広　報　資　料
平成27年９月17日
警　　察　　庁

平成27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) 標的型メール攻撃の認知件数の増加

○　警察が把握した標的型メール攻撃は1,472件。

○　日本年金機構を始めとする我が国の多数の団体、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。

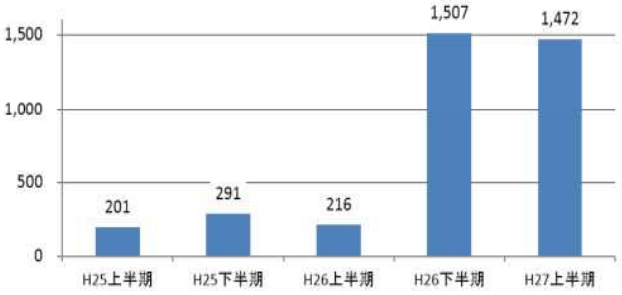
○　非公開メールアドレスに対する攻撃が全体の約９割。

○　送信元アドレスの詐称、確定申告制度を踏まえた攻撃等手口が巧妙化。

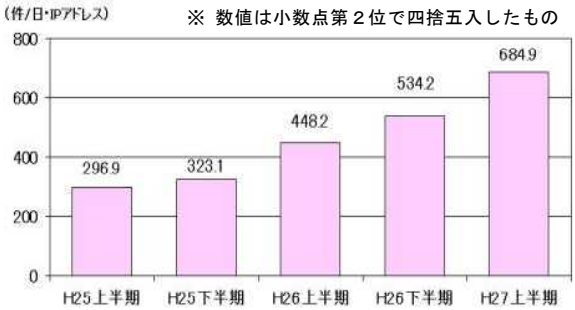
(2) サイバー空間における探索行為の増加

○　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684.9件。

○　攻撃の踏み台となり得るプロキシ等に対する探索行為が増加。



【警察が把握した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) 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拡大

○　27年上半期の被害額は約15億4,400万円で、前年下半期を上回り、引き続き大きな脅威。

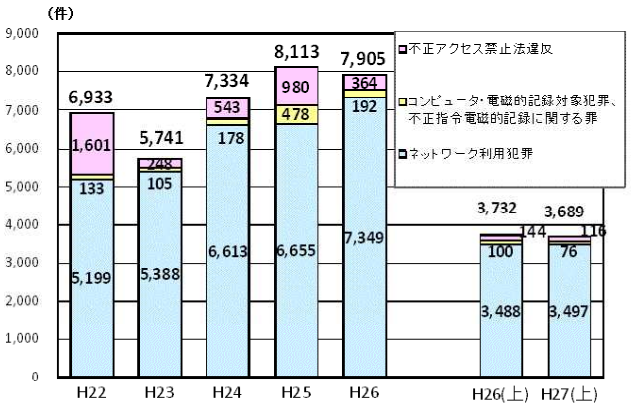
○　信用金庫、信用組合、農業協同組合及び労働金庫に被害が拡大。

２　サイバー犯罪の検挙状況等

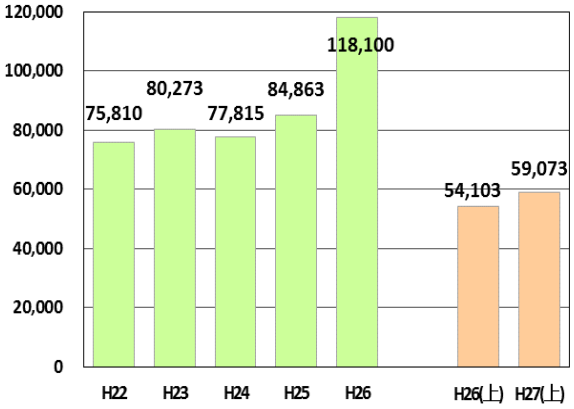
○　サイバー犯罪の検挙件数は3,689件。

○　ネットワーク利用犯罪の検挙件数は高水準で推移。

○　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59,073件。



【サイバー犯罪の検挙件数】



【サイバー犯罪等に関する相談件数】

別添

平成27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27年上半期における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　標的型メール攻撃の認知件数の増加

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

また、警察が把握した標的型メール攻撃は1,472件で、前年同期比で1,256件、581%増加した。標的型メール攻撃の特徴としては、26年下半期から「ばらまき型」攻撃が多発傾向にあることや、非公開メールアドレスに対する攻撃が全体の９割を占めていること等、攻撃が活発かつ巧妙化していることが認められる。

２　サイバー空間における探索行為の増加

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684.9件と、前年同期より52.8%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。主な要因は、攻撃の踏み台ともなり得るプロキシに対する探索行為の大幅な増加であるが、ウェブサイトで利用されるソフトウェアのぜい弱性に対する探索行為が継続的に観測されたことに加え、新たな動きとして、産業制御システムで利用されるソフトウェアのぜい弱性及びデータベースソフトウェアに対する探索行為を多数確認した。

