがあると回答した人の大半はゲーム内チャットなどのコミュニケーションにまつわるトラブルであったが、その内、3割程度がアカウント乗っ取りやDDoS 攻撃、リアルマネートレードのトラブルに巻き込まれていることが確認され、トラブルの内容としては、チャット機能等の交流機能を通じて暴言を吐かれる等の被害に遭うケースが多く見られる一方で、フィッシングやアカウント乗っ取り等の被害に遭うケースも複数発生していることが確認できた。

また、トラブルに遭った際の対応を分析したところ、アンケート規模の問題により確度は低いが、相談・連絡等の手段を取った場合には、何もアクションを取らなかった場合に対して有意にトラブルが解決しやすいことが見て取れた。

(2) メール・SMS を悪用する犯罪

メールや SMS は、フィッシングに悪用される実態がみられる。フィッシングとは、実在する組織を装ってメールや SMS のリンクから偽のウェブサイト（フィッシングサイト）へ誘導し、同サイトでアカウント情報やクレジットカード番号等を不正に入手する手口であり、これによって得られた情報はインターネットバンキングに係る不正送金やクレジットカードの不正利用に使われている（統計編 143 頁参照）。

令和 7 年におけるフィッシング報告件数は、フィッシング対策協議会によれば、245 万 4,297 件であり、右肩上がりの増加が続いている。

また、令和 7 年におけるインターネットバンキングに係る不正送金事犯の発生件数は 4,747 件、被害総額は約 103 億 9,700 万円となっており、フィッシングがその手口の約 9 割を占める。

フィッシングにおいては、令和元年頃からリアルタイム型フィッシングにより二段階認証を突破する手口が横行するなど、手口の巧妙化が見られる。

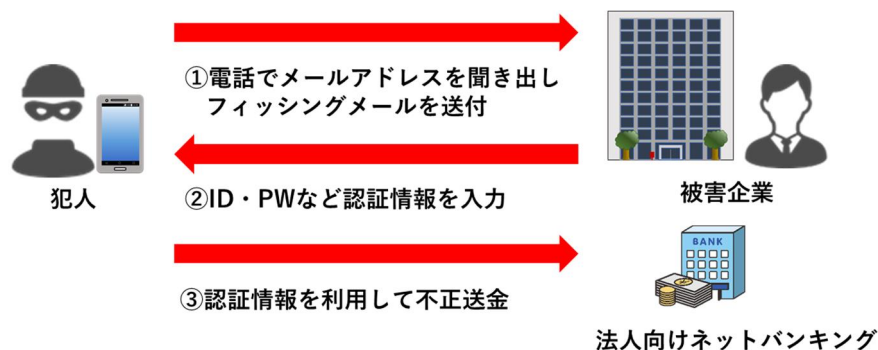
コラム：ボイスフィッシングによる不正送金被害

令和6年秋から令和7年4月にかけて、犯罪グループが企業に架電し、ネットバンキングの更新手続き等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシング（ビッシング）という手口による法人口座の不正送金被害が急増した。同年5月から10月にかけては被害の発生がみられなかったものの、11月には不正送金被害が再び急増し、地方を拠点とした中小規模の金融機関でも多くの被害が出た。

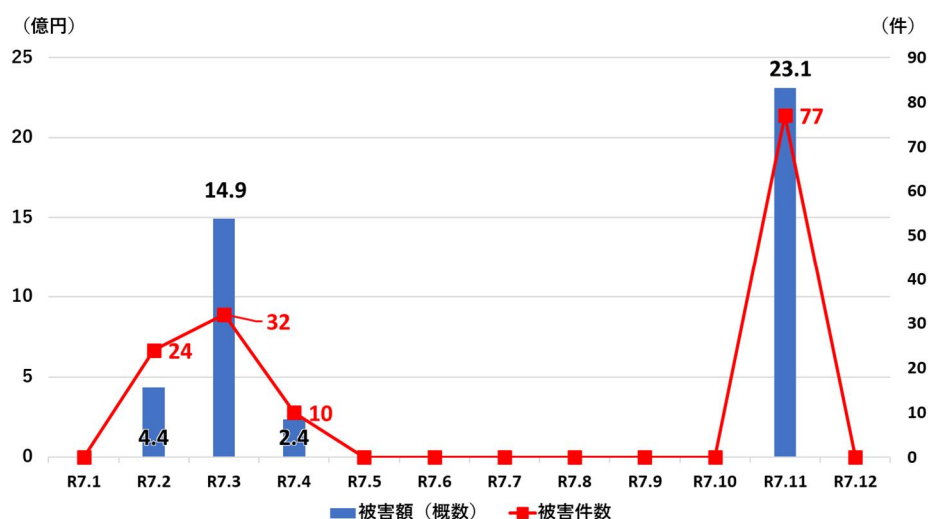
こうしたボイスフィッシングには、発信元番号が国際番号である、自動音声ガイダンスが流れた後に人間の声に切り替わる、通話中にメールアドレスを聴取されリンク付きメールが送られる、といった特徴が見られる。

そこで、ボイスフィッシングの被害を防ぐためには、銀行から電話があった場合に、営業店・代表電話に折り返して本物かどうか確認するといった対応や、インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスするといった対応を社内で徹底する必要がある。

