広　報　資　料
平成29年３月23日
警　　察　　庁

平成28年中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対するアクセス件数は、１日１IP アドレス当たり1,692.0件（前年比＋962.7件）で前年の２倍以上に増加。

○　アクセス件数の主な増加要因としては、ネットワークカメラ、デジタルビデオレコーダ等のLinux系OSが組み込まれたIoT機器等を標的とする探索行為等が挙げられる。

８月以降には、IoT機器を標的とする不正プログラム「Mirai」等による感染対象の探索行為等を観測。

(2) サイバー攻撃の情勢及び取組

ア　情勢

○　前年に引き続き、サイバー攻撃が世界的規模で発生。

○　警察が連携事業者等から報告を受けた標的型メール攻撃は4,046件（前年比＋218件）で３年連続増加。

28年に入るまでほとんど報告のなかった圧縮ファイルで送付された「.js」形式ファイルは下半期も増加傾向が続き、年間1,991ファイル（全体の54%）を確認。

○　国際的ハッカー集団「アノニマス」を名乗る者が、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、89組織に関してSNS上に掲載。

イ　取組

○　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64台（前年比＋16台）の機能停止を実施。

○　伊勢志摩サミット等の開催に際し、関係省庁、重要インフラ事業者、会議場等関係施設の管理者等と協力してサイバー攻撃対策を実施。

２　サイバー犯罪の情勢等

サイバー犯罪の検挙件数は8,324件（前年比＋228件）、相談件数は13万1,518件（前年比＋3,421件）でいずれも増加し、過去最多。

(1) インターネットバンキングに係る不正送金事犯

ア　情勢

○　発生件数は1,291件（前年比－204件）、被害額は約16億8,700万円（前年比－約13億8,600万円）で件数、被害額ともに減少。

○　特徴としては、法人口座及び信用金庫・信用組合の被害額が大幅に減少した一方で、電子決済サービスを使用して電子マネーを購入する手口が増加したことなどが挙げられる。

イ　取組

○　金融機関及び電子決済運営管理団体に対して、電子決済サービスを使用して電子マネーを購入する手口に対する対策の強化を要請。

○　口座売買等の関連事件75件・117人を検挙。

(2) 不正アクセス行為

ア　認知状況

○　認知件数は1,840件（前年比－211件）で前年に引き続き減少。

○　不正アクセス後の行為として「インターネットバンキングでの不正送金」が1,305件と最多。

イ　検挙状況

○　検挙件数502件、検挙人員200人、検挙事件数182事件で、検挙人員及び検挙事件数は平成12年の法施行後最多。

○　手口として「利用権者のパスワード設定・管理の甘さにつけ込んだもの」が244件と最多。

(3) 日本サイバー犯罪対策センター（ＪＣ３）と連携した取組

○　ＪＣ３と警察によるサイバーパトロールを行い、全国18道府県警察による口座売買等事件一斉集中取締りを実施。

○　警視庁が把握したウイルス付きメールの情報を基に、警視庁及び警察庁がSNSにより情報発信を行うとともに、ＪＣ３においてホームページ上にメール本文を含む詳細な情報を掲載。

３　今後の取組

「警察におけるサイバーセキュリティ戦略」（平成27年９月４日付け：警察庁乙官発第13号ほか）等を踏まえ、各種取組を推進する。

○　官民連携の推進

・　ＪＣ３との連携

・　重要インフラ事業者、先端技術を有する事業者、その他の事業者等との連携

○　サイバー人材の育成

・　専門的捜査員の育成（CSセンター等における教育・訓練の拡充等）

・　情報技術の解析に係る高度専門人材の育成

○　国際連携

・　外国捜査機関との連携

○　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（関係機関等との情報共有、共同対処訓練の実施等）

別　添

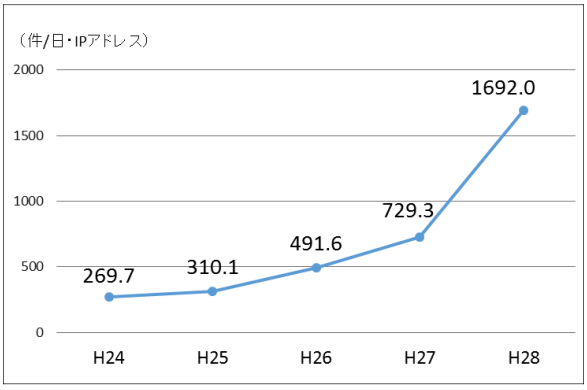
平成28年におけるサイバー空間をめぐる脅威の情勢等

１　サイバー攻撃の情勢等

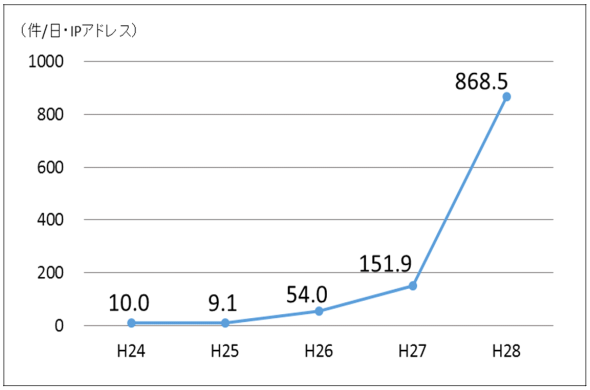
(1) サイバー空間における探索行為等

ア　センサー[*1] に対するアクセスの概況

センサーに対するアクセス件数は、１日・１IPアドレス当たり1,692.0件で、27年より962.7件増加した。



【センサーに対するアクセス件数の推移】



【宛先ポート「23/TCP」に対するアクセス件数の推移】

イ　特徴

○　IoT機器を標的とする「Mirai」ボット等による探索行為等が急増

アクセス件数の主な増加要因は、ネットワークカメラ、デジタルビデオレコーダ及びルータといったLinux系OSが組み込まれたIoT機器等を標的とする探索行為及びそれらの機器を踏み台とした攻撃活動等とみられる特定のポート[*2] へのアクセスが著しく活発化したことによるものである。

同ポートに対するアクセスにおいては、28年８月以降、IoT機器を標的とする不正プログラムである「Mirai」ボットが感染対象を探索しているとみられる活動を観測した。また、他のポートにおいても、「Mirai」ボットや同ボットの亜種によるものとみられる探索行為及び感染活動を観測した。

これを受けて、警察では「@police」等を通じて注意喚起を行った。

---

*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　コマンドの入力により遠隔制御を可能にするTelnetサービスで使用されるポート（23/TCP）

○　DNS[*3] サーバのソフトウェアの脆弱性を標的とした攻撃活動等

DNSサーバのソフトウェアであるBINDの脆弱性を標的とした攻撃活動、DNSルートサーバ[*4] に対するDoS攻撃、28年中に新たにリフレクター攻撃[*5] へ悪用される危険性が明らかとなった複数のプロトコルについて攻撃の踏み台となる機器を探索する活動も観測した。

