広　報　資　料
平成28年９月15日
警　　察　　庁

平成28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

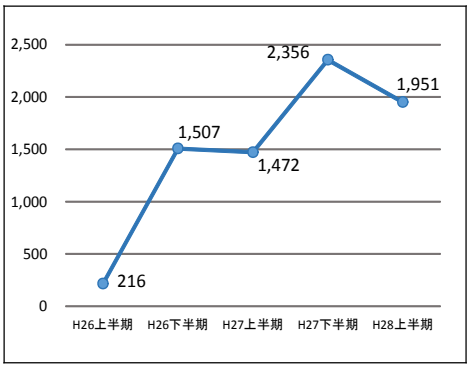
１　サイバー攻撃の情勢等

○　警察が報告を受けた標的型メール攻撃は1,951件（前期比－405件）。

　このうち、これ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」形式ファイルが472ファイルに急増。

○　攻撃ツールを用いて地方公共団体のサーバに対してDoS攻撃を行った少年を電子計算機損壊等業務妨害罪により検挙（５月、大阪）。

○　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。



【標的型メール攻撃の件数の推移】

２　サイバー犯罪の情勢等

○　サイバー犯罪の検挙件数、相談件数は増加。

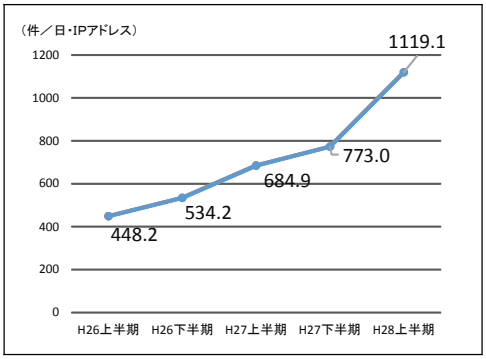
○　金融機関等と連携した取組により、インターネットバンキングに係る不正送金事犯による被害額は約９億円に減少（前期比－6.3億円）。

○　違法中継サーバや海外サーバを利用した事犯への対策を実施。

３　サイバー空間における探索行為

○ 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1,119.1件に増加（前期比＋346.1件）。

○　ルータや監視カメラ等のLinux系OSを使用する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が著しく活発化。



