広　報　資　料
平成29年９月７日
警　　察　　庁

平成29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2,008.4件（前期比－250.2件）で、28年下半期からは約１割減少したものの、28年上半期と比較してほぼ倍の水準となっている。

○　28年下半期からアクセス件数が減少した主な要因としては、平成28年に大幅に増加した「Mirai」ボットによるアクセスが減少したことが挙げられるが、継続的に当該アクセスを観測。

○　世界規模で被害をもたらしたランサムウェア「WannaCry」の感染活動を始め、当該ランサムウェアに悪用された攻撃ツールに係る攻撃活動等を観測。

(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589件（前期比－1,506件）。また、標的型メールに添付されたファイル形式については、これまでほとんど報告のなかった形式が確認されたほか、各ファイル形式の割合についても従前と異なる傾向が見られる。

○　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、60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43台（前期比＋15台）の機能停止の実施をサーバを運営する事業者等に働きかけることで促進。

○　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攻撃対策として、関係機関等との共同対処訓練、情報交換等の取組を推進。

２　サイバー犯罪の情勢等

(1)　サイバー犯罪の検挙件数及びサイバー犯罪等に関する相談件数

サイバー犯罪の検挙件数は4,209件（前年同期比－71件）、相談件数は

６万9,977件（前年同期比＋3,238件）で、相談件数は過去最多。

⑵　インターネットバンキングに係る不正送金事犯

○　発生件数は214件（前年同期比－645件）、被害額約５億6,400万円（前年同期比－３億3,300万円）で、件数、被害額ともに減少。

○　特徴としては、個人口座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仮想通貨取引所に対して送金を行う新たな手口が発生したことなどが挙げられる。

⑶　仮想通貨アカウントへの不正アクセスによる不正送金事犯

認知件数は23件、被害額約5,920万円相当で、本年5月以降に認知件数が急増

⑷　取組

○　国際的な取組「オペレーションアバランチ」に係る流出ＩＤ等対策及び感染端末対策

○　官民連携によるウイルス感染を目的としたウェブサイト改ざんの対策

○　自動送金機能を有するインターネットバンキングウイルス「DreamBot」に係る対策

○　電子決済運営管理団体、仮想通貨取引所等に対して、モニタリングの強化、ワンタイムパスワードの利用促進、本人確認の徹底等を要請

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。

○　サイバー空間における情報収集・分析の推進

○　官民連携の推進
  - JC3との連携
    - サイバー空間の安全の確保に向けた情報の共有
    - 連携した情報の発信による被害拡大防止対策
  - 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

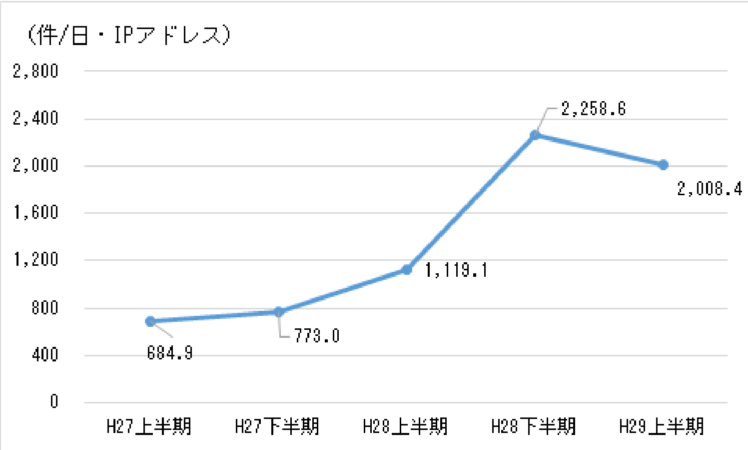
平成29年上半期におけるサイバー空間をめぐる脅威の情勢等

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2,008.4件で、28年下半期より250.2件減少した。



【センサーに対するアクセス件数の推移】

イ　特徴

○　IoT機器を標的としたアクセス

平成28年に大幅に増加した「Mirai」ボット（亜種を含む。）からのIoT機器を標的とした探索行為又は感染活動とみられるアクセス件数は、28年下半期と比較して１日・１IPアドレス当たり386.3件減少したものの、494.3件が観測された。