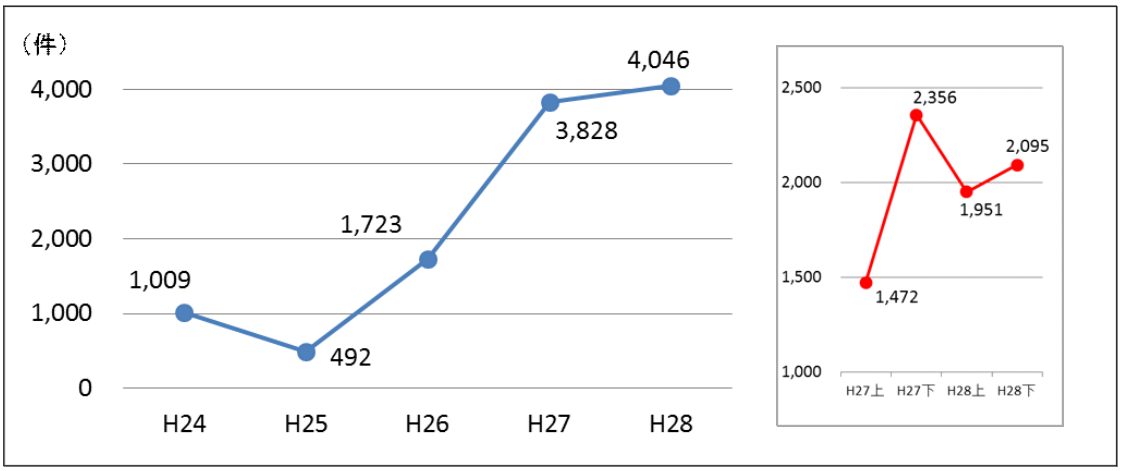
(2) サイバー攻撃の情勢及び取組

ア　情勢

(ｱ) 概況

27年に引き続き、サイバー攻撃が世界的規模で発生しており、国の治安や安全保障に影響を及ぼすおそれのある問題となっている。

警察では、サイバーインテリジェンス情報共有ネットワーク[*6] により、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4,046件で、27年より218件増加した。



【標的型メール攻撃の件数の推移】

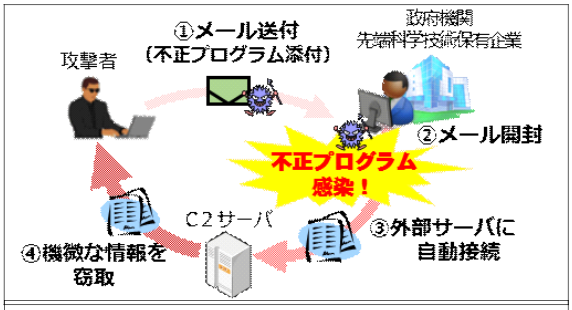
---

*3　Domain Name Systemの略。IPアドレスとホスト名を相互に変換する仕組みのこと。

*4　DNSにおいてツリー構造の起点となる最上位のサーバ群

*5　小さなサイズのリクエストに対して大きなサイズのレスポンスを返す性質のあるサーバに、送信元のIPアドレスを攻撃対象のものに偽装したリクエストパケットを送信することにより、当該サーバから攻撃対象への大量のレスポンスパケットでネットワークをあふれさせ、攻撃対象のサービス提供を妨害する攻撃手法。

*6　警察と先端技術を有する全国7,520の事業者等（平成29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。



【標的型メール攻撃の概要】

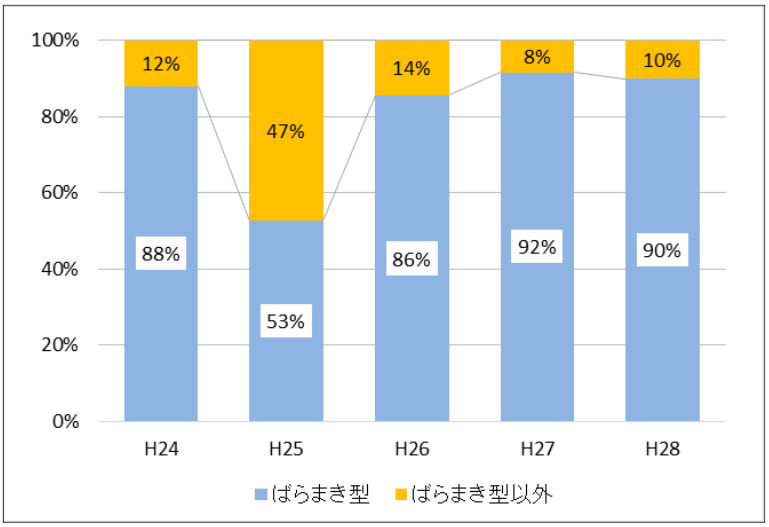
また、27年に引き続き、我が国の政府機関や地方公共団体、空港、水族館のウェブサイトに閲覧障害が生じる事案が発生した。

警察では、国際的ハッカー集団「アノニマス」を名乗る者が、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、89組織に関して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

○　「ばらまき型」攻撃の多発傾向が継続

27年から引き続き、「ばらまき型」攻撃が多数発生し、全体の90％を占めた。



【ばらまき型とそれ以外の標的型メール攻撃の割合】

○　大多数が非公開メールアドレスに対する攻撃

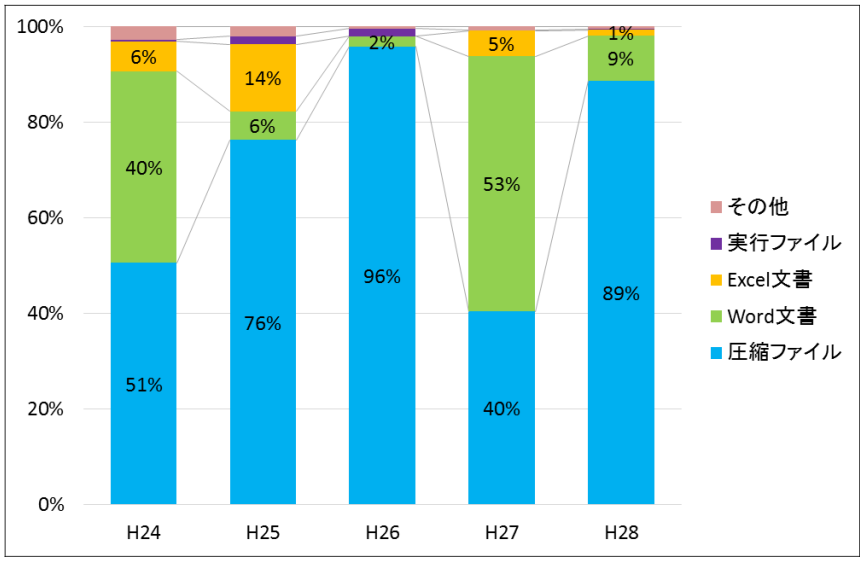
標的型メール攻撃の送信先メールアドレスについては、インターネット上で公開されていないものが全体の84％と、引き続き多数を占めており、攻撃者が攻撃対象の組織や職員について調査し、周到な準備を行った上で攻撃を実行している様子がうかがえる。

