広　報　資　料
平成28年３月17日
警　　察　　庁

平成27年におけるサイバー空間をめぐる脅威の情勢について

１　サイバー攻撃の情勢

○　日本年金機構を始めとする我が国の多数の機関、事業者等でサイバー攻撃による情報窃取等の被害が発生。

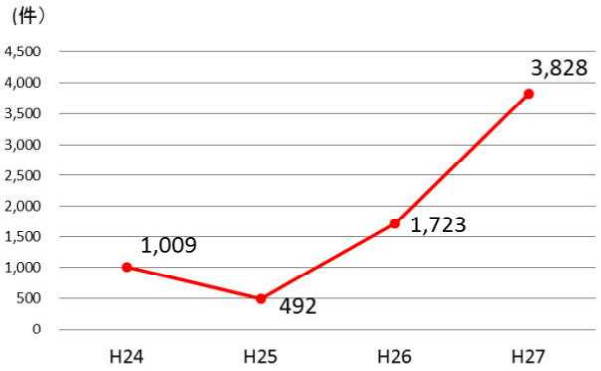
○　平成27年中に警察が連携事業者等から報告を受けた標的型メール攻撃は3,828件と過去最多。Word文書形式のファイルを添付したものが急増、過半数を占める。

○　９月以降、地方公共団体、報道機関、空港、水族館等のウェブサイトの閲覧障害事案が頻発。「アノニマス」を名乗る者が、58組織に関し、犯行声明とみられる投稿をSNS上に掲載。

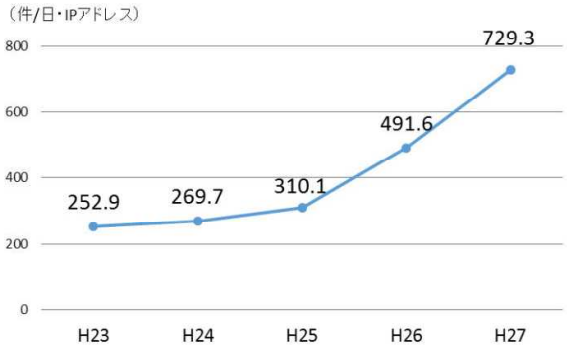
２　サイバー空間における探索行為

○　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729.3件。

○　ルータや監視カメラ等の組込み機器を標的とした探索行為等が増加。



【標的型メール攻撃の件数】



【センサーに対するアクセス件数】

３　サイバー犯罪の情勢

○　平成27年中の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は約30億7,300万円で、過去最高であった昨年を更に上回った。

○　国境を越えて行われるサイバー犯罪に係る事件を検挙。

・　海外からの接続を取り次ぐ中継サーバ事業者による不正アクセス事件

・　海外サーバを利用したわいせつ電磁的記録記録媒体陳列事件　等

４　今後の取組

○　官民連携（日本サイバー犯罪対策センターとの共同オペレーションの実施、都道府県警察における産官学連携による中小企業対策等）

○　国際連携（インターポールへの職員派遣による情報交換等）

○　態勢整備・人材育成（都道府県警察が参加するサイバーセキュリティコンテストの実施等）

1　サイバー攻撃

(1) 概況

平成27年は、日本年金機構を始めとする我が国の多数の機関、団体、事業者等において、サイバー攻撃による情報窃取等の被害が発生した。

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[*1]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、27年中、3,828件の標的型メール攻撃が発生したことを把握した。

また、同年９月以降、我が国の地方公共団体、報道機関、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頻発した。警察では、国際的ハッカー集団「アノニマス」を名乗る者が、27年中に58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。

警察では、関係機関と連携しつつ、サイバー攻撃による被害の未然防止・拡大防止を図るとともに、サイバー攻撃の実態解明を推進している。

【標的型メール攻撃の概要】

(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

平成27年中は、26年下半期から引き続き、「ばらまき型」攻撃が多数発生し、全体の約92%を占めた。その多くは、品物の発送代金の請求等の業務上の連絡を装ったものであった。

