広　報　資　料
令和２年３月５日
警　　察　　庁

令和元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　サイバー攻撃の情勢等

国内外で様々なサイバー攻撃が発生しており、今後も世界的規模でのサイバー攻撃の発生等が懸念。

(1)　サイバー空間における探索行為等

○　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件数は、１日１ＩＰアドレス当たり4,192.0件と増加傾向。

○　リモートデスクトップサービスを標的としたアクセスの急増を断続的に観測。

(2)　標的型メール攻撃

○　警察と先端技術を有する事業者等との情報共有の枠組みを通じて標的型メール攻撃を把握し、事業者等に対して分析した情報を提供。

○　把握した標的型メール攻撃5,301件のうち、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92％と引き続き高い割合。

(3)　主な取組

先端技術を有する事業者等との情報共有のほか、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。

２　サイバー犯罪の情勢等

従来から発生している犯罪に加え、新たな手口の犯罪が発生。

(1)　サイバー犯罪の検挙状況

検挙件数は9,519件と過去最多。

ア　不正アクセス禁止法違反

○　検挙件数は816件と、前年と比べて増加。

○　インターネットバンキングに係る不正送金事犯は、発生件数1,872件、被害額約25億2,100万円で、いずれも前年と比べて増加。

イ　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪

○　検挙件数は436件と、前年と比べて増加。

(2)　主な取組

インターネットバンキングに係る不正送金被害が急増したため、日本サイバー犯罪対策センター（ＪＣ３）、全国銀行協会と連携して注意喚起を実施。

３　今後の取組

○　2020年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ対策の推進

○　高度な実践型演習、検定及び学校教養を連携させた人材育成の推進

○　ＪＣ３等と連携した被害防止対策等の推進

別　添

令和元年におけるサイバー空間をめぐる脅威の情勢等

サイバー空間をめぐる脅威は深刻な情勢が続いている。

令和元年中の警察によるサイバー犯罪の検挙件数は、過去最多となった。インターネットバンキングに係る不正送金事犯は、平成28年以降、金融機関のセキュリティ対策の強化等により発生件数・被害額ともに減少傾向が続いていたが、令和元年９月から被害が急増し、発生件数・被害額のいずれも前年と比べて大幅に増加した。このほか、「コード決済」*1 不正利用事案などの国民に身近なサイバー犯罪が発生した。

（参考）

令和元年９月に警察庁が実施したアンケート調査（全国の15歳以上の男女１万人を対象に、年代別・性別・都道府県別の回答者数の割合が平成27年国勢調査の結果に準じたものとなるようインターネットを通じて実施したもの。）によれば、過去１年間にサイバー犯罪の被害に遭うおそれのある経験をしたと回答した人の割合は28.9％（2,888人）であり、過去１年間にサイバー犯罪の被害に遭ったと回答した人の割合は13.7％（1,373人）であった。

また、サイバー攻撃も後を絶たない。国外においては、豪州連邦議会等に対するサイバー攻撃、アンチドーピング関連機関に対するサイバー攻撃等が発生した。国内においても、国際的ハッカー集団によるものとみられる地方自治体、民間企業等のウェブサイトの閲覧障害が発生したほか、大手電機会社が、不正アクセスを受け、情報が流出した可能性がある旨を公表した。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にある。

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。特に、今夏には、国際的に注目される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。）が開催されることから、関係省庁等と連携し、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詰めの調整・確認を進め、東京大会の安全・円滑な開催に万全を期すための取組を推進している。

---

*1　バーコード又はＱＲコード®（株式会社デンソーウェーブの登録商標）を用いたキャッシュレス決済。

１　サイバー攻撃の情勢等

(1)　主なサイバー攻撃の事例

○　豪州連邦議会等に対するサイバー攻撃

２月、豪州のモリソン首相は、連邦議会下院において、連邦議会及び主要３政党が国家によるとみられるサイバー攻撃を受けたと認めた。被害の詳細は公表されていないが、自由党、労働党及び国民党のコンピュータ・ネットワークに攻撃があったとしている。

○　北朝鮮のサイバー攻撃集団への制裁対象指定

９月、米国財務省は、ランサムウェア「WannaCry」によるサイバー攻撃等に関与したとして、北朝鮮政府が支援するハッカー集団「Lazarus」、「Bluenoroff」及び「Andariel」の３集団を、米国内における資産凍結等の制裁対象に指定したと発表した。

○　国連安全保障理事会北朝鮮制裁委員会の報告書

９月、国連安全保障理事会北朝鮮制裁委員会の専門家パネルは、北朝鮮が大量破壊兵器の開発資金として金融機関や暗号資産（仮想通貨）交換業者へのサイバー攻撃等を実行し、推定20億ドルを違法に得た疑いがあると報告した。

○　アンチドーピング関連機関に対するサイバー攻撃

10月、マイクロソフト社は、９月16日以降、少なくとも16のスポーツ団体及びアンチドーピング関連機関が、サイバー攻撃集団「Strontium」（別名：APT28、Fancy Bear）によるサイバー攻撃を受けていたと発表した。

○　我が国の大手電機会社に対する不正アクセス事案

我が国の大手電機会社は、６月に同社内の端末で不審な挙動を検知し調査した結果、第三者による不正アクセスを受け、外部にデータを送信されていたことが判明したと令和２年１月に公表した。

○　国内のウェブサイトの閲覧障害

警察では、国際的ハッカー集団「アノニマス」を名乗る者が、日本国内の組織に対してサイバー攻撃を実行したとする犯行声明とみられる投稿をＳＮＳ上に掲載している状況を把握している。日本国内の地方自治体、民間企業等を含む８組織のウェブサイトに閲覧障害が発生した。

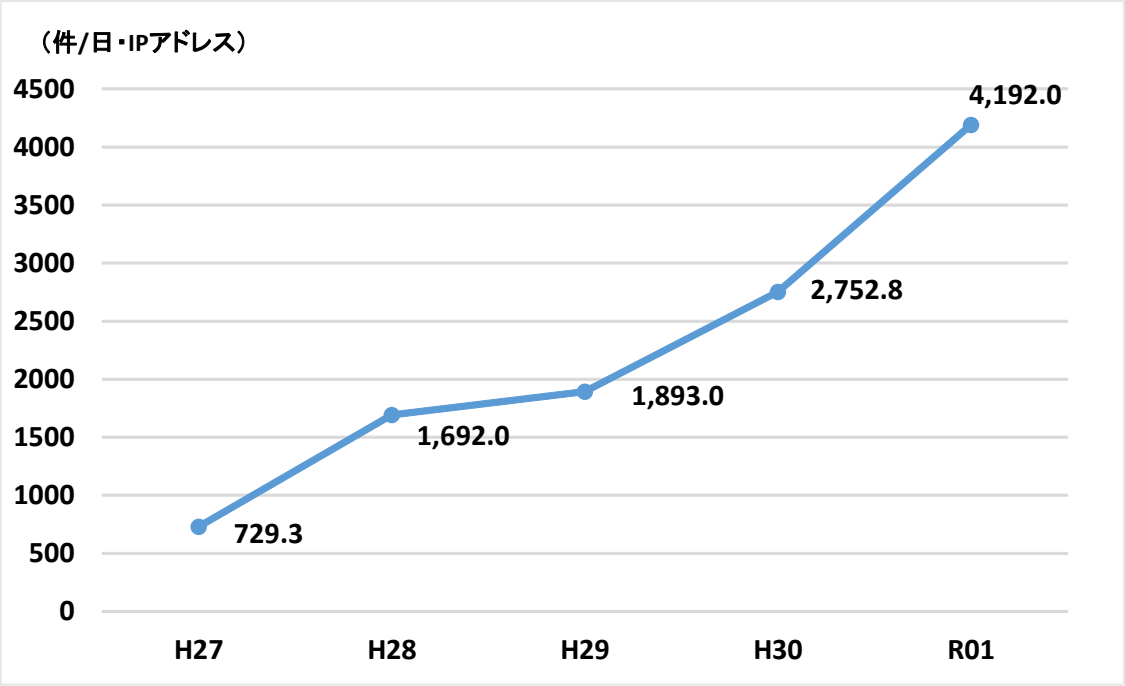
上記事案のほか、別の我が国の大手電機会社が、過去に社内サーバが不正アクセスを受けていたと令和２年に公表するなど、これまで国内外で様々なサイバー攻撃が発生しており、今後も世界的規模でのサイバー攻撃の発生等が懸念される。

