広　報　資　料
令和３年３月４日
警　　察　　庁

令和２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

１　情勢概況

新型コロナウイルス感染症の感染拡大に伴うテレワークの実施やキャッシュレス決済の普及など、サイバー空間が、日常生活を含む様々な活動を営む場となりつつある中、新たなサイバー犯罪やサイバー攻撃が国内外において発生している状況にあり、サイバー空間における脅威は、極めて深刻な情勢。

２　社会のデジタル化の進展とサイバー空間の脅威情勢

(1)　社会のデジタル化の進展に伴う脅威

○　国内において、防衛関連企業、電気通信事業者等に対する攻撃、国外において、新型コロナウイルス感染症のワクチン開発に関連する攻撃が発生。

○　ランサムウェアによる二重恐喝（ダブルエクストーション）、スマートフォン決済サービスに係る不正振替事犯等が発生。

○　新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案として、詐欺や不審メール・不審サイト等887件を都道府県警察からの報告により把握。

(2)　サイバー空間の脅威情勢

○　警察庁が国内で検知したサイバー空間における探索行為等とみられるアクセスの件数は増加傾向。

○　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・被害額は、被害が急増した前年と比べて減少しているものの、発生件数は引き続き高い水準。

○　警察によるサイバー犯罪の検挙件数は、前年と比べて増加し、過去最多を更新。

３　警察における取組

○　重要インフラ事業者等に対し、ウェブ会議システム、ＩＴインフラ管理ソフトウェアのぜい弱性等に関する注意喚起を実施。

○　スマートフォン決済サービスに係る不正振替の手口に関し、金融庁等と連携して注意喚起を実施。

○　新型コロナウイルス感染症に関連し、偽の特別定額給付金の申請サイトに誘導する手口について、ＪＣ３と連携し、注意喚起を実施。

別　添

令和２年におけるサイバー空間をめぐる脅威の情勢等

令和２年中は、世界中で新型コロナウイルス感染症が猛威を振るい、我々の生活環境も大きく変容することとなった。我が国では、感染拡大を防止するための「新しい生活様式」の導入やテレワークの積極的な実施などにより業務や取引に関するデータをオンラインで取り扱う機会が増加したことに加え、日常生活においてもキャッシュレス決済の普及が一層進むなど、サイバー空間は、全国民を活動主体として、重要な取引やコミュニケーションを含む日常の様々な活動が営まれる公共性の高い場となりつつある。

このような中、令和２年においても、サイバー攻撃・サイバー犯罪はその手口を深刻化・巧妙化させつつ国内外で多数発生しており、サイバー空間における脅威は、極めて深刻な情勢となっている。

○　サイバー空間の脅威情勢

令和２年中は、ソフトウェアやシステムのぜい弱性を悪用した攻撃や、標的型メール攻撃などを通じて各種ランサムウェア（身代金を要求する不正プログラム）に感染させるなどの事案が多数発生した。国外では、米国の大手ＩＴインフラ管理ソフトウェア会社が提供する製品のぜい弱性を悪用し、同国の政府機関等を標的としたサイバー攻撃の被害や新型コロナウイルス感染症のワクチン開発等を標的としたサイバー攻撃などが確認された。また、国内においても、複数の防衛関連企業、大手電気通信事業者が、外部からの不正アクセスを受け情報が流出した可能性があると公表したほか、大手製造業者からも、従業員が在宅勤務時に社用端末からＳＮＳを利用した際にウイルスに感染させられるなどの手法により個人情報等が流出したとの発表が行われるなど、国家の関与が疑われるものも含め、国内外で政府機関、重要インフラ事業者等を標的としたサイバー攻撃が激しさを増している。また、警察庁が国内で検知した、サイバー空間における探索行為等とみられるアクセスの件数についても増加の一途を辿っている。Mirai[*1] ボットに関連した多数のアクセスが引き続き観測されているほか、インターネットに接続されている機器やサービスのぜい弱性の有無を把握するための広範囲のポートに対するアクセスが多数行われるなど、サイバー攻撃の準備行為とみられる活動が広がりを見せている状況がうかがわれる。

同年中のサイバー犯罪については、警察による検挙件数が過去最多となった。また、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・被害額は、

---

*1　ＩｏＴ機器を感染対象とする不正プログラム

下半期に被害が急増した前年と比べて、被害額は大幅に減少したものの、発生件数はやや減少したにとどまり引き続き高水準で推移している。これらの被害の多くは、前年から継続しているＳＭＳや電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられる。このほか、特異な事案として、いわゆる「ＳＭＳ認証代行[*2]」が確認されている。「ＳＭＳ認証代行」は、サイバー空間における本人確認の手段として広く用いられるＳＭＳ認証の信頼性を貶める悪質な行為であるとともに、特殊詐欺等に必要な犯行ツールを提供する犯罪インフラにもなっている。

こうしたサイバー空間の脅威に対し、警察では、重要インフラ事業者等に対してサイバー攻撃等について注意喚起を行うなどしたほか、東京2020オリンピック・パラリンピック競技大会関連事業者等とのサイバー攻撃の発生を想定した共同対処訓練を実施して、事態対処能力の強化を図っている。また、スマートフォン決済サービスに係る不正振替事犯の手口に関して金融庁等と連携した注意喚起を実施したほか、詐欺サイト対策では、引き続き一般財団法人日本サイバー犯罪対策センター（ＪＣ３）と連携して各種対策を推進している。

○　デジタル化社会の進展と顕在化する脅威

新型コロナウイルスの感染防止のため、各組織においてテレワークの導入が進む中、事業所と比較してセキュリティが確保されていない自宅等のテレワーク環境や、テレワーク用のソフトウェアのぜい弱性等を狙ったサイバー攻撃が発生している。警察庁のリアルタイム検知ネットワークシステムにおける観測においても、リモートデスクトップサービスを標的とした広範な宛先ポートに対するアクセスの増加が認められており、このようなテレワーク関連の既知のぜい弱性の悪用を企図していると思われる攻撃は今後も継続して実行される可能性がある。

また、事業所の拠点間や関連企業との間のシステムの連携が進む中、セキュリティ対策が不十分である事業所（支店、海外拠点等）や関連取引先企業等のシステムを経由した攻撃も複数確認されている状況にある。また、12月に発表された米国の大手ＩＴインフラ管理ソフトウェア会社に係る攻撃では、当該事業者の製品に係るアップデートファイルに不正なコードが埋め込まれ、当該アップデートを行った顧客全体にぜい弱性が拡散するなど、影響がこれまでになく広がっており、各種サプライチェーンリスクへの対応は重要な課題となっている。

さらに、ランサムウェアによる被害の深刻化・手口の悪質化も全世界的に問題となっている。従来のランサムウェアによる被害は、重要データ等を暗号化

---

*2　通信当事者以外の第三者が、ＳＭＳ認証に用いる携帯電話番号や当該認証に係る認証コードを当該通信当事者に提供する行為

し、復号の対価として金銭を要求するものが一般的であったが、最近の事例ではデータの暗号化のみならず窃取を敢行し、対価を支払わなければ当該データを公開するという二重恐喝（ダブルエクストーション）を行うより悪質なケースも認められている。また、犯行に用いられるランサムウェアやそれらを用いた二重恐喝の手法そのものが闇サイト上で商品として販売されるなど、これらのより悪質な手口の拡散も見られる。６月には、国内においても、産業制御型システムに影響を及ぼすランサムウェアが確認されている。

国民の間での利用が広がるキャッシュレス決済においては、国内の事業者が提供するスマートフォン決済サービスにおいて、金融機関に開設された口座情報が不正に入手・連携され、不正なチャージが行われる事案が発生した。キャッシュレス決済の普及に伴い新たなサービスも次々と生まれているところ、これらのサービスにおいては利用者の利便性の観点に加えてセキュリティの確保や不正利用の防止の観点も十分に踏まえつつ、発生し得る脅威に応じて対策を講じる必要がある。

近年、急速に被害が広がっているEmotet[*3] についても、パスワード付きzipファイルを利用した新たな拡散の手口が認められた。このようなパスワード付きzipファイルなどのファイルは、メール配信経路におけるマルウェア検知をすり抜けてしまうことからメールの受信前に駆除できないおそれが高く、同種の手法によるマルウェア被害拡大の可能性が引き続き懸念される。

このほか、新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案として、マスク不足に便乗した詐欺サイトや偽の給付金の申請サイトなどが確認されているところ、今後も、国民の不安感などの社会情勢に乗じた新型コロナウイルス感染症の感染状況やワクチン関連の情報を騙る不審メールや不審サイト、詐欺事案などが横行する可能性がある。

---

*3　コンピュータの利用者が送受信したメールの宛先、本文等の情報を窃取し、当該情報を基になりすましのメールを作成・送信することで感染を拡大する機能を持つ不正プログラム。

令和３年１月、欧州刑事警察機構等は、オランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ及びウクライナの当局が連携し、Emotetのボットネットを破壊したと発表した。

１　令和２年中の主な事例

(1)　サイバー攻撃の事例

○　国内における事例

・　防衛関連企業に対するサイバー攻撃

防衛関連企業は、１月にはサイバー攻撃を受け情報が外部に流出した可能性があることを、２月には流出した可能性のある情報には防衛関連情報が含まれていたことをそれぞれ公表した。さらに11月、同企業は再びサイバー攻撃を受け、国内取引先の金融機関口座に関する情報が流出したと発表した。このサイバー攻撃は、１月及び２月に公表したサイバー攻撃とは異なる手口が用いられた可能性が高いとしている。

・　電気通信事業者に対するサイバー攻撃

５月、大手電気通信事業者は、海外拠点への侵入をきっかけとした国内のサーバに対する不正アクセスにより、一部の情報が社外に流出した可能性があることを発表した。さらに７月、同社はリモートアクセスを利用したＢＹＯＤ[*4] 端末を経由した不正アクセスにより、社内ファイルが閲覧された可能性があることを発表した。

・　製造業者に対するサイバー攻撃

８月、大手製造業者は、ＳＮＳを悪用したソーシャルエンジニアリングを発端として従業員の個人情報等が流出したと発表した。グループ企業の従業員が在宅勤務時に社有の端末でＳＮＳを利用した際、ウイルスを含んだファイルをダウンロードしたことでウイルスに感染、その後当該従業員が出社して社内ネットワークに接続したことで感染が拡大したとしている。

○　国外における事例

・　新型コロナウイルス感染症のワクチン開発等を標的としたサイバー攻撃

７月、米国、英国及びカナダは、新型コロナウイルス感染症に関連する研究及びワクチン開発に関連して、APT29（Cozy Bear,The Dukes）[*5] と呼ばれるサイバー攻撃集団が研究情報及び知的財産を窃取しようとしているとして、注意喚起を行った。これによれば、APT29はロシアの諜報機関に属する集団であることが確実視されており、政府機関、医療機関等を標的としてサイバー攻撃を行っているとされている。