	ばらまき型	ばらまき型以外
25年中	53%（　259件）	47%（　233件）
26年中	86%（1,474件）	14%（　249件）
27年中	92%（3,508件）	８%（　320件）

【ばらまき型とそれ以外の標的型メール攻撃の割合】

---

*1　警察と先端技術を有する全国7,333の事業者等（28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。

○　大多数が非公開メールアドレスに対する攻撃

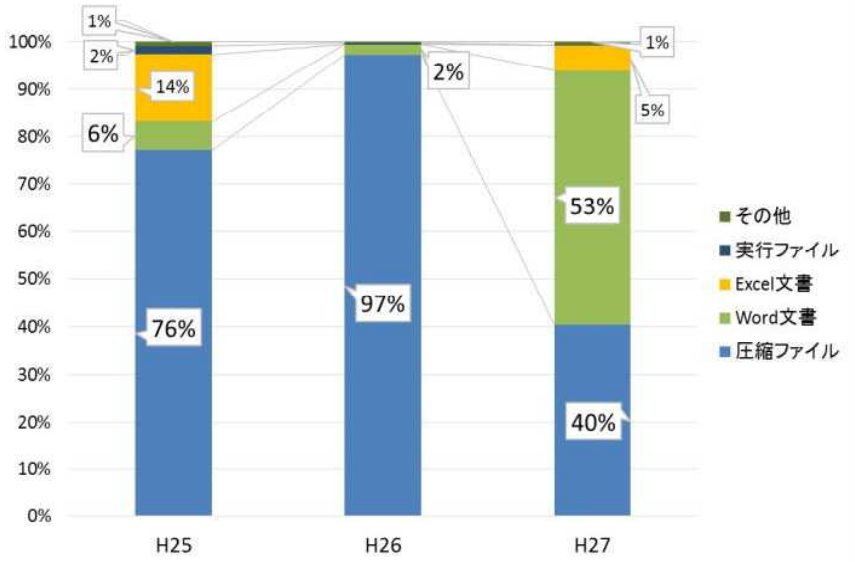
標的型メール攻撃の送信先メールアドレスについては、インターネット上で公開されていないものが全体の89%を占めており、攻撃者が攻撃対象の組織や職員について調査し、周到な準備を行った上で攻撃を実行している様子がうかがえる。

○　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77%を占めた。

○　Word文書を添付した攻撃の急増

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、Word文書が添付されたものが前年の２%から53%に大幅に増加した。その多くは、複合機[*2] のスキャナ機能により読み込んだ文書の送付や品物の発送代金の請求等の業務上の連絡を装ったものであった。



【標的型メールに添付されたファイル形式の割合】

標的型メールに添付されたWord文書には、受信者が当該文書を開くと、情報窃取等を行う不正プログラムが自動的にダウンロードされ、コンピュータが当該不正プログラムに感染するものが確認されている。このとき、画面上には正当なものを装った文書の内容が表示されているため、当該感染に気付きにくくなっている。

---

*2　プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器。

(3) 標的型メール攻撃の事例

昨今の電子機器の機能を踏まえた攻撃として、27年６月以降、複合機のスキャナ機能により読み込んだ文書の送付を装った標的型メール攻撃を継続して把握した。

この攻撃では、送信元メールアドレスが「scanner@[攻撃対象の事業者等のドメイン].jp」、「noreply@[攻撃対象の事業者等のドメイン].jp」等と偽装され、あたかも社内の複合機から文書が送付されたように装われていた。また、その多くには(2)に記載したWord文書が添付されていたが、11月には同様の機能を持つExcel文書が添付されたものも確認された。