【ボイスフィッシングの流れ】



【図表 23：ボイスフィッシングによる法人口座の不正送金被害件数・被害額】



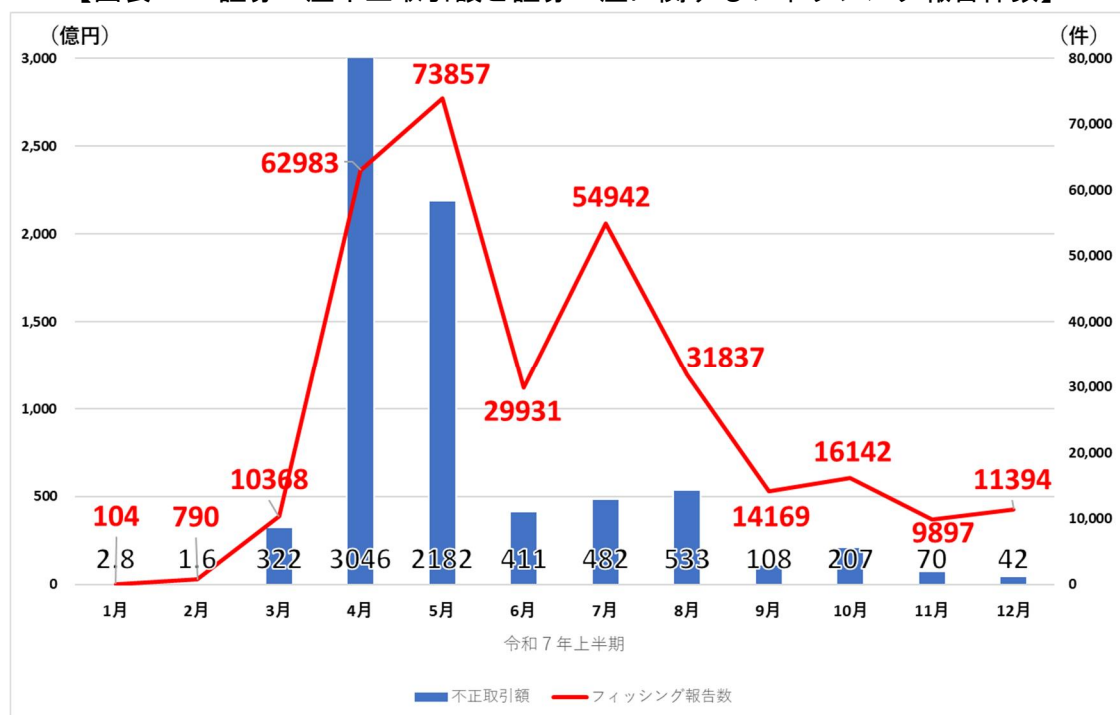
コラム：証券口座への不正アクセス等の急増及び検挙

令和7年3月から5月にかけて、証券会社をかたるフィッシングメールの送信や証券口座への不正アクセス及び不正取引が急増し、金融庁及びフィッシング対策協議会によれば、令和7年における証券口座への不正アクセス件数は1万7,668件、不正取引件数は9,824件、不正売買金額は約7,408億円、証券会社をかたるフィッシングメール報告件数は31万6,414件となるなど、深刻な被害が生じた。

令和7年11月、サイバー特別捜査部及び警視庁等の都道府県警察は、関係機関の協力を得て、捜査を推進した結果、中国籍の男(38)らを金融商品取引法違反（相場操縦行為等の禁止）及び不正アクセス禁止法違反（不正アクセス行為の禁止）で逮捕した。同男らは、自身が管理する証券口座を用いて相場操縦の対象となる株（以下「対象株」という。）を事前に大量に買い付けた上で、氏名不詳者と共謀の上、他人の証券口座に不正アクセスし、被害口座において保有していた株を売却するなどして資金を確保し、対象株を大量に買い付けることで株価を上昇させた。その後、同男が保有していた対象株を高値で売却の発注をするとともに、被害口座において対象株を買い付けることで取引を成立させ、購入額と売却額の差額を利益として得ていた。

本件を含め、多発した証券口座への不正アクセスや不正取引に対し、サイバー特別捜査部は、証券会社をかたるフィッシングメールやフィッシングサイトに関するデータの解析、暗号資産の送信先アドレスの分析、全国で発生した同事案の情報集約等により、関係都道府県警察による捜査に貢献している。

【図表 24：証券口座不正取引額と証券口座に関するフィッシング報告件数】



② 関係機関との連携を通じた情報発信

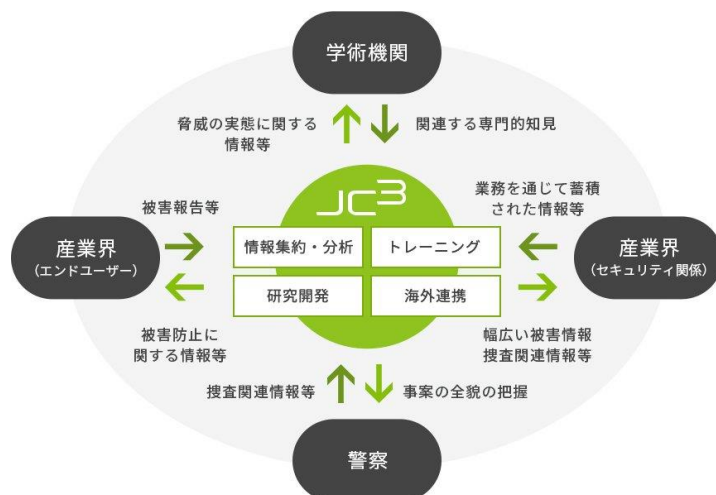
警察では、様々な関係機関と連携した情報発信を行っており、特に一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center の略）との連携を推進している。

JC3 は、米国で産学官連携の枠組みとして成果を上げている非営利組織である NCFTA¹⁶ に類似の新たな組織を構築する必要性が、平成 25 年 12 月に閣議決定された「「世界一安全な日本」創造戦略」等において、指摘されたことを受け、日本版 NCFTA として産学官の情報や知見を集約・分析し、その結果等を還元することにより、国民が安全かつ安心してインターネットを利用できる環境の構築に貢献することを目的として設立され、平成 26 年 11 月に業務を開始した。

警察では、JC3 に対しサイバー犯罪の被害実態、犯行手口等を共有し、セキュリティベンダー、金融機関等の会員企業の対策に反映し、JC3 からは会員企業における被害状況や対策の実施状況の共有を受け、警察における捜査や被害防止活動に活用している。

