広　報　資　料
平成27年３月12日
警　　察　　庁

平成26年中のサイバー空間をめぐる脅威の情勢について

１　特徴

(1)　手口の悪質・巧妙化

○　インターネットバンキングに係る不正送金事犯の被害が過去最大に。

○　情報窃取を目的とした、英文メールによる「ばらまき型」攻撃の増加、日本の制度を踏まえ巧妙に偽装された内容を含むメールの発生等を確認。

○　警察庁が設置したセンサーにおいて、攻撃パケットや攻撃の準備行為とみられる各種探索パケットを多数観測。

(2)　サイバー空間における犯罪インフラの存在

不正アクセスに悪用され得る中継サーバやDDoS攻撃に悪用され得るサービスが存在。

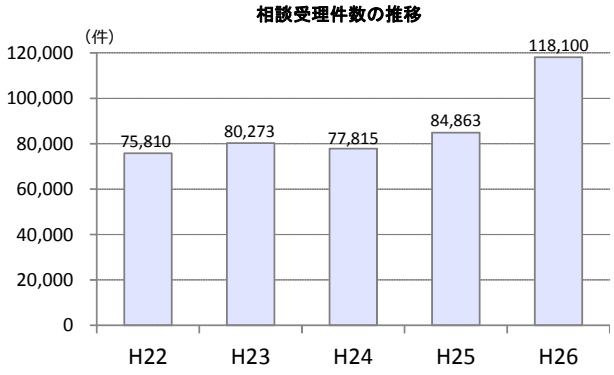
(3)　新たな技術・サービスの実社会への影響

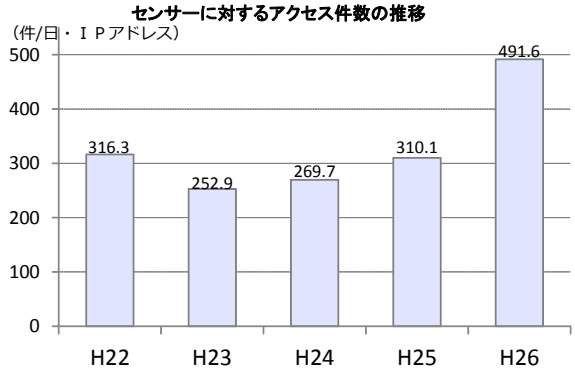
ビットコイン等の新たな技術・サービスが出現し、それらが犯罪のツールとして利用される可能性が拡大。

(4)　インターネット利用に係るリスクの拡大

インターネットにおける危険ドラッグの販路の存在、企業のウェブサイトに対するリスト型攻撃、偽サイト等に係る詐欺の多発等インターネット利用に係るリスクが拡大。

２　サイバー犯罪・サイバー攻撃の発生状況等





○　サイバー犯罪等に関する相談件数は11万8,100件(+3万3,237件、+39.2%)

○　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491.6件(+181.5件、+58.5%)

○　サイバー犯罪の検挙件数は7,905件(-208件、-2.6%)

・　ネットワーク利用犯罪の検挙件数は7,349件(+694件、+10.4%)

○　警察が把握した標的型メール攻撃は1,723件(+1,231件、+250%)

別添

平成26年中のサイバー空間をめぐる脅威の情勢

第１　総括

平成26年中は、サイバー犯罪[*1] の検挙件数は7,905件と、前年より208件（2.6％）減少した一方で、都道府県警察の相談窓口で受理したサイバー犯罪に関する相談件数は11万8,100件と、前年より３万3,237件（39.2％）増加し、過去最高の件数を記録した。また、26年中に警察が把握した標的型メール攻撃は、前年比約3.5倍となる1,723件に大幅に増加したほか、警察庁が観測したインターネット上の不審なアクセスは、１日・１IPアドレス当たり491.6件と、前年より58.5％増加し、サイバー空間における各種攻撃の試みが活発化している状況がうかがえた。

同年中におけるサイバー空間をめぐる脅威情勢には、下記のような特徴がみられた。

１　手口の悪質・巧妙化

対象とする組織やシステムの調査を入念に行い、不正プログラムやSNS等を駆使して金銭、機密情報等を窃取する手口がますます悪質・巧妙化している。

金銭の直接窃取を目的とするものとしては、インターネットバンキングに係る不正送金事犯において、発生件数が1,876件、被害額が約29億1,000万円に上り、過去最悪の被害となったほか、MITB攻撃[*2] と呼ばれる手口が確認された。

情報の窃取を目的とするサイバー攻撃としては、英文による「ばらまき型」の標的型メール攻撃が増加したほか、日本の制度を踏まえた内容のものや、特定分野の研究会等を装ったものなど、より巧妙な手口が確認された。また、それ以外にも、水飲み場型攻撃や、ソフトウェアの更新を装って不正プログラムに感染させる攻撃も発生するなど、情報の窃取を目的とするサイバー攻撃の手口は巧妙化・多様化している。

２　サイバー空間における犯罪インフラの存在

不正アクセスの温床となっている中継サーバや、目標のサーバに対して大量のデータを送り付ける有料サービス等、近年、サイバー空間における犯罪を助長し、又は容易にする基盤が着々と構築されていることが確認された。

３　新たな技術・サービスの実社会への影響

インターネット上に公開した銃の設計図データをダウンロードし、３Ｄプリンタを用いて実弾の発射が可能な拳銃を製造した事件や、匿名性が高く犯罪の各種取引に使用されているビットコインを利用して覚醒剤を購入した事件等、

---

*1　高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪

*2　２頁参照

新たな技術・サービスをめぐる事件が発生している。

4　インターネット利用に係るリスクの拡大

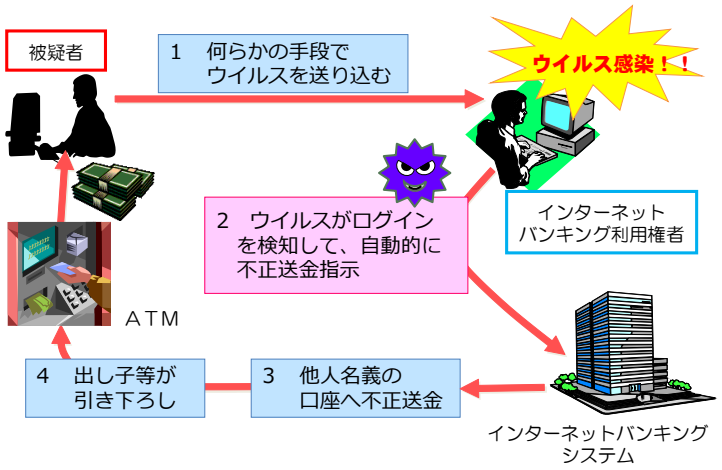
元交際相手に係る性的画像の掲載等が社会的な問題となった。また、街頭店舗に加え、インターネット上でも販路が存在する危険ドラッグが絡む事件や事故が相次いで発生した。さらに、様々な企業のウェブサイトに対する不正ログイン攻撃、無料通話アプリの乗っ取りによる電子マネー被害等、多くの利用者に関係し得る事案も発生した。

第２　手口の悪質・巧妙化

１　インターネットバンキングに係る不正送金事犯

平成25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が約14億600万円であったが、その脅威は拡大し続け、26年の被害額は過去最悪の約29億1,000万円となった。主な背景として、法人名義口座に係る被害が増加するとともに、多くの地域金融機関に被害が拡大したことが挙げられる。

また、26年に入りMITB（Man In The Browser[*3]）攻撃と呼ばれる、パソコンに感染したコンピュータ・ウイルスが、インターネットバンキングへのログインを検知し、自動的に不正送金する被害が確認されている。



