広　報　資　料
令和２年10月１日
警　　察　　庁

令和２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

１　サイバー空間の脅威情勢

新型コロナウイルス感染症の発生に乗じたものを含め、サイバー攻撃やサイバー犯罪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、引き続き深刻な情勢。

２　新型コロナウイルス感染症に関連した情勢等

(1)　サイバー攻撃・サイバー犯罪の情勢

○　新型コロナウイルス感染症に関連したサイバー攻撃として、国内外で医療機関や研究機関等に対する攻撃を確認。

○　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、詐欺や不審メール等608件を都道府県警察からの報告により把握。

(2)　警察における取組

○　国外において新型コロナウイルス感染症に関連する研究機関がサイバー攻撃の被害に遭っている状況を踏まえ、国内の製薬事業者等に対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た不審メールや悪質なショッピングサイトについて、ウェブサイト等で注意喚起を実施。

３　その他の脅威情勢等

(1)　サイバー攻撃・サイバー犯罪の情勢

○　国内外において、政府や企業等に対するサイバー攻撃が発生。

○　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下半期と比べて減少しているものの、前年同期と比べて大幅に増加。

○　警察によるサイバー犯罪の検挙件数は、年間の検挙件数が最多となった前年同期と同水準。

(2)　警察における取組

○　重要インフラ事業者等とサイバー攻撃の発生を想定した訓練を実施したほか、サイバー攻撃事案で使用されたＣ２サーバの機能停止を実施。

○　日本サイバー犯罪対策センター（ＪＣ３）等と連携し、リスト型攻撃に対する被害防止対策、インターネットショッピングに係る詐欺サイト対策等を推進。

別　添

令和２年上半期におけるサイバー空間をめぐる脅威の情勢等

令和２年上半期は、新型コロナウイルス感染症の感染拡大を受け、ＷＨＯが「国際的に懸念される公衆衛生上の緊急事態（ＰＨＥＩＣ[*1]）」を１月31日（日本時間）に宣言し、我が国においても、４月７日には７都府県[*2]を対象区域として「緊急事態宣言」が発出され、４月16日には対象区域が全国に拡大されるなどの状況にあり、５月25日に「緊急事態解除宣言」が発出された今もなお、「新しい生活様式」を踏まえながら新型コロナウイルス感染症対策を継続しているところである。

このような中、新型コロナウイルス感染症の発生に乗じたものを含め、サイバー攻撃やサイバー犯罪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、引き続き深刻な情勢が続いている。

令和２年上半期のサイバー攻撃については、国外では、豪州の首相等が、豪州の組織が国家的な主体によるサイバー攻撃の標的になっていると発表、国内では、我が国の複数の防衛関連企業、大手電気通信事業者が不正アクセスを受け、情報が流出した可能性があることが公表された。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も増加傾向が続いている。

また、警察によるサイバー犯罪の検挙件数は、年間の検挙件数が最多となった前年の同期と同水準となった。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、被害が急増した前年下半期と比べて減少しているものの、前年同期と比べて大幅に増加しており、その被害の多くは、ＳＭＳや電子メールを用いて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。

こうしたサイバー空間の脅威に対し、警察では、組織の総合力を発揮した効果的な対策を推進している。新型コロナウイルス感染症に乗じた犯罪の手口については、日本サイバー犯罪対策センター（ＪＣ３）と連携してウェブサイト等での注意喚起を実施したほか、利用者が急増しているウェブ会議システムのぜい弱性を狙うサイバー攻撃について、重要インフラ事業者等に注意喚起を行うなどした。また、引き続き2020年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）の開催に向け、東京大会を標的としたサイバー攻撃に関する脅威情報の収集・分析を行うとともに、東京大会の運営に関連する事業者等との情報共有、共同対処訓練を実施するなどの取組を推進している。

---

*1　Public Health Emergency of International Concernの略

*2　埼玉、千葉、東京、神奈川、大阪、兵庫及び福岡

1　新型コロナウイルス感染症に関連した情勢

(1)　情勢概況

新型コロナウイルス感染症に関連した特徴的なサイバー攻撃として、国内外で医療機関や研究機関等に対する攻撃が確認されている。これらの攻撃における攻撃者の意図は必ずしも明らかではないが、医療機関・研究機関の研究状況の把握や、研究成果の窃取を目的としているなどの可能性が想定される。新型コロナウイルス感染症の拡大やこれに乗じた関連事案による社会への影響は極めて大きく、攻撃者が攻撃対象として新型コロナウイルス感染症に関連した機関や事業者を狙う傾向は今後も継続する可能性がある。

また、標的型メール攻撃[*3]は、我が国でも多数発生し、しばしば情報窃取やサーバ乗っ取りなどの更なるサイバー攻撃等の端緒となっている。最近は、受信者の不安感に乗じた新型コロナウイルス感染症に関連しただまし文句を用いる例が報告されている。一般に、標的型メール攻撃では、攻撃者がその時勢に応じメールの受信者がより開封しやすい文面を用いようとする傾向にあり、新型コロナウイルス感染症に関連した標的型メールもこのような傾向の一環であるとみられる。標的型メール攻撃のような人間の心理的な隙をつく攻撃手法は、攻撃を完全に防ぐことは難しく、各セキュリティ事業者が公表する最新の攻撃動向（傾向や手口）の把握、職員のサイバーセキュリティ意識の向上等の地道な対策が引き続き求められる。

さらに、感染症対策に関連したテレワークの増加等の業務環境の変化に伴い、サーバへの遠隔接続サービス、ＶＰＮサービス、オンライン会議システムのぜい弱性が明らかになっており、同ぜい弱性を悪用したとみられる事例も確認されている。一部の事業者においては、在宅勤務を実施するのに十分なセキュリティ上の措置が講じられていないシステムや端末が用いられる、システム監視の体制がぜい弱となりサイバー攻撃の被害への対応が遅れるなどの状況が生じているものとみられる。他方、リアルタイム検知ネットワークシステム[*4]における観測においては、オンライン会議システム等の特定のサービスに関連した探索行為の著しい増加といった顕著な情勢の変化は現時点で確認されていない。

また、新型コロナウイルス感染症に関連した特徴的なサイバー犯罪として

---

*3　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。

*4　インターネットとの接続点に設置したセンサーにおいて検知したアクセス情報等を集約・分析することで、ＤｏＳ攻撃の発生や不正プログラムに感染したコンピューターの動向等の把握を可能とするシステムであり、警察庁が24時間体制で運用している。

は、サイバー空間を利用した詐欺や業務妨害事案において、マスクや消毒液の販売に関連した詐欺、新型コロナウイルス感染症への感染に関連した虚偽情報の流布等の事案が見られた。

(2) 新型コロナウイルス感染症に関連したサイバー攻撃の事例

ア　国外における事例

○　チェコ共和国の医療機関に対するサイバー攻撃

４月、チェコ共和国のサイバー情報セキュリティ庁は、同国内の医療機関等の情報通信システムに対する大規模なサイバー攻撃に対する警告を発表した。同国内での新型コロナウイルス感染症の発生状況等に関連して、非常に危険なサイバー攻撃の増加を認知したとしている。

これを受け、米国国務省は、新型コロナウイルス感染症対策を弱体化させるサイバー攻撃を断じて容認しないとし、各国に対して、自国を送信元としてそうした活動を行っている犯罪組織等を注視するよう求めた。

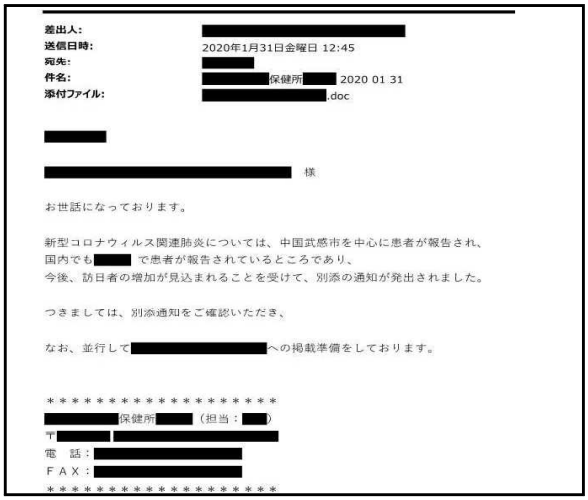
○　米国の研究機関を標的とした攻撃

５月、米国連邦捜査局（ＦＢＩ）は、中国と関連のあるサイバー攻撃集団等による、米国の新型コロナウイルス感染症に関連した研究機関を標的とした攻撃について捜査していると発表した。攻撃者は、新型コロナウイルス感染症に関連する研究に係るネットワーク等から、知的財産及びワクチン、治療法等に関連する情報の不正取得を試みていたとしている。これを受け、米国国務省は、かかる試みを非難すると発表し、中国に対して、悪意ある活動を中止するよう求めた。

イ　国内における事例

警察では、実在する保健所をかたり、新型コロナウイルス感染症に関する通知が発出されたと称して、添付ファイルを開くよう誘導するメールが送信されるなどといった、新型コロナウイルス感染症に関連したサイバー空間上の不正な活動を把握している。

【図表１：保健所をかたるメールの事例】


差出人：
送信日時：2020年1月31日金曜日 12:45
宛先：
件名：　保健所　2020 01 31
添付ファイル：　.doc

様

お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告され、
国内でも　で患者が報告されているところであり、
今後、訪日者の増加が見込まれることを受けて、別添の通知が発出されました。