○　多くの攻撃において送信元メールアドレスが偽装

標的型メールの送信元メールアドレスについては、攻撃対象の事業者をかたるものなど、偽装されていると考えられるものが全体の94%と、引き続き多数を占めた。

○　標的型メールに添付されたファイル形式の変化

標的型メールに添付されたファイル形式の割合については、圧縮ファイルが添付されたものが27年中の40%から89%に増加した。

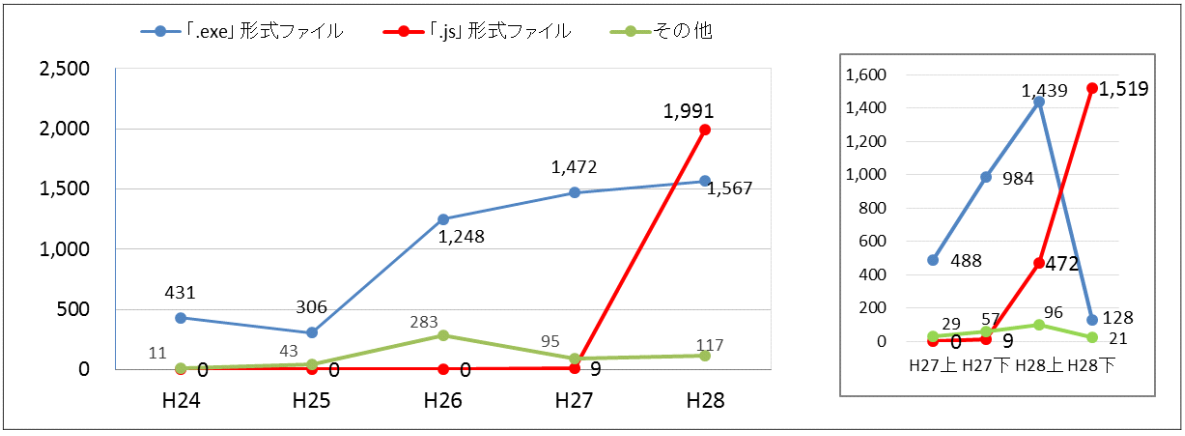


【標的型メールに添付されたファイル形式の割合】

○　圧縮ファイルで送付されたファイル形式の変化

圧縮ファイルで送付されたファイルについては、これまでほとんど報告のなかった「.js」形式ファイルが28年に入り多数確認された。

下半期も増加傾向は続き、1,519ファイルを確認し、年間の合計数は1,991ファイルと、全体の54%を占めた。一方、これまで多数を占めていた「exe」形式ファイルは、下半期に入って大幅に減少した。



【圧縮ファイルで送付されたファイル形式の推移】

イ 取組

(ｱ) サイバー攻撃事案で使用されたC2サーバのテイクダウン

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*7 64台の機能停止（テイクダウン）を実施し、27年中の48台を上回った。

(ｲ) 伊勢志摩サミット等へのサイバー攻撃対策

28年４月から９月にかけて開催された伊勢志摩サミット及び関係閣僚会合では、サイバー攻撃を警備における脅威の一つと位置づけ、

○ 会議主催省庁や内閣サイバーセキュリティセンター(NISC)等との連携の強化

○ 会場等関係施設、重要インフラ事業者等に対する管理者対策の徹底

○ 全国のサイバー攻撃特別捜査隊、サイバーフォースの特別派遣

○ 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の実施

等の取組を行った。

*7 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

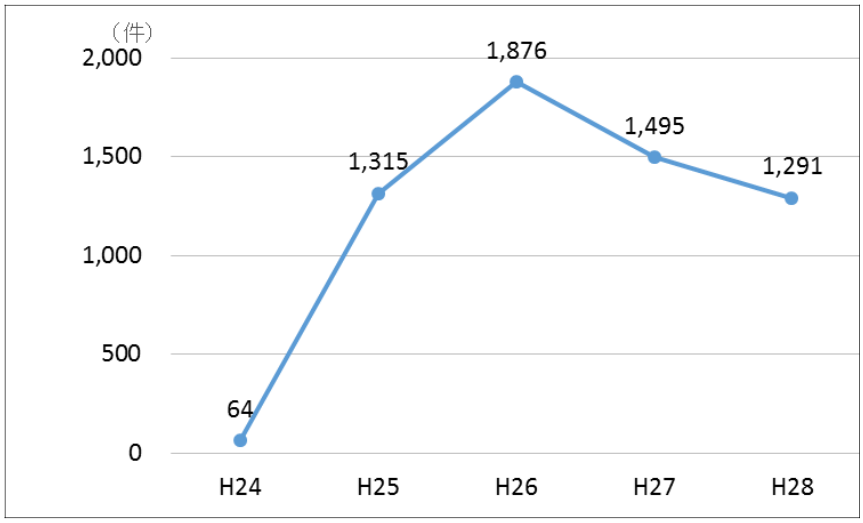
サイバー犯罪の検挙件数は8,324件で、27年より228件増加した。また、相談件数は13万1,518件で、27年より3,421件増加し、検挙件数、相談件数ともに過去最多となった。

(1) インターネットバンキングに係る不正送金事犯

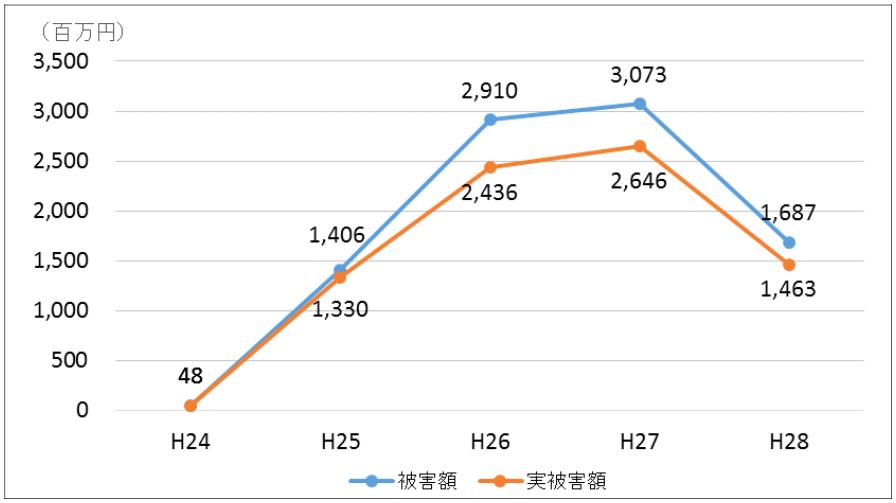
ア　情勢

(ｱ) 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1,291件、被害額約16億8,700万円で、27年と比較して、発生件数は204件、被害額は約13億8,600万円下回った。減少の要因としては、大口の法人口座被害の減少等が挙げられる。



【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の推移】



※　被 害 額：犯人が送金処理を行った全ての額

実被害額：「被害額」から金融機関が不正送金を阻止した額を差し引いた実質的な被害額

【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

○　法人口座で被害が大きく減少

法人口座の被害額については、27年と比較して、約10億3,100万円減少した。

○　信用金庫・信用組合の被害が大きく減少

信用金庫・信用組合の被害額については、27年と比較して、約７億9,400万円減少した。これは、ウイルス感染端末の早期検知等の対策によるものと考えられる。

○　電子決済サービスを用いた不正送金事犯が多発

インターネットバンキングの電子決済サービスを使用して電子マネー等を購入する手口が多発した。

○　不正送金先口座は中国人名義のものが約５割

不正送金の一次送金先として把握した1,722件の口座のうち、名義人の国籍は中国が約52％を占め、次いでベトナムが約25％、日本が約13％を占めた。

○　被害口座名義人の多くがセキュリティ対策を未実施

不正送金の被害に遭った口座のうち、個人口座で約61％、法人口座では約84％がワンタイムパスワードや電子証明書等のセキュリティ対策を実施していなかった。

イ　取組

○　不正送金事犯捜査から割り出されたレンタルサーバ情報の提供

不正送金事犯で不正アクセスに利用されたレンタルサーバからのアクセスを遮断するため、28年４月、レンタルサーバのIPアドレスを警察庁から全国都道府県警察及び一般財団法人日本サイバー犯罪対策センター（ＪＣ３）を通じて金融機関に情報提供した。