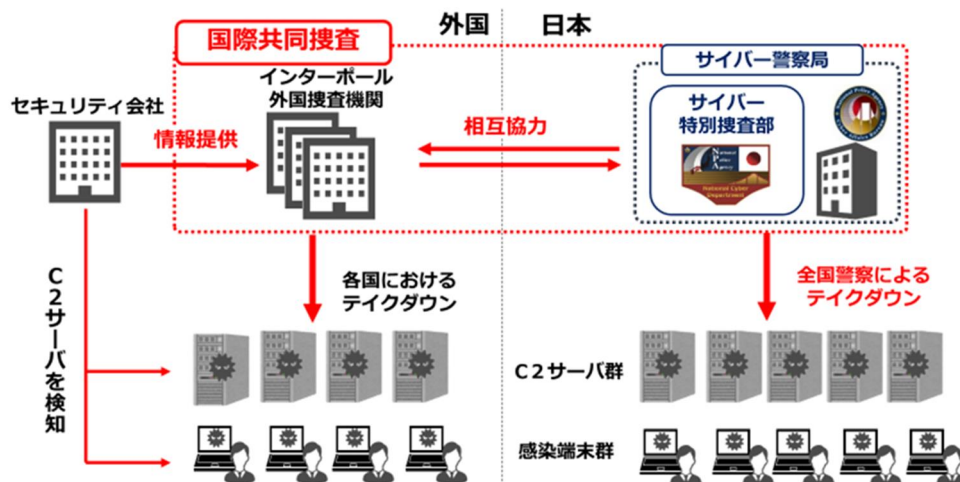
JC3 では、利用者がだまされて不正なスマートフォンアプリを導入することが原因で、個人のスマートフォンから身に覚えのない大量の SMS を配信し、料金が高額になる等の事象が確認されていることから、こうした悪性の SMS が存在することを認識し、安易な URL リンクへのアクセスやアプリの導入に危険が伴うことについて注意喚起している。さらに最近では、偽 SMS の文面の作成に生成 AI を悪用したとみられる事象を確認するなど、攻撃手法が高度化していることについての注意喚起も行っている。

【図表 42：日本サイバー犯罪対策センター（JC3）の概要】



¹⁶ National Cyber-Forensics & Training Alliance の略。

【図表 45：インフォスティーラーに対する INTERPOL との国際共同捜査】



② インターネット空間を悪用した犯罪に関するインフラへの対処

○ フィッシングサイト対策

警察庁においては、都道府県警察や一般財団法人日本サイバー犯罪対策センター（JC3）等が相談等を通じて把握した海外の偽サイト等に係る URL 情報を集約し、ウイルス対策ソフト事業者等に提供しており、当該事業者によってウイルス対策ソフトの機能による警告表示等、当該サイトの閲覧を防止する対策がとられている。

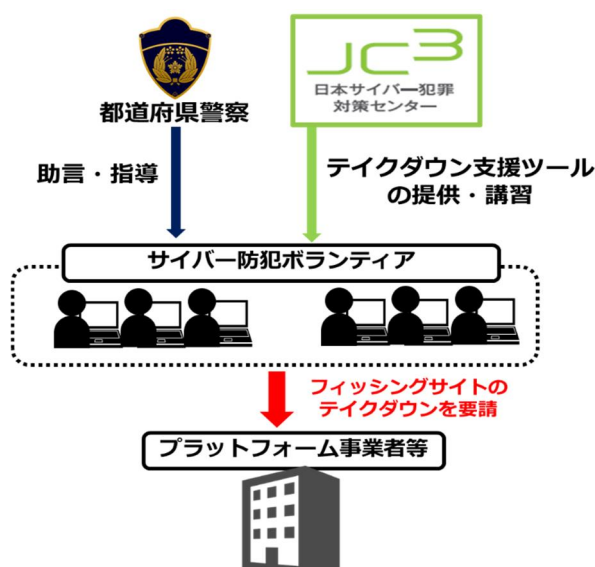
また、1つの IP アドレス上に、数百のフィッシングサイトが構築されているといったフィッシングサイトの特性を踏まえた先制的な対策として、警察庁において、同一の IP アドレスに紐づくドメイン情報を独自に収集し、未把握のフィッシングサイトを発見・提供している。

さらに、フィッシングの手口が巧妙化し、被害が急増している情勢に鑑み、利用者保護のため、フィッシングサイトにアクセスさせないための対策として、「なりすましメールを防ぐ技術（DMARC¹⁷等）への対応促進」を始め、「フィッシングサイトの閉鎖促進」や「パスワードに代わって生体認証等により簡単かつ安全にログインできる認証方法（パスキー）の普及促進」について、所管省庁を通じ、事業者に対する対策の要請を実施した。

¹⁷ Domain-based Message Authentication Reporting, and Conformance

官民が連携したフィッシングサイト対策として、JC3では、専門的な知識を持たない人であってもプラットフォーム事業者等に対してサイトのテイクダウン依頼を行うことができるツールを開発し、サイバー防犯ボランティア等に提供するとともに、警察庁後援のもと、サイバー防犯ボランティア向けの「フィッシングサイト撲滅チャレンジカップ」を実施している。

【図表 46：フィッシングサイト撲滅チャレンジカップ】

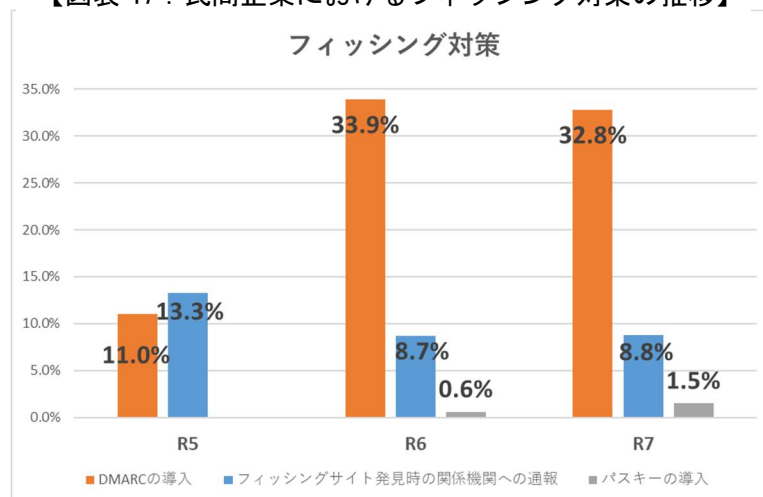


コラム：民間企業等における不正アクセス行為対策の調査結果

警察庁において、無作為に抽出した民間企業や行政機関等に対して不正アクセス行為対策等に関する調査を実施した結果、民間企業等のフィッシング対策として、DMARC 導入率は令和 6 年に大きく増加した。