つきましては、別添通知をご確認いただき、

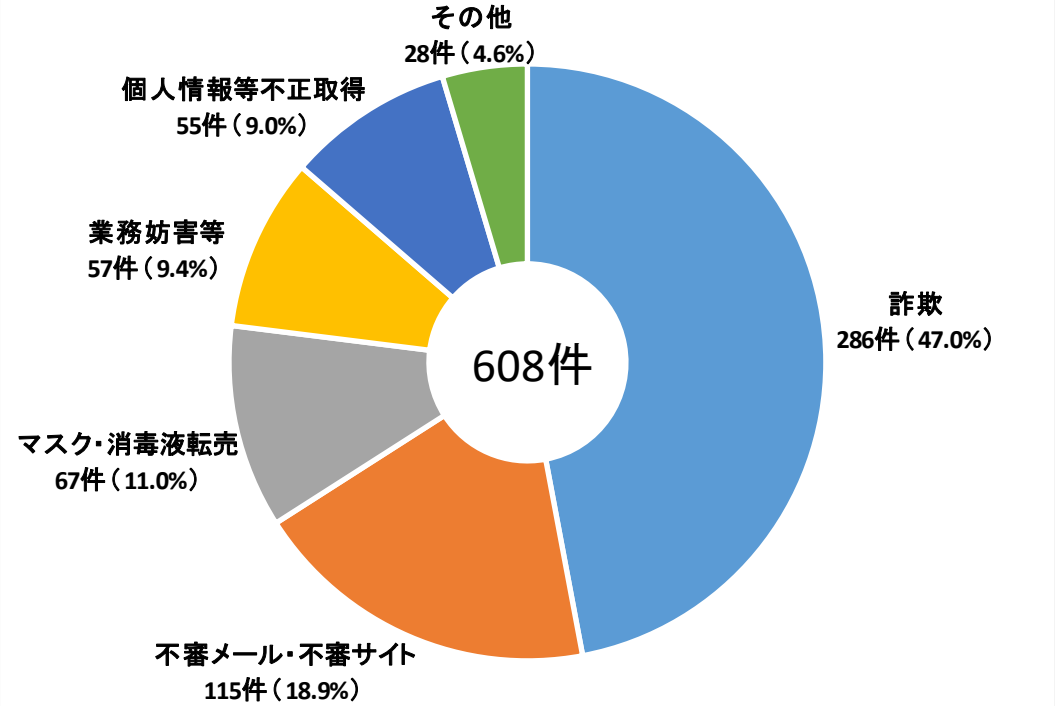
なお、並行して　への掲載準備をしております。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
　保健所　（担当：　）
〒
電　話：
ＦＡＸ：
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

(3)　サイバー犯罪が疑われる事案の発生状況

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、６月末までに都道府県警察から警察庁に報告のあった件数は608件であった。その内訳としては、詐欺が286件で全体の約47.0％と最も多く、次いで不審メール・不審サイトが115件で全体の約18.9％を占めている。

【図表２：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】



○　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が届かず、出品者とも連絡がとれない。

・　国外の取引会社に商品を発注したところ、同社社員を名乗る者から「新型コロナウイルス感染症の影響のため、いつもの銀行が利用できないので、別の口座に代金を振り込んで欲しい。」とメールで依頼があり、指定された口座に送金した。後日、取引先から支払いを求める正規のメールがあり、だまされたことに気が付いた。

○　不審メール・不審サイト

・　携帯電話事業者を名乗る者から、「政府の要請を受けて給付金を送るので記載されたＵＲＬから申請するように」という内容のメールが届いた。

○　個人情報等不正取得

・　マスクを購入するために入力したクレジットカード情報等が盗み取られた。

(4)　サイバー犯罪の検挙事例

○　業務妨害

特定の飲食店に新型コロナウイルス感染症の感染者がいるとの虚偽の事実をネット上に投稿し、業務を妨害したもの。

○　国民生活安定緊急措置法違反

ネットで購入者を募り、購入価格を大幅に超える価格でマスクを転売したもの。

○　医薬品医療機器等法違反

自社サイト上で、新型コロナウイルス感染症への効能効果をうたい、未承認医薬品の広告をしたもの。

(5)　その他の取組

○　製薬事業者等に対する注意喚起

国外において新型コロナウイルス感染症に関連する研究機関がサイバー攻撃の被害に遭っている状況を踏まえ、警察では、４月以降、国内の製薬事業者等に対して、

・　新型コロナウイルス感染症に関連したメールに注意し、安易に添付ファイルを開いたり、メール本文内のリンク先に接続したりしない。

・　不要なサービスを停止する、不要なポートを閉じるなど、保有する情報システムのセキュリティ対策を行う。

・　セキュリティ関係機関等から発信される注意喚起を定期的に確認する。

などの注意喚起を実施した。

○　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た。

○　ウェブ会議システムのぜい弱性に関する注意喚起

利用者が急増しているウェブ会議システムについて、悪意のあるユーザの用意したリンク先に接続することで、認証情報を窃取されたり、プログラムを起動されたりする可能性があるといったぜい弱性が指摘された。これを受けて、警察では、４月上旬に重要インフラ事業者等に対して、同ぜい弱性を利用したサイバー攻撃に対する注意喚起を実施した。

○　新型コロナウイルス感染症に乗じた犯罪の手口に関する注意喚起

新型コロナウイルス感染症に関連した不審メールや悪質なショッピングサイトについて、警察庁、都道府県警察及び日本サイバー犯罪対策センター（ＪＣ３）のウェブサイト、Twitter等で注意喚起を実施した。

２　サイバー空間の脅威情勢

(1)　主な事例

○　豪州に対するサイバー攻撃

６月、豪州の首相、内務大臣及び国防大臣は、豪州の組織が洗練された国家的な主体によるサイバー攻撃の標的になっていると発表した。この攻撃は、あらゆるレベルの政府、産業、政治組織、教育、医療、重要サービス等、幅広い分野にわたる豪州の組織が標的であるとしている。

○　我が国の防衛関連企業及び電気通信事業者に対する不正アクセス

我が国の複数の防衛関連企業は、不正アクセスを受けたことを１月から２月にかけて相次いで公表しており、一部企業では防衛情報が流出した可能性があるとしている。

さらに、５月、我が国の大手電気通信事業者は、不正アクセスを受け、一部の情報が外部に流出した可能性があることを確認し、公表した。同事業者の海外拠点への侵入をきっかけとし、国内のサーバへ到達したとみられている。

○　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（身代金を要求する不正プログラム）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。

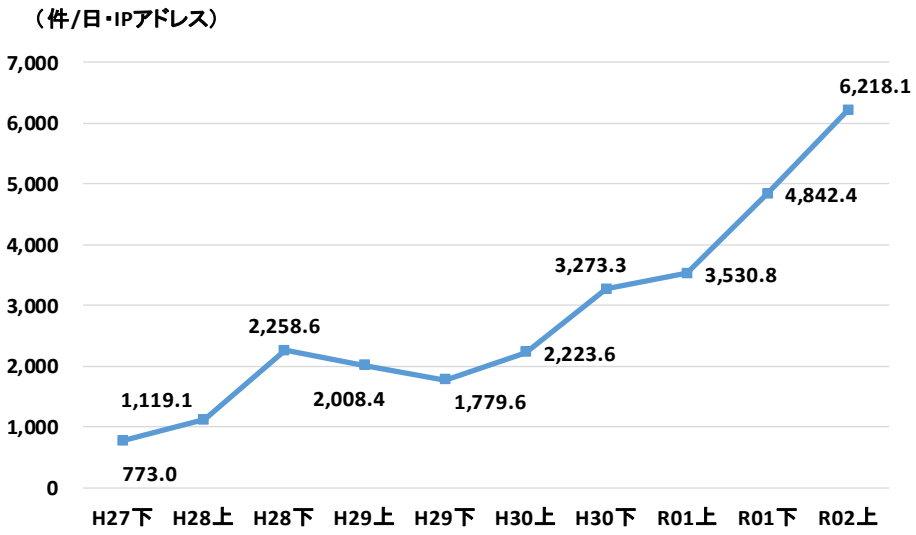
(2)　サイバー空間におけるぜい弱性探索行為等の観測状況

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ＩｏＴ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ている。

令和２年上半期に本システムにおいて検知したアクセス件数（全ポート）は、１日・１ＩＰアドレス当たり6,218.1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、2016年の大流行以降も新種のMirai亜種（自己増殖型不正プログラム）が出現し続けていることなどが背景にあるものとみられる。

