広　報　資　料
平成31年３月７日
警　　察　　庁

# 平成30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

### (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2,752.8件と増加傾向。

○　仮想通貨等を標的としたアクセスを、年間を通じて観測。

### (2)　サイバー攻撃の情勢及び取組

○　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把握した標的型メール攻撃は、6,740件と増加傾向。

○　上記枠組みにおいて、集約された情報等を総合的に分析し、事業者等に対し、分析結果に基づく情報提供を実施。

## ２　サイバー犯罪の情勢等

### (1)　サイバー犯罪の検挙状況等

サイバー犯罪の検挙件数は増加傾向にあり、30年中の検挙件数は9,040件と過去最多。また、相談件数は12万6,815件。

#### ア　不正アクセス禁止法違反

○　検挙件数は564件と、過去５年では29年に次ぐ水準。

○　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は、認知件数169件、被害額約677億3,820万円相当。

#### 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349件。このうち、不正指令電磁的記録に関する罪の検挙件数は68件と、過去５年では29年に次ぐ水準。

#### ウ　その他

児童買春・児童ポルノ法違反の検挙件数は2,057件と、全体を通じて最も多く、過去５年では29年に次ぐ水準。

### (2)　主な取組

ＩＤの不正取得対策として、一般財団法人日本サイバー犯罪対策センター（ＪＣ３）等と連携した取締りとともに、ＩＤの発行事業者等に対する申入れを実施。

## ３　今後の取組

「警察におけるサイバーセキュリティ戦略」に基づく各種取組の推進

○　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

○　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

別　添

# 平成30年におけるサイバー空間をめぐる脅威の情勢等

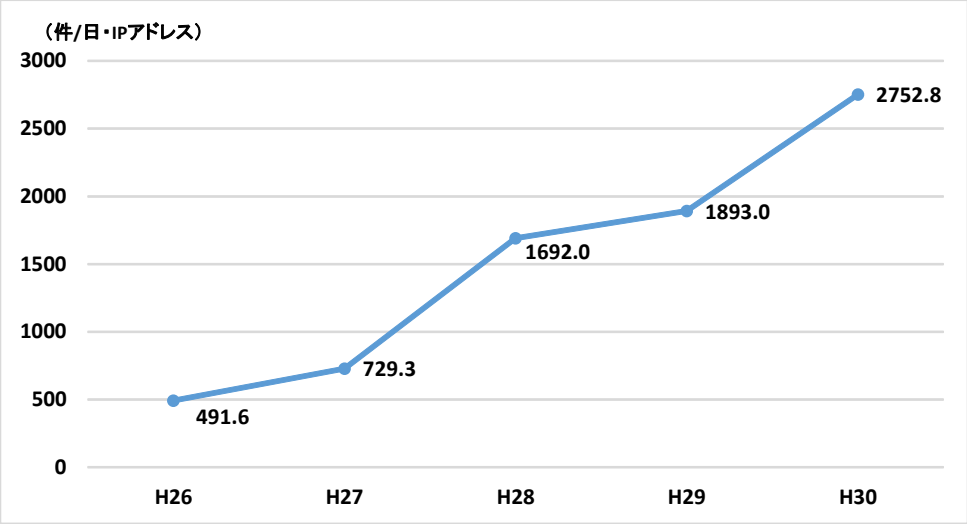
## 1　サイバー攻撃の情勢等

### (1)　サイバー空間における探索行為等

ア　センサー*1 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2,752.8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

○　宛先ポート*2 1024以上に対するアクセスの増加

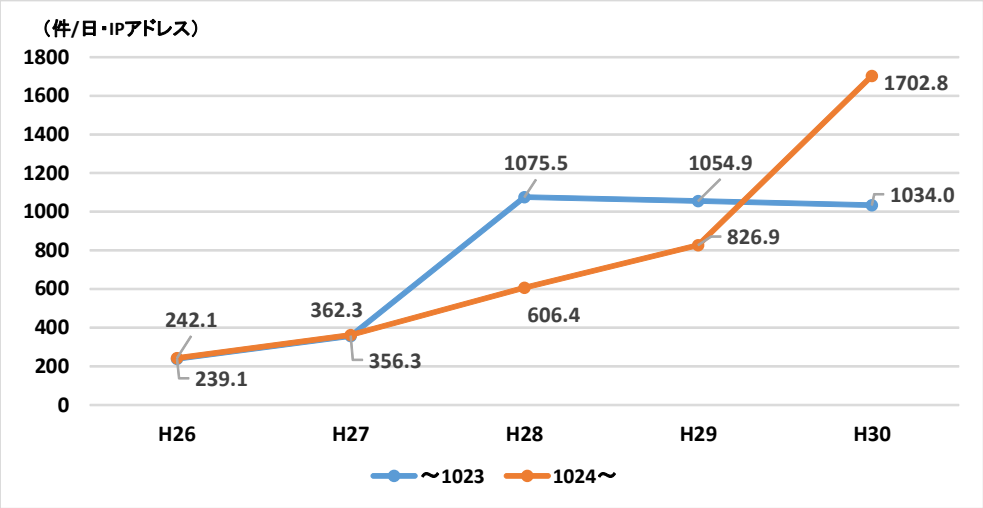
検知したアクセスの宛先ポートに着目すると、メールの送受信やウェブサイトの閲覧等一般に広く利用されるポート（1023以下のポート）に対するアクセスについては、平成28年から減少傾向に転じている一方、それ以外のポート（1024以上のポート）に対するアクセスは増加傾向にあり、30年においては、１日・１IPアドレス当たり1702.8件と、前年の約２倍となった。この増加の主な要因としては、特定の発信元からの広範なポートに対する探索行為が30年下半期に急増したことが挙げられる。

---

*1　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。

*2　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。

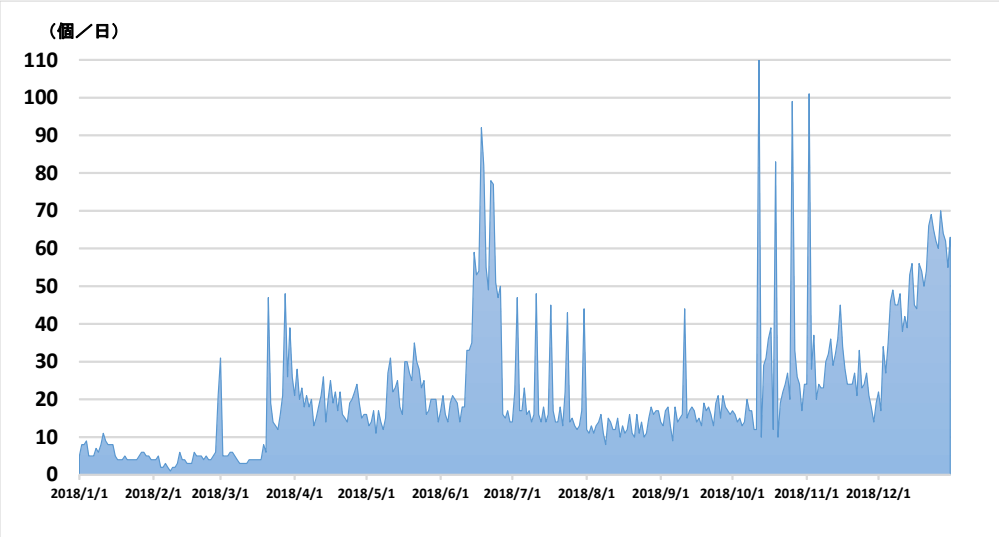
【図表２　検知したアクセスの宛先ポートで比較した１日・１IPアドレス当たり件数の推移】




○　仮想通貨のネットワーク等を標的としたアクセスの観測

仮想通貨「Ethereum（イーサリアム）」のネットワークを標的としているとみられる宛先ポート8545/TCPに対するアクセス等、仮想通貨及び仮想通貨採掘ソフトウェアを標的としたアクセスを年間を通じて観測した。