また、民間企業等が過去 1 年間で受けたサイバー攻撃は、過去 10 年間で比較すると DDoS 攻撃は半減し、マルウェア設置・感染は大幅に減少した。さらに、民間企業等における対応マニュアルや要領の策定状況については、約 55%が策定済みで、過去 10 年で増加傾向であった。（統計編 158 頁参照）

【図表 47：民間企業におけるフィッシング対策の推移】



※パスキーの導入は、令和 6 年から調査項目に追加

○ インターネットバンキングに係る不正送金対策

警察庁は、令和7年11月からボイスフィッシングによる法人口座の不正送金被害が再び急増する深刻な事態を受け、金融庁、一般社団法人全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（JC3）と連名で、広報啓発資料「サイバー警察局便り」を作成した上で、警察庁ウェブサイト等にて公開し、その手口の詳細や対策に関する注意喚起を実施した。

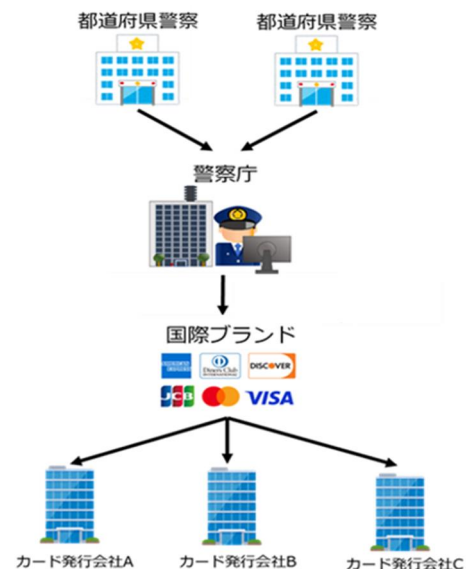
○ 証券口座不正取引対策

証券口座不正取引の被害情勢を踏まえ、警察庁は、令和7年5月、ウェブサイト等において証券会社をかたるフィッシングについて注意喚起を行ったほか、同年7月には、金融庁と連名で、日本証券業協会を含む金融関係協会に対して、被害を踏まえた具体的なフィッシングの手口やその対策を示した上で、顧客口座・アカウントの不正アクセス・不正取引対策の強化について要請した。（資料編106頁参照）

○ クレジットカード不正利用対策

各都道府県警察で把握した、悪用されたクレジットカード番号を警察庁で速やかに集約し、カード発行会社を含む決済システム全体を統括する国際ブランド各社に対し、一括して提供しており、クレジットカード発行会社における不正利用対策に活用されているところ、令和7年は、約187万件のクレジットカード番号を国際ブランド各社に提供した。

【図表48：国際ブランドに対する不正クレジットカード番号情報提供】



③ 違法・有害情報に関するインフラへの対処

警察では、サイバーパトロール等による違法・有害情報の把握に努め、これを端緒とした取締り及びサイト管理者等への削除依頼を実施している。

○ インターネット・ホットラインセンター（IHC）における取組

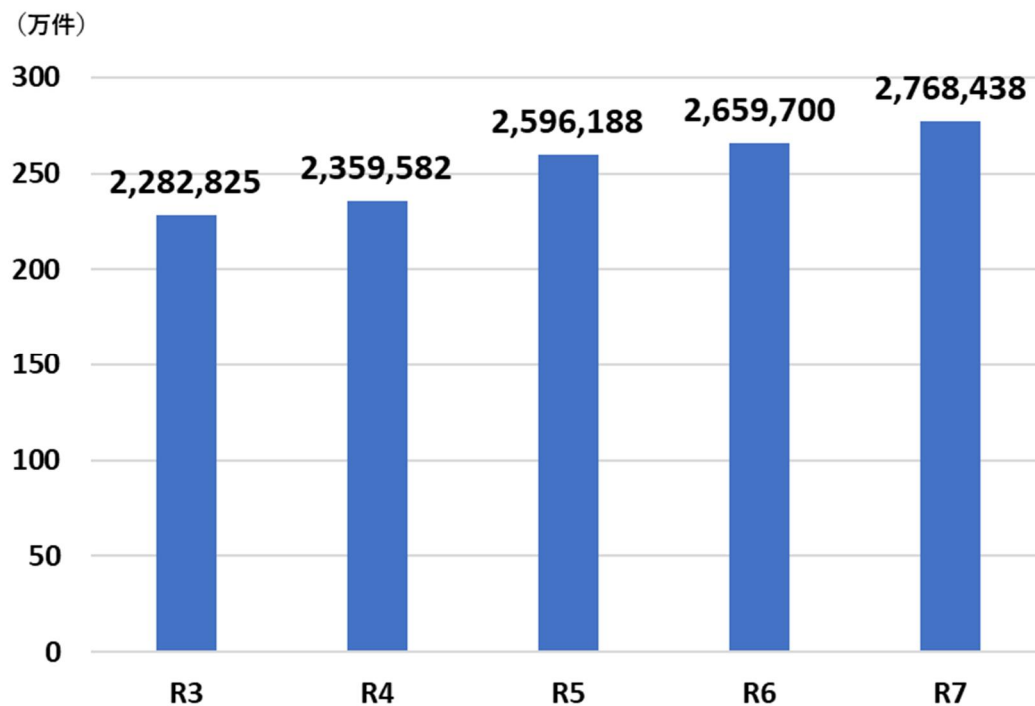
警察庁では、インターネット利用者等から違法・有害情報に関する通報を受理し、警察への通報、サイト管理者等への削除依頼等を行うインターネット・ホットラインセンター（IHC）を事業委託するとともに、違法情報、重要