【センサーに対するアクセス件数の推移】

４　今後の取組

○　人材育成（サイバーセキュリティコンテストの実施、教養体系の見直し等）

○　官民連携（日本サイバー犯罪対策センターとの連携強化、中小事業者のサイバーセキュリティ対策への支援等）

○　国際連携（インターポールにおける共同捜査訓練への参加と情報共有等）

○　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）

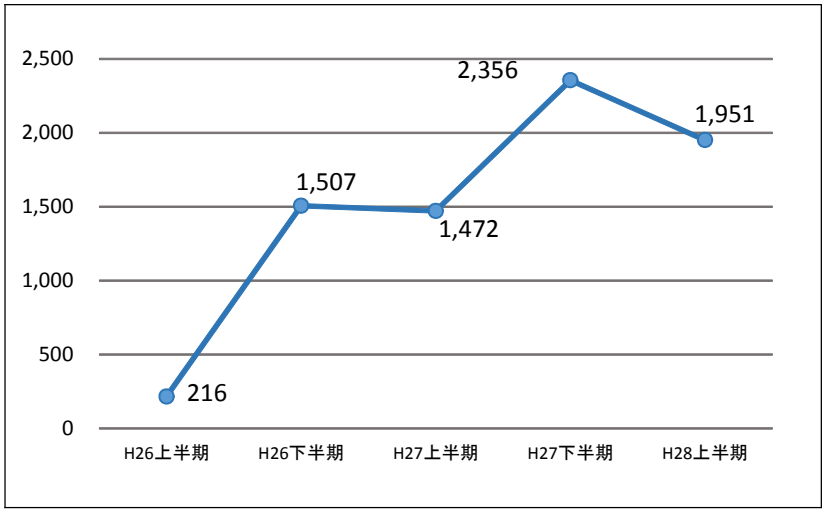
別　添

平成28年上半期におけるサイバー空間をめぐる脅威の情勢

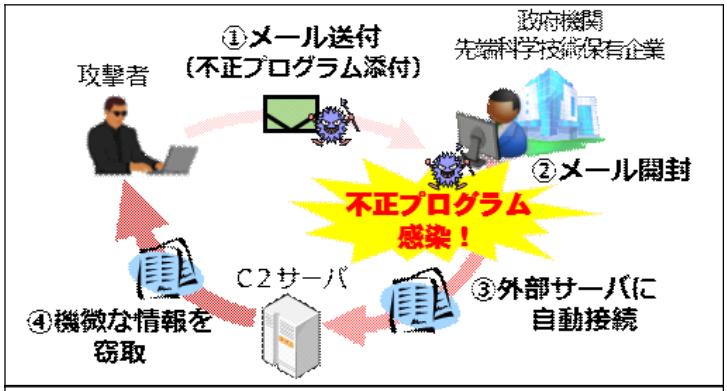
1　サイバー攻撃の情勢

(1) 概況

警察がサイバーインテリジェンス情報共有ネットワーク*1 を通じて把握した標的型メール攻撃の件数は1,951件で、27年下半期より405件減少した。



【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、我が国の政府機関や地方公共団体、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、36組織に関してSNS上に犯行声明とみられる投稿をしている状況を把握している。

---

*1　警察と先端技術を有する全国7,402の事業者等（平成28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。

(2) 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85%を占めた。

	ばらまき型	ばらまき型以外
27年上半期	92%(1,347件)	8%(125件)
27年下半期	92%(2,161件)	8%(195件)
28年上半期	85%(1,667件)	15%(284件)

【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

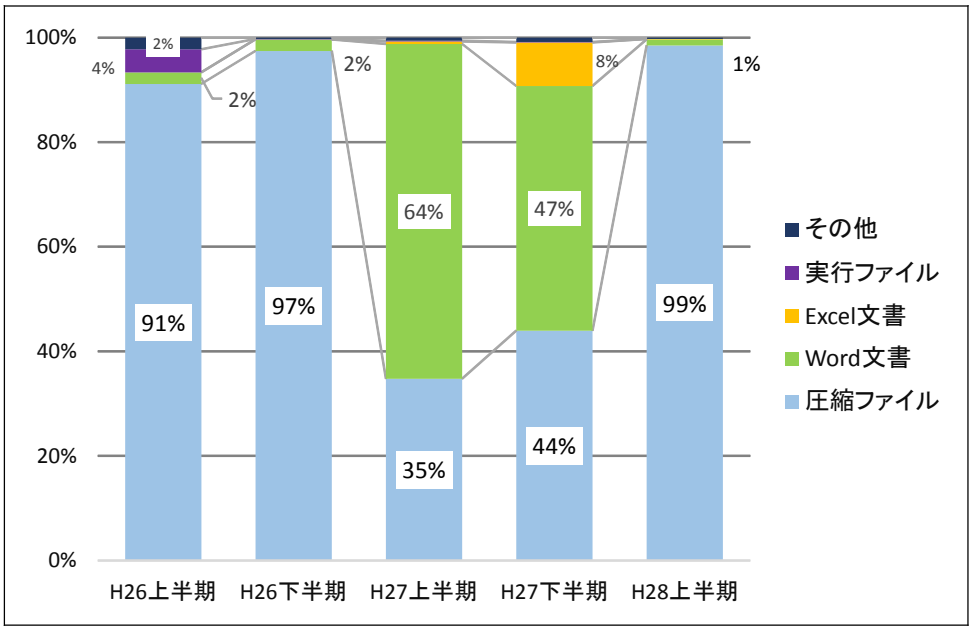
標的型メール攻撃の送信先メールアドレスについては、インターネット上で公開されていないものが全体の81%を占めており、攻撃者が攻撃対象の組織や職員について調査し、周到な準備を行った上で攻撃を実行している様子がうかがえる。