【図２－１　MITB 攻撃の概要】

２　情報窃取を企図したサイバー攻撃

(1)　概況　－標的型メール攻撃件数は過去最高－

平成26年は、我が国の事業者等からの情報窃取を企図したとみられるサイバー攻撃が大幅に増加した。警察では、「サイバーインテリジェンス情報共有

---

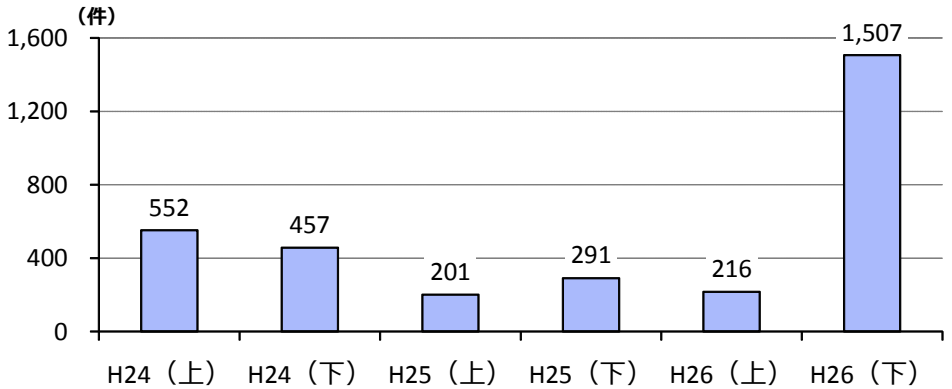
*3　あたかも人がウェブブラウザの中で監視を行っているかのように、コンピュータ・ウイルスがウェブブラウザ上の設定ファイルを変更して不正な通信を行うことから、この名がついたもの。

ネットワーク」[*4] を通じて標的型メール攻撃に係る情報を集約するとともに、事業者等による情報システムの防護に資する分析結果等の情報を共有している。本ネットワークを通じて、26年中、標的型メール攻撃1,723件（前年比+1,231件）が発生したことを把握した。またこれ以外にも、共有された情報を基に各事業者等が対策を講じた結果、標的型メール攻撃の可能性があるメール1,646件が新たに確認されており、情報共有が被害の未然防止や拡大防止につながっている。

26年中の情報窃取を企図したサイバー攻撃としては、英文による「ばらまき型」の標的型メール攻撃が増加したほか、日本の制度を踏まえた内容のものや、特定の分野の研究会等を装ったものなど、より巧妙な手口が確認されている。また、標的型メール攻撃以外にも、水飲み場型攻撃や、ソフトウェアの更新を装い不正プログラムに感染させる攻撃も発生しており、サイバー攻撃の手口は巧妙化・多様化している。そのため、情報システムの運用・管理に当たっては、基本的な対策（不審なメールを安易に開封しないこと、ソフトウェアを最新版に保つことなど）を維持しつつも、それらをすり抜けて侵入する不正プログラム等の脅威があることを前提に、機微な情報の暗号化、機密性に応じたアクセス権の設定、ネットワークの分離等といった、リスク・ベースの防護を複層的に講じることが必要である。

(2) 標的型メール攻撃の情勢と手口

平成26年中に警察が把握した標的型メール攻撃は1,723件で、前年比約3.5倍に増加した。これは、26年下半期に「ばらまき型」攻撃が大幅に増加したためである。26年中に警察が把握した「ばらまき型」攻撃以外の標的型メール攻撃のうち、「やりとり型」攻撃は、４件（前年比-33件）であった。



【図２－２　警察が把握した標的型メール攻撃の件数】

---

*4　23年８月、標的型メール攻撃に関する情報を共有することで被害拡大の防止を図ることを目的として、警察と先端技術を有する事業者等が構築した情報共有ネットワークである。内閣官房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。27年１月現在、6,833社が参画している。

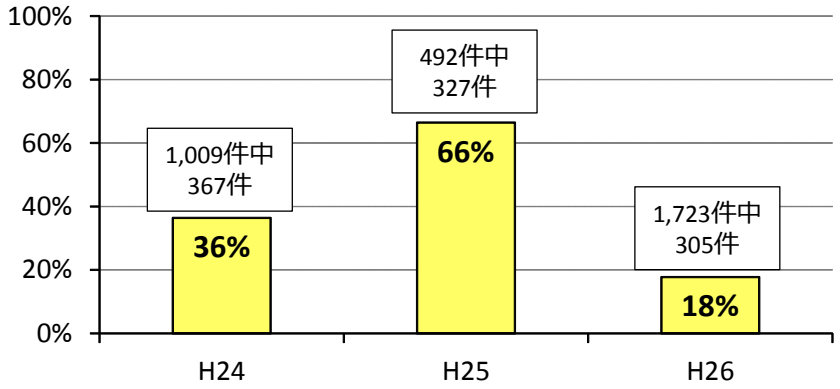
【表２－１　ばらまき型とそれ以外の標的型メール攻撃の割合】

	ばらまき型[*5]	ばらまき型以外
25年中	53％(259件)	47％(233件)
26年中	86％(1474件)	14％(249件)

「ばらまき型」攻撃は、24年から26年上半期にかけて減少傾向にあったが、26年下半期に急増した。その多くは、商品代金請求等の業務上の連絡を装った英文の標的型メール攻撃であり、「Order Details」、「RE: Important Documents」等の件名が記載されていた。このような「ばらまき型」攻撃で使用された不正プログラムのほとんどは、主要なウイルス対策ソフトウェアで検知可能であることを確認しており、ウイルス対策ソフトウェアを常に最新版に保つことが重要であるといえる。

標的型メールの送信先アドレスについては、インターネット上で公開されておらず検索サイトで調べても発見できないものが約７割を占めていることから、攻撃者が攻撃対象の組織や職員について深く調査し、周到な準備を行った上で攻撃を実施していることがうかがわれる。

標的型メール攻撃の送信元アドレスについては、「ばらまき型」攻撃の増加に伴い、フリーメールアドレス[*6] を使用するものの割合が、昨年の66％から18％に大幅に減少した。ただし、「ばらまき型」攻撃以外の標的型メール攻撃では、引き続きフリーメールアドレスが多数使用されていることから、フリーメールアドレスからの受信メールについて、メールサーバの機能により受信者に注意を促すメッセージを表示するなどの対策を講じることが有効である。

