広　報　資　料
平成26年９月11日
警　　察　　庁

平成26年上半期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

攻撃企図者がセキュリティ対策の間隙を狙う手法を開発、実践している状況がみられる。

○　ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞに係る不正送金事犯について、上半期の被害額が昨年の総被害額を上回ったほか、パソコンに感染したウイルスが不正な振込みを行う「MITB(Man In The Browser)」という手口を確認。

○　情報窃取を企図したサイバー攻撃について、メールの送付対象の少数絞込、感染を自覚させないための工作を施す傾向を確認。また、無償ソフトウェアの更新を悪用した新たな手口を確認。

○　犯罪等の準備行為とみられる各種探索パケット（各種リフレクター攻撃の踏み台、OpenSSLのぜい弱性、ビル管理システム）を多数観測。

(2)　新たな技術・サービスの実社会への影響

サイバー空間と深くつながりを持つ新たな技術・サービスが出現。社会的利益をもたらす一方、それらが犯罪のツールとして利用される可能性も拡大。

(3)　インターネット利用に係るリスクの顕在化

依然として継続的に発生する企業のウェブサイトに対する不正ログイン攻撃、元交際相手に係るわいせつ画像の掲載による名誉毀損事案、ベビーシッター仲介サイトを通じてシッターに預けられた男児の死亡事案等、普及・発展するインターネットの利用に係るリスクが顕在化。

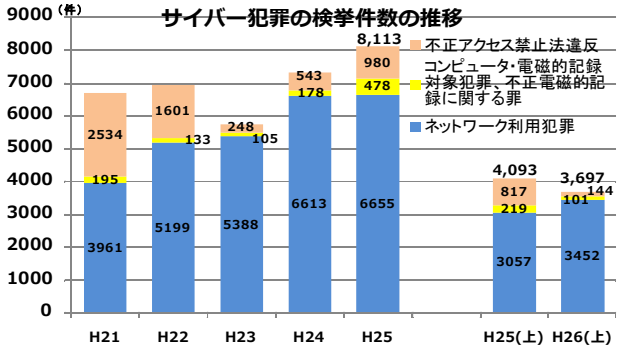
２　サイバー犯罪・サイバー攻撃の発生状況等

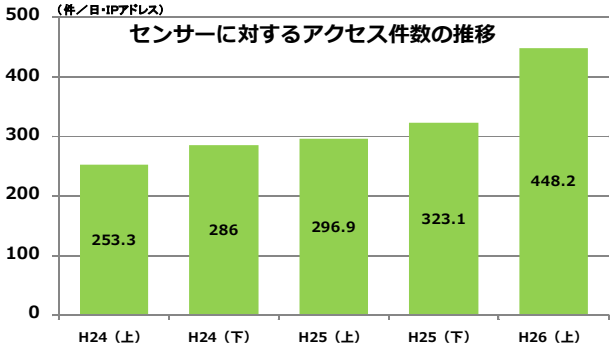
○　サイバー犯罪の検挙件数は3,697件(前年同期比-396件、-9.7%)

○　都道府県警察の相談窓口で受理したサイバー犯罪等に関する相談件数は54,103件（+14,711件、+37.3%）

○　警察が把握した標的型メール攻撃は216件（+15件、+7.5%）

○　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つのセンサー当たり１日に448.2件（+151.3件、+51.0%）





別添

平成26年上半期のサイバー空間をめぐる脅威の情勢

第１　総括

平成26年上半期中は、サイバー犯罪[*1] の検挙件数は3,697件と、前年同期より396件、9.7％減少した。また、都道府県警察の相談窓口で受理したサイバー犯罪等に関する相談件数は54,103件と、前年同期より14,711件、37.3%増加した。さらに、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448.2件と、前年同期より51.0%増加しており、各種攻撃の試みが活発化している状況がうかがえた。

サイバー空間をめぐる脅威の情勢としては、下記のような特徴がみられた。

１　手口の悪質・巧妙化

サイバー空間の安全・安心の確保のため、産学官が連携し、様々な取組を行っているところであるが、サイバー空間を舞台として金銭、機密情報等の窃取を企図する者は、それら取組の間隙を狙う手法を開発、実践している。

平成26年上半期では、例えば、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、MITB（Man In The Browser）攻撃と呼ばれる手口が確認された。手口の根幹となる技術手法は従来から確認されていたものであったが、国内のインターネットバンキングに係る不正送金事犯に応用され、被害を生み出していることが判明した。

また、標的型メール攻撃については、「ばらまき型」攻撃が減少し対象を絞り込んだ攻撃が増加したほか、Windowsのショートカットファイルが添付されたメールが増加し、手口の巧妙化がうかがえた。さらに、本年に入り、無償ソフトウェアの更新を悪用して不正プログラムに感染させるといった新たな手口も確認した。こうした手口による攻撃は、標的型メール攻撃に比べ、高い技術力や周到な準備が必要となるものの、被害が潜在化・大規模化しやすく、今後も警戒を要する。

２　新たな技術・サービスの実社会への影響

近年、新たな技術・サービスの出現により、以前では想定されなかったことが実現されつつあり、その中には、サイバー空間と深くつながりを持つものも多い。

---

*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

平成26年上半期では、例えば、３Ｄプリンタを用いた手製拳銃の製造事件が話題となったが、これについては、インターネットが世界中とつながっていることで、拳銃の設計図たる電子データが個人で密かに入手可能であったことも要因の一つになったと考えられる。また、ビットコインのようなサイバー空間上での新たな取引手段も広がり始めており、これら新たな技術・サービスの出現は社会的利益をもたらす一方、それらが犯罪のツールとして悪用される危険をはらむことがある。

３　インターネット利用に係るリスクの顕在化

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する中、スマートフォンやタブレットといった携帯型端末、主流なコミュニケーションツールとしてのソーシャル・ネットワーキング・システムの普及も相俟って、手軽・便利にインターネットを利用することができるようになった一方、インターネットの利用によって犯罪に巻き込まれるリスクも増加している。

平成26年上半期では、例えば、サイバー空間の持つ拡散性に着目した事例として、元交際相手に係るわいせつ画像の掲載等が社会的な問題となったほか、インターネット利用者の多くが複数のウェブサイトで同一のID、パスワードを使い回している状況に目を付けた不正ログイン攻撃が様々な企業のウェブサイトに対して発生した。

今後とも、インターネット上のコミュニケーション、掲示板への書き込み等を発端に犯罪に発展するケースは継続して発生するものとみられるが、こうした犯罪の被害を受けないためにも、利用者一人一人がサイバー空間を利用する上で必要なリテラシーを身に付けていく必要がある。