○ 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91%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

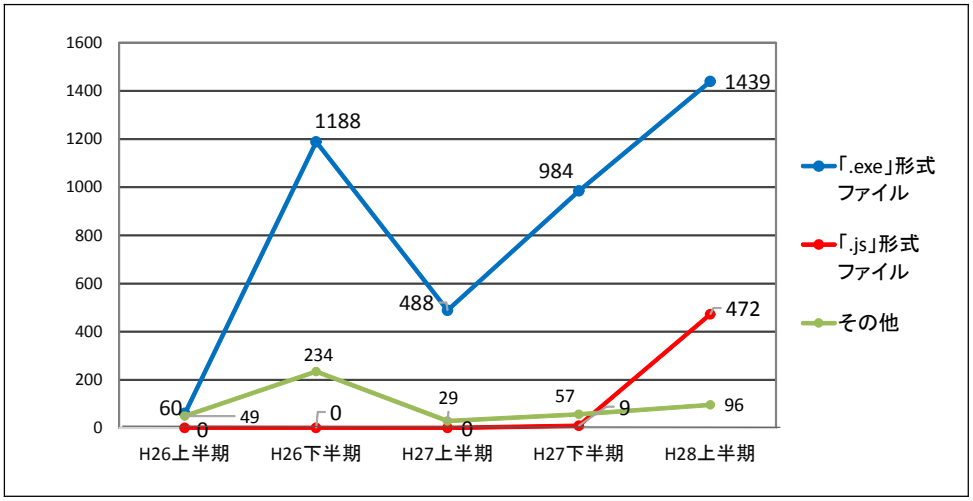
標的型メールに添付されたファイル形式の割合については、圧縮ファイルが添付されたものが27年下半期の44%から99%に増加した。



【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の中では、「exe」形式ファイルが最も多いが、これまでほとんど報告のなかった「.js」形式ファイルが472ファイルで、27年下半期より463ファイル増加した。



【圧縮ファイルで送付されたファイル形式の推移】

(3) サイバー攻撃への対策

【検挙事例】

27年11月、大量のアクセスにより地方公共団体が管理していたホームページが閲覧不能になる事案（DoS攻撃事案）が発生した。

同地方公共団体から被害の申告を受け、所要の捜査を行った結果、28年５月、電子計算機損壊等業務妨害容疑で高校生（16）を検挙した。（大阪）

【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[*2] 20台の機能停止（テイクダウン）を実施した。

(4) 伊勢志摩サミット等へのサイバー攻撃対策

28年５月に開催された伊勢志摩サミット等では、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。

---

*2　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

(1) 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による被害は、発生件数857件、被害額約８億9,800万円で、27年下半期と比較して、発生件数は117件上回ったが、被害額は約６億3,200万円下回った。

被害の特徴としては、27年下半期と比較して、信用金庫の被害額が大幅に減少（－約３億3,200万円）したこと、都市銀行等の被害額は法人口座については減少（－約３億2,700万円）したものの個人口座については増加（＋約３億200万円）したこと等が挙げられる。

取組状況として、口座売買等の関連事件を検挙しているほか、新たな手口等被害防止に直結する情報の金融機関への提供、新たな不正送金ウイルスの分析と迅速な被害防止措置の実施、日本サイバー犯罪対策センター（ＪＣ３）と連携したフィッシングサイトの早期把握等を実施している。

(2) 違法中継サーバ・海外サーバ利用事犯

○　違法中継サーバ関連

【対策事例】

27年11月に検挙した中継サーバ事業者から押収した中継サーバコンピュータを分析したところ、同サーバコンピュータから、連続自動入力プログラム97個とともに、31社の企業サイトに対する同プログラムによる不正ログイン攻撃に利用されたと認められるアカウント情報（約1,800万件）を発見した。

同プログラムを解析することにより、中継サーバを利用した不正アクセス行為の実態を解明したほか、不正アクセスの対象となった31社に対し、情報を提供して被害確認を行うとともに、認証機能の強化など不正アクセス事案の被害防止対策について要請した。（警視庁、埼玉、茨城、千葉、神奈川、長野、岐阜、大阪、兵庫、奈良、岡山、広島、愛媛、熊本、北海道）