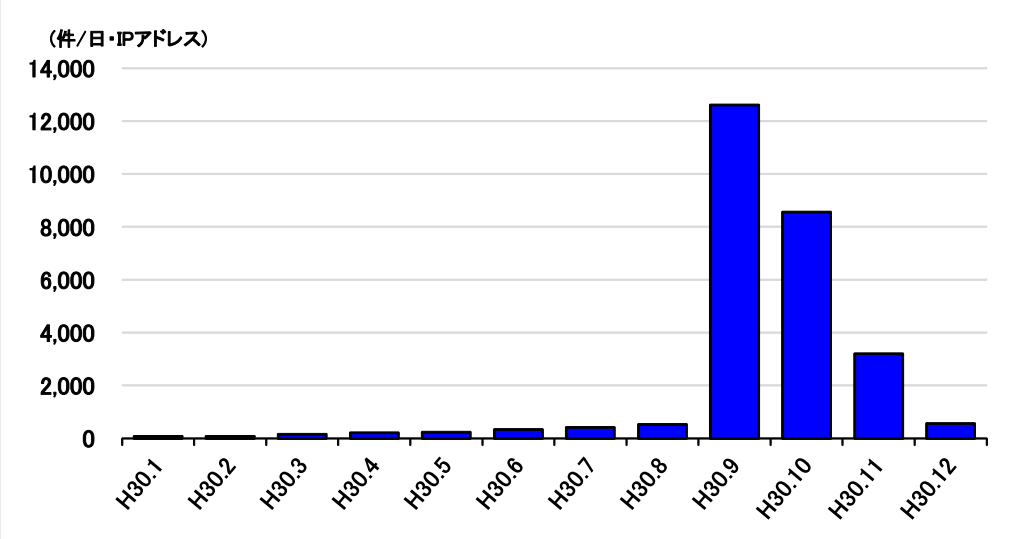
【図表３　仮想通貨「Ethereum」のネットワークを標的としているとみられる宛先ポート8545/TCPに対するアクセスの発信元IPアドレス数の推移】




○　SYN/ACKリフレクター攻撃の観測

30年９月以降、ウェブサイトの表示に用いられる宛先ポート80/TCPに対するアクセスの急増を観測した。このアクセスは、ウェブサイトの閲覧等に必要となる通信の仕組みを悪用し、攻撃対象の機器等の処理能力を超えるアクセスを集中させ、それらのサービス提供を不可能にするDoS攻撃の一種である「SYN/ACKリフレクター攻撃」を狙ったものと考えられる。

【図表４　宛先ポート80/TCPに対するアクセス件数の推移】



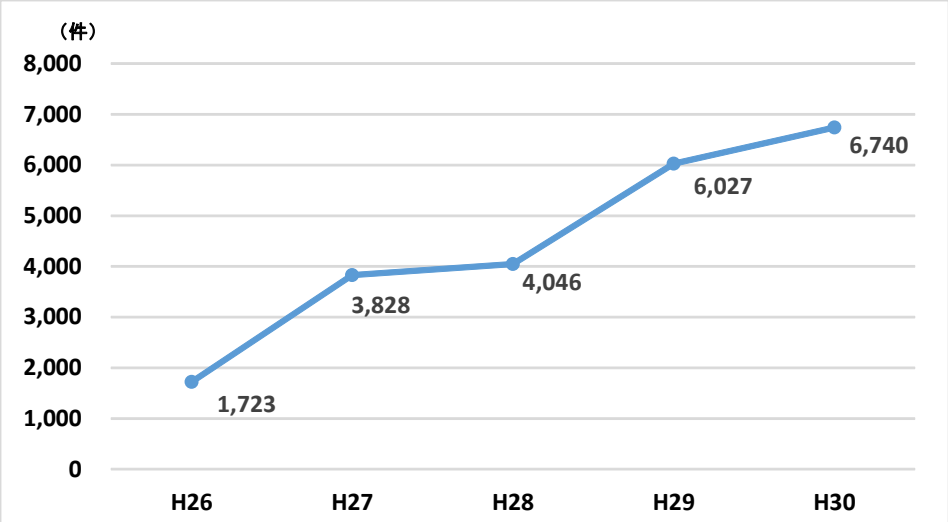

## (2)　サイバー攻撃の情勢及び取組

### ア　情勢

#### (ｱ)　概況

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[*3] により事業者等と共有しているところ、同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6,740件と近年増加傾向にある。

【図表５　標的型メール攻撃の件数の推移】



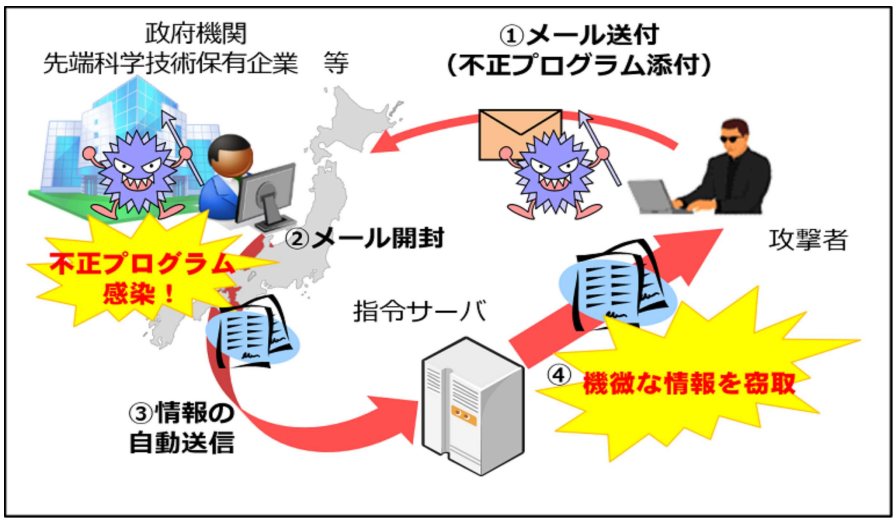

*3　警察と先端技術を有する全国7,777の事業者等（31年１月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組み。内閣サイバーセキュリティセンター（NISC）と連携し、政府機関に対する標的型メール攻撃の分析結果についても情報を共有している。

また、29年に引き続き、我が国の行政機関、公共交通機関、博物館等のウェブサイトに閲覧障害が生じる事案が発生した。

警察では、国際的ハッカー集団「アノニマス」を名乗る者が、21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。

(ｲ)　標的型メール攻撃の手口等

【図表６　標的型メール攻撃の概要】




○　「ばらまき型」攻撃[*4] の多発傾向が継続

「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。

【図表７　ばらまき型とそれ以外の標的型メール攻撃の割合】

| | ばらまき型 | ばらまき型以外 |
|---|---|---|
| H26 | 86%（1,474件） | 14%（249件） |
| H27 | 92%（3,508件） | 8%（320件） |
| H28 | 90%（3,641件） | 10%（405件） |
| H29 | 97%（5,846件） | 3%（181件） |
| H30 | 90%（6,040件） | 10%（700件） |

○　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71％を占めた。

---

*4　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」としているところ、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標的型メール攻撃を「ばらまき型」として集計している。

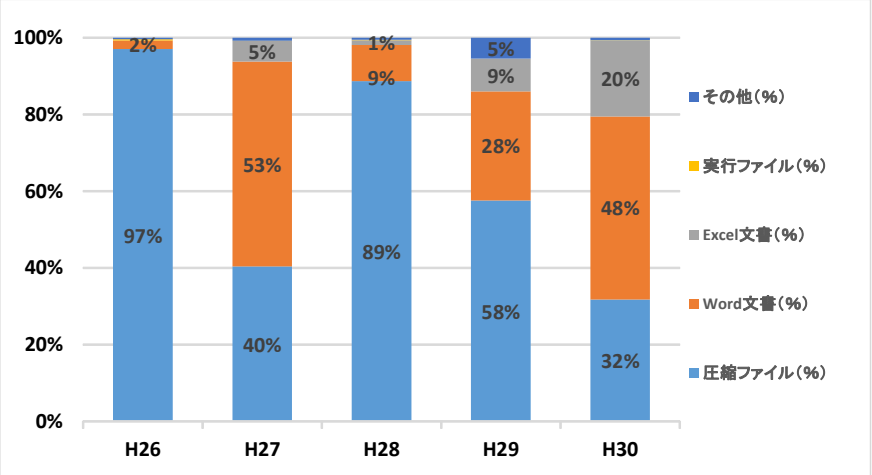
○　多くの攻撃において送信元メールアドレスを偽装

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98%を占めた。

○　標的型メールに添付されたファイルの形式の割合の変化

標的型メールに添付されたファイルの形式の割合については、引き続き、圧縮ファイル、Word文書及びExcel文書が多数を占める中、Word文書及びExcel文書の占める割合が増加した。これらの中には、マクロ機能を悪用したものや、ぜい弱性を狙ったものが確認された。