(4) 警察における対策

○　実態解明の推進

警察では、違法行為に対する捜査を推進するとともに、サイバー攻撃を受けたコンピュータや不正プログラムを解析するなどして、攻撃者及び手口に係る実態解明を進めている。

また、外国治安情報機関との情報交換を行うとともに、ＩＣＰＯ（国際刑事警察機構）を通じるなどして、海外の捜査機関との間で国際捜査協力を積極的に推進している。

【実態解明事例】

政府機関に対する不正アクセス事件に関して、犯行に使用されたレンタルサーバの契約に際し、当時日本に留学生として在留していた中国籍の男性が、氏名、住所、生年月日等、虚偽の情報により会員登録を行っていた事実が判明したことから、27年11月、警視庁は同人を私電磁的記録不正作出・同供用罪により検挙した。

同人は、これまで1,000台以上のレンタルサーバを契約した上、主に海外に居住する利用者に利用させて利益を上げていたとみられ、これらのレンタルサーバのうち数台は、他のサイバー攻撃において踏み台として悪用されたとみられており、警視庁で実態解明を進めている。

○　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

平成27年中、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[*3] 48台の機能停止（テイクダウン）を実施し、昨年中の33台を上回った。

---

*3　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。

これらC2サーバは、攻撃者が事業者等のウェブサイトを運営するサーバに対して何らかの方法で不正アクセス行為を実施し、C2サーバ機能を有するプログラムを密かに設置することにより構築されたものと考えられる。

また、警察では、これらC2サーバに対する接続記録の分析から、不正プログラムに感染したコンピュータを新たに発見し、当該コンピュータの管理者等に対して個別に注意喚起を行うことにより、被害の拡大防止を図った。

(5) 被害防止対策

近年の標的型メール攻撃の傾向を踏まえた対策としては、

○　不審なメールを安易に開封しないこと

○　端末やサーバに導入している各種ソフトウェア（基本ソフト（OS）、サーバ構築用ソフト、文書作成ソフト、ウイルス対策ソフト等）を最新の状態に維持すること

○　送信元メールアドレスを詐称する手口への対策として、SPF[*4] 等の送信ドメイン認証技術を導入し、電子メールの受信側メールサーバにおいて送信元メールアドレスの正当性を確認すること

等が有効と考えられるが、これらの対策を執ってもなお、不正プログラムの感染を完全に防ぐことは困難である。そのため、不正プログラムの感染を前提として、機微な情報の暗号化、アクセス権の適切な設定、ネットワークの分離といった被害軽減のための対策を複層的に講じることが必要である。

2　インターネットにおけるアクセス情報等の観測結果

(1) 概況

警察庁では、リアルタイム検知ネットワークシステムを24時間体制で運用し、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情報等を集約・分析している。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アクセスを検知している。

平成27年の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729.3件で、前年と比べ約1.5倍に増加した。

主な増加の要因は、宛先ポート23/TCP[*5] に対するアクセスが大幅に増加したことによるものであり、IoT[*6] の普及に伴い脅威の増加が懸念されるルー

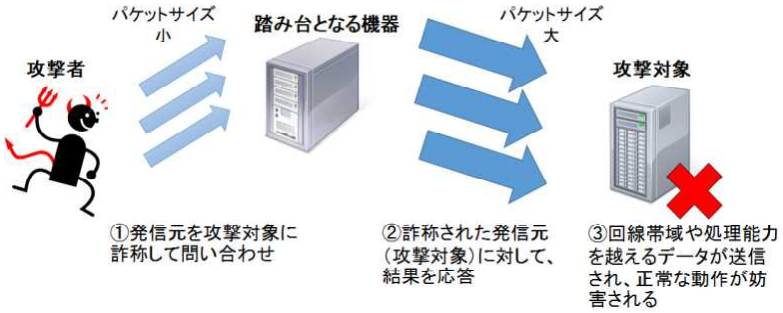
---

*4　Sender Policy Frameworkの略。電子メールの送信元メールアドレスのドメインの正当性を確認することができる仕組み。

*5　ネットワークに接続された機器を遠隔で操作する通信プロトコルTelnetで利用されているポートのこと。

*6　Internet of Thingsの略。

タ、監視カメラ等のLinux系のOSが組み込まれた機器を標的とする探索行為や同機器を踏み台としたアクセスが多数確認されている。また、27年には、依然として脅威が懸念される産業制御システムで使用されるPLC[*7] 等に対する探索行為及びDoS攻撃の一手法であるリフレクター攻撃[*8] に悪用可能な機器の探索行為を確認した。