第２　各個別事犯等の情勢

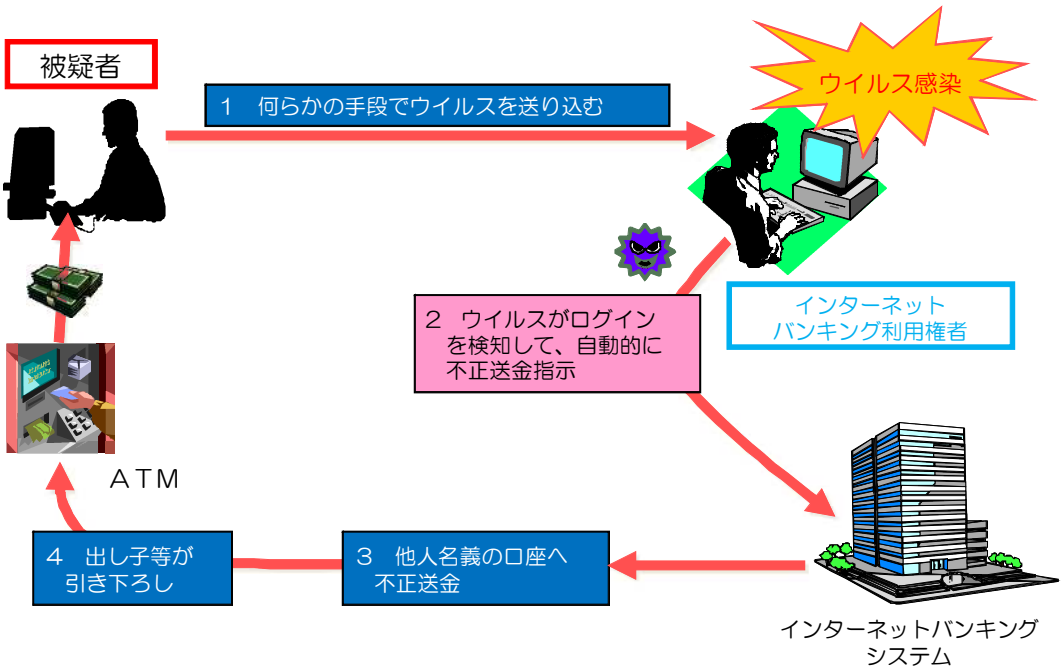
１　インターネットバンキングに係る不正送金事犯

(1)　概況　－半年足らずで昨年１年間の被害額を上回る－

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14億600万円と過去最大となったが、その脅威は拡大し続け、26年上半期の総被害額は、約18億5,200万円と既に昨年の被害額を上回った。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、犯行の手口についても、MITB攻撃と呼ばれる手口による被害が確認された。この手口は、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

ものであり、海外では以前から確認されていたが、国内でも被害が確認された。



【MITB攻撃の概要】

(2)　警察における対策

○　国際的なボットネットのテイクダウン作戦

平成26年上半期には、国際的な対策として、米国連邦捜査局（FBI）及び欧州刑事警察機構（ユーロポール）を中心に、日本警察を含む協力国の法執行機関が連携し、「Game Over Zeus」と呼ばれる不正プログラムのネットワークを崩壊させる、国際的なボットネットのテイクダウン作戦を決行した。警察では、各プロバイダ等に本作戦への協力を呼び掛けるとともに、この作戦を通じて判明した感染端末の利用者に対し、プロバイダ等を通じて不正プログラムの駆除を促している。

また、警察庁ウェブサイトに「国際的なボットネットのテイクダウン作戦」に関する専用ページを設け、作戦の概要や警察の取組について周知するとともに、感染端末利用者の対処法やインターネットバンキング利用者が講じるべき被害防止対策に関する広報啓発を行っている。

○　金融機関関係団体に対するインターネットバンキングに係る不正送金事犯への対策強化の要請等

警察では、前述のように急速に被害が拡大しているインターネットバンキングに係る不正送金事犯への対策として、金融機関関係団体に対し、セキュリティ対策強化に向けた継続的な取組や、インターネット利用者

による被害防止対策の促進等について要請を行った。

○　広報啓発用ＤＶＤの制作

広く国民に対してインターネットバンキングに係る不正送金事犯等のサイバー犯罪の発生状況や手口等の周知を図り被害を防止するための広報啓発用DVD「消えた残高」を制作し、情報セキュリティに関する講演等での放映、金融機関等への貸出、警察庁ウェブサイトへの掲載による広報啓発を行った。

(3)　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の更新

○　基本ソフト（OS)、ウェブブラウザ等各ソフトウェアの最新の状態への更新

○　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

○　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[*2] の利用

○　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

２　情報窃取を企図したサイバー攻撃

(1)　概況　－攻撃対象の絞り込みが進む－

平成26年上半期は、前年までに引き続き、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発生したことを把握した。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」[*3] 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

---

*2　インターネットバンキング等における認証用のパスワードであって、認証のたびにそれを構成する文字列が変わるもの。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

*3　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。内閣官房情報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。26年７月現在、6,556社が参画している。

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年上半期中、標的型メール攻撃が216件（前年同期比＋15件、＋7.5％）発生したことを把握した。また、共有された情報を基に各事業者等が対策を講じた結果、新たに標的型メール攻撃の可能性のあるメールが775件確認されており、被害の未然防止や拡大防止につながっている。

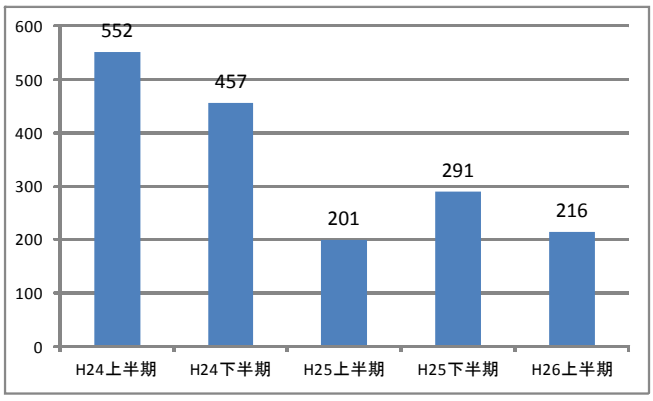
26年上半期の標的型メール攻撃の特徴としては、「ばらまき型」攻撃が減少し、対象を絞り込んだ攻撃が増加したこと、Windowsのショートカットファイル（LNK）を利用した不正プログラムが前年に続き増加したこと、就職活動を装うメールの割合が前年同期よりも増加したことなどの変化が見られる。

情報窃取を企図したサイバー攻撃としては、標的型メール攻撃に加えて、昨年確認した水飲み場型攻撃[*4]のほか、本年に入ってから、無償ソフトウェアの更新を悪用して不正プログラムに感染させる手口といった新たな手口を確認している。これらの手口による攻撃は、標的型メール攻撃に比べ、高い技術力や周到な準備が必要となるものの、被害が潜在化・大規模化しやすいことから、今後も警戒を要する。

(2) 標的型メール攻撃の情勢と手口

平成26年上半期に警察が把握した標的型メール攻撃は216件で、前年同期比で15件、7.5％増加した。「ばらまき型」攻撃が全体に占める割合については、前年中よりも減少した。「やりとり型」攻撃については、25年上半期は33件であったが、26年上半期は１件であった。

「ばらまき型」攻撃が減少傾向にあることは、標的型メール攻撃により不正プログラムを送り込む対象を少数に絞り込んだ攻撃が、増加していることを示している。また、送信先アドレスの７割は、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であった。攻撃者は、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