---

*4　Bring Your Own Deviceの略。従業員が自身で保有する端末を業務に使用すること。

*5　APT攻撃（Advanced Persistent Threat:高度で持続的な脅威）と呼ばれているサイバー攻撃を実行する集団は世界中で確認されており、セキュリティベンダー等が命名した名称で一般に呼称されている。APT攻撃を実行するサイバー攻撃集団には国家の関与が疑われるものが多く存在する。

・　米国司法省による中国籍サイバー攻撃者の起訴

７月、米国司法省は、企業、政府、非政府組織等へのサイバー攻撃で中国籍の２人を起訴したと発表した。攻撃者は中国の政府機関の利益等を目的として活動し、新型コロナウイルス感染症のワクチン開発等に関連する企業のネットワークのぜい弱性の調査等を行っていたとしている。

・　米国司法省によるＧＲＵ構成員の起訴

10月、米国司法省は、平昌大会に対するサイバー攻撃等に関与したとして、ロシア軍参謀本部情報総局（ＧＲＵ）に所属する６人を起訴したと発表した。平昌大会に対するサイバー攻撃では、国際オリンピック委員会（ＩＯＣ）職員等を標的としたサイバー攻撃及び「Olympic Destroyer」と呼ばれるマルウェアを用いたコンピュータへの侵害を行ったとしている。

・　ＩＴインフラ管理ソフトウェアのぜい弱性を利用したサイバー攻撃

12月、米国サイバーセキュリティ・インフラストラクチャー・セキュリティ庁（ＣＩＳＡ）は、遅くとも３月から米国の政府機関、重要インフラ事業者等が同国の大手ＩＴインフラ管理ソフトウェア会社が提供する製品のぜい弱性を利用したサイバー攻撃の被害を受けているとして、必要な対策を講じるよう注意喚起を発出した。さらに令和３年（2021年）１月、米国連邦捜査局（ＦＢＩ）、ＣＩＳＡ等は、当該事案にロシアが関与している可能性が高いとの共同声明を発表した。

(2)　サイバー犯罪の事例

○　企業等を対象としたランサムウェア感染事案

11月、大手企業がランサムウェアに感染し、同企業が保有する個人情報等が窃取されて暗号化された上、当該情報を公開しないことと引き換えに取引に応じるように脅迫を受ける二重恐喝とみられるランサムウェア感染事案が発生した。

○　スマートフォン決済サービスに係る不正振替事犯

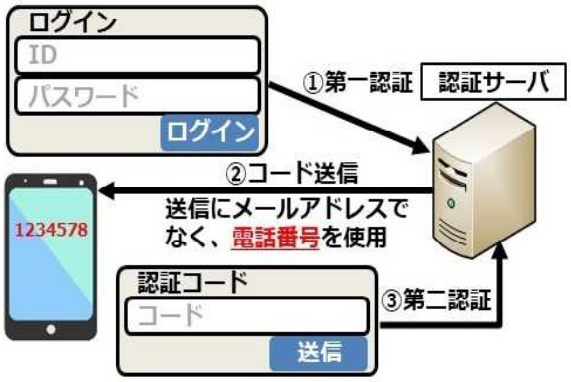
９月、事業者が提供するスマートフォン決済サービスに関して、同社と業務提携する金融機関に開設された口座情報を不正に入手・連携し、不正な振替（チャージ）を行う事案が確認された。

【図表１：スマートフォン決済サービスの不正振替のイメージ】

○　データＳＩＭカードを利用したＳＭＳ認証代行事案

２月、本人確認が行われていないＳＭＳ機能付きのデータＳＩＭカードを利用し、他人にＩＰ電話アプリのアカウント作成時に必要な電話番号及び認証コードを有償で提供し、利用者と異なる電話番号を登録させるＳＭＳ認証代行の事案が確認された。本件では、携帯電話番号や認証コードを提供するため、約100枚ものデータＳＩＭカードを悪用しており、これにより取得された電話番号の一部が、ＩＰ電話アプリを用いて特殊詐欺に悪用されていたことが確認されている。

【図表２：ＳＭＳ認証の仕組みとＳＭＳ認証代行サービスの概要】



ＳＭＳ認証の仕組み

ＳＭＳ認証代行サービスの概要

○　金融機関の公式アプリを利用した不正出金事案

金融機関の公式アプリが不正に有効化された後、キャッシュカードを用いることなく、ＡＴＭでの出金が可能なアプリの機能を用いて、被害口座から現金が不正に出金されるという新たな手口[*6] が６月に16件、７月に27件発生しており、合計約1,400万円の被害が確認されている。

---

*6　他の預貯金口座への送金がないため、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・被害額には含めていない。

○　金融資産売却に係る不正送金事案

証券会社で開設した証券口座に不正アクセスされて金融資産を売却され、不正に開設された銀行口座に送金された上で出金される新たな手口[*7]が７月から９月にかけて７件発生しており、合計約１億円の被害が確認されている。

(3)　不正プログラムの解析事例

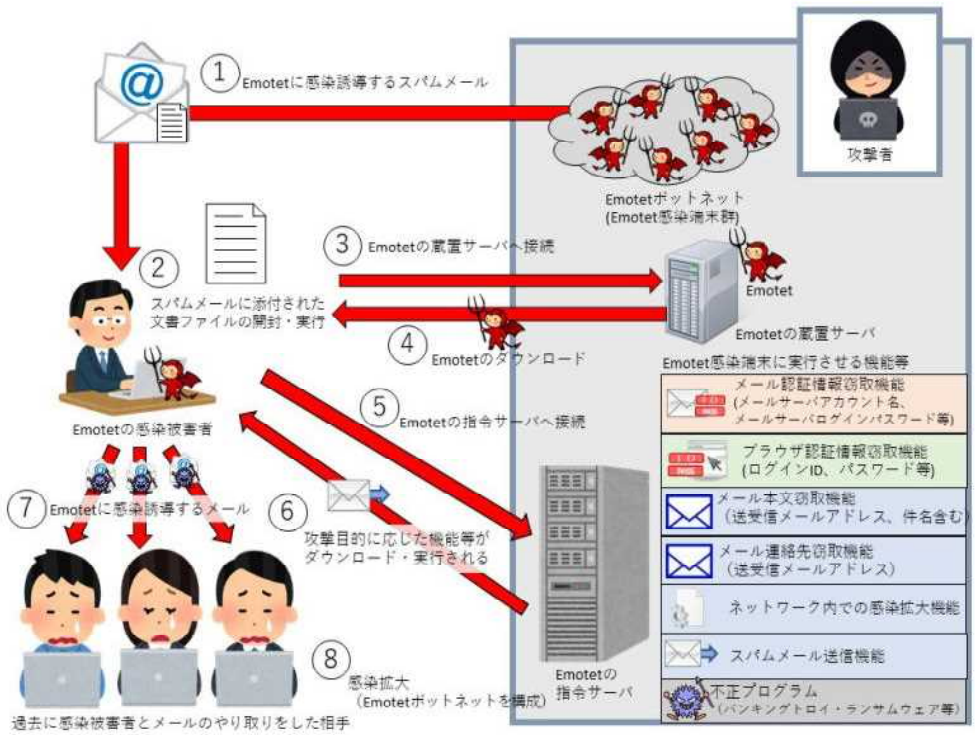
○　産業制御システムを標的としたプログラム

６月、工場の生産ライン等を制御するシステム（産業制御システム）を標的とするランサムウェアとみられるものについて、警察庁において、大規模産業型制御システム模擬装置を用いて解析を実施した結果、同不正プログラムは、攻撃対象と考えられる特定の企業の社内ネットワークのみで動作するように設計されているとみられることが確認された。

○　不正プログラムEmotet

メールの添付ファイルを主な感染経路とした不正プログラムであるEmotetについて、警察庁において検体を入手し、解析を実施した。その結果、Emotetは感染端末からメールアカウント、パスワード、メール本文等の情報を窃取し、これらの情報を悪用して、感染拡大を目的としたメールを送信する機能等を有していることを把握した。

【図表３：Emotetの動作概要】

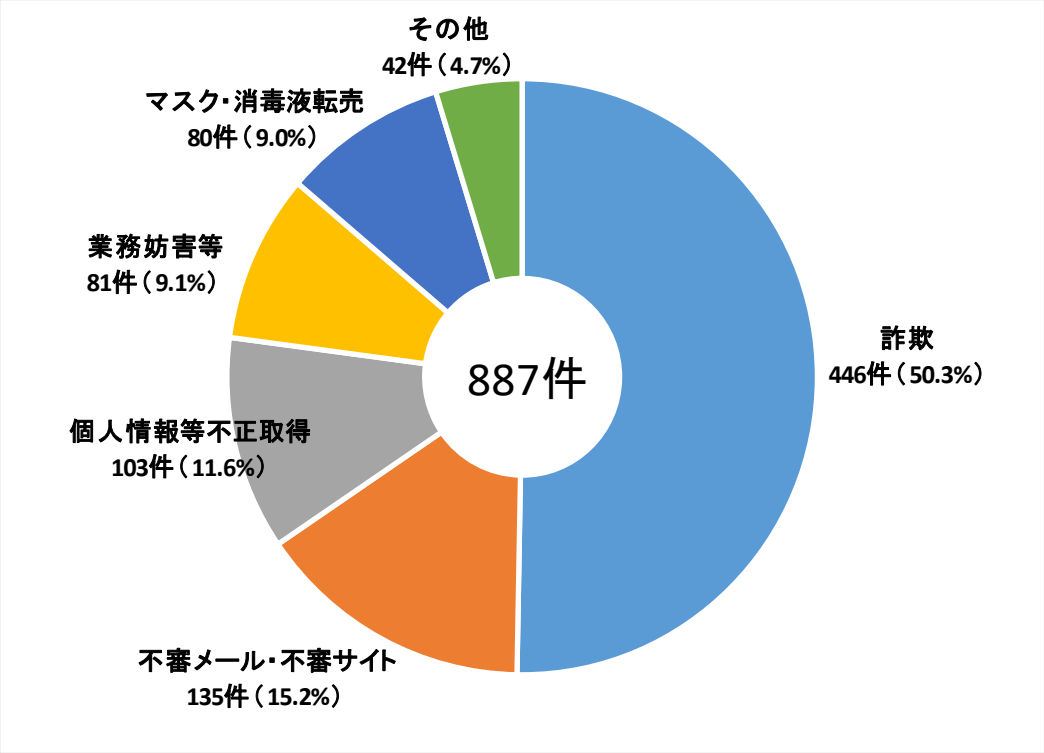


*7　証券口座における金融資産の売却のため、インターネットバンキングに係る不正送金事犯の発生件数・被害額には含めていない。

(4)　新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案

新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案として、令和２年中に都道府県警察から警察庁に報告のあった件数は887件であった。その内訳としては、詐欺が446件で全体の50.3％と最も多く、次いで不審メール・不審サイトが135件で全体の15.2％を占めている。