３　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拡大

インターネットバンキングに係る不正送金事犯の被害は、昨年過去最悪を記録したが、27年上半期の被害額は26年下半期をさらに上回った。

被害対象は、銀行から信用金庫や組合等の金融機関に拡大している。

なお、犯行に使用される不正プログラムには、対象とする金融機関を任意に変更できる機能を有するものがある。

また、サイバー空間をめぐる事犯としては、他人の無線LANを乗っ取り、不正アクセス等に利用した事件等を検挙している。

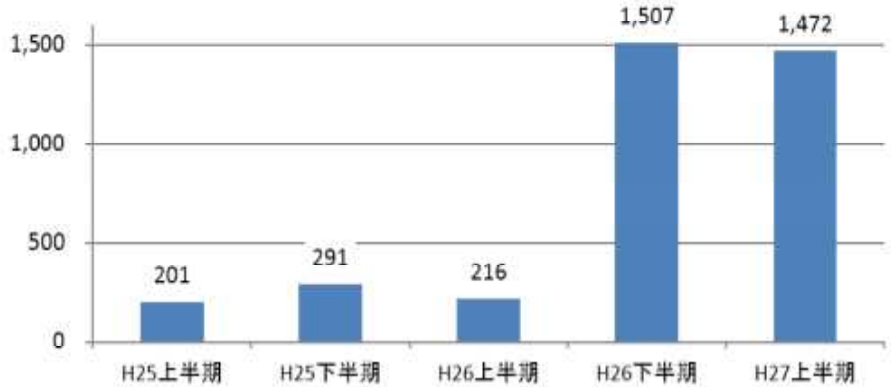
第２　各個別事犯等の情勢

１　サイバー攻撃関連

(1) 概況

平成27年上半期は、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、所要の捜査を推進するとともに、被害の未然防止・拡大防止を図っている。また、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] を通じて、27年上半期中、1,472件の標的型メール攻撃の発生を把握した。警察において把握した情報の分析結果に基づき事業者に対して注意喚起を実施した結果、新たに標的型メール攻撃の可能性のあるメールが599件確認され、被害の未然防止や拡大防止につながった。

【標的型メール攻撃の概要】



【警察が把握した標的型メール攻撃の件数】

---

*1　警察と先端技術を有する全国6,957の事業者等（27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

平成27年上半期に警察が把握した標的型メール攻撃は1,472件と、前年同期と比較して大幅に増加した。これは、26年下半期と同様に、英文の「ばらまき型」攻撃が多数発生したためであり、全体の約９割を占めた。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。

なお、この「ばらまき型」攻撃において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で検知可能であることが確認されている。

	ばらまき型	ばらまき型以外
26年上半期	40%(　86件)	60%(　130件)
26年下半期	92%(1,388件)	８%(　119件)
27年上半期	92%(1,347件)	８%(　125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約９割を占めており、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、フリーメールアドレス[*2] を使用するものの割合が昨年より大幅に減少した一方で、攻撃対象の事業者等や実在する事業者等のメールアドレスを詐称したと考えられるものが多数確認された。

○　Word文書を添付した攻撃の急増

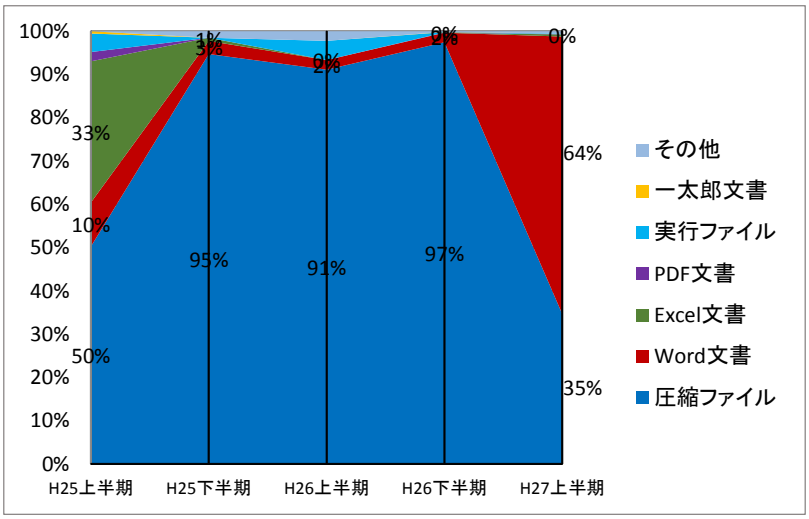
標的型メールに添付されたファイルの傾向としては、圧縮ファイルの割合が昨年より大幅に減少した一方で、Word文書が添付されたものが大幅に増加した。その多くは、複合機[*3] のスキャナ機能により読み込んだ文書の送付や品物の発送代金の請求等の業務上の連絡を装ったものであった。

---

*2　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。

*3　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。

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。



【標的型メールに添付されたファイル形式の割合】

(3) 事例

○ 我が国の確定申告制度を踏まえた攻撃

税務署からの確定申告に関する連絡を装った標的型メール攻撃を新規に把握した。これは、国税電子申告・納税システム「e-Tax」の利用者に対する確定申告に関する連絡を装ったものであり、申告書の受付時期を前にした１月下旬頃に発生した。

いずれの攻撃も、「申告に関するお知らせ.zip」という圧縮ファイルが添付され、展開（解凍）すると実行ファイル（EXE）が生成されるものであった。また、このファイルを実行すると、画面上には正当なものを装った文書の内容が表示される一方で、コンピュータが遠隔操作型の不正プログラムに感染する。