(2)　サイバー空間における探索行為等

ア　センサー*2 において検知したアクセスの概況

センサー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4,192.0件と、増加傾向にある。

【図表１　センサーにおいて検知したアクセス件数の推移】



イ　特徴

○　Mirai*3 に感染したボットの特徴を有するアクセスの観測

Miraiに感染したボットの特徴を有するアクセスは、年間を通じて増加傾向にあり、令和元年６月中旬以降は、これまで顕著なアクセスが見られなかった宛先ポート*4 に対するアクセスが観測されるようになった。対象となった宛先ポートの中には、過去にぜい弱性の存在が明らかになった機器等で使用されるものがあり、こうした宛先ポートに対するアクセスは、セキュリティ対策が講じられていない機器に対する感染拡大を狙ったものと考えられる。

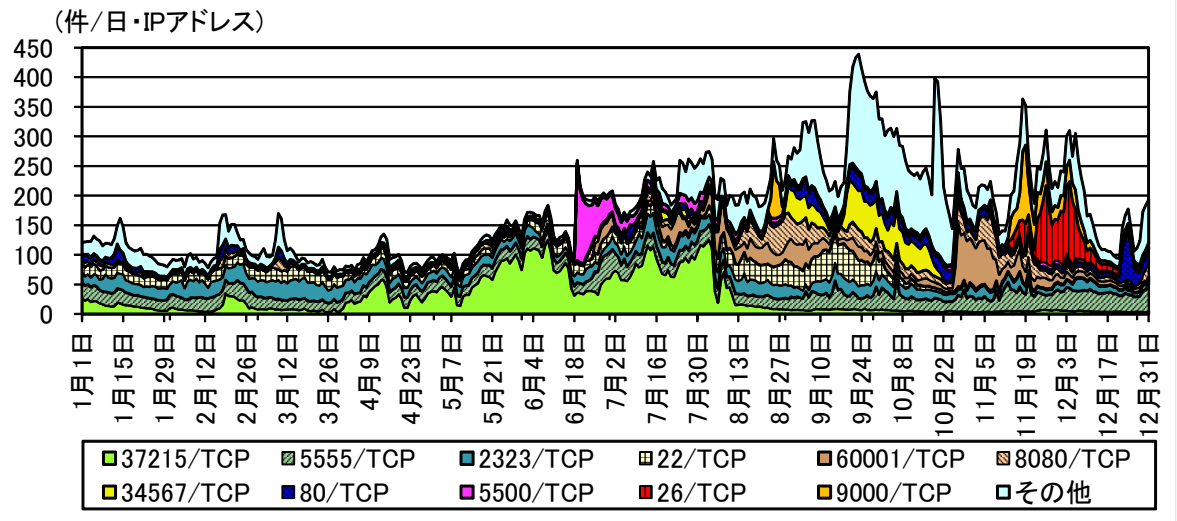
---

*2　警察庁が24時間体制で運用しているリアルタイム検知ネットワークシステムにおいて、インターネットとの接続点に設置しているセンサーのこと。本センサーでは、各種攻撃を試みるための探索行為を含む、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。

*3　ＩｏＴ機器を感染対象とする不正プログラム

*4　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。

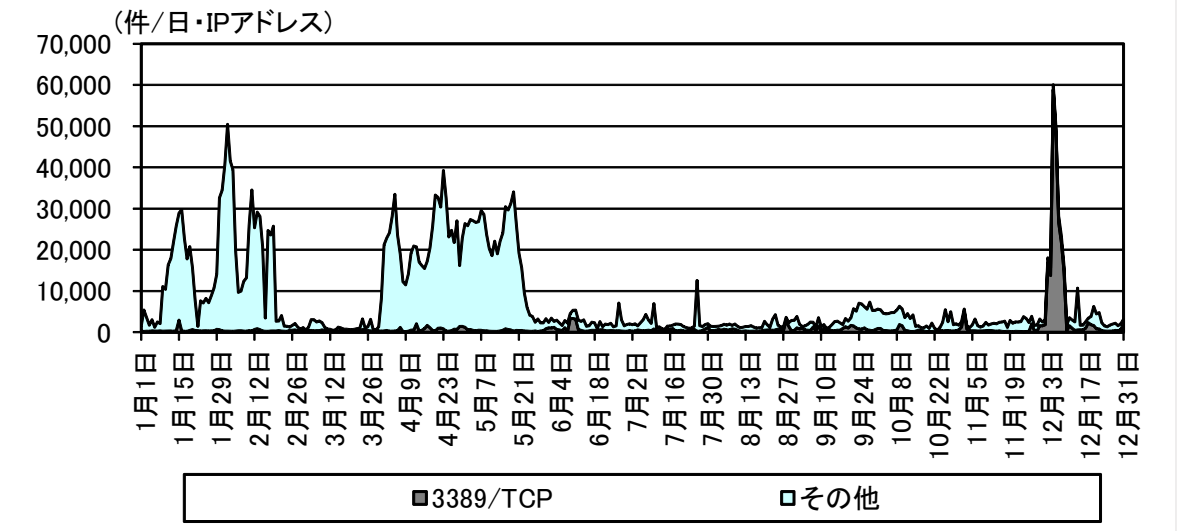
【図表２　Miraiボットの特徴を有するアクセス件数の推移（23/TCPを除く宛先ポート別）】



○　リモートデスクトップサービス[*5] を標的としたアクセスの増加

元年中は、１月上旬から２月中旬までの間、３月下旬から５月下旬までの間及び12月上旬に、Microsoft Windowsの遠隔操作に使用されるリモートデスクトップサービスを標的としたアクセスの急増を観測した。特に、上半期は、同サービスの標準設定で使用される宛先ポート3389/TCP以外にも、広範囲の宛先ポートに対するアクセスを観測した。

【図表３　リモートデスクトップサービスを標的とした広範囲の宛先ポートに対するアクセス件数の推移】



同サービスについては、５月中旬、Microsoft社から、攻撃に成功すると外部から管理者権限で任意の操作が実行可能となるぜい弱性に関する緊急の修正プログラムが公開されており、同プログラムを適用するなどセキュリティ対策を講じる必要がある。

---

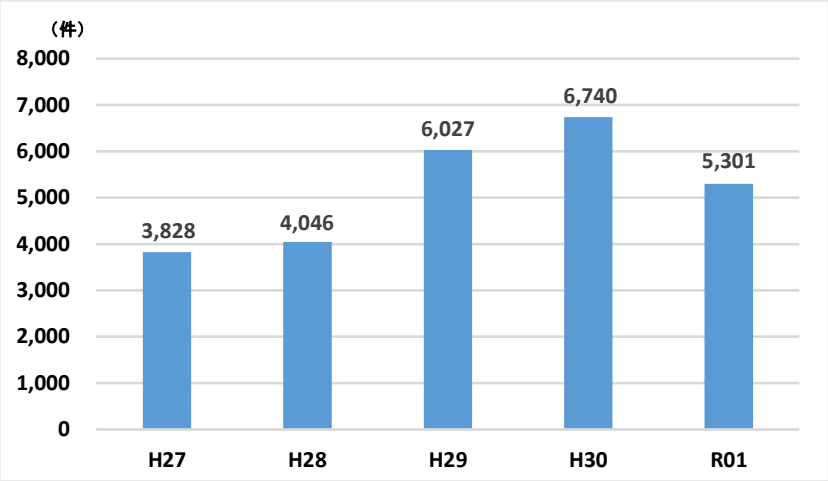
*5　職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータ等から閲覧・操作などできるサービスであり、テレワーク等で利用されている。