【警察が把握した標的型メール攻撃の件数】

*4　対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる手口による攻撃

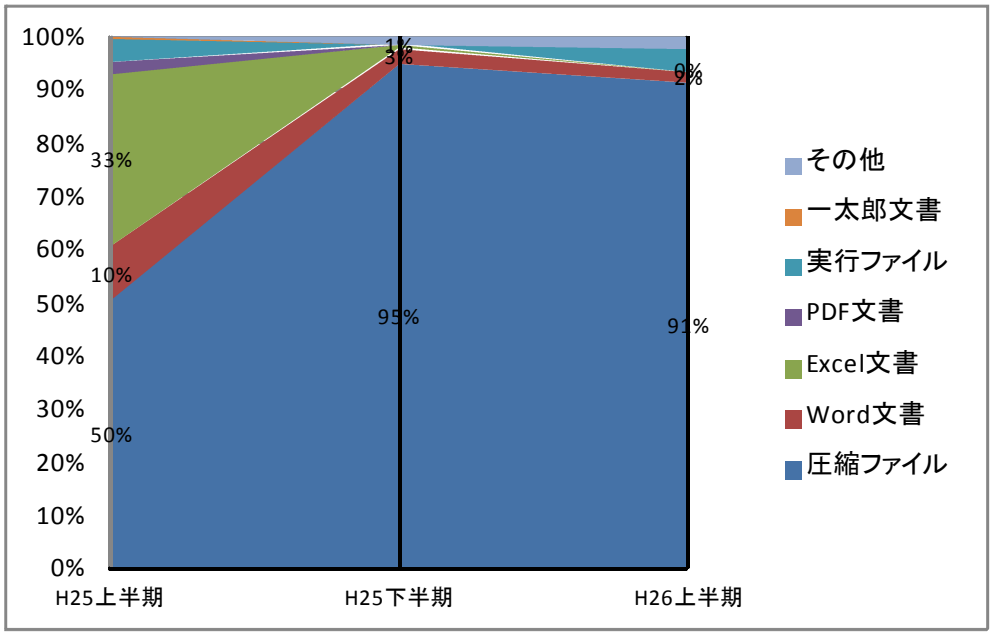
ることがうかがわれる。

	ばらまき型[*5]	ばらまき型以外
25年中	53%(259件)	47%(233件)
26年上半期	40%(86件)	60%(130件)

【ばらまき型とそれ以外の標的型メール攻撃の割合】

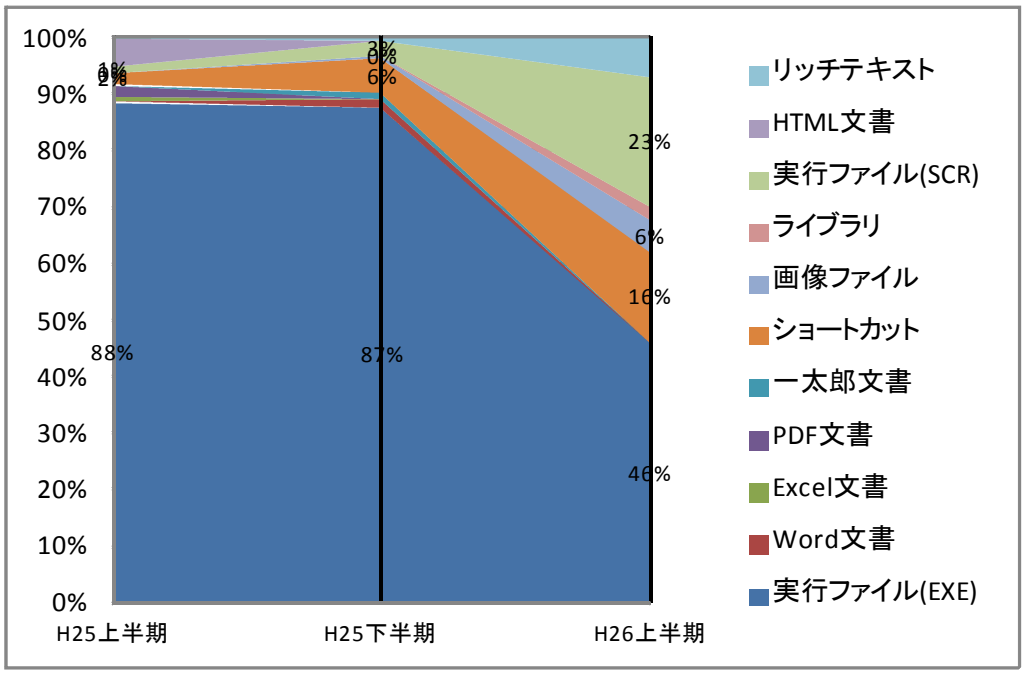
標的型メールに添付されたファイルの傾向としては、昨年と同様に、圧縮ファイルを添付するものが全体の約９割を占めた。さらに、圧縮ファイルを展開（解凍）して生成されるファイルについては、その約７割が実行ファイル（EXE又はSCR）であり、約２割がWindowsのショートカットファイル（LNK）であった。

ショートカットファイルを利用した攻撃は、昨年から発生を確認しており、本年に入って増加傾向にある。この攻撃では、「個人情報」、「履歴書」、「名簿」といったファイル名のテキストファイルに偽装したファイルが、全て日本語で記載されたメールに添付されて送られている。当該ファイルを開くと、不正なインターネット接続が実行され、更なる不正プログラムのダウンロードが行われるものの、画面上にダミーの文書を表示させるため、不正プログラムに感染したことに気付きにくくなっている。



【標的型メールに添付されたファイル形式の傾向】

*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。

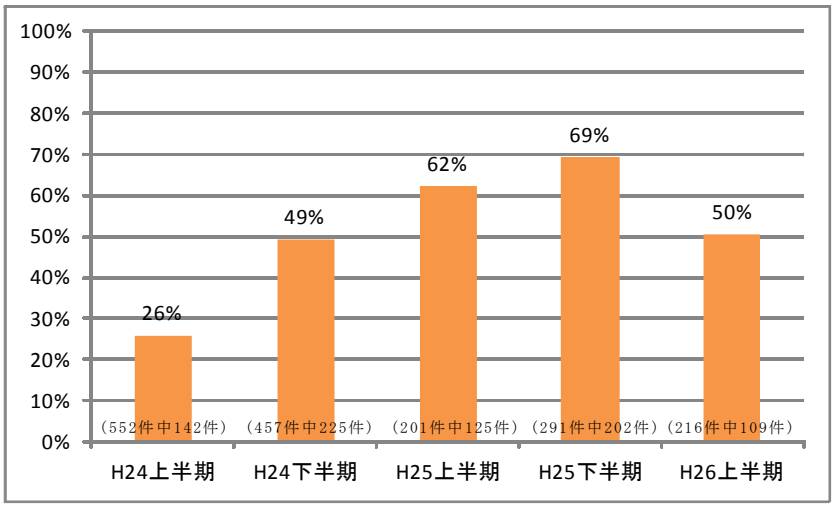


【圧縮ファイルに格納されたファイル形式の傾向】

【ショートカット（LNK）ファイル形式の不正プログラムの動作】

標的型メール攻撃の送信元アドレスとしてフリーメールアドレス*6 を使用するものの割合は、約５割（216件中109件）であった。フリーメールアドレスを使用した攻撃は、前年よりは減少したものの引き続き多数発生していることから、このようなメールについて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重要である。