【図表３：センサーにおいて検知したアクセス件数の推移】

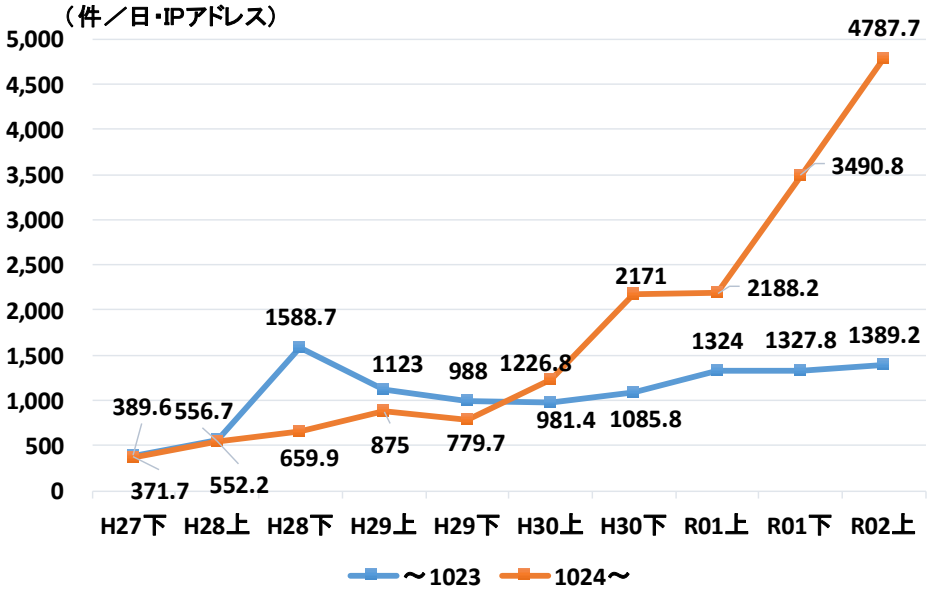


イ　特徴的な観測

○　広範な宛先ポートへアクセスする送信元が増加

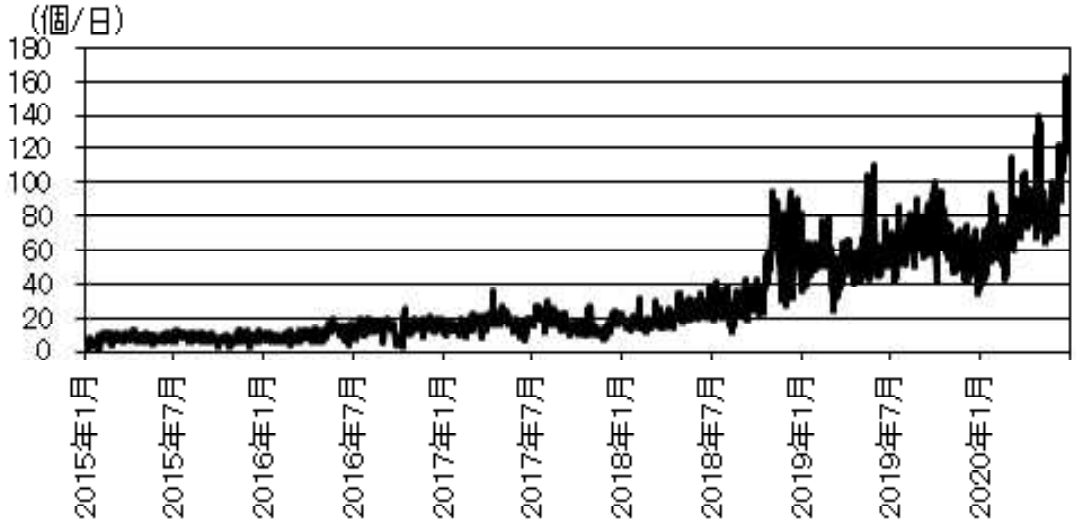
検知したアクセスの宛先ポートに着目すると、ポート番号1024以上のポートへのアクセス件数が増加を続けており、全ポートへのアクセスが増加している大きな要因となっている。1024以上のポートは、主としてＩｏＴ機器が標準設定で使用するポート番号が複数あり、多くがＩｏＴ機器に対するサイバー攻撃やぜい弱性を有するＩｏＴ機器の探索行為であるとみられる。

【図表４：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[*5] 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27年から平成30年上半期までは同水準で推移していたが、平成30年下半期から増加している。令和２年上半期における送信元ＩＰアドレス数は、１日当たり82.2個で、前年同期の54.2個と比較して、28.0個（51.7%）増加した。

【図表５：１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。把握した情報を悪用された場合は、前触れなく様々な攻撃を行われたり、短期間に広範囲の攻撃を行われたりするなどの被害が懸念される。

○　ＩｏＴ機器等のぜい弱性を狙ったアクセスの観測

令和２年上半期のMirai[*6] 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547.7件で、前年同期の466.3件と比較して、81.4件増加した。また、アクセスの多い宛先ポートに変動が見られたことから、攻撃の標的となるＩｏＴ機器が変化したものと考えられる。

例えば、５月中旬から、海外製ルータ等に使われる宛先ポート37215/ＴＣＰに対するMiraiボットの特徴を有するアクセスの増加が観測され

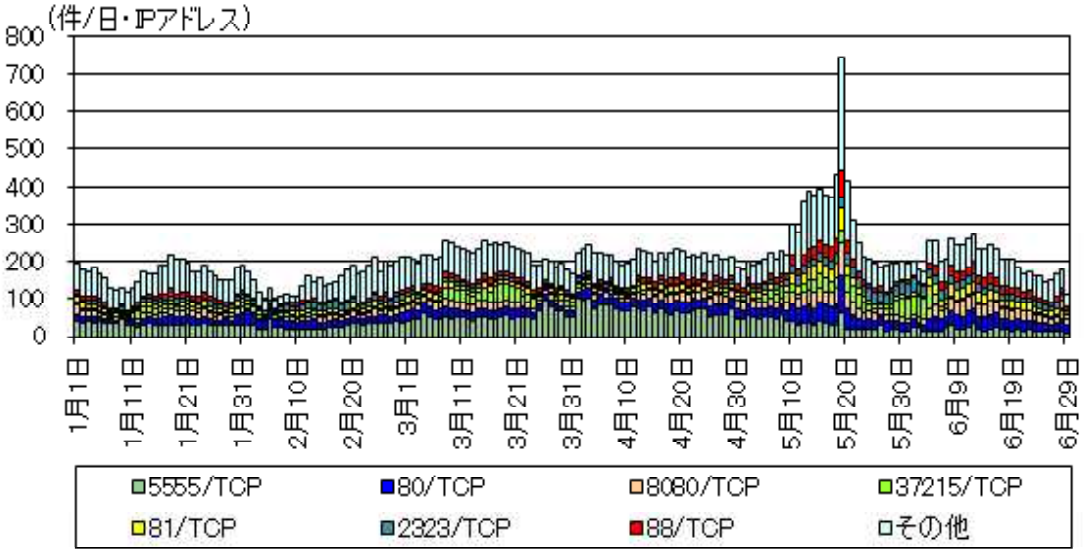
---

*5　ポートとは、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。

*6　ＩｏＴ機器を感染対象とする不正プログラム

た。当該ポートに対するアクセスは、リモートから任意のコードが実行可能となるぜい弱性に関連しており、ＩｏＴ機器等のぜい弱性を悪用し、不正プログラムの感染を狙ったものと考えられる。

【図表６：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）】

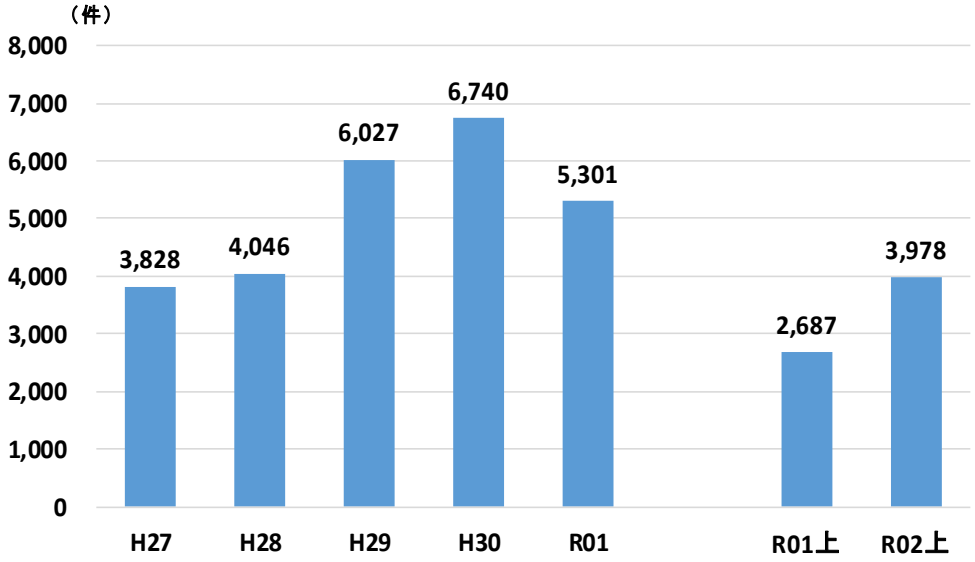


(3)　標的型メール攻撃

ア　標的型メール攻撃の件数の推移

令和２年上半期に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把握した標的型メール攻撃の件数は3,978件であった。

【図表７：標的型メール攻撃の件数の推移】



イ　標的型メール攻撃の特徴

令和２年上半期にサイバーインテリジェンス情報共有ネットワーク[*7] を通じて把握した標的型メール攻撃には、

- 「ばらまき型」攻撃[*8] の割合は全体の98％
- 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78％
- 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98％