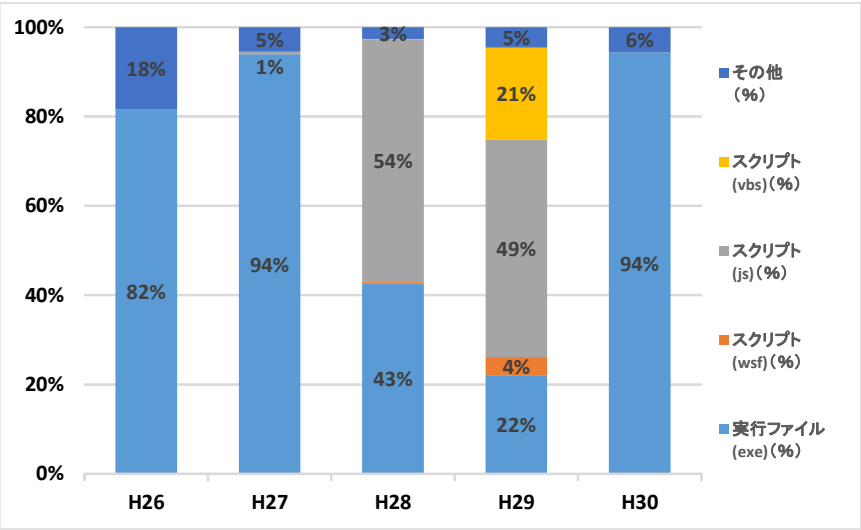
【図表８　標的型メールに添付されたファイルの形式の割合】




○　圧縮ファイルで送付されたファイルの形式の変化

圧縮ファイルで送付されたファイルの形式については、28年から高い割合を占めていたスクリプトファイル[*5]が確認されず、実行ファイルが高い割合を占めた。

【図表９　圧縮ファイルで送付されたファイル形式の推移】




*5　簡易的なプログラミング言語（スクリプト）で記述されたファイルのこと。不正な実行ファイルをダウンロードさせるために使用される場合がある。

イ　取組

(ｱ)　サイバー攻撃事案で使用されたC2サーバ[*6] 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おり、30年中においては12台の機能停止が実施された。

(ｲ)　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攻撃対策の推進

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。）に向けたサイバー攻撃対策として、サイバー攻撃の発生を想定した関係機関等との共同対処訓練、過去の大会開催国における関係機関等との情報交換等の取組を推進した。

【参考】東京大会に向けた共同対処訓練の事例

30年10月、東京大会の開催期間中に、大会の基幹システム、大会関係施設の設備、電力や鉄道の重要インフラに係る基幹システムに対するサイバー攻撃、各事業者に対する標的型メール攻撃やWebサイトへの攻撃等が発生する事態を想定した共同対処訓練を実施した。（警察庁、警視庁、茨城県、埼玉県、千葉県及び神奈川県）

*6　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。

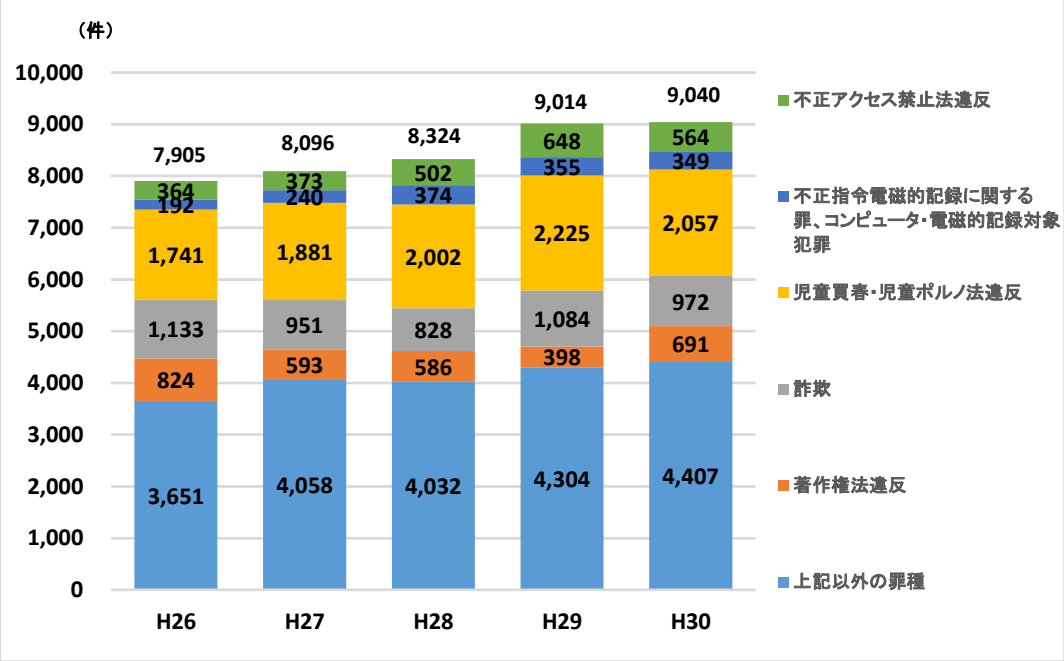
## 2　サイバー犯罪の情勢等

### (1)　サイバー犯罪の検挙状況等

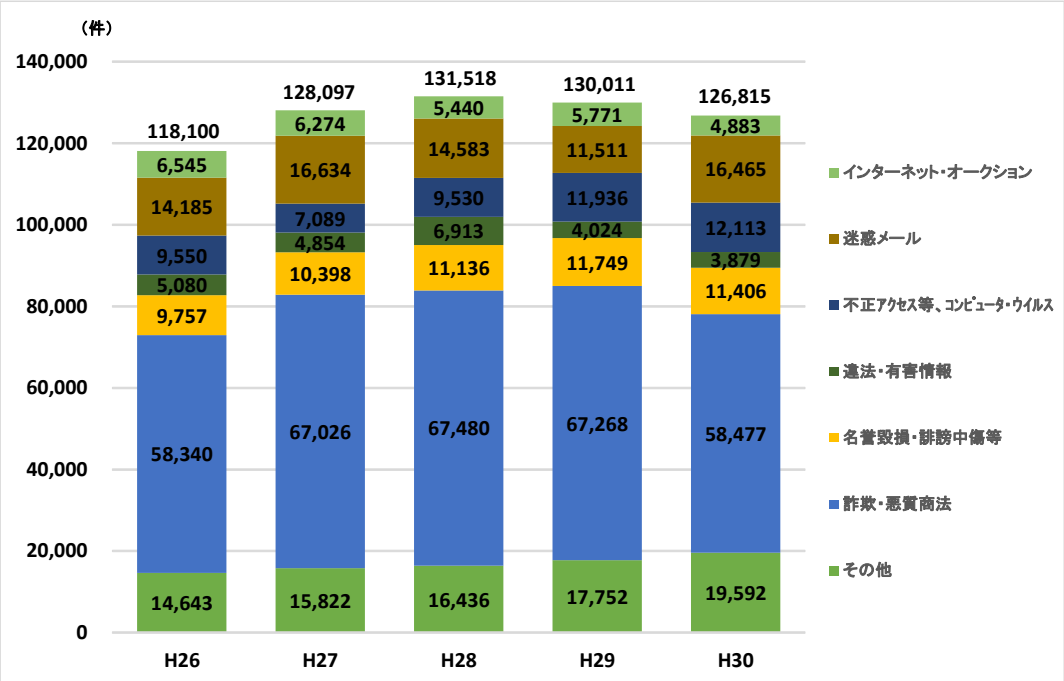
ア　サイバー犯罪の検挙件数及びサイバー犯罪に関する相談件数

サイバー犯罪の検挙件数は増加傾向にあり、30年中の検挙件数は9,040件と過去最多となった。また、相談件数は12万6,815件と、過去最多を記録した28年から減少傾向にある。