*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。



【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】

(3) 標的型メール攻撃の事例

【就職活動を装った標的型メール攻撃の増加】

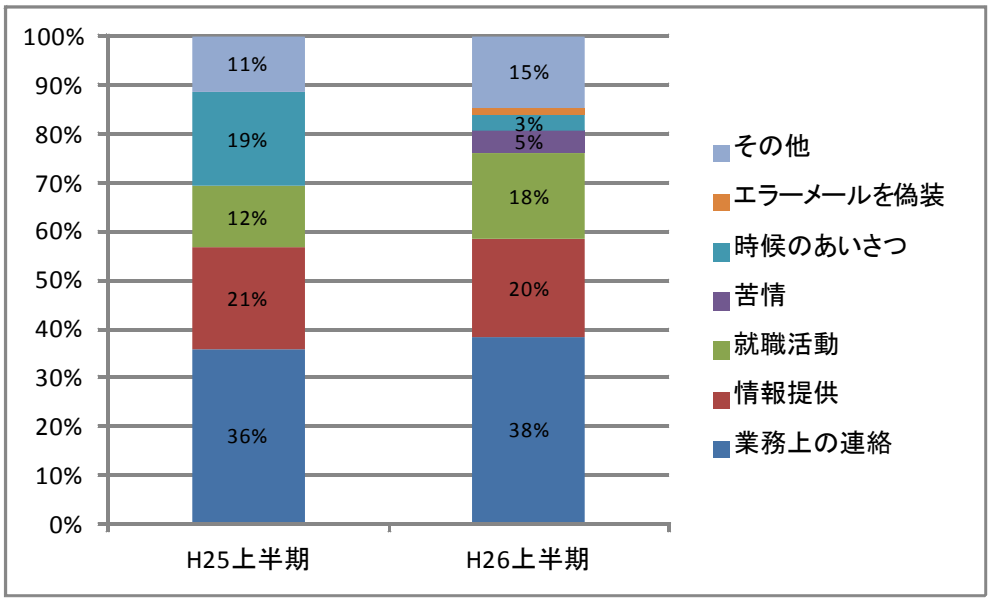
標的型メールの内容をみると、昨年同期と同様に、業務上の連絡を装ったものや情報提供を装ったものが多数みられた。また、前年にもみられた、就職活動中の学生等を装い履歴書等と称して不正プログラムを含むファイルを送り付ける手口の割合が18%（前年同期比＋６ポイント）に増加した。また、企業に対する苦情の送付を装い、詳細を記載した添付ファイルを開かせようとする手口を初めて確認した。

採用担当のメールアドレスは公開されていることが多く、履歴書等が送付されても違和感が少ないことから、就職活動を装う手口が多用されるようになっているものと考えられる。採用応募の受付で使用するコンピュータについては、社内ネットワークと隔離するなどの対策を講じることが重要である。

【Android端末を狙った標的型メール攻撃】

昨年に引き続き、Android OSを搭載したスマートフォンを狙った標的型メール攻撃を確認した。この攻撃は、メール本文に記載されたリンクをタップすることで､インターネット上のウェブサイトに接続し､Android向けの不正プログラムをダウンロードするようになっていた。

近年、企業活動において、スマートフォンやタブレット端末の活用が進んでいることから、今後も、モバイル端末を狙ったサイバー攻撃が発生するおそれがあり、警戒を要する。このような端末については、業務とは関係のないアプリを導入できないようにすることや、機密性の高い情報を取り扱う場所には持ち込みを制限するなどの対策を講じることが重要である。



【標的型メールの本文の内容】

3　新たな技術・サービスに起因する事犯

(1)　概況　－３Ｄプリンタ、ビットコイン等、新たな技術の悪用－

平成26年上半期には、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、以前は想像もできなかった新たな技術・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、３Ｄプリンタのような現実空間を対象としている新たな技術についても、サイバー空間に直接的に関わりはない一方で、手製拳銃の製造のように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った事案も発生していることから、動向を注視していく必要があると考えられる。

(2)　事例

【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とみられる手製拳銃を自宅において所持していたことにより、男１名を銃砲刀剣類等取締法違反（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。

技術の進展により家庭用の３Ｄプリンタが出回り始め、また、設計図データもインターネットを通じて容易に入手可能であったことを端に発生した事件であり、誰でも簡単に銃を作成できる時代になったことを示すものであった。

【ビットコイン】

ビットコインは、サイバー空間上での新たな取引方法として利用され、日本でも取り扱っている飲食店等が存在するなど、利用の幅が広まってきている。26年２月、大手ビットコイン取引所の取引が停止したことが大きな話題となり、電子計算機使用詐欺の疑いで警視庁が捜査を行っている。

ビットコインは、新たな決済手段として注目されている一方で、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）で検挙された男は、ビットコインを利用して覚醒剤を購入した旨を供述している。

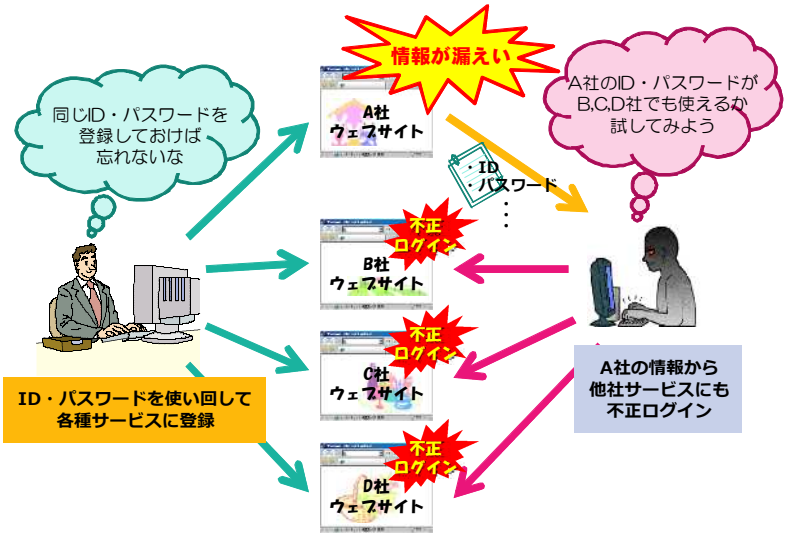
４　連続自動入力プログラムによる不正ログイン攻撃[*7]

(1)　概況　－続く不正ログイン被害－

平成26年上半期には、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、大きな話題となった。リスト型攻撃そのものは以前から発生しており、25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。本年に入っても同種のリスト型攻撃は依然として発生しているとみられ、引き続き警戒していく必要がある。

---

*7　インターネット利用者の多くが複数のウェブサイトで同一のID、パスワードを使い回ししている状況に目を付け、不正取得した他人のID、パスワードのリストを悪用して、連続自動入力プログラムを用いてID、パスワードを入力し、不正アクセス行為を敢行する手口による攻撃