統計編

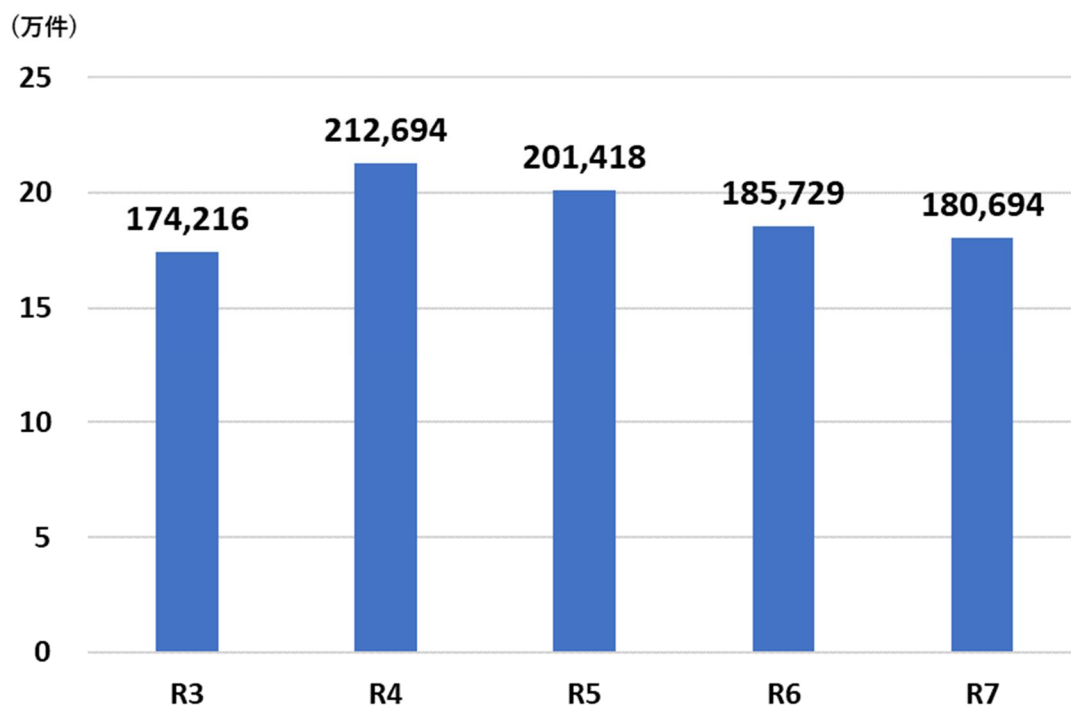
(第1部2「インターネット空間を悪用した犯罪に係る脅威情勢」関連)

警察に対する相談

1 警察で取り扱った相談件数の推移



2 警察で取り扱ったサイバー関係の相談件数の推移

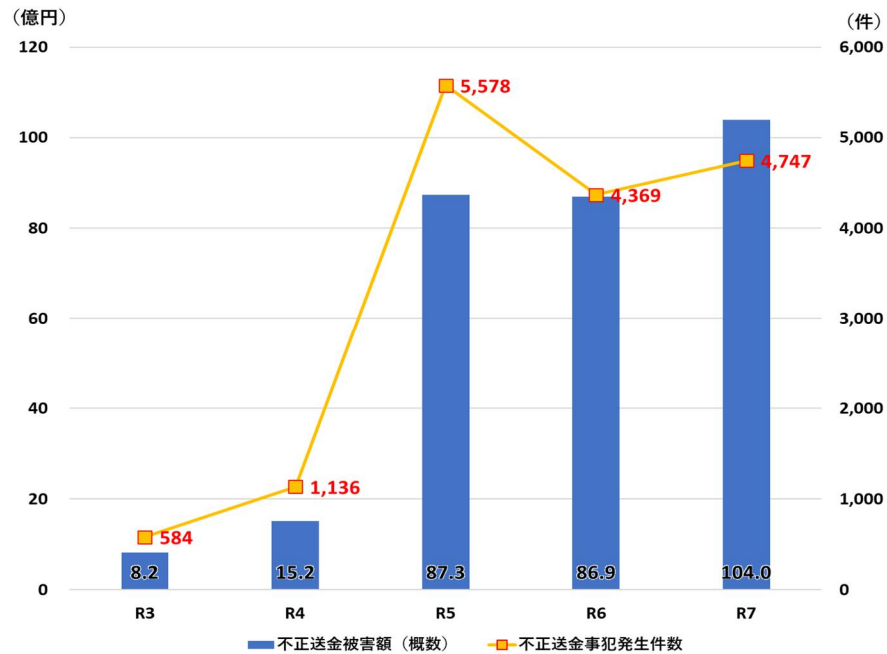


統計編

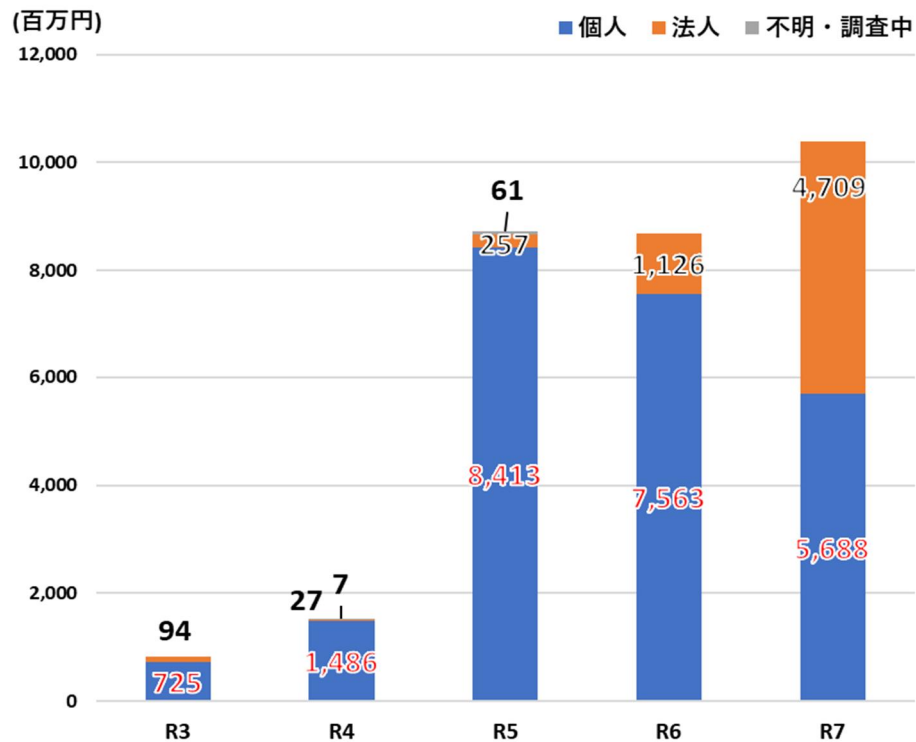
(第1部2「インターネット空間を悪用した犯罪に係る脅威情勢」関連)