【図表４：新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案の報告件数】



○　報告事例

・　詐欺

インターネットのショッピングサイトでマスクを注文して、指定された口座にお金を振り込んだが、商品の発送日を過ぎても出品者から連絡がなく、商品も届かない。

・　不審メール・不審サイト

「お客様宛の個人給付金を預り中です。口座に送金するので、説明を希望する場合は、このメールに返信して下さい。」という内容のメールが届いた。

・　個人情報等不正取得

総務省を名乗り、「２回目の特別定額給付金を支給する。」という内容のメールが届いたので、指定されたＵＲＬにアクセスし、クレジットカード番号等を入力したところ、クレジットカード情報等が盗み取られた。

(5) 警察における取組

○　重要インフラ事業者等に対する注意喚起

重要インフラ事業者等に対してサイバー攻撃に関する注意喚起を行っており、令和２年においては、製薬事業者等に対する新型コロナウイルス感染症のワクチン開発に関連したサイバー攻撃に関する注意喚起のほか、重要インフラ事業者等に対するウェブ会議システムのぜい弱性に関する注意喚起、ＩＴインフラ管理ソフトウェアのぜい弱性に関する注意喚起等を行った。

○　共同対処訓練の実施

令和２年においても重要インフラ事業者、東京2020オリンピック・パラリンピック競技大会関連事業者等とのサイバー攻撃の発生を想定した共同対処訓練を実施した。具体的には、サイバー攻撃によるテレワーク用端末の不正プログラム感染、同大会を標的としたサイバー攻撃による停電発生等を想定した共同対処訓練を実施し、対処能力の強化を図った。

○　サイバー攻撃事案で使用されたＣ２サーバ[*8] のテイクダウン

サイバー攻撃事案で使用された不正プログラムの解析等を通じて把握した国内のＣ２サーバについて、サーバを管理する事業者等に働き掛け、不正な蔵置ファイルを削除するなどのＣ２サーバのテイクダウン（機能停止）を行うよう依頼するなどして、Ｃ２サーバの無害化措置を促進した。この結果、令和２年においては89台のＣ２サーバのテイクダウンを行った。

○　スマートフォン決済サービスに係る不正振替事犯の手口に関する注意喚起

事業者が提供するスマートフォン決済サービスに関して、同社と業務提携する金融機関に開設された口座情報を不正に入手・連携し、不正な振替（チャージ）を行う手口に関し、金融庁等と連携して注意喚起を実施した。

○　金融機関、送金先事業者に対する対策強化の働き掛けの実施

インターネットバンキングに係る不正送金被害等が集中している金融機関や送金先事業者に対して、モニタリングの強化、ワンタイムパスワード及び二経路認証の利用、本人確認の徹底等の対策状況の確認や対策強化の働き掛けを実施した。

○　情報セキュリティに係る視聴覚資料等による情報発信の実施

最近のサイバー空間の脅威を広く周知することによって被害防止等を図るため、フィッシング等の手口及びその対策方法を紹介した視聴覚資料や荷物の配送連絡を装ったＳＭＳから不審なウェブサイトに誘導された事例に関する情報等を警察庁ウェブサイトに掲載し、フィッシング等に係る具体的な事例や対策方法についての情報発信を実施した。

---

*8　Command and Control server（指令制御サーバ）の略。Ｃ＆Ｃサーバと省略する場合もある。制御の中心として、不正プログラムに感染した端末に指令を送り動作させるなどするサーバのこと。

○　ＪＣ３と連携したサポート詐欺サイト[*9] に関する注意喚起

山形県警察では、サポート詐欺サイトによる被害が発生していることを踏まえ、ＪＣ３と連携して広報啓発用の動画を作成し、同県警察及びＪＣ３のウェブサイトにおいてそれぞれ注意喚起を実施した。

○　ＪＣ３と連携したインターネットショッピングに係る詐欺サイト対策

愛知県警察と埼玉県警察がそれぞれＪＣ３と共同で開発したシステムの活用により、ＪＣ３が発見した詐欺サイトのＵＲＬ情報をＡＰＷＧ[*10] 等に提供し、被害防止対策を実施している。

○　偽の特別定額給付金の申請サイトに誘導するメールに関する注意喚起

総務省を装って特別定額給付金に関するメールを送信し、偽の特別定額給付金の申請サイトに誘導する手口について、ＪＣ３と連携し、ＪＣ３のウェブサイトにおいて注意喚起を実施した。

---

*9　パソコンの画面に偽のセキュリティ警告等を表示させるなどして利用者の不安をあおり、同警告等に記載された電話番号に電話をかけさせ、必要のないソフトを購入させたり、高額な偽のサポート契約をさせる手口をいう。

*10　Anti-Phishing Working Groupの略。フィッシングサイト対策を目的として平成15年に国際的な非営利団体として米国に設立

２　サイバー空間の脅威情勢

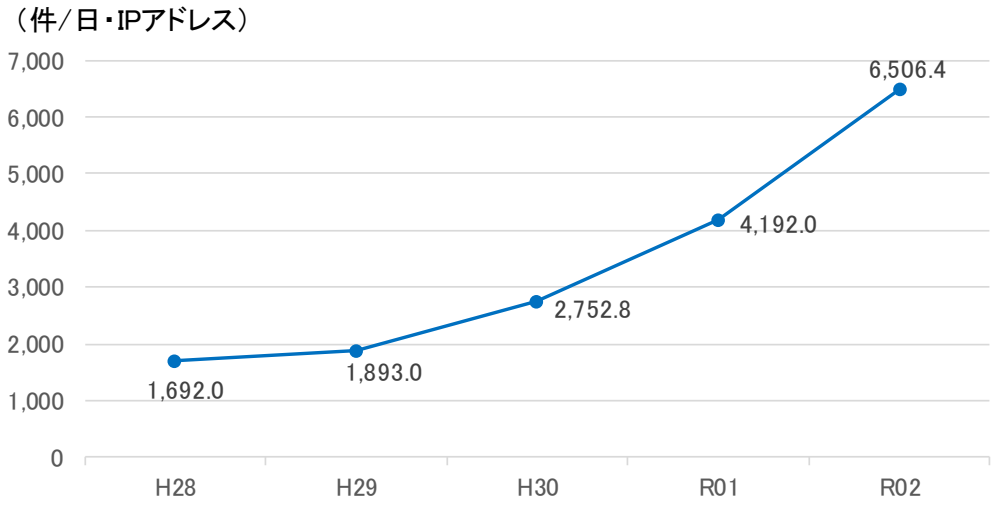
(1)　サイバー空間におけるぜい弱性探索行為等の観測状況

ア　センサーにおいて検知したアクセスの概況

警察庁は、インターネットとの接続点にセンサーを設置してリアルタイム検知ネットワークシステムを24時間体制で運用し、通常のインターネット利用では想定されない接続情報等を検知し、集約・分析している。本システムが検知するアクセスの大半は、不特定多数のＩＰアドレスを対象とするサイバー攻撃やネットワークに接続された機器のぜい弱性を探索するサイバー攻撃の準備行為とみられる。

令和２年に本システムにおいて検知したアクセス件数は、１日・１ＩＰアドレス当たり6,506.4件と増加傾向にある。アクセス件数が増加傾向にあるのは、ＩｏＴ機器の普及により攻撃対象が増加していること、攻撃側（踏み台として攻撃に利用されている機器・サーバを含む。）のシステムが年々強化されていることなどが背景にあるものとみられる。

【図表５：センサーにおいて検知したアクセス件数の推移】



イ　特徴的な観測

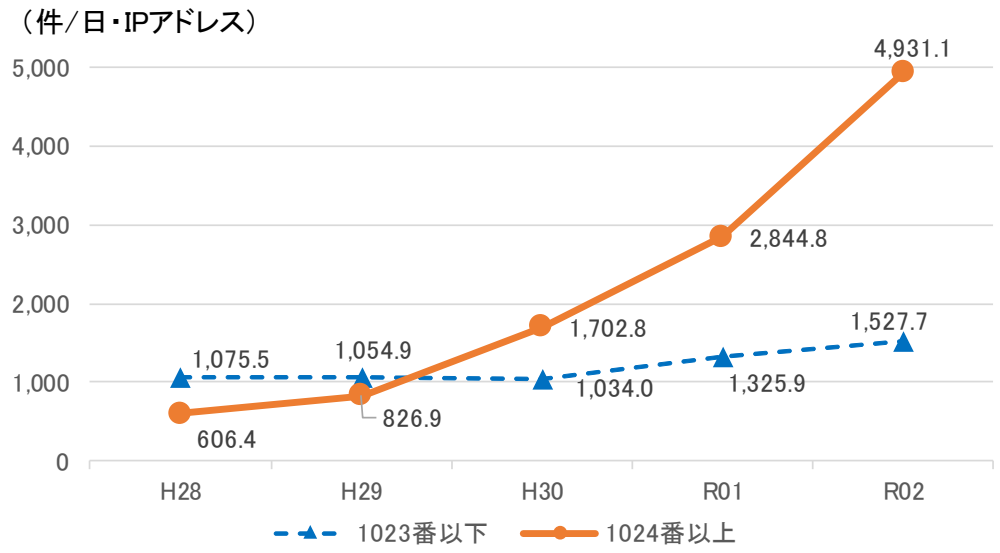
○　広範な宛先ポートへアクセスする送信元が増加

検知したアクセスの宛先ポート[*11]に着目すると、ポート番号1024以上のポートへのアクセス件数が増加し続けており、アクセス件数増加の大きな要因となっている。1024以上のポートは、主としてＩｏＴ機器が標準設定で使用するポート番号であることから、多くがＩｏＴ機器に対するサイバー攻撃やぜい弱性を有するＩｏＴ機器の探索行為であるとみられる。

---

*11　ＴＣＰ・ＵＤＰ/ＩＰ通信において、通信を行うコンピュータが、利用するサービスを識別するためのインターフェースのこと。０から65535までの番号が割り当てられている。

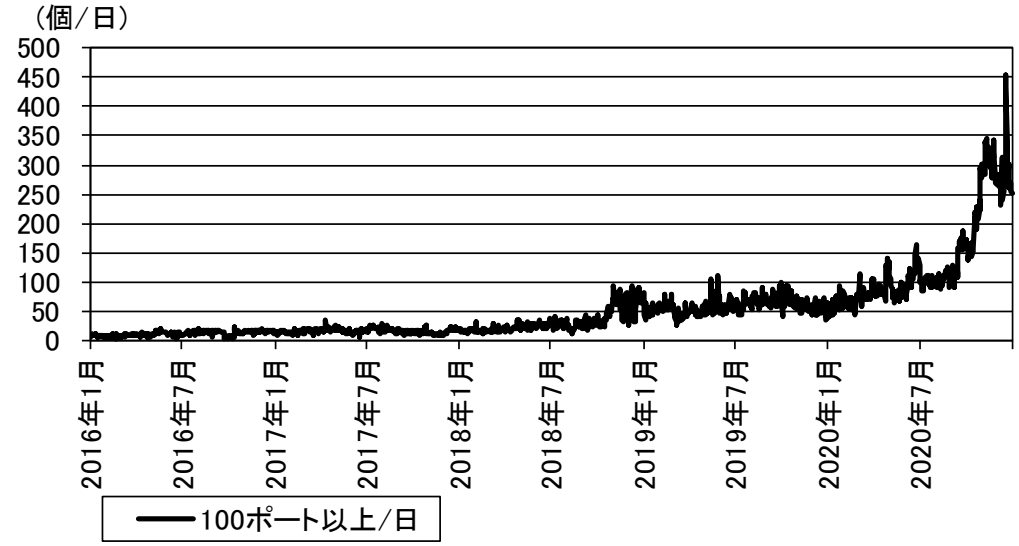
【図表６：検知したアクセスの宛先ポートで比較した１日・１ＩＰアドレス当たり件数の推移】