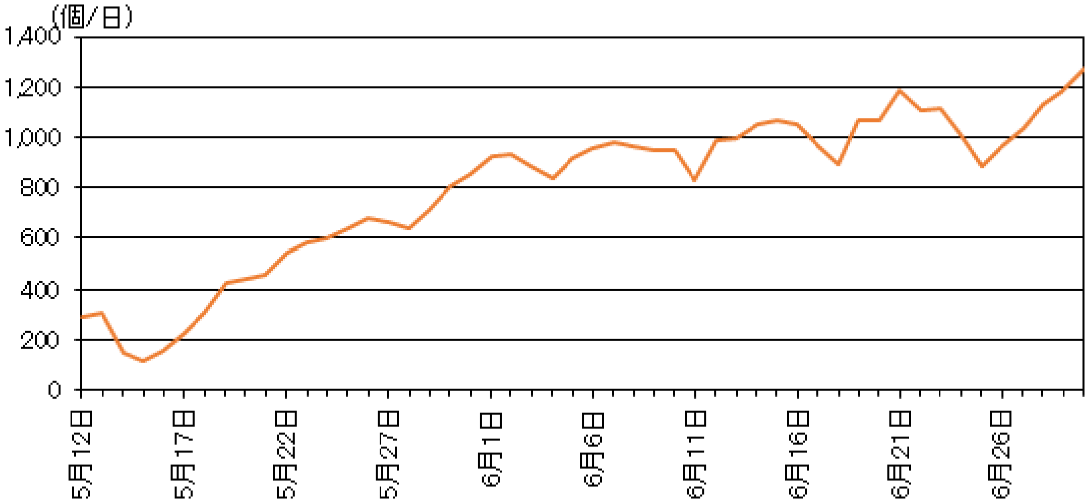
○　ランサムウェア「WannaCry」の感染活動等

４月、「The Shadow Brokers」を名乗る集団により、Microsoft Windowsを標的とした攻撃ツール「Eternalblue」及び「Doublepulsar」が公開され、それ以降、当該攻撃ツールを悪用した感染機器の探索行為又は攻撃活動を観測した。

---

[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。

５月には、「Eternalblue」及び「Doublepulsar」を悪用して作成されたランサムウェア「WannaCry」が世界的に大流行し、警察庁においても、その感染活動を観測した。また、６月には、利用者に気付かれることなく感染する「WannaCry」の亜種が感染を拡大していることも確認した。



【WannaCryの感染活動の特徴を有するポート445/TCPに対するアクセスの発信元IPアドレス数の推移】

○　Apache Struts 2[*2] の脆弱性を標的としたアクセス

３月に相次いで公表された Apache Struts 2 の深刻な脆弱性を標的とした探索行為及び攻撃活動を観測した。

(2)　サイバー攻撃の情勢及び取組

ア　情勢

(ｱ)　概況

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[*3] 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589件で、28年下半期より1,506件減少した。

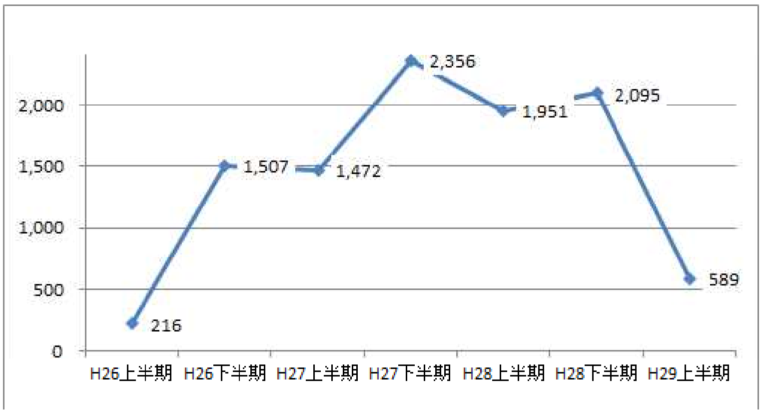
また、標的型メールに添付されたファイル形式については、これまでほとんど報告のなかった形式が確認されたほか、各ファイル形式の割合

---

*2　Java言語を用いたウェブアプリケーション開発に汎用的に使用される機能を提供して、開発の効率化等を図るもの。

*3　警察と先端技術を有する全国7,613の事業者等（平成29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。

についても従前と異なる傾向がみられる。



【標的型メール攻撃の件数の推移】

【標的型メール攻撃の概要】

また、28年に引き続き、我が国の政府機関、空港、水族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。

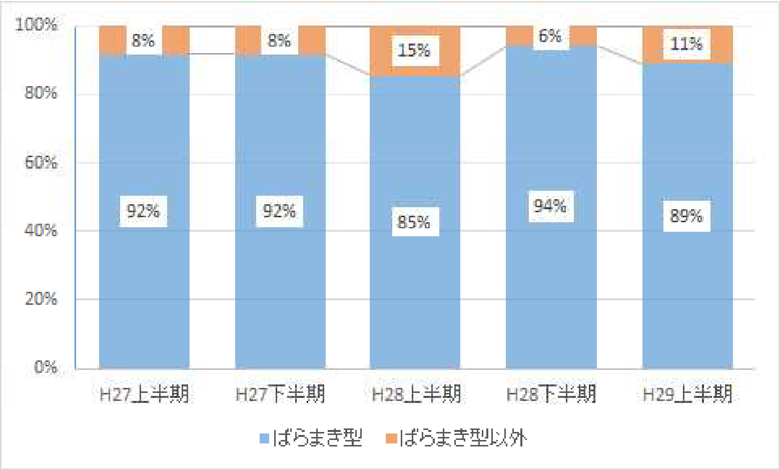
警察では、国際的ハッカー集団「アノニマス」を名乗る者が、サイバー攻撃を実行したとする犯行声明とみられる投稿を、60組織に関してSNS上に掲載している状況を把握している。