(3)　標的型メール攻撃

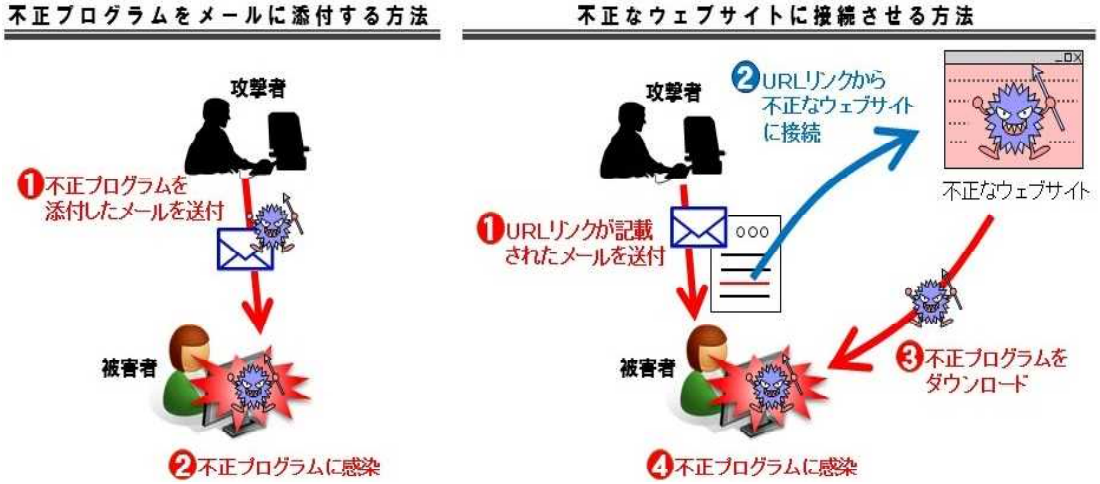
ア　標的型メール攻撃の件数の推移

令和元年中のサイバーインテリジェンス情報共有ネットワーク[*6] を通じて把握した標的型メール攻撃[*7] の件数は5,301件であった。

【図表４　標的型メール攻撃の件数の推移】



【図表５　不正プログラムに感染させる手口の例】



イ　標的型メール攻撃の特徴

○　「ばらまき型」攻撃[*8] の多発傾向が継続

---

*6　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。

*7　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。

「ばらまき型」攻撃が多数発生し、全体の90%を占め、引き続き高い割合となった。

○　多数が非公開メールアドレスに対する攻撃

標的型メールの送信先メールアドレスについては、インターネット上で公開されていないものが全体の82%を占めた。

○　多くの攻撃において送信元メールアドレスを偽装

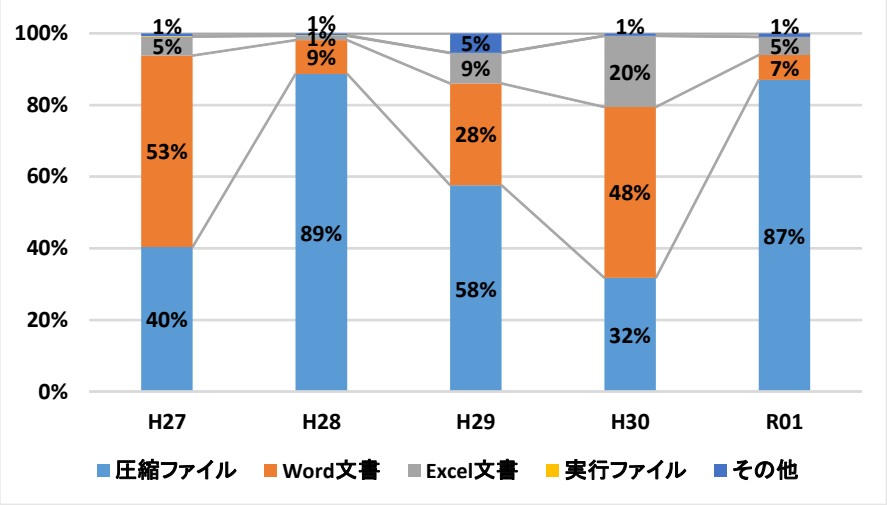
標的型メールの送信元メールアドレスについては、偽装されていると考えられるものが全体の92%を占めた。

○　標的型メールに添付されたファイル

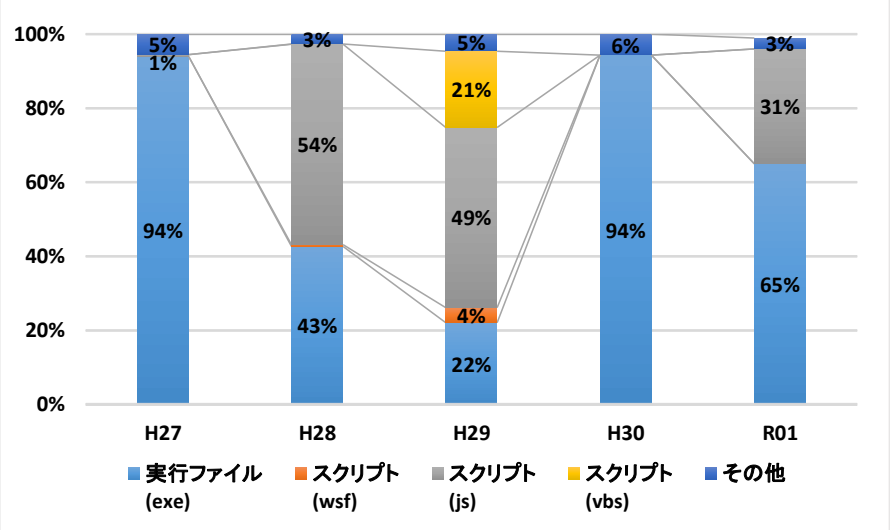
標的型メールに添付されたファイルの形式の割合及び標的型メールに添付されたファイルのうち、圧縮ファイルで送付されたファイルの形式の割合については、それぞれ以下のグラフに示すとおりである。

標的型メール攻撃の手法は日々変化しているとみられるため、引き続きその動向を注視しながら対策を講じる必要がある。

【図表６　標的型メールに添付されたファイルの形式の割合の推移】



【図表７　圧縮ファイルで送付されたファイル形式の割合の推移】



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には以下のようなものがあった。

・　安全衛生委員会への招待と称して、添付された圧縮ファイルを開くよう誘導するメールが、事業者の非公開メールアドレスに対して送信された。

・　「賞与支払届」という件名で、メール本文内のリンク先に接続するよう誘導するメールが、事業者の非公開メールアドレスに対して送信された。

【図表８　事業者に実際に送信された標的型メール】

(4)　取組

ア　サイバーインテリジェンス情報共有ネットワーク

警察では、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を、サイバーインテリジェンス情報共有ネットワークにより事業者等と共有し、集約された情報を総合的に分析し、事業者等に対し、分析結果に基づく情報提供を実施している。

イ　サイバー攻撃事案で使用されたＣ２サーバ[*9] 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サーバの機能停止（テイクダウン）を、サーバを運営する事業者等に働きかけることで促進している。警察が把握したＣ２サーバを運営する事業者に対し、不正な蔵置ファイルを削除するよう依頼するなどしてＣ２サーバの無害化措置が執られた結果、令和元年中においては16台の機能停止が実施された。

---

*9　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。

ウ　東京大会に向けたサイバー攻撃対策の推進

元年中は、金融・世界経済に関する首脳会合（G20大阪サミット）、ラグビーワールドカップ2019等に伴いサイバー攻撃対策を実施し、いずれも会合、試合等の進行に影響を与える被害の発生はなかった。他方で、過去のサイバー攻撃の発生状況を踏まえると、東京大会において、その妨害や情報窃取等を目的としたサイバー攻撃が発生することが懸念される。

警察では、東京大会に向けて、既存の重要インフラ事業者に加え、大会組織委員会、競技場をはじめとする大会関係施設等の大会関係事業者等と連携して、サイバー攻撃による被害の未然防止に努めている。また、個々の事業者等に対する脅威情報の共有等を通じ、事案発生時における警察との連絡体制を確立し、各事業者のシステムについて必要な助言等を行うなどの管理者対策を推進しているほか、サイバー攻撃事案の発生を想定したシナリオに基づき、各事業者等と共同対処訓練を実施することにより、事態対処能力の強化を図るなどしている。

○　東京大会に向けた対策事例

・　１月、都内の重要インフラ事業者等とサイバー攻撃を想定したインシデント対応共同技術訓練を実施。
・　９月、大会公式パートナー企業とサイバーインシデント対応演習を実施。
・　11月、大会関係事業者等とサイバー攻撃を想定した共同対処訓練を実施。

引き続き、関係機関と連携しつつ、サイバー攻撃対策について詰めの調整・確認を進め、東京大会の安全・円滑な開催に万全を期すための取組を推進する。

2　サイバー犯罪の情勢等

(1)　サイバー犯罪の発生状況

令和元年中のサイバー犯罪の発生状況のうち、特徴的なものは、以下のとおり。

○　インターネットバンキングに係る不正送金事犯

インターネットバンキングに係る不正送金事犯は、平成28年以降、金融機関のセキュリティ対策の強化等により発生件数・被害額ともに減少傾向が続いていたが、９月から急増した。