【図表10　サイバー犯罪の検挙件数の推移】




【図表11　サイバー犯罪に関する相談件数の推移】

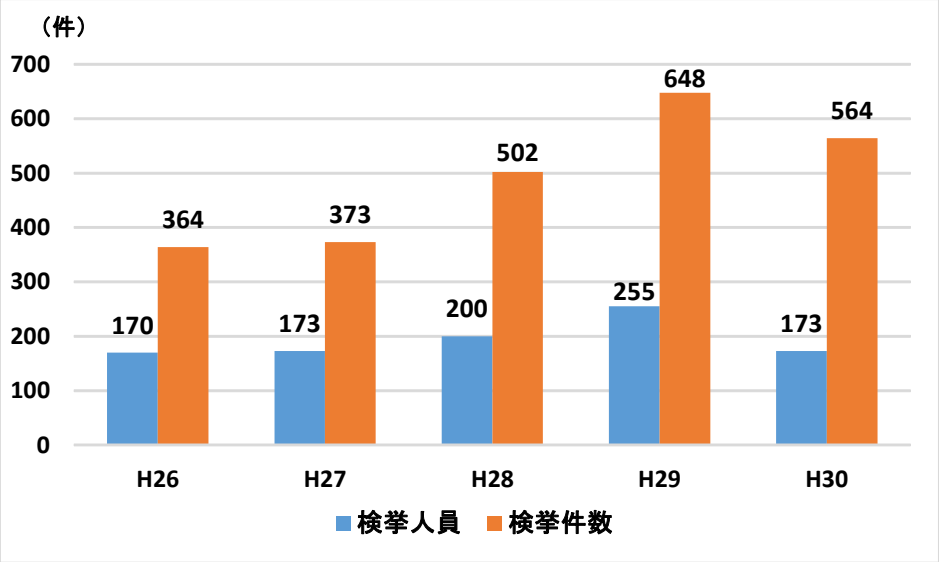


イ　不正アクセス禁止法[*7] 違反

(ｱ)　検挙件数等

○　30年中の不正アクセス禁止法違反の検挙件数は564件と、29年と比べ84件減少するも、過去５年では29年に次ぐ水準となった。検挙件数のうち、502件が識別符号窃用型[*8] で最多となっている。また、検挙人員は173人と昨年より82人減少した。

【図表12　不正アクセス禁止法違反の検挙状況の推移】




○　「パスワード設定・管理の甘さにつけ込む手口」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278件と最も多く、約55％を占めている。

○　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217件と最も多く、約43％を占めている。

○　幅広い年齢層の被疑者等

不正アクセス禁止法違反で補導又は検挙された者は、11歳から66歳まで幅広い年齢層にわたっている。

---

*7　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。）

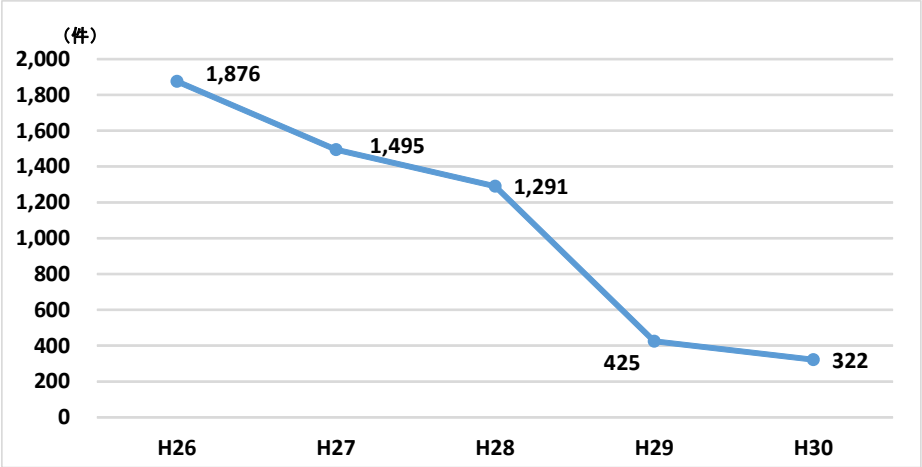
*8　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

(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

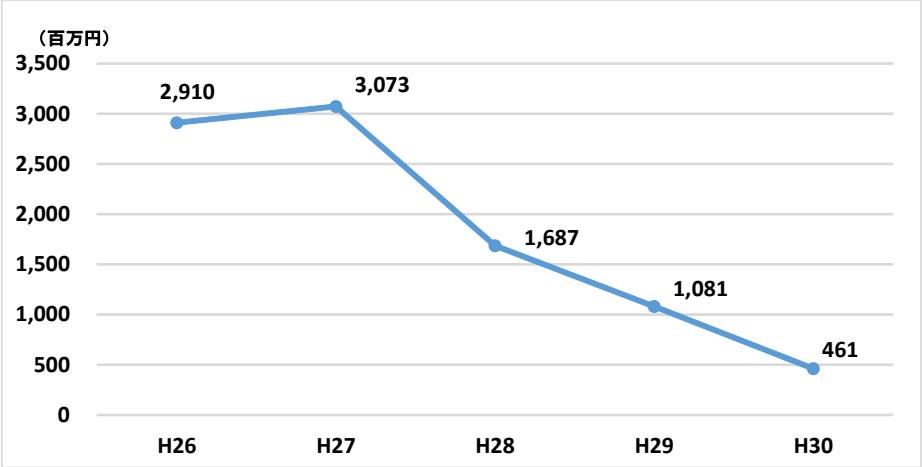
○　概況

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322件、被害額約４億6,100万円で、いずれも減少傾向にある。

【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発生件数の推移】




【図表14　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

・　法人口座の被害が大きく減少

モニタリング[*9]の強化、ワンタイムパスワードの導入等の対策により、29年と比較して、地方銀行・信用金庫等の法人口座の被害が大きく減少した。

・　不正送金先口座はベトナム人名義のものが約６割

不正送金の一次送金先として把握した562口座のうち、名義人の国籍はベトナムが約62.8％を占め、次いで日本が約14.8％、中国が約13.3％であった。

---

*9　不正送金に使用されたＩＰアドレス等に対する監視

(ｳ)　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

○　概況

・　認知件数は169件、被害額は約677億3,820万円相当で、29年（認知件数149件、被害額６億6,240万円相当）と比較して、認知件数は20件、被害額は約670億7,580万円相当上回った。

・　主な被害として、国内の仮想通貨交換業者から、昨年１月に約580億円相当、９月に約70億円相当の仮想通貨が不正に送信されたとみられる事案が発生した。

○　特徴

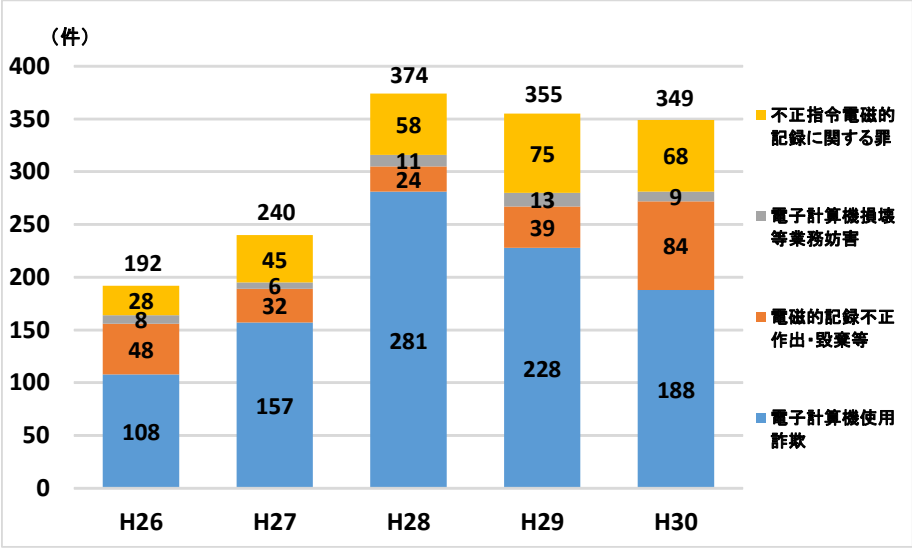
・　認知した169件のうち108件（63.9%）の利用者は、ＩＤ・パスワードを他のインターネット上のサービスと同一にしていた。