(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

28年から引き続き、「ばらまき型」攻撃[*4] が多数発生し、全体の90%近くを占めた。

[*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。



【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

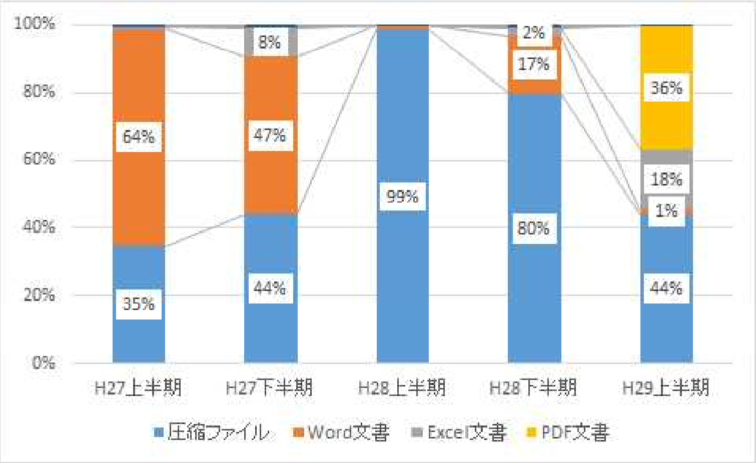
標的型メール攻撃の送信先メールアドレスについては、インターネット上で公開されていないものが全体の96%と、引き続き多数を占めた。

○　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、大学や銀行をかたるなど、偽装されていると考えられるものが全体の99%と、ほぼ全てを占めた。

○　標的型メールに添付されたファイル形式の変化

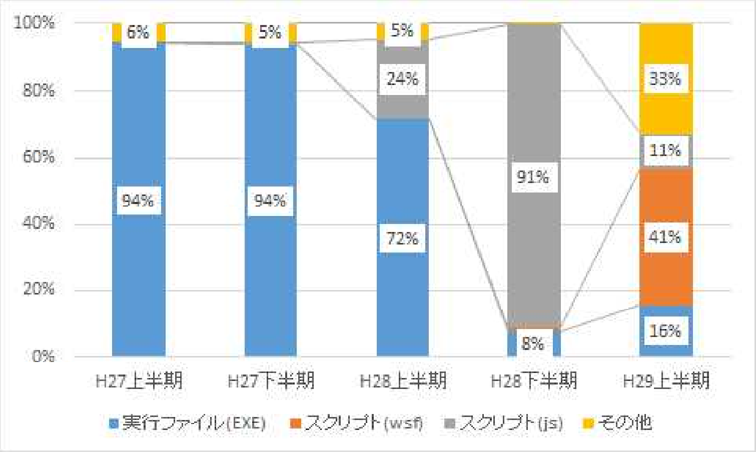
標的型メールに添付されたファイル形式については、これまではWordファイルそのものを添付していた傾向にあったが、平成28年に大きく減少し、今期においてはWordファイルを埋め込んだPDFファイルを新たに確認した。添付されたファイル形式は、対策の普及等によって変化しており、Wordファイルそのものの添付についてはある程度対策が普及したものと思われる。



【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形式については、28年下半期に多く確認された「.js」ファイルの割合が減少し、「.wsf」ファイルが増加した。近年は、スクリプトファイルが多く用いられており、今期においては、「.js」ファイルと「.wsf」ファイルを合わせると全体の５割程度を占めており、スクリプトファイルの利用が拡大するとともに、その種類も多様化しているものと思われる。



【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[*5]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、今期においては43台の機能停止が実施され、28年下半期中の28台を上回った。

(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、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。

(ｳ)　情報発信の強化

警察庁からはこれまでもサイバーセキュリティに係る関連情報を「@police」や「サイバー犯罪対策」（６月26日、「サイバー犯罪対策プロジェクト」に改名）のコーナーで発信してきたところ、６月26日、これらの情報等を取りまとめたポータルサイト“サイバーポリスエージェンシー”(https://www.npa.go.jp/cybersecurity/)を開設し、情報発信を強化した。

[*5] 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

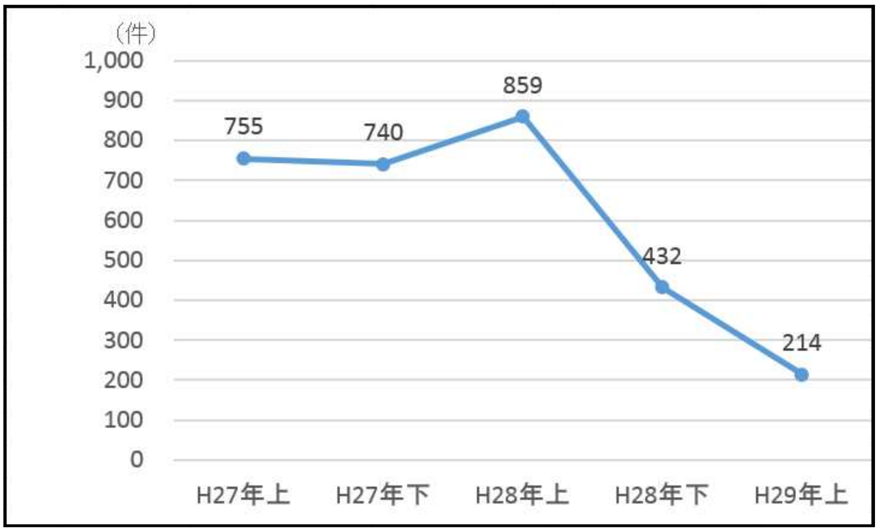
(1)　サイバー犯罪の検挙件数及びサイバー犯罪等に関する相談件数

サイバー犯罪の検挙件数は4,209件で、28年上半期より71件（－1.7％）減少した。また、相談件数は６万9,977件で、28年上半期より3,238件（＋4.9％）増加し、相談件数は過去最多となった。