【リスト型攻撃の概要】

(2)　被害防止対策

ウェブサイト管理者は複数のウェブサイトで同じパスワードを使用することの危険性を周知するとともに、個人認証を強化するなどの対策を講じる必要がある。また、インターネット利用者もパスワードの使い回しをしない、定期的にパスワードを変更するなどパスワードの適切な設定・管理に努め、リスト型攻撃による被害拡大の防止を図る必要がある。

5　その他サイバー空間の特性に起因する特徴的な事犯

(1)　概況　－匿名性・拡散性による被害の発生・拡大－

インターネットは、スマートフォン、携帯ゲーム機等のモバイル端末からも手軽に接続することができるようになったことで、人と人をつなげる非常に身近で便利なツールとして国民生活に幅広く浸透している。他方、サイバー空間には、匿名性や拡散性といった特性があり、そうした特性を踏まえた上でインターネットを利用しなければ、様々な問題に巻き込まれることがある。

平成26年上半期には、インターネットの仲介サイトで依頼したベビーシッターに預けられた男児が死亡する事件や、インターネット上への元交際相手に係るわいせつ画像等の掲載事案が社会的な問題となった。

(2)　事例

【業務仲介サイト】

平成26年３月、インターネット上のベビーシッター仲介サイトを通じてシッターに預けられた男児が死亡する事件が発生した。被疑者は偽名を使って仲介サイトに登録していた。この事件を受け、シッターの身元確認が十分でない仲介サイトも多く存在することが発覚し、インターネ

ット上でやりとりを行う業務仲介サイトの問題点が浮き彫りとなった。

【インターネット上への元交際相手に係るわいせつ画像の掲載】

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。

【SNSへの投稿】

SNSへの投稿の内容から発展して、偽計業務妨害罪、殺人未遂罪等で逮捕に至る事案も発生した。SNSは、気軽に投稿でき、特に若者の間で頻繁に利用されている。しかしながら、殺人をほのめかす投稿や自身の女性器が写った画像の投稿等、その投稿が社会にどういった影響を与えるのかという認識に欠けた投稿がなされる事案が発生している。

【犯罪の準備行為】

SNSの普及により見知らぬ者とつながることが容易となっているほか、いわゆる闇サイトのような犯罪の温床となり得るコンテンツもサイバー空間には存在している。26年４月には、中国版のスマホアプリや闇サイトの求人を通じて偽装結婚をあっせんしていたブローカー及び当該あっせんを受け内容虚偽の婚姻届を提出した偽装結婚当事者の計５名を、電磁的公正証書原本不実記録罪及び同供用罪で検挙した。

(3) 被害防止対策

インターネットを利用する際には、通信の相手方が必ずしも信用に足るとは限らないことや、自らが投稿した書き込みが不特定多数の人間に閲覧される可能性があること、また、サイバー空間上であっても当然に各種犯罪が成立することなど、インターネットを利用する上で必要な基本的リテラシーを利用者が身に付け、例えば、通信の相手方が信用に値するかに留意するなど、サイバー空間の特性を常に意識をすることが重要である。また、ひとたびインターネット上に画像が流出すると、不特定多数に拡散し、完全に消去することは困難なことから、たとえ交際相手であっても、裸の画像等を撮影させたり他人に送信したりしないよう心掛けることが必要である。

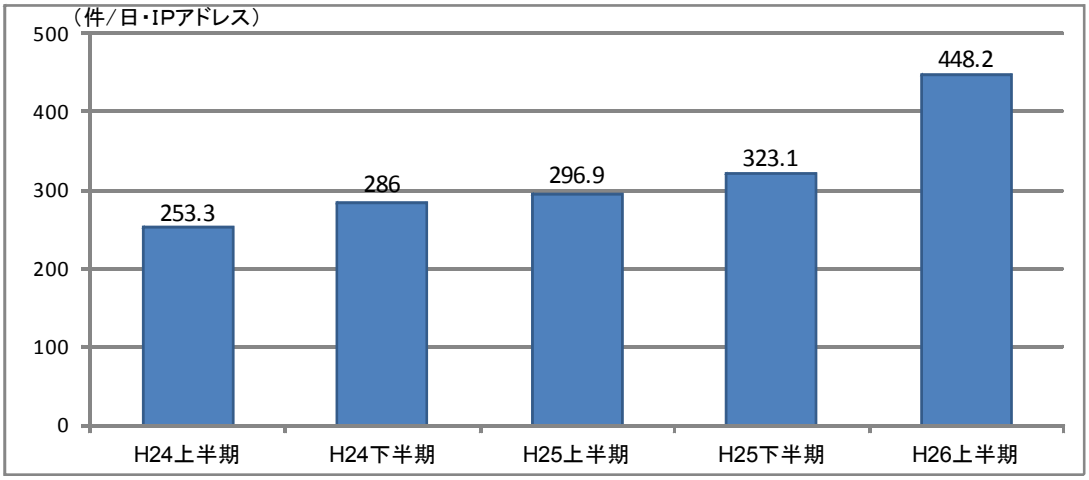
６　インターネットにおけるアクセス情報等の観測結果

(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。

平成26年上半期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448.2件で、前年同期に比べ151.3件、51.0%増加した。



【センサーに対するアクセス件数の推移】

26年上半期には、特にぜい弱性の有無等を探索する行為を多数観測した。攻撃の踏み台とすることが可能であるサーバの探索、攻撃コードが公開されているぜい弱性を有するバージョンのソフトウェア、機器等の探索等、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、ソフトウェア等の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) 事例

【各種リフレクター攻撃[*8] の踏み台となる機器の探索行為】

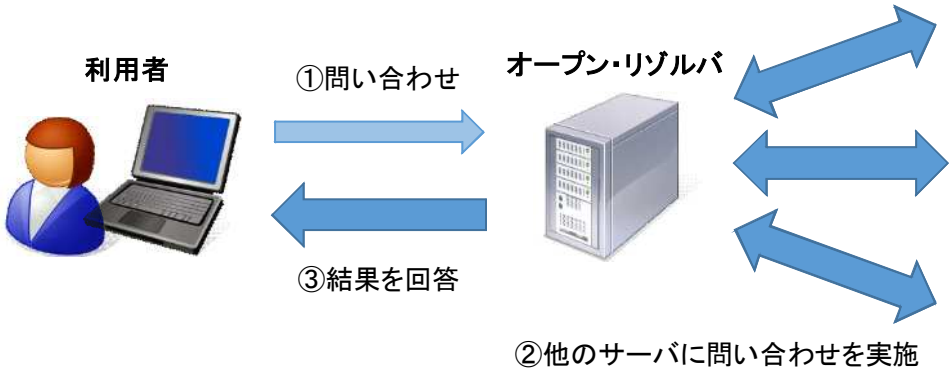
DNSリフレクター攻撃の踏み台となるオープン・リゾルバ[*9] の探索については、平成25年から継続して観測されているが、26年２月４日以降は、偽装された発信元IPアドレスからのオープン・リゾルバの探索行為に起因すると考えられるパケットも多数観測されている。またNTPやSNMPといっ