また、単一の送信元からの広範な宛先ポートに対するアクセスは、近年増加傾向にある。１日に100個以上の宛先ポートに対してアクセスを行った送信元ＩＰアドレス数の推移は、平成28年から30年上半期にかけて同水準で推移していたが、30年下半期から増加傾向となり、令和２年下半期に急増した。

また、令和２年における送信元ＩＰアドレス数は、１日当たり135.5個で、前年の59.1個と比較して、76.4個（129.3%）増加した。

【図表７：１日に100個以上の宛先ポートに対してアクセスした送信元ＩＰアドレス数の推移】

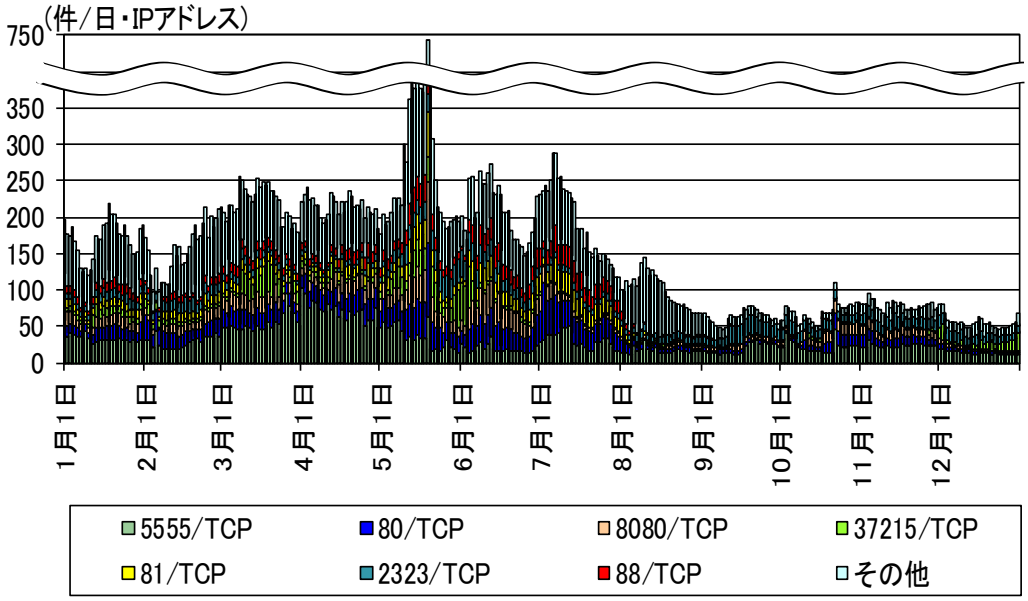


広範な宛先ポートに対するアクセスの増加の要因は、インターネットに接続されている機器やそれらが行っているサービス、さらに、そのぜい弱性の有無を網羅的かつ短期間に把握しようとする組織等が増加しているためと考えられる。

○　ＩｏＴ機器等のぜい弱性を狙ったアクセスの観測

令和２年のMiraiボットの特徴を有するアクセス件数は１日・１ＩＰアドレス当たり461.7件で、前年の522.9件と比較して、61.2件減少しているものの、Miraiが大流行した平成28年以降、一定数継続的に観測している。また、観測したアクセスを宛先ポート別に見ると、５月中旬から、宛先ポート37215/ＴＣＰに対するアクセスの増加を観測したが、これは、海外製ルータ等に使われる宛先ポートであり、遠隔から任意のコードが実行可能となるぜい弱性を悪用し、不正プログラムの感染拡大を狙ったものと考えられる。

【図表８：Miraiボットの特徴を有するアクセス件数の推移（23/ＴＣＰを除く宛先ポート別）】



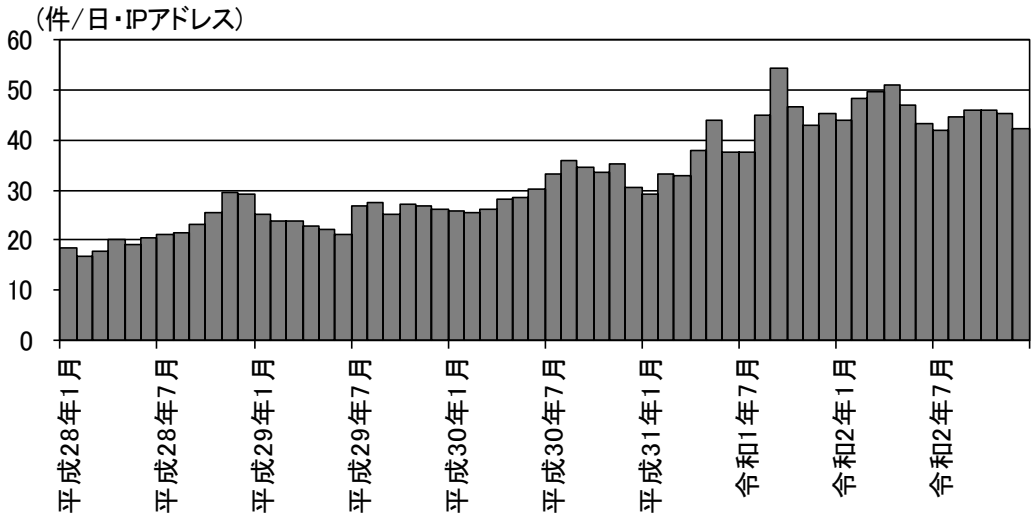
○　リモートデスクトップサービス[*12] を標的とした広範な宛先ポートに対するアクセスの観測

平成28年から令和２年にかけて、リモートデスクトップサービス（Microsoft Windowsの遠隔操作に利用）が標準で使用する3389/TCPに対するアクセスは緩やかな増加傾向にある。

また、２月中旬、リモートデスクトップサービスを標的とした広範な宛先ポートに対するアクセスの急増を観測した。これらアクセスは、リモートデスクトップサービスが標準で使用するポート以外に稼働していないかを探索する行為とみられる。

*12　職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータ等から閲覧・操作などできるサービスであり、テレワーク等で利用されている。

【図表９：リモートデスクトップサービスで使用される宛先ポート3389/TCPに対するアクセス件数の推移】



(2) 標的型メール攻撃

ア　標的型メール攻撃の特徴

令和２年にサイバーインテリジェンス情報共有ネットワーク*13 を通じて把握した標的型メール攻撃*14 の件数は4,119件であった。

これらには、

- 「ばらまき型」攻撃*15 の割合は全体の95％
- 送信先メールアドレスがインターネット上で公開されていないものが全体の75％
- 送信元メールアドレスが偽装されていると考えられるものが全体の97％

などの特徴があった。

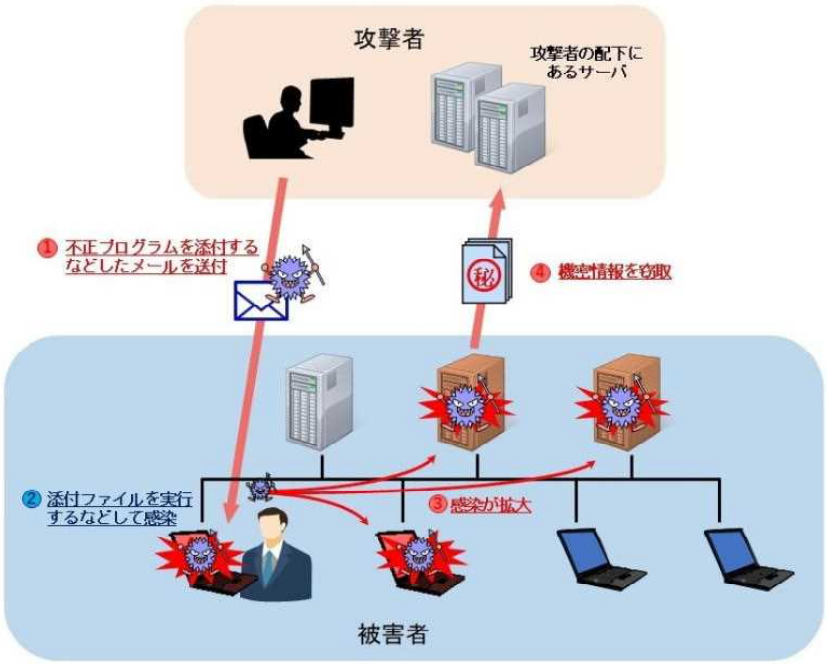
---

*13　警察と先端技術を有する全国約8,100の事業者等（令和３年１月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組み。内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携し、政府機関に対する標的型メール攻撃の分析結果についても情報を共有している。

*14　警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図るものを「標的型メール攻撃」として集計している。

*15　標的型メール攻撃のうち、同じ文面や不正プログラムが10か所以上に送付されていたものを「ばらまき型」として集計している。

【図表10：標的型メール攻撃による情報窃取の例】



イ　事例

サイバーインテリジェンス情報共有ネットワークを通じて得られた標的型メール攻撃には以下のようなものがあった。

○　見積依頼と称して、添付された圧縮ファイルを開くよう誘導するメールが、製造業者に対して送信された。

【図表11：標的型メールの事例】

差出人：[redacted]
送信日時：2020年11月16日月曜日 7:12
宛先：[redacted]
件名：見積依頼
添付ファイル：PO-0905.zip

こんにちは

いつもお世話になっております。
見積依頼させて頂きたくご連絡致しました。

図面添付致しますのでご確認お願い致します。
以上、宜しくお願い致します。

****
[redacted]
TEL: [redacted] FAX: [redacted]
MOBILE: [redacted]
E-Mail [redacted]
****

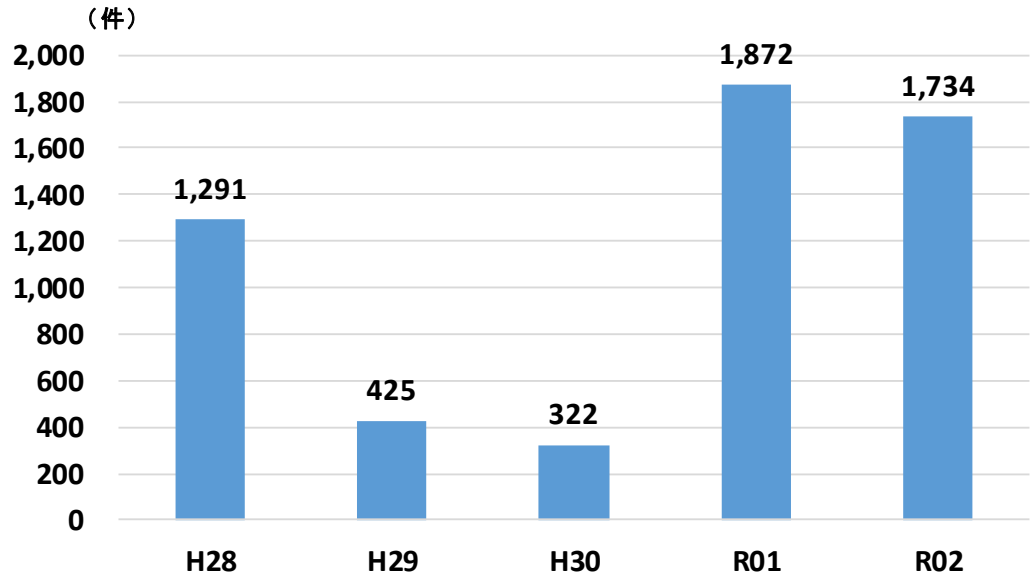
メール内の添付ファイルを開いたり、リンク先に接続したりすることにより、不正プログラムに感染する可能性がある。