○　「コード決済」の不正利用事案

「コード決済」サービスに関するアカウントやクレジットカード情報を不正に利用されて、コンビニエンスストア等で商品を大量購入される事案が発生した。

○　「Emotet」の感染事案

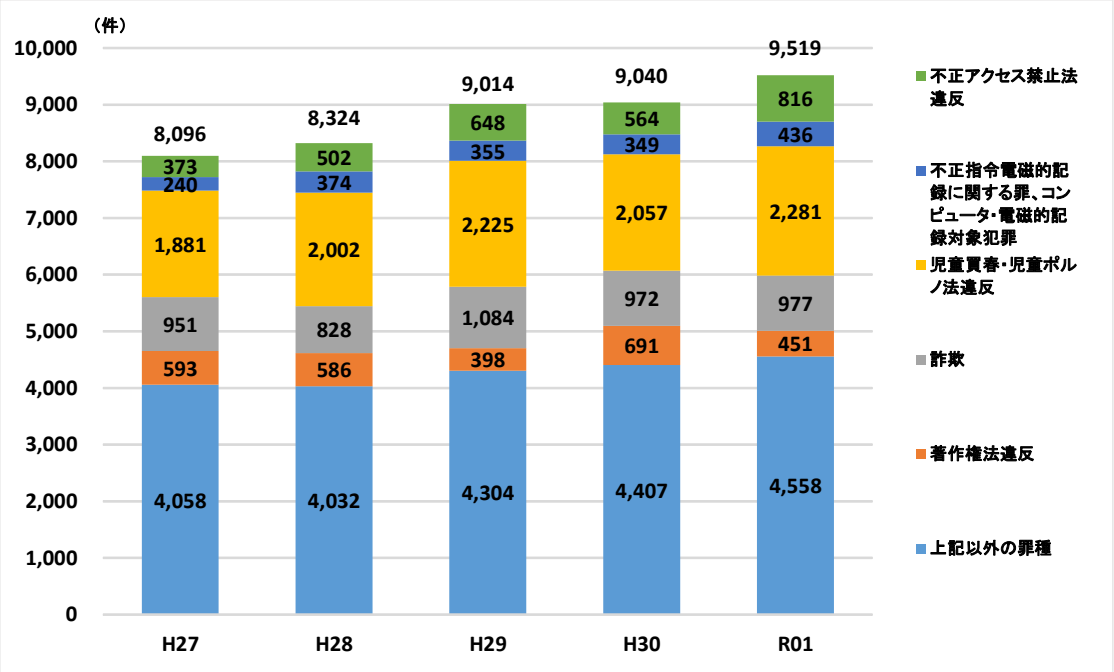
コンピュータの利用者が送受信したメールの宛先、本文等の情報を窃取し、当該情報を基に偽のメールを作成・送信することで感染を拡大するなどの機能を持つ「Emotet」と呼ばれる不正プログラムに感染する事案が発生した。

(2)　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、令和元年中の検挙件数は9,519件と、過去最多となった。

【図表９　サイバー犯罪の検挙件数の推移】

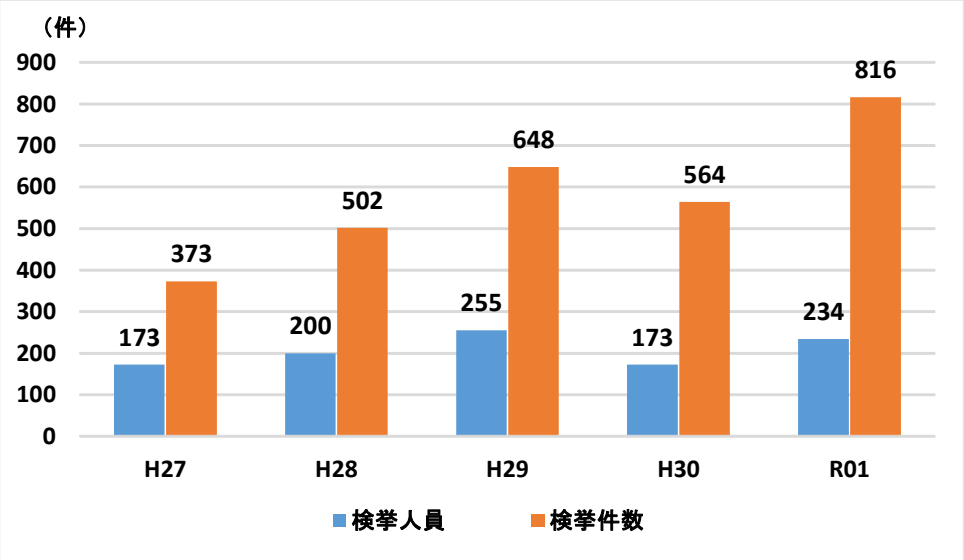


イ　不正アクセス禁止法[*10] 違反

(ｱ)　検挙件数等

○　元年中における不正アクセス禁止法違反の検挙件数は816件と、前年と比べて増加した。検挙件数のうち、785件が識別符号窃用型[*11] で全体の96.2%を占めている。

【図表10　不正アクセス禁止法違反の検挙件数の推移】



○　「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」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、利用権者のパスワードの設定・管理の甘さにつけ込んだものが310件と最も多く、全体の39.5%を占めており、次いで他人から入手したものが182件で全体の23.2%となっている。

○　被疑者が不正に利用したサービスは「オンラインゲーム・コミュニティサイト」が最多

被疑者が不正に利用したサービスは、オンラインゲーム・コミュニティサイトが224件と最も多く、全体の28.5%を占めており、次いで社員・会員用等の専用サイトが151件で全体の19.2%を占めている。

(ｲ)　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

○　概況

元年中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

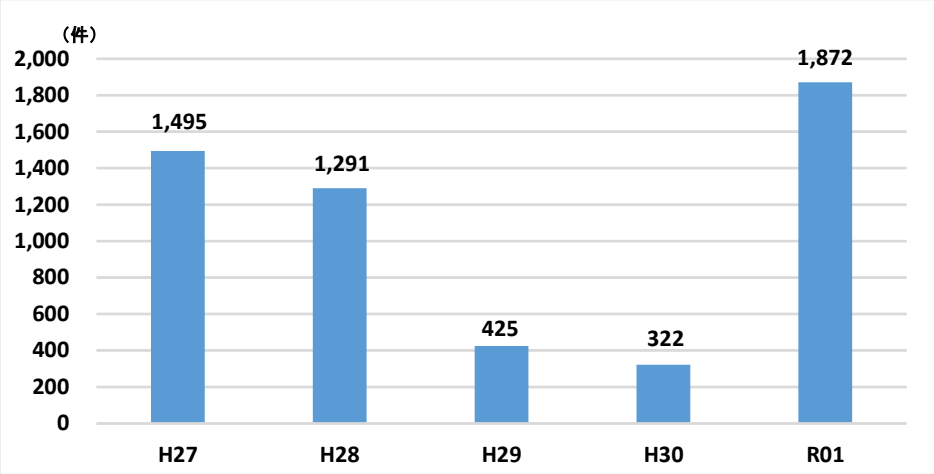
---

*10　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。）

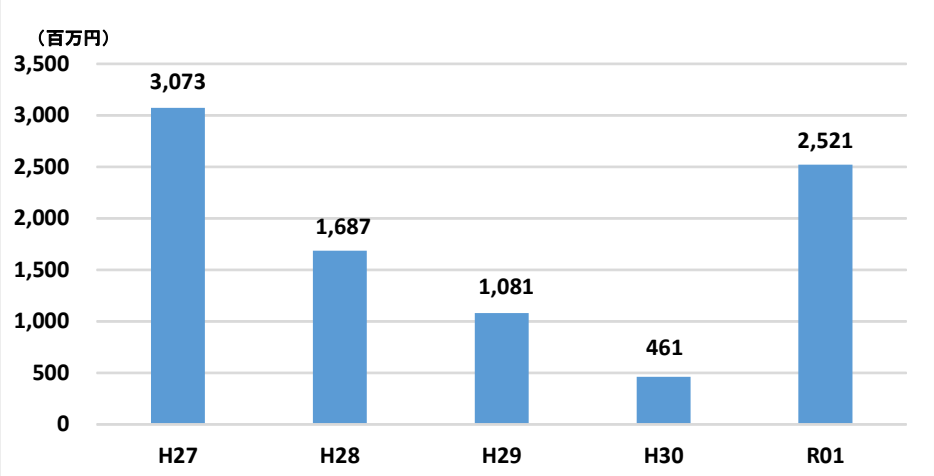
*11　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