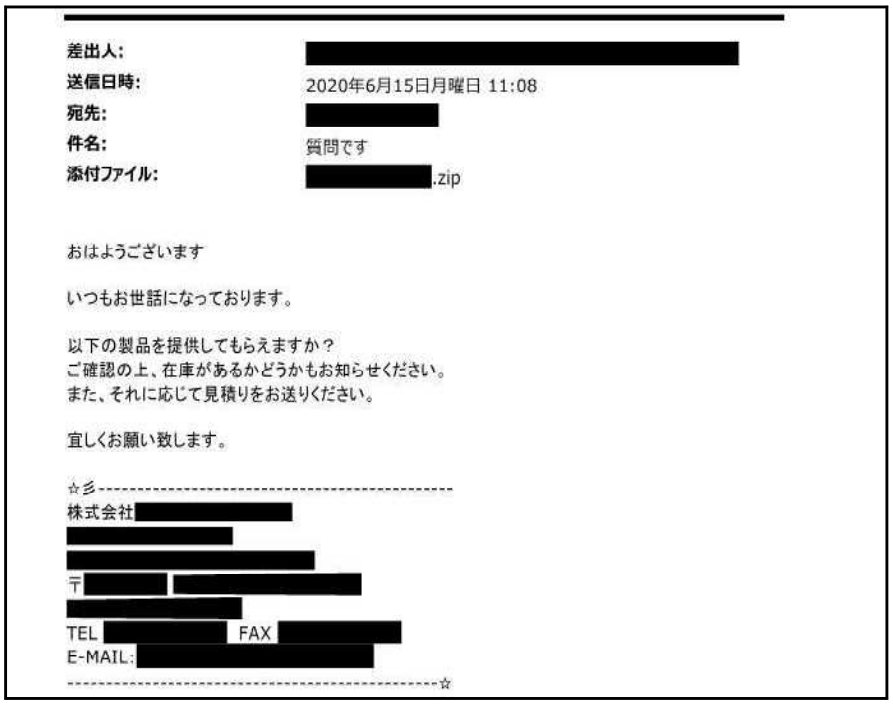
などの特徴があった。

ウ　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。

○　製品に関する質問と称して、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８：標的型メールの事例１】

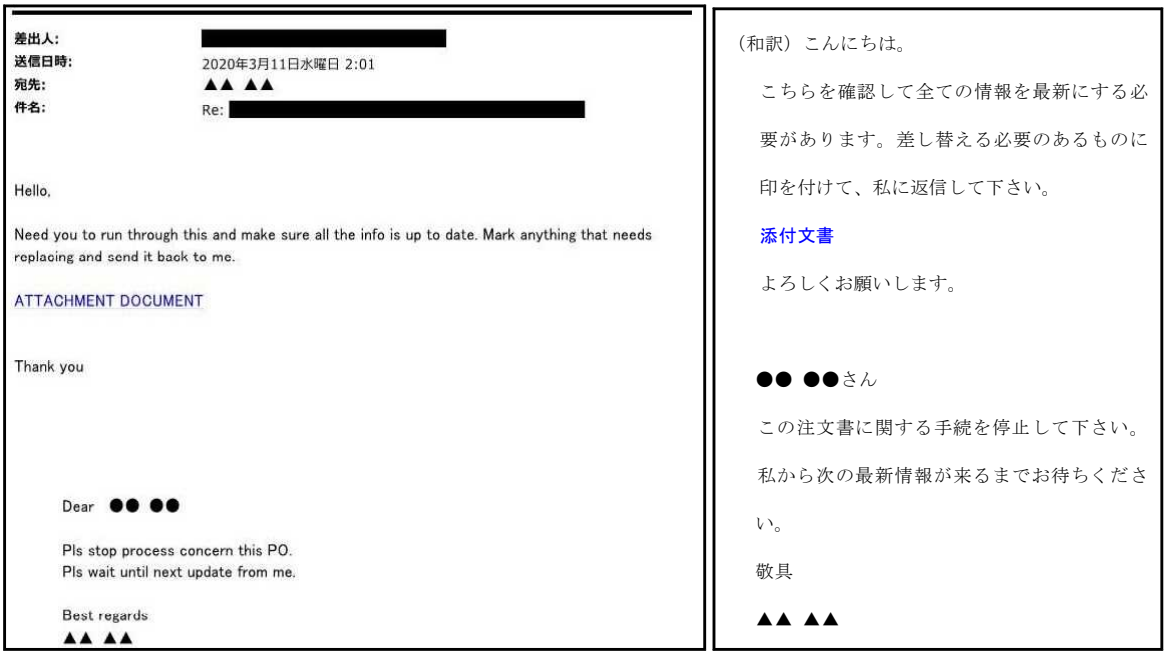


*7　警察と先端技術を有する全国約8,100の事業者等（令和２年７月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組み。内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携し、政府機関に対する標的型メール攻撃の分析結果についても情報を共有している。

*8　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。

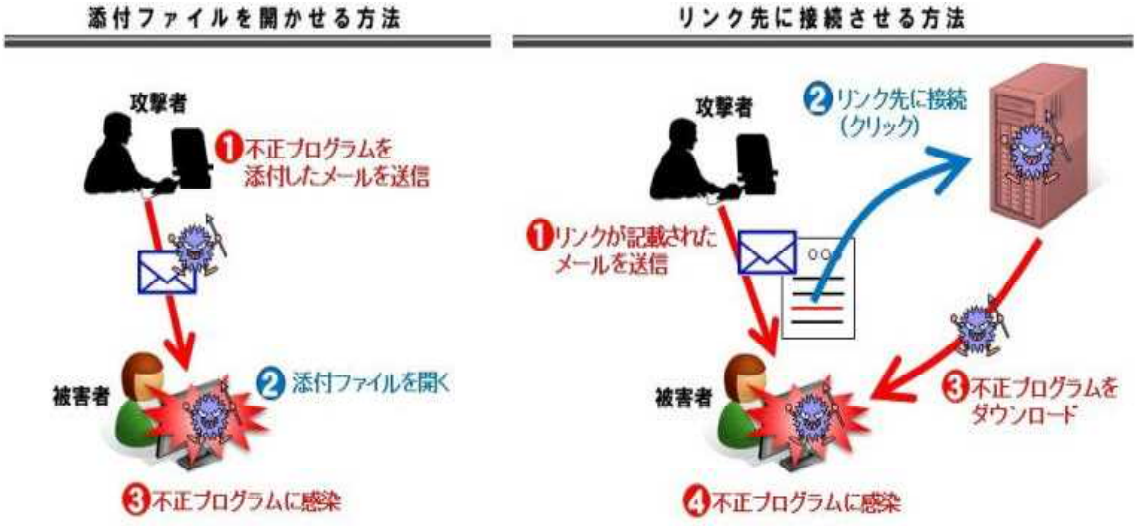
○　添付資料の内容を確認して更新するよう、メール中のリンク先に接続するよう誘導するメールが、製造業者に対して送信された。

【図表９：標的型メールの事例２】



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。

【図表10：不正プログラムに感染させる手口の例】

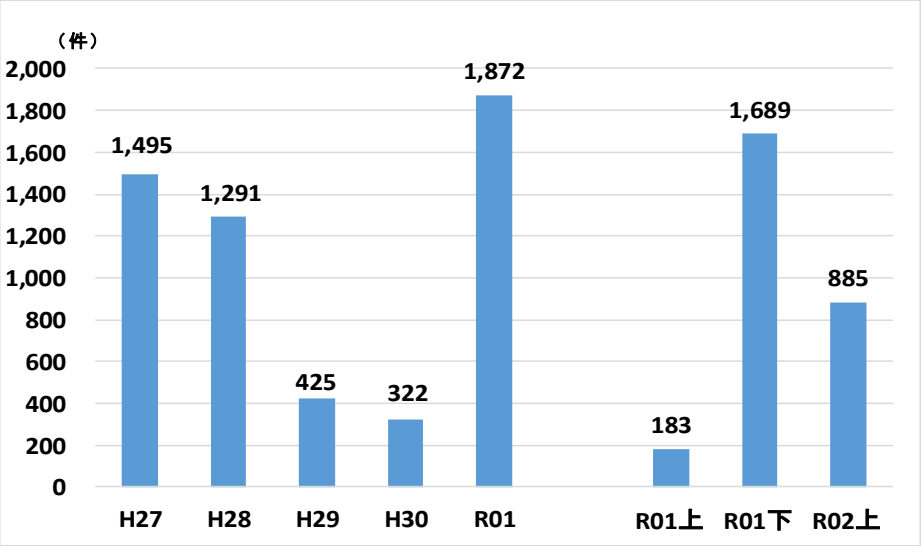


(4)　インターネットバンキングに係る不正送金事犯の発生状況等

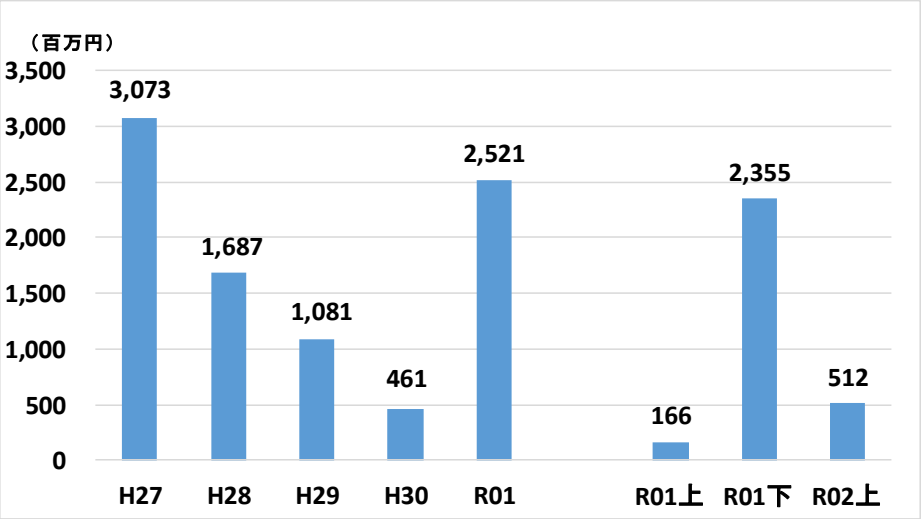
ア　概況

令和２年上半期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885件、被害額約５億1,200万円で、前年同期と比べて大幅に増加した。