---

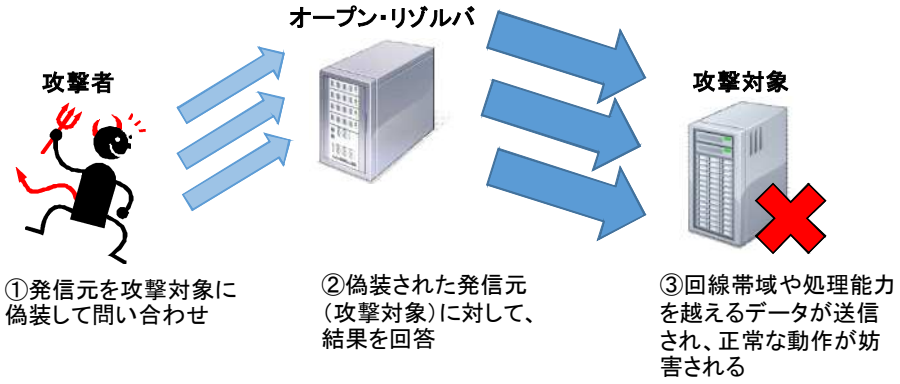
*8　サーバに対するリクエストと比較して、当該サーバからのレスポンスデータが大きくなるプロトコルを悪用して、送信元を攻撃対象に偽装してリクエストを送信することにより、攻撃対象に大量のデータを送信する攻撃手法のこと。

*9　外部ネットワークから任意のドメインについて問い合わせが可能なDNSサーバもしくは同様の機能が有効となっているコンピュータ等のこと。

たリフレクター攻撃に悪用が可能であるDNS以外のプロトコルについても、特に26年３月以降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。



【オープン・リゾルバの動作】



【DNSリフレクター攻撃の原理】

【OpenSSLのぜい弱性を標的としたアクセスの増加】

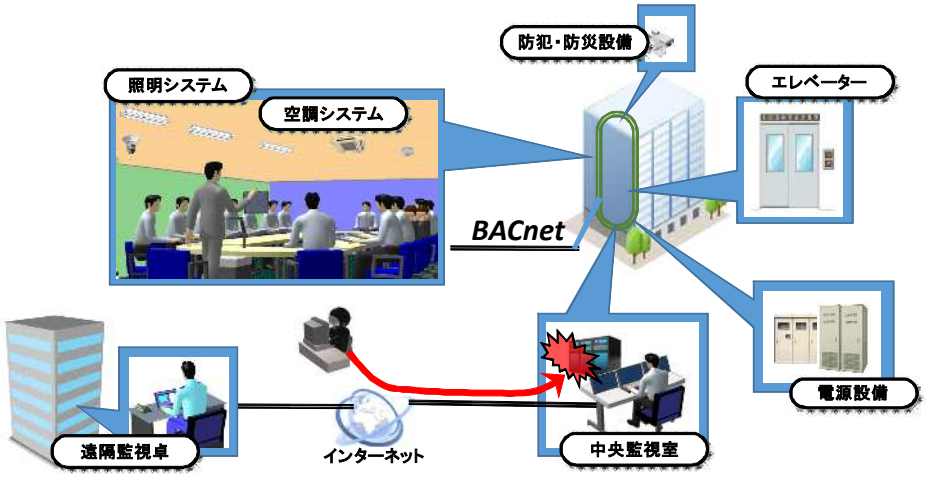
26年４月６日、個人情報、クレジットカード情報等の通信に使用されているソフトウェアである「OpenSSL」に深刻なぜい弱性が存在することが明らかとなった。ぜい弱性の有無を確認することが可能な攻撃コードも公開され、当該コードを使用したと考えられるパケットを観測した。

【ビル管理システムに対する探索行為】

26年３月中旬以降、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[*10] 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

*10 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のこと。

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。



【BACnetシステムの概要】

(3)　被害防止対策

インターネットにつながった各種機器を運用する際には、各種リフレクター攻撃に悪用される可能性があるプロトコルを使用しているサーバ等は攻撃の踏み台として悪用される可能性があること、ビル管理システムがインターネットにつながっている場合、遠隔監視等が行われる可能性があることなど、サイバー攻撃の被害に遭遇するだけでなく、攻撃の手助けをしてしまう可能性もあることを理解した上で、適切に運用することが必要である。

また、ソフトウェア等のぜい弱性を狙った攻撃の準備行為と考えられるパケットも多数観測されていることから、ぜい弱性が明らかになった際には、推奨されている対策を取る、ソフトウェアを最新のものにアップデートするなど、被害を防止するため迅速に行動することが重要である。

第３　検挙状況等

１　サイバー犯罪の検挙状況

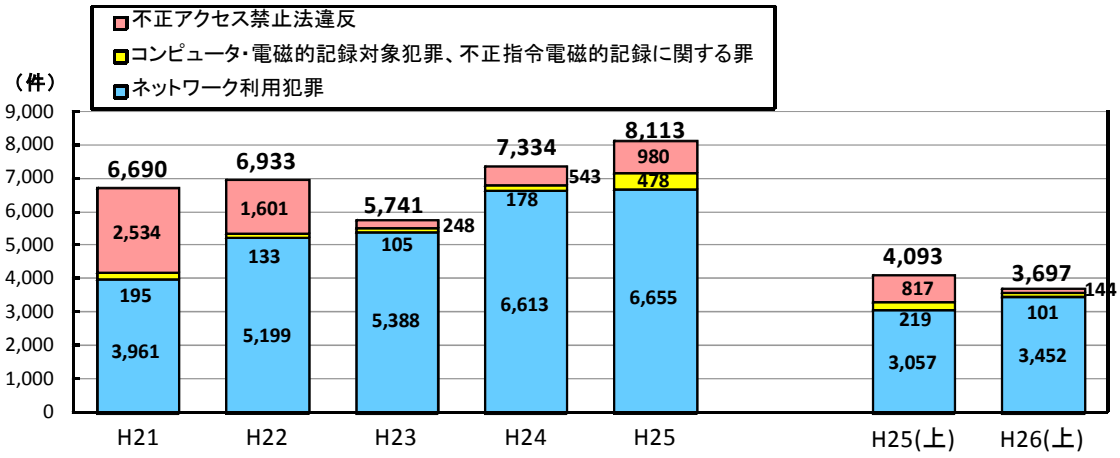
平成26年上半期のサイバー犯罪の検挙件数は3,697件(前年同期比-396件、-9.7%)

○　不正アクセス禁止法違反は144件(-673件、-82.4%)