○　海外サーバ関連

【検挙事例】

28年２月、フィリピン共和国に設置されたサーバで運営していたオンラインカジノについて、運営者ら６名を常習賭博罪等で検挙し、賭客５名を単純賭博罪で検挙した。さらに、フィリピンに逃亡中の首魁についても国際手配を実施し、逮捕により組織の全容解明と壊滅を図った。（千葉）

【国際連携の取組】

28年７月中旬から、海外サーバに開設された偽サイト等による詐欺等の被害を抑止するため、ウェブブラウザ事業者等が加盟する国際的な団体であるＡＰＷＧ[*3] への情報提供を開始した。これにより、ウイルス対策ソフト等を導入していない利用者に対してもウェブブラウザによる警告表示が可能となった。

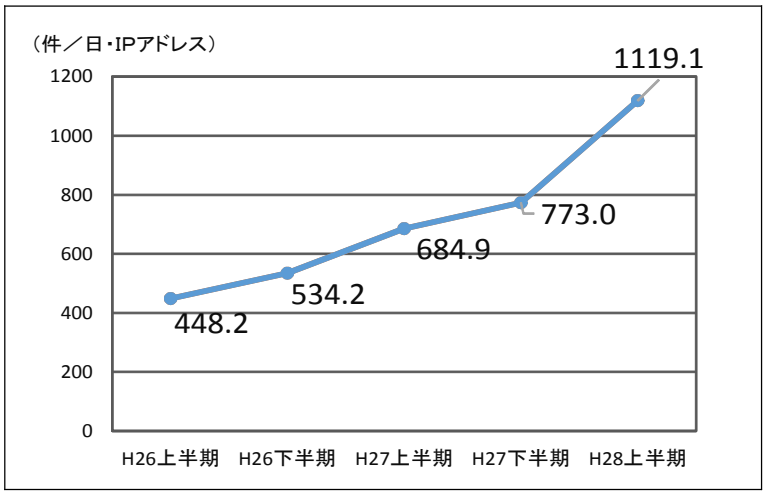
---

*3　Anti-Phishing Working Groupの略。国際的なフィッシング対策の非営利団体として米国において平成15年に設立。ウェブブラウザ事業者、金融機関、小売業者、プロバイダ、法執行機関、政府機関、大学等全世界で2,000以上の企業団体が参加。

３　サイバー空間における探索行為

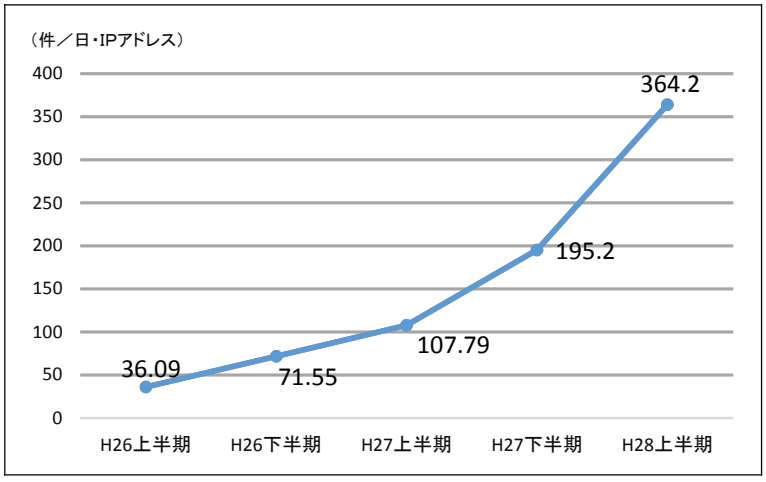
(1) センサー[*4] に対するアクセスの概況

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1,119.1件で、27年下半期より346.1件増加した。