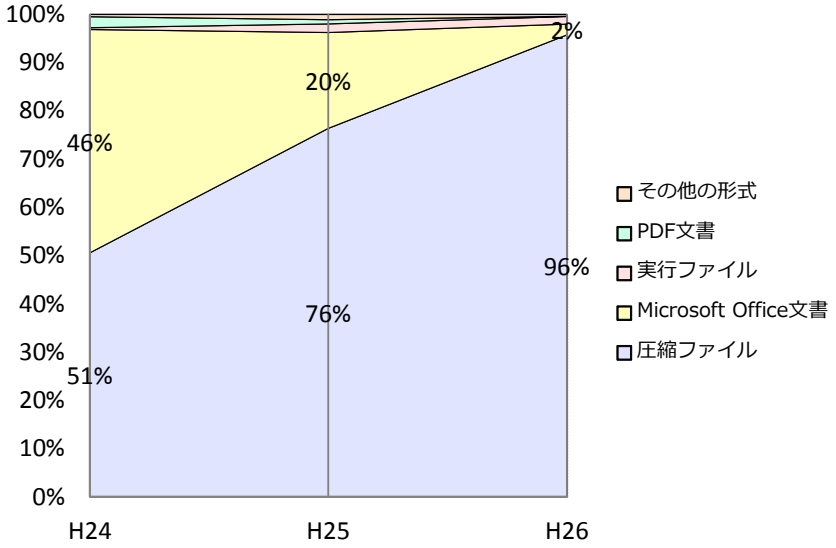


【図２－３　フリーメールアドレスを送信元とする標的型メール攻撃の割合】

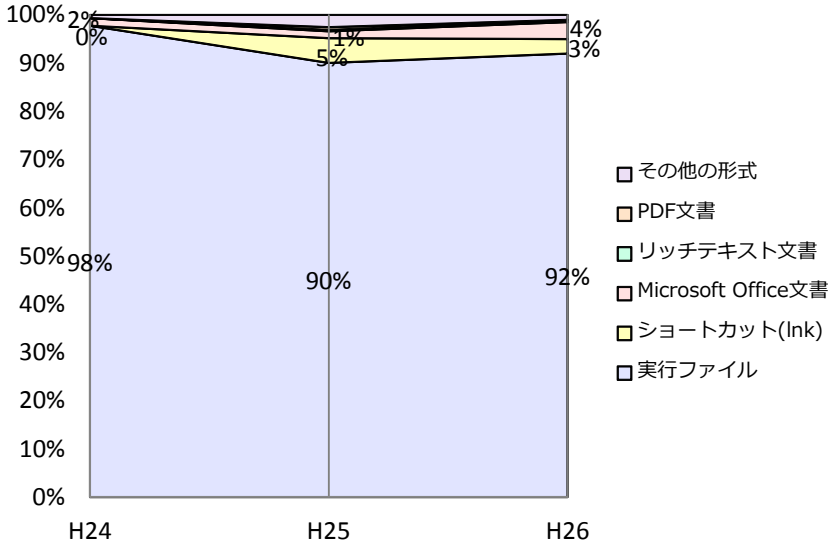
*5　同じ文面や不正プログラムが10か所以上に送付されていた標的型メール攻撃を「ばらまき型」として集計している。

*6　無料で利用可能なメールアドレスであり、国内外の様々な事業者によるサービスが提供されている。迷惑メール等の対策のためメールの送信数に制限がある場合が多く、「ばらまき型」攻撃には使用されにくい。

標的型メールに添付されたファイルについては、圧縮ファイルが占める割合が昨年の76%から96%に増加した。この圧縮ファイルを展開（解凍）して生成されるファイルについては、実行ファイルが92%と、引き続き高い割合を占めた。セキュリティ対策のためメールサーバやメールソフトによっては実行ファイルを直接添付できない制限がかかっている場合があり、このような制限を回避するため、標的型メール攻撃の添付ファイルとして圧縮ファイルが多用されているものと考えられる。



【図２－４　標的型メールに添付されたファイル形式の傾向】



【図２－５　圧縮ファイルに格納されたファイル形式の傾向】

(3)　標的型メール攻撃の事例

○　日本の制度を踏まえた内容の標的型メール攻撃

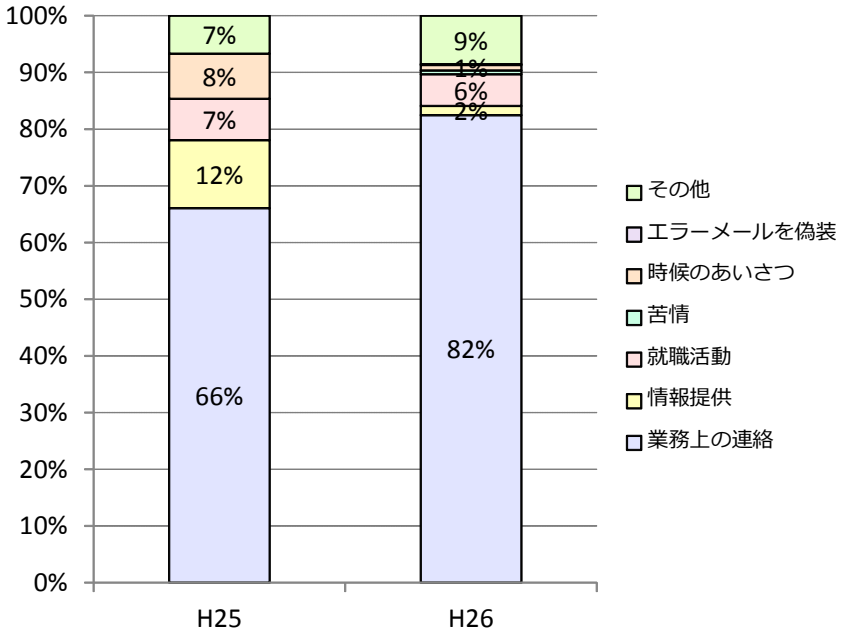
日本の制度を踏まえた内容を有する標的型メール攻撃を、新規に把握した。この標的型メール攻撃では、企業等の健康保険組合からの医療費の通

知を装ったものとなっており、第２四半期の終了する９月末ころから発生し始めた。このような攻撃は、27年に入ってからも継続的に把握されている。攻撃者が、日本の制度について理解を深めた上で、受信者が違和感を感じにくい内容のメールを作成している様子がうかがえる。

なお、標的型メールの内容については、商品代金請求等の業務上の連絡を装ったものの占める割合が、昨年の66％（492件中325件）から82％（1,723件中1,421件）に増加した。

○　特定分野の研究会等を装った標的型メール攻撃

特定分野の研究者や製造メーカーが集まる研究会や展示会に関する内容を装った標的型メール攻撃を新規に把握した。これは、当該研究会等に対する参加申込み方法の通知や名簿の送付を装ったものであり、攻撃者が関心を有する分野の研究者等を狙って、標的型メール攻撃を実施している様子がうかがえる。

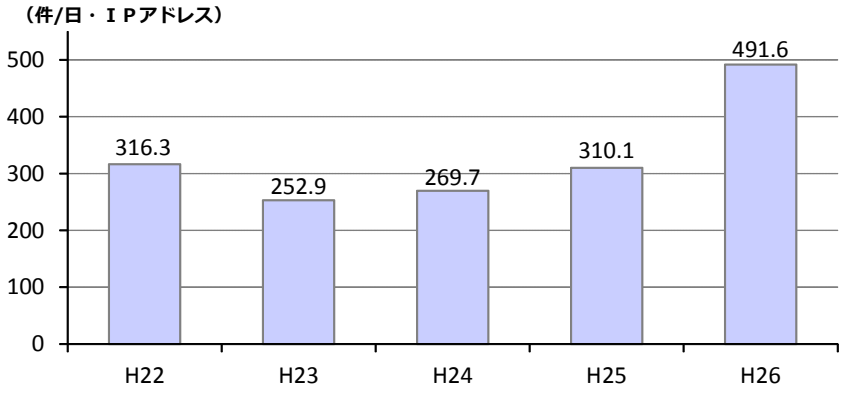


【図２－６　標的型メールの本文の内容】

３　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　－ぜい弱性を狙った攻撃準備行為－

警察庁では、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・分析するため、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。



【図２－７　センサーに対するアクセス件数の推移】

平成26年中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491.6件で、前年に比べ181.5件(58.5%)増加した。主な増加の要因は、Telnet及びSSH[*7] が使用するポート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、これらを対象とした探索行為が行われたと考えられる。また、ソフトウェアのぜい弱性の有無等を探索する行為も多数観測した。攻撃の踏み台とすることが可能なサーバ等や、攻撃コードが公開されているぜい弱性を有するサーバ等を探索するなど、攻撃の準備行為と考えられる探索行為を多数確認しており、システム管理者や利用者自身が常に対策を行うよう心掛けることが重要である。

(2)　ソフトウェアのぜい弱性を標的としたアクセス

ソフトウェアにはぜい弱性が存在する可能性があるため、いかなるソフトウェアにおいてもこれらのぜい弱性を狙った攻撃がなされる可能性がある。

例えば、平成26年４月、個人情報、クレジットカード情報等の通信に使用されているソフトウェアである「OpenSSL」に、秘密鍵等の重要な情報が漏えいする可能性がある深刻なぜい弱性が存在することが明らかとなった。当該ぜい弱性の有無を確認することが可能な攻撃コードも公開され、実際、警察庁では、当該コードを使用したと考えられるパケットも観測した。