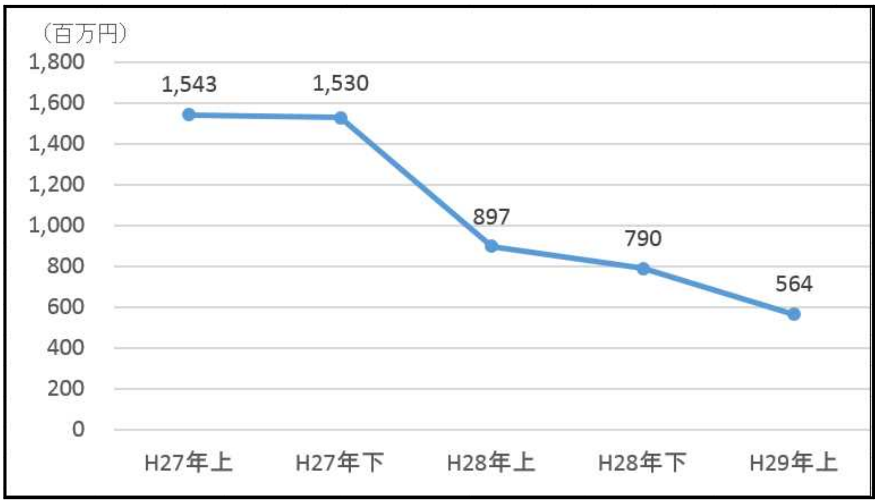
(2)　インターネットバンキングに係る不正送金事犯

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214件、被害額約５億6,400万円で、28年上半期と比較して、発生件数は645件、被害額は約３億3,300万円下回った。減少の要因としては、個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】



【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

○　個人口座の被害が大きく減少

個人口座の被害額については，28年上半期と比較して、約５億1,300万円減少した。

○　都市銀行等の個人口座被害が大きく減少

都市銀行・その他の個人口座の被害額については、28年上半期と比較して、約４億6,400万円減少した。これは、モニタリングの強化[6]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新たな不正送金事犯が発生

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仮想通貨取引所に対して送金を行う新たな手口が発生した。

この手口で仮想通貨取引所に送金された約１億400万円のうち、約6,900万円相当の仮想通貨等については、取引所において凍結措置がとられた。(仮想通貨については、29年７月のレートで換算)

○　不正送金先口座はベトナム人名義のものが約５割

不正送金の一次送金先として把握した374口座のうち、名義人の国籍はベトナムが約51％を占め、次いで中国が約23％、日本が約11％を占めた。

(3)　仮想通貨アカウントへの不正アクセスによる不正送金事犯

○　認知件数は23件、被害額約5,920万円相当で、本年５月以降に認知件数が急増。

○　被害が発生している取引所では、いずれも二段階認証を導入しているが、不正送金被害者23人のうち20人（87.0％）が、二段階認証[7]を利用していなかった。

(4)　取組

○　国際的な取組「オペレーションアバランチ」に係る流出ＩＤ等対策及び感染端末対策

国際的な取組「オペレーションアバランチ」に関し、日本国内のインターネットバンキング利用者のＩＤ・パスワード等の情報、コンピュータウ

---

[6] 不正送金に使用されたＩＰアドレス等に対する監視の強化。

[7] ログイン時、一般的な識別符号（ID、パスワード）による認証に、ワンタイムパスワード等の認証を更に一段階追加したもの。

イルスの感染端末情報等を入手するに至ったことから、関係省庁・団体と連携して、インターネットバンキング利用者、感染端末利用者等に対し、被害拡大防止のための注意喚起を実施した。

○　官民連携によるウイルス感染を目的としたウェブサイト改ざんの対策

ＪＣ３からの情報提供を元に、ＪＣ３と千葉県警察が連携して分析を行い、改ざん確認手法を確立し、全国38都道府県警察がサイト管理者に対して指導を行うなどの対策を実施した。

○　自動送金機能を有するインターネットバンキングウイルス「DreamBot」に係る対策

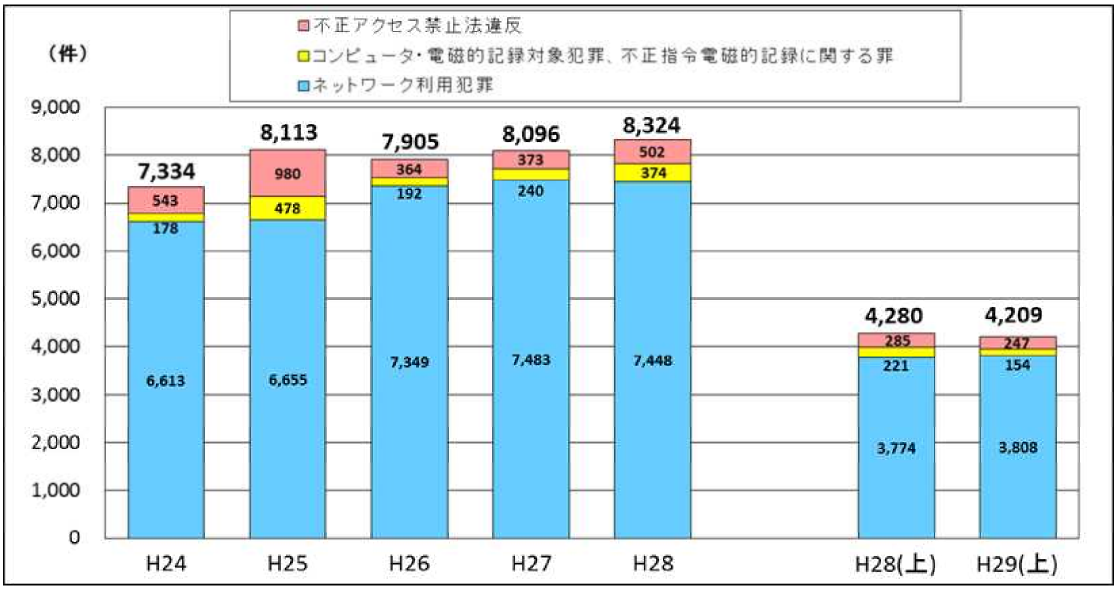
警視庁は、ＪＣ３と連携した不正送金ウイルス「DreamBot」の解析により、その機能を解明し、インターネット利用者や金融機関等に対して注意喚起を実施したほか、ＪＣ３ホームページ上にDreamBot感染チェックサイトを構築する等の対策を行った。