○　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

電子決済を使用して電子マネーを購入する手口が増加したことから、金融機関、電子決済運営管理団体に対して被害防止対策の強化を要請した。

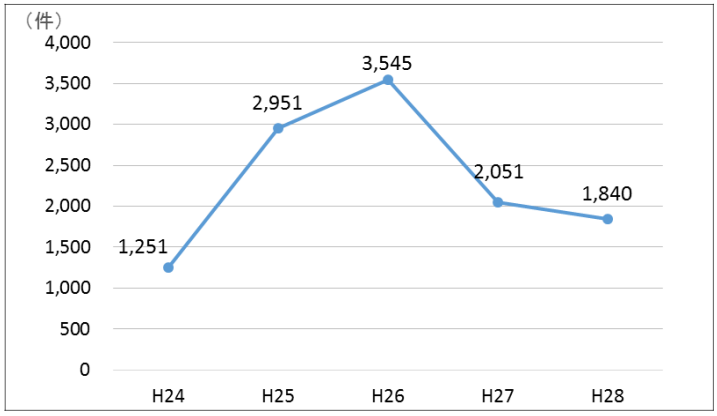
○　口座売買等の関連事件の検挙

不正送金事犯に係る口座売買の関連事件について、75件・117人を検挙した。

(2) 不正アクセス行為の発生状況等

ア　認知状況

○　28年中の不正アクセス行為の認知件数は1,840件となり、27年に続き減少した。減少の要因は、インターネットバンキングに係る不正送金事犯が減少したこと等が挙げられる。



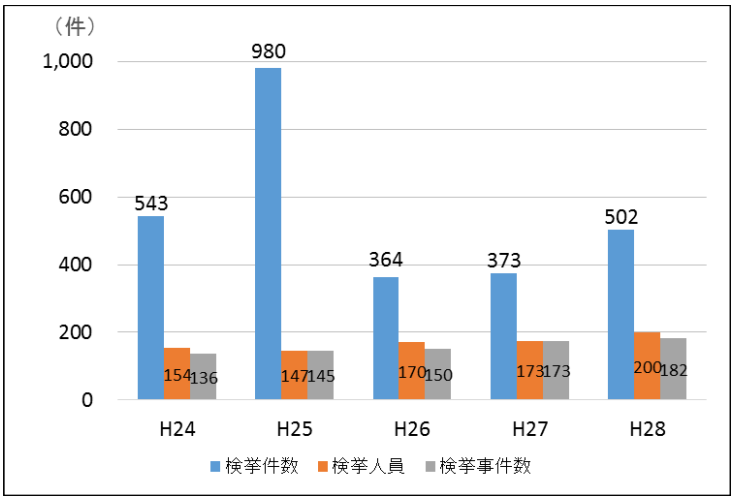
【不正アクセス行為の認知状況の推移】

○　不正アクセス後の行為として「インターネットバンキングでの不正送金」が多発

不正アクセス後の行為は、インターネットバンキングでの不正送金が、1,305件と最も多く、次いでインターネットショッピングでの不正購入が172件、オンラインゲーム、コミュニティサイトの不正操作が124件となっている。

イ　検挙状況

○　28年中の検挙件数は502件、検挙人員200人、検挙事件数182事件であり、検挙人員及び検挙事件数はいずれも平成12年の法施行後最多となった。



※　検挙事件数：事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は１事件と数える。

【不正アクセス行為の検挙状況の推移】

○　幅広い年齢層の被疑者

補導又は検挙された者は、12歳から63歳まで幅広い年齢層にわたっている。

○　不正アクセス行為の手口として「パスワード設定・管理の甘さにつけ込む手口」が最多

28年に検挙した手口の内訳は、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244件と最も多く、次いで識別符号を知り得る立場にあった元従業員や知人等によるものが61件となっている。

○　不正に利用されたサービスとして「オンラインゲーム、コミュニティサイト」が最多

28年に検挙した不正アクセス行為に係る被疑者に不正に利用されたサービスは、オンラインゲーム、コミュニティサイトが185件と最も多く、次いで電子メールが136件、社員・会員用等の専用サイトが40件となっている。

(3) 一般財団法人日本サイバー犯罪対策センター（ＪＣ３）との連携

ア　概況

26年から運用が開始されたＪＣ３においては、産学官の情報や知見を集約した分析を実施し、その結果等を還元することで、脅威の大本を特定し、これを軽減及び無効化することで、以後の事案発生の防止を図ることとしている。

警察は、捜査関連情報等をＪＣ３において共有し、産学におけるサイバーセキュリティに関する取組に貢献するとともに、ＪＣ３において共有された情報を警察活動に迅速・的確に活用することにより、安全安心なサイバー空間の構築に努めている。

イ　取組

○　フィッシングサイトの早期把握と金融機関への迅速な情報の提供

28年２月から、ＪＣ３が把握した金融機関に係るフィッシングサイト情報について、ＪＣ３から対象となる金融機関に提供するとともに、警視庁からJPCERT/CC等に提供することにより、フィッシングサイトの閉鎖を促した。

○　新たな不正送金ウイルスに対する注意喚起の実施

28年６月、不正送金事犯に係る現場情報収集活動により検出した情報を基に、ＪＣ３と警察庁が協力して分析し特定した不正送金ウイルスの情報をＪＣ３のホームページ上に掲載して注意喚起を実施した。

○　サイバー空間上の口座売買等事件一斉集中取締りの実施

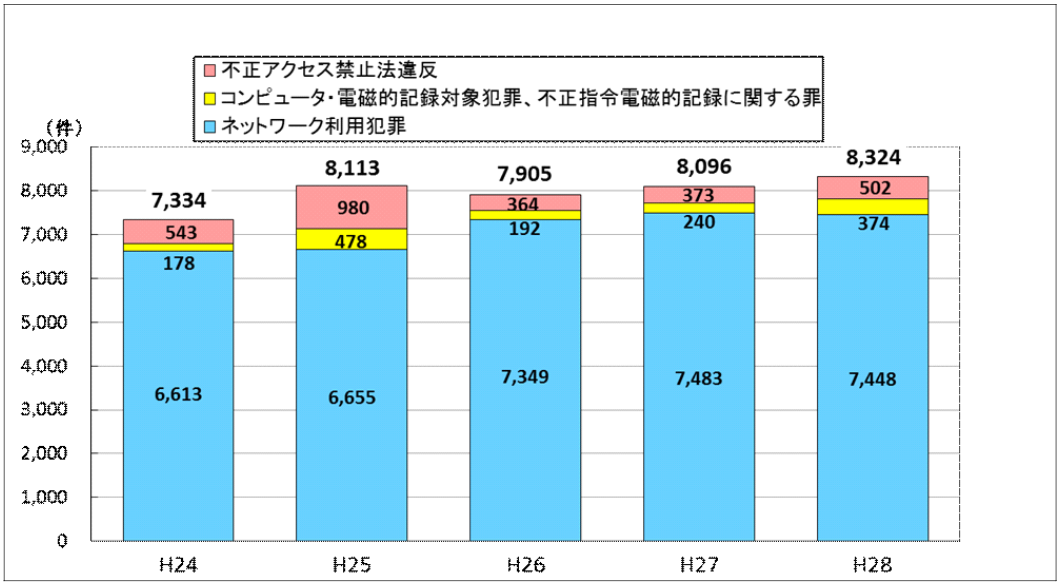
サイバー空間上には、口座売買情報が多数存在しており、これまでも各都道府県警察が独自に端緒を得て取締りを行ってきたが、ＪＣ３会員企業からの問題提起を受けて、ＪＣ３と警察によるサイバーパトロールを実施した。その結果をもとに、28年９月から10月にかけて、全国18道府県警察によるサイバー空間上の口座売買等事件一斉集中取締りを行った。