また、同年９月には、ユーザとOSを仲介するシェルというソフトウェアの一種である「Bash (Bourne-Again　Shell)」に深刻なぜい弱性が存在することが明らかとなった。Bashは、LinuxやMac OS XといったUNIX系OS等に使われており、当該ぜい弱性が悪用されると、攻撃者により遠隔操作や不正プログラムの実行等の不正操作が行われる可能性がある。警察庁では、当該ぜい弱性を狙った、

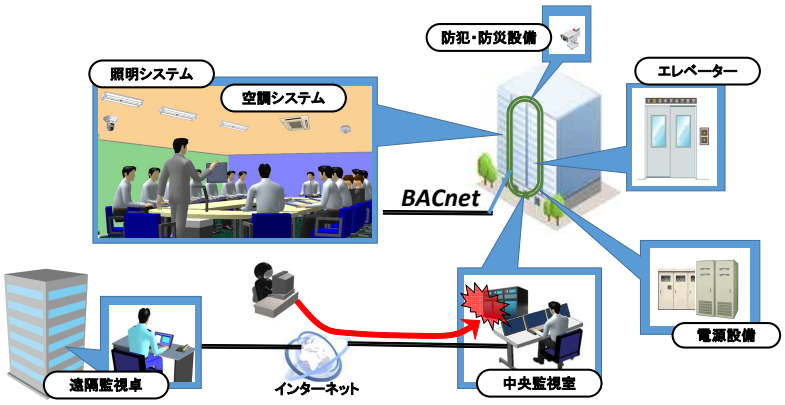
---

*7　Teletype network 及び Secure Shell の略。遠隔でネットワーク機器等を利用する際に使用されるサービスのこと。SSHによる通信は暗号化される。

ウェブサーバ、NAS[*8] 等に対する攻撃を試行したと思われるアクセスを観測した。

(3) ビル管理システム・産業制御システムに関する探索行為

平成26年３月以降、ビル管理システムの探索と考えられるアクセスを検知しており、特にBACnet[*9] システムを対象とした探索ツールによるアクセスが大半を占めていた。ビル管理システムでは、インターネットを介した遠隔監視等が可能であるため、適切な対策を施していない場合、攻撃者に侵入され、防犯・防災設備、エレベーター、電源設備等が操作される可能性がある。また、産業制御システムで使用される複数のポートに対するアクセスも観測している。その多くはぜい弱性等の調査を行っている組織からのものであるが、観測当初に比べてアクセスしている組織が増加していることから、産業制御システムに対する関心の高まりがうかがえる。



【図２－８　BACnet システムの概要】

(4) オープン・リゾルバを悪用する新たなDDoS攻撃手法及び各種リフレクター攻撃[*10] に関するアクセス

オープン・リゾルバとは、任意のドメイン[*11] について外部ネットワークからのリクエストに対して回答を送信するぜい弱性又は同ぜい弱性が存在する

---

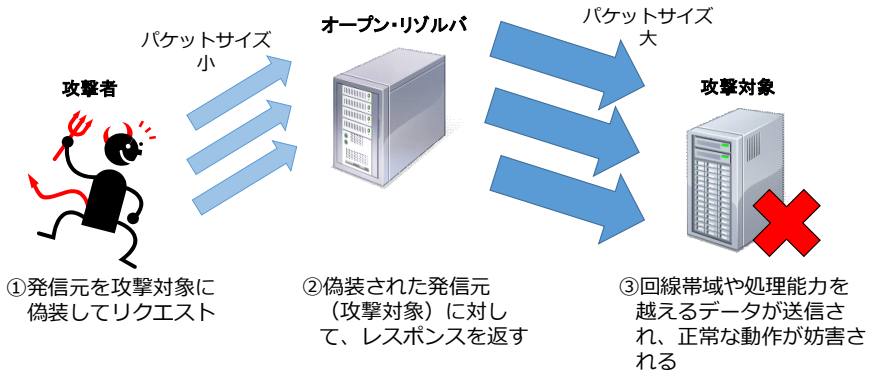
*8　Network Attached Storageの略。ネットワークに直接接続し、コンピュータ等から利用できる外部記憶装置のこと。ウェブサーバを利用しブラウザ上で管理できるものもある。

*9　Building Automation and Control Networkの略。ビル管理システムで使用される通信プロトコル用標準規格

*10　サーバに対するリクエストと比較して、当該サーバからのレスポンスデータが大きくなるプロトコルを悪用して、送信元を攻撃対象に偽装してリクエストを送信することにより、攻撃対象に大量のデータを送信する攻撃手法

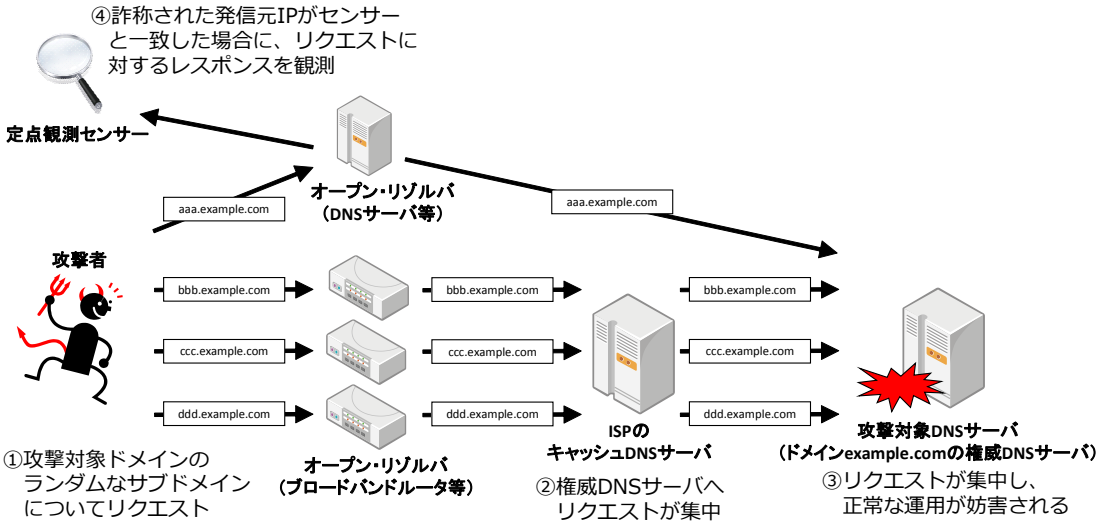
*11　npa.go.jpのように表現される、インターネット上の住所にあたるもののこと。ウェブサイトのアドレス（例：http://www.npa.go.jp/）やメールアドレス（例：xxx@npa.go.jp）に含まれている。

DNSサーバ[*12] 等の機器のことで、DNSリフレクター攻撃（図２－９）の踏み台となるおそれがある。警察庁においては、オープン・リゾルバの探索行為を、平成25年から継続して観測している。



【図２－９　DNS リフレクター攻撃の原理】

さらに、26年２月以降は、オープン・リゾルバを発信元とするパケットも多数観測している。これは、オープン・リゾルバを悪用する新たなDDoS攻撃手法（図２－10）に起因すると考えられる。この新たな攻撃手法の目的は、ある特定のドメインに関する情報を管理するDNSサーバ（「権威DNSサーバ」という。）にリクエストを集中させ、機能不全に陥らせることにある。



【図２－ 10　オープン・リゾルバを悪用する新たな DDoS 攻撃手法の原理】

*12　Domain Name System サーバの略。IPアドレスとドメインの対応に関する情報を提供するサーバ

また、NTP[*13] 、SSDP[*14] 、SNMP[*15] 等のリフレクター攻撃に悪用が可能であるプロトコルについても、多数のアクセスが観測されており、攻撃の踏み台となる機器の探索行為が活発化していると考えられる。