インターネットバンキングに係る不正送金事犯 ①

1 インターネットバンキングに係る不正送金事犯発生件数及び被害額の推移



2 インターネットバンキングに係る不正送金被害額の推移 (個人・法人別)



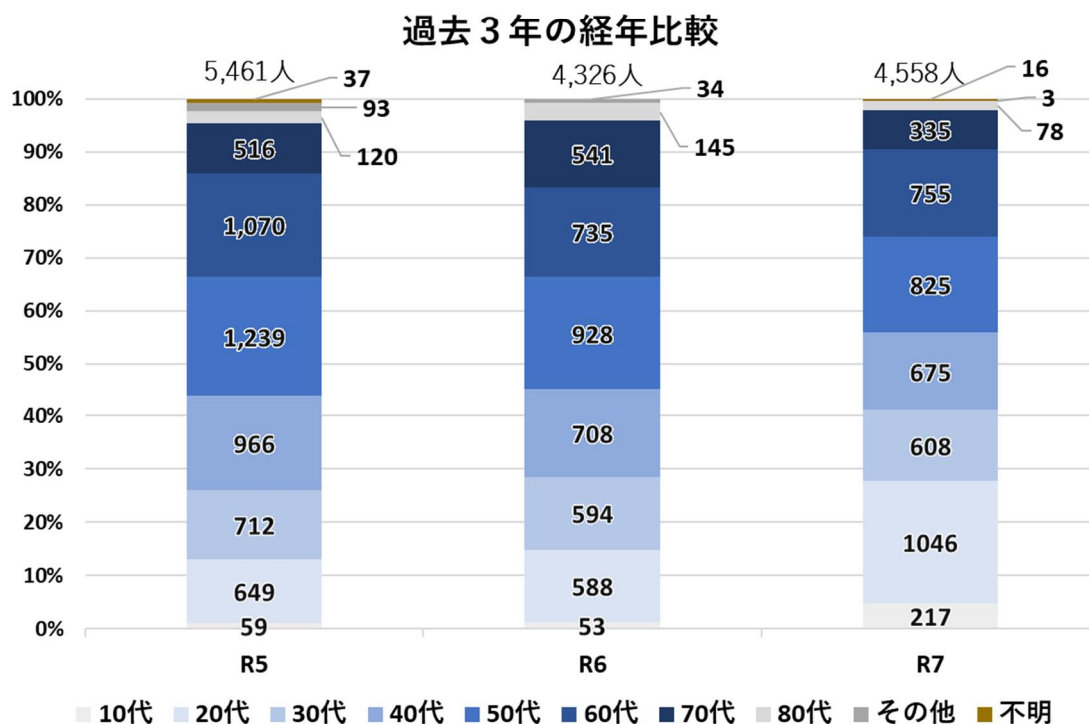
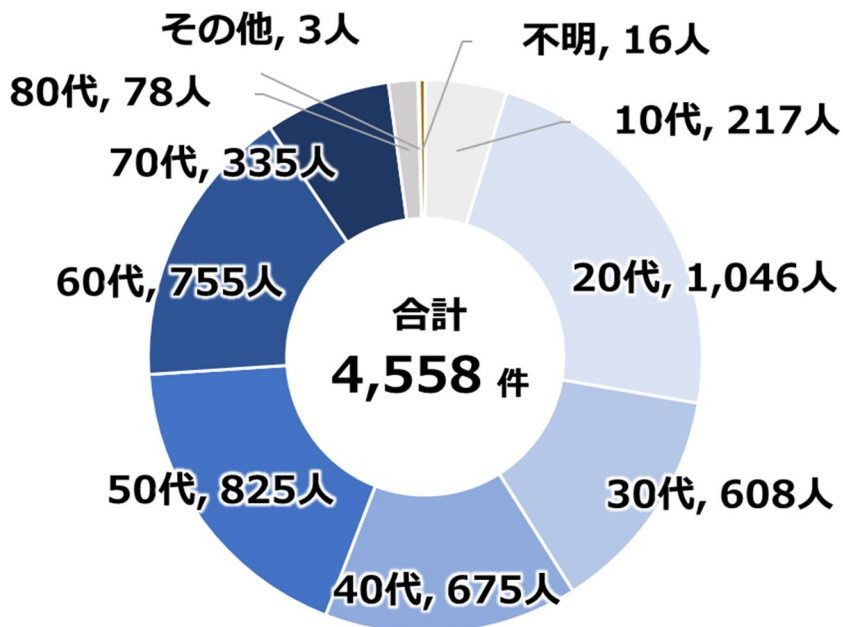
※ 令和7年中に法人被害が急増した背景として、ボイスフィッシングによる法人口座の不正送金被害が急増したことが挙げられる。

統計編

(第1部2「インターネット空間を悪用した犯罪に係る脅威情勢」関連)