○　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

金融機関、電子決済運営管理団体、仮想通貨取引所等に対して、モニタリングの強化、ワンタイムパスワードの利用促進、ログイン時の二段階認証の利用、本人確認の徹底等を要請した。

【　参考１　】

１　サイバー犯罪の検挙件数の推移



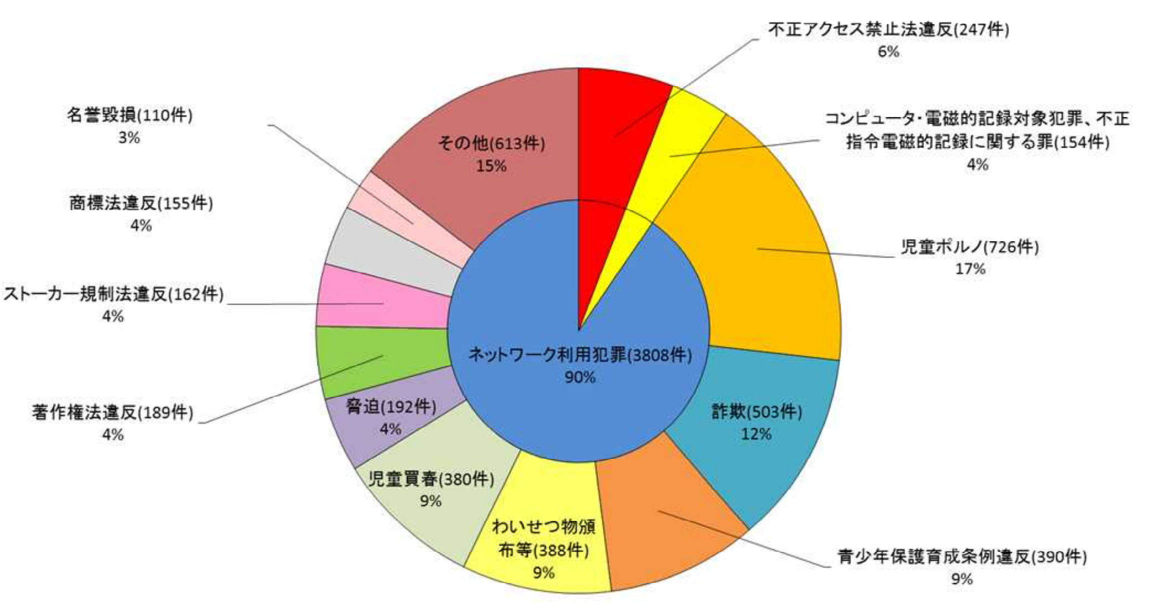
※ H29(上)は暫定値

２　検挙件数の内訳

年 罪　名	H24	H25	H26	H27	H28	H28（上）	H29（上）
不正アクセス禁止法違反	543	980	364	373	502	285	247
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	221	154
電子計算機使用詐欺	95	388	108	157	281	197	103
電磁的記録不正作出・毀棄等	35	56	48	32	24	8	20
電子計算機損壊等業務妨害	7	7	8	6	11	6	9
不正指令電磁的記録作成・提供	4	8	9	8	4	0	3
不正指令電磁的記録供用	34	14	16	21	36	5	14
不正指令電磁的記録取得・保管	3	5	3	16	18	5	5
ネットワーク利用犯罪	6,613	6,655	7,349	7,483	7,448	3,774	3,808
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	686	726
詐欺	1,357	956	1,133	951	828	475	503
うちオークション利用詐欺	235	158	381	511	208	115	140
青少年保護育成条例違反	520	690	657	693	616	343	390
わいせつ物頒布等	929	781	840	835	819	401	388
児童買春・児童ポルノ法違反（児童買春）	435	492	493	586	634	315	380
脅迫	162	189	313	398	387	194	192
著作権法違反	472	731	824	593	586	281	189
ストーカー規制法違反	78	113	179	226	267	131	162
商標法違反	184	197	308	304	298	149	155
名誉毀損	97	122	148	192	215	94	110
その他	1,294	1,260	1,206	1,410	1,430	705	613
合　　計	7,334	8,113	7,905	8,096	8,324	4,280	4,209