【図表11：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12：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

・　前年上半期は、発生件数・被害額ともに以前と比べて減少傾向にあったものの、９月から被害が急増した。

・　令和２年上半期は、被害が急増した前年下半期と比べて減少しているものの、前年同期と比べて大幅に増加しており、その被害の多くは、前年９月以降から引き続いている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。

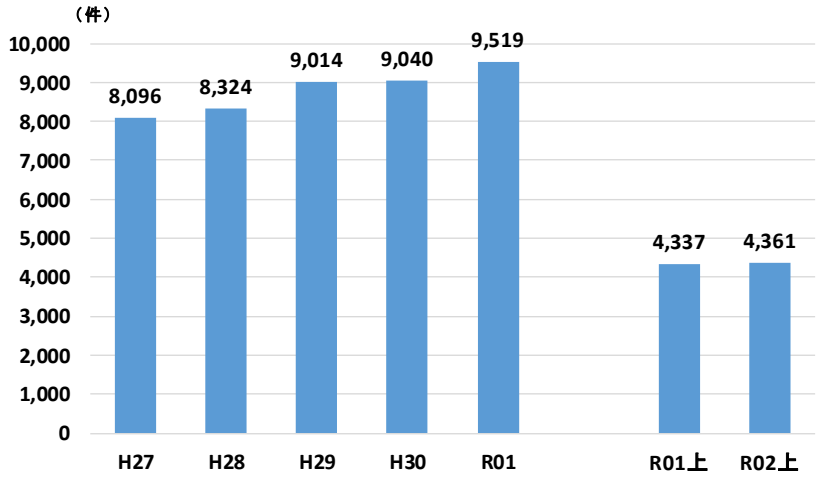
・　フィッシングサイトへの誘導には、金融機関を装ったＳＭＳ等のほか、宅配事業者からの荷物の配達連絡を装ったＳＭＳによって、金融機関を装ったフィッシングサイトへ誘導するものも確認されている。また、当該ＳＭＳからの誘導により、不正なアプリを携帯電話機等の端末にインストールさせ、当該アプリによって表示される偽の警告メッセージからフィッシングサイトへ誘導する手口も確認されている。
・　金融機関を装ったフィッシングサイトで、ＩＤやパスワード等に加えて金融機関の公式アプリの有効化手続に必要な情報[*9]を窃取され、不正に有効化されたアプリを用いて不正送金される被害も確認されている。
・　金融機関の公式アプリが不正に有効化された後、キャッシュカードを用いずにＡＴＭでの入出金が可能なアプリの機能を用いて、ＡＴＭで被害口座から現金が不正に出金される新たな手口[*10]が５件発生し、約60万円の被害が確認されている。
・　一次送金先として把握した1,244口座のうち、名義人の国籍は日本が52.0％と最も多く、次いでベトナムが12.4％、中国が3.5％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、電子マネーや暗号資産の購入、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。

(5)　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年上半期の検挙件数は4,361件と、前年同期と同水準となった。

【図表13：サイバー犯罪の検挙件数の推移】



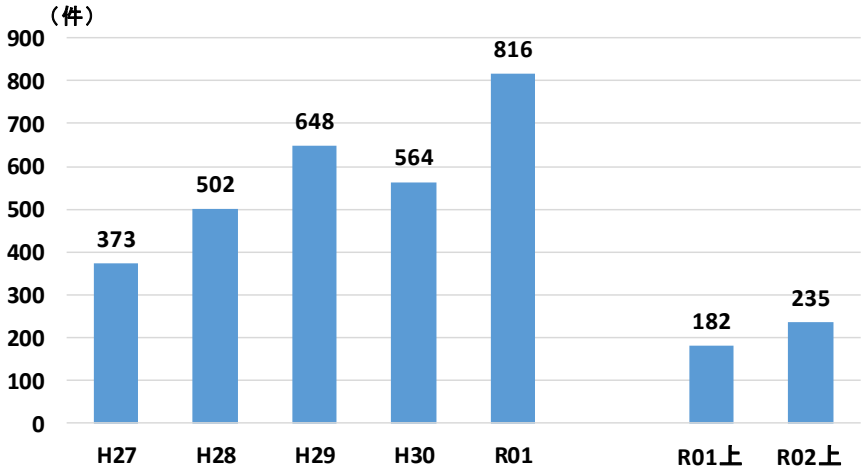
*9　金融機関によって異なるが、生年月日、電話番号、乱数表の文字列、自動音声電話による認証で用いるコード番号等の情報。

*10　他の預貯金口座への送金が無いため、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。

イ　不正アクセス禁止法[*11] 違反

令和２年上半期における不正アクセス禁止法違反の検挙件数は235件と、前年同期と比べて増加した。検挙件数のうち、222件が識別符号窃用型[*12]で全体の94.5％を占めている。

【図表14：不正アクセス禁止法違反の検挙件数の推移】



○　「言葉巧みに利用権者から聞き出した又はのぞき見たもの」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、言葉巧みに利用権者から聞き出した又はのぞき見たものが91件と最も多く、全体の41.0％を占めており、次いで他人から入手したものが59件で全体の26.6％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108件と最も多く、全体の48.6％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32件で全体の14.4％を占めている。

ウ　コンピュータ・電磁的記録対象犯罪[*13]

(ｱ)　検挙件数

令和２年上半期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218件で、前年同期と比べて増加した。

---

*11　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。）

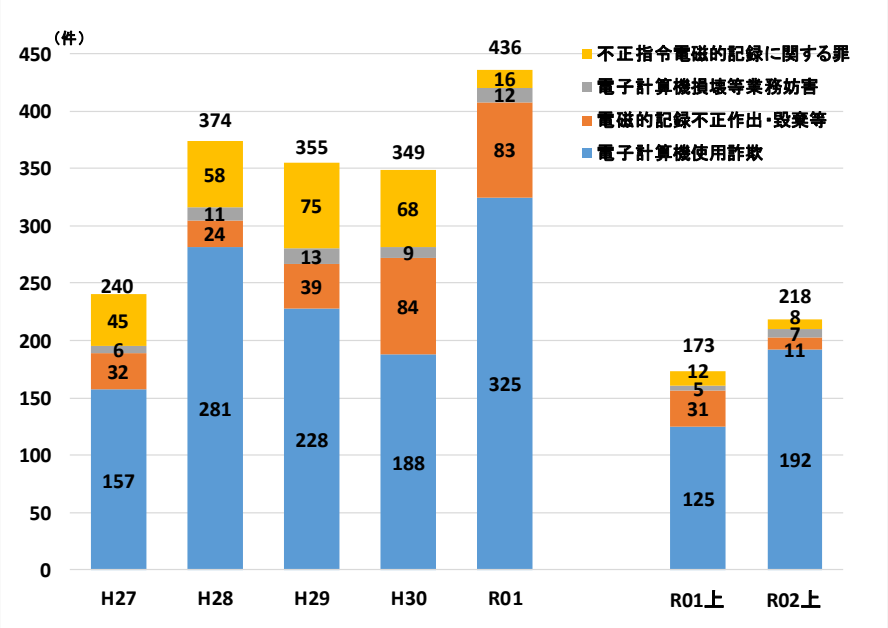
*12　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

*13　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)　特徴

検挙件数のうち、電子計算機使用詐欺が192件と最も多く、全体の88.1%を占めている。

【図表15 ：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935件と、前年同期と比べて減少した。

○　詐欺の検挙件数は609件と、前年同期と比べて増加した。

(6)　主な取組

○　サイバー攻撃の発生を想定した訓練

警察では、令和２年上半期においても重要インフラ事業者、東京大会関連事業者等とのサイバー攻撃の発生を想定した訓練を実施した。具体的には、当該事業者等と協力して、当該事業者等の職員に対して訓練用の標的型メールを送信し、職員の対処能力の向上を図る訓練等を行った。

○　サイバー攻撃事案で使用されたＣ２サーバ*14 のテイクダウン

警察では、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サーバの機能停止（テイクダウン）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

*14　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。攻撃者の命令に基づいて動作する、不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

進した。この結果、令和２年上半期においては５台のＣ２サーバの機能停止を行った。

○　リスト型攻撃[*15] に対する被害防止対策

千葉県警察及び茨城県警察では、ＪＣ３と連携して、押収したリスト型攻撃ツールを解析し、この仕組みや攻撃手口を解明したことから、ＪＣ３のホームページで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ＪＣ３が共同で開発したツールの活用等により、ＪＣ３が発見した詐欺サイトのＵＲＬ情報をＡＰＷＧ[*16] 等に提供し、被害防止対策を実施している。