【リフレクター攻撃の原理】

(2) 被害防止対策

ブロードバンドルータ等個人で利用している機器であっても、不正にアクセスされたり、攻撃の踏み台となったりするおそれがあるため、最新のセキュリティ情報を定期的に確認し、適切な設定を行うなど、利用者自らがセキュリティ意識を高く持ってこれらの機器を管理する必要がある。

また、産業制御システムやサーバ等をインターネットに接続する際には、その必要性を検討し、不要なインターネット接続を行わないことが重要である。インターネットに接続する場合には、ID・パスワードやアクセス権を適切に設定する必要がある。

3 インターネットバンキングに係る不正送金事犯

(1) 概況

平成26年、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過去最高の約29億1,000万円となったが、その脅威は27年に入っても続いており、27年中の被害額は、約30億7,300万円と26年を更に上回った。

被害の特徴としては、被害金融機関数が倍増し、特に信用金庫、信用組合に被害が拡大したこと、農業協同組合と労働金庫で被害が発生したこと等が挙げられる。

---

*7 Programmable Logic Controler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。

*8 踏み台となる機器に送信する問い合わせと比較して、当該機器からの応答が大きくなる通信プロトコルを悪用して、発信元IPアドレスを攻撃対象に詐称した問い合わせをすることにより、攻撃対象に大量のデータを送信する攻撃手法のこと。

(2) 被害防止対策

金融機関関連情報を窃取する機能を持つ不正プログラムは数多くあり、新たな手口も次々と出現していることから、インターネットバンキング利用者は、被害に遭わないために、以下の対策を講じる必要がある。

○　ウイルス対策ソフトの導入及び最新のパターンファイルへ更新する。

○　基本ソフト（OS)、ウェブブラウザ等各ソフトウェアを最新の状態へ更新する。

○　インターネットバンキングにアクセスした際に不審な入力画面等が表示された場合、ID、パスワード等を入力せずに金融機関等へ通報する。

○　可変式パスワード生成機（ハードウェアトークン）等によるワンタイムパスワードを利用する。

○　メールで受信する形式のワンタイムパスワードを利用する際、パソコンの不正プログラム感染等により情報が流出するおそれがあるため、メールの受信先に携帯電話のメールアドレス等を登録する。

○　金融機関が二経路認証やトランザクション認証など高度なセキュリティ対策を導入している場合は、これらを利用する。

○　不審なログイン履歴や、自己口座の送金状況等がないか、頻繁に確認する。

4　国境を越えて行われるサイバー犯罪

(1) 概況

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着し、サイバー空間が国民の日常生活の一部となる一方、サイバー犯罪は国外の被疑者によって敢行されたり、海外のサービスを経由・利用して行われており、サイバー空間における脅威は国内だけで全て対処できるものではなくなってきている。

国境を越えて行われるサイバー犯罪に係る事件として、27年中には下記の事例を検挙している。

(2) 事例

【違法中継サーバ対策】

インターネット接続を取り次ぐ中継サーバについては、利用者のIPアドレスが置き換わるなどの特性を有しており、その匿名性から犯罪インフラとなっている実態がある。

平成27年11月、15都道府県警察合同捜査本部において、他人の認証IDを不正利用してインターネット接続していた日本国内の中継サーバ事業者による不正アクセス事件を検挙した。被疑者らは、中国からのインターネット接続を取り次ぐための中継サーバ事業を日本国内で営む会社の経営者や社員であ