【センサーに対するアクセス件数の推移】

アクセス件数の主な増加要因は、ルータや監視カメラといったLinux系OSが組み込まれた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見られる特定のポート[*5] 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。



【宛先ポート「23/TCP」に対するアクセス件数の推移】

---

*4　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　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）

また、公表されたApache Struts 2 [*6] の深刻な脆弱性を標的とする攻撃活動、国内メーカー製のPLC[*7] を始めとした産業制御システムに対する探索行為及びIP電話機で使用されるサーバ等に対する探索行為も観測されている。

(2) 不正プログラム解析の推進

○　解析事例

【日本サイバー犯罪対策センター（ＪＣ３）と連携した対策】

インターネットバンキングの暗証番号、クレジットカード情報等を窃取することを目的に作成された不正プログラムを解析した。

解析結果等を踏まえ、感染端末の接続先である指令サーバを特定し、迅速に同サーバの機能停止を実施したほか、日本サイバー犯罪対策センター（ＪＣ３）と連携し、インターネット利用者等に対し注意喚起を実施した。

【通信記録が偽装される措置が講じられた不正プログラムの解析】

被害者の端末に感染した不正プログラムを解析したところ、攻撃の追跡を困難にする目的で、指令サーバからの通信内容に係る記録が偽装される措置が講じられていることを把握した。