インターネットバンキングに係る不正送金事犯 ③

4 個人のインターネットバンキングに係る年齢別の不正送金被害者数



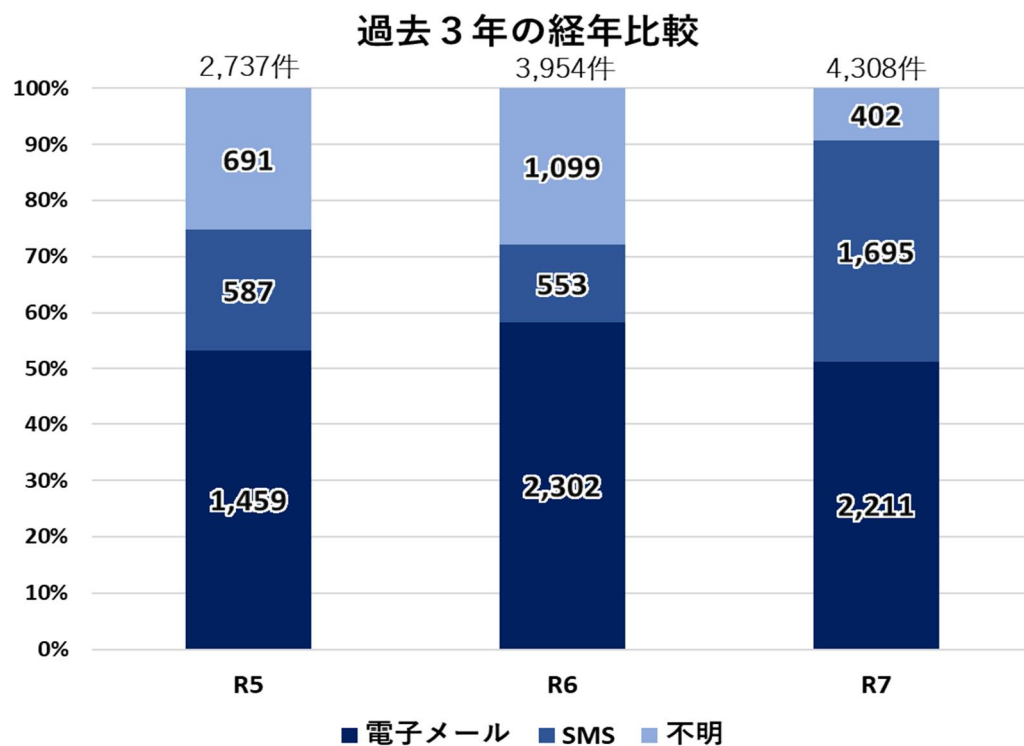
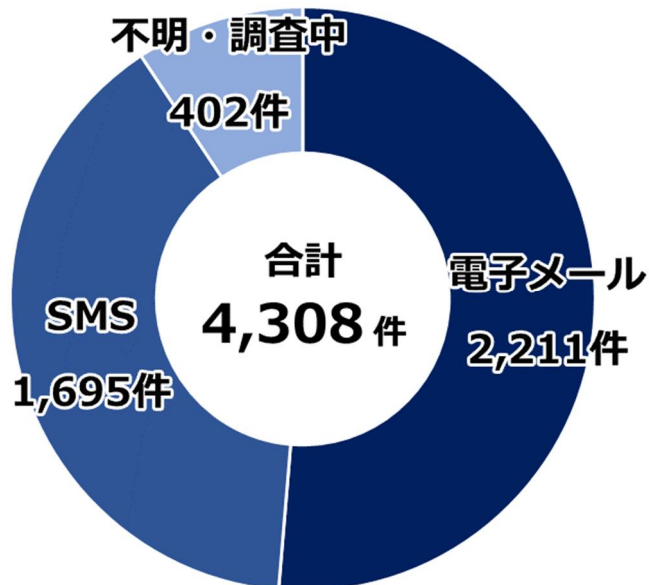
※ 発生件数が異なるため、各年の合計数値（被害者数）は異なる。

統計編

(第1部2「インターネット空間を悪用した犯罪に係る脅威情勢」関連)

インターネットバンキングに係る不正送金事犯 ④

5 フィッシングサイトへ誘導する手口別の不正送金発生件数



※ 発生件数が異なるため、各年の合計数値は異なる。

※ 令和7年中にSMSが増加した要因として、モバイルマルウェアに感染した端末を悪用して、フィッシングサイトへ誘導する悪質なSMSを大量配信されていることが考えられる。

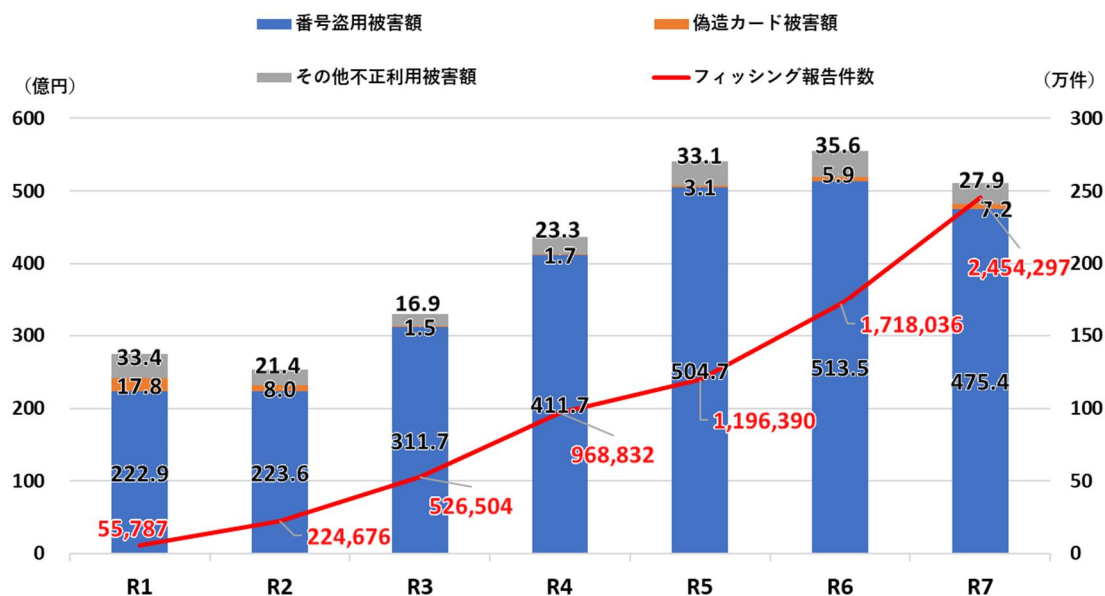
統計編

(第1部2「インターネット空間を悪用した犯罪に係る脅威情勢」関連)