○ 昨今の電子機器の機能を踏まえた攻撃

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新規に把握した。

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」や「xerox2@[攻撃対象の事業者等のドメイン].jp」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おり、また、(2)に記載したWord文書が添付されていた。

(4) C2サーバの現況

平成27年上半期中、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[*4] 38台の機能停止（テイクダウン）を実施しており、昨年一年間を通じてテイクダウンを実施した33台を既に上回った。

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[*5] 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。

---

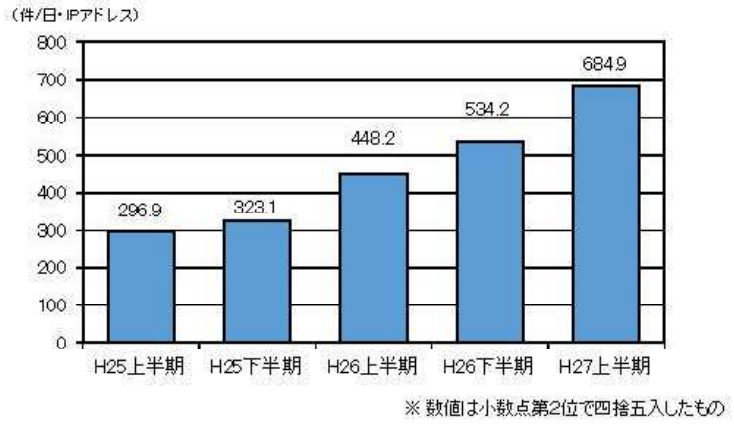
*4　Command and Control server（指令制御サーバ）の略。C&Cサーバと省略する場合もある。攻撃者の命令に基づいて動作する、不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

*5　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。

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。



【センサーに対するアクセス件数の推移】

平成27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684.9件で、前年同期に比べ増加した。主な増加の要因は、不正アクセス等の攻撃の踏み台として悪用することを企図したと考えられるプロキシに対する探索行為が大きく増加したためである。また、27年上半期には、これまでの観測と同様にウェブサイトで利用されるソフトウェアのぜい弱性を標的とした探索行為を継続して観測したことに加え、新たな探索行為として、産業制御システムで利用されるソフトウェアのぜい弱性を標的とした探索行為及びデータベースソフトウェアに対する探索行為を多数確認した。

(2) 事例

【ウェブサイトのぜい弱性を標的としたアクセス】

ウェブサイトのぜい弱性を標的としたアクセスについては、従来から継続的に観測されているものであるが、平成27年上半期においても引き続き多く観測した。

ブログサイト等のウェブサイトの構築に広く使用されているソフトウェアであるWordPressのぜい弱性は、これまでも多く公表されてきているが、27年上半期には、当該ぜい弱性を利用したウェブサイトの改ざんを確認しており、センサーにおいても、WordPressで構築されたウェブサイトに対するアクセスを観測した。

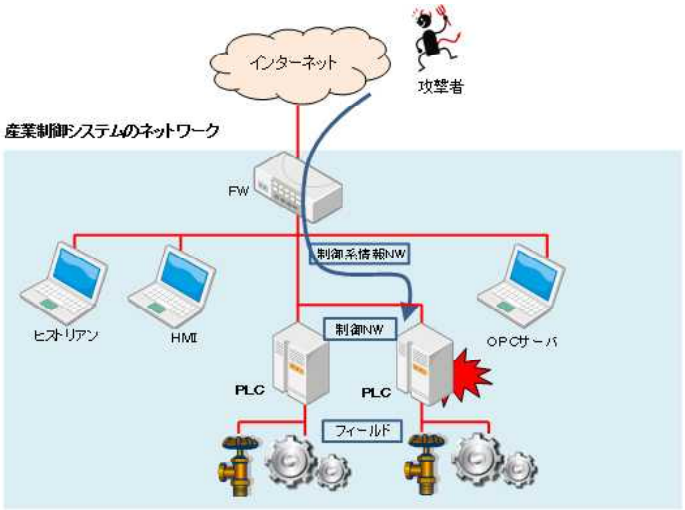
特に、WordPressの管理画面に対してアクセスを試みるものが多く、これは、WordPressの管理機能にログイン可能なウェブサイトを探索しているものであると考えられる。

また、Bash[*6] のぜい弱性（26年９月公表）やCGI[*7] 版PHP[*8] のぜい弱性（24年５月公表）等公表されてから時間が経過したぜい弱性を標的としたアクセスも継続的に観測している。

【産業制御システムを標的としたアクセス】

産業制御システムは、製造業を始めとして、電力・水道等のライフライン、石油化学プラント等のインフラ設備等における監視制御に利用されているシステムである。適切な対策を施さずにインターネットに接続している場合は、攻撃者に侵入され、システムを不正に操作されるおそれがある。

27年上半期には、産業制御システムで使用される特定のPLC[*9] のソフトウェアのぜい弱性を標的としたアクセスを観測した。また、このほかにも、産業制御システムで使用される複数のプロトコルを標的としたアクセスを継続して観測した。アクセスの多くは、セキュリティに関する調査を実施している組織からのものであるが、目的の判明しないアクセスも観測しており、当該ぜい弱性を悪用する目的で探索が行われている可能性も考えられる。