解析結果等を踏まえ、同様の攻撃を無害化する方法等について、ネットワーク管理者等に対し注意喚起を行った。

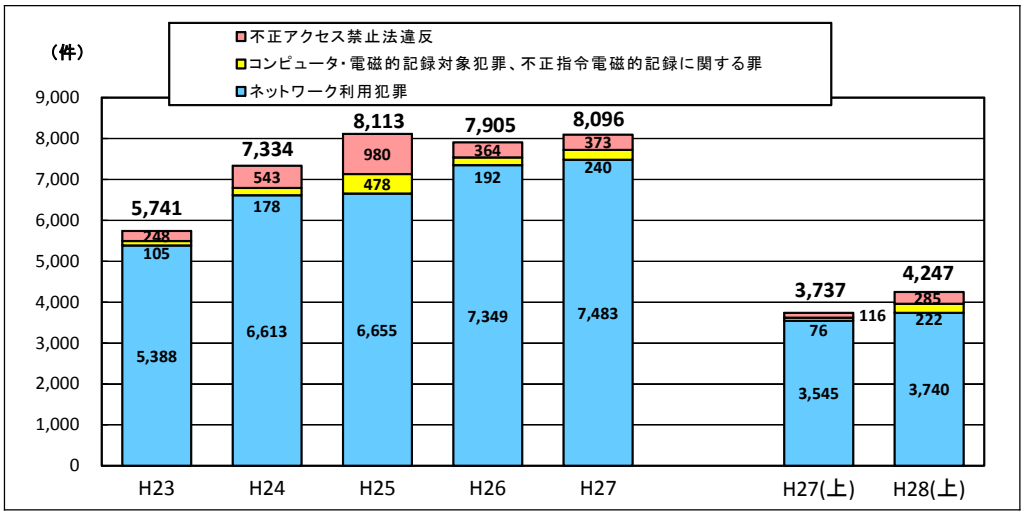
---

*6　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。

＊7　Programmable Logic Controllerの略。プログラム可能なフィールド機器（バルブ、メータ、ファン等）の監視・制御装置のこと。

【　参　考　】

1　サイバー犯罪の検挙件数の推移



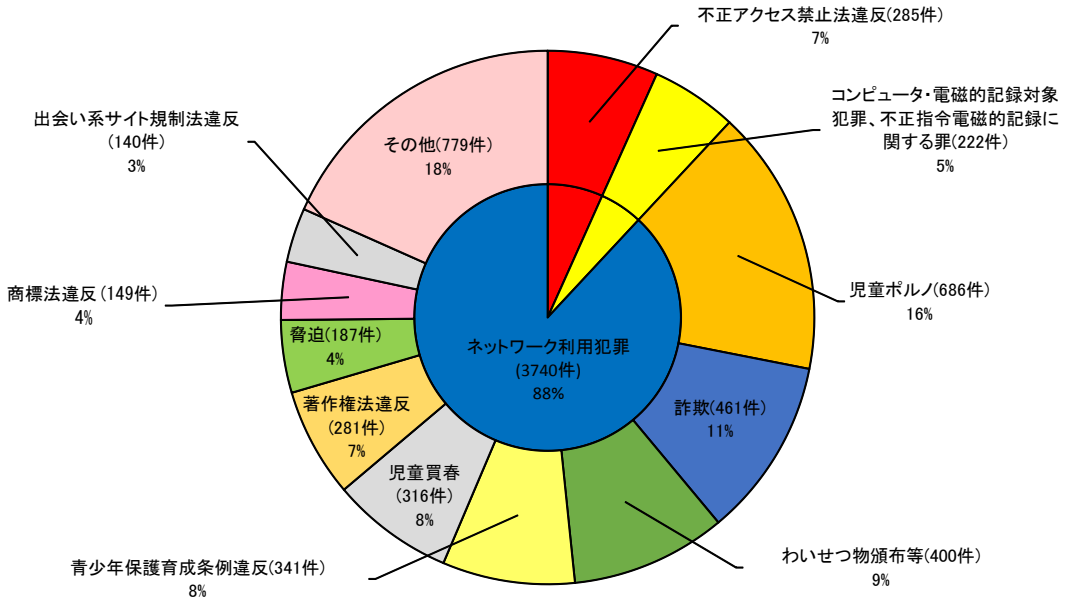
※ H28（上）は暫定値

2　検挙件数の内訳

罪名＼年	H23	H24	H25	H26	H27	H27（上）	H28（上）
不正アクセス禁止法違反	248	543	980	364	373	116	285
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	105	178	478	192	240	76	222
電子計算機使用詐欺	79	95	388	108	157	47	197
電磁的記録不正作出・毀棄等	17	35	56	48	32	12	9
電子計算機損壊等業務妨害	6	7	7	8	6	4	6
不正指令電磁的記録作成・提供		4	8	9	8	3	
不正指令電磁的記録供用	1	34	14	16	21	8	5
不正指令電磁的記録取得・保管	2	3	5	3	16	2	5
ネットワーク利用犯罪	5,388	6,613	6,655	7,349	7,483	3,545	3,740
児童買春・児童ポルノ法違反（児童ポルノ）	883	1,085	1,124	1,248	1,295	563	686
詐欺	899	1,357	956	1,133	951	344	461
うちオークション利用詐欺	389	235	158	381	511	144	115
わいせつ物頒布等	699	929	781	840	835	387	400
青少年保護育成条例違反	434	520	690	657	693	344	341
児童買春・児童ポルノ法違反（児童買春）	444	435	492	493	586	289	316
著作権法違反	409	472	731	824	593	304	281
脅迫	81	162	189	313	398	198	187
商標法違反	212	184	197	308	304	161	149
出会い系サイト規制法違反	464	363	339	279	235	112	140
その他	863	1,106	1,156	1,254	1,593	843	779
合　　計	5,741	7,334	8,113	7,905	8,096	3,737	4,247

※ H28（上）は暫定値

３　ネットワーク利用犯罪の内訳



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】

○　無職の少年（17）は28年１月、高校生の少年（16）は同年５月、県の教育関係機関が設置、管理するシステムに不正アクセスしてサーバ内の情報を不正に入手するなどした。28年６月までに、不正アクセス禁止法違反で検挙した。（警視庁、佐賀）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　簡易宿所経営の男（54）らは、27年４月、旅行会社のインターネットサイトに、簡易宿所に宿泊する意思がないにも関わらず、ポイント利用による架空の宿泊情報を入力し、同社から宿泊料金を詐取した。28年２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保管等】