---

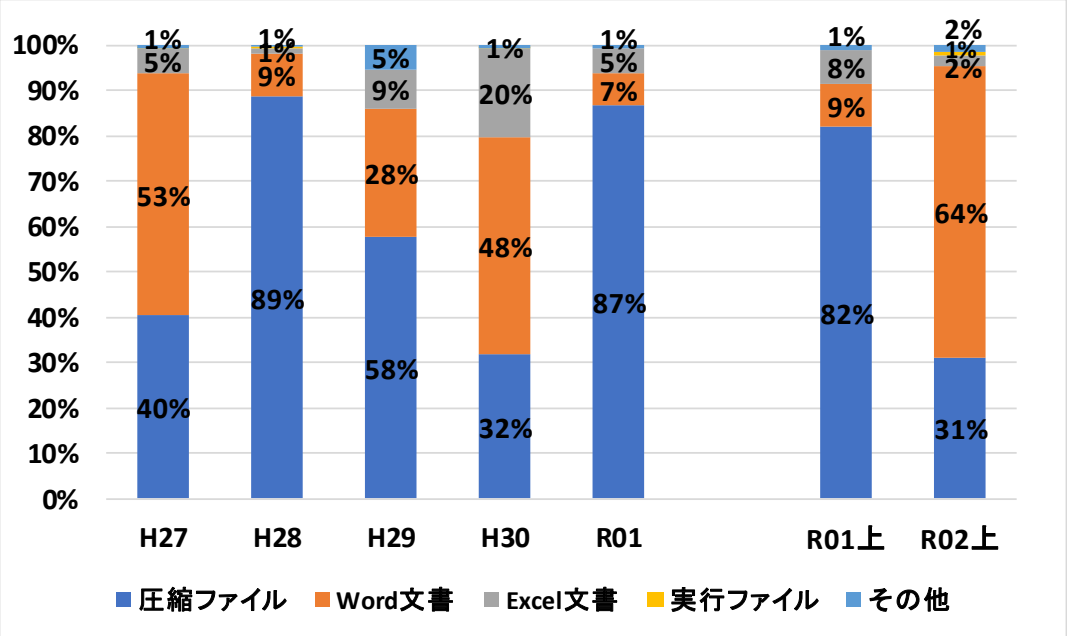
*15　オンラインサービスで使用するアカウントやパスワードからなるリストを使って、様々なオンラインサービスにログインを試みる攻撃