り、同年６月下旬ころ、インターネット接続事業者が第三者を正規利用権者として付与した認証ID・パスワードを不正利用して不正アクセス行為をしていた。

また、中継サーバ事業者の通信回線は、被疑者の検挙後も契約が継続されたままで、サーバを接続すれば直ちに事業が再開できる環境にあり、犯罪被害の拡大防止の観点から回線契約を解除する必要性があったことから、悪質な中継サーバ事業者への対策として、大手通信事業者に働き掛けを行った結果、同年12月、事業者が契約約款を改正し、契約解除に応じることとなった。

【海外サーバ利用犯罪】

海外サーバは匿名性が高く、サイバー犯罪の隠れ蓑として利用されるなか、インターネットバンキングに係る不正送金事犯の被害原因の多くがウイルス感染によるものであり、アダルトサイトが感染源の一つになっていると指摘される状況にあり、取締りを強化している。

27年11月、茨城県警察など18都道府県警察において、海外サーバを利用したアダルトアフィリエイトサイトに係る一斉集中取締りを実施し、わいせつ電磁的記録記録媒体陳列により13人を検挙した。一斉集中取締りは、一般財団法人日本サイバー犯罪対策センター（ＪＣ３）の協力を得て実施した。

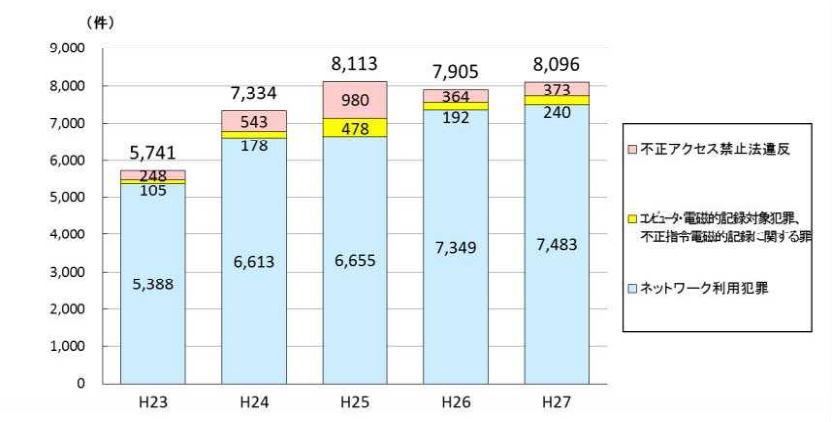
このほか、京都府警察において、発売前の週刊漫画雑誌の誌面をデジタル化した上で海外サイトに蔵置してインターネット利用者に無料公開していた被疑者６人を著作権法違反で検挙した。

【サイバー犯罪捜査における国際連携】

27年５月以降、DD4BC等と名乗って金融機関、IT企業等のサーバにDDoS攻撃を仕掛け、当該攻撃回避のための支払いをビットコインで要求する恐喝未遂事件が発生した。同種手口事案は海外でも発生していたことから、ユーロポール及び国際刑事警察機構（ICPO）の調整の下、国際捜査が行われ、ボスニア・ヘルツェゴビナ警察等が関連する被疑者２名を検挙した。