ウ　不正指令電磁的記録に関する罪[*10]及びコンピュータ・電磁的記録対象犯罪[*11]

○　検挙件数

30年中の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349件で、過去５年でみると28年から減少傾向にある。

【図表15　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】




*10　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）

*11　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）

○　不正指令電磁的記録に関する罪

・　30年中の不正指令電磁的記録に関する罪の検挙件数は68件で、29年と比べ７件減少するも、過去５年では29年に次ぐ水準となった。検挙件数のうち不正指令電磁的記録供用の検挙件数が37件と、29年と比べ13件増加した。

・　手口としては、サイトに接続したパソコンに不当な料金請求画面を繰り返し表示させる不正プログラムを使用したものがみられた。

・　不正指令電磁的記録に関する罪で補導又は検挙された者は、10歳から58歳まで幅広い年齢層にわたっている。

エ　その他

○　児童買春・児童ポルノ法違反の検挙件数が2,057件と、全体を通じて最も多く、過去５年でみると29年に次ぐ水準となっている。

○　著作権法違反の検挙件数は691件と、29年と比べて大きく増加しており、過去５年でみると26年に次ぐ水準となっている。

**(2)　取組**

○　インターネットバンキングに係る不正送金の被害防止に直結する情報の提供と被害防止対策強化の要請

金融機関等に対して、モニタリングの強化、ワンタイムパスワードの利用促進、ログイン時の二経路認証[*12]の利用、本人確認の徹底等を働き掛けた。

○　仮想通貨不正送信事犯に係る対策

金融庁及び消費者庁と局長級の３省庁連絡会議を開催し（２月、６月、11月）、仮想通貨交換業者等に対する検査・モニタリング、無登録業者への対応、消費者への注意喚起等について、意見交換を実施した。

○　ＪＣ３等と連携したＩＤの不正取得対策

埼玉県警察は、ＪＣ３等と連携の上、付与されるポイントの販売を目的としたＩＤの不正取得事件に対する取締りを実施するとともに、ＩＤの発行事業者及びＩＤの売買に利用されたインターネットオークション運営事業者の双方に対して対策を申し入れた。

その結果、両事業者において、ＩＤ取得の厳格化やＩＤの出品禁止措置の対策がとられ、ＩＤの売買が減少した。

---

*12　振込データ等をパソコンで作成してスマートフォンで認証を行うなど、２つの経路で取引を成立させる認証方式のこと。仮にパソコンがコンピュータウイルス等に感染して不正な振込操作をされた場合でも、別経路（スマートフォン）での認証が必要となるため、不正利用を防止できる。

○　不正トラベル対策

ＪＣ３からの情報を元に、埼玉県警察等が、不正に入手した他人名義のクレジットカード情報で旅行予約を行う、いわゆる不正トラベルに対する取締りを実施するとともに、旅行業関係事業者へ情報提供を行い、被害防止対策を実施した。

○　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

ＪＣ３は、愛知県警察と共同で開発したツールの活用等により詐欺サイトを発見し、当該詐欺サイトのＵＲＬ情報をＡＰＷＧ[*13] 等に対し提供、ＡＰＷＧを通じて事業者に情報提供し、被害防止対策を実施している。

*13　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　サイバー犯罪に関する相談

| | H26 | H27 | H28 | H29 | H30 |
|---|---|---|---|---|---|
| 詐欺・悪質商法 | 58,340 | 67,026 | 67,480 | 67,268 | 58,477 |
| 名誉毀損・誹謗中傷等 | 9,757 | 10,398 | 11,136 | 11,749 | 11,406 |
| 違法・有害情報 | 5,080 | 4,854 | 6,913 | 4,024 | 3,879 |
| 不正ｱｸｾｽ等、ｺﾝﾋﾟｭｰﾀ・ｳｲﾙｽ | 9,550 | 7,089 | 9,530 | 11,936 | 12,113 |
| 迷惑メール | 14,185 | 16,634 | 14,583 | 11,511 | 16,465 |
| インターネット・オークション | 6,545 | 6,274 | 5,440 | 5,771 | 4,883 |
| その他 | 14,643 | 15,822 | 16,436 | 17,752 | 19,592 |
| 合計 | 118,100 | 128,097 | 131,518 | 130,011 | 126,815 |