る被害は、発生件数1,872件、被害額約25億2,100万円で、発生件数は過去最多であった平成26年に次ぐ件数となり、被害額も前年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】



○　特徴

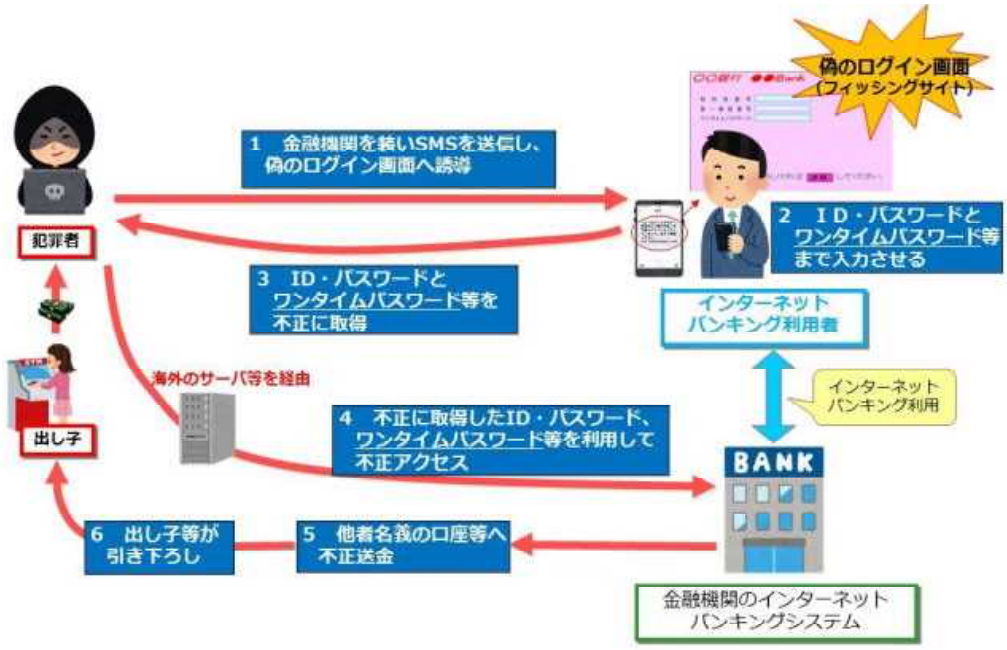
・　上半期は、発生件数、被害額ともに前年同期を下回っていたものの、９月から被害が急増した。被害の多くは、ＳＭＳや電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられる。

・　誘導されたフィッシングサイトで、ＩＤ・パスワード、ワンタイムパスワード等を窃取されて金融機関のウェブサイトから不正送金される被害や、ＩＤ・パスワード等に加えて生年月日、電話番号等の情報を窃取され、金融機関の公式アプリを用いて不正送金される被害などが確認されている。

・　一次送金先として把握した2,399口座のうち、名義人の国籍は日本が58.6％と最も多く、次いでベトナムが13.5％、中国が8.8％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、電子マネーの購入、プリペイド型のバーチャルクレジットカードへのチャージ、大手通信販売サイトの電子ギフト券の購入等の手口が確認されている。

【図表13　ＳＭＳを悪用した不正送金の手口の例】



(ｳ)　仮想通貨[*12] 交換業者等への不正アクセス等による不正送信事犯

元年中における仮想通貨交換業者等への不正アクセス等による不正送信事犯については、認知件数22件、被害額約31億2,860万円相当で、いずれも前年（認知件数169件、被害額約677億3,820万円相当）と比べて大幅に減少した。

ウ　不正指令電磁的記録に関する罪[*13] 及びコンピュータ・電磁的記録対象犯罪[*14]

○　検挙件数

元年中における不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数は436件で、前年と比べて増加した。

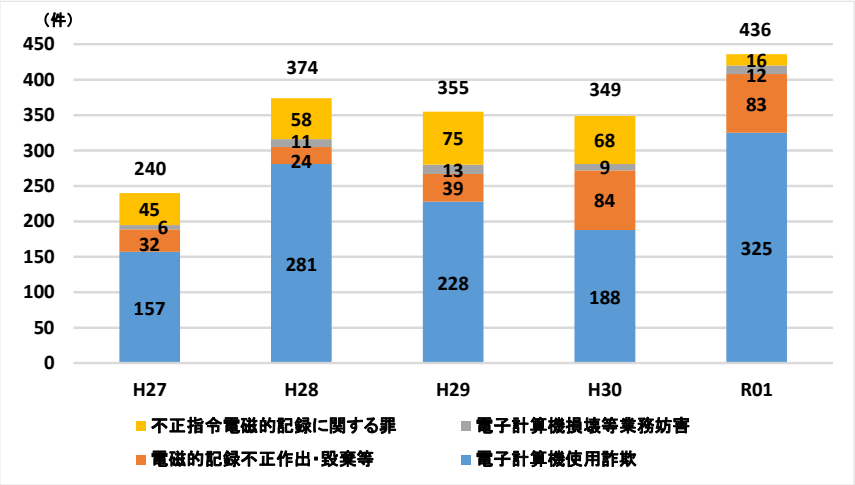
---

*12　令和元年（2019年）、第198回国会において、「仮想通貨」の呼称の「暗号資産」への変更等を内容とする情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律が成立した。

*13　刑法第168条の２第１項（不正指令電磁的記録作成、提供）、同法第168条の２第２項（不正指令電磁的記録供用）、同法第168条の３（不正指令電磁的記録取得、保管）

*14　刑法第161条の２第１項（私電磁的記録不正作出）、同法第161条の２第２項（公電磁的記録不正作出）、同法第163条の２第１項（支払用カード電磁的記録不正作出）、同法第234条の２（電子計算機損壊等業務妨害（電子計算機を物理的に損壊し業務を妨害した事犯を除く。））、同法第246条の２（電子計算機使用詐欺）、同法第258条（公用電磁的記録毀棄）、同法第259条（私用電磁的記録毀棄）

【図表14　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数の推移】



○　特徴

検挙件数のうち、電子計算機使用詐欺が325件と最も多く、全体の74.5％を占めている。

エ　その他

○　児童買春・児童ポルノ法違反の検挙件数は2,281件と、前年と比べて増加した。

○　詐欺の検挙件数は977件と、前年と同水準であった。

○　著作権法違反の検挙件数は451件と、前年と比べて減少した。

(3)　取組

○　インターネットバンキングに係る不正送金被害防止対策

インターネットバンキングの不正送金被害の急増を受けて、10月、ＪＣ３と連携し、警察庁及びＪＣ３のウェブサイトで、注意喚起を実施した。

また、全国銀行協会と手口や被害状況等に関する情報共有を行うとともに、12月、同協会と連携し、それぞれのウェブサイトにおいて、被害防止の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[*15]等に提供し、被害防止対策を実施している。