【産業制御システムへの攻撃のイメージ】

---

*6　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。

*7　Common Gateway Interfaceの略。ウェブサーバ上でプログラムを起動させるための仕組み。

*8　PHP:Hypertext Preprocessorの略。ウェブアプリケーションで多く使われているプログラミング言語。

*9　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。

【NoSQLデータベースソフトウェアに対する探索行為】

近年、「ビッグデータ」といった用語で表現される大規模データの収集、分析等の需要が増大する中、従来のデータベース管理システムでは実現できない性能や特性を持つ新しいデータベース管理システムが「NoSQL」と総称され、注目を集めている。

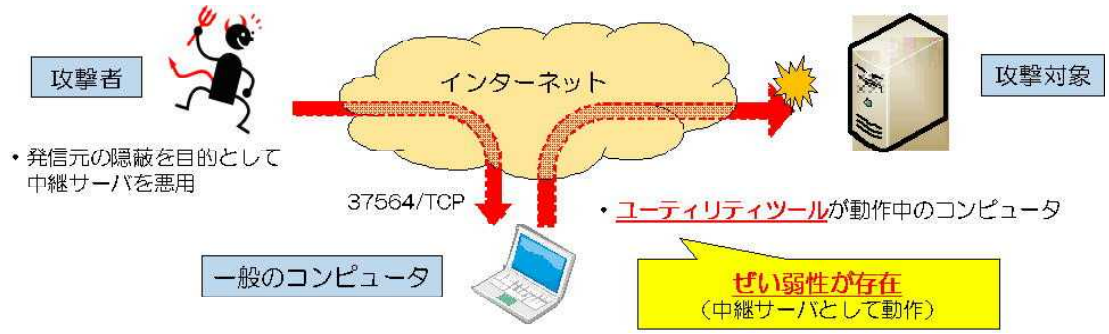
27年１月から２月にかけて、「NoSQL」に分類されるデータベース管理システムであるMongoDB、Redis及びmemcachedが稼働しているコンピュータを探索し情報収集を試みるアクセスの増加が認められ、２月以降も依然として高い水準で推移している。これらアクセスの中には、情報窃取を目的とし、アクセス制限や適切な認証等が施されていないデータベースソフトウェアを探索するアクセスも含まれる可能性があることから、これらのデータベース管理システムを使用している企業や組織においては、適切な対策を行うことが望ましい。また、これらの情報の蓄積を行い、その結果を検索サイトで公表している組織が存在し、その組織からのアクセスも観測されている。攻撃を企図する者が、この情報を悪用する可能性も危惧される。

【プロキシを標的とした探索行為】

「プロキシ」は、接続を中継するサービスであり、通信の高速化や安全性の強化等を目的として利用される。設定の不備等により外部から利用可能な状態となっているプロキシは、「オープンプロキシ」と呼ばれ、利用者のIPアドレスを匿名化するなどの特徴から、不正アクセス等の攻撃の踏み台として悪用される可能性がある。

27年上半期は、プロキシソフトウェアで使用される様々なポートに対するアクセスを多数観測した。これらのアクセスは、攻撃の踏み台を探索する目的で行われていると考えられる。以前から多数観測しているプロキシサーバで汎用的に利用されるポートを対象とした探索に加え、一般のコンピュータで稼働するプロキシソフトウェア等で利用されるポートを対象とした探索も多く観測した。

特に、５月には、プロキシサーバを探索しているアクセスの急増を観測したことから、調査を実施したところ、日本国内のオンラインゲームのユーティリティツール（ゲーム利用を簡便化するツール）に、誰もが利用可能なプロキシサーバとして動作するぜい弱性が存在することを確認した。ぜい弱性の存在する当該ユーティリティツールを動作させた日本国内の一般のコンピュータが、意図せずプロキシサーバとして踏み台にされ、サイバー犯罪・サイバー攻撃等への悪用が懸念されたことから、早期に注意喚起を実施した。



【ぜい弱性のあるユーティリティツールを悪用した攻撃】

(3) 被害防止対策

インターネットを利用する際には、使用しているソフトウェアのバージョンを確認し、ぜい弱性がある場合にはバージョンアップを行うことが必要である。また、各種サーバを運用する際には、不要なサービスは停止し、インターネットを介したアクセスが不要な場合には、インターネットからの接続を遮断することが重要である。さらに、インターネットを介してアクセスする場合にも、適切なアクセス制限や認証を実施する必要がある。