不正アクセス等、コンピュータ・ウイルスに関する相談

○　宅配業者を装ったショートメールに記載されていたURLに接続し、表示された画面に個人情報を入力したところ、何者かに不正に利用された。

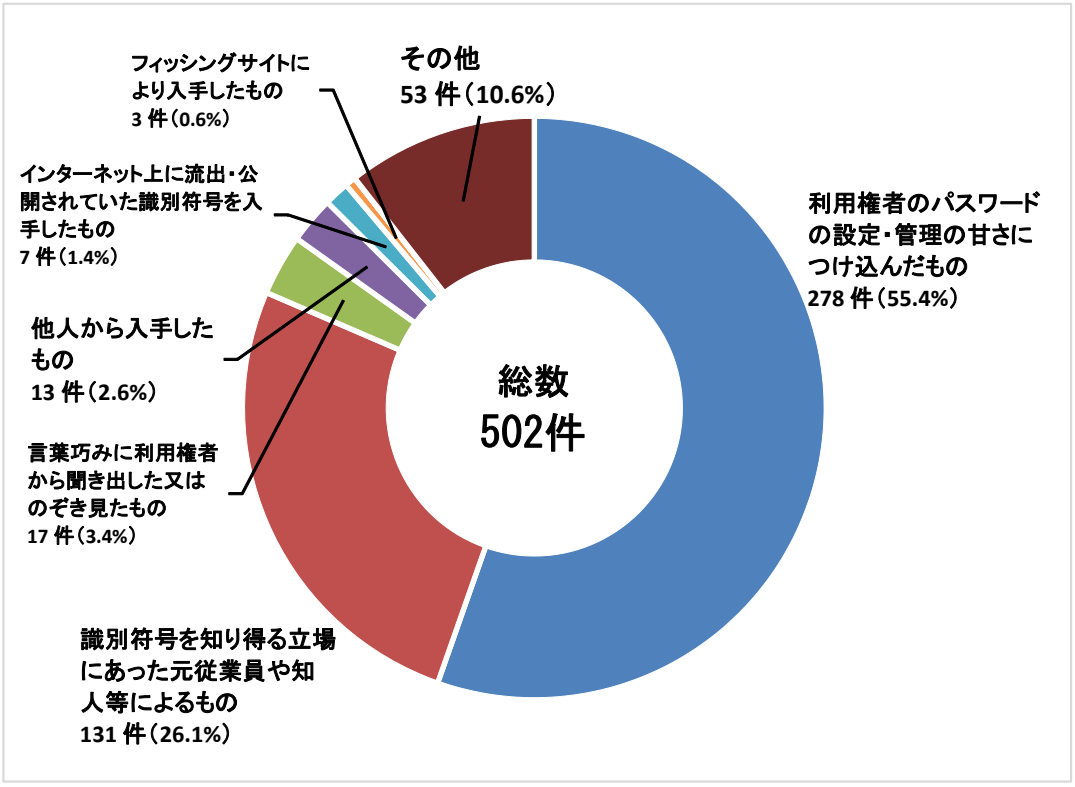
詐欺・悪質商法に関する相談

○　インターネット閲覧中に、身に覚えのないアダルトサイト閲覧等料金未納の画面が表示され、料金を請求された。

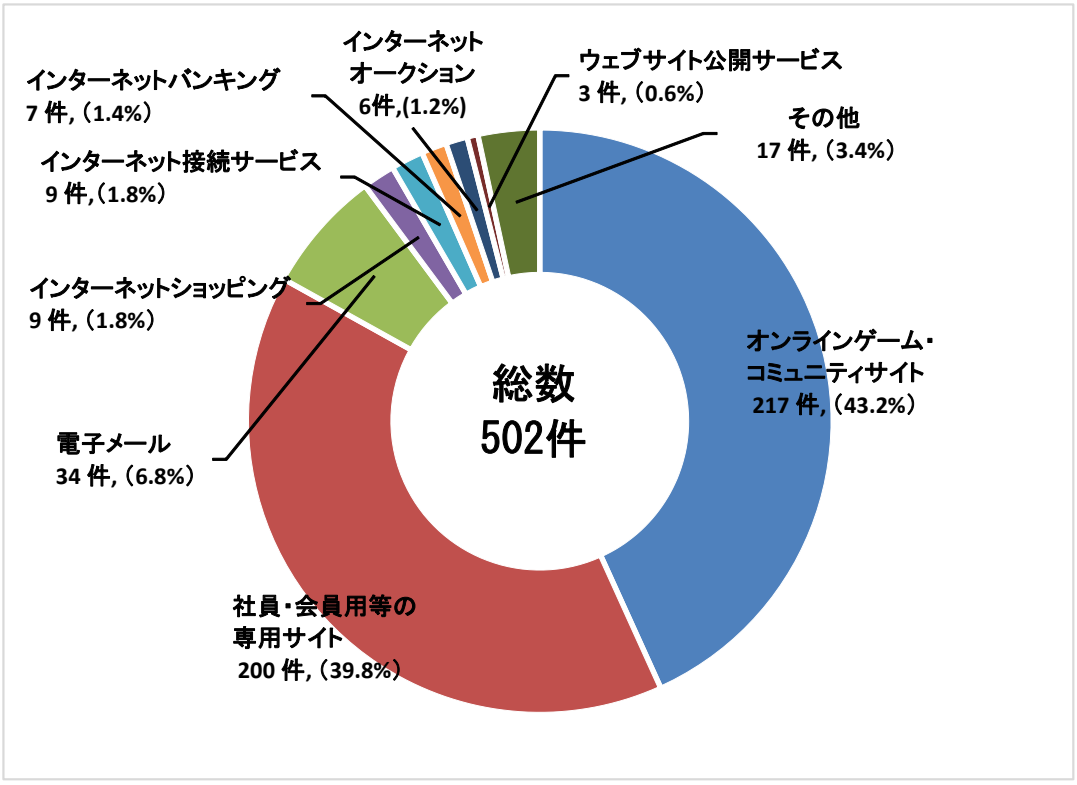
○　インターネットのサイトで商品を購入し、代金を振り込んだが品物が届かない。

## 2　不正アクセス禁止法違反の検挙状況等

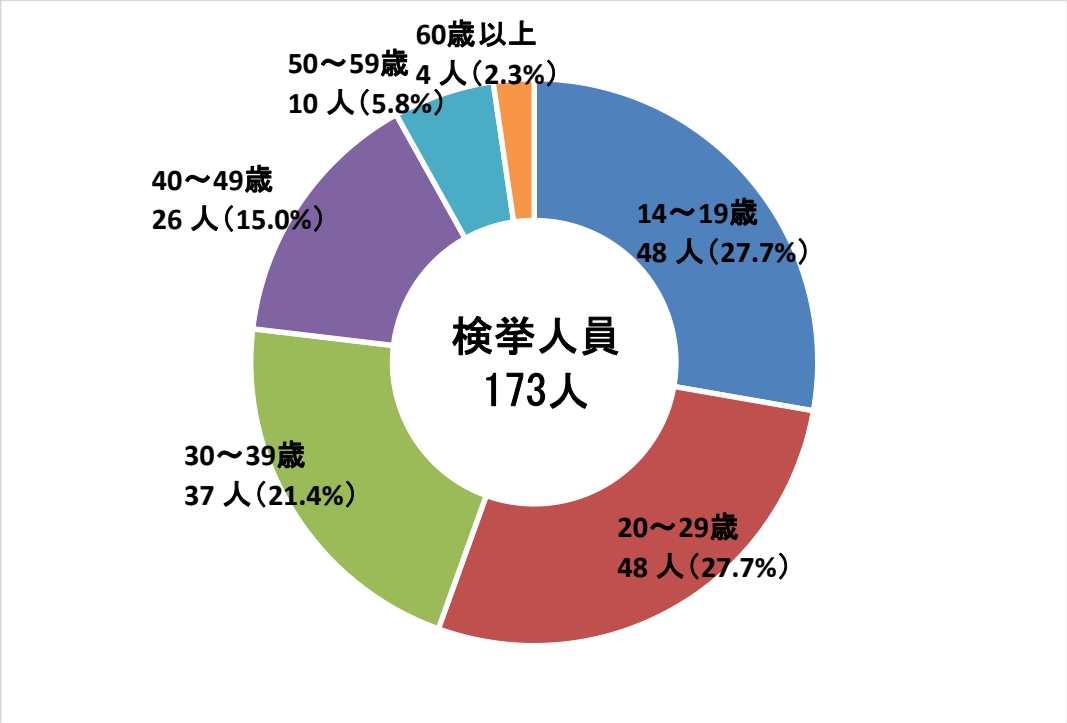
### (1) 不正アクセス行為（識別符号窃用型）に係る手口別検挙件数




### (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）



(3) 年代別被疑者数（触法少年を除く）



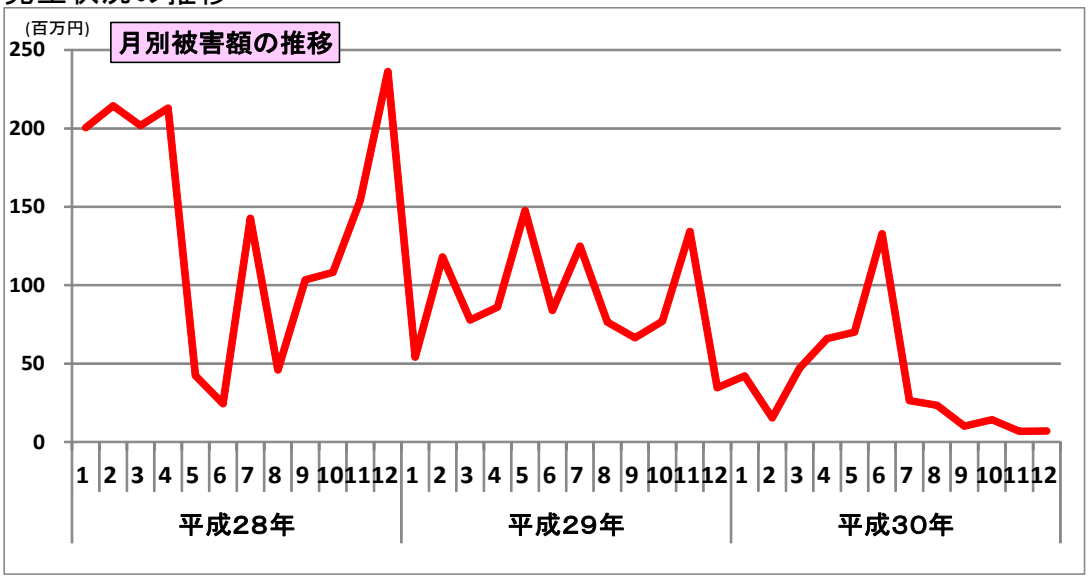

不正アクセス禁止法違反

○　旅館従業員の男（32）は、30年３月、鉄道会社のウェブサイトにサイト管理者のＩＤ・パスワードを使用して不正アクセスし、同サイトのデータを削除して閲覧不能にした。30年10月、男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機損壊等業務妨害で検挙した。（宮崎）