(3) インターネットバンキングに係る不正送金事犯の発生状況等

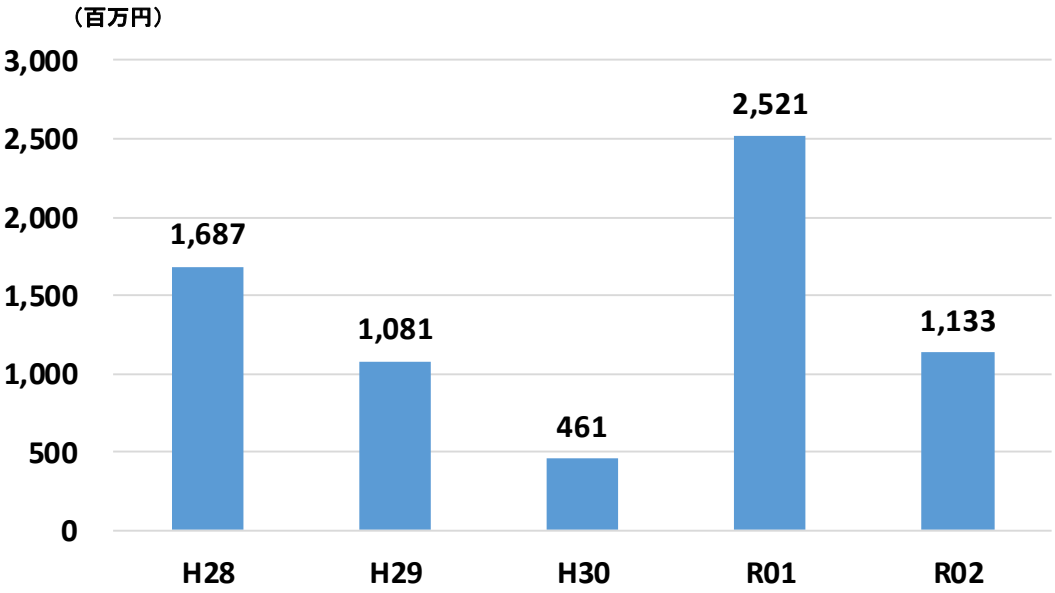
ア 概況

令和２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による被害は、発生件数1,734件、被害額約11億3,300万円で、前年と比べて発生件数、被害額ともに減少した。

【図表12：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の推移】



【図表13：インターネットバンキングに係る不正送金事犯の被害額の推移】



イ　特徴

・　令和２年は、被害が急増した前年と比べて、被害額は大幅に減少したものの、発生件数はやや減少と引き続き高水準で推移しており、被害の多くは、前年から継続しているＳＭＳや電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられる。

・　フィッシングサイトへの誘導には、金融機関を装ったＳＭＳ等のほか、宅配事業者や通信販売事業者からの荷物の配達連絡を装ったＳＭＳによって、金融機関を装ったフィッシングサイトへ誘導するものも確認されている。また、当該ＳＭＳからの誘導により、不正なアプリを携帯電話機等の端末にインストールさせ、当該アプリによって表示される偽の警告メッセージからフィッシングサイトへ誘導する手口も確認されている。

・　一次送金先として把握した2,181口座のうち、名義人の国籍は日本が37.8％と最も多く、次いでベトナムが17.9％、中国が2.4％であった。

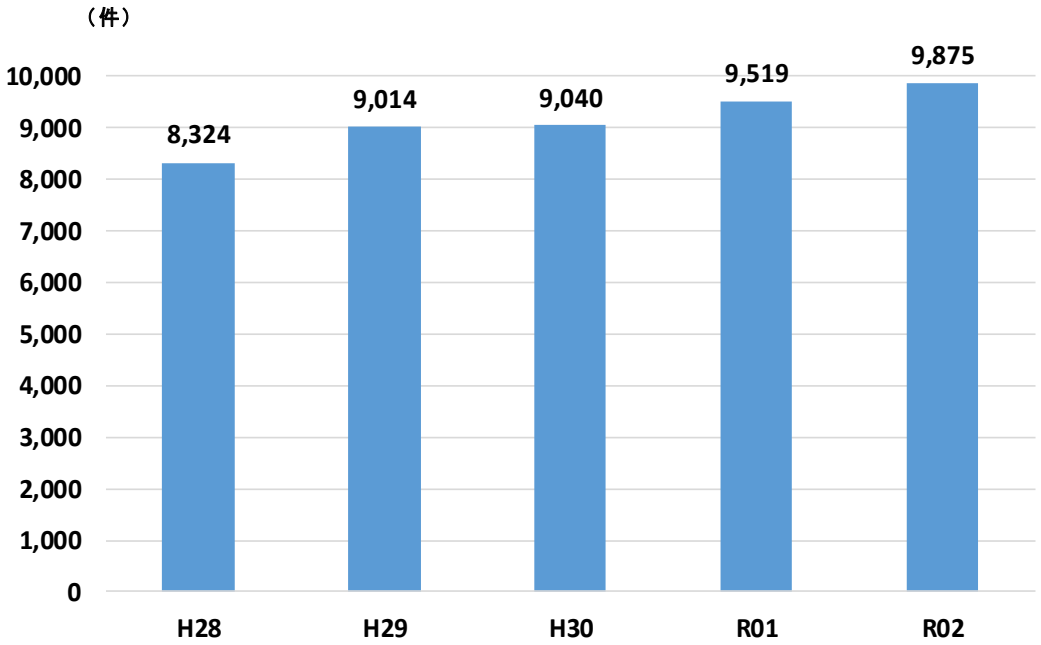
　従来の手口である預貯金口座への不正送金のほか、暗号資産や電子マネーの購入、プリペイドカードへのチャージ等の手口が確認されている。

(4)　サイバー犯罪の検挙状況

ア　サイバー犯罪の検挙件数

　サイバー犯罪の検挙件数は増加傾向にあり、令和２年における検挙件数は9,875件と、前年と比べて増加した。

【図表14：サイバー犯罪の検挙件数の推移】



イ　不正アクセス禁止法[*16] 違反

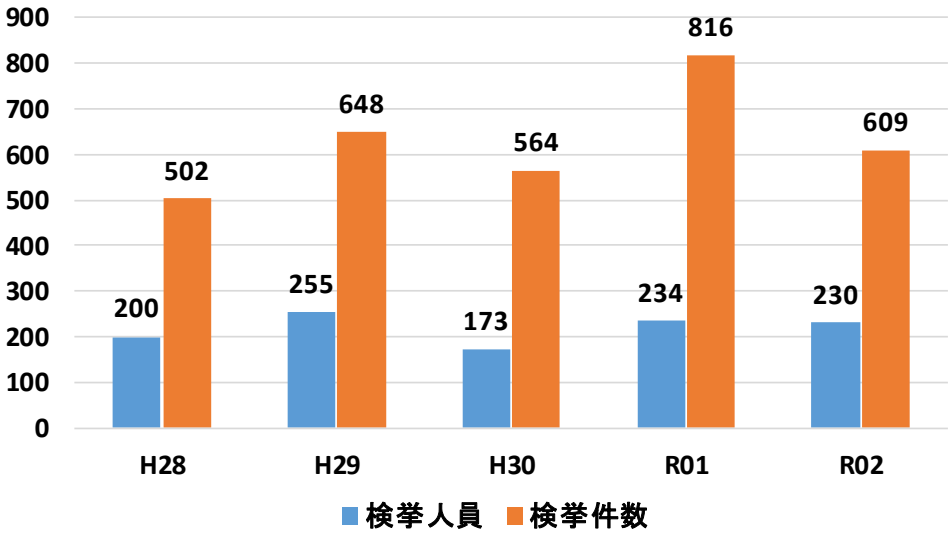
(ｱ)　検挙件数

令和２年における不正アクセス禁止法違反の検挙件数は609件と、前年と比べて減少した。

(ｲ)　特徴

○　検挙件数のうち、576件が識別符号窃用型[*17] で全体の94.6%を占めている。

【図表15：不正アクセス禁止法違反の検挙件数の推移】



○　「フィッシングサイトにより入手したもの」が最多

識別符号窃用型の不正アクセス行為に係る手口では、フィッシングサイトにより入手したものが172件と最も多く、全体の29.9%を占めており、次いで言葉巧みに利用権者から聞き出したもの又はのぞき見たものが115件で全体の20.0%を占めている。

○　被疑者が不正に利用したサービスは「社員・会員用等の専用サイト」が最多

識別符号窃用型の不正アクセス行為に係る被疑者が不正に利用したサービスは、社員・会員用等の専用サイトが174件と最も多く、全体の30.2%を占めており、次いでオンラインゲーム・コミュニティサイトが88件で全体の15.3%を占めている。

---

*16　不正アクセス行為の禁止等に関する法律（「不正アクセス行為・他人の識別符号を不正に取得する行為・不正アクセス行為を助長する行為・他人の識別符号を不正に保管する行為・識別符号の入力を不正に要求する行為」の５つの違反行為が定められている。）

*17　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

ウ　コンピュータ・電磁的記録対象犯罪[*18]