※ H29(上)は暫定値

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】

○　定時制高校生の男（20）は、28年10月、注目を集める目的で、ＳＮＳサイトの利用者であった殺人事件被害者の過去の書き込み等からパスワードを推測し、同被害者が利用していたID・パスワードを使用して同サイト等に不正にアクセスし投稿した。29年１月、不正アクセス禁止法違反（不正アクセス行為）で送致した。（千葉）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　無職の男（36）らは、27年８月、宿泊予約サイトを運営する会社に対し、他人名義のクレジットカード情報を利用してカード決済をして、宿泊料金の支払いを免れた。29年３月、被疑者３名を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（14）は、29年１月、自宅において、身代金要求型ウイルスであるランサムウェアを作成するとともに保管した。29年６月、不正指令電磁的記録作成等で検挙した。（神奈川）

ネットワーク利用犯罪

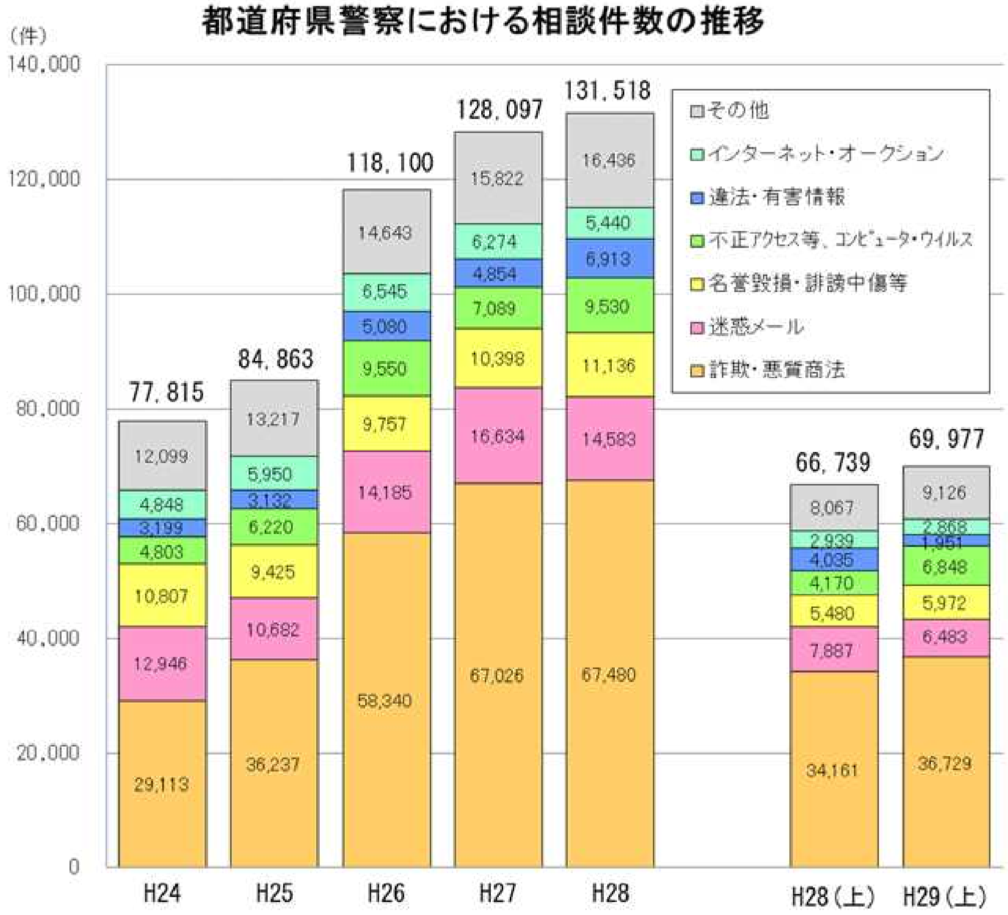
【詐欺】

○　会社役員の男（33）らは、アダルト動画サイトにアクセスした者に対して、真実は入金契約が締結されていないのに、これが締結されたと欺いて金員を詐取しようと企て、28年６月及び29年１月、退会料金名下に計35万円分の電子ギフト券の利用権を取得した。29年２月から同年３月までに、被疑者９名を詐欺で検挙した。（京都）

【公然わいせつ】

○　無職の男（36）らは、29年５月、閲覧数に応じてポイントを取得・換金できるインターネット動画配信サイトを利用し、マンションの一室から20代女性のわいせつな行為を生中継で配信し、不特定多数が閲覧できる状態にした。同月、公然わいせつで逮捕するとともに、６月までにパフォーマーと称して出演していた女性らを公然わいせつで検挙した。（大阪）

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	H28 (上)	H29 (上)
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	34,161	36,729
迷惑メールに関する相談	12,946	10,682	14,185	16,634	14,583	7,887	6,483
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	5,480	5,972
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	4,170	6,848
違法・有害情報に関する相談	3,199	3,132	5,080	4,854	6,913	4,035	1,951
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	2,939	2,868
その他	12,099	13,217	14,643	15,822	16,436	8,067	9,126
合　計	77,815	84,863	118,100	128,097	131,518	66,739	69,977

７　相談事例

詐欺・悪質商法に関する相談

- インターネットサイトで商品を注文し、代金を振り込んだが商品が届かない。
- 動画を閲覧しようとしたところ、登録料金を要求された。

迷惑メールに関する相談

- 「相続人がいないため、十数億円の遺産をあなたに相続したい」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要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。