○　クレジットカード情報窃取被害防止対策

ショッピングサイト等を改ざんし、クレジットカード情報を窃取する手口が明らかになったことから、ＪＣ３と連携し、サイトの運営者や利用者に対して、注意喚起を実施した。

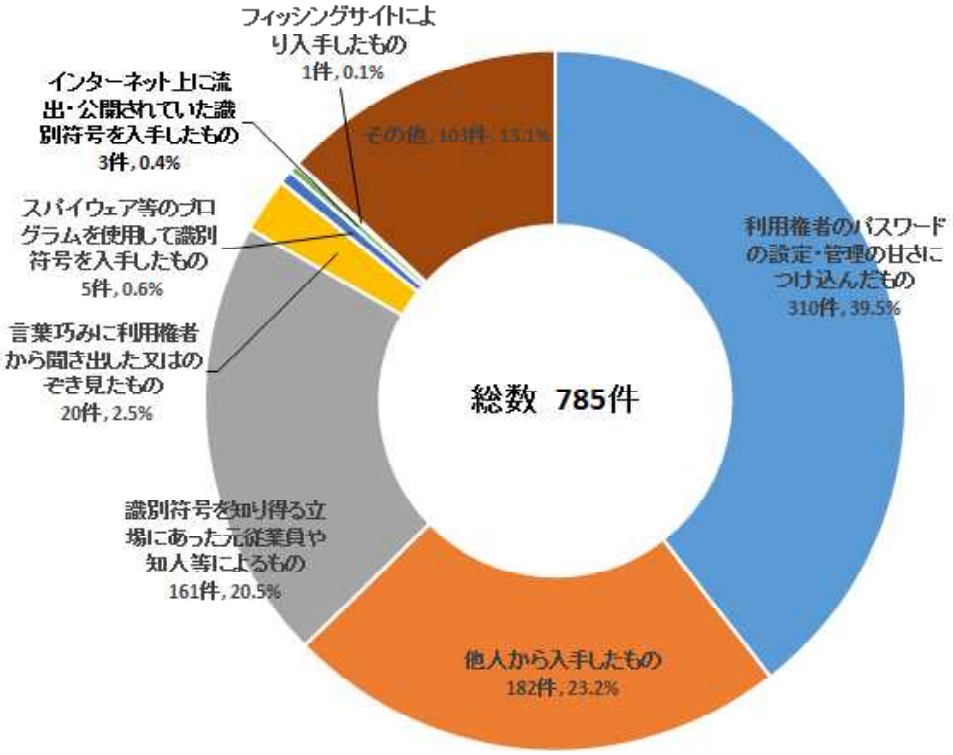
---

*15　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。

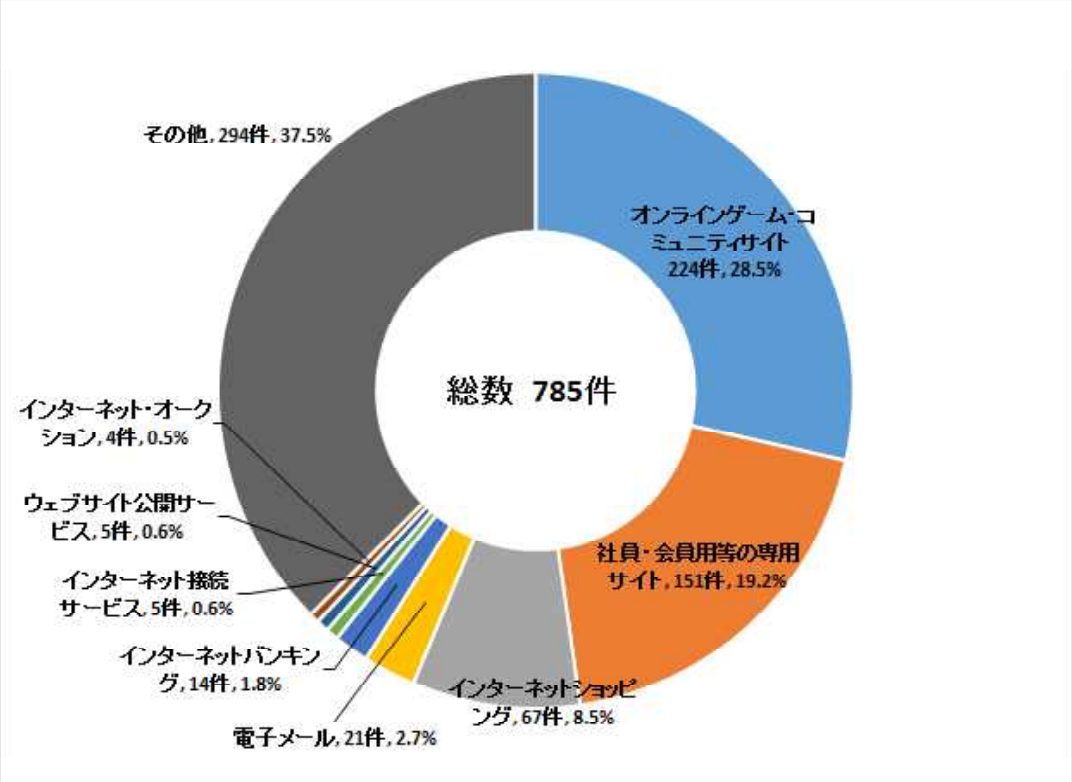
【　参考　】

1　不正アクセス禁止法違反の検挙状況等

(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）



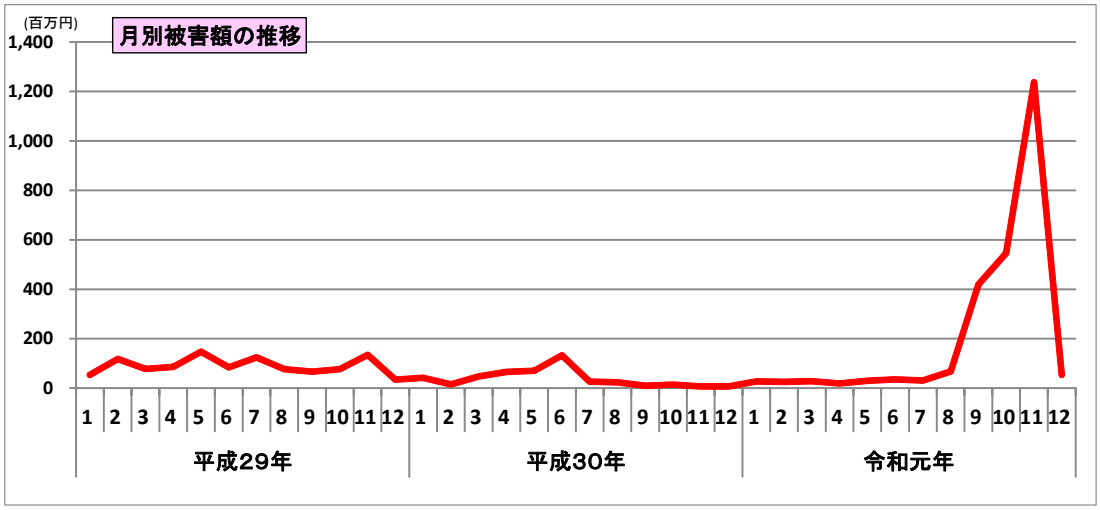
不正アクセス禁止法違反

○　公務員の男（50）は、平成29年１月から平成31年２月までの間、勤務先のサーバに対して、勤務先の職員のＩＤ・パスワードを無断で使用して不正アクセスし、データを不正に入手した。令和元年９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。（長崎）

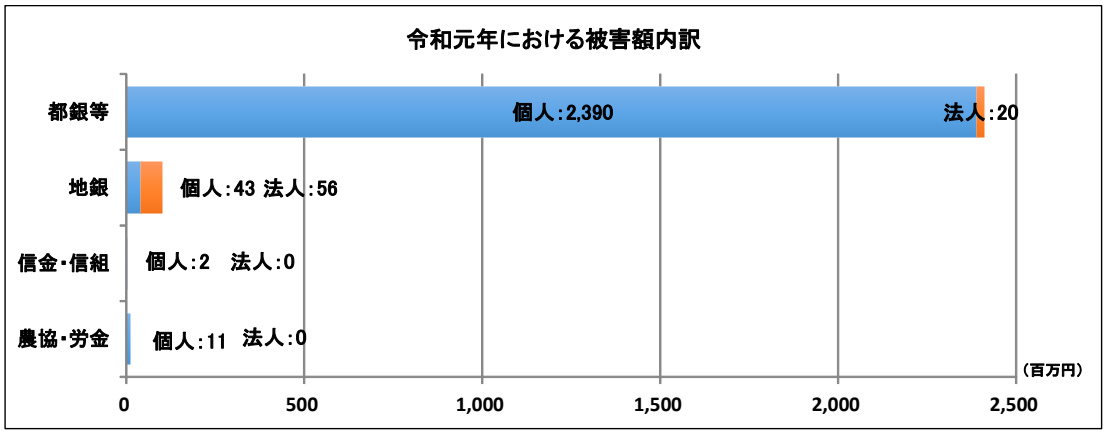
○　中国国籍の男（29）は、令和元年７月、不正に取得したＩＤ・パスワードを使用してコード決済システムに不正アクセスし、コンビニエンスストアにおいて、持っていたスマートフォンに表示した他人がユーザー登録した同システムのバーコード画面を提示し、電子タバコカートリッジを詐取した。令和元年10月、男を不正アクセス禁止法違反（不正アクセス行為）及び詐欺で検挙した。（熊本）