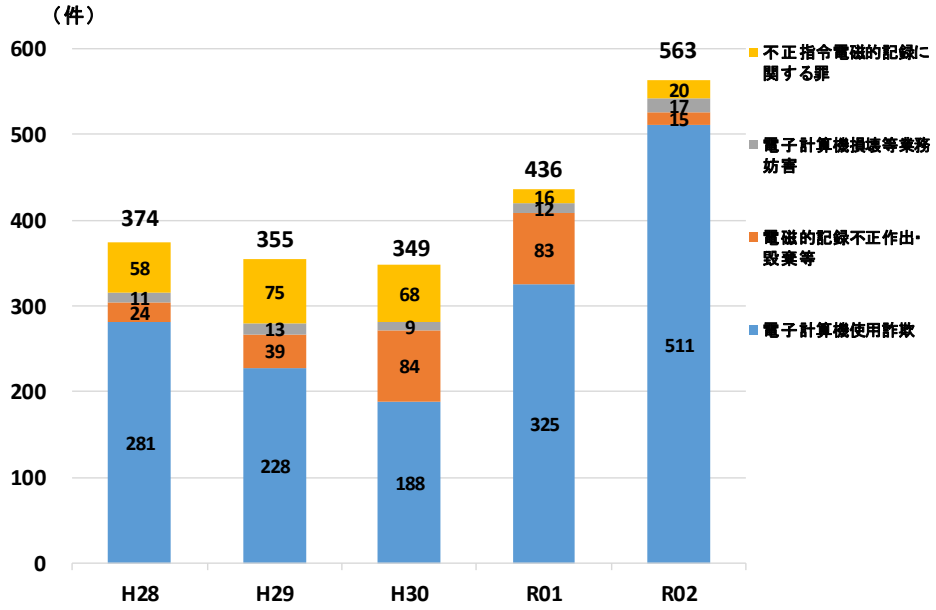
(ｱ)　検挙件数

令和２年におけるコンピュータ・電磁的記録対象犯罪の検挙件数は563件で、前年と比べて増加した。

(ｲ)　特徴

検挙件数のうち、電子計算機使用詐欺が511件と最も多く、全体の90.8%を占めている。

【図表16 ：コンピュータ・電磁的記録対象犯罪の検挙件数の推移】



エ　その他

○　児童買春・児童ポルノ法違反の検挙件数は2,015件と、前年と比べて減少した。

○　詐欺の検挙件数は1,297件と、前年と比べて増加した。

(5)　関係事業者等との連携

サイバーセキュリティ対策の現状について、民間事業者等において、

・　新型コロナウイルス感染症の感染拡大の影響で急きょテレワークを導入したため、貸与するルータを全員分準備できず、一部の社員は家庭用ルータを使用している。

・　実際にやり取りしているメールアドレスを使って送信されるなど、真偽を見分けるのがどんどん困難になっていると感じている。

・　海外支店のセキュリティレベルは、支店の規模によってばらつきがある。ばらつきをどのように解消するかは今後の課題である。

といった声も聞かれていることから、警察では、事業者や事業者団体等とサ

*18　刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪

イバーセキュリティに関連する協定の締結や協議会の設置を進めているほか、サイバーテロ対策協議会[*19] 等を通じて、情報提供や情報共有、注意喚起等を強化している。

○　新型コロナウイルス感染症指定医療機関等との連携強化

富山県警察では、新型コロナウイルス感染症指定医療機関を含む、県内24の公的病院が所属する富山県公的病院長協議会と、新型コロナウイルス感染症に関連するサイバー犯罪の被害防止対策及び通報体制の確立による被害拡大防止等に向けた協定を締結し、注意喚起の情報提供や被害防止に関する研修等を行っている。

○　産学官一体の協議会設立による多様な主体の連携強化

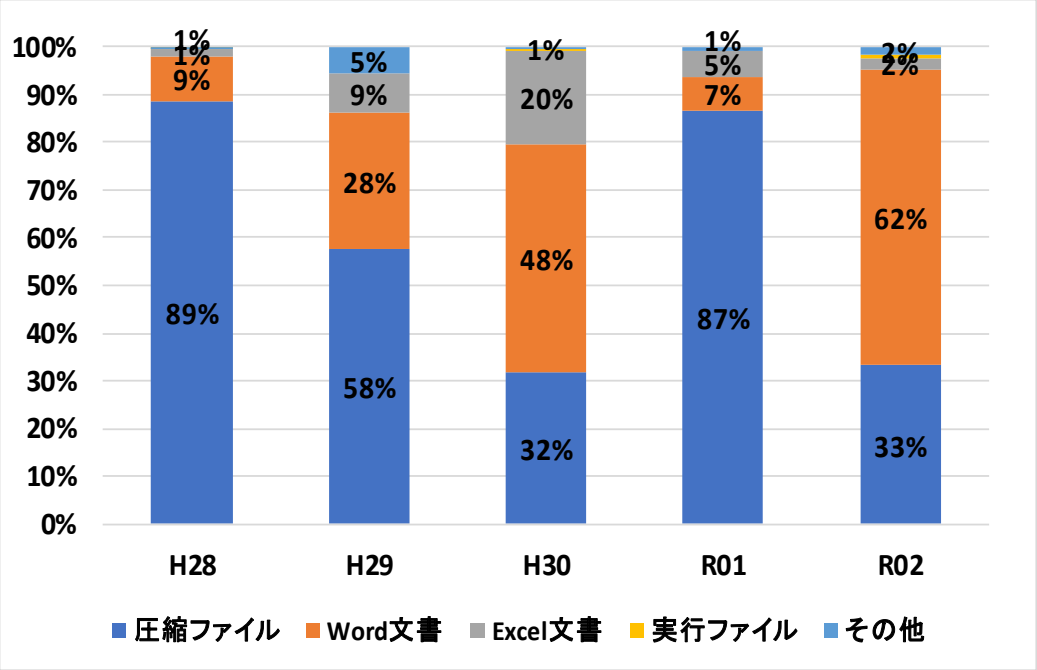
宮城県警察では、宮城県と一体となった取組を推進し、重要インフラ事業者、民間企業・団体、サイバー関連事業者、教育機関など合計118事業者からなるサイバーセキュリティ協議会を発足させ、情報共有や講演会の開催などを活性化させ、サイバーセキュリティに強い地域社会づくりを推進している。

*19　各都道府県警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等とで構成する協議会。サイバー攻撃等の情報提供、共同対処訓練等を行っている。