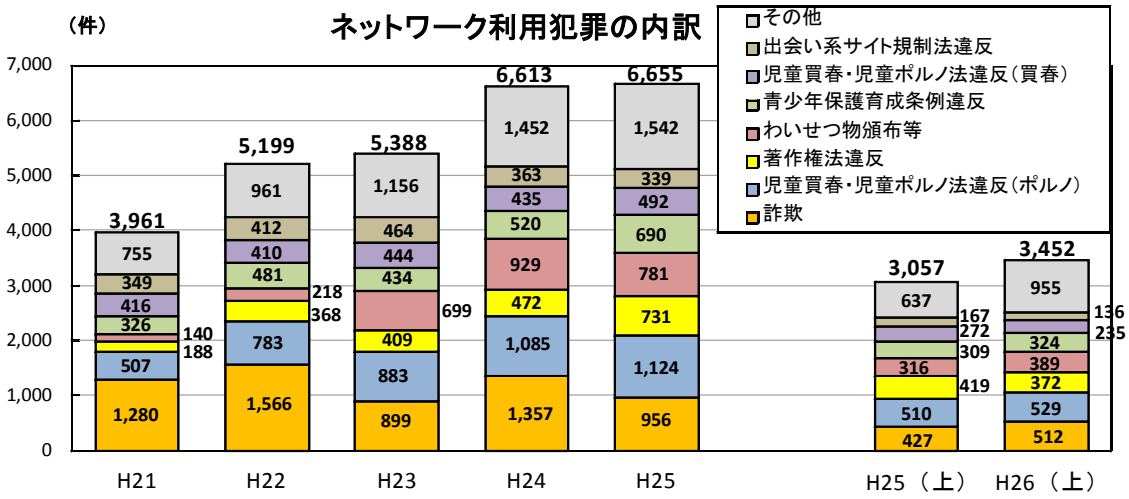
○　コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪は101件(-118件、-53.9%)

○　ネットワーク利用犯罪は3,452件(+395件、+12.9%)

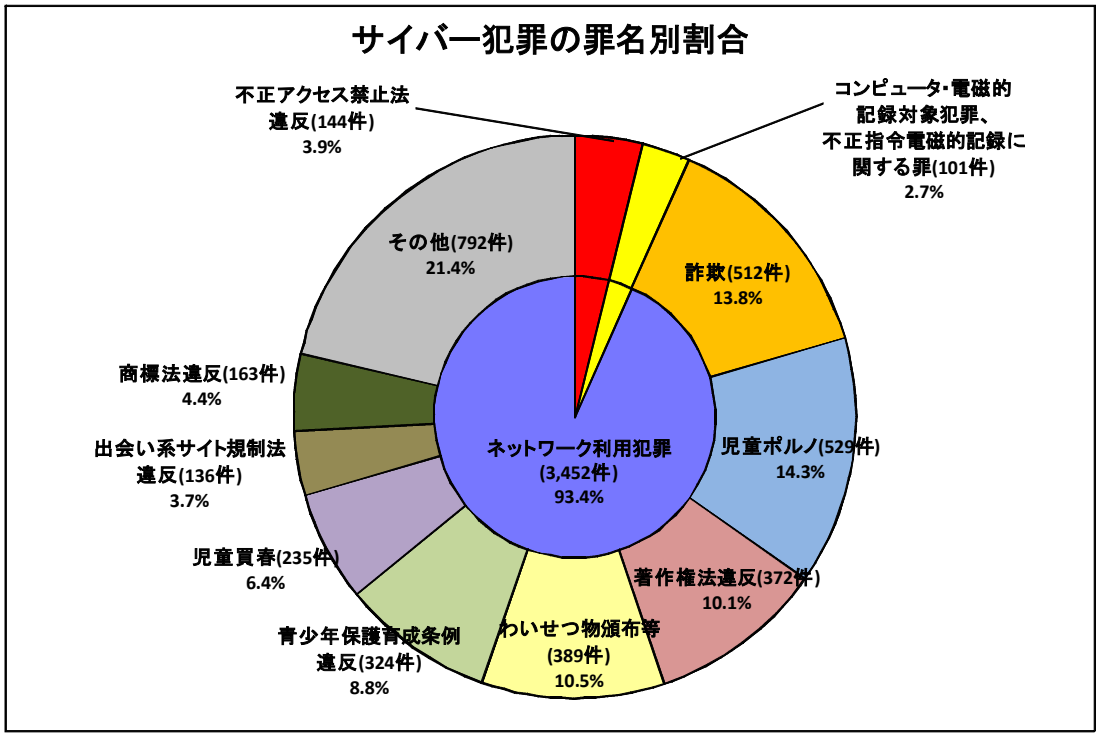
サイバー犯罪の検挙件数の推移



ネットワーク利用犯罪の内訳



サイバー犯罪の罪名別割合



【サイバー犯罪の検挙件数の内訳】

罪名＼年	H21	H22	H23	H24	H25	H25(上)	H26(上)	前年同期比増減	
不正アクセス禁止法違反	2,534	1,601	248	543	980	817	144	－ 673	－ 82.4%
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	195	133	105	178	478	219	101	－ 118	－ 53.9%
電子計算機使用詐欺	169	91	79	95	388	198	50	－ 148	－ 74.7%
電磁的記録不正作出・毀棄等	22	36	17	35	56	17	31	＋ 14	＋ 82.4%
電子計算機損壊等業務妨害	4	6	6	7	7	3	3	± 0	＋ 0.0%
不正指令電磁的記録作成・提供				4	8		6	＋ 6	－
不正指令電磁的記録供用			1	34	14	1	8	＋ 7	＋ 700.0%
不正指令電磁的記録取得・保管			2	3	5		3	＋ 3	－
ネットワーク利用犯罪	3,961	5,199	5,388	6,613	6,655	3,057	3,452	＋ 395	＋ 12.9%
詐欺	1,280	1,566	899	1,357	956	427	512	＋ 85	＋ 19.9%
うちオークション利用詐欺	522	677	389	235	158	70	134	＋ 64	＋ 91.4%
児童買春・児童ポルノ法違反（児童ポルノ）	507	783	883	1,085	1,124	510	529	＋ 19	＋ 3.7%
著作権法違反	188	368	409	472	731	419	372	－ 47	－ 11.2%
わいせつ物頒布等	140	218	699	929	781	316	389	＋ 73	＋ 23.1%
青少年保護育成条例違反	326	481	434	520	690	309	324	＋ 15	＋ 4.9%
児童買春・児童ポルノ法違反（児童買春）	416	410	444	435	492	272	235	－ 37	－ 13.6%
出会い系サイト規制法違反	349	412	464	363	339	167	136	－ 31	－ 18.6%
商標法違反	126	119	212	184	197	103	163	＋ 60	＋ 58.3%
その他	629	842	944	1,268	1,345	534	792	＋ 258	＋ 48.3%
合　　計	6,690	6,933	5,741	7,334	8,113	4,093	3,697	－ 396	－ 9.7%

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】

○　会社役員の男（34）ほか１名は、中国から日本のインターネット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25年10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。26年２月、不正アクセス禁止法違反で検挙した。

なお、中継サーバを使うと、海外の利用者が日本国内のパソコンを装ってネットに接続できる上、利用者のIPアドレスの履歴を保存せずに匿名化するため、犯罪に悪用されても追跡できない仕組みであった。（警視庁、埼玉）

○　大学生の男（24）は、25年６月、インターネットのチャットで購入した大手インターネットショッピングサイトのID、パスワードを用いて不正アクセ

スし、同サイト利用者に付与されたポイントを電子マネーに交換する虚偽の情報を与え財産上不法な利益を得た。25年12月、不正アクセス禁止法違反及び電子計算機使用詐欺で検挙した。(岐阜、兵庫)