○　インターネットバンキング不正送金事犯に係るウイルス付きメールの早期警戒情報の発信

28年11月、警視庁において、民間事業者と連携してインターネットバンキング不正送金事犯に使用されるウイルス付メールを配信するウイルスの解析を行い、ウイルス付メールの内容を把握することが可能となった。ウイルス付メールの配信に係る指令を把握する毎に警視庁及び警察庁のSNSを利用し情報発信を行うとともに、ＪＣ３において、ホームページ上にメール本文を含む詳細な情報を掲載した。

【　参考１　】

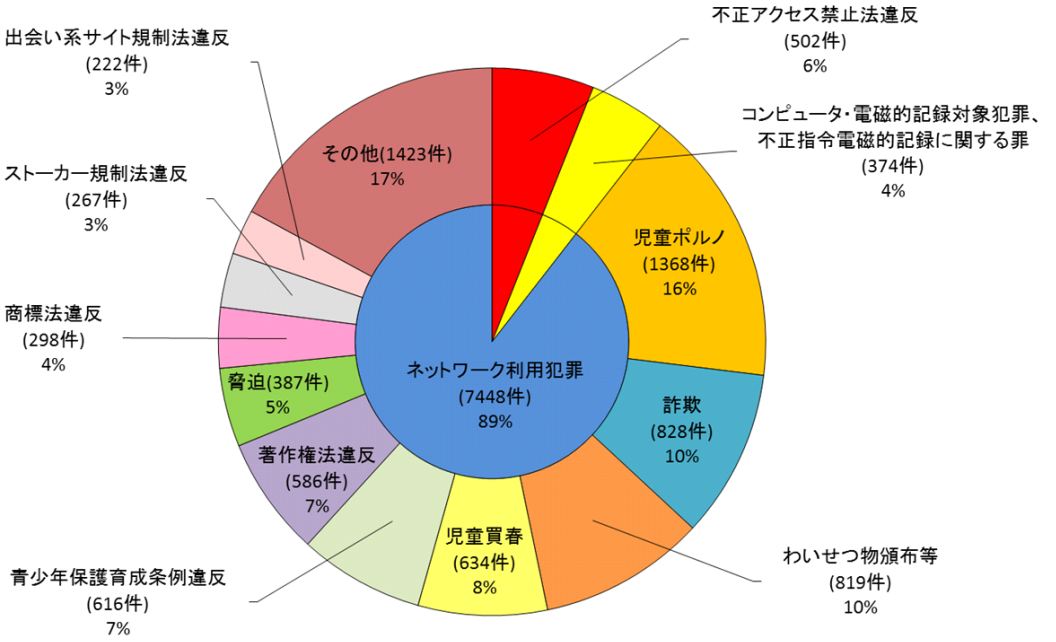
１　サイバー犯罪の検挙件数の推移



２　検挙件数の内訳

罪名＼年	H24	H25	H26	H27	H28
不正アクセス禁止法違反	543	980	364	373	502
コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪	178	478	192	240	374
電子計算機使用詐欺	95	388	108	157	281
電磁的記録不正作出・毀棄等	35	56	48	32	24
電子計算機損壊等業務妨害	7	7	8	6	11
不正指令電磁的記録作成・提供	4	8	9	8	4
不正指令電磁的記録供用	34	14	16	21	36
不正指令電磁的記録取得・保管	3	5	3	16	18
ネットワーク利用犯罪	6,613	6,655	7,349	7,483	7,448
児童買春・児童ポルノ法違反（児童ポルノ）	1,085	1,124	1,248	1,295	1,368
詐欺	1,357	956	1,133	951	828
うちオークション利用詐欺	235	158	381	511	208
わいせつ物頒布等	929	781	840	835	819
児童買春・児童ポルノ法違反（児童買春）	435	492	493	586	634
青少年保護育成条例違反	520	690	657	693	616
著作権法違反	472	731	824	593	586
脅迫	162	189	313	398	387
商標法違反	184	197	308	304	298
ストーカー規制法違反	78	113	179	226	267
出会い系サイト規制法違反	363	339	279	235	222
その他	1,028	1,043	1,075	1,367	1,423
合　　計	7,334	8,113	7,905	8,096	8,324

３　ネットワーク利用犯罪の検挙状況の内訳



４　検挙事例

不正アクセス禁止法違反

【不正アクセス禁止法違反】

○　高校生の少年（16）らは、27年５月から同年11月までの間、SQLインジェクションによる不正アクセスにより、企業のサーバコンピュータから多数の他人のID・パスワードを不正に取得し、同ID・パスワードを使用してショッピングサイトに不正にアクセスして玩具を購入した。28年９月、不正アクセス禁止法違反（不正アクセス行為）等で送致した。（宮城）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　会社員の男（33）らは、28年１月、他人又は架空人の運転免許証画像等を用いた上、他人名義のクレジットカードを使用して、ビットコイン取引所サイトにて約90万円分のビットコインを購入する旨の虚偽の情報を送信するなどして、同購入代金の支払いを免れた。28年11月、電子計算機使用詐欺で検挙した。（警視庁）

不正指令電磁的記録に関する罪

【不正指令電磁的記録供用等】

○　少年（15）らは、無料オンラインストレージサービスにチートツールを装った遠隔操作ウイルスをアップロードし、これをダウンロードした者のコンピュータに感染させるなどした。28年９月から同年12月までに、遠隔操作ウイルスを感染させた少年９名を不正指令電磁的記録供用等で検挙した。（北海道、宮城、群馬、神奈川、新潟、静岡、福井、滋賀、島根、岡山、徳島、愛媛、鹿児島）

ネットワーク利用犯罪

【犯罪収益移転防止法違反】

○　口座売買サイト管理者の男（41）らは、口座売買サイトや匿名掲示板に他人名義の口座を販売する旨の広告を出して顧客を募り、購入申込みをした者に提供するなどした。日本サイバー犯罪対策センターの協力を得て、全国規模の一斉集中取締りを実施し、28年９月から同年12月までに、口座売買サイトの管理者を含む28名を犯罪収益移転防止法違反等で検挙した。（北海道、宮城、茨城、埼玉、千葉、神奈川、岐阜、愛知、京都、大阪、岡山、広島、香川、福岡、熊本）