第３　サイバー空間における犯罪インフラの存在

近年、サイバー空間において敢行される犯罪に関しても、犯罪を企図する者の匿名性を高める様々なサービスや、いわゆる闇サイトを始めとする犯罪に関わるウェブサイト等、犯罪を助長し、又は容易にする基盤が着々と構築されてきている。

平成26年中には、不正アクセス行為等に悪用されると認識しながらサービスを提供していた悪質な中継サーバ運営者の一斉摘発を実施したほか、高校生が海外業者の提供するサービスを悪用し、オンラインゲーム会社にDDoS[*16] 攻撃を仕掛ける事件が発生した。

１　悪質な中継サーバ

平成26年11月、悪質な中継サーバ運営者らによる不正アクセス禁止法違反等について、全国20都道府県警察において一斉摘発を実施した。

中継サーバを利用すると、利用者のIPアドレスが中継サーバに割り当てられたIPアドレスに置き換わる上、通信記録（ログ）を保存していないことから、匿名性が高く、サイバー犯罪等に悪用されるなど、これらの犯罪インフラがサイバー犯罪の温床となっている。そのため、警察では、中継サーバを悪用したサイバー犯罪の抑止を目的に、中継サーバがサイバー犯罪に悪用されていると認識しながらサービスを提供している悪質な運営者ら12名を一斉に検挙した。実際、これらの中継サーバの中には、インターネットバンキングに係る不正送金事犯、会員制サービスへの不正ログイン等に使用されていたものも確認された。

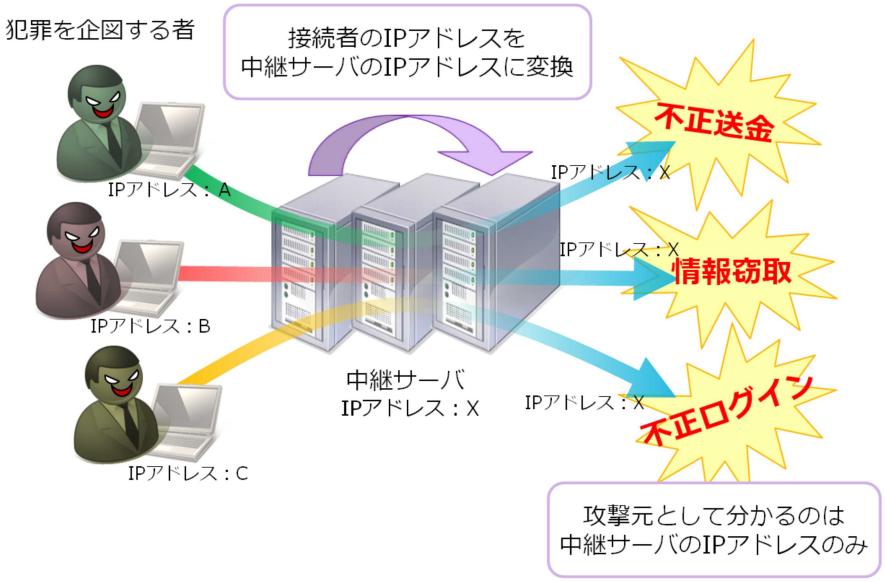
---

*13　Network Time Protocolの略。ネットワーク経由でコンピュータ等の時刻を同期させる際に用いられる。

*14　Simple Service Discovery Protocolの略。ネットワーク機器同士の接続機能であるUPnP（Universal Plug and Play）で用いられる。

*15　Simple Network Management Protocolの略。ネットワーク経由で機器の監視や制御を行う際に用いられる。

*16　Distributed Denial of Service の略。特定のコンピュータに対し、複数のコンピュータから大量のアクセスを繰り返し行い、対象コンピュータのサービス提供を不可能にする攻撃



【図３－１　中継サーバの悪用】

２　DDoS攻撃に悪用され得るサービス

平成26年９月、海外業者が提供するサービスを悪用し、オンラインゲーム会社へDDoS攻撃を仕掛け、同ゲーム会社の業務を妨害したとして、男子高校生１名を電子計算機損壊等業務妨害罪で検挙した。インターネットを通じて手軽、容易にDDoS攻撃が敢行できるサービスを提供している業者は多数存在している。

３　サイバーインテリジェンス事案で使用されたＣ２サーバのテイクダウン

Ｃ２[*17] サーバとは、不正プログラムに感染したコンピュータに対して指令を送り、これを制御するために攻撃者が使用するサーバ・コンピュータである。攻撃者は、サイバー攻撃の指令をＣ２サーバに中継させることにより、不正プログラムに感染した多くのコンピュータに対して、悪意のある活動を身元を隠しつつ効率よく行うことが可能となる。

平成26年中、警察では、サイバーインテリジェンス事案で使用された不正プログラムの解析等を通じ、国内に構築されたＣ２サーバ33台の存在を把握した。その多くは、中小企業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を行い、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、構築されたものである。

警察では、これらのウェブサイトの管理者と連携し、Ｃ２機能の停止（テイクダウン）を行うとともに、Ｃ２サーバへの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、個別に注意喚起を行うことにより、被害拡大の防止を図った。

---

*17　Command and Control（指令制御）の略であり、Ｃ＆Ｃと省略する場合もある。

第４　新たな技術・サービスの実社会への影響

平成26年中には、新たな技術・サービスを犯罪に悪用した事案も話題となった。技術の進歩はめざましく、３Ｄプリンタのように以前は高価であった機器が家庭用に出回り始めたほか、情報通信技術の進展によりビットコインのような新たな決済手段が使われ始めるなど、新たな技術・サービスが急速に普及している。

サイバー空間の安全・安心を確保するためには、ビットコインのようにインターネット上で使用される技術について情報を収集することはもちろんのこと、現実空間を対象としている新たな技術についても、インターネット上の情報と組み合わせることで犯罪につながり得ることから、動向を注視していく必要がある。

１　３Ｄプリンタによる拳銃の製造

平成26年５月、３Ｄプリンタを用いて製造された手製拳銃を自宅において所持していたことにより、大学職員の男１名を銃砲刀剣類所持等取締法違反（拳銃複数所持）で逮捕した後、同年６月に武器等製造法違反（無許可製造）で再逮捕した。男は、米国の団体がインターネット上に公開した銃の設計図データをダウンロードし、自ら補正するなどして、３Ｄプリンタを用いて実弾の発射が可能な拳銃を製造した。

この事案を契機に、インターネット・ホットラインセンター[*18]（IHC）では、同年８月から「ホットライン運用ガイドライン」において「３Ｄプリンタによる銃砲の製造を助長等する設計図データ」を有害情報に追加した。有害情報とされたことで、警察への通報やウェブサイト管理者等への削除要請が可能となり、３Ｄプリンタによる銃砲製造等の事案の未然防止・検挙に資すると期待される。

２　ビットコイン

ビットコインについては、事業者による自主規制団体が発足するなど、利活用促進の動きが起こっているが、その一方で、匿名性が高いことから犯罪に悪用され得るという側面もあり、同年５月に覚せい剤取締法違反（営利目的輸入）で検挙された男がビットコインを利用して覚醒剤を購入した旨を供述した例もある。

第５　インターネット利用に係るリスクの拡大

インターネットの利用者が増えるにつれて、インターネット上では、動画や音楽の視聴、ショッピング、ゲーム、SNS等、様々なサービスが提供されるようになった。こうした各種サービスにより利便性が高まる一方で、利用者のID・パスワード等が窃取されることによる不正ログイン攻撃が発生しているほか、サイバー

---

*18　警察庁からの業務委託を受け、一般のインターネット利用者等から、違法情報・有害情報に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行う機関