○　少年（14）は、匿名掲示板に不正送金ウイルスや遠隔操作ウイルス等を販売する旨の広告を出して顧客を募り、購入申込みをした少年らにウイルスを提供するなどした。27年12月、ウイルスを提供した少年を不正指令電磁的記録提供等で検挙するとともに、提供を受けた少年６名を不正指令電磁的記録取得等で検挙した。さらに、28年５月、ウイルスの動作検証などを行っていた大学職員の男（26）を、不正指令電磁的記録保管・同提供幇助・同供用幇助で検挙した。（警視庁、福島、千葉、愛知、滋賀）

ネットワーク利用犯罪

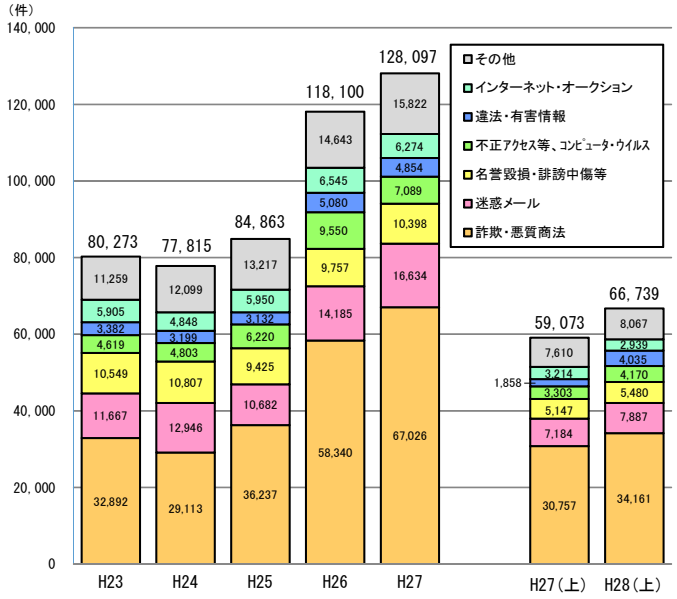
【威力業務妨害】

○　少年（14）は、タブレット端末を使用して、電子掲示板にＡ小学校に小型時限爆弾を仕掛けた旨を複数回にわたり掲載し、Ａ小学校の業務を妨害した。28年６月、威力業務妨害で検挙した。（千葉）

【児童買春・児童ポルノ法違反】

○　スマートフォン用画像共有アプリ運営会社代表取締役の男（55）らは、27年10月、画像投稿者の少年（14）らと共謀の上、同アプリのサーバに児童ポルノ画像を蔵置し、投稿者が設定した合言葉を入力することで受信、閲覧することが可能な状況に設定して児童ポルノ画像等を公然と陳列した。28年２月、児童買春・児童ポルノ法違反等で検挙した。（神奈川）

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

	H23	H24	H25	H26	H27	H27（上）	H28（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）	32,892	29,113	36,237	58,340	67,026	30,757	34,161
迷惑メールに関する相談	11,667	12,946	10,682	14,185	16,634	7,184	7,887
名誉毀損・誹謗中傷等に関する相談	10,549	10,807	9,425	9,757	10,398	5,147	5,480
不正アクセス等、コンピュータ・ウイルスに関する相談	4,619	4,803	6,220	9,550	7,089	3,303	4,170
違法・有害情報に関する相談	3,382	3,199	3,132	5,080	4,854	1,858	4,035
インターネット・オークションに関する相談	5,905	4,848	5,950	6,545	6,274	3,214	2,939
その他	11,259	12,099	13,217	14,643	15,822	7,610	8,067
合　　計	80,273	77,815	84,863	118,100	128,097	59,073	66,739

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

・　出会い系サイト等の広告メールが大量に届く。
・　身に覚えのない懸賞金の当選を通知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。
・　自分の顔写真を使用されたコミュニティサイトのアカウントが作成され、なりすまされている。

不正アクセス等、コンピュータ・ウイルスに関する相談

・　身代金要求型ウイルス「ランサムウェア」に感染してコンピュータがロックされ、それを解除するために金銭の支払いを要求された。
・　無料通話・メールアプリのアカウントを乗っ取られ、知人に対して電子マネーの購入を勝手に依頼されていた。