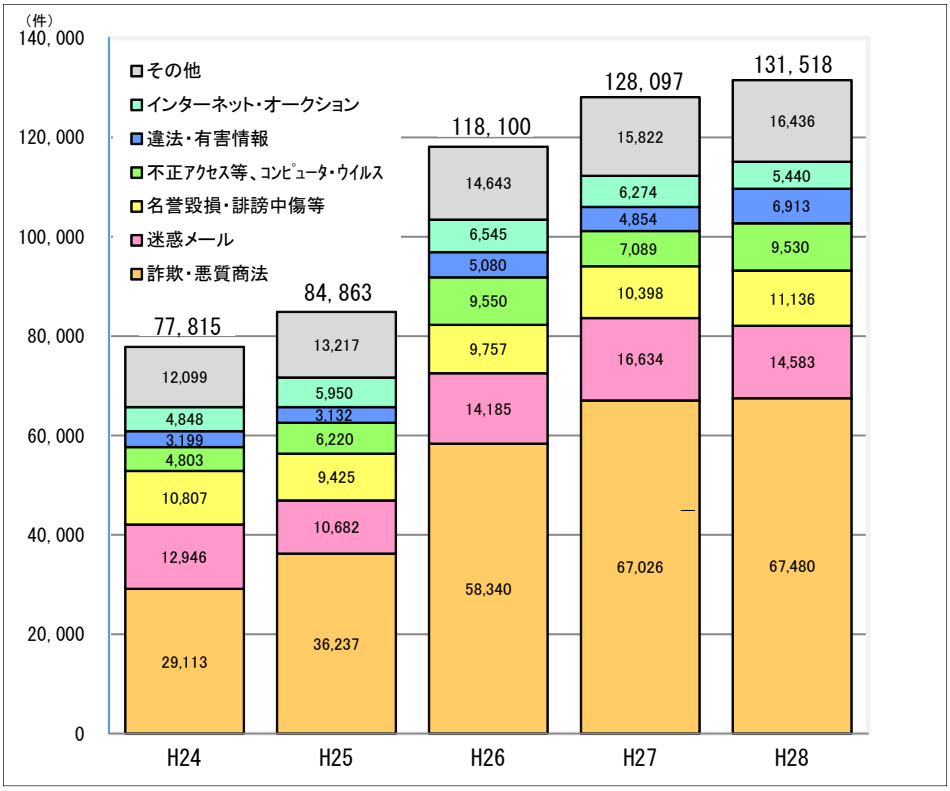
【著作権法違反】

○　自営業の男（54）は、27年６月、日本未公開の映画や海外ドラマ等の台詞を翻訳した日本語字幕ファイルを作成し字幕専用サイトに送信した。28年７月、著作権法違反（翻訳権の侵害）で検挙した。

無職の男（58）は、27年12月から28年１月までの間、字幕専用サイトに投稿された字幕ファイルと動画ファイルを同期させた上、ファイル共有ソフト等を利用して字幕付き動画ファイルを無断で公開した。28年７月、著作権法違反（公衆送信権の侵害）で検挙した。

中国人の男（30）らは、「字幕組」と称し、28年７月から同年８月までの間、日本で放送されたアニメに中国語の字幕を付し、ファイル共有ソフト等を利用しインターネット上に無断で公開した。28年９月及び10月、著作権法違反（公衆送信権の侵害）で検挙した。（京都）

５　サイバー犯罪等に関する相談件数の推移



６　相談件数の内訳

	H24	H25	H26	H27	H28
詐欺・悪質商法に関する相談（ｲﾝﾀｰﾈｯﾄ･ｵｰｸｼｮﾝ関係を除く）	29,113	36,237	58,340	67,026	67,480
迷惑メールに関する相談	12,946	10,682	14,185	16,634	14,583
名誉毀損・誹謗中傷等に関する相談	10,807	9,425	9,757	10,398	11,136
不正アクセス等、コンピュータ・ウイルスに関する相談	4,803	6,220	9,550	7,089	9,530
違法・有害情報に関する相談	3,199	3,132	5,080	4,854	6,913
インターネット・オークションに関する相談	4,848	5,950	6,545	6,274	5,440
その他	12,099	13,217	14,643	15,822	16,436
合　　計	77,815	84,863	118,100	128,097	131,518