空間の持つ匿名性や拡散性といった特性により様々な問題が発生していることから、インターネットの適切な利用が求められている。

平成26年中には、前述のインターネットバンキングに係る不正送金事犯のみならず、インターネットサービスを提供する多くの大手企業が、連続自動入力プログラムによる不正ログイン攻撃（以下「リスト型攻撃」という。）を受けたことを公表したことが大きな話題となった。また、オンラインゲームやソーシャルゲームのアカウントが乗っ取られるなどの事件や、インターネット上への元交際相手に係る性的画像等の掲載事案（いわゆるリベンジポルノ）、危険ドラッグ取引、インターネットオークションに係る詐欺等、インターネット利用者の増加に伴い、これらの利用に係るリスクが拡大した。

１　リスト型攻撃

インターネット上には数多くのサービスがあるため、複数のウェブサイトで同一のID・パスワードを使い回す利用者も多い。そうした状況に目を付けた攻撃がリスト型攻撃である。不正取得した他人のID・パスワードのリストを悪用し、連続自動入力プログラムを用いてそれらのID・パスワードを異なるウェブサイトに入力することにより不正アクセスを敢行する。

リスト型攻撃そのものは以前から発生しており、平成26年中にも事業者からの申告により約80万件のリスト型攻撃を受けていたことが判明している。

【図５－１　リスト型攻撃の概要】

２　インターネット上への性的画像の掲載（いわゆるリベンジポルノ）

元交際相手の裸の画像をインターネット上に流出させ、名誉毀損罪で逮捕に至った事案等が発生した。画像の流出はなくとも、「裸の写真をインターネット上にばらまく」などと元交際相手を脅したり復縁を迫ったりした者を、脅迫罪や強要未遂罪で逮捕した事案も発生した。

こうした問題を受け、平成26年11月、私事性的画像記録の提供等による被害

の防止に関する法律が成立、公布[*19] された。

３　危険ドラッグ

危険ドラッグについては、その影響によるとみられる事件・事故が発生するなど、依然として深刻な状況にある。取締りに当たっては販売店舗の減少と販売方法の潜在化を見据え、店舗対策のみならずインターネット上での販売に対しても厳しく取り締っていく必要がある。警察では、指定薬物の検出例がある危険ドラッグをインターネット上で販売していたウェブサイトに削除を要請し、その結果、多くの販売サイトが閉鎖されたほか、IHCでは、指定薬物の広告及び危険ドラッグに係る未承認医薬品の広告を違法情報に、危険ドラッグに係る未承認医薬品の疑いがある広告を有害情報に追加した。

４　SNSの利用

SNSは身近なコミュニケーションツールとして有用であるが、犯罪のツールとして悪用されることもあれば、誤った使い方により様々な問題を引き起こしてしまう可能性もある。

例えば、前述の元交際相手に係る性的画像の掲載のほか、無料通話アプリの乗っ取りによる電子マネー被害、SNS利用時に必要なメールアドレス及びパスワードを窃取する偽サイト等、利用者の誰もが被害者になり得る事件が発生した。また、SNS上での殺人をほのめかす投稿等、多くの者が見ることのできる場に投稿した場合に発生する影響を考慮していない投稿や、無料通話アプリ上で行われるいじめが話題となるなど、SNSを利用する上での問題点が顕在化した。

５　インターネットオークション詐欺の急増等

インターネットオークションにおける詐欺被害が増加している。統計を取り始めた平成21年以降、被害件数は年々減少していたが、25年には前年の約２倍となり、26年中の被害件数は統計を取り始めて以降過去最高の3,234件を記録した。

また、海外のサーバを通じてインターネット上に掲載された、実在する企業のサイトを模したサイトや、インターネットショッピングに係る詐欺や偽ブランド品販売を目的とするサイト（以下「海外の偽サイト等」という。）に係る被害も多発している。

そのため、警察庁では、都道府県警察が相談等で受理した海外の偽サイト等のURL等の情報を集約し、ウイルス対策ソフト事業者等に提供して、これらのサイトを閲覧しようとする利用者のコンピュータ画面に警告表示等を行う被害拡大防止対策を25年12月より実施し、注意喚起を図っている。

インターネットによるオークション等の利用には利点もあるものの、商品が届かない、偽ブランド品が送付されるなど様々な問題が発生しており、警察が

---

*19　26年11月27日　公布、一部同日施行

民間事業者と連携して被害拡大防止対策を推進していくとともに、利用者自身が危険性を理解した上で利用することが必要である。

６　インターネット等を利用した選挙運動の解禁後、初の衆議院議員総選挙

平成25年４月に公職選挙法の一部が改正され、インターネット等を利用した選挙運動が可能となった。26年12月14日に施行された第47回衆議院議員総選挙は解禁後初の衆議院議員総選挙であったが、27年１月13日（期日後30日）現在、インターネット等を利用した違法な選挙運動に対する検挙はなく、公示前の特定の候補者や政党への投票依頼を行ったことなどにより８件の警告を行った。