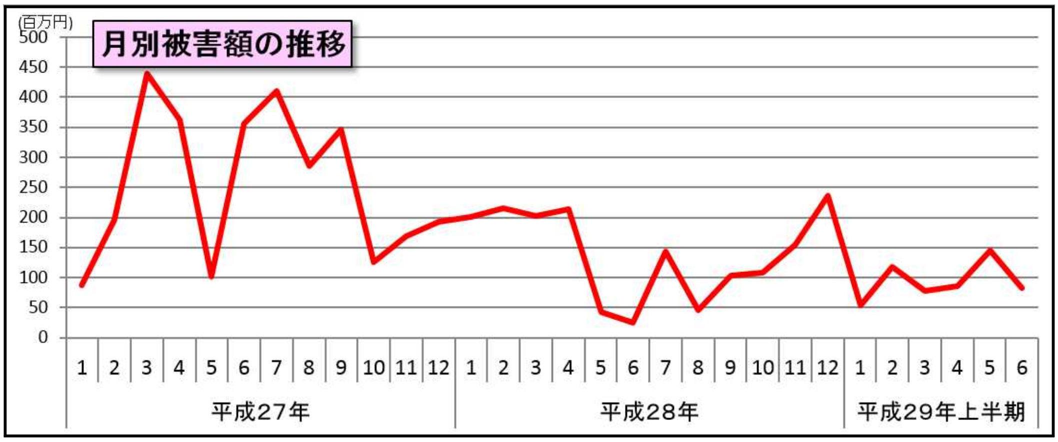
不正アクセス等、コンピュータ・ウイルスに関する相談

- ウイルス感染を警告する画面が表示され、画面に表示されていた電話番号に電話するとウイルス駆除料金を要求された。
- パソコンに保存していたデータが暗号化され、仮想通貨を要求された。

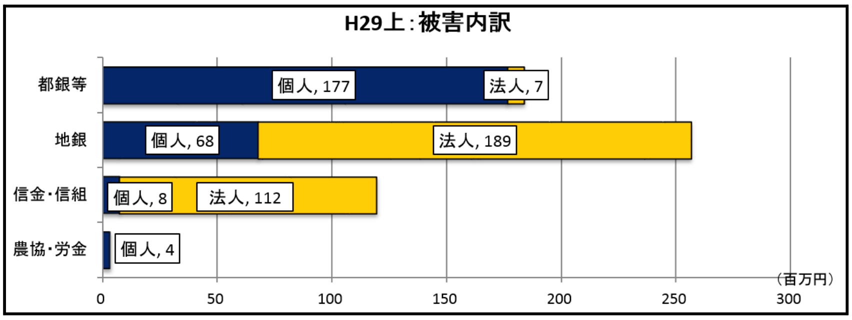
【　参考２　】

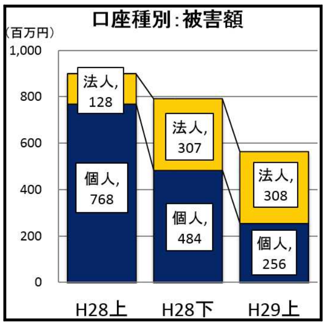
インターネットバンキングに係る不正送金事犯の発生状況

(1) 発生状況の推移



(2) 被害内訳

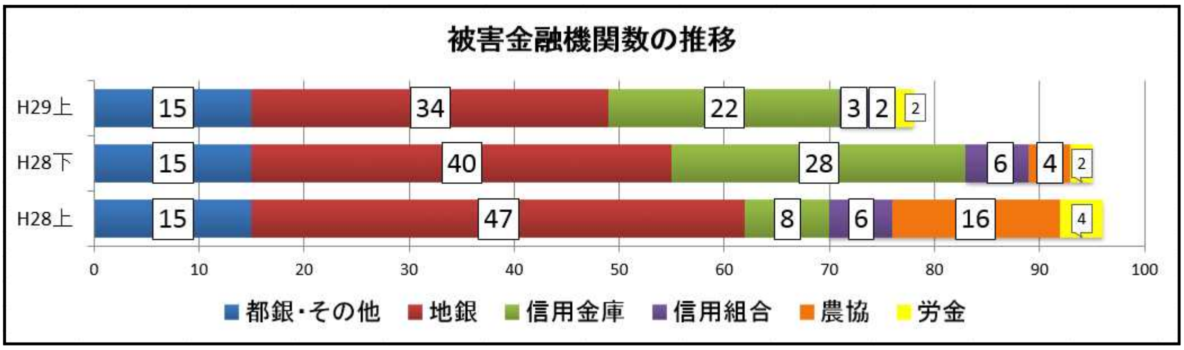




(3) 被害金融機関

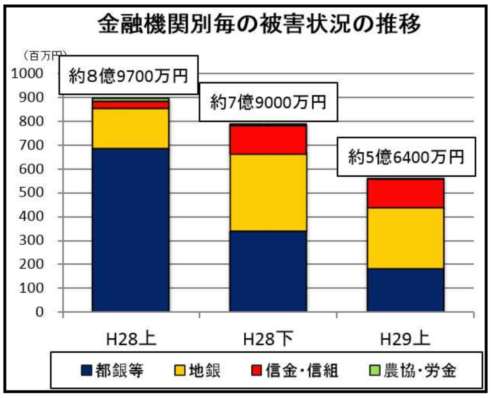
７８金融機関

都市銀行・ネット専業銀行・信託銀行・その他の銀行	１５行
地方銀行	３４行
信用金庫	２２金庫
信用組合	３組合
農業協同組合	２組合
労働金庫	２金庫



(4) 金融機関別毎の被害状況

金融機関別	H28上	H28下	H29上
都銀等	約6億8500万円	約3億4100万円	約1億8400万円
地　銀	約1億7100万円	約3億2400万円	約2億5700万円
信金・信組	約2700万円	約1億1900万円	約1億2000万円
農協・労金	約1400万円	約700万円	約400万円
合　計	約8億9700万円	約7億9000万円	約5億6400万円