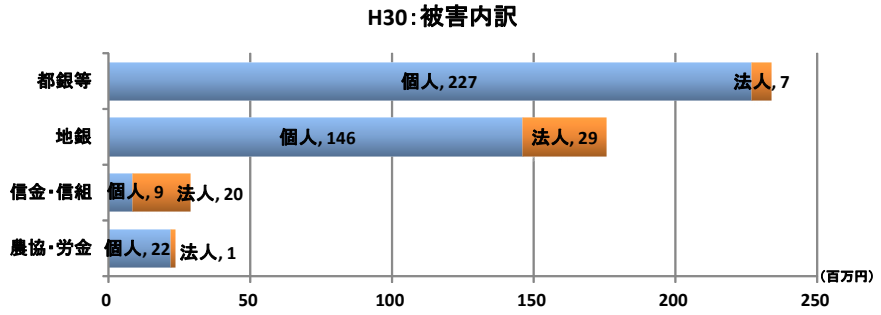
○　会社員の男（39）は、30年５月、他人のＩＤ・パスワードを使用してスマートフォン用オンラインゲームのデータ引継機能に不正アクセスし、他人のゲームデータを乗っ取った。30年11月、男を不正アクセス禁止法違反（不正アクセス行為）、私電磁的記録不正作出・同供用等で検挙した。（福島）

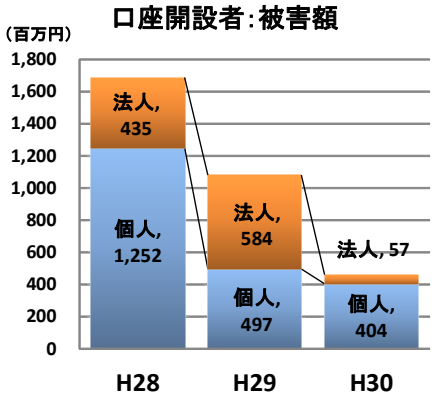
## 3　インターネットバンキングに係る不正送金事犯の発生状況等

### (1) 発生状況の推移

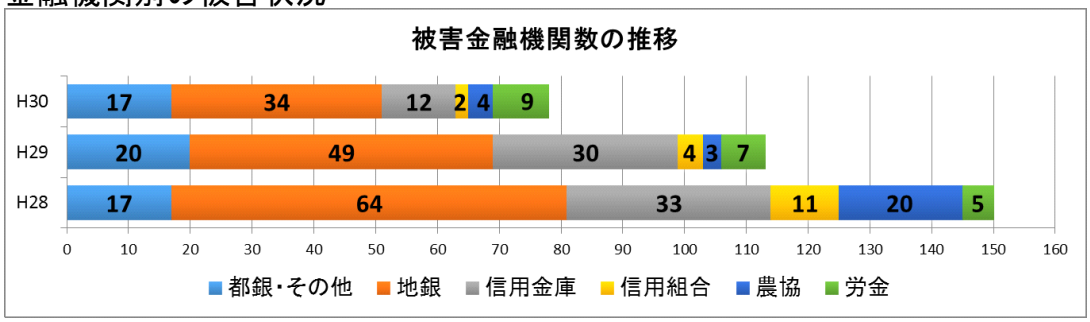


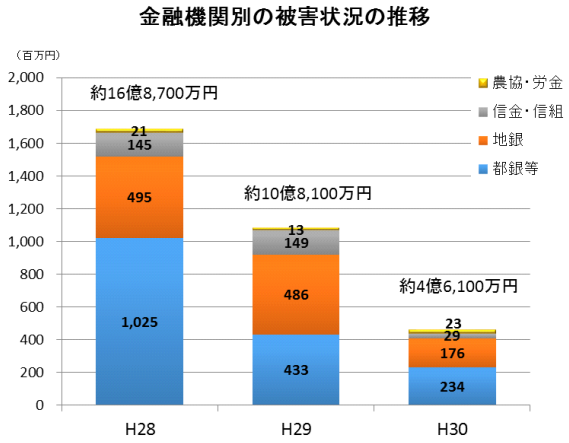

### (2) 被害額内訳



## (3) 金融機関別の被害状況

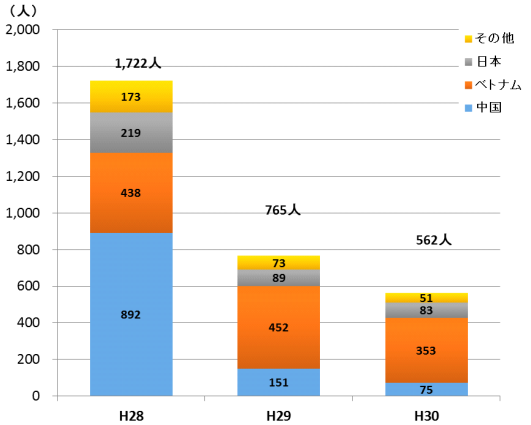


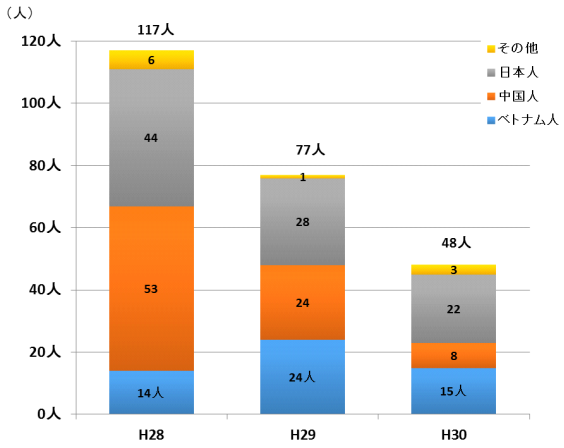

## (4) 口座開設者別の被害状況

| 口座開設者 | | 平成30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2億2，700万円（49．2%） | 約1億4，600万円（31．7%） | 約900万円（1．9%） | 約2，200万円（4．8%） | 約4億400万円（87．6%） |
| | 実被害額 | 約2億200万円（50．0%） | 約1億3，200万円（32．6%） | 約900万円（2．2%） | 約2，100万円（5．2%） | 約3億6，400万円（90．0%） |
| 法人 | 被害額 | 約700万円（1．4%） | 約2，900万円（6．4%） | 約2，000万円（4．3%） | 約100万円（0．3%） | 約5，700万円（12．4%） |
| | 実被害額 | 約400万円（0．9%） | 約1，600万円（4．0%） | 約1，900万円（4．7%） | 約100万円（0．3%） | 約4，000万円（10．0%） |
| 合計 | 被害額 | 約2億3，400万円（50．7%） | 約1億7，600万円（38．1%） | 約2，900万円（6．2%） | 約2，300万円（5．1%） | 約4億6，100万円（100．0%） |
| | 実被害額 | 約2億600万円（50．9%） | 約1億4，800万円（36．7%） | 約2，800万円（6．9%） | 約2，200万円（5．5%） | 約4億400万円（100．0%） |