第６　検挙状況等

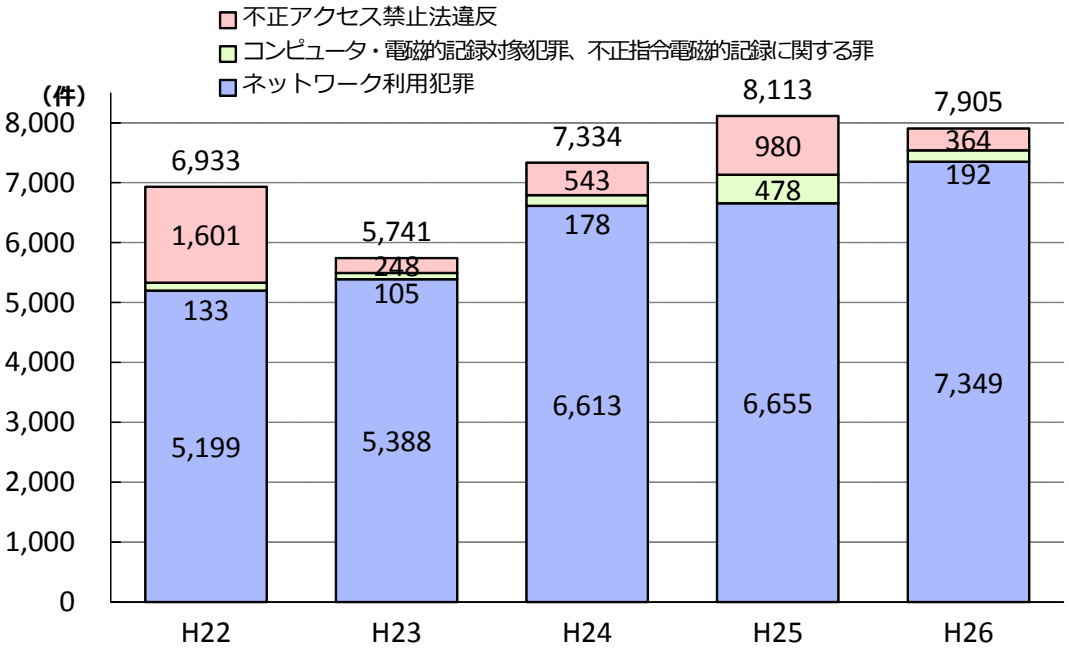
１　サイバー犯罪の検挙状況

平成26年中のサイバー犯罪の検挙件数は7,905件（前年比208件（2.6％）減少）

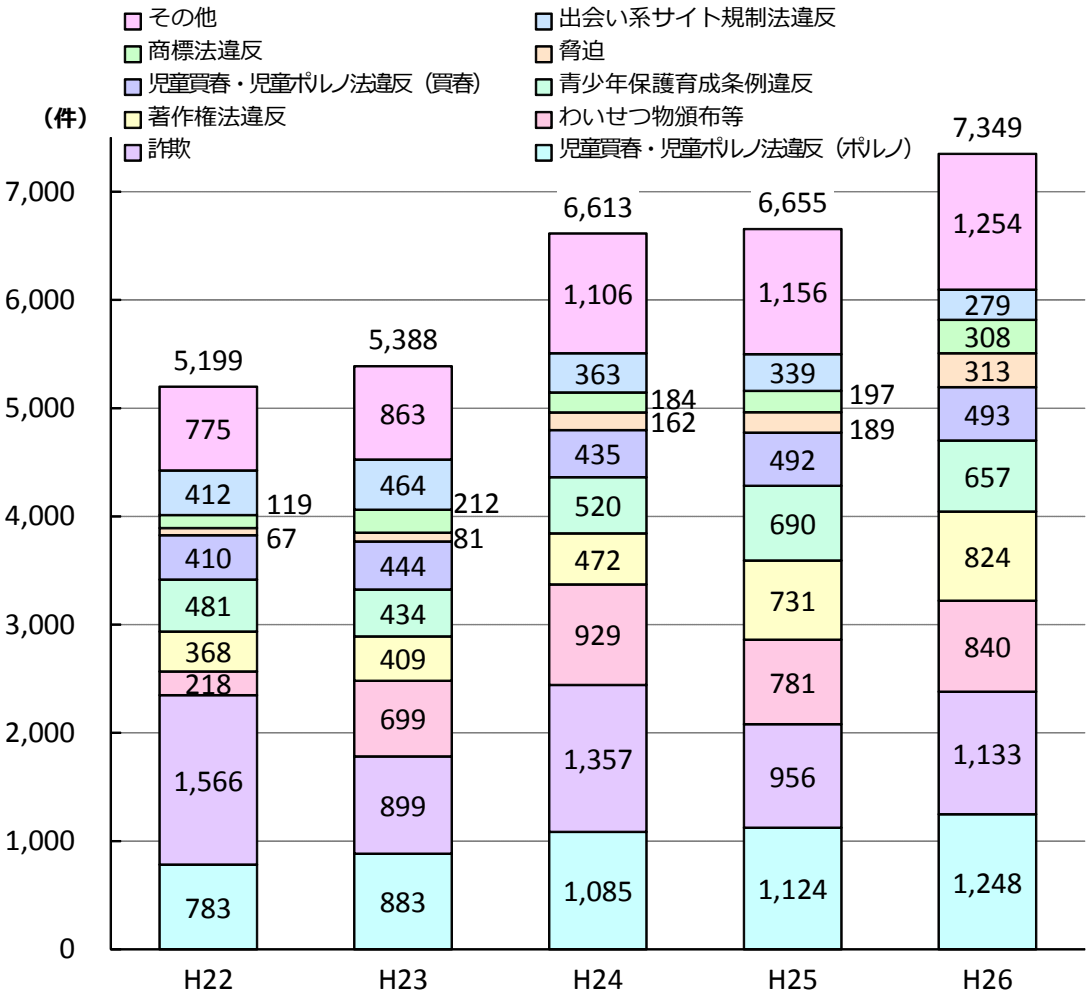
○　不正アクセス禁止法違反は364件（前年比616件（62.9％）減少）

○　コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪は192件（286件（59.8％）減少）

○　ネットワーク利用犯罪は7,349件（694件（10.4％）増加）



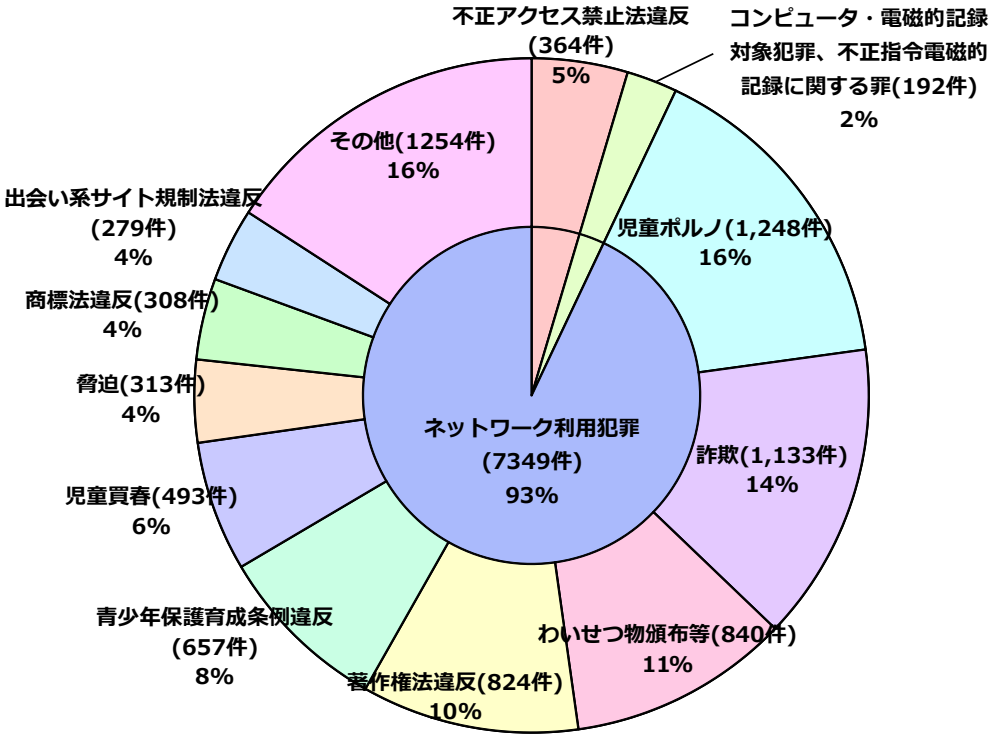
【図６－１　サイバー犯罪の検挙件数の推移】



【図６－２　ネットワーク利用犯罪の内訳】

【表６－１　サイバー犯罪の検挙件数の内訳】

罪名＼年	H22	H23	H24	H25	H26	前年比増減	
不正アクセス禁止法違反	1,601	248	543	980	364	－ 616	－ 62.9%
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	133	105	178	478	192	－ 286	－ 59.8%
電子計算機使用詐欺	91	79	95	388	108	－ 280	－ 72.2%
電磁的記録不正作出・毀棄等	36	17	35	56	48	－ 8	－ 14.3%
電子計算機損壊等業務妨害	6	6	7	7	8	± 1	＋ 14.3%
不正指令電磁的記録作成・提供	－	0	4	8	9	＋ 1	＋ 12.5%
不正指令電磁的記録供用	－	1	34	14	16	＋ 2	＋ 14.3%
不正指令電磁的記録取得・保管	－	2	3	5	3	－ 2	－ 40.0%
ネットワーク利用犯罪	5,199	5,388	6,613	6,655	7,349	＋ 694	＋ 10.4%
児童買春・児童ポルノ法違反（児童ポルノ）	783	883	1,085	1,124	1,248	＋ 124	＋ 11.0%
詐欺	1,566	899	1,357	956	1,133	＋ 177	＋ 18.5%
うちオークション利用詐欺	677	389	235	158	381	＋ 223	＋ 141.1%
わいせつ物頒布等	218	699	929	781	840	＋ 59	＋ 7.6%
著作権法違反	368	409	472	731	824	＋ 93	＋ 12.7%
青少年保護育成条例違反	481	434	520	690	657	－ 33	－ 4.8%
児童買春・児童ポルノ法違反（児童買春）	410	444	435	492	493	＋ 1	＋ 0.2%
脅迫	67	81	162	189	313	＋ 124	＋ 65.6%
商標法違反	119	212	184	197	308	＋ 111	＋ 56.3%
出会い系サイト規制法違反	412	464	363	339	279	－ 60	－ 17.7%
その他	775	863	1,106	1,156	1,254	＋ 98	＋ 8.5%
合　　計	6,933	5,741	7,334	8,113	7,905	－ 208	－ 2.6%