3　インターネットバンキングに係る不正送金事犯関連

(1) 概況

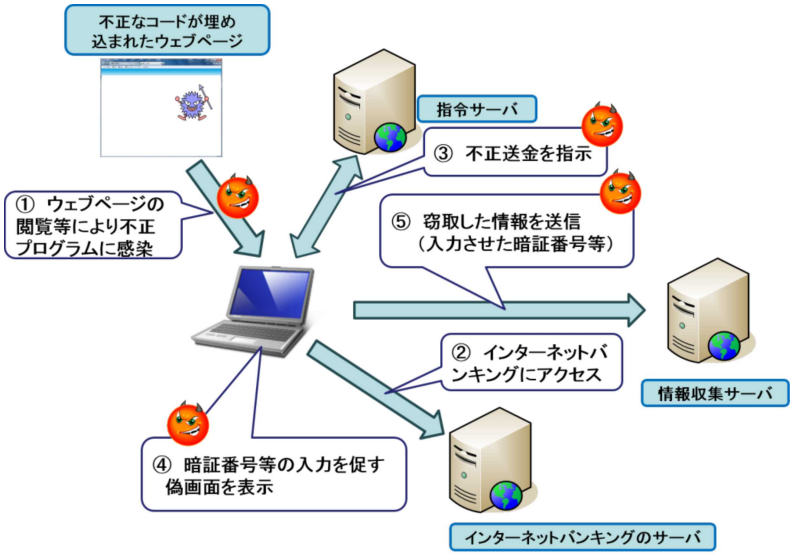
平成26年、インターネットバンキングに係る不正送金事犯による被害額は過去最悪の約29億1,000万円となったが、その脅威は本年に入っても続いており、27年上半期の被害額は、約15億4,400万円と26年下半期を上回っている。被害の特徴としては、信用金庫、信用組合に被害が拡大したこと、農業協同組合と労働金庫で被害が発生したこと等が挙げられる。

インターネットバンキングに係る不正送金事犯で使用される不正プログラムの特徴としては、主に以下が挙げられる。

○　不正プログラムがインターネット上のサーバと通信することにより、対象とする金融機関を任意に変更できる機能を有するものがある。

○　同様に、指令サーバを任意に変更できる機能を有するものがある。

○　ブラウザで送受信される情報を盗むのみならず、キーボードの入力情報を記録してインターネット上のサーバに送信するものもある。



【不正送金事犯で使用される不正プログラムの例】

(2) 警察における対策

○　民間事業者等と連携した抑止対策

警察では、金融機関に対し、インターネットバンキングのセキュリティ機能強化のための注意喚起、不正送金に悪用される口座を凍結するための口座情報・凍結口座名義人情報の提供を行うとともに、資金移動業者への国外送金の審査強化に関する働き掛け等を行っている。

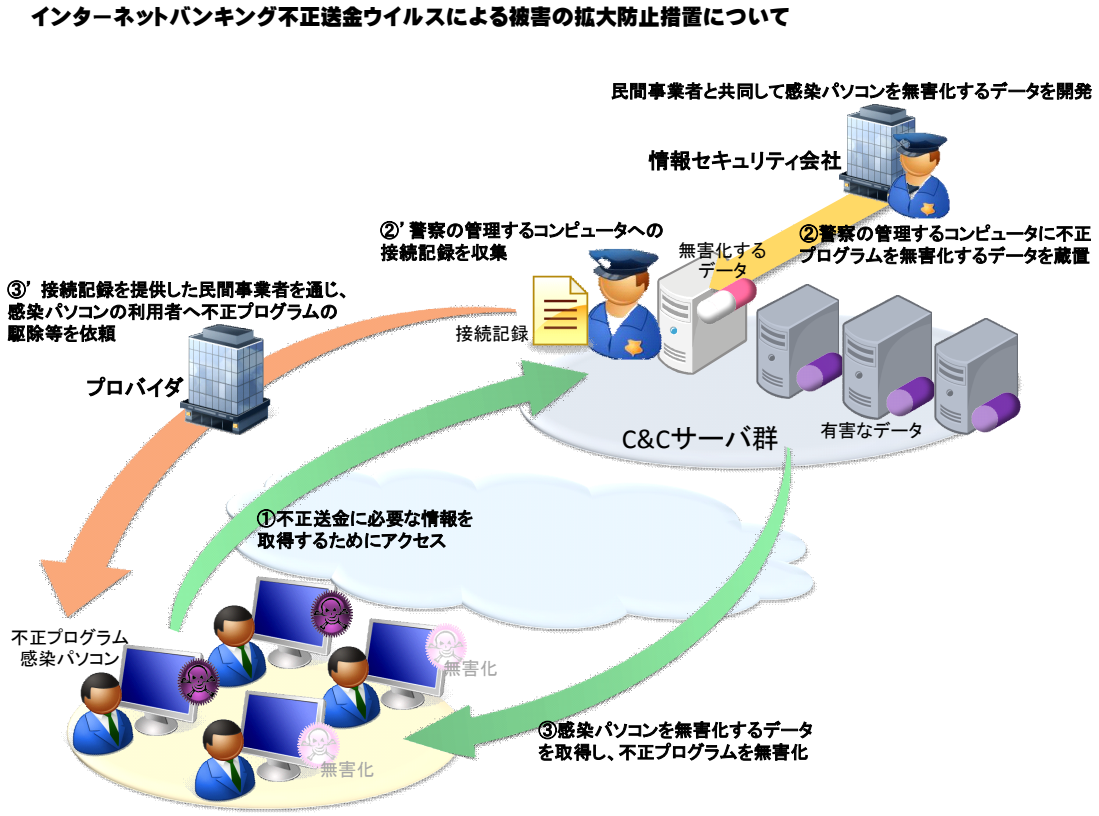
また、ウイルス対策ソフト事業者との情報交換を通じて、不正送金事犯に悪用されているボットネットの情報を入手し、金融機関と連携した口座停止措置を行うなどの対策を行っている。

○　不正プログラムの無害化作戦の実施

平成27年４月、警視庁は、インターネットバンキングに係る不正送金に利用されるC&Cサーバの動作を観測することにより、国内外において約８万2,000台の端末が不正プログラムに感染していることを把握し、不正プログラムによる被害の拡大防止措置を実施した。