７　相談事例

詐欺・悪質商法に関する相談

- インターネットショッピングで購入したブランド品が偽物だった。
- 登録した覚えのない有料サイトの料金を請求された。

迷惑メールに関する相談

- 儲け話を教えてくれるというメールが送られてきた。
- 身に覚えのないアダルトサイト利用料金を請求するメールが送られてきた。

名誉毀損・誹謗中傷等に関する相談

- 掲示板サイトに個人情報を掲載されて、誹謗中傷する内容を書き込まれた。
- 自分の店の名前を騙って勝手に情報発信された。

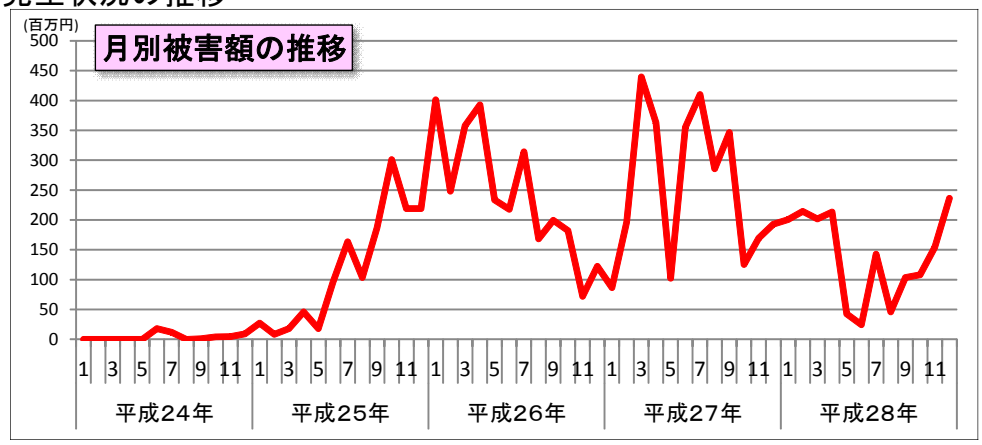
不正アクセス等、コンピュータ・ウイルスに関する相談

- ポイントサービス会社のアカウントが不正に利用され、勝手にポイントが利用されて、商品を購入された。

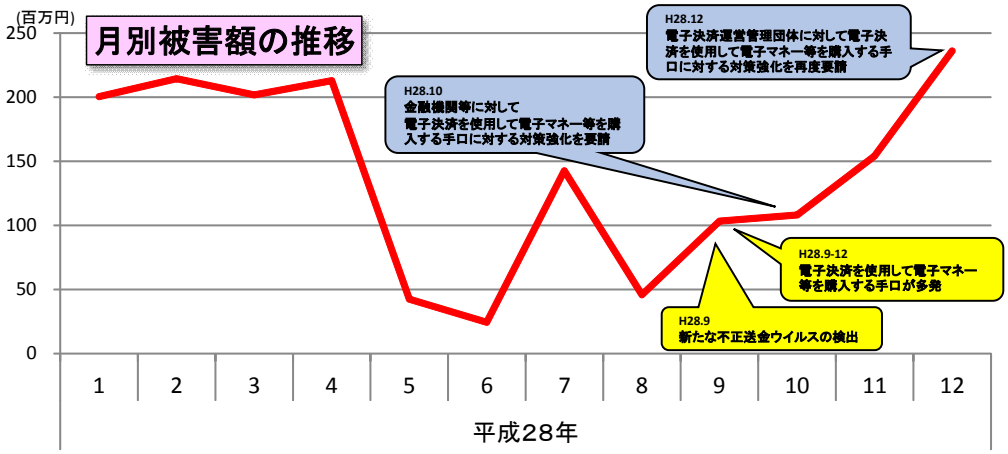
【　参考２　】

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

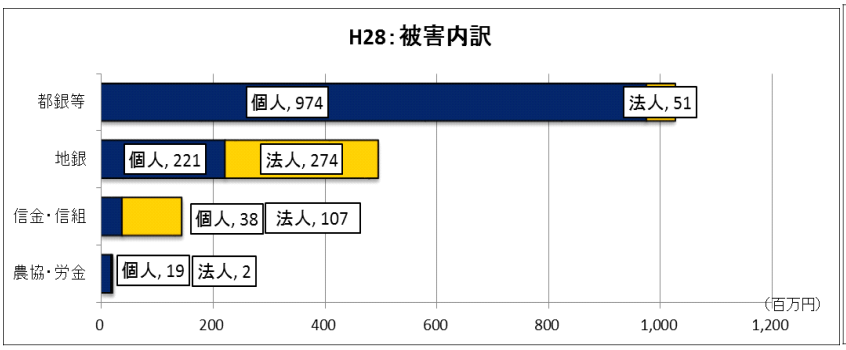
(1) 発生状況の推移

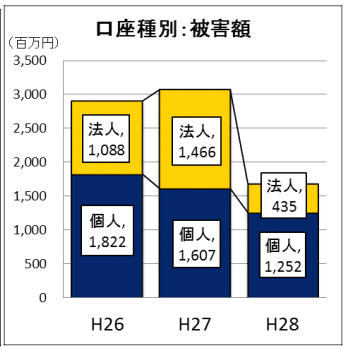


(2) 月別被害額の推移



(3) 被害内訳

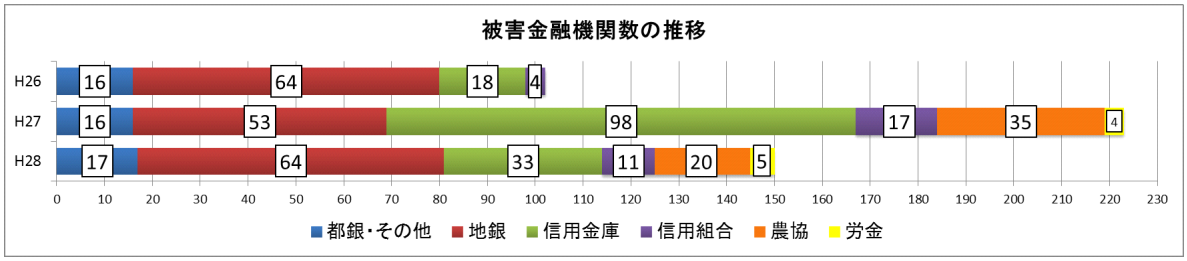




(4) 被害金融機関

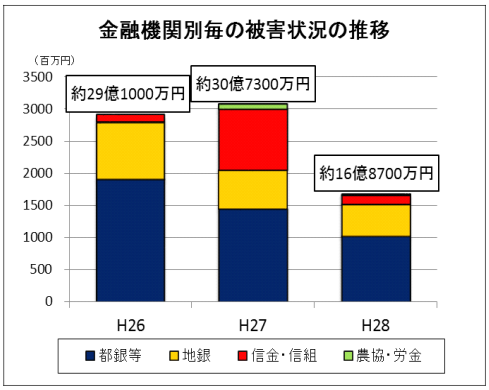
１５０金融機関

都市銀行・ネット専業銀行・信託銀行・その他の銀行	１７行
地方銀行	６４行
信用金庫	３３金庫
信用組合	１１組合
農業協同組合	２０組合
労働金庫	５金庫



(5) 金融機関別毎の被害状況

金融機関別	H26	H27	H28
都銀等	約19億500万円	約14億4600万円	約10億2500万円
地　銀	約8億8200万円	約6億円	約4億9500万円
信金・信組	約1億2300万円	約9億4000万円	約1億4500万円
農協・労金	0円	約8700万円	約2100万円
合　計	約29億1000万円	約30億7300万円	約16億8700万円

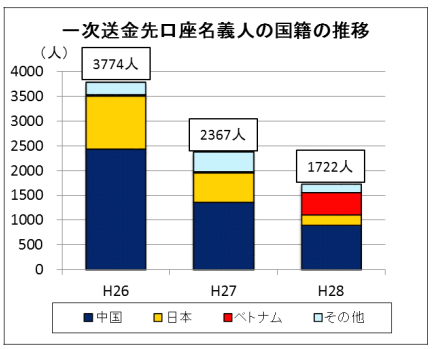


(6) 口座種別毎の被害状況

口座種別		平成28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9億7400万円（57.7%）	約2億2100万円（13.1%）	約3800万円（2.2%）	約1900万円（1.1%）	約12億5200万円（74.2%）
	実被害額	約8億5900万円（58.7%）	約2億100万円（13.7%）	約3700万円（2.5%）	約1800万円（1.3%）	約11億1400万円（76.1%）
法人	被害額	約5100万円（3.0%）	約2億7400万円（16.2%）	約1億700万円（6.4%）	約200万円（0.1%）	約4億3500万円（25.8%）
	実被害額	約3900万円（2.7%）	約2億600万円（14.1%）	約1億200万円（7.0%）	約200万円（0.2%）	約3億4900万円（23.9%）
合計	被害額	約10億2500万円（60.8%）	約4億9500万円（29.3%）	約1億4500万円（8.6%）	約2100万円（1.3%）	約16億8700万円（100.0%）
	実被害額	約8億9700万円（61.3%）	約4億600万円（27.8%）	約1億3900万円（9.5%）	約2100万円（1.4%）	約14億6300万円（100.0%）

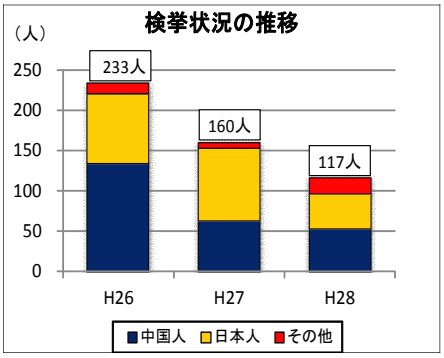
(7) 一次送金先口座名義人の国籍

	H26		H27		H28	
中　国	2,420	64.1%	1,350	57.0%	892	51.8%
日　本	1,079	28.6%	603	25.5%	219	12.7%
ベトナム	28	0.7%	25	1.1%	438	25.4%
その他	247	6.5%	389	16.4%	173	10.0%
合　計	3,774	100.0%	2,367	100.0%	1,722	100.0%



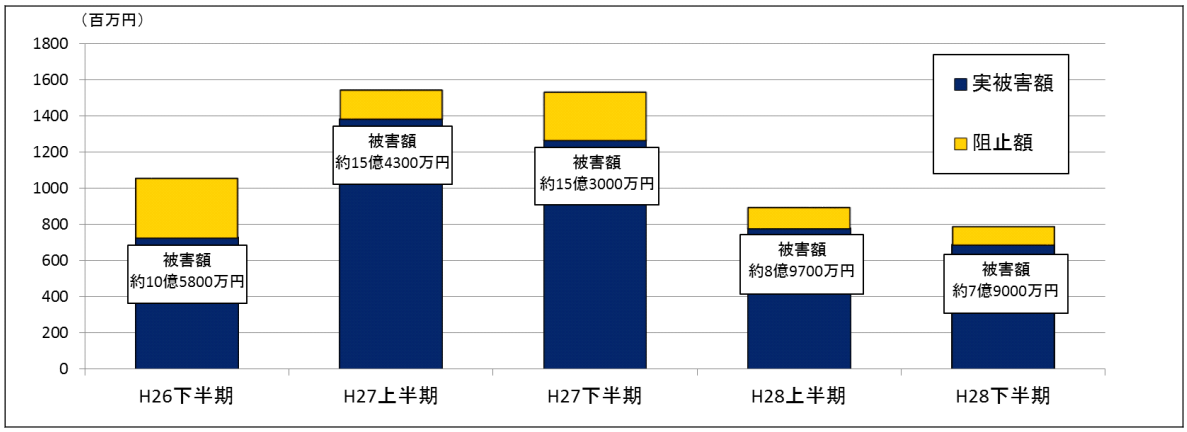
(8) 関連事件の検挙状況

		H26		H27		H28	
検挙事件		115件		97件		75件	
検挙人数		233人		160人		117人	
内訳	中国人	134人	57.5%	63人	39.4%	53人	45.3%
	日本人	86人	36.9%	90人	56.3%	44人	37.6%
	その他	13人	5.6%	7人	4.4%	20人	17.1%