【図６－３　サイバー犯罪の罪名別割合】

２　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】

○　会社経営の男（30）ほか４名は、中国から日本のウェブサイトを利用するための中継サーバを国内に設置し、顧客に提供する事業を営んでいる者であるが、平成26年７月、中継サーバから、インターネット接続事業者が管理する認証サーバに、同事業者が第三者を正規利用者として付与した認証ID等を中継サーバ内のインターネット接続ソフトにあらかじめ設定するなどの方法で入力等して不正アクセスした。同年11月、20都道府県警察による中継サーバ事業者の一斉取締りを実施し、上記被疑者らを含め、12名を不正アクセス禁止法違反等で検挙した。（20都道府県警察）

コンピュータ・電磁的記録対象犯罪

【電子計算機損壊等業務妨害】

○　高校生の男（16）は、26年３月、海外サイトを利用して、オンラインゲーム運営会社が使用するサーバコンピュータに対し、大量の情報を送信し高負荷を与える攻撃（DDoS攻撃）を仕掛けて同社の業務を妨害した。同年９月、電子計算機損壊等業務妨害罪で検挙した。（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】

○　自営業の男(43)らは、26年１月、女性になりすましチャットサイト上で知り合った男性に対し、無料通話アプリを使用して、スマートフォン内の電話帳データを窃取する不正アプリを送信し、実行させた。さらに男らは、言葉巧みに男性の性的動画を送信させた上で、同動画の拡散を奇貨として現金を恐喝した。同年３月、不正指令電磁的記録供用、恐喝罪で検挙した。（千葉）

ネットワーク利用犯罪

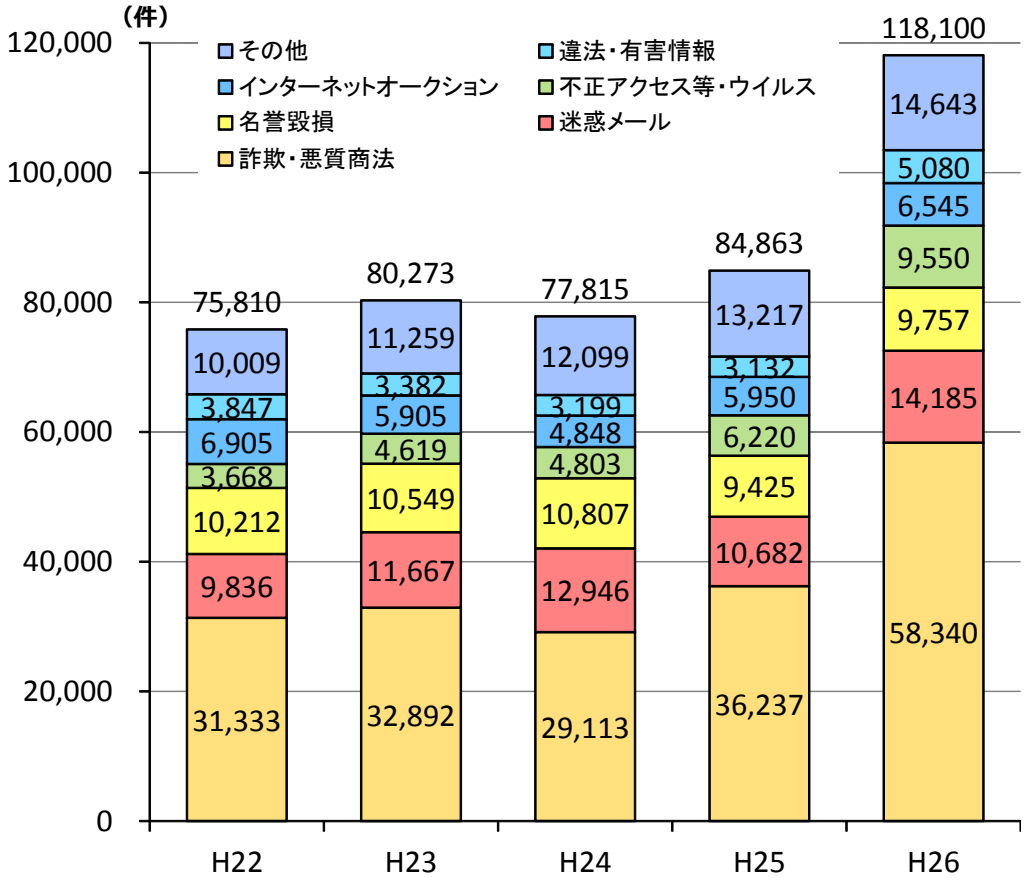
【特定商取引法違反（未承諾電子メール広告の提供の禁止）及び詐欺】

○　サイト運営者の男（32）らは、運営する出会い系サイトを利用させる目的で、相手方となる者の承諾を得ていないにもかかわらず、当該サイトにリンクされるURL等が表示された電子メール広告を送信するとともに、当該サイトにおいて実在しない登録会員になりすまし、会員からメッセージ交換等のサイト利用料金をだまし取った。26年８月、特定商取引法律反で検挙するとともに、同年９月、詐欺罪で検挙した。（北海道、警視庁）

【著作権法違反】

○　無職の男（51）らは、著作権者の承諾を受けないで、著作物であるテレビ番組を動画サイトに投稿してインターネットを利用する不特定多数の者が閲覧できる状態にし、著作権を侵害した。26年９月、動画サイトを利用した著作権法違反事件の一斉取締りを実施し、上記被疑者を含め、全国で16名を一斉検挙した。（警視庁、神奈川、大阪、鹿児島）

３　サイバー犯罪に関する相談件数



【図６－４　相談受理件数の推移】

【表６－２　相談の受理内容】

	H22	H23	H24	H25	H26	前年比増減	
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）	31,333	32,892	29,113	36,237	58,340	＋ 22,103	＋ 61.0%
迷惑メールに関する相談	9,836	11,667	12,946	10,682	14,185	＋ 3,503	＋ 32.8%
名誉毀損・誹謗中傷等に関する相談	10,212	10,549	10,807	9,425	9,757	＋ 332	＋ 3.5%
不正アクセス等、コンピュータ・ウイルスに関する相談	3,668	4,619	4,803	6,220	9,550	＋ 3,330	＋ 53.5%
インターネットオークション	6,905	5,905	4,848	5,950	6,545	＋ 595	＋ 10.0%
違法・有害情報に関する相談	3,847	3,382	3,199	3,132	5,080	＋ 1,948	＋ 62.2%
その他	10,009	11,259	12,099	13,217	14,643	＋ 1,426	＋ 10.8%
合　計	75,810	80,273	77,815	84,863	118,100	＋ 33,237	＋ 39.2%

４　相談事例

詐欺・悪質商法に関する相談

○　ネットショッピングで商品の購入手続きをし代金も支払ったが商品が届かず、連絡先に電話したところ、販売サイトとは全く関係のない会社で、騙されたことが分かった。

○　契約した覚えのないアダルトサイトの料金を請求された。

迷惑メールに関する相談

○　出会い系サイトを利用した後から、大量の広告メールなどが送られてくるようになった。

○　お金を振り込むので口座番号を教えてほしいという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

○　掲示板サイトなどに、個人や会社を誹謗中傷する書き込みをされた。

○　自分の写真と実名を使って勝手にSNSのアカウントを作成されて、自分に成り済まされ、他人を誹謗中傷する内容を書き込まれていた。

不正アクセス等に関する相談

○　無料通話・メールアプリのアカウントを乗っ取られ、勝手に知人に対してプリペイドカードの購入を依頼されていた。

○　オンラインゲームでアカウントを乗っ取られ、ゲーム内のアイテムなどを勝手に使用された。