警視庁は、プロバイダを通じた国内の感染端末の利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供に加え、画期的な被害拡大防止措置として、不正プログラムの無害化措置の実施にも成功した。

この不正プログラムは、ワンタイムパスワード[*10]の入力を促すための入力画面を表示させ、不正送金処理を自動で行うといった機能を有するものであった。C&Cサーバと定期的に通信を行うことで不正送金に必要な情報を入手するというこの不正プログラムの性質を逆手に取り、その代わりに無害なデータを取得させ、不正プログラムの無害化を行ったものである。



【インターネットバンキング不正送金に関する不正プログラムの無害化措置】

---

*10　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) 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。

○　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　サイバー空間の特性を利用した事犯

(1) 概況

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が、サイバー空間の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。さらに、サイバー空間を舞台とした事犯では、サイバー空間の匿名性、無痕跡性等の悪用が懸念されている。

27年上半期には、不正アクセス事犯、薬物の密輸入事犯等において、無線LANの乗っ取り、ビットコインの利用等の匿名化工作が確認された。

(2) 事例

【無線LANの乗っ取り】

無線LANはケーブル（有線）ではなく電波を使ってインターネット等に接続するシステムであり、電波が届く範囲であれば離れた場所でも使えることから、ホテルや駅、空港等公共の場での普及が進められる一方、不正アクセスに使われたり、情報を盗み見られたりする危険性が指摘されている。

27年上半期には、インターネットバンキングの不正送金に関わったとして別件不正アクセス禁止法違反事件で検挙した被疑者が、不正アクセスの際に隣家が設置する無線LANを乗っ取り利用していたことについても電波

法違反を適用し検挙した（警視庁：６月）。被疑者は、遠くの電波を受信することができるアダプターを自宅のパソコンに接続した上で無許可で無線局を開設し、隣家の無線LANに勝手に接続し、ただ乗りをしたとみられている。

また、不正に入手したIDとパスワードを使い、昨年12月、出版社のサーバに不正アクセスしてホームページを改ざんした少年を検挙している（警視庁：６月）が、この事案でも他人宅の無線LANを使用して犯行に及んでいたことが判明している。

【ビットコイン関連】

27年上半期において、ビットコインを利用した事件としては、海外の闇サイトから他人のクレジットカード情報を不正購入した事件（兵庫：３月）、危険ドラッグの原料となる指定薬物を密輸入した事件（警視庁：３月）、中国からの麻薬密輸入事件（警視庁：４月）がある。

検挙された被疑者らは、ビットコインを利用した理由について、匿名性が高いこと、正規の海外送金よりも手数料が安いことを供述している。

【その他】

サイバー空間をめぐるその他の事犯としては、少年による動画配信サイトへの投稿内容が社会的に大きな反響を呼んだ事案が発生しており、威力業務妨害等で検挙した。また、コミュニティサイト等を利用してプライベートな性的画像を公表する行為についても検挙している。

警察による危険ドラッグ事犯の取締りの徹底や関係機関と連携した各種取組等の結果、危険ドラッグの販売店舗は、27年７月に閉鎖が確認された[*11]が、一方で、インターネットを利用して危険ドラッグが流通している状況がうかがわれており、販売行為や輸入行為を検挙している。