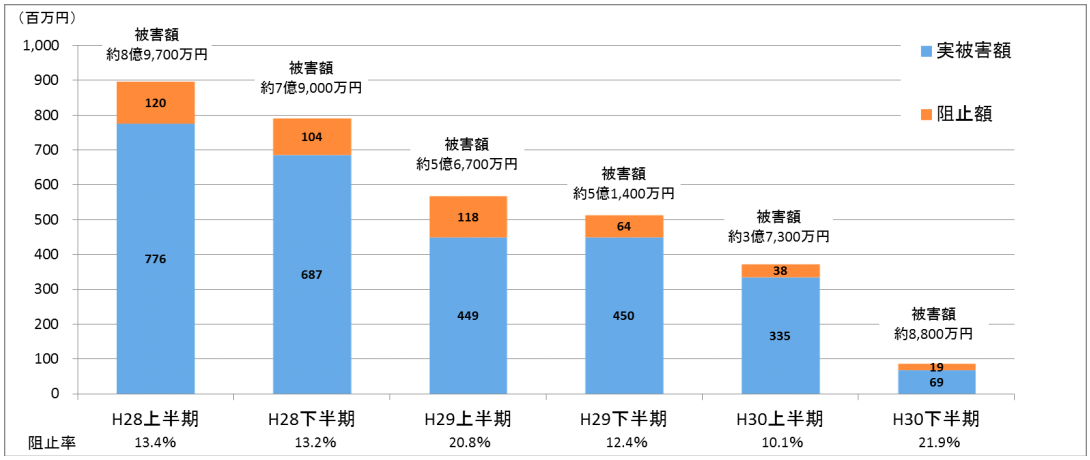
## (5) 一次送金先口座名義人の国籍



## (6) 関連事件の検挙状況




## (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

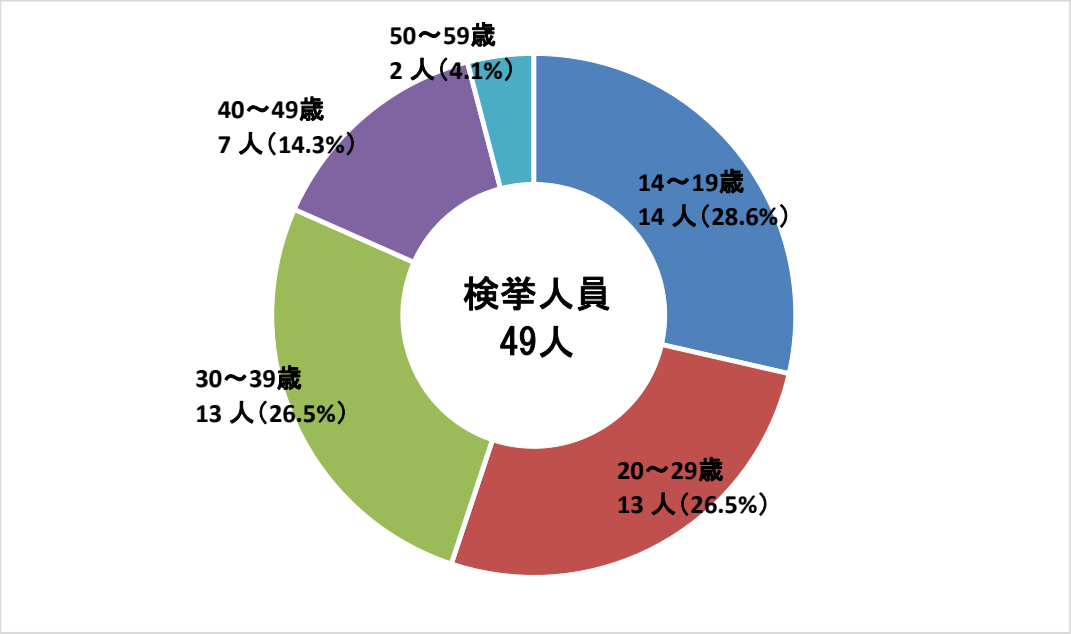
| | 利用していた | | 利用していない | | 不 明 | | 合 計 |
|---|---|---|---|---|---|---|---|
| ワンタイムパスワード(個人口座) | 99 | 32.5% | 185 | 60.7% | 21 | 6.9% | 305 |
| 電子証明書(法人口座) | 8 | 47.1% | 9 | 52.9% | 0 | 0.0% | 17 |

## 4　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

### (1) 検挙件数の推移

| | H26 | H27 | H28 | H29 | H30 |
|---|---|---|---|---|---|
| 不正指令電磁的記録作成･提供 | 9 | 8 | 4 | 29 | 12 |
| 不正指令電磁的記録供用 | 16 | 21 | 36 | 24 | 37 |
| 不正指令電磁的記録取得･保管 | 3 | 16 | 18 | 22 | 19 |
| 電子計算機使用詐欺 | 108 | 157 | 281 | 228 | 188 |
| 電磁的記録不正作出･毀棄等 | 48 | 32 | 24 | 39 | 84 |
| 電子計算機損壊等業務妨害 | 8 | 6 | 11 | 13 | 9 |
| 合計 | 192 | 240 | 374 | 355 | 349 |

### (2) 不正指令電磁的記録に関する罪の年代別被疑者数（触法少年を除く）




不正指令電磁的記録に関する罪

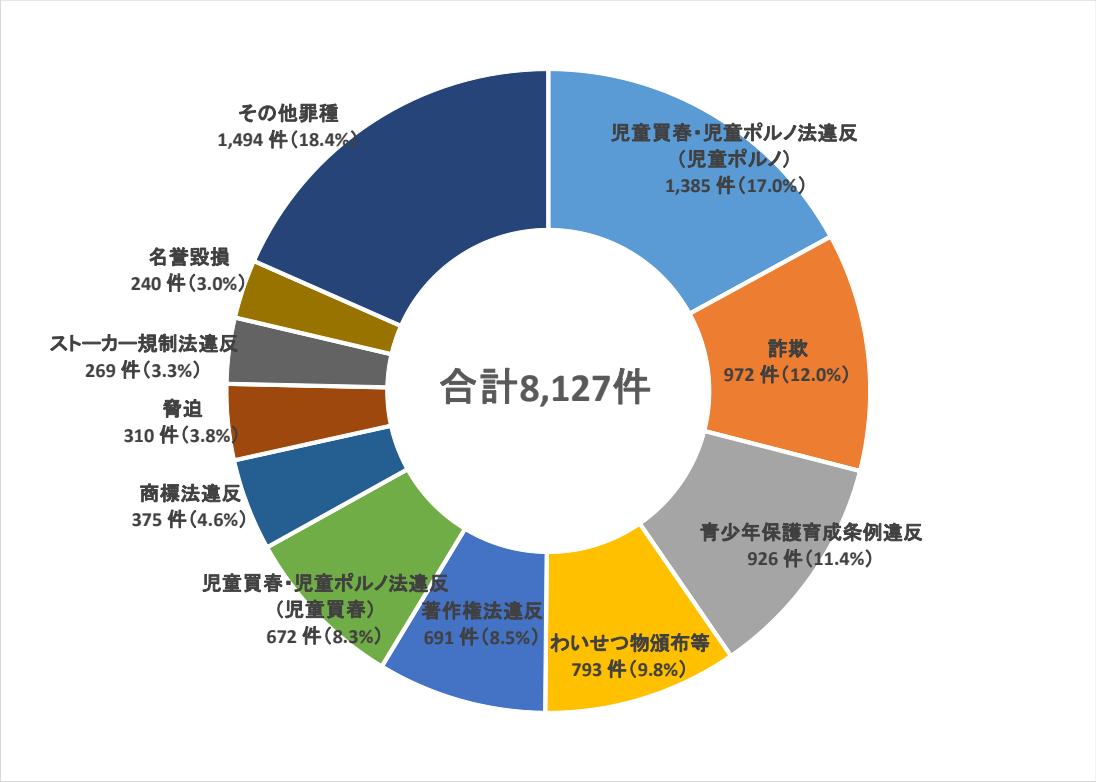
○　会社役員の男（40）らは、29年７月、サイト閲覧者のパソコンに不当な料金請求画面を繰り返し表示させる不正プログラムを供用し、真正なものと誤信させ現金を詐取した。30年７月、男らを不正指令電磁的記録供用・詐欺で検挙した。（愛知、宮城、静岡、石川、愛媛、鹿児島）

○　団体職員の男（40）は、30年３月、正当な理由がないのに、使用者の意図に反して位置情報等をサーバに送信させるなどの指令を与える不正指令電磁的記録を被害者のスマートフォンに蔵置し、供用した。30年５月、男を不正指令電磁的記録供用で検挙した。（福岡）

コンピュータ・電磁的記録対象犯罪

○　会社役員の男（27）は、29年12月、不正に入手した他人名義のクレジットカード情報を利用して、宿泊予約サイト運営会社に宿泊施設の予約を行い、カード決済をして宿泊料金の支払いを免れた。30年10月、男を電子計算機使用詐欺等で検挙した。（埼玉）

## ５　その他




児童買春・児童ポルノ禁止法違反

○　無職の男（53）は、29年３月、児童ポルノ画像ファイルを自らが運営するダークウェブサイト上に蔵置し、不特定多数のサイト会員に対して閲覧させた。30年６月、男を児童ポルノ禁止法違反で検挙した。（京都）

詐欺等

○　無職の女（33）は、28年10月頃、架空の人物の自動車運転免許証を真正なもののように装って、スマートフォンから預金口座開設とキャッシュカードの交付を申込み、金融機関からキャッシュカードを詐取した。30年10月、女を詐欺等で検挙した。（岩手）

著作権法違反

○　会社員の女（23）は、30年１月、著作権者の許可を受けないで著作物である漫画をインターネット上で公衆送信し得るようにして、著作権を侵害した。30年１月、女を著作権法違反で検挙した。（島根）