(9) 不正送金阻止状況

	被害額	実被害額	阻止額	阻止率
H26下半期	約10億5800万円	約7億2600万円	約3億3200万円	31.4%
H27上半期	約15億4300万円	約13億8300万円	約1億6100万円	10.4%
H27下半期	約15億3000万円	約12億6400万円	約2億6600万円	17.4%
H28上半期	約8億9700万円	約7億7600万円	約1億2000万円	13.4%
H28下半期	約7億9000万円	約6億8700万円	約1億400万円	13.2%



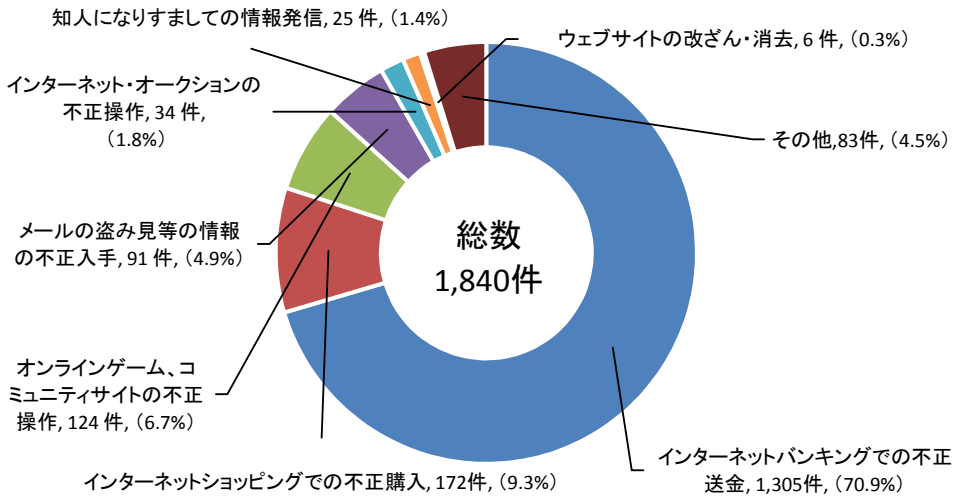
(10) 不正送金被害に係る口座名義人のセキュリティ対策実施状況

	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）	378	32.0%	719	60.9%	84	7.1%	1,181
電子証明書（法人口座）	11	10.0%	92	83.6%	7	6.4%	110

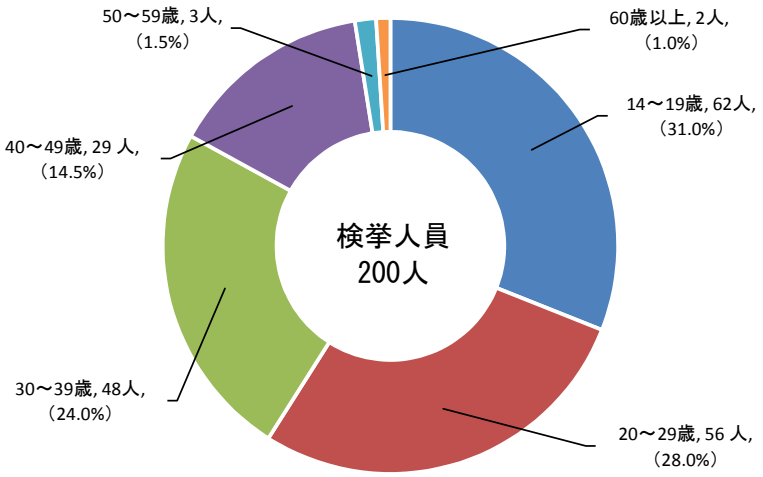
【　参考３　】

不正アクセス行為の発生状況

(1) 不正アクセス後の行為別認知件数

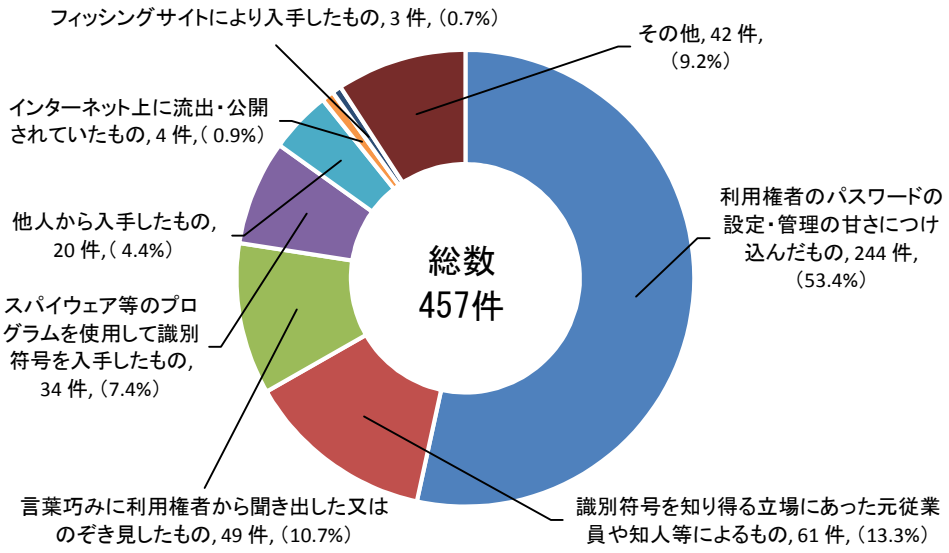


(2) 年代別被疑者数

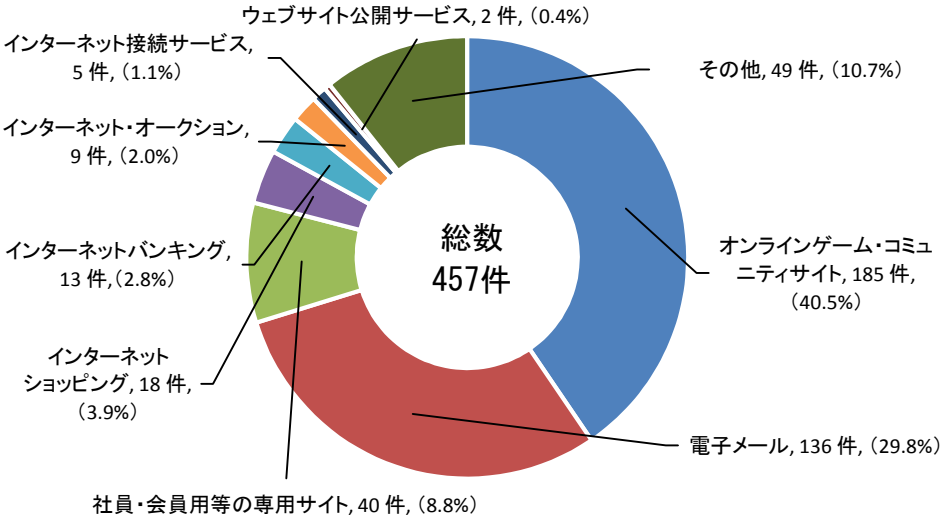


※　このほか、不正アクセス禁止法違反により、14歳未満の少年５名が触法少年として補導されている。

(3) 不正アクセス行為（識別符号窃用型[*8]）に係る手口別検挙件数



(4) 不正に利用されたサービス別検挙件数（識別符号窃用型）



*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