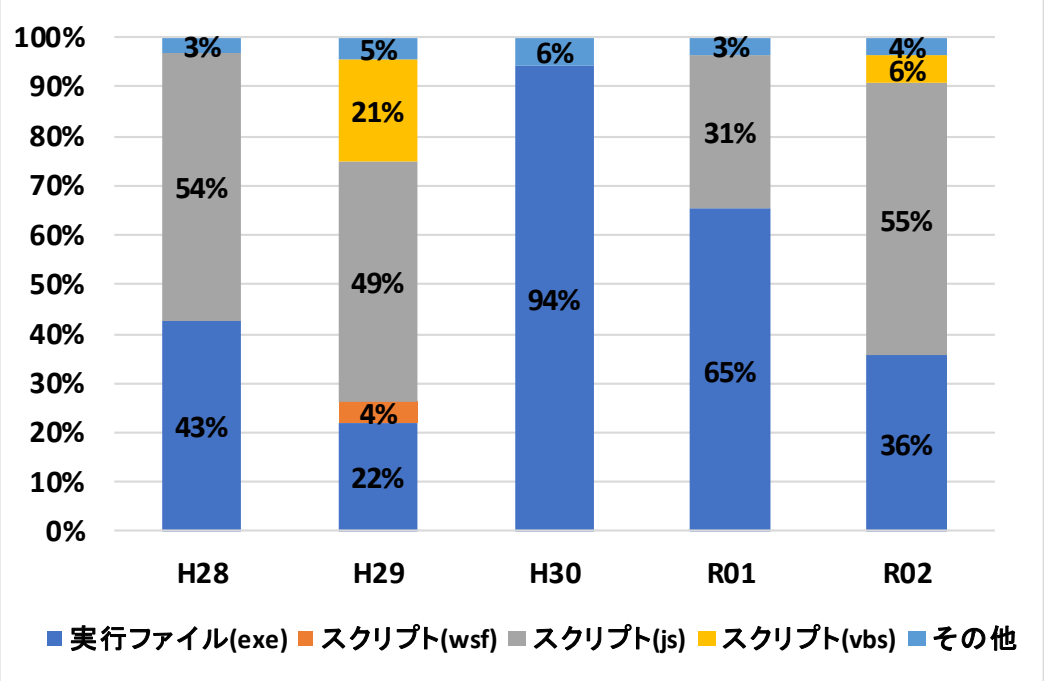
【　参考　】

1　標的型メールに添付されたファイル

(1)　標的型メールに添付されたファイル形式の割合の推移

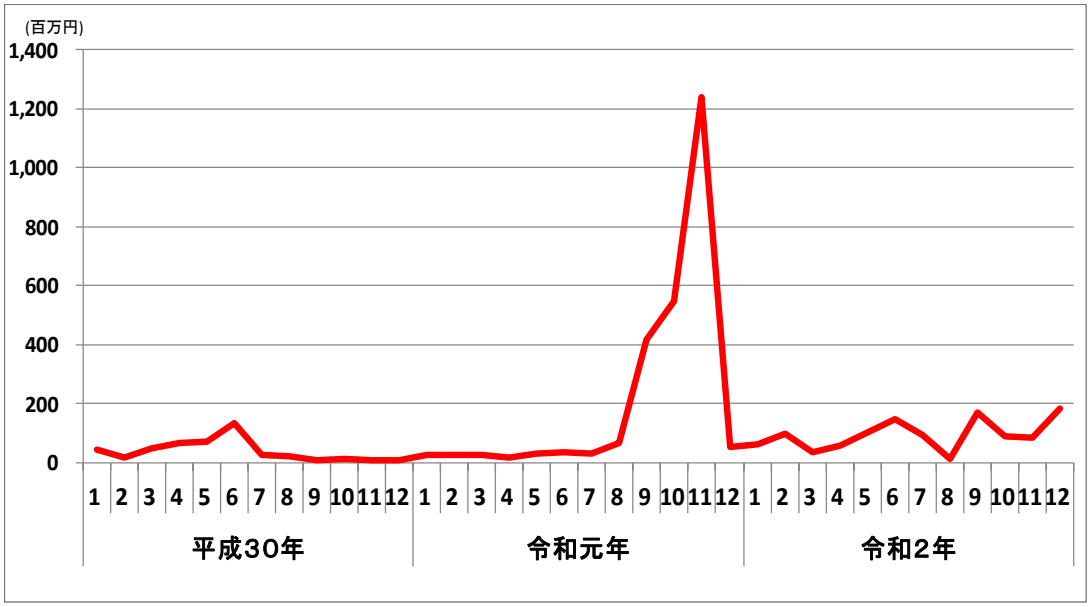


(2)　圧縮ファイルで送付されたファイル形式の割合の推移

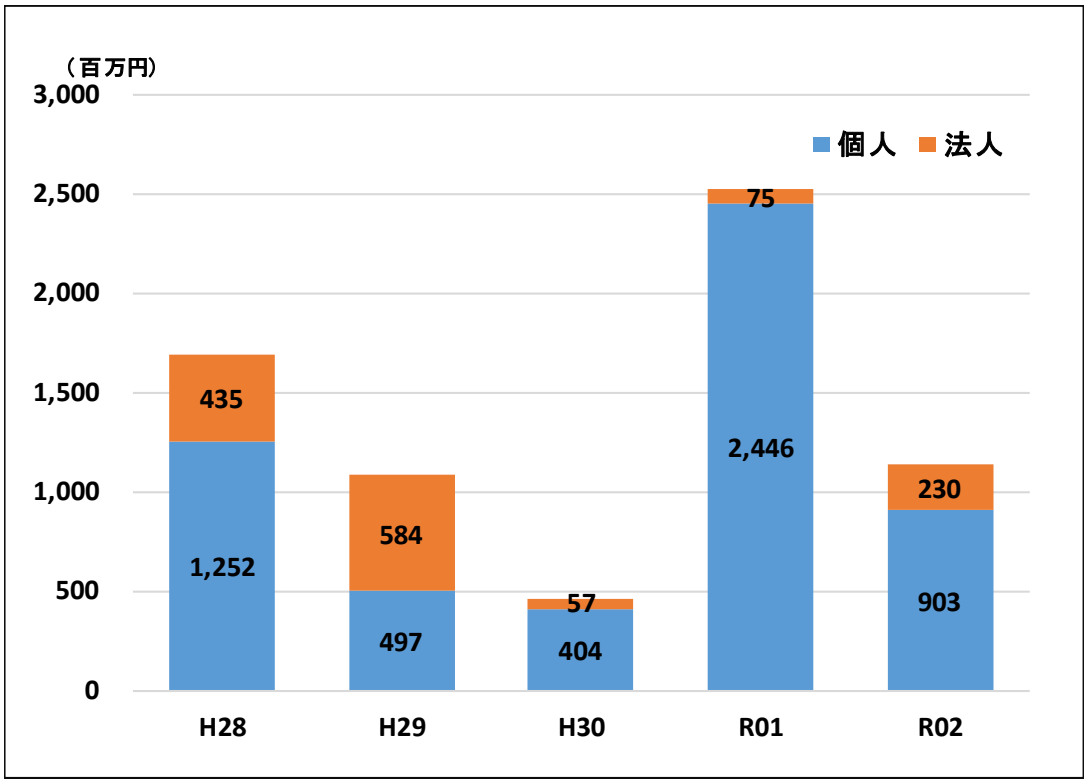


2　インターネットバンキングに係る不正送金事犯の発生状況等

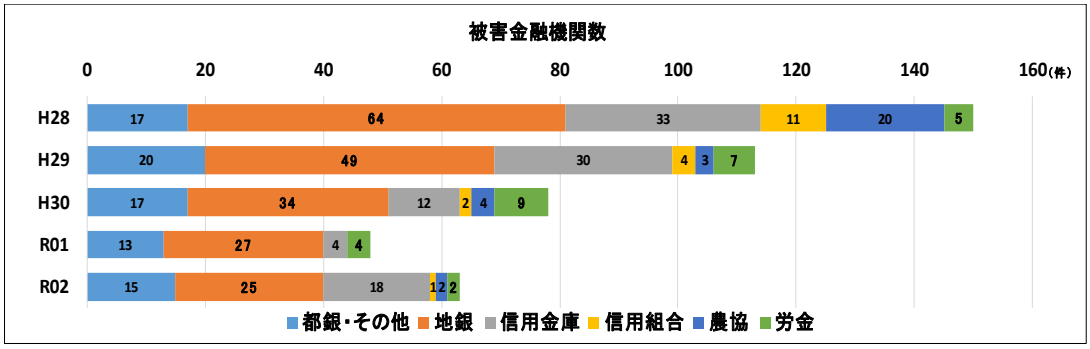
(1)　被害額の推移

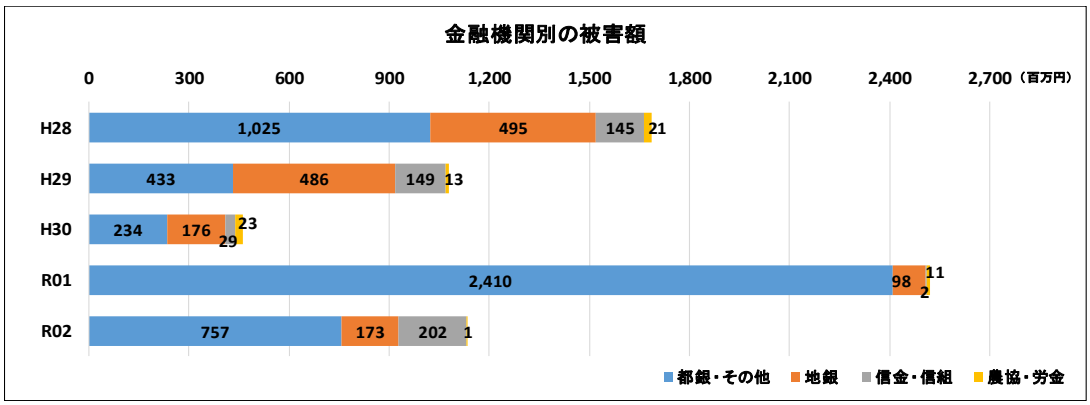


(2)　口座開設者別の被害状況

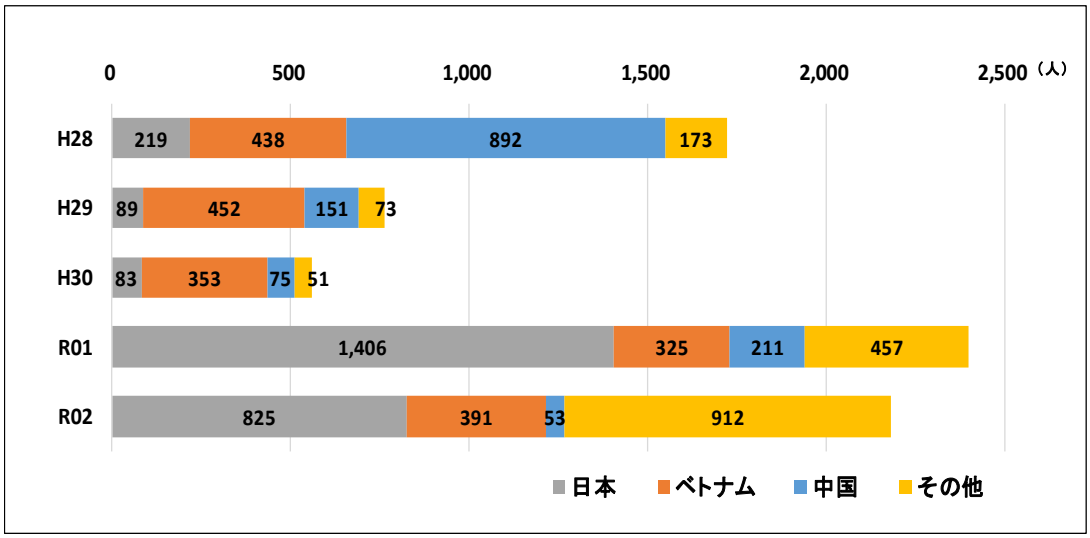


(3)　金融機関別の被害状況

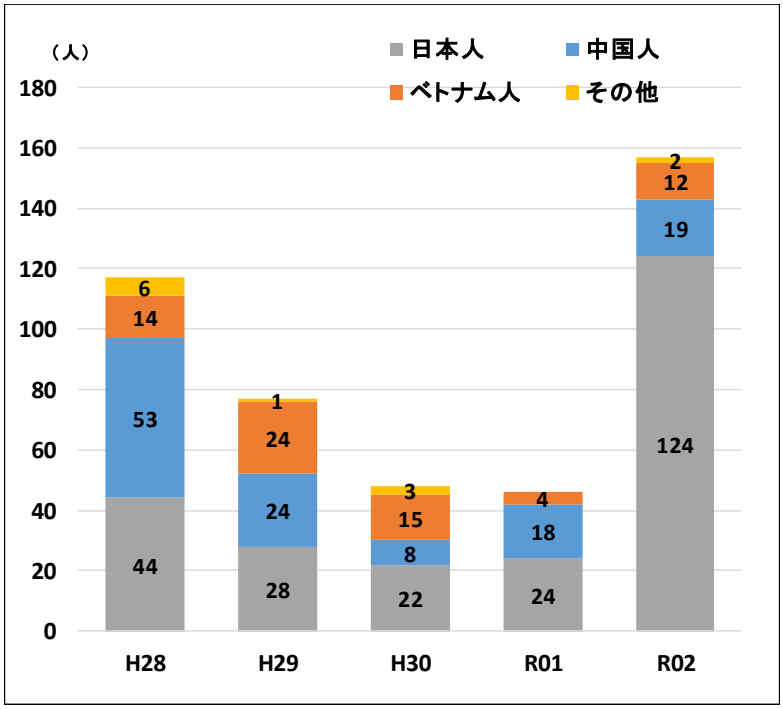




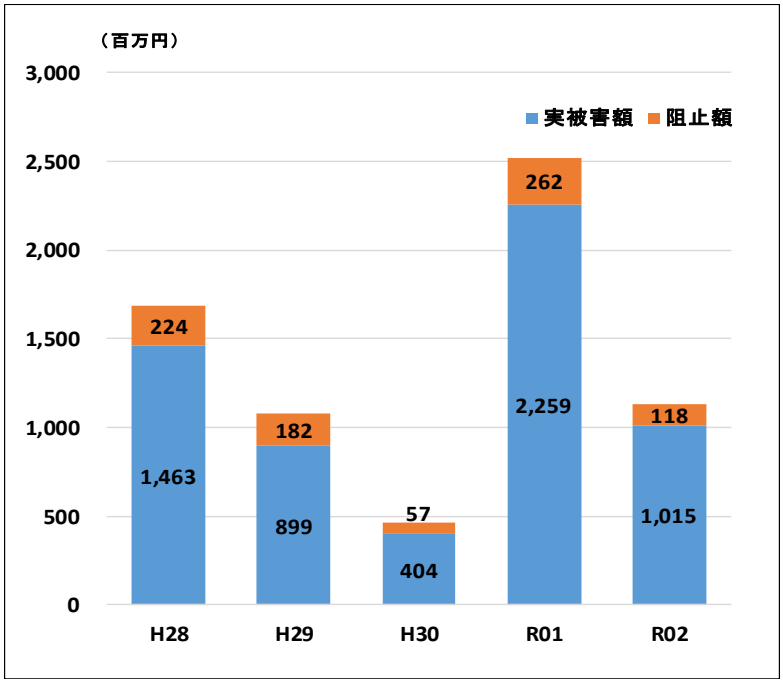
(4)　一次送金先口座名義人の国籍



(5)　国籍別の関連事件検挙状況



(6)　不正送金阻止状況

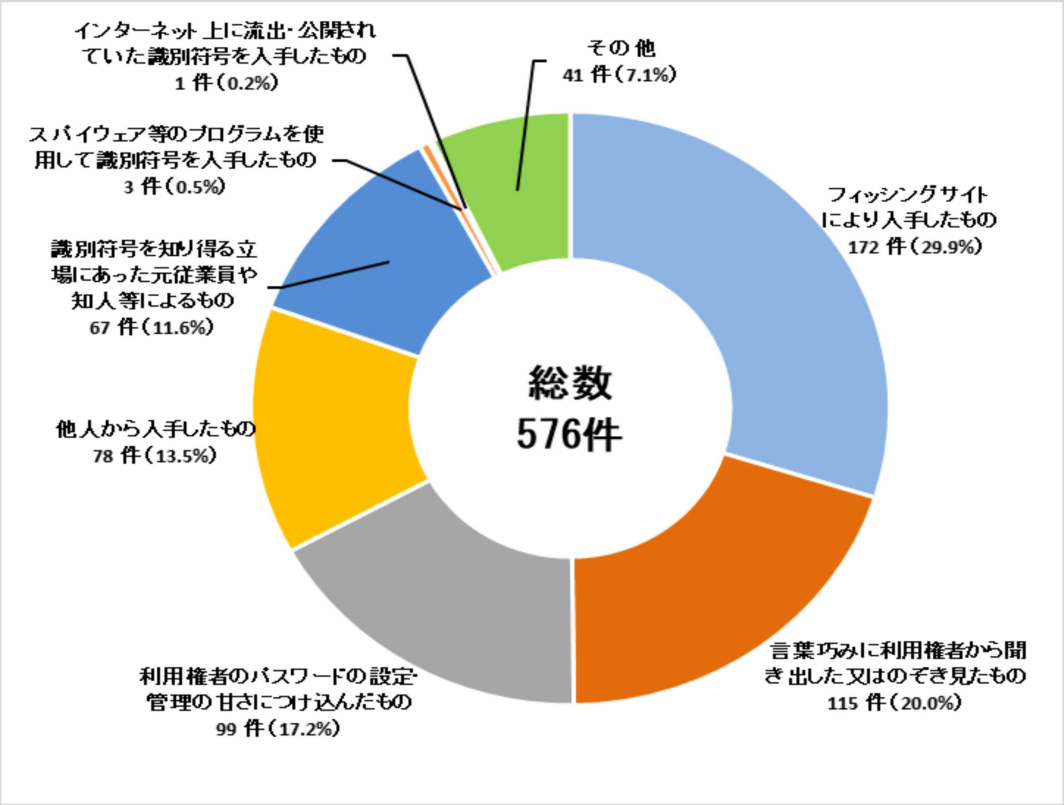


(7)　不正送金被害に係る口座名義人のセキュリティ対策実施状況

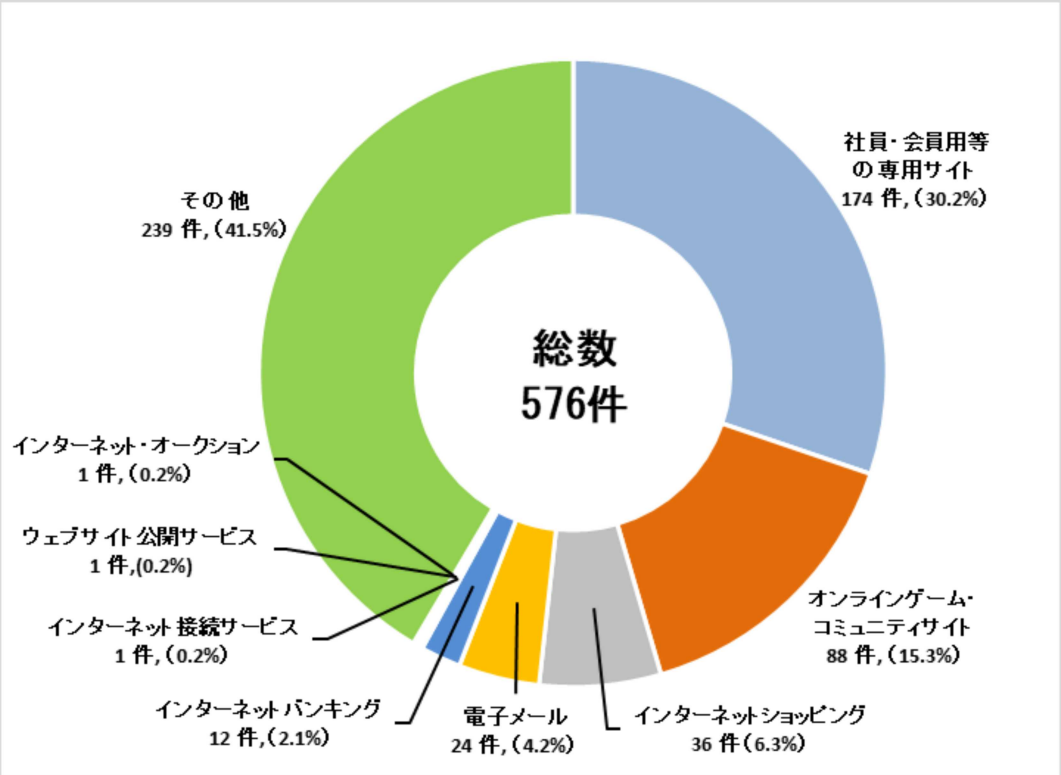
	利用していた		利用していない		不　明		合　計
ワンタイムパスワード（個人口座）	767	45.9%	587	35.1%	316	18.9%	1,670
電子証明書（法人口座）	5	7.8%	51	79.7%	8	12.5%	64

３　不正アクセス禁止法違反の検挙状況

(1)　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



(2)　不正に利用されたサービス別検挙件数（識別符号窃用型）



不正アクセス禁止法違反

○　会社員の男（21）は、令和２年１月、不正に取得したＩＤ・パスワードを使用して電気通信事業者が提供するポイントサイトに不正アクセスし、電子書籍等を不正に注文し詐取した。同年８月、男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺で検挙した。（三重）