【 参 考 】

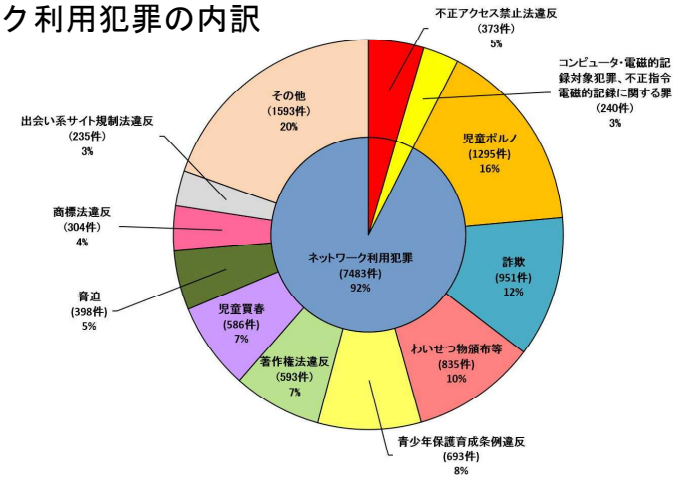
1　サイバー犯罪の検挙件数の推移



2　検挙件数の内訳

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

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（19）は27年２月、インターネットの会員向けサービスに掲示板サイトから入手した他人のID及びパスワードを入力して不正アクセスし、登録メールアドレスを変更した。27年10月、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用で検挙した。（神奈川）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　パート従業員の女（53）らは、25年11月、勤務先で知り得た他人のクレジットカード情報を、インターネットオークションで落札した代金の支払いに使用した。27年10月、電子計算機使用詐欺で検挙した。（山梨）

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】

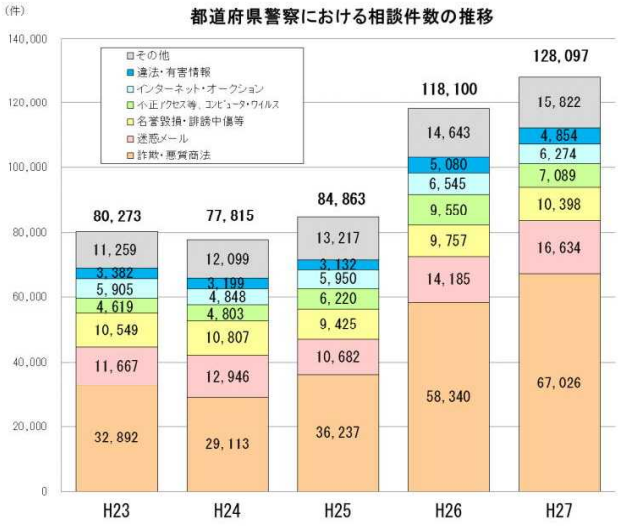
○　少年（18）は、匿名化通信ソフトを使用し、Ａ社が管理するサーバコンピュータに、Ｂ社を利用権者として付された識別符号を入力して不正アクセスするなどした。更に同人は、27年６月ころ、身代金要求型ウイルス「ランサムウェア」を第三者に配付する目的で、同ウイルスの作成ツールを保管していた。27年８月、不正指令電磁的記録保管等で検挙した。（警視庁）

ネットワーク利用犯罪

【商標法違反及び詐欺】

○　出会い系サイト運営者の男（42）らは、同人が運営する出会い系サイトへの集客目的で、何ら権限がないのに、無料通話アプリ事業者が商標登録を受けている商標に類似する商標を掲載したウェブサイトを開設した。27年５月、商標法違反で検挙した。その後、同出会い系サイトにおけるサクラを利用した組織的詐欺を解明し、組織を壊滅した。（千葉）

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
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
迷惑メールに関する相談	11,667	12,946	10,682	14,185	16,634
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
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
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
違法・有害情報に関する相談	3,382	3,199	3,132	5,080	4,854
その他	11,259	12,099	13,217	14,643	15,822
合　　計	80,273	77,815	84,863	118,100	128,097

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商品を購入し、指定された口座へ代金を支払ったが、商品が届かず、相手とも連絡が取れない。
・　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

・　メールのフィルタリング設定を行っても、毎回ドメインが変更された大量の迷惑メールが届く。
・　身に覚えのない懸賞金の高額当選を通知するメールが送られてきた。

名誉毀損、誹謗中傷に関する相談

・　掲示板サイトに個人を誹謗中傷する内容を書き込まれた。
・　掲示板サイトに無断で顔写真を掲載された。

不正アクセス等に関する相談

・　オンラインゲームのアカウントを乗っ取られ、ゲーム内のアイテムを勝手に利用された。
・　無料通話・メールアプリのアカウントを乗っ取られ、勝手にメッセージを送信された。