(第2部1「検挙に向けた取組」関連)

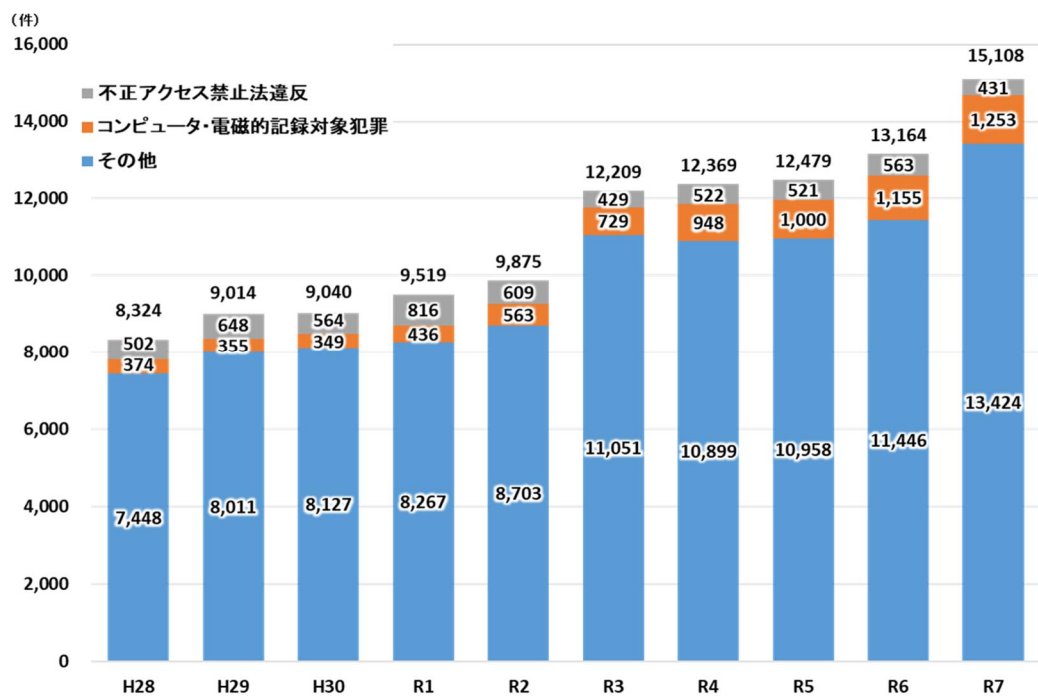
フィッシング報告件数及びクレジットカード不正利用被害額

1 フィッシング報告件数及びクレジットカード不正利用被害額の推移



サイバー犯罪・サイバー事案 ①

1 サイバー犯罪³の検挙件数の推移



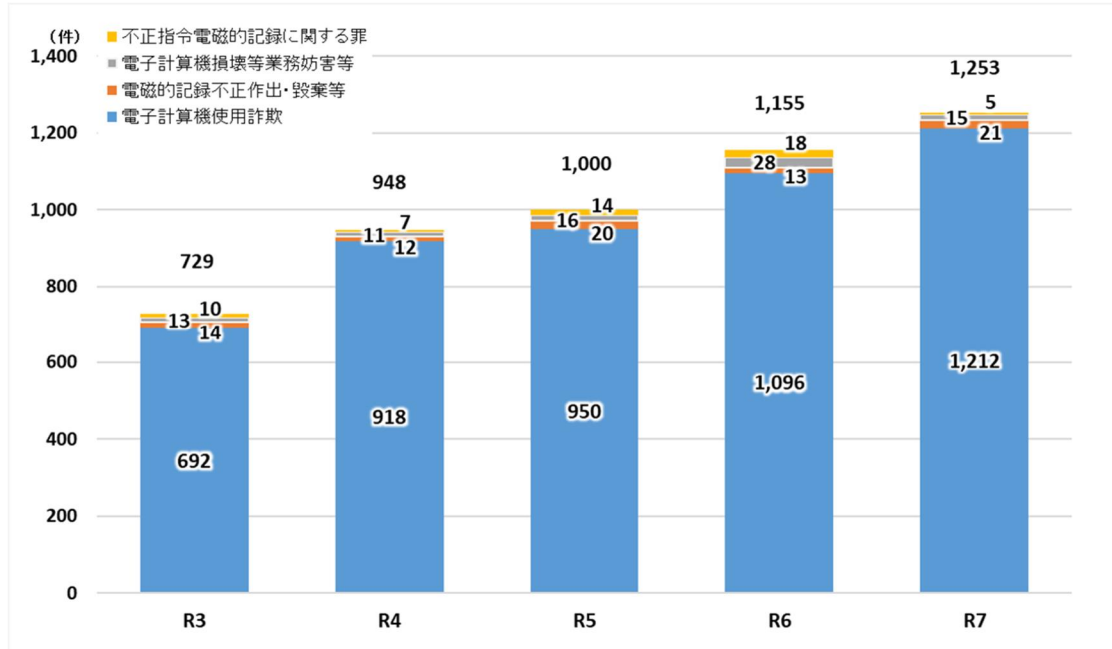
³ 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

統計編

(第2部1「検挙に向けた取組」関連)

サイバー犯罪・サイバー事案 ②

2 前記1中、コンピュータ・電磁的記録対象犯罪の検挙件数の推移



3 サイバー犯罪の検挙数の年齢構成