*16　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

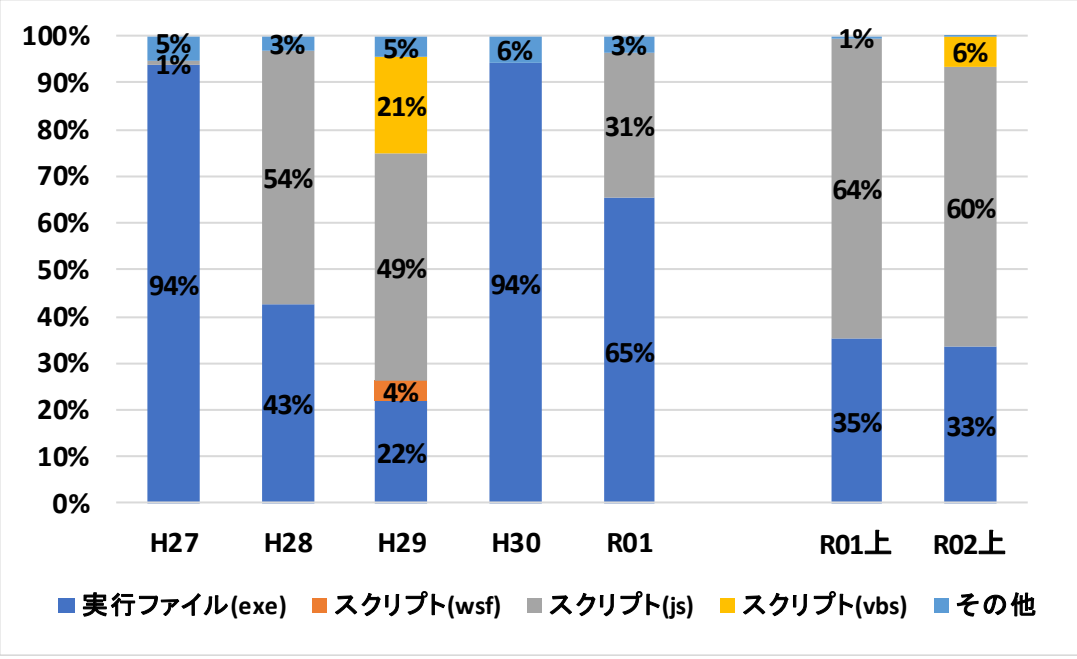
【　参考　】

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

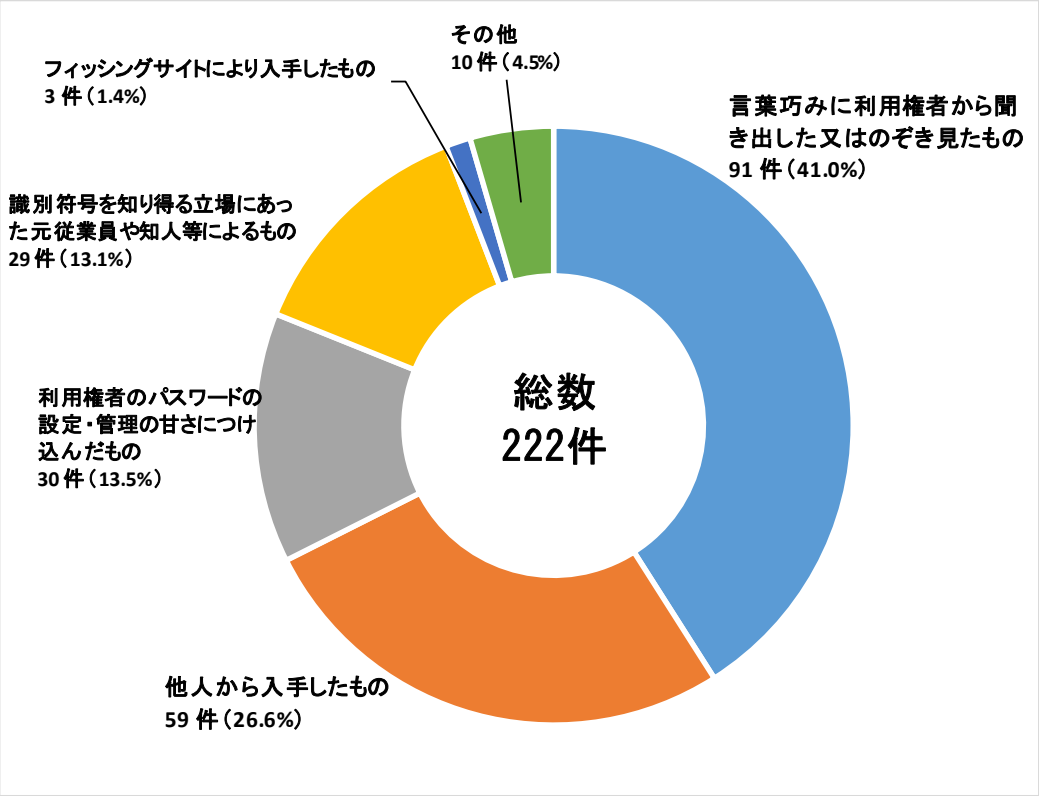


（2）　圧縮ファイルで送付されたファイル形式の割合の推移

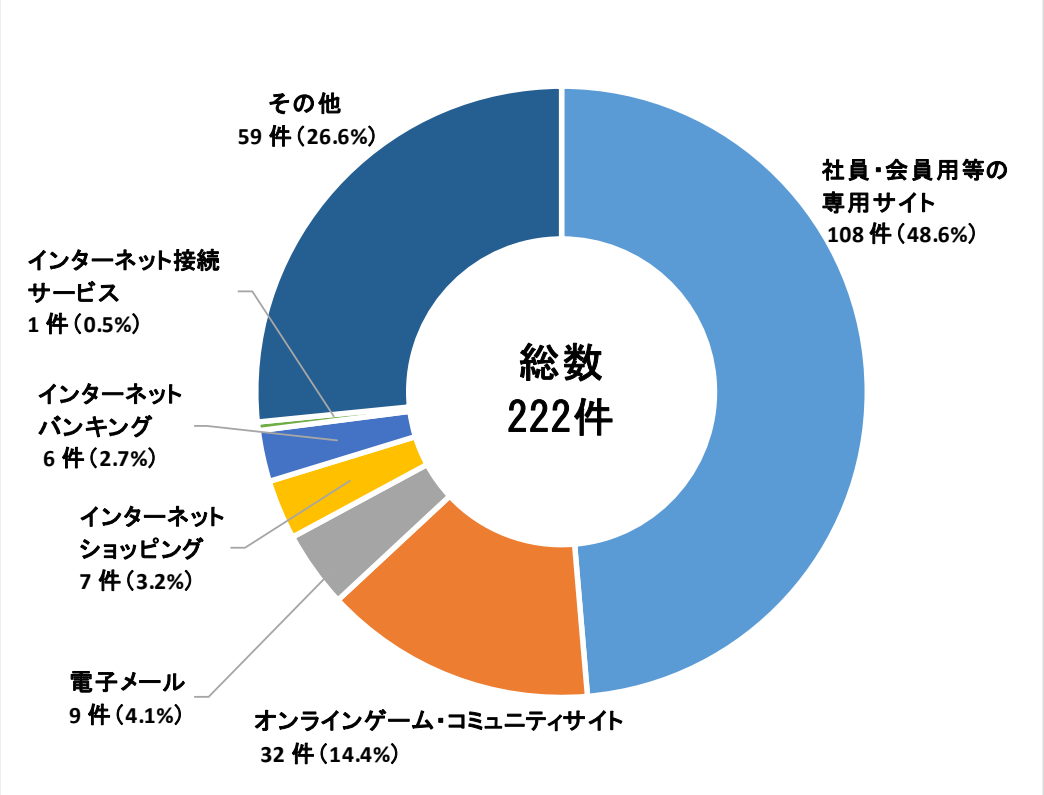


2　不正アクセス禁止法違反の検挙状況

(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

○　アルバイトの男（32）は、平成31年１月から同年２月までの間、インターネット通販サイトに対して、元勤務先の会社のＩＤ・パスワードを無断で使用して不正アクセスし、電子マネーのギフト券を不正に注文し窃取した。令和２年２月、男を不正アクセス禁止法違反（不正アクセス行為）等で検挙した。（京都）

○　アルバイトの男（25）は、平成29年12月から令和元年５月までの間、ＳＮＳにおいて、元交際相手のＩＤ・パスワードを無断で使用して不正アクセスし、同アカウントを乗っ取り、同人を誹謗中傷する内容を投稿して名誉を毀損した。令和２年２月、男を不正アクセス禁止法違反（不正アクセス行為）等で検挙した。（広島）

３　コンピュータ・電磁的記録対象犯罪の検挙状況

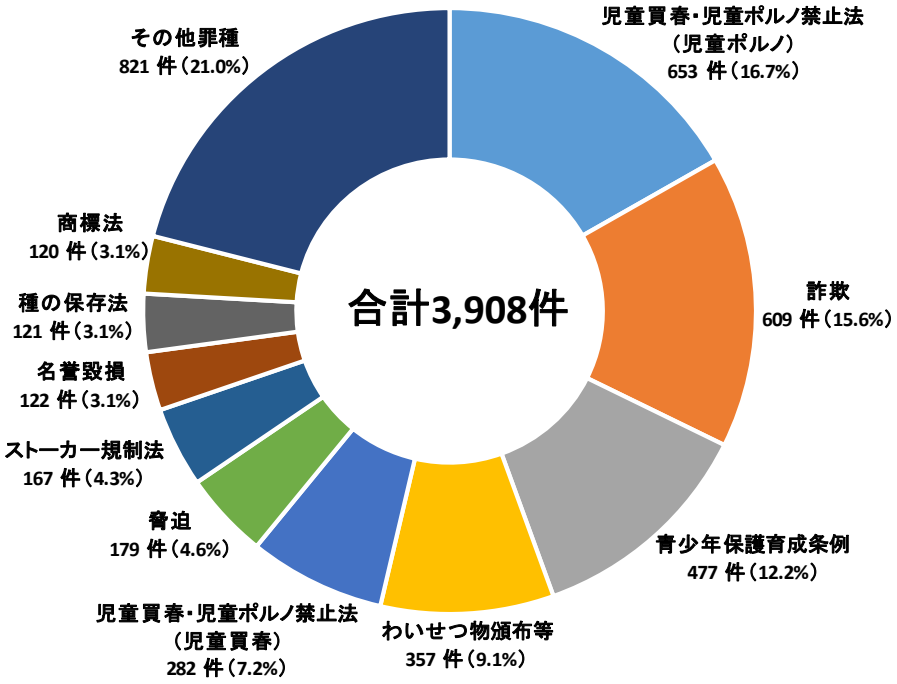
	H27	H28	H29	H30	R1	R01(上)	R02(上)
電子計算機使用詐欺	157	281	228	188	325	125	192
電磁的記録不正作出･毀棄等	32	24	39	84	83	31	11
電子計算機損壊等業務妨害	6	11	13	9	12	5	7
不正指令電磁的記録供用	21	36	24	37	6	5	5
不正指令電磁的記録取得･保管	16	18	22	19	6	4	3
不正指令電磁的記録作成･提供	8	4	29	12	4	3	0

コンピュータ・電磁的記録対象犯罪

○　会社員の男（51）は、平成31年４月、宅配注文を仲介するサイトにおいて、嫌がらせ目的で元交際相手の住所・氏名を使用して弁当等の虚偽注文をした。令和２年１月、男を私電磁的記録不正作出・同供用で検挙した。（栃木）

○　飲食店従業員の男（28）は、令和元年10月から同年12月までの間、インターネットショッピングサイトにおいて、勤務先の飲食客が支払いに使用したクレジットカードの情報を盗用し、家庭用テレビゲーム機等を注文して詐取した。令和２年４月、男を電子計算機使用詐欺で検挙した。（愛知）

４　その他の検挙状況



商標法違反

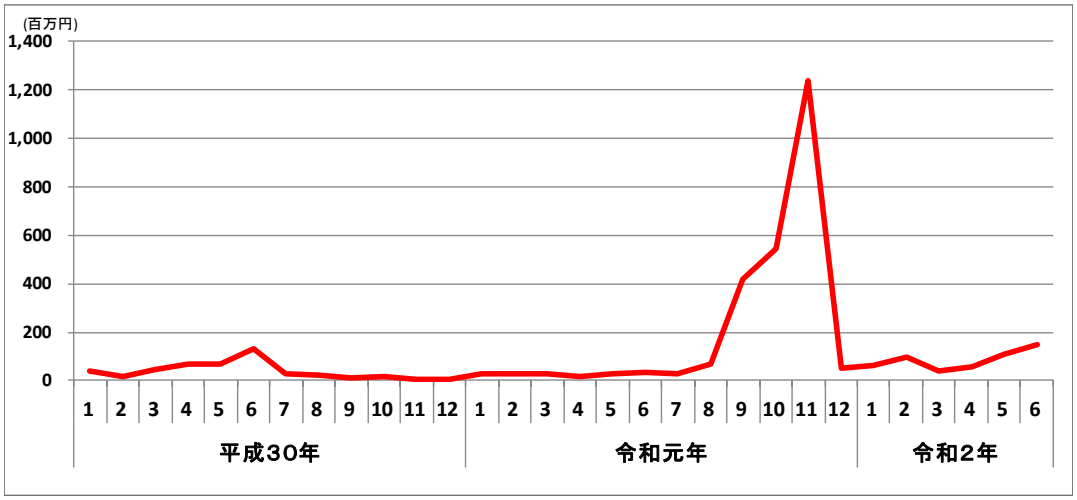
○　無職の男（19）は、令和元年８月から同年12月までの間、商標の使用に際し何ら権限がないのに、商標が付されたスマートフォンの内蔵プログラムを改変して販売し、商標権者の商標権を侵害した。令和２年３月、男を商標法違反で検挙した。（京都）

チケット不正転売禁止法違反

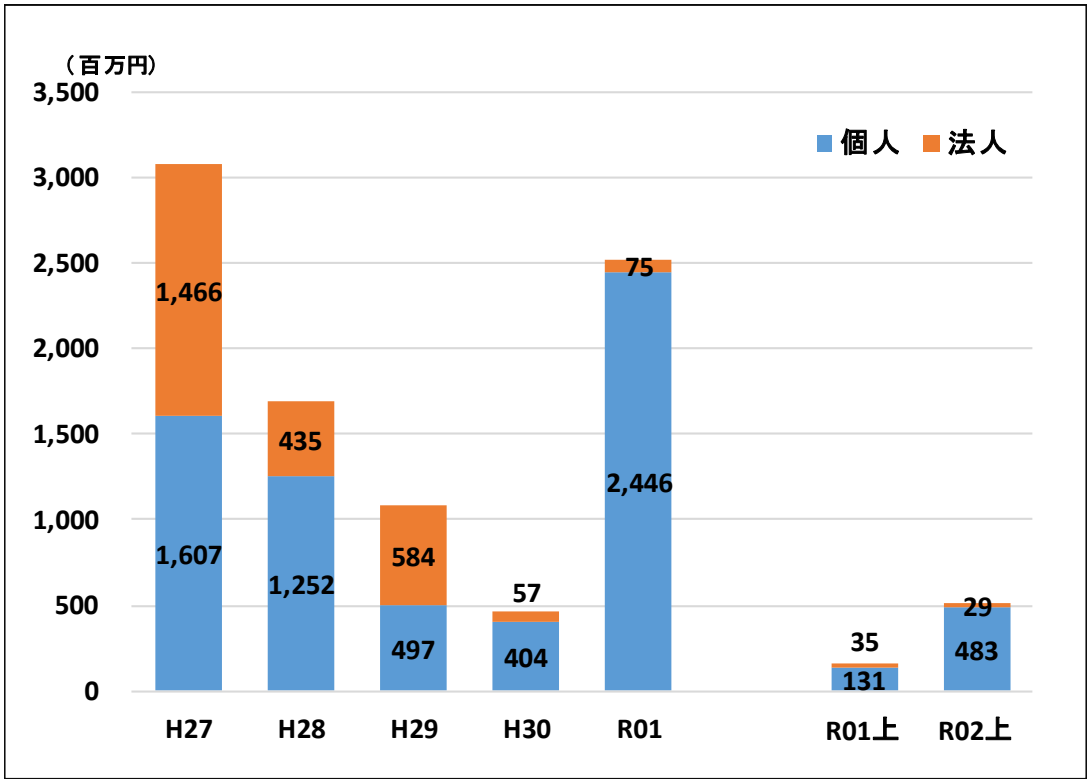
○　無職の男（38）は、令和元年９月、チケット売買仲介サイトにおいて、特定興行入場券である公演チケット３枚を販売価格を超える価格で不正に転売した。令和２年２月、男を特定興行入場券の不正転売の禁止等による興行入場券の適正な流通の確保に関する法律違反で検挙した。（埼玉）