○　中学校教諭の男（43）は、25年10月から同年12月にかけて、知人女性が登録している旅行情報サイトに、女性のID、パスワードを用いて不正アクセスし、ホテルの予約履歴などを閲覧した。26年３月、不正アクセス禁止法違反で検挙した。(広島)

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】

○　会社員の男（27）は、24年５月、元交際相手のスマートフォンに、同スマートフォンの遠隔操作を可能にさせるアプリケーションを秘匿にインストールし、同女に無断で音声を録音したり位置情報を取得したりした。26年４月、不正指令電磁的記録供用で検挙した。(青森)

ネットワーク利用犯罪

【詐欺及び組織的犯罪処罰法違反（組織的詐欺）】

○　サイト運営者の男（33）らは、運営する出会い系サイトにおいて、あらかじめ準備していたメールアドレスを、女性会員のメールアドレスと偽って男性会員に販売して、購入代金をだまし取った。26年５月、詐欺及び組織犯罪処罰法で検挙した。(京都)

【わいせつ電磁的記録記録媒体陳列】

○　サイト運営者の男（43）らは、運営する出会い系サイトにおいて、女性会員が投稿したわいせつ動画の閲覧ができないという閲覧者の申し出に対して、わいせつ性を認識しながらシステムを操作して、閲覧可能な状態にした。26年２月、わいせつ電磁的記録記録媒体陳列で検挙した。(警視庁)

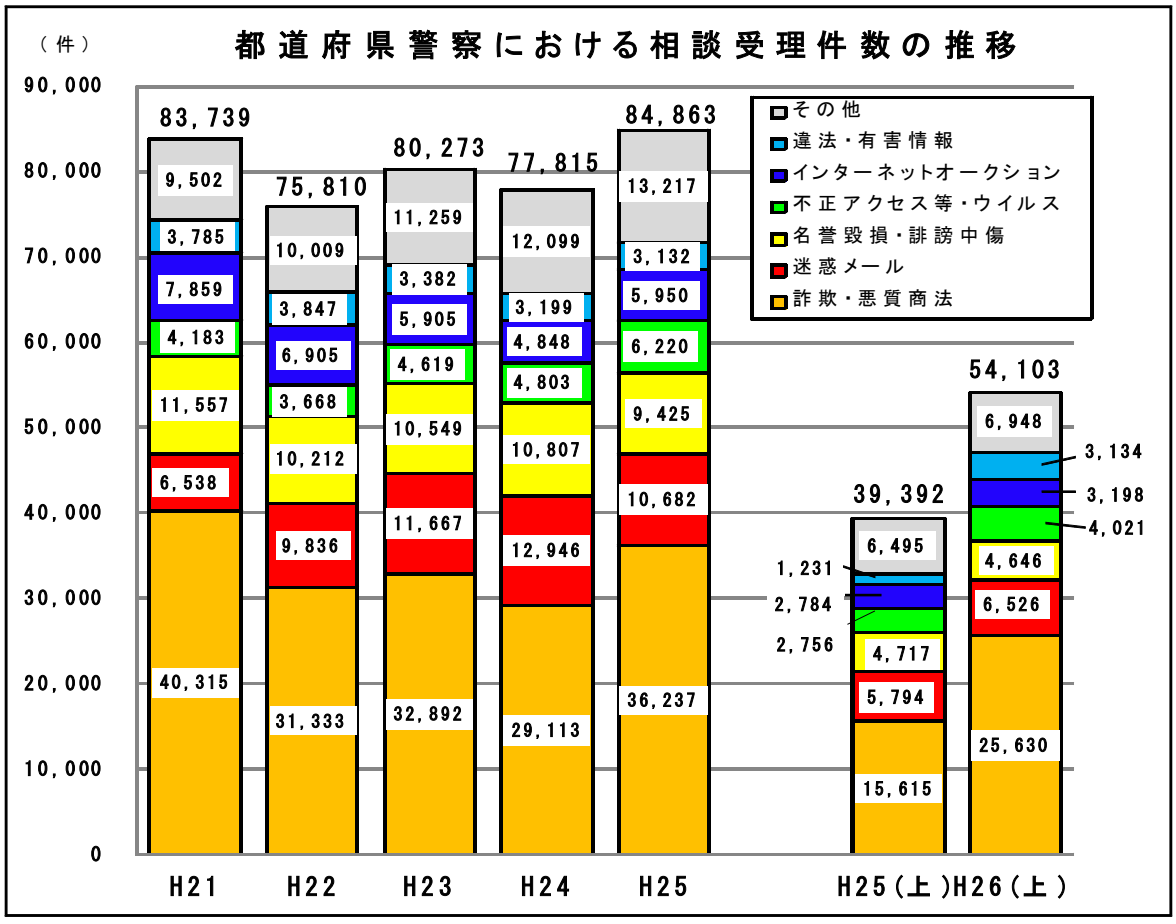
【不正競争防止法違反等】

○　会社役員の男（38）らは、不正な利益を得る目的で、電子書籍に施されている複製防止機能を解除するプログラムを提供し、不正競争を行った。26年２月、不正競争防止法違反等で検挙した。(京都)

３　サイバー犯罪に関する相談件数

【サイバー犯罪に関する相談の内訳】

	H21	H22	H23	H24	H25	H25（上）	H26（上）	前年同期比増減	
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）	40,315	31,333	32,892	29,113	36,237	15,615	25,630	+ 10,015	+ 64.1%
迷惑メールに関する相談	6,538	9,836	11,667	12,946	10,682	5,794	6,526	+ 732	+ 12.6%
名誉毀損・誹謗中傷等に関する相談	11,557	10,212	10,549	10,807	9,425	4,717	4,646	− 71	− 1.5%
不正ｱｸｾｽ等、ｺﾝﾋﾟｭｰﾀ･ｳｲﾙｽに関する相談	4,183	3,668	4,619	4,803	6,220	2,756	4,021	+ 1,265	+ 45.9%
インターネット・オークションに関する相談	7,859	6,905	5,905	4,848	5,950	2,784	3,198	+ 414	+ 14.9%
違法・有害情報に関する相談	3,785	3,847	3,382	3,199	3,132	1,231	3,134	+ 1,903	+ 154.6%
その他	9,502	10,009	11,259	12,099	13,217	6,495	6,948	+ 453	+ 7.0%
合　　計	83,739	75,810	80,273	77,815	84,863	39,392	54,103	+ 14,711	+ 37.3%



４　相談事例

詐欺・悪質商法に関する相談

○　身に覚えのないアダルトサイトの退会料金を支払えと請求された。

○　ネットショッピングで商品を購入し代金を支払ったが、商品が届かず、相手と連絡も取れなくなった。

迷惑メールに関する相談

○　出会い系サイトやアダルトサイトの広告メールが大量に送られてきた。

○　懸賞金が当たったとか財産を分与するという怪しい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実名を載せられ、誹謗中傷する内容を書き込まれた。

○　会社の信用を低下させるような事実無根の書き込みをされた。

不正アクセス等に関する相談

○　ＳＮＳのアカウントを乗っ取られ、勝手に利用された。

○　インターネットバンキングで不正アクセスされ、他人の口座宛てに送金された。