４月に施行された第18回統一地方選挙においては、インターネット等を利用した違法な選挙運動について38件の警告を行った。

---

*11　厚生労働省の調査による。

第３　検挙状況等

１　サイバー犯罪の検挙状況

○　27年上半期のサイバー犯罪の検挙件数は3,689件

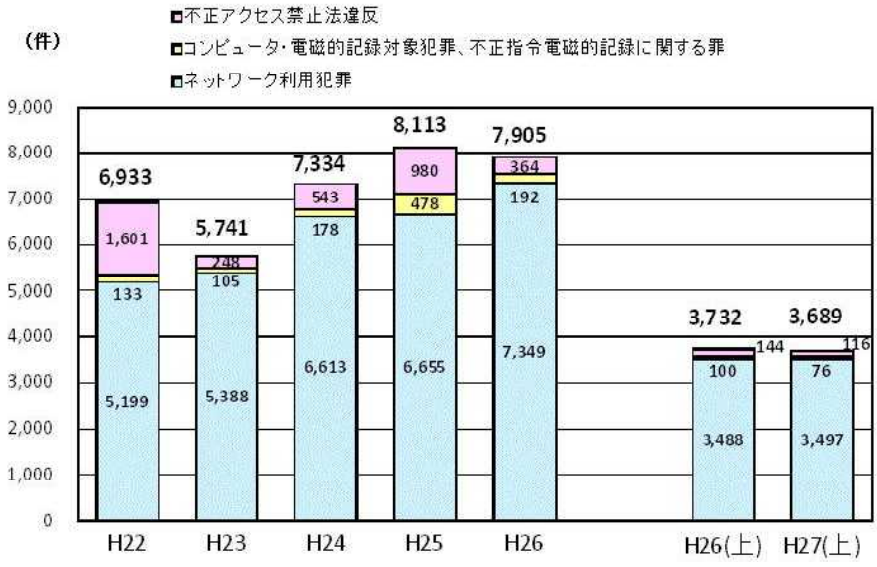
○　不正アクセス禁止法違反は116件

○　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76件

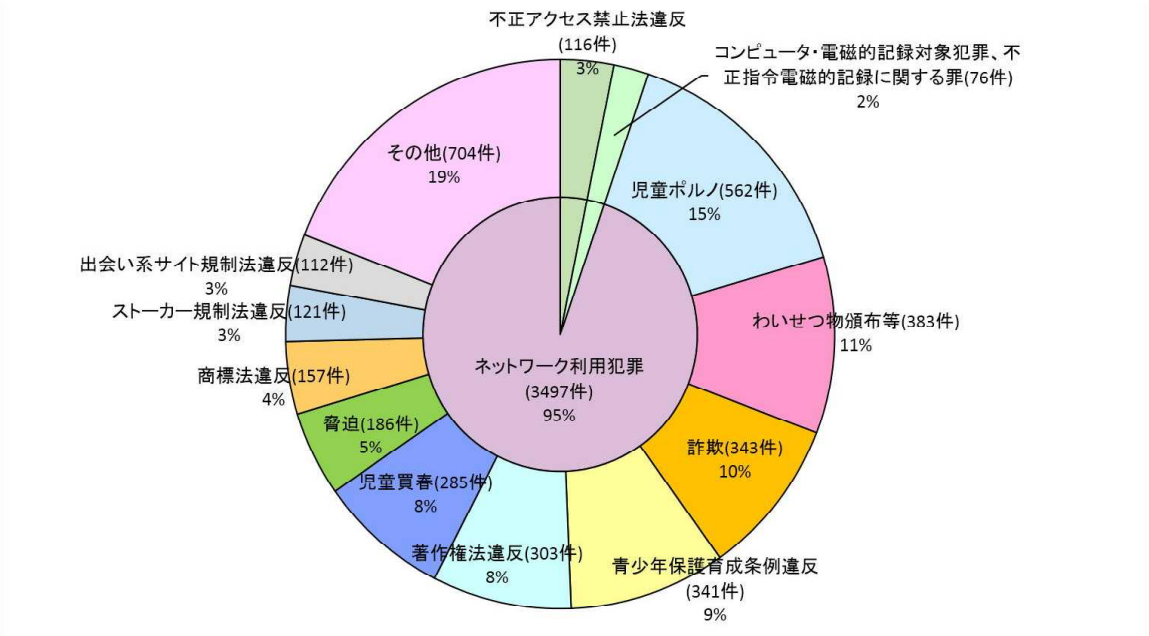
○　ネットワーク利用犯罪は3,497件

罪名＼年	H22	H23	H24	H25	H26	H26(上)	H27(上)
不正アクセス禁止法違反	1,601	248	543	980	364	144	116
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	100	76
電子計算機使用詐欺	91	79	95	388	108	50	47
電磁的記録不正作出・毀棄等	36	17	35	56	48	30	12
電子計算機損壊等業務妨害	6	6	7	7	8	3	4
不正指令電磁的記録作成・提供			4	8	9	6	3
不正指令電磁的記録供用		1	34	14	16	8	8
不正指令電磁的記録取得・保管		2	3	5	3	3	2
ネットワーク利用犯罪	5,199	5,388	6,613	6,655	7,349	3,488	3,497
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	530	562
わいせつ物頒布等	218	699	929	781	840	394	383
詐欺	1,566	899	1,357	956	1,133	516	343
うちオークション利用詐欺	677	389	235	158	381	135	143
青少年保護育成条例違反	481	434	520	690	657	325	341
著作権法違反	368	409	472	731	824	373	303
児童買春・児童ポルノ法違反（児童買春）	410	444	435	492	493	237	285
脅迫	67	81	162	189	313	165	186
商標法違反	119	212	184	197	308	164	157
ストーカー規制法違反	39	36	78	113	179	83	121
出会い系サイト規制法違反	412	464	363	339	279	136	112
その他	736	827	1,028	1,043	1,075	565	704
合　　計	6,933	5,741	7,334	8,113	7,905	3,732	3,689

【サイバー犯罪の検挙件数の内訳】　※H27(上）は暫定値



【サイバー犯罪の検挙の推移】　※H27(上）は暫定値



【ネットワーク利用犯罪の内訳】

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】

○　ホテル従業員の男（30）は26年９月、自身が運用する中継サーバに、不正に入手した他人のID及びパスワードを入力し、プロバイダ事業者のサーバへ不正アクセスしてインターネットへ接続した。27年１月、不正アクセス禁止法違反で検挙した。（山梨、神奈川、長野、静岡）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　接客業の男（29）は、26年９月から12月にかけて、勤務先の店舗内でスマートフォンを使用して来店客のクレジットカード情報を撮影し、その情報を使用して電子マネーを不正購入した。27年５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供用】

○　少年（17）らは、26年５月、スマートフォンから自動的に110番発信させる不正指令電磁的記録へ接続する短縮URLを、スマートフォンアプリにより拡散し、スマートフォン使用者が意図しない110番発信を全国で多数発生させた。27年２月、不正指令電磁的記録供用で検挙した。（兵庫・沖縄）