５　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

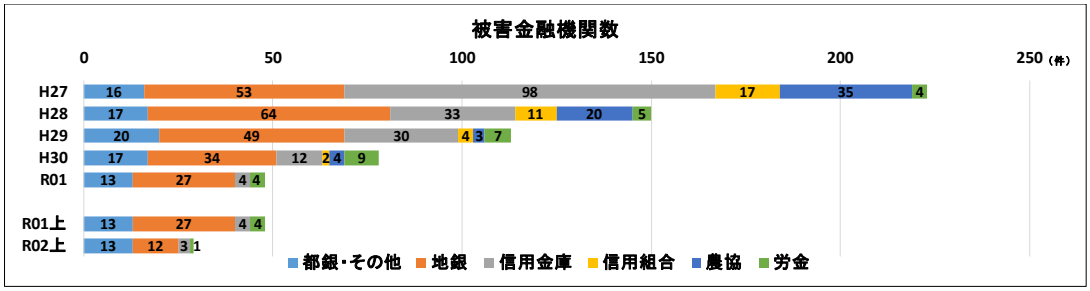
(1)　被害額の推移

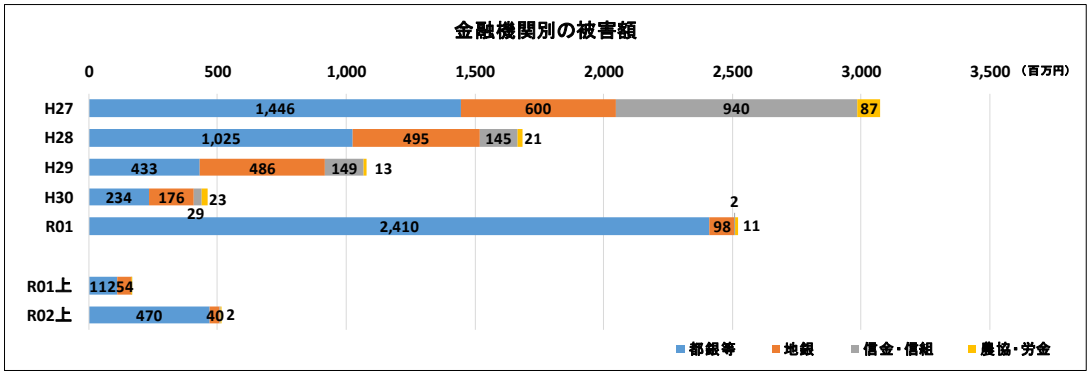


(2)　口座開設者別の被害状況

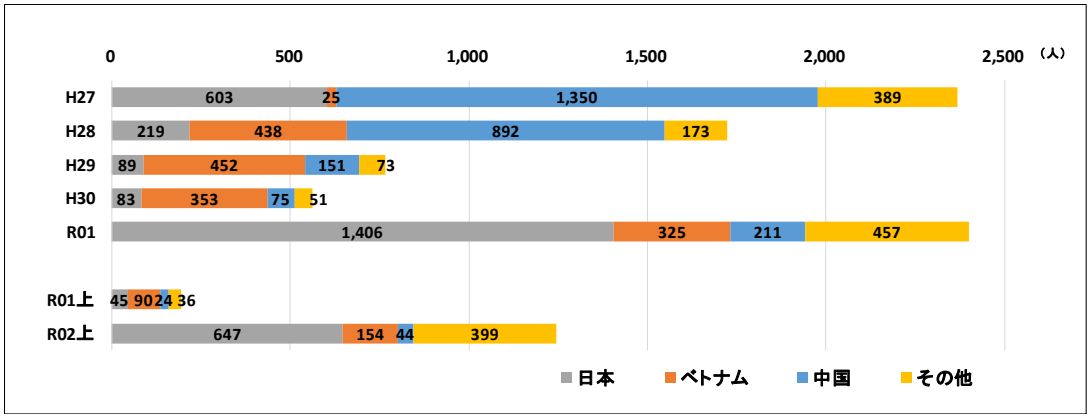


(3)　金融機関別の被害状況

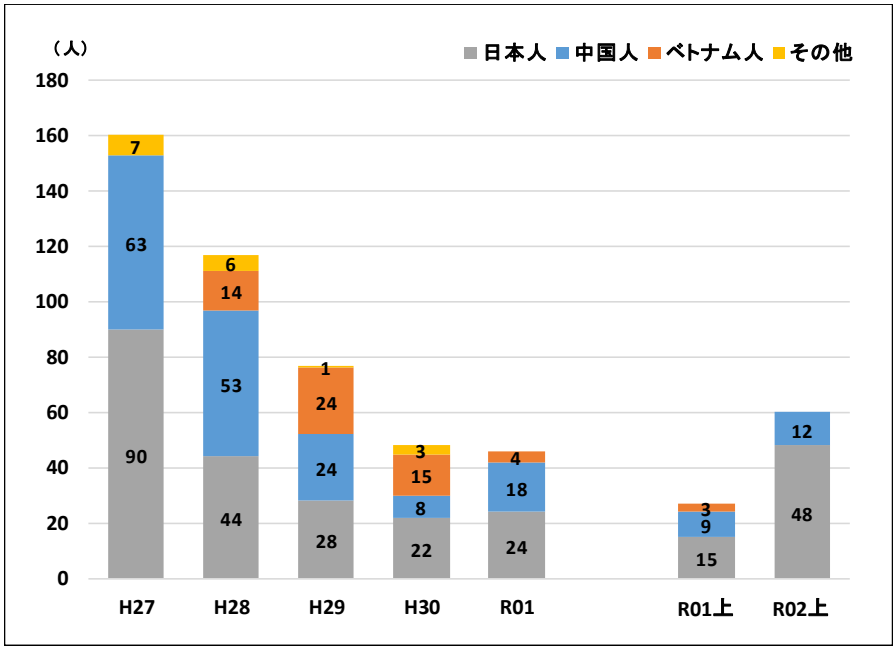




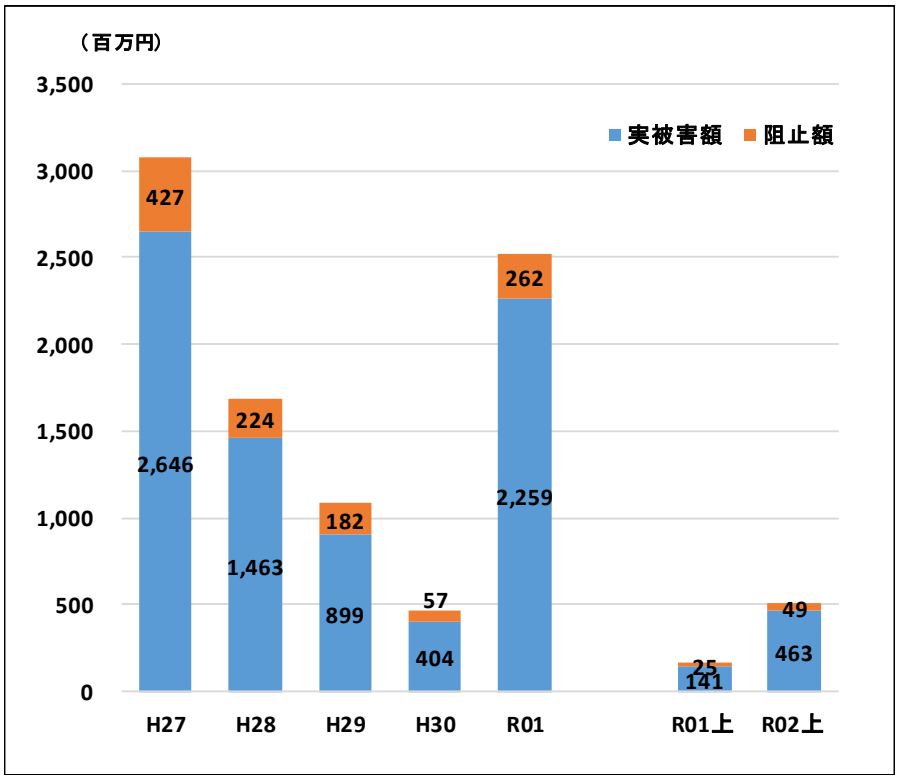
(4)　一次送金先口座名義人の国籍



(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）	439	50.8%	256	29.6%	170	19.7%	865
電子証明書（法人口座）	0	0.0%	16	80.0%	4	20.0%	20