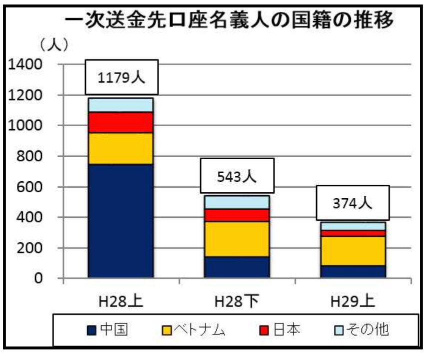


(5) 口座種別毎の被害状況

口座種別		平成29年上半期				
		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1億7700万円 (31.3%)	約6800万円 (12.1%)	約800万円 (1.4%)	約400万円 (0.6%)	約2億5600万円 (45.4%)
	実被害額	約1億5300万円 (34.2%)	約6300万円 (14.1%)	約600万円 (1.4%)	約400万円 (0.8%)	約2億2500万円 (50.6%)
法人	被害額	約700万円 (1.3%)	約1億8900万円 (33.5%)	約1億1200万円 (19.9%)		約3億800万円 (54.6%)
	実被害額	約700万円 (1.6%)	約1億900万円 (24.4%)	約1億500万円 (23.4%)		約2億2200万円 (49.4%)
合計	被害額	約1億8400万円 (32.6%)	約2億5700億円 (45.5%)	約1億2000万円 (21.2%)	約400万円 (0.6%)	約5億6400万円 (100.0%)
	実被害額	約1億6000万円 (35.9%)	約1億7200万円 (38.5%)	約1億1100万円 (24.8%)	約400万円 (0.8%)	約4億4600万円 (100.0%)

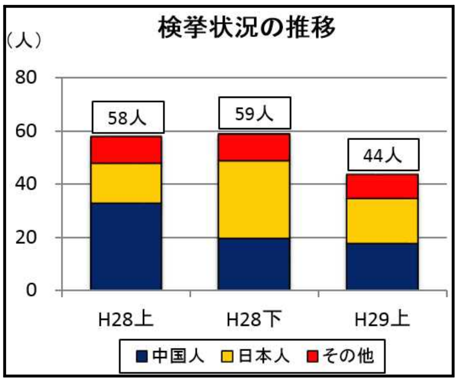
(6) 一次送金先口座名義人の国籍

	H28上		H28下		H29上	
中　国	745	63.2%	147	27.1%	87	23.3%
ベトナム	208	17.6%	230	42.4%	191	51.1%
日　本	136	11.5%	83	15.3%	42	11.2%
その他	90	7.6%	83	15.3%	54	14.4%
合　計	1,179	100.0%	543	100.0%	374	100.0%



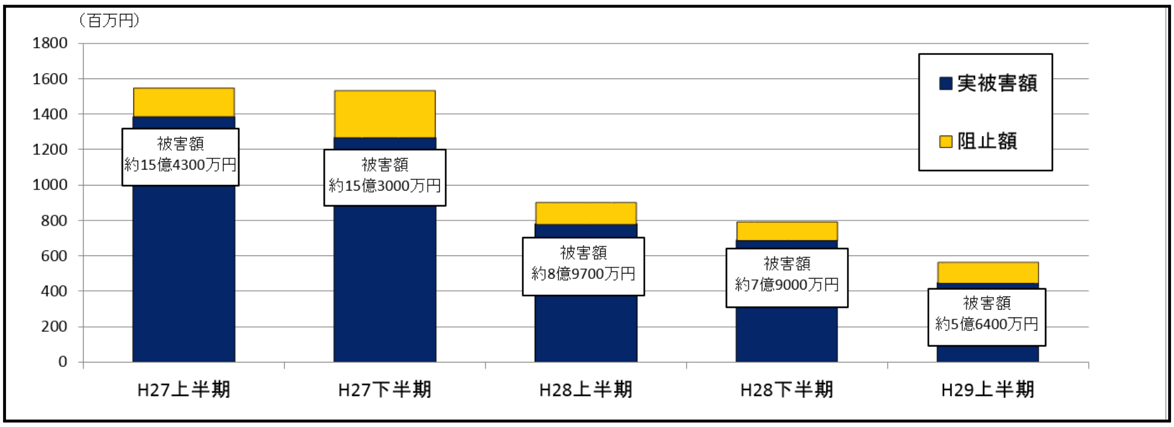
(7) 関連事件の検挙状況

		H28上		H28下		H29上	
検挙人数		58人		59人		44人	
内訳	中国人	33人	56.9%	20人	33.9%	18人	40.9%
	日本人	15人	25.9%	29人	49.2%	17人	38.6%
	その他	10人	17.2%	10人	16.9%	9人	20.5%



(8) 不正送金阻止状況

	被害額	実被害額	阻止額	阻止率
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%
H29上半期	約5億6400万円	約4億4600万円	約1億1800万円	20.9%



(9) 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）	43	26.5%	102	63.0%	17	10.5%	162
電子証明書（法人口座）	13	25.0%	35	67.3%	4	7.7%	52