ネットワーク利用犯罪

【詐欺】

○　アルバイトの男（32）らは、女性向け無料アダルトサイトを騙って客を募り、サイト利用のために無料会員登録手続をさせ、後日、「登録したアダルトサイトを解約しなかったため延滞料金が発生している。支払わなければ裁判になるが、本日中に和解するためには和解金が必要。」などと連絡して現金を送付させた。27年２月、詐欺で検挙した。（千葉）

【特定商取引に関する法律違反】

○　サイトの運営法人及び同サイトの運営者の男（28）らは、同法人の業務に関し、インターネットによる申込みを受けて異性の紹介等の役務を提供する通信販売をするに当たり、相手方の承諾を得ていないにもかかわらず、電子メール広告をした。27年４月、特定商取引に関する法律違反で検挙した。（警視庁）

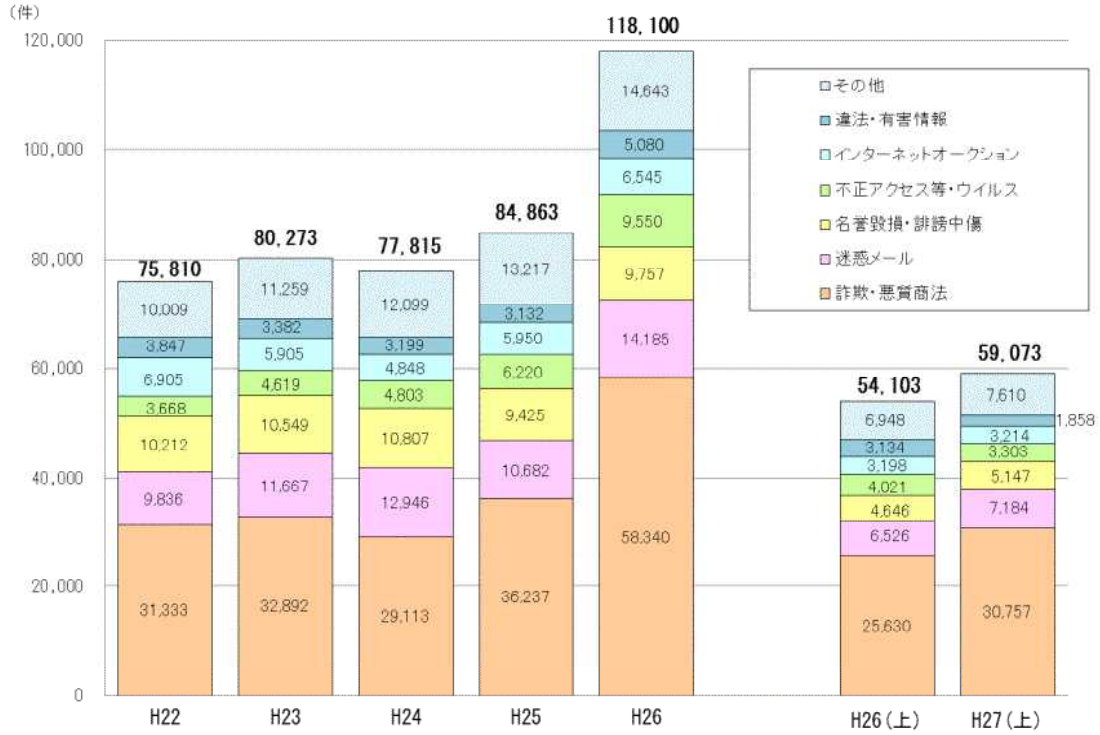
３　サイバー犯罪等に関する相談件数

○　27年上半期のサイバー犯罪等に関する相談件数は59,073件

○　最も多い相談内容は、詐欺・悪質商法に関する相談（ただしインターネット・オークション関係を除く）30,757件であり、増加率も大きい。

	H22	H23	H24	H25	H26	H26（上）	H27（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）	31,333	32,892	29,113	36,237	58,340	25,630	30,757
迷惑メールに関する相談	9,836	11,667	12,946	10,682	14,185	6,526	7,184
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	4,646	5,147
不正ｱｸｾｽ等、ｺﾝﾋﾟｭｰﾀ・ｳｲﾙｽに関する相談	3,668	4,619	4,803	6,220	9,550	4,021	3,303
インターネット・オークションに関する相談	6,905	5,905	4,848	5,950	6,545	3,198	3,214
違法・有害情報に関する相談	3,847	3,382	3,199	3,132	5,080	3,134	1,858
その他	10,009	11,259	12,099	13,217	14,643	6,948	7,610
合　　計	75,810	80,273	77,815	84,863	118,100	54,103	59,073

【サイバー犯罪等に関する相談の内訳】



【都道府県警察における相談受理件数の推移】

４　相談事例

詐欺・悪質商法に関する相談

- スマートフォンでアダルトサイトの動画再生ボタンを押したら、登録になり料金を請求された。
- 「有料サイトの料金が未納になっている。」といったメールが送られてきた。

迷惑メールに関する相談

- 「お金を差し上げます。連絡をください。」というようなメールが送られてきた。
- 出会い系サイトなどの広告メールが頻繁に送られてきた。

名誉毀損、誹謗中傷に関する相談

- 掲示板サイトに誹謗中傷する内容を書き込まれた。
- ＳＮＳで相手とトラブルになり、悪口を書かれた。

不正アクセス等に関する相談

- ゲームのIDが盗まれてログインできなくなってしまった。
- 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。