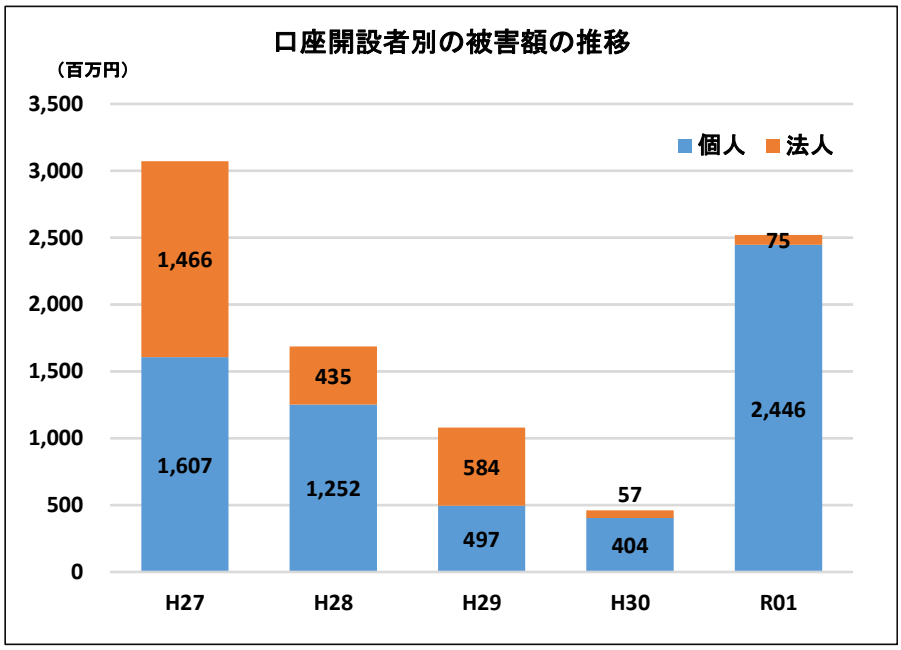
2　インターネットバンキングに係る不正送金事犯の発生状況等

(1) 発生状況の推移

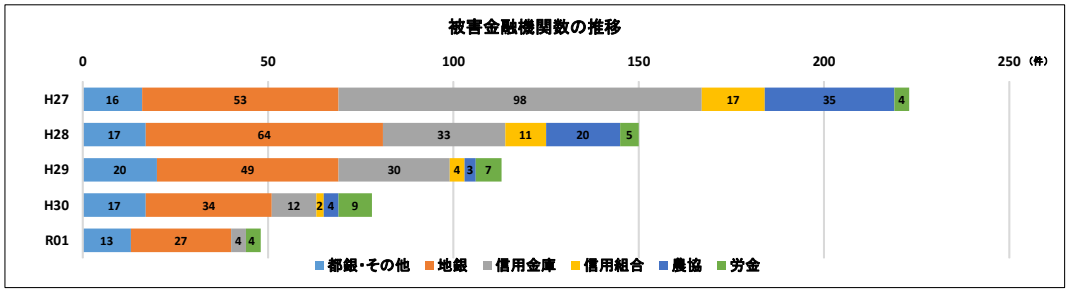


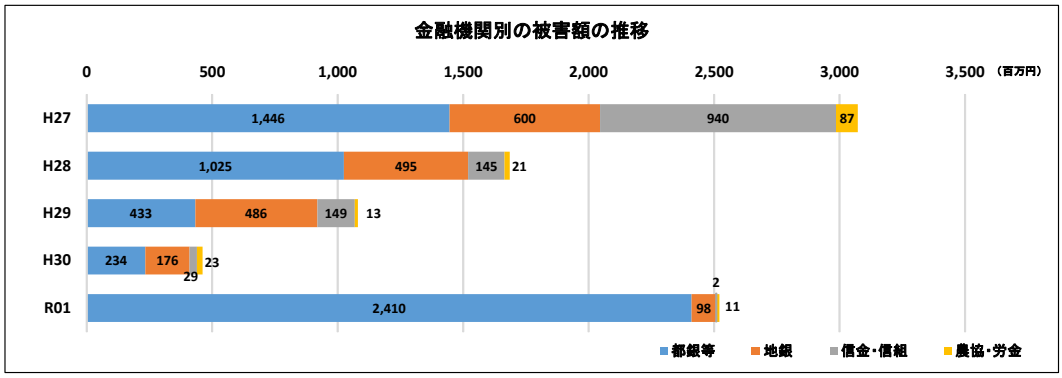
(2) 被害額内訳





(3) 金融機関別の被害状況

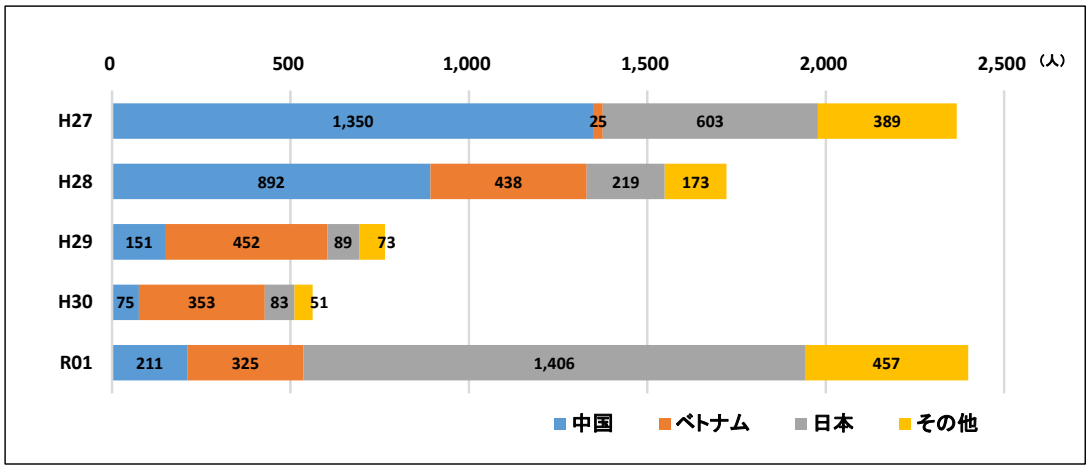




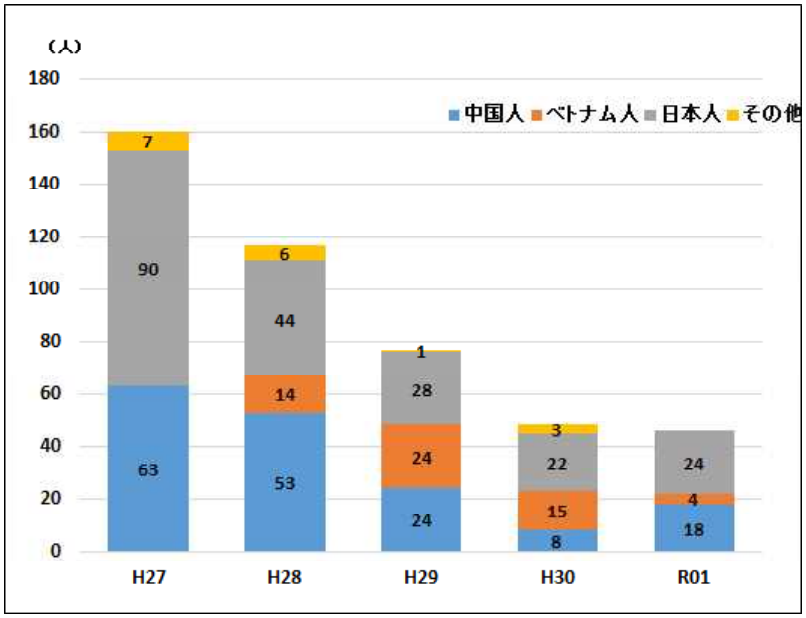
(4) 口座開設者別の被害状況

口座開設者		令和元年				
		都市銀行等	地方銀行	信金・信組	農協・労金	合計
個人	被害額	約23億9,000万円 (94.8%)	約4,300万円 (1.7%)	約200万円 (0.1%)	約1,100万円 (0.4%)	約24億4,600万円 (97.0%)
	実被害額	約21億4,900万円 (95.2%)	約4,000万円 (1.8%)	約200万円 (0.1%)	約1,100万円 (0.5%)	約22億200万円 (97.5%)
法人	被害額	約2,000万円 (0.8%)	約5,600万円 (2.2%)	0円 (0.0%)	0円 (0.0%)	約7,500万円 (3.0%)
	実被害額	約800万円 (0.3%)	約4,900万円 (2.2%)	0円 (0.0%)	0円 (0.0%)	約5,700万円 (2.5%)
合計	被害額	約24億1,000万円 (95.6%)	約9,800万円 (3.9%)	約200万円 (0.1%)	約1,100万円 (0.4%)	約25億2,100万円 (100.0%)
	実被害額	約21億5,700万円 (95.5%)	約8,900万円 (3.9%)	約200万円 (0.1%)	約1,100万円 (0.5%)	約22億5,900万円 (100.0%)