○　無職の男（46）は、令和２年４月、元同僚のＩＤ・パスワードを使用して元勤務先のメールサーバに不正アクセスし、同社社内のメールを盗み見た上、同メールを取引先の企業に転送し漏洩させた。同年７月、男を不正アクセス禁止法違反（不正アクセス行為）で検挙した。（栃木）

４　コンピュータ・電磁的記録対象犯罪の検挙状況

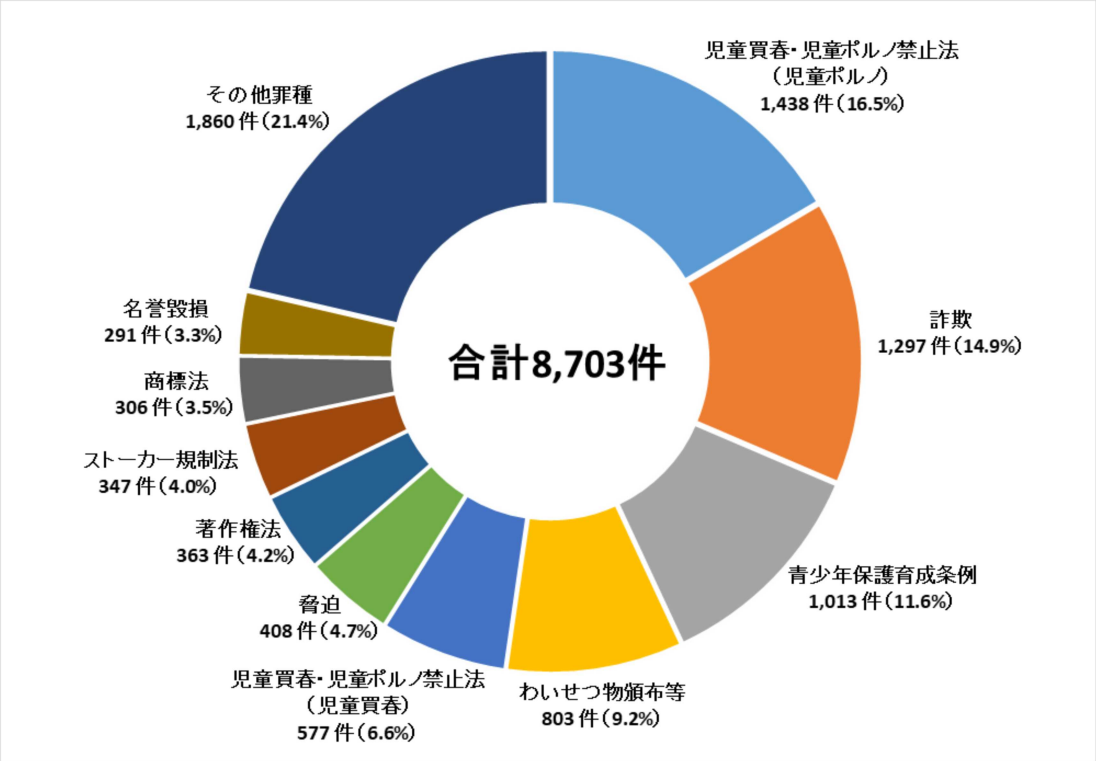
	H28	H29	H30	R01	R02
電子計算機使用詐欺	281	228	188	325	511
電磁的記録不正作出・毀棄等	24	39	84	83	15
電子計算機損壊等業務妨害	11	13	9	12	17
不正指令電磁的記録供用	36	24	37	6	9
不正指令電磁的記録取得・保管	18	22	19	6	8
不正指令電磁的記録作成・提供	4	29	12	4	3

コンピュータ・電磁的記録対象犯罪

○　無職の男(35)は、令和２年３月、当時勤務していた職場の同僚女性らのメールを盗み見る目的で、同人らの使用する社内パソコンに、キー入力情報等を秘密裏に記録するプログラムを仕掛けた上、同人らが使用するアカウントのＩＤ・パスワードを盗み取り、社内ネットワークに不正アクセスした。同年７月、男を不正指令電磁的記録供用及び不正アクセス禁止法違反（不正アクセス行為）で検挙した。（福井）

○　韓国籍の男（20歳代）は、平成29年４月、在日本朝鮮人総聯合会（朝鮮総聯）が運営するウェブサイトを改ざんし、当該ウェブサイトを閲覧した者の端末を不正プログラムに感染させようとした。令和２年12月、男を不正指令電磁的記録供用未遂で検挙した。（警視庁）

５　その他の検挙状況



詐欺

○　無職の男（44）は、令和２年３月から同年９月までの間、偽造された運転免許証を利用して、金融機関がインターネット上で配信しているアプリケーションソフトの口座開設欄に虚偽の情報を入力するなどして口座開設及びキャッシュカードの交付を申し込み、同金融機関の職員にキャッシュカードの発行及び郵送手続きを取らせて詐取した。同年12月、男を詐欺で検挙した。（兵庫）

著作権法違反

○　会社役員の男（39）らは、令和元年12月、著作権者の許可を受けないで、著作物であるアニメキャラクターを使用したスマートフォン用のゲームアプリをインターネット上で公衆送信し得る状態にして、著作権を侵害した。令和２年９月、男らを著作権法違反で検挙した。（佐賀）