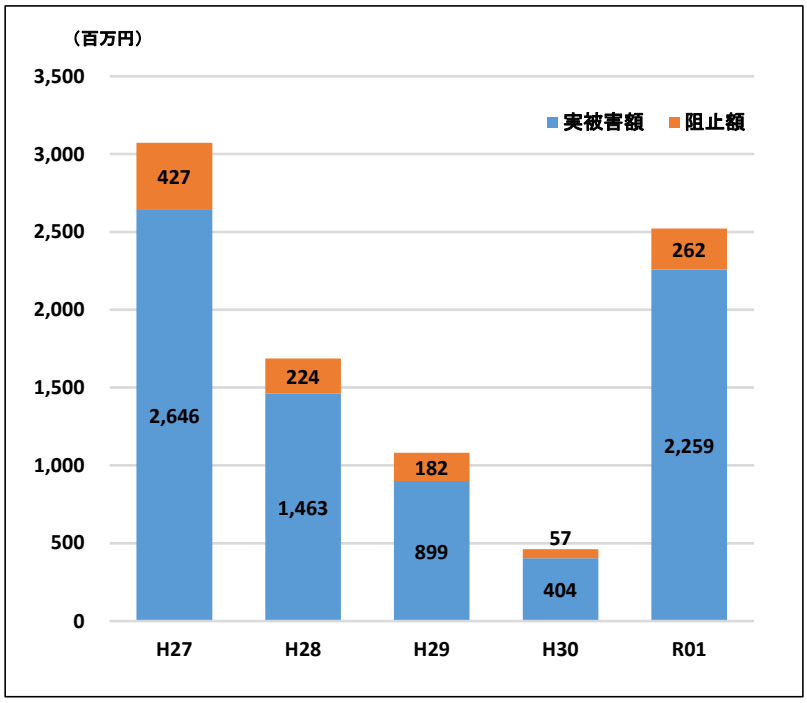
(5) 一次送金先口座名義人の国籍



(6) 国籍別の関連事件検挙状況



(7) 不正送金阻止状況



(8) 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）	1032	55.7%	182	9.8%	638	34.4%	1,852
電子証明書（法人口座）	5	25.0%	10	50.0%	5	25.0%	20

３　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙状況

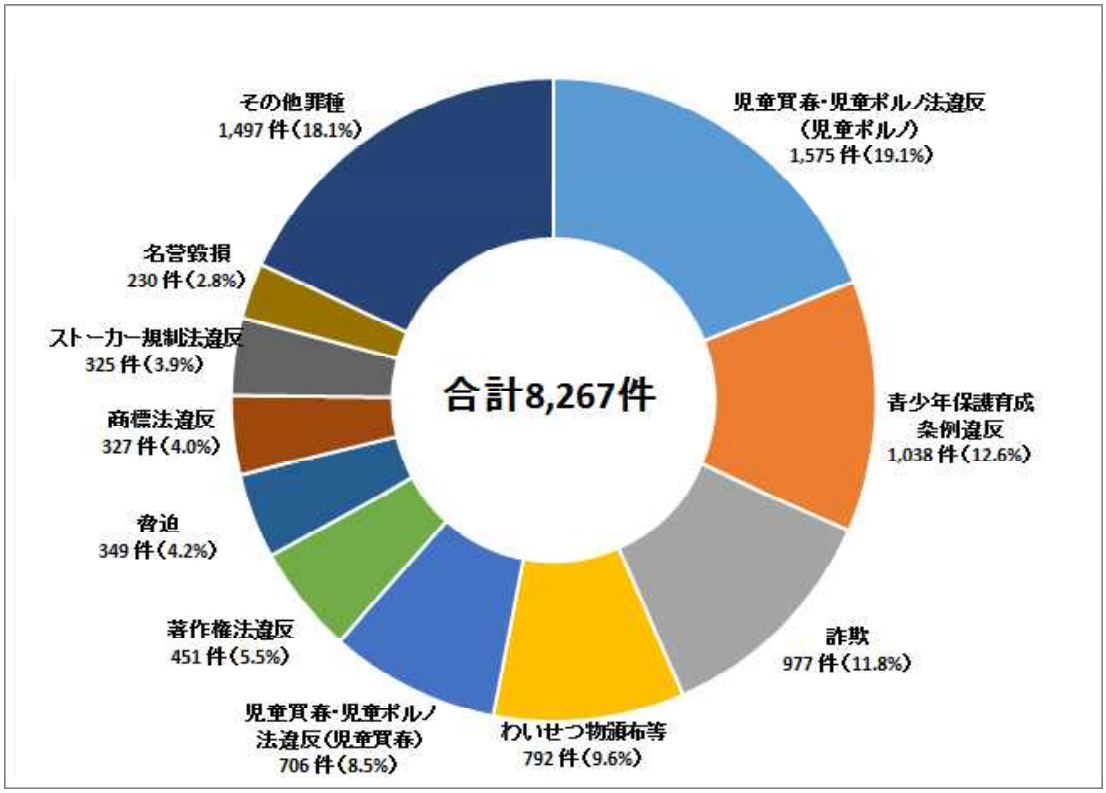
	H27	H28	H29	H30	R01
電子計算機使用詐欺	157	281	228	188	325
電磁的記録不正作出･毀棄等	32	24	39	84	83
電子計算機損壊等業務妨害	6	11	13	9	12
不正指令電磁的記録供用	21	36	24	37	6
不正指令電磁的記録取得･保管	16	18	22	19	6
不正指令電磁的記録作成･提供	8	4	29	12	4
合計	240	374	355	349	436

コンピュータ・電磁的記録対象犯罪

○　無職の男（28）は、平成31年３月から同年４月までの間、SNSで知り合った女性の携帯電話のキャリア決済を無断で自己のアカウントに係る支払方法に設定して、デジタルコンテンツを購入した。令和元年10月、男を私電磁的記録不正作出・同供用で検挙した。（鹿児島）

○　無職の男（31）は、令和元年８月、当時勤務していたインターネット通信販売会社において、注文情報を並び替えるプログラムを改変して動作不能にさせ、商品発送等の業務を妨害した。令和元年10月、男を電子計算機損壊等業務妨害で検挙した。（香川）

４　その他



詐欺

○　会社員の女（29）は、平成31年３月、コンビニエンスストアにおいて、他人名義のクレジットカード情報が登録されたスマートフォンを使用し、加熱式タバコカートリッジを詐取した。令和元年11月、女を詐欺等で検挙した。（警視庁）

有印公文書偽造・同行使、詐欺

○　アルバイトの男（25）らは、平成30年４月、偽造した自動車運転免許証を使用して携帯電話の契約を行い、携帯電話を詐取した。平成31年１月から同年２月までの間、男らを有印公文書偽造・同行使、詐欺で検挙した。（滋賀）

著作権法違反

○　無職の男（27）らは、平成29年２月から平成30年２月までの間、設置場所不詳のサーバコンピュータに、著作物である漫画の画像データを記録保存し、インターネットを利用する不特定多数の者に自動的に公衆送信できる状態にして、海賊版サイトを運営し、著作権者等の著作権等を侵害した。令和元年７月から10月までの間、男らを著作権法違反で検挙した。

　また、当該男については、同年12月、組織的犯罪処罰法違反（犯罪収益等の隠匿）で検挙した。（福岡、警視庁、栃木、鳥取、熊本、大分）